Processes and Programs

- Basic Terms
- Process List
- System Load
- Process Management, Signals
- Process Activity
- Resources and their limits
- Managing Services
- Audit Records (logs)
- Managing Packages, Updates

Process

- Running instance of a program.
- Created by calling `fork()` (or `clone()`) as a copy of the caller process.
- Uniquely identified by PID.
- Assigned UID and GID of the user that started the process.
- Communicates via files (`stdin, stdout, stderr`) and signals.
- Consumes system resources (memory, cpu time).
- Service/Server – process running in the background (typically).

Process List (1)

- `ps` command shows information about running processes:
  - PID, PPID,
  - UID,
  - state (R, T, D, S, I, Z),
  - memory usage, cpu usage,
  - command name, arguments, ...
- Filters
  - filter output e.g. based on the user
- Output format, ordering.

Process List (2)

- All processes in the system:
  - `ps aux`
  - `ps –e`
- Processes of specified user
  - `ps –Fu user`
- Show relations
  - `ps –eH; ps axjf; pstree`
  - `ps –feHu`
- Information about threads
  - `ps –eLf`

Searching for Processes

- `ps aux | grep sshd`
- `pgrep` – search by multiple criteria.
- Lists corresponding PIDs.
  - `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`

System Load (1)

- Overall view
  - `uptime`
    - current time, time from boot (up time),
    - number of logged-in users,
    - load averages (1, 5, 15 minutes),
- Periodic (interactive) process monitoring
  - `top`
    - processes, (threads), memory (swap),
    - sorting by CPU usage, memory usage, PID, CPU time, ...

System Load (2)

- `top`
  - f: selection of view parameters
  - H: information about threads
  - u: filtering by user
  - M: sort by memory usage (%)
  - P: sort by CPU usage (%)
  - O: selection of filtering criteria
  - k: kill / send signal
- Free memory
  - `free, vmstat`

Signals – Terminate Process

- Send signal to processes with specified PID(s)
  - `man kill`
  - `kill 1234; kill -9 1234; kill -SIGKILL 1234`
  - `kill -l`, shows list of signals
- Send signal to processes based on the name
  - `pkill`, similar to pgrep (supports regular expressions)
  - `killall` (specified name must match exactly)
  - `killall -TERM telnet`
- Signals to terminate process (stops existing)
  - `SIGTERM, SIGKILL`

Signals – Stop Process

- Stopped process is not scheduled and therefore does not run and does not consume CPU time (also does not process signals).
- Can be restarted from the point it was stopped.
- Start and stop a process:
  - `SIGSTOP, SIGCONT`
  - `kill –STOP 1234`
  - `pkill –STOP –u user bash`
  - `pkill –CONT –u user bash`

Signals – Other

- Reload configuration file
  - `SIGHUP`
  - Some daemons react to this signal by re-reading their configuration without the need to stop them.
  - `killall –HUP sshd`
  - `pkill –HUP named`
- Show I/O statistics (command `dd`)
  - `USR1`, after receiving this signal, dd prints statistics to stderr.
  - `killall –USR1 –u user dd`
  - Note: for statistics with other commands, see `pv`

Monitoring Process Activity (1)

- `lsof`, List of all open files
  - `man lsof`
- Processes with name beginning with “ba”
  - `lsof –c ba, lsof –c /^ba/`
- Processes that have open files from /tmp/ and its subdirectories
  - `lsof +D /tmp/`
- Listing of files for process with PID 1
  - `lsof –p 1`
- `fuser`, List of processes using a specific file
  - `man fuser`
  - `fuser /bin/*sh`
- By default lists only PIDs and type of access. Options ‘-u’ and ‘-v’ to list user and commands
  - `fuser –u ~`
  - `fuser –v /tmp`

Monitoring Process Activity (2)

- Open network connections
- List all sockets in the system
  - `man netstat`
- With option ‘-p’ lists also command and PID of the process to which the socket belongs (only root).
  - `netstat –nap`
- Show listening sockets.
  - `netstat –protocol=ip –nlp`
  - `netstat –tunlp`

Monitoring Process Activity (3)

- List system calls used by a process
  - `man strace`
  - `strace -p 123 -f -o output.txt`
- Monitor library calls
  - `man ltrace`
  - `ltrace -p 234 -s 255 -e read`
- Only root can monitor other users' processes.

Process Resource Limits

- Resource limits for a process
  - `man ulimit` (shell built-in command)
  - `ulimit -a`, list current settings
  - core file, data segment, virtual memory, number of files, file size, number of locks, CPU time, number of processes, ...
  - regular user can only decrease,
  - user settings:
    - `/etc/security/limits.conf`
  - global settings:
    - `/etc/rc.local`

Process Scheduling Priority

- Scheduling priority of a process can be altered by changing its `nice` value:
  - range: from +19 (lowest priority) to -20 (highest priority).
- Start process with changed priority
  - `man nice`
  - `nice –n –10 csh`
- Changing priority of a running process
  - `man renice`
  - `renice 10 1234`
  - only root can increase the priority.

Managing Services (1)

- Some processes execute tasks needed for correct system behaviour, or they can provide different services, e.g.
  - `init, systemd, crond, rsyslogd, sendmail, sshd, …`
- Services are started and managed by init system (init daemon).
- Historically there have been multiple init system implementations. Currently most modern distributions use **systemd**. Other popular option is **init** (SysV init) and its variants.
- Init uses init scripts typically located in */etc/init.d/* or */etc/rc.d/init.d*.
- Systemd uses service units typically located in */etc/systemd/system* or */usr/lib/systemd/system*. The main advantage is easier control of services and parallelized job execution.
- Systemd is backwards compatible with init.

Managing Services (2)

- List services
  - `systemctl list-unit-files`
  - `chkconfig --list`
  - `service --status-all`
- Check service status
  - `systemctl status httpd`
  - `service httpd status`
- Start/stop service
  - `systemctl start/stop httpd`
  - `service httpd start/stop`
- Enable/disable on startup
  - `systemctl enable/disable httpd`
  - `chkconfig httpd off`

Logs

- Files with audit records about process activities are (typically) saved in `/var/log`
- Log rotation (avoiding disk fill-up)
  - based on size, time, ...
  - `man logrotate.conf`
- Format: <timestamp> <hostname> <process/kernel>: message
- Kernel messages: dmesg
- System logs
  - `rsyslogd, /etc/rsyslog.conf`
  - `/var/log/{messages,secure,cron,debug}`

Application Logs

- sendmail service (electronic mail)
  - `/var/log/maillog`
  - logs about running and functioning of the service
  - about processing aliases
  - about every e-mail
- httpd service (apache web server)
  - server logs are in `messages,`
  - logs about all accesses:
    - `/var/log/httpd/access_log`
    - `/var/log/httpd/error_log`
    - `/var/log/httpd/ssl_{access,error,request}_log`

Checking installed programs

- Package Management
  - `rpm`, low level
    - `man rpm`
    - `rpm -qi kernel`
    - `rpm -qf `which top``
    - `rpm -ql openssh-server`
  - Verify package integrity
    - `rpm -V sendmail`

Managing packages (1)

- Programs are distributed in the form of packages and downloaded from repositories
- Package managers may vary based on the Linux distribution.
  - `yum, dnf,` high level
  - `man yum; man dnf`
  - `yum list installed`
- Install / update
  - `yum search apache`
  - `yum install httpd`
- List configured repositories
  - `yum repolist`

Managing packages (2)

- Automatic updates
  - `service yum-cron status`
  - `systemctl enable yum-cron`
  - `vi /etc/yum/yum-cron.conf`
  - `systemctl enable yum-cron --now`
- Manual updates
  - `yum update`
- Always Update software after installing a new system!

Related Topics

- Linux Security Module SELinux
  - `getenforce, man selinux`
- Process accounting
  - psacct, `accton`
- Linux auditing system
  - `auditd`
- Boot process
  - `telinit, runlevel`
- Changing root directory for process
  - `chroot`

References

- Manual pages
  - 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