



# Troubleshooting

Stephen Bee



**All trademarks used herein are  
the sole property of their  
respective owners.**



# Managing the system from the CLI



**Backup before modifying!**



## Paths To Etch Into Your Brain

»» `/usr/local/cpanel/logs`

»» `/scripts`

»» `/var/cpanel`



# Managing Accounts



# Creating a cPanel Account

**`/scripts/wwwacct example.com user pass`**

- Execute with no arguments to view full usage
- Removal can be performed with **`/scripts/killacct user`**



# Post Creation Customizations

## **/scripts/postwwwacct**

```
#!/bin/bash
```

```
/scripts/addpop some-user@$1 password  
perl -pi -e 's/LANG=.* /LANG=swahili/g' /var/cpanel/users/  
$2
```

- **/scripts/postwwwacct** is called when account creation is completed
- Can be any language, just needs to exist and be executable



## Creating an E-mail Account

```
/scripts/addpop user@example.com pass
```

➤➤ The mail user gets defined in:

- **/home/user/etc/example.com/passwd**
- **/home/user/etc/example.com/shadow**

➤➤ The mail user data directory exists at:

- **/home/user/mail/example.com/user**



# Modifying Account Parameters

»» `/var/cpanel/users/username`

»» Changes can be made on the fly

## Frequently Abused Settings

- »» **RS** – The user's theme
- »» **PLAN** – The user's package
- »» **MAX\*** - Number of allowed items
- »» **DNS** – The user's primary domain

```
DNS=domain.com
RS=x3
OWNER=root
MAXFTP=unlimited
HASCGI=1
MAXSUB=unlimited
MAXSQL=unlimited
MAXPOP=unlimited
MAXLST=unlimited
MAXPARK=0
MAXADDON=0
FEATURELIST=default
PLAN=default
```



# User to Domain Associations

## Relevant Paths

- » `/etc/trueuserdomains`
- » `/etc/userdomains`
- » `/etc/trueuserowners`

## `/etc/userdomains`

```
example.com: owner
*.example.com: wildcard
sub.example.com: owner
*: nobody
```

## Useful Information

- » Managed by `/scripts/updateuserdomains`
- » Should never be modified directly
- » `/etc/trueuserowners` creates reseller to user associations



# Modifying User Quotas

**`/scripts/editquota username 1024M`**

- »» Calls the system's quota utilities to set user quotas
- »» Stores quota definitions in **`/etc/quota.conf`**

## Related Scripts

- »» **`/scripts/fixquotas`** - rebuild the system quota databases
- »» **`/scripts/initquotas`** - initialize with quota.conf values



# Suspending an Account

**`/scripts/suspendacct username`**

- »» Suspends access to all services but **inbound** e-mail
- »» Creates an empty file at **`/var/cpanel/suspended/user`**
- »» Locks all logins by modifying password hashes
- »» Denies HTTP traffic through an .htaccess based redirect
- »» **`/scripts/unsuspendacct user`** will unsuspend a user



# Managing and Monitoring Services



## Restarting Services

**`/scripts/restartsv_[servicename]`**

**`/scripts/restartsv_httpd`**



## Disabling Services

```
touch /etc/${service_name}disable
```

```
touch /etc/eximdisable
```

➤➤ Can also be done in WHM -> Service Manager

```
➤➤ grep --color '\etc\.*disable' /scripts/restartsrv_*
```



# Monitoring Services

**`/usr/local/cpanel/libexec/chkservd`**

## Associated Components

**`>>> /etc/init.d/chkservd`**

**`>>> /etc/chkserv.d/*`**

**`>>> /var/run/chkservd/*`**



# Configuring chkservd

**/etc/chkservd.d/chkservd.conf**

➤➤ Configured from **WHM -> Service Manager**

➤➤ Restart required for manual changes to take effect

## Example Configuration

```
cpsrvd:1  
exim:1  
httpd:0
```



# TCP Based Monitoring

**service[SERVICE]=port, SEND, EXPECT, COMMAND**

```
root@host [~]# cat /etc/chkserv.d/imap
service[imap]=143,A001 LOGOUT,\\*\sOK,/scripts/restartsrv_imap
root@host [~]#
```



# Process Based Monitoring

**service[SERVICE]=x,x,x, COMMAND, USER, PROCESS**

```
root@host [~]# cat /etc/chkserv.d/tomcat
service[tomcat]=x,x,x,/scripts/restartsrv_tomcat,tomcat,tomcat
root@host [~]#
```



# The chkserverd log

**`/var/log/chkserverd.log`**

```
[Thu May 8 10:12:02 2008] Service check ....cpsrvd [+]....named [+]...tomcat [+]...Done
[Thu May 8 10:20:26 2008] Service check ....cpsrvd [+]...named [+]...tomcat [+]...Done
[Thu May 8 10:56:17 2008] Service check ....cpsrvd [+]...exim [+]...httpd [-Notification =>
admin@example.com via EMAIL [level => 1]
Restarting httpd....]...mysql [+]...named [+]...tomcat [+]...Done
```

➤ Can be used to determine frequency of reported failures

– `egrep 'exim \[-' /var/log/chkserverd.log`



# Managing Updates



## When should you update?

»» /usr/local/cpanel/cpanel -V

```
# /usr/local/cpanel/cpanel -V  
11.23.3-CURRENT_25049  
#
```

»» <http://changelog.cpanel.net/>



# Updating cPanel

**`/scripts/upcp [--force]`**

## Associated Components

»» `/scripts/uptdatenow`

»» `/scripts/sysup`

»» `/scripts/rpmup`

»» <http://httpupdate.cpanel.net/cpanelsync/>



# Updating Individual Services

`/scripts/{service_name}up`

## Associated Components

➤➤ /scripts/ft pup

➤➤ /scripts/courierup

➤➤ /scripts/mysqlup

➤➤ /scripts/eximup

➤➤ /scripts/bandminup



# Configuring Updates

**`/etc/cpupdate.conf`**

## Example Configuration

```
CPANEL=current  
RPMUP=manual  
SYSUP=manual  
BANDMINUP=inherit  
COURIERUP=never
```

```
MYSQLUP=inherit  
PYTHONUP=inherit  
EXIMUP=inherit  
FTPUP=inherit
```

# Update Hooks

**`/scripts/post{service_name}up`**  
**`/scripts/pre{service_name}up`**

## Associated Components

**`>>> egrep --color '\scripts\post.*up' /scripts/*`**

**`>>> egrep --color '\scripts\pre.*up' /scripts/*`**

**`>>> /scripts/preupcp`**

**`>>> /scripts/postupcp`**



# Determining and Debugging Process Behaviour



# Determine Where a Process is Listening

## netstat -lnp

Active Internet connections (only servers)						
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:2082	0.0.0.0:*	LISTEN	13469/cpsrvd - wait
tcp	0	0	0.0.0.0:2083	0.0.0.0:*	LISTEN	13469/cpsrvd - wait

## lsof -i

couriertc	2621	root	3u	IPv6	5356	TCP *:pop3s (LISTEN)
pure-ftpd	2755	root	4u	IPv4	5834	TCP *:ftp (LISTEN)
pure-ftpd	2755	root	5u	IPv6	5835	TCP *:ftp (LISTEN)
httpd	10026	nobody	5u	IPv4	17287854	TCP *:http (LISTEN)



## Determining a Process's Network Activity

**tcpdump -n dst port \${PORT} and src host \${YOUR\_IP}**  
**tcpdump -n dst port 80 and src host 10.0.0.2**

```
# tcpdump -qn dst port 80 or src port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13:50:40.048015 IP 192.168.1.102.59902 > 192.168.1.10.http: tcp 0
13:50:40.048098 IP 192.168.1.10.http > 192.168.1.102.59902: tcp 0
13:50:40.048850 IP 192.168.1.102.59902 > 192.168.1.10.http: tcp 0
```



# File Activity



# lsof

lsof -c COMM

lsof -p PID

lsof /path/to/mount\_point

```
# lsof /tmp
COMMAND  PID  USER  FD  TYPE  DEVICE  SIZE  NODE NAME
postmaste 18250 postgres 3u  unix 0xf5214480 11630097 /tmp/.s.PGSQL.5432
mysqld 22873 mysql 6u  REG  7,0 0 10164 /tmp/ibyE8Pwd (deleted)
mysqld 22873 mysql 7u  REG  7,0 0 10165 /tmp/ibzOYVZe (deleted)
mysqld 22873 mysql 11u  REG  7,0 0 10167 /tmp/ibGYNAEg (deleted)
```



# Using Debuggers



## bash debug mode

**bash -x /path/to/bash/script.sh**

**bash -x /etc/init.d/mysql restart**

- Helpful for determining arguments passed from init scripts
- [http://tldp.org/LDP/Bash-Beginners-Guide/html/sect\\_02\\_03.html](http://tldp.org/LDP/Bash-Beginners-Guide/html/sect_02_03.html)

```
+ echo -n 'Starting MySQL'  
Starting MySQL+ test -x /usr/sbin/mysqlmanager -a 1 = 0  
+ test -x /usr/bin/mysqld_safe  
+ pid_file=/var/lib/mysql/server.hostname.com.pid  
+ /usr/bin/mysqld_safe --datadir=/var/lib/mysql --pid-file=/var/lib/mysql/server.hostname.com.pid
```



## **gdb**

- » Useful for troubleshooting segmentation faults and core dumps
- » <http://httpd.apache.org/dev/debugging.html>

**gdb /path/to/binary [core.file]**

**gdb /usr/local/apache/bin/httpd httpd.core.3946**



**strace ... the final frontier**



## What is strace?

- Traces system calls made by supplied process or command
- Available with any Linux distribution, and FreeBSD



## Installing strace

»» /scripts/ensurerpm strace

»» <http://sourceforge.net/projects/strace/>



# Performing Your First strace

`strace touch test.file`



# Understanding the Output

## Typical System Call

```
execve("/bin/touch", ["touch", "test.file"], [/* 26 vars */]) = 0
```

## Typical Error Response

```
open("test.file", O_WRONLY|O_CREAT, 0666) = -1 EACCES (Permission denied)
```

## Useful man pages

- syscalls
- [errno.h](#)



## Storing strace output to file

```
strace -o ~/strace.out touch test.file
```

## Turning up the volume

```
strace -v -o ~/strace.out touch test.file
```

```
strace -v -s 4096 -o ~/strace.out touch test.file
```

➤➤ Prints out valuable environment information

➤➤ Increased buffers prevent truncating of valuable information



## Attaching to an existing process

```
strace -v -o ~/strace.cpsrvd -p `cat /var/run/cpsrvd.pid`
```

- Multiple PIDs can be specified
- Useful for troubleshooting services
- You can break out of the trace by pressing **Control - C**



## Follow that fork!

```
strace -v -o trace.out -Ff -p `cat /var/run/cpsrvid.pid`
```

➤➤ '-f' will cause strace to follow child processes called by fork()

➤➤ '-F' will cause strace to follow processes called by vfork()



## Getting precisely what you want

```
strace -vFf -o trace.out -e execve -p `cat /var/run/cpsrvd.pid`
```



## File Operations

**strace -e trace=file touch test.file**

```
execve("/bin/touch", ["touch", "test.file"], [/* 26 vars */]) = 0
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY) = 3
open("/lib/tls/librt.so.1", O_RDONLY) = 3
open("/lib/tls/libc.so.6", O_RDONLY) = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/usr/lib/locale/locale-archive", O_RDONLY|O_LARGEFILE) = 3
open("test.file", O_WRONLY|O_CREAT|O_NOCTTY|O_NONBLOCK|O_LARGEFILE, 0666) = 3
utime("test.file", NULL) = 0
```



## Process Operations

**strace -Ff -e trace=process sh -c 'touch test.file'**

```
execve("/bin/sh", ["sh", "-c", "touch test.file"], [/* 26 vars */]) = 0  
execve("/bin/touch", ["touch", "test.file"], [/* 26 vars */]) = 0  
exit_group(0)
```



# Network Operations

**strace -e trace=network /usr/local/cpanel/cpkeyclt**

```
socket(PF_FILE, SOCK_STREAM, 0) = 5
connect(5, {sa_family=AF_FILE, path="/var/run/nscd/socket"}, 110) = -1 ENOENT (No such file or directory)
socket(PF_FILE, SOCK_STREAM, 0) = 5
connect(5, {sa_family=AF_FILE, path="/var/run/nscd/socket"}, 110) = -1 ENOENT (No such file or directory)
socket(PF_INET, SOCK_DGRAM, IPPROTO_UDP) = 5
Updating Internal cPanel Information.....--- SIGCHLD (Child exited) @ 0 (0) ---
.Done
```



# Isolating the Errors



## Using -c to display error frequency

`touch immutable.file && chattr +i immutable.file && strace -c touch immutable.file`

```
touch: cannot touch `immutable.file': Permission denied
% time   seconds  usecs/call   calls   errors syscall
-----  -
91.49    0.003945    3945         1         execve
 8.51    0.000367     61         6         fstat64
 0.00    0.000000     0          5         read
 0.00    0.000000     0          4         write
 0.00    0.000000     0         19         13 open
 0.00    0.000000     0          8         close
 0.00    0.000000     0          1         1 access
-----  -
100.00   0.004312                    76        15 total
```



## Isolating the Affected System Calls

**strace -e access,open touch immutable.file**

```
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY) = 3
open("/lib/librt.so.1", O_RDONLY) = 3
open("/lib/libc.so.6", O_RDONLY) = 3
open("/lib/libpthread.so.0", O_RDONLY) = 3
open("immutable.file", O_WRONLY|O_CREAT, 0666) = -1 EACCES (Permission denied)
touch: cannot touch `immutable.file': Permission denied
Process 2102 detached
```



## Other Commands to Isolate Affected Calls

- `egrep '= -1' trace.out`
- `cat trace.out | awk '$2 ~ /-1/ { print substr($1,0,index($1,"(")-1) "\t" $2 } FS="=" | sort | uniq -c`

```
1 access -1 ENOENT (No such file or directory)\n1 open -1 EACCES (Permission denied)
```



# Permissions Errors

**Search for EPERM or EACCES**

## Why this could happen

- »» File permissions, or the permissions on any directory leading up to that file are forbidding that user/group from accessing it.

## Supplemental Information

- »» Do a back search from point of error for setuid/setgid calls



# Everyday Commands



# Tracing cPanel

```
strace -vFf -s 4096 -o /root/strace.cpsrvd -p `cat /var/run/cpsrvd.pid`
```

## What does this do?

- »» Attaches to the PID stored in `/var/run/cpsrvd.pid`
- »» Stores output in `/root/strace.cpsrvd`

# Tracing Apache

```
strace -vFf -s 4096 -o /root/strace.httpd $(ps -C httpd h | awk ' { print "-p " $1 }')
```

## What does this do?

➤➤ Forms an argument list for Apache using a bash subshell

```
# echo $(ps -C httpd h | awk ' { print "-p " $1 }')  
-p 23241 -p 23243 -p 23244 -p 23245 -p 23246 -p 23247 -p 24155  
#
```

➤➤ Stores strace output in **/root/strace.httpd**



## Determining What a Process Executes

```
strace -vFf -s 4096 -e execve -p `cat /var/run/cpsrvd.pid` 2>&1 |  
awk '$0 ~ /execve\(\/ { print $3 }' FS="["
```

## Example Output from WHM -> Show Current Running Processes

```
"/usr/local/cpanel/whostmgr/bin/whostmgr2", "./top"],  
"ps", "-eo", "pid,user,nice,pmem,pcpu,command"],  
"ps", "-eo", "pid,user,nice,pmem,pcpu,command"],
```



# Tracing Randomly Dying Processes

```
strace -vFf -s 4096 -e trace=signal $(ps -C exim h | awk '{ print "-p " $1 }')
```

## Example Output

```
[pid 15422] --- SIGCHLD (Child exited) @ 0 (0) ---  
[pid 15422] rt_sigaction(SIGCHLD, {SIG_DFL}, NULL, 8) = 0  
[pid 15422] sigreturn() = ? (mask now [])  
[pid 15422] rt_sigaction(SIGCHLD, {0x805dbea, [], SA_RESTORER, 0x279a98},  
NULL, 8) = 0  
[pid 15416] +++ killed by SIGKILL +++  
[pid 15422] +++ killed by SIGKILL +++
```



**Q & A**