

N- Partner N-REPORTER

如何使用 NXLOG 管理配置 Windows Server 日誌 V 005 (繁體)



前言

本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLOG 管理配置 Windows Server 2003/2008/2012 的日誌(Eventlog) · 將事件(Event)轉成 syslog · 再轉發到 N-Reporter 做正規化、稽 核與分析。本文件配置的環境分別為 Windows Server 2003、Windows Server 2008、Windows Server 2012。

NXLOG 適用於記錄大量事件的環境。當 Windows Server 日誌(Eventlog)每秒最大記錄速率超過 700 筆,請選用本文件介紹的 NXLOG 的配置方式。

本章節內容如下

1	安裝設定 \	Windows Server 環境中的 NXLog	2
	1.1	For Windows Server 2003	2
	1.2	For Windows Server 2008	5
	1.3	For Windows Server 2012	8
2	Windows 2	003 Server 稽核設定	12
	2.1	設定本機登入登出的稽核原則	12
	2.2	設定本機共享資料夾權限與稽核原則	16
3	Windows 2	008 Server 稽核設定	25
	3.1	設定本機登入登出的稽核原則	25
	3.2	設定本機共享資料夾權限與稽核原則	30
4	Windows 2	012 Server 稽核設定	43
	4.1	設定本機登入登出的稽核原則	43
	4.2	設定共享資料夾權限與稽核原則	47
5	將設備加ノ	人系統及 Syslog 資料格式及 Facility 的設定	53
連續	絡資訊		54

1 安裝設定 Windows Server 環境中的 NXLog 1.1 For Windows Server 2003

1. 下載 NXLOG:

前往 URL: http://nxlog.org/products/nxlog-community-edition/download

請下載網頁中提供的最新版 nxlog-ce-x.x.xxxx.msi,本例為下載 nxlog-ce-2.9.1716.msi。

2. 安裝 NXLOG:

滑鼠雙點剛下載的 nxlog-ce-2.9.1716.msi,點選[Install],執行 NXLog 程式後續的安裝步驟。

3. 下載設定 Windows 2003 NXLOG 配置檔 nxlog_win2k3.conf:

前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2k3.conf

開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 的 NXLOG 配置檔, 將 上面的 URL 上的 nxlog_win2k3.conf 檔案裡的設定內容複製, 然後將其貼上並覆 C:\Program Files (x86)\Prxlog\Conf\Prxlog.conf 間路徑中的 nxlog.conf 檔案中的參數設定後存檔。

註 1:預設建議使用者採用此設定檔.此設定只輸出主機稽核、物件存取、帳戶管理等

Eventlog, 會過濾大部分非必要的 Eventlog 雜訊, 減輕 NXLOG 程式對 Windows AD 主機效 能的負擔。

註 2:32 位元 OS 的 NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf " 64 位元 OS 的 NXLOG 安裝路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

4. 下載設定 Windows 2003 的 NXLOG 配置檔 nxlog_win2k3_all.conf (輸出全部的 Eventlog):

前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2k3_all.conf N-Reporter 提供法規報表統計 Windows Server 所有 Eventlog。使用者若是需要 Windows Server 的法規報表,請將 nxlog_win2k3_all.conf 檔案裡的設定內容複製, 然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf" 路徑中的 nxlog.conf 的參數設定後存檔。 此設定將會輸出所有 Windows Server 的 Eventlog, <u>此設定檔會需要 Windows Server 主機配備</u> 較高的硬體效能來執行 NXLOG。

This is a sample configuration file. See the nxlog reference manual about the ## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html

Please set the ROOT to the folder your nxlog was installed into, ## otherwise it will not start.

#define ROOT C:\Program Files\nxlog define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules CacheDir %ROOT%\data Pidfile %ROOT%\data\nxlog.pid

🔊 NHReporter

```
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log
<Extension syslog>
 Module
            xm_syslog
</Extension>
<Input in_eventlog>
# For windows 2003 and earlier use the following:
 Module
              im_mseventlog
 Exec parse_syslog_bsd(); \
        if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or $EventID == 538 or $EventID
== 540 or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID == 624 or $EventID == 626 or $EventID == 627 or $EventID
== 628 or $EventID == 629 or $EventID == 630 or $EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID
== 635 or $EventID == 636 or $EventID == 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 645 or $EventID
== 646 or $EventID == 647) { $SyslogFacilityValue = 13; } \
            else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
            else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
        else\
        {\
          drop();\
        }
</Input>
<Output out_eventlog>
 Module
              om_udp
 Host
     Port
                  514
     Exec $Message = string($EventID) + ": " + $Message;
     Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
      else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
         else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5; }
 Exec to syslog bsd();
</Output>
<Route eventlog>
 Path
              in_eventlog => out_eventlog
</Route>
緣色文字部位請依 OS 環境為 32 位元或 64 位元選擇 NXLOG 正確的安裝路徑。
```

※ し 入 丁 即 世 明 11 U U 城 坑 河 J2 世 ル 3, U4 世 ル 送]羊 INALUU 単 唯 时 幺 衣 ഥ 住 。

本文件範例環境為 64 位元 OS 系統, 選擇 " define ROOT C:\Program Files (x86)\nxlog " 。

紅色文字部位輸入 N-Reporter 機器 IP,本文件範例為輸入 "192.168.2.64 "。

設定範例如下圖:

🔡 C:\P:	ogram Files (x86)\nxklog/conf\nxklog.conf - Notepad++	_ 🗆 🗵
檔案①	編輯(注) 尋找(2) 檢視(2) 編碼(4) 程式語言(1) 自訂(1) 巨集 執行 外掛棋組(2) 親窗(2) 2	Х
) H & L L A L A L A L A L A L A L A L A L A	
indo;	sol spoke in the second s	
7	#define ROOT C:\Program Files\nxlog	
8	define ROOT C:\Program Files (x86)\nxlog	
9		
10	Moduledir %R00T%\modules	
11	CacheDir %ROOT%\data	
12	Pidtile %KOUT%\data\nxlog.pid	
13		
15	LogFILE AROUTA (data(nxlog.log	
16	(Extension evelop)	
17	Note and a set of the	
18	Notate All_System	
19		
20	# For windows 2003 and earlier use the following:	
21	Module im meventlog	
22	Exec parse syslog bs(): \	
23	1f (\$EventID == 672 or \$EventID == 673 or \$EventID == 675 or \$EventID == 528 or \$EventID == 529 or \$EventID == 538 or \$EventID ==	540
	or \$EventID == 551 or \$EventID == 560 or \$EventID == 612 or \$EventID == 624 or \$EventID == 626 or \$EventID == 627 or \$EventID ==	628
	or \$EventID == 629 or \$EventID == 630 or \$EventID == 631 or \$EventID == 632 or \$EventID == 633 or \$EventID == 634 or \$EventID ==	635
	or \$EventID == 636 or \$EventID == 637 or \$EventID == 638 or \$EventID == 641 or \$EventID == 642 or \$EventID == 645 or \$EventID ==	646
	or \$EventID == 647) { \$SyslogFacilityValue = 13; } \	
24	else if (\$SourceName == "Service Control Manager") { \$SyslogFacilityValue = 13; } \	
25	else if (\$SourceName =~ /^MSSQL*/) { \$SyslogFacilityValue = 18; } \	
26	else	
27		
28	drop();\	
29		
30		
31		
32	<pre>cutput out_eventiog></pre>	
33	Noaute om Lap	
35	NOSC 152,100,2,04 Poot 51/	
36	Func SMacsang - string(SEventTD) + ", " + SMacsang.	
37	Even if (EventType = 'FRRM' on (EventType = 'AUDIT FAILURE') { (SyclonSavenity/slue = 3: })	
38	$= \left\{ \frac{1}{2} \left\{ \frac{1}$	
39	else if (\$EventType == 'INFO' or \$EventType == 'AUDIT SUCCESS') { \$Svs1orSeverityValue = 5; }	
40	Execto system bid():	
41		
42		
43	<route eventlog=""></route>	
44	Path in_eventlog => out_eventlog	
45		
		-
Perl sourc	e file length : 2025 lines : 45 Ln : 45 Col : 9 Sel : 0 DosWindows ANSI	INS

5. 啟動 NXLOG:

a. 以系統管理員身份執行[命令提示字元]啟動 NXLOG:
 [開始]→[所有程式]→[應用附屬程式]→[命令提示字元]·滑鼠右鍵點[命令提示字元]·選擇[以系統管理員身分執行]。

命令提示字元輸入:

	net stop nxlog							
	net start nxlog							
b.	或是從[開始] →[所有程式]→[系統管理工具]→[服務] · 找到[nxlog] · 右鍵點服務							
	[nxlog]→ 點選[啟動]或[重新啟動]。							
6.	檢查 NXLOG 是否正常啟動:							
	開啟檢查 NXLOG 的 log 檔, 檔案路徑為 " C:\Program Files (x86)\nxlog\data\nxlog.log "							
	若沒顯示 Error 的訊息·表示正常啟動。							
2	🚰 C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++							
檔	檔案 EP 編輯 EP 尋找 ③ 檢視 (V) 編碼 M 程式語言 LD 自訂 (I) 巨集 執行 外掛 模組 (P) 視窗 (W) ? X							
	🔓 🖶 🖺 🛍 😼 💪 🤞 👘 🛅 🥥 😋 📾 🍇 👒 🤜 🖳 🔂 🔚 🗐 🗮 💌 💌 🔤 🕿 🐣							
	🔚 nulog.conf 📄 nulog.log							
	 2014-07-04 14:16:08 INFO nxlog-ce-2.7.1191 started 2014-07-04 14:16:27 WARNING stopping nxlog service 2014-07-04 14:16:27 WARNING nxlog-ce received a termination request signal, exiting 2014-07-04 14:16:29 INFO nxlog-ce-2 7 1191 started 							
	5							
Nor	m length : 244 lines : 5 Ln : 1 Col : 1 Sel : 0 Dos\Windows ANSI INS //							
	4							

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

🐼 NReporter

7. 新增 Windows Server 2003 Syslog 設備時, 資料格式請選擇 [Windows]:

註:因 NXLOG 沒有將事件編碼轉成 UTF8 編碼的功能[,]所以新增 Windows Server 2003 設備 時請注意語系選擇,避免出現亂碼。

8. 語系選擇:

OS Windows Server 2003 繁體版 請選擇[BIG5]編碼。 OS Windows Server 2003 簡體版 請選擇[GB2312]編碼。 OS Windows Server 2003 英文版 請選擇[UTF8]編碼。

1.2 For Windows Server 2008

1. 下載 NXLOG:

前往 URL http://nxlog.org/products/nxlog-community-edition/download

請下載網頁中提供的最新版 nxlog-ce-x.x.xxxx.msi,本例為下載 nxlog-ce-2.9.1716.msi。

2. 安裝 NXLOG:

滑鼠雙點剛下載的 nxlog-ce-2.9.1716.msi,點選[Install],執行 NXLog 程式後續的安裝步驟。

3. 下載 Windows 2008 NXLOG 配置檔 nxlog_win2k8.conf:

前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2k8.conf

開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 的 NXLOG 配置檔, 將

上面的 URL 上的 nxlog_win2k8.conf 檔案裡的設定內容複製, 然後將其貼上並覆蓋

C:₩Program Files (x86)₩nxlog₩conf₩nxlog.conf"路徑中的 nxlog.conf 檔案中的參數設定後存檔。

註 1:預設建議使用者採用此設定檔. 此設定只輸出主機稽核、物件存取、帳戶管理等 Eventlog, 會過濾大部分非必要的 Eventlog 雜訊, 減輕 NXLOG 程式對 Windows AD 主機效 能的負擔 [。]

註 2:32 位元 OS 的 NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf "

64 位元 OS 的 NXLOG 安裝路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

4. 下載設定 Windows 2008 的 NXLOG 配置檔 nxlog_win2k8_all.conf(輸出全部的 Eventlog):

前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2k8_all.conf

N-Reporter 提供法規報表統計 Windows Server 所有 Eventlog。使用者若是需要 Windows Server 的法規報表, 請將 nxlog_win2k3_all.conf 檔案裡的設定內容複製, 然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf" 路徑中的 nxlog.conf 的參數設定後存檔。 此設定將會輸出所有 Windows Server 的 Eventlog, <u>此設定檔會需要 Windows Server 主機配備</u> 較高的硬體效能來執行 NXLOG。 ## This is a sample configuration file. See the nxlog reference manual about the ## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html

Please set the ROOT to the folder your nxlog was installed into, ## otherwise it will not start.

#define ROOT C:\Program Files\nxlog define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules CacheDir %ROOT%\data Pidfile %ROOT%\data\nxlog.pid SpoolDir %ROOT%\data LogFile %ROOT%\data\nxlog.log

<Extension syslog> Module xm_syslog </Extension> <Input in_eventlog> # For windows 2008/vista/7/8/2012/2012r2 and latter use the following: Module im_msvistalog ReadFromLast TRUE SavePos TRUE Query <QueryList> \

<query id="0"> \</query>	
<select path="Security">*[System[(EventID=4768)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4769)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4771)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4624)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4625)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4634)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4647)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4648)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4656)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4719)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4720)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4722)]]<th>:t> ∖</th></select>	:t> ∖
<select path="Security">*[System[(EventID=4723)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4724)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4725)]]<th>:t> ∖</th></select>	:t> ∖
<select path="Security">*[System[(EventID=4726)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4727)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4728)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4729)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4730)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4731)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4732)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4733)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4734)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4735)]]<td>:t> \</td></select>	:t> \
<select path="Security">*[System[(EventID=4737)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4738)]]<td>:t> \</td></select>	:t> \
<select path="Security">*[System[(EventID=4739)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4741)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4742)]]<th>:t> \</th></select>	:t> \
<select path="Security">*[System[(EventID=4743)]]<th>:t> \</th></select>	:t> \
<select path="System">*[System[(EventID=7036)]]<td>> \</td></select>	> \
<select path="Application">*[System[(EventID=18454)]]<td>elect</td></select>	elect
<pre><select path="Application">*[System[(EventID=18456)]]</select></pre>	elect
\	
ntion	

</Input>

<Output out_eventlog>
Module om_udp
Host 192.168.2.64
Port 514
Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message;
Exec if (\$EventID == 18454 or \$EventID == 18456) { \$SyslogFacilityValue = 18; }\
else { \$SyslogFacilityValue = 13; }
Exec if (\$EventType == 'ERROR' or \$EventType == 'AUDIT_FAILURE') { \$SyslogSeverityValue = 3; }\
else if (\$EventType == 'WARNING') { \$SyslogSeverityValue = 4; }\
else if (\$EventType == 'INFO' or \$EventType == 'AUDIT_SUCCESS') { \$SyslogSeverityValue = 5; }
Exec to_syslog_bsd();
</Output>

Path in_eventlog => out_eventlog </Route> 綠色文字部位請依 OS 環境為 32 位元或 64 位元選擇 NXLOG 正確的安裝路徑。 本文件範例環境為 64 位元 OS 系統,選擇 " define ROOT C:\Program Files (x86)\nxlog "。 紅色文字部位輸入 N-Reporter 機器 IP·本文件範例為輸入 " 192.168.2.64 "。 設定範例如下圖:



5. 啟動 NXLOG:

a. 以系統管理員身份執行[命令提示字元]啟動 NXLOG:

[開始]→[所有程式]→[應用附屬程式]→[命令提示字元]·滑鼠右鍵點[命令提示字 元]·選擇[以系統管理員身分執行]。

命令提示字元輸入:

net stop nxlog net start nxlog

- b. 或是從[開始]→[所有程式]→[系統管理工具]→[服務]·右點服務[nxlog]· 左點[啟動]或[重新啟動]。
- 6. 檢查 NXLOG 是否正常啟動:

檢查 NXLOG 的 log 檔 " C:\Program Files (x86)\nxlog\data\nxlog.log " · 沒有顯示 Error 的訊 息 · 表示正常啟動 ·

📸 C.\Program Files (x86)\nxlog\data\nxlog.log - Notepad++						
檔案(F) 編輯(E) 尋找(S) 檢視	!(∀) 編碼(N) 程式語言(L)	自訂(T) 巨集 執行 :	外掛棋組(P) 視窗(₩) ?	X		
🕞 🖴 🖷 🖷 🔓 🤷	4 🗅 🛍 🤉 e a	***	🚍 🛛 🐺 🐷 💽	■ ▶ ▶ ≫		
🔚 nxlog.conf 📙 nxlog.log						
1 2014-07-03 17:57:2	2 WARNING stopping nxl	og service				
2 2014-07-03 17:57:2	2 WARNING nxlog-ce rec	eived a termination	n request signal, ex	citing		
3 2014-07-03 17:57:2	3 INFO nxlog-ce-2.7.11	.91 started				
4						
length : 192 lines : 4	Ln:1 Col:1 Sel:0	Dos\Wind	ows ANSI	INS //		

7. 新增 Windows Server 2008 設備時, 資料格式請選擇 [Windows]。

7

1.3 For Windows Server 2012

3. 下載 NXLOG:

前往 URL: http://nxlog.org/products/nxlog-community-edition/download 請下載網頁中提供的最新版 nxlog-ce-x.x.xxxx.msi,本例為下載 nxlog-ce-2.9.1716.msi。

4. 安装 NXLOG:

滑鼠雙點剛下載的 nxlog-ce-2.9.1716.msi,點選[Install],執行 NXLog 程式後續的安裝步驟。

3. 下載設定 Windows 2012 NXLOG 配置檔 nxlog_win2012.conf:

前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2012.conf 開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 的 NXLOG 配置檔, 將 上面的 URL 上的 nxlog_win2012.conf 檔案裡的設定內容複製, 然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf"路徑中的 nxlog.conf 檔案中的參數設定後存檔 註 1:預設建議使用者採用此設定檔. 此設定只輸出主機稽核、物件存取、帳戶管理等 Eventlog, 會過濾大部分非必要的 Eventlog 雜訊, 減輕 NXLOG 程式對 Windows AD 主機效 能的負擔。

註 2:32 位元 OS 的 NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf "

64 位元 OS 的 NXLOG 安装路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

4. 下載設定 Windows 2012 的 NXLOG 配置檔 nxlog_win2012_all.conf (輸出全部的 Eventlog): 前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2012_all.conf N-Reporter 提供法規報表統計 Windows Server 所有 Eventlog。使用者若是需要 Windows Server 的法規報表,請將 nxlog_win2012_all.conf 檔案裡的設定內容複製, 然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf" 路徑中的 nxlog.conf 的參數設定後存檔。 此設定將會輸出所有 Windows Server 的 Eventlog, <u>此設定檔會需要 Windows Server 主機配備</u> 較高的硬體效能來執行 NXLOG。

🐼 NHReporter

This is a sample configuration file. See the nxlog reference manual about the ## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html

Please set the ROOT to the folder your nxlog was installed into, ## otherwise it will not start.

#define ROOT C:\Program Files\nxlog define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules CacheDir %ROOT%\data Pidfile %ROOT%\data\nxlog.pid SpoolDir %ROOT%\data LogFile %ROOT%\data\nxlog.log

<Extension syslog> Module xm_syslog </Extension> <Input in_eventlog> # For windows 2008/vista/7/8/2012/2012r2 and latter use the following: Module im_msvistalog ReadFromLast TRUE SavePos TRUE Query <QueryList> \

<qi< th=""><th>uery Id="0"> \</th></qi<>	uery Id="0"> \
	<select path="Security">*[System[(EventID=4768)]]</select> \
	<select path="Security">*[System[(EventID=4769)]]</select> \
	<select path="Security">*[System[(EventID=4771)]]</select> \
	<select path="Security">*[System[(EventID=4624)]]</select> \
	<select path="Security">*[System[(EventID=4625)]]</select> \
	<select path="Security">*[System[(EventID=4634)]]</select> \
	<select path="Security">*[System[(EventID=4647)]]</select> \
	<select path="Security">*[System[(EventID=4648)]]</select> \
	<select path="Security">*[System[(EventID=4656)]]</select> \
	<select path="Security">*[System[(EventID=4719)]]</select> \
	<select path="Security">*[System[(EventID=4720)]]</select> \
	<select path="Security">*[System[(EventID=4722)]]</select> \
	<select path="Security">*[System[(EventID=4723)]]</select> \
	<select path="Security">*[System[(EventID=4724)]]</select> \
	<select path="Security">*[System[(EventID=4725)]]</select> \
	<select path="Security">*[System[(EventID=4726)]]</select> \
	<select path="Security">*[System[(EventID=4727)]]</select> \
	<select path="Security">*[System[(EventID=4728)]]</select> \
	<select path="Security">*[System[(EventID=4729)]]</select> \
	<select path="Security">*[System[(EventID=4730)]]</select> \
	<select path="Security">*[System[(EventID=4731)]]</select> \
	<select path="Security">*[System[(EventID=4732)]]</select> \
	<select path="Security">*[System[(EventID=4733)]]</select> \
	<select path="Security">*[System[(EventID=4734)]]</select> \
	<select path="Security">*[System[(EventID=4735)]]</select> \
	<select path="Security">*[System[(EventID=4737)]]</select> \
	<select path="Security">*[System[(EventID=4738)]]</select> \
	<select path="Security">*[System[(EventID=4739)]]</select> \
	<select path="Security">*[System[(EventID=4741)]]</select> \
	<select path="Security">*[System[(EventID=4742)]]</select> \
	<select path="Security">*[System[(EventID=4743)]]</select> \
	<select path="System">*[System[(EventID=7036)]]</select> \
	<pre><select path="Application">*[System[(EventID=18454)]]</select></pre>
	<pre><select path="Application">*[System[(EventID=18456)]]</select></pre>
<td>uery> \</td>	uery> \

</Input>

<

Path in_eventlog => out_eventlog </Route> 綠色文字部位請依 OS 環境為 32 位元或 64 位元選擇 NXLOG 正確的安裝路徑。 本文件範例環境為 64 位元 OS 系統, 選擇 " define ROOT C:\Program Files (x86)\nxlog " 。 紅色文字部位輸入 N-Reporter 機器 IP · 本文件範例為輸入 " 192.168.2.64 " 。 設定範例如下圖:

25 Query Id="0"> \ 26 Select Path="Security">*[System[(EventID=4768)]] \ 27 Select Path="Security">*[System[(EventID=4778)]] \ 28 Select Path="Security">*[System[(EventID=4625)]] \ 29 Select Path="Security">*[System[(EventID=4625)]] \ 30 Select Path="Security">*[System[(EventID=4625)]] \ 31 Select Path="Security">*[System[(EventID=4625)]] \ 32 Select Path="Security">*[System[(EventID=4648)]] \ 33 Select Path="Security">*[System[(EventID=4625)]] \ 34 Select Path="Security">*[System[(EventID=4720)]] \ 35 Select Path="Security">*[System[(EventID=4720)]] \ 36 Select Path="Security">*[System[(EventID=4720)]] \ 37 Select Path="Security">*[System[(EventID=4720)]] \ 38 Select Path="Security">*[System[(EventID=4720)]] \ 39 Select Path="Security">*[System[(EventID=4720)]] \ 41 Select Path="Security">*[System[(EventID=4720)]] \ 42 Select Path="Security">*[System[(EventID=4720)]] \ 43 Select Path="Security">*[System[(EventID=4720)]] \ 44 Select Path="Security">*[^				
26 (select Path="Security">*[System] (EventID=4768)]] \ 27 (select Path="Security">*[System] (EventID=4768)]] \ 28 (select Path="Security">*[System] (EventID=4768)]] \ 29 (select Path="Security">*[System] (EventID=4624)]] \ 30 (select Path="Security">*[System] (EventID=4624)]] \ 31 (select Path="Security">*[System] (EventID=4634)]] \ 32 (select Path="Security">*[System] (EventID=4634)]] \ 33 (select Path="Security">*[System] (EventID=4634)]] \ 34 (select Path="Security">*[System] (EventID=4634)]] \ 35 (select Path="Security">*[System] (EventID=4709)] \ 36 (select Path="Security">*[System] (EventID=4719)]] \ 37 (select Path="Security">*[System] (EventID=4723)]] \ 38 (select Path="Security">*[System] (EventID=4723)]] \ 40 (select Path="Security">*[System] (EventID=4723)]] \ 41 (select Path="Security">*[System] (EventID=4723)]] \ 42 (select Path="Security">*[System] (EventID=4723)]] \ 43 (select Path="Security">*[System] (EventID=4723)]] \ 44 (select Path="Security">*[System] (EventID=4723)]]					
27 Cselect Path="Security">"[System] (EventID=4769)]] (/Select) \ 28 Cselect Path="Security">[System] (EventID=4721)] (/Select) \ 30 Cselect Path="Security">[System] (EventID=4625)] (/Select) \ 31 Cselect Path="Security">[System] (EventID=4625)] (/Select) \ 32 Cselect Path="Security">[System] (EventID=4631)] (/Select) \ 33 Cselect Path="Security">[System] (EventID=4648)] (/Select) \ 34 Cselect Path="Security">[System] (EventID=4688)] (/Select) \ 35 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 36 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 36 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 37 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 38 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 39 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 41 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 42 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 43 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 44 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ 45 Cselect Path="Security">[System] (EventID=4720)] (/Select) \ <td></td>					
28 Cselect Path="Security"*[System] (EventID=4771)]](/Select) \ 29 Cselect Path="Security"*[System] (EventID=4624)]](/Select) \ 30 Cselect Path="Security"*[System] (EventID=4634)](/Select) \ 31 Cselect Path="Security"*[System] (EventID=4634)](/Select) \ 32 Cselect Path="Security"*[System] (EventID=4648)](/Select) \ 33 Cselect Path="Security"*[System] (EventID=4668)](/Select) \ 34 Cselect Path="Security"*[System] (EventID=4780)](/Select) \ 35 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 36 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 37 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 38 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 39 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 40 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 41 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 42 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 43 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 44 Cselect Path="Security"*[System] (EventID=4720)](/Select) \ 45 Cselect Path="Security"*[System] (EventID=4730)](/Select) \ <					
29 Select Path="Security">*[System] (EventID=4624)]] 30 Select Path="Security">*[System] (EventID=4625)]] 31 Select Path="Security">*[System] (EventID=4623)]] 32 Select Path="Security">*[System] (EventID=4643)]] 33 Select Path="Security">*[System] (EventID=4648)]] 34 Select Path="Security">*[System] (EventID=4648)]] 35 Select Path="Security">*[System] (EventID=4648)]] 36 Select Path="Security">*[System] (EventID=4719)]] 37 Select Path="Security">*[System] (EventID=4720)]] 38 Select Path="Security">*[System] (EventID=4720)]] 39 Select Path="Security">*[System] (EventID=4720)]] 40 Select Path="Security">*[System] (EventID=4720)]] 41 Select Path="Security">*[System] (EventID=4720)]] 42 Select Path="Security">*[System] (EventID=4720)]] 43 Select Path="Security">*[System] (EventID=4720)]] 44 Select Path="Security">*[System] (EventID=4720)]] 42 Select Path="Security">*[System] (EventID=4720)]] 44 Select Path="Security">*[System] (EventID=4720)]] 45 Select Path="Security">*[System] (EventID=4730)]] 46 Select Path="Security">*[System] (EventID=4730)]]					
30Select Path="Security">*[System](EventID=4625)]] \31Select Path="Security">*[System](EventID=4633)]] \32Select Path="Security">*[System](EventID=4634)]] \33Select Path="Security">*[System](EventID=4643)]] \34Select Path="Security">*[System](EventID=4643)]] \35Select Path="Security">*[System](EventID=4720)]] \36Select Path="Security">*[System](EventID=4720)]] \37Select Path="Security">*[System](EventID=4720)]] \38Select Path="Security">*[System](EventID=4720)]] \39Select Path="Security">*[System](EventID=4720)]] \40Select Path="Security">*[System](EventID=4720)]] \41Select Path="Security">*[System](EventID=4720)]] \42Select Path="Security">*[System](EventID=4720)]] \43Select Path="Security">*[System](EventID=4720)]] \44Select Path="Security">*[System](EventID=4720)]] \45Select Path="Security">*[System](EventID=4720)]] \46Select Path="Security">*[System](EventID=4730)]] \47Select Path="Security">*[System](EventID=4730)]] \48Select Path="Security">*[System](EventID=4730)]] \49Select Path="Security">*[System](EventID=4730)]] \51Select Path="Security">*[System](EventID=4730)]] \52Select Path="Security">*[System](EventID=4730)]] \53Select Path="Security">*[System](EventID=4730)]]54Select					
31 <select path="Security">*[System] (EventID=4634)]]</select> 32 <select path="Security">[System] (EventID=4634)]]</select> 33 <select path="Security">[System] (EventID=4686)]]</select> 34 <select path="Security">[System] (EventID=4686)]]</select> 35 <select path="Security">[System] (EventID=4720)]</select> 36 <select path="Security">[System] (EventID=4720)]</select> 37 <select path="Security">[System] (EventID=4720)]</select> 38 <select path="Security">[System] (EventID=4720)]</select> 39 <select path="Security">[System] (EventID=4720)]</select> 40 <select path="Security">[System] (EventID=4720)]</select> 41 <select path="Security">[System] (EventID=4720)]</select> 42 <select path="Security">[System] (EventID=4720)]</select> 43 <select path="Security">[System] (EventID=4720)]</select> 44 <select path="Security">[System] (EventID=4720)]</select> 45 <select path="Security">[System] (EventID=4720)]</select> 46 <select path="Security">[System] (EventID=4720)]</select> 47 <select path="Security">[System] (EventID=4720)]</select> 48 <select path="Security">[System] (EventID=4720)]</select> 49 <select path="Security">[System] (EventID=4720)]</select> 50 <select path="Security">[System] (EventID=4720)]</select> 51 <select path="Security">[System] (EventID=4720)]</select> 52 <select path="Security">[System] (EventID=4720)]</select> 53 <select path="Security">[System] (EventID=4720)]54<select path="Security">[System] (EventID=472</select></select>					
32 Cselect Path="Security">*[System](EventID=4647)]] \ 33 Cselect Path="Security">*[System](EventID=4648)]] \ 34 Cselect Path="Security">*[System](EventID=4648)]] \ 35 Cselect Path="Security">*[System](EventID=4729)]] \ 36 Cselect Path="Security">*[System](EventID=4720)]] \ 37 Cselect Path="Security">*[System](EventID=4720)]] \ 38 Cselect Path="Security">*[System](EventID=4721)] \ 39 Cselect Path="Security">*[System](EventID=4720)]] \ 40 Cselect Path="Security">*[System](EventID=4720)]] \ 41 Cselect Path="Security">*[System](EventID=4720)]] \ 42 Cselect Path="Security">*[System](EventID=4720)]] \ 43 Cselect Path="Security">*[System](EventID=4720)]] \ 44 Cselect Path="Security">*[System](EventID=4720)]] \ 45 Cselect Path="Security">*[System](EventID=4720)]] \ 46 Cselect Path="Security">*[System](EventID=4720)]] \ 47 Cselect Path="Security">*[System](EventID=4730)]] \ 48 Cselect Path="Security">*[System](EventID=4731)]] \ 50 Cselect Path="Security">*[System](EventID=4732)]] \					
33Select Path="Security">*[System](EventID=4648)]]34Select Path="Security">*[System](EventID=47656)]]35Select Path="Security">*[System](EventID=4720)]]36Select Path="Security">*[System](EventID=4720)]]37Select Path="Security">*[System](EventID=4720)]]38Select Path="Security">*[System](EventID=4720)]]39Select Path="Security">*[System](EventID=4723)]]40Select Path="Security">*[System](EventID=4723)]]41Select Path="Security">*[System](EventID=4728)]]42Select Path="Security">*[System](EventID=4728)]]43Select Path="Security">*[System](EventID=4728)]]44Select Path="Security">*[System](EventID=4728)]]45Select Path="Security">*[System](EventID=4728)]]46Select Path="Security">*[System](EventID=4728)]]47Select Path="Security">*[System](EventID=4728)]]48Select Path="Security">*[System](EventID=4728)]]49Select Path="Security">*[System](EventID=4728)]]51Select Path="Security">*[System](EventID=4738)]]52Select Path="Security">*[System](EventID=4728)]]53Select Path="Security">*[System](EventID=4738)]]54Select Path="Security">*[System](EventID=4738)]]55Select Path="Security">*[System](EventID=4738)]]56Select Path="Security">*[System](EventID=4738)]]56Select Path="Security">*[System](EventID					
34 (Select Path="Security">*[System](EventID=4656)]] \ 35 (Select Path="Security">*[System](EventID=4719)]] \ 36 (Select Path="Security">*[System](EventID=4720)] \ 37 (Select Path="Security">*[System](EventID=4720)] \ 38 (Select Path="Security">*[System](EventID=4723)] \ 39 (Select Path="Security">*[System](EventID=4723)] \ 40 (Select Path="Security">*[System](EventID=4723)]] \ 41 (Select Path="Security">*[System](EventID=4726)]] \ 42 (Select Path="Security">*[System](EventID=4726)]] \ 43 (Select Path="Security">*[System](EventID=4726)]] \ 44 (Select Path="Security">*[System](EventID=4726)]] \ 45 (Select Path="Security">*[System](EventID=4726)]] \ 46 (Select Path="Security">*[System](EventID=4730)] \ 47 (Select Path="Security">*[System](EventID=4733)]] \ 48 (Select Path="Security">*[System](EventID=4733)]] \ 49 (Select Path="Security">*[System](EventID=4733)]] \ 51 (Select Path="Security">*[System](EventID=4734)]] \ 52 (Select Path="Security">*[System](EventID=4734)]] \ <					
35 (Select Path="Security">*[System](EventID=4719)]] 36 (Select Path="Security">*[System](EventID=4720)]] 37 (Select Path="Security">*[System](EventID=4720)]] 38 (Select Path="Security">*[System](EventID=4721)]] 39 (Select Path="Security">*[System](EventID=4721)]] 40 (Select Path="Security">*[System](EventID=4721)]] 41 (Select Path="Security">*[System](EventID=4721)]] 42 (Select Path="Security">*[System](EventID=4726)]] 43 (Select Path="Security">*[System](EventID=4728)]] 44 (Select Path="Security">*[System](EventID=4728)]] 45 (Select Path="Security">*[System](EventID=4728)]] 46 (Select Path="Security">*[System](EventID=4728)]] 47 (Select Path="Security">*[System](EventID=4728)]] 48 (Select Path="Security">*[System](EventID=4728)]] 49 (Select Path="Security">*[System](EventID=4728)]] 48 (Select Path="Security">*[System](EventID=4738)]] 49 (Select Path="Security">*[System](EventID=4738)]] 50 (Select Path="Security">*[System](EventID=4738)]] 51 <td< th=""><td></td></td<>					
36Select Path="Security">*[System[(EventID=4720)]] \37Select Path="Security">*[System[(EventID=4720)]] \38Select Path="Security">*[System[(EventID=4723)]] \39Select Path="Security">*[System[(EventID=4723)]] \40Select Path="Security">*[System[(EventID=4725)]] \41Select Path="Security">*[System[(EventID=4726)]] \42Select Path="Security">*[System[(EventID=4726)]] \43Select Path="Security">*[System[(EventID=4726)]] \44Select Path="Security">*[System[(EventID=4728)]] \45Select Path="Security">*[System[(EventID=4728)]] \46Select Path="Security">*[System[(EventID=4730)]] \47Select Path="Security">*[System[(EventID=4730)]]48Select Path="Security">*[System[(EventID=4731)]]49Select Path="Security">*[System[(EventID=4731)]]50Select Path="Security">*[System[(EventID=4731)]]51Select Path="Security">*[System[(EventID=4731)]]52Select Path="Security">*[System[(EventID=4731)]]53Select Path="Security">*[System[(EventID=4731)]]54Select Path="Security">*[System[(EventID=4731)]]55Select Path="Security">*[System[(EventID=4733)]]56Select Path="Security">*[System[(EventID=4733)]]56Select Path="Security">*[System[(EventID=4733)]]55Select Path="Security">*[System[(EventID=4738)]]56Select Path="Security">*[System[(EventID=4738)]]56Select Path="Security">*[System[(EventID=4738)]] </th <td></td>					
37Select Path="Security">*[System](EventID=4722)]]38 <select path="Security">*[System](EventID=4723)]]</select> 39 <select path="Security">*[System](EventID=4724)]]</select> 40 <select path="Security">*[System](EventID=4725)]]</select> 41 <select path="Security">*[System](EventID=4726)]]</select> 42 <select path="Security">*[System](EventID=4726)]]</select> 43 <select path="Security">*[System](EventID=4728)]]</select> 44 <select path="Security">*[System](EventID=4728)]]</select> 45 <select path="Security">*[System](EventID=4730)]]</select> 46 <select path="Security">*[System](EventID=4730)]]</select> 47 <select path="Security">*[System](EventID=4730)]]</select> 48 <select path="Security">*[System](EventID=4733)]]</select> 49 <select path="Security">*[System](EventID=4733)]]</select> 50 <select path="Security">*[System](EventID=4733)]]</select> 51 <select path="Security">*[System](EventID=4733)]]</select> 52 <select path="Security">*[System](EventID=4733)]]</select> 53 <select path="Security">*[System](EventID=4738)]]</select> 54 <select path="Security">*[System](EventID=4738)]]</select> 55 <select path="Security">*[System](EventID=4738)]]</select> 56 <select path="Security">*[System](EventID=4738)]]</select>					
38CSelect Path="Security">*[System](EventID=4723)]] \39CSelect Path="Security">*[System](EventID=4724)]] \40CSelect Path="Security">*[System](EventID=4725)]] \41CSelect Path="Security">*[System](EventID=4726)]] \42CSelect Path="Security">*[System](EventID=4726)]] \43CSelect Path="Security">*[System](EventID=4728)]] \44CSelect Path="Security">*[System](EventID=4728)]] \45CSelect Path="Security">*[System](EventID=4728)]] \46CSelect Path="Security">*[System](EventID=4728)]]47CSelect Path="Security">*[System](EventID=4730)]]48CSelect Path="Security">*[System](EventID=4730)]]49CSelect Path="Security">*[System](EventID=4731)]]50CSelect Path="Security">*[System](EventID=4734)]]51CSelect Path="Security">*[System](EventID=4734)]]52CSelect Path="Security">*[System](EventID=4733)]]53CSelect Path="Security">*[System](EventID=4738)]]54CSelect Path="Security">*[System](EventID=4738)]]55CSelect Path="Security">*[System](EventID=4738)]]56CSelect Path="Security">*[System](EventID=4741)]]56CSelect Path="Security">*[System](EventID=4743)]]					
39Gelect Path="Security">*[System] [GventID=4724)] {/Select> \40(Select Path="Security">*[System] [EventID=4726)]] {/Select> \41(Select Path="Security">*[System] (EventID=4726)]] {/Select> \42(Select Path="Security">*[System] (EventID=4727)]] {/Select> \43(Select Path="Security">*[System] (EventID=4728)]] {/Select> \44(Select Path="Security">*[System] (EventID=4729)] {/Select> \45(Select Path="Security">*[System] (EventID=4729)] {/Select> \46(Select Path="Security">*[System] (EventID=4730)] {/Select> \47(Select Path="Security">*[System] (EventID=4731)] {/Select> \48(Select Path="Security">*[System] (EventID=4731)] {/Select> \49(Select Path="Security">*[System] (EventID=4731)] {/Select> \50(Select Path="Security">*[System] (EventID=4731)] {/Select> \51(Select Path="Security">*[System] (EventID=4731)] {/Select> \52(Select Path="Security">*[System] (EventID=4731)] {/Select> \53(Select Path="Security">*[System] (EventID=4731)] {/Select> \54(Select Path="Security">*[System] (EventID=4731)] {/Select> \55(Select Path="Security">*[System] (EventID=4731)] {/Select> \54(Select Path="Security">*[System] (EventID=4731)] {/Select> \55(Select Path="Security">*[System] (EventID=4731)] {/Select> \56(Select Path="Security">*[System] (EventID=4731)] {/Select> \					
40 <					
41 <					
42 <					
43 <					
44 <					
45 <select path="Security">*[System[(EventID=4730)]]</select> \ 46 <select path="Security">*[System[(EventID=4730)]]</select> \ 47 <select path="Security">*[System[(EventID=4731)]]</select> \ 48 <select path="Security">*[System[(EventID=4731)]]</select> \ 49 <select path="Security">*[System[(EventID=4733)]]</select> \ 50 <select path="Security">*[System[(EventID=4734)]]</select> \ 51 <select path="Security">*[System[(EventID=4735)]]</select> \ 52 <select path="Security">*[System[(EventID=4737)]]</select> \ 53 <select path="Security">*[System[(EventID=4737)]]</select> \ 54 <select path="Security">*[System[(EventID=4739)]]</select> \ 55 <select path="Security">*[System[(EventID=4739)]]</select> \ 56 <select path="Security">*[System[(EventID=4731)]]</select> \					
46 <select path="Security">(System[(EventID=4730)]]</select> \ 46 <select path="Security">(System[(EventID=4731)]]</select> \ 47 <select path="Security">(System[(EventID=4731)]]</select> \ 48 <select path="Security">(System[(EventID=4732)]]</select> \ 49 <select path="Security">(System[(EventID=4732)]]</select> \ 50 <select path="Security">(System[(EventID=4732)]]</select> \ 51 <select path="Security">(System[(EventID=4733)]]</select> \ 52 <select path="Security">(System[(EventID=4737)]]</select> \ 53 <select path="Security">(System[(EventID=4737)]]</select> \ 54 <select path="Security">(System[(EventID=4737)]]</select> \ 55 <select path="Security">(System[(EventID=4739)]]</select> \ 56 <select path="Security">*[System[(EventID=4739)]]</select> \					
47 <select path="Security">*[System[(EventID=4732)]]</select> \ 47 <select path="Security">*[System[(EventID=4732)]]</select> \ 48 <select path="Security">*[System[(EventID=4733)]]</select> \ 49 <select path="Security">*[System[(EventID=4733)]]</select> \ 50 <select path="Security">*[System[(EventID=4733)]]</select> \ 51 <select path="Security">*[System[(EventID=4735)]]</select> \ 52 <select path="Security">*[System[(EventID=4737)]]</select> \ 53 <select path="Security">*[System[(EventID=4737)]]</select> \ 54 <select path="Security">*[System[(EventID=4738)]]</select> \ 55 <select path="Security">*[System[(EventID=4738)]]</select> \ 56 <select path="Security">*[System[(EventID=4738)]]</select> \					
47 (Select Path="Security">*[System[(EventID=4732)]] \ 48 (Select Path="Security">*[System[(EventID=4733)]] \ 49 (Select Path="Security">*[System[(EventID=4733)]] \ 50 (Select Path="Security">*[System[(EventID=4733)]] \ 51 (Select Path="Security">*[System[(EventID=4737)]] \ 52 (Select Path="Security">*[System[(EventID=4737)]] \ 53 (Select Path="Security">*[System[(EventID=4738)]] \ 54 (Select Path="Security">*[System[(EventID=4738)]] \ 55 (Select Path="Security">*[System[(EventID=4741)]] \ 56 (Select Path="Security">*[System[(EventID=4742)]] \					
46 CSELECT Path="Security">"[System[(EventID=4735)]] \ 49 <select path="Security">"[System[(EventID=4734)]]</select> \ 50 <select path="Security">"[System[(EventID=4737)]]</select> \ 51 <select path="Security">"[System[(EventID=4737)]]</select> \ 52 <select path="Security">"[System[(EventID=4737)]]</select> \ 53 <select path="Security">"[System[(EventID=4737)]]</select> \ 54 <select path="Security">"[System[(EventID=4739)]]</select> \ 55 <select path="Security">"[System[(EventID=4739)]]</select> \ 56 <select path="Security">"[System[(EventID=4734)]]</select> \					
49 Cselect Path="Security">"[system[(EventID=4734)]] \ 50 <select path="Security">"[System[(EventID=4735)]]</select> \ 51 <select path="Security">"[System[(EventID=4735)]]</select> \ 52 <select path="Security">"[System[(EventID=4738)]]</select> \ 53 <select path="Security">"[System[(EventID=4738)]]</select> \ 54 <select path="Security">"[System[(EventID=4739)]]</select> \ 55 <select path="Security">"[System[(EventID=4741)]]</select> \ 56 <select path="Security">"[System[(EventID=4743)]]</select> \					
50 Cselect Path="Security">*[System[(EventID=4735)]] \ 51 <select path="Security">*[System[(EventID=4737)]]</select> \ 52 <select path="Security">*[System[(EventID=4738)]]</select> \ 53 <select path="Security">*[System[(EventID=4739)]]</select> \ 54 <select path="Security">*[System[(EventID=4739)]]</select> \ 55 <select path="Security">*[System[(EventID=4741)]]</select> \ 56 <select path="Security">*[System[(EventID=4742)]]</select> \					
51 Cselect Path="Security">"[system[(EventID=4737)]] \ 52 <select path="Security">"[system[(EventID=4738)]]</select> \ 53 <select path="Security">"[system[(EventID=4739)]]</select> \ 54 <select path="Security">"[system[(EventID=4739)]]</select> \ 55 <select path="Security">"[system[(EventID=4741)]]</select> \ 56 <select path="Security">"[system[(EventID=4742)]]</select> \					
52 Cselect Path="Security">"[system[(EventID=4738)]] \ 53 <select path="Security">*[System[(EventID=4738)]]</select> \ 54 <select path="Security">*[System[(EventID=4741)]]</select> \ 55 <select path="Security">*[System[(EventID=4742)]]</select> \ 56 <select path="Security">*[System[(EventID=4743)]]</select> \					
53 Cselect Path="Security">*[System[[EventID=4739]] \ 54 Cselect Path="Security">*[System[[EventID=4741]]] \ 55 Cselect Path="Security">*[System[[EventID=4742]]] \ 56 Cselect Path="Security">*[System[[EventID=4743]]]					
54 <select path="Security">*[System[(EventID=4741)]]</select> \ 55 <select path="Security">*[System[(EventID=4742)]]</select> \ 56 <select path="Security">*[System[(EventID=4743)]]</select> \					
55 <select path="Security">*[System[(EventID=4742)]]</select> \ 56 <select path="Security">*[System[(EventID=4743)]]</select> \					
56 <pre><select path="Security">*[System[(EventID=4743)]]</select> \</pre>					
57 <pre><select path="System">*[System[(EventID=7036)]]</select> \</pre>					
58 <pre><select path="Application">*[System[(EventID=18454)]]</select> \</pre>					
59 <pre><select path="Application">*[System[(EventID=18456)]]</select> \</pre>					
60 - \	=				
61 -					
62 L					
63					
64 📮 <output out_eventlog=""></output>					
65 Module om_udp					
66 Host 192.168.2.64					
67 Port 514					
68 Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message;	<pre>b8 Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message;</pre>				
69 Exec if (\$EventID == 18454 or \$EventID == 18456) { \$SyslogFacilityValue = 18; } \					
/70 else { \$5yslogFacilityValue = 13; }					
71 Exec if (\$EventType == 'ERROR' or \$EventType == 'AUDIT_FAILURE') { \$SyslogSevenityValue = 3; } \					
72 else if (\$EventType == 'WARNING') { \$SyslogSeverityValue = 4; } \					
73 else if (\$EventType == 'INFO' or \$EventType == 'AUDIT_SUCCESS') { \$SyslogSeverityValue = 5; }					
74 Exec to syslog bsd();					
75					
76					
77 📮 < Route eventlog>					
78 Path in eventlog => out eventlog					
79					
80	\sim				
< III	>				

5. 啟動 NXLOG:

[Windows PowerShell]輸入:

net stop nxlog					
net start hxlog					
或具從 [開妝] 、	、多体管理工目 1	「服殺」	战利[pylog]	士鉀點昭致[pylog]	型上)理 「 戶小

b. 或是從[開始]→[系統管理工具]→[服務]·找到[nxlog]·右鍵點服務[nxlog]→ 點選[啟動]或[重新啟動]。

a. 滑鼠左點[開始],滑鼠右點[Windows PowerShell],左點[以系統管理員身分執行]。

 檢查 NXLOG 是否正常啟動:
 開啟檢查 NXLOG 的 log 檔, 檔案路徑為 " C:\Program Files (x86)\nxlog\data\nxlog.log " · 若沒 有顯示 Error 的訊息,表示正常啟動。

C:\Program	m Files (x86)\nxlog\data\nxlog.log - Notepad++	_ _ X			
檔案(F) 編輯(E) 尋找(S) 檢視(V) 編碼(N) 程式 ② ⑤ ⑥ ⑧ ⑨ ② 灸 ⑥ ◎	【語言(L) 自訂(T) 巨集 執行 外掛模組(P) 視窗(W)	² ▲ ₩ ➡ ₹ *			
<pre>1 2014-07-04 15:02:38 INFO nxlog-ce-2.7.1191 started 2 2014-07-04 15:02:43 WARNING stopping nxlog service 3 2014-07-04 15:02:43 WARNING nxlog-ce received a termination request signal, exiting 4 2014-07-04 15:02:45 INFO nxlog-ce-2.7.1191 started 5</pre>					
Normal text file length : 244 lines : 5	Ln:1 Col:1 Sel:0 Dos\Wind	lows ANSI INS			

7. 新增 Windows Server 2012 Syslog 設備時, 資料格式請選擇 [Windows]。

2 Windows 2003 Server 稽核設定

本章節說明的 Windows 2003 Server 本機稽核原則,這裡的本機是指該主機為**獨立主機**,並不屬 於任何的網域。

主要說明以下操作設定:

1. 設定本機登入登出的稽核原則。2. 設定本機共享資料夾權限與稽核原則。

安裝 NXLOG 的步驟,詳細請參閱第一章節。

2.1 設定本機登入登出的稽核原則

設定步驟如下:

1. 以系統管理員權限的 Administrator 登入 Windows 2003 Server。

點選 [開始功能表 / 所有程式 / 系統管理工具 / 本機安全性原則]。



12

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

2. 前往 [本機原則 / 稽核原則]

🏪 本機安全性設定		
檔案 (E) 執行 (A) 檢視 (V) 說明 (H) ← → E] [I] × [E] (2) [I]		
 ▶ 安全性設定 ● 帳戶原則 ● 捲核原則 ● 遊 捲核原則 ● 逆 捲核原則 ● 愛 安全性選項 ● 公開金鑰原則 ● 公開金鑰原則 ● 軟體限制原則 ● 蒙 空性原則 (位置:本機電腦) 	 原則▲ 職稽核目錄服務存取 職稽核系統事件 職稽核原則變更 職稽核原則變更 職稽核帳戶登入事件 職稽核帳戶管理 職稽核程序追蹤 	安全性設定 沒有稽核 沒有稽核 成功,失敗 沒有稽核 沒有稽核 成功,失敗 沒有稽核 成功,失敗 沒有稽核 成功,失敗 沒有稽核 成功,失敗 沒有稽核 成功,失敗 沒有稽核 成功,失敗

- 3. 定義下列的原則設定值:
 - (1) 稽核登入事件:

滑鼠雙擊 [稽核登入事件], 勾選 [成功]及 [失敗], 設定完成後按 [確定]。

檔案(P) 執行(Δ) 檢視(V) 説明(D) マ → Image: Second state s	
← → ● <td></td>	
→ ☆ 安全性設定 原則 定会性設定 定会性設定 定会性設定 定会性設定 没有稽核 没有稽核 没有稽核 没有稽核 没有稽核 迎着核物件存取 沒有稽核 没有稽核 迎着核物件存取 沒有稽核 没有稽核 迎着核物件存取 沒有稽核 没有稽核 迎着積核同則 没有稽核 没有稽核 四 沒有稽核 沈有稽核 加 没有稽核 加 加 省核核同則 ① で会	
回 回 1 <th1< th=""> <th1< th=""> <th1< th=""> <th1< th=""></th1<></th1<></th1<></th1<>	T
回 國 潜核系統事件 沒有稽核 回 稽核原則 國 踏核物件存取 沒有稽核 回 續 使用者權利指派 國 稽核原則變更 沒有稽核	
● ●<	
□ □ □ 使用者權利指派	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
四·13 正安主任原則(120章:平侯电脑) [13]]稽核登入事件 沒有稽核 沒有稽核	
過] 稽核指导追蹤 沒有稽核	
構核登入≧件內容 ?	×
· · · · · · · · · · · · · · · · · · ·	
恰似这些"甘品"。	
■ 成功②	
✓ 失敗(F)	

(2) 稽核帳戶登入事件:

滑鼠雙擊 [稽核帳戶登入事件]·勾選 [成功]及 [失敗]·設定完成後按 [確定]。

🌇 本機安全性設定		_ 🗆 ×
檔案(玊) 執行(Δ) 檢視(♡) 說明(丑)		
	「 <u>「</u> 」」	
● 父王庄武だ	20) 稽核日錄服務存取	
	調糖核系統事件	没有稽核
	おおおいていたい。	沒有稽核
🕀 🧰 使用者權利指派	121 稽核原則變更	沒有稽核
	副藉核特殊權限使用	沒有稽核
┃ 田────── 公開金舗原則	盟 稽核帳戶登入事件	沒有稽核
┃ □□□■ 軟配改制原列 □□■ 軟配改制原列 □□■ 軟配改制原列	·····································	没用借板
		成功,失敗
	1991始核提 医组织 携核能后者 人 事件 內容	2 2 2
	本機安全" 認定 說明此設定	(
	-	
	att +tz ≥	
	格核這些昏訊;	
	▼ 成功(2)	
	▼ 医腹(症)	
	œc	 取消

(3) 稽核物件存取:

滑鼠雙擊 [稽核物件存取]

成功:若欲稽核成功事件的 Log, 請勾選 [成功] 核取方塊。

失敗:若欲稽核失敗事件的 Log,請勾選 [失敗]核取方塊。

設定完成後按[確定]。

註:若 Windows 2003 Server 不做檔案伺服器稽核(File server audit)[,]建議不要勾選此稽核物 件存取的成功與失敗的設定值, 以避免 Windows 稽核多餘且冗長的物件存取事件然後轉換成 syslog 後發送給 N-Reporter,會影響主機的運作效能。



(4) 稽核原則變更:

滑鼠雙擊 [稽核帳戶管理]·勾選 [成功]及[失敗]·設定完成後按 [確定]。

2.2 設定本機共享資料夾權限與稽核原則

設定步驟如下:

- 1. 在欲共用的資料夾上點擊滑鼠右鍵,點選[內容]。
- 點選[共用]索引標籤,點選[共用此資料夾]。
 點選[使用權限]。

share	e_folde	・内容	?	×
一般	共用	安全性 自訂		
	2 惣可以 啓用這	與網路上的其他使用者共用此資料夾。 相資料夾的共用,請按一下[共用此資料	腰 夾]。	
	不共用此资料	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		
共	用名稱(H):	share_folder		
註	解(C):			
使	用者限制:	○ 允許最大就(M)		
		○ 允許這個數目的使用者(型):	÷	
若的	要設定使用 權限,請按	者透過網路存取此資料來 使用權限([權限]。	<u>P</u>)	
若取	要設定離線 處理]。	存取設定值,諸按一下[快 快取處理(G)	
		確定 取消 套	∄(<u>A</u>)	

- 3. 使用者設定:
 - (1) 點選[新增],來新增一使用者。
 - (2) 若要選擇其他電腦名稱,可點選 [位置],選擇其他電腦名稱。
 - (3) 可於此空白處直接輸入已知的使用者帳號後,按[檢查名稱]檢查存不存在。
 - (4) 若使用者帳號存在的話,按[確定]完成設定。

shart_folder 的種限 共用權限 群組或使用者名稱(G):		? ×		
Everyone 的權限(P) 完全控制 變更 讀取	新增①	移除(E) 拒絕 ———————————————————————————————————	選擇使用者或群組 選擇這個物件類型(S): 使用者、群組或內建安全性原則 從這個位置(P): SQL-SERVER 輸入物件名稱來選取(範例)(E): cris	 ? × 物件類型(0) 位置(L) 検查名稱(C)
	取消	套用(<u>A</u>)		取消

- 4. 設定使用者權限:
 - (1) 點選使用者帳號。
 - (2) 勾選允許 [完全控制]及[變更]權限。
 - (3) 設定完成後按 [確定]。

shart_folder 的補限		? ×
共用權限		
推组或使用类名稱(G)·		
🔮 cris (SQL-SERVER\cris)		
W Everyone		
2	新增(D)	移除(R)
cris的權限(P)	允許	拒絕
完全控制		
■ ■ 變更	\checkmark	
● / 變更 ● 讀取	N N	
一	N N	
● 「 變更 讀取 	N N	
· · · · · · · · · · · · · · · · · · ·	N N	
· 變更 讀取		
變更 讀取		

- 5. 安全性設定:
 - (1) 點選[安全性]索引標籤。
 - (2) 點選 [新增],來新增一使用者。
 - (3) 若要選擇其他電腦名稱,可點選 [位置],選擇其他電腦名稱。
 - (4) 可於此空白處直接輸入已知的使用者帳號後,按[檢查名稱]檢查存不存在。

(5) 若使用者帳號存在的話,按[確定]完成設定。

shart_folder 內容 一般 ① 安全性 目訂 詳組或使用者名稱(G): ② Administrator (SQL-SERVER) ③ Administrators (SQL-SERVER) ③ SYSTEM	Administrator) Administrators)	? x		
1	新增① 利	多除(<u>R)</u>	選擇 使用者 或 群組	? ×
使用權限 完全控制	允許 :	拒絕	使用者、群組或內建安全性原則	物件類型(0)
修改 請取及執行 法 開 發料本由容			從這個位置(乎):	位置①…
			<mark>ஆ√</mark> 大物件名稱來選取 (<u>範例</u>)伍): cris	檢查名稱(C)
特殊權限或進階設定諸按 [進階]	。 	[階(\7)	· · · · · · · · · · · · · · · · · · ·	
			進階(点) 確定	取消
確定	取消	套用(A)		

- 6. 設定使用者權限:
 - (1) 點選使用者帳號。
 - (2) 勾選允許 [完全控制] 權限,以取得所有權限。
 - (3) 設定完成後按 [套用]·

shart_folder 內容		? ×			
一般共用安全性自訂					
群組或使用者名稱(G):					
Administrator (SQL-SERVER\Administrator)					
Administrators (SQL-SERVE	R\Administrators)				
🕵 cris (SQL-SERVER\cris)					
SYSTEM					
	_新增①	<u>移除(R)</u>			
cris的權限(P)	允許	拒絕			
完全控制					
修改					
讀取及執行					
■ 請取及執行 清單資料夾內容 ■ ま取					
請取及執行 清單資料夾內容 請取 會 3	য ত ত ত ।				
讀取及執行 清單資料夾內容 讀取 寫入 時班娜呢					
讀取及執行 清單資料夾內容 讀取 寫入 共社類限 特殊權限或進階設定請按 [進階					
讀取及執行 清單資料夾內容 讀取 寫入 性社類呢 特殊權限或進階設定請按 [進階		□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□			
讀取及執行 清單資料夾內容 讀取 寫入 些社類呢 特殊權限或進階設定請按 [進階		□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□			

🐼 NHReporter

- 7. 進階安全性設定:
 - (1) 點選 [進階]。
 - (2) 點選 [稽核]索引標籤。
 - (3) 點選[新增]。
 - (4) 若要選擇其他電腦名稱,可點選 [位置],選擇其他電腦名稱。
 - (5) 可於此空白處直接輸入已知的使用者帳號後, 按[檢查名稱]檢查存不存在。
 - (6) 若使用者帳號存在的話,按 [確定]完成設定。



8. 稽核項目設定:

勾選所有稽核項目的 [成功]及 [失敗]的項目,設定完成後按 [確定]。

shart_folder 的稽核項目			? ×
物件 名稱(N): Cris (SQL-SERVER/cris))	變更(<u>C</u>)	
套用在(Q): 這個資料夾,子資料及	灰及檔案		-
存取(2):	成功	失敗	
完全控制 周遊資料夾/執行檔案 列出資料夾/讀取資料 讀取屬性 讀取擴充屬性 建立檔案/寫入資料 建立資料夾/附加資料 寫入屬性 寫入擴充屬性 刪除子資料夾及檔案 刪除 讀取權限	\[\] \[বরেরেরেরেরেরে	
□ 這些稽核項目只套用到這個容器 □ 物件及 (或) 容器(I)	器中的	全部清除(IJ
	確定	取消	

9. 在進階安全性設定完成後,點選 [確定]。

shart_folder 的進階安全性設定	×				
權限 稽核 擁有者 有效權限					
若要檢視其他有關特殊發核項目的資訊, 深擇一個發核項目, 然後按「編輯]。					
新增(D) 編輯(E) 格除(R)					
▼ 允許從父項繼承稽核項目套用到這個物件和所有的子物件,包括明確定義於此的項目(点)					
□ 1)题示於此答用到乙物件的项目,装件所有乙值物件上的链接项目(2)					
从额小水缸头用到于物件的项目,是10种用于项物件工的程序项目(2)					
了解其他有關稽核。					

10. 在分享資料夾設定完成後·點選 [確定]。

shart_folder 内容			? ×		
一般 共用	安全性自訂	1			
群組或使用者名和	⊈(<u>G</u>):				
🛃 Administrator (SQL-SERVER\Administrator)					
🚮 🚮 Administrator	s (SQL-SERVER'	Administrators)			
🗾 🕵 cris (SQL-SEI	RVER\cris)				
🕵 SYSTEM					
I					
	_	新增(D)	移除(R)		
cris的權限(P)		允許	拒絕		
完全控制					
修改		\checkmark			
讀取及執行					
清單資料夾內容	ŝ				
調取					
—————————————————————————————————————					
特殊權限或進階讀	没定請按 [進階]	•	3年15号70V		
		<u>i.</u>			
	確定	取消	(A) (A)		

11. 點選 [開始功能表 / 所有程式 / 系統管理工具 / 電腦管理]。



12. 點選 [系統工具 / 共用資料夾 / 共用]。

🔒 電腦管理				_ 🗆 🗙
📕 檔案(E) 執行(A) 檢視(⊻)	視窗(₩) 説明(H)			_ Ð ×
	1 💭			
	共用名稱 ∧	資料夾路徑	類型	# 用戶端連
▲ <mark>狐 系統工具</mark>	ADMIN\$	C:\WINDOWS	Windows	0
■ ■ 事件檢視器	ISIC\$	C:\	Windows	0
日 具 共用資料夾			Windows	0
	NETLOGON	C:\WINDOWS\S	Windows	U
	Share_luider	C:\DUCUMENIS a	Windows	0
		C. (MINDON 3 (3	001110000S	0
■ 戦 双胞記球及管不				
┃				
日 🗃 行放教旦				
1111111111111111111111111111111111111				
● 磁味里租工兵				
	•			Þ

13. 滑鼠左鍵雙擊被設定分享的分享資料夾,點選[共用使用權限]索引標籤。點選使用者名稱,勾 選允許[完全控制]、[變更]及[讀取]權限,設定完成後按[確定]。



3 Windows 2008 Server 稽核設定

本章節說明的 Windows 2008 Server 本機稽核原則,這裡的本機是指該主機為**獨立主機**,並不屬於任何的網域。

主要說明以下操作設定:

1.設定本機登入登出的稽核原則。2.設定本機共享資料夾權限與稽核原則。

安裝 NXLOG 的步驟,詳細請參閱第一章節。

3.1 設定本機登入登出的稽核原則

設定步驟如下:

1. 以系統管理員權限的 Administrator 登入 Windows 2008 Server。

點選 [開始功能表 / 系統管理工具 / 本機安全性原則]。



2. 前往 [本機原則 / 稽核原則]。

🖥 本機安全性原則		
本機安全性原則 檔案(F) 執行(A) 檢視(V) 說明(H) ●	原則 ● 稽核原則變更 ● 稽核帳戶登入事件 ● 稽核帳戶管理 ● 稽核物件存取 ● 稽核特殊權限使用 ● 稽核目錄服務存取 ● 稽核程序追蹤 ● 稽核系統事件	 □× 安全性設定 沒有稽核 成功,失敗 沒有稽核 成功,失敗 沒有稽核 成功,失敗 沒有稽核 沒有稽核 沒有稽核 沒有稽核 沒有稽核 沒有稽核
		J

- 3. 定義下列的原則設定值:
 - (1) 稽核登入事件:

滑鼠雙擊 [稽核登入事件], 勾選 [成功]及 [失敗], 設定完成後按 [確定]。



(2) 稽核帳戶登入事件:

滑鼠雙擊 [稽核帳戶登入事件], 勾選 [成功]及 [失敗], 設定完成後按 [確定]。



(3) 稽核物件存取:

註:若 Windows 2008 Server 不做檔案伺服器稽核(File server audit)[,]建議不要勾選此稽核物 件存取的成功與失敗的設定值, 以避免 Windows 稽核多餘且冗長的物件存取事件然後轉換成 syslog 後發送給 N-Reporter,會影響主機的運作效能。



(4) 稽核原則變更:

滑鼠雙擊 [稽核原則變更],勾選 [成功]及[失敗],設定完成後按[確定]。
 (5) 稽核帳戶管理:

滑鼠雙擊 [稽核帳戶管理]·勾選 [成功] 及 [失敗]·設定完成後按 [確定]。

3.2設定本機共享資料夾權限與稽核原則

設定步驟如下:

- 1. 在欲共用的資料夾上點擊滑鼠右鍵,點選[內容]。
- 2. 點選[共用]索引標籤,點選[共用]。



3. 在檔案分享權限設定中,點下拉選單,選擇一位此電腦中已建立的使用者帳戶後,此文件例子為

選擇 dola · 選擇完使用者帳戶後點選 [新增]。

案分享權限設定 23. 檔案分享權限設定	<u>×</u>
選擇要共用的人員 使用者必須擁有此電腦的使用者帳戶以及密碼,才能存取您共用的檔案。 用中心。	要變更此設定,請使用 <u>網路和共</u>
admin Administrator dola	▼ 新增(A)
npartner pikachu user1 win2k8_user1 Everyone (此濟單中的所有使用者) 建立新使用者	÷
告訴我可在 Windows 中共用的各種方法。	4000 (Betty (
	余分享種限設定 選擇要共用的人員 使用者必須擁有此電腦的使用者帳戶以及密碼,才能存取您共用的檔案。 用中心。 admin admin Administrator domain doministrator domain domain Administrator bit domain bit admin Administrator bit cola npartner pikachu user1 win2k8_user1 Everyone (此演單中的所有使用者) 速立新使用者

4. 點選[共用]。

	案分享權限設定 ■ 費安△含筆限設定			×
\bigcirc				
	選擇要共用的人員			
	使用者必須擁有此電腦的使用者帳戶以及密碼,才能存取您共用的檔 <u>用中心</u> 。	実・要變更此設定	[,] 請使用	網路和共
	[▼	沂增(A)	
	名稱	權限層級		
	3 Administrator	擁有者 ▼		
	💈 dola	讀取裝置 ▼		
	l			
	告訴我可在 Windows 中共用的各種方法。			
		🛞 共用	(H)	取消

5. 等待共用設定完成後,再按[完成]。



🐼 NHReporter

- **6**. 安全性設定:
 - (1) 點選[安全性]索引標籤。
 - (2) 點選 [編輯]。
 - (3) 選擇使用者。
 - (4) 勾選允許 [完全控制]權限,以取得所有權限。
 - (5) 設定完成後按 [確定]。

🔋 temp 內容 📃 📉	🔒 temp 的權限	×
一般 [1] 安全性] 以前的版本 [目訂]	安全性	
物件名稱: C:\Users\Administrator\Desktop\temp	物件名稱: C:\Users\Administrator\Desktop\temp	
群組或使用者名稱(G):	3 詳組或使用者名稱(G):	
a dola (WIN2K8/dola)	👗 dola (WIN2K8\dola)	
& Administrator (WIN2K8\Administr & Administrators (WIN2K8\Administr	Administrator (WIN2K8\Administrator)	
若要變更使用權限,請按一下 [編輯]。 編輯(E)		
dola的權限(P) 允許 拒絕	4 <u>新增(D)</u> <u></u> 冊	I除(R)
完全控制	dola的權限(P)	巨絕
◎	完全控制 🔽 🔽 🖓 🖓 🖓	
	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	片
<u></u>		╞╴╻║
如需特殊權限或進階設定,請按一下 [進進階(\/) 階]。	深人瞭解存取控制及權限	
深入瞭解存取控制及權限		套用(A)
開閉 取消 套用(A)		

- 7. 進階安全性設定:
 - (1) 點選[進階]。
 - (2) 點選 [稽核]索引標籤。
 - (3) 點選 [編輯]。
 - (4) 點選 [新增]。
 - (5) 若要選擇其他電腦名稱,可點選 [位置],選擇其他電腦名稱。
 - (6) 可於此空白處直接輸入已知的使用者帳號後,按[檢查名稱]檢查存不存在。
 - (7) 設定完成後按 [確定]。

● 長 共用 英全性 以約約5%年 目前 ● 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	🕌 temp 內容	📔 temp 的進階安全性設定
特片名稱、CVUserAddmaintaturDeskap kmg 第14年後期各名類(5): 夏、STSTEM 夏、STSTEM	一般 共用 安全性 以前的版本 自訂	(で) 「「「「「「「「「」」」」「「「」」」」「「」」」」
	物件名稱: C:\Users\Administrator\Desktop\temp	若要檢視或編輯稽核項目的詳細資料,請選取該項目,再按一下[編輯]。
● (1): ▲ (Abacimizetory) ▲ (Abacimizetory) ▲ (Abacimizetory) ▲ (Abacimizetory) ★ (Abacimizetory) # (Abacimizetory)	群組或使用者名稱(G):	物件名稱: C:\Users\Administrator\Desktop\temp
● Administration (1982):SAdministration) ● Administration (1982):SAdministration (1982): ● Administration (1982):	Asia (WINOKOdala)	稽核項目(T):
	Administrator (WIN2K8\Administrator)	
	🧸 Administrators (WIN2K8\Administrators)	
● ab 的编现(P) 九許 拒絕 ● ab 的编现(P) 九許 拒絕 ● get (b) ● get (b) ● get (b) <th>,若要變更使用權限,諸按一下 [編輯]。 編輯(E)…</th> <th></th>	,若要變更使用權限,諸按一下 [編輯]。 編輯(E)…	
	dola的權限(P) 允許 拒絕	
「 <	完全控制 ✓ ▲	
別出資料実内容 調求 1 別面較等準備現或編建設定,請按一下(確) 1 「加肉」 取用 取用(A) 「加肉」 取用 要用(A) 「「加肉」 取用 要用(A) 「「加肉」 取用 要用(A) 「「加肉」 取用 要用(A) 「「「加肉」 取用 要用(A) 「「「「「」」 「「」」」」 「「」」 「「」」」」 「「」」 「「」」」 「「」」」 「」」」」 「「」」」 「」」」」」 「「」」」」 「」」」」」 「「」」」」」 「」」」」」 「」」」 「」」」」」」 「」」」 「」」」」」」」 「」」」」 「」」」」」	18℃ ✓ → → → → → → → → → → → → → → → → → →	3
通報 通報(0)		
W WW WW WW WW WW WW WW WW WW WW WW WW WW WH WW WW WW WW WW WW WW WH WW WH WW WW WW WW WW WH WW WW WW WH WW WW WW WW WW WH WW WW WW WH WW WW WW <th></th> <th>編輯(E)</th>		編輯(E)
除了: 1 深入鏡窗音和短海川泛耀梁 留花 1 1 1 1 <		▼ 従此物件的父項包括繼承諾核項目(1)
諸法物件存取的端求為例2 服用 取消 取消 至用(A) 確定 取消 取消 至用(A) 確定 取消 部内 市方 要核視或編載褶枝項目的評細資料,諸選取該項目,再按一下協議)。 特件名額: C.VJsexkAdministabarDeskoptemp 福枝項目(1): 選擇這個物件類型(0): 「健用者、評組 或 內建安全性原則 (5) 「健用者、評組 或 內建安全性原則 (5) 「健用者、評組 或 內建安全性原則 (5) 「健用者、評組 或 內建安全性原則 (5) (1): 「健用者、評組 或 內建安全性原則 (1): 「健用者、評組 或 內建安全性原則 (1): (2): (1): (1): (2): (1): (1): (2): (1): (1): (3): (1): (1): (4): (1): (1): (5): (1): (1): (4): (1): (1): (4): (1): (1): (5): (1): (1): (1): (1): (1): (2): (1): (1): (4): (1): (1):		
顧用 取消 室用(A) 確定 取消 変用(A) 確定 取消 変用(A) 確定 取消 変用(A) 確定 取消 変用(A) 確比 市場の 特件名稱: C: VBerk\Administrator/Desktop!emp 福校項目(1): 種型 名額 存取 ● ● ● ● ● ● ●	深入瞭解存取控制及權限	<u> </u>
benp 衍建院安全性設定 × 宿核 若要檢視或編輯稽核項目的詳細資料,請還取該項目,再按一下[編輯]。 物件名額: C.VUserskAdministrator/Desktop/temp 稽核項目(): 願型 名額 存取 遵承目 便用者、群組或內建安全性原則 5 炒供類型(0) (從這個份堂(0) 《社場件的交項包括繼承稽核項目(0) (以此物件的繼承稽核項目(0) 以此物件的繼承稽核項目取代所有子条現有的繼承稽核項目(0) 確定<取消 取消 確定 取消		確定 取消 要用(&)
裕核 若要被視或論輪稽核項目的詳細資料,請選取該項目,再按一下 [編輯]。 物什名額: C.VJserskådministrator/Desktop/temp 宿枝項目(): 「健用者、群組 或內違安全性原則」 「服型」 名編 「客取」 21× 「「」 「健用者、群組 或內違安全性原則」 「使用者、群組 或內違安全性原則」 5 「炒け物理型(0)」 (位置(1) 「「」 「「」」 「」 「」 「」 「」 「」 「」 「」 「」」 「」 「」」 「」 「」」 「」 「」 「」 「」 「新增(2)」 」 「」 「」」」 「」 「」」 「」 「」 「」 「」」 「」 「」」」 「」 「」」」 「」 「」」 「」 「」 「」 「」」 「」 「」」」 「」 「」」」 「」 「」」 「」 「」」」 「」 「」」」 「」 「」」」 「」 <th>🔒 temp 的進階安全性設定</th> <th>X</th>	🔒 temp 的進階安全性設定	X
若要被視或編輯褶枝項目的詳細資料,諸選取該項目,再按一下[編輯]。 物件名稱: C:Userskidministrator/Desktop/temp 稽校項目(1): 選擇這個物件類型(2): 類型 名稱 存取 准承自 繁月30 (位居者、群組或內建安全性原則) 後還個位置(P): (位置(L)) (WIN2X8) (位置(L)) 新增(D) ////////////////////////////////////	稽核	
地位 A Mark (1) D Mark (2) 物件名籍: C: Users\& dministrator\Desktop\temp 这 使用者 或 群組 交 (注 使用者 或 群組 交 (注 原則 (使用者 或 群組 (使用者 动 群組 (使用 (使用 (か)((使用 (使用 (か)((' 若要檢視或編輯藉核項目的詳細資料,諸選取該項目,再按—下	v£e#1 ∘
P/P 名稱: C:00 sers Administrator Uesk top temp 糖核項目(T): 選擇這個物件類型(S):		
推荐或信目(). 通音本面信的/开来型(0). 推型 名稱 存取 繼承自 要用到 使用者、群組或內違安全性原則 (動件類型(0) 從這個位置(p): 位置(L) WIN2K8 位置(L) 節輸(四) (師時(四) 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	物件名稱: C:VU sersilla d ministrator Wesktop temp	
★ ●<	181% (只有)(1). 「括刑」 (名紹 (左下))	
● ●		
4 (1) ● 新增(D) 編輯(D) ● 従此物件的父項包括繼承稽核項目(D) (1) ● 以此物件的繼承稽核項目取代所有子条現有的繼承稽核項目(P) 2 確定 取消 確定 取消 確定 取消 確定 取消 確定 取消 確定 取消		1023回回亚直(F). WIN2K8 位罢(L)
新增(D) 新辑(E) 一 一 一 他 他 他 他 他 他 他 他 他 他 他 ● </th <th></th> <th></th>		
新增(D) 編輯(E) 刪除(R) ☑ 從此物件的父項包括繼承稽核項目(D) 進階(A) 確定 取消 □ 以此物件的繼承稽核項目取代所有子系現有的繼承稽核項目(P) 確定 取消 確定 取消 確定 取消	A	
 ✓ 從此物件的父項包括繼承稽核項目(1) □ 以此物件的繼承稽核項目取代所有子系現有的繼承稽核項目(2) 種挖物件存取的需求為何? 確定 取消 確定 取消 確定 取消 	<u>4</u>	・ ・
 ✓ 從此物件的父項包括繼承稽核項目(1) □ 以此物件的繼承稽核項目取代所有子系現有的繼承稽核項目(2) <u>稽花物件存取的需求為何?</u> <u>確定</u>取消 <u>雲用(Δ)</u> 	4 新増の) [編輯(E) [删除(R)]	諸朝人初伴名稱來違取 (<u>重妙</u>)(<u>E</u>): dola 7
□ 以此物件的繼承稽核項目取代所有子系現有的繼承稽核項目(P) <u> 藉核物件存取的需求為何?</u> <u> 確定 取消 </u>	4 新増 □) 編輯(E) ■ 間除(R)	諸朝人初伴名福米違取(<u>朝砂</u>)(<u>b</u>): 検宣名額(C) dola 夜宣名額(C) 進階(A) 確定 取消
്	4 新增(D) 编辑(E) 删除(R) ✓ 從此物件的父項包括繼承稽核項目(1)	·
	 新增(D) 編輯(E) 剛除(R) 從此物件的父項包括繼承稽核項目(D) 以此物件的繼承稽核項目取代所有子条現有的繼承稽核項目(P) 	諸輸入物件名補來違取 (重型)(重): 檢查名稱(C) dola 7 進階(A) 確定
確定 取消 裏用(A) 第二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十	 新增(D) 編輯(E) 刪除(R) 從此物件的父項包括繼承稽核項目(D) 以此物件的繼承稽核項目取代所有子系現有的繼承稽核項目(P) 	諸輸入物件名稱來違取 (重控)(也): 檢查名稱(C) dola 7 進階(A) 確定 取消
	 新增 (□) (編輯(□) 剛除(ℝ))	諸輸人物伴名補外違取 (重控)(也): 檢查名稱(C) 」 一 建階(A) 確定

8. 稽核項目設定:

勾選所有稽核項目的 [成功]及 [失敗], 設定完成後按 [確定]。

🕌 temp 的稽核項目		×
物件		
名稱(N): dola (WIN2K8Vdola)		變更(C)
安州社(0). 這個員科交、丁員科 存取(3):	成功	上
完全控制 周遊資料夾/執行檔案 列出資料夾/續取資料 讀取屬性 讀取擴充屬性 建立檔案/寫入資料 建立資料夾/附加資料 寫入屬性 寫入擴充屬性 刪除子資料夾及檔案 刪除	র র র র র র র র র	
□ 僅套用這些稽核項目到此容器 □ 及(或)容器(T) 管理稽核		治防清除(L)
	確定	取消

9. 在進階安全性設定完成後,點選 [確定]。

液 吉要檢視或編輯					
' 苦要檢視或編輯					
	罐核项目的详细资料,常	·骤取该项日,重按——7	≂ 12度時号1。		
	*181%**********************************		Dumated 1		
勿件名稱:	C:\Users\Administrator\De	sktop\temp			
著核項目(T):					
類型	名稱	存取	繼承自	▲ 套用到	
全部	dola (WIN2K8\dola)	完全控制	<非繼承的>	這個資料夾、子資…	
	(6株)(7)	mulite /m x			
新増(U)		mthrs (K)			
✔ 従此物件的;	父項包括繼承稽核項目(I)				
- 以此物件的:	繼承藉核項目取代所有子	多現有的繼承藉核項日	ውነ		
	@#481X-X H4X14/1/31	луурлаладин түсүр ш	¥7		
满核物件存取的	如季求首何?				
			確定	取消)

temp 的進	階安全	性設定					×
使用權限	稽核	擁有者 有效權限					
若要檢視或	或編輯稽	液項目的詳細資料,該	耀取該項目,再	朝安一下 [编輯]。		
物件名稱:	C	:\Users\Administrator\De	sktop\temp				
稽核項目((T):						
類型	名	稱	存取	#		套用到	
全部	do	la (WIN2K8Vdola)	完全控制			這個資料夾	、子資
編輯()	E)						
🔽 従此物	件的父	頁包括繼承稽核項目(I)					
<u> 藉核物件</u> 7	存取的需	求為何?					
					確定	取消	套用(A)

10. 在分享資料夾設定完成後·點選 [關閉]。

📕 temp 內容				×
一般 共用	安全性以前的	的版本 自訂	1	
物件名稱:	C:\Users\Administi	ator\Desktop\ten	np	
群組或使用者名	稱 (G):			
& SYSTEM				
al dola (WIN2	K8Vdola)			
🤱 👗 Administrat	or (WIN2K8\Admi	nistrator)		I
🤽 Administrat	ors (WIN2K8\Adm	inistrators)		
若要變更使用權	驟,請按一下 係	编輯]。	編輯(E)	
dola的權限(P)		允許	拒絕	
完全控制		\checkmark	_	
修改		~		
讀取和執行		~		I
列出資料夾的]容	~		I
調取		\checkmark	-	
如需符然權限到 階]。	3進階設定,調技	一下[建 	進階(∀)	
深入瞭解存取招	制及權限			
	關閉	取消	套用(A)	

11. 點選 [開始功能表 / 系統管理工具 / 電腦管理]。



12. 點選 [系統工具 / 共用資料夾 / 共用]。

🛃 電響管理				
檔案(F) 執行(A) 檢視(V) 說明(H)				
🗢 🔿 📶 🖸 🔂 📷				
 ■ 脳管理(本機) ● 千作排程器 ● 千作排程器 ● 千件掛視器 ● 共用資料夾 ● 共用資料夾 ● 東田 ○ 丁作階段 ◎ 同靠性和效能 ● 装置管理員 □ ● 存放装置 ● 磁碟管理 ● 服務及應用程式 	共用 ▲ MADMIN\$ MADMIN\$ C\$ IPC\$ NETLO NETLO SYSVOL temp Users	資料夾路徑 C:\Windows\SYSVO C:\Windows\SYSVO C:\temp\npartner C:\Windows\SYSVO C:\temp C:\Users	製 朝 製 朝 製 前 d 製 前 d の 家 製 前 d の 家 製 前 d の 家 製 前 d の 家 製 前 d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 家 製 い d の 来 と い 古 の 来 の 、	##月 0 0 0 0 0 0 0 0
	,			

13. 在[共用]點擊滑鼠右鍵,點選[新增共用]。



- 14. 建立共用資料夾精靈:
 - (1) 點選 [下一步]。

建立共用資料夾精靈		×
	歡迎使用建立共用資料夾精靈	
22	這個精靈協助您共用電腦資料夾,讓您的網路或工作群 組中的其他電腦因此可以存取它。	
	Windows防火牆將會設定允許這個資料夾和其他電腦共 用,請詳閱這對於 Windows防火牆和您電腦的安全性會 有何影響。	
	深入了解 <u>Windows防火牆</u>	
	請按 [下一步] 繼續。	
	<上一步(B) 下一步(N) > 取消	

(2) 按 [瀏覽] 指定欲共用資料夾的檔案路徑,完成後按 [下一步]。

建立共用資料夾精囊	ž	×
資料夾路徑 指定您想要共	用的資料夾路徑。	22
電腦名稱(C):	WIN2K8	
請輸入您要共用的	的資料夾路徑或按[瀏覽]選取或新增資料夾。	
資料夾路徑(F):	C:\Users\Administrator\Desktop\temp	瀏覽(0)
範例:	C:\Docs\Public	Γ
	<u> < 上一步(B</u> 下一步)	N) > 取消

(3) 點選 [下一步]。

建立共用資料夾精靈		×
名称、描述和設定 指定其他人如何]透過網路看到和使用此共用。	22
輸入共用的相關資言 更]∘	R以供使用者参考。若要修改 離 線時內容的使用方法,	請按一下 [變
共用名稱(S):	temp	
共用路徑(P):	WWIN2K8\temp	
描述(D):		
離線設定(0) :	已選取離線時可供使用的檔案和程式	變更(C)
	<上一步(E) 下一步(N) >	取消

(4) 點選 [完成]。

建立共用資料夾精靈 🛛 🔀
共用資料夾種限 您可以使用權限來控制哪些人可以看到這個資料夾,以及其存取權層級。
為共用的資料夾設定您要的權限種類。
● 所有使用者都有唯讀存取權(A)
○ 糸統管理員有完整存取權;其他使用者只有唯讀存取權(R)
系統管理員有完整存取權;其他使用者沒有任何存取權(O)
○ 自訂使用權限(C)
自訂(U)
根據預設值,此資料夾上僅設定共用使用權限。若要控制此資料夾的本機存取權限 或資料夾中的物件,請按一下 [自訂],然後修改 [安全性] 索引標籤中的權限,以在 資料夾上套用特定權限。
< 上一步(B) 完成 取消

(5) 點選 [完成]。

共 用成功
出た前に(丁)・
您已成功完成共用資料夾精靈。
▼ ★ 西 (*)、
摘要(s): 您已經在 \\WIN2K8 選取下列共用設定: 資料夾路徑: C:\Users\Administrator\Desktop\temp 共用名稱: temp 共用路徑: \\WIN2K8\temp
v
□ 當我按 [完成] 時,再次執行精靈以共用另一個資料 夾(₩)
要關閉這個精靈,諸按一下 [完成]。

- 15. 設定共用資料夾使用者:
 - (1) 滑鼠雙擊分享的資料夾。
 - (2) 點選 [共用使用權限] 索引標籤。
 - (3) 點選 [新增]。
 - (4) 若要選擇其他電腦名稱,可點選 [位置],選擇其他電腦名稱。
 - (5) 可於此空白處直接輸入已知的使用者帳號後,按[檢查名稱]檢查存不存在。
 - (6) 設定完成後按 [確定]。

』。 電腦管理			_ 0	X	
檔案(F) 執行(A) 檢視(V) 說	明(H)				
🗢 🔿 🞽 💼 🕒 🗟	2				
🛃 電腦管理 (本機)	_ 共用… ▲ 資料夾路徑	類型	動作	_	
□ 🎁 系統工具	ADMIN\$ C:\Windows	Windows	共用		
日 🕑 工作排程符		Windows	其他動作	•	
	share fo C.\share folder	Windows			
武力 共用	📷 temp C:\Users\Administrator\Desktop\temp	Windows	temp	<u> </u>	
1 工作階段	B Users C:\Users	Windows	其他動作	•	
11月00 11月00 111余 11 ● ● 本機使用者和群組					
 □ 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	te. Cy		×		
▲ 装置管理員	——般 共用使用權限 ————————————————————————————————————				
□ □ 27 15以後直	群组或使用者名称(G);				
■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	& Everyone		-		
				-	
<u>,</u>) 除(R)		? ×
		·····	~	h.	
	Everyone 的權限(P) 方	は許 拒絶		" 建安全性原则	1000000000000000000000000000000000000
	完全控制			extina	
			WINZKO		1业置(L)
			• • • • • • • • • • • • • • • • • • •	(<u>範例</u>)(E):	
			dola		檢查名稱(C)
	深入瞭解存取控制及權限			- 6	
		- mr 1			麻完 取消
		又)月 要用			

16. 設定共用使用權限:

點選使用者帳號,勾選允許[完全控制]、[變更]及[讀取]權限,設定完成後按[確定]。

temp 內容		×
一般 共用使用權限 安全性		
群組或使用者名稱(G):		
💷 Everyone		
👗 dola (WIN2K8\dola)		
•	新增(D)	刪除(R)
dola的權限(P)	允許	拒絕
完全控制		
變更	\checkmark	
讀取		
<u> </u>		
確定	取消	套用(A)

4 Windows 2012 Server 稽核設定

本章節主要說明以下操作設定:

1. 設定本機使用者登入登出的稽核原則。2. 設定共享資料夾權限與稽核原則。

Windows 2012 Server 登入登出的稽核原則和目錄分享的稽核原則,預設是關閉的。

安裝 NXLOG 的步驟,詳細請參閱第一章節。

4.1設定本機登入登出的稽核原則

設定步驟如下:

以系統管理員權限的帳戶 administrator 登入 Windows 2012 Server。點選[開始 / 系統管理工具 / 本機安全性原則], 滑鼠點兩下開啟 [本機安全性原則(Local Security Policy)]。



2. 點選[安全性設定/本機原則/稽核原則]。

- 3. 定義下列的原則設定值:
 - (1) 稽核登入事件(Audit logon events):

滑鼠雙擊 [稽核登入事件],勾選 [成功]及 [失敗],設定完成後按 [確定]。



(2) 稽核帳戶登入事件(Audit account logon events):

滑鼠雙擊 [稽核帳戶登入事件],勾選 [成功]及[失敗],設定完成後按[確定]。



(3) 稽核物件存取(Audit object access):

滑鼠雙擊 [稽核物件存取]

成功:若欲稽核成功事件的 Log,請勾選 [成功] 核取方塊。

失敗:若欲稽核失敗事件的 Log,請勾選 [失敗] 核取方塊。

設定完成後按 [確定]。

註:若 Windows 2012 Server 不做檔案伺服器稽核(File server audit)

建議不要勾選成功與失敗的設定值, 以避免 Windows 稽核多餘且冗長的物件存取事件然後轉換 成 syslog 後發送給 N-Reporter [,] 會影響主機的運作效能



(4) 稽核原則變更(Audit policy change):

滑鼠雙擊 [稽核原則變更],勾選 [成功]及 [失敗],設定完成後按 [確定]。

(5) 稽核帳戶管理(Audit account management):
 雙擊 [稽核帳戶管理]·勾選 [成功]及[失敗]·設定完成後按 [確定]。

4.2 設定共享資料夾權限與稽核原則

設定步驟如下:

1. 點選 [伺服器管理員 / 檔案和存放服務 / 共用 / 工作 / 新增共用...]。



2. 滑鼠左點 [SMB 共用 – 快速] , 點選 [下一步]。

a	新增共用精靈	
選取此共用的設定 選取設定檔 共用位置 共用名稿 其他設定 權限 確認 結果		描述(D): 這個基本設定檔代表建立 SMB 檔案共用的最快方式,通 常會用來與 Windows 電腦共用檔案。 • 適用於一般檔案共用 • 稍後可使用 [內容] 對話方塊來設定進階選項
	< 1	步(P) 下步(N) > 建立(C) 取消

3. 點選[輸入自訂路徑] · 本例輸入 " C:\share_folder " · 點選[下一步] ·

h		新増	共用精靈				-		x
選取此共用的伺	同服器	和路徑							
港取設定標	伺服								
共用位置	同	服器名稱	狀態	叢集/	自色	擁有者節點			
	V	IN2012R2AD	線上	未叢	東處理				
大市石柄									
兵他故走									
	10000	en e							
	共用	1位置: 佐磁礎底躍取00-							
		は 確認 あん いっ し し し し し し し し し し し し し し し し し し	可用空間	容量	福宏系统				
		C:	49.8 GB	59.7 GB	NTFS				
		檔案共用的位置將會是所	選磁碟區上 \Shares	目錄中的	新資料夾。				
	۲	輸入自訂路徑(T):							
		c:\share_folder	_				濯	覽(B).	
			-						
			<	下一步	N) >	建立(0)	-	TO YAK	
			~ +	1 31		Æ11(C)		AL /P	

4. 在 共用名稱 欄位輸入所要共用的資料夾的名稱, 本例為輸入[share_folder], 然後按[下一步]。

a	新增共用精靈	×
▲ 指定共用名稱 選取設定檔 共用位置 其用名稱 其他設定 裙限 確認 結果	新增共用精整 共用名稱(A): share_folder 共用描述(D): 要共用的本機路徑(L): c:\share_folder 要共用的遠端路徑(R): \\WIN2012R2AD\share_folder	
	<上一歩(P) 下一歩(N) > 建立(C)	取消

5. 勾選 [啟用存取型列舉],點選[下一步]。

à	新增共用精靈
▶ ▶ ▶ ▶ ⇒ ⇒ ⇒ ⇒ ⇒ ⇒ ⇒ ⇒ ⇒ ⇒ ⇒ ⇒ >	 ✓ 飲用存取型列錄(A) ✓ 飲用存取型列錄(A) 存取型列錄只會顯示使用者有權存取的檔案和資料夾。如果使用者不具資料夾的讀取(或同等)權限,Windows,會陽藏該資料夾,不讓使用者看見。 ✓ 允許對共用進行快取(W) 供取讓難線使用者能夠使用共用的內容。如果已安裝網路檔案角色服務的 BranchCache,您可以 在共用上較用 BranchCache(E) BranchCache 可讓分公司的電腦快取從此共用下載的檔案,然後讓檔案可安全地提供給分公 司的其他電腦使用。 一 加密資料存取(E) 若診劑,將會加密此共用的場端檔案存取。此舉可確保資料在從共用購入/移出時。免於遭受 未經授權的存取。如果此方塊已勾選旦變成灰色,即表示系統管理員已對整個伺服器開啟加密功 能。

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

6. 點選 [自訂權限... / 稽核 / 新增]。

		新增共用精靈			- 🗆 X
設定權限以控制	存取權				
選取設定檔	己使用資料	夾權限,共用權限(可能還有)	集中存取原則)的組合,來設定存取共用上之	當案的權
共用位置	限•				
共用名稱	共用權限:	所有人完整控制			
其他設定	資料夾權限	(F):	78-2		
權限	類型	主體	存取	客用到 ロタスペリナスペロ	
確認	元計	CREATOR OWNER	完主控制	六月于資料灭反個柔 這個營料本及子營料本	
結果	允許	BUILTIN\Users	讀取與執行	這個資料夾、子資料夾及檔案	
	允許	BUILTIN\Administrators	完全控制	這個資料夾、子資料夾及檔案	
	允許	NT AUTHORITY\SYSTEM	完全控制	這個資料夾、子資料夾及檔案	
	允許	Everyone	完全控制	這個資料夾、子資料夾及檔案	
	自訂權网	R(C)			
	1				
	/				
	1				
		< 上-	-步(P) 下-	-步(N) > 建立(C)	取消
	1				
B .	_/	share_folder 的進階安全	性設定		_ D ×
名稿: c:\share_folder					
擁有書: Administrators (NPW	2012R2\Admi	inistrators) 関更(C)			
權限 共用 稲	核有效有	取權			
如需其他資訊,請按關下積核項目	如果要修改稽核	項目,請選取項目,然後按一下	[編輯] (如果適	用) •	
稽核項目:					
類型 主體		存取 编	承目	賽用到	
総全部 Everyone		完全控制 無	l l	這個資料夾、子資料夾	及橫案
新增(D) 移除(R) 檢視(V)				
新墳(D) 修除(R) 檢視(停用編承()	VJ				
新増(0) 修除(R) 協視(停用編承(0) 以此物件中的可编承稽核項目取代	V)	項目(P)			
新増(D) 修除(R) 檢視(「停用編承() 」以此物件中的可編承欄核項目取代	V) ;所有子物件種枝	項目(P)		28-75 S-134	客田(山)

7. 左點 [選取一個主體]·如果欲稽核所有使用者·在物件名稱欄位的空白處輸入 "everyone "後, 點選檢查名稱·按 [確定]。

類型: 成功	> 選取使	用者、電腦、服務帳戶或群組	×	
 (第四到): 這個資料次、子資料応及欄裏 (第金控制) (第金控制) (修改) (※) 列出資料次内容 (※) 列出資料次内容 	使用者、群組或内護安全性主體 <th></th> <th>約件類型(O) 位置(L) 檢查名稱(C)</th> <th>顯示遠暗橋</th>		約件類型(O) 位置(L) 檢查名稱(C)	顯示遠暗橋
□ 高入 □ 特殊浮取權限 □ 只烧這些積核設定套用至此容器內的 所増一個條件以限制此積核項目的範圍	唐谷(石)(或) 音繇(石) 唐器(石) 唐器(石) 唐器(石) 月方當條件符合時,才會記錄安全性事件。	確定	,]	全部清除
新増焼件(D)				

8. 類型 下拉選 [全部],基本權限勾選 [完全控制],然後按點 [確定]。

₿.	share_folder 的稽核項目	_ D X
主體: 類型: 套用到:	Everyone 選取一個主體 全部	
基本權限	 ● 完全控制 ● 修改 ● 補取和執行 ● 列出資料夾内容 ● 補取 ● 「補取 ● 「補取 	顯示進階權限
□ 只將這 新増一個 新増條件(□ 时末行和X值和X 雲遊福核設定套用至此容器內的物件和(或) 容器(T) 「條件以限制此稽核項目的範圍。只有當條件符合時,才會記錄安全性事件。 (D)	全部遺除
	確定	取消

9. 若稽核設定完成後·按[確定]。按[下一步]。按[建立]/[關閉],完成設定。

			share	e_folder 的進階安全性設定	
名稿:	c:\share_fold	er			
擁有者:	Administrato	rs (NPWIN201	12R2\Administrators)) 奠更(C)	
權限	共用	稽核	有效存取權		
如需其他資」 稽核項目:	讯·請按兩下稽核	§項目・如果勇	更修改稽核項目,請	灌取項目,然後按一下 [編輯] ()	如果適用)。
項型 終 全部	主體 Everyone		存取 完全控制	/ 建承自 無	春用到 這個資料夾、子資料夾及檔案
			/		
新增(D)	移陳(R)	編輯(E)			
停用繼承(0				
□ 以此物件	中的可繼承稽核功	自取代所有于	子物件稽核項目(P)		
					確定 取消 套用(A)
0					確定 取満 麥用(A)
3				新增共用精靈	確定 取消 套用(A)
確認刻	巽取項目			新增共用精靈	確定 取満 套用(A)
確認建	矍取項目	1 Tř	笔器以下為正確	新增共用精靈	建立].
了 確認到 ^{選取設} 共用位	選取項目 _{定橋 署}	荷	筆認以下為正確 共用位置	新増共用精靈 新聞 (記)	確定 取満 変用(A) ■ □ □
2 確認效 選取設 共用名	豊取項目 ^{定橋} ^営	1 64	筆認以下為正確 共用位置 何服器: 要集角会:	新增共用精靈 新增共用精靈 新増共用精靈 ジェ ジェーン ジェ	建立] -
■ 石在記 変取設 共用名 其他設 櫂限	選取項目 ^{定橋} ^営 ^第	- All	筆認以下為正確 共用位置 伺服器: 菱集角色: 本機路徑:	新増共用精靈 新増共用精靈	建立] -
百 在 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	矍取項目 ^{定橋} ^営 定	稻	筆認以下為正確 共用位置 伺服集為色: 本機路徑: 共用内容 共用内容	新增共用精靈 新增共用精靈 <	建立] -
■ 石宿 一 一 一 一 一 一 二 一 二 二 二 二 二 二 二 二 二 二 二 二 二	豊取項目 ^{定橋} 置 編 定	Ξ.	 筆認以下為正確 共用位置 伺服器: 電機角色: 本機路徑: 共用內容 共用名稱: 通訊協定: 	新增共用精靈 翻當決定 · 然後按一下 [發 WIN2012R2AD 未叢集處理 c\share_folder share_folder1 SMB	確定 取満 変用(A) ■ □ □
百 在 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	選取項目 ^{定橋} 署 程	Τά	筆認以下為正確 共用位置 伺服集角色: 本機路徑: 共用訊器丸容 其用訊器型列舉: 快取處理:	新增共用精靈 新增共用精靈 新増共用精靈 WIN2012R2AD 未叢集處理 c:\share_folder share_folder1 SMB 已設用 已設用 已設用 已設用 こ SMB 日 SMB 日 SMB 日 SMB 日 SM S SM S SM S SM S	建立] -
■ 石 確 認 一 一 一 一 一 一 一 二 二 二 二 二 二 二 二 二 二 二 二 二	選取項目 ^{定檔} 置 編 定	ά Π	筆認以下為正確 共用位置 伺服器: 電集角色: 本機路徑: 共用內容 共用名稱: 通訊磁型列舉: 快取處理: BranchCache: 加密容料:	新增共用精靈	確定 取満 委用(A) ■ □ □
■ 確認 選取用名設 確認 建築	豊取項目 ^{定橋} 置 報 定	Τά	筆認以下為正確 共用位置 伺服集會色: 本機路徑: 共用內容 共用名稱: 通訊盛定: 存取型列舉: 快取處理: BranchCache: 加密資料:	新增共用精靈 新增共用精靈 WIN2012R2AD 未叢集處理 c:\share_folder share_folder1 SMB 已設用 已較用 已停用 已停用	建立] -
■ 石 確 認 認 説 成 位 名 設 し 位 名 設 し 位 名 設 、 二 、 、 、 、 、 、 、 、 、 、 、 、 、	豊取項目 ^{定橋} 置 編 定	τ. Τ	筆認以下為正確 共用位置 伺服器: 毒機路色: 本機路徑: 共用內容 共用名稱: 通訊留定: 存取型列舉: 快取處理: BranchCache: 加密資料:	新增共用精靈	· 確定 取消 委用(A) - □ 3 建立] -
■ 確認認 選共用用他限 確認 編果		ά	筆認以下為正確 共用位置 伺服集角色: 本機路徑: 共用內容 共用內容 共用和名稱: 通訊短處理: BranchCache: 加密資料:	新增共用精靈 新增共用精靈 WiN2012R2AD 未叢集處理 c:\share_folder share_folder SMB 已設用 已較用 已使用 已停用 已停用 日停用 日停用 日	建立] -
■ 石 在 記 2 3 3 3 3 3 3 3 3 3 3 3 3 3	豊取項目 ^{定橋} 置 編 定	T T	筆認以下為正確 共用位置 伺服器: 毒機路合: 本機路徑: 共用內容 共用名稱: 通訊留定: 存取型列舉: 快取處理: BranchCache: 加密資料:	新增共用精靈 翻進定 · 然後按一下 [刻 WIN2012R2AD 未叢集處理 c\share_folder1 SMB 已較用 已較用 已停用 已停用	· 確定 取消 委用(A) - □ 3 建立] -
在在記 一次 一次 一次 一次 一次 一次 一次 一次 一次 一次 一次 一次 一次	<u>異取項</u> 目 ^{定檔} 署 稱 定	Τ	筆認以下為正確 共用位置 伺服器: 毒柴機路徑: 共用內容 共用內容 共用和醫定: 存取處理: BranchCache: 加密資料:	新增共用精靈 新增共用精靈 ¥設定 · 然後按一下 [刻 WIN2012R2AD 未叢集處理 c:\share_folder1 SMB 已設用 已較用 已候用 已停用	確定 取消 委用(A) 重立]-

5 將設備加入系統及 Syslog 資料格式及 Facility 的設定

- (1) 登入 N-Reporter / N-Cloud 系統



(3) 滑鼠點選 [未知設備的編輯圖示],在 IP 欄位中應該能看見此台的設備的 IP。請輸入一個方便 記憶的設備名稱,接著在[資料格式]下拉選單中依設備的類型選擇{Windows},勾選[啟動接 收],按下[確定],即完成設備的系統新增程序

G	設備管理 ► Sysle	og 設備 🗌 頁面自動更新 (12	10秒)	新増或編	輯Syslog設備		×
h	所屬:頁域 ▶	All Devices	 □ 計封 *設備議 □ <l< th=""><th>step 1</th><th>區域: 名稱:</th><th>Root</th><th>•</th></l<>	step 1	區域: 名稱:	Root	•
	總筆 数:15				設備IP:	100.10.1.66	
• ?	操作	所屬領域 ▲	Ib		設備種類: 資料格式:	 Action 設備 Windows 	•
•	-	未知設備 (Global)	101100.000		Facility:		¥
					語条:	UTF8	•
	18	未知設備 (Global)	192.168.2.15	step 2	接收狀態: 所屬資料夾:	 ● 敵動接收 ● 暫停接收 其他 [28] 	¥
	\$\. \$\.	Global	192.168.0.251			確定	取消

連絡資訊

N-Partner 公司連絡方式: TEL: +886-4-23752865 FAX: +886-4-23757458 有關技術問題請洽: Email: support@npartnertech.com Skype : support@npartnertech.com 有關業務相關問題請洽: Email: sales@npartnertech.com

