

政府組態基準(GCB) 管理實務分享

執行長兼首席顧問：鍾榮翰

Email: barbet@r-adv.com.tw

Mobile: 0932391546

May 9, 2017

- 鍾榮翰(容易相處的男子漢)
- GCB組態管理的頂尖高手
- 雷擎先進執行長兼首席顧問
- Can not measure, will not control是我堅持的信念！
- 曾任行政院國家資通安全會報技術服務中心顧問，編撰政府資安作業共通規範、參考指引。
- 推廣資安度量觀念，致力於發展安全度量之技術與服務。



**Can not measure,
will not control !**

無法度量，就無法控制！

- 行政院資安政策要求
- 組態管理的重要性！
- AD GPO 佈署實務!
- 如何得知GCB佈署結果？
- 網域內套用二種以上Account Policy
- 你可以有更SMART的方法！
- 分散式弱點掃描與管理
- 軟體派送機制(主動弱點修補)

行政院資安政策要求

行政院資通安全處 函

機關地址：10058 臺北市忠孝東路1段1號
聯絡人：余柏賢
電子信箱：bsy1@cy.gov.tw

受文者：

發文日期：中華民國105年12月30日
發文字號：院臺護字第1050189725號
類別：普通件
密等及解密條件或保密期限：
附件：如文

主旨：有關政府組態基準(GCB)之調整推廣及推動導入一案，請依說明事項配合辦理並轉知所屬，請查照。

說明：

- 一、依據「國家資通通訊安全發展方案(102年至105年)」行動方案2.3.2「推展資安基礎環境安全設定」之執行要點1「持續規劃不同系統政府組態基準設定」辦理。
- 二、本院國家資通安全會報自102年起推動各部會導入微軟個人電腦作業系統Windows 7及瀏覽器IE8之GCB項目，嗣經本處蒐集各機關(構)回饋意見據以檢討，建議Windows 7有關互動式登入、電源管理及密碼原則等GCB項目調整為不規範或放寬，爰請各機關(構)參考本次調整結果並協助推廣至所屬機關(構)導入。
- 三、另，針對103年及104年制訂之GCB項目(分別為微軟伺服器作業系統Windows Server 2008 R2、Red Hat伺服器作業系統RHEL、微軟個人電腦作業系統Windows 8.1、瀏覽器IE11及無線網路)，為持續加強GCB推動之深廣度，請資安責任等級列A級及B級機關(構)推動導入前揭5項GCB項目。
- 四、GCB相關說明文件、部署資源、教育訓練教材、數位教材影片及常見問題請參考本院國家資通安全會報技術服務中

第1頁、共2頁

- 行政院資通安全處函
- 發文日期：中華民國105年12月30日
- 發文字號：院臺護字第1050189725號
- TWGCB文件已發行 Win7, Win8, IE8, IE11, Windows Server 2008 AD、Red Hat、無線網路等
- 請資安責任等級列A級及B級機關(構)推動導入前揭5項GCB項目。

行政院資安稽核

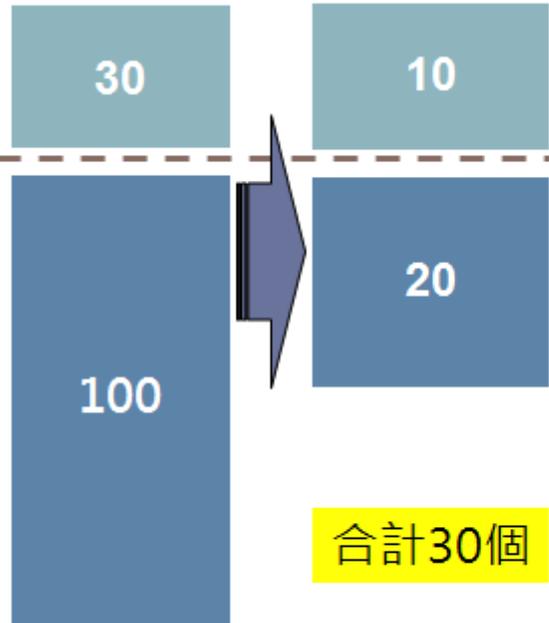
- ❖ 採**全年稽核**方式，提列130個候選機關，從中遴選30個受稽機關，**分季**執行稽核作業
- ❖ 分季公布受稽機關名單
- ❖ 遴選原則

1. 關鍵基礎設施提供者 (金融、通訊 2 類)

2. 符合以下情形者之政府機關

- 提供共用(通)性資訊系統服務
- 曾列入稽核建議名單，因故未實施者
- 近4年稽核結果，建議持續關注協助者
- 近年曾發生3級以上重大資安事件者
- 攻防演練結果有增進空間者
- 近期已執行重大系統改版者
- 未完成應辦事項者(防護縱深/安全性檢測)
- AB級機關未參與歷年稽核者(102年迄今)

候選機關 受稽機關



行政院資安稽核

❖ 總分 = 技術檢測 (30%) + 實地稽核 (70%)

項次	技術檢測項目	檢測子項	配分	構面	實地稽核項目	配分
1	使用者電腦安全檢測	使用者電腦弱點掃描	10	策略面 30	1.導入資訊安全管理系統範圍適切性	5
		使用者電腦安全防護檢測	20		2.機關首長對資安業務支持度	5
		組態設定安全防護檢測	5		3.資源投入資安業務狀況	5
4.資安業務運作規劃與落實	15					
2	惡意中繼站連線阻擋檢測	惡意中繼站連線阻擋檢測	5	管理面 30	5.個人資料保護與管理	10
		核心資訊系統內網滲透測試	30		6.資訊資產管理與風險評鑑	8
3	核心資訊系統安全檢測	系統防護檢測	10		7.人力資源管理	5
		網路架構檢測	10		8.資訊委外安全管理	7
4	網路架構檢測	網路架構檢測	10	技術面 40	9.通訊與作業管理適切性與落實執行狀況	20
5	AD主機安全防護檢測	AD主機安全防護檢測	10		10.資安事件通報與管理	10
		11.資訊系統開發與維護安全管理	10			
合計			100	合計		100

組態管理的重要性

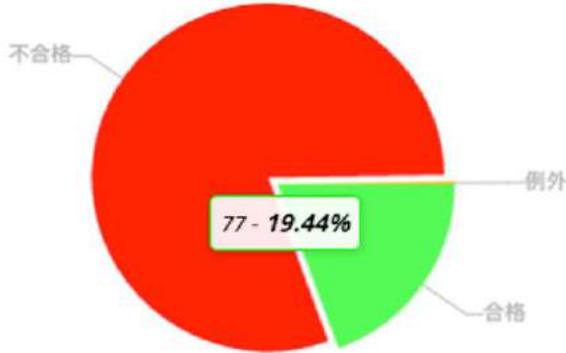
Twenty Critical Security Controls for Effective Cyber Defense

- **CIS Critical Security Controls - Version 6.1**
 - CSC 1: Inventory of Authorized and Unauthorized Devices
 - CSC 2: Inventory of Authorized and Unauthorized Software
 - **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
 - **CSC 4: Continuous Vulnerability Assessment and Remediation**
 - CSC 5: Controlled Use of Administrative Privileges
 - CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
 - CSC 7: Email and Web Browser Protections
 - **CSC 8: Malware Defenses**
 - CSC 9: Limitation and Control of Network Ports, Protocols, and Services
 - CSC 10: Data Recovery Capability

預設組態，安全堪虞

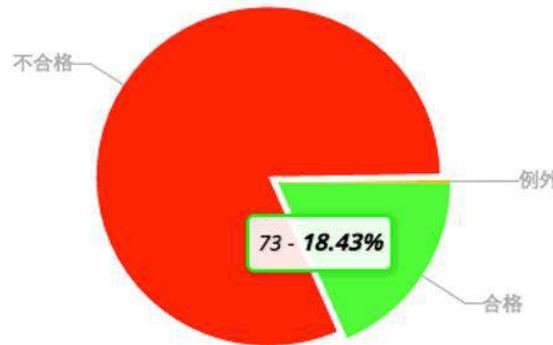
Win7

合格率 (不含 Security Patches)



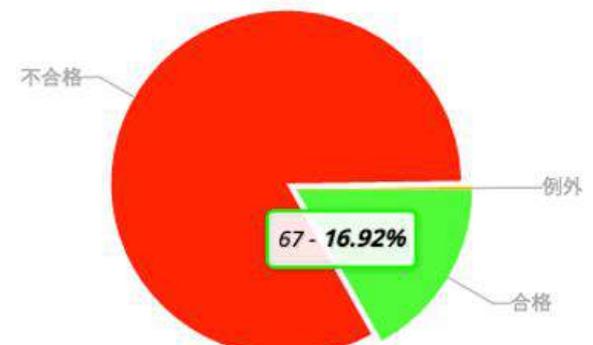
Win8

合格率 (不含 Security Patches)



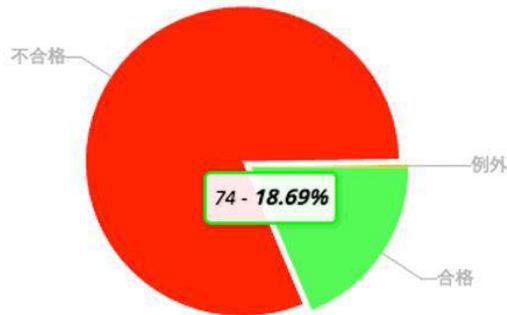
Win10

合格率 (不含 Security Patches)



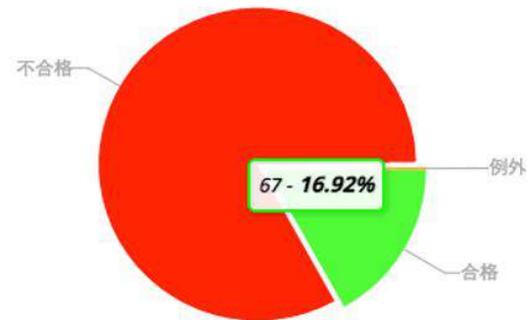
Win Server 2008R2 SP1

合格率 (不含 Security Patches)



Win Server 2012

合格率 (不含 Security Patches)



正確組態派送，提升安全程度

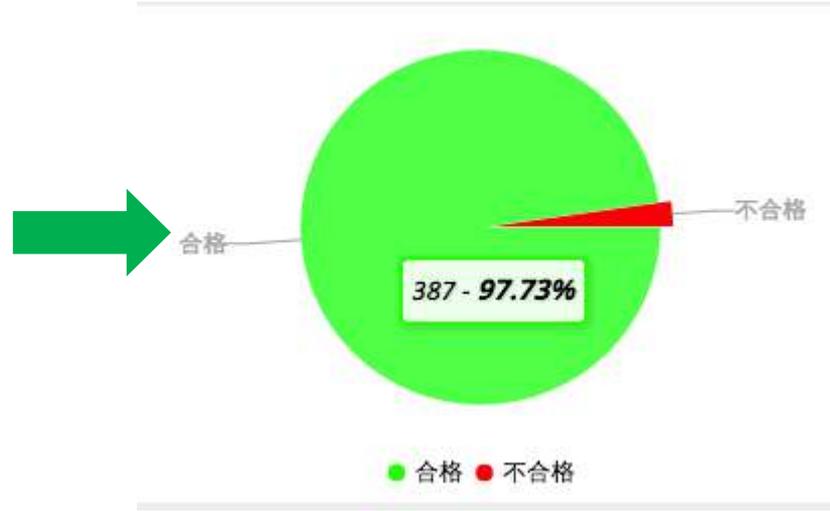
正確的組態派送，可以快速的提升安全組態之符合程度，但可彈性的保留必要之組態，進行例外管理。

組態檢視 - GCB_OMSS(Default)

名稱: GCB_OMSS(Default)

編號	項目名稱	CCE ID
✓ 14	網路安全性: 強制限制登入時數	CCE-970+8
✓ 15	帳戶: 重新命名系統管理員帳戶	CCE-848+8
✓ 16	帳戶: 重新命名來賓帳戶名稱	CCE-9229-6
✓ 17	網路存取: 允許匿名 SID 名稱翻譯	CCE-9531-5
✓ 18	帳戶: Administrator 帳戶狀態	CCE-9199-1
✓ 19	帳戶: Guest 帳戶狀態	CCE-9714-8
✓ 20	修復主控台: 允許自動系統管理登入	CCE-9807-0
✓ 21	修復主控台: 允許軟體複製以及存取所有磁碟和所有資料夾	CCE-9945-8
✓ 22	裝置: CD-ROM 存取只限於登入本機的使用者	CCE-9304-7
✓ 23	裝置: 軟體儲存存取只限於登入本機的使用者	CCE-9440-9
✓ 24	互動式登入: 網路控制站無法使用時, 要快取的先前登入次數	CCE-9487-1
✓ 25	互動式登入: 要求網路控制站驗證以解除鎖定	CCE-9818-7
✓ 26	互動式登入: 在密碼到期前提示使用者變更密碼	CCE-9307-0
✓ 27	互動式登入: 智慧卡移除操作	CCE-9067-0
✓ 28	使用者帳戶控制: 在管理員核准模式, 系統管理員之提升權限提示的行為	CCE-9958-1
✓ 29	使用者帳戶控制: 標準使用者之提升權限提示的行為	CCE-9813-8
✓ 30	互動式登入: 不要按 CTRL+ALT+DEL 鍵	CCE-9317-9
✓ 31	互動式登入: 不要顯示上次登入的使用者名稱	CCE-9449-0
✓ 32	使用者帳戶控制: 偵測應用程式安裝, 並提示提升權限	CCE-9616-4
✓ 33	使用者帳戶控制: 所有系統管理員均以管理員核准模式執行	CCE-9189-2
✓ 34	使用者帳戶控制: 僅針對在安全位置安裝的 UIAccess 應用程式, 提高其權限	CCE-9189-2
✓ 35	使用者帳戶控制: 將檔案及登錄寫入失敗虛假化並儲存至每一使用者位置	CCE-9817-9
✓ 36	使用者帳戶控制: 使用內建的 Administrator 帳戶的管理員核准模式	CCE-9817-9
✓ 37	網路安全性: 設定 Kerberos 允許的加密類型	CCE-9532-3
✓ 38	互動式登入: 給登入使用者的訊息標題	CCE-8740-3
✓ 39	互動式登入 3: 給登入 3 使用者的訊息內容	CCE-9872+0

組態派送

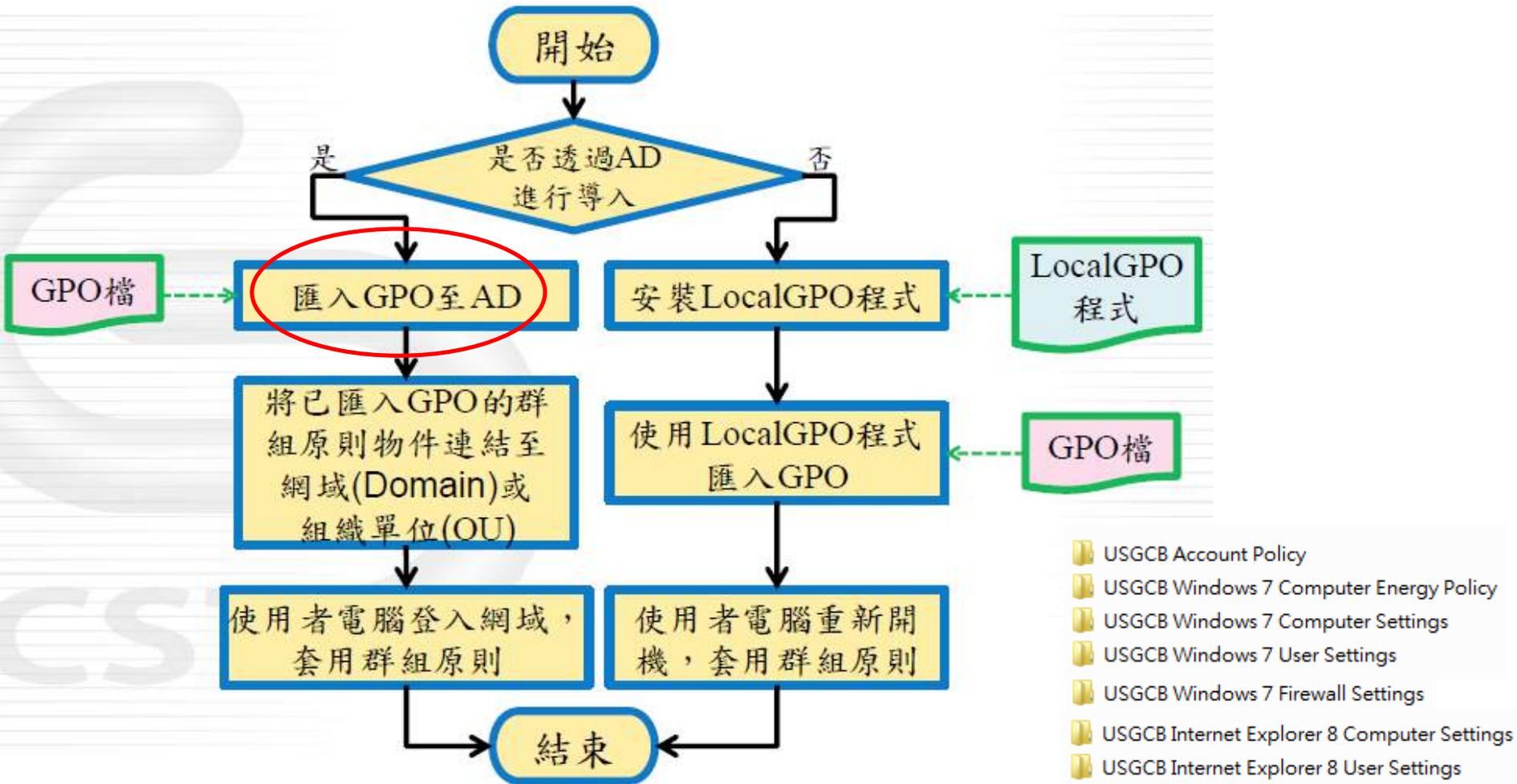


Host Status	Account Policy	Computer Energy	Computer Settings	User Settings
✓	106	使用者權限指派	設定檔單一處理程序	PASS
✓	107	使用者權限指派	執行磁碟區維護工作	PASS
✓	108	使用者權限指派	修改韌體環境值	PASS
✓	109	使用者權限指派	修改物件標籤	PASS
✓	110	使用者權限指派	管理稽核及安全性記錄檔	PASS
✗	111	使用者權限指派	以服務方式登入	FAIL
✗	112	使用者權限指派	以批次工作登入	FAIL
✓	113	使用者權限指派	鎖定記憶體中的分頁	PASS
✓	114	使用者權限指派	載入及解除載入裝置驅動程式	PASS
✓	115	使用者權限指派	增加排程優先順序	PASS
✓	116	使用者權限指派	增加處理程序工作組	PASS
✓	117	使用者權限指派	在驗證後模擬用戶端	PASS

例外管理

AD GPO 佈署實務

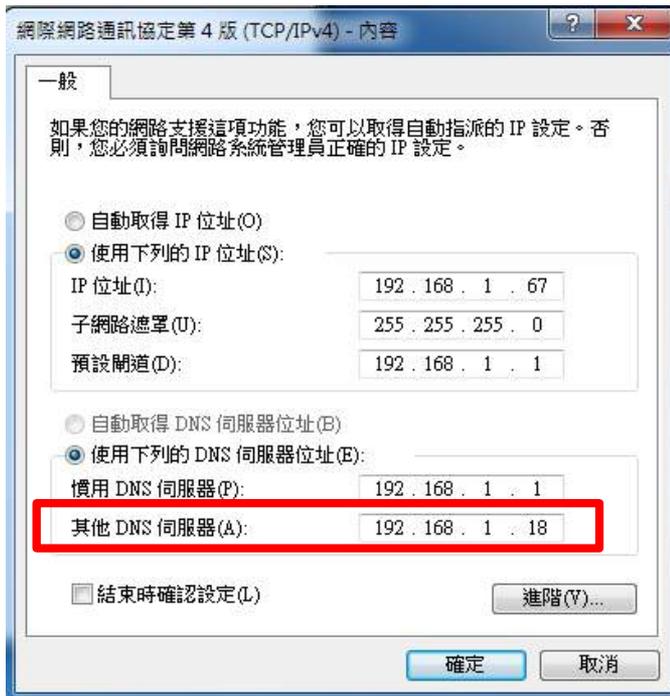
Microsoft GPO派送方法



DNS IP Address 設定錯誤

- GPO能夠完整的執行工作，電腦必須要能夠正確的被AD網域所管理，而網域的鑑別機制主要是經由DNS得知網域控制站的所在位置，同樣的經由DNS得知Kerberos資訊，才能夠確保GPO正確執行。

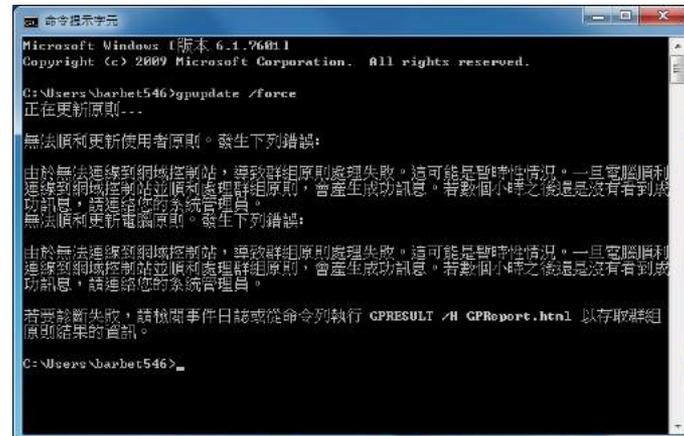
DNS : 192.168.1.18



連線至網路閘道



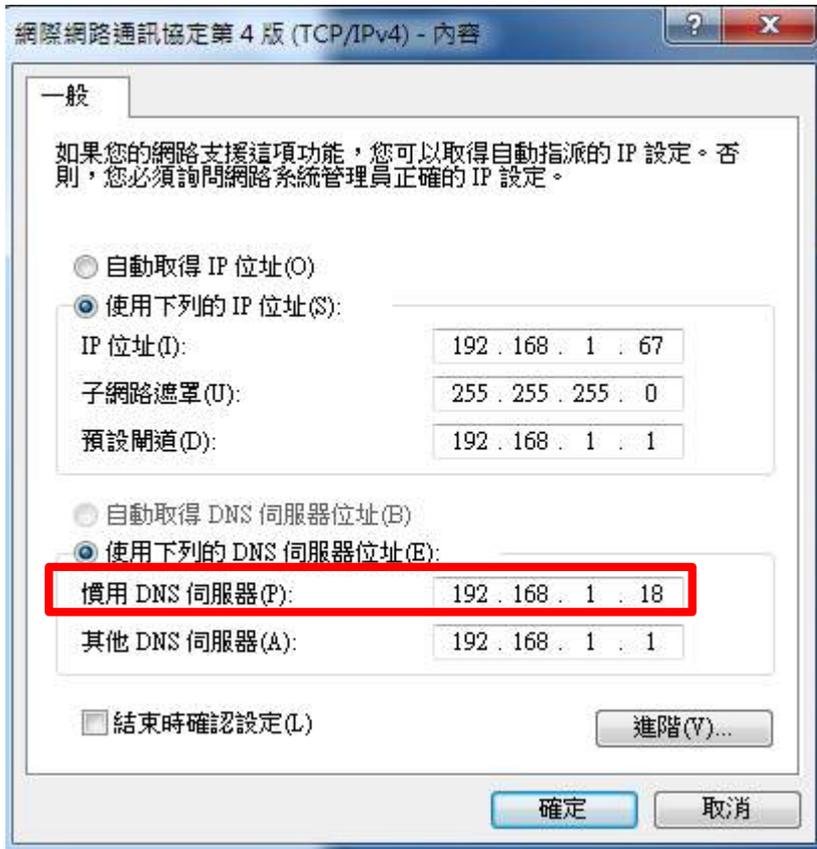
錯誤DNS設定，群組原則無法更新



正確的DNS設定

DNS : 192.168.1.18

連線至網域



檢視您基本的網路資訊並設定連線



正確DNS設定，群組原則更新完成



GPO沒有正確的啟用連結

Radiant_HQ

已連結的群組原則物件 | 群組原則繼承 | 委派

連結順序	GPO	強制	啟用連結	GPO 狀態
1	USGCB Account Policy	否	否	啟用
2	USGCB Win7 Computer Energy	否	是	啟用
3	USGCB Win7 Computer Settings	否	是	啟用
4	USGCB Win7 Firewall Settings	否	是	啟用
5	USGCB Win7 User Settings	否	否	啟用
6	USGCB IE8 Computer Settings	否	是	啟用
7	USGCB IE8 User settings			
8	WMI遠端管理開放			

Radiant_HQ
 USGCB Account Policy
 USGCB IE8 Comp
 USGCB IE8 User
 USGCB Win7 Co
 USGCB Win7 Co
 USGCB Win7 Fire
 USGCB Win7 Use
 WMI遠端管理開放
 Radiant_Taipei
 測試區
 群組原則物件
 WMI 篩選器
 Domain Controler
 IE 11
 IE 8.9.10

編輯(E)...
 強制(O)
 啟用連結(L)
 儲存報告(S)...
 檢視(V)
 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)

GPO 之物件類型設定錯誤

Radiant_HQ

已連結的群組原則物件 | 群組原則繼承 | 委派

連結順序	GPO	強制	啟用連結	GPO 狀態
1	USGCB Account Policy	否	是	啟用
2	USGCB Win7 Computer Energy	否	是	啟用
3	USGCB Win7 Computer Settings	否	是	啟用
4	USGCB Win7 Firewall Settings	否	是	啟用
5	USGCB Win7 User Settings	否	是	啟用
6	USGCB Win7 Computer Settings	否	是	啟用
7	USGCB IE8 User settings	否	是	啟用
8	Win7遠端管理開啟	否	是	啟用

User Settings

使用者並未加入至組織單位

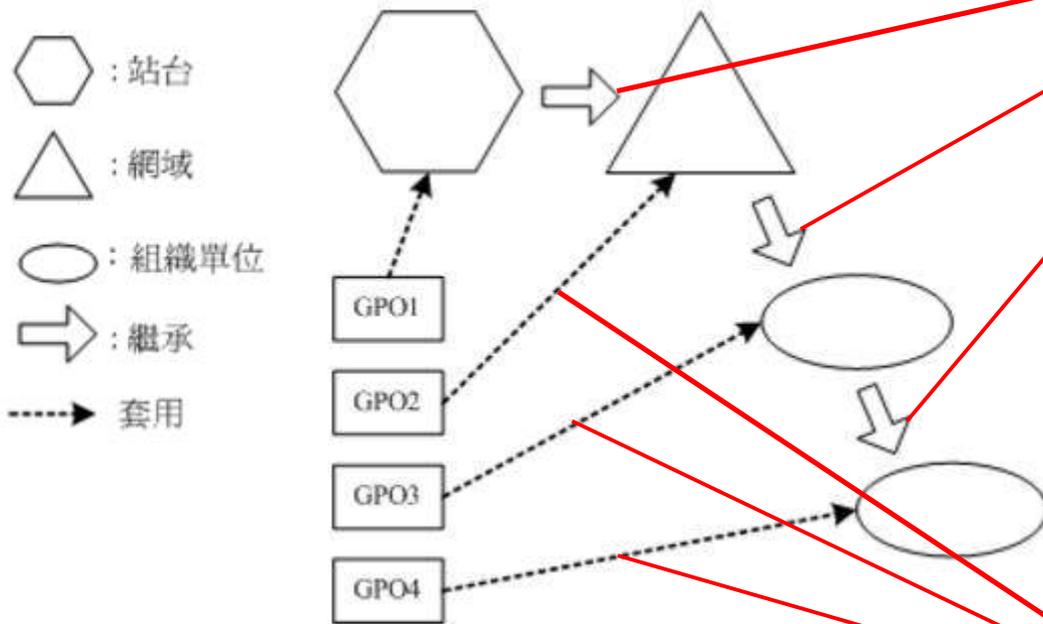
Active Directory 使用者和電腦

檔案(F) 執行(A) 檢視(V) 說明(H)

名稱	類型
Win10x64-MAC	電腦
WIN2012-MAC	電腦
Win7x64-MBP7	電腦
Win81-MAC	電腦
WS2008R2-SP1	電腦

AD群組原則特性

• 繼承 (Inheritance)



先繼承

當上層的組態設定項目與下層不同時，有效群組原則是上下層的聯集；若是對同一項目做不同的設定，則先套用的原則（上層原則）會被後套用的原則（下層原則）覆蓋。

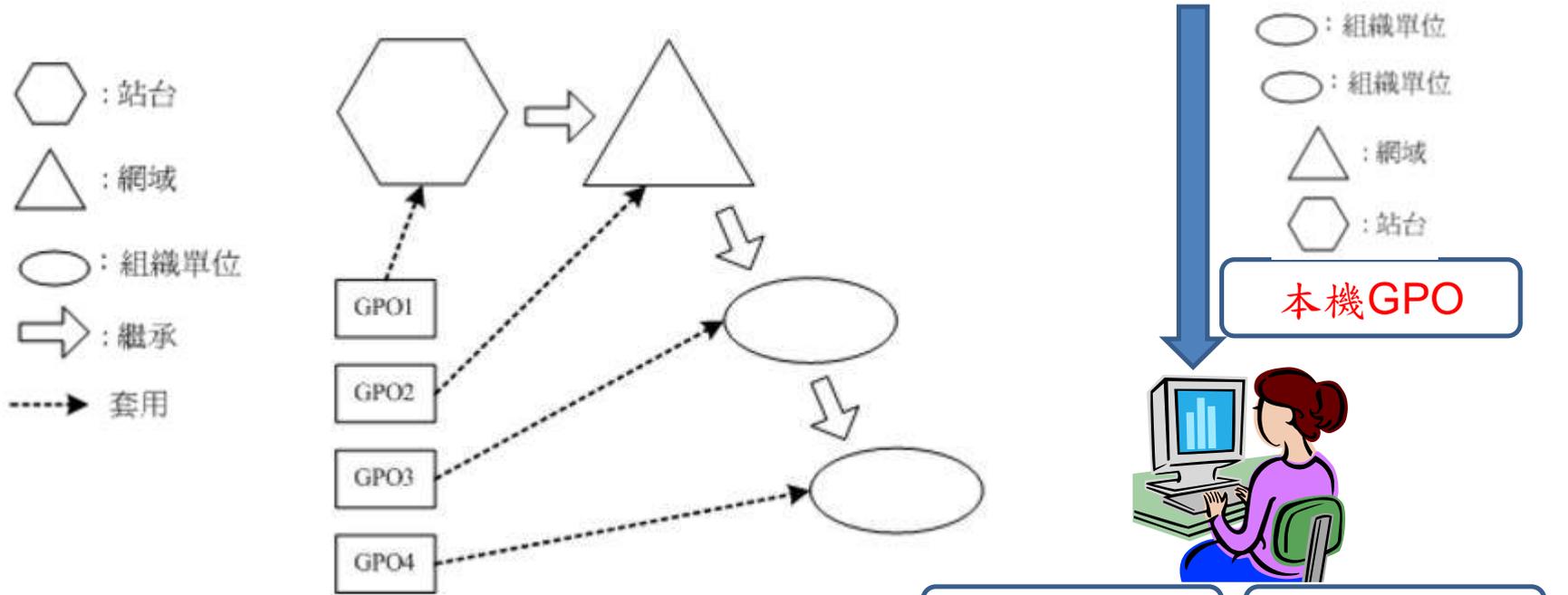
後累加

• 累加 (Cumulation)

GPO 套用優先順序

• 套用順序

— 本機 → 站台 → 網域 → 上層組織單位 → 下層組織單位



自動更新時間：
 預設為 90 分鐘 ± 隨機時間 (1~30 分鐘)
 手動更新：`gpupdate /force` 立即更新

電腦設定	使用者設定
重開機生效	使用者登入生效

**RSoP.msc (Gpedit.msc) 是
期望值，而非最終的結果！**

RSoP群組結果組

RSoP群組結果組(RSoP.msc)顯示GPO套用之期望值，而非最終結果！

The screenshot shows the RSoP.msc console with a list of Group Policy Objects (GPOs) and their application status. The '電腦設定 - 內容' (Computer Settings - Content) dialog box is open, displaying the following table:

群組原則物件	篩選
WMI遠端管理開放	已套用
Windows8.1AccountPolicy_20161202	已套用
本機群組原則	已套用
稽核原則	已停用 (GPO)
WindowsServer2008R2SP1ComputerSettings	已停用 (GPO)
Default Domain Controllers Policy	已停用 (GPO)

Below the table, there are checkboxes for filtering options:

- 顯示所有的 GPO 及篩選狀態(G)
- 顯示管理領域(M)
- 顯示修訂資訊(R)

Buttons for '安全性(S)...', '編輯(E)...', '確定', '取消', and '套用(A)' are also visible.

原則結果組報告(gpresult)

儲存路徑與檔名

`C:\Windows\system32>gpresult /h C:\GPO\RSoPresult.html /f` 強制覆寫

命令提示字元

指令 以HTML格式存報告

```

系統管理員: 命令提示字元 - gpresult /h C:\gpo\RsoPresult.html /f
Microsoft Windows [版本 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpresult /h C:\gpo\RsoPresult.html /f

C:\Windows\system32>gpresult /h C:\gpo\RsoPresult.html /f

C:\Windows\system32>gpresult /h C:\gpo\RsoPresult.html /f
正在建立 WIN7-MAC5\barbet 的 RSOP 工作階段 ...
    
```



gpresult報告內容

電腦名稱與時間

使用者設定摘要

群組原則結果

WIN7X32-GCB-MAC\barbet 在 WIN7X32-GCB-MBP
資料收集: 2016/3/21 上午 11:50:53

摘要

電腦設定摘要

電腦名稱	WIN7X32-GCB-MBP
網域	Local
站台	(無)
上次群組原則處理時間	2016/3/21 上午 10:27:53

使用者設定摘要

一般

使用者名稱	WIN7X32-GCB-MAC\barbet
網域	Local
上次群組原則處理時間	2016/3/21 上午 10:27:53

群組原則物件

已套用的 GPO

名稱	連結位置	修訂
本機群組原則	Local	AD (4), Sysvol (0)

群組原則物件

已套用的 GPO

名稱	連結位置	修訂
本機群組原則	Local	AD (4), Sysvol (4)

被拒絕的 GPO

名稱	連結位置	拒絕理由
無		

被拒絕的 GPO

名稱	連結位置	拒絕理由
無		

群組原則套用時的安全性群組成員資格

Mandatory Label\系統強制制層級
Everyone
WIN7X32-GCB-MBP\SQLServer\MSSQLServer\ADHelperUser\EA RBET546C90E
BUILTIN\Users
NT AUTHORITY\SERVICE
登入主控台
NT AUTHORITY\Authenticated Users
NT AUTHORITY\This Organization
NT SERVICE\BDESVC
NT SERVICE\BITS
NT SERVICE\CertPropSvc
NT SERVICE\EapHost
NT SERVICE\hkmsvc
NT SERVICE\KEXEEX
NT SERVICE\iphlpsvc
NT SERVICE\...
NT SERVICE\...

電腦設定

原則

Windows 設定
安全性設定
公開金鑰原則\憑證服務用戶端 - 自動註冊設定

原則	設定	優勢 GPO
自動憑證管理	啟用	[預設設定]
選項	設定	
註冊新憑證，更新到期的憑證、處理擱置的憑證要求並移除撤銷的憑證	停用	
更新和管理使用 Active Directory 中憑證範本的憑證	停用	

WMI遠端RSOP 摘要

群組原則管理 樹系: radiant-tech.com.tw 群組原則結果\WIN2012-MAC 的 barbet546

WIN2012-MAC 的 barbet546

摘要 設定 原則事件

群組原則結果

RADIANT-TECH\barbet546 在 RADIANT-TECH\WIN2012-MAC

資料收集: 2016/3/9 上午 02:38:39

摘要 全部隱藏 隱藏

電腦設定摘要 隱藏

一般 隱藏

電腦名稱	RADIANT-TECH\WIN2012-MAC
網域	radiant-tech.com.tw
站名	
上次群組原則處理時間	2016/3/9 上午 02:31:57

群組原則物件 隱藏

已套用的 GPO 隱藏

名稱	連結位置	修訂
Local Group Policy	Local	AD (6), Sysvol (6)
WMI遠端管理開放	radiant-tech.com.tw/Radiant_HQ	AD (1), Sysvol (1)
USGCB IE8 Computer Settings	radiant-tech.com.tw/Radiant_HQ	AD (1), Sysvol (1)
USGCB Win7 Firewall Settings	radiant-tech.com.tw/Radiant_HQ	AD (19), Sysvol (19)
USGCB Win7 Computer Settings	radiant-tech.com.tw/Radiant_HQ	AD (26), Sysvol (26)
USGCB Win7 Computer Energy	radiant-tech.com.tw/Radiant_HQ	AD (1), Sysvol (1)
USGCB Account Policy	radiant-tech.com.tw/Radiant_HQ	AD (1), Sysvol (1)
WMI遠端管理開放	radiant-tech.com.tw	AD (1), Sysvol (1)

被拒絕的 GPO 隱藏

名稱	連結位置	拒絕理由
{31B2F340-016D-11D2-945F-00C04FB964F9}	radiant-tech.com.tw	無法存取
{1F161802-A9D0-4FF4-8CCA-916C3D711F5F}	radiant-tech.com.tw/Radiant_HQ	無法存取

WMI遠端RSOP設定值

群組原則管理 樹系: radiant-tech.com.tw \群組原則結果\WIN2012-MAC 的 barbet546

WIN2012-MAC 的 barbet546

摘要 設定 原則事件

群組原則結果

RADIANT-TECH\barbet546 在 RADIANT-TECH\WIN2012-MAC

資料收集: 2016/3/9 上午 02:38:39

全部隱藏

電腦設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 隱藏

原則	設定	優勢 GPO
使用可還原的加密來存放密碼	停用	USGCB Account Policy
密碼必須符合複雜性需求	啟用	USGCB Account Policy
密碼長度最小值	12 個字元	USGCB Account Policy
密碼最長使用期限	60 天	USGCB Account Policy
密碼最短使用期限	1 天	USGCB Account Policy
強制密碼歷程記錄	已記憶 24 個密碼	USGCB Account Policy

帳戶原則/帳戶鎖定原則 隱藏

原則	設定	優勢 GPO
重設帳戶鎖定計數器的時間	15 分	USGCB Account Policy
帳戶鎖定期間	15 分	USGCB Account Policy
帳戶鎖定閾值	5 次無效的登入嘗試	USGCB Account Policy

本機原則/使用者權限指派 隱藏

原則	設定	優勢 GPO
允許本機登入	Administrators, Users	USGCB Win7 Computer Settings
允許透過終端機服務登入	Remote Desktop Users, Administrators	USGCB Win7 Computer Settings
以批次工作登入		USGCB Win7 Computer Settings
以服務方式登入		USGCB Win7 Computer Settings
同步處理目錄服務資料		USGCB Win7 Computer Settings
在驗證後模擬用戶端	Administrators, LOCAL SERVICE, NETWORK SERVICE	USGCB Win7 Computer Settings

本機gresult report

群組原則結果

RADIANT-TECH\barbet546

資料收集: 2017/1/16 上午 01:08:08

摘要

電腦設定摘要

沒有可用的資料。

使用者設定摘要

一般

使用者名稱
網域
上次群組原則處理時間

群組原則物件

已套用的 GPO

名稱	連結位置
本機群組原則	Local
TWGCB Account Policy	radiant-tech.com.tw
軟體派送(電腦軟體安裝)	radiant-tech.com.tw/測試區
WMI遠端管理開放	radiant-tech.com.tw

被拒絕的 GPO

名稱	連結位置
GCB_IE11_User_Settings	radiant-tech.com.tw/測試區
GCB_IE11_Computer_Settings	radiant-tech.com.tw/測試區
Windows8.1UserSettings	radiant-tech.com.tw/測試區
Windows8.1FirewallSetting	radiant-tech.com.tw/測試區
Windows8.1ComputerSettings(Other)	radiant-tech.com.tw/測試區
Windows8.1Computer_Settings_AuditSettings	radiant-tech.com.tw/測試區
Windows8.1AccountPolicy	radiant-tech.com.tw/測試區

WIN7X64-MAC 的 barbet546

摘要 設定 原則事件

群組原則結果

RADIANT-TECH\barbet546 在 RADIANT-TECH\WIN7X64-MAC
資料收集: 2017/1/16 上午 01:06:51

電腦設定

原則

軟體設定

Windows 設定

安全性設定

帳戶原則/密碼規則

原則	設定	優勢 GPO
使用可還原的加密來存放密碼	停用	TWGCB Account Policy
密碼必須符合複雜性需求	啟用	TWGCB Account Policy
密碼長度最小值	9 個字元	TWGCB Account Policy
密碼最長使用期限	90 天	TWGCB Account Policy
密碼最短使用期限	1 天	TWGCB Account Policy
強制密碼歷程記錄	已記憶 0 個密碼	TWGCB Account Policy

帳戶原則/帳戶鎖定原則

原則	設定	優勢 GPO
重設帳戶鎖定計數器的時間	15 分	TWGCB Account Policy
帳戶鎖定期間	15 分	TWGCB Account Policy
帳戶鎖定閾值	5 次無效的登入嘗試	TWGCB Account Policy

具有進階安全性的 Windows 防火牆

全域設定

原則	設定	優勢 GPO
原則版本	2.10	本機群組原則
停用可設定狀態的 FTP	未設定	
停用可設定狀態的 PPTP	未設定	
IPsec 豁免	未設定	
經過 NAT 的 IPsec	未設定	
預先共用金鑰編碼	未設定	
SA 閒置時間	未設定	
強式 CRL 檢查	未設定	

元件狀態資訊

WIN7X64-MAC 的 barbet546

摘要 設定 原則事件

群組原則結果

RADIANT-TECH\barbet546 在 RADIANT-TECH\WIN7X64-MAC
資料收集: 2017/1/16 上午 01:06:51

電腦設定

原則

軟體設定

Windows 設定

安全性設定

帳戶原則/密碼規則

原則	設定	優勢 GPO
使用可還原的加密來存放密碼	停用	TWGCBAccount Policy
密碼必須符合複雜性需求	啟用	TWGCBAccount Policy
密碼長度最小值	9 個字元	TWGCBAccount Policy
密碼最長使用期限	90 天	TWGCBAccount Policy
密碼最短使用期限	1 天	TWGCBAccount Policy
強制密碼歷程記錄	已記憶 0 個密碼	TWGCBAccount Policy

帳戶原則/帳戶鎖定原則

原則	設定	優勢 GPO
重設帳戶鎖定計數器的時間	15 分	TWGCBAccount Policy
帳戶鎖定期間	15 分	TWGCBAccount Policy
帳戶鎖定閾值	5 次無效的登入嘗試	TWGCBAccount Policy

具有進階安全性的 Windows 防火牆

全域設定

原則	設定	優勢 GPO
原則版本	2.10	本機群組原則
停用可設定狀態的 FTP	未設定	
停用可設定狀態的 PPTP	未設定	
IPsec 豁免	未設定	
經過 NAT 的 IPsec	未設定	
預先共用金鑰編碼	未設定	

元件狀態

元件名稱	狀態	上次處理時間
群組原則基礎結構	成功	2017/1/15 下午 11:59:41
Security	成功	2016/1/29 上午 01:24:04
Software Installation	成功	2016/1/29 上午 01:24:04
登錄	成功	2016/1/29 上午 01:24:03

GCB Doctor 檢測結果

4MOSAn GCB Doctor (GCB Configuration & Check)

檔案 掃描 工具 組態 備份檔 語言 說明

Host Status Account Policy **Computer Settings** User Settings Firewall Settings Internet Explorer Google Chrome Security Patches

項次	Computer Settings	說明	結果
10	安全性選項\Microsoft 網路用戶端	Microsoft 網路用戶端：傳送未加密的密碼到其他廠商的 SMB 伺服器	PASS
11	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章用戶端的通訊(如果伺服器同意)	PASS
12	安全性選項\Microsoft 網路用戶端	Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)	FAIL
13	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：伺服器 SPN 目標名稱驗證層級	FAIL
14	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章伺服器的通訊(自動)	PASS
15	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)	PASS
16	安全性選項\Microsoft 網路伺服器	Microsoft 網路伺服器：暫停工作階段前，要求的閒置時間	PASS
17	安全性選項\Microsoft 網路伺服器	網路伺服器：當登入時數到期時，中斷用戶端連線	PASS
18	安全性選項\MSS	MSS：[NoDefaultExempt] Configure IPSec exemptions for various types of network traffic	FAIL
19	安全性選項\MSS	MSS：[KeepAliveTime] How often keep-alive packets are sent in milliseconds	FAIL
20	安全性選項\MSS	MSS：[TcpMaxDataRetransmissions] How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	FAIL
21	安全性選項\MSS	MSS：[EnableICMPRedirect] Allow ICMP redirects to override OSPF generated routes	PASS
22	安全性選項\MSS	MSS：[Hidden] Hide computer from the browse list (Not Recommended except for highly secure environments)	FAIL
23	安全性選項\MSS	MSS：[DisableIPSourceRouting] IP source routing protection level (protects against packet spoofing)	FAIL
24	安全性選項\MSS	MSS：[DisableIPSourceRouting IPv6] IP source routing protection level (protects against packet spoofing)	FAIL
25	安全性選項\MSS	MSS：[NoNameReleaseOnDemand] Allow the computer to ignore NetBIOS name release requests except from WINS servers	FAIL
26	安全性選項\MSS	MSS：[TcpMaxDataRetransmissions IPv6] How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	FAIL
27	安全性選項\MSS	MSS：[PerformRouterDiscovery] Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	FAIL
28	安全性選項\MSS	MSS：[AutoReboot] Allow Windows to automatically restart after a system crash (recommended except for highly secure environmen	FAIL
29	安全性選項\MSS	MSS：[WarningLevel] Percentage threshold for the security event log at which the system will generate a warning	FAIL
30	安全性選項\MSS	MSS：[SafeDllSearchMode] Enable Safe DLL search mode (recommended)	FAIL
31	安全性選項\MSS	MSS：[AutoAdminLogon] Enable Automatic Logon (not recommended)	PASS
32	安全性選項\MSS	MSS：[AutoShareServer] Enable Administrative Shares (recommended except for highly secure environments)	FAIL
33	安全性選項\MSS	MSS：[ScreenSaverGracePeriod] The time in seconds before the screen saver grace period expires (0 recommended)	FAIL
34	安全性選項\互動式登入	互動式登入：在密碼到期前提示使用者變更密碼	PASS
35	安全性選項\互動式登入	互動式登入：要求網域控制站驗證以解除鎖定工作站	FAIL
36	安全性選項\互動式登入	互動式登入：網域控制站無法使用時，要快取的先前登入次數	FAIL

選擇上方資訊列可檢視內容描述

IP [192.168.1.18] Scan complete 全部檢測完畢... 100%

套用與實際不符合案例

區分 檢測數	Account Policy 9	Computer Settings 223	User Settings 8	Firewall Settings 35	Internet Explorer 154	Google Chrome 30	總檢測數 459	合格頂數	合格比率
IP 位址	Account Policy	Computer Settings	User Settings	Firewall Settings	Internet Explorer	Google Chrome	合格頂數	合格比率	
172.21.45.129	9	220	0	35	143	0	407	<input type="text" value="407"/>	89 %
172.21.63.192	9	220	0	35	143	0	407	<input type="text" value="407"/>	89 %
172.21.63.21	9	220	0	35	143	0	407	<input type="text" value="407"/>	89 %
172.21.63.175	9	220	0	35	143	0	407	<input type="text" value="407"/>	89 %
172.21.63.196	9	220	0	35	143	0	407	<input type="text" value="407"/>	89 %
172.21.63.31	9	219	0	35	143	0	406	<input type="text" value="406"/>	88 %
172.21.63.25	9	219	0	35	143	0	406	<input type="text" value="406"/>	88 %
172.21.66.19	9	220	6	35	3	0	273	<input type="text" value="273"/>	59 %
172.21.61.5	9	220	6	35	3	0	273	<input type="text" value="273"/>	59 %
172.21.67.43	9	220	6	35	3	0	273	<input type="text" value="273"/>	59 %
172.21.66.184	9	221	0	35	2	0	267	<input type="text" value="267"/>	58 %
172.21.63.16	9	220	0	35	2	0	266	<input type="text" value="266"/>	58 %
172.21.63.7	9	220	0	35	2	0	266	<input type="text" value="266"/>	58 %
172.21.62.16	9	220	0	35	2	0	266	<input type="text" value="266"/>	

套用與實際不符合案例

Windows 元件/Internet Explorer/網際網路控制合/安全性網頁受限制的網站區域

原則	設定
Java 檢視	啟用
Java 檢視	容許 Java
下載已簽署的 ActiveX 控制項	啟用
下載已簽署的 ActiveX 控制項	容許
下載未簽署的 ActiveX 控制項	禁用
下載未簽署的 ActiveX 控制項	容許
允許 Internet Explorer 網頁瀏覽器控制項的指令碼	禁用
Internet Explorer 網頁瀏覽器控制項	容許

Computer : 下載已簽署的 ActiveX 控制項 - 指定的網際網路區域	undefined	FAIL
Computer : JAVA 檢視 - 指定的網際網路區域	0	PASS
Computer : 僅允許批准的網域使用 ActiveX 控制項而且不提示 - 指定的網際網路區域	undefined	FAIL
Computer : 關閉 SmartScreen 防護工具掃描 - 指定的網際網路區域	undefined	FAIL
Computer : 允許在使用者電腦上執行 CD 的主動式內容	0	PASS

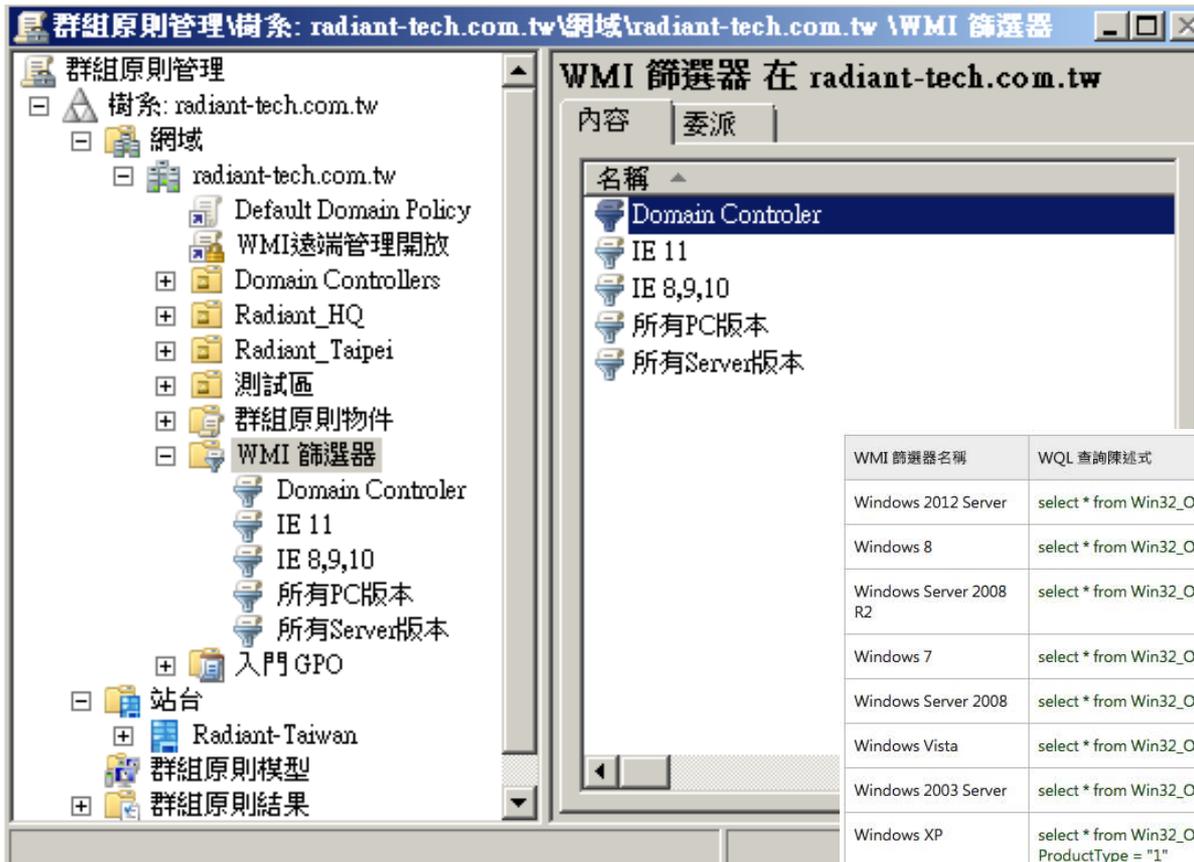
GPO如何套用至網域中 各種版本之OS及IE？

GPO of TWGCB

- TWGCB文件已發行:
 - Win7,Win8/(10)
 - IE8/(9,10),IE11,
 - Winserver2008 /(2012) AD
- 技服中心提供之GPO：
 - GCB-Windows7-gpos
 - Windows7AccountPolicy
 - Windows7ComputerSettings
 - Windows7FirewallSettings
 - Windows7UserSettings
 - GCB-IE8-gpos
 - InternetExplorer8ComputerSettings
 - InternetExplorer8UserSettings

WMI 篩選器應用

透過WMI篩選器可以在同一組織單位中，針對不同之作業系統或是IE版本，套用不同之GPO檔，以因應未來有更多之TWGCB範本頒佈套用。



WMI 篩選器名稱	WQL 查詢陳述式
Windows 2012 Server	select * from Win32_OperatingSystem where Version like "6.2%" and ProductType = "3"
Windows 8	select * from Win32_OperatingSystem where Version like "6.2%" and ProductType = "1"
Windows Server 2008 R2	select * from Win32_OperatingSystem where Version like "6.1%" and ProductType = "3"
Windows 7	select * from Win32_OperatingSystem where Version like "6.1%" and ProductType = "1"
Windows Server 2008	select * from Win32_OperatingSystem where Version like "6.0%" and ProductType = "3"
Windows Vista	select * from Win32_OperatingSystem where Version like "6.0%" and ProductType = "1"
Windows 2003 Server	select * from Win32_OperatingSystem where Version like "5.2%" and ProductType = "3"
Windows XP	select * from Win32_OperatingSystem where (Version like "5.1%" or Version like "5.2%") and ProductType = "1"

GCB Doctor 檢測項目

OS/Configuration	Item	Category
Win7+IE8+Chrome (項目: 420) v1.7	9	Account Policy
	223	Computer Settings
	8	User Settings
	35	Firewall Settings
	115	Internet Explorer
	30	Google Chrome
Win7+IE11+Chrome (項目: 459) v1.7	9	Account Policy
	223	Computer Settings
	8	User Settings
	35	Firewall Settings
	154	Internet Explorer
	30	Google Chrome
Win8.1+IE11+Chrome (項目: 518) v1.2	9	Account Policy
	279	Computer Settings
	13	User Settings
	33	Firewall Settings
	154	Internet Explorer
	30	Google Chrome
Win Server DC (項目: 332) v1.3	9	Account Policy
	302	Computer Settings
	21	Firewall Settings

GCB Doctor報告

4MOSA GCB 政府組態基準管理中心 2017-05-03 00:25:03

使用者: barbet
用戶管理 設定 登出

儀錶板 排程 軟體資產 報告 GCB 統計

單位主機列表 - [Radiant-Tech] 回單位列表

Windows 7 + IE8	Windows 7 + IE11	Windows 8/10 + IE11	WinServer 2008/2012 DC
主機名稱			
檢視	WIN-WELL-IE11-2	192.168.95.1	
檢視	9889-PC	172.20.10.5	

HTML 報表 PDF 報表 輸入備註

報表選項: 統計圖表 Account Policy Computer Settings User Settings Firewall Settings Internet Explorer

主機詳細資料 - [Radiant-Tech] WIN-Well-ie11-2.localdomain : 192.168.95.135 2017-05-02 18:10:14 回上一頁

組態名稱: 將檢測結果儲存為新組態 (可作為其他主機的組態範本或回溯主機組態設定)

檢測資訊 Account Policy(1/8) Computer Settings(71/152) Firewall Settings(0/35) Internet Explorer(1/153) User Settings(0/8) Google Chrome(0/30)

檢測資訊

合格率 (不含 Security Patches)

狀態	數量
合格	71
不合格	152
例外	0

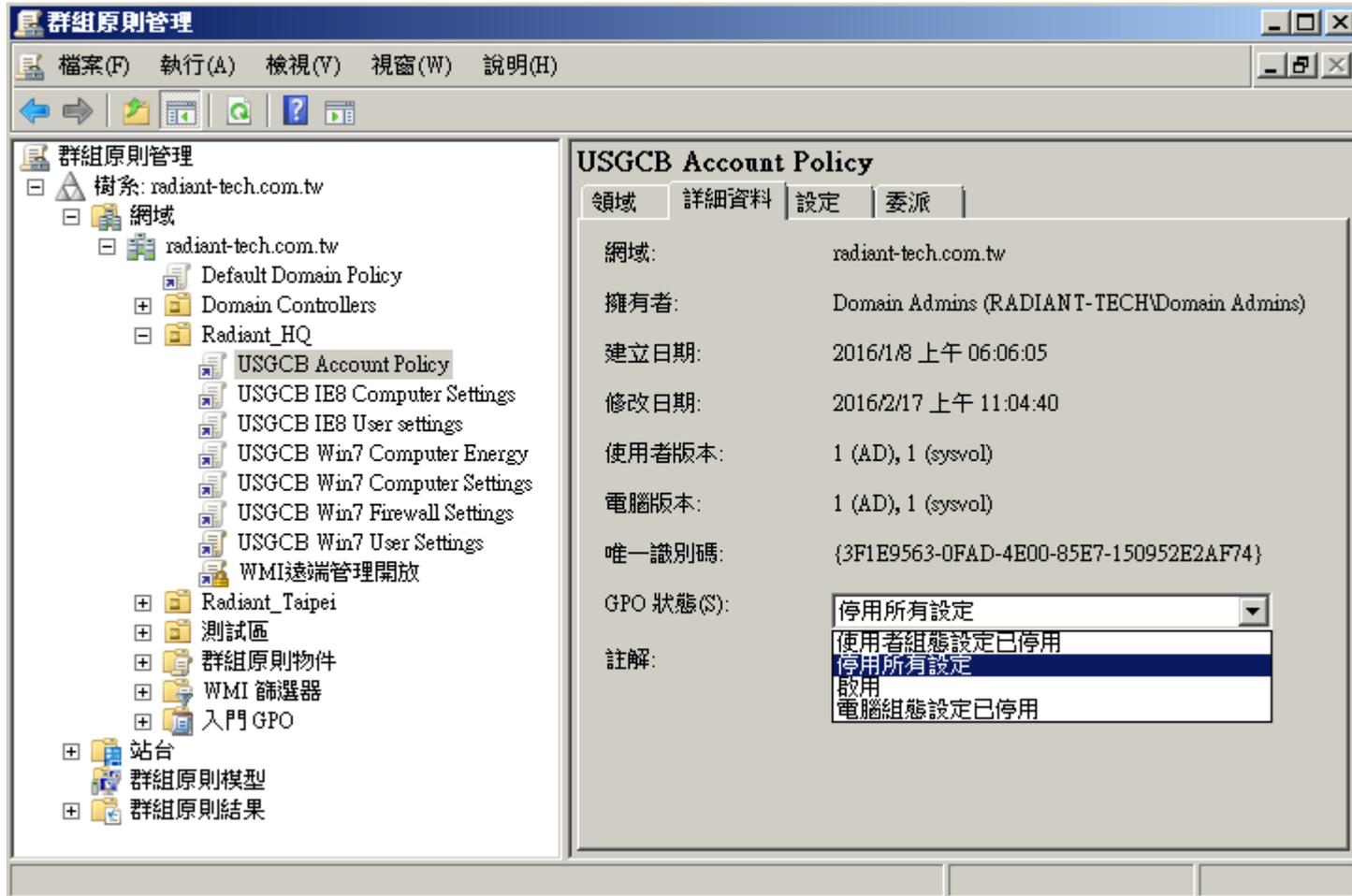
GPO 套用可以安全回復嗎？

LocalGPO復原作業

- 在LocalGPO工具的目錄下—執行cscript LocalGPO.wsf /Restore

```
C:\Windows\system32>cd "c:\Program Files\LocalGPO"  
c:\Program Files\LocalGPO>cscript LocalGPO.wsf /Restore  
Microsoft (R) Windows Script Host Version 5.0  
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.  
  
Modifying Local Policy... this process can take a few moments.  
  
Restoring Security Settings...  
Restoring Administrative Template settings...  
Restoring Advanced Audit Policy...  
Restoring MLGPO...  
Refreshing Local Group Policy...  
  
Local Policy default values restored!  
  
Please restart the computer to refresh the Local Policy  
  
c:\Program Files\LocalGPO>
```

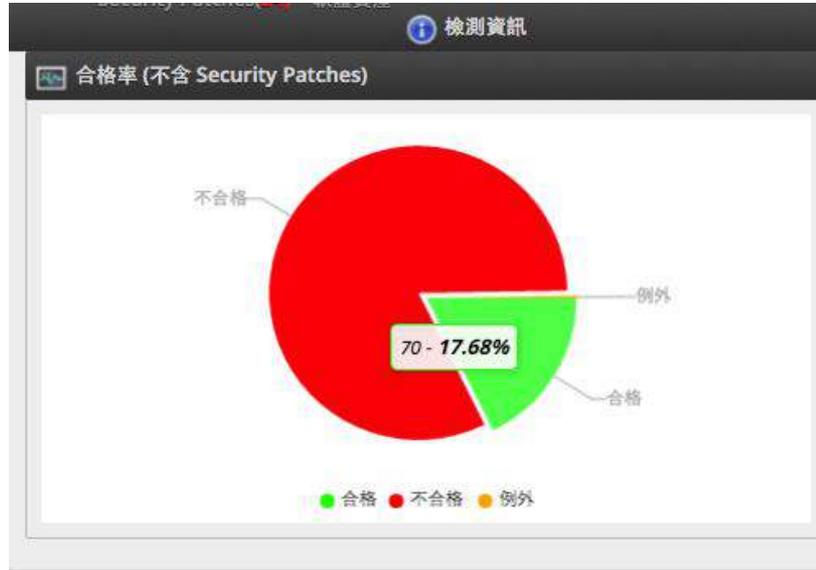
AD GPO 停用/復原



The screenshot shows the Group Policy Management console for the domain 'radiant-tech.com.tw'. The left pane displays a tree view of Group Policy Objects (GPOs) under the 'Radiant_HQ' container, with 'USGCB Account Policy' selected. The right pane shows the details for this GPO, including its domain, owner, creation and modification dates, and user/computer versions. The 'GPO 狀態(S):' dropdown menu is open, showing the current status as '停用所有設定' (Disabled All Settings).

領域	詳細資料	設定	委派
網域:	radiant-tech.com.tw		
擁有者:	Domain Admins (RADIANT-TECH\Domain Admins)		
建立日期:	2016/1/8 上午 06:06:05		
修改日期:	2016/2/17 上午 11:04:40		
使用者版本:	1 (AD), 1 (sysvol)		
電腦版本:	1 (AD), 1 (sysvol)		
唯一識別碼:	{3F1E9563-0FAD-4E00-85E7-150952E2AF74}		
GPO 狀態(S):	停用所有設定 使用者組態設定已停用 停用所有設定 啟用 電腦組態設定已停用		
註解:			

Local/ AD GPO套用無法完全復原



套用前



復原後

主機比對資料 - WIN-NGV69FEB4SA.localdomain : 172.16.197.130 (差異項目數量: 6)				
項次	GPO	原則設定名稱	2016-02-16 14-13-39	2016-02-16 15-07-59
10	Computer Energy Policy	關閉顯示器(使用電池)	FAIL	PASS
11	Computer Energy Policy	關閉顯示器(使用一般電源)	FAIL	PASS
12	Computer Energy Policy	指定系統休眠逾時(使用電池)	FAIL	PASS
13	Computer Energy Policy	指定系統休眠逾時(使用一般電源)	FAIL	PASS
97	Computer Settings	MSS : (AutoAdminLogon) Enable Automatic Logon (not recommended)	PASS	FAIL
111	Computer Settings	以服務方式登入	FAIL	PASS

網域內如何套用二種以上 Account Policy

精細密碼原則修訂

GPO在同一網域內，僅可以有一組密碼政策，若要有二套以上之密碼政策，則需要透過精細密碼原則，才可以達到要求。

● 已發展GCB之密碼原則對照

項次	項目名稱	原設定值	調整後之 Windows 7 設定值	調整後之 Windows 8.1 設定值	調整後之 Windows Server 2008 R2 設定值
1	密碼最長使用期限	60(天)	90(天)以下	90(天)以下	90(天)以下
2	最小密碼長度	12(碼)	8(碼)以上	8(碼)以上	12(碼)
3	強制執行密碼歷程記錄	24(次)	3(次)以上	3(次)以上	3(次)以上

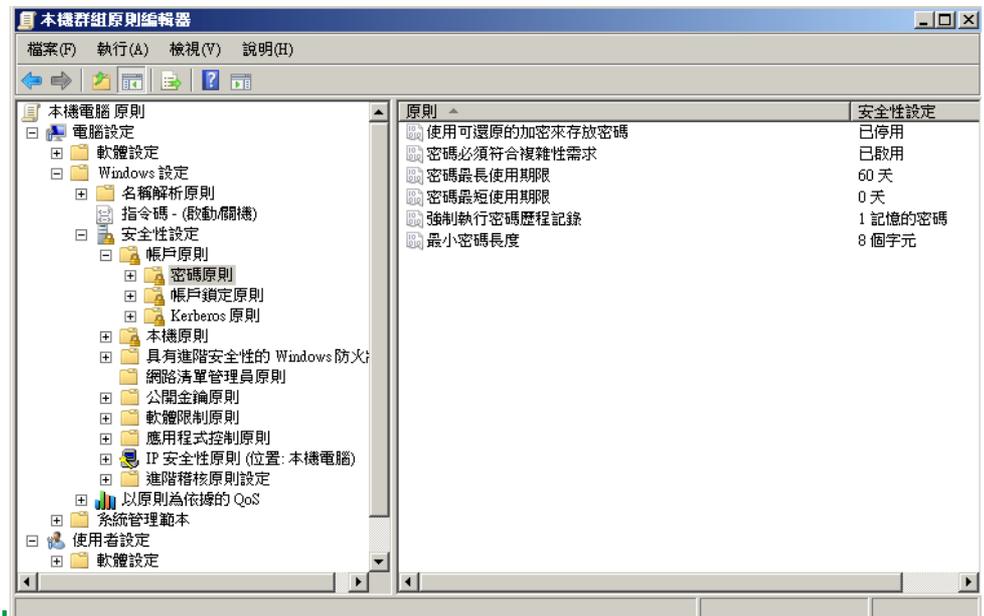
● 伺服器主機之最小密碼長度維持12個字元

– 將於各年度資安稽核時，針對網域控制站(DC)主機進行實際密碼長度設置符合12個字元之檢測

網域 Account Policy 設定

網域 Account Policy 設定之作用，群組原則管理，僅能套用至「網域」，不能套用至「組織單位」，但亦可套用於網域控制站之本機群組原則。

故原則上整個網域僅能有一組 Account Policy 設定值。若是不同之「組織單位」要套用不同之密碼原則，GPO 是無法達成的，必須利用精細密碼原則才可以。



精細密碼原則

- Windows Server 2008 AD以後版本，提供設定網域內的[使用者]與[群組]，採用不同的密碼原則之功能。
- 需要用到ADSI編輯器來建立及設定密碼物件 Password Setting objects (PSO)，
- 設定密碼原則屬性後，可套用至指定之「使用者」或「群組」，但是不能像GPO套用至OU。
- 設定上很繁瑣，需要有經驗之顧問協助
- 在Windows Server 2012 AD 可以利用Active Directory 管理中心，簡化精細密碼原則設定。

精細密碼原則設定

■ 密碼設定容區(Password Settings Container ; PSC)

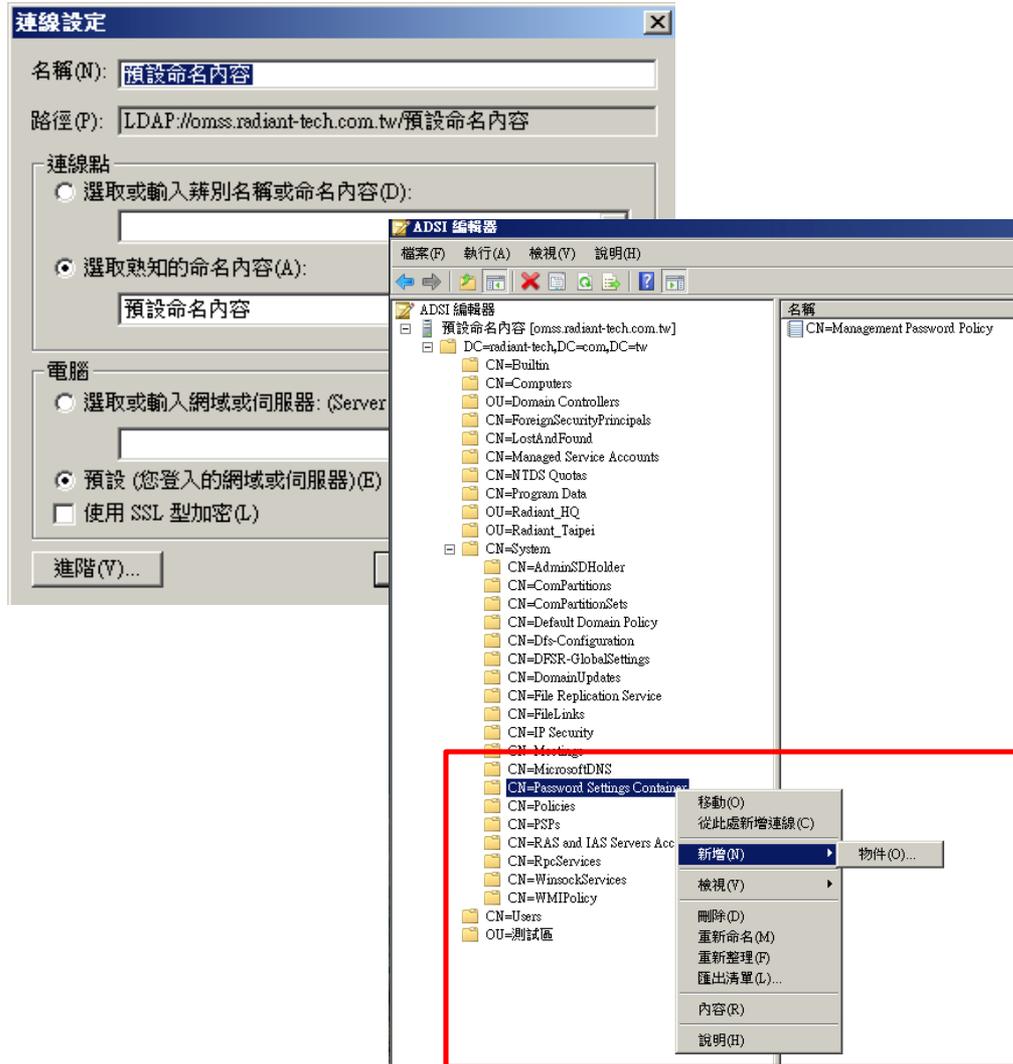
密碼設定容器(Password Settings Container,PSC)』物件類別預設會建立在網域的

『SYSTEM』容區底下，此容區用以儲存網域的密碼設定物件 (PSO)，你並無法重新命名、移動或刪除這個容器。

■ 密碼設定物件(Password Settings objects ; PSO)

PSO提供所有密碼原與鎖定原則的內容屬性，包括了密碼最短使用期限、密碼最長使用期限、最短密碼長度、帳戶鎖定閾值.....等，此外，它還包括了一個多值連結屬性(Multivalued link attribute)可將此PSO連結套用至使用者或群組，並且還有一個整數型類的優先值(precedence value)用以解決特定使用者或群組一旦被連結至多個PSO時所產生的衝突狀況。

ADSI編輯器創設PSO

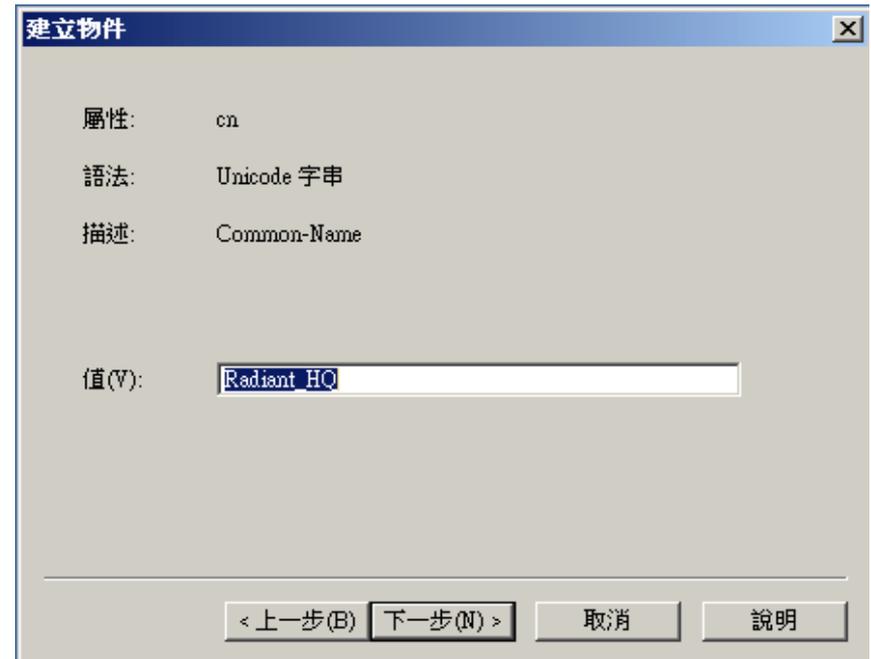
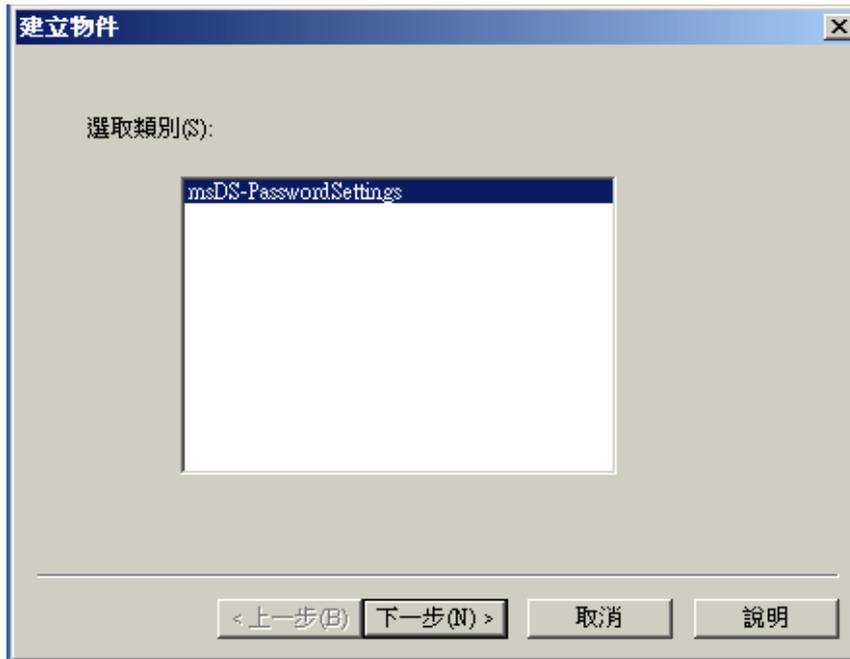


- 開啟ADSI編輯器(adsiedit.msc)
- 執行→連線到→預設命名內容
- DC=XXXX,DC=XXXX,DC=XX
→CN=System
→CN>Password Settings Container
→新增物件

Password Settings Container

建立 Password Settings Container 物件

設定物件名稱：「XXXXX」(字串)



最小密碼長度、最短使用期限

最小密碼長度，TWGCB針對Server之建議值為12，

密碼最短使用期限，GCB之建議值為1天
設定值：dd:hh:mm:ss (01:00:00:00)



建立物件

屬性: msDS-MinimumPasswordLength

語法: 整數

描述: Minimum Password Length for user accounts

值(V):

< 上一步(B) 下一步(N) > 取消 說明



建立物件

屬性: msDS-MinimumPasswordAge

語法: 持續時間

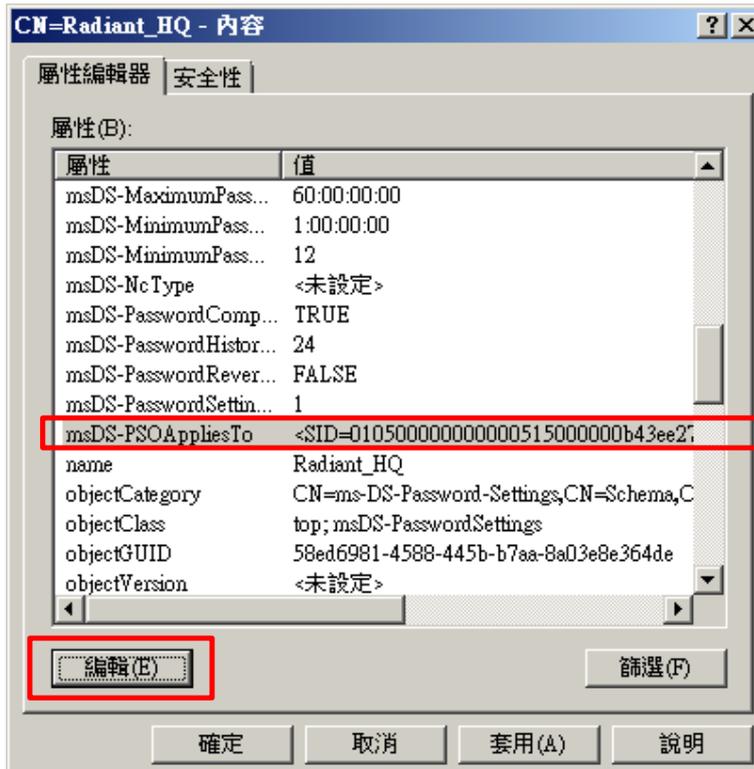
描述: Minimum Password Age for user accounts

值(V):

< 上一步(B) 下一步(N) > 取消 說明

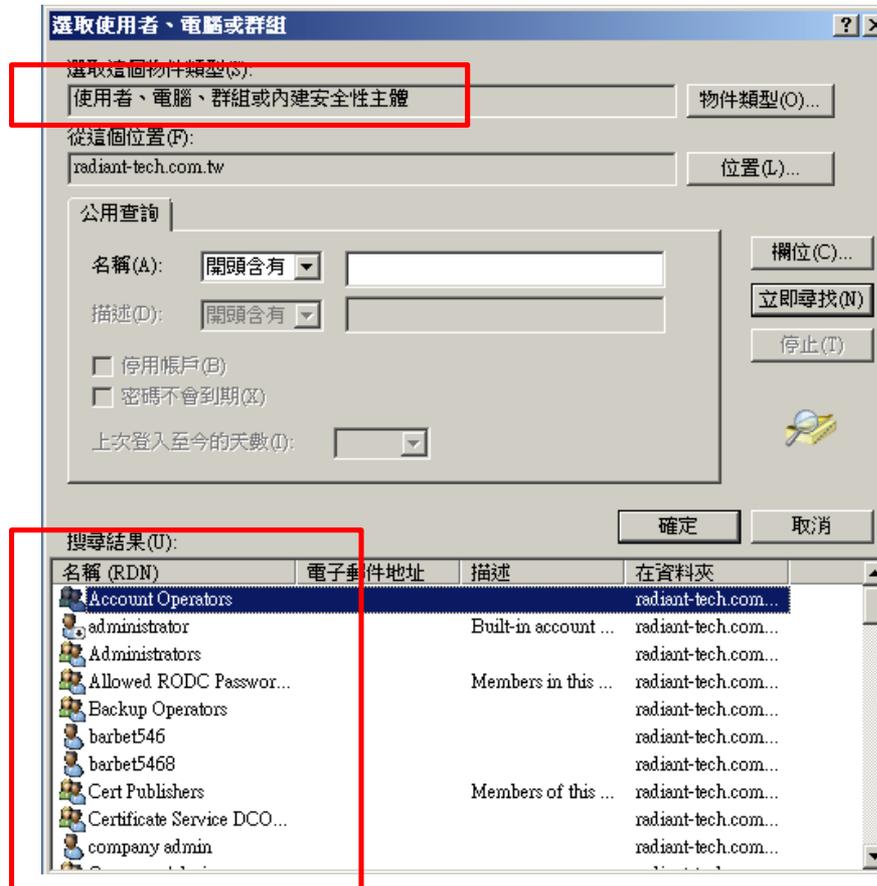
msDS-PSOAppliesTo 設定

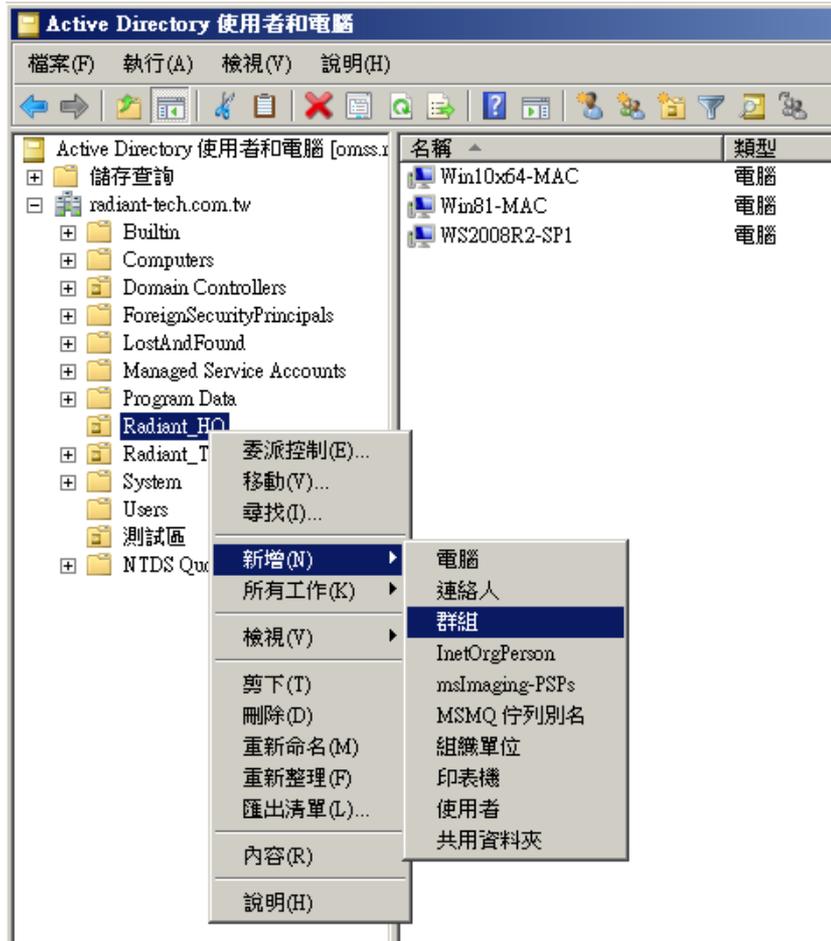
開啟PSO物件之內容，編輯msDS-PSOAppliesTo，套用至指定之「使用者」或「群組」。建議套用至所有的Administrators群組。但不要套用至Domain Users。



msDS-PSOAppliesTo

msDS-PSOAppliesTo只能套用於使用者、群組或電腦，
注意：並不能套用於組織單位(OU)



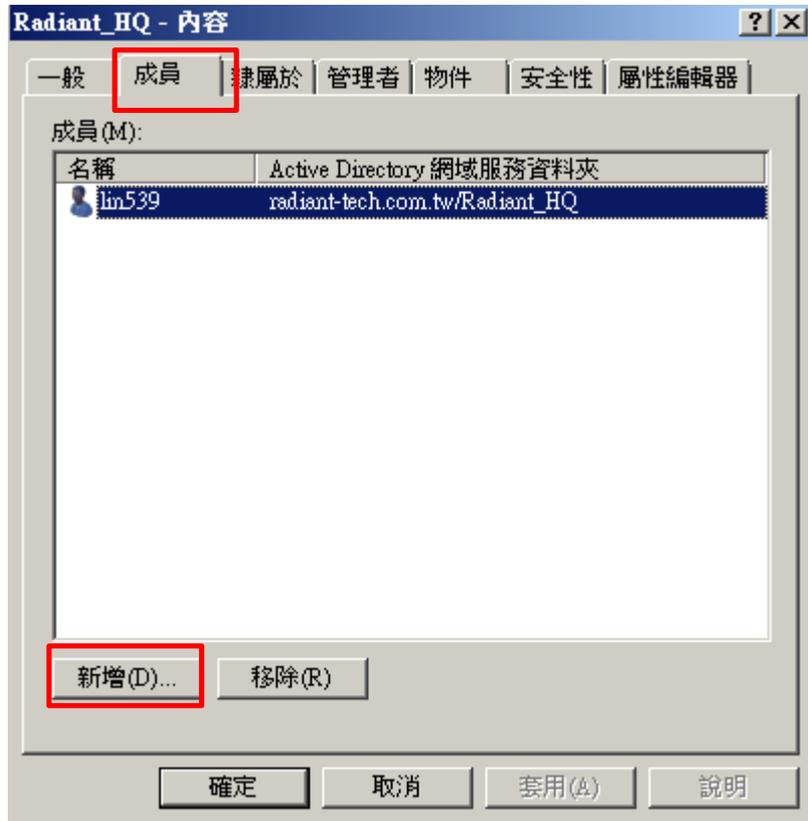


- 開啟AD使用者與電腦管理工具
- 在選定的「組織」→新增→群組
- 「群組名稱」建議與「組織單位」名稱相同

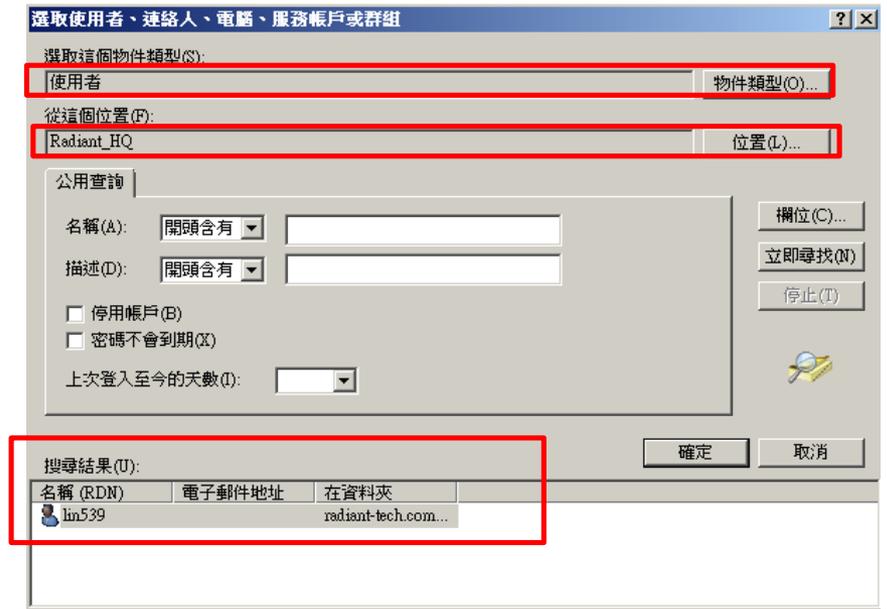


設定群組之成員

開啟群組內容，選取「成員」

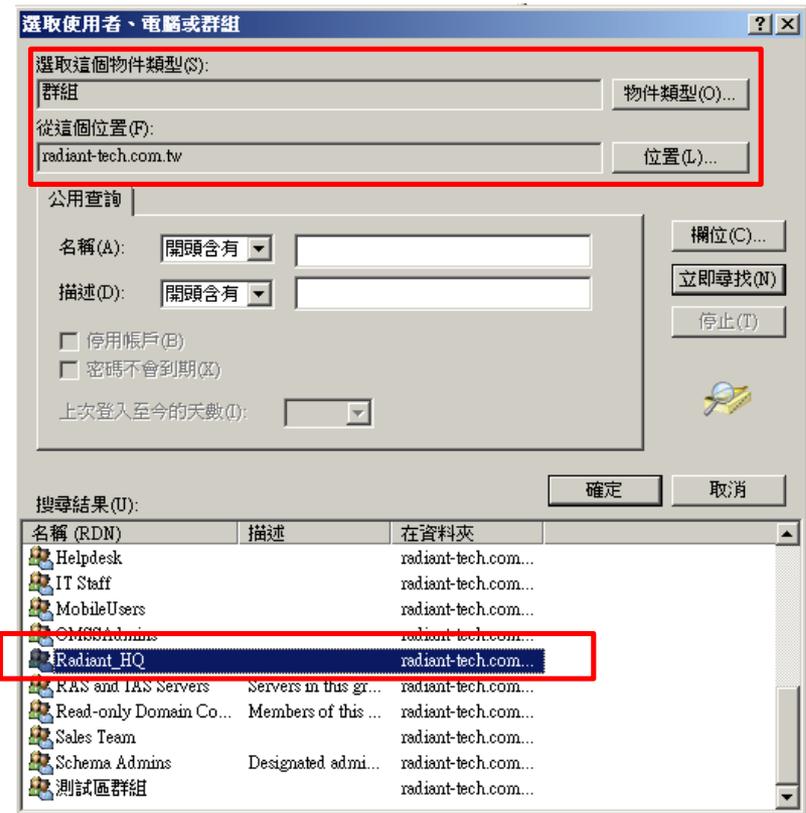
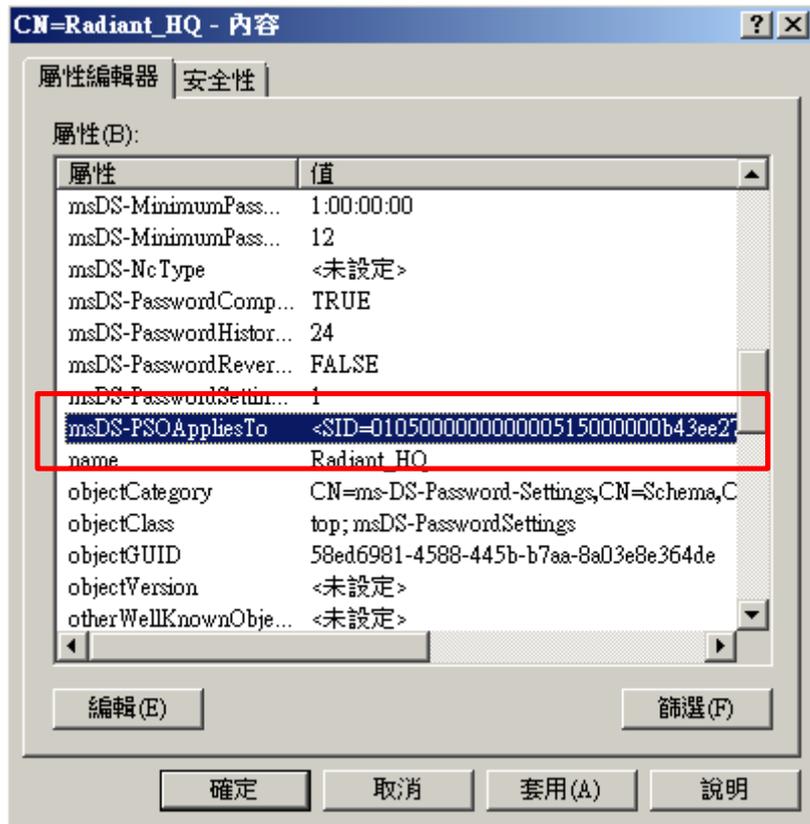


新增成員→物件類型：使用者→
位置：選定之組織單位
將所有隸屬於選定之「組織單位」
所有之使用者，加入在本群組中



msDS-PSOAppliesTo 指定群組

msDS-PSOAppliesTo Radiant_HQ



你可以有更SMART的方法！



請看 GCB Doctor 如何滿足您的需求！

4MOSAn GCB Doctor

4MOSAn GCB 政府組態基準管理中心

歡迎使用: barbet
2016-05-03 01:27:01

系統組態基準 V1.4 (共計: 670)

- Account Policy: 9
- Computer Energy Policy: 4
- Computer Settings: 473
- User Settings: 13
- Firewall Settings: 36
- Internet Explorer: 115

系統稽核狀態

- 1032 總稽核數量
- 40 合格稽核數量
- 8 稽核中數量
- 66 待稽核數量
- 25 已同意候檢主機
- 21 未同意候檢主機

系統稽核趨勢分析

HTML 報表 PDF 報表 輸入帳號

報表選擇: 統計圖表 Account Policy Computer Energy Policy Computer Settings User Settings Firewall Settings Internet Explorer Security Patches

主機詳細資料 - [Radiant-Tech] Win7-MAC2.radiant-tech.com.tw : 192.168.1.67 2016-05-03 00:51:15

組態名稱: [輸入名稱] 將檢測結果儲存為新組態

檢測資訊: Account Policy(9) Computer Energy Policy(4) Computer Settings(95/1/125) Firewall Settings(35) Internet Explorer(110/0) User Settings(0/0) Security Patches(7)

檢測結果

合格率 (不含 Security Patches)

合格 不合格 例外

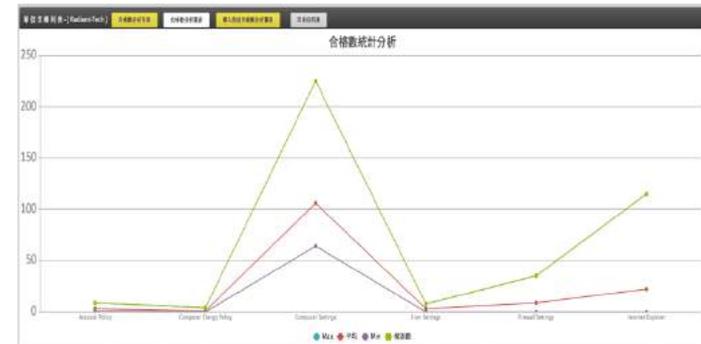
檢測時間: 2016-05-03 00:51:15 - 2016-05-03 00:51:28

- IP 位址: 192.168.1.67
- 主機名稱: Win7-MAC2.radiant-tech.com.tw
- MAC 位址: 00-1C-42-E3-41-85(2 Parallels, Inc.)
- 作業系統: Windows 7 Ultimate Service Pack 1 Build 7601
- NB 名稱: WIN7-MAC2
- NB 群組: RADIANT-TECH
- NB 作業系統: Windows 7 Ultimate Service Pack 1
- 使用者帳號: barbet546
- CPU 規格: Intel(R) Core(TM) i7-3615QM CPU @ 2.30GHz
- RAM 規格: 2,048 MBytes
- IE 版本: IE8
- 防毒軟體名稱: Microsoft Security Essentials (Ver: 4.8.204.0) Up to date
- 程式版本: 4.1.5.1
- 程式 SHA-256: B56DA325A1E230B5155BF30D1282A29C386A41AD5265033B8ED5DA4999CFDE5F3
- 資料更新: 2016-04-14
- 不合格項目: 142 (不含 Security Patches)
- 備註:

4MOSAn GCB Doctor (GCB Configuration & Check)

系統資訊

- IP 位址: 192.168.1.67
- MAC 位址: 00-1C-42-E3-41-85 (2: Parallels, Inc.)
- 主機名稱: Win7-MAC2.radiant-tech.com.tw
- 使用者帳號: barbet546
- CPU 規格: Intel(R) Core(TM) i7-3615QM CPU @ 2.30GHz
- RAM 規格: 2,048 MBytes
- 作業系統: Windows 7 Ultimate Service Pack 1 Build 7601
- 作業系統名稱: Windows 7 Ultimate Service Pack 1 Build 7601
- 作業系統版: Windows 7 Ultimate Service Pack 1
- NetBIOS 名稱: Win7-MAC2
- NetBIOS 群組: RADIANT-TECH
- NetBIOS 作業系統: Windows NT 6.1
- 作業系統: Windows
- 作業系統: Windows



組態套用至全機關

指定組態套用至全機關

4MOSA GCB 政府組態基準管理中心 2017-05-03 01:12:42

使用者: barbet
用戶管理 設定 登出

儀錶板 排程 軟體資產 報告 GCB 統計 健診統計 組態

[組態] 單位組態設定 - [Radiant-Tech] 回單位列表

Windows 7 + IE8 Windows 7 + IE11 Windows 8/10 + IE11 WinServer 2008/2012 DC

Windows 7 + IE11 WIN7_IE11_10604014_V 變更下列全部主機的組態 搜尋 IP:

組態列表 + 新增組態 (Windows 7 + IE11) 例外項目 (Windows 7 + IE11)

名稱	IP	群組
WIN-WIN7-I11	192.168.95.133	WORKGROUP

指定組態套用至個別主機

組態	狀態	動作
未設定		
✓ WIN7_IE11_null	2017-03-28 13:43 套用	未驗證
WIN7_IE11_1060407V		
WIN7_IE11_10604014_V	2017-05-02 18:15 套用	未驗證
WIN7_IE11_all_v		
WIN7_IE11_EX		
WIN7_IE11_ALL		
未設定	未指定	
	未指定	

例外組態管理

4MOSAN GCB 政府組態基準管理中心 2017-05-03 01:10:59

使用者: barbet 用戶管理 設定 登出

儀錶板 排程 軟體資產 報告 GCB 統計 健診統計 組態 電腦列表 維護 說明

[組態] 設定 組態例外項目 - [適用於全機關] 回組態設定 儲存例外項目 版本: Windows 7 + IE8

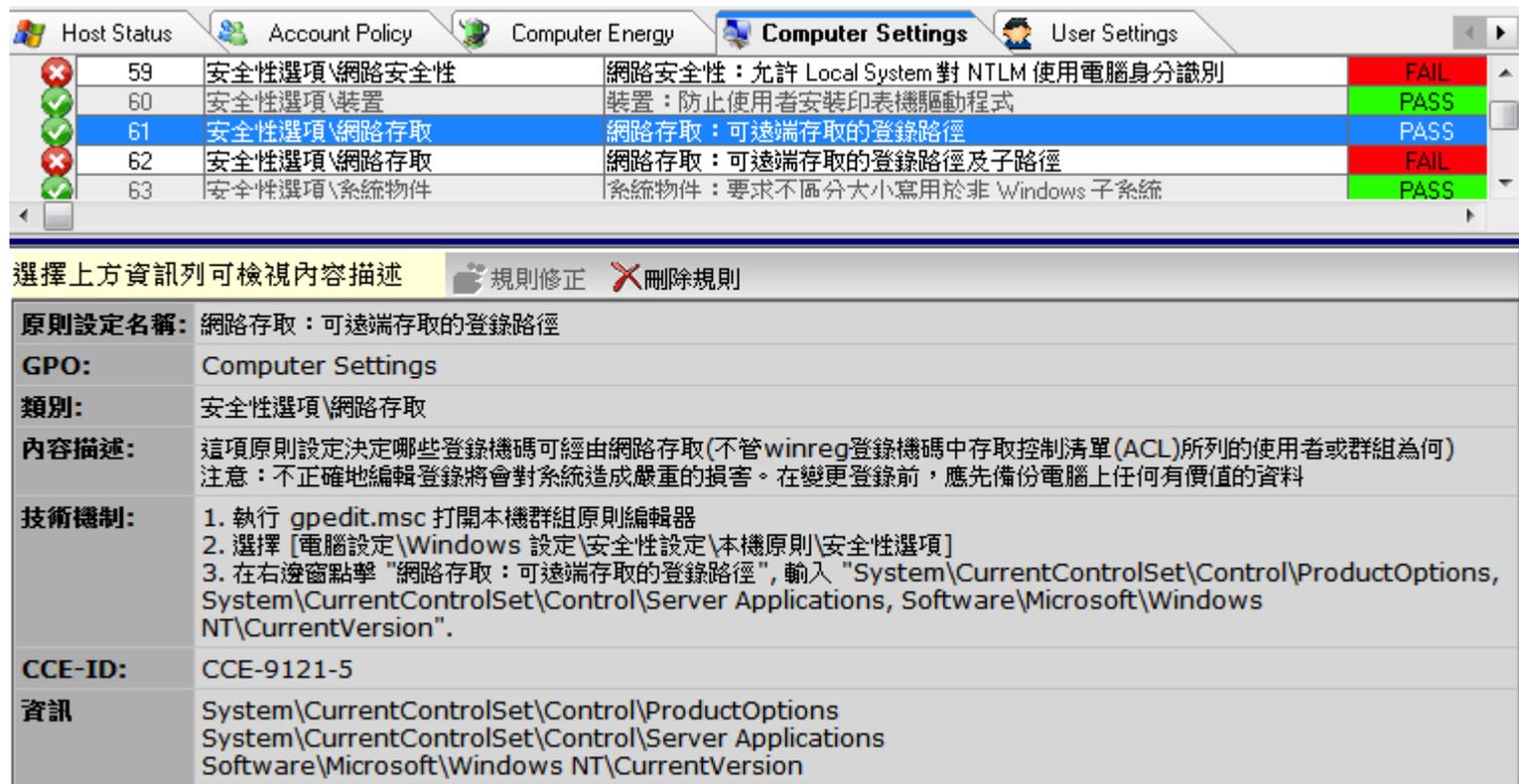
Account Policy(9) Computer Energy Policy(4) Computer Settings(8) User Settings(0) Firewall Settings(0) Internet Explorer(0) Google Chrome(0) 幫助

應用程式	影響項次
<ul style="list-style-type: none"> ● 二代健保補充保費系統 ● 自然輸入法 V10 ● "全景" 影像檔管系統 ● 觀看 HTTPS 網址之 YouTube 影片 	系統加密編譯: Use FIPS 140 相容加密演算法, 包括加密、雜湊以及簽署演算法
<ul style="list-style-type: none"> ● 人事管理資訊系統 (pemis2k) 	Computer Settings - 使用者帳戶控制: 在管理員核准模式, 系統管理員之提升權限提示的行為 Computer Settings - 使用者帳戶控制: 標準使用者之提升權限提示的行為 Computer Settings - 使用者帳戶控制: 偵測應用程式安裝, 並提示提升權限 Computer Settings - 使用者帳戶控制: 所有系統管理員均以管理員核准模式執行 Computer Settings - 使用者帳戶控制: 僅針對在安全位置安裝的 UIAccess 應用程式, 提高其權限 Computer Settings - 使用者帳戶控制: 將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置 Computer Settings - 使用者帳戶控制: 使用內建的 Administrator 帳戶的管理員核准模式 Computer Settings - 使用者帳戶控制: 提示提升權限時切換到安全桌面
<ul style="list-style-type: none"> ● Adobe Acrobat Professional 	Computer Settings - 禁止非系統管理員套用廠商簽署的更新
<ul style="list-style-type: none"> ● 遠端桌面連線 	Computer Settings - 允許使用者使用遠端桌面服務從遠端連線
<ul style="list-style-type: none"> ● 遠端 VDI 連線 VMware Horizon View 	Computer Settings - 拒絕透過遠端桌面服務登入 Computer Settings - 停用遠端桌面共用 Computer Settings - 允許遠端存取隨插即用介面 Computer Settings - 允許使用者使用遠端桌面服務從遠端連線 Firewall Settings - 網域設定檔: 套用本機防火牆規則 Firewall Settings - 網域設定檔: 套用本機連線安全性規則 Firewall Settings - 私人設定檔: 套用本機防火牆規則 Firewall Settings - 私人設定檔: 套用本機連線安全性規則 Firewall Settings - 共用設定檔: 套用本機防火牆規則 Firewall Settings - 共用設定檔: 套用本機連線安全性規則
<ul style="list-style-type: none"> ● 連接其他電腦的網路共享資料夾 	Computer Settings - Microsoft 網路用戶端: 數位簽署用戶端的通訊(自動)
<ul style="list-style-type: none"> ● 提供網路共享資料夾給其他電腦連接 - 發生: 網路旁鄰共用磁碟機無法連線 	Computer Settings - 從網路存取這台電腦
<ul style="list-style-type: none"> ● Internet Explorer 相關作業需要新增信任網站 - 發生: 網站有加入信任網站但是開啟卻一直顯示 "請加入信任網站" 	Internet Explorer - Computer: 安全性區域: 不允許使用者新增與移除網站 Internet Explorer - Computer: 安全性區域: 不允許使用者變更原則 Internet Explorer - Computer: 安全性區域: 只使用電腦設定

分散式弱點掃描與管理

網路存取：可遠端存取的登錄路徑

Windows 在 Vista 之後(包含Win7/Server2008) ， Remote Registry 預設為 LocalService 啟動，導致無法由遠端進行檢測



Host Status	Account Policy	Computer Energy	Computer Settings	User Settings
59	安全性選項\網路安全性	網路安全性：允許 Local System 對 NTLM 使用電腦身分識別	FAIL	
60	安全性選項\裝置	裝置：防止使用者安裝印表機驅動程式	PASS	
61	安全性選項\網路存取	網路存取：可遠端存取的登錄路徑	PASS	
62	安全性選項\網路存取	網路存取：可遠端存取的登錄路徑及子路徑	FAIL	
63	安全性選項\系統物件	系統物件：要求不區分大小寫用於非 Windows 子系統	PASS	

選擇上方資訊列可檢視內容描述 規則修正 刪除規則

原則設定名稱：	網路存取：可遠端存取的登錄路徑
GPO：	Computer Settings
類別：	安全性選項\網路存取
內容描述：	這項原則設定決定哪些登錄機碼可經由網路存取(不管winreg登錄機碼中存取控制清單(ACL)所列的使用者或群組為何) 注意：不正確地編輯登錄將會對系統造成嚴重的損害。在變更登錄前，應先備份電腦上任何有價值的資料
技術機制：	<ol style="list-style-type: none"> 執行 gpedit.msc 打開本機群組原則編輯器 選擇 [電腦設定\Windows 設定\安全性設定\本機原則\安全性選項] 在右邊窗點擊 "網路存取：可遠端存取的登錄路徑"，輸入 "System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion".
CCE-ID：	CCE-9121-5
資訊	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

網路型弱點掃描-遠端檢測

WIN7X64(16-03-28_00-31)

政策: Default (TCP) IP 篩選: IP 選擇 嚴重性: 選擇

IP 位址	主機	Mac 位址	閘道器
192.168.1.47	WIN7X64-MBP7	00-1C-42-CD-35-9F	

儀錶板	主機	稽核
儀錶板	主機	稽核
主機統計: 1		
等待檢測: 0		
正在檢測: 0		
中斷檢測: 0		
完成檢測: 1		
作用中的主機: 1		
檢測狀態: 全部檢測完畢 (耗費時間: 00:02:25)		

儀錶板	主機	稽核
一般		
IP 位址	192.168.1.47	
MAC 位址	00-1C-42-CD-35-9F - (2 Parallels, Inc.)	
主機名稱	WIN7X64-MBP7	
平均回應時間	0 ms	
開啟時間	128	
封包大小	56	
檢測時間	2016/3/28 上午 12:31:13 - 2016/3/28 上午 12:33:37	
作業系統		
作業系統偵測	Windows 7 Ultimate 7601 SP 1	
作業系統	Windows 7 Ultimate 7601 Service Pack 1	
LAN Manager	Windows 7 Ultimate 6.1	
通訊埠		
135	Microsoft Remote Procedure Call (RPC) service	
137	NETBIOS Name Service	
139	NETBIOS Session Service	
445	Microsoft-DS	
554	Real Time Streaming Protocol (RTSP)	
5357	Web Services for Devices	
Windows 帳戶		
SMB 分享		

單一台PC檢測所需時間

網路型弱點掃描-檢測結果

WIN7X64(16-03-28_00-31)

政策: Default (TCP) IP 篩選: IP 選擇 嚴重性: 選擇

IP 位址	主機	Mac 位址	閘道器
 192.168.1.47	WIN7X64-MBP7	00-1C-42-CD-35-9F	

儀錶板	主機	稽核
	稽核	
	資訊	NetBIOS NetBIOS Null階段作業已啟用
	資訊	NetBIOS NetBIOS 名稱資訊可存取
	資訊	Web Servers 偵測到 Web Server HTTP Protocol Version
	資訊	Web Servers 偵測到隱藏 WWW 伺服器名稱

遠端檢測，弱點數僅有4項，成效有限

分散式弱點掃描-檢測

檢測狀態	稽核
IP 位址	192.168.1.47
MAC 位址	00-1C-42-CD-35-9F - (2 Parallels, Inc.)
主機名稱	Win7x64-MBP7.radiant-tech.com.tw
平均回應時間	0 ms
開啟時間	128
封包大小	56
檢測時間	2016/3/28 上午 01:19:16 - 2016/3/28 上午 01:20:12
作業系統	Windows 7 Ultimate 7601 SP 1
作業系統偵測	Windows 7 Ultimate 7601 Service Pack 1
LAN Manager	Windows 7 Ultimate 6.1
NetBIOS 名稱	WIN7X64-MBP7
NetBIOS 群組	WORKGROUP
NetBIOS 作業系統	Windows NT 6.1
SystemRoot	C:\Windows
Service Pack	1

通訊埠	服務名稱
135	Microsoft Remote Procedure Call (RPC) service
137	NETBIOS Name Service
139	NETBIOS Session Service
445	Microsoft-DS
554	Real Time Streaming Protocol (RTSP)
5357	Web Services for Devices
Windows 帳戶	
Administrator	Built-in account for administering the computer/domain
barbet	
eileen	
Guest	Built-in account for guest access to the computer/domain
HomeGroupUser\$	Built-in account for homegroup access to the computer
SMB 分享	
ADMIN\$	遠端管理
C\$	預設共用
IPC\$	遠端 IPC
print\$	Printer Drivers

分散式弱點掃描-檢測結果

主機詳細資料- [Radiant-Tech] Win7x64-MBP7.radiant-tech.com.tw : 192.168.1.47

弱點稽核 通訊埠 Windows 帳號 Windows 服務 軟體資產 網芳分享 檢測資訊

主機詳細資料- [Radiant-Tech] Win7x64-MBP7.radiant-tech.com.tw : 192.168.1.47 - 2016-03-28 01-19-16

回上一頁

檢測資訊

- ✔ 檢測時間: 2016-03-28 01-19-16 - 2016-03-28 01-20-12
- ✔ IP 位址: 192.168.1.47
- ✔ 主機名稱: Win7x64-MBP7.radiant-tech.com.tw
- ✔ MAC 位址: 00-1C-42-CD-35-9F(2 Parallels, Inc.)
- ✔ 作業系統: Windows 7 Ultimate 7601 SP 1
- ✔ 網路開道:
- ✔ NB 名稱: WIN7X64-MBP7
- ✔ NB 群組: WORKGROUP
- ✔ NB 作業系統: Windows 7 Ultimate 7601 Service Pack 1
- ✔ 通訊埠數量: 6
- ✔ 弱點數量: 25

弱點稽核

嚴重性	弱點名稱
緊急	密碼歷程紀錄未強制執行
緊急	密碼長度最小值太短或未設定
緊急	密碼不會過期
緊急	不限制存取光碟
緊急	不限制存取軟碟
嚴重	POSIX 子系統啟用
嚴重	危險的 Windows AutoRun
高	帳戶鎖定閾值
中	印表機驅動程式安全
中	自動分享磁碟-伺服器(Server)
中	自動分享磁碟-工作站(WorkStation)
中	未登入關機啟用
低	快取的網域登入資訊
低	密碼不能更改
低	預設的管理員帳號
低	分頁檔案未清除
低	預設的來賓帳戶名稱
資訊	NetBIOS Null 階段作業已啟用
資訊	NTFS 8.3 名稱建立啟用
資訊	DCOM 啟用
資訊	允許匿名列舉 SAM 帳號與網路分享
資訊	NetBIOS 名稱資訊可存取
資訊	密碼必須符合複雜性需求
資訊	Adobe Reader 及 Acrobat 偵測
資訊	防毒軟體偵測

本機VS遠端弱點檢測

本機端檢測

Report Details for RADIANT-TECH - WINSERVER2008R2 (2017-05-02 22:40:58)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name: RADIANT-TECH\WINSERVER2008R2
 IP address: 192.168.1.48
 Security report name: RADIANT-TECH - WINSERVER2008R2 (2017-5-2 下午 10-40)
 Scan date: 2017/5/2 下午 10:40
 Scanned with MBSA version: 2.3.2211.0
 Catalog synchronization date:
 Security update catalog: Microsoft Update

Sort Order:

Security Update Scan Results

109個弱點未修補

Score	Issue	Result
	Windows Security Updates	109 security updates are missing. 2 service packs or update rollups are missing. What was scanned Result details How to correct this
	Developer Tools, Runtimes, and Redistributables	No security updates are missing. What was scanned Result details
	SQL Server Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	Updates are not automatically downloaded or installed on this computer. What was scanned How to correct this
	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the i What was scanned How to correct this
	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this

遠端檢測

Report Details for RADIANT-TECH - WINSERVER2008R2 (2017-05-02 22:41:24)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name: RADIANT-TECH\WINSERVER2008R2
 IP address: 192.168.1.48
 Security report name: RADIANT-TECH - WINSERVER2008R2 (2017-5-2 下午 10-41)
 Scan date: 2017/5/2 下午 10:41
 Scanned with MBSA version: 2.3.2211.0
 Catalog synchronization date:

Sort Order:

無法檢測

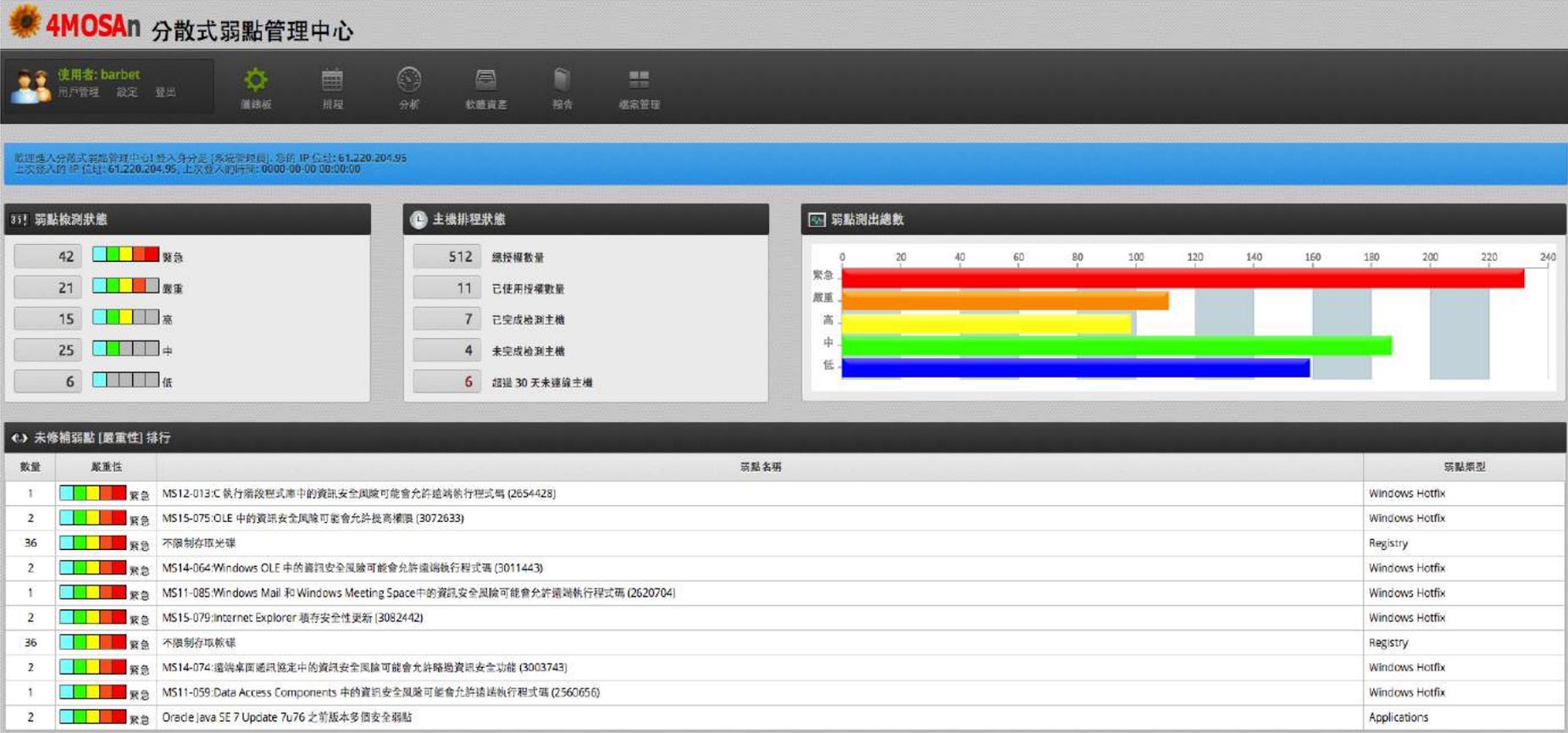
Security Update Scan Results

Score	Issue	Result
	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	Updates are not automatically downloaded or installed on this computer. What was scanned How to correct this
	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the i What was scanned How to correct this
	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
	Windows Firewall	This check was skipped because it cannot be done remotely.



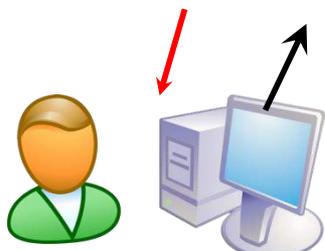
■ 管理員從Web介面安排子單位 排程掃描

使用者: admin
設定 用戶管理 登出

VULNERABILITY MANAGEMENT 分散式弱點管理中心

單位列表

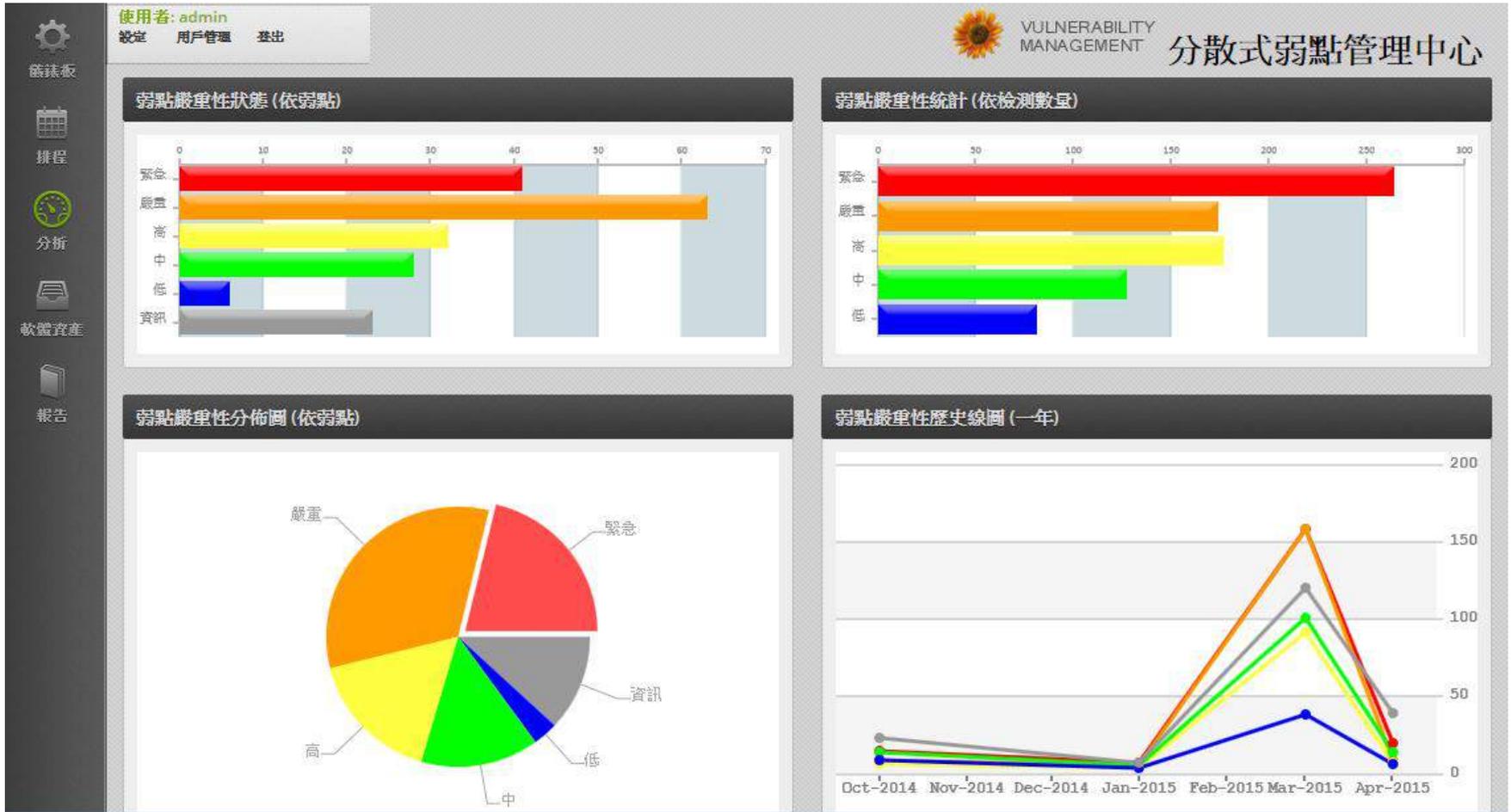
單位名稱	主機數量	已經完成	未完成	未完成排程	排程執行	下次排程	授權
Unit-Tech	2	1	1	2014-05-30	過期 347 天	2015-05-20	還有 276 天
Unit	3	3	0		9 天後	2015-05-21	還有 276 天
Unit	1	1	0		23 天後	2015-06-04	還有 91 天
Unit(測試)	1	1	0		31 天後	2015-06-12	還有 272 天
Unit	1	1	0		13 天後	2015-05-25	還有 276 天
Unit	5	5	0		9 天後	2015-05-21	還有 273 天



弱點稽核管理員



管理中心--分析功能



管理中心--軟體資產功能

使用者: wecki
設定 用戶管理 登出

VULNERABILITY MANAGEMENT 分散式弱點管理中心

單位軟體統計 - [Demo(測試)] 回單位列表

軟體統計 黑名單軟體

軟體統計		
數量	軟體名稱	版本
1	7-Zip 9.20	
1	Adobe Flash Player 11 Plugin	11.9.900.170
1	Adobe Flash Player 16 ActiveX	16.0.0.235
1	Adobe Reader XI (11.0.10) - Chinese Traditional	11.0.10
1	Backup Folder Sync	1.3.1
1	BDE_ENT	5.1.1
1	Boost Libraries for C++Builder XE2	9.0
1	CCleaner	4.00

管理中心--稽核報告功能

使用者: admin
[設定](#) [用戶管理](#) [登出](#)



VULNERABILITY
MANAGEMENT

分散式弱點管理中心

[產生報表選項] 格式: HTML PDF | 嚴重性篩選: 緊急 嚴重 高 中 低 資訊

單位主機列表-[VM] 回單位列表

<input checked="" type="checkbox"/> 全部勾選	IP 位址	MAC 位址	作業系統	完成檢測	弱點數	掃描狀態
<input checked="" type="checkbox"/> 檢視 ✔ WIN7-64	192.168.0.3	00-0C-29-DE-B9-3D	Windows 7 Home Basic 7601 SP 1	2015-02-21 13-27-21	65	8 天後
<input checked="" type="checkbox"/> 檢視 ✔ WIN8-BETA	192.168.0.11	00-0C-29-AE-86-8F	Windows 8 Consumer Preview 8250	2015-02-20 21-45-57	48	8 天後
<input checked="" type="checkbox"/> 檢視 ✔ WIN-SERVER-8	192.168.0.12	00-0C-29-E7-77-59	Windows Server 8 Beta Datacenter 8250	2015-02-21 13-41-28	37	8 天後
<input checked="" type="checkbox"/> 檢視 ✔ VM-WIN81	192.168.0.5	00-0C-29-CC-1D-00	Windows 8.1 9600	2015-02-21 13-19-41	52	8 天後
<input checked="" type="checkbox"/> 檢視 ✔ WIN-KMVNE5051B	192.168.153.134	00-0C-29-9F-7C-18	Windows 10 Pro Technical Preview 9926	2015-02-21 13-12-58	25	8 天後

弱點統計(全部)

產生報表(選擇項目)

4MOSAn Cloud Security

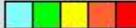
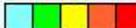
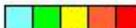
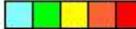
管理中心--修補狀態

修補狀態 - 位址: 192.168.0.3 名稱: WIN7-64.home 檢討: 2015-02-21 13-26-38 回上一頁				
風險	弱點名稱	處理	處理情形	
緊急	密碼歷程紀錄未強制執行	新弱點	新弱點	
緊急	密碼長度最小值太短或未設定	新弱點	新弱點	
緊急	密碼最短使用期限未設置	新弱點	新弱點	
緊急	密碼最長使用期限太短	新弱點	新弱點	
緊急	密碼不會過期 - Administrator	待修補	待修補	
緊急	密碼不會過期 - Guest	待修補	待修補	
緊急	不限制存取光碟	待修補	待修補	
緊急	MS11-059:Data Access Components 中的資訊安全風險可能會允許遠端執行程式碼 (2560656)	待修補	待修補	
緊急	MS11-085:Windows Mail 和 Windows Meeting Space中的資訊安全風險可能會允許遠端執行程式碼 (2620704)	待修補	待修補	
緊急	MS12-001:Windows 核心中的資訊安全風險可能允許部分安全功能被略過 (2644615)	待修補	待修補	
緊急	MS12-013:C 執行階段程式庫中的資訊安全風險可能會允許遠端執行程式碼 (2654428)	待修補	待修補	
緊急	MS11-025:Microsoft Foundation Class (MFC) 程式庫中的資訊安全風險可能會允許遠端執行程式碼 (2500212)	待修補	待修補	

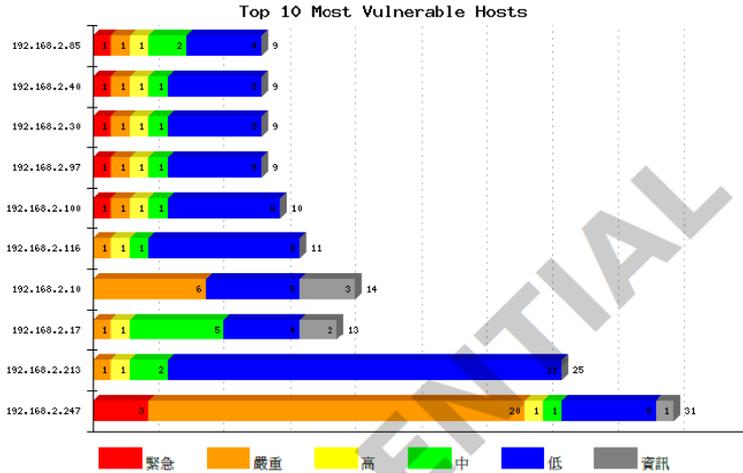
管理中心--弱點統計

嚴重性篩選: 緊急 嚴重 高 中 低 資訊 篩選

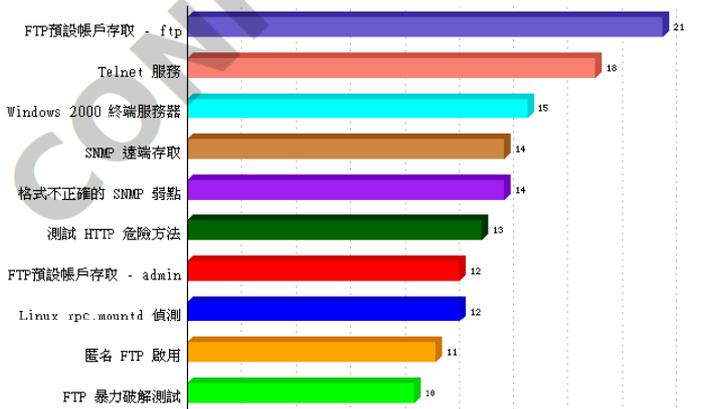
單位弱點列表 - [測試] 回單位主機列表

嚴重性	弱點名稱	主機
 緊急	 密碼歷程紀錄未強制執行	FSERVER, 112.104.105.116 1
		gate7.home, 192.168.0.6 1
		2core-win7, 25.127.19.241 1
 緊急	 密碼長度最小值太短或未設定	FSERVER, 112.104.105.116 1
		gate7.home, 192.168.0.6 1
		2core-win7, 25.127.19.241 1
 緊急	 密碼最短使用期限未設置	FSERVER, 112.104.105.116 1
		gate7.home, 192.168.0.6 1
		2core-win7, 25.127.19.241 1
 緊急	 密碼最長使用期限太短	2core-win7, 25.127.19.241 1
 緊急	 密碼不會過期	FSERVER, 112.104.105.116 12

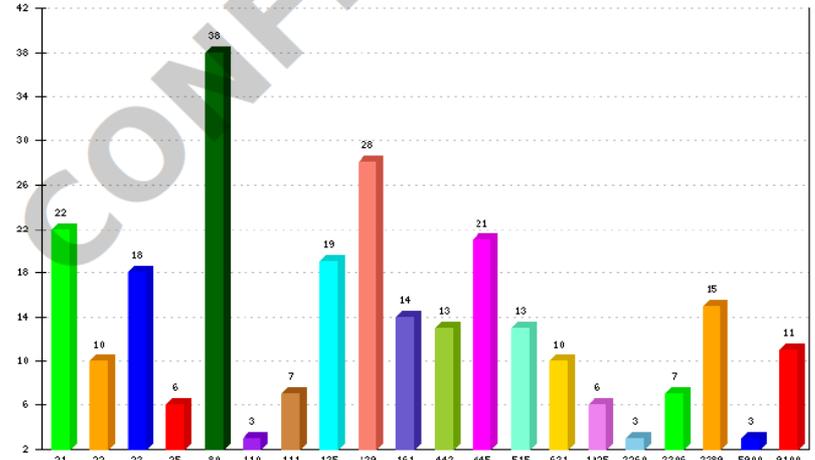
前 10 名高風險主機分佈



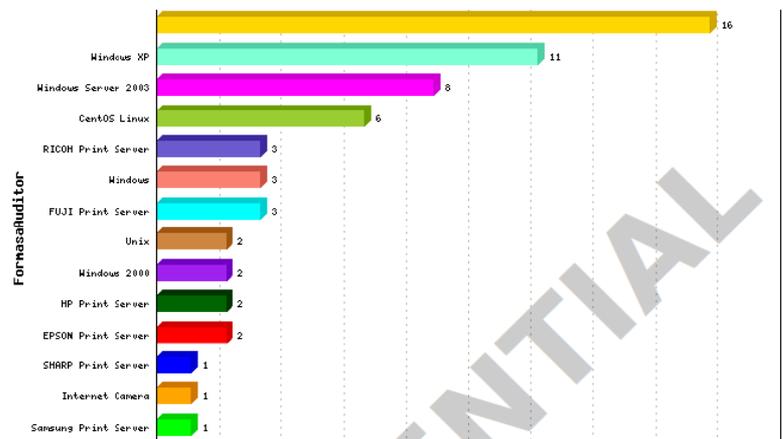
前 10 名弱點分佈



前 20 名網路服務統計



作業系統統計摘要



DVMS 2.0 專業版 (軟體派送)

提供exe、msi、msu及xml檔案派送，支援靜默安裝，主動修補弱點



主動弱點修補

4MOSAn 分散式弱點管理中心 2017-05-03 00:39:41

使用者: barbet
 用戶管理 設定 登出

儀錶板 排程 分析 軟體資產 報告 例外 電腦列表 維護 說明

搜尋包含特定弱點 (完整弱點名稱): MS15-034:HTTP.sys 中的資訊安全風險可能會允許遠端執行程式碼 (3042553) 作業系統: 全部 搜尋

派送單位主機列表 - [Radiant-Tech] 回派送單位列表

新增整個單位 (全部主機) 派送軟體 刪除整個單位 (全部主機) 派送軟體

電腦名稱	作業系統	派送檔案
<input checked="" type="checkbox"/> WIN7-YUYUYU	(JUST GUESSING): Windows 7, Server 2008 R2 (x64)	
<input checked="" type="checkbox"/> WIN7X32-GCB-MAC	Windows 7 Pro 7601 SP 1	

Showing 1 to 2 of 2 entries

選擇檔案 請選擇

- 派送 FGCB_setup-Radiant-Tech_20160521.msi
- 派送 vcredist_x64 (KB2467173).exe
- 派送 JavaSetup8u121.exe
- 派送 Windows6.1-KB2536275-x64.msu
- MS11-048-x86.msu
- MS11-059x64.msu
- 派送 install_flash_player_ax.exe
- MS11-059x86.msu
- MS11-060 2007x86-glb.exe
- MS11-0602010-x64-glb.exe
- MS11-073office2010-x64-glb.exe
- MS15-034(KB3042553 : x64 系統的 Windows 7 安全性更新)**

選擇命令: 安裝 移除

新增派送軟體至已勾選主機

4MOSAn Security Technology Co., Ltd.
ver: 20170421

共同供應契約採購案

共同供應契約採購案

案號/案名：**1050204 / 105** 第四次電腦軟體共同供應契約採購案

政府組態基準 (Government Configuration Baseline, GCB)

組別	項次	品名	建議售價
6	145	4MOSAn GCB Doctor 管理中心系統模組	243,249
6	146	4MOSAn GCB Doctor PC 終端模組 (單套授權數: 256)	243,249
6	147	4MOSAn GCB Doctor Windows Server 終端模組 (單套授權數: 256)	243,249
6	148	4MOSAn GCB Doctor 管理系統軟體壹年保固授權 (終端模組單套授權數: 256 或 管理中心系統模組)	58,071

共同供應契約採購案

案號/案名：**1050204 / 105** 第四次電腦軟體共同供應契約採購案

分散式弱點掃描與管理 (Distributed Vulnerability Management System)

組別	項次	品名	建議售價
6	154	4MOSAn 分散式弱點管理中心系統模組	243,249
6	155	4MOSAn 分散式弱點管理系統終端模組 (單套授權數: 256)	162,031
6	156	4MOSAn 分散式弱點管理系統軟體 (壹年保固授權) (系統終端模組單套授權數: 256 或 管理中心系統模 組)	48,325

Q&A

測試帳號申請
請洽授權經銷商

與會者問題

- GCB的設定要項有那幾項?會影響到哪些操作?
- 如有新系統新功能上線時，(TWGCB)是否能及時公布相對應版本?
- 機關導入GCB過程中，應否允許特定電腦進行例外設定?
- 因新機已不支援Win7，作業系統一定要升Win10，對應的GCB何時公佈。
- Win7GCB可套用在Win10的比例約如何。
- 機關導入GCB的最理想化是怎樣的情景?
- 政府機關導入後，民間必須配合的項目為何?