

RE: Exchange, BadMail Folder

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-03/msg03131.html>

- *From:* v-jaluo@xxxxxxxxxxxxxxxxxxxxxxxx ("Jacky Luo [MSFT]")
 - *Date:* Thu, 22 Mar 2007 08:07:30 GMT
-

Hi Robb,

Thanks for posting here.

From the description, I understand the issue is that the badmail folder is always growing after you have removed files from folder and unplug server from network. If I am off base, please don't hesitate to let me know.

I assume that the folder you mentioned is C:\Program Files\Exchsrvr\Mailroot\vis 1\BadMail folder. The BadMail folder is used to collect the undeliverable messages. Please try the following steps to remove the contents in this folder:

1. Open Windows Explorer, Navigate to C:\Program Files\Exchsrvr\Mailroot\vis 1\ Right-click BadMail folder and choose "Rename". Rename this folder to BadMail1.
2. Create a new folder named "BadMail".
3. Press Shift+Del keys to delete BadMail1 folder.

Furthermore, Please refer to the following KB article to clean up the SMTP queue.

How to block open SMTP relaying and clean up Exchange Server SMTP queues in Windows Small Business Server
<http://support.microsoft.com/kb/324958/en-us>

Clean up the Exchange Server's SMTP queues

Warning During this process, ALL messages that are destined for external SMTP recipients are deleted. Internal e-mail and incoming e-mail from the Internet are not affected. The settings below are temporary and steps to undo these changes will be included later in this section.

Note A webcast is available that demonstrates how to clean up the Exchange

RE: Exchange, BadMail Folder

Server's SMTP queues. To view this webcast, click the following link:

http://support.microsoft.com/servicedesks/ShowMeHow/101904_3.aspx
(http://support.microsoft.com/?scid=http%3a%2f%2fsupport.microsoft.com%2fservicedesks%2fshowmehow%2f101904_3.aspx)

1. In Exchange System Manager, click SmallBusiness SMTP Connector under Connectors. This phase requires an SMTP connector. If the Exchange server does not have an SMTP connector, create one. To do this, follow these steps: a. Right-click Connectors, click New, and then click SMTP Connector.

b. On the General tab, type a temporary name (Temp Connector, for example) in the Name box.

c. Click Add at the bottom, select the server name and its associated SMTP Virtual Server, and then click OK.

d. Click Address Space.

e. Click Add, click SMTP, and then click OK.

f. In the Internet Address Space Properties dialog box, leave the default settings (E-mail domain * and Cost 1), and then click OK.

g. Click the General tab, and then go to step 4.

2. Right-click SmallBusiness SMTP Connector, and then click Properties. If you have more than one SMTP Connector, the one that you want to work with in the following steps is the one that contains the "*" (asterisk) for the SMTP address on the Address Space tab.

3. Click the General tab. Make a note of all the settings on this tab. You have to return these settings later in this article.

4. Click Forward all mail through this connector to the following smart hosts.

5. In the field provided, type a false IP address and enclose it in brackets. For example, type [99.99.99.99].

6. Click the Deliver Options tab .

7. Click Specify when messages are sent through this connector.

8. In the Connection Time list, click Run daily at 11:00 PM.

9. Click OK to close the SMTP Connector Properties dialog box.

10. Expand Servers, expand Servername, expand Protocols, expand SMTP. Right-click the Default SMTP Virtual Server, and then click Stop.

11. It may take several minutes for the SMTP Virtual Server to stop. After the Default SMTP Virtual Server has stopped, right-click the Default SMTP Virtual Server again, and then click Start. It may take several minutes for the Default SMTP Virtual Server to start.

12. After the Default SMTP Virtual Server has started, wait about 10 minutes.

Now the Default SMTP Virtual Server can re-enumerate the messages and put them in a single queue for the SmallBusiness SMTP Connector or for the one that you named when you created it in step 1.b.

13. After about 10 minutes, expand Default SMTP Virtual Server, and then click Queues.

14. Note the total number of messages on the right next to the Small Business SMTP Connector.

RE: Exchange, BadMail Folder

This number has to stabilize so that all the messages can be deleted at the same time.

15. Right-click Queues, and then click Refresh approximately every 15 minutes.
16. Repeat step 15 until the total number of messages remains constant.
17. Locate the queue for the SmallBusiness SMTP Connector. The queue is indicated by the small red clock on the yellow folder icon.
18. Depending on your version of Small Business Server installation, follow the appropriate section to delete the messages from the queues: ? Small Business Server 2003: Right-click SmallBusiness SMTP Connector, and then click Find Messages. In the corresponding box, click the dropdown and select an appropriate number in Number of messages to be listed in the search. Click Find Now. In the results, select all the messages (SHIFT+PAGE DOWN). Right-click the selected messages, and then click Delete All Messages (No NDR).
? Small Business Server 2000: Right-click SmallBusiness SMTP Connector, and then click Delete All Messages (No NDR).
19. Click Yes when you are prompted with the question of whether to delete messages in the selected queue. Deleting these message may take some time, depending on the number of messages in the queue.
20. After the messages are deleted, right-click Queues, and then click Refresh.
21. Note the total number of messages for the SmallBusiness SMTP Connector queue. The number is zero.
22. Wait approximately 5 minutes, and then refresh Queues again. The goal is to have the number of messages in the SmallBusiness SMTP Connector queue reach zero and stay at zero. If this number increases, the Exchange server is still processing messages for external delivery through the SmallBusiness SMTP Connector. Repeat this step until the number stabilizes again.
23. Repeat steps 19 through 23 until the number of messages in the SmallBusiness SMTP Connector queue is consistently zero. When it is, the Exchange server's SMTP queues have been purged of the unsolicited commercial e-mail.

After Exchange has been cleaned of the unsolicited commercial e-mail, you have to undo the changes that you made in steps 2 through 8. To undo the changes, follow these steps: 1. In Exchange System Manager, expand Connectors, right-click the SmallBusiness SMTP Connector, and then click Properties.

If you created a temporary SMTP connector in step 1, click Delete instead of Properties, and then go to step 7.

2. On the General tab, change these settings to those documented in step 3 under Clean Up the Exchange Server's SMTP Queues.
3. Click the Delivery Options tab.
4. Verify that Specify when messages are sent through this connector is selected.
5. In the Connection Time list, click Always Run.

RE: Exchange, BadMail Folder

6. Click OK.
7. Expand Servers, expand Servername, expand Protocols, and then expand SMTP. Right-click Default SMTP Virtual Server, and then click Stop.
8. After the SMTP Virtual Server has stopped, right-click Default SMTP Virtual Server again, and then click Start.

and make sure you block open SMTP relaying.

In addition, the messages in this folder could be caused by a spam attacking. The external Spam servers send e-mails with the inexistent destination addresses such as abc@xxxxxxxxxxxxxxxx 123@xxxxxxxxxxxxxxxx Since these mail addresses cannot be resolved in Exchange server, the server will send NDR notifications to the sender. However, the spams always use a fake e-mail address as the sender address, the outgoing NDR notifications will be stuck in the SMTP queue and finally, the messages will be moved to BadMail folder. Here, I would like to suggest you check the SMTP queues. Do you see many NDR notifications stuck in the queue?

1. Open Exchange System Manager, navigate to "Servers"<ServerName>"Queues". In the right panel, do you see a large amount of queues?
2. If so, please double-click the queue, open the message in the queue. What's the sender of these messages? Does it seem like postmaster@xxxxxxxxxxxxxxxx ?
3. If there are many NDR messages stuck in the SMTP queue, your mail server is probably attacked by NDR attacking. Please try the following steps to filter the unresolved e-mails:
 - a. Enable reverse DNS lookup on the Exchange. Open "Exchange System Manager", navigate to "Servers"<Server Name>"Protocols"SMTP", right-click "Default SMTP Virtual Server"-->"Properties". Click "Advanced" button in "Delivery" tab. Check "Perform reverse DNS lookup on incoming messages" box and then click "OK" to close the dialog boxes. Restart the SMTP virtual server.
 - b. We can configure the Exchange server to drop the connection of the unknown user delivery by using the recipient filtering. Open "Exchange System Manager", expand "Global Settings", right-click "Message Delivery" and click "Properties". In the window, click "Recipient filtering" tab and check "Filter recipients who are not in the Directory" box. Click "OK". Navigate to "Servers"<Server Name>"Protocols"SMTP", right-click "Default SMTP Virtual Server" and click "Properties". In the properties window, click "Advanced" button and click "Edit" in the advanced window. Check "Apply Recipient Filter" box and click "OK". Restart the SMTP virtual server.

I hope the above information helps.

I appreciate your time. I am happy to be of assistance and look forward to

RE: Exchange, BadMail Folder

your reply.

Have a nice day!

Best regards,

Jacky Luo (MSFT)
Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

PLEASE NOTE: The partner managed newsgroups are provided to assist with break/fix issues and simple how to questions. We also love to hear your product feedback! Let us know what you think by posting

from the web interface: Partner Feedback
from your newsreader: microsoft.private.directaccess.partnerfeedback.

We look forward to hearing from you!

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from this issue.

This posting is provided "AS IS" with no warranties, and confers no rights.

.