技能解封中間章程-城內防禦機關重啟(Azure Policy)

前言

<https://ithelp.ithome.com.tw/articles/10214082>

成本評估

Azure 原則為免費

Azure Policy Q&A

**哪些區域可使用 Azure 原則？**

* Azure 原則已在所有提供 Azure 的區域正式推出，包括國家雲端。

**可以自建原則嗎？**

* 可以。Azure 原則隨附一組內建原則，但您也可以建立[自訂原則](https://docs.microsoft.com/zh-tw/azure/governance/policy/tutorials/create-custom-policy-definition/)。

Azure 原則支援哪些 Azure 資源？

* 所有 Azure 資源。

可排除資源或訂用帳戶嗎？

* 可從原則指派中排除資源、資源群組、帳戶訂閱或管理群組。

服務架構

上一篇章RBAC多屬於人為本身的權力委派控制這段，而最終目的還是資源，故回歸保護監視限制在訂閱->資源群組->資源本身的政策執行的保護就是此服務的優勢。

一張含有 文字 的圖片

自動產生的描述

簡易實測環境

僅 Allowed storage account SKUs 來做為示範

以下是透過已提供的 JSON 檔作為範例：

<https://docs.microsoft.com/en-us/azure/governance/policy/samples/allowed-storage-account-skus>

圖1. 透過此範本來做佈署，最下面有個 Azure Portal 佈署按鈕

一張含有 文字 的圖片

自動產生的描述

圖2. 選擇範圍(通常是整個訂閱為主，並建立新項目名稱這樣日後自訂的都可以放此比較好辨識)

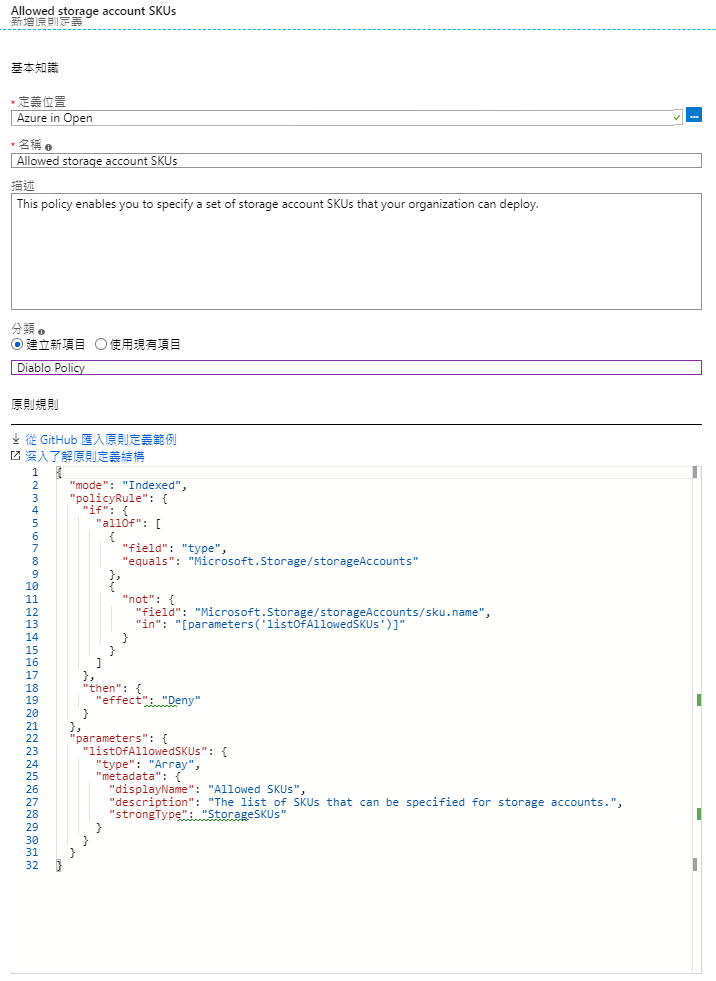
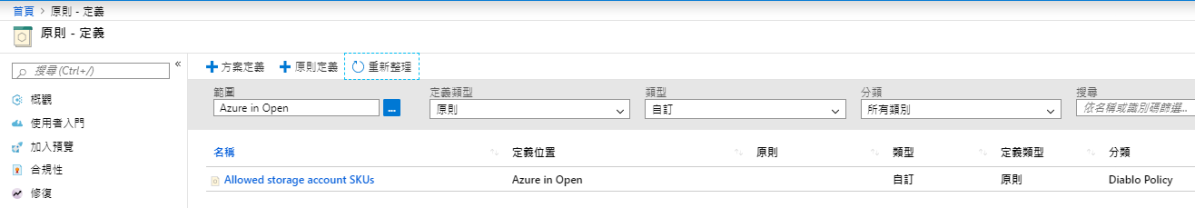


圖3. 確認剛剛設置的原則在自訂類型確實已建立



一張含有 文字 的圖片

自動產生的描述

圖4. 套用剛剛建立的原則

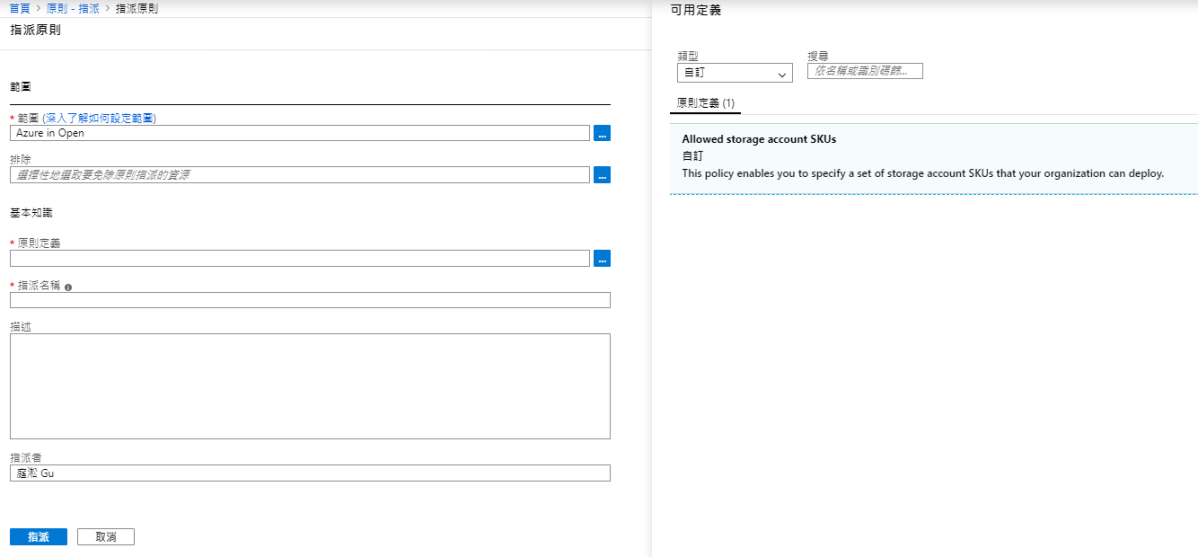


圖5. 除了指派套用剛剛的原則外重要的是下面允許的SKU (我只允許標準LRS層級其餘皆不允許)

一張含有 文字 的圖片

自動產生的描述

圖6. 最後範圍地區我選擇了美國東部(也就是整個訂閱下只要是美國東部地區建立儲存體都不允許標準層LRS以外的建立)

一張含有 文字 的圖片

自動產生的描述

圖7. 指派建立完成

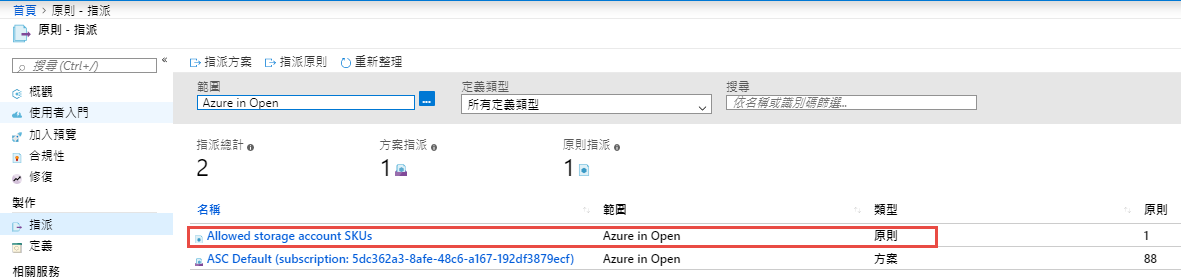


圖8. 在美國東部示範建立儲存體選用標準層LRS以外的等級(此時還沒經過原則偵測顧驗證是正常)

一張含有 文字 的圖片

自動產生的描述

圖9. 有了，很明顯寫到原則限制讓此次建立失敗，可以套用各公司企業避免無預警誤建或亂建導致成本上升的情事

一張含有 文字 的圖片

自動產生的描述

圖10. 進一步看就會檢視到JSON檔裡僅允許的層級，此層及以外的都擋掉

一張含有 文字 的圖片

自動產生的描述