Postfix

Mails mit 'postsuper' löschen

If you host customers’ email domains for them, you probably have experienced them getting viruses, etc. that fill your mail queue with spam. This can be a real pain in the ass to clean out if it’s a very large number of messages so below I’ll post a simple way to clean the messages just from that user and none of the other legit messages still in the queue. Here’s the steps you’d go through to do the cleanup:

1. Identify the hacked or virus-infected sender (and immediately change their password). This may be as easy as running “postqueue -p” to display the mail queue and finding their address as the sender of all the messages. Sometimes though, the virus or hacker will be sending using random return paths so you may have to work harder to identify all the bad messages.For example, if you know the IP the sender was using, block it of course, then try running this command:

   ```
   find /var/spool/postfix -type f -exec grep -l 192.0.2.1 {} \; |
   cut -f 7 -d '/'| sort | uniq
   ```

   That will run through your entire postfix queue directory hierarchy and find the files that have the matching IP address 192.0.2.1 present in them, extract just those filenames from the output by taking the 7th field of the output (separated by slashes), sort them and then eliminate duplicates (since there maybe be the same message id in multiple directories).

2. Once you’ve identified the bad message sender patterns, you can run something like this to extract the message id’s of all the bad messages if they’re easily identified by the sender and you don’t need to do something more complicated like the above ip address example:

   ```
   postqueue -p | grep "user@domain.com" | cut -f 1 -d ' '
   ```

   or if multiple senders

   ```
   postqueue -p | egrep "user@first.com|user@second.com|user@third.
   com" | cut -f 1 -d ' '
   ```

3. Now that you have a command you can use that prints just the relevant message id’s, simply add this to the end of the command to automatically call the postfix message deletion command against each of those messages id’s: | xargs -n 1 postsuper -d
4. The -n 1 argument tells it to execute the command with a maximum of one argument; i.e. call postsuper for every single line of input instead of the default xargs behavior of running a large number of arguments in, which won’t work for the postsuper command.

So you’ll end up running something like one of these commands:

```
find /var/spool/postfix -type f -exec grep -l 192.0.2.1 {} \; | cut -f
 7 -d '/'| sort | uniq | xargs -n 1 postsuper -d

postsuper -d postqueue -p | grep "user@domain.com" | cut -f 1 -d ' ' |
 xargs -n 1 postsuper -d
```

Eindeutige ID: #1012
Verfasser: Christian Frey
Letzte Änderung: 2015-12-28 11:03