1. **mysql error in Cpanel**  
   /scripts/autorepair fix\_mariadb\_show\_grants\_roles
2. **AWS restoration**mkdir /restore

mounting attached drive to restore foldet  
mount -o nouuid /dev/nvme2n1p1 /restore

cd /restore

 ll | grep auau3514

 mv /restore/auau3514 .

 umount /restore/

lsof | grep /restore  
fuser -cuk /restore

===

if restore process is in awcp666

**tar the account**

**==**

**if mounted in same server**

**to copy public html to the account**

**in restores >>thth3689**

**give this command to copy public\_html to thth3689**

**cp -ar public\_html /home/thth3689**

to start new session which will not close  
 screen -S ARQ-389

to go into  session

 screen -r ARQ-389  
  
to see session

 screen -ls  
  
to go out  of session  
ctrl +AD

**3)find**

grep -lr gtag \*

grep -lr keyword \*

find / -name my.cnf

to find post directory in a path

find /websites/sp/spherepr.com.au -type d -name post

4) **Google decetive page**

1)   
<https://search.google.com/search-console?hl=en&utm_source=wmx&utm_medium=deprecation-pane&utm_content=home&resource_id=https://progressmining.com.au/>2)  
<https://prnt.sc/vqwamr>

3) <https://prnt.sc/vqwash>

4) create file under public html and then verfiy  
5) will take 20 hrs

5) **Cpanel Restore steps**

goto bne shell  
- ssh restores@gsx-0001aweb.server-web.com  
-enter  password 1w4n7myr3570r3  
 goto path  
e.g cd /opt/restore/restores/restore\_id\_3265

move the files to new server  
 scp cpmove-kckc1228.tar.gz anitin@cp345.ezyreg.com:/home/anitin/

entergosa password (bne shell password)

=======================

In the new server of cpanel

cd /home/anitin/  
ls -la

**un tar file**

 tar -xzvf cpmove-kckc1228.tar.gz  
 cd cpmove-kckc1228  
 ls -la  
 cd homedir  
 cd public\_html/

remove the account if there are no files(conditions apply)  
 /scripts/removeacct kckc1228

 mv cpmove-kckc1228.tar.gz /home/  
 /scripts/restorepkg kckc1228

===  
1: check if cpanel account is accesssible  
2: check if reseller account is created

====

**to find backup in the server**

[root@cp454 ~]# cd backups/cp454.ezyreg.com  
ll | grep alal3111

===

cp454  
cd *backups/cp454.ezyreg.com*  
ll | grep alal3111

**move to htdocs folder of the same old server**  
cp backups/cp454.ezyreg.com/cpmove-alal3111.tar.gz  /usr/local/apache/htdocs

**new server** awcp012

**goto account**  
cd ~alal3111/pubic\_html/

**get the backup from old server to new server**  
wget cp454.ezyreg.com/cpmove-alal3111.tar.gz

**untar the tar file**  
/scripts/restorepkg cPanel-user --force cpmove.tar.gz

====

**Akshay method easy method**

==

**In new cp server**

cd /home/anitin/  
scp restores@gsx-0001aweb.server-web.com:/opt/restore/restores/restore\_id\_3271/\* /home/anitin

1w4n7myr3570r3

**mail   rsync**

mkdir test  
 mv rere2453\_mail.tar.gz test/  
cd test/  
 tar -xzvf rere2453\_mail.tar.gz

**2 -3 steps are still there ask someone**

 rsync -azvh \* /home/rere2453/mail/redlondonbus.com.au/sergio/

==

 rsync -azvh  /home/sales/  /home/envirocy/mail/envirocyclensw.com.au/sales/

enter password of restores  
 /scripts/restorepkg gege8648 --force cpmove-gege8648.tar.gz

==

cat /var/cpanel/users/wwww3255  | grep OWNER

ok it's not under any reseller and cPanel service is already cancelled for it.. terminate it

**6)Webmail issue  
Webmail issue**

**cloud server**

    -log into  automation server

    -    find user

**webmail opening error**  
remove dovecot.index and dovecot-uidlist

==

console and mr coffee password for mail  should be same

    update in console APP support will be doing

Backups in  
/clientmail/mail-1/.snapshot/

cd /clientmail/mail-1/s/y/sydneywestbiz.com.au

**to give permissions**

chown webmail:mail admin -R

    ==

**Tail Syslog for cloud server accounts**

  log into**ssh syslog**

     tail -f /var/log/mainlog | grep angelab@sydneywestbiz.com.au

e.g root@syslog:~# tail -f /var/log/mainlog | grep angelab@sydneywestbiz.com.au  
Jan 23 15:11:46 mx-shared-4.private.netregistry.net exim[18699]: **1iuTqM-0004rb-FS** HISTORY:

==

to get detailed report

    search with Id

    e.g cat /var/log/mainlog | grep **1iuTqM-0004rb-FS**

        It should come as complete  
        Jan 23 15:11:47 mx-shared-4.private.netregistry.net exim[18700]: 1iuTqM-0004rb-FS **Completed** QT=1s

7) **IP block reason**

 iptables -L -n --line | grep 58.171.143.140

1 REJECT all -- 58.171.143.140 0.0.0.0/0 reject-with icmp-port-unreachable

to check the reason why ip is getting blocked

cat /var/log/messages | grep 58.171.143.140

iptables -nL --line-number | more

iptables -D f2b-exim 87

iptables -D f2b-splunk 367

iptables -D cphulk 6  
iptables -D INPUT 12

iptables -D INPUT\_imunify360 367  
iptables -D f2b-apache-wordpress 367

8) comman commands  
**Websites not working  
disable cagefs and enable it**

/usr/sbin/cagefsctl --disable baba3710  
[root@cp630 ~]# /usr/sbin/cagefsctl --enable baba3710

**enable-all**  
/usr/sbin/cagefsctl --enable-all

**Memory issue**

service httpd stop; service lve restart; service lvectl restart; service lvestats restart; service httpd start

**To give permission to files in server**

find . -type f -exec chmod 644 {} \;  
find . -type d -exec chmod 755 {} \;

==

01. cat /var/cpanel/accounting.log  | grep username  
e.g cat /var/cpanel/accounting.log  | grep arar1269

to see user creation and deletion

**To find main domain of a sub domain**

cat /etc/trueuserdomains |grep birkettc

**puppet**

    01. ps axuf |grep puppet

    02. kill -9 process\_number

        e.g  kill -9 27462

    03. systemctl start puppet or service puppet start

check again  ps axuf |grep puppet

==OR==  
service puppet status  
service puppet restart  
ps aux | grep yum  
kill -9 3836925 3841866 3842385  
ps aux | grep yum  
ps aux | grep rpm  
rpm -qa  
yum-complete-transaction  
ps aux | grep yum  
yum clean all  
ps aux | grep puppet  
tail -f /var/log/messages | grep puppet-agent

==  
**change password of cpanel**  
ALLOW\_PASSWORD\_CHANGE=1 /scripts/realchpass User Password

**Install Modules on PHP 7.3**

    goto the server

  run command directly>  yum groupinstall alt-php73\*

**to restart crond**  
systemctl restart crond

**to restart exim**

 systemctl restart exim

**to check status of exim**  
systemctl status  exim

**to find ip address those are attacking on http**

cat /usr/local/apache/domlogs/\*/\* | grep wp-login.php | grep POST |  awk '{print $1}' | sort | uniq -c | sort -n

cat /usr/local/apache/domlogs/\*/\* | grep xmlrpc.php | grep POST |  awk '{print $1}' | sort | uniq -c | sort -n

netstat -anp |grep 'tcp\|udp' | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n

**to block ip address only block ip of non australian user**  
 iptables -A INPUT -s ADDRESS -j DROP

**Disk warning Alert**

**df -h**

**1: to search large file of all accounts**

find / -path '/home/virtfs/\*' -prune -o -type f -size +256000k -exec ls -lh {} \; | awk '{ print $9 ": " $5 }'

2: to see the backup creation date  
ll /home/ozoz6788/backup-2.1.2019\_14-56-15\_ozoz6788.tar.gz

3: remove file

rm path

rm /home/ozoz6788/backup-2.1.2019\_14-56-15\_ozoz6788.tar.gz

enter y  
**done**

**==**

**find large file   
find / -size +10000k**

**Cpanel not accessible**

/usr/local/cpanel/scripts/modify\_accounts --theme=paper\_lantern --users=**username** --style=basic

e.g

/usr/local/cpanel/scripts/modify\_accounts --theme=paper\_lantern --users=whwh8214 --style=basic

**===**

**to remove folder**

**rm -rf foldername**

**==**

**to block in null server**ssh null.network.netregistry.net

**To unblock in null server**  
 route del -host 69.162.79.242  dev lo

**To block in null server**  
route add -host 51.77.111.224 dev lo

**to search if ip is block or not**  
ip route show | grep 132.232.115.212

iptables -L INPUT -v -n | grep 58.171.143.140

[root@awcp040 ~]# iptables -nL | grep 58.171.143.140

8)

**unable to create email box**

goto  
/home/user/etc/domainname.com  
edit passwd  
comment the mailbox

9) **mail re sync**

webmail

**BNE**

**backups in /mnt/mailstore/.snapshot/**

[root@bne003mu:/mnt/mailstore/.snapshot/weekly.2020-07-19\_0015/3/5/9/vs40953/mboxes/mb40953j]#

====

**Cloud**

In bne shell

    ssh  automation-1

    sudo su -

cd /clientmail/mail-1/

and first two letters

    e.g cd /clientmail/mail-1/d/i

find backups in

root@automation-1:/clientmail/mail-1# cd .snapshot/  
root@automation-1:/clientmail/mail-1/.snapshot# ll

or

root@dovecot-shared-2:/clientmail/mail-1/.snapshot/daily.2020-07-17\_0010/w/a/warregofarm.com.au# pwd  
/clientmail/mail-1/.snapshot/daily.2020-07-17\_0010/w/a/warregofarm.com.au  
root@dovecot-shared-2:/clientmail/mail-1/.snapshot/daily.2020-07-17\_0010/w/a/warregofarm.com.au#

==============

also works for cp to aws

in old server

**to tar a file**  
tar -czvf playlistpumppr.agency.tar.gz playlistpumppr.agency  
mv hdrep.com.au.tar.gz /usr/local/apache/htdocs/

into new server

cd /usr/local/src/  
 wget cp329.ezyreg.com/hdrep.com.au.tar.gz

**to untar a file**

 tar -xvf hdrep.com.au.tar.gz  
 rsync -avz sim/\* /home/s1067731/mail/hdrep.com.au/sim/

10) SSL issue queued in WHM

cd *var/cpanel*  
mv autossl\_queue\_cpanel.sqlite  autossl\_queue\_cpanel.sqlite\_bak

11) **Delete mails from webmail**

05:20] 4000 getmbx.sh craig@gfcconsultants.comcraig@gfcconsultants.com  
4001 getmbx.sh craig@gfcconsultants.com  
4002 cd /mnt/mailstore/0/8/0/vs343080/mboxes/mb343080a/  
4003 showMaildirByMonth.sh  
4004 splitMD Maildir 20191101 j26566493  
eg. splitMD Maildir 20200310 j26683744 :::: YYYYMMDD jjobid  
4005 tar -cvzf /mnt/mailstore/archives/tars/mb343080a\_Maildir-to-31-Oct-2019\_j26566493.tar.gz Maildir-to-31-Oct-2019 && rm -rf Maildir-to-31-Oct-2019  
4006 clearCache.sh craig@gfcconsultants.com  
4007 clearCache.sh craig@gfcconsultants.com  
4008 grep headersp .openwebmailrc  
4009 cd mail/  
4010 grep headersp .openwebmailrc

**12) HTTPS on cloud**# Enable HTTPS  
RewriteEngine On  
RewriteCond %{HTTP\_NR\_SSL} !="1"  
RewriteRule ^(.\*)$ https://%{SERVER\_NAME}%{REQUEST\_URI} [R,L]

**13) FTP**for windows  
<https://prnt.sc/tnnc04>

or hostname   
bne3ftp01.server-web.com

or [203.19.190.11](http://203.19.190.11/)

Never share username and password

Hi,

I have tried to connect FTP using following credentials and it worked.

Please have customer to use the below details to connect to the site via FTP:

FTP Hostname: bne3ftp01.server-web.com  
FTP Username: FTP username  
FTP Password: FTP password

Please let us know how it goes

Regards

**14) EXIM  
  
to view current mail sending or receiving**

tail -f  /var/log/exim\_mainlog | grep  westernsydneycomplianceservice.com.au

 cat /var/log/exim\_mainlog | grep 1j3tvx-0007JY-Nz

locate email id

 reset password of that email id and then **service exim restart**

service exim status

remove frozen mail

remove particular domain mails

exim -bp|grep **frozen** |awk '{print $3}' |xargs exim -Mrm  
e.g exim -bp|grep **mrpl.com.au** |awk '{print $3}' |xargs exim -Mrm

remove all mails from queue  
exim -bp | exiqgrep -i | xargs exim -Mrm

cat  /var/log/exim\_mainlog | grep **username** | awk '{print $5}' | sort | uniq -c | sort -n

grep 'cwd=' /var/log/exim\_mainlog | awk '{print $3}' | cut -d= -f2 | sort | uniq -c | sort -n

iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -m state --state NEW -j LOG --log-uid --log-prefix  "OUTBOUND PORT 80: "

tail -f /var/log/messages|grep -oP UID.\*

find . -type f -name '\*.php' -exec perl -ne '{print "{}\n" if ( length>=3000 && $\_ =~ /preg\_replace|eval|GLOBALS\(/i ) }' {} \;|uniq

**15) Auto responder**To set the autoresponder  
  
#   enable\_autoreply.sh mb11569g  
#   getmbx.sh mb11569g  
#   set\_autoreplytext.sh mb11569g  
#   getmbx.sh mb11569g  
  
#   delmbx.sh mb11569g >> to delete the account  
  
[12:11] ======  
To set store and forward on mails:  
From tardis :  
jump root@bne003mu  
  
Command : enable\_store-forward.sh <user|email> <mailForwardingAddress>  
  
# enable\_store-forward.sh accounts@millennium3.com.au Accounts@m3fs.com.au  
=============================  
  
To disable autoresponder:  
  
disable\_autoreply.sh mail-id

**16)   
installatron access issue**

**https://hostingfixes.wordpress.com/2014/08/30/internal-server-error500no-response-from-subprocess-usrlocalcpanelbase3rdpartyinstallatronindex-cgi/  
  
17) cpanel email issues**tail -f /var/log/exim\_mainlog | grep exports.com.au

cat

tail -n 300 /var/log/exim\_mainlog | grep clamd

===  
tail -n 300 /var/log/exim\_mainlog | grep clamd

yum -y remove $(rpm -qa |grep cpanel-clamav-0)  
/scripts/check\_cpanel\_rpms --fix  
pkill clam  
pkill inotify  
rm -f /etc/cron.daily/maldet  
rm -f /usr/local/cpanel/3rdparty/share/clamav/main.cld /usr/local/cpanel/3rdparty/share/clamav/main.cvd  
/usr/local/cpanel/3rdparty/bin/freshclam --update-db=main  
/etc/init.d/exim restart

tail -n 300 /var/log/exim\_mainlog | grep clamd

===  
  
{[[ exim.conf file corrupted

copy exim.conf file from another server

[root@awcp040 etc]# pwd  
/etc  
[root@awcp040 etc]# ll | grep exim  
  
move file to htdocs

[root@awcp040 htdocs]# ll | grep exim  
-rw-r--r-- 1 root root 79165 Jun 9 06:24 exim.conf  
-rw-r--r-- 1 root root 17710 Jul 3 05:33 exim.conf.tar.gz  
[root@awcp040 htdocs]#  
==  
wget in the server where the file is corrupted and untar the file

[root@awcp015 ~]# wget awcp040.server-cpanel.com/exim.conf.tar.gz

[root@awcp015 ~]# tar -xzvf exim.conf.tar.gz

[root@awcp015 ~]# service exim restart

]]}

**18) cpanel issues**

/scripts/check\_cpanel\_rpms --fix; /scripts/fix-cpanel-perl

**19) autossl issue**

add code in htacess  
======  
RewriteEngine On  
RewriteCond %{HTTPS} !=on  
RewriteRule ^(.\*)$ https://%{HTTP\_HOST}%{REQUEST\_URI} [L,R=301,NE]  
======

**20) useful commands**<https://www.ucartz.com/clients/index.php?rp=/knowledgebase/81/Common-cPanel-Commands-List.html>

<https://www.2daygeek.com/cpanel-whm-command-line-utility-scripts/>

21) exim count  
to find count of mails sent  
for particular date  
  
cat /var/log/exim\_mainlog | grep daniel@carnivalpromotions.com.au | grep "2020-05-29" | wc -l   
  
22) php info  
    root@automation-1:/websites/em/emilyferratohair.com.au# cat php.ini  
memory\_limit = 512M  
root@automation-1:/websites/em/emilyferratohair.com.au#

root@automation-1:/websites/em/emilyferratohair.com.au# cat phpinfo.php  
<?php

phpinfo();  
root@automation-1:/websites/em/emilyferratohair.com.au#

23) A record issue   
server IP should be assigned   
check via WHM > edit dns

or

[root@awcp070 ~]# cat /var/named/striven.com.au.db  
check via above command to see current A record

cpanel issue not propagating A record issue

24) find in a server  
grep -ilr "filename"  
  
25) cpanel error logs  
Goto the server to find

**TAIL**

tail -f  /usr/local/apache/logs/error\_log  | grep orasyhos

[root@cp624 ~]# tail -f /usr/local/apache/logs/error\_log

cat  /usr/local/apache/logs/error\_log  | grep stst5213

**Cpanel error logs**

tail -f /usr/local/cpanel/logs/error\_log | grep mgmg2140

==

**DO not increase memory on aws server**

Memory issue

to increase Vmem (virtual memory  
 goto whm of that server  
    search cloud  
    search user  
        -increase vmem

===

**optimize website through cpanel.**

25) cpanel account migrate  
cpanel to aws

in cpanel server  
scp restores@gsx-0001aweb.server-web.com:/opt/restore/restores/restore\_id\_3302/\* /home/anitin

**password 1w4n7myr3570r3**  
give permission in cp server  
chmod 755 cpmove-s1040162.tar.gz  
move to htdocs  
mv cpmove-s1040162.tar.gz /usr/local/apache/htdocs/  
  
  
  
  
in aws server  
goto cd /home  
wget cp384.ezyreg.com/cpmove-s1040162.tar.gz  
 /scripts/restorepkg cpmove-s1040162.tar.gz

26) cpanel theme issue  
  
**Cpanel not accessible**

/usr/local/cpanel/scripts/modify\_accounts --theme=paper\_lantern --users=**username** --style=basic

e.g

/usr/local/cpanel/scripts/modify\_accounts --theme=paper\_lantern --users=whwh8214 --style=basic

**Cpanel not accessible**

-create backup

-remove account

-create account in whm

- restore account

**move command**

move mail to usr

e.g     mv mail /usr/local/src/

e.g mv .trash/ /usr/local/src/

e.g mv public\_html /usr/local/src/

**create backup of account**

/scripts/pkgacct lala8860

**to find size of file**

du -sch \*

e.g du -sh cpmove-lala8860.tar.gz

du -sh .trash/

**to find database**

cd /var/lib/mysql/

 ll | grep lala8860\*

**to remove account after taking backup**

/scripts/removeacct lala8860

**to restore account**

/scripts/restorepkg cpmove-lala8860.tar.gz

**to restore account using force command**

/scripts/restorepkg lala8860 --force cpmove-lala8860.tar.gz

**to rename folder mail folder to mail.bak**

 mv mail mail.bak

**to give permission to folder**

chown lala8860.lala8860 mail -R

27) attacks on a domain  
got to user> access logs

 [root@cp459 access-logs]#grep "POST" stylishoutdoorweddings.com.au  
  
28) missing php modules  
  
    goto the server

    yum groupinstall alt-php73\*

-29) installtron error  
installatron  error  
tweak settings  
 search binaries  
set {Allow other applications to run the cPanel and admin binaries} to on  
  
30) serach domain  
  
 cat /etc/userdomains | grep hiko.com.au

 cat /var/cpanel/accounting.log | grep jeanioustassietours.com.au

 cat /var/cpanel/accounting | grep hiko.com.au  
cat /usr/local/cpanel/logs/accounting.log | grep hiko.com.au

grep asymex.com /var/cpanel/accounting.log

31) mail account not creating issue  
  
**mail account not creating issue**

   goto**to**server give permission to folder

goto user >goto etc >

e.g chown gygy2529.gygy2529 gybeimporting.com -R

to check mail permission  
 /scripts/mailperm gygy2529

32) exim   
01. To remove spam mail from the queue  
exim -bp | grep username -B 1 | awk '{print $3}'|xargs exim -Mrm  
e.g exim -bp | grep gugu4047 -B 1 | awk '{print $3}'|xargs exim -Mrm    
or  exim -bp | grep enquiries@edu-dance.com.au -B 1 | awk '{print $3}'|xargs exim -Mrm  
  
  
  
01. exim -bp  
 to see who is common user sending more mails  
  
    copy the username  
  
02. exim -Mvb 1igLMq-0002sE-NQ  
e.g exim -Mvb username  
  
-Mvb= to see body  
-Mvh = to see subject of mail  
  
  
03.  cat /var/log/exim\_mainlog | grep username  
e.g cat /var/log/exim\_mainlog | grep 1igLMq-0002sE-NQ  
  
  
  
04. cat /var/log/exim\_mainlog | grep 1igLMp-0002s6-4y  
  
05. /scripts/whoowns edu-dance.com.au  
to see the user of the domain