

# SUSE Linux Enterprise Server

10 SP3

[www.novell.com](http://www.novell.com)

2009 年8 月28 日

安装和管理



# 安装和管理

所有内容的版权都属于 © Novell, Inc.

## 法律声明

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

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

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

有关 Novell 商标的列表，请参见 Novell 商标和服务标记列表

(<http://www.novell.com/company/legal/trademarks/tmlist.html>) [<http://www.novell.com/company/legal/trademarks/tmlist.html>]\* Linux 是 Linus Torvalds 的注册商标。所有第三方商标均属其各自所有者的财产。商标符号（®、™ 等）代表 Novell 商标；星号 (\*) 代表第三方商标。

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

# 目录

关于本指南	xv
部分 I 部署	1
1 SUSE Linux Enterprise 的规划	3
1.1 部署 SUSE Linux Enterprise 的注意事项	4
1.2 SUSE Linux Enterprise 的部署	5
1.3 SUSE Linux Enterprise 的运行	5
2 部署策略	7
2.1 最多部署 10 个工作站	7
2.2 最多部署 100 个工作站	9
2.3 部署 100 多个工作站	15
3 使用 YaST 进行安装	17
3.1 IBM POWER: 系统启动以进行网络安装	17
3.2 IBM System z: 系统启动以进行安装	18
3.3 系统启动以进行安装	18
3.4 安装工作流程	20
3.5 引导屏幕	20
3.6 语言	23
3.7 IBM System z: 硬盘配置	23
3.8 媒体检查	26
3.9 许可证协议	26
3.10 安装方式	26
3.11 时钟和时区	27
3.12 安装设置	27

3.13	执行安装	31
3.14	已安装系统的配置	34
3.15	图形登录	41
<b>4</b>	<b>远程安装</b>	<b>43</b>
4.1	远程安装的方案	43
4.2	设置存放安装源的服务器	51
4.3	准备目标系统的引导	59
4.4	引导用于安装的目标系统	69
4.5	监视安装过程	73
<b>5</b>	<b>自动安装</b>	<b>77</b>
5.1	简单的大规模安装	77
5.2	基于规则的自动安装	87
5.3	有关详细信息	92
<b>6</b>	<b>部署自定义预安装</b>	<b>93</b>
6.1	准备主计算机	94
6.2	自定义 Firstboot 安装	94
6.3	复制主安装	102
6.4	个性化安装	102
<b>7</b>	<b>高级磁盘设置</b>	<b>103</b>
7.1	LVM 配置	103
7.2	软 RAID 配置	111
<b>8</b>	<b>使用 YaST 进行系统配置</b>	<b>117</b>
8.1	YaST 语言	118
8.2	YaST 控制中心	118
8.3	软件	119
8.4	硬件	132
8.5	系统	138
8.6	网络设备	148
8.7	网络服务	148
8.8	AppArmor	154
8.9	安全性和用户	154
8.10	虚拟化	163
8.11	杂项	164
8.12	文本方式的 YaST	166
8.13	通过命令行管理 YaST	169



8.14	SaX2 . . . . .	172
8.15	故障诊断 . . . . .	177
8.16	更多信息 . . . . .	177
<b>9</b>	<b>通过 ZENworks 管理软件</b>	<b>179</b>
9.1	从命令行使用 rug 更新包 . . . . .	180
9.2	用 ZEN 工具管理包 . . . . .	183
9.3	更多信息 . . . . .	187
<b>10</b>	<b>更新 SUSE Linux Enterprise</b>	<b>189</b>
10.1	更新 SUSE Linux Enterprise . . . . .	189
10.2	安装服务包 . . . . .	191
10.3	从 V9 到 V10 的软件更改 . . . . .	201
	<b>部分 II 管理</b>	<b>215</b>
<b>11</b>	<b>OpenWBEM</b>	<b>217</b>
11.1	设置 OpenWBEM . . . . .	218
11.2	更改 OpenWBEM CIMOM 配置 . . . . .	223
11.3	更多信息 . . . . .	243
<b>12</b>	<b>经由 IP 网络的大容量储存 — iSCSI</b>	<b>245</b>
12.1	设置 iSCSI 目标 . . . . .	245
12.2	配置 iSCSI 发起程序 . . . . .	250
<b>13</b>	<b>iSNS for Linux 概述</b>	<b>255</b>
13.1	iSNS 的工作原理 . . . . .	255
13.2	iSNS for Linux 安装和设置 . . . . .	257
13.3	设置 iSNS . . . . .	257
13.4	更多信息 . . . . .	260
<b>14</b>	<b>Oracle Cluster File System 2</b>	<b>261</b>
14.1	O2CB 群集服务 . . . . .	262
14.2	磁盘的检测信号 . . . . .	263
14.3	内存中的文件系统 . . . . .	264
14.4	管理实用程序和命令 . . . . .	264
14.5	OCFS2 包 . . . . .	266
14.6	创建 OCFS2 卷 . . . . .	267

14.7	装入 OCF52 卷 . . . . .	271
14.8	其他信息 . . . . .	272
<b>15</b>	<b>Linux 中的访问控制列表</b>	<b>273</b>
15.1	传统文件权限 . . . . .	273
15.2	ACL 的优势 . . . . .	274
15.3	定义 . . . . .	275
15.4	处理 ACL . . . . .	276
15.5	应用程序中的 ACL 支持 . . . . .	283
15.6	更多信息 . . . . .	283
<b>16</b>	<b>RPM — 包管理器</b>	<b>285</b>
16.1	校验包真实性 . . . . .	285
16.2	管理包：安装、更新和卸载 . . . . .	286
16.3	RPM 和增补程序 . . . . .	287
16.4	增量 RPM 包 . . . . .	288
16.5	RPM 查询 . . . . .	289
16.6	安装和编译源包 . . . . .	292
16.7	使用 build 编译 RPM 包 . . . . .	294
16.8	用于 RPM 存档和 RPM 数据库的工具 . . . . .	295
<b>17</b>	<b>系统监视实用程序</b>	<b>297</b>
17.1	调试 . . . . .	297
17.2	文件和文件系统 . . . . .	299
17.3	硬件信息 . . . . .	302
17.4	联网 . . . . .	304
17.5	/proc文件系统 . . . . .	305
17.6	进程 . . . . .	308
17.7	系统信息 . . . . .	312
17.8	用户信息 . . . . .	316
17.9	时间和日期 . . . . .	316
<b>18</b>	<b>使用 Shell</b>	<b>317</b>
18.1	Bash shell 入门 . . . . .	317
18.2	用户和访问权限 . . . . .	328
18.3	重要的 Linux 命令 . . . . .	331
18.4	vi 编辑器 . . . . .	342

<b>部分 III 系统</b>	<b>347</b>
<b>19 64 位系统环境中的 32 位和 64 位应用程序</b>	<b>349</b>
19.1 运行时支持	350
19.2 软件开发	350
19.3 Biarch 平台上的软件编译	351
19.4 内核规范	353
<b>20 引导和配置 Linux 系统</b>	<b>355</b>
20.1 Linux 引导进程	355
20.2 init 进程	358
20.3 通过 /etc/sysconfig 配置系统	366
<b>21 引导加载程序</b>	<b>369</b>
21.1 选择引导加载程序	370
21.2 通过 GRUB 引导	370
21.3 使用 YaST 配置引导加载程序	378
21.4 卸载 Linux 引导加载程序	383
21.5 创建引导 CD	383
21.6 图形 SUSE 屏幕	384
21.7 查错	385
21.8 有关详细信息	386
<b>22 特别的系统功能组件</b>	<b>387</b>
22.1 特殊软件包的相关信息	387
22.2 虚拟控制台	394
22.3 键盘映射	394
22.4 语言和国家/地区特定的设置	395
<b>23 打印机操作</b>	<b>399</b>
23.1 打印系统工作流程	400
23.2 连接打印机的方法和协议	401
23.3 安装软件	401
23.4 设置打印机	402
23.5 网络打印机	406
23.6 图形打印接口	408
23.7 从命令行打印	409
23.8 SUSE Linux Enterprise 中的特殊功能	409
23.9 查错	413

<b>24 使用 udev 进行动态内核设备管理</b>	<b>421</b>
24.1 /dev 目录	421
24.2 内核 uevents 和 udev	422
24.3 驱动程序、内核模块和设备	422
24.4 引导和启动设备设置	423
24.5 调试 udev 事件	423
24.6 使用 udev 规则影响内核设备事件处理	424
24.7 永久设备命名	425
24.8 已替换的 hotplug 包	425
24.9 有关详细信息	426
<b>25 Linux 中的文件系统</b>	<b>429</b>
25.1 术语	429
25.2 Linux 中的主要文件系统	430
25.3 其他一些支持的文件系统	435
25.4 Linux 中对大型文件的支持	436
25.5 有关详细信息	437
<b>26 X Window 系统</b>	<b>439</b>
26.1 手动配置 X Window 系统	439
26.2 安装和配置字体	445
26.3 更多信息	450
<b>27 通过 PAM 进行身份验证</b>	<b>451</b>
27.1 PAM 配置文件的结构	451
27.2 sshd 的 PAM 配置	453
27.3 PAM 模块的配置	455
27.4 有关详细信息	457
<b>28 电源管理</b>	<b>459</b>
28.1 省电功能	459
28.2 APM	461
28.3 ACPI	462
28.4 硬盘的休眠	468
28.5 powersave 包	470
28.6 YaST 电源管理模块	478
<b>29 无线通讯</b>	<b>483</b>
29.1 无线 LAN	483

## 部分 IV 服务 493

### 30 基本联网知识 495

30.1	IP 地址和路由	498
30.2	IPv6 — 下一代的因特网	500
30.3	名称解析	508
30.4	使用 YaST 配置网络连接	509
30.5	在 SUSE Linux 上配置 VLAN 接口	525
30.6	使用 NetworkManager 管理网络连接	526
30.7	手动配置网络连接	528
30.8	作为拨号助手的 smpppd	542

### 31 网络中的 SLP 服务 545

31.1	激活 SLP	545
31.2	SUSE Linux Enterprise 中的 SLP 前端	546
31.3	通过 SLP 安装	546
31.4	用 SLP 提供服务	547
31.5	有关详细信息	548

### 32 使用 NTP 同步时间 549

32.1	使用 YaST 配置 NTP 客户机	549
32.2	在网络中配置 xntp	552
32.3	设置本地参考时钟	553

### 33 域名系统 555

33.1	DNS 术语	555
33.2	用 YaST 配置	556
33.3	启动名称服务器 BIND	564
33.4	配置文件 /etc/named.conf	566
33.5	区域文件	570
33.6	区域数据的动态更新	574
33.7	安全事务	574
33.8	DNS 安全性	575
33.9	更多信息	576

### 34 DHCP 577

34.1	使用 YaST 配置 DHCP 服务器	578
34.2	DHCP 软件包	586
34.3	DHCP 服务器 dhcpd	586
34.4	更多信息	590

<b>35 使用 NIS</b>	<b>591</b>
35.1 配置 NIS 服务器	591
35.2 配置 NIS 客户机	597
<b>36 LDAP - 目录服务</b>	<b>599</b>
36.1 对比 LDAP 和 NIS	600
36.2 LDAP 目录树的结构	601
36.3 使用 slapd.conf 配置服务器	604
36.4 LDAP 目录中的数据处理	609
36.5 使用 YaST 配置 LDAP 服务器	613
36.6 使用 YaST 配置 LDAP 客户机	617
36.7 在 YaST 中配置 LDAP 用户和组	624
36.8 浏览 LDAP 目录树	625
36.9 有关详细信息	627
<b>37 Samba</b>	<b>629</b>
37.1 术语	629
37.2 启动和停止 Samba	630
37.3 配置 Samba 服务器	631
37.4 配置客户机	636
37.5 将 Samba 用作登录服务器	637
37.6 带有 Active Directory 的网络中的 Samba 服务器	638
37.7 将 Windows NT Server 迁移到 Samba	640
37.8 有关详细信息	642
<b>38 通过 NFS 共享文件系统</b>	<b>645</b>
38.1 安装所需软件	645
38.2 使用 YaST 导入文件系统	646
38.3 手动导入文件系统	647
38.4 使用 YaST 导出文件系统	648
38.5 手动导出文件系统	653
38.6 采用 Kerberos 的 NFS	656
38.7 更多信息	656
<b>39 文件同步</b>	<b>657</b>
39.1 可用的数据同步软件	657
39.2 选择程序时的决定性因素	658
39.3 CVS 简介	661
39.4 rsync 简介	664

<b>40</b>	<b>Apache HTTP 服务器</b>	<b>667</b>
40.1	快速入门	667
40.2	配置 Apache	669
40.3	启动和停止 Apache	682
40.4	安装、激活和配置模块	683
40.5	使 CGI 脚本运行	690
40.6	使用 SSL 设置安全性 Web 服务器	692
40.7	避免安全性问题	698
40.8	查错	699
40.9	更多信息	700
<b>41</b>	<b>代理服务器 Squid</b>	<b>703</b>
41.1	有关代理缓存的一些事实	703
41.2	系统要求	705
41.3	启动 Squid	706
41.4	配置文件 /etc/squid/squid.conf	708
41.5	配置透明代理	713
41.6	cachemgr.cgi	716
41.7	squidGuard	717
41.8	使用 Calamaris 生成缓存报告	719
41.9	更多信息	720
<b>部分 V</b>	<b>安全性</b>	<b>721</b>
<b>42</b>	<b>管理 X.509 认证</b>	<b>723</b>
42.1	数字认证的原理	723
42.2	用于 CA 管理的 YaST 模块	727
<b>43</b>	<b>伪装和防火墙</b>	<b>737</b>
43.1	使用 iptables 过滤包	737
43.2	关于伪装的基础知识	739
43.3	防火墙基础知识	740
43.4	SUSEfirewall2	741
43.5	有关详细信息	745
<b>44</b>	<b>SSH: 安全性网络操作</b>	<b>747</b>
44.1	OpenSSH 包	747
44.2	ssh 程序	748
44.3	scp — 安全复制	748
44.4	sftp — 安全的文件传送	749

44.5	SSH 守护程序 (sshd) — 服务器端 . . . . .	749
44.6	SSH 身份验证机制 . . . . .	750
44.7	X、身份验证和转发机制 . . . . .	751
<b>45</b>	<b>网络身份验证 — Kerberos</b>	<b>753</b>
45.1	Kerberos 术语 . . . . .	753
45.2	Kerberos 的工作原理 . . . . .	755
45.3	从用户的角度讨论 Kerberos . . . . .	758
45.4	有关详细信息 . . . . .	758
<b>46</b>	<b>安装和管理 Kerberos</b>	<b>761</b>
46.1	选择 Kerberos 领域 . . . . .	761
46.2	设置 KDC 硬件 . . . . .	762
46.3	时钟同步 . . . . .	763
46.4	配置 KDC . . . . .	763
46.5	手动配置 Kerberos 客户机 . . . . .	766
46.6	使用 YaST 配置 Kerberos 客户机 . . . . .	768
46.7	远程 Kerberos 管理 . . . . .	770
46.8	创建 Kerberos 主机主体 . . . . .	772
46.9	启用 Kerberos 的 PAM 支持 . . . . .	773
46.10	配置 SSH 进行 Kerberos 身份验证 . . . . .	774
46.11	使用 LDAP 和 Kerberos . . . . .	775
<b>47</b>	<b>对分区和文件进行加密</b>	<b>779</b>
47.1	用 YaST 设置已加密的文件系统 . . . . .	780
47.2	使用加密的用户主目录 . . . . .	782
47.3	使用 vi 加密单个 ASCII 文本文件 . . . . .	783
<b>48</b>	<b>通过 AppArmor 限制特权</b>	<b>785</b>
48.1	安装 Novell AppArmor . . . . .	786
48.2	启用和禁用 Novell AppArmor . . . . .	786
48.3	构建应用程序的配置文件入门 . . . . .	787
<b>49</b>	<b>安全性和机密性</b>	<b>795</b>
49.1	本地安全和网络安全 . . . . .	796
49.2	一些常用的安全提示和技巧 . . . . .	803
49.3	使用中央安全报告地址 . . . . .	805



<b>部分 VI 查错</b>	<b>807</b>
<b>50 帮助和文档</b>	<b>809</b>
50.1 使用 SUSE 帮助中心 . . . . .	809
50.2 手册页 . . . . .	812
50.3 信息页 . . . . .	813
50.4 Linux 文档计划 . . . . .	814
50.5 Wikipedia: 免费的联机百科全书 . . . . .	814
50.6 指南和手册 . . . . .	815
50.7 包文档 . . . . .	815
50.8 Usenet . . . . .	816
50.9 标准和规范 . . . . .	817
<b>51 常见问题及其解决方案</b>	<b>819</b>
51.1 查找和收集信息 . . . . .	819
51.2 安装问题 . . . . .	821
51.3 引导问题 . . . . .	829
51.4 登录问题 . . . . .	831
51.5 网络问题 . . . . .	837
51.6 数据问题 . . . . .	841
51.7 IBM System z: 将 initrd 用作救援系统 . . . . .	852
<b>索引</b>	<b>857</b>



# 关于本指南

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

本指南包含如下内容：

## 部署

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

## 管理

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

## 系统

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

## 服务

SUSE Linux Enterprise 被设计为一个网络操作系统。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 客户机和服务器在内的异构环境中。

## 安全性

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

## 查错

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

# 1 反馈

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

# 2 文档更新

关于此文档的最新版本，请参见 SUSE Linux Enterprise Server 网站 [<http://www.novell.com/documentation/sles10/index.html>]。

# 3 其他文档

有关本产品的附加文档，请参见 <http://www.novell.com/documentation/sles10/index.html>：

## 入门指南

有关安装类型和工作流程的基本信息。

## *Architecture-Specific Information*

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

## *Novell AppArmor Administration Guide*

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

## *Storage Administration Guide*

管理 SUSE Linux Enterprise 上的不同类型储存设备的介绍。

## *Heartbeat Guide*

用 Heartbeat 设置高可用性场景的深入管理指南。

### *Novell Virtualization Technology User Guide*

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

有关 SUSE® Linux Enterprise Desktop 产品文档概述，请参见<http://www.novell.com/documentation/sled10/index.html>。以下手册仅用于 SUSE Linux Enterprise Desktop：

### *GNOME User Guide*

GNOME 桌面及其最重要的应用程序的综合指南。

### *KDE User Guide*

KDE 桌面及其最重要的应用程序的综合指南。

### *Deployment Guide*

适用于管理员的有关 SUSE Linux Enterprise Desktop 部署和管理的详细指导。

### *Novell AppArmor Administration Guide*

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

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

## 4 文档约定

以下是本手册中使用的版式约定：

- `/etc/passwd`：文件名和目录名
- `placeholder`：将 `placeholder` 替换为实际值
- `PATH`：环境变量 `PATH`
- `ls`、`--help`：命令、选项和参数
- `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 ipf:** 本段只与指定的体系结构有关。箭头标记文本块的开始位置和结束位置。 ◀
  - ▶ **ipseries s390 zseries:** 本段只与指定的体系结构有关。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. 部署





# SUSE Linux Enterprise 的规划

不管是在现有的 IT 环境中还是作为全新的批量部署而实施操作系统，都必须仔细地加以准备。通过 SUSE Linux Enterprise 10 获得了大量新功能。在这不可能介绍它所有的新功能。下面只是列出可能相关的主要增强功能。

## Xen 3.0 虚拟化

在简单服务器中运行许多虚拟机，每一个都带有自己的操作系统实例。有关此技术的更多信息，请参见 <http://www.novell.com/documentation/sles10/index.html> 上的虚拟化手册。

## YaST

已为 YaST 开发几个新的配置选项。它们通常在关于相关技术的章节中描述。

## 用 openWBEM 来进行 CIM 管理

通用信息模型对象管理器 (CIMON) 是一个基于 Web 的企业管理实用程序。它提供了一个成熟的管理框架。另请参见第 11 章 *OpenWBEM* [217]。

## SPident

管理实用程序 SPident 提供了对已安装软件库的概览，并阐明了系统现有服务包的水平。

## 目录服务

有几种可用的 LDAP 兼容目录服务：

- Microsoft Active Directory
- OpenLDAP

## Novell AppArmor

使用 Novell AppArmor 技术强化您的系统。该服务 *Novell AppArmor Administration Guide* ([↑Novell AppArmor Administration Guide](#)) 中有详细描述。

## iSCSI

iSCSI 提供了一种简便且价格合理的解决方案，可将 Linux 计算机连接到中央储存系统。有关 iSCSI 的更多信息，请参见 [第 12 章 经由 IP 网络的大容量储存 — iSCSI](#) [245]。

## Network File System v4

从版本 10 开始，SUSE Linux Enterprise 在版本 4 中也支持 NFS v4。这为您提供了性能的改进、强大的安全性和“全状态”协议。另请参见 [第 38 章 通过 NFS 共享文件系统](#) [645]。

## Oracle Cluster File System 2

OCFS2 是一个一般用途的日记文件系统，与 Linux 2.6 内核和更高版本完全集成。中有 OCFS2 的概述。 [第 14 章 Oracle Cluster File System 2](#) [261]

## Heartbeat 2

Heartbeat 2 提供了一个群集成员资格和消息传递的基础架构。 *Heartbeat Guide* 中说明了此类群集的设置。

## Multipath I/O

设备映射多路径 IO 的特点是为各种安装自动配置子系统。有关细节，请参见 *Storage Administration Guide*（储存管理指南）中关于多路径 I/O 的章节。

## Linux Kernel Crash Dump

使用 Kexec 和 Kdump 可以轻松地调试与内核相关的问题。此技术可用于 x86、AMD64、Intel 64 和 POWER 平台。

# 1.1 部署 SUSE Linux Enterprise 的注意事项

在开始计划时，您必须尝试定义项目目标和所需功能。必须对每个项目分别设定，但下面这些问题必须回答：

- 要安装多少？根据这个问题，最好的部署方法也是不同的。另请参见 [第 2 章 部署策略](#) [7]。

- 系统会处于恶劣的环境下吗？在**第49章 安全性和机密性**[795]中查看一下结果的概要。
- 如何定时更新？为注册用户联机提供所有增补程序。在<http://support.novell.com/patches.html> 中查找注册和增补程序支持数据库。
- 本地安装需要帮助吗？Novell 提供对 SUSE Linux Enterprise 所有主题的培训、支持和咨询。有关详细信息，请参见<http://www.novell.com/products/server/>。
- 需要第三方的产品吗？确定所需产品在所需平台上可以支持。Novell 也可以在需要时就在不同平台上安装软件提供帮助。

## 1.2 SUSE Linux Enterprise 的部署

要确保您的系统完好地运行，请始终使用认证硬件。硬件认证过程是一个持续的过程，认证硬件的数据库也是定期更新的。<http://developer.novell.com/yessearch/Search.jsp>上有认证硬件的搜索表单。

按照所需安装的数量，使用安装服务器或完全自动安装是有利的。看一下**第2章 部署策略** [7]以了解详细信息。当使用 Xen 虚拟化技术时，网络根文件系统或网络储存解决方案（如 iSCSI）应该加以考虑。另请参见**第12章 经由 IP 网络的大容量储存 — iSCSI** [245]。

SUSE Linux Enterprise 可为您提供大量多样化的服务。在本书的**关于本指南** [xv] 中，查看本文档的概述。多数所需配置都可以使用 YaST（SUSE 配置实用程序）执行。此外，在相应的章节里也描述了许多手动配置。

除了一般软件安装之外，还应考虑培训系统的最终用户和支持员工。

## 1.3 SUSE Linux Enterprise 的运行

SUSE Linux Enterprise 操作系统是一个经过良好测试的稳定系统。遗憾的是，它不会防止硬件故障或运行停止及数据丢失的其他原因。对于任何可能发生数据丢失的重要计算任务，应定期备份。

为了更安全地工作，您必须定期更新所有操作的计算机。如果有非常重要的服务器，可能应运行另一台一模一样的计算机，可以在真实系统上应用所有更改之前先测试。这也使您可能在出现硬件故障时切换计算机。

# 部署策略

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

## 2.1 最多部署 10 个工作站

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

### 从 SUSE Linux Enterprise 媒体进行安装 [7]

如果想安装单个断开连接的工作站，请考虑使用此方法。

### 通过使用 SLP 来从网络服务器进行安装 [8]

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

### 从网络服务器进行安装 [8]

如果想安装一个工作站或几个工作站并且网络安装服务器可用，请考虑使用此方法。

**表 2.1** 从 SUSE Linux Enterprise 媒体进行安装

---

安装源	SUSE Linux Enterprise 媒体工具包
-----	-----------------------------

要求手动交互的任务	<ul style="list-style-type: none"> <li>• 插入安装媒体</li> <li>• 引导安装目标</li> <li>• 更改媒体</li> <li>• 决定 YaST 安装范围</li> <li>• 用 YaST 系统配置系统</li> </ul>
远程控制的任务	无
细节	第 3.3.2 节 “从 SUSE Linux Enterprise 媒体进行安装” [19]

**表 2.2** 通过使用 SLP 来从网络服务器进行安装

安装源	含有 SUSE Linux Enterprise 安装媒体的网络安装服务器
要求手动交互的任务	<ul style="list-style-type: none"> <li>• 插入引导磁盘</li> <li>• 引导安装目标</li> <li>• 决定 YaST 安装范围</li> <li>• 用 YaST 配置系统</li> </ul>
远程控制的任务	无，但此方法可以与 VNC 组合
细节	第 3.3.3 节 “通过使用 SLP 来从网络服务器进行安装” [19]

**表 2.3** 从网络服务器进行安装

安装源	含有 SUSE Linux Enterprise 安装媒体的网络安装服务器
-----	---------------------------------------

要求手动交互的任务

- 插入引导磁盘
- 提供引导选项
- 引导安装目标
- 决定 yast 安装范围
- 用 YaST 配置系统

远程控制的任务

无，但此方法可以与 VNC 组合

细节

第 3.3.4 节 “从没有 SLP 的网络源安装” [19]

---

## 2.2 最多部署 100 个工作站

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

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

从以下选项中选择：

### 通过 VNC—静态网络配置的简单远程安装 [10]

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

### 通过 VNC—动态网络配置的简单远程安装 [11]

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

### 通过 VNC—PXE 引导和 LAN 唤醒的远程安装 [11]

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

通过 SSH—静态网络配置的简单远程安装 [12]

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

通过 SSH—静态网络配置的简单远程安装 [12]

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

通过 SSH—PXE 引导和 LAN 唤醒的远程安装 [13]

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

简单的大规模安装 [14]

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

基于规则的自动安装 [14]

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

表 2.4 通过 VNC—静态网络配置的简单远程安装

安装源	网络
准备工作	<ul style="list-style-type: none"><li>• 设置安装源</li><li>• 从安装媒体引导</li></ul>
控制和监视	远程：VNC
最适合	有不同硬件的小规模和中等规模部署情况



缺点	<ul style="list-style-type: none"> <li>• 每台计算机必须单独安装</li> <li>• 引导需要物理访问</li> </ul>
细节	第 4.1.1 节 “通过 VNC 静态网络配置进行简单远程安装” [44]

表 2.5 通过 VNC— 动态网络配置的简单远程安装

安装源	网络
准备工作	<ul style="list-style-type: none"> <li>• 设置安装源</li> <li>• 从安装媒体引导</li> </ul>
控制和监视	远程：VNC
最适合	有不同硬件的小规模和中等规模部署情况
缺点	<ul style="list-style-type: none"> <li>• 每台计算机必须单独安装</li> <li>• 引导需要物理访问</li> </ul>
细节	第 4.1.2 节 “通过 VNC 动态网络配置进行简单远程安装” [45]

表 2.6 通过 VNC— PXE 引导和 LAN 唤醒的远程安装

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

控制和监视	远程：VNC
最适合	<ul style="list-style-type: none"> <li>• 有不同硬件的小规模和中等规模部署情况</li> <li>• 完全远程安装；跨站点部署</li> </ul>
缺点	每台计算机必须手动安装
细节	第 4.1.3 节 “通过 VNC—PXE Boot 和“网络唤醒”进行远程安装” [46]

**表 2.7** 通过 SSH— 静态网络配置的简单远程安装

安装源	网络
准备工作	<ul style="list-style-type: none"> <li>• 设置安装源</li> <li>• 从安装媒体引导</li> </ul>
控制和监视	远程：SSH
最适合	<ul style="list-style-type: none"> <li>• 有不同硬件的小规模和中等规模部署情况</li> <li>• 低带宽连接到目标</li> </ul>
缺点	<ul style="list-style-type: none"> <li>• 每台计算机必须单独安装</li> <li>• 引导需要物理访问</li> </ul>
细节	第 4.1.4 节 “通过 SSH 静态网络配置进行简单远程安装” [47]

**表 2.8** 通过 SSH— 静态网络配置的简单远程安装

安装源	网络
-----	----

准备工作	<ul style="list-style-type: none"> <li>• 设置安装源</li> <li>• 从安装媒体引导</li> </ul>
控制和监视	远程: SSH
最适合	<ul style="list-style-type: none"> <li>• 有不同硬件的小规模和中等规模部署情况</li> <li>• 低带宽连接到目标</li> </ul>
缺点	<ul style="list-style-type: none"> <li>• 每台计算机必须单独安装</li> <li>• 引导需要物理访问</li> </ul>
细节	第 4.1.5 节“通过 SSH 动态网络配置进行简单远程安装” [49]

表 2.9 通过 SSH—PXE 引导和 LAN 唤醒的远程安装

安装源	网络
准备工作	<ul style="list-style-type: none"> <li>• 设置安装源</li> <li>• 配置 DHCP、TFTP，PXE 引导和 WOL</li> <li>• 从网络引导</li> </ul>
控制和监视	远程: SSH
最适合	<ul style="list-style-type: none"> <li>• 有不同硬件的小规模和中等规模部署情况</li> <li>• 完全远程安装；跨站点部署</li> <li>• 低带宽连接到目标</li> </ul>

缺点	每台计算机必须单独安装
细节	第 4.1.6 节 “通过 SSH—PXE Boot 和“网络唤醒”进行远程安装” [50]

**表 2.10** 简单的大规模安装

安装源	最好是网络
准备工作	<ul style="list-style-type: none"> <li>• 收集硬件信息</li> <li>• 创建 AutoYaST 配置文件</li> <li>• 设置安装服务器</li> <li>• 分发配置文件</li> <li>• 设置网络引导（DHCP、TFTP、PXE、WOL）</li> </ul> <p>或</p> <p>从安装媒体引导目标</p>
控制和监视	通过 VNC 或 SSH 本地或远程
最适合	<ul style="list-style-type: none"> <li>• 大规模部署情况</li> <li>• 相同硬件</li> <li>• 不能访问系统（网络引导）</li> </ul>
缺点	仅适用于有相同硬件的计算机
细节	第 5.1 节 “简单的大规模安装” [77]

**表 2.11** 基于规则的自动安装

安装源	最好是网络
-----	-------

准备工作	<ul style="list-style-type: none"><li>• 收集硬件信息</li><li>• 创建 AutoYaST 配置文件</li><li>• 创建 AutoYaST 规则</li><li>• 设置安装服务器</li><li>• 分发配置文件</li><li>• 设置网络引导（DHCP、TFTP、PXE、WOL）</li></ul> <p>或</p> <p>从安装媒体引导目标</p>
控制和监视	通过 SSH 或 VNC 本地或远程
最适合	<ul style="list-style-type: none"><li>• 不同硬件</li><li>• 跨站点部署</li></ul>
缺点	复杂规则安装
细节	第 5.2 节 “基于规则的自动安装” [87]

---

## 2.3 部署 100 多个工作站

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

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



## 使用 YaST 进行安装

在准备好硬件以安装 SUSE Linux Enterprise®（如 *Architecture-Specific Information* 手册中所述）并与安装系统建立连接之后，将会显示 SUSE Linux Enterprise 系统助手 YaST 的界面。YaST 在整个安装和配置过程中为您全程指导。

### 3.1 IBM POWER：系统启动以进行网络安装

对于 IBM POWER 平台，系统按 *Architecture-Specific Information* 手册中所述进行初始化 (IPL)。对于网络安装，SUSE Linux Enterprise Server 不在这些系统上显示启动屏幕或引导加载程序命令行。在安装期间，请手动装载内核。在通过 VNC、X 或 SSH 与安装系统建立连接后，YaST 会立刻启动安装屏幕。因为无启动屏幕或引导加载程序命令行，内核或引导参数无法在屏幕上输入，但必须使用 `mkzimage_cmdline` 实用程序包含在内核映像中。有关说明，请参见 *Architecture-Specific Information* 手册中的“准备”一章。

---

**提示：IBM POWER：** 执行下面的步骤

要进行安装，请按照从 [第 3.6 节 “语言”](#) [23] 开始介绍的过程使用 YaST 进行安装。

---

# 3.2 IBM System z：系统启动以进行安装

对于 IBM System z 平台，系统按 *Architecture-Specific Information* 手册中所述进行初始化 (IPL)。SUSE Linux Enterprise 不在这些系统上显示启动屏幕。在安装期间，需要手动装载内核、initrd 和 parmfile。一旦通过 VNC、X 或 SSH 建立了与安装系统的连接，YaST 就会立即启动并显示安装屏幕。由于没有启动屏幕，所以不能在屏幕上输入内核或引导参数，但必须在 parmfile 中指定它们（请参见附录 A, *Appendix (↑Architecture-Specific Information)* 中的 parmfile 信息）。

---

**提示：IBM System z：** 下面的步骤

要进行安装，请按照从 **第 3.6 节 “语言”** [23] 开始介绍的过程使用 YaST 进行安装。

---

## 3.3 系统启动以进行安装

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

### 3.3.1 引导选项

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

**表 3.1** 引导选项

引导选项	说明
DVD/CD-ROM	这是最简单的引导选项。如果系统具有 Linux 支持的本地 CD/DVD-ROM 驱动器，则可以使用此选项。



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

## 3.3.2 从 SUSE Linux Enterprise 媒体进行安装

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

## 3.3.3 通过使用 SLP 来从网络服务器进行安装

如果您的网络设置支持 OpenSLP，并且已配置网络安装源通过 OpenSLP 通知自己（在第 4.2 节“设置存放安装源的服务器”[51]中有说明），请从媒体或使用其他引导选项引导系统。在引导屏幕中，选择所需的安装选项。按 **F4**，然后选择 *SLP*。

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

## 3.3.4 从没有 SLP 的网络源安装

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

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

## 3.4 安装工作流程

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

## 3.5 引导屏幕

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

### 安装

常规安装方式。将启用所有常用的硬件功能。将启用所有最新的硬件功能。

### 安装 — 禁用 ACPI

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

### 安装 — 禁用本地 APIC

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

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

### 安装 — 安全设置

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

## 救援系统

启动不带图形用户界面的最小 Linux 系统。有关详细信息，请参见“[使用救援系统](#)”一节 [848]。

## 内存测试

通过反复的读写操作过程来测试系统的 RAM。通过重引导来终止测试。有关详细信息，请参见[第 51.2.5 节 “无法引导”](#) [825]。

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

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

### F1 帮助

获取引导屏幕的活动元素的上下文相关帮助。

### F2 语言

选择安装的显示语言。默认语言为英语。

### F3 视频方式

选择安装的多种图形显示方式。如果图形安装出现问题，则选择文本方式。

### F4 源

通常情况下都是从插入的安装媒体来执行安装。在此处，选择其他源，如 FTP 或 NFS 服务器。如果在具有 SLP 服务器的网络中执行安装，则可以使用此选项选择服务器上可用的安装源。有关 SLP 的更多详细信息，请参见[第 31 章 网络中的 SLP 服务](#) [545]。

### F5 驱动程序

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

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

---

**提示：无鼠标安装**

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

---

## 3.5.1 提供访问 SMT 服务器的数据

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

**smturl**

SMT 服务器的 URL。该 URL 具有固定的格式，为

`https://FQN/center/regsvc/` *FQN* 必须是 SMT 服务器的完全限定的主机名。示例：

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

**smtcert**

SMT 服务器证书的位置。指定以下位置之一：

**URL**

可以下载证书的远程位置（`http`、`https` 或 `ftp`）。示例：

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

**软盘**

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

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

**本地路径**

本地计算机上证书的绝对路径。示例：

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

**交互式**

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

```
smtcert=ask
```

#### 停用证书安装

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

```
smtcert=done
```

---

### 警告：当心键入错误

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

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

---

## 3.6 语言

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

您可在稍后的安装过程中更改语言，如[第 3.12 节“安装设置”](#) [27]中所述。有关已安装系统中语言设置的信息，请参见[第 8.1 节“YaST 语言”](#) [118]。

## 3.7 IBM System z：硬盘配置

当在 IBM System z 平台上进行安装时，在语言选择对话框之后会出现一个用来配置挂接硬盘的对话框。选择 DASD、光纤通道挂接式 SCSI 磁盘 (zFCP) 或 iSCSI 来安装 SUSE Linux Enterprise。

选择配置 *DASD* 磁盘后，概述列出了所有可用的 DASD。要更清楚地显示可用设备，可使用列表上方的输入字段来指定要显示的通道的范围。要根据这一范围过滤此列表，请选择过滤器。请参见[图 3.1 “IBM System z：选择 DASD”](#) [24]。

图 3.1 IBM System z：选择 DASD

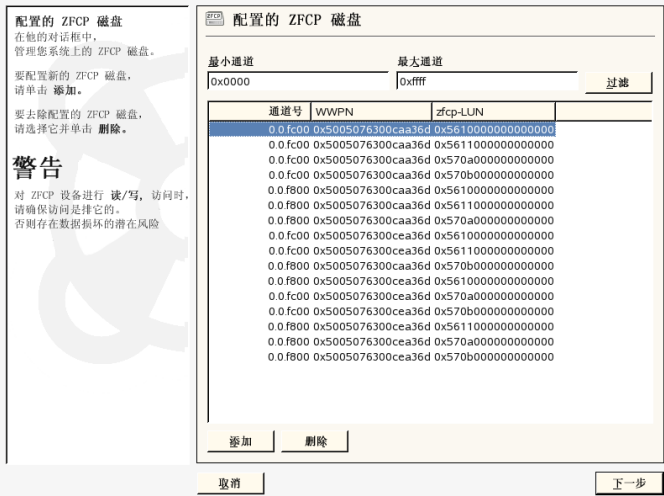


现在指定用于安装的 DASD，方法是在列表中选择相应的项，然后单击 **选择或取消选择**。此后，激活 DASD 并使其可用于安装，方法是选择 **执行操作 > 激活**。请参见图 3.2 “IBM System z：激活 DASD” [24]。要格式化 DASD，请立即选择 **执行操作 > 格式化**或稍后使用 YaST 分区程序（如中第 8.5.7 节 “使用 YaST 分区程序” [139]所述）。

图 3.2 IBM System z：激活 DASD



图 3.3 IBM System z：可用 zFCP 磁盘概述



要使用 zFCP 磁盘进行 SUSE Linux Enterprise 安装，请在选择对话框中选择**配置 ZFCP 磁盘**。这样将打开一个对话框，其中显示系统上可用 zFCP 磁盘的列表。在此对话框中，选择**添加**打开另一个对话框，然后在该对话框中输入 zFCP 参数。请参见图 3.3 “**IBM System z：可用 zFCP 磁盘概述**” [25]。

要使 zFCP 磁盘可用于 SUSE Linux Enterprise 安装，从下拉列表中选择一个可用的**通道号**。获取 **WWPN**（全球端口号）和获取 **LUN**（逻辑单元号）分别返回可用 **WWPN** 和 **FCP-LUN** 的列表，以供选择。完成后，选择下一步退出 zFCP 对话框，然后选择**完成**退出常规硬盘配置对话框，接下来继续进行其他配置。

**提示：在后续阶段添加 DASD 或 zFCP 磁盘**

不仅在安装工作流程中可以添加 **DASD** 或 **zFCP** 磁盘，还可以在显示安装建议书时添加。要在该阶段添加磁盘，单击**专家**，然后向下滚动。**DASD** 和 **zFCP** 项显示在最底部。

添加磁盘后，重新读取分区表。返回到安装建议书屏幕，选择分区，然后选择**重读取分区表**。此操作将读取新的分区表，并重设置所有先前输入的信息。

## 3.8 媒体检查

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

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

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

---

### 警告：媒体检查失败

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

---

如果媒体检查的结果表明没有问题，请单击*下一步*继续安装。

## 3.9 许可证协议

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

## 3.10 安装方式

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

### 新安装

选择该选项从头开始新安装。

### 更新现有系统

选择该选项更新到较新的版本。关于系统更新的更多信息，请参见[第 10 章更新 SUSE Linux Enterprise](#) [189]。



### 其他选项

该选项使您可以放弃安装和引导，或者修复已安装的系统。要引导已安装的 SUSE Linux Enterprise，请选择 *引导已安装的系统*。如果引导已安装的 SUSE Linux Enterprise 时有问题，请参见 [第 51.3 节 “引导问题”](#) [829]。

为修复引导失败的已安装系统，请选择 *修复已安装的系统*。有关系统修复选项的说明，请参见 [“使用 YaST 系统修复”一节](#) [843]。

---

### 注意：更新已安装系统

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

---

初次安装过程中，您可以选择和 SUSE Linux Enterprise 系统一起安装附加产品，或者以后任何时候安装，如 [第 8.3.2 节 “安装附加产品”](#) [125] 中所述。附加产品是 SUSE Linux Enterprise 的扩展。附加产品可包含专有第三方产品或您系统的其他软件。

要在 SUSE Linux Enterprise 的安装中包含附加产品，请选择 *包含来自独立媒体的附加产品*，并单击下一步。在下个对话框中单击 *添加*，选择用于安装附加产品的来源。有许多来源类型可用，例如 CD、FTP 或本地目录。添加外接式媒体后，可能需要同意第三方产品的附加许可证协议。

## 3.11 时钟和时区

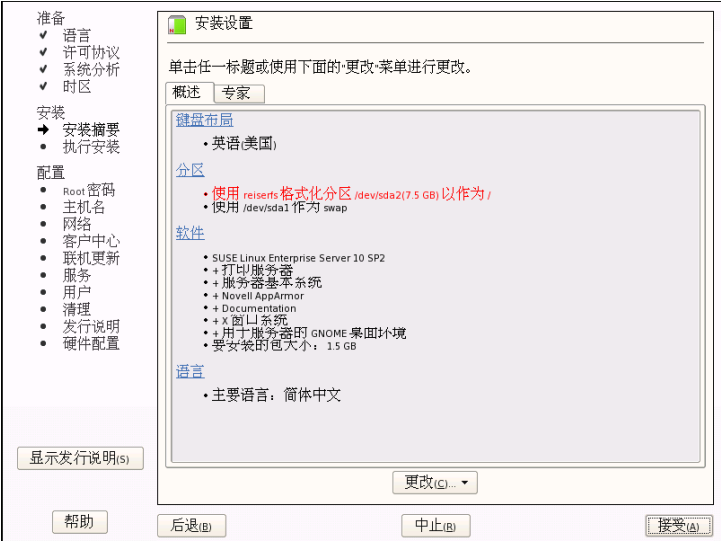
在此对话框中，从列表中选择您所在地区和时区。在安装期间，将根据所选的安装语言预先选择这两项。在 *硬件时钟设置* 下选择 *本地时间* 和 *UTC(GMT)*。此选择取决于计算机上 BIOS 硬件时钟的设置。如果将它设置为与 UTC 相对应的 GMT，则您的系统便可以依赖 SUSE Linux Enterprise 在标准时间和夏令时之间自动切换。单击 *更改* 可设置当前日期和时间。安装后，单击 *下一步* 继续安装。

## 3.12 安装设置

在进行了全面的系统分析之后，YaST 将显示所有安装设置的合理建议。可在 *概述* 选项卡中更改基本设置，*专家* 选项卡中有高级选项。要修改建议的值，请单击 *更改*，然后选择要更改的类别，或单击其中一个标题。在完成了对显示在

这些对话框中的项的配置之后，总是会返回到摘要窗口，而且每次返回此窗口都会进行相应的更新。

图 3.4 安装设置



**提示：**将更改重设置为默认值

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

### 3.12.1 概述

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

#### 键盘布局

要更改键盘布局，选择键盘布局。默认情况下，布局对应于安装时所选的语言。从列表中选择键盘布局。使用对话框底部的测试字段检查是否可以正确输入该布局的特殊字符。在第 8.4.10 节“键盘布局”[135]中查找有关更改键盘布局的更多信息。完成后，单击接受返回到安装摘要。

► **zseries:** 在 IBM System z 平台上，安装是从远程终端执行的。这样的主机没有本地连接键盘或鼠标。 ◀

## 分区

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

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

要对提议进行微小改动，请选择该提议中的**基础分区设置**，并在下个对话框中调整分区。要获得完全不同的分区，请选择**创建自定义分区设置**。在下一个对话框中，请选择要分区的特定磁盘，或者如果您想要访问所有磁盘，请选择**自定义分区**。有关自定义分区的更多信息，请参考 [第 8.5.7 节 “使用 YaST 分区程序”](#) [139] SUSE Linux Enterprise Server 文档。YaST 分区程序还提供用于创建 LVM 的工具。要创建 LVM 建议书，选择**创建基于 LVM 的建议书**。有关 LVM 的更多信息，请参见 [第 7.1 节 “LVM 配置”](#) [103]。

---

**注意：使用 z/VM 中的迷你磁盘**

如果 SUSE Linux Enterprise Server 安装在 z/VM 中驻留在同一物理磁盘上的迷你磁盘中，迷你磁盘的访问路径 (/dev/disk/by-id/) 不是唯一的，而是物理磁盘的 ID。所以，如果同一物理磁盘上有两个或更多迷你磁盘，它们的 ID 都相同。

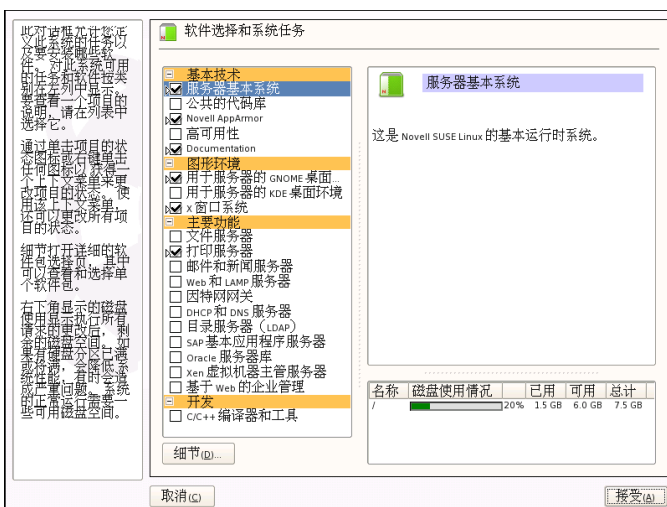
要避免在装入迷你磁盘时发生问题，请始终“按路径”或“按 UUID”装入它们。

---

## 软件

SUSE Linux Enterprise 包含许多用于各种应用目的的软件包。在建议窗口中单击**软件**以启动软件选择并根据需要修改安装范围。从中间的列表选择您的模式，并在窗口右侧部分中查看说明。每种模式都包含一些特定功能所需的软件包（例如多媒体或办公软件）。如果希望根据要安装的软件包来获取更为详细的选项，请选择**细节**切换到 YaST 软件管理器。请参见 [图 3.5 “使用 YaST 软件管理器安装和删除软件”](#) [30]。

**图 3.5** 使用 YaST 软件管理器安装和删除软件



以后任何时候，您都可以安装其他软件包，或从系统中删除软件包。有关详细信息，请参见第 8.3.1 节“安装和删除软件”[119]。

### 注意：默认桌面

SUSE Linux Enterprise 的默认桌面为 GNOME。要安装 KDE，请单击 **软件**，然后从图形环境选择 **KDE 桌面环境**。

## 语言

要更改系统语言或配置对第二语言的支持，请选择**语言**。从列表中选择一种语言。主语言用作系统语言。选择一种或多种次要语言，用于在无需安装其他包的情况下，即可随时切换到这些语言之一。有关详细信息，请参见**第 8.5.15 节“语言选择”** [147]。

### 3.12.2 专家

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

## 系统

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

## 附加产品

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

## 引导

- ▶ **zseries:** 此模块无法用于在 IBM System z 平台上配置引导加载程序 (zipl)。
- ◀

YaST 会为您的系统建议引导配置。通常，您可以保持这些设置不变。但是，如果您需要自定义设置，则可修改对系统的建议。有关信息，请参见 [第 21.3 节 “使用 YaST 配置引导加载程序”](#) [378]。

## 时区

这和先前在 [第 3.11 节 “时钟和时区”](#) [27] 中显示的配置相同。

## 默认运行级别

SUSE Linux Enterprise 可以引导到不同的运行级别。通常情况下无需更改此处的任何内容，但是如果需要，可使用此对话框设置默认的运行级别。有关运行级别配置的信息，请参见 [第 20.2.3 节 “使用 YaST 配置系统服务（运行级别）”](#) [365]。

# 3.13 执行安装

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

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

## 3.13.1 IBM System z: 对已安装系统执行 IPL

在多数情况下，YaST 会自动重引导到 IBM System z 平台上安装的系统。这种情况的已知例外情况是，在一台计算机上的 LPAR 早于 z9 或 z/VM 早于版本 5.3，并且引导加载程序驻留在这种环境下的 FCP 设备中。引导加载程序写入存放 `/boot` 目录的设备中。如果 `/boot` 不在独立的分区上，则在与根文件系统 / 相同的分区上。

如果无法自动重引导，YaST 将显示一个对话框，其中包含关于从哪个设备进行 IPL 的信息。接受关机选项，并在关机后执行 IPL。此过程将随安装类型的不同而有所不同：

### LPAR 安装

在 IBM System z HMC 中，选择**装载**，再选择**清除**，然后输入装载地址（存放带有引导加载程序的 `/boot` 目录的设备的设备地址）。如果适用 ZFCP 磁盘作为引导设备，请选择从 *SCSI* 装载，并指定 FCP 适配器的装载地址，以及引导设备的 WWPN 和 LUN。现在启动装载进程。

### z/VM 安装

作为 LINUX1 登录到 VM Guest（关于配置，请参见例 2.2 “Configuration of a z/VM Directory”（[↑Architecture-Specific Information](#)）），然后继续对已安装的系统执行 IPL。

```
IPL 151 CLEAR
```

151 是 DASD 引导设备的地址示例，请用正确的地址替换该值。

如果将 ZFCP 磁盘用作引导设备，则应在启动 IPL 之前指定引导设备的 ZFCP WWPN 和 LUN。参数长度不得超过 8 个字符。较长的数字必须用空格隔开：

```
SET LOADDEV PORT 50050763 00C590A9 LUN 50010000 00000000
```

最后，启动初始程序装载：

```
IPL FC00
```

FC00 是 ZFCP 适配器的地址示例，请用正确的地址替换该值。

## 3.13.2 IBM System z: 连接到已安装系统

对已安装系统进行初始程序装载后，应建立与它的连接以完成安装。所涉及的步骤随最初使用的连接类型的不同而有所不同。

### 使用 VNC 进行连接

3270 终端中有一条消息要求您使用 VNC 客户程序连接到 Linux 系统。但您很可能会忽略此消息，因为它与内核消息混杂在一起，而且在您注意到此消息时终端进程可能已退出。如果在 5 分钟内无任何反应，请尝试使用 VNC 查看器来启动与 Linux 系统的连接。

如果使用支持 Java 的浏览器进行连接，请输入完整的 URL，其中包括已安装系统的 IP 地址和端口号，具体形式如下：

```
http://<IP of installed system>:5801/
```

### 使用 X 进行连接

对已安装系统执行 IPL 时，请确保在安装第一阶段使用的 X 服务器已启动，并在从 DASD 引导之前仍然可用。YaST 会在此 X 服务器上打开以完成安装。如果系统已引导但无法及时连接到 X 服务器，情况就比较复杂。

### 使用 SSH 进行连接

---

**重要： IBM System z: 从 Linux 或 UNIX 系统进行连接**

在 xterm 中启动 SSH。其他终端模拟器不能完全支持 YaST 的基于文本的界面。

---

3270 终端中有一条消息要求您使用 SSH 客户程序连接到 Linux 系统。但您很可能会忽略此消息，因为它与内核消息混杂在一起，而且在您注意到此消息时终端进程可能已退出。

一旦出现该消息，请作为 root 使用 SSH 登录到 Linux 系统。如果连接被拒绝或超时，则等待数分钟后再重试。

建立连接后，执行命令 `/usr/lib/YaST2/startup/YaST2.ssh`。yast 在这种情况下不足以完成此操作。

此后，YaST 将开始安装剩余的包并创建初始系统配置。

## 3.14 已安装系统的配置

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

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

### 3.14.1 系统管理员“root”的密码

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

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

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

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

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



## 3.14.2 主机名和域名

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

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

要在安装后随时更改主机名设置，请使用 YaST 网络设备 > 网卡。有关更多信息，请参见第 30.4.1 节“使用 YaST 配置网卡”[509]。

## 3.14.3 网络配置

---

### 提示：IBM System z：网络配置

对于 IBM System z 平台，在安装时需要一个有效的网络连接以连接到目标系统、安装源和控制此进程的 YaST 终端。*Architecture-Specific Information* 手册的网络配置一章（第 2 章 *Preparing for Installation* (↑*Architecture-Specific Information*)) 介绍了设置网络的步骤。IBM System z 平台只支持该章中提及的网络接口类型（OSA Token Ring、OSA Ethernet、OSA Gigabit Ethernet、OSA Express Fast Ethernet、Escon、IUCV 以及 OSA Express High-Speed Token Ring）。YaST 对话框只显示接口及其先前配置的设置。确认此对话框来继续进行配置。

---

默认情况下，将启用不带 *NetworkManager* 小程序的传统方法。如果需要，还可以使用 *NetworkManager* 管理所有网络设备。但是，传统方法是服务器解决方案的首选选项。有关 *NetworkManager* 的更多详细信息，请参见第 30.6 节“使用 *NetworkManager* 管理网络连接”[526]。

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

除了设备配置，还可在此步骤中配置以下网络设置：

### 网络模式

启用或禁用 NetworkManager，如上所述。

### 防火墙

默认情况下，在所有已配置的网络接口上启用 SuSEfirewall2。要对此计算机全局禁用防火墙，请单击禁用。如果启用了防火墙，则可打开 SSH 端口以便允许通过安全壳层进行远程连接。要打开详细的防火墙配置对话框，请单击防火墙。有关详细信息，请参见第 43.4.1 节“使用 YaST 配置防火墙”[742]。

### IPv6

默认启用 IPv6 支持。要禁用它，请单击禁用 IPv6。有关 IPv6 的更多信息，请参见第 30.2 节“IPv6 — 下一代的因特网”[500]。

### VNC 远程管理

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

### 代理

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

---

#### 提示：将网络配置重设置为默认值

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

---

## 测试因特网连接

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

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

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

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

## 3.14.4 Novell Customer Center 配置

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

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

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

除激活并注册您的产品外，该模块还会向您的配置添加官方更新编目。此编目为已知 bug 和安全问题提供了修复，这些修复可通过联机更新进行安装。

为保持您的编目有效，请选择定期与客户中心同步。此选项将检查您的编目并添加新可用的编目，或删除旧编目。它不会改动手动添加的编目。

---

### 提示：技术支持

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

---

## 3.14.5 联机更新

如果 Novell Customer Center 配置成功，则选择是否执行 YaST 联机更新。如果这些服务器上有任何增补程序包，请立即下载并安装它们，以修复已知错误或安全问题。有关如何在已安装系统中执行联机更新的指导，请参见第 8.3.5 节“YaST 联机更新” [127]

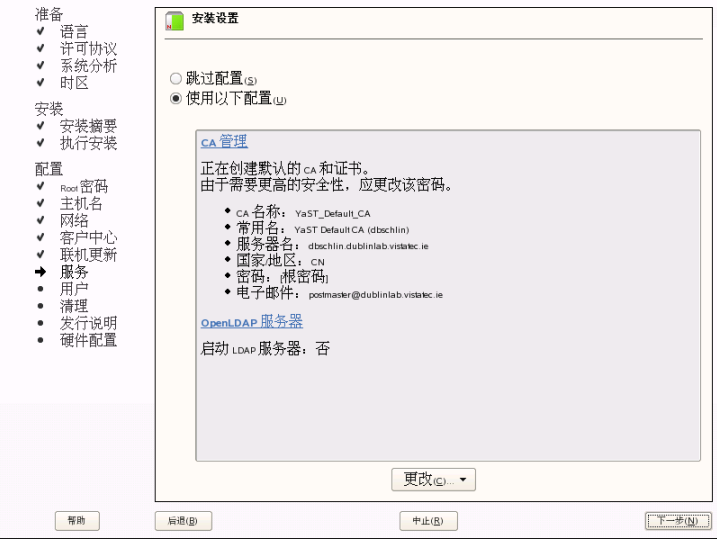
重要：下载软件更新程序

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

3.14.6 网络服务

配置网络后，将打开一个对话框，您可以在其中启用并配置两个重要的网络服务：证书颁发机构和OpenLDAP服务器。如果愿意，可以暂时跳过此配置建议。在安装完成后，您仍可以借助 YaST 配置和启动相同的服务。

图 3.6 网络服务的建议设置



CA 管理

CA（证书颁发机构）用于确保互相通讯的所有网络服务之间存在信任关系。无 CA 的情况下，您可以针对每个单独的服务分别保护与 SSL 和 TLS 的服务器通讯。默认情况下，在安装期间将创建并启用 CA。在**第 42 章 管理 X.509 认证** [723]中查找有关通过 YaST 创建 CA 的细节。

## OpenLDAP 服务器

您可以在主机上运行 LDAP 服务，以便集中管理一系列配置文件。通常，LDAP 服务器处理用户帐户数据，但通过 SUSE Linux Enterprise，它也可用于邮件、DHCP 和 DNS 数据。有关 LDAP 以及使用 YaST 配置 LDAP 的细节，请参见第 36 章 *LDAP - 目录服务* [599]。

---

**提示：将服务配置重设置为默认值**

恢复到默认值的方法是单击 **更改 > 重设置为默认值**。这会放弃所作的任何更改。

---

## 3.14.7 用户数

如果已在先前的安装步骤中成功配置了网络访问，则现在您可以从若干用户管理选项中进行选择。如果尚未配置网络连接，请创建本地用户帐户。有关用户管理的详细信息，请参见第 8.9.1 节“*用户管理*”[155]SUSE Linux Enterprise Server 文档。

### 本地 (/etc/passwd)

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

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

### LDAP

在 LDAP 服务器上对网络中的所有系统进行集中用户管理。有关更多信息，请参见第 36.6 节“*使用 YaST 配置 LDAP 客户机*”[617]。

### NIS

在 NIS 服务器上对网络中的所有系统进行集中用户管理。有关更多信息，请参见第 35.2 节“*配置 NIS 客户机*”[597]。

### Windows 域

在 Linux 和 Windows 混用的网络中经常使用 SMB 身份验证。有关详细信息，请参见第 37.6 节“*带有 Active Directory 的网络中的 Samba 服务器*”[638]。

---

### 注意：身份验证菜单的内容

如果使用自定义包选择，而菜单中缺少一种或多种身份验证方式，所需包可能未安装。

---

您可以与选定的用户管理方式一起使用 Kerberos 身份验证。这对于将 SUSE Linux Enterprise 集成到 Active Directory 域很关键，在[第 37.6 节“带有 Active Directory 的网络中的 Samba 服务器”](#) [638]中对此有说明。要使用 Kerberos 身份验证，请选择安装 *Kerberos 身份验证*。

## 3.14.8 发行说明

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

## 3.14.9 硬件配置

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

---

### 提示：IBM System z：硬件配置

在 IBM System z 上，XFree 将不支持任何显示。相应地，在这些系统上找不到 *图形卡* 项。

---

如[第 8.4 节“硬件”](#) [132]中所述，您可以跳过任何外围设备，并在以后配置它们。要跳过配置，请选择 *跳过配置*，然后单击 *下一步*。

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

---

**提示：将硬件配置重设置为默认值**

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

---

## 3.14.10 完成安装

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

AutoYaST 系统用于自动安装一个或多个 SUSE Linux Enterprise 系统而无需用户操作。AutoYaST 安装是通过使用具有安装和配置数据的控制文件来执行的。有关详细信息，请参见 [第 5 章 自动安装](#) [77]。单击最后一个对话框中的 **完成** 来完成 SUSE Linux Enterprise 的安装。

## 3.15 图形登录

---

**提示：IBM System z：无图形登录**

在 IBM System z 平台上图形登录不可用。

---

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





## 远程安装

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

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

---

### 注意

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

---

## 4.1 远程安装的安装方案

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

---

## 重要

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

---

### 4.1.1 通过 VNC 静态网络配置进行简单远程安装

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

对于此类型安装，请确保满足以下要求：

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

要执行此种安装，请执行如下操作：

- 1 按[第 4.2 节 “设置存放安装源的服务器”](#) [51]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参见[第 4.2.5 节 “管理 SMB 安装源”](#) [58]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。

- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的 VNC 选项和安装源的地址。第 4.4 节“引导用于安装的目标系统”[69]中对此有详细描述。

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

- 4 在控制工作站上，按第 4.5.1 节“VNC 安装”[74]中所述打开 VNC 查看应用程序或 Web 浏览器，并连接到目标系统。
- 5 按第 3 章使用 YaST 进行安装[17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 6 完成安装。

## 4.1.2 通过 VNC 动态网络配置进行简单远程安装

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

对于此类型安装，请确保满足以下要求：

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

要执行此种安装，请执行如下操作：

- 1 按第 4.2 节 “设置存放安装源的服务器” [51]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参见第 4.2.5 节 “管理 SMB 安装源” [58]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。
- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的 VNC 选项和安装源的地址。第 4.4 节 “引导用于安装的目标系统” [69]中对此有详细描述。

目标系统引导后进入一个基于文本的环境，它给出了网络地址和显示编号，任何 VNC 查看器应用程序或浏览器都可以藉此寻址到图形安装环境。VNC 安装将通过 OpenSLP 发布自身通告，并且在 `service:/` 方式或 `slp:/` 方式下使用 Komqueror 可将其找到。
- 4 在控制工作站上，按第 4.5.1 节 “VNC 安装” [74]中所述打开 VNC 查看应用程序或 Web 浏览器，并连接到目标系统。
- 5 按第 3 章 使用 YaST 进行安装 [17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 6 完成安装。

### 4.1.3 通过 VNC—PXE Boot 和“网络唤醒”进行远程安装

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

要执行此类型安装，请确保满足以下要求：

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

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

要执行此类型安装，请执行如下操作：

- 1 按第 4.2 节 “设置存放安装源的服务器” [51]中所述设置安装源。选择 NFS、HTTP、或 FTP 网络服务器或按第 4.2.5 节 “管理 SMB 安装源” [58]中所述配置 SMB 安装源。
- 2 设置存放引导映像（可被目标系统拉出）的 TFTP 服务器。第 4.3.2 节 “设置 TFTP 服务器” [61]中对此进行了说明。
- 3 设置 DHCP 服务器以向所有计算机提供 IP 地址，并向目标系统显示 TFTP 服务器的位置。第 4.3.1 节 “设置 DHCP 服务” [59]中对此进行了说明。
- 4 准备目标系统的 PXE 引导。第 4.3.5 节 “准备目标系统的 PXE 引导” [67]中对此有详细说明。
- 5 使用“网络唤醒”开始目标系统的引导过程 第 4.3.7 节 “局域网唤醒” [68]中对此进行了说明。
- 6 在控制工作站上，按第 4.5.1 节 “VNC 安装” [74]中所述打开 VNC 查看应用程序或 Web 浏览器，并连接到目标系统。
- 7 按第 3 章 使用 YaST 进行安装 [17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 8 完成安装。

## 4.1.4 通过 SSH 静态网络配置进行简单远程安装

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

对于此类型安装，请确保满足以下要求：

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

要执行此种安装，请执行如下操作：

- 1 按第 4.2 节 “设置存放安装源的服务器” [51] 中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参见第 4.2.5 节 “管理 SMB 安装源” [58]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。
- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的网络连接参数、安装源地址以及 SSH 支持。第 4.4.3 节 “使用自定义引导选项” [71] 中对此有详细描述。

目标系统引导后进入一个基于文本的环境，它给出了一个网络地址，通过该地址，任何 SSH 客户机都可以寻址到图形安装环境。

- 4 在控制工作站上，按“连接到安装程序”一节 [76] 中所述打开终端窗口并连接到目标系统。
- 5 按第 3 章 使用 YaST 进行安装 [17] 中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 6 完成安装。

## 4.1.5 通过 SSH 动态网络配置进行简单远程安装

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

对于此类型安装，请确保满足以下要求：

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

要执行此种安装，请执行如下操作：

- 1 按第 4.2 节“设置存放安装源的服务器”[51]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参见第 4.2.5 节“管理 SMB 安装源”[58]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。
- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的网络连接参数、安装源位置以及 SSH 支持。关于如何使用这些参数的详细说明，请参见第 4.4.3 节“使用自定义引导选项”[71]。

目标系统引导后进入一个基于文本的环境，它给出了一个网络地址，通过该地址，任何 SSH 客户机都可以寻址到图形安装环境。

- 4 在控制工作站上，按“连接到安装程序”一节[76]中所述打开终端窗口并连接到目标系统。
- 5 按第 3 章使用 YaST 进行安装[17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。

6 完成安装。

## 4.1.6 通过 SSH—PXE Boot 和“网络唤醒”进行远程安装

此类安装是完全无人值守的。目标计算机是远程启动和引导的。

要执行此类型安装，请确保满足以下要求：

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

要执行此类型安装，请执行如下操作：

- 1 按第 4.2 节“设置存放安装源的服务器”[51]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。有关 SMB 安装源的配置，请参见第 4.2.5 节“管理 SMB 安装源”[58]。
- 2 设置存放引导映像（可被目标系统拉出）的 TFTP 服务器。第 4.3.2 节“设置 TFTP 服务器”[61]中对此进行了说明。
- 3 设置 DHCP 服务器以向所有计算机提供 IP 地址，并向目标系统显示 TFTP 服务器的位置。第 4.3.1 节“设置 DHCP 服务”[59]中对此进行了说明。
- 4 准备目标系统的 PXE 引导。第 4.3.5 节“准备目标系统的 PXE 引导”[67]中对此有详细说明。
- 5 使用“网络唤醒”开始目标系统的引导过程 第 4.3.7 节“局域网唤醒”[68]中对此进行了说明。
- 6 在控制工作站上，按第 4.5.2 节“SSH 安装”[75]中所述启动 SSH 客户机并连接到目标系统。



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

## 4.2 设置存放安装源的服务器

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

---

### 提示

您甚至可以将 Microsoft Windows 计算机用作 Linux 部署的安装服务器。有关详细信息，请参见第 4.2.5 节“管理 SMB 安装源” [58]。

---

### 4.2.1 使用 YaST 设置安装服务器

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

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

定义安装数据所在的 FTP 或 HTTP 服务器的 root 目录的别名。该安装源以后将放在 `ftp://Server-IP/Alias/name(ftp)` 或 `http://Server-IP/Alias/Name(HTTP)` 下。Name 代表安装源的名称，该名称将在下面的步骤中定义。如果您在上一步中选择了 NFS，请定义通配符和导出选项。可在 `nfs://Server-IP/Name` 下访问 NFS 服务器。

---

### 提示：防火墙设置

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

---

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

### 提示

如果您的网络设置支持此选项，请考虑通过 OpenSLP 就安装源发布通告。这样就无需在每台目标计算机上输入网络安装路径。将使用 SLP 引导选项引导这些目标系统，并且无需进一步的配置就可以找到网络安装源。有关该选项的详细信息，请参见第 4.4 节“[引导用于安装的目标系统](#)” [69]。

---

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

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

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

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

## 4.2.2 手动设置 NFS 安装源

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

要创建存放安装数据的目录，请执行如下操作：

**1** 以 root 身份登录。

**2** 创建稍后用于存放所有安装数据的目录，然后切换到该目录。例如：

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

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

**3** 对媒体工具包中的每张 CD，执行以下命令：

**3a** 将安装 CD 的所有内容复制到安装服务器目录中：

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

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

**3b** 将目录重命名为 CD 编号。

```
mv path_to_your_CD-ROM_drive CDx
```

将其中的 *x* 替换您 CD 的实际编号。

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

**1** 以 root 身份登录。

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

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

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

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

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

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

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

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

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

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

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

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

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

关于 OpenSLP 的更多信息，请参见位于 `/usr/share/doc/packages/openslp/` 下的包文档，或参见第 31 章 [网络中的 SLP 服务](#) [545]。

## 4.2.3 手动设置 FTP 安装源

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

- 1 按第 4.2.2 节“[手动设置 NFS 安装源](#)” [53]中所述创建存放安装源的目录。
- 2 配置 FTP 服务器以分发安装目录的内容：

**2a** 以 root 身份登录，然后使用 YaST 包管理器安装 `vsftpd` 包。

**2b** 输入 FTP 服务器 root 目录：

```
cd /srv/ftp
```

**2c** 在 FTP root 目录中创建存放安装源的子目录：

```
mkdir instsource
```

将 `instsource` 替换为产品名称。

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

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

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

- 2e** 通过 `vsftpd` 启动 `vsftpd`。

- 3** 通过 OpenSLP 就安装源发布通告（如果网络设置对此支持）：

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

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

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

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

## 4.2.4 手动设置 HTTP 安装源

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

- 1** 按第 4.2.2 节“手动设置 NFS 安装源”[53]中所述创建存放安装源的目录。
- 2** 配置 HTTP 服务器以分发安装目录的内容：
  - 2a** 如第 40.1.2 节“安装”[668]所述安装 Web 服务器 Apache。
  - 2b** 输入 HTTP 服务器的 root 目录（`/srv/www/htdocs`）并创建用于存放安装源的子目录：

```
mkdir instsource
```

将 *instsource* 替换为产品名称。

- 2c** 创建一个从安装源位置到 Web 服务器 root 目录（*/srv/www/htdocs*）的符号链接：

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

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

```
Options None
```

使用

```
Options Indexes FollowSymLinks
```

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

- 3** 通过 OpenSLP 就安装源发布通告（如果网络设置对此支持）：

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

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

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

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

## 4.2.5 管理 SMB 安装源

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

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

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

要将 SMB 装入共享用作安装源，请执行如下操作：

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

按 Enter 键，YaST 将启动，然后您就可以执行安装了。

## 4.2.6 使用服务器上安装媒体的 ISO 映像

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



- 1 下载 ISO 映像并将它们保存到用作安装服务器的计算机上。
- 2 以身份 `root` 登录。
- 3 按照第 4.2.2 节“手动设置 NFS 安装源”[53]、第 4.2.3 节“手动设置 FTP 安装源”[55]或第 4.2.4 节“手动设置 HTTP 安装源”[56]中的说明，选择并创建安装数据的合适位置。
- 4 创建每张 CD 或 DVD 的子目录。
- 5 要将各个 ISO 映像安装和解开到最终位置，请发出以下命令：

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

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

- 6 多次重复上述步骤，以安装产品所需的全部 ISO 映像。
- 7 按照第 4.2.2 节“手动设置 NFS 安装源”[53]、第 4.2.3 节“手动设置 FTP 安装源”[55]或第 4.2.4 节“手动设置 HTTP 安装源”[56]中的说明，与往常一样启动安装服务器。

## 4.3 准备目标系统的引导

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

### 4.3.1 设置 DHCP 服务

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

## 用 YaST 设置 DHCP 服务器

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

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

要配置 DHCP 以向特定主机提供静态 IP 地址，请输入 DHCP 服务器配置模块 ( ) 的专家设置步骤 4 [60] 并添加主机类型的新声明。将选项 hardware 和 fixed-address 添加到此主机声明并提供适当的值。

## 手动设置 DHCP 服务器

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

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

```
group {
    # PXE related stuff
    #
    # "next server" defines the tftp server that will be used
    next server ip_tftp_server;
```

```

#
# "filename" specifies the pxelinux image on the tftp server
# the server runs in chroot under /srv/tftpboot
filename "pxelinux.0";
}

```

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

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

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

```

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

```

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

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

## 4.3.2 设置 TFTP 服务器

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

## 使用 YaST 设置 TFTP 服务器

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

## 手动设置 TFTP 服务器

- 1 以 root 身份登录，然后安装 *tftp* 包和 *xinetd* 包。
- 2 如果这两个包不可用，请创建 */srv/tftpbboot* 目录和 */srv/tftpbboot/pxelinux.cfg* 目录。
- 3 按第 4.3.3 节“使用 PXE 引导”[63]中所述添加引导映像所需的相应文件。
- 4 修改位于 */etc/xinetd.d/* 下的 *xinetd* 的配置，以确保 TFTP 服务器在引导时启动：
  - 4a 如果该配置文件不存在，请使用 `touch tftp` 命令在该目录下创建一个名为 *tftp* 的文件。然后运行 `chmod 755 tftp`。
  - 4b 打开文件 *tftp*，添加以下几行：

```
service tftp
{
    socket_type      = dgram
    protocol         = udp
    wait             = yes
    user             = root
    server            = /usr/sbin/in.tftpd
```

```

server_args      = -s /srv/tftpboot
disable          = no
}

```

**4c** 保存该文件，然后使用 `rcxinetd restart` 命令重新启动 `xinetd`。

## 4.3.3 使用 PXE 引导

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

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

```

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

```

- 2 通过 YaST 直接从 CD 或 DVD 安装 `syslinux` 包。
- 3 输入以下命令来将 `/usr/share/syslinux/pxelinux.0` 文件复制到 `/srv/tftpboot` 目录中：

```

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

```

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

```

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

```

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

```
insmod=kernel module
```

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

```
netdevice=interface
```

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

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

该条目定义了用于客户机安装的分发服务器和安装源。请将

*ip\_instserver* 替换为安装服务器的实际 IP 地址。

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

---

## 重要

如果需要向安装例程指定其他引导选项，如 SSH 或 VNC 引导参数，请将它们追加到 `install` 条目中。在 [第 4.4 节“引导用于安装的目标系统”](#) [69] 提供了参数的概述和一些例子。

---

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

```
default linux
```

```
# default
```

```
label linux
```

```
kernel linux
```

```
append initrd=initrd ramdisk_size=65536 insmod=e100 \
```

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

```
# failsafe
```

```
label failsafe
```

```
kernel linux
```

```
append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
```

```
insmod=e100 install=nfs://ip_instserver/path_instsource/product/CD1
```

```

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

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

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

# memory test
label memtest
    kernel memtest

# hard disk
label harrdisk
    localboot 0

implicit      0
display      message
prompt       1
timeout      100

```

将 *ip\_instserver* 和 *path\_instsource* 替换为您设置中使用的值。

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

## 4.3.4 PXELINUX 配置选项

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

**DEFAULT** *kernel options...*

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

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

`APPEND options...`

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

`LABEL label KERNEL image APPEND options...`

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

请注意 GRUB 使用以下语法：

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

PXELINUX 使用以下语法：

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

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

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

`APPEND -`

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

`LOCALBOOT type`

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



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

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

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

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

```
F2 filename
F1 filename
...etc...
F9 filename
F10 filename
```

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

### 4.3.5 准备目标系统的 PXE 引导

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

---

### 警告：BIOS 引导顺序

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

---

## 4.3.6 准备目标系统的网络唤醒

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

## 4.3.7 局域网唤醒

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

---

### 重要：不同网段的“网络唤醒”

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

---

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

## 4.3.8 使用 YaST 的“网络唤醒”

- 1 以 root 身份登录。
- 2 启动 *YaST > 网络服务 > WOL*。
- 3 单击添加并输入目标系统的主机名和 MAC 地址。
- 4 要打开此计算机，请选择适当的输入框并单击唤醒。

## 4.3.9 手动进行网络唤醒

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

```
ether-wake mac_of_target
```

请将 `mac_of_target` 替换为目标计算机的实际 MAC 地址。

## 4.4 引导用于安装的目标系统

除了在第 4.3.7 节“局域网唤醒”[68]和第 4.3.3 节“使用 PXE 引导”[63]中提到的那些方法之外，主要有两种方法来定义用于安装的引导过程。您既可以使用默认的引导选项和功能键，也可以使用安装引导屏幕上的引导选项提示来指定安装内核对该特定硬件可能需要的任何引导选项。

### 4.4.1 使用默认的引导选项

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

如果发生问题，请使用安装 — 禁用 *ACPI* 或安装 — 安全设置。有关安装过程故障诊断的更多信息，请参见第 51.2 节“安装问题”[821]。

### 4.4.2 使用 F 键

屏幕底部的菜单栏提供了某些安装中所需的几项高级功能。使用 F 键可以指定其他选项传递到安装路由，而不需要了解这些参数（参见第 4.4.3 节“使用自定义引导选项”[71]）的详细语法。

请查看下表以了解所有的可用选项。

表 4.1 安装期间的 F 键

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

# 4.4.3 使用自定义引导选项

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

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

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

将该字符串中的所有值 (...) 替换为适用于您安装的值。

表 4.2 本章中使用的安装（引导）方案

安装方案	引导时所需 的参数	引导选项
第 3 章 使用 <i>YaST</i> 进行安装 [17]	无：系统自 动引导	不需要任何选项
第 4.1.1 节 “通过 VNC 静态网络配置进行简单远程安装” [44]	<ul style="list-style-type: none"><li>• 安装服务器的位置</li><li>• 网络设备</li><li>• IP 地址</li><li>• 网络掩码</li><li>• 网关</li><li>• VNC 支持</li><li>• VNC 密码</li></ul>	<ul style="list-style-type: none"><li>• <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code></li><li>• <code>netdevice=some_netdevice</code>(仅当有多个网络设备可用时才需要)</li><li>• <code>hostip=some_ip</code></li><li>• <code>netmask=some_netmask</code></li><li>• <code>gateway=ip_gateway</code></li><li>• <code>vnc=1</code></li><li>• <code>vncpassword=some_password</code></li></ul>

安装方案	引导时所需的参数	引导选项
第 4.1.2 节 “通过 VNC 动态网络配置进行简单远程安装” [45]	<ul style="list-style-type: none"> <li>• 安装服务器的位置</li> <li>• VNC 支持</li> <li>• VNC 密码</li> </ul>	<ul style="list-style-type: none"> <li>• <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code></li> <li>• <code>vnc=1</code></li> <li>• <code>vncpassword=some_password</code></li> </ul>
第 4.1.3 节 “通过 VNC—PXE Boot 和“网络唤醒”进行远程安装” [46]	<ul style="list-style-type: none"> <li>• 安装服务器的位置</li> <li>• TFTP 服务器的位置</li> <li>• VNC 支持</li> <li>• VNC 密码</li> </ul>	不适用；进程通过 PXE 和 DHCP 管理
第 4.1.4 节 “通过 SSH 静态网络配置进行简单远程安装” [47]	<ul style="list-style-type: none"> <li>• 安装服务器的位置</li> <li>• 网络设备</li> <li>• IP 地址</li> <li>• 网络掩码</li> <li>• 网关</li> <li>• SSH 支持</li> <li>• SSH 密码</li> </ul>	<ul style="list-style-type: none"> <li>• <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code></li> <li>• <code>netdevice=some_netdevice</code>(仅当有多个网络设备可用时才需要)</li> <li>• <code>hostip=some_ip</code></li> <li>• <code>netmask=some_netmask</code></li> <li>• <code>gateway=ip_gateway</code></li> <li>• <code>usessh=1</code></li> <li>• <code>sshpassword=some_password</code></li> </ul>

安装方案	引导时所需的参数	引导选项
第 4.1.5 节“通过 SSH 动态网络配置进行简单远程安装” [49]	<ul style="list-style-type: none"><li>• 安装服务器的位置</li><li>• SSH 支持</li><li>• SSH 密码</li></ul>	<ul style="list-style-type: none"><li>• <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code></li><li>• <code>usessh=1</code></li><li>• <code>sshpassword=some_password</code></li></ul>
第 4.1.6 节“通过 SSH—PXE Boot 和“网络唤醒”进行远程安装” [50]	<ul style="list-style-type: none"><li>• 安装服务器的位置</li><li>• TFTP 服务器的位置</li><li>• SSH 支持</li><li>• SSH 密码</li></ul>	不适用；进程通过 PXE 和 DHCP 管理

提示：有关 `linuxrc` 引导选项的更多信息

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

## 4.5 监视安装过程

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

## 4.5.1 VNC 安装

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

### 准备进行 VNC 安装

在准备 VNC 安装时，只需要为安装目标指定合适的引导选项供初始安装引导过程使用即可。（请参见第 4.4.3 节“使用自定义引导选项”[71]）。目标系统引导后进入一个基于文本的环境中，并等待 VNC 客户机连接到安装程序。

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

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

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

### 连接到安装程序

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

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



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

要连接到目标计算机上运行的安装程序，请执行如下操作：

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

`ip_address:display_number`

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

使用 Web 浏览器连接到安装程序，将使您完全不必依赖任何 VNC 软件或底层操作系统。只要浏览器应用程序启用了 Java 支持，就可以使用任意浏览器（Firefox、Internet Explorer、Konqueror、Opera 等等）来执行 Linux 系统的安装。

要执行 VNC 安装，请执行如下操作：

- 1 启动首选的 Web 浏览器。
- 2 在地址栏中输入以下内容：  
`http://ip_address_of_target:5801`
- 3 在看到输入 VNC 密码的提示时输入此密码。浏览器窗口此刻显示的 YaST 屏幕与正常本地安装中所显示的相同。

## 4.5.2 SSH 安装

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

### 准备进行 SSH 安装

除了安装相应的软件包（用于 Linux 的 OpenSSH 和用于 Windows 的 PuTTY），您只需指定相应的引导选项来为安装启用 SSH。有关细节，请参见第 4.4.3 节

“使用自定义引导选项”[71]。默认情况下，OpenSSH 安装在所有基于 SUSE Linux 的操作系统上。

## 连接到安装程序

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

- 2 在命令行中输入以下命令：

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

将 *ip\_address\_of\_target* 替换为安装目标的实际 IP 地址。

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

# 自动安装

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

## 5.1 简单的大规模安装

---

### 重要：相同硬件

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

---

要准备 AutoYaST 大规模安装，请执行以下操作：

- 1 如第 5.1.1 节 “创建 AutoYaST 配置文件” [78] 中所述创建 AutoYaST 配置文件，该配置文件包含您的部署所需的安装细节。
- 2 如第 5.1.2 节 “分发配置文件并确定 `autoyast` 参数” [79] 中所述，确定 AutoYaST 配置文件的来源以及要传递到安装例程的参数。
- 3 如第 5.1.3 节 “提供安装数据” [82] 所述确定 SUSE Linux Enterprise 安装数据源。
- 4 如第 5.1.4 节 “设置引导方案” [82] 中所述确定并设置自动安装引导方案。

- 5 如第 5.1.5 节“创建 info 文件”[84]所述，通过手动添加参数或创建 info 文件，将命令行传递到安装例程。
- 6 如第 5.1.6 节“启动并监视自动安装”[87]中所述，启动自动安装进程。

## 5.1.1 创建 AutoYaST 配置文件

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

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

要复制新的参考安装，请执行以下操作：

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

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

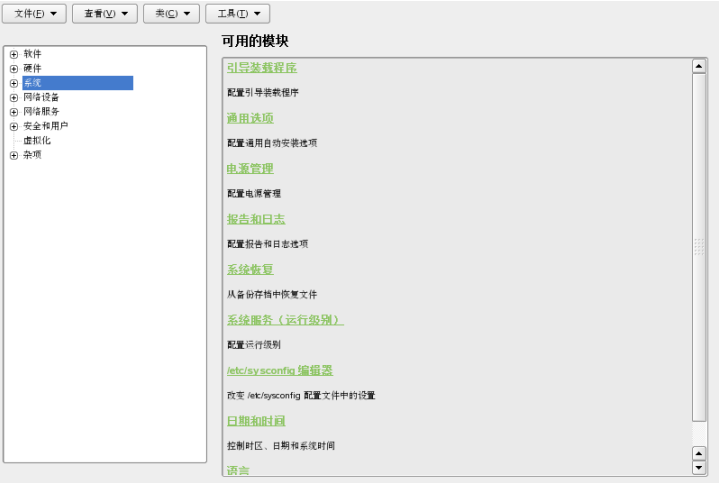
- 1 作为 root 启动 YaST。
- 2 选择 *其他 > 自动安装* 来启动图形 AutoYaST 前端。
- 3 选择 *工具 > 创建参考控制文件* 以准备 AutoYaST，将当前系统配置镜像到 AutoYaST 配置文件。
- 4 除了默认资源（如引导加载程序、分区和软件选择）之外，可以通过查看 *创建参考控制文件* 列表内的项目，将系统的各种其他方面添加到配置文件。
- 5 单击 *创建* 使 YaST 收集所有系统信息并将其写到新配置文件。

6 要继续，请选择下列操作之一：

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

7 使用文件 > 退出退出 AutoYaST 模块。

图 5.1 使用 AutoYaST 前端编辑 AutoYaST 配置文件



### 5.1.2 分发配置文件并确定 autoyast 参数

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

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

用与实际安装匹配的值来替代服务器和路径。

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

要使用此功能，请执行以下操作：

- 1 使用客户机的 MAC 地址作为文件名来创建不同配置文件，并将其放置到 HTTP 服务器来存放您的 AutoYaST 配置文件。
- 2 在创建 `autoyast=` 参数时，删除包括文件名在内的实际路径，例如：

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

- 3 启动自动安装。

YaST 尝试以下列方式确定配置文件位置：

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

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

## 5.1.3 提供安装数据

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

要提供网络上的安装源，请如第 4.2.1 节“使用 YaST 设置安装服务器”[51]所述设置网络安装服务器（HTTP、NFS、FTP）。使用 info 文件将服务器位置传递到安装例程。

## 5.1.4 设置引导方案

客户机可以用以下几种不同的方式引导：

### 网络引导

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

### 可引导 CD-ROM

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

以下几节简要叙述网络引导或 CD-ROM 引导的基本程序。

## 准备网络引导

中讨论了如何使用“网络唤醒”、PXE 和 TFTP 进行网络引导。第 4.1.3 节“通过 VNC—PXE Boot 和“网络唤醒”进行远程安装”[46] 要使用已介绍的步骤进行自动安装，请修改起重要作用的 PXE Linux 配置文件 (/srv/tftp/pxelinux.cfg/default)，以使其包含指向 AutoYaST 配置文件位置的 autoyast 参数。标准安装的示例项如下：

```
default linux

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



自动安装的相同示例如下：

```
default linux

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

用安装中使用的数据替代示例 IP 地址和路径。

## 准备从 CD-ROM 引导

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

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

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

需要对包含每：

- SUSE Linux Enterprise 媒体
- 提供配置文件数据的网络服务器（详见第 5.1.2 节“分发配置文件并确定 **autoyast 参数**” [79]）
- 包含 info 文件的软盘，以告知安装例程在哪里找到配置文件

或

访问系统引导提示，以便在手动输入 `autoyast=` 参数的地方进行安装

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

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

需要对包含每：

- SUSE Linux Enterprise 媒体
- 存放配置文件和 info 文件的软盘

或

访问目标的引导提示以输入 `autoyast=` 参数

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

## 5.1.5 创建 info 文件

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

这要通过根据安装引导提示手动传递这些参数来进行，或者通过提供由安装例程 (linuxrc) 读取的名为 info 的文件来进行。前者要求对任何要安装的客户机进行物理访问，这便使得这种方法不适合于大规模部署。后者使您能够提供一些媒体上的 info 文件，该文件要在自动安装前准备好并插入客户机驱动器。或者，如“[准备网络引导](#)”一节 [82]所示使用 PXE 引导并将 linuxrc 参数包括在 pxelinux.cfg/default 文件中。

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

重要：分隔参数和值	
当根据引导提示向 linuxrc 传递参数时，请使用 = 分隔参数和值。当使用 info 文件时，请使用 : 分隔参数和值。	
关键字	值
netdevice	网络安装所使用的网络设备（根据 BOOTP/DHCP 的请求）。仅在几个网络设备可用的条件下需要。

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

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

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

如果要在安装时间使用静态网络安装，则 info 文件将如下所示：

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

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

info数据可以几种不同的方式用于 linuxrc:

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

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

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

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

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

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

## 5.1.6 启动并监视自动安装

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

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

要启用远程控制自动安装，请如第 5.1.5 节“创建 `info` 文件”[84]中所述使用 VNC 或 SSH 参数，并如第 4.5 节“监视安装过程”[73]所述，从另一台计算机连接到客户机。

## 5.2 基于规则的自动安装

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

### 5.2.1 了解基于规则的自动安装

基于规则的 AutoYaST 安装使您能够处理异构硬件环境：

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

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

理，AutoYaST 通过把可以匹配 AutoYaST 规则的不同配置文件合成为一个来生成最后的配置文件。有关该过程的示例，请参见第 5.2.2 节“基于规则自动安装的示例方案” [89]。

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

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

---

## 注意

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

---

要准备基于规则的 AutoYaST 大规模安装，请执行以下操作：

- 1 创建几个 AutoYaST 配置文件，这些配置文件包含第 5.1.1 节“创建 AutoYaST 配置文件” [78]中描述的异构安装所需的安装细节。
- 2 定义规则以匹配第 5.2.2 节“基于规则自动安装的示例方案” [89]中所显示的硬件安装的系统属性。
- 3 如第 5.1.2 节“分发配置文件并确定 `autoyast` 参数” [79]中所述，确定 AutoYaST 配置文件的来源以及要传递到安装例程的参数。
- 4 如第 5.1.3 节“提供安装数据” [82]所述确定 SUSE Linux Enterprise 安装数据源
- 5 如第 5.1.5 节“创建 `info` 文件” [84]所述，通过手动添加参数或创建 `info` 文件，将命令行传递到安装例程。
- 6 如第 5.1.4 节“设置引导方案” [82]中所述确定并设置自动安装引导方案。
- 7 如第 5.1.6 节“启动并监视自动安装” [87]中所述，启动自动安装进程。

## 5.2.2 基于规则自动安装的示例方案

要基本了解如何创建规则，请考虑图 5.2 “AutoYaST 规则” [90]中描述的如下示例。一次性 AutoYaST 安装下列设置：

### 打印服务器

计算机只需要无桌面环境的最小化安装和一套有限的软件包。

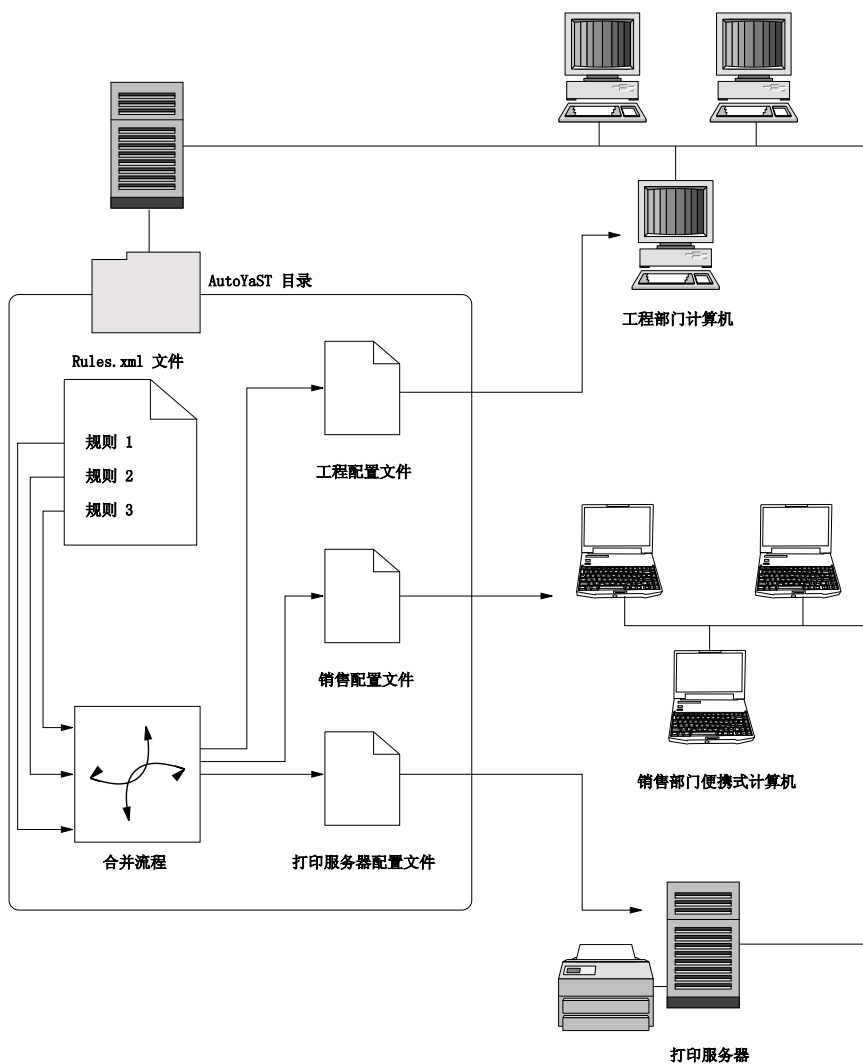
### 工程设计部的工作站

这些计算机需要桌面环境和一整套开发软件。

### 销售部的笔记本电脑

这些计算机需要桌面环境和一套有限的专用应用程序（如办公和日历软件）。

图 5.2 AutoYaST 规则



在第一步中，请使用第 5.1.1 节“创建 AutoYaST 配置文件”[78]中所述的方法之一来为每次使用情况创建配置文件。在本例中，您将创建 `print.xml`、`engineering.xml` 和 `sales.xml`。



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

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

大致上，这可以转换为具有下列内容的 rules.xml 文件：

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

```

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

```

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

剩余的自动安装程序像往常一样进行。

## 5.3 有关详细信息

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

## 部署自定义预安装

将自定义 SUSE Linux Enterprise 预安装到大量相同的计算机上，使您不必在每一台上单独安装，并使最终用户感到安装是标准化的。使用 YaST firstboot 创建自定义预安装映像，并确定涉及最终用户交互的最终个性化步骤的工作流程。这与允许完全自动化安装的 AutoYaST 不同；有关更多信息，请参见第 5 章 *自动安装* [77]。

创建自定义安装、部署到硬件及使最终产品个性化包括以下步骤：

- 1 准备磁盘要复制到客户机的主计算机。有关更多信息，请参考第 6.1 节 *“准备主计算机”* [94]。
- 2 自定义 firstboot 工作流程。有关更多信息，请参考第 6.2 节 *“自定义 Firstboot 安装”* [94]。
- 3 复制主计算机磁盘，将映像转到客户机磁盘上。有关更多信息，请参考第 6.3 节 *“复制主安装”* [102]。
- 4 让最终用户个性化 SUSE Linux Enterprise 的实例。有关更多信息，请参考第 6.4 节 *“个性化安装”* [102]。

## 6.1 准备主计算机

为 firstboot 工作流程准备主计算机，请按以下步骤操作：

- 1 将安装媒体插入主计算机中。
- 2 引导计算机。
- 3 执行包含所有必要配置步骤的正常安装，等待安装好的计算机进行引导。同时安装 `yast2-firstboot` 包。
- 4 要定义自己的最终用户 YaST 配置步骤工作流程，或将自己的 YaST 模块添加到该工作流程，请转到第 6.2 节“自定义 Firstboot 安装”[94]。否则的话，直接转到步骤 5 [94]。
- 5 以 root 启用 firstboot：
  - 5a 创建空文件 `/etc/reconfig_system` 触发 firstboot 的执行。成功完成 firstboot 配置后，该文件将被删除。用以下命令创建该文件：

```
touch /etc/reconfig_system
```
  - 5b 通过 YaST 运行级别编辑器启用 firstboot 服务。
- 6 转到第 6.3 节“复制主安装”[102]。

## 6.2 自定义 Firstboot 安装

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

- 按第 6.2.1 节“自定义 YaST 消息”[95]中所述自定义最终用户收到的消息。
- 按第 6.2.2 节“自定义许可证操作”[96]中所述自定义许可证和许可证操作。
- 按第 6.2.3 节“自定义发行说明”[96]中所述自定义要显示的发行说明。

- 如第 6.2.4 节 “自定义工作流程” [97]中所述，自定义安装中涉及的组件的顺序和编号。
- 如第 6.2.5 节 “配置其他脚本” [102]中所述配置其他可选脚本。

要自定义其中的任何组件，请调整以下配置文件：

```
/etc/sysconfig/firstboot
```

配置 `firstboot` 的不同方面，例如发行说明、脚本和许可证操作。

```
/etc/YaST2/firstboot.xml
```

通过启用或禁用组件或者添加自定义组件，配置安装工作流程。

## 6.2.1 自定义 YaST 消息

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

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

```
FIRSTBOOT_WELCOME_DIR="/usr/share/firstboot/"
```

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

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

如未设置，将假定为默认值 `welcome.txt`。

- 3 创建欢迎文件和本地化版本，并将它们置于 `/etc/sysconfig/firstboot` 配置文件中指定的目录中。

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

## 6.2.2 自定义许可证操作

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

**halt**

`firstboot` 安装已中止，整个系统关闭。这是默认设置。

**继续**

`firstboot` 安装继续。

**中止**

`firstboot` 安装已中止，但系统尝试引导。

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

## 6.2.3 自定义发行说明

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

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

## 6.2.4 自定义工作流程

默认情况下，标准 firstboot 工作流程包含以下部分：

- 语言选择
- 欢迎
- 许可证协议
- 主机名
- 网络
- 时间和日期
- 桌面
- root 密码
- 用户身份验证方法
- 用户管理
- 硬件配置
- 完成安装

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

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

## 例 6.1 配置提议屏幕

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

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

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



## 例 6.2 配置工作流程部分

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

工作流程部分的总体结构和提议部分很相似。容器包含工作流程元素，工作流程元素都包括和例 6.1 “配置提议屏幕”[98]中所介绍的提议相同的阶段、标签和方式信息。最显著的差别是默认设置部分，它包含工作流程组件的基本设计信息：

`enable_back`

在所有对话框中包含上一步按钮。

`enable_next`

在所有对话框中包含下一步按钮。

`archs`

指定使用该工作流程的硬件体系结构。

## 例 6.3 配置工作流程组件列表

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

❶ 所有工作流程组件的容器。

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

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

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

- 3 应用更改并关闭配置文件。

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

要切换 `firstboot` 工作流程中模块的状态，请按以下步骤操作：

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

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

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

### 3 应用更改并关闭配置文件。

要向工作流程添加自定义模块，请按以下步骤继续：

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

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

**4a** 在标签元素中输入要在模块上显示的标签。

**4b** 请确保已启用已设置为 `true`，将您的模块包括在工作流程中。

**4c** 在名称元素中输入您模块的文件名。省略完整路径和 `.ycp` 后缀。

### 5 应用您的设置并关闭配置文件。

---

#### 提示：有关详细信息

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

---

## 6.2.5 配置其他脚本

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

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

## 6.3 复制主安装

用您可以获得的任何映像机制复制主计算机磁盘，将映像转到目标计算机。

## 6.4 个性化安装

引导已复制磁盘映像后，`firstboot` 会启动，安装会严格按第 6.2.4 节“自定义工作流程”[97]中的安排继续。只有 `firstboot` 工作流程配置中包含的组件会启动。任何其他安装步骤都将跳过。最终用户可调整语言、键盘、网络和密码设置，以个性化工作站。这一过程完成后，`firstboot` 已安装系统的行为就会像 SUSE Linux Enterprise 的任何其他实例一样。

# 高级磁盘设置

高级系统配置需要特定的磁盘设置。所有常用分区任务都可以用 YaST 完成。为实现块设备的统一设备命名，请使用 `/dev/disk/by-id/` 下的块设备。逻辑卷管理 (LVM) 是一种磁盘分区模式，旨在比标准设置中使用的物理分区更加灵活。它的快照功能方便了数据备份的创建。独立磁盘冗余阵列 (RAID) 提高了数据完整性、性能和容错能力。SUSE® Linux Enterprise Server 还支持多路径 I/O。有关细节，请参见 *Storage Administration Guide*（储存管理指南）中有关多路径 I/O 的章节。从 SUSE Linux Enterprise 10 开始，还可以选择使用 iSCSI 作为联网磁盘。有关 iSCSI 的详细信息，请参见第 12 章 *经由 IP 网络的大容量储存 — iSCSI* [245]。

## 7.1 LVM 配置

本节简要介绍 LVM 的原理及其基本功能，这些功能使 LVM 在许多情况下都很有用。在第 7.1.2 节“用 YaST 配置 LVM” [105] 中，将学习如何用 YaST 设置 LVM。

---

### 警告

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

---

# 7.1.1 逻辑卷管理器

逻辑卷管理器 (LVM) 支持在多个文件系统上灵活分配硬盘空间。开发逻辑卷管理器是因为有时只有在安装过程中初始分区完成后才需要更改硬盘空间的分段。因为在运行的系统中修改分区比较困难，LVM 提供了内存空间的虚拟池（卷组，简称 VG），如果需要，可以从中生成逻辑卷 (LV)。操作系统访问这些逻辑卷而不是物理分区。卷组可以跨多个磁盘，这样多个磁盘或部分磁盘可以构成一个 VG。LVM 以这种方式提供了一种对物理磁盘空间的抽象，从而能够以比物理分区更方便、更安全的方式更改硬盘空间的分段。“分区类型”一节 [141] 和第 8.5.7 节 “使用 YaST 分区程序” [139] 中提供了有关物理分区的背景信息。

图 7.1 物理分区与 LVM

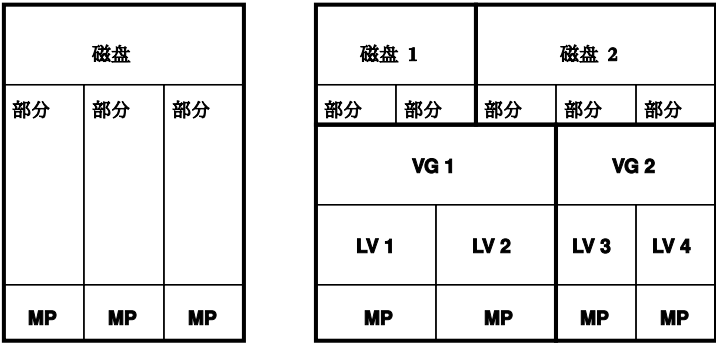


图 7.1 “物理分区与 LVM” [104] 比较物理分区（左）和 lvm 分段（右）。在左侧，将一个磁盘分成 3 个物理分区 (PART)，每个分区指派了一个装入点 (MP)，以便操作系统可以访问它们。在右侧，有两个磁盘，一个磁盘分为 2 个物理分区，另一个磁盘分为 3 个物理分区。定义了两个 LVM 卷组 (VG1 和 VG2)。VG1 包含 DISK1 中的 2 个分区和 DISK2 中的 1 个分区。VG2 包含 DISK2 中剩余的 2 个分区。在 LVM 中，将卷组中包含的物理磁盘分区称为物理卷 (PV)。在卷组中，定义了 4 个逻辑卷（从 LV1 到 LV4），操作系统可通过相关的装入点使用这些逻辑卷。不同逻辑卷之间的边界不一定是任何分区边界。请参见本示例中 LV 1 和 LV 2 之间的边界。

LVM 功能：

- 可以将多块硬盘或多个分区合并为一个较大的逻辑卷。
- 如果配置合适，当可用空间用完后，可以扩大 LV（例如 /usr）。

- 通过使用 LVM，可以在正在运行的系统中添加硬盘或 LV。但这需要能执行此类操作的可热插拔的硬件。
- 可以激活将逻辑卷的数据流分布在多个物理卷上的“分带方式”。如果这些物理卷驻留在不同的磁盘上，则可以提高读写性能，这与 RAID 0 类似。
- 使用快照功能可以在正在运行的系统中执行一致的备份（尤其适合服务器）。

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

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

除 LVM2 外，您还可以使用 EVMS（企业卷管理系统），它为逻辑卷和 RAID 卷提供了统一的接口。与 LVM2 类似，EVMS 也使用内核 2.6 中的设备映射器。

## 7.1.2 用 YaST 配置 LVM

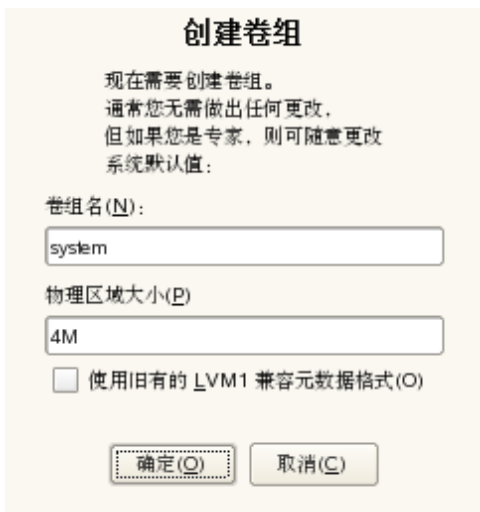
YaST 专家分区程序完成 YaST LVM 配置（请参见 [第 8.5.7 节“使用 YaST 分区程序”](#) [139]）。此分区工具用于编辑和删除现有分区并创建用于 LVM 的新分区。在此，首先单击 **创建 > 不格式化创建 IVM 分区**，然后选择 **0x8e Linux LVM** 作为分区标识符。创建好所有要与 LVM 一起使用的分区后，请单击 **LVM 开始 LVM 配置**。

### 创建卷组

如果系统上仍无卷组存在，则系统将提示您添加一个卷组（请参见 [图 7.2“创建卷组”](#) [106]）。也可以通过 **添加组** 创建其他组，但通常单独一个卷组就已足够。建议使用 **system** 作为包含 SUSE Linux Enterprise® 系统文件的卷组名。物理区域大小定义卷组中物理块的大小。卷组中的所有磁盘空间都是按此大小的区块来处理的。通常将这个值设置为 **4 MB**，并允许物理卷和逻辑卷的最大大小

采用 256 GB。如果要设置大于 256 GB 的逻辑卷，则只应增加物理区域大小（例如，增加到 8、16 或 32 MB）。

图 7.2 创建卷组



**创建卷组**

现在需要创建卷组。  
通常您无需做出任何更改，  
但如果您是专家，则可随意更改  
系统默认值：

卷组名(N):  
system

物理区域大小(P)  
4M

☐ 使用旧有的 LVM1 兼容元数据格式(O)

确定(O) 取消(C)

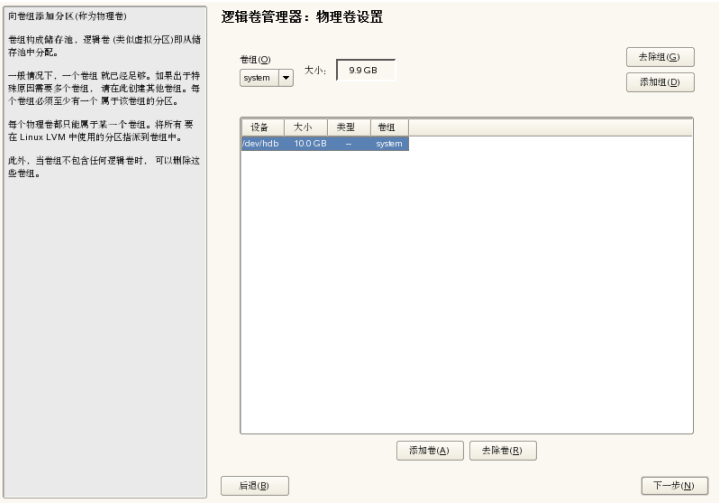
## 配置物理卷

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

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



图 7.3 物理卷设置

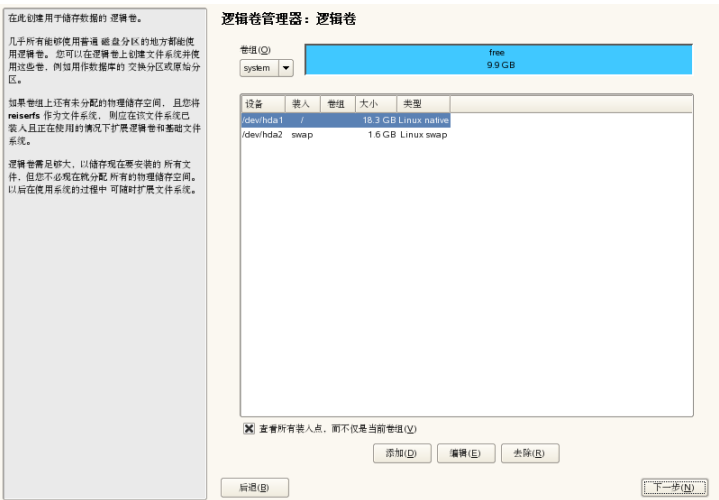


要将以前未指派的分区添加到所选的卷组中，请先单击该分区，然后单击添加卷。此时，卷组的名称就被输入到所选分区的旁边。将为 LVM 预留的所有分区指派给卷组。否则，分区中的空间仍处于未使用状态。在退出对话框前，必须为每个卷组指派至少一个物理卷。在指派所有物理卷后，单击下一步继续逻辑卷的配置。

## 配置逻辑卷

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

图 7.4 逻辑卷管理



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

---

**警告：分带**

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

---

图 7.5 创建逻辑卷

格式化

☐ 不格式化(N)

☒ 格式化(E)

文件系统(S)

Reiser

选项(P)

☐ 对文件系统加密(E)

逻辑卷名(N)

(如 var, opt)

大小: (如 4.0 GB 210.0 MB)(S)

2.4 GB

最大值 = 9.9 GB

最大值(X)

分带(P)

1

分带大小(S)

64

Fstab 选项(I)

装入点(M)

/home

确定(O)

取消(C)

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

## 直接 LVM 管理

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

### 7.1.3 使用 EVMS 进行储存管理

企业卷管理系统 2 (EVMS2) 是一种功能丰富的可扩展卷管理器，它带有内置群集感知。它的插件框架允许插件添加用于支持和识别任意分区类型的功能。由于具有群集感知，EVMS2 可确保受管设备名称在群集的每个节点上易于识别，从而更便于管理。

EVMS2 提供统一界面（`evmsgui` 和命令行）来管理以下储存资源：

- 本地媒体和基于 SAN 的媒体上的物理磁盘以及逻辑设备（包括 iSCSI）
- 软件 RAID 0、1、4 和 5（高可用性）
- 支持群集的多路径 I/O（容错）
- 带有 Cluster Segment Manager（CSM）插件的群集储存对象
- 所有文件系统的卷（具有用于 EVMS2 的文件系统接口模块（FSIM））
- 卷快照

在 SUSE Linux Enterprise Server 10 中，包含了以下新功能：

- EVMS2 和 CLVM2（Cluster Linux Volume Manager 2）使用内核中的相同多磁盘（MD）驱动程序和设备映射器（DM）驱动程序。
- 文件系统插件可用于 Heartbeat 2 Cluster Manager 和 Oracle Cluster File System 2。

## EVMS 设备

EVMS 管理实用程序可区分五种不同级别的设备：

### 磁盘

这是最低级别的设备。所有可作为物理磁盘访问的设备都会被当作磁盘。

### 段

段由磁盘上的分区和其他内存区域组成，如主引导记录（MBR）。

### 容器

容器相当于 LVM 中的卷组。

### 区域

可在区域中将可用设备分组为 LVM2 和 RAID。

### 卷

所有设备（无论这些设备是由真实分区、逻辑卷还是 RAID 设备表示）都可通过相应的装入点来访问。

如果选择使用EVMS，则必须使用EVMA设备名替换您的设备名。可在 `/dev/evms/` 中找到简单分区，逻辑卷位于 `/dev/evms/lvm/` 中，RAID设备位于 `/dev/evms/md` 中。要在引导时激活EVMS，请在YaST运行级别编辑器中向引导脚本添加 `boot.evms`。另请参见第20.2.3节“使用YaST配置系统服务（运行级别）”[365]。

## 更多信息

有关使用EVMS管理储存资源的信息，请参见 *Storage Administration Guide*（储存管理指南），安装包 `sles-stor_evms_en` 后可在 `/usr/share/doc/manual/sles-stor_evms_en` 中找到。有关EMVS的更多通用信息还可以在SourceForge\*托管的EVMS project [<http://evms.sourceforge.net/>]（EVMS项目）上的EVMS User Guide [[http://evms.sourceforge.net/users\\_guide/](http://evms.sourceforge.net/users_guide/)]（EVMS用户指南）中找到。

## 7.2 软 RAID 配置

RAID（独立磁盘冗余阵列）的用途是将多个硬盘分区合并成一个大的虚拟硬盘，以便优化性能和/或数据安全性。大多数RAID控制器使用SCSI协议，因为对大量硬盘，它可用比IDE协议更高效的方式寻址，更适于命令的并行处理。还有一些支持IDE或SATA硬盘的RAID控制器。软件RAID具有RAID系统的优势，并且没有硬件RAID控制器的额外成本。但是这需要一些CPU时间以及内存，所以不适用于真正高性能的计算机。

### 7.2.1 RAID 级别

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

常用的RAID级别如下：

#### RAID 0

此级别通过将每个文件按块分放到多个磁盘驱动器上，提高了数据访问性能。这实际上并不是真正的RAID，因为它未提供数据备份，但RAID 0已

成为这种类型的系统的标准名称。使用 RAID 0，可以将两块或多块硬盘组合在一起。这样性能固然很好，但如果有任何一块硬盘出现故障，都将损坏 RAID 系统并丢失数据。

#### RAID 1

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

#### RAID 2 和 RAID 3

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

#### RAID 4

级别 4 与级别 0 一样，也是在块一级进行分带，只是结合使用了专用的校验磁盘。当数据盘发生故障时，则可以利用奇偶校验数据来制作一块替代盘。不过，这块校验磁盘可能造成写访问的瓶颈。尽管如此，有时仍使用级别 4。

#### RAID 5

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

#### 其他 RAID 级别

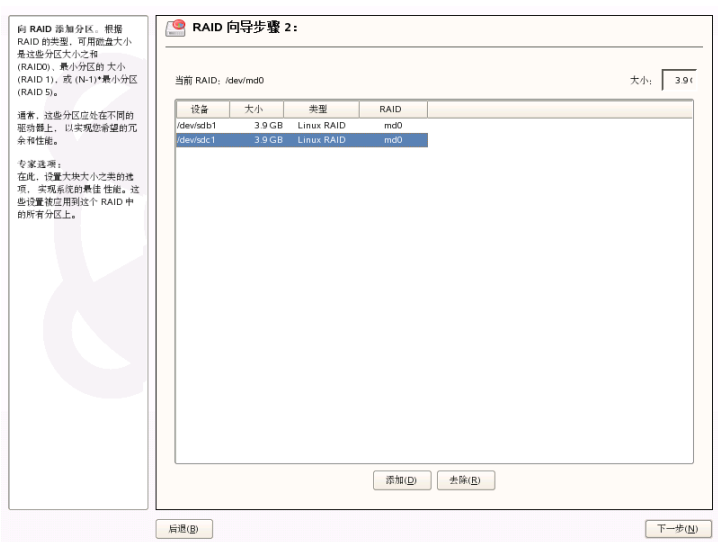
其他多种 RAID 级别也已开发出来（RAID n、RAID 10、RAID 0+1、RAID 30、RAID 50 等），其中某些级别属于硬件厂商创建的专有实施方法。由于这些级别并不是很普及，所以在此不再赘述。

# 7.2.2 使用 YaST 配置软 RAID

YaST Expert Partitioner 完成 YaST 软 RAID 配置，如第 8.5.7 节“使用 YaST 分区程序”[139]中所述。此分区工具用于编辑和删除现有分区并创建用于软 RAID 的新分区。利用该工具可创建 Raid 分区，方法是首先单击创建> 不格式化，然后选择 0xFD Linux RAID 作为分区标识符。对于 RAID 0 和 RAID 1，至少需要两个分区，对于 RAID 1，通常只需要两个分区。如果使用 RAID 5，则至少需要 3 个分区。建议只采用相同大小的分区。应将 RAID 分区储存在不同硬盘上，以降低由于某块硬盘出现问题而丢失数据的风险（RAID 1 和 5），同时还可以优化 RAID 0 的性能。创建了所有用于 RAID 的分区后，请单击 RAID > 创建 RAID 开始 RAID 配置。

在下一个对话框中选择 RAID 级别 0、1 和 5（有关详细信息，请参见第 7.2.1 节“RAID 级别”[111]）。单击下一步后，随即显示的对话框将列出类型为“Linux RAID”或“Linux native”的所有分区（请参见图 7.6“RAID 分区”[113]）。未显示交换分区或 DOS 分区。如果已将某个分区指派给 RAID 卷，则在列表中显示此 RAID 设备的名称（例如，/dev/md0）。用“--”表示未指派的分区。

图 7.6 RAID 分区



要将以前未指派的分区添加到所选的 RAID 卷中，请先单击该分区，然后单击添加。此时，RAID 设备的名称就被输入到所选分区的旁边。指派所有为 RAID

保留的分区。否则，分区中的空间仍处于未使用状态。指派了所有分区后，单击下一步进入设置对话框，从中对性能进行微调（请参见图 7.7“文件系统设置”[114]）。

图 7.7 文件系统设置



与传统的分区一样，设置所用的文件系统，以及RAID卷的加密方法和装入点。单击完成完成配置后，请查看 /dev/md0 设备和专家分区工具中指示为 RAID 的其他设备。

### 7.2.3 查错

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

### 7.2.4 有关详细信息

位于下列位置的 HOWTO 文档提供了软 RAID 的配置说明和详细信息：



- [http://www.novell.com/documentation/sles10/stor\\_evms/data/bookinfo.html](http://www.novell.com/documentation/sles10/stor_evms/data/bookinfo.html)
- </usr/share/doc/packages/mdadm/Software-RAID.HOWTO.html>
- <http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html>

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



# 使用 YaST 进行系统配置

在 SUSE Linux Enterprise 中，YaST 同时处理系统的安装和配置。本章将介绍系统部件（硬件）、网络访问、安全性设置和用户管理的配置。可在第 8.12 节“文本方式的 YaST”[166]中找出基于文本的 YaST 界面简介。对于手动系统配置的描述，请参见第 20.3 节“通过 /etc/sysconfig 配置系统”[366]。

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

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

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

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

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

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

## 8.1 YaST 语言

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

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

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

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

## 8.2 YaST 控制中心

以图形方式启动 YaST 时，会打开 YaST 控制中心，如 [图 8.1 “YaST 控制中心”](#) [119] 所示。左侧框架包含可用的类别。单击一个类别时，右边框架中会列出该类别的内容。然后选择希望使用的模块。例如，如果选择 **硬件** 并单击右框架中的 **声卡**，就会打开声卡的配置对话框。各个项目的配置通常需要多个步骤。按 **下一步** 继续进行下一步骤。

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

图 8.1 YaST 控制中心



---

**注意：YaST 软件管理 Gtk 和 Qt 前端**

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

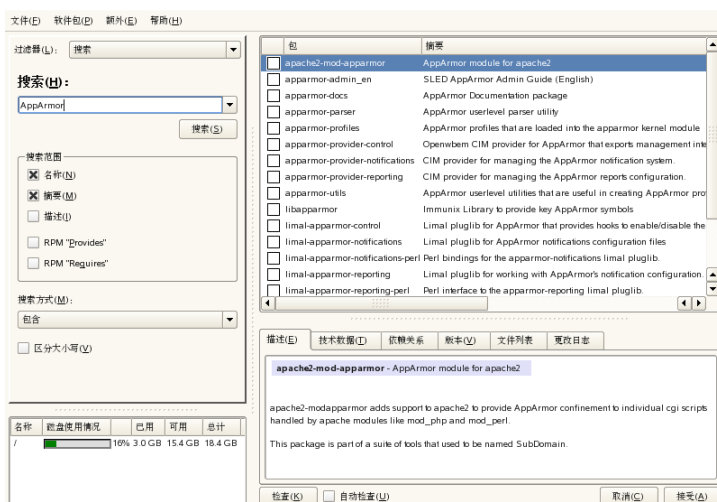
---

## 8.3 软件

### 8.3.1 安装和删除软件

要安装、卸载和更新计算机上的软件，请使用 **软件 > 软件管理**。这时会打开如图 8.2 “YaST 包管理器” [120] 中所示的包管理器对话框。

图 8.2 YaST 包管理器



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

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

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

## 安装包

要安装包，请选择要安装的包，然后单击接受。所选包应带有安装状态图标。包管理器会自动检查依赖性并选择所需要的任何其他包（解决依赖性）。要在单击接受前查看安装所需要的其他包，请从主菜单中选择其他 > 显示自动包更改。安装包后，单击安装更多可继续使用包管理器，或者单击完成将其关闭。

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

---

### 提示：所有可用包的列表

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

---

## 安装和删除模式

模式过滤器根据用途（如文件或打印服务器）对程序包进行分组。列出多组 模式过滤器和及安装过的预选包。

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

## 安装和删除语言支持

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

要从系统卸载语言，请从语言列表选择语言并取消选中行首的状态框。

---

### 注意

因为指定语言的包可能依赖于其他包，所以包管理器将选择安装其他包。

---

## 包和安装源

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

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

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

## 安装资源包

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

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

## 保存包选择

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

---

### 重要：硬件兼容性

因为此功能可保存确切的包列表，所以只有在源系统和目标系统上的硬件完全相同时，该功能才可靠。关于更复杂的情况，[第 5 章 自动安装](#) [77] 中所述的 **AutoYaST** 可能是更好的选择。

---

## 删除包

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

## 重安装包

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



## 搜索包、应用程序和文件

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

---

### 提示：快速搜索

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

---

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

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

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

## 安装摘要

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

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

## 有关包的信息

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

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

## 磁盘使用情况

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

## 检查依赖性

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

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

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

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

例如，可能无法同时安装 sendmail 和 postfix。图 8.3 “包管理器的冲突管理”[125]显示了冲突消息，提示您作出决定。已经安装了 postfix。因此，您可以选择不安装 sendmail、删除 postfix 或冒险同时安装二者并忽略冲突。

---

## 警告：处理包冲突

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

---

**图 8.3** 包管理器的冲突管理



## 安装 -devel 包

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

### 8.3.2 安装附加产品

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

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

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

---

#### 提示: 创建自定义的附加产品

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

---

## 8.3.3 选择安装源

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

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

## 8.3.4 注册 SUSE Linux Enterprise

要获取技术支持和产品更新, 必须注册和激活系统。如果安装期间跳过了注册, 请从 *软件 Novell Customer Center* 配置模块注册。此对话框与 [第 3.14.4 节 “Novell Customer Center 配置”](#) [37] 中所述的对话框一样。

## 8.3.5 YaST 联机更新

使用 YaST 联机更新来安装重要的更新和改进。包含增补程序的特定于产品的更新编目中提供 SUSE Linux Enterprise 的最新更新。添加或删除目录,用 **软件 > 安装源模块**（第 8.3.3 节“**选择安装源**”[126]里的说明。）

---

### 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 附带一年或三年订购期，在此期间，您可访问更新编目。订购结束后，将拒绝您访问更新编目。

如果对更新编目的访问遭到拒绝，您将看到一条警告消息，建议您访问 Novell Customer Center 并检查您的订购。可从 <http://www.novell.com/center/> 访问 Novell Customer Center。

---

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

## 术语定义

### 包

包是 rpm 格式的压缩文件，包含特定程序的文件。

### 增补程序

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

### patchrpm

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

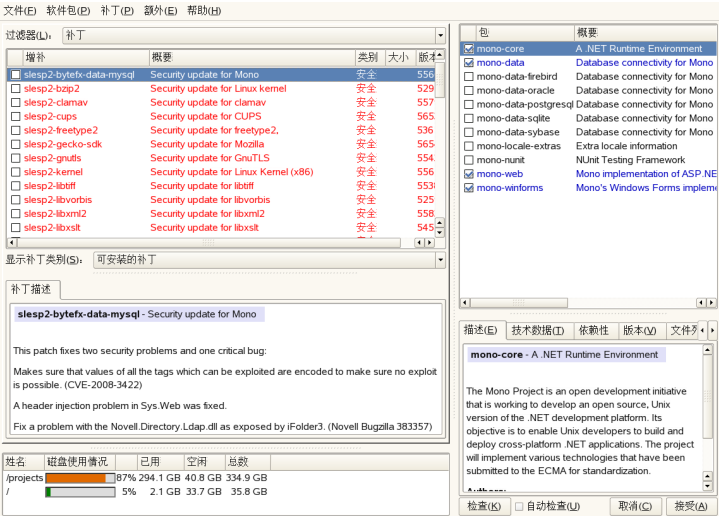
### deltarpm

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

# 手动安装增补程序

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

图 8.4 YaST 联机更新



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

## 可安装增补程序（默认视图）

当前未安装的适用于系统上已安装的包的增补程序。

## 可安装和已安装的增补程序

应用到系统上安装的包的所有增补程序

## 所有增补程序

SUSE Linux Enterprise 可用的所有增补程序。

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

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

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

---

### 提示：禁用 **deltarpm**

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

---

更新软件的另一种备选方法就是使用 KDE 和 GNOME 的 ZENworks 更新程序小程序。ZENworks 更新程序能够帮助监视新增补程序。它还提供快速更新功能。有关更多信息，请参考第 9.2 节“用 ZEN 工具管理包”[183]。

## 8.3.6 自动联机更新

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

选中仅下载增补程序后，将在指定时间下载增补程序但不会进行安装。它们必须手动进行安装。默认情况下，增补程序将下载到 **rug** 缓存目录 `/var/cache/zmd/web`。使用命令 `rug get-prefs cache-directory` 获取当前 **rug** 缓存目录。有关 **rug** 的详细信息，请参见第 9.1 节“从命令行使用 **rug** 更新包”[180]。

## 8.3.7 从增补程序 CD 更新

---

### 注意

在 s390 系统上，增补程序 CD 更新选项不可用。

---

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

## 8.3.8 更新系统

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

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

### 更新选项

设置您的系统的更新方法。有两个选项可用。

用“基于选择的新软件和功能安装”更新。

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

仅更新已安装的包

此选项仅更新系统上已存在的包。不会安装任何新功能。

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



## 包

单击 *包* 来启动包管理器并选择或取消选择要更新的各个包。应使用一致性检查来解决任何包冲突。中详细介绍了包管理器的使用。[第 8.3.1 节“安装和删除软件”](#) [119]

## 备份

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

---

### 重要：备份的范围

这里的备份不包括软件。它只包括配置文件。

---

## 语言

此处会列出系统上当前安装的主要和其他语言。可通过在显示的配置中单击 *语言* 或通过 *更改 > 语言* 来更改语言。（可选的）调整键盘布局和时区以适应使用该主要语言的地区。有关语言选择的详细信息请参见[第 8.5.15 节“语言选择”](#) [147]。

## 有关更新的重要信息

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

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

## 8.3.9 安装到“目录”

此 YaST 可让您将包安装到指定的目录。确定放置根目录的位置、命名目录的方式和希望安装的系统和软件类型。进入了此模块后，YaST 会确定系统设置

并列出默认目录、安装说明和要安装的软件。通过单击**更改**来编辑默认设置。必须通过单击**接受**来确认所有更改。在完成所有修改之后，连续单击**下一步**直到通知安装完成。单击**完成**退出对话框。

## 8.3.10 检查媒体

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

## 8.4 硬件

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

---

### 重要：型号指定

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

---

### 8.4.1 红外设备

用**硬件 > 红外线设备**配置红外线设备。单击**启动 IrDa**开始配置。您可在此配置**端口**和**波特率限制**。

### 8.4.2 图形卡和监视器

使用**硬件 > 图形卡和监视器**配置图形卡和监视器。它使用 SaX2 界面，如第 8.14 节“**SaX2**”[172]中所述。

## 8.4.3 打印机

通过 **硬件 > 打印机** 配置打印机。如果打印机正确地连接到系统，则应该会自动检测到打印机。有关使用 YaST 配置打印机的详细说明，请参见 [第 23.4 节“设置打印机”](#) [402]。

## 8.4.4 硬盘控制器

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

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

---

### 警告：硬盘控制器的配置

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

---

## 8.4.5 硬件信息

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

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

## 8.4.6 IDE DMA 方式

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

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

---

### 注意

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

---

## 8.4.7 IBM System z: DASD 设备

要在现有系统上添加 DASD，有两种途径：

### YaST

要向已安装系统添加 DASD，请使用 YaST DASD 模块（硬件 > *DASD*）。在第一个屏幕中，选择要用于 Linux 安装的磁盘，然后单击 **执行操作**。选择 **激活**，然后单击 **下一步退出对话框**。

### 命令行

执行以下命令：

```
dasd_configure 0.0.0150 1 0
```

用实际连接 DASD 的通道号替换 *0.0.0150*。如果要以 **DIAG** 模式访问 DASD，命令行的最后一个零应该变为 1。

---

### 注意

不管什么情况，都必须输入以下命令

```
mkinitrd  
zipl
```

以永久保留修改

---

## 8.4.8 IBM System z: ZFCP

要向已安装系统添加更多支持 FCP 的 SCSI 设备，请使用 YaST ZFCP 模块（*硬件>ZFCP*）。选择添加添加其他设备。从列表中选择通道号（适配器），并指定 *WWPN* 和 *FCP-LUN*。选择下一步和关闭后完成设置。通过检查 `cat /proc/scsi/scsi` 的输出，校验是否已添加此设备。

---

### 注意

运行以下命令，在重引导后永久保留您的修改。

```
mkinitrd  
zipl
```

---

## 8.4.9 游戏杆

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

如果是 USB 设备，则无需此配置。插入游戏杆即可使用。

## 8.4.10 键盘布局

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

单击 *专家设置* 来微调设置。通过在 *启动状态* 中选择所需的设置来调整键重复率以及延迟并配置启动状态。对于要锁定的设备，输入要应用 *Scroll Lock*、*Num Lock* 和 *Caps Lock* 设置的以空格隔开的设备列表。单击 *确定* 以完成微调。最后，在完成了所有选择之后，单击 *接受* 以使更改生效。

要设置图形环境的键盘，请运行图形 YaST，然后选择 **键盘布局**。有关图形配置的信息，请参见第 8.14.3 节“**键盘属性**” [176]。

## 8.4.11 鼠标方式

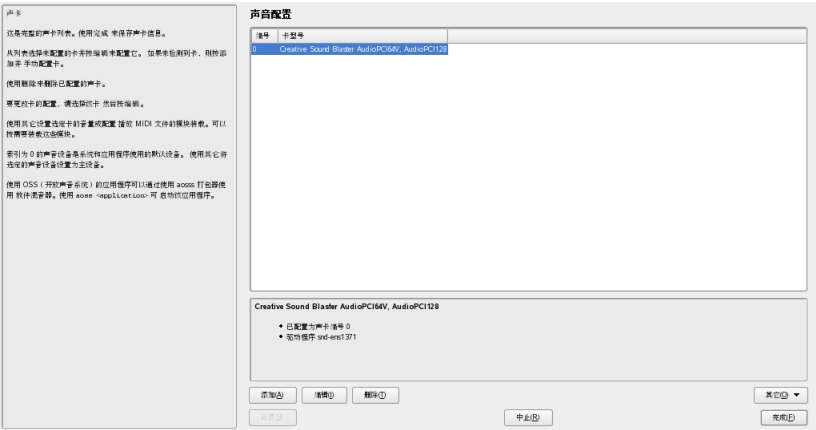
为图形环境配置鼠标时，请单击 **鼠标型号** 以访问 SaX2 鼠标配置。有关详细信息，请参见第 8.14.2 节“**鼠标属性**” [175]。

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

## 8.4.12 Sound

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

图 8.5 声音配置



如果 YaST 无法自动检测到您的声卡，请执行以下操作：

- 1 单击 **添加** 打开一个对话框，在此对话框中选择一个声卡供应商和型号。有关详细信息，请参考声卡文档。/usr/share/doc/packages/alsa/cards.txt 和

中提供了 ALSA 所支持的声卡及其对应声卡模块的参考列表。<http://www.alsa-project.org/alsa-doc/> 完成选择后，单击下一步。

## 2 在声卡配置中，在第一个设置屏幕中选择配置级别：

### 快速自动设置

不要求您进一步执行配置和任何声卡测试。这时将自动配置声卡。

### 常规设置

调整输出音量并播放测试声音。

### 可更改选项的高级设置

手动自定义所有设置。

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

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

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

单击其他手动自定义以下选项之一：

### 卷

使用此对话框设置音量。

### 启动序列器

要播放 MIDI 文件，请选中此选项。

### 设置主卡

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

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

## 8.5 系统

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

---

**提示：IBM System z：继续**

对于 IBM System z，请按照[第 8.5.3 节“引导加载程序配置”](#) [139]继续进行配置。

---

### 8.5.1 备份

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

### 8.5.2 恢复

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

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

---

**警告：系统恢复**

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

---



## 8.5.3 引导加载程序配置

要配置计算机现有系统的引导，请使用系统 > 引导加载程序模块。有关如何使用 YaST 配置引导加载程序的详细说明，请参考 [第 21.3 节 “使用 YaST 配置引导加载程序”](#) [378]。

## 8.5.4 群集

在 *Heartbeat Guide* 中查找关于检测信号和使用 YaST 的高可用性配置的信息。

## 8.5.5 LVM

逻辑卷管理器 (LVM) 是一种利用逻辑驱动器对硬盘进行自定义分区的工具。有关 LVM 的信息，请参见 [第 7.1 节 “LVM 配置”](#) [103]。

## 8.5.6 EVMS

企业卷管理系统 (EVMS) 与 LVM 一样，是一种将硬盘自定义分区和分组为虚拟卷的工具。它灵活、可扩展，并可以使用插件模型来满足不同卷管理系统的需要。

EVMS 兼容现有的内存和卷管理系统，如 DOS、Linux LVM、GPT（GUID 分区表）、IBM System z、Macintosh 和 BSD 分区。有关详细信息，请参考 <http://evms.sourceforge.net/>。

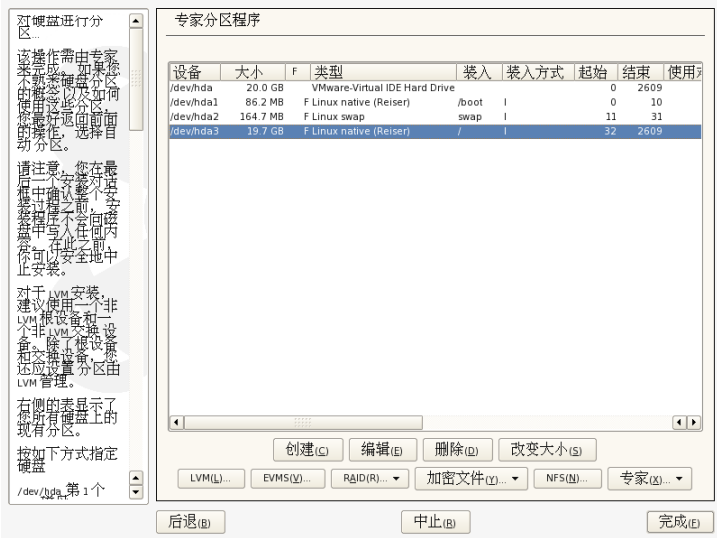
## 8.5.7 使用 YaST 分区程序

使用如 [图 8.6 “YaST 分区程序”](#) [140] 所示的专家分区程序，可以手动修改一个或多个硬盘的分区。可以添加、删除和编辑分区，并对分区重调整大小。还请从此 YaST 模块中获取软 RAID、EVMS 和 LVM 配置。

警告：对运行中的系统重新分区

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

图 8.6 YaST 分区程序



提示：IBM System z：设备名称

IBM System z 只能识别 DASD 和 SCSI 硬盘。不支持 IDE 硬盘。因此，如果这些设备是第一个识别出的设备，它们将在分区表中显示为 dasda 或 sda。

YaST 专家分区程序对话框中列出了所有已连接硬盘上的所有现有分区或建议分区。将整个硬盘作为不带编号的设备列出，如 /dev/hda 或 /dev/sda（或 /dev/dasda）。将分区作为这些设备的部分列出，如 /dev/hda1 或 /dev/sda1（或相应地列为 /dev/dasda1）。此外还显示硬盘的大小、类型、文件系统和装入点以及硬盘的分区。装入点描述分区在 Linux 文件系统树中的位置。

如果在安装期间运行专家对话框，还会列出并自动选中所有可用硬盘空间。要为 SUSE Linux Enterprise® 提供更多磁盘空间，请在列表中自下而上（从硬盘的最后一个分区向上到第一个分区）释放所需空间。例如，如果您有 3 个分区，

则不能将第 2 个分区专用于 SUSE Linux Enterprise，而为其他操作系统保留第 3 个和第 1 个分区。

## 分区类型

---

### 提示：IBM System z：硬盘

在 IBM System z 平台上，SUSE Linux Enterprise Server 支持 SCSI 硬盘以及 DASD（直接访问储存设备）。虽然可以按照以下介绍的方式对 SCSI 磁盘进行分区，但 DASD 在其分区表中的分区项不能超过 3 个。

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

主分区由指派给特定操作系统的一系列连续的柱面（物理磁盘区域）组成。仅使用主分区时，限制每个硬盘最多具有 4 个分区，因为超过 4 个分区就不能与分区表相符。这就是使用扩展分区的原因。扩展分区同样是一系列连续的磁盘柱面，但扩展分区本身可以再分为多个逻辑分区。逻辑分区不要求在分区表中有对应的项。换句话说，扩展分区是逻辑分区的容器。

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

---

### 提示：带有 GPT 磁盘标签的硬盘

对于使用 GPT 磁盘标签的体系结构，不限制主分区的数目。因此，将没有逻辑分区。

---

## 创建分区

要从头开始创建分区，请按以下步骤操作：

- 1 选择**创建**。如果连接了多个硬盘，则会出现一个选择对话框，可以在其中选择要用于新分区的硬盘。

- 2 指定分区类型（主要类型和扩展类型）。最多可以创建 4 个主分区或 3 个主分区和 1 个扩展分区。在扩展分区内，可以创建多个逻辑分区（请参见“[分区类型](#)”一节 [141]）。
- 3 如有必要，选择要使用的文件系统和装入点。YaST 会为所创建的每个分区建议一个装入点。有关各种文件的详细信息，请参考第 25 章 [Linux 中的文件系统](#) [429]。
- 4 如果您的设置需要其他文件系统选项，请指定它们。例如，如果您需要永久设备名称，则此操作是必需的。关于可用选项的细节，请参见“[编辑分区](#)”一节 [142]。
- 5 单击 **确定** > **应用** 应用您的分区设置并退出分区模块。

如果安装期间创建了分区，将返回到安装概述屏幕。

## 编辑分区

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

- 1 选择分区。
- 2 单击 **编辑** 来编辑分区并设置以下参数：

### 文件系统 ID

即使不希望在此阶段格式化分区，仍需要为它指派一个文件系统 ID 来确保正确注册分区。可能值包括 *Linux*、*Linux swap*、*Linux LVM*、*Linux EVMS* 和 *Linux RAID*。有关 LVM 和 RAID 的详细信息，请参考第 7.1 节“[LVM 配置](#)”[103]和第 7.2 节“[软 RAID 配置](#)”[111]。

### 文件系统

在此处更改文件系统或格式化分区。更改文件系统或重格式化分区将以不可逆转的方式从该分区删除所有数据。有关各种文件系统的细节，请参见第 25 章 [Linux 中的文件系统](#) [429]。

### 文件系统选项

在此可设置所选文件系统的各种参数。多数情况下可接受默认设置。

## 加密文件系统

如果激活加密，则将所有数据以加密形式写入硬盘。这可以提高敏感数据的安全性，但会稍微降低系统速度，因为加密需要一些时间。有关文件系统加密的详细信息，请参见[第 47 章 对分区和文件进行加密](#) [779]。

## Fstab 选项

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

## 装入点

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

### 3 选择确定 > 应用可激活分区。

## 专家选项

使用专家可打开包含以下命令的菜单：

### 重读取分区表

重读取磁盘中的分区。例如，在文本控制台中进行手动分区后需要此命令。

### 删除分区表和磁盘标签

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

## 更多分区提示

以下部分包含有关分区的一些提示，它们会在您设置系统时帮助您作出正确决定。

---

### 提示：柱面值

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

---

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

### 例 8.1 `/etc/fstab`: 分区数据

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

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

## 分区和 LVM

从专家分区工具中，使用 *LVM* 访问 LVM 配置（请参见 [第 7.1 节“LVM 配置”](#) [103]）。但是，如果系统中已经存在有效的 LVM 配置，当您在会话中首次进入 LVM 配置时将自动激活该配置。这种情况下，凡是包含属于激活卷组的分区的磁盘都无法进行重分区，因为当硬盘上有任何活动分区时，Linux 内核就无法重读取已经修改的该硬盘分区表。不过，如果系统上已存在有效的 LVM 配置，则不必进行物理重分区。但需要更改逻辑卷的配置。

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

---

### 警告：用于引导的文件系统

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

---

# 8.5.8 PCI 设备驱动程序

提示：IBM System z：继续

对于 IBM System z，请按照第 8.5.12 节“系统服务（运行级别）”[146]继续进行配置。

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

图 8.7 添加一个 PCI ID



要添加 ID，请单击添加并选择指派方式：方法是从列表中选择 PCI 设备或手动输入 PCI 值。在第一个选项里，从选择列表里选择 PCI 设备并输入驱动程序名和目录名。如果不输入目录名，则驱动程序名称将用作目录名。当手动指定 PCI ID 值的时候，输入正确的数据设置 PCI ID。单击确定保存修改。

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

## 8.5.9 电源管理

系统 > 电源管理模块提供使用节能技术工作的帮助。此功能对延长便携式计算机的工作时间非常重要。使用此模块的详情请参见 [第 28.6 节 “YaST 电源管理模块”](#) [478]。

## 8.5.10 Powertweak 配置

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

## 8.5.11 配置文件管理器

使用系统 > 配置文件管理（YaST 系统配置文件管理 (SCPM) 模块）来创建、管理和切换系统配置。它尤其适用于在不同位置（在不同网络中）和由不同用户使用的便携式计算机。这个功能对于固定计算机来说也同样有用，因为它使您能够使用多种不同的硬件部件或测试配置。

## 8.5.12 系统服务（运行级别）

使用系统 > 系统服务（运行级别）配置运行级别和以运行级别启动的服务。有关 SUSE Linux Enterprise 的运行级别的详细信息和 YaST 运行级别编辑器的介绍，请参考 [第 20.2.3 节 “使用 YaST 配置系统服务（运行级别）”](#) [365]。

## 8.5.13 /etc/sysconfig 编辑器

目录 `/etc/sysconfig` 所包含的文件中具有 SUSE Linux Enterprise 最重要的设置。使用系统 > */etc/sysconfig Editor* 修改值并将值保存到各配置文件。通常情况下不需要手动编辑，因为在安装包或配置服务时会自动调整这些文件。有关 `/etc/sysconfig` 和 YaST `sysconfig` 编辑器的详细信息，请参考 [第 20.3.1 节 “使用 YaST Sysconfig 编辑器更改系统配置”](#) [366]。



## 8.5.14 时间和日期的设置

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

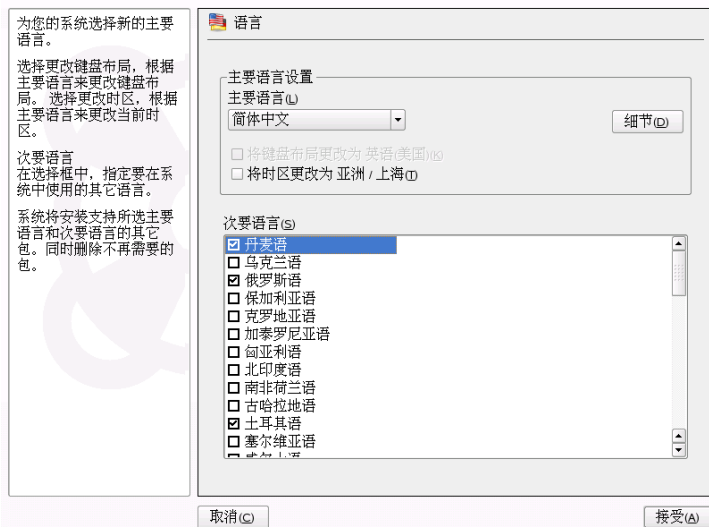
要更改时区，请在左栏选择区域，在右栏选择位置和时区。使用 **硬件时钟设置** 为将系统时钟设置为 **本地时间** 或 **UTC**（世界协调时间）。**UTC** 在 Linux 系统中会经常使用，而使用其他操作系统的计算机（如 Microsoft Windows）多数使用本地时间。

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

## 8.5.15 语言选择

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

图 8.8 设置语言



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

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

## 8.6 网络设备

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

### 8.6.1 DSL、SDN、调制解调器或网卡

要配置 DSL、ISDN、网络接口或调制解调器，请从 *网络设备* 部分选择相应的模块。对于自动检测到的设备，请从列表中选择它，然后单击 *编辑*。如果未检测到您的设备，请单击 *添加* 并手动选择它。要编辑现有设备，请选中该设备，然后单击 *编辑*。有关详细信息，请参见 [第 30.4 节“使用 YaST 配置网络连接”](#) [509]。有关无线网络接口，请参见 [第 29 章 无线通讯](#) [483]。

---

**提示：CDMA 和 GPRS 调制解调器**

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

---

## 8.7 网络服务

此组包含在网络中配置各种服务的工具。这包括名称解析、用户身份验证和文件服务。

### 8.7.1 邮件传送代理

如果您使用 sendmail、postfix 或服务提供商的 SMTP 服务器来发送电子邮件，可在 *网络服务 > 邮件传送代理* 中配置您的邮件设置。您可以通过 fetchmail 程序

获取邮件，还可以为此输入服务提供商的 POP3 或 IMAP 服务器的详细信息。此外，还可使用自己选择的邮件程序（如 KMail 或 Evolution）来设置您的访问数据。在这种情况下就不需要此模块。

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

#### 永久

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

#### 拨号

此项适用于在家中有电脑、不在网络中但有时连接到因特网的用户。

#### 没有连接

如果既不能访问因特网，又不在某个网络中，就无法发送或接收电子邮件。

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

## 8.7.2 邮件服务器

---

### 重要：基于 LDAP 的邮件服务器配置

SUSE Linux Enterprise 的邮件服务器模块仅当使用 LDAP 来管理用户、组以及 DNS 和 DHCP 服务时才有用。

---

邮件服务器模块允许将 SUSE Linux Enterprise 配置为邮件服务器。YaST 将协助配置过程的以下步骤：

#### 全局设置

配置本地邮件服务器的标识以及接收和发送信件的最大大小和邮件传送的类型。

本地发送

配置本地邮件发送的类型。

邮件传送

根据邮件的目标地址为其配置特殊的传送路由。

垃圾邮件防护

配置邮件服务器的垃圾邮件防护设置。这激活了 AMaViS 工具。设置 SPAM 检测的类型和严格性。

邮件服务器中继

确定不能从哪些网络使用邮件服务器来发送非本地邮件。

获取邮件

配置通过多种协议从外部邮箱帐户的邮件接收。

邮件服务器域

它确定着邮件服务器应负责哪些域。如果不希望服务器作为仅用于发送而不接收邮件的空客户机来运行，就必须至少配置一个主域。

3 种不同域类型的区分：

主域

本地邮件服务器的主域

本地

可以在主域中接收邮件的所有用户都可以在本地域中接收邮件。如果消息在本地域中，就仅对 @ 以前的部分求值。

虚拟域

只有在虚拟域中具有显式地址的用户才能接收邮件。虚拟邮件地址是在 YaST 的用户管理模块中设置的。

## 8.7.3 其他可用服务

YaST 网络服务提供了许多其他网络模块。

DHCP 服务器

使用它只需几个步骤就可以设置自定义 DHCP 服务器。[第 34 章 DHCP](#) [577] 提供了有关此主题的基本知识，并逐步介绍了配置进程。

## DNS 服务器

对于较大的网络，建议您配置 DNS 服务器来进行名称解析。为此，您可以使用 [第 33.2 节“用 YaST 配置”](#) [556] 中说明的 *DNS 服务器*。[第 33 章 域名系统](#) [555] 提供了有关 DNS 的背景信息。

## DNS 和主机名

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

## HTTP 服务器

要运行您自己的 Web 服务器，请在 *HTTP 服务器* 中配置 Apache。有关详细信息，请参见 [第 40 章 Apache HTTP 服务器](#) [667]。

## 主机名

引导并在小型网络中时，您可以使用 *主机名* 代替 DNS 进行主机名解析。此模块中的项反映文件 `/etc/hosts` 的数据。有关详细信息，请参见 [“/etc/hosts”一节](#) [533]。

## Kerberos 客户机

如果在您的网络中有 Kerberos 服务器用于网络身份验证，使用 *Kerberos 客户机*。有关使用 YaST 配置客户机的详细说明，请参见 [第 46.6 节“使用 YaST 配置 Kerberos 客户机”](#) [768]。

## LDAP 客户机

如果在网络中使用 LDAP 进行用户身份验证，请配置 *LDAP 客户机* 中的客户机。有关 LDAP 的信息和使用 YaST 进行客户机配置的详细说明，请参见 [第 36.6 节“使用 YaST 配置 LDAP 客户机”](#) [617]。

## LDAP 服务器

LDAP 服务器不仅能在中央目录中储存各种数据，还能将它们分发到您网络中的所有客户机。通常用它来储存共享联系信息，但它的功能不限于此。也能用一个 LDAP 服务器执行身份验证操作。有关 LDAP 的信息和使用 YaST 进行服务器配置的详细说明，请参见 [第 36 章 LDAP - 目录服务](#) [599]。

## NFS 客户机

使用 NFS 客户机，在您自己的文件树中装入 NFS 服务器提供的目录。使用 *NFS 客户机* 来配置您的系统以访问网络中的 NFS 服务器。

## NFS 服务器

使用 NFS，运行您的网络所有成员都能访问的文件服务器。使用此文件服务器可将一些应用程序、文件和储存空间供用户使用。在 *NFS 服务器* 中，可以将您的主机配置为 NFS 服务器，并确定要导出供网络用户共同使用的目录。具有适当权限的所有用户均可将这些目录装入他们自己的文件树中。介绍了 YaST 模块并提供了有关 NFS 的背景信息。[第 38 章 通过 NFS 共享文件系统](#) [645]

## NIS 客户机

如果在控制中心运行 NIS 服务器管理用户数据，并分发给客户，在这里设置客户机。有关 NIS 客户机和使用 YaST 进行配置的详细信息，请参见 [第 35.2 节 “配置 NIS 客户机”](#) [597]。

## NIS 服务器

如果您运行了多个系统，本地用户管理（使用文件 `/etc/passwd` 和 `/etc/shadow`）就变得不切实际，并需要很多的维护工作。在这种情况下，请在中央服务器上管理用户数据并从这里分发到客户机。NIS 是这样的一个选项。有关 NIS 和使用 YaST 对其进行配置的详细信息，请参见 [第 35.1.1 节 “配置 NIS 主服务器”](#) [592]。

## NTP 客户机

NTP（网络时间协议）是一个用于同步网络上硬件时钟的协议。有关 NTP 的信息和使用 YaST 进行配置的说明，请参见 [第 32 章 使用 NTP 同步时间](#) [549]。

## 网络服务 (xinetd)

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

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

---

### 警告：配置网络服务 (xinetd)

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

---

## 代理

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

## 远程管理

要通过另一台计算机来远程管理您的计算机，请使用 *远程管理*。要远程维护系统，请使用 VNC 客户程序（如 *krdc* 或支持 Java 的浏览器）。尽管使用 VNC 的远程管理非常简单和快速，但是它没有使用 SSH 安全，您在使用 VNC 服务器时应始终记住这点。有关安装 VNC 客户程序的详细信息，请参见 [第 4.1.1 节“通过 VNC 静态网络配置进行简单远程安装”](#) [44]。

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

强烈建议使用 YaST *远程管理* 模块来在计算机上配置 VNC。尽管 SaX2 接口也允许您设置远程访问属性，但是它不能替代 YaST。它只允许您将 X 服务器配置为主机以供 VNC 会话。

## 路由选择

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

## Samba 服务器

在包含 Linux 和 Windows 主机的异构网络中，Samba 控制着这两个世界之间的通讯。有关 Samba 以及服务器的配置的信息，请参考 [第 37 章 Samba](#) [629]。

## SLP 服务器

使用 *服务定位协议 (SLP)*，您无需知道服务器名称和服务即可设置网络中的客户机。有关 SLP 服务器和使用 YaST 进行配置的详细信息，请参见 [第 31 章网络中的 SLP 服务](#) [545]。

## TFTP 服务器

TFTP 服务器不同于 FTP 服务器。FTP 服务器采用“文件传送协议” (FTP)，而 TFTP 服务器采用没有安全功能简单多的“普通文件传送协议”。TFTP 服

务器常常用来引导无盘工作站、X 终端和路由器。有关 TFTP 服务器和使用 YaST 进行配置的详细信息，请参见第 4.3.2 节“设置 TFTP 服务器”[61]。

## WOL

WOL（网络唤醒）是指使用特殊包通过网络将计算机从待机方式中唤醒的功能。只有在 BIOS 支持的主板中才能实现该功能。使用 YaST 配置 WOL 的信息请参见第 4.3.7 节“局域网唤醒”[68]。

## Windows 域成员资格

在包含 Linux 和 Windows 主机的异构网络中，Samba 控制着这两个世界之间的通讯。用 *Samba* 客户机模块，可以把您的电脑设置为一个 Windows 域的成员。有关 Samba 和客户机的设置信息，参见第 37 章 *Samba* [629]。

## iSCSI 目标

iSCSI 技术提供了一种简便且价格合理的解决方案，可将 Linux 计算机连接到中央储存系统。要配置服务器端，请使用杂项 > *iSCSI* 目标。使用 YaST 配置 iSCSI 的更多信息请参见第 12 章 *经由 IP 网络的大容量储存 — iSCSI* [245]。

## iSCSI 发起程序

要配置与中央储存区的连接，请使用杂项 > *iSCSI* 发起程序。使用 YaST 配置 iSCSI 的更多信息请参见第 12 章 *经由 IP 网络的大容量储存 — iSCSI* [245]。

# 8.8 AppArmor

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

# 8.9 安全性和用户

多用户功能是 Linux 的一个基本特点。因此，多个用户可以相互独立地在同一个 Linux 系统上工作。每个用户都有一个由登录名标识的用户帐户和一个用于



登录系统的个人密码。所有用户都有自己的主目录，其中储存着他们的个人文件和配置。

## 8.9.1 用户管理

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

---

**提示：**在不关闭模块的情况下应用配置更改

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

---

### 添加用户

要添加新的用户，请如下继续操作：

- 1 单击“添加”。
- 2 为用户数据输入必需的数据。如果您不需要为此新用户调整任何其他の詳細设置，请继续**步骤 5** [155]。
- 3 要更改用户的 ID、主目录名、默认主目录、组、组成员资格、目录权限或登录 shell，请打开**细节**选项卡并更改默认值。
- 4 要调整用户的密码失效、长度和失效警告，请使用**密码设置**选项卡。
- 5 通过单击**接受**写入用户帐户配置。

新用户随后就可以使用创建的登录名和密码登录。

### 删除用户

要删除用户，请如下继续操作：

- 1 从列表中选择用户。

- 2 单击删除。
- 3 确定如何删除或保留要删除的用户的主目录。
- 4 单击是来应用设置。

## 更改登录配置

要更改登录配置，请执行如下操作：

- 1 从列表中选择用户。
- 2 单击编辑。
- 3 调整用户数据、细节和密码设置下的设置。
- 4 通过单击接受保存用户帐户配置。

## 管理加密的用户主目录

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

- 1 单击“添加”。
- 2 为用户数据输入必需的数据。
- 3 在细节选项卡中，激活使用加密用户主目录。
- 4 单击接受应用您的设置。

要为现有用户创建加密用户主目录，请执行以下操作：

- 1 在列表中选择用户并单击编辑。
- 2 在细节选项卡中，启用使用加密用户主目录。
- 3 输入选定用户的密码。

4 单击 **接受** 应用您的设置。

要禁用用户主目录的加密，请执行以下操作：

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

有关加密用户主目录的详细信息，请参见 [第 47.2 节 “使用加密的用户主目录”](#) [782]。

## 自动登录

---

### 警告：使用自动登录

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

---

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

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

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

## 不用密码登录

---

### 警告：允许不用密码登录

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

---

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

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

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

## 禁用用户登录

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

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

要为现有用户禁用登录，请执行以下操作：

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

## 强制实施密码策略

在有多个用户的系统上，最好至少强制实施基本的密码安全性策略。用户应该定期更改其密码并使用不能轻易识破的可靠密码。关于如何强制实施更严格的密码规则的信息，请参考第8.9.3节“本地安全”[161]。要强制实施密码循环，请创建密码失效策略。

要为新用户配置密码失效策略，请执行以下操作：

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

要为现有用户更改密码失效策略，请执行以下操作：

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

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

## 更改新用户的默认设置

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

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

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

**3** 单击接受应用您的更改。

可使用本地安全性模块更改与安全性相关的几个其他默认设置。相关信息请参见 [第 8.9.3 节“本地安全”](#) [161]。

## 更改密码加密

---

### 注意

密码加密中的更改仅适用于本地用户。

---

SUSE Linux Enterprise 可使用 DES、MD5 或 Blowfish 进行密码加密。加密方法的默认密码是 Blowfish。如 [第 3.14.1 节“系统管理员“root”的密码”](#) [34]中所述，加密方法是在系统安装期间设置的。要更改已安装系统中的密码加密方法，请选择 **专家选项 > 密码加密**。

## 更改身份验证和用户源

如 [第 3.14.7 节“用户数”](#) [39]中所述，用户管理方法（如 NIS、LDAP、Kerberos 或 Samba）是在安装期间设置的。要更改已安装系统中的用户身份验证方法，请选择 **专家选项 > 身份验证和用户源**。该模块提供配置概述和配置客户机的选项。使用此模块还能够进行高级客户程序配置。

## 8.9.2 组管理

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

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

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

单击 *专家选项* 以进行高级组管理。有关这些选项的详细信息请参见 [第 8.9.1 节“用户管理”](#) [155]。

## 8.9.3 本地安全

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

详细的或自定义的设置包括：

### 密码设置

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

### 引导设置

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

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

### 登录设置

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

### 用户添加

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

### 其他设置

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

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

按 *完成* 以完成安全性配置。



## 8.9.4 证书管理

证书做通讯使用，并且能在例如公司ID卡类的地方找到。要管理证书或导入普通服务器证书，请使用**安全和用户 > CA 管理**。有关证书及其技术和使用 YaST 管理的详细信息，请参见**第 42 章 管理 X.509 认证** [723]。

## 8.9.5 防火墙

SuSEfirewall2 可以保护您的计算机免受来自因特网的攻击。用**安全性和用户 > 防火墙**对其进行设置。有关 SuSEfirewall2 的详细信息，请参见**第 43 章 伪装和防火墙** [737]。

---

**提示：自动激活防火墙**

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

---

## 8.10 虚拟化

虚拟化允许在一台物理计算机上运行多个操作系统。为不同系统提供的硬件都是虚拟化的。虚拟化 YaST 模块提供有关 Xen 虚拟化系统的配置。有关此技术的更多信息，请参见<http://www.novell.com/documentation/sles10/index.html> 上的虚拟化手册。

以下模块在**虚拟化**部分中可用：

安装 Hypervisor 和工具

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

创建虚拟机

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

## 8.11 杂项

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

### 8.11.1 创建“自定义安装 CD”

通过杂项 > *CD 刻录程序*，您可以从原始安装集中创建自定义的安装 CD。要开始创建，单击添加。使用包管理器选择包或某 AutoYaST 控制文件，从而使用预配置的 AutoYaST 配置文件以用于创建。

### 8.11.2 “安装服务器”设置

对于网络安装，需要安装服务器。要配置此类服务器，请使用杂项 > *安装服务器*。有关使用 YaST 配置安装服务器的更多信息，请参见第 4.2.1 节“使用 YaST 设置安装服务器” [51]。

### 8.11.3 自动安装

AutoYaST 工具用于自动安装。在*其他 > 自动安装*中，准备此工具的配置文件。使用 AutoYaST 自动安装的详情，请参见第 5 章 *自动安装* [77]。关于使用自动安装模块的信息，请参见第 5.1.1 节“创建 AutoYaST 配置文件” [78]。

### 8.11.4 支持查询

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

### 8.11.5 版本发行说明

发行说明是有关安装、更新、配置和技术问题的重要信息来源。发行说明将通过联机更新不断更新和发布。使用*其他 > 发行说明*来查看发行说明。

## 8.11.6 启动日志

在*其他 > 启动日志*中查看有关计算机的启动的信息。当系统发生问题或进行故障诊断时，您可能会首先希望查看此模块。它显示引导日志 `/var/log/boot.msg` 中包含计算机启动时显示的屏幕消息。查看此日志有助于确定计算机是否正确启动，以及所有服务和功能是否正确启动。

## 8.11.7 系统日志

使用*其他 > 系统日志*来查看 `var/log/messages` 中跟踪计算机操作的系统日志。这里还记录着内核消息，并按照日期和时间进行排序。使用顶部的框查看特定系统组件的状态。系统日志和引导日志模块中可能有以下选项：

`/var/log/messages`

这是常规系统日志文件。在此处，您可以查看内核消息、作为 `root` 登录的用户和其他非常有用的信息。

`/proc/cpuinfo`

此选项显示处理器信息，包括处理器类型、制造商、型号和性能。

`/proc/dma`

此选项显示当前使用的 DMA 通道。

`/proc/interrupts`

此选项显示正在使用的中断和已使用的中断数量。

`/proc/iomem`

此选项显示输入/出内存的状态。

`/proc/ioports`

此选项显示当时正在使用的 I/O 端口。

`/proc/meminfo`

此选项显示内存状态。

`/proc/modules`

此选项显示各个模块。

/proc/mounts

此选项显示当前装入的设备。

/proc/partitions

此选项显示所有硬盘的分区。

/proc/version

此选项显示当前的 Linux 版本。

/var/log/YaST2/y2log

此选项显示所有 YaST 日志消息。

/var/log/boot.msg

此选项显示关于系统启动的信息。

/var/log/faillog

此选项显示登录故障。

/var/log/warn

此选项显示所有系统警告。

## 8.11.8 供应商驱动程序 CD

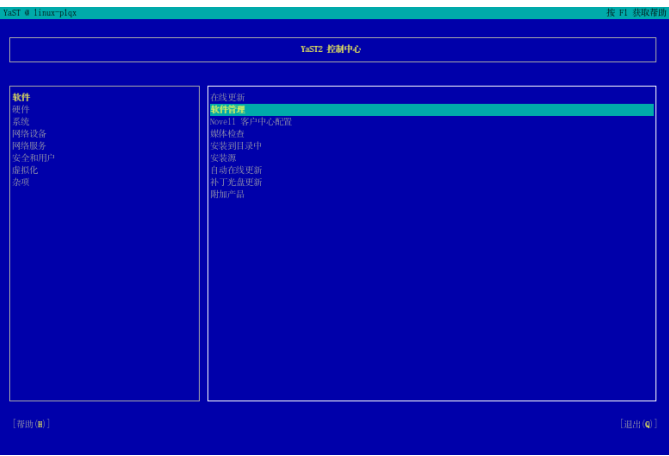
使用 *其他 > 供应商驱动程序 CD*，从包含 SUSE Linux Enterprise 驱动程序的 Linux 驱动程序 CD 安装设备驱动程序。当从头开始安装 SUSE Linux Enterprise 时，在安装后应使用此 YaST 模块从供应商 CD 装载所需的驱动程序。

## 8.12 文本方式的 YaST

本节所针对的读者是在其系统上不运行 X 服务器而依赖于基于文本的安装工具的系统管理员和专家。它提供了与以文本方式启动和操作 YaST 有关的基本信息。

当以文本方式启动 YaST 时，将首先出现 YaST 控制中心。请参见图 8.9 “**文本方式下 YaST 的主窗口**” [167]。该窗口包含三个区域。左框架有一个深白色边框，其中列出各个模块所属的类别。它使用有色背景来指示活动类别。具有狭窄的白色边框的右框架提供了活动类别中可用模块的概述。底部框架中包含 *帮助* 和 *退出* 按钮。

图 8.9 文本方式下 YaST 的主窗口



启动 YaST 控制中心时，将自动选择软件类别。使用 ↓ 键和 ↑ 键可更改类别。要从所选类别启动某个模块，请按 → 键。模块选择此时显示有深色边框。使用 ↓ 键和 ↑ 键可选择所需模块。按住箭头键在可用模块列表中滚动。选中某个模块后，即会以彩色背景显示模块标题，同时在底部框架中显示简要说明。

按 Enter 键启动所需模块。模块中的各种按钮和选择字段中包含一个具有不同颜色（默认为黄色）的字母。使用 Alt + yellow\_letter 可直接选择按钮，而无需使用 Tab 键导航到那里。通过按 Alt + Q 组合键或选择退出并按 Enter 退出 YaST 控制中心。

## 8.12.1 在模块中导航

下面在介绍 YaST 模块中的控制元素时，均假定所有功能键和 Alt 组合键都可用并且没有被指派不同的全局功能。有关可能出现的异常的信息，请参见第 8.12.2 节“组合键的限制” [168]。

在按钮和选择列表中导航

使用 Tab 和 Alt + Tab 或 Shift + Tab 可在按钮和包含选择列表的框架中导航。

在选择列表中导航

使用箭头键（↑ 和 ↓）可浏览包含选择列表的活动框架中的各个元素。如果框架内的项超出了框架宽度，请使用 Shift + → 或 Shift + ← 来左右水平滚

动。也可以使用 Ctrl + E 或 Ctrl + A 。如果使用 → 或 ← 键会导致更改活动框架或当前选择列表（像在控制中心中那样），则可以使用此组合键。

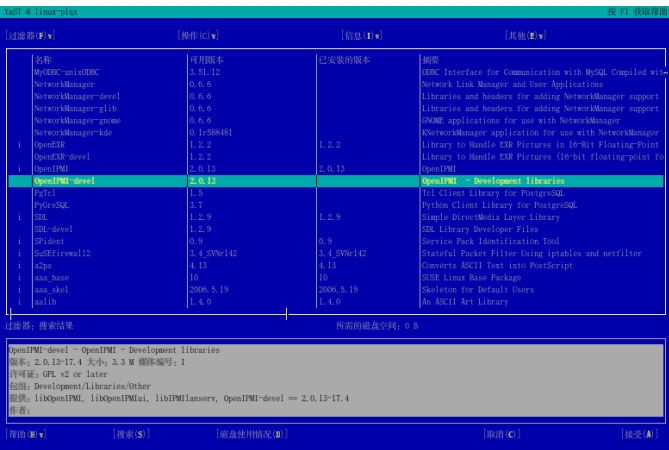
按钮、单选项按钮和复选框

要选择带空方括号（复选框）或空圆括号（单选按钮）的按钮，请按 Space 或 Enter 键。也可以直接使用 Alt + yellow\_letter 来选择单选按钮和复选框。在这种情况下，无需使用 Enter 键进行确认。如果使用 Tab 键导航到某个项目，请按 Enter 键执行所选操作或激活相应的菜单项。

功能密钥

使用各功能键（F1 到 F12）可快速访问多个按钮。功能键和按钮的实际映射关系取决于活动 YaST 模块，因为不同的模块提供不同的按钮（详细信息、信息、添加、删除等）。可以将 F10 键用作确定、下一步和完成。按 F1 键可访问 YaST 帮助，其中显示了与各个 F 键对应的功能。

图 8.10 软件安装模块



8.12.2 组合键的限制

如果您的窗口管理器使用全局 Alt 组合键，则 YaST 中的 Alt 组合键可能无效。像 Alt 或 Shift 这样的键也可能被终端设置占用。

使用 Esc 代替 Alt

Esc 可以代替 Alt 来执行 Alt 快捷键。例如，Esc - H 可代替 Alt + H。（首先按 Esc，然后按 H 键。）

使用 **Ctrl + F** 和 **Ctrl + B** 执行向后和向前导航

如果 **Alt** 和 **Shift** 组合键被窗口管理器或终端占用，可改用组合键 **Ctrl + F**（向前）和 **Ctrl + B**（向后）。

功能键的限制

功能键也可用于执行多种功能。某些功能键可能会被终端占用而不能用于 YaST。但 **Alt** 组合键和功能键应该始终在纯文本控制台上完全可用。

## 8.13 通过命令行管理 YaST

任务只需执行一次时，图形或 **ncurses** 界面通常是最佳的解决方案。如果任务需要重复执行，则可能使用 YaST 命令行界面更佳简便。自定义脚本也可以使用此界面来自动执行任务。

要查看系统上所有可用模块名称的列表，请使用 `yast -l` 或 `yast --list`。要显示某个模块的可用选项，请输入 `yast module_name help`。如果模块没有命令行模式，则会显示告知您此情况的消息。

要显示某个模块命令选项的帮助，请输入 `yast module_name command help`。要设置选项值，请输入 `yast module_name command option=value`。

因为已存在具有同样功能的命令行工具，所以某些模块不支持命令行模式。涉及的模块和可用命令行工具为：

**sw\_single**

`sw_single` 提供包管理和系统更新功能。请在脚本中使用 `rug`，而不是 YaST。请参考 [第 9.1 节“从命令行使用 rug 更新包”](#) [180]。

**online\_update\_setup**

`online_update_setup` 配置系统的自动更新。它可以用 `cron` 进行配置。

**inst\_suse\_register**

使用 `inst_suse_register` 来注册您的 SUSE Linux Enterprise。关于注册的详细信息，请参见 [第 8.3.4 节“注册 SUSE Linux Enterprise”](#) [126]。

**hwinfo**

`hwinfo` 提供系统的硬件信息。命令 `hwinfo` 也可以实现同样的功能。

GenProf、LogProf、SD\_AddProfile、SD\_DeleteProfile、SD\_EditProfile、SD\_Report 和 子域

这些模块控制或配置 AppArmor。AppArmor 具有自己的命令行工具。

## 8.13.1 管理用户

用于用户管理的 YaST 命令与传统的命令不一样，它们考虑到了创建、修改或删除用户时系统上已配置的身份验证方法和默认用户管理设置。例如，您在添加用户期间或之后无需创建用户主目录或复制 `skel` 文件。输入用户名和密码后，所有其他设置将按照默认配置自动完成。命令行提供的功能与图形界面一样。

YaST `users` 模块用于用户管理。要显示命令行选项，请输入 `yast users help`。

要添加多个用户，请用要添加用户的列表来创建一个 `/tmp/users.txt` 文件。每行输入一个用户名并使用以下脚本：

### 例 8.2 添加多个用户

```
#!/bin/bash
#
# adds new user, the password is same as username
#

for i in `cat /tmp/users.txt`;
do
    yast users add username=$i password=$i
done
```

与添加一样，您可以删除 `tmp/users.txt` 中定义的用户。



### 例 8.3 删除多个用户

```
#!/bin/bash
#
# the home will be not deleted
# to delete homes, use option delete_home
#

for i in `cat /tmp/users.txt`;
do
yast users delete username=$i
done
```

## 8.13.2 配置网络和防火墙

脚本中通常需要网络和防火墙配置命令。请使用 `yast lan` 配置网络，使用 `yast firewall` 来配置防火墙。

要显示 YaST 网卡配置选项，请输入 `yast lan help`。要显示 YaST 防火墙卡配置选项，请输入 `yast firewall help`。YaST 网络和防火墙配置始终保持不变。重引导后，无需再次执行脚本。

要显示网络的配置摘要，请使用 `yast lan list`。例 8.4 “`yast lan list` 的输出样本” [171] 输出中的第 1 项是设备 ID。要获取设备配置的详细信息，请使用 `ast lan show id=<number>`。此示例中正确的命令为 `yast lan show id=0`。

### 例 8.4 `yast lan list` 的输出样本

```
0          Digital DECchip 21142/43, DHCP
```

YaST 防火墙配置的命令行界面是用来启用和禁用服务、端口或协议的快捷方法。要显示允许的服务、端口和协议，请使用 `yast firewall services show`。要获取如何启用服务或端口的示例，请使用 `yast firewall services help`。要启用伪装，请输入 `yast firewall masquerade enable`。

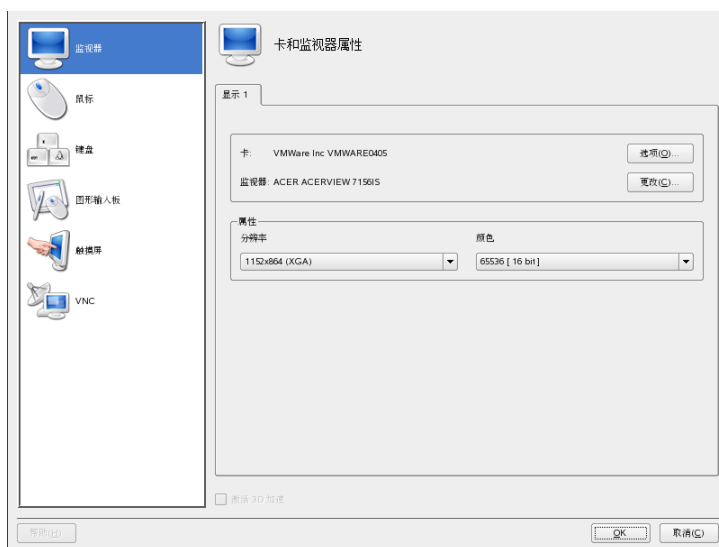
## 8.14 SaX2

通过 **硬件 > 图形卡和监视器** 配置系统的图形环境。这会打开 SUSE 高级 X11 配置接口 (SaX2)，您可以在其中配置设备(如鼠标、键盘或显示设备)。此界面还可以通过使用 **计算机 > 更多应用程序 > 系统 > Sax2** 从 GNOME 主菜单中访问或通过使用 **系统 > 配置 > SaX2** 从 GNOME 主菜单访问。

### 8.14.1 卡和监视器属性

在 **卡和监视器属性** 中调整图形卡和显示设备的设置。如果您安装了多个图形卡，则每个设备会显示在不同的对话框中，可以通过选项卡来使用对话框。在对话框的顶部，可查看选定图形卡和与该图形卡连接的监视器的当前设置。如果可以将多个屏幕与卡连接（双头），则会显示主输出上的监视器。通常，在安装期间系统会自动检测到卡和显示设备。但是，您可以手动调整一些参数，甚至完全更改显示设备。

图 8.11 卡和监视器属性



---

### 提示：自动检测新的显示硬件

如果在安装后更改了显示硬件，请在命令行上使用 `sax2 -r` 让 **SaX2** 检测您的硬件。您必须是 `root` 用户才能通过命令行运行 **SaX2**。

---

## 图形卡

不能更改图形卡，因为仅支持已知型号，并且将自动检测这些型号。但是，您可以更改影响卡的行为的一些选项。通常，并不需要更改，因为安装期间系统已适当地设置了这些选项。如果您是专家并且希望精确调整一些选项，则单击图形卡旁的选项并选择要更改的选项。要将所需值指派到特定选项，在选择该选项之后出现的对话框中输入该值。单击**确定**关闭选项对话框。

## 监视程序

要更改监视器的当前设置，请单击监视器旁的**更改**。将会打开一个新对话框，您可以在其中调整各种特定于监视器的设置。此对话框有若干用于各个监视器操作部分的选项卡。选择第一个选项卡来在两个列表中手动选择显示设备的供应商和型号。如果未列出监视器，则您可以选择适合需要的 **VESA** 或 **LCD** 方式，如果您有供应商驱动程序磁盘或 **CD**，则单击**使用磁盘**并遵循屏幕上的指示来使用。选中**激活 DPMS**来使用显示电源管理信号。系统通常已正确设置显示大小（*监视器的几何属性*）和同步频率（*监视器的水平和垂直同步频率的范围*），但您也可以手动修改这些值。在进行了所有的调整之后，单击**确定**关闭此对话框。

---

### 警告：更改监视器频率

虽然提供有安全机制，但在手动更改所允许的监视器频率时仍要非常小心。不正确的值可能损坏监视器。更改频率之前，您应始终参考监视器的手册。

---

## 分辨率和颜色深度

可以从对话框中间的两个列表直接选择分辨率和颜色深度。您在此处选择的分辨率表示要使用的最高分辨率。最低为 **640x480** 的所有常用分辨率也会被自动添加到配置中。根据使用的图形桌面，您稍后可以切换为任意选项而无需重配置。

## 双头

如果您的计算机上安装了带有两个输出的图形卡，则您可以将两个屏幕与系统连接。连接到相同图形卡的两个屏幕被称为双头。SaX2 会自动检测系统中的多个显示设备并会相应地准备配置。要使用图形卡的双头方式，请选中对话框底部的激活双头方式并单击配置来在双头对话框中设置双头选项和屏幕排列。

在此对话框的顶部有一行选项卡，每个选项卡对应于系统中的一个图形卡。选择要配置的卡并在下面的对话框中设置其多头选项。在多头对话框的上方，单击更改来配置其他屏幕。可能的选项与第一个屏幕的选项相同。从列表中选择此屏幕使用的分辨率。在三个可能的多头方式中选择一个。

### 克隆多头

在此方式下，所有监视器均显示相同的内容。鼠标仅在主屏幕上可见。

### Xinerama 多头

所有屏幕组合起来构成一个大屏幕。可以将程序窗口放置在所有屏幕上，也可以调整为填满多个监视器的某一大小。

---

### 注意

Linux 目前尚未提供对 Xinerama 多头环境的 3D 支持。在这种情况下，SaX2 将取消 3D 支持。

---

双头环境的排列描述各个屏幕的顺序。默认情况下，SaX2 将配置符合检测出的屏幕的顺序的标准布局，将所有屏幕从左到右排列成一行。在对话框的排列部分，通过选择一个顺序按钮来确定监视器排列的方式。单击确定关闭对话框。

---

### 提示：通过便携式计算机使用投影机

要将投影机连接到便携式计算机，请激活双头模式。在这种情况下，SaX2 以 1024x768 的分辨率和 60 hz 的刷新率配置外部输出。这些值对多数投影机都非常适用。

---

## 多头

如果在计算机中安装了多个图形卡，则可以为系统连接多个屏幕。连接到不同图形卡的两个或多个屏幕被称为多头。SaX2 会自动检测系统中的多个图形卡并会相应地准备配置。默认情况下，SaX2 将配置符合所检测出的图形卡的顺序的

标准布局，将所有屏幕从左到右排列成一行。其他 *排列* 选项卡允许手动更改此布局。在网格中拖动表示各个屏幕的图标，并单击 *确定* 来关闭对话框。

## 测试配置

在完成对监视器和图形卡的配置后，在主窗口中单击 *确定*，然后测试您的设置。这可以确保您的配置适合自己的设备。如果图像不稳定，请通过按 **Ctrl+Alt+Backspace** 来立即终止测试，然后降低刷新率或分辨率和颜色深度。

---

### 注意

无论您是否运行测试，所有修改均在您重新启动 X 服务器后被激活。

---

## 8.14.2 鼠标属性

在 *鼠标属性* 中调整鼠标的设置。如果您有安装了不同驱动程序的多鼠，则每个驱动程序会显示在不同的选项卡中。使用相同驱动程序运行的多个设备会显示为一个鼠标。要激活或取消当前选定的鼠标，请使用对话框顶部复选框。在复选框的下面可以查看该鼠标的当前设置。通常，会自动检测到鼠标，但是如果自动检测失败，您可以手动更改。请参考鼠标文档来获取型号描述。单击 *更改* 以从两个列表中选择供应商和型号，然后单击 *确定* 来确认选择。在对话框的选项部分中，设置用于运行鼠标的各种选项。

### 激活 3 键仿真

如果您的鼠标只有两个按键，则当您同时单击两个按键即是仿真第三个按键。

### 激活鼠标滚轮

选中此框以使用滚轮。

### *Invert X-Axis* 和 *Invert Y-Axis*

如果选择了以下选项之一，请将鼠标指针向相反方向移动。对触摸屏，该功能有时很有用。

### 用鼠标按键模拟滚轮

如果您的鼠标没有滚轮，但是您希望使用类似功能，则您可以为此功能指派一个附加按键。选择要使用的按钮。在按此按键时，鼠标的任何移动都会被转换为滚轮命令。此功能对于轨迹球特别有用。

当您对设置满意时，单击 **确定** 来确认更改。

---

### 注意

只有在您重新启动 X 服务器之后，您在此处所做的更改才会生效。

---

## 8.14.3 键盘属性

使用此对话框来调整在图形环境中操作键盘的设置。在对话框的上边，选择类型、语言布局和变体。使用对话框底部的测试字段来检查特殊字符是否正确显示。从中间的列表中选择要使用的其他布局 and 变体。根据桌面的类型，可以在运行的系统中切换这些选项而无需重配置。在您单击 **确定** 之后，将立即应用更改。

## 8.14.4 图形输入板属性

使用此对话框来配置连接到您系统的图形输入板。单击 **图形输入板** 选项卡来从列表中选择供应商和型号。目前支持有限数量的图形输入板。要激活输入板，选中对话框顶部的 **激活此输入板**。

在 **端口和方式** 对话框中，配置到输入板的连接。SaX2 支持将图形输入板配置为连接到 USB 端口或串口端口。如果将输入板连接到串行端口，请校验此端口。`/dev/ttyS0` 指第 1 个串行端口。`/dev/ttyS1` 指第 2 个串行端口。其他端口使用类似的表示法。从列表选择适当的选项并选择适合您需要的主输入板方式。

如果您的图形输入板支持电子笔，则在 **电子笔** 中配置电子笔。添加橡皮和笔，并在单击 **属性** 之后设置它们的属性。

当您对设置满意时，单击 **确定** 来确认更改。

## 8.14.5 触摸屏属性

使用此对话框来配置连接到您系统的触摸屏。如果您安装了多个触摸屏，则每个设备会显示在不同的对话框中，可以通过选项卡来使用对话框。要激活当前选定的触摸屏，请选中对话框顶部的 **指派要显示的触摸屏**。从下面的列表中选择供应商和型号并在底部设置相应的 **连接端口**。您可以配置连接到 USB 端口或

串口端口的触摸屏。如果触摸屏连接到串行端口，请校验此端口。`/dev/ttyS0` 指第 1 个串行端口。`/dev/ttyS1` 指第 2 个串行端口。其他端口使用类似的表示法。当您对设置满意时，单击**确定**来确认更改。

## 8.15 故障诊断

目录 `/var/log/YaST2` 中记录了所有错误消息和警报。查找 YaST 问题的最重要文件是 `y2log`。

## 8.16 更多信息

可在以下网站和目录中找到有关 YaST 的更多信息：

- `/usr/share/doc/packages/yast2` - 本地 YaST 开发文档
- [http://www.opensuse.org/YaST\\_Development](http://www.opensuse.org/YaST_Development) - openSUSE wiki 中的 YaST 项目页
- <http://forge.novell.com/modules/xfmod/project/?yast> - 另一 YaST 项目页





## 通过 ZENworks 管理软件

SUSE Linux Enterprise 能够集成到由 Novell ZENworks Linux Management 管理的环境中。它包括开放式源代码 ZENworks 管理代理、后端守护程序和用户空间软件管理工具。Novell ZENworks 包管理工具使用 ZENworks Linux Management 服务器下载包和更新。如果本地网络上无可用的 ZENworks Linux Management 服务器，系统可以从 Novell Customer Center 获取更新，如第 3.14.4 节“Novell Customer Center 配置” [37]中所述。

Novell ZENworks Linux Management 代理的后端守护程序为 ZENworks Management 守护程序 (ZMD)。ZMD 执行软件管理功能。守护程序在引导期间自动启动。

使用 `rczmd status` 检查守护程序的状态。要启动守护程序，请输入 `rczmd start`。要重新启动它，请使用 `rczmd restart`。要停用它，请使用 `rczmd stop`。

ZMD 还可以通过特殊的选项启动以控制其行为。要始终通过某些特殊选项启动 ZMD，请在 `/etc/sysconfig/zmd` 中设置 `ZMD_OPTIONS`，然后运行 `SuSEconfig`。可用选项如下：

- `-n, --no-daemon`  
不在后台运行守护程序。
- `-m, --no-modules`  
不装载任何模块。
- `-s, --no-services`  
不装载初始服务。

`-i, --no-remote`  
不启动远程服务。

ZMD 配置储存在 `/etc/zmd/zmd.conf` 中。您可以手动或使用 `rug` 更改配置。`zmd` 在初始启动时使用的 ZENworks 服务的 URL 和注册密钥储存在 `/var/lib/zmd` 中。将更新下载到 `/var/cache/zmd` 中的 ZMD 缓存。

ZMD 仅为后端。软件管理任务是通过命令行工具 `rug` 或图形化 Software Updater 小程序启动的。

## 9.1 从命令行使用 `rug` 更新包

`rug` 使用 `zmd` 守护程序根据提供的命令来安装、更新和删除软件。它可以从本地文件或服务器安装软件。您可以使用已知为服务的一个或多个远程服务器。对于本地文件，支持的服务是 `mount`，对于服务器，支持的服务是 `yum` 或 ZENworks。

`rug` 将软件从服务器排序为编目（也称为通道），这些编目对应相似软件的组。例如，一个编目可包含来自更新服务器的软件以及来自第三方软件供应商的软件。可以订阅各个编目以控制可用包的显示并防止意外安装不需要的软件。通常只对您所订阅的编目中的软件执行操作。

### 9.1.1 从 `rug` 获取信息

`rug` 可以提供大量有用的信息。它使您可以检查 `zmd` 的状态、查看注册的服务和编目或查看关于可用增补程序的信息。

如果一段时间内不使用 `zmd`，可将其切换为休眠方式。要检查 `zmd` 状态并重新激活该守护程序，请使用 `rug ping`。此命令将唤醒 `zmd` 并记录其状态信息。

要查看已注册的服务，请使用 `rug sl`，要查看您的系统支持哪些服务，请使用 `rug st`。

要查找新的增补程序，请使用 `rug pch`。要获取关于增补程序的信息，请输入 `rug patch-info patch`。

## 9.1.2 订购 rug 服务

默认情况下，新安装的系统订购了几项服务。要添加新服务，请使用 `rugsa URI service_name`。将 `service_name` 替换为能标识新服务的有意义并且唯一的字符串。

---

**注意：访问更新编目时出错**

如果您不能访问更新编目，可能是由于订购已过期。通常，SUSE Linux Enterprise 附带一年或三年订购期，在此期间，您可访问更新编目。订购结束后，将拒绝您访问更新编目。

如果对更新编目的访问遭到拒绝，您将看到一条警告消息，建议您访问 Novell Customer Center 并检查您的订购。可从 <http://www.novell.com/center/> 访问 Novell Customer Center。

---

## 9.1.3 用 rug 安装和删除软件

要从任何已订购的编目安装包，请使用 `rugin package_name`。要仅从选定编目进行安装，请使用 `-c catalog name`。用 `rug if package_name` 获取关于包的更多信息。

要删除包，请使用 `rugrm package_name`。如果其他包依赖该包，`rug` 将显示它们的名称、版本和类型。确认您确实要删除该包。

## 9.1.4 管理 rug 用户

`rug` 的主要优点之一是其用户管理。通常，只有 `root` 能更新或安装新包。使用 `rug`，您可以把更新系统的权限指派给其他用户，并对其进行限制（例如，只能更新不能删除软件）。您可分发的特权包括：

安装

用户可安装新软件

锁定

用户可给包上锁

删除

用户可删除软件

订阅

用户可修改通道订阅

可信

用户被视为可信，因此他可以安装包而不需要包签名

升级

用户可以更新软件包

查看

此项允许用户查看已安装的软件和通道内可用的软件。此选项只用于远程用户，通常允许本地用户查看已安装和可用包。

超级用户

允许除用户管理和设置（只能在本地执行）以外的其他所有 **rug** 命令。

要授予某用户更新系统的权限，请使用命令 `rug ua username upgrade`。使用用户名替换 *username*。要取消某用户特权，请使用命令 `rug ud username`。要列出注明权限的用户列表，请使用 `rug ul`。

要更改用户的当前特权，请使用 `rug ue username`，并用所需用户名替换 *username*。将获得选定用户的权限的列表。`edit` 命令是交互式的。使用加号 (+) 或减号 (-) 来添加或删除用户特权，然后按 **Enter** 键。例如，授予用户删除软件的权利，输入 + 删除。保存并且退出，在空白提示符处按 **Enter** 键。

## 9.1.5 安排更新

使用 `rug`，可以自动更新系统（例如，通过脚本）。最简单的示例就是全自动更新。要完成此操作，请作为 `root` 配置执行 `rug up -y` 的 `cron` 作业。`up -y` 选项从编目下载并安装增补程序而不要求确认。

但是，您可能不想自动安装增补程序，而是想在以后检索并选择要安装的增补程序。如果只想下载增补程序，请使用命令 `rug up -dy`。`up -dy` 选项从您的编目下载增补程序而不要求确认，并将它们保存到 `rug` 缓存中。`rug` 缓存的默认位置是 `/var/cache/zmd`。

## 9.1.6 配置 rug

rug 使您可以通过一组自选设置自定义其设置。有些自选设置是在安装期间预配置的。使用命令 `rug get` 可获取可用自选设置的列表。要编辑自选设置，请输入 `rug set preference`。例如，如果需要通过代理更新系统，则调整设置。在下载更新之前，向代理服务器发送用户名和密码。要完成此操作，请使用以下命令：

```
rug set proxy-url url_path
rug set proxy-username name
rug set proxy-password password
```

使用您的代理服务器的名称替换 `url_path`。使用您的用户名替换 `name`。使用您的密码替换 `password`。

## 9.1.7 更多信息

要从命令行获取有关更新的更多信息，请输入 `rug --help` 或查看 `rug(1)` 手册页。`--help` 选项也适用于所有 `rug` 命令。例如，如果需要关于 `rug update` 的帮助，请输入 `rug update --help`。

# 9.2 用 ZEN 工具管理包

ZEN 工具可用作 ZENworks 管理守护程序 (zmd) 的图形前端，只需单击几次鼠标即可用它方便地安装或卸装软件，应用安全更新，以及管理服务和编目。

## 9.2.1 获取许可权限

管理 Linux 系统上的包需要 `root` 特权。ZEN 工具和 rug 有自己的用户管理系统，可让用户安装软件更新。用户第一次在 ZEN 工具中调用需要特殊特权的操作时，将显示 `root` 密码提示。校验密码后，ZEN 工具自动用更新许可权限将用户帐户添加到用户管理系统。要查看或更改这些设置，请使用 `rug` 用户管理命令（有关信息请参见第 9.1.4 节“管理 rug 用户”[181]）。

## 9.2.2 获取和安装软件更新

Software Updater 位于面板的通知区域 (GNOME) 中或系统任务栏 (KDE) 中，表示为球形图标。它会根据网络链接和新更新的可用性改变颜色和外观。Software Updater 会每天自动检查一次是否有系统更新可用（右键单击应用程序图标并选择 *刷新* 可强制立即检查）。有新的更新可用时，面板中的 Software Updater 小程序会从地球状变为橘黄色背景上的叹号。

---

### 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 附带一年或三年订购期，在此期间，您可访问更新编目。订购结束后，将拒绝您访问更新编目。

如果对更新编目的访问遭到拒绝，您将看到一条警告消息，建议您访问 Novell Customer Center 并检查您的订购。可在 <http://www.novell.com/center/> 访问 Novell Customer Center。

---

左键单击面板图标可打开更新程序窗口。它会显示可用的增补程序和新包版本列表。每一项都有简短说明，如果适用还有一个类别图标：安全增补程序标有一个黄色盾牌。可选增补程序标有淡蓝色圆圈。推荐的增补程序未标有图标。安全增补程序列在首位、然后依次是推荐的增补程序、可选增补程序以及新包版本。可使用 *所有*、*包* 和 *增补程序* 链接来过滤显示的包列表。

---

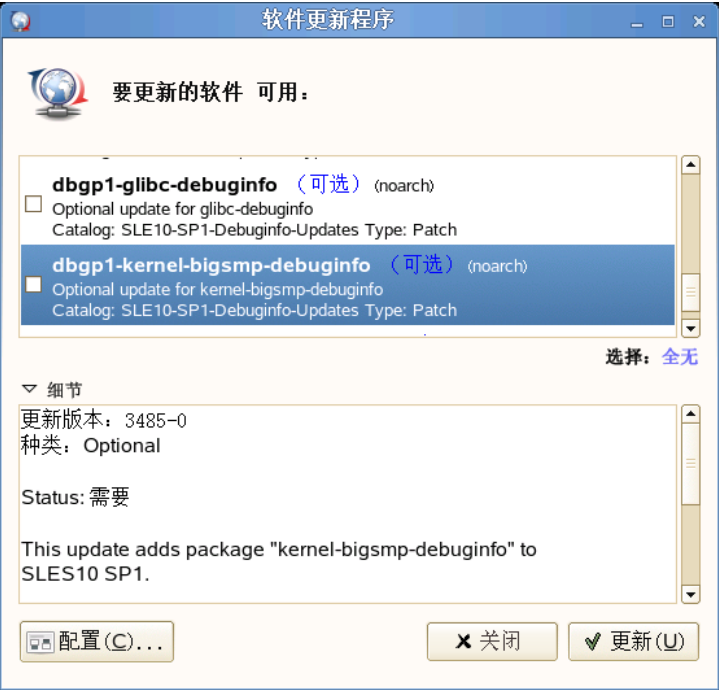
### 注意：包和增补程序比较

Novell 官方发布的更新显示为 *增补程序*。来自其他源的新包版本显示为 *包*。

---

要了解某一项的细节，请用鼠标标记它，并单击列表窗口下的 *细节* 链接。要选择安装某项，请选中该项的复选框。使用 *所有* 和 *无* 链接，可选择或取消选择所有增补程序。单击 *更新* 可安装所选程序。

图 9.1 选择软件更新



### 9.2.3 安装软件

要安装软件包，请从菜单启动安装软件，或运行 zen-installer。该界面几乎和 Software Updater 一样（请参见第 9.2.2 节“获取和安装软件更新”[184]）。唯一区别是用于搜索包或过滤列表的搜索面板。选中要安装的包的复选框，然后按安装启动包的安装。安装程序会自动解析可能存在的对其他包的依赖性。

### 9.2.4 删除软件

从菜单启动删除软件，或运行 zen-remover 卸装软件包。可使用产品（卸装整个产品）、模式（模式细节请参见“安装和删除模式”一节 [121]）、包和增补程序链接来缩小包的范围。选中要删除的列表项的复选框，然后按删除启动包的卸装。如果其他包依赖您标记的包，它们也会被删除。您必须确认其他包的删除。如果您在确认对话框中单击取消，则不会卸装包。

## 9.2.5 配置 Software Updater

要配置 ZEN 工具，请在“软件更新程序”窗口中单击**配置**。将打开有三个选项卡的窗口：*服务*、*编目*和*自选设置*。

### 服务和编目

服务主要是提供软件包及其相关信息的来源。每个服务可提供一个或多个编目。

“服务”选项卡将列出所有可用服务，以及类型和状态信息（如果看不到后两者，请调整窗口大小）。使用*删除服务*或*添加服务*可添加或删除服务。有以下服务类型可用：

#### YUM

对包数据使用 RPM-MD 格式的 HTTP、HTTPS 或 FTP 服务器。

#### ZYPP

ZYPP 服务是使用 YaST 中的**软件 > 安装源**添加的 YaST 安装源。用 Software Updater 或 YaST 添加安装源。最初安装的源（多数情况下是 DVD 或 CD-ROM）是预配置好的。如果更改或删除该来源，则要替换为其他有效安装源（ZYPP 服务），否则就无法安装新软件。

---

#### 注意：术语

术语 YaST 安装源、YaST 包储存库和 ZYPP 服务是可从中安装软件的源的同一名称。

---

#### 装入

使用 *Mount* 可嵌入在计算机上装入的目录。这在有些场合很有用，比如处于定期要镜像 Novell YUM 服务器并将其内容导出至本地网络的网络中时。要添加目录，请在*服务 URI* 中提供该目录的完整路径。

#### NU

NU 代表 Novell Update。Novell 专门以 NU 服务的形式为 SUSE Linux Enterprise 提供更新。如果在安装时已配置更新，则该列表中已存在官方 Novell NU 服务器。



如果安装时跳过了更新配置，请在命令行或 YaST 模块软件 > 产品注册中以 root 用户运行 `suse_register`。Novell Update 服务会自动添加到 Software Updater。

## RCE 和 ZENworks

只有您的公司或组织在内部网络中设置了 Opencarpet、Red Carpet Enterprise 或 ZENworks 服务时，它们才可用。例如，如果您的组织使用的是第三方软件，其更新是部署在单个服务器上的，则可能是这种情况。

安装 SUSE Linux Enterprise 之后，将预配置两个服务：安装源（DVD、CD-ROM 或网络资源）作为 ZYPP 服务，以及 SUSE Linux Enterprise 更新服务器作为 NU 服务（在产品注册时添加）。通常无需更改这些设置。如果未看到 NUYUM 服务，请打开 root 壳层并执行命令 `suse_register`。服务会自动添加。

## 编目

服务能为软件不同部分或不同软件版本提供包（通常由 RCE 或 ZENworks 服务执行）。将这些包归入称为**编目**的不同类别中。通过选中或取消选中编目前面的复选框，可订购或取消订购编目。

目前，SUSE Linux 服务（YUM 和 ZYPP）不提供多个编目。每个服务都只有一个编目。如果 Software Updater 是在安装时配置的或者用 `suse_register` 配置的，它将自动订购 YUM 和 ZYPP 编目。如果手动添加服务，则必须订购其编目。

## 自选设置

在自选设置选项卡上指定 Software Updater 是否应在启动时起动。作为 root 用户，您还可以修改 Software Updater 设置。作为非特权用户，您只能查看设置。有关这些设置的说明，请参见 `rug` 手册页。

## 9.3 更多信息

查找有关 ZENworks Linux Management 和 ZMD 的更多信息，请访问 <http://www.novell.com/products/zenworks/linuxmanagement/index.html>。



# 更新 SUSE Linux Enterprise

SUSE® Linux Enterprise 使您可以将现有系统更新为新版本而不用完全重安装系统。不需新安装。用户主目录和系统配置等旧数据保持不变。在产品使用周期内，您可以使用“服务包”提高系统安全性和更正软件缺陷。从本地 CD 或 DVD 驱动器安装或从中央网络安装源安装。

## 10.1 更新 SUSE Linux Enterprise

例如，如果您要从 SUSE Linux Enterprise Server 9 更新到 SUSE Linux Enterprise Server 10，请遵循本节描述的步骤。如果您从 SUSE Linux Enterprise 10 SP1 更新到 SUSE Linux Enterprise 10 SP2，也可以遵循这些步骤。

从旧版本到新版本，软件的大小具有“增长”的趋势。因此，在进行更新之前，请使用 `df` 查看可用分区空间。如果您怀疑磁盘空间不足，请在进行更新和重分区系统前保护好您的数据。对于每个分区应该具有多少空间，没有一般的经验可以借鉴。空间要求取决于特定的分区配置文件和选定的软件。

### 10.1.1 准备工作

在进行更新之前，将旧的配置文件复制在单独的媒体上（例如磁带设备、可卸硬盘、USB 记忆棒或 ZIP 驱动器）以保护数据。这主要适用于储存在 `/etc` 中的文件以及 `/var` 和 `/opt` 中的一些目录和文件。最好将 `/home`（HOME 目录）中的用户数据也写入备份媒体。以 `root` 用户的身份备份此数据。只有 `root` 用户具有读取所有本地文件的权限。

在开始更新之前，记录必要的 **root** 分区信息。命令 `df /` 可以列出根分区的设备名。在例 10.1 “使用 `df -h` 列示信息” [190] 中，要记录的根分区是 `/dev/hda3`（作为 `/` 装入）。

### 例 10.1 使用 `df -h` 列示信息

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/hda3	74G	22G	53G	29%	/
tmpfs	506M	0	506M	0%	/dev/shm
/dev/hda5	116G	5.8G	111G	5%	/home
/dev/hda1	44G	4G	40G	9%	/data

## 10.1.2 可能的问题

如果将默认系统从上一版本更新到这一版本，则 **YaST** 将分析出所需更改并执行更改。根据您的自定义，一些更新步骤或整个更新过程都可能失败，此时必须将备份数据复制回来。开始系统更新之前检查以下问题。

### 检查 `/etc` 中的 `passwd` 和 `group`

在更新系统之前，确保 `/etc/passwd` 和 `/etc/group` 不包含任何语法错误。为此，以 **root** 用户身份启动校验实用程序 `pwck` 和 `grpck` 并消除任何报告的错误。

## PostgreSQL

在更新 PostgreSQL (`postgres`) 之前，先转储数据库。请参见 `pg_dump` 的手册页。只有当实际上是在更新之前使用了 PostgreSQL 时才需要执行此操作。

## 10.1.3 使用 YaST 进行更新

完成了第 10.1.1 节 “准备工作” [189] 中介绍的准备过程后可以开始更新系统了：

- 1 （可选）准备安装服务器。有关背景信息，请参见第 4.2.1 节 “使用 YaST 设置安装服务器” [51]。

- 2 像进行安装时那样引导系统，如 [第 3.3 节“系统启动以进行安装”](#) [18] 中所述。在 YaST 中，请选择语言并在安装方式对话框中选择更新。不要选择全新安装。
- 3 YaST 确定是否有多个 root 分区。如果只有一个根分区，则继续下一步。如果有多个根分区，则选择正确的分区并单击下一步（的示例中选中了 /dev/hda3 [第 10.1.1 节“准备工作”](#) [189]）进行确认。YaST 在此分区中读取旧的 `fstab` 进行分析，并装入此处列出的文件系统。
- 4 在安装设置对话框中，请根据需要调整设置。通常情况下，可保留默认设置不动，但如果要增强系统，则选中 *软件选择* 子菜单中提供的包或添加其他语言支持。
  - 4a 单击 *更新选项* 只更新已经安装的软件（*只更新已安装的包*）或根据选定的模式对系统添加新软件和功能。建议接受该建议。稍后可以用 YaST 进行调整。
  - 4b 您也可以备份各种系统组件 (*Backup*)。选择备份将减慢更新进程的速度。如果没有最近的系统备份，则使用此选项。
- 5 单击 *接受并确认开始更新* 以开始软件安装过程。

在安装结束时请阅读发行声明，然后单击 *完成* 以重新启动计算机并登录。

## 10.2 安装服务包

用服务包更新一个 SUSE Linux Enterprise 安装。有几种不同方法可以应用服务包。即可更新现有的安装，也可用服务包媒体开始全新安装。这里介绍可能的系统更新和设置中央网络安装源的情形。

---

### 提示：安装更改

阅读服务包媒体里的安装指导以进一步了解更改。

---

## 10.2.1 为服务包媒体设置网络安装源

初次安装 SUSE Linux Enterprise，在网络上有一个为所有客户服务的中央安装源要比用一套物理媒体分别对他们进行安装要高效的多。

### 在 SUSE Linux Enterprise 上使用 YaST 设置一个网络安装源

基本上，按照第4.2节“设置存放安装源的服务器”[51]里列出的过程操作即可。只需要添加另外一个安装源 `SLE-10-SP-x-arch`、`SLES-10-SP-x-arch` 或 `SLED-10-SP-x-arch`（`x` 是服务包的编号，`arch` 是您硬件体系结构的名称），并且让这个服务包能够被 NFS、HTTP 或 FTP 使用。

## 10.2.2 安装服务包

---

### 注意

要将现有 SUSE Linux Enterprise 10 系统更新为 SUSE Linux Enterprise 10 服务包 (SP)，请参见第 10.2.3 节“更新到服务包”[194]。

---

安装 SUSE Linux Enterprise 服务包与安装原始 SUSE Linux Enterprise 媒体的方法很类似。在原始安装中，可选择从本地 CD 或 DVD 驱动器安装或从中央网络安装源安装。

### 从本地 CD 或 DVD 驱动器安装

在启动 SUSE Linux Enterprise SP 的新安装之前，请确保所有的服务包安装媒体（CD 或 DVD）都可用。

#### 过程 10.1 从服务包媒体引导

- 1 插入第一张 SUSE Linux Enterprise SP 媒体（CD 1 或 DVD 1）后引导计算机。一个类似于 SUSE Linux Enterprise 10 原始安装的引导屏幕就会出现。
- 2 选择安装并按照第 3 章 *使用 YaST 进行安装* [17] 中的 YaST 安装说明所述继续。

# 网络安装

在启动 SUSE Linux Enterprise SP 网络安装前，确认满足以下要求：

- 根据第 10.2.1 节 “为服务包媒体设置网络安装源” [192] 建立的网络安装源。
- 连接安装服务器和目标计算机的有效网络连接，目标计算机要包含一个名称服务、DHCP（可选，但对于 PXE 引导是必需的）和 OpenSLP（可选）。
- 引导目标系统的 SUSE Linux Enterprise SP CD 1 或 DVD 1 或根据第 4.3.5 节 “准备目标系统的 PXE 引导” [67] 为 pxe 引导安装的目标系统。

## 网络安装 — 从 CD 或 DVD 引导

要用 SP CD 或 DVD 作为引导媒体执行网络安装，请执行如下操作：

- 1 插入 SUSE Linux Enterprise SP CD 1 或 DVD 1 后引导计算机。一个类似于 SUSE Linux Enterprise 10 原始安装的引导屏幕就会出现。
- 2 单击安装引导 SP 内核，然后使用 F3 选择网络安装源的类型（FTP、HTTP、NFS 或 SMB）。
- 3 提供相应的路径信息或选择 *SLP* 作为安装源。
- 4 从所提供的服务器里选择相应的安装服务器，或用引导选项提示提供安装源类型和实际地址（如第 3.3.4 节 “从没有 SLP 的网络源安装” [19] 中所示）。YaST 启动。

按第 3 章 使用 *YaST* 进行安装 [17] 中所述完成安装。

## 网络安装 — PXE 引导

要通过网络执行 SUSE Linux Enterprise 服务包网络安装，请执行以下操作：

- 1 按照第 4.3.5 节 “准备目标系统的 PXE 引导” [67] 调整您的 DHCP 服务器设置以提供 PXE 引导需要的地址信息。
- 2 设置 TFTP 服务器来储存 PXE 引导需要的引导映像。

用 SUSE Linux Enterprise 服务包的第一张 CD 或 DVD 执行此操作，或按照第 4.3.2 节 “设置 TFTP 服务器” [61] 的说明进行。

- 3 在目标计算机上准备 PXE 引导和局域网唤醒。
- 4 对目标系统引导进行初始化，并用 VNC 远程连接到此计算机正运行的安装例程上。有关更多信息，请参见第 4.5.1 节“VNC 安装”[74]。
- 5 接受许可证协议，然后选择语言、默认桌面以及其他安装设置。
- 6 单击是，安装开始安装。
- 7 照常继续安装（输入 root 的密码，完成网络设置，检测网络连接，激活联机更新服务，选择用户身份验证方法并输入用户名和密码）。

有关安装 SUSE Linux Enterprise 的详细说明，请参见第 3 章 *使用 YaST 进行安装* [17]。

## 10.2.3 更新到服务包

将系统更新到服务包 (SP) 功能级别有两种首选方法。一种方法是从 SP 媒体引导。另一种方法是运行“YaST 联机更新”或 zen-updater，然后选择更新到服务包 X 增补程序。通过更新到新的功能级别，可为系统提供新驱动程序或软件增强等附加功能。

---

### 警告：请勿忽略更新到服务包增补程序

如果没有选择更新到服务包增补程序，系统将保持先前的功能级别，且您将只在有限的时间内（对于 SUSE Linux Enterprise 10 SP2，该期限现在延长到 6 个月）获得错误修复和安全更新。因此，为了获得持续系统完整性，建议尽早切换到新功能级别。

---

其他更新方法有手动运行 rug 命令、使用增补程序 CD（请参见第 8.3.7 节“从增补程序 CD 更新”[130]），或使用本地安装的 SMT 系统。

---

### 注意

在 s390 系统上，增补程序 CD 更新选项不可用。

---



# 从 SP 媒体引导以进行更新

从 SP 媒体引导并选择更新作为 YaST 中的安装方式。关于详细信息和如何完成更新，请参见第 10.1.3 节 “使用 YaST 进行更新” [190]。

## 用 YaST 联机更新启动

在启动 YaST 联机更新以更新到 SP 功能级别之前，请确保符合以下要求：

- 整个更新过程中系统必须联机，因为此过程需要访问 Novell Customer Center。
- 如果安装涉及第三方软件或附加软件，请在另一台计算机上测试此过程，以确保更新不会破坏相关性。
- 确保整个过程成功完成。否则系统将不一致。

先完全安装服务包 1 之后，才能更新到服务包 2。如果尚未安装服务包 1，请先如“SUSE Linux Enterprise GA 到 SP1 和 SP2”一节 [200]中所述更新到服务包 1。

图 10.1 服务包 1 包管理更新

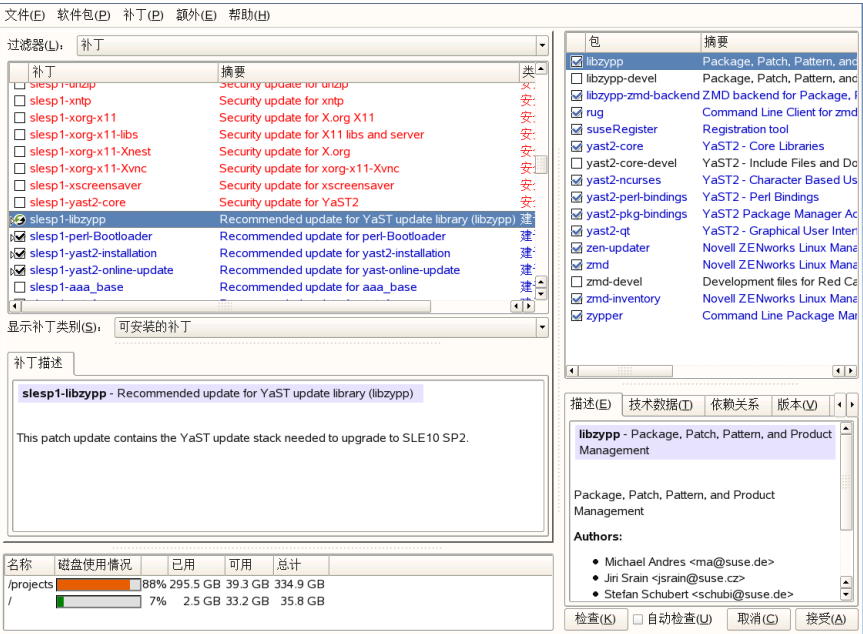
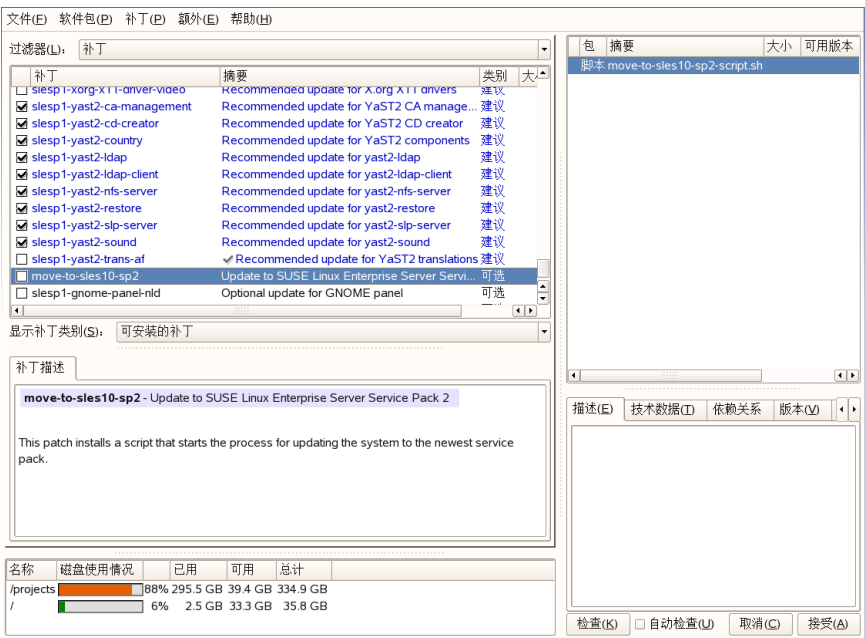


图 10.2 更新到服务包 2



注意

在使用“YaST 联机更新”的更新迁移期间，ZMD 堆栈被更新且 ZMD 守护程序也会重新启动。因此，建议避免使用任何其他软件管理工具，例如 rug、zen-updater、zen-installer 和 zen-remover。建议在迁移期间退出 zen-updater。

- 1 在运行的 SUSE Linux Enterprise 系统中，选择计算机 > YaST > 软件 > 联机更新。

如果不是以 root 用户登录，系统提示时输入 root 密码。

- 2 则显示联机更新对话框。会预先选择几个增补程序。向下滚动增补程序列表，校验确实已预先选择了与管理相关的增补程序和 SUSE Linux Enterprise 10 SP2 维护堆栈更新 (slesplu-libzypp)。然后按接受以应用选定更新。

- 3 增补程序下载和安装对话框将跟踪进度日志。当总进度达到 100% 时，请单击关闭。然后联机更新将自动重新启动。
- 4 重新启动后，按接受以应用所有可用更新和一个新内核。安装后，必须重引导系统。
- 5 在重新启动的联机更新中，现在应向下滚动增补程序列表并选择更新到服务包 2(move-to-sles10-sp2)，如图 10.2 “更新到服务包 2” [196] 中所示。在弹出窗口中，单击接受确认已开始更新到服务包功能级别的过程。

move-to-sles10-sp2 增补程序标记为 optional。如果没有选择它，您的系统将停留在 SP1 功能级别，且您将只在有限的时间里（SP2 可用后 6 个月）可以获得错误修复和安全更新。
- 6 增补程序下载和安装对话框跟踪迁移增补程序安装的进展日志。当总进展达到 100% 时，请单击完成。
- 7 再次启动 YaST 联机更新。应用 product-sles10-sp2 和 slesp2o-sp2\_online 增补程序，将系统更新到 SP2 级别。如果在之前步骤中已安装 move-to-sles10-sp2，会预先选择这些增补程序（因为它们必需的）。
- 8 单击关闭以完成到 SUSE Linux Enterprise 10 SP2 的更新，然后重引导。

## 使用 zen-updater 启动

有关 ZENworks 的背景信息，请参见第 9 章 [通过 ZENworks 管理软件](#) [179]。

请先确保满足“[用 YaST 联机更新启动](#)”一节 [195] 中列出的要求，再使用 zen-updater 启动联机更新以更新到 SP 功能级别。

图 10.3 应用 SLE10 SP2 维护堆栈更新



- 1 在正在运行的 SUSE Linux Enterprise 系统中，通过单击底部的更新程序图标启动 zen-updater。

---

#### 提示：唤醒 ZMD

如果看到 **ZMD** 未在运行消息，请以 root 身份通过 `rczmd status` 检查 **ZMD** 是否处于活动状态。如果出现问题，请输入 `rug restart --clean` 以强制重新启动并清理 **ZMD** 及其数据库。

---

如果不是以 root 用户登录，系统提示时输入 root 密码。

- 2 应用系统所有可用的维护更新。

- 3 应用 SLE10 SP2 维护堆栈更新 (slesplu-libzypp)。应预先选择这些项目，单击 **更新** 可启动此步骤。解析所有依赖性后，单击 **应用**。完成时，通过单击 **关闭** 确认消息弹出框。
- 4 在重新启动的软件更新程序中，浏览并选择可选的 move-to-sles10-sp2 增补程序并应用它。如果没有选择它，您的系统将停留在 SP1 功能级别，且您将只在有限的时间里（SP2 可用后 6 个月）可以获得错误修复和安全更新。
- 5 在软件更新程序中应用 product-sles10-sp2 和 slesp2o-sp2\_online 增补程序，将系统更新到 SP2 级别。两个增补程序都是强制的，如果在之前的步骤中已安装 move-to-sles10-sp2，则它们会被预先选择。
- 6 单击 **关闭** 以完成到 SUSE Linux Enterprise 10 SP2 的更新，然后重引导。

## 使用 rug

有关 rug 命令行工具的背景信息，请参见第 9.1 节“从命令行使用 rug 更新包”[180]。如果需要编写脚本的解决方法来进行更新，请使用 rug。

请先确保满足“用 YaST 联机更新启动”一节 [195] 中列出的要求，再使用 rug 启动联机更新以更新到 SP 功能级别。

下面是将系统迁移到 SP2 增补程序级别所需的最小命令序列：

```
rug in -t patch slesplu-libzypp && rug ping -a
rug in -t patch move-to-sles10-sp2 && rug ping -a
rug refresh && rug ping -a
rug up -t patch -g recommended && rug ping -a
reboot
```

---

### 注意

rug ping -a 确保在先前的 rug 命令后已完成 ZMD 初始化。

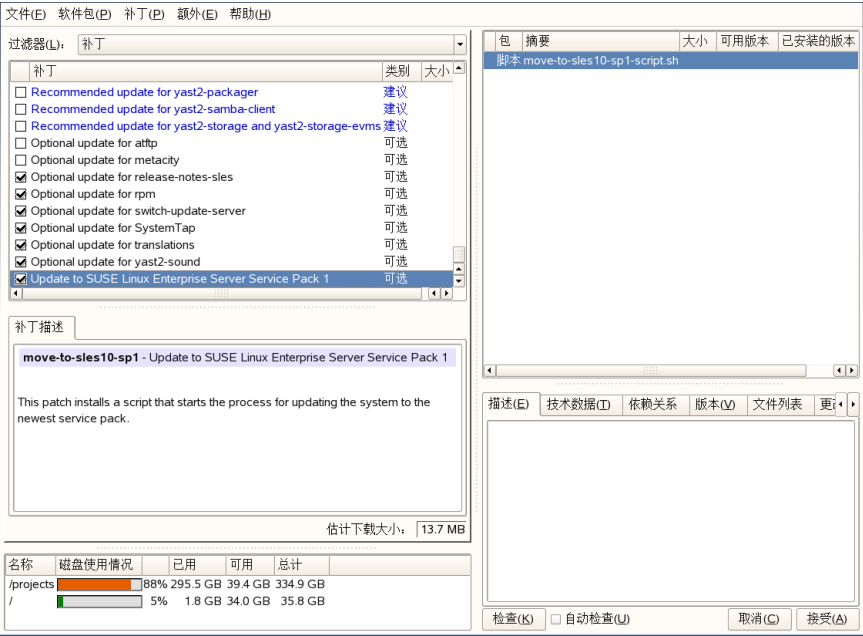
---

# SUSE Linux Enterprise GA 到 SP1 和 SP2

## 注意

仅当您的系统仍然在 GA 增补程序级别运行时，以下步骤才适用。

图 10.4 更新到 Service Pack 1



- 1 在运行的 SUSE Linux Enterprise 系统 (GA) 中，选择 **计算机 > YaST > 软件 > 联机更新**。
- 2 则显示联机更新对话框。如图 10.4 “更新到 Service Pack 1” [200] 中所示，下滚增补程序列表并选择 **更新到服务包 1**。在弹出窗口中，单击接受确认已开始更新到服务包功能级别的过程。
- 3 增补程序下载和安装对话框跟踪迁移增补程序安装的进展日志。当总进展达到 100% 时，请单击完成。

- 4 再次运行联机更新。一旦完成，在增补程序下载和安装中单击关闭。在第二次运行期间，YaST 将安装内核和所有其他软件。
- 5 在过程日志末尾看到 *Installation Finished* 报告时，单击完成。
- 6 要完成更新，请手动重引导系统以激活新内核。

现在，SUSE Linux Enterprise 已在 SP1 增补程序级别运行了。继续“[用 YaST 联机更新启动](#)”一节 [195] 以将系统升级为 SP2 增补程序级别。

## 10.3 从 V9 到 V10 的软件更改

以下内容详细介绍了 V9 到 V10 各方面进行的更改。本摘要指出了是否已完全重配置基本设置、是否已将配置文件移动到其他位置以及是否对常用应用程序进行了重大更改。此处将介绍用户级别或管理员级别的重大修改，它将影响系统的日常使用。

---

**注意：从 SLES 10 到 SLES 10 SP 1 的软件更改**

要查看从 SUSE Linux Enterprise Server 10 到 SUSE Linux Enterprise Server 10 SP1 的软件和配置更改的详细列表，请参见服务包的发行说明。在已安装的系统用 YaST 发行说明模块查看它们。

---

### 10.3.1 多个内核

可以同时安装多个内核。此功能旨在支持管理员从一个内核升级到另一个内核，方法是安装新内核，确认新内核能按预期运行后，卸载旧内核。尽管 YaST 尚不支持此功能，仍可以使用 `rpm -i package.rpm` 通过 shell 轻松地安装和卸载内核。

默认的引导加载程序菜单中包含一个内核项。在安装多个内核前，为这些加装的内核添加一个对应项很有用，这样便于选择这些内核。在安装新内核前处于活动状态的内核可以作为 `vmlinuz.previous` 和 `initrd.previous` 进行访问。通过创建类似于默认项的引导加载程序项，并令此项指向 `vmlinuz.previous` 和 `initrd.previous` 而不是 `vmlinuz` 和 `initrd`，可以访问先前活动的内核。另外，GRUB 和 LILO 支持带通配符的引导加载程序项。有关详细信息，请参考 GRUB 信息页 (`info grub`) 和 `lilo.conf` (5) 手册页。

## 10.3.2 内核模块的更改

以下内核模块已不再可用：

- `km_fcdsl` — `avm FRITZ!Card Dsl`
- `km_fritzcap` — `avm FRITZ! ISDN 适配器`

对以下内核模块包的内部进行了更改：

- `km_wlan` — 用于无线 `lan` 卡的各种驱动程序。从 `km_wlan` 删除了 `Atheros WLAN` 卡的 `madwifi` 驱动程序。

由于技术原因，必须除去对 `Ralink WLAN` 卡的支持。分发中未包含以下模块并且以后也不会添加这些模块：

- `ati-fglrx` — `ati FIREGL` 显卡
- `nvidia-gfx` — `nvidia GFX` 驱动程序
- `km_smartlink-softmodem` — `smart Link` 软调制解调器

## 10.3.3 控制台编号更改和串行设备

直至 2.6.10，`ia64` 上的串行设备是根据 `ACPI` 和 `PCI` 枚举顺序来命名的。`ACPI` 名称空间中的第一个设备（如有）成为 `/dev/ttyS0`，第二个设备成为 `/dev/ttyS1` 并以此类推，而 `PCI` 设备的命名在 `ACPI` 设备之后开始。

在 `HP` 系统上，必须重配置 `EFI` 控制台，然后您才能够从内核引导命令中除去控制台参数。作为变通方法，可尝试使用 `console=ttyS1...` 作为引导参数，而非 `console=ttyS0...`。

可在 `/usr/src/linux/Documentation/ia64/serial.txt` 中找到详细信息，该文件是 `kernel-source` 软件包的一部分。



# 10.3.4 LD\_ASSUME\_KERNEL 环境变量

不再设置 LD\_ASSUME\_KERNEL 环境变量。过去可能会使用该环境变量来强制 LinuxThreads 支持（该支持已被除去）。如果在 SUSE Linux Enterprise 10 中设置 LD\_ASSUME\_KERNEL=2.4.x，则一切连接都会中断，因为 ld.so 会在不存在的路径中查找 glibc 和相关工具。

# 10.3.5 tar 语法更为严格

tar 的使用语法现在更加严格。tar 选项必须出现在指定文件或目录之前。追加选项（诸如 --atime-preserve 或 --numeric-owner）在文件或目录指定之后，会使 tar 失败。请检查备份脚本。诸如以下的命令不再有效：

```
tar czf etc.tar.gz /etc --atime-preserve
```

关于更多信息，请参见 tar 信息页。

# 10.3.6 Apache 2 替换为 Apache 2.2

Apache Web 服务器（版本 2）已由版本 2.2 代替。Apache 版本 2.2 中已对第 40 章 *Apache HTTP 服务器* [667]进行了完全改写。此外，在 <http://httpd.apache.org/docs/2.2/upgrading.html> 查找常规升级信息，在 [http://httpd.apache.org/docs/2.2/new\\_features\\_2\\_2.html](http://httpd.apache.org/docs/2.2/new_features_2_2.html) 查找新功能的描述。

# 10.3.7 用于网络身份验证的 Kerberos

Kerberos 已代替 heimdal 成为默认的网络身份验证方法。不能自动转换现有的 heimdal 配置。在系统更新过程中，配置文件的备份副本将按表 10.1 “备份文件” [203]中所示创建。

表 10.1 备份文件

旧文件	备份文件
/etc/krb5.conf	/etc/krb5.conf.heimdal

旧文件	备份文件
/etc/krb5.keytab	/etc/krb5.keytab.heimdal

客户机配置 (/etc/krb5.conf) 与 heimdal 的配置很相似。如果没有任何特殊配置，完全可以将 kpasswd\_server 参数替换为 admin\_server。

不能复制与服务器相关 (kdc 和 kadmind) 的数据。系统更新后，旧的 heimdal 数据库在 /var/heimdal 下仍可用；MIT kerberos 在 /var/lib/kerberos/krb5kdc 下维护其数据库。有关更多信息，请参见第 45 章 *网络身份验证 — Kerberos* [753] 和第 46 章 *安装和管理 Kerberos* [761]。

## 10.3.8 Hotplug 事件由 udev 守护程序处理

Hotplug 事件现在已经完全由 udev 守护程序 (udev) 处理。不再使用 /etc/hotplug.d 和 /etc/dev.d 中的事件多路转换器系统。相反，udev 会根据规则直接调用所有的热插拔帮助程序工具。Udev 和其他包提供 Udev 规则和帮助程序工具。

## 10.3.9 安装期间激活防火墙

为提高安全性，安装结束时在建议对话框中激活附带的防火墙解决方案 SUSEFirewall2。这意味着最初将关闭所有端口，如果需要，可以在建议对话框中将其打开。默认情况下，不能从远程系统登录。此外，还会影响网络浏览和多路广播应用程序，如 SLP、Samba (“网络邻居”) 以及某些游戏程序。您可以使用 YaST 对防火墙设置进行微调。

如果在安装或配置服务过程中需要进行网络访问，则相应的 YaST 模块将为所有内部和外部接口打开所需的 TCP 和 UDP 端口。如果不想这样，则在 YaST 模块中关闭端口或指定其他具体的防火墙设置。

## 10.3.10 KDE 和 IPv6 支持

默认情况下，不能在 KDE 中启用 IPv6 支持。您可以使用 YaST 的 /etc/sysconfig 编辑器启用该支持。禁用此功能的原因在于 IPv6 地址得不到所有

因特网服务提供者的充分支持，从而导致浏览 Web 时出现错误消息，并且显示网页时出现延迟。

## 10.3.11 联机更新和增量包

联机更新现支持一种特殊的 RPM 包，这种包仅储存与给定基础包不同的二进制内容。这项技术显著减少了包的大小并缩短了下载时间。不过，因需要重组最终包，致使 CPU 负载加重。关于技术详细信息，请参见 `/usr/share/doc/packages/deltarpm/README`。

## 10.3.12 打印系统配置

安装结束时（建议对话框），必须在防火墙配置中打开打印系统所需的端口。CUPS 需要端口 631/TCP 和端口 631/UDP，要执行一般操作，不应关闭这两个端口。要通过 LPD 或 SMB 进行打印，还应该打开端口 515/TCP（用于以前的 LPD 协议）和 Samba 使用的端口。

## 10.3.13 更改为 X.Org

兼容性链接简化了从 XFree86 到 X.Org 的更改，这些链接支持访问使用以前名称的重要文件和命令。

表 10.2 命令

XFree86	X.Org
XFree86	Xorg
xf86config	xorgconfig
xf86cfg	xorgcfg

**表 10.3** */var/log* 中的日志文件

XFree86	X.Org
XFree86.0.log	Xorg.0.log
XFree86.0.log.old	Xorg.0.log.old

在更改为 X.Org 的过程中，将包的名称从 XFree86\* 重命名为 xorg-x11\*。

## 10.3.14 X.Org 配置文件

配置工具 SaX2 将 X.Org 配置设置写入 */etc/X11/xorg.conf*。在从头安装过程中，不会创建从 XF86Config 到 *xorg.conf* 的任何兼容性链接。

## 10.3.15 取消了 XView 和 OpenLook 支持

已删除包 *xview*、*xview-devel*、*xview-devel-examples*、*olvwm* 和 *xttoolpl*。以前只提供了 XView (OpenLook) 基础系统。在系统更新后将不再提供 XView 库。更重要的是，OLVWM (OpenLook Virtual Window Manager) 也将不再可用。

## 10.3.16 适用于 X11 的终端模拟器

已删除了多个终端模拟器，原因是不再进行维护或者在默认环境下不能使用，尤其是不支持 UTF-8。SUSE Linux Enterprise Server 提供各种标准终端，如 *xterm*、KDE 终端、GNOME 终端和 *mlterm*（适用于 X 的多语言终端模拟器，有可能代替 *aterm* 和 *eterm*）。

# 10.3.17 OpenOffice.org (OOo)

## 目录

OOo 现在安装在 `/usr/lib/ooo-2.0` 而不是 `/opt/OpenOffice.org` 中。用户设置的默认目录现在是 `~/.ooo-2.0` 而不是 `~/OpenOffice.org1.1`。

## 包装程序

一些新包装程序可用于启动 OOo 部件。新名称显示在 [表 10.4 “包装程序” \[207\]](#) 中。

表 10.4 包装程序

旧名称	新建
<code>/usr/X11R6/bin/OOo-calc</code>	<code>/usr/bin/oocalc</code>
<code>/usr/X11R6/bin/OOo-draw</code>	<code>/usr/bin/oodraw</code>
<code>/usr/X11R6/bin/OOo-impress</code>	<code>/usr/bin/ooimpress</code>
<code>/usr/X11R6/bin/OOo-math</code>	<code>/usr/bin/oomath</code>
<code>/usr/X11R6/bin/OOo-padmin</code>	<code>/usr/sbin/oopadmin</code>
<code>/usr/X11R6/bin/OOo-setup</code>	—
<code>/usr/X11R6/bin/OOo-template</code>	<code>/usr/bin/oofromtemplate</code>
<code>/usr/X11R6/bin/OOo-web</code>	<code>/usr/bin/ooweb</code>
<code>/usr/X11R6/bin/OOo-writer</code>	<code>/usr/bin/oowriter</code>
<code>/usr/X11R6/bin/OOo</code>	<code>/usr/bin/ooffice</code>
<code>/usr/X11R6/bin/OOo-wrapper</code>	<code>/usr/bin/ooo-wrapper</code>

包装程序现在支持使用选项 `--icons-set` 在 KDE 和 GNOME 图标之间进行切换。不再支持以下选项：`--default-configuration`、`--gui`、`--java-path`、`--skip-check`、`--lang`（语言现在由区域设置决定）、`--messages-in-window` 和 `--quiet`。

### KDE 和 GNOME 支持

可以在 `OpenOffice_org-kde` 和 `OpenOffice_org-gnome` 包中获得 KDE 和 GNOME 扩展。

## 10.3.18 混音器 **kmix**

预设混音器 `kmix` 作为默认设置。对于高端硬件，还提供其他混音器，如 `QAMix/KAMix`、`envy24control`（仅限 ICE1712）或 `hdspmixer`（仅限 RME Hammerfall）。

## 10.3.19 DVD 烧录

以往，从 `cdrecord` 包中应用 `cdrecord` 二进制文件的增补程序以支持 DVD 烧录功能。而现在安装的新二进制文件 `cdrecord-dvd` 即提供这个增补程序。

`dvd+rw-tools` 包中的 `growisofs` 程序现在支持烧录所有 DVD 媒体（DVD+R、DVD-R、DVD+RW、DVD-RW、DVD+RL）。尝试用此程序来代替经过修补的 `cdrecord-dvd`。

## 10.3.20 在内核提示符处启动手动安装

手动安装方式已不再出现在引导加载程序屏幕上。不过，您仍可以在引导提示符处使用 `manual=1` 令 `linuxrc` 转换为手动方式。通常不必这样做，因为您可以在内核提示符处直接设置安装选项，例如 `textmode=1` 或将 `URL` 设为安装源。

## 10.3.21 JFS：不再支持

由于 JFS 的技术问题，不再支持 JFS。其中虽仍有内核文件系统驱动程序，但 YaST 不提供具有 JFS 的分区。

## 10.3.22 用 AIDE 替换 Tripwire

作为入侵检测系统，请使用 AIDE（包名称为 `aide`），它是在 GPL 下发布的。SUSE Linux 上不再提供 Tripwire。

## 10.3.23 PAM 配置

*新配置文件（包含更多信息的注释）*

`common-auth`  
auth 部分的默认 PAM 配置

`common-account`  
帐户部分的默认 PAM 配置

`common-password`  
密码更改的默认 PAM 配置

`common-session`  
会话管理的默认 PAM 配置

您应该在特定于应用程序的配置文件中包括这些默认的配置，因为修改和维护一个文件比修改和维护系统中以往有的约 40 个文件要容易些。如果您稍后安装某个应用程序，该程序将继承已应用的更改，而且管理员也不必记着调整该配置。

所做的更改很简单：如果您使用下面的配置文件（应该是多数应用程序的默认配置）：

```
##PAM-1.0
auth      required      pam_unix2.so
account   required      pam_unix2.so
password  required      pam_pwcheck.so
password  required      pam_unix2.so      use_first_pass use_authtok
#password required      pam_make.so      /var/yp
session   required      pam_unix2.so
```

可以将其改为：

```
##PAM-1.0
auth      include      common-auth
account   include      common-account
```

```
password include      common-password
session include       common-session
```

### 10.3.24 使用 su 成为超级用户

默认情况下，调用 su 成为 root 并没有为 root 设置 PATH。如果要更改 su 的默认行为，则调用 su - 使用 root 的完整环境启动登录 shell，或者在 /etc/default/su 中将 ALWAYS\_SET\_PATH 设置为 yes。

### 10.3.25 powersave 包中的更改

/etc/sysconfig/powersave 中的配置文件已更改：

**表 10.5** 拆分 /etc/sysconfig/powersave 中的配置文件

旧名称	现在拆分为
/etc/sysconfig/powersave/ common	common
	cpufreq
	events
	battery
	sleep
	thermal

/etc/powersave.conf 已不再使用。现有变量已移至表 10.5 “拆分 /etc/sysconfig/powersave 中的配置文件” [210]中列出的文件。如果更改 /etc/powersave.conf 中的“event”变量，则必须在 /etc/sysconfig/powersave/events 中进行调整。

休眠状态的名称从：



- 暂停（ACPI S4、APM 暂停）
- 待机（ACPI S3、APM 待机）

收件人：

- 暂停到磁盘（ACPI S4、APM 暂停）
- 暂停到 RAM（ACPI S3、APM 暂停）
- 待机（ACPI S1、APM 待机）

## 10.3.26 Powersave 配置变量

为保持一致性更改 powersave 配置变量的名称，但 sysconfig 文件仍保持不变。有关详细信息，请参见第 28.5.1 节“配置 powersave 包”[470]。

## 10.3.27 PCMCIA

cardmgr 不再管理 PC 卡。而是与 Cardbus 卡和其他子系统相同，由内核模块管理 PC 卡。通过 hotplug 执行所有需要的操作。pcmcia 启动已删除的脚本，并将 cardctl 替换为 pccardctl。有关更多信息，请参见 /usr/share/doc/packages/pcmciautils/README.SUSE。

## 10.3.28 设置 D-BUS 进行 .xinitrc 中的进程间通信

现在许多应用程序都依靠 D-BUS 进行进程间通信 (IPC)。调用 dbus-launch 会启动 dbus-daemon。系统范围内的 /etc/X11/xinit/xinitrc 使用 dbus-launch 来启动窗口管理器。

如果具有本地 ~/.xinitrc 文件，则必须相应地进行更改。否则像 f-spot、banshee、tomboy 这样的应用程序或网络管理器 banshee 可能会失败。保存旧的 ~/.xinitrc。接着使用以下命令将新的模板文件复制到主目录中：

```
cp /etc/skel/.xinitrc.template ~/.xinitrc
```

最后，从已保存的 `.xinitrc` 添加定制的内容。

## 10.3.29 NTP 相关的文件已重命名

因为要与 LSB 兼容（Linux 标准库），大多数配置文件和初始化脚本都从 `xntp` 重命名为 `ntp`。这些新文件名是：

- `/etc/slp.reg.d/ntp.reg`
- `/etc/init.d/ntp`
- `/etc/logrotate.d/ntp`
- `/usr/sbin/rcntp`
- `/etc/sysconfig/ntp`

## 10.3.30 GNOME 应用程序的文件系统更改通知

为了确保正常运行，GNOME 应用程序依赖于文件系统更改通知支持。仅对于本地文件系统，安装 `gamin` 包（推荐）或运行 FAM 守护程序。对于远程文件系统，在服务器和客户机上都运行 FAM 并通过 FAM 打开 RPC 调用的防火墙。

GNOME（`gnome-vfs2` 和 `libgda`）包含一个包装程序，它选择 `gamin` 或 `fam` 来提供文件系统更改通知：

- 如果 FAM 守护程序未运行，最好使用 `gamin`（理由：Inotify 只有 `gamin` 才支持，它对于本地文件系统更为高效）。
- 如果 FAM 守护程序在运行，最好用 FAM（理由：如果 FAM 在运行，可能需要远程通知，只有 FAM 支持该功能）。

## 10.3.31 启动 FTP 服务器 (vsftpd)

默认情况下，`xinetd` 不再启动 `vsftpd` FTP 服务器。它现在是一个独立守护程序，必须使用 YaST 运行时编辑器来配置它。

## 10.3.32 Firefox 1.5: Url Open 命令

使用 Firefox 1.5 时，应用程序打开 Firefox 实例或窗口的方法已经更改。新方法在以前的版本中已说明了一部分，在以前的版本中行为是在包装程序脚本中实施的。

如果应用程序不使用 `mozilla-xremote-client` 或 `firefox -remote`，则不需要更改任何内容。否则，打开 `url` 的新命令是 `firefox url`，并且此时 `firefox` 是否已经运行并不重要。如果已经正在运行，则它遵循从其他应用程序打开链接中配置的自选设置。

从命令行，可以通过使用 `firefox -new-window url` 或 `firefox -new-tab url` 来影响行为。



## 部分 II. 管理



# OpenWBEM

Novell® 已包含分布式管理任务组 (DMTF) [<http://www.dmtf.org/home>] 建议的“基于 Web 的企业管理”(WBEM) 开放式标准战略。实施这些策略可以大大减少在网络中管理不同系统的复杂度。

以下信息说明 DMTF 标准所建议的一些组件。了解这些组件的概念以及它们如何互相关联可帮助您了解 OpenWBEM 的概念以及如何在网络中最有效地使用 OpenWBEM。

- “基于 Web 的企业管理”(WBEM) 是一套管理和因特网标准技术，开发它的目的是统一企业计算环境的管理。WBEM 使本行业能够利用新兴 Web 技术提供良好集成且基于标准的管理工具集。DMTF 已开发了一套核心标准来完善 WBEM：
  - 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 (CIM) 是一种说明管理的概念信息模型，它并不依赖于特定实施。这允许在管理系统和应用程序之间交换管理信息。此信息交换可以是分布系统管理提供的代理到管理器通信或管理器到管理器通信。CIM 有两部分：CIM 规范和 CIM 纲要。

CIM 规范说明语言、命名和元模式。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”。元模式还支持将“指示”和“关联”作为“类”类型，将“参考”作为“属性”类型。

CIM 模式可提供实际模型说明。CIM 模式提供具有属性和关联的类集合，这些类可提供能够被很好理解的概念框架，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 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。

SUSE® Linux Enterprise Server 包含来自 OpenWBEM 项目 [<http://openwbem.org>]的 CIMOM 开放源代码。

“基于 Web 的企业管理”软件选择包括一个包集合，这些包包含基本 Novell 提供者（包括一些示例提供者）以及附带的 Novell 模式基础集合。

随着 OpenWBEM 的推动和特定提供者的开发，Novell 将提供包括以下重要功能的工具：

- 有效监视网络系统
- 记录现有管理配置中的变更
- 硬件详细目录和资产管理

了解如何安装 OpenWBEM CIMOM 和如何配置 OpenWBEM CIMOM 将能够帮助您更自信而又轻松地监视和管理网络中的不同系统。

## 11.1 设置 OpenWBEM

要设置 OpenWBEM，请在安装 SUSE Linux Enterprise Server 时在 YaST 中选择“基于 Web 的企业管理”软件选择或模式，或在已运行 SUSE Linux Enterprise Server 的服务器上选择作为组件安装 OpenWBEM。此软件选择包括以下包：



cim-schema, “通用信息模型”（CIM）模式：

此包包含“通用信息模型”（CIM）。CIM 是说明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。

openwbem, “基于 Web 的企业管理”（WBEM）实施：

此包包含 OpenWBEM 实施。OpenWBEM 是一个软件组件集合，可帮助您更便利地部署“分布式管理任务组”（DMTF）CIM 和 WBEM 技术。如果您不熟悉 DMTF 及其技术，则可访问 DMTF 网站 [<http://www.dmtf.org>]。

openwbem-base-providers:

此包包含基础操作系统组件（如计算机、系统、操作系统和 OpenWBEM CIMOM 的进程）的 Novell Linux 实施。

openwbem-smash-providers:

此包包含 OpenWBEM CIMOM 的“服务器硬件系统管理架构”（SMASH）提供者的 Novell Linux 实施。

yast2-cim, YaST2—CIM 绑定：

此包将 CIM 绑定添加到 YaST2（YaST2 是 SUSE 系统工具管理器的图形用户界面）。这些绑定可为“通用信息模型对象管理器”（CIMOM）提供客户程序接口。

本部分包含下列信息：

- 第 11.1.1 节 “启动、停止 owcimomd 或检查 owcimomd 的状态” [219]
- 第 11.1.2 节 “确保安全访问” [220]
- 第 11.1.3 节 “设置日志记录” [223]

## 11.1.1 启动、停止 owcimomd 或检查 owcimomd 的状态

安装“基于 Web 的企业管理”软件时，默认情况下会启动守护程序 owcimomd。下表说明如何启动、停止 owcimomd 和检查 owcimomd 的状态。

表 11.1 用于管理 *owcimomd* 的命令

任务	Linux 命令
启动 <i>owcimomd</i>	作为 root 用户，在控制台 shell 中输入 <code>rcowcimomd start</code> 。
停止 <i>owcimomd</i>	作为 root 用户，在控制台 shell 中输入 <code>rcowcimomd stop</code> 。
检查 <i>owcimomd</i> 状态	作为 root 用户，在控制台 shell 中输入 <code>rcowcimomd status</code> 。

## 11.1.2 确保安全访问

OpenWBEM 的默认设置相对来说比较安全。但是，您可能会希望查看下面的内容，以确保 OpenWBEM 组件的访问如组织所希望的一样安全。

- “证书”一节 [220]
- “端口”一节 [221]
- “身份验证”一节 [222]

### 证书

安全套接字层（SSL）传输需要安全通信的证书。当安装了 OES 时，OpenWBEM 会为其生成一个自签署证书。

如果需要，可将默认证书的路径替换为到已购买的商业证书的路径或替换为已在 `/etc/openwbem/openwbem.conf` 文件的 `http_server.SSL_cert = path_filename` 设置中生成的其他证书。

默认生成的证书位置如下：

```
/etc/openwbem/servercert.pem
```

如果希望生成新证书，则可使用以下命令。运行此命令将替换当前证书，因此 Novell 建议在生成新证书之前先保存旧证书的副本。

作为 root 用户，在控制台壳层中输入

```
sh/etc/openwbem/owgencert
```

如果希望更改 OpenWBEM 使用的证书，请参见第 11.2.2 节 “更改证书配置” [230]。

## 端口

默认情况下，OpenWBEM 被配置为接受安全端口 5989 的所有通信。下表说明端口通信设置和建议配置。

表 11.2 端口通信设置和建议配置

端口	类型	说明和建议
5989	安全	<p>OpenWBEM 通信通过 HTTPS 服务使用的安全端口。</p> <p>这是默认的配置。</p> <p>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。用户必须通过客户程序应用程序进行身份验证来查看此信息。</p> <p>Novell 建议您将此设置保存在配置文件中。</p> <p>为了使 OpenWBEM CIMOM 能够与必要应用程序进行通信，当正在监视的客户程序和节点之间存在路由器和防火墙时，则必须在路由器和防火墙中打开此端口。</p>
5988	不安全	<p>OpenWBEM 通信通过 HTTP 服务使用的不安全端口。</p> <p>在默认情况下会禁用该设置。</p> <p>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信时，将打开并查看 CIMOM 和客户程序应用程序之间的所有通信。</p>

端口	类型	说明和建议
		Novell 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 OpenWBEM CIMOM 能够与需要非安全访问的必要应用程序进行通信，当正在监视的客户程序和节点之间存在路由器和防火墙时，则必须在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 11.2.3 节“更改端口配置” [231]。

## 身份验证

SUSE Linux Enterprise Server 中会对 OpenWBEM 设置以下身份验证设置并将这些设置启用为默认设置。

您可以更改所有的默认设置。请参见第 11.2.1 节“更改“身份验证”配置” [224]。

- `http_server.allow_local_authentication = true`
- `http_server.ssl_client_verification = disabled`
- `http_server.use_digest = false`
- `owcimmd.allow_anonymous = false`
- `owcimmd.allowed_users = root`
- `owcimmd.authentication_module = /usr/lib/openwbem/authentication/libpamauthentication.so`

默认情况下，OpenWBEM CIMOM 会启用 PAM；因此本地 root 用户可以通过本地 root 用户身份凭证来获得 OpenWBEM CIMOM 身份验证。

## 11.1.3 设置日志记录

您可以更改所有的默认设置。有关更多信息，请参见[第 11.2.4 节“更改默认日志记录配置”](#) [232]。

默认情况下，OpenWBEM 的日志记录设置将如下所示。

- `log.main.components = *`
- `log.main.level = ERROR`
- `log.main.type = syslog`

这表示 `owcimomd` 日志记录被设置为根据 `syslogd` 的配置来转至 `/var/log/messages` 文件或其他文件。它将记录所有组件（`owcimomd`）的全部错误。

## 11.2 更改 OpenWBEM CIMOM 配置

当 OpenWBEM CIMOM（`owcimomd`）启动时，它将从 `openwbem.conf` 文件度取运行时配置。`openwbem.conf` 文件位于 `/etc/openwbem` 目录中。

由分号（`;`）或井号（`#`）注释的选项的所有设置都使用默认设置。

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平台的本机格式，则可以使用此文本编辑器更改文件。

可以在 `openwbem.conf` 文件来更改这些设置。本节讨论以下配置设置：

- [第 11.2.1 节“更改“身份验证”配置”](#) [224]
- [第 11.2.2 节“更改证书配置”](#) [230]
- [第 11.2.3 节“更改端口配置”](#) [231]
- [第 11.2.4 节“更改默认日志记录配置”](#) [232]
- [第 11.2.5 节“配置“调试”日志记录”](#) [240]
- [第 11.2.6 节“配置其他日志”](#) [242]

## 11.2.1 更改“身份验证”配置

更改“身份验证”配置时，您可以控制以下方面：

- 能够访问 CIMOM 的人员
- 所使用的身份验证模块

请参见以下设置：

- “[http\\_server.allow\\_local\\_authentication](#)”一节 [224]
- “[http\\_server.digest\\_password\\_file](#)”一节 [225]
- “[http\\_server.ssl\\_client\\_verification](#)”一节 [226]
- “[http\\_server.ssl\\_trust\\_store](#)”一节 [226]
- “[http\\_server.use\\_digest](#)”一节 [227]
- “[owcimomd.ACL\\_superuser](#)”一节 [228]
- “[owcimomd.allow\\_anonymous](#)”一节 [228]
- “[owcimomd.allowed\\_users](#)”一节 [229]
- “[owcimomd.authentication\\_module](#)”一节 [229]
- “[simple\\_auth.password\\_file](#)”一节 [230]

### http\_server.allow\_local\_authentication

#### 目的

指示 http\_server 以允许本地身份验证而无需提供密码，这取决于本地系统文件权限。

可将此设置与“基本”或“摘要”设置一起使用。

## 语法

```
http_server.allow_local_authentication = option
```

选项	描述
true	启用本地身份验证。 这是默认设置。
false	禁用本地身份验证。

## 示例

```
http_server.allow_local_authentication = true
```

## http\_server.digest\_password\_file

### 目的

指定密码文件的位置。如果启用了 `http_server.use_digest` 设置，则需要指定密码文件的位置。

### 语法

```
http_server.digest_password_file = path_filename
```

以下是摘要密码文件的默认路径和文件名：

```
/etc/openwbem/digest_auth.passwd
```

### 示例

```
http_server.digest_password_file =  
/etc/openwbem/digest_auth.passwd
```

# http\_server.ssl\_client\_verification

## 目的

确定服务器是否应尝试通过 SSL 客户机证书验证来身份验证客户机。  
在默认情况下会禁用该设置。

## 语法：

```
http_server.ssl_client_verification = option
```

选项	描述
自动更新	指定与 <i>可选</i> 选项相同的功能；但是，会将传递 HTTP 身份验证的先前未知的客户机证书添加到可信储存以便带有相同证书的后续客户机连接无需进行 HTTP 身份验证。
已禁用	禁用客户机证书检查。  这是默认设置。
可选	允许身份验证可信证书（无需 HTTP 身份验证）。  档客户机传递 HTTP 身份验证时，还允许不可信证书传递 SSL 握手。
必需	需要可信证书以使 SSL 握手成功。

## 示例

```
http_server.ssl_client_verification = disabled
```

# http\_server.ssl\_trust\_store

## 目的

指定包含 OpenSSL 可信储存的目录。



## 语法

```
http_server.ssl_trust_store = path
```

以下是可信储存文件的默认路径。

```
/etc/openwbem/truststore
```

## 示例

```
http_server.ssl_trust_store = /etc/openwbem/truststore
```

## http\_server.use\_digest

### 目的

指示 HTTP 服务器使用“摘要”身份验证，这将绕过“基本”身份验证机制。要使用摘要，必须使用 `owdigestgenpass` 来设置摘要密码文件。

摘要不使用 `owcimomd.authentication_module` 配置设置所指定的身份验证模块。

## 语法

```
http_server.use_digest = option
```

选项	描述
false	启用“基本”身份验证机制。  这是默认设置。
true	禁用“基本”身份验证机制。

## 示例

```
http_server.use_digest = false
```

# owcimomd.ACL\_superuser

## 目的

指定用户的用户名，该用户能够访问由 owcimomd 维护的所有名称空间中的所有“通用信息模型”（CIM）数据。此用户可用来管理 /root/security 名称空间，该名称空间储存所有 ACL 用户权限。

在导入 OpenWBEM\_Acl1.0.mof 文件之前，将不启用 ACL 处理。

## 语法

```
owcimomd.ACL_superuser = username
```

## 示例

```
owcimomd.ACL_superuser = root
```

# owcimomd.allow\_anonymous

## 目的

启用或禁用匿名登录 owcimomd。

## 语法

```
owcimomd.allow_anonymous = option
```

选项	描述
false	需要使用用户名和密码登录以访问 owcimomd 数据。  这是默认和建议设置。
true	允许匿名登录 owcimomd。  这将禁用身份验证。无需用户名或密码就能够访问 owcimomd 数据。

示例

```
owcimomd.allowed_anonymous = false
```

owcimomd.allowed\_users

目的

指定允许访问 owcimomd 数据的用户列表。

语法

```
owcimomd.allowed_users = option
```

选项	描述
用户名	指定允许访问 owcimomd 数据的一个或多个用户。  每个用户名之间使用空格隔开。  root 用户为默认设置。
*	允许身份验证所有用户（例如，如果选择使用 ACL 来控制访问）。  除非将 owcimomd.allow_anonymous 设置为 true，否则将对所有身份验证方法强制设置此选项。

示例

```
owcimomd.allowed_users = bcwhitely jkcarey jlanderson
```

owcimomd.authentication\_module

目的

指定 owcimomd 使用的身份验证模块。此设置应为到包含身份验证模块的共享库的绝对路径。

## 语法

```
owcimomd.authentication_module = path_filename
```

以下是身份验证模块的默认路径和文件名：

```
/usr/lib/openwbem/authentication/libpamauthentication.so
```

## 示例

```
owcimomd.authentication_module =  
/usr/lib/openwbem/authentication/libpamauthentication.so
```

## simple\_auth.password\_file

### 目的

指定使用简单身份验证模块时密码文件的路径。

在默认情况下会禁用该设置。

### 语法

```
simple_auth.password_file = path_filename
```

### 示例

```
simple_auth.password_file =  
/etc/openwbem/simple_auth.passwd
```

## 11.2.2 更改证书配置

`http_server.SSL_cert` 和 `http_server.SSL_key` 设置指定包含主机私用密钥以及证书（OpenSSL 使用该证书进行 HTTPS 通讯）的文件的位置。

.pem 文件位于以下默认位置中：

```
/etc/openwbem/servercert.pem
```

```
/etc/openwbem/serverkey.pem
```

## 语法

```
http_server.SSL_cert = path_filename
```

或

```
http_server.SSL_key = path_filename
```

---

### 注意

密钥和证书可位于相同文件中。在此情况下，`http_server.SSL_cert` 和 `http_server.SSL_key` 的值应相同。

---

## 示例

```
http_server.SSL_cert = /etc/openwbem/servercert.pem
```

```
http_server.SSL_key = /etc/openwbem/servercert.pem
```

```
http_server.SSL_key = /etc/openwbem/serverkey.pem
```

## 11.2.3 更改端口配置

`http_server.http_port` 和 `server.https_port` 设置指定 `owcimomd` 侦听所有 HTTP 和 HTTPS 通讯所使用的端口号。

## 语法

```
http_server.http_port = option
```

或

```
http_server.https_port = option
```

选项	描述
<i>Specific_port_number</i>	指定 HTTP 或 HTTPS 通信的特定端口。  对于 HTTP，默认端口为 5988。  对于 HTTPS，默认端口为 5989。
-1	禁用 HTTP 或 HTTPS 连接（例如，如果您只希望支持 HTTPS 连接）。
0	运行时动态指派端口号。

## 示例

这些设置将禁用 HTTP 端口并启用端口 5989 来进行 HTTPS 通信：

```
http_server.http_port = -1
http_server.https_port = 5989
```

## 11.2.4 更改默认日志记录配置

owcimomd.conf 文件中的以下日志设置使您能够指定日志记录发生的位置和数量、记录的错误类型、日志大小、文件名和格式：

- “log.main.categories”一节 [233]
- “log.main.components”一节 [234]
- “log.main.format”一节 [235]
- “log.main.level”一节 [237]
- “log.main.location”一节 [238]
- “log.main.max\_backup\_index”一节 [238]
- “log.main.max\_file\_size”一节 [239]

- “log.main.type”一节 [240]

如果希望设置调试日志记录，请参见第 11.2.5 节 “配置“调试”日志记录” [240]。

如果希望设置其他日志，请参见第 11.2.6 节 “配置其他日志” [242]。

## log.main.categories

### 目的

指定日志输出的类别。

### 语法

```
log.main.categories = option
```

选项	描述
<i>category_name</i>	<p>指定使用空格分隔列表记录的类别。</p> <p>owcimomd 中使用的类别有：</p> <ul style="list-style-type: none"><li>• DEBUG</li><li>• ERROR</li><li>• FATAL</li><li>• INFO</li></ul> <p>有关这些选项的更多信息，请参见“log.main.level”一节 [237]。</p> <p>如果在此选项中指定，则将不会作为级别来处理预定义的类别，而是作为独立类别来处理预定义的类别。无默认值可用；如果未设置类别，则将不会记录类别并且将使用 log.main.level 设置。</p> <p>* 记录所有类别。</p>

选项	描述
	这是默认设置。

### 示例

```
log.main.categories = FATAL ERROR INFO
```

## log.main.components

### 目的

指定日志输出的组件。

### 语法

```
log.main.components = option
```

选项	描述
<i>component_name</i>	指定使用空格分隔列表记录的组件（如 owcimomd）。
	提供者可使用自己的组件。
*	指定记录所有组件。
	这是默认设置。

### 示例

```
log.main.components = owcimomd nssd
```



# log.main.format

## 目的

指定日志消息的格式（文本与 printf() 样式转换指定符混用）。

## 语法

```
log.main.format = conversion_specifier
```

选项	指定
%%	%
%c	组件（如 owcimomd）
%d	<p>Date</p> <p>可后跟日期格式指定符，以大括号括起。例如，%d{%H:%M:%S} 或 %d{%d %b %Y %H:%M:%S}。如果未提供日期格式指定符，则将假定使用 ISO 8601 格式。</p> <p>唯一的例外是 %Q，它是毫秒数。</p> <p>有关日期格式指定符的更多信息，请参见有关 strftime() 函数的文档（以 &lt;ctime&gt; 为标题）。</p>
%e	XML CData 格式的消息。这包含“<![CDATA[“ and ending “]]>”
%F	文件名
%l	文件名和行号。例如，file.cpp(100)
%L	行号

选项	指定
%M	发出日志记录请求的方法名称（仅在支持 <code>__PRETTY_FUNCTION__</code> 或 C99 的 <code>__func__</code> 的 C++ 编译器上工作）。
%m	消息
%n	依赖于平台的行分隔符（一个分隔符时为 <code>\n</code> 或多个分隔符时为 <code>\r\n</code> ）。
%p	类别，也称为级别或优先级。
%r	从应用程序启动到创建日志记录事件所经过的毫秒数。
%t	线程 ID
\n	换行
\t	Tab
\r	换行
\\	\
\x<hexDigits>	以十六进制表示的字符

可以更改最小字段宽度、最大字段宽度和对齐方式。可选格式修饰符位于百分比符号（%）和转换字符之间。第一个格式修饰符为左对齐标志，该标记为减号（-）字符。可选最小字段宽度修饰符跟在第一个格式修饰符之后，最小字段宽度修饰符为整数，表示输出的最小字符数。如果数据项需要较少的字符，则将根据对齐标志在数据项左侧或右侧补加空格。如果数据项大于最小字段宽度，则将扩展字段以适应数据长度。

最小字段宽度修饰符以句点（.）表示，后跟十进制常量。如果数据项长度长于最大字段，则将从数据项开头（默认设置）或从数据项末尾（如果指定了左对齐标志）删除多余字符。

## 示例

Log4j TTCC 布局:

```
"%r [%t] %-5p %c - %m"
```

与 TTCC 类似，但带有一些固定大小的字段:

```
"%-6r [%15.15t] %-5p %30.30c - %m"
```

符合 log4j.dtd 1.2 的 XML 输出，可由 Chainsaw 处理（如果使用此输出，则输出必须为一行；此处断行是为了可读性需要）:

```
"<log4j:event logger=\"%c\" timestamp=\"%d{%s%Q}\" level=\"%p\"
thread=\"%t\"> <log4j:message>%e</log4j:message>
<log4j:locationInfo class=\"\" method=\"\" file=\"%F\"
line=\"%L\"/></log4j:event>"
```

以下为默认值:

```
log.main.format = [%t]%m
```

## log.main.level

### 目的

指定日志输出的级别。如果设置该值，则日志将以指定级别或高于指定级别来输出所有预定义类别。

### 语法

```
log.main.level = option
```

选项	描述
DEBUG	记录所有“调试”、“信息”、“错误”和“致命”错误消息。
ERROR	记录所有“错误”和“致命”错误消息。

选项	描述
	这是默认设置。
FATAL	仅记录“致命”错误消息。
INFO	记录所有“信息”、“错误”和“致命”错误消息。

## 示例

```
log.main.level = ERROR
```

## log.main.location

### 目的

档 `log.main.type` 设置选项指定将日志记录发送到文件时，指定 `owcimomd` 使用的日志文件的位置。

### 语法

```
log.main.location = path_filename
```

### 示例

```
log.main.location = /system/cimom/var/owcimomd.log
```

## log.main.max\_backup\_index

### 目的

指定删除旧日志之前将保存的备份日志数量。

### 语法

```
log.main.backup_index = option
```

选项	描述
<i>unsigned_integer_above_0</i>	指定保存的备份日志数量。  默认设置是 1 个日志文件。
0	当达到最大文件大小时，将不会再创建备份日志并且日志会备截断。

### 示例

```
log.main.max_backup_index = 1
```

## log.main.max\_file\_size

### 目的

指定 owcimomd 日志的最大大小（以 KB 为单位）。

### 语法

```
log.main.max_file_size = option
```

选项	描述
<i>unsigned_integer_in_KB</i>	将日志限制为特定大小（以 KB 为单位）。
0	使日志的大小不受限制。  这是默认设置。

### 示例

```
log.main.max_file_size = 0
```

## log.main.type

### 目的

指定 owcimomd 使用的主日志类型。

### 语法

```
log.main.type = option
```

选项	描述
file	将所有消息发送到 log.main.location 配置设置中标识的文件中。
null	禁用日志记录。
syslog	将所有消息发送到 syslog 接口。 这是默认设置。

### 示例

```
log.main.type = syslog
```

## 11.2.5 配置“调试”日志记录

如果 owcimomd 以调试方式运行，则调试日志将为活动状态并由以下设置：

- log.debug.categories = \*
- log.debug.components = \*
- log.debug.format = [%t] %m
- log.debug.level = \*
- log.debug.type = stderr

# 为调试日志设置颜色

如果希望调试日志以彩色显示，则使用以下 ASCII 转义码：

```
log.debug.format =
\x1b[1;37;40m[\x1b[1;31;40m%- .6t\x1b[1;37;40m]\x1b[1;32;40m
%m\x1b[0;37;40m
```

如果希望使用其他颜色，则对 `log.debug.format` 命令使用以下代码：

**表 11.3** *log.debug.format* 命令的其他颜色代码

颜色	代码
红色	\x1b[1;31;40m
深红色	\x1b[0;31;40m
绿色	\x1b[1;32;40m
深绿色	\x1b[0;32;40m
黄色	\x1b[1;33;40m
深黄色	\x1b[0;33;40m
蓝色	\x1b[1;34;40m
深蓝色	\x1b[0;34;40m
紫色	\x1b[1;35;40m
深紫色	\x1b[0;35;40m
青色	\x1b[1;36;40m
深青色	\x1b[0;36;40m
白色	\x1b[1;37;40m

颜色	代码
暗灰色	\x1b[0;37;40m
灰色	\x1b[0;37;40m
重置颜色	\x1b[0;37;40m

## 11.2.6 配置其他日志

如果希望创建其他日志，则在以下设置中列处日志名称：

```
owcimomd.additional_logs = logname
```

日志名称之间以空格隔开。

### 语法

```
owcimomd.additional_logs = logname
```

为每个日志应用以下设置：

- `log.log_name.categories`
- `log.log_name.components`
- `log.log_name.format`
- `log.log_name.level`
- `log.log_name.location`
- `log.log_name.max_backup_index`
- `log.log_name.max_file_size`



## 示例

```
owcimomd.additional_logs = errorlog1 errorlog2 errorlog3
```

## 11.3 更多信息

有关 OpenWBEM 的更多信息，请参见以下信息：

- 本地服务器文件系统中 `usr/share/doc/packages/openwbem` 中的文档：
  - `readme`
  - `openwbem-faq.html`
- Novell 超酷解决方案条目：WBEM and OpenWBEM in SUSE Linux [<http://www.novell.com/coolsolutions/feature/14625.html>]（SUSE Linux 中的 WBEM 和 OpenWBEM）的介绍
- OpenWBEM 网站 [<http://www.openwbem.org>]
- DMTF 网站 [<http://www.dmtf.org>]



# 经由 IP 网络的大容量储存 — iSCSI

# 12

计算机中心和运行服务器时的核心问题之一是为服务器系统提供硬盘容量。在大型主机领域，经常使用光纤通道来解决这一问题。到目前为止，UNIX 计算机和多数服务器尚未连接到中央储存解决方案。

linux-iSCSI 提供了一种简单且价格合理的解决方案来将 Linux 计算机连接到中央储存系统。大体上说，iSCSI 表示在 IP 层次上传送 SCSI 命令。如果有程序对这种设备发出查询，操作系统将生成必要的 SCSI 命令。然后，会将这些命令嵌入到 IP 中并在需要时由软件进行加密，该软件通常为 *iSCSI 发起程序*。而后这些包将被传送到相应的 iSCSI 远程工作站（也称为 *iSCSI 目标*）。

许多储存解决方案允许通过 iSCSI 进行访问，但是也可以运行提供 iSCSI 目标的 Linux 服务器。在此情况下，针对文件系统服务对 Linux 服务器进行优化设置将非常重要。iSCSI 目标只是访问 Linux 中的块设备。因此，可以使用 RAID 解决方案增加磁盘空间以及大量内存从而改善数据缓存。有关 RAID 的更多信息，请参见第 7.2 节“软 RAID 配置”[111]。

## 12.1 设置 iSCSI 目标

SUSE® Linux Enterprise Server 附带从 Ardis iSCSI 目标进化而来的开放源代码 iSCSI 目标解决方案。基本设置可以通过 YaST 来完成，但是要充分利用 iSCSI，将需要手动设置。

## 12.1.1 通过 YaST 创建 iSCSI 目标

iSCSI 目标配置会将现有块设置活文件系统映像导出到 iSCSI 发起程序。首先，通过 YaST 创建所需块设备，或创建文件系统映像。有关分区概述，请参见第 8.5.7 节“使用 YaST 分区程序”[139]。必须手动创建文件系统映像。例如，如果希望创建大小为 4GB 的映像 `/var/lib/xen/images/xen-0`，则首先确保存在该目录，然后创建映像本身：

```
mkdir -p /var/lib/xen/images
dd if=/dev/zero of=/var/lib/xen/images/xen-0 seek=1M bs=4096 count=1
```

要配置 iSCSI 目标，请在 YaST 中运行 *iSCSI 目标* 模块。将在三个选项卡中完成配置。在 *服务* 选项卡中，选择启动方式和防火墙设置。如果希望从远程计算机访问 iSCSI 目标，则选择在防火墙中打开端口。如果 iSNS 服务器应管理发现和访问控制，则激活 *iSNS 访问控制* 并输入 iSNS 服务器的 IP 地址。请注意，您甚至不能使用有效的主机名，而必须使用 IP 地址。有关 iSNS 的更多信息，请阅读第 13 章 *iSNS for Linux 概述* [255]。

全局选项卡提供 *iSCSI 服务器* 的设置。此处的身份验证设置用于发现服务而非用于访问目标。如果不希望限制对发现的访问，则使用 *无身份验证*。

如果需要身份验证，则需要考虑两种可能性。一种可能性时发起程序必须证明它有权在 iSCSI 目标上运行发现。可通过 *进来的身份验证* 完成此操作。另一种可能性时 iSCSI 目标必须向发起程序证明它是所希望的目标。因此，iSCSI 目标还可提供用户名和密码。可通过 *发出的身份验证* 完成此操作。可在 RFC 3720 中找到有关身份验证的更多信息（请参见 <http://www.ietf.org/rfc/rfc3720.txt>）。

目标在 *目标* 选项卡中定义。使用 *添加* 创建新的 iSCSI 目标。第一个对话框会询问有关要导出的设备的信息。

### 目标

目标行有固定语法，如下所示：

```
iqn.yyyy-mm.<reversed domain name>
```

语法始终以 `iqn` 开头。`yyyy-mm` 是日期格式（日期为激活此目标的日期）。可在 RFC 3722 中找到有关命名约定的更多信息（请参见 <http://www.ietf.org/rfc/rfc3722.txt>）。

标识符

可自由选择标识符。标识符应跟在某模式之后以使整个系统具有良好的结构。

LUN

可以向目标指派多个 LUN。为此，请在*目标选项卡*中选择一个目标，然后单击*编辑*。在此，向某现有目标添加新的 LUN。

路径

添加到块设备的路径，或添加到要导出的文件系统映像的路径。

下个菜单配置目标的访问限制。配置与发现身份验证的配置非常相似。在此情况下，至少应设置一个进入的身份验证。

下一步完成新目标配置，并返回到*目标选项卡*的概述页面。可通过单击*完成*来激活更改。

## 12.1.2 手动配置 iSCSI 目标

在 `/etc/ietd.conf` 中配置 iSCSI 目标。此文件中第一个*目标声明*之前的所有参数对于文件来说是全局的。此部分的身份验证信息具有特殊的意义 — 它不是全局的，而是用于发现 iSCSI 目标。

如果有权访问 iSNS 服务器，首先要配置的是将有关此服务器的信息告知该目标。请注意，iSNS 服务器的地址必须始终用 IP 地址给出。普通的域名是不合格的。此功能的配置类似如下所示：

```
iSNSServer 192.168.1.111
iSNSAccessControl no
```

此配置使得 iSCSI 目标可在 iSNS 服务器中自我注册，反之，还提供对启动程序的发现。有关 iSNS 的更多信息，请阅读[第 13 章 iSNS for Linux 概述](#) [255]。请注意，不支持 iSNS 发现的访问控制。仅保留 `iSNSAccessControl no`。

所有直接 iSCSI 身份验证都可双向进行。iSCSI 目标可要求 iSCSI 发起程序使用 `IncomingUser` 来验证，可添加多次。iSCSI 发起程序还可要求 iSCSI 目标身份验证。在此情况下请使用 `OutgoingUser`。这两个方向的语法相同：

```
IncomingUser <username> <password>
OutgoingUser <username> <password>
```

身份验证后跟一个或多个目标定义。为每个目标添加 Target 部分。此部分总是以 Target 标识符开头，后跟逻辑单元编号定义：

```
Target iqn.yyyy-mm.<reversed domain name>[:identifier]
    Lun 0 Path=/dev/mapper/system-v3
    Lun 1 Path=/dev/hda4
    Lun 2 Path=/var/lib/xen/images/xen-1,Type=fileio
```

在 Target 行中，yyyy-mm 是激活此目标的日期，并可自由选择标识符。可在 RFC 3722 中找到有关命名约定的更多信息（请参见 <http://www.ietf.org/rfc/rfc3722.txt>）。在此示例中导出了三个不同的块设备。第一个块设备是逻辑卷（另见第 7.1 节“LVM 配置”[103]），第二个块设备是 IDE 分区，第三个设备是可在逻辑文件系统中获得的映像。对 iSCSI 发起程序来说，所有这三个块设备是相同的。

激活 iSCSI 目标之前，请在 Lun 定义后至少添加一个 IncomingUser。此操作身份验证此目标的使用。

要激活所有更改，可使用 `rcopen-iscsi restart` 重新启动 `iscsitarget` 守护程序。在 `/proc` 文件系统中检查配置：

```
cat /proc/net/iet/volume
tid:1 name:iqn.2006-02.com.example.iserv:systems
    lun:0 state:0 iotype:fileio path:/dev/mapper/system-v3
    lun:1 state:0 iotype:fileio path:/dev/hda4
    lun:2 state:0 iotype:fileio path:/var/lib/xen/images/xen-1
```

还有一些选项可控制 iSCSI 目标的行为。可在 `ietd.conf` 的手册页中找到这些选项。

`/proc` 文件系统中还会显示活动会话。对于每个连接的发起程序，会向 `/proc/net/iet/session` 额外添加一个项：

```
cat /proc/net/iet/session
tid:1 name:iqn.2006-02.com.example.iserv:system-v3
    sid:562949957419520
initiator:iqn.2005-11.de.suse:cn=rome.example.com,01.9ff842f5645
    cid:0 ip:192.168.178.42 state:active hd:none dd:none
    sid:281474980708864 initiator:iqn.2006-02.de.suse:01.6f7259c88b70
    cid:0 ip:192.168.178.72 state:active hd:none dd:none
```

## 12.1.3 通过 ietadm 配置联机目标

当需要更改 iSCSI 目标配置时，必须始终重新启动目标以激活配置文件中所作的更改。不幸的是，在此过程中将中断所有活动会话。要使操作不受干扰，应在主配置文件 `/etc/ietd.conf` 中执行更改，但是还要通过管理实用程序 `ietadm` 来手动更改当前配置。

要通过 LUN 创建新 iSCSI 目标，请首先更新配置文件。以下是附加项：

```
Target iqn.2006-02.com.example.iserv:system2
    Lun 0 Path=/dev/mapper/system-swap2
    IncomingUser joe secret
```

要手动设置此配置，请如下继续操作：

- 1 使用命令 `ietadm --op new --tid=2 --params Name=iqn.2006-02.com.example.iserv:system2` 创建新目标。
- 2 使用 `ietadm --op new --tid=2 --lun=0 --params Path=/dev/mapper/system-swap2` 添加逻辑单元。
- 3 使用 `ietadm --op new --tid=2 --user --params=IncomingUser=joe,Password=secret` 设置此目标上的用户名和密码组合。
- 4 使用 `cat /proc/net/iet/volume` 检查配置。

还可以删除活动连接。首先，使用命令 `cat /proc/net/iet/session` 检查所有活动连接。此操作可能如下所示：

```
cat /proc/net/iet/session
tid:1 name:iqn.2006-03.com.example.iserv:system
    sid:281474980708864 initiator:iqn.1996-04.com.example:01.82725735af5
    cid:0 ip:192.168.178.72 state:active hd:none dd:none
```

要删除会话 ID 为 `281474980708864` 的会话，请使用命令 `ietadm --op delete --tid=1 --sid=281474980708864 --cid=0`。请注意：此操作会导致在客户机系统上无法访问设备并且访问此设备的进程可能会挂起。

`ietadm` 还可用来更改各种配置参数。使用 `ietadm --op show --tid=1 --sid=0` 获取全局变量列表。输出将如下所示：

```
InitialR2T=Yes
ImmediateData=Yes
MaxConnections=1
MaxRecvDataSegmentLength=8192
MaxXmitDataSegmentLength=8192
MaxBurstLength=262144
FirstBurstLength=65536
DefaultTime2Wait=2
DefaultTime2Retain=20
MaxOutstandingR2T=1
DataPDUInOrder=Yes
DataSequenceInOrder=Yes
ErrorRecoveryLevel=0
HeaderDigest=None
DataDigest=None
OFMarker=No
IFMarker=No
OFMarkInt=Reject
IFMarkInt=Reject
```

可以轻松地更改所有这些参数。例如，如果希望将最大连接数更改为两个连接，则使用 `ietadm --op update --tid=1 --params=MaxConnections=2`。在文件 `/etc/ietd.conf` 中，关联行应类似于 `MaxConnections 2`。

---

**警告：**根据通过 **ietadm** 所作的更改来更新 **ietd.conf**

系统上使用命令 `ietadm` 所作的更改不是永久性的。如果未将更改添加到配置文件 `/etc/ietd.conf` 中，则下次重引导时这些更改将丢失。根据网络中 iSCSI 的使用，此操作可能会导致严重的问题。

---

还有多个选项可用于命令 `ietadm`。可使用 `ietadm -h` 查找概述。该处的缩写为目标 ID（tid）、会话 ID（sid）和连接 ID（cid）。还可在 `/proc/net/iet/session` 中找到这些缩写。

## 12.2 配置 iSCSI 发起程序

iSCSI 发起程序也称为客户程序，可用来连接到任意 iSCSI 目标。连接不限于以上说明的 iSCSI 目标解决方案。iSCSI 发起程序配置包括两个主要步骤 — 发现可用 iSCSI 目标和设置 iSCSI 会话。这两个步骤都可通过 YaST 完成。



## 12.2.1 使用 YaST 配置 iSCSI 发起程序

将在三个选项卡中完成配置。可使用*服务*选项卡来在引导时启用 iSCSI 启用器。它还允许设置唯一的*启动程序名称*和 iSNS 服务器以用于发现。iSNS 的默认端口为 3205。*已连接目标*选项卡概述了当前已连接的 iSCSI 目标。与*已发现目标*选项卡相似，它提供用于向系统添加新目标的选项。*已发现目标*是首先要使用的选项卡。它使您能够发现网络中的 iSCSI 目标。

- 1 使用发现来打开发现对话框。
- 2 输入 IP 地址并根据需要更改端口。
- 3 如果需要，可添加入或出身份验证。
- 4 单击下一步来启动发现。

发现成功后，可使用登录激活目标。将会询问身份验证信息以使用选定 iSCSI 目标。单击下一步完成配置。如果操作一切顺利，则目标将会显示在*已连接目标*中。

虚拟 iSCSI 设备现在为可用。可使用 `lsscsi` 来查找实际设备：

```
lsscsi
[1:0:0:0]    disk      IET          VIRTUAL-DISK    0          /dev/sda
```

## 12.2.2 手动设置 iSCSI 发起程序

发现和配置 iSCSI 连接都要求 `iscsid` 正在运行。首次运行发现时，将在 `/var/lib/open-iscsi` 目录中创建 iSCSI 发起程序的内部数据库。

如果发现受密码保护，则向 `iscsid` 提供身份验证信息。由于首次执行发现时内部数据库并不存在，因而因此将无法使用内部数据库。相反，必须编辑配置文件 `/etc/iscsid.conf` 以提供信息。要为发现添加密码信息，请在 `/etc/iscsid.conf` 末尾添加以下行：

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = <username>
discovery.sendtargets.auth.password = <password>
```

发现会将所有接收到的值储存在一个内部持久数据库中。此外，它会显示所有检测到的目标。使用命令 `iscsiadm -m discovery --type=st`  
`--portal=<targetip>` 来运行此发现。输出应如下所示：

```
149.44.171.99:3260,1 iqn.2006-02.com.example.iserv:systems
```

要在 iSNS 服务器上发现可用目标，请使用命令 `iscsiadm --mode`  
`discovery --type isns --portal <targetip>`

对于 iSCSI 目标上定义的每个目标，将显示一行。要了解如何获取有关储存数据的更多信息，请参见第 12.2.4 节“iSCSI 客户机数据库”[253]。

`iscsiadm` 的特殊 `--login` 选项会创建所有需要的设备：

```
iscsiadm -m node -n iqn.2006-02.com.example.iserv:systems --login
```

新生成的设备会显示在 `ls SCSI` 的输出中，并且现在可以通过 `mount` 访问这些设备。

## 12.2.3 在 iSCSI 设备上配置 LVM 自动组装

LVM 启动受 `udev` 支持，所以一旦检测到所有必需的物理卷之后，所有 LVM 卷组将通过 `udev` 自动激活。

`udev` 中的 LVM 自动组装利用 `udev` 帮助程序 `collect`。此程序取一个要检查的抽象 ID 后跟组件 ID 列表作为第一个自变量。一旦使用每个组件 ID 作为第一个自变量调用该程序时，它将返回 0。

因此，对于自动组装，给定卷组的物理卷 UUID 注册为 `collect` 的自变量列表。`udev`（或 `vol_id`）能够检测到一个设备上的物理卷 UUID，因此可以作为第一个自变量传递给 `collect`。

使用所有物理卷 UUID 调用 `collect`（即 `udev` 收到所有组件设备的事件）后，将激活后面只调用 `vgchange -a y <vgname>` 的规则触发器和该卷组。

### 如何配置

使用脚本 `/usr/share/doc/packages/lvm2/lvm-vg-to-udev-rules.sh`。它取您想要自动启动的卷组作为自变量。该脚本将生成所需的 `udev` 规则。现在，重新启动 iSCSI 以激活这些卷组。如果想要在引导时自动启动该阵列，则

必须将 iSCSI 组件设备切换为 `automatic`，以便发起程序在引导时自动登录目标。

## 12.2.4 iSCSI 客户机数据库

iSCSI 发起程序发现的所有信息都储存在位于 `/var/lib/open-iscsi` 的两个数据库文件中。一个数据库用于发现的目标，另一个数据库用于发现的节点。访问数据库时，首先必须选择是希望从发现获取数据还是从节点数据库获取数据。可使用 `iscsiadm` 的参数 `-m discovery` 和 `-m node` 来执行此操作。仅将 `iscsiadm` 与其中一个参数一起使用可提供储存记录概述：

```
iscsiadm -m discovery
149.44.171.99:3260,1 iqn.2006-02.com.example.iserv:systems
```

本示例中的目标名称为 `iqn.2006-02.com.example.iserv:systems`。与此特殊数据集相关的所有操作都需要此名称。要检查 ID 为

`iqn.2006-02.com.example.iserv:systems` 数据记录的内容，可使用以下命令：

```
iscsiadm -m node --targetname iqn.2006-02.com.example.iserv:systems
node.name = iqn.2006-02.com.example.iserv:systems
node.transport_name = tcp
node.tpgt = 1
node.active_conn = 1
node.startup = manual
node.session.initial_cmdsns = 0
node.session.reopen_max = 32
node.session.auth.authmethod = CHAP
node.session.auth.username = joe
node.session.auth.password = *****
node.session.auth.username_in = <empty>
node.session.auth.password_in = <empty>
node.session.timeo.replacement_timeout = 0
node.session.err_timeo.abort_timeout = 10
node.session.err_timeo.reset_timeout = 30
node.session.iscsi.InitialR2T = No
node.session.iscsi.ImmediateData = Yes
....
```

要编辑这些变量的值，可将 `iscsiadm` 与更新操作一起使用。例如，如果希望 `iscsid` 在初始化时登录 iSCSI 目标，则将变量 `node.startup` 的值设置为 `automatic`：

```
iscsiadm -m node -n iqn.2006-02.com.example.iserv:systems --op=update
--name=node.startup --value=automatic
```

执行操作删除来删除过时的数据集。如果目标

`iqn.2006-02.com.example.iserv:systems` 不再是有效的记录, 请使用命令 `iscsiadm -m node -n`

`iqn.2006-02.com.example.iserv:systems --op=delete` 删除此记录。使用此选项时应谨慎, 因为它会删除该记录而无任何附加确认提示。

要获取所有已发现目标的列表, 请运行命令 `iscsiadm -m node`。

## 12.2.5 更多信息

iSCSI 协议已面世多年。有许多评论和其他文档将 iSCSI 与 SAN 解决方案作比较, 通常是比较性能基准, 或只说明硬件解决方案。有关 `open-iscsi` 的更多信息, 请参见以下重要页面:

- <http://www.open-iscsi.org/>
- <http://www.open-iscsi.org/cgi-bin/wiki.pl>
- <http://www.novell.com/coolsolutions/appnote/15394.html>

还有一些联机文档。请参见 `iscsiadm`、`iscsid`、`ietd.conf` 和 `ietd` 的手册页, 以及示例配置文件 `/etc/iscsid.conf`。

## iSNS for Linux 概述

储存区域网络 (SAN) 可包含分布在复杂网络间的许多磁盘驱动器。这会使设备发现和设备所有权变得复杂。iSCSI 发起程序必须能够识别 SAN 中的储存资源，并确定是否可对其进行访问。

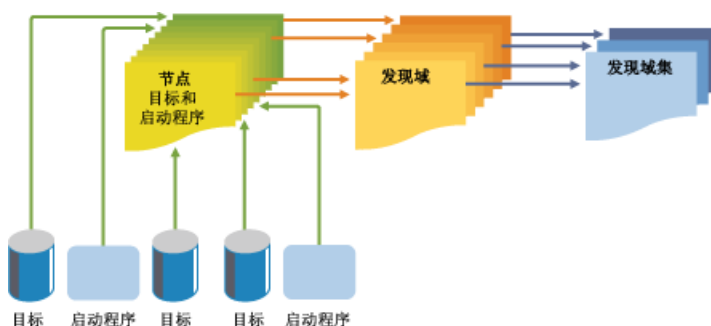
因特网储存名称服务 (iSNS) 是基于标准的服务，由 SUSE Linux Enterprise Server (SLES) 10 支持包 2 提供。iSNS 实现了 iSCSI 设备在 TCP/IP 网络上的自动发现、管理和配置。与光纤通道网络中的服务相比，iSNS 可提供智能的储存发现和管理服务。

### 13.1 iSNS 的工作原理

iSCSI 发起程序要发现 iSCSI 目标，需要识别网络中的哪些设备是储存资源以及访问这些资源需要哪些 IP 地址。对 iSNS 服务器的查询会返回启动程序有权访问的一个 iSCSI 目标和 IP 地址的列表。

使用 iSNS，可以创建 iSNS 发现域和发现域集。然后，将 iSCSI 目标和启动程序分组或组织为发现域，并将发现域分组到发现域集。通过将储存节点划分到域，您可以将每个主机的发现进程限制为在 iSNS 中注册的最合适的目标子集，这使得储存网络可通过降低不必要的发现数和限制每个主机在建立发现关系时花费的时间而按比例缩放。这使您可以控制和简化必须发现的目标和启动程序的数目。

图 13.1 iSNS 发现域和发现域集



iSCSI 目标和 iSCSI 发起程序都使用 iSNS 客户程序启动通过 iSNS 协议与 iSNS 服务器的事务。然后，它们在公共发现域中注册设备属性信息、下载有关其他注册客户程序的信息，以及接收出现在其发现域中的事件的异步通知。

iSNS 服务器响应由 iSNS 客户程序使用 iSNS 协议作出的 iSNS 协议查询和请求。iSNS 服务器启动 iSNS 协议状态更改通知，并正确储存由 iSNS 数据库中的注册请求提交的身份验证信息。

iSNS for Linux 的某些优点包括：

- 提供信息设备以供注册、发现和管理联网储存资产。
- 与 DNS 基础结构集成。
- 统一 iSCSI 储存的注册、发现和管理。
- 简化储存管理实施。
- 与其他发现方法相比，改进了可伸缩性。

以下情境可以帮助您更好地理解 iSNS 的优点：

假定您拥有一家配有 100 个 iSCSI 发起程序和 100 个 iSCSI 目标的公司。根据您的配置，所有 iSCSI 发起程序都可能尝试发现并连接到 100 个 iSCSI 目标的任一个。这将造成可怕的发现和连接状况。通过将启动程序和目标分组到发现域，您可以阻止某个部门的 iSCSI 发起程序发现其他部门的 iSCSI 目标。因此，某特定部门中的 iSCSI 发起程序只发现属于该部门发现域中的那些 iSCSI 目标。

## 13.2 iSNS for Linux 安装和设置

iSNS for Linux 随附在 SLES 10 SP2 中，但默认情况下不会安装或配置。必须安装 iSNS 包模块（`isns` 和 `yast2-isns` 模块），并配置或设置 iSNS 才能使用它。

---

### 注意

iSNS 可以与 iSCSI 目标或启动程序安装在同一台服务器上。不支持在同一台计算机上使用 iSCSI 目标和启动程序。

---

安装 iSNS for Linux：

- 1 启动 YaST，然后选择*软件管理*。
- 2 在搜索字段中，输入 `isns`。
- 3 选择 `isns` 和 `yast2-isns` 包，然后单击接受。

## 13.3 设置 iSNS

iSNS 必须在服务器上启动。您可以通过在安装它的服务器的控制台上输入 `rcisns start` 或 `/etc/init.d/isns start` 来执行此操作。您还可以对 iSNS 使用停止、状态和重新启动选项。

iSNS 还可以配置为在每次重引导服务器时自动启动。执行的操作

- 1 启动 YaST，然后在*网络服务*下选择 *iSNS 服务器*。
- 2 使用所选的*服务选项卡*，指定 iSNS 服务器的 IP 地址，然后单击*保存地址*。
- 3 在屏幕的“服务启动”部分，选择*引导时*。

还可以选择手动启动 iSNS 服务器。然后，每次重新启动服务器时，必须使用 `rcisns start` 命令启动该服务。

## 13.3.1 创建 iSNS 发现域

为使 iSCSI 发起程序和目标使用 iSNS 服务，它们必须属于某个发现域。安装 iSNS 服务时，将会自动创建一个名为默认 *DD* 的默认发现域。已配置为使用 iSNS 的现有 iSCSI 目标和启动程序会自动添加到默认的发现域。

创建新的发现域：

- 1 启动 YaST，然后在*网络服务*下选择 *iSNS 服务器*。

- 2 单击*发现域*选项卡，然后单击*创建发现域*按钮。

还可以选择现有发现域，然后单击*删除按钮*删除该发现域。

- 3 指定创建的发现域的名称，然后单击*确定*。

## 13.3.2 创建 iSNS 发现域集

发现域必须属于某个发现域集。您可以创建一个发现域，并向该发现域添加节点，但除非将该发现域添加到某发现域集，否则，它是不活动的，且 iSNS 服务不起作用。安装 iSNS 时将自动创建一个名为默认 *DDS* 的默认发现域集，默认发现域将自动添加到该域集。

创建发现域集：

- 1 启动 YaST，然后在*网络服务*下选择 *iSNS 服务器*。

- 2 单击*发现域集*选项卡，然后单击*创建发现域集*按钮。

还可以选择现有发现域集，然后单击*删除按钮*删除该发现域集。

- 3 指定创建的发现域集的名称，然后单击*确定*。

## 13.3.3 向发现域添加 iSCSI 节点

- 1 启动 YaST，然后在*网络服务*下选择 *iSNS 服务器*。



- 2 单击 *iSCSI* 节点选项卡，确保要使用 iSNS 服务的 iSCSI 目标和启动程序已列出。

如果未列出 iSCSI 目标或启动程序，可能需要在节点上重新启动 iSCSI 服务。还可以通过运行 `rcopen-iscsi restart` 命令重新启动启动程序或 `rciscsitarget restart` 命令重新启动目标来完成此操作。

可以选择某 iSCSI 节点，然后单击 **删除按钮** 从 iSNS 数据库中删除该节点。如果不再使用某 iSCSI 节点或已对其重命名，这十分有用。

除非删除或注释掉 iSCSI 配置文件的 iSNS 部分，否则，在重新启动 iSCSI 服务或重引导服务器时，iSCSI 节点将再次自动添加到列表（iSNS 数据库）。

- 3 单击 **发现域** 选项卡，选择所需的发现域，然后单击 **显示成员按钮**。
- 4 单击 **添加现有 iSCSI 节点**，选择要添加到域中的节点，然后单击 **添加节点**。
- 5 重复上一步骤（重复次数等于要向发现域添加的节点数），然后在添加节点完成后单击 **完成**。

一个 iSCSI 节点可能属于多个发现域。

## 13.3.4 将发现域添加到发现域集

- 1 启动 YaST，然后在 **网络服务** 下选择 *iSNS 服务器*。
- 2 单击 **发现域集** 选项卡。
- 3 选择 **创建发现域集** 将新集添加到发现域集列表。
- 4 选择要修改的发现域集。
- 5 单击 **添加发现域**，选择要添加到发现域集中的发现域，然后单击 **添加发现域**。
- 6 重复上一步骤（重复次数等于要向发现域集添加的发现域数），然后单击 **完成**。

一个发现域可属于多个发现域集。

## 13.4 更多信息

linuxisns 项目托管于 <http://sourceforge.net/projects/linuxisns/>。该项目的邮件列表可在 [http://sourceforge.net/mailarchive/forum.php?forum\\_name=linuxisns-discussion](http://sourceforge.net/mailarchive/forum.php?forum_name=linuxisns-discussion) 中找到。有关 iSNS 的一般信息写在 rfc4171 中。另请参见<http://www.ietf.org/rfc/rfc4171>。

# Oracle Cluster File System 2

Oracle Cluster File System 2 (OCFS2) 是一个一般用途的日志文件系统，它完全集成到 Linux 2.6 和更高版本的内核中。OCFS2 允许您在 SAN 中的设备上储存应用程序二进制文件、数据文件和数据库。群集中的所有节点对文件系统都有并行的读和写权限。分布式锁管理器能够防止文件访问冲突。OCFS2 支持最多 32,000 个子目录，每个目录中有数百万的文件。O2CB 群集服务（驱动程序）在每个节点上运行以管理群集。

SUSE Linux Enterprise Server 9 中添加了 OCFS2 以支持 Oracle Real Application Cluster (RAC) 数据库及其应用程序文件 Oracle Home。在 SUSE Linux Enterprise Server 10 和更高版本中，OCFS2 可用于以下任何储存解决方案：

- Oracle RAC 和其他数据库
- 一般应用程序和工作负荷
- 在群集中储存的 XEN 图形

XEN 虚拟计算机和虚拟服务器可以储存在由群集服务器安装的 OCFS2 卷上，以在服务器之间提供 XEN 虚拟机的快速、简便性。

- LAMP（Linux、Apache、MySQL 和 PHP | PERL | Python）堆栈

另外，它完全与 Heartbeat 2 集成。

作为一个高性能、均衡的并行群集文件系统，OCFS2 支持以下功能：

- 群集中的所有节点都可以使用应用程序文件。用户只需在群集中的 OCFS2 上安装它一次。

- 所有节点可以通过标准的文件系统接口直接同时读写到储存器，方便地管理运行在群集中的应用程序。

- 通过分布式锁管理器（DLM）协调文件访问。

DLM 控制适合大多数情况，但是如果应用程序的设计与 DLM 竞争来协调文件的访问，则可能会限制其可测量性。

- 所有后端储存上都可以使用储存备份功能。可以方便地创建共享应用程序文件的图形，它能够帮助提供有效的故障恢复。

OCFS2 还提供以下功能：

- 元数据高速缓存
- 元数据日志
- 跨节点的文件数据一致性
- 通过 `ocfs2console` 实用程序的 GTK 基于 GUI 的管理
- 作为共享根文件系统的操作
- 支持最大为 4 KB 的多块大小（每个卷可以有不同块大小），支持最大为 16 TB 的卷大小。
- 支持最多 255 个群集节点
- 上下文相关的符号链接（CDSL）支持节点特定的本地文件
- 用于数据库文件的异步和直接 I/O 支持改进了数据库性能

## 14.1 O2CB 群集服务

O2CB 群集服务是一组模块和内存中文件系统，管理 OCFS2 服务和卷时需要它们。您可以在系统引导期间装载和装入这些模块。有关指导，请参见第 14.6.2 节“配置 OCFS2 服务” [267]。

表 14.1 O2CB 群集服务堆栈

服务	说明
节点管理器 (NM)	跟踪 <code>/etc/ocfs2/cluster.conf</code> 文件中的所有节点
Heartbeat (HB)	节点连接或离开群集时发出向上/向下通知
TCP	处理使用 TCP 协议的节点之间的通信
分布式锁管理器 (DLM)	了解全部锁和它们的所有者及状态
CONFIGFS	用户空间配置文件系统。有关细节，请参见第 14.3 节 “内存中的文件系统” [264]
DLMFS	内核空间 DLM 的用户空间接口。有关细节，请参见第 14.3 节 “内存中的文件系统” [264]

## 14.2 磁盘的检测信号

OCFS2 要求节点在网络上活动的。O2CB 群集服务发送通常保持活动的包以确保它们的存在。它在节点之间使用专用的连接（而不是 LAN）以避免发生网络延迟，这种延迟可能会被认为是节点消失，因此会导致节点的自我封闭。

OC2B 群集服务通过磁盘的检测信号与节点状态进行通信。检测信号系统文件驻留在储存区域网络 (SAN) 上，它对于群集中的所有其他节点都可用。文件中的块分配先后对应于每个节点的槽分配。

每个节点在两秒钟的时间间隔内读写它所分配到的块。对节点的时间戳记的更改表明该节点是活动的。如果在指定的时间间隔内（称为检测信号阈值）节点对检测信号文件没有进行写操作，则表明该节点已经死了。即使只有一个节点是活动的，O2CB 群集服务也必须执行此检查，因为在任何时候都可以动态地添加其他节点。

您可以使用 `O2CB_HEARTBEAT_THRESHOLD` 参数修改 `/etc/sysconfig/o2cb` 文件中的磁盘检测信号阈值。等待时间按如下所示的方法计算：

`(O2CB_HEARTBEAT_THRESHOLD value - 1) * 2 = threshold in seconds`

例如，如果O2CB\_HEARTBEAT\_THRESHOLD值设置成默认值7，则等待时间是12秒  $((7 - 1) * 2 = 12)$ 。

## 14.3 内存中的文件系统

OCFS2 为通信使用两种内存中的文件系统：

表 14.2 OCFS2 使用的内存中的文件系统

内存中的文件系统	说明	装入点
configfs	群集中的节点列表与内核中的节点管理器进行通信，用于检测信号的资源与内核中检测信号线程进行通信	/config
ocfs2_dlmfs	锁定和解锁资源的群集范围锁与内核中分布式锁管理器（了解所有锁以及锁的所有者和状态）之间进行通信	/dlm

## 14.4 管理实用程序和命令

OCFS2将特定于节点参数文件储存在节点上。群集配置文件(/etc/ocfs2/cluster.conf) 驻留在每个指派给群集的节点上。

ocfs2console 实用程序是一个 GTK 基于 GUI 的接口，它用于管理群集中 OCFS2 服务的配置。使用此实用程序设置并将 /etc/ocfs2/cluster.conf 文件保存到群集的所有成员节点。另外，您可以使用它格式化、调整、安装和卸载 OCFS2 卷。

---

**重要**

`ocfs2console` 实用程序中的文件浏览器列非常慢，且在群集间不一致。建议您使用 `ls(1)` 命令来列出文件。

---

下表描述了其他 OCFS2 实用程序。有关这些命令的语法信息，请参见它们的手册页。

**表 14.3** *OCFS2 实用程序*

OCFS2 实用程序	说明
<code>debugfs.ocfs2</code>	为了调试检查 OCFS 文件系统的状态。
<code>fsck.ocfs2</code>	检查文件系统的错误并进行选择性的修改。
<code>mkfs.ocfs2</code>	在某个设备上创建 OCFS2 文件系统，通常是共享物理或逻辑磁盘上的某个分区。此工具需要启动 O2CB 群集服务。
<code>mounted.ocfs2</code>	检测并列出群集系统上所有的 OCFS2 卷。检测并列出已经安装了 OCFS2 设备的系统上的所有节点或列出所有的 OCFS2 设备。
<code>ocfs2cdsl</code>	为节点的指定文件名（文件或目录）创建上下文相关的符号链接（CDSL）。CDSL 文件名有它自己的特定节点的图像，但是在 OCFS2 中有一个公共名称。
<code>tune.ocfs2</code>	更改 OCFS2 文件系统参数，包括卷标、节点槽号、所有节点槽的日志大小和卷大小。

---

使用以下命令管理 O2CB 服务。有关 `o2cb` 命令语法的更多信息，请参见其手册页。

**表 14.4** *O2CB 命令*

命令	说明
<code>/etc/init.d/o2cb status</code>	报告是否加载和装入 O2CB 服务。

命令	说明
<code>/etc/init.d/o2cb load</code>	加载 O2CB 模块和内存中文件系统。
<code>/etc/init.d/o2cb online</code> <code>ocfs2</code>	名为 ocfs2 的群集联机。  群集中至少有一个节点必须对要联机的群集来说是活动的。
<code>/etc/init.d/o2cb offline</code> <code>ocfs2</code>	名为 ocfs2 的群集脱机。
<code>/etc/init.d/o2cb unload</code>	卸载 O2CB 模块和内存中文件系统。
<code>/etc/init.d/o2cb start</code> <code>ocfs2</code>	如果设置群集引导时装入，则装入 o2cb 并联机群集时会启动名为 ocfs2 的群集。  群集中至少有一个节点必须对要联机的群集来说是活动的。
<code>/etc/init.d/o2cb stop</code> <code>ocfs2</code>	如果群集被设置成引导时装入，则通过脱机群集并卸载 O2CB 模块和内存中文件系统停止名为 ocfs2 的群集。

## 14.5 OCFS2 包

OCFS2 内核模块（`ocfs2`）在 SUSE Linux Enterprise Server 10 和更高版本中是自动安装的。要使用 OCFS2，使用 YaST（如果您喜欢可以使用命令行）在群集的每个节点上安装 `ocfs2-tools` 和 `ocfs2console` 包。

- 1 以 `root` 用户身份登录，然后打开 YaST 控制中心。
- 2 选择 **软件 > 软件管理**。
- 3 在 **搜索** 字段中，输入 `ocfs2`。



软件包 `ocfs2-tools` 和 `ocfs2console` 应该在右侧面板中列出。如果它们是被选的，则说明已经安装了这些包。

- 4 如果您需要安装这些包，则选择它们，然后单击安装并遵循屏幕上的指示进行操作。

## 14.6 创建 OCFS2 卷

按照本部分中的过程配置您的系统以使用 OCFS2 并创建 OCFS2 卷

### 14.6.1 前提条件

开始操作之前，请完成以下操作：

- 在 SAN 磁盘上根据需要初始化、分割或配置 RAID（独立磁盘冗余阵列），为计划用于 OCFS2 卷的设备作准备。将这些设备留作可用空间。

建议您在不同的 OCFS2 卷上储存应用程序文件和数据文件，但是，只有当您的应用程序卷和数据卷有不同的装入要求时，才强制您这样做。例如，Oracle RAC 数据库卷要求 `datavolume` 和 `nointr` 装入选项，而 Oracle Home 卷从不会使用这些选项。

- 确保已经安装了 `ocfs2console` 和 `ocfs2-tools` 包。使用 YaST 或命令行方法安装它们（如果它们不存在）。有关 YaST 的说明，请参见第 14.5 节“OCFS2 包”[266]。

### 14.6.2 配置 OCFS2 服务

创建 OCFS2 卷之前，必须配置 OCFS2 服务。在以下过程中，生成 `/etc/ocfs2/cluster.conf` 文件，在所有节点上保存 `cluster.conf` 文件并创建和启动 O2CB 群集服务 (`o2cb`)。

为群集中的某个节点执行本部分描述的过程。

- 1 打开终端窗口并以 `root` 用户身份登录。

- 2 如果还未启用 o2cb 群集服务，请输入 `chkconfig --add o2cb`。

当您添加一个新服务时，`chkconfig` 确保在每个运行级别上，服务都有一个启动或杀死条目。

- 3 如果还未启用 ocfs2 服务，请输入 `chkconfig --add ocfs2`。

- 4 配置 o2cb 群集服务驱动程序以在引导时加载。

**4a** 输入 `/etc/init.d/o2cb configure`

**4b** 在 `Load O2CB driver on boot (y/n) [n]` 提示下，输入 `y`（是）以在引导时启用装载。

**4c** 在 `Cluster to start on boot (Enter "none" to clear) [ocfs2]` 提示下，输入 `none`。此选项假设您是第一次设置 **OCFS2** 或重新设置该服务。当您设置 `/etc/ocfs2/cluster.conf` 文件时，请在下一个步骤中指定群集名称。

- 5 使用 `ocfs2console` 实用程序设置并将 `/etc/ocfs2/cluster.conf` 文件保存至群集的所有成员节点。

此文件应该在群集中的所有节点上都是相同的。使用以下步骤设置第一个节点。然后，您可以使用 `ocfs2console` 将新节点动态添加到群集并将修改过的 `cluster.conf` 文件传播到所有节点。

但是，如果您更改其他设置，如群集名称和 IP 地址，则必须重新启动该群集使更改生效，请参见 [步骤 6 \[269\]](#)。

**5a** 输入 `ocfs2console` 以打开 `ocfs2console` GUI。

**5b** 在 `ocfs2console` 中，选择 **群集 > 群集节点**。

如果 `cluster.conf` 不存在，则控制台将创建一个，其默认群集名为 `ocfs2`。根据需要修改群集名。

**5c** 在“节点配置”对话框中，单击 **添加** 以打开“添加节点”对话框。

- 5d** 在“添加节点”对话框中，指定主节点的唯一名称、唯一 IP 地址（如 192.168.1.1）和端口号（可选的，默认值是 7777），然后单击确定。

ocfs2console 控制台从 0 到 254 开始依次分配节点槽号。

- 5e** 在“节点配置”对话框中，单击应用，然后单击关闭以离开“添加节点”对话框。

- 5f** 单击群集 > 传播配置以将 cluster.conf 文件保存至所有节点。

- 6** 如果您需要重新启动 OCFS2 群集以使更改生效，输入以下内容，等待返回 OK 状态的过程。

```
/etc/init.d/o2cb stop  
/etc/init.d/o2cb start
```

## 14.6.3 创建 OCFS2 卷

应该仅在群集中的某个节点上执行创建 OCFS2 文件系统并将新节点添加到群集。

- 1** 打开终端窗口并以 root 用户身份登录。
- 2** 如果 O2CB 群集服务是脱机的，则输入以下命令启动它，并等待返回确定状态的过程。

```
/etc/init.d/o2cb online ocfs2
```

用 OCFS2 群集的实际名称替换 ocfs2。

OCFS2 群集必须是联机的，因为格式化操作必须首先确保群集中的任何节点上没有安装卷。

- 3** 使用以下方法之一创建和格式化卷：
  - 在 EVMSGUI 中，转至“卷”页，选择制作文件系统 > OCFS2，然后指定配置设置。

- 使用 `mkfs.ocfs2` 实用程序。有关此命令语法的信息，请参见 `mkfs.ocfs2` 手册页。
- 在 `ocfs2console` 中，单击 *任务 > 格式化*，在您要用于 OCFS2 卷的可用设备列表表中选择一个设备，为卷指定配置设置，然后单击 *确定* 以格式化该卷。

请参见下表以获得建议的设置。

OCFS2 参数	描述和建议
卷标	<p>卷的描述性名称能够在不同节点上安装卷时唯一标识它。</p> <p>使用 <code>tuneefs.ocfs2</code> 实用程序根据需要修改该卷标。</p>
群集大小	<p>群集大小是分配给文件以保存数据的最小空间单元。</p> <p>选项是 4、8、16、32、64、128、256、512 和 1024 KB。格式化卷后不能再修改群集大小了。</p> <p>Oracle 建议数据库卷的群集大小是 128 KB 或更大。Oracle 还建议 Oracle Home 的群集大小是 32 或 64 KB。</p>
节点槽的号码	<p>可以同时安装卷的最大节点数。在装入时，OCFS2 为每个节点创建不同的系统文件，如日志。访问卷的节点可以是小尾端结构（如 x86 x86-64 和 ia64）和大尾端结构（如 ppc64 和 s390x)的组合。</p> <p>特定于节点的文件作为本地文件。节点槽号附加到该本地文件。例如：journal:0000 属于任何槽号为 0 的节点。</p> <p>当您创建卷时，要根据您希望同时安装卷的节点数，设置每个卷的最大节点槽号。使用 <code>tuneefs.ocfs2</code> 实用程序根据需要增加节点槽号；该值不能减少。</p>
块大小	<p>文件系统可寻址的最小空间单元创建卷时请指定块大小。</p> <p>选项有 512 字节（不建议使用）、1 KB、2 KB 或 4 KB（对大多数卷建议使用）。格式化卷后不能再修改块大小了。</p>

## 14.7 装入 OCFS2 卷

- 1 打开终端窗口并以 root 用户身份登录。
- 2 如果 O2CB 群集服务是脱机的，则输入以下命令启动它，并等待返回 *OK* 状态的过程。

```
/etc/init.d/o2cb online ocfs2
```

用 OCFS2 群集的实际名称替换 *ocfs2*。

OCFS2 群集必须是联机的，因为格式化操作必须确保群集中的任何节点上没有装入卷。

- 3 使用以下某个方法装入卷。
  - 在 *ocfs2console* 中，选择可用设备列表中的一个设备，然后单击装入。可以选择指定目录装入点和装入选项，然后单击确定。
  - 使用 *mount* 命令从命令行装入卷。
  - 在系统引导时，会从 */etc/fstab* 文件装入该卷。

装入 OCFS2 卷需要 5 分钟时间，这取决于检测信号线程稳定下来的时间长短。成功安装后，*ocfs2console* 中的设备列表显示装入点和设备。

---

### 提示：添加新节点

当新节点尝试连接到群集时，不允许其连接，因为这些节点还未添加到其连接列表中。要解决此问题，手动进入每个节点，发出以下命令以更新相应的连接列表。

```
o2cb_ctl -H -n ocfs2 -t cluster -a online=yes
```

---

有关使用这些方法装入 OCFS2 卷的信息，请参见 OCFS2 project at Oracle [<http://oss.oracle.com/projects/ocfs2/>]（Oracle 上的 OCFS2 项目）处的 *OCFS2 User Guide* [<http://oss.oracle.com/projects/ocfs2/documentation/>]（OCFS2 用户指南）。

运行 Oracle RAC 时，确保为 OCFS2 卷使用了 `datavolume` 和 `nointr` 装入选项，该卷包含 Voting 磁盘文件（CRS）、群集注册表（OCR）、数据文件、重做日志和控制文件。装入 Oracle Home 卷时不要使用这些选项。

选项	描述
<code>datavolume</code>	确保 Oracle 进程打开具有 <code>o_direct</code> 标志的文件。
<code>nointr</code>	没有中断。确保 IO 未被信号中断。

## 14.8 其他信息

有关使用 OCFS2 的信息，请参见 OCFS2 project at Oracle [<http://oss.oracle.com/projects/ocfs2/>]（Oracle 上的 OCFS2 项目）处的 *OCFS2 User Guide* [<http://oss.oracle.com/projects/ocfs2/documentation/>]（OCFS2 用户指南）。

# Linux 中的访问控制列表

可以将 POSIX ACL（访问控制列表）作为文件系统对象的传统权限概念的扩展来使用。利用 ACL，可以比传统权限概念更灵活地定义权限。

POSIX ACL 这一术语表明它是一种真正的 *POSIX*（可移植操作系统接口）标准。由于多种原因，相应的标准草案 POSIX 1003.1e 和 POSIX 1003.2c 已被撤销。但是，在属于 UNIX 系列的许多系统上使用的 ACL 都基于这两个草案，并且本章中介绍的文件系统 ACL 的实施也遵照这两个标准。有关它们的信息，请参见 <http://wt.xpilot.org/publications/posix.1e/>。

## 15.1 传统文件权限

中解释了传统 Linux 文件权限的基础。第 18.2 节“用户和访问权限”[328] 更多高级功能有 `setuid`、`setgid` 和粘滞位。

### 15.1.1 `setuid` 位

在某些情况下，访问权限可能过于严格。因此，Linux 另有一些设置，允许为执行特定操作临时更改当前用户和组标识。例如，`passwd` 程序通常要求拥有根权限才能访问 `/etc/passwd`。此文件包含一些重要信息，如用户主目录及用户和组 ID。因此，普通用户将无法更改 `passwd`，因为授予所有用户直接访问此文件的权限太过危险。解决该问题的一种可行方案就是 *setuid* 机制。`setuid`（设置用户 ID）是一个特殊的文件属性，它指示系统使用特定用户 ID 执行已相应标记的程序。以 `passwd` 命令为例：

```
-rwsr-xr-x 1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

您可以看见 `s`，它表示为用户许可设置了 `setuid` 位。通过设置 `setuid` 位，启动 `passwd` 命令的所有用户都以 `root` 用户身份执行该命令。

## 15.1.2 `setgid` 位

`setuid` 位适用于用户。而对组而言也有一个等价的属性：`setgid` 位。设置了此位的程序基于保存该程序的组 ID 运行，而不论是哪个用户启动了该程序。因此，在设置了 `setgid` 位的目录中，所有新建文件和子目录都被指派到该目录所属的组。请考虑下面的示例目录：

```
drwxrws--- 2 tux archive 48 Nov 19 17:12 backup
```

您可以看见 `s`，它表示为组许可设置了 `setgid` 位。目录的拥有者和组 `archive` 的成员可以访问此目录。不是该组成员的用户会“映射”到各自的组中。所有写入文件的有效组 ID 为 `archive`。例如，以组 ID `archive` 运行的备份程序即便没有根特权也能访问此目录。

## 15.1.3 粘滞位

另外还可以设置粘滞位。属于可执行程序的粘滞位和属于目录的粘滞位在作用上有所不同。如果属于某个程序，以这种方式标记的文件将被装入 RAM，而不必在每次使用时从硬盘读取。由于目前硬盘的速度已经足够快，此属性已经很少使用。如果为目录指派了此位，则可以防止用户删除彼此的文件。典型示例如 `/tmp` 目录和 `/var/tmp` 目录：

```
drwxrwxrwt 2 root root 1160 2002-11-19 17:15 /tmp
```

## 15.2 ACL 的优势

传统情况下，会为 Linux 系统上的每个文件对象定义三组权限。这三组权限包括用于每种类型用户（即文件所有者、组和其他用户这三种用户）的读(`r`)、写(`w`)和执行(`x`)许可权限。此外，还可以设置设置用户 ID、设置组 ID 和粘滞位。这种简缩概念完全适用于大多数实际情况。但对于较复杂的方案或高级应用程序，系统管理员在以前必须采用多种技巧来避开传统权限概念的限制。



可以将ACL作为传统文件权限概念的扩展来使用。它们可用于向单个用户或组分配权限，即使这些权限并不与原始拥有者或所属组相对应。访问控制列表是Linux内核的一项功能。目前，ReiserFS、Ext2、Ext3、JFS和XFS都支持访问控制列表。通过使用ACL，无需在应用程序级别实施复杂的权限模型就可以实现复杂的方案。

如果您想用Linux服务器代替Windows服务器，则ACL的优势尤为明显。即使在移植后，一些已连接的工作站仍可以继续在Windows下运行。Linux系统利用Samba向Windows客户机提供文件和打印服务。有了Samba支持访问控制列表，则既可以在Linux服务器上配置用户权限，也可以在具有图形用户界面的Windows（仅限Windows NT和更高版本）中配置用户权限。利用winbindd（samba套件的一部分），甚至可以向仅存在于Windows域中而在Linux服务器中没有任何帐户的用户分配权限。

## 15.3 定义

### 用户类别

传统的POSIX许可权限概念使用三类用户在文件系统中指派权限：拥有者、拥有的组和其他用户。可以为每个用户类别设置三个权限位，用于分配读(r)、写(w)和执行(x)权限。

### 访问 ACL

各种文件系统对象（文件和目录）的用户和组访问权限均通过访问ACL来确定。

### 默认 ACL

默认ACL只能应用于目录。它们确定文件系统对象在创建时从其父目录继承的权限。

### ACL 项

每个ACL都包含一组ACL项。ACL项中包含一个类型、一个此项所关联的用户或组的限定符和一组权限。对于某些项类型，未定义组或用户的限定符。

# 15.4 处理 ACL

**表 15.1 “ACL 项类型”** [276]总结了 ACL 项 6 种可能出现的类型，每种类型都定义了一个或一组用户的权限。拥有者项定义了拥有该文件或目录的用户的权限。所属组项定义了文件所属组的权限。超级用户可以使用 `chown` 或 `chgrp` 更改拥有者或所属组，而在这种情况下，拥有者和所属组项表示新的拥有者和所属组。每个已命名用户项定义了在该项的限定符字段中指定的用户的权限。每个已命名组项定义了在该项的限定符字段中指定的组的权限。只有已命名用户和已命名组项具有非空的限定符字段。其他项定义了所有其他用户的权限。

通过定义这些项中的有效权限和要屏蔽的权限，掩码项进一步限制了已命名用户、已命名组和所属组项授予的权限。如果权限同时存在于上述项之一和掩码中，它们就是有效的。仅包含在掩码或实际项中的权限是无效的 — 表示未授予这些权限。拥有者和所属组项中定义的所有权限始终有效。中的示例说明了这种机制。**表 15.2 “屏蔽访问权限”** [277]。

有两种基本的 ACL 类：一种是最小 ACL，仅包含用于类型拥有者、所属组和其他的项，对应于文件和目录的传统权限位。另一种是扩展 ACL，它比前一种要复杂得多。它必须包含一个掩码项，并可能包含若干已命名用户和已命名组类型的项。

**表 15.1** ACL 项类型

类型	文本形式
拥有者	<code>user::rwx</code>
已命名用户	<code>user:name:rwx</code>
所属组	<code>group::rwx</code>
已命名组	<code>group:name:rwx</code>
掩码	<code>mask::rwx</code>
其他	<code>other::rwx</code>

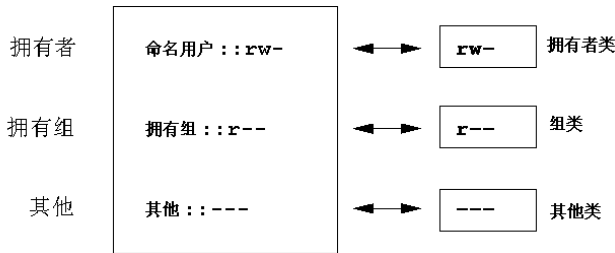
表 15.2 屏蔽访问权限

项类型	文本形式	许可权限
已命名用户	user:geeko:r-x	r-x
掩码	mask::rw-	rw-
	有效权限:	r--

15.4.1 ACL 项和文件方式权限位

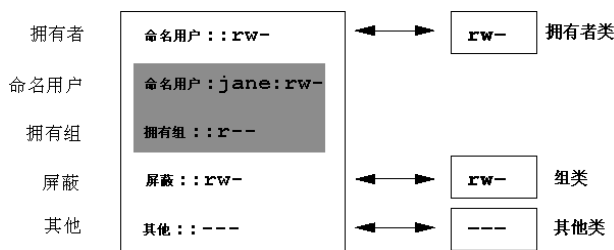
图 15.1 “最小 ACL：与许可权限位相比的 ACL 项” [277]和图 15.2 “最小 ACL：与许可权限位相比的 ACL 项” [278]说明了最小 ACL 和扩展 ACL 这两种情况。这些图分为三块：左边一块显示 ACL 项的类型规范，中间一块显示一个示例 ACL，右边一块显示对应于传统权限概念的各个权限位（如 ls-l 所显示的）。在这两种情况下，拥有者权限均被映射到 ACL 拥有者项。其他类别权限也被映射到各自的 ACL 项。但是，组类别权限的映射在这两种情况中是不同的。

图 15.1 最小 ACL：与许可权限位相比的 ACL 项



对于最小 ACL（没有屏蔽），组类别许可权限被映射到 ACL 项所属的组。中显示了这一工具。图 15.1 “最小 ACL：与许可权限位相比的 ACL 项” [277] 对于扩展 ACL（具有屏蔽），组类别许可权限被映射到屏蔽项。中显示了这一工具。图 15.2 “最小 ACL：与许可权限位相比的 ACL 项” [278]

图 15.2 最小 ACL：与许可权限位相比的 ACL 项



不管应用程序是否具有 ACL 支持，这种映射方式都可以确保应用程序的流畅交互。通过权限位方式分配的访问权限表示通过 ACL 所进行的所有其他“微调”的上限。对权限位的更改将由 ACL 反映出来，反之亦然。

## 15.4.2 具有访问 ACL 的目录

命令行上显示 `getfacl` 和 `setfacl` 的情况下，您可以访问 ACL。以下示例演示了这些命令的用法。

在创建目录之前，使用 `umask` 命令来定义每次创建文件对象时应屏蔽哪些访问权限。命令 `umask 027` 设置了默认权限，即为拥有者分配全部权限 (0)，拒绝组写访问 (2)，并且不为其他用户分配任何权限 (7)。umask 实际上屏蔽了相应的权限位或将它们关闭。有关详细信息，请参考 `umask` 手册页。

`mkdir mydir` 创建具有由 `umask` 设置的默认权限的 `mydir` 目录。使用 `ls -dl mydir` 来检查是否已正确分配所有权限。该示例的输入为：

```
drwxr-x--- ... tux project3 ... mydir
```

使用 `getfaclmydir`，检查 ACL 的初始状态。这样会得出如下信息：

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

输出的前三行显示了目录的名称、拥有者和所属组。随后三行包含三个 ACL 项，即拥有者、所属组和其他。事实上，对于最小 ACL，`getfacl` 命令不会生成您使用 `ls` 所不能获得的任何信息。

使用以下命令修改 ACL，为附加用户 `geeko` 和附加组 `mascots` 指派读、写和执行权限：

```
setfacl -m user:geeko:rx,group:mascots:rx mydir
```

选项 `-m` 提示 `setfacl` 修改现有的 ACL。以下参数指示要修改的 ACL 项（各项之间用逗号隔开）。最后部分指定了应该对其应用这些修改的目录的名称。使用 `getfacl` 命令来查看所生成的 ACL。

```
# file: mydir
# owner: tux
# group: project3
user::rx
user:geeko:rx
group::r-x
group:mascots:rx
mask::rx
other::---
```

除了为用户 `geeko` 和组 `mascots` 创建的项外，还生成了一个掩码项。系统自动设置此掩码项，以便使所有权限生效。`setfacl` 自动使现有的掩码项与已修改的设置相适应，但前提是不要用 `-n` 取消此功能。掩码为组类别中的所有项定义了最大有效访问权限。其中包括已命名用户、已命名组和所属组。由 `ls-dl mydir` 显示的组类别权限位现在与掩码项相对应。

```
drwxrwx---+ ... tux project3 ... mydir
```

输出的第一栏包含一个附加的 `+`，表明此项存在一个扩展 ACL。

根据 `ls` 命令的输出，掩码项的权限包含写访问权限。传统情况下，这样的权限位意味着所属组（这里是 `project3`）也具有对 `mydir` 目录的写访问权限。但是，所属组的有效访问权限对应于为所属组和掩码定义的权限的重叠部分——在我们的示例中是 `r-x`（参见表 15.2“屏蔽访问权限”[277]）。对本例中的所属组的有效权限而言，即使是在添加了 ACL 项之后，也未发生任何改变。

用 `setfacl` 或 `chmod` 编辑掩码项。例如，使用 `chmod g-w mydir`。`ls -dl mydir` 输出以下结果：

```
drwxr-x---+ ... tux project3 ... mydir
```

`getfaclmydir` 提供以下输出：

```
# file: mydir
# owner: tux
# group: project3
user::rx
```

```
user:geeko:rwX          # effective: r-x
group::r-x
group:mascots:rwX       # effective: r-x
mask::r-x
other::---
```

执行 `chmod` 命令将写权限从组类别位删除后，从 `ls` 命令的输出就可看出掩码位肯定已被相应地更改了：写权限再次被限制为 `mydir` 的所有者。`getfacl` 的输出证实了这一点。这个输出包含了对有效权限位与原始权限不对应的所有项的注释，因为已根据掩码项对它们进行了过滤。可以随时用 `chmod g+w mydir` 来恢复原始权限。

## 15.4.3 具有默认 ACL 的目录

目录可以具有默认 ACL，这是一种特殊的 ACL，它定义的是此目录下的对象在创建时继承的访问权限。默认 ACL 影响子目录和文件。

### 默认 ACL 的效果

将目录的默认 ACL 的权限传递到文件和子目录时，有两种方式：

- 子目录继承父目录的默认 ACL 作为其默认 ACL 和访问 ACL。
- 文件继承默认 ACL 作为其访问 ACL。

创建文件系统对象的所有系统调用都使用 `mode` 参数，该参数定义新创建的文件系统对象的访问权限。如果父目录没有默认 ACL，则从 `mode` 参数传递的权限中删除 `umask` 定义的权限位，同时将结果分配到新对象。如果父目录存在默认 ACL，则分配到新对象的权限位对应于 `mode` 参数的权限和默认 ACL 中定义的权限的重叠部分。这种情况下忽略了 `umask`。

### 默认 ACL 的应用

以下三个示例说明了目录和默认 ACL 的主要操作：

1. 将默认 ACL 添加到现有目录 `mydir`，语句为：

```
setfacl -d -m group:mascots:r-x mydir
```

setfacl 命令中的选项 -d 提示 setfacl 在默认 ACL 中执行以下修改（选项 -m）。

仔细查看此命令的结果：

```
getfacl mydir

# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other:---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other:---
```

getfacl 返回访问 ACL 和默认 ACL。默认 ACL 由以 default 开头的所有行组成。虽然您只是对 mascots 组的一个项执行 setfacl 命令来创建默认 ACL，但 setfacl 将自动复制访问 ACL 中的所有其他项来创建有效的默认 ACL。默认 ACL 对访问权限没有直接效果。它们只在创建文件系统对象时起作用。这些新对象只从其父目录的默认 ACL 中继承权限。

2. 在下一个示例中，我们将使用 mkdir 在 mydir 中创建一个子目录，它将继承默认 ACL。

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other:---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other:---
```

根据预期，新创建的子目录 `mysubdir` 具有父目录的默认 ACL 的权限。`mysubdir` 的访问 ACL 准确反映了 `mydir` 的默认 ACL。该目录将向其从属对象传递的默认 ACL 也是相同的。

3. 使用 `touch` 在 `mydir` 目录中创建一个文件，例如 `touch mydir/myfile`。  
`ls -l mydir/myfile` 输出以下结果：

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

`getfacl mydir/myfile` 的输出是：

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascots:r-x   # effective:r--
mask::r--
other::---
```

当创建新文件时，`touch` 使用值为 `0666` 的 `mode`，这意味所创建的新文件具有用于所有用户类别的读和写权限，前提是 `umask` 或默认 ACL 中不存在任何其他限制（请参见“默认 ACL 的效果”一节 [280]）。实际上，这意味着 `mode` 值中不包含的所有访问权限均将从各自的 ACL 项中删除。虽然没有从组类别的 ACL 项中删除任何权限，但仍修改了掩码项来屏蔽不在 `mode` 中设置的权限。

这种方式确保应用程序（如编译器）与 ACL 的流畅交互。您可以创建具有有限访问权限的文件，然后将其标记为可执行文件。`mask` 机制确保适当的用户和组可以在需要时执行它们。

## 15.4.4 ACL 检查算法

在为任何进程或应用程序授予访问受 ACL 保护的文件系统对象的权限之前，将应用检查算法。作为基本规则，按照以下序列检查 ACL 项：拥有者、命名用户、所属组或命名组以及其他组。访问将根据最适合进程的项进行处理。权限不能累加。

如果某个进程属于多个组并且潜在适合多个组项，情况会更为复杂。这时将从具有所需权限的合适项中随机选择一个。它与是哪些项触发了最终结果“已授权访问”无关。同样，如果合适的组项中没有包含所需的权限，则随机选择的项将触发最终结果“访问被拒绝”。



## 15.5 应用程序中的 ACL 支持

ACL 可用于实施非常复杂的权限方案以满足目前应用程序的要求。可以用一种智能方式将传统权限概念和 ACL 结合在一起。像 Samba 和 Konqueror 一样，基本的文件命令（cp、mv、ls 等）支持 ACL。

遗憾的是，许多编辑器和文件管理器仍缺少 ACL 支持。例如，当用 Emacs 复制文件时，这些文件的 ACL 会丢失。当用编辑器修改文件时，文件的 ACL 有时会被保留，有时则会丢失，这取决于所使用编辑器的备份方式。如果编辑器将更改写入原始文件，访问 ACL 就会被保留。如果编辑器将已更新的内容保存到一个新文件，然后将此文件重命名为旧文件名，则 ACL 就可能丢失，除非此编辑器支持 ACL。除了 star 存档程序外，当前没有任何其他备份应用程序保留 ACL。

## 15.6 更多信息

有关 ACL 的详细信息，请参见 <http://acl.bestbits.at/>。另请参见 `getfacl(1)`、`acl(5)` 和 `setfacl(1)` 的手册页。



## 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；重构建 RPM 数据库；查询 RPM 库或独立 RPM 存档；包的完整性检查以及签署包。`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）。可以通过名称扩展 `-devel` 确定这些开发包，例如包 `alsa-devel`、`gimp-devel` 和 `kdelibs3-devel`。

---

## 16.1 校验包真实性

RPM 包具有 GnuPG 签名。包括指纹的密钥是：

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>  
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

命令 `rpm --checksig package-1.2.3.rpm` 可用于校验 RPM 包的签名，从而确定它确实来自 SUSE 还是其他可信工具。特别建议对来自因特网的更新包使用此命令。SUSE 公共包签名密钥通常驻留在 `/root/.gnupg/` 中。该密钥还位于目录 `/usr/lib/rpm/gnupg/` 中，允许一般用户校验 RPM 包的签名。

## 16.2 管理包：安装、更新和卸载

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`（即 `--upgrade`）和 `-F`（即 `--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。
- 如果更新前配置文件已被系统管理员更改，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` 是从旧系统格式更新为 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` 只在依赖性问题都解决的情况下才会删除该包。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。如果出于任何原因或在任何特殊情况下不能进行这一删除操作（即使不存在任何其他依赖性），则最好使用 `--rebuilddb` 选项重建 RPM 数据库。

## 16.3 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。这样，对只有小文件中存在错误的较大的包进行替换时就很容易产生大量数据。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描述：

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）。

## 16.4 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** 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"。

## 16.5 RPM 查询

使用 -q 选项，rpm 将初始化查询，使查看 RPM 存档（通过添加选项 -p）并查询已安装包的 RPM 数据库成为可能。可以使用多个开关指定所需信息的类型。请参见表 16.1 “最重要的 RPM 查询选项” [289]。

**表 16.1** 最重要的 RPM 查询选项

-i	包信息
-l	文件列表
-f FILE	查询包含文件 <i>FILE</i> 的包（必须使用 <i>FILE</i> 指定完整路径）
-s	带有状态信息的文件列表（间接指定 -l）

<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 16.1 “`rpm -q -i wget`” [290] 中所示的信息。

### 例 16.1 `rpm -q -i wget`

```

Name           : wget                               Relocations: (not relocatable)
Version        : 1.9.1                             Vendor: SUSE LINUX AG,
Nuernberg, Germany
Release        : 50                                Build Date: Sat 02 Oct 2004
03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group          : Productivity/Networking/Web/Utilities Source RPM:
wget-1.9.1-50.src.rpm
Size           : 1637514                             License: GPL
Signature      : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID
a84edae89c800aca
Packager       : http://www.suse.de/feedback
URL            : http://wget.sunsite.dk/
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-4.1.1-191  
wget-1.9.1-50

如果只知道部分文件名，则可以使用壳层脚本，如例 16.2 “搜索包的脚本” [291] 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 16.2 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 按照日期显示有关特定包更改信息的详细列表。此示例显示有关包 rpm 的信息。

借助已安装的 RPM 数据库，可以进行校验检查。使用 -v、-y 或 --verify 对其进行初始化。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 16.2 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	所有者
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) 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_RPMDB_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。

## 16.6 安装和编译源包

所有源包都带有 `.src.rpm` 扩展名（源 RPM）。

---

### 提示

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/rpmsrc` 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

在此目录中解包、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

不要对系统部件（`glibc`、`rpm`、`sysvinit` 等）进行试验，因为这将会影响系统的可操作性。

---

下面的示例使用 `wget.src.rpm` 包。在使用 YaST 安装此包之后，您应该具有与以下所列相似的文件：

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
/usr/src/packages/SOURCES/wget-wrong_charset.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。

## 16.7 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，它将创建构建包的确定环境。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（如上面的示例中），请以 root 用户的身份使用以下命令：

```
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。

## 16.8 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。

KDE 提供 kpackage 工具，作为 rpm 的前端。还提供作为 YaST 模块的功能齐全的包管理器（请参见 [第 8.3.1 节“安装和删除软件”](#) [119]）。



## 系统监视实用程序

一些程序和机制（在此对其中的某些进行了介绍）同时介绍了可用于日常工作的一些实用程序，以及它们最重要的参数。

对于所介绍的每个命令，都将提供相关输出的示例。在这些示例中，第一行是命令本身（在>或#符号提示后）。使用方括号([...])表示省略，必要时对较长的行进行换行。较长的行的换行符由反斜线(\)表示。

```
# command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

这里尽量缩短对每个实用程序的说明，从而介绍尽量多的实用程序。手册页中提供了所有命令的详细信息。大多数命令还接受参数--help，该参数将生成可能参数的简要列表。

### 17.1 调试

#### 17.1.1 指定必需的库：ldd

使用命令 ldd 查找出哪些库将装载指定为参数的动态可执行文件。

```
tux@mercury:~> ldd /bin/ls
linux-gate.so.1 => (0xfffffe000)
librt.so.1 => /lib/librt.so.1 (0xb7f97000)
libacl.so.1 => /lib/libacl.so.1 (0xb7f91000)
libc.so.6 => /lib/libc.so.6 (0xb7e79000)
libpthread.so.0 => /lib/libpthread.so.0 (0xb7e67000)
/lib/ld-linux.so.2 (0xb7fb6000)
libattr.so.1 => /lib/libattr.so.1 (0xb7e63000)
```

静态二进制文件不需要任何动态库。

```
tux@mercury:~> ldd /bin/sash
not a dynamic executable
tux@mercury:~> file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for
GNU/Linux 2.6.4, statically linked, for GNU/Linux 2.6.4, stripped
```

## 17.1.2 程序运行的库调用：ltrace

命令 `ltrace` 使您可以跟踪进程的库调用。此命令的使用方式与 `strace` 类似。参数 `-c` 输出所发生的库调用的次数和持续时间：

```
tux@mercury:~> ltrace -c find ~
% time      seconds    usecs/call      calls      function
-----
 34.37      6.758937          245      27554    __errno_location
 33.53      6.593562          788      8358     __fprintf_chk
 12.67      2.490392          144     17212    strlen
 11.97      2.353302          239      9845    readdir64
  2.37      0.466754           27     16716    __ctype_get_mb_cur_max
  1.17      0.230765           27      8358    memcpy
[...]
```

% time	seconds	usecs/call	calls	function
0.00	0.000036	36	1	textdomain
100.00	19.662715		105717	total

## 17.1.3 程序运行的系统调用：strace

实用程序 `strace` 使您可以跟踪当前运行的进程的所有系统调用。以正常方式输入命令，在行开头添加 `strace`：

```
tux@mercury:~> strace ls
execve("/bin/ls", ["ls"], [/ * 61 vars *]) = 0
uname({sys="Linux", node="mercury", ...}) = 0
brk(0) = 0x805c000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or \
directory)
```



```

open("/etc/ld.so.cache", O_RDONLY)          = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=89696, ...}) = 0
mmap2(NULL, 89696, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb7ef2000
close(3)                                     = 0
open("/lib/librt.so.1", O_RDONLY)           = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\000\36\0"... , 512) \
    = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=36659, ...}) = 0
[...]
stat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
    = 0xb7ca7000
write(1, "bin Desktop Documents music\tM"... , 55bin Desktop Documents \
    \ music      Music public_html tmp
) = 55
close(1)                                     = 0
munmap(0xb7ca7000, 4096)                    = 0
exit_group(0)                              = ?

```

例如，要跟踪打开特定文件的所有尝试，请使用以下命令：

```

tux@mercury:~> strace -e open ls .bashrc
open("/etc/ld.so.cache", O_RDONLY)          = 3
open("/lib/librt.so.1", O_RDONLY)           = 3
open("/lib/libacl.so.1", O_RDONLY)          = 3
open("/lib/libc.so.6", O_RDONLY)            = 3
open("/lib/libpthread.so.0", O_RDONLY)      = 3
open("/lib/libattr.so.1", O_RDONLY)         = 3
[...]

```

要跟踪所有子进程，请使用参数 `-f`。可以在很大程度上控制 `strace` 的行为和输出格式。有关信息，请参见 `man strace`。

## 17.2 文件和文件系统

### 17.2.1 确定文件类型：file

命令 `file` 可通过检查 `/etc/magic` 而确定一个文件或一个文件列表的类型。

```

tux@mercury:~> file /usr/bin/file
/usr/bin/file: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
    for GNU/Linux 2.2.5, dynamically linked (uses shared libs), stripped

```

参数 `-f` 列表指定带有要检查的文件名的列表的文件。 `-z` 允许 `file` 查看压缩文件的内部：

```
tux@mercury:~> file /usr/share/man/man1/file.1.gz
usr/share/man/man1/file.1.gz: gzip compressed data, from Unix, max compression
tux@mercury:~> file -z /usr/share/man/man1/file.1.gz
/usr/share/man/man1/file.1.gz: ASCII troff or preprocessor input text \
(gzip compressed data, from Unix, max compression)
```

## 17.2.2 文件系统和它们的使用：mount、df 和 du

命令 `mount` 显示在哪个装入点装入哪个文件系统（设备和类型）：

```
tux@mercury:~> mount
/dev/sda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/sda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/sda4 on /local type reiserfs (rw,acl,user_xattr)
/dev/fd0 on /media/floppy type subfs (rw,nosuid,nodev,noatime,fs=floppyfs,p
```

使用命令 `df` 可以获得有关文件系统全部使用情况的信息。参数 `-h`（或 `--human-readable`）将输出转换为普通用户可以理解的形式。

```
tux@mercury:~> df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        11G   3.2G   6.9G   32% /
udev             252M   104K   252M    1% /dev
/dev/sda1         16M    6.6M    7.8M   46% /boot
/dev/sda4        27G    34M    27G    1% /local
```

使用命令 `du` 可以显示给定目录及其子目录中所有文件的总大小。使用参数 `-s` 将不输出详细信息。`-h` 再次将数据转化为人可读的格式：

```
tux@mercury:~> du -sh /local
1.7M    /local
```

## 17.2.3 有关 ELF 二进制文件的其他信息

用 `readelf` 实用程序来读取二进制文件的内容。这甚至可用于为其他硬件体系结构生成的 ELF 文件：

```
tux@mercury:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
```

```

Class: ELF32
Data: 2's complement, little endian
Version: 1 (current)
OS/ABI: UNIX - System V
ABI Version: 0
Type: EXEC (Executable file)
Machine: Intel 80386
Version: 0x1
Entry point address: 0x8049b60
Start of program headers: 52 (bytes into file)
Start of section headers: 81112 (bytes into file)
Flags: 0x0
Size of this header: 52 (bytes)
Size of program headers: 32 (bytes)
Number of program headers: 9
Size of section headers: 40 (bytes)
Number of section headers: 30
Section header string table index: 29

```

## 17.2.4 文件属性：stat

命令 stat 显示文件属性：

```

tux@mercury:~> stat /etc/profile
  File: `/etc/profile'
  Size: 8080          Blocks: 16          IO Block: 4096   regular file
Device: 806h/2054d   Inode: 64942        Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/   root)   Gid: (    0/   root)
Access: 2007-07-16 23:28:18.000000000 +0200
Modify: 2006-09-19 14:45:01.000000000 +0200
Change: 2006-12-05 14:54:55.000000000 +0100

```

参数 --filesystem 将生成指定文件所在文件系统的属性详细信息：

```

tux@mercury:~> stat /etc/profile --filesystem
  File: "/etc/profile"
    ID: 0          Namelen: 255          Type: reiserfs
Block size: 4096      Fundamental block size: 4096
Blocks: Total: 2622526   Free: 1809771    Available: 1809771
Inodes: Total: 0        Free: 0

```

## 17.3 硬件信息

### 17.3.1 PCI 资源：lspci

命令 `lspci` 列出 PCI 资源：

```
mercury:~ # lspci
00:00.0 Host bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    DRAM Controller/Host-Hub Interface (rev 01)
00:01.0 PCI bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    Host-to-AGP Bridge (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801DB/DBM \
    (ICH4/ICH4-M) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 81)
00:1f.0 ISA bridge: Intel Corporation 82801DB/DBL (ICH4/ICH4-L) \
    LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801DB (ICH4) IDE \
    Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801DB/DBL/DBM (ICH4/ICH4-L/ICH4-M) \
    SMBus Controller (rev 01)
00:1f.5 Multimedia audio controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) AC'97 Audio Controller (rev 01)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. G400/G450 (rev 85)
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM) \
    Ethernet Controller (rev 81)
```

使用 `-v` 可以生成更加详细的列表：

```
mercury:~ # lspci
[...]
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM)\
    Ethernet Controller (rev 81)
    Subsystem: Fujitsu Siemens Computer GmbH: Unknown device 1001
    Flags: bus master, medium devsel, latency 66, IRQ 11
    Memory at d1000000 (32-bit, non-prefetchable) [size=4K]
    I/O ports at 3000 [size=64]
    Capabilities: [dc] Power Management version 2
```

从文件 `/usr/share/pci.ids` 中获取有关设备名称解析的信息。此文件中未列出的 PCI ID 标有“未知设备”。

参数 `-vv` 生成程序可查询的所有信息。要查看纯数字值，请使用参数 `-n`。

## 17.3.2 USB 设备：lsusb

`lsusb` 命令可列出所有 USB 设备。使用 `-v` 选项，可打印更加详细的列表。详细信息从目录 `/proc/bus/usb/` 中读取。以下是连有 USB 设备集线器、内存条、硬盘和鼠标的 `lsusb` 的输出。

```
mercury:/ # lsusb
Bus 004 Device 007: ID 0ea0:2168 Ours Technology, Inc. Transcend JetFlash \
    2.0 / Astone USB Drive
Bus 004 Device 006: ID 04b4:6830 Cypress Semiconductor Corp. USB-2.0 IDE \
    Adapter
Bus 004 Device 005: ID 05e3:0605 Genesys Logic, Inc.
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 005: ID 046d:c012 Logitech, Inc. Optical Mouse
Bus 001 Device 001: ID 0000:0000
```

## 17.3.3 关于 SCSI 设备的信息：scsiinfo

`scsiinfo` 命令可列出关于 SCSI 设备的信息。使用选项 `-l`，可列出系统已知的所有 SCSI 设备（通过 `lsscsi` 命令可获取类似的信息）。下面是 `scsiinfo -i /dev/sda` 的输出，它提供关于一个硬盘的信息。选项 `-a` 可提供更加详细的信息。

```
mercury:/ # scsiinfo -i /dev/sda
Inquiry command
-----
Relative Address          0
Wide bus 32               0
Wide bus 16               1
Synchronous neg.         1
Linked Commands           1
Command Queueing         1
SftRe                     0
Device Type               0
Peripheral Qualifier      0
Removable?                0
Device Type Modifier      0
ISO Version               0
ECMA Version              0
ANSI Version              3
AENC                      0
```

```
TrmIOP                                0
Response Data Format                    2
Vendor:                                FUJITSU
Product:                                MAS3367NP
Revision level:                         0104A0K7P43002BE
```

该选项 `-d` 可产生缺陷列表，带有两个硬盘坏区表：第一个是供应商提供的（制造商表），第二个是操作中显示的坏区列表（增长表）。如果增长表中的项目数增加，则最好更换硬盘。

## 17.4 联网

### 17.4.1 显示网络状态：netstat

`netstat` 显示的是网络连接、路由表 (`-r`)、接口 (`-i`)、伪装连接 (`-M`)、多点广播成员 (`-g`) 和统计信息 (`-s`)。

```
tux@mercury:~> netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
192.168.2.0      *                255.255.254.0   U        0  0        0 eth0
link-local       *                255.255.0.0     U        0  0        0 eth0
loopback         *                255.0.0.0       U        0  0        0 lo
default          192.168.2.254   0.0.0.0         UG       0  0        0 eth0
```

```
tux@mercury:~> netstat -i
Kernel Interface table
Iface  MTU Met  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0   1500  0  1624507 129056      0      0   7055      0      0      0 BMNRU
lo     16436  0   23728      0      0      0  23728      0      0      0 LRU
```

显示网络连接或统计数据时，可指定要显示的套接字类型：`TCP` (`-t`)、`UDP` (`-u`) 或 `raw` (`-r`)。 `-p` 选项显示套接字所属程序的 `PID` 和名称。

下例列出了所有 `TCP` 连接和使用这些连接的程序。

```
mercury:~ # netstat -t -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address State      PID/Pro

tcp      0      0 mercury:33513   www.novell.com:www-http ESTABLISHED 6862/fi
tcp      0      352 mercury:ssh     mercury2.:trc-netpoll ESTABLISHED
19422/s
tcp      0      0 localhost:ssh   localhost:17828 ESTABLISHED -
```

下面，显示 TCP 协议的统计信息：

```
tux@mercury:~> netstat -s -t
Tcp:
  2427 active connections openings
  2374 passive connection openings
  0 failed connection attempts
  0 connection resets received
  1 connections established
  27476 segments received
  26786 segments send out
  54 segments retransmitted
  0 bad segments received.
  6 resets sent
[...]
TCPAbortOnLinger: 0
TCPAbortFailed: 0
TCPMemoryPressures: 0
```

## 17.5 /proc 文件系统

/proc 文件系统是一个伪文件系统，在该文件系统中，内核以虚拟文件的形式保留重要信息。例如，使用以下命令显示 CPU 类型：

```
tux@mercury:~> cat /proc/cpuinfo
processor       : 0
vendor_id      : AuthenticAMD
cpu family     : 6
model          : 8
model name     : AMD Athlon(tm) XP 2400+
stepping       : 1
cpu MHz        : 2009.343
cache size     : 256 KB
fdiv_bug       : no
[...]
```

用下列命令查询中断的分配和使用：

```
tux@mercury:~> cat /proc/interrupts
CPU0
0:   3577519      XT-PIC  timer
1:       130      XT-PIC  i8042
2:         0      XT-PIC  cascade
5:   564535      XT-PIC  Intel 82801DB-ICH4
7:         1      XT-PIC  parport0
8:         2      XT-PIC  rtc
9:         1      XT-PIC  acpi, uhci_hcd:usb1, ehci_hcd:usb4
10:        0      XT-PIC  uhci_hcd:usb3
11:    71772      XT-PIC  uhci_hcd:usb2, eth0
```

```

12:      101150      XT-PIC  i8042
14:       33146      XT-PIC  ide0
15:     149202      XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0

```

一些重要的文件及其内容如下：

```

/proc/devices
    可用设备

```

```

/proc/modules
    装载的内核模块

```

```

/proc/cmdline
    内核命令行

```

```

/proc/meminfo
    有关内存使用的详细信息

```

```

/proc/config.gz
    当前运行的内核的 gzip 压缩配置文件

```

文本文件 `/usr/src/linux/Documentation/filesystems/proc.txt` 中提供了详细信息。在 `/proc/NNN` 目录中提供了当前运行进程的信息，其中 `NNN` 是相关进程的进程 ID (PID)。每个进程都可以在 `/proc/self/` 中找到它自己的属性：

```

tux@mercury:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2007-07-16 13:03 /proc/self -> 5356
tux@mercury:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tux users 0 2007-07-16 17:04 attr
-r----- 1 tux users 0 2007-07-16 17:04 auxv
-r--r--r-- 1 tux users 0 2007-07-16 17:04 cmdline
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 cwd -> /home/tux
-r----- 1 tux users 0 2007-07-16 17:04 environ
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 exe -> /bin/ls
dr-x----- 2 tux users 0 2007-07-16 17:04 fd
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 loginuid
-r--r--r-- 1 tux users 0 2007-07-16 17:04 maps
-rw----- 1 tux users 0 2007-07-16 17:04 mem
-r--r--r-- 1 tux users 0 2007-07-16 17:04 mounts
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 oom_adj

```



```

-r--r--r-- 1 tux users 0 2007-07-16 17:04 oom_score
lwxrwxrwx 1 tux users 0 2007-07-16 17:04 root -> /
-rw----- 1 tux users 0 2007-07-16 17:04 seccomp
-r--r--r-- 1 tux users 0 2007-07-16 17:04 smaps
-r--r--r-- 1 tux users 0 2007-07-16 17:04 stat
[...]
dr-xr-xr-x 3 tux users 0 2007-07-16 17:04 task
-r--r--r-- 1 tux users 0 2007-07-16 17:04 wchan

```

maps文件中包含可执行文件和库的地址指派:

```

tux@mercury:~> cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:03 17753      /bin/cat
0804c000-0804d000 rw-p 00004000 03:03 17753      /bin/cat
0804d000-0806e000 rw-p 0804d000 00:00 0          [heap]
b7d27000-b7d5a000 r--p 00000000 03:03 11867      /usr/lib/locale/en_GB.utf8/
b7d5a000-b7e32000 r--p 00000000 03:03 11868      /usr/lib/locale/en_GB.utf8/
b7e32000-b7e33000 rw-p b7e32000 00:00 0
b7e33000-b7f45000 r-xp 00000000 03:03 8837        /lib/libc-2.3.6.so
b7f45000-b7f46000 r--p 00112000 03:03 8837        /lib/libc-2.3.6.so
b7f46000-b7f48000 rw-p 00113000 03:03 8837        /lib/libc-2.3.6.so
b7f48000-b7f4c000 rw-p b7f48000 00:00 0
b7f52000-b7f53000 r--p 00000000 03:03 11842      /usr/lib/locale/en_GB.utf8/
[...]
b7f5b000-b7f61000 r--s 00000000 03:03 9109        /usr/lib/gconv/gconv-module
b7f61000-b7f62000 r--p 00000000 03:03 9720        /usr/lib/locale/en_GB.utf8/
b7f62000-b7f76000 r-xp 00000000 03:03 8828        /lib/ld-2.3.6.so
b7f76000-b7f78000 rw-p 00013000 03:03 8828        /lib/ld-2.3.6.so
bfd61000-bfd76000 rw-p bfd61000 00:00 0          [stack]
ffffe000-fffff000 ---p 00000000 00:00 0          [vdso]

```

## 17.5.1 procinfo

命令 procinfo 对 /proc 文件系统中的重要信息进行了总结:

```

tux@mercury:~> procinfo
Linux 2.6.18.8-0.5-default (geeko@buildhost) (gcc 4.1.2 20061115) #1 2CPU

Memory:      Total      Used      Free      Shared      Buffers
Mem:         2060604    2011264    49340      0          200664
Swap:        2104472      112      2104360

Bootup: Tue Jul 10 10:29:15 2007      Load average: 0.86 1.10 1.11 3/118 21547

user   :      2:43:13.78    0.8%  page in :      71099181  disk 1:  2827023r 968
nice   :    1d 22:21:27.87  14.7%  page out:  690734737
system:    13:39:57.57    4.3%  page act:  138388345
IOwait:    18:02:18.59    5.7%  page dea:  29639529
hw irq:      0:03:39.44    0.0%  page flt: 9539791626
sw irq:      1:15:35.25    0.4%  swap in :           69

```

```

idle   :    9d 16:07:56.79   73.8%  swap out:           209
uptime:    6d 13:07:11.14      context :   542720687

irq  0: 141399308 timer           irq 14:  5074312 ide0
irq  1:    73784 i8042           irq 50: 1938076 uhci_hcd:usb1, ehci_
irq  4:         2                irq 58:         0 uhci_hcd:usb2
irq  6:         5 floppy [2]      irq 66:  872711 uhci_hcd:usb3, HDA I
irq  7:         2                irq 74:         15 uhci_hcd:usb4
irq  8:         0 rtc            irq 82: 178717720 0          PCI-MSI  e
irq  9:         0 acpi          irq169: 44352794 nvidia
irq 12:         3                irq233:  8209068 0          PCI-MSI  1

```

要查看所有信息，请使用参数 `-a`。参数 `-nN` 每 *N* 秒更新一次信息。在这种情况下，按 `Q` 键终止程序。

默认情况下显示累积值。使用参数 `-d` 将生成差异值。`procinfo -dn5` 显示最近 5 秒内更改的值：

## 17.6 进程

### 17.6.1 进程间通讯：ipcs

命令 `ipcs` 生成当前正在使用的 IPC 资源的列表：

```

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes      nattch     status
0x00000000   58261504   tux        600         393216      2          dest
0x00000000   58294273   tux        600         196608      2          dest
0x00000000   83886083   tux        666         43264       2
0x00000000   83951622   tux        666         192000      2
0x00000000   83984391   tux        666         282464      2
0x00000000   84738056   root       644         151552      2          dest

----- Semaphore Arrays -----
key          semid      owner      perms      nsems
0x4d038abf   0          tux        600         8

----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

```

## 17.6.2 进程列表：ps

命令 `ps` 生成进程的列表。书写大多数参数时一定不能带减号。请参考 `ps --help` 可获得简要帮助或者参考主页获得详细帮助。

使用 `ps axu` 列出所有进程以及用户和命令行信息：

```
tux@mercury:~> ps axu
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   696   272 ?        S    12:59   0:01 init [5]
root        2  0.0  0.0     0     0 ?        SN   12:59   0:00 [ksoftirqd
root        3  0.0  0.0     0     0 ?        S<   12:59   0:00 [events]
[...]
tux       4047  0.0  6.0 158548 31400 ?        Ssl  13:02   0:06 mono-best
tux       4057  0.0  0.7   9036  3684 ?        Sl   13:02   0:00 /opt/gnome
tux       4067  0.0  0.1   2204   636 ?        S    13:02   0:00 /opt/gnome
tux       4072  0.0  1.0  15996  5160 ?        Ss   13:02   0:00 gnome-scre
tux       4114  0.0  3.7 130988 19172 ?        SLl  13:06   0:04 sound-juic
tux       4818  0.0  0.3   4192  1812 pts/0    Ss   15:59   0:00 -bash
tux       4959  0.0  0.1   2324   816 pts/0    R+   16:17   0:00 ps axu
```

要检查有多少个 `sshd` 进程正在运行，请将选项 `-p` 与命令 `pidof` 一起使用，这将列出给定进程的进程 ID。

```
tux@mercury:~> ps -p `pidof sshd`
  PID TTY          STAT TIME  COMMAND
 3524 ?           Ss    0:00 /usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid
 4813 ?           Ss    0:00 sshd: tux [priv]
 4817 ?           R     0:00 sshd: tux@pts/0
```

可以根据需要设置进程列表的格式。选项 `-L` 返回所有关键字的列表。输入以下命令可以生成所有进程按内存使用量排序的列表：

```
tux@mercury:~> ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2     0 [ksoftirqd/0]
    3     0 [events/0]
    4     0 [khelper]
    5     0 [kthread]
   11     0 [kblockd/0]
   12     0 [kacpid]
   472     0 [pdflush]
   473     0 [pdflush]
[...]
 4028 17556 nautilus --no-default-window --sm-client-id default2
 4118 17800 ksnapshot
 4114 19172 sound-juicer
 4023 25144 gnome-panel --sm-client-id default1
```

```
4047 31400 mono-best --debug /usr/lib/beagle/Best.exe --autostarted
3973 31520 mono-beagled --debug /usr/lib/beagle/BeagleDaemon.exe --bg --aut
```

## 17.6.3 进程树：pstree

命令 `pstree` 生成树结构的进程列表：

```
tux@mercury:~> pstree
init--+-NetworkManagerD
      |-acpid
      |-3*[automount]
      |-cron
      |-cupsd
      |-2*[dbus-daemon]
      |-dbus-launch
      |-dcopserver
      |-dhcpcd
      |-events/0
      |-gpg-agent
      |-hald-+-hald-addon-acpi
      |     `--hald-addon-stor
      |-kded
      |-kdeinit-+-kdesu---su---kdesu_stub---yast2---y2controlcenter
      |         |-kio_file
      |         |-klaucher
      |         |-konqueror
      |         |-konsole-+-bash---su---bash
      |         |         `--bash
      |         `--kwin
      |-kdesktop---kdesktop_lock---xmatrix
      |-kdesud
      |-kdm-+-X
      |     `--kdm---startkde---kwrapper
      [...]
[...]
```

参数 `-p` 将进程 ID 添加到给定的名称。要让命令行也显示出来，请使用 `-a` 参数：

## 17.6.4 进程：top

`top` 命令（代表“进程表”）可显示进程的列表，该列表每两秒钟刷新一次。要终止程序，请按 `Q` 键。参数 `-n 1` 在显示一次进程列表后终止程序。下面是 `top -n 1` 命令的示例输出：

```
tux@mercury:~> top -n 1
top - 17:06:28 up 2:10, 5 users, load average: 0.00, 0.00, 0.00
Tasks: 85 total, 1 running, 83 sleeping, 1 stopped, 0 zombie
Cpu(s): 5.5% us, 0.8% sy, 0.8% ni, 91.9% id, 1.0% wa, 0.0% hi, 0.0% si
Mem: 515584k total, 506468k used, 9116k free, 66324k buffers
Swap: 658656k total, 0k used, 658656k free, 353328k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	16	0	700	272	236	S	0.0	0.1	0:01.33	init
2	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
3	root	10	-5	0	0	0	S	0.0	0.0	0:00.27	events/0
4	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	khelper
5	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	kthread
11	root	10	-5	0	0	0	S	0.0	0.0	0:00.05	kblockd/0
12	root	20	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
472	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pdflush
473	root	15	0	0	0	0	S	0.0	0.0	0:00.06	pdflush
475	root	11	-5	0	0	0	S	0.0	0.0	0:00.00	aio/0
474	root	15	0	0	0	0	S	0.0	0.0	0:00.07	kswapd0
681	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	kseriod
839	root	10	-5	0	0	0	S	0.0	0.0	0:00.02	reiserfs/0
923	root	13	-4	1712	552	344	S	0.0	0.1	0:00.67	udevd
1343	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	khubb
1587	root	20	0	0	0	0	S	0.0	0.0	0:00.00	shpchpd_event
1746	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_control
1752	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_bus_master1
2151	root	16	0	1464	496	416	S	0.0	0.1	0:00.00	acpid
2165	messageb	16	0	3340	1048	792	S	0.0	0.2	0:00.64	dbus-daemon
2166	root	15	0	1840	752	556	S	0.0	0.1	0:00.01	syslog-ng
2171	root	16	0	1600	516	320	S	0.0	0.1	0:00.00	klogd
2235	root	15	0	1736	800	652	S	0.0	0.2	0:00.10	resmgrd
2289	root	16	0	4192	2852	1444	S	0.0	0.6	0:02.05	hald
2403	root	23	0	1756	600	524	S	0.0	0.1	0:00.00	hald-addon-acpi
2709	root	19	0	2668	1076	944	S	0.0	0.2	0:00.00	NetworkManagerD
2714	root	16	0	1756	648	564	S	0.0	0.1	0:00.56	hald-addon-stor

如果当 `top` 正在运行时按 **F** 键，则将打开一个菜单，使用该菜单可以对输出的格式进行全面更改。

参数 `-U UID` 只监视与特定用户关联的进程。将 `UID` 替换为用户 **ID**。`top -u `Id -u`` 基于用户名返回用户 **UID**，并显示他的进程。

## 17.7 系统信息

### 17.7.1 系统活动信息：sar

要使用 `sar`，需要运行 `sadc`（系统活动数据收集程序）。使用 `rcsysstat` `\{start|status\}` 检查其状态或启动它。

`sar` 可以生成关于几乎所有重要的系统活动的各种报告，其中包括 CPU、内存、IRQ 使用率、IO 或联网。对于这许多选项，要在这进行进一步的解释是非常复杂的。请参见各种文档中的参考手册页上的例子。

### 17.7.2 内存使用：free

实用程序 `free` 检查 RAM 使用情况。将显示有关可用内存和已使用内存以及交换区域的详细信息：

```
tux@mercury:~> free
```

	total	used	free	shared	buffers	cached
Mem:	515584	501704	13880	0	73040	334592
-/+ buffers/cache:		94072	421512			
Swap:	658656	0	658656			

选项 `-b`、`-k`、`-m` 和 `-g` 分别以字节、KB、MB 或 GB 为单位显示输出。参数 `-d delay` 可以确保显示每 `delay` 秒刷新一次。例如，`free -d 1.5` 每 1.5 秒进行一次更新。

### 17.7.3 访问文件的用户：fuser

它可用于确定当前哪些进程或用户正在访问特定的文件。例如，假定您需要卸装已装入 `/mnt` 的文件系统。`umount` 返回“设备正忙”。然后可使用 `fuser` 命令确定哪些进程正在访问该设备：

```
tux@mercury:~> fuser -v /mnt/*
```

	USER	PID	ACCESS	COMMAND
/mnt/notes.txt	tux	26597	f....	less

在终止 `less` 进程之后（该进程在另一个终端上运行），便可以成功卸装该文件系统了。

## 17.7.4 内核信号缓冲区：dmesg

Linux 内核在信号缓冲区中保存某些消息。要查看这些消息，请输入命令 `dmesg`：

```
$ dmesg
[...]  
end_request: I/O error, dev fd0, sector 0  
subfs: unsuccessful attempt to mount media (256)  
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex  
NET: Registered protocol family 17  
IA-32 Microcode Update Driver: v1.14 <tigran@veritas.com>  
microcode: CPU0 updated from revision 0xe to 0x2e, date = 08112004  
IA-32 Microcode Update Driver v1.14 unregistered  
boot splash: status on console 0 changed to on  
NET: Registered protocol family 10  
Disabled Privacy Extensions on device c0326ea0(lo)  
IPv6 over IPv4 tunneling driver  
powernow: This module only works with AMD K7 CPUs  
boot splash: status on console 0 changed to on
```

以前的事件记录在文件 `/var/log/messages` 和 `/var/log/warn` 中。

## 17.7.5 打开的文件的列表：lsdf

要查看为具有进程 ID `PID` 的进程打开的所有文件的列表，请使用 `-p`。例如，要查看当前 `shell` 使用的所有文件，请输入：

```
tux@mercury:~> lsdf -p $$  
COMMAND  PID    USER  FD   TYPE DEVICE        SIZE  NODE NAME  
bash     5552  tux   cwd   DIR    3,3      1512 117619 /home/tux  
bash     5552  tux   rtd   DIR    3,3        584 2 /  
bash     5552  tux   txt   REG    3,3  498816 13047 /bin/bash  
bash     5552  tux   mem   REG    0,0          0 [heap] (stat: No such  
bash     5552  tux   mem   REG    3,3  217016 115687 /var/run/nscd/passwd  
bash     5552  tux   mem   REG    3,3  208464 11867 /usr/lib/locale/en_GB.  
bash     5552  tux   mem   REG    3,3  882134 11868 /usr/lib/locale/en_GB.  
bash     5552  tux   mem   REG    3,3 1386997 8837 /lib/libc-2.3.6.so  
bash     5552  tux   mem   REG    3,3  13836 8843 /lib/libdl-2.3.6.so  
bash     5552  tux   mem   REG    3,3  290856 12204 /lib/libncurses.so.5.5  
bash     5552  tux   mem   REG    3,3  26936 13004 /lib/libhistory.so.5.1  
bash     5552  tux   mem   REG    3,3  190200 13006 /lib/libreadline.so.5.  
bash     5552  tux   mem   REG    3,3    54 11842 /usr/lib/locale/en_GB.  
bash     5552  tux   mem   REG    3,3  2375 11663 /usr/lib/locale/en_GB.  
bash     5552  tux   mem   REG    3,3   290 11736 /usr/lib/locale/en_GB.  
bash     5552  tux   mem   REG    3,3   52 11831 /usr/lib/locale/en_GB.  
bash     5552  tux   mem   REG    3,3   34 11862 /usr/lib/locale/en_GB.  
bash     5552  tux   mem   REG    3,3   62 11839 /usr/lib/locale/en_GB.
```

```
bash      5552 tux  mem    REG    3,3      127 11664 /usr/lib/locale/en_GB.
bash      5552 tux  mem    REG    3,3      56 11735 /usr/lib/locale/en_GB.
bash      5552 tux  mem    REG    3,3      23 11866 /usr/lib/locale/en_GB.
bash      5552 tux  mem    REG    3,3    21544 9109 /usr/lib/gconv/gconv-m
bash      5552 tux  mem    REG    3,3      366 9720 /usr/lib/locale/en_GB.
bash      5552 tux  mem    REG    3,3    97165 8828 /lib/ld-2.3.6.so
bash      5552 tux   0u    CHR   136,5          7 /dev/pts/5
bash      5552 tux   1u    CHR   136,5          7 /dev/pts/5
bash      5552 tux   2u    CHR   136,5          7 /dev/pts/5
bash      5552 tux  255u   CHR   136,5          7 /dev/pts/5
```

使用了特殊 shell 变量 \$\$，它的值是 shell 的进程 ID。

如果不带任何参数使用命令 `lsOf`，它将列出当前打开的所有文件。由于有数千个打开的文件，大多数情况下不必列出所有这些文件。但是，所有文件的列表可以与搜索功能组合在一起产生有用的列表。例如，列出所有使用过的字符设备：

```
tux@mercury:~> lsOf | grep CHR
bash      3838   tux    0u      CHR   136,0          2 /dev/pts/0
bash      3838   tux    1u      CHR   136,0          2 /dev/pts/0
bash      3838   tux    2u      CHR   136,0          2 /dev/pts/0
bash      3838   tux    255u    CHR   136,0          2 /dev/pts/0
bash      5552   tux    0u      CHR   136,5          7 /dev/pts/5
bash      5552   tux    1u      CHR   136,5          7 /dev/pts/5
bash      5552   tux    2u      CHR   136,5          7 /dev/pts/5
bash      5552   tux    255u    CHR   136,5          7 /dev/pts/5
X          5646   root   mem     CHR    1,1        1006 /dev/mem
lsOf       5673   tux    0u      CHR   136,5          7 /dev/pts/5
lsOf       5673   tux    2u      CHR   136,5          7 /dev/pts/5
grep       5674   tux    1u      CHR   136,5          7 /dev/pts/5
grep       5674   tux    2u      CHR   136,5          7 /dev/pts/5
```

# 17.7.6 内核和 udev 事件序列浏览器： udevmonitor

`udevmonitor` 可监听由 `udev` 规则发送的内核 `uevent` 和 `event` 并能将事件的设备路径 (`DEVPATH`) 打印到控制台。当连接 USB 记忆棒时会出现一系列事件：



```

UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806687] add@/class/scsi_host/host4
UEVENT[1138806687] add@/class/usb_device/usbdev4.10
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806687] add@/class/scsi_host/host4
UDEV [1138806687] add@/class/usb_device/usbdev4.10
UEVENT[1138806692] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806692] add@/block/sdb
UEVENT[1138806692] add@/class/scsi_generic/sg1
UEVENT[1138806692] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806693] add@/class/scsi_generic/sg1
UDEV [1138806693] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/block/sdb
UEVENT[1138806694] add@/block/sdb/sdb1
UDEV [1138806694] add@/block/sdb/sdb1
UEVENT[1138806694] mount@/block/sdb/sdb1
UEVENT[1138806697] umount@/block/sdb/sdb1

```

## 17.7.7 X11 客户机所使用的服务器资源： xrestop

xrestop 提供每个连接的 X11 客户机服务器端资源的统计信息。输出与第 17.6.4 节“进程：top”[310] 非常相似。

```

xrestop - Display: localhost:0
Monitoring 40 clients. XErrors: 0
Pixmaps: 42013K total, Other: 206K total, All: 42219K total

```

res-base	Wins	GCS	Fnts	Pxms	Misc	Pxm mem	Other	Total	PID	Identifier
3e00000	385	36	1	751	107	18161K	13K	18175K	?	NOVELL: SU
4600000	391	122	1	1182	889	4566K	33K	4600K	?	amaroK - S
1600000	35	11	0	76	142	3811K	4K	3816K	?	KDE Deskto
3400000	52	31	1	69	74	2816K	4K	2820K	?	Linux Shel
2c00000	50	25	1	43	50	2374K	3K	2378K	?	Linux Shel
2e00000	50	10	1	36	42	2341K	3K	2344K	?	Linux Shel
2600000	37	24	1	34	50	1772K	3K	1775K	?	Root - Kon
4800000	37	24	1	34	49	1772K	3K	1775K	?	Root - Kon
2a00000	209	33	1	323	238	1111K	12K	1123K	?	Trekstor25
1800000	182	32	1	302	285	1039K	12K	1052K	?	kicker
1400000	157	121	1	231	477	777K	18K	796K	?	kwin
3c00000	175	36	1	248	168	510K	9K	520K	?	de.comp.la
3a00000	326	42	1	579	444	486K	20K	506K	?	[opensuse-
0a00000	85	38	1	317	224	102K	9K	111K	?	Kopete
4e00000	25	17	1	60	66	63K	3K	66K	?	YaST Contr
2400000	11	10	0	56	51	53K	1K	55K	22061	suseplugge
0e00000	20	12	1	50	92	50K	3K	54K	22016	kded

3200000	6	41	5	72	84	40K	8K	48K	?	EMACS
2200000	54	9	1	30	31	42K	3K	45K	?	SUSEWatche
4400000	2	11	1	30	34	34K	2K	36K	16489	kdesu
1a00000	255	7	0	42	11	19K	6K	26K	?	KMix
3800000	2	14	1	34	37	21K	2K	24K	22242	knotify
1e00000	10	7	0	42	9	15K	624B	15K	?	KPowersave
3600000	106	6	1	30	9	7K	3K	11K	22236	konqueror
2000000	10	5	0	21	34	9K	1K	10K	?	klipper
3000000	21	7	0	11	9	7K	888B	8K	?	KDE Wallet

## 17.8 用户信息

### 17.8.1 哪些用户在执行哪些操作：w

使用命令 `w`，可以查看哪些用户登录到系统上以及每个用户正在执行哪些操作。例如：

```
tux@mercury:~> w
 16:33:03 up 3:33, 2 users, load average: 0.14, 0.06, 0.02
USER      TTY      LOGIN@  IDLE   JCPU   PCPU WHAT
tux      :0        16:33   ?xdm?   9.42s  0.15s /bin/sh /opt/kde3/bin/startk
tux      pts/0     15:59    0.00s  0.19s  0.00s w
```

如果其他系统的任何用户远程登录，则参数 `-f` 将显示这些用户从其上建立连接的计算机。

## 17.9 时间和日期

### 17.9.1 使用 `time` 进行时间度量

用 `time` 实用程序的命令来确定花费的时间。此实用程序有两个版本：内置 `shell` 和程序 (`/usr/bin/time`)。

```
tux@mercury:~> time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

## 使用 Shell

引导 Linux 系统时，您通常会被定向到一个图形用户界面，此界面将引导您完成登录过程以及与系统的后续交互操作。图形用户界面已变得越来越重要且易于使用，但这并不是与系统通信的唯一方式。您也可以使用面向文本的通信方式，如通常称为 shell 的命令行解释器，在 shell 中可以输入命令。Linux 提供通过图形用户界面启动 shell 窗口的选项，因此您可以方便地使用两种方式。

在管理中，基于文本的应用程序对于通过慢速网络链接控制计算机或在您希望作为 root 在命令行上执行任务时非常重要。对于 Linux“菜鸟”，在 shell 中输入命令可能不太习惯，但不久后您就会意识到 shell 不仅仅是为管理员而准备的——其实，shell 通常是执行日常任务的最快捷、最方便的方式。

UNIX 或 Linux 有多个 shell。SUSE® Linux Enterprise 中的默认 shell 是 Bash (GNU Bourne-Again Shell)。

本章介绍使用 shell 时必须了解的一些基础知识。包含以下主题：如何输入命令、Linux 的目录结构、如何使用文件和目录以及如何使用一些基本功能、Linux 的用户和权限概念、重要 shell 命令的概要以及 vi 编辑器（Unix 和 Linux 系统中始终可用的默认编辑器）的简短描述。

### 18.1 Bash shell 入门

在 Linux 中，您可以使用与图形用户界面并行的命令行并在两者之间轻松切换。要通过 KDE 中的图形用户界面启动终端窗口，请单击面板中的 Konsole 图标。在 GNOME 中，单击面板中的 GNOME 终端图标。

此时出现 Konsole 或 GNOME 终端窗口，窗口的第一行显示类似于图 18.1 “Bash 终端窗口示例”[318]所示的提示符。此提示符通常显示您的登录名（在本例中为 tux）、计算机的主机名（此处为 knox）以及当前路径（本例中您的用户主目录，用波浪符 ~ 表示）。当您登录到远程计算机时，您始终可以通过此信息了解到您当前在哪个系统上工作。当光标移到该提示后面时，您可以直接向所在计算机系统发送命令。

**图 18.1** Bash 终端窗口示例



## 18.1.1 输入命令

一条命令包含若干元素。第一个元素总是真正的命令，随后是参数或选项。通过使用 ←、→、←—、Del 和 Space，您可以输入和编辑命令。您还可以添加选项或更正输入错误。按 Enter 时命令将被执行。

---

### 重要：没有消息就是好消息

该 shell 很简洁：与某些图形用户界面不同，它在执行命令后通常不提供确认消息。只有在出现问题或错误的情况下才会显示消息。

使用命令来删除对象时也要牢记这点。输入 rm 之类的命令删除文件之前，您应了解是否确实要删除此对象：它会被无可挽回地删除，而不会询问您。

---

## 使用不带选项的命令

用一个简单的例子看看命令的结构：`ls` 命令，用于列出目录内容。此命令可带选项也可不带选项。只输入 `ls` 命令将显示当前目录的内容：

图 18.2 `ls` 命令

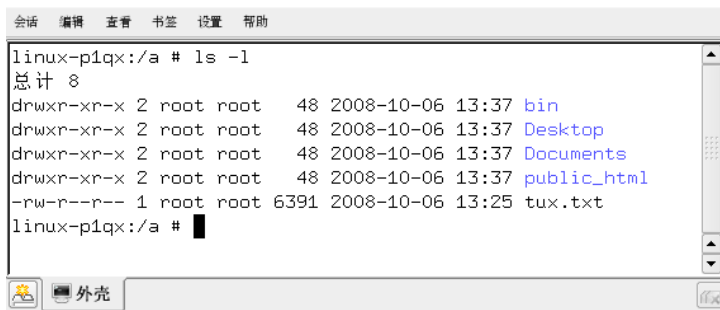


与其他操作系统不同，Linux 中的文件可带有 `.txt` 等文件扩展名，但扩展名不是必需的。这会造成难以区分 `ls` 输出中的文件和文件夹。默认设置下的颜色可给您提示：目录通常以蓝色显示，文件以黑色显示。

## 使用带选项的命令

要获得有关目录内容的更多细节，最好使用带选项字符串的 `ls` 命令。选项可修改命令的工作方式，使您能够使用命令来执行特定任务。选项以连字符为前缀，通过空格与命令分隔。命令 `ls -l` 将显示同一目录中内容的详细信息（长列表格式）：

图 18.3 `ls -l` 命令



每个对象名称的左侧都会显示几列有关此对象的信息。最重要的原则如下：第一列显示对象的文件类型（在本例中，`d` 为目录，`-` 为普通文件）。接下来的 9 列显示对象的用户权限。第 11 和 12 列显示文件拥有者和组的名称（本例中为 `tux` 和 `users`）。有关用户权限和 Linux 的用户概念的详细信息，请参见第 18.2 节“用户和访问权限”[328]。下一列显示文件大小，单位为字节。然后显示上次更改的日期和时间。最后一列显示对象名称。

如果您想要了解更多信息，您可以组合 `ls` 命令的两个选项并输入 `ls -la`。`shell` 此时还会显示目录中的隐藏文件，通过在前面加一个圆点来表示（例如 `.hiddenfile`）。

## 获得帮助

任何用户都没有必要记忆所有命令的所有选项。如果您记住了命令名称但对选项不太确定，您可以先输入命令，紧接着输入一个空格和 `--help`。许多命令都有这个 `--help` 选项。输入 `ls --help` 可以显示 `ls` 命令的所有选项。

## 18.1.2 Linux 目录结构

`shell` 不提供与文件管理器中的树视图类似的目录和文件图形化概览，因此有关 Linux 系统中的默认目录结构的基础知识非常有用。您可以将目录视为储存文件、程序和子目录的电子文件夹。层次中的顶级目录是根目录，用 `/` 表示。从此目录可以访问其他所有目录。

**图 18.4** 显示了 linux 中的标准目录树，其中的用户主目录包含示例用户 `yxz`、`linux` 和 `tux`。`/home` 目录包含用于储存个人用户私人文件的目录。

---

### 注意：网络环境中的用户主目录

如果您在网络环境中工作，您的用户主目录可能不是 `/home`。可将它映射到文件系统中的任何目录。

---

以下列表简要说明了 Linux 中的标准目录。

图 18.4 标准目录树节选

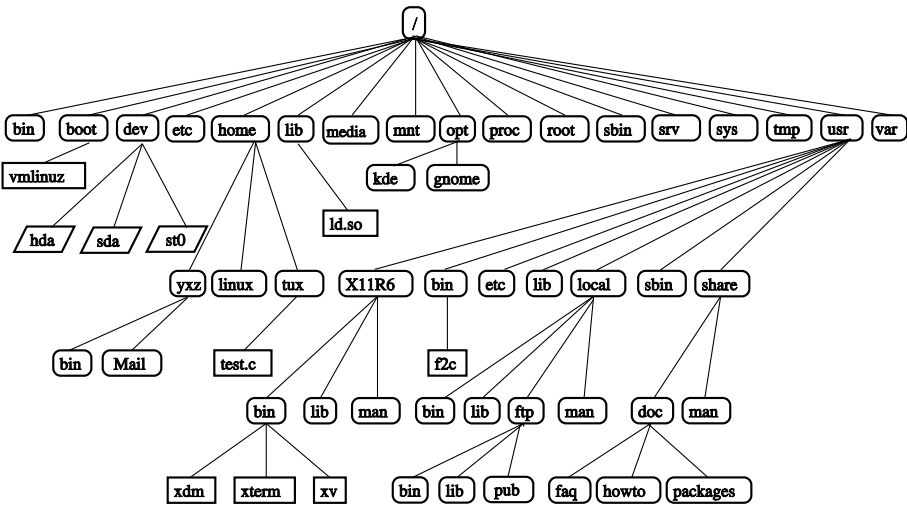


表 18.1 标准目录树概述

/	根目录，目录树的起点
/home	用户的个人目录
/dev	代表硬件组件的设备文件
/etc	重要的系统配置文件
/etc/init.d	引导脚本
/bin、/sbin	引导过程中早期所需的程序（/bin）和管理员的程序（/sbin）
/usr、/usr/local	所有应用程序和本地的、与发布版无关的扩展（/usr/local）
/usr/bin、/usr/sbin	通常可访问的程序（/usr/bin）和供系统管理员访问的程序（/usr/sbin）

<code>/usr/share/doc</code>	各种文档文件
<code>/tmp</code> 、 <code>/var/tmp</code>	临时文件（不要在此目录中保存文件，除非您不需要这些文件）
<code>/opt</code>	选件，大型装载程序包（如 KDE、GNOME 和 Netscape）
<code>/proc</code>	处理文件系统
<code>/sys</code>	system 文件系统，在其中收集内核的所有设备信息
<code>/var/log</code>	系统日志文件

---

### 18.1.3 使用目录和文件

要寻址某一特定文件或目录，您必须指定通向该目录或文件的路径。指定路径的方法有两种：

- 从根目录到相应文件的完整（绝对）路径
- 从当前目录开始的路径（相对路径）

绝对路径始终以斜线开头。相对路径的开头没有斜线。

---

#### 注意：Linux 区分大小写

Linux 在文件系统中区分大小写。例如，Linux 区别对待输入的 `test.txt` 和 `Test.txt`。输入文件名或路径时请牢记这点。

---

要更改目录，请使用 `cd` 命令。

- 要切换到用户主目录，请输入 `cd`。
- 用一个圆点 (`.`) 表示当前目录。这主要对其他命令（`cp`、`mv` 和 ...）有用。



- 树的上一级用两个点 (..) 来表示。例如，要切换到当前目录的父目录，请输入 `cd ..`。

## 文件寻址示例

第 18.1.3 节“使用目录和文件”[322]中的 `cd` 命令使用相对路径。您也可以使用绝对路径。例如，假设您要将文件从用户主目录复制到 `/tmp` 的一个子目录：

- 1 首先，通过用户主目录在 `/tmp` 中创建一个子目录：
  - 1a 如果当前目录不是用户主目录，请输入 `cd ~` 切换到用户主目录。无论在文件系统中的何处，您都可以输入 `cd ~` 进入用户主目录。
  - 1b 在用户主目录中输入 `mkdir /tmp/test`。`mkdir` 代表“make directory”，即创建目录。此命令会在 `/tmp` 目录下创建一个名为 `test` 的新目录。此时，使用绝对路径来创建目录。
  - 1c 此时要检查目录中的变化，请输入 `ls -l /tmp`。新目录 `test` 应显示在 `/tmp` 目录的内容列表。
- 2 接下来，在用户主目录中创建一个新文件并将使用相对路径它复制到 `/tmp/test` 目录。
  - 2a 输入 `touch myfile.txt`。带有 `myfile.txt` 选项的 `touch` 命令会在当前目录下创建一个新的空文件，名为 `myfile.txt`。
  - 2b 输入 `ls -l` 进行检查。内容的列表中应出现新文件。
  - 2c 输入 `cp myfile.txt ../tmp/test`。这会将 `myfile.txt` 复制到 `/tmp/test` 目录，文件名不会改变。
  - 2d 输入 `ls -l /tmp/test` 进行检查。文件 `myfile.txt` 应出现在 `/tmp/test` 的内容列表。

要列出其他用户主目录的内容，请输入 `ls ~username`。在图 18.4“标准目录树节选”[321]的示例目录树中，其中一个样本用户是 `tux`。这样，使用 `ls ~tux` 就会列出 `tux` 用户主目录的内容。

---

**注意：处理文件名或目录名中的空格**

如果文件名包含空格，可在空格前面使用反斜杠 (\) 将空格转义或将文件名包含在单引号或双引号中。否则 **Bash** 会将 `My Documents` 这样的文件名解释为两个文件或目录的名称。单引号和双引号的区别在于双引号中可发生变量扩展。而单引号确保 **shell** 按字面查看括起来的字符串。

---

## 18.1.4 shell 的实用功能

在 **Bash** 中输入命令可能包含大量键入操作。以下介绍 **Bash** 的一些功能，这些功能可大大简化您的工作，省去大量按键操作。

### 历史记录和完成

默认情况下，**Bash** 会“记忆”您输入的命令。此功能称为 *历史记录*。要重复以前输入过的命令，请按 `↑` 键，直到所希望的命令在提示符处出现。按 `↓` 键以在先前输入命令列表中执行向前移动。使用 `Ctrl + R` 可在历史记录中搜索。

在按 **Enter** 键执行命令之前，可编辑选定的命令，如更改文件名。要编辑命令行，只需使用箭头键将光标移至所需位置并开始键入。

键入文件名或目录名的前几个字母后即补全完整的名称，这是 **Bash** 的另一个实用功能。只需在键入前几个字母后按 `→|` 键即可实现此功能。如果可唯一标识文件名或路径，则会立即补全并且光标移动到文件名的末端。然后您可以输入命令的下一选项（如有必要）。如果文件名或路径不能唯一确定（因为有多多个文件名以这些字母开头），则只会将它们补全到之后会有多个选项的那一点。此时再按一次 `→|` 键可获取选项列表。然后您可以输入文件或路径的下一字母并按 `→|` 键再次尝试补全。借助 `→|` 补全文件名和路径的同时，您可以检查您要输入的文件或路径是否确实存在（而且您可以保证拼写无误）。

### 通配符

**shell** 的便捷之处还体现在支持路径名扩展的通配符上。通配符是可代表其他字符的字符。**Bash** 提供三种不同的通配符：

？  
完全匹配任一字符

\*

匹配任意数目的字符

[*set*]

匹配在方括号中指定的字符组中的任一字符，这里用字符串 *set* 表示字符组。作为 *set* 的一部分，还可以使用语法 [*:class:*] 指定字符类别，其中类别可以是 *alnum*、*alpha* 或 *ascii* 等。

使用组开头的 **!** 组开头的或 **^** (**[!set]**) 匹配 *set* 标识的字符之外的任一字符。

假设 *test* 目录包含文件 *Testfile*、*Testfile1*、*Testfile2* 和 *datafile*。

- 命令 `ls Testfile?` 会列出文件 *Testfile1* 和 *Testfile2*。
- 命令 `ls Testfile?` 会列出文件 *Testfile1* 和 *Testfile2*。
- 使用 `ls Test*`，列表还会包含 *Testfile*。
- 命令 `ls *fil*` 用于显示所有示例文件。
- 使用 *set* 通配符代表最后字符是数字的所有样本文件：`ls Testfile[1-9]` 或使用类：`ls Testfile[[:digit:]]`。

四个通配符中匹配范围最广的是星号。使用它可以将某个目录内的所有文件复制到另一个目录，或通过一个命令删除所有文件。例如，使用命令 `rm *fil*` 可以删除当前目录中文件名包含字符串 *fil* 的所有文件。

## 使用 **Less** 和 **More** 查看文件

Linux 包含两个直接在 *shell* 中查看文本文件的小程序：*less* 和 *more*。不必启动编辑器来阅读 *Readme.txt* 之类的文件，只需输入 `less Readme.txt` 即可在控制台窗口中显示其中的文本。使用 **Space** 可以向下滚动一页。使用 **Page Up** 和 **Page Down** 可以在文本中前后移动。要退出 *less*，请按 **Q**。

除使用 *less* 之外，您还可以使用 *more* 这种较早的程序。不过，该程序使用起来不太方便，因为它不允许向后滚动。

less 程序得名于 *less is more*（少即是多）原则，并且还可用来方便地查看命令输出。要了解该程序的这种功能，请参见“[重定向和管道](#)”一节 [326]。

## 重定向和管道

通常，shell 的标准输出界面是您的屏幕或控制台窗口，而标准输入设备是键盘。但是，您可用通过 shell 的功能将输入或输出重定向到另一对象，如文件名或另一命令。例如，借助 `>` 和 `<` 符号，您可以将命令的输出转发到一个文件（输出重定向），或者将某文件用作命令的输入（输入重定向）。举例来说，若要将 `ls` 等命令的输出写入文件，请输入 `ls -l > file.txt`。这会创建一个名为 `file.txt` 的文件，此文件包含 `ls` 命令所生成的当前目录的内容列表。但是，如果已存在名为 `file.txt` 的文件，则此命令会覆盖现有文件。要防止这种情况，请使用 `>>`。输入 `ls -l >> file.txt` 只会将 `ls` 命令的输出追加到名为 `file.txt` 的现有文件。如果不存在此文件，则会创建它。

有时将文件用作命令的输入也很实用。例如，通过 `tr` 命令，您可以替换重定向向文件的字符，并将结果写入标准输出，即屏幕。假设要将上例中 `file.txt` 的所有字符 `t` 替换为 `x` 并将结果输出到屏幕上。输入 `tr t x < file.txt` 即可完成此操作。

标准错误输出和标准输出一样，都发送至控制台。要将标准错误输出重定向到名为 `errors` 的文件，则需要在相应命令中追加 `2> errors`。如果追加的是 `>& alloutput`，标准输出和标准错误都将保存到名为 `alloutput` 的文件中。

使用管线或管道也是一种重定向，虽然管道的使用并不局限于文件。通过管道 (`|`)，您可以组合多个命令，将命令的输出用作下一命令的输入。例如，要在 `less` 中查看内容或当前目录，请输入 `ls | less`。这只是在 `ls` 命令正常输出过长时才有意义。例如，当您使用 `ls /dev` 命令查看 `dev` 目录的内容时，您只能在窗口中看到一小部分。而使用 `ls /dev | less` 命令则能够查看整个列表。

### 18.1.5 存档和数据压缩

您已经创建了一些文件和目录，现在该考虑一下存档和数据压缩的问题了。假定您想将整个 `test` 目录打包在一个文件中，以便备份到 USB 储存条或通过电子邮件发送。要执行该操作，请使用命令 `tar`（代表 *tape archiver*，即磁带存

档程序)。使用 `tar --help` 可查看 `tar` 命令的所有选项。下面对最重要的一些选项进行了说明：

- `-c`  
（代表 `create`）创建新档案。
- `-t`  
（代表 `table`）显示档案中的内容。
- `-x`  
（代表 `extract`）对档案解包。
- `-v`  
（代表 `verbose`）创建档案时在屏幕上显示所有文件。
- `-f`  
（代表 `file`）为档案文件选择一个文件名。创建档案时，此选项总应放在最后。

要将 `test` 目录下的所有文件和子目录打包到名为 `testarchive.tar` 的档案中，请指定以下操作：

- 1 打开 `shell`。
- 2 使用 `cd` 来转到 `test` 目录所在的用户主目录。
- 3 输入 `tar -cvf testarchive.tar test`。`-c` 选项会创建存档文件，使其成为 `-f` 所指示的文件。`-v` 选项会按照这些文件的处理顺序列出文件。
- 4 可使用 `tar -tf testarchive.tar` 查看档案文件的内容。

`test` 目录及其所有文件和目录都在您的硬盘上保持不变。要对档案解包，请输入 `tar -xvf testarchive.tar`，但目前不要尝试。

对文件压缩，典型的选择是 `gzip`，为了得到更好的压缩率，也可选择 `bzip2`。只需输入 `gzip testarchive.tar`（或 `bzip2 testarchive.tar`，但本例中使用的是 `gzip`）。通过 `ls`，您可以看到文件 `testarchive.tar` 已不复存在，取而代之的是文件 `testarchive.tar.gz`。这个文件要小得多，因此也更适于通过电子邮件传送或储存在 USB 储存条上。

现在，将该文件解包到先前创建的 `test2` 目录中。这需要输入 `cp testarchive.tar.gz test2` 将文件复制到该目录中。使用 `cd test2` 转至该目录。扩展名为 `.tar.gz` 的压缩档案可用 `gunzip` 命令解压缩。输入 `gunzip testarchive.tar.gz` 将生成文件 `testarchive.tar`，然后还需使用 `tar -xvf testarchive.tar` 命令抽取或执行 *untar* 操作。您也可以使用以下命令一次完成解压缩并抽取压缩存档：`tar -xvf testarchive.tar.gz`（不再需要添加 `-z` 选项）。通过 `ls`，您会看到新建的 `test` 目录，其内容与用户主目录中的 `test` 目录的内容完全相同。

## 18.1.6 清理

经过上面的速成培训，您应该对 Linux shell 或命令行的基础知识有了一定的了解。最后，您最好使用 `rm` 和 `rmdir` 命令删除各种测试文件和文件夹，清理您的用户主目录。在 [第 18.3 节“重要的 Linux 命令”](#) [331] 中，查找最重要命令的列表及其功能的简要描述。

# 18.2 用户和访问权限

自 20 世纪 90 年代初期推出以来，Linux 一直是一种多用户系统。它支持任意数目的用户同时操作。用户在自己的工作站上启动会话之前必须先登录到系统中。每个用户都有一个用户名及对应的密码。设置用户名和密码可以确保未经授权的用户无法查看他们无权查看的文件。而且，进行这种设置后，通常也不可能对系统进行较大改动（如安装新程序），或者限制普通用户执行此类操作。只有 `root` 用户或超级用户才能不受限制地对系统进行更改并且不受限制地访问所有文件。有效运用这种概念的用户只在必要时才使用不受限制的 `root` 用户权限登录，这样可以减小意外丢失数据的风险。由于一般情况下只有 `root` 用户才能删除系统文件或格式化硬盘，所以来自特洛伊木马的威胁或意外输入破坏性命令的风险得以显著降低。

## 18.2.1 文件系统权限

一般而言，Linux 文件系统系统中的每个文件都属于某个用户和某个组。可以为这些专有组和其他所有组授予读、写或执行这些文件的权限。

在这种情况下，可以将组定义为具有特定集合权限的一组相互连接的用户。例如，可以将共同处理某个项目的组称为 `project3`。Linux 系统中的每个用户都是至少一个专有组（通常是 `users`）的成员。可以根据需要设置系统中组的数目，但只有 `root` 才能添加组。每个用户都可以使用 `groups` 命令查出自己所属的组。

文件访问

文件系统中的权限组织结构不同于文件和目录的组织结构。使用 `ls -l` 命令可以显示文件权限信息。命令输出可能如 [例 18.1 “显示文件权限的示例输出”](#) [329] 中所示。

例 18.1 显示文件权限的示例输出

```
-rw-r----- 1 tux project3 14197 Jun 21 15:03 Roadmap
```

如第三列中所示，此文件属于用户 `tux`。该文件被指派给组 `project3`。要确定 `Roadmap` 文件的用户权限，必须仔细检查第一列。

-	rw-	r--	---
类型	用户权限	组权限	其他用户的权限

此列含有一个前置字符，后接九个字符，每三个字符为一组。这十个字符中的第一个字符代表文件系统组件的类型。连字符(-)表示这是一个文件。也可以用 `d` 表示目录、`l` 表示链接、`b` 表示块设备，或指明字符设备。

后面的三组字符遵循标准模式。前三个字符表示该文件可读(`r`)还是不可读(`-`)。中间的 `w` 表示可以编辑相应的对象，而连字符(`-`)意味着不能写入该文件。排在第三位的 `x` 表示可以执行该对象。由于本例中的文件是不可执行的文本文件，所以不必为这个特定文件授予可执行权限。

在本例中，作为文件 `Roadmap` 的拥有者，`tux` 有权读(`r`)写(`w`)该文件，但无法执行它(`x`)。`project3` 组中的成员可以读取该文件，但不能修改或执行它。其他用户无权访问此文件。通过 **ACL**（Access Control List，访问控制列表）可以指派其他权限。

目录许可权限

目录的访问权限类型用 `d` 来表示。对目录而言，各种权限的含义稍有不同。

### 例 18.2 显示目录权限的示例输出

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15 ProjectData
```

在例 18.2 “显示目录权限的示例输出” [330] 中，很容易识别出目录 ProjectData 的拥有者 (tux) 和所属组 (project3)。与 [文件访问](#) [329] 中的文件访问权限相比，设置读权限 (r) 表示可以显示该目录的内容。写权限 (w) 表示可以创建新文件。执行权限 (x) 表示用户可以转到此目录。上例中，用户 tux 及组 project3 中的成员可以转到 ProjectData 目录 (x)、查看其中的内容 (r) 并添加或删除文件 (w)。其他用户的权限则受到限制。他们可以进入目录 (x) 并浏览其中的内容 (r)，但不能插入任何新文件 (w)。

## 18.2.2 修改文件权限

### 更改访问权限

文件或目录的访问权限可以由拥有者更改，当然也可以由 root 用户更改；更改时要使用命令 chmod，后接更改权限的参数及一个或多个文件名。参数可归为四类：

#### 1. 用户相关参数

- u (用户) — 文件的拥有者
- g (组) — 文件所属的组
- o (其他) — 其他用户 (如果未指定参数，更改将应用到所有类别)

#### 2. 用于删除 (-)、设置 (=) 或插入 (+) 的字符

#### 3. 缩写

- r—读
- w—写
- x—执行

#### 4. 一个文件名或由空格分隔的多个文件名



例如，在 [例 18.2“显示目录权限的示例输出”](#) [330] 中，如果用户 `tux` 还想授予其他用户写入 (`w`) 目录 `ProjectData` 的权限，则可以使用命令 `chmod o+w ProjectData` 执行该操作。

不过，如果该用户不希望任何用户具有写权限（其本人除外），则可以输入命令 `chmod go-w ProjectData` 执行该操作。要防止所有用户向 `ProjectData` 添加新文件，请输入 `chmod -w ProjectData`。现在，如果不首先重建写许可权，则即使拥有者也无法在目录中创建新文件。

### 更改所有权

另有一些重要的命令可用来控制文件系统组件的所有权和权限，这些命令包括 `chown`（更改拥有者）和 `chgrp`（更改组）。使用命令 `chown` 可将文件所有权转让给另一用户。不过，只有 `root` 用户才有权执行该操作。

假定 [例 18.2“显示目录权限的示例输出”](#) [330] 中的文件 `Roadmap` 不应再属于 `tux`，而应属于用户 `geeko`，则 `root` 用户应该输入 `chown geeko Roadmap`。

`chgrp` 用于更改文件的组所有权。不过，文件的拥有者必须是新组的成员。这样，使用命令 `chgrp project4 ProjectData`，[例 18.1“显示文件权限的示例输出”](#) [329] 中的用户 `tux` 即可将文件 `ProjectData` 所属的组更换为 `project4`，只要该用户是这个新组的成员。

## 18.3 重要的 Linux 命令

本节将讨论最重要的命令。本章所列命令只是众多命令中的一小部分。伴随各个命令列出了参数，并且适当的时候还给出了典型的示例应用程序。有关各个命令的详细信息，请使用 `man`，并在后面键入命令名称来查看其手册页，例如 `man ls`。

在参考手册页中，用 `PgUp` 和 `PgDn` 可以上下移动。用 `Home` 和 `End` 可以切换显示文档的开头和结尾。按 `Q` 可以结束这种查看模式。使用 `man man` 可以了解有关 `man` 命令本身的更多信息。

下面的概述中使用不同的字体来表示各个命令元素。实际命令及其必需选项始终显示为命令选项。需要指定的内容或非必需参数均放在 [方括号] 中。

按需调整设置。如果没有名称为 `file` 的文件存在，就不需要写入 `ls file`。通常可以将几个参数组合起来，例如用 `ls -la` 来代替 `ls -l -a`。

## 18.3.1 文件命令

下节将列出最重要的文件管理命令。它包括从总体文件管理到文件系统 ACL 操纵的所有文件管理命令。

### 文件管理

`ls[options][files]`

如果运行 `ls` 时未附加任何参数，程序将以缩写格式列出当前目录中的内容。

`-l`  
详细列表

`-a`  
显示隐藏文件

`cp[options]source target`

将 `source` 复制到 `target`。

`-i`  
在覆盖现有 `target` 之前等待确认（如果需要）

`-r`  
递归复制（包含子目录）

`mv[options]source target`

将 `source` 复制到 `target`，然后删除原始 `source`。

`-b`  
在移动 `source` 之前创建该文件的备份副本

`-i`  
在覆盖现有 `targetfile` 之前等待确认（如果需要）

`rm[options]files`

从文件系统中删除指定文件。除非使用选项 `-r`，否则不能使用 `rm` 删除目录。

`-r`

删除所有现有子目录

`-i`

在删除各个文件之前等待确认

`ln[options]sourcetarget`

创建从 `source` 到 `target` 的内部链接。通常这种链接直接指向同一文件系统上的 `source`。但是，如果执行带 `-s` 选项的 `ln` 命令，则可以创建一个符号链接，仅指向 `source` 所在的目录，支持跨文件系统的链接。

`-s`

创建符号链接

`cd[options][directory]`

更改当前目录。执行不带任何参数的 `cd` 命令将转到用户主目录。

`mkdir[options]directory`

创建新目录。

`rmdir[options]directory`

删除指定的目录（如果该目录已清空）。

`chown[options] username[:[group]]files`

将文件所有权转让给具有指定用户名的用户。

`-R`

更改所有子目录中的文件和目录

`chgrp[options]groupnamefiles`

将特定 `file` 的组所有权转让给具有指定组名的组。如果文件所有者既是当前组也是新组的成员，该拥有者只能转让组所有权。

`chmod[options]modefiles`

更改访问权限。

mode 参数有三部分：group、access 和 access type。组可接受以下字符：

u  
    用户

g  
    组

o  
    其他

对于 access，用 + 可以授予权限，用 - 可以拒绝授予权限。

access type 受以下选项控制：

r  
    读

w  
    写

x  
    执行 - 执行文件或切换到目录

s  
    设置 uid 位 — 就像由文件拥有者启动那样启动应用程序或程序。

也可以选择使用数字代码。此代码的四位数字由值 4、2 和 1 之和组成 - 即二进制掩码的十进制结果。第一位设置“设置用户 ID (SUID) (4)”标志、“设置组 ID (2)”和粘滞 (1) 位。第二位定义文件拥有者的权限。第三位定义组成员的权限，最后一位设置其他所有用户的权限。用 4 设置读权限，2 设置写权限，1 设置执行文件的权限。文件的拥有者通常都会收到 6 或 7，表示可执行文件。

gzip[parameters]files

此程序使用复杂的数学算法压缩文件内容。以这种方式压缩的文件的扩展名为 .gz，而且使用前需解压缩。要压缩若干文件甚至是整个目录，请使用 tar 命令。

**-d**  
将打包的 **gzip** 文件解压缩，使其恢复原始大小，并且能够正常处理（类似命令 **gunzip**）

**tar options archive files**

**tar** 将一个或多个文件放入档案。压缩是可选操作。**tar** 是相当复杂的命令，可以附带若干选项。最常用的选项如下：

**-f**  
将输出结果写入文件，而不是按惯例显示在屏幕上

**-c**  
创建新的 **tar** 档案

**-r**  
将文件添加到现有档案中

**-t**  
输出档案内容

**-u**  
添加文件，但仅适用于文件比档案中已有的文件更新的情况

**-x**  
将档案中的文件解包（抽取）

**-z**  
用 **gzip** 将生成的档案打包

**-j**  
用 **bzip2** 压缩生成的档案

**-v**  
列出已处理的文件

由 **tar** 创建的档案文件以 **.tar** 结尾。如果这个 **tar** 档案还使用 **gzip** 进行了压缩，则以 **.tgz** 或 **.tar.gz** 结尾。如果是使用 **bzip2** 压缩的，则以 **.tar.bz2** 结尾。

`locatepatterns`

只有在安装 `findutils-locate` 包后，此命令才可用。使用 `locate` 命令可以查找指定文件所处的目录。如果需要，可使用通配符来指定文件名。该程序的速度非常快，因为它使用专为此目的创建的数据库（而不是搜索整个文件系统）。但这一事实也导致了一个重大缺陷：`locate` 无法找到其数据库最近更新后创建的任何文件。以 `root` 用户身份使用 `updatedb` 可以生成该数据库。

`updatedb[options]`

此命令可以对 `locate` 使用的数据库进行更新。要包含所有现有目录中的文件，请以 `root` 用户身份运行程序。最好通过追加与号 (&) 令程序在后台运行，这样您就可以紧接着处理同一命令行 (`updatedb &`)。此命令通常作为 `daily cron` 作业运行（请参见 `cron.daily`）。

`find[options]`

使用 `find` 可以在指定目录中搜索文件。第一个参数指定搜索的起始目录。选项 `-name` 后面必须紧跟搜索字符串，字符串中也可以包含通配符。与使用数据库的 `locate` 不同，`find` 扫描的是实际目录。

## 用于访问文件内容的命令

`file[options][files]`

使用 `file` 可检测指定文件的内容。

`-Z`

尝试查看压缩文件的内部

`cat[options]files`

`cat` 命令用于显示文件的内容，使用它可以将所有内容连续打印输出到屏幕上。

`-n`

在左侧对输出编号

`less[options]files`

此命令可用于浏览指定文件的内容。使用 **PgUp** 和 **PgDn** 可以向上或向下滚动半屏，使用 **Space** 可以向下滚动一整屏。使用 **Home** 和 **End** 可以跳转至文件的开头和结尾。按 **Q** 可以退出程序。

`grep[options]searchstringfiles`

`grep` 命令用于在指定文件中查找特定的搜索字符串。如果找到搜索字符串，该命令将显示找到的 `searchstring` 所在的行及文件名。

`-i`

忽略大小写

`-H`

只显示各个文件的名称，不显示文本行

`-n`

另外显示含有匹配项的行的编号

`-l`

只列出其中不含 `searchstring` 的文件

`diff[options]file1file2`

`diff` 命令用于比较任意两个文件的内容。该程序生成的输出将列出所有不匹配的行。这是只需发送程序变更而不是全部源代码的编程人员经常使用的命令。

`-q`

只报告两个文件是否不同

`-u`

生成一个“统一”的 `diff`，从而增加输出的可读性。

## 文件系统

`mount[options][device]mountpoint`

使用此命令可以将任意数据介质（如硬盘、CD-ROM 驱动器和其他设备）装入 Linux 文件系统的某个目录。

`-r`

只读装入

`-t filesystem`

指定文件系统，通常包括：`ext2`（表示 Linux 硬盘）、`msdos`（表示 MS-DOS 介质）、`vfat`（表示 Windows 文件系统）、`iso9660`（表示 CD）。

对于没有在 `/etc/fstab` 中定义的硬盘，还须同时指定设备类型。在这种情况下只能由 `root` 用户装入。如果其他用户也应该能够装入文件系统，则应在 `/etc/fstab` 文件的对应行中输入选项 `user`（用逗号分隔多个用户），并保存所做更改。有关详细信息，请参见 `mount(1)` 手册页。

`umount [options] mountpoint`

此命令可用于从文件系统中卸载装入的驱动器。为防止数据丢失，请在将可移除的数据媒体从其所在驱动器中移除之前运行此命令。通常只有 `root` 用户才能运行 `mount` 和 `umount` 命令。要使其他用户也能运行这些命令，需编辑 `/etc/fstab` 文件，以便为相应的驱动器指定选项 `user`。

## 18.3.2 系统命令

下节列出了用于检索系统信息以及控制进程和网络的几个最重要的命令。

### 系统信息

`df [options] [directory]`

`df`（可用磁盘）命令如不与任何选项一同使用，则可以显示磁盘空间总量、当前占用磁盘空间以及所有已装入驱动器上的可用空间等相关信息。如果指定了目录，则只显示有关该目录所在的驱动器的信息。

`-h`

以用户可读的格式显示占用的块数（以 `GB`、`MB` 或 `KB` 为单位）

`-T`

文件系统的类型（`ext2`、`nfs`，等等）

`du [options] [path]`

执行此命令时若不带任何参数，则可以显示当前目录中的文件和子目录所占用的磁盘空间总量。



- a  
显示各个文件的大小
- h  
以用户可读的格式输出
- s  
仅显示计算的总大小

`free [options]`

`free` 命令用于显示有关占用 **RAM** 和交换空间的信息，可指明这两个类别中的空间总量和占用量。有关更多信息，请参见第 22.1.6 节“**free 命令**”[392]。

- b  
以字节为单位输出
- k  
以 **KB** 为单位输出
- m  
以 **MB** 为单位输出

`date [options]`

这个简单程序可以显示当前系统时间。如果以 `root` 用户身份运行，该程序也可用于更改系统时间。有关该程序的详细信息，请参见 `date(1)` 手册页。

## 进程

`top [options]`

`top` 提供有关当前运行的进程的快速概览。按 **H** 键可访问一个页面，其中简要说明了用于自定义该程序的主要选项。

`ps [options] [process ID]`

如果运行时未指定任何选项，此命令将显示一个表，其中包含您已经启动的所有程序或进程。此命令的选项前不带连字符。

**aux**

显示所有进程的详细列表，不区分拥有者

`kill [options] process ID`

有时程序并不能正常终止。多数情况下，通过在执行 `kill` 命令时指定相应的进程 ID 就应能够停止此类异常程序（请参见 `top` 和 `ps`）。`kill` 将发送 *TERM* 信号，指示程序自行关闭。如果仍无效，可使用以下参数：

**-9**

发送一个 *KILL* 信号而不是 *TERM* 信号，这将在几乎所有情况下终止指定的进程。

`killall [options] processname`

此命令类似 `kill`，但它使用进程名（而不是进程 ID）作为参数，可以取消具有该名称的所有进程。

## 网络

`ping [options] 主机名或 IP 地址`

`ping` 命令是用于测试 TCP/IP 网络基本功能的标准工具。它可以向目标主机发送一个小的数据包，请求立即回复。如果发送有效，`ping` 将据此显示一条消息，指明网络链接基本有效。

**-c 编号**

确定要发送的包总数，并且在发送这些包后终止（默认情况下未设置任何限制）。

**-f**

*flood ping*：发送尽可能多的数据包；这是为 `root` 用户保留的用于测试网络的常用方法。

**-i 值**

指定发送两个数据包之间的时间间隔（默认值：1 秒）。

`nslookup`

域名系统将域名解析为 IP 地址。使用此工具可以将查询发送到名称服务器（DNS 服务器）。

`telnet [options] 主机名或 IP 地址 [port]`

Telnet 实际上是一种因特网协议，能支持您跨网络在远程主机上操作。telnet 同时也是一个 Linux 程序的名称，该程序使用此协议支持远程计算机上的操作。

---

## 警告

切勿在第三方可能“窃听的网络上使用 Telnet。”特别是在因特网上，请使用 ssh 之类的加密传送方法，避免恶意使用密码（请参见有关 ssh 的参考手册页）。

---

## 杂项

`passwd [options] [username]`

用户可以使用此命令随时更改自己的密码。root 用户管理员可以使用该命令更改系统中任意用户的密码。

`su [options] [username]`

使用 su 命令可在当前正在运行的会话中以其他用户名登录。指定用户名和相应的密码。采用 root 用户身份时无需提供密码，因为 root 用户有权采用任意用户的身份。在未指定用户名的情况下使用该命令时，系统将提示您输入 root 用户密码并切换到超级用户 (root)。

-

使用 `su -` 可为另一个用户启动登录 shell

`halt [options]`

为避免丢失数据，您应该始终使用此程序关闭系统。

`reboot [options]`

与 halt 的操作相同，只不过系统会立即重引导。

`clear`

此命令用于清空控制台中的可见区域。该命令不带选项。

## 18.3.3 有关详细信息

本章所列命令只是众多命令中的一小部分。有关其他命令的信息或更详细的信息，建议您参考 O'Reilly 出版的《*Linux in a Nutshell*》。

## 18.4 vi 编辑器

文本编辑器仍用于执行许多系统管理任务和编程。在 Unix 世界中，vi 是一款很好的编辑器，它提供了便于使用的编辑功能，而且比许多具有鼠标支持的编辑器更符合人体工程学。

### 18.4.1 操作方式

---

**注意：按键的显示**

在下面找到使用按键就可以在 vi 中输入的一些命令。它们以大写方式显示在键盘上。如果要输入大写的字母，则会通过显示按键组合明确说明，其中包括 Shift 键。

---

vi 基本上使用三种操作模式：*插入模式*、*命令模式*和*扩展模式*。根据操作方式，各按键具有不同的功能。启动时，vi 通常被设置为命令方式。首先需要了解如何在这些方式之间进行切换：

命令方式切换到插入方式

此时有许多选择，其中使用 A 可以进行追加，使用 I 可以进行插入，使用 O 可以在当前行下创建一个新行。

插入方式切换到命令方式

按 Esc 键退出插入方式。不能在插入方式下终止 vi，所以一定要习惯于按 Esc 键。

命令方式切换到扩展方式

通过输入冒号 (:) 可以激活 vi 的扩展方式。扩展或 ex 方式类似于一个独立的面向行的编辑器，可用于多种简单和较复杂的任务。

扩展方式切换到命令方式

在扩展方式下执行命令后，编辑器将自动返回命令方式。如果决定不在扩展方式下执行任何命令，请使用 <— 键删除冒号。编辑器即返回到命令方式。

必须先从插入方式切换到命令方式，之后才能切换到扩展方式。

vi 与其他编辑器一样，也有自己的终止程序的过程。您不能在插入方式下终止 vi。首先，按 *Esc* 键退出插入方式。接下来有两种选择：

1. 退出而不保存：要终止编辑器而不保存更改，请输入：-Q-！（在命令方式中）。感叹号 (!) 使 vi 忽略任何更改。
2. 保存并退出：有多种可能的方法可保存更改并终止编辑器。在命令方式下，使用 Shift + Z Shift + Z。要使用扩展方式保存所有更改并退出程序，请输入 -W-Q。在扩展方式中，w 表示写，q 表示退出。

## 18.4.2 使用 vi

vi 可用作常规编辑器。在插入方式下，可以输入文本，也可以使用 <— 和 Del 删除文本。使用箭头键可以移动光标。

但这些控制键经常会出现问题，因为有许多终端类型使用特殊键代码。这时就要使用命令方式。按 *Esc* 键从插入方式切换到命令方式。在命令方式下，使用 H、J、k 和 l 键移动光标。这些键具有以下功能：

H	左移一个字符
J	下移一行
K	上移一行
L	右移一个字符

在命令方式下，允许命令采用多种变化形式。要多次执行一个命令，只需要在输入实际命令之前输入重复次数即可。例如，输入 5L 可将光标右移 5 个字符。

表 18.2 “vi 编辑器中的简单命令” [344] 中显示了重要命令的选择。此列表不完整。可在 第 18.4.3 节 “有关详细信息” [345] 的文档中找到更完整的列表

表 18.2 vi 编辑器中的简单命令

Esc	更改为命令方式
I	改为插入模式（字符显示在当前光标位置）
一个	改为插入模式（字符插入到当前光标位置之后）
Shift + A	改为插入模式（在行末添加字符）
Shift + R	更改为替换方式（覆盖旧文本）
R	替换光标下的字符
O	改为插入模式（在当前行之后插入新行）
Shift + O	改为插入模式（在当前行之前插入新行）
X	删除当前字符
D – D	删除当前行
D – W	删除到当前单词的末尾
C – W	改为插入模式（用随后输入的内容覆盖当前单词的剩余部分）
U	复原上一个命令
Ctrl + R	重做复原的更改
Shift + J	连接下一行与当前行
.	重复上一个命令

## 18.4.3 有关详细信息

vi 支持多种不同的命令。它支持使用宏、快捷方式、命名缓冲区和许多其他有用的功能。本手册不包含各种选项的详细描述。SUSE Linux Enterprise 附带 vim（经过改进的 vi），它是 vi 的改进版本。此应用程序有许多信息源：

- vimtutor 是 vim 的交互式教程。
- 在 vim 中，输入命令 :help 可以获得有关许多主题的帮助。
- 上联机提供了一本有关 vim 的参考书。<http://www.truth.sk/vim/vimbook-OPL.pdf>
- 位于 <http://www.vim.org> 上的 vim 项目网页提供了各类新闻、邮件列表和其他文档。
- 因特网上有许多 vim 源：<http://www.selflinux.org/selflinux/html/vim.html>、<http://www.linuxgazette.com/node/view/9039> 和 [http://www.apmaths.uwo.ca/~xli/vim/vim\\_tutorial.html](http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html)。有关指向各教程的链接，请参见<http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html>。

---

### 重要：VIM 许可证

vim 是一款“慈善软件”，这意味着作者不对此软件收取任何费用，但鼓励您进行捐款以支持一项非营利计划。此项目恳请帮助乌干达的可怜儿童。有关详细信息，请访问<http://iccf-holland.org/index.html>、<http://www.vim.org/iccf/> 和 <http://www.iccf.nl/>。

---





## 部分 III. 系统



# 64 位系统环境中的 32 位和 64 位应用程序

# 19

SUSE Linux Enterprise® 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 支持在 64 位系统环境中使用 32 位应用程序。本章简单介绍了如何在 64 位 SUSE Linux Enterprise 平台上实现这种支持。它解释了如何执行 32 位应用程序（运行时支持）以及应该如何编译 32 位应用程序以使它们既可以在 32 位系统环境中运行，又可以在 64 位系统环境中运行。另外，您还可以了解有关内核 API 的信息和 32 位应用程序如何在 64 位内核下运行的解释。

---

**注意：IBM System z 上的 31 位应用程序：**

IBM System z 上的 s390 使用 31 位环境。以下对 32 位应用程序的参照也适用于 31 位应用程序。

---

用于 64 位平台 ia64、ppc64、s390x 和 x86\_64 的 SUSE Linux Enterprise 被设计为可以让现有 32 位应用程序无需进行额外设置即可在 64 位环境中运行。相应的 32 位平台是 x86（对于 ia64）、ppc（对于 ppc64）、s390（对于 s390x）、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。

## 19.1 运行时支持

---

### 重要：应用程序版本之间的冲突

如果某个应用程序在 32 位和 64 位环境中都可用，则两个版本的并行安装必定会导致出现问题。在这种情况下，在两个版本中选一个，然后安装并使用这一版本。

---

若要正确执行，每个应用程序都需要一系列库。不巧的是，这些库的 32 位和 64 位版本的名称是相同的。必须通过另一种方法对它们加以区分。

同样的方法用于 64 位平台 ppc64、s390x 和 x86\_64：为了保留与 32 位版本的兼容性，库在系统中的储存位置与在 32 位环境中相同。在 32 位和 64 位环境中，libc.so.6 的 32 位版本都位于 /lib/libc.so.6 下。

所有 64 位库和对象文件都位于名为 lib64 的目录中。通常可以在 /lib、/usr/lib 和 /usr/X11R6/lib 下找到的 64 位对象文件现在可以在 /lib64、/usr/lib64 和 /usr/X11R6/lib64 下找到。这意味着 /lib、/usr/lib 和 /usr/X11R6/lib 下有储存 32 位库的空间，因此两个版本的文件名都可以保持不变。

如果对象目录的数据内容不取决于此大小，则不移动 32 位 /lib 目录的任何子目录。例如，X11 字体仍位于 /usr/X11R6/lib/X11/fonts 下的常规位置。此方案符合 LSB（Linux 标准库）和 FHS（文件系统层次标准）。

► **ipf**: 用于 ia64 的 64 位库位于标准 lib 目录。这种情况下，既没有 lib64 目录，也没有 lib32 目录。ia64 将在仿真下执行 32 位 x86 代码。一组基本库将安装在 /emul/ia32-linux/lib 和 /emul/ia32-linux/usr/X11R6/lib 中。 ◀

## 19.2 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。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。对于 GCC，此特殊标志是 `-m32`（对于生成 `s390` 库，此特殊标志是 `-m31`）。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。现有 `amd64`（支持 `x86` 和 `amd64` 指令的开发）、`s390x` 和 `ppc64` 的 `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 当前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 `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）。普通 SUSE Linux Enterprise 环境是根据此原则设计的。如果是手动更新的库，请自行解决此问题。

## 19.3 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 `s390x`）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。使用 `s390` 作为第二个体系结构的 `s390x` 或使用 `ppc` 作为第二个体系结构的 `ppc64` 的相关示例是类似的。该示例不适用于未建立 32 位包的 `ia64`。

---

## 提示

使用 `s390` 作为第二个体系结构时，必须使用 `-m31`，而不是 `-m32`，因为这是 31 位系统。

---

### 1 使用 32 位编译器：

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

### 2 指示链接器处理 32 位对象（总是使用 `gcc` 作为链接器前端）：

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

### 3 设置组装机生成 32 位对象：

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

### 4 确定 `libtool` 等的库是否来自 `/usr/lib`：

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

### 5 确定库是否储存在 `lib` 子目录中：

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

### 6 确定是否使用了 32 位 X 库：

```
--x-libraries=/usr/X11R6/lib/
```

并不是每个程序都需要这些变量。根据各个程序对这些变量进行调整。

在 `x86_64`、`ppc64` 或 `s390x` 上编译本机 32 位应用程序的示例 `configure` 调用可以如下所示：

```
CC="gcc -m32" \
LD_FLAGS="-L/usr/lib;" \
    .configure \
        --prefix=/usr \
        --libdir=/usr/lib
make
make install
```

## 19.4 内核规范

x86\_64、ppc64 和 s390x 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

某些应用程序需要单独的内核可装载模块。如果要在 64 位系统环境中使用此类 32 位应用程序，请与此应用程序的提供商和 Novell 联系以确保内核可装载模块的 64 位版本和内核 API 的 32 位编译版本可用于此模块。

---





# 引导和配置 Linux 系统

引导 Linux 系统包括多个不同组件。硬件本身是由 BIOS 初始化，而 BIOS 通过引导加载程序启动内核。此后，引导过程（包括 `init` 和 `runlevel`）完全受操作系统控制。`runlevel` 概念使您可以维护日常使用的设置，也可以对系统执行维护任务。

## 20.1 Linux 引导进程

Linux 引导进程包括多个阶段，每个阶段由一个组件来代表。下表概要总结了引导进程并介绍了所涉及的所有主要组件。

1. **BIOS** 在打开计算机后，BIOS 将初始化屏幕和键盘并测试主存储器。直到这一阶段，计算机不访问任何大容量储存媒体。随后，将从 CMOS 值装载有关当前日期、时间和最重要的外设的信息。当识别出第一块硬盘及其几何属性之后，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. **Boot Loader** 第一块硬盘的前 512 个字节的物理数据扇区将被装载到主存储器中，位于此扇区开始位置的引导加载程序将接管系统控制。引导加载程序执行的命令决定了引导进程剩余的部分。因此，第一块硬盘的前 512 个字节被称为主引导记录 (MBR)。引导加载程序随后将控制传递到实际的操作系统（在本例中即 Linux 内核）。有关 Linux 引导加载程序 GRUB 的详细信息，可以在第 21 章 [引导加载程序](#) [369] 中找到。对于网络引导，BIOS 充当了引导加载程序。它先获取映像以从引导服务器上启动，然后启动系统。这完全不依赖本地硬盘。

3. **内核和 initramfs** 为了传递系统控制，引导加载程序将内核和基于 RAM 的初始文件系统 (initramfs) 装载到内存中。内核可以直接使用 initramfs 的内容。initramfs 包含一个小的可执行文件，称为 init，可以进行真实文件系统的装入处理。如果在访问大容量储存区之前需要特殊硬盘驱动程序，则这些程序必须在 initramfs 中。有关 initramfs 的详细信息，请参考第 20.1.1 节“initramfs”[356]。如果系统没有本地硬盘，则 initramfs 必须向内核提供根文件系统。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 作为根设备。
4. **initramfs 中的 init** 这个程序执行装入正确的 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。如果该操作成功，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 20.1.2 节“initramfs 中的 init”[357]。有关 udev 的更多信息，请参见第 24 章 使用 udev 进行动态内核设备管理[421]。
5. **init** init 通过提供不同功能的多个不同的级别来处理系统的实际引导。有关 init 的介绍，请参见第 20.2 节“init 进程”[358]。

## 20.1.1 initramfs

initramfs 是一个小型 cpio 归档，在此内核可以装载到 RAM 磁盘。它提供了一个最小的 Linux 环境，可在装入实际 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。可使用 initramfs 上的 init 装载根目录文件系统所需的模块。模块装载之后，udev 将为 initramfs 提供所需的设备。在引导过程的后面，更改 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。

如果需要在已安装的系统中更改硬件（例如硬盘），并且该硬件要求在引导时内核中有其他驱动程序，则必须更新 initramfs 文件。其操作方法和其前身 initrd 一样，即调用 mkinitrd。调用 mkinitrd 无需任何参数便可创建 initramfs。调用 mkinitrd -R 创建 initrd。在 SUSE Linux Enterprise® 中，要装载的模块由 /etc/sysconfig/kernel 中的变量 INITRD\_MODULES 指定。

安装后，自动将此变量设置为正确的值。将严格按照这些模块在 `INITRD_MODULES` 中出现的顺序来装载它们。只有您依赖正确的设备文件 `/dev/sd?` 设置时，这才显得重要。然而，在当前系统下，也可以使用 `/dev/disk/` 下的设备文件。这些文件以几个子目录的形式排序，分别为 `by-id`、`by-path` 和 `by-uuid`，并始终代表相同的磁盘。也可以在安装时通过指定相应的装入选项完成此操作。

---

### 重要：更新 `initramfs` 或 `initrd`

引导加载程序装载 `initramfs` 或 `initrd` 的方式与内核相同。在更新 `initramfs` 或 `initrd` 后无需重安装 GRUB，因为 GRUB 会在引导时搜索目录以获得正确的文件。

---

## 20.1.2 `initramfs` 中的 `init`

`initramfs` 中的 `init` 的主要用途是准备真实 `root` 文件系统的装入和访问。根据系统配置的不同，`init` 负责以下任务。

### 装载内核模块

根据硬件配置的不同，可能需要一些特殊的驱动程序来访问计算机的硬件部件（特别是硬盘）。要访问根文件系统，内核需要装载适当的文件系统驱动程序。

### 提供块特殊文件

内核对每个装载的模块生成设备事件。`udev` 处理这些事件，并在 `RAM` 文件系统上的 `/dev` 中生成必需的块特殊文件。没有这些特殊文件，文件系统和其他设备将不可访问。

### 管理 RAID 和 LVM 设置

如果将系统配置为在 RAID 或 LVM 下保存根文件系统，则 `init` 将设置 LVM 或 RAID 以支持稍后对根文件的访问。有关 RAID 的信息请参见第 7.2 节“软 RAID 配置” [111]。有关 LVM 的信息，请参见第 7.1 节“LVM 配置” [103]。可在 *Storage Administration Guide* 中查找有关 EVMS 和特殊储存设置的信息。

### 管理网络配置

如果对系统进行配置以使用通过网络装入的 `root` 文件系统（通过 NFS 装入），则 `init` 必须确保装载了适当的网络驱动器，并确保对其进行设置以允许对 `root` 文件系统的访问。

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

在初始引导期间调用 **init** 时（安装进程一部分），要执行的任务将与前面提到的任务不同：

#### 查找安装媒体

启动安装进程时，计算机将通过安装媒体中的 YaST 安装程序装载一个安装内核和一个特殊的 **initrd**。YaST 安装程序在 RAM 文件系统中运行，它需要有关安装媒体位置的信息以访问安装媒体并安装操作系统。

#### 启动硬件识别并装载适当的内核模块

如第 20.1.1 节“**initramfs**”[356]中所述，引导进程从可用于大多数硬件配置的一组最小的驱动程序启动。**init** 将启动初始硬件扫描进程，以确定适合您的硬件配置的一组驱动程序。引导进程所需的模块名写进

`/etc/sysconfig/kernel` 中的 `INITRD_MODULES`。这些名称用来生成引导该系统所需要的自定义 **initramfs**。如果模块不是用于引导，而是用于冷插入，则模块要写进 `/etc/sysconfig/hardware/hwconfig-*`。本目录下用配置文件描述的所有设备均要在引导过程中进行初始化。

#### 装载安装系统或救援系统

一旦正确地识别出硬件并装载了适当的驱动程序并且 **udev** 创建了设备特殊文件后，**init** 就会启动安装系统，其中包含实际的 YaST 安装程序或救援系统。

#### 启动 YaST

最后，**init** 将启动 YaST，由后者启动包安装和系统配置。

## 20.2 **init** 进程

**init** 程序是进程 ID 为 1 的进程，负责按所要求的方式对系统进行初始化。**init** 由内核直接启动，并且抵制信号 9（该信号通常会杀死进程）。所有其他程序由 **init** 直接启动，或由它的其中一个子进程启动。

**init** 在 `/etc/inittab` 文件中进行集中配置，其中运行级别已定义（请参见第 20.2.1 节“运行级别”[359]）。该文件还指定了在每个级别有哪些服务和守护程序可用。根据 `/etc/inittab` 中的项，**init** 将运行若干个脚本。为了清楚起见，这些称作 *init* 脚本的脚本都位于目录 `/etc/init.d` 中（请参见第 20.2.2 节“**Init 脚本**”[361]）。

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。

## 20.2.1 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 20.1 “可用运行级别” [359]。也可以选择 在引导时指定运行级别（例如，在引导提示符后添加运行级别号）。任何不直接由内核本身求值的参数均将被传递给 `init`。要引导到 `runlevel 3`，只需向引导提示符添加一个数字 3。

表 20.1 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	未使用
5	有网络和 X 显示管理器的完全多用户方式 — KDM、GDM 或 XDM
6	系统重引导

**重要：避免运行级别 2 与通过 NFS 装入的分区**

如果您的系统通过 NFS 装入了 `/usr` 分区，则不应使用运行级别 2。如果程序文件或库丢失，系统可能会异常运行，因为 NFS 设备不能以运行级别 2（没有远程网络的本地多用户方式）提供。

要在系统运行时更改运行级别，请输入 `telinit` 和作为参数的相应数字。仅允许系统管理员执行该操作。下表总结了运行级别区域中最重要的命令。

`telinit 1` 或 `shutdown now`

系统更改为单用户方式。该方式用于系统维护和管理任务。

`telinit 3`

启动了所有基本的程序和服务（包括网络），允许普通用户登录并在不具备图形环境的系统中工作。

`telinit 5`

启用了图形化环境。通常启动诸如 `XDM`、`GDM` 或 `KDM` 之类的显示管理器。如果启用 `autologin`，则本地用户便可登录到预先选择的窗口管理器（`GNOME` 或 `KDE` 或其他任何窗口管理器）中。

`telinit 0` 或 `shutdown -h now`

系统暂停。

`telinit 6` 或 `shutdown -r now`

系统暂停后重引导。

运行级别 5 是所有 SUSE Linux Enterprise 标准安装中的默认运行级别。提示用户使用图形界面登录，或者默认用户将自动登录。如果默认运行级别是 3，必须按照 [第 26 章 X Window 系统](#) [439] 中的描述正确配置 X Window 系统，才能将运行级别切换为 5。完成切换后，请通过输入 `telinit 5` 来检查系统是否以预期方式运行。如果一切合乎预期，就可以使用 YaST 将默认运行级别设置为 5。

---

#### 警告：/etc/inittab 中的错误可能导致系统引导出现问题

如果 `/etc/inittab` 损坏，则可能无法正常引导系统。因此，在编辑 `/etc/inittab` 时要特别小心。在重引导计算机前，使 `init` 使用 `telinit q` 命令重读 `/etc/inittab`。

---

通常情况下，更改运行级别时会发生两件事情。首先是启动当前运行级别的停止脚本，同时关闭当前运行级别必需的一些程序。然后启动新运行级别的启动脚本。在大多数情况下，这时会启动多个程序。例如，将运行级别从 3 更改到 5 时会发生以下情况：

1. 通过输入 `telinit 5`，管理员 (root) 要求 `init` 更改为另一个运行级别。
2. `init` 检查当前运行级别 (`runlevel`) 并确定是否应使用新的运行级别作为参数来启动 `/etc/init.d/rc`。
3. `rc` 现在调用当前运行级别的停止脚本，但仅限新运行级别中没有启动脚本的那些停止脚本。在本例中，这些就是位于 `/etc/init.d/rc3.d` (旧的运行级别是 3) 中以 `K` 开头的所有脚本。`K` 后跟的编号指定使用 `stop` 参数运行脚本的顺序，因为有很多依赖性要考虑。
4. 最后要启动的是新运行级别的启动脚本。在本例中，这些是位于 `/etc/init.d/rc5.d` 中以 `S` 开头的脚本。`S` 后跟的编号确定启动脚本的顺序。

当更改为与当前运行级别相同的运行级别时，`init` 仅检查 `/etc/inittab` 的更改，并启动相应的步骤（例如，在另一个界面上启动 `getty` 所需的步骤）。使用命令 `telinit q` 也达到相同的作用。

## 20.2.2 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 20.2 “可



能的 **init 脚本选项**”[362]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 20.2** 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装载配置。
<code>force-reload</code>	如果服务支持，则重装载配置。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。有关详细信息，请参见手册页 `insserv(8)`。

所有这些设置也可能在 `YaST` 模块的帮助下发生变化。如果需要检查命令行的状态，请使用 `chkconfig(8)` 手册页中所描述的 `chkconfig` 工具。

下面分别简要介绍最先或最后启动的引导和停止脚本，并对脚本的维护进行了描述。

`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。在由这些脚本触发的操作（运行几个子脚本，例如使块特殊文件变为可用的）完成之后它停止。**blogd** 将所有屏幕输出写入日志文件 `/var/log/boot.msg`（前提是装入的 `/var` 是可读写的）。否则，**blogd** 将缓冲所有屏幕数据，直到 `/var` 可用。有关 **blogd** 的详细信息，请参见手册页 **blogd(8)**。

脚本 **boot** 还负责启动 `/etc/init.d/boot.d` 中名称以 **s** 开头的脚本。在这里，将检查文件系统并根据需要配置回路设备。同时设置系统时间。如果在自动检查和修复文件系统时出错，系统管理员可以在输入根密码后进行干预。最后执行的是脚本 **boot.local**。

**boot.local**

在这里，输入引导时在更改为某个运行级别之前执行的其他命令。这类似于 **DOS** 系统上的 **AUTOEXEC.BAT**。

**boot.setup**

在从单用户方式更改为任何其他运行级别时均执行该脚本，它负责许多基本设置，如键盘布局和虚拟控制台的初始化。

**halt**

仅当更改为运行级别 **0** 或 **6** 时执行该脚本。它在这里作为 **halt** 或 **reboot** 来执行。是关闭系统还是重引导系统取决于调用 **halt** 的方式。

**rc**

此脚本调用当前运行级别的相应停止脚本和新选择的运行级别的启动脚本。

您可以创建自己的脚本并方便地将它们集成到上面描述的方案中。有关格式化、命名和组织自定义脚本的描述，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。第 20.2.1 节“运行级别”[359]中有一些有关 **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备份，然后根据需要编辑相关程

序和文件名、路径及其他详细信息。您可能还需要用自己的部分来增强此脚本，以便 `init` 过程可以触发正确的操作。

位于顶部的 `INIT INFO` 块是脚本的一个必需部分，应进行编辑。请参见 [例 20.1 “最小的 `INIT INFO` 块” \[364\]](#)。

### 例 20.1 最小的 `INIT INFO` 块

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

在 `INFO` 块第一行上 `Provides:` 后，指定由此 `init` 脚本控制的程序或服务的名称。在 `Required-Start:` 和 `Required-Stop:` 行中，指定在启动或停止服务本身之前，需要启动或停止的所有服务。这些信息稍后用于生成脚本名的编号（可以在运行级别目录中找到）。在 `Default-Start:` 和 `Default-Stop:` 后，指定应自动启动或停止的服务所在的运行级别。最后，在 `Description:` 下，提供对相关服务的简短描述。

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` 程序对 `INIT INFO` 标题进行求值，以便为运行级别目录 (`/etc/init.d/rc?.d/`) 中的启动和停止脚本创建必要的链接。此程序还负责保证每个运行级别的启动和停止顺序正确无误，方法是在这些链接的名称中包含必要的数字。如果要使用图形工具来创建这样的链接，请按照 [第 20.2.3 节 “使用 YaST 配置系统服务（运行级别）” \[365\]](#) 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。

# 20.2.3 使用 YaST 配置系统服务（运行级别）

使用 YaST> 系统> 系统服务（运行级别）启动此 YaST 模块后，它将显示一个概要，列出所有可用的服务和每个服务的当前状态（禁用或启用）。确定是以简单方式还是以专家方式使用此模块。默认的简单方式足以完成大多数操作。左边的列显示服务的名称，中间的列指示其当前状态，而右边的列则给出简短描述。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。

图 20.1 系统服务（运行级别）



要对所启动或停止的服务所在运行级别进行更具体的控制，或者更改默认运行级别，请先选择专家方式。将在顶部显示当前默认的运行级别或“initdefault”（默认情况下将系统引导至的运行级别）。通常情况下，SUSE Linux Enterprise 系统的默认运行级别是运行级别 5（有网络和 X 的完全多用户方式）。运行级别 3（有网络的完全多用户方式）是合适的替代选择。

此 YaST 对话框用于选择一个运行级别（如 表 20.1 “可用运行级别” [359] 中所列）作为新的默认运行级别。此外，可使用此窗口中的表来启用或禁用各个服务和守护程序。此表列出可用的服务和守护程序，显示它们当前是否已在您的系统上启用，如果已启用，则指示它们用于哪些运行级别。用鼠标选择其中的一行后，请单击表示运行级别（B、0、1、2、3、5、6 和 S）的复选框来确定所选服务或守护程序的运行级别。未对运行级别 4 进行定义，目的是供用户创建自定义运行级别。表概要下方提供了当前所选服务或守护程序的简要说明。

用启动、停止或刷新来确定是否应激活某服务。刷新状态用来检查当前状态。设置或重设置用于选择是将更改应用到系统，还是恢复启动运行级别编辑器之前存在的设置。选择完成即可将已更改的设置保存到磁盘。

---

**警告：有问题的运行级别设置可能会对您的系统造成损害**

有问题的运行级别设置可能会导致系统无法使用。在应用您的更改之前，请确保您清楚这些设置可能产生的结果。

---

## 20.3 通过 `/etc/sysconfig` 配置系统

SUSE Linux Enterprise 的主配置是由 `/etc/sysconfig` 中的配置文件控制的。只有与 `/etc/sysconfig` 中的各个文件相关的脚本才会读取它们。这样有很多好处，例如确保了网络设置只需要由与网络相关的脚本来分析。

可以使用两种方法编辑系统配置。使用 YaST `sysconfig` 编辑器或手动编辑配置文件。

### 20.3.1 使用 YaST Sysconfig 编辑器更改系统配置

YaST `sysconfig` 编辑器为系统配置提供了一种使用方便的前端。无需了解需要更改的配置变量的实际位置，只需使用该模块的内置搜索功能，就可以根据需要更改配置变量的值，并使 YaST 负责应用这些更改以及根据 `sysconfig` 中设置的值更新配置和重新启动服务。

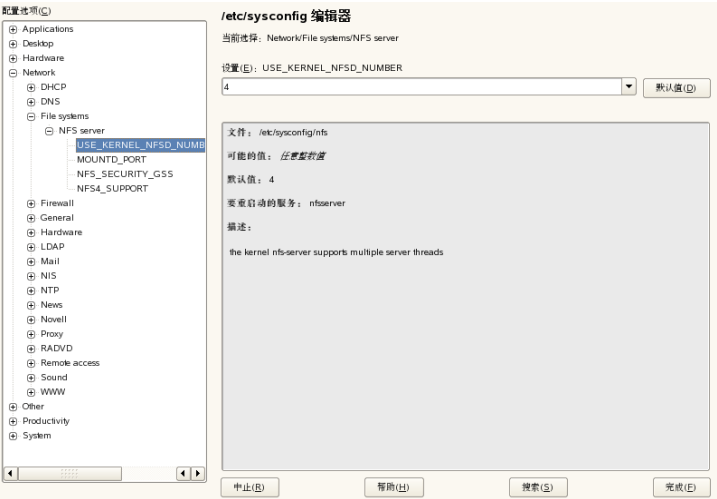
---

**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 20.2 使用 sysconfig 编辑器进行系统配置



YaST sysconfig 对话框分为三个部分。对话框左边的部分显示了一个树视图，其中列出了所有可配置变量。当您选择某个变量时，右边的部分会显示当前选择和此变量的当前设置。在下部的第三个窗口中，简要描述了变量的用途、可能的值、默认值以及作为此变量来源的实际配置文件。此对话框还提供了有关更改变量后将执行哪些配置脚本，以及作为更改的结果将启动哪些新服务等信息。YaST 将提示您确认更改，并通知您在选择完成退出对话框后将执行哪些脚本。在这里还可以选择需要现在跳过而在以后启动的服务和脚本。YaST 将自动应用所有的更改并重启动涉及的所有服务以使更改生效。

## 20.3.2 手动更改系统配置

要手动更改系统配置，请执行如下操作

- 1 成为 root 用户。
- 2 使用 `init 1` 将系统转入单用户方式（运行级别 1）。
- 3 使用您选择的编辑器根据需要对配置文件进行更改。

如果不使用 YaST 来更改 `/etc/sysconfig` 中的配置文件，则要确保将空变量值用两个引号表示 (`KEYTABLE=""`)，并将含有空白的值用引号括起来。只包括一个单词的值不需要用引号括起来。

- 4 执行 `SUSEconfig` 来确保更改生效。
- 5 使用类似 `init default_runlevel` 的命令将系统返回到先前的运行级别。使用系统的默认运行级别替代 `default_runlevel`。如果想返回有网络和 X 的完全多用户方式，请选择 5；如果希望在有网络的完全多用户方式下工作，请选择 3。

这一过程主要用于更改整个系统范围的配置，例如网络配置。若要进行较小的更改，不一定要切换到单用户方式，但这样做可以完全确保正确重新启动所有相关的程序。

---

#### 提示：配置自动系统配置

要禁用 `SUSEconfig` 设定的自动系统配置，请将 `/etc/sysconfig/suseconfig` 中的变量 `ENABLE_SUSECONFIG` 设置为 `no`。如果要使用 SUSE 安装支持，请不要禁用 `SUSEconfig`。也可以部分禁用自动配置。

---

## 引导加载程序

本章介绍如何配置 GRUB（在 SUSE Linux Enterprise® 中使用的引导加载程序）。一个特殊的 YaST 模块可用于执行所有设置。如果您不熟悉在 Linux 中进行引导的相关内容，请阅读下面几节获得一些背景信息。本章还介绍了使用 GRUB 进行引导时经常遇到的一些问题和它们的解决方案。

本章主要介绍引导加载程序 GRUB 的引导管理和配置。[第 20 章 引导和配置 Linux 系统](#) [355] 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) 之间的接口。引导加载程序的配置直接影响到操作系统的启动。

本章经常出现以下术语，可能需要进行解释：

### 主引导记录

MBR 的结构是由独立于操作系统的约定定义的。前 446 个字节为程序代码保留。它们通常保存部分引导加载程序或操作系统选择器。随后的 64 个字节为最多包含 4 项的分区表提供空间（请参见[“分区类型”一节](#) [141]）。分区表包含有关硬盘分区和文件系统类型的信息。操作系统需要使用此表来处理硬盘。如果 MBR 中有传统通用代码，则只应将一个分区标记为活动。MBR 的最后两个字节包含静态“幻数”(AA55)。一些 BIOS 会将包含不同值的 MBR 视为无效，因此引导时不会考虑此 MBR。

### 引导扇区

引导扇区是硬盘分区（除扩展分区之外）上的前几个扇区，扩展分区只充当其他分区的“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。

## 21.1 选择引导加载程序

默认情况下，引导加载程序 GRUB 用于 SUSE Linux Enterprise 中。但是，在某些情况下以及对于特殊的硬件和软件，使用 LILO 可能是必需的。如果您更新较早的 SUSE Linux Enterprise 版本（该版本使用 LILO），则将安装 LILO。

有关安装和配置 LILO 的信息可以在支持数据库中的关键字“LILO”和文件 `/usr/share/doc/packages/lilo` 下获得。

## 21.2 通过 GRUB 引导

GRUB (Grand Unified Bootloader) 由两段组成。stage1 包含 512 个字节，它的唯一任务就是装载引导加载程序的第二段。随后，装载 stage2。这一段包含引导加载程序的主要部分。

在一些配置中，可以使用中间段 1.5，它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。

stage2 可以访问许多文件系统。当前，支持 Ext2、Ext3、ReiserFS、Minix，以及 Windows 使用的 DOS FAT 文件系统。在某种程度上还支持 BSD 系统使用的、XFS、UFS 和 FFS。从版本 0.95 开始，GRUB 还能够从包含 ISO 9660 标准文件系统、符合“El Torito”规范的 CD 或 DVD 进行引导。即使是在引导系统之前，GRUB 也可以访问支持的 BIOS 磁盘设备（BIOS 检测到的软盘或硬盘、CD 驱动器和 DVD 驱动器）的文件系统。因此，对 GRUB 配置文件 (`menu.lst`) 进行更改不要求重安装引导管理器。当引导系统时，GRUB 重装载菜单文件以及内核或初始 ram 磁盘 (`initrd`) 的有效路径和分区数据，并对这些文件进行定位。

GRUB 的实际配置是基于三个文件进行的，下面对这三个文件进行介绍：



/boot/grub/menu.lst

此文件包含有关可通过 GRUB 进行引导的分区或操作系统的所有信息。没有这些信息，GRUB 命令行将提示用户如何继续（请参见“[在引导过程中编辑菜单项](#)”一节 [375] 获取详细信息）。

/boot/grub/device.map

此文件将 GRUB 和 BIOS 符号中的设备名转换为 Linux 设备名。

/etc/grub.conf

此文件包含 GRUB shell 正确安装引导加载程序所需的命令、参数和选项。

可以通过多种方式控制 GRUB。可以在图形菜单（启动屏幕）中选择现有配置的引导项。配置是从文件 menu.lst 装载的。

在 GRUB 中，在引导前可以更改所有引导参数。例如，可以通过这种方式更正编辑菜单文件时出现的错误。还可以在输入提示符处以交互的方式输入引导命令（请参见“[在引导过程中编辑菜单项](#)”一节 [375]）。GRUB 能够在引导前确定内核和 initrd 的位置。通过这种方式，您甚至可以引导在引导加载程序配置中不存在任何项的已安装操作系统。

GRUB 实际上以两个版本存在：作为引导加载程序以及作为 /usr/sbin/grub 中的普通 Linux 程序。此程序被称为 *GRUB shell*。它在已安装系统中提供 GRUB 的仿真，并且可用来安装 GRUB 或在应用新设置之前对其进行测试。将 GRUB 作为引导加载程序安装在硬盘或软盘上的功能以 install 和 setup 命令的形式集成在 GRUB 中。当装载了 Linux 后在 GRUB shell 中可用。

## 21.2.1 GRUB 引导菜单

带有引导菜单的图形启动屏幕基于 GRUB 配置文件 /boot/grub/menu.lst，该文件包含有关可以通过菜单引导的所有分区或操作系统的所有信息。

每次引导系统时，GRUB 都从文件系统装载菜单文件。出于此原因，不必每次更改文件后都重安装 GRUB。使用 YaST 引导加载程序修改 GRUB 配置，如 [第 21.3 节“使用 YaST 配置引导加载程序”](#) [378] 中所述。

菜单文件中包含命令。语法非常简单。每行都包含一条命令，后跟可选参数，可选参数之间用空格隔开，就像在 shell 中一样。出于历史原因，某些命令允许在第一个参数前使用 =。注释以井号 (#) 开头。

若要在菜单概述中标识菜单项，请为每项设置一个 `title`。关键字 `title` 后的文本（包括任何空格）显示为菜单中的可选择选项。当选择此菜单项时，将执行下一个 `title` 前的所有命令。

最简单的情况是重定向到其他操作系统的引导加载程序。命令是 `chainloader`，参数通常是 GRUB 中另一个分区的引导块 `block notation`。例如：

```
chainloader (hd0,3)+1
```

GRUB 中的设备名在“[硬盘和分区的命名约定](#)”一节 [372] 中有所解释。此示例指定第一个硬盘第四个分区中的第一个块。

使用命令 `kernel` 指定内核映像。第一个参数是指向分区中内核映像的路径。命令行上的其他参数将被传递到内核。

如果内核不具有访问根分区的内置驱动程序，或者使用了具有高级热插拔功能的最新 `linux` 系统，则必须用单独的 GRUB 命令指定 `initrd`，该命令的唯一参数便是指向 `initrd` 文件的路径。因为 `initrd` 的装载地址会被写入装载的内核映像中，所以 `initrd` 命令必须紧接在 `kernel` 命令之后。

命令 `root` 简化了内核和 `initrd` 文件的指定。`root` 的唯一参数是一个设备或分区。此设备用于所有内核、`initrd` 或下一个 `root` 命令前未显式指定设备的其他文件路径。

每个菜单项的末尾都间接指定 `boot` 命令，因此无需将其写入菜单文件中。但是，如果以交互方式使用 GRUB 进行引导，则必须在最后输入 `boot` 命令。该命令本身没有参数。它只引导装载的内核映像或指定的链装载程序。

在写入所有菜单项之后，将其中一项定义为 `default` 项。否则，将使用第一项（项 0）。您还可以指定在一段时间后引导默认项的超时值（以秒为单位）。`timeout` 和 `default` 通常在各菜单项前面。示例文件在“[示例菜单文件](#)”一节 [373] 中有所介绍。

## 硬盘和分区的命名约定

GRUB 用于硬盘和分区的命名约定不同于普通 `Linux` 设备使用的命名约定。它更类似于 BIOS 执行的简单磁盘枚举，而语法类似于一些 `BSD` 衍生程序中使用的语法。在 GRUB 中，分区的编号从 0 开始。它表示 `(hd0, 0)` 是第一块硬盘

的第一个分区。在普通台式机上，作为 **Primary Master**（第一个 IDE 控制器上的主设备）连接的硬盘所对应的 **Linux** 设备名为 `/dev/hda1`。

4 个可能的主分区所分配的分区号为 }0 到 3。逻辑分区的编号从 4 开始：

```
(hd0,0)    first primary partition of the first hard disk
(hd0,1)    second primary partition
(hd0,2)    third primary partition
(hd0,3)    fourth primary partition (usually an extended partition)
(hd0,4)    first logical partition
(hd0,5)    second logical partition
```

**GRUB** 依赖于 **BIOS** 设备，它不区分 **IDE**、**SATA**、**SCSI** 和硬件 **RAID** 设备。**BIOS** 或其他控制器识别的所有硬盘将按照 **BIOS** 中显示的引导顺序进行编号。

不过，通常不能将 **Linux** 设备名准确映射为 **BIOS** 设备名。它借助某种算法生成这一映射并将其保存到文件 `device.map` 中，可以根据需要对该文件进行编辑。有关文件 `device.map` 的信息在 [第 21.2.2 节“文件 `device.map`”](#) [376] 中有所介绍。

完整的 **GRUB** 路径包含写在括号中的设备名和指向指定分区的文件系统中文件的路径。路径以斜线开头。例如，在具有一个 **IDE** 硬盘（该硬盘的第一个分区中包含 **Linux**）的系统上，可以按如下方式指定可引导内核：

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

## 示例菜单文件

以下示例说明了 **GRUB** 菜单文件的结构。该示例安装包括 `/dev/hda5` 下的 **Linux** 引导分区、`/dev/hda7` 下的引导分区和 `/dev/hda1` 下的 **Windows** 安装。

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd

title windows
    chainloader (hd0,0)+1
```

```

title floppy
    chainloader (fd0)+1

title failsafe
    kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3
    initrd (hd0,4)/initrd.shipped

```

第一块定义了启动屏幕的配置：

**gfxmenu (hd0,4)/message**

背景图像 `message` 位于 `/dev/hda5` 分区的顶级目录中。

**color white/blue black/light-gray**

色彩模式：白色（前景色）、蓝色（背景色）、黑色（所选内容）、浅灰色（所选内容的背景）。颜色方案对启动屏幕没有任何影响，它只影响通过按 `Esc` 键退出启动屏幕后所访问的可自定义的 **GRUB** 菜单。

**default 0**

第一个菜单项 `title linux` 是默认情况下引导的对象。

**timeout 8**

如果 8 秒钟后无任何用户输入，**GRUB** 将自动引导默认项。要检测自动引导，请删除 `timeout` 行。如果设置 `timeout 0`，**GRUB** 将立即引导默认项。

第二块（也就是最大的块）列出了各个可引导的操作系统。各个操作系统的不同部分由 `title` 引出。

- 第一项 (`title linux`) 负责引导 **SUSE Linux Enterprise**。内核 (`vmlinuz`) 位于第一块硬盘的第一个逻辑分区（引导分区）。内核参数（例如引导分区和 **VGA** 方式）也被追加在此处。引导分区是根据 **Linux** 命名约定 (`/dev/hda7/`) 指定的，这是因为此信息将被内核读取而与 **GRUB** 无关。`initrd` 也位于第一块硬盘的第一个逻辑分区中。
- 第二项负责装载 **Windows**。**Windows** 将从第一块硬盘的第一个分区 (`hd0,0`) 引导。命令 `chainloader +1` 将导致 **GRUB** 读取并执行指定分区的第一个扇区。
- 下一项支持从软盘进行引导，而无需修改 **BIOS** 设置。

- 引导选项 `failsafe` 用一组内核参数启动 Linux，这些参数使 Linux 甚至可以在有问题的系统上引导。

随时可以根据需要更改菜单文件。GRUB 会在下次引导时使用修改后的设置。使用 YaST 或所选的编辑器对文件进行永久编辑。或者，使用 GRUB 的编辑功能可以按交互方式进行临时更改（请参见“在引导过程中编辑菜单项”一节 [375]）。

## 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 51.1 “美式键盘布局” [825] 的图。

---

编辑菜单条目简化了无法再进行引导的有问题系统的修复工作，因为可以通过手动输入参数规避引导加载程序中配置文件的配置。在引导过程中手动输入参数还可用于测试新设置而避免损坏本机系统。

在激活编辑方式后，可以使用箭头键选择要编辑其配置的菜单项。若要使配置可以编辑，请再次按 `E` 键。通过这种方式，可以编辑不正确的分区或路径指定，从而防止它们对引导进程产生负面影响。按 `Enter` 键退出编辑方式并返回菜单。随后按 `B` 键引导此项。可以进行的进一步操作显示在底部的帮助文本中。

若要永久输入更改的引导选项并将它们传递到内核，则以 `root` 用户身份打开文件 `menu.lst` 并将相应的内核参数追加到现有的行上，用空格分隔：

```
title linux
    kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
    initrd (hd0,0)/initrd
```

GRUB 会在下次引导系统时自动采用新参数。或者，还可以通过 YaST 引导加载程序模块进行此更改。将新参数追加到现有的行上，用空格分隔。

## 21.2.2 文件 device.map

文件 `device.map` 将 GRUB 和 BIOS 设备名映射为 Linux 设备名。在包含 IDE 和 SCSI 硬盘的混合系统中，GRUB 必须通过特殊过程尝试确定引导顺序，因为 GRUB 不能访问 BIOS 上有关引导顺序的信息。GRUB 会将此分析的结果保存在文件 `/boot/grub/device.map` 中。对于 BIOS 中引导顺序设置为 IDE 在 SCSI 之前的系统，文件 `device.map` 如下所示：

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

因为 IDE、SCSI 和其他硬盘的顺序取决于不同的因素，并且 Linux 无法标识映射，所以可以在 `device.map` 文件中手动设置顺序。如果在引导时遇到问题，则检查此文件中的顺序是否对应于 BIOS 中的顺序，如果需要，使用 GRUB 提示符对其进行临时修改。引导了 Linux 系统之后，便可以使用 YaST 引导加载程序模块或所选的编辑器对文件 `device.map` 进行永久编辑。

---

### 重要：SATA 磁盘

根据控制器，将 SATA 磁盘识别为 IDE (`/dev/hdx`) 或 SCSI (`/dev/sdx`) 设备。

---

在手动更改 `device.map` 之后，请执行以下命令重安装 GRUB。此命令导致重装文件 `device.map` 并且执行 `grub.conf` 中列出的命令：

```
grub --batch < /etc/grub.conf
```

## 21.2.3 文件 /etc/grub.conf

除了 menu.lst 和 device.map 之外，第三个重要的 GRUB 配置文件就是 /etc/grub.conf。此文件包含 GRUB shell 正确安装引导加载程序所需的命令、参数和选项：

```
root (hd0,4)
  install /grub/stage1 (hd0,3) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

各个项的含义：

**root (hd0,4)**

此命令指示 GRUB 将以下命令应用到第一块硬盘的第一个逻辑分区（引导文件的位置）。

**install parameter**

应使用参数 install 来运行命令 grub。应将引导加载程序的 stage1 安装在扩展分区树枝（/grub/stage1 (hd0,3)）中。此配置较为深奥，但是在许多情况下适用。应将 stage2 装载到内存地址 0x8000（/grub/stage2 0x8000）中。最后一项((hd0,4)/grub/menu.lst) 指示 GRUB 查找菜单文件的位置。

## 21.2.4 设置引导密码

即使是在引导操作系统之前，GRUB 也支持对文件系统的访问。没有根权限的用户可以访问 Linux 系统中的文件，而一旦引导系统后，他们将无权访问这些文件。若要阻止这种访问或防止用户引导某些操作系统，可以设置引导密码。

---

### 重要：引导密码和启动屏幕

如果对 GRUB 使用引导密码，则不显示通常的启动屏幕。

---

以 root 用户身份按如下步骤设置引导密码：

- 1 在根提示符处，使用 grub-md5-crypt 加密密码：

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- 2 将经过加密的字符串粘贴到 menu.lst 文件的全局部分：

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

现在，只有在按 **P** 键并输入密码后，才可以在引导提示符处执行 GRUB 命令。但是，用户仍可以从引导菜单引导所有操作系统。

- 3 要防止从引导菜单引导一个或多个操作系统，请将项 lock 添加到 menu.lst 中不输入密码就不能引导的每个部分。例如：

```
title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd
    lock
```

在重引导系统并从引导菜单中选择 Linux 项后，将显示以下错误消息：

```
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）。

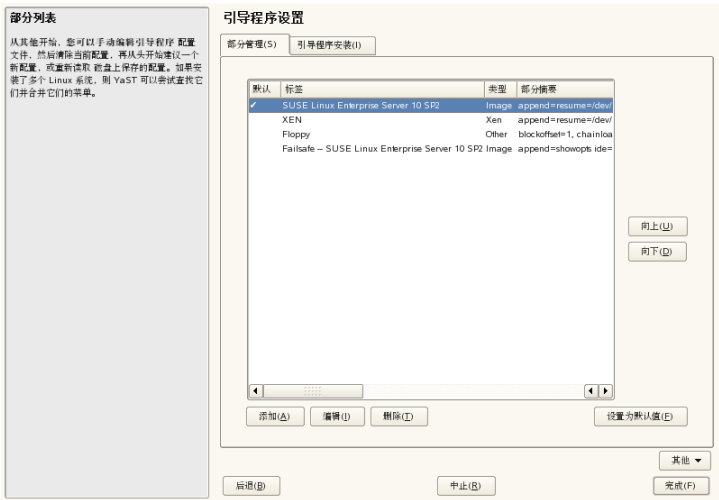
## 21.3 使用 YaST 配置引导加载程序

在您的 SUSE Linux Enterprise 系统中配置引导加载程序最简单的方式就是使用 YaST 模块。在 YaST 控制中心，选择系统 > 引导加载程序。如图 21.1 “Boot



**Loader 设置** [379] 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 21.1 Boot Loader 设置



使用扇区管理选项卡可编辑、更改和删除单个操作系统的引导加载程序扇区。若要添加某个选项，请单击添加。要更改现有选项的值，请用鼠标选中它，然后单击编辑。要删除现有的条目，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 21.2 节“通过 GRUB 引导” [370]。

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

从单击其他后打开的下拉菜单中访问高级配置选项。内置编辑器让您可以更改 GRUB 配置文件（细节请参见第 21.2 节“通过 GRUB 引导” [370]）。也可以删除现有配置并从头开始或让 YaST 建议新配置。也可以向磁盘写入配置或从磁盘重新读取配置。要恢复在安装期间保存的原始主引导记录，请选择恢复硬盘的主引导记录。

## 21.3.1 引导加载程序类型

在引导加载程序安装中设置引导加载程序类型。SUSE Linux Enterprise 中默认的引导加载程序是 GRUB。如要使用 LILO，请执行如下操作：

## 过程 21.1 更改引导加载程序类型

- 1 选择引导加载程序安装选项卡。
- 2 对于引导加载程序，请选择 *LILO*。
- 3 在打开的对话框中，选择以下某个操作：

建议新配置

让 YaST 推荐一个新的配置。

转换当前配置

让 YaST 转换当前的配置。在转换配置时，有些设置可能会丢失。

从头开始新的配置

编写自定义配置。此操作在安装 SUSE Linux Enterprise 期间时不可用。

读取保存在磁盘上的配置

装载自己的 `/etc/lilo.conf`。此操作在安装 SUSE Linux Enterprise 期间不可用。

- 4 单击确定保存更改。
- 5 在主对话框中单击完成以应用更改。

转换时，旧的 GRUB 配置将保存到磁盘上。如要使用它，只需将引导加载程序类型改回 GRUB，然后选择恢复转换前保存的配置。此操作仅在已安装的系统上可用。

---

### 注意：自定义引导加载程序

如果想要使用 GRUB 或 LILO 以外的引导加载程序，请选择不安装任何引导加载程序。在选择该选项之前，请仔细阅读您的引导加载程序文档。

---

## 21.3.2 引导加载程序位置

要更改引导加载程序的位置，请遵循以下步骤：

## 过程 21.2 更改引导加载程序位置

- 1 选择引导加载程序安装选项卡，然后为引导加载程序位置选择以下某个选项：

从引导分区引导

/boot 分区的引导扇区。

从扩展分区引导

这将在扩展分区容器中安装引导加载程序。

从主引导记录引导

本操作会在第一个磁盘的 MBR 中安装引导加载程序（根据 BIOS 中预设的引导顺序）。

从引导分区引导

这将在 / 分区的引导扇区安装引导加载程序。

自定义引导分区

手动使用此选项来指定引导加载程序的位置。

- 2 单击结束来应用更改。

## 21.3.3 默认系统

要更改默认引导的系统，请按如下所示继续：

### 过程 21.3 设置默认系统

- 1 打开扇区管理选项卡。
- 2 从列表中选择所需的条目。
- 3 单击设为默认。
- 4 单击完成以激活这些更改。

## 21.3.4 引导加载程序超时

引导加载程序不会立即引导默认系统。超时期间，可以选择要引导的系统或编写一些内核参数。要设置引导加载程序超时值，请执行如下操作：

### 过程 21.4 更改引导加载程序超时值

- 1 打开引导加载程序安装选项卡。
- 2 单击引导加载程序选项。
- 3 用鼠标单击相应的方向键或者使用键盘上的方向键来更改超时秒数中的值，或者输入新的值。
- 4 单击确定。
- 5 单击完成以保存更改。

## 21.3.5 安全性设置

使用此 YaST 模块，还可以设置密码来保护引导。这提供了更高的安全性级别。

### 过程 21.5 设置引导加载程序密码

- 1 打开引导加载程序安装选项卡。
- 2 单击引导加载程序选项。
- 3 在菜单界面密码中设置密码。
- 4 单击确定。
- 5 单击完成以保存更改。

## 21.4 卸载 Linux 引导加载程序

YaST 可用于卸载 Linux 引导加载程序并将 MBR 恢复为安装 Linux 之前的状态。在安装过程中，YaST 自动创建原始 MBR 的备份副本并根据请求进行恢复。

要卸载 GRUB，请启动 YaST 引导加载程序模块（系统 > 引导加载程序）。选择其他 > 恢复硬盘的主引导记录然后选择是，重写加以确认。

## 21.5 创建引导 CD

如果使用引导管理器引导系统时出现问题或如果不能将引导管理器安装在硬盘的 MBR 或软盘上，那么还可以创建包含所有必需的 Linux 启动文件的可引导 CD。这需要您的系统中安装有 CD 刻录机。

用 GRUB 创建可引导 CD-ROM 只需要特殊形式的 *stage2*（名为 *stage2\_eltorito*）以及自定义的 *menu.lst*（可选）。不需要标准文件 *stage1* 和 *stage2*。

### 过程 21.6 创建引导 CD

1 将目录更改为要创建 ISO 映像的目录，例如：`cd /tmp`

2 创建 GRUB 的子目录：

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

3 将内核、文件 *stage2\_eltorito*、*initrd*、*menu.lst* 和 *message* 复制到 *iso/boot/*：

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

4 调整 *iso/boot/grub/menu.lst* 中的路径条目使其指向 CD-ROM 设备。执行此操作的方法是将路径名中硬盘的设备名（以 *(sd\*)* 格式列出）替换为 CD-ROM 驱动器的设备名（即 *(cd)*）：

```

timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
    root (cd)
    kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
    splash=verbose showopts
    initrd /boot/initrd

```

使用 `splash=silent` 代替 `splash=verbose` 来防止引导过程中出现引导消息。

## 5 用以下命令创建 ISO 映像：

```

mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso /tmp/iso

```

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

# 21.6 图形 SUSE 屏幕

从 SUSE Linux 7.2 开始，如果将选项 `vga=value` 用作内核参数，则会在第一个控制台上显示图形 SUSE 屏幕。如果您使用 YaST 进行安装，则将依照所选的分辨率和图形卡自动激活此选项。可以根据需要通过三种方法禁用 SUSE 屏幕：

在必要时禁用 SUSE 屏幕。

在命令行上输入命令 `echo 0 >/proc/splash` 以禁用图形屏幕。要将其再次激活，请输入 `echo 1 >/proc/splash`。

默认禁用 SUSE 屏幕。

将内核参数 `splash=0` 添加到您的引导加载程序配置中。[第 21 章 引导加载程序](#) [369] 提供了有关此内容的详细信息。但是，如果您倾向于使用文本方式（这是早期版本中的默认方式），请设置 `vga=normal`。

完全禁用 SUSE 屏幕

编译新内核并禁用帧缓冲支持中的选项使用启动屏幕而不是引导徽标。

---

## 提示

在内核中禁用帧缓冲支持也会自动禁用启动屏幕。如果您使用自定义内核运行 SUSE，则它不能为系统提供任何支持。

---

## 21.7 查错

本节列出使用 GRUB 进行引导的一些常见问题并提供可能解决方案的简短描述。在位于支持数据库 <http://support.novell.com/> 的文章中介绍了其中一些问题。用搜索对话框搜索 *GRUB*、*引导*和*引导加载程序*之类的关键词。

### GRUB 和 XFS

XFS 未在分区引导块中为 *stage1* 预留任何空间。因此，不要指定 XFS 分区作为引导加载程序的位置。此问题可以通过创建单独的引导分区（不使用 XFS 进行格式化）得到解决。

### GRUB 报告 GRUB Geom 错误

当引导系统时，GRUB 将检查连接的硬盘的磁盘空间。有时，BIOS 将返回不一致的信息，GRUB 将报告 GRUB Geom 错误。如果出现这种情况，请使用 LILO 或更新 BIOS。有关安装、配置和维护 LILO 的详细信息，可以在支持数据库中关键字“LILO”下获得。

如果将 Linux 安装在未在 BIOS 中注册的其他硬盘上，GRUB 也会返回此错误消息。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 IDE 和 SCSI 硬盘的系统未引导

安装时，YaST 可能没有正确确定硬盘的引导顺序。例如，GRUB 可能将 `/dev/hda` 视为 `hd0` 并将 `/dev/sda` 视为 `hd1`，虽然 BIOS 中的引导顺序是相反的（SCSI 先于 IDE）。

在这种情况下，在引导进程中借助 GRUB 命令行对硬盘进行更正。在引导系统后，编辑 `device.map` 永久应用新映射。然后，检查 `/boot/grub/menu.lst` 和 `/boot/grub/device.map` 文件中的 GRUB 设备名，并使用以下命令重安装引导加载程序：

```
grub --batch < /etc/grub.conf
```

## 从第二块硬盘引导 Windows

某些操作系统（例如 Windows）只能从第一块硬盘进行引导。如果这样的操作系统安装在第一块硬盘之外的硬盘上，您可以影响相应菜单项的逻辑更改。

```
...
title windows
    map (hd0) (hd1)
    map (hd1) (hd0)
    chainloader (hd1,0)+1
...
```

在此示例中，将从第二块硬盘启动 Windows。出于此目的，请使用 `map` 更改硬盘的逻辑顺序。此更改不会影响 GRUB 菜单文件中的逻辑。因此，必须为 `chainloader` 指定第二块硬盘。

## 21.8 有关详细信息

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



## 特别的系统功能组件

本章提供有关各种软件包、虚拟控制台和键盘布局的信息。讨论诸如 `bash`、`cron` 和 `logrotate` 等软件组件，因为在最后的发行周期中已对这些组件进行了更改或增强。即使这些组件很小或者被认为不太重要，但是用户可能希望更改它们的默认行为，因为这些组件通常是与系统紧密结合的。本章的最后是有关语言和国家/地区特定设置（I18N 和 L10N）的内容。

### 22.1 特殊软件包的相关信息

程序 `bash`、`cron`、`logrotate`、`locate`、`ulimit` 和 `free`，以及文件 `resolv.conf` 对于系统管理员和许多用户是非常重要的。手册页和信息页是命令相关信息的两个有用来源，但是它们并不是始终可用的。GNU Emacs 是一种流行的并且非常容易配置的文本编辑器。

#### 22.1.1 `bash` 包和 `/etc/profile`

Bash 是默认的系统 shell。在用作登录 shell 时，它将读取几个初始化文件。Bash 按照这些文件在列表中出现的顺序处理它们：

1. `/etc/profile`
2. `~/.` 配置文件
3. `/etc/bash.bashrc`

#### 4. ~/.bashrc

在 ~/.profile 或 ~/.bashrc 中进行自定义设置。要确保正确处理这些文件，需要将基本设置从 /etc/skel/.profile 或 /etc/skel/.bashrc 复制到用户的主目录中。建议在更新后从 /etc/skel 复制这些设置。执行以下 shell 命令可防止个人调整的损失：

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

然后从 \*.old 文件将个人调整复制过来。

## 22.1.2 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 22.1 “/etc/crontab 中的项” [388] 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 22.1 /etc/crontab 中的项

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

不能通过调用命令 crontab -e 来编辑 /etc/crontab。必须直接将该文件装载到编辑器中，对其进行修改，然后保存。

许多包将 shell 脚本安装到目录 /etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly 和 /etc/cron.monthly 中，它们的执行是由 /usr/lib/cron/run-crons 控制的。/usr/lib/cron/run-crons 每隔 15 分钟在主表 (/etc/crontab) 中运行一次。这样可以确保在适当的时间运行可能被忽略的进程。

要运行 hourly、daily 或在自定义时间运行其他周期性维护脚本，请删除通常使用 /etc/crontab 项的时戳文件（请参见例 22.2 “/etc/crontab：删除时戳文件” [389]，它删除了每个整点之前的 hourly 和每天早上 2:14 的 daily 等）。

## 例 22.2 /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 `cron.daily` 应该启动的时间。`MAX_NOT_RUN` 的设置确保日常作业被触发运行，即使用户在很长时间里没有在指定的 `DAILY_TIME` 打开计算机。`MAX_NOT_RUN` 的最大值为 14 天。

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

## 22.1.3 日志文件：包 logrotate

有许多系统服务（守护程序）以及内核本身定期将系统状态和特定事件记录到日志文件中。这样，管理员可以定期检查系统在某一时刻的状态，识别错误或故障功能，并精确诊断它们。这些日志文件通常储存在 `FHS` 指定的 `/var/log` 中，文件大小每天都会增长。`logrotate` 包可以帮助控制这些文件的生长。

用文件 `/etc/logrotate.conf` 配置 `logrotate`。特别地，`include` 规范主要配置了其他要读取的文件。在 `/etc/logrotate.d` 中产生日志文件、安装的各个配置文件的程序。例如，随包 `apache2(/etc/logrotate.d/apache2)` 和 `syslogd(/etc/logrotate.d/syslog)` 一起提供的文件。

### 例 22.3 */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。

---

## 22.1.4 **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。

## 22.1.5 ulimit 命令

使用 `ulimit` (*user limits*) 命令，可以对系统资源的使用设置限制并将这些信息显示出来。`ulimit` 尤其适用于限制应用程序可用的内存。使用此命令，可以防止某个应用程序自己占用太多内存，这可能导致系统停顿。

可以对 `ulimit` 使用多个选项。要限制使用内存，请使用 [表 22.1 “ulimit：为用户设置资源”](#) [391] 中列出的选项。

**表 22.1** *ulimit：为用户设置资源*

---

<code>-m</code>	物理内存的最大大小
<code>-v</code>	虚拟内存的最大大小
<code>-s</code>	堆栈的最大大小
<code>-c</code>	核心文件的最大大小
<code>-a</code>	显示限制设置

---

可以在 `/etc/profile` 中创建系统范围的项。在这里可以创建编程人员进行调试所需的 `core` 文件。普通用户不能增加系统管理员在 `/etc/profile` 中指定的值，但可以在 `~/.bashrc` 中进行特殊输入。

### 例 22.4 *ulimit：~/.bashrc 中的设置*

```
# Limits of physical memory:
ulimit -m 98304

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

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

---

### 重要

并非所有 **shell** 都支持 `ulimit` 指令。如果您依赖于这些限制的内含设置，则 **PAM**（例如 `pam_limits`）提供了全面的调整功能。

---

## 22.1.6 free 命令

如果您的目的是查看当前使用了多少 RAM，则 `free` 命令可能会令人产生误解。`/proc/meminfo` 中提供了此信息。目前，使用 Linux 等现代操作系统的用户实际上无需过多地担心内存。可用 RAM 的概念可追溯到统一内存管理之前。可用内存不是好的内存这种说法非常适用于 Linux。因此，Linux 一直在平衡缓存方面下功夫，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）`slab` 缓存。

## 22.1.7 /etc/resolv.conf 文件

系统通过文件 `/etc/resolv.conf` 处理域名解析。请参见第 33 章 域名系统 [555]。

此文件仅由脚本 `/sbin/modify_resolvconf` 进行更新，任何其他程序都没有直接修改 `/etc/resolv.conf` 的权限。只有实施这条规则才能确保系统的网络配置和相关文件保持一致。

## 22.1.8 手册页和信息页

对于某些 GNU 应用程序（如 `tar`），已不再保留手册页。对于这些命令，可使用 `--help` 选项快速查看信息页，其中提供更多深入的说明。`info` 是 GNU 的超文本系统。通过输入 `info info` 可以看到此系统的介绍。通过输入 `emacs -f Info` 可使用 Emacs 查看信息页，也可以在控制台中使用 `info` 直接查看信息页。还可以使用 `tkinfo`、`xinfo` 或 帮助系统来查看信息页。

## 22.1.9 GNU Emacs 的设置

GNU Emacs 是一个复杂的工作环境。下面几节介绍当启动 GNU Emacs 时处理的配置文件。有关详细信息，请参见 <http://www.gnu.org/software/emacs/>。

启动时，Emacs 读取包含用户、系统管理员和经销商的设置的多个文件以进行自定义或预配置。初始化文件 `~/.emacs` 被安装到 `/etc/skel` 中各个用户的主目录中。`.emacs` 又会读取文件 `/etc/skel/.gnu-emacs`。要自定义程序，请（通过 `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`）将 `.gnu-emacs` 复制到用户主目录并在那里进行所需的设置。

`.gnu-emacs` 将文件 `~/.gnu-emacs-custom` 定义为 `custom-file`。如果用户通过 Emacs 中的 `customize` 选项进行设置，则这些设置将保存到 `~/.gnu-emacs-custom` 中。

通过 SUSE® Linux Enterprise，emacs 包将文件 `site-start.el` 安装在目录 `/usr/share/emacs/site-lisp` 中。文件 `site-start.el` 在初始化文件 `~/.emacs` 之前进行装载。除其他作用之外，`site-start.el` 确保自动装载通过 Emacs 扩充包分发的特殊配置文件（例如 `psgml`）。此类型的配置文件也位于 `/usr/share/emacs/site-lisp` 中，总是以 `suse-start-` 开头。本地系统管理员可以在 `default.el` 中指定整个系统范围的设置。

初始化文件下的 EMACS 信息文件中提供了有关这些文件的详细信息：<info:/emacs/InitFile> 此位置还提供了有关如何禁止装载这些文件（如果需要）的信息。

Emacs 的部件被分成多个包：

- 基础包 `emacs`。
- `emacs-x11`（通常已安装）：支持 X11 的程序。
- `emacs-nox`：不支持 X11 的程序。
- `emacs-info`：info 格式的联机文档。
- `emacs-el`：Emacs Lisp 中未编译的库文件。运行时不需要这些库文件。

- 如果需要，可安装众多附加包：emacs-auctex（用于 LaTeX）、psgml（用于 SGML 和 XML）、gnuserv（用于客户机和服务器操作）以及其他。

## 22.2 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。

## 22.3 键盘映射

为了标准化程序的键盘映射，对以下文件进行了更改：

```
/etc/inputrc  
/etc/X11/Xmodmap  
/etc/skel/.Xmodmap  
/etc/skel/.exrc  
/etc/skel/.less  
/etc/skel/.lesskey  
/etc/csh.cshrc  
/etc/termcap  
/usr/lib/terminfo/x/xterm  
/usr/share/X11/app-defaults/XTerm  
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

这些更改只影响使用 terminfo 项的应用程序或其配置文件被直接更改（vi、less 等）的应用程序。不是系统附带的应用程序应该根据这些默认设置进行调整。

在 X 下，可以使用 Ctrl + Shift（右边的）访问组合键 (multikey)。同时可以在 /etc/X11/Xmodmap 中看到对应的项。

可以通过“X 键盘扩展”(XKB) 进行进一步的设置。桌面环境 GNOME (gswitchit) 和 KDE (kxkb) 也使用此扩展。



---

## 提示：更多信息

有关 XKB 的信息，请参见 `/etc/X11/xkb/README` 和那里列出的文档。

有关中文、日文和韩文 (CJK) 输入的详细信息，请参见 Mike Fabian 的网页：  
<http://www.suse.de/~mfabian/suse-cjk/input.html>

---

## 22.4 语言和国家/地区特定的设置

该系统在很大程度上实施了国际化，可通过灵活的方式进行修改以满足本地需要。换句话说，国际化 (*I18N*) 允许特定的本地化 (*L10N*)。I18N 和 L10N 这两个缩写词使用原单词的第一个和最后一个字母，中间的数字表示省略的字母数。

设置是通过文件 `/etc/sysconfig/language` 中定义的 `LC_` 变量进行的。这不仅指本地语言支持，还指消息（语言）、字符集、排序顺序、日期和时间、数字和货币等类别。这些类别中的每一种都可以使用其自己的变量直接定义或使用文件 `language` 中的主变量间接定义（请参见手册页 `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 `shell`，它们代表所列出的类别。下面列出了相关 `shell` 配置文件。可以使用命令 `locale` 显示当前设置。

`RC_LC_ALL`

此变量（如果设置）将覆盖上述变量的值。

`RC_LANG`

如果未设置上述的任何变量，则这是后备变量。默认情况下，只设置 `RC_LANG`。这便于用户输入他们自己的值。

`ROOT_USES_LANG`

`yes` 或 `no` 变量。如果将其设置为 `no`，则 `root` 用户始终在 `POSIX` 环境中工作。

这些变量可通过 YaST `sysconfig` 编辑器进行设置（请参见第 20.3.1 节“使用 YaST Sysconfig 编辑器更改系统配置”[366]）。此类变量的值中包含语言代码、国家/地区代码、编码和修饰符。各部分之间通过特殊字符连接：

```
LANG=<language>[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

## 22.4.1 一些示例

语言和国家/地区代码始终应该一起设置。语言设置遵循 ISO 639 标准（可从 <http://www.evertype.com/standards/iso639/iso639-en.html> 和 <http://www.loc.gov/standards/iso639-2/> 上获取）。国家/地区代码在 ISO 3166（可从 [http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en\\_listp1.html](http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html) 上获取）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。严格来说，此设置目前已过时，因为 UTF-8 也包含欧元符号。该设置仅在应用程序不支持 UTF-8 但支持 ISO-8859-15 时才有用。

SUSEconfig 读取 `/etc/sysconfig/language` 中的变量并将必需的更改写入 `/etc/SuSEconfig/profile` 和 `/etc/SuSEconfig/csh.cshrc`。`/etc/SuSEconfig/profile` 被 `/etc/profile` 读取或用作其数据的来源。`/etc/SuSEconfig/csh.cshrc` 被用作 `/etc/csh.cshrc` 的数据来源。这使设置在整个系统范围内可用。

用户可以通过相应地编译他们的 `~/.bashrc` 覆盖系统默认值。例如，如果不想将整个系统范围的 `en_US` 用于程序消息，请包括 `LC_MESSAGES=es_ES`，这样消息将以西班牙语显示。

## 22.4.2 `~/.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
```

## 22.4.3 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。

## 22.4.4 有关详细信息

- 《GNU C 库参考手册“》中的“区域设置和国际化”一章。”它包含在 glibc-info 中。
- Markus Kuhn 编写的 *Unix/Linux 的 UTF-8 和 Unicode 常见问题解答*，当前位于 <http://www.cl.cam.ac.uk/~mgk25/unicode.html>。
- *Unicode-Howto*，作者 Bruno Haible: /usr/share/doc/howto/en/html/Unicode-HOWTO.html。

# 打印机操作

SUSE Linux Enterprise® 支持用许多类型的打印机进行打印，包括远程网络打印机。打印机可以用 YaST 或手动进行配置。启动和管理打印作业时既可以使用图形实用程序，也可以使用命令行实用程序。如果打印机未能按预期正常工作，请参见第 23.9 节“查错”[413]。

CUPS 是 SUSE Linux Enterprise 中的标准打印系统。CUPS 高度面向用户。在很多情况下，它与 LPRng 兼容或者可以相对方便地进行调整。仅出于兼容性的原因，LPRng 包括在 SUSE Linux Enterprise 中。

可以根据接口（例如 USB 或网络）以及打印机语言对打印机进行区分。购买打印机时，请确认打印机具有一个您的硬件上可用的接口（比如 USB 或并行接口）和合适的打印机语言。可以按照以下三类打印机语言对打印机进行分类：

## PostScript 打印机

Linux 和 Unix 中的内部打印系统使用 PostScript 这种打印机语言生成并处理大部分打印作业。这种语言已经有很长的历史并且非常有效。如果打印机可以直接处理 PostScript 文档而不需要在打印系统中通过附加步骤转换这些文档，则可以降低可能出现的错误的数目。因为 PostScript 打印机购买许可证要花费大量的成本，所以购买这些打印机的花费比不带 PostScript 解释器的打印机要高得多。

## 标准打印机（PCL 和 ESC/P 等语言）

虽然这些打印机语言有相当长的历史，但它们仍在进行扩展以处理打印机中的新功能。对于已知的打印机语言，打印系统可以借助 Ghostscript 将 PostScript 作业转换为相应的打印机语言。这一处理阶段被称为解释。最有名的语言有 PCL（主要是 HP 打印机及其克隆产品使用）和 ESC/P（Epson 打印机使用）。这些打印机语言通常受 Linux 支持，可以生成相当好的打

印效果。Linux 可能不能处理非常新以及非常特别的打印机的一些功能，原因是开放源代码的开发人员可能仍在开发这些功能的代码。除了 HP 开发的 `hpijs` 驱动程序之外，当前尚没有其他打印机制造商开发 Linux 驱动程序并在开发源代码许可证下将这些驱动程序提供给 Linux 经销商。这些打印机中大多数价格适中。

专有打印机（也称作 GDI 打印机）

这些打印机不支持任何常见的打印机语言。这些打印机使用自己的无文档记录打印机语言，该语言在发布新版本时可能发生变化。通常只有 Windows 驱动程序供这些打印机使用。有关更多信息，请参见第 23.9.1 节“**打印机没有标准打印机语言支持**”[413]。

在您购买新打印机之前，请参考以下资源以了解您要购买的打印机的支持情况：

<http://www.linuxprinting.org/>

LinuxPrinting.Org 打印机数据库。

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

Ghostscript 网页

`/usr/share/doc/packages/ghostscript/catalog.devices`

包括的驱动程序的列表。

联机数据库总是显示最新的 Linux 支持状态。但是，Linux 分发只能集成生产时可用的驱动程序。因此，在最新的 SUSE Linux Enterprise 版本发布时，当前标为“完全支持”的打印机不一定具有此状态。这样，数据库不一定可以指出正确的状态，只是提供大致估计而已。

## 23.1 打印系统工作流程

用户创建一个打印作业。该打印作业包含有要打印的数据以及假脱机程序的信息，例如打印机的名称或打印机队列的名称，还可能包括过滤器的信息，例如打印机特定的选项。

每台打印机至少有一个专用打印机队列。假脱机程序储存着队列中的打印作业，直到所需打印机已做好接收数据的准备。打印机准备就绪后，假脱机程序通过过滤器和后端将数据发送到打印机。

过滤器将转换正在打印的应用程序生成的数据（通常为 PostScript 或 PDF，也可能为 ASCII、JPEG 等）特定于打印机的数据（PostScript、PCL、ESC/P 等）。PPD 文件中描述了打印机的功能。PPD 文件包含打印机特定的选项以及在打印机上启用这些选项所需的参数。过滤器系统用于确保用户选择的选项被启用。

如果使用的是 PostScript 打印机，则过滤器系统将数据转换为打印机特定的 PostScript。这样做不需要打印机驱动程序。如果使用的是非 PostScript 打印机，则过滤器系统会使用 Ghostscript 将数据转换为打印机特定的数据。这样做需要一个适合您的打印机的 Ghostscript 打印机驱动程序。后端从过滤器接收打印机特定的数据，然后将其传递到打印机。

## 23.2 连接打印机的方法和协议

可以通过多种方法将打印机连接到系统。CUPS 打印系统的配置不能区分本地打印机和通过网络连接到系统的打印机。在 Linux 中，必须按照打印机制造商提供的手册中所说明的方法连接本地打印机。CUPS 支持串口、USB、并口和 SCSI 连接。有关打印机连接的更多信息，请阅读位于 [http://en.opensuse.org/SDB:CUPS\\_in\\_a\\_Nutshell](http://en.opensuse.org/SDB:CUPS_in_a_Nutshell) 的支持数据库中的文章 *CUPS in a Nutshell*。

► **zseries:** CUPS 或 LPRng 不支持 z/VM 提供的可与 IBM System z 大型主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。

---

## 23.3 安装软件

PPD（PostScript 打印机描述）是描述属性（例如，分辨率）和选项（例如，双面打印单位的可用性）的计算机语言。这些描述对于使用 CUPS 中的各个打印机选项是必需的。如果没有 PPD 文件，打印数据将被以“原始”状态转发到打印机，通常这不是希望出现的情况。在 SUSE Linux Enterprise 安装过程中，将预安装多个 PPD 文件，使系统甚至可以使用不带 PostScript 支持的打印机。

要配置 PostScript 打印机，最佳的方法是获得一个合适的 PPD 文件。包 `manufacturer-PPDs` 中提供许多 PPD 文件，标准安装会自动安装此包。请参见第 23.8.3 节“多种包中的 PPD 文件”[411]和第 23.9.2 节“没有合适的 PPD 文件可用于 PostScript 打印机”[414]。

可以将新 `ppd` 文件储存在目录 `/usr/share/cups/model/` 中或使用 YaST 添加到打印系统中（请参见“用 YaST 添加 PPD 文件”一节[405]）。随后，可以在安装过程中选择 PPD 文件。

如果打印机制造商要求您除修改配置文件之外安装整个软件包，则一定要注意。首先，这种安装将导致丢失 SUSE Linux Enterprise 提供的支持；其次，打印命令将以不同的方式工作，系统可能不再能处理其他制造商的设备。出于此原因，不建议安装制造商软件。

## 23.4 设置打印机

YaST 可用于配置直接连接到您计算机的本地打印机（通常带有 USB 或并行端口），或设置通过网络打印。还可以用 YaST 为您的打印机添加 PPD (PostScript Printer Description) 文件。

### 23.4.1 配置本地打印机

如果检测到未配置的本地打印机，YaST 会自动启动配置它。如果能够自动设置并行或 `usb` 端口并检测到所连接的打印机，则 YaST 能够自动配置打印机。打印机型号也必须列在自动硬件检测期间使用的数据库中。

如果打印机型号未知或无法自动检测出来，请手动配置它。没有自动检测到打印机，可能的原因有两个：

- 打印机无法正确识别自身。这可能适用于很老的设备。试试按“手动配置”一节[403]中所述配置打印机。
- 如果手动配置不起作用，就不可能在打印机和计算机间进行通讯。检查电缆和插头，确保打印机连接正确。如果是这种情况，问题可能并非和打印机相关，而是与 USB 或并行端口有关。



## 手动配置

要手动配置打印机，请在 YaST 控制中心中选择 **硬件 > 打印机**。这将打开 **打印机配置** 主窗口，窗口上部列出了检测到的设备。下半部分列出了目前为止已配置的所有队列（关于打印队列的更多信息，请参见 [第 23.1 节“打印系统工作流程”](#) [400]）。如果未检测到打印机，配置窗口的两部分都将是空的。用 **编辑更改** 列出的打印机的配置，或用 **添加安装未自动检测出来的打印机**。编辑现有的配置会使用 **手动添加本地打印机** [403] 中相同的对话框。

在 **打印机配置** 中，您还可以删除现有的条目。单击 **其他** 将打开具有高级选项的列表。选择 **重新启动检测** 以手动启动自动打印机检测。如果有多台打印机连接到计算机，或者为某打印机配置了多个队列，可标记活动条目为默认设置。**CUPS 专家设置** 和 **更改 IPP 侦听** 是高级配置选项 — 细节请参考 [第 23 章 打印机操作](#) [399]。

### 过程 23.1 手动添加本地打印机

---

#### 提示：YaST 打印测试

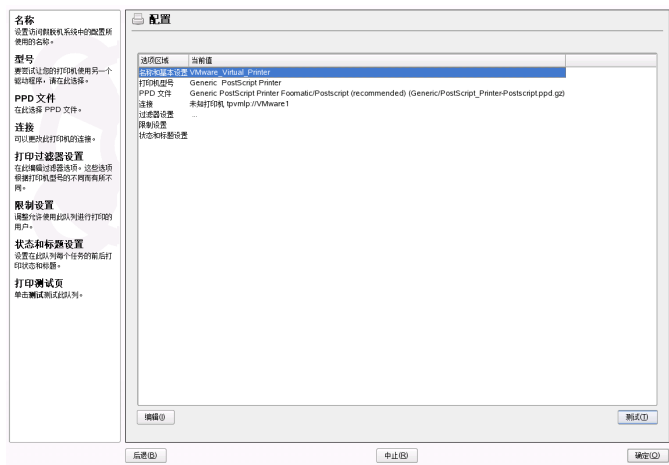
为了确保一切工作正常，应使用 YaST 的打印测试功能对关键配置步骤进行检查。测试页还提供了有关测试的配置的重要信息。如果输出不正常（例如有多页几乎是空白的），则应首先取出所有纸张，然后从 YaST 停止测试，这样便可以停止打印机。

---

- 1 启动 YaST，选择 **硬件 > 打印机** 打开 **打印机配置** 对话框。
- 2 单击 **添加** 打开 **打印机类型** 窗口。
- 3 选择 **直接连接的打印机**。
- 4 选择该打印机要连接的端口（通常是 USB 或并行端口），在下一个配置屏幕中选择设备。建议在此时 **测试打印机连接**。如果出现问题，请选择正确的设备，或选择 **返回** 回到上个对话框。
- 5 在 **队列名称** 中，设置打印队列。必须指定 **打印名称**。建议选择一个方便识别的名称，用该名称您以后可以在应用程序的打印对话框中认出该打印机。用 **打印机说明** 和 **打印机位置** 进一步描述打印机。这是可选的，但如果您有多台打印机连接到一台计算机上，或者安装打印机服务器，就很有用。应选中 **执行本地过滤**，这是本地打印机必需的。

- 6 在打印机型号中用制造商和型号指定打印机。如果未列出您的打印机，您可以尝试制造商列表中的 *UNKNOWN MANUFACTURER*，从型号列表选择适当的标准语言（控制打印机的一组命令）（请参见打印机的文档查找打印机可接受哪种语言）。如果不起作用，请参见“用 YaST 添加 PPD 文件”一节 [405] 了解其他可能的解决方案。
- 7 配置屏幕列出了打印机安装的摘要。从 YaST 模块的开始屏幕编辑现有打印机配置时，也会显示该对话框。

图 23.1 打印机配置摘要



该摘要包含以下条目，您也可以编辑进行修改：

- 名称和基本设置、打印机型号和连接可用于按该步骤更改已有的条目。
- 有关 PPD 文件的细节，请参见“用 YaST 选择备用 PPD 文件”一节 [405]。
- 用过滤器设置微调打印机设置。在这里配置页面大小、颜色模式和分辨率之类的选项。
- 默认设置下，每个用户都能使用打印机。用限制设置列出禁止使用打印机的用户或允许使用它的用户。

- 举例来说，用状态和标题页设置，您可以通过更改其状态取消激活打印机，指定每个作业前后是否打印开始标题页或结束标题页的页面（默认是不打印）。

## 用 YaST 添加 PPD 文件

如果您的打印机未在打印机型号对话框中显示，则缺少您型号的 PPD (PostScript Printer Description) 文件（第 23.3 节“安装软件”[401]中有关于 PPD 文件的更多信息）。用添加 PPD 文件至数据库从本地文件系统或 FTP、HTTP 服务器添加 PPD 文件。

直接从您的打印机供应商或打印机的驱动程序 CD 获得 PPD 文件（细节请参见第 23.9.2 节“没有合适的 PPD 文件可用于 PostScript 打印机”[414]）。另一个 PPD 文件的来源是 <http://www.linuxprinting.org/>，“Linux 打印数据库”。从 linuxprinting.org 下载 PPD 文件时，请记住它总显示最新的 Linux 支持状态，SUSE Linux Enterprise 未必符合。

## 用 YaST 选择备用 PPD 文件

对许多打印机型号，都有几个 PPD 文件可用。配置打印机时，YaST 默认为标有推荐的那个，这是一般规则。要获取某打印机可用的 PPD 文件列表，请在配置中选择 PPD 文件，然后单击编辑。请参见图 23.1 “打印机配置摘要”[404]。

通常没有必要更改 PPD 文件，YaST 选择的 PPD 文件应能产生最佳效果。但是，如果希望彩色打印机只打印黑白两种颜色，使用不支持彩色打印的 PPD 文件最为方便。如果用 PostScript 打印机打印图形时遇到性能问题，从 PostScript PPD 文件换到 PCL PPD 文件（假定您的打印机能读 PCL）可能有帮助。

## 23.4.2 用 YaST 配置网络打印机

无法自动检测到网络打印机。必须使用 YaST 打印机模块手动进行配置。视您的网络设置而定，可以打印到打印服务器（CUPS、LPD、SMB 或 IPX）或直接打印到网络计算机（首选通过 TCP）。关于在您的环境中配置网络打印机的细节，请咨询您的网络管理员。

## 过程 23.2 使用 YaST 配置网络打印机

- 1 启动 YaST 并选择 **硬件 > 打印机**，以打开 **打印机配置** 对话框。
- 2 单击 **添加**，以打开 **打印机类型** 窗口。
- 3 选择 **网络打印机** 以打开一个对话框，并在对话框中指定由网络管理员提供的进一步详细信息。

# 23.5 网络打印机

网络打印机可以支持多种协议，其中某些甚至是同时进行的。虽然大多数支持的协议是标准化的，但某些制造商因为测试尚未正确实施标准的系统或要提供标准中未提供的功能，所以对标准进行了扩展（修改）。于是制造商提供仅用于几个操作系统的驱动程序，解决使用这些系统遇到的困难。不过很少提供 Linux 驱动程序。当前的情况是您在执行操作时不能假定每个协议都可以在 Linux 中正常工作。因此，您可能需要试验不同的选项来实现工作正常的配置。

---

### 重要：远程访问设置

默认情况下，**cupsd** 仅侦听内部网络接口 (**localhost**)。设置 **CUPS** 网络服务器时，您需要调整 **/etc/cups/cupsd.conf** 中的侦听指令以侦听外部网络。

---

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

### 套接字

套接字是指未先执行数据握手就将数据发送到因特网套接字所使用的连接。一些常用的套接字端口号包括 9100 或 35。设备 URI（统一资源标识符）的语法为 **socket://打印机 IP:端口**，例如 **socket://192.168.2.202:9100/**。

### LPD（行式打印机守护程序）

**RFC 1179** 中对经过证明的 **LPD** 协议进行了介绍。在此协议下，在发送实际打印数据之前，将先发送一些与作业相关的数据，例如打印机队列的 **ID**。因此，在为数据传送配置 **LPD** 协议之前，必须指定打印机队列。不同打印机制造商的实施非常灵活，可以接受任何名称作为打印机队列。如果需要，打印机手册应该指出要使用的名称。通常使用 **LPT**、**LPT1**、**LP1** 或类似的

名称。可以在不同 Linux 或 Unix 主机的 CUPS 系统中配置 LPD 队列。LPD 服务的端口号是 515。示例设备 URI 有 `lpd://192.168.2.202/LPT1`。

### IPP（因特网打印协议）

IPP 是一个基于 HTTP 协议的相对较新的 (1999) 协议。使用 IPP，所传送的与作业有关的数据比其他协议要多一些。CUPS 使用 IPP 进行内部数据传送。这是在两个 CUPS 服务器之间转发队列的首选协议。要正确配置 IPP，必须提供打印队列的名称。IPP 的端口号是 631。示例设备 URI 有 `ipp://192.168.2.202/ps` 和 `ipp://192.168.2.202/printers/ps`。

### SMB（Windows 共享）

CUPS 还支持在连接到 Windows 共享的打印机上进行打印。用于此目的的协议是 SMB。SMB 使用端口号 137、138 和 139。示例设备 URI 有 `smb://user:password@workgroup/smb.example.com/printer`、`smb://user:password@smb.example.com/printer` 和 `smb://smb.example.com/printer`。

必须在配置之前确定打印机支持的协议。如果制造商未提供所需的信息，则可以使用命令 `nmap`（附带 `nmap` 包）来猜测协议。`nmap` 检查主机是否有打开的端口。例如：

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

## 23.5.1 使用命令行工具配置 CUPS

除了用 YaST 设置 CUPS 选项，配置网络打印机时，CUPS 也可以用命令行工具进行配置，比如 `lpadmin` 和 `lpoptions`。您需要一个设备 URI，该 URI 由一个后端（例如 USB）和多个参数（例如 `/dev/usb/lp0`）组成。例如，完整的 URI 可能是 `parallel:/dev/lp0`（连接到第一个并行端口的打印机）或 `usb:/dev/usb/lp0`（所检测到的第一个连接到 USB 端口的打印机）。

使用 `lpadmin`，CUPS 服务器管理员可添加、删除或管理类和打印队列。要添加打印队列，请使用以下语法：

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

使用指定的 PPD 文件（`-p`），则设备（`-v`）将用作队列（`-P`）。这意味着如果要手动配置打印机，则必须了解 PPD 文件和设备名称。

不要使用 `-E` 作为第一个选项。对于所有 CUPS 命令，将 `-E` 用作第一个参数设置使用加密连接。要启用打印机，必须使用 `-E`，如下面的示例所示：

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

以下示例配置了网络打印机：

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

有关 `lpadmin` 的更多选项，请参考 `lpadmin(1)` 的手册页。

在系统安装期间，某些选项被设置为默认值。可以为每个打印作业修改这些选项（根据所使用的打印工具）。也可以使用 YaST 来更改这些默认选项。使用命令行工具设置默认选项，如下所示：

### 1 首先，列出所有选项：

```
lpoptions -p queue -l
```

示例：

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

激活的默认选项通过加星号前缀 (\*) 进行标识。

### 2 使用 `lpadmin` 更改选项：

```
lpadmin -p queue -o Resolution=600dpi
```

### 3 检查新设置：

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

普通用户运行 `lpoptions` 时，设置将写到 `~/.lpoptions`。但是，根设置将写到 `/etc/cups/lpoptions`。

## 23.6 图形打印接口

像 `xpp` 这样的工具和 KDE 程序 `KPrinter` 都提供了一个图形界面，用于选择队列以及设置 cups 标准选项和通过 PPD 文件可用的打印机特定的选项。您甚至可

以使用 KPrinter 作为非 KDE 应用程序的标准打印接口。在这些应用程序的打印对话框中，指定 `kprinter` 或 `kprinter --stdin` 作为打印命令。使用的命令取决于应用程序的数据传输方式 — 只需通过尝试看哪个能启动 KPrinter。如果正确设置，应用程序无论何时发布打印作业均应打开 KPrinter 对话框，这样您就可以使用此对话框来选择队列并设置其他打印选项了。这要求应用程序本身的打印设置不能与 KPrinter 的打印设置冲突，而且在启用 KPrinter 后，只能通过它来更改打印选项。

## 23.7 从命令行打印

要从命令行打印，请输入 `lp -d queuefilename`，使用相应的名称替换 `queue` 和 `filename`。

有些应用程序依赖于 `lp` 命令来进行打印。在这种情况下，请在应用程序的打印对话框中输入正确的命令（通常无需指定 `filename`），例如 `lp -d queue`。

## 23.8 SUSE Linux Enterprise 中的特殊功能

已对 CUPS 的许多功能进行了调整以用于 SUSE Linux Enterprise。这里将介绍一些最重要的更改。

### 23.8.1 CUPS 和防火墙

执行默认 SUSE Linux Enterprise 安装后，`SuSEfirewall2` 是活动的，且将外部网络设备配置为在外部区域中（该区域将阻止入站通讯）。使用 CUPS 时，必须调整这些默认设置。在[第 43.4 节“SUSEfirewall2”](#)<sup>[741]</sup>中提供了有关 `SUSEfirewall2` 配置的更多信息。

## CUPS 客户程序

通常 CUPS 客户程序在使用防火墙的网络中的常规工作站上运行。在这种情况下，建议将外部网络设备配置为在内部区域中，这样可以从网络内部访问工作站。

## CUPS 服务器

如果 CUPS 服务器在受防火墙保护的网路中，则应将外部网络设备配置为在防火墙的内部区域中。属于外部区域时，需要打开 TCP 和 UDP 端口 631，以便可以在网路中访问 CUPS 服务器。

## 23.8.2 CUPS 打印服务中的更改

### BrowseAllow 和 BrowseDeny 的一般功能

为 BrowseAllow 和 BrowseDeny 设置的访问权限适用于发送到 cupsd 的所有类型的包。/etc/cups/cupsd.conf 中的默认设置如下所示：

```
BrowseAllow @LOCAL
BrowseDeny All
```

和

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

这样，只有 LOCAL 主机可以访问 CUPS 服务器上的 cupsd。LOCAL 主机是其 IP 地址属于非 PPP 接口（未设置其 IFF\_POINTOPOINT 标志的接口）并且其 IP 地址与 CUPS 服务器属于同一个网络的主机。将立即拒绝来自所有其他主机的包。



## 默认激活 cupsd

在标准安装中，将自动激活 cupsd，从而可以方便地访问 CUPS 网络服务器的队列，而无需执行任何其他手动操作。“[BrowseAllow 和 BrowseDeny 的一般功能](#)”一节 [410]中所述的项目是此功能的重要前提，否则对于 cupsd 自动激活，安全性将不够。

## 23.8.3 多种包中的 PPD 文件

YaST 打印机配置仅使用系统上 `/usr/share/cups/model/` 中安装的 PPD 文件为 CUPS 设置队列。为查找用于某个打印机型号的合适的 ppd 文件，YaST 将在硬件检测过程中确定的供应商和型号与存在于系统上 `/usr/share/cups/model/` 中的所有 PPD 文件中的供应商和型号进行比较。为此，YaST 打印机配置根据从 PPD 文件抽取的供应商和型号信息生成一个数据库。当您从供应商和型号列表中选择打印机时，将收到符合该供应商和型号的 PPD 文件。

仅使用 PPD 文件而不使用其他信息源的配置的优点在于可以随意修改 `/usr/share/cups/model/` 中的 PPD 文件。YaST 打印机配置可以识别更改并重生成供应商和型号数据库。例如，如果您具有 PostScript 打印机，通常您不需要 cups-drivers 包中的 Foomatic PPD 文件或 cups-drivers-stp 包中的 Gimp-Print PPD 文件。而可以将您的 PostScript 打印机的 PPD 文件直接复制到 `/usr/share/cups/model/`（如果它们尚不存在于 manufacturer-ppds 包中）以实现打印机的最佳配置。

### cups 包中的 CUPS PPD 文件

为 PostScript 级别 1 和级别 2 打印机调整的 Foomatic PPD 文件对 cups 包中的通用 PPD 文件进行了补充：

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

## cups-drivers 包中的 PPD 文件

通常，Foomatic 打印机过滤器 `foomatic-rip` 与非 PostScript 打印机的 Ghostscript 一起使用。合适的 Foomatic PPD 文件具有项“`*NickName: ... Foomatic/Ghostscript driver`”和“`*cupsFilter: ... foomatic-rip`”。这些 PPD 文件位于 `cups-drivers` 包中。

如果具有项 `*NickName: ... Foomatic ... (recommended)` 的 Foomatic PPD 文件符合打印机型号并且 `manufacturer-PPDs` 包不包含更合适的 PPD 文件，则 YaST 倾向于使用 Foomatic PPD 文件。

## cups-drivers-stp 包中的 Gimp-Print PPD 文件

Gimp-Print 中的 CUPS 过滤器 `rastertoprinter`（而不是 `foomatic-rip`）可用于许多非 PostScript 打印机。`cups-drivers-stp` 包中提供此过滤器和合适的 Gimp-Print PPD 文件。Gimp-Print PPD 文件位于 `/usr/share/cups/model/stp/` 中并具有项 `*NickName: ... CUPS+Gimp-Print` 和 `*cupsFilter: ... rastertoprinter`。

## manufacturer-PPDs 包中来自打印机制造商的 PPD 文件

`manufacturer-PPDs` 包中包含来自打印机制造商的 PPD 文件，这些文件是在充分自由的许可证下发布的。应该用打印机制造商的合适 PPD 文件配置 PostScript 打印机，因为此文件支持使用 PostScript 打印机的所有功能。如果满足以下条件，YaST 倾向于使用 `manufacturer-PPDs` 包中的 PPD 文件：

- 硬件检测过程中确定的供应商和型号符合 `manufacturer-PPDs` 包的 PPD 文件中的供应商和型号。
- `manufacturer-PPDs` 包中的 PPD 文件是唯一适合该打印机型号的 PPD 文件，或者有一个具有 `*NickName: ... Foomatic/Postscript (recommended)` 项的 Foomatic PPD 文件，该项也符合该打印机型号。

因此，在以下情况下，YaST 不使用 `manufacturer-PPDs` 包中的任何 PPD 文件：

- `manufacturer-PPDs` 包中的 PPD 文件不符合供应商和型号。如果 `manufacturer-PPDs` 包只包含用于类似型号的 PPD 文件（例如，如果某个型号系列中的各个型号没有单独的 PPD 文件，而是在 PPD 文件中以类似于 `Funprinter 1000 series` 的形式指定型号名），则可能发生这种情况。
- 不“建议”使用 `Foomatic PostScript` PPD 文件。这可能是因为该打印机型号在 `PostScript` 方式中不能充分有效地操作。例如，因为打印机内存太少而导致它在这种方式中不可靠，或者因为处理器太弱而导致打印机速度太慢。此外，因为 `PostScript` 支持只作为可选模块提供，所以打印机可能不默认支持 `PostScript`。

如果 `manufacturer-PPDs` 包中的 PPD 文件适合 `PostScript` 打印机，但 `YaST` 由于上述原因不能对其进行配置，则在 `YaST` 中手动选择相应的打印机型号。

## 23.9 查错

下面几节介绍一些最常遇到的打印机硬件和软件问题以及解决或避免这些问题的方法。讨论的主题有 `GDI` 打印机、PPD 文件和端口配置。另外还讨论常见网络打印机问题、打印件问题以及队列处理。

### 23.9.1 打印机没有标准打印机语言支持

这些打印机不支持任何常见的打印机语言，只能使用专门的专有控制系列来进行寻址。因此这些打印机只能用于制造商提供了驱动程序的操作系统版本。`GDI` 是 `Microsoft*` 为图形设备开发的编程接口。通常制造商只提供 `Windows` 的驱动程序，而因为 `Windows` 驱动程序使用 `GDI` 界面，所有这些打印机也被称作 *GDI 打印机*。实际问题不是编程接口，而是这些打印机只能通过相应打印机型号的专用打印机语言进行处理。

某些 `GDI` 打印机可进行切换以 `GDI` 方式或一种标准打印机语言进行操作。请参见打印机手册看这是否可行。有些型号需要有专门的 `Windows` 软件来进行切换（注：`Windows` 打印机驱动程序在通过 `Windows` 进行打印时可能总是将打印机切换回 `GDI` 模式）。对于其他 `GDI` 打印机，还有针对标准打印机语言的扩展模块。

某些制造商为他们的打印机提供专有驱动程序。专有打印机驱动程序的缺点在于不能保证这些驱动程序可用于已安装的打印系统，也不能保证它们适合各种硬件平台。相反，支持标准打印机语言的打印机不依赖于特殊的打印系统版本或特殊的硬件平台。

与其花时间使专有 Linux 驱动程序工作，不如购买一台支持的打印机，这样更经济一些。这可以一次性全部解决驱动程序问题，从而无需安装并配置特殊驱动程序软件，也无需获取由于打印系统中开发的新功能而必须安装的驱动程序更新。

## 23.9.2 没有合适的 PPD 文件可用于 PostScript 打印机

如果 manufacturer-PPDs 包不包含任何用于 PostScript 打印机的合适 PPD 文件，则可以使用打印机制造商提供的驱动程序 CD 上的 PPD 文件或从打印机制造商网页下载合适的 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。

## 23.9.3 并行端口

最安全的方法是将打印机直接连接到第一个并行端口并在 BIOS 中选择以下并行端口设置：

- I/O 地址：378（十六进制）
- 中断：无关
- 模式：Normal、SPP 或 Output Only
- DMA：禁用

如果即便进行了这些设置仍无法对并行端口上的打印机进行寻址，则按照 BIOS 中的设置在 `/etc/modprobe.conf` 中以 `0x378` 形式显式输入 I/O 地址。如果有两个并行端口，分别被设置为 I/O 地址 378 和 278（十六进制），则以 `0x378,0x278` 形式输入这两个端口。

如果中断 7 可用，则可以用 例 23.1 “`/etc/modprobe.conf`：第一个并行端口的中断方式” [415] 中显示的项将其激活。在激活中断方式之前，检查文件 `/proc/interrupts` 看看哪些中断仍在使用中。只显示当前正在使用的中断。根据哪些硬件部件处于活动状态，这可能会有所变化。用于并行端口的中断一定不能被任何其他设备使用。如果您不确定，则使用巡回检测方式，设置 `irq=none`。

### 例 23.1 `/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
```

## 23.9.4 网络打印机连接

### 确定网络问题

将打印机直接连接到计算机。出于测试目的，将该打印机配置为本地打印机。如果打印机可以工作，则问题与网络有关。

### 检查 TCP/IP 网络

TCP/IP 网络和名称解析必须可以正常工作。

### 检查远程可访问性

默认情况下，`cupsd` 仅侦听内部网络接口 (`localhost`)。检查 `/etc/cups/cupsd.conf` 中的侦听指令是否允许从外部网络访问：

```
Listen 192.168.2,*:631
```

### 检查防火墙设置

CUPS 服务器需要在内部防火墙区域中时或者处于外部区域时必须能够通过 UDP 和 TCP 端口 631 发送和接收数据。

### 检查远程 `lpd`

使用以下命令测试是否可以与 `host` 上的 `lpd`（端口 515）建立 TCP 连接：

```
netcat -z host 515 && echo ok || echo failed
```

如果不能建立与 `lpd` 的连接，则 `lpd` 可能不处于活动状态或可能存在基本网络问题。

以 `root` 用户身份使用以下命令查询远程 `host` 上 `queue` 的状态报告（可能非常长），前提是相应的 `lpd` 处于活动状态并且主机接受查询：

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

如果 `lpd` 不响应，则它可能不处于活动状态或可能存在基本网络问题。如果 `lpd` 响应，响应应该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 23.2 “来自 `lpd` 的错误消息” [416] 中的响应，则问题是由远程 `lpd` 引起的。

### 例 23.2 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`

默认情况下，`CUPS` 网络服务器应该每隔 30 秒在 `UDP` 端口 631 上广播其队列。因此，以下命令可用于测试网络中是否有 `CUPS` 网络服务器。

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

如果广播 `CUPS` 网络服务器存在，则输出如例 23.3 “来自 `CUPS` 网络服务器的广播” [416] 所示。

### 例 23.3 来自 `CUPS` 网络服务器的广播

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

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

以下命令可用于测试是否可以与 `host` 上的 `cupsd`（端口 631）建立 `TCP` 连接：

```
netcat -z host 631 && echo ok || echo failed
```

如果不能建立与 `cupsd` 的连接，则 `cupsd` 可能不处于活动状态或可能存在基本网络问题。如果 `cupsd` 处于活动状态并且主机接受查询，`lpstat -h host -l -t` 会返回 `host` 上所有队列的状态报告（可能非常长）。

下一个命令用于测试 *host* 上的 *queue* 是否接受由单个回车字符组成的打印作业。不应打印任何内容。可能会弹出一页空白纸。

```
echo -en "\r" \  
| lp -d queue -h host
```

## 对网络打印机或打印服务器计算机进行查错

当在打印服务器计算机中运行的假脱机程序要处理大量打印作业时，有时会导致出现问题。因为这是由打印服务器计算机中的假脱机程序引起的，所以没什么办法。作为替代解决方法，可以直接通过 **TCP** 套接字对连接到打印服务器计算机的打印机进行寻址来绕过打印服务器计算机中的假脱机程序。请参见第 23.5 节“网络打印机”[406]。

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。

## 23.9.5 打印件有问题但没有错误消息

对于打印系统，打印作业完成的标志是 CUPS 后端完成到接收方（打印机）的数据传送。如果在接收方的进一步处理失败（例如，如果打印机无法打印打印机特定的数据），则打印系统不会对此进行通知。如果打印机无法打印打印机特定的数据，则选择另一个更适合该打印机的 PPD 文件。

## 23.9.6 禁用的队列

如果向接收方传送数据在多次尝试后都失败，则 CUPS 后端（例如 USB 或 socket）向打印系统（向 cupsd）报告一个错误。后端决定在报告数据传送无法完成之前是否继续尝试以及进行多少次尝试。由于继续尝试可能也是徒劳，cupsd 将禁用相应队列的打印。在消除了问题的起因后，系统管理员必须使用 `/usr/bin/enable` 命令重启用打印。

## 23.9.7 CUPS 浏览：删除打印作业

如果 CUPS 网络服务器通过浏览向客户机主机广播其队列并且客户机主机上合适的本地 cupsd 处于活动状态，则客户机 cupsd 接受来自应用程序的打印作业并将它们转发到服务器上的 cupsd。当 cupsd 接受打印作业后，会为该作业指派一个新的作业号。因此，客户机主机上的作业号与服务器上的作业号不同。因为通常都将打印作业立即转发，所以不能用客户机主机上的作业号将其删除，原因是一旦将打印作业转发到服务器 cupsd，客户机 cupsd 就会将打印作业视为已完成。

要删除服务器上的打印作业，请使用命令（例如 `lpstat -h cups.example.com -o`）确定服务器上的作业号（必须在服务器尚未完成该打印作业，即尚未完全将其发送到打印机的情况下）。使用此作业号，可以删除服务器上的打印作业：

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



## 23.9.8 有问题的打印作业和数据传送错误

如果打印进程中将打印机关闭或关闭计算机，则打印作业保留在队列中，当打开打印机或重引导计算机后，打印继续。必须使用 `cancel` 从队列中删除有问题的打印作业。

如果打印作业有问题或主机和打印机之间的通讯出现错误，则打印机会打印出很多张带有乱码的纸张，这是因为它不能正确处理数据。要解决此问题，请执行以下步骤：

- 1 要停止打印，请将所有纸张从喷墨打印机中取出或打开激光打印机的纸盒。高质量的打印机具有一个用于取消当前打印件的按钮。
- 2 打印作业可能仍在队列中，因为只有将作业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` 可以删除打印作业。
- 3 即使已将打印作业从队列中删除，某些数据仍会被传送到打印机。检查 CUPS 后端进程是否仍在为相应的队列运行并将其终止。例如，对于连接到并行端口的打印机，可以使用命令 `fuser -k /dev/lp0` 终止仍在访问打印机（更准确地说是并行端口）的所有进程。
- 4 通过关闭打印机一段时间完全重设置打印机。然后插入纸张并打开打印机。

## 23.9.9 对 CUPS 打印系统进行调试

使用以下通用过程确定 CUPS 打印系统中的问题：

- 1 在 `/etc/cups/cupsd.conf` 中设置 `LogLevel debug`。
- 2 停止 `cupsd`。
- 3 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。

# 使用 udev 进行动态内核设备管理

# 24

从版本 2.6 开始，内核几乎可以添加或删除正在运行的系统中的任何设备。设备状态的更改（无论插入还是删除设备）需要通知用户空间。一旦插入或者发现设备时就需要进行配置。特定设备的用户需要知道此设备的所有状态更改。udev 提供必需的结构来动态维护设备节点文件以及 /dev 目录中的符号链接。udev 规则提供一种将外部设备插入到内核设备事件处理的方法。这使得您可以定制 udev 设备处理，例如通过添加特定脚本作为内核设备处理的一部分来执行，或者请求并导入额外数据从而在设备处理期间进行评估。

## 24.1 /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从头创建的。手动创建或有意更改的文件不会在重引导后保留下来。无论相应内核设备的状态如何都出现在 /dev 目录中的静态文件和目录，可以放置在 /lib/udev/devices 目录中。系统启动时，此目录的内容复制到 /dev 目录，它们与 /lib/udev/devices 中的文件具有相同的所有权和许可权限。

## 24.2 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，内核发送 **uevent** 来通知 **udev** 此情况。

一旦启动后，**udev** 守护程序从 `/etc/udev/rules.d/*.rules` 文件读取并解析所有提供的规则并将它们保存在内存中。如果更改、添加或删除规则文件，则守护程序接收一个事件并更新该规则在内存中的表示。

每个接收到的事件都根据所提供的规则集进行匹配。这些规则可以增加或更改事件环境关键字、为要创建的设备节点请求特定名称、添加指向该节点的符号链接或者添加设备节点创建后运行的程序。从内核 **netlink** 套接字接收驱动程序内核 **uevent**。

## 24.3 驱动程序、内核模块和设备

设备的内核总线驱动程序探测。内核为每个检测到的设备创建内部设备结构，驱动程序内核将 **uevent** 发送到 **udev** 守护程序。总线设备通过特殊格式的 ID 来标识自己，这可以识别设备的类型。通常，这些 ID 由供应商和产品 ID 以及其他特定于子系统的值组成。每个总线都有自己对于这些 ID 的方案，称为 **MODALIAS**。内核获取设备信息，由此组成一个 **MODALIAS** ID 字符串，并将该字符串与事件一起发送。对于 **USB** 鼠标，如下所示：

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

每个设备驱动程序都带有它可以处理的设备的已知别名列表。这个列表包含在内核模块文件中。程序 **depmod** 读取 ID 列表并在内核的 `/lib/modules` 目录中为所有当前可用的模块创建文件 `modules.alias`。使用这种基础结构，模块的装载就如为每个带有 **MODALIAS** 关键字的事件调用 **modprobe** 一样简单。如果调用 **modprobe** `$MODALIAS`，它将组成该设备的设备别名与模块提供的别名相匹配。如果找到匹配的项，则装载该模块。这个通过 **udev** 触发并且自动发生。

## 24.4 引导和启动设备设置

在 `udev` 守护程序运行之前的引导过程中发生的所有设备事件都会丢失，因为处理这些事件的基础结构保存在根文件系统中，并且此时不可用。为了弥补损失，内核为 `sysfs` 文件系统中的一个设备提供一个 `uevent` 文件。通过将 `add` 写入到该文件，内核将再次发送引导时丢失的相同事件。`/sys` 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 鼠标可能不会在早期引导逻辑中初始化，因为驱动程序在那时不可用。此设备发现的事件丢失并且不能为该设备查找内核模块。不是手动搜索可能连接的设备，`udev` 在 `root` 文件系统可用后直接从内核请求所有设备事件，所以 USB 鼠标设备的事件可以再次运行。现在它在装入的 `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。

## 24.5 调试 `udev` 事件

程序 `udevmonitor` 可以用于将驱动程序核心事件和 `udev` 事件处理的计时可视化。

```
UEVENT[1132632714.285362] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UEVENT[1132632714.288166] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UEVENT[1132632714.309485] add@/class/input/input6
UEVENT[1132632714.309511] add@/class/input/input6/mouse2
UEVENT[1132632714.309524] add@/class/usb_device/usbdev2.12
UDEV [1132632714.348966] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UDEV [1132632714.420947] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UDEV [1132632714.427298] add@/class/input/input6
UDEV [1132632714.434223] add@/class/usb_device/usbdev2.12
UDEV [1132632714.439934] add@/class/input/input6/mouse2
```

`UEVENT` 行显示内核已经通过 `netlink` 发送的事件。`UDEV` 行显示已经完成的 `udev` 事件处理程序。计时以微秒为单位显示。`UEVENT` 和 `UDEV` 之间的时间是 `udev` 用于处理此事件或者 `udev` 守护程序延迟执行从而同步此事件与相关以及已运行的事件的时间。例如，硬盘分区的事件总是等待主磁盘设备事件完成，因为分区事件可能依赖主磁盘事件从硬件查询的数据。

`udevmonitor --env` 显示完整的事件环境：

```
UDEV [1132633002.937243] add@/class/input/input7
UDEV_LOG=3
ACTION=add
DEVPATH=/class/input/input7
SUBSYSTEM=input
SEQNUM=1043
PHYSDEVPATH=/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
PHYSDEVBUS=usb
PHYSDEVDRIVER=usbhid
PRODUCT=3/46d/c03e/2000
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.1-2/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0 0 0 0 0
REL=103
```

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

## 24.6 使用 `udev` 规则影响内核设备事件处理

`udev` 规则可以与内核添加到事件本身的属性或者内核导出到 `sysfs` 的任何信息相匹配。规则还可以从外部程序请求其他信息。根据提供的规则匹配每个事件。所有规则都位于 `/etc/udev/rules.d` 目录下。

规则文件中的每一行至少包含一个关键字值对。有两种类型的关键字，匹配关键字和指派关键字。如果所有匹配关键字与它们的值匹配，则应用此规则并将指派关键字指派给特定的值。匹配规则可以指定设备节点的名称、将符号链接指向该节点或者运行特定程序作为事件处理的一部分。如果找不到匹配的规则，则使用默认设备节点名来创建设备节点。在 `udev` 手册页中描述了规则语法和提供用来匹配或导入数据的关键字。

## 24.7 永久设备命名

动态设备目录和 `udev` 规则基础结构可以为所有磁盘设备提供固定名称，而不考虑它们的识别顺序或设备使用的连接。内核创建的每个相应的块设备由工具根据有关特定总线、驱动器类型或者文件系统的特殊知识进行检查。除了动态内核提供的设备节点名，`udev` 还保留各种指向该设备的永久符号链接：

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

## 24.8 已替换的 hotplug 包

先前使用的 `hotplug` 包已经完全替换为 `udev` 和 `udev` 相关的内核基础结构。先前 `hotplug` 基础结构的以下部分已经过时或者功能已经被 `udev` 取代：

```
/etc/hotplug/*.agent
    不再需要或者移动到 /lib/udev

/etc/hotplug/*.rc
    已经替换为 /sys/*/uevent 触发器
```

`/etc/hotplug/blacklist`

替换为 `modprobe.conf` 中的 `blacklist` 选项

`/etc/dev.d/*`

替换为 `udev` 规则 `RUN` 关键字

`/etc/hotplug.d/*`

替换为 `udev` 规则 `RUN` 关键字

`/sbin/hotplug`

替换为侦听 `netlink` 的 `udev`d，仅用在初始 `RAM` 文件系统中，直到根文件系统可以装入后才禁用它

`/dev/*`

替换为动态 `udev` 和 `/lib/udev/devices/*` 中的静态内容

以下文件和目录包含 `udev` 基础结构的关键元素：

`/etc/udev/udev.conf`

主 `udev` 配置文件

`/etc/udev/rules.d/*`

`udev` 事件匹配规则

`/lib/udev/devices/*`

静态 `/dev` 内容

`/lib/udev/*`

从 `udev` 规则调用的帮助程序

## 24.9 有关详细信息

有关 `udev` 基础结构的更多信息，请参见以下手册页：

`udev`

有关 `udev`、关键字、规则和其他重要配置问题的常规信息。

`udevinfo`

`udevinfo` 可以用于从 `udev` 数据库查询设备信息。



## udev

有关 udev 事件管理守护程序的信息。

## udevmonitor

udevmonitor 将内核和 udev 事件序列显示给控制台。这个工具主要用于调试。



# Linux 中的文件系统

SUSE Linux Enterprise® 随许多不同的文件系统发送，包括 ReiserFS、Ext2、Ext3 和 XFS，安装时可从中选择。每个文件系统都有其自身的优缺点，更适合某种场合的需要。为了满足高性能群集情况的要求，SUSE Linux Enterprise Server 包含 OCFS2（Oracle 群集文件系统 2）。

## 25.1 术语

### 元数据

文件系统 - 确保能正确组织和访问磁盘上所有数据的内部数据结构。从本质上讲，它是“有关数据的数据。”几乎每个文件系统都有自己的元数据结构，这也是文件系统为何表现出不同性能属性的部分原因。维护元数据的完整性非常重要，因为如果不这样，则可能无法访问文件系统中的所有数据。

### inode

Inode 包含关于文件的各种信息，包括大小、链接数、指向实际储存文件内容的磁盘块的指针以及创建、修改和访问的日期和时间。

### 日记

在文件系统的上下文中，日记是包含某种日志的磁盘上结构，文件系统将要对本系统中的元数据所做的更改储存在此日志中。日记可以显著缩短 Linux 系统的恢复时间，因为它取消了在系统启动时检查整个文件系统这一冗长的搜索过程。而只是重放日记。

## 25.2 Linux 中的主要文件系统

与两三年前不同，为 Linux 系统选择文件系统不再是花几秒钟就能完成的操作（选择 Ext2 或 ReiserFS）。从版本 2.4 开始，内核提供了多种供选择的文件系统。下面概述了这些文件系统的基本工作原理以及它们的优点。

您一定要记住一点，即没有任何一个文件系统能适合所有应用环境。每个文件系统都有各自的特定优点和缺点，必须将这些因素考虑在内。但是，即使是最复杂的文件系统也不能替代合理的备份策略。

本章中使用的术语 *数据完整性和数据一致性* 并不是指用户空间数据（您的应用程序写入其文件的数据）的一致性。此数据是否一致必须由应用程序本身控制。

---

### 重要：设置文件系统

除非本章另行声明，否则可以使用 YaST 执行设置或更改分区和文件系统所需的所有步骤。

---

### 25.2.1 ReiserFS

作为 2.4 内核版本的正式的重要功能之一，ReiserFS 作为 2.2.x SUSE 的内核增补程序提供，因为 V6.4. ReiserFS 是由 Hans Reiser 和 Namesys 开发团队设计的。ReiserFS 已证明它自己是 Ext2 功能强大的替代系统。ReiserFS 的主要优点是更高的磁盘空间利用率、更高的磁盘访问性能以及更快的崩溃恢复速度。

以下内容是对 ReiserFS 优点的详细说明：

更高的磁盘空间利用率

在 ReiserFS 中，采用一种名为 B<sup>\*</sup>-Tree（平衡树）的结构组织所有数据。这种树结构有助于提高磁盘空间的利用率，这是因为可以将小文件直接储存在 B<sup>\*</sup> 树叶节点而不是其他位置，并且只维护一个指向实际磁盘位置的指针。此外，不按照 1 KB 或 4 KB 的大块来分配储存区，而是根据所需的准确大小进行。另一个优点是 inode 的动态分配。这使得此文件系统比传统的文件系统（例如 Ext2）更灵活，而传统文件系统中的 inode 密度必须在创建文件系统时指定。

更高的磁盘访问性能

对于小文件，文件数据和“stat\_data”(inode)信息经常被储存在相邻的位置。这样通过一个磁盘 I/O 操作就可以访问它们，这意味着只需访问磁盘一次就可以检索到所有需要的信息。

更快的崩溃恢复速度

使用日记来跟踪最近的元数据更改使对文件系统的检查可以很快完成，即使对大型文件系统也是如此。

通过数据日记确保可靠性

ReiserFS 还支持与 Ext3 一节 **第 25.2.3 节“Ext3”** [432] 中介绍过的概念类似的数据日记和有序数据方式。默认方式是 data=ordered，它确保了数据和元数据的完整性，但只对元数据使用日记。

## 25.2.2 Ext2

Ext2 的起源可以追溯到 Linux 历史的早期。1992 年 4 月推出了 Ext2 的前身 Extended File System（扩展文件系统），并将其集成到 Linux 0.96c 中。扩展文件系统经过多次修改，并（像 Ext2 一样）成为多年来最流行的 Linux 文件系统。但随着日记文件系统的创建以及其恢复时间的大大缩短，Ext2 的重要性逐渐降低。

简要总结 Ext2 的优点有助于您了解为什么它以前是（在某些领域现在仍是）许多 Linux 用户最喜欢使用的 Linux 文件系统。

可靠性

Ext2 确实是一个“老古董”，它经历了许多改进和频繁的测试。这可能是人们将其称之为坚如磐石的文件系统的原因。在系统中断后，如果无法彻底卸装文件系统，则 e2fsck 将开始分析文件系统数据。系统使元数据恢复一致的状态，并将挂起的文件或数据块写入指定的目录（名为 lost+found）。与日记文件系统相比，e2fsck 会分析整个文件系统，而不仅仅是最近修改的元数据位。这种操作所花的时间要远远超过检查日记文件系统的日志数据所花的时间。根据文件系统的大小，此过程可能需要半小时或更长时间。因此，对于任何要求高可用性的服务器，不要选择 Ext2。但是，因为 Ext2 不维护日记且使用的内存也少得多，所以其速度常常超过其他文件系统。

可方便地升级

Ext2 的代码是 Ext3 成为广受欢迎的下一代文件系统的坚实基础。它的可靠性和稳定性与日记文件系统的优点完美地结合在一起。

## 25.2.3 Ext3

Ext3 是由 Stephen Tweedie 设计的。与所有其他下一代文件系统不同，Ext3 并没有采用全新的设计原则。它是在 Ext2 的基础上设计的。这两个文件系统密切相关。可以方便地在 Ext2 文件系统中建立 Ext3 文件系统。Ext2 和 Ext3 最重要的区别是 Ext3 支持日记。总之，Ext3 有三个主要优点：

方便并高度可靠地从 Ext2 升级

因为 Ext3 以 Ext2 代码为基础并且共享 Ext2 的磁盘上格式和元数据格式，所以从 Ext2 升级到 Ext3 非常简单。与转换到其他日记文件系统不同，转换到 Ext3 只需要花几分钟，而转换到其他日记文件系统（如 ReiserFS 或 XFS）会相当繁琐（备份整个文件系统并从头开始重创建文件系统）。这样操作还很安全，因为从头重创建整个文件系统很可能会出现错误。考虑到等待升级到日记文件系统的现有 Ext2 系统的数量，就很容易明白为什么 Ext3 对许多系统管理员来说如此重要。从 Ext3 降级到 Ext2 与升级一样简单。只需彻底卸载 Ext3 文件系统，然后作为 Ext2 文件系统重装入即可。

可靠性和性能

某些其他日记文件系统采用“仅元数据”的日记方法。这意味着元数据始终保持一致的状态，但无法自动保证文件系统数据本身一致。Ext3 的设计既可以照顾到元数据，又可以照顾到数据。“照顾”的程度可以自定义。在 `data=journal` 方式中启用 Ext3 可以提供最大的安全性（数据完整性），但因为要将元数据和数据都记入日记，所以可能降低系统的速度。一个相对较新的方法是采用 `data=ordered` 方式，这种方式确保了数据和元数据的完整性，但只对元数据使用日记。文件系统驱动程序收集与一次元数据更新对应的所有数据块。这些数据块在更新元数据之前被写入磁盘中。这样，在不牺牲性能的情况下，元数据和数据的一致性得以实现。第三个可以使用的选项是 `data=writeback`，它允许在将某些数据的元数据提交给日记后，将这些数据写入主文件系统。在性能方面，此选项常被认为是最佳选项。但它在维护内部文件系统完整性的同时，允许以前的数据在系统崩溃并恢复后再次出现在文件中。除非指定了其他选项，否则运行 Ext3 时，`data=ordered` 为默认设置。

## 25.2.4 将 Ext2 文件系统转换为 Ext3

要将 Ext2 文件系统转换为 Ext3，请按如下所示继续：

- 1 通过作为 root 运行 `tune2fs -j` 创建 Ext3 日志。此命令将用默认参数创建 Ext3 日记。

要自己确定日志的大小和所在的设备，请改为运行 `tune2fs -j`，同时带所需的日志选项 `size=` 和 `device=`。可以在 `tune2fs` 程序的 `tune2fs` 手册页中获得关于此程序的更多信息。

- 2 要确保正确地识别 Ext3 文件系统，请作为 root 编辑文件 `/etc/fstab`，将为对应的分区指定的文件系统类型从 `ext2` 更改为 `ext3`。此更改将在下次重引导后生效。
- 3 要引导设置为 Ext3 分区的根文件系统，请将模块 `ext3` 和 `jbd` 包含在 `initrd` 中。要执行此操作，请作为 root 编辑 `/etc/sysconfig/KERNEL`，将 `ext3` 和 `jbd` 添加到 `INITRD_MODULES` 变量。保存更改后，请运行 `mkinitrd` 命令。这将构建一个新的 `initrd`，并准备使用它。

## 25.2.5 XFS

SGI 在 20 世纪 90 年代初开始开发 XFS，最初计划将 XFS 作为 IRIX OS 的文件系统。开发 XFS 的目的是创建一个高性能的 64 位日记文件系统来满足当今对计算能力的极高要求。XFS 适合操纵大型文件，在高端硬件上表现优异。但即使是 XFS 也有缺点。与 ReiserFS 类似，XFS 非常注重元数据的完整性，但不太注重数据的完整性。

快速回顾 XFS 的关键功能将解释为什么此文件系统被证明是在高端计算方面其他日记文件系统的强大竞争对手。

通过使用分配组实现高伸缩性

在创建 XFS 文件系统时，文件系统底层的块设备被分成 8 个或 8 个以上相同大小的线性区域。这些线性区域被称为分配组。每个分配组管理自己的 inode 和可用空间。实际上，可以将分配组看作文件系统上的文件系统。因为分配组相互独立，所以内核可同时对多个分配组进行寻址。此功能对 XFS 优异的可伸缩性非常关键。独立分配组的概念自然适合多处理器系统的需要。

通过有效管理磁盘空间获得高性能

可用空间和 inode 是由分配组内的 B<sup>+</sup> 树处理的。使用 B<sup>+</sup> 树将大大增强 XFS 的性能和可伸缩性。XFS 使用延迟分配。它通过将进程分成两部分来处理分配。将挂起事务储存在 RAM 中并保留适当数量的空间。XFS 仍不决定应储存数据的准确位置（指出文件系统块）。此决定将被延迟到最后的时刻。某些生存期很短的临时数据可能永远不会被储存到磁盘上，这是因为在 XFS 决定保存它们的实际位置时，这些数据可能已经过时了。这样，XFS 增强了写性能，并减少了文件系统碎片的数目。因为延迟分配引起写事件的频率比其他文件系统引起写事件的频率要低，所以如果写操作期间发生系统崩溃，则数据丢失可能会更加严重。

进行预分配以避免文件系统碎片

在将数据写入文件系统前，XFS 保留（预分配）文件所需的可用空间。这样会大大减少文件系统碎片的数目。因为文件的内容不会分散在整个文件系统中，所以性能得以提高。

## 25.2.6 Oracle Cluster File System 2

OCFS2 是一个日志文件系统，此文件系统是为群集设置量身定制的。与标准的单节点文件系统（如 Ext3）相反，OCFS2 能够管理多个节点。OCFS2 允许跨共享储存区扩展文件系统，如 SAN 或多路径安装。

OCFS2 设置中的每个节点都具有对所有数据的并发读写访问权。这需要 OCFS2 支持群集，表示 OCFS2 必须包含一种方法来确定群集由哪些节点组成以及这些节点是否真正存在并可用。为了计算群集的成员资格，OCFS2 包含一个节点管理器 (NM)。为了监视群集中节点的可用性，OCFS2 包含一个简单的检测信号实施工具。为避免各节点直接访问文件系统而导致的混乱，OCFS2 还包含一个锁管理器，DLM（分布式锁管理器）。节点之间的通讯通过基于 TCP 的消息交换系统处理。

OCFS2 的主要功能和优点包括：

- 元数据缓存和日记
- 异步和直接 I/O 支持已提高了数据库性能的数据库文件
- 支持最大为 4 KB 的多块大小（每个卷可以有不同块大小），支持最大为 16 TB 的卷大小
- 跨节点的文件数据一致性



- 支持最多 255 个群集节点

有关 OCFS2 的进一步详细信息，请参见第 14 章 *Oracle Cluster File System 2* [261]。

## 25.3 其他一些支持的文件系统

表 25.1 “Linux 中的文件系统类型” [435] 对 linux 支持的其他一些文件系统进行了总结。支持这些文件系统主要是为了确保与不同类型的媒体或异操作系统实现兼容和数据交换。

**表 25.1** *Linux 中的文件系统类型*

cramfs	压缩的 ROM 文件系统：一种经压缩的只读 ROM 文件系统。
hpfs	高性能文件系统：IBM OS/2 标准文件系统，只在只读方式下支持此文件系统。
iso9660	CD-ROM 上的标准文件系统。
minix	此文件系统源自有关操作系统的学术项目，是在 Linux 中使用的第一个文件系统。目前，它被用作软盘的文件系统。
msdos	<i>fat</i> （最初由 DOS 使用的文件系统）现在已被多种操作系统采用。
ncpfs	通过网络装入 Novell 卷的文件系统。
nfs	网络文件系统：在此文件系统中，可以将数据储存在网络中的任何计算机上，并可以通过网络授予访问权限。
smbfs	<i>Windows</i> 等产品使用服务器消息块来支持通过网络进行文件访问。
sysv	在 SCO UNIX、Xenix 和 Coherent（用于个人电脑的商用 UNIX 系统）上使用。

ufs	供 BSD、SunOS 和 NeXTSTEP 使用。只在只读方式下支持此文件系统。
umsdos	<i>MSDOS 上的 UNIX</i> ：应用于常规 fat 文件系统上，通过创建特殊文件获得 UNIX 功能（权限、链接和长文件名）。
vfat	<i>虚拟 FAT</i> ：fat 文件系统的扩展（支持长文件名）。
ntfs	<i>Windows NT 文件系统</i> ，只读。

## 25.4 Linux 中对大型文件的支持

最初，Linux 支持的最大文件大小为 2 GB。在大量使用多媒体之前，只要用户不在 Linux 中操纵大型数据库，这个大小已足够了。但由于服务器计算变得越来越重要，所以当使用一组应用程序必须使用的新接口时，对内核和 C 库进行了修改以支持大小大于 2 GB 的文件。当今，几乎所有的主要文件系统都提供 LFS 支持，从而允许您执行高端计算。[表 25.2“文件系统的最大大小（磁盘上格式）”](#) [436] 概述了 Linux 文件和文件系统的当前限制。

**表 25.2** 文件系统的最大大小（磁盘上格式）

文件系统	文件大小（字节）	文件系统大小（字节）
Ext2 或 Ext3（1 KB 块大小）	2 <sup>34</sup> (16 GB)	2 <sup>41</sup> (2 TB)
Ext2 或 Ext3（2 KB 块大小）	2 <sup>38</sup> (256 GB)	2 <sup>43</sup> (8 TB)
Ext2 或 Ext3（4 KB 块大小）	2 <sup>41</sup> (2 TB)	2 <sup>44</sup> -4096（16 TB-4096 字节）
Ext2 或 Ext3（8 KB 块大小） （系统采用 8 KB 的页，与 Alpha 类似）	2 <sup>46</sup> (64 TB)	2 <sup>45</sup> (32 TB)
ReiserFS v3	2 <sup>46</sup> (64 TB)	2 <sup>45</sup> (32 TB)

文件系统	文件大小（字节）	文件系统大小（字节）
XFS	$2^{63}$ (8 EB)	$2^{63}$ (8 EB)
NFSv2（客户端）	$2^{31}$ (2 GB)	$2^{63}$ (8 EB)
NFSv3（客户端）	$2^{63}$ (8 EB)	$2^{63}$ (8 EB)

**重要：Linux 内核限制**

表 25.2 “文件系统的最大大小（磁盘上格式）” [436]介绍了有关磁盘上格式的限制。2.6 内核自身的大小限制同样适用于其处理的文件和文件系统大小。限制如下：

文件大小  
在 32 位系统上，文件不能超过 2 TB（ $2^{41}$  字节）。

文件系统大小  
文件系统最大可以为  $2^{73}$  字节大小。但是，目前可用的硬件尚不会超出这一限制。

# 25.5 有关详细信息

上面介绍的每个文件系统项目都有自己的主页，可以在其中找到邮件列表信息、更多文档和常见问题解答。

- <http://e2fsprogs.sourceforge.net/>
- <http://www.zipworld.com.au/~akpm/linux/ext3/>
- [http://chichkin\\_i.zelnet.ru/namesys/](http://chichkin_i.zelnet.ru/namesys/)
- <http://oss.sgi.com/projects/xfst/>
- <http://oss.oracle.com/projects/ocfs2/>

可以在 *IBM developerWorks* 中找到关于 linux 文件系统的多部分综合性教程，网址为：<http://www-106.ibm.com/developerworks/library/l-fs>

.html Wikipedia 项目 [http://en.wikipedia.org/wiki/Comparison\\_of\\_file\\_systems#Comparison](http://en.wikipedia.org/wiki/Comparison_of_file_systems#Comparison) 中有文件系统的深入比较（不只是 Linux 文件系统）。

## X 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® 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 8.6 节“网络设备”](#) [148]。

---

### 26.1 手动配置 X Window 系统

默认设置下，X Window 系统以 [第 8.14 节“SaX2”](#) [172] 中所述 SaX2 界面配置。或者也可以通过编辑其配置文件手动配置它。

---

**警告：错误的 X 配置可能会损坏您的硬件。**

配置 X 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 的创建者不对导致的任何损坏负责。这里提供的信息已经仔细斟酌，但不能保证所提供的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**

用 `X -configure` 配置您的 X 安装（如果之前尝试 SUSE Linux Enterprise 的 **SaX2** 失败）。如果您的安装涉及专用的仅二进制驱动程序，`X -configure` 不起作用。

---

下面小节介绍配置文件 `/etc/X11/xorg.conf` 的结构。它由多个部分组成，每个部分处理配置的某个特定方面。每个部分都以关键字 `Section` `<designation>` 开头，以 `EndSection` 结尾。以下惯例适用于所有章节：

```
Section "designation"
    entry 1
    entry 2
    entry n
EndSection
```

**表 26.1 “`/etc/X11/xorg.conf` 中的部分”** [440]中列出了可用的部分类型。

**表 26.1** *`/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	服务器应载入的模块列表。
InputDevice	此部分配置输入设备，例如键盘和特殊输入设备（触摸板、游戏杆等）。此部分的重要参数有 <code>Driver</code> 以及定义 <code>Protocol</code> 和 <code>Device</code> 的选项。对连接到计算机的每个设备，通常都有一个 <code>InputDevice</code> 部分。
Monitor	使用的显示器。此部分的重要元素是标识符（稍后在 <code>Screen</code> 定义中引用）、刷新率 <code>VertRefresh</code> 和同步频率限制（ <code>Horizsync</code> 和 <code>VertRefresh</code> ）。这些设置采用的单位为 MHz、kHz 和 Hz。通常，服务器拒绝不符合监视

类型	含义
	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）。
Device	特定的图形卡。系统通过其描述性名称来引用图形卡。
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 (Virtual) 的大小、ViewPort 以及此屏幕所用的 Modes。
ServerLayout	单个或多头配置的布局。此部分将输入设备 InputDevice 和显示设备 Screen 绑定在一起。
DRI	提供 Direct Rendering Infrastructure (DRI) 的信息。

下面详细介绍 Monitor、Device 和 Screen。X.Org 和 xorg.conf 的手册页提供了有关其他部分的详细信息。

xorg.conf 中可以存在多个不同的 Monitor 和 Device 部分。甚至可以存在多个 Screen 部分。ServerLayout 部分确定使用其中哪个部分。

## 26.1.1 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 26.1 “文件 /etc/X11/xorg.conf 的 Screen 部分” [442] 类似。

## 例 26.1 文件 `/etc/X11/xorg.conf` 的 `Screen` 部分

```
Section "Screen"❶
    DefaultDepth 16❷
    SubSection "Display"❸
        Depth 16❹
        Modes "1152x864" "1024x768" "800x600"❺
        Virtual 1152x864❻
    EndSubSection
    SubSection "Display"
        Depth 24
        Modes "1280x1024"
    EndSubSection
    SubSection "Display"
        Depth 32
        Modes "640x480"
    EndSubSection
    SubSection "Display"
        Depth 8
        Modes "1280x1024"
    EndSubSection
    Device "Device[0]"
    Identifier "Screen[0]"❼
    Monitor "Monitor[0]"
EndSection
```

- ❶ Section 确定该部分的类型，在本示例中是 `Screen`。
- ❷ `DefaultDepth` 决定默认使用的颜色深度（除非明确指定其他颜色深度）。
- ❸ 对每种颜色深度指定不同的 `Display` 子部分。
- ❹ `Depth` 决定对本组 `Display` 设置使用的颜色深度。可用值有 8、15、16、24 和 32，尽管并非所有 X 服务器模块或分辨率都可以支持所有这些值。
- ❺ `Modes` 部分由可能的屏幕分辨率列表组成。X 服务器从左到右检查此列表。对于每个分辨率，X 服务器均会在 `Modes` 部分中搜索合适的 `Modeline`。`Modeline` 取决于监视器和图形卡的功能。`Monitor` 设置确定最终的 `Modeline`。

找到的第一个分辨率是 `Default mode`。使用 `Ctrl+Alt++`（在数字小键盘上）向右切换到列表中的下一个分辨率。使用 `Ctrl+Alt+-`（在数字小键盘上）切换到上一个。这使您能够在 X 运行时改动分辨率。

- ❻ 包含 `Depth 16` 的 `Display` 子部分的最后一行指出了虚拟屏幕的大小。虚拟屏幕的最大可能大小取决于图形卡中安装的内存量和所需的颜色深度，而不取决于监视器的最大分辨率。如果忽略此行，虚拟分辨率就是物理分



分辨率。因为目前的图形卡都具有大量视频内存，所以您可以创建非常大的虚拟桌面。但是，如果您将大部分视频内存用于虚拟桌面，则可能不能再使用 3D 功能。例如，如果图形卡有 16 MB 视频 RAM，则当采用 8 位颜色深度时，虚拟屏幕最多可以有 4096x4096 个像素。但建议不要将所有内存用于虚拟屏幕，因为图形卡的内存还要用于多种字体和图形缓存，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。

## 26.1.2 Device 部分

Device 部分描述特定的图形卡。您可以在 xorg.conf 中包含任意多个设备项，前提是要使用关键字 Identifier 对这些项的名称进行区分。如果您安装了多个图形卡，通常按顺序对这些部分进行编号。第一个设备称为 Device[0]，第二个设备称为 Device[1]，依此类推。以下文件是从安装有 Matrox Millennium PCI 图形卡（由 SaX2 配置）的计算机的 Device 部分摘出的一段：

```
Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"❶
    Driver         "mga"❷
    Identifier     "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection
```

- ❶ BusID 是指安装图形卡的 PCI 或 AGP 插槽。它与使用命令 lspci 显示的 ID 相匹配。X 服务器需要采用十进制形式的详细信息，但 lspci 以十六进制形式显示这些信息。BusID 的值由 SaX2 自动检测。
- ❷ Driver 的值由 SaX2 自动设置，指定哪个驱动程序用于您的图形卡。如果此卡是 Matrox Millennium，则将驱动程序模块称为 mga。然后，X 服务器通过 drivers 子目录的 Files 部分中定义的 ModulePath 进行搜索。在标准安装中，是 /usr/X11R6/lib/modules/drivers 或 /usr/X11R6/lib64/modules/drivers 目录。然后将 \_drv.o 添加到名称中。因此，对于 mga 驱动程序，将装载驱动程序文件 mga\_drv.o。

还可以通过其他选项影响 X 服务器或驱动程序的行为。在 Device 部分中设置的选项 `sw_cursor` 就是这方面的一个示例。此选项取消激活硬件鼠标光标并使用软件显示鼠标光标。根据驱动程序模块，有不同的选项可用，它们位于目录 `/usr/share/doc/package_name` 中驱动程序模块的说明文件中。通常还可以在手册页（`man xorg.conf`、`man X.Org` 和 `man 4 chips`）中查看有效的选项。

如果图形卡有多个视频连接器，可以将这一个卡的不同设备配置为单一视图。使用 `SaX2` 以这种方式对图形接口进行设置。

## 26.1.3 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）。

---

### 警告

除非您对监视器和图形卡功能有深入了解，否则建议不要更改 `modelien`，因为这可能严重损坏监视器。

---

尝试过开发自己的监视器说明的人应对 `/usr/X11R6/lib/X11/doc/` 中的文档非常熟悉（必须安装 `xorg-x11-doc` 包）。

现在，很少需要手动指定方式行。如果您使用的是最新的多频同步监视器，则通常由 X 服务器通过 `DDC` 直接从监视器中读取允许的频率和最佳分辨率，如 `SaX2` 配置一节所述。如果由于某种原因无法执行此操作，请使用 X 服务器中包含的 `VESA` 方式之一。这种方式可用于几乎所有图形卡和监视器的组合。

## 26.2 安装和配置字体

在 SUSE Linux Enterprise 中安装附加字体非常简单。只需要将字体复制到位于 X11 字体路径中的任何目录即可（请参见第 26.2.1 节“X11 核心字体”[446]）。安装目录应是 `/etc/fonts/fonts.conf` 中配置的目录的子目录（请参见第 26.2.2 节“Xft”[447]），或用 `/etc/fonts/suse-font-dirs.conf` 包含到此文件中。

以下是 `/etc/fonts/suse-font-dirs.conf` 中的摘录。因为此文件被链接到目录 `/etc/fonts/conf.d`（由 `/etc/fonts/fonts.conf` 包含），所以它包含在该配置中。在此目录中，以两位数字开头的所有文件或符号链接均由 `fontconfig` 装载。有关此功能的更详细描述，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>
<dir>~/.fonts/kde-override</dir>
<include ignore_missing="yes">suse-font-dirs.conf</include>
```

`/etc/fonts/suse-font-dirs.conf` 会自动生成，以引入随（多为第三方）应用程序附送的字体，如 OpenOffice.org、Java 或 Adobe Acrobat Reader。`/etc/fonts/suse-font-dirs.conf` 的典型条目外观如下：

```
<dir>/usr/lib/ooo-2.0/share/fonts</dir>
<dir>/usr/lib/ooo-2.0/share/fonts/truetype</dir>
<dir>/usr/lib/jvm/java-1.5.0-sun-1.5.0_update10/jre/lib/fonts</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font/PFM</dir>
```

要在整个系统安装其他字体，请手动将字体文件复制至适当的目录（如 `root`），例如 `/usr/share/fonts/truetype`。或者，可以使用 KDE 控制中心中的 KDE 字体安装程序来执行此任务。结果是一样的。

您还可以创建符号链接，而不复制实际字体。例如，如果已装入的 Windows 分区上的字体已获得许可并要使用，则可能要执行此操作。随后，运行 `SuSEconfig --module fonts`。

`SuSEconfig --module fonts` 执行脚本 `/usr/sbin/fonts-config`，该脚本处理字体的配置。有关此脚本的更多信息，请参见其手册页 (`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* 及 *fontconfig* 系统。下面几节简要介绍这两种系统。

## 26.2.1 X11 核心字体

目前，X11 核心字体系统不仅支持位图字体，还支持可缩放字体（例如 Type1 字体）、TrueType 以及 OpenType 字体。X11 核心字体系统只在没有反锯齿处理和子像素显示的情况下支持可缩放字体，并且装载许多语言具有字形的大型可缩放字体可能需要较长的时间。也支持 Unicode 字体，但使用它们的速度比较慢，而且需要更多内存。

X11 核心字体系统带有一些固有缺陷。它已经过时，而且不再能以有意义的方式扩展。虽然为了实现向后兼容而不得不保留 X11 核心字体系统，但应尽可能使用更先进的 Xft 和 fontconfig 系统。

为了执行相应的操作，X 服务器需要知道它可使用的字体以及在系统中的哪些位置可找到这些字体。这由 `FontPath` 变量来处理，该变量包含所有有效系统字体目录的路径。在其中每个目录中，一个名为 `fonts.dir` 的文件会列出此目录中的可用字体。`FontPath` 由 X 服务器在启动时生成。它将在配置文件 `/etc/X11/xorg.conf` 的每个 `FontPath` 项中搜索有效的 `fonts.dir` 文件。这些项位于 `Files` 部分。使用 `xset q` 可显示实际的 `FontPath`。运行时也可以使用 `xset` 更改该路径。要添加其他路径，请使用 `xset+fp <path>`。要删除不需要的路径，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 shell 启动 `SuSEconfig--module fonts` 时，此命令才能发挥作用。实现此操作最简单的方法是通过输入 `su` 和 `root` 密码获得 `root` 权限。`su` 会将启动 X 服务器的用户的访问权限转移到 `root` 外壳。要检

查是否正确安装了字体以及是否可以通过 X11 核心字体系统使用字体，请使用命令 `xlsfonts` 列出所有可用字体。

默认情况下，SUSE Linux Enterprise 使用 UTF-8 区域设置。因此，应首选 Unicode 字体（`xlsfonts` 输出中以 `iso10646-1` 结尾的字体名称）。可以使用 `xlsfonts | grep iso10646-1` 列出所有可用的 Unicode 字体。几乎所有在 SUSE Linux Enterprise 中可用的 unicode 字体都至少包括欧洲语言所需的字形（以前编码为 `iso-8859-*`）。

## 26.2.2 Xft

从一开始，Xft 的编程人员就确保该系统可以很好地支持可缩放字体（包括反锯齿处理）。如果使用 Xft，则是由使用字体的应用程序显示字体，而不是像 X11 核心字体系统中由 X 服务器显示字体。采用这种方式，相应的应用程序能够访问实际字体文件并完全控制如何显示字形。这就为正确显示多种语言的文本奠定了基础。直接访问字体文件对于用于打印的嵌入字体非常有用，因为这样可以确保打印输出与屏幕输出看上去完全一样。

在 SUSE Linux Enterprise 中，两个桌面环境 KDE 和 GNOME、Mozilla 和许多其他应用程序均已默认使用 Xft。使用 Xft 的应用程序在数目上已经超过了使用以前的 X11 核心字体系统的应用程序。

Xft 使用 `fontconfig` 库来查找字体并影响字体的显示方式。`fontconfig` 的属性由全局配置文件 `/etc/fonts/fonts.conf` 和用户特定的配置文件 `~/.fonts.conf` 控制。所有这些 `fontconfig` 配置文件的开头必须是

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

并且结尾必须是

```
</fontconfig>
```

要添加用于搜索字体的目录，请追加类似下面内容的一行：

```
<dir>/usr/local/share/fonts/</dir>
```

但通常没有必要这样做。默认情况下，已经在 `/etc/fonts/fonts.conf` 中输入了用户特定的目录 `~/.fonts`。因此，要安装附加字体，只需将它们复制到 `~/.fonts` 即可。

您还可以插入用来确定字体外观的规则。例如，输入

```
<match target="font">
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

来禁用所有字体的反锯齿处理，或输入

```
<match target="font">
  <test name="family">
    <string>Luxi Mono</string>
    <string>Luxi Sans</string>
  </test>
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

来禁用特定字体的反锯齿处理。

默认情况下，大多数应用程序使用字体名称 sans-serif（或等效的 sans）、serif 或 monospace。它们不是真正的字体，而只是可解析为合适的字体（取决于语言设置）的别名。

用户可以方便地将规则添加到 ~/.fonts.conf 中，以将这些别名解析为他们喜欢的字体：

```
<alias>
  <family>sans-serif</family>
  <prefer>
    <family>FreeSans</family>
  </prefer>
</alias>
<alias>
  <family>serif</family>
  <prefer>
    <family>FreeSerif</family>
  </prefer>
</alias>
<alias>
  <family>monospace</family>
  <prefer>
    <family>FreeMono</family>
  </prefer>
</alias>
```

因为几乎所有应用程序都默认使用这些别名，所以这几乎影响到整个系统。这样，您可以方便地在几乎所有位置都使用自己喜欢的字体，而无需在各个应用程序中修改字体设置。

使用 `fc-list` 命令可以查看已安装了哪些字体以及哪些字体可用。例如，命令 `fc-list` 返回所有字体的列表。要查看可用的可缩放字体 (`:scalable=true`) 中有哪些包含希伯来语 (`:lang=he`) 所需的所有字形、它们的字体名称 (`family`)、字型 (`style`)、粗细 (`weight`) 以及包含这些字体的文件的名称，请输入以下命令：

```
fc-list ":lang=he:scalable=true" family style weight
```

此命令的输出类似于下面：

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

可以使用 `fc-list` 查询的重要参数包括：

表 26.2 *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。

参数	含义和可能值
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。
pixelsize	以像素为单位表示的字体大小。与 fc-list 一起使用时，此选项仅对位图字体有意义。

## 26.3 更多信息

安装包 `xorg-x11-doc` 和 `howtoenh` 以获得关于 X11 的详细信息。有关 X11 开发的更多信息，请参见该项目的主页：<http://www.x.org>。



## 通过 PAM 进行身份验证

Linux 在身份验证进程中使用 PAM（可插拔身份验证模块）作为用户和应用程序之间的中间层。PAM 模块在系统范围内可用，所以任何应用程序都可以请求这些模块。本章介绍模块化身份验证机制的工作原理和配置方法。

系统管理员和编程人员经常要将访问限制在系统的某些部分或限制对应用程序某些功能的使用。如果不使用 PAM，则每次引入新的身份验证机制（例如 LDAP、Samba 或 Kerberos）时都必须对应用程序进行调整。但是，此过程相当耗费时间并且容易出现错误。避免这些缺点的一种方法是将应用程序从身份验证机制中分开并将身份验证委托给集中管理的模块。当需要使用最近所需的身份验证方案时，只要调整或编写合适的 PAM 模块供相关程序使用即可。

依赖于 PAM 机制的每个程序在目录 `/etc/pam.d/programname` 中都有自己的配置文件。这些文件定义用于身份验证的 PAM 模块。另外，`/etc/security` 下有用于 PAM 模块的全局配置文件，这些文件定义这些模块的精确行为（例如 `pam_env.conf`、`pam_pwcheck.conf`、`pam_unix2.conf` 和 `time.conf`）。使用 PAM 模块的每个应用程序实际上调用一组 PAM 函数，这些函数随后将处理不同配置文件中的信息并将结果返回到调用这些函数的应用程序。

### 27.1 PAM 配置文件的结构

PAM 配置文件中的每一行最多包含 4 列：

```
<Type of module> <Control flag> <Module path> <Options>
```

PAM模块是成批处理的。不同类型的模块具有不同的用途。例如一个模块检查密码，另一个模块校验访问系统的位置，第三个模块读取用户特定的设置。PAM 可以识别四种不同类型的模块：

#### `auth`

这种类型的模块的用途是检查用户的真实性。传统上，这是通过查询密码完成的，但也可以借助芯片卡或通过生物测定学（指纹或虹膜扫描）实现。

#### `account`

这种类型的模块检查用户是否具有使用所请求服务的一般权限。例如，应执行这种检查以确保任何人都不能使用失效帐户的用户名进行登录。

#### `password`

这种类型的模块的用途是启用身份验证令牌的更改。在大多数情况下，这是密码。

#### `session`

这种类型的模块负责管理和配置用户会话。在身份验证前后启动这些模块以在系统日志中注册登录尝试并配置用户的特定环境（邮件帐户、用户主目录、系统限制等）。

第二列包含的控制标志影响所启动模块的行为：

#### `required`

在进行身份验证之前，必须先成功处理带有此标志的模块。在处理带有 `required` 标志的模块失败后，将继续处理带有相同标志的所有其他模块，之后用户才会收到有关身份验证尝试失败的消息。

#### `requisite`

也必须成功处理带有此标志的模块，处理方式在很大程度上与带有 `required` 标志的模块类似。但是，如果某个带有此标志的模块失败，将立即向用户提供反馈并且不再继续处理其他模块。如果成功，则将处理随后的模块，就像带有 `required` 标志的任何模块一样。`requisite` 标志可用于基本过滤器，该过滤器检查进行正确身份验证所必需的某些条件是否存在。

#### `sufficient`

在成功处理带有此标志的模块后，发出调用的应用程序立即收到处理成功的消息并且不再处理其他模块，但前提是前面没有带有 `required` 标志的模块失败。带有 `sufficient` 标志的模块失败没有任何直接后果，所有随后的模块都将按其各自的顺序进行处理。

optional

带有此标志的模块成功或失败不会产生任何直接后果。此标志可用于只用来显示消息（例如，通知用户收到了邮件）而不采取任何进一步操作的模块。

include

如果给出此标志，则在此处插入指定为参数的文件。

只要模块位于默认目录 `/lib/security`（对于 SUSE Linux Enterprise® 支持的所有 64 位平台，默认目录是 `/lib64/security`）中，就无需显式指定模块路径。第四列可能包含给定模块的选项，例如 `debug`（启用调试）或 `nullok`（允许使用空密码）。

## 27.2 sshd 的 PAM 配置

为了说明 PAM 背后的工作原理，让我们看一下 `sshd` 的 PAM 配置这一实际示例：

### 例 27.1 `sshd` 的 PAM 配置

```
##PAM-1.0
auth    include      common-auth
auth    required      pam_nologin.so
account include      common-account
password include      common-password
session include      common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session optional    pam_resmgr.so fake_ttyname
```

应用程序（在本例中是 `sshd`）的典型 PAM 配置包含 4 个 `include` 语句，引用 4 种模块类型的配置文件：`common-auth`、`common-account`、`common-password` 和 `common-session`。这 4 个文件包含每种模块类型的默认配置。通过将它们包含在内而不是单独为每个 PAM 应用程序调用各个模块，在管理员更改默认值时可自动更新 PAM 配置。以前，在 PAM 发生更改或安装新应用程序时，必须手动调整所有应用程序的所有配置文件。而现在 PAM 配置是通过中央配置文件进行的，每个服务的 PAM 配置都将自动继承所有的更改。

第一个包括文件(`common-auth`)调用 `auth` 类型的两个模块：`pam_env` 和 `pam_unix2`。请参见例 27.2 “`auth` 部分的默认配置” [454]。

### 例 27.2 *auth* 部分的默认配置

```
auth    required    pam_env.so
auth    required    pam_unix2.so
```

第一个模块 `pam_env` 装载文件 `/etc/security/pam_env.conf` 以按照此文件中指定的内容设置环境变量。这可以用于将 `DISPLAY` 变量设置为正确的值，原因是 `pam_env` 模块知道进行登录的位置。第二个模块 `pam_unix2` 根据 `/etc/passwd` 和 `/etc/shadow` 检查用户的登录名和密码。

在成功调用 `common-auth` 中指定的模块后，第三个模块 `pam_nologin` 将检查文件 `/etc/nologin` 是否存在。如果存在，则只有 `root` 用户方可登录。在 `sshd` 得到登录是否成功的任何反馈之前，整批 `auth` 模块都将完成处理。假设这批模块中的所有模块都带有 `required` 控制标志，则必须先成功处理所有这些模块，在此之后 `sshd` 才能收到有关处理成功的消息。如果其中的某个模块不成功，则仍将继续处理整批模块，在此之后 `sshd` 才能得到处理失败的通知。

成功处理了 `auth` 类型的所有模块后，将立即处理另一个 `include` 语句（在本例中即例 27.3 “*account* 部分的默认配置” [454] 中的语句）。`common-account` 只包含 `pam_unix2` 一个模块。如果 `pam_unix2` 返回的结果证明用户存在，则 `sshd` 会收到一条处理成功的消息，然后处理下一批模块 (`password`)，如例 27.4 “*password* 部分的默认配置” [454] 中所示。

### 例 27.3 *account* 部分的默认配置

```
account required    pam_unix2.so
```

### 例 27.4 *password* 部分的默认配置

```
password required    pam_pwcheck.so    nullok
password required    pam_unix2.so      nullok use_first_pass use_authtok
#password required    pam_make.so      /var/yp
```

此外，`sshd` 的 PAM 配置只涉及一条引用 `password` 模块的默认配置的 `include` 语句，这些模块位于 `common-password` 中。当应用程序请求身份验证令牌的更改时，必须成功完成这些模块（控制标志 `required`）。更改密码或另一个身份验证令牌需要进行安全检查。使用 `pam_pwcheck` 模块可完成此操作。随后使用的 `pam_unix2` 模块存有来自 `pam_pwcheck` 的任何旧密码和新密码，因此用户无需再次身份验证。该模块还确保不能绕过 `pam_pwcheck` 所执行的检查。只要前面的 `account` 或 `auth` 类型的模块被配置为指出失效的密码，就应该使用 `password` 类型的模块。

### 例 27.5 session 部分的默认配置

```
session required      pam_limits.so
session required      pam_unix2.so
session optional      pam_umask.so
```

最后，调用 `session` 类型的模块（捆绑在 `common-session` 文件中）以根据相关用户的设置来配置会话。虽然再次处理 `pam_unix2`，但由于在该模块的相应配置文件 `pam_unix2.conf` 中指定了 `none` 选项，所以没有实际后果。`pam_limits` 模块装载文件 `/etc/security/limits.conf`，该文件定义对某些系统资源使用的限制。当用户注销时，将再次调用 `session` 模块。

## 27.3 PAM 模块的配置

某些 PAM 模块是可配置的。对应的配置文件位于 `/etc/security` 中。本节简要介绍与 `sshd` 示例相关的一些配置文件 - `pam_unix2.conf`、`pam_env.conf`、`pam_pwcheck.conf` 和 `limits.conf`。

### 27.3.1 pam\_unix2.conf

传统的基于密码的身份验证方法是由 PAM 模块 `pam_unix2` 控制的。它可以从 `/etc/passwd`、`/etc/shadow`、NIS 映射、NIS+ 表或 LDAP 数据库中读取必要的数据库。通过配置各个应用程序自己的 PAM 选项或通过编辑 `/etc/security/pam_unix2.conf` 进行全局配置可以影响此模块的行为。中说明了该模块一个非常基本的配置文件。例 27.6 “`pam_unix2.conf`” [455]

#### 例 27.6 pam\_unix2.conf

```
auth:      nullok
account:
password:      nullok
session:      none
```

用于模块类型 `auth` 和 `password` 的 `nullok` 选项指定允许相应类型的帐户使用空密码。允许用户更改他们帐户的密码。`session` 类型的模块的 `none` 选项指定不为它记录任何消息（这是默认设置）。通过文件本身中的注释和 `pam_unix2(8)` 的手册页可以了解其他配置选项。

## 27.3.2 pam\_env.conf

此文件可用于定义调用 `pam_env` 模块时为用户设置的标准化环境。它允许您使用以下语法预设环境变量：

```
VARIABLE [DEFAULT=[value]] [OVERRIDE=[value]]
```

`VARIABLE`

要设置的环境变量的名称。

```
[DEFAULT=[value]]
```

设置的管理员所需的默认值。

```
[OVERRIDE=[value]]
```

可能由 `pam_env` 查询并设置的值，覆盖默认值。

有关 `pam_env` 如何使用的典型示例就是 `DISPLAY` 变量的调整，在发生远程登录是该变量会改变。例 27.7 “`pam_env.conf`” [456] 中显示了这一工具。

### 例 27.7 `pam_env.conf`

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}  
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

第一行将 `REMOTEHOST` 变量的值设置为 `localhost`，当 `pam_env` 不能确定任何其他值时就会使用该值。`DISPLAY` 变量又包含 `REMOTEHOST` 的值。文件 `/etc/security/pam_env.conf` 中的注释提供了详细信息。

## 27.3.3 pam\_pwcheck.conf

此配置文件用于 `pam_pwcheck` 模块，该模块为所有 `password` 类型的模块读取此文件中的选项。储存在此文件中的设置优先于单个应用程序的 **PAM** 设置。如果尚未定义应用程序特定的设置，则应用程序使用全局设置。例 27.8 “`pam_pwcheck.conf`” [456] 指示 `pam_pwcheck` 允许使用空密码和修改密码。文件 `/etc/security/pam_pwcheck.conf` 中介绍了模块的更多选项。

### 例 27.8 `pam_pwcheck.conf`

```
password: nullok
```

## 27.3.4 limits.conf

可以在文件 `limits.conf` 中以用户或组为基础设置的系统限制，该文件由 `pam_limits` 模块读取。该文件允许您设置硬限制（根本不能超出的限制）和软限制（可以临时超出的限制）。要了解语法和可用选项，请阅读文件中包含的注释。

## 27.4 有关详细信息

在已安装系统的 `/usr/share/doc/packages/pam` 目录中，可以找到以下附加文档：

### 自述文件

在此目录的最高一级，存有一些常规自述文件。子目录 `modules` 保存有关可用 PAM 模块的自述文件。

### Linux-PAM 系统管理员指南

此文档包括系统管理员应该了解的有关 PAM 的所有内容。它讨论了一系列主题，从配置文件的语法到 PAM 的安全属性。此文档以 PDF 文件、HTML 格式和纯文本格式提供。

### Linux-PAM 模块编写人员手册

此文档从开发人员的角度对多个主题进行了总结，提供了有关如何编写符合标准的 PAM 模块的信息。此文档以 PDF 文件、HTML 格式和纯文本格式提供。

### Linux-PAM 应用程序开发人员指南

此文档包括要使用 PAM 库的应用程序开发人员所需的所有内容。此文档以 PDF 文件、HTML 格式和纯文本格式提供。

Thorsten Kukuk 开发了许多 PAM 模块并提供了有关这些模块的信息，网址为：

<http://www.suse.de/~kukuk/pam/>。





## 电源管理

电源管理对于便携式计算机特别重要，但对于其他系统也是有用的。有两种技术：APM（高级电源管理）和 ACPI（高级配置和电源界面）。除了这两项技术，还可以通过控制 CPU 频率调节达到省电或降低噪声的目的。这些选项可以手动配置或使用特殊的 YaST 模块配置。

► **zseries:** 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。所有现代计算机（便携式计算机、台式机和服务器的）上都提供有 ACPI（高级配置与电源接口）。电源管理技术需要合适的硬件和 BIOS 例程。大多数便携式计算机、许多目前的台式机和服务器的都符合这些要求。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。

APM 用在许多以前的计算机上。因为 APM 主要由在 BIOS 中实施的功能集组成，所以 APM 支持的级别因硬件的不同而有所不同。而这对 ACPI 而言就更是如此，ACPI 更加复杂。因此，实际上很难决定是向您推荐 APM 还是 ACPI。在您的硬件上测试各种过程，然后选择支持情况最好的技术即可。

### 28.1 省电功能

省电功能不仅对便携式计算机的移动使用很重要，而且对台式机系统也很重要。电源管理系统 APM 和 ACPI 中的主要功能及其用途是：

## 待机

此运行方式将关闭屏幕显示。在某些计算机上，处理器性能会受到限制。此功能对应于 ACPI 状态 S1 或 S2。

## 暂挂（到内存）

此方式将整个系统状态写入 RAM。随后，除 RAM 外，整个系统都进入休眠状态。在此状态下，计算机消耗的电量非常少。此状态的优点是无需引导和重新启动应用程序就可以在数秒内将工作恢复到原来的进度。此功能对应于 ACPI 状态 S3。对此状态的支持仍在开发中，因此目前主要依靠硬件来实现支持。

## 休眠（暂挂到磁盘）

在此运行方式下，将整个系统状态写入硬盘并关闭系统电源。至少要有一个像 RAM 一样大的交换分区才能写入所有活动的数据。从该状态重激活大约需要 30 至 90 秒的时间。将恢复到暂停之前的状态。某些制造商提供这种方式的有用的混合变体（例如 IBM Thinkpad 中的 RediSafe）。对应的 ACPI 状态是 S4。在 Linux 中，由独立于 APM 和 ACPI 的内核例程执行暂挂到磁盘。

## 电池监视

ACPI 和 APM 检查电池电量状态并提供相关信息。另外，当达到临界电量状态时，两个系统都将协调要执行的操作。

## 自动关闭电源

关闭后，将关闭计算机的电源。当在电池电量用完前立即执行自动关闭时，此功能特别重要。

## 系统部件的关闭

关闭硬盘是整个系统中省电潜力最大的一个方面。根据整个系统的可靠性，硬盘可以休眠一段时间。但是，休眠期间丢失数据的风险也会增加。可使用 ACPI（至少从理论上说可行）取消激活或在 BIOS 设置中永久禁用其他组件（如可处于特殊省电模式的 PCI 设备）。

## 处理器速度控制

在 CPU 方面，有三种方法可以节省电能：频率和电压调节（也称为 PowerNow! 或 Speedstep）、节流和让处理器休眠（C 状态）。根据计算机的运行方式，还可以将这三种方法结合起来使用。

## 28.2 APM

APM BIOS 本身会执行一些省电功能。在许多便携式计算机上，可以使用组合键或通过合上机盖来激活待机状态和暂挂状态，无需任何特殊的操作系统功能。但是，要通过命令激活这些方式，则必须在暂停系统前触发某些特定的操作。要查看电池电量水平，需要特殊的程序包和合适的内核。

SUSE Linux Enterprise® 内核具有内置的 APM 支持。但是，只有在 BIOS 中未实施 ACPI 且检测到 APM BIOS 的情况下才能激活 APM。要激活 APM 支持，必须在引导提示符下使用 `acpi=off` 禁用 ACPI。输入 `cat /proc/apm` 检查 APM 是否处于活动状态。由多个数字组成的输出表示一切正常。现在应该能使用命令 `shutdown -h` 关闭计算机。

不完全符合标准的 BIOS 实施可能使 APM 出现问题。可以使用特殊的引导参数来避免某些问题。在引导提示符下以 `apm=parameter` 形式输入所有参数，*parameter* 为以下的一个：

`on or off`

启用或禁用 APM 支持。

`(no-)allow-ints`

在执行 BIOS 功能时允许中断。

`(no-)broken-psr`

BIOS 的 “GetPowerStatus” 功能工作不正常。

`(no-)realmode-power-off`

关闭前将处理器重设置为实际方式。

`(no-)debug`

在系统日志中记录 APM 事件。

`(no-)power-off`

在关闭后关闭系统电源。

`bounce-interval=n`

暂停事件后的一段时间（以百分之一秒为单位），在这段时间中将忽略其他暂停事件。

`idle-threshold=n`

系统不活动百分比，从这个百分比开始执行 BIOS 功能 `idle`（0 表示始终执行，100 表示从不执行）。

`idle-period=n`

开始测量系统活动前所经过的时间（以百分之一秒为单位）。

不再使用 APM 守护程序 (`apmd`)。其功能现在由新的 `powersaved` 处理，后者也支持 ACPI 并能提供许多其他功能。

## 28.3 ACPI

ACPI（高级配置和电源接口）支持操作系统设置和控制各个硬件部件。ACPI 可以取代 PnP 和 APM。它提供有关电池、AC 适配器、温度、风扇和系统事件（例如“合上机盖”或“电池电量低”）的信息。

BIOS 提供包含有关各个部件和硬件访问方法信息的表。操作系统使用这些信息执行指派中断或激活和取消激活部件等任务。因为操作系统执行 BIOS 中储存的命令，所以功能取决于 BIOS 实施。`/var/log/boot.msg` 中报告了 ACPI 能够检测并装载的表。有关对 ACPI 问题进行故障诊断的详细信息，请参见第 28.3.4 节“故障诊断”[467]。

### 28.3.1 使用 ACPI

如果内核在引导系统时检测到 ACPI BIOS，则会自动激活 ACPI。某些较旧的计算机可能需要引导参数 `acpi=force`。计算机必须支持 ACPI 2.0 或更高版本。检查 `/var/log/boot.msg` 中的内核引导消息，了解是否已激活了 ACPI。

随后，必须装载多个模块。这是由 `Aacpid` 的启动脚本完成的。如果这些模块中的任何一个模块引起问题，则可以在 `/etc/sysconfig/powersave/common` 中排除相应模块的装载或卸载。系统日志 (`/var/log/messages`) 包含模块的消息，使您了解检测到了哪些组件。

`/proc/acpi` 目前包含多个文件，这些文件提供有关系统状态的信息，也可用于更改某些状态。某些功能仍在开发中，所以尚不能使用，而对某些功能的支持主要取决于制造商的实施。

通过 `cat` 可以读取所有文件（`dsdt` 和 `fadt` 除外）。在某些文件中，可使用 `echo`（例如 `echo X > file`）来修改设置，以指定适用于 `X` 的值。能够简化访问这些值的其中一种可行方法就是使用 `powersave` 命令，它将充当 `Powersave` 守护程序的前端。下面介绍一些最重要的文件：

`/proc/acpi/info`  
有关 **ACPI** 的一般信息。

`/proc/acpi/alarm`  
这里指定应将系统从休眠状态唤醒的时间。当前不完全支持此功能。

`/proc/acpi/sleep`  
提供有关可能的休眠状态的信息。

`/proc/acpi/event`  
在这里报告所有事件并由 `Powersave` 守护程序 (`powersaved`) 对这些事件进行处理。如果没有任何守护程序访问该文件，则可以使用 `cat /proc/acpi/event` 读取事件（如短暂单击电源按钮或合上机盖）（用 `Ctrl + C` 终止）。

`/proc/acpi/dsdt` 和 `/proc/acpi/fadt`  
这些文件包含 **ACPI** 表 **DSDT**（区分系统说明表和 **FADT**（固定 **ACPI** 说明表））。可以使用 `acpidmp`、`acpidisasm` 和 `dmdecode` 读取这些文件。包 `pmtools` 中提供了这些程序及其文档。例如，`acpidmpDSDT | acpidisasm`。

`/proc/acpi/ac_adapter/AC/state`  
显示是否连接了 **AC** 适配器。

`/proc/acpi/battery/BAT*/{alarm,info,state}`  
有关电池状态的详细信息。通过将 `info` 中的 `last full capacity` 与 `state` 中的 `remaining capacity` 进行比较来读取电量水平。一个更方便的方法是使用 [第 28.3.3 节“ACPI 工具”](#) [467] 中引入的特殊程序之一。可以在 `alarm` 中指定电量水平，达到该电量水平将触发电池事件（例如警告、低和严重）。

`/proc/acpi/button`  
该目录中包含各种切换模式的相关信息，比如便携式计算机机盖和按钮。

`/proc/acpi/fan/FAN/state`

显示风扇当前是否处于活动状态。将0（开）或3（关）写入此文件可以手动激活或取消激活风扇。但是，当系统变得过热时，内核中的ACPI代码和硬件（或BIOS）将覆盖此设置。

`/proc/acpi/processor/*`

为系统中的每个CPU保留了一个单独的子目录。

`/proc/acpi/processor/*/info`

有关处理器省电选项的信息。

`/proc/acpi/processor/*/power`

有关当前处理器状态的信息。c2旁边的星号表示处理器处于空闲状态。这是最常见的状态，可以从usage值中观察到。

`/proc/acpi/processor/*/throttling`

可用于设置处理器时钟的节流。通常，可以将节流分为8个级别。这与CPU的频率控制无关。

`/proc/acpi/processor/*/limit`

如果守护程序自动控制性能（已过时）和节流，则可以在这里指定最大限制。某些限制是由系统确定的。某些限制可由用户进行调整。

`/proc/acpi/thermal_zone/`

每个热区有单独的子目录。热区是具有类似热属性的区域，其编号和名称由硬件制造商指定。但是，很少实施ACPI提供的许多功能。而温度控制通常是由BIOS处理的。因为关系到硬件的使用寿命，所以操作系统很少有机会进行干预。因此，部分文件只具有理论价值。

`/proc/acpi/thermal_zone/*/temperature`

热区的当前温度。

`/proc/acpi/thermal_zone/*/state`

此状态指出一切是否ok或ACPI是采用active散热还是passive散热。对于独立于ACPI的风扇控制，此状态始终是ok。

`/proc/acpi/thermal_zone/*/cooling_mode`

选择由ACPI控制的散热方法。选择被动散热方式（性能较低，但很经济）还是主动散热方式（全部性能，但有风扇噪音）。

```
/proc/acpi/thermal_zone/*/trip_points
```

允许您确定温度限制，达到这些温度限制将触发特定操作（例如，被动散热或主动散热、暂停(hot)或关闭(critical)）。DSDT 中定义了可能的操作（取决于设备）。ACPI 规范中确定的临界点是 critical、hot、passive、active1 和 active2。即使不是实施所有临界点，也必须始终在此文件中以此顺序输入它们。例如，项 `echo 90:0:70:0:0 > trip_points` 将 critical 的温度设置为 90，将 passive 的温度设置为 70（所有温度以摄氏度为单位）。

```
/proc/acpi/thermal_zone/*/polling_frequency
```

如果在温度改变时没有自动更新 temperature 中的值，请在这里切换巡回检测方式。使用命令 `echoX >`

`/proc/acpi/thermal_zone/*/polling_frequency` 将每 X 秒查询一次温度。设置 `x=0` 禁用巡回检测。

不需要手动编辑这些设置、信息和事件。这可以通过 Powersave 守护程序 (powersaved) 及其各种前端（例如 powersave、kpowersave 和 wmpowersave）来完成。请参见第 28.3.3 节“ACPI 工具”[467]。

## 28.3.2 控制 CPU 性能

CPU 可以采用三种省电方法。根据计算机的运行方式，还可以将这三种方法合起来使用。省电还意味着系统温度不会升得过高并且激活风扇的频率会降低。

### 频率和电压调节

PowerNow! 和 Speedstep 是 AMD 和 Intel 为这一技术指定的名称。但是，其他制造商的处理器中也应用了这一技术。CPU 的时钟频率及其核心电压同时降低，因而采用这一技术所节省的电量远远超过了线性省电量。这意味着，如果频率减半（一半的性能），所节省的电量远不止一半。此技术独立于 APM 或 ACPI。可使用两种主要的方法来执行 CPU 频率调节：通过内核本身或通过用户空间应用程序。因此，可以在 `/sys/devices/system/cpu/cpu*/cpufreq/` 下设置不同的内核管理器。

#### userspace governor

如果设置了用户空间管理器，则内核会将 CPU 频率调节的控制指定给用户空间应用程序（通常是守护程序）。在 SUSE Linux Enterprise 分发中，此守护程序是 powersaved 程序包。使用此实施时，将根据当前系统负载调整 CPU 的频率。默认情况下，将使用某个内核实施。但

是，在某个硬件上或对于特定处理器或驱动器，用户空间实施仍是唯一的工作解决方法。

#### ondemand governor

它是动态 CPU 频率策略的内核实施，应该可在大多数系统上运行。只要系统负载过高，CPU 频率将立即增加。它在系统负载较低时也较低。

#### conservative governor

此管理器与按需实现相似，只是使用更保守的策略。对于 CPU 频率增加之前的特定时间内，系统的负载必须很高。

#### powersave governor

静态地将 cpu 频率设置为最低。

#### performance governor

静态地将 cpu 频率设置为最高。

### 节流时钟频率

此技术将忽略一定百分比的 CPU 时钟信号脉冲。如果节流 25%，则将忽略四分之一的脉冲，如果节流 87.5%，则只有八分之一的脉冲到达处理器。但是，采用这种方法所节省的电量稍微低于线性省电量。通常，只有在频率调节不可用或要最大程度节省电量时才使用节流。此技术也必须由特殊的进程控制。系统接口是 `/proc/acpi/processor/*/throttling`。

### 使处理器进入休眠状态

操作系统在处理器不执行任何任务时使处理器进入休眠状态。在这种情况下，操作系统向 CPU 发送一个 `halt` 命令。有三种状态：C1、C2 和 C3。最经济的状态是 C3，在这种状态下，连处理器高速缓存与主存之间的同步都将暂停。因此，只有在没有任何其他设备通过总线主控芯片活动修改主储存器的内容时才能应用此状态。某些驱动程序禁止使用 C3。当前状态显示在 `/proc/acpi/processor/*/power` 中。

只有当处理器忙时，才需要进行频率调节和节流，这是因为当处理器处于空闲状态时总是会应用最经济的 C 状态。如果 CPU 忙，则建议采用的省电方法是频率调节。处理器经常只在部分负载的状态下工作。在这种情况下，可以以较低的频率运行。通常，由内核按需管理器 (kernel on demand governor) 或一个守护程序（如 `powersaved`）控制的动态频率调节是最佳方法。如果使用电池工作或如果您想让计算机冷却或安静，则静态设置为低频率会非常有用。



节流应作为最后没有办法时采用的方法，例如，虽然系统负载很高，但为延长电池工作时间而采用节流。但是，如果节流程度过高，某些系统将不会正常运行。此外，如果 CPU 处理的任务量很少，则 CPU 节流就没什么作用。

在 SUSE Linux Enterprise 中，这些技术是由 powersave 守护程序控制的。对此配置进行了说明。第 28.5 节“powersave 包”[470]

## 28.3.3 ACPI 工具

一系列相对全面的 ACPI 实用程序包含这样一些工具：只显示信息（例如，电池电量水平和温度）的工具（acpi、klaptopdaemon 和 wmacpimon 等）、简化对 /proc/acpi 中的结构进行访问的工具或协助监视更改的工具（akpi、acpiw 和 gtkacpiw）以及用于编辑 BIOS 中 ACPI 表的工具（包 pmttools）。

## 28.3.4 故障诊断

问题有两种不同的类型。一种是内核的 ACPI 代码可能包含未及时检测出的错误。在这种情况下，可以通过下载获得解决方案。而另一种更常见的问题，是由 BIOS 引起的。有时，会故意将一些不符合 ACPI 规范的配置集成在 BIOS 中，用于避免其他常用操作系统中 ACPI 实施中的错误。在 ACPI 实施中有严重错误的硬件部件会被记录在一个黑名单中，防止 Linux 内核对这些部件使用 ACPI。

在遇到问题时，首先要做的是更新 BIOS。如果计算机根本未引导，则使用以下引导参数之一可能会解决问题：

`pci=noacpi`

不使用 ACPI 配置 PCI 设备。

`acpi=ht`

只执行简单的资源配置。不要将 ACPI 用于其他目的。

`acpi=off`

禁用 ACPI。

---

## 警告：不使用 ACPI 引导会出现问题

某些较新的计算机（特别是 SMP 系统和 AMD64 系统）需要 ACPI 以正确配置硬件。在这些计算机上，禁用 ACPI 可能会产生问题。

---

引导后，用命令 `dmesg | grep -2i acpi` 来监视系统的引导消息（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) 可替换为更高的版本。在这种情况下，将忽略 BIOS 中有问题的 DSDT。中对这一过程进行了介绍。第 28.5.4 节“查错”[475]

在内核配置中，可以使用开关来激活 ACPI 调试消息。如果已编译并安装了具有 ACPI 调试功能的内核，则支持对详细信息执行错误专家搜索。

如果遇到 BIOS 或硬件问题，则最好与制造商联系。特别是如果制造商不常对 Linux 提供支持，他们就应该面对这些问题。只有在制造商意识到有很多客户在使用 Linux 时，他们才会重视这一问题。

## 更多信息

有关 ACPI 的其他文档和帮助：

- <http://www.cpqlinux.com/acpi-howto.html>（详细的 ACPI HOWTO 文档，包含 DSDT 增补程序）
- <http://www.intel.com/technology/iapc/acpi/faq.htm> (ACPI FAQ @Intel)
- <http://acpi.sourceforge.net/>（Sourceforge 中的 ACPI4Linux 项目）
- <http://www.poupinou.org/acpi/>（Bruno Ducrot 开发的 DSDT 增补程序）

## 28.4 硬盘的休眠

在 Linux 中，如果不使用硬盘，则可以使硬盘完全进入休眠状态，或者在更经济或更安静的方式下运行。在目前的便携式计算机上，您无需手动关闭硬盘，因为硬盘会在不运行时自动进入经济的运行方式。但是，如果要最大限度地省

电，请尝试使用以下一些方法。powersaved 和 YaST 电源管理模块可以控制大多数的功能，这将在第 28.6 节“YaST 电源管理模块”[478]中作进一步的讨论。

hdparm 应用程序可用于修改多种硬盘设置。选项 -y 将硬盘立即切换到待机方式。-Y 使硬盘进入休眠状态。hdparm -S x 会使硬盘在一段时间（未活动）后减慢运行速度。将 x 替换如下：0 表示禁用此机制，导致硬盘持续运行。值 1 到 240 表示的时间为所选的值乘以 5 秒。值 241 到 251 对应的时间分别是 30 分钟的 1 到 11 倍。

使用选项 -B 可以控制硬盘的内部省电选项。在 0 到 255 之间选择一个值，0 表示最大省电方式，255 表示最大吞吐量方式。结果取决于所使用的硬盘，难以估算。要让硬盘安静一些，请使用选项 -M。在 128 到 254 之间选择一个值，128 表示最安静，254 表示速度最快。

通常，让硬盘进入休眠状态并不容易。在 Linux 中，大量的进程对硬盘执行写操作，因而会经常将其唤醒。因此，一定要了解 Linux 如何处理需要写入硬盘的数据。首先，在 RAM 中对所有数据进行缓冲。此缓冲区由内核更新守护程序 (kupdated) 进行监视。当数据达到一定的有效期限或缓冲区已被填充到一定程度时，就会清理缓冲区，将其中的内容写入硬盘。缓冲区大小是动态的，取决于内存的大小和系统负载。默认情况下，将 kupdated 设置为较短的时间间隔可以获得最好的数据完整性。它每 5 秒检查一次缓冲区，当数据存放时间超过 30 秒或缓冲区填充程度达到 30% 时，它会向 bdflush 守护程序发出通知。随后，bdflush 守护程序将数据写入硬盘。此守护程序还独立于 kupdated 写入数据，例如，当缓冲区已满时。

---

### 警告：对数据完整性的损害

更改内核更新守护程序设置将损害数据完整性。

---

除了这些进程之外，日记文件系统（例如 ReiserFS 和 Ext3）独立于 bdflush 写入它们的元数据，这也会妨碍硬盘减慢运行速度。为了避免这种情况，已为移动设备开发了特殊的内核扩展。有关详细信息，请参见 /usr/src/linux/Documentation/laptop-mode.txt。

另一个重要因素是活动程序的行为方式。例如，好的编辑器会定期将当前已修改文件的隐藏备份写入硬盘，而这会唤醒磁盘。可以禁用此类功能，但这会影响数据的完整性。

在此连接中，邮件守护程序 postfix 使用变量 POSTFIX\_LAPTOP。如果将此变量设为 yes，则 postfix 访问硬盘的频率将显著降低。但是，如果增加 kupdated 的时间间隔，则这样做没有什么作用。

## 28.5 powersave 包

powersave 包中包含了先前描述的所有省电功能。通常来说，由于对低能源消耗的需求的增加，它的某些功能在工作站和服务器的上也相应变得重要，例如暂停、待机或 CPU 频率调节。

此包包含计算机的所有电源管理功能。它支持使用 ACPI、APM、IDE 硬盘以及 PowerNow! 或 SpeedStep 技术的硬件。包 apmd、acpid、ospmd 和 cpufreqd（现在是 cpuspeed）中的功能已被合并到 powersave 包中。这些包中的守护程序（除了充当 acpi 事件多路转换器的 acpid）不应该与 powersave 守护程序并发运行。

即使您的系统未包含上面列出的所有硬件元素，也应使用 powersave 守护程序控制省电功能。因为 ACPI 和 APM 是互斥的，所以您的计算机上只能使用其中一个系统。此守护程序将自动检测硬件配置中的任何更改。

### 28.5.1 配置 powersave 包

powersave 的配置分布在多个文件中。此处列出的所有配置选项都包含有关其功能的其他文档。

/etc/sysconfig/powersave/common

此文件包含 powersave 守护程序的一般设置。例如，通过增大变量 DEBUG 的值可以增加 /var/log/messages 中调试消息的数量。

/etc/sysconfig/powersave/events

powersave 守护程序需要此文件来处理系统事件。可以将事件指派给外部操作，也可以指派给守护程序本身执行的操作。对于外部操作，守护程序尝试运行 /usr/lib/powersave/scripts/ 中的可执行文件（通常是 Bash 脚本）。预定义的内部操作有：

- ignore

- throttle
- dethrottle
- suspend\_to\_disk
- suspend\_to\_ram
- standby
- do\_suspend\_to\_disk
- do\_suspend\_to\_ram
- do\_standby
- 通知
- screen\_saver
- reread\_cpu\_capabilities

throttle 按 MAX\_THROTTLING 中定义的值减慢处理器的速度。此值取决于当前方案。dethrottle 设置处理器发挥全部性能运行。

suspend\_to\_disk、suspend\_to\_ram 和 standby 触发休眠方式的系统事件。这三个操作通常负责触发休眠方式，但应始终将它们与特定的系统事件关联起来。

目录 /usr/lib/powersave/scripts 包含处理事件的脚本：

switch\_vt

如果暂停或待机后屏幕移位，则可以使用此脚本。

wm\_logout

保存设置并从 GNOME、KDE 或其他窗口管理器中注销。

wm\_shutdown

保存 GNOME 或 KDE 设置并关闭系统。

set\_disk\_settings

执行 /etc/sysconfig/powersave/disk 中所作的磁盘设置。

例如，如果设置了变量

`EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"`，则用户一旦将休眠方式暂挂到磁盘的命令提供给 `powersaved`，就将按指定的顺序处理这两个脚本或操作。守护程序首先运行外部脚本 `/usr/lib/powersave/scripts/prepare_suspend_to_disk`。在成功处理此脚本后，守护程序运行内部操作 `do_suspend_to_disk`，然后在此脚本卸载了关键模块并停止了服务后，将计算机设置为休眠方式。

可修改休眠按钮事件的操作，如 `EVENT_BUTTON_SLEEP="notify suspend_to_disk"` 中所示。在这种情况下，`X` 中会出现一个弹出窗口或者控制台上会出现一条消息，从而提示用户操作暂停。随后，将生成事件 `EVENT_GLOBAL_SUSPEND2DISK`，从而执行指定的操作和安全暂挂方式。可以使用 `/etc/sysconfig/powersave/common` 中的变量 `NOTIFY_METHOD` 自定义内部操作 `notify`。

`/etc/sysconfig/powersave/cpufreq`

包含用来优化动态 CPU 频率设置以及是否使用用户空间或内核实施的变量。

`/etc/sysconfig/powersave/battery`

包含电池电量限制和其他电池特定的设置。

`/etc/sysconfig/powersave/sleep`

在此文件中，激活休眠方式并确定在暂停事件或待机事件之前应卸载哪些关键模块以及停止哪些服务。当系统恢复时，将重装载这些模块并重新启动这些服务。例如，甚至可以延迟已触发的休眠方式以便保存文件。默认设置主要涉及 `USB` 和 `PCMCIA` 模块。暂停或待机失败通常是由某些模块引起的。有关确定错误的详细信息，请参见 [第 28.5.4 节“查错”](#) [475]。

`/etc/sysconfig/powersave/thermal`

激活散热和热量控制。文件 `/usr/share/doc/packages/powersave/README.thermal` 中提供了有关此主题的详细信息。

`/etc/sysconfig/powersave/disk`

此配置文件包含根据硬盘所作的操作和设置。

`/etc/sysconfig/powersave/scheme_*`

提供多种耗电量与特定部署方案相适应的方案。许多方案都是预配置的，使用时无需进行更改。可以在这里保存自定义方案。

## 28.5.2 配置 APM 和 ACPI

### 暂停和待机

有三种基本的 ACPI 休眠方式和两种 APM 休眠方式：

暂停到磁盘（ACPI S4、APM 暂停）

将整个内存内容保存到硬盘。计算机完全关闭且不消耗任何电源。此休眠方式是默认启用的，并且应该在所有系统上都有效。

暂停到 RAM（ACPI S3、APM 暂停）

将所有设备的状态保存到主存储器。只有主存储器继续消耗电源。SUSE Linux Enterprise 通常不支持该休眠方式（尽管您可以对许多计算机使用它）。

默认启用该休眠方式，但只有数据库中将当前计算机列为能够支持该方式时，才会执行。该数据库包含在 suspend 包提供的 /usr/sbin/s2ram 二进制数据中。

要修改默认参数（例如，要通常情况下禁用暂挂到 ram 休眠方式，或者即使对数据库中未列出的计算机也强制执行它），可在 /etc/sysconfig/powersave/sleep 配置文件中查找关于可用选项的更多信息。

要了解关于 s2ram 二进制数据的更多信息，请参见自述文件（/usr/share/doc/packages/suspend）。

待机（ACPI S1、APM 待机）

关闭某些设备（取决于制造商）。

为了正确处理暂挂、待机和恢复，确保在文件 /etc/sysconfig/powersave/events 中设置了以下默认选项（SUSE Linux Enterprise 安装之后的默认设置）：

```
EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk screen_saver do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram screen_saver do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
    "prepare_standby screen_saver do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
```

```
EVENT_GLOBAL_RESUME_STANDBY=  
    "restore_after_standby"
```

## 自定义电池状态

文件 `/etc/sysconfig/powersave/battery` 中定义了三个电池电量水平（用百分比表示），在达到这些电池电量水平时，将触发系统警报或特定的操作。

```
BATTERY_WARNING=12  
BATTERY_LOW=7  
BATTERY_CRITICAL=2
```

配置文件 `/etc/sysconfig/powersave/events` 中定义了电池电量水平降至指定限度时执行的操作或脚本。可以按 [第 28.5.1 节“配置 powersave 包”](#) [470] 中所述修改按钮的标准操作。

```
EVENT_BATTERY_NORMAL="ignore"  
EVENT_BATTERY_WARNING="notify"  
EVENT_BATTERY_LOW="notify"  
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

## 调整耗电量以适应各种情况

可以根据电源类型调整系统行为。当系统从 AC 电源断开并使用电池运行时，应降低系统的耗电量。同样，系统一连接到 AC 电源，性能就应自动提高。CPU 频率、IDE 省电功能和许多其他参数都可以进行修改。

`/etc/sysconfig/powersave/events` 中定义了计算机从 AC 电源断开或连接到 AC 电源时要执行的操作。在 `/etc/sysconfig/powersave/common` 中选择要使用的方案：

```
AC_SCHEME="performance"  
BATTERY_SCHEME="powersave"
```

这些方案被储存在 `/etc/sysconfig/powersave` 下的文件中。文件名采用 `scheme_name-of-the-scheme` 的格式。该示例参考了两个模式：`scheme_performance` 和 `scheme_powersave`。`performance`、`powersave`、`presentation` 和 `acoustic` 是预配置的。借助于 YaST 电源管理模块



（第 28.6 节 “YaST 电源管理模块” [478] 中有述），可以编辑、创建、删除现有的方案，也可以将其与不同的电源状态关联起来。

## 28.5.3 其他 ACPI 功能

如果您使用 ACPI，则可以控制系统对 *ACPI 按钮*（电源、休眠、机盖打开和机盖合上）的响应。在 `/etc/sysconfig/powersave/events` 中配置操作的执行。有关各个选项的解释，请参考此配置文件。

`EVENT_BUTTON_POWER="wm_shutdown"`

当按下电源按钮后，系统将通过关闭相应的窗口管理器（KDE、GNOME、fvwm 等）进行响应。

`EVENT_BUTTON_SLEEP="suspend_to_disk"`

当按下休眠按钮后，系统会被设置为暂挂到磁盘方式。

`EVENT_BUTTON_LID_OPEN="ignore"`

当机盖打开时，不执行任何操作。

`EVENT_BUTTON_LID_CLOSED="screen_saver"`

当机盖合上时，激活屏幕保护程序。

`EVENT_OTHER="ignore"`

如果守护程序遇到了未知事件，则此事件将发生。未知事件包括某些计算机上的 ACPI 热键。

如果在指定时间内 CPU 负载未超过指定的限制，则可以进一步限制 CPU 性能。在 `PROCESSOR_IDLE_LIMIT` 中指定负载限度，在 `CPU_IDLE_TIMEOUT` 中指定超时值。如果 CPU 负载保持在限度之下的时间长于超时值，则将激活 `EVENT_PROCESSOR_IDLE` 中配置的事件。如果 CPU 再度处于忙碌状态，将执行 `EVENT_PROCESSOR_BUSY`。

## 28.5.4 查错

文件 `/var/log/messages` 中记录了所有错误消息和警报。如果您未能找到所需的信息，请使用文件 `/etc/sysconfig/powersave/common` 中的 `DEBUG` 增加 `powersave` 消息的详细程度。请将变量的值增加到 7，或甚至增加到 15，

然后重新启动守护程序。`/var/log/messages` 中更详细的错误消息应有助于您找到错误。以下几节介绍 `powersave` 最常见的问题。

## 硬件支持已激活 **ACPI**，但功能不工作

如果使用 **ACPI** 时遇到问题，请使用命令 `dmesg|grep -i acpi` 在 `dmesg` 的输出中搜索 **ACPI** 特定的消息。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。

- 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 如果下载的表的文件扩展名是 `.asl`（**ACPI** 源语言），则必须使用 `iasl`（`pmtools` 包）对其进行编译。为此，请输入命令 `iasl -sa file.asl`。提供了最新版本的 `iasl`（Intel **ACPI** 编译器）<http://developer.intel.com/technology/iapc/acpi/downloads.htm>
- 3 将文件 `DSDT.aml` 复制到任何位置（建议的位置为 `/etc/DSDT.aml`）。编辑 `/etc/sysconfig/kernel` 并相应地调整指向 **DSDT** 文件的路径。启动 `mkinitrd`（包 `mkinitrd`）。一旦安装了内核并使用 `mkinitrd` 创建了 `initrd`，引导系统时就会集成并装载已修改的 **DSDT**。

## **CPU** 频率不工作

请参考内核源代码 (`kernel-source`) 查看是否支持您的处理器。您可能需要特殊内核模块或模块选项来激活 **CPU** 频率控制。`/usr/src/linux/Documentation/cpufreq/*` 中提供了此信息。如果需要特殊模块或模块选项，则通过变量 `CPUFREQD_MODULE` 和 `CPUFREQD_MODULE_OPTS` 在文件 `/etc/sysconfig/powersave/cpufreq` 中进行配置。

## 暂挂和待机不工作

ACPI 系统由于 DSDT 实现 (BIOS) 有问题，可能在暂挂和待机中会遇到问题。如果出现这种情况，请更新 BIOS。

在 ACPI 和 APM 系统上：试卸载有问题的模块时，系统被阻止执行操作或暂停事件未被触发。如果您未卸载模块或停止成功暂停的服务，也会发生相同的情况。在这两种情况下，尝试确定阻止采用休眠方式的有问题的模块。/var/log/suspend2ram.log 和 /var/log/suspend2disk.log 中的 powersave 守护程序生成的日志文件对确定有问题的模块很有用。如果计算机未进入休眠方式，则原因在最后卸载的模块上。请配置 /etc/sysconfig/powersave/sleep 中的下列设置以在暂停或待机前卸载有问题的模块。

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

如果您在不断变化的网络环境中使用暂停或待机，或将暂停或待机用于远程装入的文件系统（例如 Samba 和 NIS），请使用 automounter 装入它们，或在上述变量中添加相应的服务，例如 smbfs 或 nfs。在远程装入的文件系统进入暂停或待机前，如果某个应用程序访问此文件系统，则无法正确停止服务且无法正确卸装该文件系统。在恢复系统后，文件系统可能被损坏，因此必须重装入文件系统。

## 28.5.5 有关详细信息

- /usr/share/doc/packages/powersave — 本地 Powersave 守护程序文档
- <http://powersave.sourceforge.net> — 最新 powersave 守护程序文档
- [http://www.opensuse.org/Projects\\_Powersave](http://www.opensuse.org/Projects_Powersave) — openSUSE wiki 中的项目页

# 28.6 YaST 电源管理模块

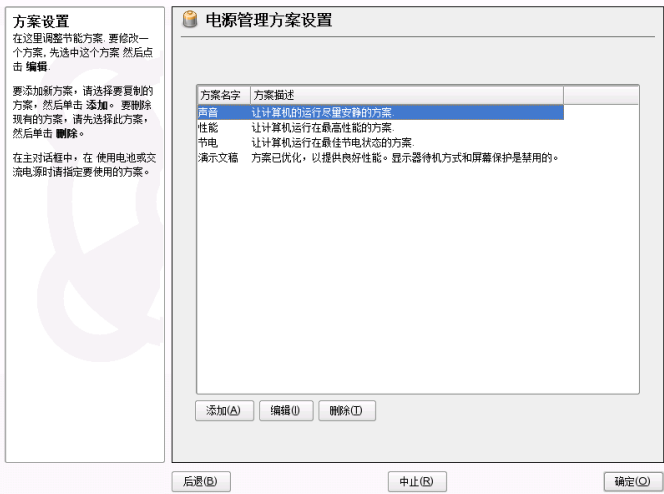
YaST 电源管理模块可以配置先前所述的所有电源管理设置。在通过系统 > 电源管理从“YaST 控制中心”启动此模块时，会打开此模块的第一个对话框（请参见图 28.1 “方案选择” [478]）。

图 28.1 方案选择



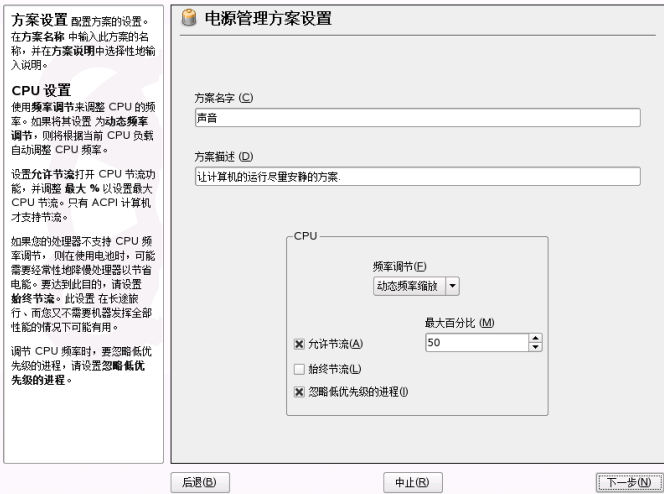
在此对话框中，选择使用电池运行和使用 AC 运行时要使用的方案。要添加或修改方案，请单击编辑方案，这将打开现有方案的概述，如图 28.2 “现有方案的概述” [479] 所示。

图 28.2 现有方案的概述



在方案概述中，选择要修改的方案，然后单击**编辑**。要创建新方案，请单击**添加**。这两种情况打开的是同一个对话框，如 图 28.3 “配置方案” [479] 所示。

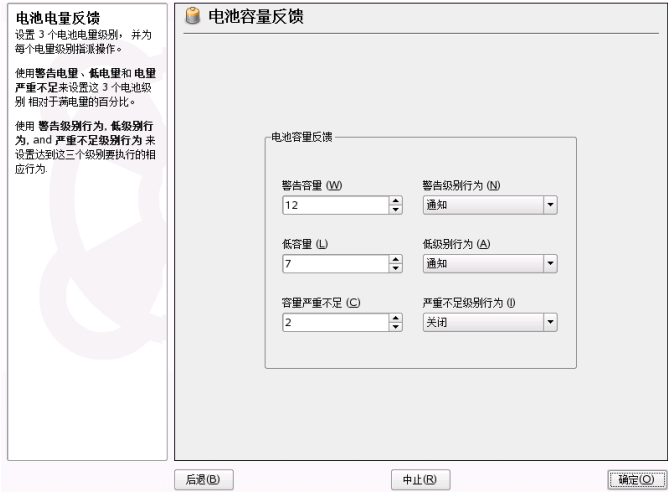
图 28.3 配置方案



首先，为新方案或已编辑的方案输入合适的名称和说明。确定此方案是否应控制 CPU 性能及如何控制 CPU 性能。确定是否应使用频率调节和节流以及应使用的频率调节和节流范围，确定调整 CPU 频率时是否应忽略低优先级进程（低优先级进程）。随后的对话框是针对硬盘的，它定义了待机策略是为实现最佳性能还是为实现最大省电。声音策略控制硬盘的噪音级别（少数几种硬盘支持这一功能）。散热策略确定要使用的散热方法。遗憾的是 BIOS 很少支持这种类型的热量控制。请阅读 `/usr/share/doc/packages/powersave/powersave_manual.html#Thermal` 以了解如何使用风扇和被动散热方法。

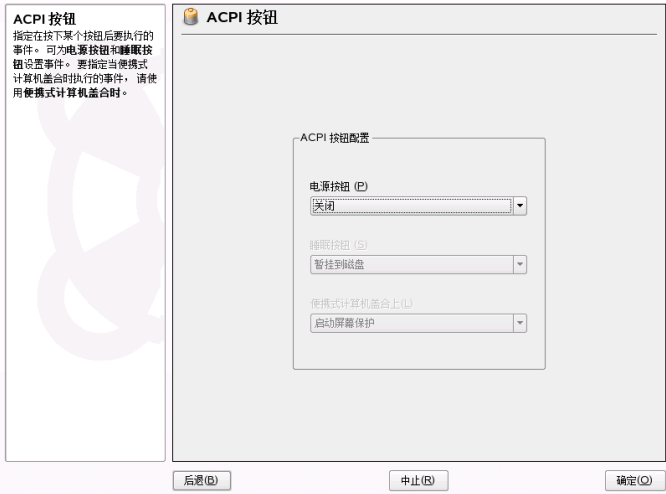
可以在最初的对话框中使用电池警告、ACPI 设置或暂挂权限进行全局电源管理设置。通过单击其他设置并从菜单选择相应项来访问这些控制。单击电池警告以访问电池电量水平对话框，如图 28.4 “电池电量水平” [480] 所示。

图 28.4 电池电量水平



每当电量水平降至特定的可配置限制之下时，系统的 BIOS 就会通知操作系统。在此对话框中定义三个限制：警告电量、电量低和临界电量。当电量水平降至这些限制之下时将触发特定的操作。通常，前两个状态只触发发送给用户的通知。第三个关键电量水平触发关闭操作，原因是剩余的电量不足以支持系统继续运行。选择合适的电量水平和所需的操作，然后单击确定返回到起始对话框。

图 28.5 ACPI 设置



通过 *ACPI* 设置访问用于配置 *ACPI* 按钮的对话框。图 28.5 “*ACPI* 设置” [481] 中显示了这一工具。对 *ACPI* 按钮进行的设置确定系统应如何对特定的开关进行响应。配置系统对按电源按钮、按休眠按钮和合上便携式计算机盖的响应。单击确定完成配置并返回到起始对话框。

单击 *启用暂停* 进入一个对话框，可以在这个对话框中确定此系统的用户是否及如何使用暂停或待机功能。单击 *确定* 返回到主对话框。再次单击 *确定* 退出此模块并确认您的电源管理设置。





## 无线通讯

无线 LAN 可用于建立 SUSE Linux Enterprise® 计算机间的通讯。本章介绍无线联网的原则和无线联网的基本配置。

### 29.1 无线 LAN

无线 LAN 已成为移动计算的不可缺少的一部分。当今，大多数笔记本电脑都配有内置 WLAN 卡。用于 WLAN 卡无线通讯的 802.11 标准是由 IEEE 组织制订的。最初，此标准实现的最大传送速率是 2 Mbit/s。此后，此标准进行了多次补充以提高数据传送速率。这些补充定义了调制、传送输出和传送速率等详细内容：

**表 29.1** 各种 WLAN 标准的概述

名称	频带 (GHz)	最大传送速率 (MBit/s)	记事
802.11	2.4	2	已过时；目前市场上不销售采用此标准的最终设备
802.11b	2.4	11	广泛采用
802.11a	5	54	较少使用
802.11g	2.4	54	向后兼容 11b

此外还有一些专有标准，如 Texas Instruments 对 802.11b 进行调整后形成的标准（有时也称为 802.11b+），其最大传送速率为 22 Mbit/s。但采用这种标准的卡的普及程度有限。

## 29.1.1 硬件

SUSE Linux Enterprise® 不支持 802.11 卡。支持采用 802.11a、802.11b 和 802.11g 的大多数卡。现在新推出的卡通常符合 802.11g 标准，但采用 802.11b 的卡仍然是可用的。通常，支持具有以下芯片的卡：

- Aironet 4500、4800
- Atheros 5210、5211、5212
- Atmel at76c502、at76c503、at76c504、at76c506
- Intel PRO/Wireless 2100、2200BG、2915ABG 和 3945ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Lucent/Agere Hermes
- Texas Instruments ACX100、ACX111

- ZyDAS zd1201

还支持许多很少用到且市面上不再有售的较早的卡。*Absolute Value Systems* 的网站中提供了一个列表，详尽列出了各种 WLAN 卡及其使用的芯片，网址是：[http://www.linux-wlan.org/docs/wlan\\_adapters.html.gz](http://www.linux-wlan.org/docs/wlan_adapters.html.gz) 查找各种 WLAN 芯片的概述：<http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz>。

有些卡需要固件映像，该映像必须在初始化驱动程序时载入卡中。Intersil PrismGT、Atmel 以及 TI ACX100 和 ACX111 就是这种情况。使用 YaST 联机更新可以方便地安装固件。SUSE Linux Enterprise 附带了 Intel PRO/Wireless 卡的固件，在检测到此类型的卡时，YaST 将自动安装该卡。已安装系统的 `/usr/share/doc/packages/wireless-tools/README.firmware` 中提供了有关此主题的详细信息。

## 29.1.2 功能

在无线联网中，会使用各种技术和配置来确保连接的快速、高质量和安全。不同的操作类型适合不同的设置。很难选择正确的身份验证方法。各种可用加密方法有各自的优点和缺陷。

### 操作方式

无线网络基本上可分为受管网络和特殊网络。受管网络具有一个管理元素，即访问点。在这种方式（也称为基础结构方式）中，WLAN 工作站在网络中的所有连接都通过访问点运行，后者也可用作与以太网的连接。特殊网络没有访问点。各个工作站直接互相通讯。在特殊网络中，传送范围和参与工作站的数目都受到很大限制。因此，采用访问点通常更加有效。甚至可以将 WLAN 卡用作访问点。大多数卡支持此功能。

与使用缆线连接的网络相比，无线网络中的数据更容易被截获，无线网络更容易受到攻击，所以各标准都包括了身份验证和加密方法。IEEE 802.11 标准最初的版本在术语 WEP 下对这些方法进行了描述。但是，WEP 被证明是不安全的（请参见“**安全性**”一节 [491]），因此 WLAN 行业（组织名为 *Wi-Fi 联盟*）制订了一个名为 WPA 的新扩展，用以弥补 WEP 的缺陷。后来的 IEEE 802.11i 标准（也称为 WPA2，因为 WPA 基于 802.11i 的草案版本）包括 WPA 和其他一些身份验证和加密方法。

## 身份验证

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：

### 打开

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“**加密**”一节 [487]）。

### 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（按照 IEEE 802.1x）

WPA-PSK（PSK 代表“预共享密钥”）的工作方式与共享密钥过程类似。所有参与工作站和访问点需要相同的密钥。该密钥长度为 256 位，通常以密码短语形式输入。此系统不需要像 WPA-EAP 那样的复杂密钥管理，并且更适合个人使用。因此，有时将 WPA-PSK 称为 WPA“家庭”。

### WPA-EAP（按照 IEEE 802.1x）

实际上，WPA-EAP 不是一个身份验证系统，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 提供了连接和身份验证服务器的三种不同方式：TLS (Transport Layer Security)、TTLS (Tunneled Transport Layer Security) 和 PEAP (Protected Extensible Authentication Protocol)。在 nutshell 中，这些选项的作用如下所示：

### EAP-TLS

TLS 身份验证依赖于服务器和客户机的证书互相交换。首先，服务器为客户机（客户机会评估服务器）提供其证书。如果证书被认为有效，则接下来客户机会对服务器提供其证书。当 TLS 是安全的，它要求在网络中具有运转的认证管理基础结构。此基础结构在专用网络中很少见。

## EAP-TTLS 和 PEAP

TTLS 和 PEAP 都是两个阶段的协议。在第一个阶段，将建立安全性，在第二个阶段，将交换客户机身份验证数据。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。

## 加密

有多种加密方法可确保所有未授权用户不能读取无线网络中交换的数据包并且不能访问网络：

### WEP（在 IEEE 802.11 中定义）

此标准使用 RC4 加密算法，最初密钥长度为 40 位，后来也使用 104 位的密钥。通常，将此长度声明为 64 位或 128 位，这取决于是否包括初始化矢量的 24 位。但是，此标准有一些缺陷。攻击者能够成功攻击此系统生成的密钥。不过，使用 WEP 总比根本不加密网络要好。

### TKIP（在 WPA/IEEE 802.11i 中定义）

WPA 标准中定义的这一密钥管理协议使用与 WEP 相同的加密算法，但弥补了其缺陷。由于为每个数据包生成一个新密钥，从而有效阻止了对这些密钥的攻击。TKIP 与 WPA-PSK 一起使用。

### CCMP（在 IEEE 802.11i 中定义）

CCMP 对密钥管理进行了描述。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。

## 29.1.3 用 YaST 配置

要配置您的无线网卡，请启动 YaST 网卡模块。还可在此处选择是使用 YaST 还是使用 NetworkManager 来管理网卡。如果选择 YaST，则在网络地址设置中选择设备类型无线，然后单击下一步。在无线网卡配置（如 [图 29.1 “YaST：配置无线网卡”](#) [488] 所示）中为 WLAN 操作进行基本设置：

图 29.1 YaST：配置无线网卡



## 操作方式

我们可以将工作站以三种不同的方式集成到 WLAN 中。适用的模式取决于通讯所用的网络：**特殊网络**（对等网络，无访问点）、**受管网络**（网络由访问点管理）或者**主网络**（您的网卡应用作访问点）。要使用 WPA-PSK 或 WPA-EAP 方式，必须将操作方式设置为受控。

## 网络名称 (ESSID)

为实现相互通讯，无线网络中的所有工作站都需要相同的 ESSIDu163。如果未指定任何内容，则网卡会自动选择一个访问点，但它可能不是您所希望使用的。

## 身份验证方式

为您的网络选择合适的身份验证方式：**开放**、**共享密钥**、**WPA-PSK**或**WPA-EAP**。如果选择了 WPA 身份验证，则必须设置网络名称。

## 专家设置

单击此按钮将打开一个对话框，用于对 WLAN 连接进行详细配置。下面的内容提供了此对话框的详细说明。

完成基本设置后，即可将您的工作站部署在 WLAN 中。

---

## 重要：无线网络中的安全性

确保使用所支持的身份验证和加密方法之一来保护您的网络通讯。如果未加密 WLAN 连接，则第三方便可以截获所有网络数据。即使进行弱加密 (WEP)

也比根本不加密要好。相关信息请参考“**加密**”一节 [487] 和“**安全性**”一节 [491]。

根据所选的身份验证方法，YaST 会提示您在另一个对话框中微调这些设置。对于**开放**，无需进行任何配置，因为此设置实施的是无需身份验证的未加密操作。

### 共享密钥

设置密钥输入类型。选择**通行密码**、**ASCII**或**十六进制**。您最多可以保留 4 个不同的密钥来加密所传送的数据。单击 **WEP 密钥** 进入密钥配置对话框。设置密钥长度：**128 位**或**64 位**。默认设置是 **128 位**。在对话框底部的列表区域中，最多可以指定 4 个不同的密钥，您的工作站将使用这些密钥进行加密。按**设置默认密钥**可将其中一个密钥定义为默认密钥。除非更改默认设置，否则 YaST 会将第一个输入的密钥用作默认密钥。如果删除了标准密钥，则必须将其他密钥中的一个手动标记为默认密钥。单击**编辑**可以修改现有列表项或创建新密钥。此时将出现一个弹出窗口，提示您选择输入类型（**通行密码**、**ASCII**或**十六进制**）。如果选择的是**通行密码**，则输入一个单词或字符串，将从该单词或字符串按照先前指定的长度生成密钥。**ASCII**要求为 64 位密钥输入 5 个字符，为 128 位密钥输入 13 个字符。如果选择的是**十六进制**，则按照十六进制表示法为 64 位密钥输入 10 个字符，或为 128 位密钥输入 26 个字符。

### WPA-PSK

要输入用于 WPA-PSK 的密钥，请选择输入方法**通行密码**或**十六进制**。在**通行密码**方式下，输入必须为 8 到 63 个字符。在**十六进制**方式下，请输入 64 个字符。

### WPA-EAP

输入网络管理员提供的身份凭证。对于 TLS，请提供**身份**、**客户机证书**、**客户机密钥**和**服务器证书**。TTLS 和 PEAP 需要**身份**和**密码**。**服务器证书**和**匿名身份**为可选。YaST 会在 /etc/cert 下搜索所有证书，因此将提供给您的证书保存到此位置中并将这些文件的访问权限限制为 0600（所有者读写）。

单击**细节**可进入 WPA-EAP 设置的高级身份验证对话框。选择 **EAP-TTLS** 或 **EAP-PEAP** 通信第二阶段的身份验证方法。如果在前面的对话框中已选择 **TTLS**，则选择任意、MD5、GTC、CHAP、PAP、MSCHAPv1 或 MSCHAPv2。如果已选择 **PEAP**，则选择任意、MD5、GTC 或 MSCHAPv2。如果自动确定的设置不起作用，则 **PEAP** 版本可用于强制使用特定的 PEAP 实施。

单击专家设置可退出 WLAN 连接的基本配置对话框并进入专家配置对话框。此对话框中有以下选项可用：

#### 通道

只有在特殊和主方式下才需要指定 WLAN 工作站要工作于的通道。在受控方式下，网卡将自动搜索访问点的可用通道。在特殊方式下，可从提供的 12 个通道中选择一个，用于在您的工作站和其他工作站之间进行通信。在主方式下，确定您的网卡应该在哪个通道上提供访问点功能。此选项的默认设置是*自动*。

#### 位速率

根据网络的性能，您可能要为从一点到另一点之间的传送设置特定位速率。在默认设置*自动*中，系统会尽可能地使用最高数据传送速率。一些 WLAN 卡不支持比特率设置。

#### 接入点

在具有多个访问点的环境中，通过指定 MAC 地址可以预先选择多个访问点中的一个。

## 29.1.4 实用程序

hostap（包 hostap）用于将 WLAN 卡作为访问点运行。有关此包的详细信息，请访问项目主页 (<http://hostap.epitest.fi/>)。

kismet（包 kismet）是一个网络诊断工具，使用它可以监听 WLAN 包流量。通过这种方式，您可以检测到网络中的所有入侵企图。有关详细信息，请参见手册页和 <http://www.kismetwireless.net/>。

## 29.1.5 建立 WLAN 的提示和技巧

这些提示可帮助精确调整 WLAN 的速度、稳定性和安全性。

### 稳定性和速度

无线网络的性能和可靠性主要取决于参与的工作站是否能够清楚地接收到来自其他工作站的信号。障碍物（例如，墙壁）极大地削弱了信号。信号强度越低，传送速率就越慢。在网络运行过程中，可以在命令行（Link Quality 字



段)中使用 Iwconfig 实用程序或使用 NetworkManager 或 KNetworkManager 来检查信号强度。如果信号质量存在问题,可尝试将设备放在其他位置,或调整访问点天线的位置。很多 PCMCIA WLAN 卡都配有辅助天线,可充分提高接收效果。制造商指定的速率(例如 54Mbit/s)是一个额定值,它表示理论最大值。实际上,最大数据吞吐量不大于该值的一半。

## 安全性

如果要建立一个无线网络,则一定要记住,如果不实施任何安全措施,则传送范围内的任何人都可以方便地访问此网络。因此,一定要激活某种加密方法。所有 WLAN 卡和访问点都支持 WEP 加密。虽然这并非完全安全,但还是对潜在攻击者设置了一道屏障。WEP 通常可满足个人使用。WPA-PSK 的安全性更好,但不能在较早的访问点或具有 WLAN 功能的路由器中实施。在某些设备上,可以通过固件更新来实施 WPAu163 此外, Linux 在所有硬件组件上不支持 WPA。在准备此文档时, WPA 只适用于采用 Atheros、Intel PRO/Wireless 或 Prism2/2.5/3 芯片的卡。在 Prism2/2.5/3 上,仅当使用 hostap 驱动程序时, WPA 才能运行(请参见“有关 Prism2 卡的问题”一节 [492])。如果 WPA 不可用,则使用 WEP 要好过不加密。在具有高级安全要求的企业中,无线网络工作时必须采用 WPA。

## 29.1.6 查错

如果 WLAN 卡未能作出响应,请检查您是否下载了所需的固件。请参考第 29.1.1 节“硬件”[484]。以下几段介绍了一些常见问题。

## 多个网络设备

现在的便携式计算机通常都有网卡和 WLAN 卡,如果使用 DHCP(自动地址指派)来配置这两个设备,则您可能会遇到名称解析和默认网关的问题。可以 Ping 路由器但不能浏览因特网就是这方面问题的典型示例。位于 [http://en.opensuse.org/SDB:Name\\_Resolution\\_Does\\_Not\\_Work\\_with\\_Several\\_Concurrent\\_DHCP\\_Clients](http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients) 的支持数据库提供了一篇有关这一主题的文章。

## 有关 Prism2 卡的问题

采用 Prism2 芯片的设备有多个驱动程序可用。不同的卡与不同的驱动程序之间的适用性是不一样的。使用这些卡时，只有在使用 `hostap` 驱动程序时，才能实施 WPA。如果这样的卡不能正常工作或根本不工作，或者您要使用 WPA，请参见 `/usr/share/doc/packages/wireless-tools/README.prism2`。

## WPA

SUSE Linux Enterprise 是最近才支持 WPA 的，并且仍然在开发中。因此，YaST 并不支持配置所有 WPA 身份验证方法。不是所有无线 LAN 卡和驱动程序都支持 WPA。一些卡需要更新固件以启动 WPA。如果要使用 WPA，请参见 `/usr/share/doc/packages/wireless-tools/README.wpa`。

### 29.1.7 有关详细信息

Jean Tourrilhes 开发了用于 Linux 的无线工具，他的因特网网页上有很多关于无线网络的有用信息。请参见[http://www.hpl.hp.com/personal/Jean\\_Tourrilhes/Linux/Wireless.html](http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html)。

## 部分 IV. 服务



## 基本联网知识

Linux 提供集成进各类网络结构中所需的联网工具和功能。TCP/IP 是 Linux 惯用的协议，具有多种服务和特殊功能，本章将对此进行介绍。使用网卡、调制解调器或其他设备的网络访问可以通过 YaST 来配置。也可以手动进行配置。不过本章的讨论仅限于基本机制和相关网络配置文件。

Linux 和其他 Unix 操作系统均使用 TCP/IP 协议。该协议不是单个网络协议，而是提供多种服务的一系列网络协议。中所列的协议专用于在两台计算机之间通过 TCP/IP 交换数据。表 30.1 “TCP/IP 系列协议中的若干协议” [495] 由 TCP/IP 连接而成的网络构成了世界范围的网络，就整体而言也称作“因特网”。

RFC 代表注释请求。RFC 由一些文档组成，用来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。可以通过 <http://www.ietf.org/rfc.html> 访问这些联机文档。

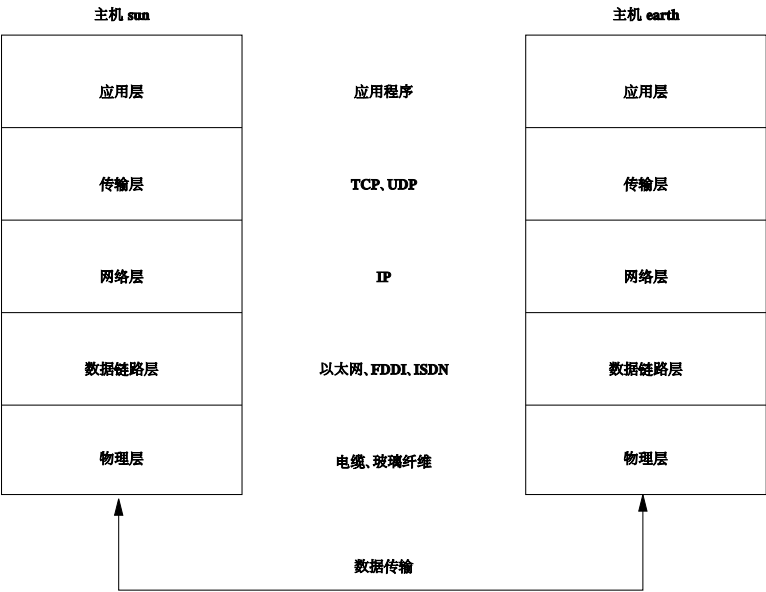
**表 30.1** TCP/IP 系列协议中的若干协议

协议	描述
TCP	传送控制协议：面向连接的安全协议。要传送的数据首先由应用程序作为数据流发送，然后由操作系统转换为相应的格式。数据到达目标主机上的相应应用程序时采用最初发送时的原始数据流格式。TCP 确定传送过程中是否丢失了数据，并确保格式没有混乱。只要涉及到数据序列就会实施 TCP。

协议	描述
UDP	用户数据报文协议：无连接、不安全的协议。要传送的数据以应用程序生成的数据包的形式发送。不能保证数据以正确的顺序到达接收方，还可能丢失数据。UDP 适用于面向记录的应用程序。它的等待时间比 TCP 稍短。
ICMP	因特网控制消息协议：这实际上不是一个面向最终用户的协议，而是一个特殊的控制协议，用来发出错误报告，还可以控制参与 TCP/IP 数据传送的计算机的行为。此外，它还提供一种特殊的回应方式，可以通过 ping 程序查看该方式。
IGMP	因特网组管理协议：此协议控制实施 IP 多路广播时的计算机行为。

如图 30.1 “TCP/IP 的简化层次模型”[496]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 30.1 TCP/IP 的简化层次模型

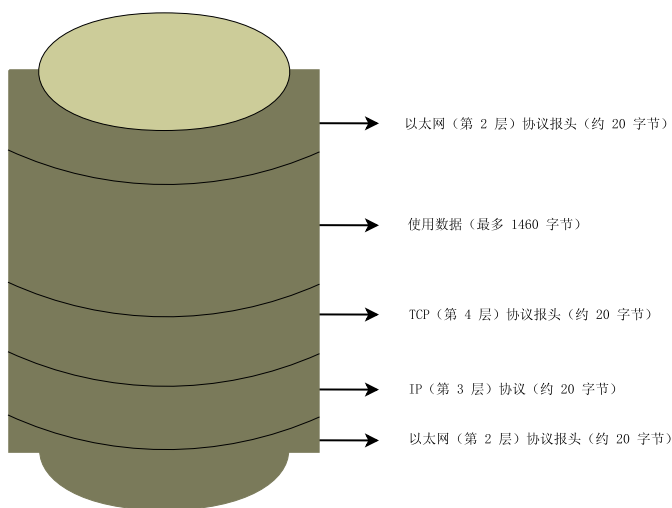


该图为每一层都提供了一到两个示例。层次按照抽象程度排序。最底层非常接近硬件。最上层则几乎就是硬件的完全抽象化。每一层都有自己的特殊功能。每一层的特殊功能多隐含在其描述中。数据链路层和物理层表示所用的物理网络（如以太网）。

几乎所有硬件协议都在面向数据包的基础上发挥作用。因为无法一次传送所有数据，所以要将这些数据封装在包中。TCP/IP 包最大约为 64 KB。通常的包还要小得多，因为可能还要受到网络硬件的限制。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 30.2 “TCP/IP 以太网包”[497] 校验和位于包的末尾而不是开头，这样更便于网络硬件处理。

图 30.2 TCP/IP 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。

## 30.1 IP 地址和路由

各节的论述仅限于 IPv4 网络。有关 IPv6 协议（IPv4 的后续协议）的信息，请参见 [第 30.2 节“IPv6 下一代的因特网”](#) [500]。

### 30.1.1 IP 地址

因特网上的每台计算机都有一个唯一的 32 位地址。这些 32 位（或 4 字节）地址通常按 [例 30.1 “编写 IP 地址”](#) [498] 的第二行所示的格式书写。

#### 例 30.1 编写 IP 地址

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.      168.      0.      20
```

在十进制格式中，四字节以十进制数书写，其间以句点分隔。IP 地址被指派给主机或网络接口。除此之外不能用在其他任何地方。这条规则也有例外，但这些例外与以下消息无关。

IP 地址中的点表示分级系统。直到 20 世纪 90 年代，IP 地址仍然有严格的分类。不过，这个系统经证实太过死板，已经废止。现已改为使用无类别路由 -（CIDR，无类别域间路由）。

### 30.1.2 网络掩码和路由

网络掩码用于定义子网的地址范围。如果两台主机在同一个子网中，则它们可直接相互访问，如果不在同一个子网中，则需要网关地址，它处理子网和其他网络之间的所有流量。要检查两个 IP 地址是否位于同一个子网中，只需分别将两个地址与网络掩码进行“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 30.2 “将 IP 地址链接到网络掩码” [499]。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 30.2 “将 IP 地址链接到网络掩码” [499]中，第一个 24 位也可写作 192.168.0.0/24。

例 30.2 将 IP 地址链接到网络掩码

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
-----
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:      192.      168.      0.      0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
-----
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:      213.      95.      15.      0
```

再举个例子：通过同一以太网电缆相连的所有计算机通常都位于同一子网中，可直接访问。即使用交换机或网桥物理分隔该子网，这些主机仍然可以直接访问。

仅在网关是为目标网络配的时，才能访问本地子网外部的 IP 地址。通常情况下，只有一个网关处理所有外部流量。然而，也可能为不同的子网配置多个网关。

如果配置了网关，所有的外部 IP 包将发送到相应的网关。此网关随后会尝试以相同的方式转发该包（从主机到主机）直到到达目标主机或超过该包的 TTL（存活时间）。

表 30.2 特定地址

地址类型	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 30.2 “将 IP 地址链接到网络掩码” [499] 中的 Result（结果）所示。不能将此地址指派给任何主机。

地址类型	描述
广播地址	这大体表示“访问此子网内的所有主机”。要生成此地址，需要将网络掩码反转为二进制格式，并使用逻辑 OR 链接到基本网络地址。因此，以上示例会生成 192.168.0.255。该地址无法指派给任何主机。
本地主机	地址 127.0.0.1 指派给每台主机的“回路设备”。可以使用此地址与您自己的计算机建立连接。

由于 IP 地址必须在全球范围内唯一，您不能随机选择地址。共有三个地址域可用于建立基于 IP 的专用网络。这些地址无法与因特网上的其他地址建立任何连接，因为它们不能通过因特网传送。这些地址域在 RFC 1597 中指定，并且列在表 30.3 “专用 IP 地址域” [500]中。

表 30.3 专用 IP 地址域

网络/网络掩码	域
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

## 30.2 IPv6 — 下一代的因特网

**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 (Web) 的出现，过去十五年中越来越多的计算机开始通过 TCP/IP 通讯，这使因特网有了突飞猛进的发展。自从 1990 年在 CERN(<http://public.web.cern.ch>) 任职的 Tim Berners-Lee 开创了 WWW，因特网主机的数量已从几千台猛增至上亿台。

如上所述，IPv4 地址只有 32 位。而且还有不少 IP 地址丢失 - 因网络组织结构的原因而无法使用。子网中可用的地址数量是位数的平方减 2。举例来说，某个子网可以有 2 个、6 个或 14 个可用地址。如果要将 128 台主机连接到因特网，您的子网要提供 256 个 IP 地址，其中只有 254 个可用，因为有两个 IP 地址需要供该子网本身的结构使用：广播和基础网络地址。

在当前的 IPv4 协议下，DHCP 或 NAT（网络地址转换）是用来避免出现地址短缺的典型机制。这些方法与用来分隔专用地址空间和公用地址空间的规定相结合，肯定能够缓解短缺状况；它们的问题在于不仅配置烦琐，而且也加重了维护的负担。要在 IPv4 网络内设置主机，您需要若干地址项，如主机本身的 IP 地址、子网掩码、网关地址，可能还要提供名称服务器地址。所有这些项都是必需的，而且无法从其他任何地方得到这些项。

利用 IPv6，地址的短缺和复杂的配置都将成为过去。以下各节进一步描述了 IPv6 带来的改进和优点，以及如何从旧协议过渡到新协议。

## 30.2.1 优点

新协议中最为重要同时也最为显著的改进在于对可用地址空间的极大扩容。IPv6 地址由 128 位值而不是传统的 32 位值组成，它提供的 IP 地址数目多达 10 的 15 次方的若干倍。

不过，IPv6 与以前的不同不仅限于长度，其内部结构也发生了变化，这种结构可以包含更多的有关系统和系统所属网络的具体信息。有关详细信息，请参见第 30.2.2 节“地址类型和结构”[502]。

以下列出了新协议的其他一些优点：

### 自动配置

IPv6 使网络可以支持“即插即用”，这意味着无需任何手动配置即可将新安装的系统集成到（本地）网络中。新主机可以使用其自动配置机制，依赖名为邻居发现(ND)的协议从邻近的路由器提供的信息中得到自己的地址。这种方法不要求管理员参与，并且无需维护用于分配地址的中央服务器 - 这是 ipv4 无法媲美的（在 ipv4 中需要使用 DHCP 服务器来自动分配地址）。

### 移动能力

利用 IPv6，为一个网络接口同时指派多个地址成为可能。这使得用户能方便地访问几个网络，可比作手机公司提供的国际漫游服务：您携带手机出境时，手机一旦进入相应区域就会自动登录外国服务，因此无论您在哪儿，都可以用同一号码联系您，并且可以像在家乡一样拨打电话。

## 安全通讯

在 IPv4 中，网络安全是一项附加功能。IPv6 则将 IPsec 作为其核心功能之一，允许系统通过安全隧道通讯，避免被因特网上的外来者窃听。

## 向后兼容性

实际上，要想将整个因特网一下子从 IPv4 转换为 IPv6 是不可能的。因此，这两个协议不仅要能在因特网上同时存在，还应能够同时存在于一个系统中，这一点至关重要。要实现这一点，一方面两种地址应兼容（IPv4 地址可以轻松转换为 IPv6 地址），另一方面还要使用一定数量的隧道。请参见第 30.2.3 节“IPv4 与 IPv6 并存”[506]。此外，系统可以依赖双栈 IP 技术同时支持两种协议，这意味着系统中有两种完全分开的网络堆栈，从而避免这两种版本的协议相互影响。

## 通过多路广播的自定义服务

在 IPv4 中，有些服务（如 SMB）需要向本地网络中的所有主机广播其数据包。IPv6 则采用一种更为精确的方式，通过多路广播支持服务器对主机寻址，即对属于一组的若干主机寻址（这不同于通过广播对所有主机寻址或通过单路广播对每台主机逐个寻址）。将哪些主机作为一组来寻址可能要取决于具体的应用程序。可使用一些预定义的组来寻址，例如对所有名称服务器寻址（所有名称服务器多路广播组），或对所有路由器寻址（所有路由器多路广播组）。

# 30.2.2 地址类型和结构

如上所述，目前的 IP 协议在两个重要方面有缺陷：IP 地址日益短缺，配置网络、维护路由选择表的任务变得越来越复杂和艰难。IPv6 通过将地址空间扩展到 128 位解决了第一个问题。通过引入分级地址结构，结合先进的网络地址分配技术和多宿主功能（将多个地址指派给同一个设备，从而支持对多个网络的访问），第二个问题也迎刃而解。

使用 IPv6 时，了解三种类型的地址十分有用：

### 单路广播

这类地址只与一个网络接口关联。采用这类地址的包只传递到一个目标。因此，使用单路广播地址可以将包传送到本地网络或因特网上的单个主机。

### 多路广播

这类地址与一组网络接口相关。采用这类地址的包将传递到属于该组的所有目标。多路广播地址主要供特定网络服务使用，用于以有序的方式与特定的主机组通讯。

任意广播

这类地址与一组接口相关。采用这类地址的包将根据基础路由协议的原则，传递给该组中与发送方最为接近的成员。任意广播地址便于主机在特定网络区域内找到提供特定服务的服务器。同一类型的所有服务器都具有相同的任意广播地址。在请求服务时，主机会收到路由协议决定的最接近它的服务器的回复。如果出于某种原因此服务器无法回复，协议会自动选择距离稍远一些的服务器，依此类推。

IPv6 地址分为八组，每组四位数字，代表十六位，采用十六进制表示法。各组之间用冒号 (:) 分隔。可以删除某组中的前置零字节，但不能删除组中或组末的零。另一个约定是：连续的零字节若超过四个，则可以省略为双冒号形式。不过，每个地址只允许有一个这样的 ::。中演示了这种简写表示法，其中的三行全部表示同一地址。例 30.3 “示例 IPv6 地址” [503]

例 30.3 示例 IPv6 地址

```
fe80 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                                : 10 : 1000 : 1a4
```

IPv6 地址的每个部分都有明确的功能。前面的字节构成前缀，用于指定地址类型。中间部分是地址的网络部分，但可以不用。地址的结尾构成主机部分。在 IPv6 中，网络掩码是通过在地址末尾的斜杠后指明前缀的长度来定义的。例 30.4 “指定前缀长度的 IPv6 地址” [503] 中的地址包含上述信息，即：前 64 位构成地址的网络部分，后 64 位构成地址的主机部分。换言之，64 表示网络掩码由左起的 64 个 1 位值构成。正如 IPv4，要用 AND 将 IP 地址与子网值结合起来，以确定主机位于同一子网中还是其他网络中。

例 30.4 指定前缀长度的 IPv6 地址

```
fe80::10:1000:1a4/64
```

IPv6 可以识别几种预定义的前缀类型。其中有些列在表 30.4 “各种 IPv6 前缀” [503] 中。

表 30.4 各种 IPv6 前缀

前缀（十六进制）	定义
00	IPv4 地址和 IPv6 上的 IPv4 兼容地址。这些用于与 IPv4 保持兼容。要使用这些地址，仍然需要依赖路由器将

前缀（十六进制）	定义
	IPv6 包转换为 IPv4 包。有若干特殊地址（如用于回路设备的地址）也采用此前缀。
2 或 3 作为第一个数字	可聚合全局单路广播地址。类似 IPv4 的情况，可以指定某个接口作为特定子网的一部分。目前，有以下地址空间：2001::/16（生产质量地址空间）和 2002::/16（6to4 地址空间）。
fe80::/10	链路本地地址。不应路由带有这种前缀的地址，而只能从同一子网中访问。
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。

站点拓朴结构

第二部分包含要将包传递到的子网的路由信息。

接口 ID

第三部分标识要将包传递到的接口。其中允许使用 MAC。由于 MAC 是硬件厂商编程到设备中的全球唯一的固定标识符，配置过程得到了极大简化。事实上，前 64 个地址位共同构成 EUI-64 令牌，后 48 位从 MAC 中提取，其余的 24 位包含有关令牌类型的特殊信息。这样还可以将 EUI-64 令牌指派给没有 MAC 的接口，如基于 PPP 或 ISDN 的接口。

在这个基础结构之上，IPv6 还区分五种不同的单路广播地址：

:: (未指定)

在首次初始化接口时，即无法通过其他方法确定地址时，这类地址可用作主机的源地址。

::1 (回路)

回路设备的地址。

### IPv4 兼容地址

IPv6 地址由 IPv4 地址和 96 个零位组成的前缀构成。这类兼容地址用于隧道通讯进程（请参见第 30.2.3 节“IPv4 与 IPv6 并存”[506]），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。

## 30.2.3 IPv4 与 IPv6 并存

将与因特网相连的所有主机从 IPv4 迁移到 IPv6 是一个逐步的过程。这两种协议将在未来一定时间内并存。通过双栈技术来实施这两种协议，可以在同一系统上同时支持这两种协议。但这仍然没有解决支持 IPv6 的主机如何与 IPv4 主机通讯，以及应如何通过当前网络（主要基于 IPv4）传输 IPv6 包的问题。最好的解决方案就是提供隧道处理功能和兼容地址（请参见第 30.2.2 节“地址类型和结构”[502]）。

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。

## 30.2.4 配置 IPv6

要配置 IPv6，通常无需在各个工作站上执行任何更改。默认情况下启用 IPv6。安装期间，您可以在第 3.14.3 节“网络配置”[35]中所述的网络配置步骤中禁用它。要在已安装系统上禁用或启用 IPv6，请使用 YaST 网卡。不要更改方式，单击下一步。然后选择卡，单击地址选项卡中的高级>IPv6。要手动启用 IPv6，请以 root 身份输入 `modprobe ipv6`。

由于 IPv6 使用自动配置，将给网卡指派链路-本地网络中的地址。一般不在工作站上管理路由选择表。工作站可以使用路由器广告协议查询网络路由器，了解应实施的前缀和网关。使用 `radvd` 程序可以设置 IPv6 路由器。此程序会通知工作站对 IPv6 地址使用哪个前缀和哪个路由器。或者，可以使用 `zebra` 自动配置两个地址和路由选择。

有关如何使用 `/etc/sysconfig/network` 文件设置各种隧道的信息，请参见 `ifup(8)` 手册页。

## 30.2.5 有关详细信息

上文的概述中并未全面论述 IPv6 这一主题。有关这种新协议的深入讨论，请参见以下联机文档和书目：

<http://www.ipv6.org/>

学习 IPv6 知识的起点。

<http://www.ipv6day.org>

启动您自己的 IPv6 网络所需的所有信息。

<http://www.ipv6-to-standard.org/>

已启用 IPv6 的产品列表。

<http://www.bieringer.de/linux/IPv6/>

在此可找到 Linux IPv6-HOWTO 以及许多与该主题有关的链接。

RFC 2640

有关 IPv6 的基础 RFC。

IPv6 Essentials

Silvia Hagen 所著的 *IPv6 Essentials*(ISBN 0-596-00125-8) 中描述了该主题的所有重要方面。

## 30.3 名称解析

DNS 有助于将 IP 地址指派给一个或多个名称，并将名称指派给 IP 地址。在 Linux 中，这种转换通常由一种特殊的称为 bind 的软件来完成。负责这种转换的计算机称为**名称服务器**。这些名称构成了分级系统，各个名称组成部分之间用圆点分隔。不过，这个名称层次与上述 IP 地址层次无关。

考虑以 `hostname.domain` 格式书写的完整名称，如 `earth.example.com`。完整名称，即**完全限定的域名(fqdn)**，由主机名和域名(`example.com`)组成。后者还包含**顶级域或 TLD**(`com`)。

TLD 的指派由于历史原因已经变得十分混乱。传统的指派方法是美国所用的三字母域名，而世界其他地方采用的标准是双字母 ISO 国家/地区代码。此外，2000 年还引进了较长的 TLD，表示特定的活动领域（例如 `.info`、`.name` 和 `.museum`）。

在因特网发展的早期阶段（1990 年之前），文件 `/etc/hosts` 被用来储存因特网上表示的所有计算机的名称。后来事实证明随着接入因特网的计算机与日俱增，这种方法很快就行不通了。为此人们开发了一个分散式数据库，以十分分散的方式储存主机名。这个数据库类似名称服务器，它并不储存与因特网上的所有主机相关的数据，但可以向其他名称服务器发送请求。

位于层次顶级的是**根名称服务器**。这些根名称服务器管理顶级域，并由网络信息中心 (NIC) 运行。每个根名称服务器都了解负责特定顶级域的名称服务器。有关顶级域 NIC 的信息，请参见 <http://www.internic.net>。

DNS 不仅可以解析主机名，还能够为整个域识别出负责接收整个域的电子邮件的主机 - **邮件交换器 (MX)**。

为解析 IP 地址，您的计算机必须了解至少一个名称服务器及其 IP 地址。借助 YaST 可以轻松指定这样的名称服务器。如果建立的是调制解调器拨号连接，则根本无需手动配置名称服务器。拨号协议可以在建立连接后提供名称服务器

的地址。有关如何使用 SUSE Linux Enterprise® 配置名称服务器访问，请参见第 33 章 **域名系统** [555]。

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。另请阅读 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>。

---

## 30.4 使用 YaST 配置网络连接

Linux 上有多个支持的联网类型。其中多数使用不同的设备名，配置文件分布在文件系统上的多个位置。关于手动网络配置方面的详细概述，请参见第 30.7 节 **“手动配置网络连接”** [528]。

在安装过程中，可使用 YaST 自动配置所有已检测的接口。安装后，可在已安装的系统中随时配置额外的硬件。以下各节将介绍 SUSE Linux Enterprise 支持的所有类型的网络连接的配置。

---

**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。

---

### 30.4.1 使用 YaST 配置网卡

要在 YaST 中配置网络有线网卡或无线网卡，请选择 **网络设备 > 网卡**。启动 YaST 模块后，其中将显示一个常规网络配置对话框。选择是使用 YaST 还是 NetworkManager 来管理所有网络设备。如果想使用 YaST 按照传统方法配置网络，请选中 **通过 ifup 的传统方法**，然后单击 **下一步**。要使用 NetworkManager，

请选择使用 *NetworkManager* 控制用户，然后单击下一步。有关 *NetworkManager* 的更多详细信息，请参见第 30.6 节“使用 *NetworkManager* 管理网络连接”[526]。

**注意：网络连接方法和 Xen**

*NetworkManager* 不能用于 Xen。Xen 中只能使用通过 *ifup* 的传统方法。

下一对话框的上部会显示列个列表，列出适用于配置的所有网卡。所有已正确检测的网卡将连同其名称一起列出。要更改选定设备的配置，请单击编辑。可使用添加配置未能检测到的设备，如“配置未检测到的网卡”一节 [515]中所述。

**图 30.3 配置网卡**



## 更改网卡的配置

要更改网卡的配置，请在 YaST 网卡配置模块中已检测到的网卡列表选择一个网卡，然后单击编辑。将显示网络地址设置对话框，可在其中使用地址和常规选项卡调整网卡配置。有关无线网卡配置的信息，请参见第 29.1.3 节“用 YaST 配置”[487]。

## 配置 IP 地址

安装期间可用的有线网卡可能会自动被配置为使用自动地址设置和 DHCP。

---

### 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。

---

如果您用的是 DSL 线路，但 ISP 没有指派静态 IP，则此时还应该使用 DHCP。如果决定使用 DHCP，请在 *DHCP 客户机选项* 中配置详细信息。可通过选择 *高级 > DHCP 选项* 来从 *地址选项卡* 查找此对话框。指定 DHCP 服务器是否应始终允许广播请求并允许使用标识符。如果您使用虚拟主机设置，其中不同的主机都通过同一接口通信，则需要用标识符来区分它们。

DHCP 比较适合客户机配置，但不太适合服务器配置。要设置静态 IP 地址，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击 *编辑*。
- 2 在 *地址选项卡* 中，选择 *静态地址设置*。
- 3 输入 *IP 地址* 和 *子网掩码*。
- 4 单击“下一步”。
- 5 要激活配置，请单击 *完成*。

如果使用静态地址，则不会自动配置名称服务器和默认网关。要配置网关，请单击 *路由选择* 并添加默认网关。要配置名称服务器，请单击 *主机名和名称服务器* 并添加名称服务器和域的地址。

## 配置别名

一个网络设备可以有多个 IP 地址，称为别名。要为网络设置别名，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击 *编辑*。

- 2 在地址选项卡中，选择高级 > 其他地址。
- 3 单击“添加”。
- 4 输入别名、IP 地址和网络掩码。
- 5 单击确定。
- 6 再次单击“确定”。
- 7 单击“下一步”。
- 8 要激活配置，请单击完成。

## 配置主机名和 DNS

如果安装期间没有更改网络配置并且有线网卡可用，则将为计算机自动生成主机名并且会激活 DHCP。这同样适用于主机连接到网络环境所需的名称服务信息。如果网络地址设置使用了 DHCP，则会向域名服务器列表自动填充相应数据。如果希望使用静态设置，则手动设置这些值。

要更改计算机名称并调整名称服务器搜索列表，则如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击编辑。
- 2 在地址选项卡中，单击主机名和名称服务器。
- 3 要禁用 DHCP 驱动的主机名配置，请取消选择通过 DHCP 更改主机名。
- 4 输入主机名，如果需要，还输入域名。
- 5 要禁用 DHCP 驱动的名称服务器列表更新，请取消选择通过 DHCP 更新名称服务器和搜索列表。
- 6 输入名称服务器和域搜索列表。
- 7 单击确定。
- 8 单击“下一步”。

9 要激活配置，请单击完成。

## 配置路由选择

要使计算机能够与其他计算机和其他网络进行通信，必须提供路由选择信息以使网络流量使用正确的路径。如果使用 DHCP，则将自动提供此信息。如果使用静态设置，则必须手动添加此数据。

- 1 在 YaST 网卡配置模块的已检测到的网卡列表选择一个网卡，然后单击编辑。
- 2 在地址选项卡中，单击路由选择。
- 3 输入默认网关的 IP。
- 4 单击确定。
- 5 单击“下一步”。
- 6 要激活配置，请单击完成。

## 添加特殊硬件选项

有时，网卡模块会需要特殊参数以正确运行。要使用 YaST 来设置这些参数，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表选择一个网卡，然后单击编辑。
- 2 在地址选项卡中，单击高级 > 硬件细节。
- 3 在选项中，为网卡输入参数。如果两个网卡配置为使用相同模块，则这些参数将同时用于这两个网卡。
- 4 单击确定。
- 5 单击“下一步”。
- 6 要激活配置，请单击完成。

## 启动设备

如果您使用通过 ifup 的传统方法，则可以在引导期间、连接电缆后、检测到网卡后、手动启动或从不启动要配置的设备。要更改设备启动，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表选择一个网卡，然后单击 *编辑*。
- 2 在 *常规* 选项卡中，从 *设备激活* 选择所希望的项。
- 3 单击“下一步”。
- 4 要激活配置，请单击 *完成*。

## 配置防火墙

无须输入详细的防火墙设置（如第 43.4.1 节“使用 YaST 配置防火墙” [742] 中所述），您就能在设备设置过程中确定设备的基本防火墙设置。按如下所示继续：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表选择一个网卡，然后单击 *编辑*。
- 2 进入网络配置对话框的 *常规* 选项卡。
- 3 确定应指派接口的防火墙区域。下列选项可用：

*无区域，阻止所有交通*

将阻止此接口的所有通讯。

*内部区域（未保护）*

防火墙运行，但不会强制执行任何规则来保护此接口。仅当计算机属于受外置防火墙保护的大型网络时才使用此选项。

*隔离区域*

隔离区域是位于内部网络和（恶意）因特网之前的附加防线。可从内部网络和因特网访问指派到此区域的主机，但指派到此区域的主机无法访问内部网络。

*外部区域*

防火墙在此接口上运行并且全面保护其不受其他（假设为恶意）网络流量攻击。这是默认选项。



- 4 单击“下一步”。
- 5 单击完成即可激活配置。

## 配置未检测到的网卡

网卡可能会未被正确检测到。在此情况下，已检测到网卡列表中不会包含此网卡。如果确定系统包含网卡的驱动程序，则可以手动对其进行配置。要配置未检测到的网卡，请如下继续操作：

- 1 单击“添加”。
- 2 从可用选项（*配置名称和模块名称*）设置接口的设备类型。如果网卡为 PCMCIA 或 USB 设备，则激活相应的复选框，并选择下一步退出此对话框。否则，请在从列表中*选择*中选择您的网卡型号。然后，YaST 将自动选择适合网卡的内核模块。

硬件配置名称指定 `/etc/sysconfig/hardware/hwcfg-*` 文件的名称，该文件包含网卡的硬件设置。它包含内核模块的名称以及初始化硬件所需的选项。

- 3 单击“下一步”。
- 4 在*地址*选项卡中，设置接口的设备类型、配置名称和 IP 地址。要使用静态地址，请选择*静态地址设置*，然后完成 *IP 地址*和*子网掩码*。在此处，还可选择配置主机名、名称服务器和路由选择详细信息（请参见“*配置主机名和 DNS*”一节 [512]和“*配置路由选择*”一节 [513]）。

如果选择无线作为接口的设备类型，则在下一个对话框中配置无线连接。有关无线设备配置的详细信息可在第 29.1 节“*无线 LAN*” [483]中获得。

- 5 在*常规*选项卡中，设置防火墙区域和设备激活。通过用户控制向一般用户授权连接控制。
- 6 单击“下一步”。
- 7 要激活新网络配置，请单击完成。

有关配置名称约定的信息，请参见 `getcfg(8)` 的手册页。

# 30.4.2 调制解调器

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。如果未自动检测到您的调制解调器，请单击添加，打开用于手动配置的对话框。在随后打开的对话框中，请在调制解调器设备下输入调制解调器连接到的接口。

提示：CDMA 和 GPRS 调制解调器

就跟配置普通调制解调器一样，用 YaST 调制解调器模块配置支持的 CDMA 和 GPRS 调制解调器。

图 30.4 调制解调器配置



如果处在专用交换机 (PBX) 之后，则可能需要输入拨号前缀。该前缀通常是零。请参考随 PBX 附带的描述了解相关信息。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不具备根权限的普通用户，请激活**用户控制**。这样，不具备管理员权限的用户即可激活或取消激活某个接口。在**拨号前缀正则表达式**下，指定正则表达式。KInternet 中的**拨号前缀**（可由普通用户修改）必须符合此正则表达式。如果将此字段留空，用户则无法在不具备管理员权限的情况下设置其他**拨号前缀**。

在下一个对话框中，选择 ISP（因特网服务提供者）。要从您所在国家/地区的 ISP 的预定义列表中进行选择，请选择**国家/地区**。也可以单击**新建**打开一个对话框，从中为您的 ISP 提供数据。这些数据包括用于拨号连接的名称、ISP 的名称，以及 ISP 提供的登录名和密码。启用**始终询问密码**，在您每次连接时都提示输入密码。

在最后一个对话框中，指定附加连接选项：

#### **按需拨号**

如果启用**按需拨号**，请设置至少一个名称服务器。

#### **连接后修改 DNS**

默认情况下启用此选项，其作用是在每次连接因特网时都更新名称服务器地址。

#### **自动检索 DNS**

如果提供者未在连接后传送其域名服务器，则禁用此选项并手动输入 DNS 数据。

#### **愚蠢方式**

默认情况下该选项是启用的。通过它可以忽略 ISP 服务器发送的输入提示，防止它们影响连接进程。

#### **外部防火墙接口**

选择此选项将激活 SUSEfirewall2 并将接口设置为外部。这样系统就可以在连接到因特网期间防范外部攻击。

#### **空闲超时（秒）**

使用此选项可以指定网络不活动的时间，一超过该时间调制解调器即自动断开连接。

IP 详细信息

使用此选项可打开地址配置对话框。如果您的 ISP 没有为您的主机指派动态 IP 地址，请禁用*动态 IP 地址*，然后输入主机的本地 IP 地址及远程 IP 地址。请向您的 ISP 询问这些信息。保持*默认路由*的启用状态，然后通过选择*确定*关闭该对话框。

选择下一步可返回初始对话框，其中显示调制解调器配置的概要。选择完成可关闭此对话框。

30.4.3 ISDN

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 未能检测到您的 ISDN 网卡，则请单击*添加*并以手动方式选择。可以使用多个接口，但您可以为一个接口配置多个 ISP。在随后的对话框中，设置该网卡正常工作所需的 ISDN 选项。

图 30.5 ISDN 配置

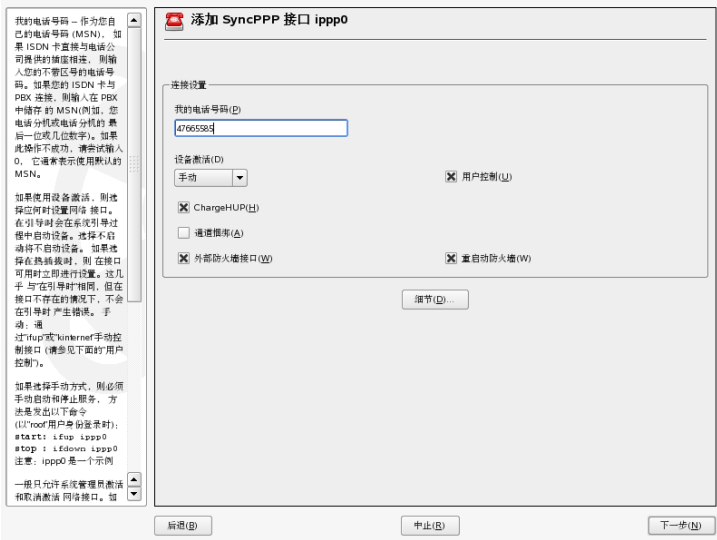


在下一个对话框中（如图 30.5 “ISDN 配置” [518]所示），选择要使用的协议。默认值是 *Euro-ISDN (EDSSI)*，但是对于旧式或大型交换机，请选择 *1TR6*。如果是在美国，请选择 *NII*。在相关字段中选择您所在的国家/地区。相应的国家/地区代码将显示在该字段旁边的字段中。最后，提供您的区号和拨号前缀（如果需要）。

设备激活定义如何启动 ISDN 接口：使用引导时可以在系统每次引导时初始化 ISDN 驱动程序。手动要求您以 root 的身份使用命令 `rcisdn start` 来装载 ISDN 驱动程序。热插拔，用于 PCMCIA 或 USB 设备，用于在插入设备后加载驱动程序。在完成这些设置后，请选择确定。

在下一个对话框中，为您的 ISDN 网卡指定接口类型，并将 ISP 添加到现有接口中。接口的类型可能是 SyncPPP 或 RawIP，但多数 ISP 以 SyncPPP 方式操作，如下文所述。

图 30.6 ISDN 接口配置



要为我的电话号码输入的值取决于特定的设置：

ISDN 网卡直接连接到电话插座

标准的 ISDN 线路提供三个电话号码（称为多用户号码或 MSN）。如果用户需要更多号码，最多可提供十个号码。必须在此处输入其中一个 MSN，

但不要区号。如果输入的号码有误，您的电话运营商将自动退回到为您的 ISDN 线路指派的第一个 MSN。

## ISDN 网卡连接到专用交换机

同样，配置可能随安装设备的不同而变化：

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。有关进一步信息，请参见随电话交换机附带的文档。

2. 为公司设计的大型电话交换机通常使用 1TR6 协议用于内部呼叫。它们的 MSN 称为 EAZ 并且通常对应直拨号码。要在 Linux 中配置，只需输入 EAZ 的最后一位即可。如果各种方法都行不通，可尝试 1 到 9 之间的各位数字。

要在下一个收费单位开始之前及时终止连接，请启用 *ChargeHUP*。但要记住，该选项不是对每个 ISP 都奏效。您也可以通过选择相应的选项启用信道绑定（多链接 PPP）。最后，您可以通过选择外部防火墙接口和重启防火墙为链接启用 SUSEfirewall2。要使不具备管理员权限的普通用户能够激活或取消激活接口，请选中 *用户控制*。

*细节*将打开一个对话框，在其中配置回拨方式、到此接口的远程连接和其他 *ipppd* 设置。通过选择 *确定*退出 *细节*对话框。

在下一个对话框中设置 IP 地址。如果您的提供者没有为您指定静态 IP，请选择 *动态 IP 地址*。否则，根据 ISP 指定的信息，使用提供的字段输入您主机的本地 IP 地址及远程 IP 地址。如果接口应该成为与因特网连接的默认路由，请选择 *默认路由*。每台主机都只能有一个接口配置为默认路由。选择 *下一步*可退出此对话框。

使用随后的对话框，您可以设置您所在的国家/地区并选择 ISP。列表中的 ISP 都只是 *call-by-call*（通过呼叫进行呼叫）提供者。如果列表中未列出您的 ISP，请选择 *新建*。随即打开 *提供者参数*对话框，可以在其中输入 ISP 的所有详细信息。输入电话号码时，切勿在数字之间加空格或逗号。最后，输入 ISP 为您提供的登录名和密码。输完之后，请选择 *下一步*。

要在独立工作站上使用按需拨号，还需指定名称服务器（DNS 服务器）。多数 ISP 都支持动态 DNS，这意味着每次用户连接时，都由 ISP 发送名称服务器的 IP 地址。不过，对于单个工作站，您仍然需要提供 192.168.22.99 之类的占位符地址。如果您的 ISP 不支持动态 DNS，请指定 ISP 的名称服务器 IP 地址。如果需要，可以为连接指定超时值 — 即网络不活动的时间（以秒计），一超过该时间即自动终止连接。选择下一步确认设置。YaST 将显示配置好的接口的概要。要使所有这些设置有效，请选择完成。

## 30.4.4 电缆调制解调器

---

**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。

---

在有些国家/地区（例如奥地利和美国），人们往往通过有线电视网访问因特网。有线电视用户通常将调制解调器一端接在有线电视插座上，另一端与计算机网卡相连（使用 10Base-TG 双绞线）。随后电缆调制解调器就能通过固定 IP 地址提供专用因特网连接。

在配置网卡时需要根据您的 ISP 提供的说明选择 *自动地址设置（通过 DHCP）* 或 *静态地址设置*。目前多数提供商都使用 DHCP。通常只有特殊的公司帐户才使用静态 IP 地址。

有关配置电缆调制解调器的进一步信息，请联机访问 [http://en.opensuse.org/SDB:Setting\\_Up\\_an\\_Internet\\_Connection\\_via\\_Cable\\_Modem\\_with\\_SuSE\\_Linux\\_8.0\\_or\\_Higher](http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higher)，阅读关于这一主题的“支持数据库”文章。

## 30.4.5 DSL

---

**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

基于 PPPoE 或 PPTP 配置 DSL 连接时，要求已经正确设置相应的网卡。如果尚未这样做，应首先通过选择配置网卡来配置网卡（请参见第 30.4.1 节“使用 YaST 配置网卡” [509]）。使用 DSL 链接时，可以自动指派地址但并不通过 DHCP，这就是不应启用自动地址设置（通过 DHCP）选项的原因。相反，应该为接口输入静态虚设地址，如 192.168.22.1。在子网掩码中，输入 255.255.255.0。如果配置的是独立工作站，则将默认网关留空。

---

**提示**

IP 地址字段和子网掩码中的值只是占位符。它们只用于初始化网卡，而不会将 DSL 链接表示成这样。

---

**图 30.7 DSL 配置**



要着手配置 DSL（请参见图 30.7 “DSL 配置” [522]），首先应选择 PPP 方式及 DSL 调制解调器连接到的 Ethernet 网卡（多数情况下是 eth0）。然后使用设



备激活指定是否应在引导进程中建立 DSL 链接。单击 *用户控制* 可授权不具备根权限的普通用户通过 **KInternet** 激活或取消激活接口。使用该对话框还可以选择您所在的国家/地区，并可以在该区域内的若干 ISP 中进行选择。随后的所有 DSL 配置对话框的详细信息都取决于目前已设置的选项，因此下面几段只对这些对话框进行了简要介绍。有关可用选项的详细信息，请阅读这些对话框中提供的详细帮助信息。

要在独立工作站上使用 *按需拨号*，还需指定名称服务器（DNS 服务器）。多数 ISP 都支持动态 DNS — 每次用户连接时，都由 ISP 发送名称服务器的 IP 地址。不过，对于单个工作站，应提供 192.168.22.99 之类的占位符地址。如果您的 ISP 不支持动态 DNS，请输入 ISP 提供的名称服务器 IP 地址。

*空闲超时（秒）* 定义网络不活动的时间，一超过该时间即自动终止连接。合理的超时值介于 60 到 300 秒之间。如果禁用了 *按需拨号*，则最好将超时值设置为零以防止自动挂断。

T-DSL 的配置与 DSL 的设置非常相似。只需将 *T-Online* 选为您的提供者，YaST 将打开 T-DSL 配置对话框。在此对话框中，提供 T-DSL 所需的一些其他信息——线路 ID、T-Online 号码、用户代码和密码。所有这些信息都会包含在订阅到 T-DSL 后收到的信息中。

## 30.4.6 IBM System z：配置网络设备

用于 IBM System z 的 SUSE Linux Enterprise 支持几种不同类型的网络接口。可使用 YaST 来配置所有接口。

### qeth-hsi 设备

要将 `qeth-hsi` (Hipersocket) 接口添加到已安装系统中，请启动 YaST 网卡模块（*网络设备 > 网卡*）。选择标记为 *IBM Hipersocket* 的设备之一，用作 READ 设备地址，然后单击 *配置*。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 *完成* 退出网络配置。

### 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 网卡模块（*网络设备 > 网卡*）。选择标记为 *IBM OSA Express Ethernet* 网卡的设备之一，用作 READ 设备地址，然后单击 *配置*。输入所需端

口名称、一些附加选项（请参见位于 [http://www.ibm.com/developerworks/linux/linux390/documentation\\_novell\\_suse.html](http://www.ibm.com/developerworks/linux/linux390/documentation_novell_suse.html) 的手册 *Linux for IBM zSeries: Device Drivers, Features, and Commands*（Linux for IBM zSeries：设备驱动程序、功能和命令））、您的 IP 地址及相应的网络掩码。选择 **下一步**和**完成**退出网络配置。

## 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 网卡模块（**网络设备 > 网卡**）。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。选择 **下一步**和**完成**退出网络配置。

---

### 警告

不建议使用此接口。在 SUSE Linux Enterprise 的未来版本中将不支持此接口。

---

## 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 网卡模块（**网络设备 > 网卡**）。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](http://www.ibm.com/developerworks/linux/linux390/documentation_novell_suse.html) 的手册 *Linux for IBM zSeries: Device Drivers, Features, and Commands*（Linux for IBM zSeries：设备驱动程序、功能和命令））、您的 IP 地址及相应的网络掩码。选择 **下一步**和**完成**退出网络配置。

## IUCV 设备

要将 `iucv`（IUCV）接口添加到已安装系统中，请启动 YaST 网卡模块（**网络设备 > 网卡**）。选择标记为 *IUCV* 的设备，然后单击**配置**。YaST 将提示您输入 IUCV 合作伙伴的名称。输入该名称（此项区分大小写），然后选择**下一步**。指定您的 IP 地址及合作伙伴的 IP 地址。如果需要，可使用**高级 > 详细设置**调整 MTU 的大小。选择 **下一步**和**完成**退出网络配置。

警告

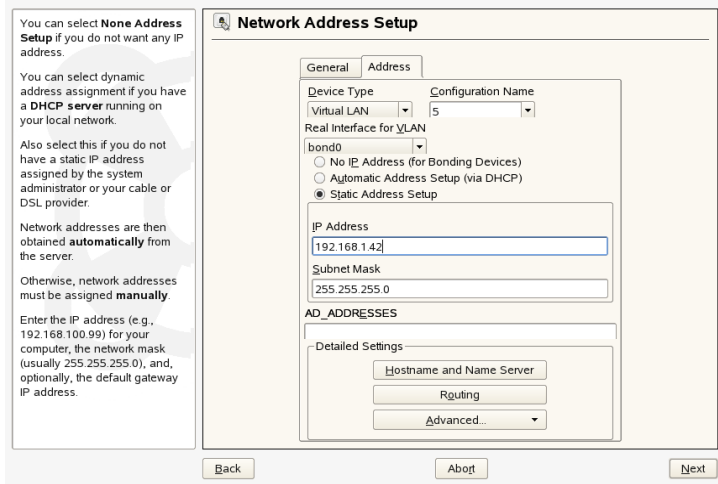
不建议使用此接口。在 SUSE Linux Enterprise 的未来版本中将不支持此接口。

# 30.5 在 SUSE Linux 上配置 VLAN 接口

VLAN 是虚拟局域网 (Virtual Local Area Network) 的缩写。它允许通过单个物理 Ethernet 运行多个逻辑 (虚拟) Ethernet。它以逻辑方式将网络分为不同的广播域, 以便数据包仅在为同一 VLAN 指定的端口之间交换。如果要在网络安装中使用 VLAN, 请确保安装了软件包 `vlan`。

如果 Linux 的网络连接不是专门用于特定逻辑 LAN 的, 则可以设置访问一个或多个此类逻辑 LAN。通过普通的 `ifup` 支持 VLAN 接口配置, 同时也对所有其他网络接口使用 `ifdown` 脚本。YaST 支持安装 VLAN 设备。

图 30.8 YaST VLAN 配置



运行 YaST 模块网络设备 > 网卡, 选择使用 `ifup` 的传统方法, 然后按下一步。遵循该过程实际安装 VLAN 设备。

## 过程 30.1 使用 YaST 设置 VLAN 接口

- 1 按添加可创建新的网络接口。

- 2 在网络配置中，选择设备类型 *虚拟 LAN*。
- 3 将配置名称的值更改为 VLAN 的 ID。请注意 VLAN ID 1 通常用于管理用途。
- 4 按下一步。
- 5 将 VLAN 设备应连接到的借口选择为下面的 *VLAN 的实际接口*。
- 6 选择将 IP 地址指派到 VLAN 设备的所需方法。
- 7 按下一步完成配置。

关于 VLAN 的更多信息，请参见<http://www.candelatech.com/~greear/vlan.html>和 `/usr/share/doc/packages/vlan/` 处的软件包文档。

## 30.6 使用 NetworkManager 管理网络连接

NetworkManager 是一种用于移动工作站的理想解决方案。有了 NetworkManager，您无需担忧要在更改位置时重配置网络接口和在网络之间切换。NetworkManager 可以自动连接到已知的 WLAN 网络。如果有两种或多种连接选择，则连接速度可能会更快一些。

NetworkManager 在以下情况下不适用：

- 您要通过一个接口使用多个提供商拨号。
- 您的计算机是网络的路由器。
- 您的计算机将为网络中的其他计算机（例如，DHCP 或 DNS 服务器）提供网络服务。
- 您的计算机为 Xen 服务器或您的系统是 Xen 内的虚拟系统。
- 您想在网络配置管理中使用 SCPM。如果同时使用 SCPM 和 NetworkManager，SCPM 就无法控制网络资源。.

- 您想要同时使用多个活动的网络连接。

要在安装期间启用或禁用 NetworkManager，请单击网络配置的网络模式中的启用 *NetworkManager* 或禁用 *NetworkManager*。要在已安装系统上启用或禁用 NetworkManager，请遵循以下步骤：

- 1 打开 YaST。
- 2 选择 *网络设备 > 网卡*。
- 3 在第一个屏幕上，将网络安装方法选项设置到使用 *NetworkManager* 的用户控制来使用 NetworkManager。要禁用 NetworkManager，将网络安装方法设置到通过 *ifup* 的传统方法。

选择方法后，请使用通过 DHCP 或静态 IP 地址的自动配置安装网卡，或配置您的调制解调器。在[第 30.4 节“使用 YaST 配置网络连接”](#) [509]和[第 29.1 节“无线 LAN”](#) [483]中查找 YaST 网络配置的描述。直接在 NetworkManager 中配置所支持的无线网卡。

要配置 NetworkManager，请使用 NetworkManager 小程序。KDE 和 GNOME 都具有各自的 NetworkManager 小程序。适当的小程序会随着桌面环境一起自动启动。该小程序之后会在系统盘中显示为图标。这两种小程序的功能相似，但是它们的接口有些不同。它们还能用在支持标准系统盘的其他图形环境中。

## 30.6.1 ifup 和 NetworkManager 的区别

如果使用 NetworkManager 进行网络安装，则可以使用一个小程序，随时从您的桌面环境内轻松地开关、停止或启动网络连接。NetworkManager 也可以改变和配置无线网卡连接，无需 root 特权。因此，NetworkManager 是一种用于移动工作站的理想解决方案。

使用 ifup 的传统配置也提供一些开关、停止或启动连接的方法，或需要或不需要用户参与（如用户管理设备），但通常需要 root 特权来改变或配置网络设备。这对于移动计算常常是个问题，因为移动计算不可能预配置所有的连接功能。

传统配置和 NetworkManager 都可以处理与无线网络（WEP、WPA-PSK 和 WPA-Enterprise 访问）、拨号连接和使用 DHCP 和静态配置的有线网络之间的网络连接。它们也支持通过 VPN 的连接。

NetworkManager 尝试使用可用的最好连接使您的计算机随时保持连接状态。如果可用，它使用最快的有线连接。如果网络电缆意外断开，它将尝试重连接。它可以从您的无线连接列表中找到带有最佳信号强度的网络并自动用其进行连接。要用 ifup 获得同样的功能，需要花功夫进行配置。

## 30.6.2 有关详细信息

有关 NetworkManager 的信息，可以从以下 网站和目录处获取：

- <http://www.gnome.org/projects/NetworkManager/>—NetworkManager 项目页
- <http://en.opensuse.org/Projects/KNetworkManager>—NetworkManager KNetworkManager 项目页

## 30.7 手动配置网络连接

应该始终将手动配置网络软件作为最后的选择。建议使用 YaST。但是，对网络配置背景信息的了解将对您使用 YaST 有所帮助。

可以通过热插拔检测并配置所有内置网卡及热插拔网卡（PCMCIA、USB 和某些 PCI 卡）。系统以两种不同的方式处理网卡，首先将其作为物理设备对待，其次将其作为接口对待。设备的插入或检测将触发一个热插拔事件。此热插拔事件通过脚本 hwup 触发设备的初始化。当将网卡作为新网络接口进行初始化时，内核将生成另一个热插拔事件，该事件触发通过 ifup 设置接口的操作。

内核按照接口注册的时间顺序对接口名进行编号。对于名称的指派，初始化顺序是决定性的。如果多个网卡中的一个失败，则所有随后初始化的网卡的编号将发生变化。对于真正的可热插拔网卡，连接设备的顺序非常重要。

为了实现灵活的配置，设备（硬件）的配置和接口的配置是分开进行的，配置到设备和接口的映射不再以接口名为基础进行管理。设备配置位于 `/etc/sysconfig/hardware/hwcfg-*` 中。接口配置位于 `/etc/sysconfig/network/ifcfg-*` 中。指派配置名的方式使这些名称可以描述所关联的设备和接口。因为以前从驱动程序到接口名的映射需要静态接口名，所以 `/etc/modprobe.conf` 中不再进行此映射。在新概念中，此文件中的别名项可能导致不希望出现的副作用。

配置名（hwcfg- 或 ifcfg- 后的任何内容）可以通过插槽、设备特定的 ID 或接口名对设备进行描述。例如，某个 PCI 卡的配置名可能是 bus-pci-0000:02:01.0（PCI 插槽）或 vpid-0x8086-0x1014-0x0549（厂商和产品 ID）。关联接口的名称可能是 bus-pci-0000:02:01.0 或 wlan-id-00:05:4e:42:31:7a（MAC 地址）。

若要将某个网络配置指派给某种类型的任何一个卡（一次只插入一个该类型的卡）而不是某个特定的卡，请选择不是非常特定的配置名。例如，可以将 bus-pcmcia 用于所有 PCMCIA 卡。另一方面，可以通过在前面加上接口类型对名称进行限制。例如，可以为连接在 USB 端口上的 WLAN 卡指派 wlan-bus-usb。

系统始终使用对接口或提供接口的设备描述最清楚的配置。搜索最合适的配置是由 getcfg 处理的。getcfg 的输出提供可用于描述设备的所有信息。getcfg 的手册页中介绍了有关指定配置名的详细信息。

使用上面介绍的方法，即使不总是以相同的顺序初始化网络设备，也可以用正确的配置对网络接口进行配置。但是，接口的名称仍取决于初始化顺序。有两种方法可以确保对特定网卡的接口进行可靠的访问：

- `getcfg-interfaceconfiguration name` 返回关联的网络接口的名称。因此，在某些配置文件中，可以输入配置名（例如，防火墙、dhcpd、路由、多种虚拟网络接口（隧道））而不是非持久的接口名。
- 自动向每个接口指定永久接口名。可以根据需要调整它们。创建接口名时，请按 `/etc/udev/rules.d/30-net_persistent_names.rules` 中所述继续。但是，持久性名称 `pname` 不应该与内核可能自动指派的名​​称相同。因此，不允许使用 `eth*`、`tr*`、`wlan*`、`qeth*`、`iucv*` 等名称。请改用 `net*` 或者像 `external`、`internal` 或 `dmz` 等描述性名称。确保同一个接口名仅使用一次。接口名中的字符的范围是 `[a-zA-Z0-9]`。只能紧接在接口注册之后为接口指派持久性名称，这意味着必须重装载网卡的驱动程序或者必须执行 `hwupdevice description`。命令 `rcnetworkrestart` 不足以实现此目的。

---

### 重要：使用持久性接口名

持久性接口名的使用尚未在所有领域中进行测试。因此，某些应用程序不能顺畅地处理所选的接口名。

---

ifup 需要现有的接口，因为它不初始化硬件。硬件的初始化是由命令 hwup 处理的（由 hotplug 或 coldplug 执行）。当初始化设备时，将通过 hotplug 为新接口自动执行 ifup，如果启动方式是 onboot、hotplug 或 auto 并且启动了 network 服务，则将设置接口。以前，命令 ifup *interfacename* 触发硬件初始化。目前的过程与以前的过程相反。首先初始化硬件部件，随后执行所有其他操作。这样，使用现有的这组配置，总能以可能的最佳方式配置数目不固定的设备。

**表 30.5 “手动网络配置脚本”** [530]总结了网络配置中所涉及的最重要的脚本。只要有可能，硬件和接口将对脚本进行区分。

**表 30.5** 手动网络配置脚本

配置阶段	命令	功能
硬件	hw{up,down,status}	热插拔子系统执行此 hw* 脚本来初始化设备、撤消初始化或查询设备的状态。hwup 的手册页中提供了详细信息。
接口	getcfg	getcfg 可用于查询与配置名或硬件描述关联的接口名。getcfg 的手册页中提供了详细信息。
接口	if{up,down,status}	if* 脚本启动现有的网络接口或返回指定接口的状态。ifup 的手册页中提供了详细信息。

有关热插拔和持久性设备名的详细信息在**第 24 章 使用 udev 进行动态内核设备管理** [421]中有所介绍。

### 30.7.1 配置文件

本节对网络配置文件进行了概述并解释了它们的作用和所使用的格式。



## /etc/syconfig/hardware/hwcfg-\*

这些文件包含网卡和其他设备的硬件配置。它们包含所需的参数，例如内核模块、启动方式和脚本关联。有关详细信息，请参见 hwup 的手册页。不管现有硬件如何，都会在启动冷插拔时应用 hwcfg-static-\* 配置。

## /etc/sysconfig/network/ifcfg-\*

这些文件包含网络接口的配置。它们包含启动方式和 IP 地址等信息。可能的参数在 ifup 的手册页中有所介绍。另外，如果应将常规设置只用于一个接口，则文件 dhcp、wireless 和 config 中的所有变量都可用于 ifcfg-\* 文件。

► **zseries:** 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。 ◀

## /etc/sysconfig/network/{config,dhcp,wireless}

文件 config 包含 ifup、ifdown 和 ifstatus 行为的常规设置。dhcp 包含用于无线 LAN 卡的 DHCP 和 wireless 设置。对所有这三个配置文件中的变量都进行了注释，它们还可用于 ifcfg-\* 文件中，该文件将以较高的优先级处理这三个配置文件。

## /etc/sysconfig/network/{routes,ifroute-\*}

在这里确定 TCP/IP 包的静态路由。在 /etc/sysconfig/network/routes 文件中输入各种系统任务所需的所有静态路由：主机的路由、主机通过网关的路由以及网络的路由。对于需要个别路由的每个接口，定义另一个配置文件：/etc/sysconfig/network/ifroute-\*。用接口名称替换 \*。路由选择配置文件中的项如下所示：

# Destination	Dummy/Gateway	Netmask	Device
#			
127.0.0.0	0.0.0.0	255.255.255.0	lo
204.127.235.0	0.0.0.0	255.255.255.0	eth0
default	204.127.235.41	0.0.0.0	eth0
207.68.156.51	207.68.145.45	255.255.255.255	eth1
192.168.0.0	207.68.156.51	255.255.0.0	eth1

路由目标位于首列。此列可以包含网络或主机的 IP 地址，或者在有可访问名称服务器时，包含完全限定的网络或主机名。

第二列包含默认网关或通过其可访问主机或网络的网关。第三列包含网关后的网络或主机的子网掩码。例如，网关后主机的掩码为 255.255.255.255。

第四列只与本地主机连接的网络有关，如回路、以太网、ISDN、PPP 和虚拟设备。必须在此输入设备名。

（可选）可以使用第五列来指定路由的类型。不需要的列中应该包含一个减号 -，这样才能确保分析程序正确解析命令。关于详细信息，请参见 `routes(5)` 手册页。

## **/etc/resolv.conf**

在此文件中指定主机所属的域（关键字 `search`）。同时列出的还有要访问的名称服务器地址的状态（关键字 `nameserver`）。可以指定多个域名。当解析不是完全限定的名称时，将尝试通过附加单独的 `search` 项生成一个完全限定的名称。通过输入多行可以输入多个名称服务器，每行都以 `nameserver` 开头。注释以 `#` 符号开头。YaST 在此文件中输入指定的名称服务器。**例 30.5** `“/etc/resolv.conf”` [532] 显示 `/etc/resolv.conf` 的内容。

### **例 30.5** `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

某些服务（例如 `pppd(wvdial)`、`ipppd(isdn)`、`dhcp(dhcpd)` 和 `dhclient`）、`pcmcia` 和 `hotplug` 通过脚本 `modify_resolvconf` 修改文件 `/etc/resolv.conf`。如果文件 `/etc/resolv.conf` 已被此脚本临时修改，则它将包含预定义的注释，给出有关修改它的服务的信息、备份原始文件的位置以及如何关闭自动修改机制。如果 `/etc/resolv.conf` 被多次修改，则该文件以嵌套的形式包括修改。即使还原的顺序不同于进行修改的顺序，也可以以一种彻底的方式进行还原。可能需要这种灵活性的服务包括 `isdn`、`pcmcia` 和 `hotplug`。

如果未以正常、彻底的方式终止服务，则可以使用 `modify_resolvconf` 恢复原始文件。另外，在系统引导时，将检查是否有由未彻底终止产生的、经修改

的 `resolv.conf`（例如，系统崩溃后），如果有，则将恢复原始（未经修改的）`resolv.conf`。

YaST 使用命令 `modify_resolvconfcheck` 检查 `resolv.conf` 是否已被修改并将随后警告用户这些更改将在恢复文件后丢失。除此之外，YaST 将不使用 `modify_resolvconf`，这意味着通过 YaST 更改 `resolv.conf` 的效果与任何手动更改的效果相同。在两种情况下，更改都具有永久效果。上述服务请求的修改只是临时的。

## **/etc/hosts**

在此文件中，如 [例 30.6 “/etc/hosts” \[533\]](#) 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 30.6** */etc/hosts*

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.1 earth.example.com earth
```

## **/etc/networks**

在这里，网络名称被转换为网络地址。格式类似于 `hosts` 文件的格式，只是网络名称在地址的前面。请参见 [例 30.7 “/etc/networks” \[533\]](#)。

### **例 30.7** */etc/networks*

```
loopback      127.0.0.0
localnet      192.168.0.0
```

## **/etc/host.conf**

此文件控制名称解析，即通过解析程序库转换主机名和网络名称。此文件只用于链接到 `libc4` 或 `libc5` 的程序。对于当前的 `glibc` 程序，请参见 `/etc/nsswitch`

.conf 中的设置。参数必须始终单独在一行上。注释以 # 符号开头。表 30.6 “/etc/host.conf 的参数” [534] 显示了可用的参数。例 30.8 “/etc/host.conf” [534]中显示了 /etc/host.conf 的示例。

**表 30.6** /etc/host.conf 的参数

order <i>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
multi <i>on/off</i>	定义 /etc/hosts 中输入的主机是否可以具有多个 IP 地址。
nospoof <i>on</i> spoofalert <i>on/off</i>	这些参数影响名称服务器 <i>spoofing</i> ，但除此之外，它们对网络配置没有任何影响。
trim <i>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）。此选项仅当来自本地域的名称在 /etc/hosts 文件中时才可用，但仍要用附加的域名进行组织。

**例 30.8** /etc/host.conf

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

## /etc/nsswitch.conf

GNU C Library 2.0 的引入与 名称服务转换 (NNS) 的引入是同时进行的。有关详细信息，请参见 nsswitch.conf (5) 手册页和 *GNU C Library 参手册*。

查询的顺序是在文件 `/etc/nsswitch.conf` 中定义的。中显示了 `nsswitch.conf` 的示例。**例 30.9 “`/etc/nsswitch.conf`” [535]** 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 33 章 域名系统** [555]）将请求发送到 `/etc/hosts (files)`。

**例 30.9** *`/etc/nsswitch.conf`*

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files

netgroup:    files
automount:   files nis
```

**表 30.7 “通过 `/etc/nsswitch.conf` 可用的数据库” [535]**中列出了 NSS 上可用的“数据库”。另外，近期将推出 `automount`、`bootparams`、`netmasks` 和 `publickey`。**表 30.8 “NSS“数据库”的配置选项” [536]**中列出了 NSS 数据库的配置选项。

**表 30.7** 通过 `/etc/nsswitch.conf` 可用的数据库

<code>aliases</code>	<code>sendmail</code> 实施的邮件别名；请参见 <code>man5 aliases</code> 。
<code>ethers</code>	以太网地址。
<code>group</code>	<code>getgrent</code> 使用的用户组。另请参见 <code>group</code> 的手册页。
<code>hosts</code>	<code>gethostbyname</code> 和类似函数使用的主机名和 IP 地址。
<code>netgroup</code>	网络中用于控制访问权限的主机和用户列表，请参见 <code>netgroup(5)</code> 手册页。

networks	getnetent使用的网络名称和地址。
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 30.8** 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
nis、nisplus	NIS，另请参见 <a href="#">第 35 章 使用 NIS</a> [591]
dns	仅可用作 hosts 和 networks 的扩展名
compat	仅可用作 passwd、shadow 和 group 的扩展名

## /etc/nscd.conf

此文件用于配置 nscd（名称服务缓存守护程序）。请参见 nscd(8) 和 nscd.conf(5) 手册页。默认情况下，passwd 和 groups 的系统项由 nscd 进行缓存。这对于目录服务（例如 NIS 和 LDAP）的性能很重要，因为如果不是这样，每次访问名称或组都需要网络连接。默认情况下，不对 hosts 进行缓存，因为 nscd 中缓存主机的机制将导致本地系统无法信任正向和反向查找检查。请设置缓存 DNS 服务器，而不是让 nscd 缓存名称。

如果激活 `passwd` 的缓存，则通常需要 15 秒才能识别新添加的本地用户。通过使用命令 `rcnscdrestart` 重启动 `nscd` 可缩短此等待时间。

## **/etc/HOSTNAME**

此文件提供不附带域名的主机名。当引导计算机时，此文件将被多个脚本读取。它可能只包含一行，该行中设置了主机名。

## **30.7.2 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描述更改。如果未在正确的配置文件中输入配置，重引导时将丢失已更改的网络配置。

## **使用 ip 配置网络接口**

`ip` 是用来显示和配置路由选择、网络设备、策略路由选择以及隧道的工具。它被设计为替换较早的工具 `ifconfig` 和 `route`。

`ip` 是非常复杂的工具。它的常用语法为 `ip options object command`。可使用以下对象：

`link`

此对象表示网络设备。

`address`

此对象表示设备的 IP 地址。

`neighbour`

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 addr add 192.168.12.154/30 brd + dev eth0`。

要拥有活动连接，还必须配置默认网关。要设置系统的网关，请输入 `ip route get gateway_ip_address`。要将一个 IP 地址转换为另一个 IP 地址，请使用 `nat:ip route add nat_ip_address via other_ip_address`。

要显示所有设备，可使用 `ip link ls`。要只显示正在运行的接口，可使用 `ip link ls up`。要打印设备的接口统计信息，可输入 `ip -s link ls device_name`。要查看设备的地址，请输入 `ip addr`。在 `ip addr` 的输出中，还可找到有关设备 MAC 地址的信息。要显示所有路由，可使用 `ip route show`。

有关使用 `ip` 的更多信息，请输入 `iphelp` 或查看 `ip(8)` 手册页。`help` 选项还可用于所有 `ip` 对象。例如，如果希望阅读 `ipaddr` 的帮助，请输入 `ipaddr help`。可在 `/usr/share/doc/packages/iproute2/ip-cref.pdf` 中找到 `ip` 手册。



## 使用 ping 测试连接

ping 命令是用于测试 TCP/IP 连接是否有效的标准工具。它使用 ICMP 协议来将小数据包和 ECHO\_REQUEST 数据报文发送到目标主机，并请求即时答复。如果发送有效，ping 将据此显示一条消息，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：它还能提供关于连接质量的基本信息。在例 30.10 “命令 ping 的输出” [539] 中，可查看 ping 输出示例。倒数第二行包含有关已发送的包数、丢失的包和 ping 运行的总时间量的信息。

您可以使用主机名或 IP 地址（例如 pingexample.com 或 ping130.57.5.75）作为目标。程序会一直发送包，直到您按 Ctrl + C。

如果只需要检查连接功能，则可使用 -c 选项来限制包数。例如，要将 ping 限制为三个包，请输入 ping-c 3 192.168.0。

### 例 30.10 命令 ping 的输出

```
ping -c 3 example.com
PING example.com (130.57.5.75) 56(84) bytes of data.
64 bytes from example.com (130.57.5.75): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (130.57.5.75): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (130.57.5.75): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

两个包之间的默认时间间隔为一秒。ping 提供了选项 -i 来更改时间间隔。例如，要将 ping 时间间隔延长为十秒，则输入 ping-i 10 192.168.0。

在带有多个网络设备的系统中，有时通过特定接口地址发送 ping 将会非常有用。要执行此操作，可将 -I 选项结合选定设备名称一起使用，例如 ping-I wlan1 192.168.0。

有关使用 ping 的更多选项和信息，请输入 ping-h 或查看 ping (8) 手册页。

## 使用 ifconfig 配置网络

ifconfig 是传统的网络配置工具。与 ip 相比，您只能将 ifconfig 用于接口配置。如果希望配置路由选择，可使用 route。

---

## 注意: ifconfig 和 ip

程序 ifconfig 已过时。请使用 ip。

---

毫无疑问, ifconfig 可显示当前活动接口的状态。在例 30.11 “命令 ifconfig 的输出”[540]中可见 ifconfig 具有非常整齐和详细的输出。输出的第一行中还包含关于设备 MAC 地址的信息和 HWaddr 的值。

### 例 30.11 命令 ifconfig 的输出

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255 Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 Mb)
```

有关使用 ifconfig 的更多选项和信息, 请输入 ifconfig-h 或参见 ifconfig (8) 手册页。

## 使用 route 配置路由选择

route 是用于操作 IP 路由选择表的程序。可使用它来查看路由选择配置和添加或删除路由。

注意：route 和 ip

程序 route 已过时。请使用 ip。

如果需要有关路由选择配置的快速而又易懂的信息来确定路由选择问题，则route 将非常有用。要查看当前路由配置，请输入 route-n 作为 root。

例 30.12 命令 -n 的输出

```
route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags   MSS Window  irtt Iface
10.20.0.0        *                255.255.248.0    U        0 0        0 eth0
link-local       *                255.255.0.0      U        0 0        0 eth0
loopback         *                255.0.0.0        U        0 0        0 lo
default          styx.exam.com    0.0.0.0          UG       0 0        0 eth0
```

有关使用 route 的更多选项和信息，请输入 route-h 或参见 route (8) 手册页。

### 30.7.3 启动脚本

除了上面介绍的配置文件之外，还有多个脚本在引导计算机时装载网络程序。只要系统切换到某个多用户运行级别，就将启动这些脚本。中介绍了其中的一些脚本。表 30.9 “网络程序的一些启动脚本” [541]

表 30.9 网络程序的一些启动脚本

/etc/init.d/network	此脚本处理网络接口的配置。硬件必须已被 /etc/init.d/coldplug (通过 hotplug) 初始化。如果未启动 network 服务，当通过热插拔插入网络接口时，不实施任何网络接口。
/etc/init.d/inetd	启动 xinetd。xinetd 可用于在系统上提供服务器服务。例如，它可以在初始化 FTP 连接时启动 vsftpd。

<code>/etc/init.d/portmap</code>	启动RPC服务器所需的端口映射器，例如NFS服务器。
<code>/etc/init.d/nfsserver</code>	启动NFS服务器。
<code>/etc/init.d/postfix</code>	控制postfix进程。
<code>/etc/init.d/ypserv</code>	启动NIS服务器。
<code>/etc/init.d/ypbind</code>	启动NIS客户机。

---

## 30.8 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 KDE 小程序或命令行界面来控制拨号连接。如果因特网网关不是您所用的主机，最好通过网络主机来控制拨号连接。

这时就需要 `smpppd` 了。该程序为辅助程序提供统一的界面，并且可以双向执行。首先，它要对所需的 `pppd` 或 `ippd` 编程，并控制其拨号属性。然后，向用户程序提供各种提供商，并传送有关当前连接状态的信息。由于还可以通过网络来控制 `smpppd`，该程序适用于从专用子网中的工作站控制与因特网的拨号连接。

### 30.8.1 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`，必须将此选项设置为 `yes`。`smpppd` 的监听端口为 3185。如果此参数设置为 `yes`，则还需相应设置 `bind-address`、`host-range` 和 `password` 等参数。

`bind-address = ip address`

如果主机有多个 IP 地址，使用此参数可以确定 `smpppd` 应在哪个 IP 地址上接受连接。默认值是监听所有地址。

`host-range = min ip max ip`

参数 `host-range` 用于定义网络范围。IP 地址属于这一范围的主机将被授予访问 `smpppd` 的权限。此范围之外的所有主机均不具备访问权。

`password = password`

通过指派密码可使客户机仅限于授权主机。由于这是个纯文本密码，不应高估该密码提供的安全性。如果未指派任何密码，所有客户机都有权访问 `smpppd`。

`slp-register = yes/no`

使用此参数，可以通过 SLP 在网络中声明 `smpppd` 服务。

关于 `smpppd` 的详细信息，请参见 `smpppd(8)` 和 `smpppd.conf(5)` 手册页。

## 30.8.2 配置供远程使用的 KInternet、cinternet 和 qinternet

KInternet、cinternet 和 qinternet 可用于控制本地或远程 `smpppd`。cinternet 是图形 KInternet 的命令行版本。qinternet 与 KInternet 基本相同，但不使用 KDE 库，所以可以在没有 KDE 库的情况下使用，并且必须单独安装。要使这些实用程序可用于远程 `smpppd`，请手动编辑配置文件 `/etc/smpppd-c.conf` 或使用 KInternet。此文件仅使用三个选项：

`sites = list of sites`

此选项可以向前端通知 `smpppd` 的搜索位置。前端将按照在此指定的选项顺序来测试这些选项。`local` 选项规定建立到本地 `smpppd` 的连接。`gateway` 指向网关上的 `smpppd`。将按照 `config-file` 的 `server` 中的指定建立连接。`slp` 指示前端连接通过 SLP 发现的 `smpppd`。

`server = server`

在此指定 `smpppd` 运行所在的主机。

`password = password`

插入为 `smpppd` 选择的密码。

如果 `smpppd` 处于活动状态，现在即可访问它，例如通过 `cinternet--verbose --interface-list` 来访问。如果此时遇到困难，请参见 `smpppd-c.conf(5)` 和 `cinternet(8)` 手册页。

## 网络中的 SLP 服务

制定 *服务位置协议* (SLP) 是为了简化本地网络中联网客户机的配置。要配置网络客户机（包括所有必需服务），管理员通常需要对网络中提供的服务器有详细了解。SLP 可以向本地网络中的所有客户机声明选中服务是否可用。支持 SLP 的应用程序则可以利用这一发布信息并进行自动配置。

SUSE Linux Enterprise® 支持使用 SLP 提供的安装源进行安装，并且包含许多集成了 SLP 支持的系统服务。YaST 和 Konqueror 都有适用于 SLP 的前端。您可以使用 SLP 为联网客户机（如系统上的安装服务器、文件服务器或打印服务器）提供核心功能。

---

### 重要：SUSE Linux Enterprise 中的 SLP 支持

提供 SLP 支持的服务包括 cupsd、rsyncd、ypserv、openldap2、openwbem (CIM)、ksysguardd、saned、kdm vnc login、smpppd、rpasswd、postfix 和 sshd（通过 fish）。

---

## 31.1 激活 SLP

要用 SLP 提供服务，您的系统上必须运行 slpd。如果只需发出服务查询，则不必启动此守护程序。类似 SUSE Linux Enterprise 中的大多数系统服务，slpd 守护程序通过单独的初始化脚本来控制。默认情况下该守护程序处于非活动状态。要在会话期间激活该守护程序，请以 root 身份运行 rcslpdstart 来启动它，运行 rcslpdstop 来停止它。使用 restart 或 status 可分别执行重启或状态检查。如果默认激活 slpd，请在 YaST 系统 > 系统服务（运行级别）中启用

slpd，或以 root 身份运行一次 `insserv slpd` 命令。这样即可在引导系统时将 slpd 自动加入要启动的一组服务。

## 31.2 SUSE Linux Enterprise 中的 SLP 前端

要查找您网络中 SLP 提供的服务，请使用 SLP 前端。SUSE Linux Enterprise 包含几个前端：

### slptool

slptool 是一个简单的命令程序，可用于在网络中声明 SLP 查询或声明专有服务。slptool--help 列出了所有可用选项和功能。也可以从处理 SLP 信息的脚本调用 slptool。

### YaST SLP 浏览器

YaST 包含一个单独的 SLP 浏览器，可以在树图中列出本地网络中通过 SLP 声明的所有服务。用 *网络服务 > SLP 浏览器* 查找它。

### Konqueror

用作网络浏览器时，Konqueror 可以在 `slp:/` 中显示本地网络中的所有可用的 SLP 服务。单击主窗口中的图标可获得有关相关服务的详细信息。如果在 Konqueror 中使用 `service:/`，在浏览器窗口中单击相关图标可与选定服务建立连接。

## 31.3 通过 SLP 安装

如果在网络内提供了带 SUSE Linux Enterprise 安装媒体的安装服务器，则可以通过 SLP 注册。有关详细信息，请参见 [第 4.2.1 节“使用 YaST 设置安装服务器”](#) [51]。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。



## 31.4 用 SLP 提供服务

SUSE Linux Enterprise 中的许多应用程序都已使用 `libslp` 库集成了 SLP 支持。如果服务未集成 SLP 支持，请使用以下方法之一使其可通过 SLP 声明。

通过 `/etc/slp.reg.d` 进行的静态注册

为每个新服务创建单独的注册文件。下面显示了注册扫描仪服务的文件的示例：

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

此文件中最重要的一行是以 *service:* 开头的服务 URL。其中包含服务类型 (`scanner.sane`) 以及该服务在服务器上的地址。`$HOSTNAME` 自动用完整主机名替换。随后是可以找到相关服务的 TCP 端口的名称，端口与主机名之间用冒号分隔。然后输入服务的显示语言及以秒计的注册持续时间。应该用逗号分隔服务 URL 之后的各项内容。将注册持续时间设置为 0 到 65535 之间的值。0 表示禁止注册。65535 表示取消所有限制。

注册文件中还包含两个变量，`watch-tcp-port` 和 `description`。`watch-tcp-port` 链接 SLP 服务，声明相关服务是否是通过使 `slpd` 检查服务的状态来激活的。第二个变量为显示在适合的浏览器中的服务提供了更为准确的描述。

---

### 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

与 `/etc/slp.reg.d` 过程的唯一差别即在于：这种注册方式要将所有服务都集中到一个核心文件中。

使用 `slptool` 进行的动态注册

如果应该从专有脚本为某项服务注册 SLP 支持，请使用 `slptool` 命令行前端。

## 31.5 有关详细信息

以下来源提供了有关 SLP 的详细信息：

RFC 2608、2609、2610

RFC 2608 主要描述了 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`

此目录包含有关 SLP 的所有现有文档，其中包括 `README.SuSE`（包含 SUSE Linux Enterprise 详细信息、上述 RFC 和两个介绍性的 HTML 文档）。要使用 SLP 功能的编程人员应该安装 `openslp-devel` 包，以便参见随包附带的 *编程人员指南*。

## 使用 NTP 同步时间

NTP（网络时间协议）机制是用于同步网络上的系统时间的协议。首先，计算机从作为可靠时间源的服务器获得时间。然后将此计算机用作网络中其他计算机的时间源。这样做有双重目的：既可维护绝对时间，又可保持网络中所有计算机系统时间的同步。

维护确切的系统时间在许多情况下都非常重要。内置硬件(BIOS)时钟往往不能满足数据库这样的应用程序的要求。手动更正系统时间可能会导致许多严重问题，例如向后调整时间将使关键应用程序出现故障。在网络中，通常需要同步所有计算机上的系统时间，但是手动调整时间是一种不好的方法。`xntp` 提供了解决这些问题的机制。该机制随时借助网络中的可靠时间服务器调整系统时间。它还支持对本地参考时钟（如无线电控制的时钟）进行管理。

### 32.1 使用 YaST 配置 NTP 客户机

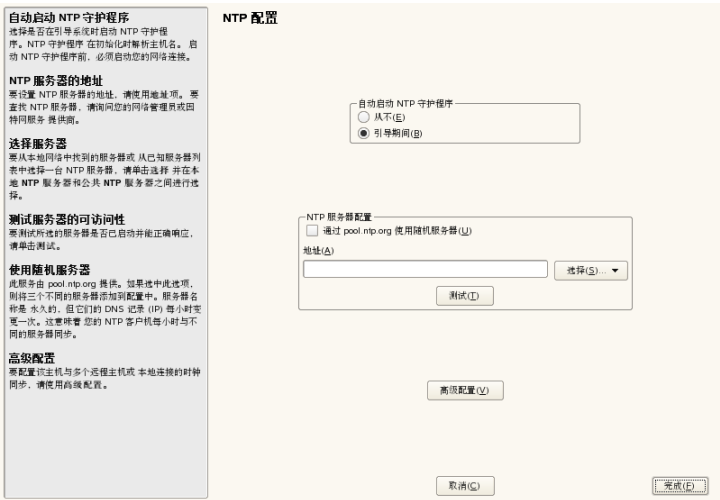
`xntp` 已预先设置为以本地计算机时钟为时间参考。但是，只有在没有更精确的时间源的情况下才使用(BIOS)时钟最为替代。YaST 为 NTP 客户机的配置提供方便。对于不运行防火墙的系统，请使用快速或高级配置。对于受到防火墙保护的系统，高级配置可能打开 `SuSEfirewall2` 中需要的端口。

#### 32.1.1 快速的 NTP 客户机配置

快速 NTP 客户机配置（*网络服务 > NTP 配置*）由两个对话框组成。在第一个对话框中设置 `xntpd` 的启动方式和要查询的服务器。要在引导系统时自动启动 `xntpd`，请单击 *引导期间*。然后指定 *NTP 服务器配置*。如果不能使用本地时间

服务器，则单击使用来自 *pool.ntp.org* 的随机服务器，或者单击选择访问要为网络选择合适的时间服务器的第二个对话框。

图 32.1 YaST：配置 NTP 客户机

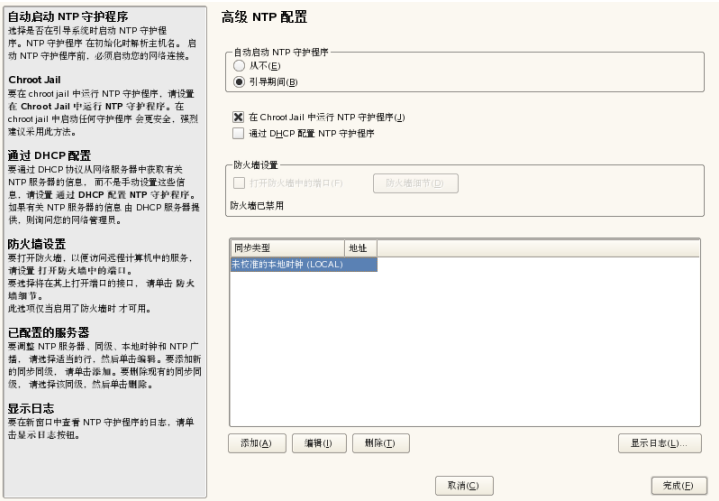


在详细的服务器选择对话框中，确定是使用本地网络中（本地 NTP 服务器）的时间服务器实施时间同步，还是使用考虑到所在时区的基于因特网的时间服务器（公共 NTP 服务器）实施时间同步。要使用本地时间服务器，请单击查找启动 SLP 查询，查找网络中的可用时间服务器。从搜索结果列表中选择最适合的时间服务器，然后单击确定退出该对话框。要使用公共时间服务器，请选择您所在的国家或地区（时区），并从公共 NTP 服务器列表中选择适合的服务器，然后单击确定退出该对话框。在主对话框中，可单击测试测试选定服务器的可用性，单击完成退出该对话框。

### 32.1.2 高级 NTP 客户机配置

选择快速配置中所述的启动方式之后，可以通过选择 NTP 客户机模块的主对话框中的高级配置对 NTP 客户机进行复杂配置（如图 32.1 “YaST：配置 NTP 客户机” [550] 所示）。

图 32.2 YaST: 复杂的 NTP 配置



在高级 *NTP* 配置中，确定是否应在 *chroot jail* 中启动 *xntpd*。默认情况下，在 *Chroot Jail* 中运行 *NTP* 守护程序是被激活的。在 *chroot jail* 中启动可以在遭受通过 *xntpd* 发起的攻击时提高安全性，因为这种方式可以防止攻击者危害整个系统。选择通过 *DHCP* 配置 *NTP* 守护程序，可以设置 *NTP* 客户机通过 *DHCP* 获取网络中可用的 *NTP* 服务器列表。

如果 *SuSEfirewall* 为默认的活动状态，则请启用打开防火墙中的端口。如果保持端口的关闭状态，则不可能建立与事件服务器的连接。

供客户机查询的服务器和其他时间资源列在下半部分。使用添加、编辑和删除可按需修改此列表。显示日志使您能够查看客户机的日志文件。

单击添加可添加新的时间信息源。在随后的对话框中，选择要与其进行时间同步的源类型。下列选项可用：

服务器

可供您选择 *NTP* 服务器的另一个对话框（如第 32.1.1 节“快速的 *NTP* 客户机配置”[549]所述）。激活用于初始同步，可以在引导系统时触发服务器和客户机之间的时间信息同步。选项使您可以指定 *xntpd* 的其他选项。有关详细信息，请参见 */usr/share/doc/packages/xntp-doc*（*xntp-doc* 包的一部分）。

### 同级

同级是一台要与其建立对称关系的计算机：它将同时用作时间服务器和客户机。要在同一网络中用同级代替某个服务器，请输入系统的地址。该对话框的其他部分与服务器对话框相同。

### 无线电时钟

要在系统中使用无线电时钟来同步时间，请在此对话框中输入时钟类型、单元号码、设备名和其他选项。单击驱动程序校准可对该驱动程序进行微调。

有关本地无线电时钟如何操作的详细信息，请参见 `/usr/share/doc/packages/xntp-doc/refclock.html`。

### 发出的广播

也可以通过在网络内广播的方式来传送时间信息和查询。在此对话框中，输入应将这类广播信息发送到的地址。除非使用了像无线电控制的时钟这样的可靠时间源，否则不要激活广播。

### 进来的广播

如果希望客户机通过广播接收信息，请在此字段中输入应接受来自哪个地址的相应数据包。

## 32.2 在网络中配置 xntp

要使用网络中的时间服务器，最简便的方式就是设置服务器参数。例如，如果可以从网络访问名为 `ntp.example.com` 的时间服务器，请通过添加以下行将其名称添加到文件 `/etc/ntp.conf` 中：

```
server ntp.example.com
```

要添加更多时间服务器，请使用关键字 `server` 插入更多行。使用命令 `rcntpd start` 初始化 `xntpd` 后，等待时间稳定并且创建用于更正本地计算机时钟的偏移文件需要大约一个小时的时间。利用偏移文件，只要计算机一启动，就可以计算出硬件时钟的系统误差。可以立即使用更正功能，使系统时间保持较高的稳定性。

有两种方法可将 NTP 机制用作客户机：第一种方法是客户机可以定期从已知服务器查询时间。在存在许多客户机的情况下，这种方法会给服务器带来很高的负荷。第二种方法是客户机可以等待网络中的广播时间服务器发送 NTP 广播。这种方法的缺点在于服务器的可靠性是未知的，而且如果服务器发出错误信息将导致严重问题。

如果通过广播获取时间，则不需要服务器名称。此时只需在配置文件 `/etc/ntp.conf` 中输入 `broadcastclient` 一行。要以独占方式使用一个或多个已知时间服务器，请在以 `servers` 开头的行中输入它们的名称。

## 32.3 设置本地参考时钟

软件包 `xntp` 包含用于连接本地参考时钟的驱动程序。 `xntp-doc` 包的文件 `/usr/share/doc/packages/xntp-doc/refclock.html` 中提供了受支持时钟的列表。每个驱动程序都有一个关联数字。在 `xntp` 中，实际配置是通过伪 IP 地址来完成的。时钟被输入 `/etc/ntp.conf` 文件，就像已经在网络中存在一样。为此专门给它们指派了 `127.127.t.u` 格式的特殊 IP 地址。其中 `t` 代表时钟的类型并确定要使用的驱动程序，`u` 代表设备并确定要使用的接口。

通常，各个驱动程序都有特殊的参数来描述配置详细信息。文件 `/usr/share/doc/packages/xntp-doc/drivers/driverNN.html`（其中 `NN` 是驱动程序的编号）提供了有关特定类型时钟的信息。例如，“8 型”时钟（通过串行接口的无线电时钟）需要额外的方式更精确地指定时钟。以 `Conrad DCF77` 接收模块为例，该模块需要使用 `mode 5`。要使用此时钟作为首选参考，应指定关键字 `prefer`。由此构成的 `Conrad DCF77` 接收模块的完整 `server` 行如下：

```
server 127.127.8.0 mode 5 prefer
```

其他时钟也采用相同的模式。安装 `xntp-doc` 包之后，可以在目录 `/usr/share/doc/packages/xntp-doc/` 中找到 `xntp` 的文档。文件 `/usr/share/doc/packages/xntp-doc/refclock.html` 提供指向描述驱动程序参数的驱动程序页的链接。





# 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 192.168.0.1 指派给 earth。在设置您自己的名称服务器前，请阅读第 30.3 节“名称解析”[508]中有关 DNS 的一般信息。以下配置示例都涉及到 BIND。

## 33.1 DNS 术语

### 区域

域名称空间由一些区域(zone)组成。例如，如果您有 example.org，则您的 org 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

转发器是一种 DNS 服务器，它能接收您 DNS 服务器无法回答的查询。

## 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。

## 33.2 用 YaST 配置

可以使用 YaST 的 DNS 模块来为您的本地网络配置 DNS 服务器。要配置 Samba 服务器，请启动 YaST 并选择 *网络服务 > DNS 服务器*。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，例如设置 ACL、日志记录、TSIG 密钥和其他选项。

### 33.2.1 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。

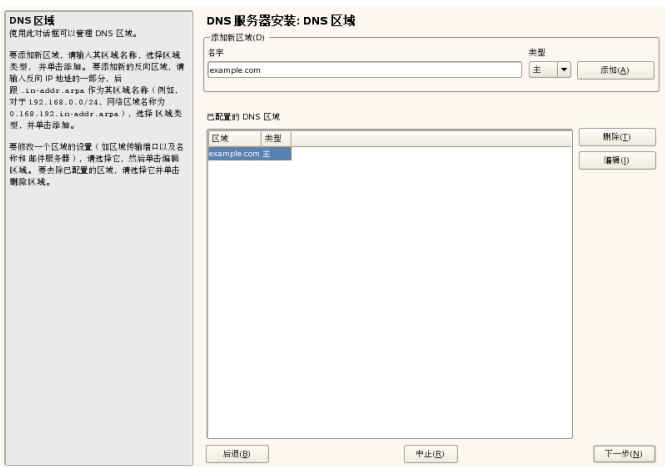
- 1 第一次启动模块时，您将看到图 33.1 “DNS 服务器安装：转发器设置” [557] 中显示的转发器设置对话框将打开。此对话框允许您决定是让 PPP 守护程序在通过 DSL 或 ISDN 进行拨号时提供转发器列表（PPP 守护程序设置转发器）还是提供您自己的列表（手动设置转发器）。

图 33.1 DNS 服务器安装：转发器设置



2 DNS 区域对话框由多个部分组成，负责管理区域文件（如第 33.5 节“区域文件” [570]中所述）。对于新区域，请在区域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，选择区域类型（主区域或从属区域）。参见图 33.2“DNS 服务器安装：DNS 区域” [557]。单击编辑区域来配置现有区域的其他设置。要删除区域，请单击删除区域。

图 33.2 DNS 服务器安装：DNS 区域



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。然后决定是否要启动 DNS 服务器（开或关）。您还可以激活 LDAP 支持。请参见图 33.3 “DNS 服务器安装：完成向导” [558]。

图 33.3 DNS 服务器安装：完成向导



### 33.2.2 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：

### 启动 DNS 服务器

在服务启动下，定义是要在引导系统时启动还是要手动启动 DNS 服务器。要立即启动 DNS 服务器，请选择 **立即启动 DNS 服务器**。要停止 DNS 服务器，请选择 **立即停止 DNS 服务器**。要保存当前设置，请选择 **立即保存设置并重新启动 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。

# DNS 服务器：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。

## 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，还可以指定最大文件大小（以兆字节为单位）和要储存的日志文件的版本数目。

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 33.4“DNS 服务器：日志记录” [559]。

图 33.4 DNS 服务器：日志记录

启动

转发器

基本选项

日志记录

ACL

TSIG 密钥

DNS 区域

DNS 服务器: 日志记录

日志类型

☐ 系统日志(S)

☒ 文件(F)

文件名(F)

浏览(B)...

最大大小 (MB)(S)

0

最大版本数(V)

0

附加日志记录

☐ 日志记录所有 DNS 查询(Q)

☐ 记录区域更新(U)

☐ 记录区域传送(T)

取消(C)

完成(F)

## 使用 ACL

使用此窗口定义 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）：

```
{ 10.10/16; }
```

配置文件的语法要求地址以分号结尾且放在花括号中。

## 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 33.7 节“安全事务”](#) [574]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）。按添加按钮确认您的选择。

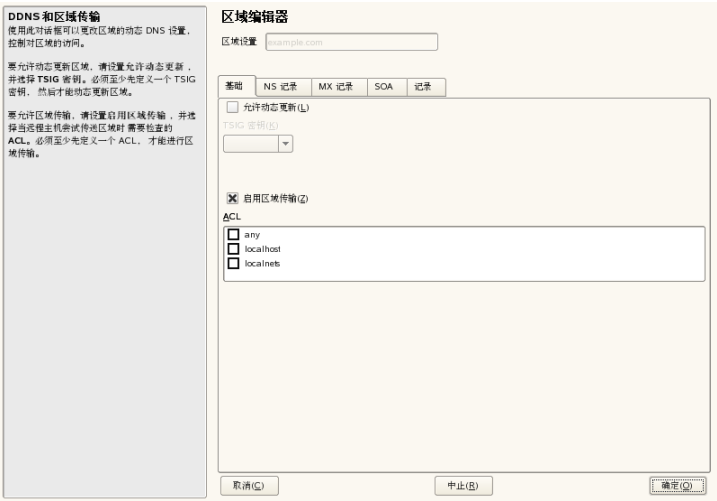
要使用以前创建的密钥，请将密钥 *ID* 字段保留为空，并在文件名下选择储存这个密钥 ID 的文件。选择后，请用添加按钮进行确认。

## 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并单击添加。

在主 *DNS 服务器 IP* 下的区域编辑器中，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，可从列表中选择一个 ACL。请参见[图 33.5“DNS 服务器：从属区域编辑器”](#) [561]。

图 33.5 DNS 服务器：从属区域编辑器



## 添加主区域

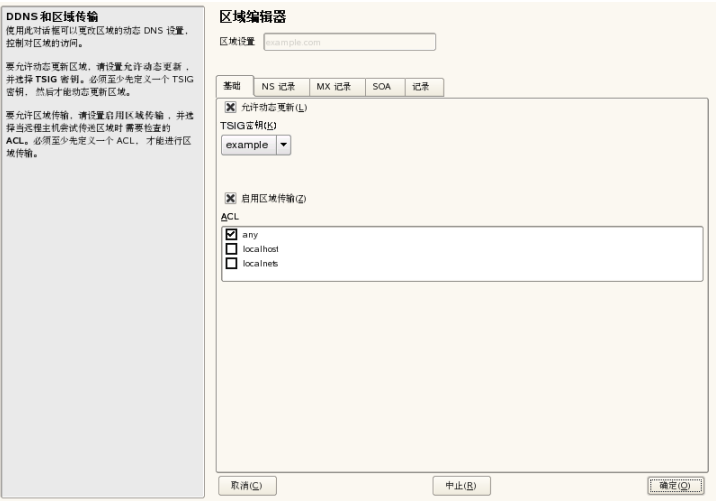
要添加主区域，请选择 *DNS 区域*，然后选择区域类型主，写入新区域名称并单击添加。

## 编辑主区域

要编辑主区域，请选择 *DNS 区域*，随后选择区域类型主，再从表中选择主区域，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 33.6“DNS 服务器：区域编辑器（基本）”[562]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机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。

图 33.6 DNS 服务器：区域编辑器（基本）



区域编辑器（NS 记录）

此对话框用于为指定的区域定义替代名称服务器。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 33.7 “DNS 服务器：区域编辑器（NS 记录）” [562]。

图 33.7 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 33.8 “DNS 服务器：区域编辑器（MX 记录）” [563]。

图 33.8 DNS 服务器：区域编辑器（MX 记录）

**MX 记录**

要添加新的邮件服务器，请输入地址和优先级，然后点击添加。要删除所列的邮件服务器之一，请选择该邮件服务器，然后点击删除。

**区域编辑器**

区域设置

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)
<input type="text"/>	<input type="text" value="0"/>

邮件中世列表

邮件服务器	优先级
-------	-----

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 33.6 “文件 /var/lib/named/world.zone” [570]。通过 LDAP 管理的动态区域不支持更改 SOA 记录。

图 33.9 DNS 服务器：区域编辑器 (SOA)

SOA 记录配置

设置 SOA 记录的选项。

序列号是用于确定区域是否已在主服务器上覆盖的数字 (目前从属服务器不必与主服务器同步)。

TTL 指定区域中所有没有显示 TTL 的记录的存在时间。

刷新指定区域在主服务器上刷新和从属服务器之间同步的频率。

重试指定在同步失败时，从属服务器尝试与主服务器同步的频率。

失效时间是指从属服务器上到期的时间，超过该时间后，从属服务器将停止应答该区域，直到同步为止。

最小值指定从属服务器应保存否定应答 (各种解析失败) 的时间。

区域编辑器

区域设置

基础NS 记录MX 记录SOA记录

序列(S)

TTL(L)

单元(U)

天

刷新(R)

单元(U)

小时

重试(R)

单元(U)

小时

失效时间(E)

单元(U)

周

最小值(M)

单元(U)

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。

33.3 启动名称服务器 BIND

在 SUSE Linux Enterprise® 系统中，已预配置名称服务器 BIND（*Berkeley* 因特网名称域，*Berkeley Internet Name Domain*），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 通过根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，它才能成为一个正常的 DNS。`/usr/share/doc/packages/bind/sample-config` 的文档中包含这种情况的简单示例。

---

## 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。为此，请将文件 `/etc/sysconfig/network/config` 中的变量 `MODIFY_NAMED_CONF_DYNAMICALY` 设置为 `yes`。

---

但是，在相关机构指派域之前，请不要设置任何正式域。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”，则描述已成功启动名为 `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 33.1 “named.conf 中的转发选项”** [565]中包含的地址仅用作示例。请根据您的设置调整这些项。

### 例 33.1 *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; 192.168.0.99; };
    allow-query { 127/8; 192.168.0/24; };
    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 `rndc restart` 停止并重启动名称服务器也会获得相同的效果。输入 `rndc stop` 可以随时停止服务器。

## 33.4 配置文件 `/etc/named.conf`

BIND 名称服务器本身的所有设置都被储存在文件 `/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 `/var/lib/named` 目录下单独的文件中。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 33.2 “基本的 `/etc/named.conf`” [566]显示了一个最小的 `/etc/named.conf`。

### 例 33.2 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";
};
```

## 33.4.1 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）。用 IP 地址（例如 `10.0.0.1`）替换 `ip-address`。

`forward first;`

在尝试通过根名称服务器解析 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根名称服务器。这可以用于防火墙配置。

`listen-on port 53 { 127.0.0.1; ip-address; };`

指示 BIND 通过哪些网络接口和哪个端口来接受客户机查询。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 客户机请求。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; };`

定义客户机可以自此发送 DNS 请求的网络。用地址信息（例如 `192.168.1/24`）替换 `net`。末尾的 `/24` 是网络掩码的缩写表示，本例中，网络掩码是 `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新启动时得到通知。

## 33.4.2 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，默认设置已足够了。**例 33.3 “禁用日志记录的项”** [568] 显示了此项最简单的形式，并完全禁止任何日志记录。

### 例 33.3 禁用日志记录的项

```
logging {  
    category default { null; };  
};
```

## 33.4.3 区域项

### 例 33.4 *my-domain.de* 的区域项

```
zone "my-domain.de" in {
    type master;
    file "my-domain.zone";
    notify no;
};
```

在 `zone` 后，指定要管理的域名 `my-domain.de`，后跟 `in` 和用花括号括起来的相关选项块，如 例 33.4 “*my-domain.de* 的区域项” [569] 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 33.5 “*other-domain.de* 的区域项” [569] 所示。

### 例 33.5 *other-domain.de* 的区域项

```
zone "other-domain.de" in {
    type slave;
    file "slave/other-domain.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）用于设置根名称服务器。此区域定义可以保留原样。

`file my-domain.zone` 或 `file "slave/other-domain.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，这将允许客户机创建 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。

## 33.5 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**

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。点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 world.zone，该区域文件负责域 world.cosmos，如例 33.6 “文件 /var/lib/named/world.zone” [570] 所示。

**例 33.6** 文件 /var/lib/named/world.zone

```
$TTL 2D
world.cosmos. IN SOA      gateway root.world.cosmos. (
                        2003072441 ; serial
                        1D          ; refresh
                        2H          ; retry
                        1W          ; expiry
                        2D )        ; minimum

                        IN NS      gateway
                        IN MX      10 sun

gateway IN A      192.168.0.1
        IN A      192.168.1.1
sun     IN A      192.168.0.2
moon    IN A      192.168.0.3
earth   IN A      192.168.1.2
mars    IN A      192.168.1.3
www     IN CNAME   moon
```



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 world.cosmos。这个域名以 . 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 gateway 扩展为 gateway.world.cosmos, 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@world.cosmos, 此项必须是 root.world.cosmos.. 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。这里为一周。

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。gateway 扩展为 gateway.world.cosmos, 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 world.cosmos 的电子邮件的邮件服务器。在本例中, 邮件服务器是主机 sun.world.cosmos。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 12–17 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 . 结尾, 因为它们不包含自己的域, 所以会将 world.cosmos 添加到所有名称。因为主机 gateway 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 AAAA 标记该记录。如果地址是 IPv6 地址, 则使用 AAAA 0 标记此项。IPv6 地址以前的标记只是 AAAA, 现在该标记已过时。

---

### 注意: IPv6 语法

IPv6 记录与 IPv4 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。即使要使用没有分段的地址, 也应该提供此信息。对于使用该语法的 IPv4 记录

```
pluto IN          AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN          AAAA 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

需要以 IPv6 格式添加有关缺失位的信息。由于上述示例是完整的 (未缺失任何位), 所以此记录的 IPv6 格式如下:

```
pluto IN          AAAA 0 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN          AAAA 0 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

请勿使用具有 IPv6 映射的 IPv4 地址。

---

第 18 行:

别名 `www` 可用于确定 `mond` (`CNAME` 是指规范名称) 的地址。

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 `192.168.1` 解析成 `1.168.192.in-addr.arpa`。参见 [例 33.7 “反向查找” \[573\]](#)。

**例 33.7 反向查找**

```
$TTL 2D
1.168.192.in-addr.arpa. IN SOA gateway.world.cosmos. root.world.cosmos. (
                                2003072441      ; serial
                                1D                ; refresh
                                2H                ; retry
                                1W                ; expiry
                                2D )              ; minimum

                                IN NS              gateway.world.cosmos.

1                               IN PTR            gateway.world.cosmos.
2                               IN PTR            earth.world.cosmos.
3                               IN PTR            mars.world.cosmos.
```

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 `192.168.1.0` 的反向查找。由于区域名为 `1.168.192.in-addr.arpa`, 因此不应将此区域添加到主机名中。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 `world.cosmos` 示例介绍的那些内容。

第 3–7 行:

请参见上一个关于 `world.cosmos` 的示例。

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 的不同版本间传送区域，不会产生任何问题。

## 33.6 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 33.7 节“安全事务”](#) [574] 中介绍的 TSIG 密钥执行此类更新。

## 33.7 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` 之间的安全通讯：

```
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 `192.168.2.3`）的密钥，服务器的 `/etc/named.conf` 必须包含下列规则：

```
server 192.168.2.3 {  
    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。

## 33.8 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-makekeyset` 将生成的所有密钥打包成一个密钥集，然后必须采用安全方式将这个密钥集传送给父区域。在父区域，用 `dnssec-signkey` 对此密钥集进行签名。然后，通过 `dnssec-signzone` 使用此命令生成的文件对区域进行签名，这又会为 `/etc/named.conf` 中的每个区域生成要包含的文件。

## 33.9 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 中 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上逐一本地配置。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机。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）来标识每个客户机，然后在客户机每次连接到服务器时为它提供相同的设置。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机动态指派地址。在后一种情况下，DHCP 服务器每次在收到客户机的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机数不超过地址数时，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会特别有用。

DHCP 服务器不仅提供 IP 地址和网络掩码，还提供客户机要使用的主机名、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，例如客户机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。

## 34.1 使用 YaST 配置 DHCP 服务器

---

### 重要：LDAP 支持

在这个版本的 SUSE Linux Enterprise 中，可以将 YaST DHCP 模块设置为在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 服务器进行管理。如果要使用 LDAP，请在配置 DHCP 服务器前设置 LDAP 环境。

---

YaST DHCP 模块允许您设置自己的用于本地网络的 DHCP 服务器。此模块可以以简单方式或专家方式运行。

### 34.1.1 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。

#### 卡选择

在第 1 步中，YaST 查找您的系统上可用的网络接口，然后将它们显示在列表中。从列表中选择侦听 DHCP 服务器所在的接口，然后单击添加。随后，请选择打开所选接口的防火墙打开此接口的防火墙。请参见图 34.1 “DHCP 服务器：卡选择” [579]。



图 34.1 DHCP 服务器：卡选择



全局设置

使用此复选框来确定是否由 LDAP 服务器自动保存您的 DHCP 设置。在输入字段中，提供 DHCP 服务器应管理的所有客户机的网络细节。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 客户机的混合网络）、网关地址和租用时间。请参见图 34.2 “DHCP 服务器：全局设置” [579]。

图 34.2 DHCP 服务器：全局设置



动态 DHCP

在此步骤中，我们将配置如何为客户机指派动态 IP 地址。为此，应首先指定服务器为 DHCP 客户机指派地址时使用的 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，在此期间客户机可以保留它的 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

定客户机保留某个 IP 地址的时间。请参见图 34.3 “DHCP 服务器：动态 DHCP” [580]。

图 34.3 DHCP 服务器：动态 DHCP



完成配置并设置启动方式  
在完成配置向导的第 3 部分后，会出现最后一个对话框，用于定义应如何启动 DHCP 服务器。在这里指定是在引导系统时自动启动还是在需要时手动启动 DHCP 服务器（例如进行测试）。单击完成以完成对服务器的配置。请参见图 34.4 “DHCP 服务器：启动” [580]。或者，您可以从左侧的树结构中选择主机管理以配置基本配置之外的特殊主机管理功能（请参见图 34.5 “DHCP 服务器：主机管理” [581]）。

图 34.4 DHCP 服务器：启动



主机管理

除了前面描述的方式使用动态 DHCP 之外，您也可以将服务器配置为以准静态方式指派地址。为此，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机。具体地说就是为客户机指派的名称和 IP 地址、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机列表。请参见图 34.5 “DHCP 服务器：主机管理” [581]。

图 34.5 DHCP 服务器：主机管理



34.1.2 专家配置

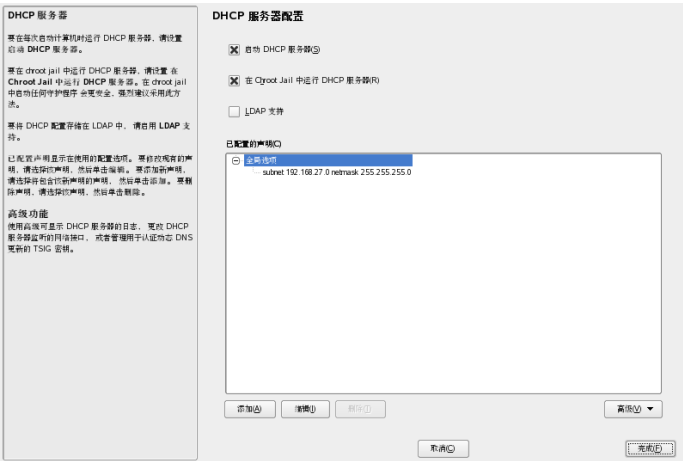
除了前面介绍的配置方法外，还有一种专家配置方式，用于精确调整 DHCP 服务器设置。在对话框左侧的树视图中选择专家设置，即可启动专家配置。

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（即 chroot jail）中运行，以便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 34.6 “DHCP 服务器：Chroot Jail 和声明” [582]。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 34.6 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 34.7 “DHCP 服务器：选择声明类型” [583]）。

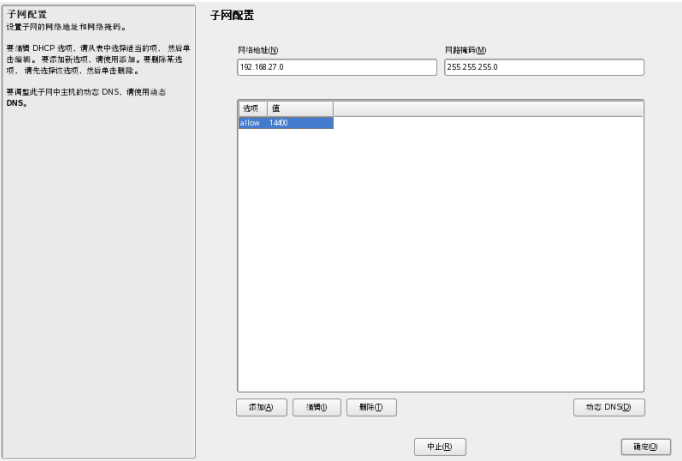
图 34.7 DHCP 服务器：选择声明类型



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。

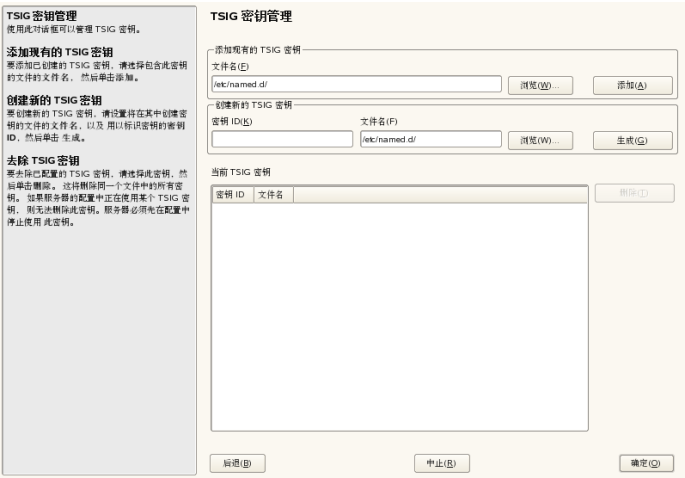
图 34.8 DHCP 服务器：配置子网



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 34.10 “DHCP 服务器：动态 DNS 的接口配置” [585]）。

图 34.9 DHCP 服务器：TSIG 配置



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。如果名称服务器与 DHCP 服务器在相同的主机上运行，则可以将这些字段留空。选择**确定**返回子网配置对话框（请参见图 34.8 “DHCP 服务器：配置子网” [583]）。再次选择**确定**将返回最初的专家配置对话框。

图 34.10 DHCP 服务器：动态 DNS 的接口配置

启用动态 DNS

要对此子网启用动态 DNS 更新，请设置 对此子网启用动态 DNS。

TSIG 密钥

要进行动态 DNS 更新，必须设置身份验证密钥。使用 TSIG 密钥可選擇用于身份验证的密钥。DHCP 服务器和 DNS 服务器的密钥必须相同。指定正向区域和反向区域的密钥。

全局 DHCP 服务器设置

必须更新 DHCP 服务器的全局设置才能使动态 DNS 正常工作。要自动进行更新，请设置更新全局动态 DNS 设置。

要更新的区域

指定要更新的正向区域和反向区域。还要为这两个区域指定主名称服务器。如果名称服务器与 DHCP 服务器在同一主机上运行，则可以省略这些字段。

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)

主 DNS 服务器(P)

反向区域(Y)

主 DNS 服务器(I)

后退(B)

中止(F)

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机都能与服务器通讯，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 34.11 “DHCP 服务器：网络接口和防火墙” [586]），之后您可以通过选择确定返回到原始对话框。

图 34.11 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。

## 34.2 DHCP 软件包

DHCP 服务器和 DHCP 客户机都可用于 SUSE Linux Enterprise。可用的 DHCP 服务器是 `dhcpd`（由因特网软件联盟发布）。在客户端，选择两个不同的 DHCP 客户机之一：`dhcp-client`（也来自 ISC）和 `dhcpcd` 包中的 DHCP 客户端守护程序。

SUSE Linux Enterprise 在默认情况下安装 `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 `dhcp-client`，它是通过配置文件 `/etc/dhclient.conf` 来控制的。

## 34.3 DHCP 服务器 `dhcpcd`

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 34.1 “配置文件 `/etc/dhcpd.conf`” [587]中的基本示例 `/etc/dhcpd.conf` 文件。

### 例 34.1 配置文件 `/etc/dhcpd.conf`

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;             # 2  hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.10 192.168.1.20;
    range 192.168.1.100 192.168.1.200;
}
```

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机的默认秒数 (`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 33 章 域名系统 [555]。
- 行 `option broadcast-address` 定义了请求客户机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` 用于指定为客户机指派的网络掩码。

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机指派 IP 地址。在例 34.1 “配置文件 `/etc/dhcpd.conf`” [587] 中，可以为客户机指派 192.168.1.10 和 192.168.1.20 之间以及 192.168.1.100 和 192.168.1.200 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，您应能够发现出现的问题。

在默认 SUSE Linux Enterprise 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。

## 34.3.1 具有固定 IP 地址的客户机

DHCP 用来向特定客户机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，服务器需要在客户机之间重新分发这些地址。

要确定配置有静态地址的客户机，`dhcpd` 将使用硬件地址，这是一个全局唯一的固定数字代码，其中包含 6 个八进制数对，用于标识所有网络设备（例如 `00:00:45:12:EE:F4`）。如果将相应的各行（如例 34.2 “配置文件的添加项” [589] 中的行）添加到例 34.1 “配置文件 `/etc/dhcpd.conf`” [587] 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机。

### 例 34.2 配置文件的添加项

```
host earth {  
hardware ethernet 00:00:45:12:EE:F4;  
fixed-address 192.168.1.21;  
}
```

在第 1 行输入相应客户机的名称 (*hosthostname*, 在这里是 *earth*), 在第 2 行输入 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 00:00:45:12:EE:F4
```

在上面的示例中, 具有 MAC 地址为 `00:00:45:12:EE:F4` 的网卡的客户机获得自动指派的 IP 地址 `192.168.1.21` 和主机名 `earth`。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 `ethernet`,

## 34.3.2 SUSE Linux Enterprise 版本

为了提高安全性, ISC 的 DHCP 服务器的 SUSE Linux Enterprise 版本附带有 Ari Edelkind 编写的非 `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`。

## 34.4 更多信息

有关 DHCP 的更多信息，请访问因特网软件联盟网站(<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 NIS

一旦网络内的多个 UNIX 系统都要访问公共资源，那么对于该网络内的所有计算机，所有用户和组身份是否相同就显得很重要了。网络对用户应该是透明的：无论他们用哪台计算机，他们总觉得是在同样的环境中。可以通过 NIS 和 NFS 服务完成此操作。NFS 通过网络分发文件系统。

NIS（网络信息服务）可以说是一种数据库式服务，用于跨网络访问 `/etc/passwd`、`/etc/shadow` 和 `/etc/group` 的内容。NIS 也可用于其他目的（如提供 `/etc/hosts` 或 `/etc/services` 之类文件的内容），但这里不作介绍。人们常把 NIS 称作 *YP*，也就是网络中的“电话黄页”。

### 35.1 配置 NIS 服务器

要想通过网络分发 NIS 信息，可以让一台服务器（主）管理所有客户机，或者让多台 NIS 从属服务器从该主服务器请求此信息，然后将它们转接到各自的客户机。

- 要只为网络配置一台 NIS 服务器，请参见第 35.1.1 节“配置 NIS 主服务器”[592]继续操作。
- 如果您的 NIS 主服务器应该将数据导出到其他子网中的从属服务器，则请按第 35.1.1 节“配置 NIS 主服务器”[592]中所述设置主服务器，并按第 35.1.2 节“配置 NIS 从属服务器”[596]中所述在子网中设置从属服务器。

# 35.1.1 配置 NIS 主服务器

要为网络配置 NIS 主服务器，请按如下所示继续：

- 1 启动 *YaST* > 网络服务 > *NIS* 服务器。
- 2 如果网络中只需要一个 NIS 服务器或者如果此服务器将充当更下级 NIS 从属服务器的主服务器，请选择安装和设置 *NIS* 主服务器。*YaST* 将安装需要的包。

## 提示

如果 NIS 服务器软件已安装在计算机上，请通过单击 *创建 NIS 主服务器* 来创建 NIS 主服务器。

图 35.1 NIS 服务器设置



- 3 确定基本 NIS 设置选项：
  - 3a 输入 NIS 域名。
  - 3b 通过选择 *该主机也是 NIS 客户机*，决定该主机是否还应该是 NIS 客户机，这样用户便可登录并从 NIS 服务器访问数据。

选择**更改密码**以允许网络中的用户（本地用户和通过 NIS 服务器管理的用户）更改其在 NIS 服务器上的密码（使用命令 `yppasswd`）。

这会相应激活**允许更改 GECOS 字段**和**允许更改登录壳层**选项。“GECOS”意味着用户还可以使用命令 `ypchfn` 更改其名称和地址设置。“SHELL”允许用户使用命令 `ypchsh` 来更改他们的默认 shell，例如从 `bash` 切换为 `sh`。新的 shell 必须是 `/etc/shells` 中预定义的条目。

- 3c 如果 NIS 服务器应该充当其他子网中 NIS 从属服务器的主服务器，请选择**存在活动的从属 NIS 服务器**。
- 3d 选择**打开防火墙中的端口**使 YaST 适应 NIS 服务器的防火墙设置。

图 35.2 主服务器设置



- 3e 单击**下一步**退出此对话框，或单击**其他全局设置**来进行其他设置。其他全局设置包括更改 NIS 服务器的源目录（默认为 `/etc`）。此外，也可以在此合并密码。应设置为是，以便使用文件（`/etc/passwd`、`/etc/shadow` 和 `/etc/group`）构建用户数据库。还要确定 NIS 应该提供的最小用户和组 ID。单击**确定**来确认设置并返回上一个屏幕。

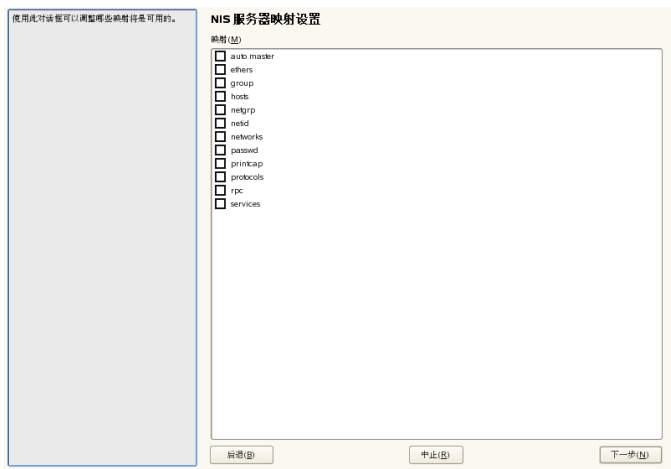
图 35.3 更改 NIS 服务器目录并同步文件



- 4 如果先前启用了存在活动的从属 NIS 服务器, 则输入用作从属服务器的主机的名称, 然后单击下一步。
- 5 如果未使用从属服务器, 就会跳过从属服务器配置, 直接转至数据库配置对话框。在此指定映射, 可以将部分数据库从 NIS 服务器传送至客户机。默认设置通常就足够了。选择下一步可退出此对话框。
- 6 选择可用映射, 然后单击下一步继续。



图 35.4 NIS 服务器映射设置



**7** 输入可以查询NIS服务器的主机。可通过单击相应的按钮来添加、编辑或删除主机。指定可以向NIS服务器发送来自哪个网络的请求。通常为内部网络。在当前情况下，应有以下两项：

255.0.0.0	127.0.0.0
0.0.0.0	0.0.0.0

第一项允许从您自己的主机（即NIS服务器）连接。第二项允许所有主机向服务器发送请求。

图 35.5 为 NIS 服务器设置请求权限



8 单击完成，保存更改并退出设置。

## 35.1.2 配置 NIS 从属服务器

要在网络中配置其他 NIS 从属服务器，请按如下所示继续：

- 1 启动 YaST > 网络服务 > NIS 服务器。
- 2 选择安装并设置 NIS 从属服务器，然后单击下一步。

### 提示

如果 NIS 服务器软件已安装在计算机上，则请通过单击创建 NIS 从属服务器来创建 NIS 从属服务器。

3 完成 NIS 从属服务器的基本设置：

- 3a 输入 NIS 域。
- 3b 输入主服务器的主机名或 IP 地址。

**3c** 如果要使用户能够登录到此服务器，请设置该主机也是 *NIS* 客户机。

**3d** 通过打开防火墙中的端口来调整防火墙设置。

**3e** 单击下一步。

- 4** 输入允许查询 *NIS* 服务器的主机。可通过单击相应的按钮来添加、编辑或删除主机。指定可以从哪些网络向 *NIS* 服务器发送请求。通常指的是所有主机。在当前情况下，应有以下两项：

```
255.0.0.0      127.0.0.0
0.0.0.0        0.0.0.0
```

第一项启用来自您自己的主机（即 *NIS* 服务器）的连接。第二项允许所有可访问同一网络的主机向服务器发送请求。

- 5** 单击完成，保存更改并退出设置。

## 35.2 配置 *NIS* 客户机

使用 YaST 模块 *NIS* 客户程序将工作站配置为使用 *NIS*。请选择主机是已有静态 IP 地址，或接受由 DHCP 发布的静态 IP 地址。DHCP 还提供 *NIS* 域和 *NIS* 服务器。有关 DHCP 的更多信息，请参见第 34 章 *DHCP* [577]。如果使用静态 IP 地址，请手动指定 *NIS* 域和 *NIS* 服务器。请参见图 35.6 “设置 *NIS* 服务器的域和地址” [598]。使用查找可让 YaST 在整个网络中搜索活动的 *NIS* 服务器。根据本地网络的大小，此进程可能会耗费一定的时间。广播可在指定的服务器没有响应后，在本地网络中寻找 *NIS* 服务器。

也可通过在 *NIS* 服务器地址中输入服务器地址（用空格分隔）来指定多个服务器。

根据本地安装，您可能还想激活 automounter。如果需要，此选项还会安装其他软件。

在专家设置中，如果不希望其他主机能查询您的客户机所用的服务器，请取消选中只应答本地主机。通过选中断开的服务器，客户机将能够接收通过非特权端口通讯的服务器的答复。有关进一步信息，请参见 manypbind。

完成设置后，请单击完成保存更改并返回 YaST 控制中心。

图 35.6 设置 NIS 服务器的域和地址


输入您的 NIS 域(例如 example.com) 和 NIS 服务器的地址(例如 nis.example.com 或 10.20.1.1)。

指定多台服务器，服务器的地址之间用空格分隔。

使用□□选项可以在指定服务器响应失败后，在本地网络中进行搜索来查找服务器。这存在安全风险。

如果您正在使用 DHCP 并且服务器提供 NIS 域名或服务器，则可以在此使用它们。DHCP 本身可以在网络模块中进行设置。

Automounter 是一个守护程序，它会自动装入目录，例如用户的主目录。假定在本地或 NIS 中已存在该守护程序的配置文件 (auto.\*)。

 NIS 客户机的配置

☐ 不使用 NIS(M)  
☒ 使用 NIS(U)

NIS 客户机

☐ 自动设置(通过 DHCP)(I)  
☒ 静态设置(S)

NIS 域(I)  
example.com

NIS 服务器的地址(A)  
192.168.27.4

☐ 广播(B) 查找(F)

附加 NIS 域  
localdomain 编辑(E)

☐ 启动 Automounter(M)

专家(X)...

后退(B)

中止(B)

完成(E)

## LDAP - 目录服务

轻量级目录访问协议 (LDAP) 是一组设计用来访问和维护信息目录的协议。LDAP 可用于多种目的，如用户和组管理、系统配置管理或地址管理。本章简要介绍 `openldap` 的工作原理以及如何使用 YaST 管理 LDAP 数据。尽管实施多个 LDAP 协议，但本章着重介绍 OpenLDAP 实施。

在互联网环境中保持重要信息组织有序并且访问便捷是非常重要的。这可以通过目录服务实现。目录服务就像常见的电话黄页，可以将信息组织得井然有序，便于快速搜索。

理想情况下，应该有一个中央服务器将数据组织到目录中，并使用特定协议将其分发给所有客户机。数据以特定的方式组织，以支持众多应用程序进行访问。这样，各种日历工具和电子邮件客户程序就不必保持自己的数据库，只需访问中央储存库即可。这种方式极大地减轻了管理这些信息的工作。利用 LDAP 之类的开放且标准化的协议，可以保证让尽量多的客户应用程序都能访问这些信息。

这里所说的目录实际上是指一种为快速有效的读取和搜索而优化的数据库。

- 为支持大量并行读取访问，需要限制写访问，只允许管理员执行次数较少的更新。要对常规数据库进行优化，使其能够在短时间内接受尽量多的数据。
- 由于只能在受限模式下执行写访问，所以可以采用目录服务来管理几乎不变的静态信息。常规数据库中的数据通常频繁变化（动态数据），而公司名录中的电话号码并不像会计数字（举例来说）那样经常变化。
- 管理静态数据时，极少更新现有数据集。而处理动态数据时，特别是在涉及像银行帐户或会计帐户这样的数据集时，数据的一致性举足轻重。如果

要将从某处减去的数目加到另一个位置，必须在一个事务中同时执行这两个运算，以确保数据存量保持平衡。数据库支持处理这类事务，而目录却不行。短期内数据之间的不一致在目录中是完全可以接受的。

LDAP 这类目录服务并不是为支持复杂的更新或查询机制而设计的。访问此服务的所有应用程序都应能够便捷地获取访问权。

## 36.1 对比 LDAP 和 NIS

Unix 系统管理员以往使用 NIS 服务在网络内进行名称解析和数据分发。/etc 中的文件所包含的配置数据以及目录 group、hosts、mail、netgroup、networks、passwd、printcap、protocols、rpc 和 services 都通过客户程序在网络中分发。这些文件很容易维护，因为它们都是简单的文本文件。但随着数据量的不断增大，处理起来就会因为缺乏组织结构而愈发困难。NIS 仅适用于 Unix 平台。就是说它不适合在异构网络中充当集中式数据管理工具。

有别于 NIS，LDAP 服务不仅仅适用于单纯的 Unix 网络。Windows 2000 之后的服务器都支持 LDAP 作为目录服务。上述应用程序任务在非 Unix 系统中同样受支持。

LDAP 原理适用于所有需要集中管理的数据结构。以下是一些应用示例：

- 用于替代 NIS 服务
- 邮件路由选择（postfix、sendmail）
- 邮件客户机（如 Mozilla、Evolution 和 Outlook）的通讯录
- 为 BIND9 名称服务器管理区域说明
- 异构网络中使用 Samba 进行用户身份验证

可以扩展此列表，因为 LDAP 是可扩展的，这是 NIS 所不能及的。由于更便于搜索数据，明确定义的数据层次结构简化了对大量数据的管理。

## 36.2 LDAP 目录树的结构

要深入了解 LDAP 服务器工作方式和数据储存方式的背景知识，关键在于了解数据在服务器上的组织方式，以及该结构如何可以使 LDAP 能够提供对所需数据的快速访问。要成功进行 LDAP 设置，还需要熟悉一些基本 LDAP 术语。本节介绍 LDAP 目录树的基本布局，并提供了在 LDAP 环境中使用的基本术语。如果您已经了解一些 LDAP 背景知识，只是想了解如何在 SUSE Linux Enterprise 中设置 LDAP 环境，可跳过这个介绍部分。分别在[第 36.5 节“使用 YaST 配置 LDAP 服务器”](#) [613]或[第 36.3 节“使用 slapd.conf 配置服务器”](#) [604]上阅读。

LDAP 目录具有树形结构。目录中的所有项（称为对象）在此层次结构中都有确定的位置。此层次结构称为*目录信息树 (DIT)*。指向所需项的完整路径（可以明确标识该项）被称为*判别名*或 DN。沿路径指向此项的单个节点称为*相对判别名*或 RDN。通常可以向以下两种可能类型之一指派对象：

### 容器

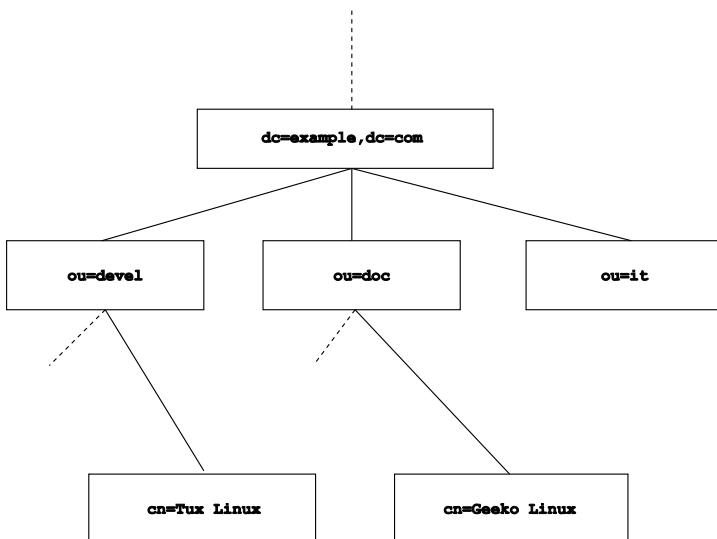
这些对象本身可以包含其他对象。这些对象类包括 `root`（目录树的根元素，实际并不存在）、`c`（国家/地区）、`ou`（组织单元）和 `dc`（域组件）。此模型类似文件系统中的目录（文件夹）。

### 叶

这些对象位于分支的末梢，没有任何从属对象。`person`、`InetOrgPerson` 或 `groupofNames` 都属于此类对象。

目录层次的顶端有一个根元素 `root`。其中可包含 `c`（国家/地区）、`dc`（域组件）或 `o`（组织）作为从属元素。LDAP 目录树中的关系在下例中尤为明显，如 [图 36.1“LDAP 目录的结构”](#) [602] 所示。

图 36.1 LDAP 目录的结构



完整的图是一个虚构的目录信息树。其中描述了三个层次上的项。每一项都对应图中的一个框。在本例中，虚构的雇员 *Geeko Linux* 的完整有效判别名为 `cn=Geeko Linux,ou=doc,dc=example,dc=com`。该名称是通过将 RDN `cn=Geeko linux` 添加到前一项的 DN `ou=doc,dc=example,dc=com` 而构成的。

应该储存 DIT 的对象类型是按照模式全局确定的。对象类型由对象类决定。对象类决定必须或可以给相关对象指派哪些属性。因此，方案中必须包含所需应用方案中使用的所有对象类和属性的定义。已存在一些常用方案（请参见 RFC 2252 和 2256）。不过，可以创建自定义方案或使用多个互补的方案（如果 LDAP 服务器的运行环境要求这样做）。

表 36.1 “常用对象类和属性” [603] 提供了示例所用的 `core.schema` 和 `inetorgperson.schema` 中的对象类的简要概览（包括必需属性和有效属性值）。



表 36.1 常用对象类和属性

对象类	含义	示例项	必需属性
dcObject	<i>domainComponent</i> ( 域的名称 组件 )	示例	dc
organizationalUnit	<i>organizationalUnit</i> ( 组织单 元 )	doc	ou
inetOrgPerson	<i>inetOrgPerson</i> ( 内部网或因特 网中与个人有关的数据 )	Geeko Linux	sn 和 cn

例 36.1 “引自 [schema.core](#)” [603]引自一个方案指令，并附有解释（为便于解释对行进行了编号）。

例 36.1 引自 *schema.core*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2         DESC 'RFC2256: organizational unit this object belongs to'
#3         SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5         DESC 'RFC2256: an organizational unit'
#6         SUP top STRUCTURAL
#7         MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
        $ x121Address $ registeredAddress $ destinationIndicator
        $ preferredDeliveryMethod $ telexNumber
        $ teletexTerminalIdentifier $ telephoneNumber
        $ internationaliSDNNumber $ facsimileTelephoneNumber
        $ street $ postOfficeBox $ postalCode $ postalAddress
        $ physicalDeliveryOfficeName
        $ st $ l $ description) )

...
```

属性类型 `organizationalUnitName` 和相应的对象类 `organizationalUnit` 在此仅作为示例。第 1 行说明属性的名称、其唯一 `OID`（对象标识符）（数字），及属性缩写方式。

第 2 行通过 `DESC` 对该属性进行了简要说明。在此还提到了定义所基于的相应 `RFC`。第 3 行中的 `SUP` 表明此属性所属的上级属性类型。

从第 4 行开始是对象类 `organizationalUnit` 的定义；与属性定义类似，该定义也包含对象类的 **OID** 和名称。第 5 行对该对象类进行了简要说明。第 6 行通过项 `SUP top` 表明此对象类不从属于其他对象类。第 7 行以 **MUST** 开头，列出必须与类型为 `organizationalUnit` 的对象一同使用的所有属性类型。第 8 行以 **MAY** 开头，列出可以与此对象类一同使用的所有属性类型。

有关方案用法的详尽介绍，请参见文档 **OpenLDAP**。安装 **OpenLDAP** 之后，可以在 `/usr/share/doc/packages/openldap2/admin-guide/index.html` 中找到该文档。

## 36.3 使用 `slapd.conf` 配置服务器

已安装系统的 `/etc/openldap/slapd.conf` 中包含 LDAP 服务器的完整配置文件。在此简述了其中的各个项并说明了必要的调整。以符号 **(#)** 为前缀的项处于非活动状态。必须取消这个注释字符才能激活这些项。

### 36.3.1 `slapd.conf` 中的全局指令

**例 36.2** *`slapd.conf`: 用于模式的 `Include` 指令*

```
include      /etc/openldap/schema/core.schema
include      /etc/openldap/schema/cosine.schema
include      /etc/openldap/schema/inetorgperson.schema
include      /etc/openldap/schema/rfc2307bis.schema
include      /etc/openldap/schema/yast.schema
```

这是 `slapd.conf` 中的第一个指令（如例 36.2 “`slapd.conf`：用于模式的 `Include` 指令” [604] 所示），用于指定组织 LDAP 目录所依据的模式。`core.schema` 是必需项。所需的其余模式会追加到此指令中。在包含的 OpenLDAP 文档中查找信息。

### 例 36.3 `slapd.conf`： `pidfile` 和 `argsfile`

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

这两个文件包含启动 `slapd` 进程所用的 PID（进程 ID）和一些参数。在此没必要进行修改。

### 例 36.4 `slapd.conf`：访问控制

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
#       access to * by self write
#               by users read
#               by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

例 36.4 “`slapd.conf`：访问控制” [605] 节选自 `slapd.conf`，涉及如何管理服务上的 LDAP 目录的访问权限。只要在数据库特定部分没有声明任何自定义访问规则，`slapd.conf` 的全局部分中的设置将始终有效。这些自定义声明会重写全局声明。如本例所示，所有用户都可以读取目录，但只有管理员 (`rootdn`) 才能写入此目录。LDAP 中的访问控制管理是一个非常复杂的过程。以下提示会有所帮助：

- 每条访问规则都具有如下结构：

```
access to <what> by <who> <access>
```

- *what* 是一个占位符，表示授权访问的对象或属性。可以使用单独的规则来明确保护各个目录分支。还可以使用正则表达式通过一条规则处理目录树的各个区域。*slapd*按照各条规则列在配置文件中的先后顺序依次评估它们。较通用的规则应列在较特定的规则之后 — 在评估 *slapd* 认为有效的第一条规则之后，随后的所有项都将被忽略。
- *who* 确定应该授权谁来访问 *what* 确定的区域。可以使用正则表达式。*slapd* 同样会在评估第一条有效规则之后中止对随后的 *who* 的评估，所以应将较具体的规则列在较抽象的规则之前。可以使用 [表 36.2 “用户组及其访问授权”](#) [606] 所示的项。

**表 36.2** 用户组及其访问授权

标记	范围
*	所有用户，无一例外
anonymous	未身份验证“匿名”用户
users	已身份验证用户
self	与目标对象连接的用户
dn.regex=<regex>	与正则表达式匹配的所有用户

- *access* 指定访问类型。请使用 [表 36.3 “访问类型”](#) [606] 所列的选项。

**表 36.3** 访问类型

标记	访问范围
none	无访问权
auth	用于联系服务器
compare	授予要进行比较访问的对象

标记	访问范围
search	用于应用搜索过滤器
read	读权限
write	写权限

slapd 会将客户机请求的访问权限与 slapd.conf 中授予的权限进行对比。如果规则允许的权限等于或高于请求的权限，则可以授予客户机权限。如果客户机请求的权限高于规则中声明的权限，便会拒绝授予权限。

**例 36.5 “slapd.conf: 访问控制示例”** [607]显示了一个简单示例，使用正则表达式可以随意指定这样的简单访问控制。

**例 36.5** *slapd.conf: 访问控制示例*

```
access to dn.regex="ou=([^,]+),dc=example,dc=com"  
by dn.regex="cn=Administrator,ou=$1,dc=example,dc=com" write  
by user read  
by * none
```

此规则声明只有各个 ou 项的管理员才有权写入他/她所管理的项。其他所有通过身份验证的用户只有读权限，其余人没有任何权限。

**提示：建立访问规则**

如果没有 access to 规则或匹配的 by 指令，则拒绝访问。只有经过显式声明才能授予访问权限。如果根本没有声明任何规则，默认规则是管理员具有写权限，其他所有用户都具有读权限。

有关 LDAP 访问权限的详细信息和示例配置，请参见所安装的 openldap2 包中的联机文档。

除了可以使用中央服务器配置文件 (slapd.conf) 管理访问权限之外，还可以使用访问控制信息 (ACI)。ACI 允许储存 LDAP 树中各个对象的访问信息。这种访问控制尚未普及，开发人员认为它目前仍处于试用阶段。相关信息请参见 <http://www.openldap.org/faq/data/cache/758.html>。

## 36.3.2 slapd.conf 中的数据库特定指令

### 例 36.6 slapd.conf: 特定于数据库的指令

```
database bdb❶
suffix "dc=example,dc=com"❷
checkpoint 1024 5❸
cachesize 10000❹
rootdn "cn=Administrator,dc=example,dc=com"❺
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slapasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret❻
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap❼
# Indices to maintain
index objectClass eq❽
overlay ppolicy❾
ppolicy_default "cn=Default Password Policy,dc=example,dc=com"
ppolicy_hash_cleartext
ppolicy_use_lockout
```

- ❶ 数据库类型（本案例中为 Berkeley）是在本部分的第一行设置的（请参见例 36.6 “slapd.conf: 特定于数据库的指令” [608]）。
- ❷ suffix 确定服务器应负责的 LDAP 树的部分。
- ❸ checkpoint 确定写入真实数据库前保留在事务日志中的数据量（以 KB 为单位）以及两次写操作之间的时间（以分钟为单位）。
- ❹ cachesize 设置保留在数据库缓存中的对象数。
- ❺ rootdn 确定拥有此服务器的管理员权限的用户。在此声明的用户不必拥有 LDAP 项，也不必是普通用户。
- ❻ rootpw 设置管理员密码。在此不必使用 secret，可以输入 slapasswd 创建的管理员密码的哈希值。
- ❼ directory 指令表明数据库目录储存在服务器的文件系统哪个目录中。
- ❽ 最后一个指令 index objectClass eq 指示对所有对象类的索引进行维护。可以在此根据经验添加用户最常搜索的属性。
- ❾ overlay ppolicy 添加一个密码控制机制层。ppolicy\_default 指定给定用户项上未设置特定策略时要使用的 pwdPolicy 对象的 DN。如果对某

项无特定策略，且未给定默认值，则不会强加任何策略。

`ppolicy_hash_cleartext` 指定显示在添加和修改请求中的明文密码在储存到数据库之前会执行哈希运算。使用此选项时，建议拒绝所有目录用户对 `userPassword` 属性的比较、搜索和读访问，因为

`ppolicy_hash_cleartext` 违反了 X.500/LDAP 信息模型。当某客户机尝试连接锁定帐户时，`ppolicy_use_lockout` 会发送一个特定的错误代码。如果您的站点对安全问题敏感，请禁用此选项，因为错误代码会向攻击者提供有用的信息。

在此为数据库自定义的 Access 规则将取代全局 Access 规则。

### 36.3.3 启动和停止服务器

在根据第 36.4 节“LDAP 目录中的数据处理”[609]所述的模式对 LDAP 服务器进行完全配置并设置全部所需项之后，可通过输入 `rcldap start` 以 `root` 身份启动 LDAP 服务器。要手动停止服务器，请输入命令 `rcldap stop`。使用 `rcldap status` 可请求运行中的 LDAP 服务器的状态。

可以使用第 20.2.3 节“使用 YaST 配置系统服务（运行级别）”[365]中所述的 YaST 运行级别编辑器，在引导和暂停系统时相应地自动启动和停止服务器。还可以如第 20.2.2 节“Init 脚本”[361]所述，在命令提示中使用 `insserv` 命令创建指向启动脚本和停止脚本的相应链接。

## 36.4 LDAP 目录中的数据处理

OpenLDAP 提供一系列工具，可用于在 LDAP 目录中管理数据。下文简要说明了四种最重要的工具，分别对储存的数据执行添加、删除、搜索和修改等操作。

### 36.4.1 将数据插入 LDAP 目录

在 `/etc/openldap/lsapd.conf` 中正确配置 LDAP 服务器并且准备就绪后（即已配置好 `suffix`、`directory`、`rootdn`、`rootpw` 和 `index` 这些项之后），接下来可以输入记录。OpenLDAP 为此任务提供了 `ldapadd` 命令。如果可行，最好以捆绑方式向数据库添加对象，这是较为实用的做法。LDAP 能够为此处理 LDIF 格式（LDAP 数据交换格式）。LDIF 文件是一个简单的文本文

件，可以包含任意数量的属性和值对。请参见 `slapd.conf` 中声明的纲要文件，了解可用的对象类和属性。为图 36.1 “LDAP 目录的结构” [602] 中的示例创建大致框架的 LDIF 文件将如例 36.7 “LDIF 文件示例” [610] 所示：

### 例 36.7 LDIF 文件示例

```
# The Organization
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
o: Example dc: example

# The organizational unit development (devel)
dn: ou=devel,dc=example,dc=com
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=example,dc=com
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=example,dc=com
objectClass: organizationalUnit
ou: it
```

---

#### 重要：LDIF 文件的编码

LDAP 采用 UTF-8 (Unicode) 编码。必须对元音变音符正确编码。请使用支持 UTF-8 的编辑器，如 Kate 或 Emacs 的最近版本。否则请避免使用元音变音符和其他特殊字符，或使用 `recode` 将输入内容重新编码为 UTF-8。

---

以 `.ldif` 为后缀保存该文件，然后使用以下命令将其传递给服务器：

```
ldapadd -x -D <dn of the administrator> -W -f <file>.ldif
```

`-x` 在本例中用于关闭通过 SASL 身份验证。`-D` 用于声明调用操作的用户。在此输入管理员的有效 DN，就如同已经在 `slapd.conf` 中配置。在当前示例中为 `cn=Administrator,dc=example,dc=com`。`-W` 用于避免在命令行中输入密码（以明文形式），而改为激活单独的密码提示。此密码此前已在 `slapd.conf` 中通过 `rootpw` 确定。`-f` 用于传递文件名。请参见例 36.8 “example.ldif 中的 ldapadd” [611] 中关于运行 `ldapadd` 的详细信息。



### 例 36.8 *example.ldif* 中的 *ldapadd*

```
ldapadd -x -D cn=Administrator,dc=example,dc=com -W -f example.ldif
```

```
Enter LDAP password:
adding new entry "dc=example,dc=com"
adding new entry "ou=devel,dc=example,dc=com"
adding new entry "ou=doc,dc=example,dc=com"
adding new entry "ou=it,dc=example,dc=com"
```

个人的用户数据可以储存在单独的 LDIF 文件中。例 36.9 “Tux 的 LDIF 数据” [611] 向新的 LDAP 目录添加了 Tux。

### 例 36.9 *Tux* 的 LDIF 数据

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@example.com
uid: tux
telephoneNumber: +49 1234 567-8
```

LDIF 文件可以包含任意数目的对象。一次可以将整个目录分支都传递到服务器中，也可以仅传递部分目录，如单个对象的示例所示。如果需要对某些数据进行较为频繁的修改，建议对单个对象进行细分。

## 36.4.2 修改 LDAP 目录中的数据

使用 `ldapmodify` 工具可以修改储存数据。最简单的方法是修改相应的 LDIF 文件，然后将这个修改过的文件传递给 LDAP 服务器。若要将同事 Tux 的电话号码从 +49 1234 567-8 改为 +49 1234 567-10，请像在例 36.10 “修改过的 LDIF 文件 *tux.ldif*” [611] 中那样编辑 LDIF 文件。

### 例 36.10 修改过的 LDIF 文件 *tux.ldif*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

使用以下命令将修改过的文件导入 LDAP 目录：

```
ldapmodify -x -D cn=Administrator,dc=example,dc=com -W -f tux.ldif
```

或者，直接将要更改的属性传递给 `ldapmodify`。该过程如下所述：

**1** 启动 `ldapmodify` 并输入您的密码：

```
ldapmodify -x -D cn=Administrator,dc=example,dc=com -W
Enter LDAP password:
```

**2** 输入更改，同时要小心地采用如下所示的语法顺序：

```
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

有关 `ldapmodify` 及其语法的详细信息，请参见 `ldapmodify` 手册中的语法。

## 36.4.3 搜索或读取 LDAP 目录中的数据

OpenLDAP 提供 `ldapsearch` 命令行工具，用于搜索 LDAP 目录中的数据并从中读取数据。简单查询将采用以下语法：

```
ldapsearch -x -b dc=example,dc=com "(objectClass=*)"
```

选项 `-b` 用于确定搜索基础 — 要执行搜索的树的对应部分。在当前情况下为 `dc=example,dc=com`。要在 LDAP 目录的某个子部分中执行更为精确的搜索（例如仅在 `devel` 部门内搜索），请使用 `-b` 将此部分传递给 `ldapsearch`。`-x` 用于请求激活简单身份验证。`(objectClass=*)` 用于声明应该读取目录包含的所有对象。可以在创建新目录树后使用此命令选项，用来校验是否正确记录所有项并且服务器是否能按预期响应。有关 `ldapsearch` 用法的详细信息，请参见相应的手册页 (`ldapsearch(1)`)。

## 36.4.4 删除 LDAP 目录中的数据

使用 `ldapdelete` 可以删除不需要的项。该命令的语法与上述命令的语法相似。例如，要彻底删除 Tux Linux 项，请发出以下命令：

```
ldapdelete -x -D cn=Administrator,dc=example,dc=com -W cn=Tux \
Linux,ou=devel,dc=example,dc=com
```

## 36.5 使用 YaST 配置 LDAP 服务器

使用 YaST 设置 LDAP 服务器。使用 LDAP 服务器的一个典型例子包括管理用户帐户数据和配置邮件、DNS 和 DHCP 服务器。

图 36.2 YaST LDAP 服务器配置

要为用户帐户数据设置 LDAP 服务器，如下操作：

- 1 以 root 身份登录。
- 2 启动 YaST 并选择网络服务 > LDAP 服务器。

- 3 将 LDAP 设置成在系统自举时启动。
- 4 如果 LDAP 服务器应该通过 SLP 宣告其服务，则选取在 *SLP 守护程序中注册*。
- 5 选择 *配置* 以配置一般设置和数据库。

要配置 LDAP 服务器的全局设置，继续如下操作：

- 1 通过选择对话框左面部分的 *纲要文件*，接受或修改服务器配置中包括的纲要文件。纲要文件的默认选择适用于提供 YaST 用户帐户数据源的服务器。
- 2 使用 *日志级别设置*，可以配置 LDAP 服务器的日志记录活动的程度（冗长级别）。从预定义列表中，根据需要选择或取消选择日志记录选项。启用的选项越多，日志文件就会越大。
- 3 确定 LDAP 服务器允许的连接类型。选择自：

`bind_v2`

此选项支持从使用上一版本协议 (LDAPv2) 的客户机发出的连接请求（联结请求）。

`bind_anon_cred`

通常 LDAP 服务器拒绝所有身份凭证（DN 或密码）为空的身份验证尝试。但启用此选项后，可以在使用密码但不提供 DN 的情况下建立匿名连接。

`bind_anon_dn`

若启用此选项，则可以使用 DN 但不提供密码以无身份验证方式（匿名地）建立连接。

`update_anon`

启用此选项支持以非身份验证（匿名）方式执行更新操作。访问要受 ACL 和其他规则的限制（请参见 [第 36.3.1 节“slapd.conf 中的全局指令”](#) [604]）。

- 4 要在客户机和服务器之间配置安全通信，继续 *TLS 设置操作*：

**4a** 将 *TLS 活动* 设置成是以启用客户机 / 服务器通信的 TLS 和 SSL 加密。

**4b** 单击 *选择证书* 并确定如何获得有效证书。选择 *导入证书*（从外部源导入证书）或 *使用普通服务器证书*（使用安装期间创建的证书）。

- 如果您选择导入证书，则 YaST 提示您指定其位置的准确路径。
- 如果您选择使用公共服务器证书并且安装期间未创建该证书，则会在以后的操作中创建它。

要配置 LDAP 服务器管理的数据库，继续如下操作：

- 1 在对话框的左面部分选择 *数据库* 项。
- 2 单击 *添加数据库* 以添加新的数据库。
- 3 输入请求的数据：

*基本 DN*

输入 LDAP 服务器的基本 DN。

*根 DN*

输入负责服务器的管理员的 DN。如果选中 *追加基本 DN*，只需提供管理员的 cn，系统会自动填充其余部分。

*LDAP 密码*

输入数据库管理员的密码。

*加密*

确定要用于保护根 DN 的密码的加密算法。选择 *crypt*、*smd5*、*ssha* 或 *sha*。该对话框还包含 *明文* 选项，支持使用明文密码；但出于安全考虑，不建议启用此选项。要确认设置并返回上一个对话框，请选择 *确定*。

- 4 启用强制密码策略以对 LDAP 服务器提供额外的安全性：

**4a** 选择 *密码策略设置* 以指定密码策略。

**4b** 任何时候添加或修改明文密码时，激活 *哈希明文密码* 以在写入数据库前对明文密码执行哈希运算。

- 4c** 公开“帐户锁定”状态提供了对于将请求绑定到锁定帐户有价值的错误消息。

---

**警告：对安全性敏感的环境中的锁定帐户**

如果环境对安全性问题敏感，请不要使用公开“帐户锁定”状态选项，因为“锁定帐户”错误消息提供的安全敏感信息可能会被潜在的攻击者利用。

---

- 4d** 输入默认策略对象的 DN。要使用不同于 YaST 建议的 DN，请输入您的选择。否则，接受默认设置。

**5 通过单击完成以完成数据库配置。**

如果未选择密码策略，服务器将准备好在此时运行。如果选择启用密码策略，继续配置密码策略的细节。如果选择了还不存在的密码策略对象，YaST 会创建一个：

**1 输入 LDAP 服务器密码。**

**2 配置密码更改策略：**

**2a** 确定储存在密码历史中的密码个数。用户可能无法重复使用已保存的密码。

**2b** 确定用户是否可更改其密码，以及在管理员进行重设置后，用户是否需要更改密码。可以选择在更改密码时要求提供旧密码。

**2c** 确定是否应对密码进行质量检查以及检查的程度。设置为使密码有效而必须满足的最小密码长度。如果选择接受不可检查的密码，尽管无法执行质量检查，用户仍可使用加密的密码。如果选择只接受已检查的密码，则只有通过质量测试的那些密码可作为有效密码被接受。

**3 配置密码过期策略：**

**3a** 确定最短（两次有效密码更改之间需经过的时间）和最长密码使用期限。

**3b** 确定密码失效警告和实际密码失效之间的时间。

**3c** 设置密码完全失效前宽限使用失效密码的次数。

**4** 配置锁定策略：

**4a** 启用密码锁定。

**4b** 确定触发密码锁定的绑定失败次数。

**4c** 确定密码锁定的持续时间。

**4d** 确定清除密码故障前将其保留在缓存中的时长。

**5** 选择接受应用密码策略设置。

要编辑此前创建的数据库，请在左侧的目录树中选择其基本 DN。在窗口的右侧，YaST 显示与创建新数据库时所用相似的对话框 — 主要区别在于基本 DN 项已灰化且无法更改。

选择完成以退出 LDAP 服务器配置后，就可以使用 LDAP 服务器的基本工作配置了。要对此设置进行微调，请相应地编辑文件 `/etc/openldap/slapd.conf`，然后重启服务器。

## 36.6 使用 YaST 配置 LDAP 客户机

YaST 包含一个用于设置基于 LDAP 的用户管理的模块。如果安装期间未启用此功能，请通过选择 **网络服务 > LDAP 客户机** 来启动模块。YaST 会自动启用 LDAP 所需的任何 PAM 和 NSS 相关更改并安装所需文件。

### 36.6.1 标准过程

进程在客户机的后台运行的背景知识可帮助您理解 YaST LDAP 客户机模块是如何运行的。如果为进行网络身份验证激活了 LDAP 或是调用了 YaST 模块，系统会安装包 `pam_ldap` 和 `nss_ldap` 并调整两个相应的配置文件。`pam_ldap` 是负责在登录进程和 LDAP 目录（作为身份验证数据源）之间进行协商的 PAM

模块。将安装专用模块 `pam_ldap.so` 并调整 PAM 配置（请参见例 36.11 “为适应 LDAP 而调整的 `pam_unix2.conf`” [618]）。

**例 36.11** 为适应 LDAP 而调整的 `pam_unix2.conf`

```
auth:      use_ldap
account:   use_ldap
password:  use_ldap
session:   none
```

手动配置其他服务使用 LDAP 时，请将该服务对应的 PAM 配置文件中的 PAM LDAP 模块加入 `/etc/pam.d`。可以在 `/usr/share/doc/packages/pam_ldap/pam.d/` 中找到为适应各种服务而调整过的配置文件。将相应文件复制到 `/etc/pam.d` 中。

使用 `nss_ldap` 可以对通过 `nsswitch` 机制执行的 `glibc` 名称解析进行调整，使其适应 LDAP 的部署。安装此包时将在 `/etc` 中创建新的调整过的文件 `nsswitch.conf`。有关 `nsswitch.conf` 工作的更多信息，请参见第 30.7.1 节“配置文件” [530]。`nsswitch.conf` 中必须存在以下行才能进行用户管理及 LDAP 身份验证。请参见例 36.12 “`nsswitch.conf` 中的调整” [618]。

**例 36.12** `nsswitch.conf` 中的调整

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

这些行指示 `glibc` 的解析程序库首先评估 `/etc` 中的相应文件，而后还要访问作为身份验证和用户数据来源的 LDAP 服务器。测试这种机制，例如通过使用命令 `getent passwd` 读取用户数据库中的内容。返回的结果集不仅应该包含您系统中本地用户的调查结果，还应包含所有储存在 LDAP 服务器上的用户的调查结果。

要防止通过 LDAP 管理的普通用户使用 `ssh` 或 `login` 登录该服务器，文件 `/etc/passwd` 和 `/etc/group` 都需要添加另外一行。这一行在 `/etc/passwd` 中为 `+:::/:sbin/nologin`，在 `/etc/group` 中为 `+:::`。



# 36.6.2 配置 LDAP 客户端

在YaST 初始调整了 nss\_ldap、pam\_ldap、/etc/passwd 和 /etc/group 之后，您只需将客户机连接到服务器并使 YaST 通过 LDAP 来管理用户。中描述了基本设置。“基本配置”一节 [619]

使用 YaST LDAP 客户端来进一步配置 YaST 组 and 用户配置模块。这包括为新用户和组执行默认设置和为用户或组指派的属性数和性质。LDAP 用户管理允许您为用户和组指派比传统用户或组管理解决方案更多的不同属性。中对此进行了描述。“配置 YaST 组 and 用户管理模块”一节 [622]

## 基本配置

如果您选择 LDAP 用户管理或当您在已安装系统的 YaST 控制中心中选择网络服务 > LDAP 客户端时，基本 LDAP 客户端配置对话框（图 36.3 “YaST：LDAP 客户程序的配置” [619]）在安装期间会打开。

图 36.3 YaST：LDAP 客户程序的配置



要针对 OpenLDAP 服务器来身份验证计算机的用户并通过 OpenLDAP 来启用用户管理，请按如下操作：

- 1 单击使用 *LDAP* 以启用 *LDAP*。如果您希望使用 *LDAP* 来进行身份验证但不希望其他用户登录到此客户机，则选择使用 *LDAP 但禁用登录*。
- 2 输入要使用的 *LDAP* 服务器的 IP 地址。
- 3 输入 *LDAP* 基本 *DN* 以在 *LDAP* 服务器上选择搜索基础。要自动检索基本 *DN*，请单击获取 *DN*。然后 YaST 会在上面指定的服务器地址检查所有 *LDAP* 数据库。从 YaST 给出的搜索结果中选择适当的基本 *DN*。
- 4 如果需要与服务器进行 *TLS* 或 *SSL* 受保护通信，则选择 *LDAP TLS/SSL*。
- 5 如果 *LDAP* 服务器仍然使用 *LDAPv2*，则通过选择 *LDAP 版本 2* 来显式启用此协议版本。
- 6 选择启动*Automounter*来在客户机上装入远程目录，如远程管理的 */home*。
- 7 选择登录时创建用户主目录可在用户第一次登录时自动创建用户主目录。
- 8 单击结束来应用设置。

图 36.4 YaST：高级配置



要作为管理员修改服务器上的数据，请单击高级配置。以下对话框显示在两个选项卡中。请参见图 36.4 “YaST：高级配置” [620]。

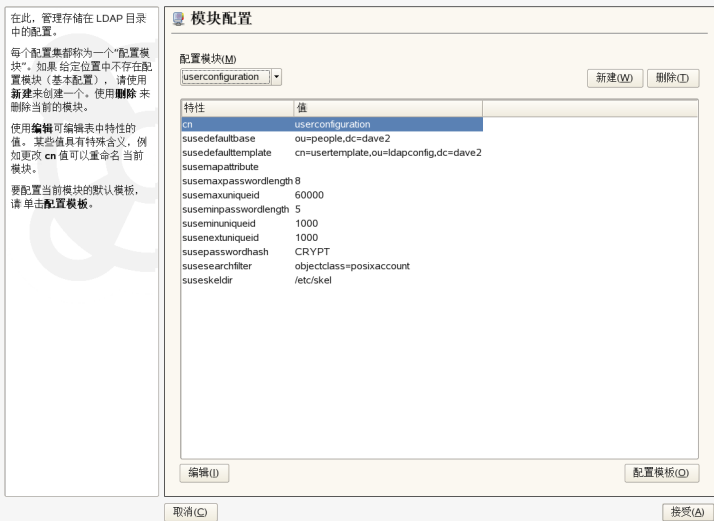
- 1 在客户机设置选项卡中，根据需要来调整以下设置：
  - 1a 如果用户、密码和组的搜索基础与指定 *LDAP* 基本 *DN* 的全局搜索基础不同，则在用户映射、密码映射和组映射中输入这些不同的命名上下文。
  - 1b 指定密码更改协议。无论何时更改密码，使用的标准方法都为 *crypt*，它表示使用 *crypt* 生成的密码哈希值。有关此选项和其他选项的详细信息，请参见 *pam\_ldap* 手册页。
  - 1c 指定与组成员属性一起使用的 *LDAP* 组。默认值为 *member*。
- 2 在管理设置中，调整以下设置：
  - 2a 通过配置基本 *DN* 来设置储存用户管理数据的基础。
  - 2b 为管理员 *DN* 输入合适的值。此 *DN* 必须与 */etc/openldap/slapd.conf* 中指定的 *rootdn* 值相同以使此特定用户能够处理 *LDAP* 服务器上储存的数据。输入完整的 *DN*（例如 *cn=Administrator*、*dc=example* 和 *dc=com*）或激活追加基本 *DN*，使您输入 *cn=Administrator* 时能够自动添加基本 *DN*。
  - 2c 单击创建默认配置对象以在服务器上创建基本配置对象以通过 *LDAP* 启用用户管理。
  - 2d 如果您的客户机在网络中应作为用户主目录的文件服务器，请选中此计算机上的用户主目录。
  - 2e 使用密码策略部分选择、添加、删除或修改要使用的密码策略设置。用 *YaST* 配置密码策略是 *LDAP* 服务器安装的一部分。
  - 2f 单击接受以关闭高级配置，然后单击结束以应用设置。

使用配置用户管理设置编辑 *LDAP* 服务器上的项。随后将根据服务器上储存的 *ACL* 和 *ACI* 授予对服务器上的配置模块的访问权。请遵循“配置 *YaST* 组和用户管理模块”一节 [622] 中说明的过程。

# 配置 YaST 组和用户管理模块

使用 YaST LDAP 客户程序可以调整 YaST 模块使其适应用户和组管理，并按需扩展这些模块。使用个别属性的默认值来定义模板以简化数据注册。在此创建的预设值将作为 LDAP 对象储存在 LDAP 目录中。用户数据的注册仍使用常用的用户和组管理的 YaST 模块来完成。注册的数据作为 LDAP 对象储存在服务器上。

图 36.5 YaST：模块配置



模块配置对话框 (图 36.5 “YaST：模块配置” [622]) 允许创建新模块、选择和修改现有配置模块并设计和修改此类模块的模板。

要创建新的配置模块，请执行以下操作：

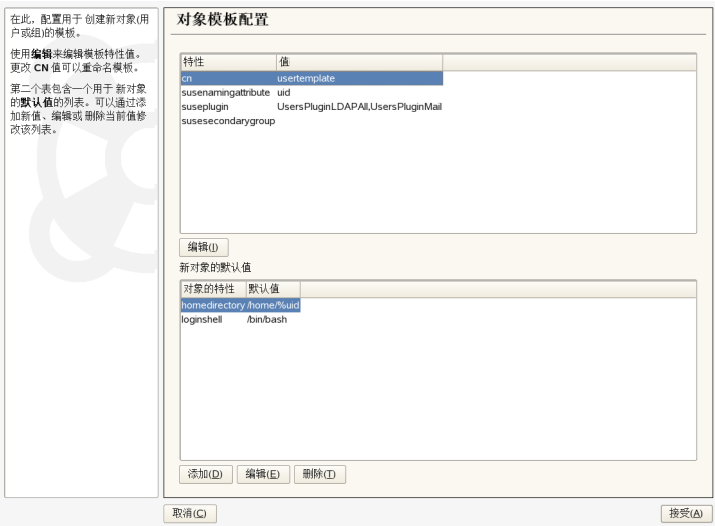
- 1 单击 **新建** 并选择要创建的模块的类型。对于用户配置模块，选择 `suseuserconfiguration`，对于组配置，选择 `susegroupconfiguration`。
- 2 为新模板选择名称。内容视图随即显示一个表，列出此模块允许使用的所有属性及其指派值。除所有已设置的属性之外，该列表还包含当前方案允许的但当前未使用的所有其他属性。

- 3 接受预设值或通过选择相关属性来调整要在组和用户配置中使用的默认值（按编辑，然后输入新值）。只需通过更改模块的 cn 属性来重命名模块。单击删除将删除当前所选模块。
- 4 在单击接受之后，新的模块将添加到选择菜单中。

用于组和用户管理的 YaST 模块会内嵌带有合理标准值的模板。要编辑与配置模块关联的模板，请如下执行操作：

- 1 在模块配置对话框中，单击配置模板。
- 2 根据您的需要来确定指派给此模板的常规属性的值或将某些值保留为空。LDAP 服务器将删除空属性值。
- 3 修改、删除或添加新对象（LDAP 树中的用户或组配置对象）的新默认值

图 36.6 YaST：对象模板的配置



通过将模块的 susedefaulttemplate 属性值设置为调整过的模板的 DN，可以将模板与模块连接起来。

---

## 提示

通过用变量代替绝对值的方法，可以从其他属性为某个属性创建默认值。例如，创建新用户时，将从 `sn` 和 `givenName` 的特性值自动创建 `cn=%sn %givenName`。

---

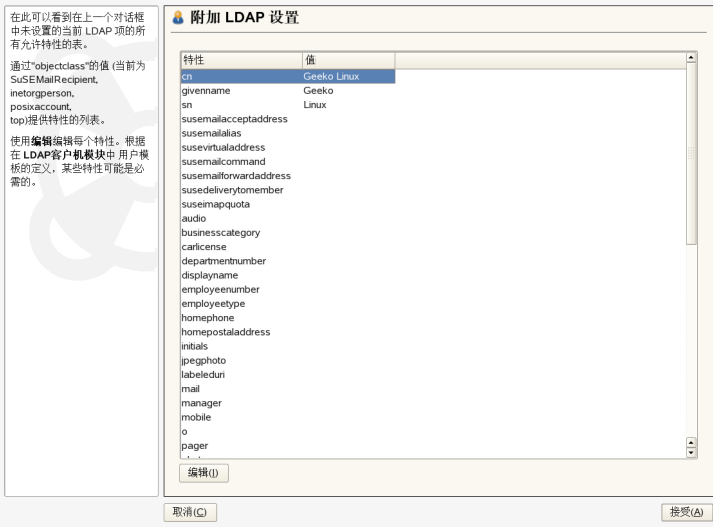
在所有模块和模板经过正确配置能够运行后，可以使用 YaST 按通常方式注册新组和用户。

## 36.7 在 YaST 中配置 LDAP 用户和组

用户和组数据的实际配置过程与不使用 LDAP 时的过程相差无几。下面简要说明了用户管理过程。管理组的过程与此相似。

- 1 通过安全性和用户 > 用户管理访问 YaST 用户管理。
- 2 使用设置过滤器来限制用户查看 LDAP 用户并输入根 DN 的密码。
- 3 单击添加并输入新用户的配置。将打开一个有四个选项卡的对话框：
  - 3a 在用户数据选项卡中指定用户名、登录和密码。
  - 3b 选中详细信息选项卡以输入新用户的组成员、登录 shell 和主目录。如果需要，将默认值更改为符合您需要的值。可以使用“配置 YaST 组和用户管理模块”一节 [622] 中描述的过程来定义默认值以及这些密码设置。
  - 3c 修改或接受默认密码设置。
  - 3d 进入插件选项卡，选择 LDAP 插件，然后单击启动以配置指派给新用户的其他 LDAP 属性（请参见图 36.7 “YaST：其他 LDAP 设置” [625]）。
- 4 单击接受以应用这些设置并关闭用户配置。

图 36.7 YaST: 其他 LDAP 设置



最初的用户管理输入表单提供了 *LDAP* 选项。通过此选项可以对一组现有用户应用 LDAP 搜索过滤器, 或者通过选择 *LDAP 用户和组配置* 转至用于配置 LDAP 用户和组的模块。

## 36.8 浏览 LDAP 目录树

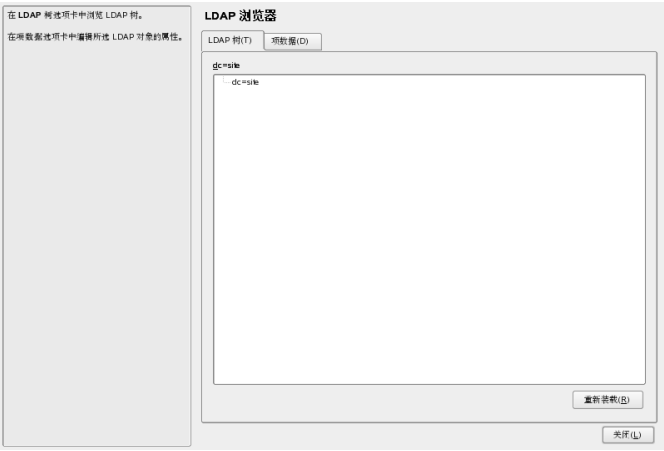
要方便地浏览 LDAP 目录树及其所有条目, 请使用 YaST LDAP 浏览器:

- 1 作为 root 登录。
- 2 启动 YaST > 网络服务 > LDAP 浏览器。
- 3 输入 LDAP 服务器地址、AdministratorDN 和该服务器的 RootDN 密码 (如果您需要这两者才能读写服务器上储存的数据)。

或者选择匿名访问, 不提供密码即可对目录进行读访问。

LDAP 树选项卡会显示您的计算机所连接的 LDAP 目录的内容。单击项目可展开其子项。

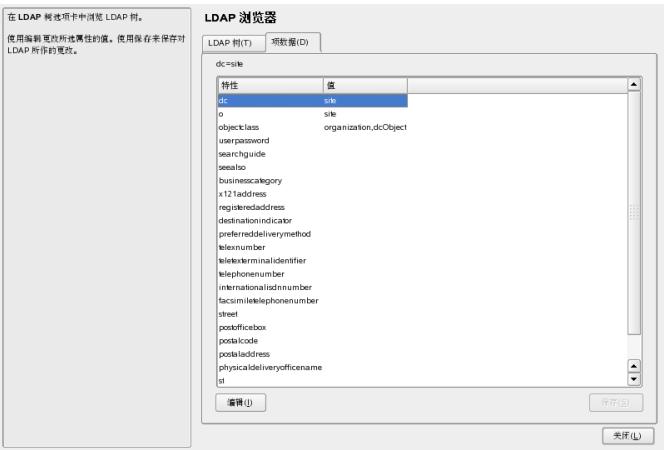
图 36.8 浏览 LDAP 目录树



4 要查看任何条目的细节，请在 *LDAP* 树视图中选择它，打开 *条目数据* 选项卡。

将显示所有和该条目相关的属性和值。

图 36.9 浏览条目数据





- 5 要更改这些属性的值，请选择该属性，单击 *编辑*，输入新值，单击 *保存*，在看到提示时提供 RootDN 密码。
- 6 用 *关闭* 退出 LDAP 浏览器。

## 36.9 有关详细信息

本章特意排除了一些较为复杂的主题，如 SASL 配置，或如何通过建立复制 LDAP 服务器在多台从属服务器上分配工作量。有关这两个主题的详细信息，请参见 *OpenLDAP 2.2 Administrator's Guide*。

OpenLDAP 项目的网站为初级和高级 LDAP 用户提供了丰富的文档：

### OpenLDAP Faq-O-Matic

涉及 OpenLDAP 的安装、配置和使用的非常详尽的问答集锦。请参见 <http://www.openldap.org/faq/data/cache/1.html>。

### 快速入门指南》

为首次安装 LDAP 服务器提供了简明的分步说明。请参见 <http://www.openldap.org/doc/admin22/quickstart.html> 或已安装系统中的 `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`。

### OpenLDAP 2.2 管理员指南

对 LDAP 配置的所有重要事项的详细介绍，包括访问控制和加密。请参见 <http://www.openldap.org/doc/admin22/> 或已安装系统上的 `/usr/share/doc/packages/openldap2/admin-guide/index.html`。

### Understanding LDAP（了解 LDAP）

关于 LDAP 基本原理的详尽的一般性介绍：<http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf>。

### LDAP 印刷文献资料：

- *LDAP System Administration* Gerald Carter 著 (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* Howes、Smith 和 Good 著 (ISBN 0-672-32316-8)

关于 LDAP 这一主题最后还可以参见相应的 RFC（请求注释）2251 到 2256。

# Samba

使用 Samba，可以将 Unix 计算机配置为 DOS、Windows 和 OS/2 计算机的文件和打印服务器。Samba 已经发展成为一个功能完备且相当复杂的产品。使用 YaST、SWAT（Web 接口）或配置文件来配置 Samba。

## 37.1 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。迫于 IBM 的压力，Microsoft 发布了该协议，这样其他软件制造商能够与 Microsoft 域网络建立连接。使用 Samba 时，SMB 协议在 TCP/IP 协议之上工作，所以必须在所有客户机上安装 TCP/IP 协议。

---

**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 是为计算机之间进行通讯而设计的软件接口 (API)。这里提供了一种名称服务。它使连接到网络的计算机能够为自己保留名称。之后便可以根据名称对这些计算机进行寻址。没有任何中心进程来检查这些名称。网络上的任何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。现在可以为不同的网络体系结构实施 NetBIOS 接口。NetBEUI 是与网络硬件结合相对密切的一种实施，但它常被称为 NetBIOS。使用 NetBIOS 实施的网络协议包括 Novell 的 IPX（通过 TCP/IP 的 NetBIOS）和 TCP/IP。

通过 TCP/IP 发送的 NetBIOS 名称与 `/etc/hosts` 中使用的名称或 DNS 定义的名称没有相同之处。NetBIOS 使用它自己的、完全独立的命名约定。但为了方便管理，仍建议您使用与 DNS 主机名对应的名称。Samba 默认采用这种方式。

## Samba 服务器

Samba 服务器是一种能够向客户机提供 SMB/CIFS 服务和 NetBIOS 基于 IP 命名服务的服务器。对 Linux，Samba 服务器有两个守护程序：用于 SMB/CIFS 服务的 `smnd` 和用于命名服务的 `nmbd`。

## Samba 客户机

Samba 客户机是一种能够通过 SMB 协议从 Samba 服务器使用 Samba 服务的系统。所有常见操作系统（Mac OS X、Windows 和 OS/2 等）都支持 SMB 协议。必须在所有计算机上安装 TCP/IP 协议。Samba 为多种不同的 UNIX 系统提供客户机。对于 Linux，有一个用于 SMB 的内核模块，它允许在 Linux 系统级别上集成 SMB 资源。不需要对 Samba 客户机运行任何守护程序。

## 共享

SMB 服务器通过共享为其客户机提供硬件空间。共享就是服务器上的打印机和目录及其子目录。可以通过名称来导出并访问共享。可以将共享名称设置为任何名称 — 它不一定是导出目录的名称。也可以为打印机指派一个名称。客户机可以根据打印机的名称来访问打印机。

# 37.2 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 37.3.1 节“使用 YaST 配置 Samba 服务器”[631]中所述的 YaST Samba 服务器配置的一部分。

要使用 YaST 停止或开始运行 Samba 服务，请使用系统 > 系统服务（运行级别）。从命令行，使用 `rcsmb stop && rcnmb stop` 停止 Samba 所需的服务，然后使用 `rcnmb start && rcsmb start` 启动它们。

## 37.3 配置 Samba 服务器

SUSE Linux Enterprise® 中的 Samba 服务器可通过两种不同方式配置：用 YaST 或手动方式。手动配置可提供更详细的信息，但没有 YaST GUI 方便。

### 37.3.1 使用 YaST 配置 Samba 服务器

要配置 Samba 服务器，请启动 YaST 并选择网络服务 > Samba 服务器。首次启动模块时，*Samba 服务器安装*对话框将打开以提示您选择几个基本选项来管理服务器，然后在配置结束时提示您输入 Samba root 用户密码。为了在稍后启动，*Samba 服务器配置*对话框将显示。

Samba 服务器安装对话框由两步组成：

工作组名或域名

在工作组名或域名中选择一个现有名称或输入一个新的名称，然后单击下一步。

Samba 服务器类型

在下一步中，指定服务器是否应该充当 PDC，然后单击下一步。

稍后，可以在 *Samba 服务器配置*对话框中使用标识选项卡来更改 Samba 服务器安装的所有设置。

### 使用 YaST 的高级 Samba 配置

首次启动 Samba 服务器模块时，*Samba 服务器配置*对话框紧接着*Samba 服务器安装*对话框显示。使用它调整您的 Samba 服务器配置。

编辑配置后，单击完成关闭配置。

## 启动服务器

在启动选项卡中，配置 Samba 服务器的启动。若想在每次系统引导时启动服务，请选择*引导时*。要激活手动启动，请选择*手动*。有关启动 Samba 服务器的更多信息，请参见第 37.2 节“启动和停止 Samba”[630]。

在此选项卡中，还可以打开防火墙中的端口。为此应选择*打开防火墙中的端口*。如果有多个网络接口，则请通过单击*防火墙细节*、选择接口并单击*确定*来为 Samba 服务选择网络接口。

## 共享

在共享选项卡中，确定要激活的 Samba 共享。存在一些预定义的共享，例如主页和打印机。使用*切换状态*可在*活动*和*不活动*之间进行切换。单击*添加*可添加新共享，单击*删除*可删除选中共享。

## 身份

在标识选项卡中，确定与主机关联的域（*基本设置*）以及是否在网络中使用备用主机名（*NetBIOS 主机名*）。要设置专家全局设置或设置用户认证（例如，LDAP），请单击*高级设置*。

## 来自其他域的用户

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*。

## 使用 LDAP

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 36 章 *LDAP - 目录服务* [599]。

## 37.3.2 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”）。

---

## 37.3.3 手动配置服务器

如果想将 Samba 用作服务器，请安装 `samba`。Samba 的主要配置文件是 `/etc/samba/smb.conf`。可以将此文件分为两个逻辑部分。`[global]` 部分包含中央和全局设置。`[share]` 部分包含各个文件和打印机共享。通过这种方式，可以在 `[global]` 部分中有区别地或全局地设置有关共享的详细设置，这样可以提高配置文件的结构透明性。

### global 部分

需要对 `[global]` 部分的以下参数进行调整以满足网络设置的要求，以便其他计算机能够在 Windows 环境中通过 SMB 访问 Samba 服务器。

`workgroup = TUX-NET`

此行将 Samba 服务器指派到工作组。将 TUX-NET 替换为您的网络环境的适当工作组。您的 Samba 服务器将出现在其 DNS 名称下，除非此名称已被指派给网络中的任何其他计算机。如果 DNS 名称不可用，请使用

`netbiosname=MYNAME` 设置服务器名称。有关此参数的详细信息，请参见 `mansmb.conf`。

`os level = 2`

此参数确定您的 Samba 服务器是否会尝试成为其工作组的 LMB（本地主浏览器）。为了避免现有 Windows 网络受到配置错误的 Samba 服务器的任何影响，应选择非常低的值。有关这一重要主题的详细信息，请参见文件 `BROWSING.txt` 和 `BROWSING-Config.txt`，它们位于包文档的 `textdocs` 子目录下。

如果网络中没有任何其他 SMB 服务器（如 Windows NT 或 2000 服务器），并且您希望 Samba 服务器保留一份本地环境中存在的所有系统的列表，请将 `os level` 设置为一个较高的值（例如 65）。然后便可以选择您的 Samba 服务器作为本地网络的 LMB。

在更改此设置时，应认真考虑这样做对现有 Windows 网络环境的影响。应该首先在一个孤立网络中或一天中的非重要时间测试这些更改。

#### wins support 和 wins server

为了将您的 Samba 服务器集成到具有活动 WINS 服务器的现有 Windows 网络中，应启用 `wins server` 选项并将其值设置为 WINS 服务器的 IP 地址。

如果将您的 Windows 计算机连接到单独的子网，同时又希望它们互相通讯，则需要设置一个 WINS 服务器。要将 Samba 服务器转变为这样的 WINS 服务器，请设置选项 `wins support = Yes`。确保网络中只有一个 Samba 服务器启用了此设置。切勿在您的 `smb.conf` 文件中同时启用选项 `wins server` 和 `wins support`。

## 共享

以下示例描述了如何使 CD-ROM 驱动器和用户目录 (`homes`) 对 SMB 客户机可用。

#### [cdrom]

为了避免意外地使 CD-ROM 驱动器变得可用，应使用注释标记（在本例中是分号）取消这些行。删除第一列中的分号，以便与 Samba 共享 CD-ROM 驱动器。

#### 例 37.1 CD-ROM 共享

```
[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

[cdrom] 和 comment

[cdrom] 项是网络上的所有 SMB 客户机均可看到的共享的名称。可以添加一个附加 `comment` 来进一步描述此共享。



```
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 37.2 主共享

```
[homes]
comment = Home Directories
valid users = %S
browseable = No
read only = No
create mask = 0640
directory mask = 0750
```

`[homes]`

只要没有其他共享使用连接到 SMB 服务器的用户的共享名称，就会使用 `[homes]` 共享指令动态生成一个共享。所生成的共享的名称就是用户名。

```
valid users = %S
```

一旦成功建立连接，就会使用共享的具体名称替换 `%S`。对于 `[homes]` 共享，用户名始终是 `%S`。这样就可以将对用户的共享的访问权限严格限制在此用户。

```
browseable = No
```

此设置使共享在网络环境中不可见。

```
read only = No
```

默认情况下，Samba 通过 `read only = Yes` 参数来禁止对任何已导出共享的写访问。要使共享可写，请设置值 `read only = No`，它与 `writable = Yes` 是等效的。

```
create mask = 0640
```

那些不是基于 MS Windows NT 的系统不能理解 UNIX 权限的概念，所以它们在创建文件时不能指派权限。参数 `create mask` 定义了为新创建文件指派的访问权限。这仅适用于可写共享。事实上，此设置意味着拥有者具有读写权限，且拥有者的主组的成员具有读权限。`valid users = %S` 禁止读访问，即使该组具有读权限。要使该组能够进行读或写访问，应取消 `valid users = %S` 一行。

## 安全性级别

要提高安全性，可以使用密码来保护每个共享访问。SMB 提供了 3 种可能的方式来检查权限：

共享级安全性 (`security = share`)

严格地为一个共享指派一个密码。任何知道此密码的用户都可以访问此共享。

用户级安全性 (`security = user`)

这里将用户的概念引入了 SMB。每个用户都必须使用自己的密码在服务器上注册。注册后，服务器可以根据用户名来授予访问各个已导出共享的权限。

服务器级安全性 (`security = server`):

从客户机来看，Samba 好像是在用户级别方式下工作。但它实际将所有密码查询传递到另一个用户级别方式下的服务器来执行身份验证。此设置需要一个附加参数 (`password server`)。

共享、用户和服务器级安全性的选择适用于整个服务器。无法既为服务器配置的某些共享提供共享级安全性，同时又为其他共享提供用户级安全性。但是，您可以为系统上每个已配置的 IP 地址运行单独的 Samba 服务器。

有关此主题的详细信息，请参见 Samba HOWTO 文档集。对于一个系统上的多个服务器，应注意选项 `interfaces` 和 `bind interfaces only`。

## 37.4 配置客户机

客户机只能通过 TCP/IP 访问 Samba 服务器。NetBEUI 和通过 IPX 的 NetBIOS 不能与 Samba 共用。

## 37.4.1 使用 YaST 配置 Samba 客户机

配置 Samba 客户机来访问 Samba 服务器上的资源（文件或打印机）。在 *网络服务 > Windows 域成员资格* 对话框中输入域或工作组。单击浏览来显示所有可用的组和域，然后可以用鼠标来选择它们。如果激活将 *SMB 信息也用于 Linux 身份验证*，则用户身份验证将在 Samba 服务器上运行。在完成所有设置后，单击完成完成配置。

## 37.4.2 Windows 9x 和 ME

Windows 9x 和 ME 都内置了对 TCP/IP 的支持。但默认情况下并不安装此支持。要添加 TCP/IP，请转到 *控制面板 > 系统*，然后选择 *添加 > 协议 > Microsoft 的 TCP/IP*。重引导您的 Windows 计算机后，双击网络环境的桌面图标便可以找到 Samba 服务器。

---

### 提示

要使用 Samba 服务器上的打印机，请安装对应 Windows 版本的标准或 Apple-PostScript 打印机驱动程序。最好将其链接到 Linux 打印机队列，它接受 Postscript 作为一种输入格式。

---

## 37.5 将 Samba 用作登录服务器

在主要由 Windows 客户机组成的网络中，使用户只能使用有效帐户和密码进行注册通常是最好的选择。在基于 Windows 的网络中，此任务由主域控制器 (PDC) 来处理。您可以使用配置为 PDC 的 Windows NT 服务器，但是此任务也可以借助 Samba 服务器来完成。中显示了必须在 smb.conf 的 [global] 部分设置的项。[例 37.3 “smb.conf 中的 global 部分”](#) [637]

### 例 37.3 smb.conf 中的 global 部分

```
[global]
workgroup = TUX-NET
domain logons = Yes
domain master = Yes
```

如果将已加密密码用于校验目的（这是保持完好的 MS Windows 9X 安装、MS Windows NT 4.0 service pack 3 和所有以后版本产品的默认设置），则 Samba 服务器必须能够处理它们。[global] 部分中的 encrypt passwords = yes 项启用了此功能（对于 Samba 版本 3，这是默认设置）。此外，还需要以适合 Windows 的加密格式来准备用户帐户和密码。使用命令 `smbpasswd -a name` 可完成此任务。使用以下命令为计算机创建 Windows NT 域概念要求的域帐户：

#### 例 37.4 设置计算机帐户

```
useradd hostname\$\n  
smbpasswd -a -m hostname
```

使用 `useradd` 命令可添加一个美元符号。命令 `smbpasswd` 在使用参数 `-m` 时自动插入此符号。带注释的配置示例 (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) 包含自动执行此任务的设置。

#### 例 37.5 计算机帐户的自动设置

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \n  
-s /bin/false %m\$\n
```

为了确保 Samba 可以正确执行此脚本，应选择具有所需管理员权限的 Samba 用户。为此，请选择一个用户并将其添加到 `ntadmin` 组。然后可以使用以下命令来为属于此 Linux 组的所有用户指派 Domain Admin 状态：

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

有关此主题的详细信息，请参见位于 `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf` 的 Samba HOWTO 文档集的第 12 章。

## 37.6 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。中介绍了安装期间的域连接。[第 3.14.7 节“用户数”](#) [39]

要在运行系统中连接 AD 域，请按如下所示继续：

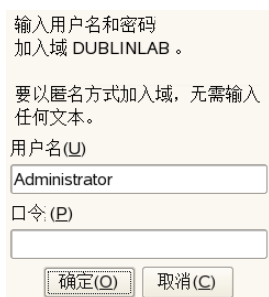
- 1 以 root 身份登录并启动 YaST。
- 2 启动网络服务 > Windows 域成员资格。
- 3 在 Windows 域成员资格屏幕上的域或工作组中输入要加入的域。或者，使用浏览获得所有可用域的列表并选择一个。

图 37.1 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 单击完成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。

图 37.2 提供管理员身份凭证



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。

## 37.7 将 Windows NT Server 迁移到 Samba

除了 Samba 和 LDAP 配置，Windows NT 服务器迁移到 SUSE Linux Enterprise Server Samba 服务器有两个基本的步骤。首先迁移概要文件，然后迁移帐户。

### 37.7.1 准备 LDAP 服务器

迁移的第一步应该是配置 LDAP 服务器。您需要添加具有密码的软件客户机帐户的基本 DN 信息和条目。有关 LDAP 配置的详细信息，请参见第 36 章 *LDAP - 目录服务* [599]。

不需要手动配置它。您可以使用 `smbldap` 工具的脚本。这些脚本是包 `samba-doc` 的一部分，并且安装该包之后，可以在 `/usr/share/doc/packages/samba/examples/LDAP` 找到它。

---

#### 注意：LDAP 和安全性

LDAP 管理 DN 应该是帐户而不是 Root DN。要使网络更加安全，您还可以使用具有 TLS 的安全连接。

---

## 37.7.2 准备 Samba 服务器

开始迁移之前，请配置 Samba 服务器。在 YaST *Samba* 服务器模块的共享选项卡中查找 `profile`、`netlogon` 和 `home` 共享的配置。要设置默认值，选择共享并单击 *编辑*。

要添加 Samba 服务器的 LDAP 配置和 LDAP 管理员的身份凭证，使用 YaST *Samba* 服务器模块的 *LDAP* 设置选项卡。LDAP 管理 DN（标签是 *管理 DN*）和密码是添加或修改储存在 LDAP 目录中的帐户所必需的。

## 37.7.3 迁移 Windows 概要文件

对于每个要迁移的概要文件，完成以下步骤：

### 过程 37.1 迁移概要文件

- 1 在 NT4 域控制器上，右键单击 *我的计算机*，然后选择 *属性*。选择 *用户概要文件* 选项卡。
- 2 选择您要迁移的用户概要文件并单击它。
- 3 单击 *复制到*。
- 4 在 *复制概要文件* 中，添加新路径，例如，`c:\temp\profiles`。
- 5 在 *允许* 中单击 *更改*。
- 6 单击 *每个人*。要关闭该框，单击 *确定*。
- 7 要保存该概要文件，单击 *确定*。
- 8 将保存的概要文件复制到 Samba 服务器上相应的概要文件目录。

## 37.7.4 迁移 Windows 帐户

### 过程 37.2 帐户迁移过程

- 1 使用 NT 服务器管理器在 Samba 服务器的老的 NT4 域中创建 BDC 帐户。  
Samba 必须不在运行。

```
net rpc join -S NT4PDC -w DOMNAME -U Administrator%passwd net rpc  
vampire  
-S NT4PDC -U administrator%passwd pdbedit -L
```

- 2 将每个 UNIX 组分配到 NT 组：

### 例 37.6 示例脚本 *initGroups.sh*

```
#!/bin/bash ##### Keep this as a shell script for future re-use #  
Known domain global groups net groupmap modify ntgroup="Domain  
Admins"  
unixgroup=root net groupmap modify ntgroup="Domain Users"  
unixgroup=users net groupmap modify ntgroup="Domain Guests"  
unixgroup=nobody # Our domain global groups net groupmap add  
ntgroup="Operation" unixgroup=operation type=d net groupmap add  
ntgroup="Shipping" unixgroup=shipping type=d
```

- 3 检查是否能够识别所有组：

```
net groupmap list
```

## 37.8 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。可以在 `examples` 子目录中找到带注释的示例配置 (`smb.conf.SuSE`)。



Samba 开发小组提供的 Samba HOWTO 文档集中有一节专门介绍查错。此外，文档的第 V 部分提供了检查配置的逐步指南。安装包 `samba-doc` 后，可在 `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf` 中找到 Samba HOWTO 集。

有关 LDAP 和从 Windows NT 或 2000 迁移的详细信息，请参见 `/usr/share/doc/packages/samba/examples/LDAP/smbldap-tools-*/doc`，其中 \* 是您的 `smbldap` 工具版本。



## 通过 NFS 共享文件系统

在企业环境中通过网络分发和共享文件系统是一项常见任务。NFS 是经过充分证实的系统，还可以与黄页协议 NIS 系统协同使用。要使用可以与 LDAP 协同使用、并且 Kerberos 化的更安全的协议，请选中 NFSv4。

NFS 与 NIS 一起使用以使网络在面向用户时是透明的。利用 NFS，可以通过网络分发任意文件系统。进行适当的设置后，用户将发现自己始终处于同一环境中，而与其当前使用的终端无关。

与 NIS 一样，NFS 也是一个客户机/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）。

---

### 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，您应使用一个有效的 DNS 系统。至少为了日志记录目的也应使用此系统，因为 `mountd` 守护程序执行反向查找。

---

## 38.1 安装所需软件

要将主机配置为 NFS 客户机，无需安装其他软件。配置 NFS 客户机所需的所有包都将默认安装。

NFS 服务器软件不会默认安装。要安装 NFS 服务器软件，请启动 YaST 并选择 **软件 > 软件管理**。立即选择 **过滤器 > 模式** 并选择 **其他服务器** 或使用 **搜索选项** 搜索 NFS 服务器。确认包的安装以完成安装进程。

## 38.2 使用 YaST 导入文件系统

经过授权的用户都可以将 NFS 服务器中的 NFS 目录装入自己的文件目录树。使用 YaST 的 NFS 客户程序模块可以完成上述操作。只需输入 NFS 服务器的主机名、要导入的目录以及要在本地的哪个装入点装入此目录。在第一个对话框中单击 **添加** 后，这些更改即会生效。单击 **打开防火墙中的端口** 打开防火墙，以便访问远程计算机上的服务。防火墙状态将显示在复选框旁边。单击 **完成** 保存更改。请参见图 38.1 “使用 YaST 配置 NFS 客户机” [646]。

配置写入 `/etc/fstab`，并将装入指定的文件系统。当您稍后启动 YaST 配置客户程序时，它还将读取此文件中的现有配置。

当前只能手动导入 NFSv4 文件系统。这在第 38.3 节 “手动导入文件系统” [647] 中有说明。

图 38.1 使用 YaST 配置 NFS 客户机



## 38.3 手动导入文件系统

还可以从 NFS 服务器手动导入文件系统。前提条件是要运行 RPC 端口映射器，以 root 身份输入 `rcportmapstart` 即可启动它。一旦满足了这个前提条件，通过以下方式使用 `mount` 命令，可以在文件系统中象装入本地硬盘那样装入远程导出的文件系统。

```
mount host:remote-path local-path
```

如果应该导入某台计算机（如 `sun`）上的用户目录，请使用以下命令：

```
mount sun:/home /home
```

### 38.3.1 导入 NFSv4 文件系统

必须在客户机上运行 `idmapd` 服务才能执行 NFSv4 导入。用 `rcidmapd start` 从命令提示符处启动 `idmapd` 服务。使用 `rcidmapd status` 检查 `idmapd` 的状态。

`idmapd` 服务将其参数储存在 `/etc/idmapd.conf` 文件中。将 `Domain` 参数的值保留为 `localdomain`。确保为 NFS 客户机和 NFS 服务器指定的值相同。

通过从 shell 提示符输入命令来执行 NFSv4 导入。要导入 NFSv4 远程文件系统，请使用以下命令：

```
mount -t nfs4 host:/ local-path
```

将 `host` 替换为主管一个或多个 NFSv4 导出的 NFS 服务器，并将 `local-path` 替换为装入的客户机中的目录位置。例如，要将用 `sun` 上的 NFSv4 导出的 `/home` 导入到 `/local/home`，请使用以下命令：

```
mount -t nfs4 sun:/ /local/home
```

服务器名称和冒号后跟的远程文件系统路径是“/”。这与为 v3 导入指定的方式不同，执行 v3 导入时要提供远程文件系统的确切路径。此概念称为伪文件系统，这在第 38.4.1 节“为 NFSv4 客户机导出”[650]中有说明。

## 38.3.2 使用自动装入服务

除了装入通常的本地设备，autofs守护程序还可以用于自动安装远程文件系统。要执行此操作，请在 `/etc/auto.master` 文件中添加以下条目：

```
/nfsmounts /etc/auto.nfs
```

如果 `auto.nfs` 文件正确完成，`/nfsmounts` 目录将作为客户机上所有 NFS 装入的 `root` 目录。文件名为 `auto.nfs` 是为了方便，也可以选择其他名称。在选定的文件（如果没有的话，就创建一个）中，如以下示例所示，添加所有 NFS 装入的条目：

```
localdata -fstype=nfs server1:/data  
nfs4mount -fstype=nfs4 server2:/
```

用 `rcautofs start` 激活设置。对于此示例，`/nfsmounts/localdata`，`server1` 的 `/data` 目录将通过 NFS 装入，`server2` 的 `/nfsmounts/nfs4mount` 将通过 NFSv4 装入。

如果在运行 `autofs` 服务时编辑 `/etc/auto.master` 文件，则必须重新启动自动装入程序才能使更改生效。请用 `rcautofs restart` 执行此操作。

## 38.3.3 手动编辑 `/etc/fstab`

通常，`/etc/fstab` 中的 NFS 装入条目如下：

```
host:/data /local/path nfs rw,noauto 0 0
```

也可以手动将 NFSv4 装入添加到 `/etc/fstab` 文件中。对于这些装入，请在第三列中使用 `nfs4` 而不是 `nfs`，并确保在第一列中的 `host:` 后面用 `/` 指定远程文件系统。在 `/etc/fstab` 中保存该信息的优点是可以缩短装入命令，只提供本地装入点，例如：

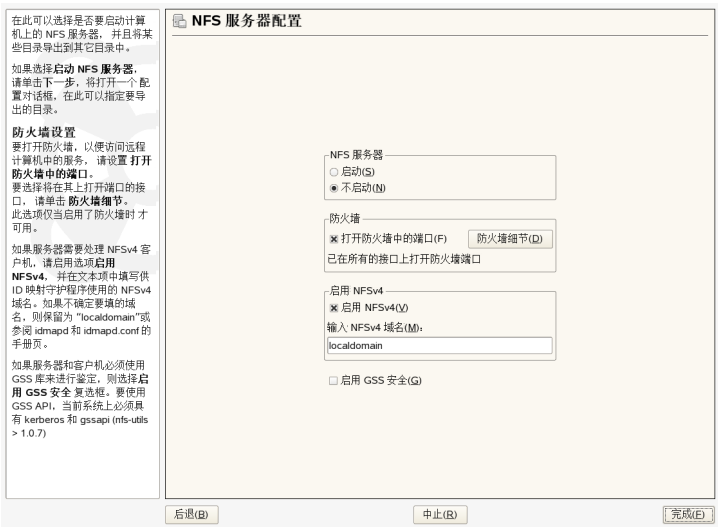
```
mount /local/path
```

## 38.4 使用 YaST 导出文件系统

使用 YaST 将网络中的某台主机转换为 NFS 服务器，即将目录和文件导出到所有有权访问它的主机的服务器。这样做可以为同一工作组中的所有成员提供应用程序，而不必在每台主机的本地都安装应用程序。要安装此类服务器，请启

动 YaST 并选择网络服务 > NFS 服务器。打开一个如图 38.2 “NFS 服务器配置工具” [649] 中所示的对话框。

图 38.2 NFS 服务器配置工具

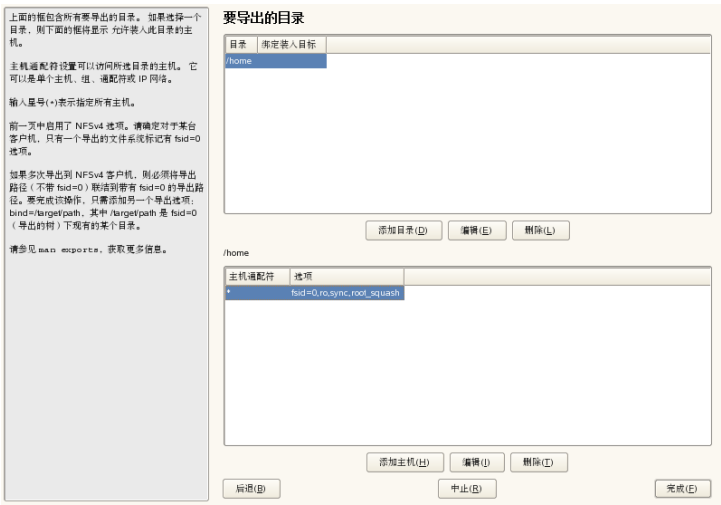


接着，激活启动 NFS 服务器并输入 NFSv4 域名。

如果您需要安全访问服务器，请单击启用 GSS 安全性。前提条件是您的域中安装了 Kerberos 并且服务器和客户机都已采用 Kerberos 系统。单击下一步。

在上面的文本字段中，输入要导出的目录。在下面输入应能访问这些目录的主机。图 38.3 “使用 YaST 配置 NFS 服务器” [650] 中显示了此对话框。该图显示了在先前对话框中启用 NFSv4 的场景。绑定装入目标显示在右边的窗格中。关于更多的细节，请参考左边窗格中显示的帮助。在对话框的下半部分，有四个可以为每个主机设置的选项：单主机、网络组、通配符和 IP 网络。关于这些选项的详细说明，请参见导出手册页。单击完成以完成配置。

图 38.3 使用 YaST 配置 NFS 服务器



重要：自动配置防火墙

如果系统启用了防火墙 (SuSEfirewall2)，在选择打开防火墙中的端口后，YaST 会通过启用 `nfs` 服务使防火墙的配置适应 NFS 服务器。

38.4.1 为 NFSv4 客户机导出

激活启用 NFSv4 支持 NFSv4 客户机。用 NFSv3 的客户机仍可访问服务器已导出的目录，如果它们已适当导出的话。这在第 38.4.3 节“并存的 v3 和 v4 导出”[653]中有描述。

激活 NFSv4 之后，请输入适当的域名。请确保输入访问此特定服务器的任何 NFSv4 客户机的 `/etc/idmapd.conf` 文件中存在的相同名称。此参数用于（服务器和客户机上）NFSv4 支持所需的 `idmapd` 服务。如果没有特殊要求，请将它保留为 `localdomain`（默认值）。有关详细信息，参见第 38.7 节“更多信息”[656]。

单击下一步。接下来的对话框有两部分。上半部分包含两列，名为目录和绑定装入目标。目录是直接可编辑的列，它列出了要导出的目录。



对于固定的客户机集合，有两类目录可以导出：作为伪 root 文件系统的目录；绑定到伪文件系统的某个子目录的目录。此伪文件系统作为基本点，为相同客户机导出的所有文件系统在其次下各就各位。对于一个或一组客户机，服务器上只有一个目录可以配置为伪根目录以供导出。对于这个客户机，通过将它们绑定为伪根目录中现有的子目录可以导出多个目录。

图 38.4 用 NFSv4 导出目录



在对话框的下半部分，输入特定目录的客户程序（通配符）和导出选项。在上半部分添加目录后，用于输入客户机和选项信息的另一个对话框会自动弹出。然后，单击添加主机添加新客户机（客户机集）。

在打开的小对话框中，输入主机通配符。可以为每个主机设置四类主机通配符：单主机（名称或 IP 地址）、网络组、通配符（如 \* 表示所有计算机都能访问服务器）和 IP 网络。然后，在选项中，将 fsid=0 包含在逗号分隔的选项列表中，以将目录配置为伪 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用 bind=/target/path 提供目标绑定路径。

例如，假定选择目录 /exports 作为能访问服务器的所有客户机的伪 root 目录。然后将这添加到上半部分并确保为此目录输入的选项包含 fsid=0。如果另一个目录 /data 也需要用 NFSv4 导出，请将此目录添加到上半部分。为此输入选项时，请确保 bind=/exports/data 在列表中，并且 /exports/data

已经是 `/exports` 的现有子目录。选项 `bind=/target/path` 中的任何更改（添加、删除或更改值）都会反映在绑定装入目标中。此列不是可以直接编辑的列，它总结了目录及其属性。信息完成后，请单击完成来完成配置或单击启动来重新启动服务。

## 38.4.2 NFSv3 和 NFSv2 导出

请确保未在初始对话框中选中启用 *NFSv4*，然后单击下一步。

下一个对话框包含两部分。在上面的文本字段中，输入要导出的目录。在下面输入应能访问这些目录的主机。可以为每个主机设置四类主机通配符：单主机（名称或 IP 地址）、网络组、通配符（如 \* 表示所有计算机都能访问服务器）和 IP 网络。

**图 38.4 “用 NFSv4 导出目录”** [651] 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 38.5** 用 NFSv2 和 v3 导出目录

上面的框包含所有要导出的目录。如果选择一个目录，则下面的框将显示允许装入此目录的主机。

**主机通配符** 设置可以访问所选目录的主机。它可以是单个主机、组、通配符或 IP 网络。

输入星号(\*)表示指定所有主机。

请参见 `man exports`，获取更多信息。

要导出的目录

目录

exports

添加目录(D) 编辑(E) 删除(L)

exports

主机通配符	选项
192.168.1.2	fsid=0,rw,sync

添加主机(H) 编辑(E) 删除(D)

后退(B) 中止(R) 完成(F)

## 38.4.3 并存的 v3 和 v4 导出

NFSv3 和 NFSv4 导出可以在一个服务器上并存。在初始的配置对话框中启用了 NFSv4 之后，选项列表中不包含 `fsid=0` 和 `bind=/target/path` 的导出将作为 v3 导出处理。考虑图 38.4 “用 NFSv4 导出目录” [651] 中的示例。如果添加另一个目录（如 `/data2`），然后在相应的选项列表中使用添加目录不会提供 `fsid=0` 或 `bind=/target/path`，此导出将作为 v3 导出。

---

### 重要

自动配置防火墙

如果系统启用了 `SuSEfirewall2`，在选择了打开防火墙中的端口后，YaST 会通过启用该服务使防火墙的配置适应 NFS 服务器。

---

## 38.5 手动导出文件系统

NFS 导出服务的配置文件是 `/etc/exports` 和 `/etc/sysconfig/nfs`。除了这些文件之外，NFSv4 服务器配置还需要 `/etc/idmapd.conf`。要启动或重新启动服务，请运行命令 `rcnfsserver restart` 和 `rcidmapd restart`。NFS 服务器依赖于运行的 RPC 端口映射器。所以，还请使用 `rcportmap restart` 启动或重新启动端口映射器。

### 38.5.1 用 NFSv4 导出文件系统

NFSv4 是 SUSE Linux Enterprise 10 上可用的 NFS 协议的最新版本。用 NFSv4 配置导出目录的过程与先前的版本略有不同。

#### `/etc/exports` 文件

此文件包含条目列表。每个条目表示共享的目录以及共享的方式。`/etc/exports` 中的条目通常包含：

```
/shared/directory host(option_list)
```

例如：

```
/export 192.168.1.2(rw,fsid=0,sync)
/data 192.168.1.2(rw,bind=/export/data,sync)
```

在选项列表中指定了 `fsid=0` 的目录称为伪根文件系统。此处使用了 IP 地址 **192.168.1.2**。您可以使用主机名、表示一组主机的通配符（`*.abc.com`、`*` 等）或网络组。

对于一组固定的客户机，NFSv4 可导出两种目录：

- 选择作为伪根文件系统的单一目录。在此例中，`/exports` 是伪根目录，因为在此条目的选项列表中指定了 `fsid=0`。
- 选定与伪文件系统的某些现有子目录绑定的目录。在上述条目示例中，`/data` 就是与伪文件系统 `/export` 的现有子目录（`/export/data`）绑定的目录。

伪文件系统是顶级目录，在其下，需要用 NFSv4 导出的所有文件系统都各就各位。对于一个或一组客户机，在服务器上只能配置一个目录作为导出的伪根目录。对于这个或这组客户机，可通过将其他多个目录绑定到伪根目录的某个现有子目录进行导出。

## **/etc/sysconfig/nfs**

此文件包含几个决定 NFSv4 服务器守护程序行为的参数。重要的是，参数 `NFSv4_SUPPORT` 必须设置为 `yes`。此参数决定了 NFS 服务器是否支持 NFSv4 导出和客户机。

## **/etc/idmapd.conf**

Linux 计算机上的每个用户都有一个名称和 ID。`idmapd` 针对服务器的 NFSv4 请求执行名称到 ID 的映射并答复客户机。这必须同时在服务器和客户机上针对 NFSv4 运行，因为 NFSv4 在其通讯中仅使用名称。

对于可能正在使用 NFS 共享文件系统的计算机，请确保在这些计算机间为用户指定用户名和 ID (`uid`) 的方式一致。这可以使用 NIS、LDAP 或域中的任何统一的域身份验证机制来实现。

要实现正确的功能，必须为客户机和服务器设置相同的参数 `Domain`。如果您不确定，请在服务器和客户机文件中将域保留为 `localdomain`。配置文件样本如下：

```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

除非确定您在执行正确操作，否则请勿更改这些参数。关于更多参考，请阅读 `idmapd` 和 `idmapd.conf` 的手册页：`man idmapd`、`man idmapd.conf`。

## 启动和停止服务

更改 `/etc/exports` 或 `/etc/sysconfig/nfs` 后，通过 `rcnfsserver restart` 启动或重新启动 NFS 服务器服务。更改 `/etc/idmapd.conf` 后，请用 `rcidmapd restart` 启动或重新启动 `idmapd` 服务。请确保两个服务都在运行。

## 38.5.2 用 NFSv2 和 NFSv3 导出文件系统

这特定于 NFSv3 和 NFSv2 导出。请参见第 38.5.1 节“用 NFSv4 导出文件系统”[653]了解用 NFSv4 导出。

用 NFS 导出文件系统涉及两个配置文件：`/etc/exports` 和 `/etc/sysconfig/nfs`。通常，`/etc/exports` 文件条目的格式如下：

```
/shared/directory host(list_of_options)
```

例如：

```
/export 192.168.1.2(rw,sync)
```

其中，目录 `/export` 是与选项列表为 `rw,sync` 的主机 `192.168.1.2` 共享的。该 IP 地址可使用通配符（如 `*.abc.com`）甚至网络组替换为一个或一组客户机名称。

关于所有选项及其含义的详细说明，请参见 `exports` (`man exports`) 的手册页。

更改 `/etc/exports` 或 `/etc/sysconfig/nfs` 后，请用命令 `rcnfsserver restart` 启动或重新启动 NFS 服务器。

## 38.6 采用 Kerberos 的 NFS

要对 NFS 使用 Kerberos 身份验证，必须启用 GSS 安全性。要执行此操作，请在初始 YaST 对话框中选择启用 GSS 安全性。另外，完成下列步骤：

- 请确保服务器和客户机都在同一 Kerberos 域中。这意味着它们访问相同的 KDC（密钥分发中心）服务器并共享其 `krb5.keytab` 文件（在任何计算机上的默认位置是 `/etc/krb5.keytab`）。
- 在客户机上用 `rcgssd start` 启动 `gssd` 服务。
- 在客户机上用 `rcsvcgssd start` 启动 `svcgssd` 服务。

关于配置采用 Kerberos 的 NFS 的更多信息，请参见第 38.7 节“更多信息”[656] 中的链接。

## 38.7 更多信息

除了 `exports`、`nfs` 和 `mount` 的手册页外，还可在 `/usr/share/doc/packages/nfs-tls/README` 和以下 Web 文档中找到关于配置 NFS 服务器和客户机的信息：

在 SourceForge [<http://nfs.sourceforge.net/>] 上联机查找详细的技术文档。

关于设置采用 Kerberos 的 NFS 的说明，请参见 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，请参见 Linux NFSv4 Frequently Asked Questions [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>] 常见问题解答。

## 文件同步

现今有很多人都在同时使用多台计算机 — 一台在家用，一台或多台在办公室用，还可能携带便携式计算机或 PDA 在路上用。很多文件是所有这些计算机上共同需要的。所以，您可能希望能在所有计算机上工作，修改文件，让所有计算机都能提供最新的数据。

### 39.1 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。

## 39.1.1 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。这些更改将被合并，若发生在同一行上，则会报告冲突。发生冲突时，数据库仍保持一致状态。冲突仅显示在客户机上并在客户机上解决。

## 39.1.2 rsync

在无需版本控制但需要通过慢速网络连接同步大型目录结构时，rsync 工具可以提供较为完善的机制，仅传送文件中的更改。其中不仅涉及文本文件，还包括二进制文件。为检测文件间的差异，rsync 会将文件划分为多个块，并计算各个块的校验和。

检测更改需要消耗一定的资源。要使用 rsync，准备同步的系统应能够伸缩自如。RAM 尤为关键。

# 39.2 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。

## 39.2.1 客户机/服务器与对等模式

在分发数据时，常用的有两个模型。在第一个模型中，所有客户机都通过中央服务器来同步文件。所有客户机都应能够访问该服务器（至少能偶尔为之）。CVS 使用该模型。

另一个模型是让所有联网主机作为同级相互同步数据。rsync 实际在客户机模式下工作，但任何客户机都可用作服务器。



## 39.2.2 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。

## 39.2.3 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。

## 39.2.4 冲突：事件和解决方案

在 CVS 中很少发生冲突，即便是多人同时在一个大型程序项目上协作时也不例外。这是因为合并文档时基于的是单个行。发生冲突时，只有一个客户机会受影响。通常很容易解决 CVS 中发生的冲突。

rsync 中不提供冲突解决功能。用户自己要避免意外覆盖文件，并手动解决所有可能的冲突。为安全起见，还可以使用 RCS 之类的版本控制系统。

## 39.2.5 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。

## 39.2.6 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。

## 39.2.7 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。

## 39.2.8 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。

## 39.2.9 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。

## 39.2.10 预防攻击

在传送数据的过程中，最好防止数据被拦截或操纵。CVS和rsync可以方便地通过ssh（安全shell）使用，从而防止遭受此类攻击。应避免通过rsh（远程shell）运行CVS。也不建议在不安全的网络中使用*pserver*机制访问CVS。

## 39.2.11 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 39.1** 文件同步工具的功能：-- = 很差，- = 差或不可用，o = 中等，+ = 好，++ = 很棒，x = 可用

	CVS	rsync
客户机/服务器	客户机-服务器	客户机-服务器

	CVS	rsync
可移植性	Lin、Un*x、Win	Lin、Un*x、Win
交互能力	x	x
速度	o	+
冲突	++	o
文件选择	所选/文件、目录	目录
历史	x	-
硬盘空间	--	o
GUI	o	-
难易程度	o	+
攻击	+(ssh)	+(ssh)
数据丢失	++	+

## 39.3 CVS 简介

如果经常编辑各个文件并且这些文件以 ASCII 文本或程序源代码文本之类的格式储存，则应该使用 CVS 来进行同步。用 CVS 同步其他格式的数据（如 JPEG 文件）固然可行，但这会产生大量数据，因为文件的所有变化都永久储存在 CVS 服务器中。这种情况下将无法利用 CVS 的大多数功能。只有在所有工作站都可以访问同一服务器时，才能使用 CVS 同步文件。

## 39.3.1 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机上都安装了 CVS 软件，则必须在客户端设置以下环境变量：

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

可使用命令 `cvsinit` 从客户端初始化 CVS 服务器。只需执行一次初始化。

最后，必须给同步指派名称。仅在客户机上选择或创建目录，以包含要使用 CVS 来管理的文件（该目录也可以为空）。目录的名称同时也是同步的名称。在本例中，目录名为 `synchome`。转到此目录并输入以下命令，将同步名称设置为 `synchome`：

```
cvs import synchome tux wilber
```

许多 CVS 命令都需要注释。为此，CVS 会启动一个编辑器（在环境变量 `$EDITOR` 中定义的编辑器；如果未定义任何编辑器，则使用 `vi`）。通过提前在命令行中输入注释（如下例所示），可以避免调用编辑器。

```
cvs import -m 'this is a test' synchome tux wilber
```

## 39.3.2 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。该操作将在客户机上创建新的子目录 `synchome`。要向服务器提交更改，请转到目录 `synchome`（或其子目录之一），然后输入 `cvscommit`。

默认情况下，所有文件（包括子目录）都要提交给服务器。若仅提交单个文件或目录，请按 `cvscommit file1 directory1` 中的方式进行指定。在将新文件和目录提交给服务器之前，必须使用 `cvsadd file1 directory1` 之类的命令先将其添加到安装源中。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。

## 39.3.3 有关详细信息

本节仅对 CVS 的多种情况进行了简要介绍。以下 URL 提供了大量的文档：

- CVS: <http://www.cvshome.org>
- Rsync: <http://www.gnu.org/manual>

## 39.4 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。

### 39.4.1 配置和操作

rsync 有两种操作方式。可用于存档或复制数据。要执行上述操作，目标系统上只需要有远程 shell，如 ssh。不过，rsync 也可用作守护程序，为网络提供目录。

rsync 的基本操作方式不需要任何特殊配置。rsync 能直接将完整目录镜像到其他系统中。举例来说，以下命令在名为 sun 的备份服务器上为 tux 的主目录创建了备份副本。

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

以下命令用于回放该目录：

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

到目前为止，该程序的操作方式与普通的复制工具 (如 scp) 的操作方式相差无几。

应该以“rsync”方式操作 rsync，以便充分利用其所有功能。这需要在其中一个系统上启动 rsyncd 守护程序。在文件 /etc/rsyncd.conf 中配置该守护程序。例如，要使目录 /srv/ftp 可用于 rsync，请使用以下配置：

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
    path = /srv/ftp
    comment = An Example
```

然后使用 rcrsyncdstart 启动 rsyncd。rsyncd 也可以在引导进程中自动启动。通过在 YaST 提供的运行级别编辑器中激活此服务或通过手动输入命令 insservrsyncd，都可以完成上述设置。也可以使用 xinetd 来启动 rsyncd。不过，建议只在很少使用 rsyncd 的服务器上采用这种启动方式。

下例还创建了一个列出所有连接的日志文件。此文件储存在 /var/log/rsyncd.log 中。

随后可以从客户机系统测试传送。请使用以下命令完成该操作：

```
rsync -avz sun::FTP
```

此命令列出服务器的 /srv/ftp 目录中现有的所有文件。此请求还记录在日志文件 /var/log/rsyncd.log 中。要启动实际的传送，请提供目标目录。使用 . 表示当前目录。例如：

```
rsync -avz sun::FTP .
```

默认情况下，使用 rsync 同步时不会删除任何文件。如果应强制删除，必须明确指定附加选项 --delete。为保证不删除任何较新的文件，可转而使用选项 --update。必须手动解决所有冲突。

## 39.4.2 有关详细信息

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。

如果要用 Subversion 或其他工具，请下载 SDK。请参见 [http://developer.novell.com/wiki/index.php/SUSE\\_LINUX\\_SDK](http://developer.novell.com/wiki/index.php/SUSE_LINUX_SDK)。



# 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 70%, 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。

## 40.1 快速入门

借助本节, 快速设置并启动 Apache。时间. 您必须是 `root` 才能安装和配置 Apache。

### 40.1.1 要求

在设置 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 30 章 **基本联网知识** [495]。

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 32 章 [使用 NTP 同步时间](#) [549] 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. 默认的 Web 服务器端口（端口 80）将在防火墙中打开。为此，配置 SUSEFirewall2 以允许服务 HTTP 服务器处于外部时区中。此操作可通过 YaST 来完成。细节请参见第 43.4.1 节 [“使用 YaST 配置防火墙”](#) [742]。

## 40.1.2 安装

在默认情况下，在 SUSE Linux Enterprise Server 上不安装 Apache。要安装它，请启动 YaST 并选择软件 > 软件管理。现在选择过滤器 > 模式，然后选择主要功能下的 Web 和 LAMP 服务器。确认安装相关的包来完成安装进程。

可使用“现成可用”的标准预定义配置来安装 Apache。安装包括多重处理模块 `apache2-prefork` 以及 PHP5 模块。有关模块的详细信息，请参见第 40.4 节 [“安装、激活和配置模块”](#) [683]。

## 40.1.3 开始

要启动 Apache 并确保它能在引导期间自动启动，请启动 YaST 并选择系统 > 系统服务（运行级别）。搜索 `apache2` 并启用该服务。Web 服务器将立即启动。单击完成保存更改后，可将系统配置为在引导期间通过运行级别 3 和 5 来自动启动 Apache。有关 SUSE Linux Enterprise Server 运行级别的详细信息和 YaST 运行级别编辑器的说明，请参见第 20.2.3 节 [“使用 YaST 配置系统服务（运行级别）”](#) [365]。

要使用壳层启动 Apache，请运行 `rcapache2 start`。为了确保 Apache 在引导期间以运行级别 3 和 5 自动启动，请使用 `chkconfig -a apache2`。

如果在启动 Apache 时未接收到错误消息，则 Web 服务器现在应该已在运行。启动浏览器，然后打开 <http://localhost/>。应该可以看到一个 Apache 测试页面以以下内容开始：“如果您可以看到此消息，说明 Apache Web 服务器软件已成功安装在此系统上。”如果看不到此页面，请参见第 40.8 节 [“查错”](#) [699]。

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。

## 40.2 配置 Apache

可用两种不同的方法配置 SUSE Linux Enterprise Server 中的 Apache：通过 YaST 或手动配置。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

对 Apache 的大多数配置值的更改仅在重新启动或重新装载 Apache 之后生效。当使用 YaST 并通过对 *HTTP* 服务选择 *已启用* 完成配置后，上述操作会自动发生。第 40.3 节“启动和停止 Apache” [682] 中对手动重新启动进行了描述。大多数配置更改仅需要使用 `rcapache2 reload` 进行重新装载即可。

---

### 40.2.1 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。

#### 配置文件

Apache 配置文件可在两个不同位置处获取：

- `/etc/sysconfig/apache2`
- `/etc/apache2/`

#### `/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。

## **/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。不编辑。

`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。它主要含有 include 语句和全局设置。重写此处列出的相应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。基于名称的虚拟托管（请参见“[基于名称的虚拟主机](#)”一节 [673]，它也是在此处配置的）。

#### magic

mime\_magic 模块的数据帮助 Apache 自动确定 MIME 类型的未知文件。不更改。

#### 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）。不编辑。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 40.4 节“安装、激活和配置模块”](#) [683]。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 40.4.4 节“多处理模块”](#) [687]）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 40.6 节“使用 SSL 设置安全性 Web 服务器”](#) [692]。

`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`。请勿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。不更改。

`vhosts.d/*.conf`

应该在此处提供虚拟主机配置。该目录中包含虚拟主机（有无 SSL 均可）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。有关细节，请参见“[虚拟主机配置](#)”一节 [672]。

## 虚拟主机配置

术语**虚拟主机**指 Apache 在一个物理计算机上为多个 URI（统一资源标识符）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。

可以通过 YaST（请参见“[虚拟主机](#)”一节 [679]）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。通过如此操作，不但可以将特定于域的配置保存在一个文件中，而且您始终能通过简单的移动、删除或重命名虚拟主机的配置文件来回到工作基本配置。因此，还应该为每个虚拟主机创建单独的配置文件。

---

`<VirtualHost></VirtualHost>` 块保存适用于特定域的信息。当 Apache 接收到客户机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 使用客户程序发送的 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机发出的在 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 40.1 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 40.2 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 40.3 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 日志文件所在的默认目录。

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信息。/var/log/apache2/ 是 Apache 日志文件所在的默认目录。

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/docs">
  Order allow,deny
  Allow from all
</Directory>
```

完整的配置文件外观如下所示：

### 例 40.4 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>
```

## 40.2.2 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**”一节 [680]中的对话框都会打开。

### 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）。默认设置就是在所有网络接口（IP 地址）的端口 80 上监听。

选择**打开所选端口上的防火墙**，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。测试时，仅在不必对 Web 服务器进行外部访问时关闭端口是有用的。

单击**下一步**继续配置。

模块

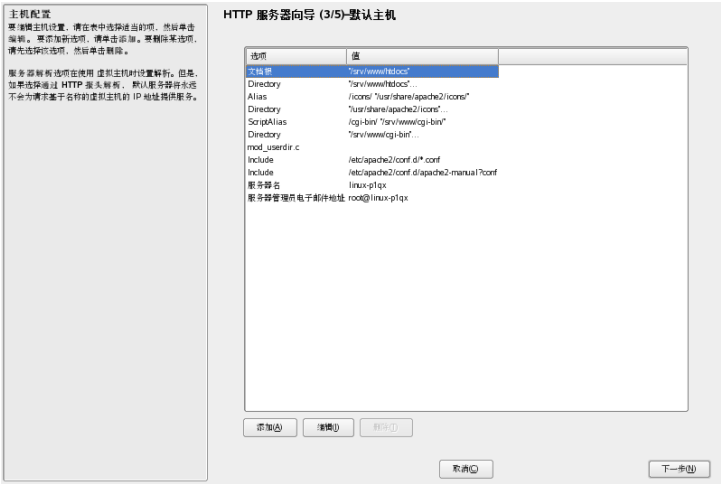
模块配置选项允许激活或停用脚本语言，Web 服务器应该支持此功能。要激活或停用其他模块，请参见“服务器模块”一节 [681]。单击下一步进入下一个对话框。

默认主机

该选项与默认的 Web 服务器相关。正如“虚拟主机配置”一节 [672]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 40.1 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 Alias /icons 指向 /usr/share/apache2/icons 以获取显示在目录索引视图中的 Apache 图标。

## 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，便可包含一组只能用于指定目录的配置选项。

目录 /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

这指定了客户机用来联系 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“[虚拟主机配置](#)”一节 [672]）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，单击添加打开一个对话框，在此输入主机的基本信息。服务器标识包括服务器名称、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 40.6.2 节“使用 SSL 配置 Apache”](#) [696] 了解有关 SSL 和证书的细节。使用目录索引选项，可指定在客户机请求目录时显示的文件（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）。使用启用公用 HTML，用户公共目录 (~user/public\_html/) 的内容便可显示在服务器上的 `http://www.example.com/~user` 下。

---

### 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“[HTTP 服务器配置](#)”一节 [680] 中所述的对话框。

图 40.2 HTTP 服务器向导：摘要



# HTTP 服务器配置

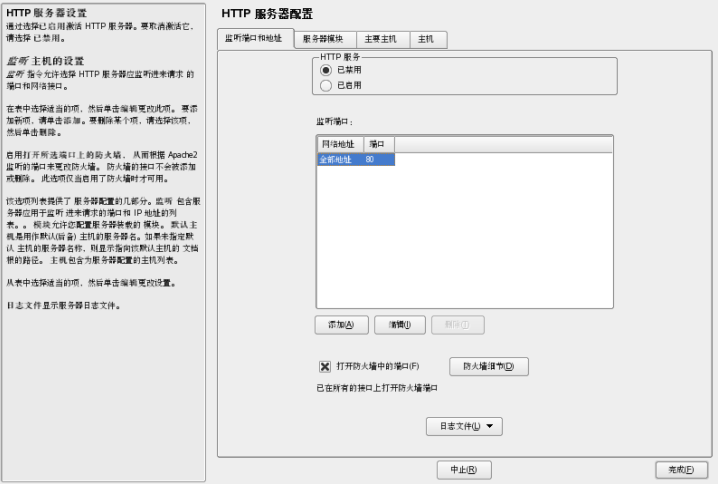
*HTTP 服务器配置*对话框还允许您对配置进行比在向导（它只在您首次配置 Web 服务器时运行）中更多的调整。它由四个如下所述的选项卡组成。在此处更改的配置选项都不会立即生效，始终需要使用完成来确认更改从而使其生效。单击取消退出配置模块并丢弃所作更改。

## 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。默认设置就是侦听端口 80 上的所有接口。始终应该选择打开所选端口上的防火墙，否则不能从外部到达 Web 服务器。测试时，仅在不必对 Web 服务器进行外部访问时关闭端口是有用的。

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，您可从该窗口重新启动或重新装载 Web 服务器（有关细节，请参见第 40.3 节“启动和停止 Apache”[682]）。这些命令将立即生效。

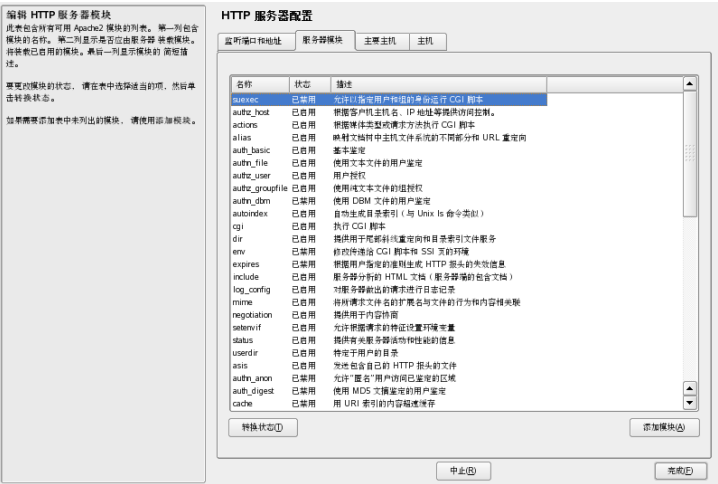
图 40.3 HTTP 服务器配置：侦听端口和地址



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 40.4 节“安装、激活和配置模块”[683]。

图 40.4 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 [677]和“虚拟主机”一节 [679]。

## 40.3 启动和停止 Apache

如果使用 YaST 配置（请参见第 40.2.2 节“使用 YaST 配置 Apache” [676]），Apache 在引导时于运行级别 3 和 5 启动，于运行级别 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。

要在运行系统上启动、停止或操纵 Apache，请使用 `init` 脚本 `/usr/sbin/rcapache2`（请参见第 20.2.2 节“Init 脚本” [361]以获取有关 `init` 脚本的常规信息。）。`rcapache2` 命令使用以下参数：

`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 40.6 节“使用 SSL 设置安全性 Web 服务器” [692]。

`stop`

通过终止父进程来停止 Apache。

`restart`

停止并重新启动 Apache。如果 Web 服务器没有预先运行，则启动它。

`try-restart`

只有在 Apache 已预先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，`rcapach2 reload` 是重新启动 Apache 的首选方法（例如，要激活配置中的更改），因为该方法允许所有客户机均得到服务，而不会造成连接中断。

---

### `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时强制执行的，所以通常不需要显式运行测试（如果发现配置错误，则 Web 服务器将不启动、重装载或重新启动）。

### `probe`

探测重装载的必要性（检查配置是否已更改）并向 `rcapach2` 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` 并启用模块 `mod_status`。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 `rcapach2` 指定其他标志，则这些标志将传到 Web 服务器。

---

## 40.4 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 40.4.2 节“[激活和取消激活](#)”[684]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 的 Apache 中仅编译进了 `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。SUSE Linux Enterprise Server 提供了几个现成可用的外部模块。

### 多处理模块

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。

## 40.4.1 模块安装

如果使用默认方法来安装 Apache（如第 40.1.2 节“安装”[668]中所述），则将安装所有基础和扩展模块、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。

## 40.4.2 激活和取消激活

可使用 YaST 来激活或停用脚本语言模块（PHP5、Perl、Python），模块配置如“HTTP 服务器向导”一节 [676] 中所述。可以按“服务器模块”一节 [681] 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。

---

## 40.4.3 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：基本身份验证 (`mod_auth_basic`) 或摘要身份验证 (`mod_auth_digest`)。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商模块 `mod_authn_*`（例如，基于身份验证的文本文件的 `mod_authn_file`）结合，并与授权模块 `mod_authz_*`（例如，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 脚本时需要有 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）。它还能自动重定向到正确的 URI（如果目录请求不包含尾部斜杠）。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

有了 mod\_expires，便可通过发送 Expires 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 处配置的

#### 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 text/html 适用于 HTML 文档）传递具有正确 MIME 标题的文件。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，但是功能更全且更为灵活。使用 `mod_rewrite`，可根据多个规则和请求标题等来重定向 URL。

#### `mod_setenvif`

基于客户机的请求细节（如客户机发送的浏览器字符串或客户机的 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 服务器和客户机之间启用加密连接。有关详细信息，请参见第 40.6 节“使用 SSL 设置安全性 Web 服务器”[692]。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` 处配置的

#### `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。

## 40.4.4 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

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，因为它隔离每个请求并通过生成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。

---

## 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。预生成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，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。

---

## 40.4.5 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。在列出的目录中查找模块的文档。

### mod\_apparmor

向 Apache 添加支持以将 Novell AppArmor 限制提供给由模块（如 mod\_php5 和 mod\_perl）处理的独立 CGI 脚本。

包名称: apache2-mod\_apparmor

更多信息: *Novell AppArmor Administration Guide* (↑*Novell AppArmor Administration Guide*)

### 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

## 40.4.6 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。

apxs2 安装的模块可用于所有 MPM。其他两个程序安装的模块只用于各自的 MPM。apxs2 将模块安装在 /usr/lib/apache2 和 apxs2-prefork 中，而 apxs2-worker 将模块安装在 /usr/lib/apache2-prefork 或 /usr/lib/apache2-worker 中。

使用命令 `cd /path/to/module/source; apxs2 -cia mod_foo.c (-c 编译模块、-i 安装模块，而 -a 激活模块)` 从源代码安装和激活模块。apxs2 的其他选项在 apxs2(1) 手册页中有描述。

## 40.5 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 能够传递由 CGI 脚本创建的内容，需要激活 `mod_cgi`。还需要 `mod_alias`。默认情况下启用这两种模块。请参见[第 40.4.2 节“激活和取消激活”](#) [684] 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 40.7 节“避免安全性问题”](#) [698] 以了解更多信息。

---



## 40.5.1 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“[虚拟主机配置](#)”一节[672]）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 40.5 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` 指令将控制默认的访问状态及 `Allow` 和 `Deny` 指令的评估顺序。在这种情况下，“`deny`”语句将在“`allow`”语句之前评估，并且可以从任何位置处访问。

## 40.5.2 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机，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机（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`。

用户 root 应该有可由 Web 服务器访问的文件（请参见第 40.7 节“避免安全性问题”[698]获取其他信息）。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”。

## 40.5.3 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，则始终要确保它们中没有编程错误。

## 40.6 使用 SSL 设置安全性 Web 服务器

只要在 Web 服务器和客户机之间传送诸如信用卡数据之类的敏感数据，就需要带有身份验证的安全加密连接。`mod_ssl` 将使用安全套接字层 (SSL) 和传输层安全 (TLS) 协议为客户机和 Web 服务器之间的 HTTP 通讯提供强大的加密功能。使用 SSL/TLS 时，将在 Web 服务器和客户机之间建立专用连接。能够确保数据完整性，并且客户机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，证书使得在客户机和服务器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://`）。

## 40.6.1 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 服务器和客户机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](http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html)。

---

## 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。它将创建或覆盖以下文件：

- `/etc/apache2/ssl.crt/ca.crt`
- `/etc/apache2/ssl.crt/server.crt`

- /etc/apache2/ssl.key/server.key
- /etc/apache2/ssl.csr/server.csr

还会将 ca.crt 的副本放在 /srv/www/htdocs/CA.crt 下以供下载。

---

## 重要

不能在生产系统上使用虚设证书。它只能用来测试。

---

## 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，则只需通过您自己的证书授权者 (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 40.1 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*。

#### 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 使用安全性通行密码加密 CA 的 RSA 私用密钥

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 使用安全性通行密码加密 SERVER 的 RSA 私用密钥

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。不建议在公共商店使用此类证书。

---

## 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`。

## 40.6.2 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 43.4.1 节“使用 YaST 配置防火墙”](#) [742]中所述使用 YaST 来完成此操作。

---

要使用 SSL，必须在全局服务器配置中激活它。在编辑器中打开 `/etc/sysconfig/apache2`，然后搜索 `APACHE_MODULES`。如果 `“ssl”` 不存在，则将它添加到模块的列表中（`mod_ssl` 在默认情况下是激活的）。下一步，请搜索 `APACHE_SERVER_FLAGS` 和 `“SSL”`。如果打算使用密码加密服务器证书，则还应该增加 `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[“虚拟主机配置”一节](#) [672]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`

---

### 重要：基于名称的虚拟主机和 SSL

用户不能在仅具有一个 IP 地址的服务器上运行多个支持 SSL 的虚拟主机。连接到此类设置的用户会在每次访问 URL 时接收到警告消息，指出证书与服务器名称不匹配。每个支持 SSL 的域需要单独的 IP 地址或端口，才能实现基于有效 SSL 证书的通信。

---

## 40.7 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。

### 40.7.1 最新软件

在 Apache 软件中发现漏洞时，SUSE 将会发出安全忠告。其中包含修正漏洞的描述，用户应该尽快地采纳这些描述意见。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 <http://en.opensuse.org/Communicate#Mailinglists>
- RSS 递送 [http://www.novell.com/linux/security/suse\\_security.xml](http://www.novell.com/linux/security/suse_security.xml)

### 40.7.2 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。

### 40.7.3 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，而是要明确启用对于 Apache 可读的所有目录的访问权（请参见“[基本虚拟主机配置](#)”一节 [675] 获取细节）。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。



## 40.7.4 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都能执行 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。

## 40.7.5 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，这些文件能够允许用户重写安全性设置。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，但是不允许用户使用 `mod_userdir`（请参见 `/etc/apache2/mod_userdir.conf` 配置文件）时重写任何 `Option` 指令。

## 40.8 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。这里是几处查找错误描述的常见位置和需要检查的重要事项。

首先，`rcapache2`（在[第 40.3 节“启动和停止 Apache”](#) [682]中有述）可详细描述有关错误，因此在实际用于运行 Apache 时十分有帮助。对于启动或停止 Web 服务器，有时倾向于使用二进制文件 `/usr/sbin/httpd2`。但请避免这样做，而使用 `rcapache2` 脚本。`rcapache2` 甚至提供了解决配置错误的技巧和提示。

其次，日志文件是非常重要的，不容忽视。如果有致命错误和非致命错误，Apache 日志文件（主要是错误日志文件）是您查找错误原因的地方。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。默认情况下，错误日志文件位于 `/var/log/apache2/error_log`。

---

### 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。

---

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 40.2.2 节“使用 **YaST** 配置 **Apache**” [676]）。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](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](mailto:comp.infosystems.www.servers.unix)。

## 40.9 更多信息

包 `apache2-doc` 中包含有关本地安装和参照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 `yast -i 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。

### 40.9.1 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](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。

## 40.9.2 Apache 模块

有关来自 第 40.4.5 节 “外部模块” [688] 的外部 Apache 模块的更多信息，可在以下位置获得：

mod-apparmor

<http://en.opensuse.org/AppArmor>

mod\_perl

<http://perl.apache.org/>

mod\_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod\_python

<http://www.modpython.org/>

## 40.9.3 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/>

## 40.9.4 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](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。



## 代理服务器 Squid

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。它将来自客户机（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程序并在硬盘缓存中保存对象副本。缓存的一个优点就是：当多个客户程序请求同一对象时，可以从硬盘缓存中提供该对象。这样客户机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机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。它确实还支持 FTP、Gopher、SSL 和 WAIS 等协议，但不支持其他的因特网协议，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。

### 41.1 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。

## 41.1.1 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 之外的所有客户机对外部服务的访问。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 41.5 节“配置透明代理”[713]描述了如何实施透明代理。它能简化客户机的配置，因为在这种情况下，它们不需要代理的任何信息。

## 41.1.2 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。

---

### 41.1.3 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。

## 41.2 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。

### 41.2.1 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。

### 41.2.2 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。

## 41.2.3 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 41.6 节“cachemgr.cgi”](#)[716]中有介绍。网络流量巨大的站点应使用内存存在 4GB 以上的 AMD64 或 Intel 64 系统。

## 41.2.4 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。

## 41.3 启动 Squid

Squid 在 SUSE® Linux Enterprise Server 中已预先配置，因此安装后即可启动。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。



## 41.3.1 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 41.4.2 节“访问控制选项”](#) [711]。

修改配置文件 `/etc/squid/squid.conf` 后，Squid 必须重新装载该配置文件。可通过 `rcsquid reload` 执行此操作。或者，通过 `rcsquid restart` 彻底重新启动 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 在断开同客户机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。要能够重新启动 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 8.5.12 节“系统服务（运行级别）”](#) [146]。

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。

## 41.3.2 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 33.3 节“启动名称服务器 BIND” [564]）。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`。此行为是在文件 `/etc/sysconfig/network/config` 中通过 `sysconfig` 变量 `MODIFY_RESOLV_CONF_DYNAMICALY`（被设置为 "yes"）控制的。通过 YaST `sysconfig` 编辑器将此变量设置为 "no"（请参见第 20.3.1 节“使用 YaST Sysconfig 编辑器更改系统配置” [366]）。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 `MODIFY_NAMED_CONF_DYNAMICALY` 设置为 YES，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` 下手动输入服务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。

---

## 41.4 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，但是外部客户程序最初不具

备访问权。代理可供 `localhost` 使用。默认端口为 3128。预装的配置文件 `/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`，配置文件可能不起作用，因为有时会修改选项并添加新的更改。

---

## 41.4.1 常规配置选项（选择）

### `http_port 3128`

这是 Squid 侦听客户机请求所用的端口。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 hostname type proxy-port icp-port`

在此输入父代理（如果您想使用 ISP 的代理）。在 `hostname` 中输入要使用代理的名称和 IP 地址，在 `type` 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机的 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。可以使用此方法来保护客户机的私密。

`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 会将客户机的 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，将分钟改为秒钟，然后单击浏览器中的重装载，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。

## 41.4.2 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*），允许拦截不需要的 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机使用因特网：

```
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 定义的所有客户机都运行 *ident* 请求以查找各个用户的身份。如果对 *<acl\_name>* 应用 *all*，此选项对所有客户机都有效。另外，必须在所有客户机上运行 *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* 查找的客户机才有权访问，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。

## 41.5 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，建议所有客户机都使用代理来浏览因特网。
- 所有客户机都必须使用代理，无论客户机是否清楚这一点。
- 网络中的代理已转移，但是现有的客户机应保留原有配置。

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。

### 41.5.1 /etc/squid/squid.conf 中的配置选项

要启动并运行透明代理，需在 `/etc/squid/squid.conf` 文件中激活的选项包括：

- `httpd_accel_host virtual`
  - `httpd_accel_port 80`
- 实际 HTTP 服务器所位于的端口号
- `httpd_accel_with_proxy on`
  - `httpd_accel_uses_host_header on`

## 41.5.2 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 SuSEfirewall2 工具完成此操作，如[第 43.4.1 节“使用 YaST 配置防火墙”](#) [742]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（请参见 `/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 Web 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 41.1 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 can be used to force all internal users to surf via your
# Squid proxy, or transparently redirect incoming Web traffic to
# a secure Web server.
#
# Choice: leave empty or use the following explained syntax of
# redirecting rules, separated with spaces.
# A redirecting rule consists of 1) source IP/net,
# 2) destination IP/net, 3) original destination port and
# 4) local port to redirect the traffic to, separated by a colon,
# e.g. "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
```

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,输入这些客户机请求发往的 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 192.168.0.0/16,0/0,tcp,21,3128"
FW_REDIRECT="192.168.0.0/16,0/0,udp,80,3128 192.168.0.0/16,0/0,udp,21,3128"
```

要启动防火墙及其新配置,请更改 /etc/sysconfig/SuSEfirewall2 文件的项。必须将 START\_FW 项设置为 "yes"。

按第 41.3 节“启动 Squid”[706]所述启动 Squid。要检查是否一切运行正常,请在 /var/log/squid/access.log 中查看 Squid 日志。要验证是否正确配置了所有端口,请在来自网络外的任何计算机上执行端口扫描。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。

## 41.6 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。

### 41.6.1 设置

首先，必须在系统上运行 Web 服务器。按第 40 章 *Apache HTTP 服务器* [667] 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`：

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

### 41.6.2 /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 41.2 “访问规则” [717]所示包含额外的 ACL。

### 例 41.2 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 41.3 “访问规则” [717]中添加规则以允许从 Web 服务器访问。

### 例 41.3 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，就应重启动 Squid。使用 `rcsquid reload` 可以轻松地重启动。

## 41.6.3 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。有关缓存管理器显示的每个项的更多详细信息，请参见 <http://www.squid-cache.org/Doc/FAQ/FAQ-9.html> 上的 Squid FAQ（常见问题解答）。

## 41.7 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：

- 限制某些用户的 Web 访问，使其只能访问一组可接受的或众所周知的 Web 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/config/> 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。squidGuard 速度很快，足以处理很多请求：在

带有 5,900 个域和 7,880 个 URL（总数为 13,780）的 500 MHz Pentium 上，10 秒内可处理 100,000 个请求。因此，不建议设置四个以上的进程，因为进程的分配会过多的占用内存。

```
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。

## 41.8 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/>。该程序很方便使用。

以 root 身份登录，然后输入 `cat access.log.files | calamaris options > 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：

- 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.2 access.log.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。

另一个功能强大的缓存报告生成器工具是 SARG（Squid 分析报告生成器）。详细信息请参见 <http://sarg.sourceforge.net/>。

## 41.9 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](mailto: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。

## 部分 V. 安全性





## 管理 X.509 认证

越来越多的身份验证机制基于加密过程。在这种情况下，为证书所有者指派密码密钥的数字证书就起着重要作用。此类证书做通讯使用，并且能在例如公司 ID 卡类的地方找到。证书的生成和管理大多由将其作为商业服务来提供的正式机构操作。但在某些情况下，您自己来执行这些任务也许更有意义。例如，如果某家公司不希望将个人数据透露给第三方。

YaST 为此提供了两个模块，它们为数字 X.509 证书提供了基本管理功能。以下部分叙述了数字证书的基础知识以及如何用 YaST 创建和管理此类证书。有关详细信息，请参考<http://www.ietf.org/html.charters/pkix-charter.html>

### 42.1 数字认证的原理

数字认证使用密码进程来加密数据，从而防止未经授权的用户访问这些数据。用户数据是使用另一种数据记录（即密钥）来进行加密的。系统在一个数学进程中将密钥应用于用户数据，从而生成一种经过更改的数据记录，在该数据记录中将不再能识别出原始内容。现在广泛使用的是非对称加密（公共密钥方法）。密钥总是成对出现的：

#### Private Key

私用密钥必须由密钥拥有者安全保管。如果不慎泄漏私用密钥对，就会损害该密钥对，并且导致它不能使用。

#### 公共密钥

密钥拥有者为第三方发布公共密钥

## 42.1.1 密钥真实性

因为公共密钥进程被广泛使用，所以有许多公共密钥处于流通中。要成功使用此系统，要求每个用户确保公共密钥真实属于所假定的拥有者。为用户颁发公共密钥，要由可信的组织通过公共密钥证书确认。这样的证书中包含密钥拥有者的姓名、相应的公共密钥和证书颁发者的电子签名。

颁发和签署密钥证书的可信机构通常是一个基础证书机构的一部分，它也同时对证书的其他方面的工作负责，例如，证书的发行、取消和更新。这种基础结构通常称为公共密钥基础结构或 *PKI*。OpenPGP 标准是一种常见的 *PKI*，在其中用户可以不通过中心授权点而自行发布证书。如果有“值得信任的 Web”中其他方的签名，这些证书就变得可信。

X.509 公共密钥基础结构 (*PKIX*) 是由 IETF（因特网工程事务组）定义的另一种模型，现在用作几乎所有公开使用的 *PKI* 的样本。在此模型中，由 证书授权机构 (CA) 在一个分级的树结构中执行身份验证。树的根是根 CA，它为所有的子 CA 提供保证。最低级别的子 CA 颁发用户证书。可在根 CA 中跟踪到的用户证书是可信的。

这样的 *PKI* 的安全性完全取决于 CA 证书的可信性。为了使认证操作对 *PKI* 客户透明，*PKI* 操作员定义了一个 认证操作细则 (CPS)，其中定义了证书管理的过程。这样可确保 *PKI* 颁发的证书都是可信的。

## 42.1.2 X.509 证书

X.509 证书是一个具有多个固定字段和可选的附加扩展的数据结构。固定字段主要包括密钥拥有者、公共密钥和与证书发布 CA 相关的数据（名称和签名）。出于安全原因，证书只能具有有限的有效期，因此还为此日期提供了一个字段。CA 确保了证书在指定期间的有效性。在期满之前，CPS 通常会要求 *PKI*（发行 CA）创建和分发一个新的证书。

扩展中可以包含任何附加信息。应用程序通常无需能够对扩展求值，除非它被标识为 关键。如果应用程序不能识别关键扩展，它就必须拒绝此证书。某些扩展只针对某个特别应用程序有用，例如签名和加密。

表 42.1 版本 3 中，显示了基础 X.509 证书的字段。

表 42.1 X.509v3 证书

字段	内容
版本	证书版本，例如 v3
序列号	独一无二的证书 ID（一个整数）
签名	用于对证书签名的 ID 算法。
颁发者	证书发布机构 (CA) 的唯一名称 (DN)。
有效性	有效期
主题	证书拥有者的唯一名称 (DN)。
主题公共密钥的信息	所有者的公共密钥以及 ID 的算法
发行者的唯一 ID	发行 CA 的唯一密钥（可选）
主题唯一密钥	所有者的唯一密钥（可选）
扩展	可选的其他信息, 例如 “KeyUsage”、 “BasicConstraints” 等。

### 42.1.3 阻止 X.509 证书

如果一个证书在期满之前就边为“不可信”，必须立即停止使用。例如，当私用密钥泄漏时，则必须这样做。这尤其适用于私用密钥属于CA而不是用户证书。在这种情况下，必须立即阻止相关 CA 发布的所有用户证书。如果阻止了某证书，PKI（对其负责的 CA）就必须通过 证书撤消列表(CRL)将此信息提供给相关方。

这些列表由 CA 定期提供给 CRL 分发点 (CDP)。在证书里命名一个 CDP 扩展（可选），这样，检查员就可取得一个当前 CRL 用于校验。实现此目的的一种方法是使用联机证书状态协议(OCSP)。CRL 的真实性有发行 CA 的签名确认。

表 42.2 “X.509 证书撤消列表 (CRL)” [726] 显示 X.509 CRL 的基础部分。

**表 42.2** X.509 证书撤销列表 (CRL)

字段	内容
版本	CRL 版本，例如 v2。
签名	用于对证书签名的算法 ID。
颁发者	CRL 发布者（通常是证书发布 CA）的唯一名称 (DN)。
此更新	此 CRL 的发布时间（日期、时间）。
下次更新	下一 CRL 的发布时间（日期、时间）。
已撤销的证书列表	每项包含证书的序列号、撤销时间和可选扩展（CRL 项扩展）。
扩展	可选 CRL 扩展。

## 42.1.4 证书和 CRL 的储存库

必须使用 储存库 使CA 的证书和 CRL 能够被公共访问。因为证书和 CRL 由于有签名而不能被伪造，所以不需要以特殊的方式来保证储存库本身的安全。相反地，它尽可能简单快速地允许访问。因此，通常在 LDAP 或 HTTP 服务器上提供证书。有关 LDAP 的解释，参见 [第 36 章 LDAP - 目录服务](#) [599]。第 40 章 [Apache HTTP 服务器](#) [667] 包含 HTTP 服务器的信息。

## 42.1.5 专有 PKI

YaST 包含用于 X.509 证书基本管理的模块。主要包括 CA、子 CA 及其证书。PKI 服务内容远不止于创建、分发证书及 CRL。PKI 的操作是要求精心构思的管理基础结构用于证书和 CRLs 的更新。此基础结构由商业 PKI 产品提供，并且能部分自动化。YaST 提供 CA 和证书的创建及分发工具,但目前不提供此背景基础结构。要设置一个小型 PKI，您可以使用可用的 YaST 模块。但是，您应使用商业产品来设置一个“正式”PKI，或是商业 PKI。

# 42.2 用于 CA 管理的 YaST 模块

YaST 提供了两个用于基本 CA 管理的模块。使用这些模块进行的主要管理任务论述如下：

## 42.2.1 创建根 CA

设置 PKI 的第一步是创建根 CA。执行下列操作：

- 1 启动 YaST 并转至安全和用户 > CA 管理。
- 2 单击 创建根 CA。
- 3 在第一个对话框中输入 CA 的基本数据，如图 图 42.1 “YaST CA 模块 — 根 CA 的基本数据” [727] 所示。文本字段的意义如下：

图 42.1 YaST CA 模块 — 根 CA 的基本数据

要生成新的 CA，需要某选项。

具体取决于配置文件中定义的策略。

CA 名称是 CA 证书的名称。仅使用 ASCII 字符，"-"和"."。

常用名称是 CA 的名称。

电子邮件地址是用户或服务管理器的有效电子邮件地址。

组织、组织单元、位置和组织元是可选的。

新建Root CA(步骤 1/3)

CA 名称(C):  
example-cert

常用名(O):  
example-ca

电子邮件地址

默认值

root@example.com ✓

删除(D)

默认值(D)

添加(A)

组织(O):  
example organization

组织单元(O):  
example

位置(L):

省/州(S):

国家/地区(C):  
中华人民共和国

中止(B)

下一步(N)

CA 名称：

输入 CA 的技术名相比其他名，目录名尤其是从技术名派生的，这就是只能使用帮助中指出的字符的原因。当启动模块时，此技术性名称也会在概述中显示出来。

通用名称

参考 CA 输入要用的名称。

“电子邮件地址”

可以输入 CA 用户能够看到的多个电子邮件地址。这对于查询会很有用。

国家/地区

在国家/地区中选择 CA 运营所在的国家/地区。

组织, 组织单位, 地点, 国家/地区

可选值。

4 单击下一步。

5 在第二个对话框中输入密码当使用 CA（创建子 CA 或生成证书）时，将始终需要此密码。文本字段的意义如下：

密钥长度

密钥长度包含一个有意义的默认值。除非某个应用程序不能处理此密钥长度，否则通常不需要更改它。

有效期（天）

CA 默认有效期是 3650 天（大约 10 年）。之所以选择这么长的时间是因为替换被删除的 CA 涉及很多管理工作。

单击 *高级选项* 打开一个对话框，在其中设置 X.509 扩展的不同属性（[图 42.4 “YaST CA 模块 — 扩展设置” \[732\]](#)）。这些值都有合理的默认设置，如非确有必要请勿更改它们。

6 YaST 会显示当前设置以供确认。单击 *创建*。就创建了根 CA，并显示在预览里。

---

## 提示

通常情况下，最好不要允许根 CA 发行用户证书。最好创建至少一个子 CA，然后在子 CA 中创建用户证书。这样做的好处在于可以将根 CA 隔离起来并保证它的安全，例如，可以将它放在位于安全场所并被孤立开来的计算机上。这就使攻击者很难攻击到根 CA。

---

# 42.2.2 创建或撤消子 CA

子 CA 的创建完全与根 CA 的创建方法一致。执行下列操作：

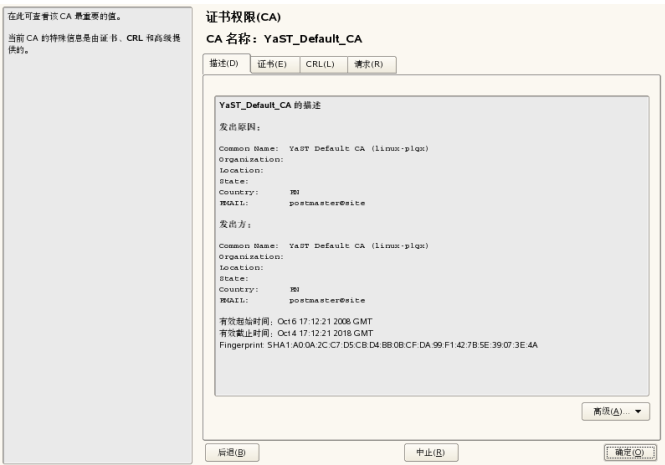
- 1 启动 YaST 并打开 CA 模块。
- 2 选择需要的 CA 并单击 输入 CA。

## 注意

子 CA 的有效期必须完全在“父”CA 的有效期内。因为始终在创建“父”CA 之后创建子 CA，所以默认值将引发错误消息。为避免这一点，请为有效期输入一个允许使用的值。

- 3 如果是第一次输入某 CA，请输入密码。YaST 在说明选项卡上显示 CA 密钥信息（请参见图 42.2）。

图 42.2 YaST CA 模块 — 使用 CA



- 4 单击高级并选择创建子 CA。这时将打开与创建根 CA 一样的对话框。
- 5 操作过程，参见 第 42.2.1 节“创建根 CA” [727]。

- 6 选择选项卡 *证书*。在此使用 *撤消* 以重设置已暴露或因其他原因而不需要的子 CA。仅执行撤消操作并不能停用子 CA。还需要在 CRL 中发布已撤消的子 CA。一节中介绍了如何创建 CRL。第 42.2.5 节 “创建 CRL” [733]

- 7 单击 *确认* 完成。

## 42.2.3 创建或撤消用户证书

创建客户机和服务器证书与第 42.2.1 节 “创建根 CA” [727] 中描述的创建 CA 的方法很类似。同样的原则也在此适用。为了签名目的证书里必须包含发信人（私人密钥持有人）的邮箱地址，以便邮件程序指派正确的证书。为了在加密期间进行证书指派，需要使收件人（公共密钥拥有者）的电子邮件地址包含在证书中。此外，对于服务器和客户证书，必须将服务器的主机名输入到 *常用名字* 字段中。证书的默认有效期是 365 天。

创建客户和服务器证书，操作步骤如下：

- 1 启动 YaST 并打开 CA 模块。
- 2 选择需要的 CA 并单击 *输入 CA*。
- 3 如果是第一次输入某 CA，请输入密码。YaST 在 *说明* 选项卡中显示 CA 密钥的信息。
- 4 单击 *证书* (参见 图 42.3 “CA 的证书” [731])。



图 42.3 CA 的证书



- 5 单击 添加添加服务器证书> 添加一个服务器证书。
- 6 单击添加> 添加客户机证书添加一个客户机证书。记得输入一个电子邮件地址。
- 7 单击 确认 完成。

撤消受到损坏或不需要的证书，操作步骤如下：

- 1 启动 YaST 并打开 CA 模块。
- 2 选择需要的 CA 并单击 输入 CA。
- 3 如果是第一次输入某 CA，请输入密码。YaST 在说明选项卡中显示 CA 密钥的信息。
- 4 单击 证书(参见 第 42.2.2 节 “创建或撤消子 CA” [729])。
- 5 选择要配置的扫描仪，然后单击 编辑。
- 6 选择撤消该证书的原因。
- 7 单击 确认 完成。

## 注意

但仅执行“撤消”并不足以取消一个证书。同样，在一个 CRL 中发布已撤消的证书。[第 42.2.5 节“创建 CRL” \[733\]](#)中说明了如何创建 CRL。发布到 CRL 中的撤消证书，可使用 *删除* 将其完全删除。

## 42.2.4 修改默认值

前面几节介绍了如何创建子 CA、客户机证书和服务器证书。在 X.509 证书的扩展中使用了一些特殊设置。已根据每种证书类型而为这些设置提供了合理的默认值，通常不需要更改。但是，您可能对这些扩展有特殊要求。如果是这样，修改默认值就变得有意义了。否则，每次创建证书时都要从头开始。

- 1 启动 YaST 并打开 CA 模块。
- 2 按照 [第 42.2.2 节“创建或撤消子 CA” \[729\]](#) 里的描述，输入相应的 CA。
- 3 单击 **高级 > 编辑默认值**。
- 4 选择要修改设置的类型。列出的修改默认值对话框，便会打开。[图 42.4 “YaST CA 模块 — 扩展设置” \[732\]](#)

**图 42.4** YaST CA 模块 — 扩展设置



- 5 用 *临界* 改变右端的联合值或创建/删除临界设置。
- 6 单击 *下一步* 显示摘要。
- 7 选择 *保存* 完成修改。

---

#### 提示

只有在此操作之后，对默认值的所有更改才生效。不会修改经存在的 CA 和证书。

---

## 42.2.5 创建 CRL

如果要排除已泄漏或因其他原因而不想要的证书防止它们继续被使用，必须首先将它们撤消。第 42.2.3 节“创建或撤消用户证书”[730]（针对子 CA）和第 42.2.2 节“创建或撤消子 CA”[729]（针对用户证书）两节中介绍了此过程。此后，必须使用此信息创建和发布一个 CRL。

系统只为每个 CA 保留一个 CRL。创建或更新此 CRL,操作如下：

- 1 启动 YaST 并打开 CA 模块。
- 2 按照 第 42.2.2 节“创建或撤消子 CA”[729] 里的描述，输入相应的 CA。
- 3 单击 *CRL*。随后出现的对话框将显示此 CA 的上最后一个 CRL 的摘要。
- 4 如果您从创建一开始就废除了新子 CA 或证书，用 *生成 CRL* 创建新 CRL。
- 5 然后为新 CRL 指定有效期（默认为 30 天）。
- 6 单击 *确定* 创建，并显示该新建 CRL。然后，必须发布此 CRL。

---

#### 提示

如果 CRL 不可用或满期，评估 CRL 的应用软件将拒绝所有证书。在当前 CRL 满期（超过有效期）之前经常创建和发布新的 CRL 是 PKI 供应商的职责。YaST 不支持此过程的自动化。

---

# 42.2.6 将 CA 对象导出到 LDAP

要进行 LDAP 导出，执行计算机应配置有 YaST LDAP 客户机。它运行时提供 LDAP 服务器信息，填写对话框字段的时候需要这些信息。否则，虽然可以进行导出，但必须手动输入所有 LDAP 数据。您总是要输入多个密码（请参见表 **表 42.3 “LDAP 导出期间的密码”** [734]）。

**表 42.3** LDAP 导出期间的密码

密码	含义
LDAP 密码	授权用户进入 LDAP 树。
证书密码	授权用户导出证书。
新“证书密码”	在 LDAP 导出期间使用 PKCS12 格式。此格式强制为所导出的证书指派新密码。

可以将证书、CA 和 CRLs 导出到 LDAP。

## 将 CA 导出到 LDAP

要导出 CA，输入 **第 42.2.2 节 “创建或撤消子 CA”** [729] 一节中介绍的 CA。在随后的对话框中选择 **扩展 > 导出到 LDAP**，打开用于输入 LDAP 数据的对话框。如果您的系统已配置 YaST LDAP 客户机，则这些字段已填写了一部分。否则，请手动输入所有数据。输入是在 LDAP 中具有“caCertificate”属性的一个单独的树中进行的。

## 将证书导出到 LDAP

进入包含要导出的证书的 CA，然后选择 **证书**。从对话框上部的证书列表中选择所需的证书，然后选择 **导出 > 导出到 LDAP**。在这里输入 LDAP 数据，方式与为 CA 输入数据时相同。证书将以“用户证书”(PEM 格式)和“用户 PKCS12”(PKCS12 格式)为属性，以用户项目保存到 LDAP 树。

## 将 CRL 导出到 LDAP

输入包含要导出的 CRL 的 CA，然后选择 **CRL**。如果需要，创建新的 CRL，然后单击 **导出**。打开的对话框中将显示导出参数。您可以一次性导出此 CA 的 CRL 或定期导出。通过选择 **导出到 LDAP** 激活该导出，然后输入相应的 LDAP 数据。要定期执行此操作，选择 **反复再创建并导出** 单选按钮，并更改间隔（如果适合）。

## 42.2.7 将“CA 项目”导出为文件

如果已经在计算机上设置了一个用来管理 CA 的储存库，则可以使用此选项在正确的位置直接以文件形式创建 CA 对象。有多种输出格式可用，如 PEM、DER 和 PKCS12。在 PEM 情况下，可以选择是否使用密钥将证书导出，以及该密钥是否要加密。在 PKCS12 情况下，可以导出证书路径。

可以采取与使用 LDAP 相同的方式导出证书、CA 文件，只是要选择以文件导出，而不是导出到 LDAP，详见第 42.2.6 节“将 CA 对象导出到 LDAP” [734]。完成上述操作后将进入一个对话框，在其中可选择所需输出格式并输入密码和文件名。单击确定后，即将证书储存在所需位置。

对于 CRL，单击导出，选择导出到文件，选择导出格式（PEM 或 DER），然后输入路径。继续单击确定，将其保存到相应的位置。

---

### 提示

您可以选择文件系统中的任何储存位置。此选项也可用于将 CA 项目保存在传输媒体（例如 USB 储存棒）上。/媒体目录通常包含除系统硬盘驱动器之外的各类驱动器。

---

## 42.2.8 导入“普通服务器证书”

如果已经在孤立的 CA 管理计算机上使用 YaST 将服务器证书导出到媒体，则可以将此证书作为普通服务器证书导入到服务器上。使用 YaST 在安装期间或稍后的步骤中执行此操作。

---

### 注意

要成功地导入证书，您需要一个 PKCS12 格式。

---

公共服务器证书储存在 /etc/ssl/servercerts 中，任何支持 CA 的服务均可在此使用它。此证书失效时，则可以使用相同的机制方便地替换此证书。要使用替代证书运行各事件，重新启动这些参与的服务。

---

## 提示

如果在这里选择了导入，则可以在文件系统中选择导入源。此选项也可用从传输媒体导入证书，例如 **USB** 储存棒。

---

导如一个一般服务器证书，操作如下：

- 1 启动 YaST 并打开安全和用户下的 *普通服务器证书*。
- 2 在 YaST 启动后，在说明字段中可查看当前证书的数据。
- 3 选择 *导如* 和证书文件。
- 4 输入密码并单击下一步。这样，导入的证书便会显示在说明字段里。
- 5 单击完成，关闭 YaST。

## 伪装和防火墙

只要在联网环境中使用 Linux，您就可以使用内核功能通过操纵网络包将内部网络区域和外部网络区域隔开。Linux netfilter 框架提供了一种建立有效防火墙的方法，可以将不同网络隔开。借助 iptables — 用于定义规则集的通用表结构 — 可以精确控制哪些包能通过网络接口。使用 SuSEfirewall2 和相应的 YaST 模块，您可以轻而易举地设置这种包过滤器。

### 43.1 使用 iptables 过滤包

部件 netfilter 和 iptables 负责网络包的过滤和操纵以及网络地址转换 (NAT)。过滤准则及与过滤准则关联的所有操作均储存在链中；各个网络包在到达时，必须依次与这些链进行匹配。要匹配的链储存在表中。使用 iptables 命令可以更改这些表和规则集。

Linux 内核维护以下三个表，分别对应包过滤器的不同功能：

#### 过滤器

此表储存大多数过滤规则，因为它执行严格意义上的包过滤机制，例如，决定是让包通过 (ACCEPT) 还是将包丢弃 (DROP)。

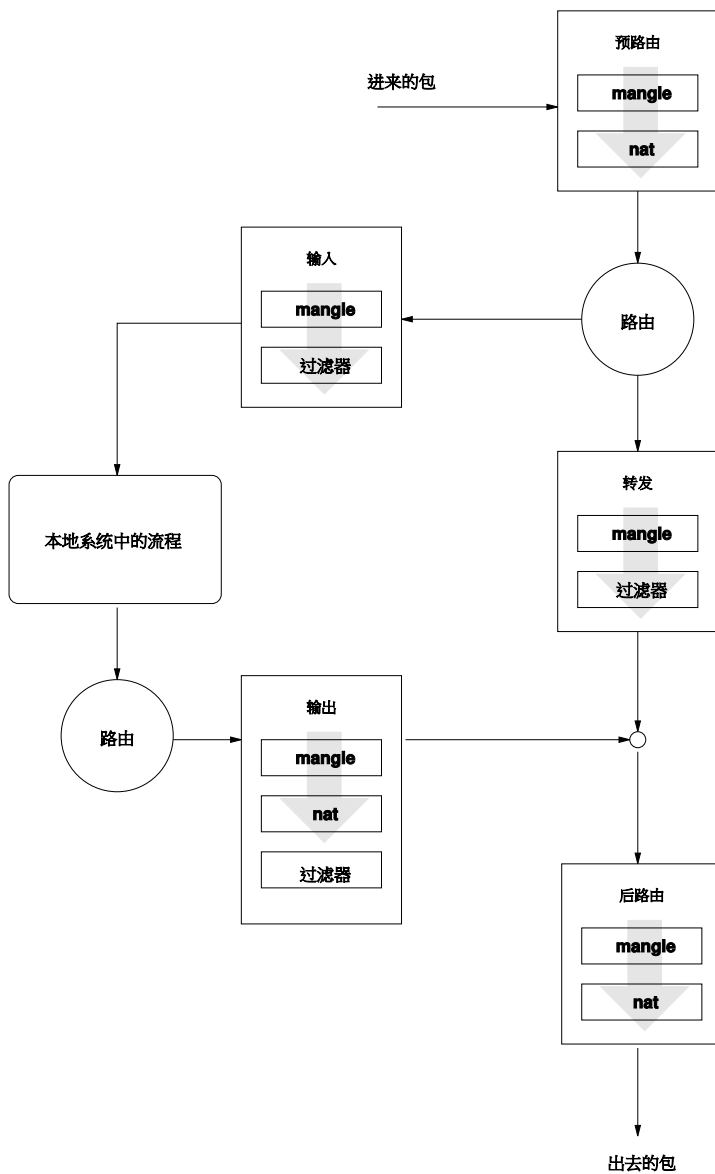
#### nat

此表定义对包的源地址和目标地址所做的任何更改。使用这些功能还能实现伪装，这是 NAT 的一个特例，用于将专用网络与因特网链接起来。

#### mangle

此表中的规则用于操纵 IP 报头中储存的值（如服务类型）。

图 43.1 iptable: 包的可能路径



这些表包含多个用于匹配包的预定义链:



## PREROUTING

此链适用于入站包。

## INPUT

此链适用于发往系统内部进程的包。

## FORWARD

此链适用于仅在系统中路由的包。

## OUTPUT

此链适用于从系统自身发出的包。

## POSTROUTING

此链适用于所有出站包。

**图 43.1 “iptables：包的可能路径”** [738]演示了网络包在特定系统中传送时可能经过的路径。为了便于说明，图中将表作为链的各个部分列出，但实际上表本身储存了这些链。

在所有可能的情况中最简单的情况是：发往系统本身的入站包到达 `eth0` 接口。数据包首先要转到 `mangle` 表的 `PREROUTING` 链，然后转到 `nat` 表的 `PREROUTING` 链。随后的步骤（涉及包的路由选择）确定包的最终目标，这是系统自身的过程。在包经过 `mangle` 表和 `filter` 表的 `INPUT` 链后，只要与 `filter` 表的规则确实匹配，那么包将最终到达目标。

## 43.2 关于伪装的基础知识

伪装是 Linux 特有的一种 NAT（网络地址转换）形式。通过伪装可以将小型 LAN（其中的主机使用专用地址范围中的 IP 地址，请参见第 30.1.2 节“网络掩码和路由”[498]）与因特网（使用正式的 IP 地址）连接起来。为使 LAN 主机能连接到因特网，需要将其专用地址转换为正式地址。这种转换是在路由器上完成的，路由器充当了 LAN 和因特网之间的网关。其中的原理只有简单的一条：路由器有多个网络接口，通常是一个网卡和与因特网连接的另一个接口。后者将路由器与外部世界链接起来，同时，还会有一个或多个其他网络接口将路由器与 LAN 主机链接起来。在本地网络中的这些主机连接到路由器的网卡（如 `eth0`）后，它们就可以将发往本地网络之外的所有包发送到其默认网关或路由器。

---

### 重要：使用正确的网络掩码

在配置网络时，确保所有本地主机的广播地址和网络掩码都相同。做不到这一点就会导致无法正确路由数据包。

---

如上所述，只要有某台 LAN 主机要向因特网地址发送包，这个包就会发送到默认路由器。但是，必须先配置路由器，然后才能转发这些包。由于安全原因，默认安装中未启用它。要提供这种支持，请将文件 `/etc/sysconfig/sysctl` 中的变量 `IP_FORWARD` 设置为 `IP_FORWARD=yes`。

连接的目标主机可以看到路由器，但对内部网络中发出包的那台主机却毫不知情。伪装技术就是因此而得名的。由于要进行地址转换，路由器自然成为所有回复包首先到达的目标。路由器必须能够识别这些入站包并转换其目标地址，这样才能将包转发给本地网络中的正确主机。

由于入站通讯数据的路由选择取决于伪装表，所以从外部根本无法打开与内部主机的连接。对于这种连接，伪装表中不会有任何对应项。此外，所有已建立的连接在该表中都被指派了一个状态项，所以其他连接无法再使用该项。

受以上各种因素影响，在使用某些应用程序协议，如 ICQ、cucme、IRC（DCC、CTCP）和 FTP（采用 PORT 方式）时，您可能会遇到一些问题。Web 浏览器、标准 FTP 程序和许多其他程序都使用 PASV 方式。就包过滤和伪装而言，这种被动方式不容易出问题。

## 43.3 防火墙基础知识

在描述不仅可以提供和管理网络间的链接，同时还能够控制网络间的数据流的机制时，*防火墙*可能是最常使用的术语。严格地说，本节所述的机制应该叫做*包过滤器*。包过滤器根据特定准则（如协议、端口和 IP 地址）来控制数据流。这样您就可以根据包的地址来拦截不应该发送到您网络中的包。举例来说，若允许对 Web 服务器进行公共访问，应明确打开相应的端口。不过，包过滤器并不扫描有合法地址的包的内容（例如那些要发送到该 Web 服务器的包）。例如，即使是在入站包想要破坏 Web 服务器上的 CGI 程序的情况下，包过滤器仍然允许它们通过。

一种更有效但同时也更复杂的机制是将多种系统结合起来使用，例如让包过滤器与应用程序网关或代理进行交互。在这种情况下，包过滤器将拒绝所有发往禁用端口的包，而只接受发往应用程序网关的包。此网关或代理伪装成服务器

的实际客户端。从某种意义上说，可以将这种代理视为应用程序使用的协议级的伪装主机。这种代理的一个示例就是 Squid（一种 HTTP 代理服务器）。要使用 Squid，必须将浏览器配置为通过代理通讯。代理缓存将提供请求的任何 HTTP 页，缓存中没有的页将由代理从因特网获取。再以 SUSE proxy-suite (proxy-suite) 为例，该程序为 FTP 协议提供了代理。

下一节着重介绍 SUSE Linux Enterprise 附带的包过滤器。有关包过滤和防火墙的详细信息，请阅读 howto 包中的 Firewall HOWTO（防火墙使用说明）。如果已安装此包，请阅读 HOWTO，方法是使用

```
less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz
```

## 43.4 SUSEfirewall2

SUSEfirewall2 是一个脚本，用来读取在 /etc/sysconfig/SUSEfirewall2 中设置的变量以生成一组 iptables 规则。该脚本定义了三个安全区域，但在以下示例配置中只涉及第一个和第二个安全区域：

### 外部区域

鉴于根本无法对外部网络进行控制，所以需要保护主机，使其免受外部网络的影响。在多数情况下，外部网络就是因特网，但也可能是其他不安全的网络，如 WLAN。

### 内部区域

内部网络是指专用网络，多为 LAN。如果此网络中的主机使用专用地址范围中的 IP 地址（请参见第 30.1.2 节“网络掩码和路由”[498]），则必须启用网络地址转换 (NAT)，内部网络中的主机才能访问外部网络。

### 网络隔离区 (DMZ)

尽管从外部网络和内部网络都可以访问此区域内的主机，但这些主机本身无法访问内部网络。这种设置可用于在内部网络前再加一道防线，因为 DMZ 系统与内部网络是隔离的。

凡是过滤规则集没有明确允许通过的网络通讯数据，iptables 都一概禁止。因此，必须将入站通讯数据所流经的各个接口放入这三个区域之一。对于每个区域，都应定义所允许的服务或协议。规则集只适用于来自远程主机的包。防火墙不截获本地生成的包。

可以使用 YaST 进行上述配置（请参见 [第 43.4.1 节“使用 YaST 配置防火墙”](#) [742]）。还可以在文件 `/etc/sysconfig/SuSEfirewall12` 中进行手动配置，该文件已作适当注释。另外，`/usr/share/doc/packages/SuSEfirewall12/EXAMPLES` 还提供了一些示例方案。

## 43.4.1 使用 YaST 配置防火墙

---

### 重要：自动配置防火墙

完成安装后，YaST 会在所有已配置接口上自动启动防火墙。如果在系统中配置并激活了某个服务器，YaST 可通过服务器配置模块中的选项 *打开防火墙中所选接口上的端口* 或 *打开防火墙中的端口* 修改自动生成的防火墙配置。某些服务器模块对话框包含 *防火墙细节* 按钮，用于激活其他服务和端口。YaST 防火墙配置模块可用于激活、取消激活防火墙或单独对其进行重配置。

---

可以从 YaST 控制中心访问图形化的 YaST 配置对话框。选择 *安全性和用户 > 防火墙*。该配置分为 7 个部分，可以在屏幕左侧的树结构上直接访问它们。

#### 币篮

在该对话框中设置启动行为。在默认安装中将自动启动 `SUSEfirewall12`。也可以在这里启动和停止防火墙。要在正在运行的防火墙上实施新的设置，请使用 *保存设置并立刻重新启动防火墙*。

#### 接口

这里列出了所有已知的网络接口。要从区域中删除某接口，请选择此接口，并在按 *更改* 后选择 *未指派任何区域*。要向区域中添加某接口，请选择此接口，并在按 *更改* 后选择任一可用区域。也可以使用 *自定义* 来创建一个采用您自己的设置的特殊接口。

#### 允许的服务

您需要此选项来从自己的系统向受保护区域提供服务。默认情况下，服务器仅免受外部区域的影响。明确允许使用外部主机可用的服务。在 *所选区域允许的服务* 中选择所需的区域后，激活该列表中的服务。

#### 伪装

对外部网络（例如因特网），伪装隐藏您的内部网络，但内部网络中的主机可以透明地访问外部网络。伪装将阻止从外部网络到内部网络的请求，而发自内部网络的请求从外部来看好像是由伪装服务器发出的。如果需要使

外部网络能够使用内部计算机的特殊服务，则可以为服务添加特殊重定向规则。

### 广播

在该对话框中配置允许广播的 UDP 端口。将所需的各个端口号或服务添加到适当区域，以空格分隔。另请参见文件 `/etc/services`。

可以在这里启用未接受的广播日志记录。这样做可能会出现问题，因为 Windows 主机使用广播来互相识别，从而生成许多未接受的包。

### IPsec 支持

在此对话框中配置是否允许从外部网络使用 IPsec 服务。在*细节*下配置可信的包。

### 日志记录级别

对于登录有两条规则：已接受和未接受的包。未接受的包为 **DROPPED** 或 **REJECTED**。可以为这两种包选择*全部记录*、*只记录关键信息*或*不记录任何信息*。

完成防火墙配置后，选择下一步退出此对话框。然后打开面向区域的防火墙配置概要。在其中检查所有的设置。所有已允许使用的服务、端口和协议均在此概要中列出。要修改配置，请使用*后退*。按*接受*即可保存您的设置。

## 43.4.2 手动配置

以下段落提供进行成功配置的分步说明。每个配置项都根据该项是与防火墙有关还是与伪装有关作了相应标记。如果适用，请使用端口范围（例如 500:510）。这里未涉及配置文件中提到的与 DMZ（网络隔离区）相关的内容。这些内容只适用于大型组织中较复杂的网络基础结构（公司网络），这需要大量配置以及对此主题的深入了解。

首先，使用 YaST 模块系统服务（运行级别）以您的运行级别（很可能是 3 或 5）启用 SUSEfirewall2。这会在 `/etc/init.d/rc?.d/` 目录中设置 SUSEfirewall2\_\* 脚本的符号链接。

### FW\_DEV\_EXT（防火墙，伪装）

链接到因特网的设备。对于调制解调器连接，请输入 `ppp0`。对于 ISDN 链接，请使用 `ipp0`。DSL 连接使用 `dsl0`。指定 `auto` 使用与默认路由对应的接口。

#### FW\_DEV\_INT ( 防火墙, 伪装 )

链接到内部专用网络的设备 ( 如 `eth0` )。如果内部网络不存在, 防火墙只保护它运行所在的主机, 则应将此项保留为空白。

#### FW\_ROUTE ( 防火墙, 伪装 )

如果需要伪装功能, 请将此项设置为 `yes`。内部主机对外将是不可见的, 因为因特网路由器将忽略内部主机的专用网络地址 ( 例如 `192.168.x.x` )。

对于未使用伪装功能的防火墙而言, 只有在您希望允许访问内部网络时才应将此项设置为 `yes`。在此情况下, 内部主机需要使用正式注册的 IP 地址。但在通常情况下, 应禁止从外部访问您的内部网络。

#### FW\_MASQUERADE ( 伪装 )

如果需要伪装功能, 则将此项设置为 `yes`。这实际上为内部主机提供了与因特网的直接连接。但更保险的做法是在内部网络主机和因特网主机之间设置代理服务器。代理服务器提供的服务不需要伪装。

#### FW\_MASQ\_NETS ( 伪装 )

指定要伪装的主机或网络, 各个项之间要留有空格。例如:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

#### FW\_PROTECT\_FROM\_INT ( 防火墙 )

将此项设置为 `yes` 可以保护防火墙主机免遭来自内部网络的攻击。只有已经显式启用服务, 才可以在内部网络中使用这些服务。另请参见

`FW_SERVICES_INT_TCP` 和 `FW_SERVICES_INT_UDP`。

#### FW\_SERVICES\_EXT\_TCP ( 防火墙 )

输入应该可用的 **TCP** 端口。对于不应提供任何服务的家用普通工作站, 应将此项保留为空白。

#### FW\_SERVICES\_EXT\_UDP ( 防火墙 )

除非您运行 **UDP** 服务并希望此服务对外部可用, 否则将此项保留为空白。使用 **UDP** 的服务包括 **DNS** 服务器、**IPsec**、**TFTP**、**DHCP** 等。在此情况下, 请输入要使用的 **UDP** 端口。

#### FW\_SERVICES\_INT\_TCP ( 防火墙 )

使用此变量定义可用于内部网络的服务。变量表示法与

`FW_SERVICES_EXT_TCP` 的表示法相同, 但变量设置适用于内部网络。只有在 `FW_PROTECT_FROM_INT` 设置为 `yes` 时才需要设置此变量。

FW\_SERVICES\_INT\_UDP ( 防火墙 )  
请参见 FW\_SERVICES\_INT\_TCP。

配置防火墙后, 请测试您的设置。以 root 身份输入 `SUSEfirewall2 start` 可创建防火墙规则集。然后, 举例来说, 可以从外部主机使用 `telnet` 查看是否确实会拒绝连接。此后, 请查看 `/var/log/messages`, 应能看到如下所示的内容:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFAULT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEB00000000001030300)
```

用于测试您的防火墙设置的其他包有 `nmap` 或 `nessus`。在安装相应的包后, `nmap` 的文档位于目录 `/usr/share/doc/packages/nmap` 中, `nessus` 的文档位于目录 `/usr/share/doc/packages/nessus-core` 中。

## 43.5 有关详细信息

`/usr/share/doc/packages/SuSEfirewall2` 中提供了有关 `SUSEfirewall2` 包的最新信息和其他文档。`netfilter` 和 `iptables` 项目的主页 <http://www.netfilter.org> 以多种语言提供了丰富的文档资料。





## SSH：安全性网络操作

随着在联网环境中安装的计算机越来越多，常常需要从远程位置访问主机。通常，这意味着用户要发送登录名和密码字符串进行身份验证。只要以明文形式传送这些字符串，攻击者就可能会截获并恶意使用这些字符串获取对该用户帐户的访问权，而授权用户根本毫无察觉。一旦得逞，攻击者不仅可以控制所有用户文件，还可能利用此非法帐户获取管理员或 `root` 访问权，或侵入其他系统。过去常用 `telnet` 建立远程连接，但该程序没有采用加密形式或其他安全机制防止窃听。还存在其他未加保护的通讯信道，例如传统的 `FTP` 协议和某些远程复制程序。

SSH 套件通过对身份验证字符串（通常由登录名和密码构成）及主机间交换的所有其他数据进行加密，能够提供必要的保护。使用 SSH，虽然第三方仍可以记录数据流，但内容是经过加密的，除非了解加密钥，否则无法将其还原为明文。这样，SSH 在不安全的网络（如因特网）上实现了安全通讯。SUSE Linux Enterprise 附带的 SSH 程序是 `OpenSSH`。

### 44.1 OpenSSH 包

SUSE Linux Enterprise 会在默认情况下安装 `OpenSSH` 包。安装之后即可由程序 `ssh`、`scp` 和 `sftp` 来替代 `telnet`、`rlogin`、`rsh`、`rcp` 和 `ftp`。在默认配置中，只能使用 `OpenSSH` 实用程序访问 SUSE Linux Enterprise 系统，而且只能在防火墙允许访问的情况下访问。

## 44.2 ssh 程序

使用 ssh 程序可以登录到远程系统并以交互方式工作。该程序取代了 telnet 和 rlogin。slogin 程序只是指向 ssh 的符号链接。例如，使用命令 sshsun 登录到主机 sun。该主机随后提示输入 sun 上的密码。

通过身份验证后，既可以使用远程命令行操作，也可以使用 YaST 之类的交互式应用程序操作。如果本地用户名不同于远程用户名，则可以使用不同的登录名通过 ssh-l augustine sun 或 sshaugustine@sun 登录。

此外，ssh 还提供了在远程系统上运行命令的功能（也就是 rsh 提供的功能）。下例在主机 sun 上运行命令 uptime 并创建了一个名为 tmp 的目录。程序输出显示在主机 earth 的本地终端上。

```
ssh otherplanet "uptime; mkdir tmp"
Password:
1:21pm up 2:17, 9 users, load average: 0.15, 0.04, 0.02
```

在此需要加引号，以便使用一个命令同时发送两条指令。只有加引号才能在 sun 上执行第二个命令。

## 44.3 scp — 安全复制

使用 scp 可以将文件复制到远程计算机。该程序取代了 rcp，是一个既安全又有加密功能的程序。例如，scpMyLetter.tex sun: 可以将文件 MyLetter.tex 从主机 earth 上复制到主机 sun 上。如果 earth 上的用户名不同于 sun 上的用户名，请使用 username@host 格式指定后者的用户名。此命令没有 -l 选项。

输入正确的密码后，scp 开始传送数据，同时显示一行不断增多的星号来模拟进度条。此外，该程序还能显示到达进度条右端的估计时间。通过提供选项 -q 可以取消显示所有输出。

scp 还提供了对整个目录的递归复制功能。命令 scp-r src/ sun:backup/ 可以将目录 src 的全部内容（包含所有子目录）都复制到主机 sun 上的 backup 目录。这个子目录若不存在，就会自动创建该子目录。

选项 `-p` 指示 `scp` 不更改文件的时间戳。`-c` 将对传送数据进行压缩。这会最大限度地减少要传送的数据量，但同时增加了处理器的负担。

## 44.4 sftp — 安全的文件传送

`sftp` 程序可以取代 `scp` 来执行安全的文件传送。在 `sftp` 会话期间，您可以使用许多来自 `ftp` 的命令。`sftp` 程序可能要优于 `scp`，特别是在传送文件名未知的数据时。

## 44.5 SSH 守护程序 (sshd) — 服务器端

要使用 SSH 客户程序 `ssh` 和 `scp`，必须在后台运行服务程序（即 SSH 守护程序），用于监听 TCP/IP port 22 上的连接。首次启动该守护程序时将生成三个密钥对。各密钥对均由私用密钥和公钥组成。因此，通常提到该过程，就认为它是基于公共密钥的。要保证通过 SSH 安全地通讯，必须限制只有系统管理员才能访问私用密钥文件。文件权限是在默认安装中相应设置的。只有在本地 SSH 守护程序才需要私用密钥，切勿将私用密钥提供给其他任何人。公钥组件（可通过扩展名 `.pub` 识别）将被发送到请求连接的客户机。所有用户都可以读取公钥组件。

连接请求是 SSH 客户机发出的。正在等待的 SSH 守护程序将与请求连接的 SSH 客户程序交换标识数据以比较协议和软件版本，防止通过错误的端口连接。由于请求是由最初的 SSH 守护程序的子进程回复的，所以可以同时建立多个 SSH 连接。

对于 SSH 服务器和 SSH 客户机间的通讯，OpenSSH 支持使用版本 1 和版本 2 的 SSH 协议。默认情况下使用的是版本 2 的 SSH 协议。用 `-1` 开关可以覆盖此默认设置，转而使用该协议的版本 -1。要在系统更新后继续使用版本 1，则请遵循 `/usr/share/doc/packages/openssh/README.SuSE` 中的指示信息。本文档还介绍了如何只通过几个步骤就将 SSH 1 环境转换为有效的 SSH 2 环境。

如果使用 SSH 版本 1，服务器将发送其公共主机密钥和一个服务器密钥（由 SSH 守护程序每小时重新生成一次）。这两个密钥都允许 SSH 客户机对自由选择的会话密钥加密（会话密钥会被发送到 SSH 服务器）。SSH 客户机还会通知服务器使用哪种加密方法（加密法）。

版本 2 的 SSH 协议不需要服务器密钥。但服务器端和客户端都要使用符合 Diffie-Helman 的算法来交换它们的密钥。

一定要使用私用主机密钥和服务器密钥对会话密钥解密，从公钥根本无法得出这些密钥。只有建立联系的 SSH 守护程序才能使用其私用密钥对会话密钥解密（请参见 `man/usr/share/doc/packages/openssh/RFC.nroff`）。打开 SSH 客户机的冗长调试选项 `-v` 可以密切监视初始阶段的连接。

在与远程主机首次建立联系之后，客户机会将所有公共主机密钥储存在 `~/.ssh/known_hosts` 中。这会防止各种中间人攻击 — 外部 SSH 服务器试图使用伪造名称和伪造 IP 地址侵入系统。如果 `~/.ssh/known_hosts` 未包含某个主机密钥，或是因未能提供正确的私钥致使服务器无法对会话密钥解密，这两种情况下都可以检测到此类攻击。

建议将储存在 `/etc/ssh/` 中的私用密钥和公钥备份到安全的外部位置。这样就可以检测到密钥修改，并可以在重装后再次使用旧密钥。用户也就无需了解那些含糊不清的警告了。如果经过校验（尽管有警告）得知这确实是正确的 SSH 服务器，则必须从 `~/.ssh/known_hosts` 中删除有关此系统的现有项。

## 44.6 SSH 身份验证机制

现在开始执行实际的身份验证，最简单的身份验证形式就是上文提到的输入密码。SSH 的目的是提供安全且方便使用的软件。由于 SSH 是用来取代 `rsh` 和 `rlogin` 的，所以 SSH 必须也能提供一种适合日常使用的身份验证方法。SSH 是通过另一个密钥对（由用户生成）来实现该功能的。为此，SSH 包提供了一个帮助程序：`ssh-keygen`。输入 `ssh-keygen-t rsa` 或 `ssh-keygen-t dsa` 后就会生成密钥对，同时系统会提示您输入储存密钥所用的基本文件名。

确认默认设置并回应针对通行密码的请求。即使软件建议输入空的通行密码，仍建议您为此处说明的过程输入一个 10 到 30 个字符的通行密码。请不要使用简短的单词或短语。再次输入通行密码进行确认。随后，您将看到私钥和公钥的储存位置，在本例中为文件 `id_rsa` 和 `id_rsa.pub`。

使用 `ssh-keygen-p -t rsa` 或 `ssh-keygen-p -t dsa` 更改旧通行密码。将公钥组件（本例中为 `id_rsa.pub`）复制到远程计算机并保存到 `~/.ssh/authorized_keys` 中。下次建立连接时，系统将要求您使用通行密码对自身进行身份验证。如果系统没有要求身份验证，请校验这些文件的位置和内容。

从长期看，此过程比每次提供密码要麻烦。所以，SSH 包提供了另一种工具 `ssh-agent`，该工具可以在 X 会话期间保留私用密钥。整个 X 会话作为 `ssh-agent` 的子进程启动。为此，最简单的方法是将 `.xsession` 文件开始位置的变量 `usessh` 设置为 `yes` 并通过显示管理器（如 KDM 或 XDM）登录。也可以输入 `ssh-agentstartx`。

现在您就可以像平常那样使用 `ssh` 或 `scp` 了。如果按上文所述分发了公钥，系统就不再提示您输入密码。终止 X 会话或用密码保护应用程序（如 `xlock`）锁定该会话时一定要小心。

文件 `/usr/share/doc/packages/openssh/README.SuSE` 还介绍了由于引入版本 2 的 SSH 协议而产生的所有相关更改。

## 44.7 X、身份验证和转发机制

除上述有关安全方面的改进之外，SSH 还简化了远程 X 应用程序的用法。如果运行带选项 `-X` 的 `ssh`，远程计算机上会自动设置 `DISPLAY` 变量，而且所有 X 输出都将通过现有 SSH 连接导出到远程计算机上。同时，如果未经授权，其他人将无法截获通过此方法远程启动并在本地查看的 X 应用程序。

通过添加选项 `-A`，可以将 `ssh-agent` 身份验证机制转移到下一台计算机上。这样，您就可以在不同计算机上工作而无需输入密码，但前提是：已将公钥分发给目标主机并在其上正确保存。

上述两种机制在默认设置中均处于取消激活状态，但可以随时在全系统范围的配置文件 `/etc/ssh/sshd_config` 或用户的 `~/.ssh/config` 中永久激活这两种机制。

`ssh` 还可用于重定向 TCP/IP 连接。在下例中，SSH 分别用于重定向 SMTP 和 POP3 端口：

```
ssh -L 25:sun:25 earth
```

使用此命令，可以通过加密信道将定向到 `earth` 端口 25 (SMTP) 的任何连接重定向到 `sun` 上的 SMTP 端口。如果用户所用的 SMTP 服务器不具备 SMTP-AUTH 或 POP-before-SMTP 功能，此命令特别有用。从与网络相连的任意位置都可以将电子邮件传送到“家庭”邮件服务器进行递送。同样，使用以下命令，可以将 `earth` 上的所有 POP3 请求（端口 110）转发给 `sun` 的 POP3 端口：

```
ssh -L 110:sun:110 earth
```

必须以 `root` 身份执行这两个命令，因为连接指向有特权的本地端口。普通用户通过现有 **SSH** 连接发送和检索电子邮件。为此，必须将 **SMTP** 和 **POP3** 主机设置为 `localhost`。有关其他信息，请参见上述每个程序的手册页以及 `/usr/share/doc/packages/openssh` 下的文件。

## 网络身份验证 — Kerberos

除了通常的密码机制外，开放网络没有提供任何其他方法来确保工作站能够正确识别其用户。在一般的安装中，用户每次访问网络中的服务时都必须输入密码。Kerberos 提供了一种认证方法，采用这种方法，用户只要注册一次，就可整个网络中获得信任以完成会话的剩余操作。要拥有安全的网络，必须满足以下要求：

- 使所有用户可以对每个所需服务证明他们自己的身份，并确保任何用户都不能使用其他用户的身份。
- 确保每个网络服务器也能证明其身份。否则攻击者就可能冒充服务器并获取传送给服务器的敏感信息。这种概念被称为*相互认证*，因为在客户机和服务器之间进行了相互认证。

Kerberos 通过提供严格加密的认证来帮助您满足这些要求。下面内容说明这是如何实现的。这里仅讨论 Kerberos 的基本原理。有关详细的技术说明，请参考随 Kerberos 的实施提供的文档。

### 45.1 Kerberos 术语

以下词汇表定义了一些 Kerberos 术语。

#### 身份凭证

用户或客户机需要提交某些身份凭证方可获得请求服务的授权。Kerberos 采用两种身份凭证 — 票证和身份验证器。

## 票证

票证是随服务器而不同的身份凭证，客户机使用票证在它请求提供服务的服务器上认证。它包含服务器的名称、客户机的名称、客户机的因特网地址、时戳、使用期限和随机会话密钥。所有这些数据都使用服务器的密钥进行了加密。

## 认证器

与票证相结合，认证器用于证明提交票证的客户机确实与其声称的身份相符。身份验证器由客户机名称、工作站 IP 地址、当前工作站时间组成。这些内容都使用会话密钥进行了加密，只有客户机和它请求提供服务的服务器才知道此密钥。与票证不同，身份验证器只能使用一次。客户机可以自己构建认证器。

## 主体

Kerberos 主体是可以对其指派票证的独特实体（用户或服务）。主体包含以下部分：

- **主部** — 主体的第一部分，如果主体是用户，则主部可以与您的用户名相同。
- **实例** — 描述主部属性的一些可选信息。此字符串和主部之间用一个 / 分隔。
- **Realm** — 指定您的 Kerberos 领域。通常情况下，领域就是您的大写域名。

## 相互认证

Kerberos 确保客户机和服务器都可以确定对方的身份。它们共享一个用来安全通讯的会话密钥。

## 会话密钥

会话密钥是由 Kerberos 生成的临时性私用密钥。客户机知道这些密钥。当客户机向服务器请求并收到票证后，将使用这些密钥来加密客户机和服务器之间的通讯。

## 重放

几乎所有在网络中发送的消息都能够被窃听、盗取和重发送。在使用 Kerberos 的情况下，如果攻击者获取了包含您的票证和认证器的服务请求，则会非常危险。他随后可能会试图重发送此请求（重放）来冒充您。然而，Kerberos 实施了多种机制来解决此问题。



服务器或服务

服务用来指要执行的特定操作。此操作背后的进程被称为服务器。

## 45.2 Kerberos 的工作原理

Kerberos 通常被称为第三方可信认证服务，这意味着其所有客户机都信任 Kerberos 对另一个客户机身份的判断。Kerberos 保存着一个包含它的所有用户及其私用密钥的数据库。

要确保 Kerberos 值得信任，需要在一台专用计算机上运行认证和票证授予服务器。确保只有管理员能直接或通过网络访问此计算机。同时将在此计算机上运行的（网络）服务的数目降到最低 — 甚至可以不运行 sshd。

### 45.2.1 首次接触

在首次接触 Kerberos 时，您的操作与在常规网络系统进行的任何登录过程类似。输入您的用户名。这一信息和票证授予服务的名称被发送到身份验证服务器 (Kerberos)。如果认证服务器确定了您的身份，则它会生成一个随机的会话密钥，供以后在客户机和票证授予服务器之间使用。身份验证服务器现在将为票证授予服务器准备一个票证。该票证包含以下信息 — 都用会话密钥加密过，该密钥只有认证服务器和授予票证的服务器知道：

- 客户机和票证授予服务器的名称
- 当前时间
- 为此票证指派的有效期
- 客户机的 IP 地址
- 新生成的会话密钥

随后，还是以加密形式将此票证与会话密钥一起发送回客户机，但这次使用的是客户机的私用密钥。只有 Kerberos 和客户机知道此私用密钥，因为它是从您的用户密码派生的。由于客户机已经收到了此响应，计算机将提示您输入密码。此密码被转换为一个密钥，利用它可解密认证服务器所发送的包。然后“解开”此包，并将密码和密钥从工作站的内存中删除。只要没有超过为用于获取其他票证的那个票证指定的有效期，工作站就能证明您的身份。

## 45.2.2 请求服务

要从网络中的任何服务器请求服务，客户机应用程序都需要向服务器证明其身份。因此，此应用程序生成一个认证器。认证器包含以下部分：

- 客户机的主体
- 客户机的 IP 地址
- 当前时间
- 校验和（由客户机选择）

所有这些信息都使用客户机为这个特殊服务器接收到的会话密钥进行了加密。用于服务器的身份验证器和票证会被发送到该服务器。该服务器使用自己的会话密钥副本来解密认证器，而该认证器为它提供所需的与请求其服务的客户机相关的所有信息，然后服务器将这些信息与票证中包含的信息进行对比。服务器将检查票证和认证器是否来自同一客户机。

如果在服务器端没有采取任何安全措施，则这一阶段是回放攻击的理想目标。某些人可能试图重发先前从网络上窃取的请求。为防止出现这种情况，服务器将不接受具有先前已收到过的时戳和票证的任何请求。此外，忽略时间戳与接收请求时的时间相差太大的请求。

## 45.2.3 相互身份验证

Kerberos 认证可以双向使用。这不仅是客户机是否是它所声称的那台客户机的问题。服务器本身也应能够向请求其服务的客户机认证自己。因此，它本身也将发送某种认证器。它将在客户机的身份验证器中接收的校验和加 1，然后使用它和客户机共享的会话密钥对其加密。客户机将此响应作为对服务器的真实性的校验，然后它们开始协作。

## 45.2.4 票证授予 — 联系所有服务器

设计票证一次用于一个服务器。这意味着您每次请求其他服务都必须获得新的票证。Kerberos 实施了一种机制来获取用于各个服务器的票证。这种服务被称为“票证授予服务”。票证授予服务与前面提到的任何服务一样，因此也使用已

介绍过的相同的访问协议。当应用程序需要一个尚未请求过的票证时，就会联系票证授予服务器。此请求包含以下部分：

- 被请求的主体
- 票证授予票证
- 认证器

与任何其他服务器一样，票证授予服务器现在将检查票证授予票证和身份验证器。如果确定它们有效，票证授予服务器将构建一个将在原始客户机和新服务器之间使用的新会话密钥。然后构建用于新服务器的票证，其中包含以下信息：

- 客户机的主体
- 服务器的主体
- 当前时间
- 客户机的 IP 地址
- 新生成的会话密钥

为新票证指派一个有效期，该有效期是票证授予票证的剩余有效期和服务的默认有效期二者中较短的一个。客户机接收此票证和会话密钥，它们是由票证授予服务发送的，但这次使用随原始票证授予票证一起提供的会话密钥来对响应进行加密。当联系新服务时，客户机可以解密此响应而不需要用户的密码。Kerberos 从而可以一个接一个地获取用于客户机的票证，而无需在登录时多次麻烦用户。

## 45.2.5 与 Windows 2000 的兼容性

Windows 2000 中包含了 Kerberos 5 的 Microsoft 实施。因为 SUSE Linux Enterprise® 使用 Kerberos 5 的 MIT 实现，请在 MIT 文档中寻找有用信息和指南。请参见第 45.4 节“有关详细信息”[758]。

## 45.3 从用户的角度讨论 Kerberos

理想情况下，用户与 Kerberos 的唯一接触是在工作站登录时发生的。登录进程包括获得一个票证授予票证。注销时，用户的 Kerberos 票证会自动损坏，这样其他人就不能模仿该用户。当用户的登录会话持续时间超过为票证授予的票证的最长时间限制时（合理的设置是 10 小时），票证的自动到期会带来一些不便因素。但用户可以通过运行 `kinit` 来获得一个新的票证授予票证。再次输入密码，Kerberos 无需其他认证即可获得对所需服务的访问。要获得由 Kerberos 为您静默获取的所有票证的列表，请运行 `klist`。

这里有一个短列表，列出了使用 Kerberos 身份验证的一些应用程序。在 `/usr/lib/mit/bin` 或 `/usr/lib/mit/sbin` 下可以找到这些应用程序。它们拥有普通 UNIX 和 Linux 应用程序的所有功能，同时具有由 Kerberos 管理的透明认证：

- `telnet`、`telnetd`
- `rlogin`
- `rsh`、`rcp`、`rshd`
- `ftp`、`ftpd`
- `ksu`

您再也不必为了使用这些应用程序而输入密码，因为 Kerberos 已经证明了您的身份。如果在具有 Kerberos 支持的情况下进行编译，`ssh` 甚至可以将为一个工作站获得的所有票证转发到另一个工作站。如果使用 `ssh` 登录到另一个工作站，`ssh` 将确保票证的加密内容会根据新情况而调整。仅在工作站之间复制票证是不够的，因为票证中包含工作站特定信息（IP 地址）。XDM、GDM 和 KDM 也提供 Kerberos 支持。请阅读<http://web.mit.edu/kerberos> 处的 *kerberos v5 unix 用户指南* 中有关 Kerberos 网络应用程序的更多信息。

## 45.4 有关详细信息

MIT Kerberos 的官方网站是<http://web.mit.edu/kerberos>。因此，找出任何有关 Kerberos（包括 Kerberos 安装、用户和管理指南）的任何其他相关资源的链接。

<ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS> 处的文章提供了对 Kerberos 基本原理的十分宽泛的、非常易于理解的见识。它还提供了许多进一步研究和了解 Kerberos 的资源。

Kerberos FAQ 的官方网站是 <http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>。Brian Tung 编著的 *Kerberos — 网络身份验证系统* 一书 (ISBN 0-201-37924-4) 提供了深入和全面的信息。



## 安装和管理 Kerberos

本节介绍 MIT Kerberos 实施的安装以及一些管理方面的问题。本节假定您熟悉 Kerberos 的基本概念（另请参见第 45 章 *网络身份验证 — Kerberos* [753]）。

### 46.1 选择 Kerberos 领域

Kerberos 安装的域被称为领域，并由一个名称来标识，如 `FOOBAR.COM` 或更简单的 `ACCOUNTING`。Kerberos 是区分大小写的，所以 `foobar.com` 实际上是一个与 `FOOBAR.COM` 不同的领域。您可根据自己的偏好选择使用大小写。但通常的做法是使用大写领域名。

使用您的 DNS 域名（或子域，如 `ACCOUNTING.FOOBAR.COM`）也是个不错的选择。如下所示，如果将 Kerberos 客户机配置为通过 DNS 来查找 KDC 和其他 Kerberos 服务，则系统管理员的工作就轻松多了。要做到这一点，则使您的领域名是 DNS 域名的子域。

与 DNS 名称空间不同，Kerberos 是不分级的。您不能设置一个名为 `FOOBAR.COM` 的领域并在其下设置两个名为 `DEVELOPMENT` 和 `ACCOUNTING` 的“子领域”并期望这两个从属领域会以某种方式从 `FOOBAR.COM` 继承主体。相反，应设置 3 个单独的领域，而且必须为其配置跨领域身份验证，这样，一个领域的用户才能与另一个领域的服务器或其他用户进行交互。

为了便于说明，假定您只为整个组织设置一个领域。在本章剩余部分中，将在所有示例中使用领域名 `SAMPLE.COM`。

## 46.2 设置 KDC 硬件

要使用 Kerberos，首先需要一台用作密钥分发中心（或简称 KDC）的计算机。这台计算机将储存整个 Kerberos 用户数据库，其中包含密码和所有信息。

KDC 是安全基础结构中最重要的一部分 — 如果有人侵入，则 Kerberos 保护的所有用户帐户和基础结构都会受到危害。能够访问 Kerberos 数据库的攻击者可以冒充数据库中的任何主体。所以应尽可能提高此计算机的安全性：

- 1 将服务器计算机放在一个以物理方式保护的位置，如只有极少数人才可进入的加锁服务器室。
- 2 除了 KDC 以外，不要在它上面运行任何网络应用程序。其中包括服务器和客户机 — 例如，KDC 不应通过 NFS 导入任何文件系统或使用 DHCP 检索其网络配置。
- 3 首先安装最小系统，然后检查已安装的包列表并除去任何不需要的包。其中包括服务器（如 `inetd`、`portmap` 和 `cups`）以及基于 X 的任何服务器。甚至安装 SSH 服务器也应该考虑是一个潜在的安全性风险。
- 4 在此计算机上不提供图形登录，因为 X 服务器具有潜在的安全风险。Kerberos 提供它自己的管理界面。
- 5 将 `/etc/nsswitch.conf` 配置为仅使用本地文件进行用户和组查找。将 `passwd` 和 `group` 的行进行如下更改：

```
passwd:      files
group:       files
```

在 `/etc` 中编辑 `passwd`、`group`、`shadow` 和 `gshadow` 文件，并删除任何以 `+` 字符开头的行（这些行用于 NIS 查找）。

- 6 禁用除 `root` 用户帐户外的所有用户帐户，方法是编辑 `/etc/shadow` 并用 `*` 或 `!` 字符。



## 46.3 时钟同步

要成功使用 Kerberos，应确保您的组织内的所有系统时钟都在给定范围内同步。这一点非常重要，因为 Kerberos 需要防范重放的身份凭证。攻击者可能会在网络上获取 Kerberos 身份凭证，并再使用它们来攻击服务器。Kerberos 采取多种保护措施进行防范。其中之一是在它们的票证中放入时间戳。如果服务器收到的票证的时间戳与当前时间不同，就会拒绝此票证。

Kerberos 在比较时间戳时允许一定的偏差。但计算机时钟的走时可能非常不准确 — 在一周内快或慢半个小时并不罕见。因此，应对网络上的所有主机进行配置，使它们的时钟与中央时间源同步。

实现此做法的简单方法就是在一台计算机上安装 NTP 时间服务器，并使所有客户机的时钟与该服务器同步。要做到这一点，要么在所有这些计算机上以客户机方式运行一个 NTP 守护程序，要么每天一次从所有客户机运行 `ntpdate`（此解决方案可能仅适用于客户机数量较少的情况）。KDC 本身也需要与公用时间源同步。因为在此计算机上运行 NTP 守护程序会有安全风险，可能通过 `cron` 项运行 `ntpdate` 以执行此操作是一个好主意。要将您的计算机配置成 NTP 客户机，如第 32.1 节“使用 YaST 配置 NTP 客户机”[549]中概述的那样继续操作。

也可以调整 Kerberos 在检查时间戳时所允许的最大偏差。此值（称为*时钟扭斜*）可以在 `krb5.conf` 文件中进行设置，请参见第 46.5.3 节“调整时钟扭斜”[768]一节。

## 46.4 配置 KDC

本节介绍 KDC 的初始配置和安装，包括创建管理主体。此过程包括几个步骤：

- 1 安装 RPM** 在指定为 KDC 的计算机上，安装特殊的软件包。有关详细信息，请参见第 46.4.1 节“安装 RPM”[764]。
- 2 调整配置文件** 必须为您的方案调整配置文件 `/etc/krb5.conf` 和 `/var/lib/kerberos/krb5kdc/kdc.conf`。这些文件 KDC 上的所有信息。
- 3 创建 Kerberos 数据库** Kerberos 保持所有主体标识和需要被认证的所有主体密码的数据库。

- 4 **调整 ACL 文件：添加管理员** 可以远程管理 KDC 上的 Kerberos 数据库。要防止未授权的主体篡改数据库，Kerberos 使用访问控制列表。您必须为管理主体启用远程访问使他能够管理数据库。
- 5 **调整 Kerberos 数据库：添加管理员** 您至少需要一个管理主体来运行和管理 Kerberos。必须在启动 KDC 之前添加了该主体。
- 6 **启动 Kerberos 守护程序** 一旦安装了 KDC 软件并且正确配置了，就可以启动 Kerberos 守护程序为您的领域提供 Kerberos 服务。
- 7 **为您自己创建主体**

## 46.4.1 安装 RPM

安装 RPM 之前，应首先安装 Kerberos 软件。在 KDC 上安装包 krb5、krb5-server 和 krb5-client。

## 46.4.2 设置数据库

下一步是初始化 Kerberos 用来保存所有主体信息的数据库。设置数据库主密钥，此密钥用于保护数据库不会被意外泄漏，特别是当它在备份到磁带时。主密钥是从密码短语派生的，储存在名为暂存文件的文件中。这就是您每次重新启动 KDC 时无需键入密码的原因。确保选择一个适当的通行密码，如从一本书随机打开的一页中找出一句话。

在对 Kerberos 数据库 (/var/lib/kerberos/krb5kdc/principal) 进行磁带备份时，切勿备份暂存文件（它位于 /var/lib/kerberos/krb5kdc/.k5.EXAMPLE.COM 中）。否则，能够读到此磁带的所有人都可以解密数据库。因此，将通行密码副本保存在安全位置也是一个很好的选择，因为在系统崩溃后从备份磁带恢复数据库时将用到它。

要创建暂存文件和数据库，请运行：

```
$> kdb5_util create -r EXAMPLE.COM -s
Initializing database '/var/lib/kerberos/krb5kdc/principal' for realm
'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
```

```
Enter KDC database master key: <= Type the master password.  
Re-enter KDC database master key to verify: <= Type it again.  
$>
```

要验证它执行的操作，请使用 `list` 命令：

```
$>kadmin.local  
kadmin> listprincs  
K/M@EXAMPLE.COM  
kadmin/admin@EXAMPLE.COM  
kadmin/changepw@EXAMPLE.COM  
krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

这表明数据库中现在有许多主体。所有这些主体由 Kerberos 内部使用。

## 46.4.3 创建主体

下一步，为自己创建两个 Kerberos 主体，一个常规主体用于日常工作，另一个用于与 Kerberos 相关的管理任务。假定您的登录名是 `newbie`，按以下步骤操作：

```
kadmin.local  
  
kadmin> ank newbie  
newbie@EXAMPLE.COM's Password: <type password here>  
Verifying password: <re-type password here>
```

接下来，创建名为 `newbie/admin` 的另一个主体，方法是在 `kadmin` 提示符处键入 `addnewbie/admin`。您的用户名的 `admin` 后缀指定了您的角色。稍后在管理 Kerberos 数据库时将使用此角色。一个用户可以有用于不同目的的多个角色。基本上，角色是具有类似名称的完全不同的帐户。

## 46.4.4 启动 KDC

启动 KDC 守护程序和 Kadmin 守护程序。要手动启动此守护程序，请输入 `rckrb5kdc start` 和 `rckadmind start`。还请确保当使用命令 `insserv krb5kdc` 和 `insserv kadmind` 重引导计算机时，会默认启动 KDC 和 `kadmind`。

## 46.5 手动配置 Kerberos 客户机

在配置 Kerberos 时，基本上可以采用两种方法 — 在 `/etc/krb5.conf` 文件进行静态配置或使用 DNS 进行动态配置。采用 DNS 配置时，Kerberos 应用程序会尝试使用 DNS 记录查找 KDC 服务。采用静态配置时，将您的 KDC 服务器的主机名添加到 `krb5.conf`（并在移动 KDC 或以其他方式重配置领域时更新文件）。

基于 DNS 的配置通常比较灵活，而且每台计算机的配置工作量也少得多。但要求您的领域名与您的 DNS 域相同或是它的子域。通过 DNS 配置 Kerberos 也会产生一个较小的安全问题 — 攻击者能够通过 DNS 严重扰乱您的基础结构（使名称服务器无效、窃取 DNS 记录等）。但这最多只会造成服务被拒绝。除非在 `krb5.conf` 中输入 IP 地址而非主机名，否则静态配置也会发生相同的情况。

### 46.5.1 静态配置

配置 Kerberos 的一种方法是编辑配置文件 `/etc/krb5.conf`。默认安装的文件中包含多个示例项。在开始编辑前需要将所有这些项删除。`krb5.conf` 由多个节组成，每节由括在括号中的节名引入，如 `[this]`。

要配置您的 Kerberos 客户机，请将以下语句添加到 `krb5.conf`（其中 `kdc.sample.com` 是 KDC 的主机名）：

```
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc.example.com
        admin_server = kdc.example.com
    }
```

`default_realm` 行设置 Kerberos 应用程序的默认领域。如果您有多个领域，只需向 `[realms]` 节添加其他的语句。

此外还要向此文件添加一条语句，指示应用程序如何将主机名映射到领域。例如，当连接到远程主机时，Kerberos 库需要知道此主机位于哪个领域中。必须在 `[domain_realms]` 节中对此进行配置：

```
[domain_realm]
```

```
.example.com = EXAMPLE.COM  
www.foobar.com = EXAMPLE.COM
```

此语句向库说明 `example.com` DNS 域中的所有主机均位于 `SAMPLE.COM` Kerberos 领域中。此外，名为 `www.foobar.com` 的外部主机也应被视为 `EXAMPLE.COM` 领域的成员。

## 46.5.2 基于 DNS 配置

基于 DNS 的 Kerberos 配置大量使用 SRV 记录。请参见 *(RFC2052) 用于指定服务位置的 DNS RR*，网址是 <http://www.ietf.org>。这些记录在早期的 BIND 名称服务器实施中不受支持。这里要求至少为 BIND 版本 8。

对于 Kerberos 而言，SRV 记录的名称始终采用 `_service._proto.realm` 格式，其中的“realm”是 Kerberos 领域。DNS 中的域名是不区分大小写的，所以当使用这种配置方法时，Kerberos 领域将无法再区分大小写。`_service` 是一个服务名（例如当尝试联系 KDC 或密码服务时会使用不同的名称）。`_proto` 可以是 `_udp` 或 `_tcp`，但不是所有服务都支持这两种协议。

SRV 资源记录的数据部分包括一个优先级值、一个权重、一个端口号和一个主机名。优先级确定了主机被尝试的顺序（值越低则优先级越高）。权重用于支持优先级相同的服务器之间的某种负载平衡。您也许不需要它们，所以将它们设为 0 即可。

MIT Kerberos 当前查找服务时将查找以下名称：

### \_kerberos

它定义了 KDC 守护程序（身份验证和票证授予服务器）的位置。典型记录如下：

```
_kerberos._udp.EXAMPLE.COM. IN SRV 0 0 88 kdc.example.com.  
_kerberos._tcp.EXAMPLE.COM. IN SRV 0 0 88 kdc.example.com.
```

### \_kerberos-adm

它描述了远程管理服务的位置。典型记录如下：

```
_kerberos-adm._tcp.EXAMPLE.COM. IN SRV 0 0 749 kdc.example.com.
```

因为 `kadmind` 不支持 UDP，所以没有 `_udp` 记录。

与静态配置文件一样，这里也提供了一种机制来向客户机指示特定主机位于 EXAMPLE.COM 领域中，即使它不是 example.com DNS 域的一部分。通过将一个 TXT 记录附加到 \_keberos.hostname 即可做到这一点，如下所示：

```
_keberos.www.foobar.com. IN TXT "EXAMPLE.COM"
```

### 46.5.3 调整时钟扭斜

时钟偏差是不完全符合主机系统时钟的票据时戳的容差，超过此容差将不接受此票据。通常，将时钟扭斜设置为 300 秒（5 分钟）。这意味着从服务器的角度看，票证的时间戳与它的偏差可以是在前后 5 分钟内。

当使用 NTP 同步所有主机时，可以将此值减少为大约一分钟。可以在 /etc/krb5.conf 中设置时钟扭斜值，如下所示：

```
[libdefaults]
    clockskew = 120
```

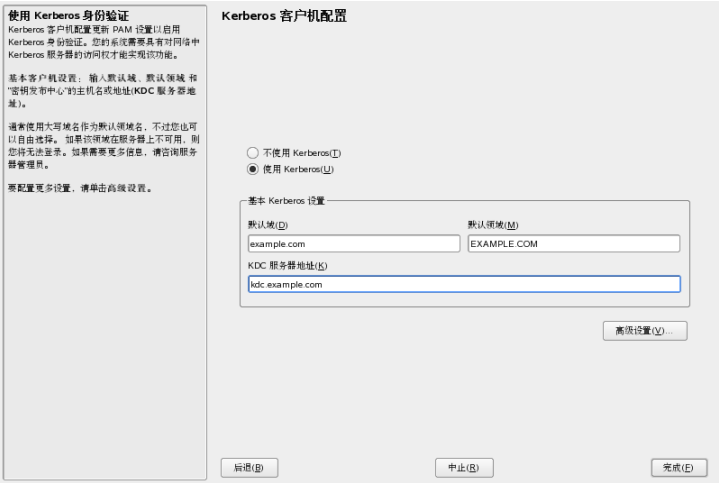
## 46.6 使用 YaST 配置 Kerberos 客户机

除上述手动配置外，还可以使用 YaST 来配置 Kerberos 客户机。按如下所示继续：

- 1 以 root 用户身份登录，然后选择 *网络服务 > Kerberos 客户机*。
- 2 选择 *使用 Kerberos*。
- 3 要配置基于 DNS 的 Kerberos 客户机，继续以下操作：
  - 3a 确认显示的基本 *Kerberos* 设置。
  - 3b 单击 *高级设置* 以配置与票有关的问题、OpenSSH 支持和时间同步的详细信息。
- 4 要配置静态 Kerberos 客户机，继续以下操作：

- 4a** 将默认域、默认领域和 *KDC* 服务器地址设置成与您的设置相匹配的值。
- 4b** 单击高级设置以配置与票有关的问题、OpenSSH 支持和时间同步的详细信息。

**图 46.1** *YaST: Kerberos 客户机的基本配置*



要在高级设置对话框中配置与票有关的选项，从以下选项选择：

- 以天、小时或分钟为单位（使用度量单位 *d*、*h* 和 *m*，值和单位之间没有空格）指定默认票证有效期和默认重生有效期。
- 要转发您的完整身份以便在其他主机上使用您的票证，请选择可转发。
- 通过选择可代理启用某些票证的传送。
- 通过启用保留，即使会话已经结束，也可以通过 PAM 模块使票证保持可用。
- 要为您的 OpenSSH 客户机启用 Kerberos 身份验证支持，请选择相应的复选框。随后，客户机使用 Kerberos 票证通过 SSH 服务器进行认证。

- 您可以使某个范围内的用户帐户不能使用 Kerberos 身份验证，方法是为此功能的用户必须具有的最小 *UID* 提供值。例如，您可能希望排除系统管理员 (*root*)。
- 最后，使用*时钟扭斜*来设置时间戳和您的主机系统时间之间可容许差异的值。
- 要保持系统时间与 NTP 服务器同步，还可以将主机设置为 NTP 客户机，方法是选择 *NTP 配置*，这会打开 YaST NTP 客户机对话框（请参见第 32.1 节“使用 YaST 配置 NTP 客户机”[549]）。在完成配置后，YaST 将执行所有必要的更改，然后就可以使用 Kerberos 客户机了。

图 46.2 YaST: Kerberos 客户机的高级配置

默认情况下，默认有效期、默认可更新有效期和时钟偏差的值以秒为单位。或者，可以指定时间单位 (a 表示分钟，h 表示小时，d 表示天) 并将时间单位用符号后缀 (例如，1d 或 24h 表示 1 天)。

使用可转发可以将您完整的身份 (TGT) 传递到另一台计算机。可代理仅允许传递 特定的票证。

如果启用了保留，则在关闭会话前 PAM 模块将保留票证。

要对 OpenSSH 客户机启用 Kerberos 支持，请选择 OpenSSH 客户机的 Kerberos 支持。在这种情况下，Kerberos 票证将用于 SSH 服务器上的用户身份验证。

当最小 UID 大于 0 时，将忽略 UID 小于指定数字的用户试图进行的身份验证。这在系统管理员 root 禁用 Kerberos 身份验证时很有用。

时钟偏差是不完全符合主机系统时钟的时差容错。单位为秒。

将您的时间与 NTP 服务器同步。请将计算机配置为 NTP 客户机。通过 NTP 配置访问此配置。

要配置用户帐户的原，请在配置用户数据中选择合适的配置模块。

高级 Kerberos 客户机配置

票证特性

默认有效期(D)

1d

默认可更新有效期(E)

1d

☒ 可转发(F)

☐ 可代理(G)

☐ 可保留(H)

☐ OpenSSH 客户机的 Kerberos 支持(I)

最小 UID(J)

1

时钟偏差(L)

300

NTP 配置(N)...

取消(O)

确定(P)

## 46.7 远程 Kerberos 管理

为了能够不直接访问 KDC 控制台而从 Kerberos 数据库添加和删除主体，请对 Kerberos 管理服务指示允许哪些主体执行哪些操作。通过编辑文件 `/var/lib/kerberos/krb5kdc/kadm5.acl` 完成此操作。ACL（访问控制列表）允许您精确指定特权。有关细节，请使用 `man 8 kadmin` 来参见手册页。

现在将以下行添加到此文件中，为您自己授予可以对数据库进行任何操作的特权：



```
newbie/admin *
```

用您自己的用户名替换 `newbie`。要使更改生效，请重新启动 `kadmind`。

## 46.7.1 使用 `kadmin` 进行远程管理

您现在应该能够使用 `kadmin` 工具远程执行 Kerberos 管理任务。首先，为您的 `admin` 角色获得一个票证，并在连接到 `kadmin` 服务器时使用此票证：

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:
kadmin: getprivs
current privileges: GET ADD MODIFY DELETE
kadmin:
```

使用 `getprivs` 命令验证您有哪些特权。上面的列表中列出了全部特权。

作为示例，现在来修改主体 `newbie`：

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:

kadmin: getprinc newbie
Principal: newbie@EXAMPLE.COM
Expiration date: [never]
Last password change: Wed Jan 12 17:28:46 CET 2005
Password expiration date: [none]
Maximum ticket life: 0 days 10:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed Jan 12 17:47:17 CET 2005 (admin/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, Triple DES cbc mode with HMAC/sha1, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Attributes:
Policy: [none]

kadmin: modify_principal -maxlife "8 hours" newbie
Principal "newbie@EXAMPLE.COM" modified.
kadmin: getprinc joe
Principal: newbie@EXAMPLE.COM
Expiration date: [never]
```

```
Last password change: Wed Jan 12 17:28:46 CET 2005
Password expiration date: [none]
Maximum ticket life: 0 days 08:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed Jan 12 17:59:49 CET 2005 (newbie/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, Triple DES cbc mode with HMAC/sha1, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Attributes:
Policy: [none]
kadmin:
```

这将票证的最长生命周期更改为 8 小时。有关 `kadmin` 命令和可用选项的更多信息，请参见 <http://web.mit.edu/kerberos/www/krb5-1.4/krb5-1.4/doc/krb5-admin.html#Kadmin%20Options> 或查看 `man 8 kadmin`。

## 46.8 创建 Kerberos 主机主体

除了确保您的网络上的每台计算机知道它所处的 Kerberos 领域以及要联系的 KDC 之外，还应为它创建一个主机主体。到目前为止，我们仅讨论了用户身份凭证。但与 Kerberos 兼容的服务通常也需要将自身身份验证到客户机用户。因此，对于领域中的每个主机，在 Kerberos 数据库中必须存在特殊主机主体。

主机主体的命名约定是 `host/<hostname>@<REALM>`，其中 `hostname` 是完全限定的主机名。主机主体类似于用户主体，但也有显著的区别。用户主体和主机主体的主要区别在于用户主体的密钥是受密码保护的 — 当用户从 KDC 获得一个票据授予票据时，需要键入他的密码以便 Kerberos 能够解密此票据。很明显，如果系统管理员必须每隔 8 个小时为 SSH 守护程序获得新的票证，对系统管理员来说是非常不方便的。

相反，用来解密主机主体的初始票证的密钥是由管理员从 KDC 一次性抽取的，并储存在一个名为 `keytab` 的本地文件中。SSH 守护程序等服务将读取此密钥并在需要时使用它来自动获得新票证。默认 `keytab` 文件位于 `/etc/krb5.keytab` 中。

要为 `test.example.com` 创建一个主机主体，请在您的 `kadmin` 会话期间输入以下命令：

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:
kadmin: addprinc -randkey host/test.example.com
WARNING: no policy specified for host/test.example.com@EXAMPLE.COM;
defaulting
to no policy
Principal "host/test.example.com@EXAMPLE.COM" created.
```

`-randkey` 标志没有为新主体设置密码，而是指示 `kadmin` 生成一个随机密钥。之所以在这里使用这个标志，是因为此主体不需要用户交互。它是计算机的一个服务器帐户。

最后，抽取密钥并将其储存在本地 `keytab` 文件 `/etc/krb5.keytab` 中。这个文件由超级用户拥有，所以您必须是 `root` 用户才能在 `kadmin shell` 中执行以下命令：

```
kadmin: ktadd host/test.example.com
Entry for principal host/test.example.com with kvno 3, encryption type Triple
DES cbc mode with HMAC/shal added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/test.example.com with kvno 3, encryption type DES
cbc mode with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.
kadmin:
```

完成后，应确保使用 `kdestroy` 命令销毁通过 `kinit` 获得的 `admin` 票证。

## 46.9 启用 Kerberos 的 PAM 支持

SUSE Linux Enterprise® 附带名为 `pam_krb5` 的 PAM 模块，它支持 Kerberos 登录和密码更新。控制台登录、`su` 和图形登录应用程序（如 `KDM`）等应用程序都可以使用此模块，在使用过程中，用户提交一个密码并希望认证应用程序代表它获得一个初始 Kerberos 票证。

`pam_unix2` 模块也支持 Kerberos 身份验证和密码更新。要在 `pam_unix` 中启用 Kerberos 支持，请编辑文件 `/etc/security/pam_unix2.conf`，使它包含以下行：

```
auth:      use_krb5 nullok
account:   use_krb5
password:  use_krb5 nullok
session:   none
```

此后，对此文件中的项求值的所有程序均使用 Kerberos 来进行用户身份验证。对于不具有 Kerberos 主体的用户，pam\_unix2 会采用常规密码身份验证机制。对于具有主体的用户，现在应该能够使用 passwd 命令透明地更改他们的 Kerberos 密码。

要对使用 pam\_krb5 的方式进行微调，请编辑文件 /etc/krb5.conf 并将默认应用程序添加到 pam。有关细节，请使用 man5 pam\_krb5 来参见手册页。

pam\_krb5 模块明确地不用于接受 Kerberos 票据作为部分用户身份验证的网络服务。这一点很特别，后面还将进行讨论。

## 46.10 配置 SSH 进行 Kerberos 身份验证

OpenSSH 在协议版本 1 和 2 中均支持 Kerberos 身份验证。在版本 1 中，存在特定的协议消息来传送 Kerberos 票据。版本 2 不再直接使用 Kerberos，而是依赖于 GSSAPI，即通用安全服务 API。这是一种不特定于 Kerberos 的编程接口 — 旨在隐藏底层身份验证系统的属性，无论它是 Kerberos、公共密钥身份验证系统（如 SPKM）还是其他系统。但是，GSSAPI 库中仅包含 Kerberos 支持。

要将 sshd 与 Kerberos 认证一起使用，请编辑 /etc/ssh/sshd\_config 并设置如下选项：

```
# These are for protocol version 1
#
# KerberosAuthentication yes
# KerberosTicketCleanup yes

# These are for version 2 - better to use this
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

然后使用 rcsshd restart 重启动您的 SSH 守护程序。

要将 Kerberos 身份验证与协议版本 2 一起使用，需要在客户端也启用它。此操作可在整个系统范围的配置文件 /etc/ssh/ssh\_config 中执行，也可通过编辑 ~/.ssh/config 在每个用户级别上执行。在这两种情况下，均应添加选项 GSSAPIAuthentication yes。

您现在应该能够使用 Kerberos 身份验证进行连接。使用 `klist` 来验证您是否具有有效票证，然后连接到 SSH 服务器。要强制使用 SSH 协议版本 1，请在命令行上指定选项 `-1`。

---

#### 提示：其他信息

文件 `/usr/share/doc/packages/openssh/README.kerberos` 中详细讨论了 OpenSSH 和 Kerberos 的交互。

---

## 46.11 使用 LDAP 和 Kerberos

在使用 Kerberos 时，在您的本地网络中分发用户信息（如用户 ID、组、主目录）的一种方法就是使用 LDAP。这需要一种强大的身份验证机制来防止包被窃取以及他攻击。一种解决方案是将 Kerberos 也用于 LDAP 通信。

OpenLDAP 通过 SASL（简单身份验证会话层）实现了大部分身份验证功能。SASL 基本上是一种用于身份验证的网络协议。SASL 实施是 `cyrus-sasl`，它支持许多不同的身份验证方法。Kerberos 身份验证是通过 GSSAPI（通用安全服务 API）执行的。默认情况下，不安装用于 GSSAPI 的 SASL 插件。请使用 `rpm -ivh cyrus-sasl-gssapi-*.rpm` 来手动安装它。

为了使 Kerberos 能够绑定到 OpenLDAP 服务器，请创建一个主体 `ldap/earth.example.com` 并将其添加到 `keytab`：

默认情况下，LDAP 服务器 `slapd` 以用户和组 `ldap` 的身份运行，但只有 `root` 用户才能读取 `keytab` 文件。因此，要么更改 LDAP 配置以便使服务器以 `root` 用户身份运行，要么使组 `ldap` 可读取 `keytab` 文件。如果 `/etc/sysconfig/openldap` 中的 `OPENLDAP_KRB5_KEYTAB` 变量中指定了 `keytab` 文件并且 `OPENLDAP_CHOWN_DIRS` 变量设置成 `yes`（这是默认设置），则由 OpenLDAP 启动脚本（`/etc/init.d/ldap`）自动执行后一项操作。如果 `OPENLDAP_KRB5_KEYTAB` 保留为空，则使用 `/etc/krb5.keytab` 下的默认 `keytab` 文件，并且您必须如以下描述的那样自己调整优先级。

要以 `root` 用户身份运行 `slapd`，请编辑 `/etc/sysconfig/openldap`。通过在 `OPENLDAP_USER` 和 `OPENLDAP_GROUP` 变量前放置一个注释字符来禁用它们。

要使 keytab 对组 LDAP 可读，请执行

```
chgrp ldap /etc/krb5.keytab  
chmod 640 /etc/krb5.keytab
```

第三个方案（可能是最好的解决方案）是指示 OpenLDAP 使用特殊的 keytab 文件。要完成此操作，启动 kadmin 然后在添加主体 ldap/earth.example.com 后输入以下命令：

```
ktadd -k /etc/openldap/ldap.keytab ldap/earth.example.com@EXAMPLE.COM
```

然后，在 shell 上运行：

```
chown ldap.ldap /etc/openldap/ldap.keytab  
chmod 600 /etc/openldap/ldap.keytab
```

要指示 OpenLDAP 使用不同的 keytab 文件，在 /etc/sysconfig/openldap 中更改以下变量：

```
OPENLDAP_KRB5_KEYTAB="/etc/openldap/ldap.keytab"
```

最后，使用 `rcldap restart` 重新启动 LDAP 服务器。

## 46.11.1 将 Kerberos 身份验证与 LDAP 一起使用

现在应该可以自动将 `ldapsearch` 等工具与 Kerberos 认证一起使用。

```
ldapsearch -b ou=people,dc=example,dc=com '(uid=newbie)'  
  
SASL/GSSAPI authentication started  
SASL SSF: 56  
SASL installing layers  
[...]  
  
# newbie, people, example.com  
dn: uid=newbie,ou=people,dc=example,dc=com
```

```
uid: newbie
cn: Olaf Kirch
[...]
```

正如您所看到的，`ldapsearch` 打印一条消息，表示它已经启动 GSSAPI 身份验证。下一条信息无疑颇具隐蔽性，它实际上表明了安全强度系数（缩写为 SSF）是 56（值 56 有些随意，之所以选择这个数字，很可能因为它是 DES 加密密钥中的位数）。这里要告诉您的是 GSSAPI 认证是成功的，并且该加密要用于为 LDAP 连接提供集成保护和机密性。

在 Kerberos 中，身份验证永远是相互的。这意味着不仅您向 LDAP 服务器身份验证自己，而且 LDAP 服务器本身也向您身份验证。这意味着您是与所需的 LDAP 服务器而不是攻击者设置的假冒服务进行通讯。

## 46.11.2 Kerberos 身份验证和 LDAP 访问控制

现在，允许每个用户修改他们的 LDAP 用户记录的登录壳层属性。假定在您的纲要中 joe 用户的 LDAP 项位于 `uid=joe,ou=people,dc=example,dc=com`，请在 `/etc/openldap/slapd.conf` 中设置以下访问控制：

```
# This is required for things to work _at all_
access to dn.base="" by * read
# Let each user change their login shell
access to dn="*,ou=people,dc=example,dc=com" attrs=loginShell
        by self write
# Every user can read everything
access to *
        by users read
```

第 2 个语句授予已通过身份验证的用户对他们自己的 LDAP 项的 `loginShell` 属性进行写访问的权限。第 3 个语句授予所有已通过身份验证的用户对整个 LDAP 目录进行读访问的权限。

这里还有个不太重要的方面未明确，即 LDAP 服务器如何能够得知 Kerberos 用户 `joe@EXAMPLE.COM` 与 LDAP 判别名

`uid=joe,ou=people,dc=example,dc=com` 相对应。这种映射必须使用 `saslExpr` 指令进行手动配置。在本例中，则是将以下语句添加到 `slapd.conf`：

```
authz-regexp
```

```
uid=(.*),cn=GSSAPI,cn=auth  
uid=$1,ou=people,dc=example,dc=com
```

要了解它的工作原理，您需要知道，当 SASL 身份验证用户时，OpenLDAP 将使用 SASL 为它指派名称（如 joe）和 SASL 功能的名称 (GSSAPI) 构成一个判别名。结果是 uid=joe,cn=GSSAPI,cn=auth。

如果已经配置了 authz-regexp，它会将第一个参数用作常规表达式来检查从 SASL 信息构成的判别名。如果此常规表达式匹配，就用 authz-regexp 语句的第 2 个参数替换此名称。占位符 \$1 被替换为 (.\*?) 表达式所匹配的子字符串。

可能有更复杂的匹配表达式。如果您的目录结构或纲要更加复杂（其中用户名不是判别名的一部分），则甚至可以使用搜索表达式来将 SASL 判别名映射为用户判别名。



## 对分区和文件进行加密

每个用户都有一些第三方不应能访问的机密数据。越是依赖移动计算以及在不同环境和网络中工作，就越应该小心处理数据。如果其他人可以通过网络或实际访问您的系统，建议对文件或整个分区进行加密。便携式计算机或可卸媒体（例如外部硬盘或 USB 记忆棒）有可能被盗或丢失。因此，建议对包含机密数据的文件部分进行加密。

可以通过以下几种加密方法来保护数据：

### 加密硬盘分区

可在安装期间或在已安装的系统中使用 YaST 创建加密分区。有关细节，请参考第 47.1.1 节“在安装过程中创建加密分区”[780]和第 47.1.2 节“在运行的系统上创建加密分区”[781]。此选项还可用于可移动媒体（如外部硬盘），如第 47.1.4 节“加密可移动媒体的内容”[782]中所述。

### 作为容器创建加密文件

可以随时使用 YaST 在硬盘或可卸媒体上创建加密文件。之后可使用加密文件来储存其他文件或文件夹。有关更多信息，请参考第 47.1.3 节“作为容器创建加密文件”[782]。

### 加密用户主目录

用 SUSE Linux Enterprise 还可以为用户创建加密的主目录。用户登录系统时，装入加密的用户主目录，内容对该用户可用。有关更多信息，请参考第 47.2 节“使用加密的用户主目录”[782]。

加密单个 ASCII 文本文件

如果只有少量 ASCII 文本文件存有敏感或机密数据，则可使用 vi 编辑器对这些文件逐个加密并加密保护。有关更多信息，请参考第 47.3 节“使用 vi 加密单个 ASCII 文本文件” [783]。

---

**警告：加密媒体提供有限的保护**

本章中描述的方法仅提供有限的保护。无法保护正在运行的系统免受危害。成功装入加密媒体后，具有适当权限的所有用户都可以访问它。但是，加密媒体在计算机丢失或被窃的情况下，可以有效防止未经授权人员读取您的机密数据。

---

## 47.1 用 YaST 设置已加密的文件系统

使用 YaST 在安装期间或已安装的系统中加密分区或部分文件系统。但是，在已安装的系统中加密分区更加困难，因为必须重调整分区大小和更改现有分区。在此情况下，创建一个定义大小的加密文件来储存其他文件或部分文件系统可能更加方便。要加密整个分区，需要在分区布局中提供一个专用于加密的分区。默认情况下，YaST 的标准分区建议并不包括加密分区。请在分区对话框中手动添加此分区。

### 47.1.1 在安装过程中创建加密分区

---

**警告：密码输入**

确保牢记加密分区的密码。没有这个密码，您将无法访问或恢复加密数据。

---

用于分区的 YaST 专家对话框提供了创建加密分区所需的选项。要创建新的加密分区，请执行以下操作：

- 1 通过系统 > 分区程序从“YaST 控制中心”运行 YaST 分区程序。
- 2 单击创建并选择一个主分区或逻辑分区。
- 3 为此分区选择所需的文件系统、大小和装入点。

- 4 如果只在必要时才装入加密文件系统，请启用 *Fstab* 选项中的不在系统启动时装入。
- 5 激活加密文件系统复选框。
- 6 单击“确定”。系统将提示您输入用于加密此分区的密码。不会显示该密码。为了避免输入错误，请输入两次密码。
- 7 单击确定完成此过程。现在已创建了新的加密分区。

除非已选中不在系统启动时装入，否则操作系统引导时将在装入分区前要求输入密码。装入分区后，此分区对所有用户都可用。

要在启动期间跳过装入加密分区，可在提示输入密码时按 **Enter** 键。然后，再次拒绝输入密码的提示。在此情况下，不装入加密文件系统，并且操作系统继续引导并阻止对您的数据的访问。

要访问引导时未装入的加密分区，请通过输入 `mount name_of_partition mount_point` 来手动装入分区。在系统提示时输入密码。完成分区装入后，使用 `umount name_of_partition` 卸载分区，以防止其他用户访问此分区。

在已存在多个分区的计算机上安装系统时，还可决定在安装期间加密现有分区。在此情况下，请遵循第 47.1.2 节“在运行的系统上创建加密分区”[781]中的描述并注意此操作将会损坏要进行加密的现有分区中的所有数据。

## 47.1.2 在运行的系统上创建加密分区

---

**警告：**在运行的系统中激活加密

还可以在正在运行的系统上创建加密分区。但是，加密现有分区会损坏现有分区中的所有数据，并需要重调整现有分区的大小以及结构。

---

在正在运行的系统上，在“YaST 控制中心”中选择系统 > 分区。单击是继续。在 *Expert Partitioner* 中选择要加密的分区，并单击编辑。其余过程与第 47.1.1 节“在安装过程中创建加密分区”[780]中描述的过程相同。

## 47.1.3 作为容器创建加密文件

除了使用分区，还可以创建特定大小的加密文件来储存包含机密数据的其他文件或文件夹。这种容器文件是从“YaST 专家分区程序”对话框中创建的。选择**加密文件**并输入该文件的完全路径及其大小。接受或更改建议的格式化设置和文件系统类型。指定装入点并确定是否应在系统引导时装入加密文件系统。

相对于加密分区，加密容器文件的优势在于可以添加加密文件而无须对硬盘进行重分区。可以借助于环路设备装入加密文件，而其行为方式与常规的分区类似。

## 47.1.4 加密可移动媒体的内容

YaST 将可移动媒体（如外部硬盘或 USB 闪存驱动器）当作任何其他硬盘一样处理。可按上述方法加密此类媒体中的容器文件或分区。但是，请在 *Fstab* 选项对话框中启用**引导时不装入**，因为可移动媒体通常只在系统运行时连接。

如果已使用 YaST 对可卸设备进行了加密，KDE 和 GNOME 桌面会自动识别加密分区并在检测到该设备时提示输入密码。在运行 KDE 或 GNOME 时，如果插入 FAT 格式的可卸设备，输入密码的桌面用户自动成为设备的拥有者并可以读写文件。对于文件系统不是 FAT 的设备，请明确更改除 root 之外的用户的所有权，以便这些用户可以在该设备上读写文件。

## 47.2 使用加密的用户主目录

要防止用户主目录中的数据在被窃或硬盘被取下时丢失，请使用 YaST 用户管理模块以启用用户主目录加密。您可以为新的或现有的用户创建加密的用户主目录。要对现有用户主目录进行加密和解密，需要知道他们的登录密码。请参见有关指导说明。

如第 47.1.3 节“**作为容器创建加密文件**”[782]所述，加密主分区是在文件容器内创建的。会在 /home 下为每个加密用户主目录创建两个文件：

`LOGIN.img`  
存放该目录的映像

`LOGIN.key`  
映像密钥，受用户的登录密码保护。

登录时用户主目录会自动解密。在内部，该功能是通过 pam 模块 pam\_mount 提供的。如果需要添加提供加密用户主目录的其他登录方法，必须在 `/etc/pam.d/` 中将该模块添加到相应的配置文件。有关更多信息，另请参见[第 27 章 通过 PAM 进行身份验证](#) [451]和 pam\_mount 的手册页。

---

#### 警告：安全性限制

对用户主目录加密并不能对其他用户的访问进行高度安全的防御。如果需要高度安全性，则不应物理共享该系统。

为增强安全性，请同时加密 swap 分区以及 `/tmp` 和 `/var/tmp` 目录，因为它们可能包含关键数据的临时映像。您可以按[第 47.1.1 节“在安装过程中创建加密分区”](#) [780]或[第 47.1.3 节“作为容器创建加密文件”](#) [782]中所述，用 YaST 分区程序加密 swap、`/tmp` 和 `/var/tmp`。

---

## 47.3 使用 vi 加密单个 ASCII 文本文件

使用加密分区也有缺点，即在装入加密分区时，至少为 `root` 用户才能访问数据。要防止出现这种情况，可以在加密方式中使用 `vi`。

使用 `vi -x filename` 编辑新文件。`vi` 将提示您设置密码，然后加密文件的内容。只要您访问此文件，`vi` 就会要求您输入正确的密码。

要想更加安全，可以将加密文本文件放入加密分区中。建议使用此方法是因为 `vi` 使用的加密并不足够安全。



## 通过 AppArmor 限制特权

许多安全漏洞是*可信赖*程序中的错误产生的。可信赖程序运行时具有某些攻击者想获取的特权，如果程序中存在的错误导致攻击者得到了此特权，则程序丧失了可信赖性。

Novell® AppArmor 是一套应用程序安全解决方案，专门设计用于为可疑程序提供最低的特权限制。AppArmor 允许管理员指定程序可执行活动的域，方法是为该应用程序构建一个安全配置文件该程序可访问的文件列表和可执行的操作。

计算机系统的有效强化要求您将可调解特权的程序数目降至最低，然后尽可能保护程序的安全。通过 Novell AppArmor，您只需对环境中的易受攻击的程序构建配置文件，这大大减轻了对计算机进行强化所需要的工作量。AppArmor 配置文件强制执行策略，以确保程序不会执行预期操作之外的任何操作。

管理员只需注意易受攻击的应用程序并生成它们的配置文件。这样系统的强化可归结为构建和维护 AppArmor 配置文件集并监视 AppArmor 报告功能记录的策略违反或异常。

定义应用程序的 AppArmor 配置文件的构建非常直接和直观。AppArmor 销售时附有若干帮助创建配置文件的工具。您无需编程或处理脚本。需要管理员做的唯一任务是为每个需要强化的应用程序确定一个最严格访问和执行权限的策略。

只有在软件配置或所需的活动范围发生变化时才有必要更新或修改应用程序配置文件。AppArmor 提供直观的工具来处理配置文件的更新或修改。

用户完全不会觉察到 AppArmor。它在“后台”运行，无需任何用户交互操作。AppArmor 对系统性能没有明显影响。如果应用程序的某些活动没有包含在

AppArmor 配置文件中，或者应用程序的某些活动被 AppArmor 阻止，管理员必须调整此应用程序的配置文件以包括此类行为。

本指南简要介绍为了有效强化系统需要通过 AppArmor 执行的基本任务。要深入了解有关详细信息，请参见 *Novell AppArmor 管理指南*。

## 48.1 安装 Novell AppArmor

默认情况下，Novell AppArmor 会在每次安装 SUSE Linux Enterprise® 时来安装和运行，而忽略所安装的模式。AppArmor 的完整功能实例需要以下所列出的包

- apparmor-parser
- libapparmor
- apparmor-docs
- yast2-apparmor
- apparmor-profiles
- apparmor-utils
- audit

## 48.2 启用和禁用 Novell AppArmor

默认情况下，Novell AppArmor 配置为在每次新安装 SUSE Linux Enterprise 时运行。可以通过两种方法来切换 AppArmor 状态：

使用 YaST 系统服务（运行级别）

通过在系统引导时所执行的脚本序列中删除和添加引导脚本来禁用或启用 AppArmor。状态更改会在下次系统引导时应用。

使用 Novell AppArmor 控制面板

可使用“YaST Novell AppArmor 控制面板”来通过在运行中的系统上关闭或打开 Novell AppArmor 来切换其状态。在控制面板中所执行的更改将即时应用。“控制面板”会触发 AppArmor 停止或启动事件并在系统引导序列中删除或添加它的引导脚本。

要通过从系统引导时所执行的脚本序列中删除 AppArmor 以永久禁用 AppArmor，请如下执行操作：



- 1 以 `root` 身份登录并启动 YaST。
- 2 选择 **系统 > 系统服务（运行级别）**。
- 3 选择 **专家方式**。
- 4 选择 `boot.apparmor` 并单击 **设置/重置 > 禁用服务**。
- 5 单击 **完成** 退出 YaST 运行级别工具。

除非您明确重新启用 AppArmor，否则 AppArmor 在下次系统引导时将不会初始化并且保持非活动状态。使用 YaST 运行级别工具重新启用服务的操作与禁用服务的操作类似。

通过使用“AppArmor 控制面板”来在运行中的系统上切换 AppArmor 状态。应用这些更改并重引导系统后，这些更改将生效。要切换 AppArmor 的状态，请继续执行以下操作：

- 1 以 `root` 身份登录并启动 YaST。
- 2 然后选择 *Novell AppArmor > AppArmor 控制面板*。
- 3 选择 **启用 AppArmor**。要禁用 AppArmor，请取消选中此选项。
- 4 单击 **完成** 以退出“AppArmor 控制面板”。

## 48.3 构建应用程序的配置文件入门

请仔细考虑以下事项以在系统上准备 Novell AppArmor 的成功部署：

- 1 确定要构建配置文件的应用程序。有关详细信息，请参见 [第 48.3.1 节“选择要构建配置文件的应用程序”](#) [788]。
- 2 根据 [第 48.3.2 节“构建和修改配置文件”](#) [789] 中的简要说明构建需要的配置文件。检查结果并在必要时调整配置文件。
- 3 运行 AppArmor 报告并处理安全事件以跟踪系统上发生的事件。请参考 [第 48.3.3 节“配置 Novell AppArmor 事件通知和报告”](#) [791]。

- 4 环境发生变化或者需要对 AppArmor 报告工具记录的安全事件作出反应时，更新您的配置文件。请参考第 48.3.4 节“更新您的配置文件”[793]。

## 48.3.1 选择要构建配置文件的应用程序

您只需保护在您的特定设置中会受到攻击的程序，因此只需为真正运行的程序使用配置文件。使用以下列表来确定最可能的候选程序：

### 网络代理

具有开放网络端口的程序（服务器端和客户端）。邮件客户程序和 Web 浏览器等用户客户程序也会调解权限。这些程序在运行时具有书写用户主目录的权限，而且他们会处理来自恶意远程来源的输入，如恶意的 Web 网站和通过电子邮件发送的恶意代码。

### Web 应用程序

Web 浏览器可以调用的程序，包括 CGI Perl 脚本、PHP 页面以及更复杂的 Web 应用程序。

### Cron 作业

cron 守护程序定期运行的程序可读取来自各种来源的输入。

要了解哪些进程当前以开放网络端口运行并且可能需要配置文件来进行限制，请作为 root 运行 aa-unconfined。

### 例 48.1 aa-unconfined 的输出

```
19848 /usr/sbin/cupsd not confined
19887 /usr/sbin/sshd not confined
19947 /usr/lib/postfix/master not confined
29205 /usr/sbin/sshd confined by '/usr/sbin/sshd (enforce)'
```

上例中标注为 not confined 的每个进程都可能需要定制的配置文件来进行限制。标注为 confined by 的进程已受 AppArmor 保护。

---

#### 提示：有关详细信息

有关选择正确的应用程序来构建配置文件的更多信息，请参见第 1.2 节“Determining Programs to Immunize”（第 1 章 *Immunizing Programs*, ↑*Novell AppArmor Administration Guide*）。

---

## 48.3.2 构建和修改配置文件

SUSE Linux Enterprise 上的 Novell AppArmor 附带预配置的配置文件集，用于最重要的应用程序。除此之外，还可使用 AppArmor 来为所希望的任意应用程序创建您自己的配置文件。

管理配置文件有两种方式。一种是使用 YaST Novell AppArmor 模块提供的图形化前端，另一种是使用 AppArmor 套件自身提供的命令行工具。这两种方式的工作方式基本相同。

按第 48.3.1 节“选择要构建配置文件的应用程序”[788]中的说明运行 `aa-unconfined` 运行会确定一个可能需要配置文件以在安全模式下运行的应用程序列表。

对每个应用程序执行以下步骤以创建配置文件：

- 1 以 root 身份运行 `aa-genprof programname` 以使 AppArmor 创建应用程序配置文件的大致轮廓。

或

通过运行 `YaST > Novell AppArmor > 添加配置文件向导` 并指定要构建配置文件的应用程序的完整路径来建立基本的配置文件。

此时大致构建了一个基本的配置文件，同时 AppArmor 进入学习模式，这意味着它会记录您正在执行的程序的每个活动，但目前还不进行限制。

- 2 运行应用程序的所有操作，让 AppArmor 了解程序的每个活动。
- 3 通过在 `aa-genprof` 中输入 `S` 来使 AppArmor 分析在步骤 2 [789]中生成的日志文件。

或

通过在添加配置文件向导中单击扫描 AppArmor 事件的系统日志，然后执行向导中提示的操作直到完成配置文件来分析日志。

AppArmor 扫描在程序运行期间记录的日志，然后请求您为每个记录的事件设置访问权限。请对每个文件进行设置或使用通配。

- 4 依据应用程序的复杂性，可能必须重复 [步骤 2](#) [789] 和 [步骤 3](#) [789]。限制应用程序，在限制条件下执行应用程序并处理任何新的日志事件。要准确限制应用程序功能的完整范围，您可能必须经常重复此过程。
- 5 设置所有访问权限后，您的配置文件将被设置为强制模式。配置文件将被应用，AppArmor 根据刚创建的配置文件对应用程序进行限制。

如果某应用程序的现有配置文件处于提示模式，对此应用程序启动 `aa-genprof` 时，它的配置文件将在退出此学习周期后仍保留在学习模式下。有关更改配置文件模式的更多信息，请参见“`aa-complain—Entering Complain or Learning Mode`”一节（第 4 章 *Building Profiles from the Command Line*, ↑*Novell AppArmor Administration Guide*）和“`aa-enforce—Entering Enforce Mode`”一节（第 4 章 *Building Profiles from the Command Line*, ↑*Novell AppArmor Administration Guide*）。

使用您刚限制的应用程序执行您需要的每一项任务以测试您的配置文件设置。被限制的应用程序通常会顺利运行，您完全不会察觉到 AppArmor 活动。但是，如果您注意到应用程序行为失常，请检查系统日志以查看 AppArmor 对应用程序的限制是否太过严格。根据系统上所使用的日志机制，可从以下几个位置查找 AppArmor 日志条目：

`/var/log/audit/audit.log`

如果安装了 `audit` 包并且 `auditd` 正在运行，则将如下记录 AppArmor 事件：

```
type=APPARMOR msg=audit(1140325305.502:1407): REJECTING w access to
/usr/lib/firefox/update.test (firefox-bin(9469) profile
/usr/lib/firefox/firefox-bin active /usr/lib/firefox/firefox-bin)
```

`/var/log/messages`

如果未使用 `auditd`，则 AppArmor 事件会记录在 `/var/log/messages` 下的标准系统日志中。以下是示例条目：

```
Feb 22 18:29:14 dhcp-81 klogd: audit(1140661749.146:3): REJECTING w access
to /dev/console (mdnsd(3239) profile /usr/sbin/mdnsd active
/usr/sbin/mdnsd)
```

`dmesg`

如果 `auditd` 没有运行，则还可使用 `dmesg` 命令检查 AppArmor 事件：

```
audit(1140661749.146:3): REJECTING w access to /dev/console (mdnsd(3239)
profile /usr/sbin/mdnsd active /usr/sbin/mdnsd)
```

要调整配置文件，可按 [步骤 3](#) [789] 所述再次分析与此应用程序相关的日志消息。发出提示时，请确定访问权限或限制。

---

**提示：**有关详细信息

有关配置文件构建和修改的更多信息，请参见第 2 章 *Profile Components and Syntax* (↑*Novell AppArmor Administration Guide*)、第 3 章 *Building and Managing Profiles with YaST* (↑*Novell AppArmor Administration Guide*) 和第 4 章 *Building Profiles from the Command Line* (↑*Novell AppArmor Administration Guide*)。

---

## 48.3.3 配置 Novell AppArmor 事件通知和报告

请在 Novell AppArmor 中设置事件通知，这样您可以查看安全性事件。事件通知是一项 Novell AppArmor 功能，可在发生所选严重性级别的系统 Novell AppArmor 活动时通知指定的电子邮件收件人。当前可在 YaST 界面中获得此功能。

要在 YaST 中设置事件通知，请执行以下操作：

- 1 确保您的系统上运行着用于传递事件通知的邮件服务器。
- 2 作为 `root` 登录并启动 YaST。然后选择 *Novell AppArmor > AppArmor 控制面板* )。
- 3 在 *启用安全事件通知* 中选择 *配置*。
- 4 为每种记录类型（*简要、汇总和详细*）设置报告频率、输入接收报告的电子邮件地址并确定要记录事件的严重性。要在事件报告中包含未知事件，请选择 *包含未知严重性的事件*。

---

### 注意：选择要记录的事件

除非您对 AppArmor 的事件分类非常熟悉，否则选择通知所有安全级别的事件。

---

- 5 选择 *确定 > 完成* 退出此对话框以应用您的设置。

通过使用 Novell AppArmor 报告，您可以阅读日志文件中报告的重要 Novell AppArmor 安全事件，而不必手动筛选只对 aa-logprof 工具有用的繁杂消息。您可以按照日期范围或程序名称对报告进行过滤，以减小报告的大小。

要配置 AppArmor 报告，请执行如下操作：

- 1 作为 `root` 登录并启动 YaST。选择 *Novell AppArmor > AppArmor 报告*。
- 2 从 *执行安全摘要、应用程序审计和安全事件报告* 中选择要检查或配置的报告类型。
- 3 选择 *编辑* 并提供请求的数据，以编辑报告生成频率、电子邮件地址、导出格式和报告位置。
- 4 要运行所选类型的报告，请单击 *立即运行*。
- 5 选择 *查看档案* 并指定报告类型，以在给定类型的存档报告中浏览。

或

删除不需要的报告或添加新报告。

---

#### 提示：有关详细信息

有关在 Novell AppArmor 中配置事件通知的更多信息，请参见第 6.2 节 “Configuring Security Event Notification” (第 6 章 *Managing Profiled Applications*, ↑*Novell AppArmor Administration Guide*)。可在第 6.3 节 “Configuring Reports” (第 6 章 *Managing Profiled Applications*, ↑*Novell AppArmor Administration Guide*) 中找到关于报告配置的更多信息。

---

## 48.3.4 更新您的配置文件

软件和系统配置会随着时间的流逝而更改。因此您经常需要对 AppArmor 的配置文件设置进行微调。AppArmor 会检查系统日志以查找策略违例或其他 AppArmor 事件，允许您对配置文件作相应的调整。您也可以使用[更新配置文件向导](#)解决应用程序行为超出配置文件定义的问题。

要更新配置文件集，请执行以下操作：

- 1 作为 `root` 登录并启动 YaST。
- 2 启动 *Novell AppArmor* > *更新配置文件向导*。
- 3 对于记录的任意资源或可执行文件，根据提示调整其访问或执行权限。
- 4 回答所有问题后离开 YaST。您的更改将被应用到对应的配置文件中。

---

### 提示：有关详细信息

有关从系统日志更新配置文件的更多信息，请参见第 3.5 节 “Updating Profiles from Log Entries” (第 3 章 *Building and Managing Profiles with YaST*, ↑*Novell AppArmor Administration Guide*)。

---





## 安全性和机密性

Linux 或 UNIX 系统的一个主要特点就是能够同时处理多个用户（多用户），并允许这些用户在同一计算机上同时执行多项任务（多任务）。此外，操作系统对网络是透明的。用户往往不知道他们所用的数据和应用程序是他们自己的计算机本地提供的，还是通过网络提供的。

利用多用户功能时，不同用户的数据必须分开储存。要确保安全性和私密性。数据安全性早在计算机能够联网之前就已经是个关键问题。和今天一样，那时人们最担心的问题就是如何保持数据可用，即便数据丢失或是数据媒体（通常是硬盘）损坏也不受任何影响。

本节侧重说明机密性问题以及保护用户隐私的方法；但是，全面的安全观离不开一些过程，即：随时准备好定期更新、可行的和经过测试的备份副本，这一点再怎么强调都不为过。做不到这一点，您可能很难恢复数据——不仅是在出现硬件故障时，在怀疑有人未经授权访问和篡改文件时，也很难恢复数据。

## 49.1 本地安全和网络安全

访问数据有以下几种方式：

- 与拥有所需信息或能访问计算机数据的人进行人际交流
- 直接从计算机控制台访问（物理访问）
- 通过串行线路
- 使用网络链接

在上述所有情况下，用户只有在通过身份验证后才能访问相关资源或数据。Web 服务器在这方面可能较为宽松，但您仍不希望它向任何访问者透露您个人的所有数据。

在上面的列表中，第一种情况需要最大程度的人际互动，例如在您联系银行职员时，您需要证明自己就是银行帐号的持有人。然后您需要提供签名、PIN 或密码，来证明您就是您自己声称的那个人。有时候，有些人可能会通过提及一些大家都知道的零散信息，利用花言巧语骗取知情人的信任，诱导知情人说出机密信息。受骗人可能会被一步步地诱骗出更多信息，而自己却一直蒙在鼓里。这种手段在黑客内部称为**社会工程**。要防止受骗，您只能对人们进行教育，并且学会言辞谨慎，不轻易透露信息。在闯入计算机系统之前，攻击者通常将目标锁定在接待员、公司内的服务人员，甚至也可能是家庭成员。在很多情况下，最终发现这种利用社会工程手段发起的攻击时，通常为时已晚。

企图未经授权访问您数据的人也可能使用传统方法直接攻击您的硬件。因此，应该防止有人对计算机做手脚，让任何人都无法拆除、替换或损坏其部件。这也适用于各种备份，甚至是各种网络电缆或电线。还应保护引导过程，因为已知有些按键组合会引起异常行为。通过为 BIOS 和引导加载程序设置密码可以提供这方面的保护。

串行终端连接到串行端口，目前很多地方仍在使用这种连接方式。与网络接口不同，它们不依赖网络协议与主机通讯。通过一根缆线或是红外端口就可以在设备间发送纯字符数据。电缆本身是这种系统最薄弱的地方：连接了较旧的打印机后，很容易记录下流过电缆的数据。通过打印机做的事情也可以通过其他方式来完成，具体取决于攻击的强度。

在一台主机的本地读取文件需要一定的访问规则，这与打开网络连接访问其他主机上的服务器所需的规则不同。本地安全不同于网络安全。区别即在于：必须将数据放入包中才能发送到其他位置。

## 49.1.1 本地安全

关于本地安全，还要从计算机运行所在的位置的物理环境说起。在符合您的安全预期和需要的地点搭建计算机系统。本地安全的主要目标是将不同用户分隔开，防止某个用户假借其他用户的权限或身份。这是要遵守的一条基本规则，但这条规则对 `root`（`root` 用户，对系统拥有最高权力）尤其适用。`root` 不必输入密码即具有其他任何本地用户的身份，还能够读取本地储存的所有文件。

## 49.1.2 密码

在 Linux 系统中，密码不是以纯文本格式储存的，而且也不能简单地将输入的文本字符串与保存的模式匹配。如果事实正好相反，只要有人取得了相应文件的访问权，就会危及系统中所有帐户的安全。所以要对储存的密码加密，并且每次输入时都要再次加密，而后对两个加密字符串进行比较。只有在无法将加密密码反向计算为原始文本字符串时，这种方式才能提高安全性。

实际上，这是通过一种特殊算法（亦称活门算法）实现的，因为该算法只能单向有效。截获加密字符串的攻击者无法通过简单地再次应用同一算法来获取您的密码。这需要测试所有可能的字符组合，直到有一种组合看似加密时的密码。对于八位字符密码，需要计算的可能组合是相当多的。

20 世纪 70 年代时，人们对这种方法是否比其他方法更安全存在争议，因为其中所用算法的计算速度相对较慢，几秒钟才能加密一个密码。而与此同时，PC 的处理能力已足够大，每秒可进行几十万次甚至是几百万次的加密。正因为这样，不应让普通用户看到加密密码（普通用户不能读取 `/etc/shadow`）。更重要的是，密码应该是不容易猜出的，以防因意外错误而暴露密码文件。因此，将“`tantalize`”这样的密码“转换”为“`t@nt@1lz3`”实际上没有任何帮助。

用相似的数字替换单词中的某些字母是不够安全的。利用字典来猜字的密码破解程序用的也是类似的替换方法。最好是编造出没有一般意义的词，即仅对您自己有意义的词，如句中各词的词首字母，或书名，如 Umberto Eco 撰写的“`The Name of the Rose`”。这样可以编写以下安全的密码：“`TN0tRbUE9`”。相比之下，像“`beerbuddy`”或“`jasmine76`”这样的密码，即便是不太了解您的人也很容易猜出。

## 49.1.3 引导过程

配置系统，让其无法从软盘或 CD 引导；配置方法为：彻底拆除驱动器，或设置 BIOS 密码，将 BIOS 配置为只能从硬盘引导。通常，Linux 系统要通过引导加载程序来启动，这样您可以向引导内核传递更多选项。通过在 `/boot/grub/menu.lst` 中设置额外的密码可防止其他用户在引导期间使用这类参数（请参见第 21 章 [引导加载程序](#) [369]）。这对您的系统安全举足轻重。不仅内核本身以 `root` 权限运行，而且内核还是在系统启动时授予 `root` 权限的第一个权威对象。

## 49.1.4 文件权限

一般来说，执行某项任务时应始终尽量使用限制性最强的特权。例如，以 `root` 权限读写电子邮件是完全没有必要的。如果邮件程序有错误，攻击者则可能利用该错误，以该程序启动时所具有的权限发起攻击。如若遵守上述规则，则可以尽量减少可能的损失。

在 SUSE Linux Enterprise 分发包中包括的所有文件的权限经过了小心的选择。系统管理员在安装附加软件或其他文件时要特别小心，尤其是在设置权限位时。经验丰富且安全意识强的系统管理员始终在命令 `ls` 后使用 `-l` 选项获取详细的文件列表，这样他们可以立即检测出有错误的文件权限。错误的文件属性不仅意味着文件可能被更改或删除，`root` 还可能执行这些改过的文件；或者如果是配置文件，程序则可能以 `root` 权限使用这些文件。这使系统很容易受到攻击。这类攻击被称为布谷鸟蛋，因为程序（蛋）由另一个用户（鸟）执行（孵化），就像是布谷鸟诱骗其他鸟代其孵蛋。

SUSE Linux Enterprise 系统中的文件 `permissions`、`permissions.easy`、`permissions.secure` 和 `permissions.paranoid` 都位于 `/etc` 目录中。这些文件用于定义特殊权限（如全局可写目录），或为文件定义 `setuser ID` 位（设置了 `setuser ID` 位的程序不以启动该程序的用户的权限运行，而以文件拥有者的权限运行，这个权限多为 `root`）。管理员可以使用文件 `/etc/permissions.local` 添加自己的设置。

要定义 SUSE Linux Enterprise 的配置使用以上哪个文件来相应地设置权限，请选择 YaST 部分 *安全性和用户* 中的 *本地安全性*。要了解这一主题的详细信息，请阅读 `/etc/permissions` 中的注释，或参考 `chmod` 手册页 (`manchmod`)。

## 49.1.5 缓冲区溢出错误和格式字符串错误

只要程序要处理的数据可以或可能被用户更改，就应该加倍小心；但这个问题更应该是应用程序编程人员的问题而不是普通用户的问题。编程人员必须确保自己编写的应用程序以正确的方式解释数据，避免将这些数据写入内存时，因为内存区域过小而无法容纳。此外，程序应能够通过专用接口一致地传递数据。

如果写入内存缓冲区时未考虑该缓冲区的实际大小，则会发生缓冲区溢出。有时这些数据（即用户生成的数据）占用的空间会超过该缓冲区所能提供的空间。结果导致数据写出缓冲区，以致于在特定情况下，程序可能执行受用户（而不是编程人员）影响的程序顺序，而不只是处理用户数据。这种错误可能导致严重后果，特别是在使用特权执行程序时（请参见第 49.1.4 节“文件权限”[798]）。

格式字符串错误的作用方式略有不同，但同样也是用户输入导致了程序出错。多数情况下，这些编程错误会被以特殊权限执行的程序（setuid 程序和 setgid 程序）利用，这也意味着您可以通过取消这些程序的相应执行特权，来防止您的数据和系统受到这种错误的影响。同样，最好的办法是使用尽可能低的特权（请参见第 49.1.4 节“文件权限”[798]）。

鉴于缓冲区溢出错误和格式字符串错误都是与用户数据处理有关的错误，攻击者不仅可以在本地帐户具有访问权的情况下利用这些错误，还可以通过网络链接利用许多已报告的错误。因此，缓冲区溢出错误和格式字符串错误与本地安全和网络安全都有关系。

## 49.1.6 病毒

Linux 上确有病毒运行，这与某些人的说法正好相反。但是，已知的这些病毒是由它们的创作者为进行概念验证而发布的，目的是为证明这种技术可以发挥预期的作用。目前尚未发现上述病毒中有任何正在流行。

没有借以寄生的宿主，病毒将无法生存和传播。对于计算机病毒来说，这个“宿主”是病毒程序代码能写入的某个程序或系统中的重要储存区域（如主引导记录）。由于 Linux 支持多用户处理，所以它可以将写权限限制到特定文件，这对系统文件尤其重要。因此，以 root 权限执行一般操作无疑会增大系统受病毒感染的机率。相反，若遵循上述规则（即使用尽可能低的特权），感染病毒的机率会非常低。

除此之外，切勿在未真正了解某个因特网站点时就仓促执行其中的程序。SUSE Linux Enterprise 的 RPM 包具有加密签名，这是个数字标签，表明在生成包时已

经考虑到必要的安全措施。病毒的存在是管理员或用户缺乏必要的安全意识的典型表现，病毒使系统受到威胁，即使是设计上高度安全的系统也无法逃避。

不应将病毒和蠕虫混为一谈，后者属于全球网络的问题。蠕虫的传播不需要宿主。

## 49.1.7 网络安全

网络安全对于保护系统免遭外部攻击至关重要。典型的登录过程（即要求提供用户名和密码以进行用户身份验证）仍然是个本地安全问题。在通过网络登录的特定情况下，应该区分这两方面的安全问题。在实际身份验证之前发生的属于网络安全问题，之后发生的属于本地安全问题。

## 49.1.8 X Window 系统和 X 身份验证

正如本文开头所述，网络透明属性是 UNIX 系统的核心属性之一。X（作为 UNIX 操作系统的窗口系统）能明显地利用这一特性。利用 X 系统，在远程主机上登录，然后启动一个图形化程序，令其随后通过网络发送并显示在您的计算机上，这个过程基本不成问题。

如果应该使用 X 服务器远程显示 X 客户机，X 服务器应该防止未经授权访问受其管理的资源（即显示）。更具体地说，必须给客户机指派特定权限。在 X Window 系统中，有两种指派权限的方法，分别为基于主机的访问控制和基于 Cookie 的访问控制。前者依赖应该运行客户程序的主机的 IP 地址。所用的控制程序为 `xhost`。使用 `xhost` 可以将合法客户机的 IP 地址输入属于 X 服务器的小型数据库。不过，依赖 IP 地址进行身份验证不是十分安全。例如，如果另有用户在发送客户程序的主机上工作，该用户将同样能够访问 X 服务器——就像是有人盗取了 IP 地址。由于存在这些缺点，在此不再详述这种身份验证方法，但您可以通过 `manxhost` 了解更多相关信息。

使用基于 Cookie 的访问控制时，将生成一个只有 X 服务器和合法用户才知道的字符串，就像是某种身份证。这个 Cookie（该词并不指普通意义上的小甜饼，而是指里面有幸运签的中国幸运饼）在登录时储存在用户主目录下的文件 `.Xauthority` 中，并且可供要使用 X 服务器显示窗口的所有 X 客户机使用。用户可以使用工具 `xauth` 检查文件 `.Xauthority`。如果将 `.Xauthority` 重命名或者意外地从主目录中删除了该文件，则无法再打开任何新窗口或 X 客户机。有关 X Window 系统安全机制的详细信息，请参见 `Xsecurity` 手册页 (`manXsecurity`)。

SSH（安全 shell）可用于对网络连接彻底加密并将其透明地转发给 X 服务器，而用户根本察觉不到这种加密机制。这也称为 X 转发。要实现 X 转发，需要在服务器端模拟 X 服务器，并在远程主机上为 shell 设置 DISPLAY 变量。有关 SSH 的更多详细信息，请参见 [第 44 章 SSH：安全性网络操作](#) [747]。

---

### 警告

如果不认为登录主机是安全主机，请不要使用 X 转发。在不安全的主机上启用 X 转发后，攻击者可能经由 SSH 连接通过身份验证，闯入您的 X 服务器并嗅探键盘输入之类的信息。

---

## 49.1.9 缓冲区溢出错误和格式字符串错误

如[第 49.1.5 节“缓冲区溢出错误和格式字符串错误”](#) [799]所述，缓冲区溢出错误和格式字符串错误应划归与本地安全和网络安全都有关系的问题。与这些错误的本地情况一样，若成功攻击了网络程序中的缓冲区溢出漏洞，常常可以获取 root 权限。即便不是这样，攻击者也可以利用该错误获取对非特权本地帐户的访问，以攻击系统中可能存在的其他任何漏洞。

一般来说，通过网络链接发起的针对缓冲区溢出错误和格式字符串错误的攻击当属远程攻击中最常见的形式。攻击的漏洞 — 用于攻击新发现的安全漏洞的程序 — 通常在安全邮件列表上发布。通过它们可以修补漏洞而不必了解代码的详细信息。多年来的经验表明：漏洞检测代码的存在成就了更为安全的操作系统，这显然是因为迫于压力，操作系统制造商不得不修复他们软件中的问题。在自由软件中，任何人都拥有访问源代码（SUSE Linux Enterprise 提供所有可用源代码），并且任何人在发现漏洞及其漏洞检测代码后都可以提交增补程序来修复相应的错误。

## 49.1.10 拒绝服务

拒绝服务 (DoS) 攻击的目的是阻断某个服务器程序或甚至阻断整个系统，通过以下方式来实现阻断：使服务器过载、用垃圾包使服务器一直繁忙或利用远程缓冲区溢出。DoS 攻击往往只有一个目的：让服务不再可用。不过，一旦某个服务不再可用，通讯就易于受到中间人攻击（嗅探、TCP 连接劫持、欺骗），或发生 DNS 中毒。

## 49.1.11 中间人：嗅探、劫持、欺骗

一般而言，由身处通讯主机之间的攻击者发起的所有远程攻击都称为*中间人攻击*。几乎所有类型的中间人攻击都有一个共同特点，即受害人通常毫无察觉。这种攻击有多种变化形式，例如，攻击者可能会截获连接请求并自行将其转发给目标计算机。现在受害者就会在不知情的情况下与错误的主机建立连接，因为连接的这一端伪装为合法的目标计算机。

最简单的中间人攻击的形式称为*嗅探* — 攻击者“只是”监听通过网络传递的数据流。更为复杂的“中间人攻击”可能会试图接管已经建立的连接（劫持）。劫持之前，攻击者需要一段时间对数据包进行分析，以便能够推测出属于该连接的TCP 顺序号。在攻击者最终夺取目标主机的角色后，受害人会注意到这一点，因为他们会收到一条错误消息，说明连接因失败而终止。由于有些协议没有通过加密来预防劫持，只是在建立连接后执行简单的身份验证过程，这给攻击者创造了可乘之机。

欺骗类型的攻击是对数据包进行修改，使其包含虚假的源数据（通常是IP 地址）。多数较活跃的攻击都依赖于发送这种虚假数据包 — 在Linux 计算机上，发送包的任务只能由超级用户 (root) 执行。

上述很多攻击都是与DoS同时进行的。一旦攻击者发现有机会让某台主机突然宕机，即便是很短的时间，攻击者也容易发起猛烈攻击，因为主机将在一段时间内无法对抗攻击。

## 49.1.12 DNS 中毒

DNS 中毒指的是通过向DNS 服务器回复伪造的DNS 回复包，试图让该服务器向请求其发送信息的受害者发送特定数据，以此破坏DNS 服务器的缓存。许多服务器都基于IP 地址或主机名与其他主机保持信任关系。攻击者需要非常熟悉主机之间信任关系的实际结构，才能将自己伪装为受信主机之一。通常，攻击者会分析一些从服务器接收的包，获取必要信息。攻击者还常常需要对名称服务器适时发动DoS 攻击。您可以使用加密连接，通过对要连接的主机的身份进行校验来保护自己。



## 49.1.13 蠕虫

蠕虫经常被误认为是病毒，但两者有着明显的区别。不同于病毒，蠕虫无需感染某个要寄生的主机程序。它们的特点就是尽快在网络结构中传播。以往的蠕虫，如 Ramen、Lion 或 Adore，全都利用 bind8 或 lprNG 之类的服务器程序中的已知安全漏洞。蠕虫的预防相对简单。鉴于在发现安全漏洞和蠕虫对服务器发起攻击之间有一段时间，很有可能及时提供受影响的程序的更新版本。只有管理员确实在受感染系统上安装了安全更新程序时，这种方法才有用。

## 49.2 一些常用的安全提示和技巧

要有效处理安全问题，关键在于随时关注安全方面的新动态并了解最新的安全问题。要保护您的系统免受各种问题的侵扰，最好的方式就是尽快获取并安装安全公告推荐的更新包。SUSE 使用邮件列表发布安全公告，您可以通过链接 <http://en.opensuse.org/Communicate/Mailinglists> 订阅该邮件列表。列表提供关于更新包的第一手信息，向其积极投稿的人当中还有 SUSE 安全小组的成员。[opensuse-security-announce@opensuse.org](mailto:opensuse-security-announce@opensuse.org)

邮件列表 [opensuse-security@opensuse.org](mailto:opensuse-security@opensuse.org) 提供了一个不错的论坛，可以在其中讨论任何相关的安全问题。在同一网页上订阅该邮件列表。

[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com) 是全球知名的安全邮件列表之一。建议阅读此列表，该列表每天要接收 15 到 20 条投递信息。有关详细信息，请参见 <http://www.securityfocus.com>。

下面是一些规则，可能有助于您处理基本的安全问题：

- 根据要对每个作业都尽量使用限制性最强的一组权限的规则，应避免使用 root 权限执行常规作业。这样即可降低受布谷鸟蛋或病毒攻击的风险，防止您自己犯错误。
- 如果可能，应尽量使用加密连接在远程计算机上工作。用 ssh（安全 shell）替代 telnet、ftp、rsh 和 rlogin，这应是标准做法。
- 避免使用仅基于 IP 地址的身份验证方法。

- 尽量使最重要的网络相关包保持最新，并且订阅相应的邮件列表，以接收这些程序（如 `bind`、`postfix`、`ssh` 等）的最新版本的声明。该做法同样适用于与本地安全相关的软件。
- 更改 `/etc/permissions` 文件，优化对系统安全至关重要的文件的权限。如果删除某个程序的 `setuid` 位，该程序很可能无法再正常执行作业。但从另一方面考虑，在多数情况下，该程序也将不再是个潜在的安全隐患。所以，您可以对全局可写目录和文件采取相同的做法。
- 禁用不是绝对需要的所有网络服务，以便服务器正常运行。这样可以使系统更加安全。使用程序 `netstat` 可以找到套接状态为 `LISTEN` 的打开端口。至于选项，建议使用 `netstat-ap` 或 `netstat-anp`。 `-p` 选项允许您查看哪个进程正以什么名称占用端口。

将 `netstat` 的结果与在主机外部执行的彻底端口扫描的结果进行比较。最适合执行这项作业的程序当属 `nmap`，该程序不仅可以检测计算机的端口，而且可以对哪些服务正等待端口处理作出一些判断。不过，端口扫描可能被认为是一种入侵行为，所以不要在未经管理员明确批准的情况下在主机上执行该操作。最后，要记住不仅要扫描 `TCP` 端口，而且要扫描 `UDP` 端口（使用选项 `-sS` 和 `-sU`），这一点至关重要。

- 要以可靠方式监视系统文件的完整性，请使用 `SUSE Linux Enterprise` 提供的程序 `AIDE`（高级入侵检测环境）。对 `AIDE` 创建的数据库加密，防止有人篡改。此外，在其他计算机上保留此数据库的备份副本，储存该副本的外部数据媒体不能通过网络链接连接到您的计算机。
- 安装任何第三方软件时都要小心谨慎。曾经有黑客在安全软件包的 `tar` 档案中嵌入了特洛伊木马病毒，不过幸好发现得及时。如果安装二进制包，则应确保下载站点是安全的。

`SUSE` 的 `RPM` 包都具有 `gpg` 签名。`SUSE` 使用以下密钥来签名：

```
ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
```

命令 `rpm--checksig package.rpm` 显示校验和及未安装包的签名是否正确。可以在本版本的第一张 `CD` 上和全球多数密钥服务器上找到该密钥。

- 定期检查用户和系统文件的备份副本。考虑如果不测试备份是否有效，实际上它可能毫无价值。

- 检查日志文件。尽可能编写小型脚本搜索可疑项。无可否认，这并不是是一项非常烦琐的任务。最终，只有您才知道哪些项异常，哪些项正常。
- 使用 `tcp_wrapper` 限制访问计算机上运行的各个服务，这样您可以明确控制哪个 IP 地址可以连接到某个服务。有关 `tcp_wrapper` 的进一步信息，请参见 `tcpd` 和 `hosts_access` 的手册页（`man8 tcpd`、`manhosts_access`）。
- 使用 `SuSEfirewall` 可以增强 `tcpd` (`tcp_wrapper`) 提供的安全性。
- 设计具有冗余性的安全性对策，看到两次消息总比没看到消息好。

## 49.3 使用中央安全报告地址

如果您发现与安全有关的问题（请首先检查可用的更新包），请向 [security@suse.de](mailto:security@suse.de) 发送电子邮件。请提供问题的详细说明以及涉及的包的版本号。SUSE 将尽快给予答复。建议您对电子邮件消息进行 `pgp` 加密。SUSE 的 `pgp` 密钥为：

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>  
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

也可以从 <http://www.novell.com/linux/security/securitysupport.html> 下载该密钥。



## 部分 VI. 查错



## 帮助和文档

SUSE Linux Enterprise® 附带各种信息和文档源。通过 SUSE 帮助中心，您可以对系统中最重要文档资源进行集中访问，而且还可以进行搜索。这些资源包括所安装的应用程序的联机帮助；硬件和软件主题的手册页、信息页、数据库；以及随本产品提供的所有手册。

### 50.1 使用 SUSE 帮助中心

首次从主菜单（*SuSE 帮助中心*）或使用 shell 中的 `susehelp` 命令启动 SUSE 帮助中心时，将显示如图 50.1 “SUSE 帮助中心的主窗口” [810] 中所示的窗口。该对话框窗口包含三个主要区域：

#### 菜单栏和工具栏

菜单栏提供主要的编辑、导航和配置选项。文件包含用于打印当前显示的内容的选项。在编辑下，可访问搜索功能。转至包含所有可用的导航：目录（帮助中心主页）、后退、前进和最后一个搜索结果。通过设置> 构建搜索索引，可以为所有选定信息源生成搜索索引。工具栏包含三个导航图标（前进、后退、主页），一个用于打印当前内容的打印机图标。

#### 带有选项卡的导航区域

窗口左侧的导航区域有一个字段，用户可在选定的信息源中快速搜索在该字段中输入的内容。有关搜索的细节和在搜索选项卡中配置搜索功能的细节，请参见第 50.1.2 节 “搜索功能” [811]。目录选项卡以树结构显示了所有可用的和当前已安装的信息源。单击书图标可打开并浏览单个类别。

## 查看窗口

视图窗口始终显示当前选定的内容，如联机手册、搜索结果或网页。

图 50.1 SUSE 帮助中心的主窗口



---

## 注意：语言选择视图

SUSE 帮助中心中可用的文档取决于当前语言。更改语言后，树视图会发生变化。

---



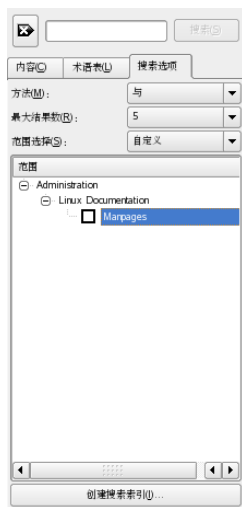
## 50.1.1 内容

通过 SUSE 帮助中心可以访问各种来源的有用信息。它包含用于 SUSE Linux Enterprise ( *Start-Up*、*KDE User Guide*、*GNOME User Guide* 及 *Reference* ) 的特殊文档、所有适用于工作站环境的信息源、已安装程序的联机帮助以及其他应用程序的帮助文本。此外，SUSE 帮助中心还提供对 SUSE 联机数据库的访问，这些数据库中包含 SUSE Linux Enterprise 的特殊硬件和软件问题。只要生成搜索索引，就可以轻松地搜索所有这些信息源。

## 50.1.2 搜索功能

要搜索 SUSE Linux Enterprise 的所有已安装的信息源，需要生成一个搜索索引并设置许多搜索参数。为此，请打开搜索选项卡，如图 50.2 “配置搜索功能”[811]所示。

图 50.2 配置搜索功能



如果以前未生成搜索索引，那么当您单击搜索选项卡或输入搜索字符串然后单击搜索时，系统会自动提示您生成搜索索引。在用于生成搜索索引的窗口中（如图 50.3 “生成搜索索引”[812]所示），使用复选框确定要建立索引的信息源。当您通过构建索引退出对话框后，将生成索引。

图 50.3 生成搜索索引



要尽可能精确地限制搜索基数和搜索结果列表，请使用三个下拉菜单，确定显示的结果个数以及要搜索的信息源选择区域。下列选项可用来确定选择区域：

默认

搜索预定义的源选择内容。

所有

搜索全部源。

无

未选择任何要搜索的源。

自定义

通过在概述中选中各自相应的复选框来确定要搜索的源。

完成搜索配置后，单击搜索。相关的项目随即显示在视图窗口中，您只需用鼠标单击它们即可查看这些内容。

## 50.2 手册页

手册页是任何 Linux 系统的基本组成部分。它们介绍命令的用法以及所有可用的选项和参数。手册页如表 50.1 “手册页 — 类别和描述” [813] 所示按类别进行排序（取自 man 命令本身的手册页）。

表 50.1 手册页 — 类别和描述

号码	说明
1	可执行程序或 shell 命令
2	系统调用（内核提供的函数）
3	库调用（程序库内的函数）
4	特殊文件（通常位于 /dev）
5	文件格式和约定 (/etc/fstab)
6	游戏
7	其他（包括宏包和约定），如 man(7)、groff(7)
8	系统管理命令（通常只用于 root 用户）
9	内核例程（非标准）

通常，手册页都是随关联的命令提供的。可以在帮助中心或者直接在 shell 中浏览手册页。要在 shell 中显示手册页，请使用 man 命令。例如，要显示 ls 的手册页，请输入 man ls。每个手册页包括标为 *NAME*、*SYNOPSIS*、*DESCRIPTION*、*SEE ALSO*、*LICENSING* 和 *AUTHOR* 的几个部分。根据具体的命令类型，可能还有其他部分。使用 Q 可退出手册页查看器。

另外一种显示手册页的方法是使用 Konqueror。例如，启动 Konqueror 并键入 man:/ls。如果某个命令具有多个不同的类别，Konqueror 会将这些类别显示为链接。

## 50.3 信息页

信息页是系统上另一个重要的信息来源。它们通常比手册页更为详细。可以使用信息浏览器浏览信息页并显示不同的部分（称作“节点”）使用 info 命令可

完成此任务。例如，要查看 `info` 命令本身的信息页，请在 `shell` 中输入 `info info`。

更加方便的方法是使用帮助中心或 `Konqueror`。启动 `Konqueror` 并键入 `info:/` 以查看顶级内容。要显示 `grep` 的信息页，请键入 `info:/grep`。

## 50.4 Linux 文档计划

Linux 文档计划 (The Linux Documentation Project, TLDP) 由一组编写 Linux 和 Linux 相关文档的自愿者负责管理（请参见 <http://www.tldp.org>）。这套文档包括初学者教程，但主要侧重于有经验的用户和职业系统管理员。TLDP 以免费许可的形式发布 HOWTO、常见问题和指南（手册）。

### 50.4.1 HOWTO

HOWTO 通常是指导完成特定任务的简短、非正式的分步指南。它是由专家为非专家以程序性的方式编写的。例如，如何配置 `DHCP` 服务器。HOWTO 位于 `howto` 包中，安装在 `/usr/share/doc/howto` 之下

### 50.4.2 常见问题

FAQ（常见问题）是一系列问题和解答。它们来自 Usenet 新闻组，该新闻组的目的是减少连续重复粘贴相同基本问题的情况。

## 50.5 Wikipedia：免费的联机百科全书

Wikipedia 是“供任何人阅读和编辑的多语种百科全书”（请参见 <http://en.wikipedia.org>）。Wikipedia 的内容由其用户创建，以免费许可 (GFDL) 的形式发布。任何访问者均可编辑文章，虽然这存在恶意删改的危险，但并没有让访问者望而止步。它包含四十多万篇文章，您几乎可以找到任何主题的答案。

## 50.6 指南和手册

对于 Linux 主题，有范围广泛的指南和手册可用。

### 50.6.1 SUSE 手册

SUSE 提供详细的参考手册。我们以不同的语言提供了这些手册的 HTML 和 PDF 版本。可在 DVD 的目录 docu 中找到 PDF 文件。对于 HTML，请安装包 `opensuse-manual_LANG`（将 *lang* 替换为您首选的语言。）安装后，您可在 SUSE 帮助中心中找到它们。

### 50.6.2 其他手册

SUSE 帮助中心为各种主题或程序提供了其他手册和指南。有关详细信息，请参见<http://www.tldp.org/guides.html>。其中包括 *Bash Guide for Beginners*（Bash 初学者指南）、*Linux Filesystem Hierarchy*（Linux 文件系统层次）和 *Linux Administrator's Security Guide*（Linux 管理员安全指南）。指南通常比 HOWTO 或常见问题更为详尽。它们一般是由专家为专家编写的。其中一些手册虽然比较早，但仍然有效。使用 YaST 可安装手册和指南。

## 50.7 包文档

如果您在系统中安装包，则将创建目录 `/usr/share/doc/packages/packagename`。您可以从包维护程序查找文件以及从 SUSE 中查找其他信息。有时也有示例、配置文件、其他脚本等等可用。通常您可以找到以下文件，但是它们并不是标准的，并且有时不是所有文件都可用。

#### AUTHORS

此包的主要开发人员列表（通常也包含他们执行的任务）。

#### BUGS

此包的已知错误或故障。通常，它还包含到 Bugzilla 网页的链接，您可以在该页面上搜索所有错误。

CHANGES , ChangeLog

每个版本的更改摘要。通常开发人员会对此感兴趣，因为它非常详细。

COPYING , LICENSE

许可信息。

FAQ

从邮件列表或新闻组收集的问题和回答。

INSTALL

在系统中安装此包的过程。通常您不需要此文件，因为您已安装了包。

README , README.\*

有关如何使用该包和使用此包能够执行的操作等等的常规信息。

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。

## 50.8 Usenet

Usenet 在因特网出现之前的 1979 年建立，它是最早的计算机网络之一，现在仍在使用。Usenet 文章的格式和传输方式与电子邮件非常相似，但它是为多对多通信而开发的。

Usenet 分为七个主题类别：comp.\*计算机关联话题，misc.\*其他主题，news.\*新闻组关联话题，rec.\*消遣与娱乐，sci.\*科技关联话题，soc.\*社会话题，talk.\*各种热点话题。顶级内容分为子组。例如，comp.os.linux.hardware 是 Linux 特定硬件问题的新闻组。

在张贴文章之前，将客户端连接到新闻服务器，然后订阅特定的新闻组。新闻客户端包括 Knode 或 Evolution。每个新闻服务器都与其他新闻服务器进行通信，与它们交换文章。您的新闻服务器可能没有包括所有新闻组。

Linux 用户的兴趣新闻组是 `comp.os.linux.apps`、`comp.os.linux.questions` 和 `Comp.os.linux.hardware`。如果您无法找到特定的新闻组，请访问 <http://www.linux.org/docs/usenetlinux.html>。按照 <http://www.faqs.org/faqs/usenet/posting-rules/part1/> 联机提供的 Usenet 一般规则进行操作。

## 50.9 标准和规范

有很多信息源都提供有关标准和规范的信息。

<http://www.linuxbase.org>

自由标准组织 (Free Standards Group) 是一个独立的旨在促进自由软件和开放源代码软件发布的非营利组织。该组织致力于制定独立于各版本的标准，以期实现上述目标。包括重要的 LSB (Linux Standard Base, Linux 标准库) 在内的若干标准均由该组织负责维护。

<http://www.w3.org>

万维网联合会 (World Wide Web Consortium, W3C) 当属最知名的标准化组织之一。该组织由 Tim Berners-Lee 在 1994 年 10 月创办，主要致力于 Web 技术的标准化。W3C 提倡发布开放、不受许可证限制并且与制造商无关的规范，如 HTML、XHTML 和 XML。这些 Web 标准由多个工作组分四个阶段完成，最后以 W3C 建议 (REC) 的形式公诸于世。

<http://www.oasis-open.org>

OASIS (Organization for the Advancement of Structured Information Standards, 结构化信息标准促进组织) 是一个国际联盟，专门负责开发 Web 安全、电子商务、交易事务处理、物流和多个市场之间的互操作性等方面的标准。

<http://www.ietf.org>

因特网工程任务组 (Internet Engineering Task Force, IETF) 是一个十分活跃的国际合作组织，由众多研究人员、网络设计人员、供应商和用户组成。该组织侧重于开发因特网体系结构以及借助协议确保因特网平稳运行。

每个 IETF 标准均作为 RFC (Request for Comments, 请求注释) 发布，并且免费提供。RFC 有六种类型：推荐标准、草案标准、因特网标准、实验标准、信息文档和历史标准。从狭义上讲，只有前三种 (建议、草拟和完整标准) 才属于 IETF 标准 (请参见 <http://www.ietf.org/rfc/rfc1796.txt>)。

<http://www.ieee.org>

电气与电子工程师协会 (Institute of Electrical and Electronics Engineers, IEEE) 是负责在信息技术、电信、医药保健、运输和其他领域内制定标准的组织。IEEE 标准需付费才可获得。

<http://www.iso.org>

ISO (International Organization for Standards, 国际标准化组织) 委员会是全球最大的标准开发组织, 负责维护由 140 多个国家/地区的国家/地区标准化协会构成的庞大网络。ISO 标准需付费才可获得。

<http://www.din.de> , <http://www.din.com>

德国标准化协会 (Deutsches Institut für Normung, DIN) 是经注册的科技领域内的协会。DIN 宣称该组织是“负责德国标准化的协会, 并且在全球和欧洲标准化组织中代表德国的利益”。

该协会汇集了制造商、客户、贸易专业组织、服务公司、科学家和其他对制定标准有兴趣的人员。该协会制定的标准需付费才可获得, 可通过 DIN 主页订购。



## 常见问题及其解决方案

本章将介绍可能发生的一些常见问题，并尽可能涵盖各种潜在的问题类型。另外，即使您所遇到的情况未在本章中列出，也可以找到类似的问题，这应该足以提供解决问题的提示。

### 51.1 查找和收集信息

Linux 会记录大量的详细信息。在您使用系统遇到问题时，有几个地方可以查看，大多数是 SUSE Linux Enterprise 系统的标准问题，有一些是特定于系统的问题。多数日志文件也可以用 YaST（*其他 > 启动日志*）查看。

YaST 可提供支持团队所需的所有系统信息。使用 *其他 > 支持查询*。选择有问题的类别。当所有信息都被集合后，将其附加在您的支持请求。

以下是一个列表，其中是最常用到的日志文件及其通常所包含的内容。

**表 51.1** 日志文件

日志文件	说明
<code>/var/log/boot.msg</code>	引导期间来自内核的消息。
<code>/var/log/mail.*</code>	来自邮件系统的消息。
<code>/var/log/messages</code>	运行时来自内核和系统日志守护程序的消息。

日志文件	说明
<code>/var/log/NetworkManager</code>	<b>NetworkManager</b> 的日志文件，用于收集网络连接性问题。
<code>/var/log/SaX.log</code>	来自 <b>SaX</b> 屏幕和 <b>KVM</b> 系统的硬件消息。
<code>/home/user/.xsession-errors</code>	来自当前运行的桌面应用程序的消息。请将 <i>user</i> 替换为实际用户名。
<code>/var/log/warn</code>	所有来自内核与系统日志守护程序的消息被指定为“警告”级别或更高级别。
<code>/var/log/wtmp</code>	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 <code>last</code> 查看它。
<code>/var/log/Xorg.*.log</code>	来自 <b>X Window</b> 系统的各种启动和运行时日志。在调试失败的 <b>X</b> 启动时，该日志很有用。
<code>/var/log/YaST2/</code>	包含 <b>YaST</b> 的操作及其结果的目录。
<code>/var/log/samba/</code>	包含 <b>Samba</b> 服务器及客户机日志消息的目录。

除了日志文件外，您的计算机还可提供关于运行中的系统的信息。请参见 [表 51.2: 系统信息](#)。

**表 51.2** 系统信息

文件	描述
<code>/proc/cpuinfo</code>	此选项显示处理器信息，包括处理器类型、制造商、型号和性能。
<code>/proc/dma</code>	此选项显示当前使用的 <b>DMA</b> 通道。
<code>/proc/interrupts</code>	此选项显示正在使用的中断和已使用的中断数量。

文件	描述
/proc/iomem	此选项显示 I/O（输入/输出）内存的状态。
/proc/ioports	此选项显示当时正在使用的 I/O 端口。
/proc/meminfo	此选项显示内存状态。
/proc/modules	此选项显示各个模块。
/proc/mounts	此选项显示当前装入的设备。
/proc/partitions	此选项显示所有硬盘的分区。
/proc/version	此选项显示当前的 Linux 版本。

Linux 带有一些用于系统分析和监视的工具。请参见 [第 17 章 系统监视实用程序 \[297\]](#) 以选择在系统诊断中使用的最重要的工具。

以下包含的每个方案，都以一个描述问题的标题开头，后面是一、两段内容，提供建议的解决方案、解决方案详细信息的参考，以及对其他可能相关的方案的交叉引用。

## 51.2 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种情况的变通方案。

### 51.2.1 检查媒体

如果您使用 SUSE Linux Enterprise 安装媒体时遇到任何问题，可用软件 >，媒体检查检查安装媒体的完整性。您自行烧录的媒体更容易发生媒体问题。要检查 SUSE Linux Enterprise CD 或 DVD，请将媒体插入驱动器，单击开始让 YaST 检查媒体的 MD5 校验和。这可能要花几分钟时间。如果检测到有任何错误，则不应使用此媒体进行安装。

## 51.2.2 硬件信息

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

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

## 51.2.3 没有可用于引导的 CD-ROM 驱动器

如果您的计算机没有可引导的 CD-ROM 或 DVD-ROM 驱动器，或者 Linux 不支持您的驱动器，则有几类无需内置 CD 或 DVD 驱动器便可安装计算机的方法：

从软盘引导

创建一张引导软盘，然后从软盘而非 CD 或 DVD 引导。

使用外置的引导设备

如果它受计算机的 BIOS 和安装内核支持，就可从外置 CD 或 DVD 驱动器引导安装。

通过 PXE 进行网络引导

如果计算机没有 CD 或 DVD 驱动器，但是提供了有效的以太网连接，则可以执行完全基于网络的安装。详情请参见第 4.1.3 节“通过 VNC—PXE Boot 和“网络唤醒”进行远程安装” [46] 和第 4.1.6 节“通过 SSH—PXE Boot 和“网络唤醒”进行远程安装” [50]。

## 从软盘引导 (SYSLINUX)

在某些较老的计算机上，没有可用于引导的 CD-ROM 驱动器，但有软盘驱动器。要在此类系统上安装，需要创建引导磁盘，然后使用引导磁盘引导系统。

引导磁盘包括装载程序 SYSLINUX 和程序 linuxrc。SYSLINUX 支持在引导过程中选择内核以及指定所使用的硬件所需的任何参数。程序 linuxrc 支持为您的硬件装载内核模块并随后启动安装。

在从引导磁盘引导时，引导过程由引导加载程序 SYSLINUX (syslinux 包) 启动。当引导系统时，SYSLINUX 运行最小硬件检测，主要由以下步骤组成：

1. 该程序将检查 BIOS 是否提供符合 VESA 2.0 标准的帧缓冲支持并相应地引导内核。
2. 读取监视数据（DDC 信息）。
3. 读取第一个硬盘的第一个块 (MBR) 以在引导加载程序配置过程中将 BIOS ID 映射到 Linux 设备名。程序将尝试通过 BIOS 的 lba32 功能读取块以确定 BIOS 是否支持这些功能。

如果在 SYSLINUX 启动时按住 Shift 键，则将跳过所有这些步骤。出于查错的目的，请将行

```
verbose 1
```

插入 `syslinux.cfg` 中，以便引导加载程序显示当前正在执行哪个操作。

如果不能从软盘引导计算机，则可能需要将 BIOS 中的引导顺序更改为 A, C, CDROM。

## 外置引导设备

支持大多数 CD-ROM 驱动器。如果从 CD-ROM 驱动器引导时发生问题，请尝试使用 CD 集的 CD 2 引导。

如果系统没有 CD-ROM 或软盘驱动器，仍有希望使用通过 USB、FireWare 或 SCSI 连接的外置 CD-ROM 来引导系统。这主要取决于 BIOS 与所使用硬件的交互。如果遇到问题，有时执行 BIOS 更新可能会有用。

### 51.2.4 从安装媒体引导失败

无法引导计算机以进行安装有两种可能的原因：

CD 或 DVD-ROM 驱动器无法读取引导映像

您的 CD-ROM 驱动器可能无法读取 CD 1 上的引导映像。在这种情况下，请使用 CD 2 来引导系统。CD 2 中包含了传统的 2.88 MB 引导映像，即使是不受支持的驱动器也能够读取该映像，该 CD 还允许您通过[第 4 章 远程安装](#) [43]中介绍的方法来执行网络安装。

BIOS 中的引导顺序不正确

BIOS 引导顺序中 CD-ROM 集必须设为第一引导项。否则计算机将尝试从其他媒体引导，通常为硬盘。关于更改 BIOS 引导顺序的指导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。在此初始化阶段，计算机执行若干诊断硬件测试。其中一项测试就是内存检查，由内存计数器指示。当显示计数器时，请查找一行（通常在计数器下面，有时也在底部），该行提到要访问 BIOS 设置需要按的键。通常，要按的键是 Del 键、F1 键或 Esc 键。按此键，直到出现 BIOS 设置屏幕。

#### 过程 51.1 更改 BIOS 引导顺序

- 1 使用由引导例程声明的适当键输入 BIOS，然后等待 BIOS 屏幕出现。
- 2 若要更改 AWARD BIOS 中的引导顺序，请查找 *BIOS FEATURES SETUP* 项。其他制造商可能对该项使用不同的名称，例如 *ADVANCED CMOS SETUP*。当您找到该项后，将其选中并按 Enter 键确认。
- 3 在所打开的屏幕中，查找名为 *BOOT SEQUENCE* 的子项。引导顺序通常被设置为 C, A 或 A, C 等。在前一种情况中，计算机首先搜索硬盘 (C)，然后搜索软盘驱动器 (A) 以查找可引导媒体。通过按 PgUp 键或 PgDown 键更改设置，直到顺序为 A、CDROM 和 C。
- 4 通过按 Esc 键离开 BIOS 设置屏幕。若要保存更改，请选择 *SAVE & EXIT SETUP* 或按 F10 键。若要确认应保存设置，按 Y 键。

#### 过程 51.2 更改 SCSI BIOS (Adaptec 主机适配器) 中的引导顺序

- 1 按 Ctrl + A 打开设置。
- 2 然后选择 **磁盘实用程序**，其中将显示已连接的硬件。  
记下您 CD-ROM 驱动器的 SCSI ID。
- 3 按 ESC 退出菜单。
- 4 打开 **配置适配器设置**。在其他选项下，选择 **引导设备选项**，然后按 Enter 键。

- 5 输入 CD-ROM 驱动器的 ID，然后再次按 Enter 键。
- 6 按 Esc 键两次以返回到 SCSI BIOS 的开始屏幕。
- 7 退出此屏幕，并确认是以引导计算机。

无论最终安装将使用何种语言及键盘布局，大多数 BIOS 配置使用下图所示的美式键盘布局：

图 51.1 美式键盘布局



## 51.2.5 无法引导

某些硬件类型（主要是过旧或非常新的硬件）可能无法安装。在许多情况下，可能由于从安装内核中丢失的此类硬件的支持或由该内核中包含的某些功能（如 ACPI，它会在某些硬件上引起问题）而引起的。

如果系统无法使用第一个安装引导屏幕上的标准安装方式进行安装，请尝试使用以下方法：

- 1 将第一张 CD 或 DVD 留在 CD-ROM 驱动器中，然后使用 Ctrl + Alt + Del 组合键或硬件重设置按钮重引导计算机。
- 2 在出现引导屏幕时，使用键盘上的箭头键浏览至安装—禁用 ACPI，然后按 Enter 键启动引导和安装过程。此选项将禁用对 ACPI 电源管理技术的支持。

### 3 按第 3 章 使用 *YaST* 进行安装 [17]中所述的步骤进行安装。

如果这失败，请按照以上步骤继续，但应选择安装—安全设置。此选项将禁用 ACPI 和 DMA 支持。大多数硬件应使用此选项引导。

如果以上两个选项都失败，请使用引导选项提示向安装内核传递支持此硬件类型所需的任何其他参数。关于可用作引导选项的参数的更多信息，请参见 `/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。

`pnpacpi=off`

此选项用于您的 BIOS 设置包含错误中断或端口时发生的串行或并行问题。



`notsc`

禁用时戳计数器。此选项可用于解决系统上的计时问题。这是个新功能，如果在您的计算机上发现性能下降，尤其是与时间相关的性能下降，甚至是整个挂起，则值得尝试使用该选项。

`nohz=off`

禁用 `nohz` 功能。如果您的计算机挂起，则此选项可能有帮助。通常不需要此选项。

一旦确定了正确的参数组合，YaST会自动将其写入引导加载程序配置中以确保系统下一次能够正确引导。

如果在装载内核或安装过程中出现无法解释的错误，则在引导菜单中选择*内存测试*以检查内存。如果*内存测试*返回一个错误，则通常这是硬件错误。

## 51.2.6 无法启动图形安装程序

在将第一张 CD 或 DVD 插入驱动器并重引导计算机之后，出现安装屏幕，但是在选择安装之后，图形安装程序没有启动。

有多种方法可解决此情况：

- 尝试为安装对话框另选一种屏幕分辨率。
- 选择文本方式进行安装。
- 使用图形安装程序进行远程安装（通过 VNC）。

要切换到其他屏幕分辨率以进行安装，请执行如下操作：

- 1 引导以安装。
- 2 按 **F3** 键打开一个菜单，从中选择一个较低的安装分辨率。
- 3 选择安装，然后按**第 3 章 使用 YaST 进行安装** [17]中所述的步骤进行安装。

要以文本方式进行安装，请执行如下步骤：

- 1 引导以安装。

- 2 按 F3，然后选择文本方式。
- 3 选择安装，然后按第 3 章 *使用 YaST 进行安装* [17]中所述的步骤进行安装。

要执行 VNC 安装，请执行如下操作：

- 1 引导以安装。
- 2 在引导选项提示下输入以下文本：

```
vnc=1 vncpassword=some_password
```

将 *some\_password* 替换为用于安装的密码。

- 3 选择安装，然后按 Enter 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到安装程序的 IP 地址和端口号。

- 4 如果使用浏览器来访问安装程序，请启动浏览器并输入由未来 SUSE Linux Enterprise 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 3 章 *使用 YaST 进行安装* [17]中所述的步骤进行安装。

---

## 重要

通过 VNC 安装这一方法可在任意操作系统下的任意浏览器上进行，只要启用了 Java 支持即可。

---

如果您在所采用的操作系统上使用了任意种类的 VNC 查看器，请在看到提示时输入 IP 地址和密码。然后，将打开一个窗口，其中显示了多个安装对话框。照常进行安装。

## 51.2.7 只能启动简陋的引导屏幕

将第一张 CD 或 DVD 插入了驱动器，BIOS 例程结束，但是系统未启动图形引导屏幕。而是启动了一个非常简陋的基于文本的界面。如果计算机的显存不足而无法生成图形引导屏幕，则可能发生这种情况。

虽然文本引导屏幕看起来比较简陋，但是它所提供的功能与图形引导屏幕几乎是相同的。

### 引导选项

与图形界面不同的是，不能使用键盘的鼠标键来选择其他引导选项。文本引导屏幕上的引导菜单提供了一些可在引导提示下输入的关键字。这些关键字与图形版本中提供的选项相对应。输入您的选择，然后按 **Enter** 键以启动引导过程。

### 自定义引导选项

在选择引导选项之后，请在引导提示下输入相应的关键字，或者根据第 51.2.5 节“无法引导”[825]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**。

## 51.3 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）。

### 51.3.1 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 在安装方式屏幕中，选择其他，然后将安装方式设置为修复已安装系统。
- 7 然后在“YaST 系统修复”模块中，选择专家工具，再选择安装新引导加载程序。
- 8 恢复原始设置并重安装引导加载程序。
- 9 退出“YaST 系统修复”模块并重引导系统。

如果由于某种原因，图形界面不显示，或宁愿手动修复系统，请参考[“使用救援系统”一节](#) [848]获取指导。

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。

## 51.3.2 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：

```
nld-machine:~ # grep "id:" /etc/inittab
id:5:initdefault:
nld-machine:~ #
```

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，则您的桌面或 X Window 软件可能发生损坏。请检验 `/var/log/Xorg.*.log` 中的日志文件，查找它尝试启动的 X 服务器发出的详细消息。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。

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。有关 X Window 系统配置的更多信息，请参见第 26 章 *X Window 系统* [439]。

## 51.4 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）。

### 51.4.1 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 51.5 节“网络问题” [837]。

- 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 51.5 节“网络问题”[837]。
- 如果系统配置为使用 Kerberos，则系统的本地时间与 Kerberos 服务器时间之间的差异可能超过了可接受的值（通常为 300 秒）。如果 NTP（网络时间协议）未正确地起作用，或者本地 NTP 服务器不起作用，则 Kerberos 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 27 章 *通过 PAM 进行身份验证* [451]。

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。

## 51.4.2 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。

- 身份验证该特定用户的 X Window 系统可能存在问题，尤其是在安装当前产品之前，该用户的主目录已被其他 Linux 产品所使用时。

要找到本地登录失败的原因，请执行如下操作：

- 1 在尝试调试整个身份验证机制之前，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”模块来更改用户的密码。
- 2 以 root 用户身份登录并检查 `/var/log/messages` 以找到登录过程和 PAM 的错误消息。
- 3 尝试从控制台登录（使用 `Ctrl+Alt+F1`）。如果成功了，则问题不在 PAM 上，因为可以在该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 51.4.3 节“登录成功但 GNOME 桌面发生故障”[835]和第 51.4.4 节“登录成功但 KDE 桌面发生故障”[836]。
- 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。然后重试图形登录。
- 5 如果图形登录依然失败，请使用 `Ctrl + Alt + F1` 进行控制台登录。尝试在另一个屏幕上启动 X 会话，第一个 (:0) 已经在使用中：

```
startx -- :1
```

这样应该可以显示图形屏幕和桌面。如果无效，请查看 X 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 51.4.3 节“登录成功但 GNOME 桌面发生故障”[835]或第 51.4.4 节“登录成功但 KDE 桌面发生故障”[836]。

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。
- 身份验证该特定用户的 X Window 系统可能存在问题，尤其是在安装当前产品之前，该用户的主目录已被其他 Linux 产品所使用时。

要通过网络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信。
- 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**）。如果成功了，则问题不在用户主目录中的 PAM 或目录服务器上，因为可以在该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 51.4.3 节“登录成功但 GNOME 桌面发生故障”[835]和第 51.4.4 节“登录成功但 KDE 桌面发生故障”[836]。
- 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。然后重试图形登录。



- 7 如果图形登录依然失败，请使用 **Ctrl + Alt + F1** 进行控制台登录。尝试在另一个屏幕上启动 X 会话，第一个 (:0) 已经在使用中：

```
startx -- :1
```

这样应该可以显示图形屏幕和桌面。如果无效，请查看 X 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 51.4.3 节“登录成功但 GNOME 桌面发生故障”[835]或第 51.4.4 节“登录成功但 KDE 桌面发生故障”[836]。

## 51.4.3 登录成功但 GNOME 桌面发生故障

如果这发生于特定用户，则可能是由于该用户的 GNOME 配置文件已损坏。可能出现的症状有键盘不起作用、屏幕几何图形变形，甚至整个屏幕变成灰色。而最重要的差别在于其他用户登录时，该计算机能正常运行。如果属于这种情况，只需将用户的 GNOME 配置目录移到某个新位置，以便使 GNOME 初始化一个新的桌面，这样就能很快地解决此问题。虽然用户不得不重配置 GNOME，但不会丢失任何数据。

- 1 按 **Ctrl + Alt + F1** 切换到文本控制台。
- 2 用您的用户名登录。
- 3 将用户的 GNOME 配置目录移到某个临时位置：

```
mv .gconf .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

- 4 注销。
- 5 再次登录，但别运行任何应用程序。
- 6 通过以下命令将 `~/ .gconf-ORIG-RECOVER/apps/` 目录复制回新的 `~/ .gconf` 目录，这样就能恢复您的个人应用程序配置数据（包括 Evolution 电子邮件客户程序数据）：

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

如果这引起登录问题，则尝试只恢复重要的应用程序数据并重配置其他的应用程序。

## 51.4.4 登录成功但 KDE 桌面发生故障

KDE 桌面不允许用户登录有多种原因。高速缓存数据以及 KDE 桌面配置文件的损坏都可能引起登录问题。

桌面在启动时会用到缓存数据，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/socket-user
```

请将 `user` 替换为实际用户名。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：

```
mv .kde .kde-ORIG-RECOVER  
mv .skel .skel-ORIG-RECOVER
```

- 4 注销。
- 5 再次登录。
- 6 在成功启动桌面之后，将用户自己的配置复制回原来的位置：

```
cp -a .kde-ORIG-RECOVER/share .kde/share
```

---

## 重要

如果用户自己的调整先前引起了登录失败并仍然如此，请重复上述步骤，但是不要复制 `.kde/share` 目录。

---

## 51.5 网络问题

系统的许多问题可能都与网络相关，即使初看起来不是这样。例如，系统不允许用户登录的原因可能是某种网络问题造成的。本节将引入一个简单的核对表，您可以使用它来确定任何所遇到的网络问题的原因。

在检查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。请确保网线已正确地插入计算机。以太网连接器旁边的控制灯（如果有的话）应全部亮起。

如果连接失败，请检查网线在别的计算机上是否正常。如果正常，则可能是网卡引起了该问题。如果网络设置中包含集线器和交换机，也需要对它们进行检查。

- 2 如果使用的是无线连接，请检查是否可与其他计算机建立此无线链接。如果无法建立，请与无线网络管理员联系。
- 3 一旦完成了对基本网络连通性的检查，请尝试找出没有响应的服务。收集设置中所需的所有网络服务器的地址信息。在相应的 YaST 模块中查找这些信息，或者询问您的系统管理员。以下列表给出了设置中涉及的一些典型网络服务器问题以及服务中断的症状。

### DNS（名称服务）

名称服务中断或发生故障会在许多方面影响网络运行。如果本地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 安装目录中，则一旦此服务停止或配置错误，应用程序将无法启动或正常运行。最坏的情况是，如果由于 NFS 服务器宕机而无法找到包含 `.gconf` 或 `.kde` 子目录的主目录，则该主目录所属的用户的个人桌面配置将无法启动。

#### Samba（文件服务）

如果任何应用程序所需的数据储存在 Samba 服务器上的某个目录中，则一旦此服务停止，则应用程序将无法启动或正常运行。

#### NIS（用户管理）

如果您的 SUSE Linux Enterprise 系统依赖于 NIS 服务器提供用户数据，则一旦 NIS 服务停止，用户将无法登录到该计算机。

#### LDAP（用户管理）

如果您的 SUSE Linux Enterprise 系统依赖于 LDAP 服务器提供用户数据，则一旦 LDAP 服务停止，用户将无法登录到该计算机。

#### Kerberos（身份验证）

如果此服务停止，则身份验证将不起作用，且用户无法登录到任何计算机。

#### CUPS（网络打印）

如果此服务停止，用户将无法进行打印。

### 4 请检查网络服务器是否正在运行并且您的网络设置是否允许您建立连接：

---

#### 重要

下面介绍的调试步骤只适用于简单的网络服务器/客户机设置，不涉及任何内部路由。假设服务器和客户机都是同一子网的成员，不需要额外的路由。

---

- 4a** 可使用 `ping hostname`（将 `hostname` 替换为服务器的主机名）来检查各台服务器是否正在运行且能够对网络作出响应。如果此命令成功，表示您所查找的主机在正常运行，并且网络的名称服务配置正确。

如果 `ping` 命令失败，同时显示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`

`your_hostname` 命令来检查您的系统是否可被访问。如果可以从其  
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。请使用 `ping -nipaddress` 尝试连接到这  
一没有名称服务的主机。如果成功，则请检查主机名的拼写是否正确  
以及网络中的名称服务是否配置正确。要对该问题进行进一步的检  
查，请参见 [步骤 4b](#) [839]。如果 `ping` 命令仍然失败，则可能网卡未正  
确配置或网络硬件存在故障。有关此问题的信息，请参见 [步骤 4c](#)  
[840]。

- 4b** 请使用 `host hostname` 来检查您尝试连接的服务器的主机名是否  
能够正确地转换为 IP 地址，反之亦然。如果此命令返回了该主机的 IP  
地址，则名称服务已在正常运行。如果 `host` 命令失败，请检查您主  
机上所有与名称和地址解析相关的网络配置文件：

`/etc/resolv.conf`

此文件用于对当前使用的名称服务器和域进行跟踪。您可手动修  
改该文件，或者由 YaST 或 DHCP 自动调整。建议采用自动调整。  
但是，请确保此文件具有以下结构并且所有的网络地址和域名都  
正确无误：

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

此文件中可以包含多个名称服务器地址，但是其中必须至少有一  
个能够对您的主机提供正确的名称解析。如果需要，可使用“YaST  
DNS 和主机名”模块调整该文件。

如果网络连接是通过 DHCP 处理的，请在“YaST DNS 和主机名”  
模块中选择 *通过 DHCP 更改主机名* 和 *通过 DHCP 更新名称服务器  
和搜索列表*，以启用 DHCP 来更改主机名和名称服务信息。

`/etc/nsswitch.conf`

此文件告诉 Linux 到何处查找名称服务信息。它应显示为：

```
...
hosts: files dns
networks: files dns
...
```

`dns` 条目是必需的。它告诉 Linux 要使用外部名称服务器。通常情况下, 这些条目是由 YaST 自动建立的, 但是从不会影响检查。

如果主机上的所有相关条目均正确, 请让系统管理员检查 DNS 服务器配置, 以确定时区信息是否正确。有关 DNS 的详细信息, 请参见 [第 33 章 域名系统](#) [555]。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的地所经过的所有网关 (中继)。它列出了每个中继的响应时间以及该中继是否可访问。请将 `traceroute` 和 `ping` 结合使用以确定故障原因并通知管理员。

一旦确定了网络故障的原因, 就可以自行解决 (如果问题出在您自己的计算机上), 或告诉网络系统管理员您的发现, 以便其重配置服务或修复必要的系统。

## 51.5.1 NetworkManager 问题

如果网络连接有问题, 请按 [837] 中所述缩小范围。如果 NetworkManager 看上去是 culprit, 请按如下步骤操作, 获得日志, 它会提供 NetworkManager 为何失效的线索:

- 1 以 root 用户身份打开 shell 并登录。

- 2 重新启动 NetworkManager:

```
rcnetwork restart -o nm
```

- 3 作为普通用户打开 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 30.6 节“使用 NetworkManager 管理网络连接”[526]。

## 51.6 数据问题

数据问题是指无论计算机是否能够正常引导，有一点是明确的，即系统上的数据损坏了，并且系统需要恢复。这些情况下需要对关键数据进行备份，以便您能够在系统出现故障时恢复故障前的状态。SUSE Linux Enterprise 提供了专用的 YaST 模块用于系统备份和恢复，此外还提供了一个救援系统，用于从外部恢复受损的系统。

### 51.6.1 备份关键数据

可使用“YaST 系统备份”模块轻松管理系统备份：

- 1 以 root 用户身份启动 YaST，然后选择系统 > 系统备份。
- 2 创建一个存放备份所需的所有详细信息、存档文件的文件名以及备份范围和类型的备份配置文件：
  - 2a 选择配置文件管理 > 添加。
  - 2b 输入存档文件的名称。
  - 2c 如果想要保留本地备份，请输入备份位置的路径。如果要将备份存档在网络服务器上（通过 NFS），请输入 IP 地址或服务器名称以及存放存档文件的目录。
  - 2d 确定存档类型，然后单击下一步。

- 2e** 确定要使用的备份选项，例如是否要对不属于任何包的文件进行备份以及在创建存档文件之前是否显示文件列表。此外，确定是否使用耗费时间的 MD5 机制来确定更改过的文件。

使用专家进入备份整个硬盘区域的对话框。目前该选项仅适用于 Ext2 文件系统。

- 2f** 最后，设置搜索约束条件，以将某些不需要备份的系统区域排除在备份区域之外，如锁文件或高速缓存文件。添加、编辑或删除项目，直到符合要求为止，然后单击**确定**退出。

- 3** 一旦完成了配置文件设置，就可以单击**创建备份**立即开始备份，或者配置自动备份。此外，还可以创建用于其他各种用途的配置文件。

要为指定的配置文件配置自动备份，请执行如下操作：

- 1** 在**配置文件管理**菜单中选择**自动备份**。
- 2** 选择**自动启动备份**。
- 3** 确定备份频率。选择**每天**、**每周**或**每月**。
- 4** 确定备份开始时间。这些设置取决于所选择的备份频率。
- 5** 确定是否保留旧的备份以及保留的个数。要自动接收备份过程自动生成的状态消息，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。

## 51.6.2 恢复系统备份

请使用“YaST 系统恢复”模块从备份恢复系统配置。可恢复整个备份，或选择已损坏并需要重置为先前状态的特定部分。



- 1 启动 *YaST* > 系统 > 系统恢复。
- 2 输入备份文件的位置。这可以是本地文件、网络安装文件或移动设备（如软盘或 CD）上的文件。然后单击下一步。

以下对话框显示了存档文件属性（如文件名、创建日期、备份类型和可选的注释）的摘要。

- 3 可单击存档文件内容来查看已存档的内容。单击确定可返回到存档文件属性对话框。
- 4 单击专家选项将打开一个对话框，在其中可对恢复过程进行微调。单击确定可返回到存档文件属性对话框。
- 5 单击下一步可打开要恢复的包的视图。按接受可恢复该存档文件中的所有文件，或者使用各个全选、取消选择全部和选择文件按钮对所选存档文件进行微调。如果 RPM 数据库损坏或被删除，且该文件包含在备份中，则只需使用恢复 RPM 数据库选项。
- 6 在单击接受之后，将恢复备份。在恢复过程完成后，单击完成将退出此模块。

## 51.6.3 恢复受损的系统

有多种原因会造成系统无法正常启动和运行。系统崩溃后造成文件系统损坏、配置文件损坏或引导加载程序配置损坏是最常见的原因。

SUSE Linux Enterprise 提供两种不同的方式来处理这种情况。您可以使用 *YaST* 系统修复功能，也可以引导救援系统。以下小节将介绍两种系统修复的功能。

### 使用 *YaST* 系统修复

在启动 *YaST* 系统修复模块之前，确定要运行该模块的方式以最佳满足您的需要。依据系统故障的严重性和原因以及您的专业知识，在三个不同的方式进行选择：

## 自动修复

如果由于未知原因系统发生故障并且您基本上不知道系统的哪个部分导致此故障，则使用 *自动修复*。将会对您安装的系统上的所有组件执行全面的自动化检查。有关此过程的详细描述，请参见“**自动修复**”一节 [844]。

## 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 [846]。

## 专家工具

如果您已经清楚地知道哪个组件发生故障和修复此故障的方法，则您可以跳过分析运行并直接应用修复相关组件的所需的工具。有关详细信息，请参见“**专家工具**”一节 [847]。

选择以上描述的一个修复方式并按以下部分所述继续执行系统修复。

## 自动修复

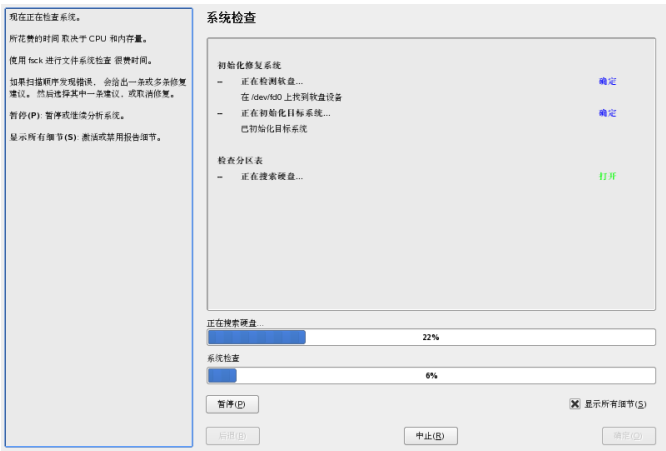
要启动 YaST 系统修复的自动修复方式，请如下执行操作：

- 1 将第一张 SUSE Linux Enterprise 安装媒体插入 CD 或 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕中选择安装。
- 4 选择语言并单击 *下一步*。
- 5 确认许可证协议并单击 *下一步*。
- 6 在系统分析中，选择 *其他 > 修复已安装系统*。
- 7 选择 *自动修复*。

YaST 现在对已安装系统启动全面分析。屏幕的底部使用两个进度条显示此过程的进度。上面的进度条显示当前正在运行的测试的进度。下面的进度条显示分析进程的总体进度。上面的日志窗口用于跟踪当前运行的

测试及其结果。请参见图 51.2 “自动修复方式” [845]。每次运行都会执行以下主要测试。这些测试又包含许多单独的子测试。

图 51.2 自动修复方式



所有硬盘的分区表

检查所有检测到的硬盘的分区表的有效性和一致性。

交换分区

检测并测试已安装系统的交换分区，并在合适的情况下建议激活交换分区。应该接受这一建议以实现更高的系统修复速度。

文件系统

所有检测到的文件系统都需要进行特定于文件系统的检查。

文件 /etc/fstab 中的项

检查文件中项的完整性和一致性。将装入所有有效的分区。

引导加载程序配置

检查已安装系统（GRUB 或 LILO）的引导加载程序配置的完整性和一致性。将检查引导和根设备，并将检查 initrd 模块的可用性。

包数据库

这将检查执行最小安装的操作所需的所有包是否存在。虽然还可以分析基础包，但因为基础包数量太大，将花费很长时间。

- 8 当出现错误时，过程将停止并打开一个对话框，其中描述了详细信息和可能的解决方案。

在接受建议修复之前仔细阅读屏幕消息。如果您确定拒绝建议的解决方案，您的系统将保持不变。

- 9 在修复过程成功终止之后，单击*确定和完成*，除去安装媒体。系统将自动重引导。

## 自定义修改

要启动*自定义修复*方式并选择性地检查所安装系统的某些组件，请如下执行操作：

- 1 将 SUSE Linux Enterprise 的第一张安装媒体插入 CD 或 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕中选择安装。
- 4 选择语言并单击*下一步*。
- 5 确认许可证协议并单击*下一步*。
- 6 在系统分析中，选择*其他 > 修复已安装系统*。
- 7 选择*自定义修复*。

选择*自定义修复*将显示一组测试，这些测试最初都被标记为准备执行。这些测试的总范围和自动修复的测试范围一致。如果您清楚哪些方面没有损坏，则取消对应测试的标记。单击*下一步*将启动一个范围相对较小的测试过程，可能将显著缩短运行时间。

并不是所有的测试组都单独适用。fstab 项的分析会始终与文件系统（包括现有的交换分区）检查一起进行。YaST 会通过选择必需运行的最少测试数量来自动解决此类依赖性。

- 8 当出现错误时，过程将停止并打开一个对话框，其中描述了详细信息和可能的解决方案。

在接受建议修复之前仔细阅读屏幕消息。如果您确定拒绝建议的解决方案，您的系统将保持不变。

- 9 在修复过程成功终止之后，单击**确定和完成**，除去安装媒体。系统将自动重引导。

## 专家工具

如果您熟悉 SUSE Linux Enterprise，并且已非常清楚系统中所需的修复，请跳过系统分析来直接应用工具。

要使用 YaST 系统修复模块的专家工具功能，请如下进行操作：

- 1 使用您用于初始安装（如**第 3 章 使用 YaST 进行安装** [17]中所述）的原始安装媒体来引导系统。
- 2 在系统分析中，选择**其他 > 修复已安装系统**。
- 3 选择**专家工具**，并选择一个或多个修复选项。
- 4 在修复过程成功终止之后，单击**确定和完成**，除去安装媒体。系统将自动重引导。

专家工具提供下列选项修复您的错误系统：

### 安装新的 Boot Loader

这将启动 YaST 引导加载程序配置模块。详细信息请参见**第 21.3 节 “使用 YaST 配置引导加载程序”** [378]。

### 启动分区工具

这将启动 YaST 中的专家分区工具。

### 修复文件系统

这将检查已安装系统的文件系统。首先将向您提供所有检测到的分区的选择，您可以在其中选择要检查的分区。

### 恢复丢失的分区

可以尝试重建损坏的分区表。首先将显示检测到的硬盘的列表以供选择。单击**确定**开始检查。这可能要花一段时间，具体取决于处理能力和硬盘的大小。

---

## 重要：重建分区表

重建分区表非常麻烦。YaST 尝试通过分析硬盘的数据扇区识别丢失的分区。在识别出丢失的分区之后，会添加它们以重建分区表。但是，此操作不能保证在所有可能的情况下都成功。

---

将系统设置保存到软盘

此选项将重要的系统文件保存到软盘上。如果这些文件中的某个文件被损坏，可以从磁盘恢复该文件。

校验安装的软件

这将检查包数据库的一致性和最重要包的可用性。使用此工具可以重安装任何损坏的已安装包。

## 使用救援系统

SUSE Linux Enterprise 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 磁盘并以根文件系统的形式装入，使您可以从外部访问 Linux 分区。使用该救援系统，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。
- 检查文件系统中的缺陷和启动自动修复进程。
- 访问“更改根”环境下的已安装系统。
- 检查、修改和重安装引导加载程序配置
- 使用 `parted` 命令调整分区大小。有关该工具的更多信息，请访问 GNU Parted 网站 (<http://www.gnu.org/software/parted/parted.html>)。

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 CD 或 DVD 上引导该救援系统：

- 1 将安装媒体插入 CD 或 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕中，选择救援系统选项。

**4** 在 Rescue：提示符处输入 root。无需密码。

如果硬件设置不包含 CD 或 DVD 驱动器，可以从网络源引导该救援系统。以下范例适用于远程引导的情形，如果使用另一引导媒体（例如软盘），则要相应地修改 info 文件，并像正常安装一样进行引导。

**1** 输入您的 PXE 引导设置的配置，并用

```
rescue=protocol://instsource 替换  
install=protocol://instsource。如同正常安装的情况一样，  
protocol 代表任何一种所支持的网络协议（NFS、HTTP、FTP 等）；  
instsource 代表网络安装源的路径。
```

**2** 如第 4.3.7 节“局域网唤醒”[68]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 + F6 到 Alt + F1 键来使用虚拟控制台。

可以在 /bin 目录下找到 shell 和许多其他有用的实用程序，如 mount 程序。sbin 目录包含重要的用于查看和修复文件系统的文件和网络实用程序。此目录还包含用于系统维护的最重要的二进制文件，如 fdisk、mkfs、mkswap、mount、mount、init 和 shutdown，以及用于维护网络的 ifconfig、ip、route 和 netstat。目录 /usr/bin 包含 vi 编辑器、find、less 和 telnet。

要查看系统消息，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 下的根文件系统，请使用如下命令：

```
mount /dev/sda6 /mnt
```

系统所有目录现在均位于 /mnt 之下

**3 将目录切换为所装入的根文件系统：**

```
cd /mnt
```

**4 在 vi 编辑器中打开有问题的配置文件。调整并保存配置。**

**5 从救援系统中卸载根文件系统：**

```
umount /mnt
```

**6 重引导计算机。**

## 修复和检查文件系统

通常，不能在正在运行的系统上修复文件系统。如果遇到严重问题，您甚至都无法装入根文件系统，系统引导可能以显示 kernel panic 结束。在这种情况下，唯一的方法是从外部修复系统。强烈建议使用 YaST 系统修复功能执行此任务（请参见“[使用 YaST 系统修复](#)”一节 [843]以了解详细信息）。但是，如果需要执行手动文件系统检查或修复，请引导救援系统。该功能包含检查并修复 ext2、ext3、reiserfs、xfs、dosfs 以及 vfat 文件系统的实用程序。

## 访问已安装系统

如果要从应急系统访问已安装系统，例如，要修改引导加载程序配置或执行硬件配置实用程序，则需要在“更改根”环境下进行。

要设置基于已安装系统的“更改根”环境，请执行以下步骤：

**1 首先装入已安装系统和设备文件系统的根分区：**

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

**2 现在可以“更改根”为新的环境：**

```
chroot /mnt
```

**3 然后装入 /proc 和 /sys：**



```
mount /proc
mount /sys
```

#### 4 最后，装入已安装系统的剩余分区：

```
mount -a
```

#### 5 现在可以访问已安装系统了。在重引导系统之前，请用 `umount -a` 卸载分区并用 `exit` 退出“更改根”环境。

---

### 警告：限制

尽管对已安装系统的文件和应用程序有完全访问权，但仍有一些限制。正在运行的内核是以前使用救援系统引导的内核。该内核只支持关键性硬件，不可能从已安装系统添加内核模块，除非内核版本完全一致（这没有可能性）。举例来说，这样您将无法访问声卡。也不可能启动图形用户界面。

还应注意，在使用 **Alt + F1** 到 **Alt + F6** 键切换控制台时，要退出“更改根”环境。

---

## 修改和重安装引导加载程序

有时，系统无法引导是因为引导加载程序配置已损坏。例如，如果没有正常工作的引导加载程序，启动例程将无法将物理驱动器转化为 Linux 文件系统中的实际位置。

要检查引导加载程序配置并重安装引导加载程序，请执行以下操作：

- 1 如“**访问已安装系统**”一节 [850]中所述执行必要的步骤以访问已安装系统。
- 2 依据**第 21 章 引导加载程序** [369]中所述 GRUB 配置原则，检查下列文件是否正确配置。

- `/etc/grub.conf`
- `/boot/grub/device.map`
- `/boot/grub/menu.lst`

如有必要，将修复程序应用于根分区及配置文件的设备映射(device.map)或位置。

- 3 使用以下命令序列重安装引导加载程序：

```
grub --batch < /etc/grub.conf
```

- 4 卸载分区，从“更改根”环境中注销并重引导该系统：

```
umount -a  
exit  
reboot
```

## 51.7 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 ziplt 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 ziplt 程序来更新 IPL 记录。

### 51.7.1 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 *Architecture-Specific Information* 中的第 2.1 节“Making the Installation Data Available”（第 2 章 *Preparing for Installation*, ↑*Architecture-Specific Information*）。此外，您还需要设备的通道号和设备内包含 SUSE Linux Enterprise Server 安装的根文件系统的分区号。

---

首先，按照 *Architecture-Specific Information* 手册中的说明对 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。

## 51.7.2 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 51.3 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 51.4 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：

```
zfcpx_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：

```
zfcpx_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。

## 51.7.3 装入根设备

如果所有所需设备都为联机, 则现在应该能够装入根设备。假定根设备位于 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 51.1 *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)
```

## 51.7.4 更改为已装入的文件系统

为了使 `zipl` 命令从已安装系统的根设备而非救援系统读取配置文件, 请使用 `chroot` 命令将根设备更改为已安装系统:

### 例 51.2 将根设备更改为已装入的文件系统

```
SuSE Instsys suse:/ # cd /mnt
SuSE Instsys suse:/mnt # chroot /mnt
```

## 51.7.5 执行 zipl

现在执行 zipl 用正确的值改写 IPL 记录。

### 例 51.3 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
```

## 51.7.6 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根目录，然后卸载 SUSE Linux Enterprise Server for IBM System z 安装的根设备。

### 例 51.4 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 3.13.1 节 “IBM System z: 对已安装系统执行 IPL”](#) [32] 一章中的说明对 SUSE Linux Enterprise Server 系统进行初始程序装载了。



# 索引

## 符号

- 64 位 Linux, 349
  - 内核规范, 353
  - 软件开发, 350
  - 运行时支持, 350
- 专用交换机, 520
- 主引导记录 (见 MBR)
- 主机名, 151
- 代理, 153, 703 (见 Squid)
  - 优点, 703
  - 缓存, 703
  - 透明, 713
- 伪装, 739
  - 用 SuSEfirewall2 进行配置, 741
- 便携式计算机
  - 电源管理, 459-470
- 信息页, 392
- 修复系统, 843
- 内存
  - RAM, 392
- 内核
  - 缓存, 392
  - 限制, 437
- 分区
  - EVMS, 142
  - fstab, 144
  - LVM, 142
  - RAID, 142
  - 分区表, 369
  - 创建, 29, 139, 141
  - 加密, 780
  - 参数, 142
  - 类型, 141
  - 重格式化, 142
- 加密, 779-783
  - 分区, 780-781

- 创建分区, 780
- 可移动媒体, 782
- 文件, 782-783
- 用 YaST, 780

## 包

- LSB, 285
- RPM, 285
- 使用 build 编译, 294
- 包管理器, 285
- 卸载, 286
- 安装, 286
- 校验, 285
- 编译, 292

## 包管理

- zmd, 179

- 包过滤器 (见 防火墙)

## 协议

- CIFS, 629
- IPv6, 500
- LDAP, 599
- SLP, 545
- SMB, 629

## 卡

- 图形, 443
- 声音, 136

## 卸载

- GRUB, 383
- Linux, 383

- 发行说明, 40, 164

## 变量

- 环境, 395

- 可插拔身份验证模块 (见 PAM)

- 名称服务器 (见 DNS)

- 命令, 331-341

- bzip2, 327
- cat, 336
- cd, 333
- chgrp, 331, 333
- chmod, 330, 333
- chown, 331, 333

- cp, 332
- date, 339
- df, 338
- diff, 337
- du, 338
- file, 336
- find, 336
- fonts-config, 446
- free, 339, 392
- getfacl, 278
- grep, 337
- grub, 370
- gzip, 327, 334
- halt, 341
- ifconfig, 539
- ip, 537
- kadmin, 765
- kill, 340
- killall, 340
- kinit, 771
- ktadd, 773
- ldapadd, 610
- ldapdelete, 613
- ldapmodify, 612
- ldapsearch, 612, 777
- less, 336
- ln, 333
- locate, 336
- lp, 409
- ls, 332
- man, 331
- mkdir, 333
- mount, 337
- mv, 332
- nslookup, 340
- passwd, 341
- ping, 340, 539
- ps, 339
- reboot, 341
- rm, 333
- rmdir, 333
- rpm, 285
- rpmbuild, 285
- scp, 748
- setfacl, 279
- sftp, 749
- slptool, 546
- smbpasswd, 638
- ssh, 748
- ssh-agent , 751
- ssh-keygen , 750
- su, 341
- tar, 326, 335
- telnet, 341
- top, 339
- umount, 338
- updatedb, 336
- 帮助, 320
- 清除, 341
- 路由, 540
- 因特网
  - cinternet, 543
  - DSL, 521
  - ISDN, 518
  - KInternet, 543
  - qinternet, 543
  - smpppd, 542-544
  - Tdsl, 523
  - 拨号, 542-544
- 国际化, 395
- 图形
  - 卡
    - 驱动程序, 443
- 域名系统 (见 DNS)
- 声音
  - 在 YaST 中配置, 136
- 备份, 131
  - 使用 YaST 创建, 138
  - 恢复, 138
- 字体, 446



- TrueType, 445
- X11 核心, 446
- Xft, 447
- 安全性, 795-805
  - DNS, 802
  - RPM 签名, 804
  - Samba, 636
  - Squid, 704
  - SSH, 747-752
  - tcpd, 805
  - telnet, 747
  - X, 800
  - 串行终端, 796
  - 密码, 797
  - 工程, 796
  - 引导, 796, 798
  - 报告问题, 805
  - 提示和技巧, 803
  - 攻击, 801-803
  - 本地, 797-800
  - 权限, 798
  - 病毒, 799
  - 网络, 800-803
  - 蠕虫, 803
  - 配置, 154-163
  - 错误, 799, 801
  - 防火墙, 163, 737
- 安装
  - GRUB, 370
  - YaST, 用, 17-41
  - 包, 286
  - 手动, 208
  - 目录, 到, 131
- 密码
  - 更改, 341
- 屏幕
  - 分辨率, 442
- 帮助, 809-812
  - HOWTO, 814
  - Linux 文档 (TLPD), 814

- SUSE 帮助中心, 809
- SUSE 手册, 815
- Usenet, 816
- Wikipedia, 814
- X, 444
- 信息页, 392, 813
- 包文档, 815
- 常见问题, 814
- 手册, 815
- 手册页, 331, 392, 812
- 指南, 815
- 标准, 817
- 规范, 817
- 并且 ALSA 配置数据
  - 配置文件, 137
- 引导, 355
  - CD, 从, 823
  - GRUB, 369-386
  - initramfs, 356
  - initrd, 356
  - 图形, 384
  - 引导扇区, 369
  - 日志, 165
  - 软盘, 从, 822
  - 配置
    - YaST, 378
- 手册页, 331, 392
- 打印, 399
  - CUPS, 408
  - GDI 打印机, 413
  - kprinter, 408
  - Samba, 630
  - xpp, 408
  - 命令行, 409
  - 查错
    - 网络, 415
  - 用 YaST 配置, 402-406
    - 本地打印机, 402
    - 网络打印机, 405
  - 网络, 415

- 控制台
  - 切换, 394
  - 图形, 384
  - 指派, 394
- 支持查询, 819
- 救援系统, 848, 852
  - 从 CD 启动, 848
  - 从网络源启动, 849
- 文件
  - 删除, 333
  - 加密, 782
  - 压缩, 326, 334
  - 同步, 657-666
    - CVS, 658, 661-664
    - rsync, 658
  - 复制, 332
  - 存档, 326, 335
  - 搜索, 336
  - 搜索内容, 337
  - 查找, 390
  - 查看, 325, 336
  - 比较, 337
  - 移动, 332
  - 解压缩, 328
  - 路径, 322
- 文件服务器, 152
- 文件系统, 429-438
  - ACL, 273-283
  - cryptofs, 779
  - Ext2, 431-432
  - Ext3, 432-433
  - LFS, 436
  - OCFS2, 261-272, 434-435
  - ReiserFS, 430-431
  - XFS, 433-434
  - 修复, 850
  - 加密, 779
  - 支持的, 435-436
  - 更改, 142
  - 术语, 429
  - 选择, 430
  - 限制, 436
- 文档 (见 帮助)
- 日志文件, 162, 389
  - boot.msg, 165, 462
  - Squid, 707, 710, 715
  - 消息, 165, 565, 745
- 时区, 147
- 更新
  - passwd 和 group, 190
  - YaST, 190
  - 增补程序 CD, 130
  - 混音器, 208
  - 联机, 127-129
    - 命令行, 180
  - 问题, 190
- 替换安全性
  - 入侵检测, 209
- 服务位置协议 (见 SLP)
- 本地 APIC
  - 禁用, 20
- 本地化, 395
- 权限
  - 文件权限, 390
  - 更改, 333
- 查找, 390
- 核心文件, 391
- 注册
  - YaST, 126
- 清除, 341
- 游戏杆
  - 配置, 135
- 源
  - 编译, 292
- 用 vi
  - 加密文件, 783
- 用户
  - /etc/passwd, 453, 618
  - 管理, 155
- 电子邮件

- 配置, 148
- 电源管理, 459-477
  - ACPI, 459, 462-468, 473
  - APM, 461-462, 473
  - cpufrequency, 470
  - cpuspeed, 470
  - powersave, 470
  - YaST, 478
  - 休眠, 460
  - 待机, 460
  - 暂挂, 460
  - 电池监视, 460
  - 电量水平, 474

## 目录

- 创建, 333
- 删除, 333
- 更改, 333
- 结构, 320
- 路径, 322

## 硬件

- DASD, 134
- ISDN, 518
- ZFCP, 135
- 信息, 133, 822
- 图形卡, 172
- 监视器, 172
- 硬盘控制器, 133

## 硬盘

- DMA, 133

## 磁盘

- 引导, 383

## 端口

- 53, 567
- 扫描, 715

## 系统

- 关闭, 341
- 安全性, 161
- 应急, 848
- 更新, 130
- 服务, 152

- 本地化, 395
- 语言, 147
- 配置, 117-166
- 重引导, 341
- 限制资源使用, 391

## 组

- 管理, 161

## 编码

- ISO-8859-1, 396

## 编辑器

- Emacs, 393-394
- vi, 342

## 网关

- YaST
  - 网关, 513

## 网卡

- 网络, 509

## 网络, 495

- DHCP, 150, 577
- DNS, 508
- SLP, 545
- TCP/IP, 495
- YaST, 509

- IP 地址, 511
- 主机名, 512
- 别名, 511
- 启动, 514

- 基本网络地址, 499

- 广播地址, 500

- 本地主机, 500

- 网络掩码, 498

- 虚拟 LAN, 525

- 路由选择, 153, 498

- 身份验证

- Kerberos, 753-759

- 配置, 148-154, 509-523, 528-542

- IPv6, 507

- 配置文件, 530-537

- 网络信息服务 (见 NIS)

- 网络文件系统 (见 NFS)

美式键盘布局, 825

脚本

- init.d, 358, 361-364, 541

  - boot.local, 363

  - boot.Setup, 363

  - halt, 363

  - network, 541

  - nfsserver, 542

  - Portmap, 542

  - postfix, 542

  - rc, 361, 363

  - squid, 707

  - Xinetd, 541

  - ypbind, 542

  - ypserv, 542

  - 引导, 362

- mkinitrd, 356

- modify\_Resolverconf, 392, 532

- SUSEconfig, 366-368

  - 禁用, 368

记录

- 登录尝试, 162

许可权限, 328

- 文件, 328

- 文件系统, 328

- 更改, 330

- 查看, 330

- 目录, 329

许可证协议, 26

访问权限 (见 许可权限)

语言, 131, 147

调制解调器

- YaST, 516

- 电缆, 521

路径, 322

- 相对, 322

- 绝对, 322

路由

- 静态, 531

路由选择, 153, 498, 531-532

伪装, 739

网络掩码, 498

路由, 531

身份验证

- Kerberos, 203

- PAM, 451-457

软 RAID (见 RAID)

软件

- 删除, 119-125

- 安装, 119-125

- 编译, 292

轻量级目录访问协议 (见 LDAP)

运行级别, 146, 359-361

- 在 YaST 中编辑, 365

- 更改, 360-361

进程, 339

- 停止, 340

- 概要, 339

通配符, 336

逻辑卷管理器 (见 LVM)

邮件服务器

- 配置, 149

配置, 366

- DASD, 134

- DNS, 151, 555

- DSL, 148, 521

- GRUB, 370, 377

- IPv6, 507

- ISDN, 148, 518

- NFS, 151-152

- NTP, 152

- PAM, 209

- powertweak, 146

- Samba, 631-636

  - 客户机, 153-154, 637

  - 服务器, 153

- Squid, 708

- SSH, 747

- T-DSL, 523

- ZFCP, 135

- 图形卡, 172
- 声卡, 136
- 安全性, 154-163
- 打印, 402-406
  - 本地打印机, 402
  - 网络打印机, 405
- 无线卡, 148
- 时区, 147
- 用户, 155
- 电子邮件, 148
- 电源管理, 146
- 电缆调制解调器, 521
- 监视器, 172
- 硬件, 132-137
- 硬盘
  - DMA, 133
- 硬盘控制器, 133
- 系统服务, 152
- 组, 161
- 网卡, 148
- 网络, 148-154, 509
  - 手动, 528-542
- 语言, 147
- 调制解调器, 148, 516
- 路由选择, 153, 531
- 软件, 119-130
- 邮件服务器, 149
- 防火墙, 163
- 配置文件, 530
  - .bashrc, 388, 391
  - .emacs, 393
  - .profile, 388
  - .xsession, 751
- acpi, 463
- crontab, 388
- cs.cshrc, 396
- dhclient.conf, 586
- dhcp, 531
- dhcpd.conf, 586
- fstab, 144, 337
- group, 190
- grub.conf, 377
- host.conf, 533
- ifcfg-\*, 531
- inittab, 358-361, 394
- inputrc, 394
- krb5.conf, 766, 768, 774
- krb5.keytab, 772
- logrotate.conf, 389
- menu.lst, 371
- modprobe.d/sound, 137
- named.conf, 564, 566-574, 708
- nscd.conf, 536
- nsswitch.conf, 534, 618
- openldap, 775
- pam\_unix2.conf, 618, 773
- passwd, 190
- powersave, 462
- powersave.conf, 210
- resolv.conf, 392, 532, 564, 706
- samba, 632
- slapd.conf, 604, 777
- smb.conf, 633, 642
- smppd.conf, 542
- smpppd-c.conf, 543
- squid.conf, 707-708, 711, 713, 716, 718
- squidguard.conf, 718
- sshd\_config, 751, 774
- ssh\_config, 774
- suseconfig, 368
- sysconfig, 146, 366-368
- termcap, 394
- wireless, 531
- XF86Config, 206
- xorg.conf, 206, 439
  - Monitor, 444
  - 屏幕, 441
  - 设备, 443
- 主机, 151, 508, 533
- 主机名, 537

- 内核, 356
- 服务, 632, 714
- 权限, 804
- 网络, 531, 533
- 语言, 395-396
- 路由, 531
- 配置文件, 387, 391, 396
- 配置系统
  - 系统, 117-166
- 错误消息
  - 权限被拒绝, 144
  - 错误解释器, 144
- 键盘
  - X 键盘扩展, 394
  - XKB, 394
  - 亚洲字符, 395
  - 布局, 394
  - 映射, 394
    - multikey, 394
    - 组合, 394
  - 配置, 135
- 防火墙, 163, 737
  - Squid 和, 714
  - SuSEfirewall2, 737, 741
  - 包过滤器, 737, 740
- 附加产品, 125
- 音效
  - 混音器, 208
- 驱动器
  - 卸载, 338
  - 装入, 337
- 鼠标
  - 配置, 136

## A

- ACL, 273-283
  - 处理, 276
  - 定义, 275
  - 影响, 280

- 掩码, 279
- 支持, 283
- 权限, 273-283
- 检查算法, 282
- 结构, 276
- 许可权限位, 277
- 访问, 275, 278
- 默认值, 275, 280
- ACPI
  - 禁用, 20
- Apache, 151, 667-701
  - CGI 脚本, 690
  - Squid, 716
  - SSL, 692-697
    - 使用 SSL 配置 Apache, 696
    - 创建 SSL 证书, 693
  - 停止, 682
  - 启动, 682
  - 安全性, 698
  - 安装, 668
  - 快速入门, 667
  - 查错, 699
  - 模块, 683-690
    - 可用, 685
    - 外部, 688
    - 多处理, 687
    - 安装, 684
    - 构建, 689
  - 配置, 669
    - YaST, 676-682
    - 手动, 669-676
    - 文件, 669
    - 虚拟主机, 672
- AutoYaST, 164
  - 克隆系统, 41

## B

- Bash, 317-328
  - .bashrc, 388

- .profile, 388
- 功能, 324
- 命令, 318
- 管道, 326
- 通配符, 324
- 配置文件, 387

BIND, 564-574

BIOS

- 引导顺序, 824

bzip2, 327

## C

cat , 336

CD

- 引导自, 823

- 检查, 132, 821

cd , 333

chgrp , 331, 333

chmod, 330, 333

chown, 331, 333

CJK, 395

cp, 332

cpuspeed, 470

cron, 388

CVS, 658, 661-664

## D

date, 339

deltarpm, 288

df, 338

DHCP, 150, 577-590

- dhcpcd, 586-588

- 使用 YaST 配置, 578

- 包, 586

- 服务器, 586-588

- 静态地址指派, 588

diff, 337

DNS, 508

- BIND, 564-574

NIC, 508

Squid 和, 708

区域

- 文件, 570

反向查找, 573

名称服务器, 532

启动, 565

域, 532

安全性, 802

日志记录, 568

术语, 555

查错, 565

转发, 565

选项, 567

邮件交换程序, 508

配置, 151, 555

顶级域, 508

DOS

- 共享文件, 629

du, 338

## E

Emacs, 393-394

- .emacs, 393

- default.el, 393

## F

file , 336

find, 336

Firefox

- URL open 命令, 213

free, 339

## G

GNOME

- shell, 317

grep, 337

GRUB, 369-386

- device.map, 371, 376

- GRUB Geom 错误, 385
- grub.conf, 371, 377
- menu.lst, 371
- 主引导记录 (MBR), 369
- 分区名, 372
- 卸载, 383
- 命令, 370-378
- 引导, 370
- 引导密码, 377
- 引导扇区, 369
- 引导菜单, 371
- 故障诊断, 385
- 菜单编辑器, 375
- 设备名, 372
- 限制, 370
- gunzip, 328
- gzip, 327, 334

## H

- halt, 341

## I

- I18N, 395
- inetd, 152
- init, 358-359
  - inittab, 358
  - 添加脚本, 363
  - 脚本, 361-364
- IP 地址, 498
- IPv6, 500
  - 配置, 507
- 伪装, 739
- 动态指派, 577
- 私用, 500
- 类别, 498
- iSCSI, 245

## K

- KDE

- shell, 317
- Kerberos, 753-759
  - KDC, 762-765
    - nsswitch.conf, 762
    - 启动, 765
    - 管理, 770
  - keytab, 772
  - LDAP 和, 775-778
  - PAM 支持, 773-774
  - SSH 配置, 774
  - 主体, 754
    - 主机, 772
    - 创建, 765
  - 主密钥, 764
  - 会话密钥, 754
  - 安装, 761-778
  - 客户机
    - 配置, 766-768
  - 时钟同步, 763
  - 时钟扭斜, 768
  - 暂存文件, 764
  - 票证, 754, 756
  - 管理, 761-778
  - 认证器, 754
  - 身份凭证, 753
  - 配置
    - 客户机, 766-768
  - 领域, 761
  - 创建, 764

- kerberos
  - 票证授予服务, 756
- kill, 340
- killall, 340

## L

- L10N, 395
- LDAP, 599-628
  - ACL, 605
  - Kerberos 和, 775-778



- ldapadd, 609
- ldapdelete, 613
- ldapmodify, 611
- ldapsearch, 612
- YaST
  - 客户机, 617
  - 模块, 619
  - 修改数据, 611
  - 删除数据, 613
  - 搜索数据, 612
  - 服务器配置
    - YaST, 613
    - 手动, 604
  - 添加数据, 609
  - 目录树, 601
  - 管理用户, 624
  - 管理组, 624
  - 访问控制, 607
  - 配置
    - YaST, 613
- less, 325, 336
- LFS, 436
- Linux
  - 与其他操作系统共享文件, 629
  - 卸载, 383
  - 网络和, 495
- linuxrc
  - 手动安装, 208
- ln , 333
- locate, 336
- logrotate , 389
- LPAR 安装
  - IPL, 32
- ls, 319, 332
- LSB
  - 安装包, 285
- LVM
  - YaST, 103

## M

- MBR, 369
- mkdir, 333
- more, 325
- mount, 337
- mv, 332

## N

- NAT (见 伪装)
- NetBIOS, 630
- NetworkManager, 526
- NFS, 645
  - 客户机, 151, 646
  - 导入, 647
  - 导出, 653
  - 服务器, 152, 648
  - 装入, 647
- NIS, 591-597
  - 主, 591-597
  - 从属, 591-597
  - 客户机, 152
  - 客户程序, 597
  - 服务器, 152
- nslookup, 340
- NSS, 534
  - 数据库, 535
- NTP
  - 客户机, 152

## O

- OpenLDAP (见 LDAP)
- OpenSSH (见 SSH)
- OpenWBEM, 217-243
- OS/2
  - 共享文件, 629

## P

- PAM, 451-457
  - 配置, 209

- passwd, 341
- PCI 设备
  - 驱动程序, 145
- ping, 340, 539
- PostgreSQL
  - 更新, 190
- powersave, 470
  - 配置, 470
- ps, 339

## R

- RAID
  - YaST, 111
- reboot, 341
- RFC, 495
- rm, 333
- rmdir, 333
- RPM, 285-295
  - deltarpm, 288
  - rpmnew, 286
  - rpmorig, 286
  - rpmsave, 286
  - SRPMS, 293
  - 依赖性, 286
  - 卸装, 287
  - 增补程序, 287
  - 安全性, 804
  - 工具, 295
  - 数据库
    - 重构建, 287, 292
    - 更新, 286
    - 查询, 289
    - 校验, 285, 291
- rpmbuild, 285
- rsync, 658, 664
- rug, 180-183

## S

- Samba, 629-643

- CIFS, 629
- SMB, 629
- swat, 632
- TCP/IP, 629
- 停止, 631
- 共享, 630, 634
- 名称, 630
- 启动, 631
- 安全性, 636
- 安装, 631
- 客户机, 153-154, 630, 636-637
- 打印, 637
- 打印机, 630
- 服务器, 153-154, 630-636
- 登录, 637
- 许可权限, 636
- 配置, 631-636

### SaX2

- 分辨率和颜色深度, 173
- 双头, 174
- 图形卡, 173
- 图形输入板, 176
- 多头, 174
- 显示设备, 173
- 显示设置, 172
- 触摸屏, 176
- 键盘设置, 176
- 鼠标设置, 175

### SCPM, 146

- shell, 317-345
  - Bash, 317
  - 命令, 331-341
  - 管道, 326
  - 通配符, 324

### SLP, 545

- Konqueror, 546
- slptool, 546
- 提供服务, 547
- 注册服务, 547
- 浏览器, 546

SMB (见 Samba)  
smbd, 629  
spm, 292  
Squid, 703  
    ACL, 711  
    Apache, 716  
    cachemgr.cgi, 716-717  
    Calamaris, 719  
    CPU, 706  
    DNS, 708  
    RAM, 706  
    squidGuard, 717  
    停止, 707  
    功能, 703  
    卸载, 707  
    启动, 706  
    安全性, 704  
    对象状态, 705  
    报告, 719  
    日志文件, 707, 710, 715  
    权限, 707, 711  
    查错, 707  
    目录, 707  
    系统要求, 705  
    统计数字, 716-717  
    缓存, 703-704  
        大小, 705  
        已损坏, 707  
    访问控制, 716  
    透明代理, 713, 715  
    配置, 708  
    防火墙和, 714  
SSH, 747-752  
    scp, 748  
    sftp, 749  
    ssh, 748  
    ssh-agent, 751  
    ssh-keygen , 750  
    sshd, 749  
X, 751

守护程序, 749  
密钥对, 749-750  
身份验证机制, 750  
su, 341  
SUSE 手册, 815

## T

tar, 326, 335  
TCP/IP, 495  
    ICMP, 496  
    IGMP, 496  
    TCP, 495  
    UDP, 496  
    包, 497  
    层次模型, 496  
telnet, 341  
TLDP, 814  
top, 339  
Tripwire  
    替换为 AIDE, 209

## U

ulimit, 391  
    选项, 391  
umount, 338  
updatedb , 336

## V

VNC  
    管理, 153

## W

whois, 509  
Windows  
    共享文件, 629

## X

X

- SaX2, 440
- SSH , 751
- TrueType 字体, 445
- X11 核心字体, 446
- xft, 445
- Xft, 447
- xorg.conf, 440
- 分辨率和颜色深度, 173
- 双头, 174
- 图形卡, 173
- 图形输入板, 176
- 多头, 174
- 字体, 445
- 字体系统, 446
- 字符集, 445
- 安全性, 800
- 帮助 , 444
- 显示设备, 173
- 显示设置, 172
- 虚拟屏幕, 442
- 触摸屏, 176
- 配置, 439-444
- 键盘设置, 176
- 驱动程序, 443
- 鼠标设置, 175
- X Window 系统 (见 X)
- X 键盘扩展 (见 键盘, XKB)
- X.509 认证
  - 储存库, 726
  - 原理, 723
  - 撤消列表, 725
  - 证书, 724
- X.509 证书
  - YaST, 723
- X.Org, 439
- Xft, 447
- xinetd, 152
- XKB (见 键盘, XKB)
- xorg.conf
  - Depth, 442

- Display, 442
- InputDevice, 440
- Monitor, 442
- ServerFlags, 440
- 文件, 440
- 方式, 441-442
- 方式行, 441-442
- 模块, 440
- 监视器, 441
- 设备, 443
- 颜色深度, 442

## Y

### YaST

- AutoYaST, 164
- CA 管理, 163, 727
- CD 刻录程序, 164
- DASD, 134
- DHCP, 578
- DNS, 151
- DSL, 521
- EVMS, 139
- GRUB, 379
- ISDN, 518
- Kerberos 客户机, 151
- LDAP, 151
  - 客户机, 617
  - 服务器, 613
- LILO, 379
- LVM, 103, 139
- ncurses, 166
- NFS 客户机, 151
- NFS 服务器, 152
- NIS 客户程序, 597
- Novell AppArmor, 154
- Novell Customer Center, 126
- NTP 客户机, 152
- PCI 设备驱动程序, 145
- powertweak, 146

- RAID, 111
- root 密码, 34
- Samba
  - 客户机, 153-154, 637
  - 服务器, 153
- SCPM, 146
- sendmail, 148
- SLP, 153
- SLP 浏览器, 546
- sysconfig editor, 146
- sysconfig 编辑器, 366
- T-DSL, 523
- X.509 认证
  - 创建 CRL, 733
  - 子 CA, 729
  - 导入公共服务器证书, 735
  - 将 CA 对象作为文件导出, 735
  - 将 CA 对象导出到 LDAP, 734
  - 更改标准值, 732
  - 根 CA, 727
  - 证书, 730
- X.509 证书, 723
- ZFCP, 135
- 主机名, 35, 151
- 修复系统, 843
- 内存测试, 21
- 分区, 29, 139
- 发行说明, 164
- 启动, 18, 117
- 命令行, 169
- 图形卡, 172
- 声卡, 136
- 备份, 131, 138
- 媒体检查, 26, 132
- 安全性, 154-163
- 安全设置, 20
- 安装到目录中, 131
- 安装摘要, 27
- 安装方式, 26
- 安装服务器, 164
- 安装源, 126
- 安装设置, 27
- 安装, 用, 17-41
- 引导加载程序
  - 位置, 380
  - 密码, 382
  - 类型, 379
- 引导配置, 378
  - 安全性, 382
  - 超时, 382
  - 默认系统, 381
- 打印机配置, 402-406
  - 本地打印机, 402
  - 网络打印机, 405
- 控制中心, 118
- 支持查询, 164, 819
- 救援系统, 21
- 文本方式, 166-169
- 时区, 27, 147
- 更新, 130, 190
- 服务器证书, 163
- 检测信号, 139
- 注册, 126
- 游戏杆, 135
- 用户管理, 155
- 电子邮件, 148
- 电源管理, 146, 478
- 电缆调制解调器, 521
- 监视器, 172
- 硬件, 132-137
  - 信息, 133, 822
- 硬盘控制器, 133
- 系统启动, 18
- 系统安全性, 161
- 组管理, 161
- 网卡, 509
- 网络配置, 35, 148-154
- 群集, 139
- 联机更新, 127-129
- 自动安装, 164

- 配置文件, 164
- 自动登录, 157
- 虚拟化, 163
  - hypervisor, 163
  - 安装, 163
- 语言, 23, 118, 131, 147
- 调制解调器, 516
- 路由选择, 153
- 软件, 119-130
- 软件更新, 37
- 运行级别, 365
- 邮件服务器, 149
- 配置, 117-166
- 配置文件管理器, 146
- 键盘, 135
- 防火墙, 163
- 附加产品, 27, 125-126
- 驱动程序 CD, 166
- 高可用性, 139

## Yast

- DMA, 133
- 媒体检查, 821

YP (见 NIS)

## Z

z/VM 安装

- IPL, 32

ZENworks

- zmd, 179

zmd, 179