Microsoft Exchange 2003 – Message Tracking

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will give you a Step by Step solution to track the flow of messages within your Exchange Organization with the help of Exchange Message Tracking.

Let's begin

First, we need to enable Message Tracking. We must enable Message Tracking for every server in our Exchange Organization manually or via an Exchange Policy. I will explain both steps.

To enable Message Tracking start the Exchange System Manager and navigate to the Servers object.

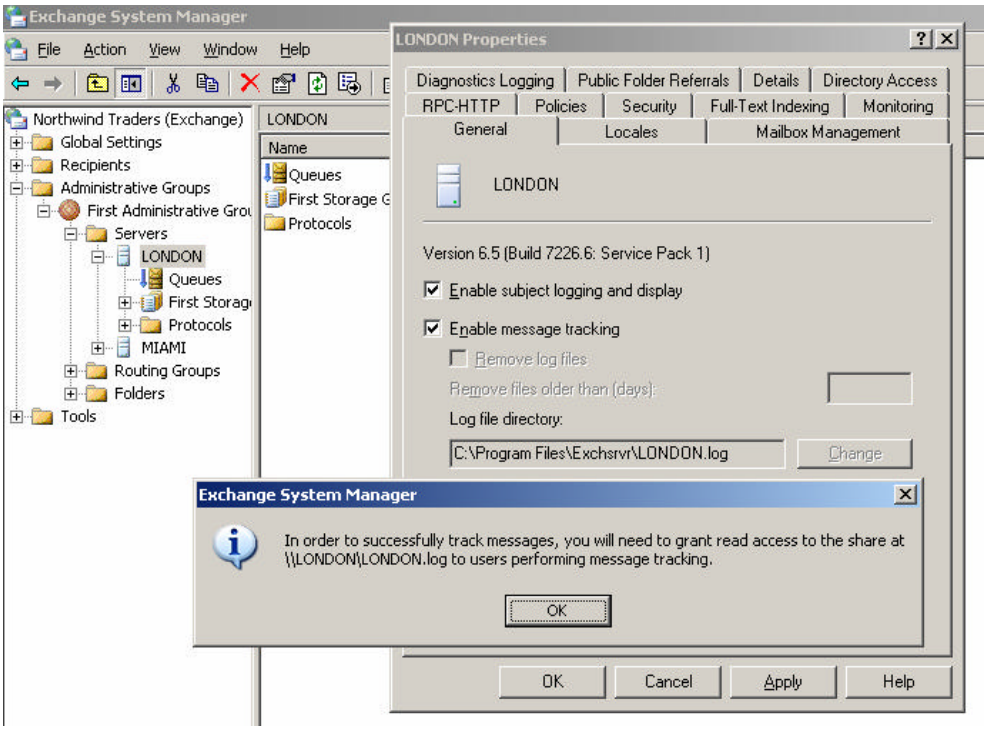

Figure 1: Enable Message tracking for a Exchange Server

Click *"Enable message tracking".* If you want to enable the logging of the subject lines from every mail click *"Enable subject logging and display".* Note that enabling of subject logging requires substantially more processing po and disk space on highly utilized Exchange Servers with thousands of mail by one hour.

It could be a good idea to "Remove log files" after xx days when you don't want to clear the logfiles manually.

Don't forget to give users who want to perform message tracking read access to the share \\SERVER\SERVER.LOG. Exchange creates this share to save the message tracking logs.

Exchange System Policy

If you have many servers it is a time consuming task to enable Message Tracking for every server. To avoid a manual config, you can create an Exchange System Policy to activate Message Tracking for many servers at the same time.

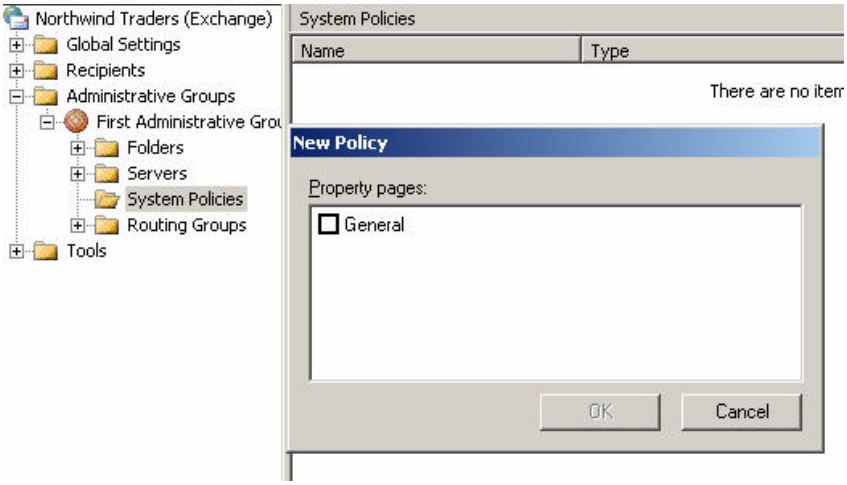

Figure 2: Create a new System Policy

After you named the Exchange System Policy you can enable Message Tracking and subject logging but not the Log file directory because not every server has the same Hard Disk and Partition configuration so Microsoft has disabled this feature in a System Policy.

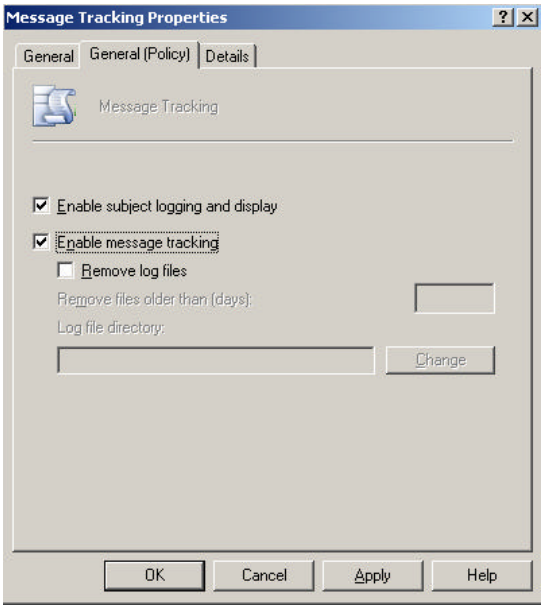

Figure 3: System Policy details

After you have enabled the new System Policy don't forget to make the servers a part of the Policy (manually add the Servers to the Policy).

After you have sent some e-mails through your Exchange Organization, the Message Tracking begins to create a log file. Message Tracking create one log file per day which is named YYYYMMDD.LOG so you can easily find the log files of your interest.

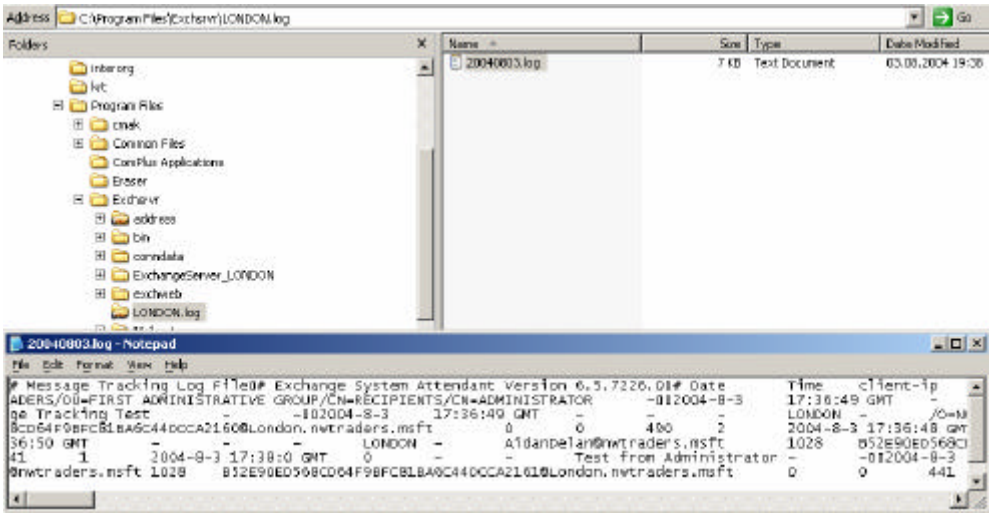

Figure 4: Message Tracking Log files

Message Tracking Center

If you think that you must read boring text files for message tracking you are wrong. Exchange 2003 has a nice Message Tracking Center where you can graphically search for messages within your Exchange Organization.

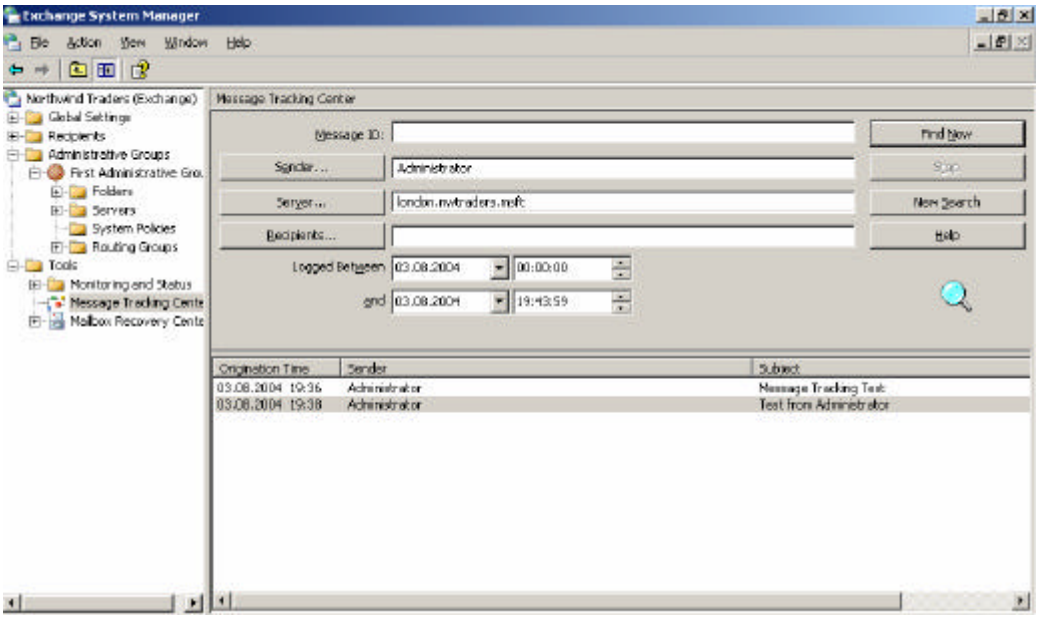

Figure 5: Message Tracking Center

The Message Tracking Center is self explaining.
Select the *Sender* and/or *recipient* of the Message and the logged time between start and end-date.

Click “*Find Now*” to start the search process. The results will be displayed in the Message Tracking detail pane

Click a tracked message and you will get more details:

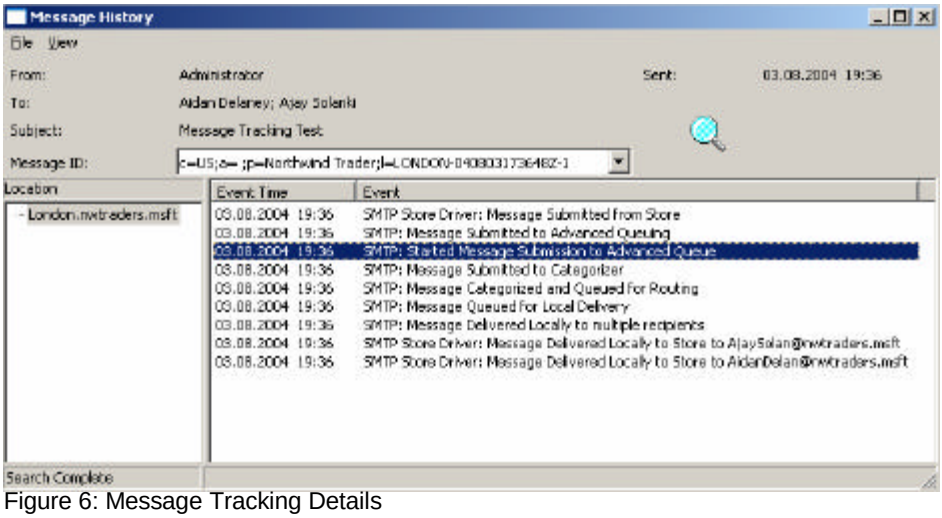

Figure 6: Message Tracking Details

What do we see here?

SMTP Store Driver: message Submitted from Store
- The Message will leave the information store to the SMTP process
SMTP: Message Submitted to Advanced Queuing
- The Message will be queued
SMTP: Message Submitted to Categorizer
- The Categorizer is a process where the message can be customized through event sinks (legal disclaimer)
SMTP: Message Categorized and Queued for Routing
- The Message will be queued for Routing to the destination
SMTP: Message Queued for local Delivery
- Exchange recognizes that the message must delivered locally to the same server and store
SMTP: Message Delivered Locally to multiple recipients
- The Message will send to multiple recipients
SMTP Store Driver: Message Delivered Locally to Store to AjaySolan@nwtraders.msft
SMTP Store Driver: Message Delivered Locally to Store to AidanDelan@nwtraders.msft

The detailed view of the Message is a powerful feature of the Message tracking to see the stations while e-mail delivery.

What is protocolled?

Field number	Field name	Description
1	Date	Date of the event.
2	Time	Greenwich mean time of the event.
3	Client-IP	IP of connecting client.
4	Client-hostname	Hostname of connecting client.
5	Partner-name	Name of the messaging service that the message is handed off to. In Exchange 2000, the service can be: SMTP, X400, MAPI, IMAP4, POP3, STORE.
6	Server-hostname	Hostname of the server that is making the log entry.
7	Server-IP	IP of the server that is making the log entry.
8	Recipient-address	Message recipient (SMTP or X.400 address).
9	Event-ID	Integer corresponding to the Event ID of the action logged, for example: sent, received, delete, retrieve.
10	MSGID	Message ID.
11	Priority	The priority is represented by -1 if low, 0 if normal, 1 if high
12	Recipient-Report-Status	A number representing the result of an attempt to deliver a report to the recipient: 0 if delivered, 1 if not delivered. This is used only for reports (non-delivery reports [NDRs], delivery receipts [DRs]). On other events, it is blank.
13	Total-bytes	Message size (in bytes).
14	Number-recipients	Total number of recipients.
15	Time-taken	Delivery time (in seconds) representing the time it takes to deliver the message. Determined from the difference between the timestamp and time encoded in Message ID. Only valid for messages within the Exchange organization (all versions); there is no requirement to decode other product message IDs such as Sendmail, and so on.
16	Encryption	For the primary body part: 0 if no encryption, 1 if signed only, 2 if encrypted. This is per message, not per recipient.
17	Service-version	Version of the service making the log entry.
18	Linked-MSGID	If there is a MSG ID from another service, it is given here to link the message across services.
19	Message-subject	The subject of the message, truncated to 256 bytes.

20	Sender-address	Primary address of the originating mailbox, if known. This could be SMTP, X.400, or Distinguished Name (DN), depending on transport.

Source: http://support.microsoft.com/default.aspx?scid=kb;en-us;246965 (for Exchange 2000)

Links to other Third Party Tracking Software

- MessageStats www.quest.com
- Fortis Software's Exchange Monitor http://www.fortissoftware.com/exchangemonitor/
- eIQ MailAnalyzer http://www.eiqnetworks.com/products/mailserveranalytics.shtml
- PROMODAG Reports http://www.promodag.com/indexmsexchg.asp

Conclusion

Message Tracking is a powerful feature to track every message in your Exchange Organization. I like this feature because it is a powerful troubleshooting instrument to see where the message is gone.

Related Links

How to move Message Logs in Exchange 2003
http://support.microsoft.com/default.aspx?scid=kb;en-us;841089
Message Tracking in a Clustered Environment
http://support.microsoft.com/default.aspx?scid=kb;en-us;327977
Message Tracking Log File description in Exchange 2000
http://support.microsoft.com/default.aspx?scid=kb;en-us;246965
Exchange 2003 Message Transport and Routing Guide
http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/extransrout.mspx