Procesy a programy

- Základné pojmy
- Zoznam procesov
- Vyťaženie systému
- Správa procesov, signály
- Aktivita procesov
- Využívané zdroje a ich limity
- Správa služieb
- Auditné záznamy (logy)
- Správa programových balíkov, aktualizácie

Proces

- Bežiaca inštancia programu.
- Vytvorený volaním `fork()` (alebo `clone()`) ako kópia volajúceho procesu.
- Jedinečný identifikátor PID.
- Priradené UID and GID používateľa, ktorý proces spustil.
- Komunikuje prostredníctvom súborov (`stdin, stdout, stderr, ...`) a signálov.
- Spotrebúva systémové prostriedky (pamäť, cpu čas).
- Služba/server/démon – proces, bežiaci v pozadí (typicky).

Zoznam procesov (1)

- `ps` zobrazí informácie o bežiacich procesoch:
  - PID, PPID,
  - UID,
  - stav (R, T, D, S, I, Z),
  - využitie pamäte, využitie procesora,
  - názov príkazu, argumenty, ...
- Filtrovanie výstupu
  - napr. podľa používateľa
- Výstupný format, zoraďovanie.

Zoznam procesov (2)

- Všetky procesy v systéme:
  - `ps aux`
  - `ps –e; ps –ef`
- Procesy konkrétneho používateľa
  - `ps –Fu user`
- Zobrazenie vzťahov
  - `ps –eH; ps axjf; pstree`
  - `ps –feHu`
- Informácie o vláknach
  - `ps –eLf`

Vyhľadávanie procesov

- `ps aux | grep sshd`
- `pgrep` – vyhľadávanie podľa rôznych kritérií.
- Vypíše zoznam zodpovedajúcich PID.
  - `man pgrep`
  - `pgrep –l bash`
  - `pgrep –u root sendmail`
  - `pgrep –u root,user ssh`
- Search string is a regular expression
  - `pgrep ^ba`
  - `pgrep '\.sh$'`
  - `pgrep sh`

Vyťaženie systému (1)

- Celkový prehľad
  - `uptime`
    - aktuálny čas, čas od štartu (up time),
    - počet prihlásených používateľov,
    - priemerná záťaž (1, 5, 15 min),
- Periodické (interaktívne) sledovanie procesov
  - `top`
    - procesy, (vlákna), pamäť (swap),
    - usporiadanie podľa využitia CPU, pamäte, PID, procesorového času, ...
  - `htop` – farebná verzia.

Vyťaženie systému (2)

- `top`
  - f: voľba zobrazovaných parametrov
  - H: informácie o vláknach
  - u: filtrovanie podľa používateľa
  - M: zoradenie podľa spotrebovanej pamäte (%)
  - P: zoradenie podľa času CPU (%)
  - O: výber kritérií zoraďovania
  - k: kill – ukončenie / poslanie signálu
- Voľná pamäť
  - `free, vmstat`

Signály – ukončenie procesu

- Odoslanie signálu procesu so špecifikovaným PID
  - `man kill`
  - `kill 1234; kill -9 123 456; kill -SIGKILL 1234`
  - `kill -l`, vypíše zoznam signálov
- Odoslanie signálu procesom podľa názvu
  - `pkill`, ako pgrep (podporuje regulárne výrazy)
  - `killall` (zadaný názov musí zodpovedať)
  - `killall -TERM telnet`
- Signály na zrušenie procesu (prestane existovať)
  - `SIGTERM, SIGKILL`

Signály – zastavenie procesu

- Zastavený proces nie je plánovaný, teda sa nevykonáva ani nespotrebováva CPU čas (tiež nespracováva signály).
- Môže byť spustený od miesta, kde bol zastavený.
- Zastavenie a spustenie procesu:
  - `SIGSTOP, SIGCONT`
  - `kill –STOP 1234`
  - `pkill –STOP –u user bash`
  - `pkill –CONT –u user bash`

Signály – ostatné

- Reload konfiguračného súboru
  - `SIGHUP`
  - Niektoré démony reaguju na tento signál znovunačítaním konfiguračného súboru bez potreby ich zastavenia.
  - `killall –HUP sshd`
  - `pkill –HUP named`
- Zobrazenie I/O štatistík (príkaz `dd`)
  - `USR1`, pri prijatí tohto signálu dd vypíše štatistiky na *stderr*.
  - `killall –USR1 –u user dd`
  - Poznámka: pre štatistiky pri iných príkazoch, pozri `pv`

Sledovanie procesov – otvorené súbory

- `lsof`, vypíše zoznam všetkých otvorených súborov
  - `man lsof`
- Procesy s názvom začínajúcim na “ba”
  - `lsof -c ba, lsof -c /^ba/`
- Procesy, ktoré majú otvorené súbory z /tmp/ a jeho podadresárov
  - `lsof +D /tmp/`
- Zoznam otvorených súborov procesu s PID 1
  - `lsof -p 1`
- `fuser`, zoznam procesov, ktoré majú otvorený daný súbor
  - `man fuser`
  - `fuser /bin/*sh`
- By default vypisuje iba PID a spôsob využitia. Prepínače ‘`-u`’ a ‘`-v`’ na zobrazenie používateľa a príkazov
  - `fuser -u ~`
  - `fuser -v /tmp`

Sledovanie procesov – otvorené sieťové spojenia

- `netstat` zobrazí zoznam všetkých soketov v systéme
  - `man netstat`
- S prepínačom ‘-p’ vypíše aj názov príkazu a PID procesu, ktorý je na konci spojenia (iba root).
  - `netstat –nap`
- Zobrazenie počúvajúcich soketov.
  - `netstat –protocol=ip –nlp`
  - `netstat –tunlp`

Sledovanie procesov – systémové a knižničné volania

- Výpis systémových volaní, ktoré proces robí
  - `man strace`
  - `strace -p 123 -f -o output.txt`
- Sledovanie knižničných volaní
  - `man ltrace`
  - `ltrace -p 234 -s 255 -e read`
- Cudzie procesy môže monitorovať iba root.

Limity zdrojov procesov

- Limity pre systémové prostriedky procesu
  - `man ulimit` (interný príkaz shell-u)
  - `ulimit -a`, výpis aktuálnych nastavení
  - core súbor, dátový segment, virt. pamäť, počet súborov, veľkosť súboru, počet zámkov, CPU čas, počet procesov, ...
  - bežný používateľ môže iba znižovať,
  - nastavenia pre používateľov:
    - `/etc/security/limits.conf`
  - globálne nastavenia:
    - `/etc/rc.local`

Priorita plánovania procesov

- Prioritu plánovania procesu je možné zmeniť zmenou hodnoty `nice`:
  - rozsah: od +19 (najnižšia priorita) do -20 (najvyššia priorita).
- Spustenie procesu so zmenenou prioritou
  - `man nice`
  - `nice –n –10 csh`
- Zmena priority bežiaceho procesu
  - `man renice`
  - `renice 10 1234`
  - zvýšiť prioritu môže iba root.

Správa služieb (1)

- Niektoré procesy zabezpečujú úlohy potrebné pre správny beh systému, alebo zabezpečujú rôzne služby, napr.
  - `init, systemd, crond, rsyslogd, sendmail, sshd, …`
- Služby sú spustené a spravované prostredníctvom init systému (init démon).
- Historicky existuje viacero implementácií init systémov. Väčšina moderných distribúcií aktuálne používa **systemd**. Ďalší populárny systém je **init** (SysV init) a jeho varianty.
- **Init** používa init skripty typicky umiestnené v */etc/init.d/* alebo */etc/rc.d/init.d*.
- **Systemd** používa “service units” typicky umiestnené v */etc/systemd/system* alebo */usr/lib/systemd/system*. Hlavnými výhodami sú jednoduchšie ovládanie a paralelné vykonávanie úloh.
- **Systemd** je spätne kompatibilný s **init**.

Správa služieb (2)

- Zoznam služieb v systéme
  - `systemctl list-unit-files`
  - `chkconfig --list`
  - `service --status-all`
- Kontrola stavu služby
  - `systemctl status httpd`
  - `service httpd status`
- Spustenie/zastavenie služby
  - `systemctl start/stop httpd`
  - `service httpd start/stop`
- Povolenie/zakázanie spúšťania pri štarte
  - `systemctl enable/disable httpd`
  - `chkconfig httpd off`

Log-y

- Súbory s auditnými záznamami o činnosti procesov sa nachádzajú (typicky) v adresári `/var/log`
- Rotácia logov (vyhnutie sa zaplneniu disku logmi)
  - podľa veľkosti, času, ...
  - `man logrotate.conf`
- Formát: <timestamp> <hostname> <proces/kernel>: správa
- Správy jadra: dmesg
- Systémové logy
  - služba `rsyslogd, /etc/rsyslog.conf`
  - `/var/log/{messages,secure,cron,debug}`

Aplikačné logy

- Služba *sendmail* (elektronická pošta)
  - `/var/log/maillog`
  - záznamy o spustení a fungovaní služby,
  - o spracovaní aliasov,
  - o každom e-maile.
- Služba *httpd* (apache web server)
  - záznamy servera sa nachádzajú v `messages`,
  - logy o všetkých prístupoch:
    - `/var/log/httpd/access_log`
    - `/var/log/httpd/error_log`
    - `/var/log/httpd/ssl_{access,error,request}_log`

Kontrola nainštalovaných programov

- Správa programových balíkov
  - `rpm`, nízka úroveň
    - `man rpm`
    - `rpm -qi kernel`
    - `rpm -qf `which top``
    - `rpm -ql openssh-server`
  - Overenie integrity balíkov
    - `rpm -V sendmail`

Správa balíkov (1)

- Programy sú distribuované vo forme programových balíkov z repozitárov.
- Správcovia balíkov (package manager) môžu byť rozni pre rôzne distribúcie
  - `yum, dnf,` vyššia úroveň
  - `man yum; man dnf`
  - `yum list installed`
- Inštalácia / aktualizácia
  - `yum search apache`
  - `yum install httpd`
- Zoznam nakonfigurovaných repozitárov
  - `yum repolist`

Správa balíkov (2)

- Automatické aktualizácie
  - `service yum-cron status`
  - `systemctl enable yum-cron`
  - `vi /etc/yum/yum-cron.conf`
  - `systemctl enable yum-cron --now`
- Manuálna aktualizácia
  - `yum update`
- Urobiť aktualizáciu vždy po inštalácii nového systému!

Súvisiace témy

- Bezpečnostné rozšírenia SELinux
  - `getenforce, man selinux`
- Process accounting
  - psacct, `accton`
- Linux auditing system
  - `auditd`
- Bootovací proces
  - `telinit, runlevel`
- Zmena root adresára pre proces (chroot jail)
  - `chroot`

Zdroje

- Manuálové stránky
  - https://linux.die.net/man/
- The Linux System Administrator’s Guide
  - https://tldp.org/LDP/sag/html/
- Red Hat 7 Security Guide
  - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/index
- Linux Administrator’s Security Guide
  - https://seifried.org/lasg/
- Enabling Process Accounting on Linux HOWTO
  - http://www.faqs.org/docs/Linux-mini/Process-Accounting.html
- Securing & Optimizing Linux: The Ultimate Solution
  - https://tldp.org/LDP/solrhe/Securing-Optimizing-Linux-The-Ultimate-Solution-v2.0.pdf