

## Check mail in Exchange 2007 (Part 2)

In part one of this article we looked at the default configuration of message tracking within Exchange 2007 and how to change those settings using PowerShell cmdlets. You can remember those major changes in Exchange 2007 mail checking on the server

**In part one of this article we looked at the default configuration of message tracking within Exchange 2007 and how to change those settings using PowerShell cmdlets. You can remember those major changes in Exchange 2007 mail checking on their Exchange 2003 replica :**

1. Message checking is enabled by default.
2. Recording is also enabled by default
3. The default records are retained for 30 days.

There are really many changes but we don't go into the first part. In this second part, we will look at the contents of the log file then how to find them in practice.

### What is a record?

You can see Figure 1 below, the log directory is shown with two log files contained within it. A familiar message tracking log directory is shown when I use the cmdlet in part one of the article to change the log path to D: Tracking Logs. The first thing you should notice is the file names. They are set in the following formats:

```
MSGTRKyyyyymmdd-n.log  
MSGTRKMyyyyyymmdd-n.log
```

This format gives us the following information:

1. **MSGTRK** is located at the top of the log files in Hub Transport or Edge Transport server.
2. **MSGTRKM** is located at the beginning of the log files in the Mailbox server.
3. **yyyy** is a number that represents the number of years of the file created.
4. **mm** is its number of months.
5. **dd** is the number of days
6. **n** is the increment count in units of days.

You can see in Figure 1, where they have log files that start with both MSGTRK and MSGTRKM on the same server. Therefore, you can reduce both the Hub Transport and Mailbox server configured on this single server. The first log file created is named MSGTRK20061217-1.log. When the file is the largest, 10MB is the default value, the next record will be named MSGTRK20061217-2.log.

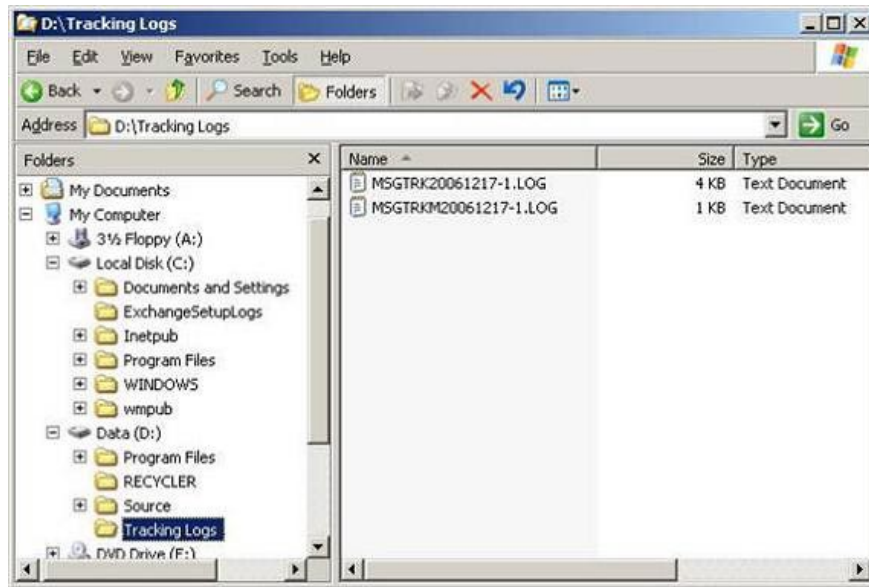


Figure 1 : Log file name

Figure 2 shows the contents of a sample message tracking log file taken from a Hub Transport server. The first thing to note here is that the data is in CSV format (Comma Separated Value: comma separated values). Figure 3 is a comparison of this problem with the sample record of Exchange 2003.

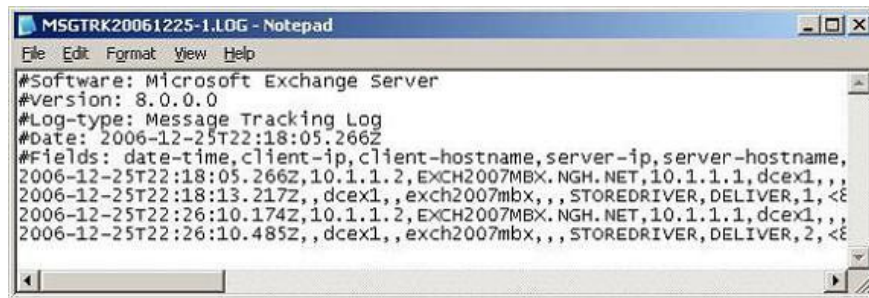
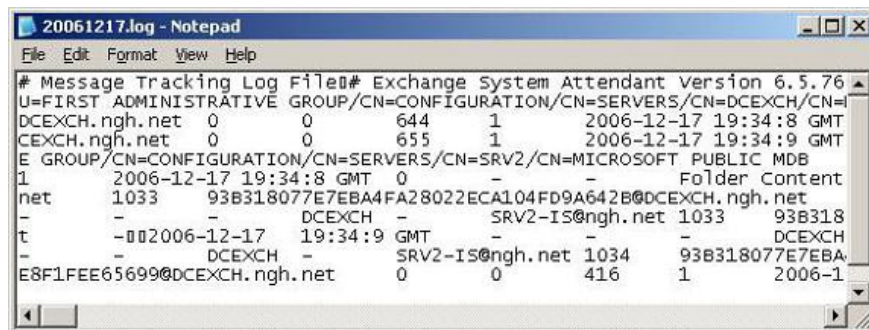


Figure 2 : Content of the message tracking log file of Exchange 2007.



*Figure 3* : Content of the message tracking log file of Exchange 2003.

From Figure 2 you will see that, the first few lines of the log file contain the file system information. It includes the following order header: #Software, #Version, # Log-Type, #Date, #Fields (# software, # versions, # types, # days, # fields). Explain these headers as follows:

1. **#Software** . This is the name of the application that created the log file, in which case they are set to the value of Microsoft Exchange Server.
2. **#Version** . This is the version number of the application that created the log file. In my test with a trial version of Exchange 2007 RTM, this value was set to 8.0.0.0. This issue is also a case of Exchange 2007 Beta 2.
3. **# Log-Type** . This is the type of log file created by the application, in which case it is set up on the Message Tracking Log
4. **#Date** . This is the date and time that the log file was created and expressed in the format **yyyy-mm-ddThh: mm: ss.fffZ** . You can almost guess that yyyy is the year, mysql-z is the month and the right, hh for the hour and mysql-zrm seconds and minutes.
5. **#Fields** . This is a field list of comma-delimited lists, the name of the field is date-time, client-ip, client-hostname, server-ip, server-hostname, source-context, connector-id, source, event-id, internal-message-id, message-id, recipient-address, recipient-status, total-bytes, recipient-count, related-recipient-address, reference, message-subject, sender-address, return-path, message-info.

We won't go into too much detail for the fields inside the article that have a description with help files. To be honestly friendly, with the exception of a few, the great majority must show it more brightly and if you can write and send some messages or reports you can work through each school value to Indicates what is happening.

## Search for a record

As you can remember in part one of this article, settings can only be configured using the Exchange Management Shell (EMS); No method can be configured through the Exchange Management Console (EMC). If you prefer to use graphical tools when administering Exchange, you can use the Message Tracking tool to check messages to find the contents of the log files. Obviously you can use EMS but you should be aware that there are some differences between them. We will introduce both of these methods here and show the differences between them.

First, look at using the Message Tracking tool to find log files. There are many reasons why we introduced you to this tool first and that is simply because the corresponding cmdlet that you ran will be displayed inside this tool, which makes it easy for you to use it. Use EMS later. Here's how to run the Message Tracking tool.

1, Run the Exchange Management Console.

2, In the window on the left, select **Toolbox** .

3, In the middle of the results section, select **Message Tracking** from Mail in the tools area.

4, Now you can select the **Open** tool option on the right or you can right-click Message Tracking in the results section and select the Open tool from the menu. This way if you do not see the Action Pane, it may be due to the current hidden view via the View menu option inside the EMC attached software module. Click **View** , then **Customize** . and in the **Customize View** window you have to make sure that the **Action** option is selected.

5, A new window will open showing you Microsoft Exchange Troubleshooting Assistant. If this is the first time you have chosen this option, you can skip a few screens to choose to upgrade. Finally you should stop at the screen as shown in Figure 4 below.

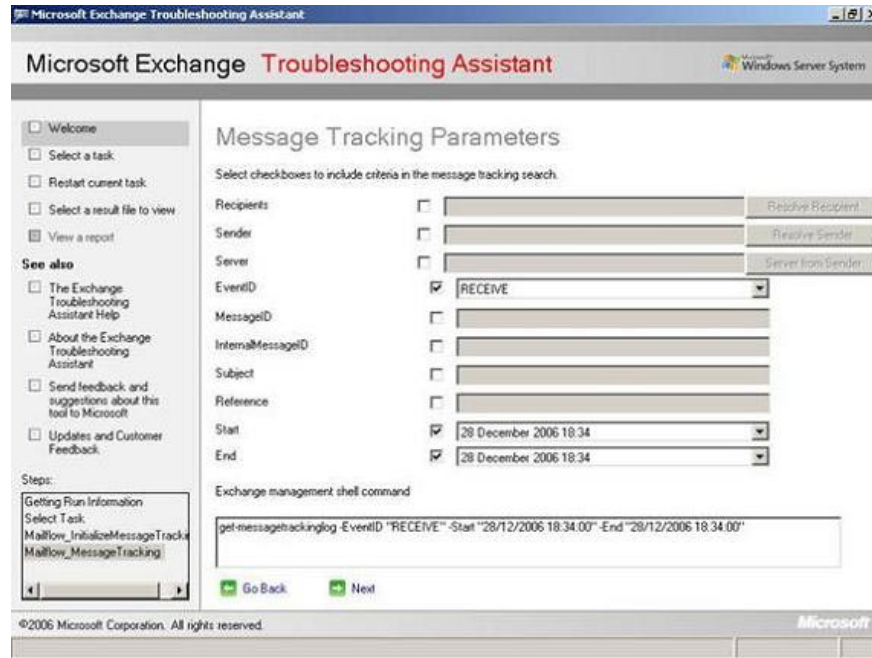


Figure 4 : Notification test tool

Here you can fill in relevant search filters such as senders, recipients, mailing topics . There are some sections here that you should pay attention to:

1. At the bottom of the screen, the Exchange management command area shows the corresponding cmdlet that you can perform the same search through EMS.
2. Note Figure 2 about the date and time of saving test records in Coordinated Universal Time (UTC) format when the search shown in Figure 4 uses local time and date formats. The mail checker tool will perform the conversion process for you.
3. The EventID search field has many different options such as **RECEIVE** , used to find messages received by the relevant server, or **DELIVER** , which is used to search for messages distributed to each mailbox.

For example, to perform a simple search for messages with the word 'hello' within the subject line, you must perform at least two tasks in Figure 4. You first need to click on the Subject check box and supply the keyword 'hello' to the next field next to it. Next, you need to make sure that the end date must be after the start date. By default these days are the same and cannot change the final day results while performing a search. In some cases, if you have separate Mailbox and Hub Transport servers and are performing a search from the Mailbox server, you will need to change the EventID to the SUBMIT option, when Mailbox servers only have **SUBMIT** events. . These problems are also used to check when Mailbox servers submit messages to the Hub Transport server. You will no doubt call from your Exchange 2007 reading about whether all mail goes through Hub Transport servers. Given that you have entered valid details and clicked on the Next button, you will see a screen similar to the one shown in Figure 5 below.

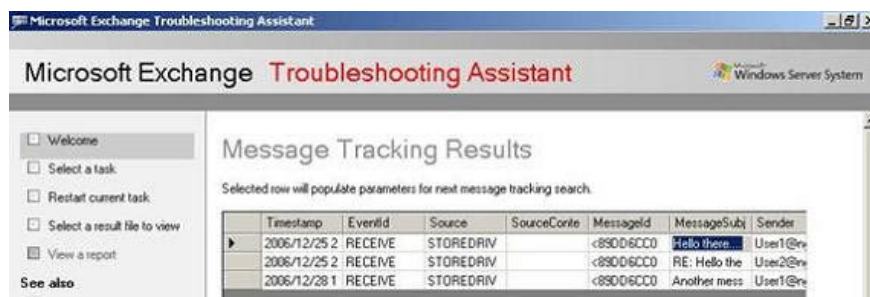


Figure 5 : Results through the mail test tool.

Note that the text that says the selected row will populate the parameters for the next message check. This shows that whatever is selected as the message subject line in Figure 5 will be used as the basis of the next search when you click the **Next** button at the bottom of the screen.

A notable extension here with checking mail depends on the **Microsoft Exchange Transport Log Search service**. You may have seen on Exchange 2007 a large number of Exchange-related services within the Services applet. Finding test logs requires running Microsoft Exchange Transport Log Search service. If the service is not running, you will only see the error message shown in Figure 6. Note that if you disable this service for any reason, the ability to search the log files will be affected. ; There are no Exchange functions affected.

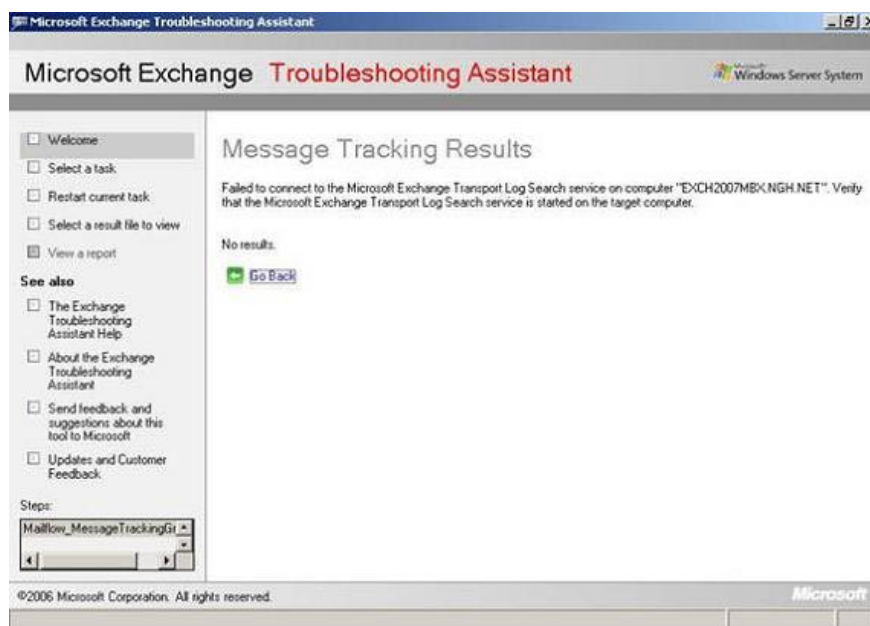


Figure 6 : Error checking mail

Now let's look at using EMS to search log files. This function focuses around using the **Get-MessageTrackingLog** cmdlet. You can use this cmdlet without any options, which will result in 1000 items of items being displayed. therefore, many parameters are added to the cmdlet to enrich our search. You can limit the number of inputs returned by using the ResultSize result size parameter. To repeat our previous search, we can simply paste into the cmdlet, so the Message Tracking tool will show us. This is shown below:

```
Get-MessageTrackingLog -EventID 'RECEIVE' -MessageSubject 'hello' -Start '01/12/2006 00:00:00'
-End 'December 28, 2006 18:50:00'
```

Note that in our example, the start and end dates are displayed in UK format.

```
Machine: dcexl | Scope: NGH.NET
[PS] C:\Documents and Settings\Administrator>Get-MessageTrackingLog -EventId "RECEIVE" -MessageSubject "hello" -Start "01/12/2006 00:00:00" -End "28/12/2006 18:50:00"
EventId Source Sender Recipients MessageSubject
-----
RECEIVE STORE... User1@ngh.net <User2@ngh.net> Hello there...
RECEIVE STORE... User2@ngh.net <User1@ngh.net> RE: Hello there...
RECEIVE STORE... User1@ngh.net <User2@ngh.net> Another message ...

[PS] C:\Documents and Settings\Administrator>
```

Figure 7 : Mailing test results via EMS

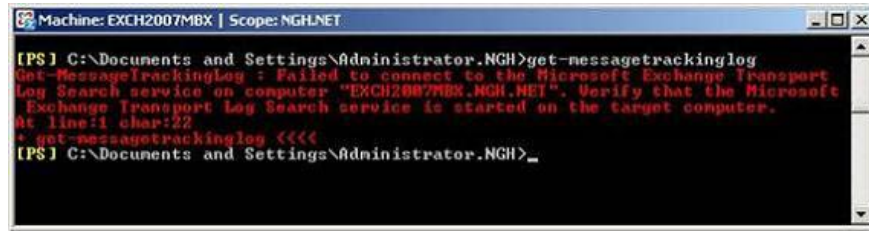
You will see in Figure 7 that the 5 default fields shown are EventId, Source, Sender, Recipients and MessageSubject. If you use the format list or **fl** formatting cmdlet, you can get more information. For example, Figure 8 shows you the details of the first search result listed in Figure 7. Obviously, you also have the option to resend the cmdlet results to the text file by appending data. Data like **> 'C: results.txt'** at the end of each cmdlet.

```
Machine: dcexl | Scope: NGH.NET
[PS] C:\Documents and Settings\Administrator>Get-MessageTrackingLog -EventId "RECEIVE" -MessageSubject "hello" -Start "01/12/2006 00:00:00" -End "28/12/2006 18:50:00" | fl
Timestamp : 25/12/2006 22:18:05
ClientIp : 10.1.1.2
ClientHostname : EXCH2007MBX.NGH.NET
ServerIp : 10.1.1.1
ServerHostname : dcexl
SourceContext :
ConnectorId :
Source : STOREDRIVER
EventId : RECEIVE
InternalMessageId : 1
MessageId : <89DD6CC0D55DF34A8740578DE7C970C41EFD0EXCH2007MBX.NGH.NET>
Recipients : <User2@ngh.net>
RecipientStatus : <>
TotalBytes : 3217
RecipientCount : 1
RelatedRecipientAddress :
Reference :
MessageSubject : Hello there...
Sender : User1@ngh.net
ReturnPath : User1@ngh.net
MessageInfo : 041:
```

Figure 8 : Mail test results using the EMS format list

Logical reasoning finds that this gives you the most sense of using the Message Tracking tool first and seeing what the corresponding cmdlet is. When you are comfortable with the relevant cmdlet, you can choose to use EMS only. However, this choice is yours.

To complete the process of considering using EMS to find log files, you should not forget that if the Microsoft Exchange Transport Log Search service is not running, an error will be encountered in the same way as you implemented within the Message Tracking tool. In the case of EMS, you will see the error shown in Figure 9.



```
Machine: EXCH2007MBX | Scope: NGH.NET
[PS] C:\Documents and Settings\Administrator.NGH>get-messagetrackinglog
Get-MessageTrackingLog : Failed to connect to the Microsoft Exchange Transport
Log Search service on computer "EXCH2007MBX.NGH.NET". Verify that the Microsoft
Exchange Transport Log Search service is started on the target computer.
At line:1 char:22
* get-messagetrackinglog <<<<
[PS] C:\Documents and Settings\Administrator.NGH>_
```

Figure 9 : Error finding Message Tracking (EMS)

## Difference

Is there any difference between using the Message Tracking tool and EMS? Yes, yes, you will first see as in Figure 4, the Message Tracking tool provides the server field as a search filter. If you use the server parameter inside EMS, it is actually used to name the server that the message tracking log files you expect to find.

Alternatively, EMS has a Reference search filter (Reference) not contained within the Message Tracking tool. This search filter is linked to the reference field within the actual record, which includes information such as the DSN (Delivery Status Notification) ID messages.

## summary

Through the two parts of the article, we gave you a useful working knowledge on how to check messages that are configured by default, how to change the configuration and how to perform searches. basic knowledge. Of course, finding logs for information will be different for each reader, so we recommend that you use some Message Tracking tools and command line interfaces.

You finished reading the article "**Check mail in Exchange 2007 (Part 2)**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.