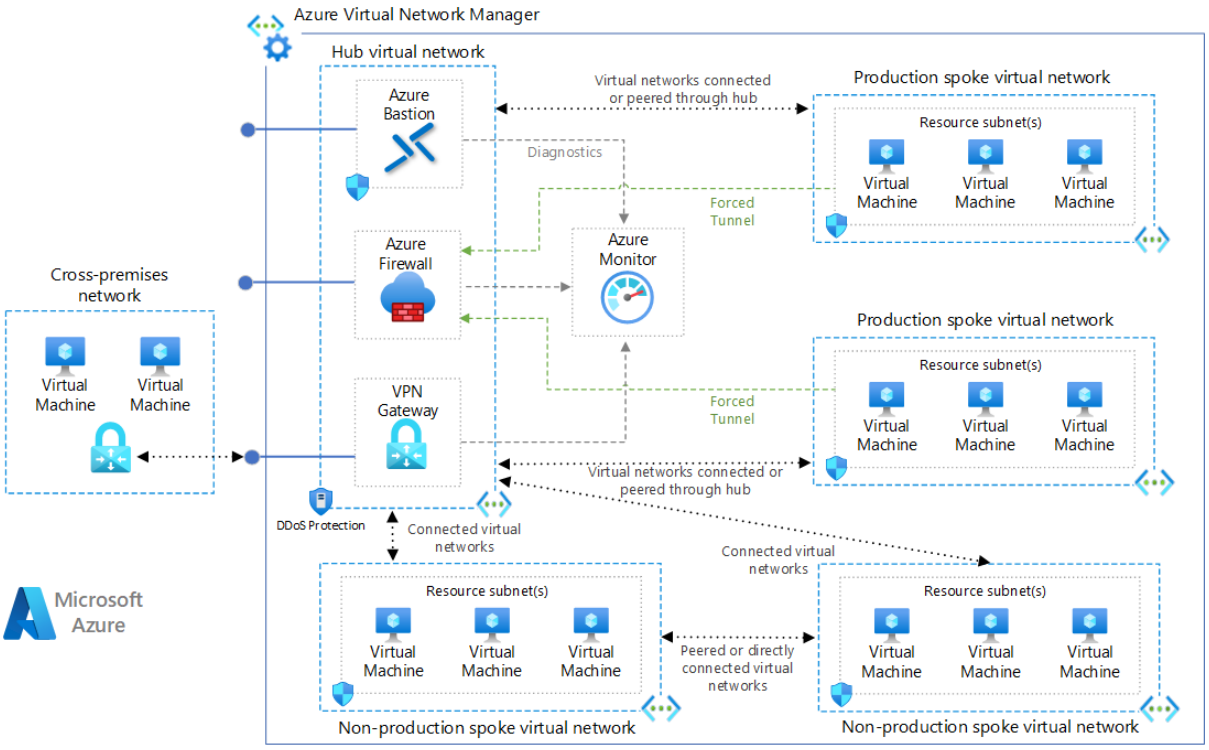
雲端基礎環境建置與安全基準配置實機操作手冊

Contents

Lab 1. Hub and spoke 部署.

此示例在中心輻射型配置中部署 Azure 虛擬網路。此外，還部署了 Azure 防火牆和堡壘主機。（可選）可以部署 VPN 閘道和範例工作負載 （虛擬機）。

在適用的情況下，每個資源都配置為將診斷發送到 Azure Log Analytics 實例。



部署範例

為部署建立資源組。

az account set --subscription “YourSubscriptionId”

LOCATION=japaneast

RESOURCEGROUP_NAME=rg-hub-spoke-${LOCATION}

az group create --name ${RESOURCEGROUP_NAME} --location ${LOCATION}

curl -o main.bicep
https://raw.githubusercontent.com/mspnp/samples/main/solutions/azure-hub-spoke/bicep/main.bicep

使用虛擬機進行部署

運行以下命令，使用部署到第一個分支網路的 Linux VM 和部署到第二個分支網路的 Windows VM 啟動部署。

az deployment group create \

--resource-group ${RESOURCEGROUP_NAME} \

--template-file main.bicep \

--parameters deployVirtualMachines=true adminUsername=azureadmin adminPassword=YourPassword2025!

解決方案部署參數

Parameter	Type	Description
location	string	部署位置。Location 必須支援可用區。
deployVirtualMachines	bool	如果為 true，則將一個基本 Linux 虛擬機部署到分支 1，將一個基本 Windows 虛擬機部署到分支 2。
adminUserName	string	如果部署虛擬機，則為兩個 VM 的 admin 使用者名。
adminPassword	securestring	如果部署虛擬機，則為兩個 VM 的管理員密碼。
deployVpnGateway	bool	如果為 true，則將虛擬網路閘道部署到中心網路（+30 分鐘部署）。

清除資源

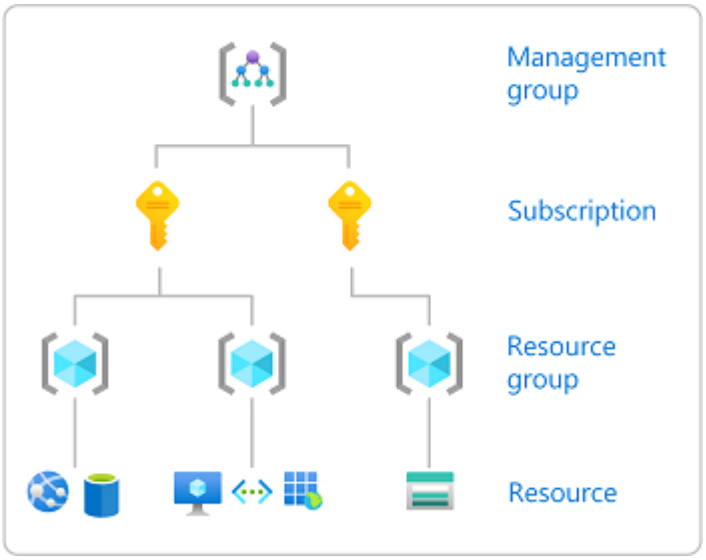
```
az group delete --name ${RESOURCEGROUP_NAME} --yes
```

Lab 2. 檢查使用者對單一 Azure 資源的存取

有時候，您需要檢查使用者對 Azure 資源具有哪些存取權。 您可以列出其指派來檢查其存取權。 檢查單一使用者的存取權的快速方法是使用**存取控制 （IAM）頁面上的 [檢查存取權]** 功能。

步驟 1：開啟 Azure 資源

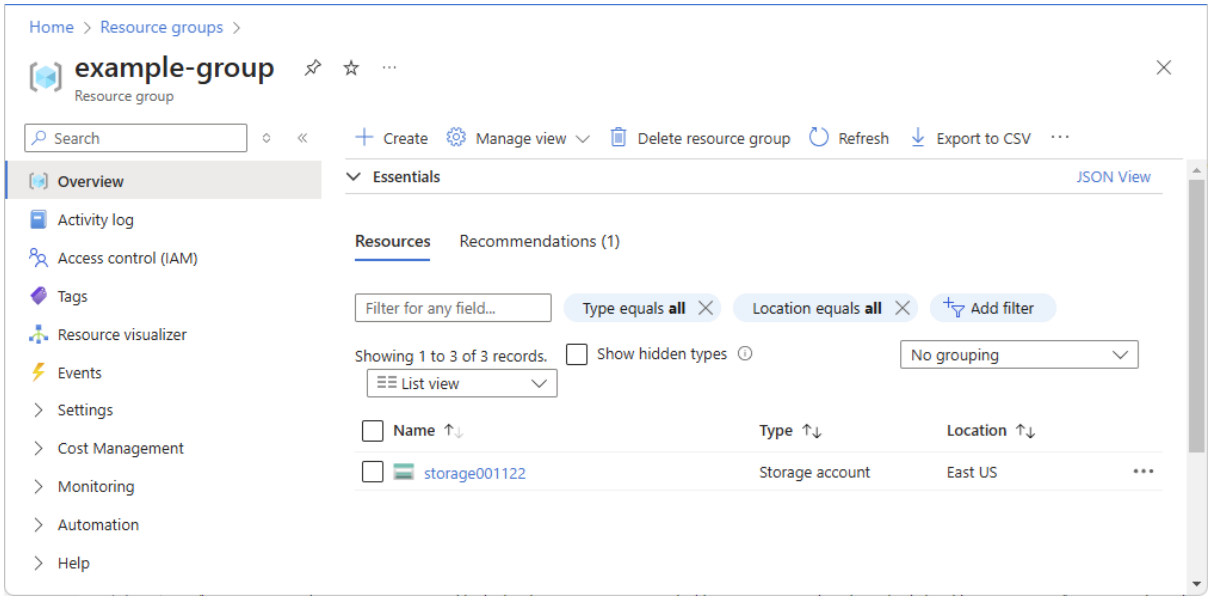
若要檢查使用者的存取權，您必須先開啟要檢查其存取權的 Azure 資源。 Azure 資源會組織成通常稱為 *範圍的*層級。 在 Azure 中，您可以在四個層級上指定範圍，從寬到窄：管理群組、訂用帳戶、資源群組和資源。



請依照下列步驟開啟您想要檢查存取權的 Azure 資源。

1. 開啟 Azure 入口網站。
2. 開啟您想要檢查其存取權的 Azure 資源，例如 **管理群組**、**訂用帳戶**、**資源群組**或特定資源。
3. 選取該範圍中的特定資源。

以下顯示範例資源群組。



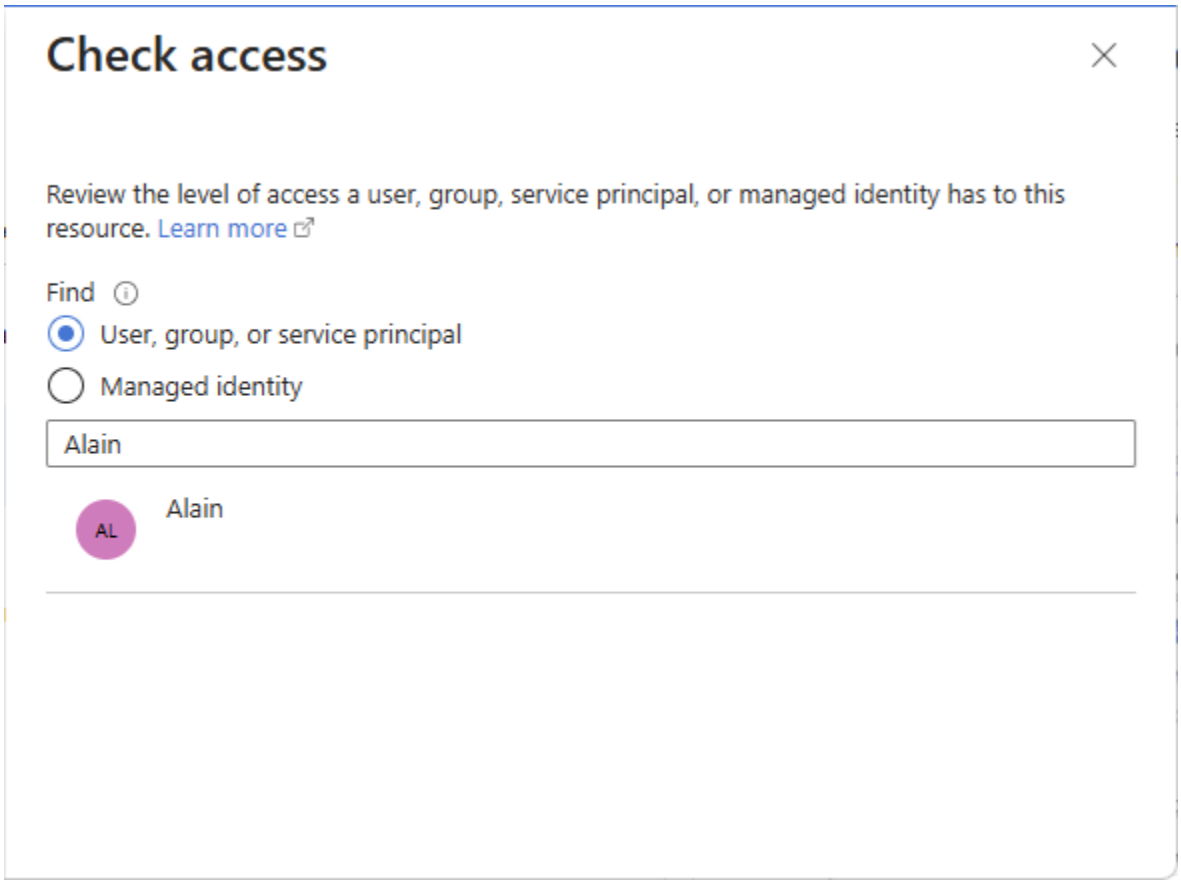
步驟 2：檢查使用者的存取權

請遵循下列步驟來檢查單一使用者、群組、服務主體或受控識別的存取權，以存取先前選取的 Azure 資源。

1. 選取 [存取控制 (IAM)]。
2. 在 [檢查存取權] 索引標籤上，選取 [檢查存取權] 按鈕。

[檢查存取] 窗格隨即出現。

3. 選取 [使用者、群組或服務主體]。
4. 在搜尋方塊中，輸入字串來搜尋目錄的名稱或電子郵件位址。

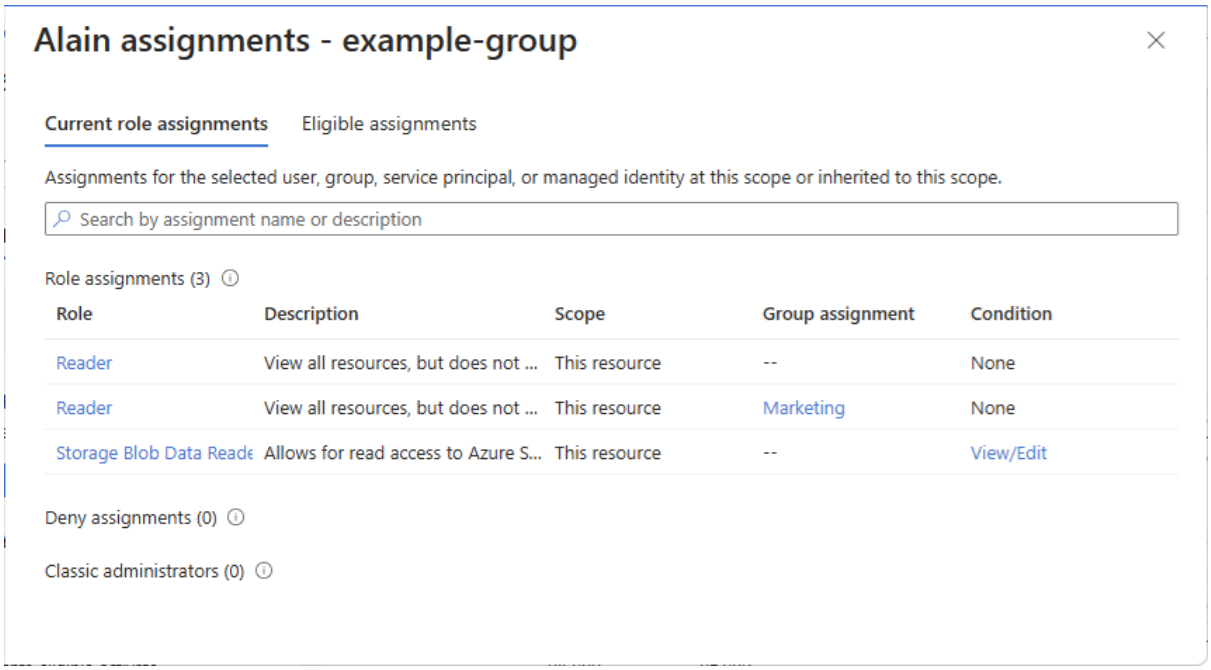


5. 選取使用者以開啟 [指派] 窗格。

在此窗格中，您可以看到此範圍中所選使用者的存取權，並繼承至此範圍。 子範圍的工作分派並未列出。 您會看到下列指派：

- 使用 **Azure RBAC** 新增的角色指派。
- 使用 **Azure** 藍圖或 **Azure** 受控應用程式新增的否定性指派。

如果有任何 合格或有時間限制的角色指派，您可以在 [合格指派] 索引標籤上 檢視這些指派 。



使用 Azure 入口網站建立或更新 Azure 自訂角色

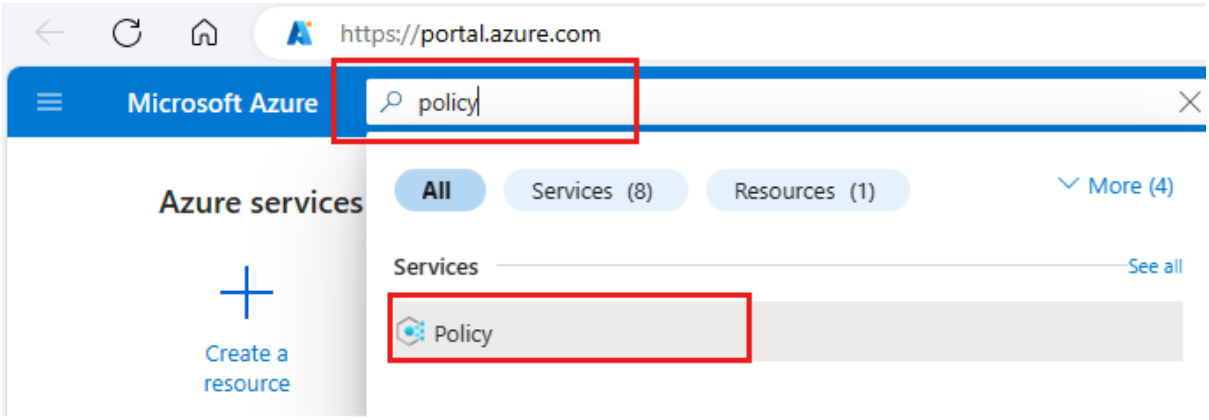
https://learn.microsoft.com/zh-tw/azure/role-based-access-control/custom-roles-portal

Lab 3. 使用 Azure 入口網站建立原則指派，以識別不相容資源

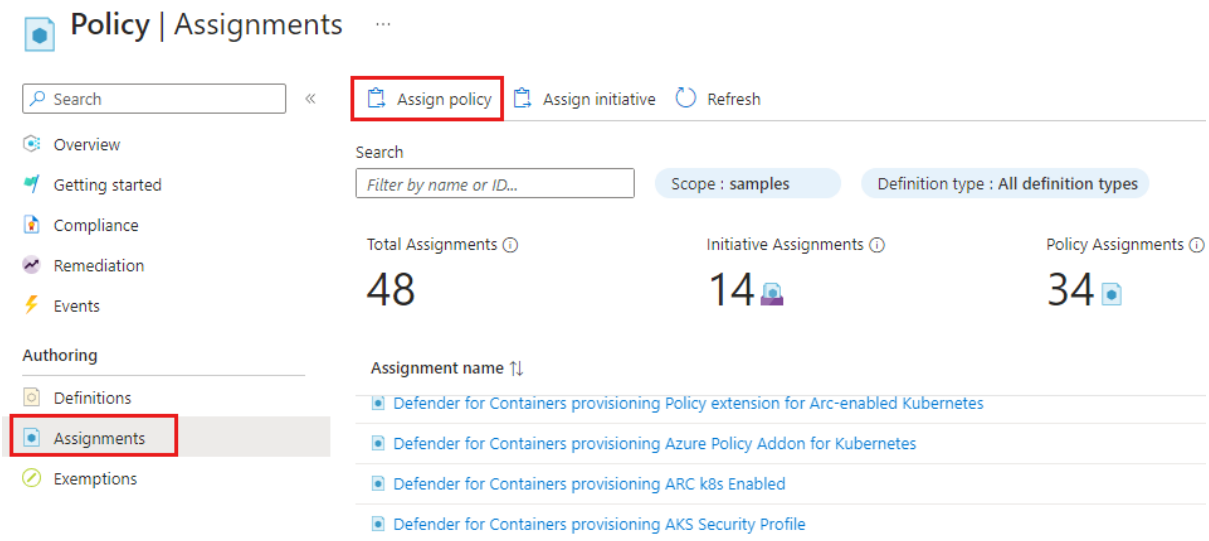
了解 Azure 中合規性的第一個步驟是識別您資源的狀態。 在本快速入門中，您將使用 Azure 入口網站來建立一個原則指派，以識別不符合規範的資源。 此原則會指派給資源群組，且其會稽核不使用受控磁碟的虛擬機器。 建立原則指派之後，您將識別不符合規範的虛擬機器。

建立原則指派

1. 登入 Azure 入口網站。
2. 搜尋 [原則]，然後從清單中選取它。

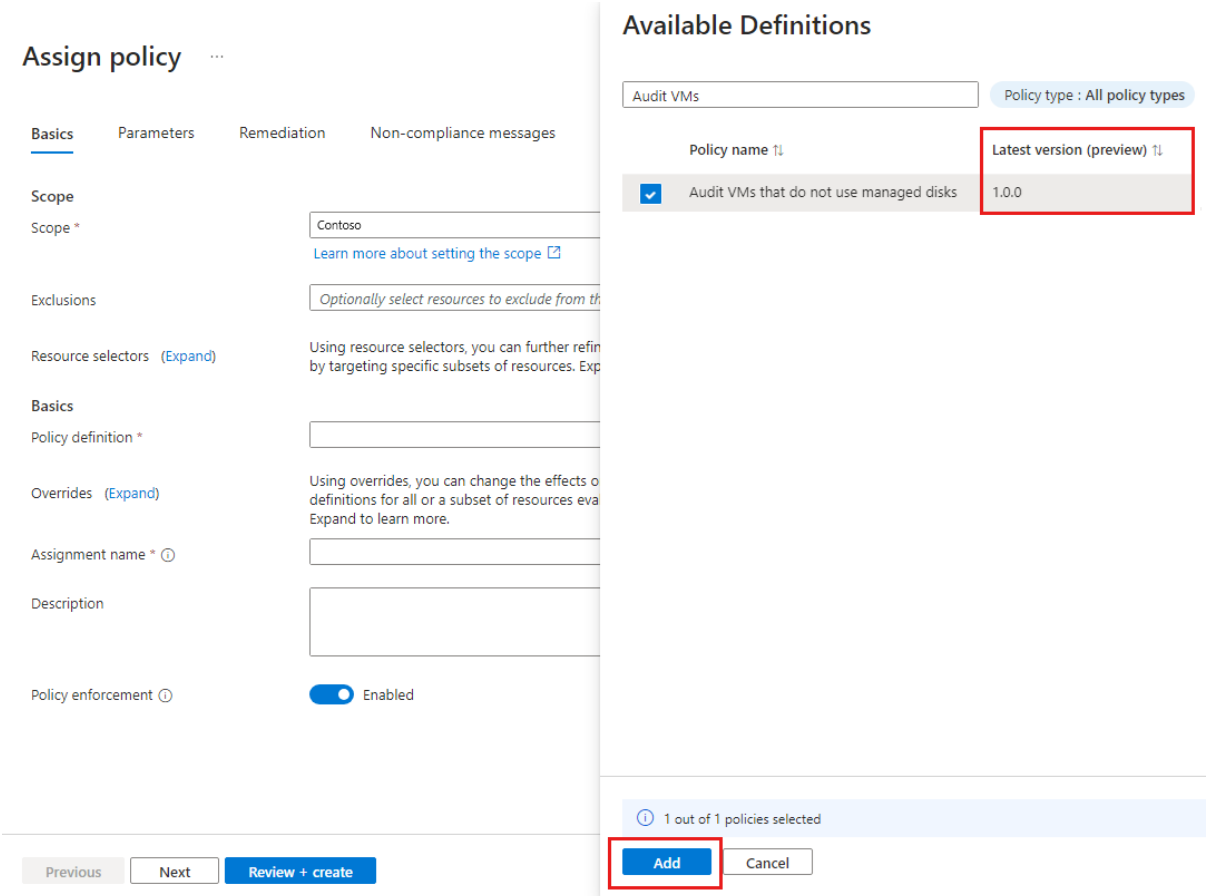


3. 選取 [原則] 窗格中的 [指派]。



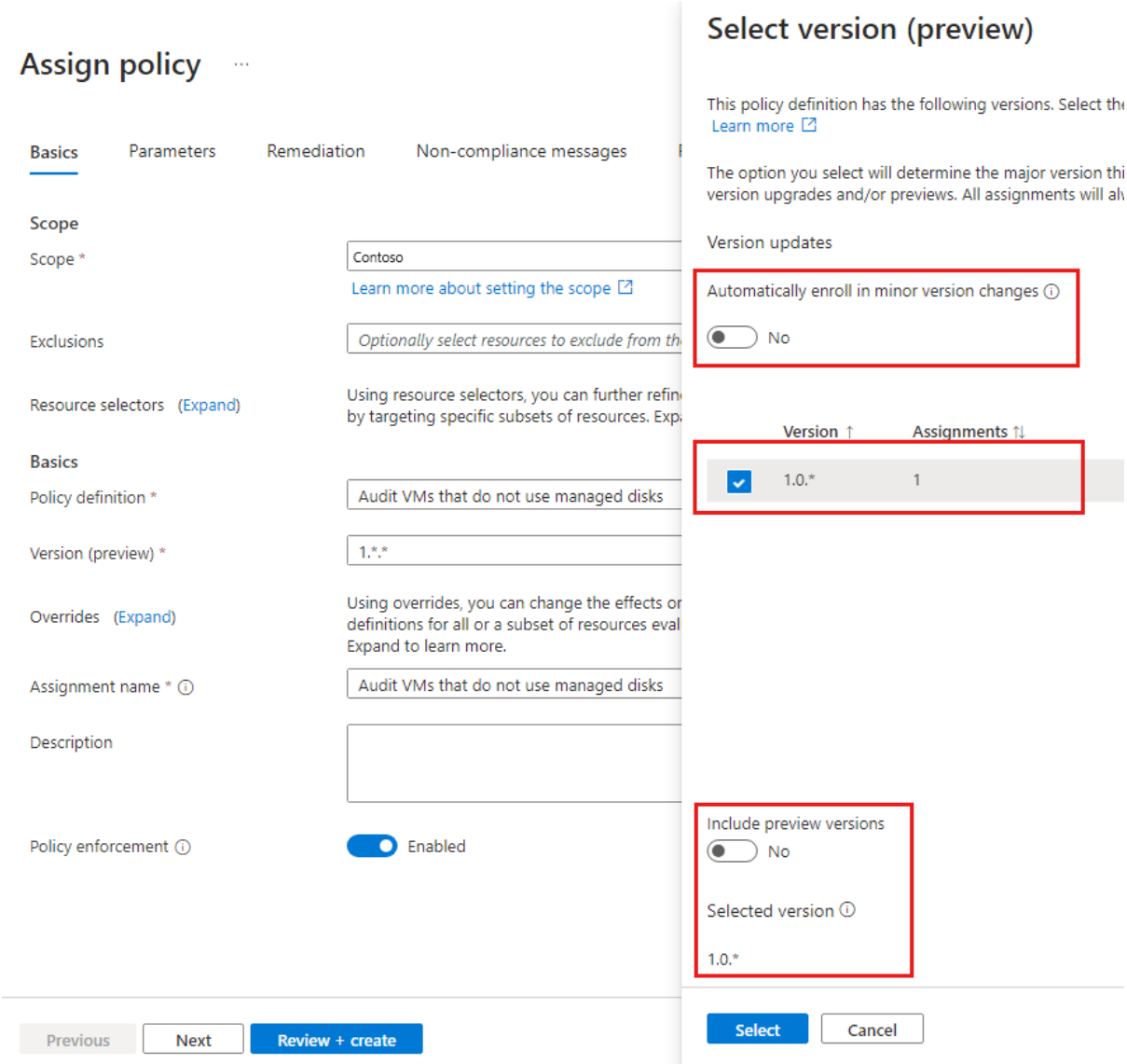
4. 從 [原則指派] 窗格選取 [指派原則]。

5. 在 [指派原則] 窗格 [基本] 索引標籤上，設定下列選項：



6. 選取 [原則定義] 之後，您可以變更 [版本 (預覽)] 選項。

例如，如果您選取影像中顯示的選項，[版本 (預覽)] 會變更為 1.0.*。



7. 選取 [下一步]，以檢視 [參數] 和 [補救] 的每個索引標籤。 此範例不需要進行任何變更。

8. 選取 [下一步]，然後在 [不符合規範訊息] 索引標籤上建立 [不符合規範訊息]，例如*虛擬機器應該使用受控磁碟*。

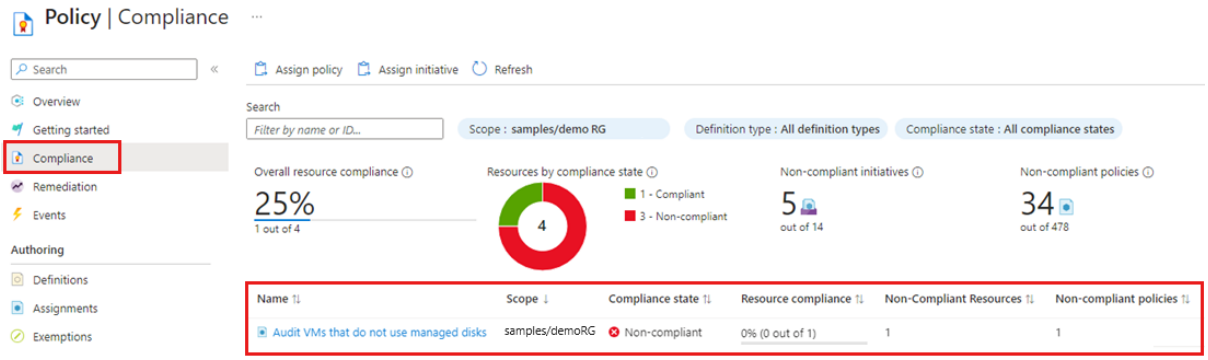
當資源遭拒絕或在一般評估期間資源不符合規範時，就會顯示此自訂訊息。

9. 選取 [下一步]，然後在 [檢閱 + 建立] 索引標籤上，檢閱原則指派詳細資料。

10. 選取 [建立] 以建立原則指派。

識別不符合規範的資源

在 [原則] 窗格上，選取 [合規性]，然後找出 [未使用受控磁碟原則指派稽核 VM]。 新原則指派的合規性狀態需要幾分鐘的時間才會生效，而且其會提供原則狀態的相關結果。



原則指派顯示不符合**合規性狀態不符合規範**的資源。 若要取得詳細資料，請選取原則指派名稱以檢視**資源合規性**。

Lab 4. 設定網路安全性群組

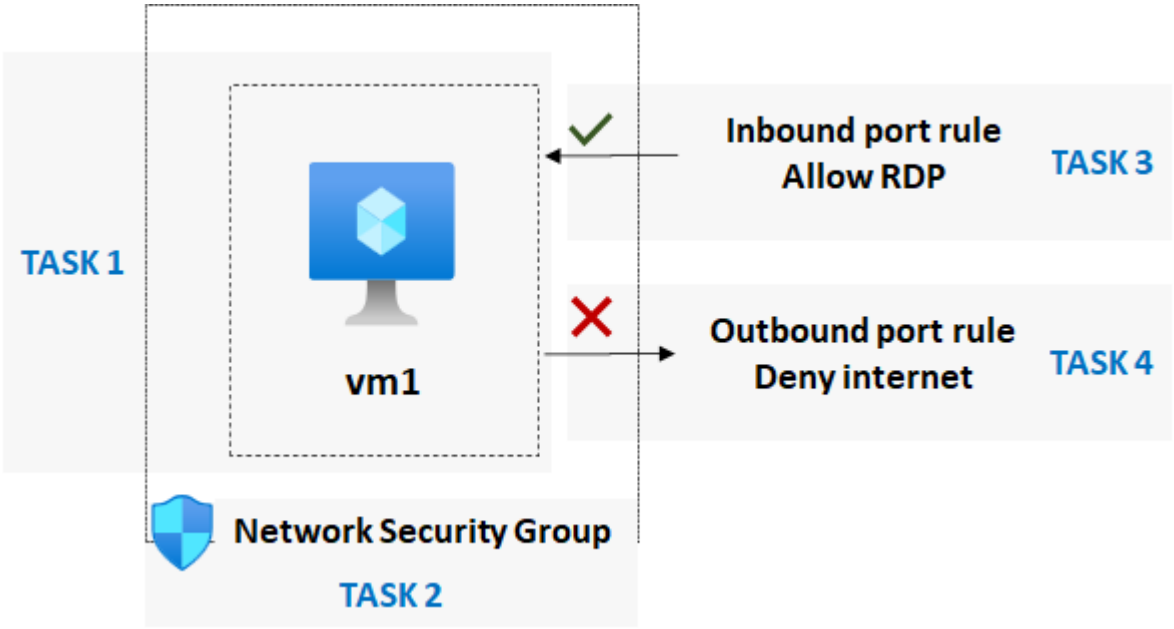
互動實驗室: https://mslearn.cloudguides.com/en-us/guides/AZ-900%20Exam%20Guide%20-%20Azure%20Fundamentals%20Exercise%2013

實驗案例

貴組織想確保虛擬機器的存取受到限制。 身為 Azure 系統管理員，您必須：

- 建立並設定網路安全性群組。
- 將網路安全性群組與虛擬機器建立關聯。
- 拒絕及允許使用網路安全性群組存取虛擬機器。

架構圖



目標

- **工作 1**：建立虛擬機器來測試網路安全性。
    - 建立 Windows Server 虛擬機器。
    - 請勿設定任何輸入連接埠規則或 NIC 網路安全性群組。
    - 確認虛擬機器已建立。
    - 檢閱 [輸入連接埠規則] 索引標籤，確認沒有與虛擬機器相關聯的網路安

全性群組。

- **工作 2**：建立網路安全性群組，並將群組與虛擬機器建立關聯。
    - 建立網路安全性群組。
    - 將網路安全性群組與虛擬機器網路介面 (NIC) 建立關聯。
- **工作 3**：設定輸入安全性連接埠規則，允許 RDP。
    - 確認您無法使用 RDP 連線到虛擬機器。
    - 新增**輸入連接埠規則**，允許 RDP 透過 3389 連接埠連線到虛擬機器。
    - 確認現在可以使用 RDP 連線到虛擬機器。
- **工作 4**：設定輸出安全性連接埠規則以拒絕網際網路存取
    - 確認您可以從虛擬機器存取網際網路。
    - 新增**輸出連接埠規則**，拒絕來自虛擬機器的網際網路存取。
    - 確認您不能從虛擬機器存取網際網路。