

- Partner

N-REPORTER How do user manage Exchange Server message tracking audit log V 1.1.4



(01-01-01-013) 2015/02/09

Prefac

This document is mainly to introduce how N-Reporter users manage Exchange Server message tracking audit log. The first step is to deploy Exchange message tracking. Secondly, use the Open Source tool, NXLOG Community Edition, to convert the message tracking record into Syslog, and send to N-Reporter. Since there are some difference setting between Windows and Exchange, the deployment of Exchange Management Console(EMC) may be different. The deploy environment of this document is Windows server 2003 64bit with Exchange 2007, Windows server 2008 R2 with Exchange 2010 and Windows server 2012 with Exchange 2013.

Message tracking record is the detailed mail record of all the message transmission including Exchange server with Hub Transport server role, Mailbox server role or the computer with Edge Transport server role. The Exchange Server with Client Access server role or Unified messaging server role does not have message tracking record. The deployment of this document is for Exchange Server with Hub Transport server role or Edge Transport server role.

Note: Exchange Server enable message tracking logging by default.

Contents:

1	Set up Exchange Server 2007 message tracking log	. 2
2	Set up Exchange Server 2010 message tracking log	. 6
3	Set up Exchange Server 2013 message tracking log	. 9
4	Set up NXLOG	12

1 Set up Exchange Server 2007 message tracking log

You can set up message tracking log file by either [Exchange Management Console] or [Exchange Management Shell].

1. Using Exchange Management Console

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All programs] → [Microsoft Exchange Server 2007]
 - → [Exchange Management Console].

Administrate	or and a second s	
Manage Your	Server 🥑 My Computer	
Command Pro	🥸 Windows Catalog 🌯 Windows Update	•
妏 Windows Expl	Microsoft Update Accessories	
🧭 Microsoft Visual	Administrative Tools	•
Notepad++	Internet Explorer Outlook Express	
Event Viewer	Remote Assistance Microsoft Silverlight 3 SDK	
Notepad	Microsoft SQL Server 2008 Microsoft Sync Framework	
Configure Your Wizard	Microsoft Visual Studio 2010 MinRAR I	
Computer Mana	Intersect Alliance Notepad++ Windows RowerShell 1.0	
All <u>P</u> rograms	Microsoft Exchange Server 2007	Exchange Management Console
🕴 Start 🛛 🚱 🥥	Log Off 🚺	s 🔯 Exchange Management Shell

(3) Click [Server Configuration] → [Exchange Server], here it is "WIN2K3ENG-AD" → Right click → Properties °

🔀 Exchange Management Console						
<u>File Action View H</u> elp						
Microsoft Exchange	🚦 Server Configurat	ion	1 object	Actions		
	Y Create Filter			Server Configura	tion	•
Mailbox		<u></u>		📃 Modify Configu	ration Domain Controller	
Client Access	WIN2K3ENG-AD	Kole Hub Trai		Evport List	1	
		1	Manage <u>Mailbox</u> Server	r Role Server Role		•
E Recipient Configuration			Manage Hub <u>T</u> ransport	: Server Role		
			Manage Diagn <u>o</u> stic Log	ging Properties		
		<u>с</u>	Properties			
			Help		Server Dole	
			Пеф	B. Managa Client		
					ALLESS DERVER KUIE	
				Manage Hub Ir	ansport Server Role	
				Manage Diagno	stic Logging Properties	
				V Properties		
				🔮 Help		
	µ			1		

(4) Click [Log settings] → Check [Enable message tracking logging] → Set the message tracking log file. Default setting is :
 "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking" °
 Click [OK], complete.

WIN2K3ENG-AD Properties
General System Settings External DNS Lookups Internal DNS Lookups Limits Log Settings
Message tracking log
Enable message tracking logging
Message tracking log file path:
C:\Program Files\Microsoft\Exchange Server\TransportRol <u>B</u> rowse
Connectivity logging
Enable connectivity logging
Connectivity log file path:
C:\Program Files\Microsoft\Exchange Server\TransportRol
Protocol log
Send connector protocol log file path:
C:\Program Files\Microsoft\Exchange Server\TransportRoles\ Browse
Receive connector protocol log file path:
C:\Program Files\Microsoft\Exchange Server\TransportRoles\ Browse
OK Cancel Apply Help

2. Using [Exchange Management Shell] To Set Up

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All Programs] → [Microsoft Exchange Server 2007] →

[Exchange Management Shell].

Administrate	or -			
Manage Your	Server 💈	My Computer		
Command Pro	🥸 Windows Cata 🍓 Windows Upda	log ite	•	
💢 Windows Expl	Accessories	ate ►		
🧭 Microsoft Visual	Administrative Startup	Tools		
Notepad++	 Internet Explo Outlook Express 	rer SS		
Event Viewer	Microsoft Silve	ance rlight 3 SDK		
Notepad	Microsoft Sync	Framework		
Exchange Mana Console	WinRAR	* 5(3d0 2010		
Configure Your Wizard	Intersect Allar Notepad++			
All Programs		ange Server 2007	🔀 Excha	ange Management Console
	1	🖉 Log Off 🛛 S	😥 Excha	ange Management Shell ange Server Help

(3) Enable message tracking. Type in program:

Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled \$True –MessageTrackingLogPath <LocalFilePath>

or

<LocalFilePath>

<ServerIdentity> is the computer name of Exchange Serve, <LocalFilePath> is the path of message tracking,

Default setting is : "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"

In this example we type in:

Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled \$True -MessageTrackingLogPath "C:\Program

Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"



(4) Check the setting of message tracking record. Type in program:

Get-TransportServer npartner-012a02 | Select-Object *Track*

🚱 Machine: npartner-012a02 Scope: npexchange.loca	l		×					
[PS] C:\>Get-TransportServer npartner-012a02 Select-Object *Track* 🔼 🔼								
MessageTrackingLogEnabled MessageTrackingLogMaxAge MessageTrackingLogMaxDirectorySize MessageTrackingLogMaxFileSize		True 30.00:00:00 250MB 10MB						
MessageTrackingLogPath MessageTrackingLogSubjectLoggingEnabled	:	C:\Program Files\Microsoft\Exchange S erver\TransportRoles\Logs\MessageTrac king True						

2 Set up Exchange Server 2010 message tracking log

You can set up message tracking log file by either [Exchange Management Console] or [Exchange Management Shell].

1. Using Exchange Management Console:

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All programs] → [Microsoft Exchange Server 2010] →

[Exchange Management Console] ·



(3) Click [Microsoft Exchange On-Premises]→ [Server Configuration] → [Hub Transport].
 Click [Exchange Server], here it is "MAIL." Then, click [Properties].

😣 Exchange Management Console				🔀 Exchange Management Console							
File Action View Help											
Microsoft Exchange	🍺 Hub Transport		1 object	Actions							
Microsoft Exchange On-Premises (mail.exchange.	Treate Filter			Hub Transport 🛛 🔺 📥							
E Server Configuration		(- ·		📑 Export List							
Mailbox	Name A	Role Hub Transport, Client Acc	Version 14-3	View							
E Client Access	- Contraction of the second se	That mansport, client Acc	Version 1445								
Unified Messaging		\mathbf{X}									
Recipient Configuration	•		F	И нер							
1 I I I I I I I I I I I I I I I I I I I	- MATI		2 objects								
	Design Constant	-	2 00,000	MAIL							
			1	늘 Manage Mailbox Role							
	Name A	Status Enabled		anage Client Access Role							
	Default MAIL	Enabled	\sim 1	🔚 Manage Diagnostic Logging Prop							
				🗔 Enter Product Key							
				2 New Receive Connector							
				Client MAIL							
				U Disable							
				Remove							

(4) Click [Log Settings]. Check [Enable message tracking log], type in [Message tracking log path].

Default setting is "C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking". Click [OK], complete.

IAIL Properties					×			
General Internal DNS I	System S Lookups	ettings Limits	E	xternal DNS Lo Log Se	okups ttings			
Message tracking log Enable message tracking log Message tracking log path: [C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Me								
Connectivity log – Connectivity log C:\Program Fil Protocol log Send protocol log C:\Program Files\ Receive protocol l C:\Program Files\	ectivity log g path: les' Microsoft\Ex path: Microsoft\Excha log path: Microsoft\Excha	ange Server\V1 ange Server\V1	\\/14\T 4\Tran 4\Tran	ransportRoles\L sportRoles\Log sportRoles\Log	-ogs\Cor s\Protoci			
	ОК	Cancel		Apply	Help			

2. Using [Exchange Management Shell]:

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All programs] → [Microsoft Exchange Server 2010] → [Exchange



(3) Enable message tracking. Type in program:

Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled \$True -MessageTrackingLogPath <LocalFilePath>

or

Set-MailboxServer <ServerIdentity> -MessageTrackingLogEnabled \$True -MessageTrackingLogPath <LocalFilePath>

<ServerIdentity> is the computer name of Exchange Server. <LocalFilePath> is the path of message tracking, default setting is

"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking".

In this example, we type in:

Set-TransportServer MAIL -MessageTrackingLogEnabled \$True -MessageTrackingLogPath "C:\Program

Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"

🚱 樓器:mail.exchange.npartnertech.com

198] C:\Windows\system32>Set-TransportServer MAIL -MessageTrackingLogEnabled \$True -MessageTrackingLogPath "C:\Program F iles\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"_

(4) Check the message tracking log deployment. Type in program:

Get-TransportServer MAIL | Select-Object *Track*

<mark>睽</mark> 穩器: mail.exchange.npartnertech.com	-	
[PS] C:\Windows\system32>get-transportse	rver MAIL ¦ select-object *track*	
MessageTrackingLogEnabled MessageTrackingLogMaxAge MessageTrackingLogMaxDirectorySize MessageTrackingLogMaxFileSize	: True : 30.00:00:00 : 1000 MB (1,048,576,000 bytes) : 10 MB (10,485,760 bytes)	
MessageTrackingLogPath MessageTrackingLogSubjectLoggingEnabled	: C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTr cking : True	a

3 Set up Exchange Server 2013 message tracking log

You can set up message tracking log file by either [Exchange Admin Center/EAC] or [Exchange Management Shell]

1. Using [Exchange Admin Center/EAC]:

- (1) Start the server.
- Internal URL: "https://<CASServerName or private IP>/ecp". The internal URL is to access EAC in the organization firewall.
- External URL: "https://<MailHostName or public IP>/ecp". The external URL is to access EAC outside the organization firewall.

```
Here we type in URL: "https://192.168.2.71/ecp", to connect Exchange Admin Center.
```

(2) Type in the Exchange Server administrator and password in the login webpage of Exchange Admin Center(EAC).

🗲 💮 🍕 https://192.168.1.100/ecp/ 🔎 👻 Certificat 🖒 🔤 mailboxes - Microsoft Exch 🗙								
1 Enterprise Office 365								
Exchange admin center								
recipients	mailboxes gro	ups resources co	ntacts shared migration					
permissions	permissions							
compliance management	+- ∕ m ዖ છ	•••						
organization	DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS					
- 9	Administrator	User	Administrator@exchange.npartnertech.com	Administrator				
protection	npartner	User	npartner@exchange.npartnertech.com	Auministrator				
mail flow	shrink	User	shrink@exchange.npartnertech.com	User mailbox Administrator@exchange.npartnertech.c				
mobile				Title:				
mobile								
public folders				work phone:				
unified messaging				Phone and Voice Features				
can/arc				Unified Messaging: Disabled				
3017013				Enable				
hvbrid		1 selec	ted of 3 total					

(3) Click [Server]. Double click Exchange Server. Here we double click "MAIL".

🗲 🕣 🌌 https://192.168.1.100/ecp/ 🔎 👻 Certificat 🖒 🖼 servers - Microsoft Exchange 🗙							
Enterprise Office 365							
Exchange admin center							
recipients	servers	databases	database availability groups	virtual directories certif			
permissions							
compliance management	/ ^ B						
organization	NAME	*	SERVER ROLES	VERSION			
protection	MAIL		Mailbox, Client Access	Version 15.0 (Build 847			
mail flow							
mobile							
public folders							
unified messaging							
servers							
hvbrid			1 selected of 1 total				

(4) Click [transport logs] → Check [Enable message tracking log]. Set the message tracking log path. Exchange 2013 default setting is

"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles \Logs\MessageTracking".

Click [Save], com	plete.	
Ø	Exchange Server - Windows Internet Explorer	_ D X
🖂 https:// 192.168.1.100 /ecp/Server	rs/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=f23ffc22-0cdb-4a3a-9cab-25f2e1ba2c51	😵 Certificate error
MAIL		Help
general databases and database availability groups POP3 IMAP4	Message tracking log ✓ Enable message tracking log Message tracking log path: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking	
unified messaging DNS lookups transport limits • transport logs	Connectivity log Cannectivity log Connectivity log path: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\Connectivity	
Outlook Anywhere	Protocol log Send protocol log path: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\ProtocolLog\Smtp Receive protocol log path: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\ProtocolLog\Smtp	
	save	cancel
		🔍 100% 🔻 🔡

2. Using [Exchange Management Shell]:

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [Exchange Management Shell].



(3) Enable message tracking. Type in program:

Set-TransportService <ServerIdentity> -MessageTrackingLogEnabled \$True -MessageTrackingLogPath <LocalFilePath> <ServerIdentity> is the computer name of Exchange Server. <LocalFilePath> is the message Tracking path, default setting is

"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles \Logs\MessageTracking".

Here we type in:

Set-TransportService win2012ad -MessageTrackingLogEnabled \$True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking"



(4) Check the message tracking log setting.

Type in program:

Get-TransportService win2012ad Select	Object *Track*	
E [PS] C:\Windows\system32>Get-Transport	Machine: WIN2012AD.win2012cht.local	x
MessageTrackingLogEnabled MessageTrackingLogMaxAge MessageTrackingLogMaxDirectorySize MessageTrackingLogMaxFileSize MessageTrackingLogPath MessageTrackingLogSubjectLoggingEnable	: True : 30.00:00:00 : 1000 MB (1,048,576,000 bytes) : 10 MB (10,485,760 bytes) : C:\Program Files\Microsoft\Exchange Server\W15\TransportRoles\Logs\MessageTr cking d : True	٩a
<mark>[PS]</mark> C:\Windows\system32>_ Microsoft New Phonetic 半:		~

4 Set up NXLOG

- (1) Log in Widnows Server as Administrator.
- (2) Download NXLOG: go to http://sourceforge.net/projects/nxlog-ce/files/,

download {nxlog-ce-x.x.x.msi}.

(3) Install NXLOG: Click {nxlog-ce-x.x.x.msi}, install NXLOG.

Note:

Install NXLOG on 32 bit operating system at " C:\Program Files\nxlog\conf\nxlog.conf "

Install NXLOG on 64 bit operating system at "C:\Program Files (x86)\nxlog\conf\nxlog.conf "

- (4) Set Up NXLOG:
- (a) Download NXLOG Exchange setting profile:

http://www.npartnertech.com/download/tech/nxlog_exchange.conf

(b) Edit NXLOG profile "C:\Program Files (x86)\nxlog\conf\nxlog.conf". Copy NXLOG Exchange setting profile contents: nxlog_exchange.conf. Paste it and overwrite

nxlog.conf.						
#define ROOT	C:\Program Files\nxlog					
define ROOT (define ROOT C:\Program Files (x86)\nxlog					
Moduledir %F	ROOT%\modules					
CacheDir %RC	DOT%\data					
Pidfile %ROO	T%\data\nxlog.pid					
SpoolDir %RC	DOT%\data					
LogFile %ROC	DT%\data\nxlog.log					
<extension sy<="" th=""><th>slog></th></extension>	slog>					
Module	xm_syslog					
define BASED	IR C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking					
<input in_exc<="" th=""/> <th>hange></th>	hange>					
Module	im_file					
File	'%BASEDIR%\MSGTRK20????*-*.LOG'					
SavePos	TRUE					
<output out_<="" th=""><th>exchange></th></output>	exchange>					
Module	om_udp					
Host	192.168.2.64					
Port	514					
Exec	\$SyslogFacilityValue = 2;					
Exec	\$SourceName = 'Exchange';					
Exec	to_syslog_bsd();					
<route excha<="" th=""><th>nge></th></route>	nge>					
Path	in_exchange => out_exchange					

Please choose the correct install path of NXLOG about green words.

The environment of this example is a 64 bit system.

Choose "define ROOT C:\Program Files (x86)\nxlog".

About red words "define BASEDIR **\$dir**", please type in the message tracking log path of Exchange Server in \$dir.

This example we use Exchange 2007

The default path is "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking". About red words "Host \$N_Reporter_IP", please setting '\$N-Reporter_IP' to real N-Reporter IP.

In this example the IP is 192.168.2.64.

For example :



(3) Start NXLOG :

a. Start NXLOG by using [Command Prompt] or b. [Services]

a. Click [Start] → [All programs] → [Accessories] → Right click [Command Prompt] →

Click [Run as administrator], run as system administrator.

Type in command prompt:

net stop nxlog			
net start nxlog			

b. Click [Start] → [All programs] → [Administrative Tools] → [Services], right click [nxlog] →
 Click [Start] or [Restart].

(4) Check whether does NXLOG runs normally:

Check the log file of NXLOG "C:\Program Files (x86)\nxlog\data\nxlog.log". If it does not show Error, means it is running normally.

Technical Support : Email: support@npartnertech.com Skype : support@npartnertech.com Sales Information : Email: sales@npartnertech.com

