

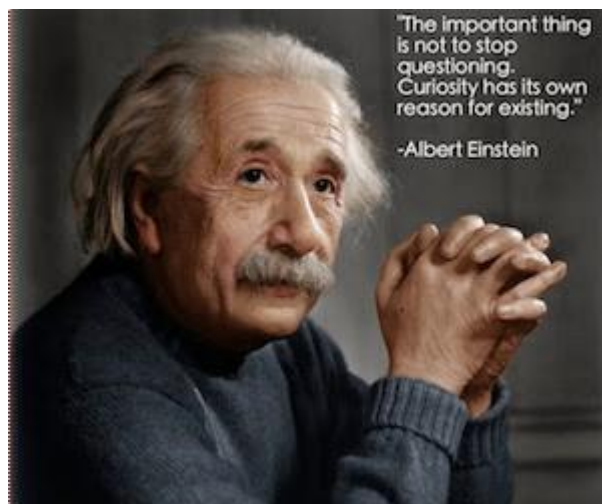
# Linux 内核进程管理

Version: 3.0

Author: 孙垒

Email:sunlei0625@163.com

Tel:18221493945



**摘要：**本文详细介绍了 Linux 内核进程管理的实现细节。本文基于 Linux kernel4.9.76 版本介绍。

版本	时间	基于内核	作者	主要修改
V1.0	2016 年 2 月	4.4.2	孙垒	
V2.0	2017 年 1 月 12	4.4.41	孙垒	
V3.0	2017 年 8 月 12	4.9.76	孙垒	

第 1 篇 基本数据结构 .....	错误！未定义书签。
第 1 章 基础知识 .....	错误！未定义书签。
1.1 字与字长.....	错误！未定义书签。
1.2 宏控制.....	错误！未定义书签。
1.2.1 宏__ASSEMBLY__ .....	错误！未定义书签。
1.2.2 宏__KERNEL__ .....	错误！未定义书签。
1.2.3 宏__linux__ .....	错误！未定义书签。
1.3 编译属性.....	错误！未定义书签。
1.4 位图.....	错误！未定义书签。
1.5 重要类型.....	错误！未定义书签。
1.5.1 dev_t 类型.....	错误！未定义书签。
1.5.2 fd_set 类型.....	错误！未定义书签。
1.5.3 umode_t 类型.....	错误！未定义书签。
1.5.4 off_t 类型.....	错误！未定义书签。
1.5.5 pid_t 类型.....	错误！未定义书签。
1.5.6 timer_t 类型.....	错误！未定义书签。
1.5.7 mqd_t 类型 .....	错误！未定义书签。
1.5.8 nlink_t 类型.....	错误！未定义书签。
1.5.9 ino_t 类型.....	错误！未定义书签。
1.6 数据对齐.....	错误！未定义书签。
1.7 字节序.....	错误！未定义书签。
1.8 内核空间与用户空间数据拷贝.....	错误！未定义书签。
1.9 小结.....	错误！未定义书签。
第 2 章 链表.....	错误！未定义书签。
2.1 介绍.....	错误！未定义书签。

2.2 双向链表.....	错误！未定义书签。
2.3 散列链表.....	错误！未定义书签。
2.4 特殊链表.....	错误！未定义书签。
2.5 散列.....	错误！未定义书签。
2.6 队列.....	错误！未定义书签。
2.7 IDR.....	错误！未定义书签。
2.8 小结.....	错误！未定义书签。
第 3 章 树.....	错误！未定义书签。
3.1 介绍.....	错误！未定义书签。
3.2 红黑树.....	错误！未定义书签。
3.3 基数树.....	错误！未定义书签。
3.4 树 B+.....	错误！未定义书签。
3.5 小结.....	错误！未定义书签。
第 4 章 位操作.....	错误！未定义书签。
4.1 引言.....	错误！未定义书签。
4.2 位相关宏描述.....	错误！未定义书签。
4.3 位操作函数.....	错误！未定义书签。
4.4 小结.....	错误！未定义书签。
第 5 章 进程数据结构 .....	错误！未定义书签。
5.1 介绍.....	错误！未定义书签。
5.2 进程描述符.....	错误！未定义书签。
5.3 相关函数.....	错误！未定义书签。
5.4 小结.....	错误！未定义书签。
第 6 章 init 进程 .....	错误！未定义书签。
6.1 介绍.....	错误！未定义书签。
6.2 基本定义.....	错误！未定义书签。
6.3 线程 thread.....	错误！未定义书签。
6.4 动态初始化.....	错误！未定义书签。
6.5 小结.....	错误！未定义书签。
第 2 篇 应用程序二进制接口 .....	错误！未定义书签。
第 7 章 ELF 格式 .....	错误！未定义书签。
7.1 介绍.....	错误！未定义书签。
7.2 目标文件格式.....	错误！未定义书签。
7.2.1 文件格式 .....	错误！未定义书签。
7.2.2 数据表示 .....	错误！未定义书签。
7.2.3 ELF 文件头.....	错误！未定义书签。

7.2.4 ELF 标识.....	错误！未定义书签。
7.2.5 ELF 数据编码.....	错误！未定义书签。
7.3 节 sections.....	错误！未定义书签。
7.3.1 节合并.....	错误！未定义书签。
7.3.2 特殊节.....	错误！未定义书签。
7.3.3 COMDAT 节.....	错误！未定义书签。
7.3.4 节组.....	错误！未定义书签。
7.3.5 注释节.....	错误！未定义书签。
7.4 重定位节.....	错误！未定义书签。
7.5 符号表节.....	错误！未定义书签。
7.6 小结.....	错误！未定义书签。
第 8 章 二进制文件装载 .....	错误！未定义书签。
8.1 介绍.....	错误！未定义书签。
8.2 程序段.....	错误！未定义书签。
8.2.1 段基地址.....	错误！未定义书签。
8.2.2 段权限.....	错误！未定义书签。
8.2.3 段内容.....	错误！未定义书签。
8.2.4 辅助信息.....	错误！未定义书签。
8.2.5 线程本地存储.....	错误！未定义书签。
8.3 程序加载(特定于处理器).....	错误！未定义书签。
8.4 小结.....	错误！未定义书签。
第 9 章 动态链接 .....	错误！未定义书签。
9.1 介绍.....	错误！未定义书签。
9.2 程序的解释.....	错误！未定义书签。
9.3 运行时动态链接.....	错误！未定义书签。
9.4 动态段.....	错误！未定义书签。
9.5 共享段依赖关系.....	错误！未定义书签。
9.6 可替换序列.....	错误！未定义书签。
9.7 全局偏移表.....	错误！未定义书签。
9.8 过程链接表.....	错误！未定义书签。

9.9 hash 表 .....	错误！未定义书签。
9.10 初始化和终止函数 .....	错误！未定义书签。
9.11 小结 .....	错误！未定义书签。
<b>第 10 章 内核加载 BIN 文件 .....</b>	<b>错误！未定义书签。</b>
10.1 引言 .....	错误！未定义书签。
10.2 数据格式 .....	错误！未定义书签。
10.3 基本函数 .....	错误！未定义书签。
10.3.1 目标文件加载类 .....	错误！未定义书签。
10.3.2 加载准备工作 .....	错误！未定义书签。
10.3.3 加载类搜索 .....	错误！未定义书签。
10.3.4 内存描述符 .....	错误！未定义书签。
10.3.5 参数页处理 .....	错误！未定义书签。
10.3.6 参数处理 .....	错误！未定义书签。
10.4 启动子进程 .....	错误！未定义书签。
10.5 小结 .....	错误！未定义书签。
<b>第 11 章 a.out 格式 .....</b>	<b>错误！未定义书签。</b>
11.1 背景 .....	错误！未定义书签。
11.2 文件格式 .....	错误！未定义书签。
11.3 加载类 .....	错误！未定义书签。
11.4 加载可执行代码 .....	错误！未定义书签。
11.5 加载共享库 .....	错误！未定义书签。
11.6 核心转储 .....	错误！未定义书签。
11.7 小结 .....	错误！未定义书签。
<b>第 12 章 elf 格式 .....</b>	<b>错误！未定义书签。</b>
12.1 介绍 .....	错误！未定义书签。
12.2 加载类 .....	错误！未定义书签。
12.3 ELF 加载 .....	错误！未定义书签。
12.4 共享库加载 .....	错误！未定义书签。
12.5 核心转储 .....	错误！未定义书签。
12.6 小结 .....	错误！未定义书签。
<b>第 13 章 script 格式 .....</b>	<b>错误！未定义书签。</b>
13.1 介绍 .....	错误！未定义书签。
13.2 加载类 .....	错误！未定义书签。
13.3 小结 .....	错误！未定义书签。

第 3 篇 内核进程资源管理 ..... 错误！未定义书签。

第 14 章 Linux 进程描述 ..... 错误！未定义书签。

- 14.1 进程与程序..... 错误！未定义书签。
- 14.2 进程状态..... 错误！未定义书签。
- 14.3 进程创建标志..... 错误！未定义书签。
- 14.4 进程与线程..... 错误！未定义书签。
- 14.5 进程组..... 错误！未定义书签。
- 14.6 会话进程..... 错误！未定义书签。
- 14.7 内存描述符..... 错误！未定义书签。
- 14.8 文件信息..... 错误！未定义书签。
- 14.9 信号..... 错误！未定义书签。
- 14.10 调试跟踪..... 错误！未定义书签。
- 14.11 vfork 支持..... 错误！未定义书签。
- 14.12 命名空间..... 错误！未定义书签。
- 14.13 信号量..... 错误！未定义书签。
- 14.14 TLS ..... 错误！未定义书签。
- 14.15 小结..... 错误！未定义书签。

第 15 章 进程与 SMP ..... 错误！未定义书签。

- 15.1 基本介绍..... 错误！未定义书签。
- 15.2 数据结构支持..... 错误！未定义书签。
- 15.3 SMP 实现..... 错误！未定义书签。
- 15.4 CPU up..... 错误！未定义书签。
- 15.5 CPU down..... 错误！未定义书签。
- 15.6 多核通信..... 错误！未定义书签。
- 15.7 PM 通知管理..... 错误！未定义书签。
- 15.8 SR 核心操作..... 错误！未定义书签。
- 15.9 总结..... 错误！未定义书签。

第 16 章 进程与信号 ..... 错误！未定义书签。

- 16.1 基本介绍..... 错误！未定义书签。
- 16.2 信号与进程..... 错误！未定义书签。
- 16.3 基本数据结构..... 错误！未定义书签。
  - 16.3.1 基本结构..... 错误！未定义书签。
  - 16.3.2 初始化..... 错误！未定义书签。
  - 16.3.3 基本函数介绍..... 错误！未定义书签。
- 16.4 进程对信号的处理..... 错误！未定义书签。
  - 16.4.1 进程创建和退出时信号处理..... 错误！未定义书签。

16. 4. 2 进程对接收信号的响应.....	错误！未定义书签。
16. 4. 3 信号的产生.....	错误！未定义书签。
16. 4. 4 信号的传递.....	错误！未定义书签。
16. 4. 5 信号的捕获及处理.....	错误！未定义书签。
16.5 信号相关系统调用.....	错误！未定义书签。
16.6 总结.....	错误！未定义书签。
第 17 章 进程与命名空间 .....	错误！未定义书签。
17.1 介绍.....	错误！未定义书签。
17.2 数据结构.....	错误！未定义书签。
17.3 IPC 空间 .....	错误！未定义书签。
17.4 MNT 空间.....	错误！未定义书签。
17.5 PID 空间 .....	错误！未定义书签。
17.6 NET 空间.....	错误！未定义书签。
17.7 小结.....	错误！未定义书签。
第 18 章 进程间通信 .....	错误！未定义书签。
18.1 介绍.....	错误！未定义书签。
18.2 管道.....	错误！未定义书签。
18. 2. 1 管道基本数据结构.....	错误！未定义书签。
18. 2. 2 管道内存管理.....	错误！未定义书签。
18. 2. 3 管道文件系统.....	错误！未定义书签。
18. 2. 4 管道系统调用.....	错误！未定义书签。
18. 2. 5 管道文件操作.....	错误！未定义书签。
18.3 FIFO.....	错误！未定义书签。
18.4 信号.....	错误！未定义书签。
18.5 消息队列.....	错误！未定义书签。
18. 5. 1 消息队列基本数据结构.....	错误！未定义书签。
18. 5. 2 基本数据结构内存分配.....	错误！未定义书签。
18. 5. 3 消息队列的初始化.....	错误！未定义书签。
18. 5. 4 消息队列处理流程.....	错误！未定义书签。

18.6 共享内存.....	错误！未定义书签。
18.6.1 基本介绍.....	错误！未定义书签。
18.6.2 基本数据结构.....	错误！未定义书签。
18.6.3 共享内存文件系统.....	错误！未定义书签。
18.6.4 文件操作.....	错误！未定义书签。
18.6.5 虚拟内存操作.....	错误！未定义书签。
18.6.6 共享内存初始化.....	错误！未定义书签。
18.6.7 处理流程.....	错误！未定义书签。
18.7 信号量.....	错误！未定义书签。
18.7.1 介绍.....	错误！未定义书签。
18.7.2 基本数据结构.....	错误！未定义书签。
18.7.3 初始化流程.....	错误！未定义书签。
18.7.4 信号量系统调用.....	错误！未定义书签。
18.8 套接口.....	错误！未定义书签。
18.8.1 匿名套接字.....	错误！未定义书签。
18.8.2 命名套接字.....	错误！未定义书签。
18.9 小结.....	错误！未定义书签。
第 19 章 进程退出 .....	错误！未定义书签。
19.1 介绍.....	错误！未定义书签。
19.2 处理过程.....	错误！未定义书签。
19.2.1 信号 .....	错误！未定义书签。
19.2.2 系统信息统计 .....	错误！未定义书签。
19.2.3 内存处理 .....	错误！未定义书签。
19.2.4 文件处理 .....	错误！未定义书签。
19.2.5 命名空间 .....	错误！未定义书签。



19.2.6 线程退出通知 .....	错误！未定义书签。
19.2.7 资源组分离 .....	错误！未定义书签。
19.2.8 父子通知 .....	错误！未定义书签。
19.3 僵尸进程.....	错误！未定义书签。
19.4 父进程处理.....	错误！未定义书签。
19.5 总结.....	错误！未定义书签。
第 20 章 进程优先级 .....	错误！未定义书签。
20.1 简介.....	错误！未定义书签。
20.2 优先级表示.....	错误！未定义书签。
20.3 优先级计算.....	错误！未定义书签。
20.4 负荷权重计算.....	错误！未定义书签。
20.5 小结.....	错误！未定义书签。
第 21 章 进程创建过程 .....	错误！未定义书签。
21.1 背景.....	错误！未定义书签。
21.2 核心处理函数.....	错误！未定义书签。
21.2.1 security_task_create() .....	错误！未定义书签。
21.2.2 dup_task_struct() .....	错误！未定义书签。
21.2.3 ftrace_graph_init_task() ....	错误！未定义书签。
21.2.4 get_seccomp_filter() .....	错误！未定义书签。
21.2.5 rt_mutex_init_task() .....	错误！未定义书签。
21.2.6 copy_creds() .....	错误！未定义书签。
21.2.7 try_module_get() .....	错误！未定义书签。
21.2.8 delayacct_tsk_init() .....	错误！未定义书签。
21.2.9 copy_flags() .....	错误！未定义书签。
21.2.10 rcu_copy_process() .....	错误！未定义书签。
21.2.11 init_sigpending() .....	错误！未定义书签。
21.2.12 task_io_accounting_init() ..	错误！未定义书签。

21.2.13 acct\_clear\_integrals() ..... 错误！未定义书签。

21.2.14 posix\_cpu\_timers\_init() .... 错误！未定义书签。

21.2.15 do\_posix\_clock\_monotonic\_gettime() 错误！未定义书签。

21.2.17 cgroup\_fork() ..... 错误！未定义书签。

21.2.18 sched\_fork() ..... 错误！未定义书签。

21.2.19 perf\_event\_init\_task() ..... 错误！未定义书签。

21.2.21 copy\_semundo() ..... 错误！未定义书签。

21.2.22 copy\_files() ..... 错误！未定义书签。

21.2.23 copy\_fs() ..... 错误！未定义书签。

21.2.24 copy\_sighand() ..... 错误！未定义书签。

21.2.25 copy\_signal() ..... 错误！未定义书签。

21.2.26 copy\_mm() ..... 错误！未定义书签。

21.2.27 copy\_namespaces() ..... 错误！未定义书签。

21.2.28 copy\_io() ..... 错误！未定义书签。

21.2.29 copy\_thread() ..... 错误！未定义书签。

21.2.30 alloc\_pid() ..... 错误！未定义书签。

21.2.31 uprobe\_copy\_process() ..... 错误！未定义书签。

21.2.32 clear\_all\_latency\_tracing() 错误！未定义书签。

21.2.33 pid\_nr() ..... 错误！未定义书签。

21.2.34 recalc\_sigpending() ..... 错误！未定义书签。

21.2.35 proc\_fork\_connector() ..... 错误！未定义书签。

21.2.36 cgroup\_post\_fork() ..... 错误！未定义书签。

21.2.37	perf_event_fork()	错误！未定义书签。
21.3	程序加载过程	错误！未定义书签。
21.3.1	unshare_files()	错误！未定义书签。
21.3.2	prepare_bprm_creds()	错误！未定义书签。
21.3.3	check_unsafe_exec()	错误！未定义书签。
21.3.4	open_exec()	错误！未定义书签。
21.3.5	sched_exec()	错误！未定义书签。
21.3.6	bprm_mm_init()	错误！未定义书签。
21.3.7	prepare_binprm()	错误！未定义书签。
21.3.8	search_binary_handler()	错误！未定义书签。
21.3.9	acct_update_integrals()	错误！未定义书签。
21.3.10	free_bprm()	错误！未定义书签。
21.4	总结	错误！未定义书签。
第 22 章	线程管理	错误！未定义书签。
22.1	介绍	错误！未定义书签。
22.2	内核线程创建	错误！未定义书签。
22.3	主要的内核线程	错误！未定义书签。
22.4	用户空间线程	错误！未定义书签。
22.4.1	LinuxThreads	错误！未定义书签。
22.4.2	NPTL	错误！未定义书签。
22.4.3	Linux 发行版线程模型	错误！未定义书签。
22.5	小结	错误！未定义书签。
第 23 章	安全管理	错误！未定义书签。
23.1	介绍	错误！未定义书签。
23.2	基本数据结构	错误！未定义书签。
23.3	主要函数	错误！未定义书签。
23.4	安全处理	错误！未定义书签。
23.5	小结	错误！未定义书签。

第 24 章 用户.....	错误！未定义书签。
24.1 介绍.....	错误！未定义书签。
24.2 基本数据结构.....	错误！未定义书签。
24.3 基本函数.....	错误！未定义书签。
24.4 init 进程的 user.....	错误！未定义书签。
24.5 用户管理.....	错误！未定义书签。
24.6 总结.....	错误！未定义书签。