Linux Tweaks For U

Best Knowledge base for linux..

Exim commands

Exim email commands

Good tricks and tips: monitor Linux Server or how to manage Linux Server if its causing load, How to find Spammer, how to check http and mysql processes. (https://linuxtweaksforu.wordpress.com/2015/08/19/good-tricks-and-tips-monitor-linux-server-or-how-to-manage-linux-server-if-its-causing-load-how-to-find-spammer-how-to-check-http-and-mysql-processes/)

□ August 19, 2015 □ linuxtweaksforu Basic Commands, DDOS / Security, Exim commands, Spamming/load monitoring □ how to check http and mysql processes., How to find Spammer, monitor Linux Server or how to manage Linux Server if its causing load

Good tricks and tips: monitor Linux Server or how to manage Linux Server if its causing load, How to find Spammer, how to check http and mysql processes.

General Commands

To check server load and which users are logged on the server with IP address you can fire this command

```
w
```

To check for the server load and watch for process

```
top
top –d2
top –c d2
```

Memory status

```
free –m
```

To see all processes running on the server

```
ps –aufx
```

With above commands you can which process is causing load on the server after that you can go with next steps.
If you see many processes of exim then you can check exim in more detail. shows the total no of email in qmail

```
exim –bpc
```

Print a listing of the messages in the queue

```
exim -bp
```

Following command will show path to the script being utilized to send mail

```
ps -C exim -fH eww
ps -C exim -fH eww | grep home
cd /var/spool/exim/input/
egrep “X-PHP-Script” * -R
```

Shows no of frozen emails

```
exim -bpr | grep frozen | wc -l
```

To remove FROZEN mails from the server

```
exim -bp | exiqgrep -i | xargs exim -Mrm
exiqgrep -z -i | xargs exim –Mrm
```

Check for spamming if anybody is using php script for sending mail through home

```
tail -f /var/log/exim_mainlog | grep home
```

If anyone is spamming from /tmp

```
tail -f /var/log/exim_mainlog | grep /tmp
```

To display the IP and no of tries done bu the IP to send mail but rejected by the server.

```
tail -3000 /var/log/exim_mainlog |grep ‘rejected RCPT’ |awk ‘{print$4}’|awk -F\[ ‘{print $2} ‘|awk -F\] ‘{print $1} ‘|sort | uniq -c | sort -k 1 -nr | head -n 5
```

Shows the connections from a certain ip to the SMTP server

```
netstat -plan|grep :25|awk {‘print $5’}|cut -d: -f 1|sort|uniq -c|sort -nk 1
```

To shows the domain name and the no of emails sent by that domain

```
exim -bp | exiqsumm | more
```

If spamming from outside domain then you can block that domain or email id on the server

```
pico /etc/antivirus.exim
```

Add the following lines:

```
if $header_from: contains “name@domain.com (//domain.com)”
then
seen finish
endif
```

Catching spammer
Check mail stats

```
exim -bp | exiqsumm | more
```

Following command will show you the maximum no of email currently in the mail queue have from or to the email address in the mail queue with exact figure.

```
exim -bpr | grep “” | awk ‘{print $4}’|grep -v “” | sort | uniq -c | sort -n
```

That will show you the maximum no of email currently in the mail queue have for the domain or from the domain with number.

```
exim -bpr | grep “” | awk ‘{print $4}’|grep -v “” |awk -F “@” ‘{ print $2}’ | sort | uniq -c | sort -n
```

Check if any php script is causing the mass mailing with

```
cd /var/spool/exim/input
egrep “X-PHP-Script” * -R
```

Just cat the ID that you get and you will be able to check which script is here causing problem for you.
To Remove particular email account email

```
exim -bpr |grep “ragnarockradio.org”|awk {‘print $3’}|xargs exim -Mrm
```

If Mysql causing the load so you can use following commands to check it.

```
mysqladmin pr
mysqladmin -u root processlist
mysqladmin version
watch mysqladmin proc
```

If Apache causing the load so check using following commands.

```
netstat -ntu | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –n
netstat -an |grep :80 |wc –l
netstat -n | grep :80 | wc -l;uptime ; netstat -n | wc –l
netstat –tupl
pidof httpd
history | netstat
lsof -p pid
```

If mysql is causing load so you can check it using following commands.

```
mysqladmin -u root processlist
mysqladmin version
watch mysqladmin proc
mysqladmin -u root processlist
```

Other Useful Commands

To check ipd of php

```
pidof php
lsof -p pid
```

```
netstat -an |grep :80 |wc –l
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
netstat -na |grep :80 |sort
```

Use below mentioned command to get top memory consuming processes

```
ps aux | head -1;ps aux –no-headers| sort -rn +3 | head
```

Use below command to get top cpu consuming processes

```
ps aux | head -1;ps aux –no-headers | sort -rn +2 |more
```

You can check if any backup is going on, run the following commands

```
ps aux | grep pkg
ps aux | grep gzip
ps aux | grep backup
```

We can trace the user responsible for high web server resource usage by the folowing command

```
cat /etc/httpd/logs/access_log | grep mp3
cat /etc/httpd/logs/access_log | grep rar
cat /etc/httpd/logs/access_log | grep wav etc
cat /etc/httpd/logs/access_log | grep 408 can be used to check for DDOS attacks on the server.
cat /etc/httpd/logs/access_log | grep rar
```

Leave a comment

Useful exim commands (https://linuxtweaksforu.wordpress.com/2015/07/13/useful-exim-commands/)

July 13, 2015August 7, 2015 linuxtweaksforu Exim commands all exim basic commands, exim commands, exim commands linux, exim queue

Exim puts all of its logs into the following directory:
# **cd /var/log**

Exim maintains three logfiles:
# **/var/log/exim_mainlog**
# **/var/log/exim_paniclog**
# **/var/log/exim_rejectlog**

exim_mainlog: This logs tracks every single mail transaction that your server handles. This is the go-to log when troubleshooting all e-mail delivery problems.

exim_rejectlog: This log only logs delivery rejections. While this can be useful, this is not the first log file you will want to search when troubleshooting a mail problem. For example, if mail is getting through on the server, but your mail client is silently failing to download mail, this log will not help you.

exim_paniclog: This log contains has information regarding the exim program itself, and not mail transactions. For this reason, it is not suitable for most mail troubleshooting.

You can find the exim logs using the exigrep utility for a particular domain using below command:

```
# exigrep domain.com (//domain.com) /var/log/exim_mainlog
```

To get a count of emails in the queue:

```
# exim -bpc
```

Print a listing of the messages in the queue (time queued, size, message-id, sender, recipient) :

```
# exim -bp
```

```
# exim -bp | less
```

To view the header of a particular email using mail ID:

```
# exim -MvH mail_id
```

To view the body of a particular email using mail ID:

```
# exim -Mvb mail_id
```

To view a message’s logs:

```
# exim -Mvl mail_id
```

To trace path:

```
# exim -d -bt user@domain.com (//domain.com)
```

To view new enteries of the email sent/received logs for particular email:

```
# tail -f /var/log/exim_mainlog | grep email_id
```

To check the email logs of particular email id:

```
# cat /var/log/exim_mainlog | grep email_id
```

To get sorted list of email sender in exim queue:

```
# exim -bpr | grep “<" | awk {'print $4'} |cut -d "” -f 1 | sort -n | uniq -c| sort -n
```

To check the script that will originate spam mails:

```
# grep “cwd=” /var/log/exim_mainlog|awk ‘{for(i=1;i<=10;i++){print $i}}'|sort| uniq -c|grep cwd|sort -n
```

If we need to find out exact spamming script. To do this, run following command:

```
# ps auxwwwe | grep user | grep –color=always "/home/user/public_html/templates/" | head
```

To delete the emails of a specific user:

```
# grep -lr 'user@domain.com (//domain.com)' /var/spool/exim/input/ | sed -e 's/^.*\/\([a-zA-Z0-9-]*\)-[DH]$/\1/g' | xargs exim –Mrm
```

OR

```
# exim -bp | grep "user_email-account" | awk '{print $3}' | xargs exim -Mrm
```

To delete Frozen emails from the email queue: (any one of the below command will work)

```
# exim -bp|grep frozen|awk '{print $3}' |xargs exim –Mrm
```

```
# grep -R -l '*** Frozen' /var/spool/exim/msglog/*|cut -b26-|xargs exim –Mrm
# exim –bpr | grep frozen | awk '{print $3}'| xargs exim –Mrm
```

```
# exiqgrep -z -i | xargs exim -Mrm
```

To check the no. of frozen mails:

```
# exiqgrep -z -c
```

To check exim logs:

```
# tail -f /var/log/exim_mainlog
```

Force delivery of one message:

```
# exim -M mail_id
```

Force another queue run:

```
# exim -qf
```

Force another queue run and attempt to flush frozen messages: (To flush the exim queue)

```
# exim -qff
```

□ Leave a comment

To start SMTP (Dovecot service), when SMTP service is down: (https://linuxtweaksforu.wordpress.com/2015/07/12/to-start-smtp-dovecot-service-when-smtp-server-is-down/)

□ July 12, 2015July 12, 2015 □ linuxtweaksforu Basic Commands, Email Issues, Exim commands □ dovecot command, how to fix smtp down issue in linux, smtp service is down, smtp service unable to start

To start SMTP (Dovecot service), when SMTP server is down:

```
# /etc/init.d/dovecot restart
```

If still it does not start with this, then use the below command to get this done.

```
# /etc/init.d/xinetd stop
# /etc/init.d/xinetd start
```

Then give a try to start SMTP service with below command.

```
# /etc/init.d/dovecot start
# /etc/init.d/dovecot status (to check the status of the service)
```

And if still the httpd or any other service does not come up, then you can try to create a file by using a command: touch k

If still it gives and error then it is the issue with the permissions. You need to contact DC and tell them to check and FSCK the server.

□ Leave a comment

Ⓦ (https://wordpress.com/?ref=footer_custom_svg)