



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 10 版

2023 年 10 月修訂

目錄

1. 開通帳號.....	1
2. 第一次登入運算雲 3.0.....	6
修改聯絡人	6
變更登入密碼	7
OTP 簡訊驗證選項設定	8
3. 開始使用運算雲 3.0.....	9
登入運算雲 3.0 的方式	9
客戶管理中心功能介紹.....	13
雲平台首頁功能介紹	26
4. vApp 管理	26
啟動 vApp.....	27
停止 vApp.....	27
暫止 vApp.....	29
移除 vApp 中的虛擬機器.....	30
重設 vApp.....	32
建立 vApp 快照	33
還原 vApp 至快照.....	36
移除 vApp 快照	37
新增 vApp 範本	39
下載 vApp 範本	48
5. VM 管理	49
VM 作業系統環境說明	49
新增 VM	50
啟動 VM	54
關閉 VM	54
暫止 VM	55

重設 VM	56
建立 VM 快照	56
還原 VM 快照	58
移除 VM 快照	60
MSSQL DBVM 啟用程序說明	62
MSSQL DBVM 驗證程序說明	70
6. VM 設定調整	81
名稱設定	81
客體作業系統自訂	82
7. VM 硬體調整	85
卸除式媒體	85
硬碟	85
計算	86
NIC	88
8. VM 資料加密	89
9. 設定組織虛擬資料中心網路(VDCNetwork)	90
新增組織虛擬資料中心網路	91
套用組織虛擬資料中心網路	95
10. Edge 管理	99
防火牆與 NAT 規則	100
DHCP	101
負載平衡器	102
IPSec VPN	104
11. 新版-設定組織虛擬資料中心網路(VDCNetwork)	109
新增組織虛擬資料中心網路	110
套用組織虛擬資料中心網路	115
組織虛擬資料中心網路啟用 DHCP 服務	118

12. 新版-Edge 管理	123
防火牆與 NAT 規則	125
負載平衡器	136
IPSec VPN	142
13. 應用一：透過辦公室進行 VM 遠端管理	148
情境說明	148
前置作業	148
設定項目	149
14. 應用二：透過辦公室進行檔案傳輸	155
情境說明	155
前置作業	156
設定項目	156
15. 應用三：建置網站服務	161
情境說明	161
前置作業	162
設定項目	162
16. 附件	174
A. 《Windows Server 檔案與磁碟加密》	174
A-1. 檔案系統(EFS)加密	174
A-2. BitLocker 加密(需重啟 Windows Server)	181
B. 《Linux 磁碟加密說明》：	191
C. Windows2008R2 修改系統管理員密碼	194
1. 設定開機進入 BIOS，使用指定的 ISO 開機	197
2. 使用指定的 ISO 開機，設定 Windows 開機使用 CMD	205
3. Windows 重設密碼作業	221
4. 復原先前的變更作業	226

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：

親愛的客戶，您申請的台灣大哥大運算雲 3.0 服務帳號開通驗證信，已寄到您指定的 Email 信箱，請於 30 天內登入信箱進行帳號驗證，謝謝。貼心提醒：若 Email 信箱收件夾未收到開通驗證信，請一併檢視垃圾郵件資料夾，謝謝。

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)

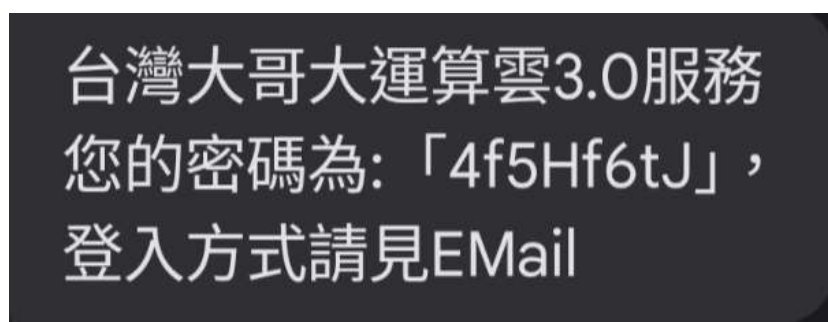


填入驗證碼以及下方驗證碼二個欄位，並按下“確定送出”按鈕

步驟5. 驗證成功，網頁顯示如下訊息，並且您申請的雲服務登入密碼將以簡訊+email 方式寄送到技術聯絡人的手機中



以下為簡訊示意圖



以下為 email 示意圖



到此帳號開通完成取得登入密碼後，請回到帳號啟用通知信，如下圖紅線處為您的登入帳號，紅框處為登入網址



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



修改技術聯繫人

聯絡人姓名*	
聯絡人行動電話*	
聯絡人Email*	

更新成功後，請重新登入資料才會更新。

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”



變更密碼

原密碼*	
新密碼*	
再次輸入新密碼*	

確定 取消

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。



選項設定

登入是否使用多因子驗證*

☐ 是 ☒ 否

確定 取消

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



登入雲平台請先通過OTP簡訊驗證

請輸入OTP簡訊驗證

OTP簡訊驗證

發送簡訊與Email驗證碼

驗證登入

Email 通知範例如下圖



運算雲3.0 登入驗證碼通知

帳 號：admin@pidcp.com

驗 證 碼：457728

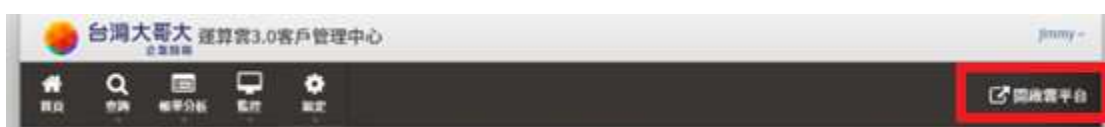
技術聯絡人行動電話會取得簡訊驗證碼，以下為簡訊範例圖



台灣大哥大運算雲 3.0 服務登入驗證
碼:457728

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。



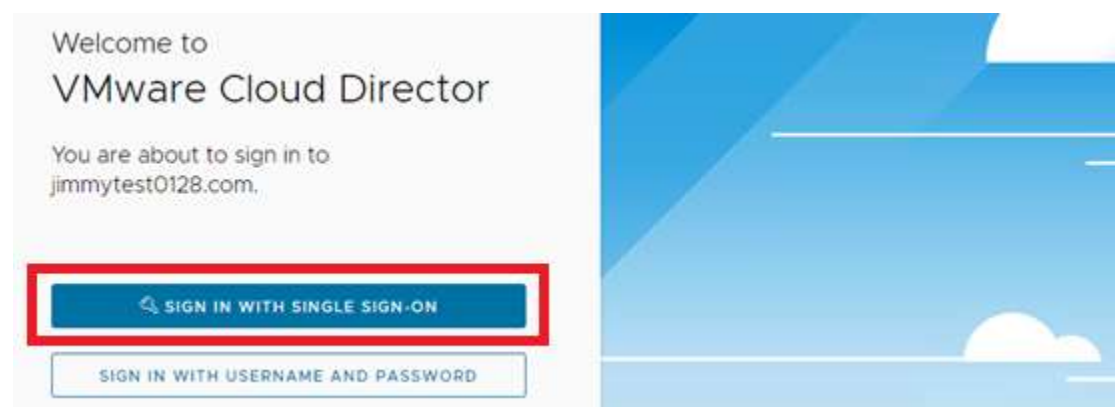
台灣大哥大 運算雲3.0客戶管理中心

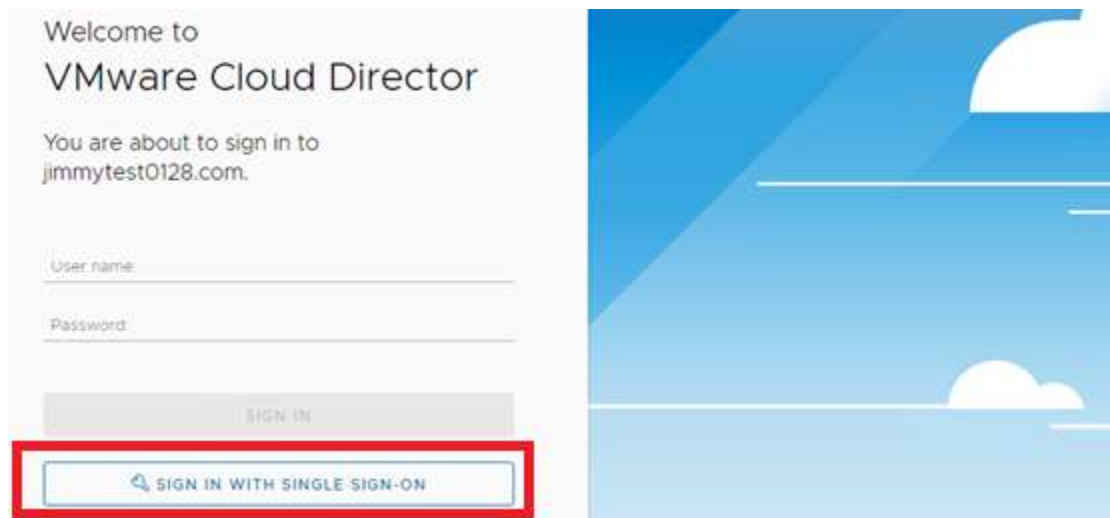
首頁 查詢 帳單分析 監控 設定

開啟雲平台



如登入時出現以下畫面，請點選「SIGN IN WITH SINGLE SIGN-ON」。





若閒置過久會自動登出，頁面會轉導如下圖。再次登入請選擇
“ 透過 SINGLE SIGN ON 登入”

請不要使用“ 以整合式使用者身分登入”



客戶管理中心功能介紹

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。



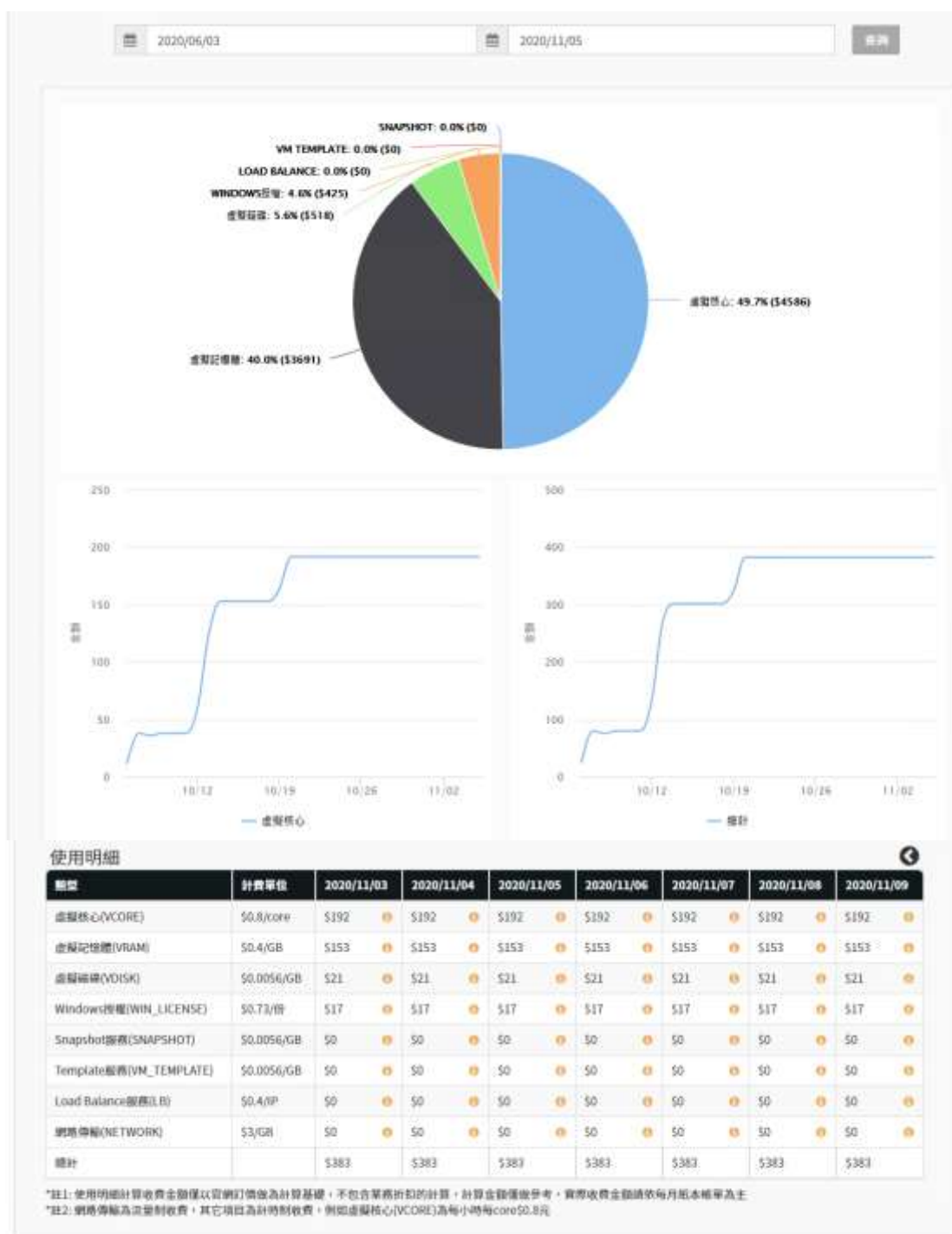
1. 首頁：查看公告、租用資源概況、帳單概況
2. 查詢：查詢特定 VAPP、特定主機使用狀態



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

(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。



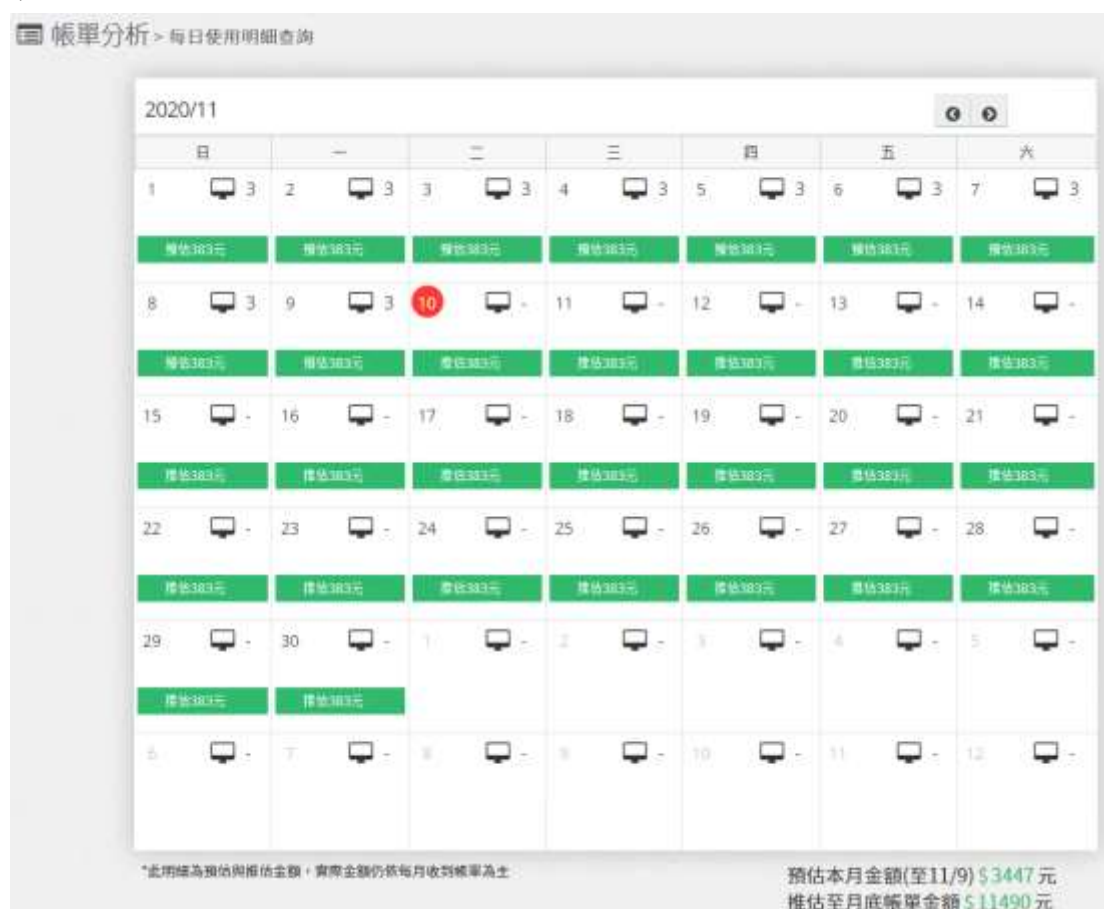
(2) 每月使用量預估費用查詢

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

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。

(3) 每日使用明細查詢

此功能將「使用明細」記錄改以月曆方式來呈現，紅圈處為當日，當日的前一天至月初會顯示預估金額並且在該日的電腦圖樣(icon)後方顯示為當日所使用的 VM 數，至於當日至月底顯示則為推估金額，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。



帳單分析 - 每日使用明細

2020/11/9 使用明細紀錄

0:00	3 0	vCore共10核	vRam共16GB	vDisk共160GB	snapshot共0GB
1:00		Windows OS授權共1套	LB IP共0個	網路傳輸共0GB	template共0GB
		\$8	\$6	\$1	\$0
		\$1	\$0	\$0	\$0
1:00	3 0	vCore共10核	vRam共16GB	vDisk共160GB	snapshot共0GB
2:00		Windows OS授權共1套	LB IP共0個	網路傳輸共0GB	template共0GB
		\$8	\$6	\$1	\$0
		\$1	\$0	\$0	\$0
2:00	3 0	vCore共10核	vRam共16GB	vDisk共160GB	snapshot共0GB
3:00		Windows OS授權共1套	LB IP共0個	網路傳輸共0GB	template共0GB
		\$8	\$6	\$1	\$0
		\$1	\$0	\$0	\$0
3:00	3 0	vCore共10核	vRam共16GB	vDisk共160GB	snapshot共0GB
4:00		Windows OS授權共1套	LB IP共0個	網路傳輸共0GB	template共0GB
		\$8	\$6	\$1	\$0
		\$1	\$0	\$0	\$0
4:00	3 0	vCore共10核	vRam共16GB	vDisk共160GB	snapshot共0GB
5:00		Windows OS授權共1套	LB IP共0個	網路傳輸共0GB	template共0GB
		\$8	\$6	\$1	\$0
		\$1	\$0	\$0	\$0
5:00	3 0	vCore共10核	vRam共16GB	vDisk共160GB	snapshot共0GB
		\$8	\$6	\$1	\$0

13447 元
11480 元

(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。

帳單分析 > 預估費用告警設定

2020/11

預估本月金額(至11/9) \$3447 元
推估至月底帳單金額 \$11490 元

帳單告警設定

☒ 開啟帳單告警功能

每月帳單預估大於多少金額 通知我 2000 \$

到達之後每增加多少金額 通知我 1000 \$

E-Mail 通知我 antonychen@taiwanmobile.com

儲存設定值

告警通知記錄

告警時間	告警內容
無任何資料	

(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。

帳單分析 > 每月VM使用時數查詢

使用時數

2020年11月

VM名稱	VAPP名稱	Private IP	作業系統	使用時數
centos7.7-vm2	vApp_linux	192.168.0.2	CentOS 7 (64-bit)	8天 0小時 0分
centos7.7 test vm	vApp_test	192.168.0.3	CentOS 7 (64-bit)	8天 0小時 0分
windows2016-vm01	vApp_system_1	192.168.0.1	Microsoft Windows Server 2016 or later (64-bit)	8天 0小時 0分

★使用時數包含VM開機及關機的加總時數，未足月份可能為系統資料尚未收集完全

VM使用時數明細記錄

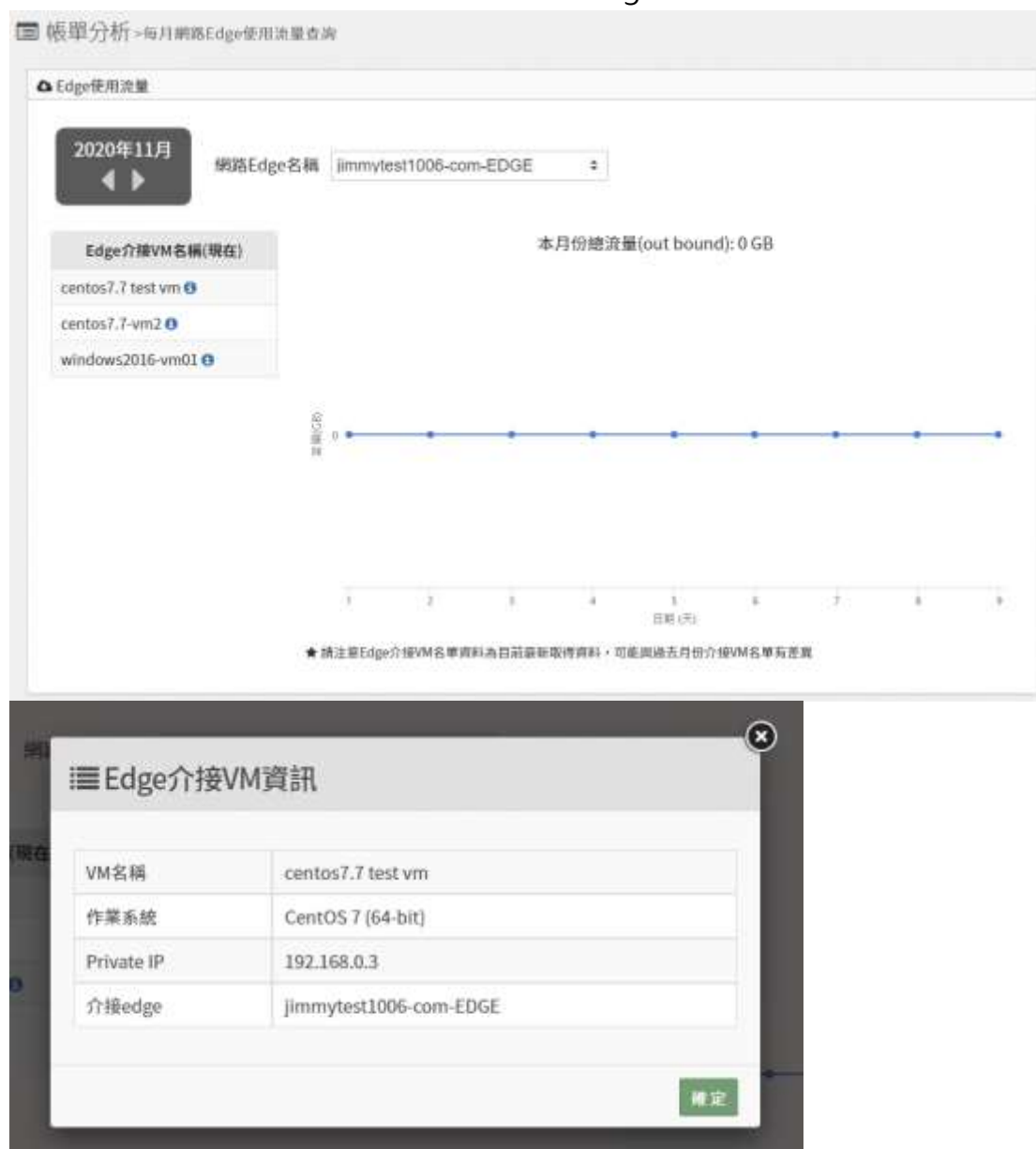
VM名稱:centos7.7-vm2 2020年11月 共開機 8天 0小時 0分

起始時間	結束時間	狀態	時長
2020-11-02 00:00:00	2020-11-10 00:00:00	開機	8天 0小時 0分

確定

(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 VM³。



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

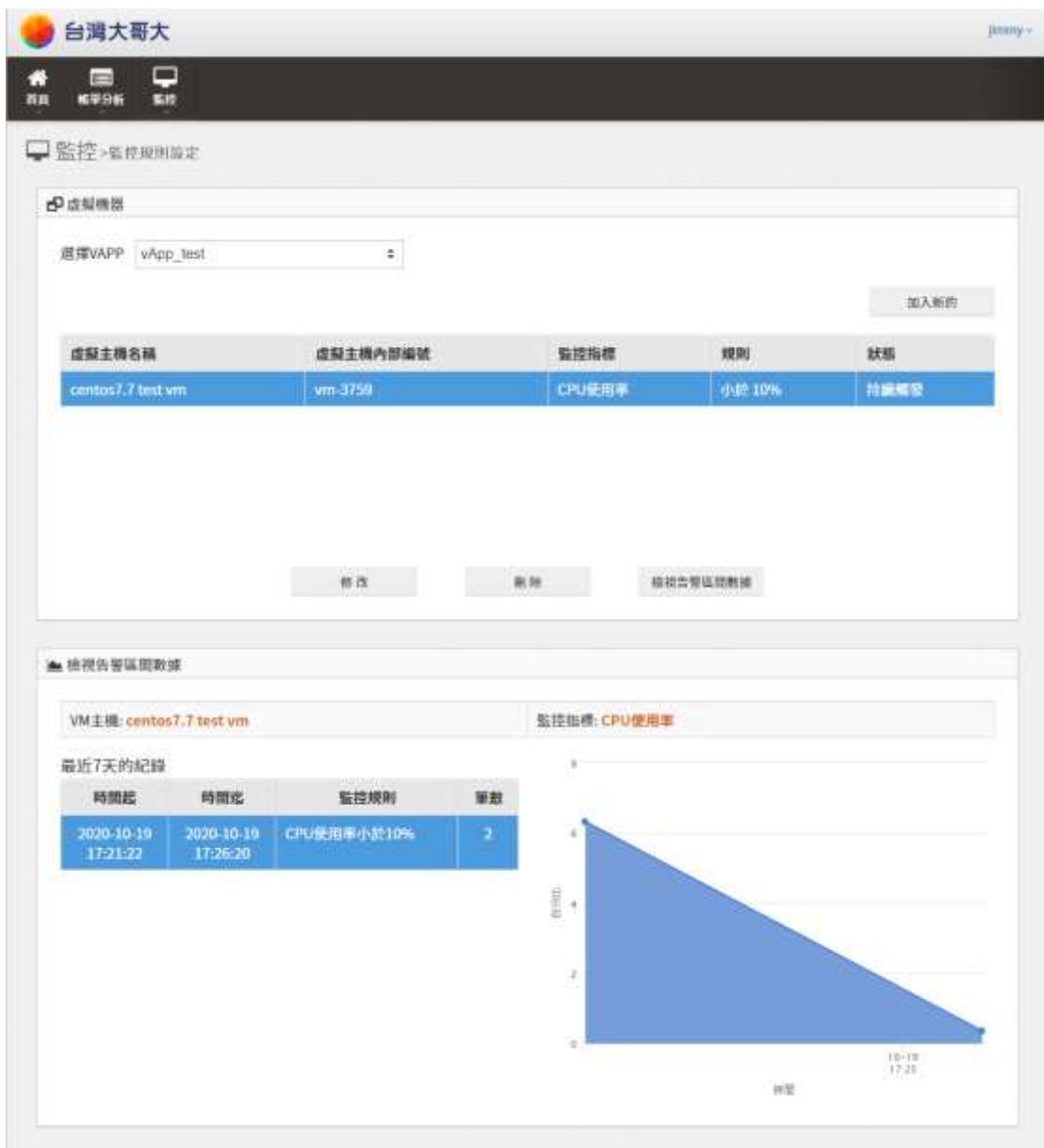
以上「新的監控規則」設定完成後，即會產生在列表上，並且從狀態欄文字如「監控中」即表示監控行為已作用，若監控到符合告警設定值就會發送告警通知⁴。VM 加入監控後會出現「檢視告警區間數據」按鈕，若有告警狀

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



台灣大哥大

監控 > 監控規則設定

選擇VAPP: vApp_test1

加入新的

虛擬主機名稱	虛擬主機內部編號	監控指標	規則	狀態
centos7.7 test vm	vm-3759	CPU使用率	小於 10%	持續觸發

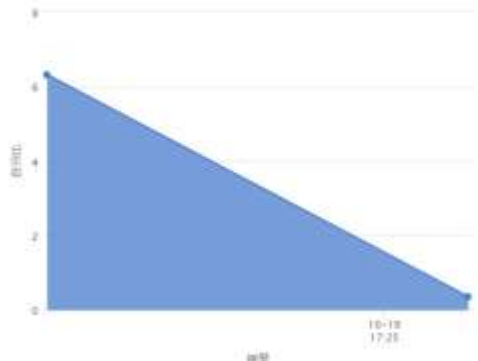
修改 刪除 檢視告警區間數據

檢視告警區間數據

VM主機: centos7.7 test vm 監控指標: CPU使用率

最近7天的紀錄

時間起	時間迄	監控規則	筆數
2020-10-19 17:21:22	2020-10-19 17:26:20	CPU使用率小於10%	2



(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。



台灣大哥大

監控 > 告警通知記錄查詢

告警通知記錄

選擇VAPP: vApp_admin_4 監控標的: windows2016-chn 告警通知日期: 2020-09-14

開始查詢

找到 0 筆告警通知記錄

告警通知時間	監控標的	通知訊息	通知人員	狀態
找不到告警通知記錄				

(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. 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

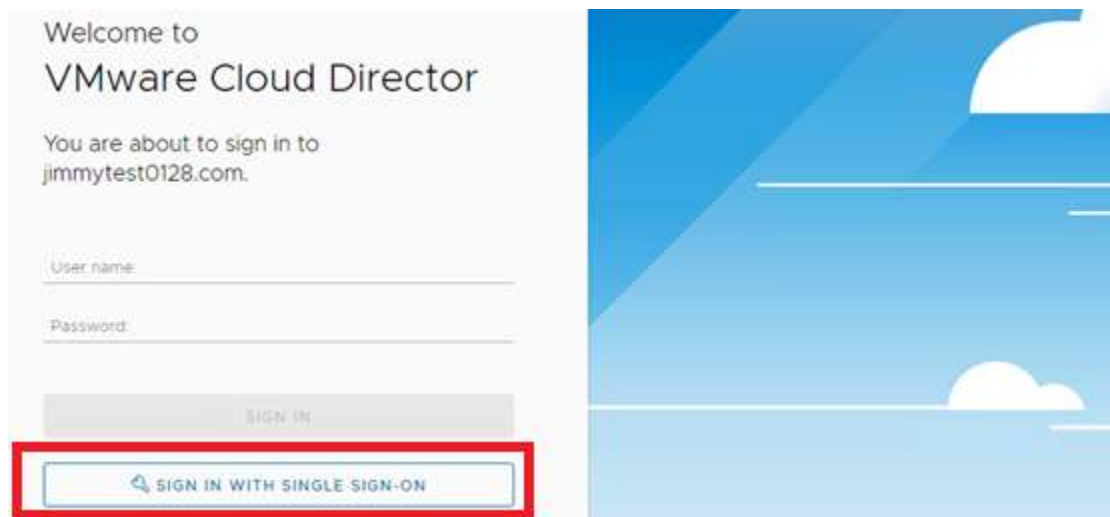


(3)子帳號登入後會自動轉導 VCD 雲平台使用者介面，請依以下步驟即可開啟雲平台



⁵ 子帳號狀態必須是關閉狀態才可以刪除

請點選「SIGN IN WITH SINGLE SIGN-ON」

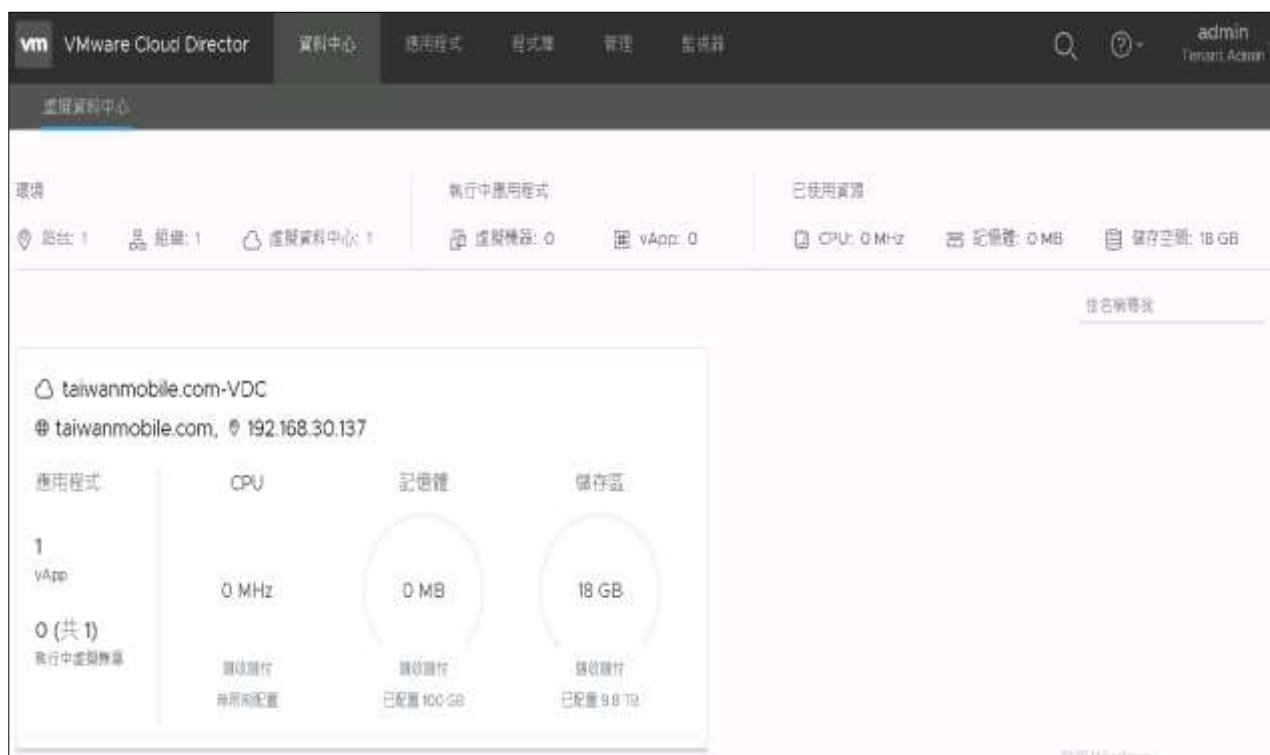


(4)子帳號沿用主帳號設定之多因子驗證，當主帳號被停用時、子帳號亦會停用

(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。

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



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. 程式庫：列出 vApp 範本、可掛載 ISO 清單
4. 管理：可修改組織管理員帳號內容
5. 監視器：可以看到工作紀錄、事件紀錄。
6. 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**應用程式**。
2. 在下方選項中，按一下**虛擬應用程式**。
3. 點選 vApp 左下角**動作**，然後選取**開啟電源**。



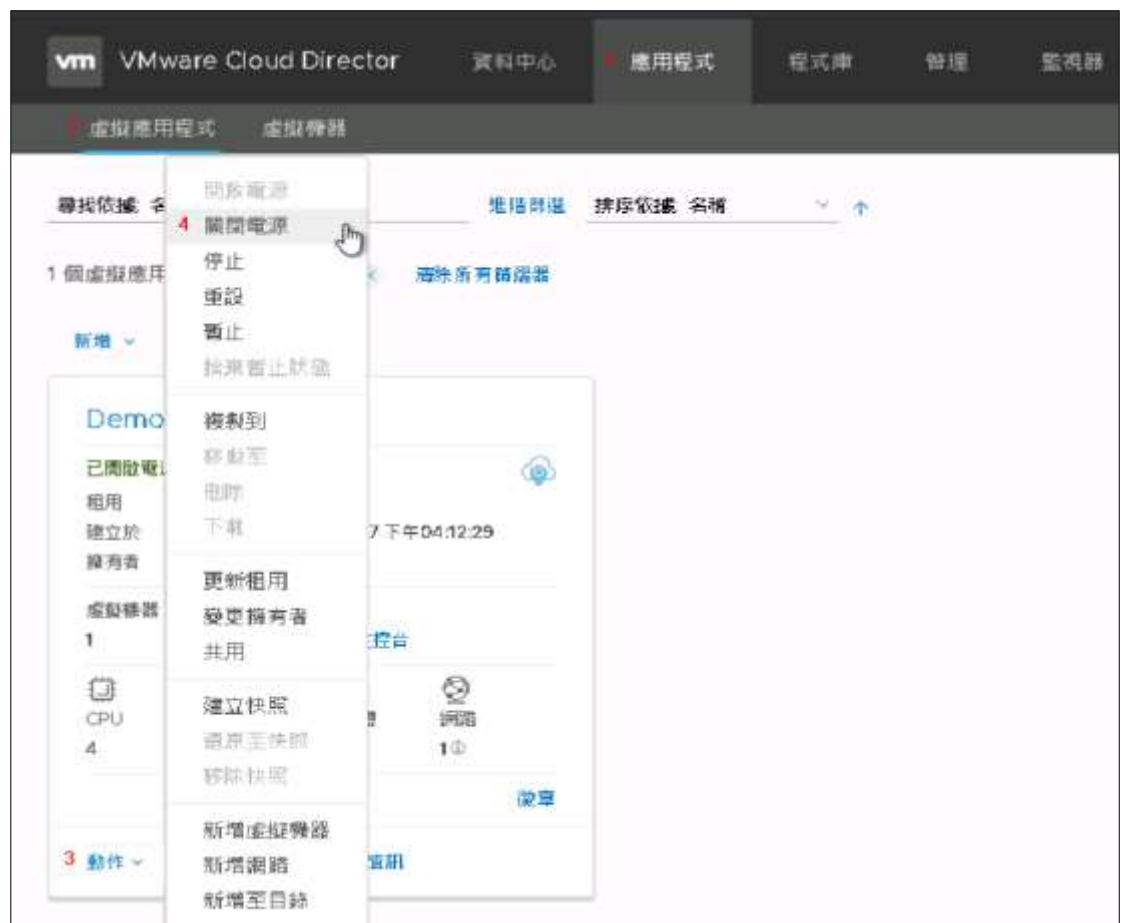
停止 vApp

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 **應用程式**。
2. 在下方選項中，按一下 **虛擬應用程式**。
3. 點選 vApp 左下角 **動作**，然後選取 **關閉電源**。



4. 按一下 **確定**。



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

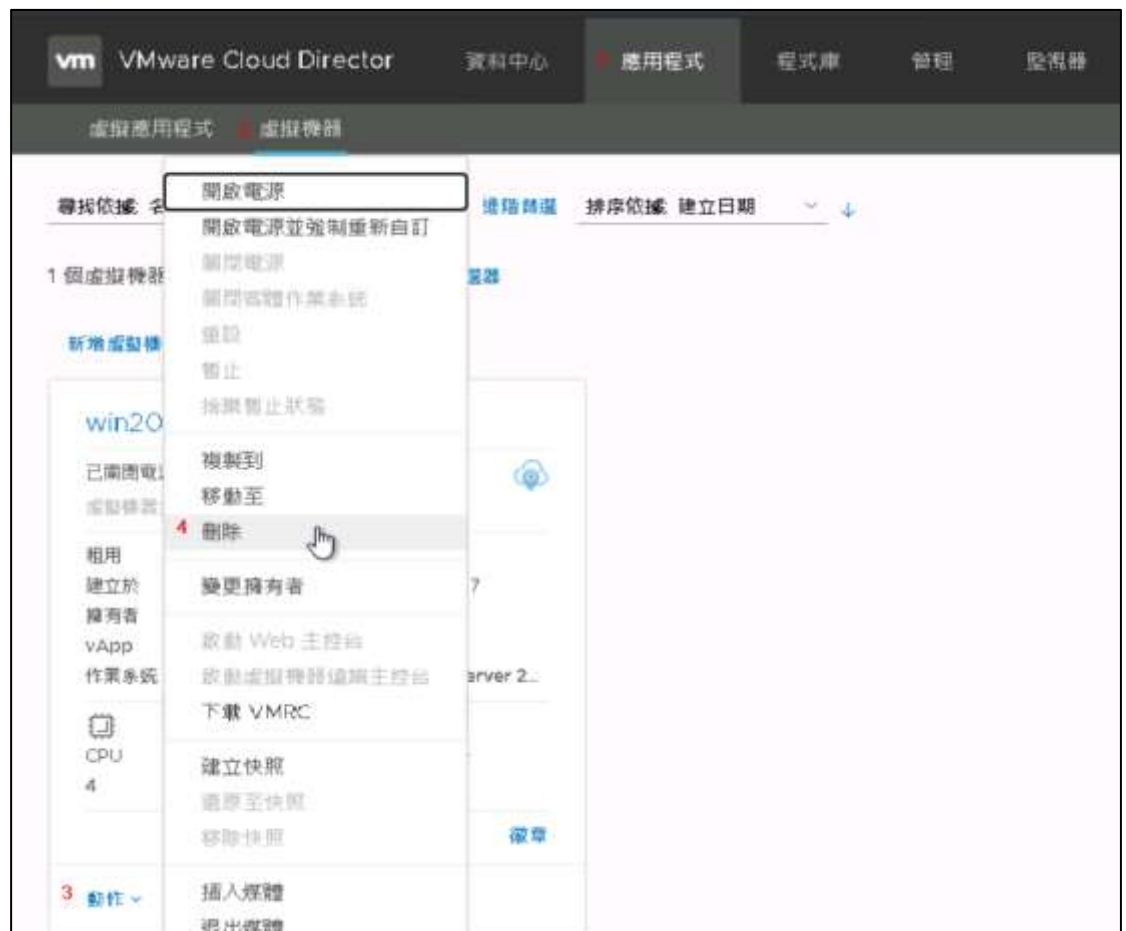


移除 vApp 中的虛擬機器

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**。

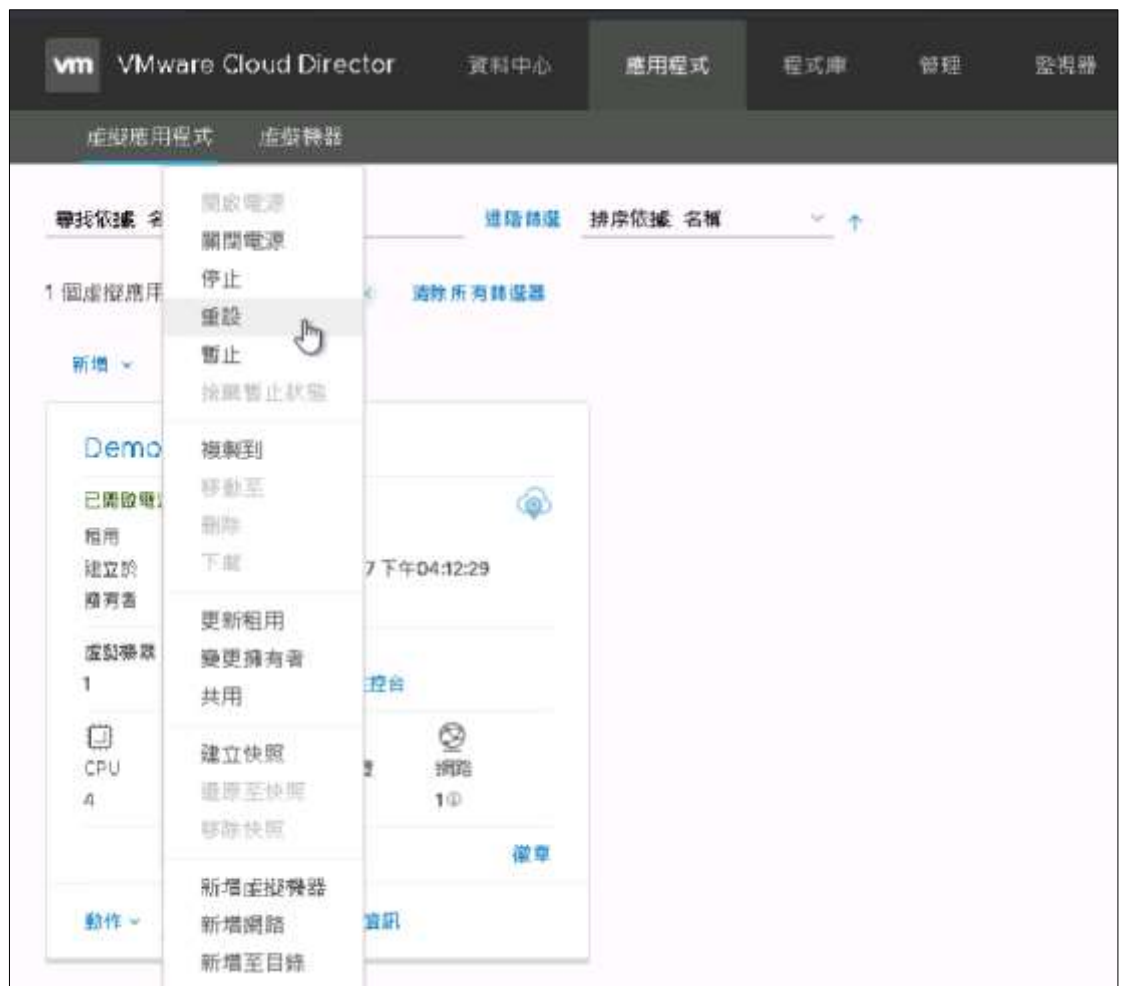


重設 vApp

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

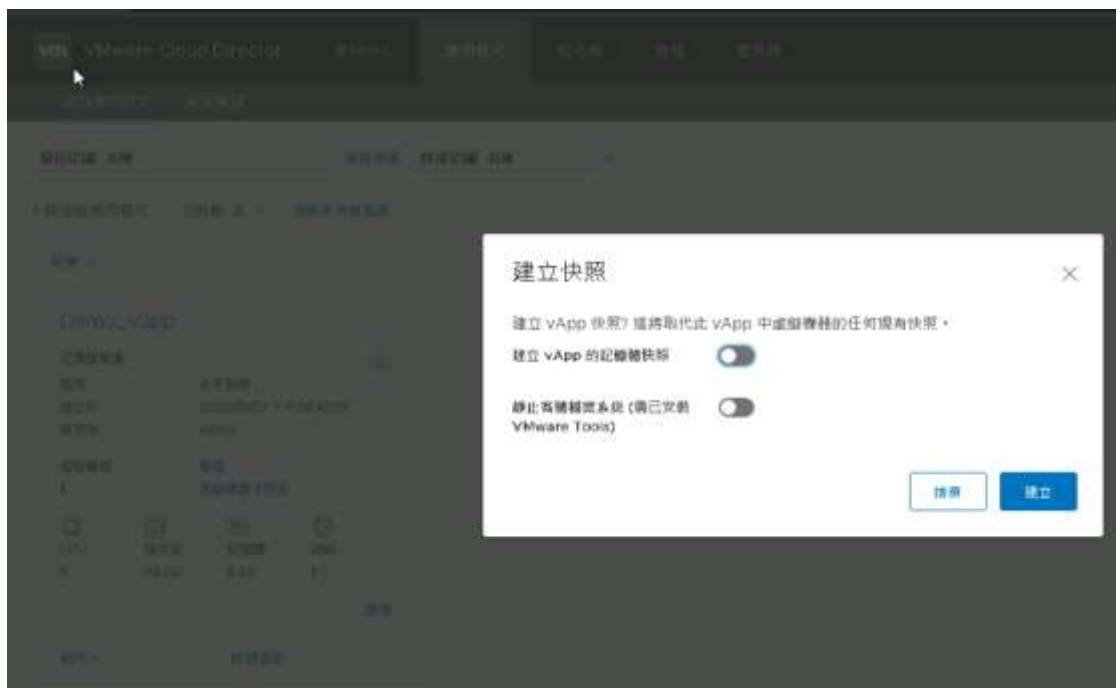
1. 按一下 **應用程式**。
2. 在下方選項中，按一下 **虛擬應用程式**。
3. 點選 vApp 左下角**動作**，然後選取**建立快照**。



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。

vm 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

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

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 1 [管理](#)
[虛擬機器主控台](#)

CPU 4 儲存區 88 GB 記憶體 8 GB 網路 1

[備單](#)

動作 [詳細資訊](#)

vm VMware Cloud Director 資料中心 應用程式 程式庫 管理 監視器

地址: 192.168.30.137 組織: training 資料中心: training-vdc

所有 vApp > Demo_Vapp

Demo_Vapp 動作

一般

虛擬機器 開始和停止順序 網路圖表 網路 實體內容 共用 中繼資料 監視器 工作 事件

詳細

資訊	
名稱	Demo_Vapp
狀態	已開啟電源
基礎	Demo
資料中心	training-vdc
擁有者	admin
快照	2020/12/01 下午05:28:37

詳細

租用

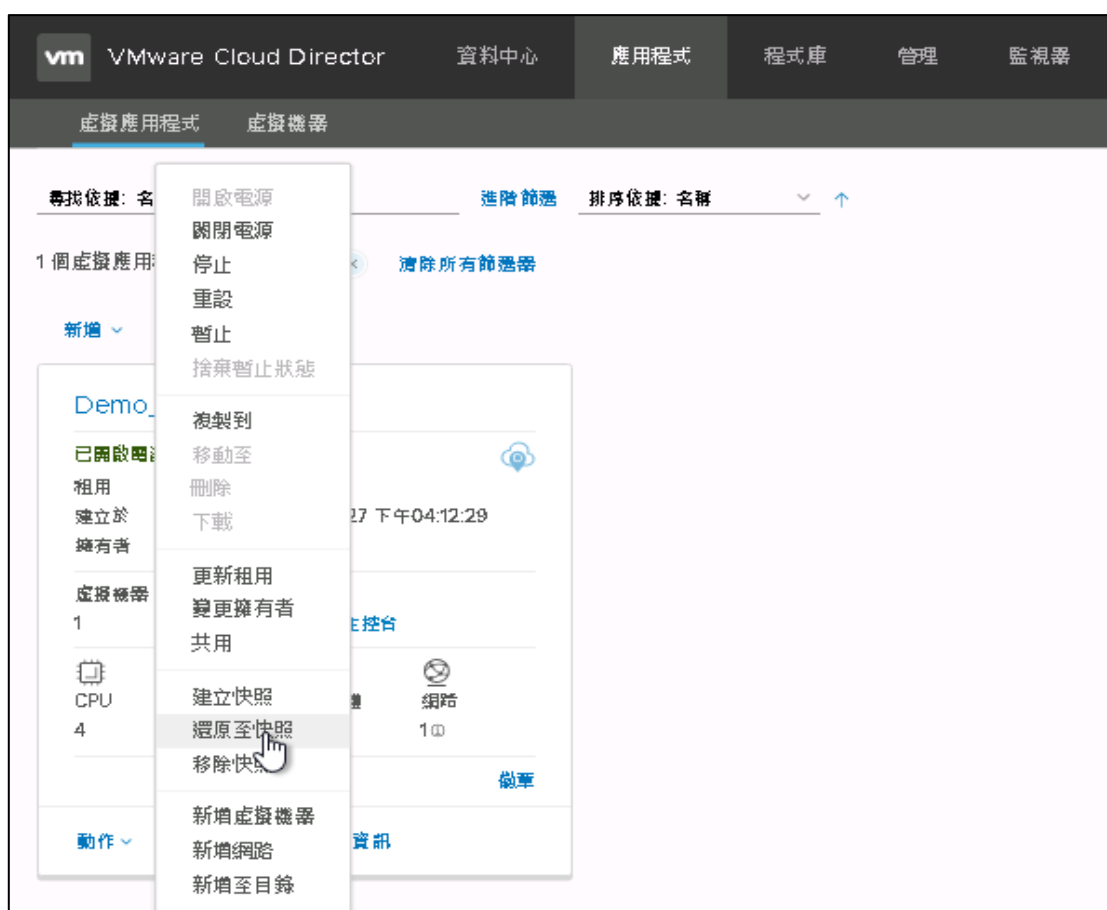
執行階段 執行階段租用永不到期。

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

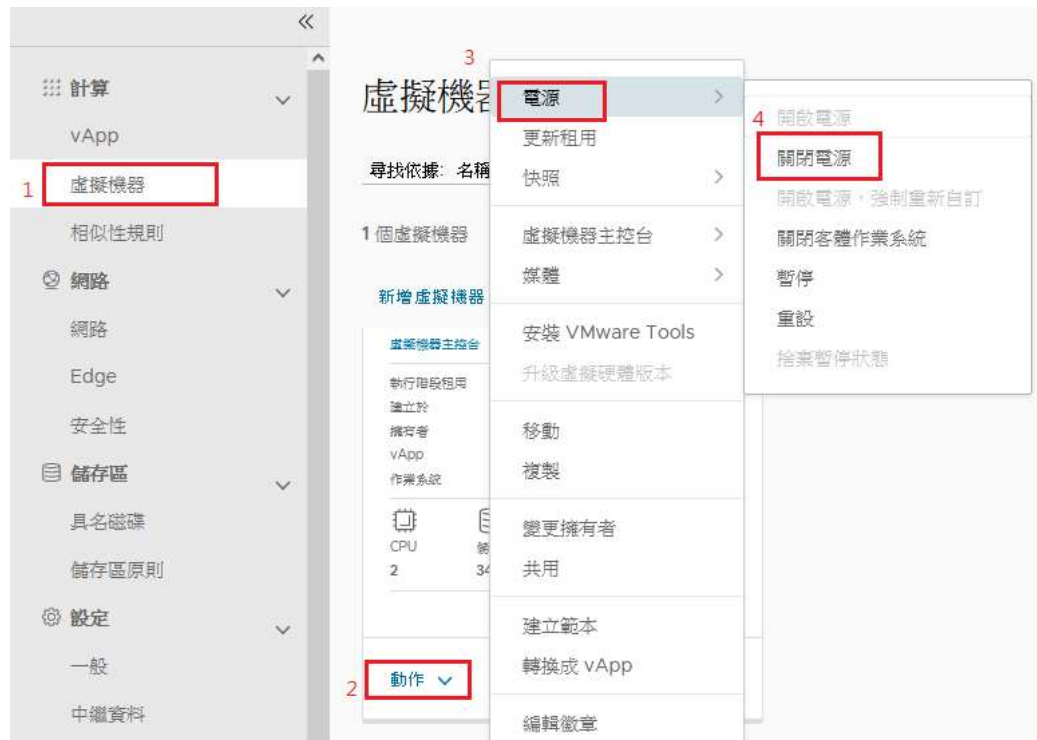
1. 按一下 **應用程式**。
2. 在下方選項中，按一下 **虛擬應用程式**。
3. 點選 vApp 左下角 **動作**，然後選取 **移除快照**。



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」。



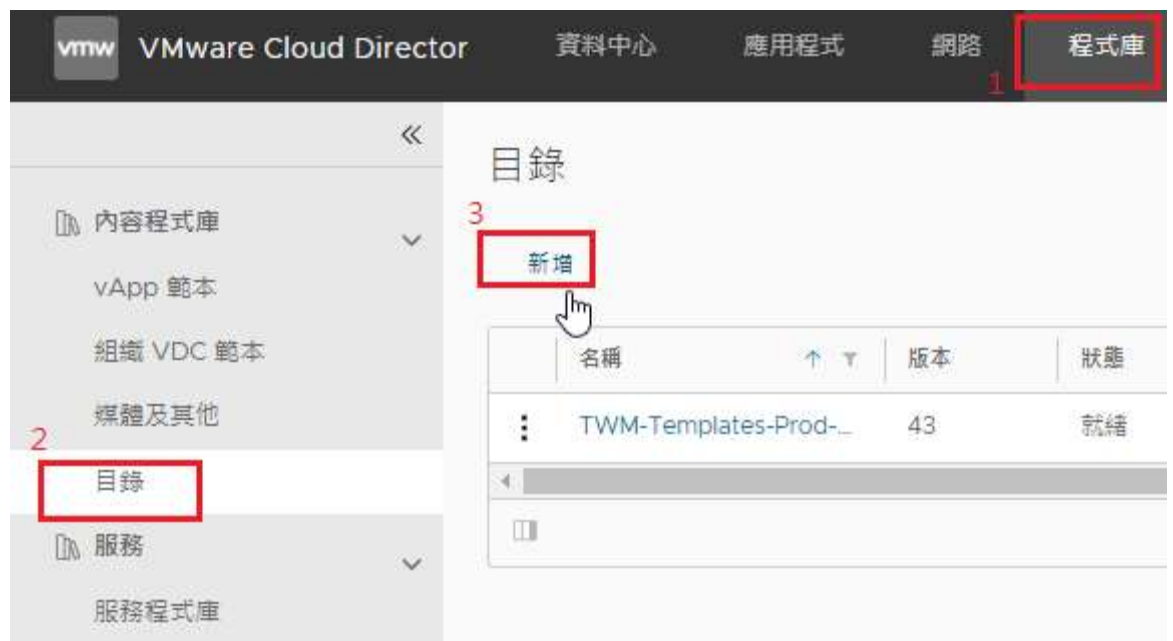
新增 vApp 對話框，包含以下欄位：

- 名稱：CentOS_Temp (已填入)
- 說明：(空白)
- 開啟電源：(未勾選)

下方有四個標籤：虛擬機器、作業系統、計算、網路。計算標籤下有一個漏斗圖示。

底部有兩個按鈕：取消 (藍色) 和 建立 (藍色，已高亮)。

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. 儲存區原則選擇 standard-policy-XXX > 下一步。



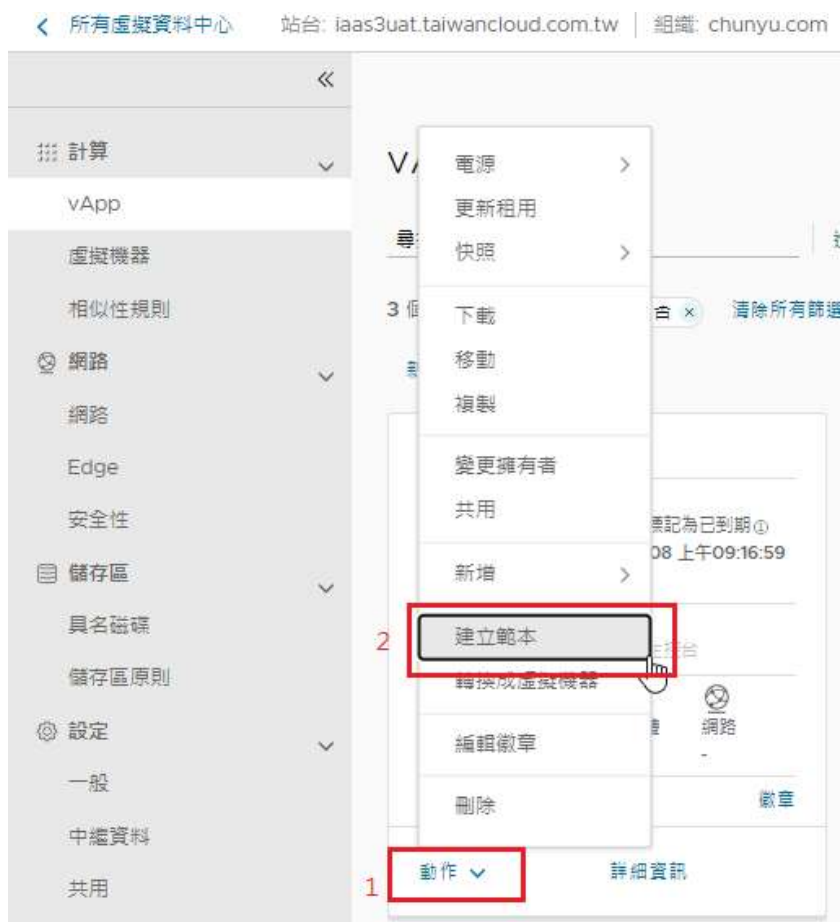
4. 點選完成。



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，到程式庫>vApp 範本會看到打包好的 vApp



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/certifications/docs/usg>

Rocky Linux Security

https://docs.rockylinux.org/guides/security/learning_selinux/

Oracle Linux Security

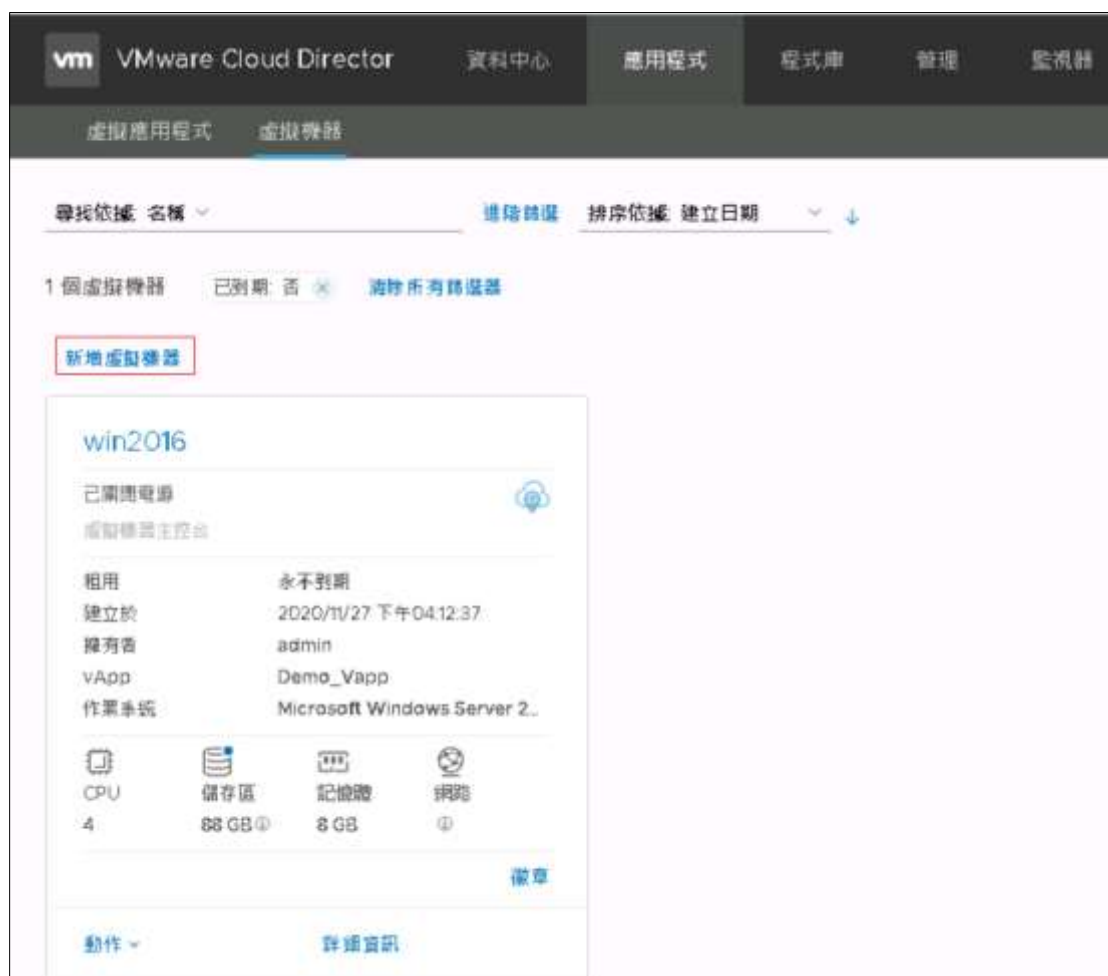
<https://linux.oracle.com/security/>

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**。



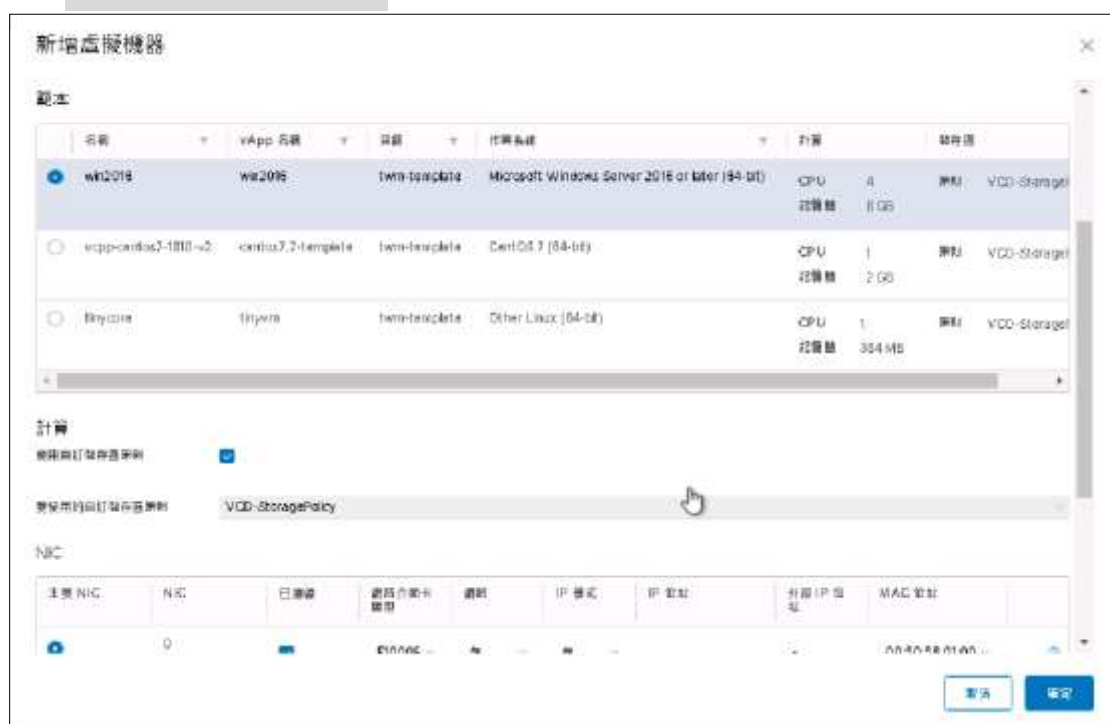
4. 選取虛擬資料中心，將 VM 新增至虛擬資料中心裡。



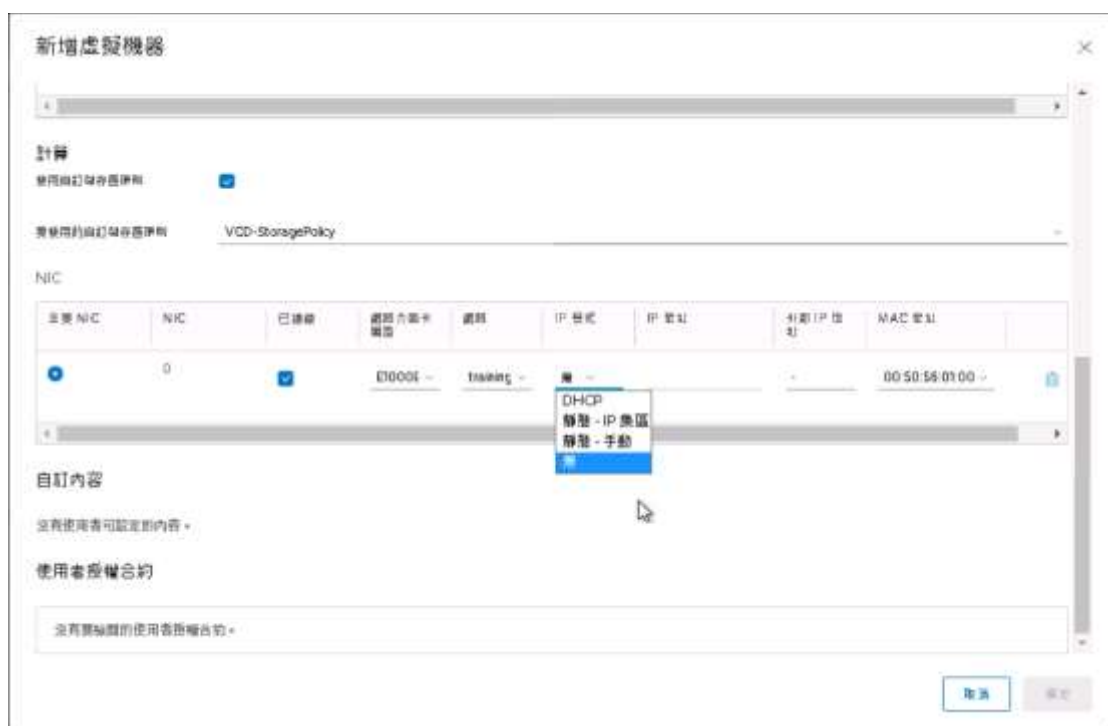
5. 輸入 VM 名稱及電腦名稱 (電腦名稱只能包含英數字元和連字號，不能只有數字)，類型選擇從範本，開啟電源選項可依需求勾選



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**。

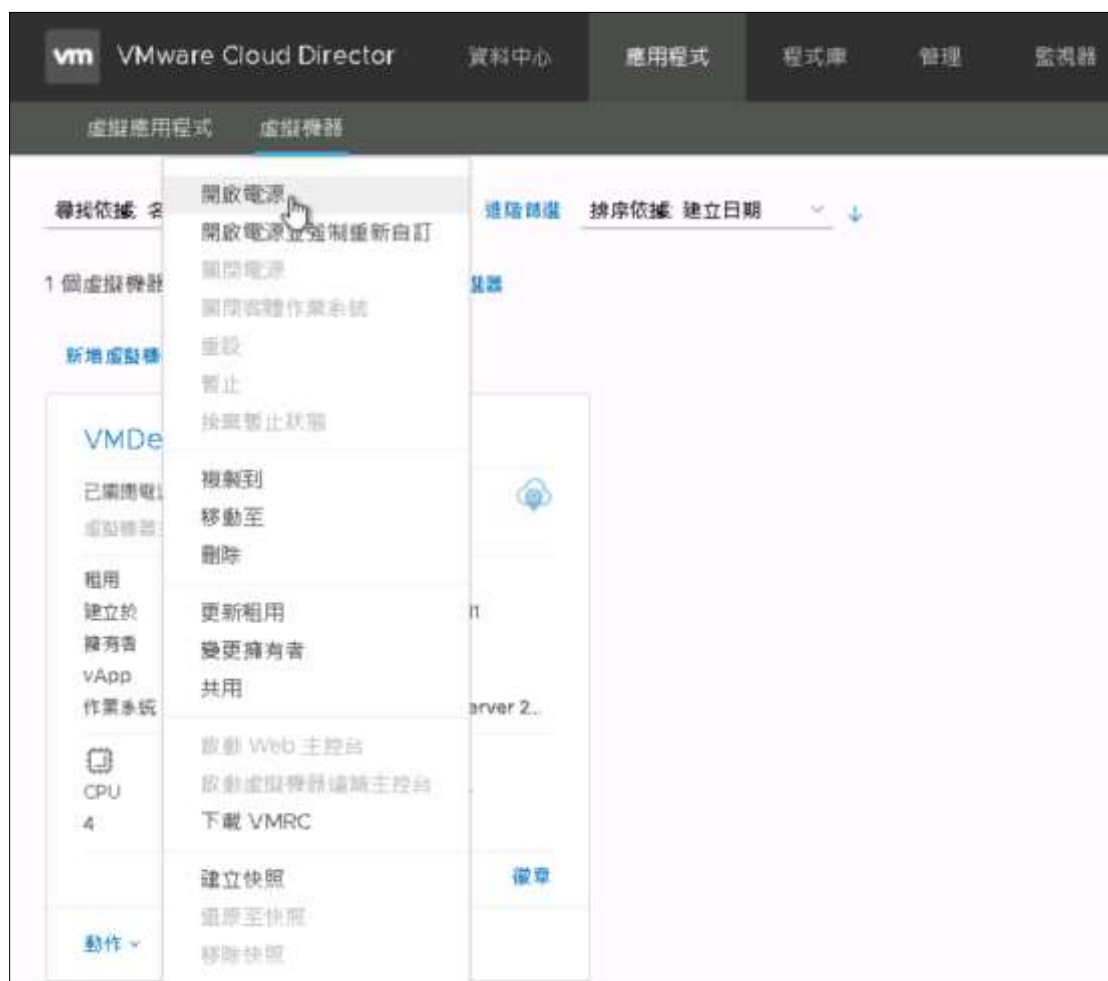


8. 新增成功的虛擬機器會出現在頁面中。



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**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**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**暫止**。

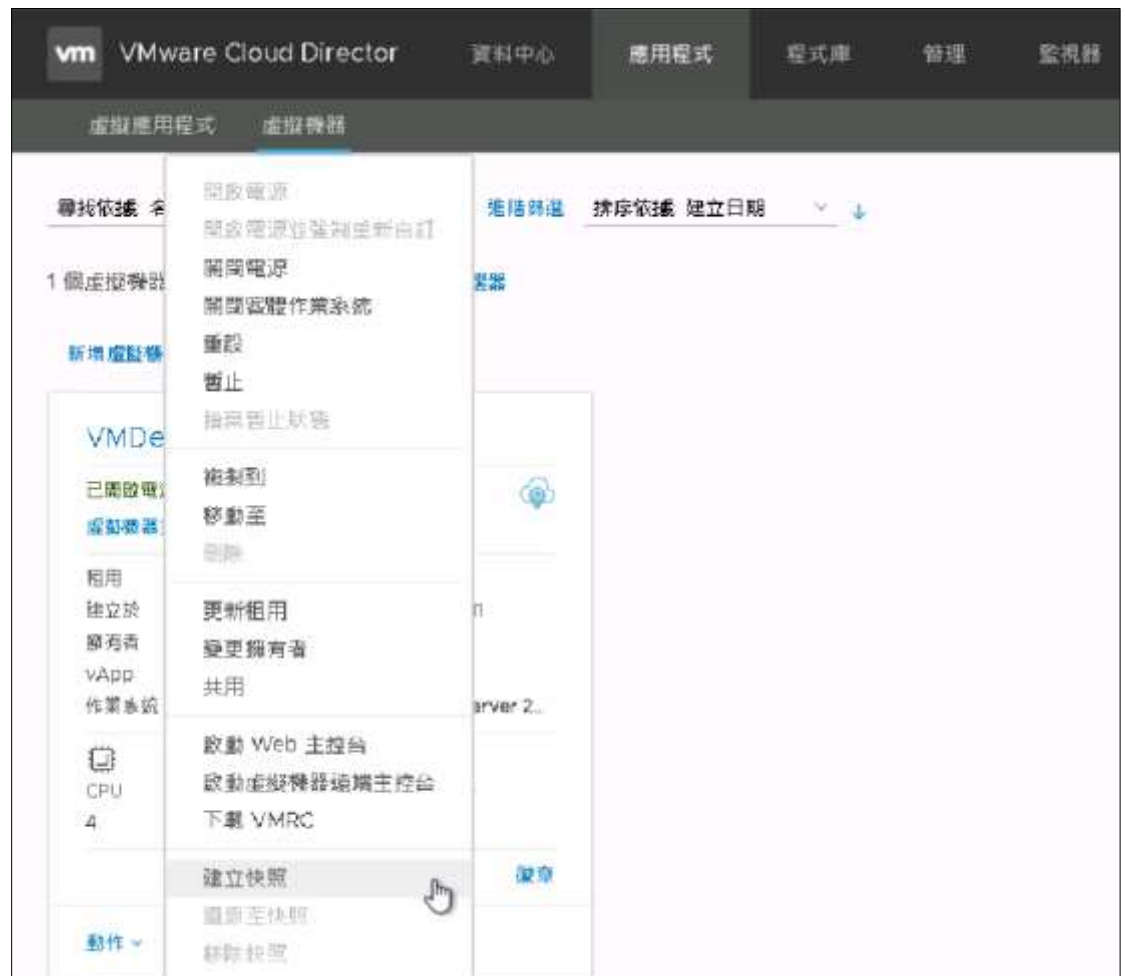


重設 VM

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



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**，然後選取 **移除快照**。



4. 確認則按**確定**。



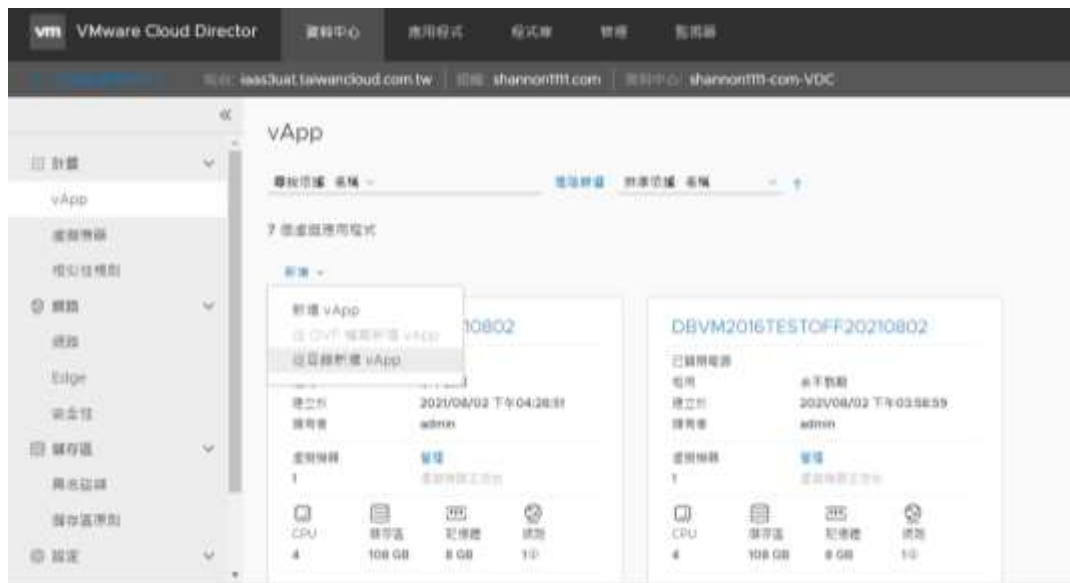
MSSQL DBVM 啟用程序說明

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：

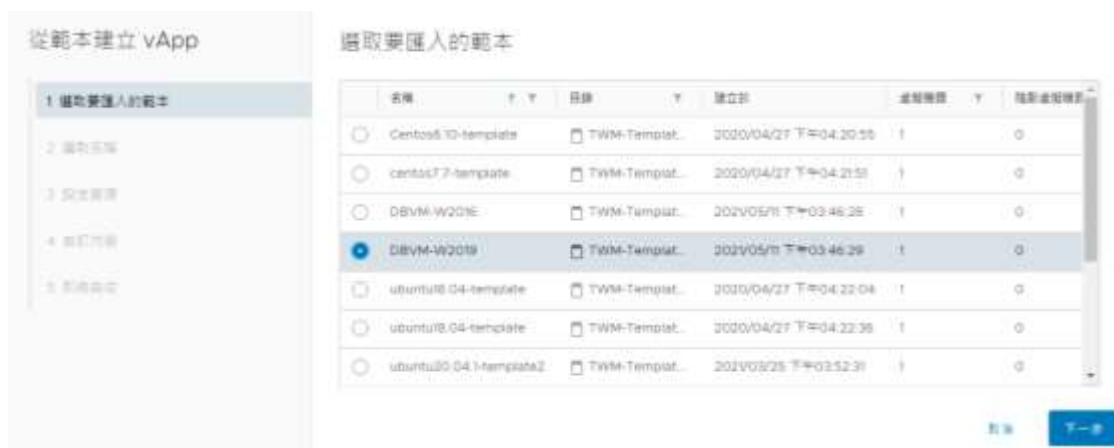
選擇 VDC



選擇從 catalog 新增 vapp



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



輸入名稱

從範本建立 vApp

1 獲取要導入的範本

2 獲取名稱

3 設定資源

4 設定原則

5 設定硬體

6 設定網路

7 設定內嵌

8 完成配置

獲取名稱

名稱 *

描述

執行策略規則

儲存策略規則

test062

永不刪滅 小機

永不刪滅 小機

此 vApp 移動停止以前，可以執行封裝策略。

此 vApp 在操作系統啟動後僅可使用的策略。

取消

上一步

下一步

如無調整請保持預設

從範本建立 vApp

1 獲取要導入的範本

2 獲取名稱

3 設定資源

4 設定原則

5 設定硬體

6 設定網路

7 設定內嵌

8 完成配置

設定資源

獲取你想讓此 vApp 的已部署虛擬機使用的儲存區原則。

名稱	儲存區原則	申請虛機儲存空間
DBVM-W2016	standard-policy	

取消

上一步

下一步

從範本建立 vApp

1 獲取要導入的範本

2 獲取名稱

3 設定資源

4 設定原則

5 設定硬體

6 設定網路

7 完成配置

運作原則

為每個虛機機器指定虛機機器資源和虛機機器大小調整原則。

虛機機器	↑ ↓	虛機機器資源原則	虛機機器大小調整原則
DBVM-W2016		無	System Default
計算			
虛機 CPU	4		
每個插槽的核心數	1		
插槽數目	4		

第 1 之 1 個虛機機器範本 - 共 1 個

取消

上一步

下一步



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

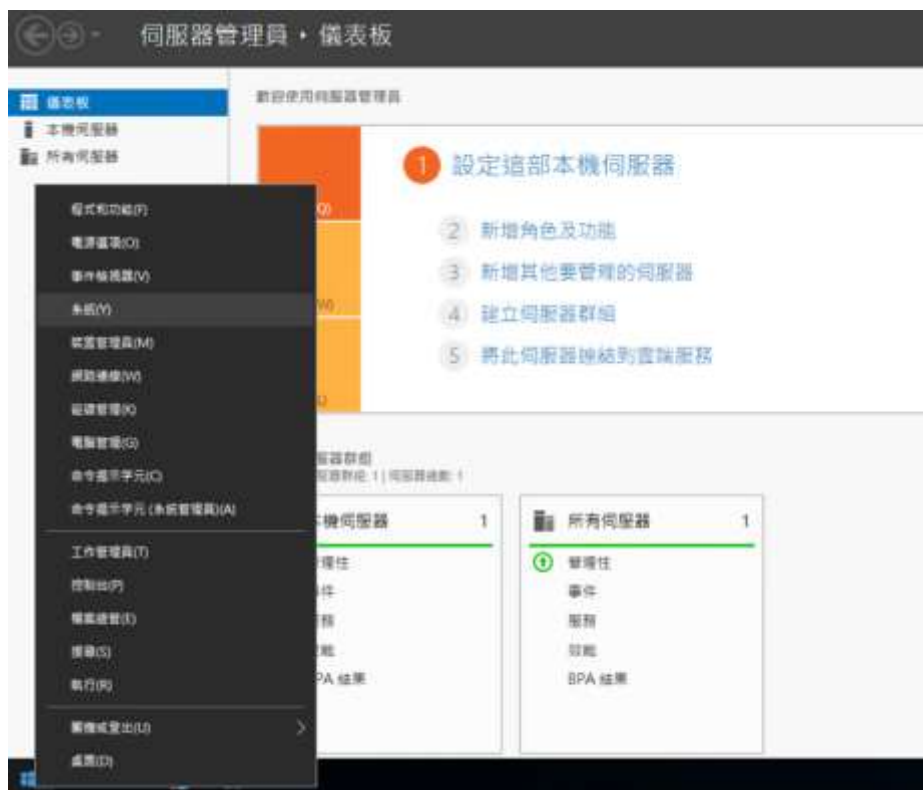


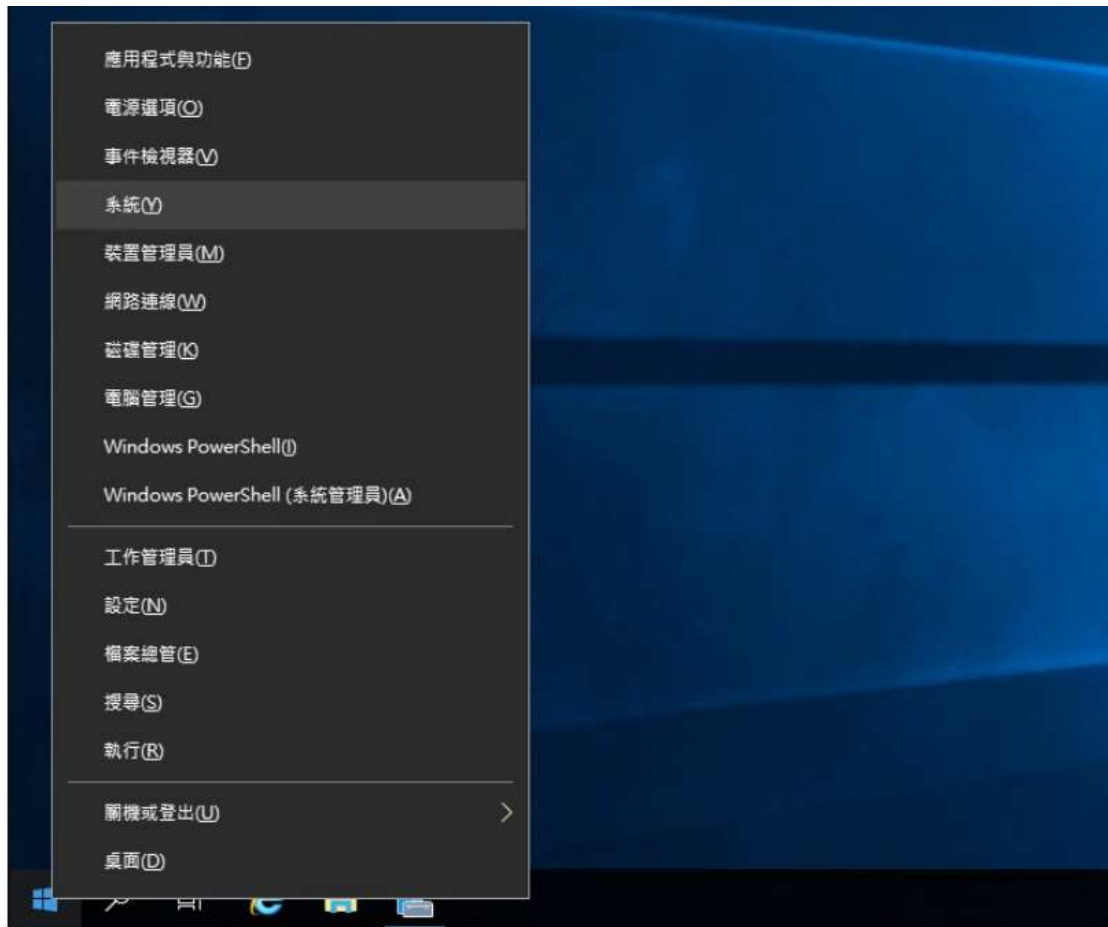
進行初始密碼設定





登入後滑鼠移到左下方按右鍵選擇系統



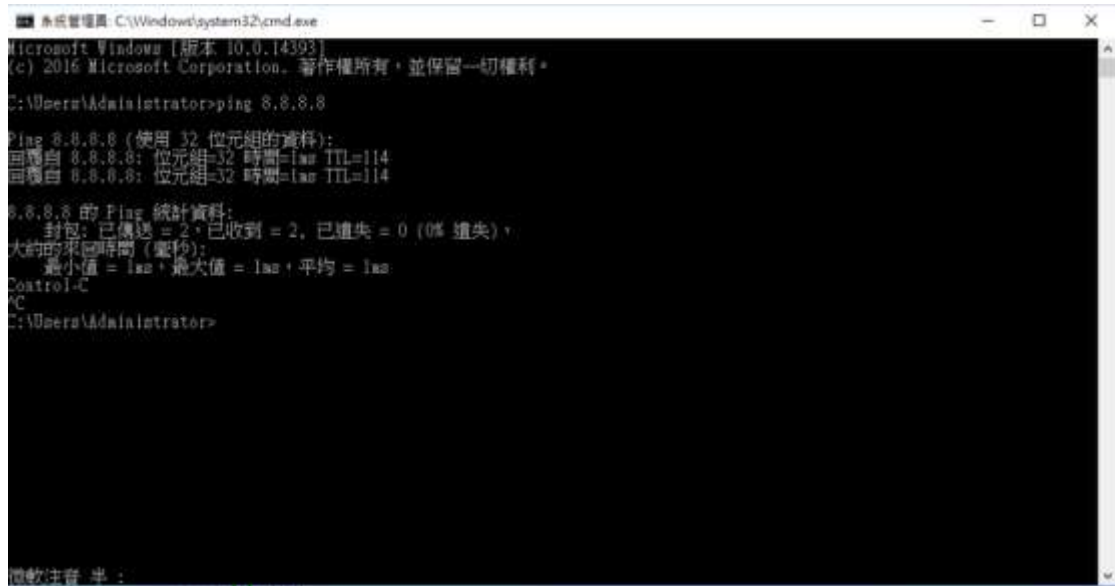


確認系統資訊/確認 Windows 已啟用





驗證 VM 對外連線正常⁷



```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Users\Administrator>ping 8.8.8.8

Ping 8.8.8.8 (使用 32 位元組的資料):
選擇自 8.8.8.8: 位元組=32 時間=1ms TTL=114
選擇自 8.8.8.8: 位元組=32 時間=1ms TTL=114

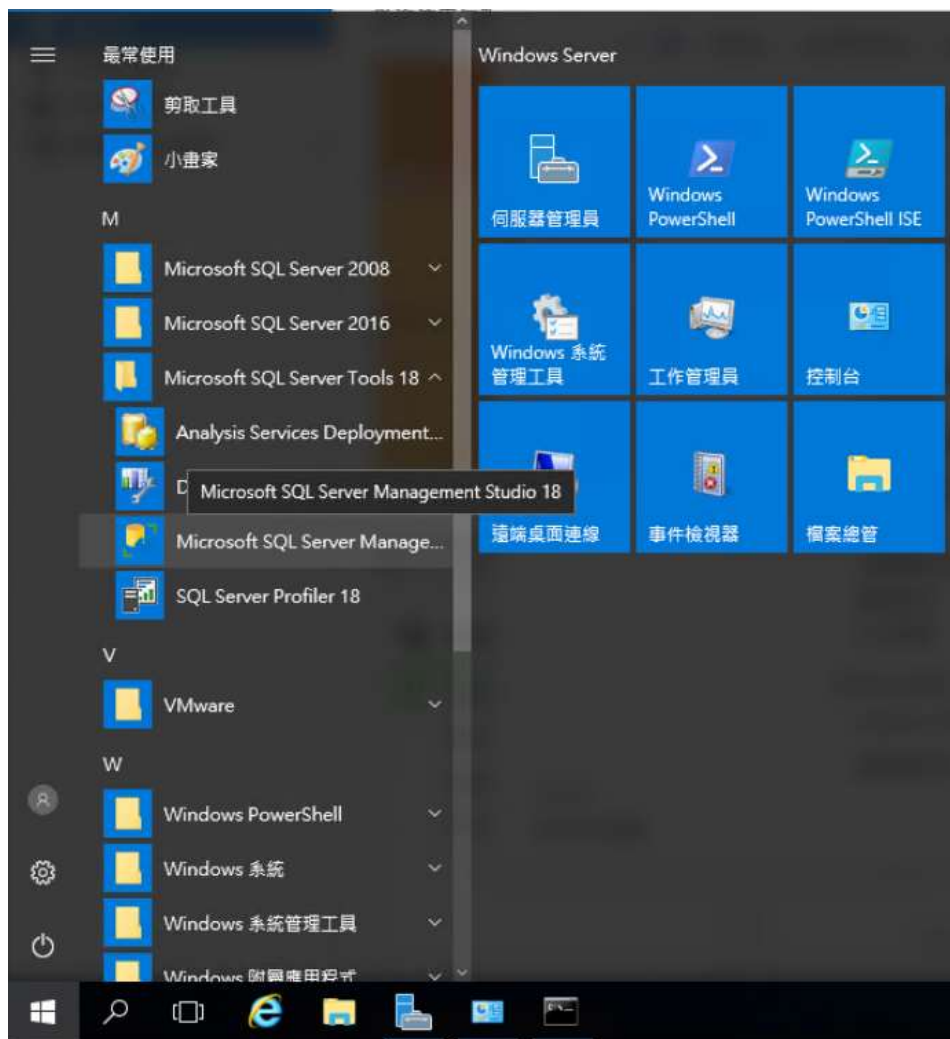
8.8.8.8 的 Ping 統計資料:
    封包: 已傳送 = 2, 已收到 = 2, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 1ms, 最大值 = 1ms, 平均 = 1ms
Control-C
^C
C:\Users\Administrator>
```

MSSQL DBVM 驗證程序說明

以下步驟驗證 DBVM 2016/2019 功能

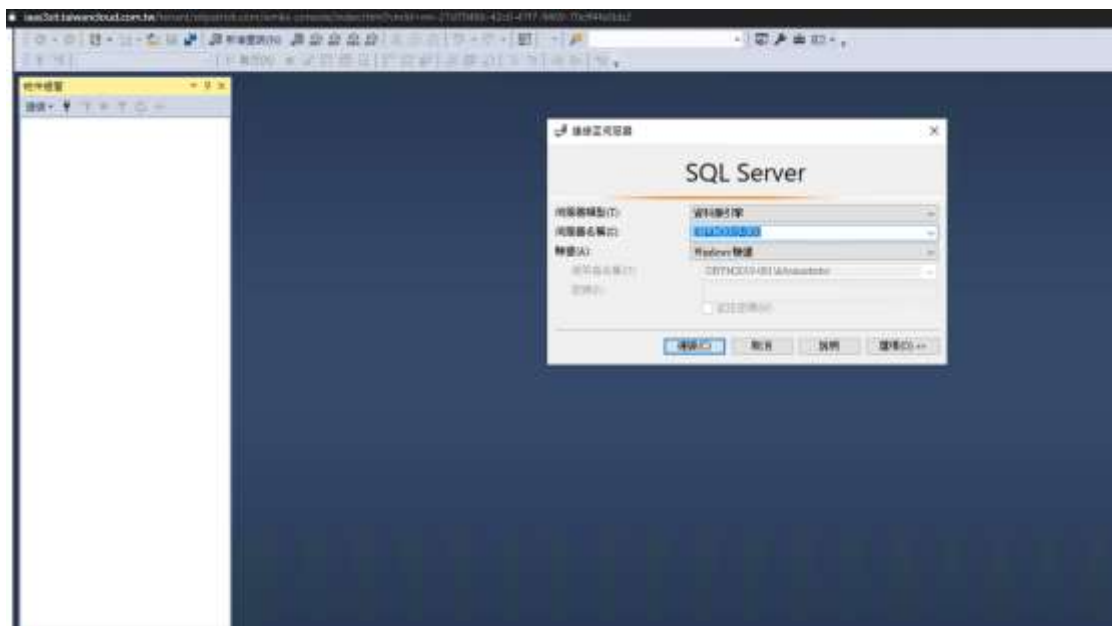
開啟 MSSQL 管理工具

⁷ 以上驗證登入與網路設定若成功,代表客體自訂成功

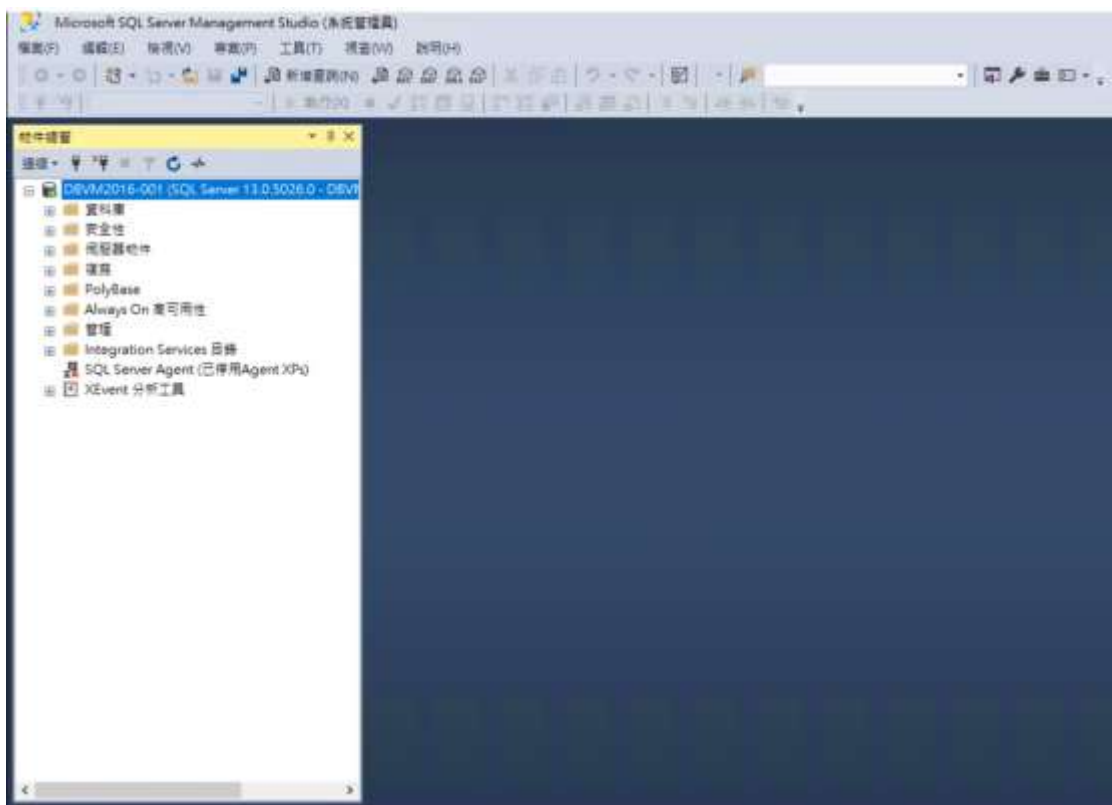


點選連線

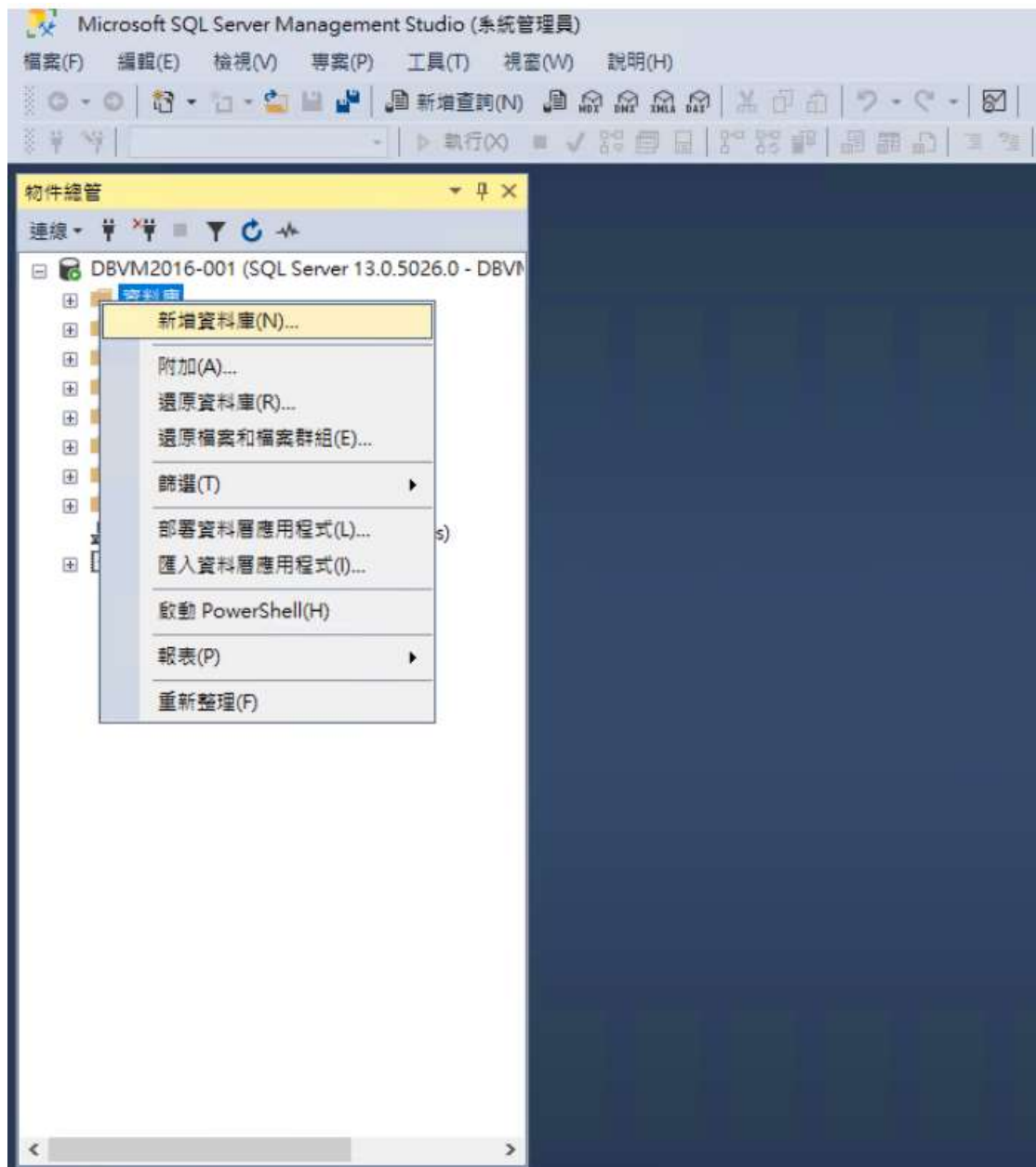




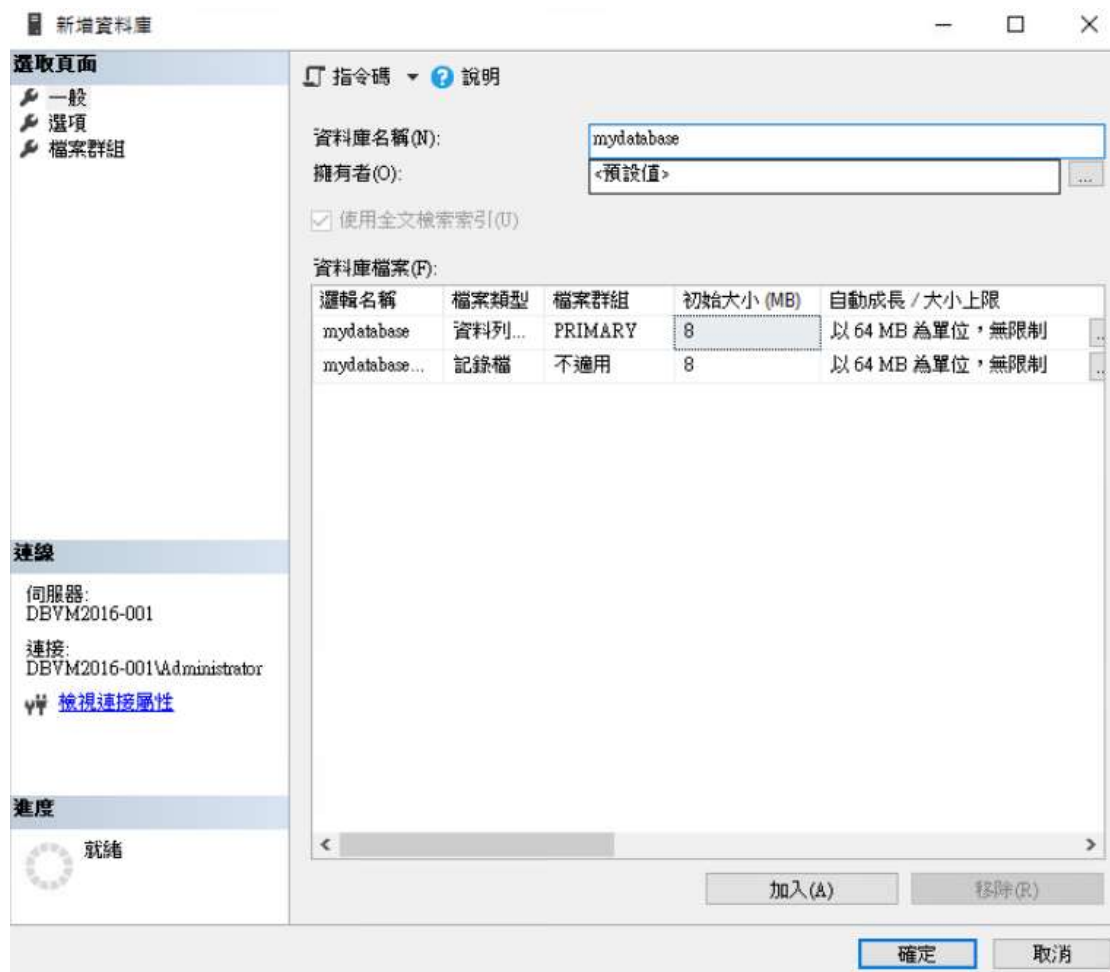
沒有錯誤訊息代表登入成功



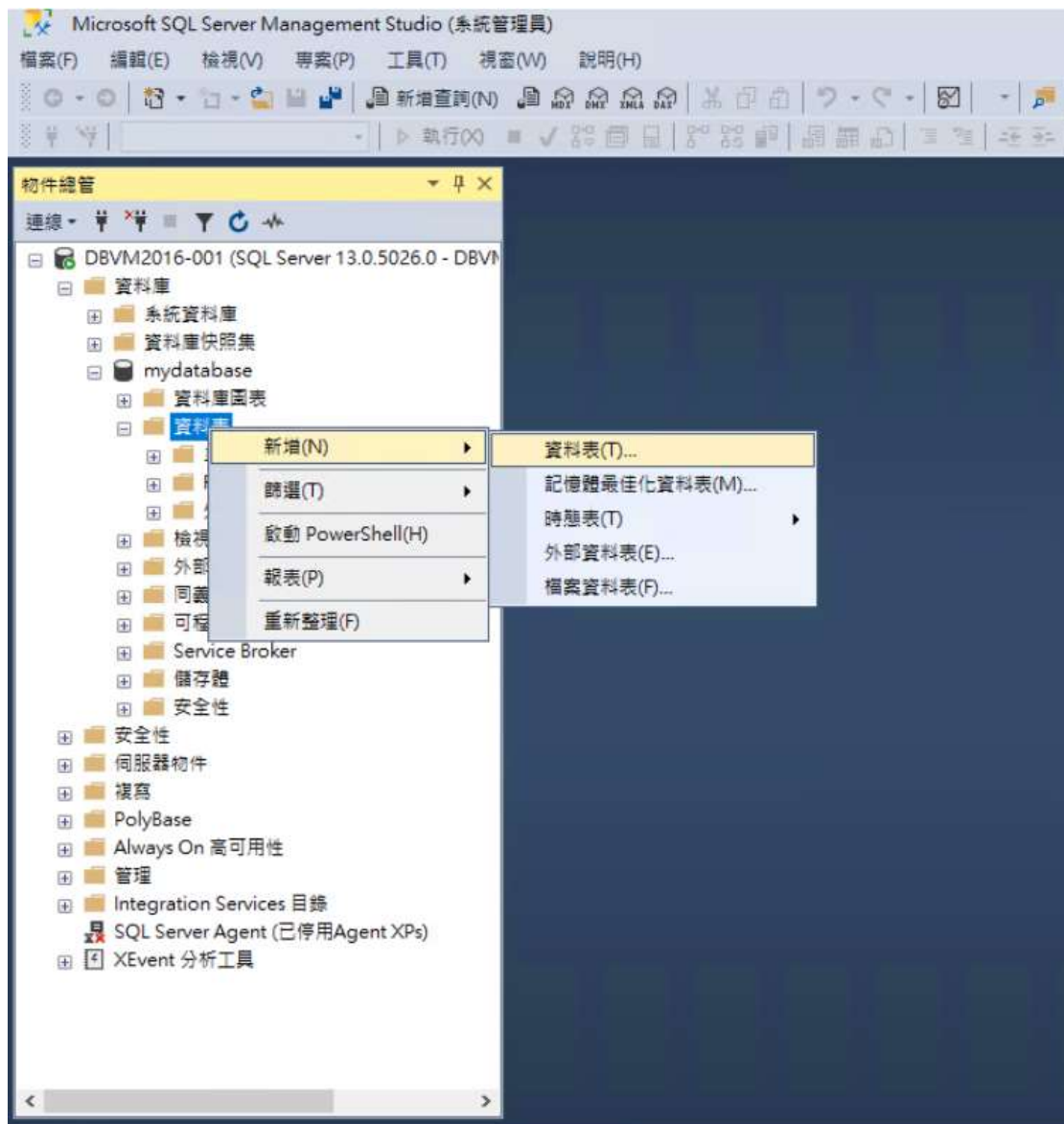
新增資料庫



輸入資料庫名稱後按確定

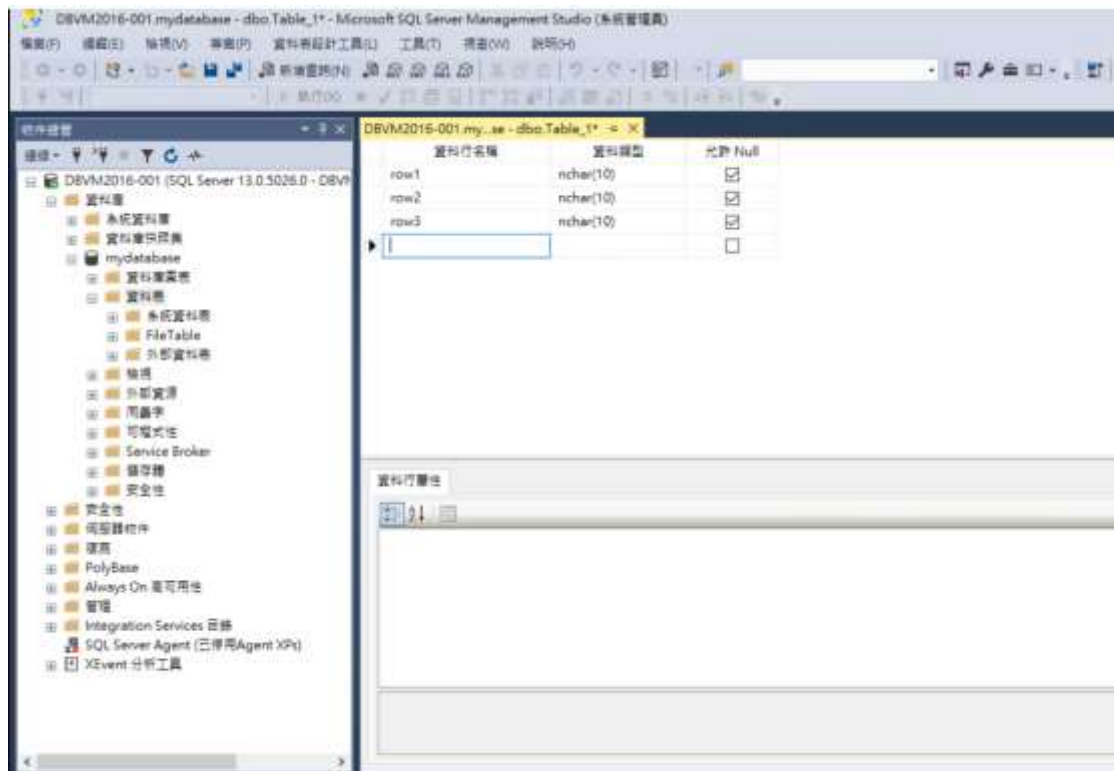


點選剛建立的資料庫/資料表/按右鍵選擇新增資料表

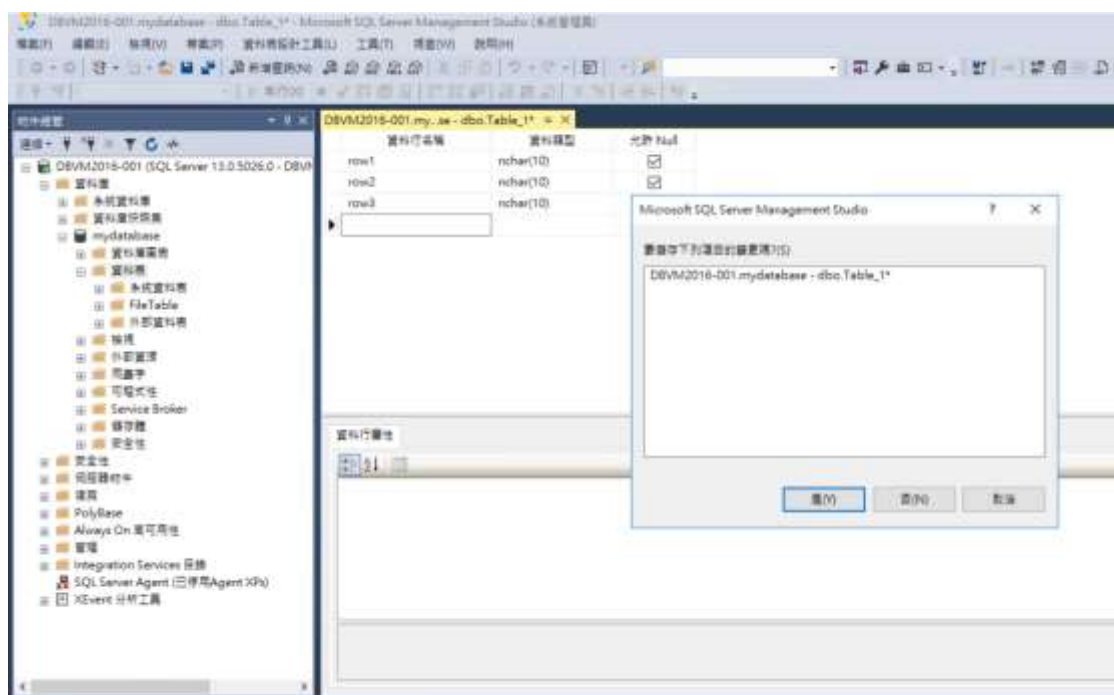


新增三個欄位

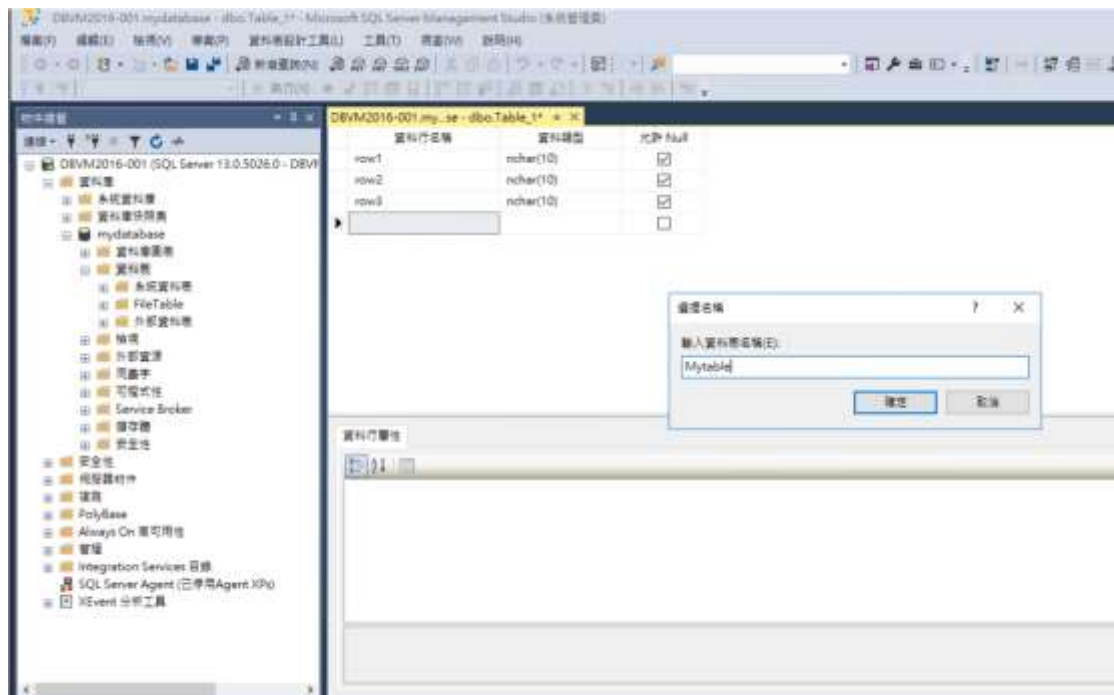
台灣大哥大運算雲 3.0 服務操作手冊



點選 X 選擇是儲存資料表



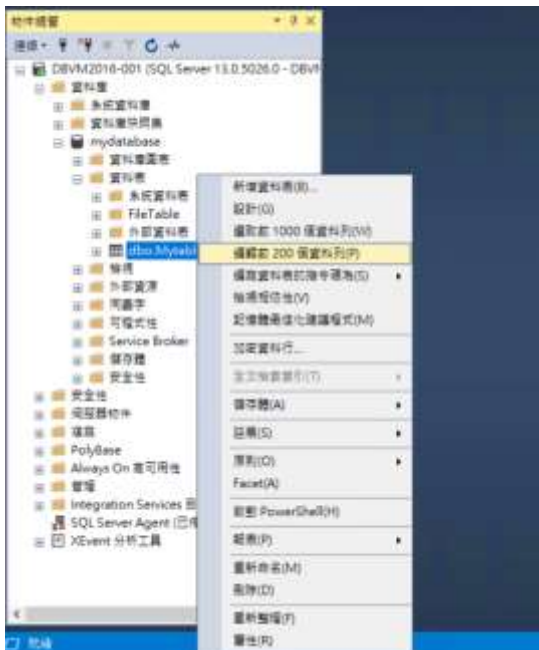
輸入資料表名稱



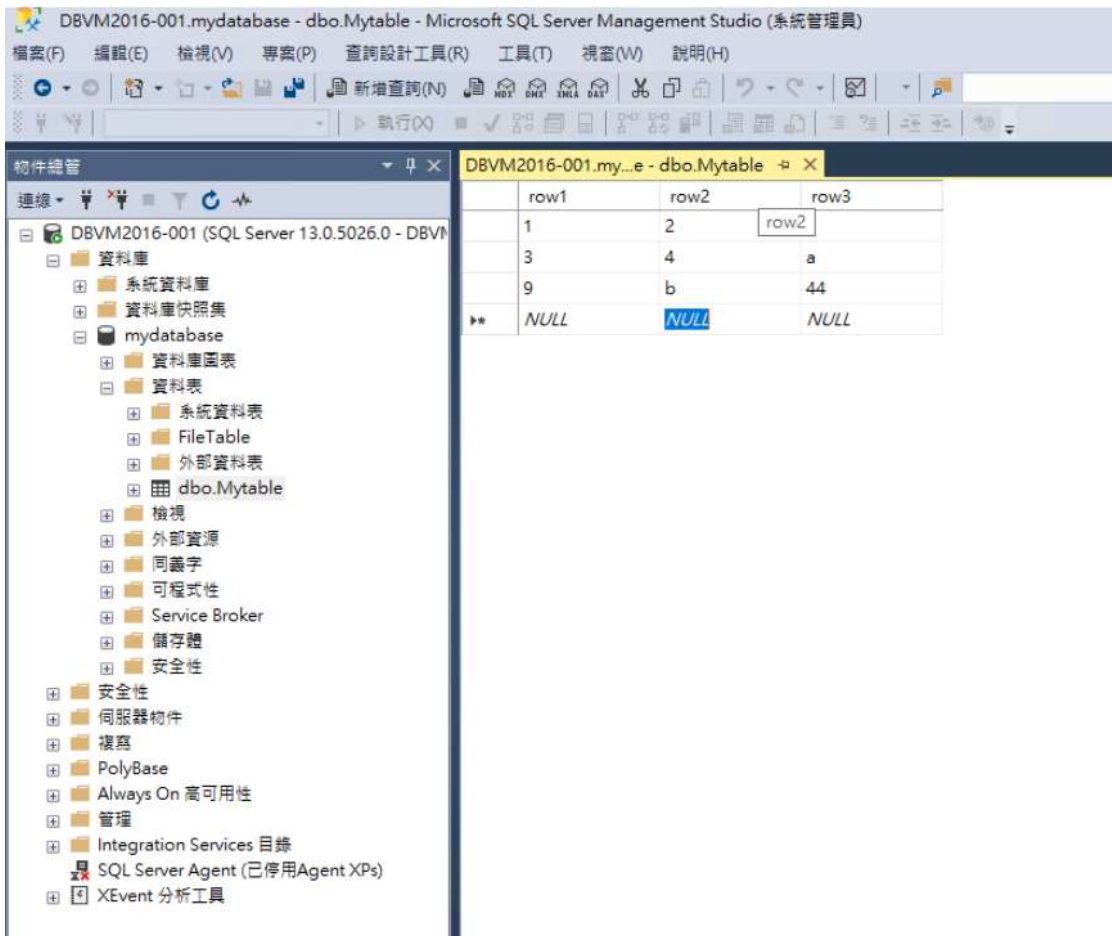
重新整理資料表



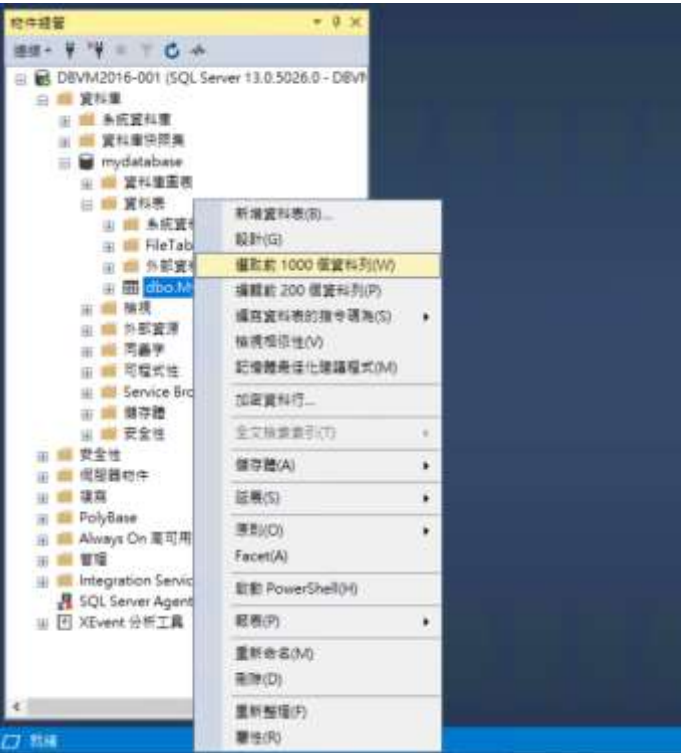
在剛建立的資料表上新增資料



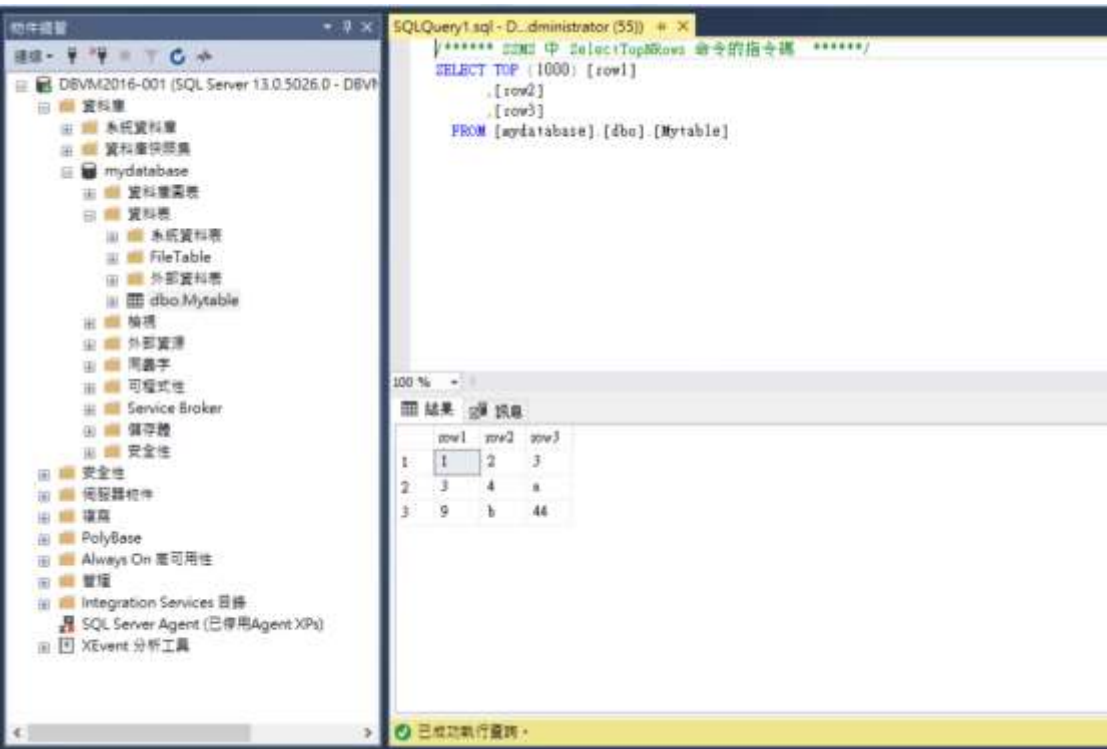
任意輸入資料後按 X 結束



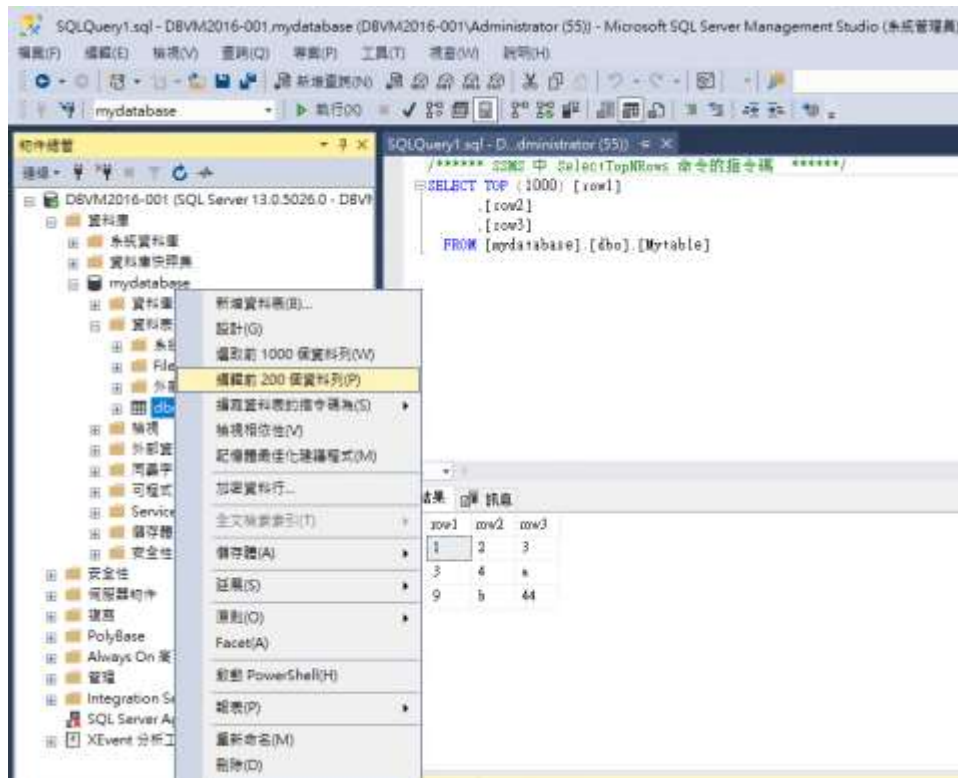
查詢資料表



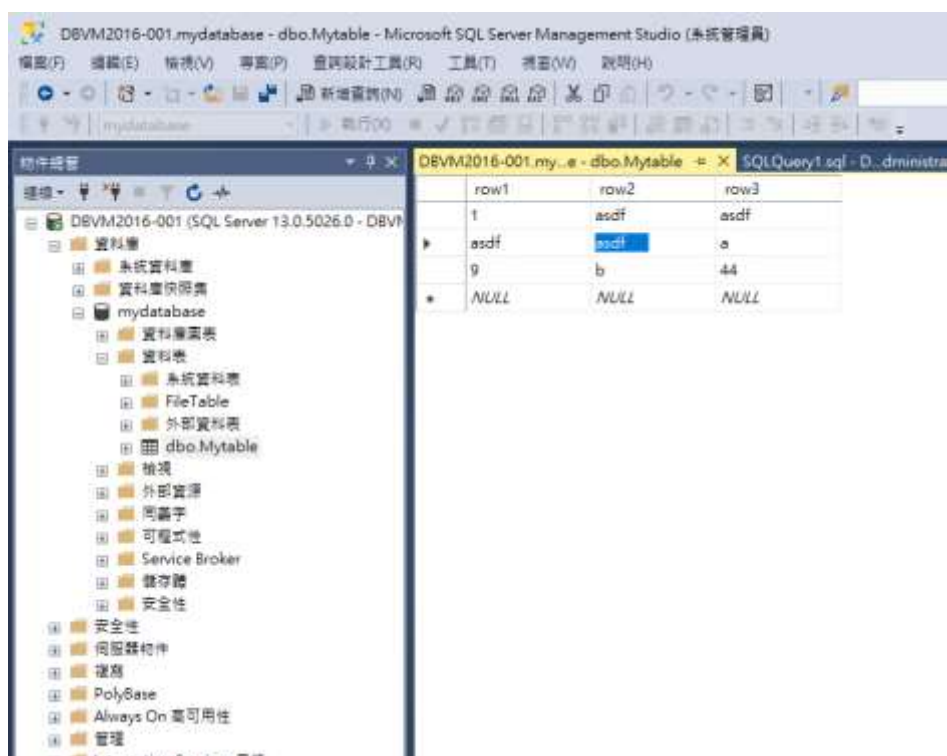
確認剛輸入的資料有顯示出來



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



The screenshot displays the VMware Cloud Director web interface. The left sidebar contains a navigation menu with categories like '計算' (Compute), '網路' (Network), '儲存區' (Storage), and '設定' (Settings). The '虛擬機器' (Virtual Machine) option is highlighted with a red box. The main content area shows the details for a specific VM named 'vcpp-centos7-1810-v2'. The VM is currently powered off. A table lists its specifications: 1 CPU, 18 GB storage, 2 GB memory, and network connectivity. At the bottom of the VM details, the '動作' (Actions) menu is visible, and the '詳細資訊' (Details) option is highlighted with a red box.

項目	值
租用	永不到期
建立於	2020/12/01 下午03:36:13
擁有者	admin
vApp	ERP-vApp
作業系統	CentOS 7 (64-bit)

圖示	名稱	值
CPU	CPU	1
儲存區	儲存區	18 GB
記憶體	記憶體	2 GB
網路	網路	①

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。

vcpp-centos7-1810-v2 動作 =	
一般	編輯
硬體	
卸除式媒體	
硬碟	
計算	
NIC	
客體作業系統自訂	
客體內容	
中繼資料	
監視器	
工作	
事件	
名稱	vcpp-centos7-1810-v2
狀態	已離開電源
電腦名稱	vcpp-centos7-1810-v2-001
說明	*
作業系統	CentOS 7 (64-bit)
開機延遲	0
儲存區策略	VCD-StoragePolicy
虛擬資料中心	taiwanmobile.com-VDC
擁有者	admin
VMware Tools	10304
虛擬硬體版本	硬體版本 13
vApp	ERP-vApp
進入 BIOS 設定	已停用

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。

vcpp-centos7-1810-v2

動作 ▾

一般

硬體

卸除式媒體

硬碟

計算

NIC

客體作業系統自訂

客體內容

中繼資料

監視器

工作

事件

編輯

一般

啟用客體自訂

已啟用

變更 SID

已停用

密碼重設

允許本機管理員密碼

已啟用

管理員在初次登入時需變更密碼

已停用

自動產生密碼

已啟用

自動登入的次數

0

加入網域

啟用此虛擬機器以加入網域

已停用

覆寫組織的網域

已啟用

指令碼

指令碼檔案

-

編輯客體內容

一般

☒ 啟用客體自訂

當虛擬機器開啟電源後，為此虛擬機器設定的電腦名稱和網路設定會套用至其客體作業系統。僅在虛擬機器第一次開啟電源或在執行「開啟電源並強制重新自訂」時，才會套用下列設定：變更 SID、密碼重設、加入網域和自訂指令碼。若虛擬機器使用客體內容進行自訂，不應啟用客體自訂。

☐ 變更 SID

適用於 Windows 虛擬機器，將執行 Sysprep 以變更 Windows SID。在 Windows NT 上，VMware Cloud Director 使用 Sidgen。執行 sysprep 是完成網域加入的必要條件。

密碼重設

☐ 允許本機管理員密碼

☐ 管理員在初次登入時需變更密碼

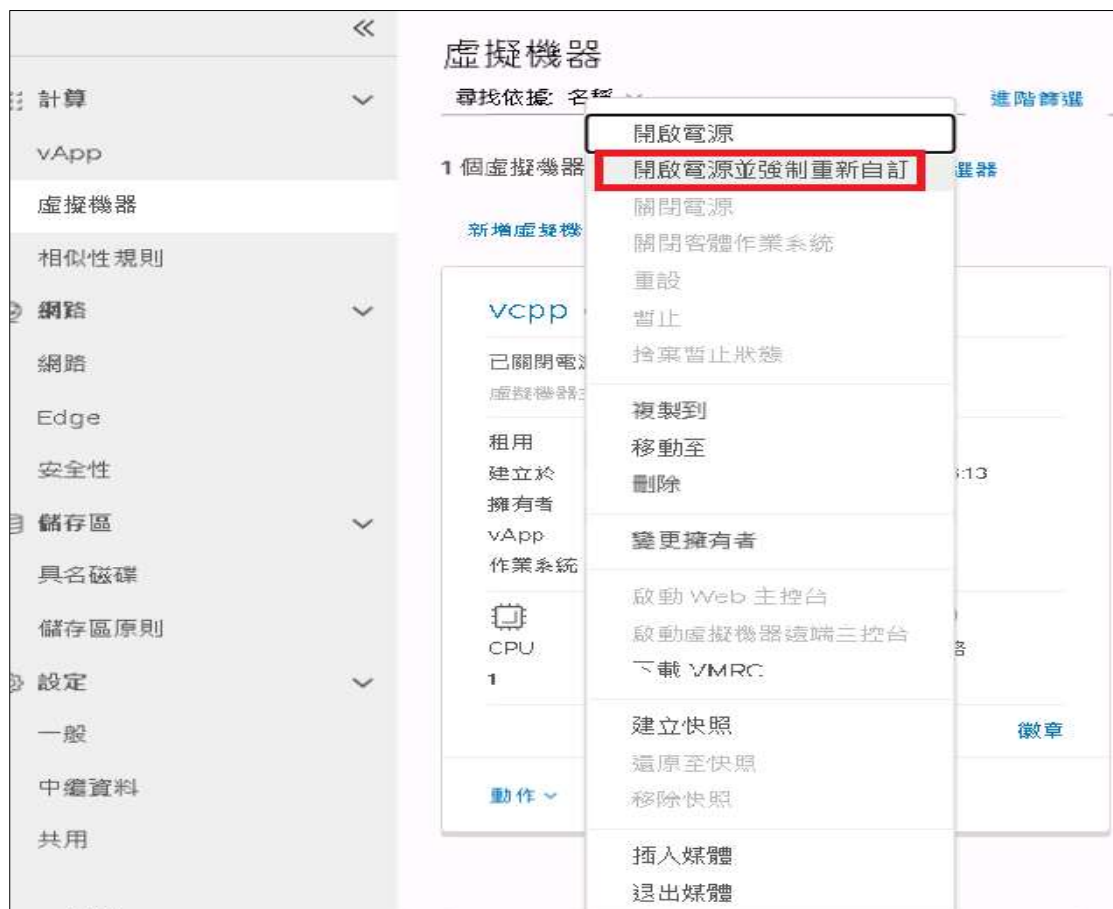
☒ 自動產生密碼

指定密碼

%4vY\$%f!

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)



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



The screenshot shows the configuration interface for a VM named 'vcpp-centos7-1810-v2'. The left sidebar contains a navigation menu with options: 一般, 硬體 (with sub-items 卸除式媒體 and 硬碟), 計算 (highlighted), NIC, 客體作業系統自訂, 客體內容, 中繼資料, 監視器 (with sub-items 工作 and 事件). The main content area is titled '編輯' and contains two sections: 'CPU' and '記憶體'. The 'CPU' section has a table with the following data:

CPU	
虛擬 CPU 數目	1
每個插槽的核心數	1
插槽數目	1
虛擬 CPU 熱新增	已停用
向客體作業系統公開硬體輔助的 CPU 虛擬化	已停用

The '記憶體' section has a table with the following data:

記憶體	
記憶體	2 GB
記憶體熱新增	已停用

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 CPU 詳細資料

虛擬 CPU

1

▼

每個插槽的核心數

1

▼

虛擬 CPU 熱新增

☒

向客體作業系統公開硬體輔助的
CPU 虛擬化

☐

捨棄

儲存

編輯記憶體詳細資料

記憶體

2

GB ▼

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



主要 NIC	NIC	已連線	網路介面卡類型	網路	IP 模式	IP 位址	外部 IP 位址	MAC 位址
是	0	已連線	VMXNET3	taiwanmobile-com.NET	靜態-IP集區	192.168.0.1	-	00:50:56:00:00:70

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 VCDNetwork。

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。

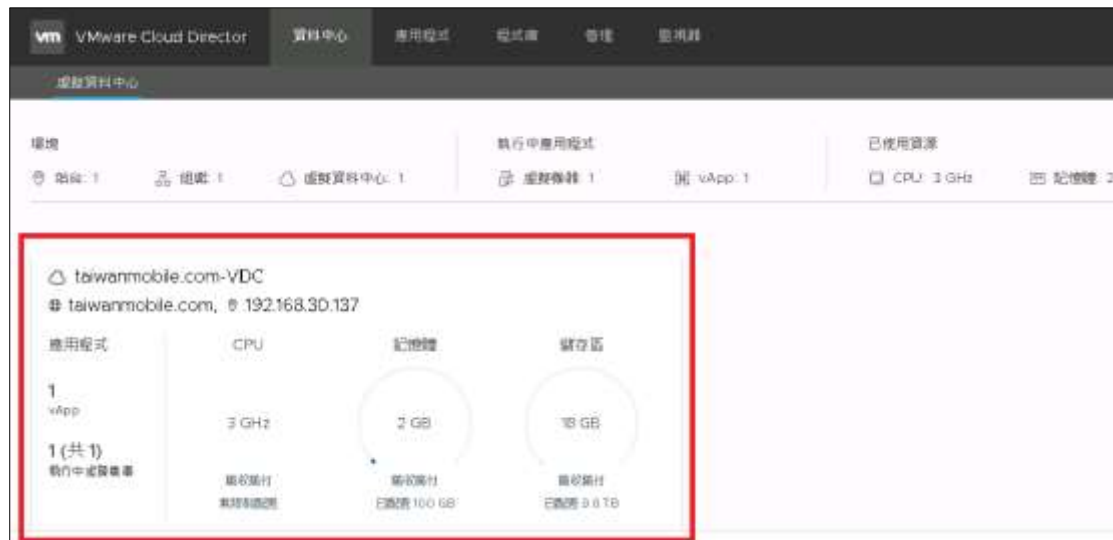
請參閱[附件 A.《Windows Server 檔案與磁碟加密》](#)

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。

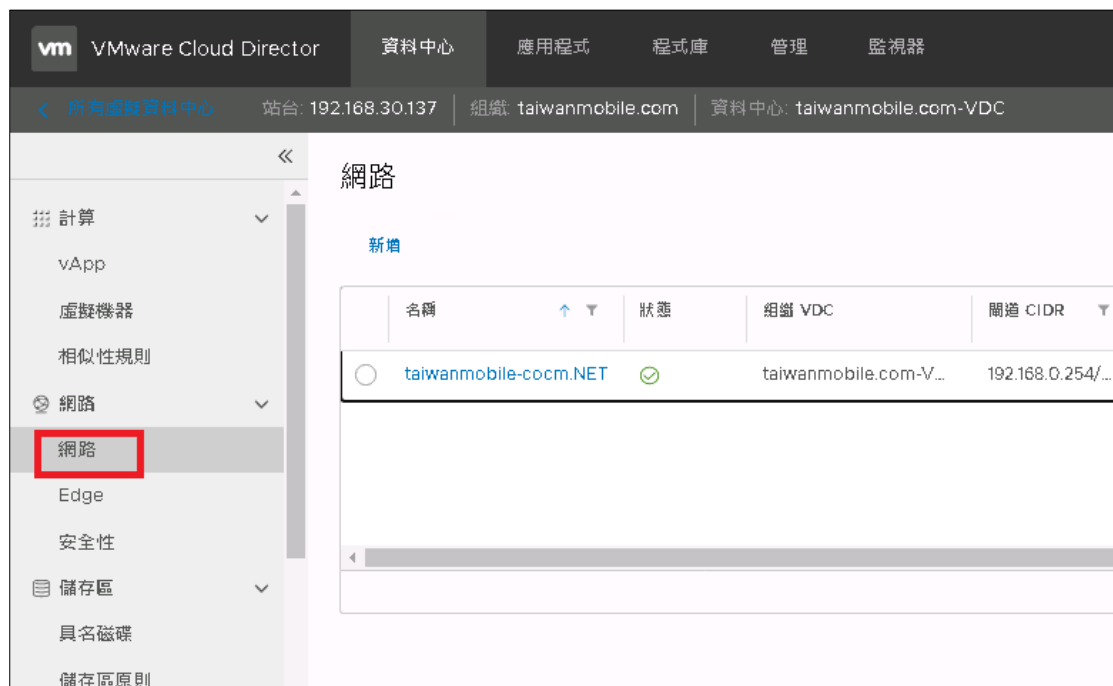
請參閱附件 [B.《Linux 磁碟加密說明》: 以 CentOS 為製作範例](#)

9. 設定組織虛擬資料中心網路(VDCNetwork)

首頁→點擊 OVDC

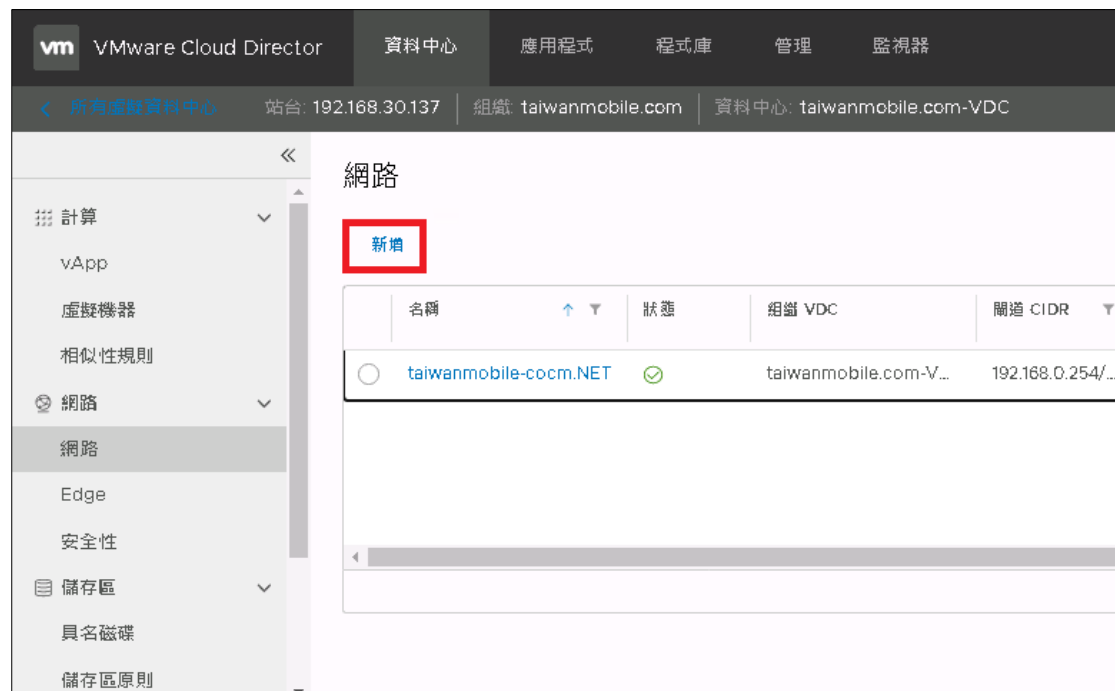


到此就可開始設定虛擬資料中心網路



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

新增組織 VDC 網路

- 網路類型
- 一般
- Edge 連線
- 靜態 IP 集區
- DNS
- 即將完成

網路類型

選取您要建立的網路類型

☐ 已隔離
此類型的網路提供完全隔離的環境，只有此組織 VDC 可存取此環境。

☒ 已路由
此類型的網路透過 Edge 閘道提供對 VDC 外部之機器和網路的控制存取權

取消 下一步

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

新增組織 VDC 網路

1 網路類型

2 一般

3 Edge 連線

4 靜態 IP 集區

5 DNS

6 即將完成

一般

名稱 * ERP-Network

閘道 CIDR * 192.168.2.254/24 ⓘ

說明

For ERP Use

共用 ☐ ⓘ

取消

上一步

下一步

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”

新增組織 VDC 網路

1 網路類型

2 一般

3 Edge 連線

4 靜態 IP 集區

5 DNS

6 即將完成

Edge 連線

名稱	外部網路	組織 VDC 網路
 taiwanmobile-com-EDGE	1	1

第1-1個 Edge 閘道，共1個

介面類型 內部 ⓘ

允許的客體 VLAN ☐

取消

上一步

下一步

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



新增組織 VDC 網路

- 1 網路類型
- 2 一般
- 3 Edge 連線
- 4 靜態 IP 集區**
- 5 DNS
- 6 即將完成

靜態 IP 集區

開道 CIDR ⓘ

靜態 IP 集區
輸入 IP 範圍 (格式: 192.168.1.2 - 192.168.1.100)

IP 位址總計: 0

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。

新增組織 VDC 網路

1 網路類型

2 一般

3 Edge 連線

4 靜態 IP 集區

5 DNS

6 即將完成

DNS

使用 Edge DNS

☒

選取此選項以使用開道的 DNS 轉送。DNS 轉送必須在開道上預先設定。

主要 DNS

192.168.2.254

次要 DNS

61.31.1.1

DNS 尾碼

取消

上一步

下一步

最後再次檢查設定，到此就新增 VDCNetwork 完成。

新增組織 VDC 網路

1 網路類型

2 一般

3 Edge 連線

4 靜態 IP 集區

5 DNS

6 即將完成

即將完成

您即將建立一個具備這些規格的組織 VDC 網路。請檢閱設定，然後按一下 [完成]。

名稱	ERP-Network
說明	For ERP Use
共用	否
開道 CIDR	192.168.2.254/24
網路類型	已路由
連線	taiwanmobile-com-EDGE
連線類型	內部
允許的客體 VLAN	否
主要 DNS	192.168.2.254
次要 DNS	61.31.1.1
DNS 尾碼	-

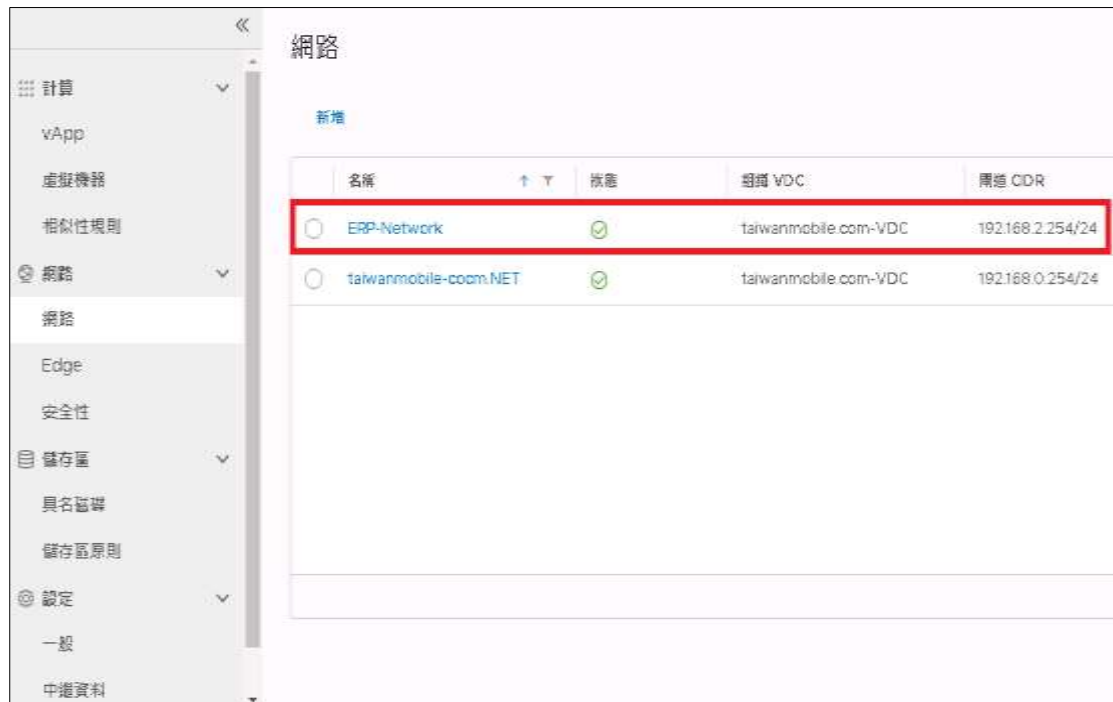
取消

上一步

完成

回到網路頁面，會看到方才新增的設定。

第94頁



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

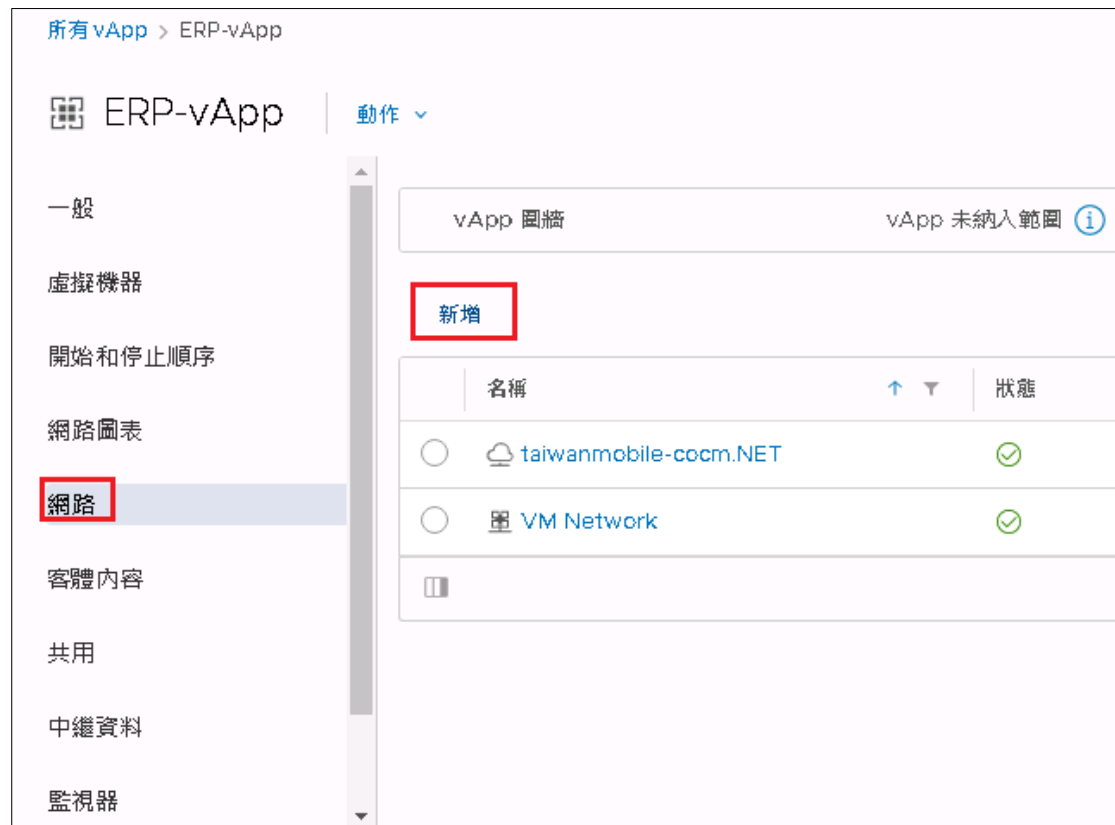
套用的 vApp 選擇詳細資訊



VMware Cloud Director 管理介面顯示了「ERP-vApp」的詳細資訊。介面包含搜尋欄、篩選器、以及資源配置表。在配置表中，「網路」欄位的值「2」被圈出，表示需要新增網路資源。

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



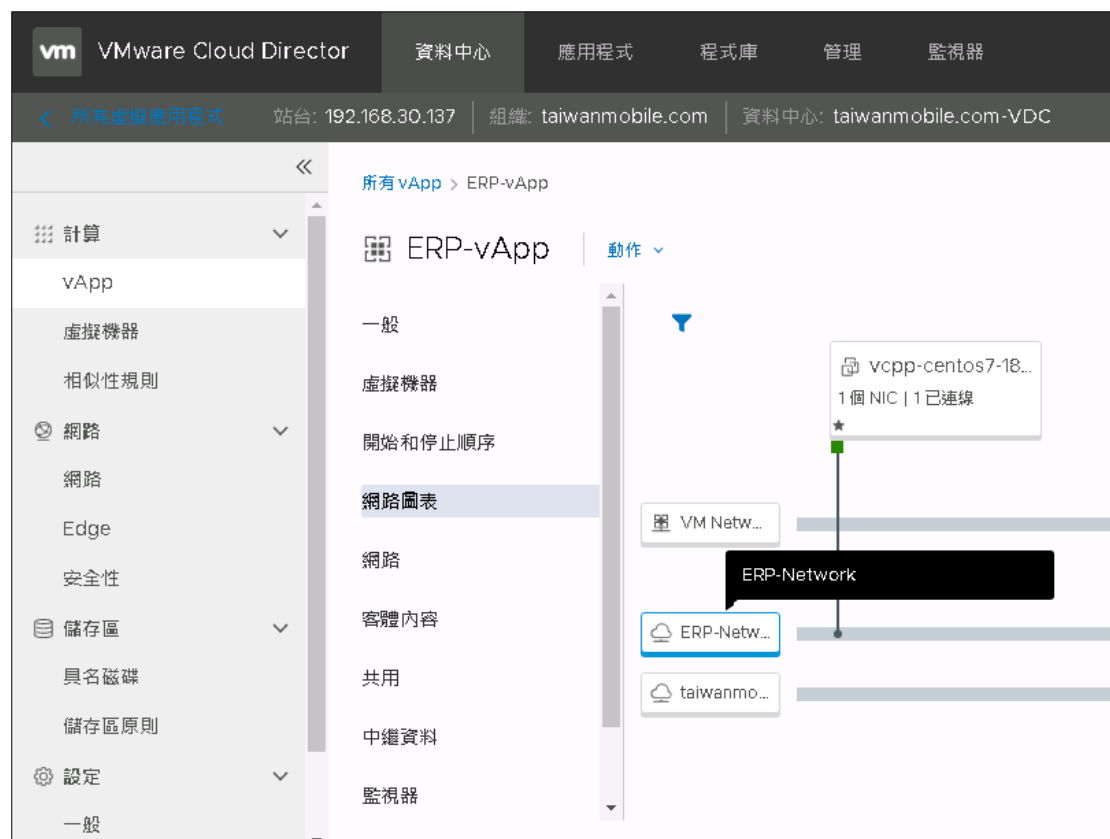
選擇組織 VDC 網路→選擇 ERP-Network→點選新增



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



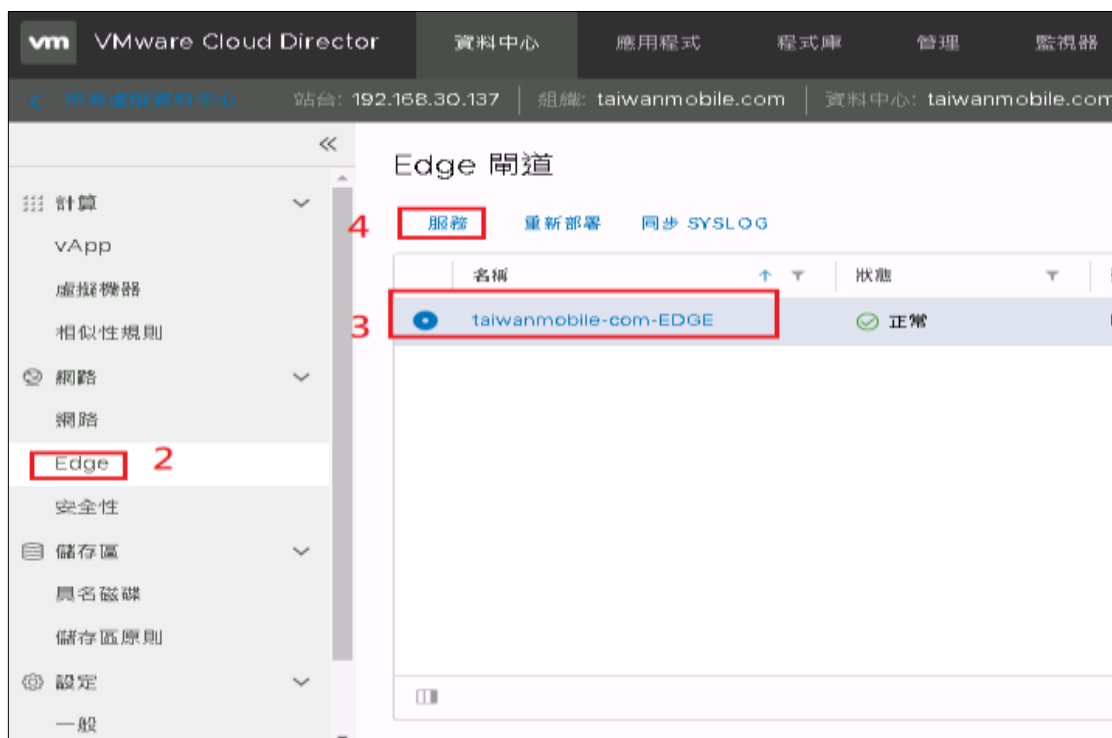
在 vApp 裡的網路圖表，可以很清楚看到 VM 套用了那些網路。



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。



Edge 閘道 - taiwanmobile-com-EDGE

防火牆 DHCP NAT 路由 負載平衡器 VPN 憑證 群組物件 統計資料 Edge 設定

NAT44 規則

新增 NAT 規則 刪除 NAT 規則 保存 取消

選擇使用這些 NAT 規則的 VM

源 IP 地址	類型	動作	目標 IP 地址	已翻譯 IP 地址	通訊類型	已啟用	記錄	說明
192.168.10.1	DMZ	192.168.10.1	192.168.10.1	192.168.10.1	192.168.10.1	✓	■	VM 使用 192.168.10.1 作為 192.168.10.1
192.168.10.2	DMZ	192.168.10.2	192.168.10.2	192.168.10.2	192.168.10.2	✓	■	
192.168.10.3	DMZ	192.168.10.3	192.168.10.3	192.168.10.3	192.168.10.3	✓	■	
192.168.10.4	DMZ	192.168.10.4	192.168.10.4	192.168.10.4	192.168.10.4	✓	■	
192.168.10.5	DMZ	192.168.10.5	192.168.10.5	192.168.10.5	192.168.10.5	✓	■	

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。

Edge 閘道 - default-gw

防火牆 DHCP NAT 路由 負載平衡器 VPN 憑證 群組物件 統計資料 Edge 設定

集區 繫結 轉送

DHCP 集區

DHCP 服務狀態 ☒

新增 編輯 刪除

IP 範圍 主要名稱伺服器 自動設定 DNS 預設網段 租用時間 (秒)

192.168.100.101-192.168.100.150	192.168.100.53	☐	192.168.100.254	86400
---------------------------------	----------------	--------------------------	-----------------	-------

編輯 DHCP 集區

IP 範圍 *

192.168.100.101-192.168.

網域名稱

自動設定 DNS

☐

主要名稱伺服器

192.168.100.53

次要名稱伺服器

61.31.1.1

預設閘道

192.168.100.254

子網路遮罩

255.255.255.0

租用永不到期

☐

租用時間 (秒)

86400

捨棄

保留

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。

Edge 閘道 - default-gw

防火牆 DHCP NAT 路由 **負載平衡器** VPN 憑證 群組物件 統計資料 Edge 設定

全域組態 應用程式設定檔 服務監視 **集區** 應用程式規則 **虛擬伺服器**

全域組態

狀態 **已啟用** ☒

已啟用加速 ☐

啟用記錄 已停用 ☐

記錄層級 資訊 ▾

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。

Edge 閘道 - default-gw

防火牆 DHCP NAT 路由 **負載平衡器** VPN 憑證 群組物件 統計資料 Edge 設定

全域組態 應用程式設定檔 服務監視 **集區** 應用程式規則 虛擬伺服器

集區

[+](#) [✎](#) [✕](#) [顯示集區統計資料](#)

集區識別碼	名稱	演算法	監視器識別碼
pool-8	ERP-Pool	round-robin	

集區 ERP-Pool 詳細資料

已啟用	名稱	IP 位址	權重	監視器...	連接埠	連線數下限	連線數上限
☒	ERP-Portal01	10.100.200.2	1	80	80	0	0
☒	ERP-Portal02	10.100.200.3	1	80	80	0	0

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。

Edge 閘道 - default-gw

防火牆 DHCP NAT 路由 **負載平衡器** VPN 憑證 群組物件 統計資料 Edge 設定

全域組態 應用程式設定檔 服務監視 集區 應用程式規則 **虛擬伺服器**

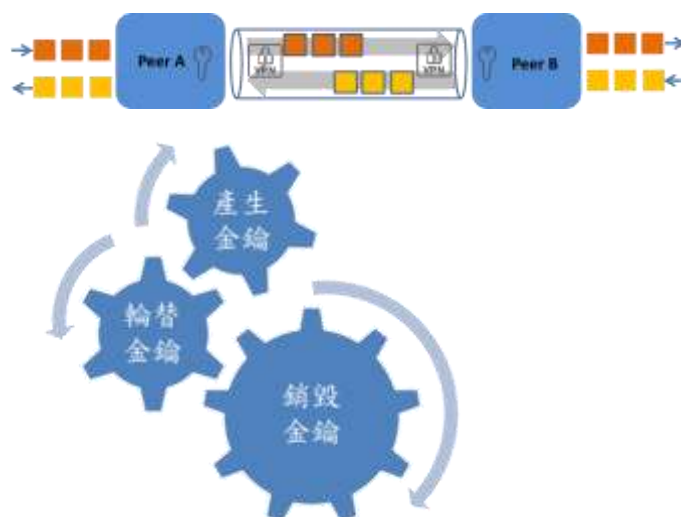
虛擬伺服器

+ ✎ ✕ ↺

虛擬伺服器...	名稱	說明	預設集區	IP 位址	通訊協定	連接埠
virtualServer-1	ERP-LoadBalance		pool-8	60.199.153.5	http	80

IPSec VPN

金鑰生命週期說明



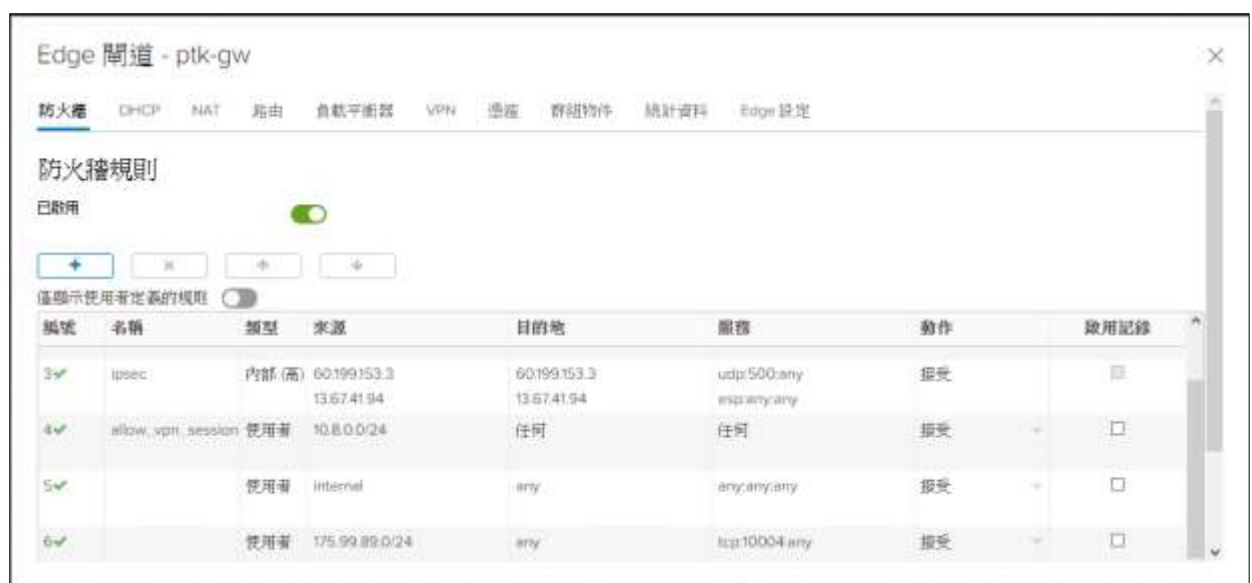
- 產生金鑰: 設定預先共用金鑰(PSK)、金鑰演算法(例:SHA1)、金鑰交換演算法(例:Diffie-Hellman)，系統產生加密金鑰。
- 輪替金鑰: 系統於固定時間(lifetime)自動進行金鑰輪替。

- 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

編輯 IPsec VPN

已啟用

☒

啟用完整轉寄密碼 (PFS)

☒

名稱

vcpp_ptk

本機識別碼 *

60.199.153.3

本機端點 *

60.199.153.3

選取

本機子網路 *

10.100.0.0/24

子網路應以 CIDR 格式輸入 (以逗號做為分隔符號)。

對等識別碼 *

13.67.41.94

對等端點 *

13.67.41.94

端點應為有效的 IP、FQDN 或 any。

對等子網路 *

10.8.0.0/24

捨棄

保留

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

子網路應以 CIDR 格式輸入 (以逗號做為分隔符號)。

延伸

延伸可以是 `passthroughSubnets=192.168.1.0/24, 192.168.2.0`

加密演算法 AES

驗證 PSK

變更共用金鑰 ☐

預先共用金鑰

顯示共用金鑰 ☐

全域預先共用金鑰 (PSK) 由對等端點設定為 [任何] 的所有站台共用。如果全域 PSK 已設定，將 PSK 變更為空白值並儲存對現有設定沒有影響。

Diffie-Hellman 群組 DH2

< >

捨棄 保留

4. Session Type 選擇 Policy Base session

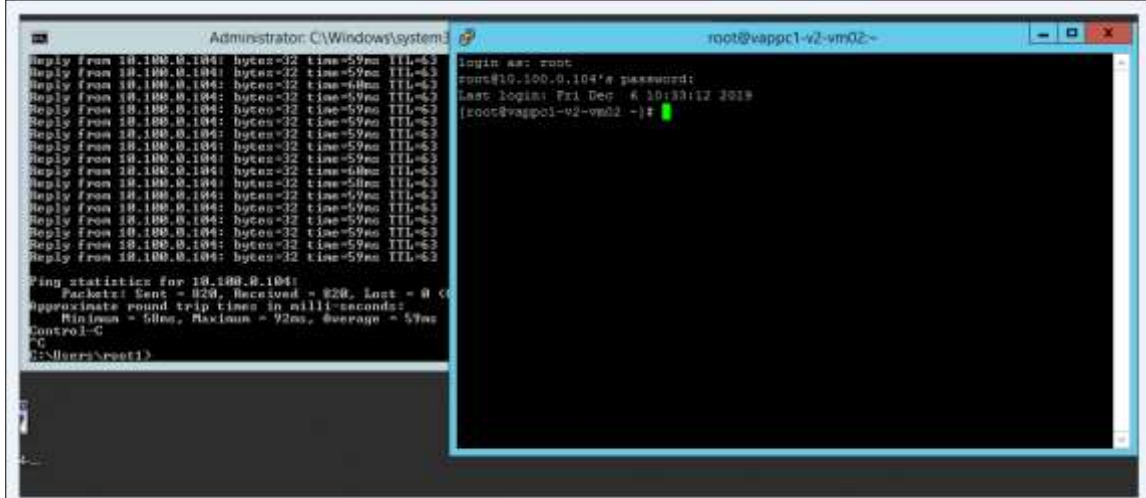
全域預先共用金鑰 (PSK) 由對等端點設定為 [任何] 的所有站台共用。如果全域 PSK 已設定，將 PSK 變更為空白值並儲存對現有設定沒有影響。

Diffie-Hellman 群組	DH2 ▾
Digest Algorithm	SHA1 ▾
IKE Option	IKEv2 ▾
IKE Responder Only	☐
Session Type	Policy Based Session ▾

捨棄 保留

5. 驗證兩端點可互通(Guest OS 的防火牆也必須搭配開通服務)

```
[root@vappc1-v2-vm02 tmp]# telnet 10.8.0.4 3389
Trying 10.8.0.4...
Connected to 10.8.0.4.
Escape character is '^'.
^]
telnet> quit
Connection closed.
[root@vappc1-v2-vm02 tmp]#
```



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。

新增組織 VDC 網路

1 範圍

2 網路類型

3 Edge 連線

4 一般

5 靜態 IP 集區

6 DNS

7 即將完成

範圍

☒ 目前組織虛擬資料中心

僅針對目前 VDC 中的虛擬機器提供連線

取消

下一步

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。

新增組織 VDC 網路

1 範圍

2 網路類型

3 Edge 連線

4 一般

5 靜態 IP 集區

6 DNS

7 即將完成

網路類型

選取您要建立的網路類型

☒ 已路由

此類型的網路透過 Edge 閘道提供對 VDC 或 VDC 群組外部的機器和網路的控制存取權。

☐ 已隔離

此類型的網路提供完全隔離的環境，只有此組織 VDC 或 VDC 群組可存取此環境。

取消

上一步

下一步

選擇已配發的 Edge。



新增組織 VDC 網路

- 1 範圍
- 2 網路類型
- 3 Edge 連線
- 4 一般
- 5 靜態 IP 配置
- 6 DNS
- 7 配置完成

Edge 連線

名稱	外部網路	組織 VDC 網路
TWM-Edge	1	0

第 1 - 1 個 Edge 閘道，共 1 個

分散式路由 ☐

允許的客體 VLAN ☐

取消 上一步 下一步

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



新增組織 VDC 網路

- 1 範圍
- 2 網路類型
- 3 Edge 連線
- 4 一般
- 5 靜態 IP 配置
- 6 DNS
- 7 配置完成

一般

名稱 * ERP-Network

說明

雙單疊模式 ☐

閘道 CIDR * 192.168.88.254/24

共用 ☐

取消 上一步 下一步

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



新增組織 VDC 網路

- 1 範圍
- 2 網路類型
- 3 Edge 連線
- 4 一般
- 5 靜態 IP 集區**
- 6 DNS
- 7 即將完成

開道 CIDR 192.168.88.254/24 ⓘ

靜態 IP 集區

輸入 IP 範圍 (格式: 192.168.1.2 - 192.168.1.100)

192.168.88.1 - 192.168.88.200

IP 位址總計: 200

取消 上一步 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)。



新增組織 VDC 網路

- 1 範圍
- 2 網路類型
- 3 Edge 連線
- 4 一般
- 5 靜態 IP 集區
- 6 DNS**
- 7 即將完成

主要 DNS 61.31.1.1

次要 DNS 8.8.8.8

DNS 尾碼

取消 上一步 下一步

最後再次檢查設定，到此就新增 VDCNetwork 完成。

新增組織 VDC 網路

- 範圍
- 網路類型
- Edge 連線
- 一般
- 靜態 IP 集區
- DNS
- 即將完成

即將完成

範圍

站台	laas3sil.taiwancloud.com.tw
範圍	TWM.com-VDC

一般

名稱	ERP-Network
說明	-
網路類型	已路由
連線	TWM-Edge
分散式路由	作用中
允許的客體 VLAN	否

關道 CIDR

雙堆疊模式	否
關道 CIDR	192.168.88.254/24

靜態 IP 集區

[取消](#)
[上一步](#)
[完成](#)

- 計算
- vApp
- 虛擬機器
- 相似性規則
- 網路
- 網路
- Edge
- 儲存區
- 異地端端
- 儲存區原則

網路

新增

	名稱	↑ ↓	狀態	關道 CIDR	↑ ↓	網路類型	已連線至	已使用的 IP 集區	占用
☐	ERP-Network		正常	192.168.88.254/24		已路由	TWM-Ed...		0%

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。



The screenshot shows the vApp management interface. At the top, there's a search bar with '尋找依據: 名稱' and a '進階篩選' link. Below that, it shows '1 個虛擬應用程式' with a filter '已到期: 否' and a '清除所有篩選器' button. A '新增' button is also present. The main content area displays the details for 'ERP-SERVER', including its status '已關閉電源', storage usage '儲存區租用 29 天 (標記為已到期)', creation time '建立於 2023/05/17 上午11:37:43', and owner '擁有者 wayne'. Below this, there's a section for '虛擬機器' (Virtual Machine) with a '管理' link and a list of 1 VM. The VM details show CPU (2), Storage (34 GB), Memory (4 GB), and Network (1). At the bottom, there's an '動作' (Actions) dropdown menu, and the '詳細資訊' (Details) button is highlighted with a red box.

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。



啟用 DHCP 一般設定

1 一般設定

2 DHCP 集區

3 透過 DHCP 的 DNS

4 檢閱並完成

子網路 192.168.88.254/24

DHCP 模式

☐ 網誌
使用此網路直接相關的靜態 DHCP 服務來取得 DHCP IP。如果網路已斷路或打不通此網路與 Edge 中斷連結，請使用網誌模式。

☒ 閘道
使用 Edge 的 DHCP 服務來取得 DHCP IP。

☐ 轉送
DHCP 訊息會從直接連接轉送至實體 DHCP 服務站中指定的 DHCP 伺服器。

撥號程式 IP 位址 192.168.88.254
IP 位址必須是網際網路的一部分。

租用時間 1 天

取消 下一步

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。



啟用 DHCP DHCP 集區

1 一般設定

2 DHCP 集區

3 透過 DHCP 的 DNS

4 檢閱並完成

新增

集區

192.168.88.231-192.168.88.250

1 個項目

IP 位址總計: 20

取消 上一步 下一步

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)。



啟用 DHCP

1 一般設定

2 DHCP 集區

3 透過 DHCP 的 DNS

4 檢閱並完成

透過 DHCP 的 DNS

當虛擬機器使用 DHCP 模式連線至網路時，將從 DHCP 服務取得這些 DNS IP。最多可以新增兩個 DNS 伺服器，對於這兩者，可以使用 IPv4 或 IPv6 位址。

DNS 伺服器 1 61.31.1.1

DNS 伺服器 2 8.8.8.8

取消 上一步 下一步

檢視相關設定。



啟用 DHCP

1 一般設定

2 DHCP 集區

3 透過 DHCP 的 DNS

4 檢閱並完成

檢閱並完成

一般設定

模式	✖ 關閉
接聽程式 IP 位址	192.168.88.254
租用時間	1天

DHCP 集區

集區	192.168.88.231 - 192.168.88.250
----	---------------------------------

透過 DHCP 的 DNS

DNS 伺服器	61.31.1.1
	8.8.8.8

取消 上一步 完成

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。

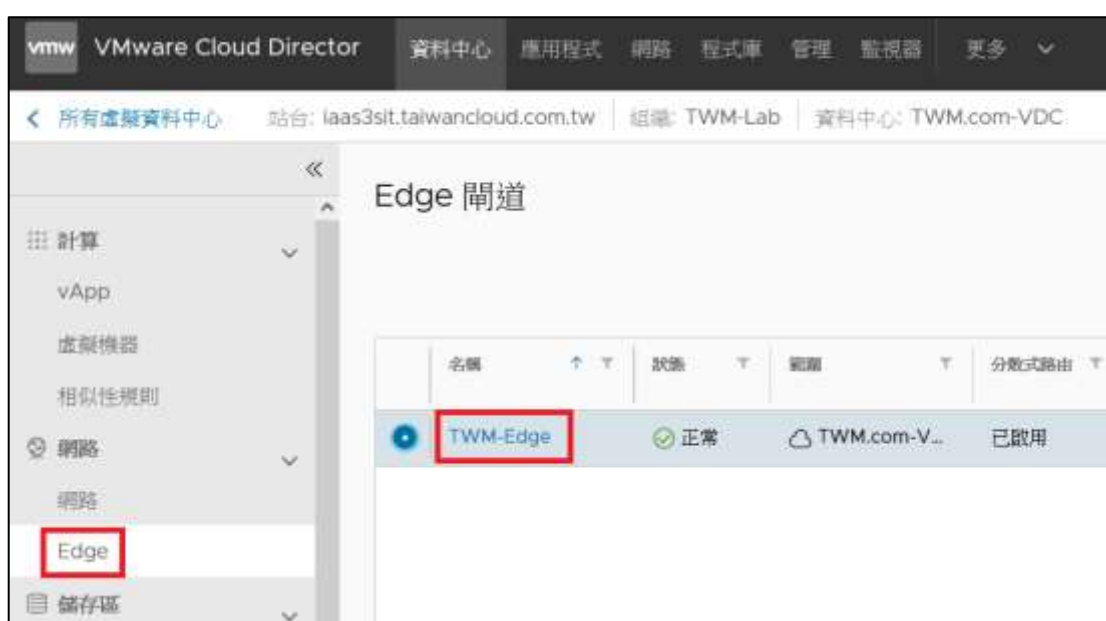


12. 新版-Edge 管理

※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)

選取應用程式

選擇特定的應用程式 

 顯示選取的项目

☐	名稱	說明	類型	通訊協定和目的地連接埠
☐	AD Server	AD Server	預設值	TCP : 1024
☐	Active Directory Server	Active Directory Server	預設值	TCP : 464
☐	Active Directory Server ...	Active Directory Server ...	預設值	UDP : 464
☐	CIM-HTTP	CIM-HTTP	預設值	TCP : 5988
☐	CIM-HTTPS	CIM-HTTPS	預設值	TCP : 5989
☐	DCM Java Object Cache ...	DCM Java Object Cache ...	預設值	TCP : 7100
☐	DHCP, MADCAP	DHCP, MADCAP	預設值	UDP : 2535
☐	DHCP-Client	DHCP-Client	預設值	UDP : 68

第 1 - 15 個應用程式，共 410 個

勾選想要使用的連接埠。

選取應用程式

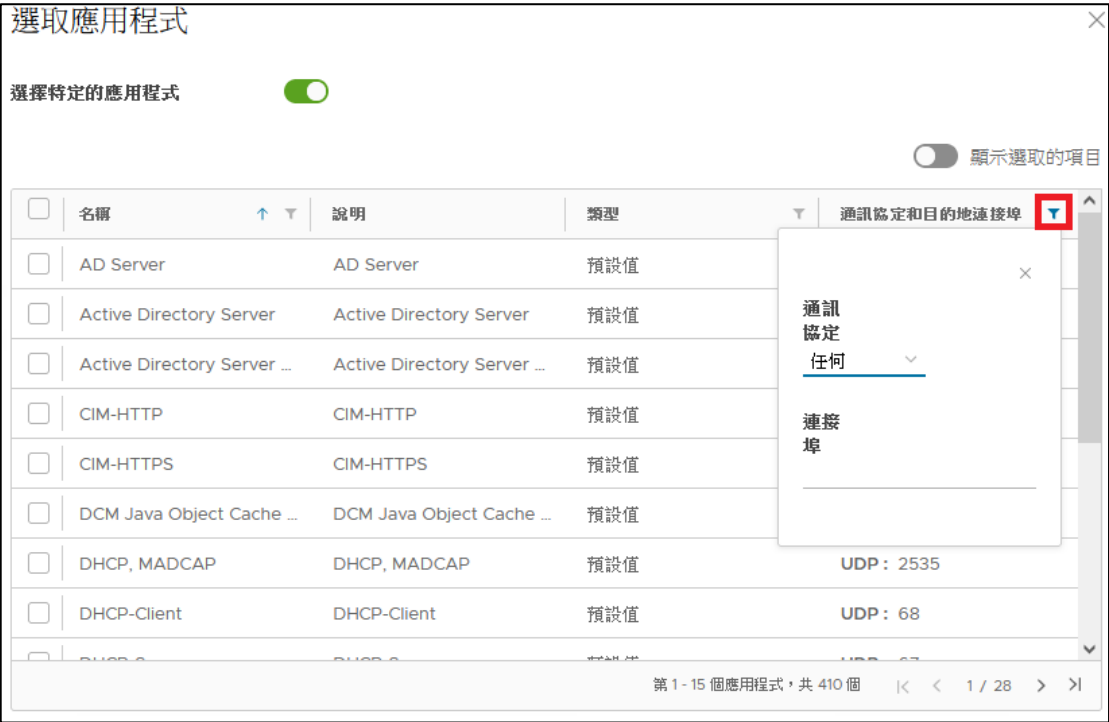
選擇特定的應用程式 

 顯示選取的项目

☐	名稱	說明	類型	通訊協定和目的地連接埠
☐	AD Server	AD Server	預設值	TCP : 1024
☐	Active Directory Server	Active Directory Server	預設值	TCP : 464
☐	Active Directory Server ...	Active Directory Server ...	預設值	UDP : 464
☐	CIM-HTTP	CIM-HTTP	預設值	TCP : 5988
☐	CIM-HTTPS	CIM-HTTPS	預設值	TCP : 5989
☐	DCM Java Object Cache ...	DCM Java Object Cache ...	預設值	TCP : 7100
☐	DHCP, MADCAP	DHCP, MADCAP	預設值	UDP : 2535
☐	DHCP-Client	DHCP-Client	預設值	UDP : 68

第 1 - 15 個應用程式，共 410 個

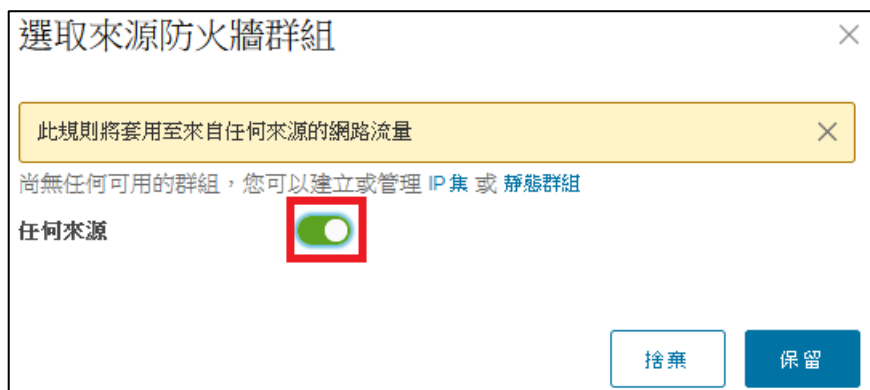
亦可在右邊進行快速篩選。



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



選取來源防火牆群組

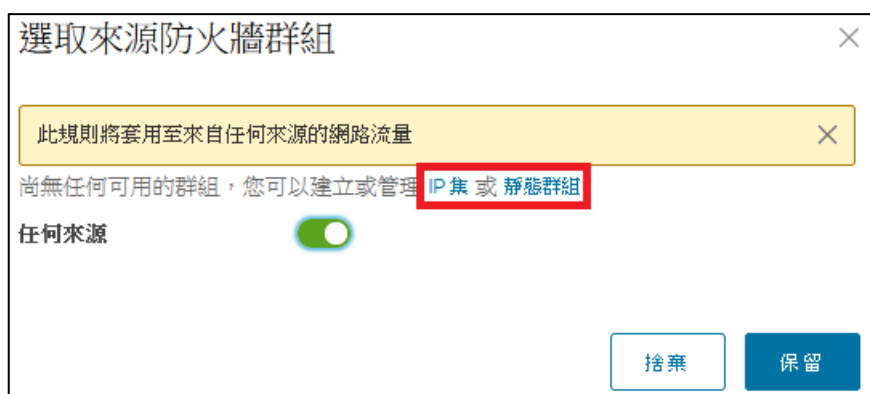
此規則將套用至來自任何來源的網路流量

尚無任何可用的群組，您可以建立或管理 [IP 集](#) 或 [靜態群組](#)

任何來源 ☒

捨棄 保留

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。



選取來源防火牆群組

此規則將套用至來自任何來源的網路流量

尚無任何可用的群組，您可以建立或管理 [IP 集](#) 或 [靜態群組](#)

任何來源 ☐

捨棄 保留

新增靜態群組



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

新增

名稱

填入可識別名稱

新增靜態群組

名稱 *

ERP

說明

捨棄

儲存

選取 ERP 靜態群組→管理成員

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

新增

編輯

管理成員

相關聯的虛擬機器

刪除

名稱	↑	↓	狀態	↓	說明
ERP			正常		-

第 1 - 1 個靜態群組，共 1 個

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。

管理群組「ERP」的成員

☐ 顯示選取的项目

☐	名稱	狀態	開道 CIDR
☒	ERP-Network	✓ 正常	192.168.88.254/24
☐	WEB-Network	✓ 正常	192.168.2.254/24

☒ 1 第 1 - 2 個成員，共 2 個

捨棄儲存

選取相關聯的虛擬機器，可以查看已關聯的虛擬機器。

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

新增編輯管理成員相關聯的虛擬機器刪除

名稱	狀態	說明
ERP	✓ 正常	-

第 1 - 1 個靜態群組，共 1 個

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。

新增 IP 集

名稱 *

Client

說明

IP 位址

輸入 IPv4 或 IPv6 位址、範圍或 CIDR ⓘ

192.168.88.100-192.168.88.150

新增

修改

移除

← 復原

捨棄

儲存

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。

選取來源防火牆群組

任何來源

顯示選取的項目

☐	名稱	↑ ↓	類型	↓	說明
☐	Client		IP 集		-
☒	ERP		靜態群組		-

☒ 1

第 1 - 2 個防火牆群組，共 2 個

捨棄

保留

規則的動作選項分為允許、捨棄、拒絕，可依需求進行調整。

編輯規則

新增規則

向上移動

刪除

上一步

下一步

幫助

學習使用說明

	#	名稱	類別	狀態	應用模式	來源	目的地	動作	IP 地址設定	記錄	註解
	1	Outbound	使用者定義		-			允許	IPv4		
		default_rule	預設值	已啟用	-	任何	任何	允許 允許 捨棄 拒絕	IPv4 和 IPv6	已停用	

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。

新增 NAT 規則

名稱 * DNAT

說明

介面類型 * DNAT

外部 IP * 60.199.153.204 ⓘ
目的地 IP 或 CIDR

外部連接埠 80
目的地連接埠

內部 IP * 192.168.2.1
轉譯的 IP 或 CIDR

應用程式 HTTP
轉譯的連接埠

> ⓘ 進階設定

捨棄 儲存

可用的外部 IP 位址
60.199.153.204 - 60.199.153.204
60.199.153.204

新增 NAT 規則

名稱 * SNAT

說明

介面類型 * SNAT

外部 IP * 60.199.153.203 ⓘ
轉譯的 IP 或 CIDR

內部 IP * 192.168.20.0/24
來源 IP 或 CIDR

目的地 IP

> ⓘ 進階設定

捨棄 儲存

可用的外部 IP 位址
60.199.153.203 - 60.199.153.203
60.199.153.203

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。

TWM-Edge 在 VDC 內基本設定

#	名稱	狀態	啟用	策略	連線模式	來源	目的地	動作
1	ERP-WebService	使用有定額	已啟用	HTTPS, HTTP	任何	Edge Public	任何	允許
2	辦公室直接連 VM	使用有定額	已啟用	SSH, RDP	外部辦公室 IP 群	Edge Public	任何	允許
3	VM 可連外	使用有定額	已啟用	-	Client	任何	任何	允許
4	VPN	使用有定額	已啟用	-	192.168.30.0/24, 10.10.10.0...	192.168.30.0/24, 10.10.10.0...	任何	允許
5	default_rule	禁連線	已啟用	-	任何	任何	任何	拒絕

TWM-Edge 在 VDC 內基本設定

名稱	狀態	啟用	策略	外網 IP	連線模式	內網 IP	自動開關	目的端 IP	動作
ERP-WebService-443	使用有定額	已啟用	DNAT	60.199.134.204	HTTPS	192.168.30.443	-	-	已啟用
ERP-WebService-80	使用有定額	已啟用	DNAT	60.199.134.204	HTTP	192.168.30.80	-	-	已啟用
VM 可連外	使用有定額	已啟用	SNAT	60.199.134.204	-	192.168.2.1	任何	-	已啟用
辦公室直接連 VM-22	使用有定額	已啟用	DNAT	60.199.134.204	SSH	192.168.30.22	-	-	已啟用
辦公室直接連 VM-443	使用有定額	已啟用	DNAT	60.199.134.204	RDP	192.168.30.3388	-	-	已啟用

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，並將成員狀態啟用，儲存。

編輯負載平衡器集區「RT-pool」

一般設定 成員 SSL 設定

新增 刪除

	IP 地址	健康狀況判斷	狀態	權重	比率
☐	192.368.0.4	開啟	☒ 已啟用	80	1
☐	192.368.0.3	開啟	☒ 已啟用	80	1

2 個成員

取消 儲存

再到虛擬服務新增。

✎ 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

新增

	名稱	健全狀況	啟
☐	RT-SLB-VIP	☒ 開啟	已

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。

新增虛擬服務

名稱 * RT-SLB-VIP 服務引擎群組 * 遍取

說明 負載平衡器集區 * 遍取

已啟用 ☒ 虛擬 IP * 

服務類型 HTTP 連接埠 80

取消 儲存

服務引擎群組選取第一組。

選取服務引擎群組

名稱	虛擬服務
 jmmysitmax011b.com-seg	1/20 已部署 (已部署 20)

負載平衡器集區選取剛才建立的集區。

選取負載平衡器集區

名稱	健全狀況	狀態	狀態	成員 (預期/統計)	虛擬服務
 RT-pool	 健康	已啟用	 正常	2 / 2	RT-SLB-VIP

填入虛擬 IP，可點選旁邊 ⓘ 符號快速看出可用的外部 IP。



新增虛擬服務

名稱 * RT-SLB-VIP 服務引擎群組 * jimmysitnsxt0118.com-seg

說明

已啟用 ☒

服務類型 HTTP 連接埠

虛擬 IP ⓘ

虛擬 IP 可以是內部或外部，外部虛擬 IP 必須屬於配置

60.199.153.122 - 60.199.153.124

60.199.153.122

確認*必填欄位填完，點選儲存。



新增虛擬服務

名稱 * Web-80 服務引擎群組 * jimmysitnsxt0118.com-seg

說明

已啟用 ☒

服務類型 HTTP 連接埠

虛擬 IP 60.199.153.122 ⓘ

80

取消 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。

新增 IPsec VPN 通道

1 一般設定

2 對等驗證模式

3 端點組態

4 即將完成

一般設定

名稱 *
TWM-VPN

說明

安全性設定檔
預設值

> IKE 設定檔

> 通道組態

> DPD 組態

狀態
☒

取消 下一步

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。

新增 IPsec VPN 通道

1 一般設定

2 對等驗證模式

3 端點組態

4 即將完成

對等驗證模式

驗證模式
☒ 預先共用金鑰
☐ 憑證

預先共用金鑰 *
vpntest

取消 上一步 下一步

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。



新增 IPsec VPN 通道

端點組態

1 一般設定

2 對等驗證模式

3 端點組態

4 密碼設定

本機端點

IP 位址 *

60.199.153.204 ⓘ

網路 *

192.168.88.0/24

可用的 IP 位址

60.199.153.204 - 60.199.153.204

60.199.153.204

以這組分組的 CIDR (例如 192.168.10.0/24, 212.138.0.0/16)

遠端端點

IP 位址 *

網路 *

取消 上一步 下一步

遠端端點填入遠端 Public IP。
網路填入遠端的子網路。



新增 IPsec VPN 通道

端點組態

1 一般設定

2 對等驗證模式

3 端點組態

4 密碼設定

遠端端點

IP 位址 *

60.199.144.206

網路 *

10.10.10.0/24

以這組分組的 CIDR (例如 192.168.10.0/24, 212.138.0.0/16)

遠端識別碼 ⓘ

取消 上一步 下一步

檢視設定。



新增 IPsec VPN 通道 即將完成

1 一般設定
2 對等驗證模式
3 端點組態
4 即將完成

一般設定

名稱	TWM-VPN
說明	-
安全性設定檔	預設值
狀態	已啟用
記錄	已停用

對等驗證模式

驗證模式	預先共用金鑰
預先共用金鑰	*****

取消 上一步 完成

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。



TWM-Edge 在 VDC 內集中管理

新增 編輯 檢視統計資料 安全性設定檔 刪除

名稱	狀態	安全性設定檔	本端 IP	遠端 IP	記錄
TWM-VPN	已啟用	預設值	60.199.153.204	60.199.144.206	否



「TWM-VPN」統計資料

狀態

通道狀態	✓ 開啟
IKE 服務狀態	✓ 開啟
IKE 失敗原因	-

流量與錯誤

子網路

本機子網路	192.168.88.0/24
對等子網路	10.10.10.0/24

一般流量

傳入的封包數	2
傳出的封包數	-

若是建立失敗會顯示。

「TWM-VPN」統計資料

狀態 

通道狀態	❗ 關閉
IKE 服務狀態	❗ 關閉
IKE 失敗原因	No proposal chosen

流量與錯誤 

▼ 子網路

本機子網路	192.168.88.0/24
對等子網路	10.10.10.0/24

▼ 一般流量

傳入的封包數	2
傳出的封包數	-

防火牆需雙向開通。

編輯規則

在頂部新增 在上方新增 刪除 上一步 下一步 移動至 移至使用會規則

	#	名稱	類別	狀態	應用程式	來源	目的地	動作	IP 通訊協定	記錄	註釋
☐		Tier1-7022...	系統	已啟用	-	任何	任何	允許	-	已停用	-
☐		Tier1-7022...	系統	已啟用	-	192.168.88.0/24, 10.10.10.0/24	任何	允許	-	已停用	-
☒		1 VPN	使用者定義	已啟用	-	192.168.88...	192.168.88...	允許	IPv4	已停用	-
☐		default_rule	預設值	已啟用	-	任何	任何	捨棄	IPv4 和 IPv6	已停用	-

◀ 新增規則

測試連線是否可 ping 通

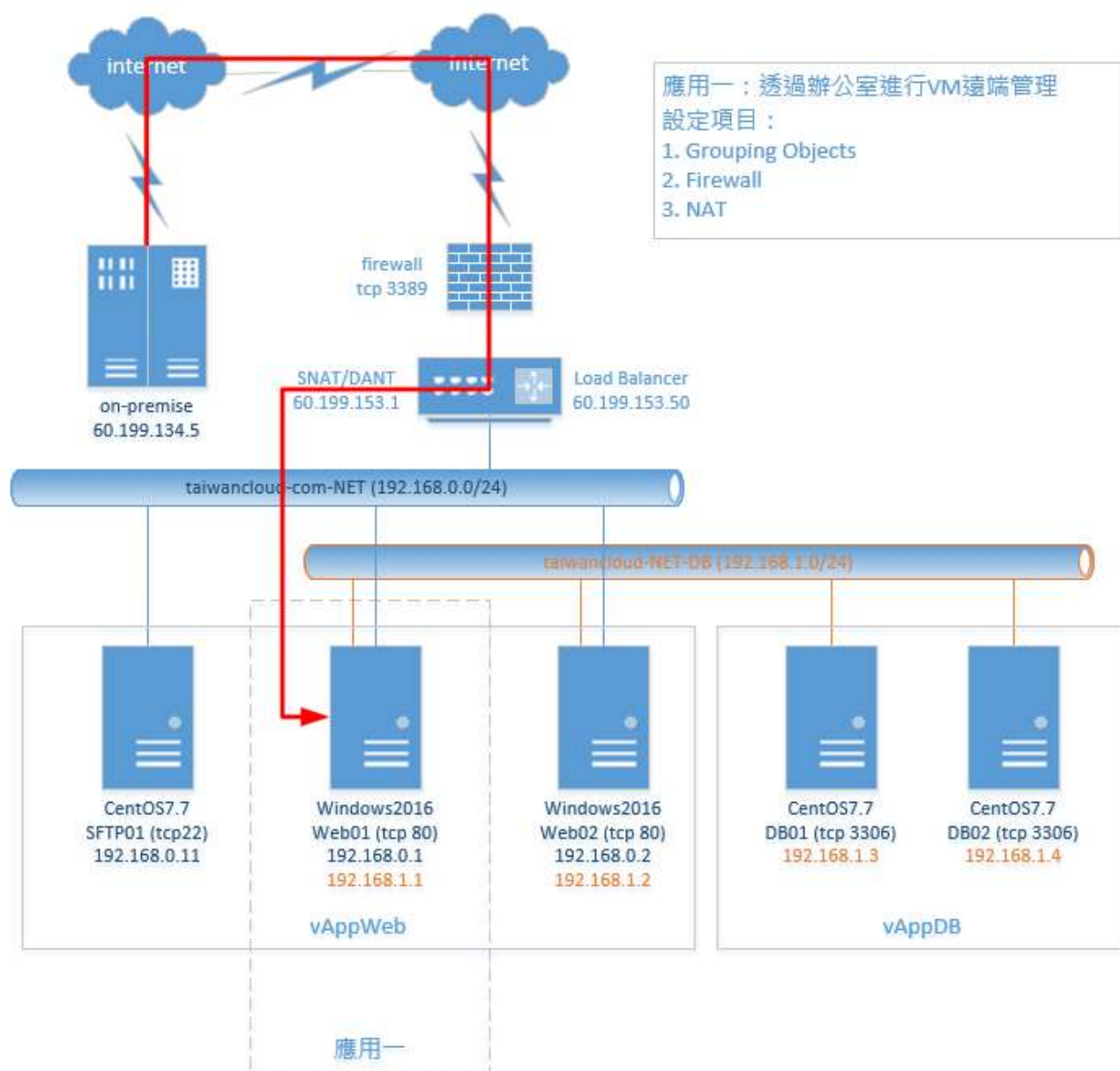
```
urf8-uapp-vm1:~ # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet 127.0.0.2/8 brd 127.255.255.255 scope host seconda
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc p
    link/ether 00:50:56:01:00:d5 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.1/24 brd 10.10.10.255 scope global eth0
urf8-uapp-vm1:~ # ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1) 56(84) bytes of data.
64 bytes from 192.168.88.1: icmp_seq=1 ttl=62 time=1.59 ms
64 bytes from 192.168.88.1: icmp_seq=2 ttl=62 time=1.09 ms
64 bytes from 192.168.88.1: icmp_seq=3 ttl=62 time=1.20 ms
```

```
[root@centos74-template-001 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue sta
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qd
    link/ether 00:50:56:01:05:a5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.88.1/24 brd 192.168.88.255 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe01:5a5/64 scope link
        valid_lft forever preferred_lft forever
[root@centos74-template-001 ~]# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=62 time=1.33 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=62 time=1.19 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=62 time=1.19 ms
```


13. 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。



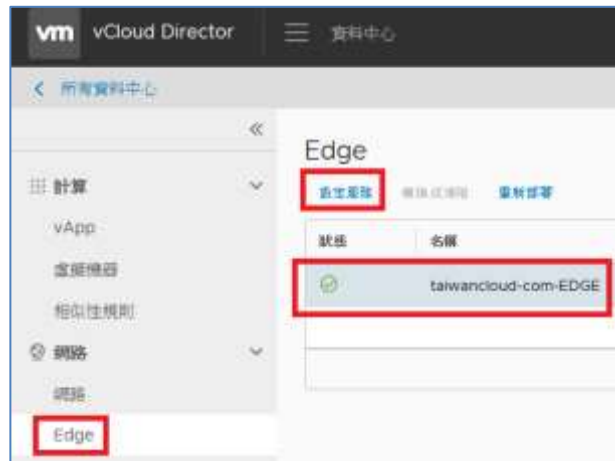
前置作業

1. 新增 vAppWeb
2. 建立 Web VM

設定項目

1 Grouping Objects

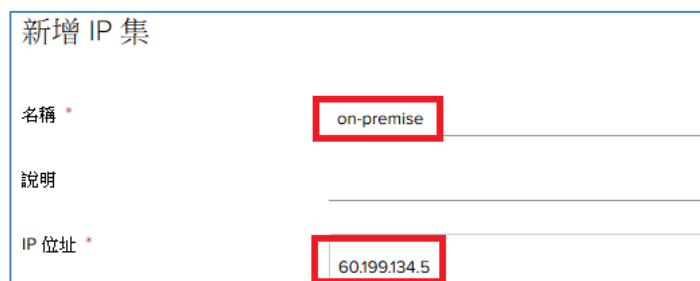
1.1 點選網路>「Edge」>「設定服務」



1.2 點選「群組物件」>「IP 集」>「新增」

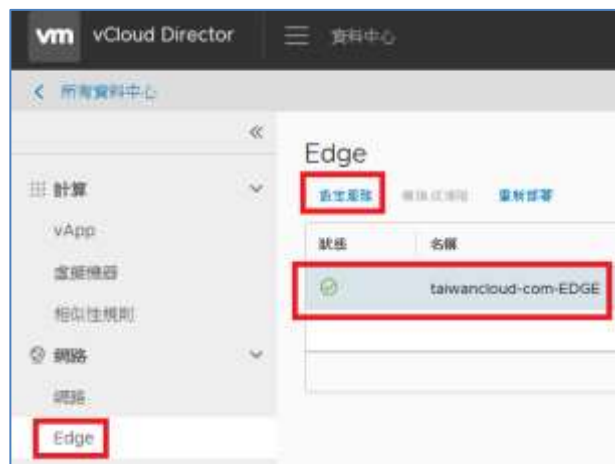


1.3 輸入名稱與 IP 後，點選「保留」



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

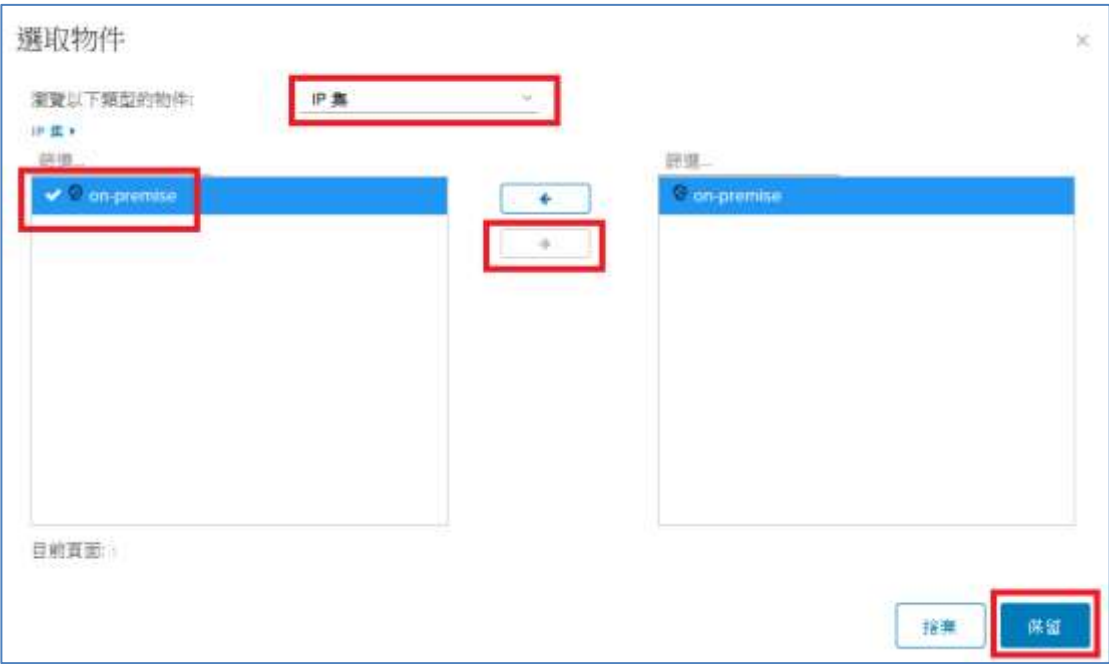
編號	名稱	類型
1 ✓	firewall	內部 (高)
2 ✓	on-premise	使用者
3 ✓	SNAT	使用者

2.4 點選「來源」>「+」

類型	來源	目的地
內部 (高)	vse	任何
使用者	任何	任何

新增物件

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」

來源	目的地	服務	動作
vse	任何	任何	接受
on-premise	任何	任何	接受

新增服務

通訊協定

TCP

來源連接埠

any

將此欄位保留為空白會使此規則套用到任何連接埠

目的地連接埠

3389

將此欄位保留為空白會使此規則套用到任何連接埠

捨棄

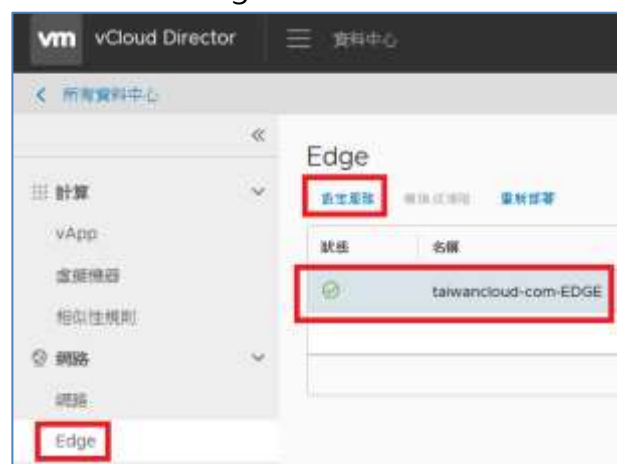
保留

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

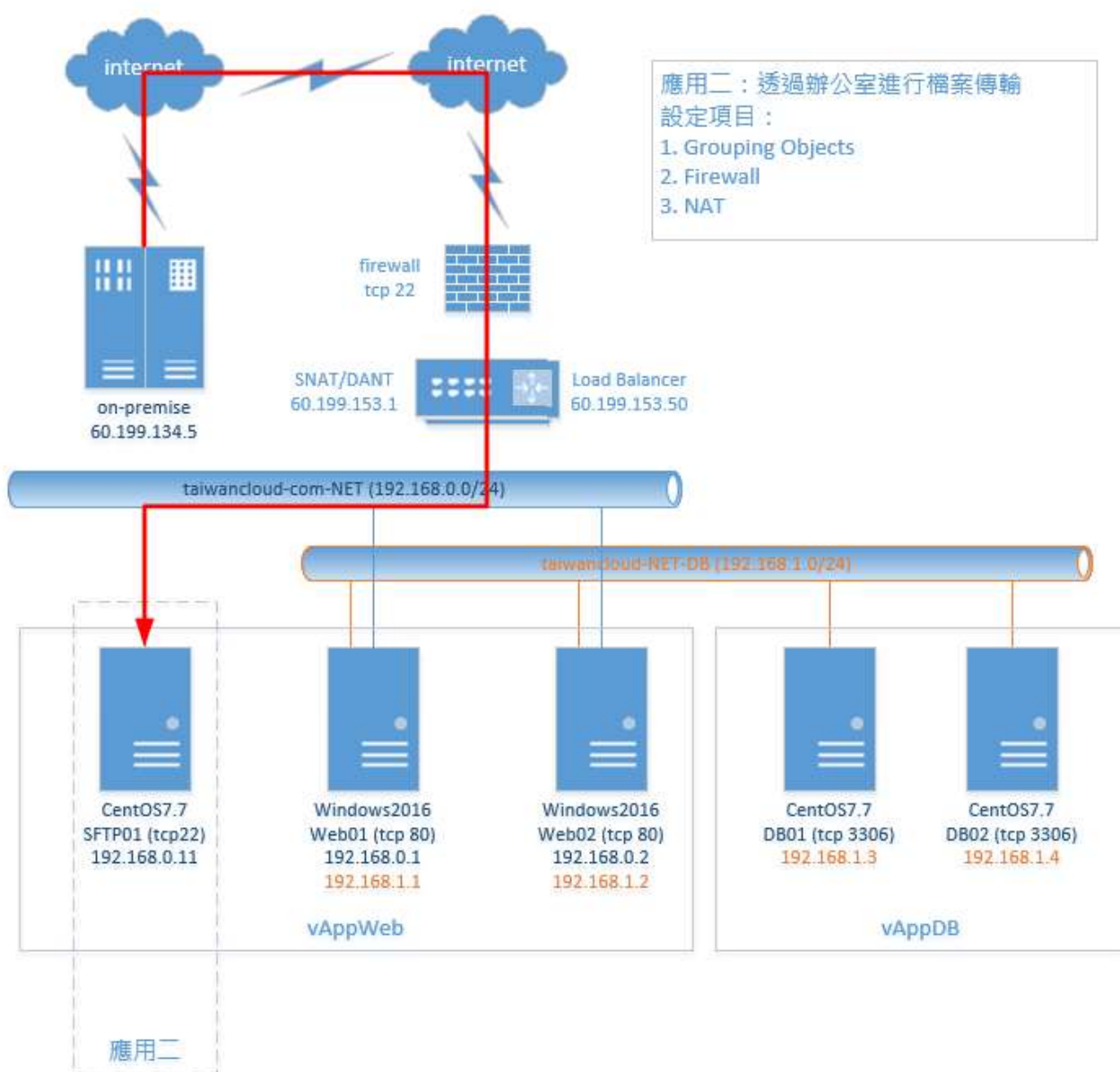
4.1 遠端透過 RDP 登入



14. 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。



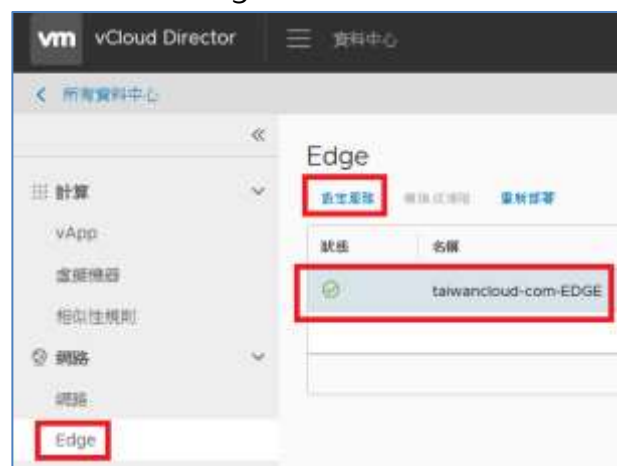
前置作業

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」



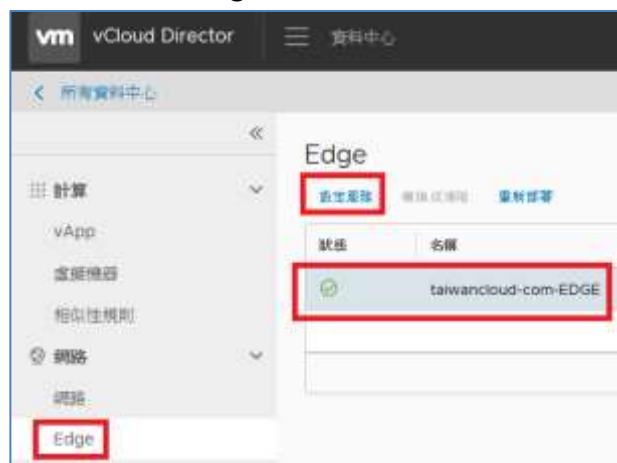
1.3 輸入名稱與 IP 後，點選「保留」

新增 IP 集

名稱 *	on-premise
說明	
IP 位址 *	60.199.134.5

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

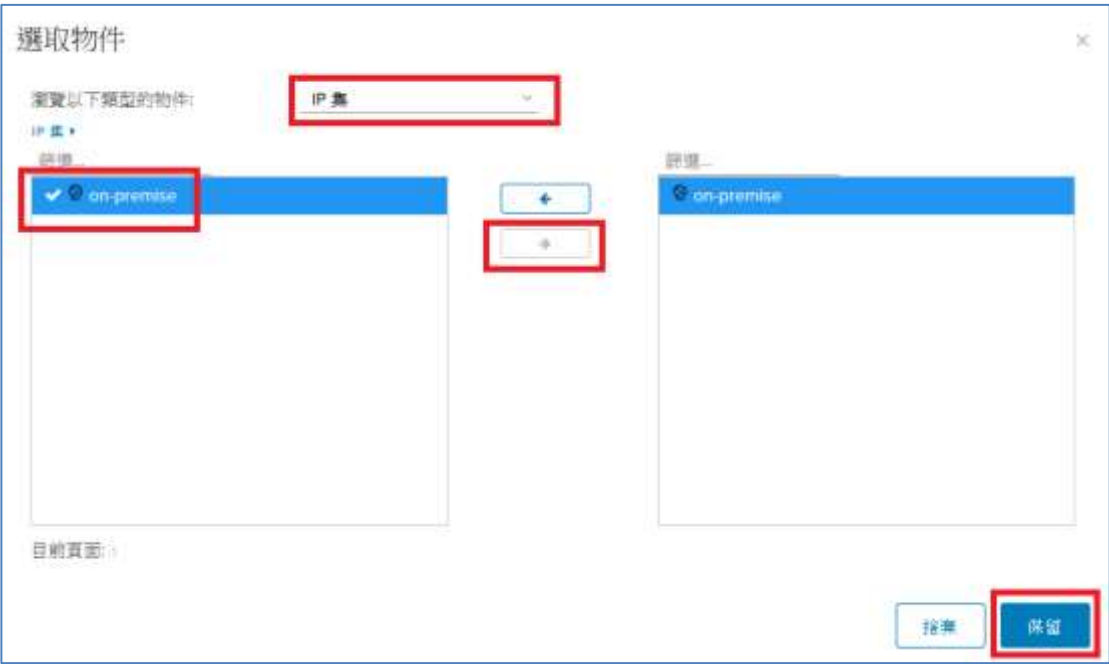
編號	名稱	類型
1✓	firewall	內部 (高)
2✓	on-premise	使用者

2.4 點選「來源」>「+」

類型	來源	目的地
內部 (高)	vse	任何
使用者	任何	任何

Below the table, there is a blue bar with a '+', 'IP', and another '+'. The second '+' is highlighted with a red box. A label '新增物件' (Add object) is positioned below the red box.

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」

來源	目的地	服務	動作
use	任何	任何	接受
on-premise	任何	任何	接受

新增服務

通訊協定

TCP

來源連接埠

any

將此欄位保留為空白會使此規則套用到任何連接埠

目的地連接埠

22

將此欄位保留為空白會使此規則套用到任何連接埠

捨棄

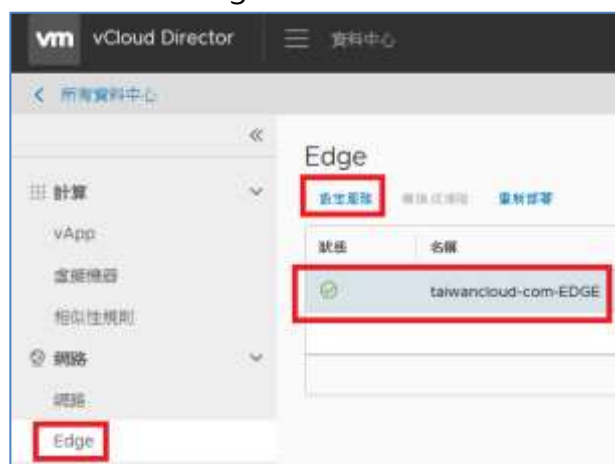
保留

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

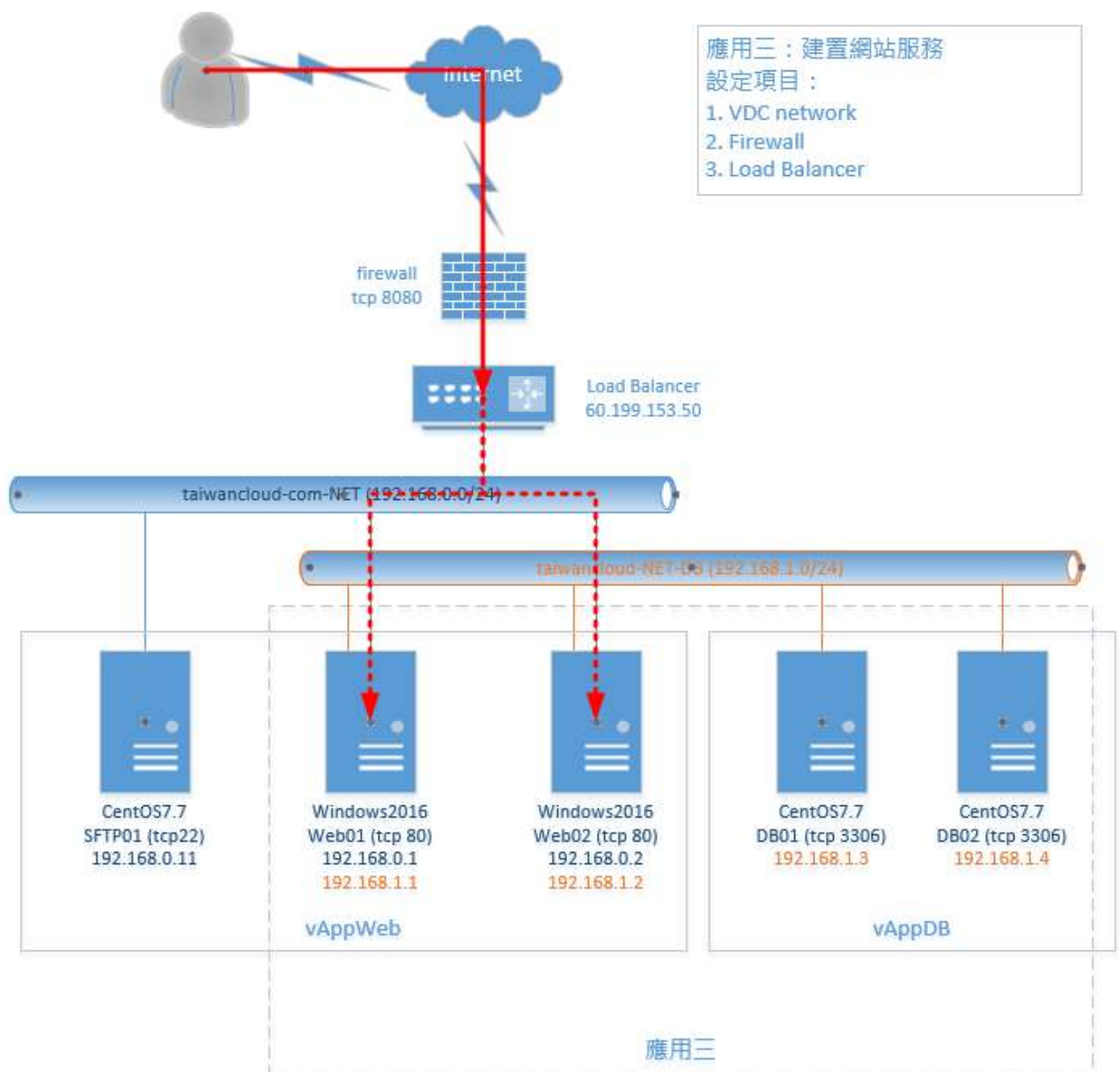
4.1 遠端透過工具連線



15. 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。



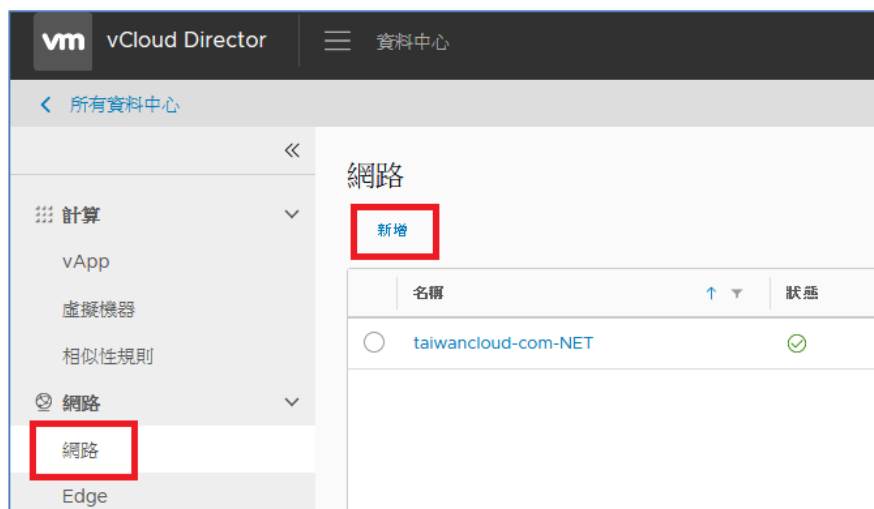
前置作業

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	網路類型
1 網路類型	選取您要建立的網路類型
2 一般	☒ 已隔離 此類型的網路提供完全隔離的環境，只有此 VDC 中的虛擬機器可以連線到該環境。
3 靜態 IP 集區	☐ 已路由 此類型的網路透過 Edge 閘道提供對 VDC 外部之機器和網路的控制存取權
4 DNS	☐ 直接 此類型的網路直接連線至外部網路
5 即將完成	

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

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

新增組織 VDC 網路

- 網路類型
- 一般
- 靜態 IP 集區
- DNS
- 即將完成

即將完成

您即將建立一個具備這些規格的組織 VDC 網路。請檢閱設定，然後按一下 [完成]。

名稱	taiwancloud-com-NET-DB
說明	-
闡述 CIDR	192.168.1.254/24
網路類型	已隔離
主要 DNS	-
次要 DNS	-
DNS 尾碼	-
靜態 IP 集區	192.168.1.1 - 192.168.1.200

取消
上一步
完成

1.3

2 Add Network(Web)

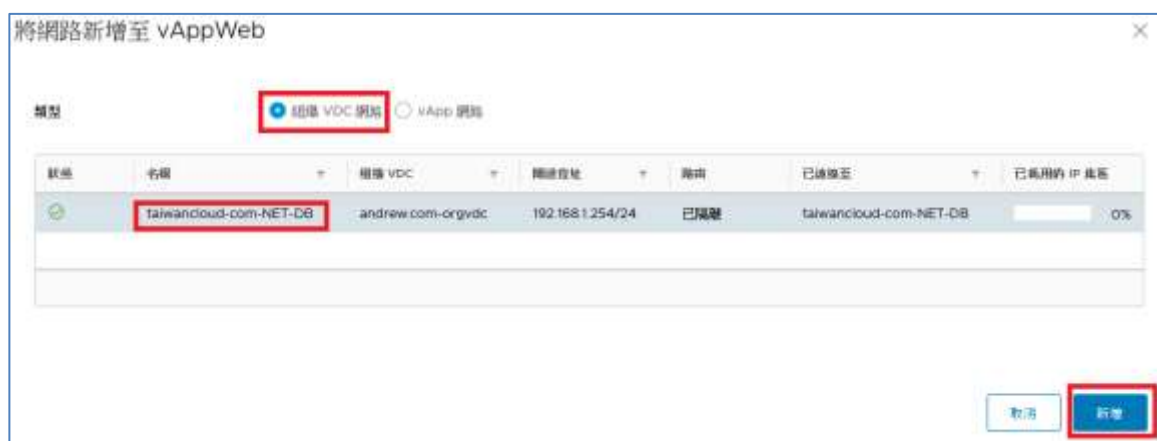
2.1 vApp > 點選 vAppWeb 詳細資訊 > 網路 > 新增

計算
vApp
虛擬機器
相似性規則
網路
網路
Edge
安全性

所有 vApp > vAppWeb
vAppWeb
詳細資料
網路圖表
網路
中繼資料
vApp 圍牆
vApp 未納入範圍
新增

名稱	狀態
taiwancloud-com-NET	✓

2.2 選取前步驟設定之網路 > 新增

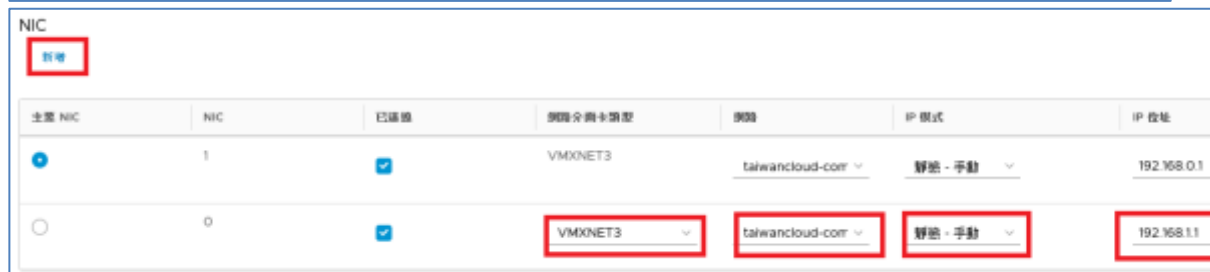
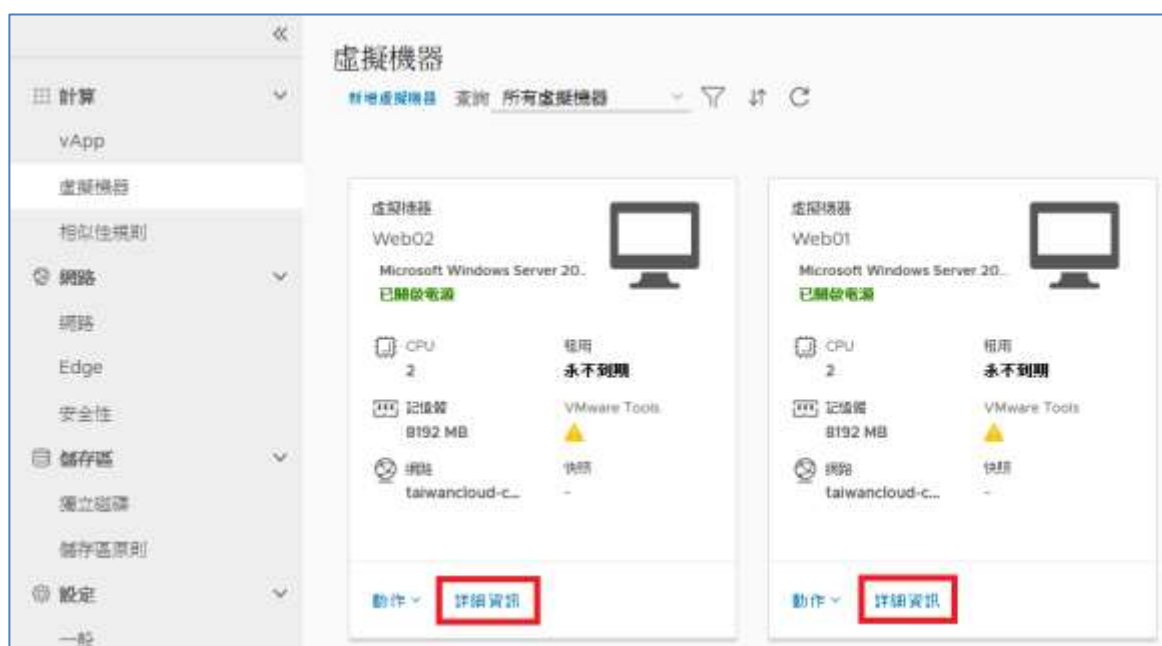


2.3 虛擬機器 > 詳細資訊 > 硬體 > NIC > 新增

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



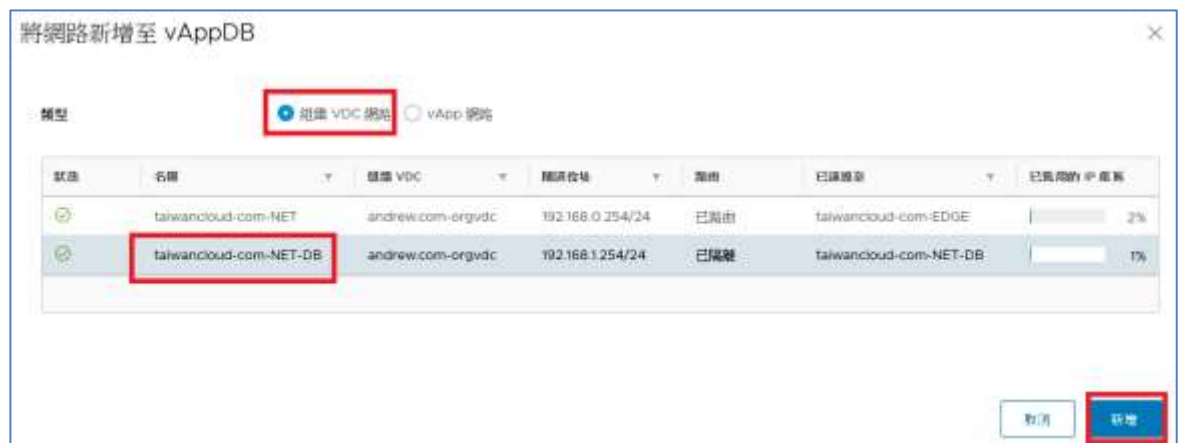


3 Add Network(DB)

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



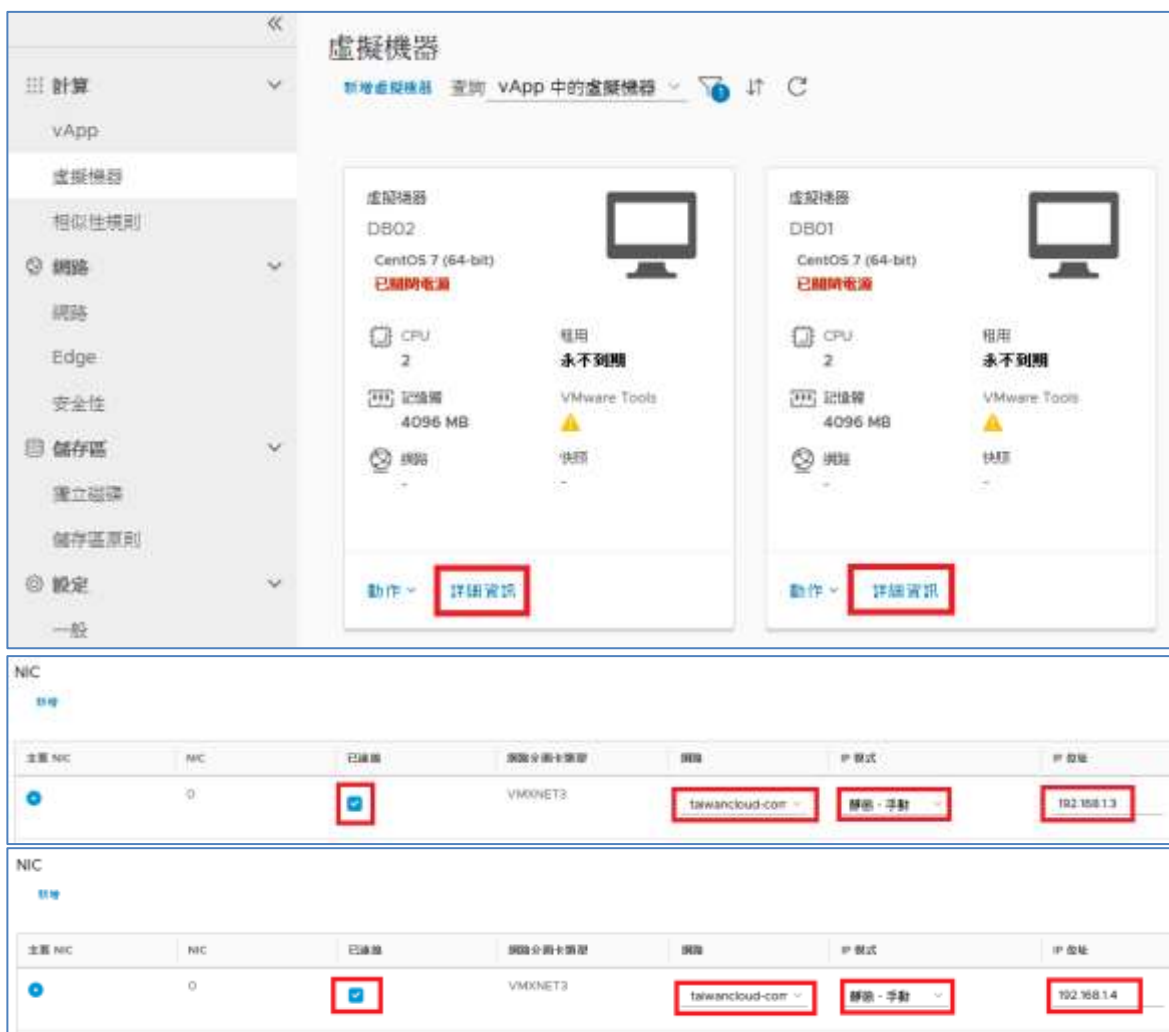
3.3 虛擬機器 > 詳細資訊 > 硬體 > NIC

勾選已連線

選取網路(此例為 taiwancld-com-NET-DB)

IP 模式為手動

設定 IP



虛擬機器

新增虛擬機器 查詢 vApp 中的虛擬機器

計算
vApp
虛擬機器
相似性規則
網路
網路
Edge
安全性
儲存區
獨立磁碟
儲存區原則
設定
一般

虛擬機器 DB02
CentOS 7 (64-bit)
已關閉電源

CPU 2 租用 永不到期
記憶體 4096 MB VMware Tools
網路 快取

動作 詳細資訊

虛擬機器 DB01
CentOS 7 (64-bit)
已關閉電源

CPU 2 租用 永不到期
記憶體 4096 MB VMware Tools
網路 快取

動作 詳細資訊

NIC

新增

主網 NIC	NIC	已連線	網路介面卡類型	網路	IP 模式	IP 位址
+	0	☒	VMXNET3	taiwancld.com	靜態 - 手動	192.168.1.3

NIC

新增

主網 NIC	NIC	已連線	網路介面卡類型	網路	IP 模式	IP 位址
+	0	☒	VMXNET3	taiwancld.com	靜態 - 手動	192.168.1.4

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)

防火牆 DHCP NAT 路由 負載平衡器 VPN SSL VPN-Plus 憑證

防火牆規則

已啟用 ☒

僅顯示使用者定義的規則 ☐

編號	名稱	類型	來源
1✓	firewall	內部 (高)	vse
2✓	Web	使用者	任何

目的地	服務
任何	任何
60.199.153.50	tcp:8080:any

新增服務

通訊協定

來源連接埠

將此欄位保留為空白會使此規則套用到任何連接埠

目的地連接埠

將此欄位保留為空白會使此規則套用到任何連接埠

4.2 點選畫面上方「儲存變更」

防火牆規則

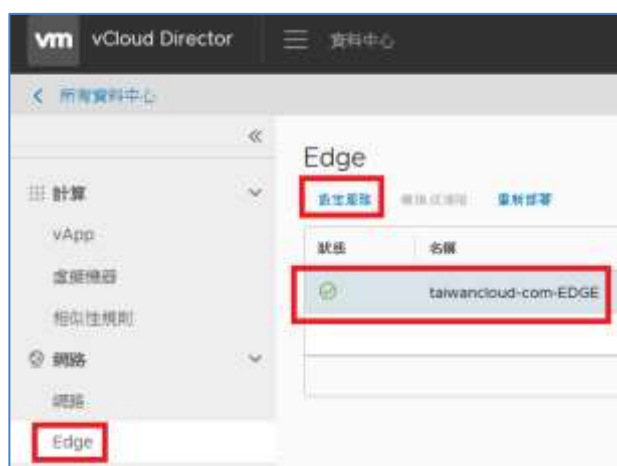
已啟用 ☒

僅顯示使用者定義的規則 ☐

編號	名稱	類型	來源	目的地	服務	動作	儲存設定
1✓	firewall	內部 (高)	vse	任何	任何	接受	儲存
2✓	Web	使用者	any	60.199.153.50	tcp:8080:any	接受	儲存

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)





名稱

說明

演算法

演算法參數

監視器

透明 ☐

成員

已...	名稱	IP 位址	權...	監...	連...	連線數下...	連線數...
☒	Web01	192.168.0.1	1		80		
☒	Web02	192.168.0.2	1		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」

防火牆

DHCP

NAT

路由

負載平衡器

VPN

SSL VPN-Plus

憑證

全域組態

應用程式設定檔

服務監視

集區

應用程式規則

虛擬伺服器

虛擬伺服器

+

×

↺

虛擬伺服器識別碼	名稱	說
----------	----	---

一般

進階

啟用虛擬伺服器

☒

啟用加速

☐

應用程式設定檔

▼

名稱 *

Web

說明

IP 位址 *

60.199.153.50

選取

通訊協定 *

HTTP ▼

連接埠 *

8080

預設集區

Web ▼

連線限制

連線速率限制 (CPS)

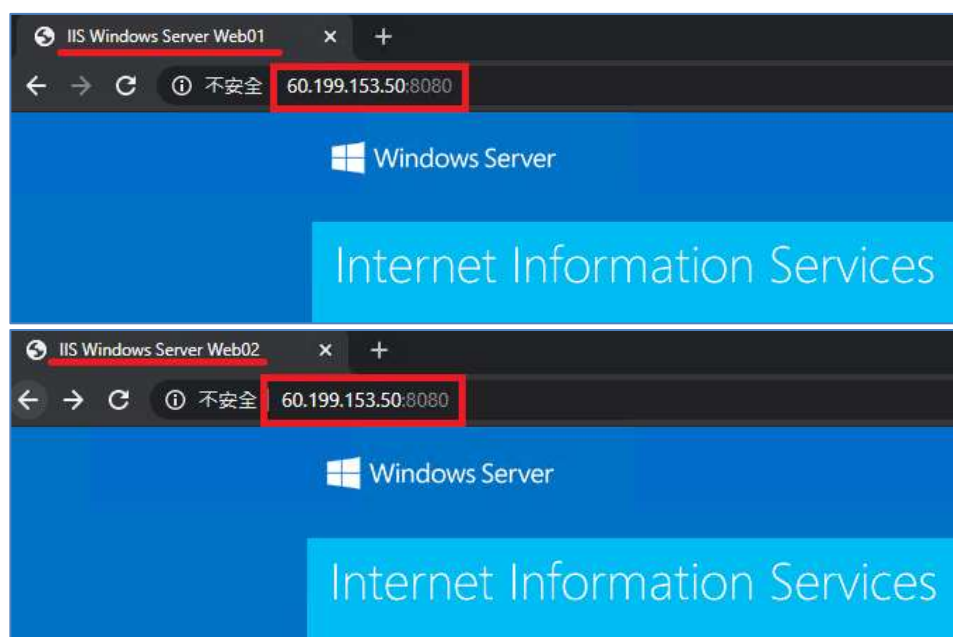
<

>

捨棄

保留

5.5 透過遠端進行測試(演算法 Round-Robin)



16. 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 Server2012R2/2016/2019 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

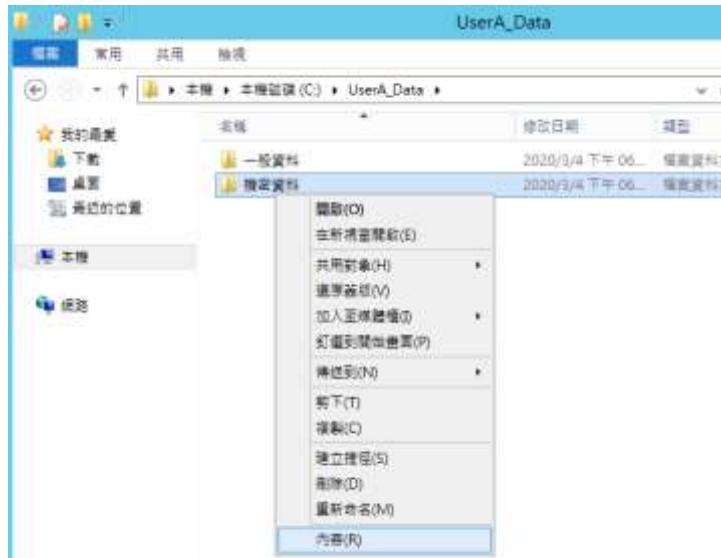
功能說明：

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

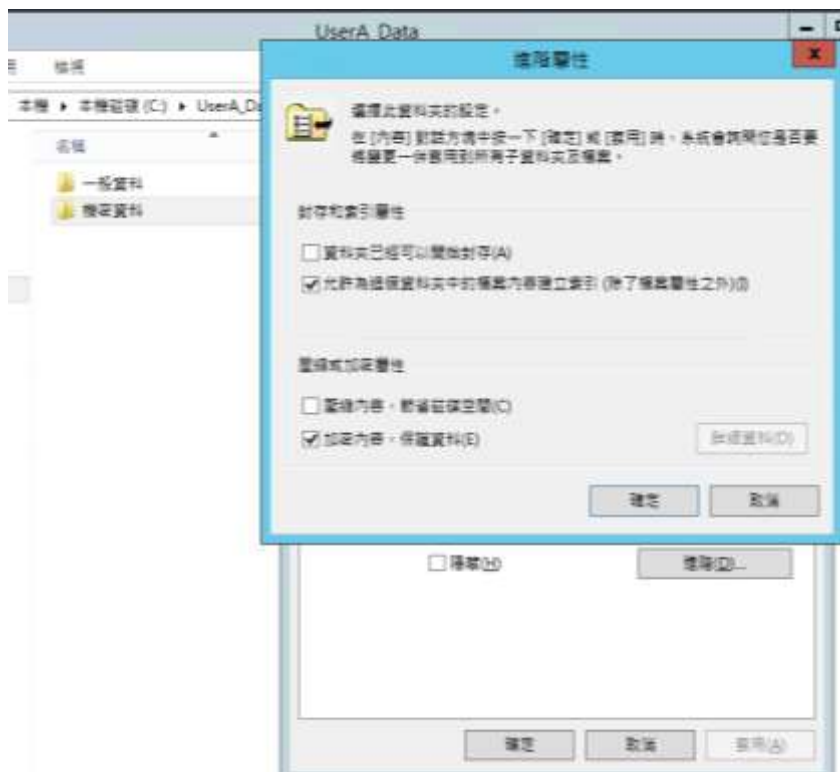
統中會被標示為加密屬性，非用戶帳號無法開啟該資料

設定步驟：

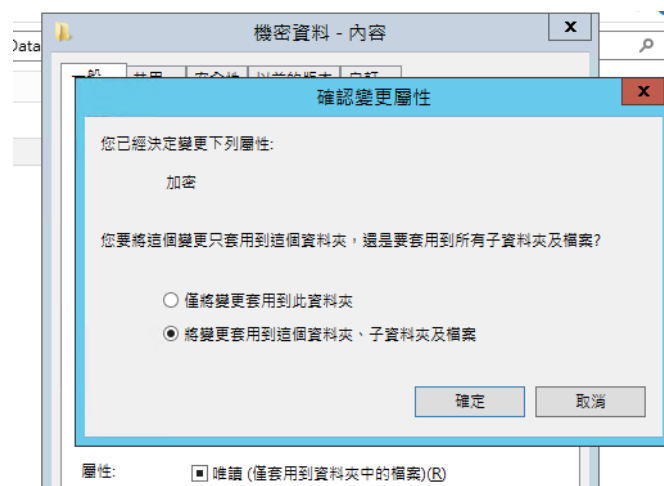
選擇要加密的資料按右鍵選擇【內容】



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】



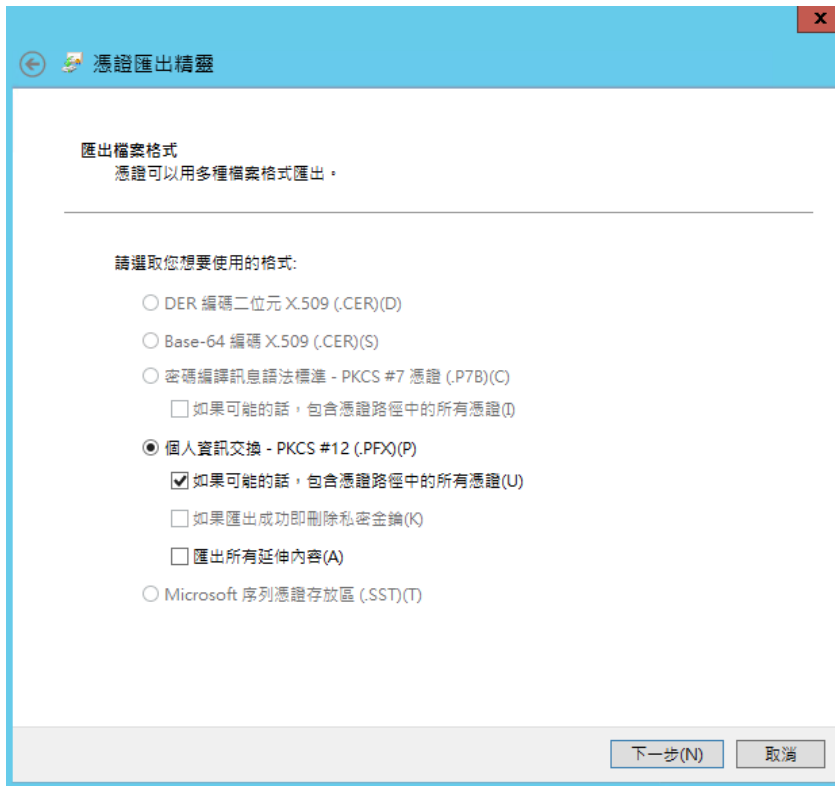
系統會提示您備份金鑰



點選【下一步】繼續



點選【下一步】繼續



憑證匯出精靈

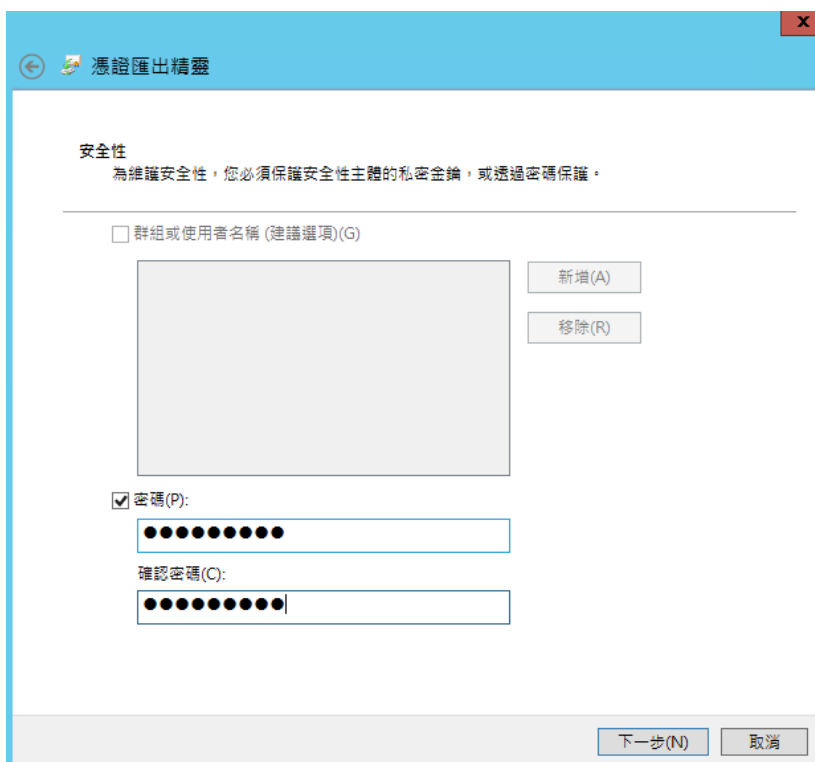
匯出檔案格式
憑證可以用多種檔案格式匯出。

請選取您想要使用的格式:

- ☐ DER 編碼二位元 X.509 (.CER)(D)
- ☐ Base-64 編碼 X.509 (.CER)(S)
- ☐ 密碼編譯訊息語法標準 - PKCS #7 憑證 (.P7B)(C)
 - ☐ 如果可能的話，包含憑證路徑中的所有憑證(I)
- ☒ 個人資訊交換 - PKCS #12 (.PFX)(P)
 - ☒ 如果可能的話，包含憑證路徑中的所有憑證(U)
 - ☐ 如果匯出成功即刪除私密金鑰(K)
 - ☐ 匯出所有延伸內容(A)
- ☐ Microsoft 序列憑證存放區 (.SST)(T)

下一步(N) 取消

輸入密碼後點選【下一步】繼續



憑證匯出精靈

安全性
為維護安全性，您必須保護安全性主題的私密金鑰，或透過密碼保護。

☐ 群組或使用者名稱 (建議選項)(G)

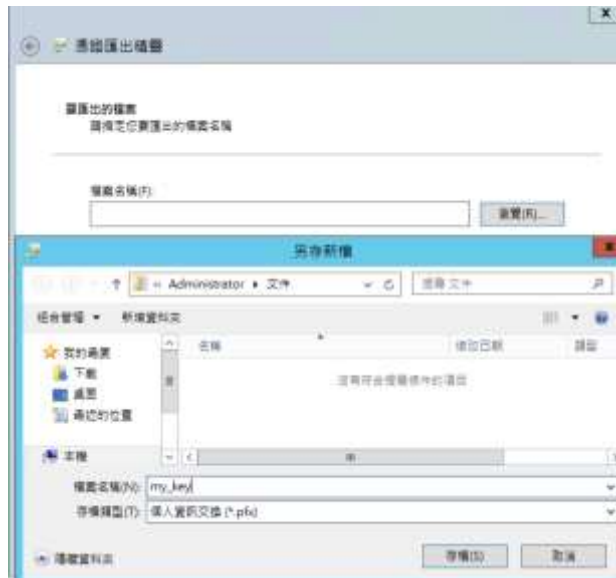
新增(A)
移除(R)

☒ 密碼(P):
●●●●●●●●

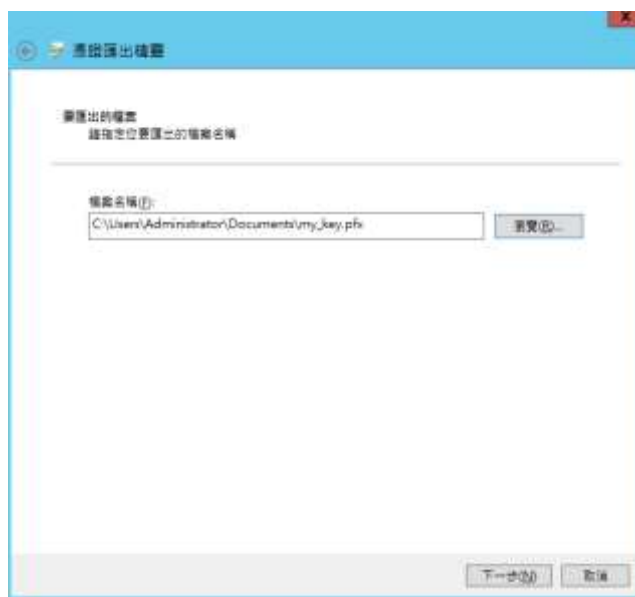
確認密碼(C):
●●●●●●●●

下一步(N) 取消

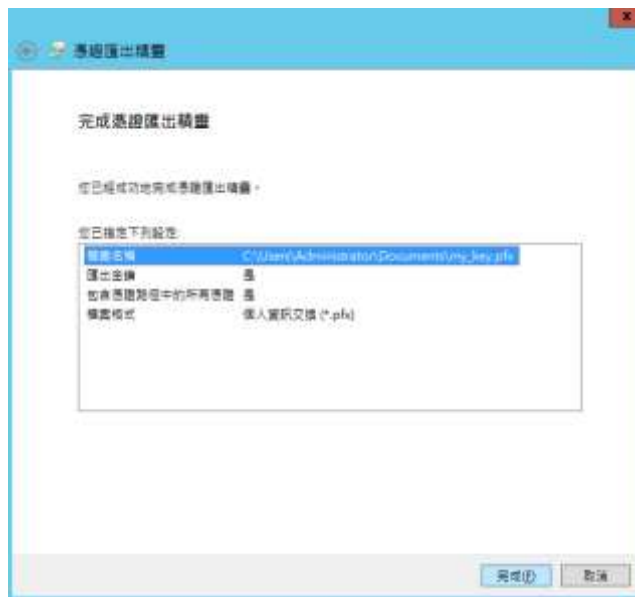
點選【瀏覽】指定存放的路徑後選擇【存檔】



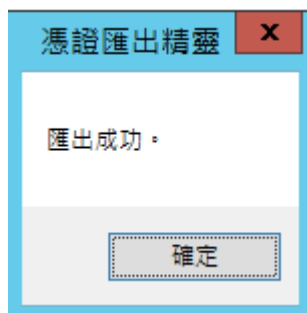
點選【下一步】繼續



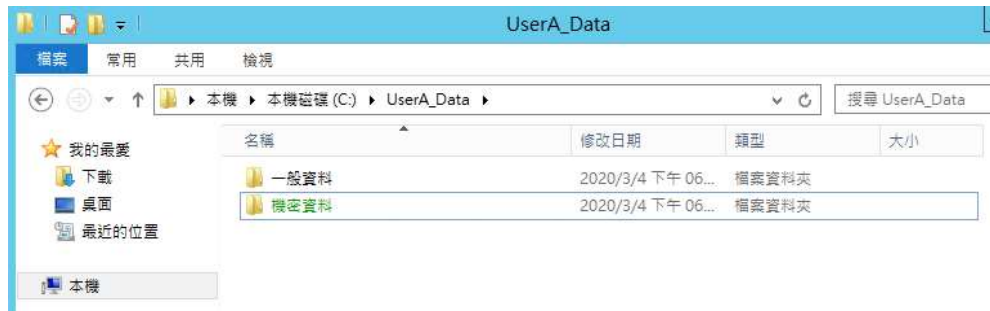
點選【完成】



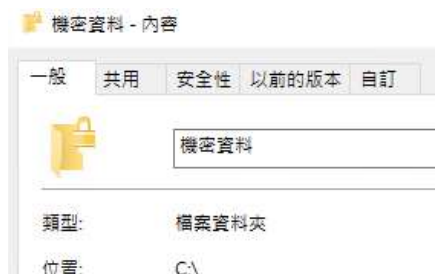
點選確定，完成設定



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



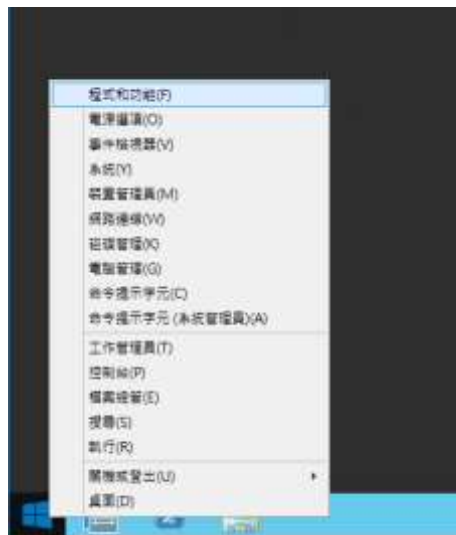
A-2. BitLocker 加密(需重啟 Windows Server)

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



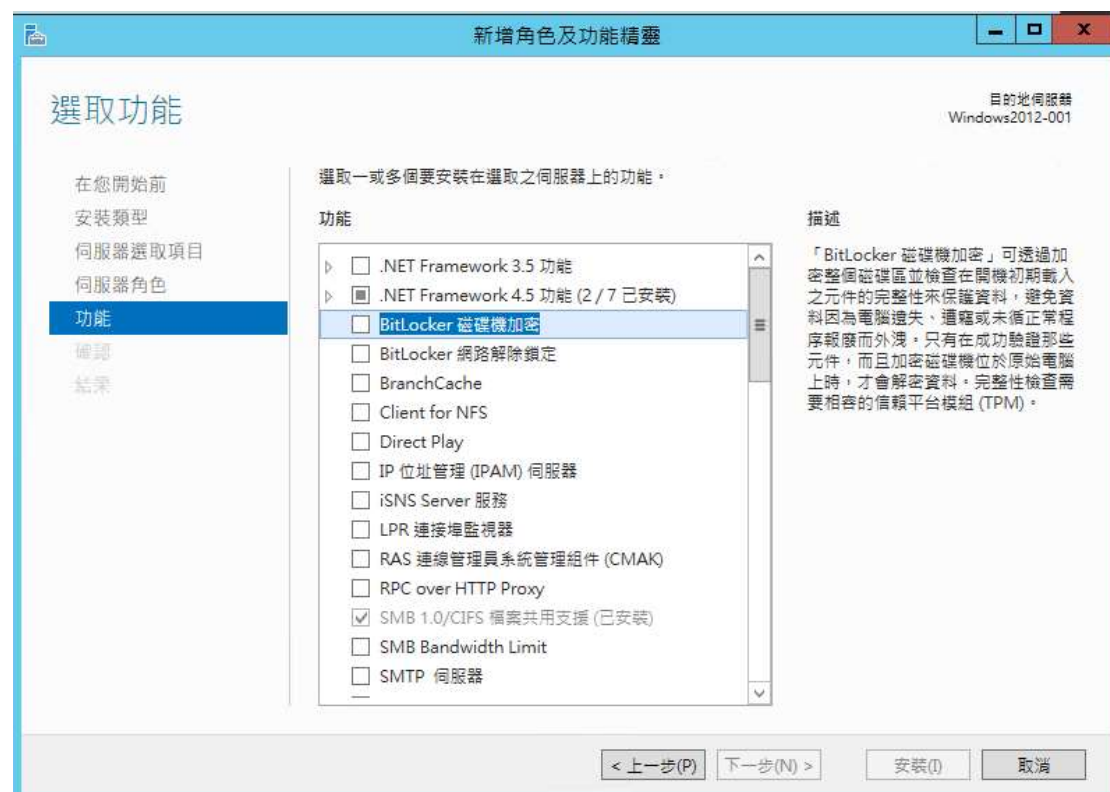
點選【下一步】繼續



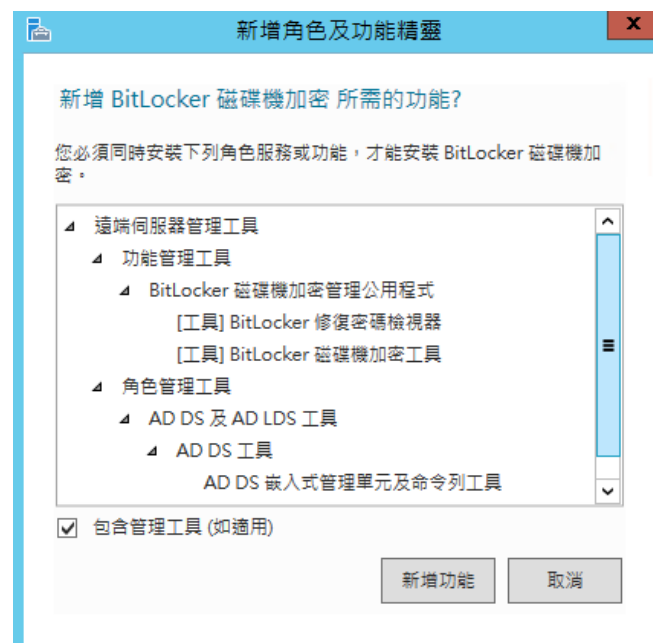
點選【下一步】繼續

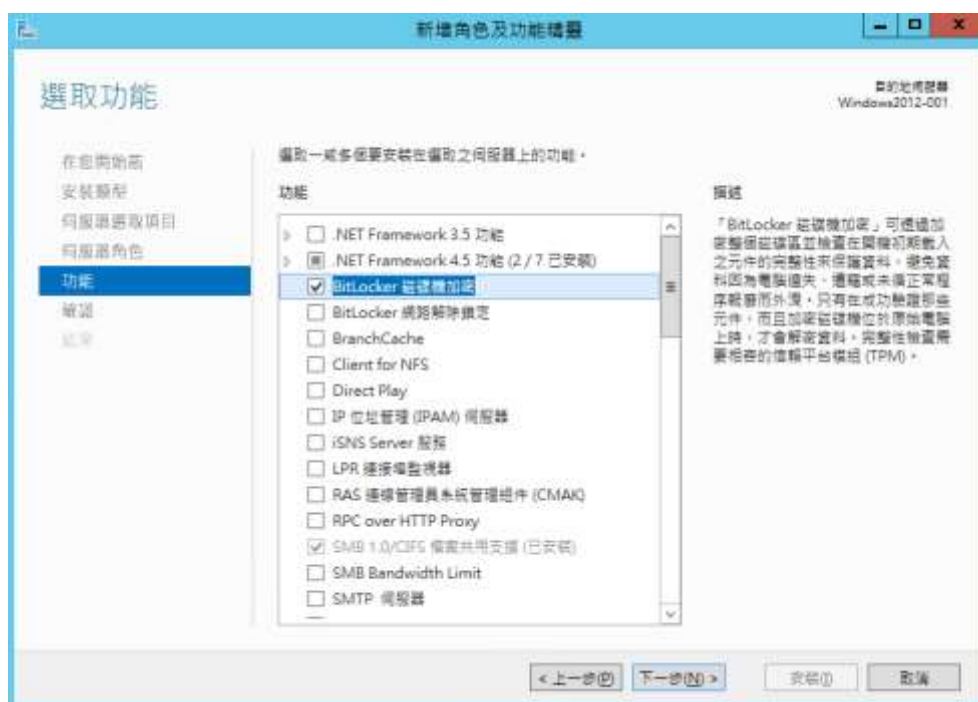


勾選【BitLocker 磁碟機加密】



勾選【新增功能】後點選【下一步】

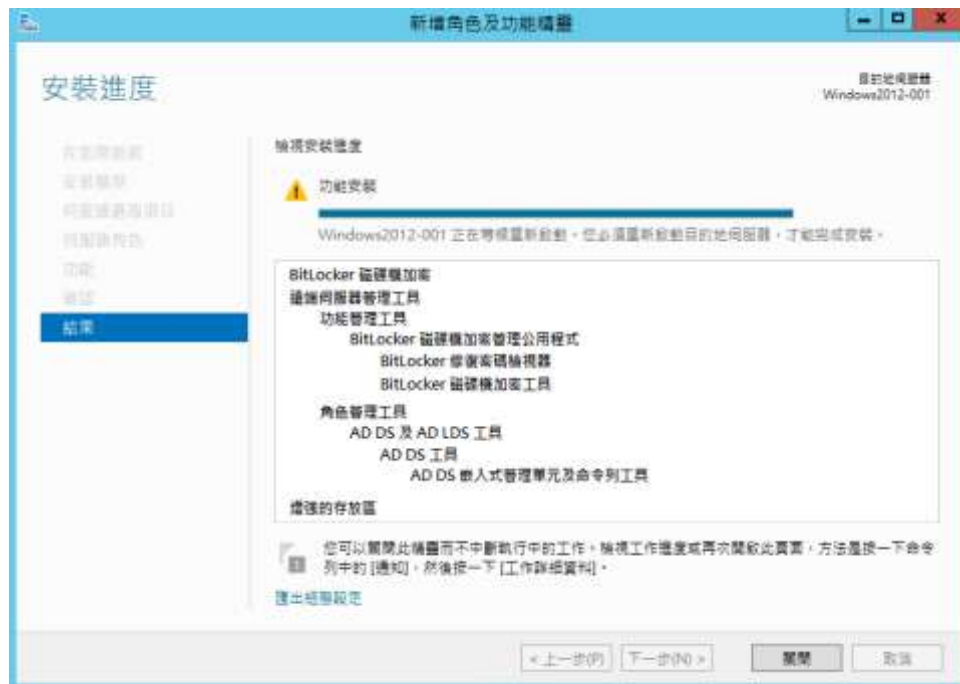




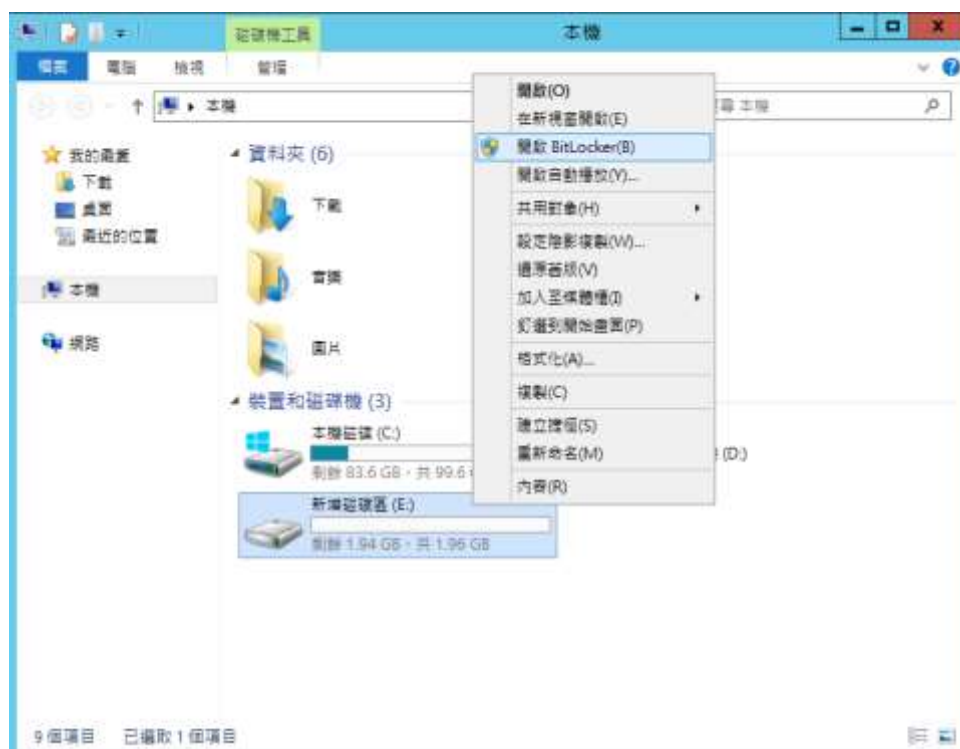
點選【安裝】



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】



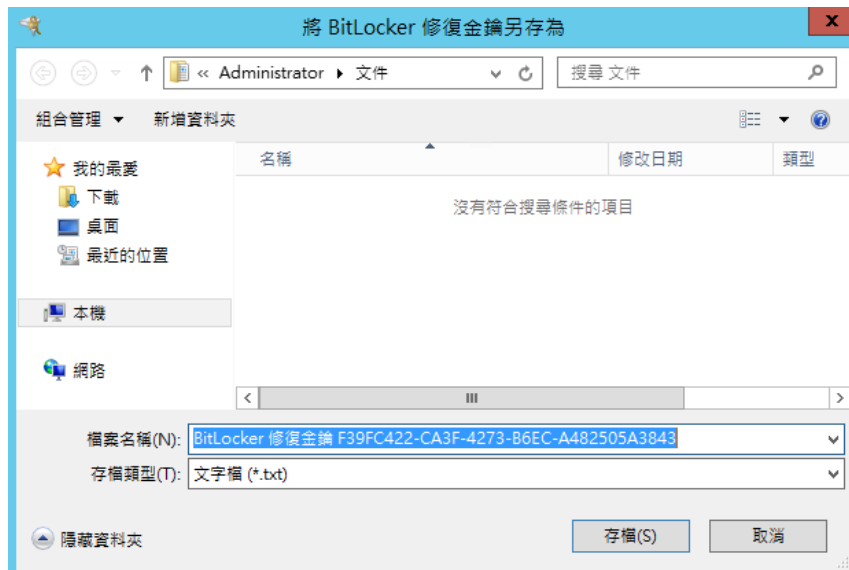
輸入解除鎖定的密碼之後按【下一步】



選擇儲存到檔案備份修復金鑰

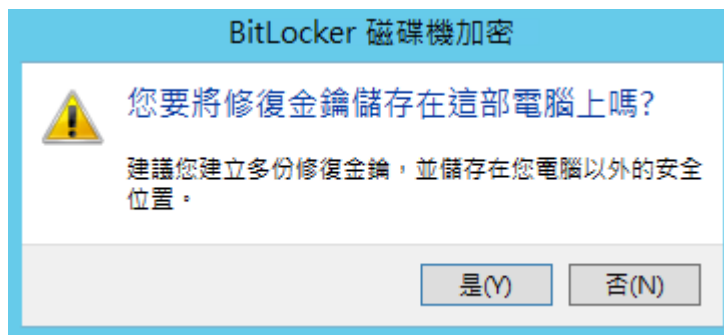


指定保存路徑

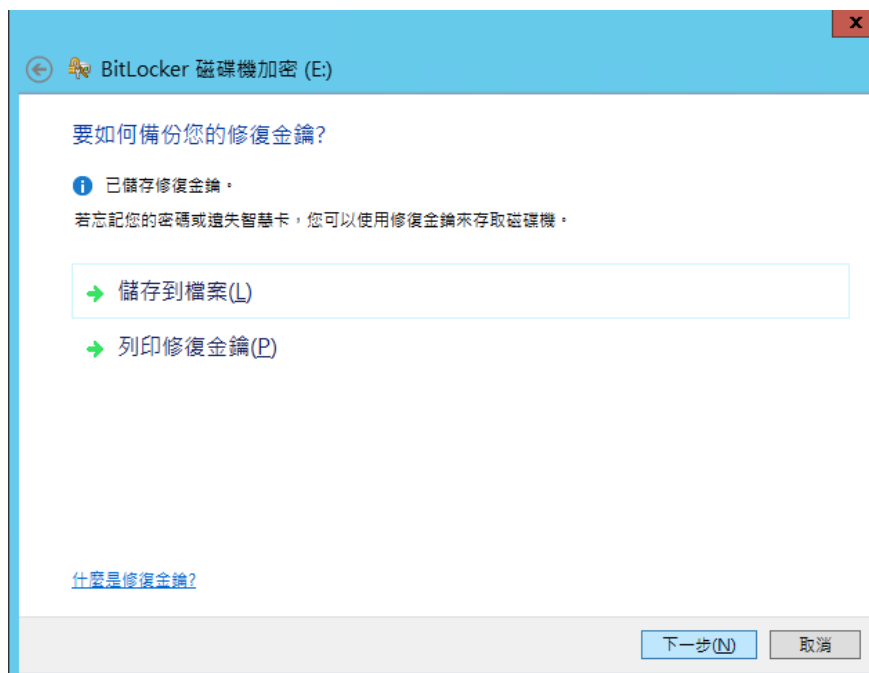


建議遵循系統提示將檔案存放多份副本在本機以外的空間，提醒您請妥善保存

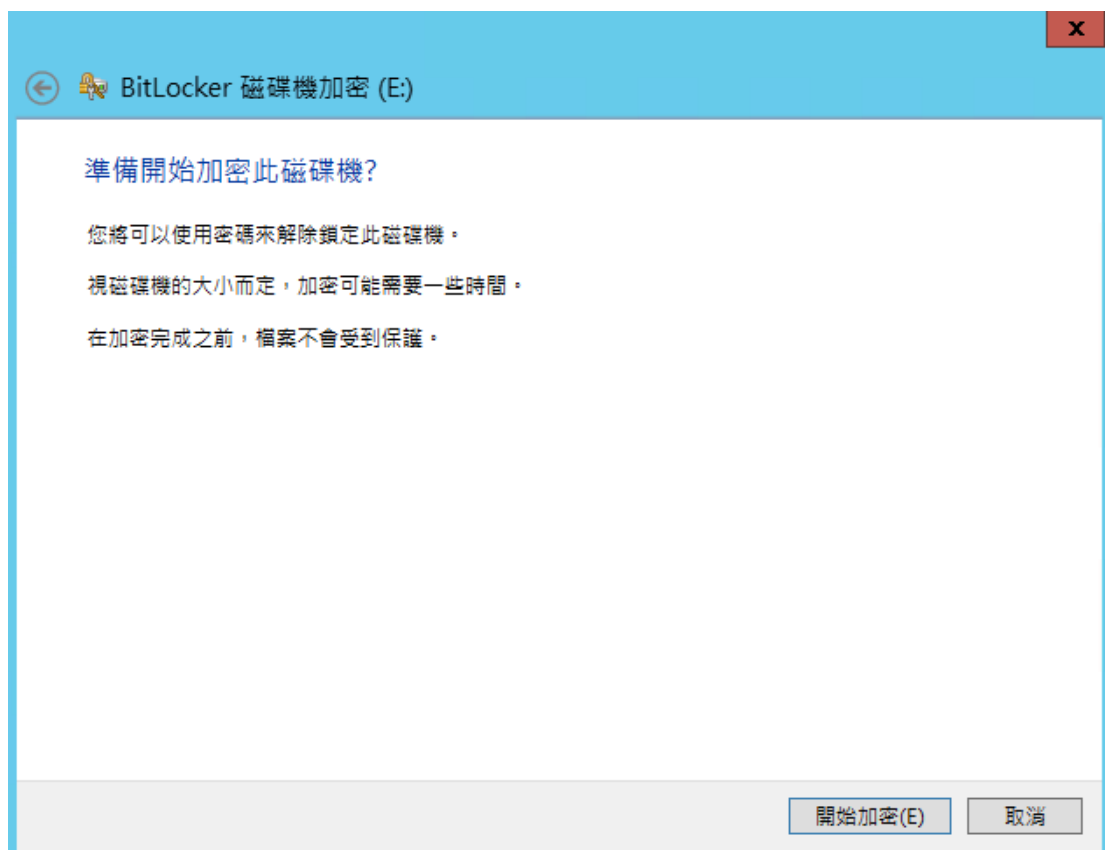
金鑰。



點選【下一步】



點選【開始加密】



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
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-size 256  
luksFormat /dev/sdb1
```

```
[root@centos77-template-001 ~]# cryptsetup --verify-passphrase --cipher aes-cbc-essiv:sha256 --key-size 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.

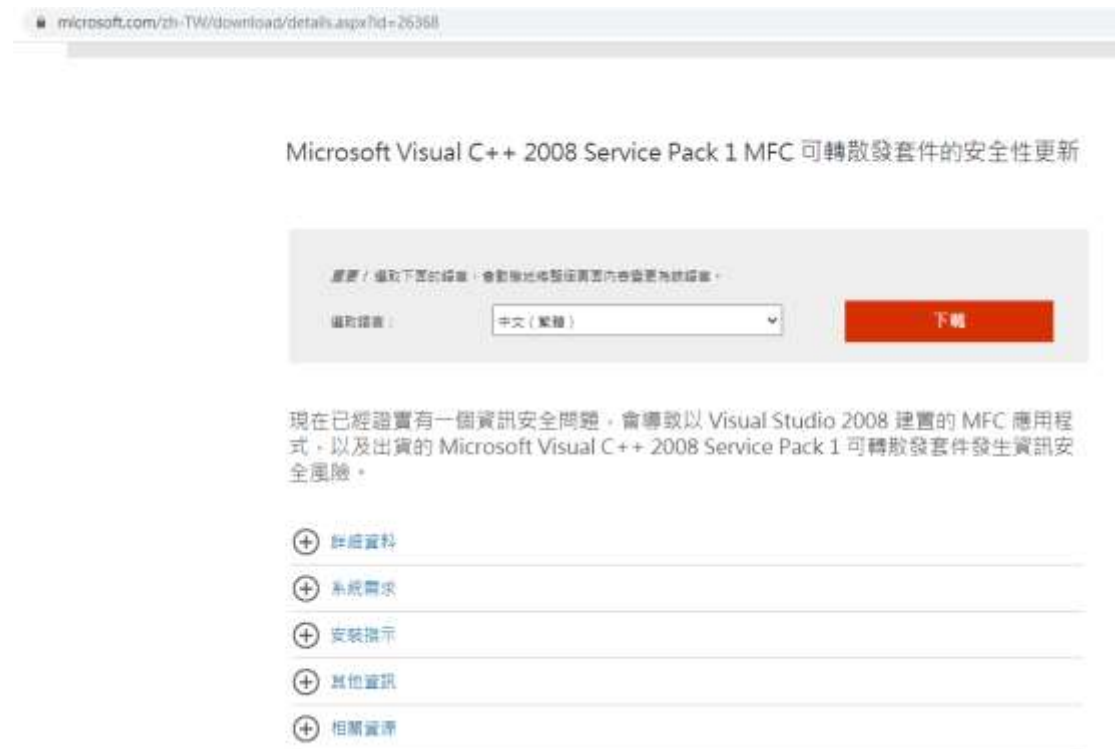
Workaround

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>

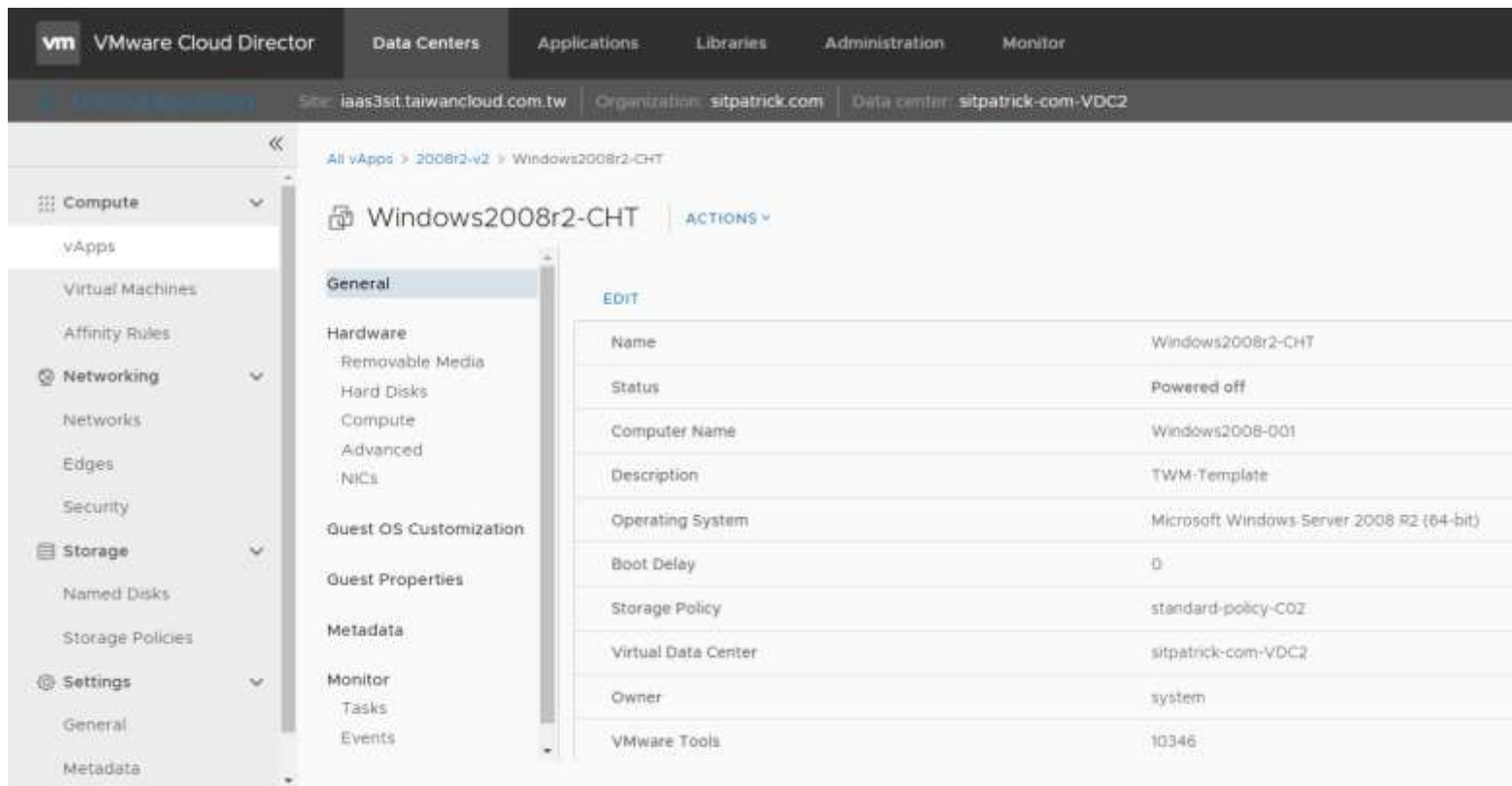


安裝完成後客體自訂功能就會生效，可以使用客體自訂修改系統管理員密碼。

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



The screenshot shows the VMware Cloud Director web interface. The top navigation bar includes 'vmware Cloud Director', 'Data Centers', 'Applications', 'Libraries', 'Administration', and 'Monitor'. Below this, a breadcrumb trail indicates the path: 'All vApps > 2008r2-v2 > Windows2008r2-CHT'. The left sidebar contains a tree view with categories like 'Compute', 'Networking', 'Storage', and 'Settings'. The main content area displays the configuration for the 'Windows2008r2-CHT' virtual machine. A left-hand menu lists various settings: General, Hardware, Guest OS Customization, Guest Properties, Metadata, Monitor, Tasks, and Events. The 'General' tab is selected, showing a table of properties. An 'EDIT' button is visible above the table.

EDIT	
Name	Windows2008r2-CHT
Status	Powered off
Computer Name	Windows2008-001
Description	TWM-Template
Operating System	Microsoft Windows Server 2008 R2 (64-bit)
Boot Delay	0
Storage Policy	standard-policy-C02
Virtual Data Center	sitpatrick-com-VDC2
Owner	system
VMware Tools	10346

開機進入 BIOS 開關打開

Edit VM Windows2008r2-CHT



Name *

Windows2008r2-CHT

Computer Name *

Windows2008-001

Description

TWM-Template

Operating System Family

Microsoft Windows

Operating System

Microsoft Windows Server 2008 R2 (64-bit)

Boot Delay *

0

Storage Policy

standard-policy-C02

Enter BIOS Setup



DISCARD

SAVE

點選 Action 選擇 Insert Media

Power On
Power On and Force Recustomization
Power Off
Shut Down Guest OS
Reset
Suspend
Discard suspended state
Copy to
Move to
Delete
Change Owner
Launch Web Console
Launch VM Remote Console
Download VMRC
Create Snapshot
Revert to Snapshot
Remove Snapshot
Insert Media
Eject Media

放入 Ubuntu 開機光碟

Insert CD



Select the media file to insert in the VM.

Media available now:

Name	Catalog	Owner	Created On	Storage Used
ubuntu-18.04.5-desktop-amd64.iso	myiso	system	12/16/2020, 10:17:59 AM	2091.91 MB
win2016r2chtsp2	myiso	twmadmin	12/15/2020, 7:56:08 PM	3068.57 MB
win2016chtsp2-ISO	ISO	system	12/15/2020, 7:39:26 PM	3068.57 MB
ubuntu-20.04.1-desktop-amd64.iso	myiso	twmadmin	12/15/2020, 8:18:43 PM	2656.00 MB

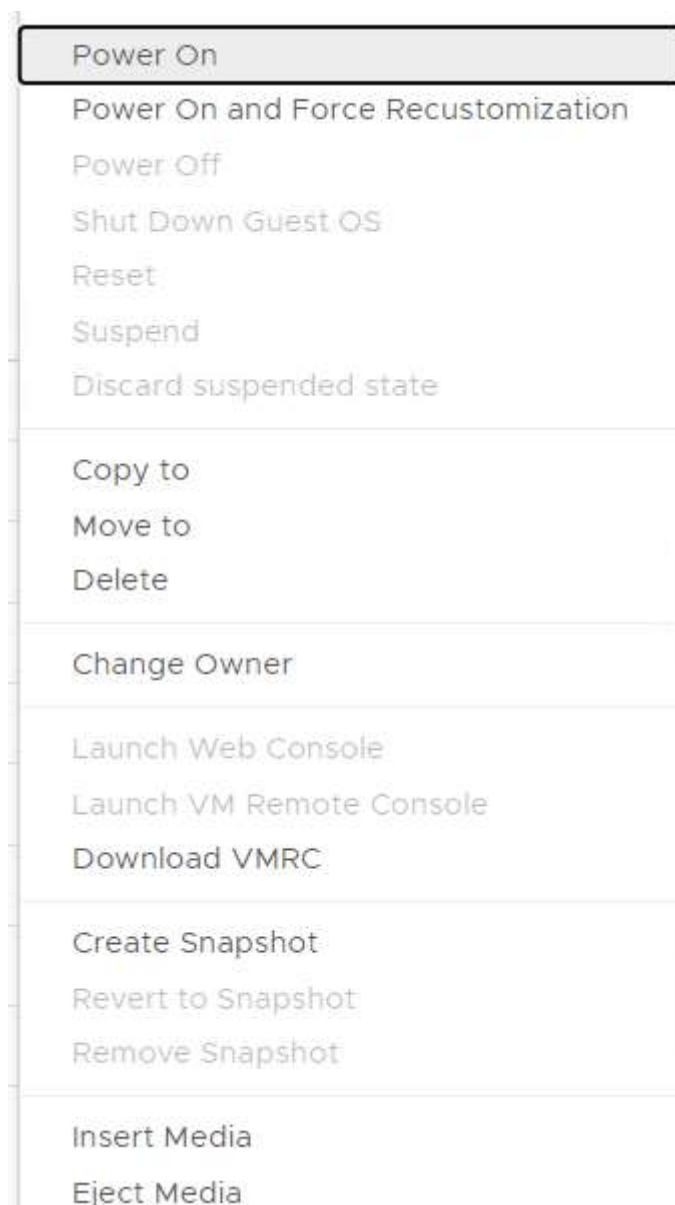
1 - 4 of 4 media

Selected media: ubuntu-18.04.5-desktop-amd64.iso

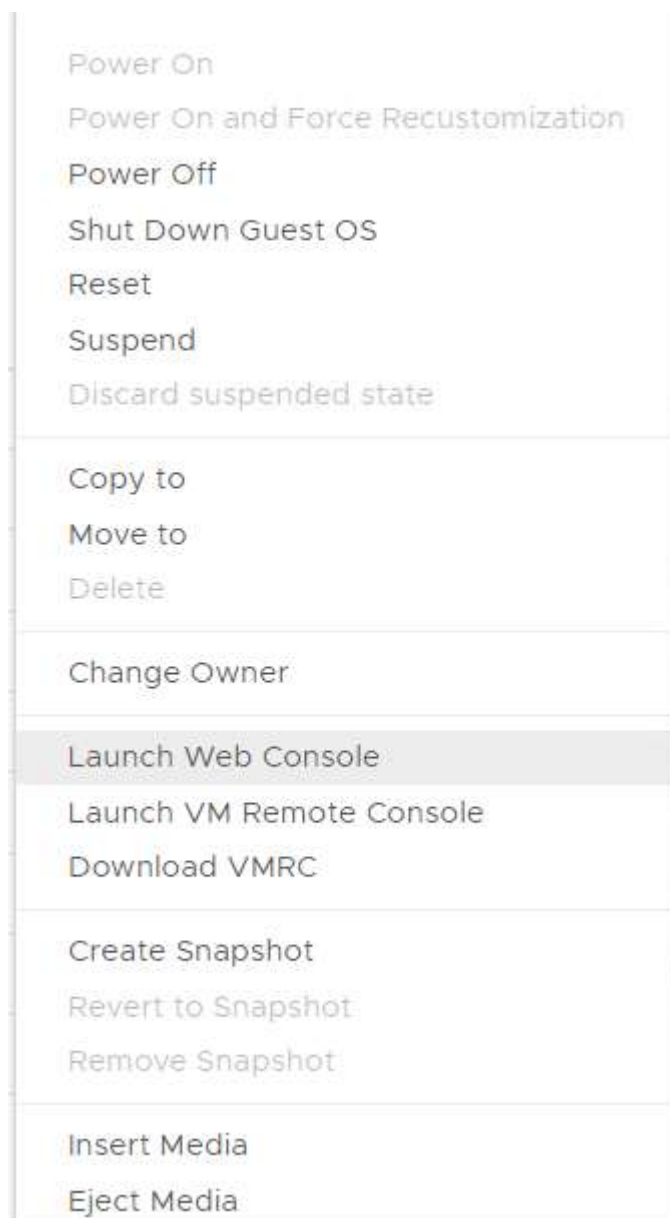
CANCEL

INSERT

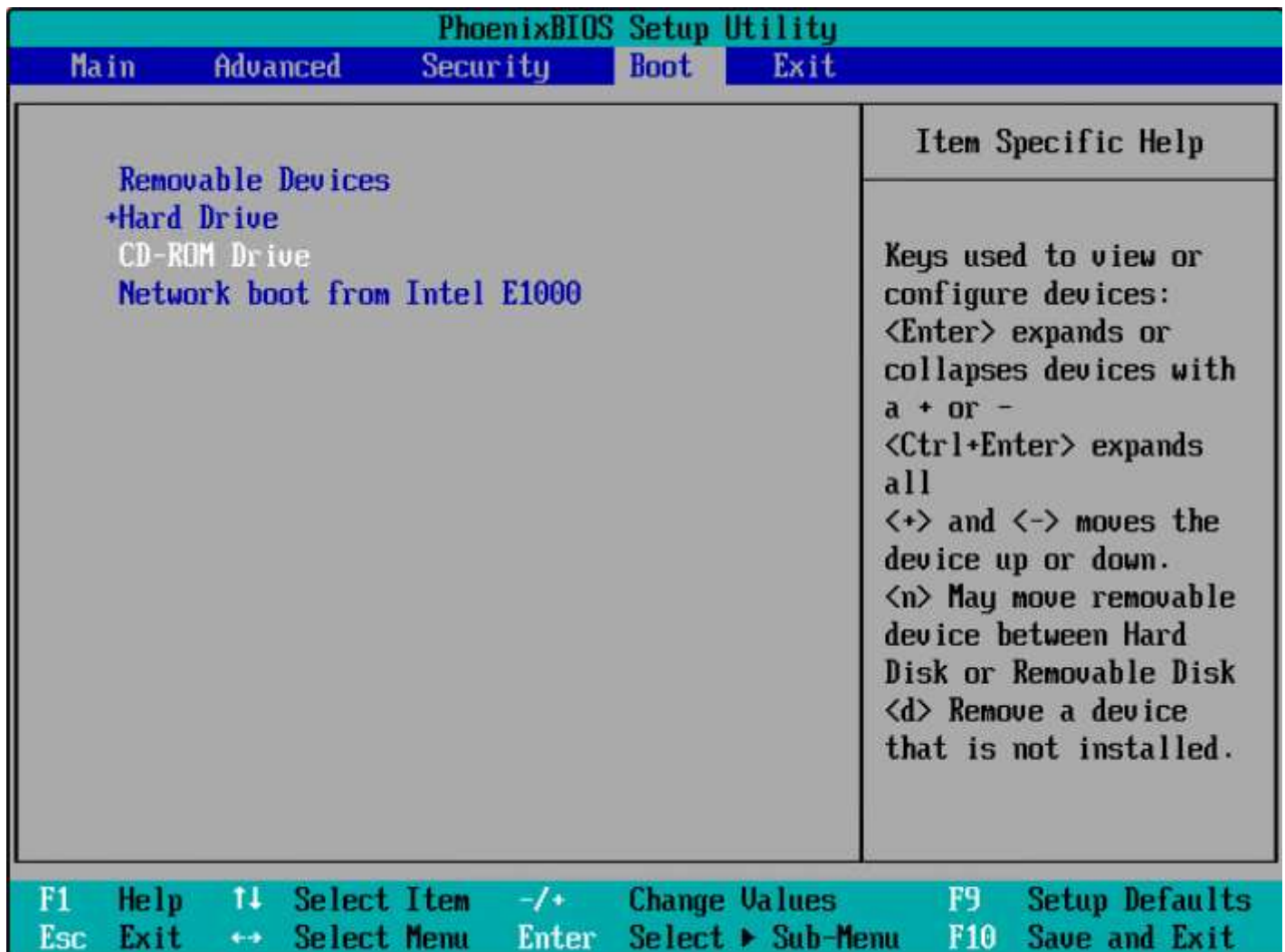
點選 Action 將 VM 開機



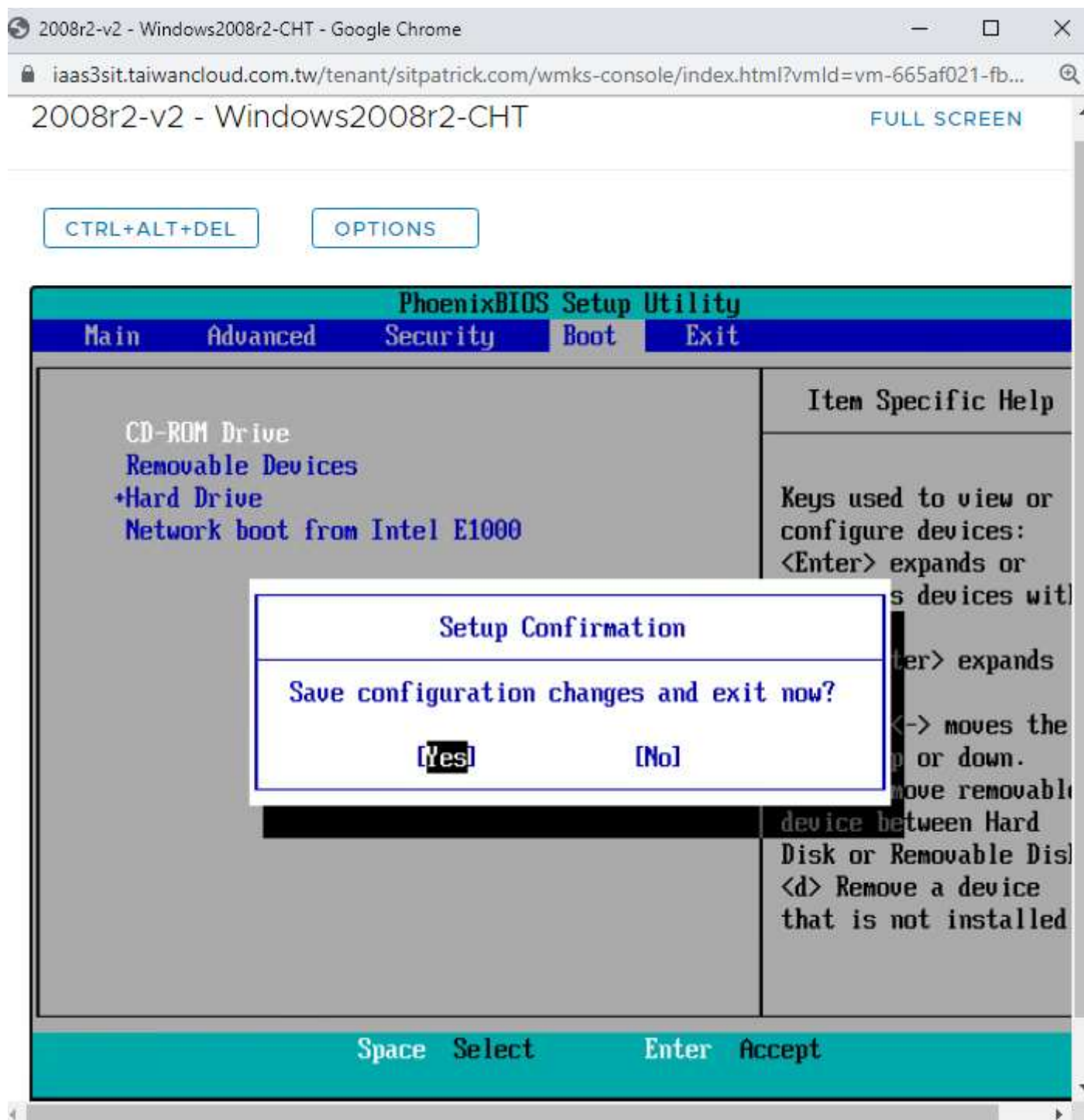
點選 Action 開啟 VM Console



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



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

2008r2-v2 - Windows2008r2-CHT

FULL SCREEN

CTRL+ALT+DEL

OPTIONS



Connected.

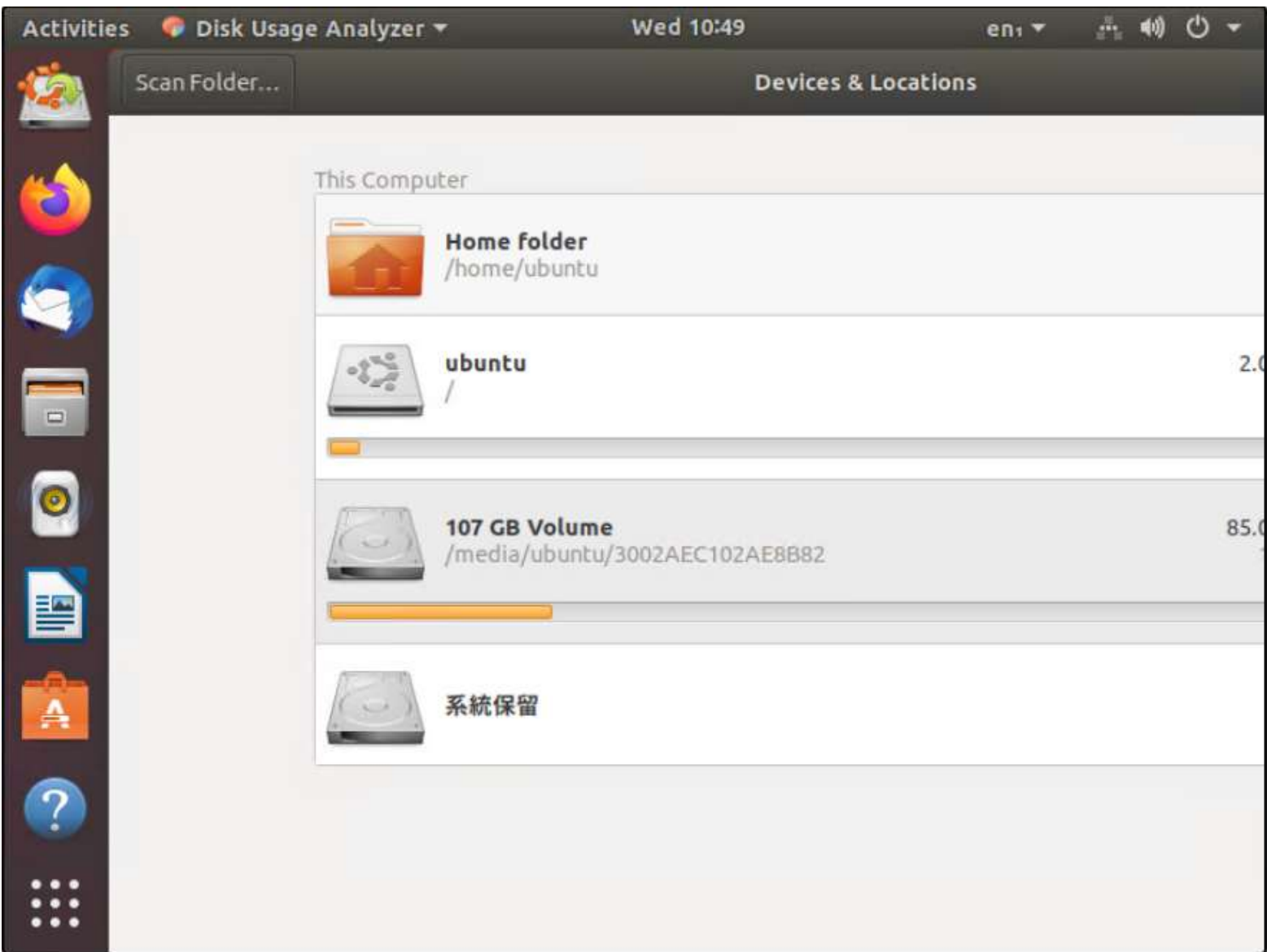
系統將會載入 ubuntu 桌面點選左下角圖示



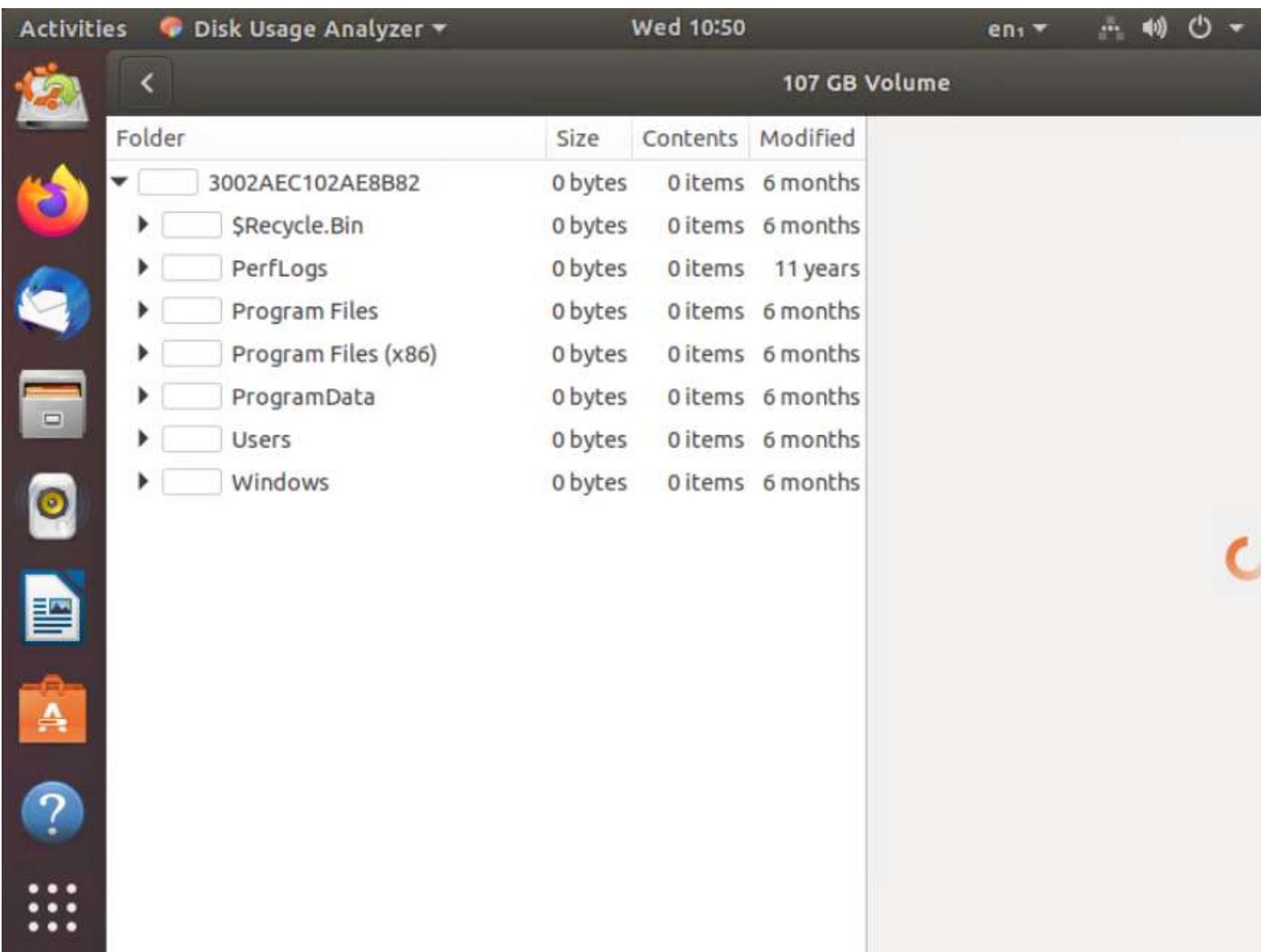
選擇 DISK...



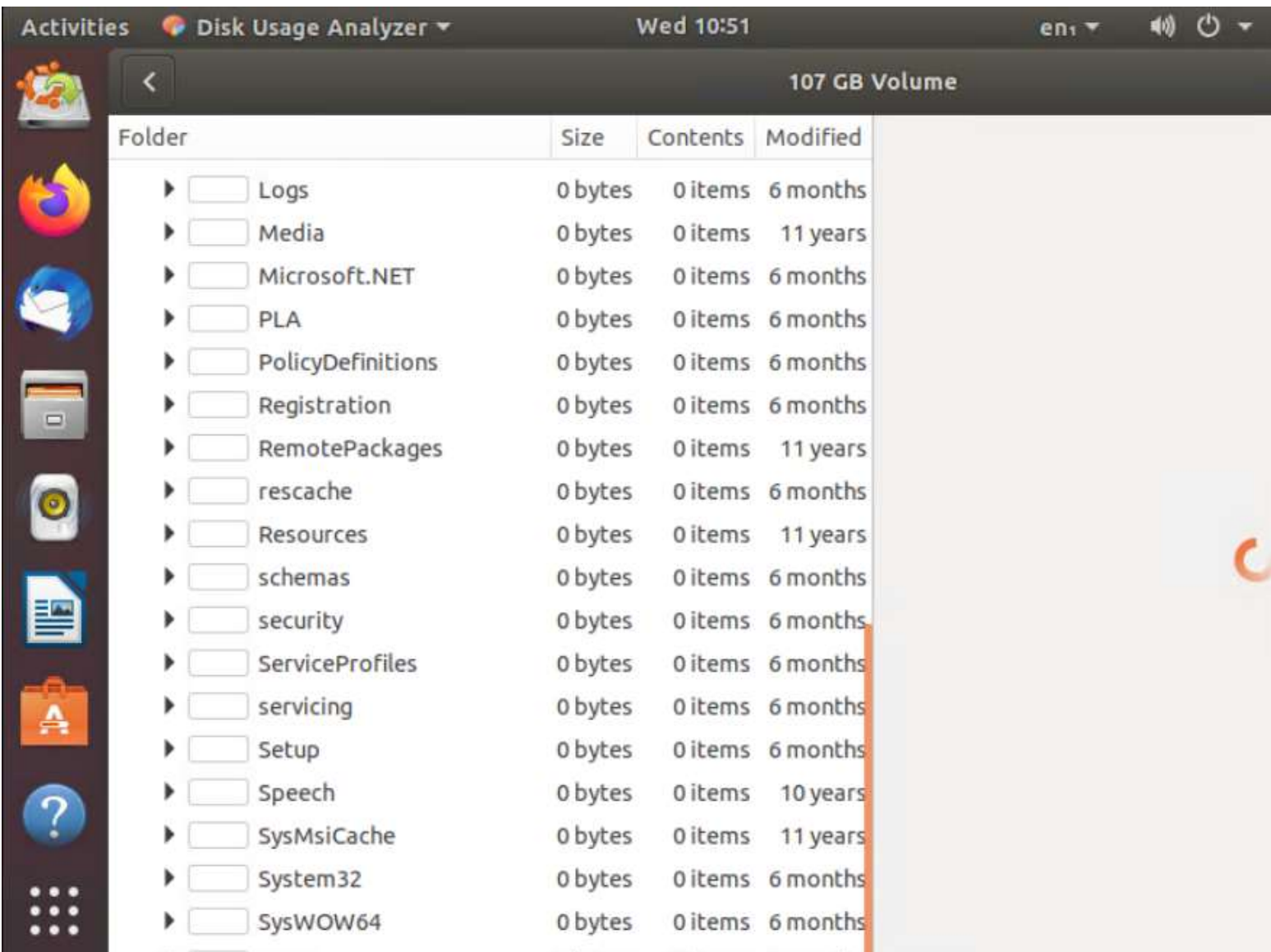
選擇大小約 100G 的磁碟



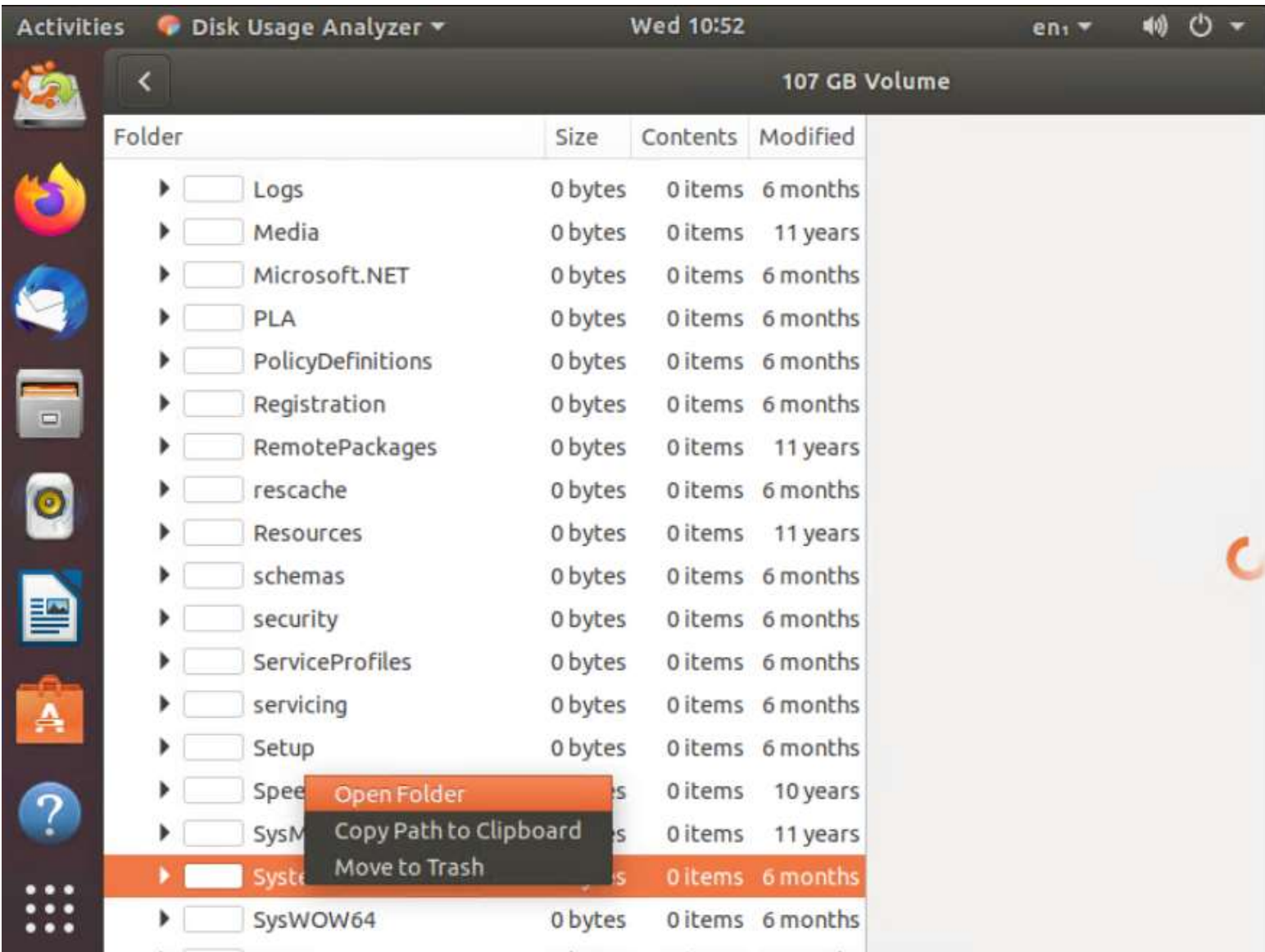
選擇 Windows



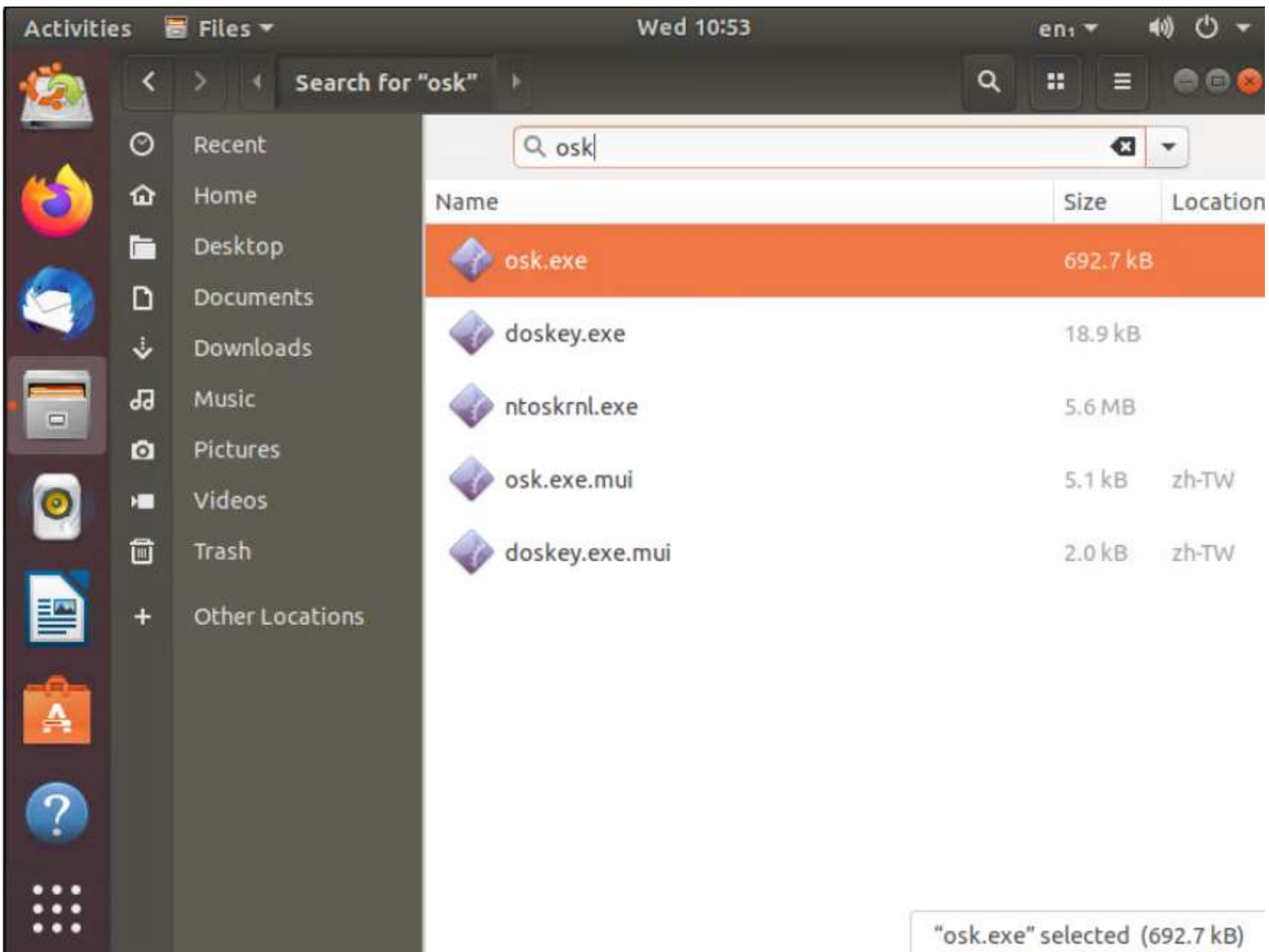
往下找到 system32



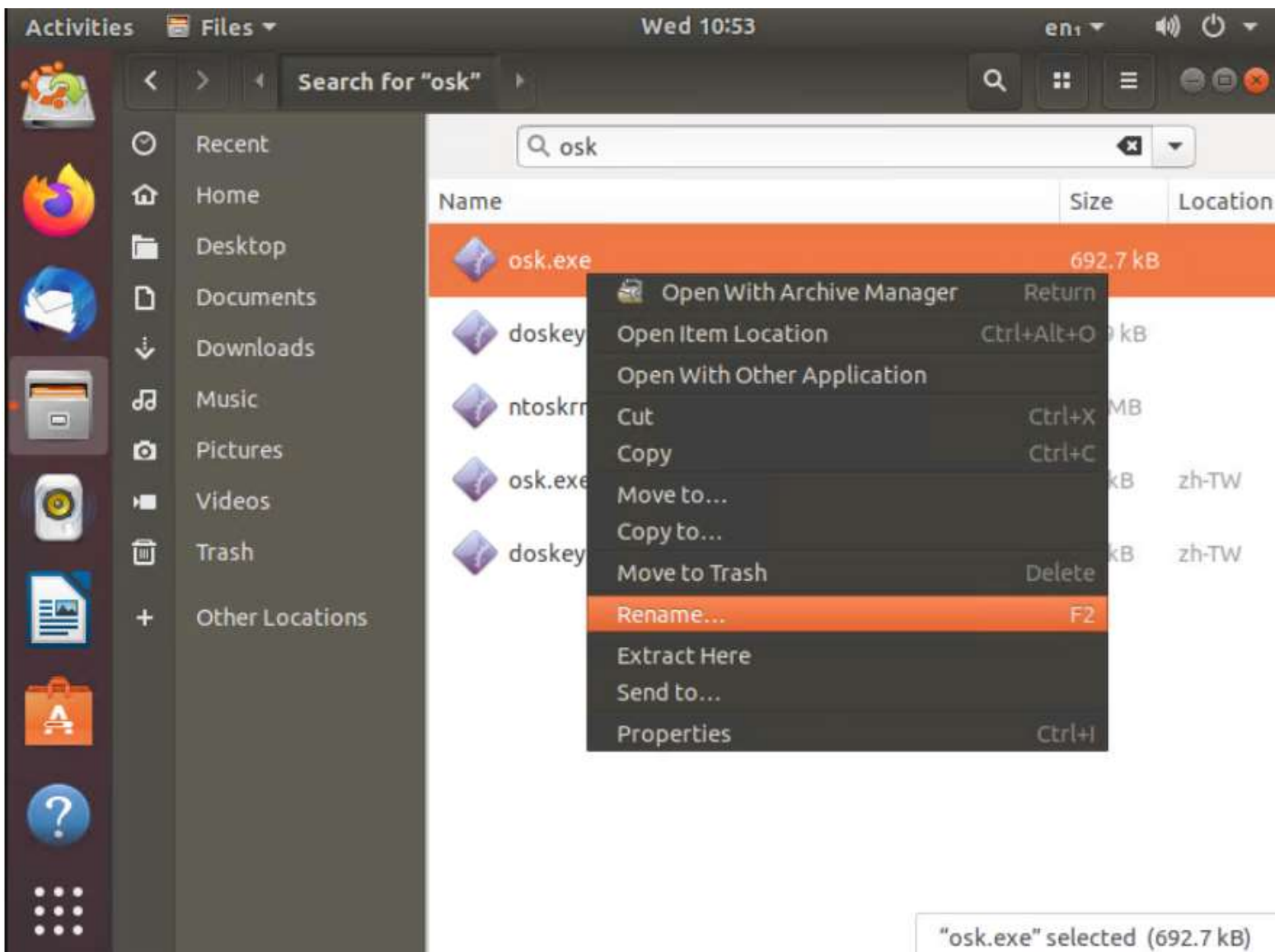
按右鍵選擇 Open Folder

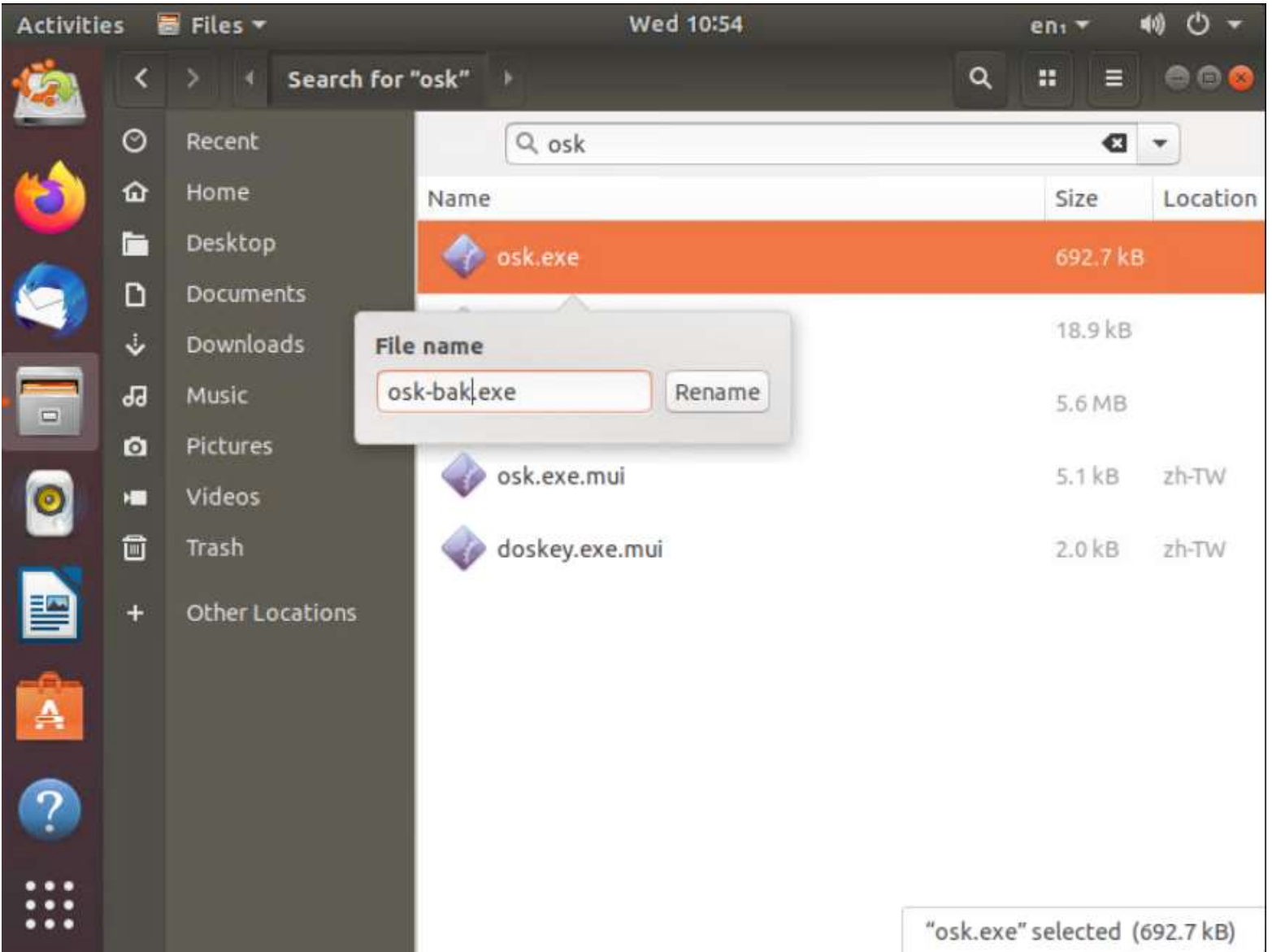


點選右邊搜尋圖示 輸入 osk

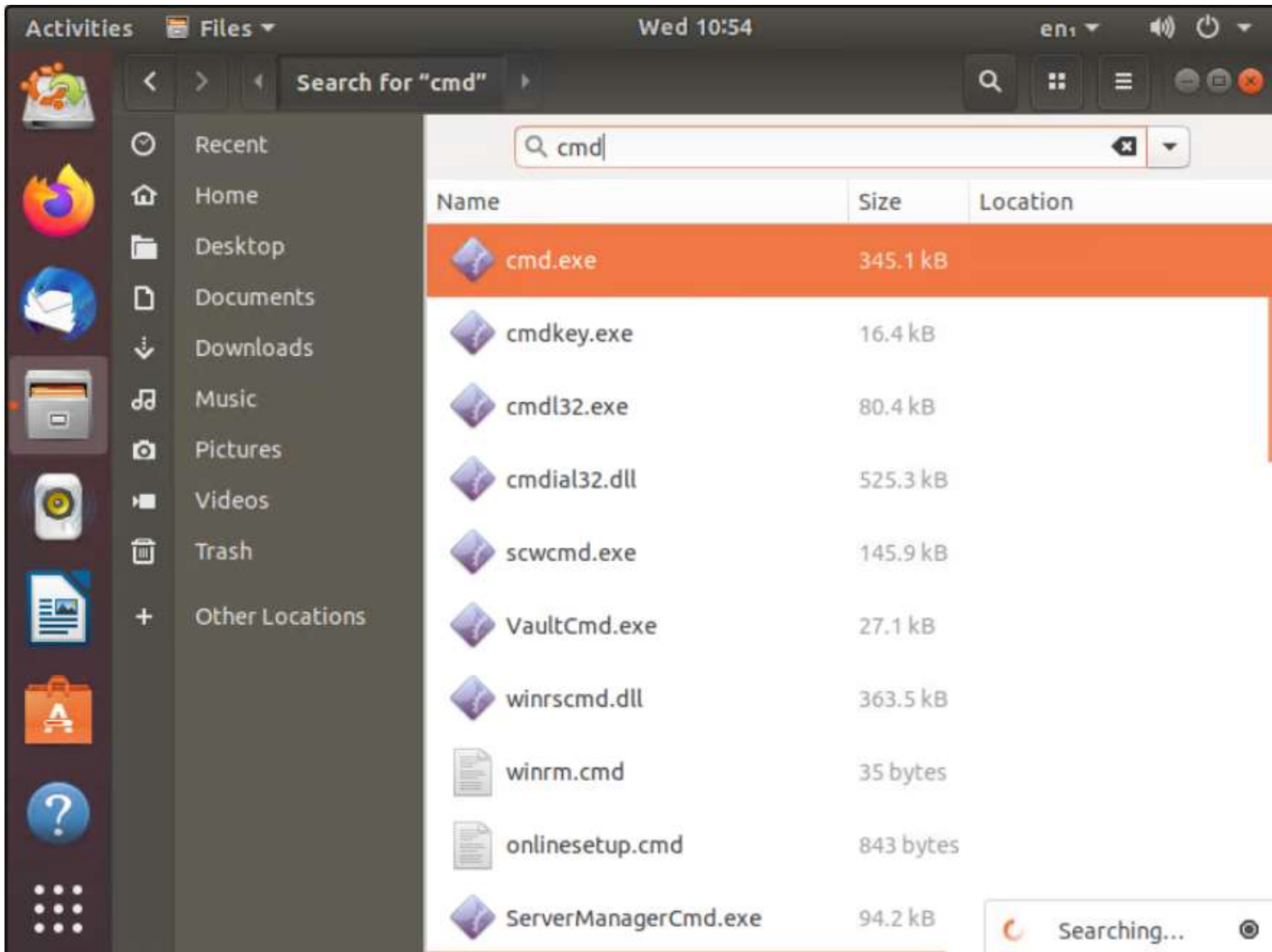


找到 osk.exe 按右鍵選擇 Rename

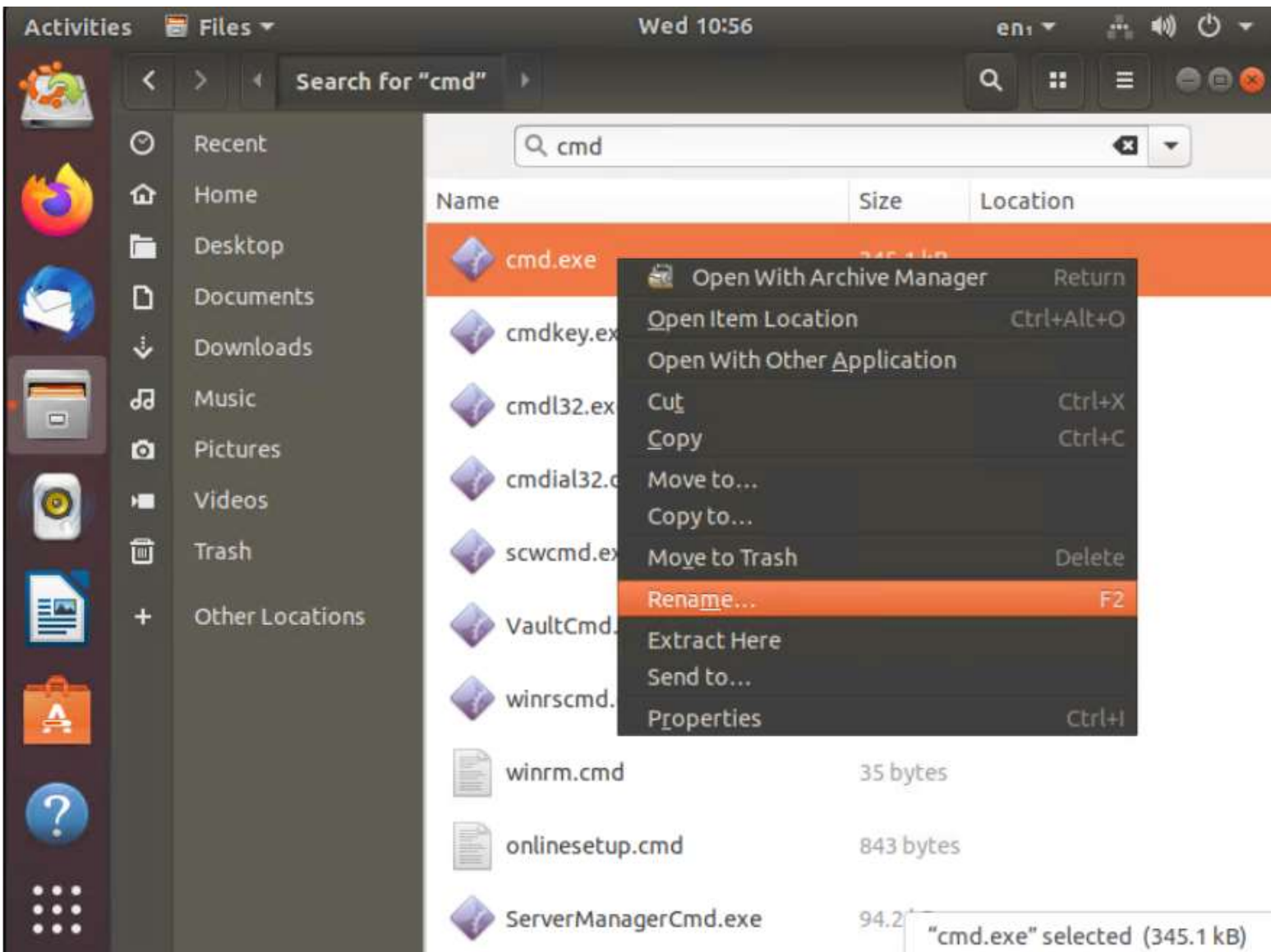


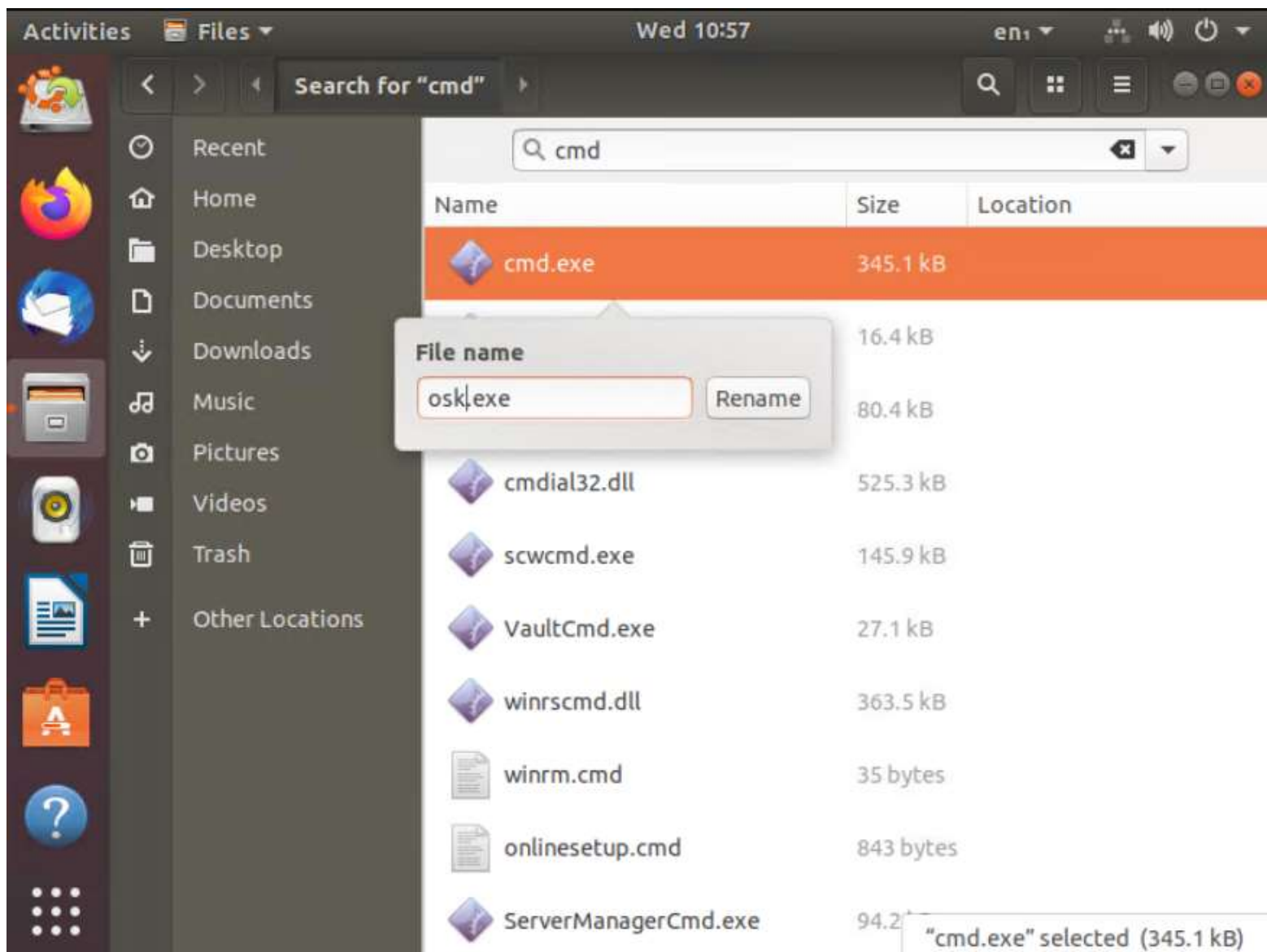


再搜尋 cmd

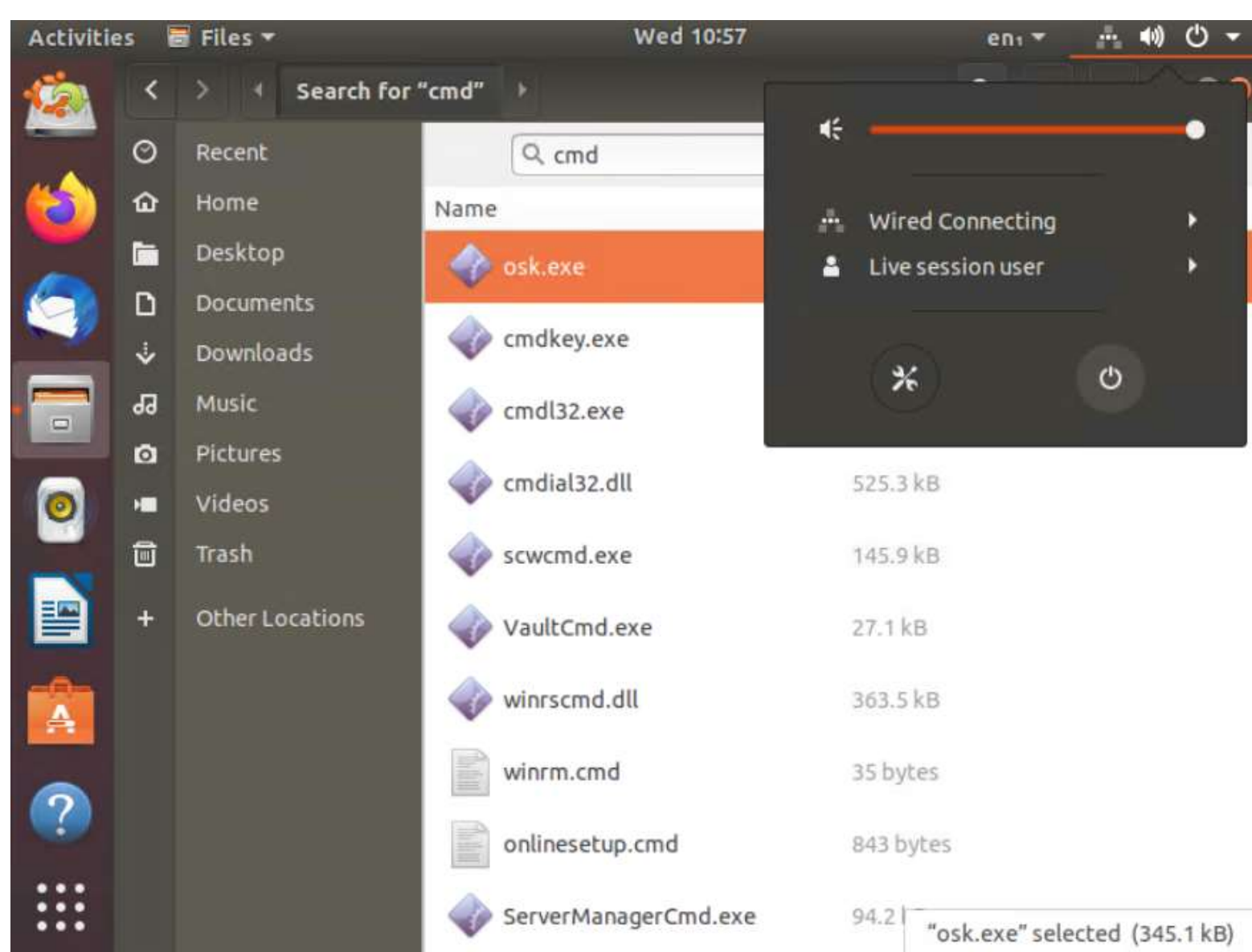


將 cmd.exe 按右鍵將檔名改為 osk.exe

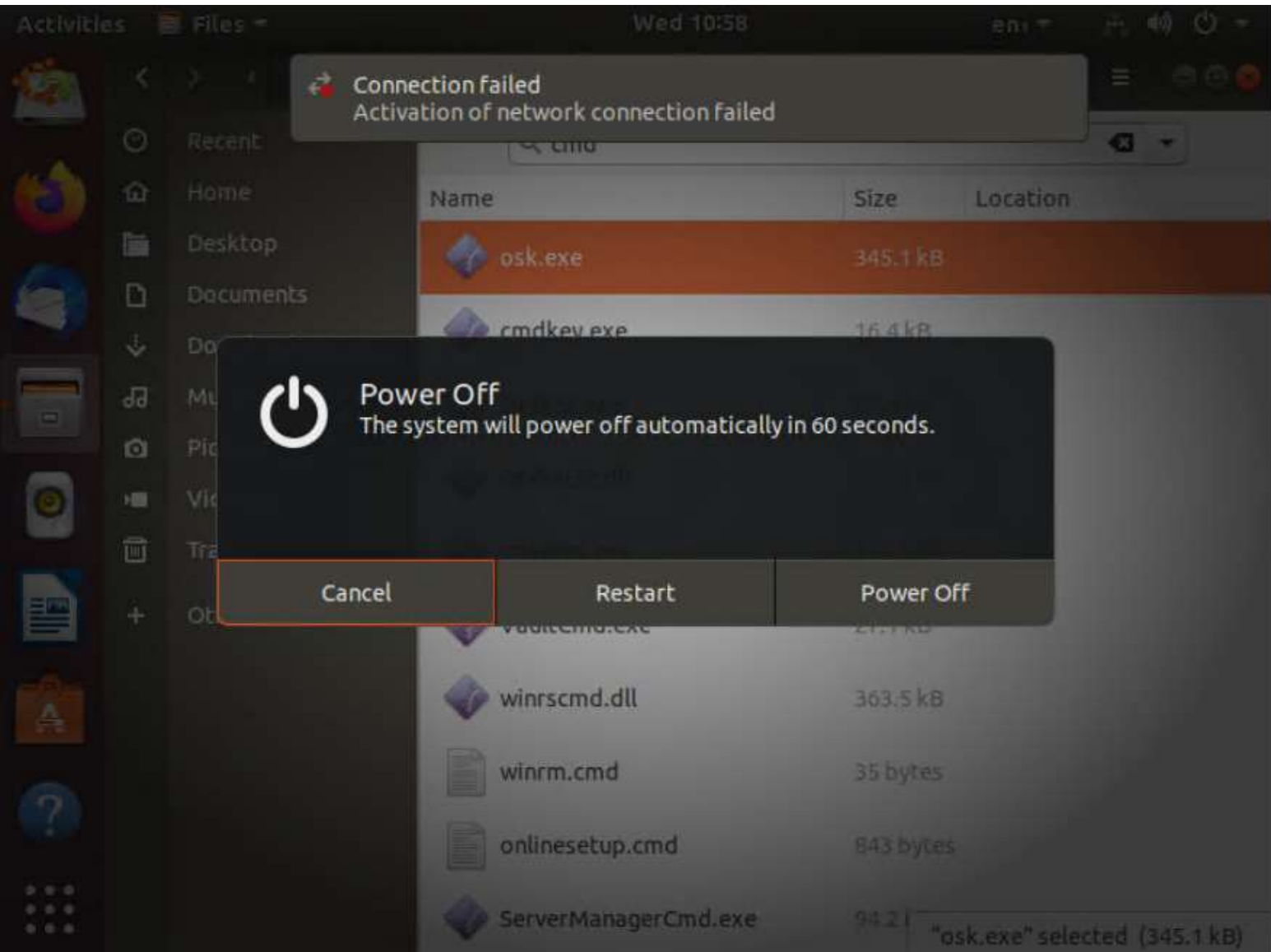




改好後準備重新開機點選右上角電源選項



選擇 restart 重開機



重開機後會到以下畫面，按 ENTER

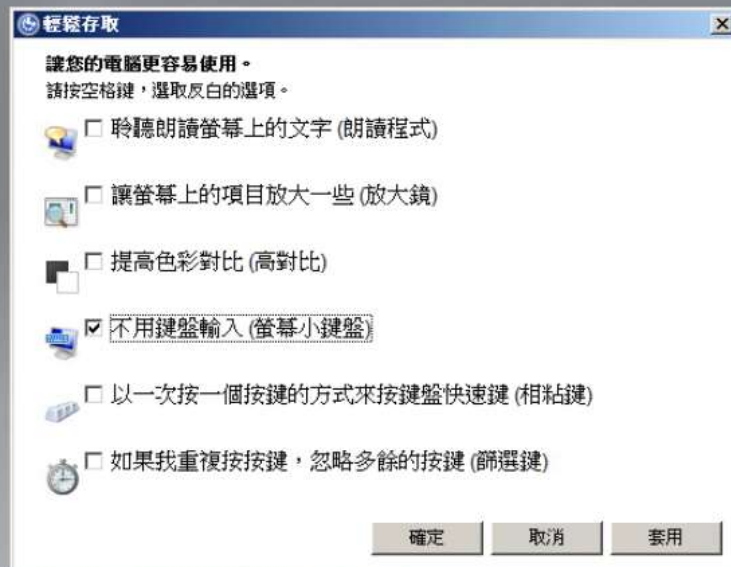


3. Windows 重設密碼作業

重開機後系統會進入原 Windows 系統



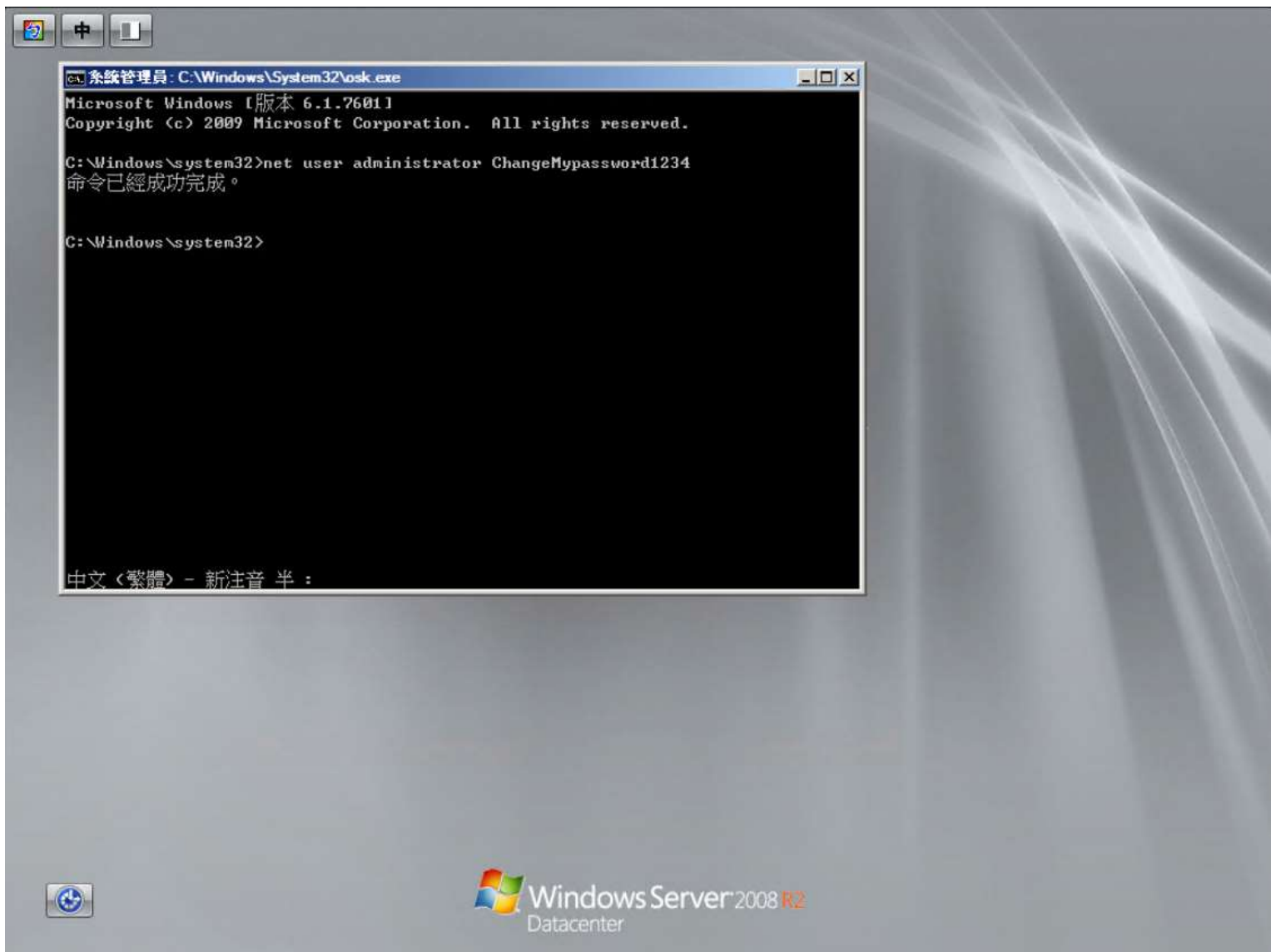
點選左下角輕鬆存取,勾選不用鍵盤輸入(螢幕小鍵盤),點選確定



TE 來登入

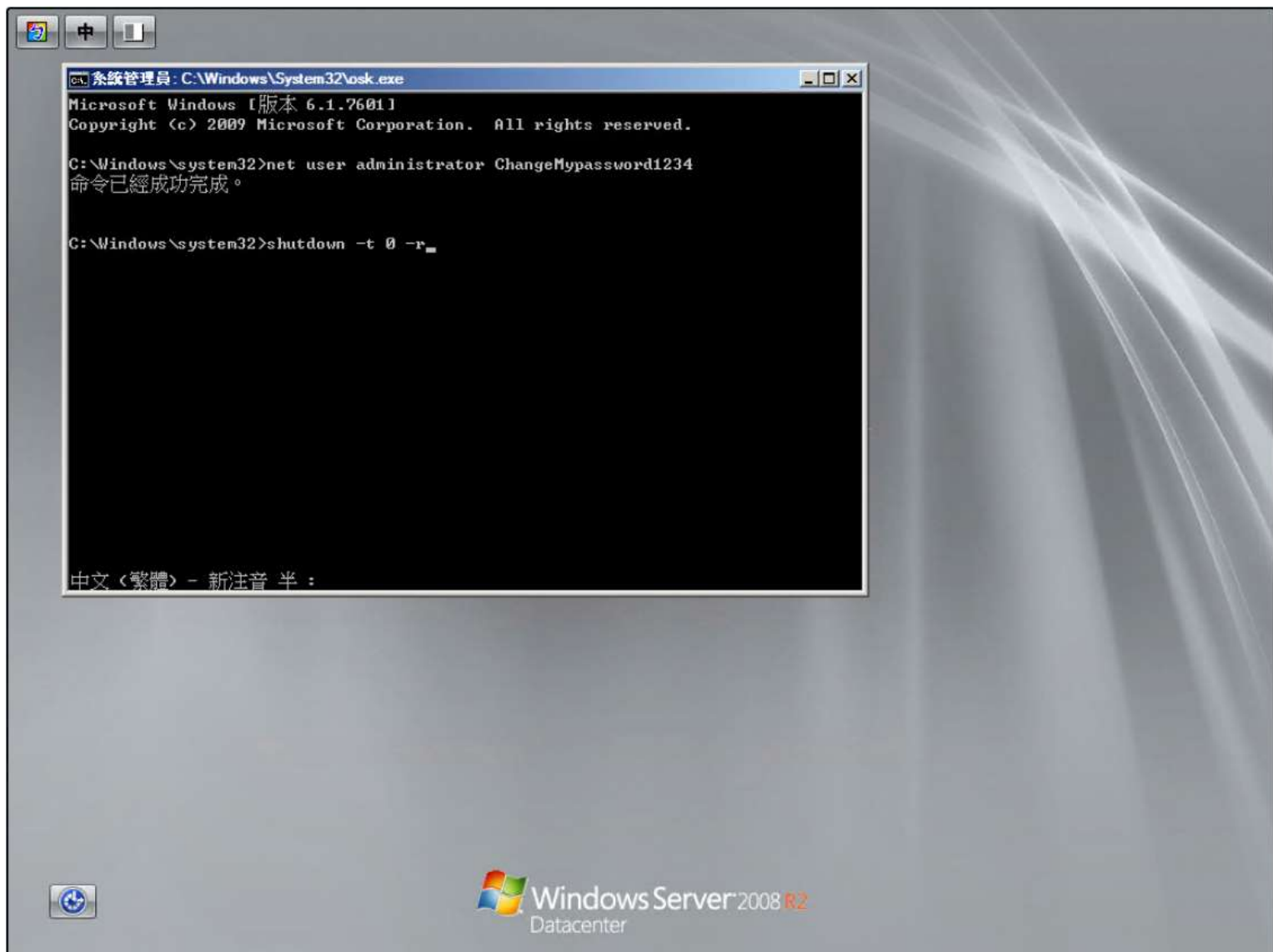
系統會出現命令提示元 請輸入以下格式修改密碼

net user 使用者名稱 密碼

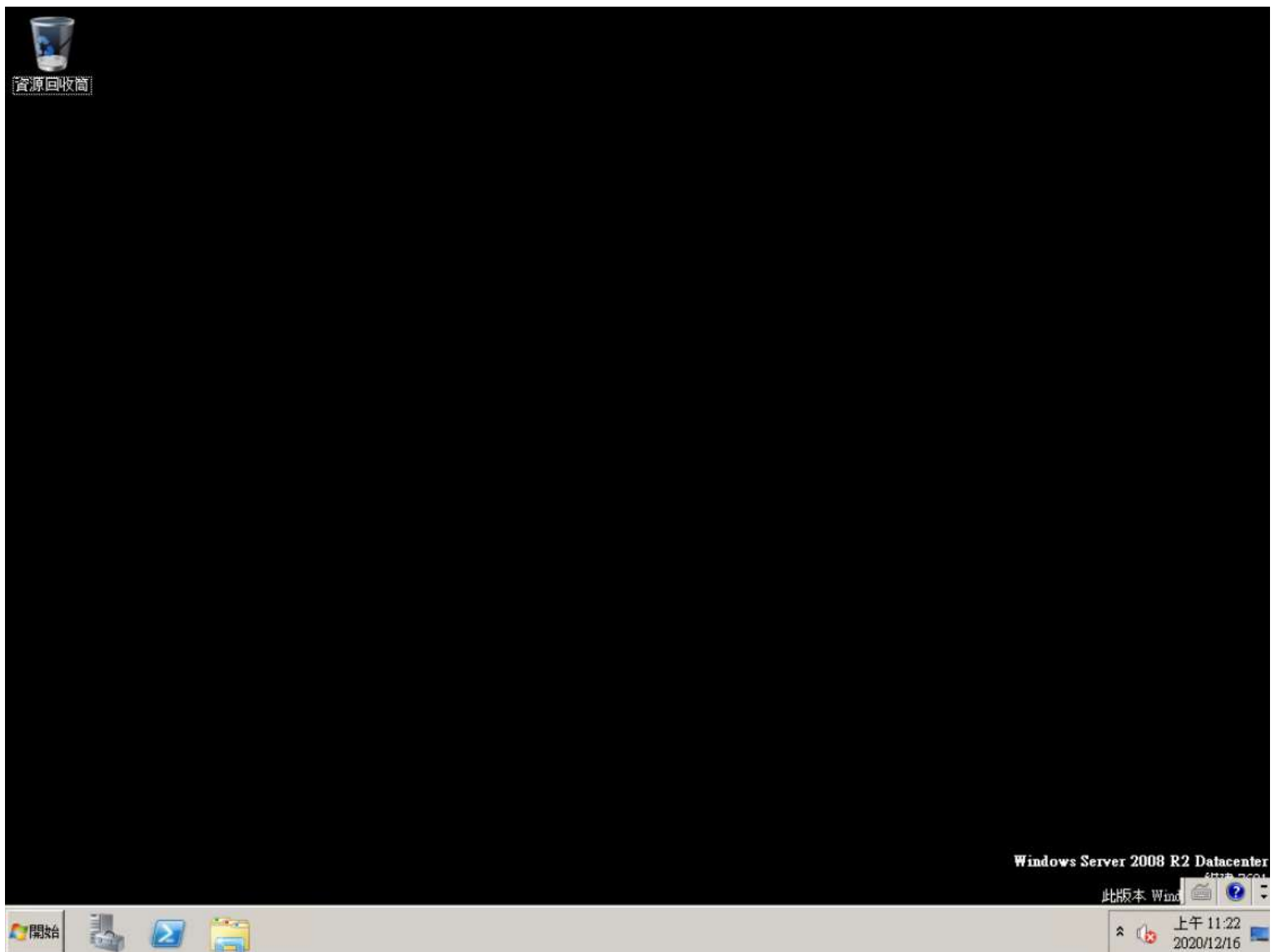


輸入以下指令重新開機

shutdown -t 0 -r



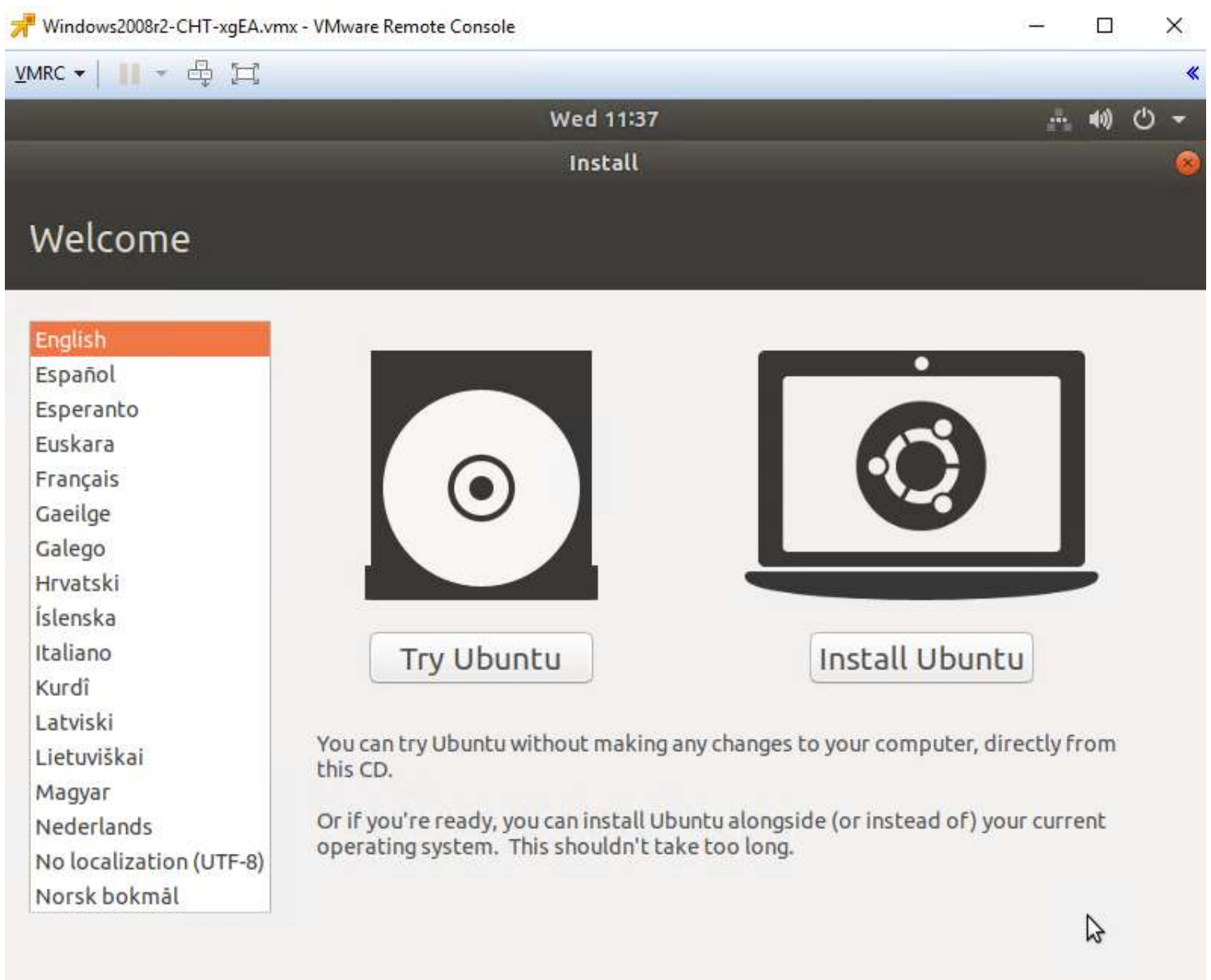
開機後以新的密碼登入



4. 復原先前的變更作業

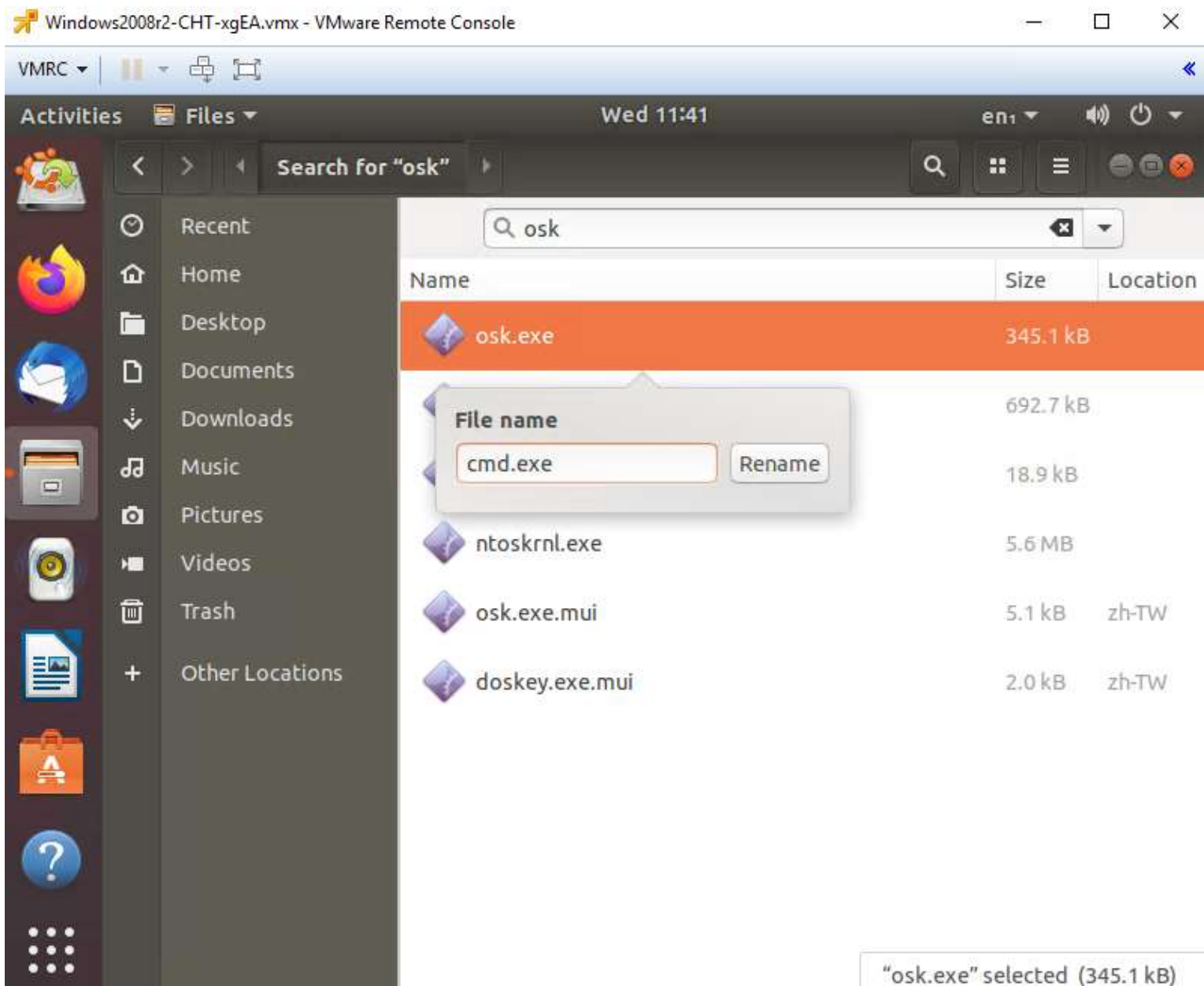
請使用 Portal 將 VM 關機,再次開機系統將會進入 ubuntu

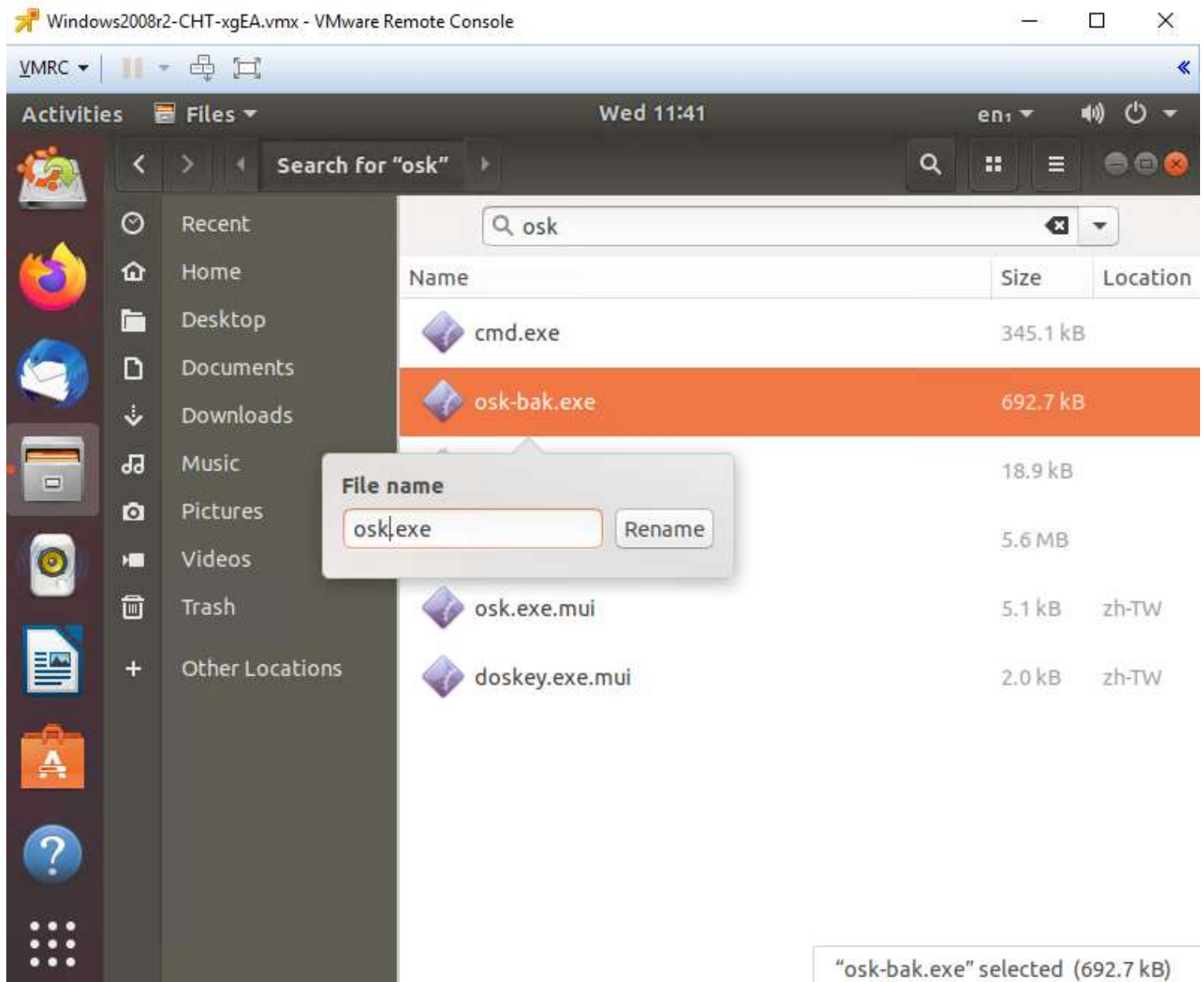
選擇 Try Ubuntu



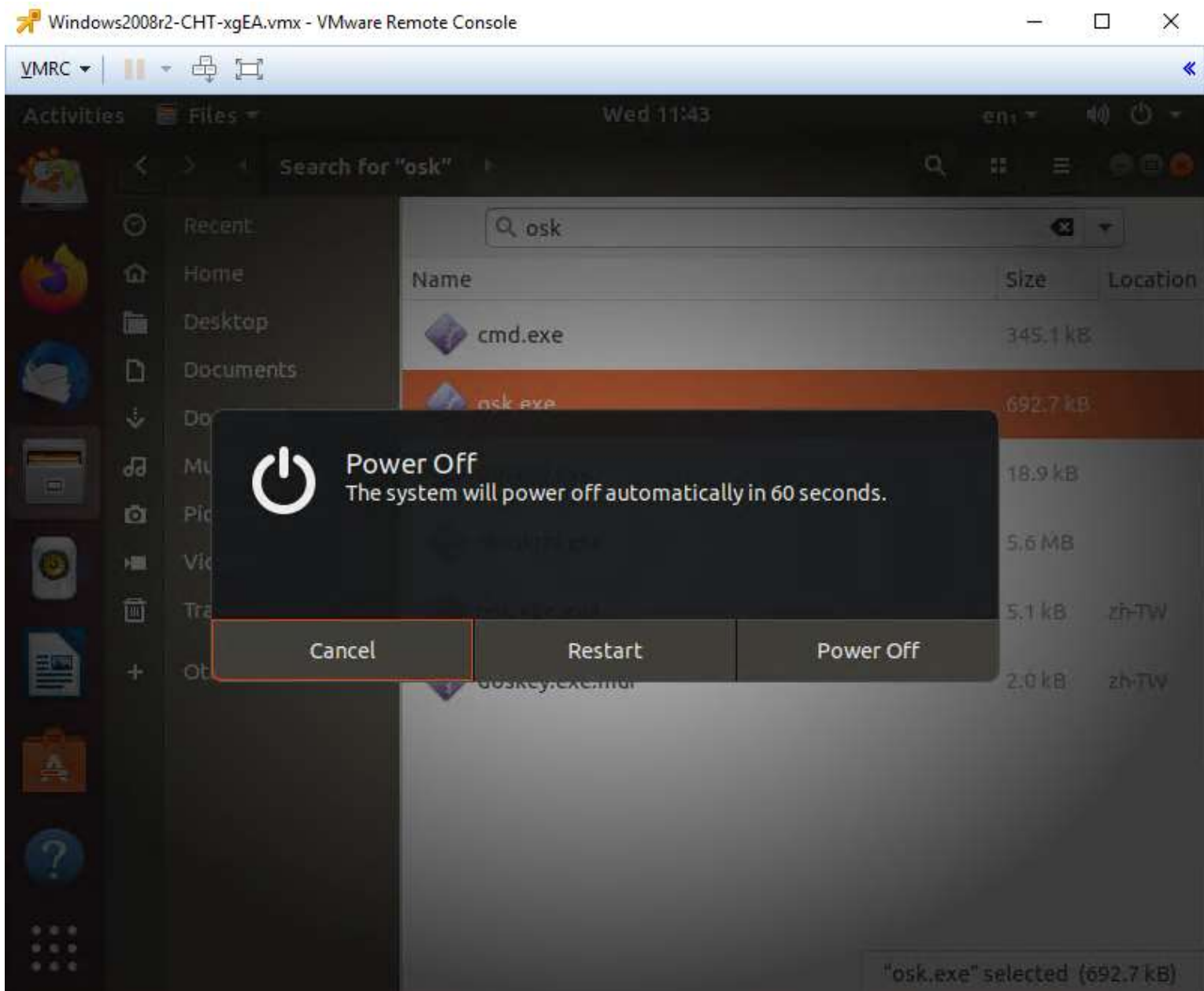
依循步驟 2 再次進入 Windows\system32 目錄將 osk.exe 變更回 cmd.exe

並將 osk-bak.exe 變更回 osk.exe





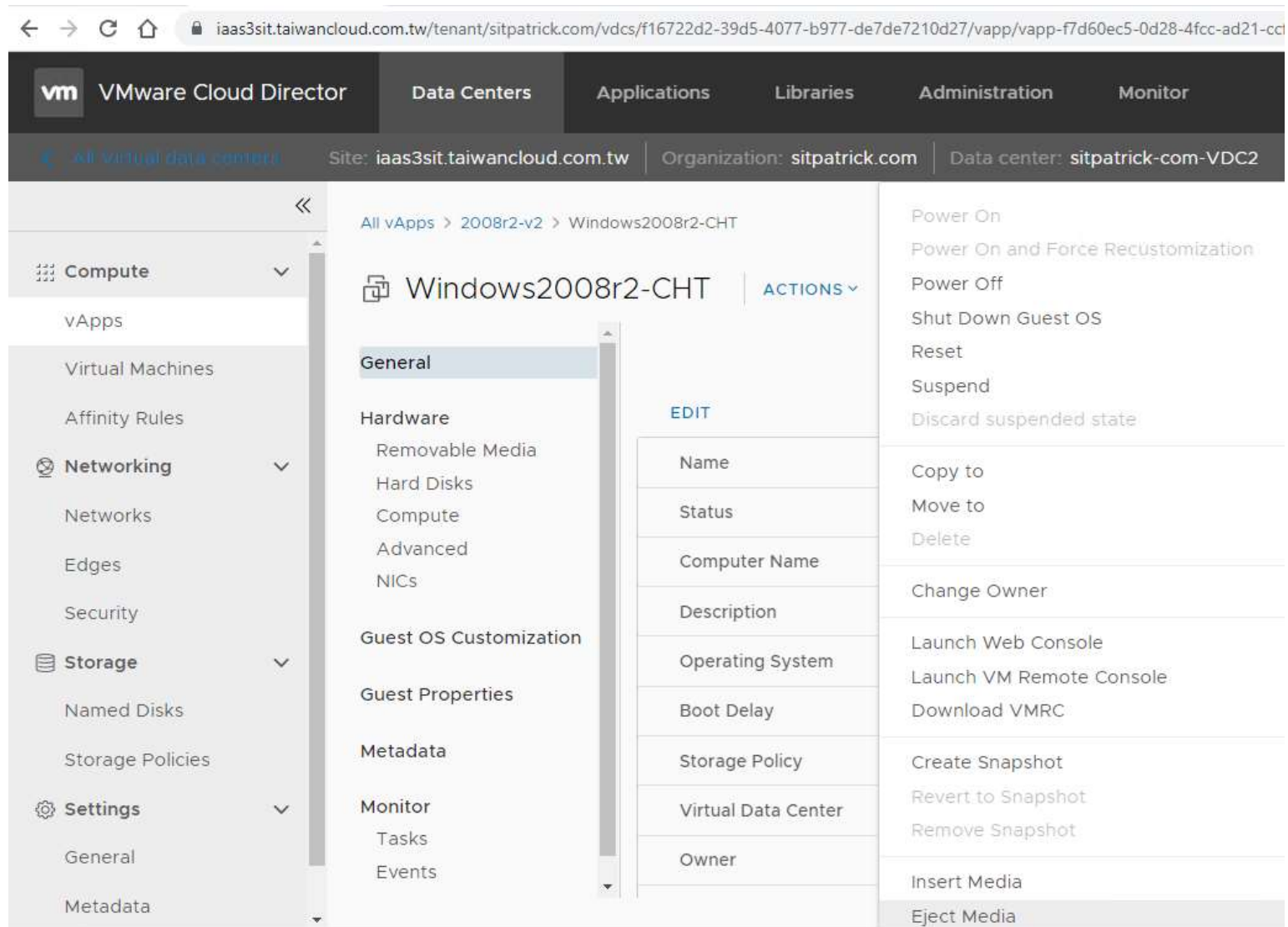
將 VM 關機



按 ENTER



進入 portal · 點選 action Eject Media 將 iso 退出



The screenshot displays the VMware Cloud Director web interface. The top navigation bar includes 'VMware Cloud Director', 'Data Centers', 'Applications', 'Libraries', 'Administration', and 'Monitor'. Below this, a breadcrumb trail shows 'All vApps > 2008r2-v2 > Windows2008r2-CHT'. The main content area is divided into three sections: a left sidebar with a tree view showing 'Compute' (vApps, Virtual Machines, Affinity Rules), 'Networking' (Networks, Edges, Security), 'Storage' (Named Disks, Storage Policies), and 'Settings' (General, Metadata); a central pane for 'Windows2008r2-CHT' with tabs for 'General', 'Hardware' (Removable Media, Hard Disks, Compute, Advanced, NICs), 'Guest OS Customization', 'Guest Properties', 'Metadata', and 'Monitor' (Tasks, Events); and a right-hand 'ACTIONS' menu. The 'ACTIONS' menu lists various operations such as 'Power On', 'Power Off', 'Shut Down Guest OS', 'Reset', 'Suspend', 'Discard suspended state', 'Copy to', 'Move to', 'Delete', 'Change Owner', 'Launch Web Console', 'Launch VM Remote Console', 'Download VMRC', 'Create Snapshot', 'Revert to Snapshot', 'Remove Snapshot', 'Insert Media', and 'Eject Media' (which is highlighted).

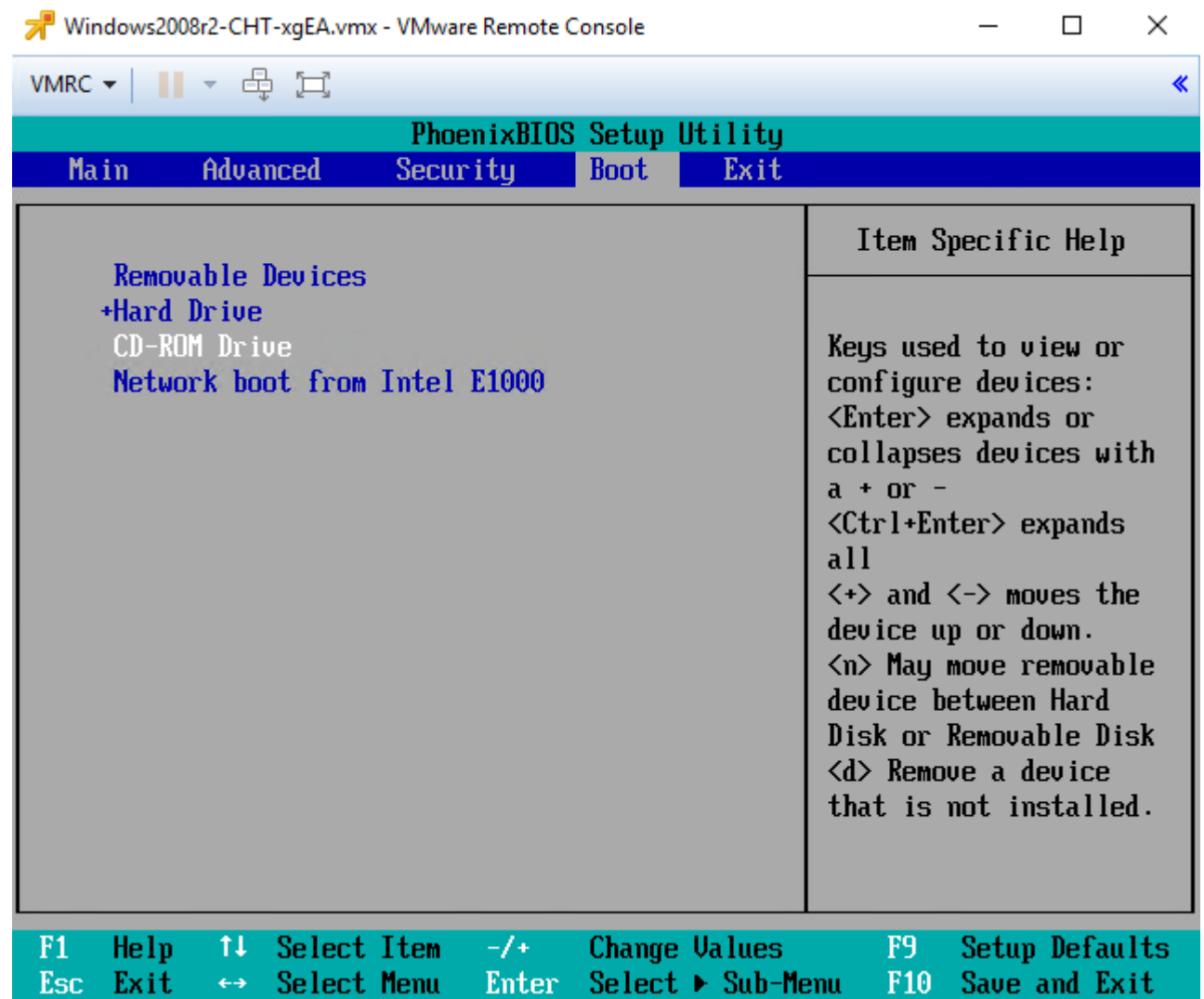
再次設定讓 VM 開機進入 BIOS，還原開機順序

Edit VM Windows2008r2-CHT

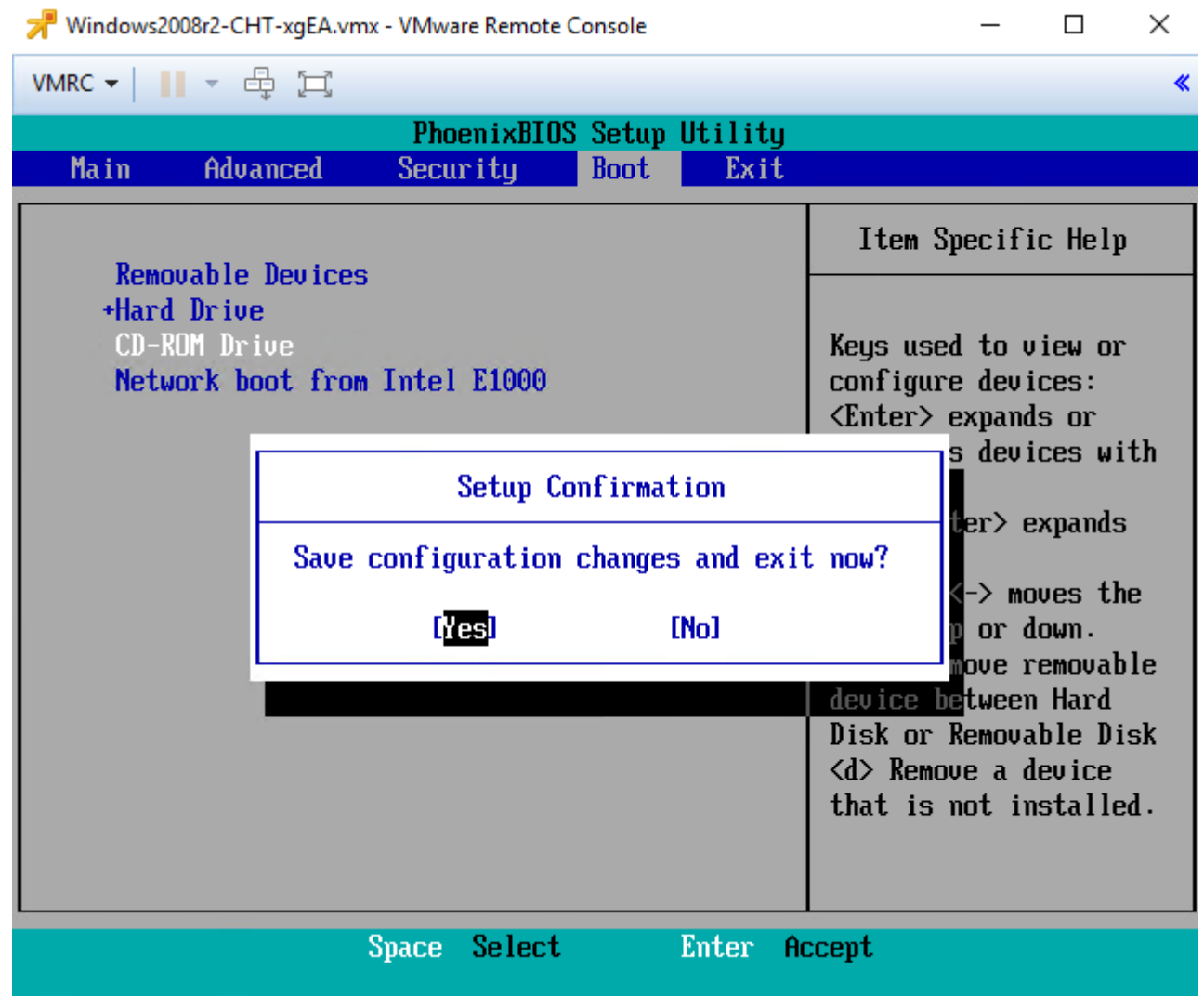


Name *	Windows2008r2-CHT
Computer Name *	Windows2008-001
Description	TWM-Template
Operating System Family	Microsoft Windows
Operating System	Microsoft Windows Server 2008 R2 (64-bit)
Boot Delay *	0
Storage Policy	standard-policy-C02
Enter BIOS Setup	☒

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



最後再回到 VM 設定把確認 BIOS 選項開關調回關閉

Edit VM Windows2008r2-CHT

✕

Name *	Windows2008r2-CHT
Computer Name *	Windows2008-001
Description	TWM-Template
Operating System Family	Microsoft Windows
Operating System	Microsoft Windows Server 2008 R2 (64-bit)
Boot Delay *	0
Storage Policy	standard-policy-C02
Enter BIOS Setup	☐

DISCARD

SAVE

到此已復原先前的變更作業。