世染纖塵難自騎 斷勝慶世證慧衷 顿醒毫揮寰宇明 吟嘯顶峰袋紅塵

Windows 技術 ▽

Windows 伺服器技術 ▽ Linux ▽

資訊安全 ▽ 雲端運算 マ 行動裝置技術 ▽

其它文章 ▽

關鍵字搜尋網站文章





網站文章:

- **2013 (8)**
- **2012** (55)
- **2011** (42)
 - ▶ 十二月 (9)
 - ▼ 十一月 (32)

使用Windows行動碟加密技術--Bitlocker To Go

架設802.1X無線網路安全性架構

可信賴平台模組 (Trusted Platform Module)

Windows 7的內建螢幕擷取 (Screen Capture)/小工具snipping tool

Bitlocker 磁碟加密 (BitLocker drive encryption)技術

Wndows 服務的主機處理程序svchost

破解802.11 WEP 金鑰

設定 Windows 7 成為 VPN 伺服

Linux網路結合(network

2011年11月12日星期六

Windows Server 2008 更細緻的密碼原則 (Windows Server 2008 Fine-**Grained Password Policy**)

前言

在以往Windows Server 2003以前的Active Directory網域中,只允許針對網域等級設定單一 密碼原則與鎖定原則,亦即網域內的所有使用者均必須遵循並使用相同的原則,這似乎不夠彈 性,因此Windows Server 2008的Active Directory網域環境提供了一個更細緻的密碼原則 (Fine-Grained Password Policies)功能,允許讓管理人員針對網域內的不同使用者或群組設定 不一樣的密碼原則與鎖定原則。

細緻的密碼原則使用二個新的物件類別來存放在原則設定:

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。

bonding)技術與實務

更改 Windows Server 憑證服務 所發行的認證到期日期

裝置容錯與負載平衡機制

簡介 IPv6

使用『問題步驟收錄程式 (Problem Steps Recorder; PSR)』

Hyper-V 的VLAN

Hyper-V 虛擬網路

覆蓋可用磁碟空間以確保刪除資料不會外洩

匯出/匯入無線網路設定檔

Windows Server 2008 更細緻 的密碼原則 (Windows Server 2008 ...

停用IPv6

談微軟啟用技術 (Windows Activation Technologies; WAT)

解決IP位址被隱藏的網卡占用而 導致目前的網卡無法設定IP的 問題

利用拖放方式(Drag and Drop) 以避免在命令列輸入冗長路 徑

解決無法刪除Hyper-v 虛擬機器 的問題

使用命令列指令設定時區-tzutil

如何避免Windows 7/2008 R2 建立100MB的隱藏系統分割 區

使用 Powercfg 執行電源管理

IIS 7.5 安裝PHP與MySQL

建立與管理虛擬磁碟

Linux 安裝後安全性功能的調整 與設定

修復Windows 無法開機的工具

■ 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。

設定細緻化的密碼原則

使用這項新的細緻化密碼原則功能,先決條件為您須要擁有網域管理人員的權限而且網域功能等級為Windows Server 2008以上。

首先,您必需使用ADSI編輯器創造並設定PSO。

- 1. 從系統管理工具功能表內開啟「ADSI編輯器(Adsiedit.msc)」。
- 2. 以滑鼠右鍵點選【ADSI編輯器】並選擇【連線到】。
- 3. 假若連線設定對話方塊上出現【預設命名內容】和網域名稱則直接按【確定】接受預設值。



Windows 基本維護工作

- 由檔案總管進入超長目錄路徑的 命令提示字元
- ▶ 十月 (1)

文章分類:

- Linux 安全性 (12)
- 網路與通訊安全性管理實務 (12)
- Windows 伺服器安全管理 (9)
- Windows 隨手小技巧 (9)
- Windows 安全性管理與實務 (8)
- Hyper-V 虛擬化 (7)
- Windows 桌面平台技術 (7)
- IIS 網站管理 (6)
- VMware 虛擬化 (6)
- Windows 伺服器技術 (6)
- Windows 偵測、監控、診斷與修 復技術 (6)
- Windows 網路 (6)
- Windows 效能調整 (4)
- android (4)
- 基礎網路 (4)
- 網路與通訊安全性理論與原理 (4)
- 行動裝置技術 (4)
- Linux網路(3)
- Windows 8 (3)
- 其它(3)
- 磁碟與檔案系統管理(3)
- Windows 整合通訊 (2)
- 攻擊手法 (2)
- Exchange 伺服器 (1)
- Linux 基礎管理 (1)
- 密碼學 (1)
- 雲端資安(1)
- 雲端運算基礎與概論(1)

4. 接下來,擴展網域名稱下的CN=System 這個容區,並往下找到CN=Password Settings Container物件,(亦即點選點至如下的路徑:DC=xx, DC=xx, CN=System, CN=Password Settings Container),並在於Password Setting Container上點選右鍵,選取【新增物件】,這將啟動精靈程式讓您開始設定PSO。



5. 首先在【建立物件】對話方塊,msDS-PasswordSettings為唯一可選用的類別,故直接按【下一步】繼續。



6. 接下來的共用名稱(Common Name; cn)屬性中請輸入一個日後容易辨別的名稱。



7. 接下來的msDS-PasswordSettingsPrecedence (Password Settings Precedence)屬性中輸入一個大於等於1的值,這個值為PSO的優先權,值越低,優先權越高,如果一個使用者所隸屬的二個群組被連結至不同的PSO,一個連結的PSO優先值為5,另一個優先權為3,則優先權3的PSO將會覆蓋過優先值為5的PSO。



8. 接下來的精靈程式將開始設定密碼原則和鎖定原則的各種屬性,需要設定的屬性名稱和說明如下表所示:

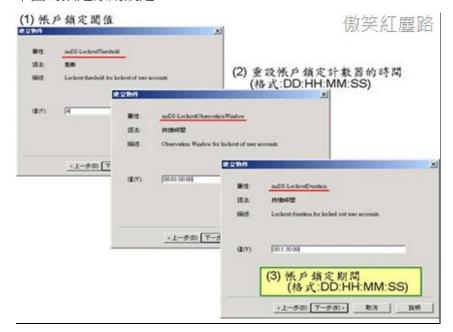
屬性名稱	說明	格式與範例
msDS- Password Reversible Encryption Enabled	是否使用可還原 的加密來存放密 碼	FALSE / TRUE (建議: FALSE)
msDS-PasswordHistoryLength	強制密碼歷程記錄	0 ~ 1024
msDS-PasswordComplexityEnabled	密碼必須符合複 雜性需求	FALSE / TRUE (建議: TRUE)
msDS-MinimumPasswordLength	最小密碼長度	0~255,建議7以上
msDS-MinimumPasswordAge	密碼最短使用期	dd:hh:mm:ss,例如

1:00:00:00 (一天) 限 msDS-MaximumPasswordAge dd:hh:mm:ss,例如 密碼最長使用期 45:00:00:00 (45天) 限 msDS-LockoutThreshold 0~ 65535 帳戶鎖定閾值 msDS-LockoutObservationWindow dd:hh:mm:ss,例如 重設帳戶鎖定計 00:01:00:00 (1小時) 數器的時間 msDS-LockoutDuration dd:hh:mm:ss,例如 帳戶鎖定期間 00:01:30:00 (90分鐘) 若設00:00:00:00 則 代,表永久鎖定直到管 理員解除

下圖為密碼原則設定畫面



下圖為鎖定原則設定:



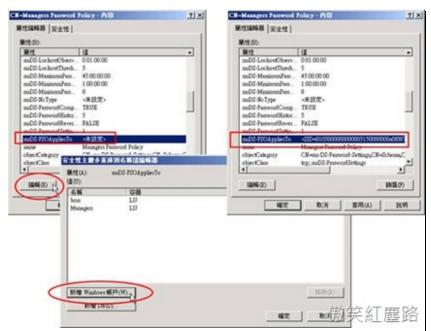
輸入屬性值時須要符合資料類型、格式與範圍,否則會出現如下圖的錯誤對話方塊。



9. 輸入一連串屬性後,請在精靈的最後一個畫面中,請按【完成】新增此PSO。



10. 接下來,請點選剛剛所建立好的物件按下右鍵功表的內容選項,以便可以設定最重要的一項屬性:msDS-PSOAppliesTo來將此PSO的密碼原則設定套用在特定的使用者或群組,所以請在內容對話方塊內編輯『msDS-PSOAppliesTo』這個屬性,並按【新增Windows帳戶】來新增想要應用這個PSO的使用者或群組。



PSO的應用優先順序問題

在大型網路環境下,使用者或群組物件可以連結到多個 PSO,因為使用者可能隸同時屬於多個群組 (而每個群組都被套用不同的 PSO),或多個 PSO 被直接套用至使用者或群組物件。但是只有唯一的一個 PSO 才能套用成為有效的密碼原則,亦即只有該 PSO 的設定才能影響使用者或群組,您並無法使用任何方式來合併多個 PSO 連結到使用者或群組的設定。

每個 PSO 都具有名為 msDS-PasswordSettingsPrecedence 的額外屬性,此屬性設計用來決定多個PSO間的使用優先權。msDS-PasswordSettingsPrecedence 屬性具有 1 以上的整數值,較小的 msDS-PasswordSettingsPrecedence 屬性值表示該 PSO 具有比其他 PSO 高的等級,或說具有較高的優先順序。例如,假設某使用者物件具有兩個連結的 PSO,其中一個 PSO 的 msDS-PasswordSettingsPrecedence 值為 10,另一個 PSO 的 msDS-

PasswordSettingsPrecedence 值為20,則在這個案例中,msDS-

PasswordSettingsPrecedence 值為 10 的 PSO 會具有較高的等級,因此它將會套用至物件,但如果有二個PSO的值相同,則需比較ObjectGUID,第一部份最右側的位元組,較小優先權較高。例如:下例中前者PSO將優先。

36429**12**-87cd-4672-ab8e-bd1e8496616b

7b33c5**4e**-a075-5a4d-869d-0b0e2455de61

綜合而論,如果有多個 PSO 連結至使用者或群組,決定要套用之結果 PSO 的方式如下:

- 1. 直接連結至使用者物件的 PSO 會成為結果 PSO,如果有多個PSO連結至使用者物件,則msDS-PasswordSettingsPrecedence 值最低者套用。
- 2. 如果沒有任何 PSO 直接連結到使用者物件,則會比較使用者所隸屬的全域安全性群組是 否有被連結到PSO,然後,具有最低 msDS-PasswordSettingsPrecedence 值的 PSO 將 會是結果 PSO。
- 3. 如果上述方式無法取得任何 PSO,則會套用預設網域密碼原則。

總之,PSO的應用優先順序為直接連接到使用者物件最為優先,次為連結到隸屬群組的PSO,

最後才是應用預設的網域密碼原則。



