運算雲 3.0 服務操作手冊

台灣大哥大運算雲 3.0 服務操作手冊第 14 版

2025 年 02 月修訂

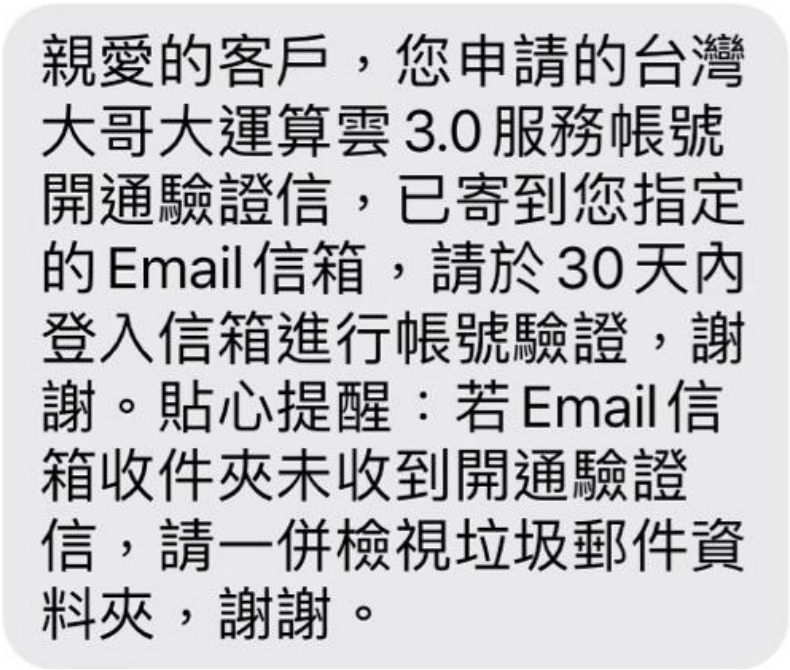
目錄

1. 開通帳號

開通台灣大哥大運算雲 3.0 帳號，請遵循以下申請步驟：

步驟1. 循台灣大哥大業務或客服 0809-000809，填寫申請異動書並完成帳號聯絡人姓名、行動電話、信箱等基本資料及相關網路設定資訊進件，待台灣大哥大客服人員審核通過後，將寄送運算雲 3.0 服務帳號啟用通知信至客戶設定的技術聯絡人信箱。

步驟2. 帳號開通時會收到簡訊通知如下圖:

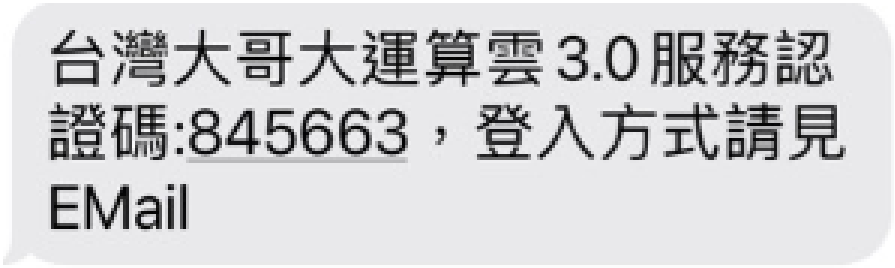


步驟3. 收到電子郵件後，點擊郵件中驗證身分網址的”點我連結”(下圖紅框處) 此為帳號開通時 OTP 驗證。驗證身分網址有效期限 30 天。請盡快在 30 天內開通。

步驟4. 點擊驗證身份網址的”點我連結”後自動開啟驗證碼網頁(如下圖)

點擊” 發送驗證碼” 按鈕，會發送簡訊+Email，請參考下圖。

系統將會發送驗證碼簡訊 (如下圖)



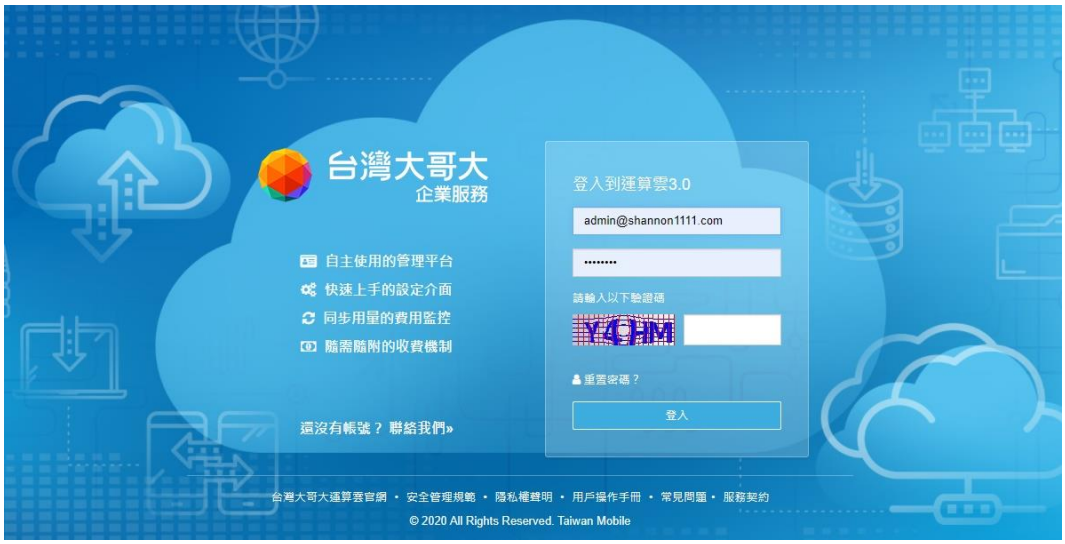
系統將會發送驗證碼通知 mail(如下圖)

填入驗證碼按下” 確定送出” 按鈕


台灣大哥大
企業服務
您的運算雲3.0登入密碼設定完成
回首頁

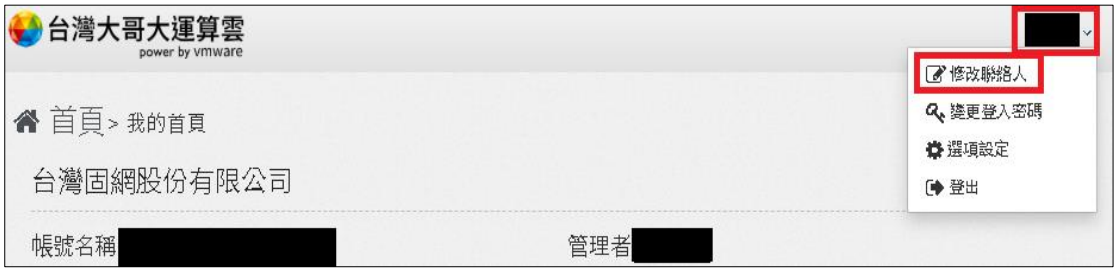
2.第一次登入運算雲 3.0

輸入帳號、密碼及驗證碼，登入運算雲 3.0



修改聯絡人

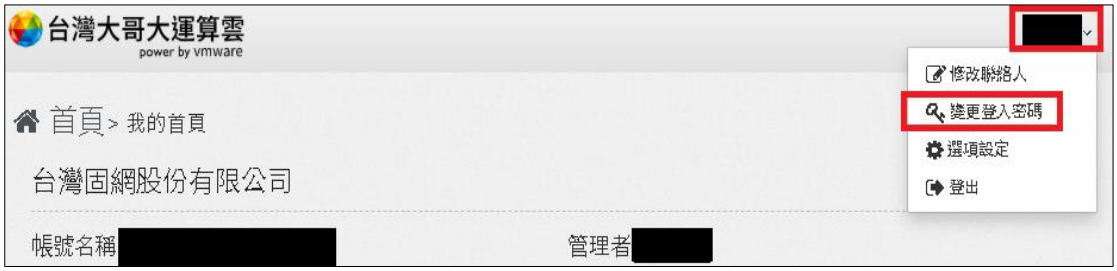
點選畫面右上角帳號 > 點選”修改聯絡人”



進行資料修改 > 點選”確定” > 重新登入

變更登入密碼

點選畫面右上角帳號 > 點選” 變更登入密碼”



輸入原密碼 > 輸入新密碼 > 再次輸入新密碼 > 點選” 確定”

OTP 簡訊驗證選項設定

點選畫面右上角帳號 > 點選" 選項設定"

此設定可選擇是否於雲平台登入時套用 OTP 簡訊驗證，預設 OTP 簡訊驗證功能是關閉。

3.開始使用運算雲 3.0

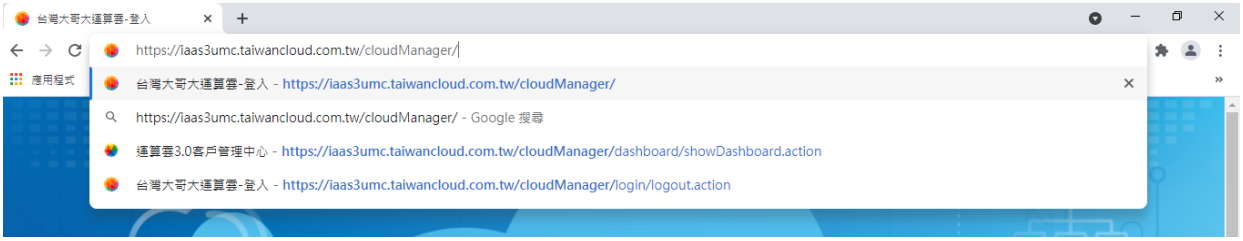
登入運算雲 3.0 的方式

歡迎使用運算雲 3.0，登入方式如下：

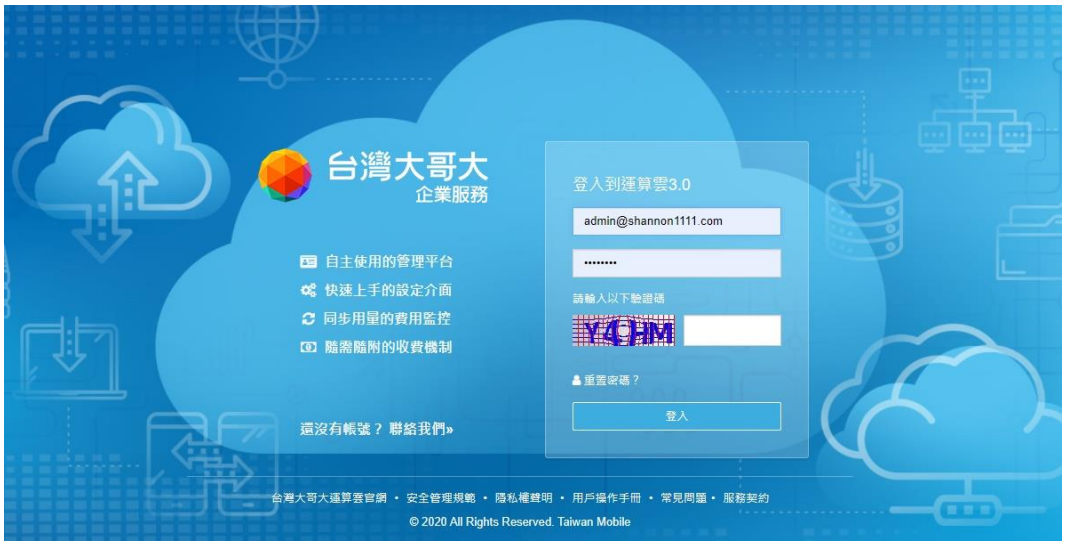
步驟1. **HTML5 統一適用**之網址說明:

https://iaas3umc.taiwancloud.com.tw/cloudManager

請參考下圖範例。



步驟2. 以下為登入網頁，輸入帳號密碼與驗證碼，按”登入”按鈕



步驟3. OTP 驗證若有開啟，登入過程中，就需要進行驗證，會出現下圖網頁，請點發送簡訊與 Email 驗證碼

Email 通知範例如下圖

技術聯絡人行動電話會取得簡訊驗證碼，以下為簡訊範例圖

步驟4.　輸入驗證碼完成驗證，即完成登入程序。

若要操作主機內容，您可以點選「開啟雲平台」後前往雲平台頁面，在雲平台中，您可以即時的在平台上進行 VM 相關服務的申裝、異動或查詢，您同時亦可進行網路相關服務的部分異動與查詢。
(點選後自動透過 Single Sign-On(單一登入)導引至運算雲平台)

客戶管理中心功能介紹(新增「5. 備份服務」說明)

在運算雲 3.0 的客戶管理中心，您可以查詢主機狀態、分析帳單內容、設定監控規則、建立子帳號、進行 VM 備份/還原設定。

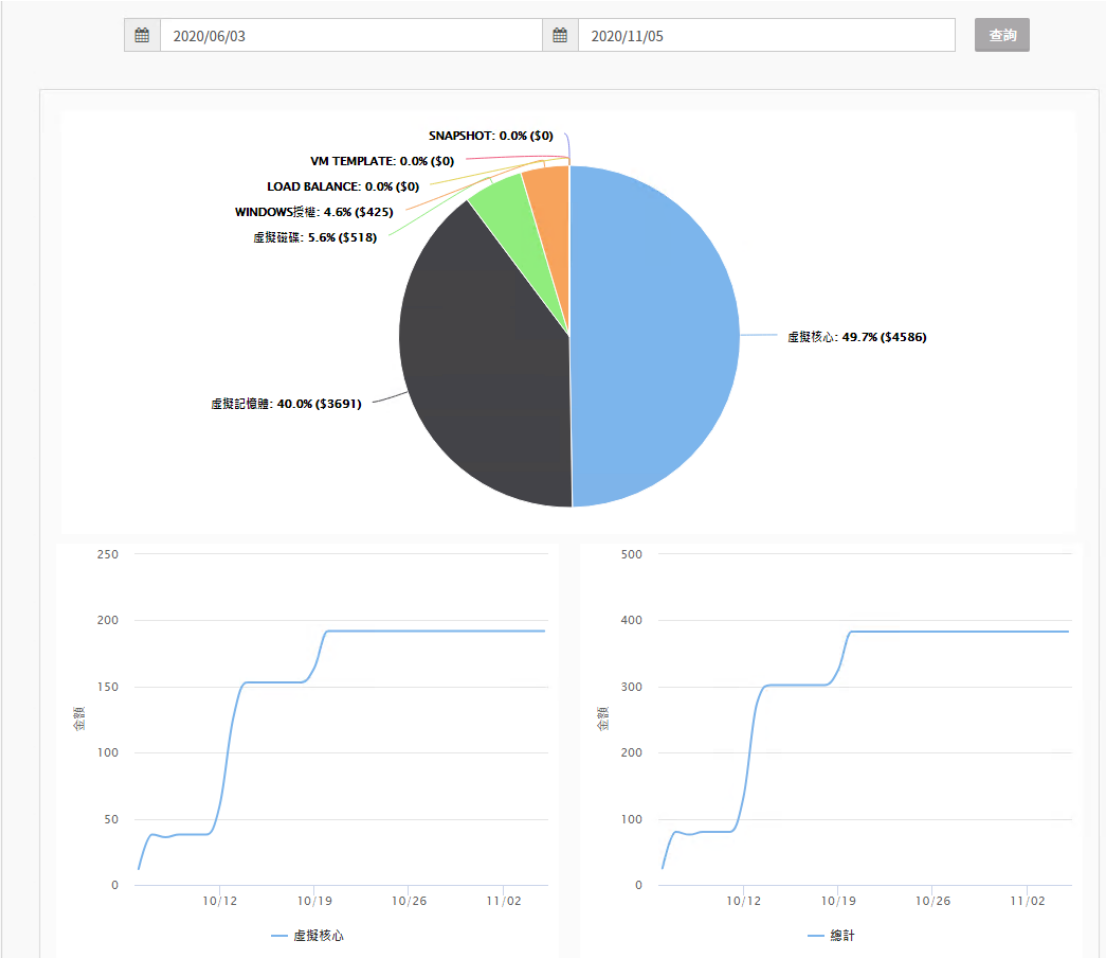
1. 首頁：查看公告、租用資源概況、帳單概況(尚不支援備份服務的費用預估)

2. 查詢：查詢特定 VAPP、特定主機使用狀態

3. 帳單分析：針對總體資源與細項產品，可查詢期間的過去使用明細、未來使用量預估，與設置費用預估告警，包含以下用量查詢與費用告警功能
(尚不支援「備份服務」的費用預估，將於未來優化加入)

(1) 每日使用量預估費用查詢

上方為一段時間內的各項預估費用的統計圖表，使用指定日期區間進行查詢一段時間內的各項預估費用組成百分比統計圖表，以及每個單項服務在這段時間內產生的預估費用曲線圖。畫面下方為最近七天的「使用明細」，以表格條列方式列出各收費項目的預估費用值，計費單位欄位顯示即為該產品牌價，使用明細單項單日所產生的費用除網路費用為流量制計費，其它各項為計時制計費，用戶可使用該表格右上的方向 icon 切換至前七天使用明細表格。



使用明細

類型	計費單位	2020/11/03	2020/11/04	2020/11/05	2020/11/06	2020/11/07	2020/11/08	2020/11/09
虛擬核心(VCORE)	$0.8/core	$192	$192	$192	$192	$192	$192	$192
虛擬記憶體(VRAM)	$0.4/GB	$153	$153	$153	$153	$153	$153	$153
虛擬磁碟(VDISK)	$0.0056/GB	$21	$21	$21	$21	$21	$21	$21
Windows授權(WIN_LICENSE)	$0.73/份	$17	$17	$17	$17	$17	$17	$17
Snapshot服務(SNAPSHOT)	$0.0056/GB	$0	$0	$0	$0	$0	$0	$0
Template服務(VM_TEMPLATE)	$0.0056/GB	$0	$0	$0	$0	$0	$0	$0
Load Balance服務(LB)	$0.4/IP	$0	$0	$0	$0	$0	$0	$0
網路傳輸(NETWORK)	$3/GB	$0	$0	$0	$0	$0	$0	$0
總計		$383	$383	$383	$383	$383	$383	$383

*註1: 使用明細計算收費金額僅以官網訂價做為計算基礎，不包含業務折扣的計算，計算金額僅做參考，實際收費金額請依每月紙本帳單為主
*註2: 網路傳輸為流量制收費，其它項目為計時制收費，例如虛擬核心(VCORE)為每小時每core$0.8元

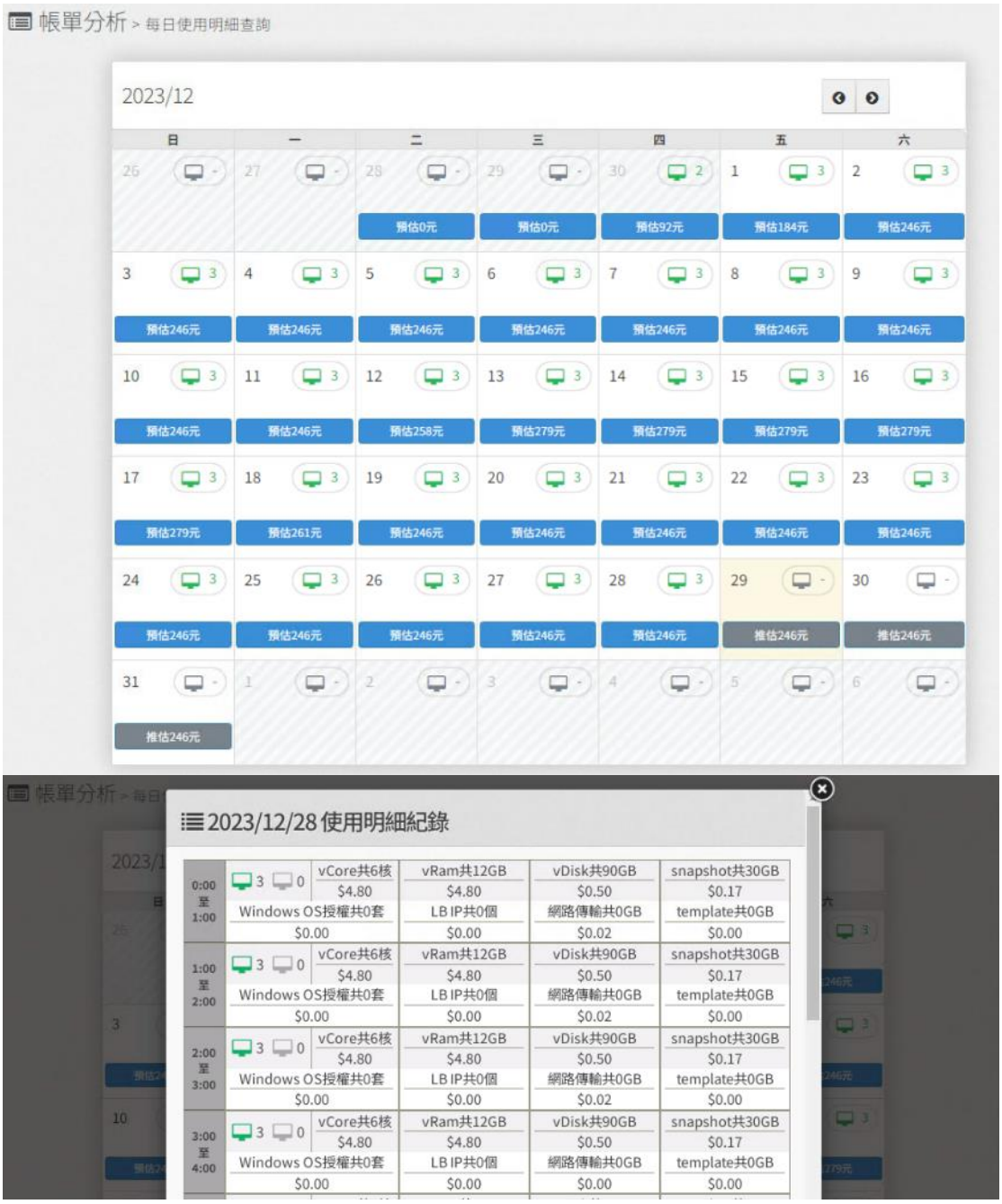
(2) 每月使用量預估費用查詢

畫面功能亦由上下二塊組成，上方由為月份區間的選擇，畫面下方是「使用明細」的表格條列，供用戶比對過去各個月份各項計費項目的預估金額。[1]

(3) 每日使用明細查詢

此功能將「使用明細」記錄以月曆方式來呈現，顯示每日預估金額，並且在每日的電腦圖樣(icon)後方顯示為當日所使用的 VM 數。右上方的方向鍵可切換月份。若在當日的前一日用滑鼠點選電腦圖樣(icon)，則會細部顯示每個小時的使用明細記錄，其中綠色的電腦圖樣為該小時的開機數，灰色的電腦圖樣為該小時的關機數，並將每個收費項目在該小時的計費以表格方式呈現。

[1] 請注意本功能只顯示過去月份的計算資訊，若用戶使用未滿足月，使用本功能時會提示查無資訊。



(4) 預估費用告警設置

此功能供用戶開啟帳單告警功能，監控預估當月帳單金額，當預估金額大於所設置警戒金額，系統將發送 E-Mail 通知。

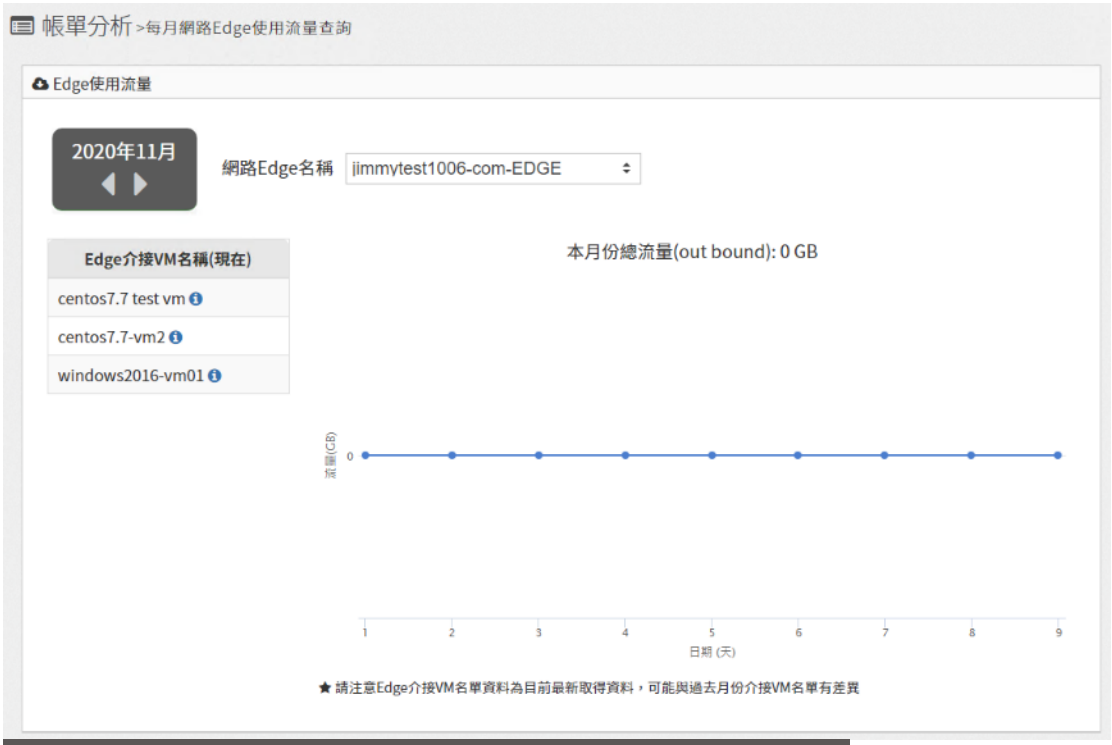
設置警戒金額分二種，一是「每月帳單預估大於多少金額」，這是讓用戶用於設置每月帳單金額的最大值警戒水準，一旦超過就會發送通知，另一個是「到達最大值警戒水準後，每增加多少金額」再額外發送通知。

(5) 每月 VM 使用時數查詢

此功能提供用戶查詢該帳號底下的每台 VM 當月的使用時數，其使用時數包含 VM 開機及關機的加總時數。每筆的使用時數欄位後面的(藍色)圖樣，可展開該 VM 當月的連續開關機時間列表。每筆的 VM 名稱欄位後面的圖樣，可連結到這台 VM 的主機狀態查詢功能。

(6) 每月網路 Edge 使用流量查詢

每個帳號在初始申裝完成時皆會配發一個網路 Edge，在 VCD 建立的 VM 一般情況下皆會介接到這個網路 Edge 進行 Internet 網路交互處理[2]，網路傳輸計費(流量制)，是將每個網路 Edge 對外(out bound)流量累計後計算預估值。此功能供用戶查詢每個月份的每個網路 Edge 所產生的流量，並且列出網路流量曲線圖以及列出與這個網路 Edge 所介接的全部 VM[3]。



[2] 如用戶有需求向台哥大申請多個網路 Edge 建構符合用戶需求的網路架構，請聯繫業務窗口

[3] 請注意介接 VM 資料為目前(現在)的最新資料，不會列出過去的資訊

4. 監控：設定監控標的、規則、通知人員以監控機器使用狀態，與查詢過去告警紀錄。

   此功能可以列出選取的 VAPP 中的全部 VM，用戶可以選取某個 VM 將之標記為「開啟監控」的 VM，只有被標記為「開啟監控」的 VM 在後續的監控設定中才會生效 VAPP。

   (1) 監控標的總覽

   (2) 監控規則設定

   加入監控規則說明方法

   (A)選取監控的 VM、監控指標以及設定比對監控指標的百分比

   (B)監控規則持續符合條件持續通知預設為每 5 分鐘，此項是預設勾選的，若把勾選拿掉指的是只有在最初比對到告警值會發告警

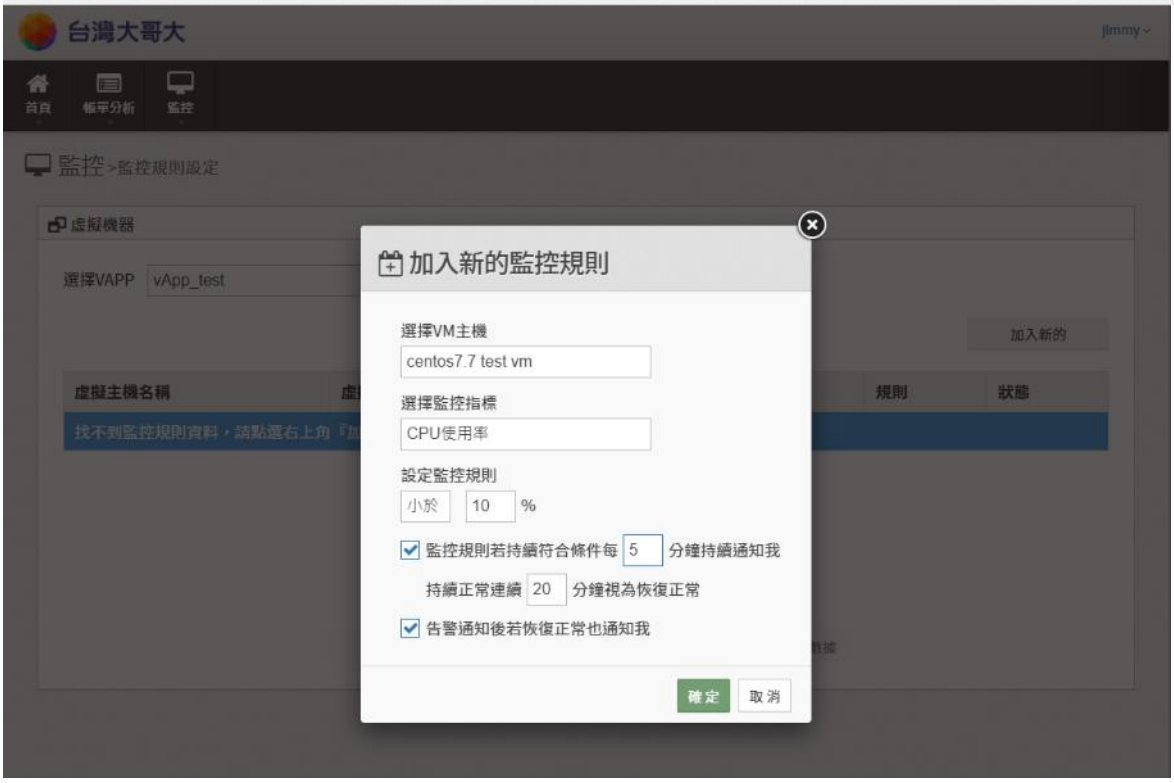
   (C)判斷恢復正常持續值預設為 20 分鐘，此值可依用戶需求修改

   (D)告警恢復正常也通知的這項預設也是勾選的，用戶也可以拿掉勾選，即恢復正常不會發出通知

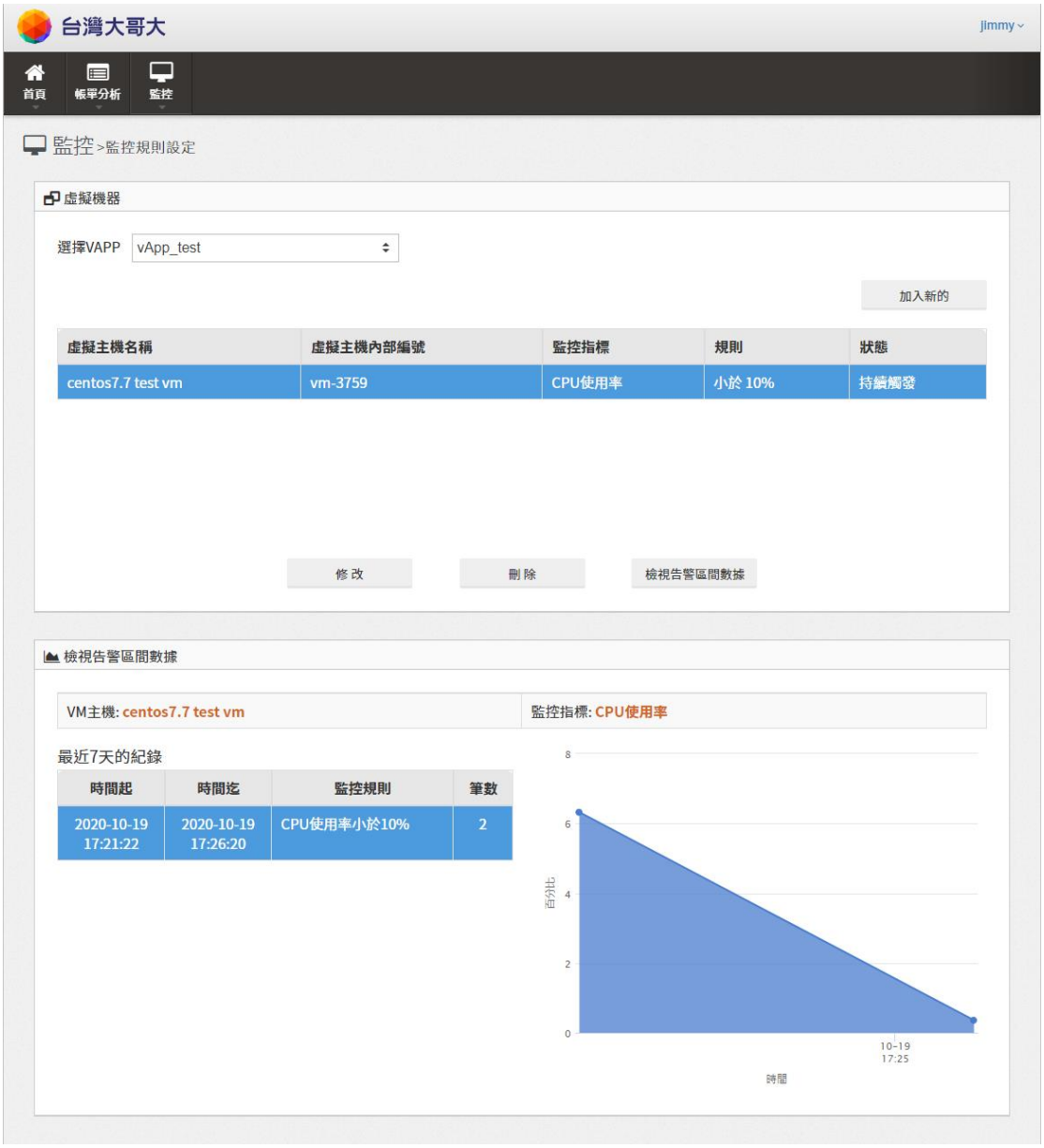
   以上「新的監控規則」設定完成後，即會產生在列表上，並且從狀態欄文字如「監控中」即表示監控行為已作用，若監控到符合告警設定值就會發送告警通知[4]。 VM 加入監控後會出現「檢視告警區間數據」按鈕，若有告警狀

[4] VM 若設定監控規則後有關機行為，監控發現也會發出通知給用戶，待重新開機完也會隨即返

態產生可在點選這個按鈕後看到每個偵測到的告警時段的歷史資訊

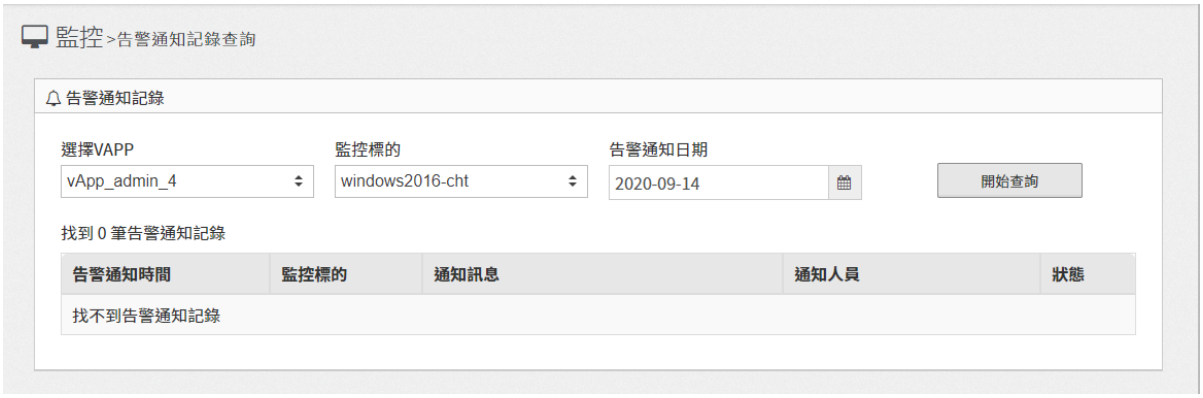


回監控狀態



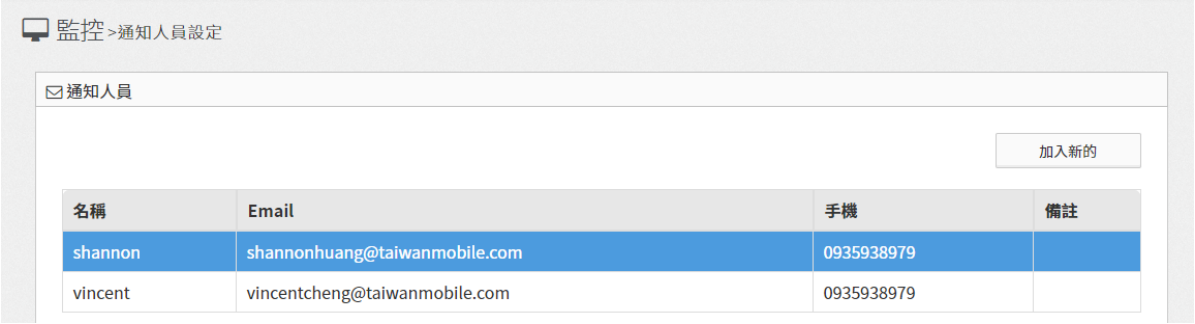
(3) 告警通知記錄查詢

選擇 VAPP、監控標的(VM)及通知日期後按查詢按鈕，可列出該日通知文字訊息。



(4) 通知人員設定

加入用戶通知人員，用於監控標的總覽中針對各別 VM 設定通知人員，並且有修改及刪除等功能。



(5) 網路流量即時監控

此功能可設定針對網路流量的即時監控規則，可以查詢當日與 30 日內的流量資料。

5. 備份還原：可針對客戶建置的 VM，進行備份與還原設定。

(1)完整流程說明：

用戶可在客戶管理中心提出需求 (單獨備份、排程備份、還原虛擬主機、刪除還原點、刪除備份排程)完成需求指令，並可追蹤查詢指令狀態和歷史活動紀錄。

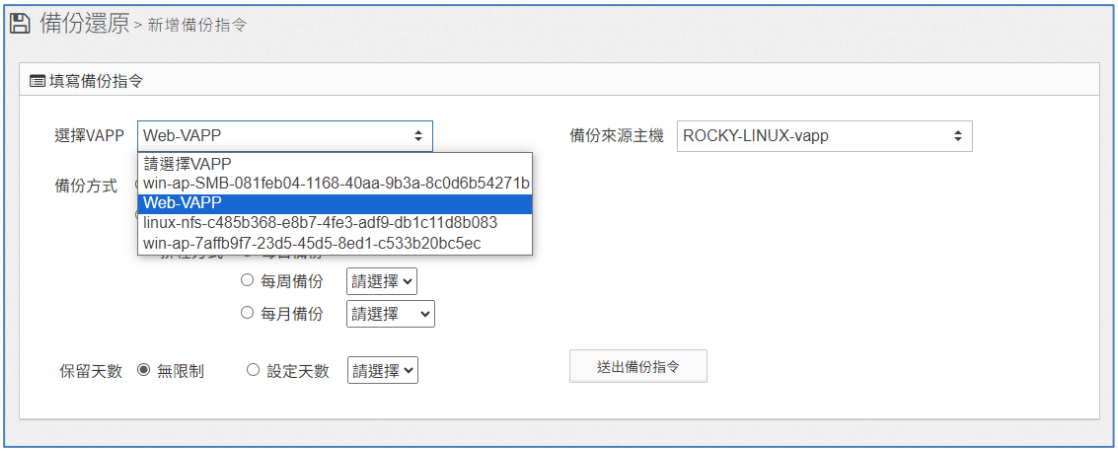
(2)單獨備份流程：

用戶在「新增備份指令」選擇單獨備份提出備份需求，，選擇一台主機作為備份來源，並設定備份檔保留１０天。用戶到「指令記錄查詢」和「備份記錄查詢」可以觀察到變化。

■ 在客戶管理中心頁面點選備份還原>新增備份指令

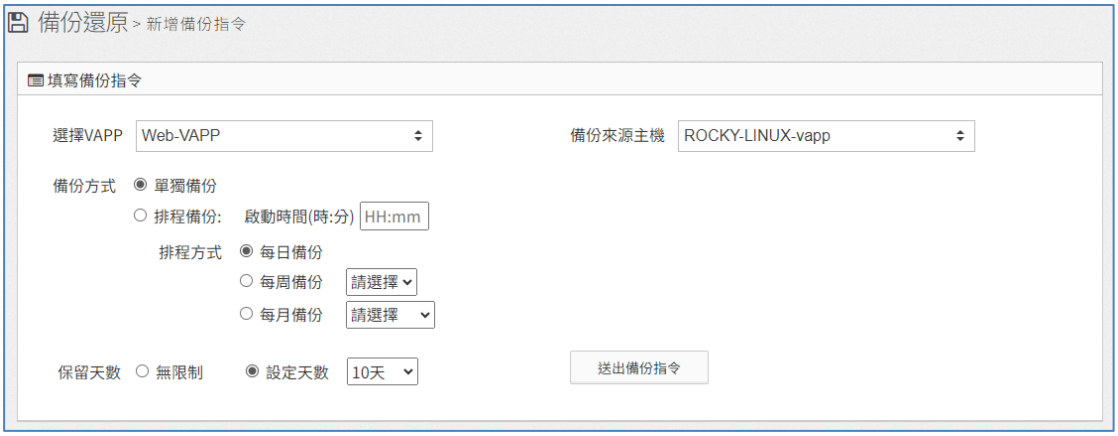
■ 選擇 VAPP、備份來源主機

(以單一虛擬機為單位，暫時不提供 VAPP 整包備份)



■ 選擇單獨備份、設定備份檔保留１０天，送出備份指令

(單獨備份允許選擇無限制的保留天數)



■ 詢問是否依目前的備份需求做送出

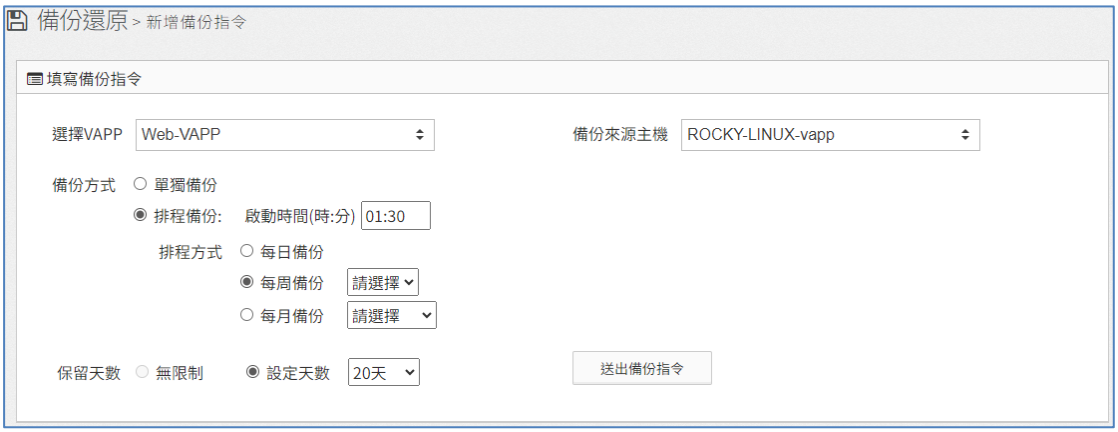
(3)排程備份流程

用戶在「新增備份指令」選擇排程備份提出備份需求，選擇一台主機作為備份來源，設定備份啟動時間 01:30、備份檔保留 20 天。用戶到「指令記錄查詢」、「備份記錄查詢」、「排程設定列表」可以觀察到變化。

■ 在客戶管理中心頁面點選備份還原>新增備份指令

■ 選擇 VAPP、備份來源主機

選擇排程備份、設定備份啟動時間(時間間隔為 5 分鐘)、備份檔保留天數，送出備份指令。



※ 啟動時間：請選擇 00:00~15:00 區間

因 15:00~24:00 為備份系統維護時段，所以無法在此時段排訂排程備份作

業。

※ 排程週期說明

每週備份：星期一 ~ 星期日

每月備份：每月 1 號 ~ 28 號

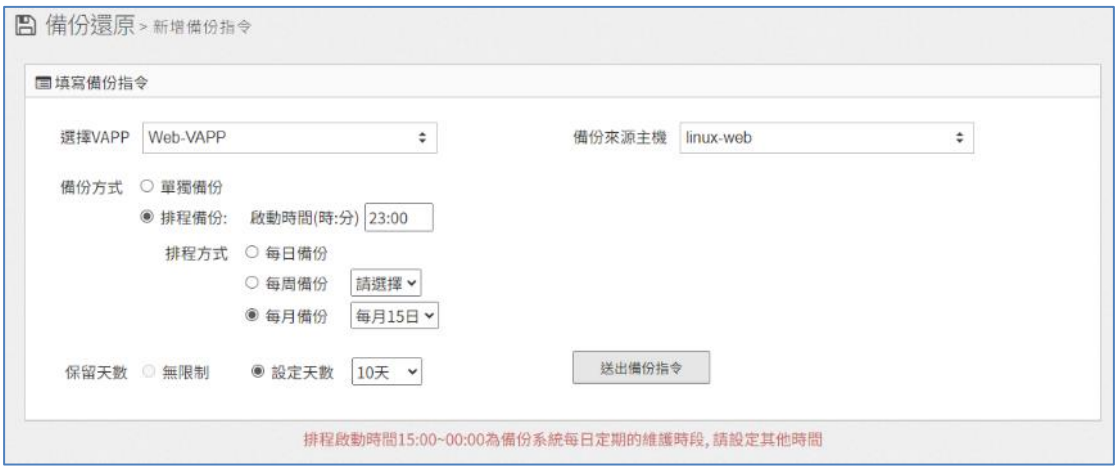
※ 排程備份，不支援無限制的保留天數，但有 1~90 天的選擇區間

■ 詢問是否依目前的備份需求做送出

(4)備份系統維護時段

為提供用戶更好服務品質以及備份檔的完整性，本備份系統於每日 15:00~00:00 為維護時段，該時段無法排訂排程備份，若在此時段使用單獨備份會於維護結束時，自動接續完成單獨備份作業。

■ 假若新增 15:00~00:00 範圍區間的排程備份，會顯示「排程啟動時間 15:00~00:00 為備份系統每日定期的維護時段，請設定其他時間」



■ 單獨備份則顯示

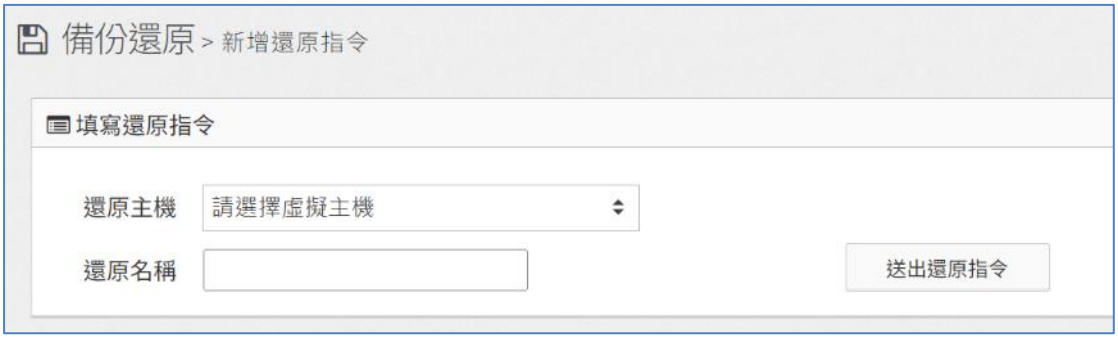
「目前備份服務正在進行備份系統每日定期的維護處理，系統將等待維護結束自動進行備份。」

(5)還原虛擬機流程

用戶在「新增還原指令」選擇需要還原的主機和要還原的還原點，採用新建虛擬主機的方式還原，所以需輸入新虛擬主機的名稱。用戶到「指令記錄查詢」可以觀察到變化。

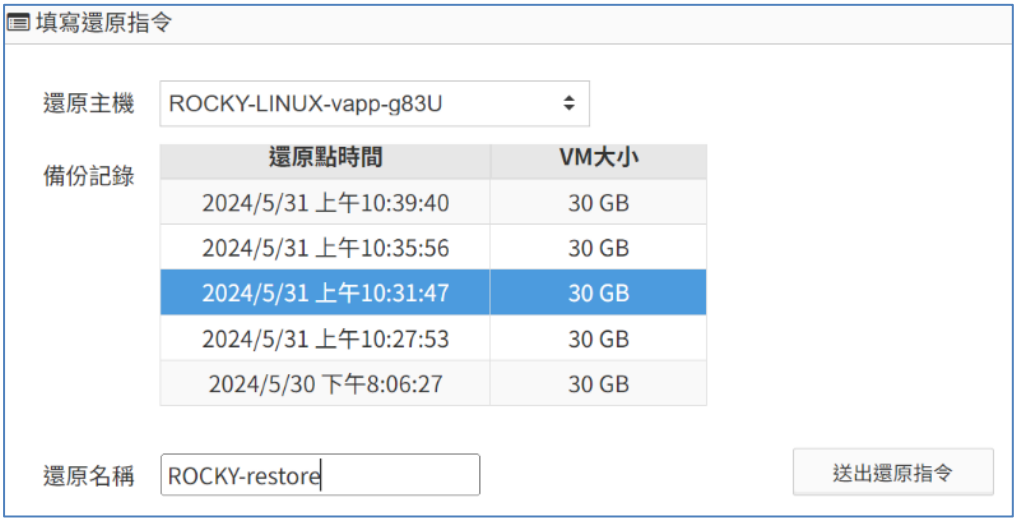
■ 在客戶管理中心頁面點選備份還原>新增還原指令

■ 挑選還原主機，這是以已經成功備份為列表



■ 選擇要還原到哪個時間點

還原採新增虛擬機的方式進行還原，所以還需填寫新主機名稱



■ 確認動作，無誤按確定即可

※重要提醒：還原指令送出後，將新增一台還原的虛擬機，屆時將會有 VM 資源的用量產生，並產生流量費用，還請客戶留意。

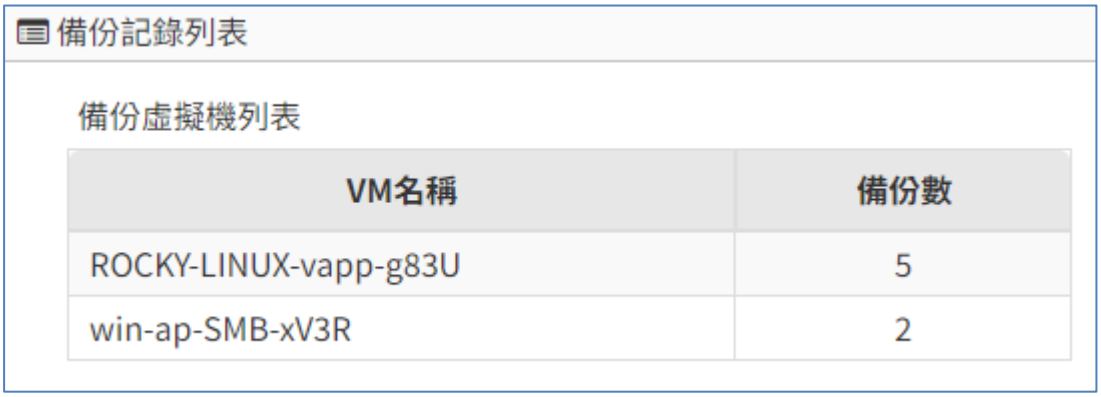
(6)刪除還原點流程

用戶在「備份記錄查詢」查詢所有虛擬機的備份數，再挑選要刪除的還原點進行申請。

用戶到「指令記錄查詢」可以觀察到變化。

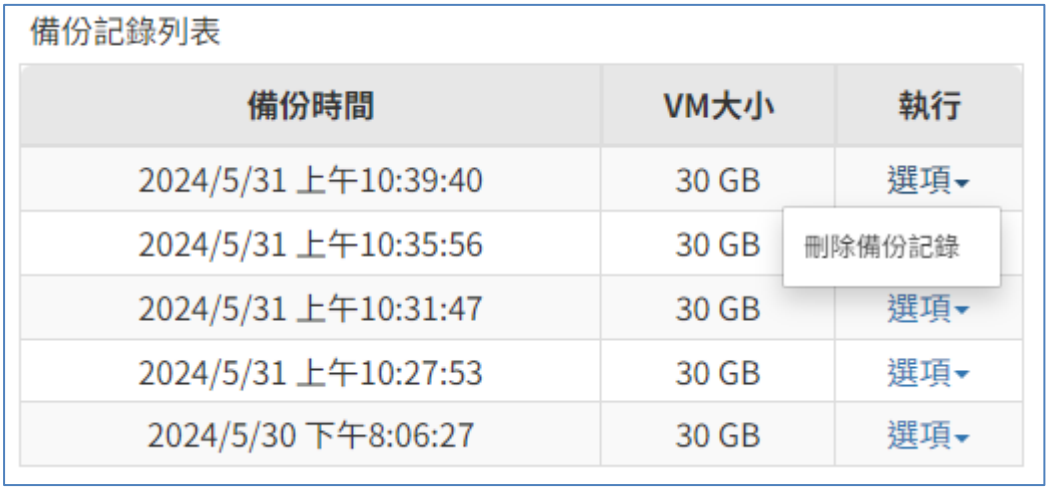
■ 在客戶管理中心頁面點選備份還原>備份記錄查

■ 顯示已備份的虛擬機和備份數量



■ 選定某一虛擬機可以展開詳細的還原點資訊

■ 可以針對其中一筆還原點進行刪除，以減少備份數量總額



■ 確認動作，無誤按確定即可

(7)刪除備份排程

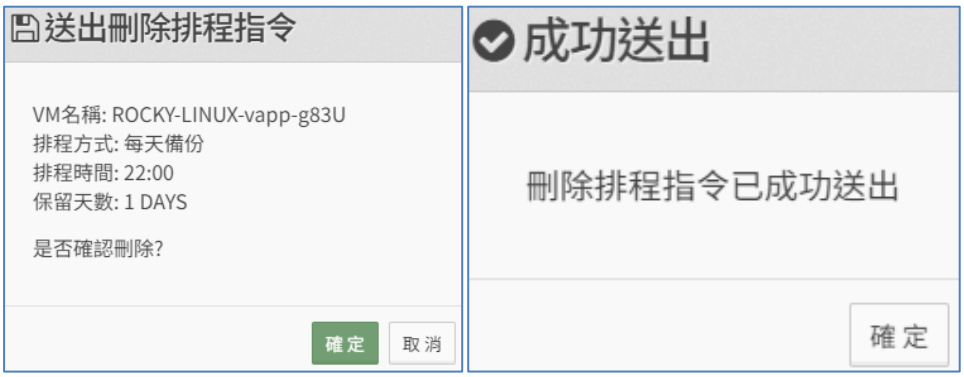
用戶在「排程設定列表」查詢所有備份排程的清單，挑選要刪除的排程進行申請。用戶到「指令記錄查詢」可以觀察到變化。

■ 在客戶管理中心頁面點選備份還原>排程設定列表

■ 顯示已設定好的排程設定

■ 可針對排程執行刪除

■ 確認動作，無誤按確定即可



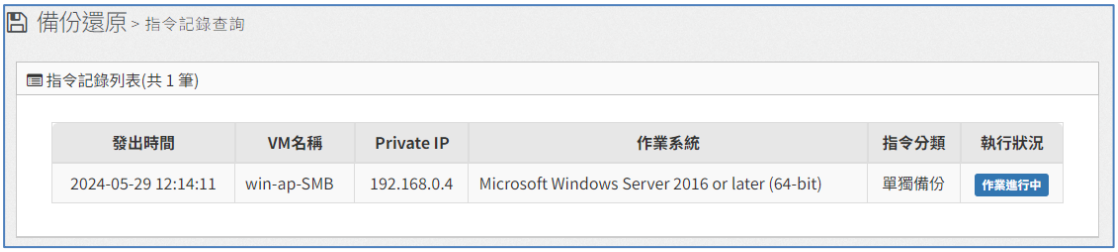
(8)查看指令記錄狀態流程

用戶在「指令記錄查詢」可以查詢所有歷史指令記錄和目前指令進度。

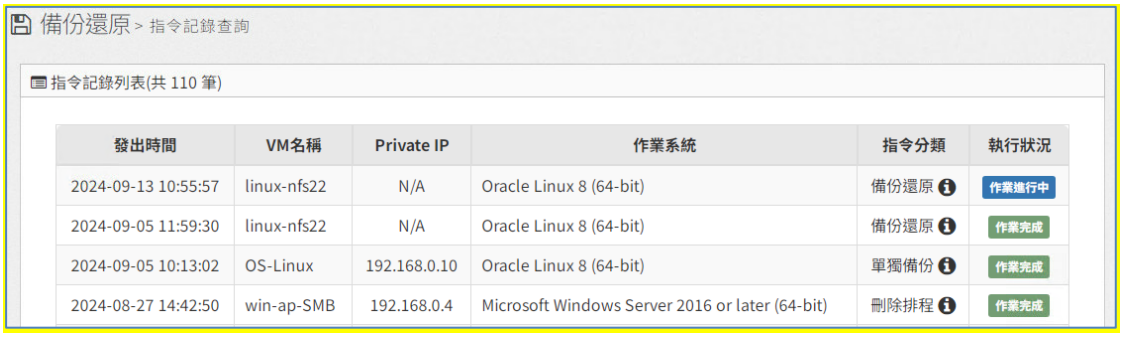
■ 在客戶管理中心頁面點選備份還原>指令記錄查詢

■ 此頁面可以看到不同的指令分類紀錄的狀態

執行狀況分為作業進行中(已送出指令，備份作業進行中)



■ 作業完成(該項作業已完成)



(8)查看活動紀錄流程

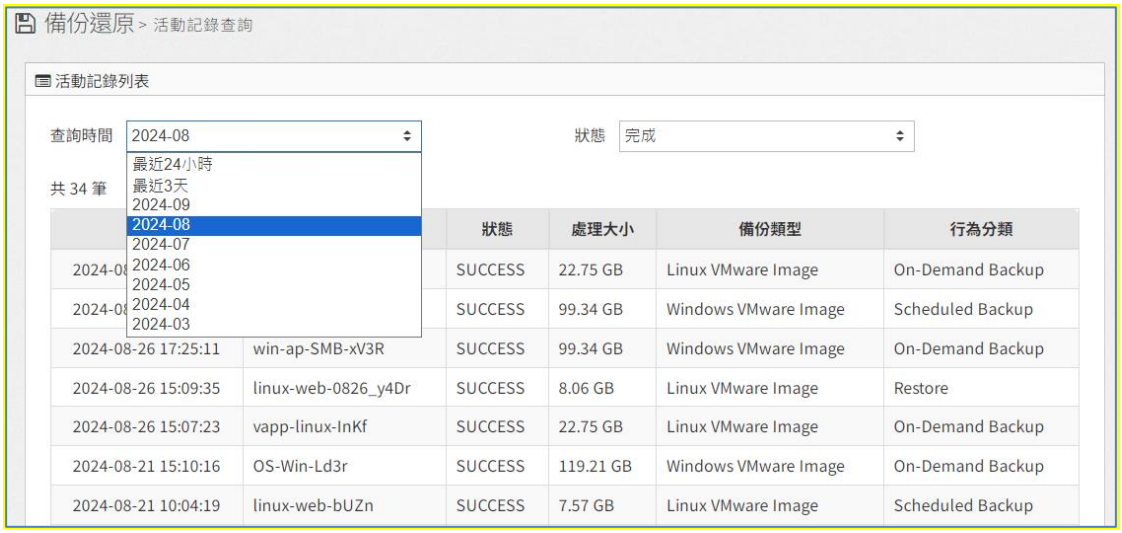
用戶在「活動記錄查詢」可以查看虛擬機的備份及歷史還原記錄。

■ 在客戶管理中心頁面點選備份還原>活動記錄查詢

■ 可以依需求篩選近期 24 小時、3 天或各別月份來查看

活動行為分類可分別為：

1. On-Demand Backup：一次性單獨備份
2. Scheduled Backup：固定週期排程備份
3. Restore：還原虛擬機



(9)修改備份排程內容

目前暫無無提供修改排程功能。

暫時解決方式為「新增備份排程」配合「刪除備份排程」達到修改備份排程的需求

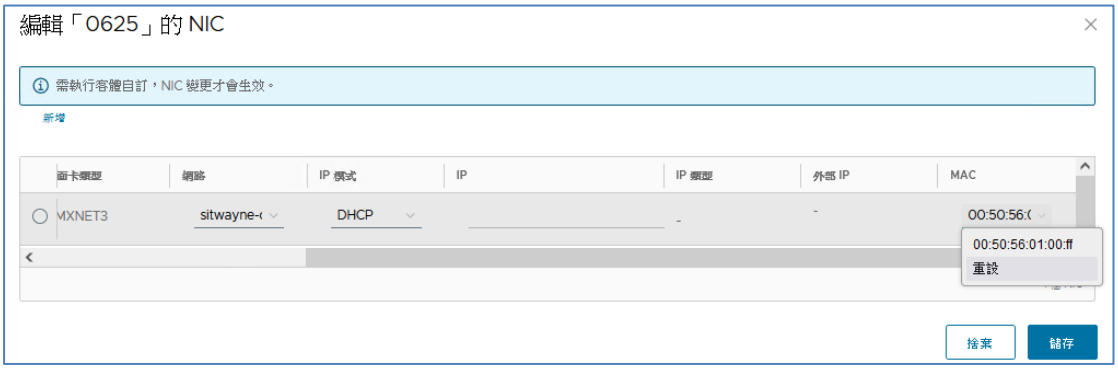
(10)開啟還原後的新虛擬機

因本備份服務是將虛擬機進行完整性的備份，後續還原新虛擬機參數會跟舊虛擬機相同，若遇到以下問題，可使用兩種方式進行排除：

1. 關閉舊虛擬機。
2. 新虛擬機 MAC 重設。

到新虛擬機的 NIC，點選編輯

重設 MAC，儲存



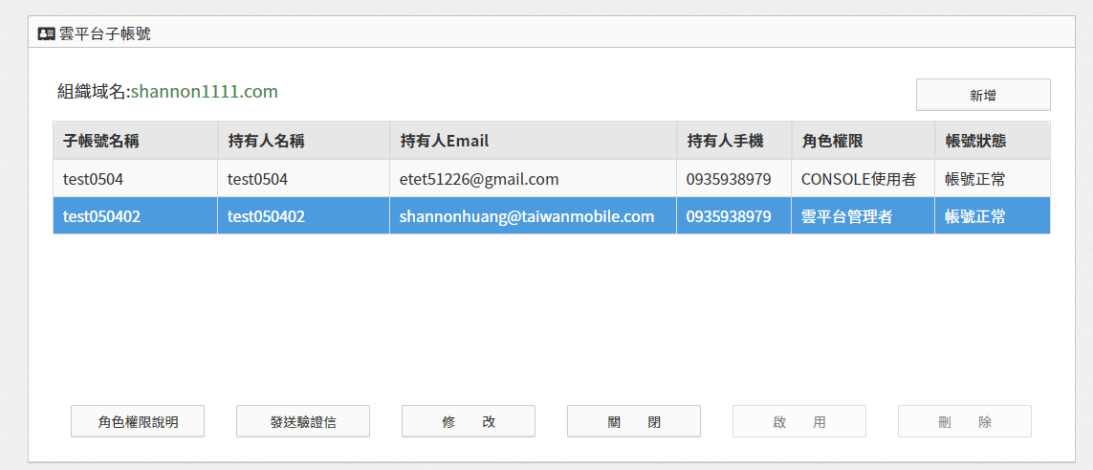
6. 設定：設定雲平台子帳號

(1)主帳號可以設定 2 種子帳號：

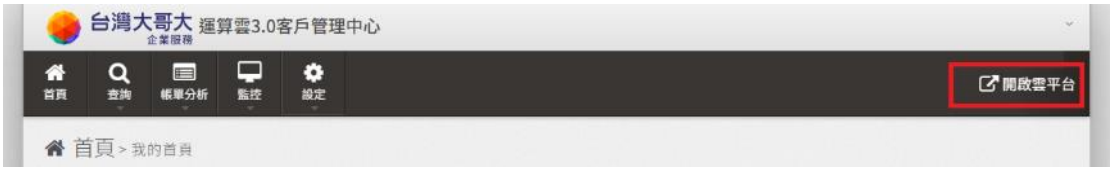
雲平台管理者：與主帳號相同有雲平台的最高權限，可看見不同帳號所擁有的資源，並且能夠進行所需權限的各項工作，但僅有主帳號才能進入客戶管理中心。

CONSOLE 使用者：可看見不同帳號所擁有的資源，但僅能進行虛擬機器的遠端 console 操作，除了 console 操作之外其它的工作可能會出現權限不足的錯誤訊息，同時也是不能登入客戶管理中心。

(2)主帳號可新增、修改、刪除[5]、關閉、啟用子帳號權限，以可於此設定發送驗證信



(3)點選[開啟雲平台後]，自動透過 Single Sign-On(單一登入)導引至運算雲平台



(4)子帳號沿用主帳號設定之多因子驗證，當主帳號被停用時、子帳號亦會停用

(5)子帳號若密碼輸入錯誤而被鎖定，主帳號可循以下方式解除鎖定「登入使用者管理中心>設定>雲平台子帳號設定>啟用」，或子帳號使用者 從使用者管理中心登入頁面的點選「重置密碼」功能，密碼重置後帳號將重新啟用。

[5] 子帳號狀態必須是關閉狀態才可以刪除

雲平台首頁功能介紹

首頁可即時查看資源使用狀況與各種管理功能

網路：列出網路與 Edge 閘道資訊並修改相關設定。

1. 資料中心：觀看 CPU、記憶體、儲存區資源使用量
2. 應用程式：列出、調整 vApp。
3. 網路：列出網路與 Edge 閘道資訊並修改相關設定。
4. 內容中樞：管理目錄與 vApp 範本。
5. 程式庫：列出 vApp 範本、可掛載 ISO 清單
6. 管理：可修改組織管理員帳號內容
7. 監視器：可以看到工作紀錄、事件紀錄。
8. xxxx.com-VDC：左下方可以看到組織 VDC，點進去可以看到網路的相關設定。

4.vApp 管理

啟動 vApp

開啟電源，會將 vApp 中尚未開啟電源的所有虛擬機器電源開啟。

1. 按一下**動作**。
2. 在選項中，按一下**電源**。
3. 在選項中，選取**啟動**。

停止 vApp

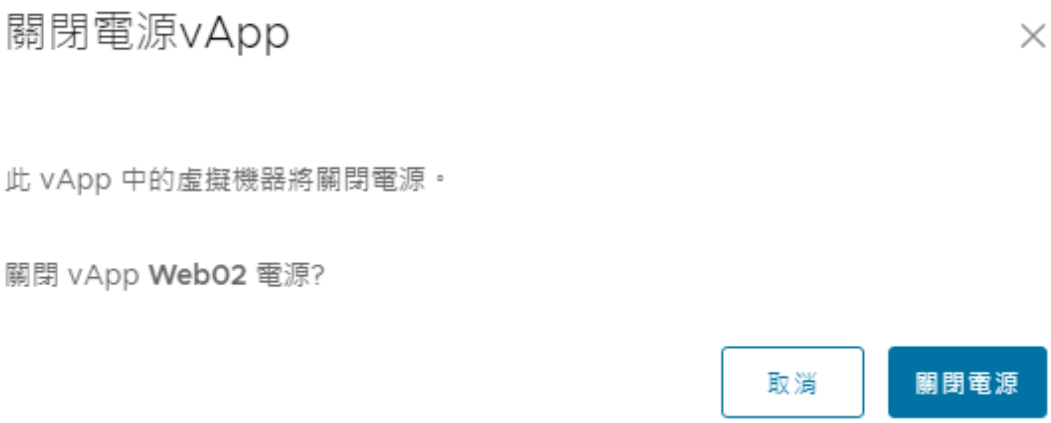
停止 vApp，會將 vApp 中所有虛擬機器的電源關閉。

您可以在 vApp 內容頁面中指定，停止 vApp 會將虛擬機器的電源關閉。

先決條件：必須啟動 vApp。

1. 按一下**動作**。
2. 在下方選項中，按一下**電源**。
3. 在選項中，選取**關閉電源**。

4. 按一下**關閉電源**。



暫止 vApp

您可以暫止 vApp，以儲存其目前狀態。

先決條件：vApp 執行狀態。

1. 按一下**動作**。
2. 在下方選項中，按一下**電源**。
3. 在選項中，選取**暫停**。

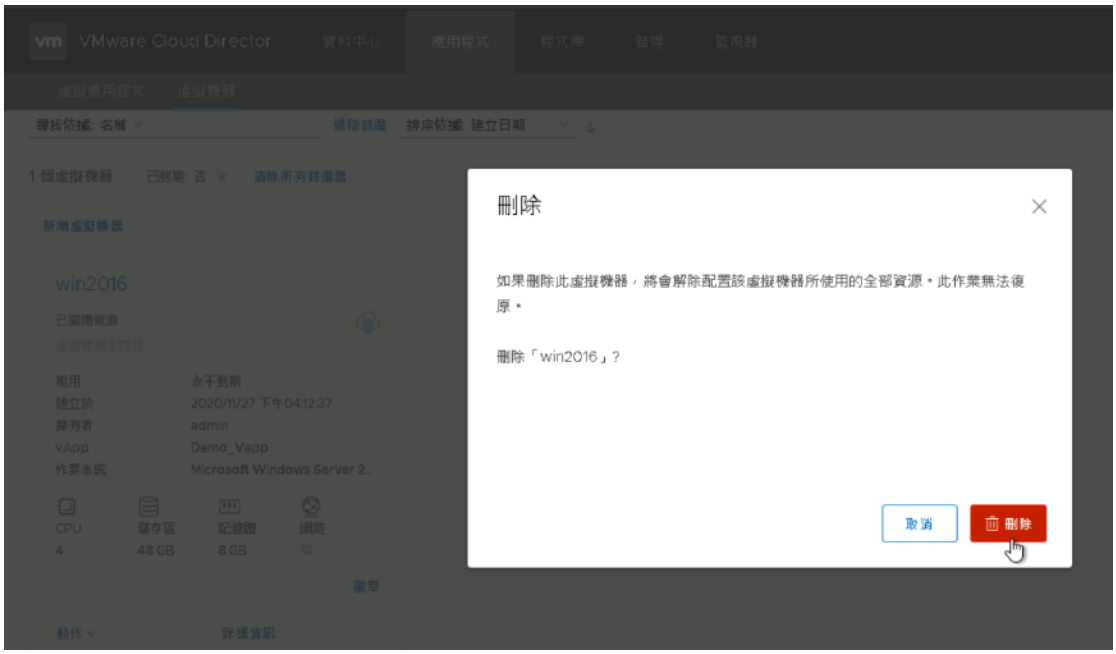
移除 vApp 中的虛擬機器

您可以移除 vApp 中的虛擬機器。

先決條件：必須先將虛擬機器電源關閉。

1. 按一下**應用程式**。
2. 在下方選項中，按一下**虛擬機器**。
3. 點選 vApp 左下角**動作**，然後選取**刪除**。

4. 系統提示刪除後無法復原。確定則點**刪除**。



重設 vApp

重設虛擬機器會清除狀態(記憶體、快取等)，但 vApp 和虛擬機器仍然會繼續執行。

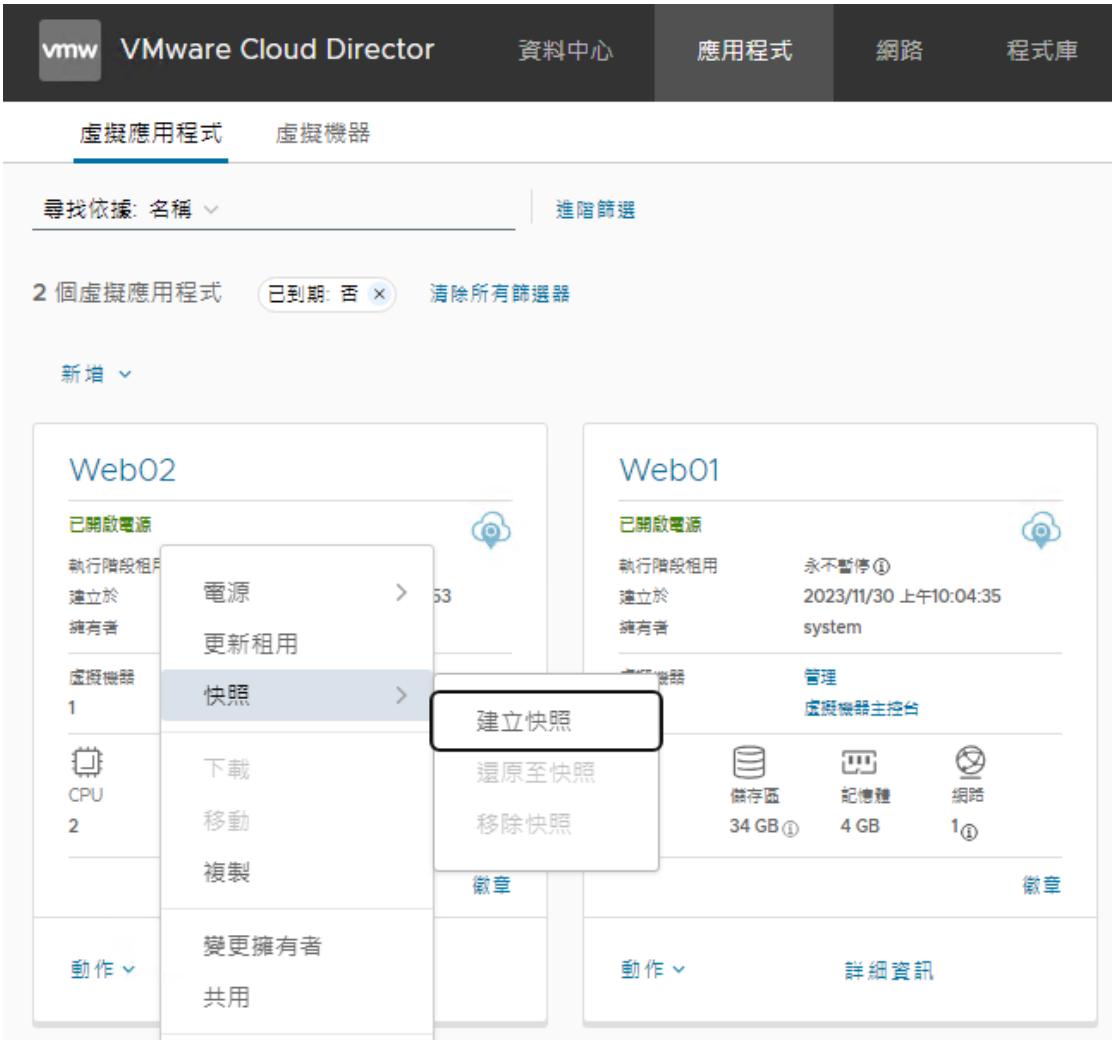
先決條件：已啟動您的 vApp，並已開啟虛擬機器的電源。

1. 按一下**動作**。
2. 在下方選項中，按一下**電源**。
3. 在選項中，選取**重設**。

建立 vApp 快照

vApp 中所有虛擬機器的快照。拍攝快照後，您可以將 vApp 內所有虛擬機器還原至最近的快照。

1. 按一下**動作**。
2. 在下方選項中，按一下**快照**。
3. 在選項中，選取**建立快照**。

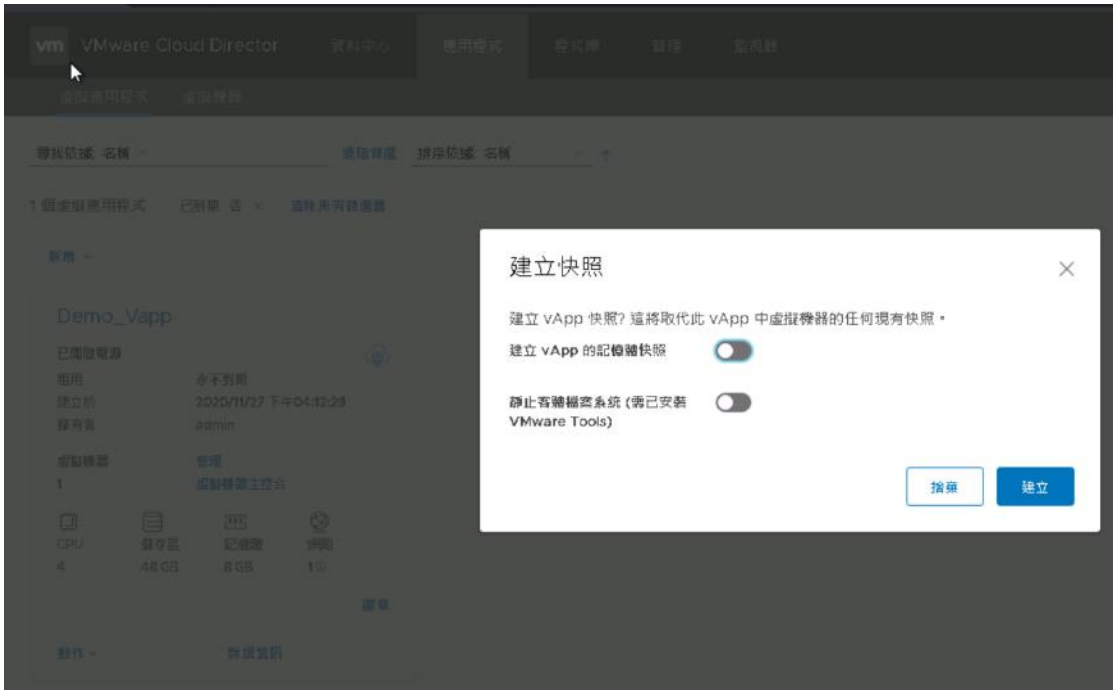


4. 依據您的需求，可選擇的選項有:

A. 建立 VApp 的記憶體快照:保留現有 VApp 記憶體狀態，建立快照。

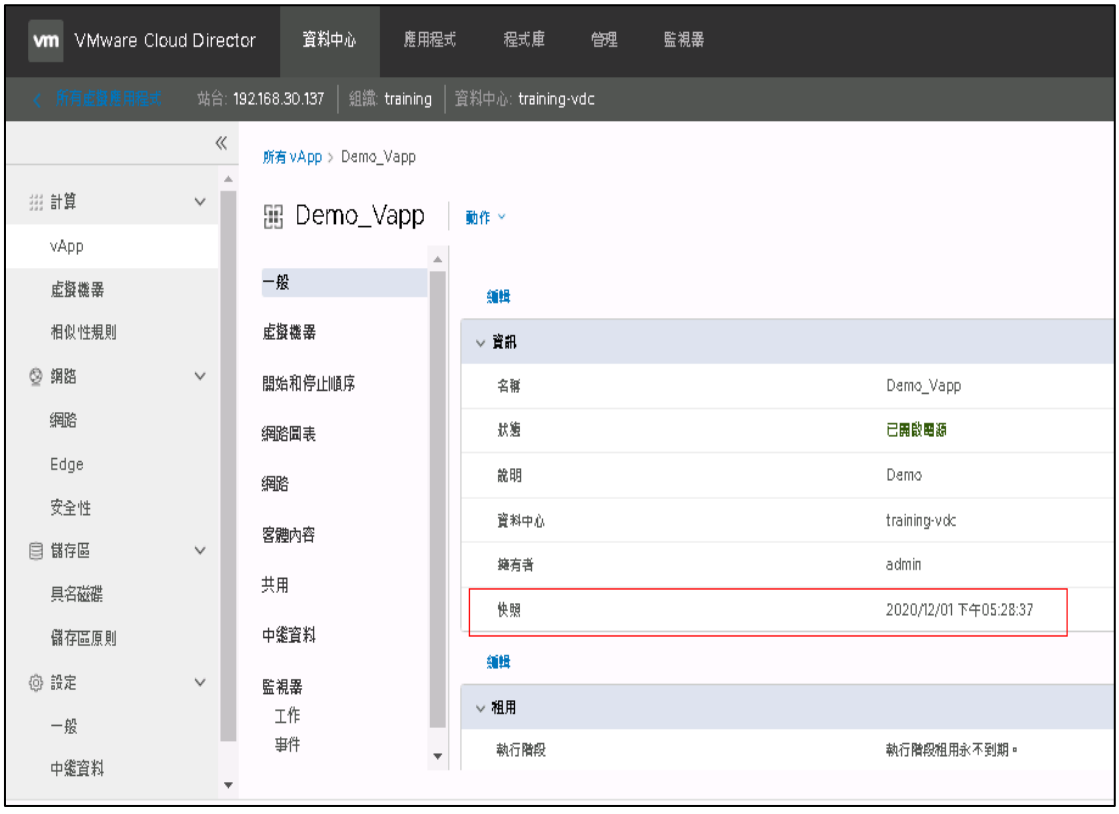
B. 靜止客體檔案系統：藉由透 VMware Tools 工具來暫時停止虛擬主機內的檔案系統，讓作業系統可以將相關的緩衝資料和虛擬記憶體中的快取資料，順利地寫回虛擬磁碟內，保持資料的一致性與可用性，建立快照。(VM 需已安裝 VMware Tools)

選擇完成後，選取**建立**



建立完成後，可點**詳細資訊**，由**一般** - **資訊**下，確認快照時間。


VMware Cloud Director
資料中心
應用程式
程式庫
管理
監視器
虛擬應用程式
虛擬機器
1 個虛擬應用程式
已到期: 否
清除所有篩選器
新增
Demo_Vapp
已開啟電源
租用
永不到期
建立於
2020/11/27 下午04:12:29
擁有者
admin
虛擬機器
管理
虛擬機器主控台
CPU
儲存區
記憶體
網路
4
88 GB
8 GB
1
動作
詳細資訊


VMware Cloud Director
資料中心
應用程式
程式庫
管理
監視器
站台: 192.168.30.137
組織: training
資料中心: training-vdc
所有 vApp > Demo_Vapp
Demo_Vapp
動作
計算
vApp
虛擬機器
相似性規則
網路
網路
Edge
安全性
儲存區
具名磁碟
儲存區原則
設定
一般
中繼資料
一般
虛擬機器
開始和停止順序
網路圖表
網路
客體內容
共用
中繼資料
監視器
工作
事件
編輯
資訊
名稱
Demo_Vapp
狀態
已開啟電源
說明
Demo
資料中心
training-vdc
擁有者
admin
快照
2020/12/01 下午05:28:37
編輯
租用
執行階段
執行階段租用永不到期。

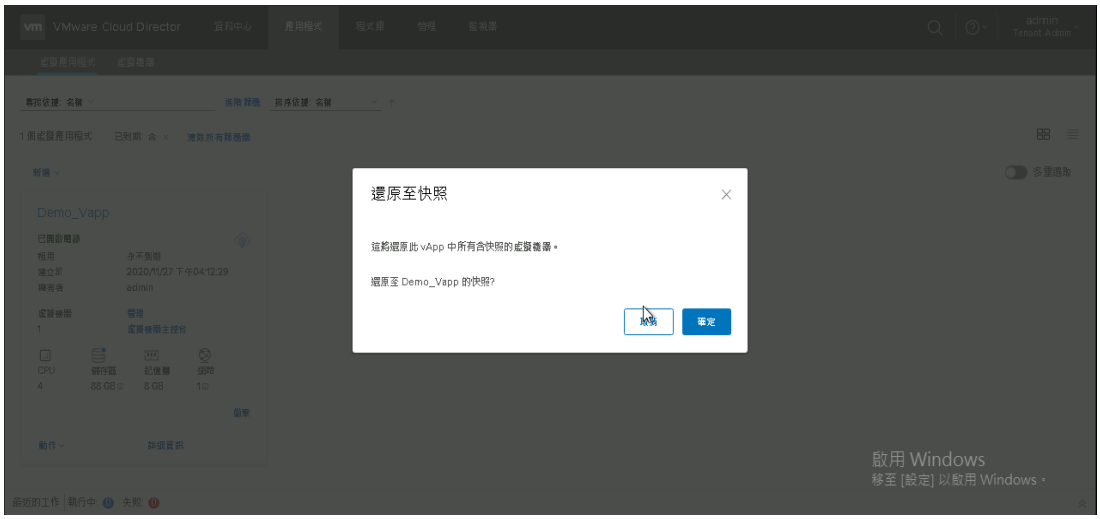
還原 vApp 至快照

您可以將 vApp 內的所有虛擬機器還原至建立 vApp 快照時的當時狀態。

先決條件：vApp 有快照。

1. 按一下**動作**。
2. 在下方選項中，按一下**快照**。
3. 在選項中，選取**還原至快照**。

4. 該操作會還原 vApp 中所有含快照的虛擬機器，確認則按確定。



移除 vApp 快照

您可以將 vApp 內的快照移除。

先決條件：vApp 有建立過快照。

1. 按一下**動作**。
2. 在下方選項中，按一下**快照**。
3. 在選項中，選取**移除快照**。


VMware Cloud Director
資料中心
應用程式
網路
程式庫
虛擬應用程式
虛擬機器
尋找依據: 名稱
進階篩選
2 個虛擬應用程式
已到期: 否
清除所有篩選器
新增
Web02
已開啟電源
執行階段租用
建立於
擁有者
虛擬機器
1
CPU
2
電源
更新租用
快照
下載
移動
複製
變更擁有者
共用
建立快照
還原至快照
移除快照
徽章
動作
Web01
已開啟電源
執行階段租用
永不暫停
建立於
2023/11/30 上午10:04:35
擁有者
system
管理
虛擬機器主控台
儲存區
34 GB
記憶體
4 GB
網路
1
徽章
動作
詳細資訊

新增 vApp 範本

一、前置準備

1. 範本 VM 準備好後請點選該虛擬主機 > 動作 > 電源 > 關閉電源。

2. 點選動作 > 媒體 > 退出媒體。

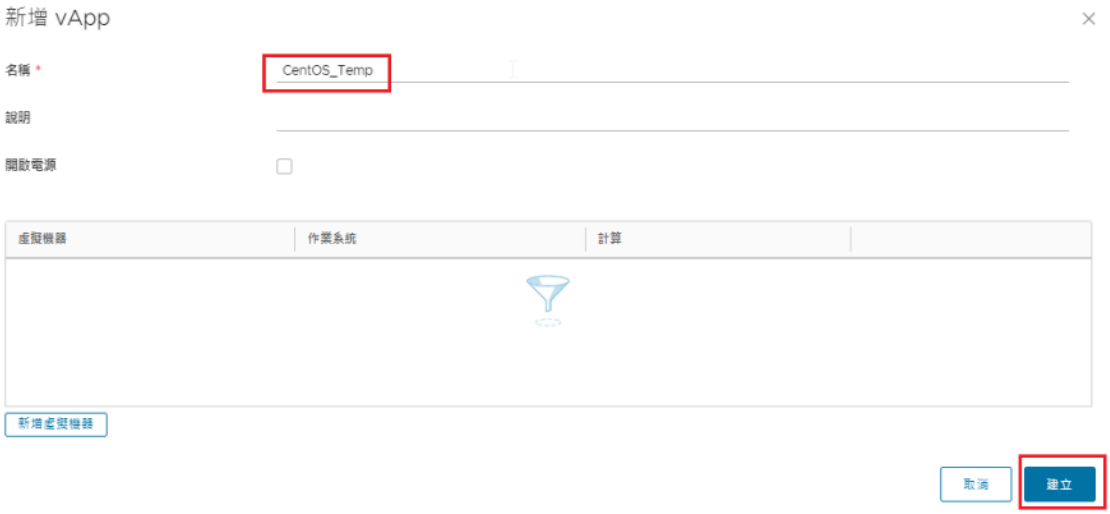
3. 網路設定移除，請點選「詳細資訊」。

4. 點選 NIC > 編輯

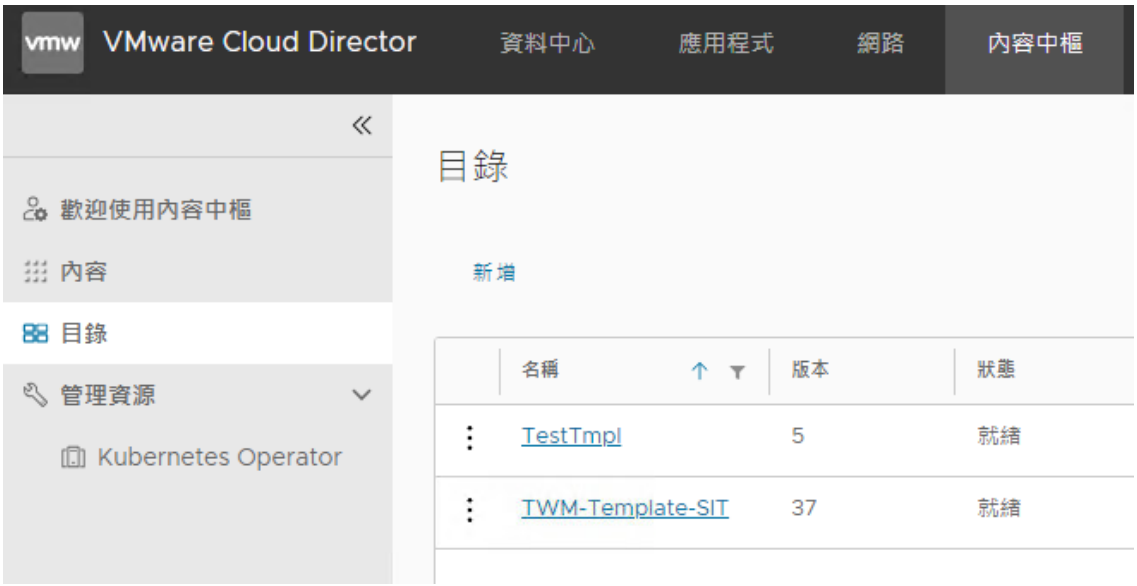
5. 取消已連線的勾選 >網路點選「無」> 儲存。

6. 至 vAPP 頁面，點選新增 vAPP，以建立一個空的打包用 vApp，1 個 vApp 限打包 1 個 VM，請勿打包 1 個以上的 VM。

7. 輸入 vAPP「名稱」，點選「建立」。



8. 到程式庫 >目錄 > 點選「新增」，新增一個打包用目錄。



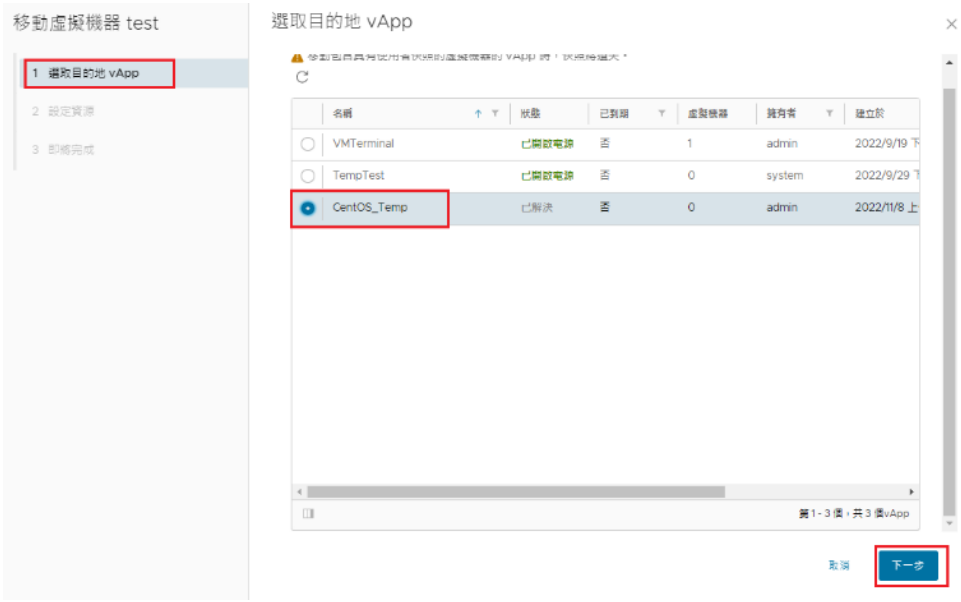
9. 輸入目錄「名稱」 > 確定。

二、範本 VM 打包

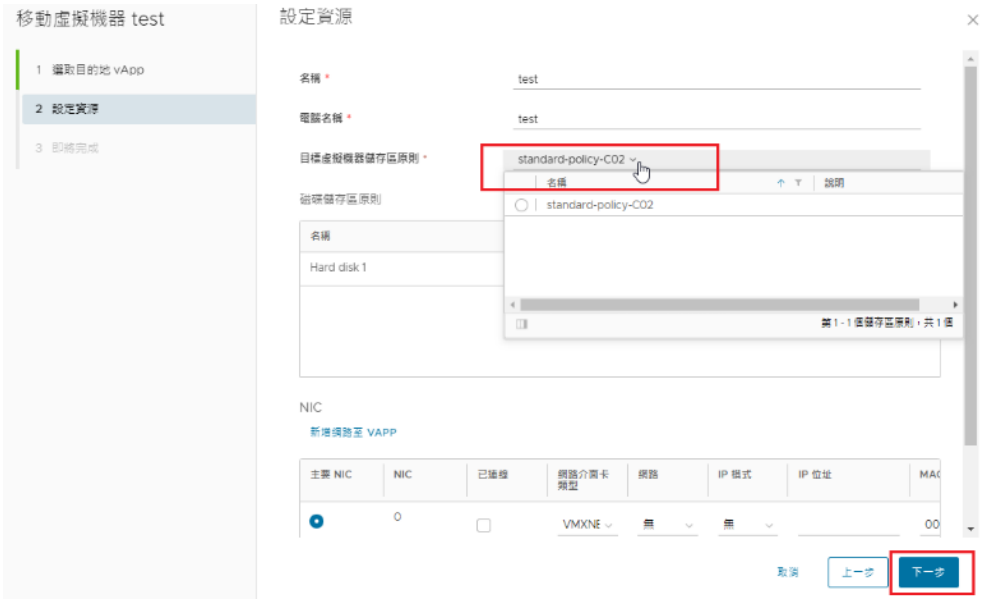
1. 至虛擬主機頁面，針對範本 VM 點選動作 >選擇「移動」或「複製」，

   下圖以移動為例。

2. 點選選取目的地 vAPP > 下一步，請注意需複製到空的 vApp。



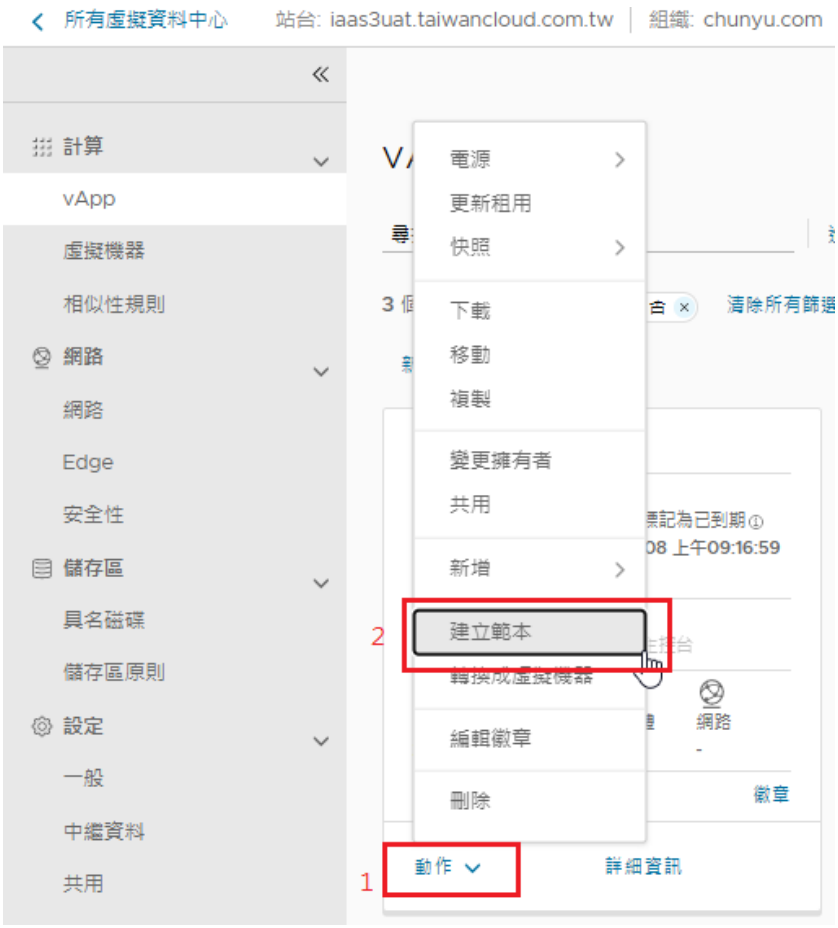
3. 選擇儲存區原則 > 下一步。



4. 點選完成。

5. 至 vApp，此時打包用的 vApp 已內含一個範本 VM。

6. 請選擇動作>建立範本。



7. 選擇之前建立好的”打包用目錄”，名稱自訂，選擇製作相同副本，按確定。

8. 到此打包完成，到內容中樞 > 目錄 > vApp 範本，會看到打包好的 vApp。

下載 vApp 範本

為確保運算雲互通性和可攜性，用戶可自行依下列步驟操作下載客戶所屬之虛擬機映像檔。

1. 點選畫面上方的「內容中樞」。
2. 點選畫面左列的「目錄」>「vApp 範本」。
3. 勾選您要下載的 vApp 範本。
4. 點選「下載」。

5. 點選確定

5.VM 管理

VM 作業系統環境說明

Windows 預設時區為 UTC+8 台北，NTP 伺服器為 time.windows.com。Linux 預設時區為 UTC+8 台北，NTP 伺服器為各 OS 預設設定值，建議依需求調整設定後啟用 NTP 校時。
VM 預設安全性基準，Windows VM 預設已啟用主機安全性原則與內建防火牆功能，並建議依需求開啟並設定 Windows Update 排程定期進行系統更新。而 Linux VM 則建議啟用 selinux 與 iptables 以提升系統整體安全性。若欲強化 VM 作業系統安全性，強烈建議參閱各 VM 作業系統原廠官方安全性指南手冊。另除了 VM 作業系統外，建議由運算雲管理介面，由管理者搭配運算雲防火牆功能設定，提高 VM 存取網際網路之安全性。

VM 作業系統原廠官方安全性指南文件參閱：(以下連結以官方公佈為主)
Windows Security baseline :
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
CentOS OS Protection:
https://wiki.centos.org/HowTos/OS_Protection
Ubuntu Security Guide:
https://ubuntu.com/security/compliance-automation
Rocky Linux Security
https://docs.rockylinux.org/guides/security/learning_selinux/
Oracle Linux Security
https://linux.oracle.com/security/

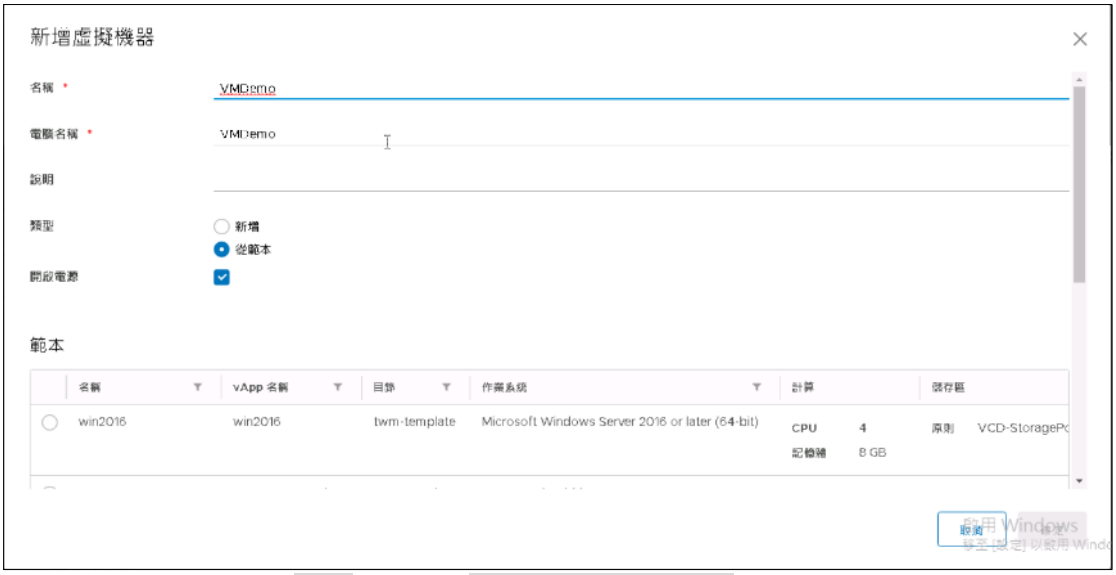
點選**應用程式→虛擬機器**會列出該 vApp 裡面的所有主機，這裡可以看到 VM name、電源狀態、建立日期、擁有者、所屬 vApp、作業系統、CPU、儲存區、記憶體、網路等資訊。左下方**動作**，可執行新增、執行暫止、停止、重設、掛載 ISO 等等功能。

新增 VM

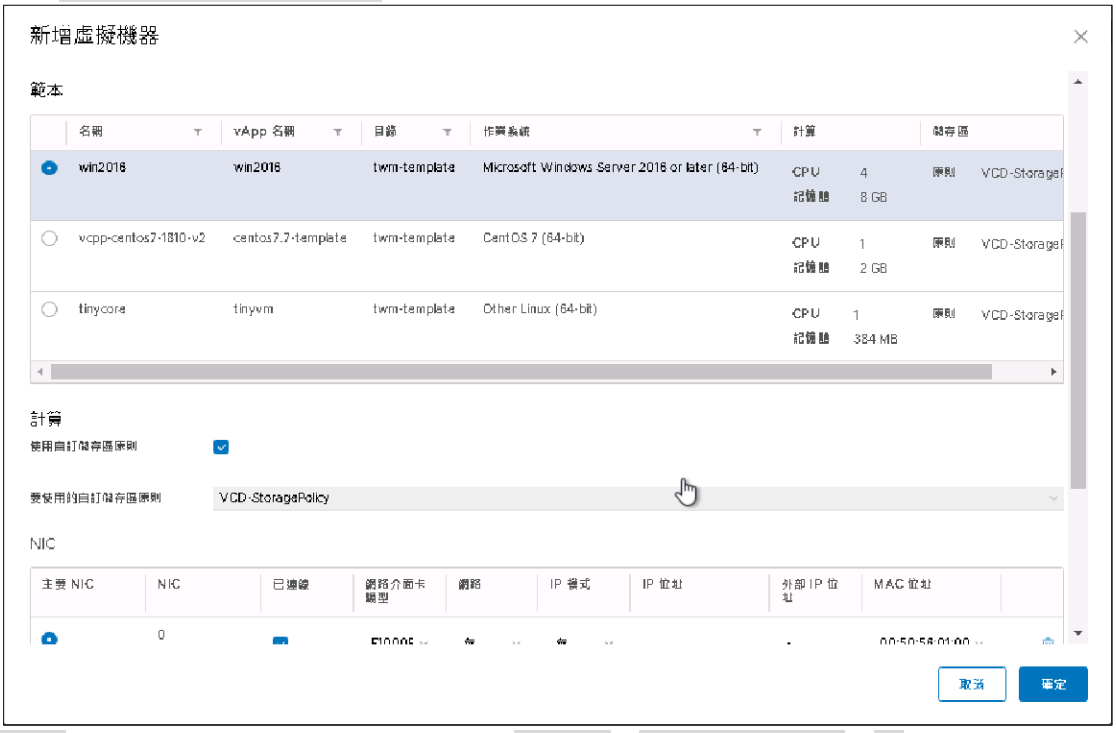
1. 點選**應用程式**。
2. 按一下**虛擬機器**。
3. 點選**新增虛擬機器**。

4. 選取虛擬資料中心，將 VM 新增至虛擬資料中心裡。

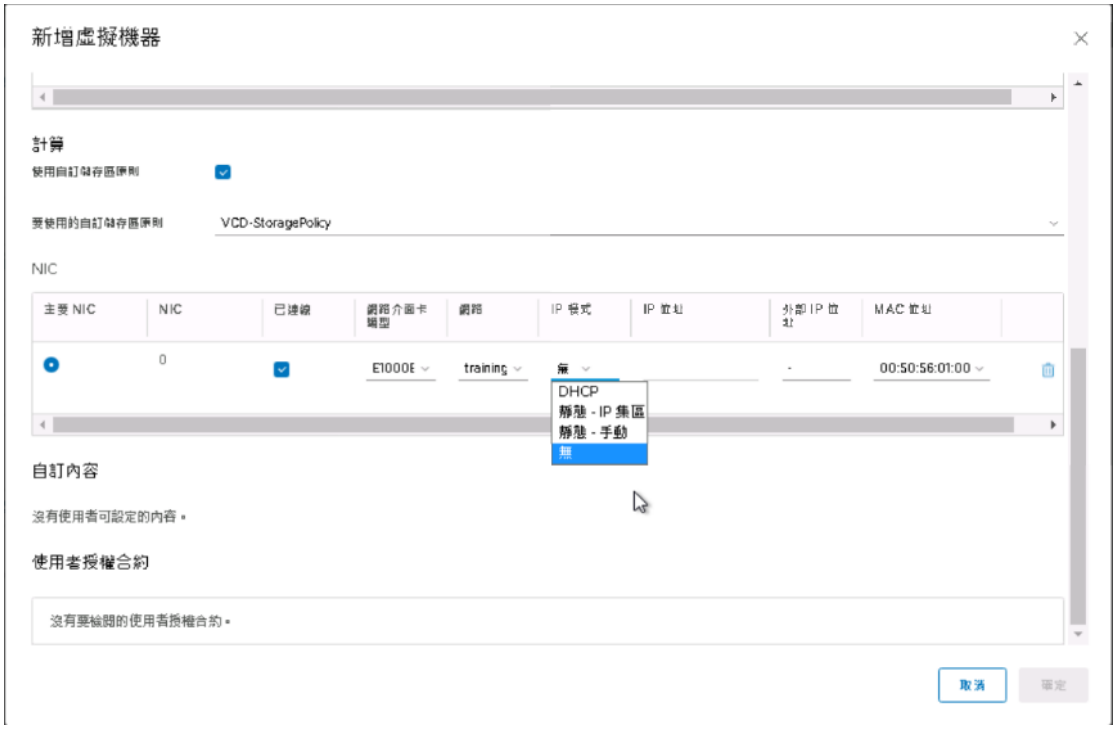
5. 輸入ＶM名稱及電腦名稱（電腦名稱只能包含英數字元和連字號。電腦名稱不能只包含數字，不能包含底線 (_)，且結尾不能是連字號 (-)），類型選擇**從範本**，**開啟電源**選項可依需求勾選



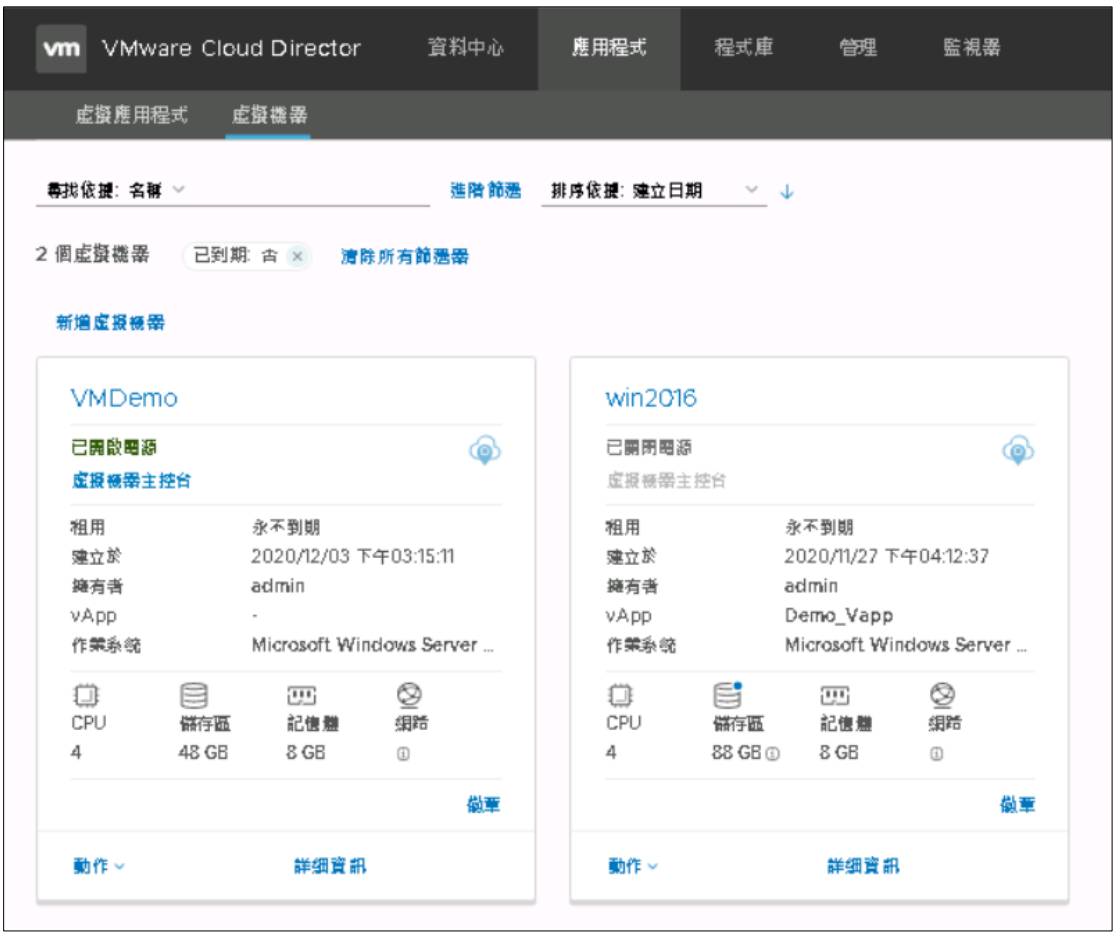
6. 點選符合需求的範本，**計算**項目中的使用自訂儲存區原則請勾選，下方選擇**要使用的自訂儲存區原則**



7. **NIC** 項目可設定網路介面卡，可設定**已連線**、**網路介面卡類型**、**網路**、**IP 模式**。若**選擇靜態-手動**，則需要手動輸入 IP 位址。設定完成後按右下**確定**。



8. 新增成功的虛擬機器會出現在頁面中。



啟動 VM

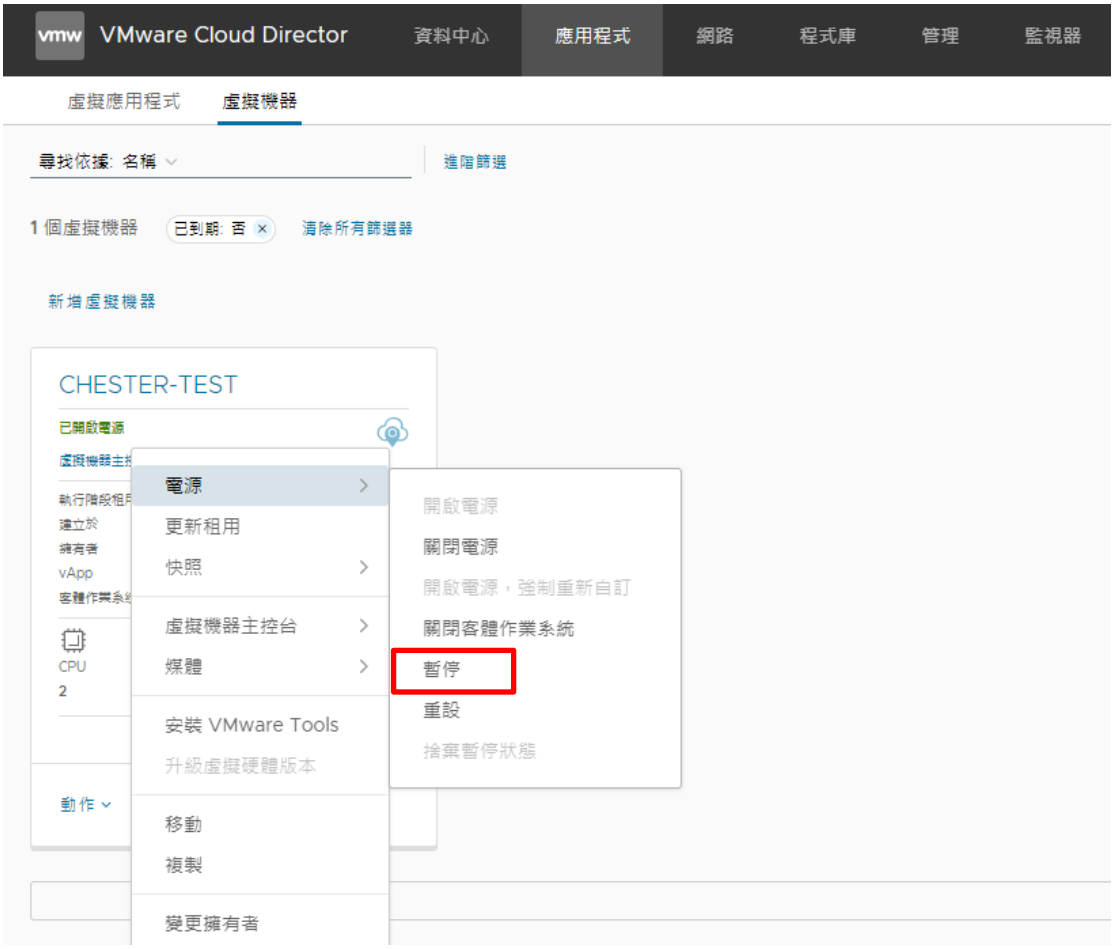
1. 點選**應用程式**。
2. 按一下**虛擬機器**。
3. 左下方**動作**，選擇**電源**，點選**開啟電源**。

關閉 VM

1. 點選**應用程式**。
2. 按一下**虛擬機器**。
3. 左下方**動作**，選擇**電源**，選擇**關閉電源**。

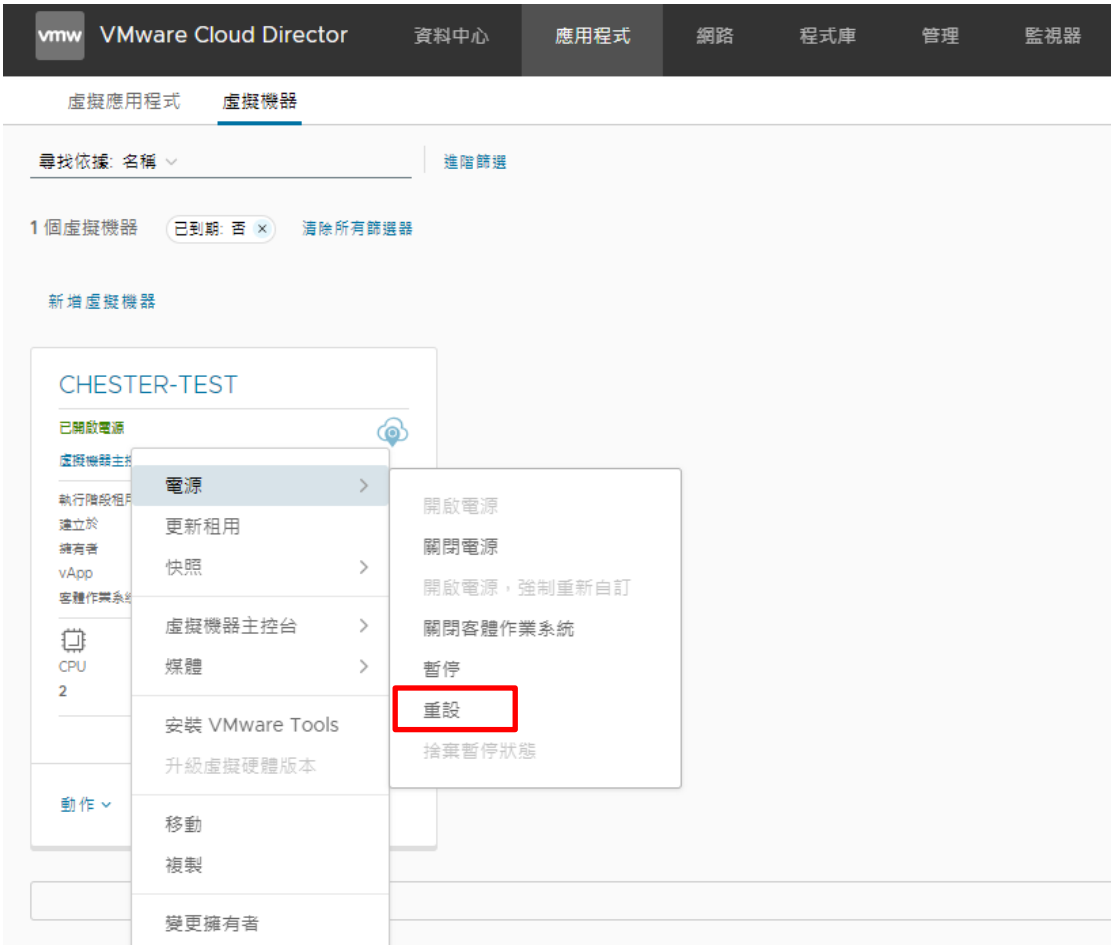
暫止 VM

1. 點選**應用程式**。
2. 按一下**虛擬機器**。
3. 左下方**動作**，選擇**電源**，選擇**暫停**。



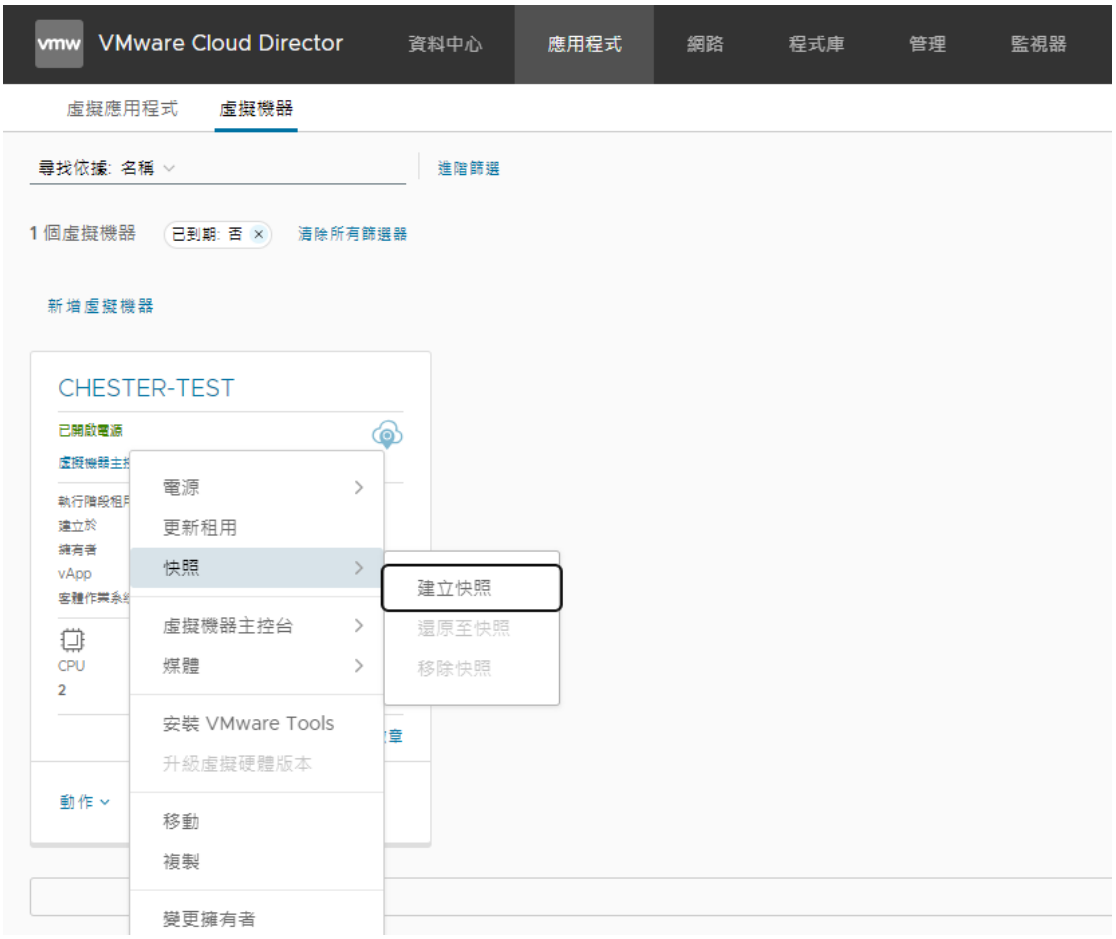
重設 VM

1. 點選**應用程式**。
2. 按一下**虛擬機器**。
3. 左下方**動作**，選擇**電源**，選擇**重設**。
   重設虛擬機器會清除狀態(記憶體、快取等)，但虛擬機器仍然會繼續執行。



建立 VM 快照

1. 點選**應用程式**。
2. 按一下**虛擬機器**。
3. 左下方**動作**，選擇**快照**，選擇**建立快照**。



4. 依據您的需求，可選擇的選項有:

   A. 快照虛擬機器的記憶體:保留現有虛擬機器記憶體狀態，建立快照。

   B. 靜止客體檔案系統：藉由透 VMware Tools 工具來暫時停止虛擬主機內的檔案系統，讓作業系統可以將相關的緩衝資料和虛擬記憶體中的快取資料，順利地寫回虛擬磁碟內，保持資料的一致性與可用性，建立快照。(VM 需已安裝 VMware Tools)

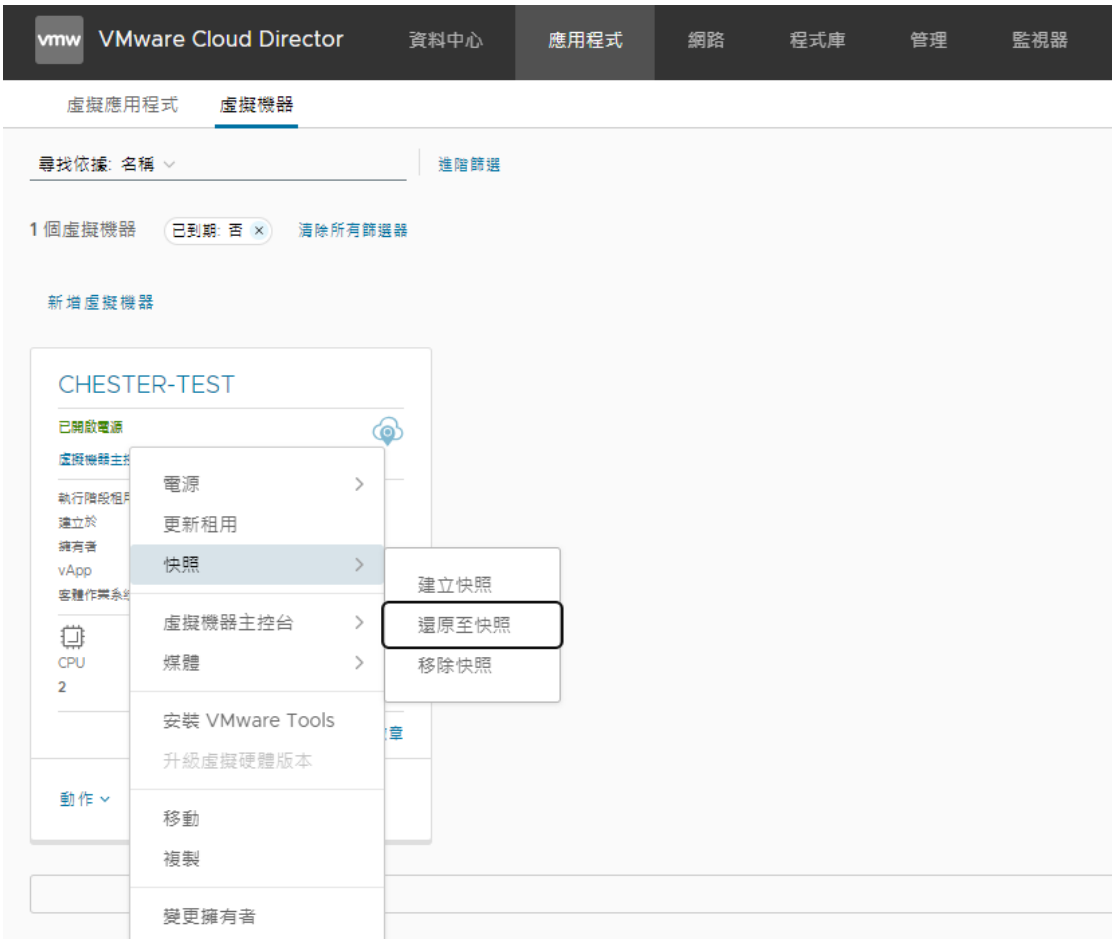
5. 選擇完成後，選取**建立**

還原VM快照

您可以將虛擬機器還原至建立快照時的當時狀態。

先決條件：VM 有快照。

1. 按一下**應用程式**。
2. 在下方選項中，按一下**虛擬機器**。
3. 左下角**動作**，選擇**快照**，然後選取**還原至快照**。


VMware Cloud Director
資料中心
應用程式
網路
程式庫
管理
監視器
虛擬應用程式
虛擬機器
尋找依據: 名稱
進階篩選
1 個虛擬機器
已到期: 否
清除所有篩選器
新增虛擬機器
CHESTER-TEST
已開啟電源
電源
更新租用
快照
虛擬機器主控台
媒體
安裝 VMware Tools
升級虛擬硬體版本
移動
複製
變更擁有者
建立快照
還原至快照
移除快照
CPU
2
動作

4. 確認則按**確定**。

移除 VM 快照

您可以將 VM 快照移除。

先決條件：VM 有建立過快照。

1. 按一下**應用程式**。
2. 在下方選項中，按一下**虛擬機器**。
3. 左下角**動作**，選擇**快照**，然後選取**移除快照**。


VMware Cloud Director
資料中心
應用程式
網路
程式庫
管理
監視器
虛擬應用程式
虛擬機器
尋找依據: 名稱
進階篩選
1 個虛擬機器
已到期: 否
清除所有篩選器
新增虛擬機器
CHESTER-TEST
已開啟電源
電源
更新租用
快照
虛擬機器主控台
媒體
安裝 VMware Tools
升級虛擬硬體版本
移動
複製
變更擁有者
建立快照
還原至快照
移除快照
vApp
CPU
2
動作

4. 確認則按**確定**。


移除快照
這將刪除為此虛擬機器建立的快照。
移除 VMDemo 的快照?
取消
確定

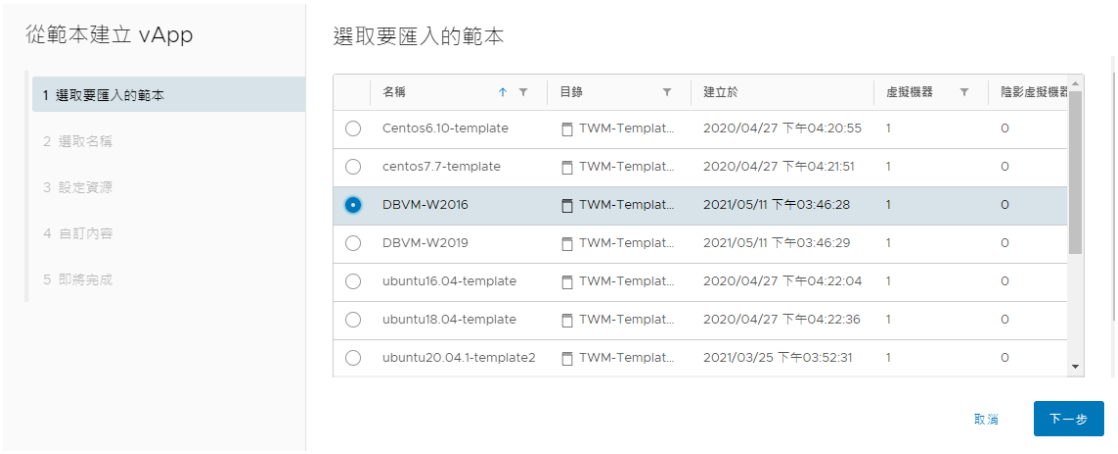
MSSQL DBVM 啟用程序說明

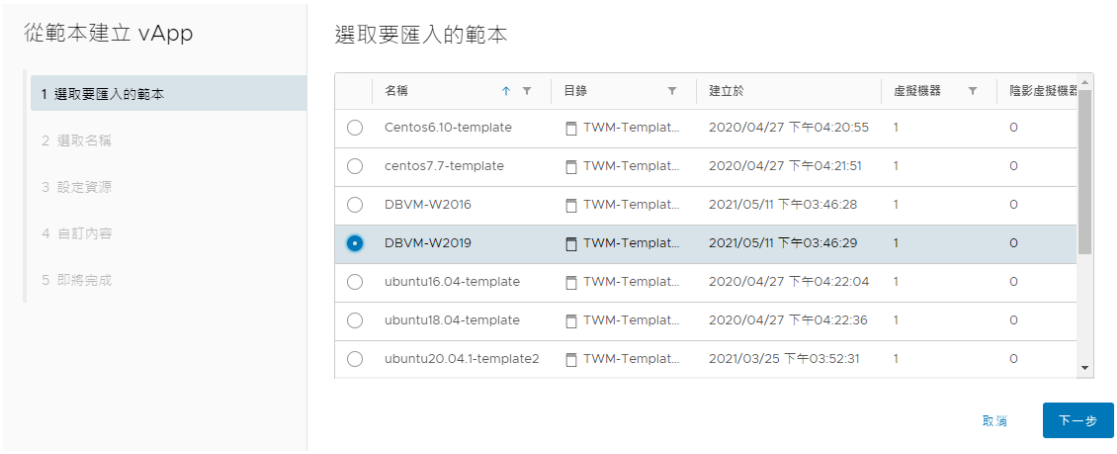
運算雲 3.0 提供客戶具備 window 作業系統的 MSSQL server 服務，用戶可於平台中選取範本申裝，計費規範詳洽業務窗口。以下說明 MSSQL 啟用與驗證程序：

選擇 VDC

選擇從 catalog 新增 vapp

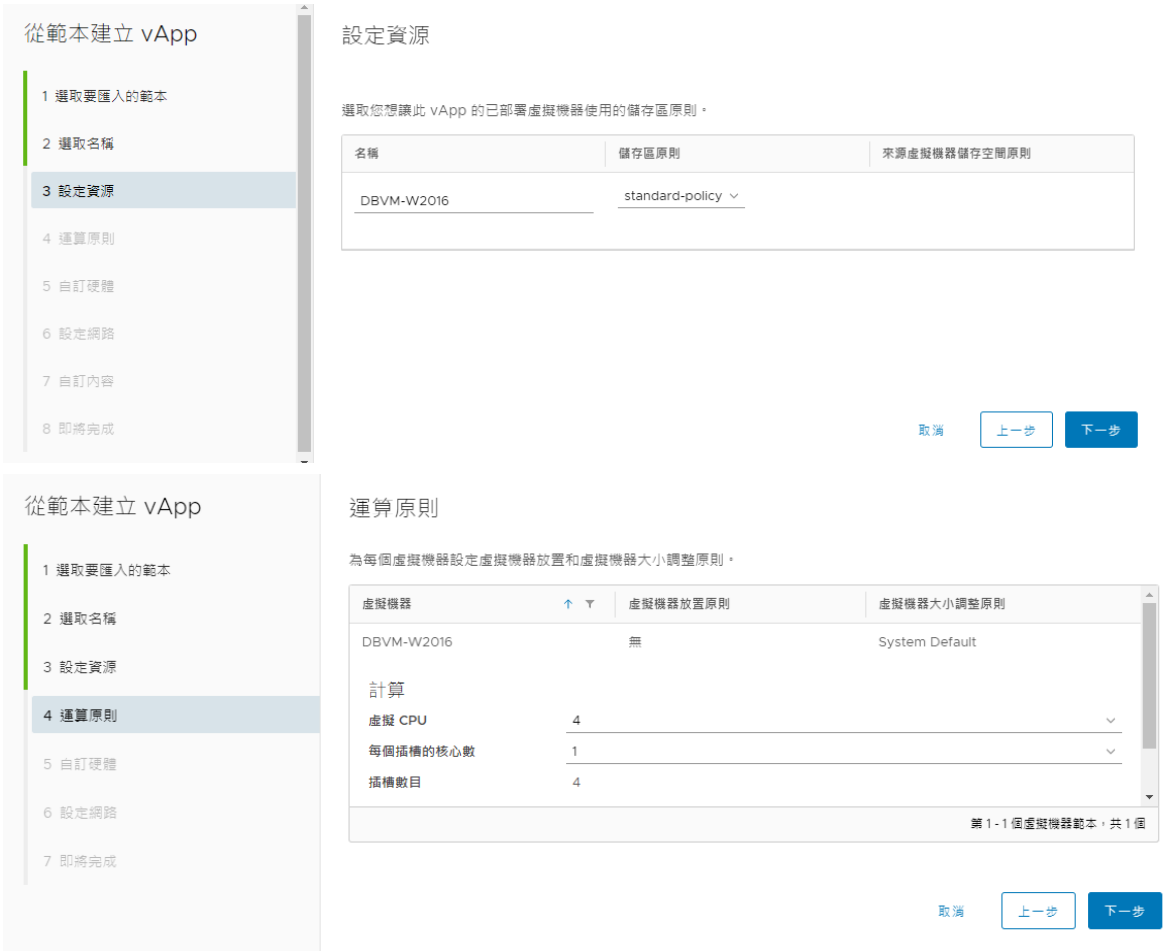
選擇 DBVM-W2016 template (或 DBVM-W2019) template





輸入名稱

如無調整請保持預設



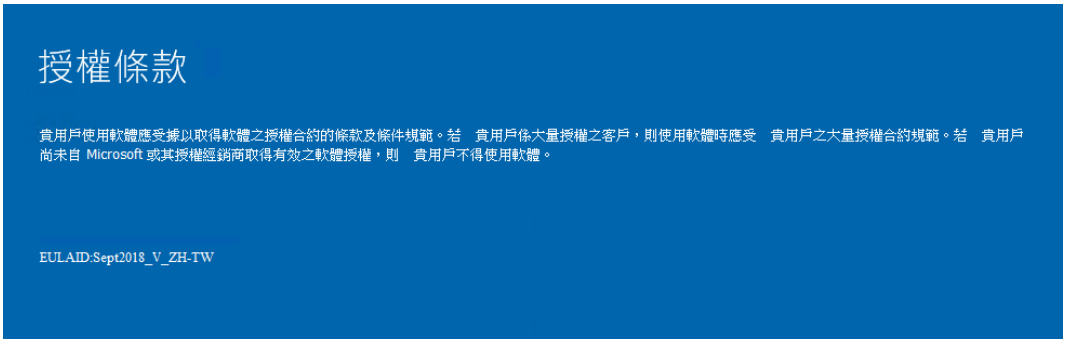
選擇可連上網路的 VDC Network [6]

完成設定

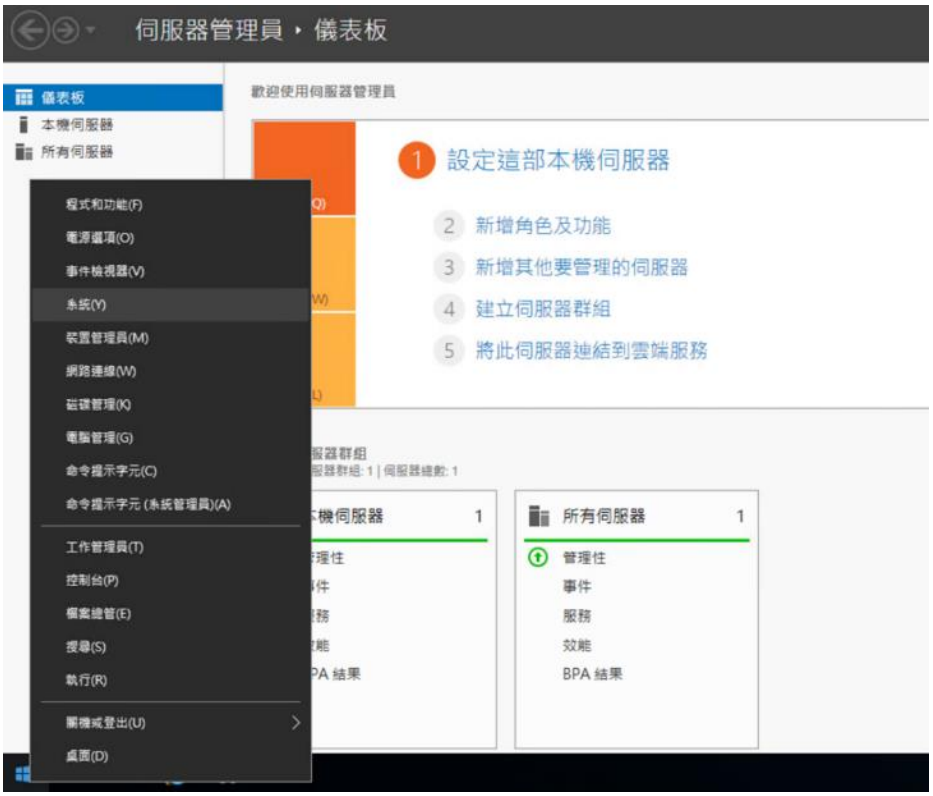
[6] Windows 必須在 internet 連通狀態才能自動啟用

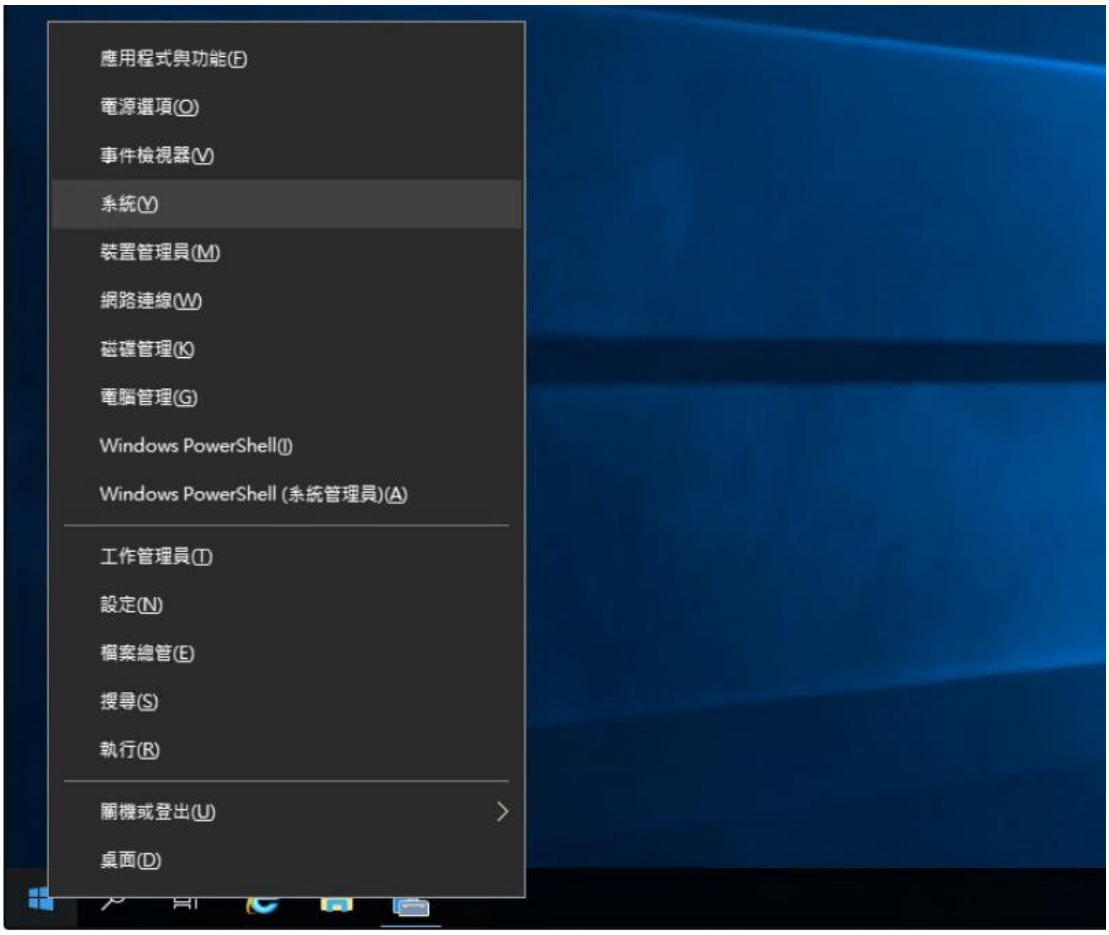
啟動 vapp

進行初始密碼設定



登入後滑鼠移到左下方按右鍵選擇系統

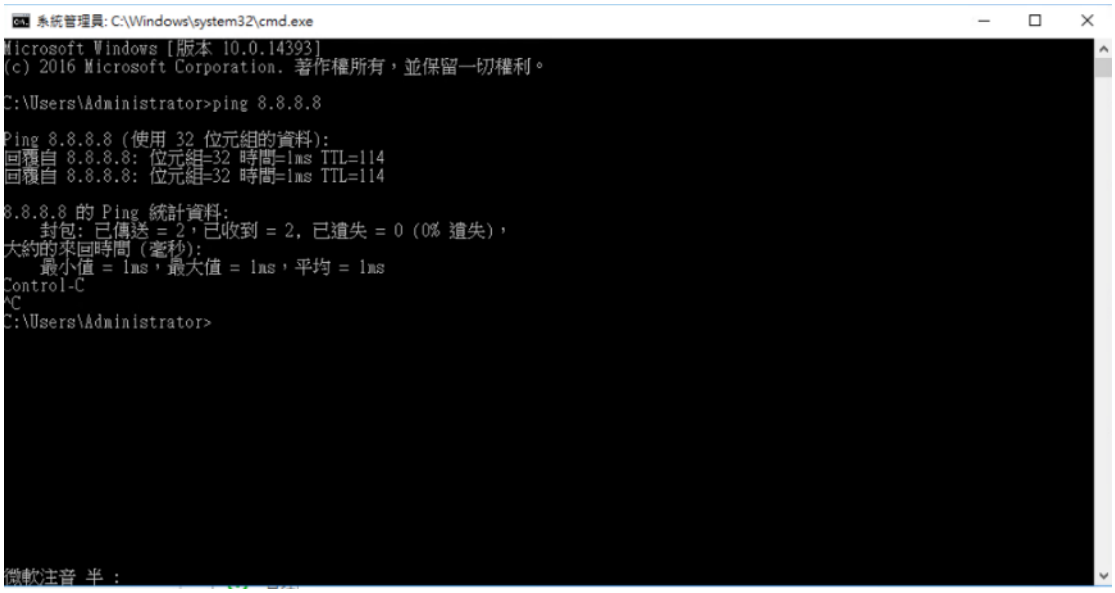




確認系統資訊/確認 Windows 已啟用


首頁
尋找設定
系統
顯示器
音效
通知與動作
專注輔助
電源與睡眠
儲存空間
平板電腦模式
多工
遠端桌面
關於
手寫筆與觸控
此顯示器不提供手寫筆或觸控式輸入功能
重新命名此電腦
Windows 規格
版本 Windows Server 2019 Datacenter
版本 1809
安裝於 2021/5/10
OS 組建 17763.1911
變更產品金鑰或升級您的 Windows 版本
閱讀適用於我們的服務的 Microsoft 服務合約
閱讀 Microsoft 軟體授權條款
相關設定
系統資訊
系統
控制台 › 系統及安全性 › 系統
控制台首頁
裝置管理員
遠端設定
進階系統設定
檢視電腦的基本資訊
Windows 版本
Windows Server 2019 Datacenter
© 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
系統
處理器: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz 2.10 GHz (4 個處理器)
已安裝記憶體 (RAM) 8.00 GB
系統類型: 64 位元作業系統，x64 型處理器
手寫筆與觸控: 此顯示器不提供手寫筆或觸控式輸入功能。
電腦名稱、網域及工作群組設定
電腦名稱: DBVM2019-001
完整電腦名稱: DBVM2019-001
電腦描述:
工作群組: WORKGROUP
Windows 啟用
Windows 已啟用 閱讀 Microsoft 軟體授權條款
產品識別碼: 00430-10385-82443-AA166
請參閱
安全性與維護

驗證 VM 對外連線正常[7]

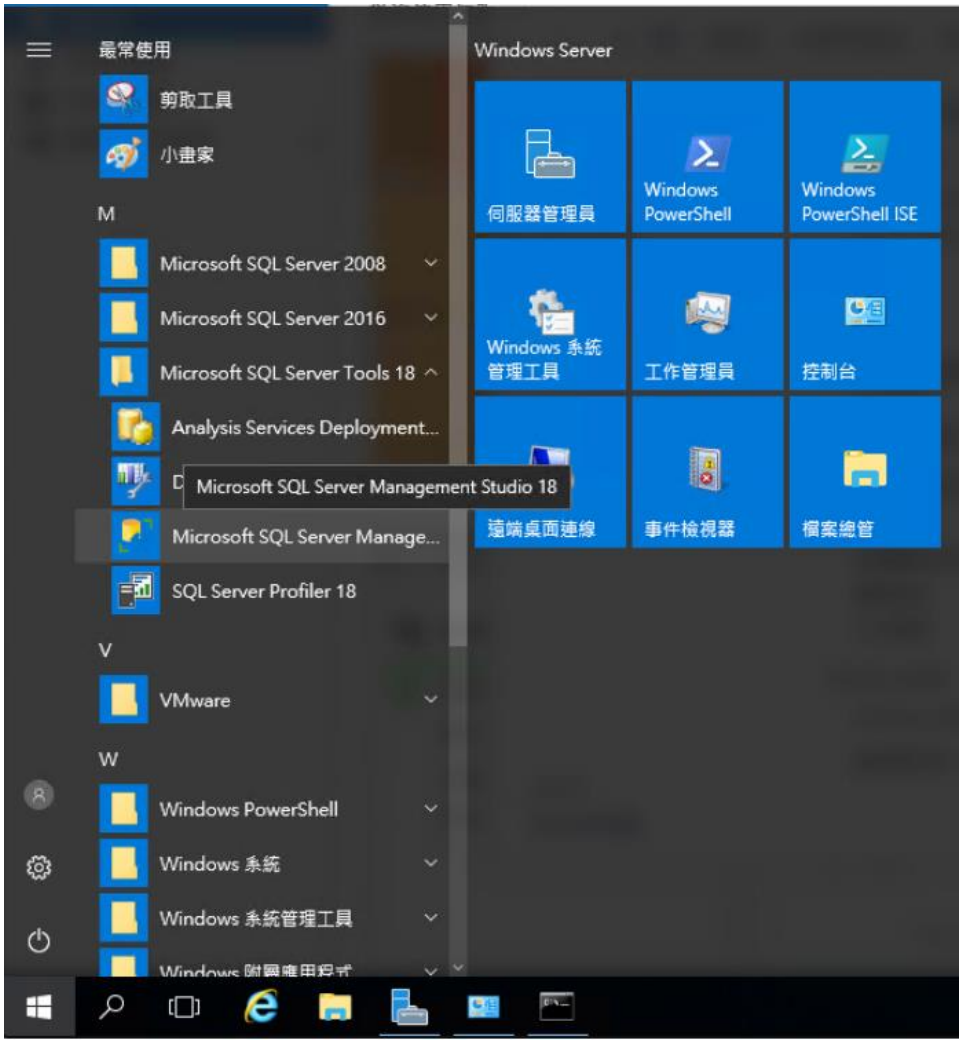


MSSQL DBVM 驗證程序說明

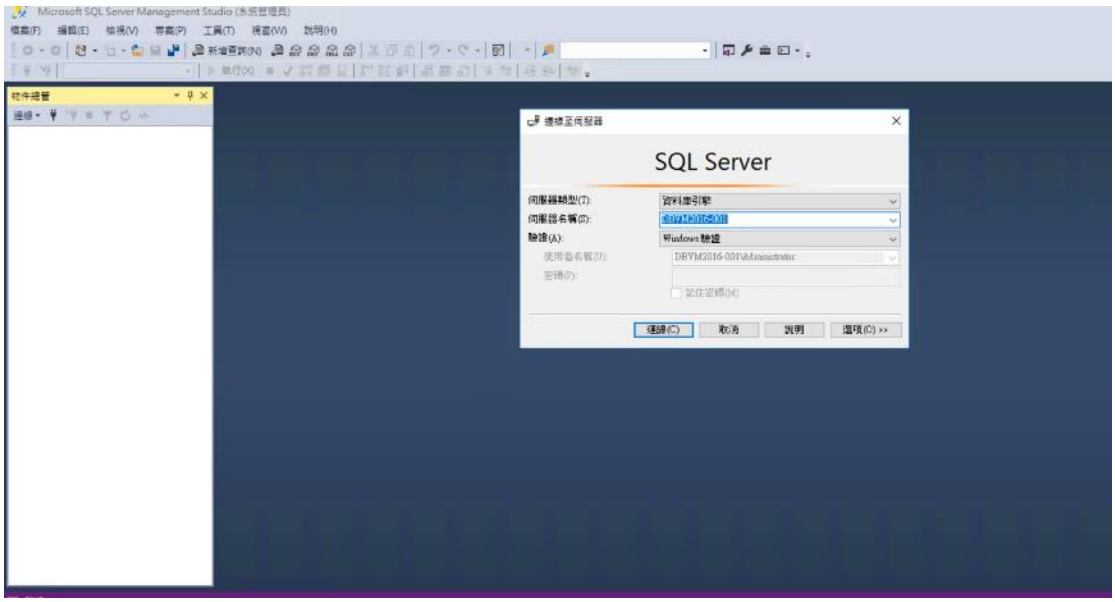
以下步驟驗證 DBVM 2016/2019 功能

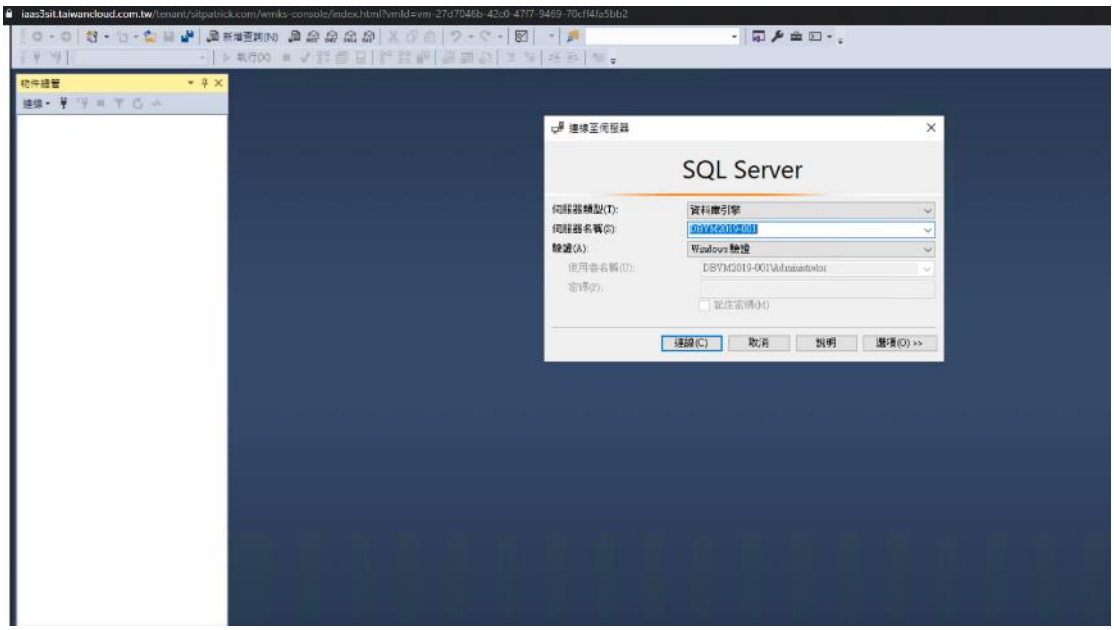
開啟 MSSQL 管理工具

[7] 以上驗證登入與網路設定若成功,代表客體自訂成功

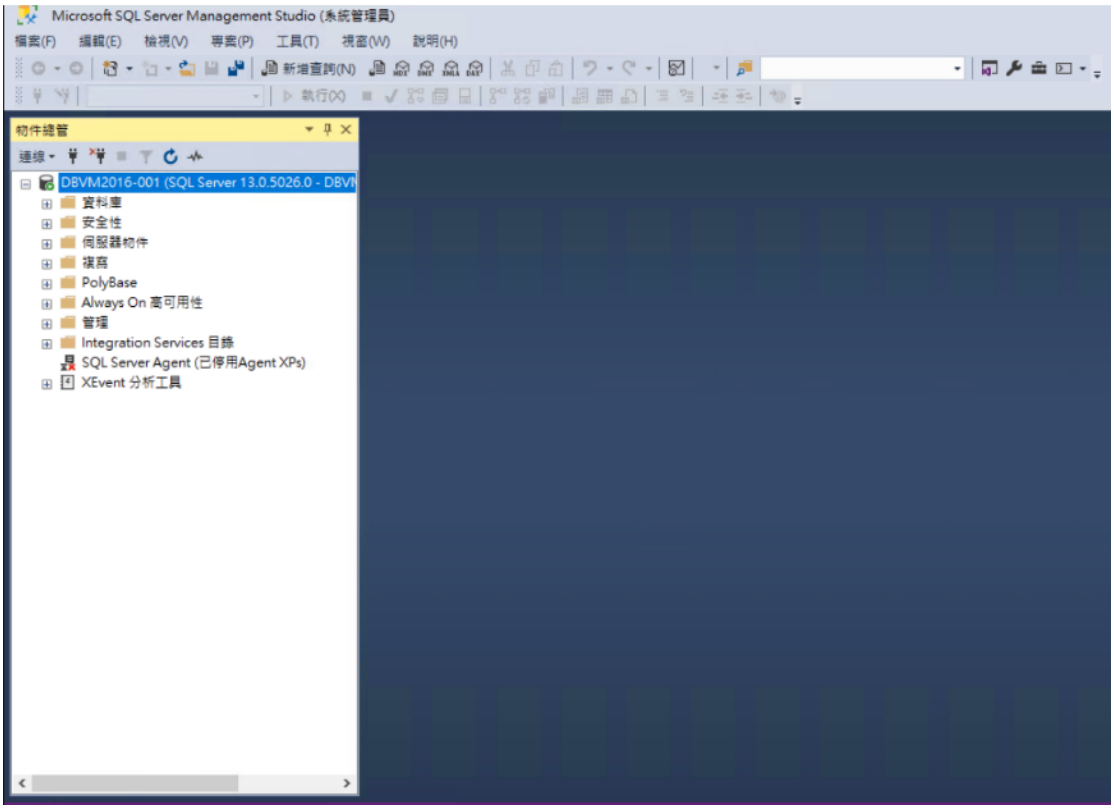

最常使用
剪取工具
小畫家
M
Microsoft SQL Server 2008
Microsoft SQL Server 2016
Microsoft SQL Server Tools 18
Analysis Services Deployment...
Microsoft SQL Server Management Studio 18
Microsoft SQL Server Manage...
SQL Server Profiler 18
V
VMware
W
Windows PowerShell
Windows 系統
Windows 系統管理工具
Windows Server
伺服器管理員
Windows PowerShell
Windows PowerShell ISE
Windows 系統管理工具
工作管理員
控制台
遠端桌面連線
事件檢視器
檔案總管

點選連線

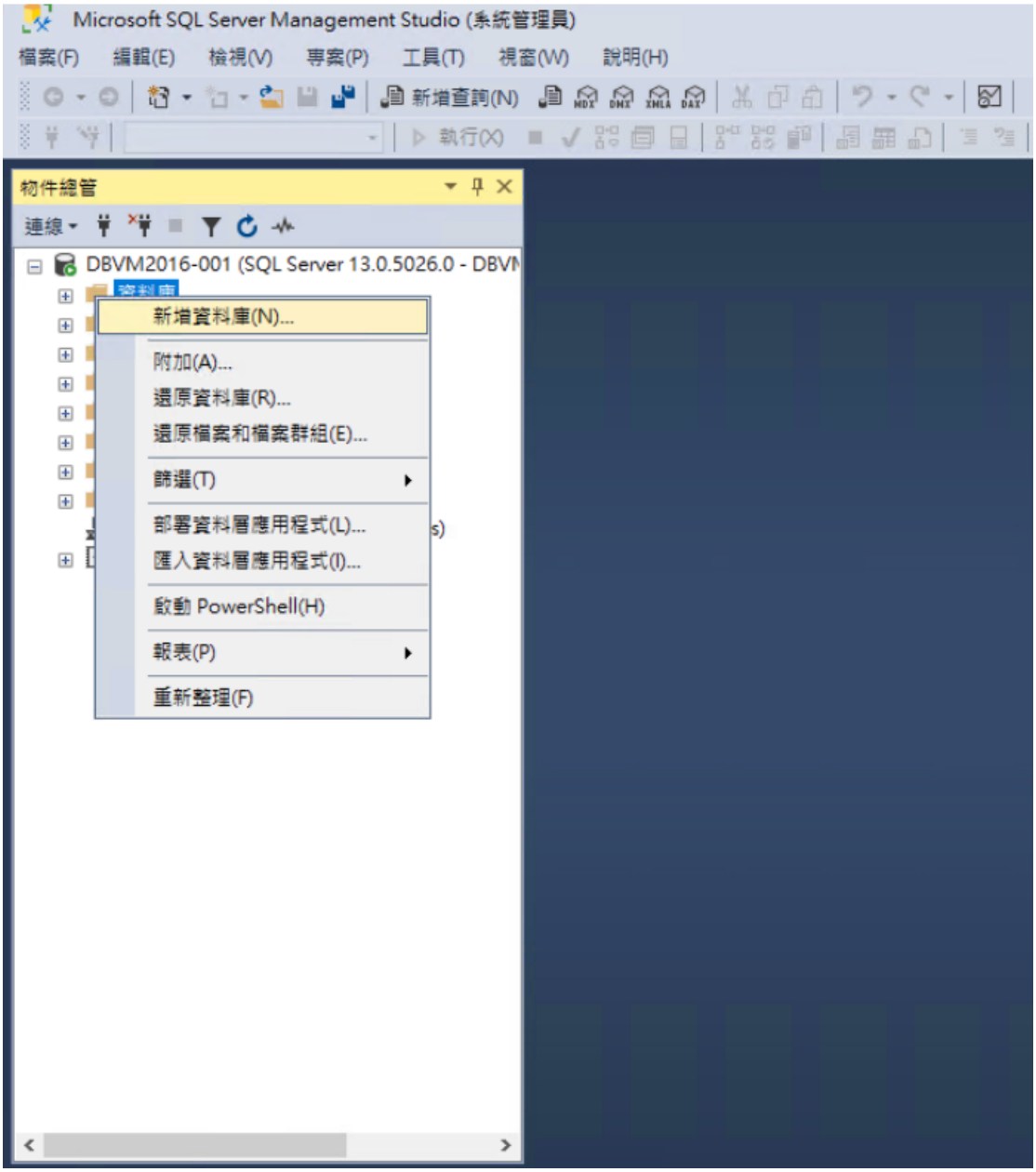

SQL Server



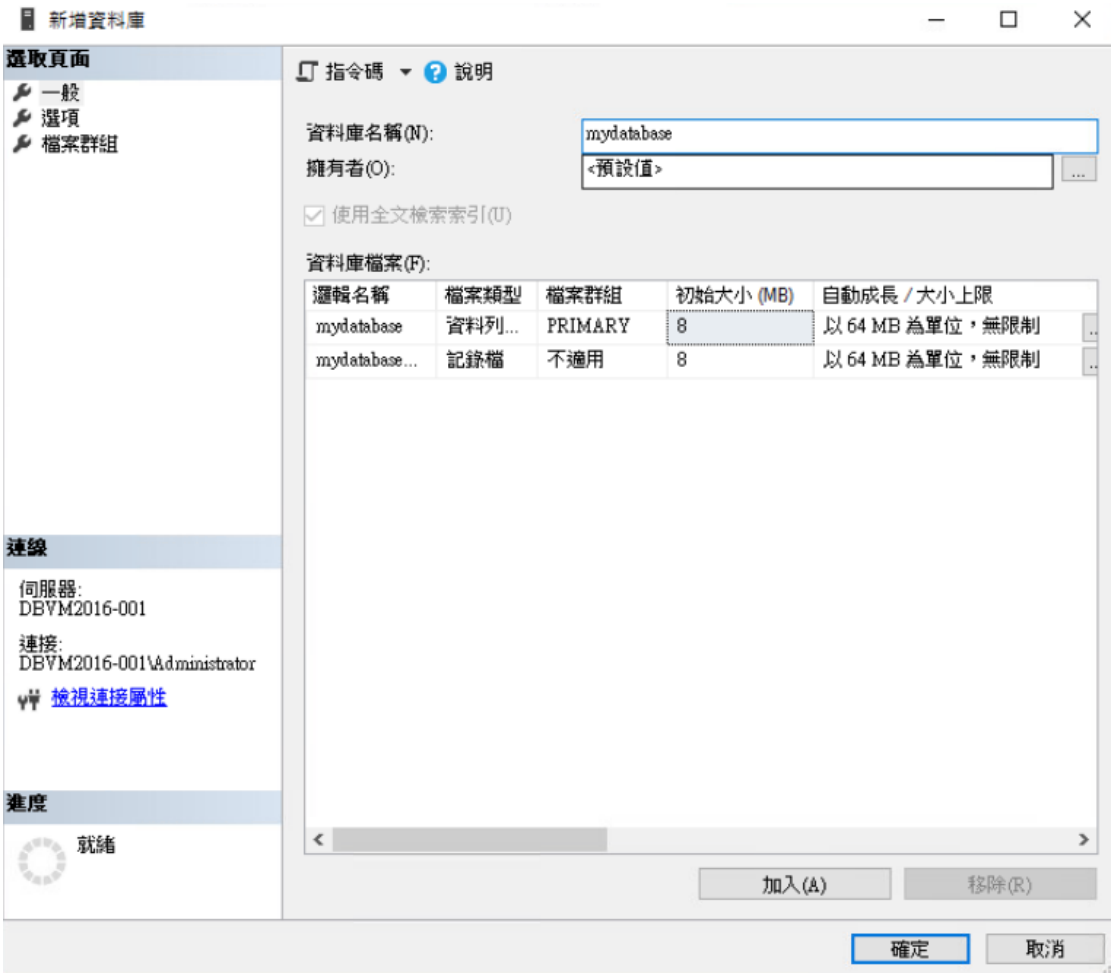
沒有錯誤訊息代表登入成功



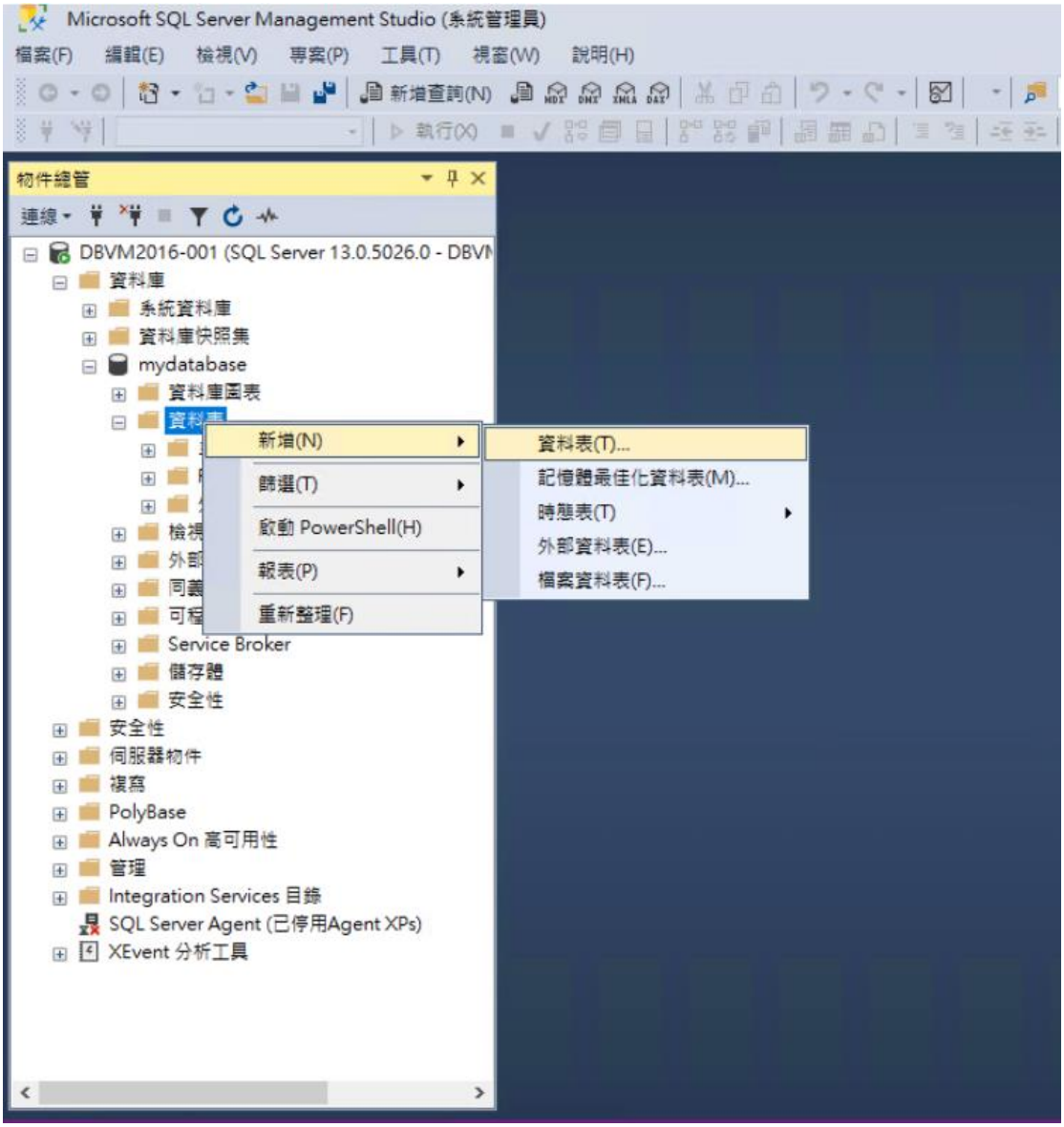
新增資料庫



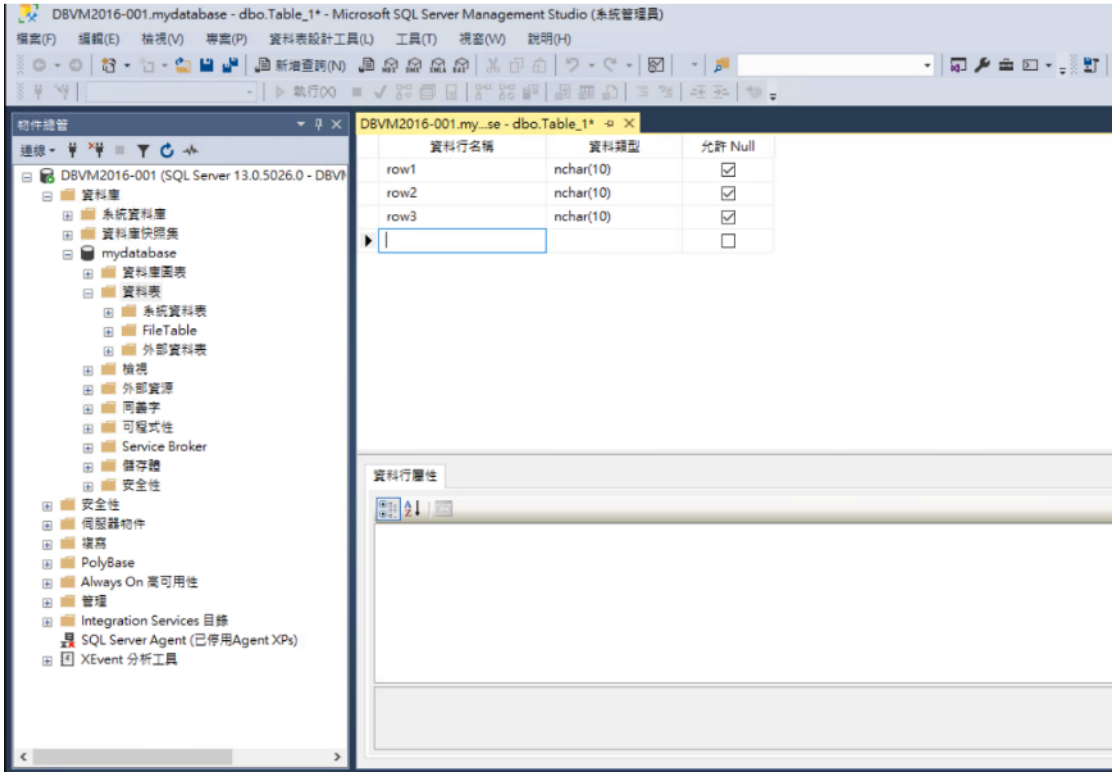
輸入資料庫名稱後按確定



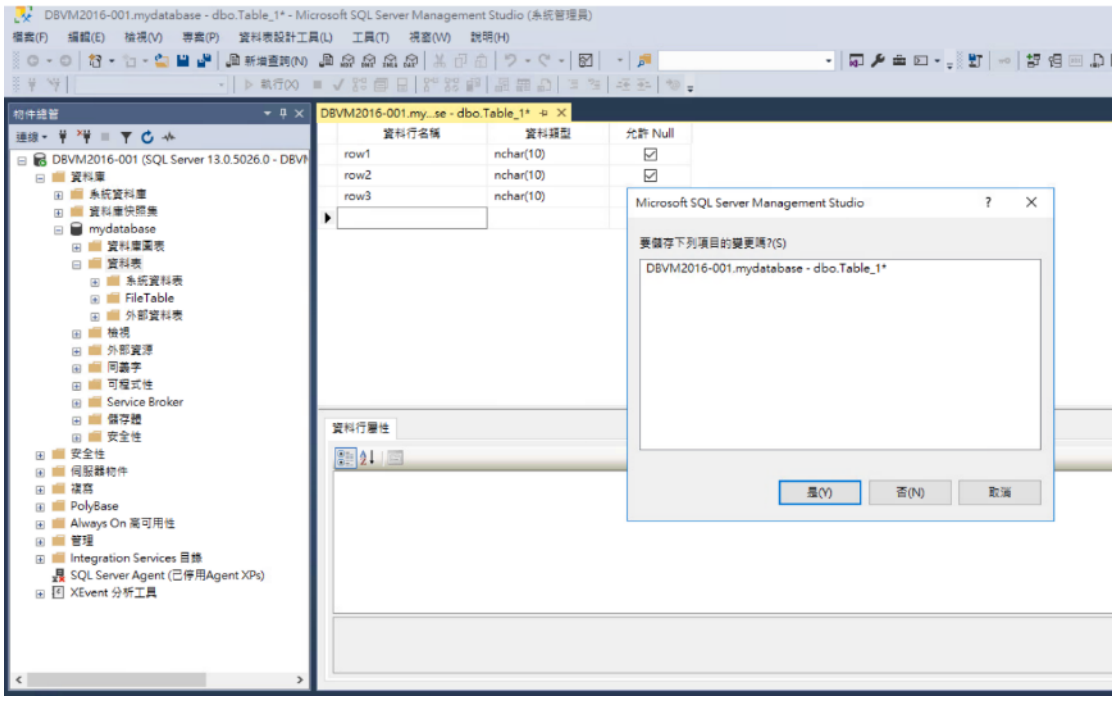
點選剛建立的資料庫/資料表/按右鍵選擇新增資料表


Microsoft SQL Server Management Studio (系統管理員)
檔案(F)
編輯(E)
檢視(V)
專案(P)
工具(T)
視窗(W)
說明(H)
新增查詢(N)
物件總管
連線
DBVM2016-001 (SQL Server 13.0.5026.0 - DBVM
資料庫
系統資料庫
資料庫快照集
mydatabase
資料庫圖表
新增(N)
篩選(T)
啟動 PowerShell(H)
報表(P)
重新整理(F)
資料表(T)...
記憶體最佳化資料表(M)...
時態表(T)
外部資料表(E)...
檔案資料表(F)...
Service Broker
儲存體
安全性
安全性
伺服器物件
複寫
PolyBase
Always On 高可用性
管理
Integration Services 目錄
SQL Server Agent (已停用Agent XPs)
XEvent 分析工具

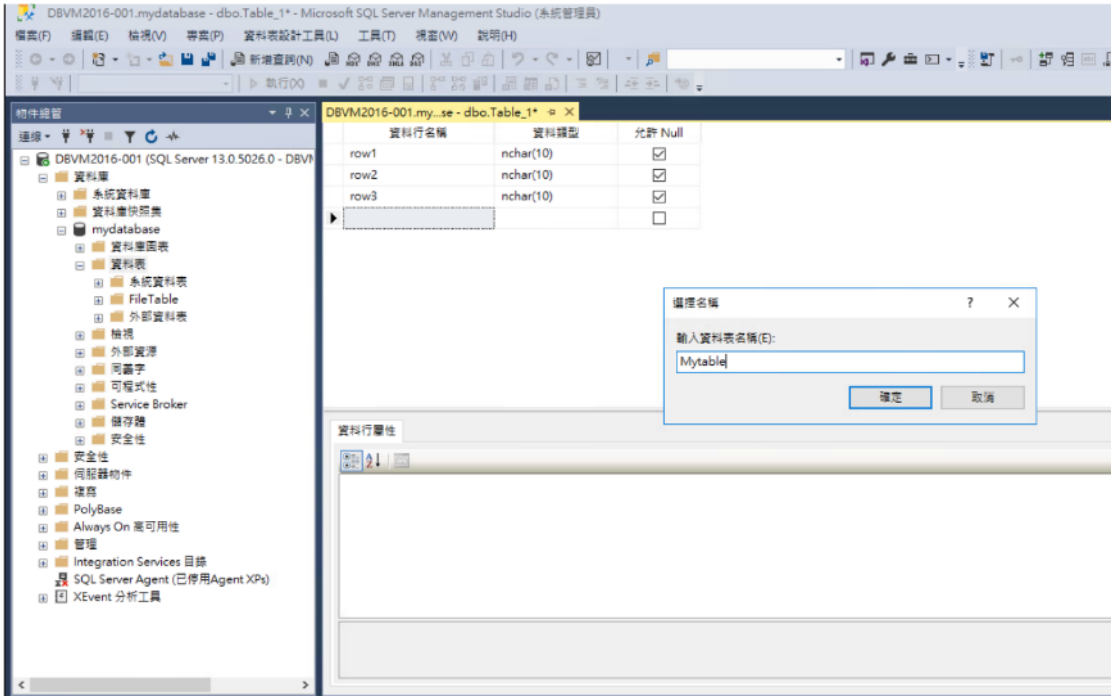
新增三個欄位



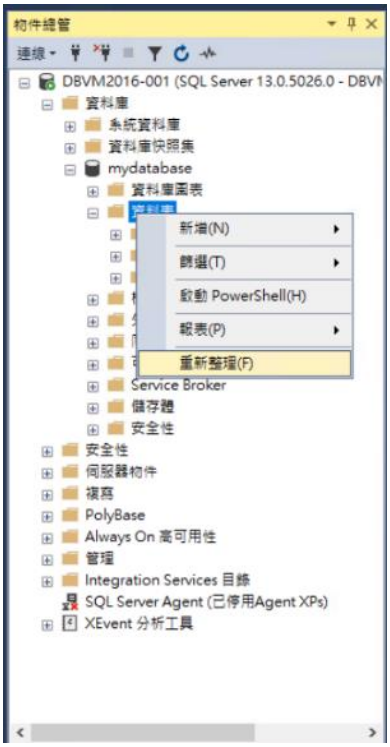
點選 X 選擇是儲存資料表



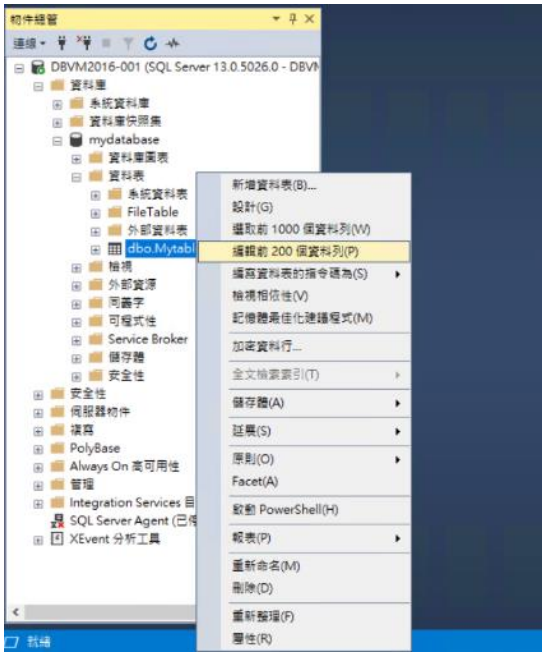
輸入資料表名稱



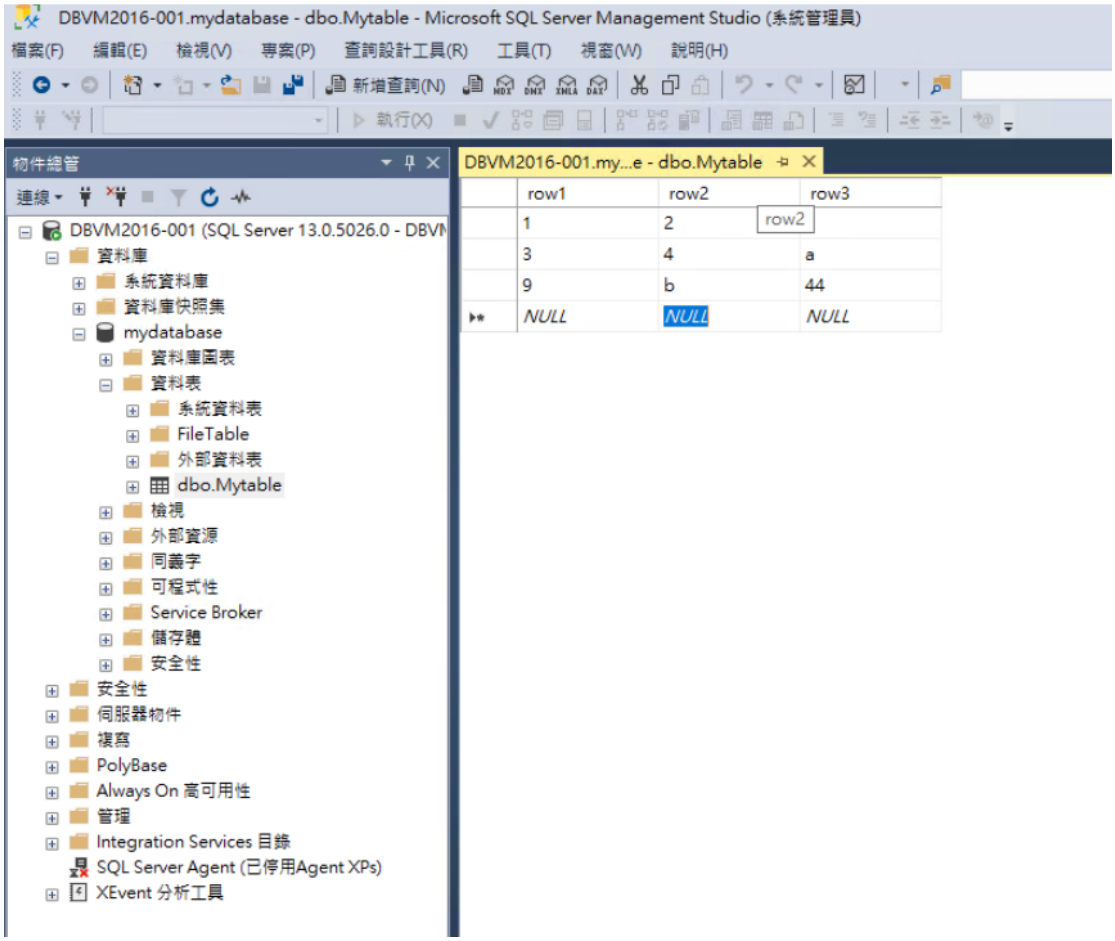
重新整理資料表



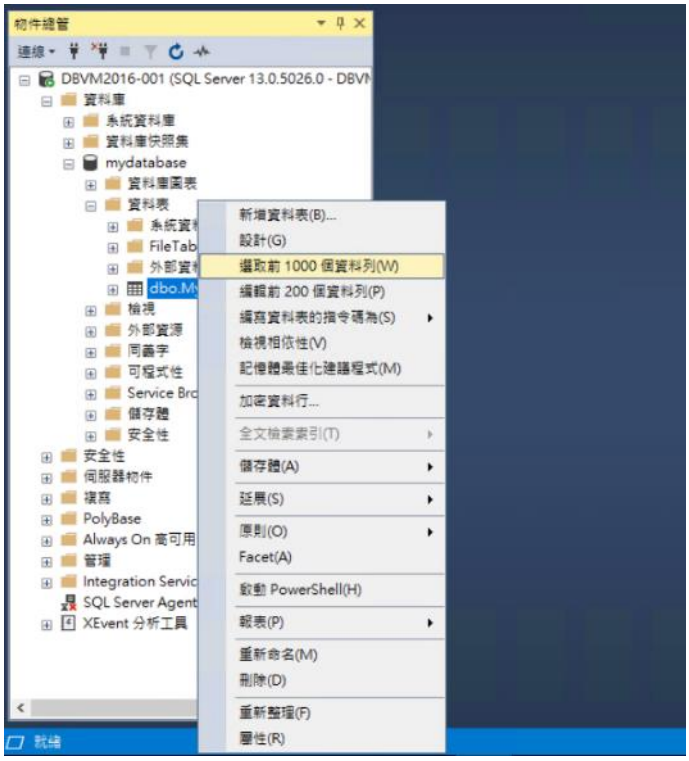
在剛建立的資料表上新增資料



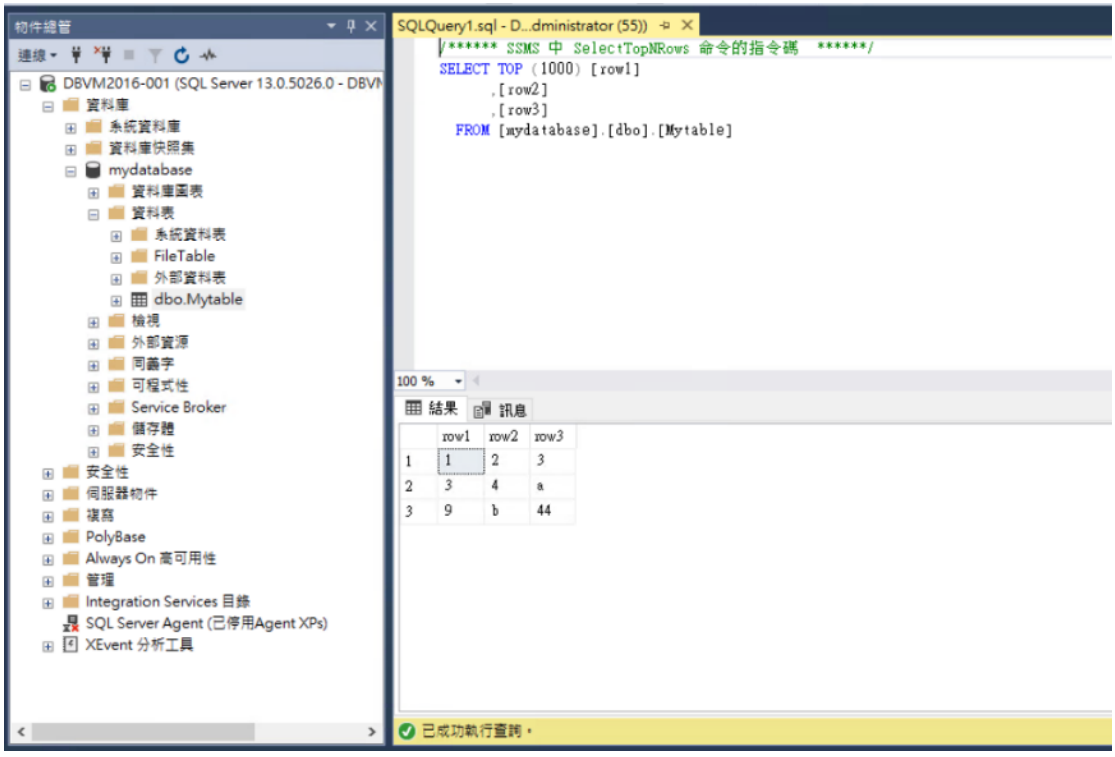
任意輸入資料後按 X 結束



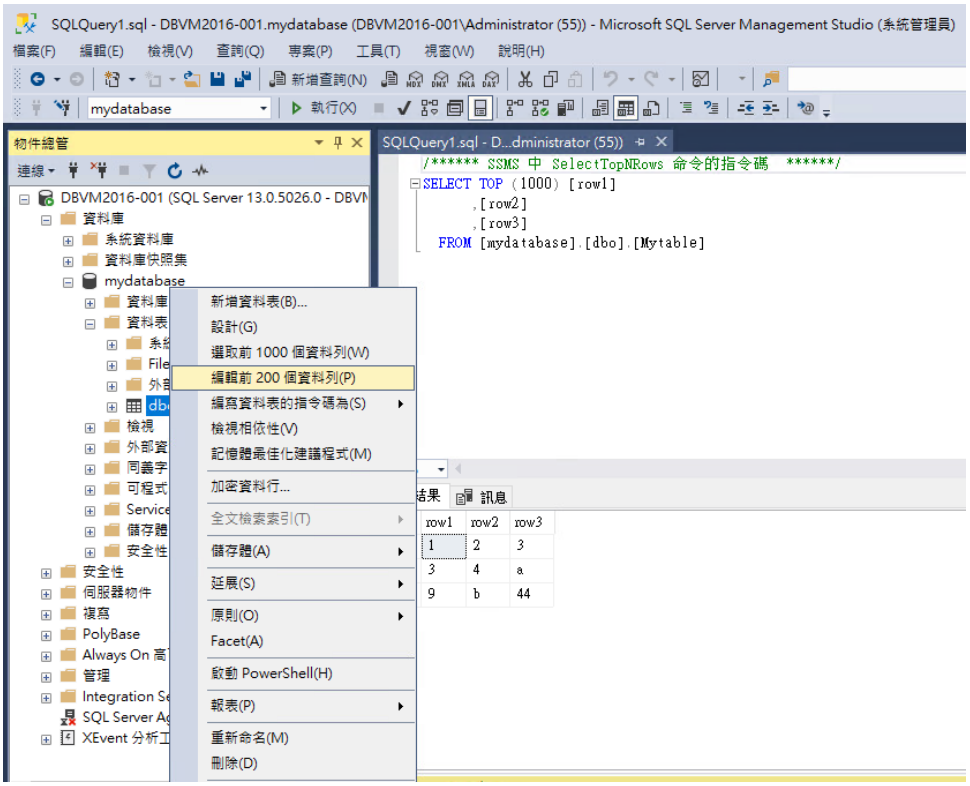
查詢資料表



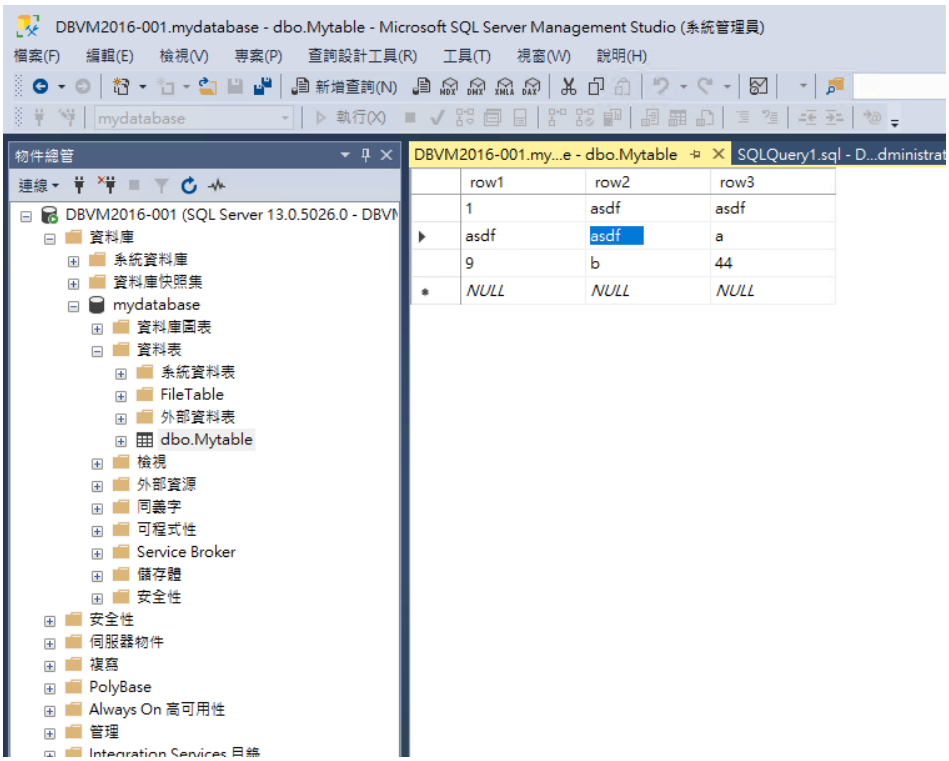
確認剛輸入的資料有顯示出來



選擇編輯前 200 個資料列



可任意修改/刪除資料內容



6.VM 設定調整

主機名稱、顯示名稱，可依據管理者資訊資產管理需求，填入名稱，例如用於資產標註、VM 分類等用途。

名稱設定

虛擬機器→詳細資訊

名稱:即為運算雲 3 平台上的顯示名稱，電腦名稱:即為主機名稱。

客體作業系統自訂

虛擬機器→詳細資訊→客體作業系統自訂

VM 第一次開機就會套用客體自訂設定，套用時機在 VM 開機時，Linux VM 開機套用完後客體自訂完成，而 Windows VM 開機套用完後則會再次重新開機(過程約需 3 分鐘)。

Linux 預設 VM 密碼強度原則為大小寫英文+數字共 8 碼，建議您依需求自行變更，並定期更換 VM 密碼。

Windows VM 預設不提供密碼，請於開機時自行開啟 VM console 進行密碼設定，建議 VM 密碼強度原則為大小寫英文+數字共 8 碼，並妥善保存密碼與定期更換，若有 VM 管理密碼變更需求，則可利用客體自訂功能進行變更。

若有網域控制站，就可以把虛擬機器加入網域。

VM 關機關電源後，可於開機時強制套用客體自訂，使用時機:

1. 強制修改 VM 登入密碼。
2. VM 開機時直接套用指定的 IP，不用登入 VM 手動輸入 IP。
3. 變更 SID。(僅限 Windows VM)

新增 Economic-policy 儲存磁碟

適用說明：建立 VM 時預設儲存原則為 standard-policy， Economic-policy-NLSAS 可於建立 VM 後，新增磁碟時使用。

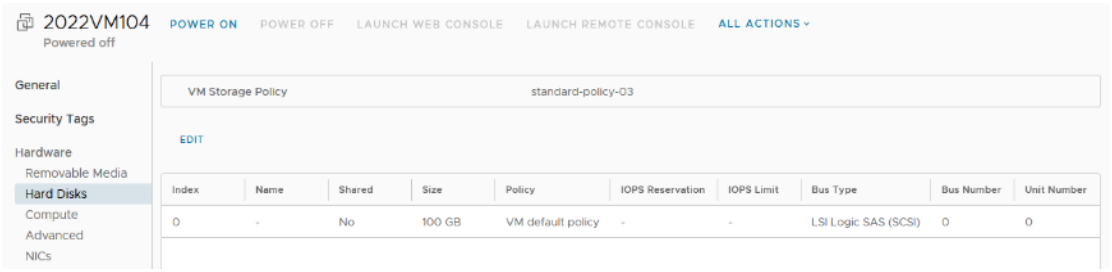
新增 Economic vDisk 儲存磁碟

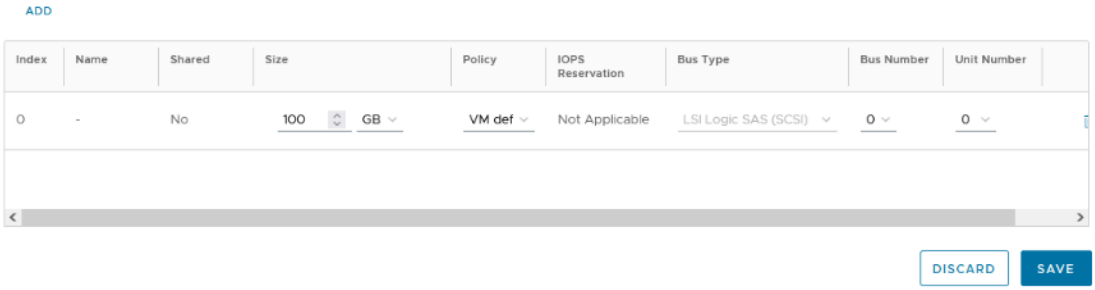
VM 關機 > 編輯 VM > Hard Disks > EDIT > ADD > (編輯下列設定) > SAVE。

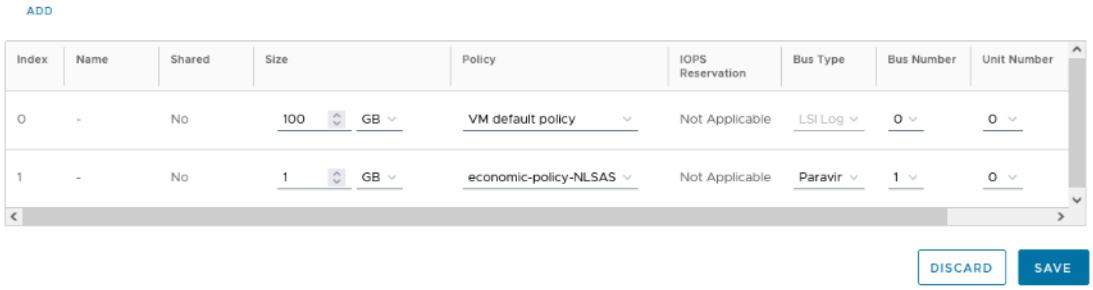
Size：依需求調整。

Policy：選擇”economic-policy-NLSAS”

Bus Type/Number/Unit Number：請依系統預設勿自行變更。



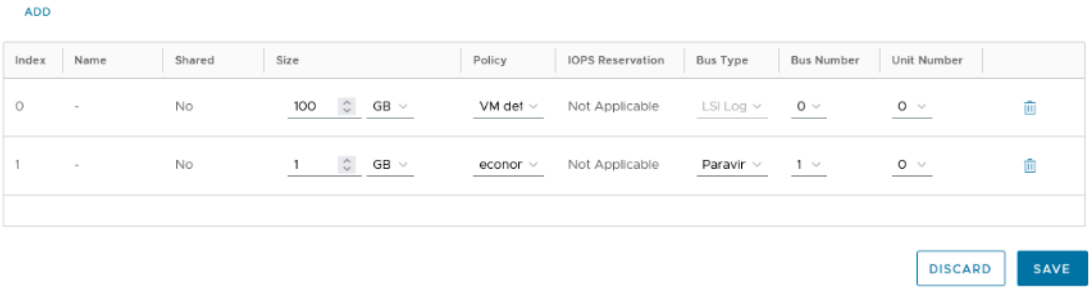




變更儲存磁碟容量

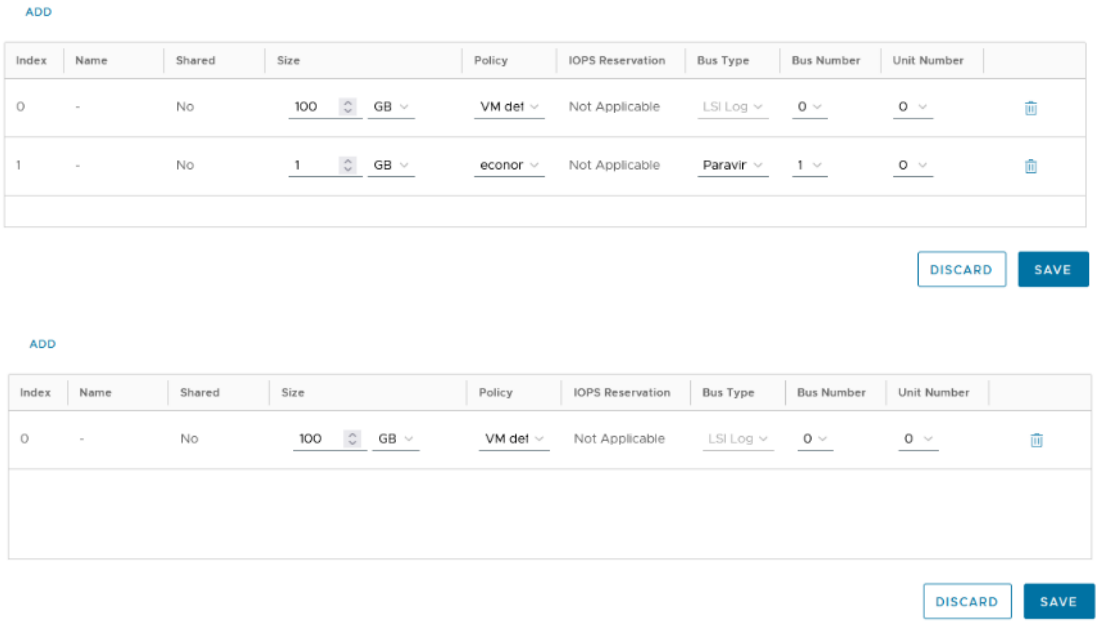
須先自行確定作業系統可支援容量變更，如 Linux 先確保格式為 LVM。

VM 關機 > 編輯 VM > Hard Disks > EDIT > 變更 Economic-policy-NLSAS 儲存磁碟容量 > SAVE。



刪除 Economic-policy 儲存磁碟

VM 關機 > 編輯 VM > Hard Disks > EDIT > 刪除 Economic vDisk 儲存磁碟 > SAVE。

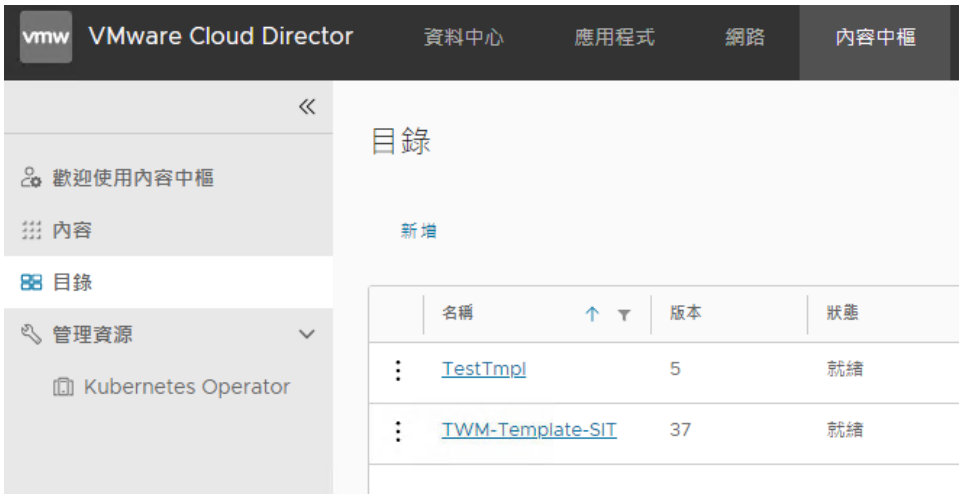


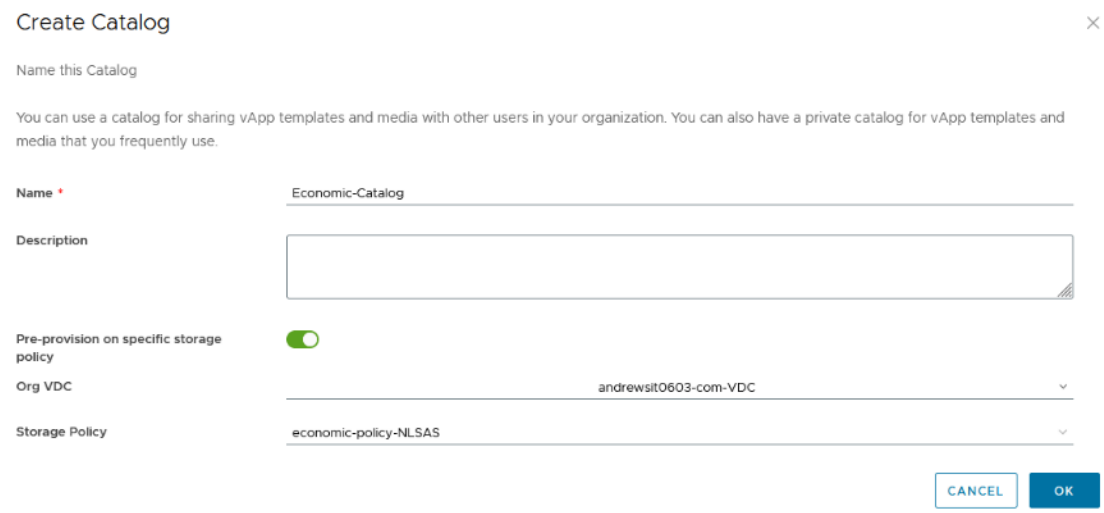
新增 Economic-policy 儲存範本目錄

點選「內容中樞」 > 目錄 > 新增 > 輸入名稱 > 勾選特定儲存區 > 選擇 OrgVDC > 選擇儲存原則”economic-policy-NLSAS” > 點選 OK。

之後建立 vApp 範本時，便可將 vApp 範本儲存於此目錄。

※建立 vApp 範本方式詳見操作手冊相關章節，建立 VM 範本請透過 vApp 建立。





7.VM 硬體調整

卸除式媒體

可以確認目前掛載的 ISO

硬碟

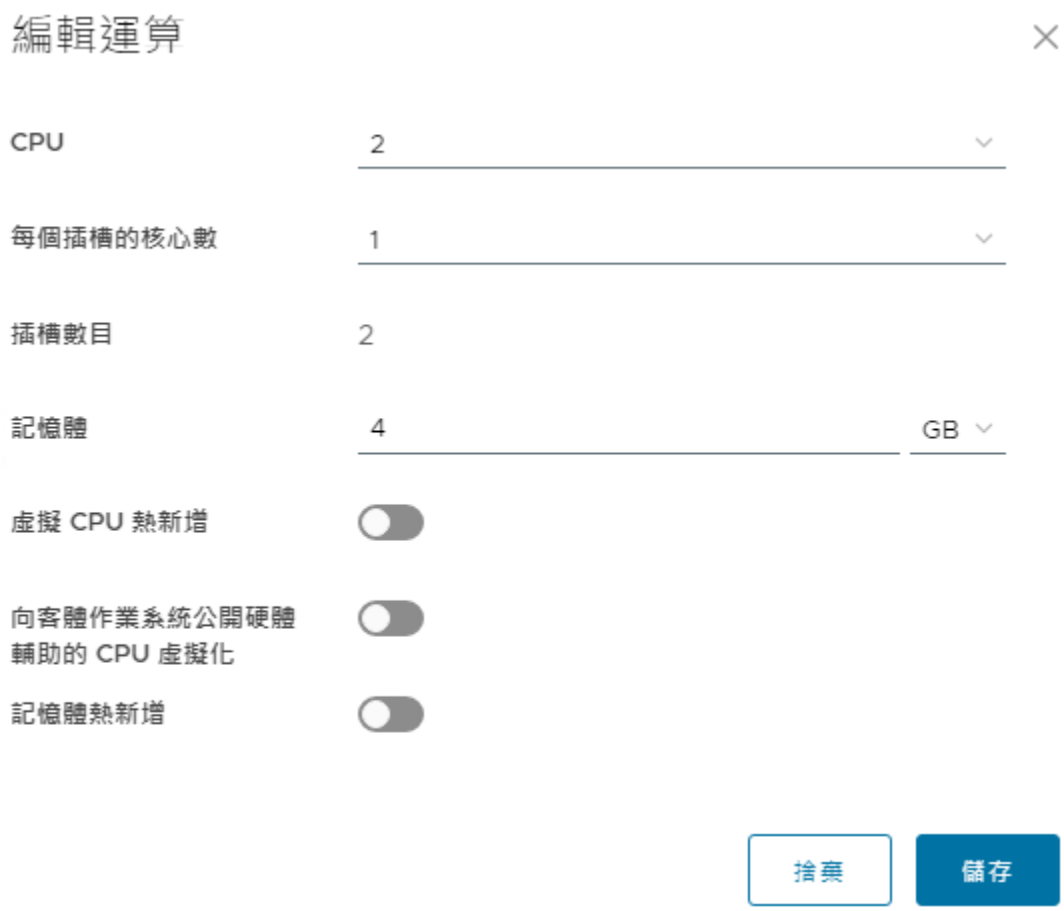
可以調整硬碟容量，以及額外新增或刪除硬碟。

計算

調整 VM 的 CPU、記憶體資源

這裡可以調整 CPU 數目與每個插槽的核心數，虛擬 CPU 熱新增若有打開，VM 開機時則限制，"每個插槽的核心數"無法熱新增。"虛擬 CPU 數目"與記憶體可熱新增，但只能加不能減，VM 關機後則可自由調整 CPU 與記憶體。

CPU 與記憶體熱新增，需 VM 關機才能套用，也要 VM OS 支援才能熱新增(win server 2016、2019 有支援)


編輯運算
CPU
2
每個插槽的核心數
1
插槽數目
2
記憶體
4
GB
虛擬 CPU 熱新增
向客體作業系統公開硬體輔助的 CPU 虛擬化
記憶體熱新增
捨棄
儲存

NIC

NIC 可以看到連線狀態、網卡類型、連接的網路(VDCNetwork)、IP 模式、MAC，點編輯可進去調整

可新增 NIC、調整連線狀態，要打勾才會連線；

網路介面卡類型建議可以選擇 VMXNET3，目前主流的 VM OS 都支援；

網路則是選擇套用的網段，在運算雲 3 平台，網段則是稱為 VDCNetwork。

VDCNetwork 可以設定一個 IP 集區。

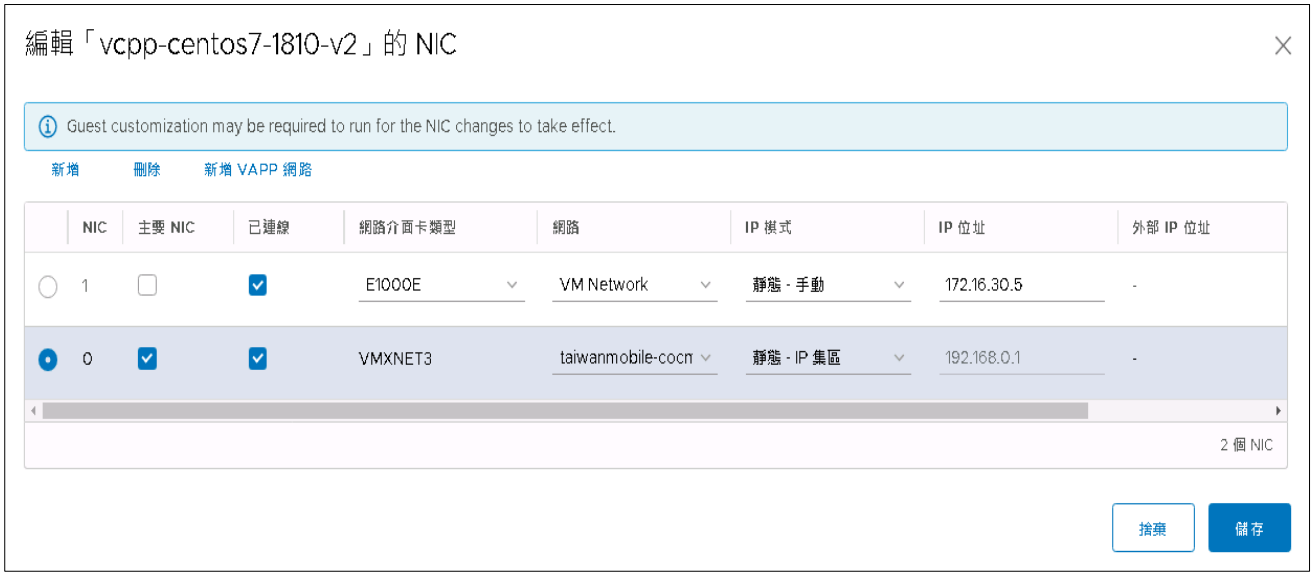
以下圖舉例，使用者規劃 192.168.0.1-192.168.0.200 這個 IP 區間作為 VM 可用 IP，此 IP 區間稱做 IP 集區。

重點:在 VM 開機狀態下，若修改 NIC 設定，則 VM 需使用客體自訂開機後，NIC 設定才會生效。

IP 模式-靜態-IP 集區:網卡從集區自動取走 IP，按照 192.168.0.1、192.168.0.2、192.168.0.3 的順序。

IP 模式-靜態-手動:可指定使用 IP 集區內的 IP。

IP 模式-DHCP:不使用 IP 集區，使用 Edge 的 DHCP 集區，前提是 DHCP 功能與 DHCP 集區要開啟與設定。



8.VM 資料加密

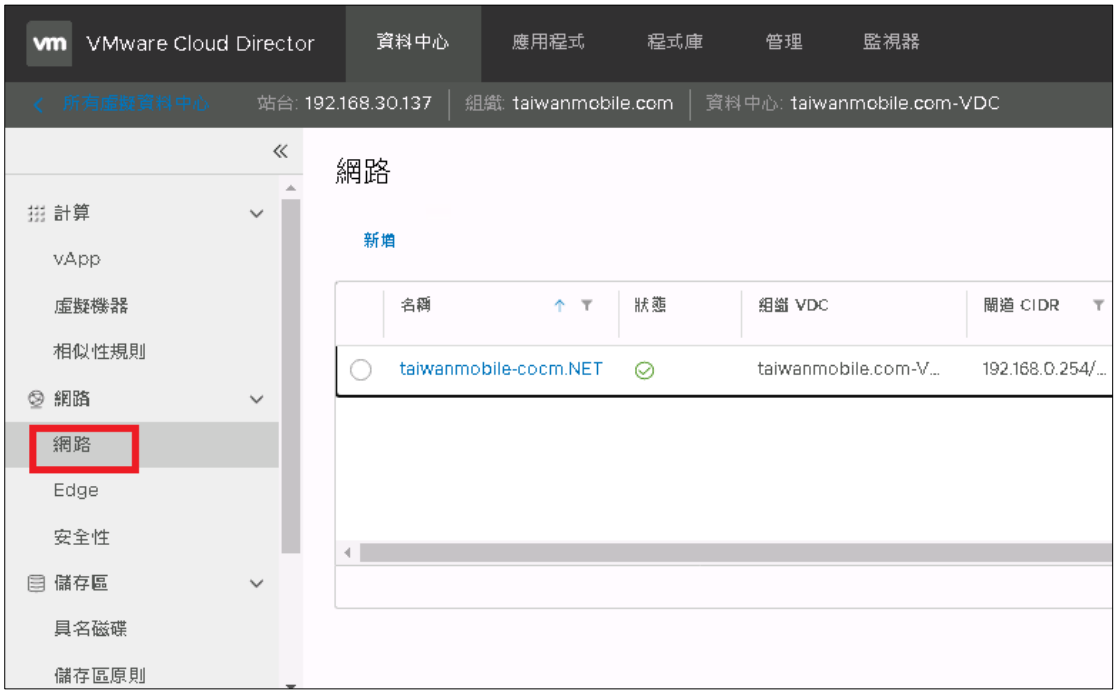
運算雲用戶若使用 Windows VM 作業系統，可透過 Windows 提供的檔案系統加密功能(Encrypting File System EFS)與 BitLocker 進行重要資料的保護，以防止檔案未經授權存取與盜竊者無法開啟檔案內容。
請參閱附件 A.《Windows Server 檔案與磁碟加密》

另若使用 Linux，如 CentOS，可使用 dm-crypt 增加安全性，加密的磁碟資料 即使 dump 出來，看到的也是亂碼。
請參閱附件 B.《Linux 磁碟加密說明》：以 CentOS 為製作範例

9.設定組織虛擬資料中心網路(VDCNetwork)

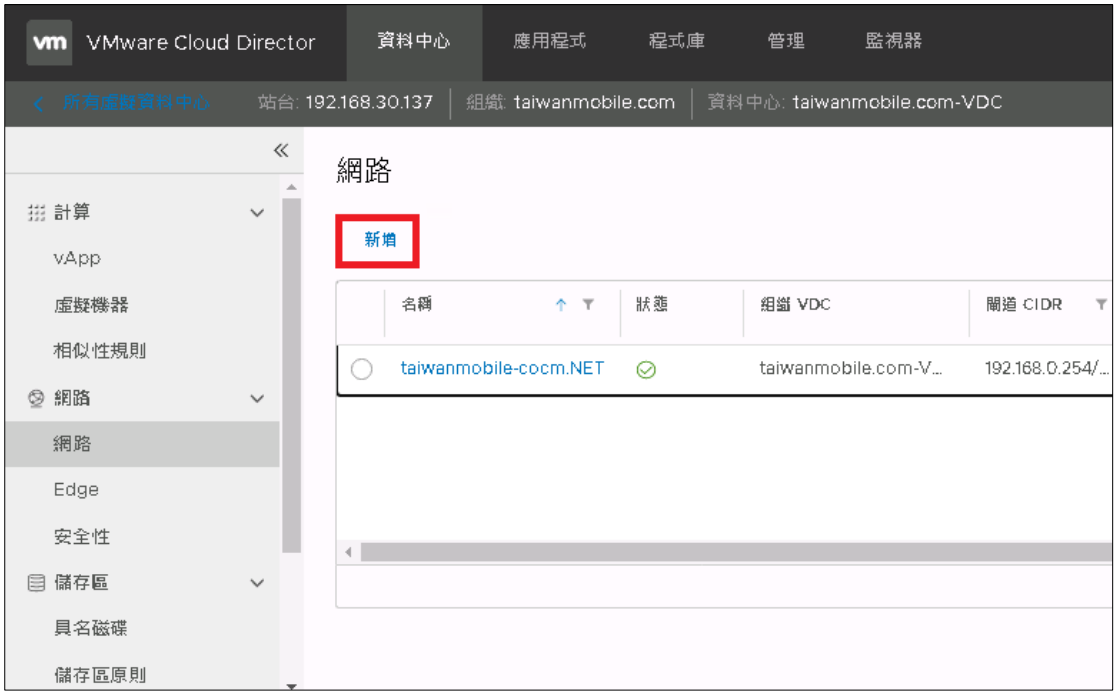
首頁→點擊 OVDC

到此就可開始設定虛擬資料中心網路



新增組織虛擬資料中心網路

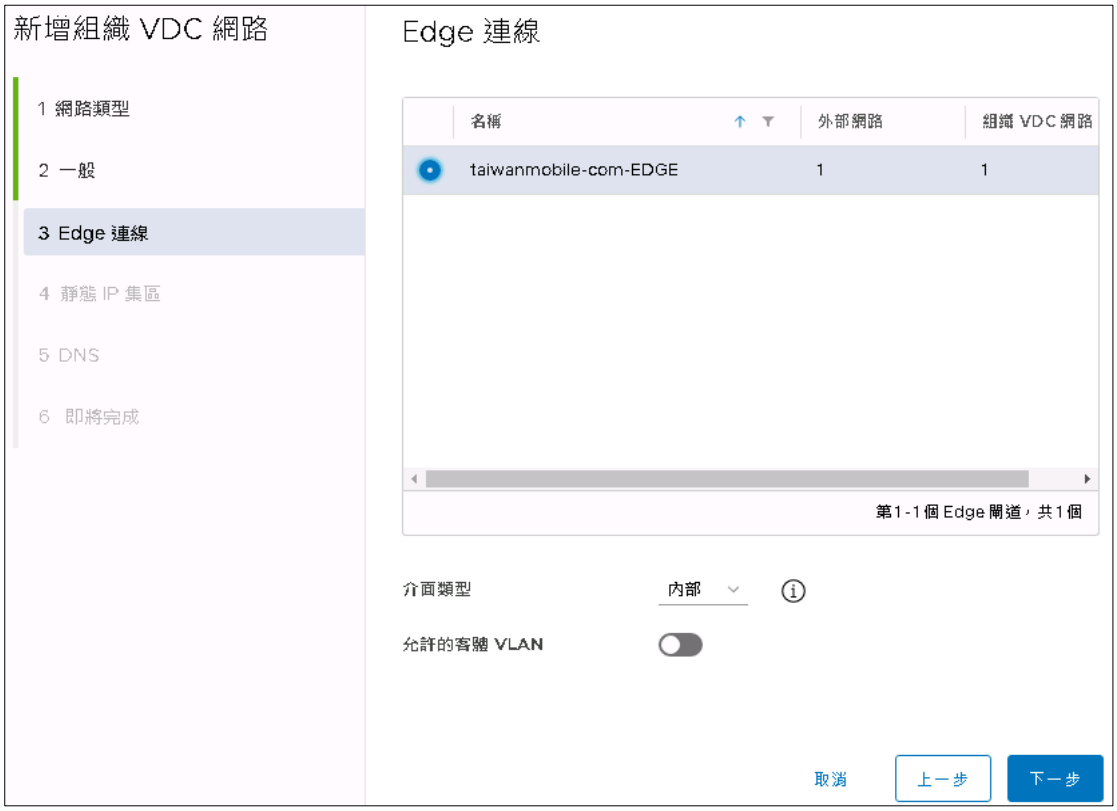
點選網路→新增



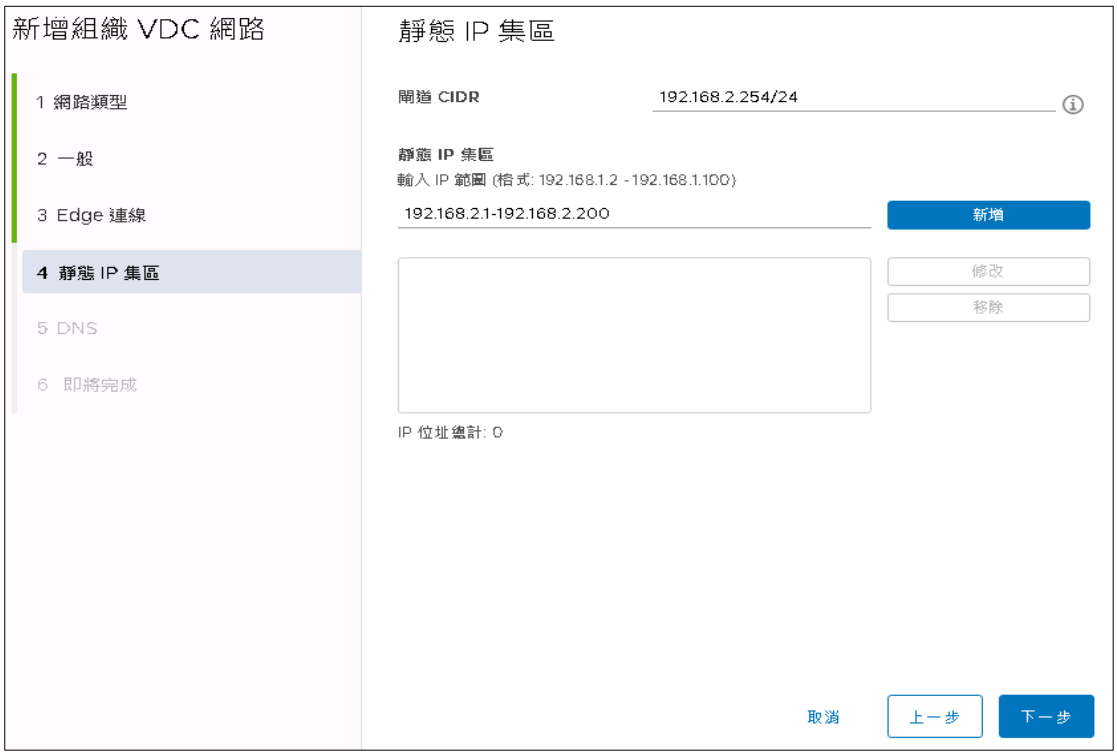
已隔離是完全封閉的網路，VM 要提供對外服務請選擇已路由

名稱請設定好辨識的名稱，閘道 CIDR 設定法為”閘道 IP/subnet mask”

選擇預設的 Edge，(允許的最大網路數目: 9)，介面類型維持預設的”內部”



靜態 IP 集區請以閘道 CIDR，擷取一段範圍，下圖就是設定 200 個 IP，新增後下一步。

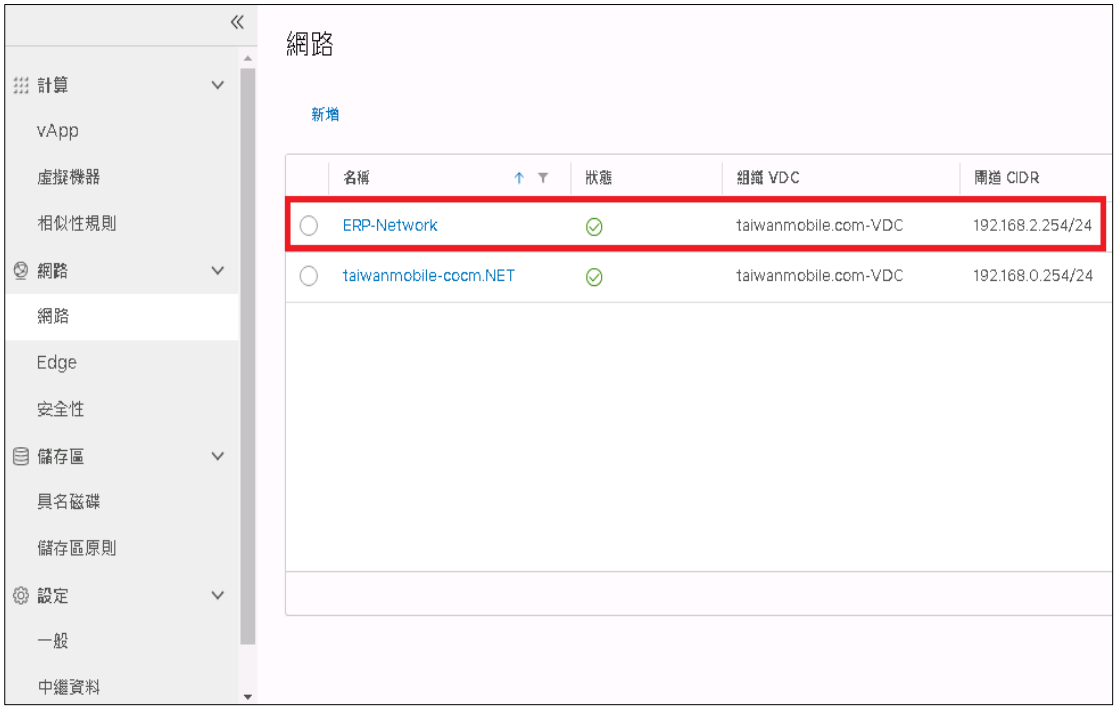


主要 DNS 預設會使用 Edge DNS，也可關掉自行指定 DNS，

次要 DNS 可以用台灣固網的 61.31.1.1，或自行指定。

最後再次檢查設定，到此就新增 VDCNetwork 完成。

回到網路頁面，會看到方才新增的設定。

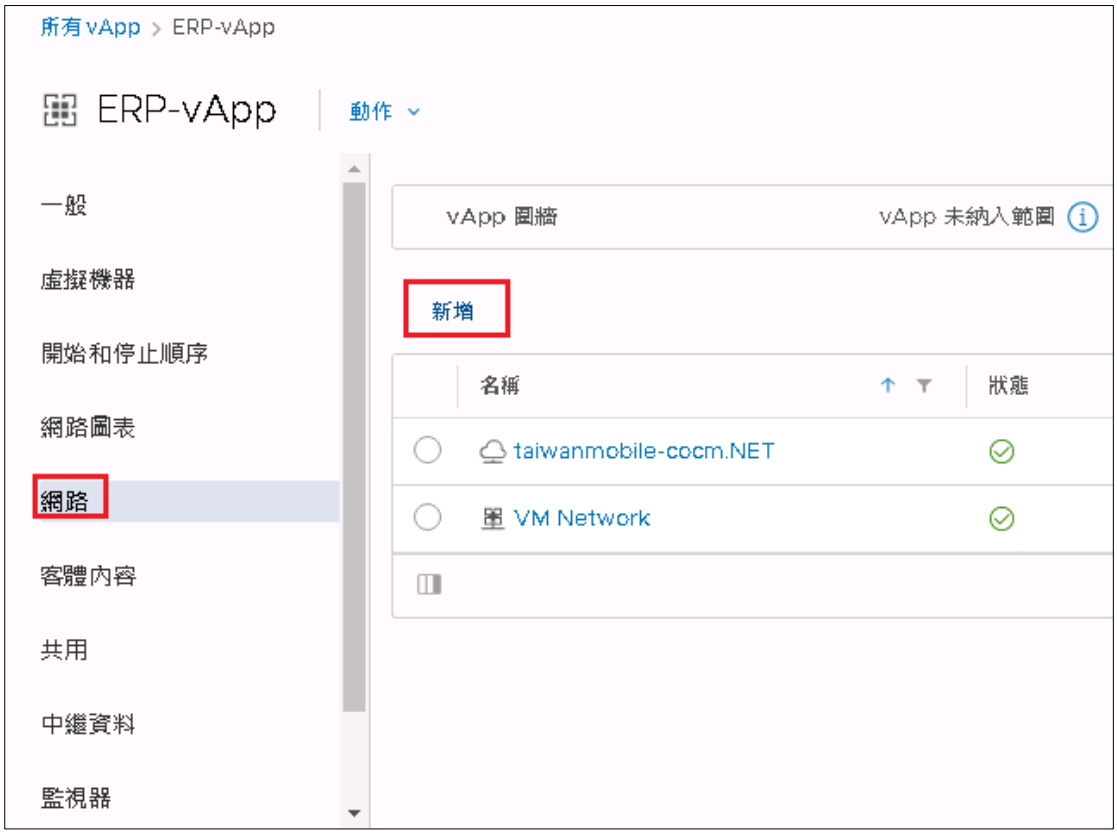


套用組織虛擬資料中心網路

之前建立的組織虛擬資料中心網路”ERP-Network”要套用到 vApp，找到要套用的 vApp 選擇詳細資訊

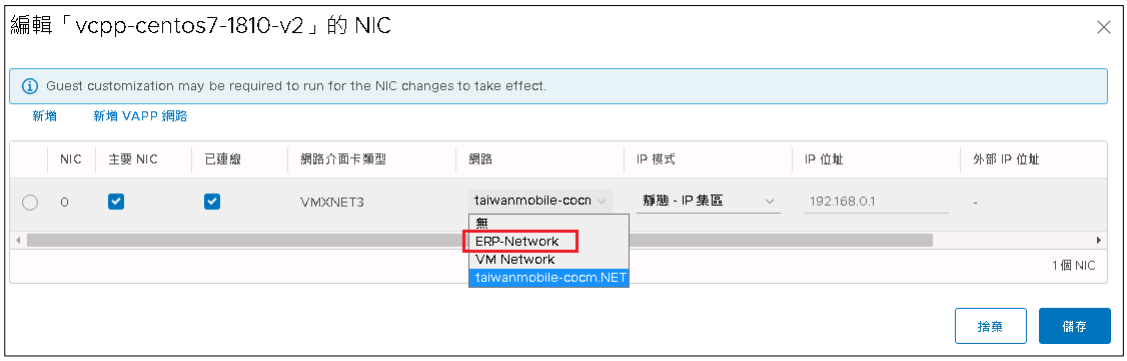

VMware Cloud Director
資料中心
應用程式
程式庫
管理
虛擬應用程式
虛擬機器
尋找依據: 名稱
進階篩選
排序依據: 名稱
1 個虛擬應用程式
已到期: 否
清除所有篩選器
新增
ERP-vApp
已開啟電源
租用
永不到期
建立於
2020/12/01 下午03:36:03
擁有者
admin
虛擬機器
管理
1
虛擬機器主控台
CPU
儲存區
記憶體
網路
1
18 GB
2 GB
2
徽章
動作
詳細資訊

網路→新增

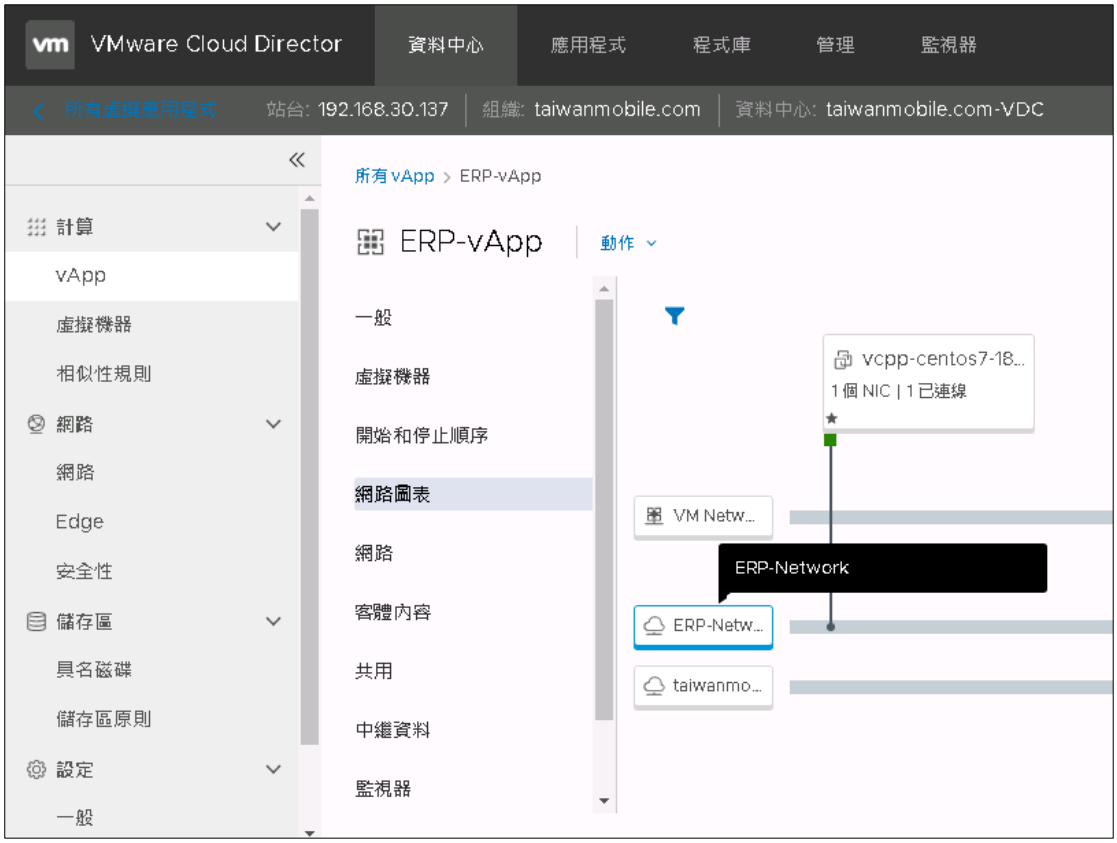


選擇組織 VDC 網路→選擇 ERP-Network→點選新增

此時在 ERP-vApp 裡的 VM NIC，就有”ERP-Network”網路可用。



在 vApp 裡的網路圖表，可以很清楚看到 VM 套用了那些網路。



10. Edge 管理

Edge 裡面有核心的網路相關設定，以下針對防火牆、DHCP、NAT、負載平衡器、IPSec VPN 功能做說明。

首頁→點選資料中心→Edge→點選設定→設定服務

這裡可以看到 Edge 的防火牆、DHCP、NAT、負載平衡器、IPSec VPN 功能

防火牆與 NAT 規則

這裡列舉最常用的三種需求，請參考對應的顏色。

1. **Web 服務:**允許外部任何來源可以連線 VM 的 80、443port。
2. **從外部辦公室直接連線 VM:**辦公室 public IP 60.199.134.2、或一段網段 60.199.135.0/24 可以 ssh、遠端桌面管理 VM。
3. **VM 連外:**預設防火牆是關閉，VM 無法連外；可把 VM IP 加到來源區塊，任何目的地、服務無限制。

VM 內部 IP 192.168.2.1，EDGE 的 Public IP 192.168.30.45

按照下圖防火牆與 NAT 的設定對應，即可滿足上述三種需求。

DHCP

之前若有設定組織虛擬資料中心網路的 IP 集區，這裡就可以不用設定。

VM 的網路卡可以選擇從 IP 集區或 DHCP 取得 IP。

這裡示範新增一條 DHCP 設定。

DHCP 服務預設關閉，可開啟。

新增 DHCP 集區可參考下圖範例，但 IP 設定需要與組織虛擬資料中心網路的網段要互通，且 IP 不要重複。

負載平衡器

以下以 2 台入口網站主機做附載平衡範例。

要使用附載平衡器，有三個地方需要設定，為全域組態、集區與虛擬伺服器。

在全域組態的狀態預設是沒有啟用，請改為啟用。

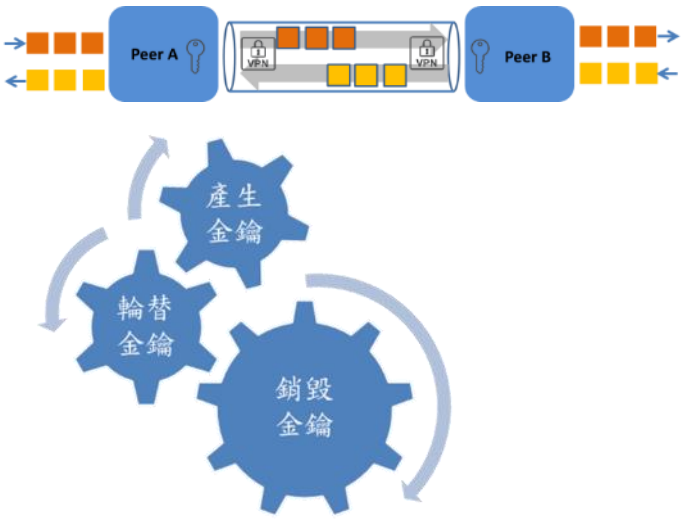
在集區的設定，新增一個集區，名稱取為好辨識的名稱，成員包含 2 台入口網站主機。

在虛擬伺服器的設定，新增一筆設定，套用之前建立好的集區設定。

到此附載平衡設定完成。

IPSec VPN

金鑰生命周期說明



- 產生金鑰: 設定預先共用金鑰(PSK)、金鑰演算法(例:SHA1)、金鑰交換演算法(例:Diffie-Hellman)，系統產生加密金鑰。
- 輪替金鑰: 系統於固定時間(lifetime)自動進行金鑰輪替。

- 銷毀金鑰: 變更共用金鑰，以銷毀既有金鑰。

設定方式:

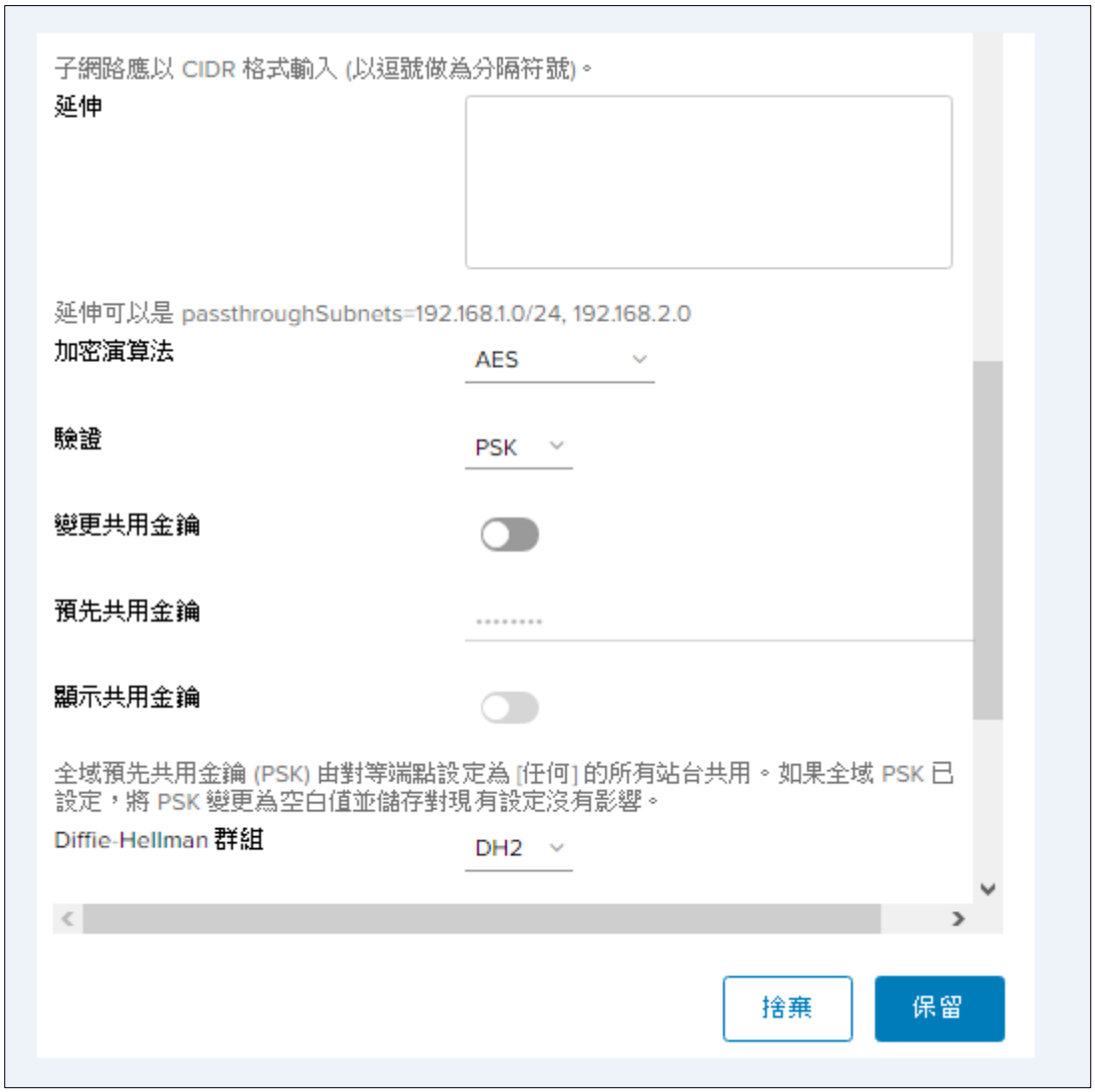
1. 開通防火牆，vcpp_edge_防火牆要放行另一端網段 IP,其餘 500 esp ah 設定完 ipsec 後會自動設定

2. 兩地端點資訊-設定範例

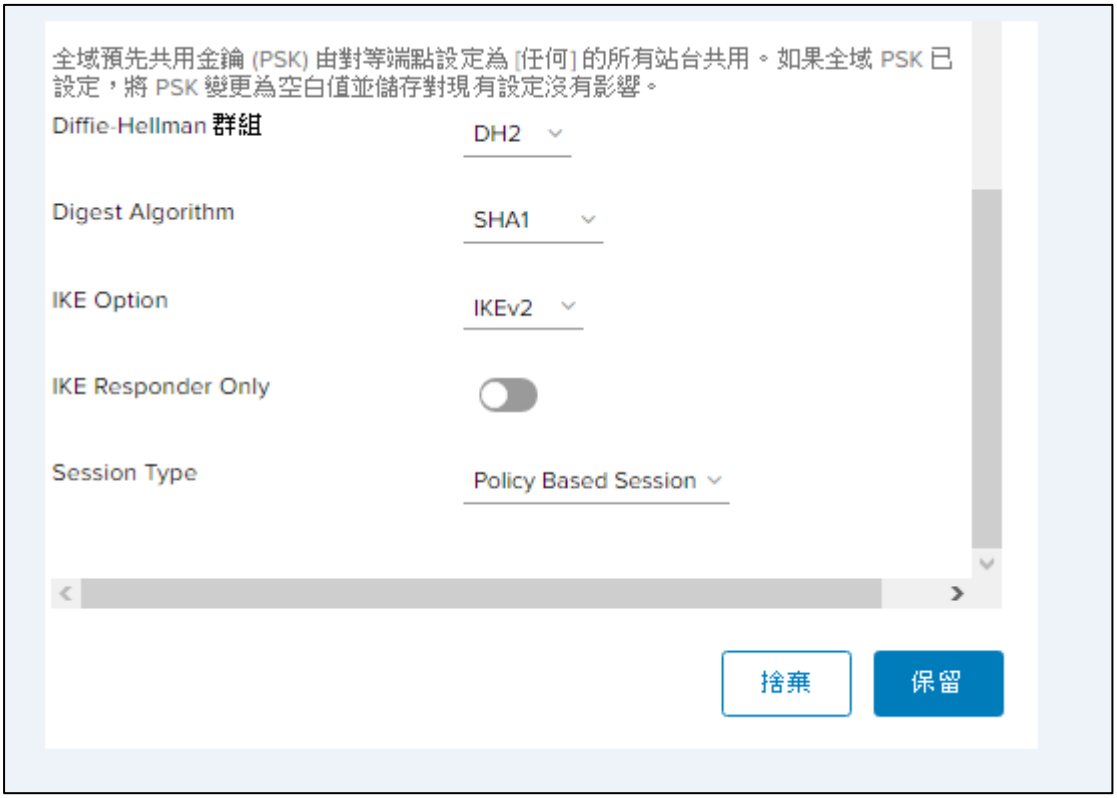
設定範例	Acompany.com	Bcompany.com	備註說明
名稱	vcpp-ptk	vcpp-ptk	易於辨識即可
本機識別碼	60.199.153.3	13.67.41.94	本機識別碼
本機端點	60.199.153.3	13.67.41.94	本地 WAN 端點
本機子網路	10.100.0.0/24	10.8.0.0/24	本地子網路
對等識別碼	13.67.41.94	60.199.153.3	對方識別碼

對等端點	13.67.41.94	60.199.153.3	對方 WAN 端點
對等子網路	10.8.0.0/24	10.100.0.0/24	對方子網路
加密演算法	AES	AES	兩地一致
驗證	PSK	PSK	兩地一致
預先共用金鑰	pass@123456	pass@123456	兩地一致

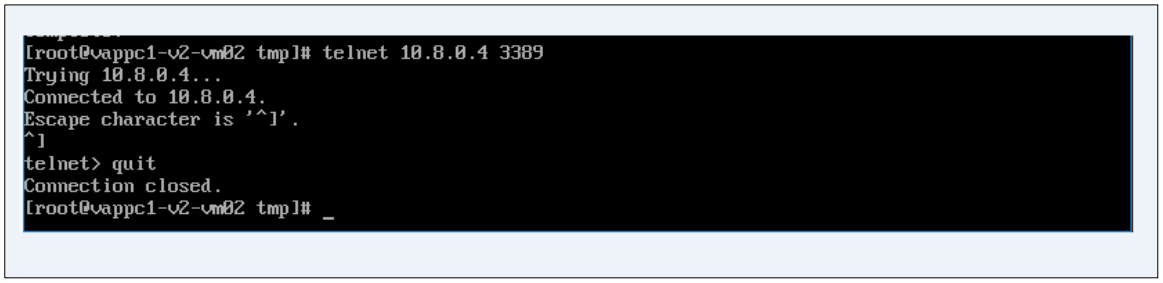
3. 以下設定兩端點的加密資訊,這裡通常是建立失敗的原因,兩端必須要互相匹配才可以建立成功

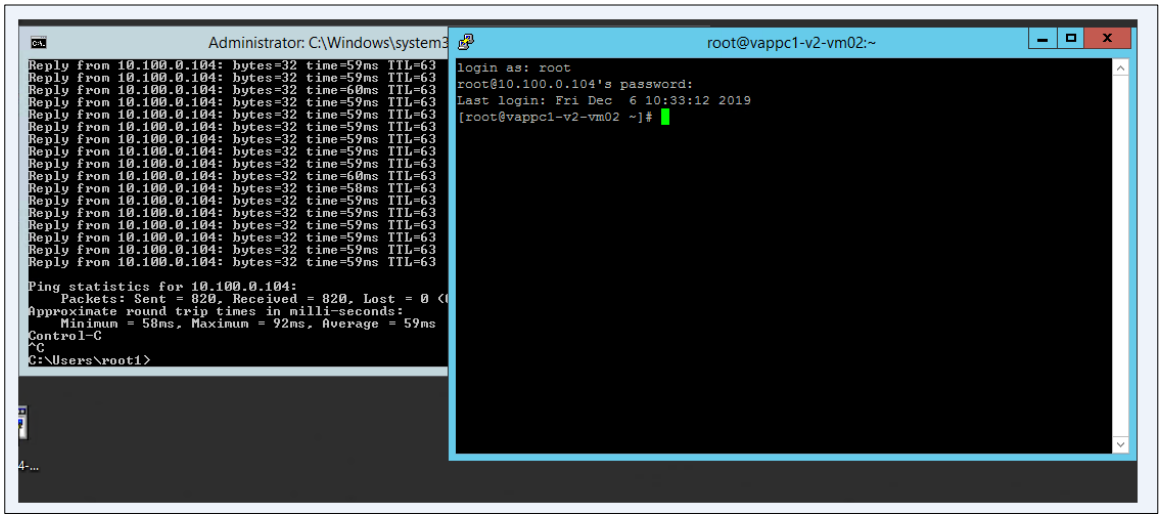


4. Session Type 選擇 Policy Base session



5. 驗證兩端點可互通(Guest OS 的防火牆也必須搭配開通服務)

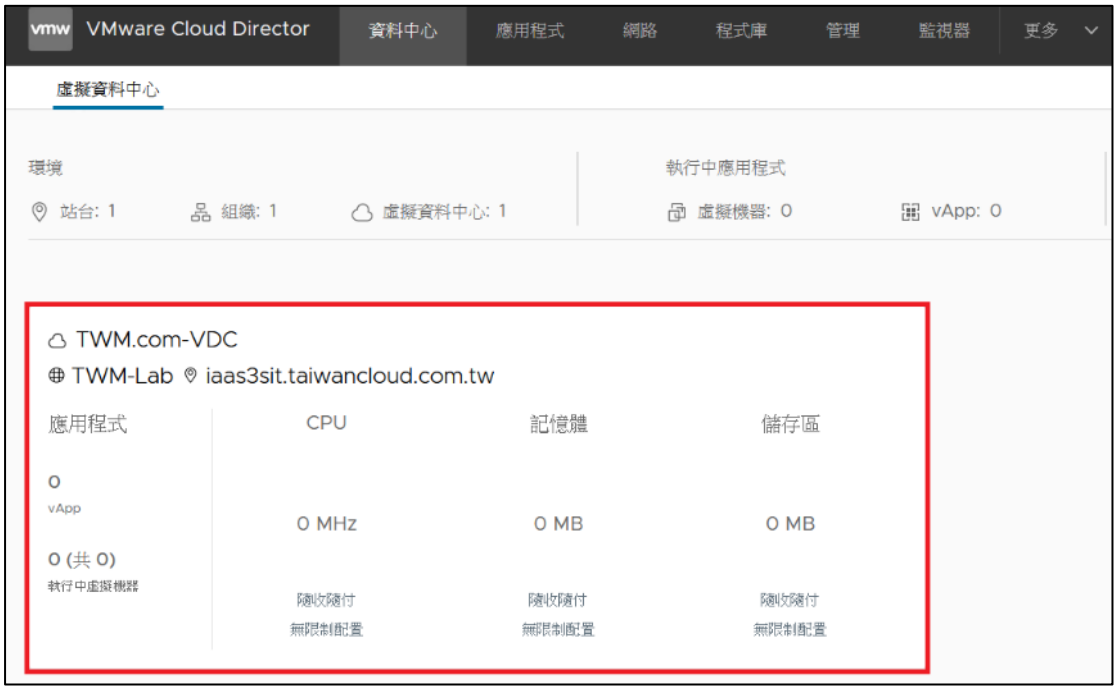




11. 新版-設定組織虛擬資料中心網路 (VDCNetwork)

※此章節適用 2023/9/5 後移轉用戶或新申裝用戶參考。

首頁→點選資料中心。



點選網路就可以開始設定虛擬資料中心網路。

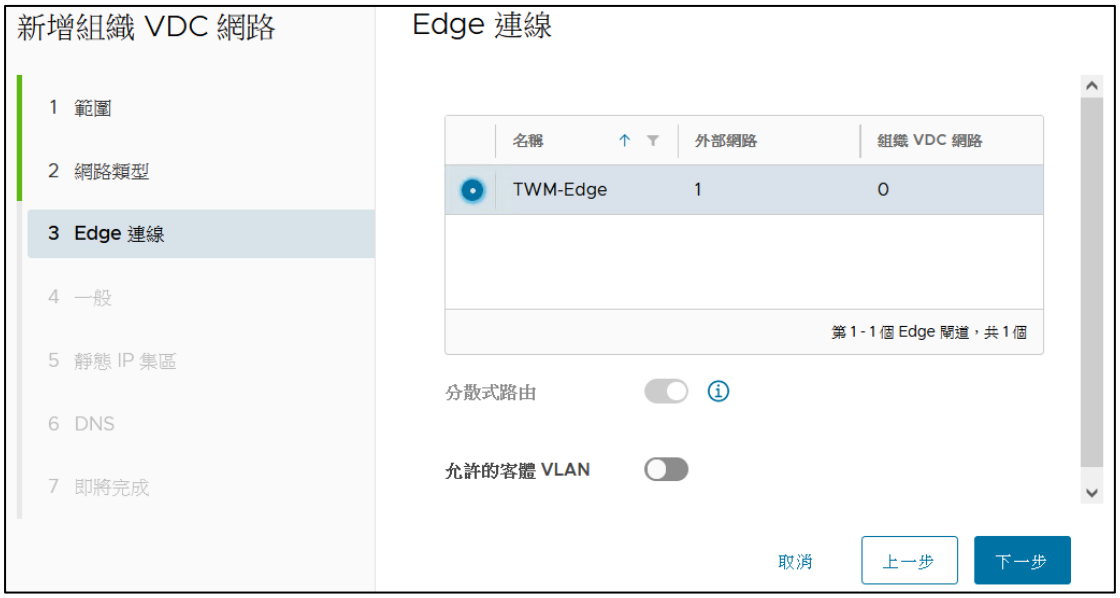
新增組織虛擬資料中心網路

點選網路→新增。

預設選擇為目前組織虛擬資料中心。

已隔離是完全封閉的網路，VM 要提供對外服務請選擇已路由。

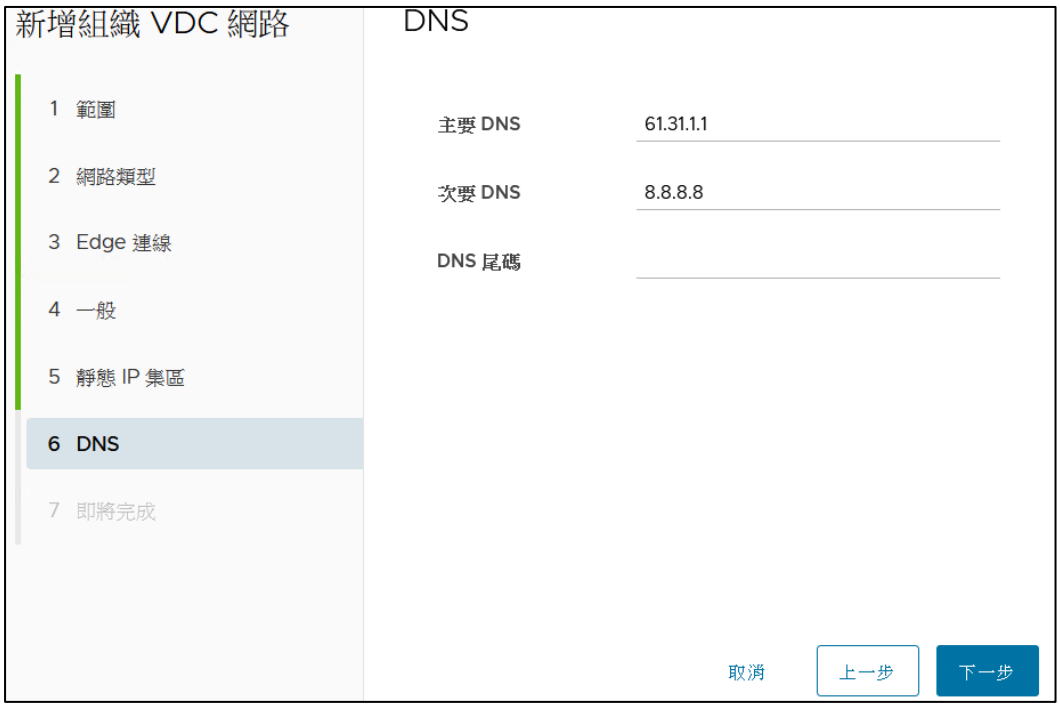
選擇已配發的 Edge。



名稱請設定好辨識的名稱，閘道 CIDR 設定法為[閘道 IP/subnet mask]。

靜態 IP 集區請以閘道 CIDR，擷取一段範圍，下圖就是設定 200 個 IP，新增後下一步。

可自行指定 DNS Server，建議設定台灣固網 DNS 61.31.233.1 與 61.31.1.1 或其他如 8.8.8.8(google)。



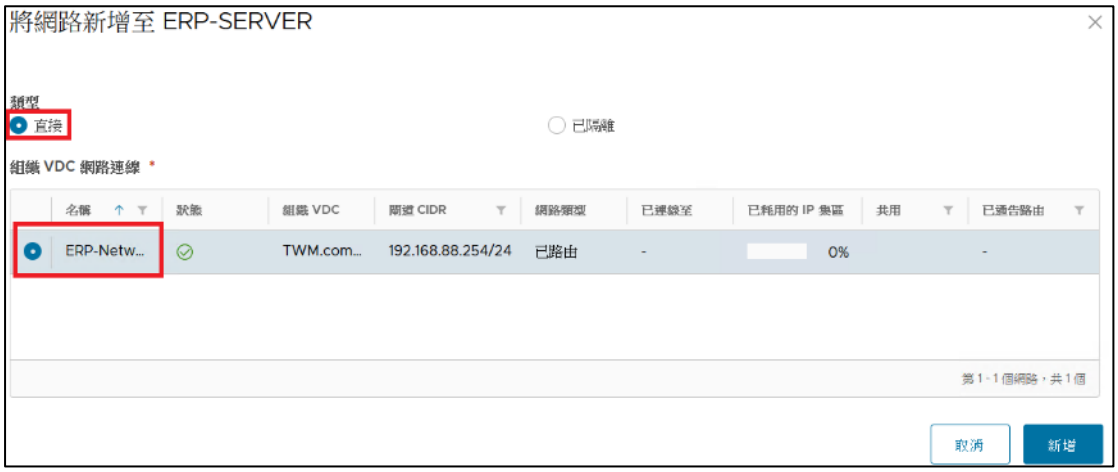
最後再次檢查設定，到此就新增 VDCNetwork 完成。

套用組織虛擬資料中心網路

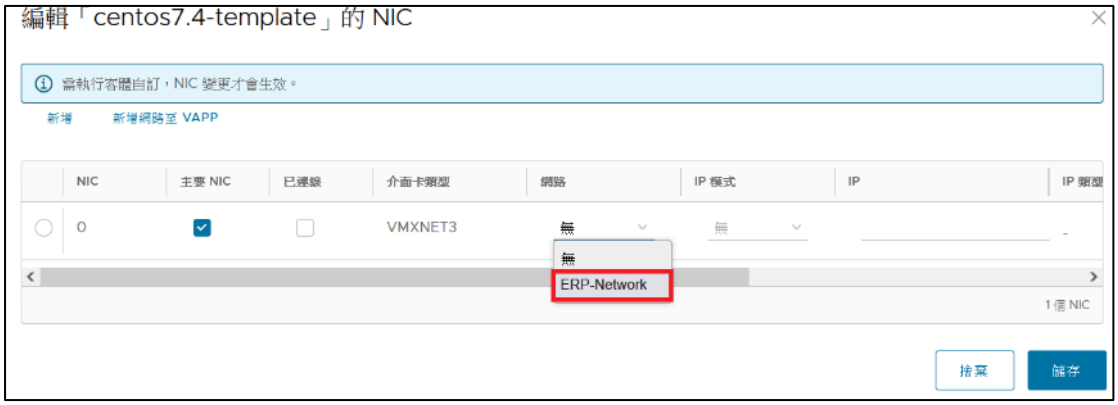
之前建立的組織虛擬資料中心網路”ERP-Network”要套用到 vApp，找到要套用的 vApp 選擇詳細資訊。

網路→新增。

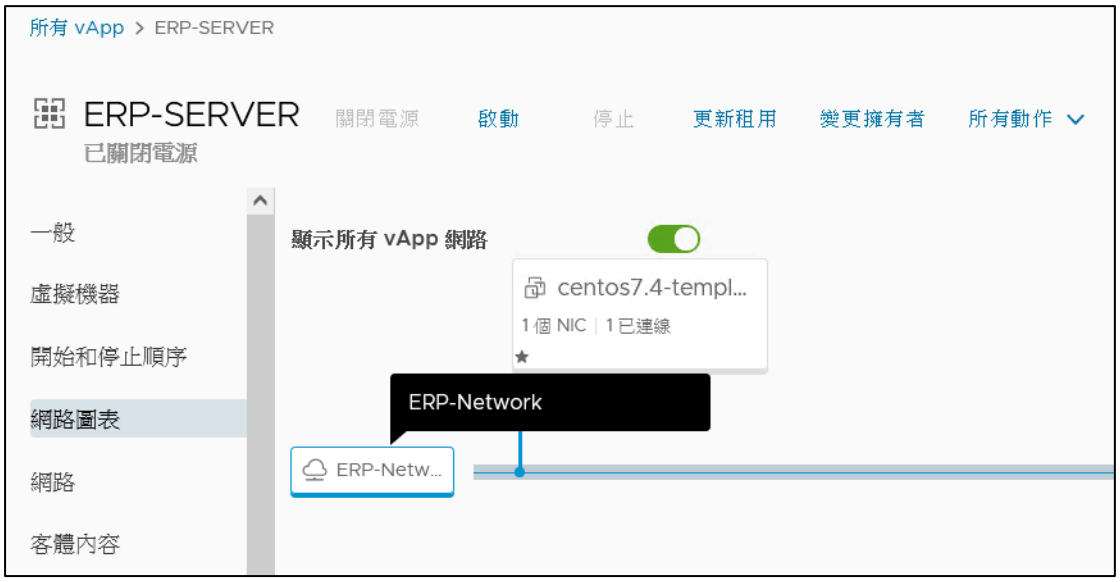
選擇直接→選擇 ERP-Network→點選新增。



此時在 ERP-SERVER 裡的 VM NIC，就有”ERP-Network”網路可用。



在 vApp 裡的網路圖表，可以很清楚看到 VM 套用網路的情形。



組織虛擬資料中心網路啟用 DHCP 服務

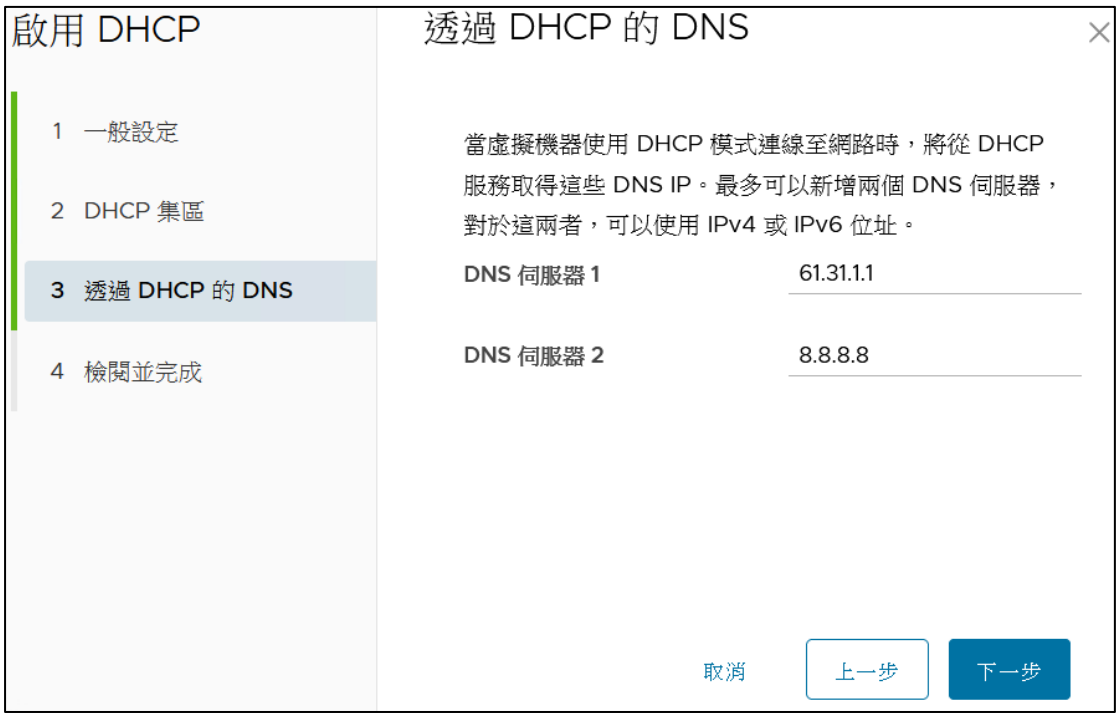
先到網路的分頁，點選要開啟 DHCP 功能的 VDCNetwork。

點選 DHCP，預設為關閉，若為首次使用會出現啟用的訊息。

選取閘道模式。

填入該 VDCNetwork 同網段範圍 IP，並注意不能與先前設定 VDCNetwork 靜態 IP 集區 IP 重疊。

DNS 建議設定台灣固網 DNS 61.31.233.1 與 61.31.1.1 或其他如 8.8.8.8(google)。



檢視相關設定。

回到 DHCP 頁面可編輯設定或停用該服務。

虛擬機器套用 DHCP，可至虛擬機器的 NIC 進行編輯。

將 IP 模式調整為 DHCP，根據提示執行客體自訂，NIC 變更才會生效。

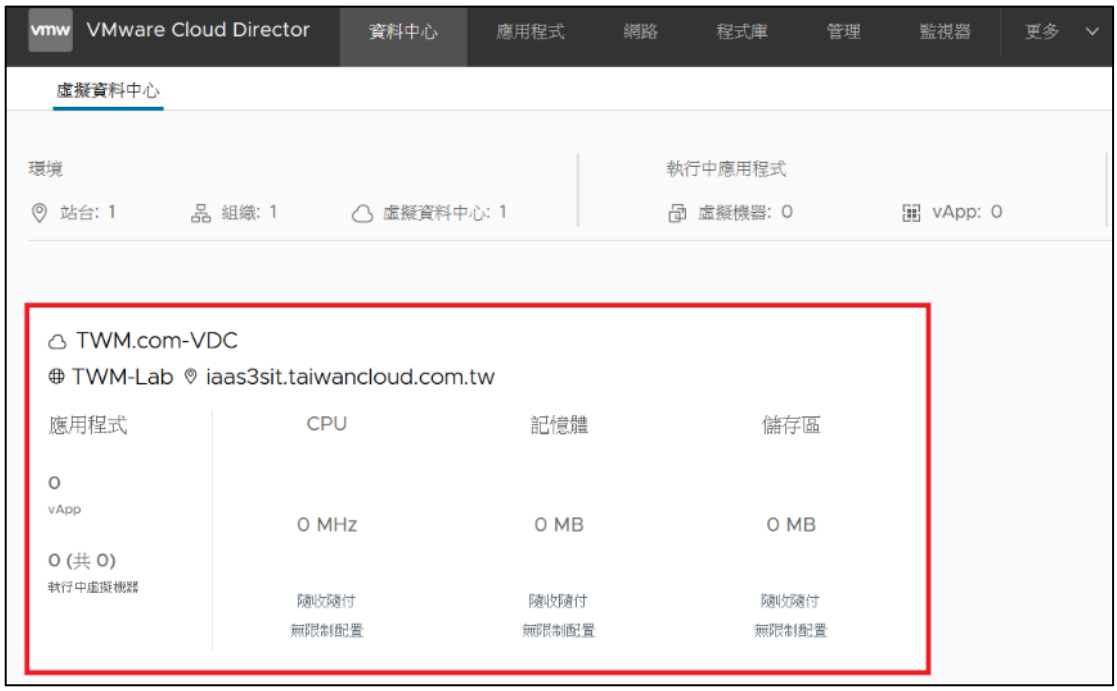
再次檢視虛擬機器已改用 DHCP 模式取得到 IP。

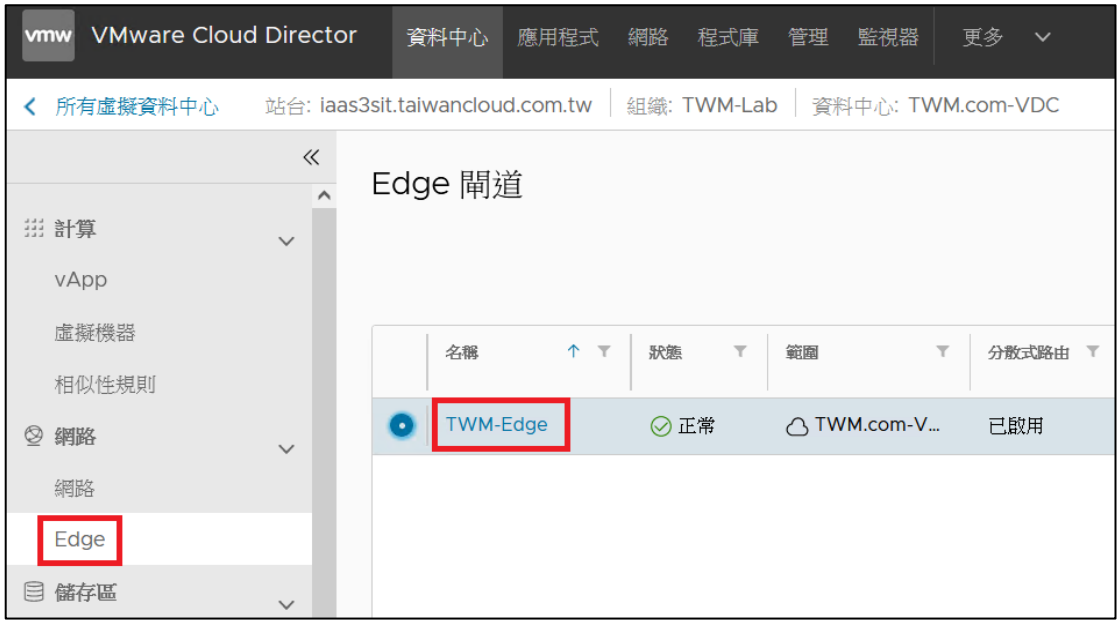
12. 新版-Edge 管理

※此章節適用 2023/9/5 後移轉用戶或新申裝用戶參考。

Edge 裡面有核心的網路相關設定，以下針對防火牆、NAT、負載平衡器、IPSec VPN 功能做說明。

首頁→點選資料中心→Edge→點選需設定 Edge→進入相關設定。






TWM-Edge
在 VDC 內容中開啟
組態
一般
速率限制
服務
防火牆
NAT
IPSec VPN
負載平衡器
一般設定
安全性
靜態群組
IP 集
應用程式連接埠設定檔
IP 管理
IP 配置
DNS
一般
名稱
TWM-Edge
狀態
正常
說明
-
允許非分散式路由
否
類型
NSX-T
已連線
是
使用專用提供者路由器
否
範圍
組織虛擬資料中心
TWM.com-VDC
組織
TWM-Lab

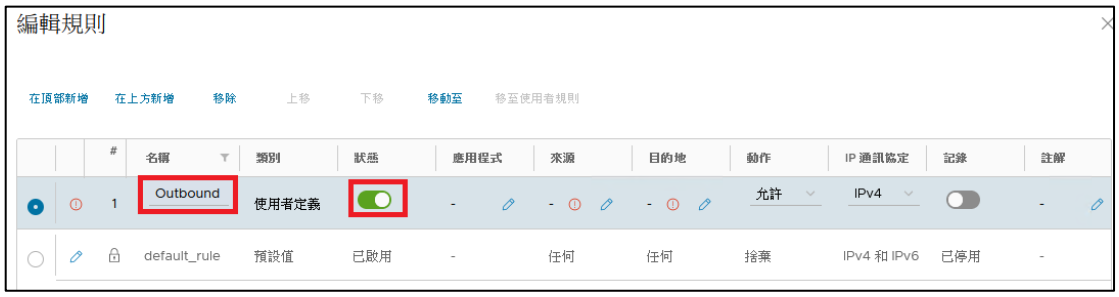
防火牆與 NAT 規則

防火牆→編輯規則

安全性因素防火牆會有一筆預設任何方向為捨棄封包的規則。

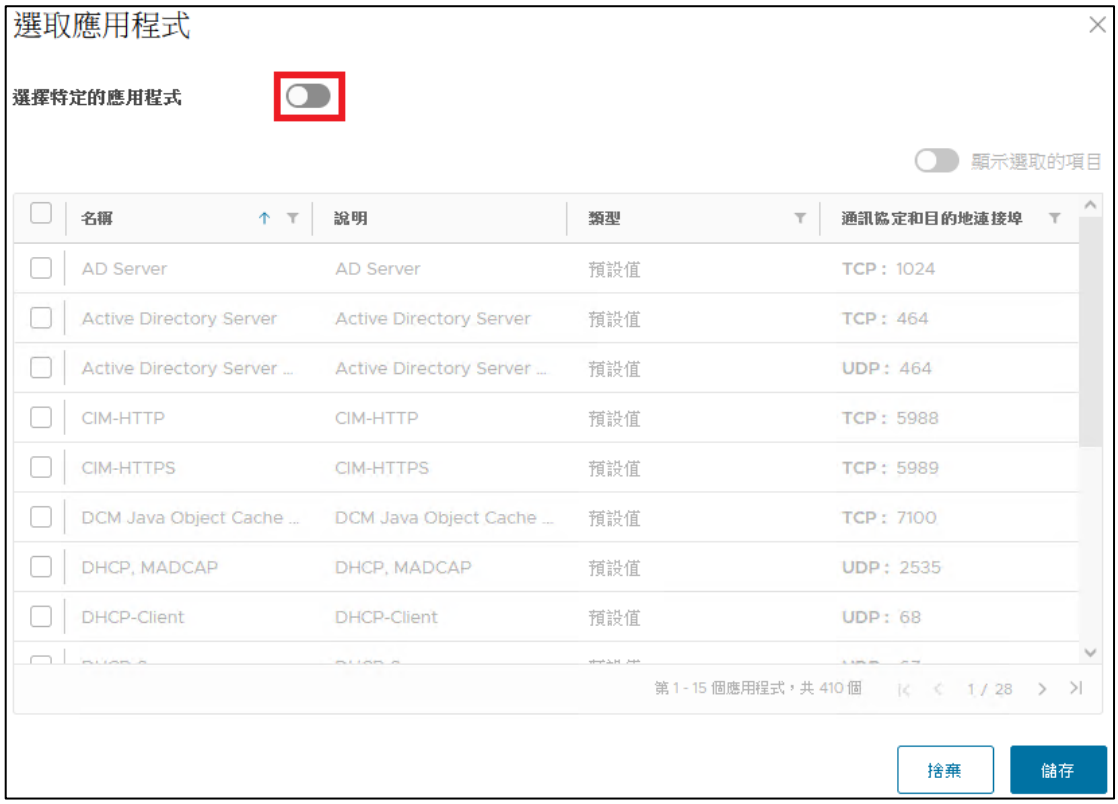
點選新增調整 Edge 防火牆規則。

填入可識別規則名稱，預設為規則啟用狀態。

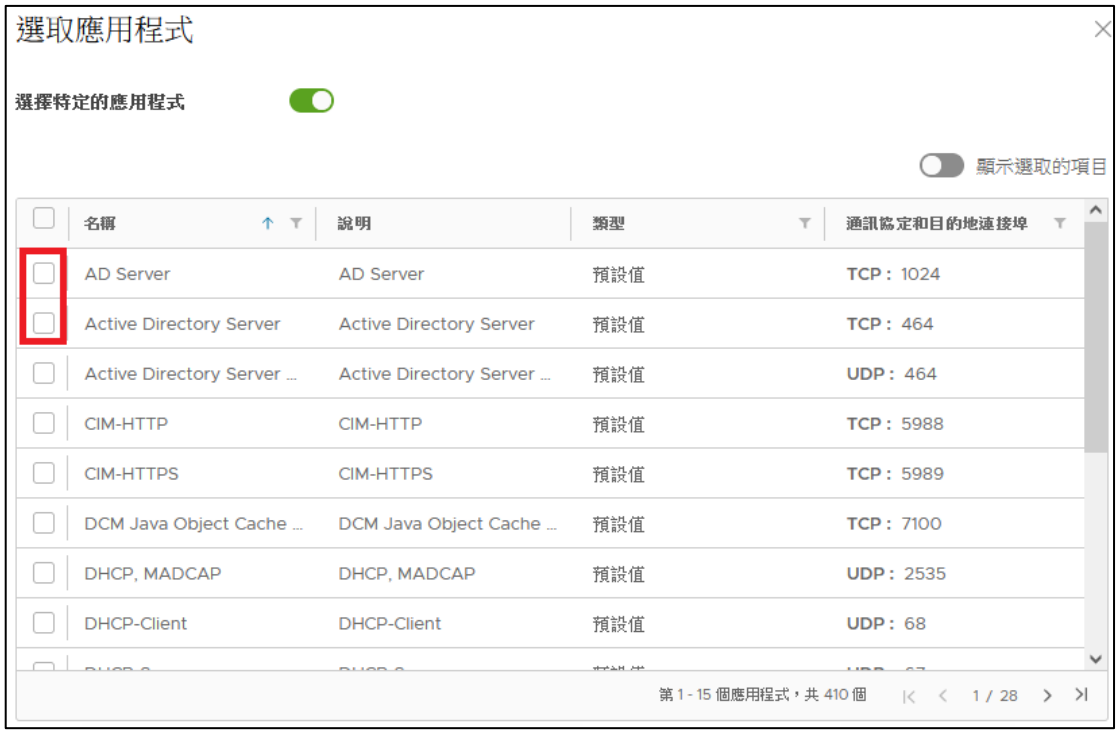


在應用程式點選鉛筆符號，進入編輯。

將選擇特定的應用程式啟用就能選擇特定連接埠(TCP/UDP)



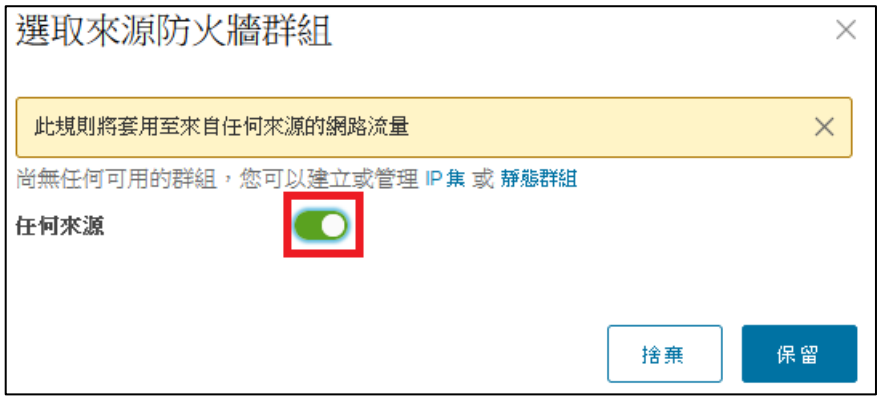
勾選想要使用的連接埠。



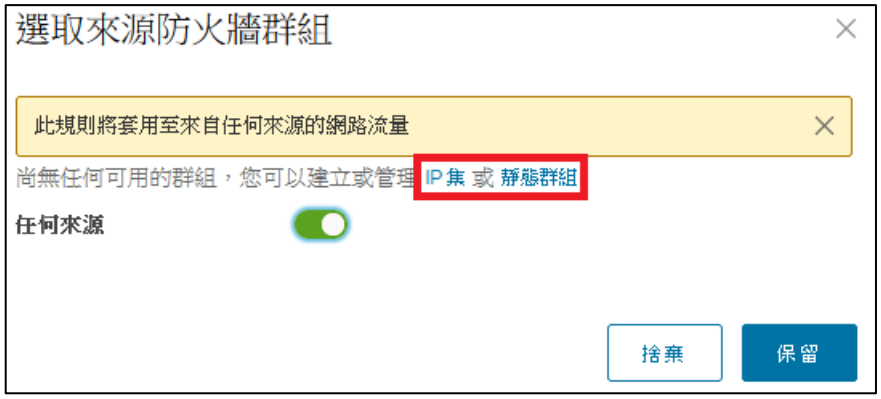
亦可在右邊進行快速篩選。

點選來源、目的地鉛筆符號進入編輯頁面。

不指定 IP 或群組，可將任何來源狀態選為啟用



若需指定則可依需求新增 IP 集或靜態群組，可由此處快速連結至對應頁面。

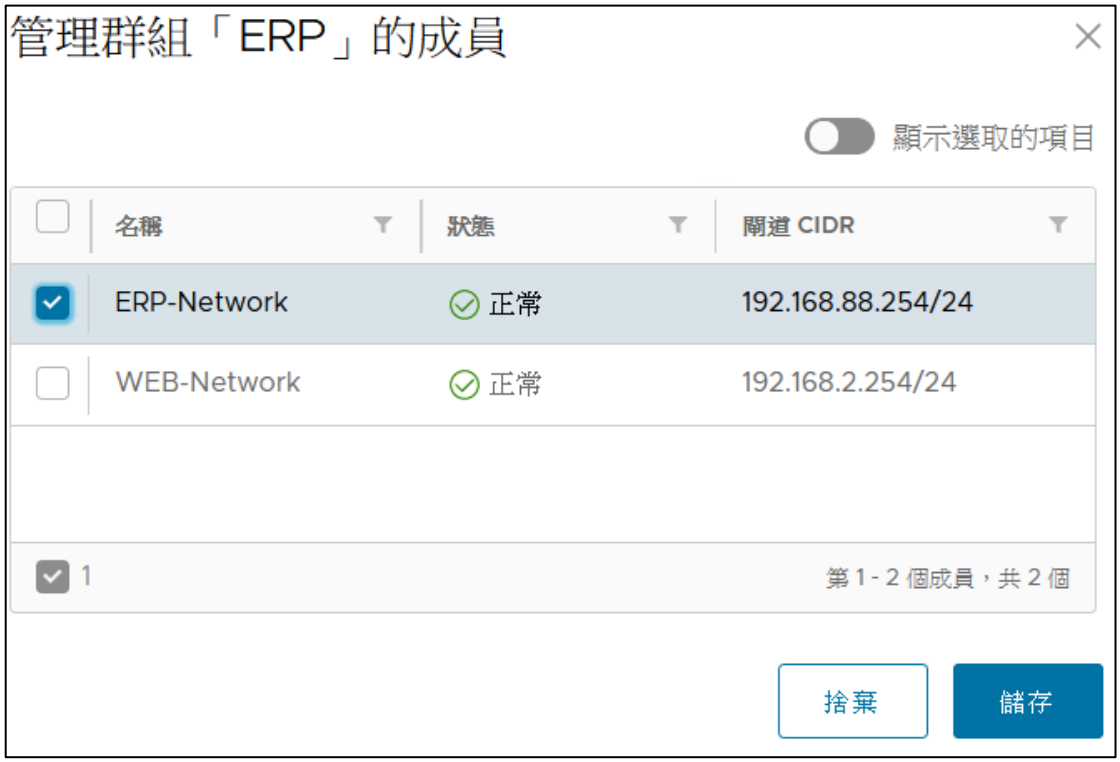


新增靜態群組

填入可識別名稱

選取 ERP 靜態群組→管理成員

靜態群組是透過選取 VDCNetwork，關聯使用該 VDCNetwork 的虛擬機器列為群組。



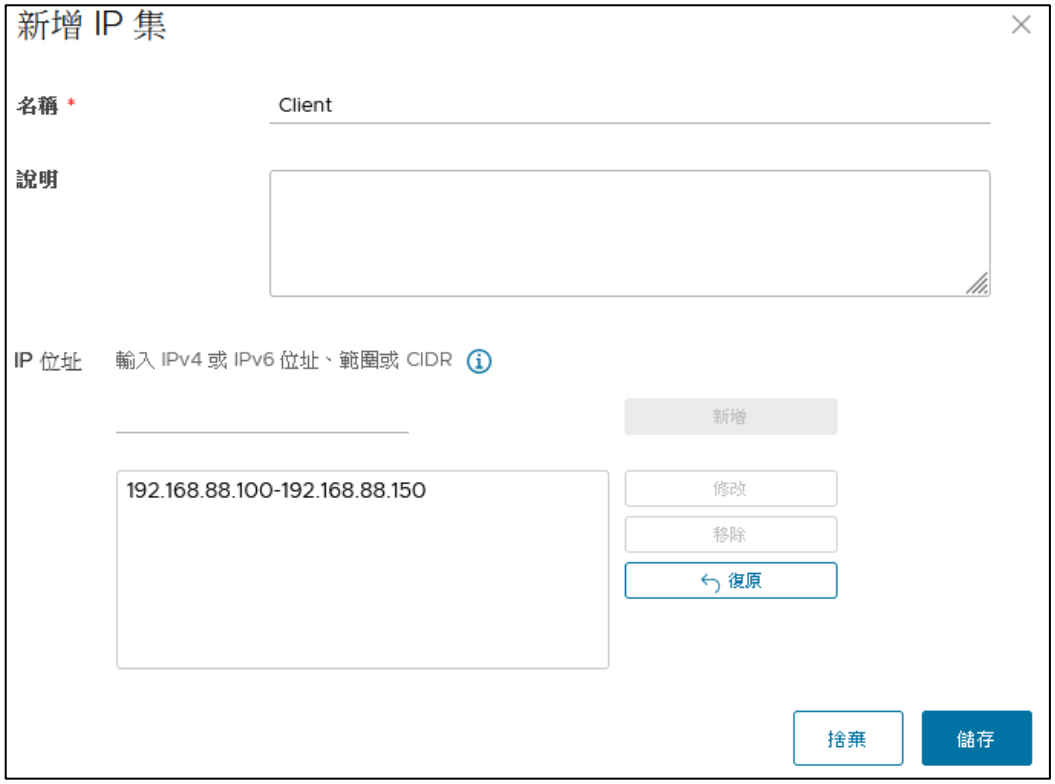
選取相關聯的虛擬機器，可以查看已關聯的虛擬機器。


群組「ERP」的相關聯虛擬機器
虛擬機器
虛擬應用程式
centos7.4-template
ERP-SERVER
確定

防火牆規則群組除了可使用靜態群組亦可使用 IP 集的方式

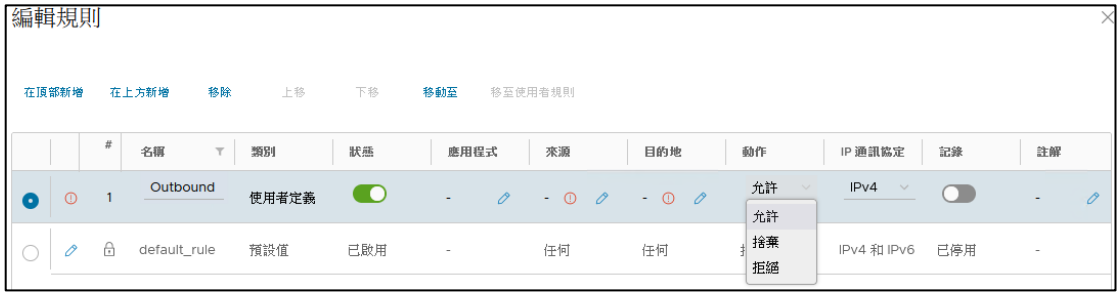
填入可識別名稱。

IP 位址可以用 CIDR 標記法輸入，可支援輸入單一 IP、範圍 IP、網段。

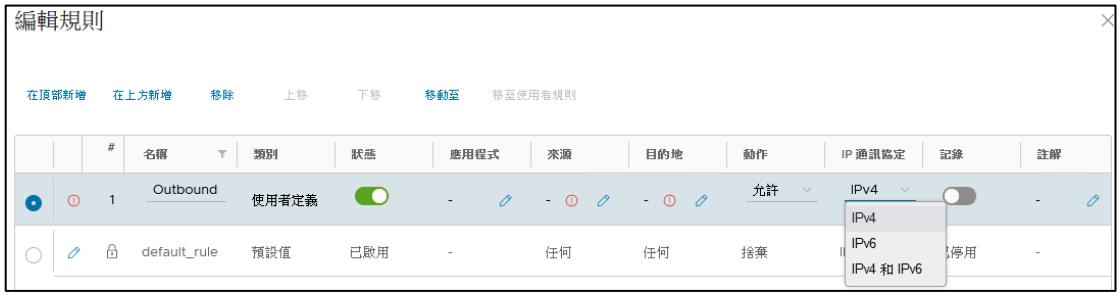


回到防火牆規則新增，在來源及目的地就能指定上述所透過 IP 集和靜態群組新增出來的物件群組。

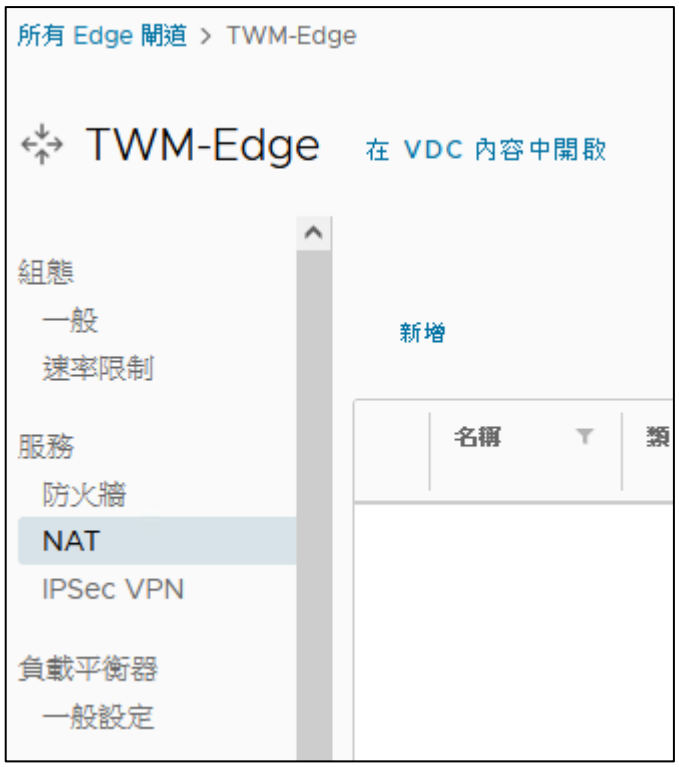
規則的動作選項分為允許、捨棄、拒絕，可依需求進行調整。



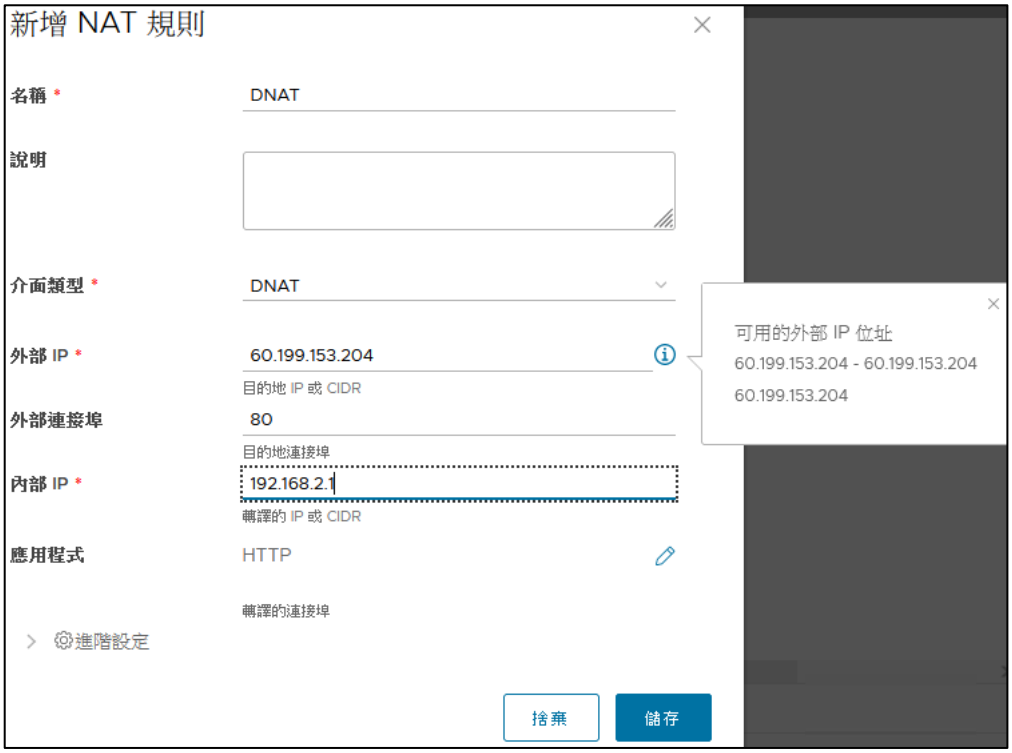
規則的 IP 通訊協定選項分為 IPv4、IPv6、IPv4 和 IPv6，可依需求進行調整。

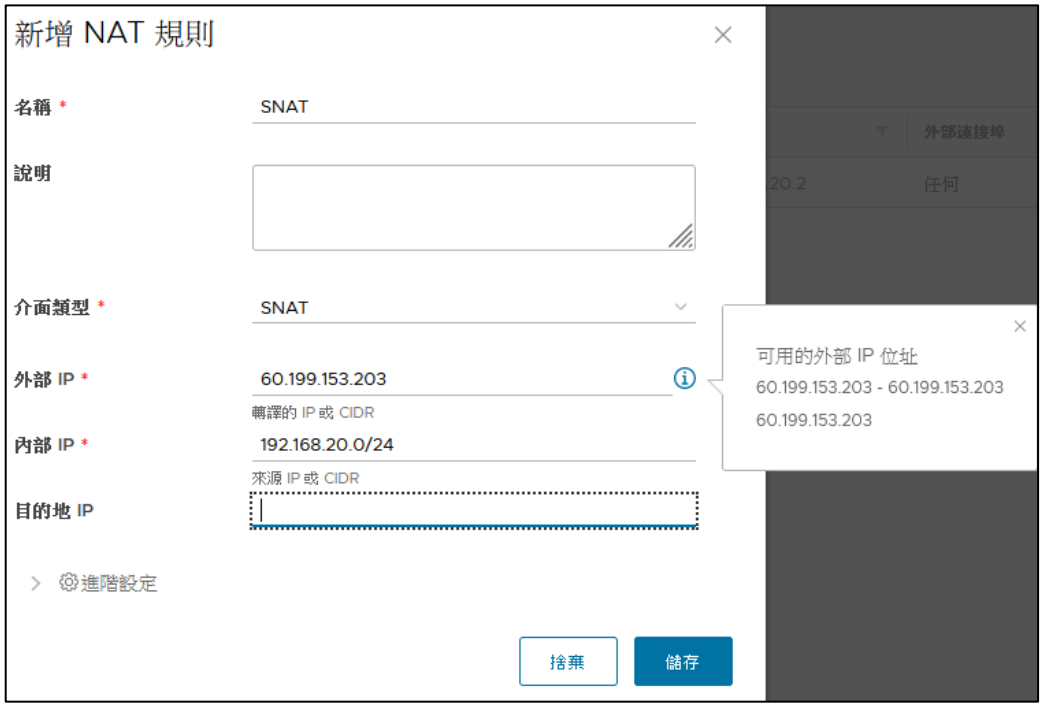


NAT 與防火牆關聯性極高，設定 NAT 可從 NAT 分頁→點選新增。



可依需求調整介面類型選為 DNAT 或 SNAT，外部 IP 可點選旁邊ⓘ快速檢視可用的外部 IP，內部 IP 為需進行 NAT 轉換的虛擬機器 IP。



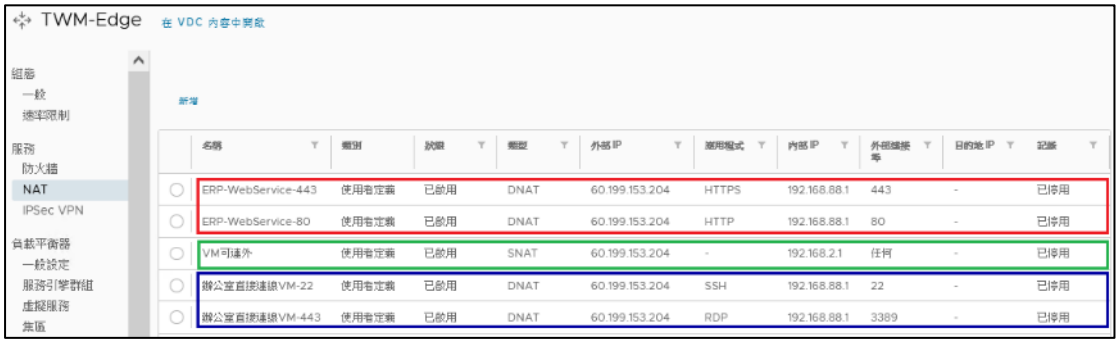


依據上述說明，這裡列舉防火牆與 NAT 組合最常見的三種情境，請參考對應的顏色。

1. **Web 服務:**允許外部任何來源可以連線 VM 的 80、443port。
2. **從外部辦公室直接連線 VM:**辦公室 public IP 60.199.134.2、或一段網段 60.199.135.0/24 可以 ssh、遠端桌面管理 VM。
3. **VM 連外:**預設防火牆是關閉，VM 無法連外；可把 VM IP 加到來源區塊，任何目的地、服務無限制。

VM 內部 IP 192.168.2.1，EDGE 的 Public IP 192.168.30.45

按照下圖防火牆與 NAT 的組合設定，即可滿足上述三種情境。

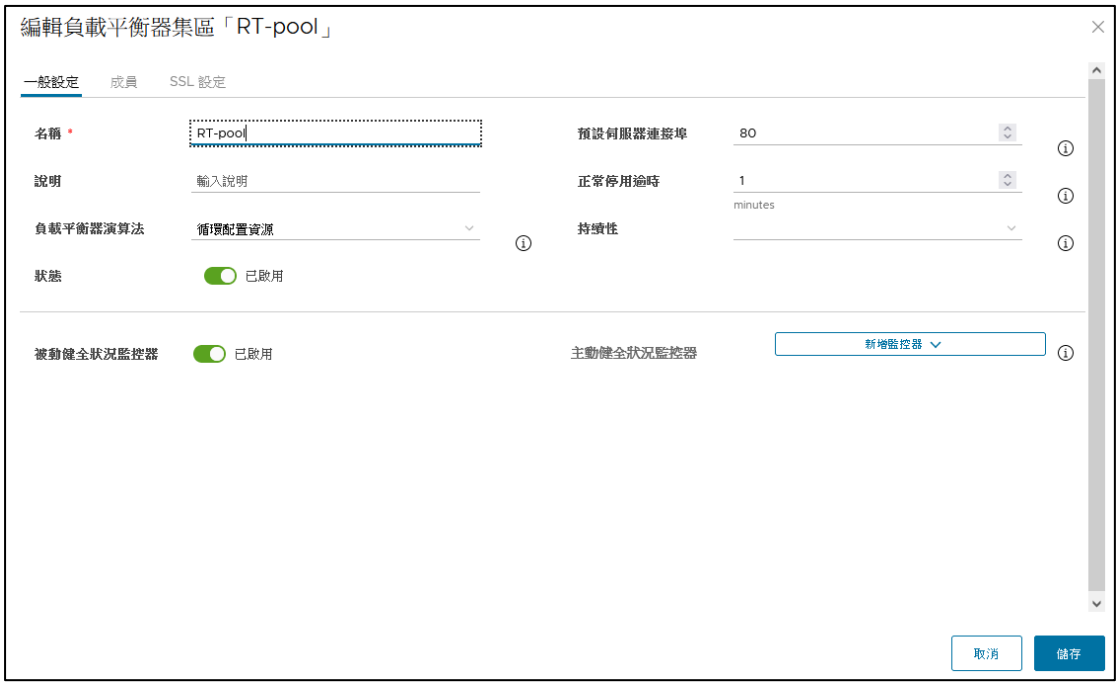


負載平衡器

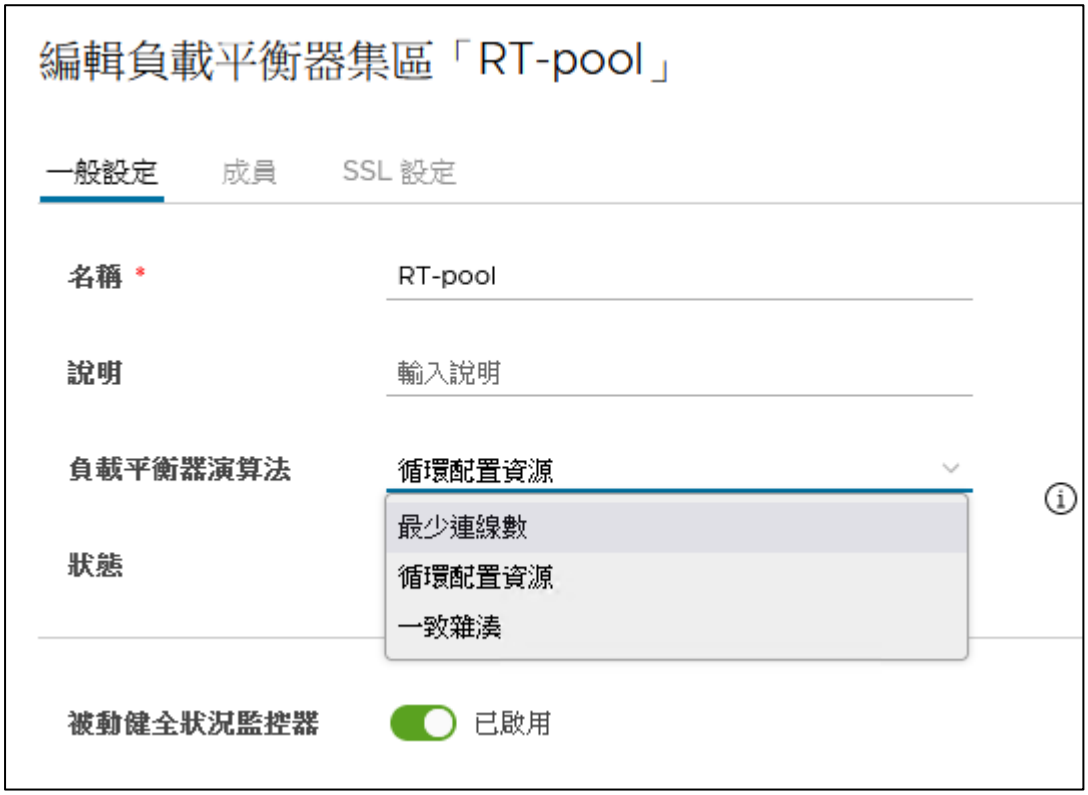
首先需設定 Server Pool，集區→新增


jimmysitnsxt0118-com-EDGE
在 VDC 內容中開啟
組態
一般
速率限制
服務
防火牆
NAT
IPSec VPN
負載平衡器
一般設定
服務引擎群組
虛擬服務
集區
安全性
靜態群組
IP 集
應用程式連接埠設定檔
新增
編輯
刪除
名稱
RT-pool

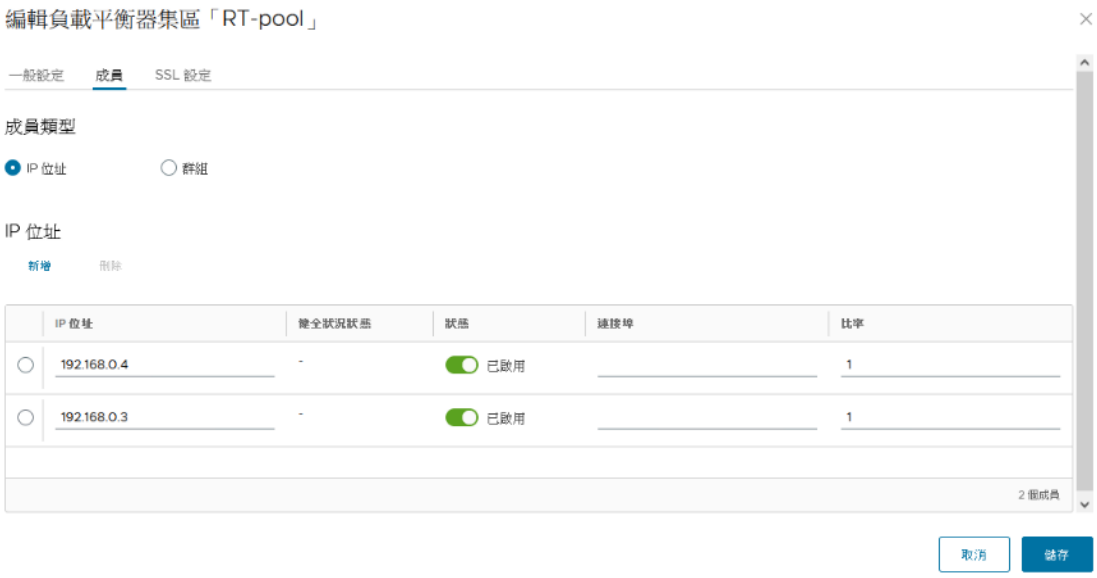
填入集區名稱、調整伺服器連埠。



可依需求調整負載平衡器演算法。



新增成員，將成員狀態啟用，按下儲存。(成員可使用 IP 位址或群組)

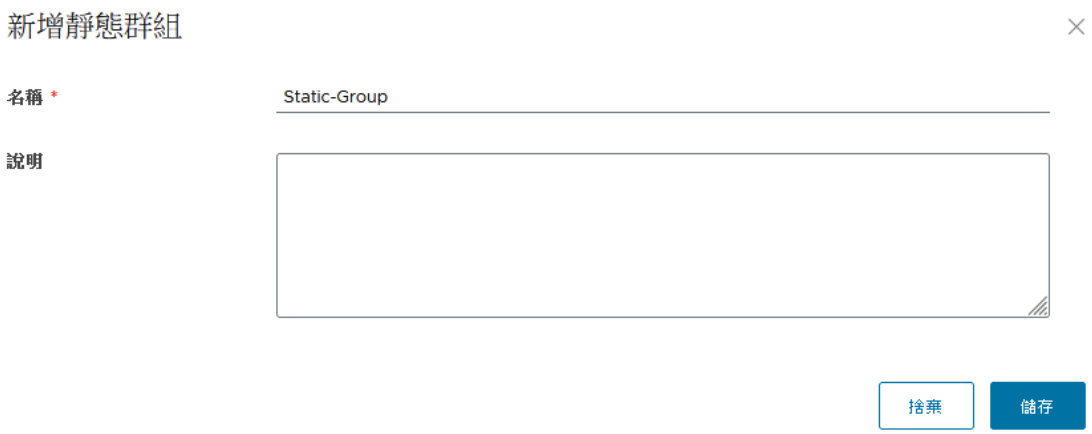


IP 位址：

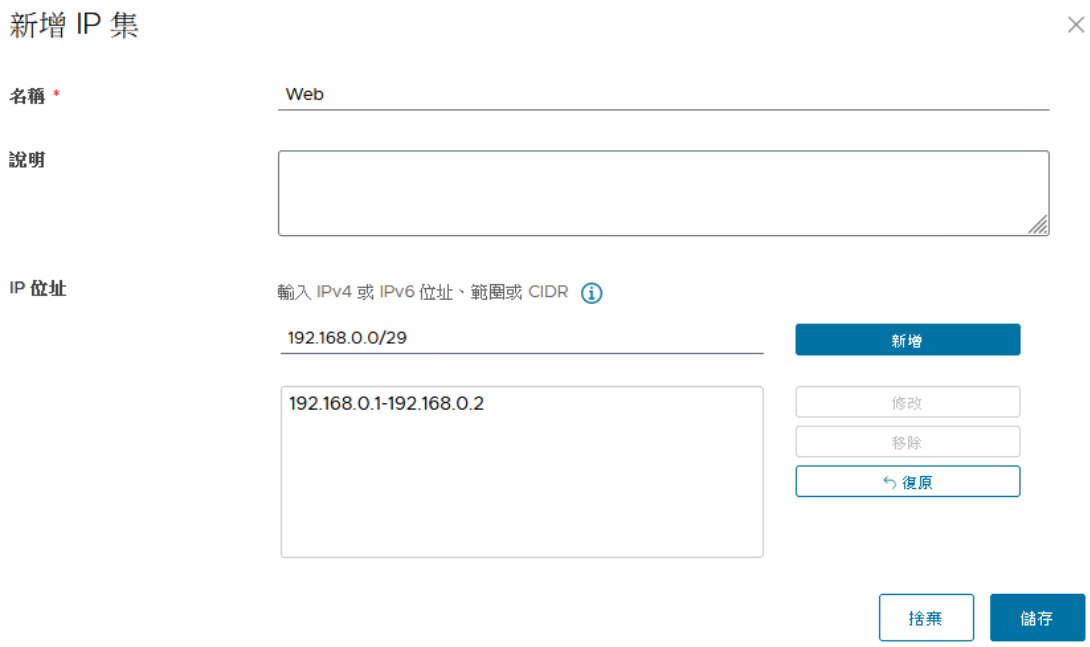
- IP 位址：輸入集區成員的 IP 位址。
- 狀態：選取是否須 " 已啟用 " 。
- 連接埠：預設使用一般設定的預設伺服器連接埠。
- 比率：每個集區成員的比率表示流向各個伺服器集區成員的流量。比率為 2 的伺服器所取得的流量將是比率為 1 的伺服器的兩倍。預設值為 1。

群組：(請先至安全性 > " 靜態群組 " 或 " IP 集 ")

- 靜態群組：新增或編輯既有的名稱後，於 " 管理成員 " 勾選既有的網路群組。



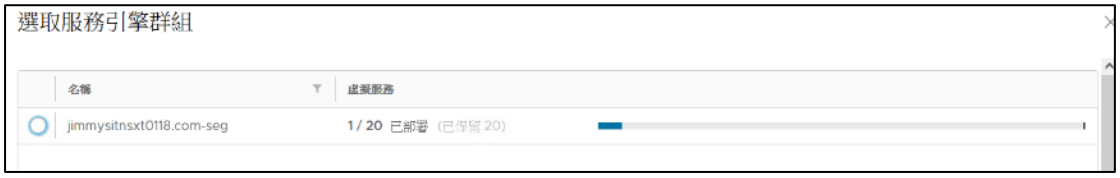
- IP 集：新增 IP 集，輸入名稱與 IP 位址、範圍或 CIDR 後，點選新增>儲存。



再到虛擬服務新增。

填入虛擬服務名稱，點選選服務引擎群組和負載平衡器集區。

服務引擎群組選取第一組。



負載平衡器集區選取剛才建立的集區。

填入虛擬 IP，可點選旁邊ⓘ符號快速看出可用的外部 IP。

確認*必填欄位填完，點選儲存。

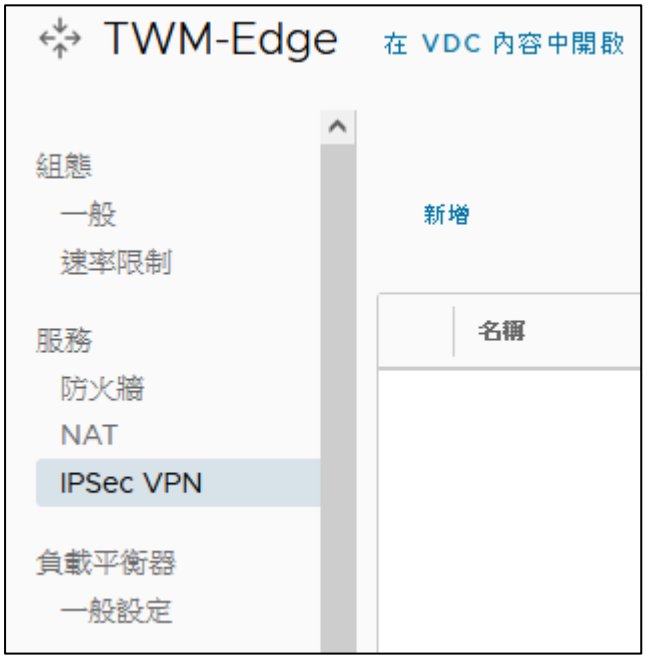
回到虛擬服務主頁可看到已設定好的虛擬服務清單。

若有單一外部 IP 共用多組服務需求(ex:http、https、ssh 共用相同外部 IP)可將 Virtual Services 的 Virtual IP 改與內部環境不衝突的 IP 進行，設定範例如下方：

DNAT			Virtual Services			Pool	
External IP	Internal IP		Virtual IP	Port		Server Pool	Port
60.199.153.123	192.168.255.1:80	→	192.168.255.1	80	→	192.168.88.10 192.168.88.11	80 80
60.199.153.123	192.168.255.2:443	→	192.168.255.2	443	→	192.168.88.10 192.168.88.11	443 443
60.199.153.123	192.168.255.3:443	→	192.168.255.3	22	→	192.168.88.10 192.168.88.11	22 22

IPSec VPN

進到 IPSec VPN→點選新增



填入可識別名稱。

選擇使用金鑰或憑證方式進行對等驗證，範例採用預先共用金鑰。

本機端點填入 Public IP，點旁邊ⓘ符號可以快速檢視可用 IP

網路填入本地的子網路。

遠端端點填入遠端 Public IP。

網路填入遠端的子網路。

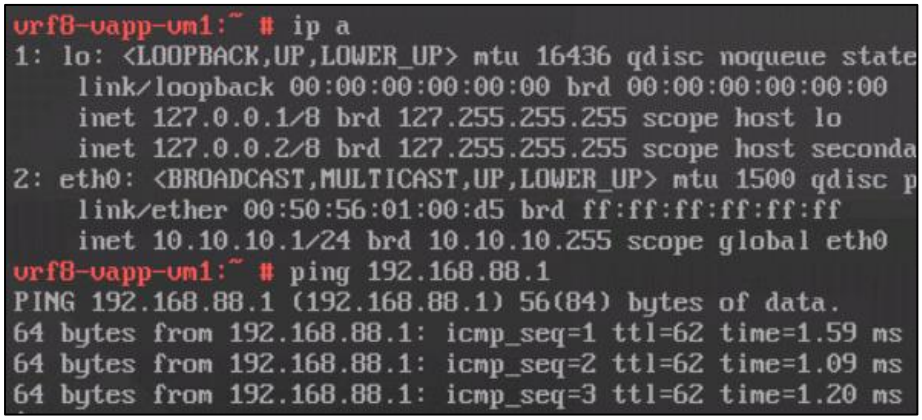
檢視設定。

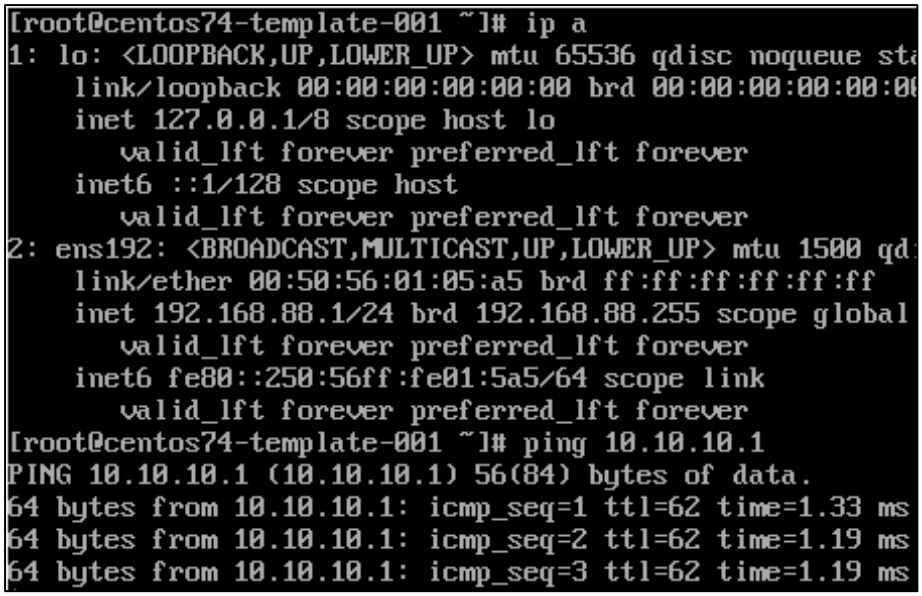
兩端都設定完成可點選檢視統計資料，查看 VPN 連線的通道是否有正確建立。

若是建立失敗會顯示。

防火牆需雙向開通。

測試連線是否可 ping 通





13. K8s 範本說明

新增 Master 節點

請參閱運算雲官網文件下載區的**【運算雲 K8S 範本】新增 Master 節點.pdf**

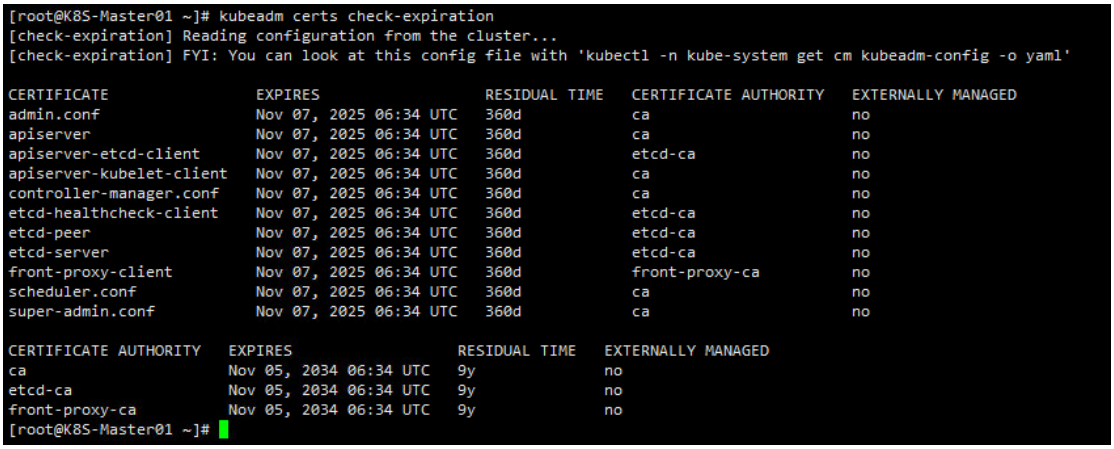
新增Worker 節點

請參閱運算雲官網文件下載區的**【運算雲 K8S 範本】新增 Worker 節點.pdf**

更新憑證說明

1. 檢視目前憑證

   kubeadm certs check-expiration



```
[root@K8S-Master01 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Nov 07, 2025 06:34 UTC   360d            ca                      no
apiserver                  Nov 07, 2025 06:34 UTC   360d            ca                      no
apiserver-etcd-client      Nov 07, 2025 06:34 UTC   360d            etcd-ca                 no
apiserver-kubelet-client   Nov 07, 2025 06:34 UTC   360d            ca                      no
controller-manager.conf    Nov 07, 2025 06:34 UTC   360d            ca                      no
etcd-healthcheck-client    Nov 07, 2025 06:34 UTC   360d            etcd-ca                 no
etcd-peer                  Nov 07, 2025 06:34 UTC   360d            etcd-ca                 no
etcd-server                Nov 07, 2025 06:34 UTC   360d            etcd-ca                 no
front-proxy-client         Nov 07, 2025 06:34 UTC   360d            front-proxy-ca          no
scheduler.conf             Nov 07, 2025 06:34 UTC   360d            ca                      no
super-admin.conf           Nov 07, 2025 06:34 UTC   360d            ca                      no

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Nov 05, 2034 06:34 UTC   9y              no
etcd-ca                 Nov 05, 2034 06:34 UTC   9y              no
front-proxy-ca          Nov 05, 2034 06:34 UTC   9y              no
[root@K8S-Master01 ~]#
```

```
[root@K8S-Master02 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Nov 12, 2025 02:10 UTC   364d            ca                      no
apiserver                  Nov 12, 2025 02:10 UTC   364d            ca                      no
apiserver-etcd-client      Nov 12, 2025 02:10 UTC   364d            etcd-ca                 no
apiserver-kubelet-client   Nov 12, 2025 02:10 UTC   364d            ca                      no
controller-manager.conf    Nov 12, 2025 02:10 UTC   364d            ca                      no
etcd-healthcheck-client    Nov 12, 2025 02:10 UTC   364d            etcd-ca                 no
etcd-peer                  Nov 12, 2025 02:10 UTC   364d            etcd-ca                 no
etcd-server                Nov 12, 2025 02:10 UTC   364d            etcd-ca                 no
front-proxy-client         Nov 12, 2025 02:10 UTC   364d            front-proxy-ca          no
scheduler.conf             Nov 12, 2025 02:10 UTC   364d            ca                      no
!MISSING! super-admin.conf

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Nov 05, 2034 06:34 UTC   9y              no
etcd-ca                 Nov 05, 2034 06:34 UTC   9y              no
front-proxy-ca          Nov 05, 2034 06:34 UTC   9y              no
[root@K8S-Master02 ~]#
```

```
[root@K8S-Master03 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Nov 12, 2025 02:38 UTC   364d            ca                      no
apiserver                  Nov 12, 2025 02:38 UTC   364d            ca                      no
apiserver-etcd-client      Nov 12, 2025 02:38 UTC   364d            etcd-ca                 no
apiserver-kubelet-client   Nov 12, 2025 02:38 UTC   364d            ca                      no
controller-manager.conf    Nov 12, 2025 02:38 UTC   364d            ca                      no
etcd-healthcheck-client    Nov 12, 2025 02:38 UTC   364d            etcd-ca                 no
etcd-peer                  Nov 12, 2025 02:38 UTC   364d            etcd-ca                 no
etcd-server                Nov 12, 2025 02:38 UTC   364d            etcd-ca                 no
front-proxy-client         Nov 12, 2025 02:38 UTC   364d            front-proxy-ca          no
scheduler.conf             Nov 12, 2025 02:38 UTC   364d            ca                      no
!MISSING! super-admin.conf

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Nov 05, 2034 06:34 UTC   9y              no
etcd-ca                 Nov 05, 2034 06:34 UTC   9y              no
front-proxy-ca          Nov 05, 2034 06:34 UTC   9y              no
[root@K8S-Master03 ~]#
```

2. 補上 super-admin.conf

   (A) cd /etc/Kubernetes

   (B) cp admin.conf super-admin.conf

   (C) sed -i 's/-admin/-super-admin/g' super-admin.conf

3. 於所有 Master 節點撰寫以下 shell 腳本並存檔。

```
#!/bin/bash
kubeadm certs renew all
mv -f /root/.kube/config /root/.kube/config.orig
cp -f /etc/kubernetes/admin.conf /root/.kube/config
# You must restart the kube-apiserver, kube-controller-manager, kube-scheduler
and etcd, so that they can use the new certificates.
for targetPOD in kube-apiserver kube-controller-manager kube-scheduler etcd
do
        for delPOD in `kubectl get pod -n kube-system |grep $targetPOD |awk
{'print $1'}`
        do
                kubectl delete pod $delPOD -n kube-system
                sleep 10
        done
done
```

4. 將 shell 腳本新增執行權限。

5. 所有 Master 節點依序執行。

6. 再次檢查

   kubeadm certs check-expiration

```
[root@K8S-Master01 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Nov 12, 2025 06:35 UTC   364d            ca                      no
apiserver                  Nov 12, 2025 06:35 UTC   364d            ca                      no
apiserver-etcd-client      Nov 12, 2025 06:35 UTC   364d            etcd-ca                 no
apiserver-kubelet-client   Nov 12, 2025 06:35 UTC   364d            ca                      no
controller-manager.conf    Nov 12, 2025 06:35 UTC   364d            ca                      no
etcd-healthcheck-client    Nov 12, 2025 06:35 UTC   364d            etcd-ca                 no
etcd-peer                  Nov 12, 2025 06:35 UTC   364d            etcd-ca                 no
etcd-server                Nov 12, 2025 06:35 UTC   364d            etcd-ca                 no
front-proxy-client         Nov 12, 2025 06:35 UTC   364d            front-proxy-ca          no
scheduler.conf             Nov 12, 2025 06:35 UTC   364d            ca                      no
super-admin.conf           Nov 12, 2025 06:35 UTC   364d            ca                      no

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Nov 05, 2034 06:34 UTC   9y              no
etcd-ca                 Nov 05, 2034 06:34 UTC   9y              no
front-proxy-ca          Nov 05, 2034 06:34 UTC   9y              no
[root@K8S-Master01 ~]#
```

```
[root@K8S-Master02 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Nov 12, 2025 06:42 UTC   364d            ca                      no
apiserver                  Nov 12, 2025 06:42 UTC   364d            ca                      no
apiserver-etcd-client      Nov 12, 2025 06:42 UTC   364d            etcd-ca                 no
apiserver-kubelet-client   Nov 12, 2025 06:42 UTC   364d            ca                      no
controller-manager.conf    Nov 12, 2025 06:42 UTC   364d            ca                      no
etcd-healthcheck-client    Nov 12, 2025 06:42 UTC   364d            etcd-ca                 no
etcd-peer                  Nov 12, 2025 06:42 UTC   364d            etcd-ca                 no
etcd-server                Nov 12, 2025 06:42 UTC   364d            etcd-ca                 no
front-proxy-client         Nov 12, 2025 06:42 UTC   364d            front-proxy-ca          no
scheduler.conf             Nov 12, 2025 06:42 UTC   364d            ca                      no
!MISSING! super-admin.conf

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Nov 05, 2034 06:34 UTC   9y              no
etcd-ca                 Nov 05, 2034 06:34 UTC   9y              no
front-proxy-ca          Nov 05, 2034 06:34 UTC   9y              no
[root@K8S-Master02 ~]#
```

```
[root@K8S-Master03 ~]# kubeadm certs check-expiration
[check-expiration] Reading configuration from the cluster...
[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'

CERTIFICATE                EXPIRES                  RESIDUAL TIME   CERTIFICATE AUTHORITY   EXTERNALLY MANAGED
admin.conf                 Nov 12, 2025 06:51 UTC   364d            ca                      no
apiserver                  Nov 12, 2025 06:51 UTC   364d            ca                      no
apiserver-etcd-client      Nov 12, 2025 06:51 UTC   364d            etcd-ca                 no
apiserver-kubelet-client   Nov 12, 2025 06:51 UTC   364d            ca                      no
controller-manager.conf    Nov 12, 2025 06:51 UTC   364d            ca                      no
etcd-healthcheck-client    Nov 12, 2025 06:51 UTC   364d            etcd-ca                 no
etcd-peer                  Nov 12, 2025 06:51 UTC   364d            etcd-ca                 no
etcd-server                Nov 12, 2025 06:51 UTC   364d            etcd-ca                 no
front-proxy-client         Nov 12, 2025 06:51 UTC   364d            front-proxy-ca          no
scheduler.conf             Nov 12, 2025 06:51 UTC   364d            ca                      no
!MISSING! super-admin.conf

CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED
ca                      Nov 05, 2034 06:34 UTC   9y              no
etcd-ca                 Nov 05, 2034 06:34 UTC   9y              no
front-proxy-ca          Nov 05, 2034 06:34 UTC   9y              no
[root@K8S-Master03 ~]#
```

刪除節點說明

1. kubectl get nodes
2. kubectl drain 節點名稱
3. kubectl get nodes
4. kubectl delete node 節點名稱

K8S Q&A 說明

1. 範本的 OS 與套件版本?

a. OS: Oracle Linux 8

b. Kubelet: 1.29.7

c. Kubeadm: 1.29.7

d. Kubectl: 1.29.7

e. Containerd: 1.6.32

2. iptables 是否要啟動? 有哪些 port 要開放?

a. 停用 iptables 和 firewalld。

b. 請根據 K8s 官方文件提供的建議開放 tcp/udp port 自行新增。

3. hostname 能否不一樣?該如何處理?

a. 不建議，Worker 節點變更 hostname 的話需要將節點退出後重新加入，Master 的話可能也得 reset 重新佈建。

4. IP 是否需要一致?不同的話該如何處理?

a. 不建議，原因與變更 hostname 相同。

5. 部署後如何驗證 pod 運作?

a. 啟動測試 pod

b. 登入 Master 節點

c. 執行以下指令

```
kubectl run test-pod --image=busybox -- sleep 3600
kubectl get pods
kubectl exec -it test-pod -- ping -c 4 google.com
kubectl delete pod test-pod
```

6. 部署後如何重新產生憑證?

a. 於 Master 節點撰寫以下 shell 腳本並存檔。

```
#!/bin/bash
kubeadm certs renew all
mv -f /root/.kube/config /root/.kube/config.orig
cp -f /etc/kubernetes/admin.conf /root/.kube/config
# You must restart the kube-apiserver, kube-controller-manager, kube-scheduler and etcd, so that they can use the new certificates.
for targetPOD in kube-apiserver kube-controller-manager kube-scheduler etcd
do
        for delPOD in `kubectl get pod -n kube-system |grep $targetPOD |awk {'print $1'}`
        do
                kubectl delete pod $delPOD -n kube-system
                sleep 10
        done
done
```

b. 將 shell 腳本新增執行權限。

c. 所有 Master 節點依序執行。

7. 如果要新增節點怎麼做?

- 以下說明前提為已建立完成新的 Master 與 Worker 節點 VM。

- 根據 Master 或 Worker 範本部署 VM：
  a. 主機名稱為 K8S-Master0X 或 K8S-Worker0X(X 為 2 開始排序)。
  b. 根據官方建議 Master 節點數量應為奇數(如 1、3、5...)。
  c. Master 節點的 IP 為 192.168.0.8X(X 為 2 開始排序)。
  d. Worker 節點的 IP 為 192.168.0.9X(X 為 2 開始排序)。
- 更新所有節點的/etc/hosts 名稱與 IP 解析。
- 登入到第一台 MASTER
  a. 確定憑證是否於有效期限內
     i. kubeadm certs check-expiration
     ii. 檢視憑證: kubeadm init phase upload-certs --upload-certs
  b. 產生 TOKEN
     - 給新增 Worker 使用
       - kubeadm token create --print-join-command
     - 給新增 Master 使用
       - kubeadm token create --print-join-command --control-plane --certificate-key 憑證
- 於 Master 或 Worker 節點
  a. Master 節點
     i. rm -rf /var/lib/kubelet ; rm -rf /etc/kubernetes
     ii. systemctl restart kubelet
     iii. modprobe br_netfilter
     iv. echo 1 > /proc/sys/net/bridge/bridge-nf-call-iptables
     v. echo 1 > /proc/sys/net/ipv4/ip_forward
     vi. kubeadm reset (中途卡住則 control+c 中斷，接著執行 join 指令)
     vii. 執行上述步驟產生的 join 指令
     viii. mkdir -p $HOME/.kube ; cp -i /etc/kubernetes/admin.conf $HOME/.kube/config ; chown $(id -u):$(id -g) $HOME/.kube/config
  b. Worker 節點
     i. rm -rf /var/lib/kubelet ; rm -rf /etc/kubernetes
     ii. systemctl restart kubelet
     iii. modprobe br_netfilter
     iv. echo 1 > /proc/sys/net/bridge/bridge-nf-call-iptables
     v. echo 1 > /proc/sys/net/ipv4/ip_forward
     vi. 執行上述步驟產生的指令
- 於 Master 節點執行: kubectl get nodes -o wide，確認所有節點皆已加入叢集。

8. 憑證定期更新做法?

a. 於 Master 節點撰寫以下 shell 腳本並存檔。

```
#!/bin/bash
kubeadm certs renew all
mv -f /root/.kube/config /root/.kube/config.orig
cp -f /etc/kubernetes/admin.conf /root/.kube/config
# You must restart the kube-apiserver, kube-controller-manager, kube-scheduler and etcd, so that
they can use the new certificates.
for targetPOD in kube-apiserver kube-controller-manager kube-scheduler etcd
do
        for delPOD in `kubectl get pod -n kube-system |grep $targetPOD |awk {'print $1'}`
        do
                kubectl delete pod $delPOD -n kube-system
                sleep 10
        done
done
```

b. 將 shell 腳本新增執行權限。

c. 於所有的 Master 節點建立 Cron Job。(※建議每個節點的 Job 排程至少間隔 10 分鐘。)

9. 如何刪除節點?

a. kubectl get nodes

b. kubectl drain 節點名稱

b-1. 復原則執行 kubectl uncordon 節點名稱

c. kubectl get nodes

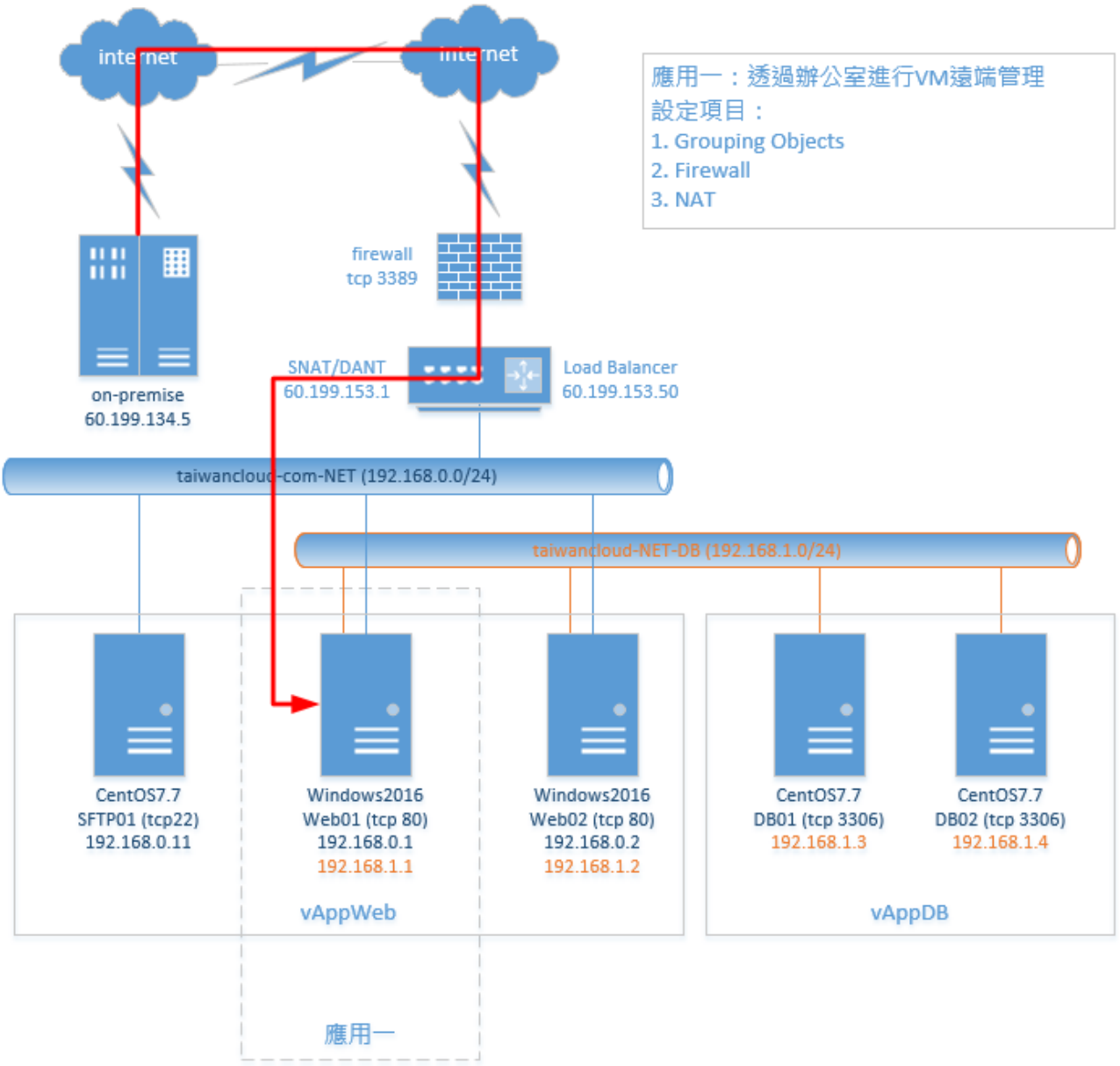
d. kubectl delete node 節點名稱

e. 結束後記得更新群集中節點的/etc/hosts

14. 應用一：透過辦公室進行 VM 遠端管理

情境說明

使用者於辦公室透過遠端連線，管理運算雲 3.0 平台上的 VM。



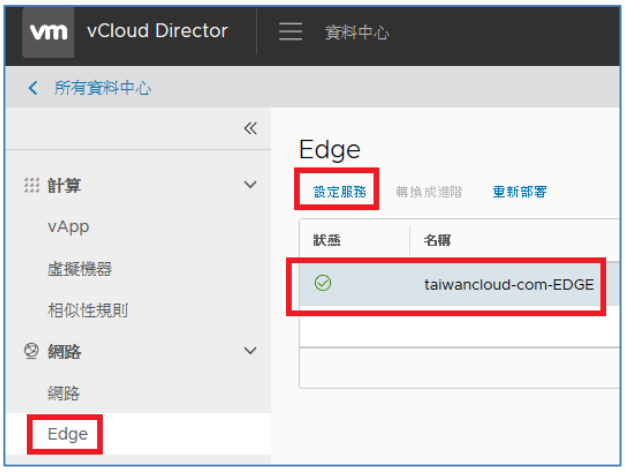
前置作業

1. 新增 vAppWeb
2. 建立 Web VM

設定項目

1 Grouping Objects

1.1 點選網路>「Edge」>「設定服務」

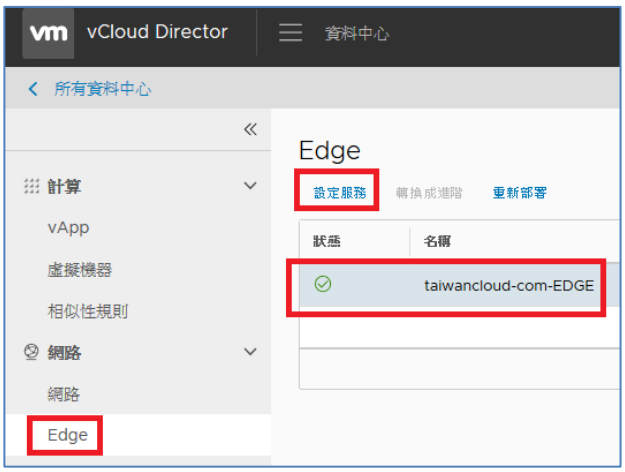


1.2 點選「群組物件」>「IP 集」>「新增」

1.3 輸入名稱與 IP 後，點選「保留」

2 Firewall

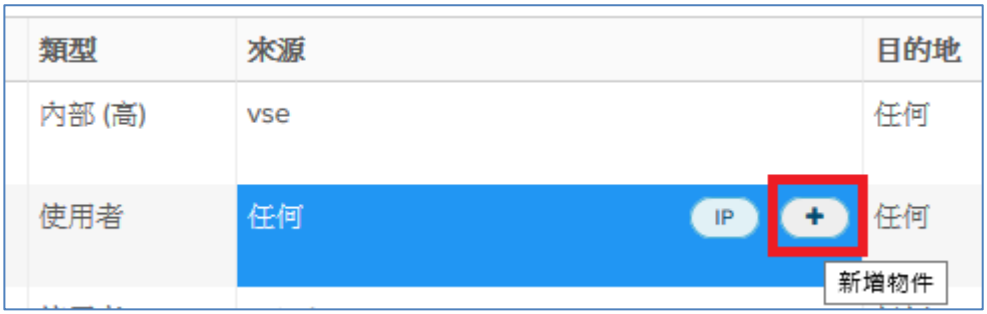
2.1 點選網路>「Edge」>「設定服務」



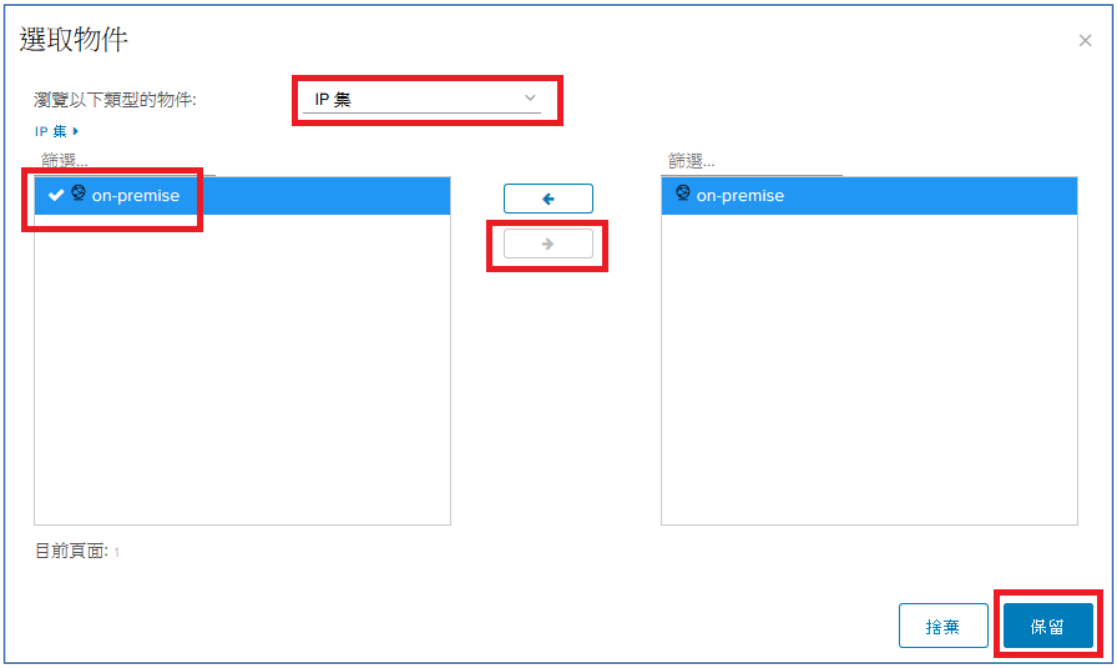
2.2 點選「防火牆」>「+」

2.3 輸入名稱

2.4 點選「來源」>「+」



2.5 選取「IP 集」>選取群組>點選「→」>點選「保留」



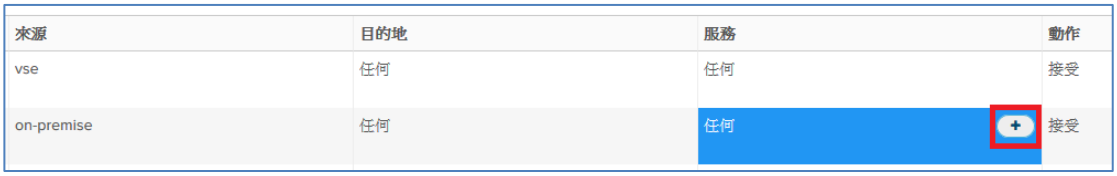
2.6 點選「服務」>

點選「+」>

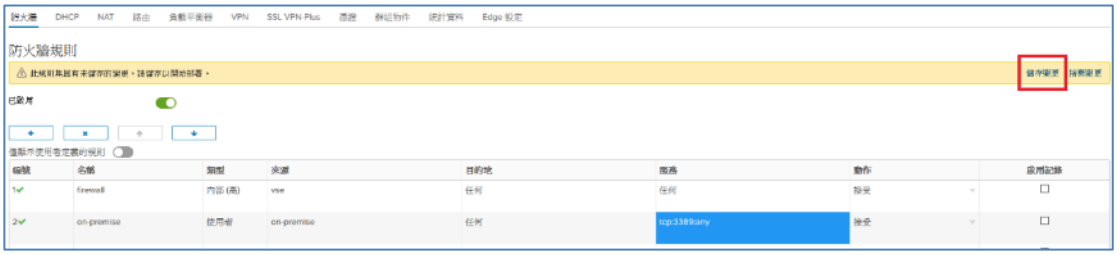
通訊協定選取「TCP」>

目的地連接埠輸入「3389」>

點選「保留」

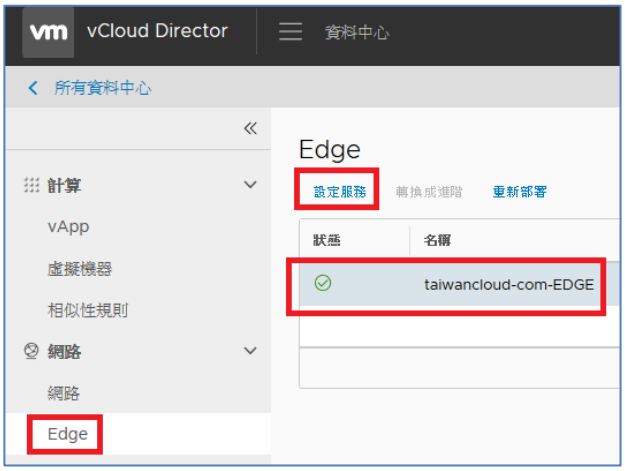


2.7 點選畫面上方「儲存變更」



3 NAT

3.1 點選網路>「Edge」>「設定服務」



3.2 點選「NAT」>「+DNAT 規則」

3.3 選取原始 IP(此例為 60.199.153.1)

選取通訊協定 TCP

輸入原始連接埠 3389

輸入轉譯的 IP(此例為 192.168.0.1)

輸入轉譯的連接埠 3389

點選「保留」

3.4 點選畫面上方的「儲存變更」

4 檢測服務

4.1 遠端透過 RDP 登入

新版設定(適用 2023/9/5 後移轉用戶或新申裝用戶)

(新版設定方式適用 2023/9/5 後移轉用戶或新申裝用戶參考。)

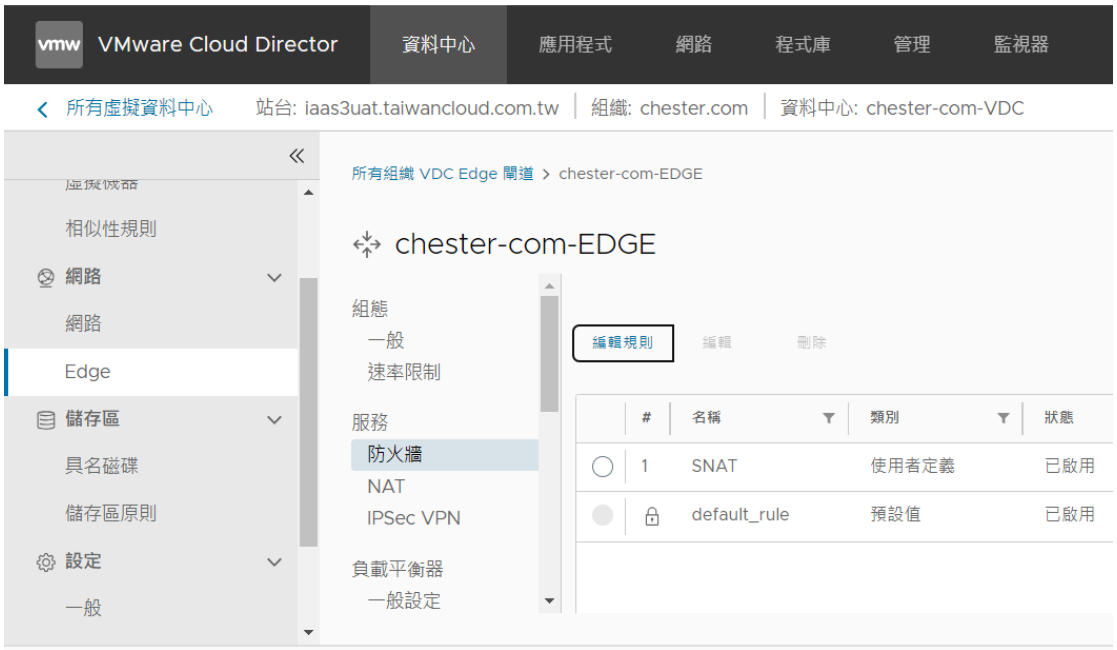
1 Grouping Objects

1.1 資料中心 > VDC > 網路 > Edge > 點選閘道名稱 > 安全性 > IP 集 > 新增

1.2 新增 IP 集，示意如下：

2 Firewall

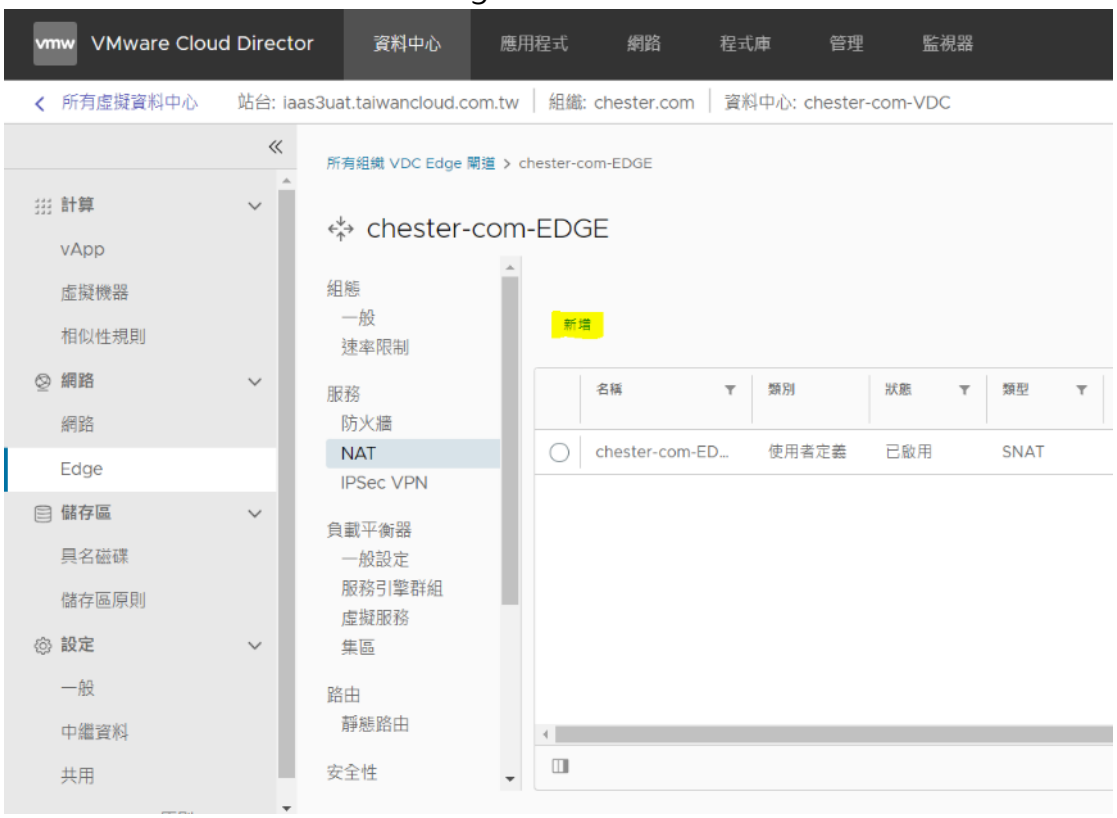
2.1 資料中心 > OVDC > 網路 > Edge > 點選閘道名稱 > 防火牆 > 編輯規則



2.2 點選[在頂部新增]

3 NAT

3.1 資料中心 > OVDC > 網路 > Edge > 點選閘道名稱 > NAT > 新增



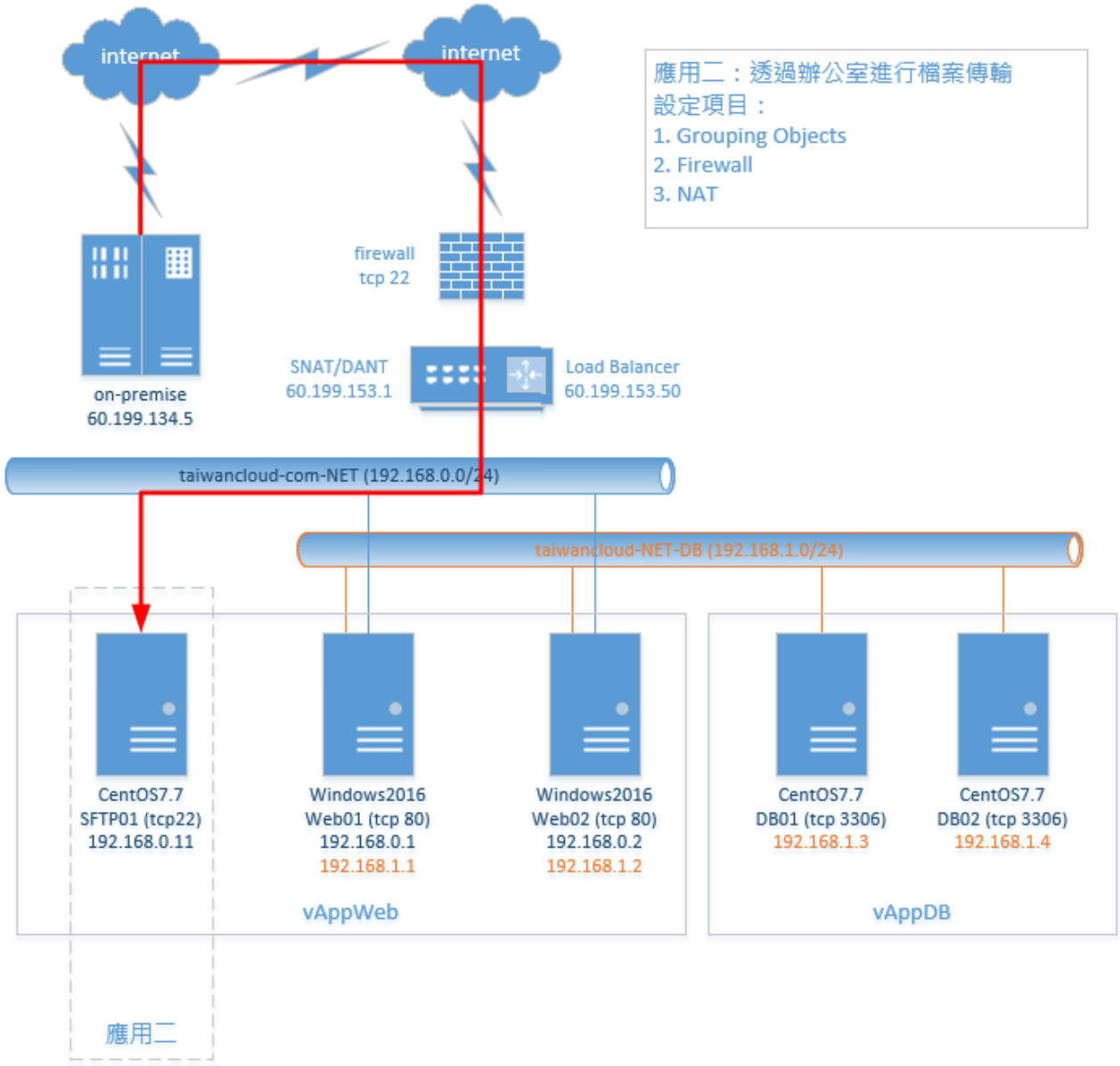
3.2 點選新增，示意如下：


新增 NAT 規則
名稱 *
需要輸入
說明
介面類型 *
DNAT
外部 IP *
目的地 IP 或 CIDR
外部連接埠
目的地連接埠
內部 IP *
轉譯的 IP 或 CIDR
應用程式
-
轉譯的連接埠
進階設定
捨棄
儲存

15. 應用二：透過辦公室進行檔案傳輸

情境說明

使用者於辦公室透過遠端連線，與運算雲 3.0 平台上的 VM 進行檔案傳輸。



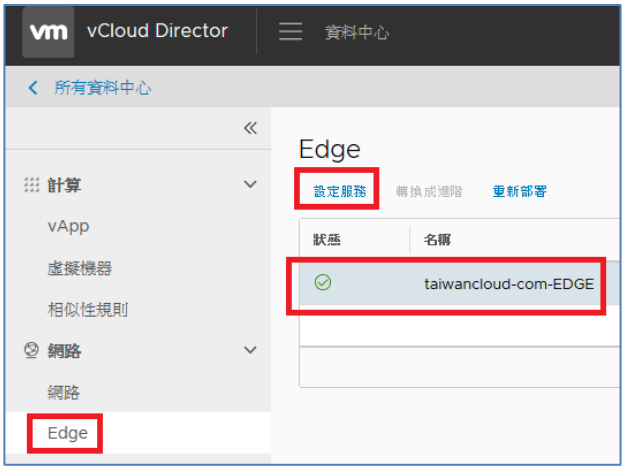
前置作業

1. 新增 vAppWeb
2. 建立 SFTP VM

設定項目

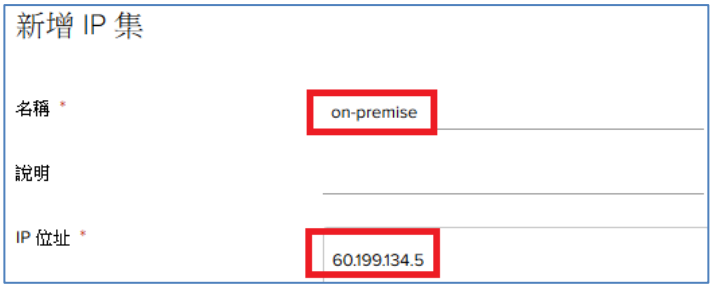
1 Grouping Objects

1.1 點選網路>「Edge」>「設定服務」



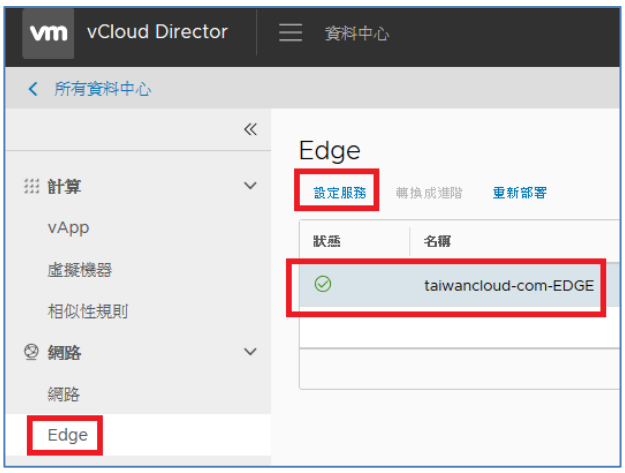
1.2 點選「群組物件」>「IP 集」>「新增」

1.3 輸入名稱與 IP 後，點選「保留」



2 Firewall

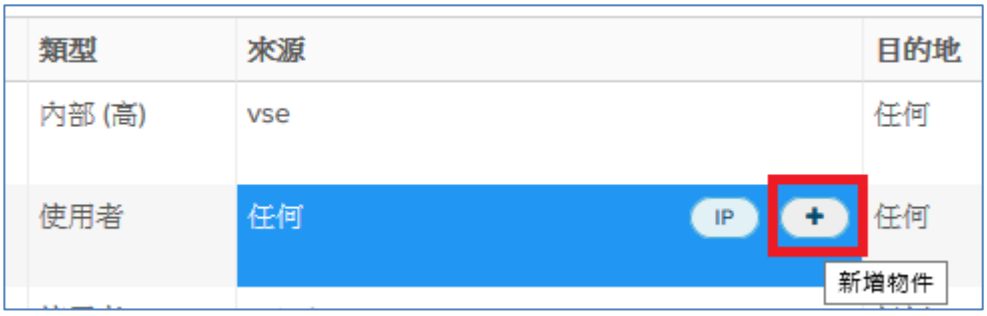
2.1 點選網路>「Edge」>「設定服務」



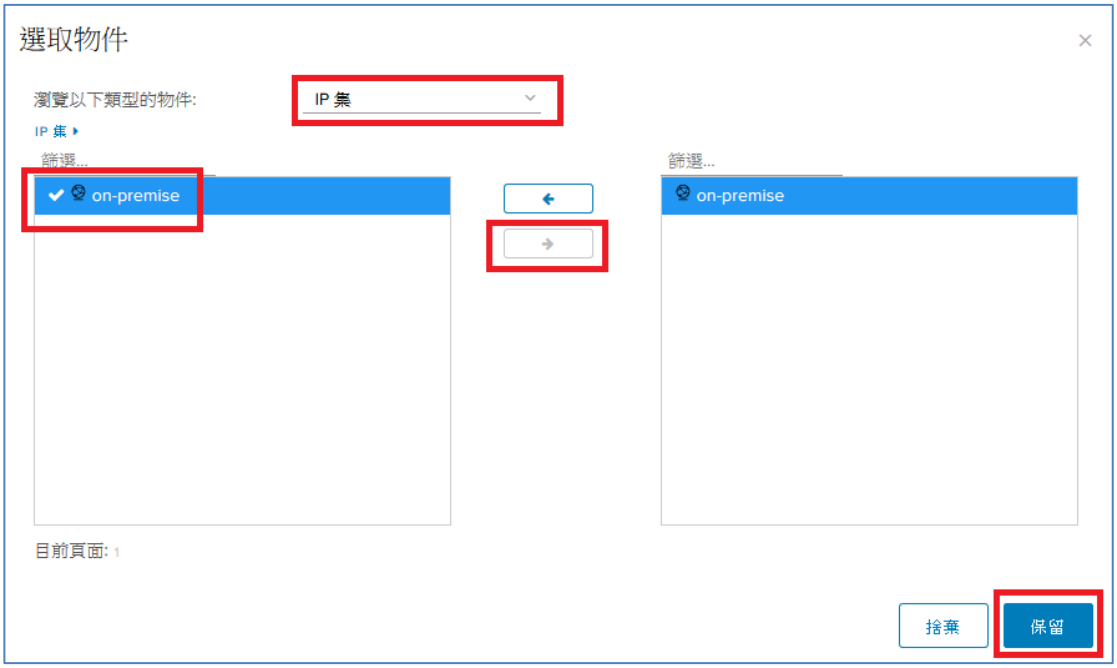
2.2 點選「防火牆」>「+」

2.3 輸入名稱

2.4 點選「來源」>「+」



2.5 選取「IP 集」>選取群組>點選「→」>點選「保留」



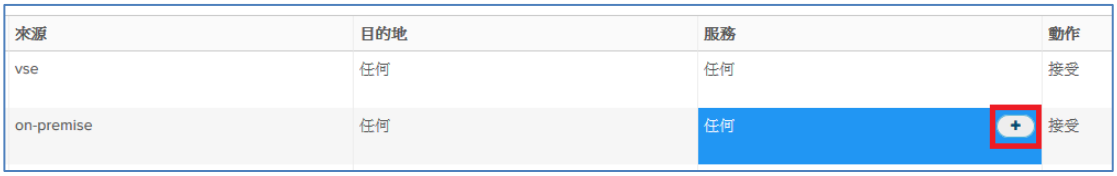
2.6 點選「服務」>

點選「+」>

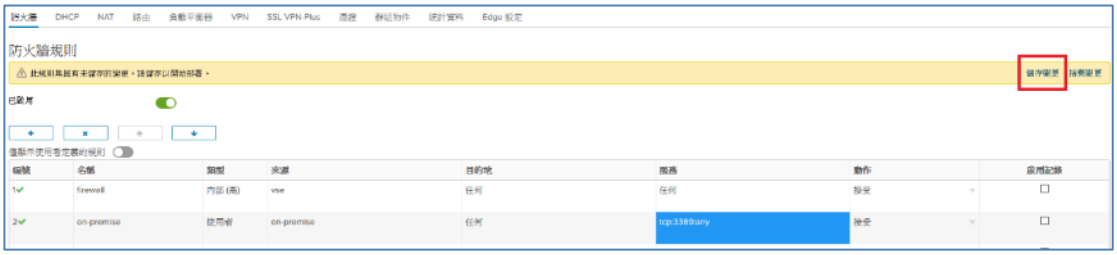
通訊協定選取「TCP」>

目的地連接埠輸入「22」>

點選「保留」

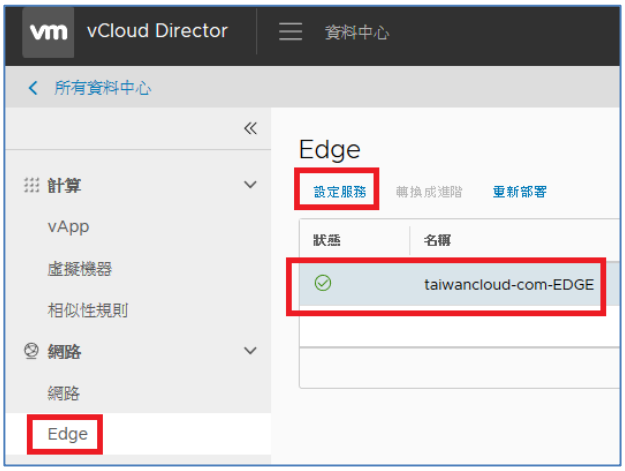


2.7 點選畫面上方「儲存變更」



3 NAT

3.1 點選網路>「Edge」>「設定服務」



3.2 點選「NAT」>「+DNAT 規則」

3.3 選取原始 IP(此例為 60.199.153.1)

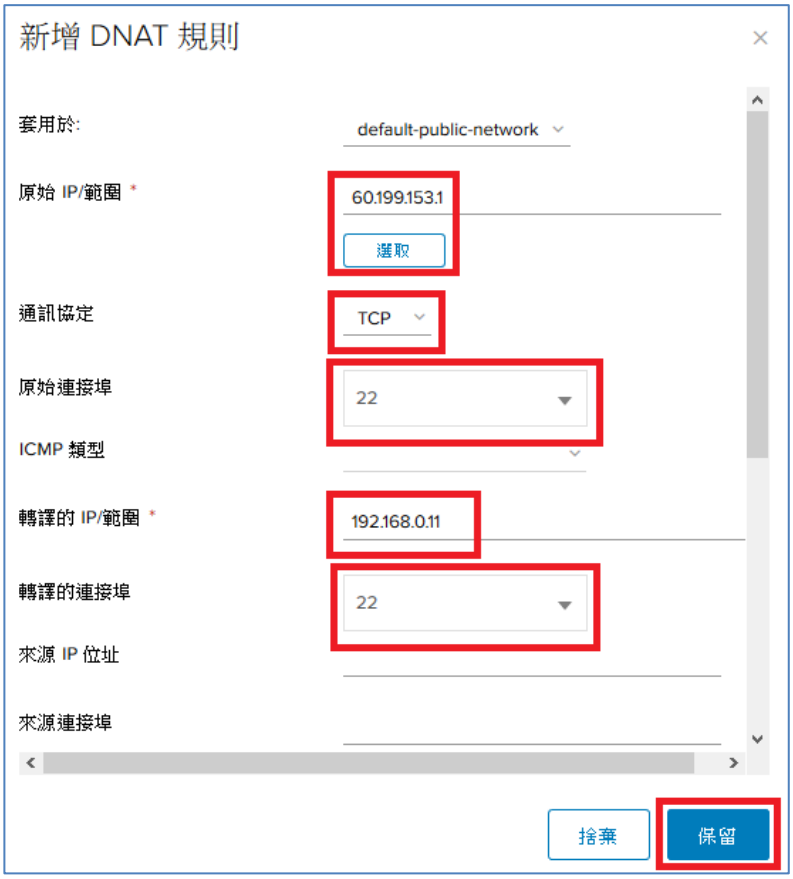
選取通訊協定 TCP

輸入原始連接埠 22

輸入轉譯的 IP(此例為 192.168.0.11)

輸入轉譯的連接埠 22

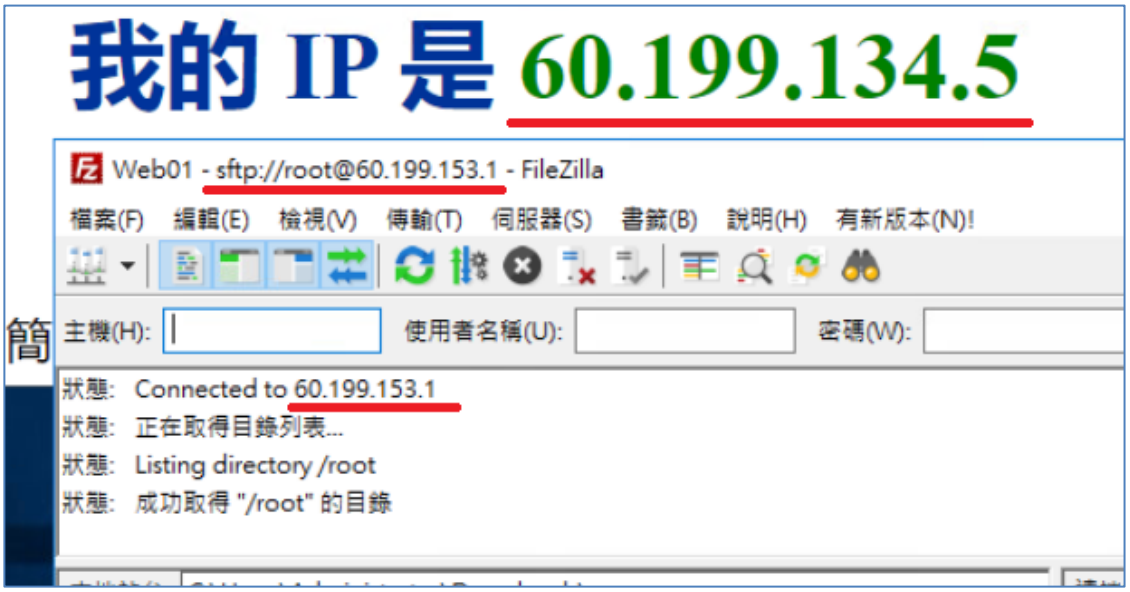
點選「保留」



3.4 點選畫面上方的「儲存變更」

4 檢測服務

4.1 遠端透過工具連線

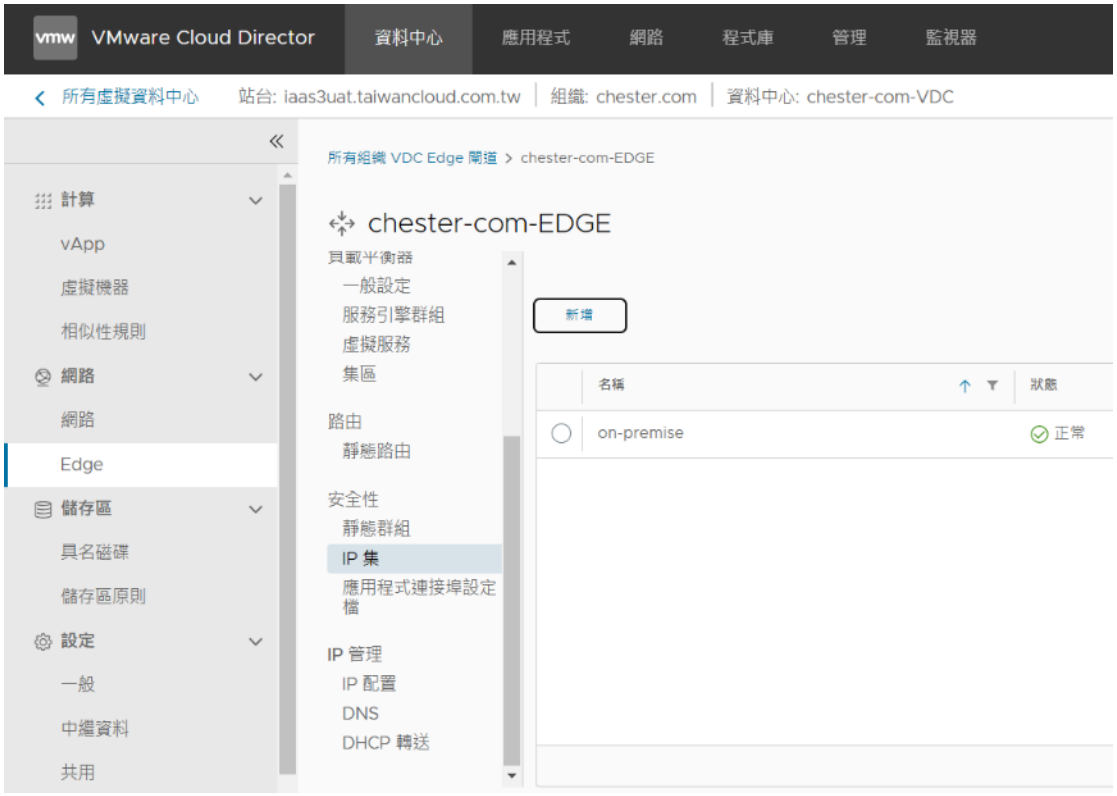


新版設定(適用 2023/9/5 後移轉用戶或新申裝用戶)

(新版設定方式適用 2023/9/5 後移轉用戶或新申裝用戶參考。)

1 Grouping Objects

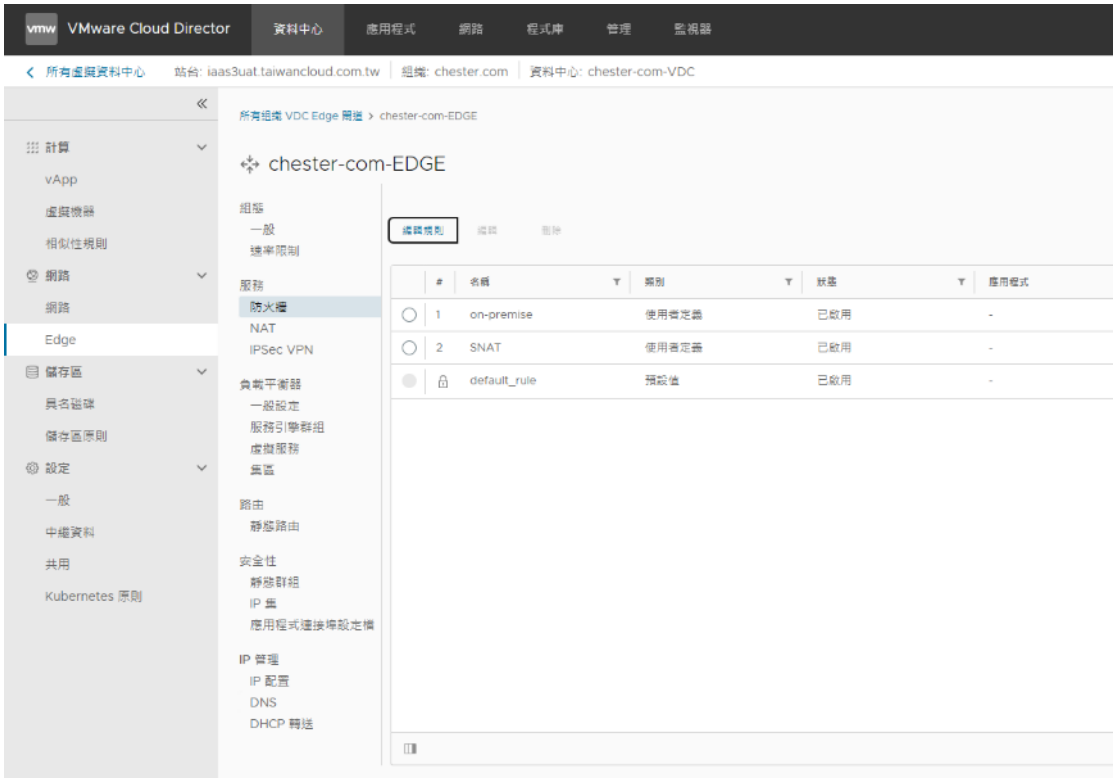
1.1 資料中心 > VDC > 網路 > Edge > 點選閘道 > 安全性 > IP 集



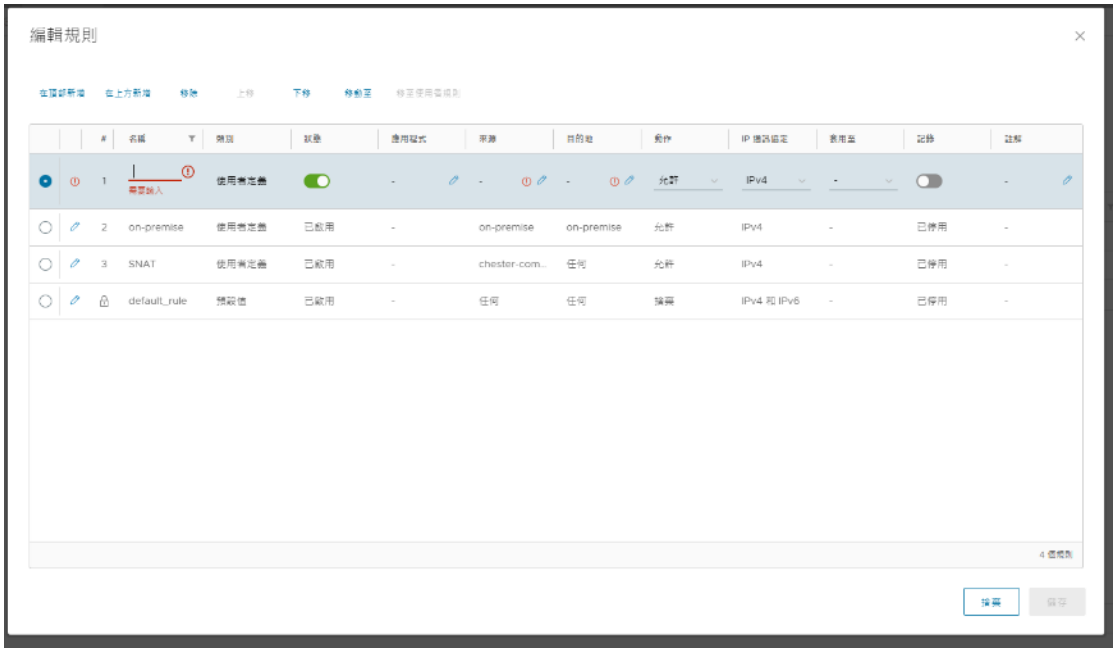
1.2 點選新增

2 Firewall

2.1 資料中心 > OVDC > 網路 > Edge > 點選閘道 > 防火牆 > 編輯規則

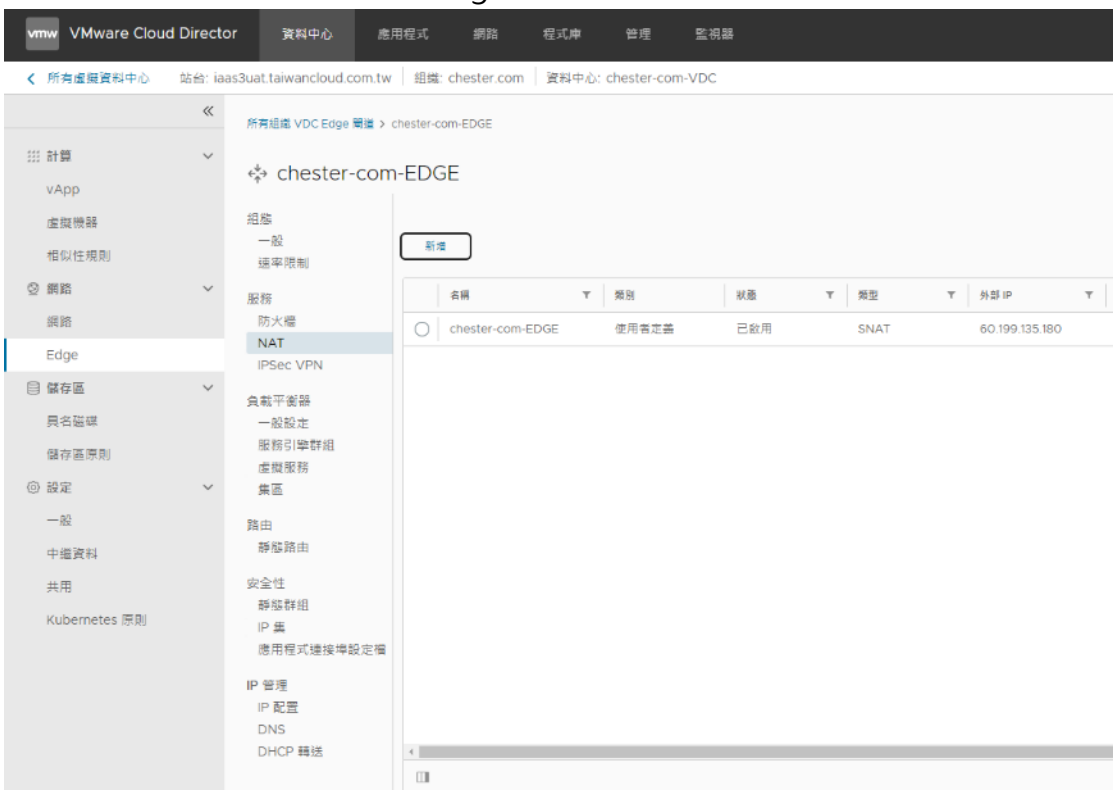


2.2 點選在頂部新增



3 NAT

3.1 資料中心 > OVDC > 網路 > Edge > 點選閘道 > NAT



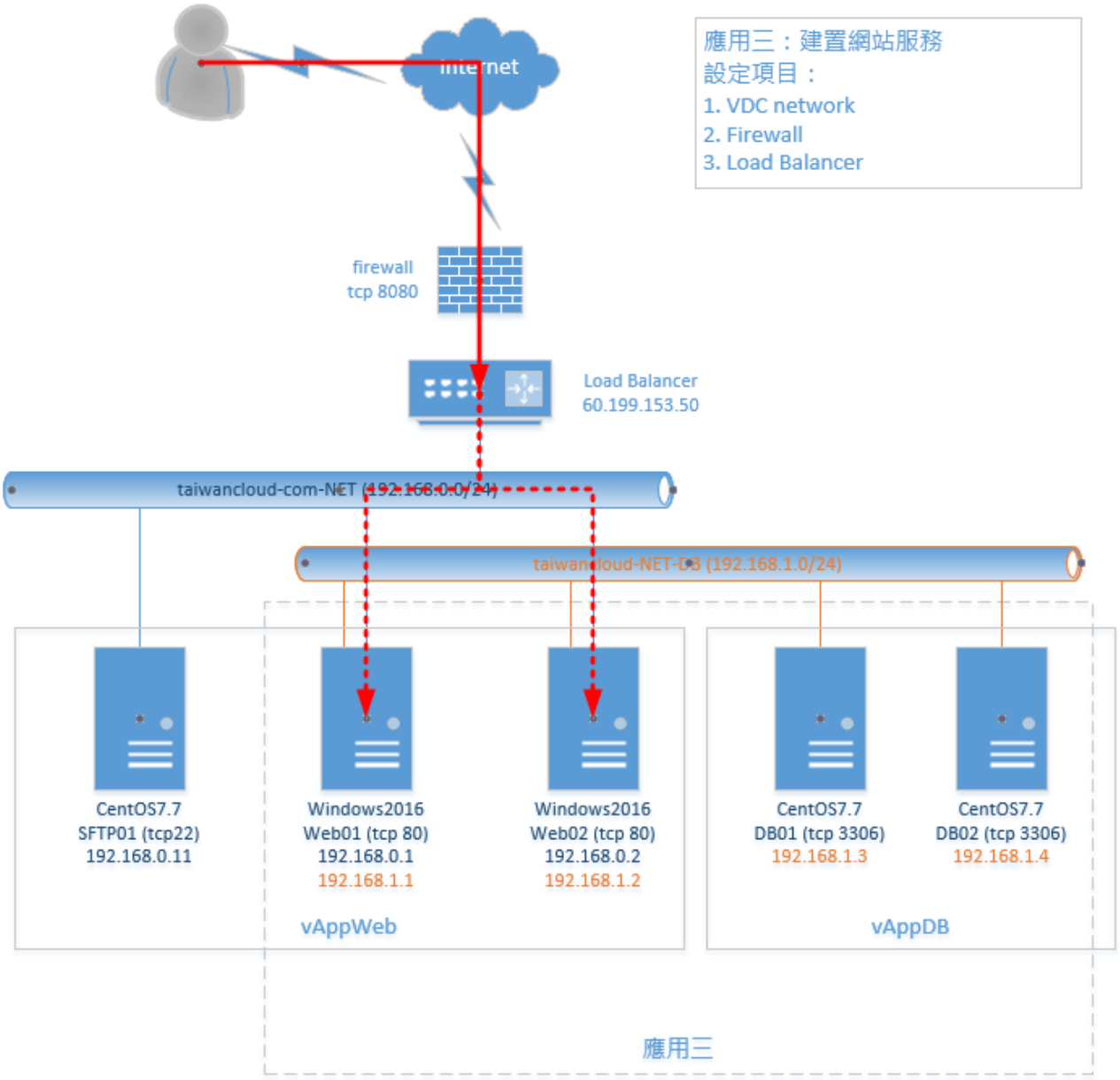
3.2 點選新增


新增 NAT 規則
名稱 *
需要輸入
說明
介面類型 *
DNAT
外部 IP *
目的地 IP 或 CIDR
外部連接埠
目的地連接埠
內部 IP *
轉譯的 IP 或 CIDR
應用程式
-
轉譯的連接埠
進階設定
捨棄
儲存

16. 應用三：建置網站服務

情境說明

建置 Web 網站服務經由負載平衡開放網路存取，並將後端資料庫透過隔離內網區隔，僅開放來源端為 Web 的 VM。



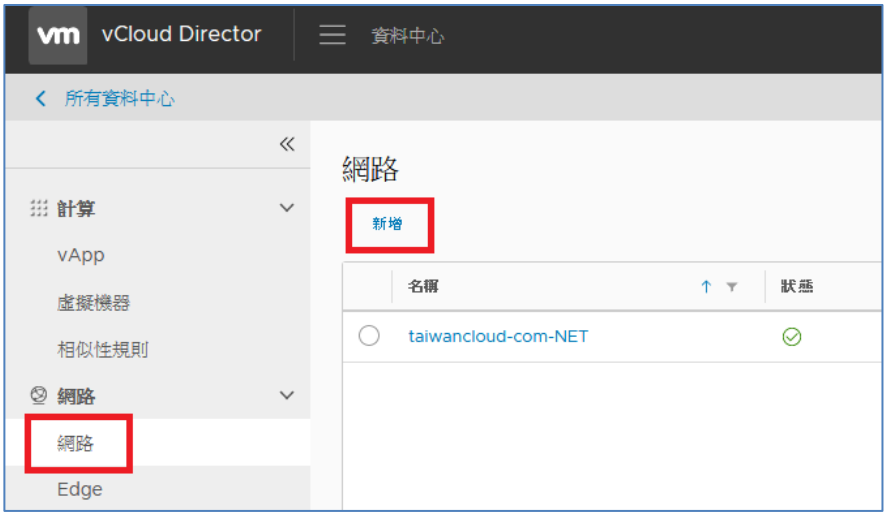
前置作業

1. 新增 vAppWeb 與兩部 Web VM
2. 新增 vAppDB 與兩部 DB VM

設定項目

1 VCD Network (DB)

1.1 點選網路>新增



1.2 點選「已隔離」

輸入名稱與 CIDR(此例為 192.168.1.254/24)

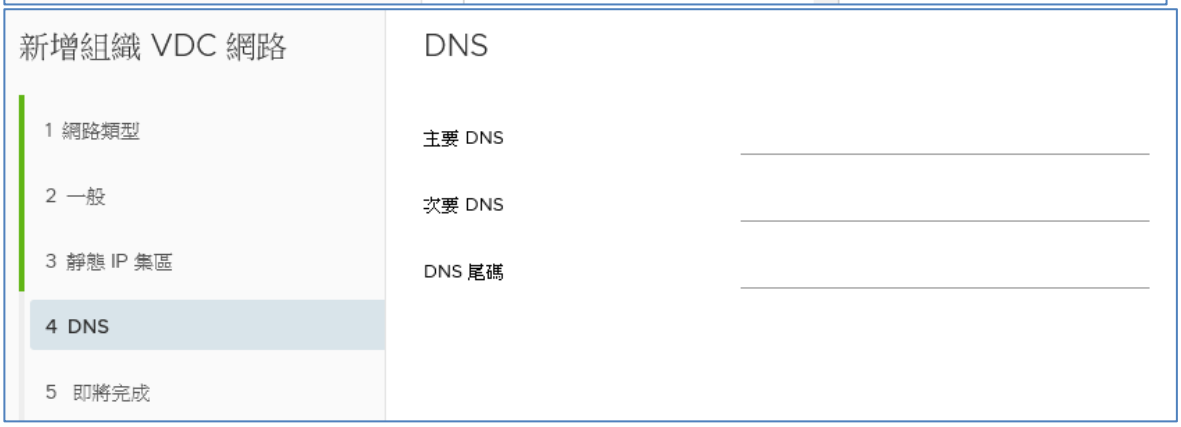
輸入靜態 IP 集區後點選「新增」

DNS 設定略過

點選「完成」


新增組織 VDC 網路
1 網路類型
2 一般
3 靜態 IP 集區
4 DNS
5 即將完成
一般
名稱 *
taiwancloud-com-NET-DB
閘道 CIDR *
192.168.1.254/24
說明

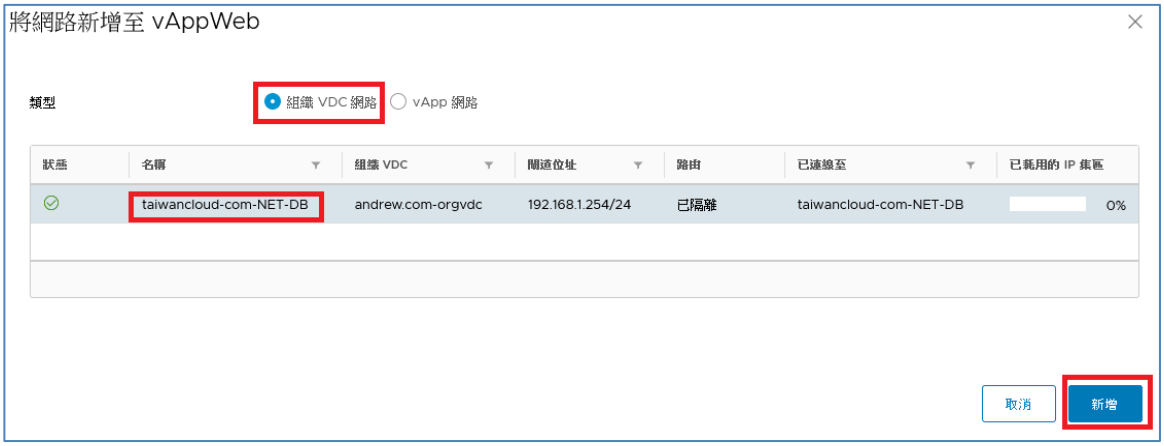

新增組織 VDC 網路
1 網路類型
2 一般
3 靜態 IP 集區
4 DNS
5 即將完成
靜態 IP 集區
閘道 CIDR
192.168.1.254/24
靜態 IP 集區
輸入 IP 範圍 (格式: 192.168.1.2 - 192.168.1.100)
192.168.1.1-192.168.1.200
新增
修改
移除


新增組織 VDC 網路
1 網路類型
2 一般
3 靜態 IP 集區
4 DNS
5 即將完成
DNS
主要 DNS
次要 DNS
DNS 尾碼

2 Add Network(Web)

2.1 vApp > 點選 vAppWeb 詳細資訊 > 網路 > 新增

2.2 選取前步驟設定之網路 > 新增

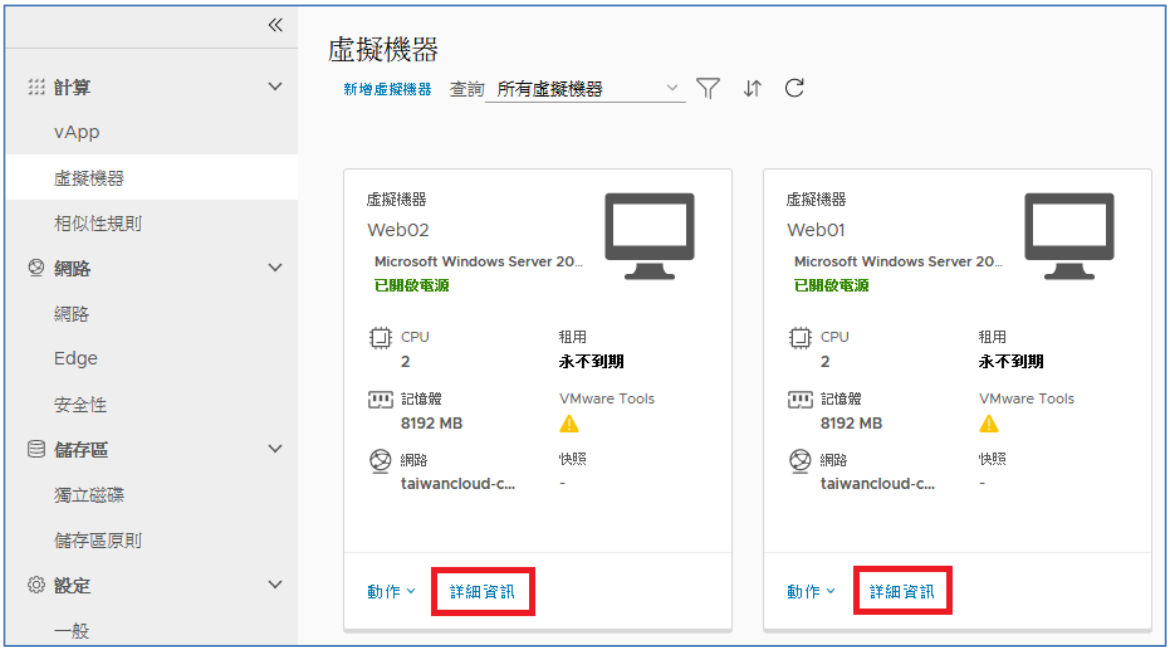


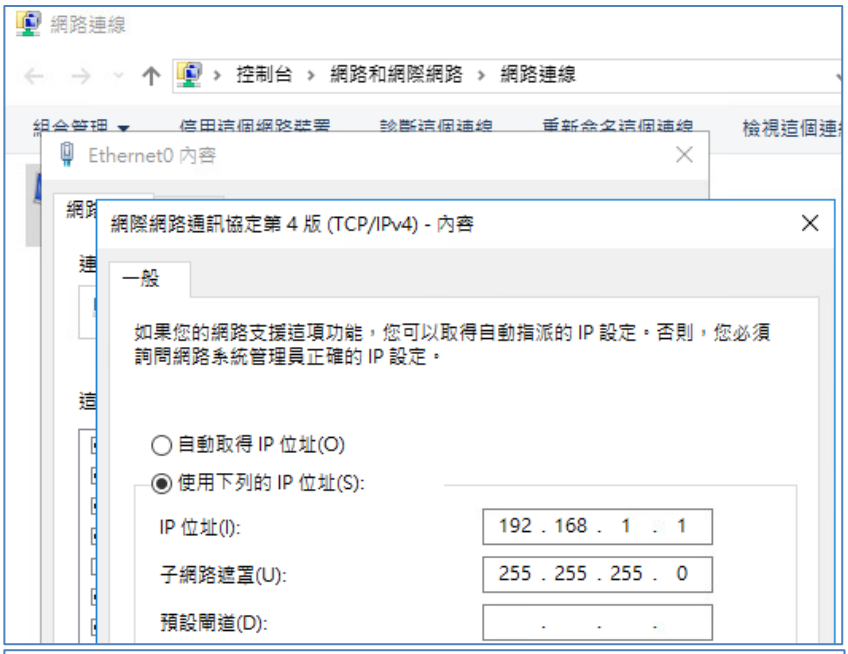
2.3 虛擬機器 > 詳細資訊 > 硬體 > NIC > 新增

類型選擇 VMXNET3

選取網路(此例為 taiwancloud-com-NET-DB)

進入 VM 再次進行 IP 設定

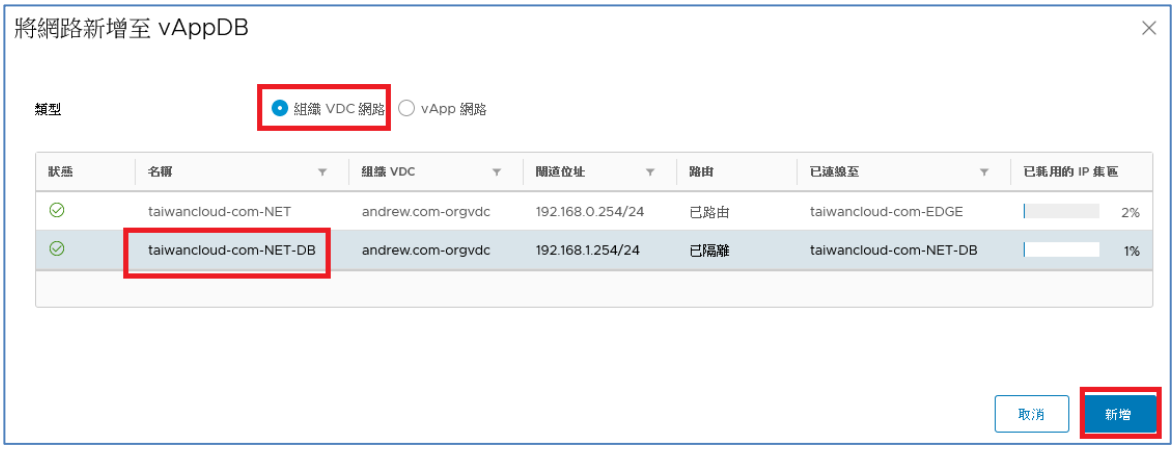




3 Add Network(DB)

3.1 vApp > 點選 vAppDB 詳細資訊 > 網路 > 新增

3.2 選取前步驟設定之網路 > 新增



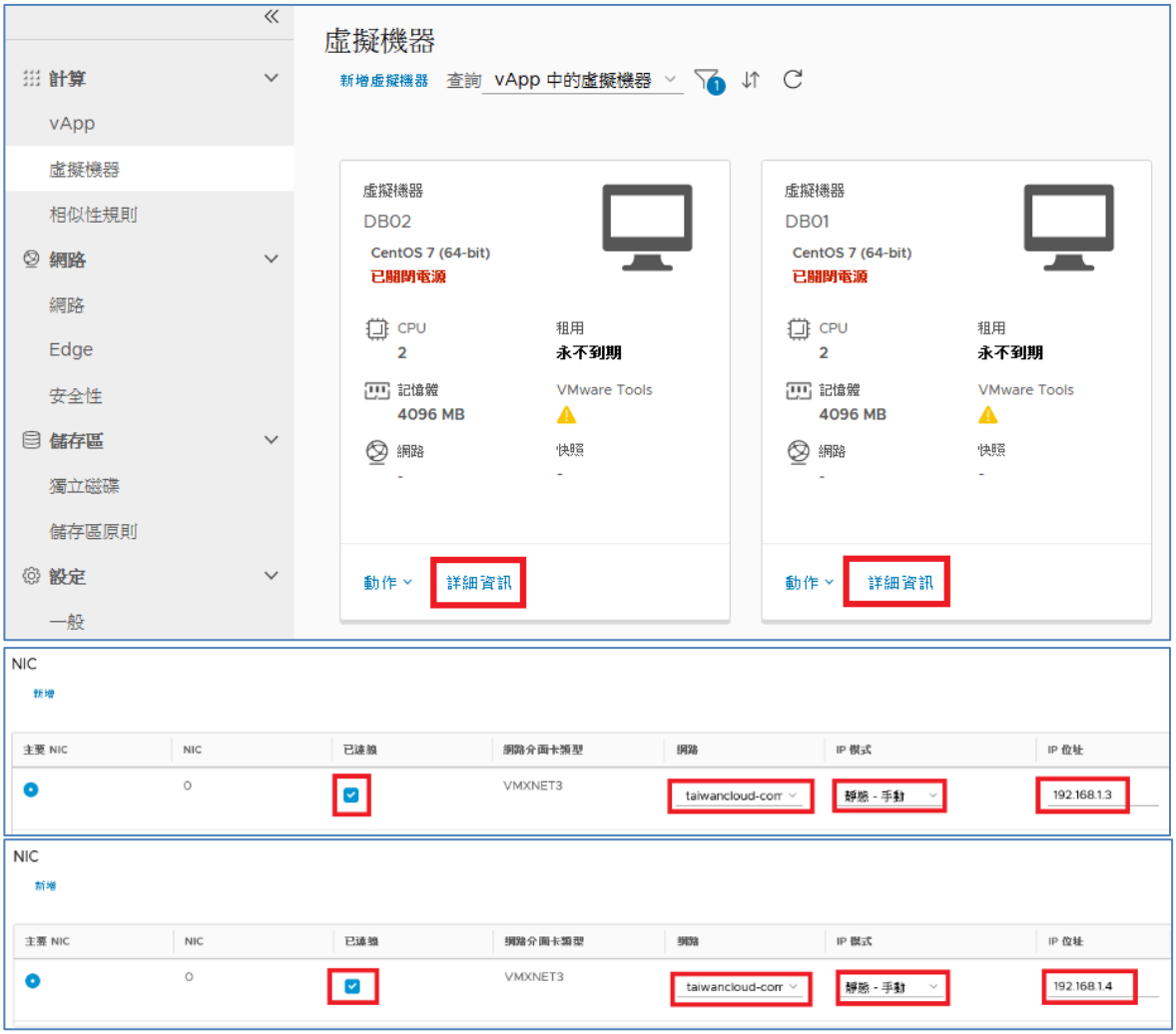
3.3 虛擬機器 > 詳細資訊 > 硬體 > NIC

勾選已連線

選取網路(此例為 taiwancloud-com-NET-DB)

IP 模式為手動

設定 IP



4 Firewall

4.1 點選「防火牆」>「+」

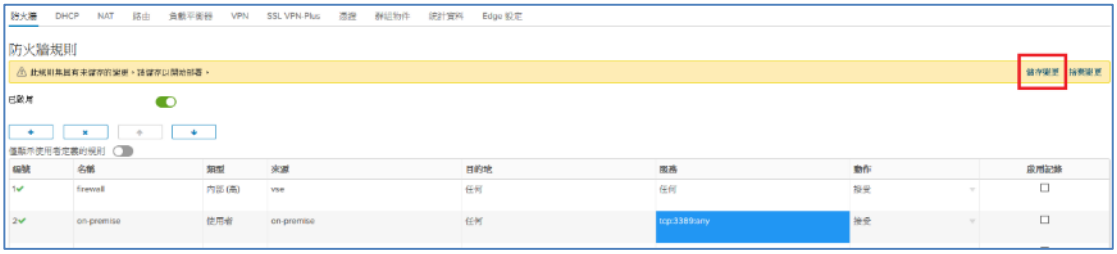
輸入名稱

來源維持任何

目的地輸入 IP(此例為 60.199.153.50)

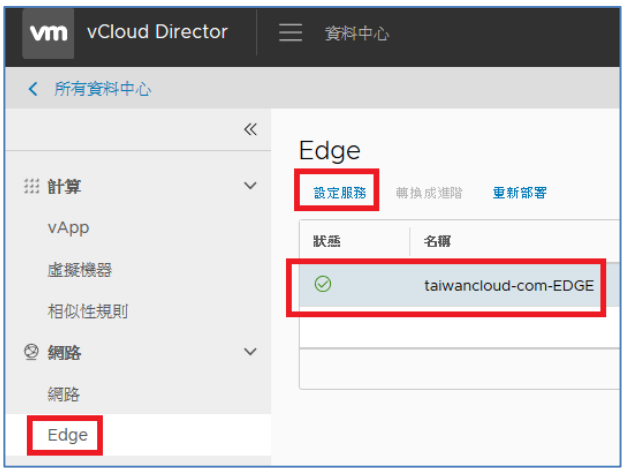
服務選 TCP 並輸入目的地連接埠(此例為 8080)

1.1 點選畫面上方「儲存變更」



5 Load Balance

5.1 點選網路>「Edge」>「設定服務」



5.2 點選「負載平衡器」>「全域組態」

勾選已啟用

點選儲存設定

5.3 點選「集區」>「+」

輸入名稱(此例為 Web)

選取演算法(此例為 Round-Robin)

點選新增成員+

輸入名稱、IP 與 port(此例為 192.168.0.1~192.168.0.2，port 80)

5.4 點選「虛擬伺服器」>「+」

勾選啟用虛擬伺服器

輸入名稱

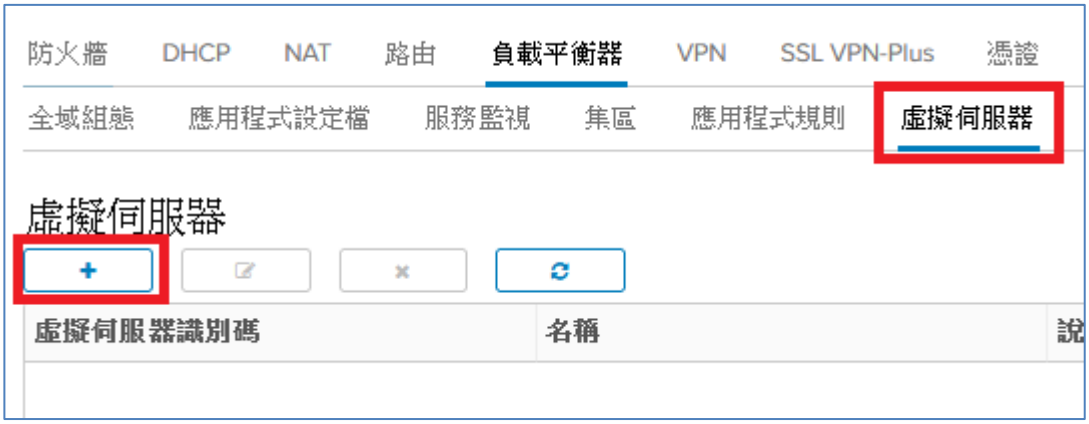
選取 IP 位址(此例為 60.199.153.50)

選取通訊設定(此例為 HTTP)

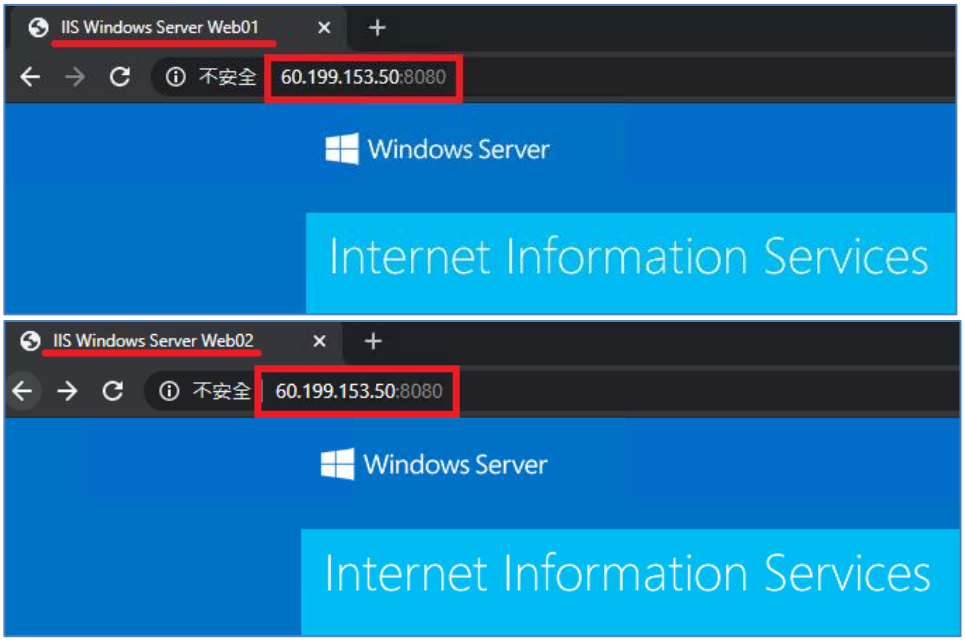
輸入連接埠(此例為 8080)

選取預設集區(此例為 Web)

點選「保留」



5.5 透過遠端進行測試(演算法 Round-Robin)

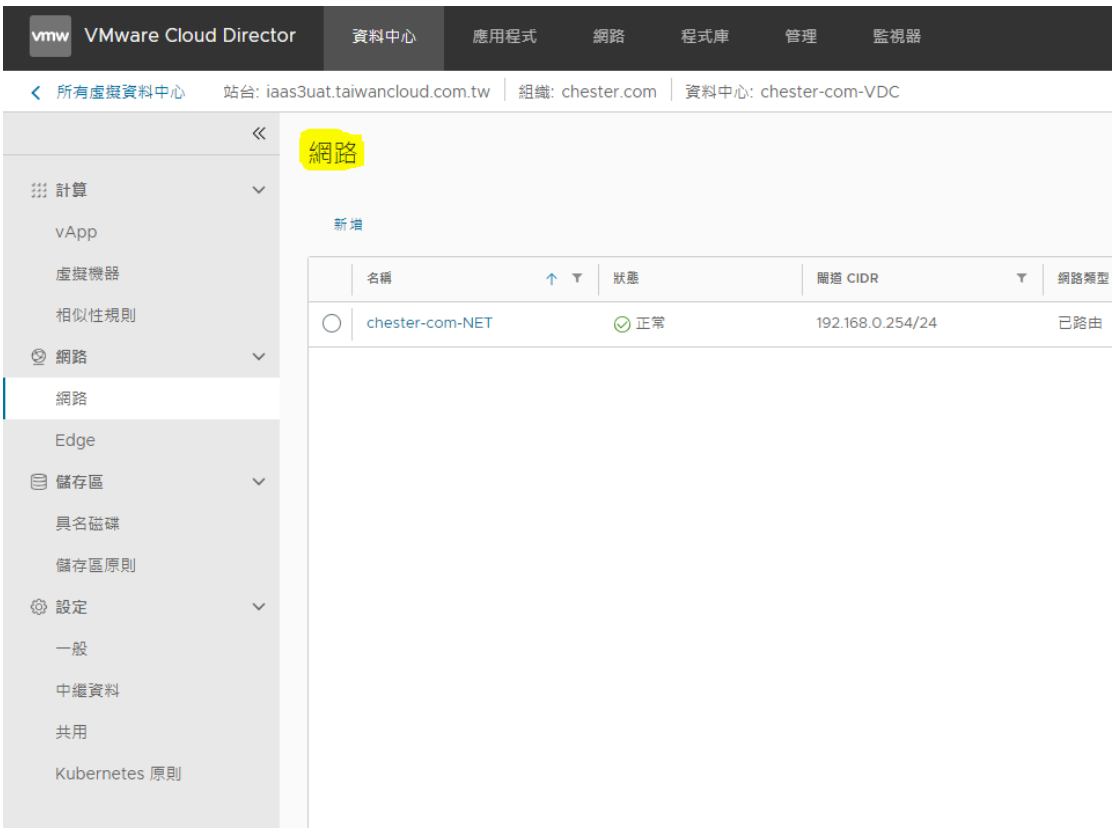


新版設定(適用 2023/9/5 後移轉用戶或新申裝用戶)

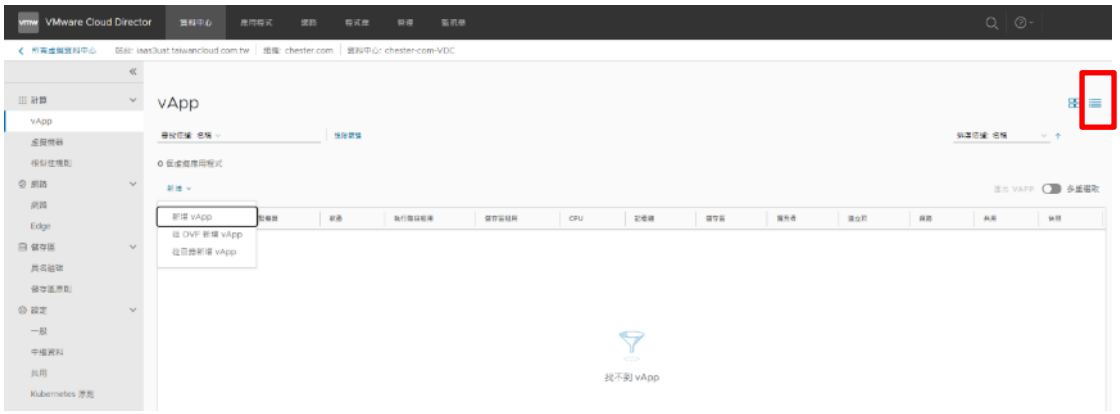
(新版設定方式適用 2023/9/5 後移轉用戶或新申裝用戶參考。)

1 Add Network(DB)

1.1 資料中心 > OVDC > 網路 > 網路 > 新增



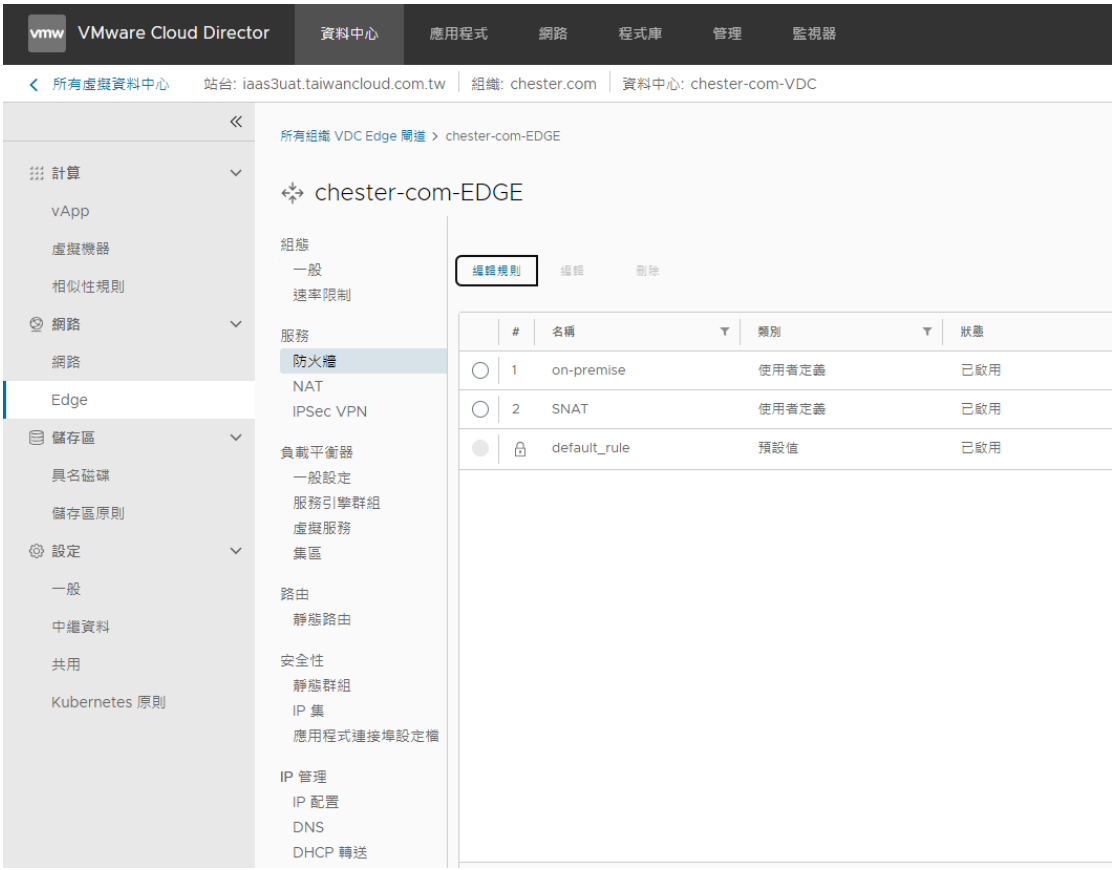
1.2 資料中心 > OVDC >計算 > vApp > 詳細資訊(紅框) > 網路 > 新增



1.3 資料中心 > OVDC >計算 > 虛擬機器 >點選硬體 > NIC > 編輯 > 新增

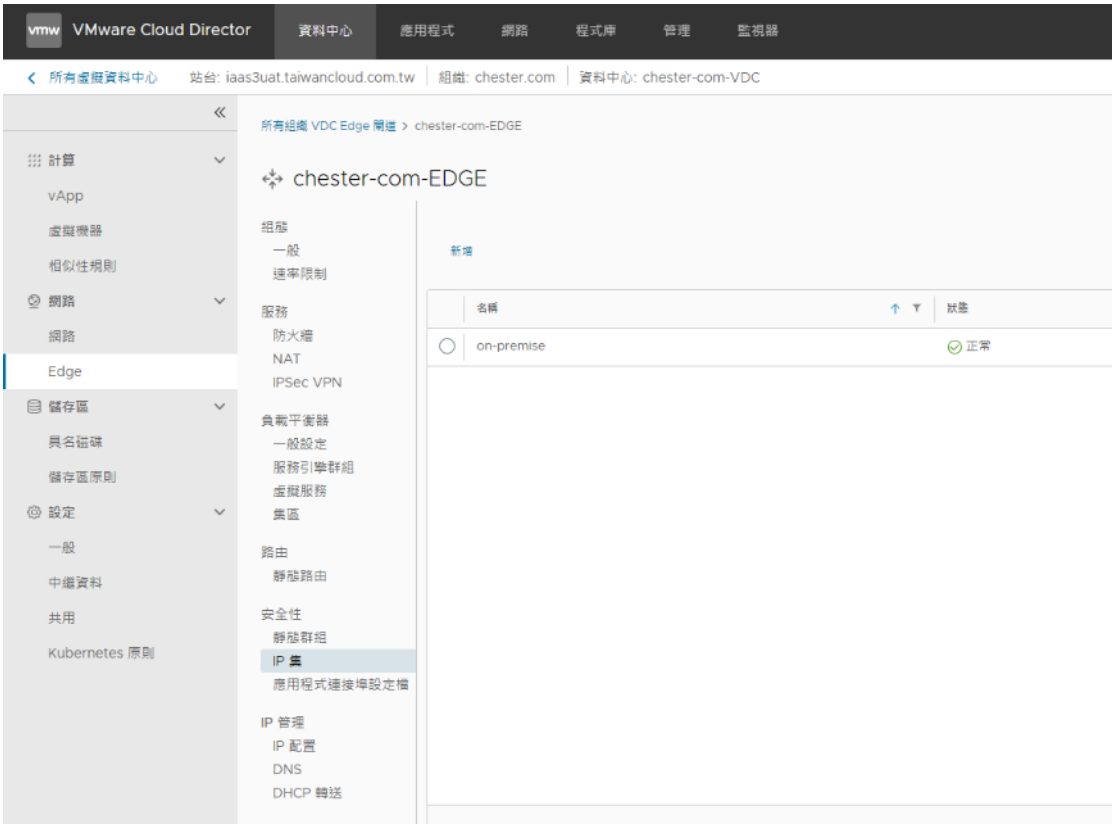
2 Firewall

2.1 資料中心 > OVDC > 網路 > Edge > 點選服務 > 防火牆 > 編輯規則 > 在頂部新增

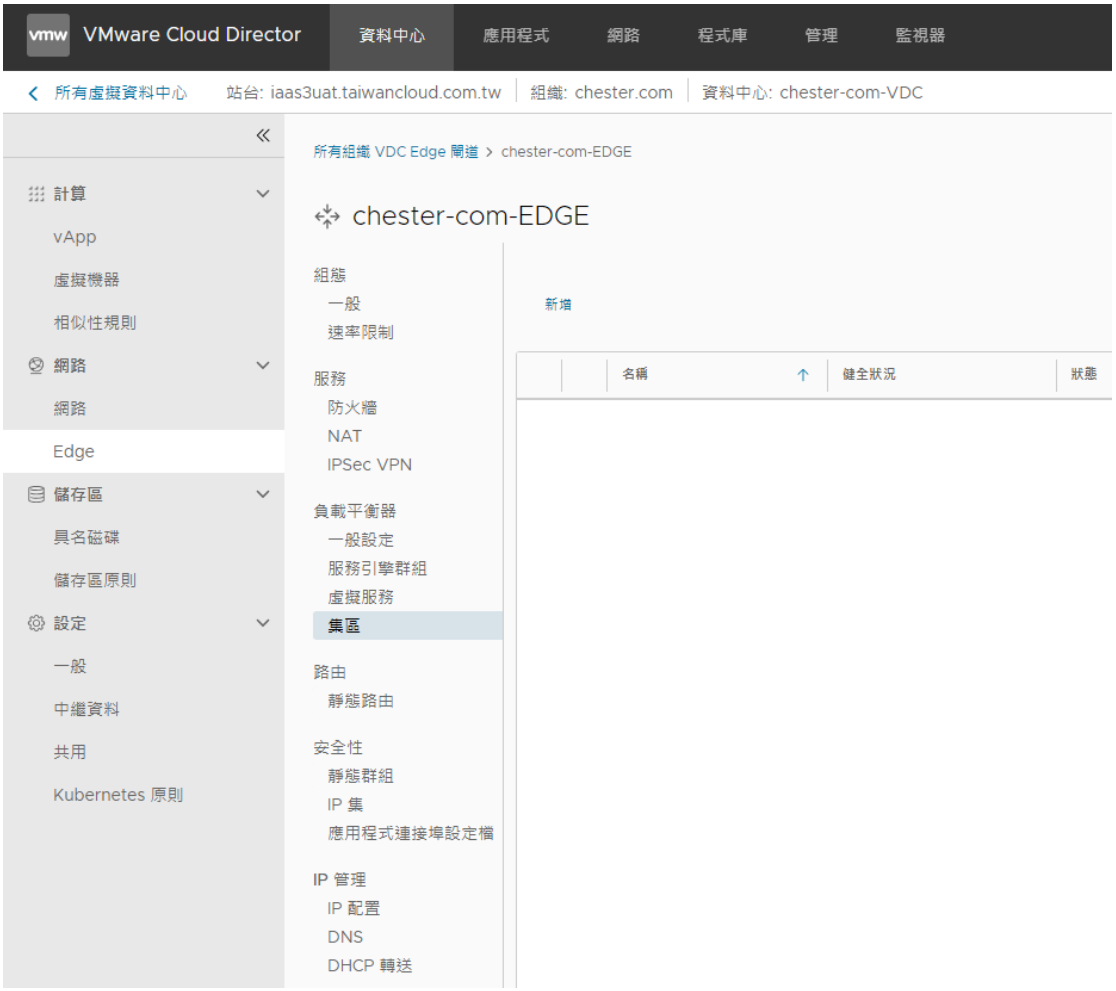


3 Load Balance

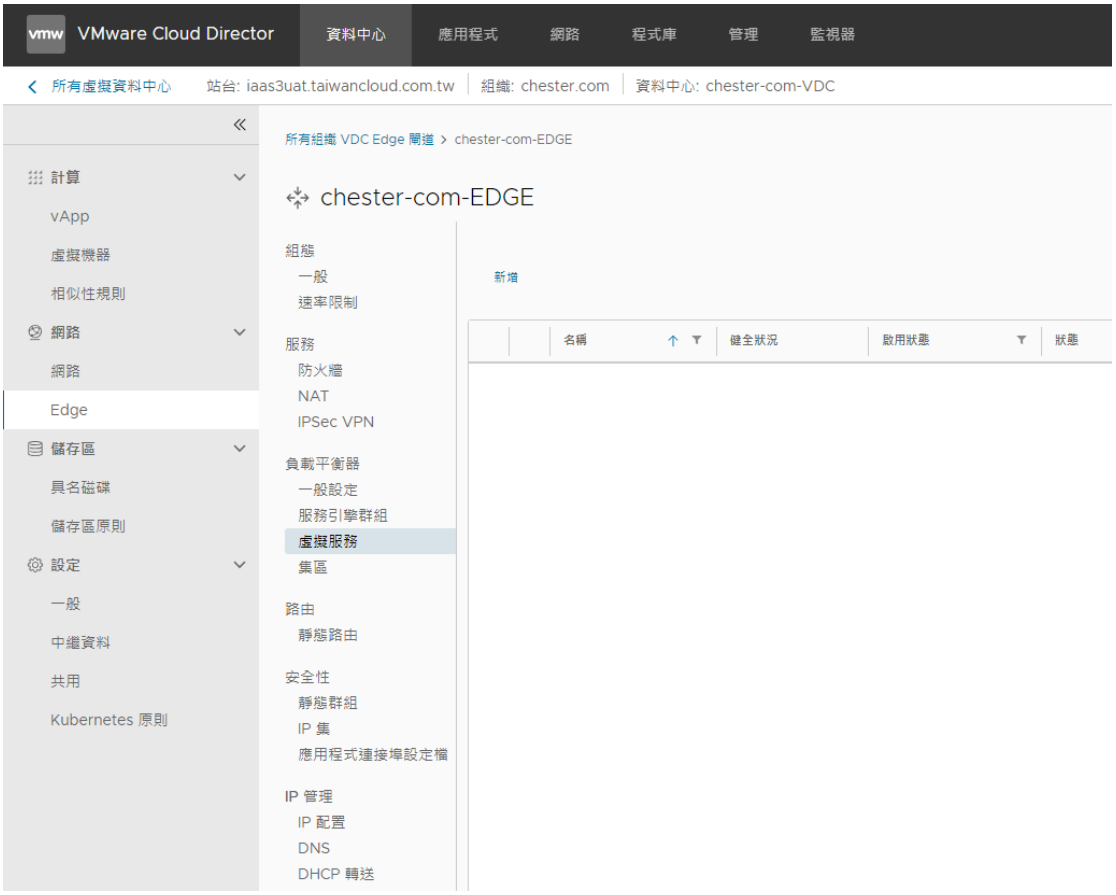
3.1 資料中心 > OVDC > 網路 > Edge > 點選服務 > 安全性 > IP 集 > 新增



3.2 資料中心 > OVDC > 網路 > Edge > 負載平衡器 > 集區



3.3 資料中心 > OVDC > 網路 > Edge > 負載平衡器 > 虛擬服務


VMware Cloud Director
資料中心
應用程式
網路
程式庫
管理
監視器
所有虛擬資料中心
站台: iaas3uat.taiwancloud.com.tw
組織: chester.com
資料中心: chester-com-VDC
計算
vApp
虛擬機器
相似性規則
網路
網路
Edge
儲存區
具名磁碟
儲存區原則
設定
一般
中繼資料
共用
Kubernetes 原則
所有組織 VDC Edge 閘道 > chester-com-EDGE
chester-com-EDGE
組態
一般
速率限制
服務
防火牆
NAT
IPSec VPN
負載平衡器
一般設定
服務引擎群組
虛擬服務
集區
路由
靜態路由
安全性
靜態群組
IP 集
應用程式連接埠設定檔
IP 管理
IP 配置
DNS
DHCP 轉送
新增
名稱
健全狀況
啟用狀態
狀態

17. 附件

A.《Windows Server 檔案與磁碟加密》

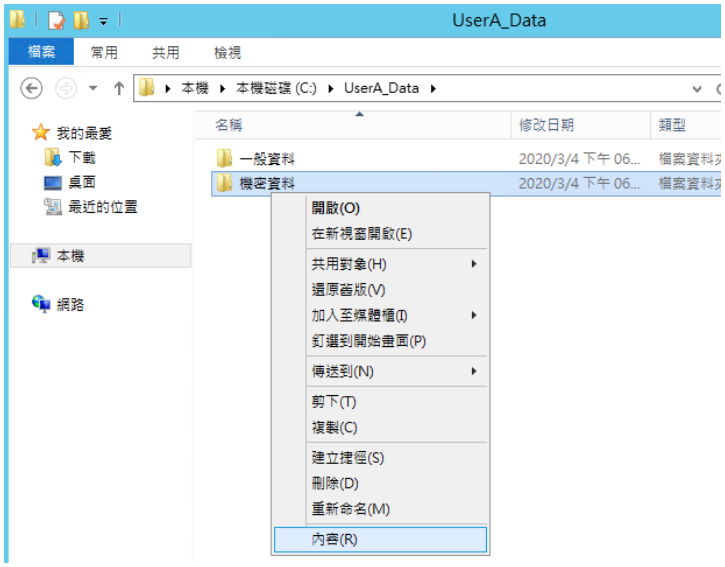
應用範圍：
本操作文件適用於運算雲 Windows Server 作業系統。

應用情境：
運算雲用戶可透過 Windows 作業系統提供的檔案系統加密功能(Encrypting File System EFS)與 BitLocker 進行重要資料的保護，以防止檔案未經授權存取與盜竊者無法開啟檔案內容。

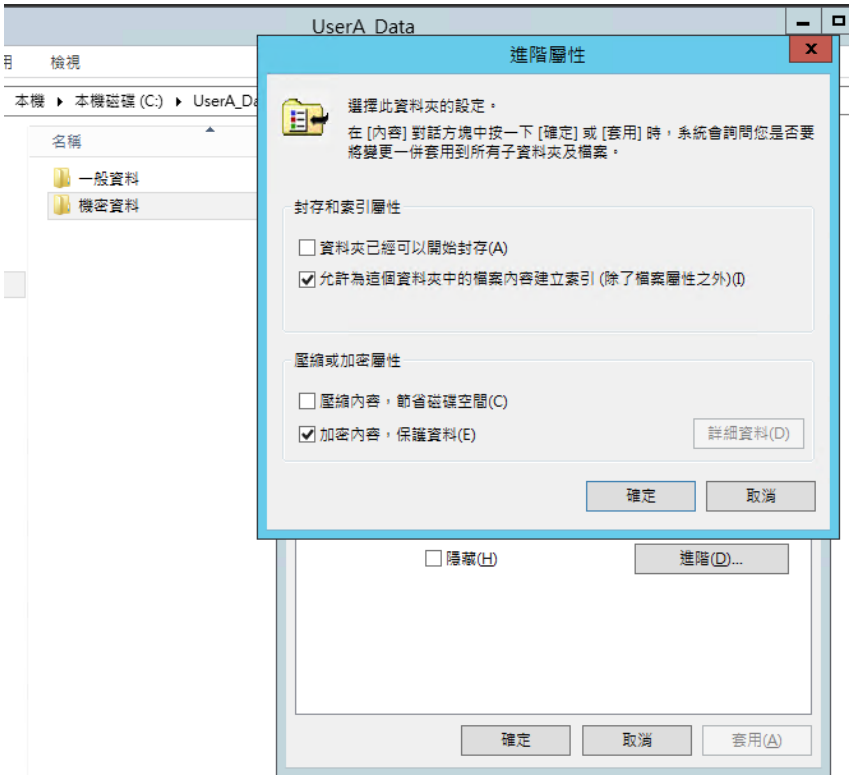
A-1. 檔案系統(EFS)加密

功能說明：
EFS 加密檔案系統資料使用對稱金鑰(File Encryption Key FEK)加密檔案，再用與檔案加密用戶關聯的公鑰(Public Key)進行加密 FEK，加密過後的資料夾在系統中會被標示為加密屬性，非用戶帳號無法開啟該資料

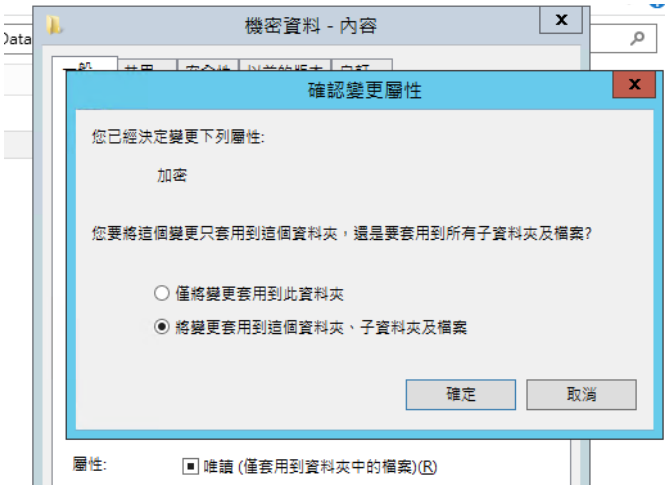
設定步驟：
選擇要加密的資料按右鍵選擇【內容】



點選【進階】打勾【加密內容，保護資料】後按【確定】

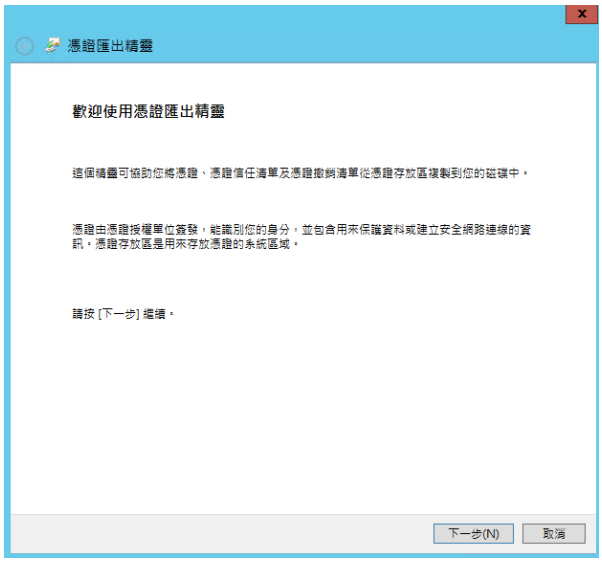


依需求選定要加密的資料夾範圍後按【確定】

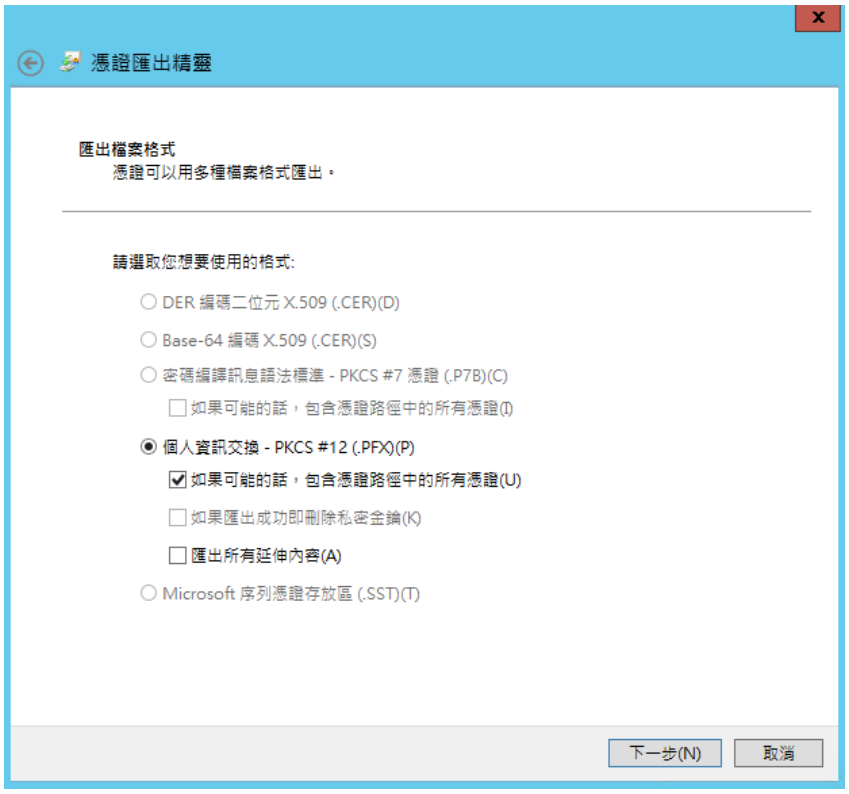


系統會提示您備份金鑰

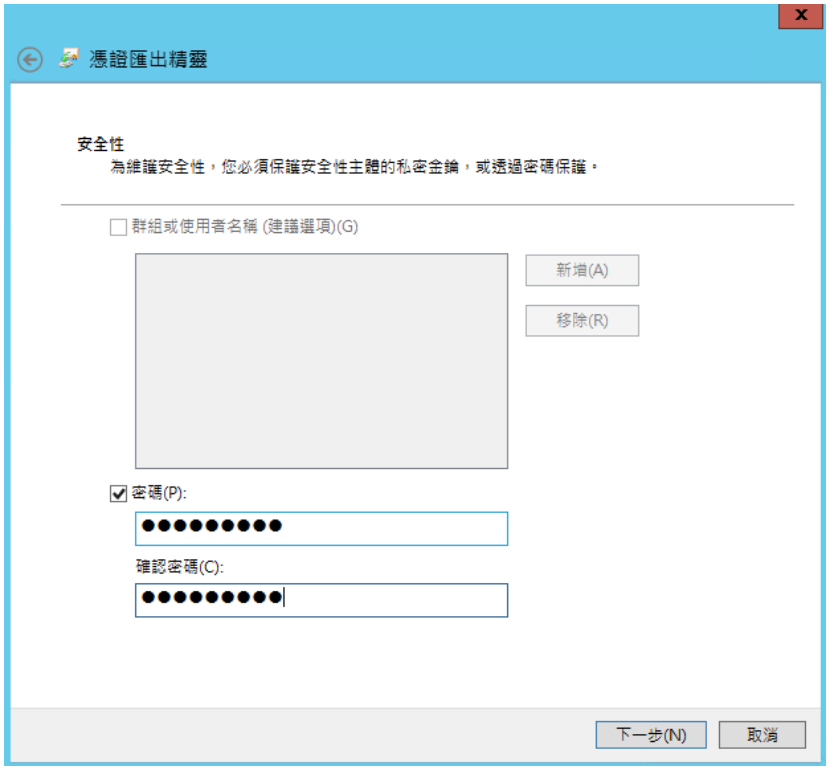
點選【下一步】繼續



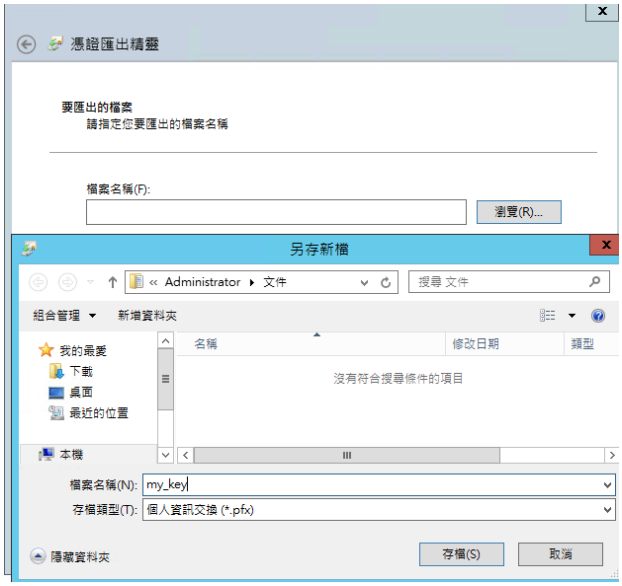
點選【下一步】繼續



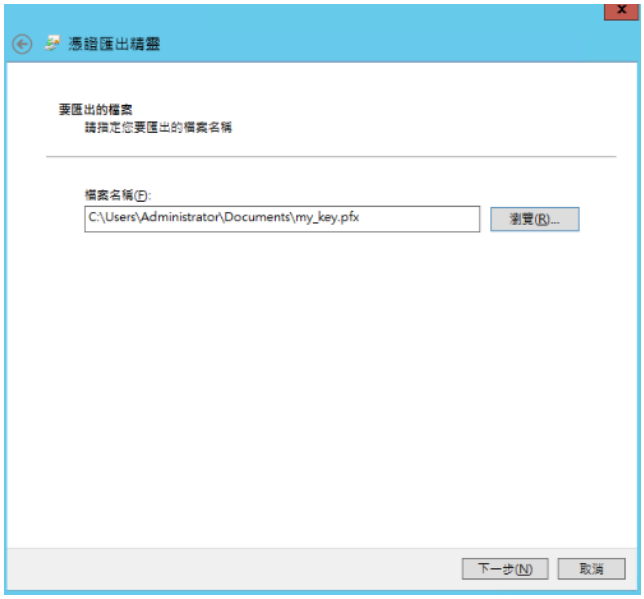
輸入密碼後點選【下一步】繼續



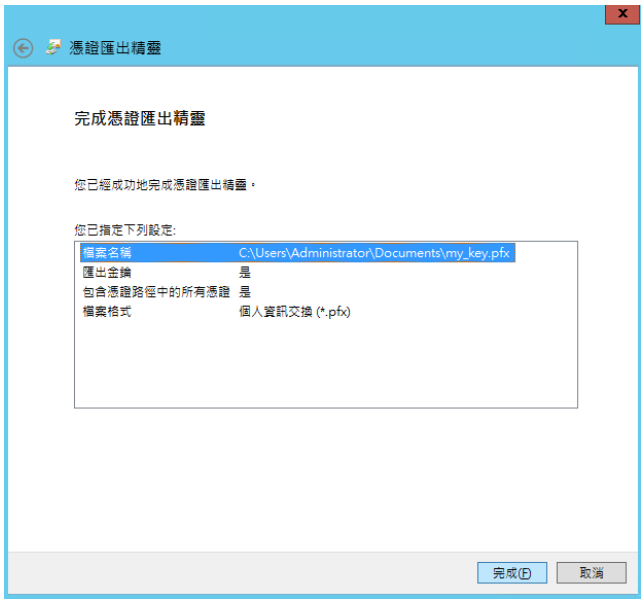
點選【瀏覽】指定存放的路徑後選擇【存檔】



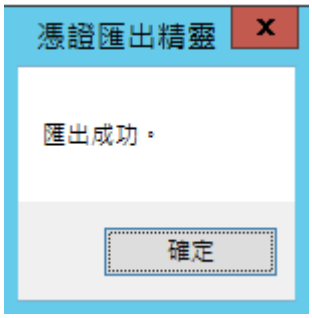
點選【下一步】繼續



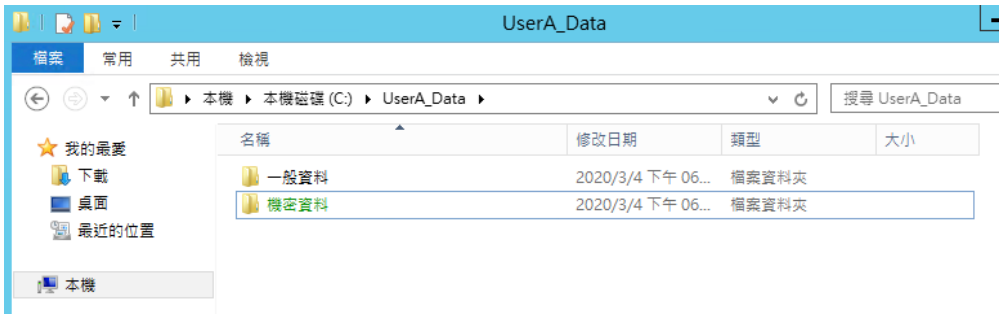
點選【完成】



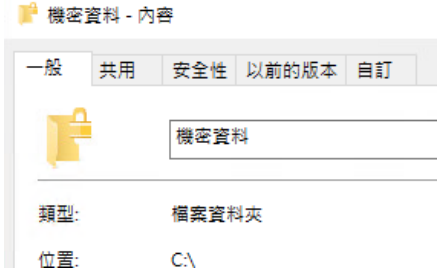
點選確定，完成設定



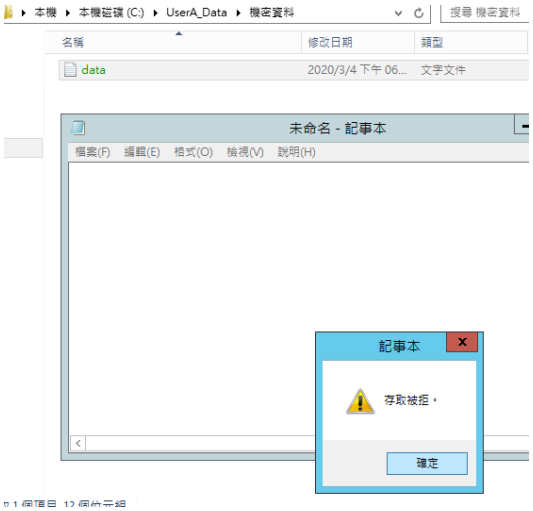
成功加密後會看到資料夾顏色變成不同(Windows 2012R2)



Windows Server 2016 以後的系統則是資料夾內容會呈現鎖頭符號



非使用者帳號無法開啟資料夾內檔案



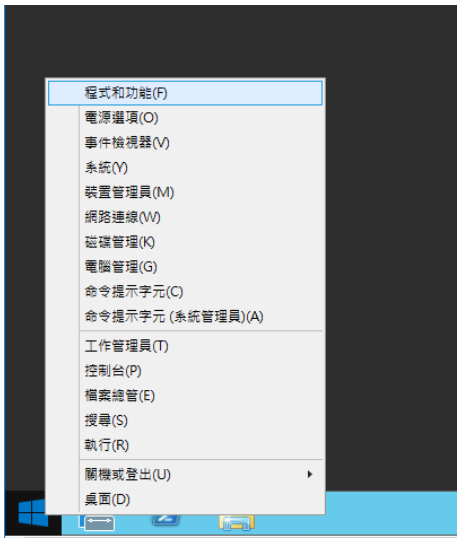
A-2. BitLocker 加密(需重啟 Windows Server)

功能說明：

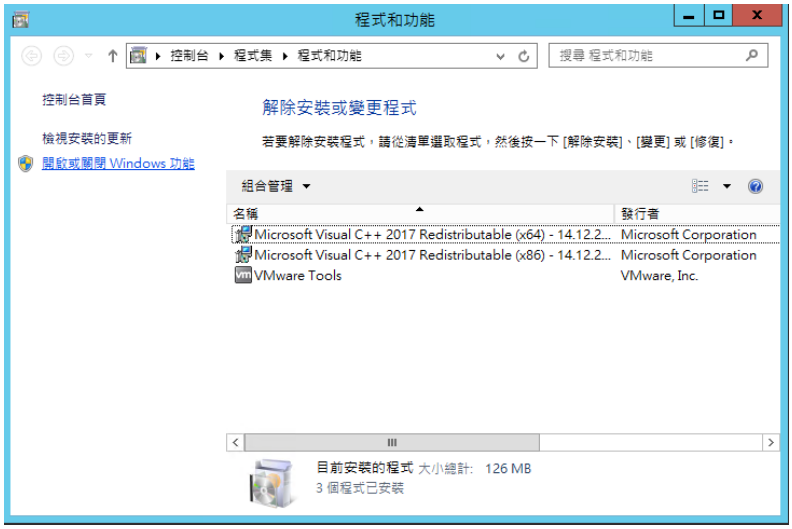
不同於 EFS 對於檔案進行加密，BitLocker 主要是針對磁碟機進行加密。當磁碟檔案遭竊取也無法存取磁碟內的資料。

設定步驟：

滑鼠桌面左下視窗圖示點選右鍵點選【程式與功能】

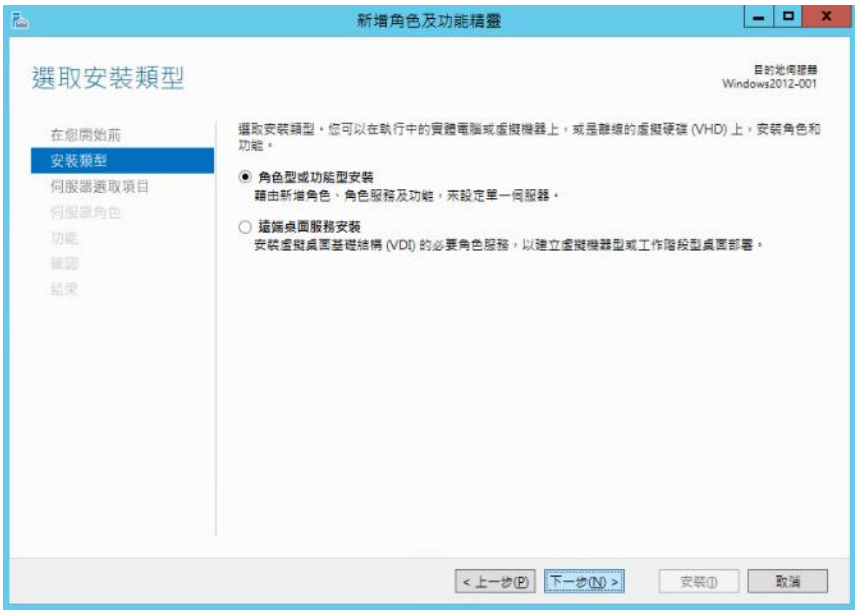


選擇開啟【開啟或關閉 Windows 功能】

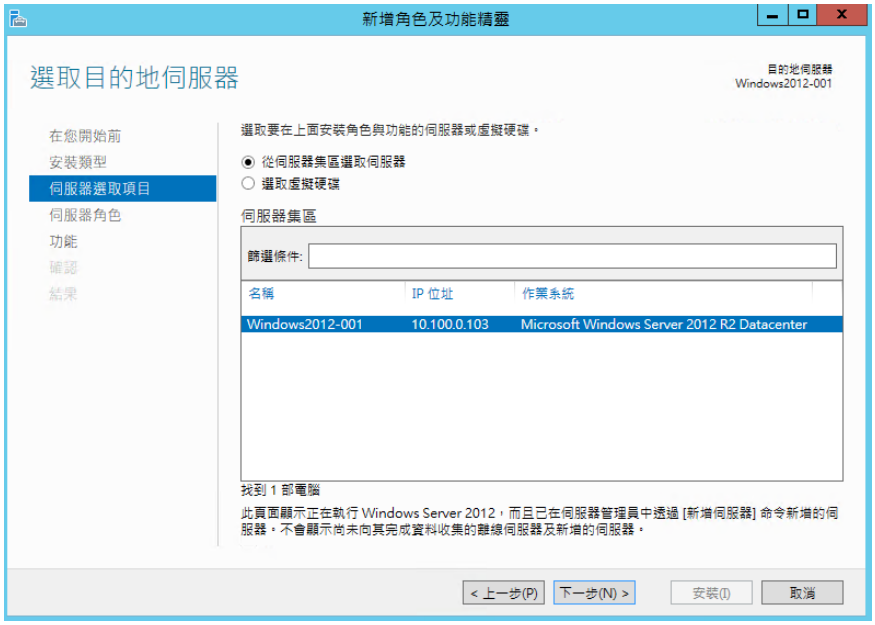


點選【下一步】繼續

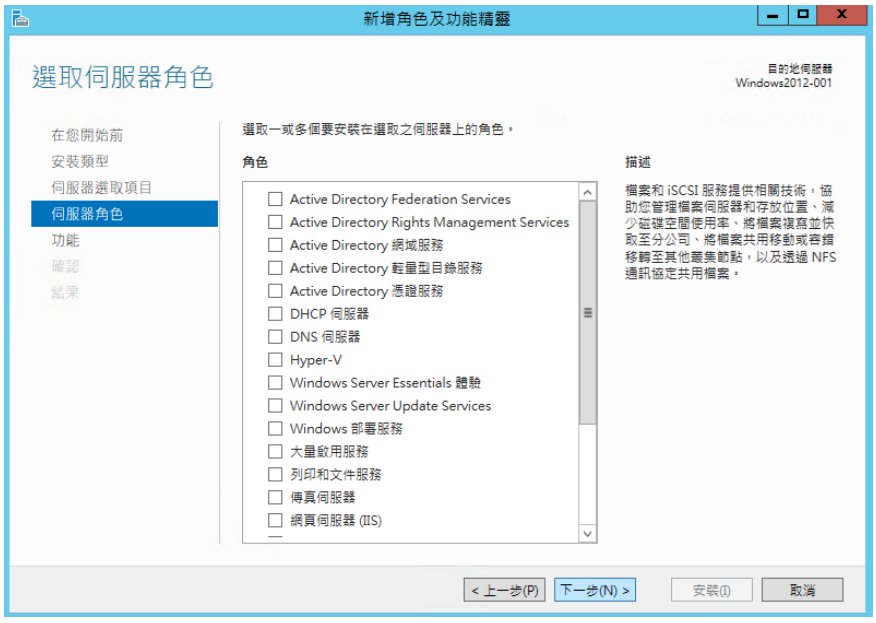
點選【下一步】繼續



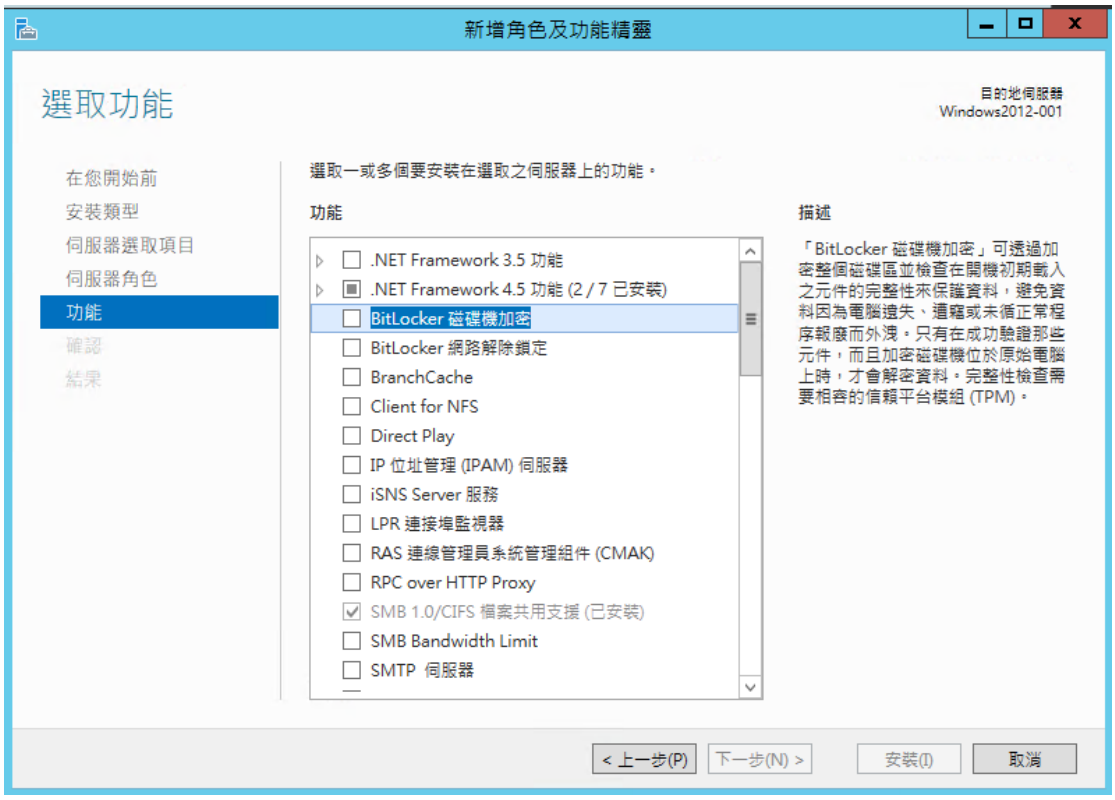
點選【下一步】繼續



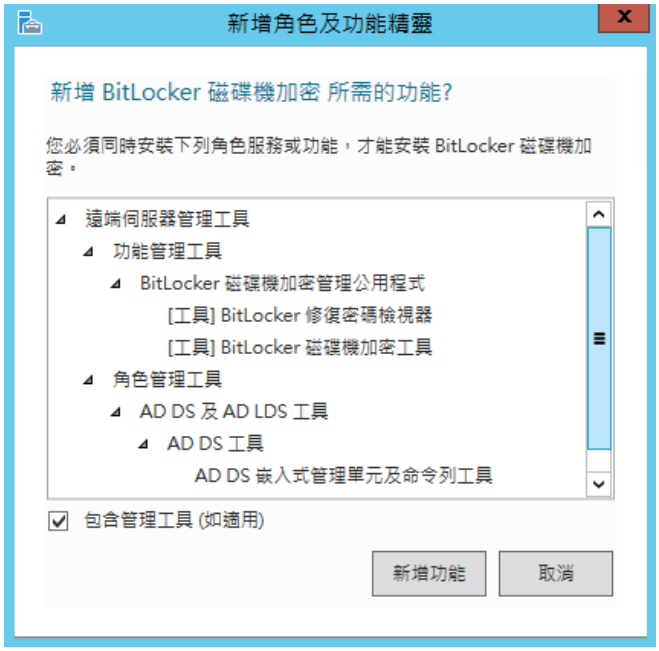
點選【下一步】繼續

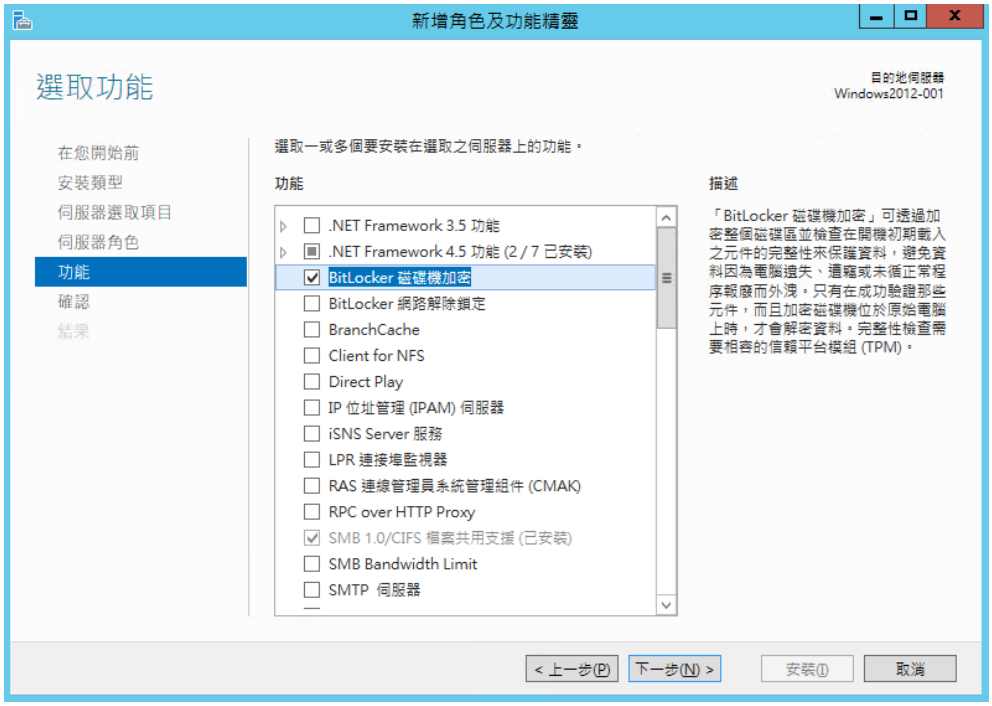


勾選【BitLocker 磁碟機加密】



勾選【新增功能】後點選【下一步】

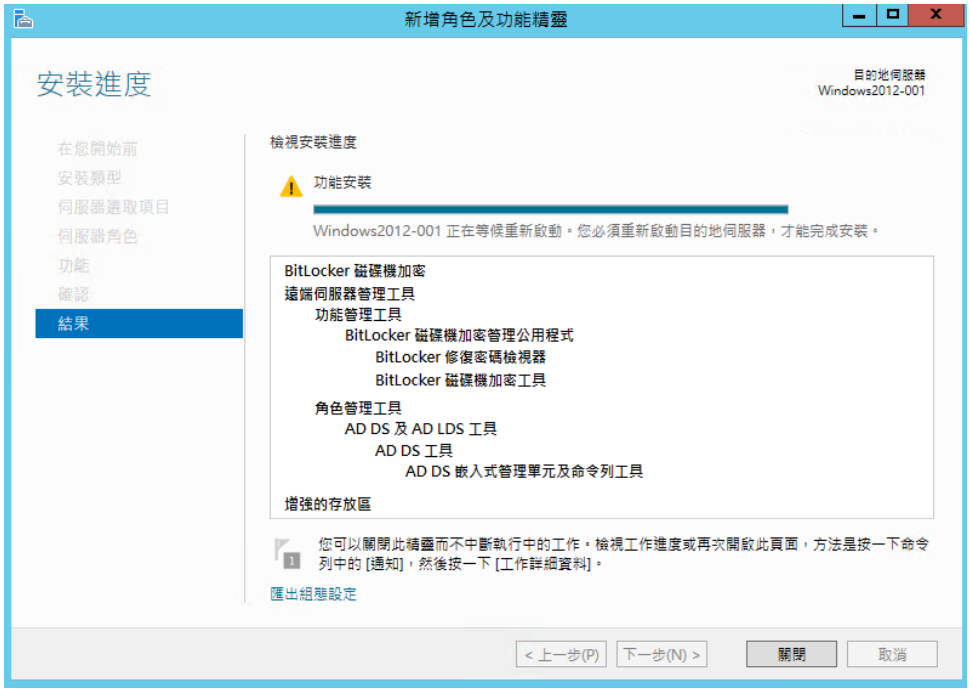



新增角色及功能精靈
選取功能
目的地伺服器
Windows2012-001
在您開始前
安裝類型
伺服器選取項目
伺服器角色
功能
確認
結果
選取一或多個要安裝在選取之伺服器上的功能。
功能
.NET Framework 3.5 功能
.NET Framework 4.5 功能 (2 / 7 已安裝)
BitLocker 磁碟機加密
BitLocker 網路解除鎖定
BranchCache
Client for NFS
Direct Play
IP 位址管理 (IPAM) 伺服器
iSNS Server 服務
LPR 連接埠監視器
RAS 連線管理員系統管理組件 (CMAK)
RPC over HTTP Proxy
SMB 1.0/CIFS 檔案共用支援 (已安裝)
SMB Bandwidth Limit
SMTP 伺服器
描述
「BitLocker 磁碟機加密」可透過加密整個磁碟區並檢查在開機初期載入之元件的完整性來保護資料，避免資料因為電腦遺失、遭竊或未循正常程序報廢而外洩。只有在成功驗證那些元件，而且加密磁碟機位於原始電腦上時，才會解密資料。完整性檢查需要相容的信賴平台模組 (TPM)。
< 上一步(P)
下一步(N) >
安裝(I)
取消

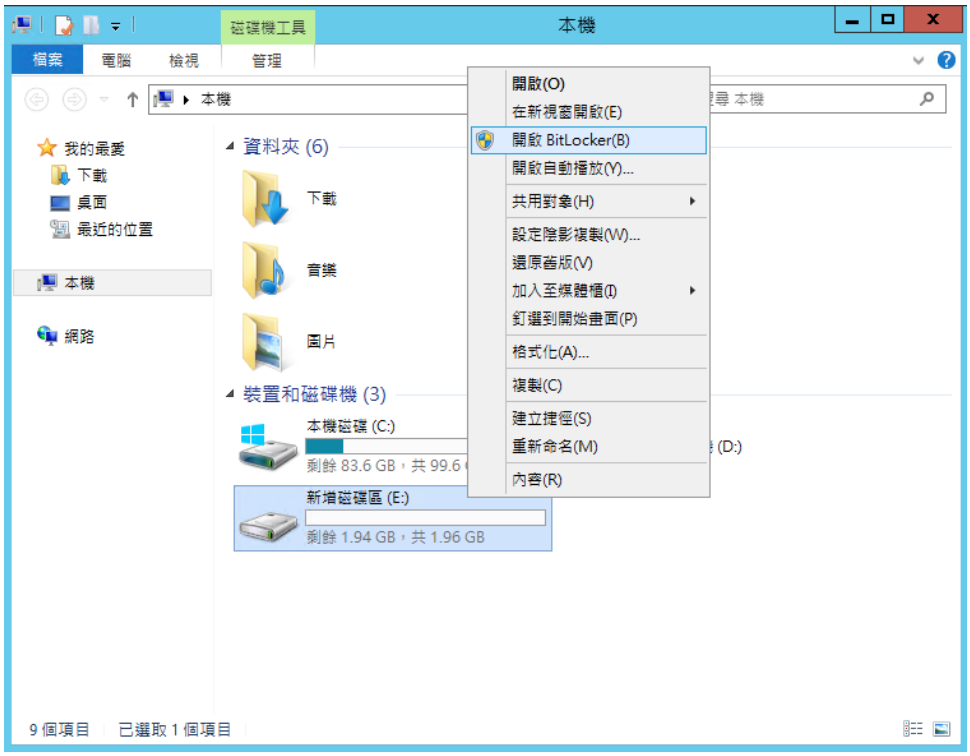
點選【安裝】


新增角色及功能精靈
確認安裝選項
目的地伺服器
Windows2012-001
在您開始前
安裝類型
伺服器選取項目
伺服器角色
功能
確認
結果
若要在選取的伺服器上安裝下列角色、角色服務或功能，請按一下 [安裝]。
必要時自動重新啟動目的地伺服器
選用功能 (例如，系統管理工具) 可能會顯示於此頁面上，因為系統已經自動選取它們。如果您不想要安裝這些選用功能，請按 [上一步] 以清除它們的核取方塊。
BitLocker 磁碟機加密
遠端伺服器管理工具
功能管理工具
BitLocker 磁碟機加密管理公用程式
BitLocker 修復密碼檢視器
BitLocker 磁碟機加密工具
角色管理工具
AD DS 及 AD LDS 工具
AD DS 工具
AD DS 嵌入式管理單元及命令列工具
增強的存放區
匯出組態設定
指定替代來源路徑
< 上一步(P)
下一步(N) >
安裝(I)
取消

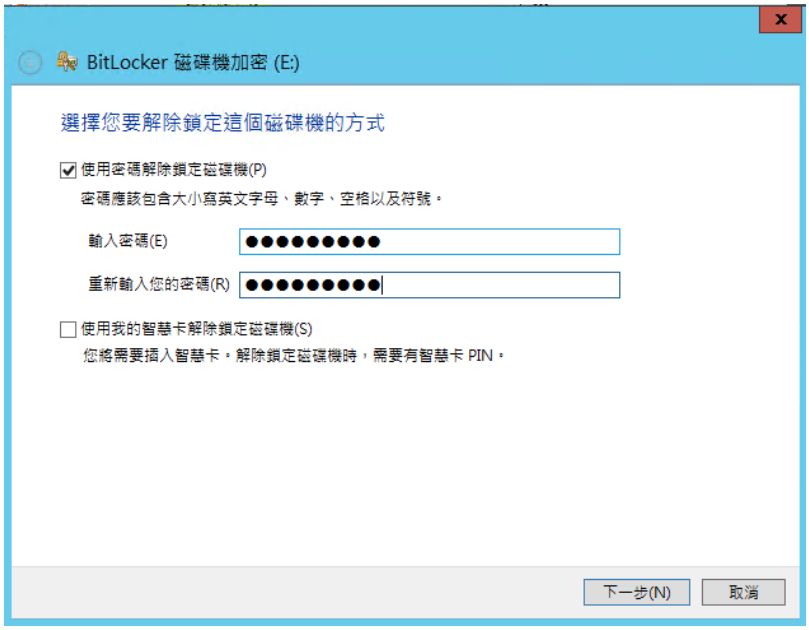
安裝完畢點選【關閉】並重新開機



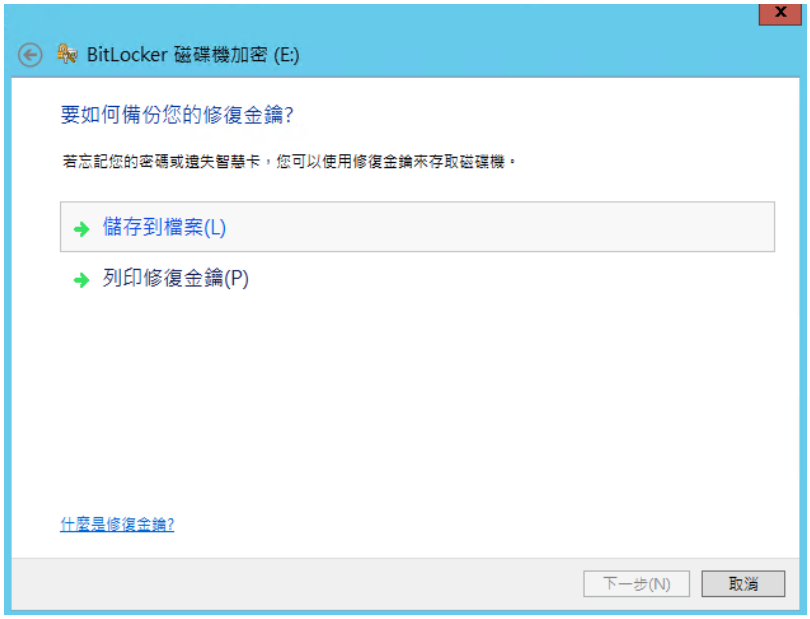
重開機後請再要加密的磁碟按右鍵選【開啟 BitLocker】



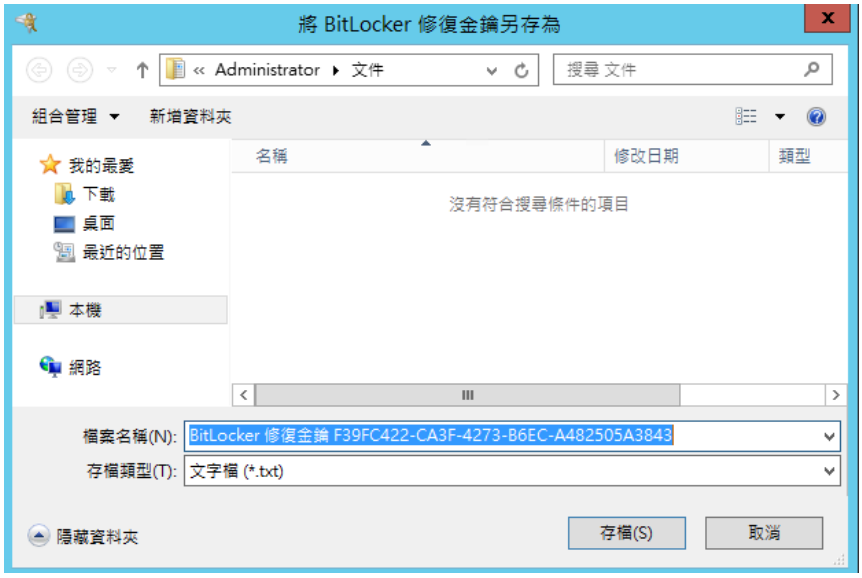
輸入解除鎖定的密碼之後按【下一步】



選擇儲存到檔案備份修復金鑰

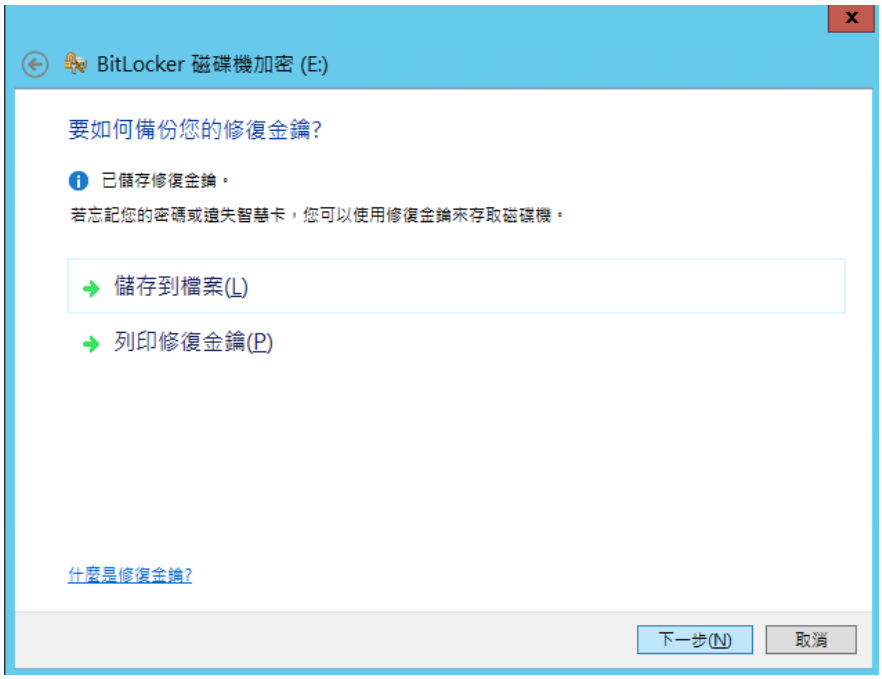


指定保存路徑

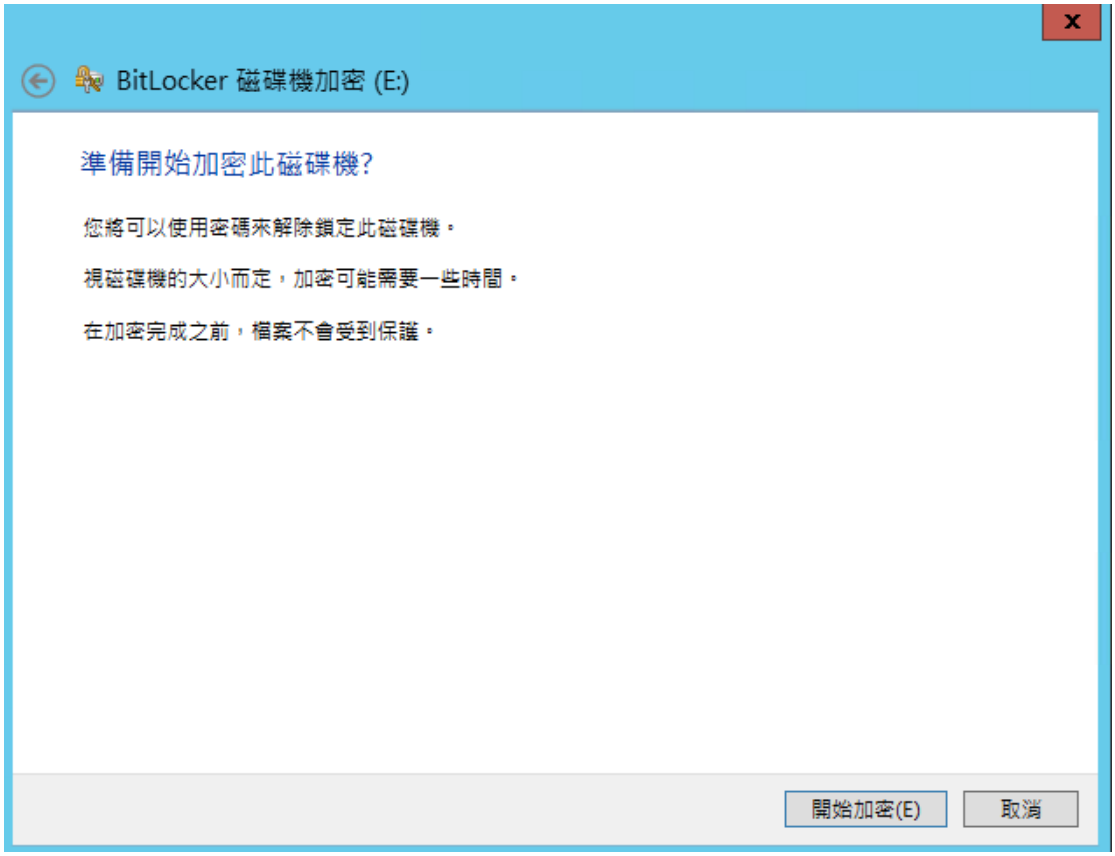


建議遵循系統提示將檔案存放多份副本在本機以外的空間，提醒您請妥善保存金鑰。

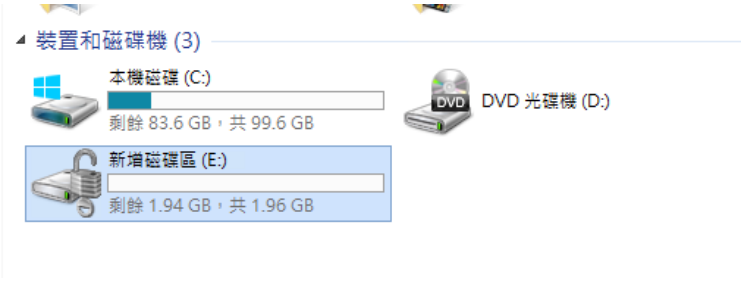
點選【下一步】


BitLocker 磁碟機加密 (E:)
要如何備份您的修復金鑰?
已儲存修復金鑰。
若忘記您的密碼或遺失智慧卡，您可以使用修復金鑰來存取磁碟機。
儲存到檔案(L)
列印修復金鑰(P)
什麼是修復金鑰?
下一步(N)
取消

點選【開始加密】


BitLocker 磁碟機加密 (E:)
準備開始加密此磁碟機?
您將可以使用密碼來解除鎖定此磁碟機。
視磁碟機的大小而定，加密可能需要一些時間。
在加密完成之前，檔案不會受到保護。
開始加密(E)
取消

加密完成後會看到有鎖頭圖示，代表設定完成。



B.《Linux 磁碟加密說明》:

CentOS、Ubuntu、Rocky Linux 與 Oracle Linux 皆可使用 dm-crypt 增加安全性，加密的磁碟資料，即使 dump 出來，看到的也是亂碼。下文將會介紹使用 dm-crypt 來建立加密檔案系統的方法。

OS	OS version	Cryptsetup version
CentOS	6.10	1.20
	7.7	2.0.3
	7.9	2.0.3
Ubuntu	20.04	2.2.2
	22.04	2.4.3
	24.04	2.7.0
Rocky Linux	8.7	2.3.7
	8.8	2.3.7
	9.1	2.6.0
	9.2	2.6.0
Oracle Linux	8.7	2.3.7
	8.8	2.3.7
	9.1	2.6.0
	9.2	2.6.0

以下以 CentOS 為範例，Ubuntu、Rocky Linux 與 Oracle Linux 步驟皆相同。

前置作業：

確認 CentOS 版本

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.9.1.el7.x86_64 on an x86_64

centos75-001 login: root
Password:
Last login: Wed Feb  5 17:11:08 on tty1
[root@centos75-001 ~]# cat /etc/*realease
cat: /etc/*realease: No such file or directory
[root@centos75-001 ~]# cat /etc/*release
CentOS Linux release 7.7.1908 (Core)
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"
```

確認已安裝 cryptsetup 套件

```
[root@centos75-001 ~]# cryptsetup --version
cryptsetup 2.0.3
```

若沒有套件就使用 yum install cryptsetup 安裝(ubuntu 請使用 apt-get)

```
[root@centos77-template-001 ~]# yum install cryptsetup
Loaded plugins: fastestmirror
Determining fastest mirrors
 * base: ftp.tc.edu.tw
 * extras: ftp.tc.edu.tw
 * updates: ftp.isu.edu.tw
base                                                     | 3.6 kB  00:00:00
extras                                                   | 2.9 kB  00:00:00
updates                                                  | 2.9 kB  00:00:00
(1/2): extras/7/x86_64/primary_db                        | 164 kB  00:00:00
(2/2): updates/7/x86_64/primary_db                       | 6.7 MB  00:00:00
Resolving Dependencies
--> Running transaction check
---> Package cryptsetup.x86_64 0:2.0.3-5.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package              Arch              Version                 Repository    Size
================================================================================
Installing:
 cryptsetup           x86_64            2.0.3-5.el7             base         154 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 154 k
Installed size: 354 k
Is this ok [y/d/N]: y
```

設定步驟：

以 Centos 7.7 示範使用 cryptsetup 對/dev/sdb1 磁碟進行加密。

建立新的/dev/sdb 磁碟分割

```
[root@centos77-template-001 ~]# fdisk /dev/sdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0xfad10cb6.

Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-4194303, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-4194303, default 4194303):
Using default value 4194303
Partition 1 of type Linux and of size 2 GiB is set

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[root@centos77-template-001 ~]# _
```

使用以下指令加密建立好的磁碟分割/dev/sdb1 輸入"大寫"YES 與密碼，進行磁碟加密。(請注意 F 是大寫)

cryptsetup --verify-passphrase --cipher aes-cbc-essiv:sha256 --key-size256 luksFormat /dev/sdb1

```
[root@centos77-template-001 ~]# cryptsetup --verify-passphrase --cipher aes-cbc-essiv:sha256 --key-s
ize 256 luksFormat /dev/sdb1

WARNING!
========
This will overwrite data on /dev/sdb1 irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase for /dev/sdb1:
Verify passphrase:
[root@centos77-template-001 ~]#
```

掛載加密的磁碟須使用 cryptsetup luksOpen /dev/sdb1 映射名稱，輸入密碼即可將加密的磁碟映射到/dev/mapper/映射名稱

```
[root@centos77-template-001 ~]# cryptsetup luksOpen /dev/sdb1 encrypted_data
Enter passphrase for /dev/sdb1:
```

第一次使用磁碟需格式化磁碟，請注意這裡使用的路徑是 /dev/mapper/encrypted_data (也就是自訂的映射名稱)

```
[root@centos77-template-001 ~]# mkfs.ext4 /dev/mapper/encrypted_data
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
131072 inodes, 523520 blocks
26176 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=536870912
16 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

最後掛載磁碟到指定的目錄上即完成設定，放入此目錄類的資料均會被加密。

```
[root@centos77-template-001 ~]# mkdir /encrypted_data
[root@centos77-template-001 ~]# mount /dev/mapper/encrypted_data /encrypted_data/
```

※請注意當作業系統重新啟動後必須使用 cryptsetup 開啟並提供密碼後才可以將加密過的磁碟進行掛載。

C. Windows2008R2 修改系統管理員密碼

【提醒】: 執行以下動作時，請用戶自行評估 VM 上之環境及服務，採最適方法，若有風險考量，請於執行前進行備份。另建議加速升版，避免遭遇不可預期的安全性及功能性問題，謝謝。

Windows 2008R2 預設無法使用客體自訂功能，若使用者忘記密碼，可以透過下述兩種方式修改。

一、 安裝 vcredist_x86 開啟客體自訂功能

VMware 官方 KB 連結，客體自訂說明

https://kb.vmware.com/s/article/66765?lang=en_us

vmware Knowledge Base | Training | Community | Store | My VMware | Tips on searching for a KB

Guest OS Customization fails on Windows Server 2008, Windows Server 2008 R2 and Windows Vista which installed VMTools 10.3.0 or above version (66765)

Symptoms

- The Windows VM's network adapter is disconnected after Guest OS Customization
- Guest OS Customization does NOT take effect
- In the `%WINDIR%\temp\toolsDeployPkg.log` file, you see that "`[ info] Command Completed with exit code -1072365566`"

Cause

This issue occurs when guest OS customization command fails to find Microsoft Visual C++ 2008 Redistributable runtime.

Resolution

Currently, there is no resolution.

Workaround

To workaround this issue, install Microsoft Visual C++ 2008 Redistributable on Windows:

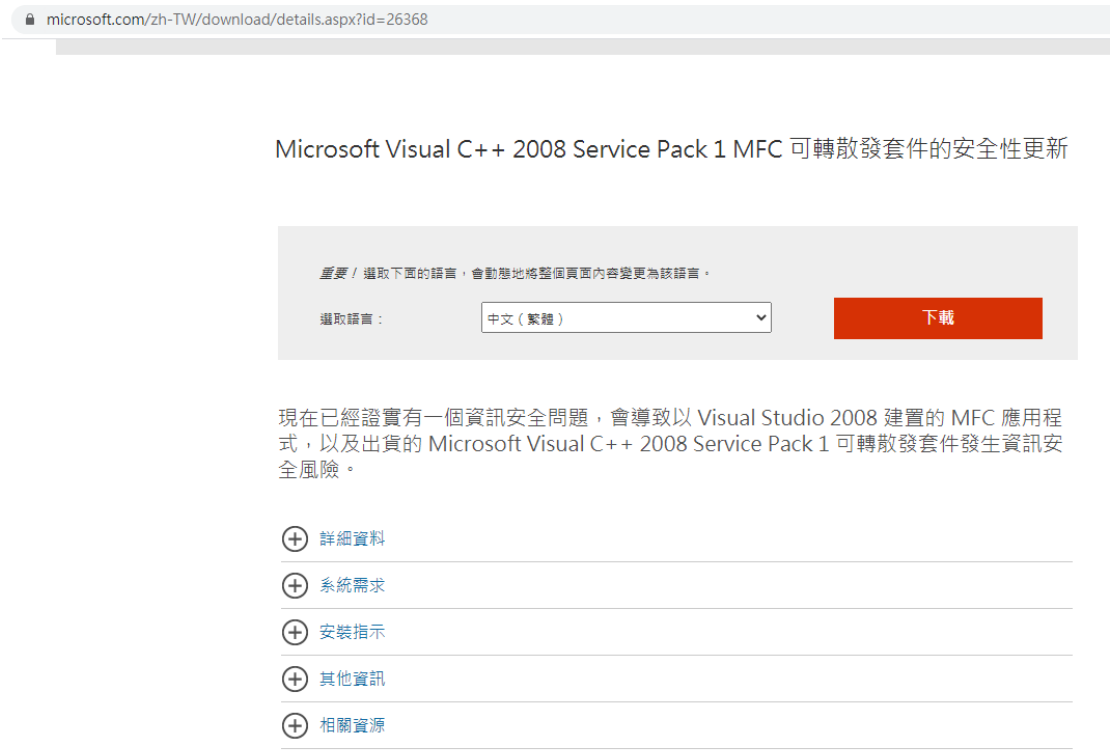
1. Go to https://www.microsoft.com/en-us/download/details.aspx?id=26368 and download:

   `Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package MFC Security Update`

2. Select `vcredist_x86.exe` to download and install it on Windows.

請到以下連結，下載安裝vcredist_x86.exe

https://www.microsoft.com/en-us/download/details.aspx?id=26368

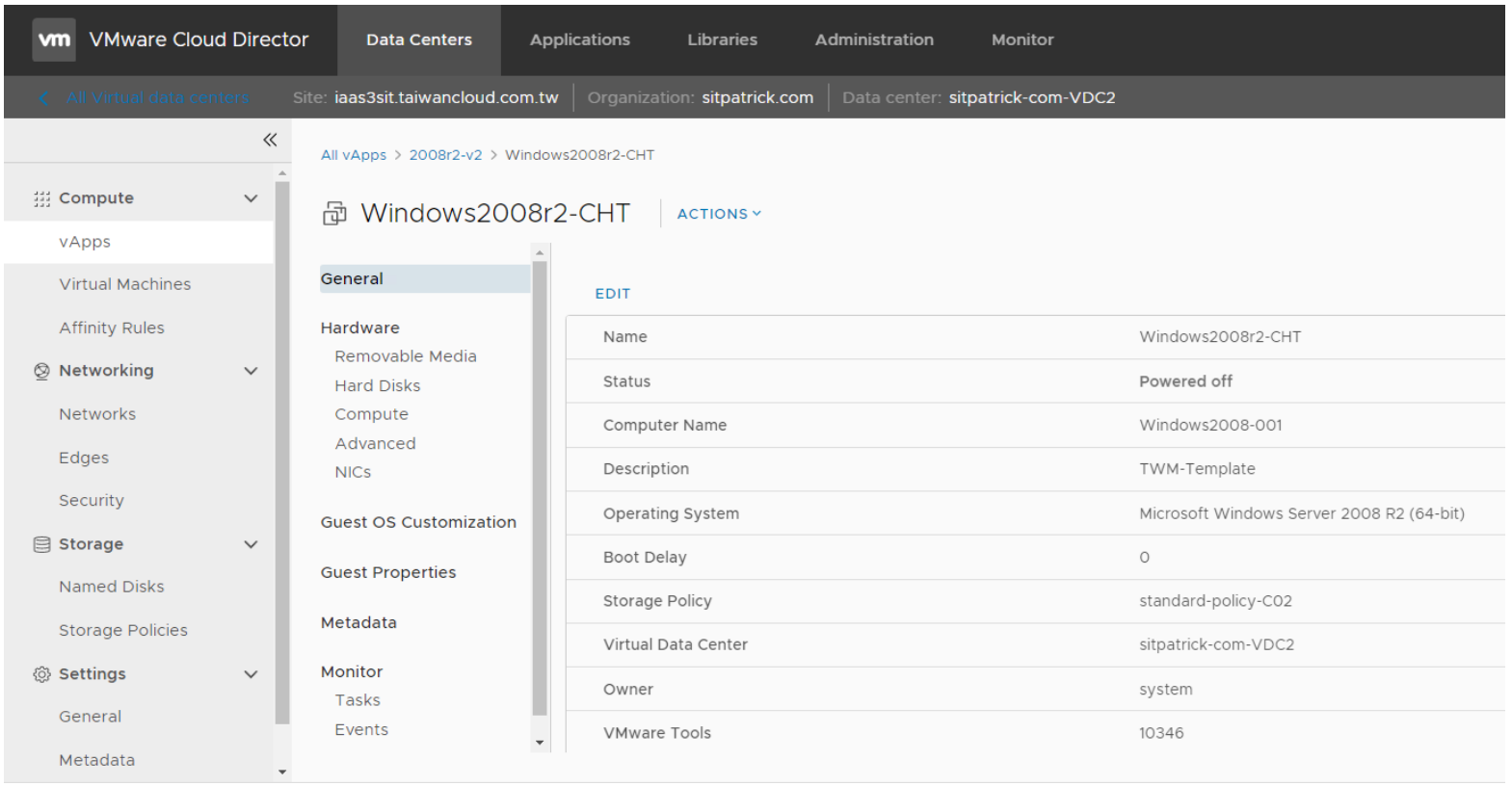


安裝完成後客體自訂功能就會生效，可以使用客體自訂修改系統管理員密碼。

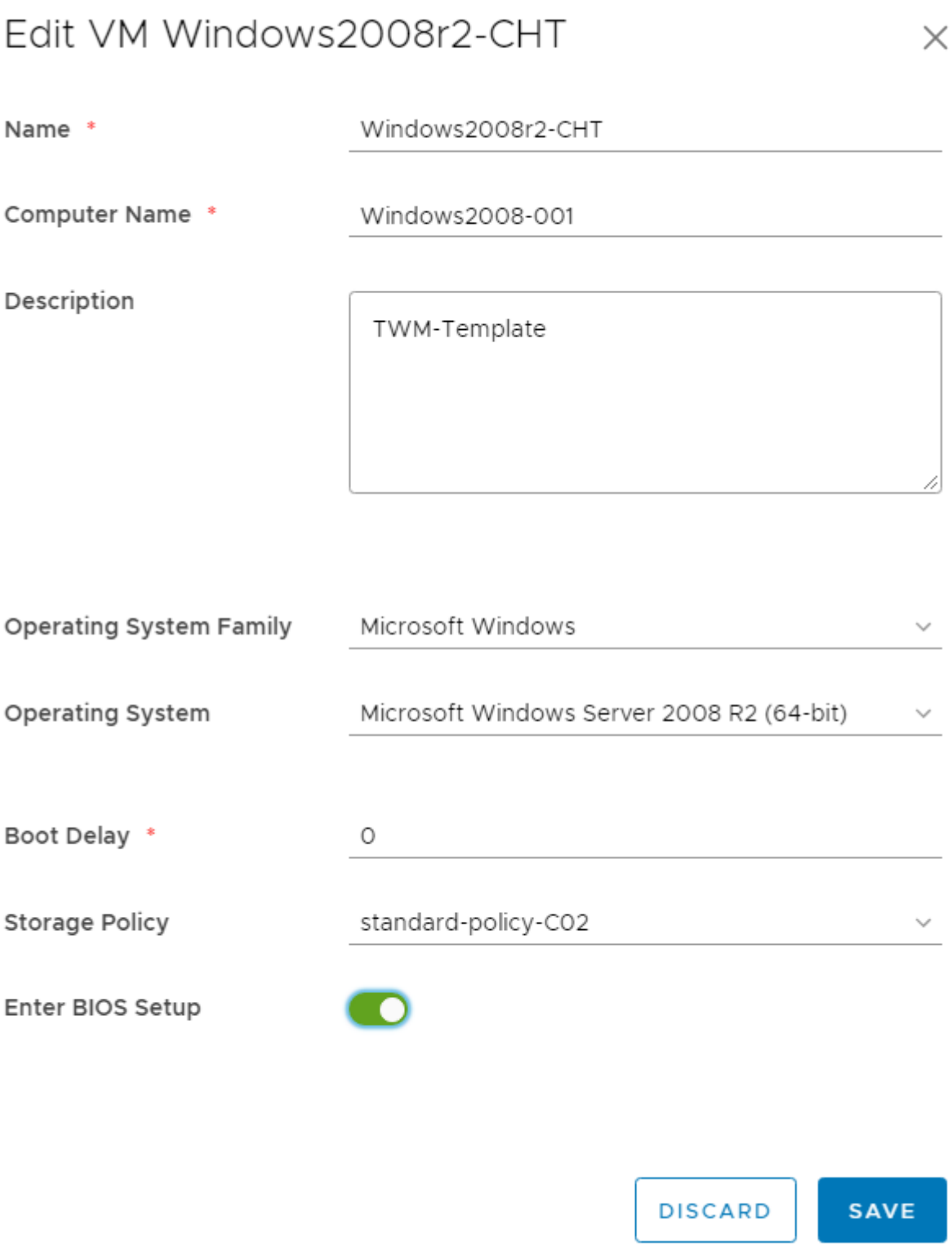
二、 手動變更密碼

1. 設定開機進入 BIOS，使用指定的 ISO 開機

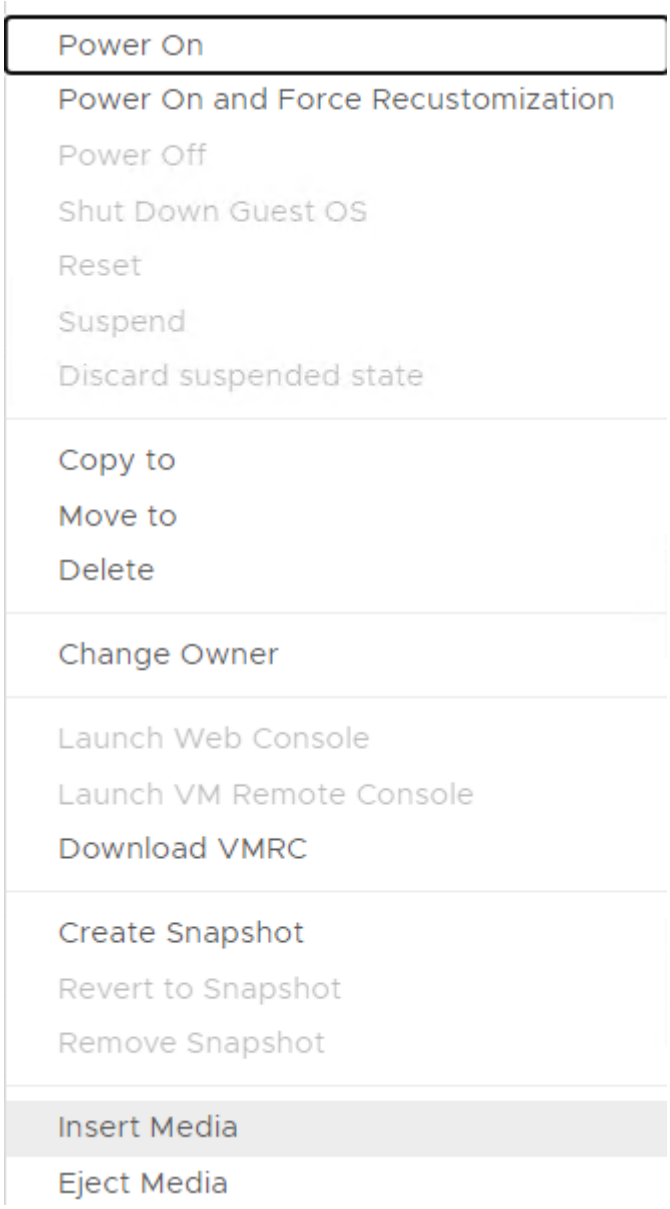
找到 2008r2 vapp 編輯 VM 的一般設定點選 edit



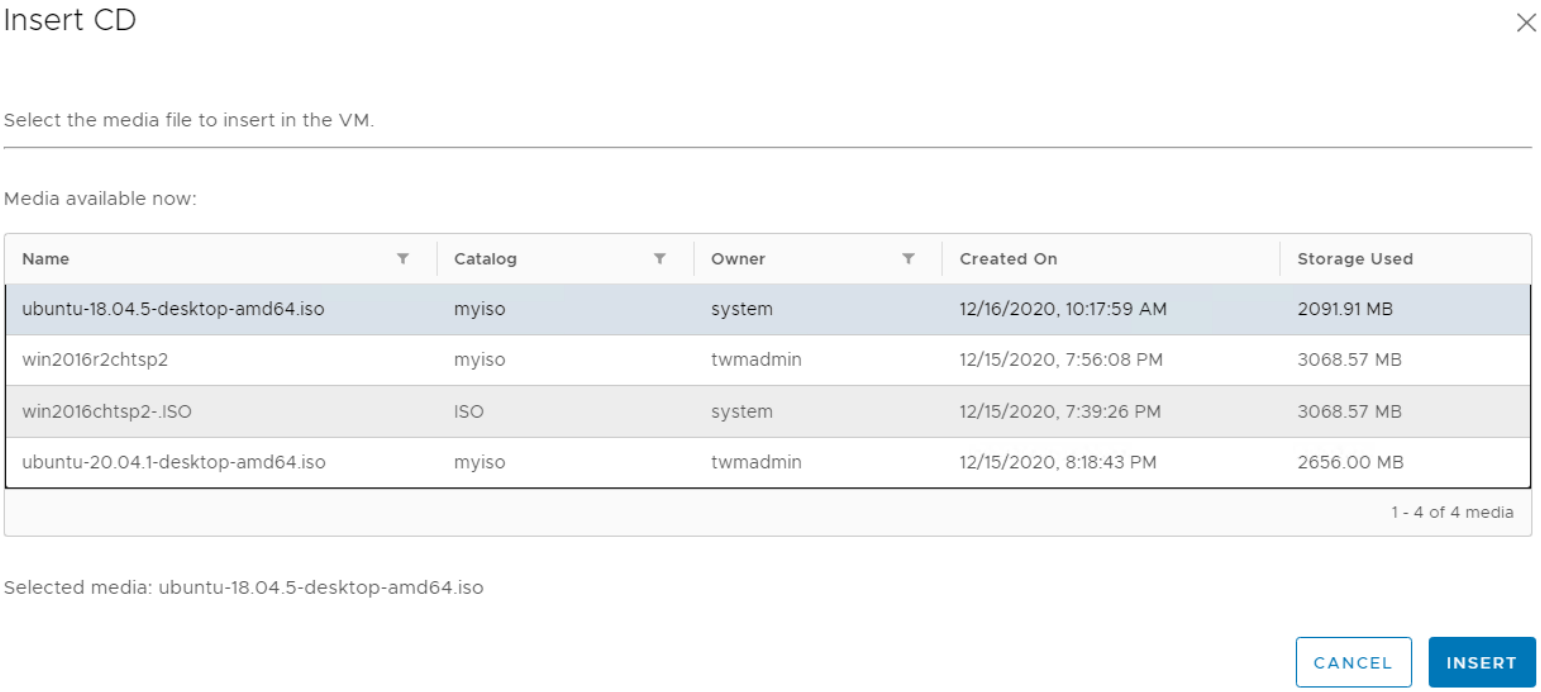
開機進入 BIOS 開關打開



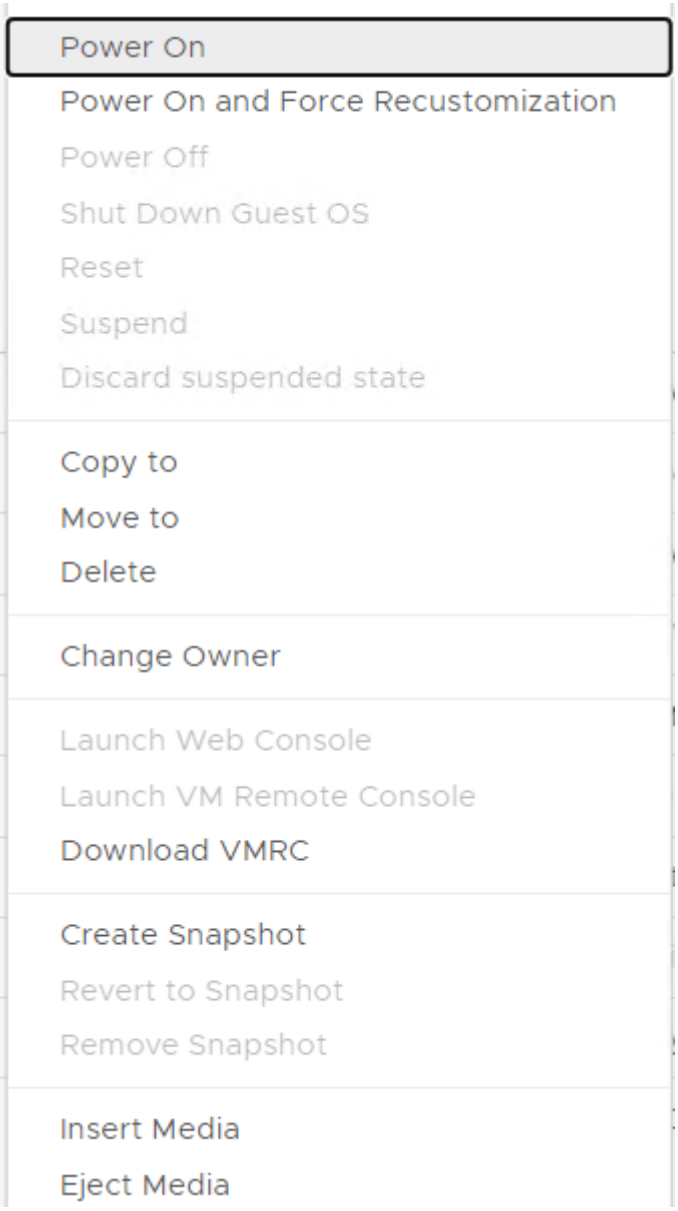
點選 Action 選擇 Insert Media



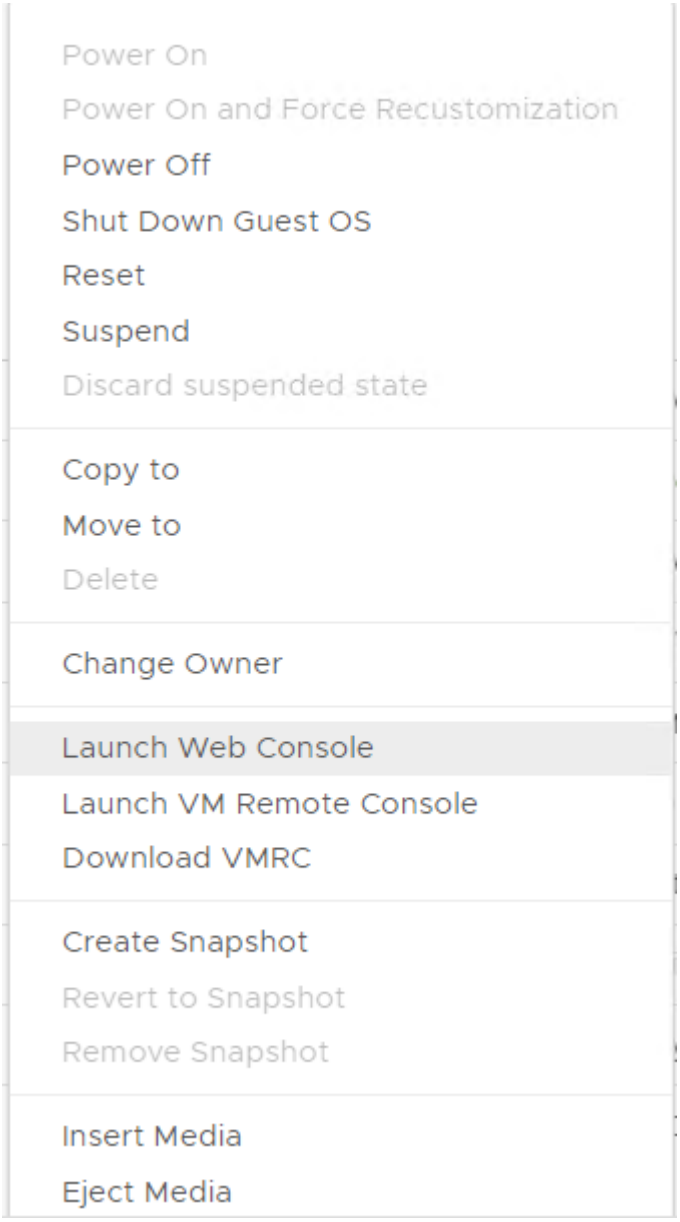
放入 Ubuntu 開機光碟



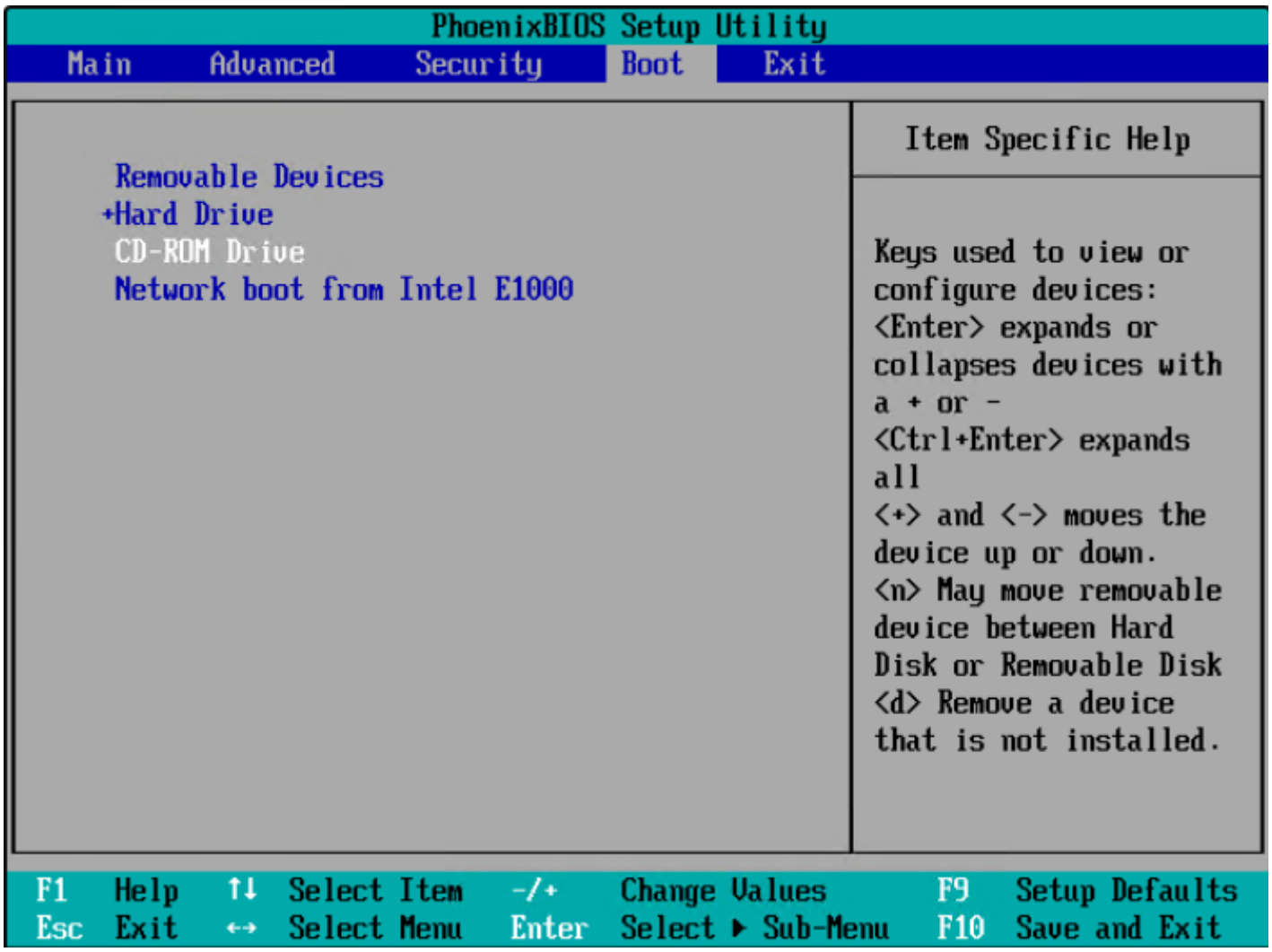
點選 Action 將 VM 開機



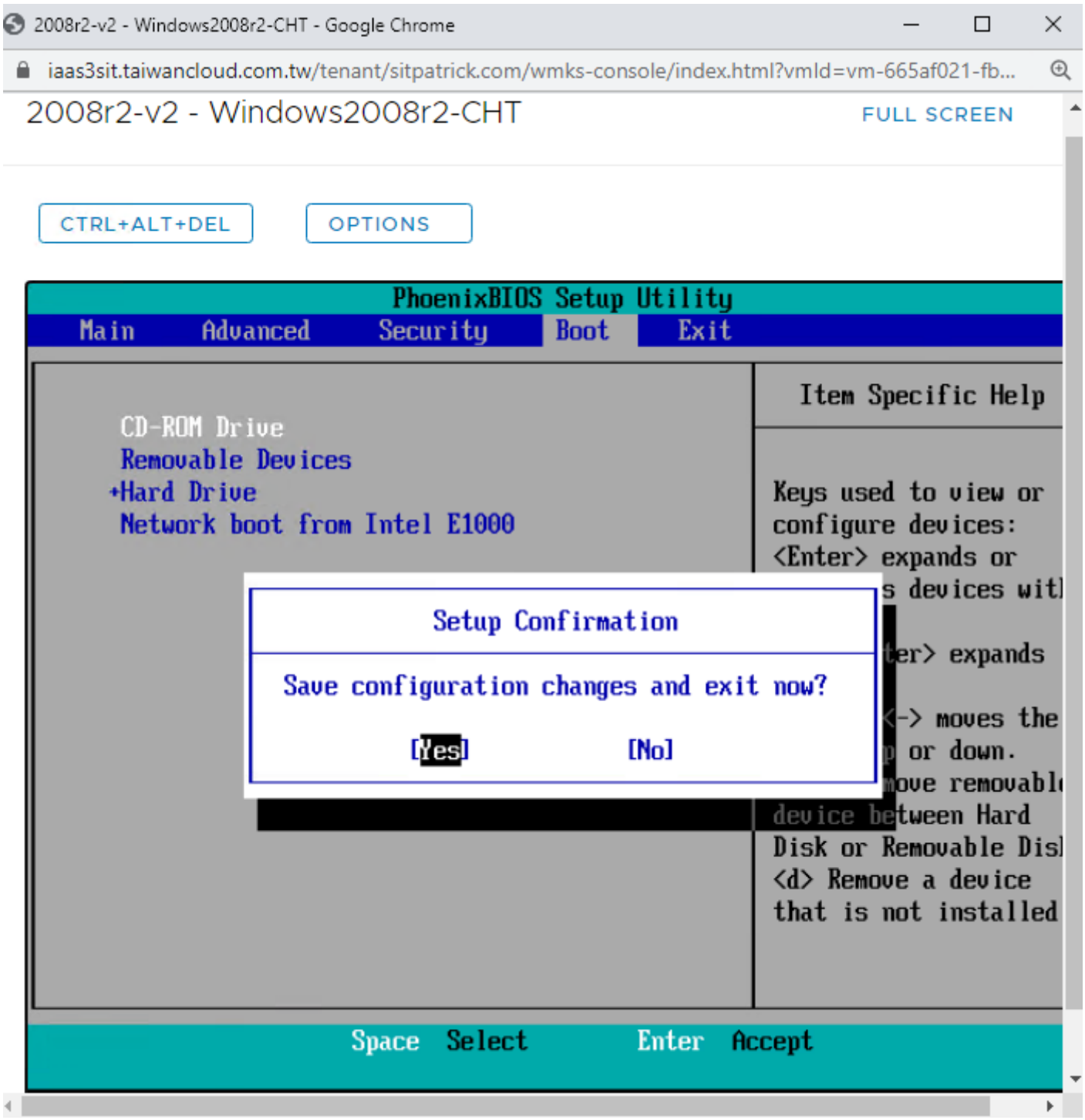
點選 Action 開啟 VM Console



開機後將直接進入 BIOS 選擇 Boot 光棒移動到 CD-ROM Drive 按+ 將順序調整到最優先

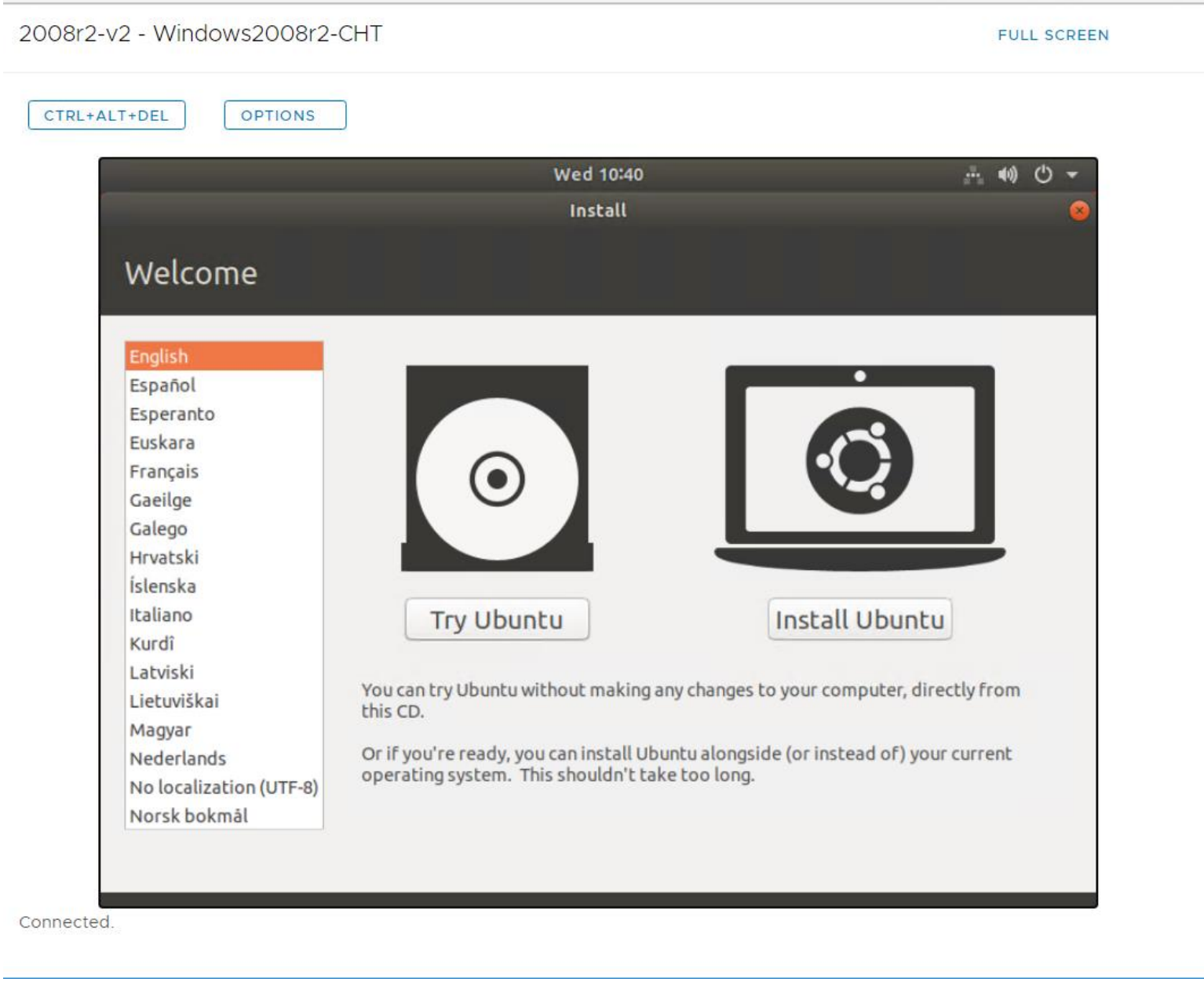


按 F10 存檔離開


2008r2-v2 - Windows2008r2-CHT - Google Chrome
iaas3sit.taiwancloud.com.tw/tenant/sitpatrick.com/wmks-console/index.html?vmId=vm-665af021-fb...
2008r2-v2 - Windows2008r2-CHT
FULL SCREEN
CTRL+ALT+DEL
OPTIONS
PhoenixBIOS Setup Utility
Main Advanced Security Boot Exit
Item Specific Help
CD-ROM Drive
Removable Devices
+Hard Drive
Network boot from Intel E1000
Keys used to view or
configure devices:
<Enter> expands or
Setup Confirmation
Save configuration changes and exit now?
[Yes] [No]
Space Select Enter Accept

2. 使用指定的 ISO 開機，設定 Windows 開機使用 CMD

離開後系統會自動開到 ubuntu 畫面,請等待至桌面出現選擇 Try Ubuntu

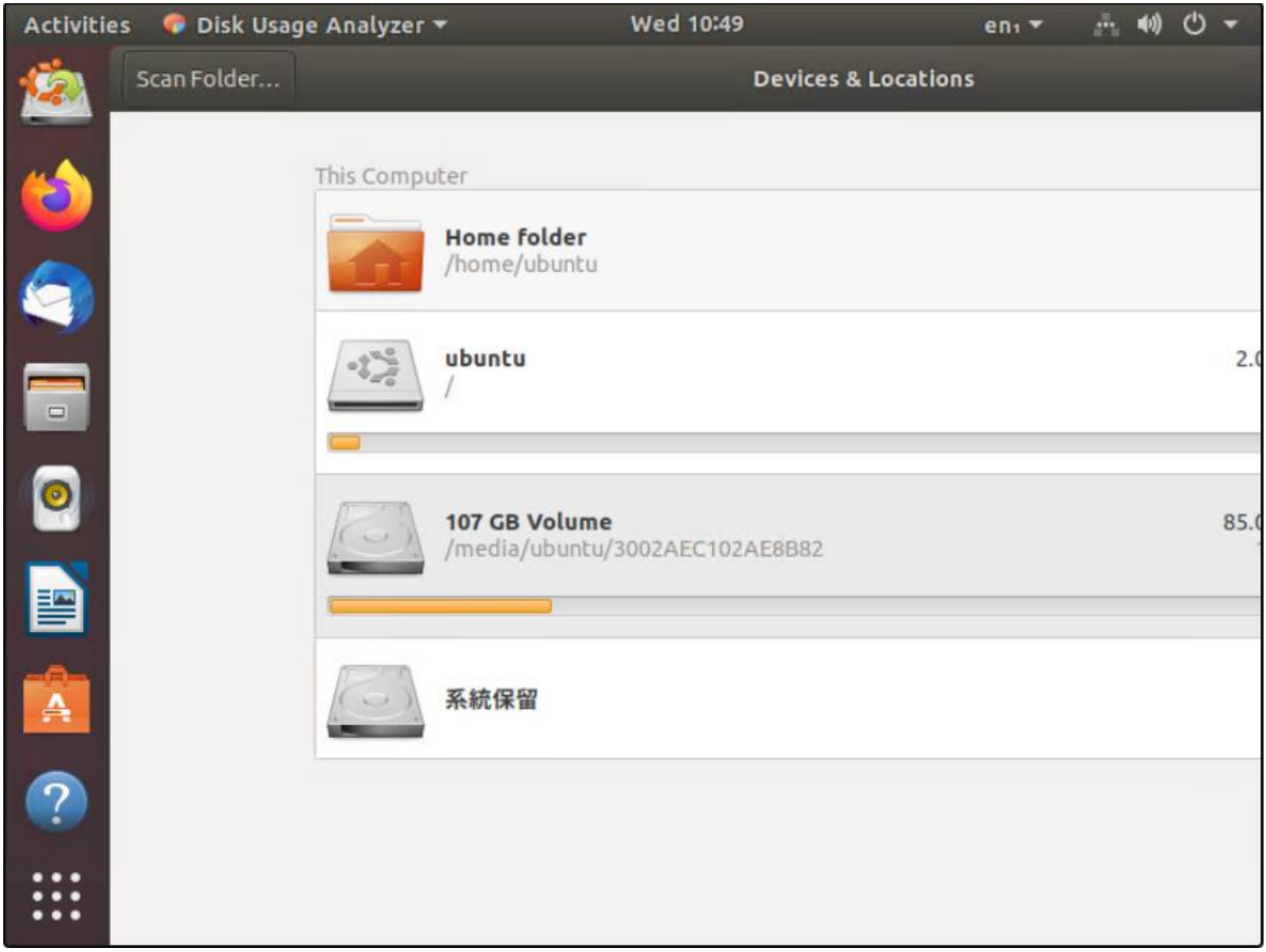


系統將會載入 ubuntu 桌面點選左下角圖示

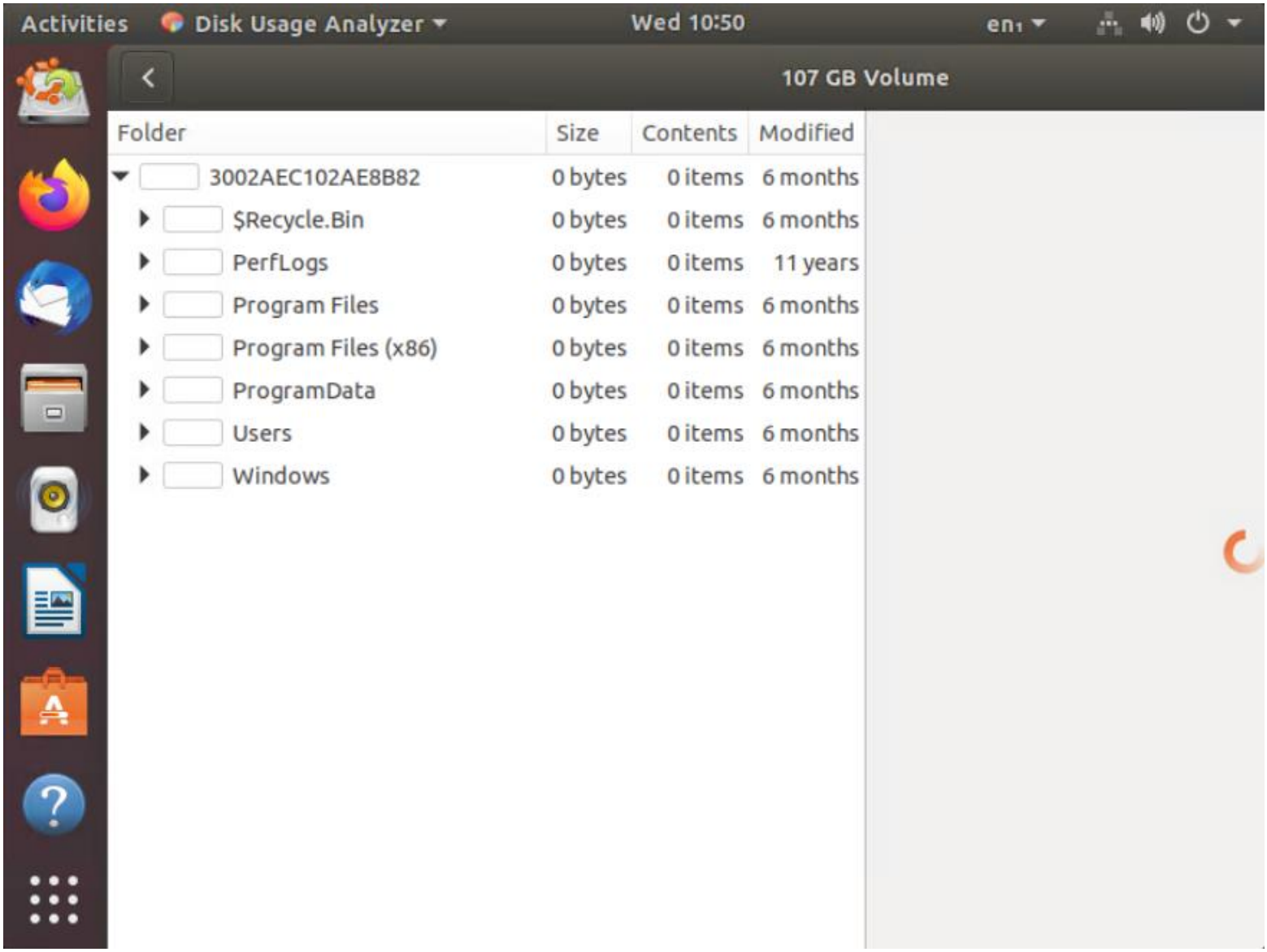
選擇 DISK...


Activities
Wed 10:48
en1
Type to search...
Aisle...
Archi...
Back...
Calcu...
Calen...
Char...
Cheese
Disk ...
Disks
Docu...
Files
Firef...
Fonts
GPar...
Help
Imag...
Input ...
Instal...
Lang...
Libre...
Libre...
Libre...
Libre...
Livep...
Frequent
All

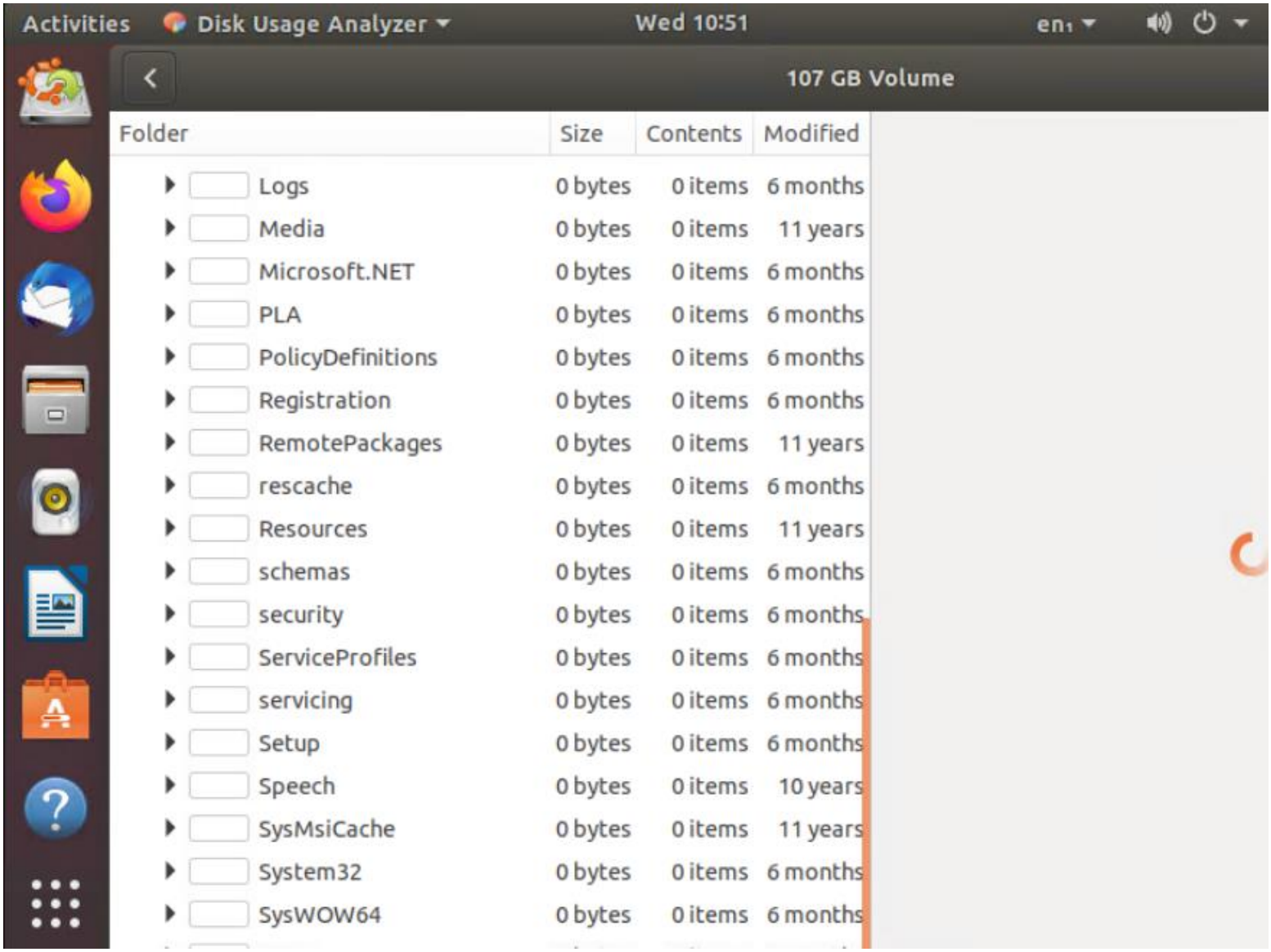
選擇大小約 100G 的磁碟



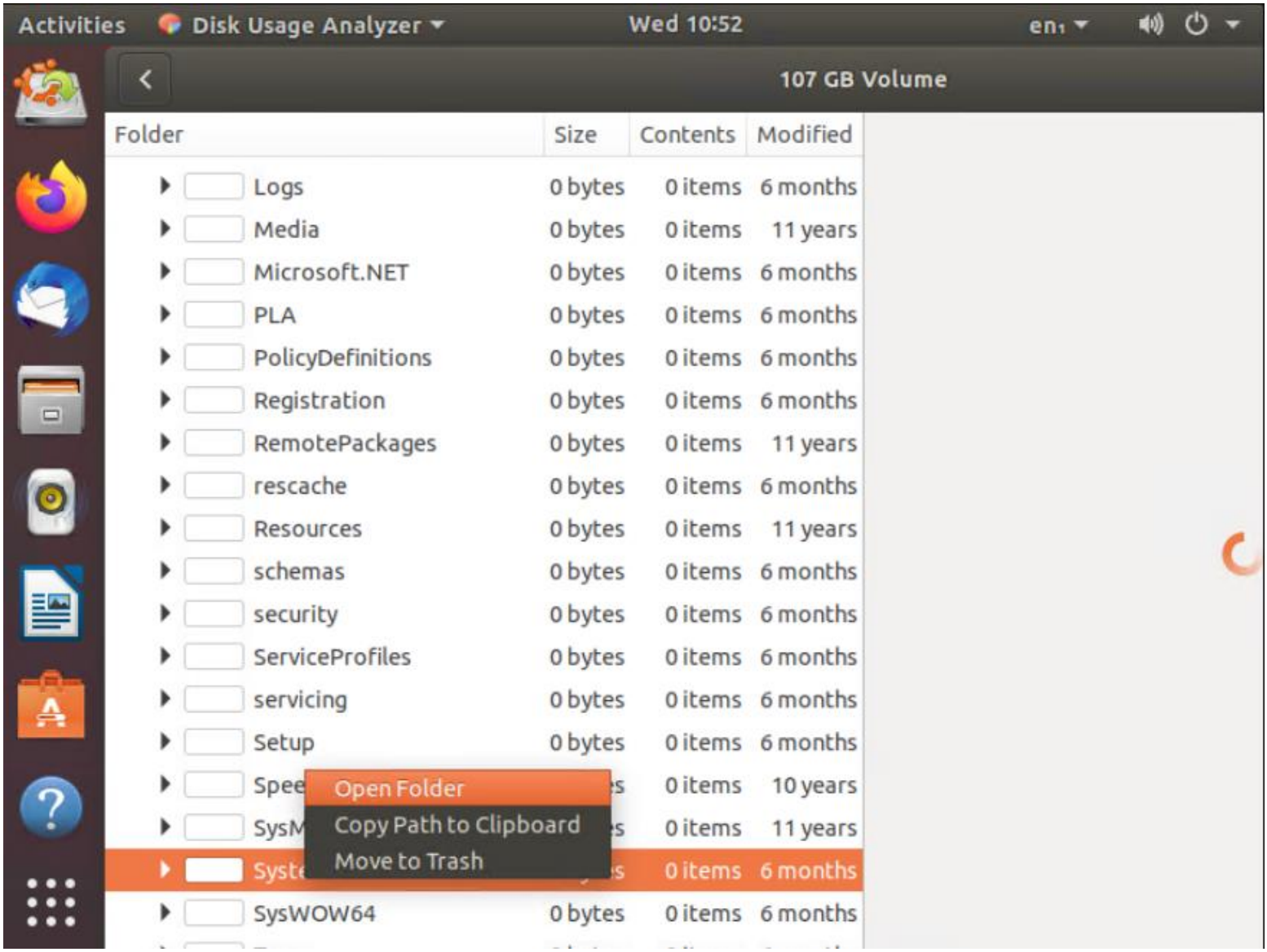
選擇 Windows


Activities
Disk Usage Analyzer
Wed 10:50
en1
107 GB Volume
Folder
Size
Contents
Modified
3002AEC102AE8B82 0 bytes 0 items 6 months
$Recycle.Bin 0 bytes 0 items 6 months
PerfLogs 0 bytes 0 items 11 years
Program Files 0 bytes 0 items 6 months
Program Files (x86) 0 bytes 0 items 6 months
ProgramData 0 bytes 0 items 6 months
Users 0 bytes 0 items 6 months
Windows 0 bytes 0 items 6 months

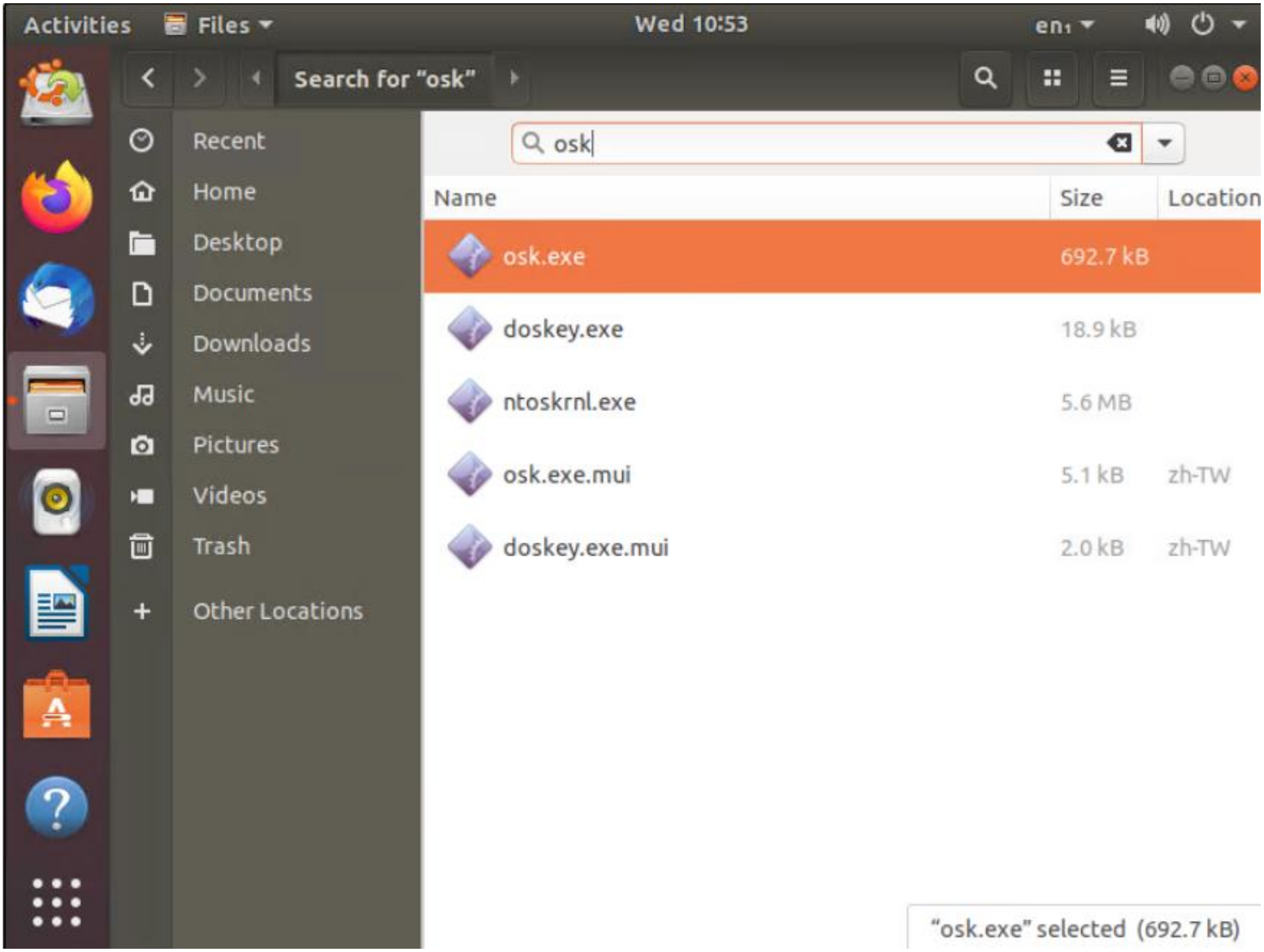
往下找到 system32



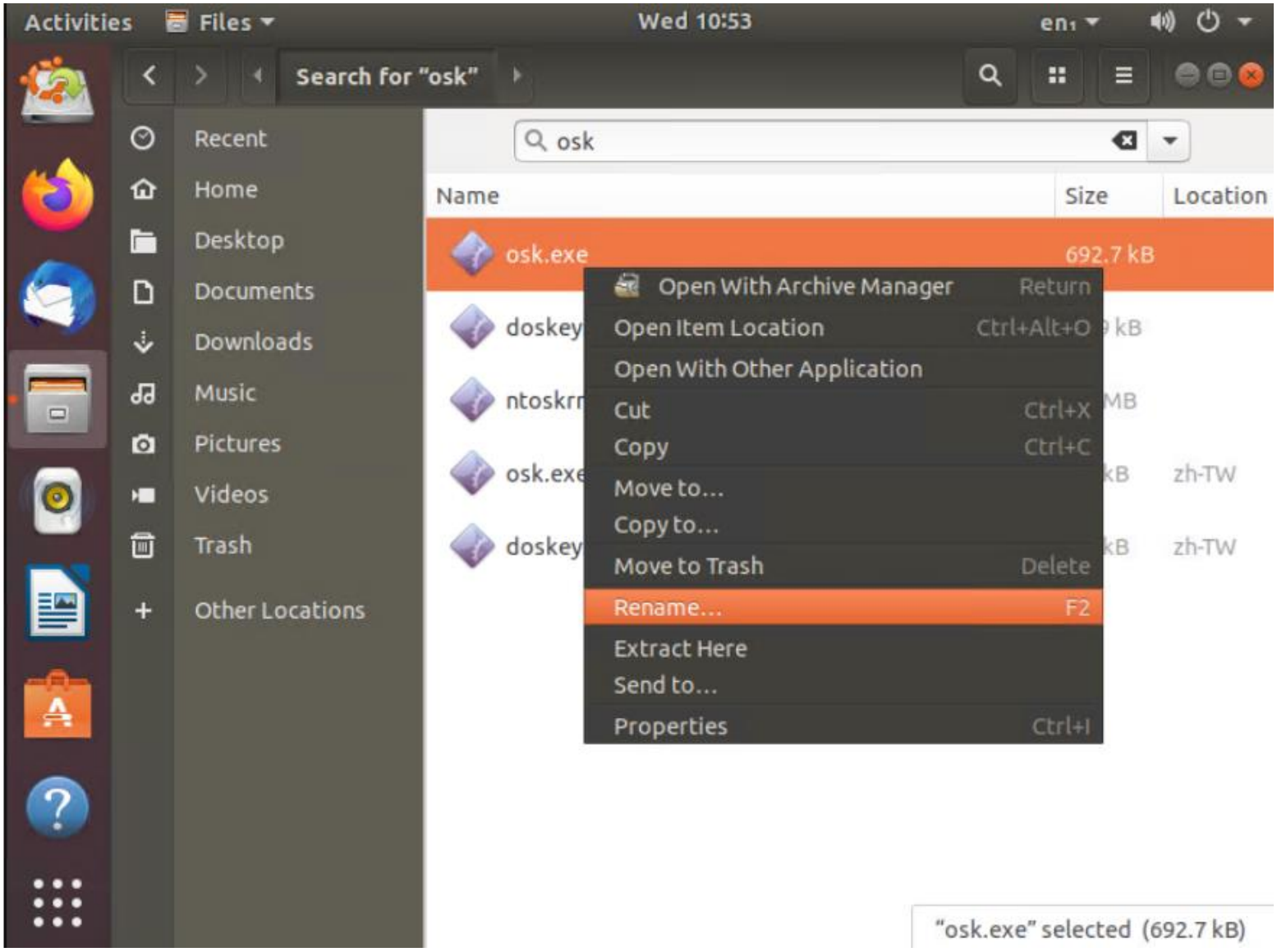
按右鍵選擇 Open Folder

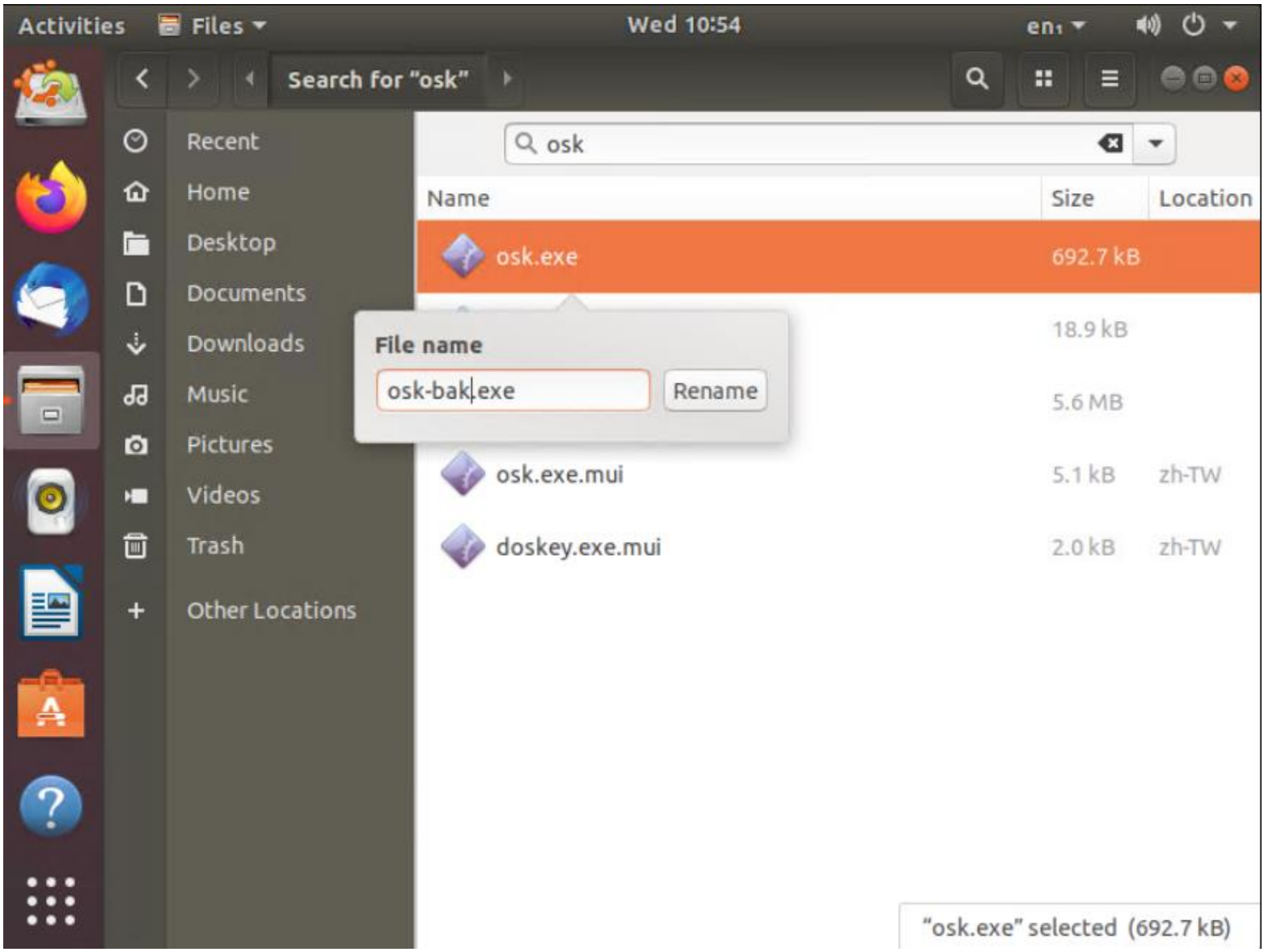


點選右邊搜尋圖示 輸入 osk

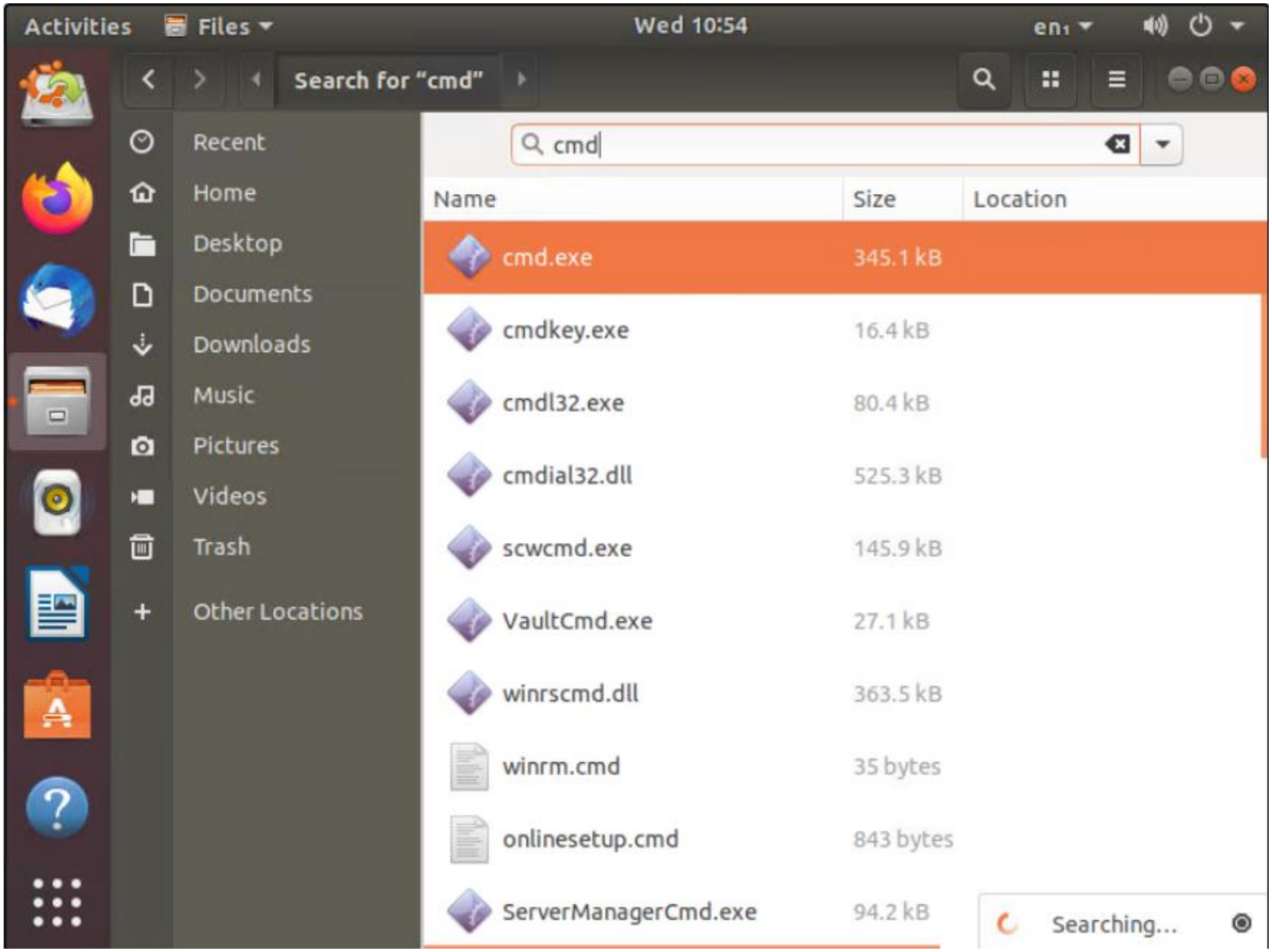


找到 osk.exe 按右鍵選擇 Rename

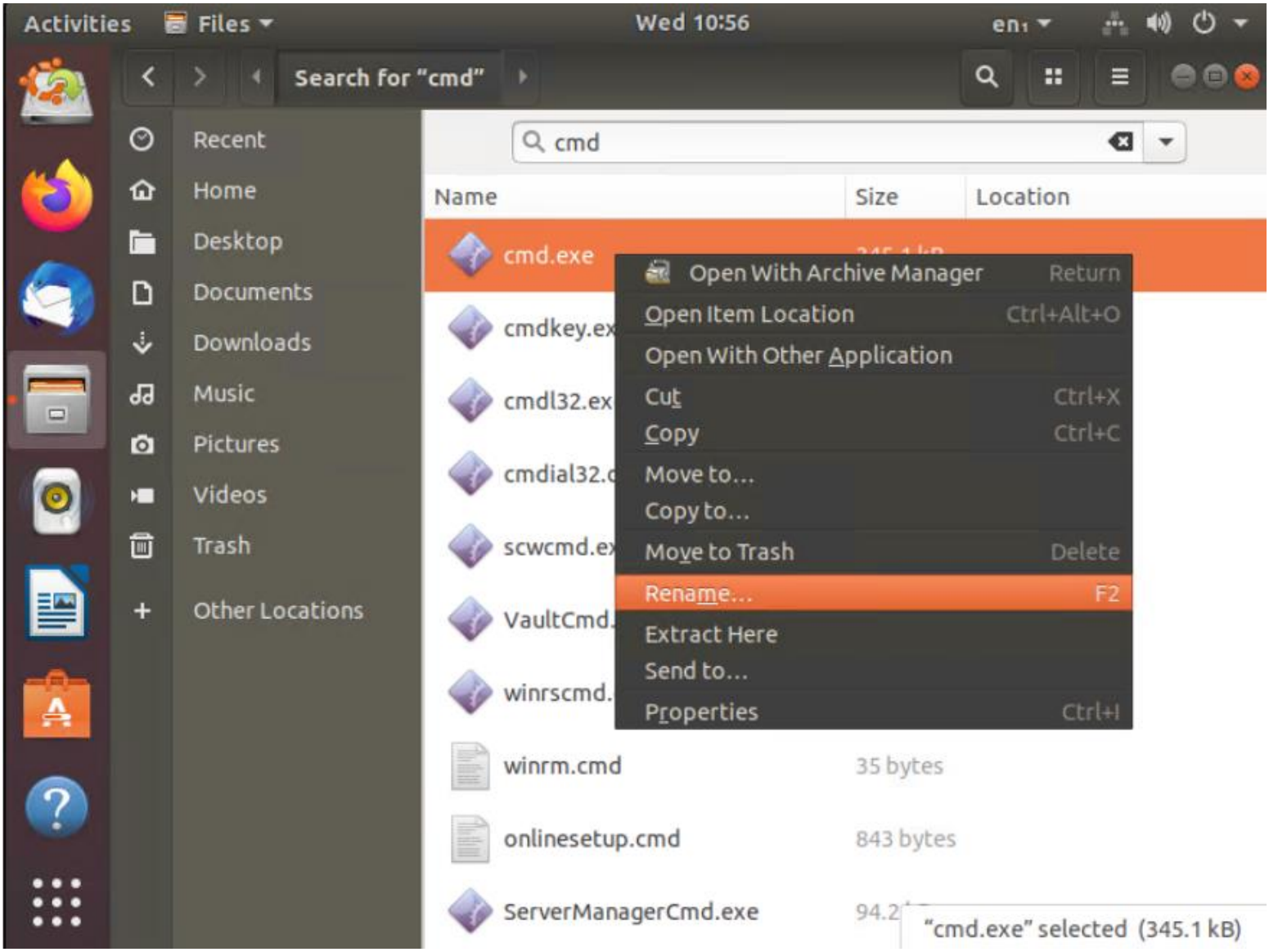


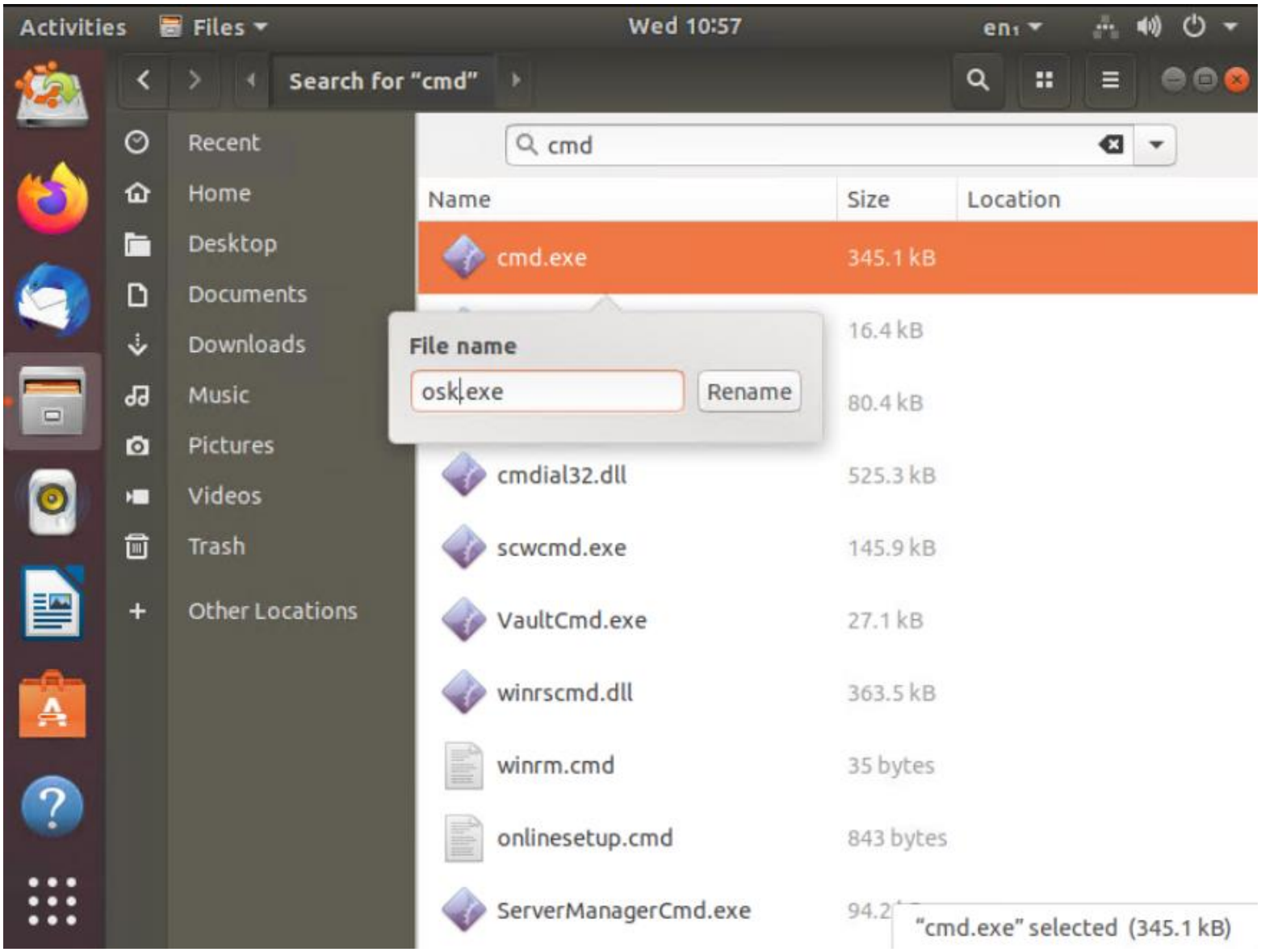

Activities
Files
Wed 10:54
en
Search for "osk"
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
osk
Name
Size
Location
osk.exe
692.7 kB
18.9 kB
5.6 MB
File name
osk-bak.exe
Rename
osk.exe.mui
5.1 kB
zh-TW
doskey.exe.mui
2.0 kB
zh-TW
"osk.exe" selected (692.7 kB)

再搜尋 cmd

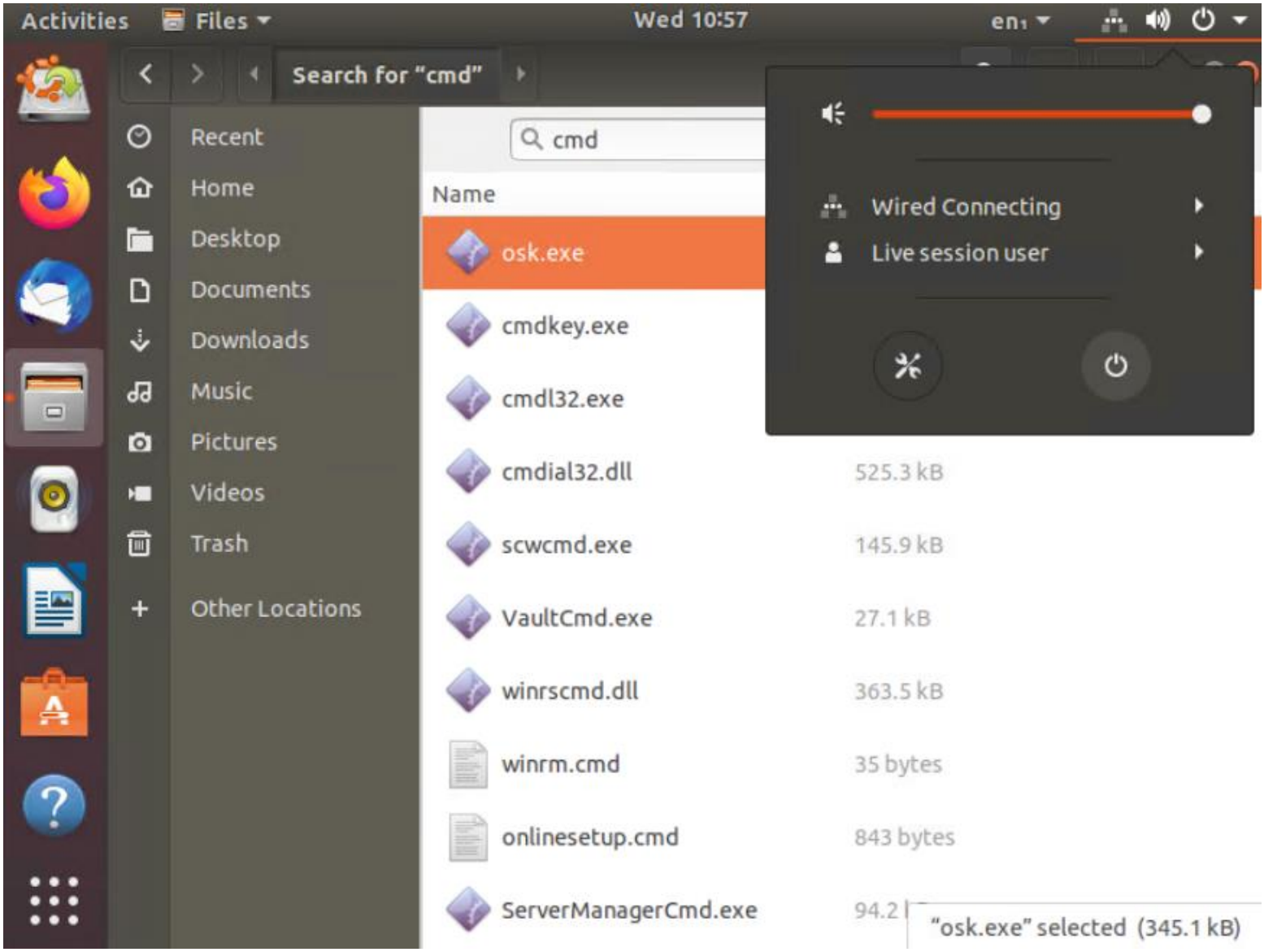

Activities
Files
Wed 10:54
en1
Search for "cmd"
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
cmd
Name
Size
Location
cmd.exe
345.1 kB
cmdkey.exe
16.4 kB
cmdl32.exe
80.4 kB
cmdial32.dll
525.3 kB
scwcmd.exe
145.9 kB
VaultCmd.exe
27.1 kB
winrscmd.dll
363.5 kB
winrm.cmd
35 bytes
onlinesetup.cmd
843 bytes
ServerManagerCmd.exe
94.2 kB
Searching...

將 cmd.exe 按右鍵將檔名改為 osk.exe

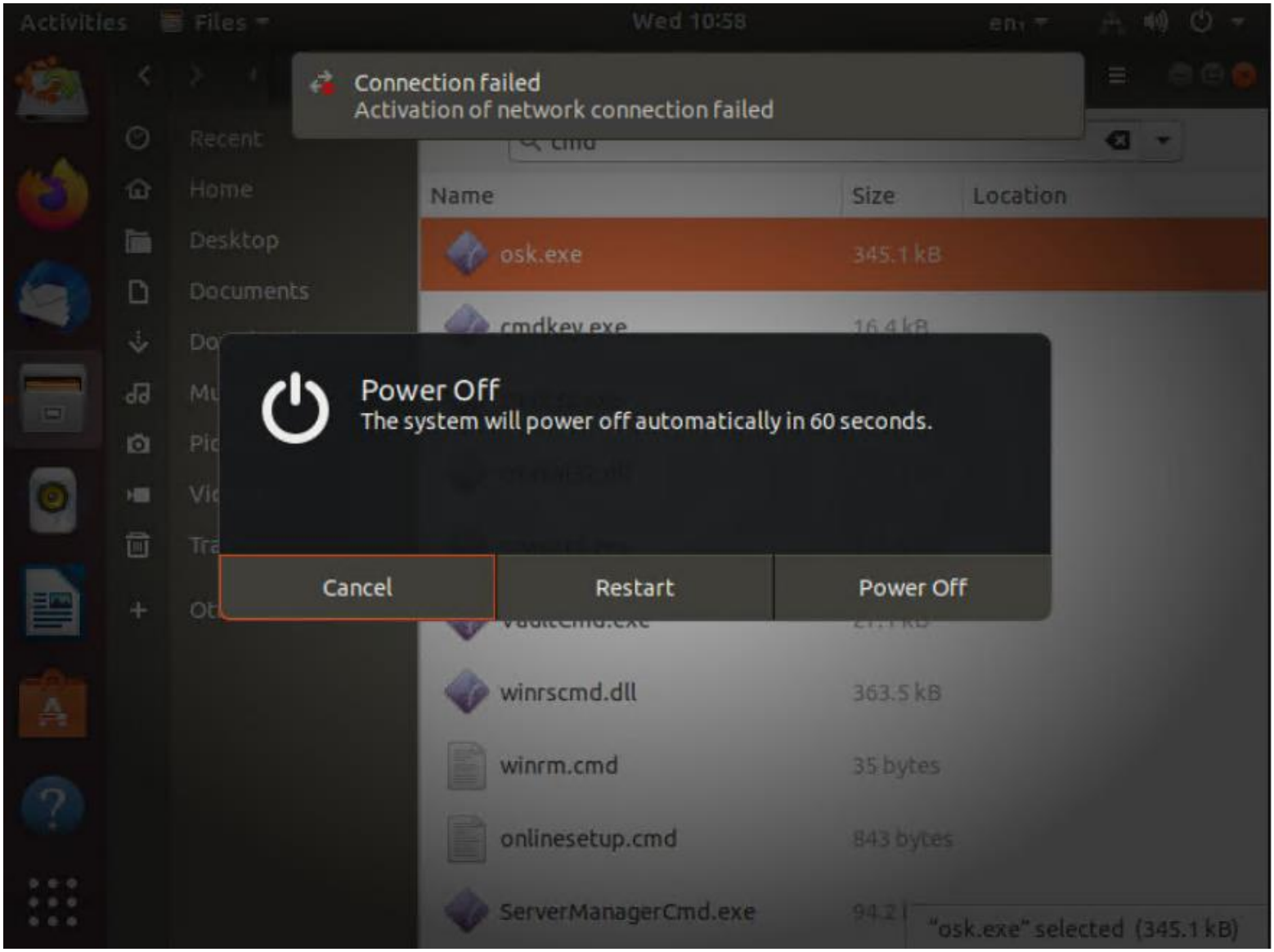



Activities
Files
Wed 10:57
en1
Search for "cmd"
cmd
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
Name
Size
Location
cmd.exe
345.1 kB
File name
osk.exe
Rename
16.4 kB
80.4 kB
cmdial32.dll
525.3 kB
scwcmd.exe
145.9 kB
VaultCmd.exe
27.1 kB
winrscmd.dll
363.5 kB
winrm.cmd
35 bytes
onlinesetup.cmd
843 bytes
ServerManagerCmd.exe
"cmd.exe" selected (345.1 kB)

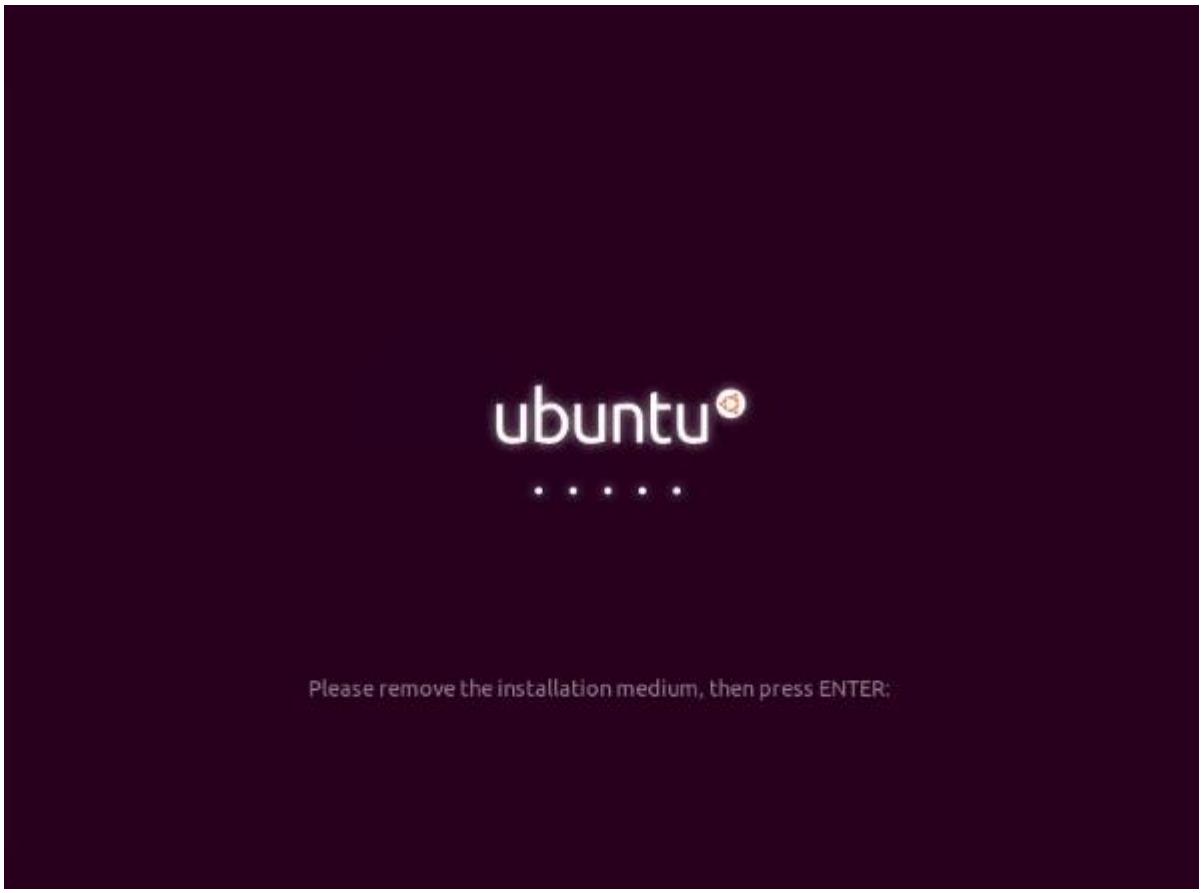
改好後準備重新開機點選右上角電源選項



選擇 restart 重開機



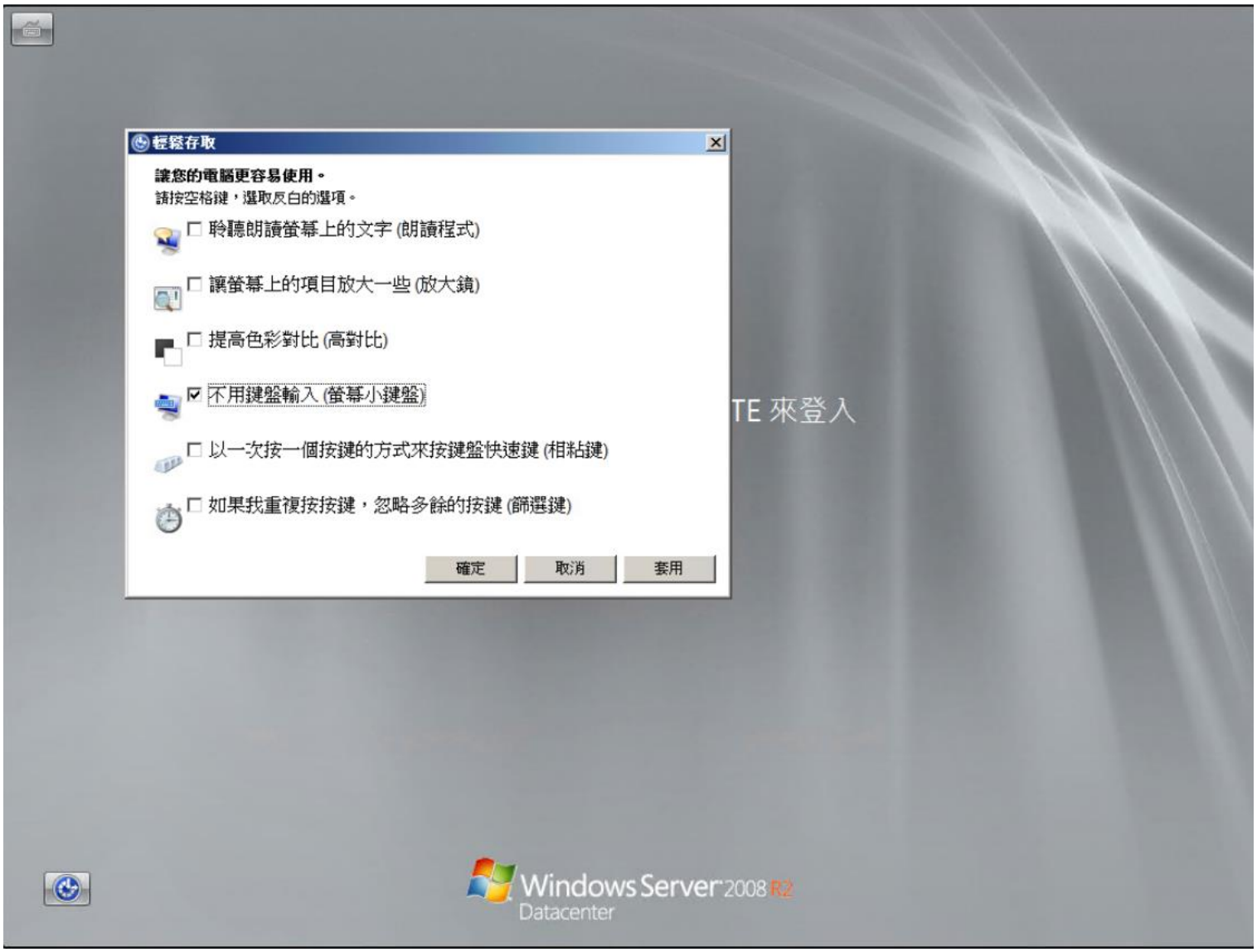
重開機後會到以下畫面，按 ENTER



3. Windows 重設密碼作業

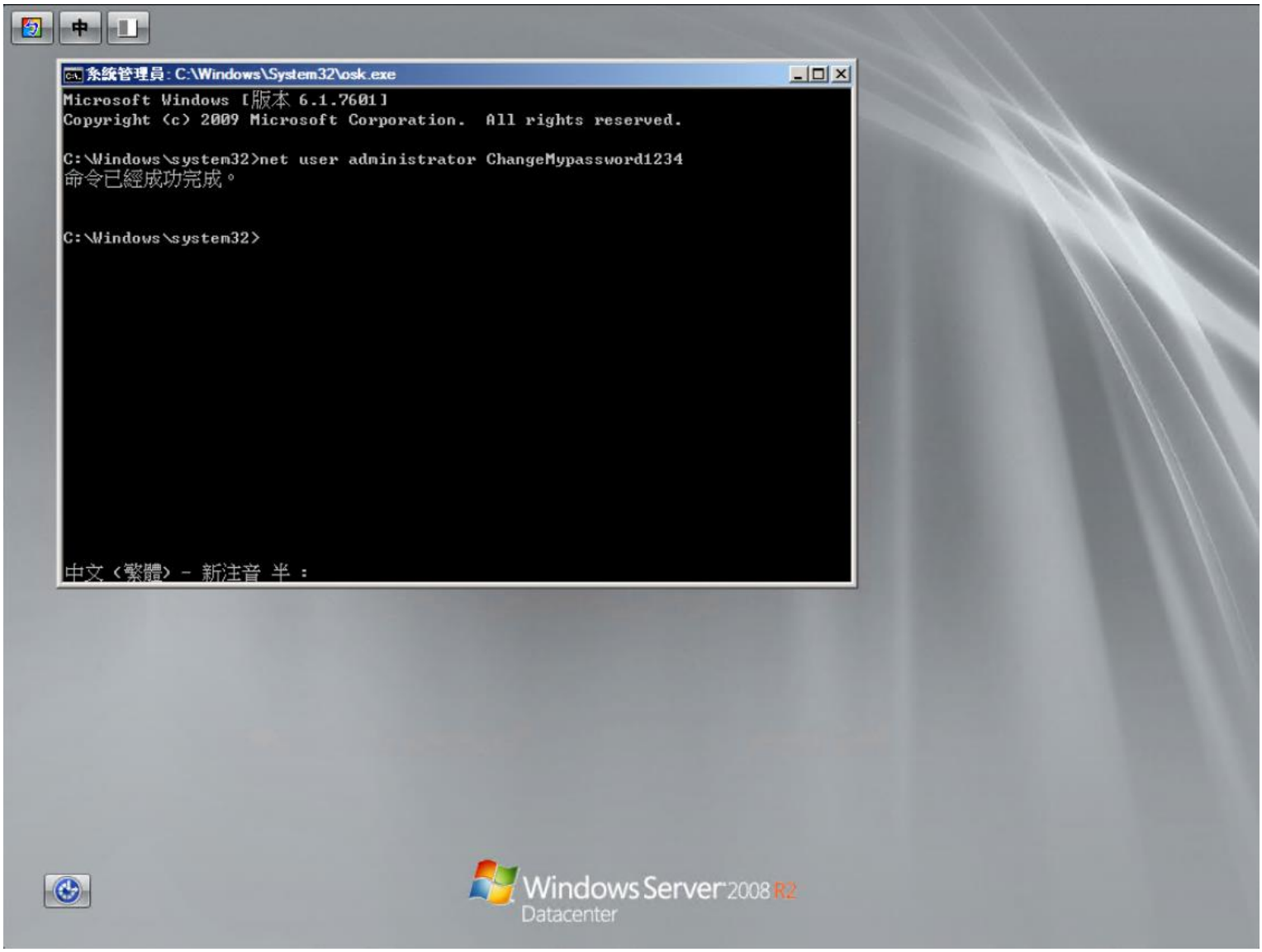
重開機後系統會進入原 Windows 系統

點選左下角輕鬆存取,勾選不用鍵盤輸入(螢幕小鍵盤),點選確定



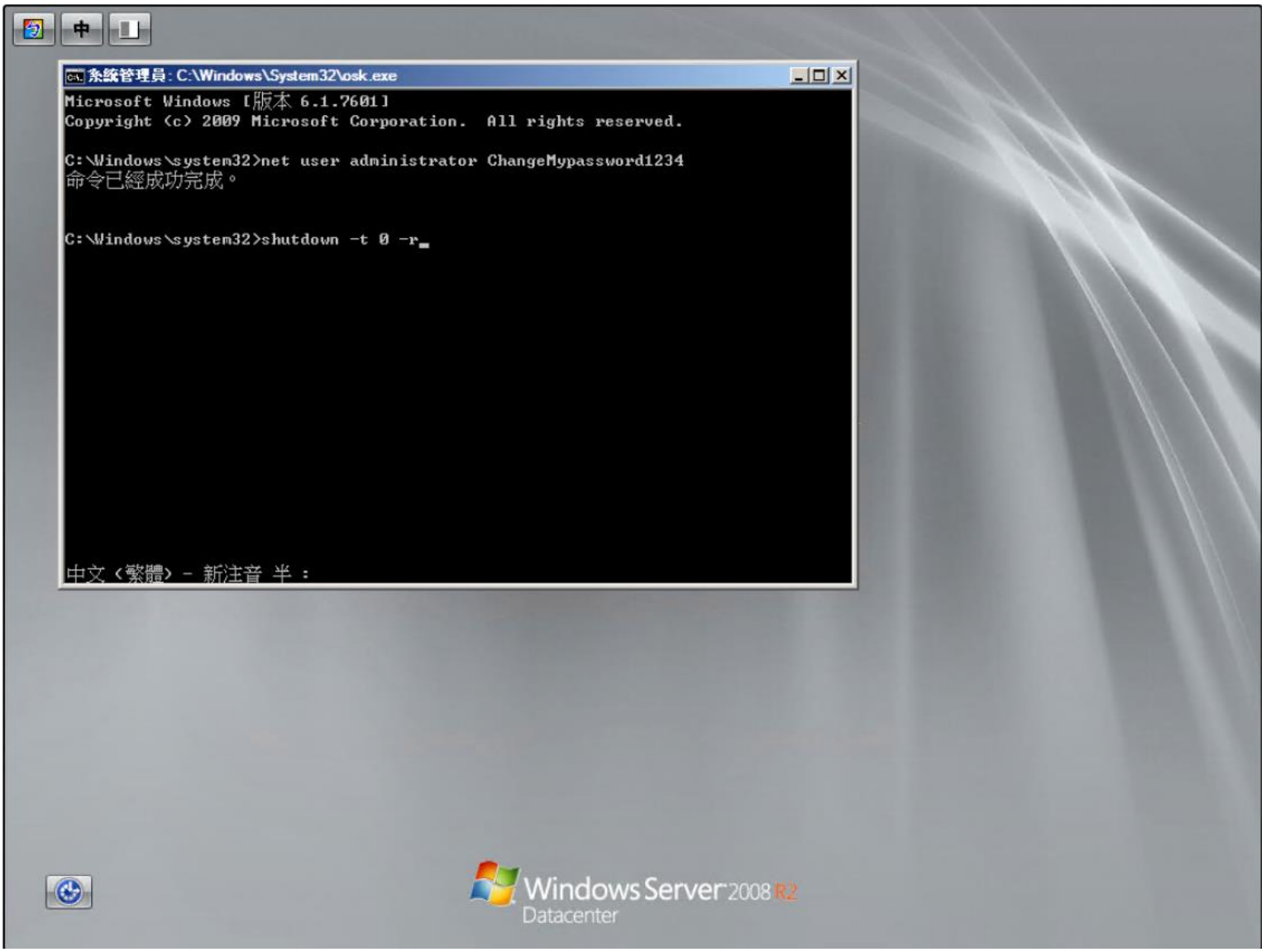
系統會出現命令提示元 請輸入以下格式修改密碼

net user 使用者名稱 密碼

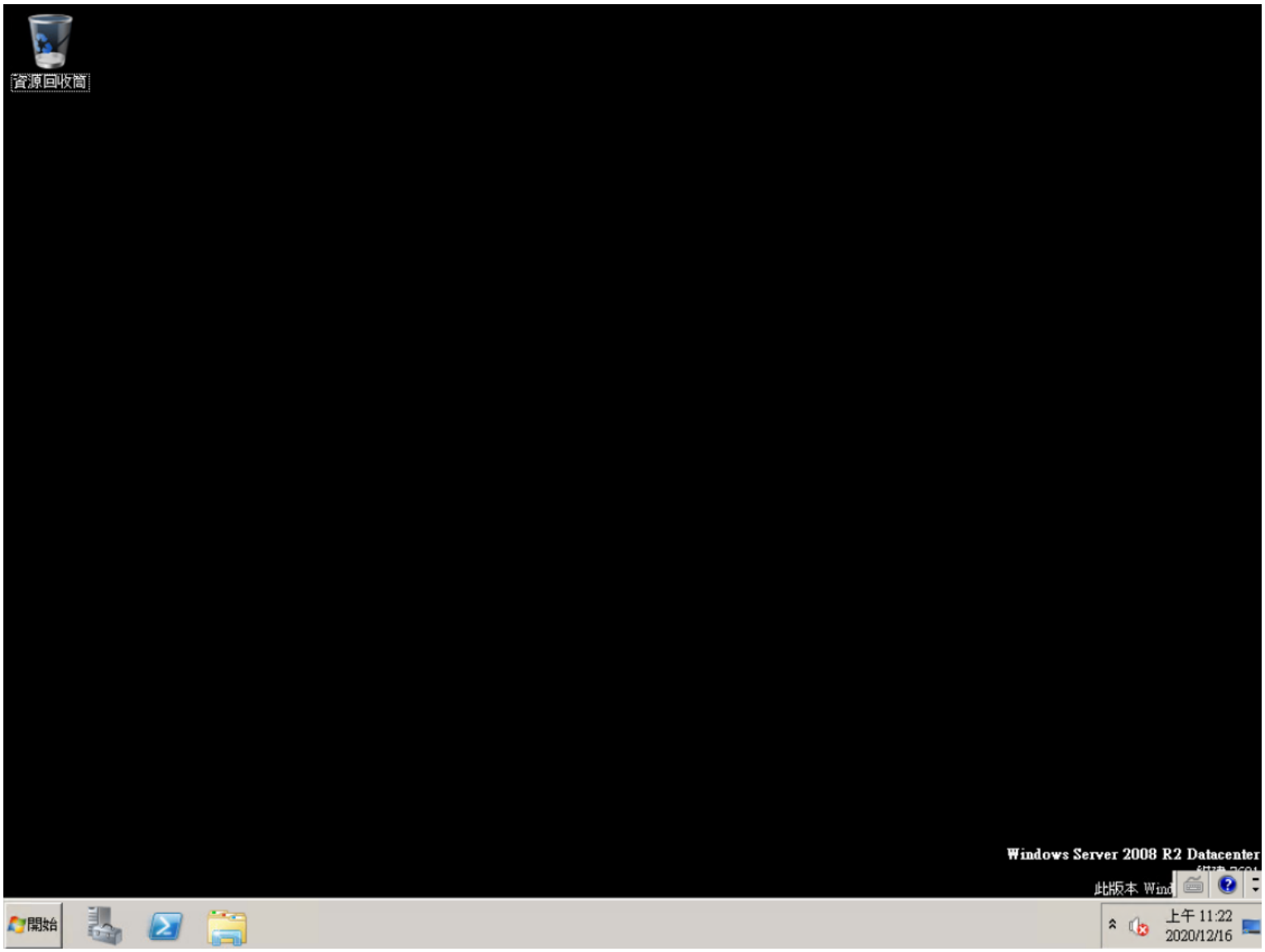


輸入以下指令重新開機

shutdown -t 0 -r



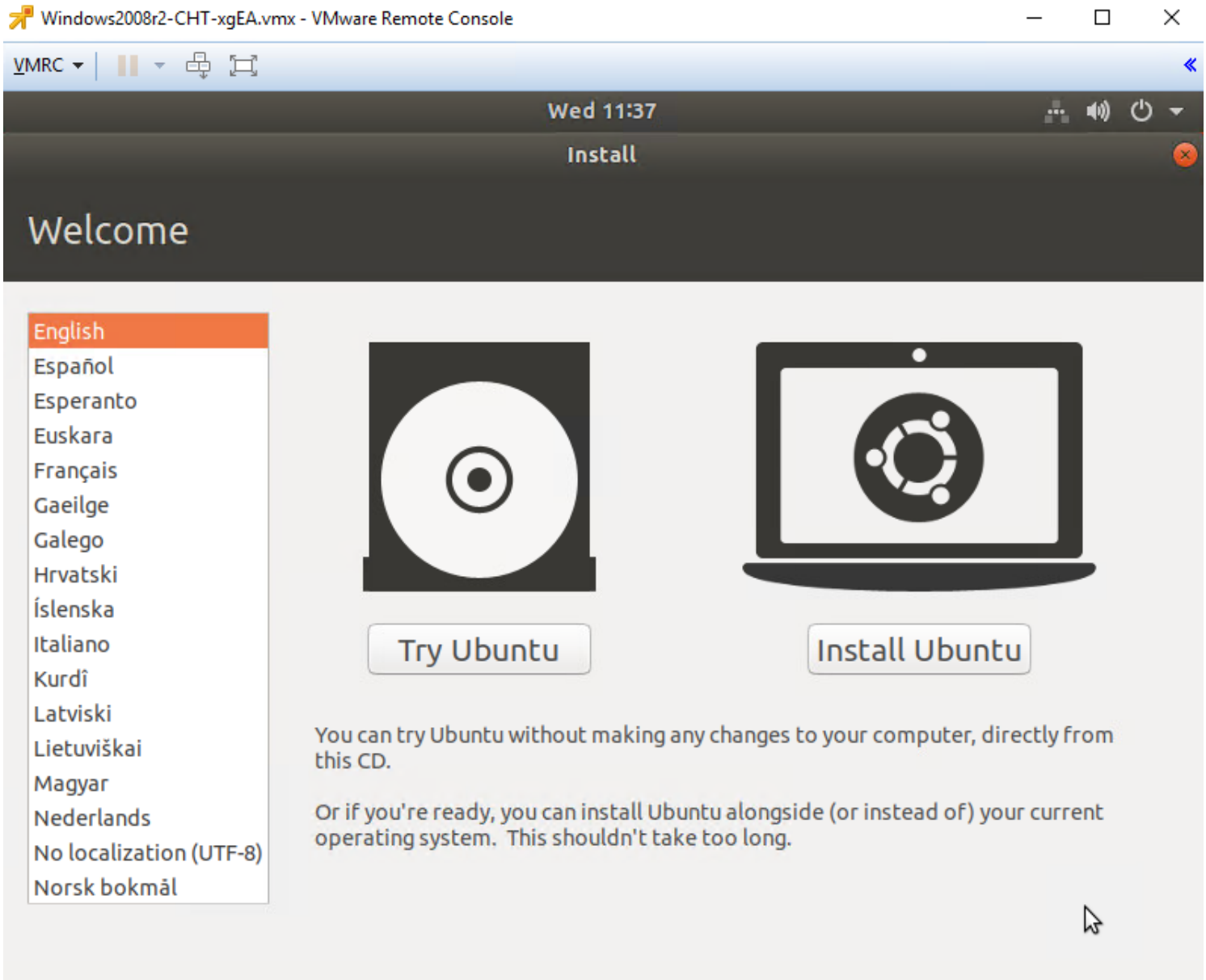
開機後以新的密碼登入


資源回收筒
Windows Server 2008 R2 Datacenter
開始
上午 11:22
2020/12/16

4. 復原先前的變更作業

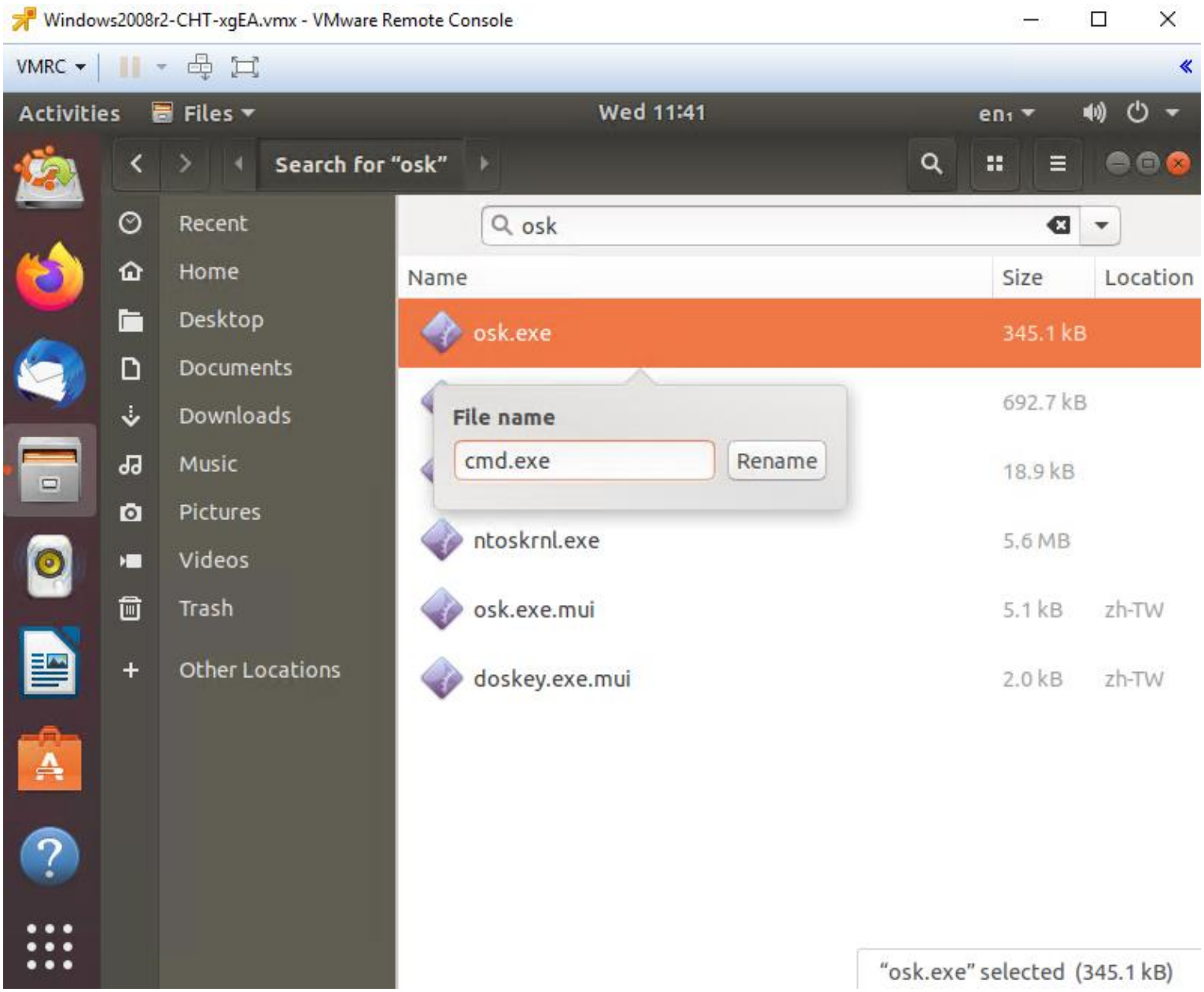
請使用 Portal 將 VM 關機,再次開機系統將會進入 ubuntu

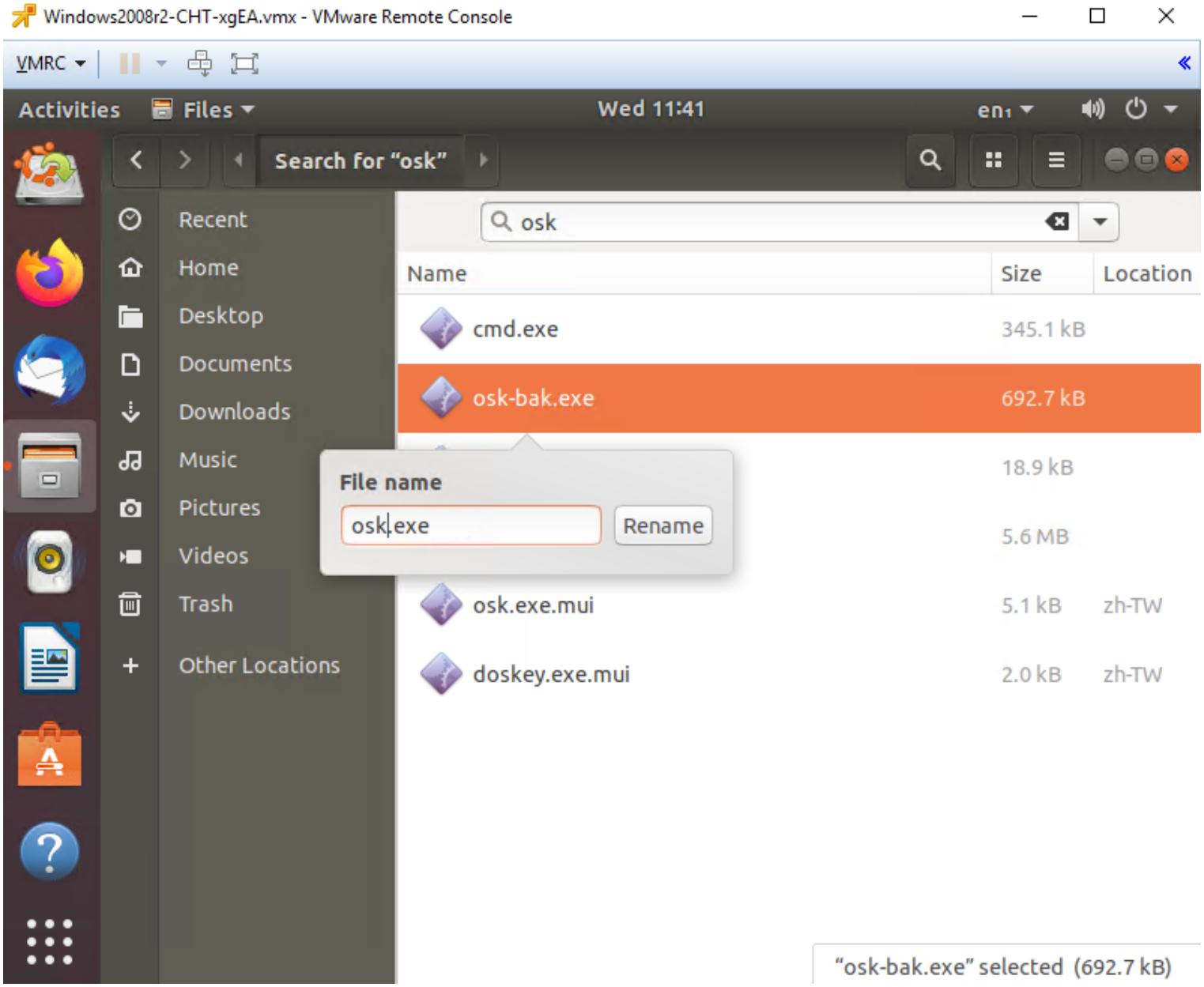
選擇 Try Ubuntu



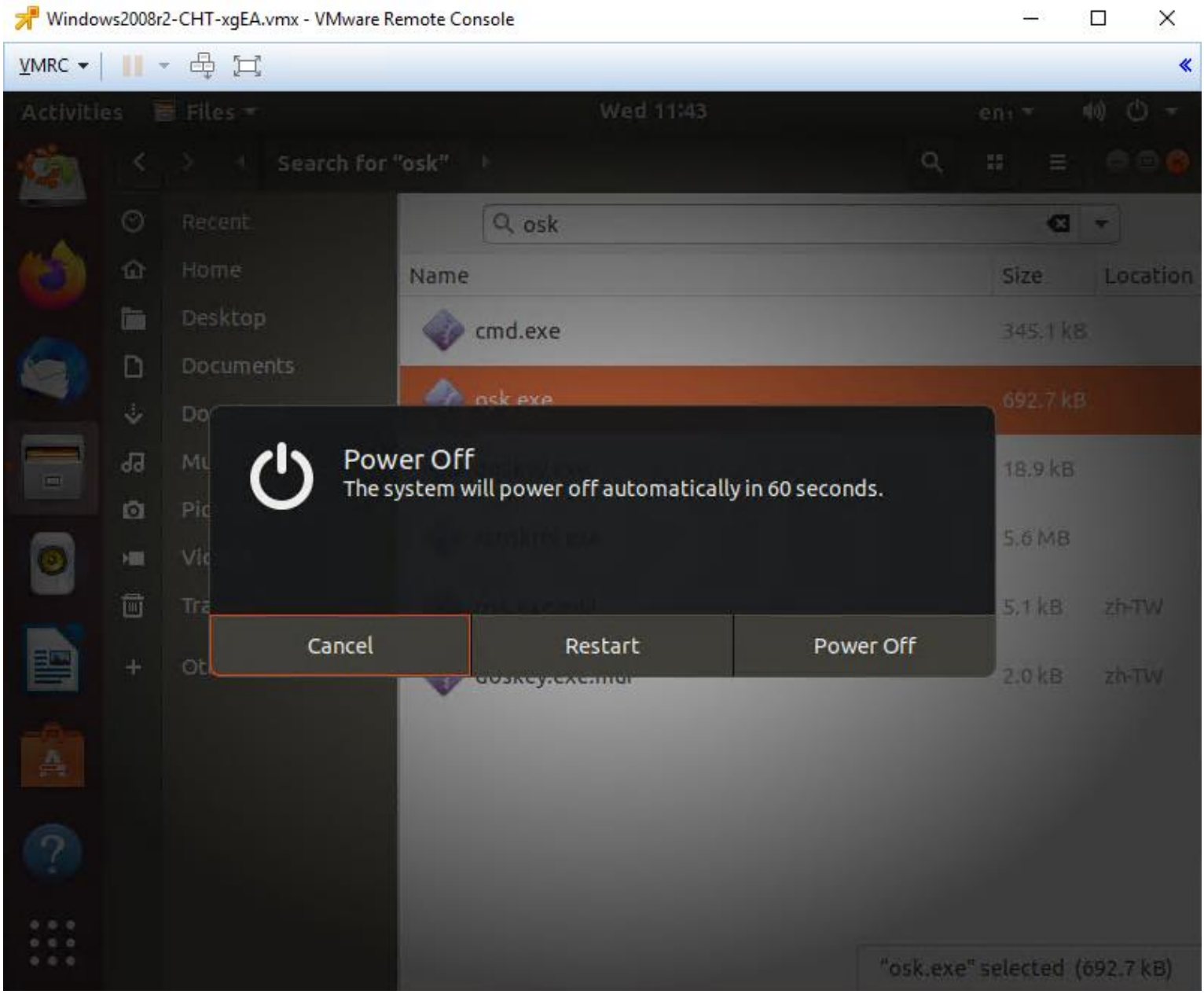
依循步驟 2 再次進入 Windows\system32 目錄將 osk.exe 變更回 cmd.exe

並將 osk-bak.exe 變更回 osk.exe

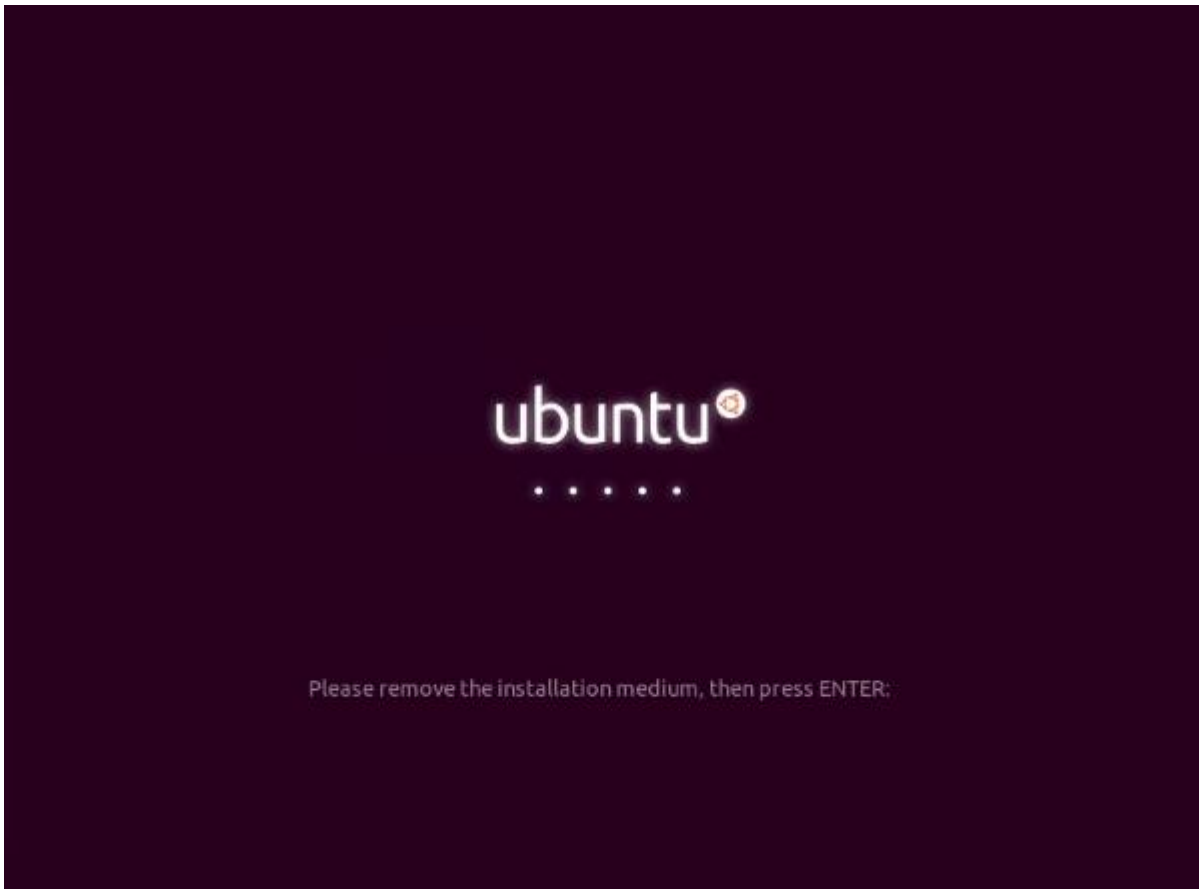



Windows2008r2-CHT-xgEA.vmx - VMware Remote Console
VMRC
Activities
Files
Wed 11:41
en1
Search for "osk"
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
osk
Name
Size
Location
cmd.exe
345.1 kB
osk-bak.exe
692.7 kB
18.9 kB
5.6 MB
osk.exe.mui
5.1 kB
zh-TW
doskey.exe.mui
2.0 kB
zh-TW
File name
osk.exe
Rename
"osk-bak.exe" selected (692.7 kB)

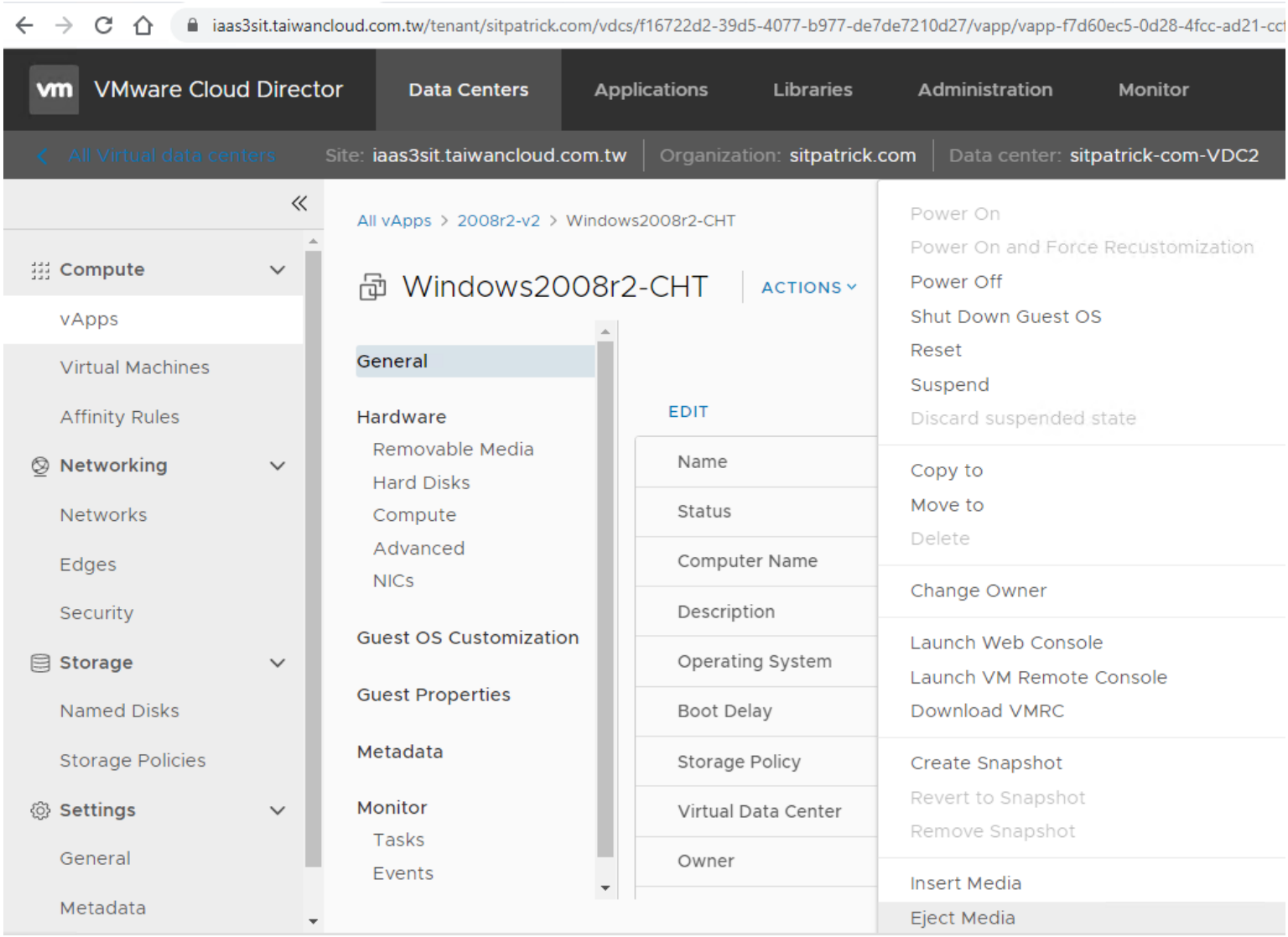
將 VM 關機


Windows2008r2-CHT-xgEA.vmx - VMware Remote Console
VMRC
Activities
Files
Wed 11:43
Search for "osk"
Recent
Home
Desktop
Documents
osk
Name
Size
Location
cmd.exe
345.1 kB
692.7 kB
18.9 kB
5.6 MB
5.1 kB
zh-TW
2.0 kB
zh-TW
Power Off
The system will power off automatically in 60 seconds.
Cancel
Restart
Power Off
"osk.exe" selected (692.7 kB)

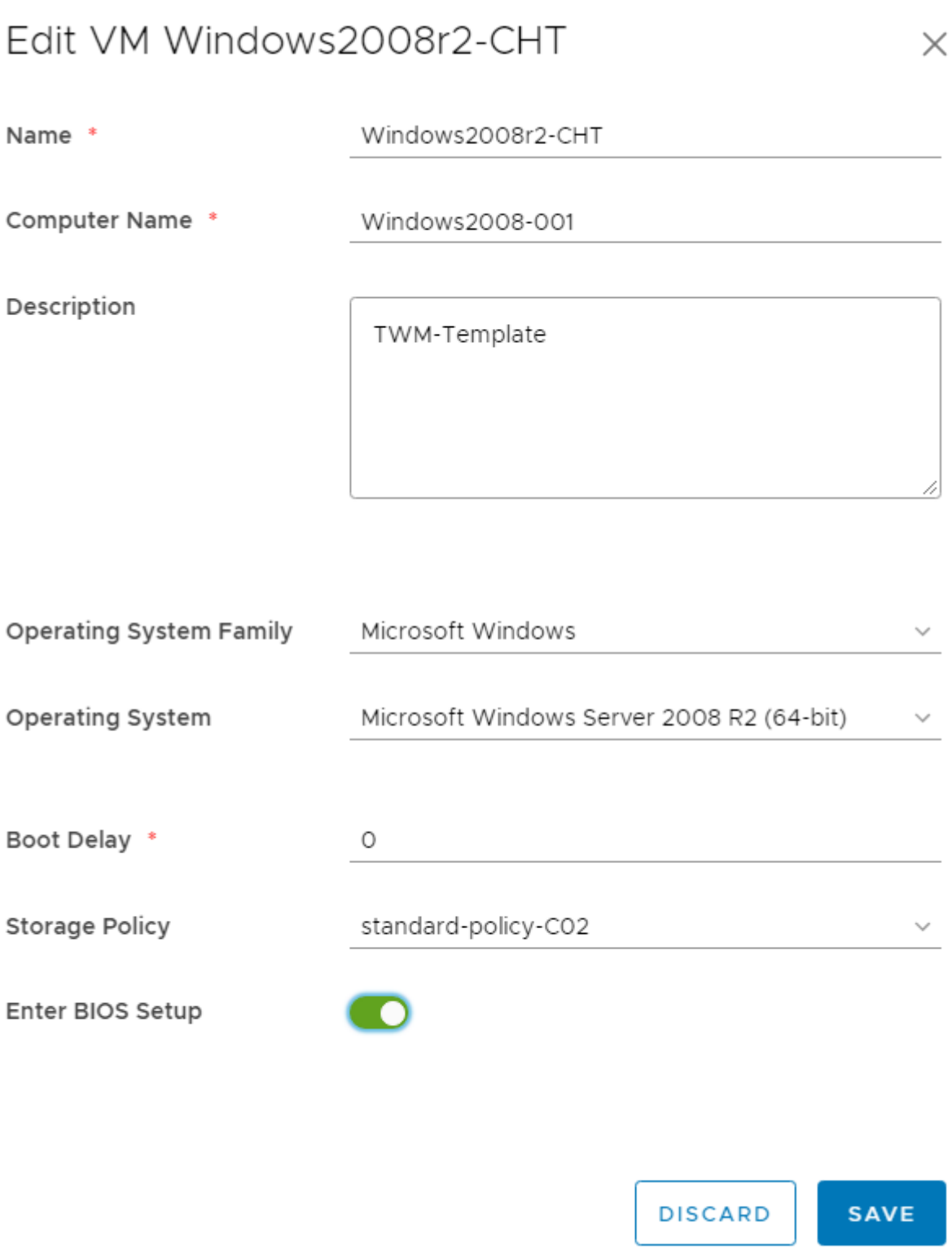
按 ENTER


ubuntu
Please remove the installation medium, then press ENTER:

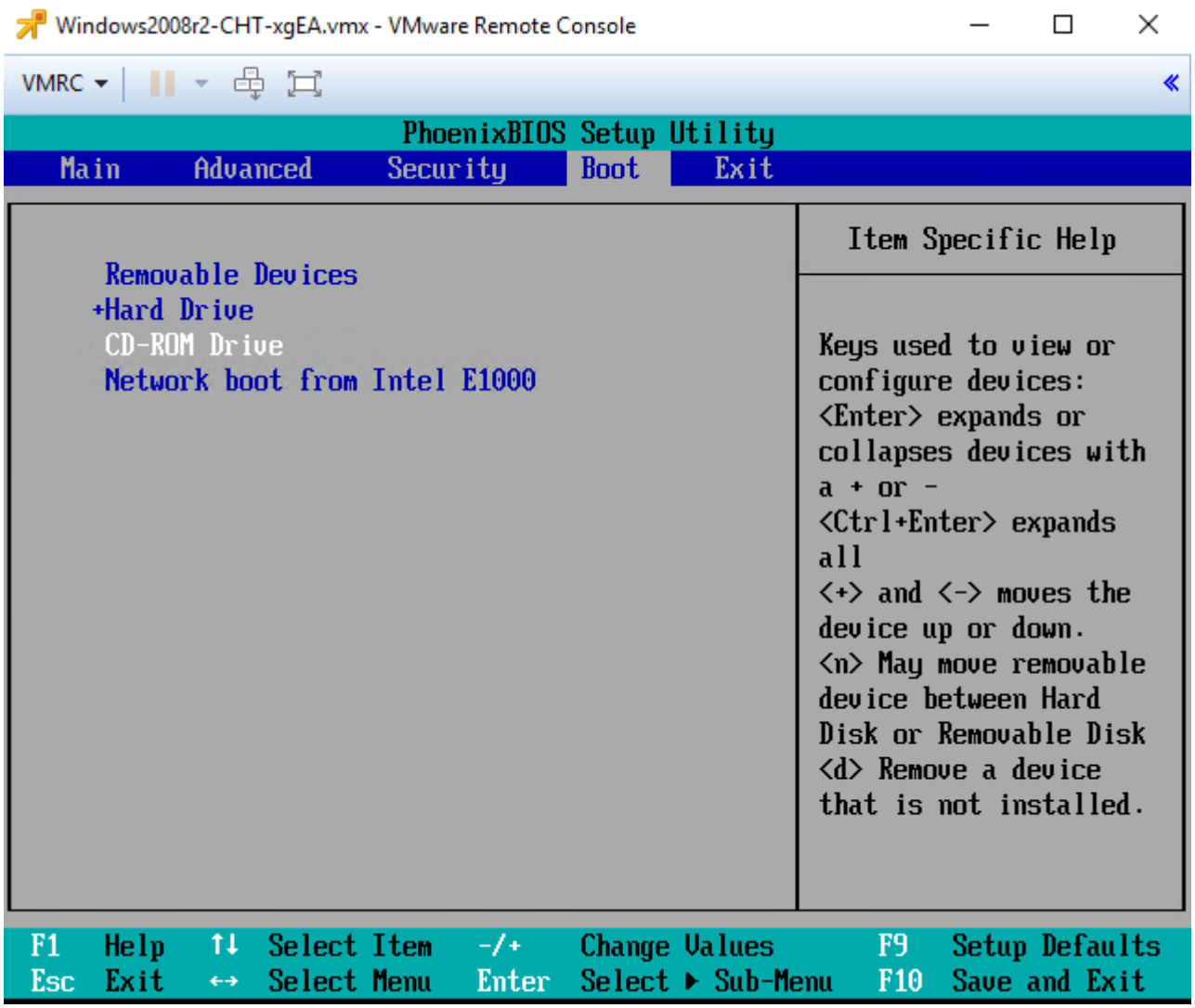
進入 portal，點選 action　Eject Media 將 iso 退出



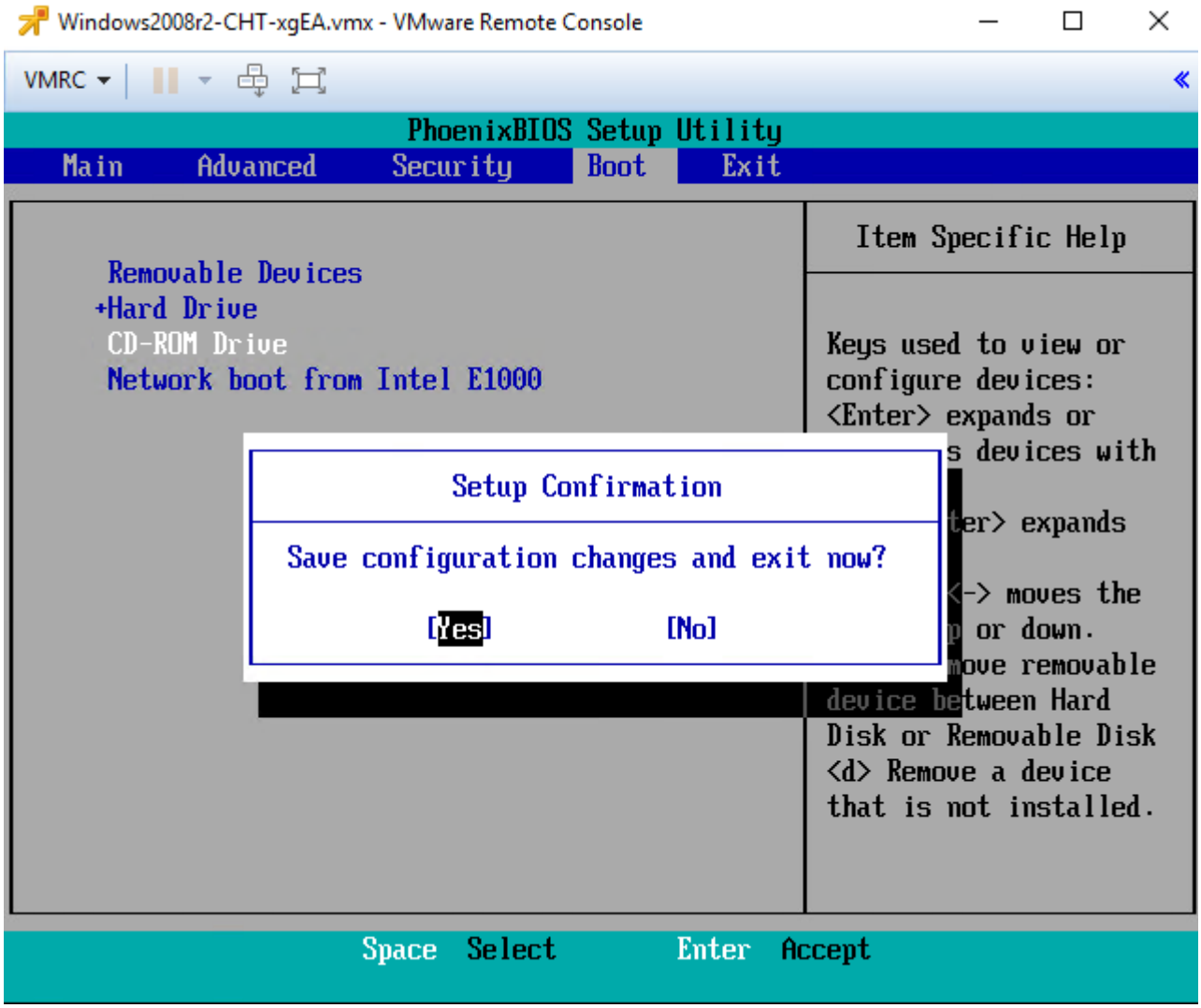
再次設定讓 VM 開機進入 BIOS，還原開機順序



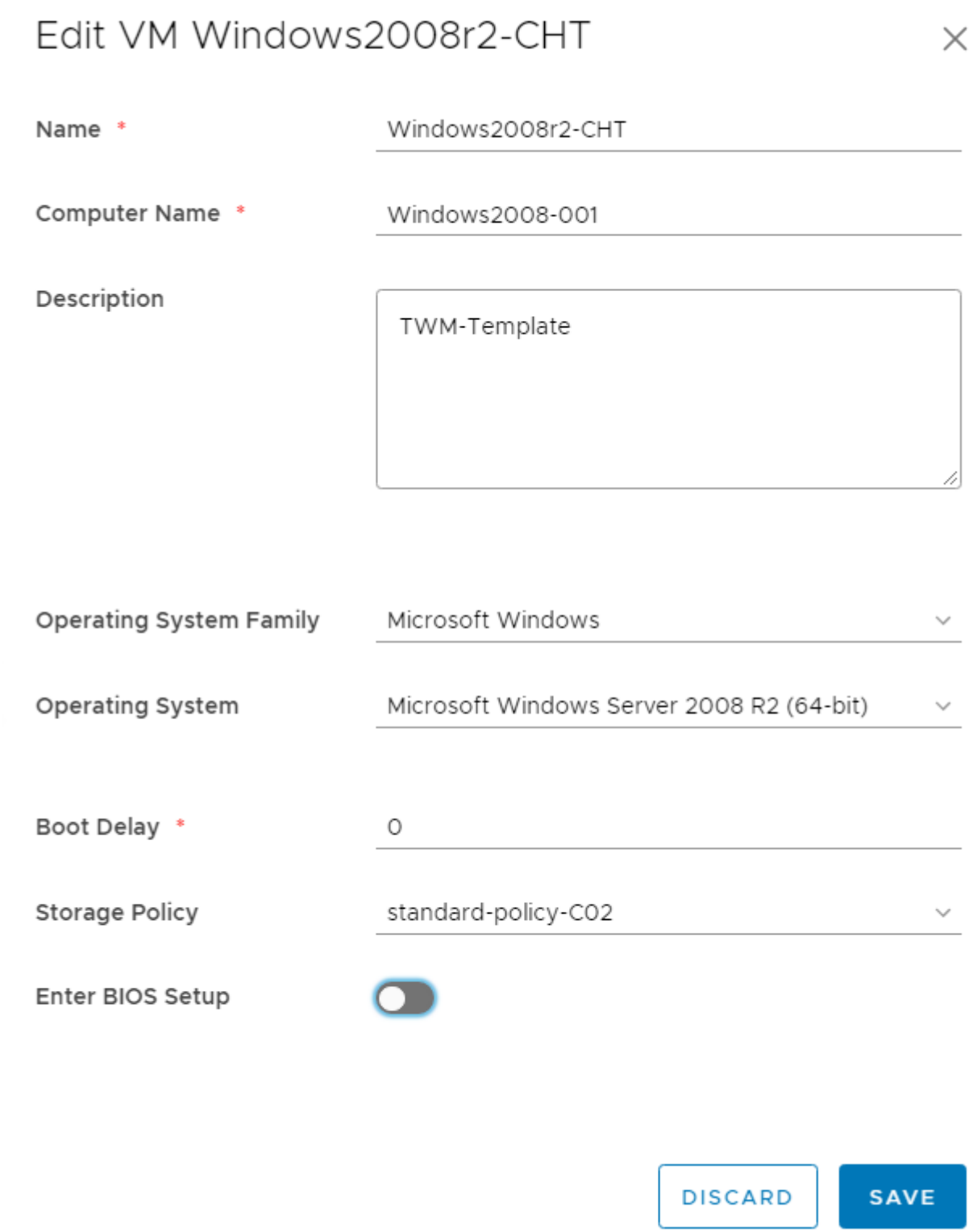
開機後選擇 Boot 按” -“號 兩次 讓 CD-ROM 回到第三順序



按 F10 存檔並離開


Windows2008r2-CHT-xgEA.vmx - VMware Remote Console
VMRC
PhoenixBIOS Setup Utility
Main
Advanced
Security
Boot
Exit
Item Specific Help
Removable Devices
+Hard Drive
CD-ROM Drive
Network boot from Intel E1000
Keys used to view or
configure devices:
<Enter> expands or
Setup Confirmation
Save configuration changes and exit now?
[Yes]
[No]
Space Select
Enter Accept

最後再回到 VM 設定把確認 BIOS 選項開關調回關閉



到此已復原先前的變更作業。