Using lsof, tcpdump, and tusc (3 friends of the sysadmin)

John Payne
HPUX Platform Engineer
Brigham Young University

HPUX @ BYU

- Over 50 HPUX servers
  - rp2470 – rp8400 in size, some Itanium
  - HPUX 10.20, HPUX 11.0, HPUX 11.11, HPUX 11.23
- At any given time, we are almost guaranteed to have change happen somewhere
- Engineering (Sysadmin) resources limited

John Payne

- 6 years (full-time) experience working with HPUX
  - Large stretches of that time as primary (read 'only') HPUX engineer
- HPUX CSA certification – June 2001
- 4th year at HP World
  - 3rd year presenting (3rd different topic)

Lsof, tcpdump, and tusc – Why these 3 tools?

- In any environment with change, things break
  - Generally not the sysadmin's fault
  - People come to sysadmin to:
    - Figure out what's going on
    - Fix it
  - This can be very annoying without tools to troubleshoot problems
- These tools can help discover root cause for a large number of problems

Lsof, tcpdump, and tusc – Why these 3 tools?

- Lsof – list open files
  - In UNIX, everything's a file…
  - Wide distribution
  - Command can handle and/or logic
- Tcpdump – dump traffic on a network
  - Watch the traffic coming in or out of your system
- Tusc – trace unix system calls
  - Attach to a process, watch what it's doing

Lsof – list open files

- Wide distribution
  - Available for almost any Unix
  - Easily compiled from source

- Where to get it
  - ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof
    - Lsof source
  - http://hpux.cs.utah.edu/hppd/hpux/Sysadmin/lsof-4.71/
    - The HP-UX Porting and Archive Centre
    - HPUX 11.0 and HPUX 11.23 binaries
    - HPUX Source

lsof

- LIst Open Files
  - Regular file
  - Directory
  - Block special file
  - Character special file
  - Executing text reference
  - Library
  - Network file
    - Socket
    - NFS

lsof output

- COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

  - COMMAND – 1st 9 characters of the name of the process
  - PID – Process ID number of the process
  - USER – Userid or login name of the owner of the process
  - FD – File Descriptor (See man page)
  - TYPE – Type of node of the file
  - DEVICE – Device numbers for file
  - SIZE/OFF – Size of file or file offset (in bytes)
  - NODE – node number of file
  - NAME – mount point, name of file, or internet address

lsof

- My favorite uses:
  - Listing who has a file open
  - Listing what's got a filesystem open
  - Finding open but deleted files
    - I usually get into this one as a direct result of something the operations staff does.
      - "I deleted some files, but the space didn't free up!"
      - Or they don't call and you have to poke around in the dark several days later
  - Finding network connections
    - Lots of uses for this one

lsof filename (no options specified)

- Find out who has a file open
  - Lsof will report back with a list processes that currently hold a file open or nothing.

Host1:/home/ucs/jjp# lsof jjp.out

Host1:/home/ucs/jjp#

Host1: /home/ucs/jjp# lsof /usr/bin/cvs

```
COMMAND   PID USER  FD   TYPE DEVICE SIZE/OFF  NODE  NAME
cvs     15816 bdm4  txt  VREG   64,0x8 3588744  21249  /usr/local/bin/cvs
cvs     15817 bdm4  txt   VREG  64,0x8 3588744  21249  /usr/local/bin/cvs
```

Host1: /home/ucs/jjp#

lsof filename (no options specified)

- Find out who has a file open
  - You can also do this on a filesystem
    - Like using 'fuser –c /filesystem'
    - If no output, nothing is listed.

```
Host1: /# bdf /data/axis /data/cvs
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg02/lvol9    1024000  172959  797885   18% /data/axis
/dev/vg05/lvol6   51200000 7057384 43798120   14% /data/cvs

Host1: /# lsof /data/axis

Host1: /# lsof /data/cvs
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF  NODE NAME
cvs     15817 bdm4    6r   VREG 64,0x40006      784   83515 /data/cvs (/dev/vg05/lvol6)
```

lsof –a +L1 /filesystem

- Find open files filling a filesystem, where an unlinked file still holds the space open
  - My personal favorite

Host1: /var/adm/syslog# lsof -a +L1 /var

```
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NLINK  NODE NAME
syslogd      708     root  10w  VREG   64,0x9 62142886        0  16607 /var (/dev/vg00/lvol9)
atswasdO8 1467     cck    6w  VREG   64,0x9         181        0      617 /var (/dev/vg00/lvol9)
swagentd   1866     root    5u   VREG   64,0x9         41        0      145 /var (/dev/vg00/lvol9)
```

Host1: /var/adm/syslog# kill -HUP 708

Host1: /var/adm/syslog# lsof -a +L1 /var

```
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF NLINK NODE NAME
atswasdO8   1467     cck    6w   VREG   64,0x9         181        0      617 /var (/dev/vg00/lvol9)
swagentd    1866     root    5u   VREG   64,0x9         41        0      145 /var (/dev/vg00/lvol9)
```

lsof –i

(network connection option)

- For searching through network connections
  - lsof –i [protocol] [@hostname or hostaddress] [:service or port]
    - Examples
      - TCP:22
      - TCP:telnet
      - @10.0.2.106
      - TCP@10.0.2.106:443
      - TCP:20-23

lsof –i

(network connection option)

- lsof –i tcp:22

Host1: /# lsof -i tcp:22

```
COMMAND   PID  USER  FD  TYPE    DEVICE  SIZE/OFF NODE NAME

sshd      849  root  4u  inet  0x48293c68       0t0  TCP  *:ssh (LISTEN)

sshd:    3120  root  5u  inet  0x5798e668 0t4617360 TCP  host1.byu.edu:ssh->
                                ukrainium.byu.edu:36408 (ESTABLISHED)

sshd:   12337  root  5u  inet 0x60903c68  0t643716  TCP  host1.byu.edu:ssh->
                                                    10.0.2.106:1144 (ESTABLISHED)

sshd:   12368   jjp  5u  inet 0x60903c68  0t643716  TCP  host1.byu.edu:ssh->
                                                    10.0.2.106:1144 (ESTABLISHED)
```

lsof –i

(network connection option)

- lsof –i tcp:telnet

```
COMMAND  PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
telnetd      2221   root   0u      inet 0x58b84a68      0t0       TCP host1.byu.edu:telnet->
                                                          10.0.2.106:1648 (ESTABLISHED)

telnetd      2221   root   1u      inet 0x58b84a68      0t0       TCP host1.byu.edu:telnet->
                                                          10.0.2.106:1648 (ESTABLISHED)

telnetd      2221   root   2u      inet 0x58b84a68      0t0       TCP host1.byu.edu:telnet->
                                                          10.0.2.106:1648 (ESTABLISHED)

inetd        4910   root   6u      inet 0x482f3a68      0t0       TCP *:telnet (LISTEN)
```

```
Host1: /# ps -ef|grep 2221
    jjp  2222  2221   0 11:36:38 pts/tb    0:00 -sh
   root  2221  4910   0 11:36:38 pts/tb    0:00 telnetd
   root  2336 13344   1 11:37:09 pts/4     0:00 grep 2221
```

lsof –i

(network connection option)

- lsof –i @10.0.2.106

```
COMMAND  PID USER FD TYPE    DEVICE SIZE/OFF  NODE NAME
sshd:       2008     root  5u    inet 0x4f733668 0t252646    TCP  host1.byu.edu:ssh->
                                                              10.0.2.106:1643 (ESTABLISHED)

sshd:       2047      jjp  5u    inet 0x4f733668 0t252646    TCP   host1.byu.edu:ssh->
                                                              10.0.2.106:1643 (ESTABLISHED)

telnetd     2221     root  0u    inet 0x58b84a68      0t0       TCP  host1.byu.edu:telnet->
                                                              10.0.2.106:1648 (ESTABLISHED)

telnetd     2221     root  1u    inet 0x58b84a68      0t0       TCP   host1.byu.edu:telnet->
                                                              10.0.2.106:1648 (ESTABLISHED)

telnetd     2221     root  2u    inet 0x58b84a68      0t0       TCP   host1.byu.edu:telnet->
                                                              10.0.2.106:1648 (ESTABLISHED)

swremove  3128 root    9u  inet 0x65681268  0t63864       TCP  host1.byu.edu:51948->
                                                              10.0.2.106:6000 (ESTABLISHED)
```

lsof –i

(network connection option)

- lsof –i TCP@10.0.2.106:443

```
COMMAND PID USER  FD   TYPE     DEVICE SIZE/OFF NODE NAME
httpd     12011  www   26u     inet 0x5a043068  0t15354  TCP    host1.byu.edu:443->
                                                              10.0.2.106:1734 (ESTABLISHED)

httpd     12413  www   26u     inet 0x59d46268  0t18916  TCP    host1.byu.edu:443->
                                                              10.0.2.106:1733 (ESTABLISHED)

httpd     18074  www   26u     inet 0x4bc16c68   0t2375   TCP    host1.byu.edu:443->
                                                              10.0.2.106:1749 (ESTABLISHED)
```

lsof –i

(network connection option)

- lsof –i TCP:20-23

```
COMMAND PID  USER  FD  TYPE     DEVICE  SIZE/OFF NODE NAME
sshd        849    root  4u    inet  0x48293c68      0t0      TCP  *:ssh (LISTEN)

sshd:       2008    root  5u    inet 0x4f733668  0t252646    TCP host1.byu.edu:ssh->
                                                  10.0.2.106:1643 (ESTABLISHED)

sshd:       2047     jjp  5u    inet 0x4f733668  0t252646    TCP host1.byu.edu:ssh->
                                                  10.0.2.106:1643 (ESTABLISHED)

telnetd     2221    root  0u    inet 0x58b84a68      0t0      TCP host1.byu.edu:telnet->
                                                  10.0.2.106:1648 (ESTABLISHED)

telnetd     2221    root  1u    inet 0x58b84a68      0t0      TCP host1.byu.edu:telnet->
                                                  10.0.2.106:1648 (ESTABLISHED)

inetd       4910    root  5u    inet 0x482f5468      0t0      TCP *:ftp (LISTEN)

inetd       4910    root  6u    inet 0x482f3a68      0t0      TCP *:telnet (LISTEN)
```

lsof [something] –r [#]
lsof [something] +r [#]

- Repeat mode
  - '-r' is an endless repeat
  - '+r' repeats until an empty interval happens
  - # is the interval you want (default: 15 sec.)
- lsof –i tcp:443 –r 1

```
=======
=======
=======
=======
=======
=======
COMMAND   PID USER   FD TYPE     DEVICE SIZE/OFF NODE NAME
httpd       23591  www   26u    inet 0x500c0068  0t19500    TCP  host1.byu.edu:443->
                                                              10.0.2.106:1814 (ESTABLISHED)
=======
=======
=======
=======
=======
=======
```

lsof

- Other useful options
  - -p [pid]
    - List files for process [pid]
  - -c[name]
    - List files opened by the command [name]
  - -N
    - List open files from an NFS mount
  - -u [userid]
    - List open files by the user userid
  - -a
    - An ‘and’ handle. Lsof defaults to ‘or’ when multiple options are listed

lsof –p [pid]

- Host1: /# lsof -p 4999

```
COMMAND  PID USER   FD   TYPE     DEVICE SIZE/OFF  NODE NAME
serevu  4999 root  cwd   VDIR    64,0x3     1024     2 /
serevu  4999 root  txt   VREG    64,0x5   475136  5664 /opt/CA/
                                                        eTrustAccessControl/bin/serevu
serevu  4999 root  mem   VREG    64,0x8    13281  4734 /usr/lib/tztab
serevu  4999 root  mem   VREG    64,0x8    40960  2043 /usr/lib/libnss_nis.1
serevu  4999 root  mem   VREG    64,0x5    20480  5694 /opt (/dev/vg00/lvol5)
serevu  4999 root  mem   VREG    64,0x8    40960 25964 /usr/lib/libnss_files.1
serevu  4999 root  mem   VREG    64,0x8   282624  4206 /usr/lib/libm.2
serevu  4999 root  mem   VREG    64,0x8   147456   153 /usr/lib/libsec.2
serevu  4999 root  mem   VREG    64,0x8   688128  2042 /usr/lib/libnsl.1
serevu  4999 root  mem   VREG    64,0x8   126976 25689 /usr/lib/libxti.2
serevu  4999 root  mem   VREG    64,0x8    24576 25798 /usr/lib/libdld.2
serevu  4999 root  mem   VREG    64,0x8  1568768 21074 /usr/lib/libc.2
serevu  4999 root  mem   VREG    64,0x8   241664 25796 /usr/lib/dld.sl
serevu  4999 root   0r   VCHR     3,0x2      0t0  2041 /dev/null
serevu  4999 root   1w   VREG    64,0x9   168057  2096 /var/adm/rc.log
serevu  4999 root   2w   VREG    64,0x9   168057  2096 /var/adm/rc.log
serevu  4999 root   3u     inet 0x66f4d468   0t0   TCP localhost:57196->localhost:8891
                                                        (CLOSE_WAIT)
serevu  4999 root 4wW   VREG    64,0x5       31  6156 /opt (/dev/vg00/lvol5)
serevu  4999 root   5w   FIFO    64,0x3   0t7155  2381 / (/dev/vg00/lvol3) wr=0x1bf3
```

lsof –c[name]

- Host1: /# lsof -cinetd

```
COMMAND  PID USER   FD   TYPE     DEVICE SIZE/OFF  NODE NAME
inetd   4910 root  cwd   VDIR    64,0x3     1024     2 /
inetd   4910 root  txt   VREG    64,0x8    57344  2241 /usr (/dev/vg00/lvol8)
inetd   4910 root  mem   VREG    64,0x8    40960  2043 /usr/lib/libnss_nis.1
inetd   4910 root  mem   VREG    64,0x8    13281  4734 /usr/lib/tztab
inetd   4910 root  mem   VREG    64,0x8    40960 25964 /usr/lib/libnss_files.1
inetd   4910 root  mem   VREG    64,0x8   126976 25689 /usr/lib/libxti.2
inetd   4910 root  mem   VREG    64,0x8   688128  2042 /usr/lib/libnsl.1
inetd   4910 root  mem   VREG    64,0x8   147456   153 /usr/lib/libsec.2
inetd   4910 root  mem   VREG    64,0x8    24576 25798 /usr/lib/libdld.2
inetd   4910 root  mem   VREG    64,0x8  1568768 21074 /usr/lib/libc.2
inetd   4910 root  mem   VREG    64,0x8   241664 25796 /usr/lib/dld.sl
inetd   4910 root   0r   VDIR    64,0x3     1024     2 /
inetd   4910 root   1r   VDIR    64,0x3     1024     2 /
inetd   4910 root   2r   VDIR    64,0x3     1024     2 /
inetd   4910 root   3w   FIFO    64,0x3    0t7155  2381 / (/dev/vg00/lvol3) wr=0x1bf3
inetd   4910 root   5u   inet 0x482f5468      0t0   TCP *:ftp (LISTEN)
inetd   4910 root   6u   inet 0x482f3a68      0t0   TCP *:telnet (LISTEN)
inetd   4910 root   7u   inet 0x480a9c68      0t0   TCP *:rsync (LISTEN)
inetd   4910 root  11u   inet 0x482f0068      0t0   TCP *:seosload (LISTEN)
inetd   4910 root  12u   inet 0x4ba8e068      0t0   TCP *:pcm (LISTEN)
```

lsof -N

- Host1: /# lsof -N

```
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sh      12372      jjp  cwd   VDIR   98,0x2     1024        841 /cdrom/Hpux
sh      14213     root  cwd   VDIR   98,0x2     1024        841 /cdrom/Hpux
sh      14245     root   28r  VREG   98,0x2    19569        845 /cdrom/Hpux/
                                                                 install_eAuditClient
sh      14270     root   28r  VREG   98,0x2    19569        845 /cdrom/Hpux/
                                                                 install_eAuditClient
zcat    14271     root    0r  VREG   98,0x2 43697851        844 /cdrom/Hpux/
                                                                 _HPUX11_AC153.63.2.tar.Z
```

lsof –u [userid]

- Host1: /# lsof -u jjp

```
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF    NODE NAME
sshd:    2047  jjp  cwd   VDIR      64,0x3     1024       2 /
sshd:    2047  jjp  txt   VREG      64,0x8  1441792   25216 /usr (/dev/vg00/lvol8)
sshd:    2047  jjp   3u  unix  0x6184ba00      0t0
                                          /var/spool/sockets/pwgr/client2047
sshd:    2047  jjp   4u  unix  0x59b0f200      0t0         ->0x5f601200
sshd:    2047  jjp   5u  inet  0x4f733668 0t252646     TCP host1.byu.edu:ssh->
                                          10.0.2.106:1643 (ESTABLISHED)
sshd:    2047  jjp   6r  PIPE  0x5ba02e08       0 2991581
sshd:    2047  jjp   7w  PIPE  0x5ba02e08       0 2991581
sh       2049  jjp  cwd   VDIR      64,0x4     2048      43 /home/ucs/jjp
sh       2049  jjp  txt   VREG      64,0x8   217088   21110 /usr/bin/sh
hpterm   2055  jjp  cwd   VDIR      64,0x4     2048      43 /home/ucs/jjp
hpterm   2055  jjp  txt   VREG      64,0x8   303104     549 /usr/bin/X11/hpterm
sh      13305  jjp   29u  VREG      64,0x4     3316   10260
                                          /home/ucs/jjp/.sh_history
```

lsof -a

- lsof defaults to an ‘or’
  - Lsof –i tcp:22 –u jjp
    - Lists all ssh connections, All files opened by userid jjp
  - Lsof -a –i tcp:22 –u jjp
    - Lists all ssh connections that are also files opened by userid jjp (All of jjp’s ssh connections.)

lsof -v

- Version

```
Host1: /# lsof -v
lsof version information:
    revision: 4.57
    latest revision: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/
    latest FAQ: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/FAQ
    latest man page: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/lsof_man
    configuration info: /dev/kmem-based, 64 bit HP-UX
    constructed: Wed Nov 28 16:43:43 MST 2001
    constructed by and on: root@host1
    compiler: /bin/cc
    compiler flags: -DHPUXV=1100 -DHASVXFS -
DHPUXKERNBITS=64 -
I/var/opt/lsof_4.57/dialects/hpux/kmem/hpux11 +DD64 -
DHAS_IPC_S_PATCH=2 -I/var/opt/lsof_4.57/dialects/hpux/kmem -
DLSOF_VSTR="B.11.00" -O
    loader flags: -L./lib -llsof  -lelf -lnsl
    system info: HP-UX host1 B.11.00 U 9000/800 573740578 unlimited-
user license
```

lsof

- lsof -?

```
lsof 4.57
 latest revision: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/
 latest FAQ: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/FAQ
 latest man page: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/lsof_man
 usage: [-?abChlnNoOPRstUvV] [-c c] [+|-d s] [+|-D D] [+|-f[cfgGn]]
 [-F [f]] [-g [s]] [-i [i]] [-k k] [+|-L [l]] [-m m] [+|-M] [-o [o]] [-p s]
 [+|-r [t]] [-S [t]] [-T [t]] [-u s] [+|-w] [--] [names]
Defaults in parentheses; comma-separate set (s) items; dash-separate ranges.
  -?|-h list help          -a AND selections (OR)     -b avoid kernel blocks
  -c c  cmd c, /c/[bix]    -C no kernel name cache    +d s  dir s files
  -d s  select by FD set   +D D  dir D tree *SLOW?*   -D D  ?|i|b|r|u[path]
  -i select IPv4 files     -l list UID numbers        -n no host names
  -N select NFS files      -o list file offset        -O avoid overhead *RISKY*
  -P no port names         -R list paRent PID         -s list file size
  -t terse listing         -T disable TCP/TPI info    -U select Unix socket
  -v list version info     -V verbose search          +|-w  Warnings (+)
  -- end option scan
  +f|-f  +filesystem or -file names     +|-f[cfgGn] Ct,Fstr,flaGs,Node
  -F [f] select fields; -F? for help    -k k   kernel symbols (/stand/vmunix)
  +|-L [l] list (+) suppress (-) link counts < l (0 = all; default = 0)
  -m m   kernel memory (/dev/kmem)      +|-M   portMap registration (-)
  -o o   o 0t offset digits (8)         -p s   select by PID set
  -S [t] t second stat timeout (15)     -T qsw TCP/TPI Q,St,Win info (s)
  -g [s] select by process group ID set and print process group IDs
  -i i   select by IPv4 address: [proto][@host|addr][:svc_list|port_list]
  +|-r [t] repeat every t seconds (15); + until no files, - forever
  -u s   exclude(^)|select login|UID set s
  names  select named files or files on named file systems
Anyone can list all files; /dev warnings disabled; kernel ID check enabled.
/.lsof_host1 is the default device cache file read path.
```

tcpdump – dump network traffic

- Wide distribution
  - Available for almost any Unix
  - Binary Depots available direct from HP
- Why tcpdump over nettl?
  - Tcpdump is available on just about any Linux distribution
    - Works the same on HPUX as Linux
    - Easier to limit the output that is displayed

tcpdump – dump network traffic

- Where to get it
  - software.hp.com Internet Express bundle
    - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXIEXP1111
    - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXIEXP1123
  - The HP-UX Porting and Archive Centre
    - http://hpux.cs.utah.edu/hppd/hpux/Networking/Admin/tcpdump-3.8.1/
  - The TCPDUMP group
    - http://www.tcpdump.org/

tcpdump

- Dumps the headers of network packets on a network interface
  - Can save output to a file to look at it later
    - Tcpdump can read from a file's data
  - Tcpdump reports
    - What lan interface it's watching
    - What traffic it sees (headers only)
    - Number of packets received
    - Number of packets dropped

tcpdump

- tcpdump
  - Defaults to lowest numbered interface
- tcpdump –i lanx
  - Listen on the interface named ‘lanx’
- tcpdump -n
  - Don’t convert host names
- tcpdump -N
  - Don’t list domains in output

tcpdump

- Tcpdump –w filename
  - Write output to the file filename.
    - If left for an extended amount of time, this file can get quite large, depending on what you are dumping and how busy the traffic on the interface is
- Tcpdump –r filename
  - Read from the file filename instead of dumping from the interface.
    - This very useful for looking through output on your own time.
    - (Avoid being up in the middle of the night just to watch the traffic…)

tcpdump time formats

- tcpdump –t
  - Suppresses timestamp messages
- tcpdump –tt
  - Gives unformatted timestamp
    - I'm not sure why they did this. It makes the timestamp look very strange.
- tcpdump –ttt
  - Print a delta instead of the timestamp (microseconds)
    - Delta is from the current entry and the one just before it.
    - Very useful in troubleshooting
- tcpdump –tttt
  - Prints date with default time format

tcpdump time formats

- tcpdump -N

  17:12:55.429411 host1.54924 > dnshost.domain: 19809+[|domain] (DF)

- tcpdump –Nt

  host1.54947 > dnshost.domain: 10368+[|domain] (DF)

- tcpdump –Ntt

  1089069262.931359 host1.54961 > dnshost.domain: 53126+[|domain] (DF)

- tcpdump –Nttt
  - 001226 host1.54866 > dnshost.domain: 16888+[|domain] (DF)
  - 000025 dnshost.domain > host1.54866: 16888*[|domain] (DF)

- tcpdump –Ntttt
  - 07/05/2004 23:11:25.986831 host1.54898 > dnshost.domain: 28025+[|domain] (DF)

tcpdump

- tcpdump -v
  - Information like time-to-live, packet length, etc are displayed
- tcpdump –vv
  - Some types of traffic have extra information which is displayed
- tcpdump –vvv
  - Most verbose mode
  - tcpdump displays all information it gets

Tcpdump – selecting what to dump

- The entire packet stream does not have to be dumped as output.
  - You can select the following as options:
    - Host
    - Network
    - Protocol
    - Source/Destination (Traffic direction)
    - Packet Size
    - Others

tcpdump

- host1:/# tcpdump host dnshost

```
tcpdump: listening on lan0
17:32:35.024444 host1.byu.edu.55185 >
  dnshost.byu.edu.domain:  56921+[|domain] (DF)
17:32:35.026725 dnshost.byu.edu.domain >
  host1.byu.edu.55185:  56921* 1/4/4 (187) (DF)
17:32:35.026750 host1.byu.edu.55186 >
  dnshost.byu.edu.domain:  56922+[|domain] (DF)
17:32:35.026770 dnshost.byu.edu.domain >
  host1.byu.edu.55186:  56922*[|domain] (DF)
```

tcpdump

```
host1:/# tcpdump net 10.0
  tcpdump: listening on lan0
  17:35:17.906795 10.0.2.106.4165 > host1.byu.edu.22: ack
    2476146254 win 65424 (DF)
  17:35:17.909105 host1.byu.edu.22 > 10.0.2.106.4165: P
    1:113(112) ack 0 win 32768 (DF) [tos 0x10]
  17:35:18.106435 10.0.2.106.4165 > host1.byu.edu.22: . ack
    113 win 65312 (DF)
  17:35:18.106461 host1.byu.edu.22 > 10.0.2.106.4165: P
    113:385(272) ack 0 win 32768 (DF) [tos 0x10]
  17:35:18.306907 10.0.2.106.4165 > host1.byu.edu.22: . ack
    385 win 65040 (DF)
```

tcpdump

```
host1:/# tcpdump port 23
  tcpdump: listening on lan0
  17:37:17.945650 10.0.2.106.4260 > host1.byu.edu.telnet: P
    2152884493:2152884494(1) ack 2658367462 win 65007
    (DF)
  17:37:17.948096 host1.byu.edu.telnet > 10.0.2.106.4260: P
    1:2(1) ack 1 win 32768 (DF)
  17:37:18.152553 10.0.2.106.4260 > host1.byu.edu.telnet: P
    1:2(1) ack 2 win 65006 (DF)
  17:37:18.152582 host1.byu.edu.telnet > 10.0.2.106.4260: P
    2:3(1) ack 2 win 32768 (DF)
```

tcpdump

host1:/# tcpdump tcp port 1721

tcpdump: listening on lan0

17:42:31.136690 host2.byu.edu.caicci > host1.byu.edu.49409: P 84473981:84474457(476) ack 1468071918 win 32768 (DF)

17:42:31.176023 host2.byu.edu.caicci > host1.byu.edu.49409: . 476:1904(1428) ack 1 win 32768 (DF)

17:42:31.176707 host1.byu.edu.49409 > host2.byu.edu.caicci: . ack 1904 win 32768 (DF)

17:42:31.176728 host2.byu.edu.caicci > host1.byu.edu.49409: P 1904:2380(476) ack 1 win 32768 (DF)

tcpdump

- host1:/# tcpdump dst host 10.0.2.106
  - tcpdump: listening on lan0
  - 17:45:28.063628 host1.byu.edu.22 > 10.0.2.106.4165: P 2476213406:2476213518(112) ack 1821731655 win 32768 (DF) [tos 0x10]
  - 17:45:28.262897 host1.byu.edu.22 > 10.0.2.106.4165: P 112:272(160) ack 1 win 32768 (DF) [tos 0x10]
  - 17:45:28.461418 host1.byu.edu.22 > 10.0.2.106.4165: P 272:416(144) ack 1 win 32768 (DF) [tos 0x10]
- host1:/# tcpdump src host 10.0.2.106
  - tcpdump: listening on lan0
  - 17:46:11.499115 10.0.2.106.4165 > host1.byu.edu.22: . ack 2476215374 win 65232 (DF)
  - 17:46:11.699597 10.0.2.106.4165 > host1.byu.edu.22: . ack 113 win 65120 (DF)
  - 17:46:11.900602 10.0.2.106.4165 > host1.byu.edu.22: . ack 241 win 64992 (DF)

tcpdump – packet size

- host1:/# tcpdump less 64
  - tcpdump: listening on lan0
  - 17:50:31.534576 10.0.2.106.4165 > host1.byu.edu.22: . ack 2476239806 win 64656 (DF)
  - 17:50:31.636342 802.1d config 8000.00:09:43:54:12:34.8060 root 1fff.00:d0:01:67:b7:34 pathcost 4 age 1 max 20 hello 2 fdelay 15
  - 17:50:31.736652 10.0.2.106.4165 > host1.byu.edu.22: . ack 113 win 64544 (DF)
  - 17:50:31.835677 arp who-has host1.byu.edu tell listen.byu.edu
  - 17:50:31.836912 arp reply host1.byu.edu is-at 0:30:6e:4b:15:3c
- host1:/# tcpdump greater 192
  - tcpdump: listening on lan0
  - 17:52:15.268316 host1.byu.edu.22 > 10.0.2.106.4165: P 2476247838:2476248126(288) ack 1821749655 win 32768 (DF) [tos 0x10]
  - 17:52:15.270638 dnshost.byu.edu.domain > host1.byu.edu.55664: 39802*[|domain] (DF)
  - 17:52:15.271726 dnshost.byu.edu.domain > host1.byu.edu.55665: 39803*[|domain] (DF)

tusc – trace unix system calls

Where to get it

- http://hpux.cs.utah.edu/hppd/hpux/Sysadmin/tusc-7.5/
  - The HP-UX Porting and Archive Centre
  - HPUX 11.0 and HPUX 11.23 binaries
  - HPUX Source

tusc – trace unix system calls

- Trace the system calls a process makes
- Trace the signals a process gets
- Attach to live processes by giving the process pid.
  - host1:/# tusc 459
  - (Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit])
  - select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
  - select(8, 0x77ff1550, NULL, NULL, NULL) ..... = 1
  - read(3, "< 1 3 > J u l 5 1 8 : 1 1 ".., 2048) ..... = 2048
  - sigblock(0x2001) ..... = 0
  - time(0x77ff1e88) ..... = 1089072668
  - writev(10, 0x77ff1e90, 6) ..... = 44
  - writev(12, 0x77ff1e90, 6) ..... = 44
  - sigsetmask(NULL) ..... = 8193
  - select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]

tusc

- Trace the system calls a process makes
- Trace the signals a process gets
- Run and trace a process by giving it's name.

```
host1:/# tusc /usr/bin/bdf
execve("/usr/bin/bdf", 0x7805e5b8, 0x7805e5c0) ..... = 0 [32-bit]
utssys(0x780575d0, 0, 0) ..... = 0
open("/usr/lib/dld.sl", O_RDONLY, 051274) ..... = 3
read(3, "02\v010e0512@ \0\0\0\0\0\0\0\0"., 128) ..... = 128
lseek(3, 128, SEEK_SET) ..... = 128
read(3, "10\0\004\0\0\0( \002\aL \0\0\0\0"., 48) ..... = 48
mmap(NULL, 132940, PROT_READ|PROT_EXEC, MAP_SHARED, 3, 0x9000) = 0xc0010000
mmap(NULL, 14584, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE, 3, 0x2a000) = 0x77fec000
close(3) ..... = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE|MAP_ANONYMOUS, -1, NULL) = 0x77fea000
sysconf(_SC_CPU_VERSION) ..... = 532
open("/opt/graphics/OpenGL/lib/libogltls.sl", O_RDONLY, 0) ERR#2 ENOENT
open("/usr/lib/libc.2", O_RDONLY, 0) ..... = 3
…
…
/dev/vg00/lvol9    1032192  255850  727844   26% /opt/unicenter
write(1, "/ d e v / v g 0 0 / l v o l 9   "., 64) ..... = 64
open("/opt/u01", O_RDONLY, 0134214) ..... = 4
fstatfs(4, 2013615948) ..... = 0
close(4) ..... = 0
/dev/vg00/lvol8    1572864  867368  661462   57% /opt/u01
write(1, "/ d e v / v g 0 0 / l v o l 8   "., 58) ..... = 58
open("/opt/prod", O_RDONLY, 0134214) ..... = 4
fstatfs(4, 2013615948) ..... = 0
close(4) ..... = 0
/dev/vg00/lvol17   10240000 1027672 8924460   10% /opt/prod
write(1, "/ d e v / v g 0 0 / l v o l 1 7 "., 60) ..... = 60
open("/home", O_RDONLY, 0134214) ..... = 4
fstatfs(4, 2013615948) ..... = 0
close(4) ..... = 0
/dev/vg00/lvol4     114688    2648  111216    2% /home
write(1, "/ d e v / v g 0 0 / l v o l 4   "., 55) ..... = 55
read(3, 0x40003700, 32768) ..... = 0
close(3) ..... = 0
exit(0) ..... WIFEXITED(0)
```

tusc - options

- tusc has a number of options:
  - tusc -o filename — write to a file
  - tusc -oa filename — append to the file
  - tusc –c — count syscalls & signals
  - tusc –C — count & give average times
  - tusc –f — follow forks
  - tusc –i — Don’t show sleeping syscalls
  - tusc –k — Wait for all children to exit
  - tusc –n — Print process names
  - tusc –p — Print pids
  - tusc –s syscalls — Select syscalls
  - tusc –S signals — Select signals
  - tusc –X — Print in exportable format
  - tusc –z — Print failed syscalls

tusc – output to a file

- tusc –o /tmp/tusc.out
  - The output of the tusc command is dumped into the file /tmp/tusc.out
  - Useful for when you don't have the brainpower to see everything fly by, or don't have time to look just then, or need the output to send to a vendor
- tusc –oa /tmp/tusc.out
  - The output of tusc will be appended to the file /tmp/tusc.out

tusc

- host1:/# tusc 459

```
( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... = 1
read(3, "< 1 3 > J u l   1 0   0 9 : 5 7 ".., 2048) ..... = 2048
sigblock(0x2001) ..... = 0
time(0x77ff1e88) ..... = 1089475076
writev(10, 0x77ff1e90, 6) ..... = 46
writev(12, 0x77ff1e90, 6) ..... = 46
sigsetmask(NULL) ..... = 8193
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
( Detaching from process 459 ("/usr/sbin/syslogd -D") )
```

- host1:/# tusc -X 459

```
( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
select  (8, 0x77ff1550, NULL, NULL, NULL) [sleeping]
select  (8, 0x77ff1550, NULL, NULL, NULL)       1
read    (3, "< 1 3 > J u l   1 0   0 9 : 5 8 ".., 2048) 2048
sigblock        (0x2001)        0
sigsetmask      (NULL)  8193
  Received signal 14    SIGALRM, in select(), [caught], no siginfo
select  (8, 0x77ff1550, NULL, NULL, NULL)       ERR#4 EINTR
alarm   (120)   0
select  (8, 0x77ff1550, NULL, NULL, NULL) [sleeping]
( Detaching from process 459 ("/usr/sbin/syslogd -D") )
```

tusc -c

- tusc -c
  - Quite easily the most useful part of the tool
  - Count syscalls a process makes
- host1:/# tusc -c 459

```
( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
( Detaching from process 459 ("/usr/sbin/syslogd -D") )
Syscall              Seconds      Calls     Errors
read                  0.00         15
time                   0.00         2
select                 0.00        15
sigblock              0.00         15
sigsetmask            0.00         15
writev                 0.00         3
-----                  -----       -----
Total                 0.00         65
```

tusc -cc

```
host1:/# tusc -cc 459
   ( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
     select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
     select(8, 0x77ff1550, NULL, NULL, NULL) ..... = 1
     read(3, "< 1 3 > J u l  1 0  1 0 : 0 6 ".., 2048) ..... = 2048
     sigblock(0x2001) ..... = 0
     time(0x77ff1e88) ..... = 1089475590
     writev(10, 0x77ff1e90, 6) ..... = 46
     writev(12, 0x77ff1e90, 6) ..... = 46
     sigsetmask(NULL) ..... = 8193
     select(8, 0x77ff1550, NULL, NULL, NULL) ..... = 1
     read(3, "< 1 3 > J u l  1 0  1 0 : 0 6 ".., 2048) ..... = 2048
     sigblock(0x2001) ..... = 0
     sigsetmask(NULL) ..... = 8193
     select(8, 0x77ff1550, NULL, NULL, NULL) ..... = 1
     read(3, "< 1 3 > J u l  1 0  1 0 : 0 6 ".., 2048) ..... = 2048
     sigblock(0x2001) ..... = 0
     sigsetmask(NULL) ..... = 8193
     select(8, 0x77ff1550, NULL, NULL, NULL) ..... = 1
     read(3, "< 2 7 > J u l  1 0  1 0 : 0 6 ".., 2048) ..... = 2048
     sigblock(0x2001) ..... = 0
     sigsetmask(NULL) ..... = 8193
     select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
     …
     ( Detaching from process 459 ("/usr/sbin/syslogd -D") )
     Syscall              Seconds      Calls     Errors
     read                    0.00          7
     time                    0.00          1
     select                  0.00          7
     sigblock                0.00          7
     sigsetmask              0.00          7
     writev                  0.00          2
     -----                   -----       -----
     Total                   0.00         31
```

tusc -C

- tusc -C
  - Count syscalls a process makes, give average times
- host1:/# tusc -C 459

```
( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
( Detaching from process 459 ("/usr/sbin/syslogd -D") )
Syscall       Seconds   Calls  Errors      Low         High      Average
read           0.0002      18       0   0.000007    0.000013    0.000010
time           0.0000       1       0   0.000005    0.000005    0.000005
select         0.0005      18       0   0.000018    0.000030    0.000025
sigblock       0.0001      18       0   0.000004    0.000011    0.000008
sigsetmask     0.0001      18       0   0.000004    0.000009    0.000006
writev         0.0000       2       0   0.000010    0.000024    0.000017
-----          -----      -----
Total          0.0009      75
```

tusc – follow fork

- tusc –f
  - tusc will by default only follow the parent process, and ignore fork'ed processes
  - This option follows all children
- tusc –k
  - Tusc will continue to trace until all children finish
  - Parent forks children, then exits, tusc will continue to watch children
    - This is not the default behavior for some reason

tusc

- tusc –i
  - Don't show sleeping syscalls
- berrien:/# tusc -c 459

```
( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
( Detaching from process 459 ("/usr/sbin/syslogd -D") )
Syscall              Seconds      Calls      Errors
read                  0.00          10
select                0.00          10
sigblock              0.00          10
sigsetmask            0.00          10
-----                 -----         -----
Total                 0.00          40
```

- berrien:/# tusc -ic 459

```
( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
( Detaching from process 459 ("/usr/sbin/syslogd -D") )
Syscall              Seconds      Calls      Errors
read                  0.00          12
time                  0.00           3
select                0.00          12
sigblock              0.00          12
sigsetmask            0.00          12
writev                0.00           6
-----                 -----         -----
Total                 0.00          57
```

tusc

- tusc –p
  - Print process ids
  - Useful when tracing more than one thing at a time

```
host1:/# tusc -p 459
   ( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
   [459] select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
   [459] select(8, 0x77ff1550, NULL, NULL, NULL) ..... = 1
   [459] read(3, 0x77ff04e0, 2048) ..... ERR#11 EAGAIN
   [459] sigblock(0x2001) ..... = 0
   [459] time(0x77ff16c8) ..... = 1089479152
   [459] writev(10, 0x77ff16d0, 6) ..... = 78
   [459] writev(12, 0x77ff16d0, 6) ..... = 78
   [459] sigsetmask(NULL) ..... = 8193
   [459] select(8, 0x77ff1550, NULL, NULL, NULL) ..... [sleeping]
   ( Detaching from process 459 ("/usr/sbin/syslogd -D") )
```

tusc

- tusc –n 459

```
( Attached to process 459 ("/usr/sbin/syslogd -D") [32-bit] )
[/usr/sbin/sy] select(8, 0x77ff1550, NULL, NULL, NULL) ... [sleeping]
( Detaching from process 459 ("/usr/sbin/syslogd -D") )
```

- tusc -n df -k /

```
[df -k /     ] execve("/usr/bin/df", 0x7802e4fc, 0x7802e50c) = 0 [32-bit]
[df -k /     ] utssys(0x78006d90, 0, 0) ..... = 0
[df -k /     ] open("/usr/lib/dld.sl", O_RDONLY, 045174) . = 3
[df -k /     ] read(3, "02\v010e0512@ \0\0\0\0\0\0\0\0\0".., 128) = 128
[df -k /     ] lseek(3, 128, SEEK_SET) ..... = 128
[df -k /     ] read(3, "10\0\004\0\0\0( \002\aL \0\0\0\0".., 48) = 48
…
[df -k /     ] ioctl(1, TCGETA, 0x78005678) ..... = 0
/                    (/dev/vg00/lvol3       ) :   520920 total allocated Kb
[df -k /     ] write(1, "/                          "., 78) = 78
                                              435744 free allocated Kb
[df -k /     ] write(1, "                            "., 77) = 77
                                               85176 used allocated Kb
[df -k /     ] write(1, "                            "., 77) = 77
                                                 16 % allocation used
[df -k /     ] write(1, "                            "., 77) = 77
[df -k /     ] exit(0) ..................................... WIFEXITED(0)
```

tusc

- tusc –s *syscall*
  - Trace specific syscalls
  - You can also choose to ignore specific syscalls

- tusc –S *signals*
  - Trace specific signals
  - You can also ignore specific signals

Questions

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP