



Linux 专家之路



Linux

网络与安全管理

宁磊 周卫 编著 雨人科技 策划



附光盘
CD-ROM

人民邮电出版社
www.pptph.com.cn



Linux 专家之路



Linux

网络与安全管理

宁磊 周卫 编著 雨人科技 策划

人民邮电出版社

图书在版编目 (CIP) 数据

Linux 网络与安全管理/宁磊, 周卫编著. —北京: 人民邮电出版社, 2001.11

(Linux 专家之路)

ISBN 7-115-09789-5

I.L... II.①宁...②周... III. Linux 操作系统—安全技术 IV.TP316.89

中国版本图书馆 CIP 数据核字 (2001) 第 079743 号

内 容 提 要

本书通过大量的 Linux 程序实例, 系统地介绍了 Linux 系统的网络和安全。本书语言生动、结构严谨、通俗易懂, 能够使读者在最短的时间内完全掌握 Linux 系统管理技术的精髓。

全书共分 11 章, 第 1 章初步介绍网络安全的基本知识以及启动、关闭系统的方式; 第 2 至 4 章详细介绍 Linux 系统管理中的用户管理、进程管理和网络管理三个方面; 第 5 至 11 章主要介绍网络安全方面的具体内容, 包括网络的基础、数据包结构和防火墙设置等重要内容。

本书主要适合那些对 Linux 操作系统有所了解, 并希望深入学习有关网络管理方面技术的读者阅读, 也可作为技术开发人员的参考资料。

linux 专家之路

Linux 网络与安全管理

◆ 编 著 宁 磊 周 卫

策 划 雨人科技

责任编辑 张瑞喜

执行编辑 郭立罡

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@pptph.com.cn

网址 <http://www.pptph.com.cn>

读者热线 010-67129212 010-67129211(传真)

北京汉魂图文设计有限公司制作

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

◆ 开本: 787 × 1092 1/16

印张: 27

字数: 655 千字

2001 年 11 月第 1 版

印数: 1-5 000 册

2001 年 11 月北京第 1 次印刷

ISBN 7-115-09789-5/TP·2538

定价: 48.00 元(附光盘)

本书如有印装质量问题, 请与本社联系 电话: (010)67129223

前 言

Linux 是当今互联网络发展中较为出色的操作系统之一。我们可以借助 Linux 的共享源代码编写一套完全中文化的系统，这将告别汉化“别人的系统”的时代，实现一个中国人自己的操作系统。

在互联网上，许许多多的网络爱好者都对它投入了无比的热情，他们就如同对待婴儿一般地呵护它、保护它。使得 Linux 飞速发展成为可以与微软公司的 Windows 操作系统相比拼的系统。在当今微软一统天下的局势下，Linux 异军突起，举起了对抗微软垄断个人计算机操作系统的大旗。

自从 Linux 的诞生到现在，它始终是结合 Internet 的进步而成长的。可以说，Linux 离不开 Internet，也只有 Internet 的不断发展，Linux 才具有更强壮的生命力。

随着 Linux 进军服务器市场，对于它的系统安全要求也就越来越高。本书是根据作者多年使用 Linux 操作系统的经验，并结合设置网络服务器的防火墙开发实例而编写的。全书以开发实例为主线，在基于 Linux 操作系统平台和 ipchains 开发工具的基础上，详细描述了网络安全管理的具体过程。本书的第 1 章初步介绍了 Linux 操作系统的基础知识；第 2 章至第 4 章则主要介绍了超级用户的几种管理模式；第 5 章至第 11 章详细介绍网络安全方面理论和防火墙实例及调试防火墙等内容。本书配有光盘。光盘内容包括部分习题参考答案，本书的源代码压缩文件，雨人科技技术支持文档，相关软件：APACHE 服务器配置的所有相关文件、CVS 配置文件、邮件服务器配置文件等。

周卫负责全书的设计、统稿和修改，并编写了第 1、5、6、7、8、9、10、11 章；宁磊负责编写了第 2、3、4 章，并负责光盘内容的制作和例子测试。参加本书编写和指导工作的还有刘会双、赵中伟及刘馨宇等同志。在此对所有关心、支持和帮助过本书编写工作的同志表示诚挚的谢意！

书中不足之处敬请读者指正，以便再版时修订。

联系邮箱：yurennet@263.net

雨人科技网站：www.yurennet.com

编著者

2001 年 8 月

目 录

第 1 章 概述	1
1.1 开机引导和关机过程	2
1.1.1 配置 init	3
1.1.2 引导系统	11
1.1.3 关闭系统	12
1.1.4 管理 init 文件	13
1.2 UNIX 相关常识	16
1.2.1 理解文件/目录许可	16
1.2.2 链接的许可管理	20
1.2.3 创建多用户服务器的许可对策	22
1.2.4 使用文件和目录	24
1.2.5 使用 ext2 文件系统	26
1.3 小结与练习	27
1.3.1 小结	27
1.3.2 习题与思考	27
第 2 章 用户的管理	29
2.1 如何使用 Linuxconf	30
2.1.1 Linuxconf 简介	30
2.1.2 如何安装 Linuxconf	32
2.1.3 如何配置 Linuxconf	33
2.1.4 如何使用 Linuxconf	34
2.2 超级用户的权力	34
2.3 使用命令行工具管理用户	40
2.3.1 创建新的用户账号	40
2.3.2 创建一个新组	42
2.3.3 修改已经存在的用户账号	42
2.3.4 修改已经存在的组	46
2.3.5 删除用户账号	46
2.3.6 创建默认的用户设置	47
2.4 使用 Linuxconf 工具管理用户	50
2.4.1 创建一个新的用户账号	50

2.4.2	修改已经存在的用户账号	51
2.4.3	删除或禁止存在的用户账号	51
2.4.4	添加、修改及删除组	52
2.5	使用用户磁盘配额	54
2.5.1	安装磁盘配额软件	54
2.5.2	配置可以支持磁盘配额的系统	54
2.5.3	为用户分配磁盘配额	55
2.5.4	磁盘使用的监视	57
2.6	小结与练习	57
2.6.1	小结	57
2.6.2	习题与思考	57
第 3 章	进程的管理	59
3.1	进程的开始	60
3.2	控制和监视进程	61
3.2.1	用 ps 获得进程状态	61
3.2.2	给运行的进程传送信号	64
3.2.3	控制进程的优先级	68
3.3	监视系统加载的进程	69
3.3.1	使用 top 工具	69
3.3.2	使用 vmstat 工具	70
3.3.3	使用 uptime 工具	70
3.4	进程日志	71
3.4.1	配置 syslog	71
3.4.2	使用 tail 监视 log	72
3.5	规划进程	73
3.5.1	使用 at 工具	73
3.5.2	使用 cron 工具	74
3.6	小结与练习	75
3.6.1	小结	75
3.6.2	习题与思考	75
第 4 章	网络的管理	77
4.1	TCP/IP 网络地址	78
4.2	IP 网络分类	78
4.2.1	A 类网络	79
4.2.2	B 类网络	79
4.2.3	C 类网络	79

4.3 建立 Internet 服务	80
4.3.1 DNS 服务的建立	80
4.3.2 E-mail 服务的建立	102
4.3.3 Web 服务的建立	119
4.3.4 FTP 服务的建立	129
4.3.5 建立在线聊天系统服务	136
4.3.6 其他服务的建立	137
4.4 配置网络接口	140
4.4.1 使用传统的方法配置网络接口	140
4.4.2 使用 netcfg 配置网络接口	142
4.5 使用默认网关	145
4.6 网络的分割	146
4.6.1 网关计算机的配置	146
4.6.2 主机的配置	146
4.7 小结与练习	147
4.7.1 小结	147
4.7.2 习题与思考	147
第 5 章 网络安全的基本概念	149
5.1 TCP/IP 网络参考模型	150
5.1.1 TCP/IP 协议的发展	151
5.1.2 OSI 参考模型	152
5.1.3 TCP/IP 参考模型	154
5.2 服务端口	156
5.3 数据包	158
5.3.1 IP 消息类型 ICMP	158
5.3.2 IP 消息类型 UDP	159
5.3.3 IP 消息类型 TCP	159
5.4 小结与练习	161
5.4.1 小结	161
5.4.2 习题与思考	161
第 6 章 包过滤的概念	163
6.1 包过滤型防火墙	165
6.1.1 包过滤型防火墙结构	165
6.1.2 包过滤防火墙的优点	166
6.1.3 包过滤路由器的局限性	166
6.2 选择一个默认的包过滤策略	166

6.3 拒绝和禁止一个包.....	167
6.4 输入包的过滤.....	167
6.4.1 利用远程源地址过滤.....	167
6.4.2 利用本地目的地址过滤.....	169
6.4.3 利用远程源端口过滤.....	169
6.4.4 利用本地目的端口过滤.....	170
6.4.5 利用输入包的 TCP 连接状态过滤.....	170
6.4.6 对刺探和扫描的过滤.....	170
6.4.7 针对拒绝服务攻击的过滤.....	172
6.4.8 过滤输入数据包的多种考虑.....	174
6.5 输出包的过滤.....	175
6.5.1 利用本地源地址过滤.....	175
6.5.2 利用远程目的地址过滤.....	176
6.5.3 利用本地源端口过滤.....	176
6.5.4 利用远程目的端口过滤.....	176
6.5.5 利用 TCP 连接状态过滤.....	177
6.6 内部专用服务的过滤.....	177
6.6.1 保护不安全的本地服务.....	178
6.6.2 选择要运行的服务.....	178
6.7 小结与练习.....	183
6.7.1 小结.....	183
6.7.2 习题与思考.....	183
第 7 章 构建和安装防火墙.....	185
7.1 Linux 防火墙管理程序.....	186
7.1.1 防火墙脚本中所使用的 ipchains 选项.....	187
7.1.2 源和目的地址选项.....	189
7.2 初始化防火墙.....	190
7.2.1 防火墙例子中的符号常量.....	190
7.2.2 删除任何已存在的规则.....	191
7.2.3 定义默认策略.....	191
7.2.4 启用回环接口.....	192
7.2.5 源地址欺骗和其他的不合法地址.....	192
7.3 ICMP 状态消息过滤.....	200
7.3.1 错误状态控制消息.....	200
7.3.2 Ping Echo Request 和 Echo Reply 控制消息.....	202
7.4 保护分配在非特权端口上的服务.....	204
7.4.1 分配给非特权端口的常用本地 TCP 服务.....	205

7.4.2 分配给非特权端口的常用本地 UDP 服务	207
7.5 激活基本的 Internet 服务	208
7.5.1 激活 DNS 服务	208
7.5.2 激活 AUTH 服务	212
7.6 激活公用 TCP 服务	213
7.6.1 激活 Usenet 新闻服务	214
7.6.2 激活 telnet 服务	215
7.6.3 激活 SSH 服务	216
7.6.4 激活 whois 服务	218
7.6.5 激活 ftp 服务	219
7.6.6 激活 Web 服务	221
7.6.7 激活 E-mail 服务	224
7.6.8 激活 finger 服务	231
7.6.9 激活 gopher 服务	232
7.6.10 激活 WAIS 服务	232
7.7 激活公用 UDP 服务	233
7.7.1 激活 traceroute 服务	233
7.7.2 访问 ISP 的 DHCP 服务器	234
7.7.3 访问远程网络时间服务器	237
7.8 记录被禁止的输入数据包	238
7.9 禁止访问有问题的站点	241
7.10 激活 LAN 访问	241
7.10.1 激活 LAN 对防火墙内部网络接口的访问	242
7.10.2 激活 LAN 访问 Internet	242
7.11 安装防火墙	243
7.11.1 安装带有静态 IP 地址的防火墙	243
7.11.2 安装带有动态 IP 地址的防火墙	244
7.12 小结与练习	244
7.12.1 小结	244
7.12.2 习题与思考	245
第 8 章 多重网络防火墙	247
8.1 LAN 安全相关问题	248
8.2 小型网络的安全配置	249
8.2.1 LAN 访问堡垒防火墙	249
8.2.2 在多个 LAN 之间转发本地网络流	250
8.2.3 LAN 通过地址隐藏访问 Internet	251
8.3 大型内部网络的安全配置	252

8.3.1	利用子网创建多个网络	253
8.3.2	利用主机地址或端口范围限制内部访问	254
8.3.3	LAN 到 Internet 的地址隐藏	261
8.3.4	端口重定向	263
8.3.5	转发从 Internet 到 LAN 内部服务器的连接请求	265
8.4	隐藏子网防火墙	266
8.4.1	防火墙规则中的符号常量	266
8.4.2	清空隔断防火墙原有安全规则	268
8.4.3	定义隔断防火墙默认策略	268
8.4.4	激活隔断防火墙计算机的回环接口	269
8.4.5	源地址欺骗过滤	269
8.4.6	过滤 ICMP 控制状态信息	272
8.4.7	激活 DNS	276
8.4.8	过滤用户认证服务	281
8.4.9	E-mail 服务的过滤	283
8.4.10	访问 Usenet 新闻组服务	293
8.4.11	Telnet 服务	296
8.4.12	SSH 服务	299
8.4.13	FTP 服务	302
8.4.14	Web 服务	312
8.4.15	finger 服务	322
8.4.16	Whois 服务	325
8.4.17	gopher 服务	326
8.4.18	WAIS 服务	327
8.4.19	RealAudio 和 QuickTime 服务	328
8.4.20	IRC 服务	332
8.4.21	CU-SeeMe 服务	336
8.4.22	网络时间服务	340
8.4.23	远程系统日志	343
8.4.24	Choke 主机作为本地 DHCP 服务器	344
8.4.25	使局域网中主机访问 Choke 防火墙主机	345
8.4.26	激活 IP 地址隐藏功能	345
8.4.27	日志记录	346
8.5	小结与练习	346
8.5.1	小结	346
8.5.2	习题与思考	346
第 9 章	调试防火墙规则	347

9.1 常用防火墙开发技巧	348
9.2 查看防火墙规则	349
9.2.1 ipchains -L input	349
9.2.2 ipchains -L input -n	350
9.2.3 ipchains -L input -v	351
9.2.4 ipchains -L input -nv	352
9.3 检查输入、输出和转发规则	353
9.3.1 检查输入规则	353
9.3.2 检查输出规则	355
9.3.3 检查转发规则	356
9.4 对防火墙进行单数据测试	357
9.5 检查打开的端口	359
9.5.1 netstat 工具	359
9.5.2 strobe 工具	361
9.5.3 nmap 工具	361
9.6 调试防火墙	362
9.7 小结与练习	380
9.7.1 小结	380
9.7.2 习题与思考	381
第 10 章 检查系统运行情况	383
10.1 用 ifconfig 检查网络接口	384
10.2 使用 Ping 检查网络连接状况	385
10.3 用 netstat 检查网络	387
10.4 用 ps-ax 检查所有进程	388
10.5 系统日志	391
10.5.1 日志记录的对象	391
10.5.2 日志记录的位置	392
10.5.3 syslog 的配置	392
10.5.4 常被刺探的端口	393
10.5.5 常见端口扫描日志举例	395
10.5.6 自动日志分析软件包	395
10.6 小结与练习	396
10.6.1 小结	396
10.6.2 习题与思考	396
第 11 章 入侵检测和事件报告	397
11.1 系统完整性检查工具	398

11.1.1 COPS 工具	398
11.1.2 Crack 工具	399
11.1.3 ifstatus 工具	399
11.1.4 MD5	399
11.1.5 SATAN	399
11.1.6 tiger	400
11.1.7 tripwire	400
11.2 系统可能受损的迹象	401
11.2.1 与系统日志有关的迹象	401
11.2.2 与系统配置有关的迹象	401
11.2.3 与文件系统有关的迹象	402
11.2.4 与用户账号有关的迹象	402
11.2.5 与安全审计工具有关的迹象	403
11.2.6 与系统性能有关的迹象	403
11.3 系统受到安全侵害后应该采取的措施	403
11.4 事件报告	404
11.4.1 报告事件的目的	404
11.4.2 报告事件类型	404
11.4.3 报告事件的对象	405
11.4.4 要提供的信息	406
11.4.5 查找更多的信息	406
11.5 小结与练习	407
11.5.1 小结	407
11.5.2 习题与思考	407
附录 部分习题参考答案	409

第1章

概述

开机引导和关机过程

UNIX 相关常识

小结与练习



对于 Linux 操作系统的网络管理，最重要的工作就是确保它的安全性，本书正是为那些希望成为管理 Linux 系统、防范黑客入侵的优秀系统管理员而设计编写的。本章主要介绍 Linux 系统的一些基础知识，以及引导和关闭过程中会出现的问题。还包括对一些文件和目录许可的问题。

1.1 开机引导和关机过程

开启计算机并引导加载操作系统的过程称为开机引导。

启动过程中，计算机首先加载一小段 bootstrap loader 程序之后再启动操作系统。bootstrap loader 通常存储在硬盘或软盘的固定位置。由于操作系统庞大而复杂，而计算机加载的这段代码很小，这样就可以避免固件不必要的复杂化。

不同计算机的 bootstrap 是不同的。对于 PC 机，它的 BIOS 通过读取软盘或硬盘的第一个扇区来引导系统。而 bootstrap loader 正是包含在这个扇区中，它加载位于磁盘和其他地方的操作系统。

Linux 的核心被读入内存才是真正的启动，因为在核心被读入之后它要做以下的最基本的工作：

- 由于 Linux 的核心是压缩在固定位置的，它首先需要对自身解压缩。在核心的映像文件开头有一段解压缩程序可以进行解压缩的工作。
- 核心检查计算机系统安装的硬件，包括硬盘、软驱、网卡等，并为它们配置适当的驱动输出相关信息。
- 核心装载文件系统。文件系统的位置在编译时设置。如果读者没有为核心指定相关的文件系统驱动，那么文件系统的装载就会失败，启动停止。
- 核心在后台运行程序 init，这是一个进程号为 1 的进程。
- init 进程通过配置文件，切换系统运行等级，并启动 getty 提供虚拟控制台和串行线。getty 是提供用户通过虚拟控制台和串行线来登录 Linux 系统的一个程序。

这样，开机引导过程结束。

Linux 核心主要包括：进程管理、存储器管理、硬件设备驱动、文件系统驱动、网络管理和其他部分管理。其中最重要的是进程管理和存储器管理。进程管理可以产生进程并管理各种进程使之协调工作，从而实现 Linux 系统的多任务功能。存储管理则负责管理各个进程的存储区域和交换空间。

用户在第一次接触 Linux 系统时，并不一定很清楚开机引导过程的整个经过。在这个过程中，如果使用的是已经设置好的 X Window，并选择图形界面登录系统，便可看到如图 1.1 所示的窗口。

作为系统的管理员，有时候必须要了解在启动过程中，系统都做了什么事情。假使 Linux 开机后没有经过这个引导过程，一般都要求管理员清楚地知道系统什么位置出了问题，以及如何解决这样的问题。

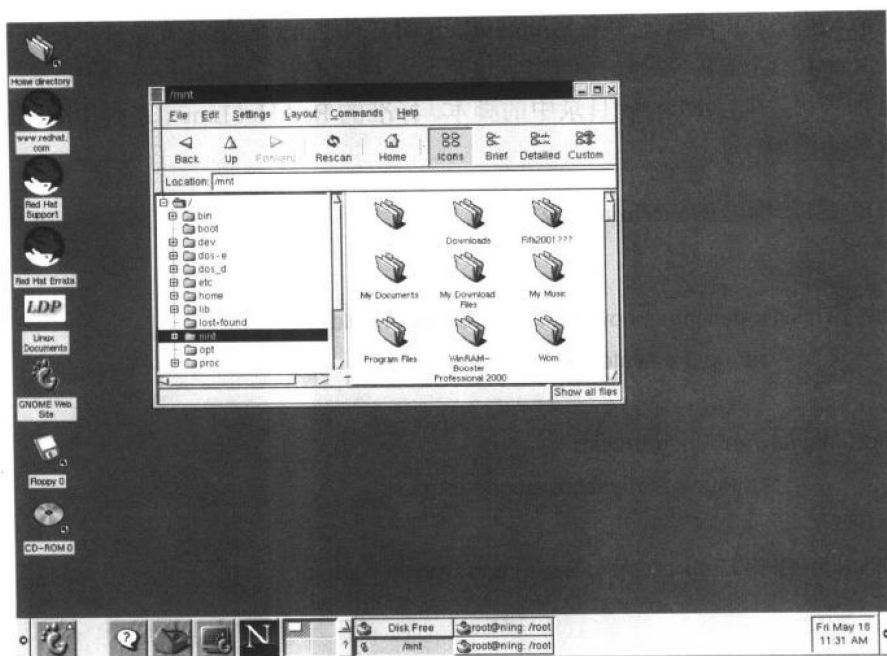


图 1.1 图形界面

★ 注意：在引导系统时，读者可以通过 **Shift+PageUp** 键，在控制台前查看系统引导信息。系统引导后，也可以运行 **dmesg** 程序查看引导信息。

Linux 系统可以在控制台上显示出启动过程中系统运行的所有命令，以及系统进行开机引导时执行任务的情况。这些信息可以使管理员很方便地了解自己的系统正在执行的命令。

作为开机引导过程的一部分，**init** 进程运行的程序是非常关键的。它决定了正在启动的系统将会提供什么服务，以及启动其他允许用户登录进行访问的进程。因此，读者可以定制自己的 **init**，选择系统的服务环境。下面将详细介绍 **init** 程序的配置。

1.1.1 配置 init

Linux 加载后，**init** 初始化硬件和设备驱动程序、然后运行 **init** 进程。UNIX (Linux) 系统中最重要服务都是由 **init** 提供的。它是 Linux 系统在核心引导时启动的第一个进程。

init 有两种风格：一种是 V 形式的 **init**；另一种就是 BSD 形式的 **init**。Red Hat 版本使用的是 UNIX 系统 V 形式的 **init**。

★ 注意：这两种形式的 **init** 之间的区别在于：V 形式的 **init** 需要使用运行等级，而 BSD 形式的 **init** 不使用运行等级。因为很少有人会使用 BSD 形式的 **init**。所以本书仅对 V 形式的 **init** 进行解释。

在程序启动时，init 读取一个名为/etc/inittab 的文件。init 的任务就是根据/etc/inittab 文件中的脚本（Script）创建系统启动后的服务进程。它通过分析/etc/inittab 中的脚本，按照需要或缺省的运行等级，执行/etc/rc.d 目录中的脚本。标准的 Red Hat Linux 系统中/etc/inittab 配置文件格式请参阅清单 1-1。

程序清单 1-1：标准的/etc/inittab 文件

```
#
# inittab This file describes how the INIT process should
#          set up the system in a certain run-level
#
# Author: Miquel van Smoorenburg,
#          <miquels@drinkel.nl.mugnet.org>
#
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
#
#      0 – halt (Do NOT set initdefault to this)
#      1 – Single-user, without NFS (The same as 3., if you do not have networking)
#      3 – Full multi-user mode
#      4 – unused
#      5 – X11
#      6 – reboot (Do NOT set initdefault to this)
#
id: 3:initdefault:
#
# System initialization
#
si: sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6
```



```
#
# Things to run in every runlevel
#
ud::once:/sbin/update
#
# Trap CTRL-ALT-DELETE
#
ca:: ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have
# a few minutes of power left. Schedule a shutdown for
# 2 minutes from now
#
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
#
pf:: powerfail:/sbin/shutdown -f -h +2 " power Failure; System Shutting Down "

#If power was restored before the shutdown kicked in, cancel it
pr: 12345:powerokwait:/sbin/shutdown -c " power Restored; Shutdown Cancelled "

# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x: 5:respawn:/usr/bin/X11/xdm -nodaemon
```



注意：开头带有符号“#”的行是注释行，而带有冒号分隔符的字段则都属于 init 配置行。