### **1. cmdline - файл, который указывает на директорию процесса.**

Процесс - программа в стадии выполнения. До того момента как мы её запустили она была файлом. Файл принадлежит определённой файловой системе и находится в каком-то каталоге.

Этот доступный только для чтения файл содержит полную командную строку для

процесса, если только процесс не зомби. в последнем случае в этом файле ничего нет: то есть чтение этого файла вернет 0 символов. Команда- строковые аргументы появляются в этом файле как набор строк разделены нулевыми байтами ('\ 0'), с последующим нулевым байтом после последней строки.

### **2. cwd - символическая ссылка. Указывает на директорию процесса.**

Это символическая ссылка на текущий рабочий каталог.процесса. Чтобы узнать текущий рабочий каталог процесса 20, например, вы можете сделать это:

$ cd / proc / 20 / cwd; pwd -P В многопоточном процессе содержимое этого символического ссылка недоступна, если основной поток уже завершается (обычно путем вызова pthread\_exit (3)). Разрешение на разыменование или чтение (ссылка для чтения (2)) символическая ссылка регулируется режимом доступа ptrace. Проверка PTRACE\_MODE\_READ\_FSCREDS; см. ptrace (2).

### **3. envirom - файл, переводится как окружение.**

10 - Line Feed (Перевод строки). Указывает на движение механизма печати или курсора дисплея к началу следующей строки (на одну строку вниз).

Этот файл содержит исходную среду, которая была установлена когда текущая выполняемая программа была запущена через execve (2). Записи разделяются нулевыми байтами ('\ 0'), и в конце может быть нулевой байт. Таким образом, чтобы распечатайте среду процесса 1, вы бы сделали: $ cat / proc / 1 / окружающая среда | tr '\ 000' '\ n'Если после execve (2) процесс изменяет свой окружение (например, вызывая такие функции, как putenv (3) или изменяя переменную окружения (7) напрямую), этот файл не будет отражать эти изменения.

Кроме того, процесс может изменить место в памяти, которое этот файл обращается через операции prctl (2), такие как PR\_SET\_MM\_ENV\_START.

Разрешение на доступ к этому файлу регулируется ptrac режим доступа Проверка PTRACE\_MODE\_READ\_FSCREDS; см. ptrace (2).

* LS\_COLORS - используется для определения цветов, с которыми будут выведены имена файлов при вызове ls.
* LESSCLOSE, LESSOPEN – определяют пре- и пост- обработчики файла, который открывается при вызове less.
* XDG\_MENU\_PREFIX, XDG\_VTNR, XDG\_SESSION\_ID, XDG\_SESSION\_TYPE, XDG\_DATA\_DIRS, XDG\_SESSION\_DESKTOP, XDG\_CURRENT\_DESKTOP, XDG\_RUNTIME\_DIR, XDG\_CONFIG\_DIRS, DESKTOP\_SESSION – переменные, необходимые для вызова xdg-open, использующейся для открытия файла или URL в пользовательском приложении.
* LANG – язык и кодировка пользователя.
* DISPLAY – указывает приложениям, куда отобразить графический пользовательский интерфейс.
* GNOME\_SHELL\_SESSION\_MODE, GNOME\_TERMINAL\_SCREEN, GNOME\_DESKTOP\_SESSION\_ID, GNOME\_TERMINAL\_SERVICE, GJS\_DEBUG\_OUTPUT, GJS\_DEBUG\_TOPICS, GTK\_MODULES, GTK\_IM\_MODULE, VTE\_VERSION – переменные среды рабочего стола GNOME.
* COLORTERM – определяет поддержку 24-битного цвета.
* USER – имя пользователя, от чьего имени запущен процесс,
* USERNAME – имя пользователя, кто инициировал запуск процесса.
* SSH\_AUTH\_SOCK - путь к сокету, который агент использует для коммуникации с другими процессами.
* TEXTDOMAINDIR, TEXTDOMAIN – директория и имя объекта сообщения, получаемого при вызове gettext.
* PWD – путь к рабочей директории.
* HOME – путь к домашнему каталогу текущего пользователя.
* SSH\_AGENT\_PID - идентификатор процесса ssh-agent.
* TERM – тип запущенного терминала.
* SHELL – путь к предпочтительной оболочке командной строки.
* SHLVL – уровень текущей командной оболочки.
* LOGNAME – имя текущего пользователя.
* PATH - список каталогов, в которых система ищет исполняемые файлы.
* \_ - полная командная строка процесса
* OLDPWD - путь к предыдущему рабочему каталогу.

### **4. exe - символическая ссылка на файл процесса.**

Часто называют как образ процесса.

В Linux 2.2 и новее этот файл представляет собой символическую ссылку.

содержащий фактический путь к выполненной команде.

Эту символическую ссылку можно разыменовать обычным образом;

попытка открыть его откроет исполняемый файл. Вы можете

даже введите / proc / [pid] / exe, чтобы запустить еще одну копию того же

исполняемый файл, запущенный процессом [pid]. Если

путь был отключен, символическая ссылка будет содержать

строка '(deleted)', добавленная к исходному имени пути.

В многопоточном процессе содержимое этого символического

ссылка недоступна, если основной поток уже

завершается (обычно путем вызова pthread\_exit (3)).

Файловые дескрипторы, которые используются процессом.

### **5. fd - file directory - директория.**

//поддиректория содержит одну запись для каждого файла, который

//открыт процессом. Имя каждой такой записи соответствует номеру файлового

//дескриптора и является символьной ссылкой на реальный файл

### **6. maps - файл, который содержит список выделенных участков памяти, используемых процессом и права доступа**

Пример:

Содержание первой строки

00000000 - 00013000 r-xs 00000400 03:03 1264

1. 00000000 - начальный адрес выделенного участка памяти
2. 00013000 - конечный адрес выделенного участка памяти
3. r-xs - права доступа

r - можно читать, w - можно писать, x - можно выполнять, s - shared разделяемый, p - private(copy on write)

1. 00000400 - смещение от которого выполняется распределение. Получается что это всегда 400, видимо 400 это для какой-то служебной информации, но руководство об этом указывает.
2. 03:03 - старший и младший номер устройства. (

6)1264 - номер inode

В системе имя файла не является идентификатором. Идентификатором является inode, соответственно inode на самом деле это структура, но есть в системе так называемые метаданные, это номера inode которые мы с вами видели когда набирали ls -ail.

[stack] - Начальный процесс (также известный как основной

поток) стек.

[stack:<tid>] стек потока

[vdso] Виртуальный динамически связанный общий объект

[heap] The process's heap.

### **8) root - это символическая ссылка(softlink). Указывает на корень файловой системы которой принадлежит образ процесса.**

### **9) stat - файл**

Информация о состоянии процесса.

(1) pid% d Идентификатор процесса.

(2) comm %s Имя исполняемого файла в скобках.

(3) (3) state %c Один из следующих символов, обозначающих состояние процесса

R Running

S Sleeping in an interruptible wait

D Waiting in uninterruptible disk sleep

Z Zombie

T Stopped (on a signal) or (before Linux 2.6.33)

trace stopped

t Tracing stop (Linux 2.6.33 onward)

W Paging (only before Linux 2.6.0)

X Dead (from Linux 2.6.0 onward)

x Dead (Linux 2.6.33 to 3.13 only)

K Wakekill (Linux 2.6.33 to 3.13 only)

W Waking (Linux 2.6.33 to 3.13 only)

P Parked (Linux 3.9 to 3.13 only)

(4) ppid %d - PID родительского процесса.

(5) pgrp %d - Идентификатор группы процессов процесса.

(6) session %d - Идентификатор сессии процесса.

(7) tty\_nr %d - управляющий терминал процесса (младший номер устройства содержится в комбинации битов с 31 по 20 и с 7 по 0; главное устройства число находится в битах с 15 по 8.)

(8) tpgid %d - уникальный идентификатор группы управляющего терминала

(14) utime %lu - количество тиков которые получил процесс выполняясь в режиме пользователя.

(15) stime %lu - количество тиков которое процесс получил, выполняясь в режиме ядра.

(16) cutime %ld - количество тиков которое получил процесс ожидая дочерние процессы, запланированные в пользовательском режиме

(17) cstime %ld - количество тиков которое получил процесс ожидая дочерние процессы, запланированные в режиме ядра

(22) starttime %llu - время с начала загрузки системы

(23) vsize %lu - размер виртуальной памяти в байтах

(35) wchan %lu - “канал” в котором процесс ожидает. Это адрес места в ядре в котором процесс находится в состоянии сна.

### **10) statm - файл**

Предоставляет информацию об использовании памяти, измеряемой в страницах.

1. size общее число страниц выделенное процессу в виртуальной памяти.
2. resident размер резидента(страницы, загруженной в физическую память)
3. shared - количество общих рездентных страниц
4. text - текст(код)
5. lib библиотека
6. data - данные + стек
7. dt dirty pages