Gestione dei Processi

aka “sparare alle ginocchia degli intrusi”

Radu Andries

Politecnico Open unix Labs

27 Marzo 2013

Cosa è un processo?

È un'istanza di un programma in esecuzione. Il kernel linux conserva le seguenti informazioni (è solo un subset):

- pid
- argomenti
- priorità
- processo padre
- memoria volatile usata
- file descriptor aperti
- stato

Segnali

I segnali sono delle "indicazioni" asincrone ad un programma. Il programma può scegliere di ignorare tutto tranne SIGKILL.

- SIGSTOP - Ferma un Programma, lo "congela"
- SIGCONT - Fa continuare un programma dopo sigstop
- SIGINT - Invia un interrupt al programma (di solito ctrl-c con la tastiera)
- SIGHUP - Di solito viene usato per ricaricare la configurazione
- SIGUSR1/2 - Segnali "custom"
- SIGTERM - Invia un segnale di arresto "gentile"
- SIGKILL - scarica dalla memoria il programma (a forza di schiaffi in faccia). Usare con cautela

Com'è fatto un processo

Un processo è composto da tre segmenti:

1. Text/Code Segment (parti di eseguibile)
2. Data Segment (heap, stack)
3. System Data Segment

I thread - processi lightweight

- I thread in linux sono quasi come processi normali.
- Condividono la sezione dati e codice con il padre.

PID

Process IDentifier

- Sono numeri (unsigned short int) che partono da 0
- Se finiscono si inizia da capo
- PID importanti
  - pid 0 - kernel
  - pid 1 - init
- Tutti i processi tranne il pid 0 hanno un padre. (PPID - Parent PID)

Stato di un processo

Un processo si può trovare in molti stati:

- D - in attesa di IO
- R - in esecuzione
- S - in attesa del proprio quanto di tempo
- T - fermato dall'utente
- Z - zombie. Processo morto ma non ancora "sepolto" dal padre

Morte di un processo/thread

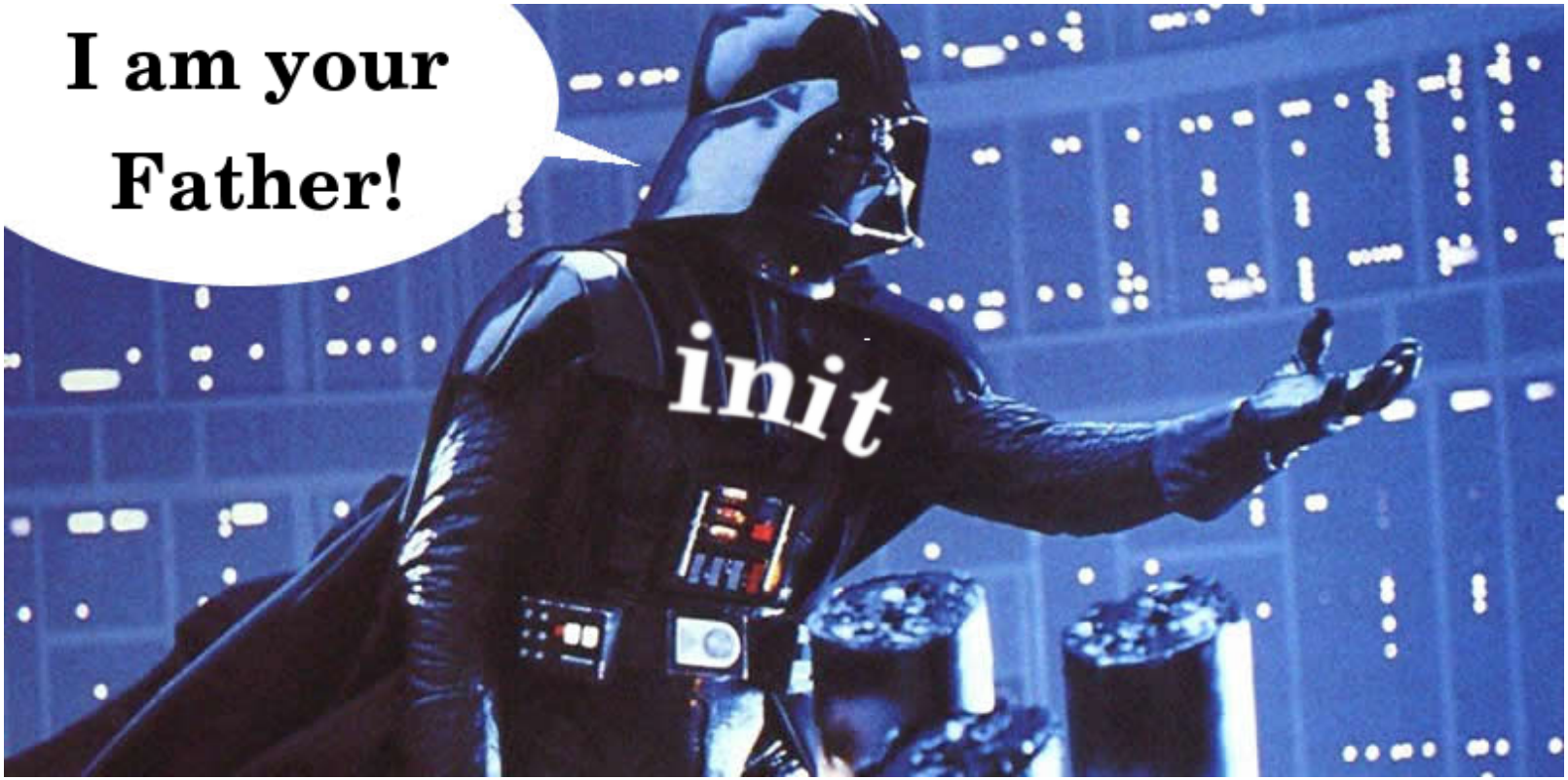
Thread

- Figlio - Il padre riceve il valore di ritorno
- Padre - I thread vengono interrotti senza preavviso

Processo

- Figlio - Il padre può aspettare con wait_pid il figlio. Può diventare zombie
- Padre - ...

Processi Figli



Priorità di un processo

La priorità di un processo va da -20 a 20. Si chiama niceness. Un processo con niceness alto è “gentile” e lascia altri processi più tempo per l’esecuzione.

/proc

È la directory dove ci sono informazioni sui processi correnti in Linux/Unix. Sono strutturate per PID, nella forma "/proc/pid". Ogni cartella ha informazioni sul processo che ha quel PID. Questa cartella è mantenuta dal kernel.

E ora passiamo alla pratica