

Re: exim HELO=fully qualified host name?

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2004-03/0300.html>

From: Derrick 'dman' Hudson (dman_at_dman13.dyndns.org)

Date: 03/02/04

Date: Tue, 2 Mar 2004 12:48:47 -0500

To: Debian-User <debian-user@lists.debian.org>

On Tue, Mar 02, 2004 at 04:31:22PM +0100, Vincent Lefevre wrote:

| On 2004-03-02 09:02:23 -0500, Derrick 'dman' Hudson wrote:

| > RFC 2821, section 4.1.1.1 Extended HELLO (EHLO) or HELLO (HELO)

| >

| > The argument field 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 [...], the

| > client SHOULD send an address literal

| >

| > If the client gives a domain name that is not fully-qualified, it

| > violates the specification. Therefore it is bad data.

|

| I was talking more about the resolution of the FQDN (when the client

| gives a valid FQDN).

Oh, ok, I thought you were speaking more generally about the checks that I perform.

| > | Same problems with machines on private networks, when NAT is used.

| >

| > Those machines could have domain names, although they might not be

| > listed in the public DNS.

|

| This is my case at home (ay.vinc17.org, which is resolvable only in

| my private network, and refusing my messages just because the server

| can't resolve it is a bad idea).

I agree here.

| > They could also provide an IP address.

|

| which would be a private address, so not more useful than a random FQDN

| for the server.

True. I originally just wanted to point out that different sites are stricter than others, and some do some really anal DNS and rDNS checks.

Debian-User: Re: exim HELO=fully qualified host name?

|> | Well, I think that requiring a FQDN (i.e. with at least a dot) is even
|> | too much, as the FQDN is completely useless and most spam messages are
|> | sent with a valid FQDN anyway.
|>
|> Many are sent without it. Here are some of my stats from last week :
|> Helo command rejected: Don't use my own hostname (total: 72)
|> Helo command rejected: Invalid name (total: 6)
|> Helo command rejected: localhost? Really? Nah, fix your hosts file. (total: 4)
|> Helo command rejected: need fully-qualified hostname (total: 215)
|> Helo command rejected: Your software is not RFC 2821 compliant (total: 194)
|>
|> That is 491 junk messages I did not receive due to simple sanity
|> checking of the HELO parameter. It works for me.
|
| How do you know they are all junk messages if you only checked the HELO?

An example :

```
Mar 2 11:05:57 dman13 postfix/smtpd[7805]: 725E59F667:  
  reject: RCPT from unknown[82.77.69.187]: 554 <dman13.dyndns.org>:  
    Helo command rejected: Don't use my own hostname;  
    from=<adam.smith@adam-smith.pl>  
    to=<dman@dman13.dyndns.org>  
    proto=ESMTP  
    helo=<dman13.dyndns.org>
```

The log shows the envelope sender and the DNS information regarding the client. I don't manually inspect each entry any more, but when I was first experimenting with the restrictions I did. Also, anyone can contact me via alternate channels in the event that a legitimate message is rejected. (note too that I don't discard the mail, I reject it so that a valid sender will receive the non-delivery notification)

| Before exim was fixed in Debian, several messages I'd sent were rejected
| by some SMTP server.

When the rejects happened you became aware of the issue and you fixed it :-). A problem is never solved before the problem is recognized.

|> It is easy enough for anyone who wants to send mail to either relay it
|> through a provider,
|
| This is what I was doing until I got bored by too many problems with
| my ISP's smarthost:
| 1) it was frequently blacklisted,
| 2) messages could be waiting for hours in the queue (either because
| it was full of spam or because many other messages were blocked
| due to timeout when trying to connect the destination server),
| 3) messages could be rejected if the destination server was down for
| several hours (as a solution of (2)).

Re: exim HELO=fully qualified host name?

Debian-User: Re: exim HELO=fully qualified host name?

I agree – some providers suck. Find a different provider. Note that it is possible to use a different email provider without changing ISP. Note also that handling the mail yourself is one way of finding a different provider, although that (naturally) shifts more administrative work to your plate.

| > or to provide a syntactically valid fully-qualified name or IP
| > address that I don't consider the checks I enforce to be too strict.
| > You're free to not enforce these checks on your own server if you
| > don't want to.
|
| You rules seem to be OK, at least concerning the RFC.

I'm glad you agree :-).

| But before doing any check, I would do some stats first.

Definitely. Each and every site must understand what any given restriction means and what effect it will have and decide for themselves whether or not that restriction fits with their policy. Never just copy some config from a web site or document without first understanding and evaluating it for yourself. :-)

| For instance, I've just seen in my mail that a friend of mine is
| using Apple Mail, which isn't RFC 2821 compliant. Forte Agent, used
| by some of my family, doesn't provide a FQDN (no dot in the HELO
| argument). Ditto for Microsoft Outlook (from a message received in
| some mailing-list).

Ah, this is a subtly different issue. The subtle difference is these programs are all User Agents, not MTAs. My solution for this is to exempt authenticated sessions from restrictions such as the HELO parameter. This allows "stupid" MUAs and their unaware users to avoid the hassle of violating the protocol while still being tough on untrusted sessions. (I do, however, still require user agents to specify valid domains in the sender and recipient)

HAND,
-D

--

A mouse is a device used to point at the xterm you want to type in.
--Kim Alm, a.s.r

www: <http://dman13.dyndns.org/~dman/>

jabber: dman@dman13.dyndns.org

--

To UNSUBSCRIBE, email to debian-user-request@lists.debian.org
with a subject of "unsubscribe". Trouble? Contact listmaster@lists.debian.org

Debian-User: Re: exim HELO=fully qualified host name?

- application/pgp-signature attachment: Digital signature