

Foxconn

AD 應用

內部使用



呂術亮

2008/9/11

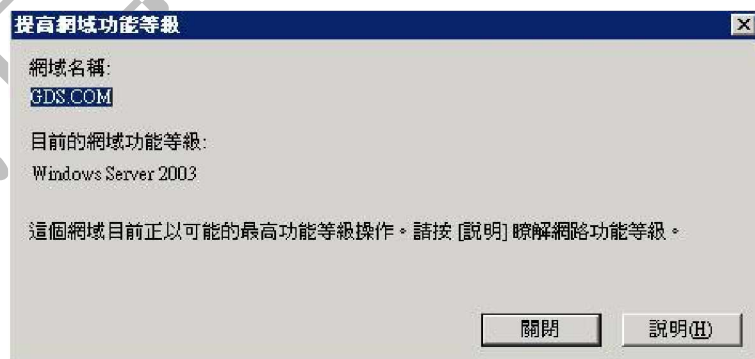
一、	提升 AD 網域功能等級	3
二、	OU 容器	4
2.1	Builtin 容器	4
2.2	Computers 容器	4
2.3	Domain Controllers 容器	4
2.4	Users 容器.....	5
三、	創建活動目錄對象	6
3.1	活動目錄介紹.....	6
3.2	新建組織單元(OU)	6
3.3	新建群組(Group)	7
3.4	新建電腦	8
3.5	新建使用者.....	9
3.6	10
四、	權限設定	11
4.1	Admins 群組權限設定(OU 管理權限)	11
4.2	群組之間權限隸屬	12
五、	委派控制	14
5.1	委派 OU 權限.....	14
5.2	其它事項	16
六、	策略套用	17
6.1	常用策略套用.....	17
6.2	軟體套用	19
6.3	批處理文件套用.....	20
6.4	腳本編寫	23
七、	外設限定	24
7.1	外設管制軟件.....	24
7.2	光驅、USB、DVD 限定.....	24
7.3	其它外設限定.....	27
7.4	用戶外設使用權限	27
八、	組策略工具	29
8.1	檢查域控制器上組策略對象--GpoTool	29
8.2	組策略結果檢查測工具-- GpResult	29
8.3	組策略刷新工具--Gpupdate	29
8.4	組策略管理控制臺--GPMC.....	30
8.5	組策略監視器--Winpolicies	31
九、	客戶端安裝 AD 管理工具	32
十、	THE END	32

一、提升 AD 網域功能等級

1. AD 建立完成后(默認為 Windows2000)，可以建立 OU，群組，但不能對群組權限進行互相加入，此時需要提升 AD 網域功能等級(Windows2003)
2. 打開 AD 管理界面【開始】---【系統管理工具】--【Active Directory 使用者及電腦】，開啟 AD 管理界面。



3. 選擇 Windows Server2003，確定即可由 2000 升級為 2003



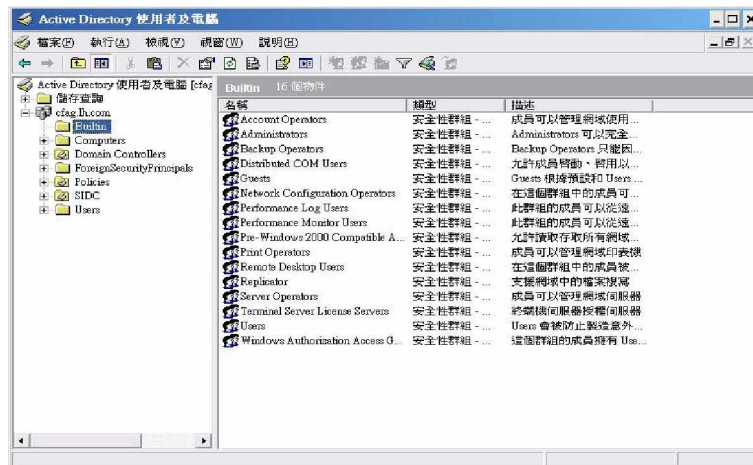
4. 此時可以進行群組間加入權限

二、OU 容器

默認容器，AD 建立完成后，打開 AD 管理界面可以看到默認容器

2.1 Builtin 容器

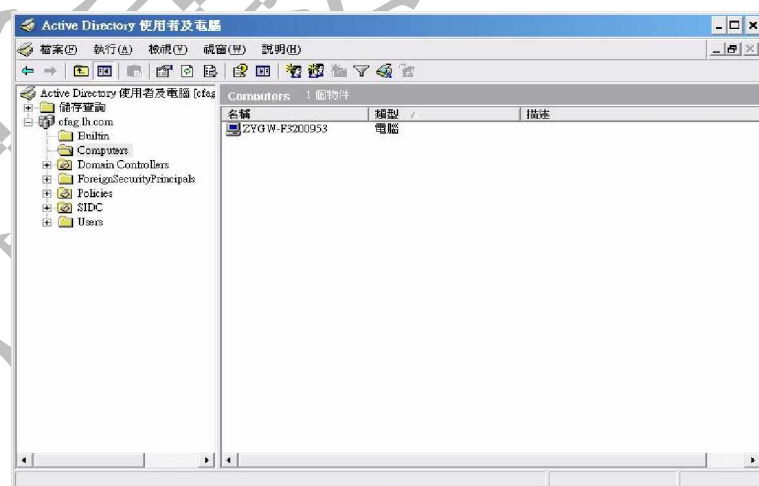
Builtin Active Directory



【Builtin 容器】

2.2 Computers 容器

Computers Active Directory
Windows Server 2003

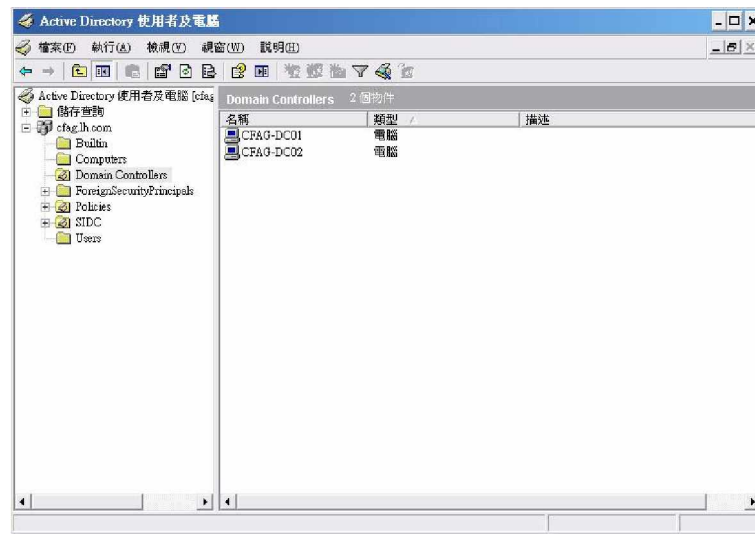


【Computers 容器】

2.3 Domain Controllers 容器

Domain Controllers 容器是一個特殊的容器，確切的說它是一個組織單元 (Organizational Unit, 以下簡稱 OU)。OU 是活動目錄中比較特殊的容器，它除了可以包

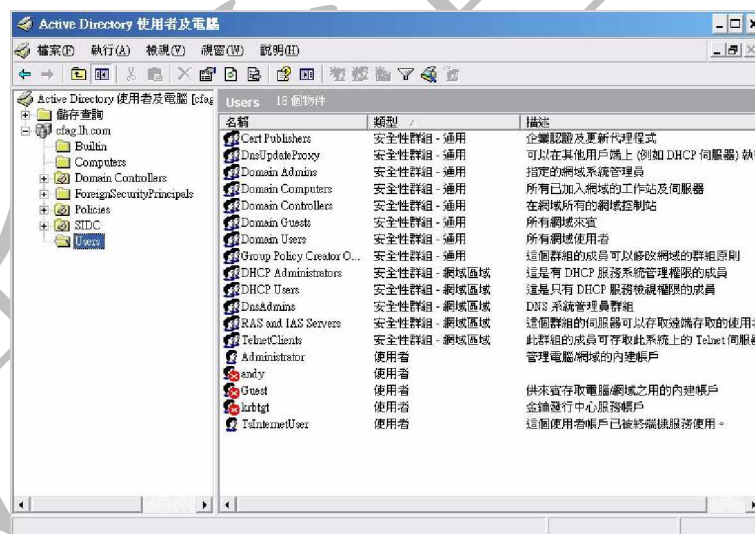
含其他對象和組織單位之外，還具有“組準則”的功能。Domain Controllers 容器也是 AD 默認生成的容器之一，主要用于存放當前域控制器下創建的所有子域和輔助域



【Domain Controllers 容器】

2.4 Users 容器

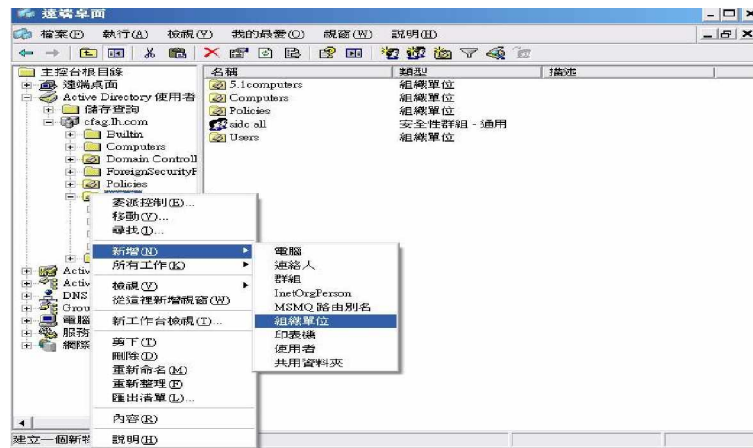
Users 容器主要用于存放安裝 AD 時系統自動創建的用戶組和登錄到當前域控制器的所有用戶帳戶



【Users 容器】

三、創建活動目錄對象

3.1 活動目錄介紹



圖：創建活動目錄對象

活動目錄對象	說明
計算機(Computer)	葉子對象。代表網絡上的計算機資源
聯系人(Contact)	葉子對象。是一個沒有 任何安全權限的賬戶，不能以聯繫人的身份登錄到域，通常用于 E-mail 聯繫
組(Group)	容器對象。可以容納用戶、計算機等對象
組織單元 (Organizational Unit)	容器對象。用來把其他活動目錄容器和葉子對象邏輯的組織在一起，就像是 Windows 資源管理器的文件夾
打印機(Print)	葉子對象。代表網絡中加入活動目錄的共享打印機
用戶(User)	葉子對象。用戶對象是活動目錄中的安全主體，所以客戶端都必須憑據有效的用戶名和密碼登錄到域控制器中，並且可以為不同的用戶分配不同的訪問權限
共享文件夾(Shared Folder)	葉子對象。代表網絡中的共享文件夾

3.2 新建組織單元(OU)

建立一個新的 OU，右鍵點擊網域名稱【新增】--【組織單位】如下圖：

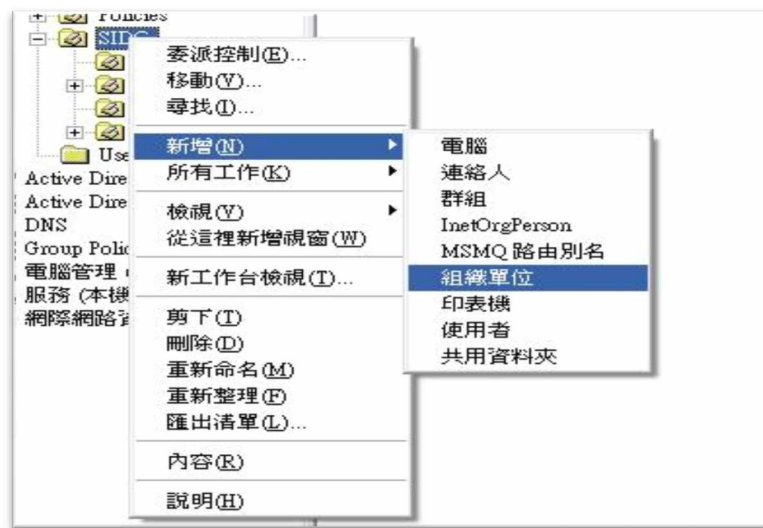


圖 3.1 【新增 OU】



圖 3.2 【OU 名稱】

點擊【確定】后，即建立一個新的 OU，在 OU 下面可以繼續建立新的 OU，可以對 OU 進行套用策略(后面會講到此節)，以方便管理。

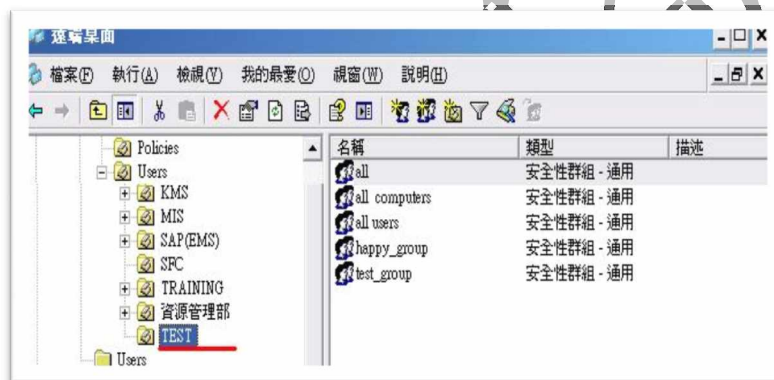
3.3 新建群組(Group)

建立一個新的 Group，右鍵點擊 OU 名稱【新增】--【群組】如上圖 3.1



圖 3.3 【新增群組】

此處輸入群組名稱，【確定】后即建立一個新的群組



可以建立多個 GROUP，群組之間可以互相隸屬。

3.4 新建電腦

新增一臺電腦，右鍵點擊 OU 名稱【新增】--【電腦】如上圖 3.1





3.5 新建使用者

新增一個使用者，右鍵點擊 OU 名稱【新增】--【使用者】如上圖 3.1



圖 3.4 【用戶名及登入名】



圖 3.5 【AD 登入密碼】



圖 3.6 【建立完成】

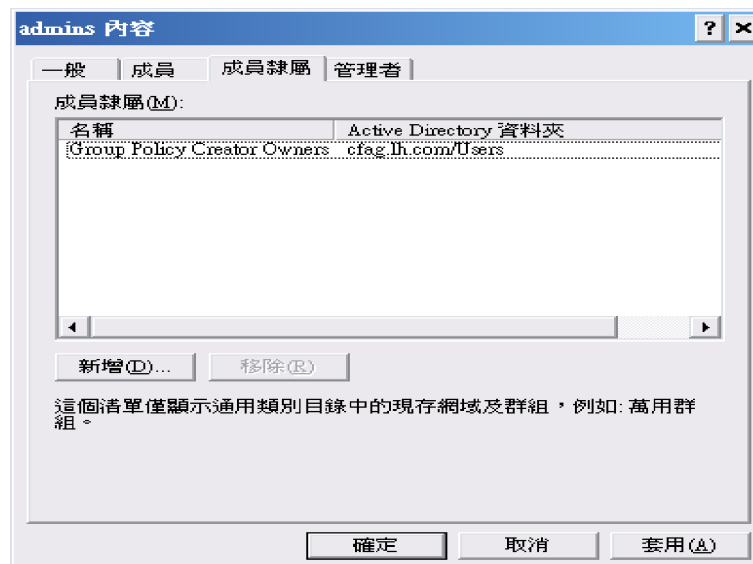
3.6

四、權限設定

4.1 Admins 群組權限設定(OU 管理權限)

在 AD 中如果有多個管理員，可以建立一個 Admins 群組，將 AD 管理員加入此群組，並給 Admins 群組賦予相應的權限即可。

Admins 權限：此群組需要有【Group Policy Creator Owners】權限



【Group Policy Creator Owners】群組的成員可以修改網域的群組原則，為客戶端加域。

管理員加入 Admins 群組：

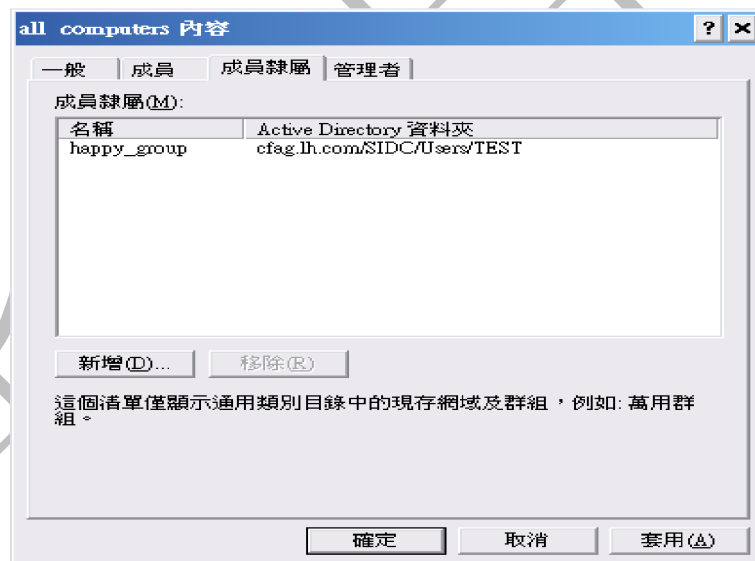
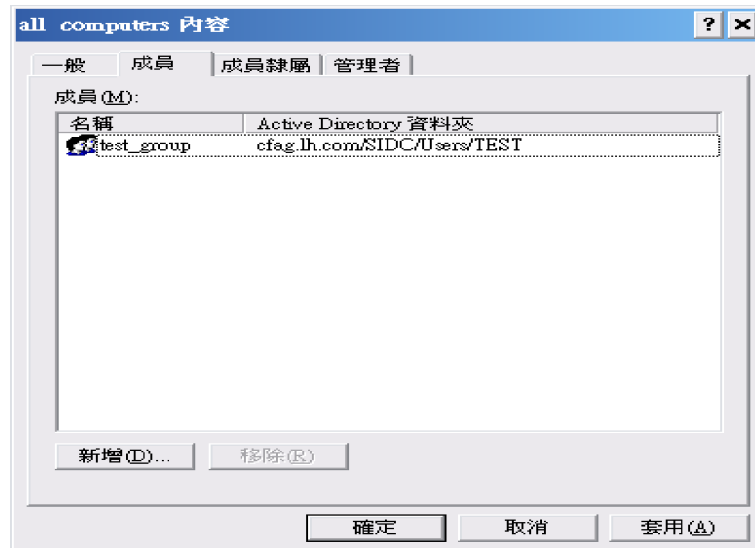
如下圖，點擊新增【張三】與【admin_group】，此時【張三】與【admin_group】群組人員就有了管理此 OU 的權限。如果此人員不在需要 OU 管理權限，從此處刪除即可。

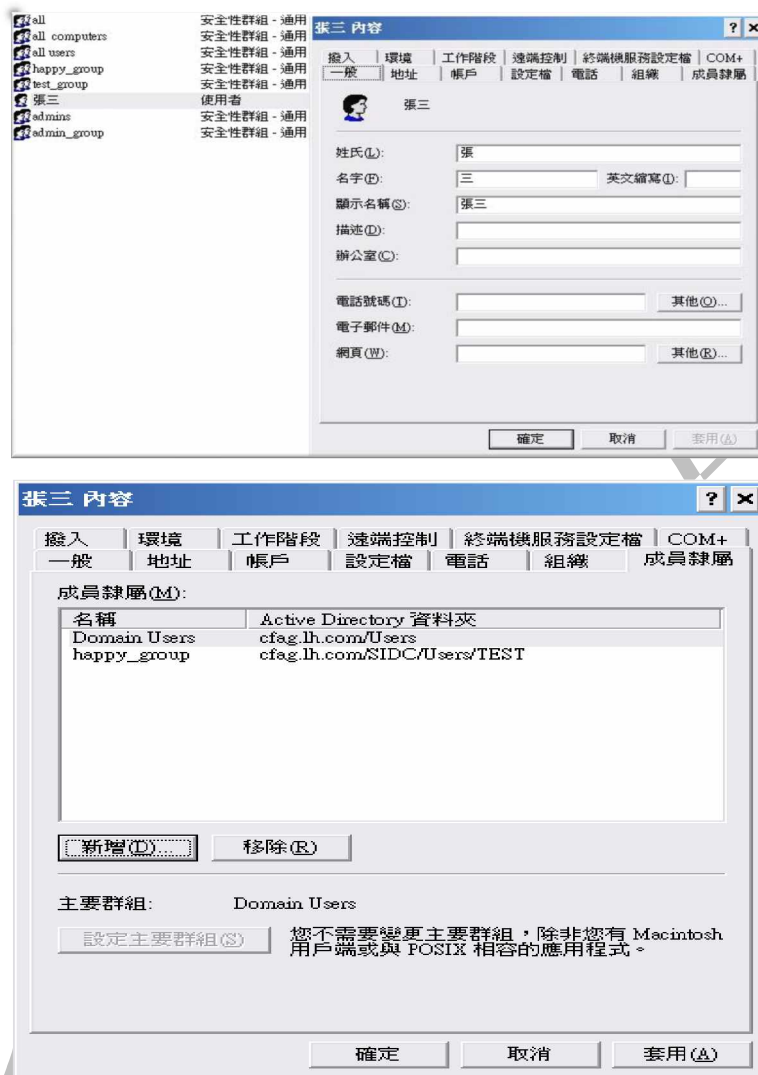


4.2 群組之間權限隸屬

當給多人權限時，可以利用群組賦予權限。

首先建立一個群組，將所有屬於此群組的群組加入此群組的【成員】，





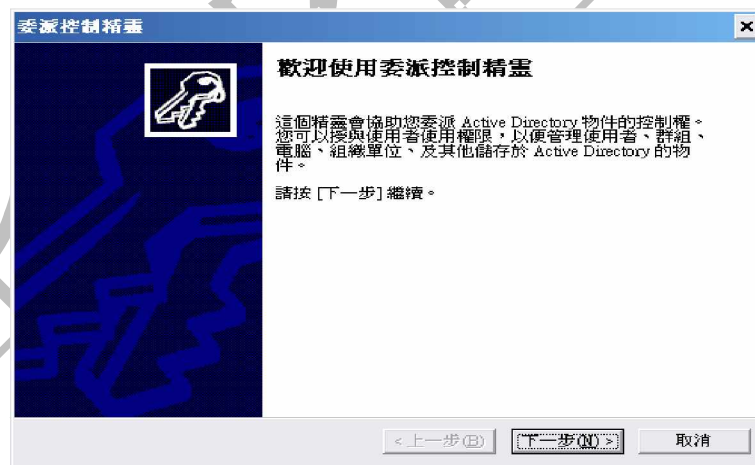
五、委派控制

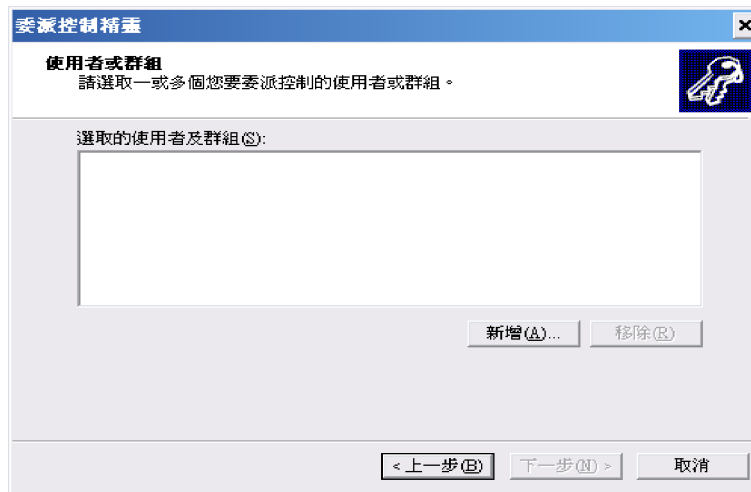
5.1 委派 OU 權限

如果一個 AD 有多個 OU，每個 OU 需要分開管理，這時就要用到委派權限。

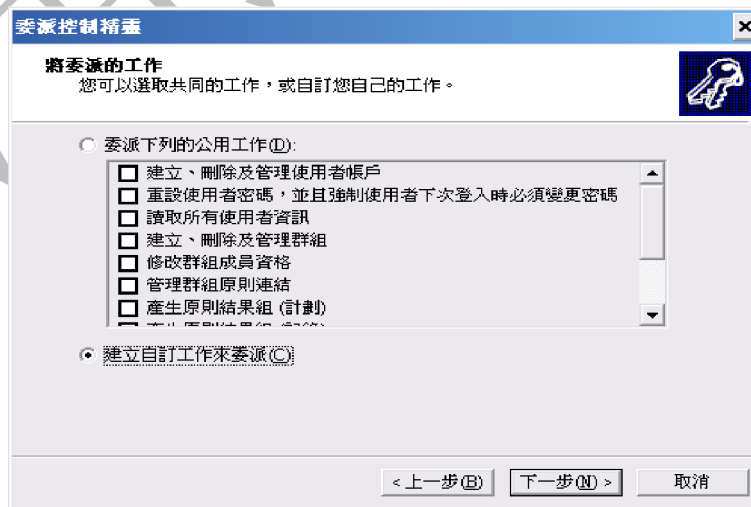
委派權限可以根據管理人員所需要的權限進行自定義設定

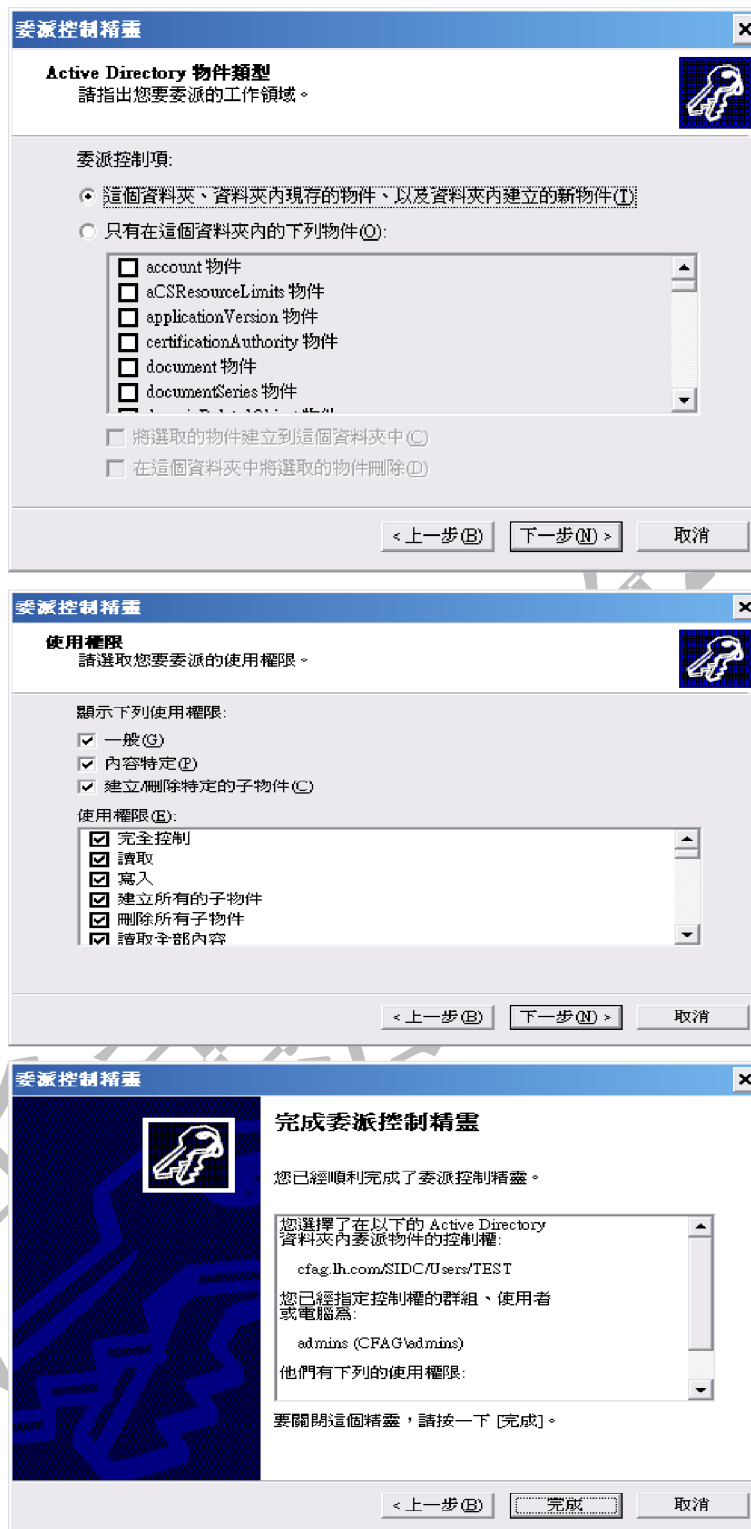
OU---





這裡可以直接委派，也可以【建立自訂工作來委派】





此時 Admins 群組就有【TEST】OU 的管理權限

5.2 其它事項

委派時可以給管理員不同權限，可以權限實際需要進行設定。

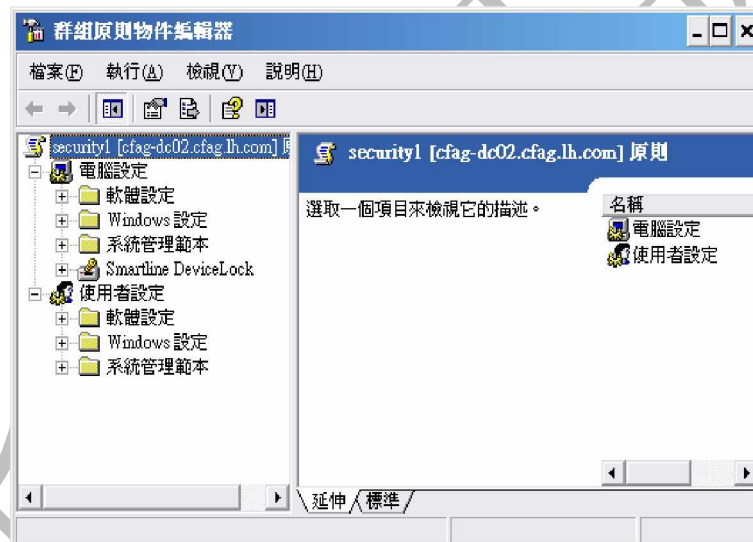
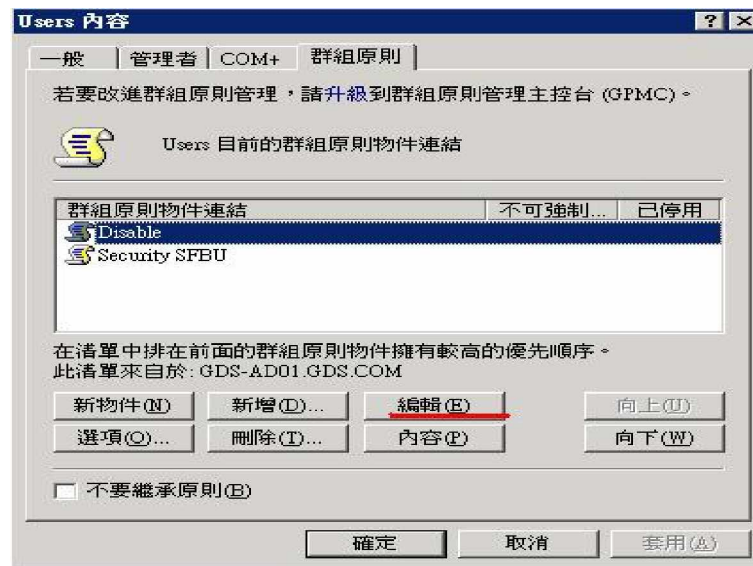
六、策略套用

6.1 常用策略套用

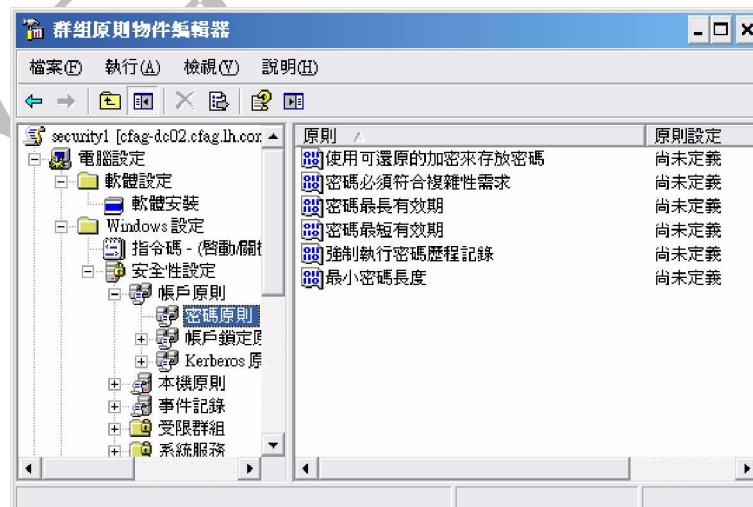
1. 新建策略

在需要套用策略的 OU，點擊右鍵【內容】---【新物件】---【編輯】





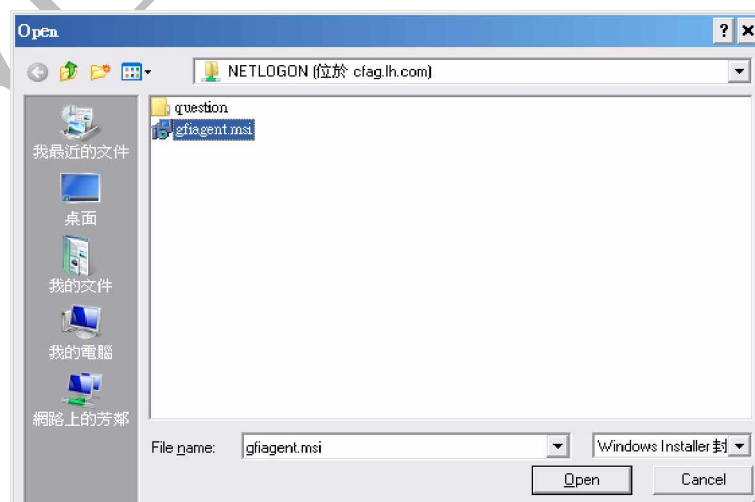
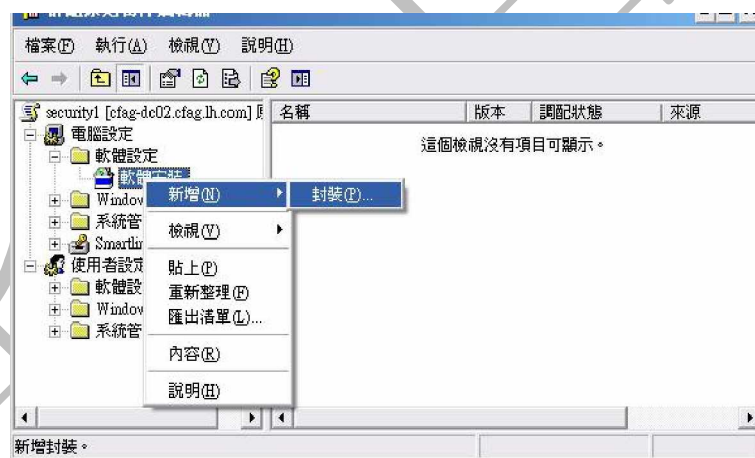
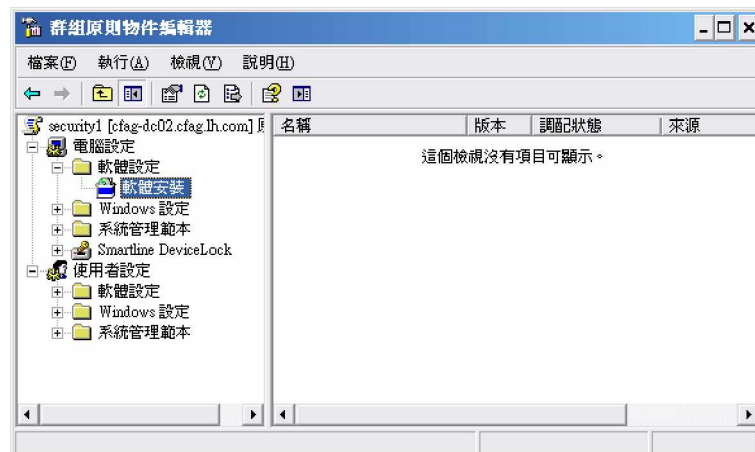
，雙擊后可以依據需要進行設定



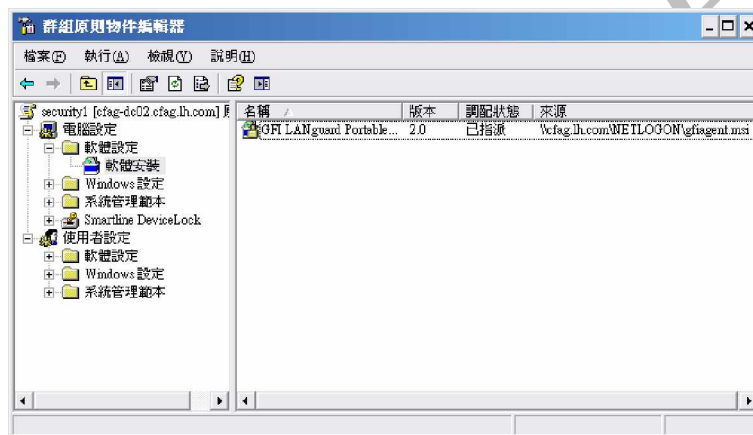
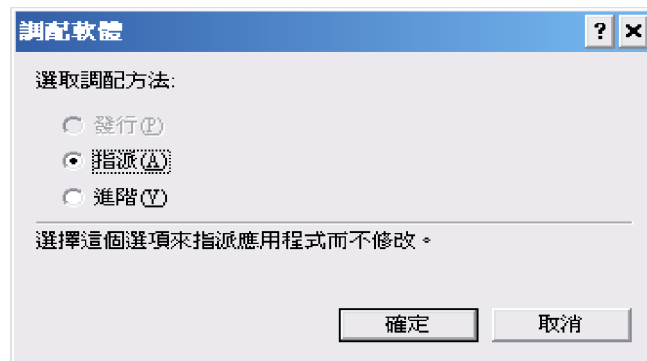
6.2 軟體套用

在【軟體安裝】-----右鍵【新增】---【封裝】，選擇對應的需要安裝的軟體。

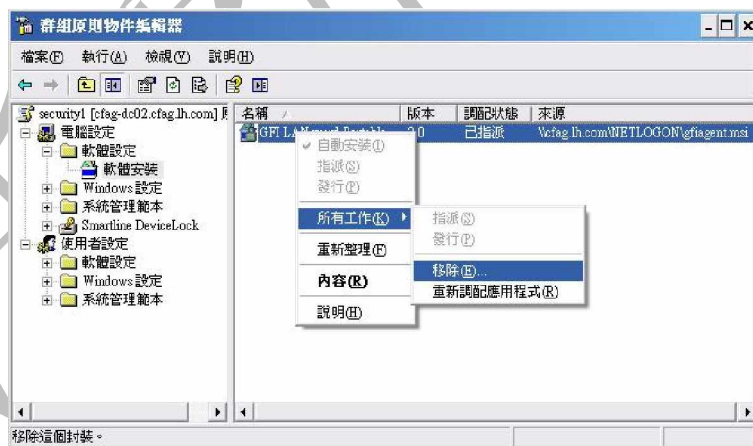
注：此軟體需要為【*.msi】文件，此文件需要上傳到 AD Server 的公用目錄 例如： \\cfag.lh.com\netlogon\gfiagent.msi



選擇對應的軟體，此軟體在 AD Server 的公用目錄中。



此時套用后，客戶端加入網域就可以套用到此軟體。



也可以將此安裝的軟件刪除

6.3 批處理文件套用

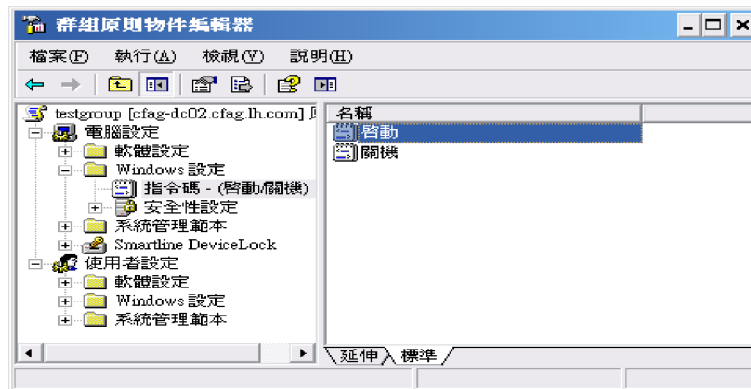
有時為了方便管理，我們會將一些文件寫成批處理的形式，在客戶端開機時進行套用，這樣更方便 AD 管理員的管理。

1. 客戶端加入 Admins,方便管理

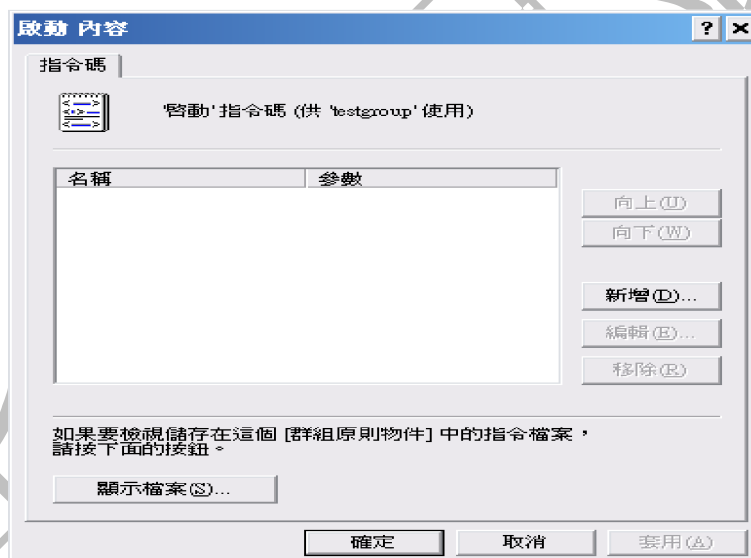
例如：開機時需要 OU 下所有客戶端電腦加入 admins 群組
 Net localgroup administrators cfag\admins /add 保存為

admins.bat，此文件套用到 OU 中，在開機時所有此 OU 的客戶端的 administrators 群組將新增 CFAG\admins 群組，這時在 admins 群組的域管理員就有了管理客戶端電腦的權限。

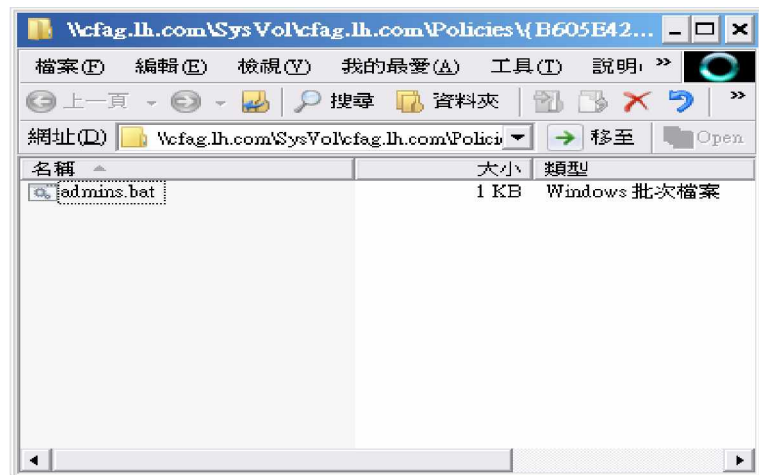
準備好 admins.bat 文件后，就可以在組策略中進行套用：



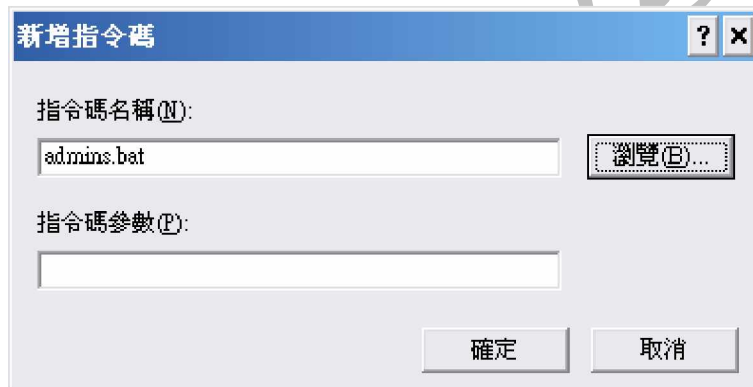
點擊啟動—彈出【啟動】窗口



點擊上圖中的【顯示檔案】，將 admins.bat 拷貝到此處(在 AD Server 中的共享文件夾)



點擊【啟動】----【新增】---彈出【新增指令碼】----【瀏覽】



選中剛剛拷貝的文件--【確定】---【啟動】對話框【套用】--【確定】
此時此 OU 下的客戶端重啟后，將會套用到此策略

2. 客戶端 Administrator 全部密碼更改，OU 下

例如：開機時需要 OU 下所有客戶端電腦更改本機管理員密碼

Net user administrator password 保存為 admin.bat，此文件套用到 OU 中，在開機時所有此 OU 的客戶端 administrator 的密碼將被改為 password

套用方法與上同

3. 客戶端遊戲刪除

將下面的文件保存為 delgame.bat

```
@echo off
```

```
@echo 刪除游戲目錄
```

```
rmdir /s/q "C:\Documents and Settings\All Users\「開始」功能表\程式集\遊樂場"
```

@以上只刪除目錄，在開始程序中找不到遊戲，但在系統目錄下還是能找到遊戲

@如果需要徹底刪除遊戲需要將下面也加入批處理中


```
@rem 接龍
del /q/s %SystemRoot%\system32\sol.exe
@rem 連環新接龍
del /q/s %SystemRoot%\system32\spider.exe
@rem 傷心小棧
del /q/s %SystemRoot%\system32\mshearts.exe
@rem 彈珠台
del /q/s "C:\Program Files\Windows NT\Pinball\PINBALL.EXE"
@rem 新接龍
del /q/s %SystemRoot%\system32\freecell.exe
@rem 踩地雷
del /q/s %SystemRoot%\system32\winmine.exe
@rem 網際網路西式拱豬
del /q/s "C:\Program Files\MSN Gaming Zone\Windows\shvlzm.exe"
@rem 網際網路西洋棋
del /q/s "C:\Program Files\MSN Gaming Zone\Windows\chkrzm.exe"
@rem 網際網路西洋骰子棋
del /q/s "C:\Program Files\MSN Gaming Zone\Windows\bckgzm.exe"
網際網路黑白棋
@del /q/s "C:\Program Files\MSN Gaming Zone\Windows\Rvsezm.exe"
@rem 網際網路傷心小棧
del /q/s "C:\Program Files\MSN Gaming Zone\Windows\hrtzzm.exe"
@end-----
```

將以上文件保存為 delgame.bat，與 7.1(1)一樣套用即可。

6.4 腳本編寫

本人現還未學會此功能，以后在做詳述。

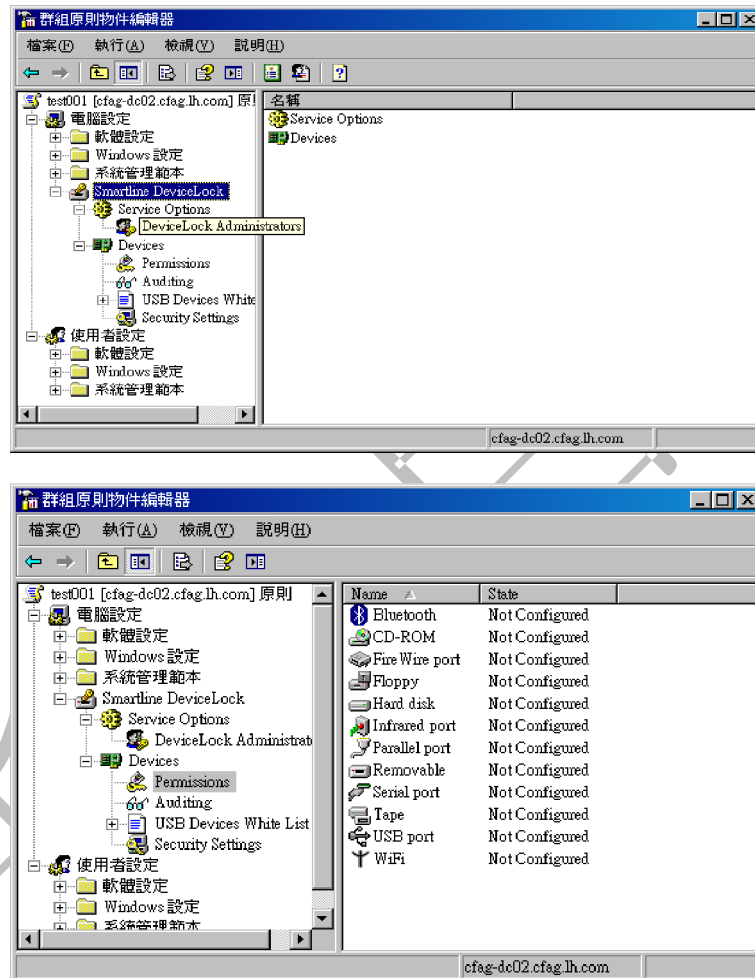
七、外設限定

7.1 外設管制軟件

外設管制軟體有 GFI, DeciceLock 等，下面主要講 DeviceLock

【Server 端】

管理軟件 DeviceLock, 服務器端安裝此軟件后，在 AD 【組策略】中會有此軟件如下圖：



安裝此軟件后，需要進行設定，在 6.2 節中將會講到

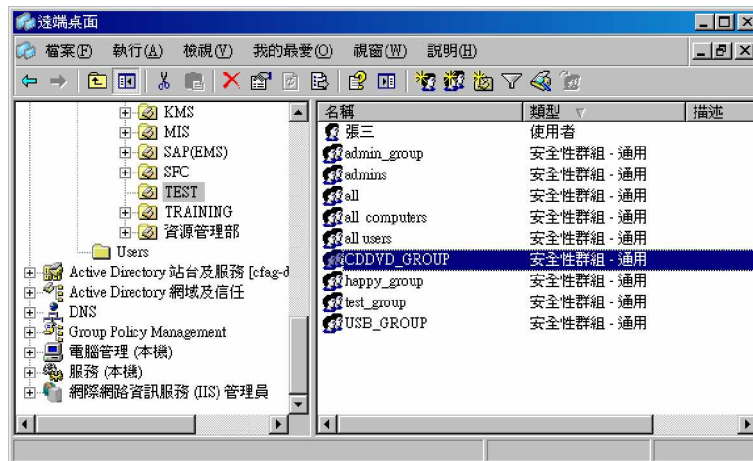
【客戶端】

客戶端軟件【DeviceLock Service.msi】通過 AD 策略套用到所有客戶端，套用部分請參考【第六章】的【7.2 節】，此軟件客戶端安裝后才能對外設進行管控

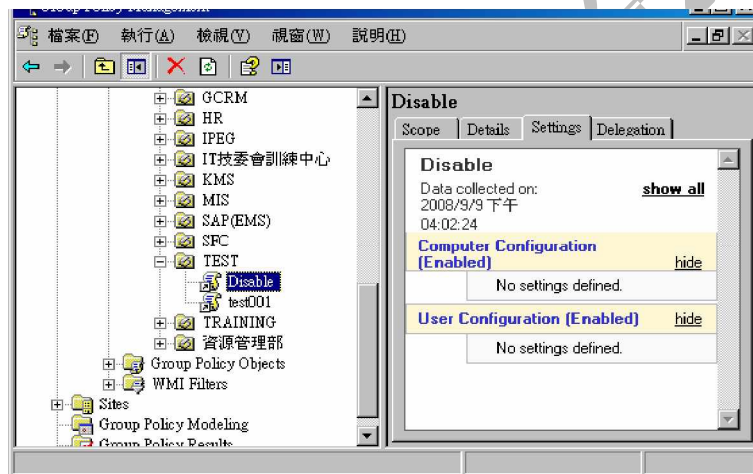
7.2 光驅、USB、DVD 限定

安裝完成管制軟件后，需要在伺服器端進行設定，下面以光驅為例：

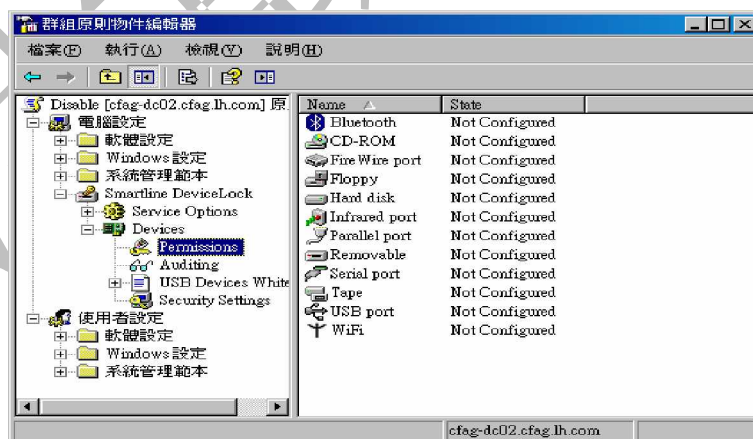
1. 我們先建一個【CDDVD_GROUP】群組



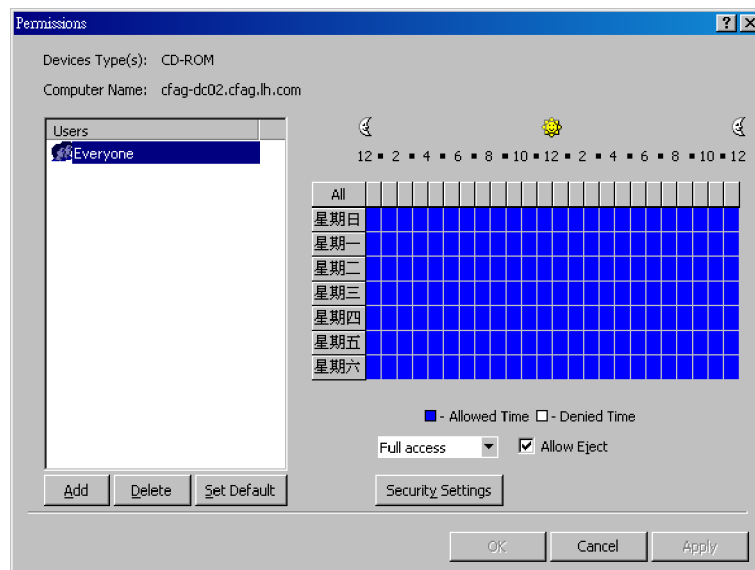
2. 創建一個新的策略命名為 Disable，此 Disable 應建在需要管控的 OU 上以確定可以套用到用戶端



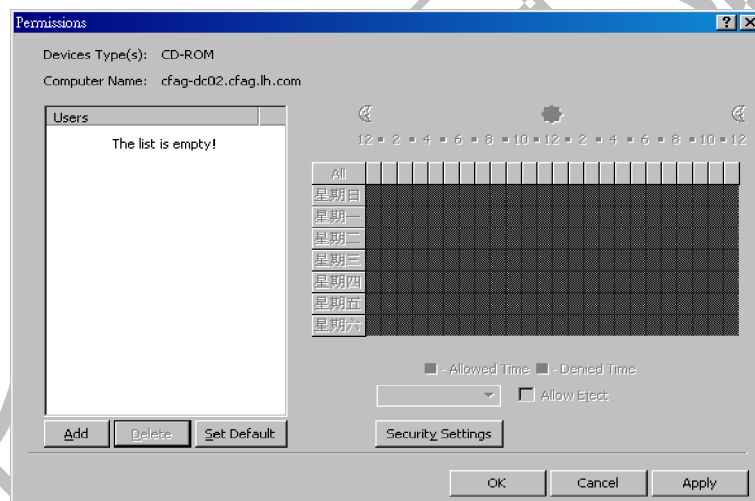
【Disable】---右鍵【Edit】



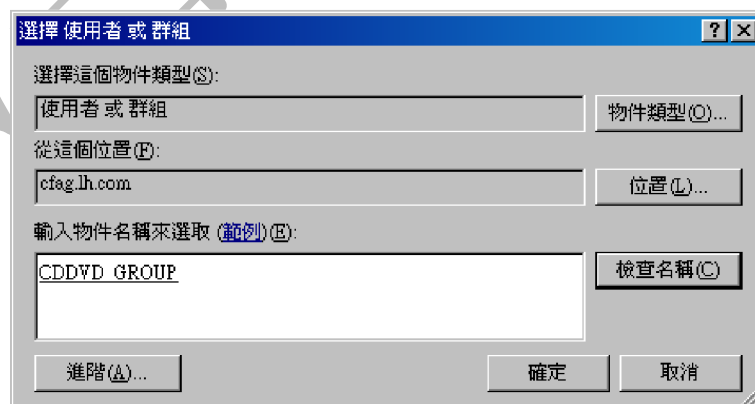
【Smartline DeviceLock】---【Devices】---【Permissions】--【CD-ROM】
---右鍵【Set Permissions】

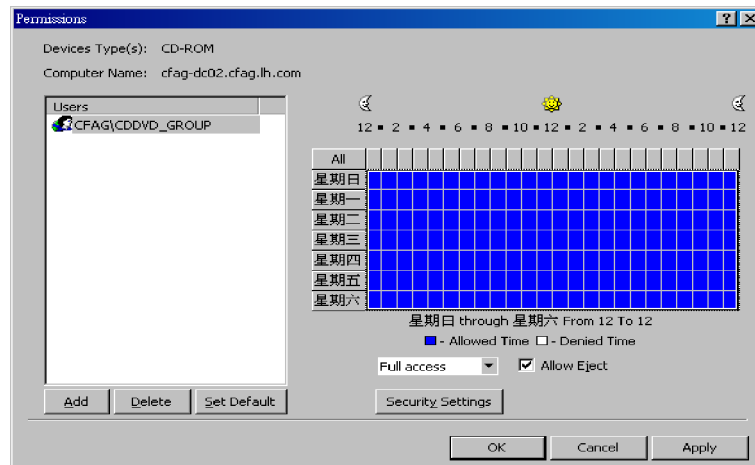


此時域中所有人都有光驅權限【Everyone】--【Full access】
刪除【Everyone】



點擊【add】--【確定】



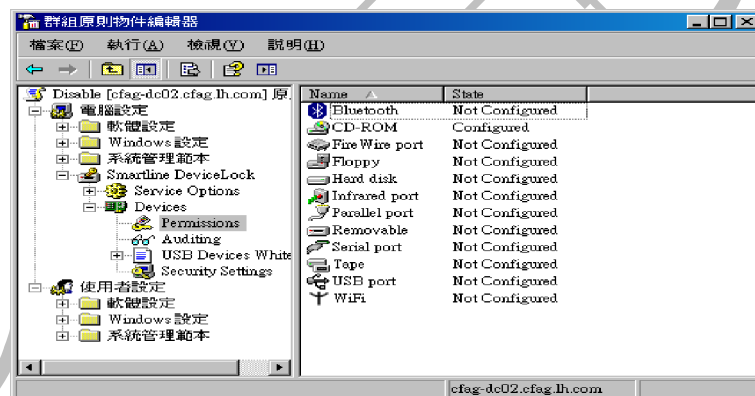


【Full access】勾選【Allow Eject】

點擊【Apply】---【OK】，此時 CDDVD_GROUP 群組成員就有了光驅使用權限

3. USB 及 Floppy 與上述一樣進行一一設定

7.3 其它外設限定

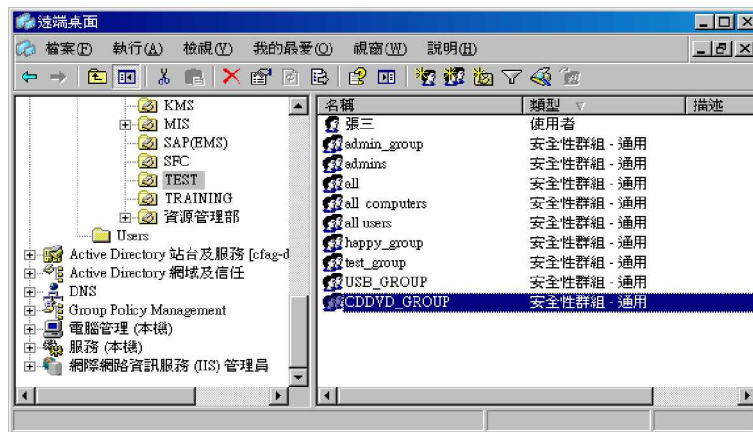


對 Bluetooth,無線等的限定，依光驅設定即可。

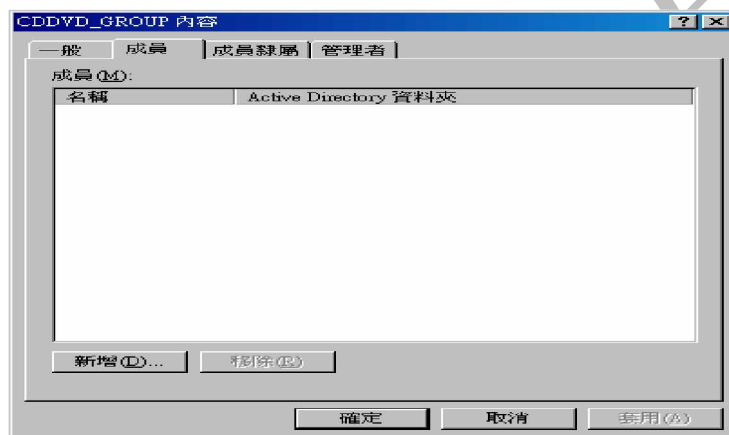
7.4 用戶外設使用權限

用戶端此時是不能使用 USB/DVD/Floppy 及限定的設備，如果需要使用，需要將用戶加入相應權限群組。

例如加入 DVD 權限：



【CDDVD_GROUP】右鍵【內容】-----【CDDVD_GROUP 內容】界面



點擊【新增】，可以需要使用光驅的使用者或電腦加入此群組，【確定】的，客戶端重啟即開通權限

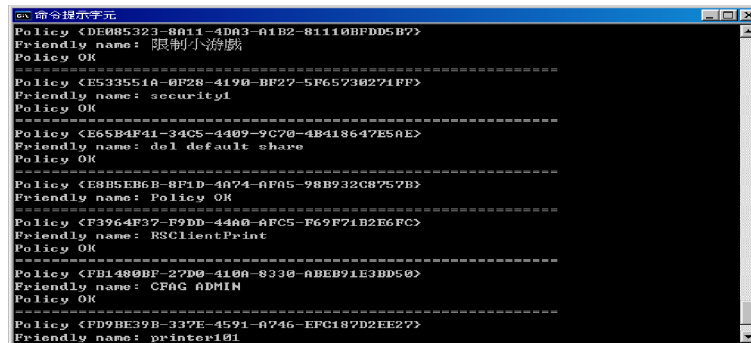
八、組策略工具

8.1 檢查域控制器上組策略對象--Gpoutil

Gpoutil 號稱組策略的“醫生”，此命令行工具用于檢查域控制器上組策略對象的健康狀況

1. 檢查當前域上所有組策略的正常配置

打開命令提示符：輸入 Gpoutil



```

C:\>命令提示字元
Policy {DE085323-8A11-4DA3-A1B2-81110BFD5B7}
Friendly name: 限制小遊戲
Policy OK
=====
Policy {E533551A-0F28-4190-BF27-5F65730271FF}
Friendly name: security1
Policy OK
=====
Policy {E65B4F41-34C5-4409-9C70-4B418647E5A0}
Friendly name: del default share
Policy OK
=====
Policy {E8B5EB6B-8F1D-4A74-AFA5-98B932C8757B}
Friendly name: Policy OK
=====
Policy {F3964F37-F9DD-44A0-AFC5-F69F71B2E6FC}
Friendly name: RSClientPrint
Policy OK
=====
Policy {FB1480BF-27D0-410A-8330-ABEB91E3BD50}
Friendly name: CFAG ADMIN
Policy OK
=====
Policy {FD9BE39B-337E-4591-A746-EFC187D2EE27}
Friendly name: printer101
  
```

2. 檢測路跟域上所有組策略的正常配置

Gpoutil /domain:cfag.lh.com

8.2 組策略結果檢查測工具-- Gpresult

組策略結果命令行工具個可用于面特定用戶或計算機驗證各種策略設置的有效性

1. 檢測當前域上所有組策略的正常配置

C:\>Gpresult



```

C:\>gpresult
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

建立於 2008/9/9 下午 04:51:23

CFAG\F3213427 的 RSOP 資料在 SLDC-MIS-F13427: 記錄模式

OS 類型: Microsoft (R) Windows (R) Server 2003, Standard Editi
on
OS 設定: 成員伺服器
OS 版本: 5.2.3790
終端機伺服器模式: 遠端系統管理
站台名稱: FOXCONN-LH
漫遊設定檔:
本地設定檔: C:\Documents and Settings\F3213427
用低連連結來連線?: 否

電腦設定
  
```

2. 顯示 book 域下的 Administrator 賬戶的計算機配置策略

Gpresult /s book.com /u administrator /scope computer

8.3 組策略刷新工具--Gpupdate

刷新本地組策略設置和存儲在 Active Directory 中的組策略設置

1. 組策略刷新完成后，重新啟動計算機

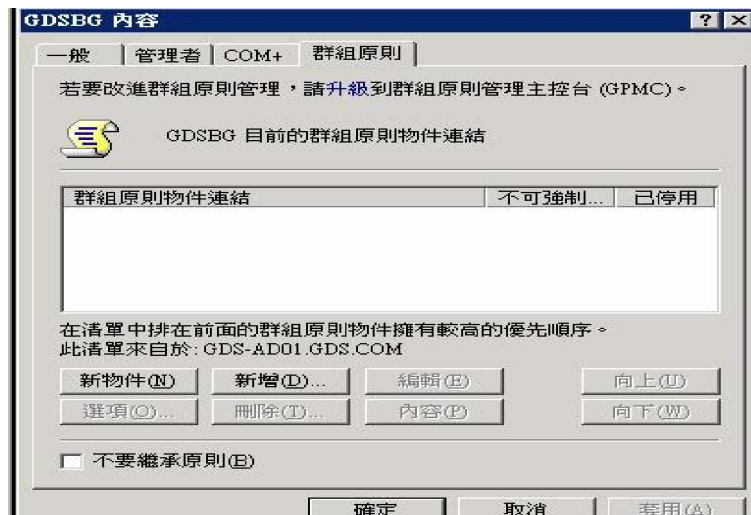
Gpupdate /boot

2. 強制立即刷新組策略

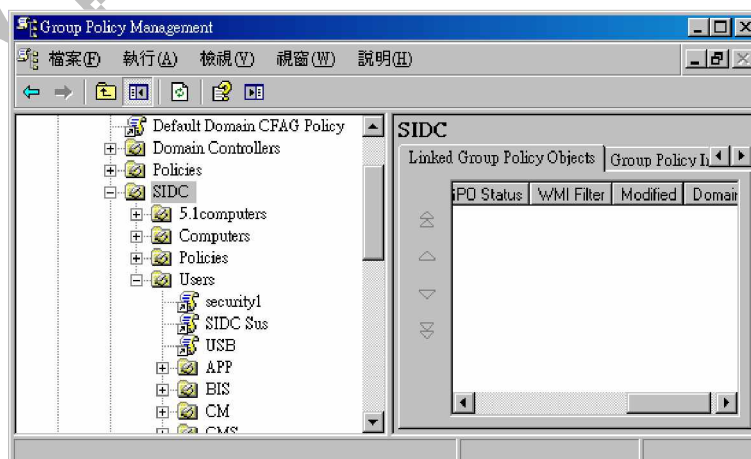
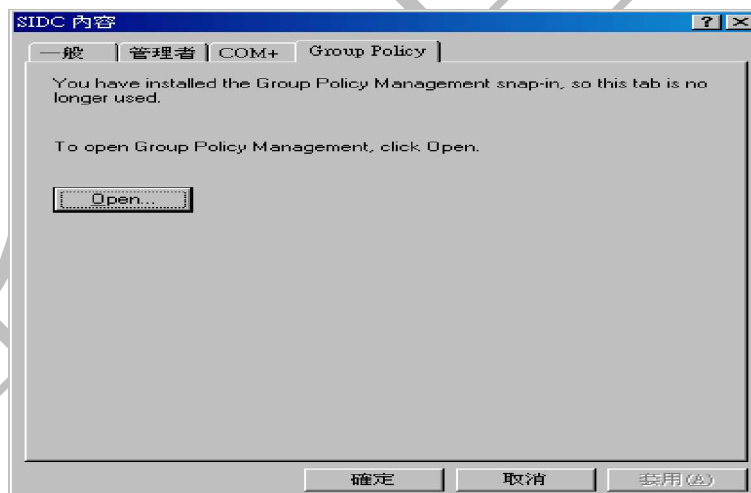
Gpupdate /force

8.4 組策略管理控制臺--GPMC

需要安裝 GPMC 軟件，安裝前如下圖：



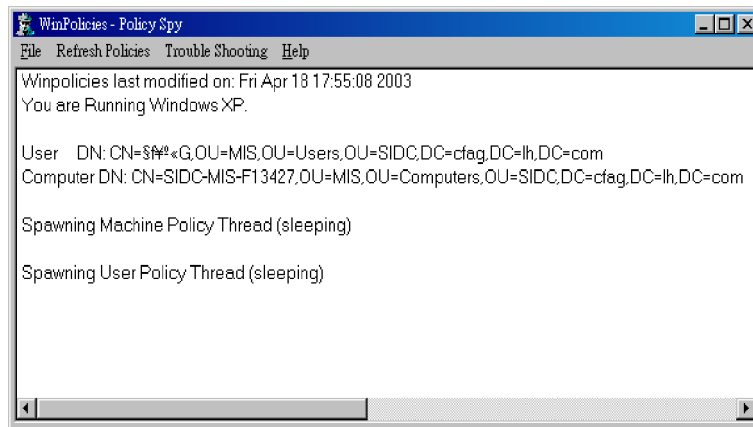
安裝后如下圖



8.5 組策略監視器--Winpolicies

1. 運行策略監視工具

運行 winpolicies



2. 刷新組策略

【Refresh Policies】---【Secedit/Gpupdate】---【User_policy(Enforced)】
(強制用戶策略刷新)--【Machine_Policy(Enforced)】(強制計算機策略刷新)

九、客戶端安裝 AD 管理工具

管理 AD 并不需要進入 AD 伺服器，可以在客戶端安裝 AD 工具進行管理，只要有管理權限人沒登入即可管理 AD Server

1. WindowsXP 系統需安裝【ADMINPAK.MSI】，此文件在 Windows2003 Server 的 I386 文件中
2. Windows 2003 系統，直接進入本機的 Windows/i386 中，找到【ADMINPAK.MSI】安裝即可

十、THE END