Home » **Unix** » **Plesk mail queue filled full with FAILURE NOTICE messages to strange addresses (qmail stuck, bounce back, reject)**

Not long ago we experienced a huge problem on our dedicated server hosted at **GoDaddy** with **Plesk 9.5** control panel installed. Please note that if you are hosted at GoDaddy with Plesk, the server has a **qMail** mail daemon installed by default, running on Plesk-specific configuration.

First we received an automated email from GoDaddy stating that our SMTP limit of 1000 outgoing emails has been reached. First thing we do is we go to `Plesk control panel -> Home -> Mail Server Settings -> Mail Queue`. There we saw over 2500 emails, mostly **FAILURE NOTICE** emails to weird email addresses of different countries around the world - Germany, Canada, Russia, Ukraine, Cuba, Brazil, Thailand, etc. This had to be dealt with as soon as possible, because while the queue was full and our SMTP was turned off by GoDaddy, the clients hosted on our server were not able to send emails if they were using our SMTP server. To find out where those FAILURE NOTICE emails are originating from, we need an SSH access to the server with root priveledges. Remember the outgoing "weird" address of one of the latest messages in your queue. As soon as you enter the server in root mode:

```
/var/qmail/bin/qmail-qread
```

This command will list a brief information about every message currently being in your mail queue. Now find the line with a "weird" email address, it should look like this:

```
8 Nov 2010 11:23:33 GMT  #11928049  1600  <>
        remote  t_mcgowankf@fh-brandenburg.de
```

where `#11928049` is the number of that message, by knowing that number you will be able to see full message with all headers. To do that, we have to first find that message, enter:

```
find /var/qmail/queue/mess/ -name 11928049
```

As a result you will get something like this:

```
/var/qmail/queue/mess/19/11928049
```

That's the path to the message you're looking for. Now view it by entering:

```
cat /var/qmail/queue/mess/19/11928049
```

You will see the whole message in your console and what you really need though is the top part of that message. Ours looked like this:

```
Received: (qmail 23254 invoked for bounce); 8 Nov 2010 11:23:33 -0500
Date: 8 Nov 2010 11:23:33 -0500
From: MAILER-DAEMON@ip-xxx-xxx-xxx-xxx.ip.secureserver.net
To: t_mcgowankf@fh-brandenburg.de
Subject: failure notice

Hi. This is the qmail-send program at ip-xxx-xxx-xxx-xxx.ip.secureserver.net.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

email@ourclient.com:
Mail quota exceeded.

--- Below this line is a copy of the message.
```

Below that was our favourite viagra advertisement line, I don't think I'm going to include it here, we only need the top part of that message. So what that top part means is that spammer sent his spam to our client's email, and because the email box is full, the server has to bounce back with a message stating that. But wait, we have SPAM

protection on our server, aren't we? Indeed we do. The problem is, although Plesk is an expensive product, it lacks the functionality it seems to have and for some reason is very very buggy. Without confusing you any further, I will tell you how we solved that problem and please read till the very end.

Go to Mail Preferences in Plesk and make sure you have these following items the way they are shown below:

`Check the passwords for mailboxes in the dictionary` - put a checkmark here. It will prevent your clients to change their email passwords to something easy like "123123", "admin" and so on. It will prevent spammers from compromising any particular user account by bruteforcing or performing a dictionary attack on your SMTP server (if you have your relay open, but read more about smtp-relay below)

`Relaying - closed` - close the relay!!! Here is the thing with GoDaddy dedicated servers with Plesk - even if you check `authorization is required` and check both `POP3 (20 min)` and `SMTP`, it will still let anyone to telnet to either port 25 (SMTP) or port 465 (Secure SSL) of your server and send email messages **WITHOUT ANY AUTHORIZATION**! Anyone is going to be able to spam from your server! We have tested it and are 100% sure that spamming will be possible from both of those ports is you open the relay and EVEN IF you require authentication, it will not ask for it. For some reason **smtp_auth** module does not work with Plesk's qMail, although it is present on the server and supposedly is running. We have managed to sniff all TCP packets coming through ports 25 and 465 and there was not a single authorization while the relay was open. Close it!

`Switch on SPF spam protection` - put a checkmark here and from a drop-down below select `Reject mail when SPF resolves to "fail" (deny)`. It will reject all incoming spam mail. In SPF Local Rules we have `include:spf.trusted-forwarder.org`

At the very bottom select `Only use of full POP3/IMAP mail accounts names is allowed` - it will force the user to login with the whole `user@domain.com` login, instead of just `user` to his/her POP3. It has to be checked!

Now go to White List in Plesk Mail Server Settings page. The only thing that should be in the white list is the host address of your server, nothing else! Add `127.0.0.1` (it will appear as `127.0.0.1 /32`)

Now last but not least, if you have SpamAssasin installed and running on your server, it does not mean it's actually working (thanks Plesk!). Remember the email of our client from the FAILURE NOTICE message above? Well we have checked several FAILURE NOTICE messages and ALL of them were bouncebacks from that same client. So we have to check his mailbox settings. In Plesk go to `Domains -> ourclient.com -> Mail Accounts -> user@ourclient.com -> Spam Filtering` (where `user@ourclient.com` is the mailbox which we found out was full and was generating FAILURE NOTICES)

Switch the spam protection `ON`, put a score of `7.00` and add a checkmark near `Delete spam mail when it comes to mailbox`. Note: even if SpamAssasin is enabled server-wide, it does NOT work unless you enable it for a specific user (well it did not work for us anyways, maybe you will have a better luck). Also, make sure that for every domain you are hosting in `Mail Accounts -> Mail Settings` you select `Reject` near `Mail to nonexistent user` (it did not help our situation at all though, the mail still gets bounced back for some Plesk-weird reason).

That is all. We removed all FAILURE NOTICE messages from the queue (you can do it with `qmHandle -Sfailure`) and on the next day the queue cleared and valid messages started getting through. You can also add this line into your crontab if you would like to remove FAILURE NOTICE messages from the mail queue every minute untill you solve the situation:

```
0-59    *       *       *       *       qmHandle -Sfailure >/dev/null 2>&1
```

Such a horrible implementation of qMail by Plesk is retarded. Although we updated to the latest version of Plesk (**Plesk 9.5.3** at the moment of writing the article) and qMail (Oct 21, 2010 version), weird problems like the one in that article are still present, so as a next step I suggest you switch to `postfix` mail server. It can be done within Plesk and all settings should get transferred from qMail to postfix. But I guess that's for you to find out :) Next I will add more info on how to capture packets to inspect the traffic going through the specific ports on your server.

PS: to find out the quality of Parallels technical support, visit this thread - **http://forum.parallels.com/showthread.php?p=427395** (regarding the Relay issue)

Posted: 2010-11-08 10:38:17 [**Link**] [**Thank you!** - 10]