Radiant Advance 雷擎先進股份有限公司

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

公司簡介

- 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。

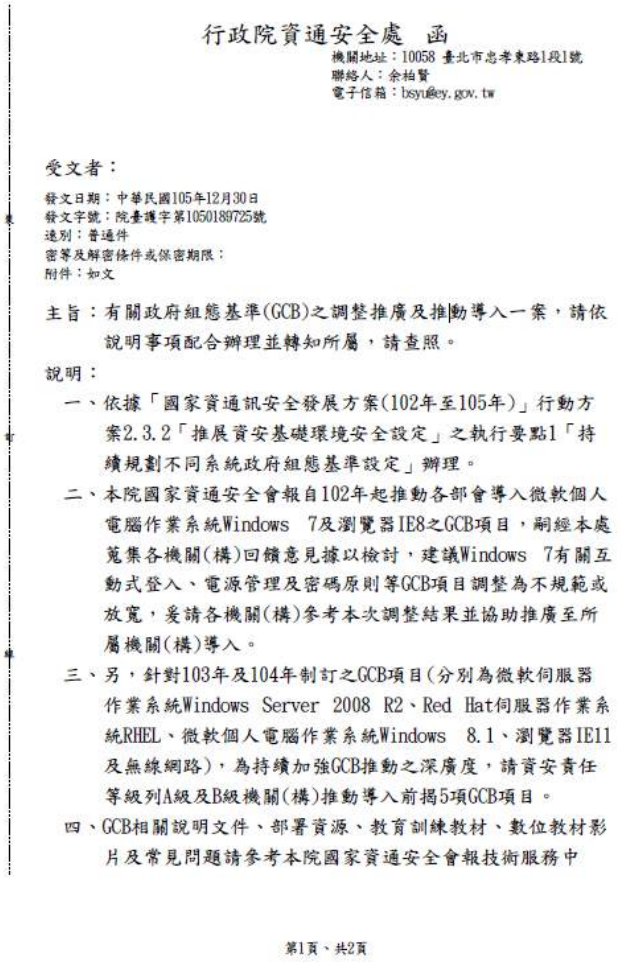
Can not measure,
will not control !

無法度量，就無法控制！

大　　綱

- 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：bsyu@ey.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
速別：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,Winserver2008 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。

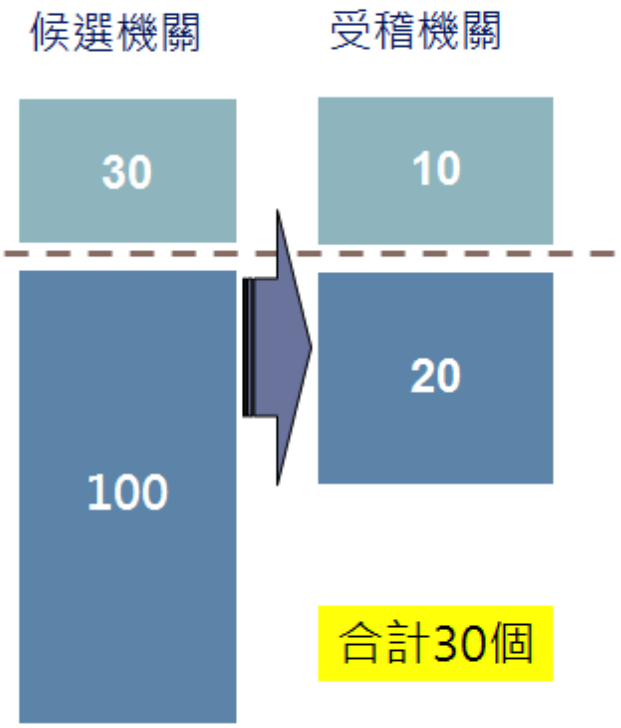
行政院資安稽核

- 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)



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
1	使用者電腦安全檢測	使用者電腦弱點掃描	10
		使用者電腦安全防護檢測	20
		組態設定安全防護檢測	5
2	惡意中繼站連線阻擋檢測	惡意中繼站連線阻擋檢測	5
3	核心資訊系統安全檢測	核心資訊系統內網滲透測試	30
		系統防護檢測	10
4	網路架構檢測	網路架構檢測	10
5	AD主機安全防護檢測	AD主機安全防護檢測	10
合計			100

構面	實地稽核項目	配分
策略面 30	1.導入資訊安全管理系統範圍適切性	5
	2.機關首長對資安業務支持度	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
管理面 30	5.個人資料保護與管理	10
	6.資訊資產管理與風險評鑑	8
	7.人力資源管理	5
	8.資訊委外安全管理	7
技術面 40	9.通訊與作業管理適切性與落實執行狀況	20
	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

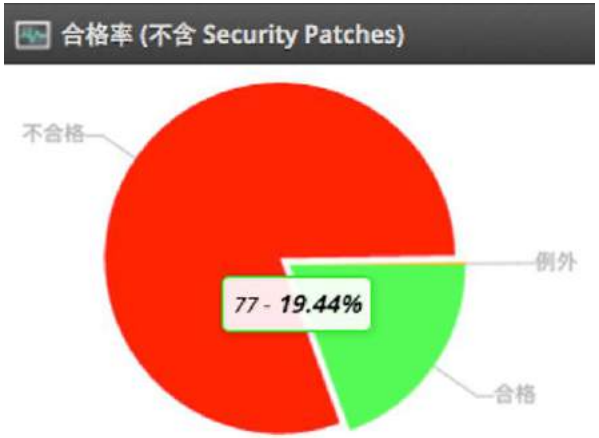
組態管理的重要性

Twenty Critical Security Controls for Effective Cyber Defense

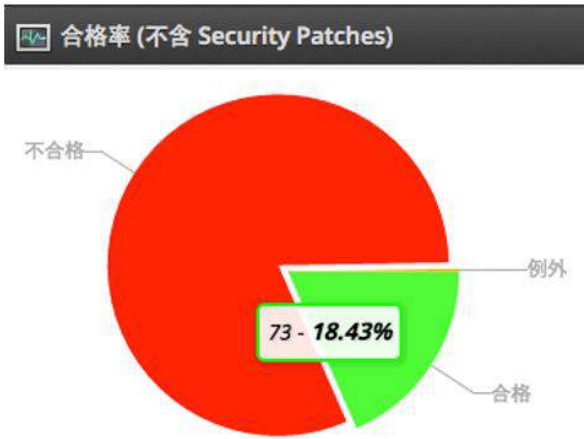
- CIS Critical Security Controls - Version 6.1
  - CSC 1: Inventory of Authorized and Unauthorized Devices
  - CSC 2: Inventory of Authorized and Unauthorized Software
  - CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
  - CSC 4: Continuous 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

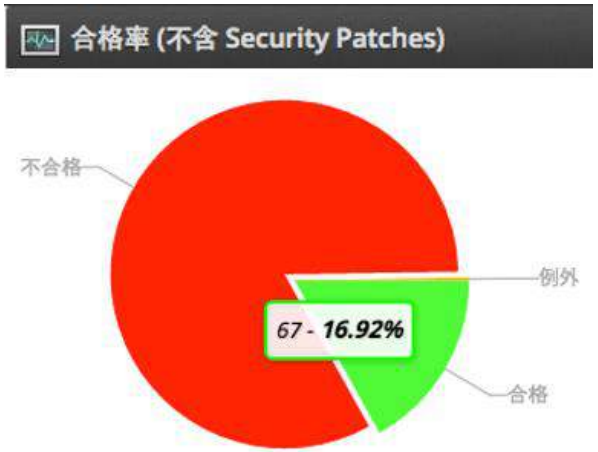
Win7



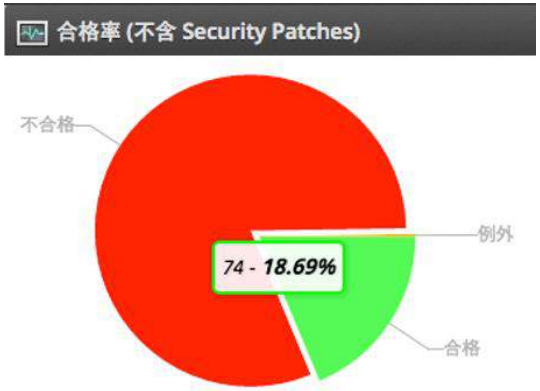
Win8



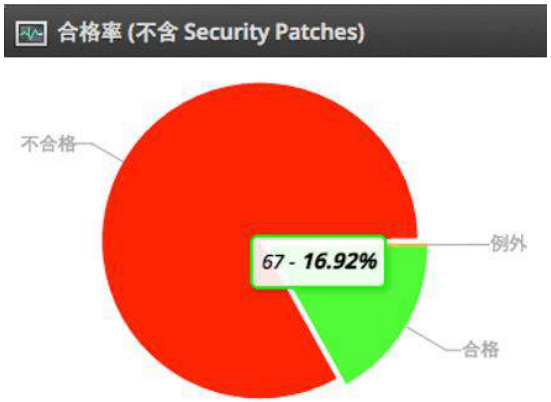
Win10



Win Server 2008R2 SP1

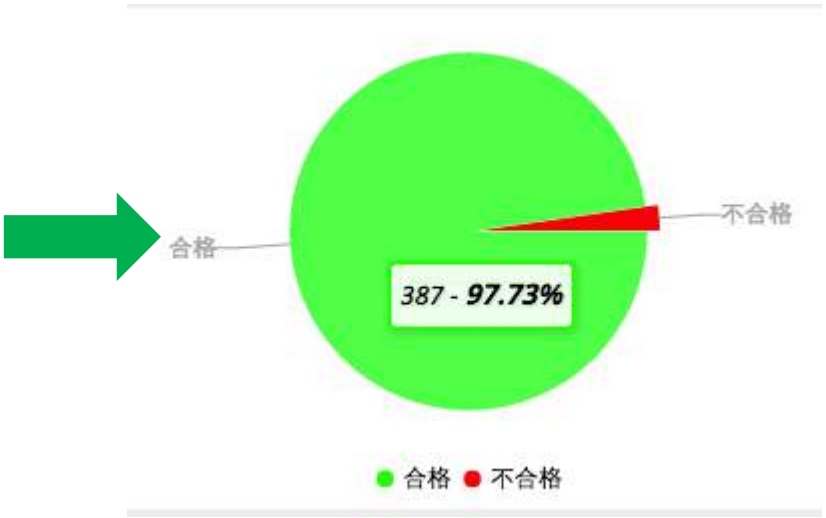


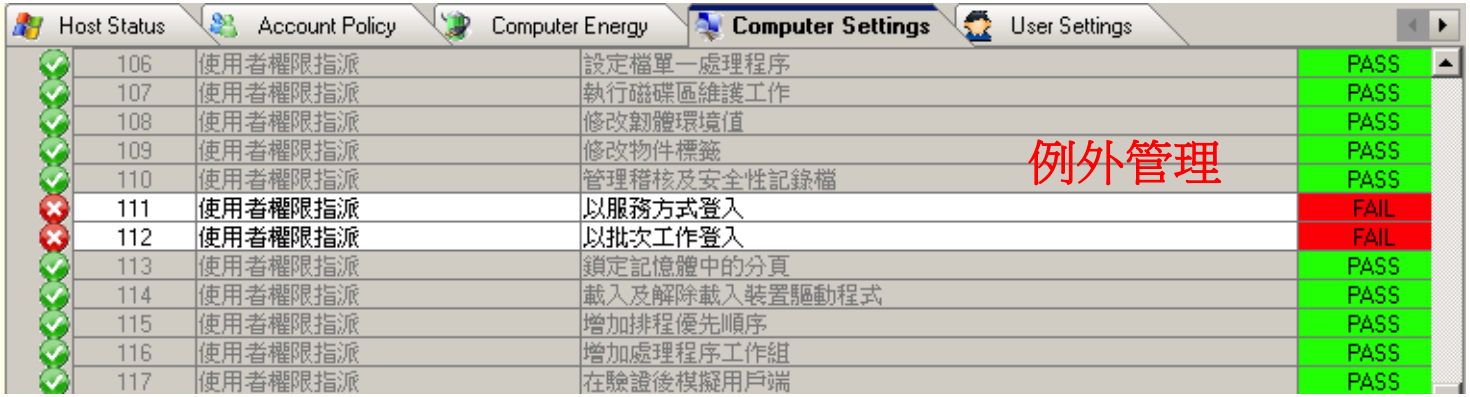
Win Server 2012



正確組態派送，提升安全程度

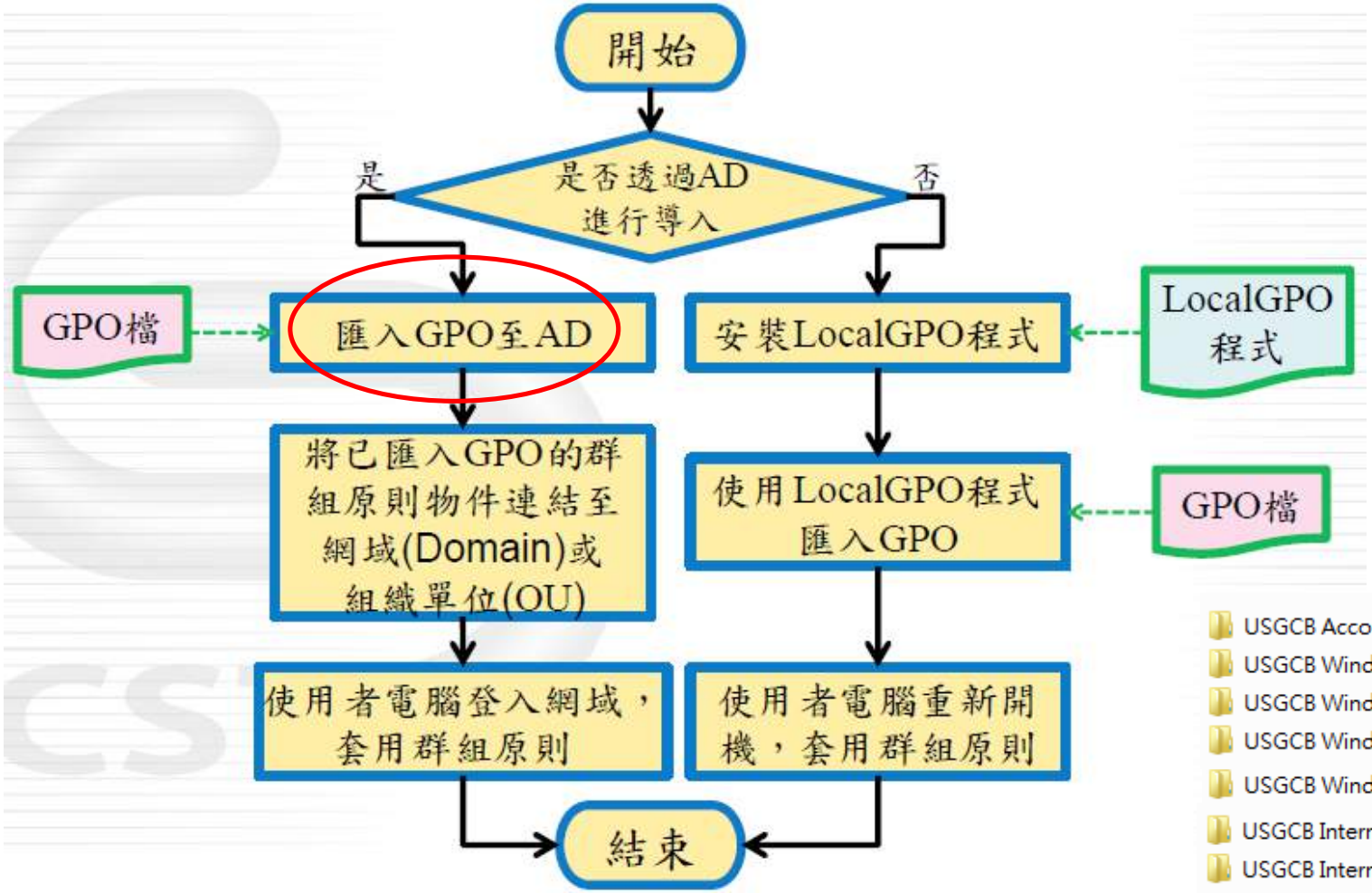
正確的組態派送，可以快速的提升安全組態之符合程度，但可彈性的保留必要之組態，進行例外管理。

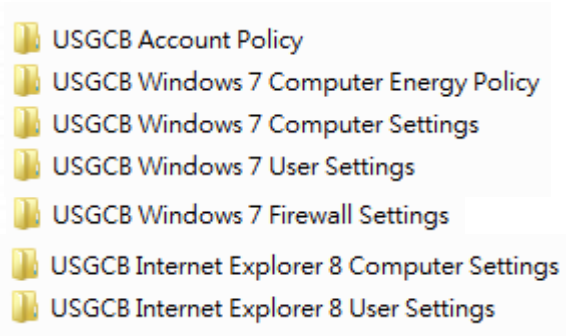




AD GPO 佈署實務

Microsoft GPO派送方法

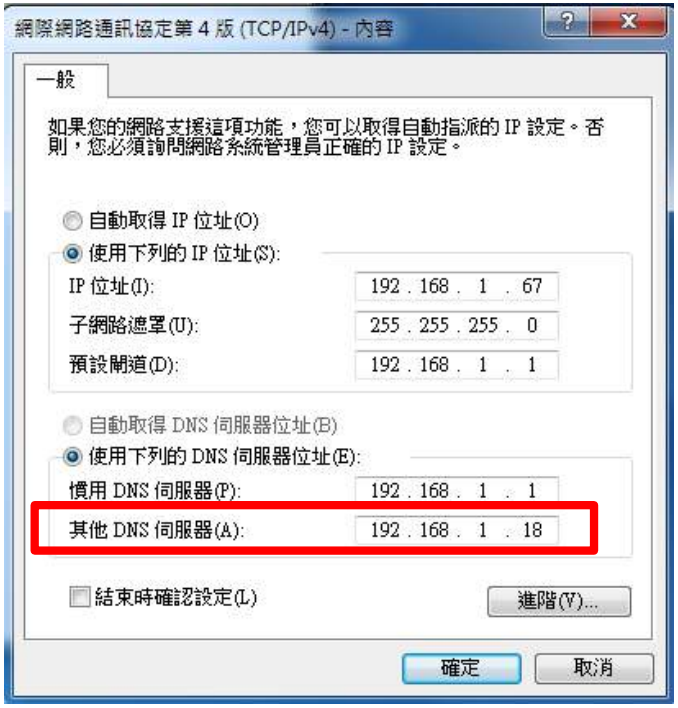




DNS IP Address設定錯誤

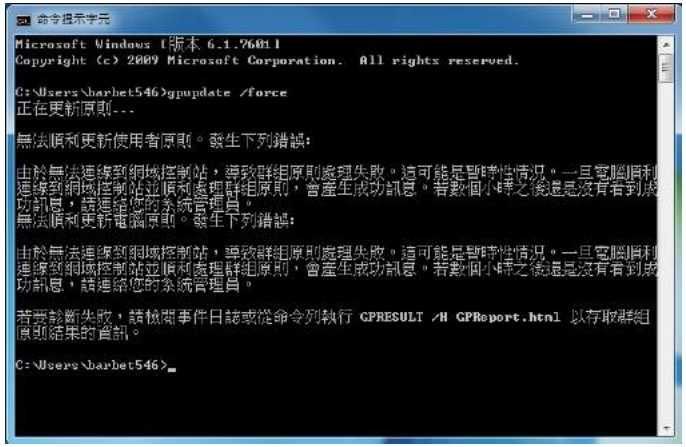
- GPO能夠完整的執行工作，電腦必須要能夠正確的被AD網域所管理，而網域的鑑別機制主要是經由DNS得知網域控制站的所在位置，同樣的經由DNS得知Kerberos資訊，才能夠確保GPO正確執行。

DNS : 192.168.1.18



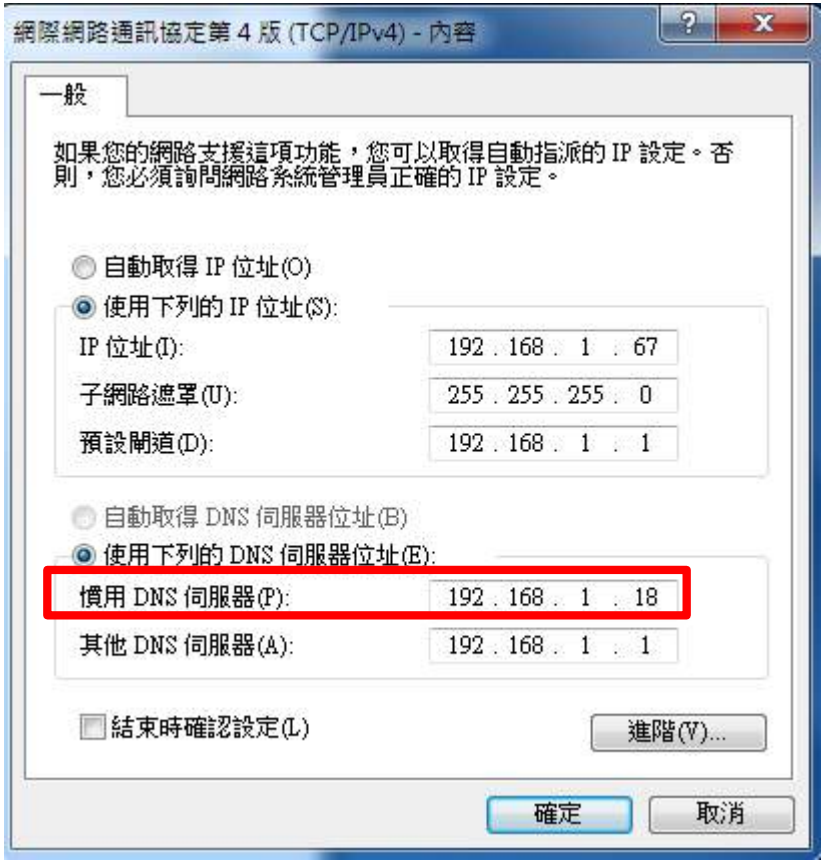
連線至網路閘道

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

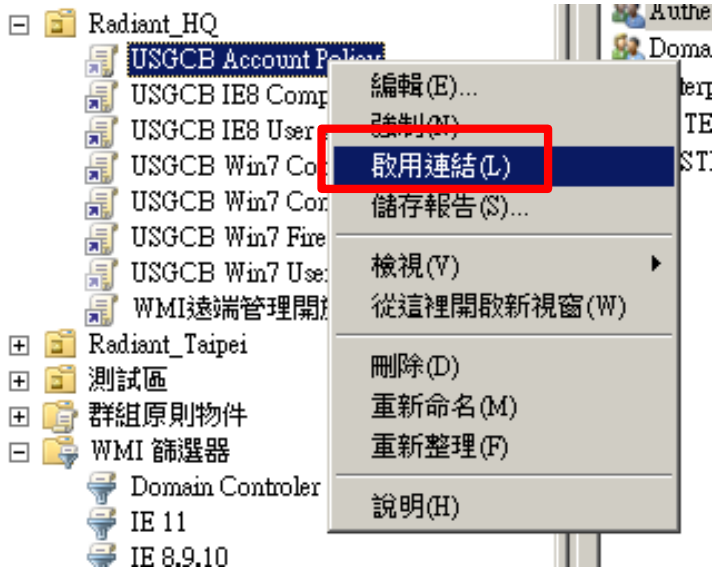
正確DNS設定，群組原則更新完成

GPO沒有正確的啟用連結

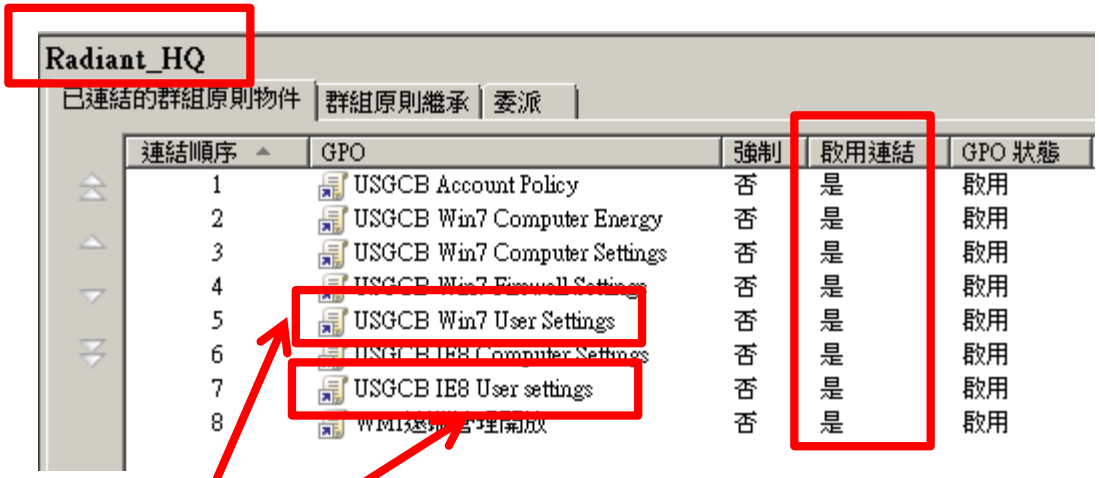
Radiant_HQ

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			

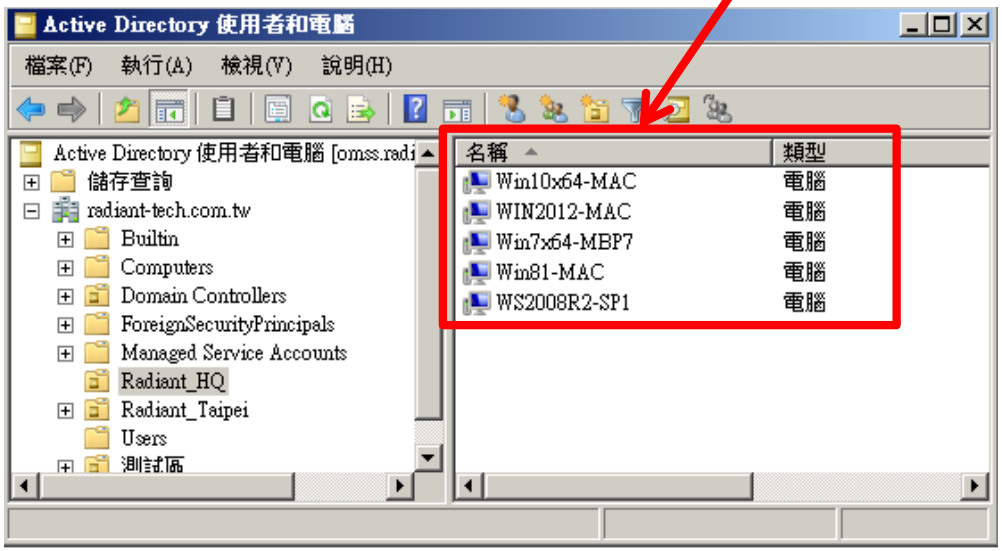


GPO 之物件類型設定錯誤



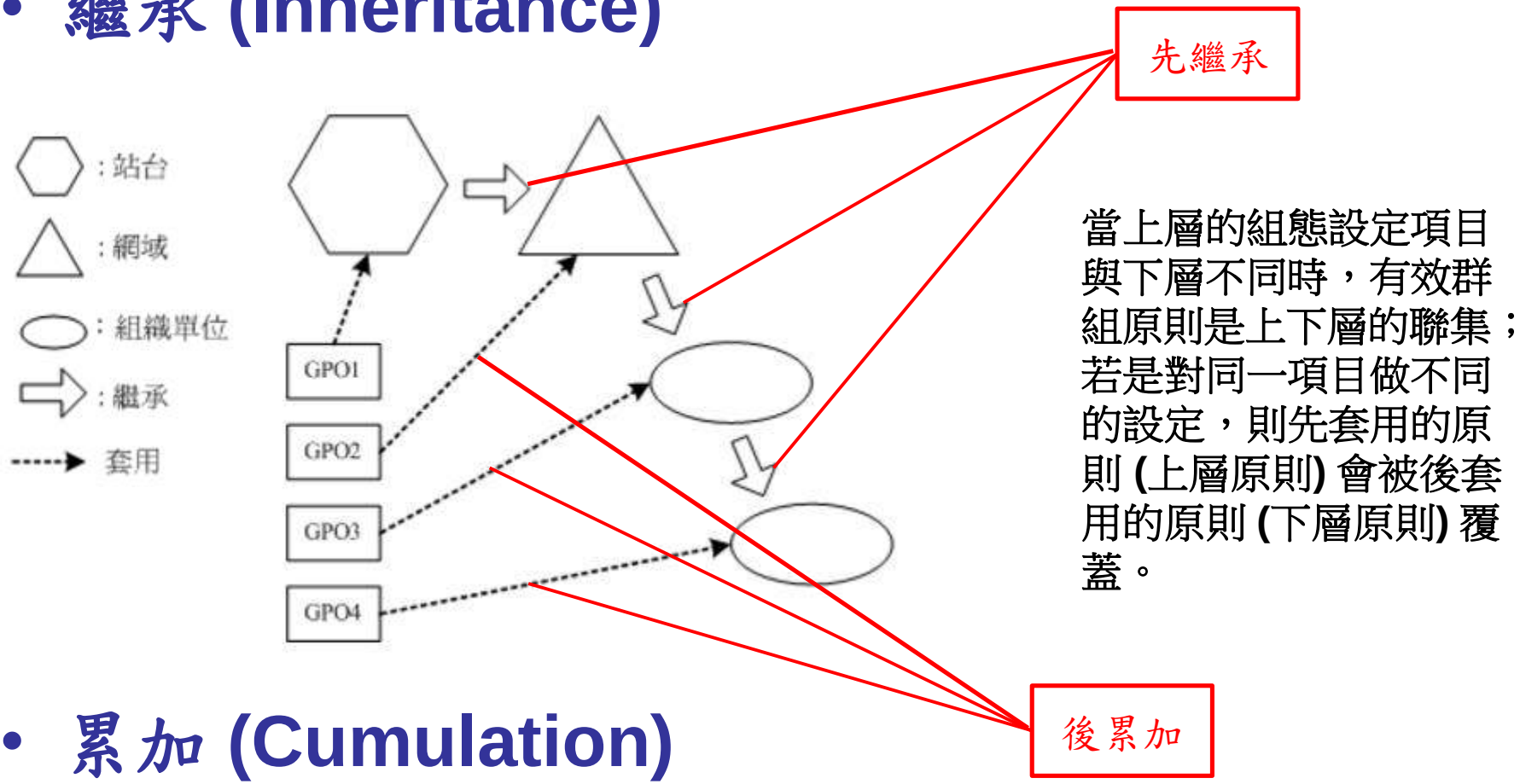
User Settings

使用者並未加入至組織單位



AD群組原則特性

- 繼承 (Inheritance)

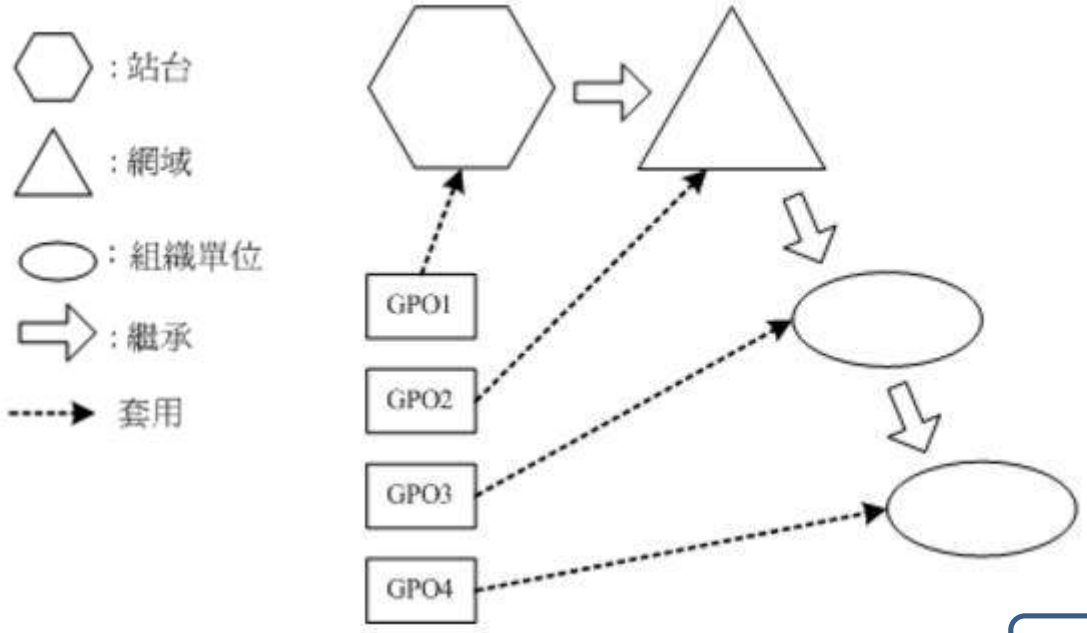


當上層的組態設定項目與下層不同時，有效群組原則是上下層的聯集；若是對同一項目做不同的設定，則先套用的原則 (上層原則) 會被後套用的原則 (下層原則) 覆蓋。

- 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



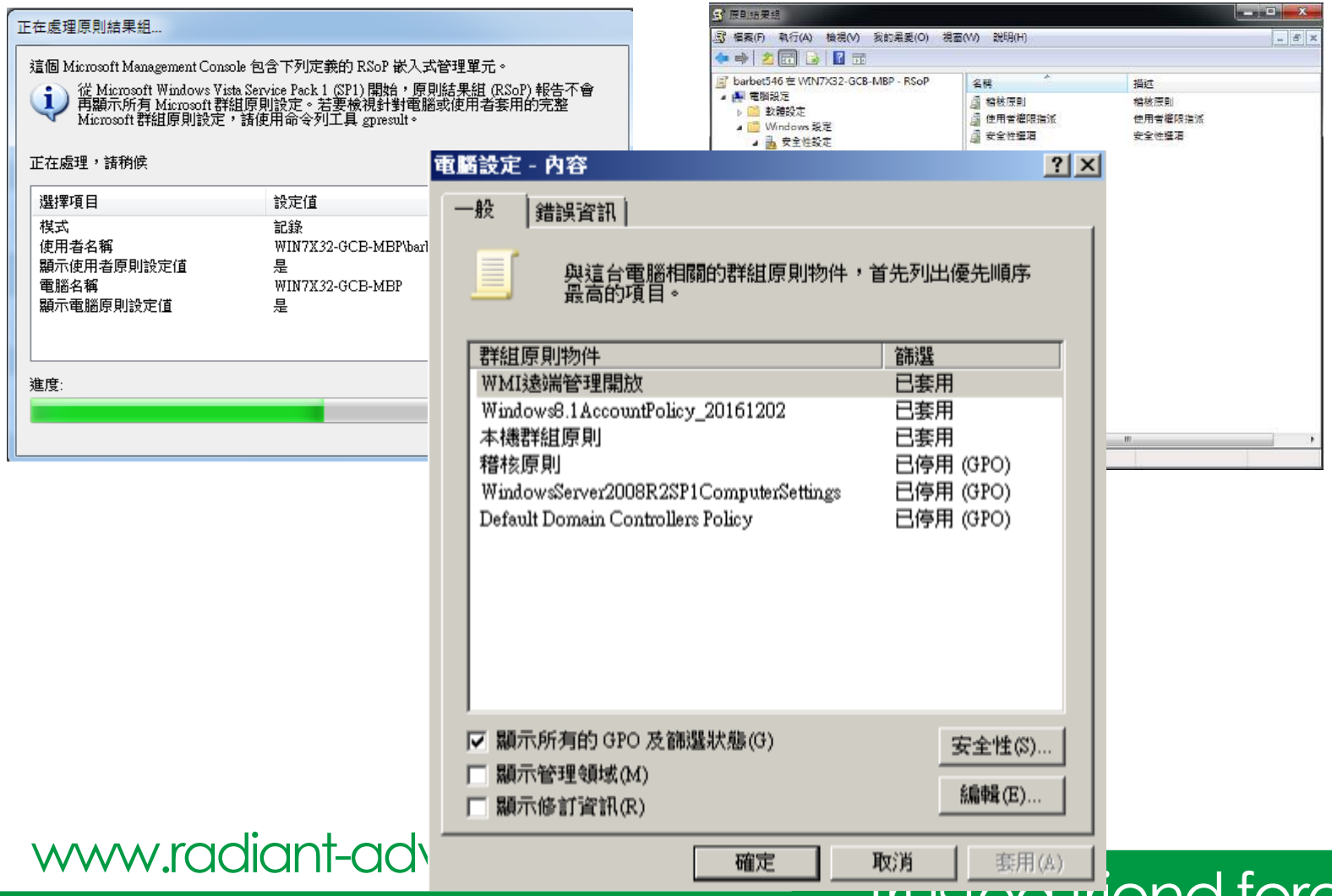
重開機生效　　使用者登入生效

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

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！

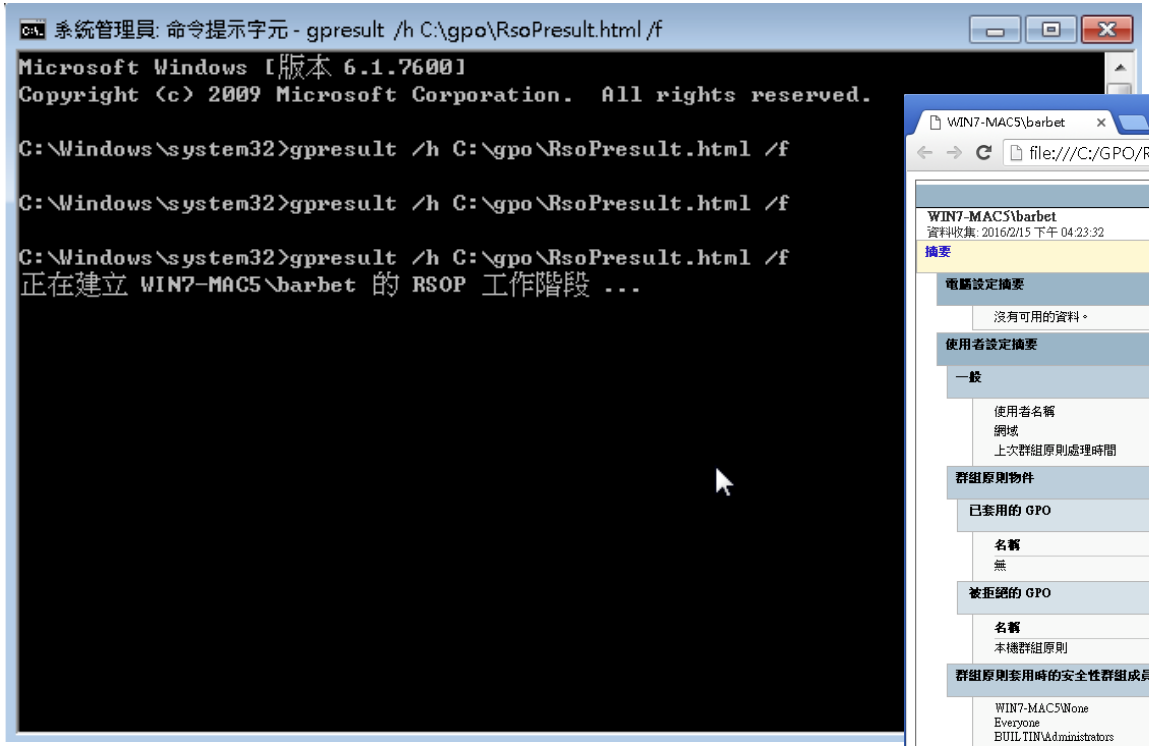


原則結果組報告(gpresult)

儲存路徑與檔名

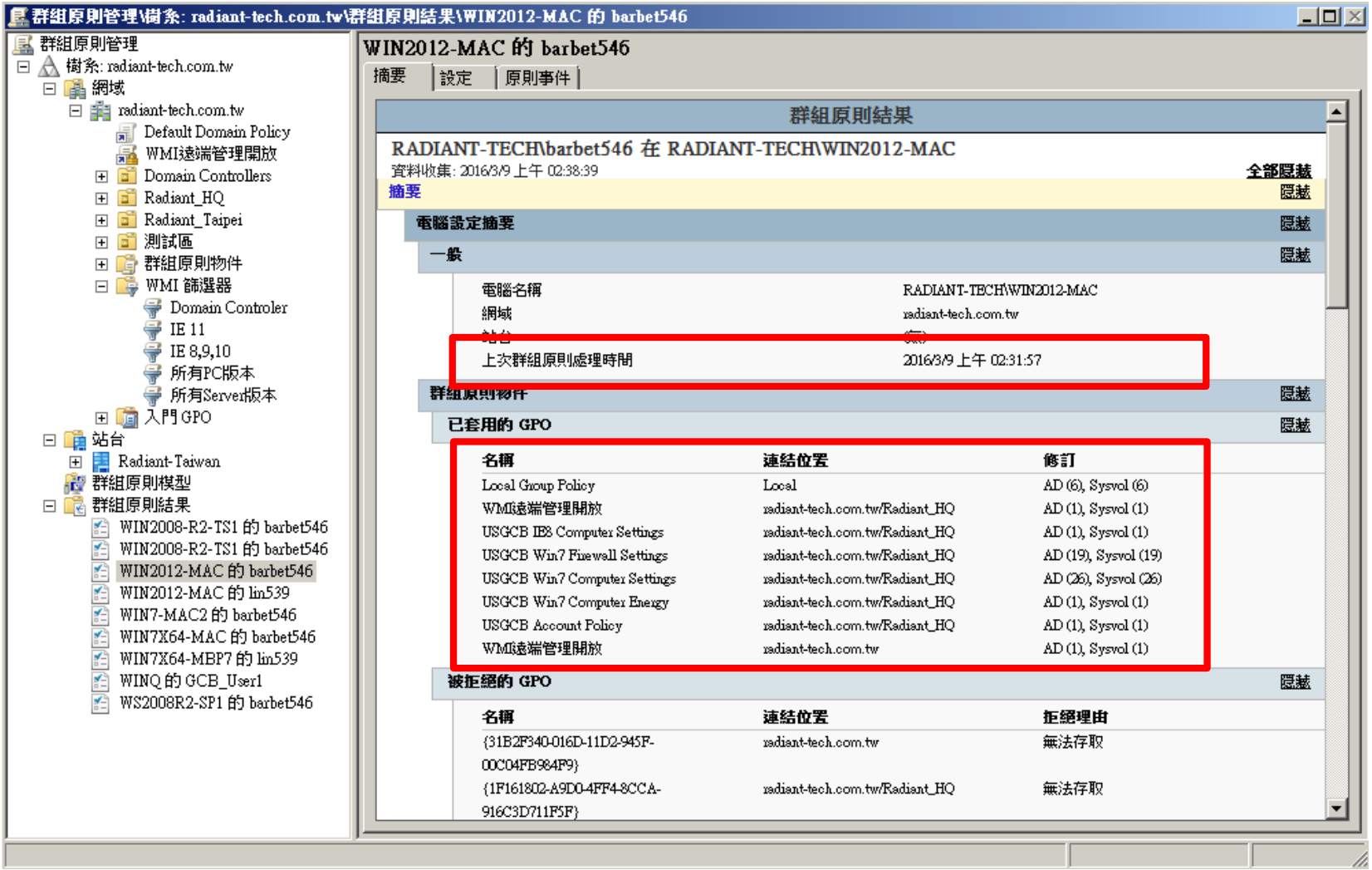
C:\Windows\system32>gpresult /h C:\GPO\RSoPresult.html /f 強制覆寫

命令提示字元　　指令　以HTML格式存報告



gpresult報告內容

WMI遠端RSoP 摘要



WMI遠端RSoP設定值

本機gpresult 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

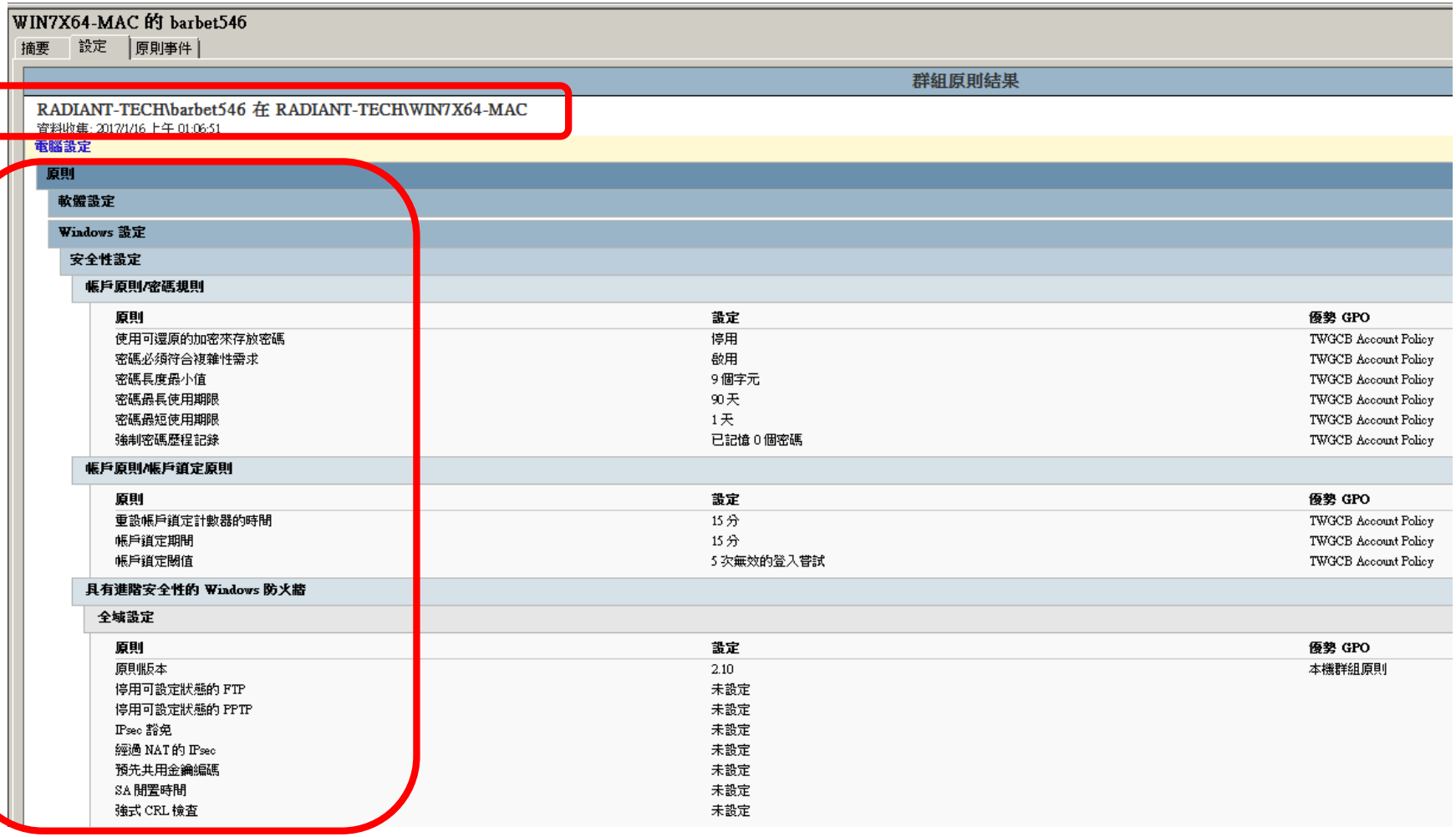
已套用的 GPO

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
Windows8.1CouputerSettings(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

遠端WMI gpresult report



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

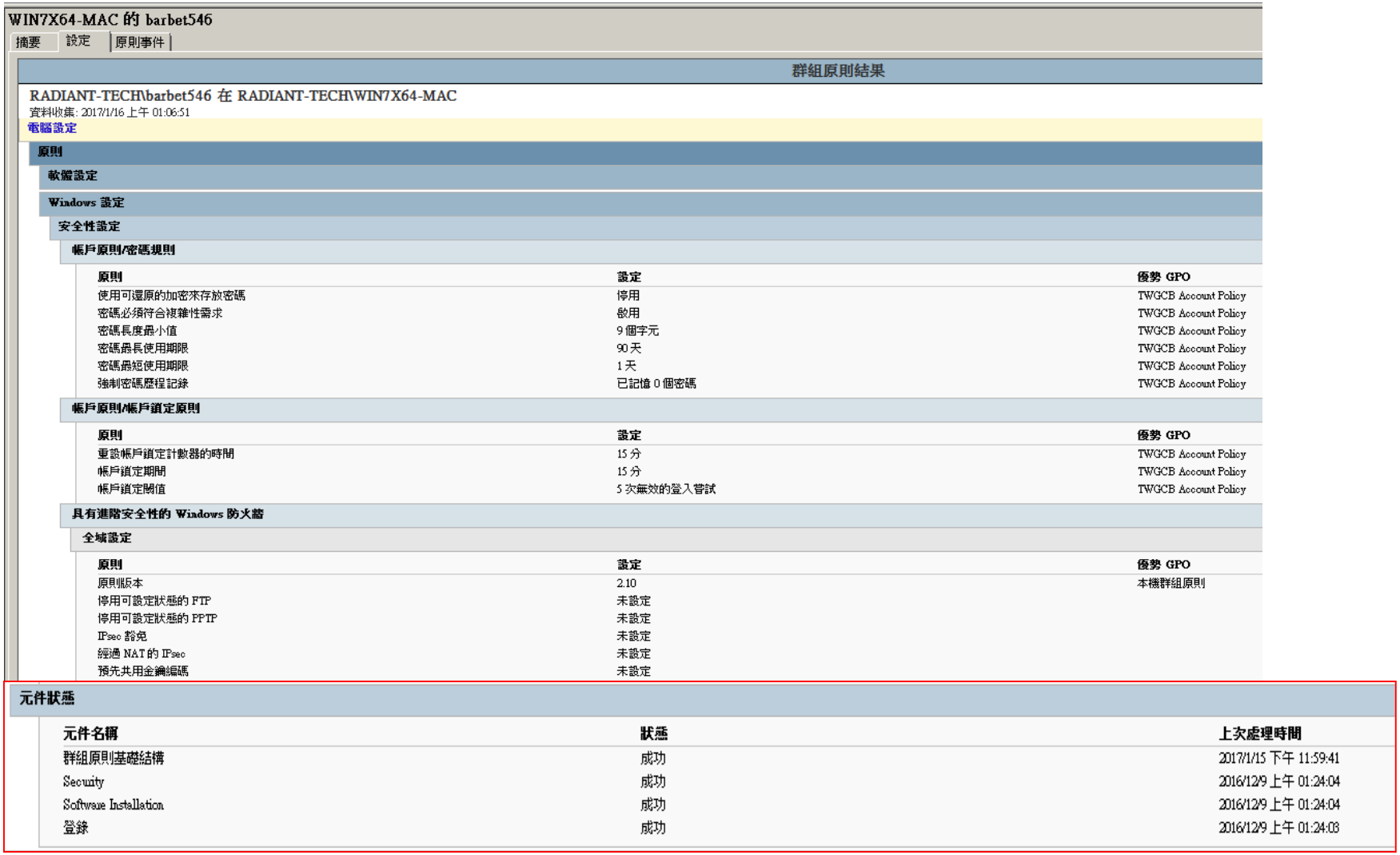
原則	設定	優勢 GPO
重設帳戶鎖定計數器的時間	15 分	TWGCB Account Policy
帳戶鎖定期間	15 分	TWGCB Account Policy
帳戶鎖定閾值	5 次無效的登入嘗試	TWGCB Account Policy

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	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

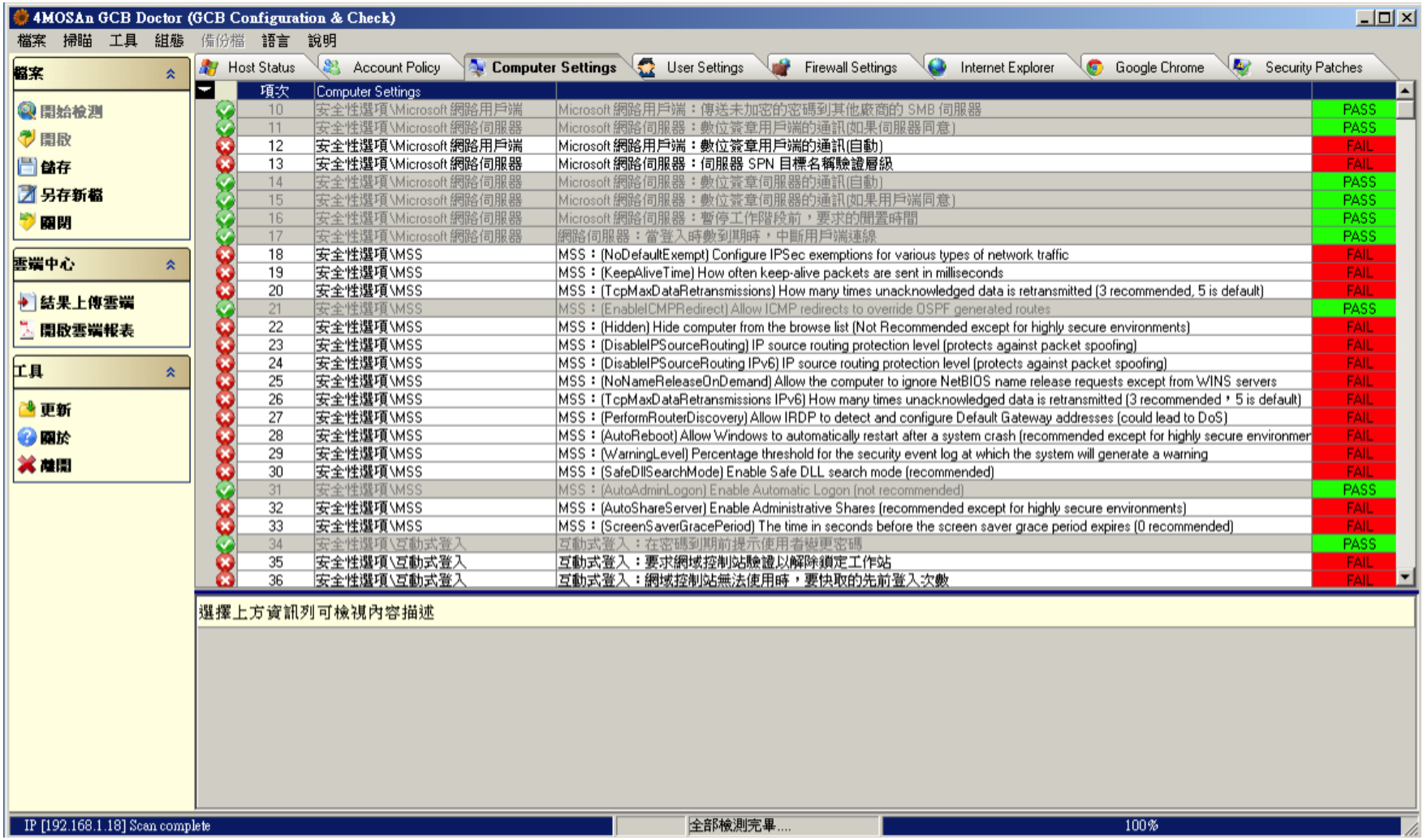
全域設定

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	

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	2016/12/9 上午 01:24:04
Software Installation	成功	2016/12/9 上午 01:24:04
登錄	成功	2016/12/9 上午 01:24:03

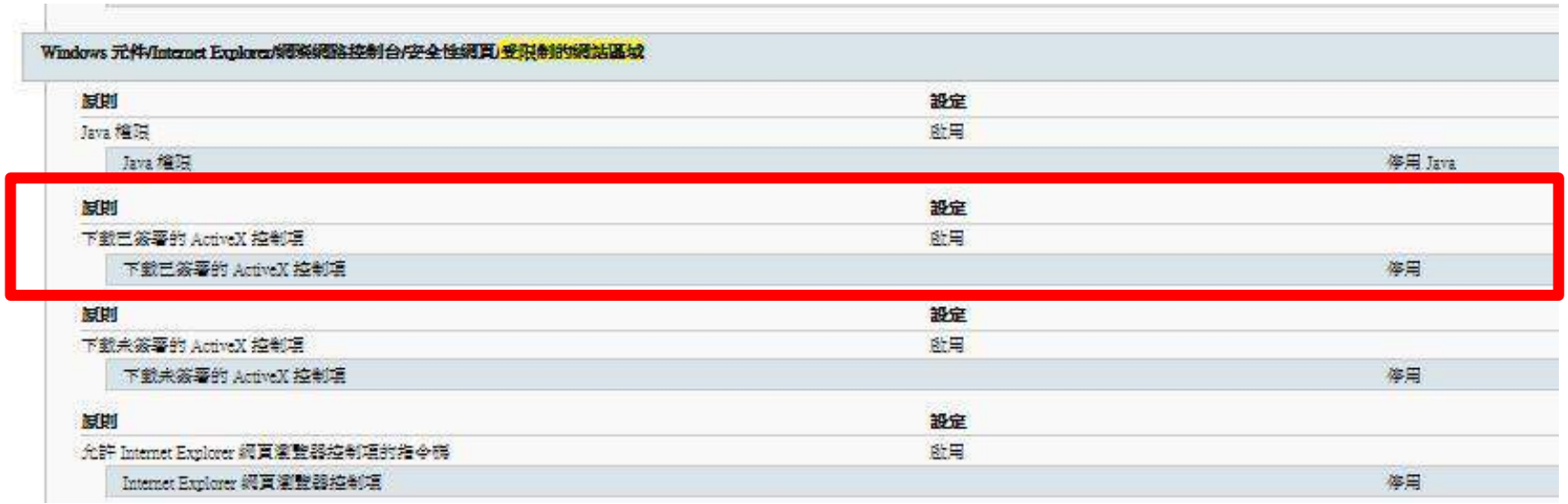
GCB Doctor檢測結果



套用與實際不符合案例

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

套用與實際不符合案例



Windows 元件/Internet Explorer/網際網路控制台/安全性網頁/受限制的網站區域		
規則	設定	
Java 權限	啟用	
Java 權限		停用 Java
規則	設定	
下載已簽署的 ActiveX 控制項	啟用	
下載已簽署的 ActiveX 控制項		停用
規則	設定	
下載未簽署的 ActiveX 控制項	啟用	
下載未簽署的 ActiveX 控制項		停用
規則	設定	
允許 Internet Explorer 網頁瀏覽器控制項的指令碼	啟用	
Internet Explorer 網頁瀏覽器控制項		停用

Computer：下載已簽署的 ActiveX 控制項 - 鎖定的網際網路區域	undefined	FAIL
Computer：JAVA 權限 - 鎖定的網際網路區域	0	PASS
Computer：僅允許批准的網域使用 ActiveX 控制項而且不提示 - 鎖定的網際網路區域	undefined	FAIL
Computer：開啟 SmartScreen 篩選工具網指 - 鎖定的網際網路區域	undefined	FAIL
Computer：允許在使用者插入時執行 CD 的主動式內容	0	PASS

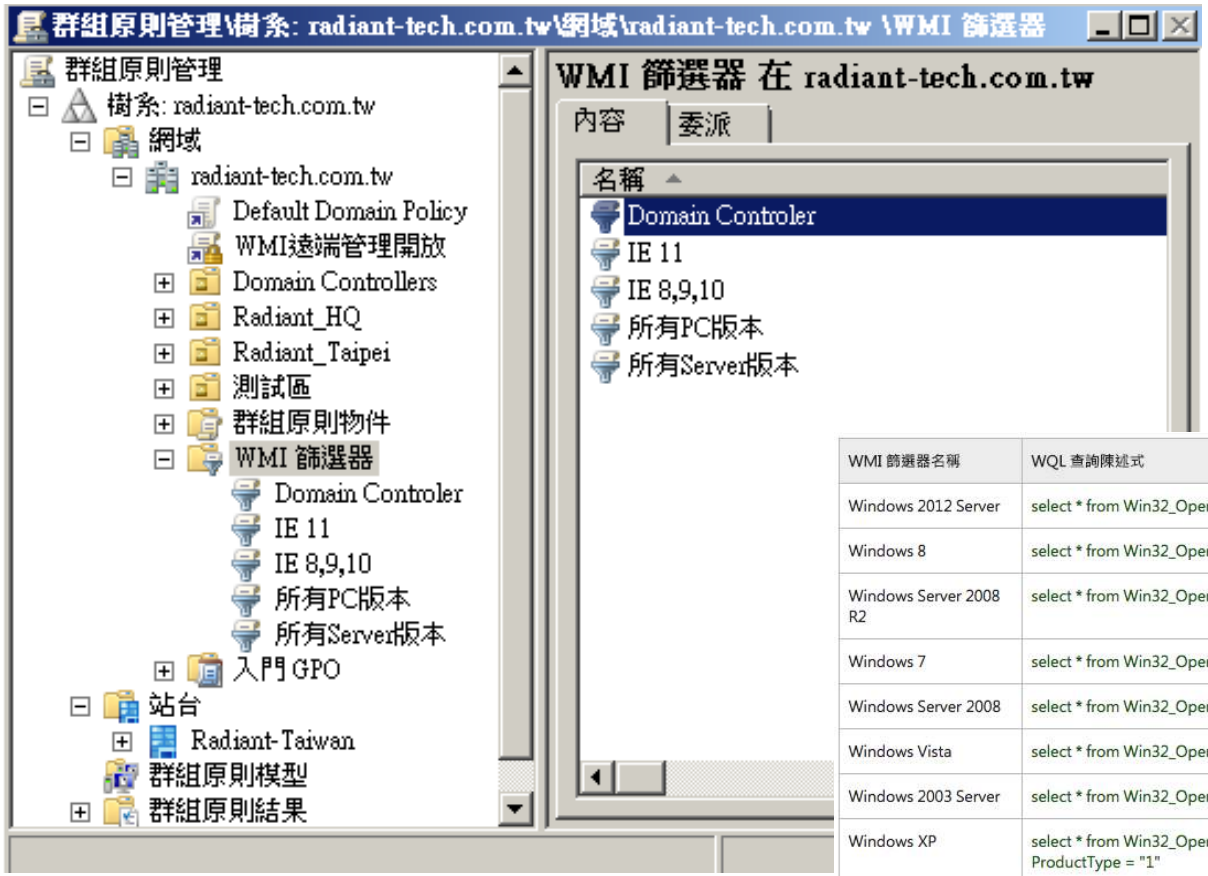
GPO如何套用至網域中各種版本之OS及IE？

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

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

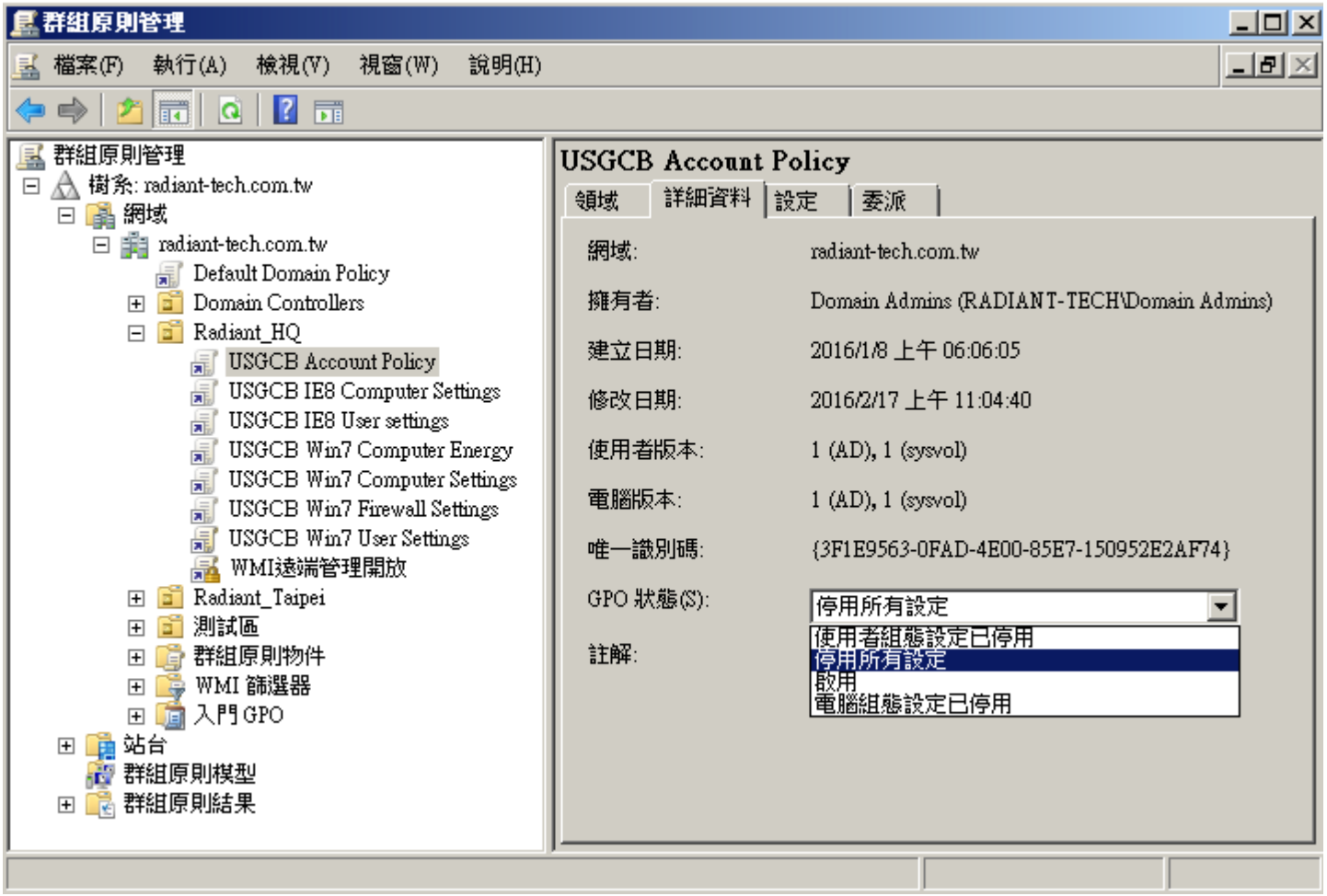
GPO套用可以安全回復嗎？

LocalGPO復原作業

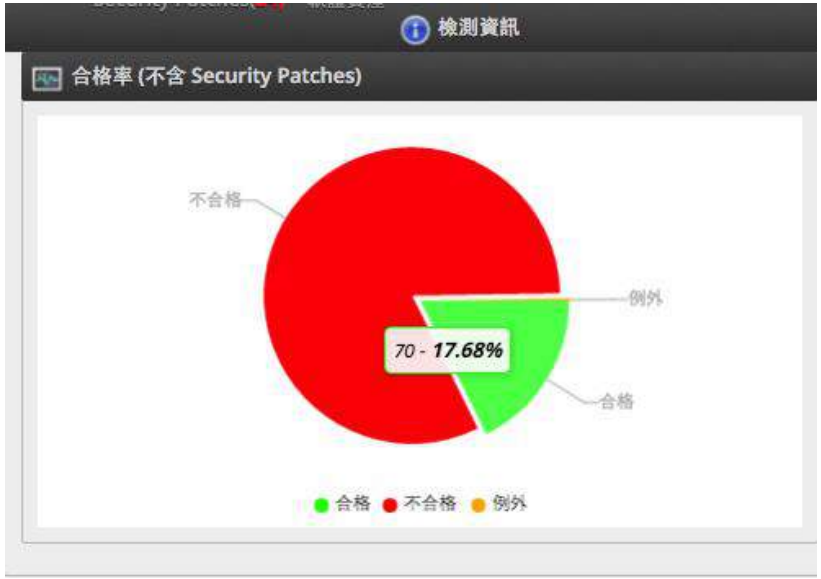
- 在LocalGPO工具的目錄下 –執行cscript LocalGPO.wsf /Restore

```
C:\Windows\system32>cd "c:\Program Files\LocalGPO"

c:\Program Files\LocalGPO>cscript LocalGPO.wsf /Restore
Microsoft (R) Windows Script Host Version 5.8
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>
```

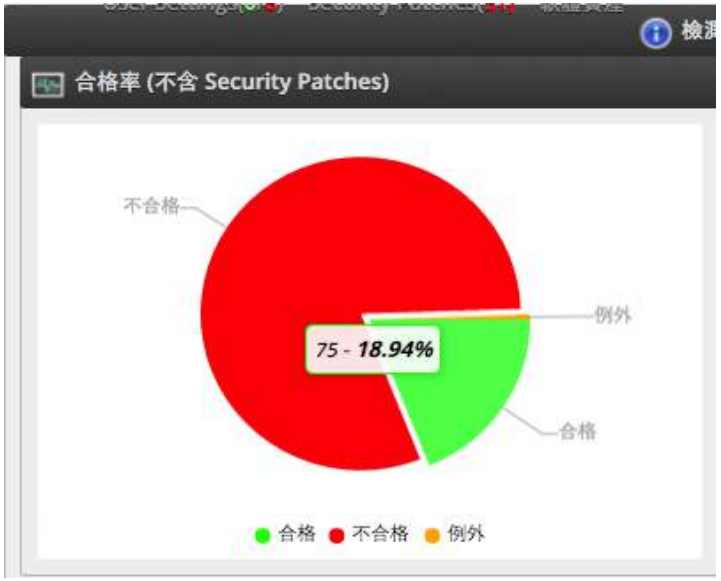
AD GPO停用/復原


群組原則管理
檔案(F) 執行(A) 檢視(V) 視窗(W) 說明(H)
群組原則管理
樹系: radiant-tech.com.tw
網域
radiant-tech.com.tw
Default Domain Policy
Domain Controllers
Radiant_HQ
USGCB Account Policy
USGCB IE8 Computer Settings
USGCB IE8 User settings
USGCB Win7 Computer Energy
USGCB Win7 Computer Settings
USGCB Win7 Firewall Settings
USGCB Win7 User Settings
WMI遠端管理開放
Radiant_Taipei
測試區
群組原則物件
WMI 篩選器
入門 GPO
站台
群組原則模型
群組原則結果
USGCB Account Policy
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。

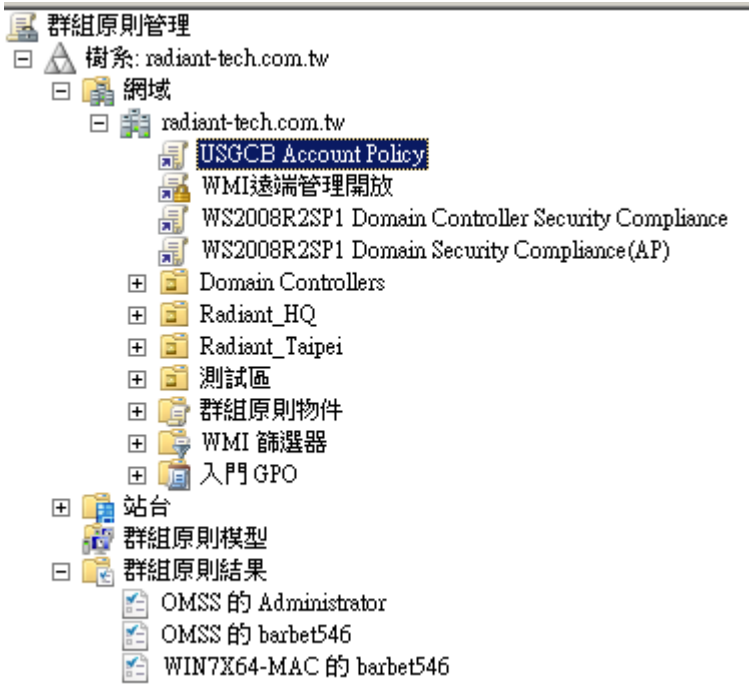
- 已發展GCB之密碼原則對照

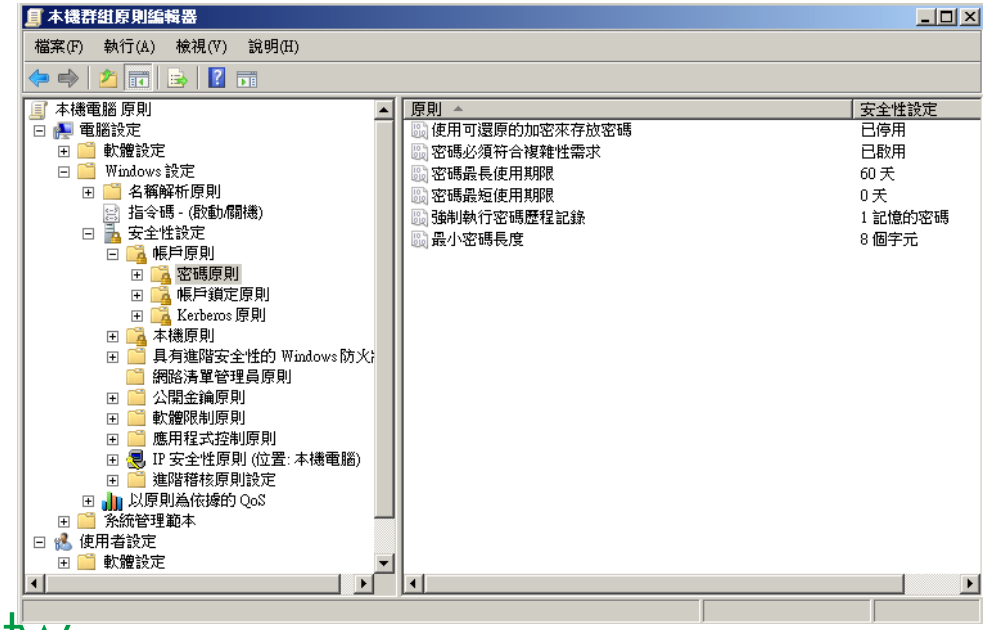
項次	項目名稱	原設定值	調整後之 Windows 7 設定值	調整後之 Windows 8.1 設定值	調整後之 Windows Server 2008 R2 設定值
1	密碼最長使用期限	60(天)	90(天)以下	90(天)以下	90(天)以下
2	最小密碼長度	12(碼)	8(碼)以上	8(碼)以上	12(碼)
3	強制執行密碼歷程記錄	24(次)	3(次)以上	3(次)以上	3(次)以上

- 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

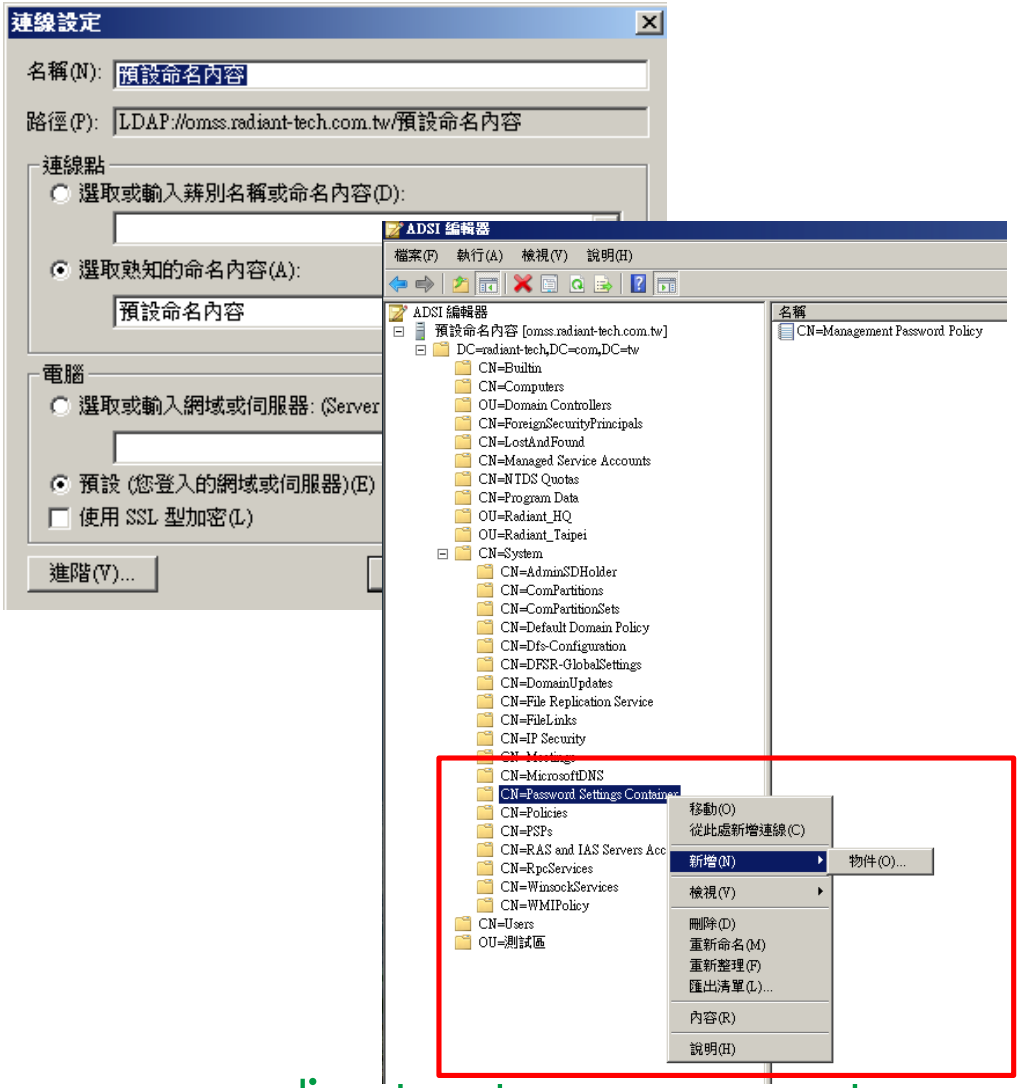
- **密碼設定容區(Password Settings Container；PSC)**

  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。

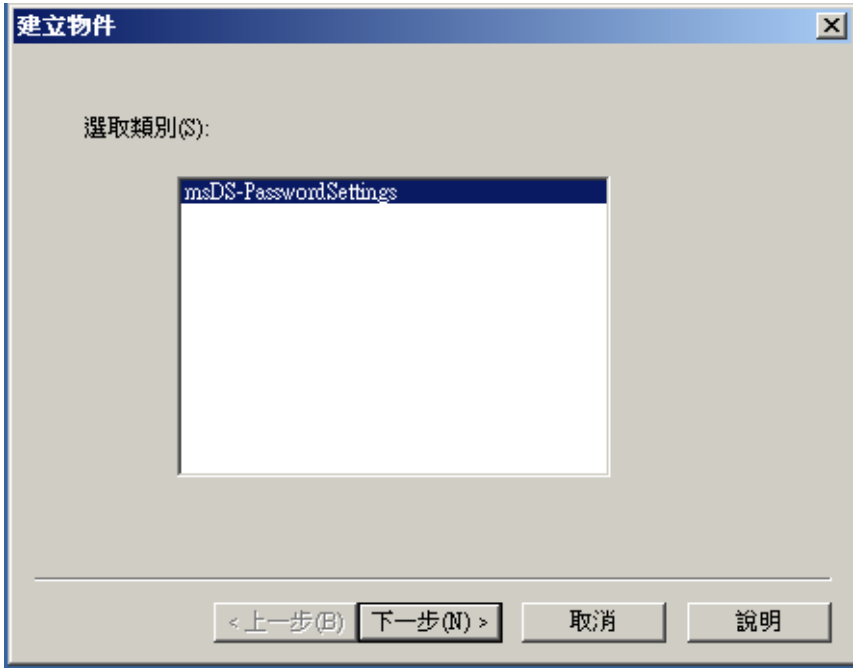
ADSI編輯器創設PSO



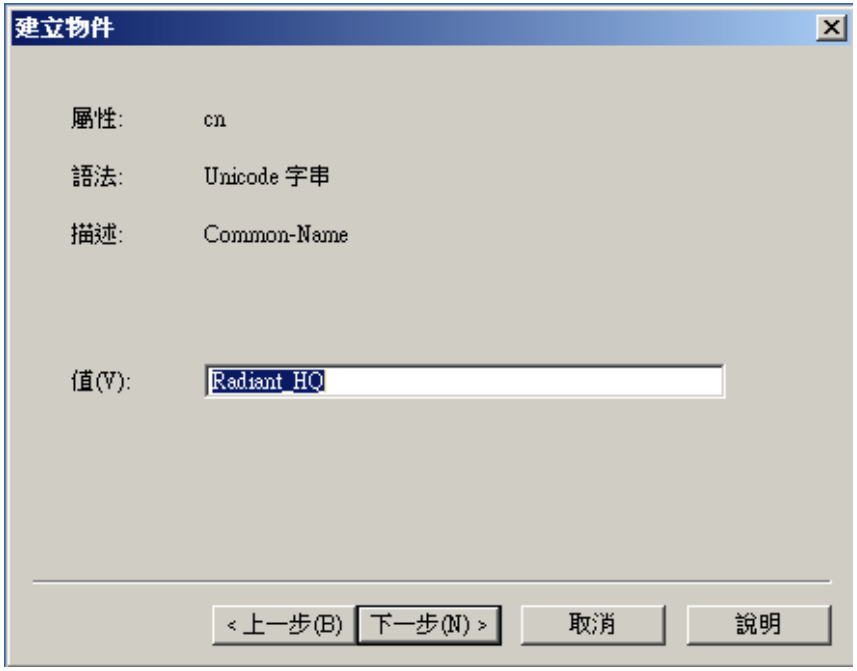
- 開啟ADSI編輯器(adsiedit.msc)
- 執行→連線到→預設命名內容
- DC=XXXX,DC=XXXX,DC=XX
  →CN=System
  →CN=Password Settings Container
  →新增物件

Password Settings Container

建立Password Settings Container物件



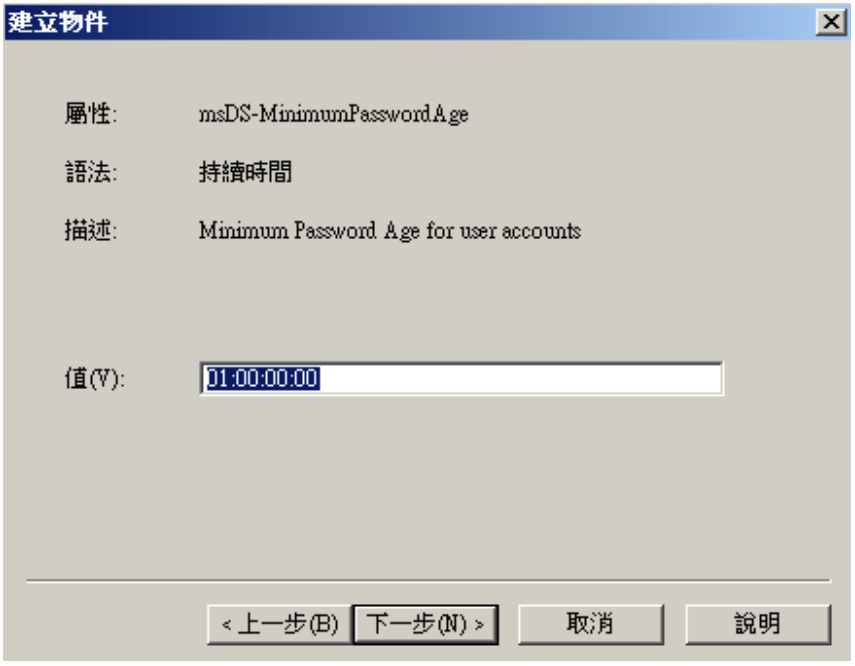
設定物件名稱：「XXXXX」(字串)



最小密碼長度、最短使用期限

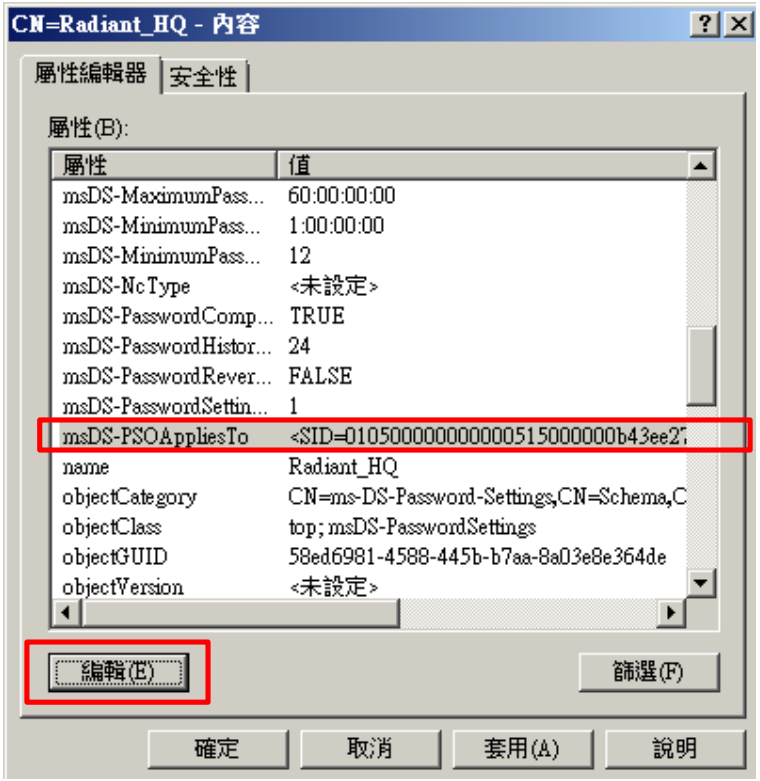
最小密碼長度，TWGCB針對Server之建議值為12，

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)



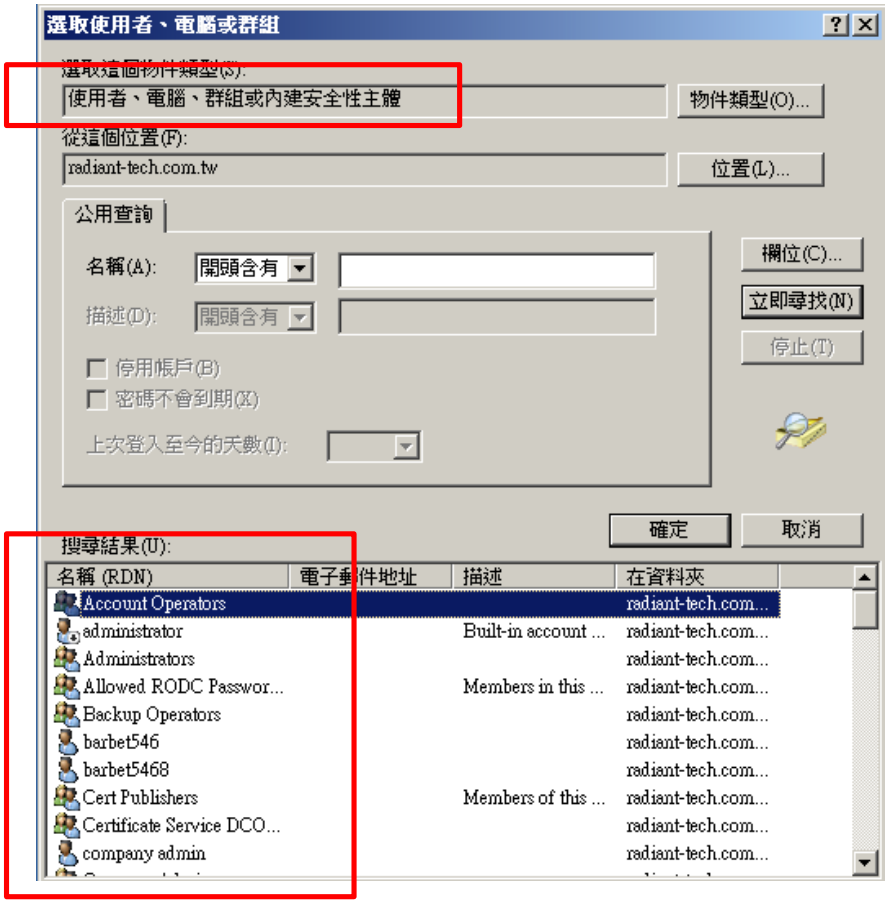
msDS-PSOAppliesTo設定

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。

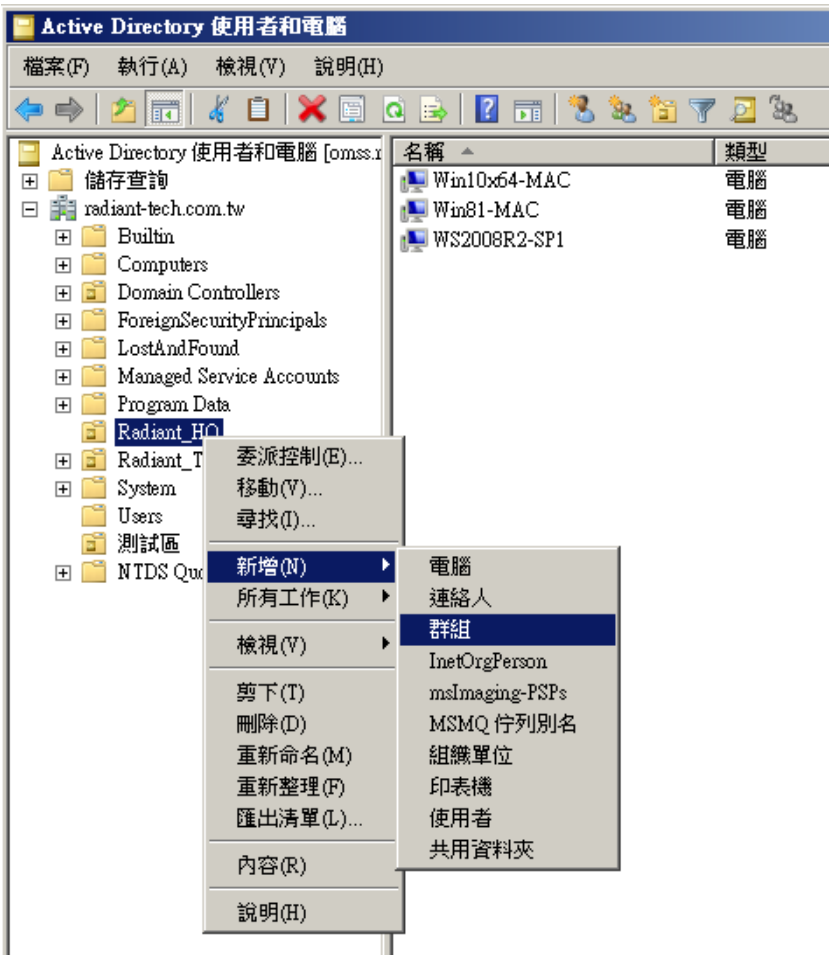


msDS-PSOAppliesTo

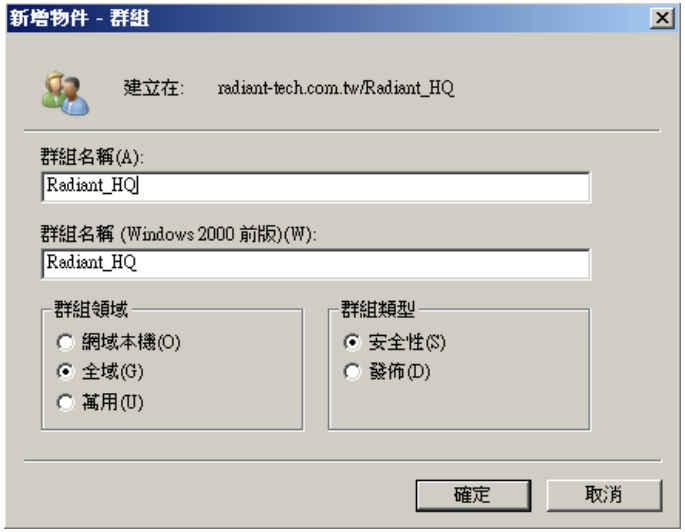
msDS-PSOAppliesTo只能套用於使用者、群組或電腦，
注意：並不能套用於組織單位(OU)



msDS-PSOAppliesTo組織單位

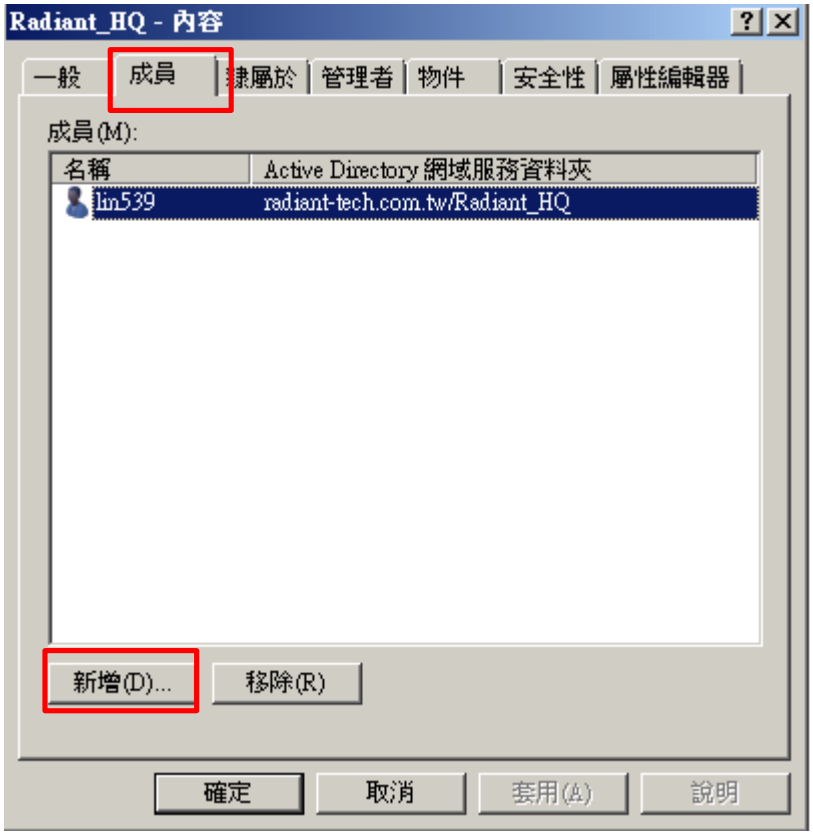


- 開啟AD使用者與電腦管理工具
- 在選定的「組織」→新增→群組
- 「群組名稱」建議與「組織單位」名稱相同

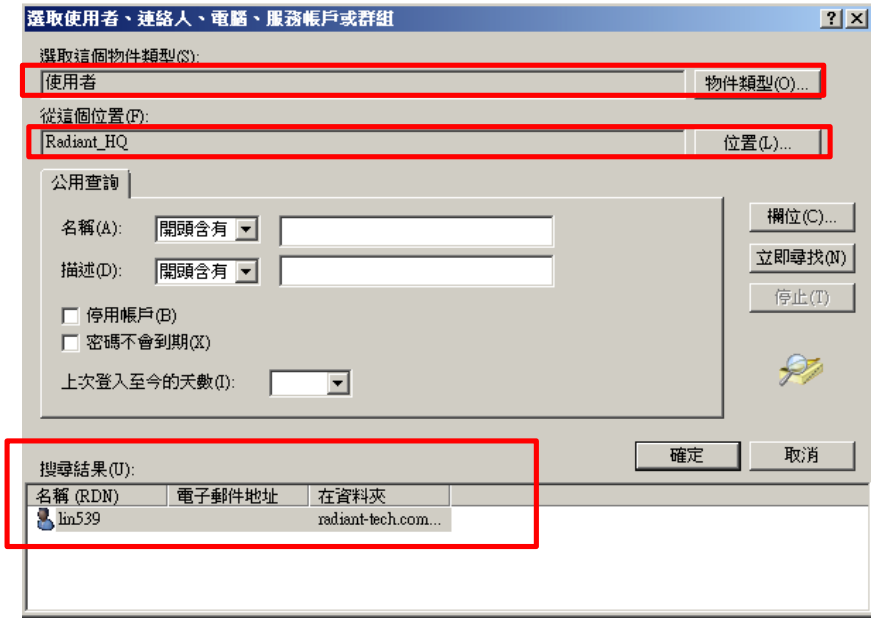


設定群組之成員

開啟群組內容，選取「成員」

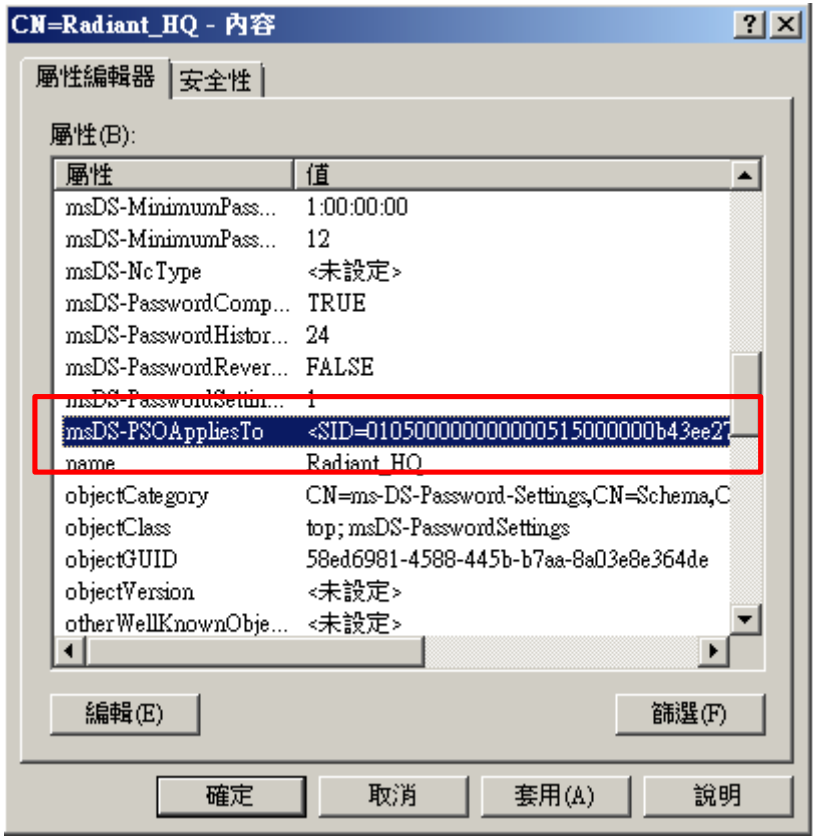


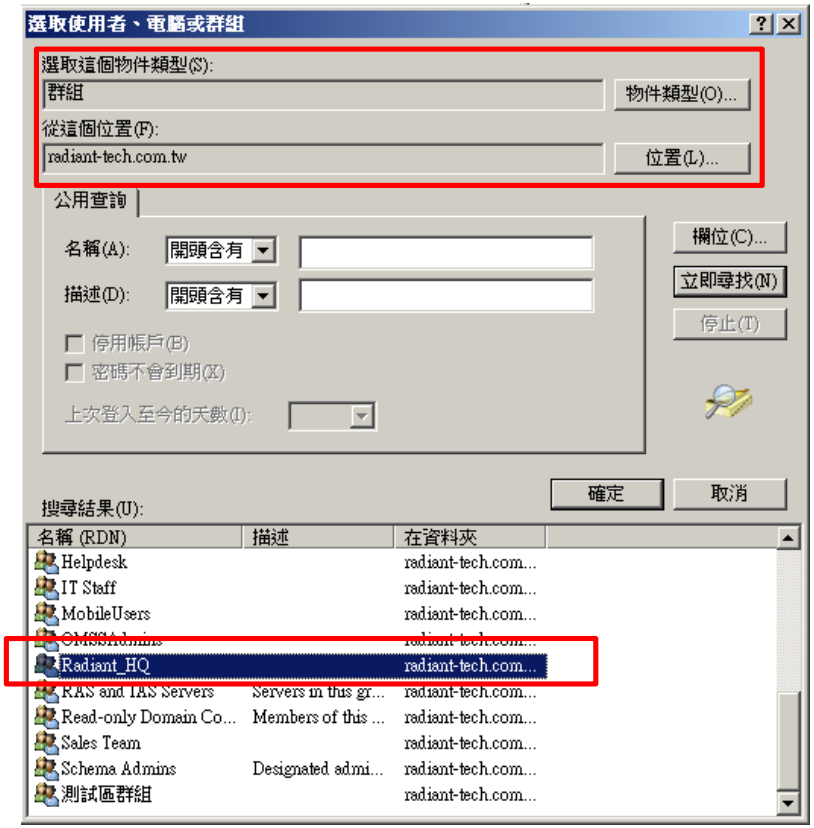
新增成員→物件類型：使用者→
位置：選定之組織單位
將所有隸屬於選定之「組織單位」
所有之使用者，加入在本群組中



msDS-PSOAppliesTo指定群組

msDS-PSOAppliesTo Radiant_HQ

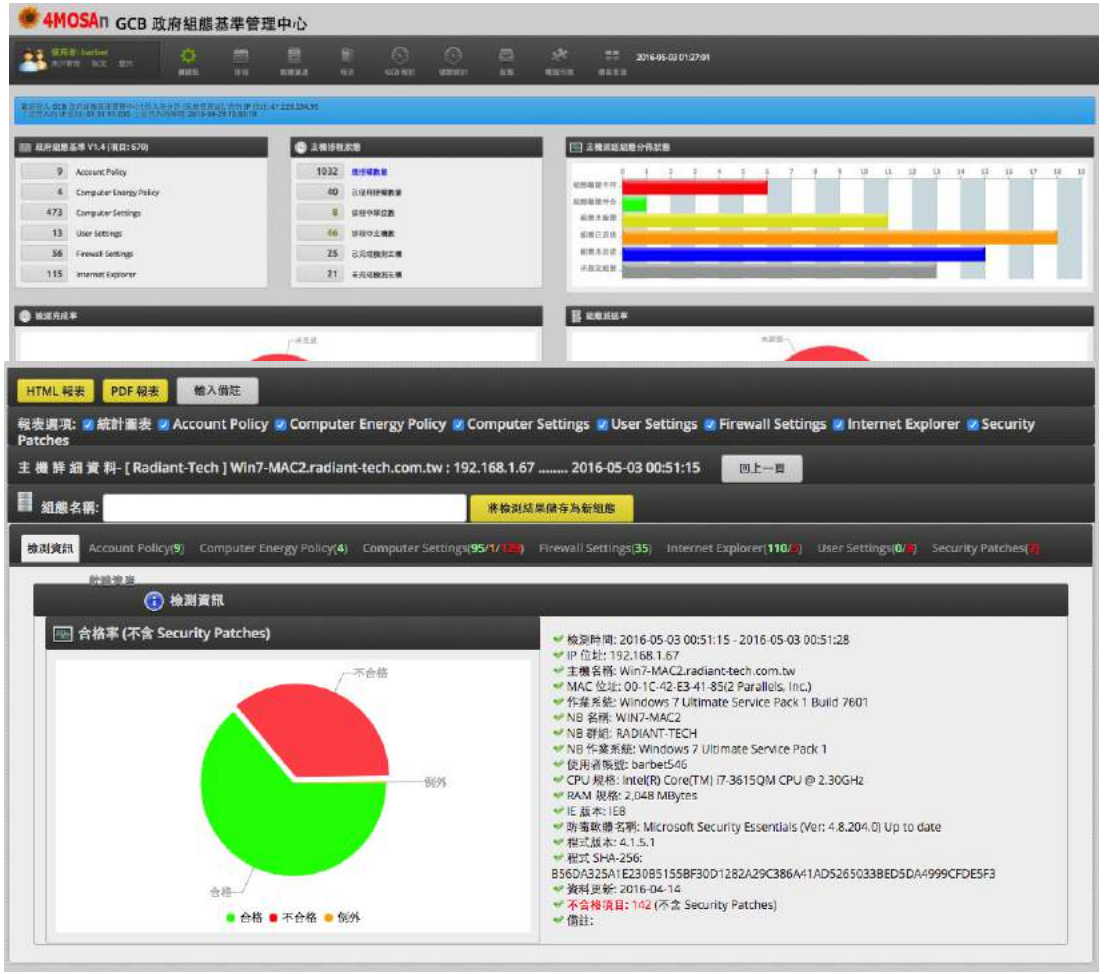


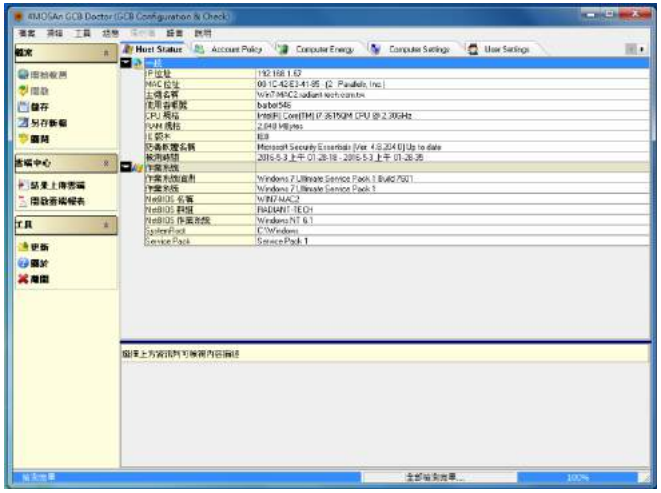


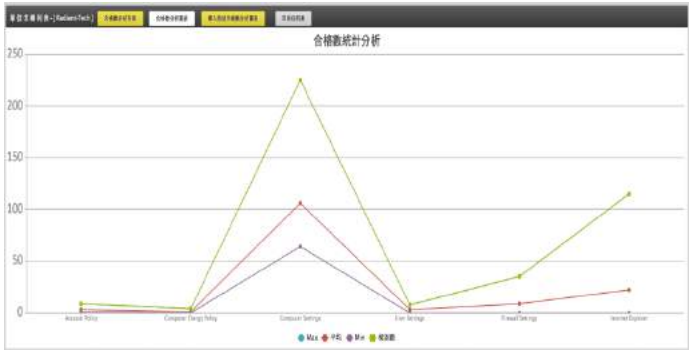
你可以有更SMART的方法！

請看GCB Doctor如何滿足您的需求！

4MOSAn GCB Doctor





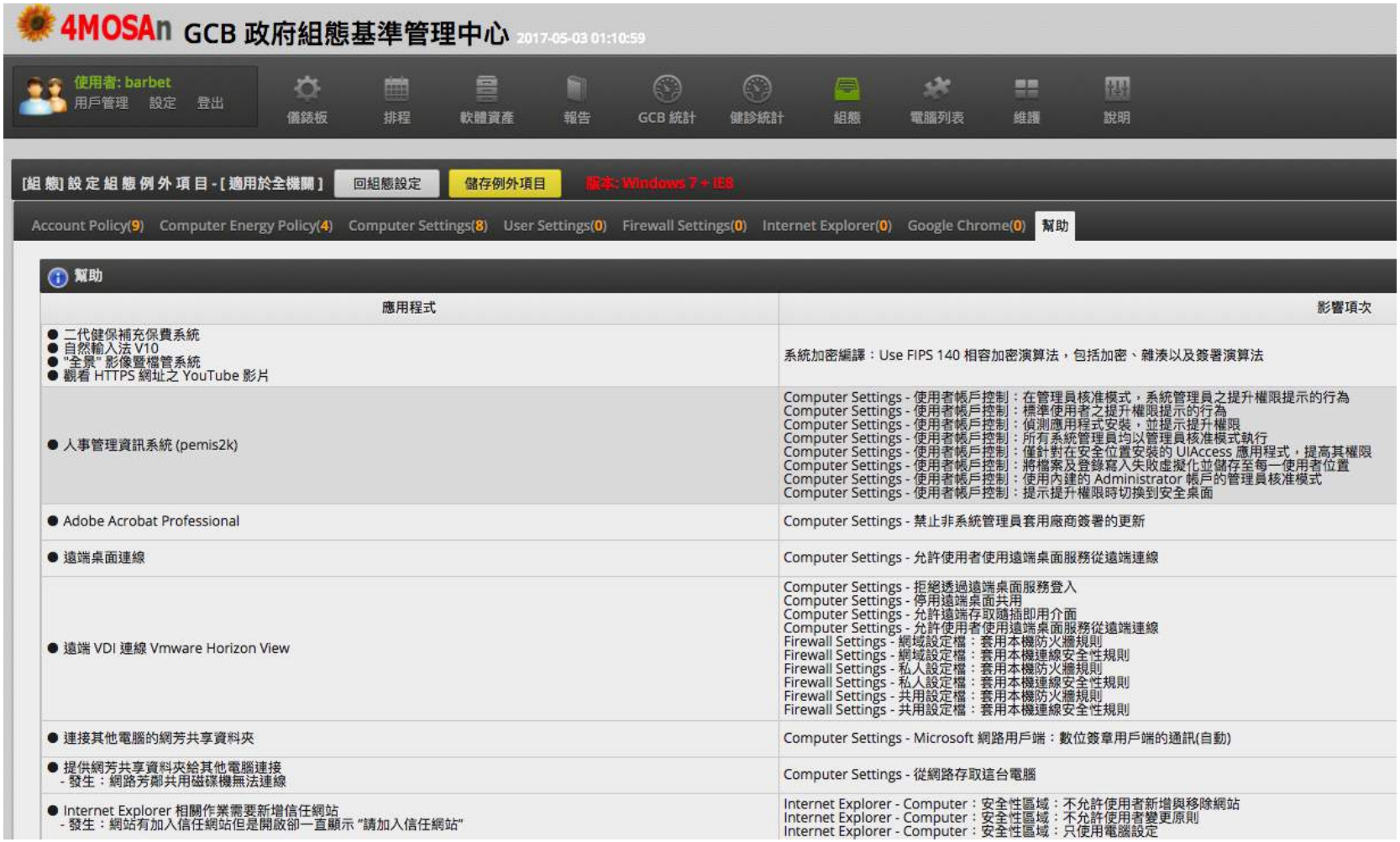


組態套用至全機關

指定組態套用至全機關

指定組態套用至個別主機

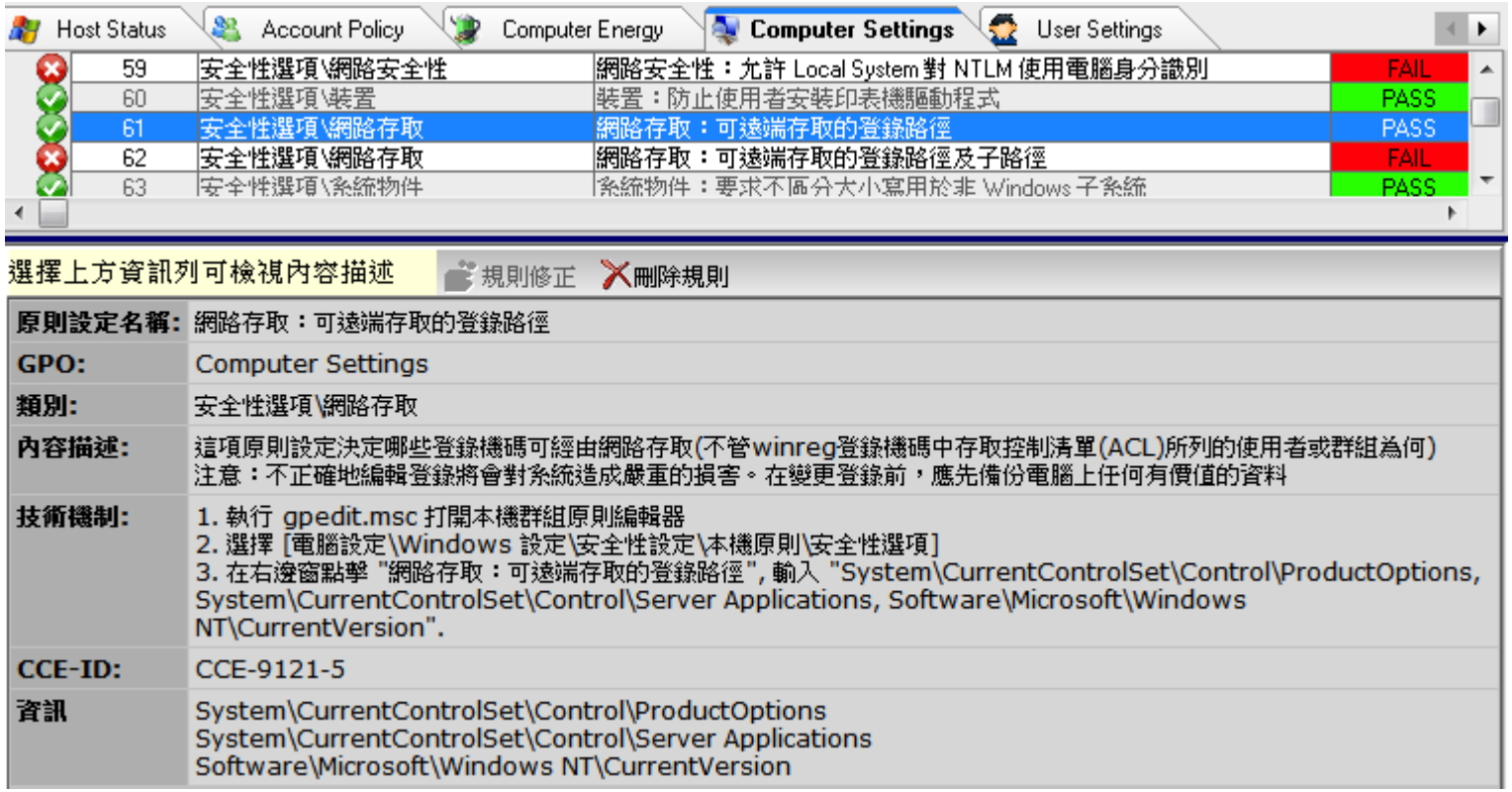
例外組態管理


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
幫助
應用程式
影響項次
● 二代健保補充保費系統
● 自然輸入法 V10
● "全景" 影像暨檔管系統
● 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
● 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
● Adobe Acrobat Professional
Computer Settings - 禁止非系統管理員套用廠商簽署的更新
● 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
● 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
● 連接其他電腦的網芳共享資料夾
Computer Settings - Microsoft 網路用戶端：數位簽章用戶端的通訊(自動)
● 提供網芳共享資料夾給其他電腦連接
- 發生：網路芳鄰共用磁碟機無法連線
Computer Settings - 從網路存取這台電腦
● 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

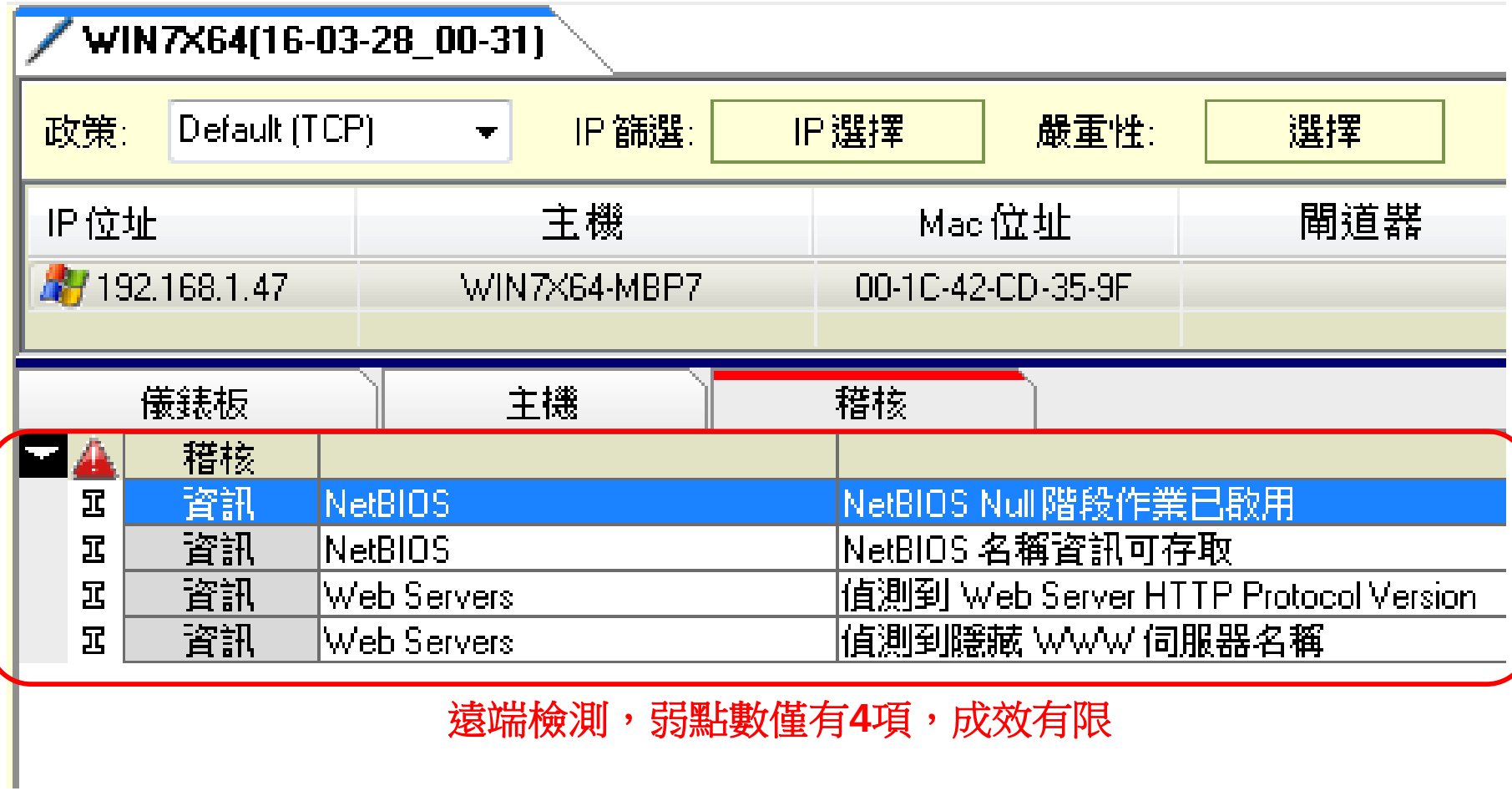
Windows 在 Vista 之後(包含Win7/Server2008) ，Remote Registry 預設為 LocalService 啟動，導致無法由遠端進行檢測



網路型弱點掃描-遠端檢測

單一台PC檢測所需時間

網路型弱點掃描-檢測結果



遠端檢測，弱點數僅有4項，成效有限

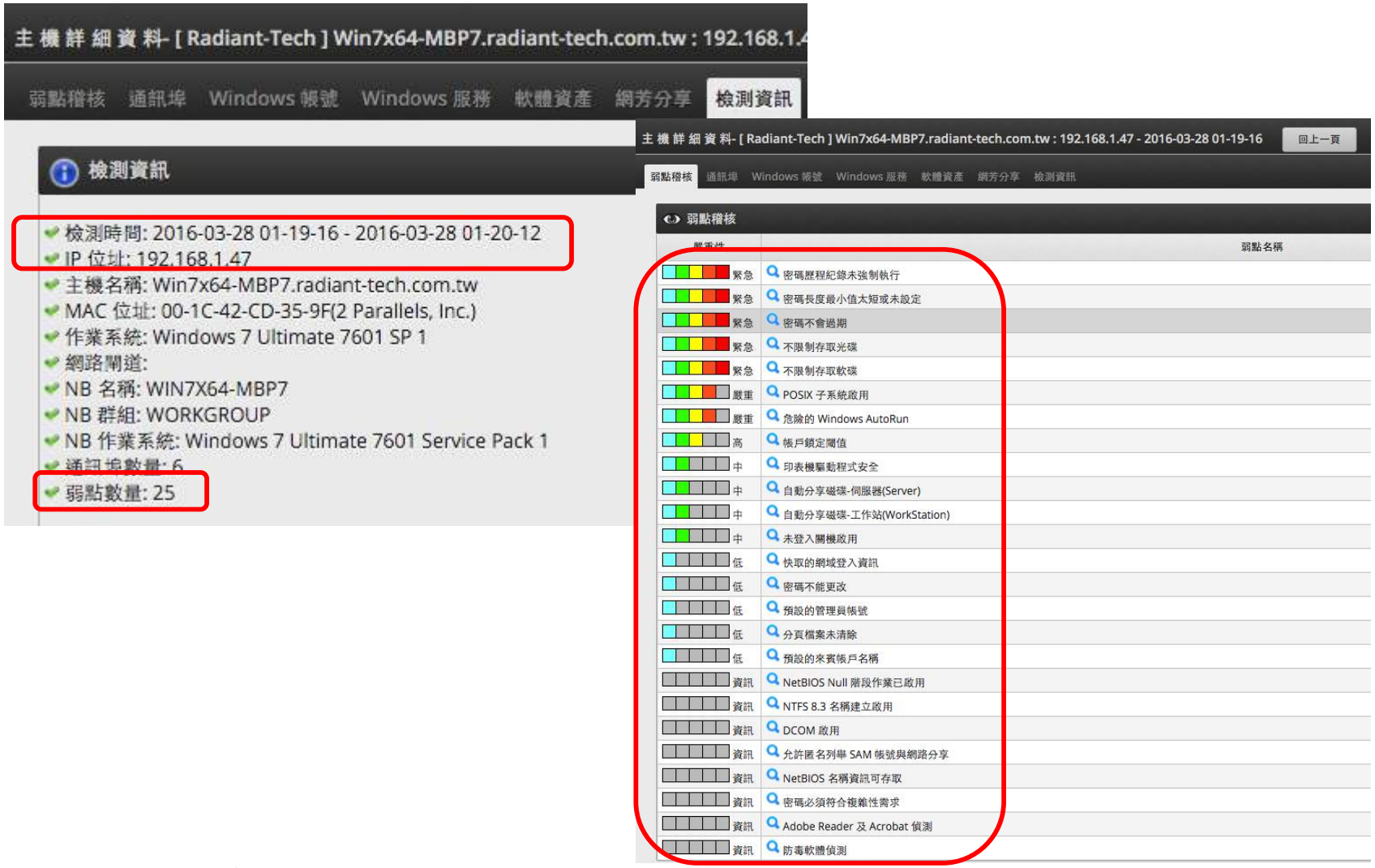
分散式弱點掃描-檢測

檢測狀態 | 稽核

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.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	
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
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	
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



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: Score (worst first)

109個弱點未修補

Security Update Scan Results

Score	Issue	Result
	Windows Security Updates	109 security updates are missing. 2 service packs or update rollups are missing.
	Developer Tools, Runtimes, and Redistributables Security Updates	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: Score (worst first)

無法檢測

Security Update Scan Results

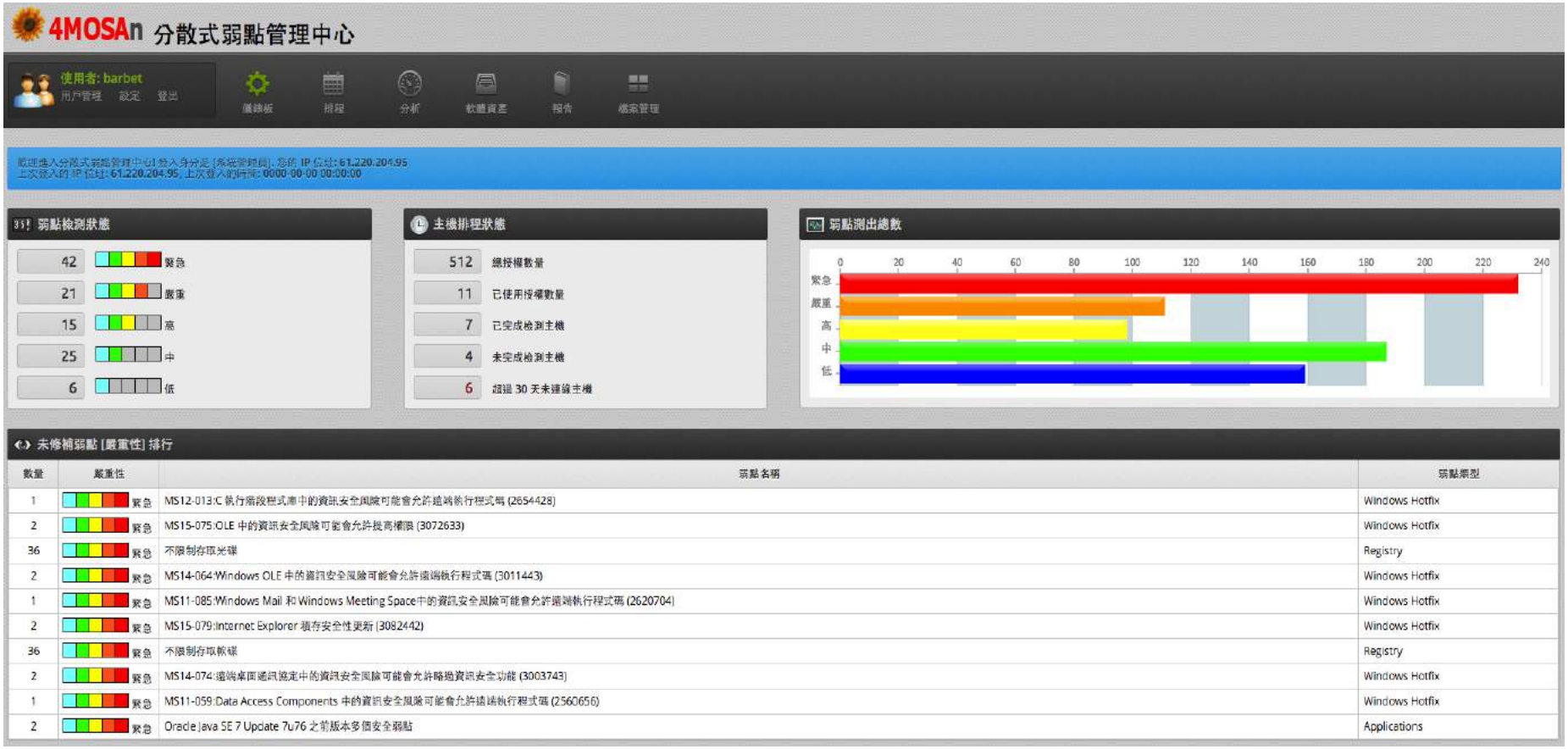
Score	Issue	Result
	Security Updates	Cannot contact Windows Update Agent on target computer, possibly due to firewall settings. What was scanned How to correct this

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 in 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.

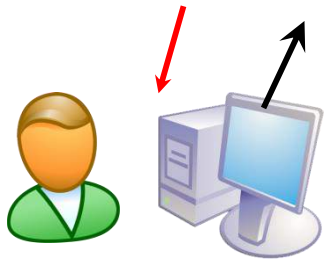
管理中心--儀表板



數量	嚴重性	弱點名稱	弱點類型
1	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)	Windows Hotfix
2	緊急	MS15-075:OLE 中的資訊安全風險可能會允許提高權限 (3072633)	Windows Hotfix
36	緊急	不限制存取光碟	Registry
2	緊急	MS14-064:Windows OLE 中的資訊安全風險可能會允許遠端執行程式碼 (3011443)	Windows Hotfix
1	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)	Windows Hotfix
2	緊急	MS15-079:Internet Explorer 累存安全性更新 (3082442)	Windows Hotfix
36	緊急	不限制存取軟碟	Registry
2	緊急	MS14-074:遠端桌面通訊協定中的資訊安全風險可能會允許略過資訊安全功能 (3003743)	Windows Hotfix
1	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)	Windows Hotfix
2	緊急	Oracle Java SE 7 Update 7u76 之前版本多個安全弱點	Applications

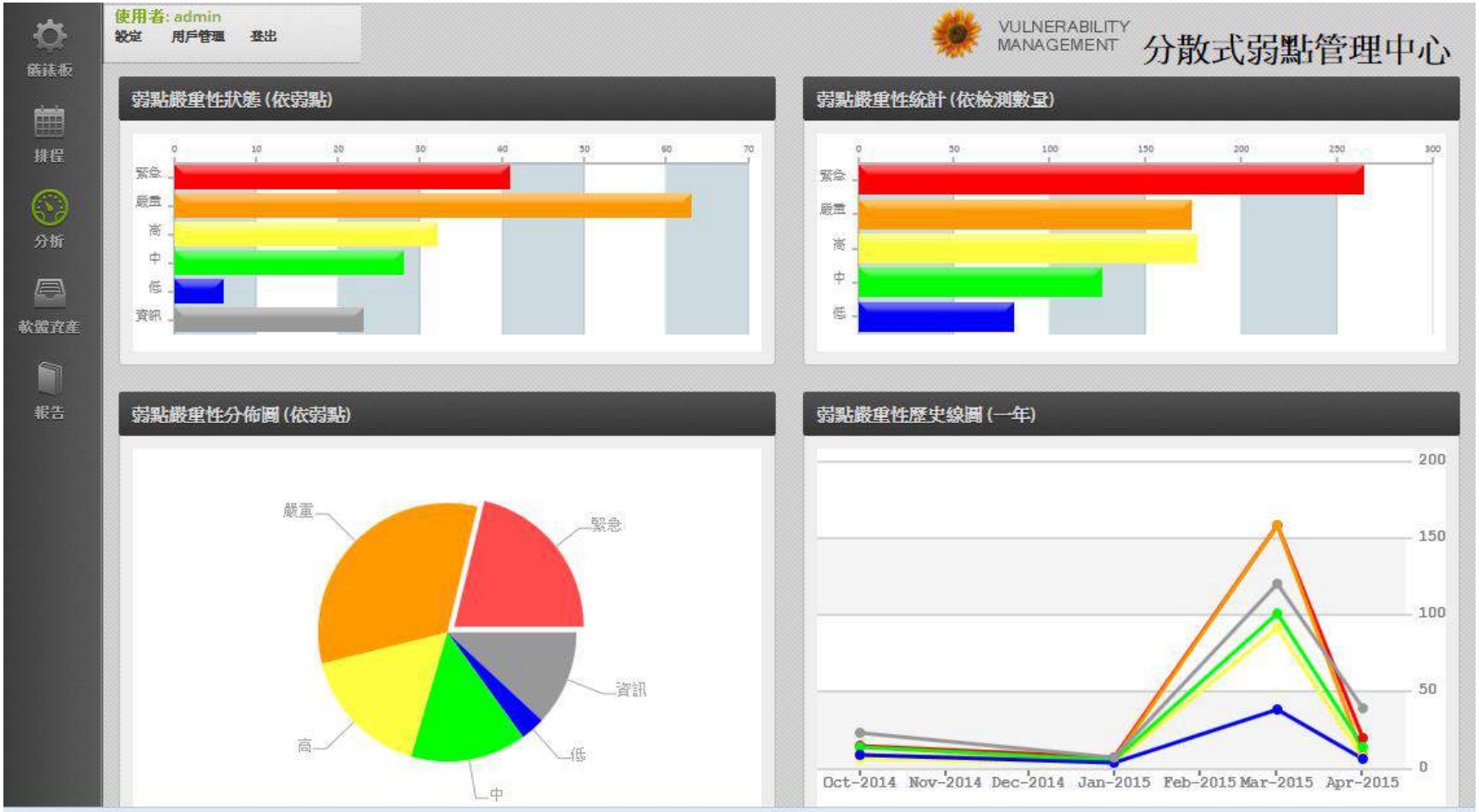
管理中心--排程功能

- 管理員從Web介面安排子單位 排程掃描



弱點稽核管理員

管理中心--分析功能


使用者: admin
設定
用戶管理
登出
儀表板
排程
分析
軟體資產
報告
VULNERABILITY MANAGEMENT
分散式弱點管理中心
弱點嚴重性狀態 (依弱點)
緊急
嚴重
高
中
低
資訊
弱點嚴重性統計 (依檢測數量)
弱點嚴重性分佈圖 (依弱點)
弱點嚴重性歷史線圖 (一年)
Oct-2014
Nov-2014
Dec-2014
Jan-2015
Feb-2015
Mar-2015
Apr-2015

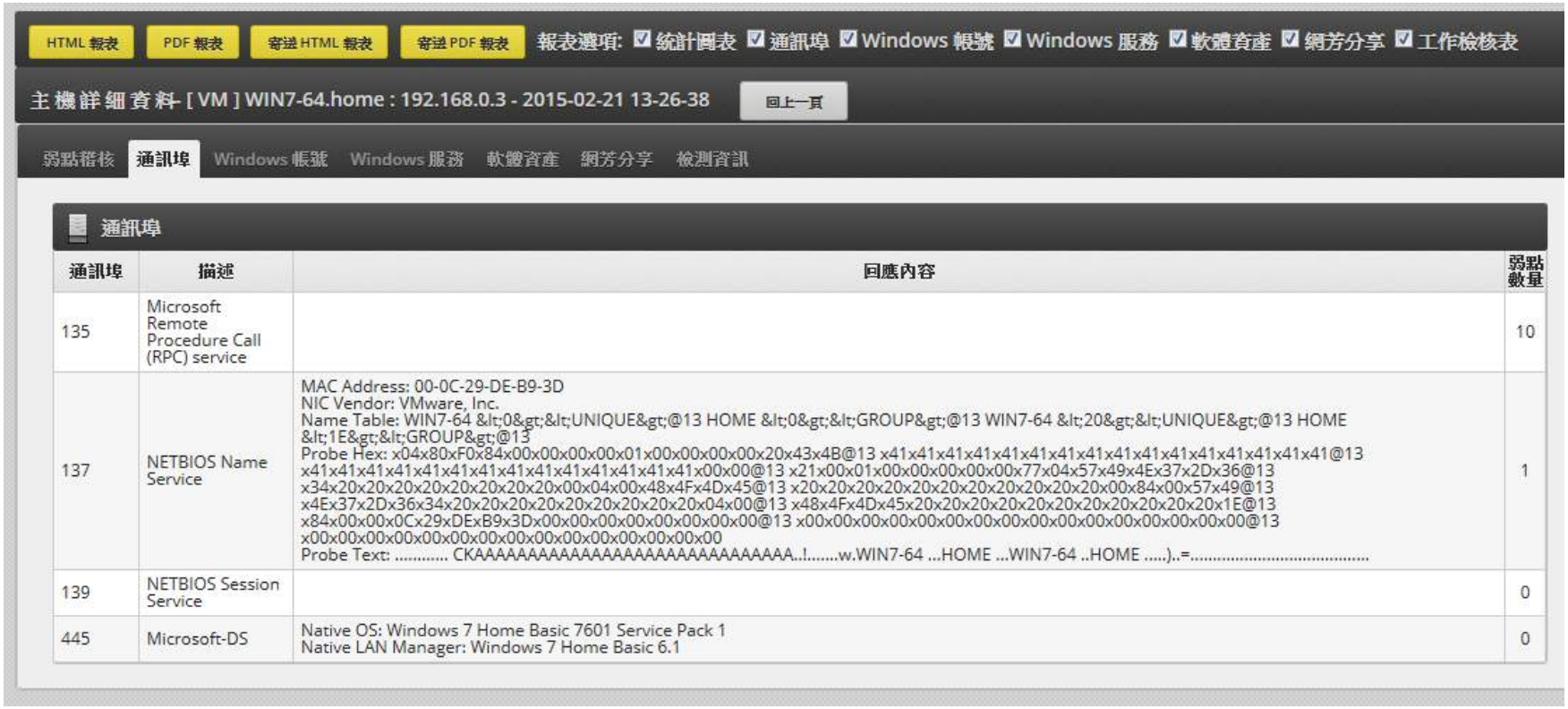
管理中心--軟體資產功能


使用者: weckl
設定
用戶管理
登出
VULNERABILITY MANAGEMENT
分散式弱點管理中心
儀錶板
排程
分析
軟體資產
報告
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

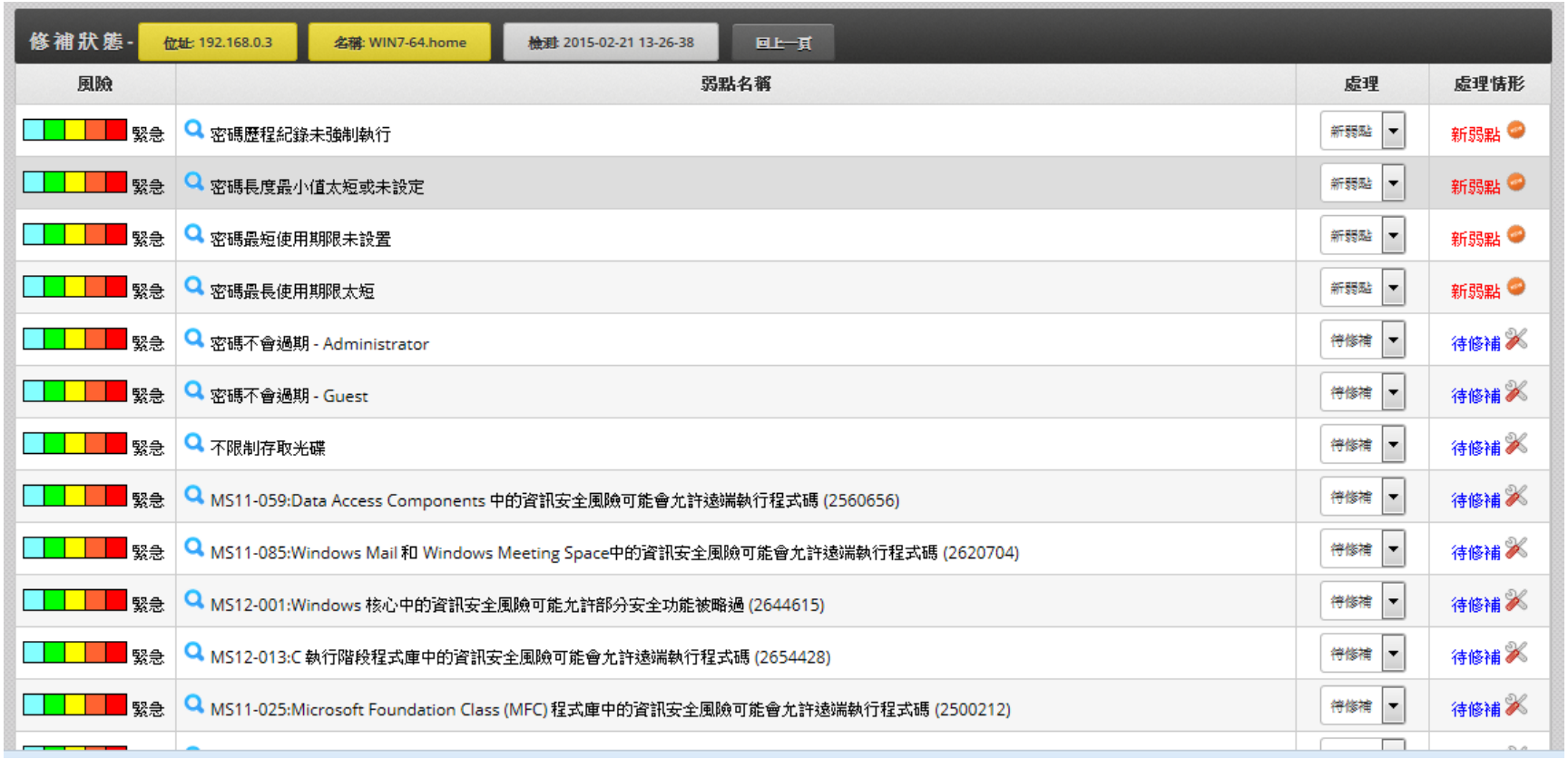

使用者: admin
設定 用戶管理 登出
VULNERABILITY MANAGEMENT
分散式弱點管理中心
[產生報表選項] 格式: HTML PDF | 嚴重性篩選: 緊急 嚴重 高 中 低 資訊
單位主機列表-[VM] 回單位列表
全部勾選
IP 位址
MAC 位址
作業系統
完成檢測
弱點數
掃描狀態
檢視 WIN7-64 192.168.0.3 00-0C-29-DE-B9-3D Windows 7 Home Basic 7601 SP 1 2015-02-21 13-27-21 65 8 天後
檢視 WIN8-BETA 192.168.0.11 00-0C-29-AE-86-8F Windows 8 Consumer Preview 8250 2015-02-20 21-45-57 48 8 天後
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
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
檢視 WIN-KMVNE5051BV 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--報告檢視功能



通訊埠	描述	回應內容	弱點數量
135	Microsoft Remote Procedure Call (RPC) service		10
137	NETBIOS Name Service	MAC Address: 00-0C-29-DE-B9-3D NIC Vendor: VMware, Inc. Name Table: WIN7-64 <0><UNIQUE>@13 HOME <0><GROUP>@13 WIN7-64 <20><UNIQUE>@13 HOME <1E><GROUP>@13 Probe Hex: x04x80xF0x84x00x00x00x00x01x00x00x00x00x20x43x4B@13 x41x41x41x41x41x41x41x41x41x41x41x41x41x41x41x41@13 x41x41x41x41x41x41x41x41x41x41x41x41x00x00@13 x21x00x01x00x00x00x00x00x77x04x57x49x4Ex37x2Dx36@13 x34x20x20x20x20x20x20x20x20x00x04x00x48x4Fx4Dx45@13 x20x20x20x20x20x20x20x20x20x20x20x00x84x00x57x49@13 x4Ex37x2Dx36x34x20x20x20x20x20x20x20x20x04x00@13 x48x4Fx4Dx45x20x20x20x20x20x20x20x20x20x20x20x1E@13 x84x00x00x0Cx29xDExB9x3Dx00x00x00x00x00x00x00x00@13 x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00x00@13 x00x00x00x00x00x00x00x00x00x00x00x00x00 Probe Text: ..... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!.....w.WIN7-64 ...HOME ...WIN7-64 ..HOME .....)..=.....	1
139	NETBIOS Session Service		0
445	Microsoft-DS	Native OS: Windows 7 Home Basic 7601 Service Pack 1 Native LAN Manager: Windows 7 Home Basic 6.1	0

管理中心--修補狀態



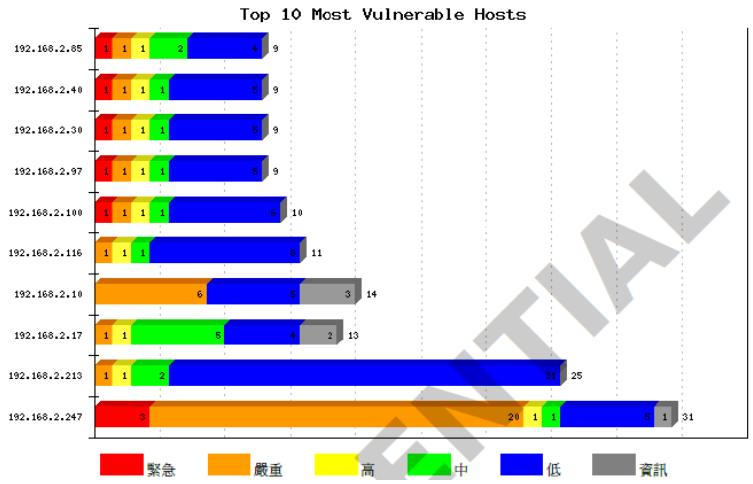
風險	弱點名稱	處理	處理情形
緊急	密碼歷程紀錄未強制執行	新弱點	新弱點
緊急	密碼長度最小值太短或未設定	新弱點	新弱點
緊急	密碼最短使用期限未設置	新弱點	新弱點
緊急	密碼最長使用期限太短	新弱點	新弱點
緊急	密碼不會過期 - Administrator	待修補	待修補
緊急	密碼不會過期 - Guest	待修補	待修補
緊急	不限制存取光碟	待修補	待修補
緊急	MS11-059:Data Access Components 中的資訊安全風險可能會允許遠端執行程式碼 (2560656)	待修補	待修補
緊急	MS11-085:Windows Mail 和 Windows Meeting 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

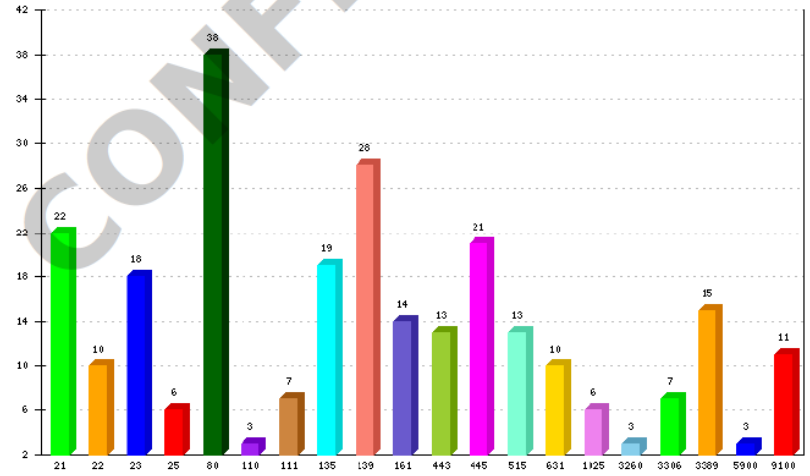

嚴重性篩選: 緊急 嚴重 高 中 低 資訊 篩選
單位弱點列表-[測試] 回單位主機列表
嚴重性
弱點名稱
主機
緊急 密碼歷程紀錄未強制執行
FSERVER, 112.104.105.116 1
gate7.home, 192.168.0.6 1
2core-win7, 25.127.19.241 1
緊急 密碼長度最小值太短或未設定
FSERVER, 112.104.105.116 1
gate7.home, 192.168.0.6 1
2core-win7, 25.127.19.241 1
緊急 密碼最短使用期限未設置
FSERVER, 112.104.105.116 1
gate7.home, 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

管理報告包含多種統計圖表

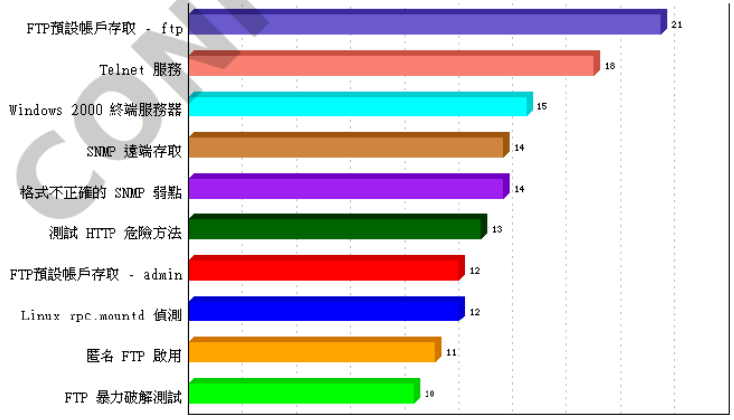
前 10 名高風險主機分佈



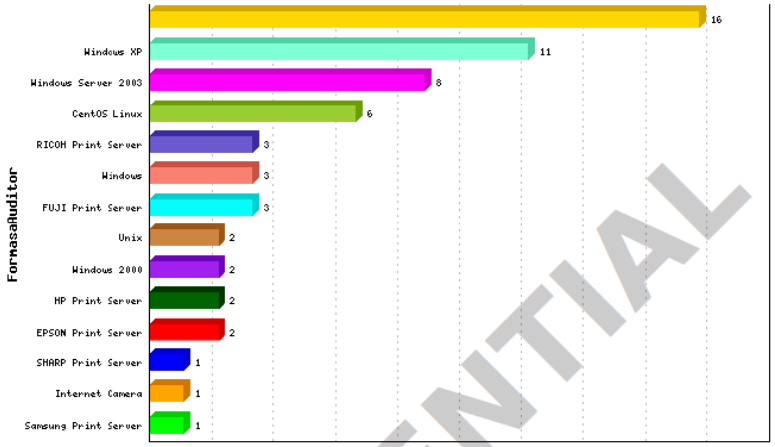
前 20 名網路服務統計



前 10 名弱點分佈



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
WIN7-YUYUYU
(JUST GUESSING): Windows 7, Server 2008 R2 (x64)
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?