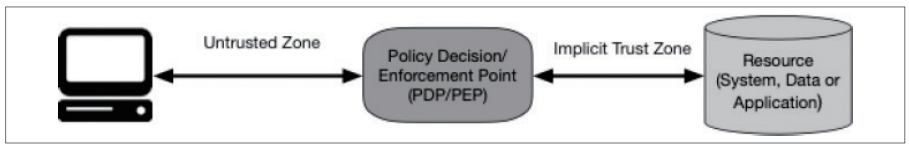
用 One Identity 啟動您在 AD/Azure AD 的零信任 (Zero Trust) 旅程！

根據 One Identity 研究調查顯示，近幾年來有將 95% 的駭客攻擊事件都是從 Microsoft Active Directory (以下簡稱 AD) 開始。這意味著在身分的資安管控上變得相當重要，如果沒有一個適當的管理、保護方式，將會讓整個企業的內部威脅急遽提升，導致從業務到個資受到衝擊和外洩都是常有的事情。

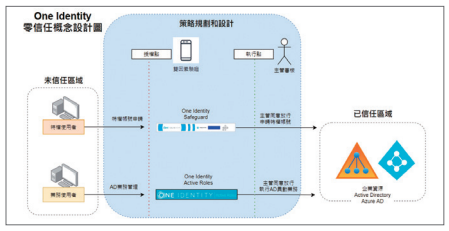
於是 NIST 也在去年 8 月正式發佈出來零信任的架構，希望企業中擔任資安長、資安主管或者資安負責人員，能夠在既有的 ISO27001 或者 NIST 的資安框架下針對自己的核心資產去做更精細的強化。這也代表著資產負責人或者管理人員需要把核心業務在管控上拆解到授權點和執行點，並有策略去規劃運作，來達到”驗證且永不信任”的方式。而 AD/Azure AD 普遍來說會是企業的核心資產，更是關鍵。在此，One Identity 提出零信任解決方案，消弭一般管理 AD/Azure AD 在整合和運維上的痛點。



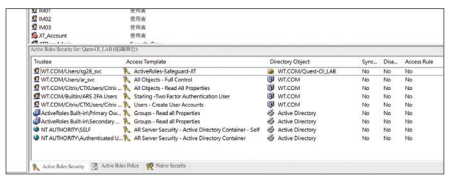
先了解零信任架構的概念。(摘自 **NIST 800-207 Zero Trust Architecture** 文章，第五頁圖)

拆解業務和特權權限，打造零信任的存取架構

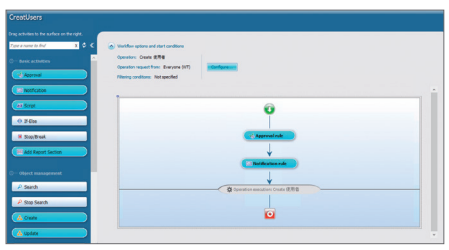
因此要怎麼兼顧資安和管理一直都是 AD/Azure AD 的挑戰，這也是多數企業難以去管控的事情。而現在利用 One Identity Active Roles(AD 帳號治理系統) 搭配 One Identity Safeguard(特權帳號管理系統)，可針對微軟環境去實施零信任的架構。其主要關鍵點在於如何訪談引導出 AD/Azure AD 該怎麼和組織業務或者維運流程進行對應，並協助客戶把業務和特權權限拆解，將這些繁瑣的設定變成零信任架構上。也就是說我們能夠透過管理 AD 的經驗和企業流程上的想法合而為一，成為專業的系統設定去規劃，如此運作上才能系統跟著組織實際流程走，甚至做到自動化。



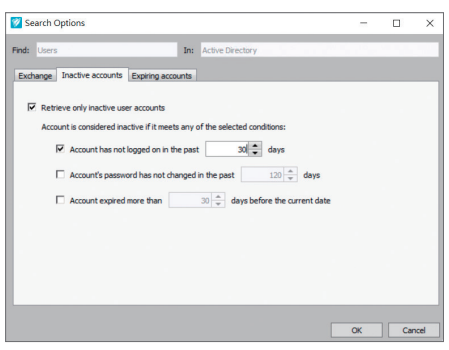
Active Roles 搭配 Safeguard



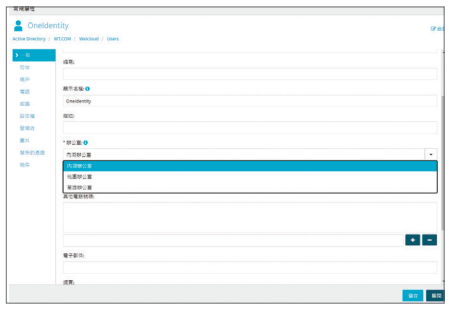
委派權限上，可看見利用範本進行委派，並且相當容易識別 **OU** 下委派了哪些權限。



業務流程經過精細拆分，可指定哪些人要創建帳號前需要經過審核流程才能創建。



也可透過自動化管理，對於超過一個月沒有登入過的帳號，進行關閉。



可根據組織策略設定好的規則，辦公室欄位只能按選單文字去創建，不用像過往設定過程中會有打錯字或者每次命名不同的問題。

當企業根據組織流程設定各種自動化或者規則化之後，接下來可以導入 Starling 2FA 的雲端雙因素驗證機制，來讓每個人要進入 Active Roles 前，必須先經過雙因素驗證來確認是否其本人；在執行業務流程的時候，還需要經過審核流程，才能異動 AD/Azure AD。如圖，流程使用者會從非信任區朝向信任區的前進，在策略上實施零信任概念中的授權點和執行點，藉此達到層層關卡，並且裝置和人對這些操作進行”驗證且永不信任”。

此外，我們也不能讓 Domain Admins 權限成為漏網之魚，因此 One Identity 將會透過 Safeguard 特權系統納管網域上面所有的特權帳號，並且利用 Active Roles 達到 Just in Time Access，我們稱之為臨時特權存取。

帳號登入後須敲打 **OTP**，來達到用裝置進行授權的動作。

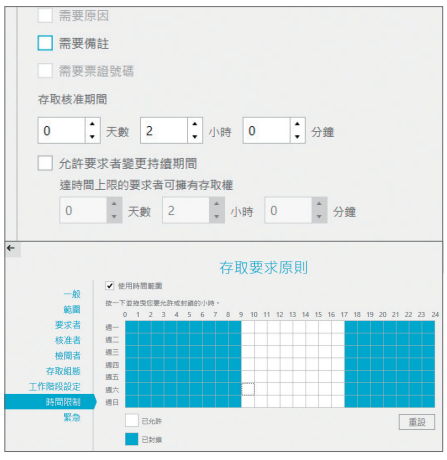
Active Directory/Azure AD 上常見的幾個難題

- 管理上無法有效的限縮執行的權限，常常讓人資或者執行人員擁有過大的權限，導致當責或者管理人員沒有辦法得知執行人員在上面的操作是否得到允許。
- 委派太多的權限在不同的 forest(樹系) 或者 OU(組織單位)，演變成難以盤查，在收斂上往往曠時費日，變成一種惡性的債務。
- 無法規則和定義上所有的業務操作，導致每個帳號中的欄位會根據不同的管理人員就有不一樣的設定。
- Domain Admins 權限為了管理方便而同仁共享帳號，或者為了辨識又創建太多特權帳號。
- Domain Admins 權限難以限縮到只剩下一個。

甚麼是臨時特權存取 (Just in Time Access) ？為何要臨時特權存取？

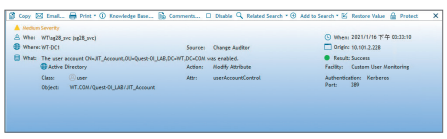
臨時特權存取是在零信任架構下延伸出來的概念，目的是為了限縮特權帳號的使用時間之外，還提供了降權和關閉帳號的功能，供管理者可按照這些選項幫組織規劃後，設計出一個符合企業本身的”最小特權原則”(principle of least privilege)。

首先我們規定了申請特權的時間，並且申請後需要主管核准；主管核准完畢，系統會把已經 disable/ 停用的帳戶進行 enable/ 啟用，接著將啟用好的帳號提權進入 Domain Admins 群組。如此一來，就可確保使用者在存取資源的時候才擁有特權，而帳號歸還或未使用之時，基本上帳號是會恢復 disable 狀態。這種被 disable 的帳號對惡意攻擊者而言，他也不會想到是特權帳號，而最後剩下的特權帳號經過 One Identity 收斂後，可以最少剩下一個，那麼接下來就可以用 Log 軟體或者 SIEM 平台仔細觀察這個帳號是否有異常活動。於是攻擊面的縮小，也讓管理人員可以更專心防禦一個點而非整個面。



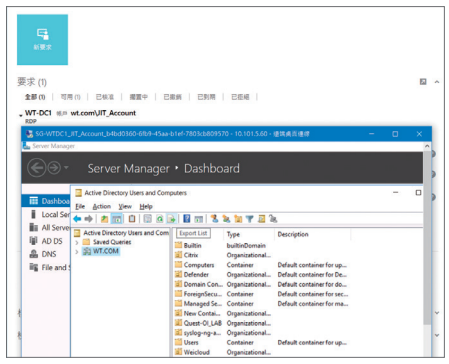
規定特權的申請使用的時間限制於白天的09:00~17:00，並且只能一次最多借取兩個小時。

經由申請特權帳號後，特權帳號會自行啟動帳號，並且自動拉入 Domain Admins 群組



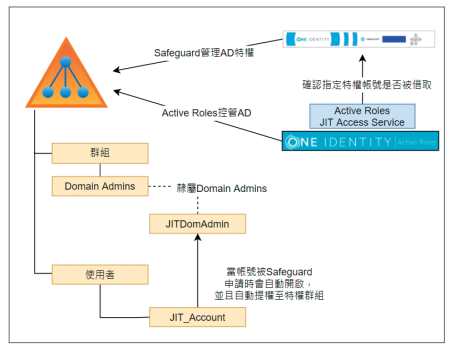
可以看見帳號被 Enable。(示意圖為 Change Auditor 的 5W 呈現)

帳號被搬進 JITDomAdmin 群組中，也就是我們設定好的 Domain Admins 群組。(示意圖為 Change Auditor 的 5W 呈現)



申請特權帳號完成，代登入進入 DC 裡面。

到此，我們終於看見整個臨時特權存取的全貌，它讓整個網域的防護並不是依賴過去網路層或者平台層的縱深保護，而是確確實實的保護在 Application 這一層。可避免掉內部人員或者有心人士造成的威脅，並在資安管控上又達到更精細更好的防護，讓惡意攻擊者又少了一個入侵的方式。



零信任架構的概念，也讓特權帳號更貼近組織所需要的高安全性。

最後，導入過程的複雜是必然

台灣目前僅有少部分的企業願意面對資安框架的設計去做權限分責的概念，通常一來時間成本太高，二來內部的組織溝通不順暢，讓很多管理階層或者執行人員難以克服。而主要造成的原因，常常是部門之間的穀倉效應所帶來的問題。因此，更要尋求有資安、身分和特權經驗的廠商一起進行溝通導入，才能讓整個零信任架構的導入事半功倍。

威雲科技 WeiCloud Tech
威雲科技股份有限公司
台北總公司：114 台北市內湖區瑞光路 335 號 5 樓 / (02)7721-8168
台中分公司：403 台中市西區忠明南路 62 號 6 樓之 2 / (04)2328-5588
contact@weicloud.com.tw / https://www.weicloud.com.tw