Redmine - Defect #38514

Email Notifications: Email Notifications: trigger rspamd symbol for bad HELO

2023-05-03 12:23 - Hendrik Jaeger

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Website (redmine.org)	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	

Description

Registration email from redmine.org triggers the following rspamd symbol:
Symbol: HFILTER_HELO_5(3.00)

From the headers:
Received: from static.126.101.4.46.clients.your-server.de ([46.4.101.126]:43352 helo=Ubuntu-2004-focal-64-minimal)

I think this HELO Ubuntu-2004-focal-64-minimal is what rspamd takes offense at. It should probably be a FQDN.
But TBH I was not able to figure out what exactly the rspamd symbol meant quickly so this might be wrong.

See https://www.rfc-editor.org/rfc/rfc5321.html#section-4.1.1.1 which says

```
These commands are used to identify the SMTP client to the SMTP
server.  The argument clause contains the fully-qualified domain name
of the SMTP client, if one is available.  In situations in which the
SMTP client system does not have a meaningful domain name (e.g., when
its address is dynamically allocated and no reverse mapping record is
available), the client SHOULD send an address literal (see
Section 4.1.3).
```

History

#1 - 2023-05-03 12:33 - Hendrik Jaeger

Sorry, pressed enter at the wrong time before I even really started …

Subject should read: Email Notifications: trigger rspamd symbol for bad HELO

Description:

Registration email from redmine.org triggers the following rspamd symbol:
Symbol: HFILTER_HELO_5(3.00)

From the headers:
Received: from static.126.101.4.46.clients.your-server.de ([46.4.101.126]:43352 helo=Ubuntu-2004-focal-64-minimal)

I think this HELO Ubuntu-2004-focal-64-minimal is what rspamd takes offense at. It should probably be a FQDN.
But TBH I was not able to figure out what exactly the rspamd symbol meant quickly so this might be wrong.

See https://www.rfc-editor.org/rfc/rfc5321.html#section-4.1.1.1 which says

```
These commands are used to identify the SMTP client to the SMTP
server.  The argument clause contains the fully-qualified domain name
of the SMTP client, if one is available.  In situations in which the
SMTP client system does not have a meaningful domain name (e.g., when
its address is dynamically allocated and no reverse mapping record is
available), the client SHOULD send an address literal (see
Section 4.1.3).
```

#2 - 2023-05-03 16:04 - Holger Just

- Subject changed from Email Notifications: to Email Notifications: Email Notifications: trigger rspamd symbol for bad HELO

- Description updated

- Category set to Website (redmine.org)

I'm editing the issue with the details from #note-1

#3 - 2023-05-03 16:14 - Holger Just

- Assignee set to Jean-Philippe Lang

Here, the MTA must be configured to use the external hostname of the server as a HELO. For that to work correctly, the following steps are required:

- The mailserver (MTA) must be configured to use use a valid hostname as its HELO name. For psotfix, you can configure this with the smtp_helo_name option on main.conf. This uses the myhostname value by default. Most likely, you thus want to just set myhostname to redmine.org in the main.conf to resolve this.
- The reverse DNS name for the IP address of the sending server must be set to this name, thus probably to redmine.org. As the server is hosted by Hetzner, you can change this in the in the server admin interface at https://robot.hetzner.com at the respective server -> IPs and click on the text field at right next to the correct IP address.
- The DNS name configured for the IP address must again resolve back to the IP. This is currently the case when using redmine.org.