

Postfix Quick Reference

This is just some notes on things I do in Postfix.

Finding User who has been hacked

1. look for messages that are sending to multiple recipients

```
grep 'postfix/smtp' /var/log/mail.log | cut -d ':' -f4 | grep -v  
'connect' | grep -v warning | grep -v SSL | sort | uniq -c | sort -nr |  
head
```

2. Grab one of the identifiers and look at where it originated. This returned 47B5F826C2

```
grep 47B5F826C2 /var/log/mail.log | grep 'from=' | cut -d ':' -f5 | cut  
-d '<' -f2 | cut -d '>' -f1
```

3. Choose a username. This returned mail.brakzijn.nl@my.server

```
grep mail.brakzijn.nl mail.log | grep RCPT | cut -d '[' -f3 | cut -d ']'  
-f1 | sort | uniq -c | sort -rn | head
```

4. see the IP they are coming from, then look for the login that is associated with it

```
grep 129.205.113.219 /var/log/mail.log | grep 'saslm_method=LOGIN' | cut  
-d '=' -f4 | sort | uniq -c | sort -rn
```

5. That is the user that has been hacked

Look for specific activity

The mail log (/var/log/mail.log on Debian derivatives) contains way too much information most of the time. Here, *grep* is your friend. You can find different things based on which daemon is reporting the line item, then further refine by adding an additional *grep* after.

For example, if you were moving a domain from one server to another, it is common to allow the old server to accept messages for a while to keep from losing your clients e-mail. So, for example, if you wanted to know the last time any mail was delivered to an example.com account, you would do.

```
grep delivered mail.log | grep example.com | tail
```

- If you want to see who is sending mail, try looking for the submission daemon in the log. You can then narrow it down with a second *grep*

```
grep submission /var/log/mail.log | grep keyword_to_search_for
```

- If you want to see who is receiving mail, look for the delivered keyword in the log. This only

shows you mail that has been accepted and delivered.

```
grep delivered mail.log | grep keyword_to_search_for
```

Change attachment max size

Actually, this is the total message size. It is in bytes, so it is a very large number.

To see what the current setting is, type

```
postconf | grep message_size_limit
```

. If the value is not explicitly entered in main.cf, the default value is show.

To set a new value, type

```
postconf -e message_size_limit=26214400
```

. The number is 25 Megabytes, or $25 \times 1024 \times 1024$ (from a calculator). Obviously, you need to reload or restart postfix for this to take effect.

From:

<https://wiki.linuxservertech.com/> - **Unix Server Tech Knowledge Base**

Permanent link:

<https://wiki.linuxservertech.com/software/postfix/quickreference>

Last update: **2020/09/24 00:09**

