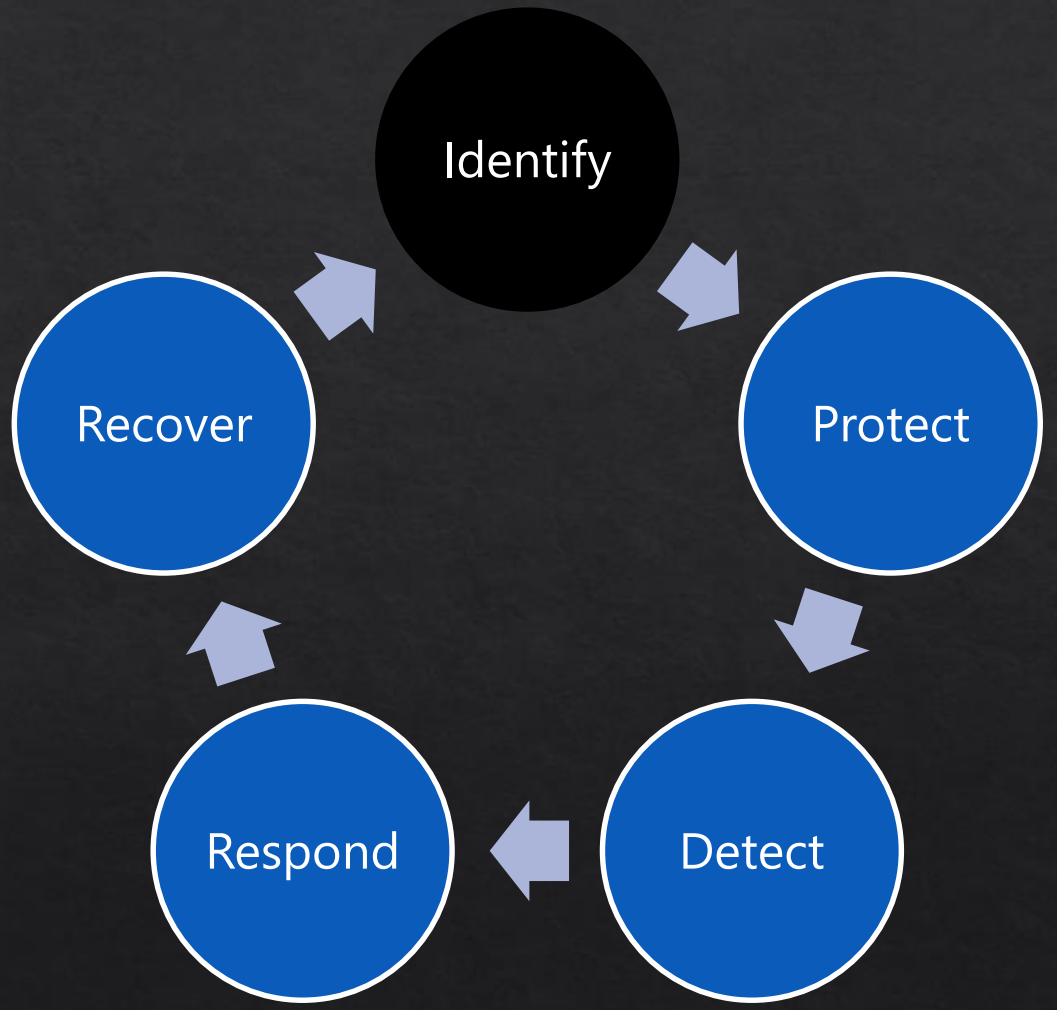
您所不知道的AD特權

台灣微軟 Enterprise Services
Cybersecurity and Secure Infrastructure
技術顧問 Justin Hung (洪健復)

資訊安全 Framework

- 識別出需要保護的資產：
  - National Institute of Standards and Technology (NIST) Framework for improving Critical Infrastructure Cybersecurity
- 優先排序：
  - 依照資產的價值決定施予保護的優先順序
- 我們的目標：**識別出**我們所需要保護的**AD特權**



特權帳號的類型 | 預設管理群組

- 預設管理群組
  - Domain Admins (S-1-5-21-domainSID-512)
  - Enterprise Admins (S-1-5-21-root domainSID-519)
  - Schema Admins (S-1-5-21-root domainSID-518)

- 預設管理帳號
  - Administrator (S-1-5-21-domainSID-500)

- 如何取得Domain SID
  - CMD.exe：dsquery * domainroot -scope base -attr objectSID
  - PowerShell：Get-ADDomain | Select-Object domainSID

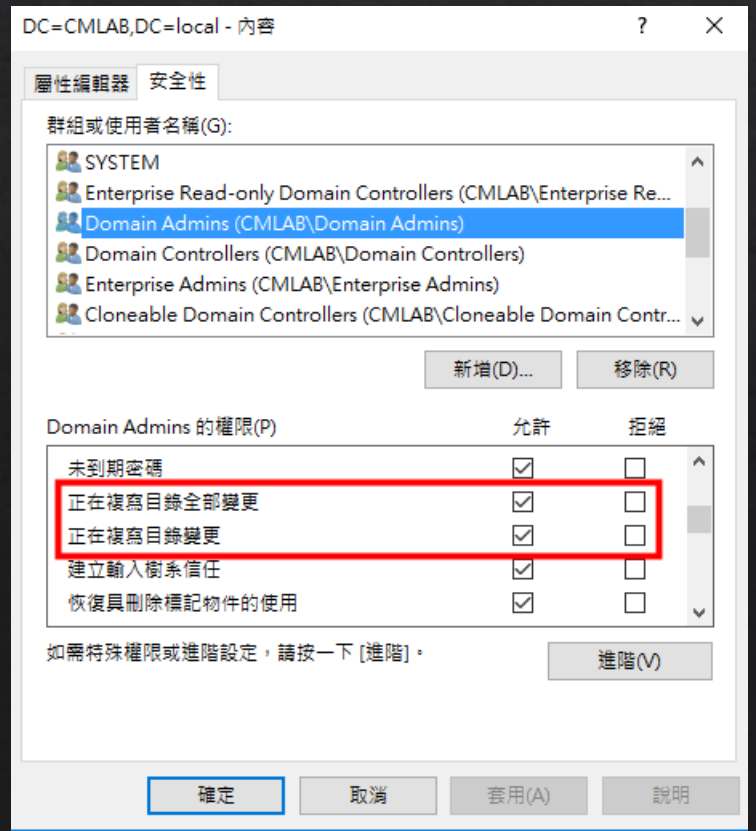
特權帳號的類型 | 預設管理群組

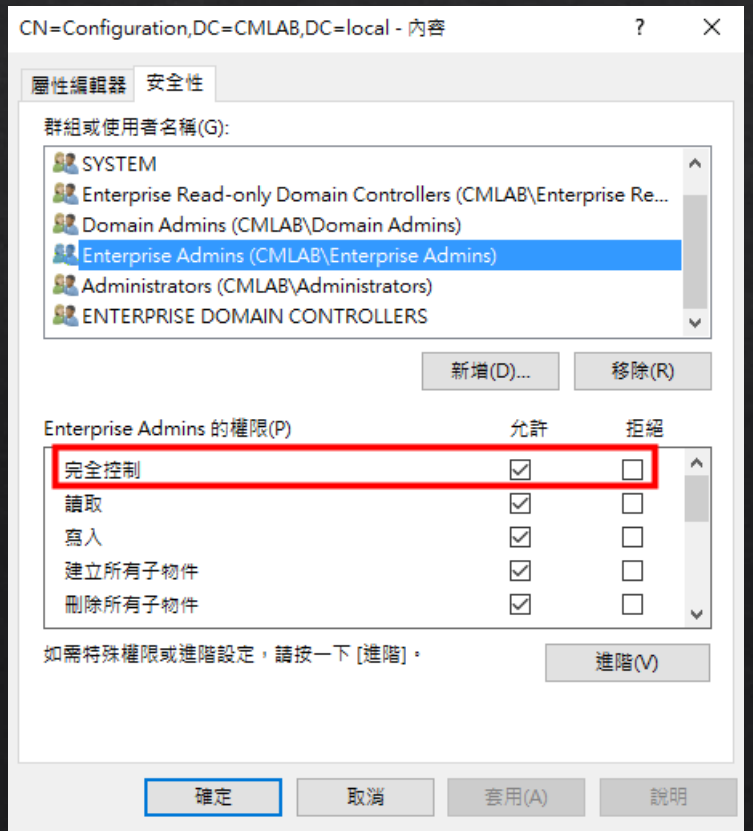
正確觀念：
預設管理權限是無法限制/降低權限的。預設管理權限群組成員永遠可以設定其所欲的權限

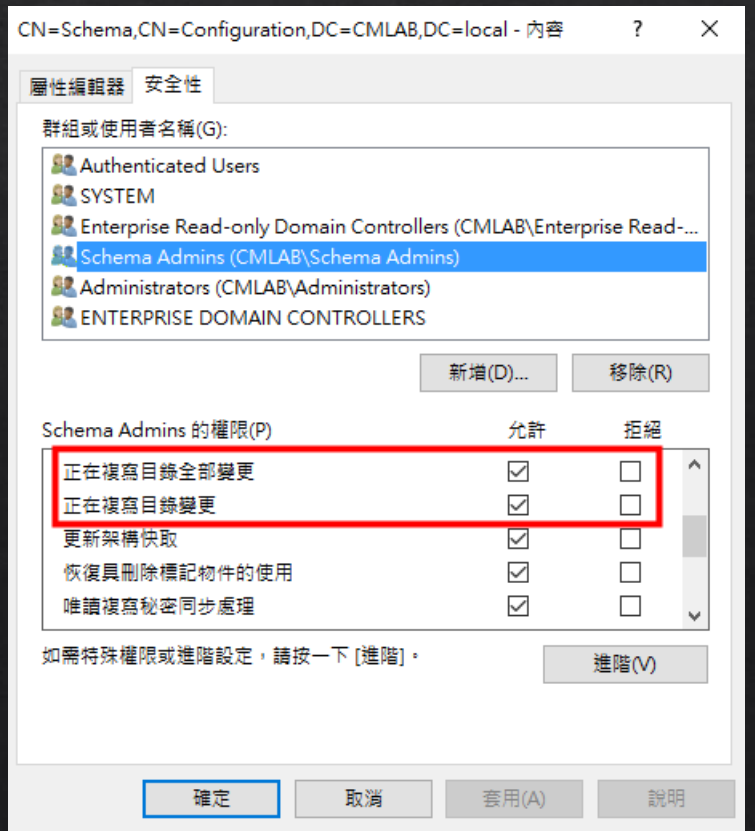
在Active Directory Object上的權限

- Domain Admins：對於Domain NC具有完全控制的權限
- Enterprise Admins：對於Configuration NC具有完全控制的權限
- Schema Admins：對於Schema NC具有完全控制的權限

名稱	類別
預設命名內容 [DC.CMLAB.local]	domainDNS
設定 [DC.CMLAB.local]	configuration
架構 [DC.CMLAB.local]	dMD







特權帳號的類型 | 預設管理群組

在網域控制站(Domain Controller)上的作業系統權限

- Access this computer from the network
- Adjust memory quotas for a process
- Back up files and directories
- Bypass traverse checking
- Change the system time
- Create a page file
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Force a shutdown from a remote system
- Increase scheduling priority
- Load and unload device drivers
- Allow log on locally
- Manage auditing and security log
- Modify firmware environment values
- Profile single process
- Profile system performance
- Remove computer from docking station
- Restore files and directories
- Shut down the system
- Take ownership of files or other objects

可以透過 whoami /PRIV 指令查詢登入帳號所具有的作業系統權限

特權帳號的類型 | 預設管理群組

在網域成員電腦/伺服器上的權限

- Domain Admins預設是所有網域成員電腦/伺服器上的本機管理者 (Local Administrators)，但這不意味著這是必要的配置。強烈建議以其他權限取代Domain Admins在網域成員電腦上的權限。

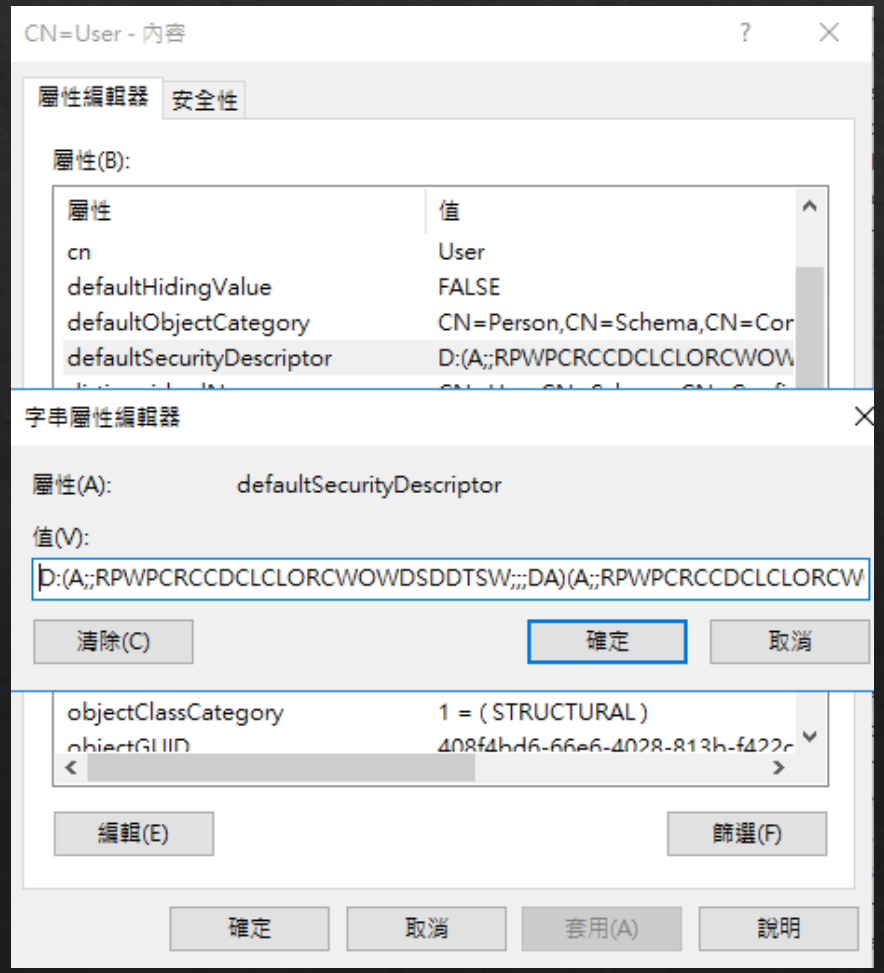
- Enterprise Admins在網域成員電腦/伺服器上並無權限，但Enterprise Admins之成員有權限將己身加入到Domain Admins中

正確觀念：
避免這類特權帳號登入(本機、遠端桌面、服務及排程工作登入)到成員電腦或伺服器，降低特權帳號遭受Pass-The-Hash或者Pass-The-Ticket類型的攻擊

特權帳號的類型 | 預設管理群組

Schema Admins有權限修改AD Object的defaultSecurityDescriptor

- 一個AD Object (例如使用者帳號、安全性群組) 的預設Security ACL，除了繼承自上層Container / OU的權限以外，主要來自於Object的defaultSecurityDescriptor
- 所有Object的defaultSecurityDescriptor統一設定於AD的Schema NC，Schema Admins具有異動的權限。
- 透過取得Schema Admins之權限來修改defaultSecurityDescriptor，可以達成惡意權限長期潛伏在環境的需求



※權限需以SDDL格式進行設定

特權帳號的類型 | Built-In群組

- 由於網域控制站本身也是Windows作業系統，因此作業系統內建的安全性群組仍是存在的。這些作業系統內建的安全性群組在網域控制站上稱為Built-In群組

- 重要的Built-In群組：
  - **Administrators** (S-1-5-32-544)
  - Backup Operators (S-1-5-32-551)
  - Server Operators (S-1-5-32-549)
  - Print Operators (S-1-5-32-550)
  - Account Operators (S-1-5-32-548)

- 這些群組的成員只在網域控制站上有效

- 基本上所有Built-In群組除非有必要，否則都不建議使用

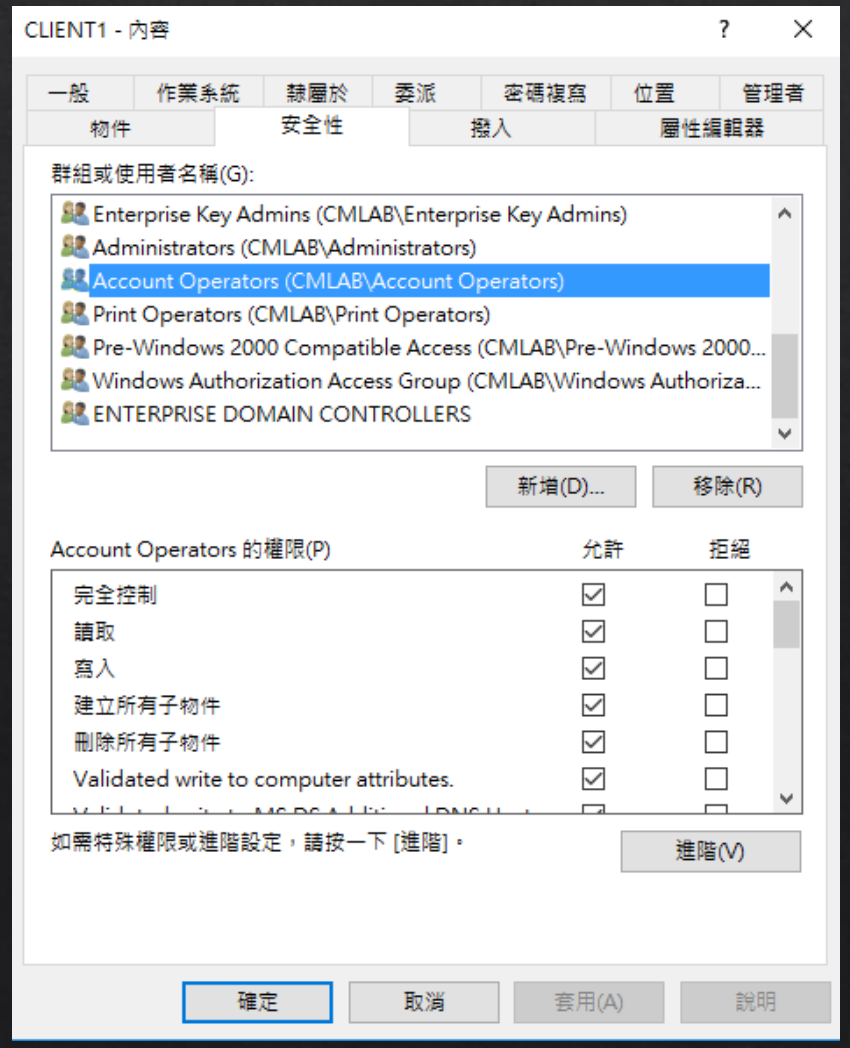
特權帳號的類型 | Built-In群組

Account Operators在AD上的權限

- 在**所有OU和預設Containers**中的使用者/電腦/群組物件上具有建立/刪除/變更密碼的權限

- 除了受到AdminCount=1屬性保護的物件外，Account Operators對於使用者/電腦物件具有完全控制的權限。

正確觀念：
永遠不應該使用此權限，應透過Directory Delegation的機制來賦予有限度(Scope)的權限



特權帳號的類型 | Built-In群組

淺談Azure AD Connector漏洞：CVE-2017-8613

- Azure AD Connector是Microsoft用來同步AD帳號到Azure AD的解決方案。若啟動了Azure AD Password Write-Back的功能時，Azure AD Connector安裝精靈自動建立的Azure AD同步帳號 (帳號名稱為MSOL_xxxxxxxx)並未正確的加上AdminCount=1的值。

- 而此Azure AD同步帳號具有重設所有帳號密碼的權限，甚至包含Domain Admins等.....預設管理權限

- 由於以上帳號缺乏AdminCount屬性的保護，因此Account Operators透過重設Azure AD同步帳號的密碼來取得同步帳號的權限後，可進一步取得Domain Admins等.....高權限的帳號。

特權帳號的類型 | Built-In群組

Server Operators / Print Operators / Backup Operator

- 這些權限在網域控制站都具有下列不等的權限，除非確有必要，且無法使用更小的權限替代，否則不建議使用：
  - Allow log on locally (SO,PO,BO)
  - Back up files and directories (SO,BO)
  - Change the system time (SO)
  - Log on as a batch job (BO)
  - Load and unload device drivers (PO)
  - Force shutdown from a remote system (SO)
  - Shut down the system (SO,PO,BO)
  - Restore files and directories (SO,BO)

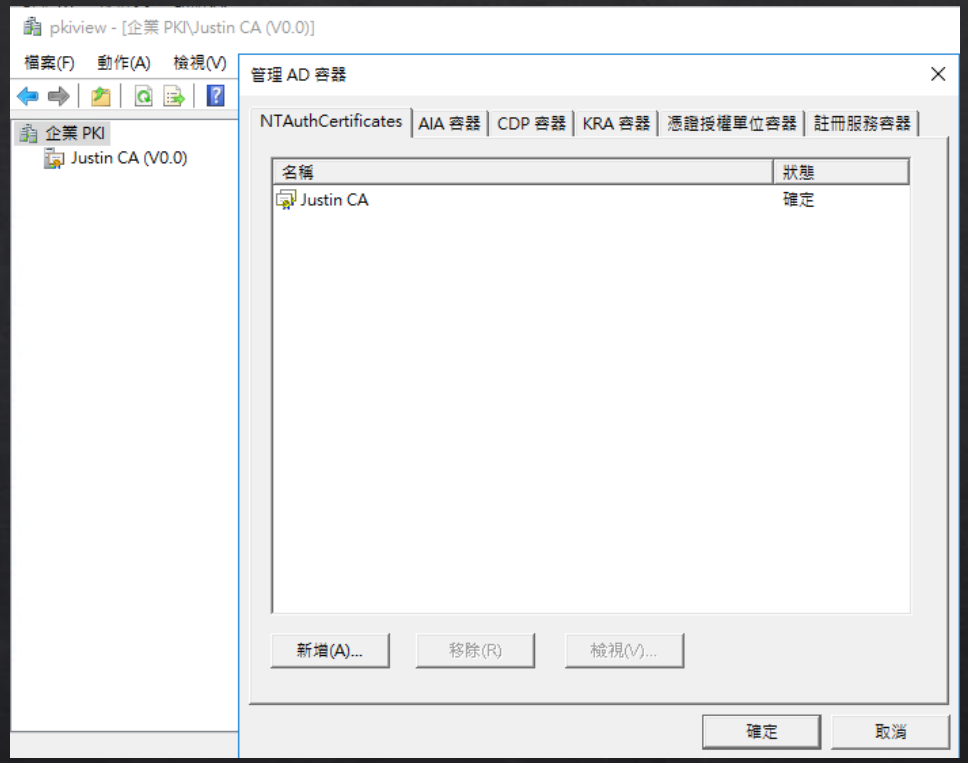
正確觀念：
AD內建權限群組的成員可以透過Technet上的Administrative Groups Collection and Report進行盤查

特權帳號的類型 | Enterprise CA Administrator

- Windows Server中的Active Directory Certificate Services是整合AD的PKI解決方案，其中的Enterprise CA更可以結合AD權限做使用者自助申請憑證/自動化憑證派發，是IT環境中常用的伺服器端服務。

- 而根據預設，所有加入AD的成員電腦及伺服器預設是信任AD憑證服務Enterprise CA的Public Key的。也接受Enterprise CA所簽發的Smart Card登入憑證。

- 若攻擊者取得Enterprise CA的管理權限，可以藉以匯出PKI的伺服器私密金鑰，透過這個私密金鑰攻擊者可以偽冒Enterprise CA進行憑證的簽發，甚至可以簽發代表任何AD帳號的Smart Card登入憑證。



※透過PKIView.msc主控台可以確認AD環境中用戶端所信任的Enterprise CA

正確觀念：
留意Enterprise CA Server的管理權限配置，甚至可搭配HSM來保護CA Private Key

特權帳號的類型 | Directory Delegation

- 在一般管理權限情境下，時常會透過Directory Delegation授權AD Object特定的權限給使用者/服務帳號使用。

- 這些授權(Delegation)需要特別注意以下面相：
  - **Scope**：盡量以OU/Container為單位，避免過大範圍的委派
  - **Object Type**：委派可以以物件類型為標的進行委派，換言之，若受委派之權限只需要管理使用者物件，自然不需要委派電腦物件或群組物件的權限
  - **Permission**：委派應以確實需要的權限為範圍，盡量避免委派Full Control、Replicating Directory Changes All的權限

正確觀念：
Directory Delegation時常為企業盤點特權時遺漏的一塊，建議可以透過ADACL Scanner等....免費工具進行權限盤查

特權帳號的類型 | Directory Delegation

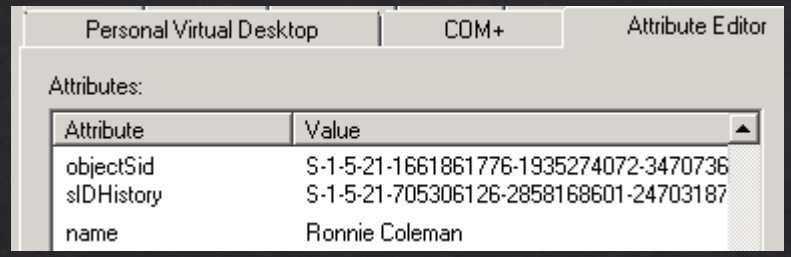
高權限委派的風險：以Replicating Directory Changes All為例

- Replicating Changes All權限具有抄寫AD Object上所有資料的權限，包含了User Object / Computer Object上的Password Hash 。
- 若攻擊者取得具有Replicating Changes All的權限，可以透過常用的惡意程式 (例如Mimikatz的DCSync功能)來獲取帳號的Password Hash。
- 坊間很多整合AD的解決方案，其服務帳號都需要此權限，以Microsoft為例，SharePoint Server的服務帳號就需要此權限(User Profile Sync Account)。結合類似CVE-2019-0604的SharePoint RCE漏洞來進行服務帳號的竊取，可進而達成Compromise AD的目的。

常見的AD管理迷思 | Forest v.s. Domain

淺談SID History Injection類型攻擊

- 常見的AD管理迷思在於，AD管理權限的分界點在於網域，而非樹系。在實務上，跨國公司或者金控公司建立單一樹系，不同子網域交由不同公司或團隊進行管理也非屬少見。



- 事實上，若子網域的AD管理權限遭到Compromise，可以透過子網域網域控制站的Administrators權限進行SID History的注入，換言之，可以將其他子網域或根網域的管理帳號的SID注入到該受駭網域的任一帳號上，而該帳號即可取得其他網域的管理權限。常見的工具有Empire或Mimikatz。

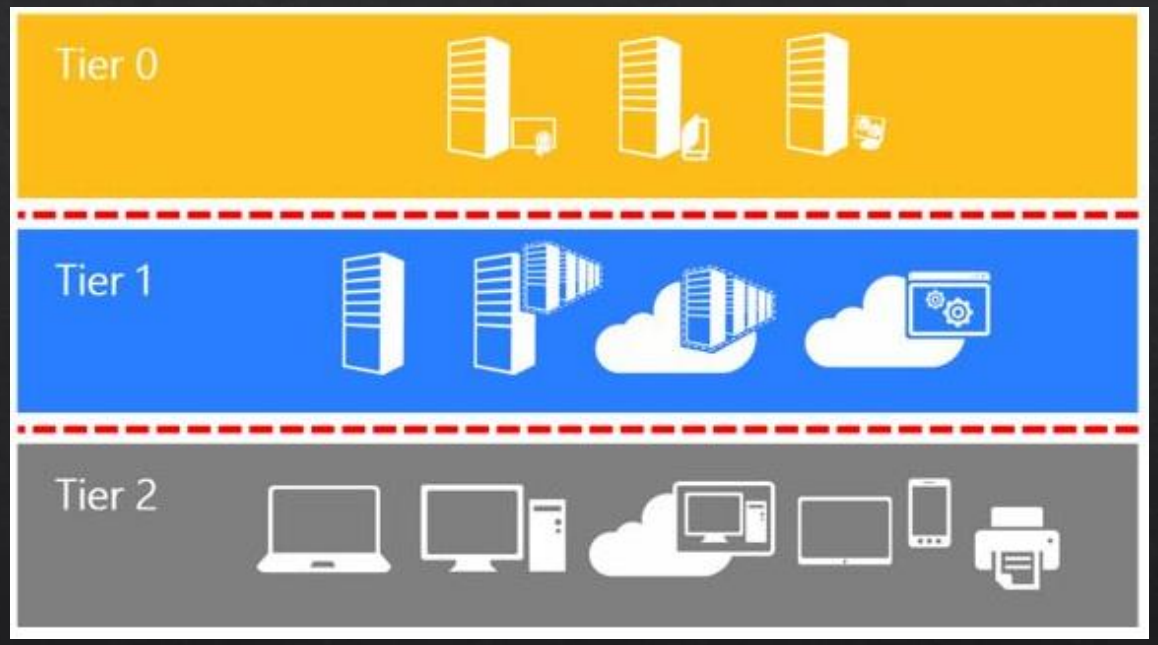
正確觀念：
樹系架構下，應確保所有網域都具有相同的安全水平。而信任的外部樹系/網域則可以透過AD信任的Quarantine及SID Filter機制來阻擋來自信任樹系/網域帳號的SID History

如何正確的保護AD特權

Active Directory Administrative Tier Model

- 由於AD的網域控制站需要使用TCP 135 (WMI)、TCP 445 (SMB)等.....具有遠端執行功能的網路埠，因此透過防火牆或網路設備保護是不現實的。因為任何網域成員電腦都需要可以存取到以上埠號，而任何加入網域的成員電腦都具備發動攻擊的可能性。

- 因此妥善的保護AD特權，才是唯一不敗兵法。Microsoft針對AD特權的管理作為，稱之為Active Directory Administrative Tier Model。

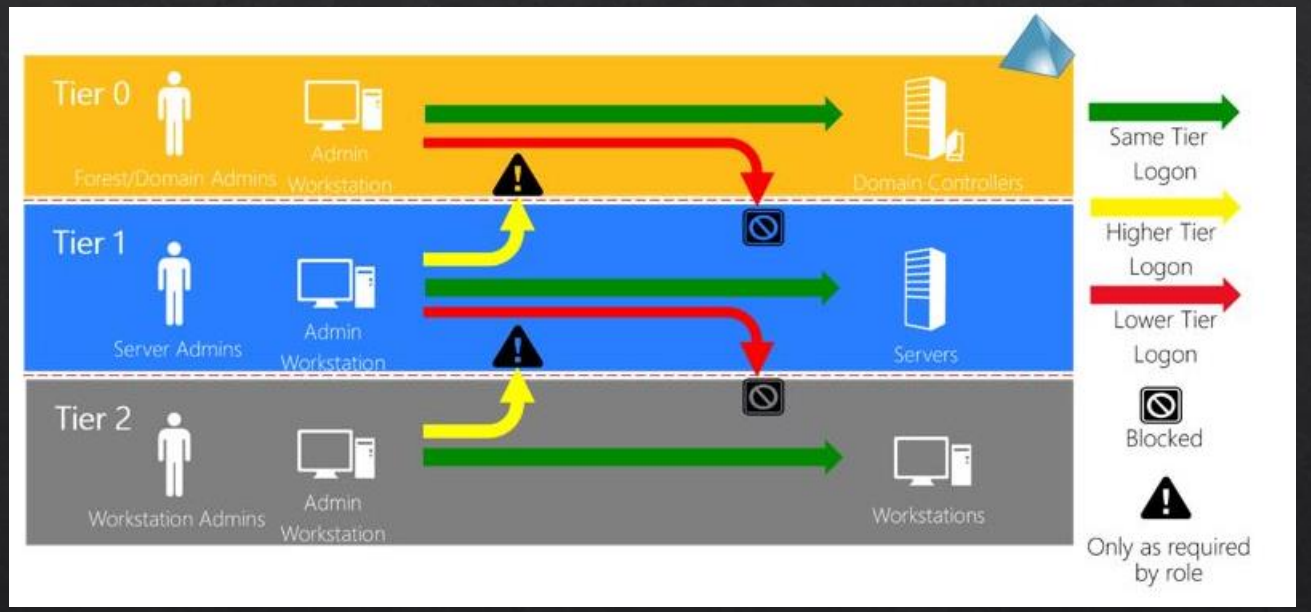


※Tier Model將AD權限與網域成員電腦區分為三個層級，分別為Tier 0、Tier 1、Tier 2

如何正確的保護AD特權

Active Directory Administrative Tier Model

- 在Tier Model中，Microsoft將AD特權區分為三個層級，分別為：
  - Tier 0：企業的身分識別系統及管理這些系統的特權
  - Tier 1：提供企業內部或外部服務的伺服器，以及具有眾多伺服器管理權限之特權
  - Tier 2：企業內部提供給使用者操作的終端電腦、網路設備或行動裝置，以及管理這些資產的管理權限。
- 不同層級的管理權限其管理範圍應僅限於相同層級，不可跨區混用。降低管理權限遭受竊取的風險。



正確觀念：
除了管理上的落實外，也必須透過登入限制等機制強制落實Tier Model

如何正確的保護AD特權

Privileged Access Workstations

- 除了Tier Model外，操作AD特權的時候，也建議透過Privileged Access Workstations來進行。特權帳號落地在一般OA電腦上是絕對禁止的，因為：
  - 透過RDP連線到Server：攻擊者可以透過Key Logger竊取帳號密碼，或者竊取儲存在RDL檔案中的儲存密碼。
  - 透過MMC連線到Server：透過MMC連線到遠端伺服器前，必須先以本機登入到用戶端電腦以便發起MMC連線。攻擊者可以透過Pass-The-Hash或者Pass-The-Ticket來竊取記憶體中快取的Credential

- PAW必須落實以下控制項目：：
  - 其佈署必須是標準化與自動化的
  - 其網路環境必須是隔離的
  - 作業系統本身必須落實安全性基準線
  - 必須佈署資安工具/稽核工具在這些終端上
  - 僅有AD特權帳號可以登入PAW

正確觀念：
管理不同層級的伺服器也需要使用不同層級的PAW，屆以達成特權的完全隔離。

如何正確的保護AD特權

Security Control for Tier privileged account

Tier 0	Tier 1	Tier 2	Standard
			Administrator Enablement, Accountability, and Lifecycle Enforcement
●	●	●	Administrative personnel standards
●	●	●	Administrative security briefing and accountability
●	●	●	Provisioning and de-provisioning processes for administrative accounts
			Operationalize Least Privilege
●	●	●	Limit count of administrators
▲	▲	▲	Dynamically assign privileges
			Manage Risk of Credential Exposure
●	●	●	Separate administrative accounts
●	●	●	Administrator logon practices
●	●	●	Use of approved support technology and methods
●	●	●	No browsing the public internet with admin accounts or from admin workstations
●	●	●	No accessing email with admin accounts or from admin workstations
●	●	●	Store service and application account passwords in a secure location.
			Strong Authentication
●	▲	▲	Enforce smartcard multi-factor authentication for all admin accounts
●	▲	▲	Enforce multi-factor authentication for all cloud admin accounts
			Rare Use / Emergency Procedures
●	N/A	N/A	Correctly follow established processes for all emergency access accounts
●	N/A	N/A	Restrict and monitor usage of emergency access accounts
●	N/A	N/A	Temporarily assign Enterprise Admin and Schema Admin membership

●	**Mandatory**
▲	**Strongly Recommended**
○	**Recommended**

https://docs.microsoft.com/en-US/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

保護AD不難，找到重點而已

- 以下都是實際案例，不要笑：
  - 我們看過AD的Built-in\Remote Desktop Users群組中放了數萬個員工帳號
  - 我們看過公司將Built-in\Account Operators權限賦予個人電腦維運廠商的員工
  - 我們看過Domain Admins權限拿去在數百台伺服器上執行系統備份 (然後其中一台伺服器被駭了，所有伺服器跟著死)
  - 我們看過國外的子網域被攻擊，打回台灣的根網域
  - 我們看過Domain Admins被竊取，全公司的電腦被加密
  - 我們看過客戶有稽核Domain Admins、Enterprise Admins的成員異動，卻沒有稽核AD Built-in\Administrators
- 人必先自助，然後天助：知道自己要保護什麼，別人才能保護你。
- 對於所有特權的使用需要有警覺性是身為AD管理者的基本素質。

Key takeaway

- 聽完這個Session，您應該知道為何保護AD特權至關重要
- 聽完這個Session，您應該知道AD特權的類型
- 聽完這個Session，您應該對於Microsoft Tier Model的內涵有所了解