

## Re: System Log Full And BadMail Out Of Hand

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.applications/2006-03/msg00043.html>

---

- *From:* Robert McCarter <[RobertMcCarter@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:RobertMcCarter@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 31 Mar 2006 07:42:02 -0800
- 

Henning,

I looked at my queue this morning. I had 2100 messages in it. I have the BadMail script running, so It had cleaned out my BadMail folder.

Am I correct in assuming that my Exchange Server (not the perimeter server) sends mail directly to the internet w/o going through the perimeter server? I know how my incoming mail is handled. I am trying to decide whether the "bogus" mail is being originated internally or if I am letting it get through my perimeter server some way or another.

—

Thank you,

Robert

"Henning Krause [MVP]" wrote:

Hello,

no need to send me those logs.

Is your badmail folder still filling up? How many mails are in the Queue folder?

Henning Krause

"Robert McCarter" <[RobertMcCarter@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:RobertMcCarter@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message <news:632AE498-04E8-4657-BDAC-D63F83851C06@xxxxxxxxxxxxxxxxxxxxx>

Your assumption was correct. I set the LDAP on the perimeter server. However, my system log on the perimeter server is still growing as well as the IIS Log File on the perimeter server. Would it be helpful if I sent you the log file?

Re: System Log Full And BadMail Out Of Hand

--

Thank you,

Robert

"Henning Krause [MVP]" wrote:

Hello,

when I understood you correctly, you are receiving your email on the following way:

Internet --> Perimeter Mail server (GFI Mail essentials)  
--> Internal  
Exchange Server

If you enabled LDAP routing on the perimeter mail server, you are fine.

If you enabled LDAP routing on your internal mail server, you have nothing won, because the GFI Mail Essential will still accept all inbound mails, because it does not know which one to reject.

Greetings,  
Henning

"Robert McCarter"

<RobertMcCarter@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in

message

[news:1D3419CC-2694-4B9A-92C2-193460AEDC26@xxxxxxxxxxxxxxxxxxxx](mailto:news:1D3419CC-2694-4B9A-92C2-193460AEDC26@xxxxxxxxxxxxxxxxxxxx)

Henning,

If I am understanding you correctly, you wanted me to Enable LDAP routing under the LDAP tab of the Default SMTP Server properties. I set this up as a test.

Re: System Log Full And BadMail Out Of Hand

If this is not what you were talking about, please clarify. As a test, I sent a mail to a non-existent user in my domain and received an NDR (sent from a personal e-mail account).

Thank you for your help.

—  
Thank you,

Robert

"Henning Krause [MVP]" wrote:

Hello Robert,

if your perimeter server can do an LDAP lookup, it can do this to reject invalid recipients.

Enabling this feature on your internal server is no help, because GFI Mail-Essentials is a relay server, AFAIK.

Most likely, you are suffering a SPAM attack. Not uncommon.

A smarter Anti-spam solution could also help to mitigate the problem.

Greetings,  
Henning Krause

"Robert McCarter"  
<RobertMcCarter@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in  
message  
[news:F0C372F5-1A10-474B-A281-6071F870813D@xxxxxxxxxxxxxxxxxxxx](mailto:news:F0C372F5-1A10-474B-A281-6071F870813D@xxxxxxxxxxxxxxxxxxxx)

Re: System Log Full And BadMail Out Of Hand

Hello,

I have an Exchange 2000 Server receiving e-mail from a perimeter server running GFI MailEssentials v12. On my perimeter server, my system log is filling up about every day or two. Also, the BadMail folder in Inetpub\mailroot\badmail is filling up rapidly. It is not uncommon to have 100,000 items in the folder after two days or so.

The messages filling my system log are typically like the following:

EventID:4000  
Message delivery to the remote domain "xxx.xxxxx.xxx" failed for

Re: System Log Full And BadMail Out Of Hand

the  
following  
reason: The  
remote  
server did  
not respond  
to a  
connection  
attempt.

On the  
perimeter  
server, I  
turned on  
logging  
with IIS  
Log  
Format. I  
viewed  
the log file  
with Excel  
in a CSV  
format. I  
notice all  
types of  
bogus  
addresses in  
the file. The  
file also  
grew at an  
alarming  
rate (1000  
lines  
or  
so after only  
5 minutes).  
I did not  
understand  
the columns  
as they  
were  
not  
labeled with  
a header  
row so I  
was unable  
to interpret  
the results  
of  
the  
log

Re: System Log Full And BadMail Out Of Hand

file.

I used the  
command  
line Telnet  
test to  
ensure that  
my mail  
server  
was  
not  
set up as an  
open relay.

Can anyone  
give me any  
ideas or  
clues as to  
how to  
ascertain  
where  
the  
e-mail is  
originating  
(internal  
due to  
spyware or  
virus, or  
coming  
in  
from  
an  
external  
source).

Also, is  
there any  
way to  
totally  
dump any  
messages  
that are  
addressed  
to  
users that  
don't exist  
in my  
organization  
such as  
"fido@xxxxxxxxxxxxx"  
where

Re: System Log Full And BadMail Out Of Hand

no user  
named  
"fido"  
exists.

Thank you  
for any help  
you can  
give. This is  
driving me  
nuts.

--  
Thank you,

Robert