

N- Partner N-REPORTER

如何使用 NXLOG 管理配置 Windows Server AD 日誌 V 009 (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 AD 2003/2008/2012/2016 的日誌(Event log)·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 AD、Windows Server 2008 AD、Windows Server 2012 AD、Windows 2016 AD。

NXLOG 適用於記錄大量事件的環境。Windows Server 日誌(Event log)每秒最大記錄速率超過700筆,請使用 NXLOG 的配置方式。

文件章節如下:

1	安裝設定	Windows Server AD 環境中的 NXLog	. 2
	1.1	For Windows Server 2003 AD	2
	1.2	For Windows Server 2008 AD	6
	1.3	For Windows Server 2012 AD	10
	1.4	For Windows Server 2016 AD	15
2	Windows 2	2003 Active Directory Server 稽核設定	19
	2.1	設定 Windows 2003 AD Server 網域使用者登入登出的稽核原則	19
	2.2	設定共享資料夾權限與稽核原則	23
3	Windows 2	2008 Active Directory Server 稽核設定	30
	3.1	設定網域使用者登入登出的稽核原則	30
	3.2	設定共享資料夾權限與稽核原則	36
4	Windows 2	2012 Active Directory Server 稽核設定	47
	4.1	設定網域使用者登入登出的稽核原則	47
	4.2	設定共享資料夾權限與稽核原則	52
5	Windows 2	2016 Active Directory Server 稽核設定	58
	5.1	設定網域使用者登入登出的稽核原則	58
	5.2	設定共享資料夾權限與稽核原則	63
6	將設備加	入系統及 Syslog 資料格式及 Facility 的設定	69
逴	極資訊		70

1 安裝設定 Windows Server AD 環境中的 NXLog

1.1 For Windows Server 2003 AD

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:

請全程以具有 系統管理員(Administrator) 的帳號權限身分登入系統並操作相關步驟。(否則可能 會因權限不足的問題導致設定無作用)

滑鼠雙點 nxlog-ce-2.9.1716.msi,點選[Install],執行 NXLog 程式安裝步驟。

3. 下載設定 Windows 2003 的 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 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 AD 所有 Eventlog。使用者若是需要 Windows AD 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 AD 的 Eventlog。

請注意!! 此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。

若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重,請使用上述章節 nxlog_win2k3.conf 的配置檔 for Windows 2003.

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 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>
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 " 。 紅色文字部位請輸入 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:\Pr	ogram Files (x86)\mxlog/conf/mxlog.conf - Notepad++	_ 🗆 ×
檔案(F)	编辑》匠母找《S 檢視 (2) 编碼 (2) 程式語言 (L) 自訂 (1) 巨集 執行 外掛 模組 (2) 視窗 (2) 2	X
🕞 🖪	▐▝▋▝▖▙▎▞▐▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖▖	
😑 nxlog	conf 🔤 sologilog	
7	#define ROOT C:\Program Files\nxlog	
8	define ROOT C:\Program Files (x86)\nxlog	
9		
10	Moduledir %ROOT%\modules	
11	CacheDir %ROOI%\data	
12	Pidfile %RCOT%\data\nxlog.pid	
13	Spooller %KOU% data	
14	LogFile anOUTA(data(nxlog.log	
16	(Extension evelop)	
17	Modula vm cvalag	
18	nouse an system	
19		
20	# For windows 2003 and earlier use the following:	
21	Module im research of	
22	Exec parse syslog bs(): \	
23	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; } \	
24	else if (\$SourceName == "Service Control Manager") {	
25	else if (\$SourceName =~ /^MSSQL*/) { \$SyslogFacilityValue = 18; } \	
26	else\	
27		
28	drop();	
29		
30		
31		
32	 vutput out_eventlog> 	
33	Hoote an_uap	
34	Post 51/	
36	rone Subsequent (Stypent TD) + "· " + Subseque.	
37	Even if (SeventType = 'FRROR' on SeventType = 'AIDIT FAILURE') { System Sevenity/Value = 3. })	
38	else if (%EventType == 'WARNING') { \$\sigma_seventTyPalue = 4: }	
39	else if (%EventType == 'INFO' or %EventType == 'AUDIT SUCCESS') { %SyslogSevenitV4]ue = 5: }	
40	Execto system bid to the territory of the contract of the system of the	
41	0utput	
42		
43	<route eventlog=""></route>	
44	Path in_eventlog => out_eventlog	
45		
erl source	file ength:2025 lines:45 Ln:45 Col:9 Sel:0 DostWindows ANSI	INS

5. 啟動 NXLOG 程式:

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	
#會看到以下訊息	
The nxlog service is starting.	
The nxlog service was started successfully.	

b. [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 " 若沒有顯示 Error 的訊息,表示正常啟動。

🞬 C:\Program Files (x86)\nxlog\data\nx	clog.log - Notepad++		
檔案 1 [2] 編輯 12] 尋找 ③ 檢視 (V) 編 13 2] □ □ □ □ 13 [2] ☆ □	500) 程式語言(L) 自訂(L) E	〕集 執行 外掛模組(2) 視窗(2) ★ □3 □3 □5 □ 1 □ [15 □2	D? X • • • • • • • • • •
🗎 nxlog.conf 📄 nxlog.log			
1 2014-07-04 14:16:08 INFO 2 2014-07-04 14:16:27 WARNI 3 2014-07-04 14:16:27 WARNI 4 2014-07-04 14:16:29 INFO 5	nxlog-ce-2.7.1191 starte NG stopping nxlog servic NG nxlog-ce received a t nxlog-ce-2.7.1191 starte	d e ermination request signal d	., exiting
Nom length : 244 lines : 5	Ln:1 Col:1 Sel:0	Dos\Windows	ANSI

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

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

N-CLOUD						
Npartner (Global) ~	✔ Home / 設備管理 / 設備樹狀圖					
≡ 爭忤	▲ 設備樹狀圖					
山 報表 1 田	授尋 Q 2 日 U	-				
📑 設備管理 🔳	الس 🕥 Global (123) 🔥 🛕	操作	所屬領域 ≑	IP	設備名稱 🗢	設備種類 令
高 多统管理 田	2 未知設備 (20)	C 🛍	Global	1.1.1.8	1.1.1.8	Syslog
	山 設備資訊編輯	× 🖉 🛍	Global	10.0.0.235	10.0.0235	Flow
	設備基本設定	· · · · · · · · · · · · · · · · · · ·	Global	10.1.34.220	10.1.34.220	🔵 Syslog
	名稱	C 🗇	Global	10.10.10.101	10.10.10.101	Syslog
	Win2003AD_192.168.1.90	2 🖬	Global	10.10.10.2	10.10.10.2	Syslog
		C 🗇	Global	10.10.10.3	10.10.10.3	Syslog
	IP	C 🗇	Global	10.143.238.95	10.143.238.95	Syslog
	192.168.1.90	C 🗇	Global	10.143.238.96	10.143.238.96	🗑 Syslog
		2 🖬	Global	10.63.136.26	10.63.136.26	Syslog
	設備種類	2 🖬	Global	10.63.136.26	10.63.136.26	Syslog
	Syslog Flow SNMP		Global	10.64.103.245	10.64.103.245	Syslog
		e 1	Global	10.64.103.44	10.64.103.44	Syslog
	Syslog 相關設定	C 🛍	Global	172.16.1.235	172.16.1.235	Syslog
		2 🖬	Global	191.168.2.252	191.168.2.252	🤁 Flow
	資料格式		Global	192.168.0.253	192.168.0.253	Flow
	Windows AD	✓ 3 2 1	Global	192.168.1.43	192.168.1.43	Syslog
		l C û	Global	192.168.1.90	192.168.1.90	Syslog
	Facility	I	Global	192.168.10.14	192.168.10.14	Syslog
		• 🖉 🗇	Global	192.168.10.15	192.168.10.15	Syslog
			Global	192.168.2.86	192.168.2.86	Syslog
	编码力式					
	BIG5	Y				
		25 🔻	▲ ▲ 第1	共1頁 ▶ ▶ 0		
	- 確定	取消				

8. 語系選擇:

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

1.2 For Windows Server 2008 AD

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. 安装 NXLOG:

請全程以具有 系統管理員(Administrator) 的帳號權限身分登入系統並操作相關步驟。(否則可能 會因權限不足的問題導致設定無作用)

滑鼠雙點 nxlog-ce-2.9.1716.msi,點選[Install],執行 NXLog 程式安裝步驟。

3. 下載設定 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 " 路徑中的 NXLOG 配置 檔, 將上面的 URL 上的 nxlog_win2k8.conf 裡的設定內容複製, 然後貼上並覆蓋 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 NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf "

64 位元 OSNXLOG 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 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 AD 所有 Eventlog。使用者若是需要 Windows AD 的法 規報表,請將 nxlog_win2k8_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 AD 的 Eventlog。

請注意!! 此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。

若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重,請使用上述章節 nxlog_win2k8.conf 的配置檔 for Windows 2008.

NREPorter Æ٧

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"> \	
<select path="Security">*[System[(EventID=1100)]]</select>	\
<select path="Security">*[System[(EventID=4769)]]</select>	\
<select path="Security">*[System[(EventID=4768)]]</select>	1
<select path="Security">*[System[(EventID=4771)]]</select>	١
<select path="Security">*[System[(EventID=4616)]]</select>	١
<select path="Security">*[System[(EventID=4624)]]</select>	۱
<select path="Security">*[System[(EventID=4625)]]</select>	۱
<select path="Security">*[System[(EventID=4634)]]</select>	۱
<select path="Security">*[System[(EventID=4647)]]</select>	١
<select path="Security">*[System[(EventID=4648)]]</select>	١
<select path="Security">*[System[(EventID=4656)]]</select>	١
<select path="Security">*[System[(EventID=4719)]]</select>	١
<select path="Security">*[System[(EventID=4720)]]</select>	١
<select path="Security">*[System[(EventID=4722)]]</select>	١
<select path="Security">*[System[(EventID=4723)]]</select>	١
<pre><select path="Security">*[System[(EventID=4724)]]</select></pre>	۰ ۱
<pre><select path="Security">*[System[(EventID=4725)]]</select></pre>	۰ ۱
<pre><select path="Security">*[System[(EventID=4726)]]</select></pre>	``
<pre><select path="Security">*[System[(EventID=4727)]]</select></pre>	``
<pre><select path="Security">*[System[(EventID=4728)]]</select></pre>	ì
<pre><select path="Security">"[System[(EventID=4720)]]</select></pre>	ì
<pre><select path="Security">*[System[(EventID=4729)]]</select></pre>	ì
<pre><select path="Security">*[System[(EventID=4730)]]</select></pre>	ì
<pre><select path="Security">"[System[[EventiD=4737)]]</select></pre>	``
<pre><select path="Security">[System[(EventiD=4732)]]</select></pre>	``
<pre><select path="Security">[System[(EventiD=4735)]]</select></pre>	``
<pre><select path="Security">[System[(EventiD=4734)]]</select></pre> <pre></pre>	\ \
<select path="Security">[System[(EventiD=4735)]]</select>	````
<select path="Security"> [System[(EventiD=4737)]]</select>	\ \
<select path="Security"> [System[(EventitD=4736)]]</select>	`
<select path="Security"> [System[(EventID=4739)]]</select>	\ \
<select path="Security"> [System[(EventID=4740)]]</select>	\ \
<select path="Security"> [System[(EventID=4741)]]</select>	\ \
<select path="Security">^[System[(EventID=4742)]]</select>	\ \
<select path="Security">^[System[(EventID=4743)]]</select>	\ \
<select path="Security">^[System[(EventID=4/44)]]</select>	\
<select path="Security">*[System[(EventID=4745)]]</select>	\
<select path="Security">*[System[(EventID=4748)]]</select>	\
<select path="Security">*[System[(EventID=4749)]]</select>	\
<select path="Security">*[System[(EventID=4750)]]</select>	\
<select path="Security">*[System[(EventID=4753)]]</select>	\
<select path="Security">*[System[(EventID=4754)]]</select>	\
<select path="Security">*[System[(EventID=4755)]]</select>	\
<select path="Security">*[System[(EventID=4756)]]</select>	\
<select path="Security">*[System[(EventID=4758)]]</select>	\
<select path="Security">*[System[(EventID=4759)]]</select>	\
<select path="Security">*[System[(EventID=4760)]]</select>	1
<select path="Security">*[System[(EventID=4763)]]</select>	١
<select path="Security">*[System[(EventID=4764)]]</select>	1
<select path="Security">*[System[(EventID=4767)]]</select>	١
<select path="Security">*[System[(EventID=4778)]]</select>	/
<select path="Security">*[System[(EventID=4783)]]</select>	١
<select path="Security">*[System[(EventID=4800)]]</select>	\
<select path="Security">*[System[(EventID=4801)]]</select>	١
<select path="System">*[System[(EventID=7036)]]</select>	(
<select path="Application">*[System[(EventID=18454)]]<td>ect></td></select>	ect>
<select path="Application">*[System[(EventID=18456)]]<td>ect></td></select>	ect>

\	
<output out_eventlog=""></output>	
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();	
<route eventlog=""></route>	
Path in_eventlog => out_eventlog	

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 " 。 紅色文字部位請輸入 N-Reporter 機器 IP · 本文件範例為輸入 " 192.168.2.64 " 。 設定範例如下圖:

38	<pre>/// /////////////////////////////////</pre>				
30	(Select Path Security / [System[(EventD-4724)]]/Select \				
10	<pre>cSalect radin Security "#[System[(kventub-4724)]]/(salect \ </pre>				
40	<pre>cSclect Path="security"*[System[[FyoatD=4725]]]/(sloct) \ </pre>				
41	<pre></pre>				
42	<pre></pre>				
43	<pre><select <="" [system[(eventd="4720)]]/Select" \="" fach="security" pre=""></select></pre>				
44	<pre> // Select Path = Security // [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]//Select \ // // Select Path = Security // * [System[[EventD=4730]]]// Select \ // // Select Path = Security // * [System[[EventD=4730]]]// Select \ // // Select Path = Security // * [System[[EventD=4730]]]// Select \ // // Select Path = Security // * [System[[EventD=4730]]]// Select \ // // Select Path = Security // * [System[[EventD=4730]]]// Select \ // // Select Path = Security // * [System[[EventD=4730]]]// Select \ // // // Select Path = Security // * [System[[EventD=4730]]]// Select \ // // // // Select Path = Security // * [System[[EventD=4730]]]/ Select \ // // // // Select Path = Security // * [System[[EventD=4730]]/ Select \ // // // // Select \ // // // // Select Path = Security // * [System[[EventD=4730]]/ Select \ // // // // Select Path = Security // * [System[[EventD=4730]]/ Select \ // // // // Select Path = Security // * [System[[EventD=4730]]/ Select \ // // // // Select Path = Security // * [System[[EventD=4700]]/ Select Path = Security // * [System[[EventD=4700]]/ Select Path = Security // * [System[[EventD=4700]]/ Select Path = Security // * [Socurity // * [Soc</pre>				
45	(Select Path Security / [3/stem[[tventD-4731]]]/Select \				
40	<pre><select <="" [system[(tvertub="473)]]//select" \="" fach="security" pre=""></select></pre>				
//8	<pre></pre>				
/19	<pre><select path="Security">*[System[(EventD=/13/4)]]/(Select \ </select></pre>				
50	<pre>cSclect Path="country"*[System[[FyoatTh=4735]]]/(clact)</pre>				
51	<pre><select <="" [system[(eventd="4737)]]//Select" \="" fach="security" pre=""></select></pre>				
52	<pre></pre>				
53	<pre></pre>				
54	<pre><select path="Security">*[System[(FuentID=4741)]]/(Select >)</select></pre>				
55	<pre><select path="Security">*[System([FuentID=4742)]]/(Select >)</select></pre>				
56	<pre><select path="Security">*[System[(FuentID=4743)]]</select> \</pre>				
57	<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>				
58	<pre><select path="Application">*[System[(EventID=18454)1]</select> \</pre>				
59	<pre><select path="Application">*[System[(EventID=18456)]]</select> \</pre>				
60	0uery \				
61	0ueryList				
62					
63					
64	<pre>H<output eventlog="" out=""></output></pre>				
65	Module om udp				
66	Host 192.168.2.64				
67	Port 514				
68	<pre>8 Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message;</pre>				
69	9 Exec if (\$EventID == 18456) { \$SyslogFacilityValue = 18; } \				
70	else { \$\$yslogFacilityValue = 13; }				
71	<pre>Exec if (\$EventType == 'ERROR' or \$EventType == 'AUDIT_FAILURE') { \$SyslogSeverityValue = 3; } \</pre>				
72	2 else if (\$EventType == 'WARNING') { \$SyslogSeverityValue = 4; } \				
73	<pre>3 else if (\$EventType == 'INFO' or \$EventType == 'AUDIT_SUCCESS') { \$SyslogSeverityValue = 5; }</pre>				
74	4 Exec to_syslog_bsd();				
75	L				
76					
77	77 🛱 <route eventlog=""></route>				

5. 啟動 NXLOG 程式:

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

#會看到以下訊息

The nxlog service is starting. The nxlog service was started successfully.

b. [開始]→[所有程式]→[系統管理工具]→[服務]→找到[nxlog],右鍵點服務[nxlog],點 [啟動]或[重新啟動]。

檢查 NXLOG 是否正常啟動: 6.

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。

(x86)\nxlog\data\nxlog.log - Notepad++		
找(S) 檢視(V) 編碼(N) 程式語言(L) 自	f(T) 巨集 執行 外掛棋組(P)) 視窗(₩) ? X
· 🔓 😂 🚜 🗅 🛍 🔁 🖻 Ə 🖻 🗰 🛬	🤫 🤫 🖪 🗟 🚍 ୩	🎼 🐷 🛛 🔳 🕨 🕨 👋
log.log		
17:57:22 WARNING stopping nxlog	service	
17:57:22 WARNING nxlog-ce receiv	ed a termination request	: signal, exiting
17:57:23 INFO nxlog-ce-2.7.1191	started	
Ln:1 Col:1 Sel:0	Dos\Windows	ANSI INS //
	(x86)\nxlog\lata\nxlog.log - Notepad++ 找(S) 檢視(V) 編碼(N) 程式語言(L) 自言 「。 △ ぷ □ □ □ ⊃ C 品 強 log.log 17:57:22 WARNING stopping nxlog 17:57:22 WARNING nxlog-ce receiv 17:57:23 INFO nxlog-ce-2.7.1191 Ln:1 Col:1 Sel:0	(x86)\mxlog\data\mxlog.log - Notepad++ 技(S) 検視(V) 編碼(N) 程式語言(L) 自訂(T) 巨集 執行 外掛模組(P) 「 合 合 4 「 ① ① ② C 鄙 強 3 ペ 『 區 급 三 1 dog.log 17:57:22 WARNING stopping mxlog service 17:57:22 WARNING mxlog-ce received a termination request 17:57:23 INFO mxlog-ce-2.7.1191 started Ln:1 Col:1 Sel:0 Dos\Windows

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

₽ П Ш	▲ 設備樹狀圖					
報表 1 田	援尋 Q 2 日 U 🔹					
設備管理 🖽	🦳 🌏 Global (123) 🛕 🛕	操作	所屬領域 \$	IP 🛋	設備名稱 🗢	設備種類 🗢
系统管理 田 2	- <mark>(2)</mark> 未知設備 (20)	a	Global	1.1.1.8	1.1.1.8	🌘 Syslog
		× 🖉 🛍	Global	10.0.0.235	10.0.0.235	🤀 Flow
	設備基本設定	^ <i>©</i> ±	Global	10.1.34.220	10.1.34.220	Syslog
	名稱	CÎ	Global	10.10.10.101	10.10.101	Syslog
	Wip2008AD 102 168 1 00	C A	Global	10.10.10.2	10.10.10.2	Syslog
	WII2000AD_192.108.1.90	C 🖬	Global	10.10.10.3	10.10.10.3	Syslog
	IP	20	Global	10.143.238.95	10.143.238.95	Syslog
	192.168.1.90	20	Global	10.143.238.96	10.143.238.96	Syslog
		C 🖬	Global	10.63.136.26	10.63.136.26	🔘 Syslog
	設備種類	C 🖬	Global	10.63.136.26	10.63.136.26	🔘 Syslog
	Syslog Flow SNMP	C 🖬	Global	10.64.103.245	10.64.103.245	🔘 Syslog
		a	Global	10.64.103.44	10.64.103.44	🔘 Syslog
	Syslog 相關設定	2 🖬	Global	172.16.1.235	172.16.1.235	🗑 Syslog
		e	Global	191.168.2.252	191.168.2.252	Flow
	資料格式	2 🛍	Global	192.168.0.253	192.168.0.253	Flow
	Windows AD 🗸	37 🛍	Global	192.168.1.43	192.168.1.43	🔘 Syslog
		2	Global	192.168.1.90	192.168.1.90	🖲 Syslog
	Facility	e	Global	192.168.10.14	192.168.10.14	🔘 Syslog
	v	e	Global	192.168.10.15	192.168.10.15	🔘 Syslog
		e	Global	192.168.2.86	192.168.2.86	🔘 Syslog
	編碼方式 UTF-8 *	25 🔻	Global	192.168.2.86 共1頁 ▶ ▶ ○	192.168.2.86	🎯 Syslog

1.3 For Windows Server 2012 AD

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. 安装 NXLOG:

請全程以具有 系統管理員(Administrator) 的帳號權限身分登入系統並操作相關步驟。(否則可能 會因權限不足的問題導致設定無作用)

滑鼠雙點 nxlog-ce-2.9.1716.msi,點選[Install],執行 NXLog 程式安裝步驟。

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

4. 下載設定 Windows 2012 的 NXLOG nxlog_win2012_all.conf (輸出全部 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 AD 所有 Eventlog。使用者若是需要 Windows AD 的法 規報表 · 請將 nxlog_win2012_all.conf 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 AD 的 Eventlog。 請注意!! 此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。

若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重,請使用上述章節 nxlog_win2012.conf 的配置檔 for Windows 2012.

NREPorter Æ٧

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> \

Quei	′y Id="0"> \
	<select path="Security">*[System[(EventID=1100)]]</select> \
	<select path="Security">*[System[(EventID=4769)]]</select> \
	<select path="Security">*[System[(EventID=4768)]]</select> \
	<select path="Security">*[System[(EventID=4771)]]</select> \
	<select path="Security">*[System[(EventID=4616)]]</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>
	<pre><select path="Security">*[System[(EventID=4727)]]</select></pre> ///////////////////////////////////
	<pre><select path="Security">*[System[(EventID=4728)]]</select></pre> //// <pre></pre>
	<pre><select path="Security">*[System[(EventID=4729)]]</select> \</pre>
	<pre><select path="Security">*[System[(EventID=4730)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4731)]]</select> \</pre>
	<pre><select path="Security">*[System[(EventID=4732)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4733)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4734)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4735)]]</select> \</pre>
	<pre><select path="Security">*[System[(EventID=4737)]]</select> \</pre>
	<pre><select path="Security">*[System[(EventID=4738)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4739)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4740)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4741)]]</select> \</pre>
	<pre><select path="Security">*[System[(EventID=4742)]]</select> \</pre>
	<pre><select path="Security">*[System[(EventID=4743)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4744)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4745)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4748)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4749)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4750)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4753)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4754)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4755)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4756)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4758)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4759)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4760)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4763)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4764)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4767)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4778)]]</select></pre>
	<pre><select path="Security">*[System[(EventID=4783)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4800)]]</select></pre> /Select> \
	<pre><select path="Security">*[System[(EventID=4801)]]</select></pre>
	<pre><select path="System">*[System[(EventID=7036)]]</select></pre>
	<pre><select path="Application">*[System[(EventID=18454)]]</select></pre> /CEUTICATION // CEUTICATION // C
	<pre><select path="Application">*[System[(EventiD=10404)]]<select path="Application">*[System[(EventiD=18456)]]</select></select></pre>

	\
	ntion>
Module	om_uap
Host 1	92.168.2.64
Port 5	14
Exec \$Messag	ie = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message;
Exec if (\$Even	tID == 18454 or \$EventID == 18456) { \$SyslogFacilityValue = 18; } \
else { \$S	vslogFacilitvValue = 13: }
Exec if (\$Even	Tupe == 'FRROR' or \$EventType == 'AUDIT_FAULURE') { \$SyslogSeverity/alue = 3: } \
	Event in a second in the second in the second in the second se
else it	r (\$Event1ype == 'INFO' or \$Event1ype == 'AUDI1_SUCCESS') { \$SyslogSeventyvalue = 5; }
Exec to_syslog	g_bsd();
<route eventlog<="" th=""><th>></th></route>	>
Path ir	n eventlog => out eventlog

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 " 。

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

設定範例如下圖:

📄 nxlo	g.conf 🔀 🧮 nxlog.log 🗵	
25	白 < Query Id="0"> \	
26	<pre><select path="Security">*[System[(EventID=4768)]]</select> \</pre>	
27	<select path="Security">*[System[[EventID=4769)]]</select> \	
28	<pre>Select Path="Security">*[System[[EventID=4771]]]</pre>	
29	Collect Path= Security > [System[[EventID=4524]]](Select >)	
- 50 - 21	(Select Path="Security") System[[EventID=4525]]](Select) (
32	<pre>cselect rath= security / [system[[teentD=+6347]]](select) (</pre>	
33	<pre><select rath="security">[system[(ventD=648)]]</select> \</pre>	
34	<pre><select path="security">[system[(tent10=4656)]]</select> \</pre>	
35	<pre><select path="Security">*[System[[EventID=4719)]]</select> \</pre>	
36	<select path="Security">*[System](EventID=4720)]]</select> \	
37	<pre><select path="Security">*[System[(EventID=4722)]]</select></pre>	
38	<pre><select path="Security">*[System[(EventID=4723)]]</select> \</pre>	
39	<pre><select path="Security">*[System[(EventID=4724)]]</select> \</pre>	
40	<pre><select path="Security">*[System[(EventID=4725)]]</select> \</pre>	
41	<pre><select path="Security">*[System[(EventID=4726)]]</select> \</pre>	
42	<pre><select path="Security">*[System[[EventID=4727)]]</select> \ </pre>	
43	<pre>Select Path="Security">*[System[[EventID=4/28]]]{/Select> \</pre>	
44	<pre>Cselect Path= SecUrity >*[System[[EventID=4729]]]{/Select> \</pre>	
45	<pre>cselect rath="security"; System[[tventID=4750]]](select) {</pre>	
40	<pre><select rath="security">[system[[tventD=737]]];select > </select></pre>	
48	<pre><select path="security">fystem((tent10=4733))]</select> \</pre>	
49	<pre><select path="Security">*[System[[EventID=4734)]]</select> \</pre>	
50	<select path="Security">*[System[(EventID=4735)]]</select> \	
51	<select path="Security">*[System[(EventID=4737)]]</select> \	
52	<pre><select path="Security">*[System[(EventID=4738)]]</select> \</pre>	
53	<pre><select path="Security">*[System[(EventID=4739)]]</select> \</pre>	
54	<pre><select path="Security">*[System[(EventID=4741)]]</select> \</pre>	
55	<pre><select path="Security">*[System[(EventID=4742)]]</select> \</pre>	
56	<select path="Security">*[System[(EventID=4743)]]</select> \	
57	<pre><select path="System">[System](Event10=7036)]]</select> \ </pre>	
58	<pre>Select Path= Application >*[System[(EventD=18454)]]</pre>	
60	Courses - Course	
61		≡
62		
63		
64	<pre><output out_eventlog=""></output></pre>	
65	Module om_udp	
66	Host 192.168.2.64	
67	Port 514	
68	Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message;	
69 70	Exec if (Seventib == 18454 or Seventib == 18456) { \$SystogFacilityValue = 18; } \	
70	Erse (psystopratificyvalue = 15,) Erse (f (Styentione == 'FBOR' or (Eventione == 'AUDIT FATURE') ((SyelogSevenituValue = 3,).)	
72	else if (%EventType == 'MARNING') { %SysJogSeverTyValue = 4: }	
73	else if (\$EventType == 'INFO' or \$EventType == 'AUDIT SUCCESS') { \$SyslogSeverityValue = 5: }	
74	Exec to syslog bsd();	
75		
76		
77	Image: A state of the state	
78	Path in_eventlog => out_eventlog	
79	L	
80		×
	III 5	

5. 啟動 NXLOG 程式:

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]·點選[以系統管理員身分執行]。

[Windows PowerShell]輸入:

net stop nxlog			
net start nxlog			
#會看到以下訊息			
nxlog 服務正在啟動.			
nxlog 服務已經啟動成功.			
	r 미고성 1	ᅶᅎᆘᇊᅭᆔᆂᆁ	ΜH

b. [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 " 若沒有顯示 Error 的訊息,表示正常啟動。

C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++		x						
檔案(F) 編輯(E) 尋找(S) 檢視(V) 編碼(N) 程式語言(L) 自訂(T) 巨集 執行 外掛模組(P) 視窗(W) ? X ※<								
<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\Windows ANSI	IN	IS 🔡						

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

Npartner (Global) ~	↔ Home / 設備管理 / 設備樹狀團					
≣事件 €	▲ 設備樹狀園					
<u>山</u> 報表 🚺 🛛 🖽	援尋 Q 2 🗄 U 📢					
副 設備管理 🛛 🖽		操作	所屬領域 ≎	IP 🛋	設備名稱 🗢	設備種類 令
	2 元 未知設備 (20)	e	Global	1.1.1.8	1.1.1.8	Syslog
	由 設備資訊紙鋼 4	< C 🛍	Global	10.0.0.235	10.0.0.235	😌 Flow
G	設備基本設定	C Ó	Global	10.1.34.220	10.1.34.220	🍯 Syslog
	名稱	C 🛍	Global	10.10.10.101	10.10.101	Syslog
	Win2012AD 192.168.1.90	CÓ	Global	10.10.10.2	10.10.10.2	🌘 Syslog
		2 🖬	Global	10.10.10.3	10.10.10.3	Syslog
	IP	2 🖬	Global	10.143.238.95	10.143.238.95	Syslog
	192.168.1.90	2 🖬	Global	10.143.238.96	10.143.238.96	Syslog
		2 🖬	Global	10.63.136.26	10.63.136.26	Syslog
	設備種類	2 🖬	Global	10.63.136.26	10.63.136.26	Syslog
	Syslog Flow SNMP	C 🛍	Global	10.64.103.245	10.64.103.245	Syslog
		a	Global	10.64.103.44	10.64.103.44	Syslog
	Syslog 相關設定	2 🖬	Global	172.16.1.235	172.16.1.235	Syslog
		C 🛍	Global	191.168.2.252	191.168.2.252	Flow
	資料格式	C 🛍	Global	192.168.0.253	192.168.0.253	Flow
	Windows AD 🗸	32 🛍	Global	192.168.1.43	192.168.1.43	Syslog
		a	Global	192.168.1.90	192.168.1.90	Syslog
	Facility	C 🛍	Global	192.168.10.14	192.168.10.14	Syslog
	т	C 🛍	Global	192.168.10.15	192.168.10.15	Syslog
		C 🛍	Global	192.168.2.86	192.168.2.86	Syslog
	推结方式 UTF-8 ▼	25 -	▲ 第1	共1頁 ▶) 0		
	確定 取消					

1.4 For Windows Server 2016 AD

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:

請全程以具有 系統管理員(Administrator) 的帳號權限身分登入系統並操作相關步驟。(否則可能 會因權限不足的問題導致設定無作用)

滑鼠雙點 nxlog-ce-2.9.1716.msi,點選[Install],執行 NXLog 程式安裝步驟。

3. 下載設定 Windows 2016 NXLOG 配置檔 nxlog_win2016.conf:

前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2016.conf 開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 NXLOG 配置 檔, 將上面的 URL 上的 nxlog_win2016.conf 裡的設定內容複製, 然後貼上並覆蓋 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 NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf " 64 位元 OSNXLOG 安裝路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "。

4. 下載設定 Windows 2016 的 NXLOG 配置檔 nxlog_win2016_all.conf (輸出全部 Eventlog) 前往 URL: http://www.npartnertech.com/download/tech/nxlog_win2016_all.conf N-Reporter 提供法規報表統計 Windows AD 所有 Eventlog。使用者若是需要 Windows AD 的法 規報表 · 請將 nxlog_win2016_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 AD 的 Eventlog。
請注意!!_此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。
若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重 · 請使用上述章節 nxlog win2016.conf 的配置檔 for Windows 2016. ## 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

<QueryList> \

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

Query

<Extension syslog> Module xm_syslog </Extension> <Input in_eventlog> # For windows 2008/vista/7/8/2012/2012R2/2016 and latter use the following: Module im_msvistalog ReadFromLast TRUE SavePos TRUE

Que	ry Id="0"> \
	<select path="Security">*[System[(EventID=1100)]]</select> \
	<select path="Security">*[System[(EventID=4769)]]</select> \
	<select path="Security">*[System[(EventID=4768)]]</select> \
	<select path="Security">*[System[(EventID=4771)]]</select> \
	<select path="Security">*[System[(EventID=4616)]]</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=4740)]]</select> \
	<select path="Security">*[System[(EventID=4741)]]</select> \
	<select path="Security">*[System[(EventID=4742)]]</select> \
	<select path="Security">*[System[(EventID=4743)]]</select>
	<select path="Security">*[System[(EventID=4744)]]</select> \
	<select path="Security">*[System[(EventID=4745)]]</select> \
	<select path="Security">*[System[(EventID=4748)]]</select> \
	<select path="Security">*[System[(EventID=4749)]]</select> \
	<select path="Security">*[System[(EventID=4750)]]</select>
	<select path="Security">*[System[(EventID=4753)]]</select>
	<select path="Security">*[System[(EventID=4754)]]</select>
	<select path="Security">*[System[(EventID=4755)]]</select>
	<select path="Security">*[System[(EventID=4756)]]</select>
	<select path="Security">*[System[(EventID=4758)]]</select>
	<select path="Security">*[System[(EventID=4759)]]</select>
	<select path="Security">*[System[(EventID=4760)]]</select>
	<select path="Security">*[System[(EventID=4763)]]</select>
	<select path="Security">*[System[(EventID=4764)]]</select>
	<select path="Security">*[System[(EventID=4767)]]</select>
	<select path="Security">*[System[(EventID=4778)]]</select>
	<select path="Security">*[System[(EventID=4783)]]</select>
	<select path="Security">*[System[(EventID=4800)]]</select>
	<select path="Security">*[System[(EventID=4801)]]</select>
	<select path="System">*[System[(EventID=7036)]]</select> \
	<select path="Application">*[System[(EventID=18454)]]</select>
	<select path="Application">*[System[(EventID=18456)]]</select>

🐼 NHReporter

\
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') { \$\$vslogSeverityValue = 4 } \
else if (\$EventType == 'INEO' or \$EventType == 'AIIDIT_SILCESS') { \$SvslogSeverity/alue = 5: }
Soupur
<route eventlog=""></route>
Path in eventlog => out eventlog

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 " 。 紅色文字部位請輸入 N-Reporter 機器 IP · 本文件範例為輸入 " 192.168.2.64 " 。 設定範例如下圖:

🔚 nxlog.	conf 🔀 🔚 mxlog.log 🔀
65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81	<pre>cont2 endodod13 (Select Path="Security">*[System[(EventID=4753)]] \</pre>
81 82 83	<pre>-</pre>
84 85 86 87 88	Coutput out_eventlog> Nodule om_udp Host 192.168.2.64
89 90 91 92 93 94 95 96	<pre>Port 514 Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message; Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message; Exec \$\frac{1}{5}\$ Exec \$\f</pre>
97 98 99 100 101	<pre> //Output> E<route eventlog=""> E vath in_eventlog => out_eventlog </route></pre>

5. 啟動 NXLOG 程式:

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]。 命令提示字示論入:

印マ淀小子儿辋八.
net stop nxlog
net start nxlog
#會看到以下訊息
The nxlog service is starting.
The nxlog service was started successfully.

b. [開始]→[所有程式]→[系統管理工具]→[服務]→找到[nxlog]·右鍵點服務[nxlog]·點
 [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
🔓 🖻 🗎 🛍 🚡 🐚 🚖 🚜 🗅 🛍 🤉 ピ 🏙 🛬 🤏 👒 🖫 🖓 🎫 1 🎼 🐷 🗉 🗵	»>
🔚 nxlog.conf 🔚 nxlog.log	
1 2014-07-03 17:57:22 WARNING stopping nxlog service	
2 2014-07-03 17:57:22 WARNING nxlog-ce received a termination request signal, exiting	
3 2014-07-03 17:57:23 INFO nxlog-ce-2.7.1191 started	
4	
length : 192 lines : 4	INS //

7. 新增 Windows Server 2016 AD Syslog 設備時, 資料格式請選擇 [Windows AD]。

N-CLOUD						
Npartner (Global) ~	❸ Home / 設備管理 / 設備樹狀圖					
≣ 事件	▲ 設備樹狀園					
山報表 1 田	援导 Q C U 4)					
📑 設備管理 🛛 🖽		操作	所屬領域 ≎	IP 🛋	設備名稱 ≑	設備種類 🗢
✿ 糸統管理 田	2 未知設備 (20)	e	Global	1.1.1.8	1.1.1.8	🔘 Syslog
6	山 設備資訊編輯	< C 🖻	Global	10.0.0.235	10.0.0.235	Flow
	設備基本設定	6	Global	10.1.34.220	10.1.34.220	Syslog
	名稱	C 🗎	Global	10.10.10.101	10.10.101	Syslog
	Win2016AD_192.168.1.90	2 🕯	Global	10.10.10.2	10.10.10.2	Syslog
		C 🛍	Global	10.10.10.3	10.10.10.3	Syslog
	IP	C 🗊	Global	10.143.238.95	10.143.238.95	Syslog
	192.168.1.90	2 🖬	Global	10.143.238.96	10.143.238.96	Syslog
		C 🖬	Global	10.63.136.26	10.63.136.26	Syslog
	設備種類	đ	Global	10.63.136.26	10.63.136.26	Syslog
	Syslog Flow SNMP	2 🖬	Global	10.64.103.245	10.64.103.245	Syslog
		C 🛍	Global	10.64.103.44	10.64.103.44	Syslog
	Syslog 相關設定	2 🕯	Global	172.16.1.235	172.16.1.235	Syslog
		2 🖬	Global	191.168.2.252	191.168.2.252	Flow
	資料格式	e	Global	192.168.0.253	192.168.0.253	Flow
	Windows AD	37 🛍	Global	192.168.1.43	192.168.1.43	Syslog
		7	Global	192.168.1.90	192.168.1.90	Syslog
	Facility	e	Global	192.168.10.14	192.168.10.14	Syslog
	·	2 🖬	Global	192.168.10.15	192.168.10.15	Syslog
		C 🛍	Global	192.168.2.86	192.168.2.86	Syslog
	推碼方式 UTF-8 ▼ 確定 取消	25 🔻	i 4 第1	共1頁 ▶ 위 0		

2 Windows 2003 Active Directory Server 稽核設定

本章節主要說明以下操作設定:

1. 設定網域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 2003 AD 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。

2.1 設定 Windows 2003 AD Server 網域使用者登入登出的稽核原則

設定步驟如下:

 以全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分登入 Windows 2003 AD Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用)



點選 [開始 / 所有程式 / 系統管理工具 / 網域控制站安全性原則]。

註:[系統管理工具]裡的[網域安全性原則]為設定整個網域裡的所有物件(所有使用者與電腦) · 而網域控制站安

全性原則為設定所有網域控制站(Domain Controllers)。建議將此兩種安全性稽核原則設定為一致。

2. 前往 [Windows 設定 / 安全性設定 / 本機原則 / 稽核原則]。

🚡 預設網域控制站安全性設定			
檔案(E) 執行(A) 檢視(V) 說明(A	Ð		
📄 Windows 設定	原則 🛆	原則設定	
	100 稽核目錄服務存取	沒有稽核	
□ □ 安全性設定	100 稽核系統事件	沒有稽核	
□ ᡂ 帳戶原則	1 2 2 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	沒有稽核	
白…」「一」本機原則	100 稽核原則變更	沒有稽核	
· · · · · · · · · · · · · · · · · · ·	100 稽核特殊權限使用	沒有稽核	
□ 劒 使用者權利指派	100 稽核帳戶登入事件	沒有稽核	
	100 稽核帳戶管理	沒有稽核	
	100 稽核登入事件	沒有稽核	
	副藉核程序追蹤	沒有稽核	

- 3. 定義下列的原則設定值:
 - (1) 稽核登入事件:

涡鼠雙擊 [稽核登入事件],勾選 [定義這些原則設定值],再勾選 [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 [定義這些原則設定值]·再勾選 [成功]及[失
 敗]·設定完成後按 [確定]。



(3) 稽核物件存取:

湯鼠雙擊 [稽核物件存取]·勾選 [定義這些原則設定值] 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 Active Directory 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, 僅需勾[定義這些原則設定值] 即可. 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:

(5) 稽核帳戶管理:

滑鼠雙擊 [稽核原則變更]·勾選 [定義這些原則設定值]·再勾選 [成功] 及 [失敗]· 設定完成後按 [確定]。

滑鼠雙擊 [稽核帳戶管理]·勾選 [定義這些原則設定值]·再勾選 [成功]及[失敗]· 設定完成後按 [確定]。

2.2設定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 [共用此資料夾]。點選 [使用權限]。

share_	_folder	「内容 ?)	×
一般	共用	安全性 自訂	
	您可以编 啓用這(與網路上的其他使用者共用此資料夾。若要 個資料夾的共用,請按一下 [共用此資料夾]。	
	不共用此資 共用此資料	料夾(N) 	
共用	名稱(H):	share_folder	
註解	2C):		
使用	者限制:	● 允許最大數(M)	
		○ 允許這個數目的使用者(例):	
若要的權	設定使用 [#] 驟,諸按	者透過網路存取此資料來(使用權限 (P) [權限]。	
若要取處	[設定離線] [理]。	存取設定值,請按一下[快 快取處理(近)	
		確定 取消 套用(A)	

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

	st	nare_folder 的權限		? ×
		共用權限		
		群組或使用者名稱(G):		
		Everyone		
選擇 使用者、電腦 或 群組	? ×			
選擇這個物件類型(2):				
使用者、群組 或 內建安全性原則	物件類型(0).			
從這個位置(P):			新增(D)	移除(R)
herb.org	位置(1)	Everyone 的權限(P)	九許	拒絕
輸入物件名稱來選取 3 (E):		完全控制		
max	檢查名稱(C)	變更 請取		
	4	1 544X		
進階(A). 確定	取消			
]/		
		確定		套用(A)

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

share_folder 的權限		? ×
共用權限		
。 【1】 【使用者名稱(①):		
Everyone		
🙍 maxmax (max@herb.org)		
6		
	新增(D)	移除(R)
maxmax的權限(P)	允許	拒絕
完全控制		
變更		
讀取		
	取 消	

- 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) 若要選擇其他網域,可點選 [位置]。
 - (4) 可於此空白處直接輸入已知的網域使用者帳號後,按[檢查名稱]檢查存不存在。

(5) 若網域使用者帳號存在的話,按 [確定]完成設定。

share_folder 內容 一般 共用 安全性 自訂 群組或使用者名稱(近):	strator)	? :	×	
🕵 Administrators (HERB\Admi	nistrators) 新婚(D)	2 移除(R)	選擇使用者、電腦或群組 選擇這個物件類型(2): 使用者、群組或內建安全性原則 從這個位置(2): beth org	? × 物件類型(2) (注異(1)
administrator 的權限(P) 完全控制 修改 讀取及執行 清單資料夾內容 讀取			輸入物件名稱來選取 (<u>節例</u>)(E): max 進階(<u>A</u>)	<u>岐</u> 直也通()… 検査名稱(C) 5 確定 取消
<u>第入</u> <u>特殊種限或進階設定</u> 諸按 [進階 <u>確定</u>]。 取消	▲ 進階(Y)		

- 6. 設定使用者權限:
 - (1) 點選要設定的使用者帳號。
 - (2) 勾選允許 [完全控制] 權限,以取得所有權限。
 - (3) 按 [套用]及[確定], 完成設定。

share_folder 丙容		? ×
一般 共用 安全性 自訂		
群組或使用者名稱(①):		
administrator (HERB'admini	strator)	
Administrators (HERB\Admi	nistrators)	
🕵 maxmax (max@herb.org)		
SYSTEM		
	新增(D)	移除(R)
naxmax的權限(P)	允許	拒絕
完全控制		
	•	
修改		
修改 讀取及執行	N N N	
修改 讀取及執行 諸單資料夾內容	<u>ত</u> য	
修改 讀取及執行 清單資料夾內容 讀取	বিবের	
修改 請取及執行 清單資料夾內容 請取 寫入		
修改 請取及執行 清單資料夾內容 請取 寫入 特殊研究		
修改 讀取及執行 清單資料夾內容 讀取 寫入 <u> 味起都呢</u> 特殊權限或進階設定諸接 [進階		□ □ □ □ ⊥ 進階(V)
修改 讀取及執行 清單資料夾內容 讀取 寫入 點社都限 特殊權限或進階設定請按 [進階		□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

- 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],來新增一使用者。
 - (4) 若要選擇其他網域,可點選 [位置]。
 - (5) 可於此空白處直接輸入已知的網域使用者帳號後,按[檢查名稱]檢查存不存在。

(6) 若網域使用者帳號存在的話,按[確定]完成設定。

share_folder 內容 ?×	share_folder的進階安全性設定
一般 共用 安全性 自訂 群組或使用者名稱(①): ① administrator (HERE Vadministrator) ② administrators (HERE Vadministrators)	權限 稽核 报2 有效權限 若要檢視其他有關特殊稽核項目的資訊,選擇一個稽核項目,然後按 [編輯]。 稽核項目(<u>]</u>):
⑦ maxmax (max@herb.org) ⑦ SYSTEM 新增① 移除①	<u>類型</u> 名稱 存取 繼承自 套用到
maxmax 的種限(P) 九許 拒絕 完全控制 ///>// /// 修改 //>/ /// 資取及執行 // /// 這酸及執行 // /// 這酸及執行 /// /// 這酸資料及內容 /// /// 資取 /// /// 第入 /// /// 特殊權限或進階設定請按 [進階]。 進階(Y)	 ● 新增①
	選擇使用者、電腦或群組 ?▼ 選擇這個物件類型②: 使用者、群組或內建安全性原則 使用者、群組或內建安全性原則 物件類型②… 從這個位置①: 位置①… herb.org 位置①… 諸輸入物件名稱來選 1000 €): max 校查名稱 €) 進階(△)… 確定<取消

8. 稽核項目設定:

點選並編輯稽核項目清單內所要的稽核項目

勾選該稽核項目的 [成功] 及 [失敗]的項目, 設定完成後按 [確定]。

share_folder 的稽核項目			? ×
物件			
名稱(11): maxmax (max@herb.org)		變更(<u>C</u>)	
套用在(Q): 這個資料夾,子資料夾及	を檔案	-	-
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/積取資料 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	<u> </u>		
□ 這些稽核項目只套用到這個容器。 □ 物件及(或)容器(I)	的	全部清除([2
	確定	取消	1

9. 在進階安全性設定完成後·點選 [確定]。

share_folder 的進階安全性設定	? ×
權限 【楷核 擁有者 有效權限	
若要檢視其他有關特殊稽核項目的資訊,選擇一個稽核項目,然後按 [編輯]。	
捲核項日(T)-	
全部 maxmax (max@herb.org) 完全控制 <非繼承的> 這個資料	挾,子…
新增D 編輯(E) 移除(B)	
▼ 允許從父項繼承藉核項目套用到清個物件和所有的子物件,包括明確定義於此的項	ie (A)
□ 以顯示於此套用到子物件的項目,替代所有子項物件上的稽核項目(P)	
了解其他有關 <u>稽核</u> 。	
確定 取消	套用(<u>A</u>)

在分享資料夾設定完成後,點選 [確定]。

share_folder 丙容		? ×
一般 共用 安全性 自訂		
群組或使用者名稱(G):		
🕵 administrator (HERB\admini	strator)	
🚮 Administrators (HERB\Admi	nistrators)	
👿 maxmax (max@herb.org)		
SYSTEM		
	新增(D)	移除(R)
maxmax的權限(P)	允許	拒絕
完全控制		
修改		
讀取及執行		
清單資料夾內容		
讀取		
寫入	\checkmark	
特殊罹限或進階設定請按し進階	'] ° _	進階(♡)
	-	
確定	取消	套用(A)

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

7.3		-	[設定您的伺服器] 精靈
TX 12		Z	Active Directory 使用者及電腦
2		53	Active Directory 站台及服務
Windows 檔 gVim Read		Se	Active Directory 網域及信任
administrator		9	DHCP
aunonostrator		2	DNS
管理您的伺服器	1 我的電腦	壶	Microsoft .NET Framework 2.0 組態
A H-T-CHH J LANK IN		۹	元件服務
6、 命令提示字元	□ 控制台(C) ・	Ŀ	分散式檔案系統
		1	伺服器管理
💢 Windows 檔案總管	🧌 系統管理工具	3	事件檢視器
		8 C 22	服務
🚺 記事本	SHIT WALLER	1	效能
	● ####################################	٩	授權
	TERTHAXIE(D)	P	終端機伺服器授權
	↓ 搜尋(5)		終端機服務設定
CA- Command Shell		皆	終端機服務管理員
2. 網域控制站安全性点	[2] 執行(B)	9	資料來源 (ODBC)
.µ□ jj ······		9	路由及遠端存取
MySQL 5.5 Command			電腦管理
Line Client		-	管理您的伺服器
SQL Server		B	網域安全性原則
·····X* Management Studio		6	網域控制站安全性原則
所有程式(E) ,		۲	網路負載平衡管理員
	アン ア ア ア ア ア ア ア ア ア ア ア ア ア ア	63	遠端桌面
	図 豆山(1) 🔽 開後(1)		憑證授權單位
🥙 開始 🥭 🚱 📶 👋		-	義集系統管理員

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

11. 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)			_8×
	1 💭			,
	共用名稱 △	資料夾路徑	類型	# 用戶端連
🔁 🌇 系統工具	Regional Admins	C:\WINDOWS	Windows	0
🔪 🖻 💼 事件檢視器	l ₽C\$	C:\	Windows	0
🔁 📄 共用資料夾	Regipc\$		Windows	0
	RETLOGON	C:\WINDOWS\S	Windows	0
1 工作階段	良 share_folder	C:\Documents a	Windows	0
┃	I SYSVOL	C:\WINDOWS\S	Windows	0
□ 劉 效能記錄及警示				

12. 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 Active Directory Server 稽核設定

本章節主要說明以下操作設定:

1. 設定網域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 2008 AD 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。

3.1 設定網域使用者登入登出的稽核原則

設定步驟如下:

 以全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分登入 Windows 2008 AD Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用) 開啟群組原則管理。

點選[開始功能表/執行]。

輸入∶**gpmc.msc** ,完成後按 [確定]。

何服器管理員 命令提示字元	2	
Windows Update	administrator 文件	
2015年本		
C Internet Explorer	網路	
Windows 檔案總管	控制台	
😵 輕鬆存取中心	条統管理工具 ▶	国執行
-	說明及支援 執行…	 動入程式、資料夾、文件或網際網路資源的名稱,Windows
	Windows安全性	開設(O): gpmc.msc
 所有程式 開始搜尋 	0	確定 取湯 瀏覽(B)

註: 若出現"Windows 找不到'gpmc.msc' "的訊息, 請依下面步驟安裝 群組原則管理 (gpmc)

1. 以系統管理員身分開啟命令提示字元。

2. 在命令提示字元[,]輸入 ServerManagerCmd -install gpmc。

3. 安裝完成時請關閉命令提示字元。

2. 以本文件為例子(實際情況請依使用者的環境做調整), 點選 [樹系 / 網域 / win2k8cht.local /

Default Domain Policy] •



註:此步驟展開網域,會有 [Default Domain Policy](預設網域安全性原則);

另外展開 Domain Controllers(網域控制站)[,]會有 [Default Domain Controllers Policy] (預設網

域控制站安全性原則)。

建議將此兩種安全性稽核原則設定為一致

3. 在 Default Domain Policy 點擊滑鼠右鍵,點選 [編輯]。



4. 展開 [電腦設定 / 原則 / Windows 設定 / 安全性設定 / 本機原則 / 點選 稽核原則]。

」 群組原則管理編輯器	_ U ×
檔案(F) 執行(A) 檢視(V) 說明(H)	
💠 🔿 🞽 📷 💥 🛃 🔝 🖬	
□ Default Domain Policy [WIN2K8-AD.WIN □ ● 軟體設定 □ ● な全性設定 ● ● 東全性認項 ● ● ● 本機原則 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	原則設定 沒有稽核 沒有稽核 沒有稽核 沒有稽核 成功,失敗 沒有稽核 沒有稽核 沒有稽核 沒有稽核

- 5. 定義下列的原則設定值:
 - (1) 稽核登入事件:

🧾 群組原則管理編輯器 _ 🗆 🗙 檔案(F) 執行(A) 檢視(V) 說明(H) 🗢 🔿 🔰 📅 💥 🗒 😖 🚺 🎫 原則 ▲ 🛒 Default Domain Policy [WIN2K8.WIN2K8CHT.L🛌 原則設定 🔐 稽核原則變更 🗆 👰 電腦設定 尚未定義 🗆 📔 原則 🔐 稽核帳戶登入事件 尚未定義 🗉 📔 軟體設定 椿核帳戶管理 尚未定義 □ 🧮 Windows 設定 11 稽核物件存取 尚未定義 🔄 指令碼 - (啟動/關機) 🔛 稽核特殊權限使用 尚未定義 🖂 📑 安全性設定 🌇 稽核登入事件 尚未定義 ∃ 📑 帳戶原則 ⊡ 📑 本機原則 🚋 楷核目錄服務仔取 尚未正莪 33 稽核程序追踪 出生出 田 ● 椿核原則
 田 ● 使用者權利
 田 ● 安全性選項 ? × 使用者權利指派 安全性原則設 E 解説 稽 登入事件 ✓ 定義這些原則設定值(D) 稽核這些嘗試: 具有進階安全性的 Window + ☑ 成功(S) 網路清單管理員原則 표 🌆 無線網路 (IEEE 802.11) 原! ☑ 失敗(F) 🗉 🧰 公開金鑰原則 🗉 🚞 軟體限制原則 + 📋 Network Access Protectior 🖽 🛃 IP 安全性原則 (位置: Activ 🗉 🍌 以原則為依據的 QoS 🗉 🧰 系統管理範本: 已從本機電腦擷頭 🗉 🚞 喜好設定 /+ m = = n.e • 這個 GPO 已連結到下列 Wi (無) 確定 取消 套用(A)

(2) 稽核帳戶登入事件:

滑鼠雙擊 [稽核帳戶登入事件]·勾選 [定義這些原則設定值]·再勾選 [成功]及[失 敗]·設定完成後按 [確定]。



(3) 稽核物件存取:

湯鼠雙擊[稽核物件存取]·勾選[定義這些原則設定值] 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 2008 Active Directory 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, 僅需勾選[定義這些原則設定值] 即可. 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 [定義這些原則設定值]·再勾選 [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 [定義這些原則設定值]·再勾選 [成功]及[失敗]·設 定完成後按[確定]。

3.2設定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]。

📕 temp	内容		×
一般	共用	安全性 以前的版本 自訂	,
- 網路 ● ● ● 網路 不り ■ ● ■ ● ■ ●	:檔案 及資料 部型 不共月 3路行 (M): 共用(S) 共用(S)	科夾共用 月	
設定 項。	E自訂權限 使 進階共	、建立多個共用,及設定其他進階共 共用(A)	:用選
		關閉 取消	套用(A)

3. 在檔案分享權限設定中,點下拉選單至 [尋找]。

载挥網路上要共用的人員	
1入您要與之共用的人員名稱,然後按一下	[新增],或者按一下箭頭,尋找人員或與每一個人共用。
	▼ 新增(A)
ver, ane	
我… Administrator	
Administrator	輝行台 ▼
新我可在 Windows 中共田的各種方法:	

- 4. 使用者設定:
 - (1) 若要選擇其他網域,可點選 [位置]。
 - (2) 可於此空白處直接輸入已知的網域使用者帳號後,按[檢查名稱]檢查存不存在。
 - (3) 若網域使用者帳號存在的話,按[確定]完成設定。

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	物件類型(O)
從這個位置(F):	
2k8cht.local	位置(L)
酮人物件名稱來選取 (<u>範例</u>)(E):	
carlos	檢查名稱(C)
	The NK

5. 點選[共用]。

🛃 檔案分享種限設定	×
🕞 ᇗ 檔案分享種限設定	
選擇鋼路上要共用的人員	
輸入您要與之共用的入員名稱,然後按一下 [新增],或者按一下;	箭頭,尋找入員或與每一個入共用·
	▼ 新增(A)
名稱	權限層級
🛃 Administrator	
💰 carlos	讀取裝置 ▼
告訴我可在 Windows 中共用的各種方法 •	
	🕐 共用(H) 取消

6. 等待共用設定完成後,再按[完成]。



🐼 N-Reporter

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

	🔐 temp 的權限 🛛 🗙
	安全性
一般 スエロ 以前的版本 目記 物件名稱· C \Users\udministrator\Deskton\temp	物件名稱: C:\Users\Administrator\Desktop\temp
が日本語 - C. iooration Look of	群組或使用者名稱(G):
研想就使用·台省構(い):	SYSTEM
arlos (carlos@win2k8cht.local)	A daministrator
Administrator	Administrators (WIN2PPCHT\Administrators)
若要變更使用權限,請按一下[編輯]。 編輯(E)	
carlos的權限(P)	
完全控制	
修改	
	讃取和執行 □
如需将然權限認進階設定,說按一下以進進階(♥)	
深入瞭解存取控制及權限	確定
	選擇使用者、電腦或群組 ?▼▼
	選擇這個物件類型(S):
	使用者、群組或內建安全性原則 (四)
	従這個位置(F):
	Ctrack (位置(L)
	calos 檢查名稱(C)
	進階(A) 確定 取消

- 8. 設定使用者權限:
 - (1) 點選新增的使用者帳號。
 - (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 [確定]。

📙 temp 的權限		×			
安全性					
物件名稱: C:\Users\Adminis	trator\Desktop\ten	лр			
群組或使用者名稱(G):					
SYSTEM administrator (WIN2K8CHT)	administrator) [\dministrators)				
arlos (carlos@win2k8cht.loc	al)				
	(
6	新增(D)				
carlos的權限(P)	允許	拒絕			
完全控制					
修改	修改 🔽 🗖				
<u>涂入瞭解仔取控制及催慨</u>					
一般に	1 取消	▲ 査田(A)			

🐼 NHReporter

- 9. 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],來新增一使用者。
 - (5) 若要選擇其他網域,可點選 [位置]。
 - (6) 可於此空白處直接輸入已知的網域使用者帳號後,按[檢查名稱]檢查存不存在。
 - (7) 設定完成後按 [確定]。

🕌 temp 內容 🛛 🗙	🛛 🕌 temp 的進階安全性設定	Ē		×
一般 共用 安全性 以前的版本 自訂	使用櫂。稽核指列	2月效權限		
物件名稱: C:\Users\Administrator\Desktop\temp	若要檢視或編輯稽核項目	一 目的詳細資料,諸選取該項目,再	ⅰ 按一下[編輯]。	
群組或使用者名稱(G):	物件名稱: C:\Users\Administrator\Desktop\temp			
Markey (under Quair 210 - 14 Jaco II)	総核項目(T)·			
administrator (WIN2K8CHT)administrator)	精明した報	方取	一	
& Administrators (WIN2K8CHT\administrators)	规空 有悔	1±4X		
, 若要變更使用權限,該按一下[編輯]。				
SYSTEM 的權限(P) 允許 拒絕				
	l (3			
到山谷料本内容				
	編輯(E)			
		婚圣楚转宿日心		
	■ 0.040101111004038 E0011	CENTRAL CONTRACTOR (C)		
深入瞭解存取控制及權限	藉核物件存取的需求為何	1?		
			確定	取消 套用(A)
		- IVI		
₩ temp 的進階安全性設定		×		
<mark>⊯</mark> temp的進階安全性設定 		×		
▲ temp 的進階安全性設定 稽核 若要檢視或編輯稽核項目的詳細資料,諸選取該項目,再按一下	[編輯]。	✓ 選擇 使用者、電腦 或 群組	Ħ	? ×
■ temp 的進階安全性設定 帮核 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 物件名稱: C:\Users\AdministratorDesktop\temp	[編輯]。	× 選擇 使用者、電腦 或 群編 選擇這個物件類型(3):	Ħ	? x
▲ temp 的進階安全性設定 稽核 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 物件名稱: C:\Users\Administrator\Desktop\temp 稽核項目(T):	[编輯]。	× 選擇 使用者、電腦 或 群経 選擇這個物件類型(3): 使用者、群組 或 內建安全	II *性原則	?× 5 物件類型(0)…
 ▶ temp 的進階安全性設定 稽核 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 物件名稱: C:\Users\AdministratorDesktop\temp 稽核項目(T): 類型 名稱 存取 	[編輯]。 繼承自 [麥用到	 ズ 選擇 使用者、電話 或 群組 選擇這個物件類型(3): (使用者、群組 或 內建安全 従這個位置(乎): 	₫ ≝性原則	?× 5 物件類型(0)
 ▶ temp 的進階安全性設定 稽核 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 物件名稱: C:\Users\Administrator\Desktop\temp 稽核項目(T): 換型 名稱 存取 	[編輯]。 繼承自	 ズ 選擇 使用者、電話 或 群組 選擇這個物件類型(\$): [使用者、群組 或 内建安全 従這個位置(P): win2k8ch1ocal 	Ħ ≥性原則	? × 5 物件類型(0) 位置(L)
▲ temp 的進階安全性設定 稽核 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 物件名稱: C:\Users\Administrator\Desktop\temp 稽核項目(T): 類型 名稱 存取 ;	鴻輯]。 檻承自 「	★ 2015 選擇 使用者、電腦 或 群組 選擇這個物件類型(S): [使用者、群組 或 內建安全 従這個位置(P): 1000000000000000000000000000000000000	Ħ ≌性原則 i例)Œ):	? × 5 物件類型(0) 位置(L)
▲ temp 的進階安全性設定 裙核 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 物件名稱: C:\Users\Administrator\Desktop\temp 稽核項目(T): 類型 名稱 存取	[編輯]。 繼承自	選擇這個物件類型(S): 健用者、群組或內建安全 從這個位置(P): win2k8ch1ocal 会議入物件名稱來選取(的) (carlos	拍 < <性原則	? × ★
▲ temp 的進階安全性設定 稽核 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 物件名稱: C:Wsers\AdministratorDesktop\temp 稽核項目(T): 項型 名稱 存取 []	[編輯]。 繼承自	文書 文書 文書 文書 本書 文書 本書 本書 本書 本書 法 <	扭 ☆性原則 例)Œ):	? × ち 物件類型(0) 位置(L) 検査名額(C)
★ temp 的進階安全性設定 稽核 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 物件名稱: C:\Users\AdministratorDesktop\temp 稽核項目(T): 類型 名稱 存取 ;	[編輯]。 繼承自 [套用到]	文書 文書 文書 文書 文書 文書 第 #	Ħ ≥性原則 例)Œ): 7	? × ★ 5 物件類型(0) 位置(L) 検査名稱(C)
№ temp 的進階安全性設定 稽核 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 物件名稱: C:\Users\Administrator\Desktop\temp 稽核項目(T): 類型 名稱 有取 新增(D) 編輯(E)	[編輯]。 繼承自 │ 套用到	ズ 選擇 使用者、電話 或 群組 選擇這個物件類型(S): (使用者、群組 或 內建安全 從這個位置(P): (min2k8chtlocal) 「「「」」」、「」」、「」」、「」」、「」」、「」」、「」」、「」」、「」」、	Ħ ≌性原則 例(E): 7	? × 5 物件類型(0) 位置(L) 検査名額(C) 確定 取消
 ▲ temp 的進階安全性設定 椿核 若要檢視或編輯楷核項目的詳細資料,請選取該項目,再按一下 物件名稱: C:\Users\Administrator\Desktop\temp 稽核項目(T): 類型 名稱 存取 : 新增(D) 編輯(E) 刪除(R) 又 從此物件的父項包括搬承獲枝項目(D) 	鴻輯]。 繼承自 [套用到]	ズ 選擇 使用者、電話 或 群組 選擇這個物件類型(S): (使用者、群組 或 內建安全 從這個位置(P): (min2k8chtlocal) 「「「」」」、「」」、「」」、「」」、「」」、「」」、「」」、「」」、「」」、	H 2性原則 (例)(E): 7	? × 5 物件類型(0) 位置(L) 検査名稱(C) 確定 取消
 ▲ temp 的進階安全性設定 榕核 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 物件名稱: C:Wsers\AdministratorDesktop\temp 稽核項目(T): 類型 名稱 存取 (請輯(E) ml除(E) 新增(D) // // // // // // // // // // // //	[編輯]。 繼承自 (<u></u> (<u></u> (()	文書 文書 文書 文書 文書 文書 (1) (2)	Ħ ≝性原則 例)Œ): 7	? × 5 物件類型(0) 位置(L) 檢查名稱(C) 確定 取消
 ▲ temp 的進階安全性設定 榕核 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 物件名稱: C:\Users\&dministratorDesktop\temp 稽核項目(T): 類型 名稱 存取 : 新增(D) 編輯(D) m\\\(\mathbf{P}\mathbf{R}\)) 「從此物件的父項包括繼承稽核項目取代所有子条現有的繼承稽核項目(C) 	[編輯]。 <u>繼承自 [套用到</u>]	文書 文書 文書 文書 文書 文書 文書 第 1	Ħ ≝性原則 例)Œ): 7	? × 5 物件類型(0) 位置(L) 檢查名稱(C) 確定 取消
 ▲ temp 的進階安全性設定 椿核 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 物件名稱: C:\Users\AdministratorDesktop\temp 稽核項目(T): 類型 名稱 存取 ; 新增(D) // 經輯(C) 刪除(R) 	[編輯] ∘ 繼承自	文書 文書 選擇這個物件類型(%): (使用者、群組或內建安全 (従這個位置(F): (前): (城前2k8chtlocal) (前): (城前2k8chtlocal) (前): (本間の本) (前): (本間) (前): (本間) (本間) (本間) (本間)	Ħ ≥性原則 (例)(Œ): 7	? × 5 物件類型(0) 位置(L) 檢查名額(C) 確定 取消
 ▶ temp 的進階安全性設定 帮核 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 物件名稱: C:\Users\Administrator\Desktop\temp 稽核項目(T): 類型 名稱 存取 : 「有取 : 「 新增(D) 編輯(E) 删除(R) 「 從此物件的父項包括繼承稽核項目(D) 」以此物件的総承稽核項目取代所有子条現有的繼承稽核項目(P)	[編輯]。 繼承自 [套用到]	ズ 選擇 使用者、電話 或 群組 選擇這個物件類型(S): (使用者、群組 或 內建安全 從這個位置(P): (min2k8chtlocal) (min	Ħ ≌性原則 例)Œ):	? × 5 物件類型(0) 位置(L) 検査名額(C) 確定 取消

10. 稽核項目設定:

點選並編輯稽核項目清單內所要的稽核項目

勾選該稽核項目的 [成功] 及 [失敗]的項目, 設定完成後按 [確定]。

📕 temp 的稽核項目		×
物件 名稱(N): carlos (carlos@win2k8cht 套用在(O): 這個資料夾、子資料2	.local)	變更(C)
存取(\$): 完全控制 周遊資料夾/執行檔案 列出資料夾/樹取資料 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	_{成功} V V V V V V V V V V V V V V V V V V V	<u>失敗</u> ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥
□ 僅套用這些稽核項目到此容器 及(或)容器(T) 管理稽核		全部清除(L)

11. 在進階安全性設定完成後,點選 [確定]。

📗 temp 的進階3	安全性設定				×
稽核					
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	、[[龍輯]。		
サールト わ おない	C.M				
物件省偶:	C: 10 sers Administrator Des	кюриетр			
稽核項日(1):	ク報2	方雨	備委員	本田和	-
全部	carlos (carlos@win2k8cht	<u>1940</u> 完全控制	遮承日 <非繼承的>	」安用到 這個資料夾、子資…	-
新增(D)	編輯(E)	刪除(R)			
	5公酒与托偿承接达酒日小				
▼ 16年10日日	92.項巴拉羅承格依項目(1) 9幾金链核項日取代所有子級	▲現有的幾番/菇枝項日/	ውነ		
			(47)		
藉核物件存取	的需求為何?				
			-		
			催疋		

12. 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 以前的間	反本│自訂	1			
物件名稱: C	\Users\Administrate	or\Desktop\tem	р			
群組或使用者名和	髴(G):					
SYSTEM	@win2k8cht local)					
administrator	(WIN2K8CHT\adm	inistrator)				
& Administrator	s (WIN2K8CHT\Ad	lministrators) 				
若要變更使用權腳	限,請按一下 [編輯	輩]。	編輯(E)			
carlos的權限(P)		允許	拒絕			
完全控制		1	_			
讀取和執行		~				
列出資料夾內?	列出資料夾内容					
富入						
如需特殊權限或進階設定,請按一下 [進進階(V) 階]。						
深入瞭解存取控制及權限						
	闘閉	取消	套用(A)			

13. 點選 [開始功能表 / 系統管理工具 / 電腦管理]。



14. 點選 [系統工具 / 共用資料夾 / 共用]。

🛃 電腦管理				
檔案(F) 執行(A) 檢視(V) 說明(H)				
🗢 🔿 📶 🖬 🙆 🔜 👔				
 ■ 潤管理(本機) ① 工作排程器 ④ 工作排程器 ● ④ 工作階段 ● ○ 工作階段 ● ○ 工作階段 ● ○ 工作階段 ● ○ 可靠性和效能 ● ○ 可靠性和效能 ● ○ 可靠性和效能 ● ○ 可靠性和效能 ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	共用 ▲ 家 ADMIN\$ 家 C\$ 家 IPC\$ NETLO 家 npartner 家 SYSVOL 家 temp 家 Users	資料夾路徑 C:\Windows\SYSVO C:\Windows\SYSVO C:\temp\npartner C:\Windows\SYSVO C:\temp C:\Users	類型 Windows Windows Windows Windows Windows Windows Windows	#用 0 0 0 0 0 0 0

15. 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]。



4 Windows 2012 Active Directory Server 稽核設定

本章節主要說明以下操作設定:

1. 設定網域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 AD 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 設定網域使用者登入登出的稽核原則

設定步驟如下:

 以全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分登入 Windows 2012 Active Directory Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用) 開啟群組原則管理:

點選[Windows PowerShell][,]輸入:**gpmc.msc** ,完成後按[Enter]



- 以本文件為例子(實際情況請依使用者的環境做調整), 點選 [樹系 / 網域 / NPWin2012r2.local / Domain Controllers / Default Domain Controllers Policy]。

	群組原則管	理		_ _ ×
🔜 檔案(F) 動作(A) 檢視(V) 視窗(W) 說明(H)				_ & ×
(+ +) 🖄 📰 💥 🙆 📲 🖬				
Kate State Sta	Default Domain Controllers 領域 詳細資料 設定 委派 連結 在這個位置顯示連結(L): 下列站台、網域及組織單位已連 2 建額(N) 2 設用連結(L)	Policy NPWin2012r2 結到這個 GPO(T): 僅制 否	2.local 飲用連結 是	× 路徑 NPWin2012r2.local/Domain Controllers
☆ 群組原則模型 ○ 群組原則結果	儲存報告(S) 檢視(V) 從這裡關歐新視豪(W) 刪除(D) 重新命名(M) 重新卷理(P)	群組、使用者及電腦()	III 5):	
	i就明(H) 新埔(D) WMI 篩躍 這個 GPO 已連結到下列 WMI 即 <無>	移除(R) 携選器(W):	内齊(P) ▼	開啟(O)
開飯 GPO 編輯器				

註:此步驟展開網域,會有 [Default Domain Policy](預設網域安全性原則);

另外展開 Domain Controllers(網域控制站)[,]會有 [Default Domain Controllers Policy] (預 設網域控制站安全性原則) [。]

建議將此兩種安全性稽核原則設定為一致

4. 點選 [電腦設定 / 原則 / Windows 設定 / 安全性設定 / 本機原則 / 稽核原則]

B	群組原則管理編輯器	_ D X
【 檔案(F) 動作(A) 檢視(V) 說明(H) ◆ ◆ ② @ ※ ☞ 图 ☶ ② Default Domain Controllers Policy [WIN2012R2AD.NPWIN20 / ④ 電磁設定 ④ で原則 ▶ ◎ 軟體設定 ▲ ○ Windows 設定 ▶ 名稱解析原則	群組原則管理編輯器 原則 ▲ 原則 ▲ 副 稽核目錄服務存取 圖 稽核条紙事件 圖 稽核称件存取 圖 稽核原則變更 圖 稽核符获權限使用	
 ::::::::::::::::::::::::::::::::::::	 □ 福枝城戶登入事件 □ 福枝城戶登入事件 □ 福枝登入事件 □ 圖 福枝程序追蹤 	成功,失敗 成功,失敗 成功,失敗 沒有稽核
> ● ●		

- 5. 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 [定義這些原則設定]·

再勾選 [成功] 及 [失敗] · 設定完成後按 [確定] •



(2) 稽核帳戶登入事件:

湯鼠雙擊 [稽核帳戶登入事件],勾選 [定義這些原則設定], 再勾選 [成功]及[失敗],設定完成後按[確定]。



(3) 稽核原則變更:

雙擊 [稽核原則變更]·勾選 [定義這些原則設定]·再勾選 [成功] 及 [失敗]·設定完成後按 [確定]。

(4) 稽核帳戶管理:

雙擊 [稽核帳戶管理]·勾選 [定義這些原則設定]·再勾選 [成功]及[失敗]·設定完成後 按 [確定]。

(5) 稽核物件存取:

滑鼠雙擊 [稽核物件存取],勾選 [定義這些原則設定]。

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 Active Directory 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, 僅需勾[定義這些原則設定值]即可. 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。



4.2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...], 開啟 新增共用精靈。

伺服器 磁碟 在放集區 其用 iSCSI 工作資料夾	新用 新有共用 總計 2 正作 ▼ 新用 中間路 中間路 中間路 中間路 中間路 中間路 中間路 中間路 中間路 中間路 中間路 中間路 中間路 中間路 	音量 WIN2012R2AD 約 NETLOGON (C) 香量: 59.7 G8 一 ご使用空間 9.82 G 一 ご使用空間 9.82 G ● ご使用空間 9.82 G 留理磁調 格式化- 延伸磁調 設定重報 内容 前往磁環區概要 >	▲ SI 重號碰碟 家統中的錯誤 清統錯誤 機代號和存取路徑 I區 I區 I面
		若要使用配額,必須交裝備案伺服器資源管理員。 若要安裝備案伺服器資源管理員,請飲動新增角色和功能積 靈,	er 20 er 2012 R v

2. 滑鼠左點 [SMB 共用-快速] · 左點 [下一步]。

a	新增共用精	· · · · · · · · · · · · · · · · · · ·
選取此共用的設定 選取設定橋 共用位置 共用名稱 其他設定 編現 確認 結果	E 檔案共用設定幅(P): SMB 共用 - 快速 SMB 共用 - 進階 SMB 共用 - 應用程式 NFS 共用 - 快速 NFS 共用 - 進階	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] 對話方魂來設定進階選項
	<.	上一步(P) 下一步(N) > 建立(C) 取満

3. 左點 [輸入自訂路徑] · 本例為輸入 " C:\share_folder " · 左點 [下一步] ·

選取設定檔	伺服器(S):					
共用位置	伺服器名稱	狀態	叢集/	自色	擁有者節點	
世田を招	WIN2012R2AD	線上	未叢	東處理		
大用有冊						
只他成正						
	共用位置:					
	○ 祝經編區選取(V):			100-00-0 (00		
	磁螺區	可用空間	管量	福案条統		
	C:	49.8 GB	59.7 GB	NIFS		
	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。		

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]。

B	新增共用精靈 — — — — — — — — — — — — — — — — — — —
▶ 店定共用名稱 選取設定檔 共用位置 其用名稱 其他設定 檔閱 諸果	新増共用精靈 X 共用名幅(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):
	< 上一步(P) 下一步(N) > 建立(C) 取消

5. 勾選 [啟用存取型列舉]·左點 [下一步]。

b	新增共用精靈
○ 設定共用設定 選取設定 選取設定 共用位置 共用名稱 任設定 催認 結果	 ★ 如田存取型列舉(A) 承取型列舉只會顯示使用者有權存取的檔案和資料表。如果使用者不具資料表的讀取(或同等)權 限,Windows會優潮該資料支,不讓使用者看見。 か計對共用進行快取(W) 快取課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。 在檔案共用上較用 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 可約其他電腦使用。 加密資料存取(E) 和密資料存取(E) 和密資料存取(E) 和客选共用的意識檔案存取,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,如果此方塊已勾選且變成灰色,即表示系統管理員已對整個伺服器開啟加密功 能。
	<上一步(P) 下一步(N) > 建立(C) 取消

6. 點選 [自訂權限... / 稽核 / 新增] 。

B		新增共用精靈			X		
設定權限以控制有	字取權						
速取設定檔	已使用資料夾	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	檔案的權		
共用位置 井田健児・所有人完整控制							
共用省柟							
兵也改走	類型	主體	存取	套用到			
1年 Hg 10年 571	允許	CREATOR OWNER	完全控制	只有子資料夾及檔案			
an an	允許	BUILTIN\Users	特殊	這個資料夾及子資料夾			
	允許	BUILTIN\Users	讀取與執行	這個資料夾、子資料夾及檔題	Rf .		
	允許	BUILTIN\Administrators	完全控制	這個資料夾、子資料夾及檔題			
	允許	NTAUTHORITY/SYSTEM	完全控制	這個資料夾、子資料夾及個調			
	元計	Everyone	完王控制	坦陶貞科兴、于真科灭及個界	R		
		<上-	-步(P) 下-	-步(N) > 建立(C)	取満		
B		share_folder 的進階安全	性設定		_ _ ×		
名稿: c:\share_folder	1						
擁有者: Administrators (NPW)	2012R2\Admini	strators) 嬰奧(C)					
權限 共用 稽	核有效存到	R權					
如佛其他資訊,請按两下租核項目,	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:		-	-				
· · · · · · · · · · · · · · · · · · ·	存	取 / //////////////////////////////////	承日		太 及檔案		
新增(D) 移除(R) 检视(V	0						
停用繼承(I)							
□ 以此物件中的可繼承稽核項目取代/	所有子物件相核項	(₽)					
		R 2 1 (2 1 (2 1 (2 1 (2 1 (2 1 (2 1 (2 1					
				耀定 取消	整用(A)		

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]。(註:若要選擇其他網域,可點選 [位置])

	Share_rouch and to be a	
慢: 選取一個主體		
型: 成功	送取使用者、電腦、服務帳戶或群組	
用到: 這個資料夾、子資料本及檔案	∽ 攝取這個物件類型(S):	
	使用者、群組或內建安全性主體 初件類型(O)	
本權限:	從這個位置(F):	顧示進階權即
□ 完全控制	NPWin2012r2.local 位置(L)	
(修 改	請輸入物件名稱來選取 (<u>範例</u>)(E):	
✓ 請取和執行 ☑ 列出資料本内容	Everyone 檢查名稱(C)	
□ 寫入		
□ 特殊存取權限	進階(A) 確定 取消	
只將這些稽核設定套用至此容器內的物件和(或)會	(T) 器(T)	全部清除
曾一個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。	
直悟(中(D)		

55 byright © All rights are reserved by N-Partner Technologies 8. 類型 下拉選 [全部],基本權限勾選 [完全控制],然後按左點 [確定]。

J.	share_folder 的稽核項目	_ D X
主體: 類型: 套用到:	Everyone 骥取一圈主體 全部	
基本權	禄: ⑦完全控制 ⑦修改 ⑦ 請取和執行 ⑦ 引出資料夾內容 ⑦ 請取 ⑦ 請取 ○ 為入 ○ 結片空取線!!	顯示進階權限
□只將 新増一 新増條(□ ^{特殊 存取 催取} 這些稽核說定套用至此容器內的物件和 (或) 容器(T) 國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。 F(D)	全部遺除
	確定	取満

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。

B			share	e_folder 的進階安全	性設定	_ 0	x
名稱:	c:\share_folde	r					
擁有者:	Administrator	(NPWIN2012	2R2\Administrators) 變更(C)			
權限	共用	稽核	有效存取權				
如需其他資訊 稽核項目:	1. 請按兩下稽核	項目・如果要	修改稽核項目,請	選取項目, <u>然後按一下</u>	[編輯] (如果遵用	B) •	
類型 88、全部	主題 Everyone		存取 完全控制	14 11	承自	家用到 這個資料夾、子資料夾及傷案	
新增(D) 停用瘧承(I 〕以此物件4		捕轤(E) 目取代所有子	物件稽核項目(P)			確定 取消 套用](A)
-							-
確認建	攫取項目	Treb	20 N T 45 J 10		T 774		
選取設定	記檔	位住	認以下為止的	#設定・ 熱後按-	-ト[建立]	8- 	_
共用(4) 共用名(其他設) 櫂眼	画 周 定		共用位置 伺服器: 囊集角色: 本機路徑:	WIN2012R2AD 未叢集處理 c:\share_folder			
確認結果			共用內容 共用名稱: 通訊協定: 存取型列舉: 快取感理: BranchCache: 加密資料:	share_folder1 SMB 已歐用 已歐用 已停用 已停用			
				< <u>+-</u>	-#(P) 下一	(N) > 建立(C) 取満	

5 Windows 2016 Active Directory Server 稽核設定

本章節主要說明以下操作設定:

1. 設定網域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 2016 AD 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。

5.1 設定網域使用者登入登出的稽核原則

設定步驟如下:

 以全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分登入 Windows 2016 Active Directory Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用) 開啟[群組原則管理]:

滑鼠左點[開始] · 右點[Windows PowerShell] · 左點[以系統管理員身分執行] • 輸入 : gpmc.msc → 完成後按 [Enter]



2. 以本文件為例子(實際情況請依使用者的環境做調整), 點選 [樹系 / 網域 / npwin2016-cht.local / Domain Controllers / Default Domain Controllers Policy]。

🔜 群組原則管理		– 🗆 X
🔜 檔案(F) 動作(A) 檢視(V) 視窗(W) 說明(H)		_ & ×
🗢 🔿 🗾 🗙 🍳 🗾 🖬		/ / /
 ■ 群组原則管理 ▲ 樹系: npwin2016-cht.local ● 鋼 npwin2016-cht.local ● I powin2016-cht.local ② Default Domain Policy ● ② Default Domain Controllers ● ③ 群组原則物件 > ● ● 群组原則物件 	Default Domain Controllers Policy 領域 詳細資料 設定 委派 連結 在這個位置顯示連結(L): npwin2016-cht.lo 下列站台、網域及組織單位已連結到這個 GPO(T): 編輯(E) 強制 啟 強制(N) 否 是	rcal ~ 用連結 路徑 npwin2016-cht.local/Domain Cor
 > □ → WMI 篩獲器 > □ 入門 GPO > □ 網站 一 網知站 一 新祖原則模型 ■ 新祖原則結果 	放用速结(L) 百 定 儲存報告(S) 儲存報告(S) 檢視(V) > 從這裡開啟新視窗(W) 群組、使用者及電腦(S): 一副除(D) 群組、使用者及電腦(S): 重新命名(M) 二 重新範望(F) 説明(H)	spwinzoro-entriocal/Domain Cor
開啟 GPO 編輯器	新増(D) ₩MI 篩選 這個 GPO 已連結到下列 WMI 篩選器(W): <無>	内容(P) 開啟(O)

註:此步驟展開網域,會有 [Default Domain Policy] (預設網域安全性原則);

另外展開 Domain Controllers(網域控制站) · 會有 [Default Domain Controllers Policy] (預 設網域控制站安全性原則) [。]

建議將此兩種安全性稽核原則設定為一致

4. 點選 [電腦設定 / 原則 / Windows 設定 / 安全性設定 / 本機原則 / 稽核原則]

■ 群組原則管理編輯器		-	×	
檔案(F) 動作(A) 檢視(V) 說明(H)				
🔶 🔿 📶 📑				
● fault Domain Controllers Policy [WI ◆ ● 電腦設定 ● 原則 ● 原則 ● 原則 ● 目前 ● 目前 ● 目前 ● 日前 ● 日前 <t< td=""><td>原則 原 職 稽核目錄服務存取 沒 職 稽核亦事件 沒 職 稽核原則量更 沒 職 稽核原則量更 沒 職 稽核原則量更 沒 職 稽核原則量更 沒 職 稽核师戶營入事件 沒 職 稽核吨戶管理 沒 職 稽核電戶追蹤 沒</td><td>則 有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有</td><td></td><td></td></t<>	原則 原 職 稽核目錄服務存取 沒 職 稽核亦事件 沒 職 稽核原則量更 沒 職 稽核原則量更 沒 職 稽核原則量更 沒 職 稽核原則量更 沒 職 稽核师戶營入事件 沒 職 稽核吨戶管理 沒 職 稽核電戶追蹤 沒	則 有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有有		

- 5. 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 [定義這些原則設定],

再勾選 [成功] 及 [失敗] · 設定完成後按 [確定] •



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

(2) 稽核帳戶登入事件:

滑鼠雙擊 [稽核帳戶登入事件]·勾選 [定義這些原則設定]· 再勾選 [成功]及 [失敗]·設定完成後按 [確定]。



(3) 稽核原則變更:

雙擊 [稽核原則變更]·勾選 [定義這些原則設定]·再勾選 [成功] 及 [失敗]·設定完成後按 [確定]。

(4) 稽核帳戶管理:

雙擊 [稽核帳戶管理]·勾選 [定義這些原則設定]·再勾選 [成功]及[失敗]·設定完成後 按 [確定]。

(5) 稽核物件存取:

滑鼠雙擊 [稽核物件存取],勾選 [定義這些原則設定]。

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 2016 Active Directory 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, 僅需勾[定義這些原則設定值]即可. 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 [。]

5.2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...], 開啟 新增共用精靈。



2. 滑鼠左點 [SMB 共用-快速] · 左點 [下一步]。

🏊 新增共用精靈		– 🗆 ×
選取此共用的	設定檔	
趨取設定檔 共用位置 共用名稱 其他設定 權限 確認 結果	檔案共用設定檔(P): SMB 共用 - 快速 SMB 共用 - 進階 SMB 共用 - 應用程 NFS 共用 - 快速 NFS 共用 - 進階	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攤項
		<上一步(P) 下一步(N) > 建立(C) 取満

3. 左點 [輸入自訂路徑],本例為輸入 "C:\share_folder ", 左點 [下一步]。

新增共用精靈					_31		×
巽取叶井田的	伺服哭和路须						
選取設定檔	伺服器(S):						
井田位置	伺服器名稱	狀態	叢集創	角色	擁有者節點		
共用位 型	WIN2016-AD-CHT	線上	未叢	東處理			
大市有個							
具他設定							
權限							
確認							
結果							
	共用位置:						
	○ 依磁碟區選取(V):						
	磁碟區	可用空間	容量	檔案系統			
	C:	81.5 GB	99.5 GB	NTFS			
	檔案共用的位置將會是所	f攫磁碟區上 \Share	s 目錄中的	新資料夾。			
	動入自訂路徑(T):						
	C:\share_folder					瀏覽(B	i)
		< +_++(D)	T -#0	ND N	建立(の)	En X4	
		< <u></u> <u>−</u> 2 (P)		N/ 2)正式(C)	RX/R	

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]。

🏊 新增共用精靈		<u></u>		×
指定共用名稱				
避 取設定檔 +	共用名稱(A): share_folder			
开用位置 井田 夕 編	共用描述(D):			
其他設定				
確認	要共用的本機路徑(L):			-
結果	C:\share_folder 要共用的遠端路徑(R): \\\WIN2016-AD-CHT\share_folder			
	<上一步(P) 下一步(N) > 建立(C)		取消	

5. 勾選 [啟用存取型列舉], 左點 [下一步]。



📥 新增共用精靈				_*		×
設定權限以控制	存取權					
選取設定檔 共用位置	已使用資料 限・	¥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材	當案的權	
共用名稱	共用權限:	所有人完整控制				
其他設定	資料夾權附	艮(F):				
權限	類型	主體	存取	套用到		
確認	允許	CREATOR OWNER	完全控制	只有子資料夾及檔案		
194 HU	允許	BUILTIN\Users	特殊	這個資料夾及子資料夾		
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		
	自訂權	谡(C)				
		< +-	-步(P) 下-	-步(N) > 連立(C)	取消	
				ALL (9)	-	

share_folde	r 的進階安全性設定				~		×
名稱:	C:\share_folder						
擁有者:	Administrators (NPW	/IN2016-CHT\Administrators) 變更	(C)				
權限	共用 和	該 有效存取權					
如需其他資訊 稽核項目:	汛,請按兩下稽核項目。	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)。			
類型	主體	存取	繼承自	套用到			
新增(D) 停用繼承(移除(R) 截落 	見(V)					70
□以此物件□	中的可繼承稽核項目取代	,所有子物件稽核項目(P)					
				確定取決	ij	套用	(A)

66 Copyright © All rights are reserved by N-Partner Technologies Co. 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]。(註:若要選擇其他網域,可點選 [位置])

🧧 share_folder 的稽核項目		- 🗆 X
主體: <u>遵取一個主體</u> 類型: 成功 賽用到 : 這個資料夾、資料夾及檔案	 ✓ ✓ 	
基本權限: 常全控制 一修改 一結取和執行 一列出資料夾內容 一結取 二章入 一特殊存取權限 一只將這些稽核設定套用至此容器內的物件和 新增一個條件以限制此稽核項目的範圍・只有很 新增條件(D)	選取使用者、電腦、服務帳戶或群组 《選取這個物件類型(5): 使用者、帮組或內建安全性主體 物件類型(0) 從這個位置(F): npwin2016-cht locsl 位置(L) 能 人物件名稱來選取(範例)(E): 上veryone 健踏(A) 確定 取消	顯示進随權限 全部
		確定 取消

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

顯示這略權的
全部海除

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。

sha	re_folder	的進階安全性設	定				- 0	×
名稱	i:	C:\share_fold	er					
擁有	ī者:	Administrato	rs (NPWIN201	6-CHT\Administrators) 摸到	E(C)			
1	雚限	共用	稽核	有效存取權				
加需 稽核)其他資訊 項目:	,請按兩下稽核	§項目。如果要	修改稽核項目,請選取項目],然後按一下 [編輯] (如果適月	用)。		
	類型	主體		存取	繼承自	套用到		
2	全部	Everyone		完全控制	無	這個資料夾、子資料	¥夾及檔案	
羗	f増(D)	移除(R)	編 輯(E)					
痛何	所増(D) 予用繼承(I) (此物件中	移除(R)	編輯(E) 夏目取代所有子	物件稽核項目(P)				,

6 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
- (2) 滑鼠點選[設備管理 / 設備樹狀圖 / 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]下拉選單中選擇

{Windows AD} · 勾選[啟動接收] · 按下[確定] · 即完成設備的系統新增程序

N-CLOUD						
Npartner (Global) ~ 🔁	Home / 設備管理 / 設備樹狀園					
i 事件 🙂 🚠	設備樹狀園					
山 報表 🚺 🛛 🔠	S Q 2 B U 49					
📑 設備管理 🛛 🖬 🖬 👘 👘	📄 Global (123) 🛕 🛕	操作	所屬領域 ≑	IP 🛋	設備名稱 🗢	設備種類 🗢
● 糸統管理 田 2	☑ 未知設備 (20)	e 🖻	Global	1.1.1.8	1.1.1.8	Syslog
A		× Câ	Global	10.0.0.235	10.0.0.235	Flow
	設備基本設定	^ ♂ □	Global	10.1.34.220	10.1.34.220	Syslog
	名稱	C 🖬	Global	10.10.10.101	10.10.10.101	🌘 Syslog
	Win2016AD 192.168.1.90	2 🖬	Global	10.10.10.2	10.10.10.2	Syslog
		2 🖬	Global	10.10.10.3	10.10.10.3	Syslog
	IP	2 🖬	Global	10.143.238.95	10.143.238.95	Syslog
	192.168.1.90	C 🖬	Global	10.143.238.96	10.143.238.96	Syslog
		C 🖬	Global	10.63.136.26	10.63.136.26	Syslog
	設備種類	C 🖬	Global	10.63.136.26	10.63.136.26	Syslog
	Syslog Flow SNMP	6 🖬	Global	10.64.103.245	10.64.103.245	Syslog
		C 🖬	Global	10.64.103.44	10.64.103.44	Syslog
	Syslog 相關設定	2 🖬	Global	172.16.1.235	172.16.1.235	Syslog
	[]	2 🖬	Global	191.168.2.252	191.168.2.252	Flow
	資料格式	2 🖬	Global	192.168.0.253	192.168.0.253	8 Flow
	Windows AD	32 ≞	Global	192.168.1.43	192.168.1.43	Syslog
		a	Global	192.168.1.90	192.168.1.90	Syslog
	Facility	C 🖬	Global	192.168.10.14	192.168.10.14	🔘 Syslog
		C 🖬	Global	192.168.10.15	192.168.10.15	Syslog
		C 🖬	Global	192.168.2.86	192.168.2.86	Syslog
	編碼方式					
	UTF-8					
		•				
	確定	25 *	● ● 第 1	」共1員 ▶ ▶ ○		

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

