Unix administrative files

```
$ cd /etc # Location of system configuration files
$ find . 2>/dev/null | wc -l
2989
$ head passwd # User accounts
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
$
```

List running processes

```
$ ps # List running processes
  PID TTY          TIME CMD
26355 pts/2    00:00:00 bash
27028 pts/2    00:00:00 ps
$ ps uw # List running processes with more details
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
dds      26355  0.0  0.0  25672  7476 pts/2    Ss   20:52   0:00 -bash
dds      28835  0.0  0.0  19100  2456 pts/2    R+   20:54   0:00 ps uw
$ ps xuw # Also include background processes
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
dds       2927  0.0  0.0  35788  1872 ?        Ss   Jun28   0:00 /lib/systemd/systemd --user
dds       2928  0.0  0.0  69812    20 ?        S    Jun28   0:00 (sd-pam)
dds       2974  0.0  0.0  10700    84 ?        Ss   Jun28   0:01 ssh-agent
dds      26352  0.0  0.0 114352  4208 ?        S    20:52   0:00 sshd: dds@pts/2
dds      26355  0.0  0.0  25672  7476 pts/2    Ss   20:52   0:00 -bash
dds      29232  0.0  0.0  19100  2480 pts/2    R+   20:54   0:00 ps uxw
$ ps auxw | head # Obtain information on all running processes
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.2  29888  3892 ?        Ss   Nov27   0:30 /sbin/init placeholder
root         2  0.0  0.0      0     0 ?        S    Nov27   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    Nov27   1:13 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   Nov27   0:00 [kworker/0:0H]
root         7  0.0  0.0      0     0 ?        S    Nov27   7:22 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    Nov27   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    Nov27   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S    Nov27   0:14 [watchdog/0]
root        11  0.0  0.0      0     0 ?        S    Nov27   0:14 [watchdog/1]
$
```

The /proc file system

```
$ cd /proc
$ ls -CF | head -5
1/      1441/   18/     26292/  355/   620/  9/           kpagecount
10/     1442/   183/    26477/  36/    622/  904/         kpageflags
11/     1443/   184/    26664/  37/    629/  941/         loadavg
11037/  1445/   19952/  26669/  38/    631/  953/         locks
12/     15/     2/      27/     40/    632/  957/         meminfo
$ head -5 cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 45
model name      : Intel(R) Xeon(R) CPU E5-1410 0 @ 2.80GHz
$ cd $$
$ ls -F
attr/            cpuset   limits      net/           projid_map  statm
```

```
autogroup        cwd@     loginuid    ns/             root@       status
auxv             environ  map_files/  numa_maps       sched       syscall
cgroup           exe@     maps        oom_adj         sessionid   task/
clear_refs       fd/      mem         oom_score       setgroups   timers
cmdline          fdinfo/  mountinfo   oom_score_adj   smaps       uid_map
comm             gid_map  mounts      pagemap         stack       wchan
coredump_filter  io       mountstats  personality     stat
$ more cmdline
-bash^@
$
```

Obtain file details

```
$ stat /etc/motd # Output file's details
  File: '/etc/motd'
  Size: 286             Blocks: 8          IO Block: 4096   regular file
Device: fe00h/65024d    Inode: 23068814    Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-28 11:00:03.588831888 +0200
Modify: 2013-06-02 23:29:42.000000000 +0300
Change: 2013-07-12 16:50:26.283933783 +0300
 Birth: -
$ stat -c '%s' /etc/motd # File size
286
$ stat -c '%Y' /etc/motd # File modification (seconds since Epoch)
1370204982
$ date -d @1370204982 # Format Epoch time
Sun Jun  2 23:29:42 EEST 2013
$ ls -l /etc/motd # Verify Epoch time
-rw-r--r-- 1 root root 286 Jun  2  2013 /etc/motd
$ stat -c '%U' $HOME # File user
dds
$
```

Access the Windows registry

```
$ cd /proc/registry # Navigate to the registry virtual folder
$ cd 'HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/'
$ ls -CF | head # List contents
Accessibility/                  KnownFunctionTableDlls/
AdaptiveDisplayBrightness/      KnownManagedDebuggingDlls/
AeDebug/                        LanguagePack/
APITracing/                     MCI Extensions/
AppCompatFlags/                 MCI32/
ASR/                            MiniDumpAuxiliaryDlls/
Audit/                          NetworkCards/
BootMgr/                        NetworkList/
BuildGUID                       NtVdm64/
BuildLab                        OpenGLDrivers/
$ more ProductName # Read installed software value
Windows 10 Pro^@
$ regtool set /HKEY_CURRENT_USER/Software/Cygwin/TestEntry 'Hello there' # Set value
$ more /proc/registry/HKEY_CURRENT_USER/Software/Cygwin/TestEntry # Read value
Hello there^@
$ regtool get /HKEY_CURRENT_USER/Software/Cygwin/TestEntry # Read value
Hello there
$
```

Obtain Windows system data

```
$ find /cygdrive/c/Windows/system32 -maxdepth 1 -type f -name \*.dll | # Find DLL files
> head | # First ten
> while read f ; do
>   wname=$(cygpath -w $f | sed 's/\\/\\\\/g') # Obtain Windows name with double \\
>   wmic datafile where "Name=\"$wname\"" get name, version # Run wmic query
> done |
> grep windows # Filter out blank lines and headers
```

```
c:\windows\system32\aaclient.dll  6.2.9200.17435
c:\windows\system32\accessibilitycpl.dll  6.1.7601.17514
c:\windows\system32\acctres.dll  6.1.7600.16385
c:\windows\system32\acledit.dll  6.1.7600.16385
c:\windows\system32\aclui.dll  6.1.7600.16385
c:\windows\system32\acppage.dll  6.1.7601.17514
c:\windows\system32\actioncenter.dll  6.1.7601.17514
c:\windows\system32\actioncentercpl.dll  6.1.7601.17514
c:\windows\system32\activeds.dll  6.1.7600.16385
c:\windows\system32\actxprxy.dll  6.1.7601.17514
$
```

List Windows services

```
$ wmic service get name,state | head # List status of Windows services
Name                            State
ACDaemon                        Running
AdobeARMservice                 Running
AdobeFlashPlayerUpdateSvc       Stopped
AeLookupSvc                     Stopped
ALG                             Stopped
AppIDSvc                        Stopped
Appinfo                         Running
AppleOSSMgr                     Running
AppleTimeSrv                    Running
$ wmic process get name,virtualsize |
> sort -k2rn | # List by reverse numerical order of second field
> head -6 # First six entries
System                      6451482624
firefox.exe                 1462980608
thunderbird.exe             943538176
Skype.exe                   711069696
explorer.exe                538497024
mintty.exe                  502165504
$
```

List Windows processes

```
$ tasklist | head

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0    164,008 K
smss.exe                       440 Services                   0        668 K
csrss.exe                      576 Services                   0      2,792 K
wininit.exe                    744 Services                   0      1,756 K
csrss.exe                      752 Console                    1     25,472 K
services.exe                   812 Services                   0     11,608 K
$
```