

礼逆袭cron运行原理

空谷幽兰ESPER 2016-05-08 | 63阅读 | 2转藏

☆ 转藏 全屏 朗读 分享



1. 前言

本文介绍的是由Paul Vixie开发的运行在SuSE Linux上的Cron。可以通过“man cron”进行确认。

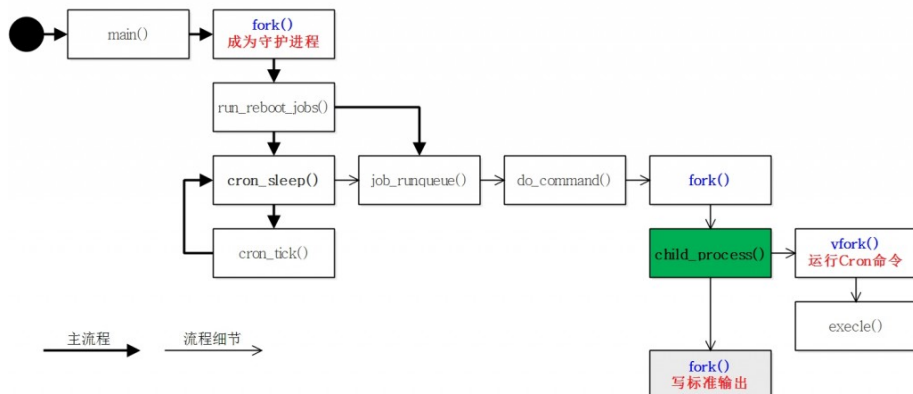
2. 示例

示例用来配合本文的说明

```
* /1 * * * * echo hello >> /tmp/hello.txt
```

3. 工作过程

Paul Vixie
版Cron工作流



Cron每分钟做一次检查，看看哪个命令可执行。

从上图可以看到，有4次fork，这4次fork分别是：

- 1) 第一个fork，让Cron自己成为Daemon进程，即成为守护进程；
- 2) 第二个fork，当Cron检查到有命令需要执行时被创建，但注意它并不执行命令，执行命令由它的子进程来做；
- 3) 第三个fork，有些版本调用的是vfork，但有些版本却是fork，它是负责执行Cron命令的进程，即会调用execl()的进程；
- 4) 第四个fork不是必须的，只有为Cron命令配置了标准输入才会用：

```
* /1 * * * * /tmp/X/x%1234567890
```

像上面有个百分符“%”，后面跟一串，则会有第四个fork，它的作用是将“%”后面的内容作为标准输入传递给第三个fork出来的进程。

注意fork出来的进程没有忽略(ignore)管道信号(SIGPIPE)，所以如果遇到SIGPIPE，则会导致进程无声无息的退出，比如标准输出重定向管道的读端被关闭了，写时就会触发SIGPIPE。

实践中，可能会遇到child_process()在做上述所说的第三个fork前因SIGPIPE信号退出，导致难以理解的问题。其中一个现象是：Cron命令被执行了若干次，但之后再也不执行了，原因



空谷幽兰ESPER



+ 关注

对话

TA的最新馆藏

- Centos下telnet的安装和配置
- Linux cron运行原理
- linux unset命令参数及用法详解
- 初识linux内核漏洞利用 | WooYun知识库
- Linux 之 rsyslog 系统日志转发
- Linux 下安装Python 以及pip包的安装...

喜欢该文的人也喜欢

更多

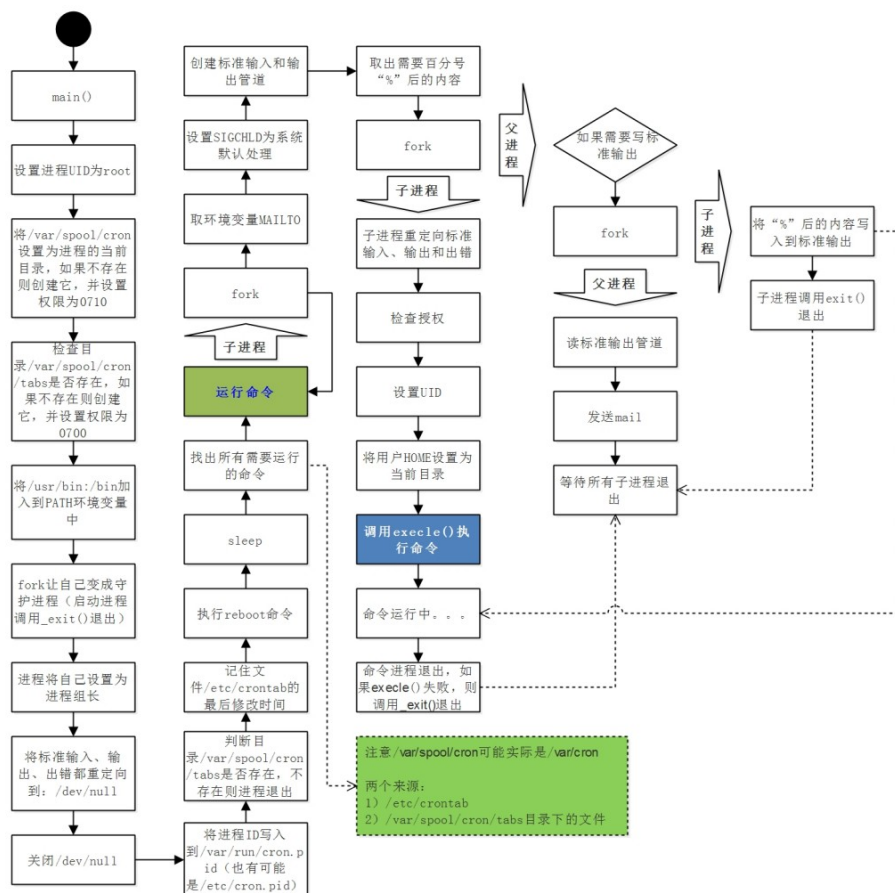
- 画山水先学画树，欣赏山水先看枯树 阅233
- 海底的鱼儿真美 (3) 阅13
- 中国人民解放军军衔牌和资历牌 阅11271
- 四大秘诀教你十年挣足一千万 阅70680
- 告别烦人的广告弹窗，教你永久关闭电脑网页弹窗广告 阅174

热门阅读

换一换

- 人教版八年级英语下册词汇表 阅44055
- 公司管理制度大全（完整版） 阅82163
- 行政事业单位内部控制报告（范文） 阅32642
- 《朱子治家格言》全文 阅112055
- 部编版语文七年级上册《春》优秀教案 教学设计一等奖 阅28357

在于第二个fork出来的进程因SIGPIPE退出了，导致没有进行第三个fork，因此Cron命令没有被调用(总是由execl()调用)。



4. 一个诡异的问题

你有可能遇到这样的情况，假设在cron中有如下一条配置：

```
*/* echo hello >> /tmp/hello.txt
```

观察到它正常运行几次后，就不再运行了，或者一次也不能，但确认无其它问题，因此十分诡异。

这个问题的原因，有可能是因为共享库Hook了cron，共享库代码触发了SIGPIPE，导致了第二个fork出的进程退出，没来得及执行vfork。

fork出来的子进程，没有对SIGPIPE进行任何处理，默认行为是悄悄退出进程。通过修改/etc/ld.so.preload，可以将共享库注入到非关联的进程中，可通过ldd观察到这种依赖，使用LD_PRELOAD也可以达到同样的效果。

5. cron&crontab

cron是一个在后台运行的守护进程，而crontab是一个设置cron的工具。cron调度的是/etc/crontab文件。

6. cron.allow&cron.deny

crontab使用的两个文件，cron不会用到它们。

7. cron.daily&cron.hourly&cron.weekly&cron.monthly

cron.daily、cron.hourly、cron.weekly和cron.monthly这四个目录均位于/etc下，但cron和crontab两个并不处理。它们是由配置在/etc/crontab中的run-crons处理，run-crons是位于目录/usr/lib/cron下的一个Shell脚本文件：

```
# cat /etc/crontab
```

```
SHELL=/bin/sh
```

```
PATH=/usr/bin:/usr/sbin:/sbin:/bin:/usr/lib/news/bin
```

```
MAILTO=root
```

```
#
```

```
# check scripts in cron.hourly, cron.daily, cron.weekly, and cron.monthly
```

```
#
```

```
*/15 * * * * root test -x /usr/lib/cron/run-crons && /usr/lib/cron/run-crons >/dev/null 2>&1
```

8. crontab编辑后cron异常

使用crontab编辑后，cron卡住不动(不是指进程卡住了，而是指命令没有被调用)，原因可能是因为“tcb table full”，最简单的办法是重启cron。

建议避免写下面这样的嵌套命令语句，它有可能导致cron不能正常工作：

```
*/1 * * * * echo "`date +%H:%M:%S` hello' >> /tmp/hello.txt
```

“echo”中嵌套了“date”，可以改成脚本调用，或者不嵌套命令，如：

```
*/1 * * * * echo 'hello' >> /tmp/hello.txt
```

一个现象是有一个cron子进程(如下述的14786)不退出了：

```
# ps -ef|grep cron
```

```
root 10325 1 0 15:08 ? 00:00:00 /usr/sbin/cron
```

```
root 14786 10325 0 15:13 ? 00:00:00 /usr/sbin/cron
```

gdb看到的调用栈为：

```
#0 0xffffe410 in __kernel_vsyscall ()
```

```
#1 0xb7e88a63 in __read_nocancel () from /lib/libc.so.6
```

```
#2 0xb7e38e38 in _IO_file_read_internal () from /lib/libc.so.6
```

```
#3 0xb7e3a0bb in _IO_new_file_underflow () from /lib/libc.so.6
```

```
#4 0xb7e3a7fb in _IO_default_uflow_internal () from /lib/libc.so.6
```

```
#5 0xb7e3bb2d in __uflow () from /lib/libc.so.6
```

```
#6 0xb7e35b7b in getc () from /lib/libc.so.6
```

```
#7 0x80005d73 in ?? () from /usr/sbin/cron
```

strace看到如下：

```
# strace -f -p 14786
```

```
Process 14786 attached
```

```
read(7,
```

借助lsof可以看到：

```
cron 14786 root 7r FIFO 0,6 117960708 pipe
```

为一个管道，read()挂住的原因可能是因为管道另一端所在进程调用_exit()退出而不是调用exit()退出。

这个时候只有人工kill这个挂起的cron子进程。



转藏



分享



献花 (0)

来自：空谷幽兰ESPER > 《文件夹1》

举报/认领

上一篇：linux unset命令参数及用法详解

下一篇：Centos下telnet的安装和配置

0条评论

写评论...

发表

请遵守用户 [评论公约](#)

类似文章

更多

AIX 里的crontab如何使用

AIX 里的crontab如何使用crontab 命令用途：提交、编辑、列出或删除 cron 作业。控制使用 crontab 命令 /var/adm/cron/cron.allow 和 /var/adm/cron/cron.deny 文件控制哪一个用户可以使用 crontab ...

SCOUNIX 基础讲座--第九讲：管理进程 - Unix爱好者家园

SCOUNIX 基础讲座--第九讲：管理进程 - Unix爱好者家园。用 crontab (C) 指令，从指定文件或标准输入拷贝或编辑成用户的 crontab 文件，该文规定了在指定日期和时间调度运行一些指令。/usr/lib/cr...

delete不是new分配的内存，如栈中内存

shell脚本放到crontab里不执行

shell脚本放到crontab里不执行 /bin/bash: /usr/local/sh/zengliang.sh: No such file or directory.X-Cron-Env: <USER=root>X-Cron-Env: <LOGNAME=root>X-Cron-Env: <ATH=/usr/bin/bi...

linux下so动态库一些不为人知的秘密（上）

为什么我不能在64位内核上mmap(MAP_FIXED)32位Linux进程中的最高虚拟页面？

strace ./a.out execve("./a.out", ["/a.out"], 0x7ffe08827c10 /* 65 vars */) = 0strace: [Process PID=1407 runs in 32 bit mode.]....mmap2(0xffffffff, 4096, PROT_READ|P...

/lib/tls/libc.so.6 出错

没有想什么，找了一个库strings /lib/libc-2.7.so |grep

GLIBCGLIBC_2.0GLIBC_2.1GLIBC_2.1.1GLIBC_2.1.2GLIBC_2.1.3GLIBC_2.2GLIBC_2.2.1GLIBC_2.2.2GLIE