Chapter 03. 시스템 모니터링

로깅과 시스템 모니터링 도구의 활용

로깅 및 시스템 모니터링 도구

- 로그 파일
  - 시스템 로그 파일
    - /var/log/*
  - 시스템 커널 메세지
    - dmesg
  - 응용 소프트웨어 로그 파일
    - /var/log/[데몬명]/*
- 로그 관리 유틸리티
  - logrotate
- 스케쥴 작업 관리
  - cron, anacron
- 시스템 모니터링 유틸리티
  - 프로세서(CPU) 사용량
    - top
    - htop
    - mpstat
  - 메모리 사용량
    - vmstat
    - /proc/meminfo
  - 디스크 IO 사용량
    - iostat
  - 종합 리소스 모니터링
    - sar

시스템 로그

다양한 시스템 로그 살펴보기 - /var/log/*

- bootstrap.log - 부팅 로그 (시스템 부팅 과정에서 발생하는 성공/실패 로그)
- dpkg.log - 패키지 설치 로그
- kern.log - 커널 로그
  - 현재 부팅 후 커널 로그는 커맨드라인 dmesg 로 확인 (시스템 디바이스 메시지 등)
- syslog - 애플리케이션 로그 (각종 시스템 소프트웨어, 응용 소프트웨어 의 로그)
- Xorg.0.log - X윈도우 각종 로그 (윈도우 애플리케이션의 오류 등)

시스템 로그 - 응용 소프트웨어 로그

다양한 응용 소프트웨어 로그 살펴보기 - /var/log/(애플리케이션)/*

- apt/history.log
  - 업그레이드 등에 수행된 명령어 로그 기록
- apt/term.log
  - 위 수행된 결과의 로그 기록

- nginx/access.log
  - 접속 로그, GET / POST, 요청 URL, 응답값 (허용 200, 실패 404 등), 등
- nginx/error.log
  - 서버 시스템의 (치명적) 오류

- apache2/access.log
  - 접속 로그 (상동)
- apache2/error.log
  - 서버 시스템의 (치명적) 오류

로그 유틸리티

시스템 로그의 자동 (용량) 관리 - logrotated

- 시스템 로그 설정파일
  - /etc/logrotate.conf
- 애플리케이션별 로그 관리 옵션
  - /etc/logrotate.d/*

```
user1@user1-VirtualBox:~$ cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# use the syslog group by default, since this is the owning group
# of /var/log/syslog.
su root syslog

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
```

```
user1@user1-VirtualBox:~$ ls /etc/logrotate.d/
alternatives  dpkg          pm-utils           ufw
apache2       lightdm       postgresql-common  unattended-upgrades
apport        mysql-server  ppp                upstart
apt           nginx         rsyslog            vsftpd
cups-daemon   php7.2-fpm    speech-dispatcher
```

```
user1@user1-VirtualBox:~$ cat /etc/logrotate.d/rsyslog
/var/log/syslog
{
        rotate 7
        daily
        missingok
        notifempty
        delaycompress
        compress
        postrotate
                /usr/lib/rsyslog/rsyslog-rotate
        endscript
}

/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/l
/var/l
/var/l
/var/l
/var/l
{
```

```
user1@user1-VirtualBox:~$ cat /etc/logrotate.d/nginx
/var/log/nginx/*.log {
        daily
        missingok
        rotate 14
        compress
        delaycompress
        notifempty
        create 0640 www-data adm
        sharedscripts
        prerotate
                if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
                        run-parts /etc/logrotate.d/httpd-prerotate; \
                fi \
        endscript
        postrotate
                invoke-rc.d nginx rotate >/dev/null 2>&1
        endscript
}
```

스케쥴 프로세스

특정 시간마다 특정 프로세스 실행 - cron, anacron

- cron 이란?
  - cron = Command Run On
  - 특정 시간마다 반복하여 작업을 수행, 특정 월, 요일, 시간, 등의 조건 설정
  - 단, 해당 일자에 시스템이 꺼져 있으면 동작하지 않음
  - 시작 위치
    - /etc/crontab

- anacron 이란?
  - 해당 작업이 정해진 시간 내에 실행된 적이 있는지를 확인하여 없다면 적절한 시점(정해진 시간 후) 에 실행
  - 시작 위치
    - /etc/anacrontab

스케쥴 프로세스 - cron

특정 시간마다 특정 스크립트 실행 - cron 상세기능

- 실행 데몬
  - cron (systemctl status cron)

- 시스템 작업
  - /etc/crontab
    - /etc/cron.hourly
    - /etc/cron.daily
    - /etc/cron.weekly
    - /etc/cron.monthly

  - 동작 조건

분	시	일	월	주	권한	명령어	
17	*	*	*	*	root	xxxxx	(매시 17분에 xxxxx 수행)
25	6	*	*	*	root	yyyyy	(매일 6:25분에 yyyyy 수행)
47	6	*	*	7	root	zzzzz	(매주 일요일 6:47분에 zzzzz 수행) -> 요일 0(일요일) ~ 6(토요일), 7 = 0
52	6	1	*	*	root	qqqqq	(매달 1일, 6:52분에 qqqqq 수행)

스케쥴 프로세스 - anacron

특정 시간마다 특정 스크립트 실행 - anacron 상세기능

- 실행 데몬
  - 없음 (cron 를 통해 실행)

- 시스템 작업
  - /etc/anacrontab

  - 동작 조건

일	분	체크디렉토리	명령어	
1	5	cron.daily	xxxxx	-> 최근 1일동안 cron.daily 가 실행되지 않았다면, 5분 후 xxxxx 실행
7	10	cron.weekly	yyyyy	-> 최근 7일동안 cron.weekly 가 실행되지 않았다면, 10분 후 yyyyy 실행
…				

스케쥴 프로세스 - 사용자별 cron

특정 시간마다 특정 프로세스 실행 - cron 상세기능

- 실행 데몬
  - crond
- 사용자별 작업
  - 스케줄 작업 만들기
    - crontab -e
  - 스케줄 작업 확인
    - crontab -l
  - 스케줄 작업 삭제
    - crontab -r
  - 저장 공간
    - /var/spool/cron/crontabs/[사용자명]

```
user1@user1-VirtualBox:~$ crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
```

시스템 모니터링 - 자원(CPU/Mem) 모니터링

top 을 사용한 CPU, Memory, Process 모니터링

- top -d 1 (갱신 주기, 1초 (기본값 2초))

```
top - 00:53:32 up 2 days,  1:44,  3 users,  load average: 0.28, 0.14, 0.05
Tasks: 236 total,   1 running, 203 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.7 us,  1.0 sy,  0.0 ni, 97.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  4039408 total,   312788 free,  1312712 used,  2413908 buff/cache
KiB Swap:   998396 total,   996348 free,     2048 used.  2407988 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 9220 user1     20   0 3027196 429780 110336 S  1.3 10.6   5:40.64 gnome-shell
 8960 user1     20   0  398484  79924  45812 S  1.0  2.0   1:11.15 Xorg
21728 user1     20   0   43208   3912   3176 R  0.7  0.1   0:00.06 top
 9480 user1     20   0  793980  24688  19048 S  0.3  0.6   0:52.17 gsd-color
 9585 user1     20   0  991404  89988  43412 S  0.3  2.2   0:05.73 nautilus-
20090 root      20   0       0      0      0 I  0.3  0.0   0:00.13 kworker/0
    1 root      20   0  225844   9408   6496 S  0.0  0.2   0:17.91 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.03 kthreadd
    4 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kworker/0
    6 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 mm_percpu
    7 root      20   0       0      0      0 S  0.0  0.0   0:03.46 ksoftirqd
    8 root      20   0       0      0      0 I  0.0  0.0   0:10.66 rcu_sched
    9 root      20   0       0      0      0 I  0.0  0.0   0:00.00 rcu_bh
   10 root      rt   0       0      0      0 S  0.0  0.0   0:00.00 migration
   11 root      rt   0       0      0      0 S  0.0  0.0   0:00.64 watchdog/
   12 root      20   0       0      0      0 S  0.0  0.0   0:00.00 cpuhp/0
   13 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kdevtmpfs
   14 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 netns
   15 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_tasks
   16 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kauditd
   17 root      20   0       0      0      0 S  0.0  0.0   0:00.16 khungtask
```

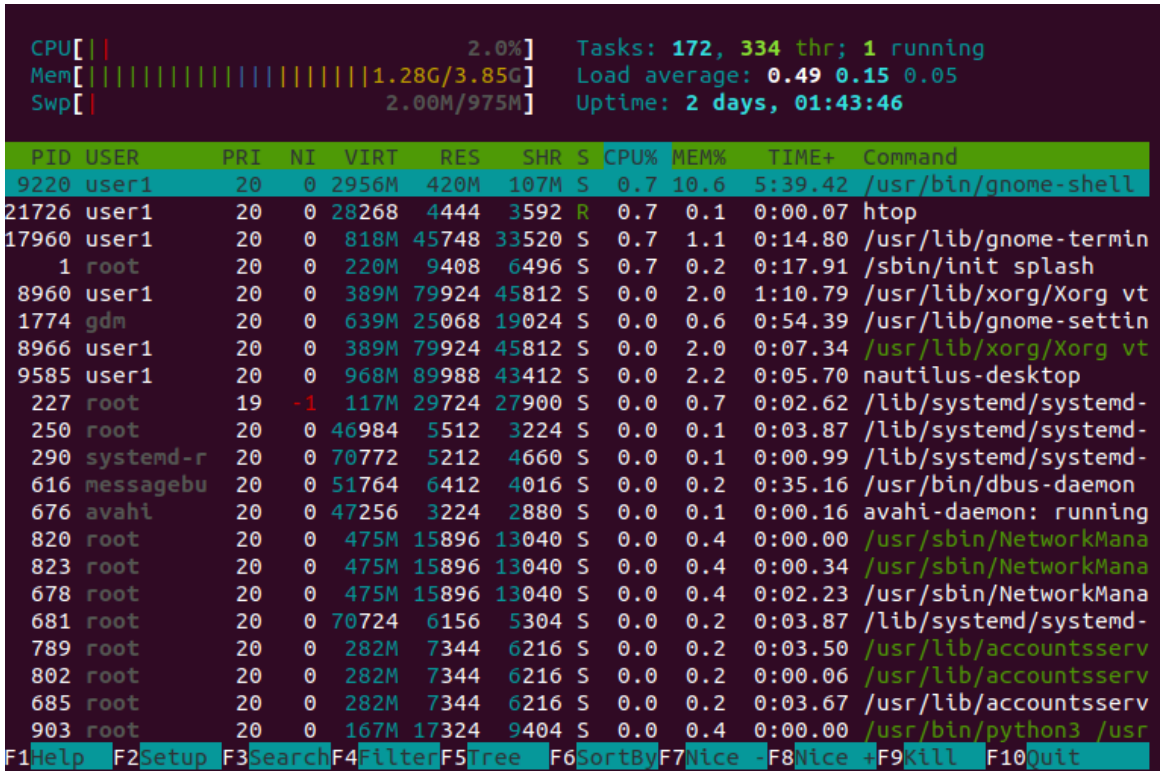
- h : 도움말
- P : 프로세서 (CPU) 사용률별 내림차순
- M : 메모리 사용률별 내림차순
- T : 프로세서 사용 시간 순 내림차순
- 1 : CPU 코어 별

```
Help for Interactive Commands - procps-ng 3.3.12
Window 1:Def: Cumulative mode Off.  System: Delay 1.0 secs; Secure mode Off.

  Z,B,E,e   Global: 'Z' colors; 'B' bold; 'E'/'e' summary/task memory scale
  l,t,m     Toggle Summary: 'l' load avg; 't' task/cpu stats; 'm' memory info
  0,1,2,3,I Toggle: '0' zeros; '1/2/3' cpus or numa node views; 'I' Irix mode
  f,F,X     Fields: 'f'/'F' add/remove/order/sort; 'X' increase fixed-width

  L,&,<,> . Locate: 'L'/'&' find/again; Move sort column: '<'/'>' left/right
  R,H,V,J . Toggle: 'R' Sort; 'H' Threads; 'V' Forest view; 'J' Num justify
  c,i,S,j . Toggle: 'c' Cmd name/line; 'i' Idle; 'S' Time; 'j' Str justify
  x,y     . Toggle highlights: 'x' sort field; 'y' running tasks
  z,b     . Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
  u,U,o,O . Filter by: 'u'/'U' effective/any user; 'o'/'O' other criteria
  n,#,^O  . Set: 'n'/'#' max tasks displayed; Show: Ctrl+'O' other filter(s)
  C,...   . Toggle scroll coordinates msg for: up,down,left,right,home,end

  k,r       Manipulate tasks: 'k' kill; 'r' renice
  d or s    Set update interval
  W,Y       Write configuration file 'W'; Inspect other output 'Y'
  q         Quit
          ( commands shown with '.' require a visible task display window )
Press 'h' or '?' for help with Windows,
Type 'q' or <Esc> to continue
```

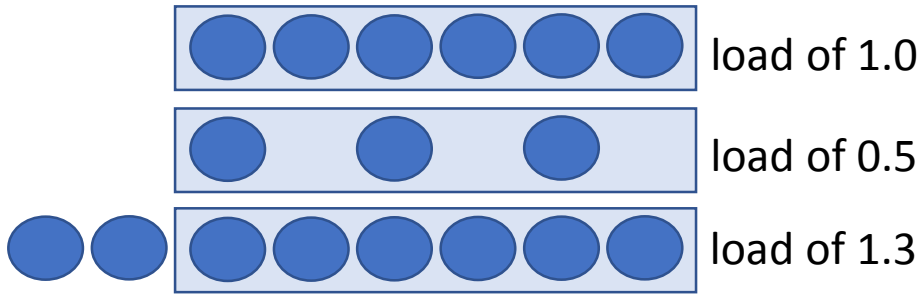
시스템 모니터링 - 자원(CPU/Mem) 모니터링

htop 을 사용한 CPU, Memory, Process 모니터링

- sudo apt install htop
- htop -d 5 (갱신주기 0.5초, 단위 주의)



- Load Average?
  - cat /proc/loadavg
  - core 별 1분/5분/15분 동안의 평균 작업량



- VIRT : 가상 메모리 크기
- RES : 물리적 메모리 크기
- SHR : 공유 메모리 크기

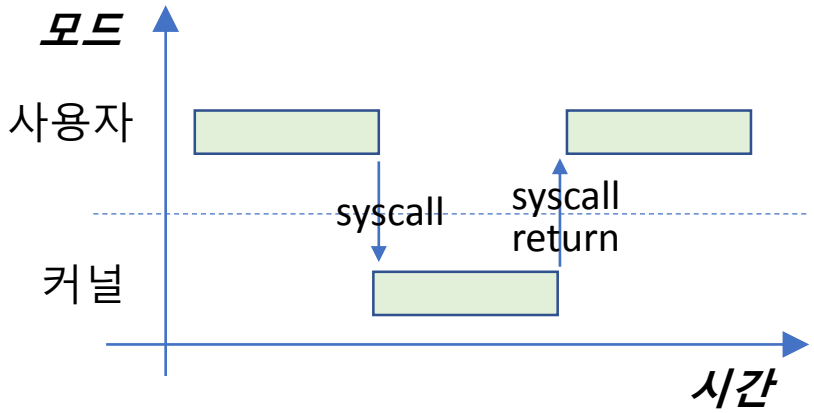
시스템 모니터링 - 프로세서(CPU) 모니터링

프로세스 동작방식 및 모드에 따른 측정 시간

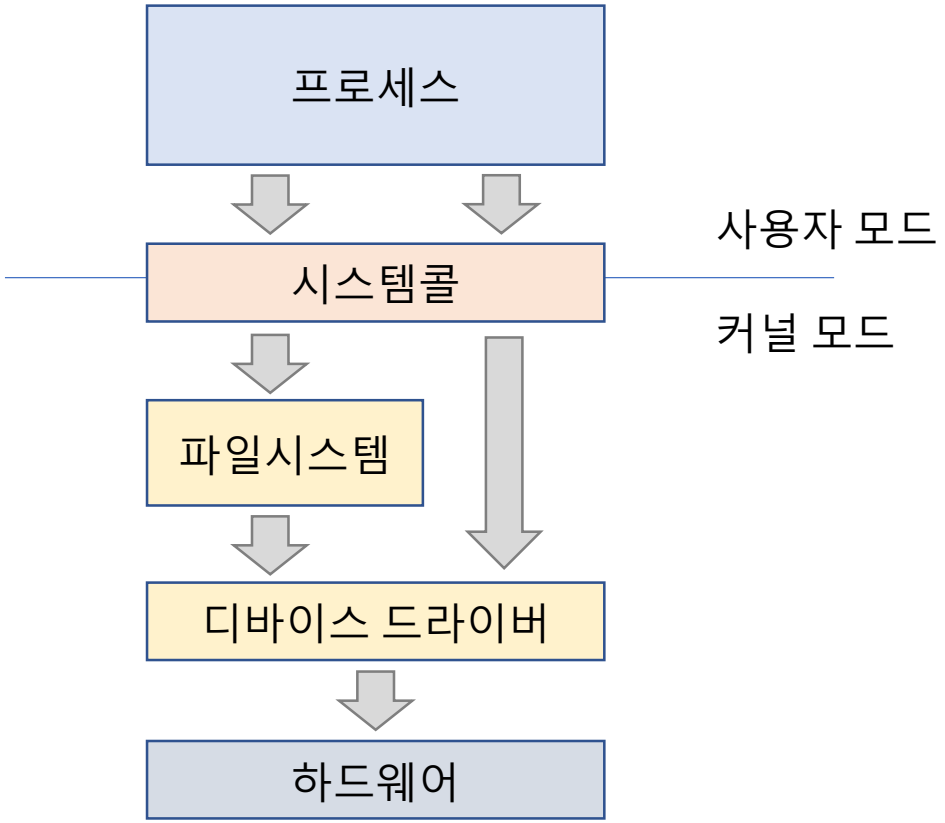
- 사용자모드와 커널모드

```
user1@user1-VirtualBox:~$ time sleep 5

real    0m5.002s
user    0m0.001s
sys     0m0.001s
```

```
user1@user1-VirtualBox:~$ time sudo hdparm -T /dev/sda

/dev/sda:
 Timing cached reads:   13092 MB in  1.99 seconds = 6564.49 MB/sec

real    0m7.092s
user    0m0.134s
sys     0m1.868s
```



- 장치파일(디바이스) 접근구조



시스템 모니터링 - 프로세서(CPU) 모니터링

mpstat을 사용한 CPU 사용량 조회

- mpstat [주기] [횟수]
- mpstat 1 (1초 갱신)
- mpstat 1 10 (1초 갱신, 10회 후 통계)
- mpstat -P ALL (CPU를 core별로 표시)

- CPU 통계?
  - /proc/stat

```
user1@user1-VirtualBox:~$ mpstat 1 10
Linux 4.15.0-101-generic (user1-VirtualBox)     2020년 06월 06일        _x86_64_ (1 CPU)

01시 30분 55초   CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
01시 30분 56초   all    2.04    0.00    1.02    0.00    0.00    0.00    0.00    0.00    0.00   96.94
01시 30분 57초   all    6.12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00   93.88
01시 30분 58초   all   20.41    0.00    2.04    0.00    0.00    0.00    0.00    0.00    0.00   77.55
01시 30분 59초   all   12.00    0.00    2.00    0.00    0.00    0.00    0.00    0.00    0.00   86.00
01시 31분 00초   all   31.31    0.00    7.07    0.00    0.00    0.00    0.00    0.00    0.00   61.62
01시 31분 01초   all   93.00    0.00    7.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
01시 31분 02초   all   71.72    0.00    3.03    0.00    0.00    0.00    0.00    0.00    0.00   25.25
01시 31분 03초   all   16.49    0.00    2.06    0.00    0.00    0.00    0.00    0.00    0.00   81.44
01시 31분 04초   all   69.70    0.00    6.06    0.00    0.00    0.00    0.00    0.00    0.00   24.24
01시 31분 05초   all   19.19    0.00    0.00    1.01    0.00    0.00    0.00    0.00    0.00   79.80
평균값:     all   34.35    0.00    3.04    0.10    0.00    0.00    0.00    0.00    0.00   62.51
```

%usr : 사용자 레벨의 CPU 사용량
%nice : nice 우선순위가 적용된 CPU 사용량
%sys : 시스템 레벨(커널)의 CPU 사용량
%iowait : I/O 처리를 위해 기다리는 CPU 시간
%irq : H/W 시스템 인터럽트 처리를 위해 사용된 CPU 시간
%soft : S/W 인터럽트 처리를 위해 사용된 CPU 시간
%steal : 하이퍼바이저에 의해 대기한(빼앗긴) CPU 시간
%guest : (호스트에서) VM 가상머신에 제공해준 CPU 시간
%gnice : (호스트에서) nice 가 적용된 guest CPU 시간
%idle : 대기한(유휴한) CPU 시간

시스템 모니터링 - 메모리 모니터링

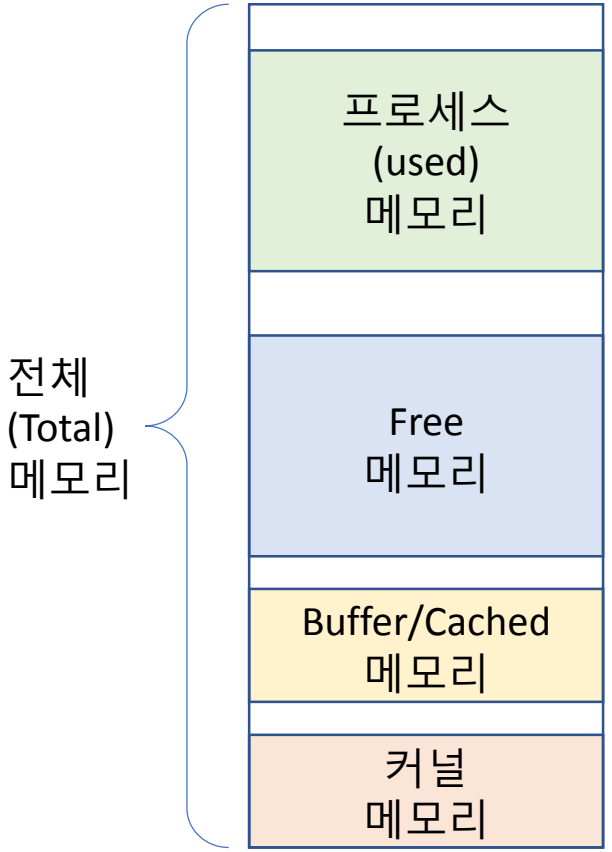
free, /proc/meminfo 를 사용한 메모리 사용량 조회

- 각 유형별 메모리 사용량
  - free
  - cat /proc/meminfo

```
user1@user1-VirtualBox:~$ free
               total        used        free      shared  buff/cache   available
Mem:         4039408     1342280      278792       33544     2418336     2376408
스왑:         998396        2048      996348
```

```
user1@user1-VirtualBox:~$ cat /proc/meminfo
MemTotal:        4039408 kB
MemFree:          314516 kB
MemAvailable:    2410076 kB
Buffers:          275996 kB
Cached:          1959248 kB
SwapCached:          212 kB
Active:          1892676 kB
Inactive:        1489220 kB
Active(anon):     868304 kB
Inactive(anon):   309876 kB
Active(file):    1024372 kB
Inactive(file):  1179344 kB
Unevictable:          16 kB
Mlocked:              16 kB
SwapTotal:        998396 kB
SwapFree:         996348 kB
Dirty:                12 kB
Writeback:             0 kB
AnonPages:       1146516 kB
Mapped:           300104 kB
Shmem:             31528 kB
Slab:             229980 kB
SReclaimable:     179024 kB
SUnreclaim:        50956 kB
KernelStack:        9120 kB
PageTables:        46748 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:     3018100 kB
Committed_AS:    5243544 kB
VmallocTotal:   34359738367 kB
VmallocUsed:           0 kB
VmallocChunk:          0 kB
HardwareCorrupted:     0 kB
AnonHugePages:         0 kB
ShmemHugePages:        0 kB
ShmemPmdMapped:        0 kB
CmaTotal:              0 kB
CmaFree:               0 kB
HugePages_Total:       0
HugePages_Free:        0
HugePages_Rsvd:        0
HugePages_Surp:        0
Hugepagesize:       2048 kB
DirectMap4k:      186304 kB
DirectMap2M:     4007936 kB
```

사용 가능 (Available) 메모리 = Free 메모리 + 반환가능 메모리



시스템 모니터링 - 메모리 및 시스템 부하 모니터링

vmstat 를 사용한 메모리 사용량 조회

- 메모리 + 시스템 통계
  - vmstat [주기]
  - vmstat 1 (1초 단위 갱신)

```
user1@user1-VirtualBox:~$ vmstat 1
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 4  0   2048 314764 275992 2138272    0    0    13    44   74  171  1  0 99  0  0
 0  0   2048 314756 275992 2138272    0    0     0     0  100  304  3  0 97  0  0
 0  0   2048 314756 275992 2138272    0    0     0     0  113  244  2  1 97  0  0
 0  0   2048 314756 275992 2138272    0    0     0     0  112  221  2  0 98  0  0
 0  0   2048 314756 275992 2138272    0    0     0     0  515 1614 11  3 86  0  0
 0  0   2048 314756 275992 2138272    0    0     0     0  291  632 15  1 84  0  0
 0  0   2048 314756 275992 2138272    0    0     0     0  108  249  4  0 96  0  0
 0  0   2048 314756 275992 2138272    0    0     0     0   89  186  3  0 97  0  0
```

- procs
  - r : 현재 동작을 대기하는 프로세스의 수 (waiting to run)
  - b : sleep 상태에 있는 프로세스 수
- memory
  - swpd : 스왑 메모리 크기
  - free : 작여 메모리 크기 (idle memory, 유휴 메모리)
  - buff : 버퍼 영역으로 사용된 메모리 크기
  - cache : 캐시 영역으로 사용된 메모리 크기
- swap
  - si / so : 초당 swap in/out 한 데이터 양 (물리적 메모리가 적을때 발생)
- io
  - bi / bo : 초당 블럭디바이스로부터 받은 데이터 in/out 양
- system
  - in : 초당 인터럽트 발생 수 (clock 인터럽트 포함)
  - cs : 초당 발생한 컨텍스트 스위칭 수
- cpu
  - us / sy / id / wa / st : CPU % 사용량 (user, system, idle, wait(IO), stolen(VM))

시스템 모니터링 - 디스크 IO 모니터링

iostat 을 사용한 디스크 IO 사용량 조회

- 디바이스 입출력
  - iostat [주기] [디바이스]
  - iostat 1 sda (1초 갱신, sda 디스크)

```
user1@user1-VirtualBox:~$ iostat
Linux 4.15.0-101-generic (user1-VirtualBox)     2020년 06월 06일        _x86_64_   (
1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          0.65    0.06    0.21    0.29    0.00   98.80

Device             tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
loop0             0.00         0.01         0.00       1292          0
loop1             0.07         0.08         0.00      14021          0
loop2             0.00         0.01         0.00       1315          0
loop3             0.00         0.00         0.00         46          0
loop4             0.00         0.00         0.00        121          0
loop5             0.00         0.00         0.00        116          0
loop6             0.00         0.01         0.00       1301          0
loop7             0.00         0.01         0.00        988          0
scd0              0.00         0.04         0.00       6758          0
sda               1.20        12.84        44.32    2290551    7908400
loop8             0.00         0.00         0.00         44          0
loop9             0.00         0.00         0.00        507          0
loop10            0.00         0.00         0.00        142          0
loop11            0.07         0.07         0.00      12856          0
loop12            0.00         0.00         0.00          8          0
```

```
user1@user1-VirtualBox:~$ iostat 1 sda
Linux 4.15.0-101-generic (user1-VirtualBox)     2020년 06월 06일        _x86_64_   (
1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          0.65    0.06    0.21    0.29    0.00   98.80

Device             tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda               1.20        12.84        44.31    2290551    7908400

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          2.02    0.00    0.00    0.00    0.00   97.98

Device             tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda               0.00         0.00         0.00          0          0
```

시스템 모니터링 - 종합 모니터링 도구

sar 를 이용한 프로세스, 메모리 모니터링 : sar = System Activity Report

- 프로세스 모니터링
  - sar [주기] [횟수]
  - sar 1 5
  - sar -P [프로세스] [주기]
  - sar -P ALL 1
- 메모리 모니터링
  - sar -r [주기]
  - sar -r 1

- sudo apt install sysstat (기본 설치)
  - sar
  - mpstat
  - vmstat
  - iostat
  - 등 모두 포함…

```
user1@user1-VirtualBox:~$ sar 1 5
Linux 4.15.0-101-generic (user1-VirtualBox)     2020년 06월 06일        _x86_64_        (1 CPU)

12시 37분 21초     CPU     %user     %nice   %system   %iowait    %steal     %idle
12시 37분 22초     all      5.00      0.00      1.00      0.00      0.00     94.00
12시 37분 23초     all      8.33      0.00      3.12      0.00      0.00     88.54
12시 37분 24초     all     16.82      0.00      7.48      0.00      0.00     75.70
12시 37분 25초     all     17.02      0.00      1.06      0.00      0.00     81.91
12시 37분 26초     all     12.37      0.00      4.12      0.00      0.00     83.51
평균값:      all     11.94      0.00      3.44      0.00      0.00     84.62
user1@user1-VirtualBox:~$ sar -r 1 5
Linux 4.15.0-101-generic (user1-VirtualBox)     2020년 06월 06일        _x86_64_        (1 CPU)

12시 37분 49초 kbmemfree   kbavail kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
12시 37분 50초    637620   2372904   3401788     84.22    286932   1623832   5287768    104.96   2192816    920136        68
12시 37분 51초    637620   2372904   3401788     84.22    286932   1623832   5287768    104.96   2192816    920136        68
12시 37분 52초    637620   2372904   3401788     84.22    286932   1623832   5287768    104.96   2192816    920136        68
12시 37분 53초    637620   2372904   3401788     84.22    286932   1623832   5287768    104.96   2192816    920136        68
12시 37분 54초    637620   2372904   3401788     84.22    286932   1623832   5287768    104.96   2192816    920136        68
평균값:     637620   2372904   3401788     84.22    286932   1623832   5287768    104.96   2192816    920136        68
user1@user1-VirtualBox:~$
```