

N- Partner N-Reporter

用户如何管理 Exchange Server 邮件追踪记录审核

V 1.1.4 (简体)



前言

本文件描述 N-Reporter 使用者如何管理 Exchange Server 邮件追踪(Message Tracking)记录审核。第 一步先配置 Exchange 的邮件追踪记录。第二步利用 Open Source 工具 NXLOG Community Edition(简称 NXLOG)将邮件追踪记录转成 Syslog,发送至 N-Reporter 接收。因 Windows 与 Exchange 版本差异,使 用[Exchange 管理命令接口]配置可能会有差异,本文件配置的环境为 Windows 2003 64 位操作系统安装 Exchange 2007、Windows 2008 R 2 操作系统安装 Exchange 2010 与 Windows 2012 操作系统安装 Exchange 2013。

邮件追踪记录是与执行 Exchange Server 且已安装集线传输服务器角色(Hub Transport server role)、 信箱服务器角色(Mailbox server role)或边际传输服务器角色(Edge Transport server role)的计算机往返传 送邮件之所有邮件活动的详细记录。已安装客户端存取服务器角色或整合通讯服务器角色的 Exchange Server 不会有邮件追踪记录。本配置文件适用安装集线传输服务器角色或边际传输服务器角色的 Exchange Server。

注: Exchange Server 预设启用邮件追踪。

文件章节如下:

连	络信	息		1
1	配置	Exchange Server 2007	邮件追踪记录	2
2	配置	Exchange Server 2010	邮件追踪记录	6
3	配置	Exchange Server 2013	邮件追踪记录	9
4	配置	NXLOG		2

连络信息 N-Partner 公司连络方式: TEL: +886-4-23752865 FAX: +886-4-23757458 **有关技术问题请洽:** Email: support@npartnertech.com Skype : support@npartnertech.com

有关业务相关问题请洽:

Email: sales@npartnertech.com



1 配置 Exchange Server 2007 邮件追踪记录

可选择[Exchange 管理命令接口]或[Exchange 管理命令接口]配置邮件追踪记录。

一、使用[Exchange 管理命令接口]配置:

- (1) 以系统管理者 Administrator 登入 Exchange Server。
- (2) 鼠标左点[开始]→[所有程序]→[Microsoft Exchange Server 2007]
 - → [Exchange 管理命令接口]。



(3) 鼠标左点[服务器组态],左点 Exchange Server,本例为"NPARTNER-012A02",

左点 [管理 Hub Transport server role]。

Section 2018 Exchange 管理主控台	
檔案(E) 執行(A) 檢視(V) 説明(H)	
Microsoft Exchange ↓ 伺服器組態	1 物件 動作
	伺服器組態
	修改組態網域控制站(C)
→ 用戶端存取 → 無線傳輸	3.6) 🕞 匯出措單(L)
	校視
	◎ 重新整理
	1 說明
	NPARINER-012A02
	≧ 管理 Mailbox server role(M)
	🛓 管理 Client ccess server role(C)
	<mark>문⊫ 管理 Hub Transport server role(T)</mark>
	■ 管理診斷記錄內容(0)
	■ 輸入產品金鑰(K):
	✓ 內容(R)
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

(4) 鼠标左点[内容]。勾选[启用邮件追踪记录],左点[浏览],设定邮件追踪记录文件路径,预设"C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"。
 左点[确定],完成配置。

				-미그
■: 集線傳輸 NPARTNER-012A02 內容	×	勿件	動作	
▼建立篩選器 ® −般 系統設定 外部 DNS 查閱 内部 DNS 查閱 限制 記錄檔設定	1		集線傳輸	-
▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●			📑 匯出清單(L)	
■ ■ NPARTNER-0: ▼ 常用郵件追蹤記錄(E)			檢視	•
郵件追蹤記錄檔路徑000:			◎ 重新整理	
C:\Puoguam Files\Microsoft\Exchange Server\TransportRoles\Logs' 瀏覽(B)			😢 說明	
連線記錄	-			•
▼ 啓用蓮線記録00)			NPARTNER-012A02	
▲ 連線記錄檔路徑(C):		▶	管理 Mailbox server role(M)	
NPARTNER C.(Program Files)Microsoft/Exchange Server/TransportRoles/Logs (別覧家)			管理 Client Access server role(C)	
接收連接器 通訊協定記錄檔	-		□ 管理診斷記錄內容(0)	
名稱			□ 輸入產品金鑰(K):	
Chent NPAR C./Phogram Files/Microsoft/Embarge Server/TransportRoles/Logs/Pro 瀏覽(W)			新增接收連接器(N)	
接收連接器通訊協定記錄檔路 🖭 🕚		- 1	▼ 内容(R)	
C.\Piogram Files\Miousont\Exphange Server\TransportRoles\Logs\Pio 瀏覽(3)		- 1	Client NPAR TNER-012A02	
		- 1	④ 停用(D)	
		- 1	▼ 移除(∀)	
		-	▼ 内容(R)	
<u>к</u>	-			

二、使用[Exchange 管理命令接口]配置:

- (1) 以系统管理者 Administrator 登入 Exchange Server。
- (2) 鼠标左点[开始]→[所有程序]→[Microsoft Exchange Server 2007]→

[Exchange 管理命令接口]。

Administrator			
管理您的伺服器	😏 我的電腦		
□	🔂 控制台(C)	+	
Windows 檔案	Windows Catalog Windows Update		
🚺 記事本	Microsoft Exchange Server 2007	Excl	hange Server 說明
捷徑 - SyslogAgentCon	〕系統管理工具] 附屬應用程式	 X Excl X Excl X Excl 	hang。管理主控台 hange 管理命令介面
🔀 Exchange 管理:1] 啓動 Internet Explorer (32-bit)	•	
🔀 Exchange 管理f	Outlook Express		
Notepad++	· 速端協助] WinRAR	•	
Internet Explored] InterSect Alliance] WinPcap	•	
所有程式(P) ▶	Wireshark Notepad++	•	
	💋 登出(L)	0 關機(1)	
🎒 開始 🛛 🥌 🧭 📶 🗍	🥥 管理您的伺服器		

(3) 启用邮件追踪。命令行输入:

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

<LocalFilePath>

或

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

<LocalFilePath>

<ServerIdentity>为 Exchange Server 的计算机名称, <LocalFilePath>为邮件追踪记录的路径,

预设为"C:\Program Files\Microsoft\Exchange

Server\TransportRoles\Logs\MessageTracking".

本例输入:

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

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

🚱 Machine: npartner-012a02 | Scope: npexchange.local

_ 8 ×

[PS] C:\>Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled \$True -M▲ essageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\TransportRoles \Logs\MessageTracking" [PS] C:\> (4) 检查邮件追踪记录布局。命令行输入:

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

🚱 Machine: npartner-012a02 Scope: npexchange.local	
[PS] C:\>Get-TransportServer npartner-Øj	2a02 Select-Object *Track* 🔺
MessageTrackingLogEnabled MessageTrackingLogMaxAge MessageTrackingLogMaxDirectorySize	: True : 30.00:00:00 - 250MB
MessageTrackingLogMaxFileSize	: 10MB
MessageTrackingLogPath	: C:\Program Files\Microsoft\Exchange S erver\TransportRoles\Logs\MessageTrac king
MessageTrackingLogSubjectLoggingEnabled	: True

2 配置 Exchange Server 2010 邮件追踪记录

可选择[Exchange Management Console]或[Exchange Management Shell]配置邮件追踪记录。

一、使用[Exchange Management Console]配置:

- (1) 以系统管理者 Administrator 登入 Exchange Server。
- (2) 鼠标左点[开始]→[所有程序]→[Microsoft Exchange Server 2010]→
 - [Exchange Management Console].



(3) 鼠标左点[Microsoft Exchange 内部部属]→[服务器组态]→[集线传输]。
 鼠标右点 Exchange Server,本例为"MAIL",左点[内容]。

😣 Exchange 管理主控台				
檔案(F) 執行(A) 檢視(V) 說明(H)				
🗢 🔿 🗾 🖬 🔢 🖬				
S Microsoft Exchange	🍡 集線傳輸		1 個物件	動作
■ Microsoft Exchange 内部部署 (mail.exchange)	💎建立篩選(R)			▲
□ □ 同服器組態		角色		🔜 匯出清單
12、1 箱	MAIL	集線傳輸,用戶端存取,	Version 14.3 (Buil	檢視 ▶
其線傳輸				重新整理
■ 整合理訊 ■ 및 收件者組態				👔 說明
				A
				MAIL
				🛼 管理信箱角色
	•		F	🔒 管理用戶端存取角色
	🏷 MAIL		2 個物件	冒 管理診斷記錄內容
	接收連接器			□ 輸入產品金鑰
	名稱 -	狀態		🤁 新增接收連接器
	Client MAIL	已敗用		✓ 內容
			I	Client MAIL
			I	③ 停用
			I	🗡 移除
			I	✓ 內容
			I	2 說明
			I	-
			I	
			I	
			I	
			I	
	<u>P</u>			

(4) 鼠标左点[记录文件设定]。勾选[启用邮件追踪记录文件], 输入[讯息追踪记录文件路

径],预设为"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"。

左点[确定],完成配置。



- 🗆 ×

二、使用[Exchange Management Shell] 配置:

- (1) 以系统管理者 Administrator 登入 Exchange Server。
- (2) 鼠标左点[开始]→[所有程序]→[Microsoft Exchange Server 2010]→[Exchange Management]

Shell].

 Fintermet Explorer (64 位元) Intermet Explorer Windows Update Microsoft Exchange Server 2010 Exchange Management Console Exchange Management Shell Exchange Server Help Notepad++ 	QUE Administrator 文件
条統管理工具 附屬應用程式 啟動 維護	電腦
	控制台
	装置和印表機
	系統管理工具 ▶
1	說明及支援
	執行
◆ 上一頁	Windows安全性
授 尋程式及檔案	登出▶

(3) 启用邮件追踪。命令行输入:

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

或

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

<ServerIdentity>为 Exchange Server 的计算机名称, <LocalFilePath>为邮件追踪记录的路径,

默认为"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"。

本例输入:

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

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

😵 禮器: mail.exchange.npartnertech.com

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

(4) 检查邮件追踪记录布局。命令行输入:

National Content and Content		_ 🗆
<mark>PS]</mark> C:\Windows\system32>get-transpor	tserver MAIL select-object *track*	
lessageTrackingLogEnabled	: Irue	
lessageTrackingLogMaxAge	: 30.00:00:00	
lessageTrackingLogMaxDirectorySize	: 1000 MB (1,048,576,000 bytes)	
lessageTrackingLogMaxFileSize	: 10 MB (10,485,760 bytes)	
lessageTrackingLogPath	: C:\Program Files\Microsoft\Exchange Server\W14\TransportRoles\Logs\Messay cking	geTra
lessageTrackingLogSubjectLoggingEnabl	ed : True	

3 配置 Exchange Server 2013 邮件追踪记录

可选择[Exchange 系统管理中心(Exchange Admin Center/EAC)]或[Exchange Management Shell] 配置邮件追踪记录。

- 一、使用[Exchange 系统管理中心(Exchange Admin Center/EAC)]配置:
- (1) 开启浏览器。
 - ▶ 内部 URL : "https://<CASServerName or private IP>/ecp", 内部 URL 用来从组织防火墙内 存取 EAC。
 - ▶ 外部 URL: "https://<MailHostName or public IP>/ecp", 外部 URL 用来从组织防火墙外存 取 EAC。

本例输入 URL " https://192.168.2.71/ecp " 连上 Exchange 系统管理中心。

(2) Exchange 系统管理中心(Exchange Admin Center/EAC)登入页面输入 Exchange Server 系统管理员和密码,登入 EAC。

CA ○ 3 https://192168.2.71/ccp/ 0 = 3 透産機能 0 × 3 透産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk 信惜 - Microsoft Exchange × CA ○ 3 使産機能 0 × Sk ○ 3 使産性 0 × Sk ○ 3 使					 ★7_4Ω	
1 企業版 Office 365 Administrate						
Exchange 系統管理	Exchange 系統管理中心					
收件者	信箱 群組 資源	連絡人 共用 移轉				
權限						
相符性管理	+-/∎ ₽8…					
組織	顯示名稱	▲ 信箱類型	電子鄭件地址			
(모:維	Administrator	使用者	Administrator@win2012cht.local	Administrator	<u> </u>	
郵件流程	quack shrink	使用者	quack@win2012cht.local shrink@win2012cht.local	使用者信箱 Administrator@win2012cht.local		
行動				職稿: 耕公室:		
公用資料夾				公司電話:		
整合通訊				電話和語音功能		
伺服器				整合通訊: 已停用 飲用		
混合				行動裝置	-	
工具		E	攟取 1 項 → 共 3 項			

(3) 鼠标左点[服务器],双点 Exchange Server,本例为双点"WIN2013AD"。



(4) 鼠标左点[传输记录文件]。勾选[启用邮件追踪记录文件]。设定邮件追踪记录文件路径,
 Exchange 2013 默认"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles
 \Logs\MessageTracking"。左点[储存],完成配置。

Copyright © All rights are reserved by N-Partner Technologies Co

- 二、使用[Exchange Management Shell]配置:
- (1) 以系统管理者 Administrator 登入 Exchange Server。
- (2) 鼠标左点[Start] → [Exchange Management Shell]。

Start					
Senier Manager	Vindows PowerShall	Group Policy	Active Directory	Sick Cleanur	Cluster-Aware
	Tack Manager		Active Directory		Internet
Control Panel		Active Directory Users and	Active Directory Administrative	Snipping Tool	Sound Recorder
Desktop	🖬 Windows Server 2012	Active Directory Sites and	DNS	Math Input Panel	Active Directory Lightweight
Administrative Tools	Store	Failover Cluster Manager	Default Programs	Exchange Management	Exchange Toolbox
		Windows Media Player	Character Map	Notepad++	

(3) 启用邮件追踪。命令行输入:

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

<ServerIdentity>为 Exchange Server 的计算机名称, <LocalFilePath>为邮件追踪记录的路径,

默认为"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles

\Logs\MessageTracking"。本例输入:

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

(4) 检查邮件追踪记录布局。

命令行输入:

Get-TransportService win2012ad | Select-Object *Track*

8	Machine: WIN2012AD.win2012cht.local	_ D X
[PS] C:\Windows\system32>Get-TransportS	ervice win2012ad ¦ select-object *Track*	<u>^</u>
MessageTrackingLogEnabled	: True	
MessageTrackingLogMaxAge	: 30.00:00:00	
MessageTrackingLogMaxDirectorySize	: 1000 MB (1,048,576,000 bytes)	
MessageTrackingLogMaxFileSize	: 10 MB (10,485,760 bytes)	
MessageTrackingLogPath	: C:\Program Files\Microsoft\Exchange Server\U15\TransportRoles\Logs\ cking	MessageTra
MessageTrackingLogSubjectLoggingEnabled	: True	
[PS] C:\Windows\sustem32>_		
Microsoft New Phonetic 半:		~

4 配置 NXLOG

- (1) 以系统管理者 Administrator 登入 Exchange Server。
- (2) 下载 NXLOG: 浏览 http://sourceforge.net/projects/nxlog-ce/files/,

下载『nxlog-ce-x.x.x.msi』。

- (3) 安装 NXLOG: 鼠标左点『nxlog-ce-x.x.x.msi』, 安装 NXLOG。
- 注:32 位操作系统 NXLOG 安装在 " C:\Program Files\nxlog\conf\nxlog.conf "

64 位系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

(4) 配置 NXLOG:

(1) 下载 NXLOG Exchange 配置文件范例:

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

(2) 编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "。
 复制 NXLOG Exchange 配置文件范例 nxlog_exchange.conf 内容,贴上并覆盖

nxlog.cor	nf.
#define ROO	T C:\Program Files\nxlog
define ROOT	C:\Program Files (x86)\nxlog
Moduledir %F	ROOT%\modules
CacheDir %R	OOT%\data
Pidfile %ROO	T%\data\nxlog.pid
SpoolDir %R0	DOT%\data
LogFile %RO	OT%\data\nxlog.log
<extension sy<="" td=""><td>/slog></td></extension>	/slog>
Module	xm_syslog
define BASE	DIR C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
<input in_exc<="" td=""/> <td>hange></td>	hange>
Module	im_file
File	'%BASEDIR%\MSGTRK20????*-*.LOG'
SavePos	TRUE
<output out_e<="" td=""><td>exchange></td></output>	exchange>
Module	om_udp
Host	192.168.2.64
Port	514
Exec	\$SyslogFacilityValue = 2;
Exec	\$SourceName = 'Exchange';
Exec	to_syslog_bsd();
<route excha<="" td=""><td>nge></td></route>	nge>
Path	in_exchange => out_exchange

绿色部位请选择 NXLOG 正确的安装路径,

本例环境为 64 位系统

选择 " define ROOT C:\Program Files (x86)\nxlog " 。

红色部分"define BASEDIR \$dir "行中的\$dir 请输入 Exchange Server 邮件追踪记录路径,

本例使用 Exchange 2007

默认路径 " C:\Program Files\Microsoft\Exchange

Server\TransportRoles\Logs\MessageTracking " .

红色部分"Host \$N_Reporter_IP"行中的\$N-Reporter_IP 改成 N-Reporter IP,

本例 IP 为 192.168.2.64。

本例配置范例:

C:\Progra	am Files (x86)\nxlog/conf\nxlog.conf - Notepad++	×
檔案 (F) 編編	輯(王) 尋找(3) 檢視(12) 編碼(12) 相對(12) 自訂(12) 巨集 執行 外掛模組(12) 視窗(122) 2	X
🕞 📥 ⊨	\$ \$ 6 6 4 10 10 10 10 10 10 10 10 10 10 10 10 10	
😑 nxlog.conf	f 🔚 xudog.log	
1 E	H# This is a sample configuration file. See the nxlog reference manual about the	
$\dot{2}$	## configuration options. It should be installed locally and is also available	
ž	## configuration of the log or sent and the inter the and the interview of the sent sent of the sent sent sent sent sent sent sent sen	
Л	## Diago set http://http://giogane.gov/controlog-location/location/	
5	## attention to the folder your hange was instance into,	
6	Hafina DOOT CADrogram Fileshavlog	
	de Sine DOOT C. Vriogram Files (1869) and a	
	define ROOT CATOgram Files (X80) (hX10g	
ð	Moduledit %ROOT %Modules	
10		
10	Piquie %ROOT%Vdatavniog.pid	
	SpoolDir %ROOT%data	
12	LogFile %ROOT%IdataInxlog.log	
13	<extension syslog=""></extension>	
14	Module xm_syslog	
15		
16	define BASEDIR C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking	
17	<input in_exchange=""/>	
- 18	Module im_file	
- 19	File '%BASEDIR%\MSGTRK20?????*-*.LOG'	
20	SavePos TRUE	
- 21		
22	<output exchange="" out=""></output>	
23	Module om udp	
24	Host 192.168.2.64	
25	Port 514	
26	Exec $\$SyslogFacilityValue = 2:$	
$\bar{27}$	Exec \$SourceName = 'Exchange':	
28	Exec to syslog bsd():	
29		
30	<route exchange=""></route>	
31	Path in exchange \Rightarrow out exchange	
32		
52		
Perl source file	e length:1127 lines:32 Ln:32 Col:9 Sel:0 DosWindows ANSI INS	

(3) 启动 NXLOG:

a.利用[命令提示字符]启动 NXLOG 或 b.[服务]启动 NXLOG。

a. [开始]→[所有程序]→[应用附属程序], 鼠标右点[命令提示字符],

左点[执行身分],以系统管理员身分执行。

命令提示字符输入:

net stop nxlog net start nxlog

b. [开始]→[所有程序]→[系统管理工具]→[服务], 右点服务[nxlog],

左点[启动]或[重新启动]。

(4) 检查 NXLOG 是否正常启动:

检查 NXLOG 的 log 檔 " C:\Program Files (x86)\nxlog\data\nxlog.log ", 没有显示 Error 的讯息, 表示正常启动。

