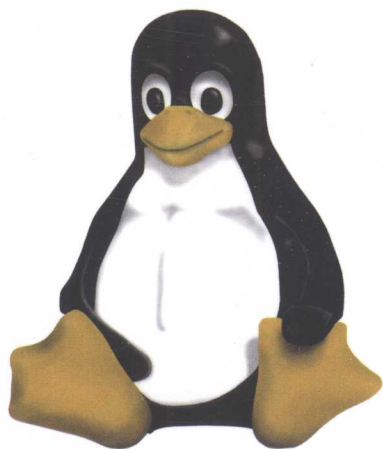


一线Linux系统运维高手根据CentOS 7编写，CentOS运维新手必读  
兼具原理与操作，分享经验与技巧，一本书轻松搞定CentOS系统运维



# CentOS Linux

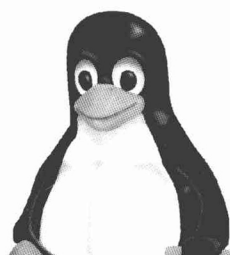
---

## 系统运维

清华大学出版社



陈祥琳 编著



# CentOS Linux

## 系统运维

陈祥琳 编著

清华大学出版社  
北京

## 内 容 简 介

《CentOS Linux 系统运维》是一本关于 Linux 系统运维的入门书籍。本书以 CentOS Linux 作为基础环境并按照从系统安装配置到系统投入使用的整个过程来讲解系统的日常维护。本书以内网为操作系统运行环境，并按照“系统安装→系统安全配置→应用部署→日常维护”的流程来编写。在系统的安装配置上主要涉及系统环境搭建、系统安全配置和日常维护，在应用上主要涉及服务的安装、配置以及日常维护。本书的内容适用基于 Red Hat 内核 2.6.32 版本的 Linux 系统，包括 CentOS Linux、Red Hat Enterprise Linux、Oracle Enterprise Linux。

本书适合 Linux 初学者、爱好者、程序员以及 Linux 服务器维护人员使用，也适合作为培训机构和大中专院校的教学用书。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。  
版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

### 图书在版编目（CIP）数据

CentOS Linux 系统运维/陈祥琳编著. —北京：清华大学出版社，2016  
ISBN 978-7-302-44872-3

I. ①C... II. ①陈... III. ①Linux 操作系统 IV. ①TP316.85

中国版本图书馆 CIP 数据核字（2016）第 201662 号

责任编辑：王金柱  
封面设计：王 翔  
责任校对：闫秀华  
责任印制：王静怡

出版发行：清华大学出版社

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

地 址：北京清华大学学研大厦 A 座 邮 编：100084

社 总 机：010-62770175 邮 购：010-62786544

投稿与读者服务：010-62776969，[c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质 量 反 馈：010-62772015，[zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

印 装 者：北京嘉实印刷有限公司

经 销：全国新华书店

开 本：190mm×260mm 印 张：24.5 字 数：628 千字

版 次：2016 年 9 月第 1 版 印 次：2016 年 9 月第 1 次印刷

印 数：1~3000

定 价：59.00 元

---

产品编号：066186-01

# 前言

自 Linux 诞生至今已吸引了不少的开发者和使用者，特别是开源技术的发展和云计算的应用更是让 Linux 得到更多用户亲睐。

本书以 CentOS Linux 系统为基础环境介绍系统的基本应用和管理，以理论知识结合实际应用的方式来编写，所涉及的内容主要包括系统的环境搭建、系统日常管理和服务的搭建。全书共 18 章，第 1~3 章主要是系统基础环境的搭建和基本应用，第 4~15 章主要是系统的基本配置，第 16~18 章主要是服务的配置应用。

第 1 章：关于操作系统的相关概念，主要涉及系统的版本（发行版本和内核版本）和系统运行的环境。

第 2 章：操作系统的安装配置，主要涉及系统安装时需要注意的事项和系统安装完成后更改系统的默认配置。

第 3 章：关于操作系统图形系统（桌面）类型及基本使用方法的介绍。

第 4 章：命令的应用，主要涉及 shell 的基本概念及各种常用命令的基本使用方法。

第 5 章：shell 脚本编程，主要包括循环脚本、算术和函数等。

第 6 章：系统的用户和用户组。

第 7 章：文件系统，主要涉及文件系统的基本组成、虚拟文件系统和文件系统块三方面的内容。

第 8 章：磁盘及磁盘分区，主要涉及磁盘分区的划分和日常的维护。

第 9 章：系统性能优化，主要涉及系统内存、CPU、进程和网络四方面的内容。

第 11 章：系统安全配置，主要涉及访问系统的控制策略、审计系统和日志系统配置应用三方面的内容。

第 12~13 章：系统网络的配置和应用。

第 14~15 章：系统启动初始化和系统的运行级别。

第 16~17 章：时间服务器的配置和应用。

第 18 章：基于 KVM 的虚拟化服务的配置和应用。

本书内容由浅入深，语言通俗易懂，旨在降低阅读难度、帮助读者快速入门。本书适用的读者对象包括但不限于：

- Linux 初学者
- Linux 爱好者
- Linux 服务器运维者
- 大中专院校和培训机构的教学用书

由于编辑水平有限，书中难免存在不足和疏漏之处，请广大读者批评指正。

编者  
2016年5月于海口

# 目 录

第 1 章 操作系统基本概念	1
1.1 系统版本的基本概念	2
1.2 系统内核基本组成	2
1.3 操作系统的运行环境	5
第 2 章 CentOS 安装配置	9
2.1 CentOS 基本概念	10
2.2 CentOS 安装	10
2.2.1 系统安装的主要事项	10
2.2.2 系统的量身定制	11
2.2.3 系统的安装过程	12
2.3 CentOS 基础环境配置	19
2.3.1 系统防火墙设置	19
2.3.2 系统 SELinux 设置	20
2.3.3 系统网络服务配置	21
2.3.4 本地 YUM 服务配置	23
第 3 章 CentOS 桌面系统	27
3.1 桌面系统的基本类型	28
3.2 桌面系统的基本应用	29
3.2.1 登录和退出系统	29
3.2.2 桌面背景图片设置	33
3.2.3 图形系统终端窗口设置	34

3.3	X-Window 图形系统	34
3.3.1	X-Window 图形系统简述	34
3.3.2	X-Window 运行原理	36
<b>第 4 章</b>	<b>命令基本应用</b>	<b>37</b>
4.1	shell 的基本概念	38
4.1.1	shell 的发展及类型	38
4.1.2	shell 的作用概述	39
4.1.3	shell 的工作原理	39
4.2	shell 的命令和符号	40
4.2.1	shell 的命令类型	41
4.2.2	shell 的通配符	42
4.2.3	shell 中的符号	44
4.3	常用命令的使用说明	45
4.3.1	文件管理命令	46
4.3.2	磁盘管理命令	51
4.3.3	压缩和解压缩命令	55
4.3.4	软件包管理命令	59
4.3.5	系统管理命令	62
4.3.6	其他常用命令	68
<b>第 5 章</b>	<b>shell 脚本编程</b>	<b>72</b>
5.1	shell 脚本的基本概念	73
5.1.1	shell 脚本编程的基础知识	73
5.1.2	shell 脚本中的变量	75
5.2	shell 脚本编程实例	79
5.2.1	脚本程序流程控制	79
5.2.2	算术运算实例	88
5.2.3	shell 函数的应用	93
5.2.4	shell 数组的应用	95

第 6 章 用户和用户组	98
6.1 系统的用户管理	99
6.1.1 系统的用户 ID 类型	99
6.1.2 CentOS 用户的分类	100
6.1.3 CentOS 用户账号管理	101
6.2 系统的用户组管理	105
6.2.1 用户组账号列表	105
6.2.2 用户组账号管理	107
6.3 用户环境配置管理	108
6.3.1 用户环境初始化文件	108
6.3.2 用户账户密码管理策略	110
第 7 章 文件系统结构	113
7.1 文件系统的组成	114
7.1.1 文件系统的基本概念	114
7.1.2 文件系统的基本组成	116
7.1.3 虚拟文件系统	118
7.2 文件系统的实际应用	121
7.2.1 文件系统的基本信息	121
7.2.2 文件系统的创建和删除	122
7.3 文件系统块维护	126
7.3.1 文件系统块设备管理	126
7.3.2 文件系统故障处理机制	127
第 8 章 数据存储空间	128
8.1 磁盘的分区结构	129
8.1.1 磁盘分区的基本概念	129
8.1.2 磁盘分区的信息获取	131
8.1.3 磁盘分区的划分	133
8.1.4 删除磁盘分区	138



8.2	逻辑卷管理的应用	140
8.2.1	逻辑卷管理基本概念	140
8.2.2	逻辑卷管理配置应用	143
8.3	磁盘空间管理	149
8.3.1	磁盘空间数据管理	149
8.3.2	磁盘空间维护	158
<b>第9章</b>	<b>系统性能监控</b>	<b>163</b>
9.1	性能优化的基本概念	164
9.2	磁盘资源配置管理	165
9.2.1	磁盘整体性能监控	165
9.2.2	磁盘空间限制	169
9.2.3	磁盘 IO 性能监测	172
9.3	系统内存管理	175
9.3.1	内存的基本概念	175
9.3.2	系统物理内存	176
9.3.3	系统虚拟内存	177
9.4	系统 CPU 管理	179
9.4.1	CPU 的基本概念	179
9.4.2	系统 CPU 监控	180
9.5	系统进程状态监控	184
9.5.1	进程的基本信息	184
9.5.2	进程创建和终止	186
9.5.3	进程优先级和后台进程	187
9.5.4	进程状态间的关系	188
9.6	系统网络性能评估	189
9.6.1	网络连通性测试	190
9.6.2	网络接口状态监控	191
9.6.3	系统网络配置参数	192

第 10 章 系统进程管理	196
10.1 进程的基本概念	197
10.2 进程的设置管理	199
10.2.1 进程状态基本操作	199
10.2.2 进程的优先级	202
第 11 章 系统安全加固	204
11.1 用户账户安全控制策略	205
11.1.1 用户身份鉴别	205
11.1.2 账号登录管理机制	207
11.2 系统防火墙配置管理	216
11.2.1 防火墙的基本概念	217
11.2.2 防火墙的 firewalld 应用	217
11.2.3 防火墙的 iptables 应用	224
11.3 系统安全审计功能	233
11.3.1 系统审计功能应用	233
11.3.2 用户空间审计系统	238
11.3.3 内核空间审计系统	245
11.4 系统日志应用管理	246
11.4.1 系统日志功能配置	247
11.4.2 系统日志功能应用	250
第 12 章 系统网络配置应用	255
12.1 网络协议概述	256
12.1.1 系统网络结构特点	256
12.1.2 系统网络协议模型	257
12.2 系统网络参数配置	259
12.2.1 网络相关配置文件	260
12.2.2 网卡设备配置参数	265
12.2.3 IP 地址应用配置	266

第 13 章 远程访问系统	269
13.1 OpenSSH 应用配置	270
13.1.1 OpenSSH 基本概念	270
13.1.2 OpenSSH 服务应用	270
13.1.3 OpenSSH 配置管理	272
13.2 Telnet 远程访问	276
13.2.1 Telnet 基本概念	276
13.2.2 Telnet 服务配置	277
13.2.3 Telnet 服务应用管理	278
13.3 VNC 远程访问	279
13.3.1 VNC 基本概念	280
13.3.2 VNC 服务配置管理	280
13.4 其他的远程访问方式	282
第 14 章 系统启动初始化	288
14.1 系统启动基本过程	289
14.1.1 BIOS 加电自检	289
14.1.2 grub2 引导程序	290
14.1.3 内核映像加载	291
14.1.4 INIT 进程初始化	291
14.2 系统运行时进程的通信	297
14.2.1 系统的守护进程	298
14.2.2 进程中的通信实现	301
14.3 关闭操作系统	306
第 15 章 系统运行级别	307
15.1 运行级别基本概念	308
15.1.1 系统的运行级别概述	308
15.1.2 系统运行级别间的切换	309
15.2 运行级别的应用	313

15.2.1	系统的单用户模式	313
15.2.2	系统的紧急模式	314
15.2.3	系统的救援模式	315
<b>第 16 章</b>	<b>资源共享服务配置</b>	<b>318</b>
16.1	文件传输协议	319
16.1.1	文件传输协议的工作原理	319
16.1.2	文件传输协议的基本模型	320
16.1.3	文件传输协议的服务配置	321
16.2	网络文件系统	323
16.2.1	网络文件系统概述	323
16.2.2	网络文件系统的搭建	325
16.3	Samba	328
16.3.1	Samba 服务的基本概念	328
16.3.2	Samba 的服务配置	330
<b>第 17 章</b>	<b>系统间的时间同步</b>	<b>334</b>
17.1	网络时间协议的基本概念	335
17.1.1	网络时间协议的模型结构	335
17.1.2	网络时间协议的工作方式	337
17.1.3	网络时间协议的工作原理	340
17.2	网络时间协议服务的搭建	341
17.2.1	时间服务组件管理	341
17.2.2	网络时间协议的配置文件	342
17.2.3	可靠时间源的获取	344
17.3	服务器间的时间同步	345
17.3.1	系统时间和时区设置	345
17.3.2	系统间的时间同步	348
17.3.3	网络时间协议安全配置	353

第 18 章 KVM 服务配置应用 .....	354
18.1 虚拟化技术概述 .....	355
18.1.1 虚拟化的结构原理 .....	355
18.1.2 虚拟化监视器的基本结构 .....	355
18.2 KVM 虚拟监视器配置 .....	358
18.2.1 KVM 虚拟化层次结构 .....	358
18.2.2 KVM 系统管理器配置 .....	358
18.3 KVM 的配置应用 .....	363
18.3.1 创建 KVM 操作系统 .....	363
18.3.2 KVM 的基本维护 .....	366
18.3.3 KVM 的操作系统克隆 .....	371
18.3.4 KVM 虚拟系统迁移 .....	373

# 第 1 章

## 操作系统基本概念

### 本章主要内容概述

---

操作系统（Operating System, OS）是管理和控制计算机硬件与软件资源的程序，是一种直接运行在“裸机”设备上最基本的系统软件，也是其他应用软件赖以运行的基础环境。

操作系统的种类比较繁多且功能的针对性也有所不同，因此用单一标准很难将它们进行统一分类。目前，对操作系统的常见分类方式有根据应用的领域、对用户数量的支持、源码的开放程度和对存储器寻址宽度的支持（也就是常说的 32 位、64 位）等。

### 本章内容导读

---

本章的主要内容是对 Linux 操作系统的基本概念和运行的环境进行介绍。Linux 是 1991 年首次发布的开源软件，任何人或机构只要遵循 GNU（GNU's Not UNIX，通用公共许可证）都可以自由地使用所有底层源代码，也可以自由地修改和再发布。

本章就 Linux 操作系统的基本概念（版本号、发布方式等）、内核的基本组成（内核源码目录、内核子系统模块等）以及运行的环境（硬件环境、网络环境等）进行介绍。

实际上 Linux 本身指的只是内核，但现在已经习惯将其视为一个操作系统。Linux 系统的原型最初是由芬兰的在校学生 Linus Torvalds（林纳斯·托瓦兹）从 Minix 上开发而来，但现在已经发展成为著名的开源、免费操作系统软件。

## 1.1 系统版本的基本概念

开放源代码的 Linux 操作系统在提供免费使用、自由传播的同时也遵循由电气和电子工业学会制定的 POSIX（Portable Operating System Interface of UNIX，可移植性操作系统接口）标准。在设计上，Linux 继承 UNIX，以网络为核心思想，且采用模块化的结构，使系统拥有高效性和灵活性。

由于 Linux 是从 UNIX 上发展起来的，因此 Linux 与 UNIX 的设计风格颇为相似，且能够在 PC 上实现多用户、多任务、多线程和多 CPU 的特性。Linux 也是一个性能稳定的多用户网络操作系统，主要运行在 Intel x86 系列 CPU 的计算机上，且支持 32 位和 64 位硬件，拥有较强的兼容性。除完整的操作系统之外，Linux 系统还包括文本编辑器、高级语言编译器 etc 等基于内核之外运行的应用软件和 X-Window 图形系统。

每个发行的内核都有一个版本号，且每个版本号都由主版本号、次版本号和修订次数号组成，其格式为“主版本号.次版本号.修订次数号”（最具有里程碑的内核版本号为 1.0.0）。每个版本号都透露该版本的类型（如 2.5.64 和 2.6.24），当次版本号为奇数时，说明此版本内核是一个测试版，为偶数时则为一个稳定版。修订次数号（如 64、24）说明该内核版本被修改的次数。

Linux 的发行套件是在发行版内核的基础上加入办公软件、编辑器等应用程序。相对来说，发行版是比较混乱的。发行版主要由一些公司及组织发布，这些公司或组织将 Linux 的内核与其他应用软件及文档包装起来并发到互联网上，以供下载。每个发行版本都有自己的特点，但发行版本号与内核版本号是独立的，所以发行版本号和内核版本号并不矛盾。

## 1.2 系统内核基本组成

Linux 内核是一个庞大而复杂的系统核心，由子系统以分层的形式组成。内核的主要用途是为了更好地与硬件进行交互。

### 1. 内核源代码目录结构

Linux 系统的内核中大多数程序之间几乎都有紧密的联系，它们之间的依赖和调用关系非常密切，所以在阅读一个源代码文件时往往还需要阅读其他相关的文件。内核源代码的项

层下有功能不同的子目录，分别组织存放各种内核子系统及文件。

Linux 系统内核源代码的目录以严格的层次构成一个有等级的文件系统。其中，这个文件系统的最高层是 Linux 目录。下面是 Linux-3.10.94 版本的内核相关信息及其下的文件。

```
.....
-rw-rw-r--.  1 root root  18736 Dec 10 02:43 README
-rw-rw-r--.  1 root root   7485 Dec 10 02:43 REPORTING-BUGS
drwxrwxr-x. 12 root root   4096 Dec 10 02:43 samples
drwxrwxr-x. 13 root root   4096 Dec 10 02:43 scripts
drwxrwxr-x.  9 root root   4096 Dec 10 02:43 security
drwxrwxr-x. 22 root root   4096 Dec 10 02:43 sound
drwxrwxr-x. 17 root root   4096 Dec 10 02:43 tools
drwxrwxr-x.  2 root root     97 Dec 10 02:43 usr
drwxrwxr-x.  3 root root    16 Dec 10 02:43 virt
```

各主要目录及功能描述如表 1-1 所示。

表 1-1 Linux 内核重要代码目录

目录名称	功能描述
arch/	所有与系统硬件体系相关的核心代码
block/	块设备核心程序代码
crypto/	加密函数库程序代码（常用加密、散列算法、压缩算法、校验算法）
drivers/	系统所有设备驱动程序代码
fs/	文件系统相关代码
ipc/	系统核心进程间的通信代码
init/	内核初始化代码
include/	存放内核头文件，主要供内核和用户使用
kernel/	内核核心部分（进程调度、中断处理、信号处理、模块）
lib/	通用内核函数
net/	网络通信协议代码
mm/	内存管理代码
samples/	内核例子
scripts/	配置核心的脚本文件代码
security/	系统安全相关代码
sound/	音频体系代码
usr/	用户的代码

## 2. 内核子系统模块组成

Linux 内核主要由 5 个子系统组成：进程调度、内存管理、文件系统、网络接口和进程通信。各个子系统之间相互协调完成系统资源的分配，并利用这些资源执行系统任务。这 5 个子系统之间的依赖关系如图 1-1 所示。



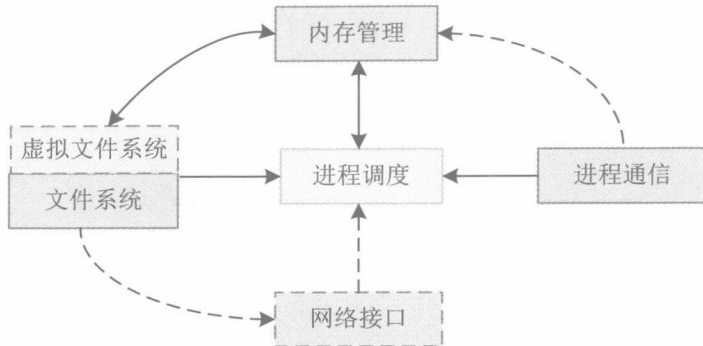


图 1-1 内核子模块及相互依赖关系

### (1) 进程调度子系统模块

进程调度控制进程对 CPU 资源的访问。Linux 采取基于优先级的调度算法选择进程，所采取的调度策略是各个进程能够公平合理地访问 CPU 资源，同时保证内核能即时操作硬件。

在需要执行一个进程时，由调度程序选择最值得运行的进程，然后为该进程分配相关的资源。实际上，调度程序所选择的进程是处于可运行状态且仅等待 CPU 资源。如果某个进程在等待的不是 CPU 资源，那么说明该进程是不可运行进程。

### (2) 内存管理子系统模块

内存管理用于确保所有进程能够安全地共享主内存区。Linux 内存管理支持虚拟内存，使得可用的内存空间比实际的还要大，这就意味着在计算机中运行的程序、代码、数据、堆栈的总量可以超过实际内存值的大小。

内存管理从逻辑上分为硬件无关部分和硬件有关部分。硬件无关部分提供了进程的映射和逻辑内存的对换；硬件相关的部分为内存管理硬件提供了虚拟接口。通常，在物理内存不足时，系统就会将当前使用的程序块保留在内存中执行，其余的都暂留在磁盘中（这部分的空间称为虚拟内存），并在需要时再交换回来。

### (3) 文件系统子系统模块

文件系统是用于对外部设备的驱动和储存，隐藏了各种硬件的具体细节，并为所有的设备提供了统一的接口。虚拟文件系统提供了多达数十种不同类型的逻辑文件系统和驱动程序。其中，逻辑文件系统是指 Linux 系统所支持的文件系统（如 ext3、ext4、fat 等）；设备驱动程序是指为每一种硬件控制器所编写的设备驱动程序模块。

### (4) 网络接口子系统模块

网络接口可分为网络协议和网络驱动程序，提供了对多种网络通信标准的访问并对各种网络硬件的支持。其中，网络协议部分负责实现每一种可能的网络传输协议；网络设备驱动程序则负责与硬件设备通信，每一种可能的硬件设备都有相应的设备驱动程序。