openSUSE admin - tickets #115238

Mail bounces on mail list

2022-08-11 12:05 - robin_listas

Status:	Resolved	**Start date:**	2022-08-11
Priority:	Normal	**Due date:**	
Assignee:	pjessen	**% Done:**	100%
Category:	Email	**Estimated time:**	0.00 hour
Target version:			

Description

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

I post to the users mail list, and on each post I get two identical
bounces, since yesterday:

Delivery has failed to these recipients or groups:

amdlnx60@googlemail.com
Your message wasn't delivered because the recipient's email provider rejected it.

Diagnostic information for administrators:

Generating server: AS8P251MB0957.EURP251.PROD.OUTLOOK.COM

amdlnx60@googlemail.com
Remote Server returned '550-5.7.26 The MAIL FROM domain [telefonica.net] has an SPF record with a hard 550-5.7.26 fail policy (-all) but it fails to pass SPF checks with the ip: 550-5.7.26 [104.47.12.57]. To best protect our users from spam and phishing, 550-5.7.26 the message has been blocked. Please visit 550-5.7.26 https://support.google.com/mail/answer/81126#authentication for more 550 5.7.26 information. bc22-20020a056402205600b0043cfd7f7afdsi11372238edb.508 - gsmtp'

the second bounce says:

amdlnx60@googlemail.com
Remote Server returned '550-5.7.26 The MAIL FROM domain [telefonica.net] has an SPF record with a hard 550-5.7.26 fail policy (-all) but it fails to pass SPF checks with the ip: 550-5.7.26 [104.47.18.111]. To best protect our users from spam and phishing, 550-5.7.26 the message has been blocked. Please visit 550-5.7.26 https://support.google.com/mail/answer/81126#authentication for more 550 5.7.26 information. di13-20020a170906730d00b0072afc158ff0si7633603ejc.315 - gsmtp'

Cheers / Saludos,

Carlos E. R.
(from 15.3 x86_64 at Legolas)

-----BEGIN PGP SIGNATURE-----

iHYEARECADYWIQQZEb51mJKK1KpcU/W1MxgcbY1H1QUCYvTwZRgcY2FybG9zLmUu
ckBvcGVuc3VzZS5vcmcACgkQtTMYHG2NR9WXwwCgg1J1zuK4fCyjEBeLhLNBwwn3
ZvIAnjVsO3QZdimHZols+V16U4BoWU/S
=WDa0
-----END PGP SIGNATURE-----

History

#1 - 2022-08-11 14:12 - pjessen

- Private changed from Yes to No

robin_listas wrote:

> Diagnostic information for administrators:
> Generating server: AS8P251MB0957.EURP251.PROD.OUTLOOK.COM

For starters, that seems odd - why should Microsoft Office365 be involved in a delivery from an openSUSE list to a googlemail address?

```
amdlnx60@googlemail.com
Remote Server returned :
550-5.7.26 The MAIL FROM domain [telefonica.net] has an SPF record with a hard
550-5.7.26 fail policy (-all) but it fails to pass SPF checks with the ip:
550-5.7.26 [104.47.12.57]. To best protect our users from spam and phishing,
550-5.7.26 the message has been blocked. Please visit
550-5.7.26 https://support.google.com/mail/answer/81126#authentication for more
550 5.7.26 information. bc22-20020a056402205600b0043cfd7f7afdsi11372238edb.508 - gsmtp'
```

So somehow Microsoft tried to deliver something to "amdlnx60@googlemail.com", but google rejected it.
Assuming "MAIL FROM" is the "MAIL FROM" used in the SMTP transaction, iow the envelope address, that also seems odd. When we deliver mail from lists, we use the list bounce address as envelope.

104.47.12.57 = mail-db3eur04lp2057.outbound.protection.outlook.com
104.47.18.111 = mail-am6eur05lp2111.outbound.protection.outlook.com

I have to assume this is someone with Office365 hosting having their mails forwarded to "amdlnx60@googlemail.com". I do not understand why Office365 should be sending anything with "MAIL FROM: something@telefonica.net".

#2 - 2022-08-11 14:31 - pjessen

- Category set to Email

- Status changed from New to Feedback

- Assignee set to pjessen

Is there anything in the NDR / bounce message that tells you which mail is being rejected? a message-id would be helpful. The timestamps might also help. I see that we send quite a few mails to 'amdlnx60' every day, e.g. from factory.lists.

FWIW, In April 2022, Felix reported something similar.

#3 - 2022-08-11 16:36 - robin_listas

- File p added

I have several bounces, 7 at least with header "Undeliverable: ".
Why MS Office365 involved, why not bouncing to the envelope address? Trust MS to do things wrong.

Messagges ID of posts which they bounced:

Message-ID: afc792db-5117-1022-5ef8-c9bd27128d63@telefonica.net
From: "Carlos E. R." robin.listas@telefonica.net
In-Reply-To: 49a6df81-b4e0-150f-2be0-feb109c4a347@j4computers.com
Date: Wed, 10 Aug 2022 17:36:56 +0200
To: oS-EN users@lists.opensuse.org

Message-ID: d3966aa4-0b65-3de6-79f1-51417930f509@telefonica.net
Date: Thu, 11 Aug 2022 12:27:13 +0200
Subject: Re: logrotate, systemd, stopped rotating a log
To: oS-EN users@lists.opensuse.org
References: 00d5eac4-95ec-d8e2-d689-b354eb940c5a@j4computers.com
20220810231721.GP22216@wahoo.no-ip.org
From: "Carlos E. R." robin.listas@telefonica.net
In-Reply-To:

Message-ID: d3966aa4-0b65-3de6-79f1-51417930f509@telefonica.net
Date: Thu, 11 Aug 2022 12:27:13 +0200
Subject: Re: logrotate, systemd, stopped rotating a log
To: oS-EN users@lists.opensuse.org
References: 00d5eac4-95ec-d8e2-d689-b354eb940c5a@j4computers.com
20220810231721.GP22216@wahoo.no-ip.org
From: "Carlos E. R." robin.listas@telefonica.net

(yes, two bounces for a single message)

Message-ID: 95334ac4-4c78-28a9-311a-cc203a7e2900@telefonica.net
Date: Thu, 11 Aug 2022 12:17:57 +0200
Subject: Re: [oS-en] Recovering dead text file
To: oS-EN users@lists.opensuse.org
References: ed884162-3bf4-e460-b681-09b082a2b43d@telefonica.net

fccd63b9-1861-d86b-6cec-860da14e395b@suddenlinkmail.com
From: "Carlos E. R." robin.listas@telefonica.net

Message-ID: 95334ac4-4c78-28a9-311a-cc203a7e2900@telefonica.net
Date: Thu, 11 Aug 2022 12:17:57 +0200
Subject: Re: [oS-en] Recovering dead text file
To: oS-EN users@lists.opensuse.org
References: ed884162-3bf4-e460-b681-09b082a2b43d@telefonica.net
fccd63b9-1861-d86b-6cec-860da14e395b@suddenlinkmail.com
From: "Carlos E. R." robin.listas@telefonica.net
In-Reply-To: fccd63b9-1861-d86b-6cec-860da14e395b@suddenlinkmail.com

Message-ID: 9b08171d-9ff2-3410-bb52-f4319b607984@telefonica.net
Date: Thu, 11 Aug 2022 13:37:54 +0200
Subject: Re: [oS-en] Recovering dead text file
To: oS-EN users@lists.opensuse.org
References: ed884162-3bf4-e460-b681-09b082a2b43d@telefonica.net
fccd63b9-1861-d86b-6cec-860da14e395b@suddenlinkmail.com
95334ac4-4c78-28a9-311a-cc203a7e2900@telefonica.net
20220811112640.yothu2esdyy264nx@grusum.dhaller.de
From: "Carlos E. R." robin.listas@telefonica.net
In-Reply-To: 20220811112640.yothu2esdyy264nx@grusum.dhaller.de

Message-ID: 9b08171d-9ff2-3410-bb52-f4319b607984@telefonica.net
Date: Thu, 11 Aug 2022 13:37:54 +0200
Subject: Re: [oS-en] Recovering dead text file
To: oS-EN users@lists.opensuse.org
References: ed884162-3bf4-e460-b681-09b082a2b43d@telefonica.net
fccd63b9-1861-d86b-6cec-860da14e395b@suddenlinkmail.com
95334ac4-4c78-28a9-311a-cc203a7e2900@telefonica.net
20220811112640.yothu2esdyy264nx@grusum.dhaller.de
From: "Carlos E. R." robin.listas@telefonica.net
In-Reply-To: 20220811112640.yothu2esdyy264nx@grusum.dhaller.de

(again, a double bounce)

I just replied to a post, and got two new bounces:

Message-ID: 1f489760-24d5-2d3d-d1a2-9774c79d1973@telefonica.net
Date: Thu, 11 Aug 2022 18:28:21 +0200
Subject: Re: [oS-en] Recovering dead text file
To: oS-EN users@lists.opensuse.org
References: ed884162-3bf4-e460-b681-09b082a2b43d@telefonica.net
fccd63b9-1861-d86b-6cec-860da14e395b@suddenlinkmail.com
95334ac4-4c78-28a9-311a-cc203a7e2900@telefonica.net
20220811112640.yothu2esdyy264nx@grusum.dhaller.de
9b08171d-9ff2-3410-bb52-f4319b607984@telefonica.net
20220811132813.GQ22216@wahoo.no-ip.org
869e3a38-04e0-7840-f2ae-c771f84aab9a@dodin.org
From: "Carlos E. R." robin.listas@telefonica.net
In-Reply-To: 869e3a38-04e0-7840-f2ae-c771f84aab9a@dodin.org

Message-ID: 1f489760-24d5-2d3d-d1a2-9774c79d1973@telefonica.net
Date: Thu, 11 Aug 2022 18:28:21 +0200
Subject: Re: [oS-en] Recovering dead text file
To: oS-EN users@lists.opensuse.org
References: ed884162-3bf4-e460-b681-09b082a2b43d@telefonica.net
fccd63b9-1861-d86b-6cec-860da14e395b@suddenlinkmail.com
95334ac4-4c78-28a9-311a-cc203a7e2900@telefonica.net
20220811112640.yothu2esdyy264nx@grusum.dhaller.de
9b08171d-9ff2-3410-bb52-f4319b607984@telefonica.net
20220811132813.GQ22216@wahoo.no-ip.org
869e3a38-04e0-7840-f2ae-c771f84aab9a@dodin.org
From: "Carlos E. R." robin.listas@telefonica.net
In-Reply-To: 869e3a38-04e0-7840-f2ae-c771f84aab9a@dodin.org

I can try to attach the full bounce message as file here.

#4 - 2022-08-11 17:23 - pjessen

robin_listas wrote:

> I have several bounces, 7 at least with header "Undeliverable: ".
> Why MS Office365 involved, why not bouncing to the envelope address? Trust MS to do things wrong.

Yes, but there is no reason for MS to be in the loop.

> Messagges ID of posts which they bounced:
> Message-ID: afc792db-5117-1022-5ef8-c9bd27128d63@telefonica.net

Remarkably, except for one, all copies were sent to Microsoft Office365 :-)

Well, my guess is that some subscriber whose mail account is hosted by Microsoft O365 has his mail forwarded to "amdlnx60@googlemail". I cannot fathom why MS would deliver such a forwarding with MAIL FROM: you@telefonica.net, that seems nonsensical.
I have no way of knowing which subscriber it is.

#5 - 2022-08-11 17:33 - robin_listas

Possibly:

Resent-From: gregormeier@outlook.com

you can see that in the attached "p" file.

#6 - 2022-08-11 18:56 - pjessen

robin_listas wrote:

> Possibly:
>
> Resent-From: gregormeier@outlook.com
>
> you can see that in the attached "p" file.

Hmm, the attachment didn't make it through, but that address is not in the logs from today.

#7 - 2022-08-11 21:06 - robin_listas

File is here: https://progress.opensuse.org/attachments/download/13649/p
It was not mailed, but uploaded to the ticket server.

#8 - 2022-08-12 08:10 - pjessen

robin_listas wrote:

> File is here: https://progress.opensuse.org/attachments/download/13649/p
> It was not mailed, but uploaded to the ticket server.

Ah, yes. Well, it is still not 100% clear, but gregormeier@outlook.com does seem to be involved. Looking in our mail logs (on anna) for all of August, we have however not sent a single email to that address.

I'm not sure if there is anything we can do or need to do - judging by the bounce text (550-5.7.26) it appears to be Microsoft trying to deliver a mail to Google (amdlnx60), using MAIL FROM: you@telefonica. Most places with SPF checks would (and should) reject that. It is however more likely that Google is looking at the header address From:, and rejecting based on that.

#9 - 2022-08-28 10:26 - pjessen

- Status changed from Feedback to Resolved

- % Done changed from 0 to 100

Closing as resolved, there is little we can do about the situation. Feel free to re-open of course.

Files

p	71 KB	2022-08-11	robin_listas