

如何設定 Windows File 事件記錄

V009





N-Partner Technologies Co. 版權所有。未經 N-Partner Technologies Co. 書面許可,不得以任何形式仿製、拷貝、 謄抄或轉譯本手冊的任何內容。由於產品一直在更新中,N-Partner Technologies Co. 保留不告知變動的權利。

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標、均屬其合法註冊公司所有。





前	言.		
1	NXL	.og	
	1.1	NXLog 安裝	
	1.2	NXLog 設定檔下載 6	5
		1.2.1 Windows 2003 或之前版本作業系統 . 6	
		1.2.2 Windows 2008 或之後版本作業系統 . 7	
	1.3	NXLog 設定檔 8	
		1.3.1 Windows 2003 或之前版本作業系統 . 8	
		1.3.2 Windows 2008 或之後版本作業系統 . 9	
	1.4	NXLog 啟動服務 11	
		1.4.1 Windows 2003 或之前版本作業系統 . 11	
		1.4.2 Windows 2008 或之後版本作業系統 . 14	6
2	Win	dows 2000	
	2.1	網域 17	
		2.1.1 組織單位設定	
		2.1.2 群組原則設定	
	2.2	工作群組	
		2.2.1 稽核原則設定	
		2.2.2 事件檔案設定	
	2.3	稽核資料夾設定30	7
3	Win	dows 2003	
	3.1	網域	
		3.1.1 組織單位設定	
		3.1.2 群組原則設定	
	3.2	工作群組	
		3.2.1 稽核原則設定 45	
		3.2.2 事件檔案設定 49	
	3.3	稽核資料夾設定	8
4	Win	dows 2008	
	4.1	網域 55	
		4.1.1 組織單位設定	
		4.1.2 群組原則設定	
	4.2	工作群組 65	

	4.2.1	稽核原則設定	·	·	•	•	·	•	·	•	•	·	·	•	·	•	65
	4.2.2	事件檔案設定			•	•					•			•			69
4.3	稽核資	『料夾設定			•	•					•			•			72
Wind	dows 20	012															77
5.1	網域																77
	5.1.1	組織單位設定															77
	5.1.2	群組原則設定															82
5.2	工作群	組															89
	5.2.1	稽核原則設定															89
	5.2.2	事件檔案設定			•	•		•			•			•			93
5.3	稽核資	『料夾設定			•	•		•			•			•			96
Wind	dows 20	016															103
6.1	網域																103
	6.1.1	組織單位設定															103
	6.1.2	群組原則設定															108
6.2	工作群	組															115
	6.2.1	稽核原則設定															115
	6.2.2	事件檔案設定															119
6.3	稽核資	〔料夾設定															122
Wind	dows 20	019															129
7.1	網域																129
	7.1.1	組織單位設定															129
	7.1.2	群組原則設定															134
7.2	工作群	組															141
	7.2.1	稽核原則設定															141
	7.2.2	事件檔案設定															145
7.3	稽核資	『料夾設定															148
Wind	dows 20	022															155
8.1	網域																155
	8.1.1	組織單位設定															155
	8.1.2	群組原則設定															160
8.2	工作群	組															167
	8.2.1	稽核原則設定															167



		8.2.2	事件檔	案設定	Ξ.							 171
	8.3	稽核資	料夾設;	定							•	 174
9	N-Re	eporter									•	 181
	9.1	Window	ws 2003	3 或之	前版	ō本	作賞	養 系	統	•	•	 183
	9.2	Windov	ws 2008	3 或之	後版	ō本	作賞	美 系	統	•	•	 186
10	問題	排除 .									•	 189
	10.1	Invoke	-GPUpo	date	誨							 189





本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLog 方式設定 Windows File 事件記錄。 NXLog 工具將 Windows 事件記錄轉成 syslog · 再轉發到 N-Reporter 做正規化、稽核與分析。 此文件適用於作業系統的 Windows Server 2000 / 2003 / 2008 / 2012 / 2016 / 2019 / 2022 版本。

稽核原則建議:https://learn.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-bes t-practices/audit-policy-recommendations 監視的事件:https://learn.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/appendix-l--event s-to-monitor

註:本文件僅做為如何將日誌吐出的設定參考,建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。



1 NXLog

1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition

前往網址 https://nxlog.co/products/nxlog-community-edition/download 下載網址最新版 nxlog-ce-x.x.xxxx.msi, 範例: nxlog-ce-3.0.2272.msi



註:若需要下載 NXLog 32bit 版本,請與我們連繫。

(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].

₩NXLog-CE Setup	
	Welcome to the NXLog-CE Setup Wizard The Setup Wizard will install NXLog-CE on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel



-> 勾選 [I accept the terms in the License Agreement], 按 [Next].

	NXLOG PUBLIC LICENSE v1.0	
1.	DEFINITIONS	
"Li L	icense" shall mean version 1.0 of the NXLOG PUBLIC ICENSE, i.e. the terms and conditions set forth in this document	
"Se	oftware" shall mean the source code and object code form, all	
as	ssociated media, printed materials, and "online" or electronic	

-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)

NXLog-CE Setup	_ 🗆 🗙
Destination Folder Click Next to install to the default folder or click Change to choose another.	
Install NXLog-CE to:	
C:\Program Files\nxlog\	
Change	
Back Next	Cancel



-> 按 [Install].



-> 按 [Finish].





<2.2> Windows 2003

點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Install] 到 [Finish].

伊 NXLog-CE Setup	-		×
Ready to install NXLog-CE			X
Click Install to begin the installation. Click Back to review or change ar installation settings. Click Cancel to exit the wizard.	ny of you	r	
Back Install		Cano	el

<2.3> Windows 2000

前往 NXLog CE 舊版網址 https://sourceforge.net/projects/nxlog-ce/, 左點 [See All Activity], 下載 NXLOG CE

支援 Windows2000 版本 nxlog-ce-2.8.1248.msi.

點擊 [nxlog-ce-2.8.1248.msi] -> 勾選 [I accept the terms in the License Agreement] -> 按 [Install] 到 [Finish].





1.2 NXLog 設定檔下載

1.2.1 Windows 2003 或之前版本作業系統

(1) 開啟 [命令提示字元]



(2) 下載 NXLog Windows 2003 File 設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔。

下載連結:http://www.npartnertech.com/download/tech/nxlog_Win2003File.conf

PS C:\> copy "C:\nxlog_Win2003File.conf" "C:\ Program Files \nxlog\conf\nxlog.conf" /y

🔤 命令提示	字元			_ 🗆 🗡
C:╰>copy 複製了 C:╰>_	"C:\nxlog_Win2003File.conf" 1 個檔案。	"C:\Program	Files\nxlog\conf\nxlog.conf	'/y 🔺
▲				▼ ▶ //

本文件範例是 64 位元作業系統,若作業系統是 32 位元,紅色文字部位請改以下設定 'C: \Program Files (x86) \nxlog\conf\nxlog.conf'



1.2.2 Windows 2008 或之後版本作業系統

(1) 開啟 [Windows PowerShell]



(2) 下載 NXLog Windows 2008 File 設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔。

下載連結:http://www.npartnertech.com/download/tech/nxlog_Win2008File.conf

PS C:\> Invoke-WebRequest -Uri`http://www.npartnertech.com/download/tech/nxlog_Win2008File.conf' -OutFile 'C:\ Program Files\nxlog\conf\nxlog.conf'

≥ 系統管理員: Windows PowerShell	-		×
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Win2 -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'	308Fi	ile.conf	^
PS C:\>			~

本文件範例是 64 位元作業系統,若作業系統是 32 位元,紅色文字部位請改以下設定 'C: \Program Files (x86)

\nxlog\conf\nxlog.conf'



1.3 NXLog 設定檔

1.3.1 Windows 2003 或之前版本作業系統

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.3.88
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%/cert
define CONFDIR %ROOT%/conf
define LOGDIR %ROOT%/data
define LOGFILE %LOGDIR%/nxlog.log
LogFile %LOGFILE%
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
## Load the modules needed by the outputs
<Extension syslog>
        Module
                            xm_syslog
</Extension>
## For windows File 2000 - 2003 Event Log use the following:
<Input in_eventlog>
        Module im_msevent.
ReadFromLast TRUE
SavePos TRUE
Exec parse_syslog
                           im_mseventlog
                      parse_syslog_bsd();\
Exec parse_systog_bsd();\
if ($EventID == 560 or $EventID == 561 or $EventID == 562 or $EventID == 563 or $EventID ==
564 or $EventID == 567 or $EventID == 528 or $EventID == 529 or $EventID == 530 or $EventID ==
531 or $EventID == 532 or $EventID == 533 or $EventID == 534 or $EventID == 535 or $EventID ==
536 or $EventID == 537 or $EventID == 538 or $EventID == 539 or $EventID == 540 or $EventID ==
531 or $EventID == 552 or $EventID == 682 or $EventID == 683 or $EventID == 672 or $EventID ==
551 or $EventID == 674 or $EventID == 675 or $EventID == 676 or $EventID == 677 or $EventID == 678 or
$EventID == 679 or $EventID == 680 or $EventID == 681){ $SyslogFacilityValue= 17; }
else if ($SourceName == "Service Control Manager"){ $SyslogFacilityValue = 17;}

                else\
{\
                        drop();\
</Input>
<Output out_eventlog>
        .
Module
                        om_udp
%NCloud%
514
        Host
        Port
        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>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

define NCloud 192.168.3.88

本文件範例環境為 64bit 作業系統,若作業系統環境為 32bit 請改為以下設定

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

修改設定檔內容後需" 另存新檔" 覆蓋原本檔案,1. 存檔類型請選擇" 所有檔案 (*.*)",2. 編碼請選擇"UTF-8" 以免編碼錯

誤造成服務無法正常開啟。

檔案名稱(N): nxlog	conf												~	
存檔類型(T): 所有檔	案 (*.*)	1											~	
藏資料夾						編碼(E):	ANSI ANSI		~	存檔(S)		取消		
							Unicode Unicode UTF-8	e bigendi 2	an					



1.3.2 Windows 2008 或之後版本作業系統



本文件範例環境為 64bit 作業系統,若作業系統環境為 32bit 請改為以下設定

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



修改設定檔內容後需"另存新檔"覆蓋原本檔案,1.存檔類型請選擇"所有檔案 (*.*)",2. 編碼請選擇"UTF-8"以免編碼錯 誤造成服務無法正常開啟。

檔案名稱(N):	nxlog.conf		~
存檔類型(T):	所有檔案 (*.*) 1		~
截資料夾		NSI ~ 存檔(S) 取消	
	Un Un UT	Inicode Inicode big endian ITF-8 2	



1.4 NXLog 啟動服務

1.4.1 Windows 2003 或之前版本作業系統

(1) 開啟 [命令提示字元]



(2) 啟動 NXLog 服務和確認 NXLog 沒有錯誤訊息





(3) 開啟 [服務] 功能





(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 🗳 點選 [內容]

物品资					_ [X		
檔案(E) 執行(A) 檢視(V) 說明(H	D							
← → 🗷 🗗 🖻 🗟 😫 🗷								
[%] 》 服務 (本機) 内容	_							
nxlog	名稱 △	描述	狀態	啓動類型	登入身分			
	🏶 Network DDE DSDM	訊息動		停用	本機系統			
<u>客動</u> 服務	🍓 Network Location Awa	收集並…	已啓動	手動	本機系統			
	🆏 Network Provisioning	在網域…		手動	本機系統			
t#\$#.	NT LM Security Suppo	爲沒有		手動	本機系統			
This service is responsible for running the	and og	This ser		自動	本機系統			
NXLog agent. See www.nxlog.co.	🎇 Performance Logs and	基於爭…		目動	網路服務			
	🍓 Plug and Play	啓用電	已啓動	自動	本機系統			
	🏶 Portable Media Serial N	Retrieve		手動	本機系統	-		
∖延伸 / 標準 /								
		ſ						

(5) [一般] 頁面 -> 確認; 啟動類型: [自動]

NXLog 內容 (本後	•電醫) ? ×
一般 登入	修復 依存性
服務名稱:	nxlog
顯示名稱(N):	NXLog
描述(<u>D</u>):	This service is responsible for running the NXLog agent. See www.nxlog.co.
執行檔所在路徑	(H):
"C:\Program File	s (x86)\nxlog\nxlog.exe" -c "C:\Program Files (x86)\nxlog'
啓動類型(正):	eð.
服務狀態:	己啓動
啓動(3)	停止(I) 暫停(2) 繼續(32)
您可以在這裡指	定啓動服務時所要套用的參數。
啓動參數(<u>M</u>):	
	確定 取消 (点)



(6) [修復] 頁面 -> 確認; 第一次失敗時: 和第二次失敗時: 和後續失敗時: [重新啟動服務] -> 按 [確定]

NXLog 內容 (本機	電腦)				? ×
一般 登入	修復	夜存性			
如果這項服務執行	行失敗時,	電腦將採取的	的回應。		
第一次失敗時④	:	重新啓動服	務		J
第二次失敗時(3)		重新啓動服	務		J
後續失敗時(U):		重新啓動服	務		<u> </u>
重設失敗計數於	(D):	0	天之後		
重新啓動服務於	(∕):	1	分鐘之後		
-執行程式 程式(2):					
				瀏覽(B)	
命令列參數(<u>C</u>):				
▶ 將失敗計劃	财加到命	令列結尾(/fail	=%1 %)(E)		
			電新啓動的	避項(<u>R</u>)	
		確定	取消	套用	



1.4.2 Windows 2008 或之後版本作業系統

(1) 開啟 [Windows PowerShell]



(2) 重新啟動 NXLog 服務,檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

```
PS C:\> Restart-Service -Name nxlog

PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'

PS C:\> Restart-Service -Name nxlog

PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

Name Status StartType

nxlog Running Automatic

PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'

2022-03-08 16:43:19 INFO nxlog-ce-3.0.2272 started

PS C:\> ______
```

本文件範例是 NXLog 64bit 版本,若是 NXLog 32bit 版本,紅色文字部位請改以下設定 'C:\Program Files

(x86)\nxlog\conf\nxlog.conf'

(3) 開啟 [服務] 功能





(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 🗐 點選 [內容]

🔍 服務					_		×
檔案(F) 動作(A) 檢視(V) 說明(⊦	Ð						
🗢 🔿 🖬 🖬 🖬 🖬 🖬	▶ ■ H IÞ						
服務 (本機) 内容							
NXLog	名稱 ^	描述	狀態	啟動類型	登入身分		^
107 - L 273 304	🌼 Network Location Awareness	收集及儲存	執行中	自動	Network S	Service	
<u>行止</u> 服務 重新動動服務	🏟 Network Setup Service	「網路設定		手動 (觸發程	Local Syst	em	
<u>10X 201</u> 0X 379	Ketwork Store Interface Service	此服務可將	執行中	自動	Local Serv	/ice	_
	🖏 NXLog	This service	執行中	自動 (延遲啟動)	Local Syst	em	
描述:	Straine Files	離線檔案服		已停用	Local Syst	em	_
running the NXL og agent. See	OpenSSH Authentication Agent	Agent to h		已停用	Local Syst	em	
www.nxlog.co.	Optimize drives	可最佳化存		手動	Local Syst	em	~
延伸 (標準/							

(5) [一般] 頁面 -> 確認; 啟動類型: [自動 (延遲啟動)]

NXLog 内] 容 (本機	電腦)					×
一般	登入	復原	相依性				
服務名	稱:	nxlo	9				
顯示名	稱:	NXL	.og				
描述:		This age	service is nt. See wy	responsibl vw.nxlog.c	e for running o.	the NXLog	~ ~
可執行 "C:\Pro	檔所在路 ogram Fi	徑 iles\nxlo	g\nxlog.ex	(e" -c "C:\F	Program Files	\nxlog\conf	\nxlog
啟動類	型(E):	自重	的(延遲啟動	1)			\sim
服務狀	態:	執行	¢				
100	(S)		停止(T)	ł	皆停(P)	繼續(F	۲)
您可以	在這裡指	定啟動服	務時所要套	医用的参數			
啟動參	數(M):	[
				確定	取消	Í	套用(A)



(6) [復原] 頁面 -> 確認; 第一次失敗時: 和第二次失敗時: 和後續失敗時: [重新啟動服務] -> 按 [確定]

NXLog 內容 (本機電腦)			×
一般 登入 復原 相依性	ŧ		
^選 取此服務失敗時的電腦回應。	協助我設定復原動作	8	
第一灾失敗時(F):	重新啟動服務		~
第二次失敗時(S):	重新啟動服務		~
後續失敗時(U):	重新啟動服務		~
經過下列天數後重設失敗計數(C)): 1	Æ	
經過下列時間後重新啟動服務(V): 1	分鐘	
□ 啟用對因錯誤而停止所採取的 □ 動行程式	句動作。	電腦重新啟動的調	崖項(R)
程式(P):			
]]寶[影	3)
命令列參數(C):			
□ 將失敗計數附加到命令列	結尾 (/fail=%1%)(E)		
	確定	取消	套用(A)



2 Windows 2000

Windows 稽核原則設定 詳細說明請參考**前言的**稽核原則建議連結 *以下分別為網域或工作群組設定方式。

2.1 網域

2.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





(3) 輸入組織單位名稱

輸入組織單位名稱:Servers <mark>註:請依客戶環境建立組織單位名稱</mark> -> 按 [確定]

新增物件 -	·組織單位				×
Ø	建立在:	npartner.local/			
名稱(A	J:				
Server	2				
					
				確定	

(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2000] 伺服器按滑鼠右鍵, 註:請依客戶環境選擇 Windows File 主機 -> 點選 [移





(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

- 🖓 npartner	n. 	
🗄 🦳 Builtin		
Computer Domain C	s ontrollers	
+ ForeignSe	curityPrincipals	
E Servers		

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 Win2000 File 伺服器已移動。

< Active Directory 使用者及電腦				- O ×
] 🌍 主控台(C) 視窗(W) 説明(Ð			_ 8 ×
」執行(▲) 檢視(型) ↓ 🗢 ⇒	🖻 💽 🗡 😭	' 🕑 🛛 😤 🗍 📆	📅 🖄 🖓 🍕	°C
樹狀目錄	Servers 1 個物件			
Active Directory 使用者及電腦	名稱	類型	描述	
Image: Servers Image: S	, ₩IN2000	電腦		



2.1.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 在 Servers 組織單位,點選內容

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [內容]





(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]

		?)
一般 管理者	¥ 群組原則	
Ser Ser	vers 目前的群組原則物件影	連結
群組原則物例	牛連結	不覆蓋 已停用
在清單中排較 此清單來自於	前面的群組原則物件的順 : WinAD2000 neartner local	序也居優先地位。
	1 +r/1-2 m 1 (6+1	
新物件(N)	新增(D) 編輯	(E) 向上(U)
新物件创 選項(<u>O</u>)	新增(1) … 編輯 移除(1)… 内容	(E) 向上(U) (P) 向下(W)
新物件(N) 選項(0)	新增(D) 編輯 移除(D) 內容	(四) 向上(四) (四) 向下(四)
新物件(M) 選項(②)…	新增(型)	他 作上の 「作」



(4) 編輯群組原則物件

輸入群組原則物件名稱:N-Partner Policy 註:請依客戶環境建立群組物件名稱 -> 按 [編輯]

Servers內容		? ×
一般 管理者 群組原則		
Servers 目前的群組原則物件連結		
群組原則物件連結	不覆蓋	已停用
N-Partner Policy		
在清單中排較前面的群組原則物件的順序也則 此清單來自於: WinAD2000.npartner.local	舌優先地位。	
新物件(N) 新增(D) 編輯(E)		向上(m)
選項(0) 移除(T) 内容(P)	4 —	向下(W)
□ 阻礙原則繼承(B)		
	Terite 1	本田(小)
19#J Fr]	4.2.7月	安用(图)



(5) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定值:] & [成功] & [失敗] -> 按 [確定]





(6) 事件記錄檔:安全性記錄保持方法

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件日誌] -> [事件日誌檔設定值] -> 點選 [安全性記錄保持方法] -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]





(7) 事件記錄檔:安全性記錄檔最大值

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件日誌] -> [事件日誌檔設定值] -> 點選 [安全性記錄檔最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]

雪 群組原則			-OX
」執行(▲) 檢視(♥) ↓ ← → 1 € 📭	🗙 🖪 🔮		
樹狀目錄	原則 🔺	電腦設定	
N-Partner Policy (Win&D2000 npartner locs	188 安全性記錄保持天數	尚未定義	
	器安全性記錄保持方法	視雲要而定	-
	間安全性記錄檔最大值	204800 KB	
白 📄 Windows 設定	<mark>跑</mark> 安全性稽核記錄檔已滿時關閉系統	尚未定義	
	醫系統記錄保持天數	尚未定義	
🖻 📑 安全性設定	醫系統記錄保持方法	尚未定義	
□ 變 帳戶原則	醫系統記錄檔最大值	尚未定義	
田 愛 本機原則	設限制來賓存取安全性記錄檔	尚未定義	
	設限制來賓存取系統記錄檔	尚未定義	
田····································	設限制來賓存取應用程式記錄檔	尚未定義	
	證應用程式記錄保持天數	尚未定義	
	100 應用程式記錄保持方法	尚未定義	
日 日 立环	證應用程式記錄檔最大值	尚未定義	
王 🔍 Active Directory上的 IP 妄	安全性原則設定		<u>?×</u>
 田● 系統管理範本 □● ● 使用者設定 □● ● 軟錬設定 	安全性記錄檔最大值		
田··□ Windows設定 田··□ 系統管理範本	▶ 定義這個原則設定(D)		
	204800 🕂 KB		
			取消
	J		

(8) 在 Windows File 伺服器,開啟 [命令提示字元]



(9) 更新群組原則

C: <> secedit /refreshpolicy machine_policy /enforce



2.2 工作群組

2.2.1 稽核原則設定

(1) 開啟搜尋



(2) 搜尋群組原則物件編輯器

輸入 gpedit.msc -> 按 [立即搜尋] -> 點選 [gpedit]





(3) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]

執行(山) 檢視(型) ◆ → • • ●
樹狀目錄 原則 △ 本機設定 有效的設定 ●
 ▲機電腦原則 ● 圖 電腦設定 ● 圖 整整定 ● 圖 整整定 ● 圖 指令檔 - (啓動,關機) ● 圖 安全性設定 ● 圖 安全性設定 ● 圖 中原原則 ● 圖 本機原則 ● 圖 本機原則 ● 圖 軟皮原則
 ● 個板原則 ● ● 公開全幅原指 ● ● 公開金編原則 ● ● 公開金編原則 ● ● 公開金編原則 ● ● 本機電腦上的 IP5 ● ● 素統管理範本 ● ● 軟體設定 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●

(4) 開啟 [命令提示字元]



(5) 更新群組原則

 $\texttt{C:} \verb> secedit / refreshpolicy machine_policy / enforce$



N-Partner

Copyright © All rights a

2.2.2 事件檔案設定

(1) 開啟事件檢視器

按[開始]-> 點選[系統管理工具]->[事件檢視器]

		🧃 [設定您的伺服器] 精靈
		🎒 元件服務
		🄓 分散式檔案系統
		🗊 本機安全性原則
		📑 事件檢視器
		🖏 服務
		🗑 效能
		資 授權
		诊 終端機伺服器授權
		🖳 終端機服務設定
		診 終端機服務管理員
		🗃 資料來源 (ODBC)
		🧕 路由及遠端存取
Administrator		💻 電腦管理
\sim	244	🧊 管理您的伺服器
1 管理您的伺服器		🧔 網路負載平衡管理員
~	按制台(C) ▶	🕝 遠端桌面
💢 ₩indows 檔案總管		题 憑證授權單位
	🍿 系統管理工具 🔹 🕨	晶 叢集系統管理員
CA 命令提示字元	印表機和傳真	
111 記事本	(2) 説明及支援(出)	
	▶ 孫幸(四)	
	? 執行(R)	
	一 執行 (R) ⑦ Windows 安全性(W)	
	?=? 執行 ℝ) ⑦ Windows 安全性(W)	
	?=? 執行(ℝ) ?=? 執行(ℝ) ?=? ₩indows安全性(₩)	
	?□ 執行 (R) ⑦ Windows 安全性(W)	
	⑦ 執行 (R) ⑦ Windows 安全性(W)	
	?=? 執行 (ℝ) ?=? 執行 (ℝ) ?=? ₩indows 安全性(₩)	
	⑦ 執行 (R) ⑦ Windows 安全性(W) ⑧ Windows 安全性(W) ◎ Windows 安全性(W)	



(2) 編輯安全性記錄

在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB <mark>註:請依客戶環境調整</mark> -> 點選 [視需要覆寫事件] -> 按 [確定]

安全性記錄檔 內容		<u>?</u> ×
一般 篩選		
顯示名稱(D):	安全性記錄檔	-
記錄檔名稱(L):	C:\WINNT\System32\config\SecEvent.Evt	-
大小:	64.0 KB (65,536 位元組)	
建立日期:	2021年6月25日 上午 11:02:38	
修改日期:	2021年6月25日 上午 11:22:59	
存取日期:	2021年6月25日 上午 11:22:59	
┌記錄檔大小―		
最大記錄檔大	:小(M): 204800 II KB	
當達到記錄檔	大小的最大值時:	
○ 視需要覆:	寫事件(0)	
○ 覆寫(型)	7 📑 天前發生的事件	
○ 不覆寫事((手動清除)	牛(N) 記録檔) 還原預設値(R)	1
□ 使用低速連絡	泉(₩) - - - - - - - - - -	0
	確定 取消 套用	(A)



2.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]





(2) 點選 [安全] 頁面 -> 按 [進階]

tmp 內容	<u>? ×</u>
一般 共用 安全	
名稱	新增①
🚮 Everyone	
	(<u>K</u>)
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	
[]	
 ✓ 允許來自父項的可繼承權限で ✓ ↔ 	可以傳播至此物件(出)
確定	取消 套用(<u>(</u>))

(3) 點選 [稽核] 頁面 -> 按 [新增]

tmp 的存取設定控 權限 權限	制 擁有者			<u>?</u> ×
稽核項目(工):	\$3T	左兩	本田	
	199	1748	2471	
 「新増型」 「○ 九許來自父」 「□ 重新設定所³ 	小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小小	依視/編輯(♡) 以傳播至此物件(目,並使傳播可 # 可 #	 且) 繼承稽核項目發生	
└── 作用 (S)				
		確定	取消	套用(盘)



(4) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [確定]

📲 選擇 使用者 或 群組			<u>? ×</u>
查詢①: 🧾 WIN2000			~
名稱	資料夾名稱		
1 Everyone			
Authenticated Users			
TANONYMOUS LOGON			
CREATOR OWNER			-
名稱(N) Everyone			
		(確定)	

(5) 勾選所有項目存取 [成功] 和 [失敗] -> 按 [確定]

tmp 的稽核項目			<u>?</u> ×
物件			
名稱: Everyone		變更(C)
套用在(Q): 這個資料夾,子資料夾及	檔案		•
存取⑤:	成功	失敗	
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 讀取使用權限 變更使用權限	<u> </u>	<u> </u>	
□ 套用這些稽核項目到此容器中的物件 /或容器(I)	+及	<u> </u>	B(L)
	確定	D B	刘


(6) 稽核項目顯示 Everyone 名稱 -> 按 [確定]

tmp 的存取設定控制		<u>? ×</u>
權限 稽核 擁有者		
稽核項目(<u>T</u>):		
類型 名稱	存取	套用
🛃 全部 Everyone	完全控制	這個資料夾,子資料夾及
新增① 移除®)	檢視/編輯(♡).	
直接在此物件上定義此稽核項目。	子項物件繼承此稽	核項目。
✓ 九許來自父項的可繼承稽核項目可 重新設定所有子項物件上的稽核功 作用③	可以傳播至此物件 頁目,並使傳播可:	田) 繼承稽核項目發生
	確定	取消 套用(鱼)

(7) 按[確定]

tmp内容	? ×
一般 共用 安全	
名稱 Ø Everyone	新增① 移除(R)
, 權限(P):	允許 拒絕
完全控制 修改 讀取及執行	
進階(型) ✓ 九許來自父項的可繼承權限可以傳述	番至此物件(出)
確定	取消



3 Windows 2003

Windows 稽核原則設定 詳細說明請參考**前言的**稽核原則建議連結 *以下分別為網域或工作群組設定方式。

3.1 網域

3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





(3) 輸入組織單位名稱

輸入組織單位名稱:Servers <mark>註:請依客戶環境建立組織單位名稱</mark> -> 按 [確定]

新增物件	- 組織軍位		×
3	建立在:	npartner.local/	
名稱(A	υ:		
Server	8		
		確定	取消

(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2003] 伺服器按滑鼠右鍵<mark>, 註:請依客戶環境選擇 Windows File 主機</mark> -> 點選 [移





(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動 ? 🗙
將物件移動到容器(M):
🖃 🗊 npartner
⊕ Builtan ⊕ — — Computers
Domain Controllers
ForeignSecurityPrincipals ForeignSecurityPrincipals Servers
確定 取消

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 Win2003 File 伺服器已移動。





3.1.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 在 Servers 組織單位,點選內容

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [內容]





(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]

Servers 內容	? ×
一般 管理者 COM+ 群組原則	
Servers 目前的群組原則物件連結	ī
群組原則物件連結	不可強制 已停用
	的原生顺度。
此清單來自於: win2003.npartner.local	1月71英7日4月/子。
新物件M 新增D 編輯(E)	上移(四)
選項(Q) 移除(I) 內容(I)	下移(四)
小安滬水県則(<u>B</u>)	
確定	取消



(4) 編輯群組原則物件

輸入群組原則物件名稱:N-Partner Policy 註:請依客戶環境建立群組物件名稱 -> 按 [編輯]

Servers 內容 ? 🗙
一般 管理者 COM+ 群組原則
Servers 目前的群組原則物件連結
群組原則物件連結 不可強制 已停用
N-Partner Policy
在清單中排在前面的群組原則物件擁有較高的優先順序。 此清單來自於: win2003.npartner.local
新物件(N) 新增(D) 【 編輯(E) 】 上移(D)
選項(0) 移除(1) 内容(2) 下移(2)
□ 不要繼承原則(B)
開閉 取消 套用(<u>A</u>)



(5) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定值] & [成功] & [失敗] -> 按 [確定]





(6) 事件記錄檔:安全性記錄保持方法

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄保持方法] -> 勾選 [定義這個原則設 定] -> 點選 [視需要覆寫事件] -> 按 [確定]





(7) 事件記錄檔:安全性記錄檔最大值

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原 則設定] -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]





(8) 在 Windows File 伺服器, 開啟 [命令提示字元]



(9) 更新群組原則





(10) 查看群組原則套用情形

C:\> gpresult /v

📧 命令提示字元		IX
C:∖>gpresult ∕v		1
Microsoft (R) Windows (R) Op Copyright (C) Microsoft Corp	erating System Group Policy Result tool v2.0 . 1981-2001	
建立於 2021/6/25 上午 09:54:	96	
WIN2003 Administrator 前 RSO 	P 資料在 WIN2003: 記錄模式	
os 類型: os 設定: os 版本: 終端微伺服器模式: 站台名稱: 漫遊設定檔: 本機設定檔: 用低速連結來連線?:	Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition 成員伺服器 5.2.3790 遠端系統管理 Default-First-Site-Name C:\Documents and Settings\Administrator 否	
電腦設定		
CN=WIN2003,OU=Servers,DC 上次套用的群組原則: 套用的群組原則來自: 群組原則低速連結關値: 網域名稱: 網域類型:	=npartner,DC=local 2021/6/25 於 上午 09:51:33 Win2003AD.npartner.local 500 kbps npartner Windows 2000	
已套用的群組原則物件		
N-Partner Policy Default Domain Polic	y	-
•		• //



3.2 工作群組

3.2.1 稽核原則設定

(1) 開啟搜尋

按[開始] -> 點選[搜尋]





(2) 搜尋群組原則物件編輯器

輸入 gpedit.msc -> 按 [搜尋] -> 點選 [gpedit.msc]





(3) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]





(4) 開啟 [命令提示字元]



(5) 更新群組原則





3.2.2 事件檔案設定

(1) 開啟事件檢視器

按[開始] -> 點選 [系統管理工具] -> [事件檢視器]

		3	[設定您的伺服器] 精靈
		۹	元件服務
		Ŀ	分散式檔案系統
		ø	本機安全性原則
		4	事件檢視器
		*	服務
		۱ ۱	效能
		1	没曜
			彩晰俄间版器按催
		-32. BUD	\$25年11月11日3月1日日 9月1日3月1日日日日
			彩炳俄服初官理員 溶料本酒(ODDC)
		er The	資料來源 (ODBC) 影由我遠端友販
Administrator		2	雷腦管理
, 10/2/2/0[10[0]			管理您的伺服器
🧊 管理您的伺服器	😡 我的電腦	a	網路負載平衡管理員
		ā	遠端桌面
妏 Windows 檔案總管	▶ 控制台(C)		憑證授權單位
	🍿 系統管理工具 🔹 🕨	5	叢集系統管理員
CA 命令提示字元	실 印表機和傳真		
***	(1) 説明及支援(出)		
1044 1044			
	▶~ (送录 (2)		
	(R)		
	😚 Windows安全性(W)		
所有程式(₽) ▶			
	💋 登出(L) 🚺 關機(U)		
29開始 🥭 😥			



(2) 編輯安全性記錄

在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB <mark>註:請依客戶環境調整</mark> -> 點選 [視需要覆寫事件] -> 按 [確定]

安全性記錄檔 內容		? ×
一般 篩選		
顯示名稱(D):	安全性記錄檔	
記錄檔名稱(正):	C:\WINNT\System32\config\SecEvent.Evt	
大小: 建立日期: 修改日期:	64.0 KB (65,536 位元組) 2021年6月25日 上午 11:02:38 2021年6月25日 上午 11:22:59 2021年6月25日 上午 11:22:59	
存取日期:	2021年6月25日 上午 11:22:59	
最大記錄檔大 當達到記錄檔	:小(<u>M</u>): 204800 子 KB 计小的最大值時:	
 ○ 視需要覆: ○ 覆寫(型) ○ 不覆寫事(手動清除) 	寫事件(型) 7 → 天前發生的事件 件(N) 還原預設値(R)	1
□ 使用低速速約		<u></u>
	確定 取消 套用(A)



3.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]





(2) 點選 [安全性] 頁面 -> 按 [進階]

1500 内容			? ×
一般 【共用	安全性 白計		
群組或使用者名	5稱(G):		
🚮 Administrat	tors (WIN2003\Ad	lministrators)	
CREATOR	OWNER		
SYSTEM			
🚮 Users (WIN	(2003\Users)		
2	,		
		新增①	移除(<u>R</u>)
Administrators É	り權限(P)	允許	拒絕
完全控制		>	
修改		4	
讀取及執行		~	
清單資料夾的	内容	1	
讀取		4	
寫入		\checkmark	
		. 6	
符/木催胶乳/進降	首記文·E:論t女 [J進P首	j.	進階(♡)
	確定	取消	套用(A)

(3) 點選 [稽核] 頁面 -> 按 [新增]

tmp 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稽核項目的習	資訊 ,選擇一個 稽核	項目,然後按	[編輯]。		
藉核項目(T)·					
類型 名稱	存取	繼承自	套用到		
	1	1			
新增①	移除(B)	J			
▶ 九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	用確定義於此的	項目(A)	
[] 以顯示於此套用到子物件的項目	,	生上的糖核項目	1(P)		
			-w		
了解具他有腳 <u>稽核</u> 。					
		確定	取消	 套用(A)	



(4) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

選擇 使用者 或 群組	? ×
選擇這個物件類型(2):	
使用者、群組 或 内建安全性原則	物件類型(0)
從這個位置(1):	
WIN2003	位置(止)
請輸入物件名稱來選取 (範例)(E):	
<u>Everyone</u>	檢查名稱(C)

(5) 存取類型 [成功] 和 [失敗] 項目都勾選 [完全控制] -> 按 [確定]

tmp 的稽核項目		?	×
物件			
			Т
名稱(N): Everyone		變更(C)	
套用在(0): 這個資料來,子資料本	丙檔案	•	
The Present of Arts	-the later	# 8h	
仔収(2):	展功	失敗	
完全控制	\checkmark		
周遊資料夾樹行檔案	\checkmark		
列出資料夾牘取資料	\checkmark		
讀取屬性	\checkmark		
遭取擴充屬性	\checkmark		
建立檔案/寫入資料	\checkmark		
建立資料夾附加資料	\checkmark		
[[[[]] []] [] [] [] [] [] [$\mathbf{\nabla}$		
易人擴充團性			
調査者が推定			
🗖 這些稽核項目只套用到這個容器	骨中的	全部清除(L)	
·□ 物件及 (或) 容器 (I)			
_		Tree of the	
	11111111111111111111111111111111111111	型	



(6) 稽核項目顯示 Everyone 名稱 -> 按 [確定]

tmp 的進	階安全的	生設定							? ×
權限	稽核	擁有者	有效權限						
若要械	祝其他 ⁷	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	■月(T):								
類型	· · · · ·	名稱		存取	:	繼承自	套	用到	
成功	I	Everyone		完全控制		<非繼承的>	這	個資料來	を'子
新	増①	編	輯(E)	移除(<u>R</u>)) [
	连洲公馆	# 承诺枝(百日本田列	- ≘個咖啡(±≨⊓66%	EénZ:	物件,句好吗	旧破完美的	经邮款值	iB(4)
J♥ 76i	511/C/X-9	₹# 2 /₽\16'0X'3	ㅋㅋ★/ハンレ		1 1 1 1	1017 - 1019	734EAC3%/	N 1464 3494	(HQ)
口以	顧示於此	法 用到子特	物件的項目	,替代所有子巧	質物件.	上的稽核項目	∃@		
了解其	他有關	膳核。							
					Г	確定	取消	肖	套用(A)

(7) 按[確定]

tmp 內容			? ×
一般 共用 安全性	自訂	1	
Administrators (WIN20	003\Adı	ministrators)	
CREATOR OWNER			
SYSTEM			
🚮 Users (WIN2003\Users	s)		
		******** 1	1000 00 1
		新增(<u>D</u>)	
Administrators 的權限(P)		允許	拒絕
完全控制		×	
修改		\checkmark	
讀取及執行		\checkmark	
信単貞科外(り谷) 清取		~	
寫入		×	
4年5生 4500月			
特殊權限或進階設定諸按	[進階]	۰	進階(🖤)
			1
確	淀		套用(A)



4 Windows 2008

Windows 稽核原則設定 詳細說明請參考前言的稽核原則建議連結 *以下分別為網域或工作群組設定方式。

4.1 網域

4.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





(3) 輸入組織單位名稱

輸入組織單位名稱:Servers 註:請依客戶環境建立組織單位名稱 -> 按 [確定]

新增物件 - 組鐵單位	×
with a second s	
名稱(A):	
Servers	7
✓ 保護容器以防止被意外刪除(P)	-
	說明

(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2008] 伺服器按滑鼠右鍵, 註:請依客戶環境選擇 Windows File 主機 -> 點選 [移 動]

📴 Active Directory 使用者和電	5		_ 🗆 X
檔案(F) 執行(A) 檢視(V) 說明	明(H)		
🗢 🔿 🖄 📅 🖌 🚺 🗙	i 🖬 🖸	🛿 🖬 浅 🗽 🛅	7 🗾 🍇
🔁 Active Directory 使用者和電腦 [名稱	類型	描述
田 🧾 儲存查詢	WIN2008	電腦	
🖃 🏬 npartner.local		加入群組中(G)	
+ Builtin		重設帳戶(A)	
the Domain Controllers		移動(V)	
ForeignSecurityPrincipals	1	管理(M)	
Managed Service Account Users		所有工作(K) ▶	
Servers		剪下(I)	
		刪除(D)	
		内容(R)	
		說明(H)	
▲	•		►
將目前的選取項目移動到另一個組織	單位。		



(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	×
將物件移動到容器(M):	
Image: Servers Managed Service Accounts Servers July Servers	
確定 取消	

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 Win2008 File 伺服器已移動。





4.1.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位,新增群組原則物件

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]





(3) 輸入群組原則物件名稱

輸入群組原則物件名稱:N-Partner Policy<mark>註:請依客戶環境建立群組物件名稱</mark> -> 按 [確定]

新増 GPO		×
_名稱(N):		
N-Partner Policy		
來源入門 GPO ③:		
(無)		•
	確定	取消

(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件按滑鼠右鍵 -> 點選 [編輯]





(5) 本機原則:稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳 戶登入事件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按 [確定]





(6) 事件記錄檔:安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定 義這個原則設定] -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]





(7) 事件記錄檔:安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔保持方法] -> 勾選 [定義 這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]





(8) 在 Windows File 伺服器 -> 開啟 [Windows PowerShell]



(9) 更新群組原則

PS C:\> gpupdate /force



(10) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell] -> 產生 Windows File 伺服器群組原則報表



紅色文字部位請輸入 Windows File 伺服器名稱和資料夾路徑檔案名稱



(11) 開啟報表,確認 Windows File 伺服器, 套用 N-Partner Policy 群組原則

🏉 NPAR TNE	R\WIN2008 - Windows Inte	rnet Explorer		_ 🗆 ×
	C:\tmp\Win2008.html	🔹 😽 🗙 🔥 Bing		ρ-
			1	
💢 4%DJH235	E NPAR INER/WIN2008			
		群組原則結果		<u>F</u>
NPARTNE	R\WIN2008			
資料収集:202	23/15 下午 04:22:27			<u>到不全静</u> 图示
香糯湯定				
EBI				E ALZER
JKRI	进 合			<u>53.995</u>
W1hdows	款 走			
安全性	裁定			記載
帳戶	原則「密碼規則			翻示
帳戶	原則小帳戶鎖定原則			翻示
帳戶」	原則/Kerberos 原則			翻示
本機	原則/楷核原則			隠藏
	原則	設定	優勢 GPO	
	稽核物件存取	成功,失敗	N-Partner Policy	
	褡核帳戶登入事件	成功,失敗	N-Partner Policy	
	稽核登入事件	成功,失敗	N-Partner Policy	
本禮	原則/使用者權限指派			翻示
本機	原則安全性運填			翻示
事件	記錄檔			隠藏
	原則	設定	優勢 GPO	
	安全性記錄檔保持方法	視需要而定	N-Partner Policy	
	安全性記錄檔容量最大值	204800 KB	N-Partner Policy	
公開	金銷原則/進證服務用戶端 - 自	動註冊設定		顯示
公開	金銷原則/加密檔案系統			顯示
公開	金鑰原則/被信任的根憑證授權	軍位		顯示
使用者設定				顯示
				v
		▶ 電腦 受保護模式: 關閉	<u>√</u>	🔍 100% 🝷 🏿



4.2 工作群組

4.2.1 稽核原則設定

(1) 開啟 [本機群組原則編輯器]

點選 [開始] -> 在 [搜尋] 欄位,輸入 group policy -> 點選 [編輯群組原則]

控制台 (1)
🝓 編輯群組原則
♀ 查看更多結果
group policy 登出 🕨



(2) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]





(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

PS C:\> gpupdate /force





(5) 查看群組原則套用情形

PS C:\> auditpol /get /category:*

🔎 Administrator: Windows PowerShell		_ 🗆 🗙
PS C:>> auditpol /get /category:*		▲
系統稽核原則 類別/子類別 金佐	設定	
系統 安全性系統延伸 多統宗整性	沒有稽核 成功及失敗	
IPSEC driver	沒有稽核	
其他系統事件	成功及失敗	
安全性狀態變更	成功	
「豆八/豆山 啓入	成功及失敗	
臺出	成功反失敗	
帳戶鎖定	成功及失敗	
IPsec 主要模式 IPsec 地球模式	成功及失敗	
IPsec 研佛模式	成功及天敗 成功及失敗	
特殊登入	成功发兵殿	
其他登入了登出事件	成功及失敗	
網路原則伺服器	成功及失敗	
檔案系統	成功及失敗	
registry	成功及失敗	
核心物件	成功及失敗	
SAM 2團 3歲 附基盤	成切及失敗	
產生的應用程式	成功及失敗	
控制代碼操縱	成功及美殿~	
檔案共用	成功及失敗	
師選半台封包云業 疑選或会連續	成切及失敗 成份及失敗	
即进丁日25% 其他物件存取事件	成功及关照 成功及失敗	
詳細檔案共用	成功及失敗	
特殊權限使用	مغنان فالمركز مراجع مراجع	
- 「「「「「「」」 	没有稽核	
其他特殊權限使用事件	2月1113	
詳細這聽		
終止處理程序 PRAN 活動	没有稽核	
BPR 事件	沒有稜核	
建立處理程序	沒有稽核	
原則變更且以過	-0-0	
稽核原則變更 醫迹度10%更	成功	
「「「「「「「「「「」」」を見ていていていていていた。	沒有證核	
MPSSUC 規則層級原則變更	17後昇稽核	
靜選平台原則變更	沒有稽核	
- 其他原則變更爭忤 雌戶勞堋	没有稽核	
使用者帳戶管理	成功	
電腦帳戶管理	成功	
安全性群組管理	成功	
酸甲酰胆管理	沒有稽懷 沒有稽絃	
其他帳戶管理事件	沒有稽核	
DS 存取) for almost the first	
目球服務要更	沒有稽核 沒有譯校	
首約6000010000 詳細目錄服務視寫	沒有稽核	
目錄服務存取	成功	
帳戶登入 四次一次 四次	and the state of the	
Kerberos 服務票證操作 其他能后登入軍化	成功及失敗	
Kerberos 驗證服務	成功及失敗	
認證驗證	成功及失敗	
PS C:\>		•
	1	- 14


4.2.2 事件檔案設定

(1) 開啟事件檢視器

按[開始] -> 點選 [系統管理工具] -> [事件檢視器]





(2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]





(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註:請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 ()	頬型: 糸繽管理)	×				
一般						
全名(F):	Security					
記錄欄路徑(L):	%SystemRoot%\System32\Winevt\Logs\Security.evtx					
記錄欄大小:	3錄欄大小: 4.07 MB(4,263,936 位元組)					
建立日期:	2021年6月21日下午 09:05:32					
修改日期:	2021年6月21日下午 05:33:07					
存取日期:	2021年6月21日下午 09:05:32					
 ▶ 飲用記錄(E) 最大記錄檔大小() 當事件記錄檔的大 ● 視需要覆寫 ● 富記錄檔E ● 不要覆寫事 	KB)(Q): 204800 - (小到達上限時: 書事件 (先覆寫最酱的事件)(W) 認滿時進行封存,不要覆寫事件(A) 副件 (手動清除記錄欄)(N) 清除記錄欄(R)					
	確定 取消 套用(P)					



4.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]





(2) 點選 [安全性] 頁面 -> 按 [進階]

📕 tmp - 内容				×
一般 共用	安全性以前的	版本 自訂		
物件名稱: (C:\tmp			
群組或使用者名	稱(G):			
& CREATOR	OWNER			-
& SYSTEM				
🧟 Administrato	rs (WIN2008\Adm	inistrators)		
Sers (WIN2	(008\Users)			
, 若要變更權限,	請按一下[編輯]	•	编輯(E)	11
				-
CREATOR OWN	ER 的權限(P)	允許	拒絕	_
完全控制				▲
修改				
讀取和執行				
列出資料夾內	容			
讀取				
寫入				<u> </u>
如需特殊權限或	進階設定,請按-	一下 [進階]・	。 ‴進階(♥)	
			<u> </u>	-
深入了解存取控	制及權限			
	確定			ŝ)

(3) 點選 [稽核] 頁面 -> 按 [新增]

🔒 tmp ff	的進階安	全性設定			Đ
權限	稽核	擁有者 有效權限			
若要被	_使 視櫂限I	 頁目的詳細資料,請按兩下	項目。若要修改權限,	請按一下 [變更權限]。	
物件名	3稱:	C:\tmp			
稽核項	頁目(T):				
類型		名稱	存取	繼承自	套用到
i	輯(E)				
区從	此物件的	1父項包括繼承稽核項目(1)			
稽核物	的件存取的	的需求為何?			
				確定	取消



(4) 按[新增]

🔓 tanp 的進階安	全性設定				×
稽核					
若要檢視或編	輯藉核項目的詳細資料,諸	湿取該項目,再按一下	(信報]。		
			[Lange and]		
物件名稱:	C:\tmp				
稽核項目(T):					
類型	名稱	存取	繼承自	套用到	
新增(D)	編輯(E)	移除(R)			
▶ 従此物件的	的父項包括繼承稽核項目(1)				
□ 以此物件的	的繼承藉核項目取代所有子類	条現有的繼承稽核項目	(P)		
藉核物件存取	的需求為何?				
				Brold a	5HT/A3
			11世化	取)月 (5	5月1(年)

(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

選取使用者或群組	? X
選取這個物件類型(S):	
使用者、群組或內建安全性主體	物件類型(O)
從這個位置(F):	
WIN2008	位置(L)
請輸入物件名稱來選取 (範例)(E):	
Everyone	檢查名稱(C)
進階(A)	確 定 取消



(6) 存取類型 [成功] 和 [失敗] 項目都勾選 [完全控制] -> 按 [確定]

🕌 tmp 的稽核項目		×
物件		
名稱(N): Everyone		變更(<u>C</u>)
套用在(0): 這個資料夾、子資料		•
存取(3):	成功	
完全控制	N	
周遊資料夾/執行檔案 列出資料夾/積取資料 請取屬性 請取擴充屬性 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	ব য য য য য য য য	
刪除		☑ -
□ 僅套用這些稽核項目到此容器 及(或)容器(I) 管理稽核	中的物件	全部清除①
	確定	取消

(7) 稽核項目顯示 Everyone 名稱 -> 按 [確定]

📗 tanp 的進階	安全性設定				×
稽核					
若要檢視或	编輯稽核項目的詳細資料	,請選取該項目,再接	〒[編輯]。		[
物件力程。	Cábur				
101十百件:	C:ump				
稽核相日(1) 精制	1: 22:142	方面	例必白	本田刻	
全部	Everyone	完全控制		這個資料夾、	子資
新增(D)	編輯(E)	移除(R)			
豆 没能物的	的公面勾托供承接故障日	a.			
✓ 1040100H	的继承藉核項日散代所有	ョ(!) [子多現有的繼承競校]	項日(P)		
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	жнү/		
<u> </u>	取的需求為何?				
			[1	
			確定		套用(A)



(8) 稽核項目顯示 Everyone 名稱 -> 按 [確定]

🔰 taop fé	進階安	全性設定				×
權限	稽核	擁有者 有效權限				
若要檢	視權限以	頁目的詳細資料,請按兩下	項目。若要修改權限,	,請按一下 [變更權限]	•	
物件名	稱:	C:\tmp				
稽核項	目(T):					
類型		名稱	存取	繼承自	套用到	
全部		Everyone	完全控制	<非繼承的>	這個資料夾、子資	
緍	輯(E)					
▼ 従	北物件的	父項包括繼承稽核項目(1)				
種核物	件存取的	的需求為何?				
				確定	取消 套用(A)

(9) 按[確定]





5 Windows 2012

Windows 稽核原則設定 詳細說明請參考前言的稽核原則建議連結 *以下分別為網域或工作群組設定方式。

5.1 網域

5.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





(3) 輸入組織單位名稱

輸入組織單位名稱:Servers 註:請依客戶環境建立組織單位名稱 -> 按 [確定]

新增物件 - 組織單位	x
🥩 建立在: npartner.local/	
名稱(A):	
Servers ✔ 保護容器以防止被意外刪除(P)	
確定 取消 說明	1



(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2012] 伺服器按滑鼠右鍵, 註:請依客戶環境選擇 Windows File 主機 -> 點選 [移 動]





(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	x
將物件移動到容器(M):	
Inpartner Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Servers Users	
確定 取消	

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 Win2012 File 伺服器已移動。

Active Dir	rectory 使用者和電腦 🗕 🗖 🗙
檔案(F) 動作(A) 檢視(V) 說明((H)
🗢 🤿 🖄 🖬 🔏 🗎 🗙 🗎	i G 🗟 🛛 🖬 🗏 📚 🛅 🍸 💆 🍇
📔 Active Directory 使用者和電腦	名稱 類型 描述
▷ 🧰 儲存查詢	win2012 電腦
⊿ 🚔 npartner.local	
Builtin	
Computers	
Domain Controllers	
Þ PoreignSecurityPrincips	
Managed Service Acco	
C Users	
Servers	
<	< III >



5.1.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位,新增群組原則物件

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]





(3) 輸入群組原則物件名稱

輸入群組原則物件名稱:N-Partner Policy 註:請依客戶環境建立群組物件名稱 -> 按 [確定]

新増 GPO	x
名稱(<u>N</u>):	
N-Partner Policy	
來源入門 GPO(<u>S</u>):	
(無)	~
確定取消	

(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件按滑鼠右鍵 -> 點選 [編輯]

- 単純 - 単純	
🔜 檔案(F) 動作(A) 檢視(V) 視窗	i(W) 説明(H)
🗢 🔿 🗔 🞑 🖬	
 ■ 群組原則管理 ▲ ▲ 樹糸: npartner.local ▲ 鍋 網域 ▲ 鍋 網域 ▲ 鍋 npartner.local 圖 Default Domain Poli ▶ ⑥ Domain Controllers ▲ ⑧ Servers 	群組原則管理 內容 名稱 ▲樹系: npartner.local
 ▶ ■ ▶ ■ ↓ ■ ↓ ■ ↓ ■ ↓ 	 編輯(E) 登制(N) 啟用連結(L) 儲存報告(S) 從這裡開啟新視窗(W) 刪除(D) 重新命名(M) 重新整理(F) 說明(H)
開啟 GPO 編輯器	



(5) 本機原則:稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳 戶登入事件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]





(6) 事件記錄檔:安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]





(7) 事件記錄檔:安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] -> 勾選 [定 義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]





(8) 在 Windows File 伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Windows File 伺服器群組原則

PS C:\> Invoke-GPUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force



紅色文字部位請輸入 Windows File 伺服器名

(10) 產生 Windows File 伺服器群組原則報表

PS C: > Get-GPResultantSetofPolicy -Computer Win2012 -Path C: \tmp\Win2012.html -ReportType html



紅色文字部位請輸入 Windows File 伺服器名稱和資料夾路徑檔案名稱



(11)	開啟報表,	・確認 Windows	File 伺服器,	套用 N-Partner Policy	y 群組原則
------	-------	-------------	-----------	---------------------	--------

() <	\sim				- 🗆 X
群組原則結果 原元全部 NPARTNER\WIN2012 変好収集: 16/3/2022 15:36.42 重元全部 確果 重元 電素 重元 電素 重元 電素 重元 電素 重二 電素 重二 元件状患 重二 原料 重重 原料 重重 原料 重重 原料 重重 原料 重重 原料 重重 原料 重量 原料 重量 東土 重量 原料 重量 東全 重量 東全 重量 東全 重量 東全 重量 東全 重量 東市学 近点 東京県 成力: 失敗 小Partner Policy 単示 単件記録 重量 原料 設定 原料 設定 原料 設定 原料 設定 原料 設定 東利 </td <td>(🔶</td> <td>😑 🙋 C:\tmp\Win2012.html</td> <td>P - C Ø NPARTNER\WIN2012</td> <td>×</td> <td>🕀 🖈 🛱</td>	(🔶	😑 🙋 C:\tmp\Win2012.html	P - C Ø NPARTNER\WIN2012	×	🕀 🖈 🛱
NPARINER/WIN2012 副元 資料で美: 16/3/2022 15:36:42 副元 全 確実 電工 電気 電工 電気 電工 電気 電工 電気 電工 プ作状患 電工 設定 運営 原 電工 Windows 設定 運営 安全社設定 運営 健児専用/金環境別 電工 報告専規/金環境別 電工 報告専規/体目録主原則 電工 報告専規/体目録主原則 電工 報告専規/体目録主原則 電工 報告専規/体目録主原則 電工 解別 設定 優勢 GPO 個板市中市政 成功 失敗 N-Partner Policy 報気場用/線 電工 学社記書報告報 成功 失敗 東市 成功 失敗 東市 成功 失敗 アークはた時備を行方法 損害要而主 要社記書報書用 運工 要社記書報書用 運工 「日本 電量 原則 設定 原則 設定 原則 設定 受益 </td <td></td> <td></td> <td>群組原則結果</td> <td></td> <td></td>			群組原則結果		
	NPA	RTNER\WIN2012			
講要 磁元 電話 通磁 元件状態 磁元 次定 磁元 設定 磁型 取 磁型 文主性設定 運載 安土性設定 運載 東川(城戸原則/城戸原則/戦万間 運流 原則(城戸原則/城戸原則) 通元 「原則(城戸原則/城戸領定原則) 通元 「原則(城戸原則/城戸領定原則) 通二 「原則(城戸原則/城戸領定原則) 通二 「原則(城戸県町) 通二 「原則(城戸県町) 運流 「原則(城戸県町) 運流 「原則(城戸県町) 運流 「原則(城戸県町) 運流 「原則(城戸県町) 運流 「原則(城戸県町) 運流 「原則(水戸県市会社) 「原山 「夏川(秋戸県市会社) 「夏二 「夏川(小田舎田県市) 「夏二 「夏川(小田舎田県市) 「夏二 「夏川(小田舎田県市) 「夏二 「夏川(小田舎田県市) 「夏二 「夏川(小田舎田舎三人) 「夏二 「夏川(小田舎田舎三人) 「夏二 「夏川(小田舎田舎三人) 「夏二 「夏川(小田舎田舎三人) 「夏二 「夏川(小田舎田舎三人)	資料	②集: 16/3/2022 15:36:42			顧示全部
地震調査 反差 一般 局元 元件状態 局元 放定 反差 原則 反素 Vindows 設定 反差 安主社設定 反差 報戶原則/应環規則 最元 報戶原則/应環規則 最元 報戶原則/位月鎖定原則 最元 報戶原則/位月鎖定原則 最元 報戶原則/依行存取 成功 原則 設定 優勢 GPO 指抗向作存取 成功 火野 水母原則/使用者權限指派 超元 摩刑 設定 優勢 GPO 指抗協力 東加 原加 東利 設定 優勢 GPO 指抗協力、失敗 N-Partner Policy 福気物(作存取 成功、失敗 N-Partner Policy 常規環則/使用者權限指派 超元 厚利 設定 優勢 GPO 安全社記録幅 超量 原則 原利 設定 優勢 GPO 安全社記録報用 認定 重差 原利 設定 優勢 GPO 安全社記録幅 夏二 通流 成加 以用 要更而 <td>摘要</td> <td></td> <td></td> <td></td> <td>題示</td>	摘要				題示
一般 展元 元件状象 局元 反定 原規 原則 原規 Vindows 設定 原規 安主性設定 居蔵 総戶原則/密碼規則 副元 総戶原則/密碼規則 副元 総戶原則/密碼規則 國元 総戶原則/修行算定原則 副元 修序原則/使行算定原則 國元 修序原則/使行算定原則 國元 修用 設定 優勢 GPO 增務保存目、成功 ·失敗 N-Partner Policy 智気中行型 点型 國元 算用 設定 優勢 GPO 增務受力事件 成功 ·失敗 N-Partner Policy 常長型/使用者確限指派 国元 国元 厚則/安全性環境 回五 国元 厚規 設定 優勢 GPO 電気 学校記辞幅 成力 ·失敗 N-Partner Policy 回五 厚規 設定 優勢 GPO 受信 受信 原則 設定 優勢 GPO 交生性原則/使用者確認指示 国元 国元 愛生 原則 設定 優勢 成定 優勢 GPO <td>電腦詳</td> <td>細資料</td> <td></td> <td></td> <td>医藏</td>	電腦詳	細資料			医藏
元件状景 照元 設定 返盛 東川 振岡 受主性設定 返盛 健斤原則/毫視則 頭元 電子原則/毫視則 頭元 健斤原則/毫視則 頭元 健斤原則/毫視則 頭元 健原則/他白鑽定原則 頭元 健原則/他白鑽定原則 頭元 健原則/他白鑽定原則 國元 健原則/他白菊電原則/面積肥間法 四元 原則 設定 優勢 GPO 管務地合変 原則 設定 原則/使用着極間指述 四元 夏和 設定 優勢 GPO 空全紀記錄幅指述 圓元 夏素 原和 設定 原則 設定 優勢 GPO 安全記記錄幅 四元 夏素 原和 設定 原則 設定 優勢 GPO 安全記記錄幅用戶編 - 自動註冊設定 回五 公置金編原則/加密幅葉系統 回五 健康原則/加密幅葉系統 四五 健康原則/加密幅震系統 四五 健正論原則/加密幅震系統 回五 健正論原則/加密幅震系統 回五 原則 設定 優勢 GPO 交生記録解則/加密幅震系統 回五 「四五	一般				顯示
設定 短端 東川 短端 文全性設定 短端 成戶原則/或視則 頭示 帳戶原則/或得與則 頭示 帳戶原則/成戶損定原則 圓示 帳戶原則/低戶損定原則 圓示 報原則/個核原則 圓式 水間原則/低白白衣 成功,失敗 原則 設定 優勢 GPO 相核鳴戶容及 成功,失敗 N-Partner Policy 相核鳴戶容及半件 成功,失敗 N-Partner Policy 相核鳴戶容及半件 成功,失敗 N-Partner Policy 電気 一 一 東剛/使用者極限指派 圖云 - 東印記 一 一 東印記 一 - 東印記 一 - 東印 設定 優勢 GPO 安全性記錄個在時方法 現需要而定 N-Partner Policy 文全性記錄個在語方法 現需要而定 - 文生健原則/感識服務用戶編 - 自動註冊設定 - - 交生健原則/激音 四、 - - 「 - - - 「 - - - 「	元件	伏戁			顯示
原則 服素 Vindows 設定 温蒸 安全性設定 温蒸 电戶原則/或環規則 圓元 电戶原則/城戶鑽定原則 圓元 电戶原則/城戶鑽定原則 圓元 電原則/城存的空 原則 圓元 東則< 設定	設定				隱藏
Windows 設定 墜速 安全性設定 墜速 転戶原則/転戶鑽定原則 圓元 転戶原則/低戶領定原則 圓元 転戶原則/低戶領定原則 圓元 電原則/低枝原則 圓元 東則<酸皮	原則				<u> </u>
安全性設定 墜速 幅戶原則/磁戶鎖定原則 圓元 幅戶原則/低戶鎖定原則 圓元 電戶原則/低戶鎖定原則 圓元 本價原則/循核原則 圓元 本價原則/循核原則 圓元 原則 設定 優勢 GPO 瘤核肉件存取 成功 · 失取 N-Partner Policy 稽核風入事件 成功 · 失取 N-Partner Policy 楷核盈入事件 成功 · 失取 N-Partner Policy 常保原則/使用着報限指派 圓元 圓元 專作記錄幅 圖元 圓元 專作記錄幅 圓室 優勢 GPO 安全性記錄幅帶現方法 視需要而定 N-Partner Policy 文全性記錄幅音量最大值 204800 KB N-Partner Policy 公開金鑰原則/感證服務用戶編 - 自動註冊設定 圓元 圓元 發星範原則/加密檔案系統 圓元 圓元 好田原則物件 自動註冊設定 圓元 「好田原則物性 自動註冊設定 圓元 「快用 算評 圓元 「「「「」」」」 「	w	indows 設定			<u> </u>
帳戶原則/處碼規則 展示 帳戶原則/低戶鎖定原則 展示 唯戶原則/低reberos 原則 服示 本機原則/循核原則 感定 優勢 GPO 格成初 / 失取 N - Partner Policy 服示 脊機原則/使用者權限指派 原元 展示 季報原則/使用者權限指派 原示 原示 原則 設定 優勢 GPO 常在標原則/安全性媒項 成功 / 失取 N - Partner Policy 常作記錄幅 原記 慶潔 原則 設定 優勢 GPO 支生性記錄幅 原記 原記 原則 設定 優勢 GPO 安全性記錄幅 空話 原記 原則 設定 優勢 GPO 安全性記錄幅 空話 原記 原則 設定 優勢 GPO 安全性記錄幅要是未恆 204800 KB N - Partner Policy 安全性記錄幅意見 自動註冊設定 原面 公園金 原元 原元 公園金 原元 原元 校用 書類 原則 回動註冊設定 原面 校明 書面 通知 優 校問 書面 優 優		安全性設定			医藏
帳戶原則/幅戶鑽定原則 壁広 帳戶原則/Kerberos 原則 圓広 本暖原則/福枝原則 圓述 原則 設定 優勢 GPO 稽核物件存取 成功 · 失取 N-Partner Policy 稽核原則/使用者權限指派 圓元 季件記錄幅 圓元 摩則 設定 優勢 GPO * 福原則/使用者權限指派 圓元 季件記錄幅 圓元 摩則 設定 優勢 GPO 安全性認頻 圓元 摩 一日 一日 東市 「日 安全性認錄幅保損方法 提需要而定 N-Partner Policy 安全性記錄幅容量最大値 204800 KB N-Partner Policy 安全性記錄幅容量最大値 204800 KB N-Partner Policy 安全性記錄幅容量最大値 204800 KB N-Partner Policy 公園金鑰原則/加密檔案系統		帳戶原則/密碼規則			顯示
報戶原則/Kerberos 原則 國元 本銀原則/循核原則 協定 原則 設定 優勢 GPO 棺核物件存取 成功 · 失敗 N-Partner Policy 棺核噪戶登入事件 成功 · 失敗 N-Partner Policy 棺核噪戶國人學件 成功 · 失敗 N-Partner Policy 棺核量人事件 成功 · 失敗 N-Partner Policy 本銀原則/使用者繼限指派 國元 季件記錄幅 國定 季件記錄幅 國定 原則 設定 優勢 GPO 安全性記錄幅保指方注 視需要而定 N-Partner Policy 安全性記錄幅容量最大信 204800 KB N-Partner Policy 公園金鑰原則/應證服務用戶編 - 自動註冊設定 優款 國元 評組原則/加容檔案系统 國元 國元 評組原則/加容檔案系统 國元 國元 評組原則/加容檔案系统 國元 國元 評価 1000000000000000000000000000000000000		帳戶原則/帳戶鎖定原則			顯示
本職原則/補核原則 盛速 優勢 GPO 解則 設定 優勢 GPO 箱核物件存取 成功 · 失取 N - Partner Policy 福核電戶登入事件 成功 · 失取 N - Partner Policy 福核電戶登入事件 成功 · 失取 N - Partner Policy 春職原則/使用者權限指派 顧云 季報原則/使用者權限指派 顧云 季年記録檔 医室 季年記録檔 医之 慶則 設定 優勢 GPO 安全住記錄幅保持方法 視需要而定 N - Partner Policy 安全住記錄幅容量最大值 204800 KB N - Partner Policy 公開金鑰原則/憑證服務用戶媛 - 自動註冊設定 顧云 「和国原則/協證服務用戶媛 - 自動註冊設定 顧云 「和国原則物件 顧云 「和国原則物件 顧云 「秋田原則物件 顧云 「秋田原調資料 「國云 「秋田原調資料 「職元		帳戶原則/Kerberos 原則			顕示
原則 設定 優勢 GPO 箱核物件存取 成功 · 失敗 N-Partner Policy 箱核型入事件 成功 · 失敗 N-Partner Policy 福核型入事件 成功 · 失敗 N-Partner Policy 福核型入事件 成功 · 失敗 N-Partner Policy 福板原則/使用者權限指派 原工 國元 本標原則/使用者權限指派 夏之 優勢 GPO 李保原則/使用者權限指派 視察要而定 N-Partner Policy 安全性證錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金嶺原則/憑證服務用戶端 - 自動註冊設定 顧元 解组系列物件 國元 國元 YMI 誇選瑟 國元 國元 使用者詳編資料 國元 國元		本概原則/箱核原則			<u> </u>
稽核物件存取 成功,失敗 N-Partner Policy 稽核順戶登入事件 成功,失敗 N-Partner Policy 楷核登入事件 成功,失敗 N-Partner Policy 增核型入事件 成功,失敗 N-Partner Policy 本機原則/使用者權限指派 顧云 本機原則/安全性趨項 國云 事件記錄幅 國五 厚則 設定 優勢 GPO 安全性記錄幅密目最大值 204800 KB N-Partner Policy 文聞金鑰原則/源溫服務用戶端 - 自動註冊設定 顧云 解組原則物件 國云 WMI 篩選器 國云 使用者詳續資料 優元		原則	設定	優勢 GPO	
相核鳴戶堂入事件 成功,失敗 N-Partner Policy 相核登入事件 成功,失敗 N-Partner Policy 本機原則/使用者權限指派 顧云 本機原則/安全性選項 圓云 事件記錄檔 圓云 摩用 設定 優勢 GPO 安全性記錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顧云 公開金鏞原則/加密檔案系統 顧云 解組原則物件 圓云 WMI 篩選器 使用者詳續資料		稽核物件存取	成功,失敗	N-Partner Policy	
相核宜入事件 成功 + 失敗 N-Partner Policy 本機原則/使用者權限指派 顯示 本機原則/安全性邁項 顯示 事件記錄檔 顯惑 厚則 設定 優勢 GPO 安全性記錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顯示 భ田金鏞原則/加鹵檔案系统 顯示 聲紅原則物件 顧示 WMI 誘選器 使用者詳續資料 ////////////////////////////////////		稽核帳戶登入事件	成功,失敗	N-Partner Policy	
本機原則/使用者權限指派 銀本 本機原則/安全性邁項 顯示 事件記錄檔 圓蒸 原則 設定 優勢 GPO 安全性記錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顕示 群組原則物件 顕示 WMI 篩趨器 使用者詳續資料 一		相反宜入事件	成功,关权	IN-Partner Policy	-
本機原則/安全性磁填 國本 國本 事件記錄檔 區蔵 原則 設定 優勢 GPO 安全性記錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顧示 群組原則物件 顧示 WMI 篩竖器 優示 使用者詳續資料 顧示		▲ 侯原則/使用 有權限 信派			銀丕
単件記録幅 陸感 原則 設定 優勢 GPO 安全性記錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顧示 採組原則物件 顧示 WMI 篩選器 ● 使用者詳續資料 ●		本機原則/安全性選順			
原則 設定 優勢 GPO 安全性記錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顯示 公開金鏞原則/加密檔案系統 顯示 弊組原則物件 顯示 WMI 篩選器		爭鬥記録福			透纖
女全性記錄檔保持方法 視需要而定 N-Partner Policy 安全性記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顯示 公開金鏞原則/加密檔案系統 顯示 群組原則物件 顯示 WMI 篩選器 顯示 使用者詳續資料 顯示		原則	設定	優勢 GPO	
公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顯示 公開金鏞原則/加密檔案系統 顯示 料組原則物件 顯示 WMI 篩選器 顯示 使用者詳續資料 圓示		女全性記録福保持万法 安全性記錄檔容量墨大值	視需要而定 204800 KB	N-Partner Policy N-Partner Policy	
計畫 200 進 200 707 707 707 707 707 707 707 707 707		公開全撞百則/馮贽昭務田后候。自	新 註冊铅定		顯示
群組原則物件 顯示 WMI 篩選器 顯示 使用者詳編資料 圓示		公開全撞百則/加索提宏多统	34 GL IIV GX AC		顧示
WMI 篩選器 圓正 使用者詳細資料 圓元	22 40 I	高加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加			調示
使用者詳編資料 題示	WAA	意識器			調示
2011年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		DIV ALL INF			<u>1987 -</u>
	使用者	詳頑貫科			→一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一



5.2 工作群組

5.2.1 稽核原則設定

(1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



(2) 搜尋群組原則物件編輯並執行

輸入 群組原則 -> 點選 [編輯群組原則]





(3) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]





(4) 開啟 [Windows PowerShell]



(5) 更新群組原則





(6) 查看群組原則套用情形

PS C:\> auditpol /get /category:*

系統管理員: Window	rs PowerShell 📃 🗖	x
PS C:> auditpol /get /category:*		^
系統稽核原則 頻如子頻期	設定	
条統		
安全性系統延伸 氢磁学動性	沒有稽核 成份解生龄	
IPSEC driver	沒有稽核	
其他系統事件	成功與失敗	
女王)1517想要更 答人/答出	10(4)	
- <u></u>	成功期失敗	
合出 媒白鋼宏	成切與失敗 成功與失敗	
IPsec 主要模式	成功興失敗	
IPsec 快速模式 IPsec 延伸模式	成功與失敗	
特殊登入	成功與失敗	
其他登入之登出事件	成功與失敗	
納路原則何旅辞 使田者/裝置宣告	成切與失敗 成功與失敗	
物件存取		
信条系統	成功與失敗	
核心物件	成功與失敗	
SAM	成功與失敗	
/②超腺粉 產生的應用程式	成切與失敗 成功與失敗	
控制代碼操縱	成功與失敗	
福茶共用 辭選巫会封句事棄	成功與失敗 成功與失敗	
開造十日月日六末 篩選平台連線	成功與失敗	
其他物件存取事件	成功與失敗	
肝細情条共用 卸除式存納裝置	成切與失敗 成功與失敗	
集中愿则暂存	成功與失敗	
特殊權限使用 非機率結理種限使田	沒有殘核	
其他特殊權限使用事件	沒有稽核	
機密特殊權限使用 #¥細追感	沒有稽核	
建立處理程序	沒有稽核	
終止處理程序	沒有糟核	
DPAPI 活動 RPC 事件	没有稽核 沒有稽核	
隨插即用事件	~~~~ 沒有稽核	
原則變更 驗證圖問題更	d214	
授權原則變更	沒有稽核	
HPSSUC 規則層級原則變更	沒有稽核	
##基于百原则変更 其他原則變更事件	沒有稽核	
稽核原則變更	成功	
限尸官埕 使用者嵁戶營班	成功	
電腦帳戶管理	成功.	
安全性群組管理	成功	
應用程式群組管理	沒有稽核	
其他帳戶營理事件	沒有稽核	
15 17 RX 目錄服務變更	沒有稽核	
目錄服務複寫	沒有禮國	
註細 目録服務復為 日 鎌 略 難 左 取	沒 月 檔 核 成 功	
帳戶登入	144793	
Kerberos 服務票證操作 其他能已發入更迭	成功與失敗	
AEPRFLACサロ Kerberos 驗證服務	成功與天敗 成功與失敗	
記證驗證	成功與失敗	
		>



5.2.2 事件檔案設定

(1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



(2) 搜尋事件檢視器並執行

輸入事件檢視器 -> 點選 [事件檢視器]





(3) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]





(4) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註:請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

	記錄內容 - 安全性 (類型: 系統管理)
一般	
全名(F):	Security
記錄檔路徑(L):	%SystemRoot%\System32\Winevt\Logs\Security.evtx
記錄檔大小:	3.07 MB(3,215,360 位元組)
建立日期:	2021年3月17日 21:40:56
修改日期:	2021年3月17日 15:00:01
存取日期:	2021年3月17日 21:40:56
 ✓ 啟用記錄(E) 最大記錄檔大小 (KB)(2) 當事件記錄檔的大小到 ● 視需要覆寫事件 ○ 當記錄檔已滿時 ○ 不要覆寫事件(5) 	0: 204800↓ 則達上限時: ★ (先覆寫最舊的事件)(W) 非進行封存,不要覆寫事件(A) 手動清除記錄權)(N) 〕 〕 〕
	確定 取消 套用(P)



5.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]





(2) 點選 [安全性] 頁面 -> 按 [進階]

🗼 tmp - 內容 🗙
一般 共用 安全性 以前的版本 自訂
韧件名稱: C:\tmp
群組或使用者名稱(G):
Secretaria CREATOR OWNER
& SYSTEM
& Administrators (WIN2012\Administrators)
& Users (WIN2012\Users)
若要變更權限,請按一下[編輯]。 編輯(E)
CREATOR OWNER 的權限(P) 允許 拒絕
完全控制 ^
修改
讀取和執行 ■
列出資料夾內容
請取
高入
如需特殊權限或進階設定,請按一下 [進階]。 進階(V)
確定 取満 套用(A)



(3) 點選 [稽核] 頁面 -> 按 [新增]

*		tmp 的蜡	1 階安全性設定		_ D X
名稱:	C:\tmp Administrators (WIN2012	Administrators) 💼 😇 🔘			
權限	相核 有效存取相				
如需其他資計 稽核項目:	1, 講按兩下稽核項目, 如果	要修改稽核項目,請鑑取項目	,然後按一下 [編輯] (如果適	用)。	
類型	主題	存取	繼承自	套用到	
新増回	移除(B) 檢視(V)				
停用繼承()					
□以此物件4		子物件稽核項目(P)			
				確定 取消	(書用(△)



(4) 點選 [選取一個主體]

	tmp 的稽核项目	_ 🗆 X
基本權限: □ 完全控制 □ 修改 ☑ 酬取和執行 ☑ 列出資料炎内容 ☑ 願取 □ 蒸入 □ 特殊存取權限		顧示達晤權限
□ 只烯這些植枝設定套用面此容器内的物件和(或) 容器(1)		全部演称
	確定	取渦

(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

選取使用者或群組	x
選取這個物件類型(S): 使用者、群組或內建安全性主體	物件蘋型(O)
從這個位置(F): WIN2012	位置(L)
請輸入物件名稱來選取 (<u>範例</u>)(E): Everyone	檢查名稱(C)
進階(A) 確定	取消



(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]

B	tmp 的檔核項目	_ D X
主糖: Everyone 選取一個主題 類型: 全部 v 変用到: 遠信資料次、子資料次及檔案 v		
基本權限: ● 修改 ● 修改 ● 嫌取和執行 ● 列出資料契内容 ● 頭取 ● 第次2 ● 時珠存取權限		顯示進階權限
□只鄉道盛積枝設定套用至此容器内的物件和(或)容器□		全部遺除
		確定 取消



(7) 稽核項目顯示 [Everyone] 名稱 -> 按 [確定]

*		tmp 的進	階安全性設定	_ _ X
名稱: 擁有者: 權限	C:\tmp Administrators (WIN2012\Ad 稽核 有效存取權	ministrators) 變更(C)		
如需其他資訊 稽核項目:	」, 請按兩下稽核項目。如果要修	F改稽核項目,請選取項目,	然後按一下 [編輯] (如果適	用)。
類型	主題	存取	繼承自	套用到
総 全部	Everyone	完全控制	無	這個資料夾、子資料夾及檔案
新増(D) 停用提承(I)	移陈(B) 编辑(E)			
口以此物件中		的件稽核項目(P)		
				確定 取満 賽用(A)



(8) 按[確定]

一般 共用 安全性 以前的版本 自訂 物件名稱: C:\tmp
物件名稱: C:\tmp
群組或使用者名稱(G):
& CREATOR OWNER
& SYSTEM
& Administrators (WIN2012\Administrators)
& Users (WIN2012\Users)
若要變更權限,請按一下[編輯]。
1000 ±44 (to / · · ·
CREATOR OWNER 的權限(P) 允許 拒絕
完全控制 个
修改
請取和執行
列出資料夾內容
高入 マークション マークション マークション シークション シークション シークション シークション アイ・シーク シークション シークシークシー シークシー シークシー シークシー シークシー シークション シークシー シークシー シークション シークション シークション シークション シークション シークシー シークシー シークシー シークション シークシー シークシー シークシー シークション シークシー シークション シークション シークション シークシー シークション シー シークション シークション シークション シークション シークション シーン シークション シーン シークション シークション シーン シーン シー シークション シークシー シー シ
~~~~~
<b>確定</b> 取満 套用(A)



# 6 Windows 2016

Windows 稽核原則設定 詳細說明請參考前言的稽核原則建議連結 *以下分別為網域和工作群組設定方式。

## 6.1 網域

### 6.1.1 組織單位設定

### (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





#### (2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]




### (3) 輸入組織單位名稱

輸入組織單位名稱:Servers 註:請依客戶環境建立組織單位名稱 -> 按 [確定]

新增物件 - 組織單位	×
建立在: npartner.local/	
名稱( <u>A</u> ):	
Servers	
☑保護容器以防止被意外刪除(P)	
確定 取消 說明	



### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2016] 伺服器按滑鼠右鍵, 註:請依客戶環境選擇 Windows File 主機 -> 點選 [移 動]





### (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	×
將物件移動到容器(M):	
Inpartner     Builtin     Computers     Omain Controllers     ForeignSecurityPrincipals     Managed Service Accounts     Servers     Users	
確定 取消	

# (6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 Win2016 File 伺服器已移動。

☑ Active Directory 使用者和電腦	_		×
檔案(F) 動作(A) 檢視(V) 說明(H)			
🗢 🔿 📶 🦌 📋 🗙 🗟 🗟 🛐 🖏	2. 🖆	7 2	<u>ی</u>
Active Directory 使用者和電腦  名稱 類型	描述	π <u>t</u>	
> 🎬 儲存查詢 🔚 🔚 🔤 📲			
✓ jiii npartner.local			
> 📫 Builtin			
Computers			
Domain Controllers			
> E ForeignSecurityPrincipa			
Managed Service Acco			
S S Users			
Servers			
< > <			>



### 6.1.2 群組原則設定

#### (1) 開啟群組原則管理

開啟 [群組原則管理]



#### (2) 在 Servers 組織單位,新增群組原則物件

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]





### (3) 輸入群組原則物件名稱

輸入群組原則物件名稱:N-Partner Policy 註:請依客戶環境建立群組物件名稱 -> 按 [確定]

新増 GPO		×
名稱( <u>N</u> ): N-Partner Policy		
來源入門 GPO( <u>S</u> ): (無)		~
	<b>確定</b> 取消	

### (4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件按滑鼠右鍵 -> 點選 [編輯]

🔜 群組原則管理	– 🗆 X
🔜 檔案(F) 動作(A) 檢視(V) 視窗(W)	說明(H) _ & ×
🗢 🏟  🖬 🙆 👘	
<ul> <li>         — 群組原則管理         <ul> <li>▲ 樹系: npartner.local</li> <li>◇ 鋼 網域</li> <li>◇ 鋼 npartner.local</li> <li>③ Default Domain Policy</li> <li>&gt; ③ Domain Controllers</li> <li>◇ Servers</li> <li>③ N-Partner Policy</li> </ul> </li> </ul>	<b>群組原則管理</b> 內容 名稱 ▲ 樹系: npartner.local
> ○ 群組原則初件 > > WMI 錦邏器 > > ↓ OP GPO> ○ 網納站○ 群組原則模型○ 詳組原則結果	編輯(E) 強制(N) 歐用連結(L) 儲存報告(S) 從這裡開啟新視窗(W)
	刪除(D) 重新命名(M) 重新整理(F) 說明(H)
	< >>
開啟 GPO 編輯器	



### (5) 本機原則:稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳 戶登入事件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]





#### (6) 事件記錄檔:安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]





#### (7) 事件記錄檔:安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] -> 勾選 [定 義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]





(8) 在 Windows File 伺服器 -> 開啟 [Windows PowerShell]



### (9) 更新 Windows File 伺服器群組原則

PS C: > Invoke-GPUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force	
➢ 選取 系統管理員: Windows PowerShell - □	×
PS C:\>  <mark>Invoke-GPUpdate</mark> -Computer <b>Win2016</b> -RandomDelayInMinutes O -Force PS C:\> _	Ŷ
<	>

### 紅色文字部位請輸入 Windows File 伺服器名

### (10) 產生 Windows File 伺服器群組原則報表

PS C:\> Get-GPResultantSetofPolicy -Computer Win2016 -Path C:\tmp\Win2016.html -Rep	ortType html
▶ 系統管理員: Windows PowerShell - □	×
PS C:\> Get-GPResultantSetofPolicy -Computer Win2016 -Path C:\tmp\Win2016.html -ReportType html	^
RsopMode : Logging Namespace : \\Win2016\Root\Rsop\NS9E1E7F6F_0C0B_4AAC_BBCD_68D16434C9FD LoggingComputer : Win2016 LoggingUser : NPARTNER\administrator LoggingMode : Computer	
PS C:\> _	× .
<	>

紅色文字部位請輸入 Windows File 伺服器名稱和資料夾路徑檔案名稱



# (11) 開啟報表,確認 Windows File 伺服器, 套用 N-Partner Policy 群組原則

) @ file:///C:/tmp/Win2016.htm & v d		×	- □ ×
	影響の問題は思	-	55 54 666
	併組尽則和不		
資料收集: 2022/3/16 下午 04:33:56			全部顯示
摘要			
電腦詳細資料			鐵不
-6			隔藏
			顧示
			顧示
設定			隱藏
原則			5美雄
Windows 設定			
安全性設定			Prill High
帳戶原則/密碼規則			58 M
他后面則/他后缀完面則			顧示
			翻示
略户原用/Kerberos 原則			顧示
本機原則/緒核原則			隔藏
原則	設定	優勢 GPO	
稽核物件存取	成功。失敗	N-Partner Po	licy
稽核帳戶登入事件	成功,失敗	N-Partner Po	licy
稽核登入事件	成功,失 <u>敗</u>	N-Partner Po	licy
本機原則/使用者權限指派			顧示
本機原則/安全性選項			21-
事件記錄檔			
版 01	設定	優熱 GPO	1番 編
安全性記錄檔保持方法	視需要而定	N-Partner Po	licy
安全性記錄檔容量最大值	204800 KB	N-Partner Po	licy
公開金鑰原則/憑證服務用戶端 - 自動註冊設定			
公開会論原則/加密檔案系统			羅示
<b>影/组成</b> 用物件			顧示
Land doctor			顯示
VVIVIE D002565			顯示
使用者詳續資料			er =
			<u> </u>



# 6.2 工作群組

# 6.2.1 稽核原則設定

# (1) 開啟本機群組原則編輯器

點選 💽 -> 輸入 群組原則 -> 點選 [編輯群組原則]

=	最佳比	對				
ŵ		編輯群 控制台	組原則			
៊ែ		ŝ	ß		□¤	11
	群組原	則				
	ρ	[]]	e			



### (2) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]





#### (3) 開啟 [Windows PowerShell]



### (4) 更新群組原則





# (5) 查看群組原則套用情形

# PS C:\> auditpol /get /category:*

➢ 系統管理員: Windows PowerShell	-	×
PS C:\> auditpol /get /category:* 糸統稽核原則		^
類別/子類別 ⁻ 糸統	設定	
安全性系統延伸 系統完整性	沒有稽核 成功與失敗	
IPSEC driver	沒有稽核	
英国の記事件	成功與大照	
金人/金出 登入	成功與失敗	
登出 帳戶鎖定	成功與失敗 成功與失敗	
IPsec 主要模式 IPsec 性速模式	成功與失敗 成功與失敗	
IPsec 延伸模式 thtmm:	成功與失敗	
行休喜へ/登出事件 其他當入/登出事件	成功與失敗	
調路原則可服器 使用者/裝置宣告	成功與失敗 成功與失敗	
	成功與失敗	
檔案系統 registry	成功與失敗 成功與失敗	
核心物件 Sam	成功與失敗	
	成功與失敗	
雇主的應用 译系 控制代碼操縱	成功與失敗	
福茶共用 師選 <u>平</u> 台封包丟棄	成功與失敗 成功與失敗	
篩選平台連線 其他物件存取事件	成功與失敗 成功與失敗	
詳細檔案共用 抽販式存放装置	成功與失敗 成功與失敗	
(集中原則審存) 時時期間(5月)	成功與失敗	
行环推强 使用 非機密 萨赫德德 用	沒有糟核	
具他特殊權限使用爭鬥 機密特殊權限使用	沒有稽核 沒有稽核	
評細追蹤 建立處理程序	沒有稽核	
終止處理程序 DPAPI 活動	沒有稽核 沒有稽核	
RPC 事件 陈插即用事件	沒有稽核 沒有糖核	
Token Right Adjusted Events	沒有稽核	
成为安定 階格原則要更	感边	
護進序則整定 授權原則變更	沒有稽核。	
MPSSVC 規則層級原則變更 篩選平台原則變更	没 月 楷 核 没 有 稽 核	
其他原則變更事件 帳戶管理	沒有稽核	
*************************************	成功 成功	
资产辞祖答理 藤市我学鲜组 \$\$**	沒有稽核	
蒸ന往れ計過管理 其他帳戶管理事件	沒有稽核	
	hX47J	
目錄服扬仔収 目錄服務變更	成功 沒有稽核	
日臻服務複寫 詳細目錄服務複寫	沒有稽核 沒有稽核	
帳戶登入 Kerberos 服務票證操作	成功與失敗	
其他帳戶登入事件 Kerberos 喻證服發	成功與失敗	
22105105 派益派初	成功與失敗	
<		>



# 6.2.2 事件檔案設定

# (1) 開啟 [檢視事件記錄檔]

點選 🧖 -> 輸入 事件記錄檔 -> 點選 [檢視事件記錄檔]

≡	最佳比	對				
ŵ		<b>檢視事</b> ( 控制台	件記錄	闇		
ŝ	<u>T</u>	<u>ي</u>	ß			13
	事件訴	己錄檔				
	ρ	([])	e			



### (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]





### (3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註:請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (類型: 糸統	管理)	×
一般		
全之(F)-	Security	
空気のか		
AL SUKTH POTE (L)-	%SystemKoot%\System32\Winevt\Logs\Security.evtx	1
記錄欄大小:	9.07 MB(9,506,816 位元組)	
建立日期:	2021年3月8日下午 09:42:35	
修改日期:	2021年3月17日下午 05:00:12	
存取日期:	2021年3月8日下午 09:42:35	
☑ 啟用記錄(E)		
最大記錄檔大小 (KB)(X):	204800 🜩	
當事件記錄檔的大小到達	上限時:	
<ul> <li>視需要覆寫事件 (外)</li> </ul>	E覆寫最適的事件)(₩)	
○ 當記錄檔已滿時進	行封存,不要覆寫事件(A)	
○ 不要覆寫事件 (手動	b清除記錄欄)(N)	
		. 1
	)適応素能ご参加(K)	
	確定 取消 套用(P)	



# 6.3 稽核資料夾設定

### (1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]





# (2) 點選 [安全性] 頁面 -> 按 [進階]

🣕 tmp - 內容	×
一般 共用 安全性 以前的版本 自訂	
物件名稱: C:\tmp	
群組或使用者名稱(G):	
SCREATOR OWNER	
SYSTEM	
& Administrators (WIN2016\Administrators)	
Konstanting (WIN2016\Users)	
若要變更權限,請按一下[編輯]。 (5.8%)	
福興(E)	
CREATOR OWNER 的權限(P) 允許 拒絕	
完全控制	^
修改	
請取和執行	
列出資料夾內容	
請取	
寫入	~
如需特殊權限或進階設定,請按一下[進階]。 進階(V)	٦
確定 取消 套用(A	)



# (3) 點選 [稽核] 頁面 -> 按 [新增]

tmp 的進階安	全性設定								-		×
名稱:	C:\tmp										
擁有者:	Administrator	rs (WIN2016\Administra	ators)	💔 變更(C)							
權限	稲核	有效存取權									
如需其他資訊	,諸按兩下稽核	」 5項目。如果要修改稽核	19月1	諸骥取項目,然後按一	-下[編輯](如果)	意用)・					
稽核項目:											
類型	主體		存取		繼承自		套用到				
新増(D)	移除(R)	檢視(V)									
停用繼承(I)	)										
□ 以此物件中	的可繼承稽核項	夏目取代所有子物件稽核	该項目(P)	")							
							確定	取	淌	套用	(A)



# (4) 點選 [選取一個主體]

	-		×
主體 强烈一個主體			
I類型: 成功 ~			
8用到: 這個資料夾、子資料夾及檔案 ~			
● 本種限: □ 中全応制	1	職示遺贈	權限
<ul> <li>&gt;&gt; 環政和執行</li> <li>&gt;&gt; 列出資料夾内容</li> </ul>			
✓ 請取			
特殊荐取權限	_		
只熵這些檔核設定賽用至此吞翻內的物件和(或) 吞翻(T)		全部演師	<u>e</u>
	確定	取	滴

# (5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

選取使用者或群組	×
選取這個物件類型(S):	
使用者、群組或內建安全性主體	物件類型(O)
從這個位置(F):	
WIN2016	位置(L)
請輸入物件名稱來選取 ( <u>範例)(E</u> ):	
Evervone	檢查名稱(C)
	_
進階(A) 確定	取消



# (6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]

tmp 的编纹项目	- 0 X
主號: Everyone 編取一個主體 頭型: 全部 ~	
(8)用到: 這個資料夾、子資料夾及檔案 ~	
基本權限: 「完全控制 「感改 「難取和執行 」別出資料夾内容	顯示進階權限
<ul> <li>☑ 編取</li> <li>☑ 寫入</li> <li>□ 特殊荐取權限</li> <li>□ 只熵遮些模核般定套用至此音器内的物件和 (或) 音器(T)</li> </ul>	全部清除
	確定 取満



# (7) 顯示稽核主體 [Everyone] -> 按 [確定]

	的進階安	8全性設定			- 0
名稱	:	C:\tmp			
雇有	者:	Administrators (WIN2016	\Administrators) 🛛 😌 變更(C)		
1	菫限	稽核 有效存取材	ž		
口需	其他資訊 項目:	A, 講按兩下稽核項目。如果	要修改稽核項目,請攤取項目	,然後按一下 [編輯] (如果適用	利)。
	類型	主體	存取	编承自	套用到
12	全部	Everyone	完全控制	無	這個資料夾、子資料夾及檔案
新	;增(D)	移除(R) 編輯(E)			
新得以	/增(D) 7用繼承(I)	移除(R) 編輯(E) ) 9)	(子物件續核項目(P)		



# (8) 按[確定]

📕 tmp - 內容						×
一般 共用	安全性	以前的版本	自訂			
物件名稱:	C:\tmp	,				
群組或使用者名	<b>3稱(G)</b> :					
SYSTEM						
See Administr	ators (WII	V2016\Admir	nistrato	rs)		
🤽 Users (WI	N2016\Us	sers)				
若要變更權限	請按一下	[編輯]。			編輯(E)	
CREATOR OW	/NER 的權	限(P)		允許	拒絕	
完全控制						^
修改						
讀取和執行						
列出資料夾位	內容					
讀取						
寫入						$\checkmark$
如需特殊權限或	成進階設定	,請按一下(	豊階]・		<b>維</b> 陸(Λ)	
					×=r=(•)	
		確定	]	取消	套用	<u>(A</u> )



# 7 Windows 2019

Windows 稽核原則設定 詳細說明請參考前言的稽核原則建議連結 *以下分別為網域和工作群組設定方式。

# 7.1 網域

# 7.1.1 組織單位設定

### (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





### (2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





### (3) 輸入組織單位名稱

輸入組織單位名稱:Servers 註:請依客戶環境建立組織單位名稱 -> 按 [確定]

新增物件 - 組織單位	×
建立在: npartner.local/	
名稱(A):	
Servers	
☑ 保護容器以防止被意外刪除(P)	
確定 取消 說	明



### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2019] 伺服器按滑鼠右鍵, 註:請依客戶環境選擇 Windows File 主機 -> 點選 [移 動]





### (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	$\times$
將物件移動到容器( <u>M</u> ):	
npartner     Builtin     Computers     Omain Controllers     ForeignSecurityPrincipals     Managed Service Accounts     Servers     Osers	
確定 取消	

#### (6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 Win2019 File 伺服器已移動。





### 7.1.2 群組原則設定

#### (1) 開啟群組原則管理

開啟 [群組原則管理]



#### (2) 在 Servers 組織單位,新增群組原則物件

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]





### (3) 輸入群組原則物件名稱

輸入群組原則物件名稱:N-Partner Policy<mark>註:請依客戶環境建立群組物件名稱</mark> -> 按 [確定]

新増 GPO		×
_名稱(N):		
N-Partner Policy		
來源入門 GPO(S):		
(無)		~
	確定 取消	

### (4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件按滑鼠右鍵 -> 點選 [編輯]





### (5) 本機原則:稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳 戶登入事件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]





#### (6) 事件記錄檔:安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定]: -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]





#### (7) 事件記錄檔:安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾 選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]





#### (8) 開啟 [Windows PowerShell]



#### (9) 更新 Windows File 伺服器群組原則

PS C: > Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force			
➢ 系統管理員: Windows PowerShell	<u>_</u>		×
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes PS C:\> _	0	-Force	\$

紅色文字部位請輸入 Windows File 伺服器名

#### (10) 產生 Windows File 伺服器群組原則報表

PS C: > Get-GPResultantSetofPolicy -Computer Win2019 -Path C: \tmp\Win2019.html -ReportType html



紅色文字部位請輸入 Windows File 伺服器名稱和資料夾路徑檔案名稱



(11) 開啟報表,確認 Windows File 伺服器, 套用 N-Partner Policy 群組原則

) (=) 🔊 C:\tmp\Win2019.html		▼ ぴ 搜尋	
NPARTNER\WIN2019 ×			
	<b>群組原則</b>	結果	
PARTNER\WIN2019			
斜收集: 2022/3/17 上午 09:56:51			<u>全部顧</u> 注
Ŧ			25
腦詳續資料			
- <b>&amp;</b>			18
<b>C件状態</b>			8
ыф.			#
1394			语
JRC9.1			13
Windows 設定			12
安全性設定			
帳戶原則/密碼規則			
帳戶原則/帳戶鎖定原則			#8
帳戶順則/Kerberos 順則			
大田町町内営業町町			#
~ 低原用/ 個 饮原用			13
原則	設定	優勢(	GPO
稽核物件存取	成功,失败	N-Pa	rtner Policy
稽核帳戶登入事件	成功,失败	N-Pa	rtner Policy
稽核登入事件	成功,失败	N-Pa	rtner Policy
本偿原則/使用者權限指派			
本偿原則/安全性選项			
审件記錄檔			80
59	±\.⊕	历教	[編
原用		N-Pa	ther Policy
安全性記録構成用の法	204800 KB	N-Pa	ther Policy
入田本社区制/在地区地内后来 古新社会	10+000 ND		and rolley
ATHAT エ 30 MF PS/ 38 20 05 75 / 25 - 白知社間	ax AL		#
公開金羅原則/加密檔案系統			
料组成则物件			
VMI 餘選器			


# 7.2 工作群組

# 7.2.1 稽核原則設定

## (1) 開啟本機群組原則編輯器

點選 🧖 [搜尋] -> 輸入 群組原則 -> 點選 [編輯群組原則]

=	1	Ľ	ŝ					篩選條件 🏏	
ŵ	最佳比	謝			_				
	1	<b>編輯群</b> 控制台	組原則						
ŝ									
	₽ ∎	¥組原則							
Ŧ	ρ	ĪĪ	e	-					



### (2) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]





#### (3) 開啟 [Windows PowerShell]



#### (4) 更新群組原則





## (5) 查看群組原則套用情形

# PS C:\> auditpol /get /category:*

≥ 系統管理員: Windows PowerShell	-	Х
S C:\> <mark>auditpol</mark> /get /category:* ystem audit policy ategory/Subcategory	Setting	
ategory/Subcategory 総称	seccing	
安全性系統延伸	No Auditing	
系統完整性	Success and Failure	
TPSEC driver	No Auditing	
县他 动航争件 怎会性野能够更	Success and rallure	
シェ (11)(18) 足足 (人)登出	0400000	
· 登入	Success and Failure	
叠世 _{2011年}	Success and Failure	
限尸硬疋 IPaac 主要指式	Success and Failure	
IPsec 快速模式	Success and Failure	
IPsec 延伸模式	Success and Failure	
<u>特殊登入</u>	Success and Failure	
其他令人/全出事件 海路眉肌河距离	Success and Failure	
使用者/选择官告	Success and Failure	
群組成員資格	Success and Failure	
性存取	0	
偏茶 赤鼠 Nagistru	Success and Failure	
核心物件	Success and Failure	
SAM	Success and Failure	
憑證服務	Success and Failure	
產生的應用權式	Success and Failure	
授刑17、吻深険 橙変光目	Success and Failure	
備深不分間	Success and Failure	
簡選率 台連線 「 」	Success and Failure	
甚低物件存取事件	Success and Failure	
\$P\$111:00 \$P\$25 \$	Success and Failure	
進中原削暫在	Success and Failure	
深橋限使用 [		
非機密特殊艦限使用	No Auditing	
其他特殊權限使用學件	No Huditing	
1展GTFF77KTEM2DE/FB 総用追蹤	No Haareing	
建立處理程序	No Auditing	
終止處理程序	No Auditing	
DPHP1 活動 DPC 室体	No Huditing	
がて 事件 勝痛的 耳毛(牛	No Auditing	
權杖權限調整事件	No Auditing	
(則變更	- -	
格核原則變更	Success	
· · · · · · · · · · · · · · · · · · ·	No Auditing	
MPSSUC 規則層級原則變更	No Auditing	
辭攀平台原則變更	No Auditing	
其他原則變更事件	No Auditing	
新藤鹿の修建	No Auditing	
安全件群組管理	No Auditing	
發佈群組管理	No Auditing	
應用程式難組賞理	No Auditing	
其他限户管理事件 使用我能与资源	No Auditing	
	No maarcing	
目錄服務存取	Success	
目縁服務變更	No Auditing	
目錄服務複寫	No Auditing	
計組日感版務優為 (百楽人	No Huditing	
Kerberos 服務累證操作	Success and Failure	
其他帳戶登入事件	Success and Failure	
Kerberos 驗證服務	Success and Failure	
「記、記式を改訂式	Success and Failure	



# 7.2.2 事件檔案設定

# (1) 開啟 [檢視事件記錄檔]

點選 🧖 [搜尋] -> 輸入 事件記錄 -> 點選 [檢視事件記錄檔]

≡	5	Ľ	\$				篩選條件 ∨	
ŵ	最佳比	;對						
	-	<b>檢視事</b> 控制台	件記錄檔					
ø								
	<u>ب</u>	目件記錄			 			
+	ρ	Π	e .					



## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]





## (3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註:請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (類型: 糸統	管理)	×					
一般							
全名(F): Security							
記錄檔路徑(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx							
記錄檔大小:		_					
建立日期:	2021年2月23日下午 05:15:05						
修改日期:	2021年3月18日 上午 09:18:18						
存取日期:	2021年3月18日 上午 09:18:18						
<ul> <li>✓ 啟用記錄(E)</li> <li>→ 記錄檔大小 (KB)(X):</li> <li>當事件記錄檔的大小到道</li> <li>④ 視需要覆寫事件(</li> <li>④ 福記錄檔已滿時進</li> <li>〇 不要覆寫事件(手)</li> </ul>	204800 建上限時: 先覆寫最適的事件)(W) 综行封存,不要覆寫事件(A) 勘清除記錄檔)(N) 清除記錄(R)						
	確定 取消 套用(P)						



# 7.3 稽核資料夾設定

## (1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]





## (2) 點選 [安全性] 頁面 -> 按 [進階]

🧵 tmp - 內容	×
一般 共用 安全性 以前的版本 自訂	
物件名稱: C:\tmp	
群組或使用者名稱(G):	
SCREATOR OWNER	
SYSTEM	
Administrators (WIN2019\Administrators)	
Sers (WIN2019\Users)	
若要變更權限,請按一下 [編輯]。	編輯(E)
CREATOR OWNER 的權限(P) 允許	F 拒絕
完全控制	^
修改	
請取和執行	
列出資料夾內容	
請取	
寫入	~
如需特殊權限或進階設定,請按一下 [進階]。	進階(V)
確定 取消	套用(A)



## (3) 點選 [稽核] 頁面 -> 按 [新增]

📙 tmp 的進階安	全性設定						-	-		×
名稱:	C:\tmp									
擁有者:	Administrator	rs (WIN2019\Administrators	) 🌎 變更(()							
權限	稽核	有效存取權								
如需其他資訊	,請按兩下稽核	5項目・如果要修改稽核項目	目,請選取項目,然後排	8一下 [編輯] (如果	適用)。					
稽核項目:										
類型	主體	存取	X	繼承自	3	劉用到				
******	64 54 m	101 10 a a								-1
新瑁(0)	◎际( <u>K</u> )	(页( <u>V</u> )								
停用瘧承()		ᇹᇊᇳᄵᇏᆃᄀᇥᄹᇔᆦᅚᆱ	3.00							
山以此物件中	的可編序相极場	R日取15所有于物件植物填目	1 (C)							
					Ŧ	龍定	取消		套用(	<u>A</u> )



## (4) 點選 [選取一個主體]

<mark>。</mark> tmp 的镭核項目	-		×
主體: 這點一個主體			
III型: 成功 ~			
8用到: 這個資料來、子資料來及檔案 ~			
基本權限:	顧力	下進階級	ERR.
☑ 讀取和執行			
□ 高人 □ 444280 #55			
□ 19/2 7 2 (m)	\$ #	部滷除	a I.
A real sector and other sector and the real sector and the real real sector.			- 1
	確定	取湯	5

# (5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

選取使用者或群組	×
選取這個物件類型(S): 使用者、群組或內建安全性主體	物件類型( <u>O</u> )
從這個位置(E): WIN2019 請輸入物件名稱來攤取 (範例)(E):	位置(1)
Everyone	檢查名稱( <u>C</u> )
進階( <u>A</u> ) 確定	取消



## (6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]

ump 的橡枝項目			×
主  主   注   注   注 </th <th></th> <th></th> <th></th>			
<ul> <li>基本權限:</li> <li>✓ 完全控制</li> <li>✓ 修改</li> <li>✓ 請取和執行</li> <li>✓ 列出資料夾内寄</li> <li>✓ 請取</li> <li>✓ 請取</li> <li>✓ 寫入</li> <li>□ 特殊存取權限</li> </ul>		⊪示進略	權限
□只將這些種枝設定套用至此吞離內的物件和(或) 吞離(T)	Y1	≧曲『満り	
	憲定	R	滴



## (7) 顯示稽核主體 [Everyone] -> 按 [確定]

	o的進階安	全性設定			- <b>-</b> >
名稱	:	C:\tmp			
擁有	者:	Administrators (WIN2019\A	dministrators) 🏾 🌎 變更(C)		
1	釐限	稽核 有效存取權			
如需	其他資訊	,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)。
稽核	項目:				
	類型	主題	存取	繼承自	套用到
88	全部	Everyone	完全控制	無	這個資料夾、子資料夾及檔案
新	^{1増(<u>D</u>)}	移除(B) 編輯(E)			
新用	<b>1増(Q)</b> ■用槴承(1) 此物件中	移除(B) 編輯(E) ) ) ) ) ) ) )	物件積核項目( <u>P</u> )		



# (8) 按[確定]

📕 tmp - 內容						×
一般 共用	安全性	以前的版本	自訂			
物件名稱:	C:\tmp	, ,				
群組或使用者名	<b>名稱(G)</b> :					
SCREATOR	OWNER					
SYSTEM						
Section 2010 Administration	ators (WII	V2019\Admir	nistrato	rs)		
🤽 Users (WII	N2019\U	sers)				
若要變更權限,	請按一下	[編輯]。			編輯(E)	
CREATOR OW	/NER 的權	P艮(P)		允許	拒絕	
完全控制						^
修改						
讀取和執行						
列出資料夾位	內容					
讀取						
寫入						~
如需特殊權限調	找進階設定	,請按一下 []	售階]。		進階(V)	
		確定	J	取消	套用	(A)



# 8 Windows 2022

Windows 稽核原則設定 詳細說明請參考前言的稽核原則建議連結 *以下分別為網域和工作群組設定方式。

# 8.1 網域

## 8.1.1 組織單位設定

## (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





### (2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





## (3) 輸入組織單位名稱

輸入組織單位名稱:Servers 註:請依客戶環境建立組織單位名稱 -> 按 [確定]

新增物件 - 組織單位	×
建立在: npartner.local/	
名稱( <u>A</u> ):	
Servers	
☑ 保護容器以防止被意外刪除(₽)	
確定 取消 診	明



### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2022] 伺服器按滑鼠右鍵, 註:請依客戶環境選擇 Windows File 主機 -> 點選 [移 動]





### (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	$\times$
將物件移動到容器(M):	
npartner     Builtin     Computers     Omain Controllers     ForeignSecurityPrincipals     Managed Service Accounts     Servers     Osers	
確定 取消	

#### (6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 Win2022 File 伺服器已移動。





## 8.1.2 群組原則設定

#### (1) 開啟群組原則管理

開啟 [群組原則管理]



#### (2) 在 Servers 組織單位,新增群組原則物件

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]





## (3) 輸入群組原則物件名稱

輸入群組原則物件名稱:N-Partner Policy<mark>註:請依客戶環境建立群組物件名稱</mark> -> 按 [確定]

新増 GPO	>
_名稱(N):	
N-Partner Policy	
來源入門 GPO(S):	
(無)	~
	確定 取消

### (4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件按滑鼠右鍵 -> 點選 [編輯]





### (5) 本機原則:稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳 戶登入事件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]





#### (6) 事件記錄檔:安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定]: -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]





#### (7) 事件記錄檔:安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾 選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]





#### (8) 開啟 [Windows PowerShell]



#### (9) 更新 Windows File 伺服器群組原則

PS	C:\>	Invoke-GPUpdate -Comp	uter Win2022	-RandomDel	ayInMinutes O	-Force			
_									
L	🛛 系統	管理員: Windows Power	Shell			_			×
PS	C:N	> Invoke-GPUpdate	-Computer	Win2022	-RandomDe	layInMinutes	Ø	-Force	
PS	C:N	> _							~
10	0.1	-							×

紅色文字部位請輸入 Windows File 伺服器名

#### (10) 產生 Windows File 伺服器群組原則報表

PS C:\> Get-GPResultantSetofPolicy -Computer Win2022 -Path C:\tmp\Win2022.html -ReportType html 承統管理員:Windows PowerShell - - - × PS C:\> Get-GPResultantSetofPolicy -Computer Win2022 -Path C:\tmp\Win2022.html -ReportType html RsopMode : Logging Namespace : \\Win2022\Root\Rsop\NSAE500EF0_23F4_4C47_9534_AB39B9DC10AA LoggingComputer : Win2022 LoggingUser : NPARINER\administrator LoggingMode : Computer PS C:\> _

紅色文字部位請輸入 Windows File 伺服器名稱和資料夾路徑檔案名稱



(11) 開啟報表,確認 Windows File 伺服器, 套用 N-Partner Policy 群組原則

	× +		-	0	×					
← → C ① 檔案   C:	/tmp/Win2022.html	£ <b>6 £</b> ≞	Ē							
群組原則結果										
本PARTNER\WIN2022										
**195.26 ^{m**}					溝線					
一般					===					
元件狀態					## <b>#</b> #					
設定										
原則					12 13					
Windows 設定					(黑 ()来					
安全社投中					围绕					
					溝倉					
順戶原則/密媽規則					98 <b>-</b>					
帳戶原則/帳戶鎖定原則					顯示					
帳戶原則/Kerberos 原則					===					
本機原則/稽核原則					温暖					
原則	設定	優勢 GPO								
稽核物件存取	成功,失敗	N-Partner Po	olicy							
稽核帳戶登入事件	成功,失敗	N-Partner Po	olicy							
稽核登入事件	成功,失敗	N-Partner Po	olicy							
本機原則/使用者權限指派					===					
本機原則/安全性選項										
事件記錄檔					88.75					
原則	設定	優勢 GPO			(兵)武					
安全性記錄檔保持方法		N-Partner Po	olicy							
安全性記錄檔容量最大值	204800 KB	N-Partner Po	olicy							
公開金鑰原則/憑證服務用戶端 - 自	動註冊設定			S						
公開金鑰原則/加密檔案系統					88.75					
群组原则物件					顧示					
11/1 (T 20) 20 50					88-					
WMI 師選發					顧示					
使用者詳細資料					81 <b>-</b>					
					ALC: N					

# 8.2 工作群組

# 8.2.1 稽核原則設定

## (1) 開啟本機群組原則編輯器

點選 🎴 [搜尋] -> 輸入 群組原則 -> 點選 [編輯群組原則]

	最佳比對	
	編輯群組原則 控制台	
=	A 🛱 💽 🚍	



### (2) 本機原則:稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事 件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]





#### (3) 開啟 [Windows PowerShell]



### (4) 更新群組原則

PS C:\> gpupdate /force





### (5) 查看群組原則套用情形

# PS C:\> auditpol /get /category:*

≥ 条統管理員: Windows PowerShell		-	×
PS C:\> <mark>auditpol</mark> /get /category:* Sustem audit policy			^
Category/Subcategory	Setting		
System Security System Extension	No Auditing		
System_Integrity	Success and	Failure	
IPsec Driver	No Auditing	<b>B</b> - <b>23</b>	
Security State Change	Success and	Failure	
Logon/Logoff	0000000		
Logon	Success and	Failure	
Logoff Account Lockout	Success and Success and	Failure	
IPsec Main Mode	Success and	Failure	
IPsec Quick Mode	Success and	Failure	
IPsec Extended Mode Special Logon	Success and Success and	Failure	
Other Logon/Logoff Events	Success and	Failure	
Network Policy Server	Success and	Failure	
User / Device Claims Group Membership	Success and	Failure	
Object Access	ouccess anu	ranure	
File System	Success and	Failure	
Kegistry Kaupal Object	Success and	Failure	
SAM	Success and	Failure	
Certification Services	Success and	Failure	
Application Generated	Success and	Failure	
File Share	Success and Success and	Failure	
Filtering Platform Packet Drop	Success and	Failure	
Filtering Platform Connection	Success and	Failure	
Detailed File Share	Success and	Failure	
Removable Storage	Success and	Failure	
Central Policy Staging	Success and	Failure	
Non Sensitive Privilege Use	No Auditing		
Other Privilege Use Events	No Auditing		
Sensitive Privilege Use	No Auditing		
Process Creation	No Auditing		
Process Termination	No Auditing		
DPAPI Activity	No Auditing		
RPG Events Plug and Play Events	No Auditing		
Token Right Adjusted Events	No Auditing		
Policy Change	• •		
Audit Policy Change Authentication Policy Change	Success		
Authorization Policy Change	No Auditing		
MPSSUC Rule-Level Policy Change	No Auditing		
Filtering Platform Policy Change Other Policy Change Events	No Auditing		
Account Management	no nutring		
Computer Account Management	Success		
Security Group Management	Success No Auditing		
Application Group Management	No Auditing		
Other Account Management Events	No Auditing		
User Account Management	Success		
Directory Service Access	Success		
Directory Service Changes	No Auditing		
Directory Service Replication	No Auditing		
Account Logon	No Huditing		
Kerberos Service Ticket Operations	Success and	Failure	
Other Account Logon Events	Success and	Failure	
Credential Validation	Success and Success and	Failure	
PS C:\>	ourooso ana	I dillaro	~



# 8.2.2 事件檔案設定

# (1) 開啟 [檢視事件記錄檔]

點選 🎴 [搜尋] -> 輸入 事件檢視 -> 點選 [事件檢視器]

最佳比對			
▶ 事件檢視器 應用程式			
▶ 事件檢視器			
오 태 💽	2		



## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]





## (3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註:請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (頚型: 糸統	管理)	×
一般		
全名(F):	Security	
記錄檔路徑(L):	%SystemRoot%\System32\Winevt\Logs\Security.evtx	
記錄檔大小:	16.07 MB(16,846,848 位元組)	
建立日期:	2022年3月8日下午 06:04:42	
修改日期:	2022年3月17日上午 10:15:30	
存取日期:	2022年3月17日上午 10:15:30	
✓ 啟用記錄(E)		
最大記錄檔大小 (KB)(X): 當事件記錄檔的大小到過	204800 🐳	
<ul> <li>● 視需要覆寫事件(5)</li> </ul>		
○ 當記錄檔已滿時進	行封存,不要覆寫事件(A)	
○ 不要覆寫事件 (手動	协清除記錄檔)(N)	
	清除記錄(R)	
	確定 取消 套用(P)	



# 8.3 稽核資料夾設定

### (1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]





## (2) 點選 [安全性] 頁面 -> 按 [進階]

🣕 tmp - 內齊	×
一般 共用 安全性 以前的版本 自訂	
物件名稱: C:\tmp	
群組或使用者名稱(G):	
SYSTEM	
Administrator (WIN2022\Administrator)	
Administrators (WIN2022\Administrators)	
若要變更權限,請按一下 [編輯]。	(5:10/E)
	加速業年(に)
SYSTEM 的權限(P) 分	許拒絕
完全控制	· ^
修改 🗸	/
請取和執行 🗸 🗸	/
列出資料夾內容 🗸	/
請取 🗸	/
高入	/ ~
如需特殊權限或進階設定,請按一下 [進階]。	進階(V)
確定 取	資 套用( <u>A</u> )



## (3) 點選 [稽核] 頁面 -> 按 [新增]

📙 tmp 的進階安	全性設定								-		×
名稿:	C:\tmp										
擁有者:	Administrate	ors (WIN2022\Adr	ministrators)	🐶 變更(C)							
權限	共用	稽核	有效存取權								
如需其他資訊	,請按兩下稽核	該項目・如果要修	20.稽核項目,	請邏取項目,然後按·	一下 [編輯] (如果	適用) •					
稽核項目:											
類型	主體		存取		繼承自		寶用到				
											-1
新増(D)	移除(R)	檢視(V)									
停用繼承(I)											
☑ 以此物件中	的可繼承稽核	項目取代所有子校	り件稽核項目(P	')							
							確定	取消	i	<b></b> 寮用	(A)


#### (4) 點選 [選取一個主體]

🧧 tmp 的瘤核項目			×
主聽: 國政一項主體			
編型: 成功 · ·			
<b>赛用劲:</b> 這個質科友、子質科友及檔案 ~			
基本權限:		顧示連席	權限
<ul> <li>□ 完全控制</li> <li>□ 修改</li> <li>② 建設和執行</li> <li>② 列出資料支内容</li> <li>② 減取</li> <li>□ 寫入</li> <li>□ 特殊存取權限</li> </ul>			
□ 只傳這圭領核股定賽用至此審腸內的物件和(或)審腸(T)		全部消	8
	確定	B	消

### (5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

邏取使用者或群組	×
選取這個物件類型(S): 使用者、群組或內建安全性主體	物件蘋型(O)
從這個位置(F): WIN2022 請輸入物件名稱來選取 (範例)(E):	位置(L)
Everyone	檢查名稱(C)
進階(A) 確定	<b>取</b> 消



#### (6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]

🧾 tmp 的瘤核項目			×
主種:     Everyone 選取一個主題       預型:     全部       客用到:     遠個資料英、子資料支及備素			
<ul> <li>基本權限:</li> <li>● 保全控制</li> <li>● 保全</li> <li>● 通知</li> <li>● 列出資料次内容</li> <li>● 留取</li> <li>● 保政 日本</li> <li>● 特殊存取權限</li> <li>□ 只將進座欄枝股定審用至此會關內的物件和(或) 審職(1)</li> </ul>		■ 示道段 全部清)	8
	確定	R	滴



#### (7) 顯示稽核主體 [Everyone] -> 按 [確定]

tmp	o 的進階安;	全性設定			- 0	>
名稱	:	C:\tmp				
擁有	者:	Administrators (WIN202	22\Administrators) 🛛 🌍 🧮 🛡 (C)			
ŧ	皇限	共用 稽核	有效存取權			
如需	其他資訊	,請按兩下稽核項目・如	果要修改稽核項目,請遵取項目,	然後按一下 [編輯] (如果適	用)。	
稽核	項目:					
	調型	主體	存取	編承自	<b></b> 滚用到	
88.	全部	Everyone	完全控制	無	這個資料夾、子資料夾及欄案	
	f増(D)	移除(R) 編輯(E	)			
1	用繼承の					
(5) 了以	■用繼承(I) 此物件中(	的可繼承稽核項目取代所	有子物件稽核項目(P)			



### (8) 按[確定]

📕 tmp - 內容						×
一般 共用	安全性	以前的版本	自訂			
物件名稱:	C:\tmp	, ,				
群組或使用者名	3稱(G):					
SYSTEM						
Administra	ator (WIN	12022\Admin	istrator)	)		
St Administra	ators (WII	N2022\Admir	nistrato	rs)		
<b>計算時再將作</b> 。	建	「任臣書臣」。				
石安建史催和	18 1X - 1	.[1篇字曰] .			編輯(E)	
SYSTEM 的權利	畏(P)			允許	拒絕	
完全控制				~		^
修改				~		
讀取和執行				~		
列出資料夾付	内容			~		
讀取				~		
寫入				~		~
如需特殊權限或	<b>戈</b> 進階設定	· 請按一下 [i	≜階]・		進階(V)	
	2000				_	
		確定	]	取消	套用	( <u>A</u> )



# 9 N-Reporter

#### (1) 新增 Windows File 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]





#### (2) 選擇設備種類

選擇 [Application/DB/OS/Server]-> 點選 [引導模式]





# 9.1 Windows 2003 或之前版本作業系統

### (1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows]-> 點選 [下一步]

#	新増設備 - 設備基本設定			×
	設備基本設定			^
	設備名稱 *			
	WinFiles-192.168.8.76			
	IP *			
	192.168.8.76			
	所屬領域 *			
	Global			~
	Syslog 資料格式 ❹			
	Windows			~
	自定義資料格式 🕄 🛛 🛨			
	未設用			~
	SNMP Model ()			
	Host Mib			~
	Web 監控 🕄			
		上一步	下一步	取消



### (2) Syslog 相關設定

Facility 選擇 [(17) local use 1 (local1)] 和編碼方式: [BIG 5] -> 點選 [下一步] (若勾選 [Raw Data 保留] · 則 [事件查詢] 顯示 Raw Data 資訊)

▲ 新増設備 - Syslog 相關設定		×
Syslog 相關設定	^	
Facility ()		
(17) local use 1 (local1)	~	
編碼方式		
BIG5	~	
Syslog 正規化資料保留天數上限 🕄		
Raw Data 保留與轉發 ✔ Raw Data 保留 ↓ 本設備於分時監控報表啟動 Syslog 轉發時,採用 Raw Data 格3	ť	
□ 轉發方式將使用來源設備的 IP		
上一步	下一步 取消	]



#### (3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

▲ 新増設備 - 其它	×
其它	^
設備 Icon	
Host	~
接收狀態	
<ul> <li>愈用</li> <li>停用</li> </ul>	
释度 程度	
	_
上一步	取消

是否啟用預設報表,將套用置相同廠牌型號設備-> 點擊 [否]





# 9.2 Windows 2008 或之後版本作業系統

### (1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows]-> 點選 [下一步]

*	新增設備 - 設備基本設定		×
	設備基本設定	^	
	設備名稱 *		ור
	WinFiles-192.168.8.76		
	IP *		
	192.168.8.76		
	所屬領域 *		
	Global	~	
	Syslog 資料格式 🗊		
	Windows	~	
	自定義資料格式 🕄 🕇 +		
	未愈用		
	SNMP Model 🚯		
	Host Mib	~	
	····································		
	啟用網頁監控功能		
		步 取	ä
			<u> </u>



### (2) Syslog 相關設定

Facility 選擇 [(17) local use 1 (local1)] 和編碼方式: [UTF-8] -> 點選 [下一步] (若勾選 [Raw Data 保留] · 則 [事件查詢] 顯示 Raw Data 資訊)

山新	/增設備 - Syslog 相關設定		×
1	Syslog 相關設定	^	
F	Facility ()		
	(17) local use 1 (local1)	~	
ŧ	編碼方式		
	UTF-8	~	
	Syslog 正規佔資料保留天數上限 ➊		
F	Raw Data 保留與轉發 ✔ Raw Data 保留		
	本設備於分時監控報表啟動 Syslog 轉發時,採用 Raw Data 格式		
	轉發方式將使用來源設備的 IP		
	上一步 下一步	取消	



#### (3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

▲ 新増設備 - 其它	×
其它	^
設備 Icon	
Host	~
接收狀態	
<ul> <li>愈用</li> <li>停用</li> </ul>	
释度 程度	
	_
上一步	取消

是否啟用預設報表,將套用置相同廠牌型號設備-> 點擊 [否]





# 10 問題排除

## 10.1 Invoke-GPUpdate 錯誤

#### (1) 在 AD 網域伺服器 -> 執行 Invoke-GPUpdate 更新 Windows File 群組原則出現錯誤訊息

≥ 系統管理員: Windows PowerShell		×
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force Invoke-GPUpdate : 距離 "Win2019" 沒有回應 - 目標距離已關閉成 Remote Scheduled Tasks Management Firewall 未 金數名稱: computer 位於 網路:1 字元:1 + Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force		Â
+ CategoryInfo : OperationTimeout: (:) [invoke-GPUpdate], ArgumentException + FullyQualifiedErrorld : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUpdateCommand PS C:\> _		

(2) 在 Windows File 伺服器, 開啟 [Windows PowerShell]



(3) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

PS C: >> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-Select-Object Name, DisplayName, Enabled, Direction, Action   Format-Table	TCP"
27 东东管理县: Windows PowerShell - ロ X	
PS C:> Oct-NotPireunlikule -Nome "MMI-VINMMT-In-TOP", "www.monitoring-rpc", "MDIG-NCCE-In-TOP" I Select-Object Name, DisplayName, Enabled, Direction, Action I Pornat-Table	•
Nune DisplayNune Unabled Direction Action	
ne-mensitoring-pp: Virtual Machine Menitoring (RPC) Folse labound Allaw NEBIC-EPCES-In-TCE Distributed Transaction Conclinator (RPC-EPNMP) Folse labound Allaw MMI-VINMOMT-In-TCE Visions Management Instrumentation (VMI-In) Folse labound Allaw	
P3 C1> _	

#### (4) 啟用 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

ļ	PS C: \> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", -Enabled True	"MSDTC-	RPCSS	- In- TCP'
	27 条统管理員: Windows PowerShell	-		×
1	PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-ICP", "vm-monitoring-rpc", "MSDIC-RPCSS-In-ICP" PS C:\> _	-Enabled	True	•



(5) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則



(6) 在 AD 網域伺服器 -> 更新 Windows File 群組原則



紅色文字部位請輸入 Windows Server 伺服器名稱



