

# 雲端基礎環境建置與安全基準配置實機操作手冊

## Contents

Lab 1. 在 Azure 入口網站中建立 Windows 虛擬機器.....	1
Lab 2. 檢查使用者對單一 Azure 資源的存取 .....	7
Lab 3. 使用 Azure 入口網站建立原則指派，以識別不相容資源.....	11
Lab 4. 設定網路安全性群組 .....	15
Lab 5. Hub and spoke 部署. ....	17

## Lab 1. 在 Azure 入口網站中建立 Windows 虛擬機器

本快速入門說明如何使用 Azure 入口網站，在 Azure 中部署執行 Windows Server 2022 Datacenter 的虛擬機（VM）。若要查看作用中的 VM，接著要以 RDP 連線至 VM，並安裝 IIS 網頁伺服器。

### 登入 Azure

登入 [Azure 入口網站](#)。

### 建立虛擬機器

1. 在 [搜尋] 中，輸入*虛擬機器*。
2. 在 [服務] 底下，選取 [虛擬機器]。
3. 在 [虛擬機器] 頁面中，選取 [建立]，然後選取 [Azure 虛擬機器]。[建立虛擬機器] 頁面隨即開啟。
4. 在 [執行個體詳細資料] 底下的 [虛擬機器名稱] 輸入 *myVM*，並在 [映像] 中選擇 [Windows Server 2022 Datacenter: Azure Edition - x64 Gen 2]。其他部分

保留預設值。

#### Instance details

Virtual machine name *	<input type="text" value="myVM"/>
Region *	<input type="text" value="(US) West US 3"/>
Availability options	<input type="text" value="No infrastructure redundancy required"/>
Security type	<input type="text" value="Trusted launch virtual machines"/> <a href="#">Configure security features</a>
Image *	<input type="text" value="Windows Server 2022 Datacenter: Azure Edition - x64 Gen2"/> <a href="#">See all images</a>   <a href="#">Configure VM generation</a>
VM architecture	<div><input type="radio"/> Arm64 <input checked="" type="radio"/> x64 <div> Arm64 is not supported with the selected image.</div></div>
Availability zone *	<input type="text" value="Zones 1"/> <div> You can now select multiple zones. Selecting multiple zones will create one VM per zone.</div>

5. 在 [系統管理員帳戶] 下方提供使用者名稱 (例如 **azureuser**) 和密碼。密碼長度至少必須有 12 個字元，而且符合[定義的複雜度需求](#)。

#### Administrator account

Username *	<input type="text" value="azureuser"/>
Password *	<input type="password" value="....."/>
Confirm password *	<input type="password" value="....."/>

6. 在 [輸入連接埠規則] 底下，選擇 [允許選取的連接埠]，然後從下拉式清單中選取 [RDP (3389)] 和 [HTTP (80)]。

#### Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *	<div><input type="radio"/> None <input checked="" type="radio"/> Allow selected ports</div>
Select inbound ports *	<input type="text" value="RDP (3389)"/>

**This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

7. 保留其餘預設值，然後在頁面底部選取 [檢閱 + 建立] 按鈕。

#### Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing  
Windows Server license? \*

☐

[Review Azure hybrid benefit compliance](#)

Review + create

< Previous

Next : Disks >

8. 執行驗證後，選取頁面底部的 按鈕。

[Home](#) > [Create a resource](#) >

## Create a virtual machine ...

✓ Validation passed

#### Basics

Subscription	myAzureSubscription
Resource group	myresourcegroup
Virtual machine name	myVM
Region	West US 3
Availability options	No infrastructure redundancy required
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2022 Datacenter: Azure Edition - Gen2
VM architecture	x64
Size	Standard B2ms (2 vcpus, 8 GiB memory)
Username	azureuser

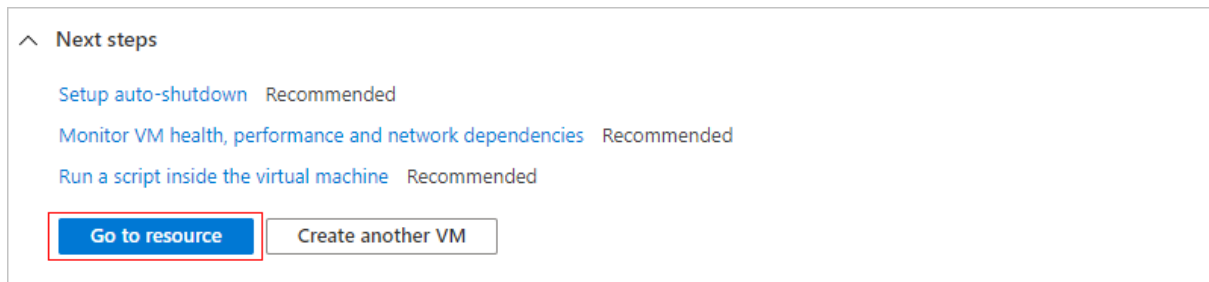
Create

< Previous

Next >

[Download a template for automation](#)

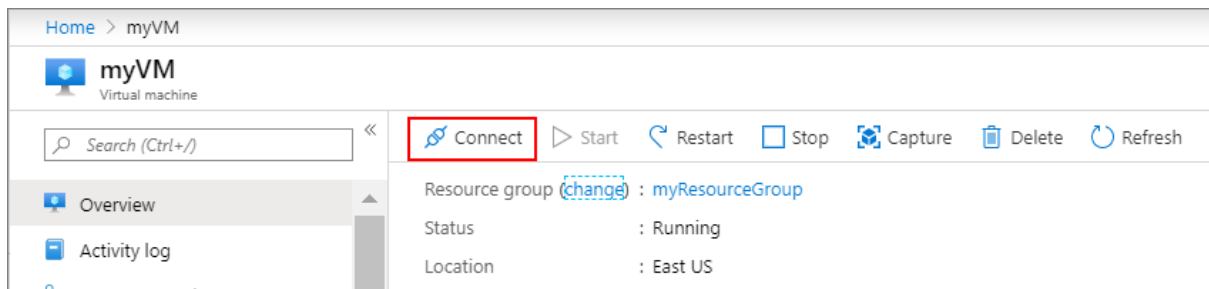
9. 當部署完成時，選取 [前往資源]。



## 連線至虛擬機器

建立虛擬機器的遠端桌面連線。這些指示會告訴您如何從 Windows 電腦連線到 VM。在 Mac 上，您需要 RDP 用戶端，例如來自 Mac App Store 的[遠端桌面用戶端](#)。

1. 在虛擬機器的概觀頁面上，選取 [連線]>[RDP]。



2. 在 [使用 RDP 連線] 索引標籤中，保留以 IP 位址透過連接埠 3389 進行連線的預設選項，然後按一下 [下載 RDP 檔案]。
3. 開啟下載的 RDP 檔案，然後在出現提示時按一下 [連線]。
4. 在 [Windows 安全性] 視窗中，選取 [其他選擇]，然後選取 [使用不同的帳戶]。輸入使用者名稱 **localhost\username**，並輸入您為虛擬機器建立的密碼，然後按一下 [確定]。
5. 您可能會在登入程序期間收到憑證警告。按一下 [是] 或 [繼續] 以建立連線。

## 安裝 Web 伺服器

若要查看作用中的 VM，請安裝 IIS 網頁伺服器。在 VM 上開啟 PowerShell 提示字元並執行下列命令：

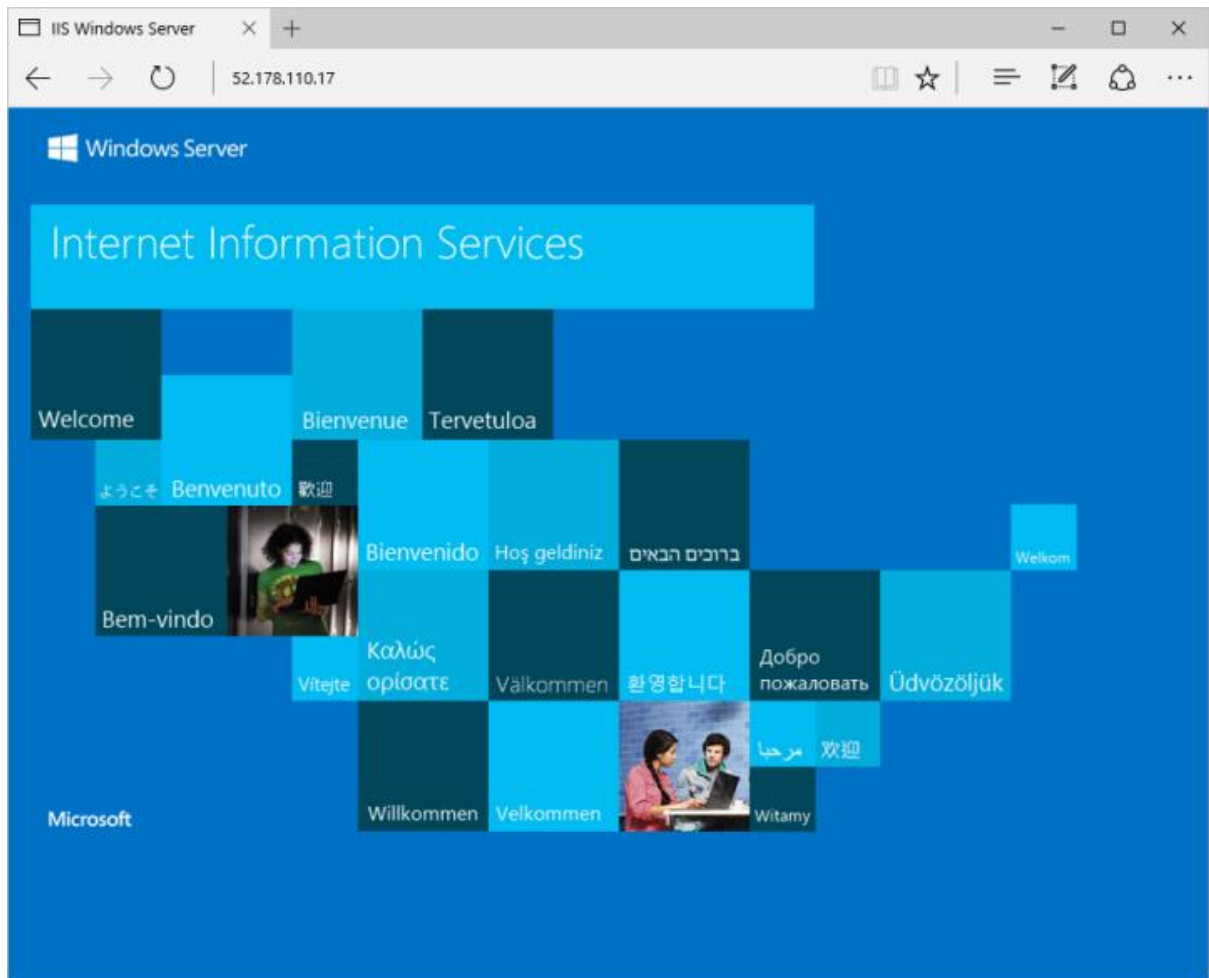
PowerShell 複製

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

完成時，關閉與 VM 的 RDP 連線。

## 檢視 IIS 歡迎使用頁面

在入口網站中選取 VM，並在 VM 概觀中，將滑鼠停留在 IP 位址上方以顯示 [複製到剪貼簿]。複製 IP 位址，並將其貼到瀏覽器索引標籤中。預設的 IIS 歡迎使用頁面將會開啟，而且應如下所示：



## 清除資源

### 刪除資源

如果不再需要，您可以刪除資源群組、虛擬機器和所有相關資源。

1. 在 VM 的 [概述] 頁上，選擇 [資源群組] 連結。
2. 在資源群組的頁面頂端，選取 [刪除資源群組]。
3. 頁面會開啟，警告您即將刪除資源。輸入資源群組的名稱，然後選取 [刪除]，即可刪除該資源和資源群組。

## 自動關機

如果仍需要 VM，Azure 會為虛擬機器提供自動關機功能，以協助管理成本，並確保不會針對未使用的資源向您收費。

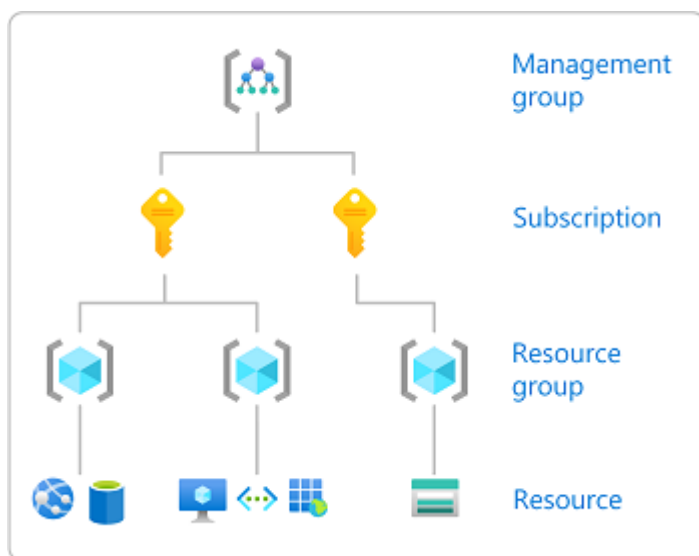
1. 在 VM 的 [作業] 區段上，選取 [自動關機] 選項。
2. 頁面隨即開啟，您可以在其中設定自動關機時間。選取 [開啟] 選項以啟用，然後設定適合您的時間。
3. 設定好時間後，請選取頂端的 [儲存] 以啟用自動關機組態。

## 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

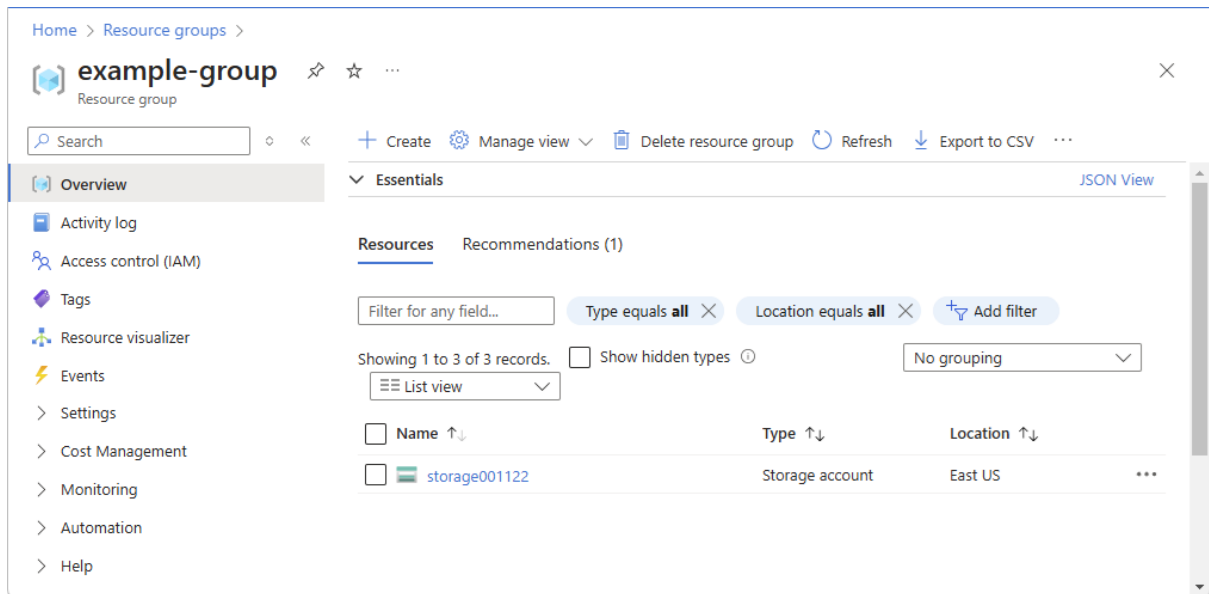
若要檢查使用者的存取權，您必須先開啟要檢查其存取權的 Azure 資源。Azure 資源會組織成通常稱為 **範圍** 的層級。在 Azure 中，您可以在四個層級上指定範圍，從寬到窄：管理群組、訂用帳戶、資源群組和資源。



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。



## Check access

×

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find ⓘ

☒ User, group, or service principal

☐ Managed identity

Alain

AL

Alain

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。

## Alain assignments - example-group

Current role assignments

Eligible assignments

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (3)

Role	Description	Scope	Group assignment	Condition
Reader	View all resources, but does not ...	This resource	--	None
Reader	View all resources, but does not ...	This resource	Marketing	None
Storage Blob Data Reader	Allows for read access to Azure S...	This resource	--	View/Edit

Deny assignments (0)

Classic administrators (0)

使用 Azure 入口網站建立或更新 Azure 自訂角色

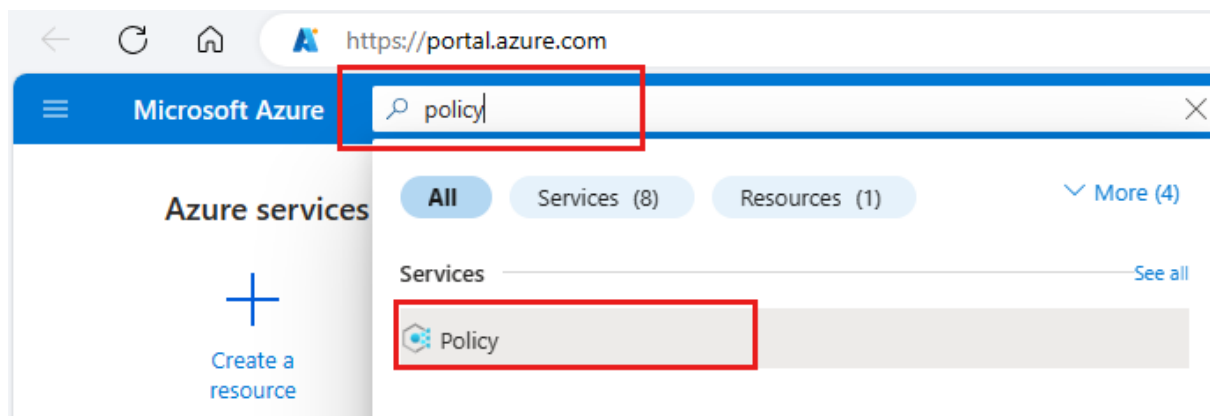
<https://learn.microsoft.com/zh-tw/azure/role-based-access-control/custom-roles-portal>

## 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]。

**Policy | Assignments** ...

Search « **Assign policy** Assign initiative Refresh

Overview  
Getting started  
Compliance  
Remediation  
Events

Authoring  
Definitions  
**Assignments**  
Exemptions

Search  
Filter by name or ID...

Scope : samples Definition type : All definition types

Total Assignments ⓘ 48 Initiative Assignments ⓘ 14 Policy Assignments ⓘ 34

Assignment name ↑↓

- Defender for Containers provisioning Policy extension for Arc-enabled Kubernetes
- Defender for Containers provisioning Azure Policy Addon for Kubernetes
- Defender for Containers provisioning ARC k8s Enabled
- Defender for Containers provisioning AKS Security Profile

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：

**Assign policy** ...

Basics Parameters Remediation Non-compliance messages

Scope  
Scope \* Contoso  
[Learn more about setting the scope](#)

Exclusions  
Optionally select resources to exclude from the scope

Resource selectors (Expand)  
Using resource selectors, you can further refine your search by targeting specific subsets of resources. Expand to learn more.

Basics  
Policy definition \*  
Overrides (Expand)  
Using overrides, you can change the effects of policy definitions for all or a subset of resources evaluated. Expand to learn more.

Assignment name \* ⓘ  
Description

Policy enforcement ⓘ Enabled

Available Definitions

Audit VMs Policy type : All policy types

Policy name ↑↓ Latest version (preview) ↑↓

☒ Audit VMs that do not use managed disks 1.0.0

1 out of 1 policies selected

**Add** Cancel

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.\*。

**Assign policy** ...

**Basics** Parameters Remediation Non-compliance messages

**Scope**

Scope \* Contoso  
[Learn more about setting the scope](#)

**Exclusions**  
*Optionally select resources to exclude from the policy.*

**Resource selectors** [\(Expand\)](#)  
Using resource selectors, you can further refine the scope of the policy by targeting specific subsets of resources. Expand to learn more.

**Basics**

Policy definition \* Audit VMs that do not use managed disks

Version (preview) \* 1.\*.\*

**Overrides** [\(Expand\)](#)  
Using overrides, you can change the effects or definitions for all or a subset of resources evaluated by the policy. Expand to learn more.

Assignment name \* ⓘ Audit VMs that do not use managed disks

Description

Policy enforcement ⓘ ☒ Enabled

[Previous](#) [Next](#) [Review + create](#)

**Select version (preview)**

This policy definition has the following versions. Select the version you want to use. [Learn more](#)

The option you select will determine the major version this policy definition upgrades to and/or previews. All assignments will be updated to the selected version.

**Version updates**

Automatically enroll in minor version changes ⓘ  
☐ No

Version ↑	Assignments ↓
<input checked="" type="checkbox"/> 1.0.*	1

**Include preview versions**  
☐ No

**Selected version** ⓘ  
1.0.\*

[Select](#) [Cancel](#)

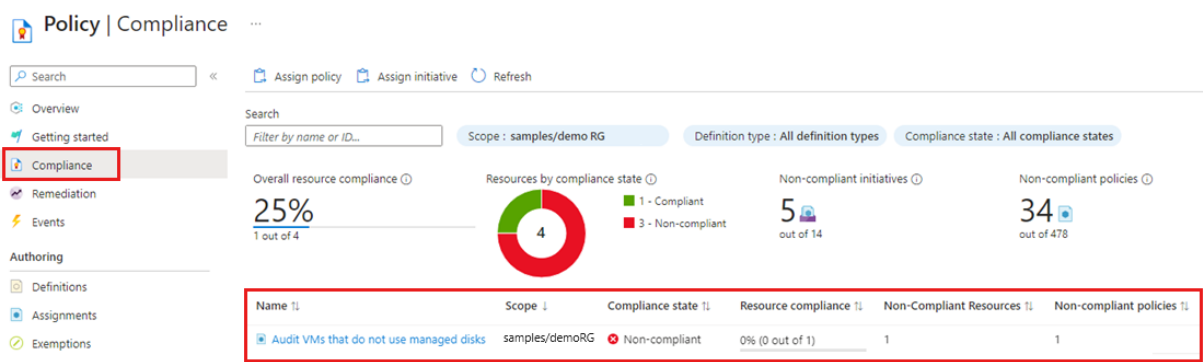
7. 選取 [下一步]，以檢視 [參數] 和 [補救] 的每個索引標籤。此範例不需要進行任何變更。
8. 選取 [下一步]，然後在 [不符合規範訊息] 索引標籤上建立 [不符合規範訊息]，例如**虛擬機器應該使用受控磁碟**。

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

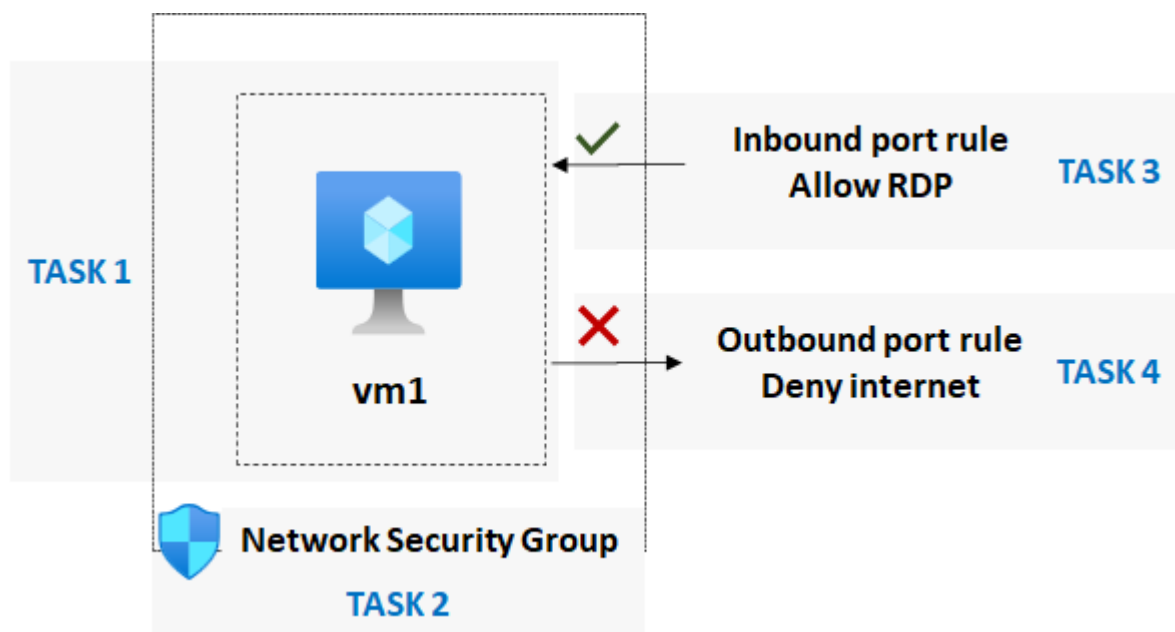
互動實驗室: <https://mslearn.cloudguides.com/en-us/guides/AZ-900%20Exam%20Guide%20-%20Azure%20Fundamentals%20Exercise%2013>

### 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。

更多 Lab:

<https://mslearn.cloudguides.com/en-us/guides/AZ-900%20Exam%20Guide%20-%20Azure%20Fundamentals>

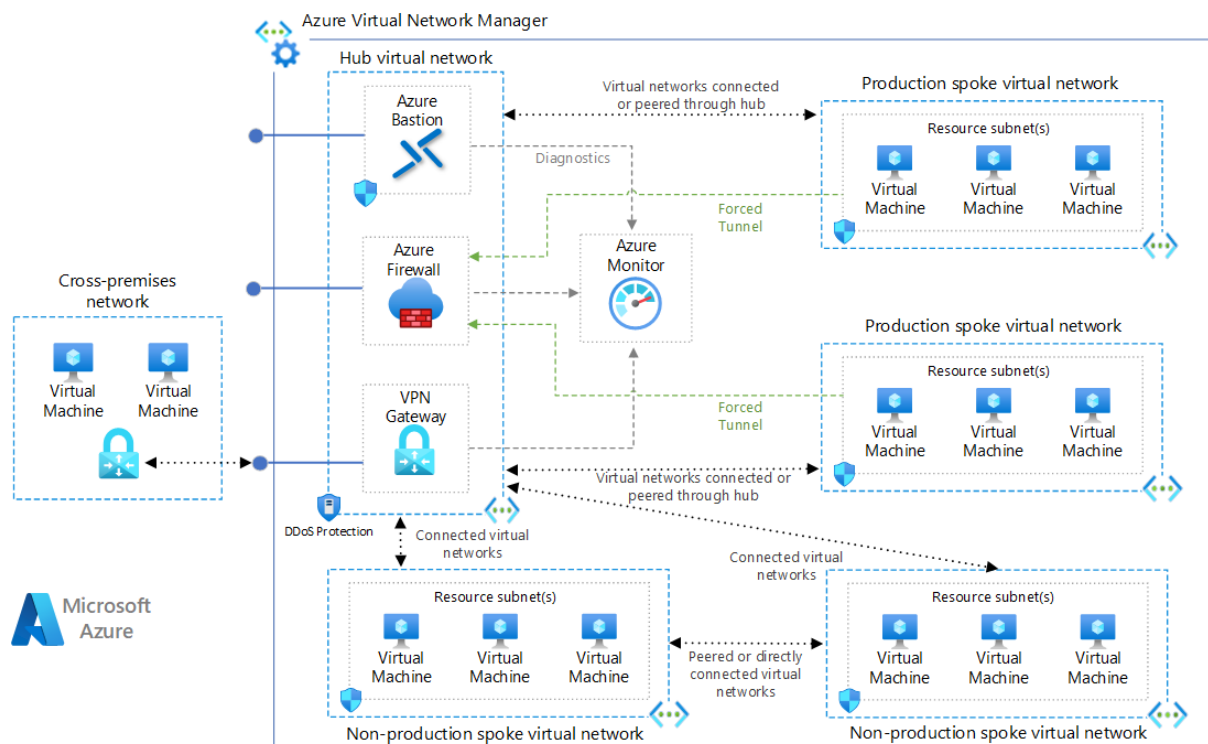


## Lab 5. Hub and spoke 部署.

此為補充 Lab，可以回到公司後自行實做

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
```