技能解封中間章程-角色權力保衛戰(RBAC)

**前言**

<https://ithelp.ithome.com.tw/articles/10214081>

RBAC Q&A

**自訂角色的問題**

* 如果無法更新現有自訂角色，請檢查目前登入的帳戶是否已獲指派具有Microsoft.Authorization/roleDefinition/write許可權角色如：擁有者或使用者存取系統管理員。

**訂用帳戶在租用戶間遷移如何復原 RBAC**

* 如何將訂用帳戶轉移至不同 Azure AD 租使用者參考如下文件https://docs.microsoft.com/zh-tw/azure/billing/billing-subscription-transfer
* 如將訂用帳戶轉移至不同的 Azure AD 租用戶，所有角色指派都會從來源 Azure AD 租用戶被移除，且不會遷移至目標 Azure AD 租用戶。 須在目標租用戶自行重建角色指派。
* 如你是 Azure AD 全域管理員且租使用者間移動後無法存取訂用帳戶，則可透過**Azure 資源存取管理**切換提高訂用帳戶存取權。

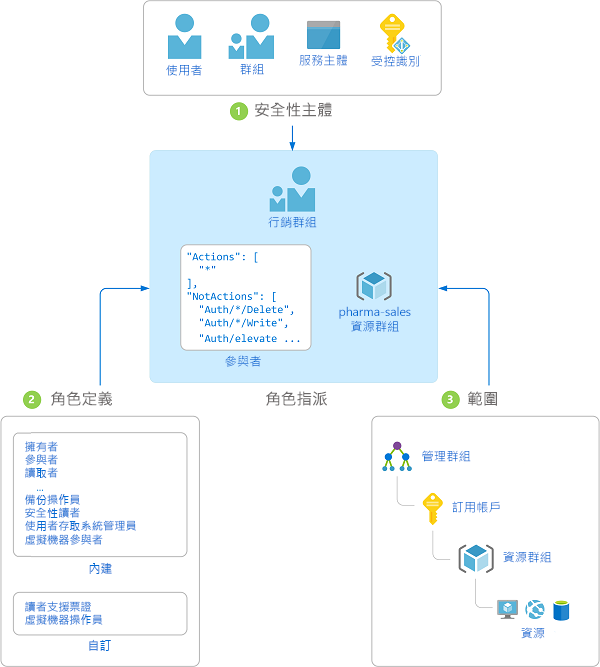
**偵測不到 RBAC 的變更**

* 建立或刪除指派角色等變更可能需要 30 分鐘的時間才會生效顯示。無論是Azure Portal、Azure PowerShell 或 Azure CLI，請透過登出再登入來強制重新整理角色指派變更。

服務架構

RBAC 可把組織角色權責最小化，僅給予作業服務標的本身所需的存取權限。除了一至兩組最高管理員外其餘接不授與他人 訂閱帳戶或資源本身無限大的存取權限，應該僅允許限制在特定範圍內執行特定動作。

下圖所示，我們可以運用 RBAC 建立角色指派來控制資源存取。角色指派包含以下三項組成：  
\* 安全性主體 – 可當作是種物件，作為要求存取資源中的發起者，包含：用戶、群組、服務主體或受控識別。  
\* 角色定義 – 為權力的集合。也就是我們常說的角色。 不管哪種角色細分都一定有每個的執行作業，如：讀取、寫入和刪除。而角色本身除了帳戶擔任外也可以是服務資源如：虛擬機讀取。  
\* 範圍 – 套用存取權給一個所指定的資源範圍。如：從上至下層級範圍分別是管理群組 -> 訂用帳戶 -> 資源群組 -> 資源。範圍結構本身是父子式關聯性擁有繼承關係。



簡易實測環境

圖1. 進到Azure 訂閱服務，在此訂閱點擊此

一張含有 文字 的圖片

自動產生的描述

圖2. 找到IAM存取控制就會看到實務上所需要只配角色授權任務的介面

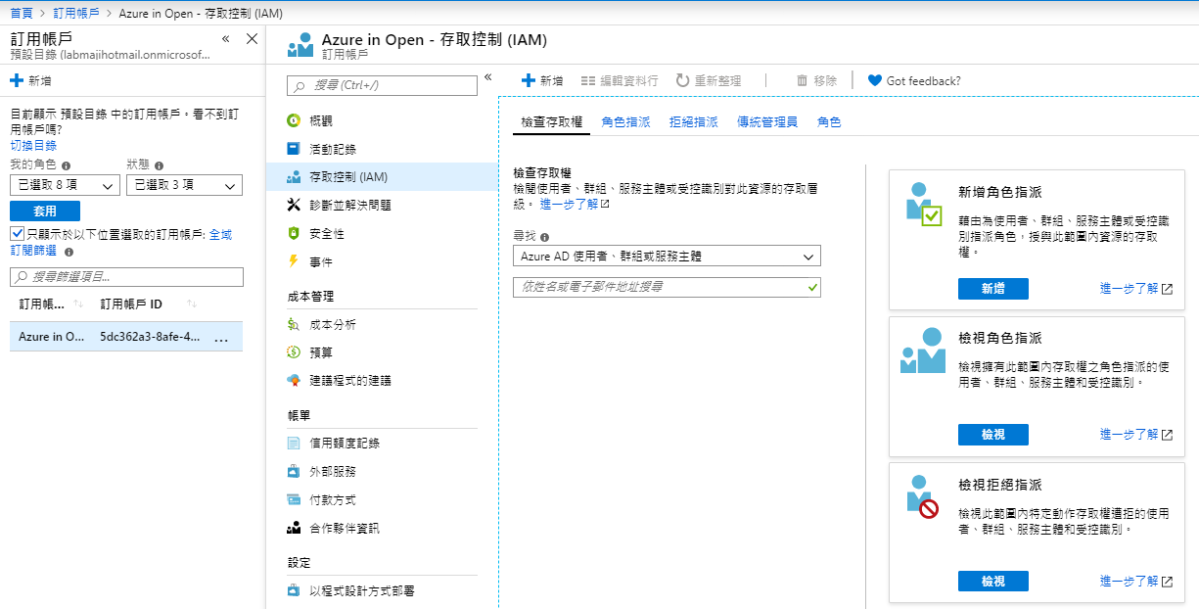


圖3. 這是之前測試已有的角色權限帳戶

一張含有 桌 的圖片

自動產生的描述

圖4. 來新增一個試試，請選擇新增角色指派

一張含有 文字 的圖片

自動產生的描述

圖5. 這就是琳琅滿目個權限角色!一般標準常用都是前三組，依各組織環境需求調整

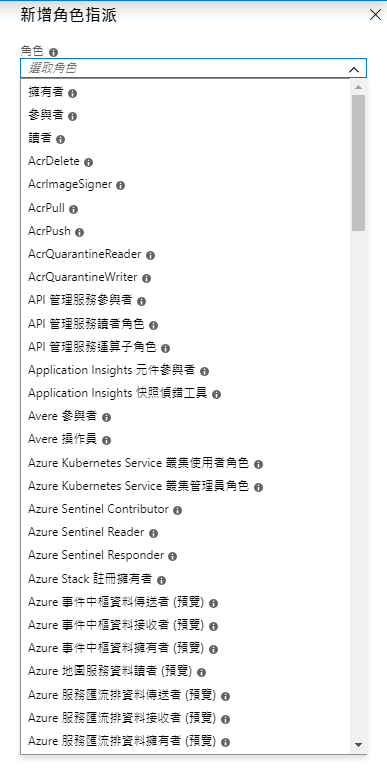


圖6. 目標對象第一項是對帳戶或群組(一般常用)

一張含有 文字 的圖片

自動產生的描述

圖7. 如果是帳戶或群組以外這些服務資源會需要另外綁定受控識別，詳細說明如下：

Azure 資源受控識別會在 Azure Active Directory 中為 Azure 服務提供自動受控識別。 我們可使用此身分識別來向任何支援 Azure AD 驗證的服務進行驗證，無需任何你程式碼中的認證。

<https://docs.microsoft.com/zh-tw/azure/active-directory/managed-identities-azure-resources/overview>

一張含有 文字 的圖片

自動產生的描述

圖8. 從指派的帳戶比較就會看到如果是其他非此訂閱目錄下的帳戶成員指派時都會標註(Guest)在既有目錄下的 AAD 帳號或是群組指派則不會.

補充：如果是 Guest 則會需要收到一封驗證確認信並點選連結才能成功綁定為此訂閱的角色成員

一張含有 文字 的圖片

自動產生的描述

圖9. 透過檢查存取功能可以查看某帳戶的權限狀況

一張含有 文字 的圖片

自動產生的描述

圖10. 進一步可以檢視到此帳戶的實際權限

一張含有 文字 的圖片

自動產生的描述

圖11. 每種權限都有更細的的功能(有可以透過此判別權限給予上再專案實際層面上是否適當)

一張含有 桌 的圖片

自動產生的描述

圖12. 檢視每個功能的讀寫與刪除的各自細部功能支援性

一張含有 桌 的圖片

自動產生的描述

圖13. 在傳統管理員上實際僅針對舊版ASM的服務有用(預設因為此帳號為一開始申請加入就會賦予)

一張含有 文字 的圖片

自動產生的描述

圖14. 示範一下加入共同管理員權限，這次改選擇共同管理員

一張含有 文字 的圖片

自動產生的描述

圖15. 指定一組來新增

一張含有 文字 的圖片

自動產生的描述

圖16. 新增完成如下

一張含有 文字 的圖片

自動產生的描述

圖17. 透過角色可以回頭統計各個角色的用戶或群組數量

一張含有 桌 的圖片

自動產生的描述

圖18. 最後還有個拒絕指派

一張含有 文字 的圖片

自動產生的描述

圖19. 不過此功能並非從此可以設置，另外要做此功能請確認有以下權限角色

一張含有 文字 的圖片

自動產生的描述

圖20. 答案揭曉，此功能是需要透過藍圖這功能範本來佈建的(與原則，政策視為同一類稽核保護服務)

一張含有 文字 的圖片

自動產生的描述

圖21. 上述都是訂閱本身的IAM，此圖是在資源群組下，可以透過範圍來檢視，可以看到訂閱就設置的會有繼承概念，而此資源群組才設置的就只在此資源



圖22. 以下就是更侷限此虛擬機器，觀念同上

