# 遠傳雲端運算服務

## 使用者手冊

**修版記錄** (Revision Record)

| 版 本 | 修版者 | 修版日期 | 修版原因及摘要 |
|---|---|---|---|
| 1.0 | Allen Liu | 2019/6/12 | 初版 |
| 1.1 | Allen Liu | 2019/6/17 | 修正遠傳 Logo |
| 1.2 | Allen Liu | 2020/5/14 | 增加新增 vApp/VM 章節 |
| 1.3 | Johnson Hsu | 2021/2/23 | Flash 操作修改成 HTML5 |
| 1.4 | Allen Liu | 2022/6/6 | 增加 SSRM |
| 1.5 | Johnson Hsu | 2023/3/30 | 新增 VM 效能監控，新增 VM 自動擴展自動調整 |
| 1.6 | Jeff Lee | 2023/12/28 | 新增資訊安全要求、變更管理流程、稽核權利與第三方評鑑。 |
| 1.7 | Johnson Hsu | 2023/11/18 | 新增 vCD 雙因子登入功能說明。 |
| 1.8 | Jeff Lee | 2024/2/18 | 依據 CSA STAR CCM4.0 STA-09 之要求，重新彙整雙方須注意事項。 |
| 1.9 | Johnson Hsu | 2025/1/23 | 增加新版防火牆設定 |
| 2.0 | Johnson Hsu | 2026/2 /11 | 增加 VCDA 和 VM 資料防止外洩操作說明 |

# Table of Content 目錄


1. vCloud Director 使用基本要求 ..... 6
2. 登入管理平台 ..... 7
3. 檢視使用紀錄 ..... 9
4. 變更登入密碼 ..... 10
5. Upload 媒體影像檔 (*.iso) ..... 11
6. 掛載 ISO 檔或 OVA 檔 ..... 13
7. 安裝 VMware Tools 工具 ..... 15
8. 建立虛擬機快照 (Snapshot) ..... 17
   - *8.1* 建立快照 ..... 17
   - *8.2* 還原快照 ..... 18
   - *8.3* 移除快照 ..... 19
9. VM 效能監控( vCloud Director ) ..... 20
10. 新增虛擬機 ..... 23
    - *10.1* 配置 NAT 設定 ..... 28
    - *10.2* *配置防火牆設定* ..... 31
    - *10.3* 配置防火牆設定(新版) ..... 33
11. VM 自動擴展功能 ..... 38
12. MFA 登入操作 ..... 44
13. VCDA 操作說明 ..... 50
14. VM 資料防止外洩操作說明 ..... 59

*Appendix 附錄:* ..... 60

- *A. 無法顯示遠端操控台 Remote Console (VMRC)* ..... *60*
- *B. 虛擬機 NTP 時間校時方法* ..... *62*
- *C. 如何保護虛擬機內的機敏資料* ..... *63*
- *D. 如何保護虛擬機的資訊安全* ..... *65*
- *E. 業務關係和提供服務的範圍、特點和位置(Scope, characteristics and location of business relationship and services offered)* ..... *66*
- *F. 雲端資訊安全要求(Information Security Requirement)* ..... *67*
- *G. 雲端資訊安全責任共擔模型(Shared Security Responsibility Model, SSRM)* ..... *68*
- *H. 雲端客戶變更需求程序(Cloud Customer Change Management Process)669*
- *I. 日誌記錄和監視能力(Logging and monitoring capability)* ..... *70*
- *J. 資安事件的通報與溝通處理(Incident management and*

***communication procedures)*** ..... *71*
***K. 稽核權利(Audit rights)*** ..... ***72***
***L. 第三方評鑑(Third party assessment)*** ..... ***73***
***M. 服務終止(Service termination)*** ..... ***74***
***N. 互操作性和可攜性要求(Interoperability and portability requirements)*** ..... ***75***
***O. 資料隱私(Data privacy)*** ..... ***76***

## Introduction 簡介

遠傳VMware vCloud Director是個自助式服務平台，提供一個易於使用的環境，來管理 VMware的自動化操作、虛擬機與應用程式的配置。此平台是架構在vCenter之上的網路控制平台，可以透過Internet瀏覽器上進行操作管理。

在多租戶的管理概念下，每個承租戶就是一個基礎單位，此基礎單位稱為組織(Organizations)。組織是使用者、群組以及計算資源集合的管理單元。VMware® vCloud Director將提供Web主控台的Role Base存取，讓組織內的成員與組織擁有的資源可以互動，用使用vApp和虛擬機器。

在存取組織之前，vCloud Director系統管理員必須先建立承租戶的組織，並將資源指定給它，然後提供URL連接，網站憑證採用RSA 2048位元以上之加密安全金鑰 SSL 憑證，憑證簽章演算法為SHA256 with RSA，且提供 TLS v1.2傳輸通道，以安全存取Web主控台。

內容可能因版本有所不同，若想進一步確認，請諮詢負業務人員。

客戶常見問題可參閱遠傳官網。
https://enterprise.fetnet.net/content/ebu/tw/product/cloud_product/cloud-service.html

# 1. vCloud Director 使用基本要求

vCloud Director與現在主要的瀏覽器版本符合相容，支援的有:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

# 2. 登入管理平台

## 登入Web主控台 (Console)進行VM管理

使用組織URL登入組織，並存取Web主控台。

程序步驟 **1 :**

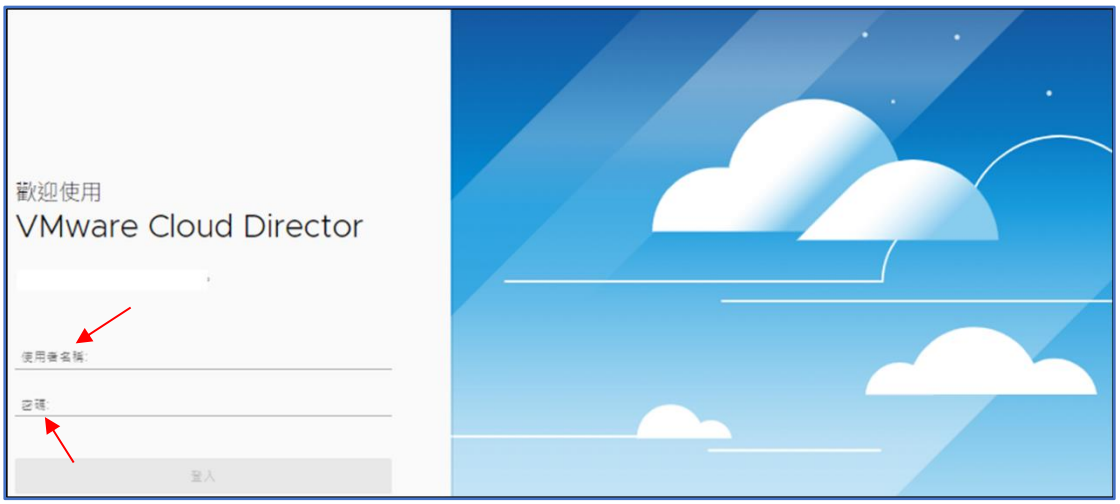
A. 在瀏覽器中，輸入組織的URL，並按 Enter 鍵。

輸入https://portal.akcloud.fetnet.net/tenant/台北用戶編號

輸入https://fetvmware.vmcloud.fetnet.net/tenant/台中用戶編號

例如: https://fetvmware.vmcloud.fetnet.net/tenant/CA1234567

B.輸入使用者名稱和密碼，並按一下登入。

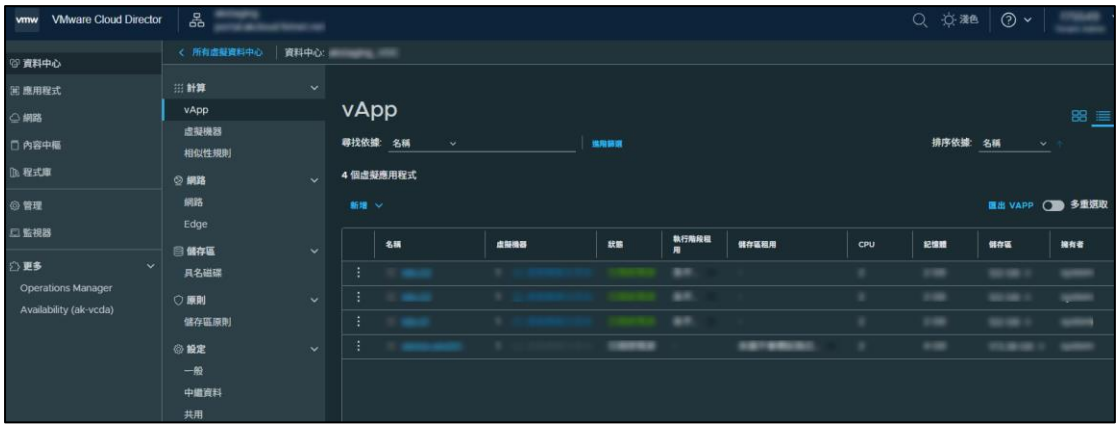



Web主控台會根據您的角色，顯示您可用的一般工作和資源清單。組織管理員可以按一下首頁索引標籤上的設定此組織連結，完成新建立組織的設定。

基於安全理由，強烈建議在登錄後更改密碼，請參考第4章的細節。

程序步驟 2：

自助平台如下:




程序步驟 3：

在虛擬機上按【 ⋮ 】，然後視需要選擇【開啟電源】【開啟電源並強制重新自訂】【關閉電源】【關閉客體作業系統】【重設】【暫止】【捨棄暫停狀態】

## 3. 檢視使用紀錄

程序步驟 1：於【監視器】中點選【事件】

程序步驟 2：點選【事件】【工作】

下方即可列出關於VM使用之紀錄

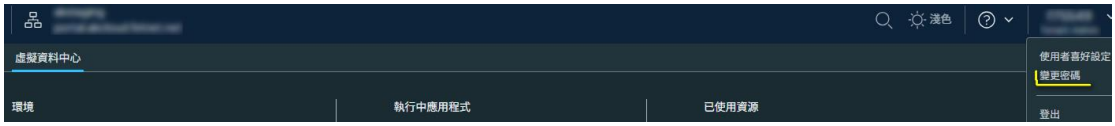
工作項目包含: VM停止/VM執行

事件項目包含:登入成功/登入失敗/開啟VM電源/關閉VM電源

## 4. 變更登入密碼

程序步驟 1：

點選帳號：用戶客編




程序步驟 2：

點選【變更密碼】，然後輸入現在和新的密碼

密碼注意事項如下:

- 每個使用者建議應有獨立帳號，禁止共用帳號密碼
- 最少每 90 天需更換一次密碼
- 密碼長度建議最少須設定七個字元以上
- 安全性密碼建議應包含英數字
- 密碼歷程建議應至少四次
- 嘗試失敗 3 次後將鎖定帳號
- 鎖定帳號後至少需等待 30 分鐘或聯絡系統管理員解除鎖定啟用帳號
- 帳號閒置超過 15 分鐘後需要重新輸入密碼才能登入

若發現帳號登入有未經授權之異常存取，請洽遠傳客服專線(02) 4499-365。

## 5. Upload媒體影像檔 (*.iso)

此項目及匯出匯入 ISO/OVF 功能需依客戶需求另行提供(需聯繫業務人員申請)

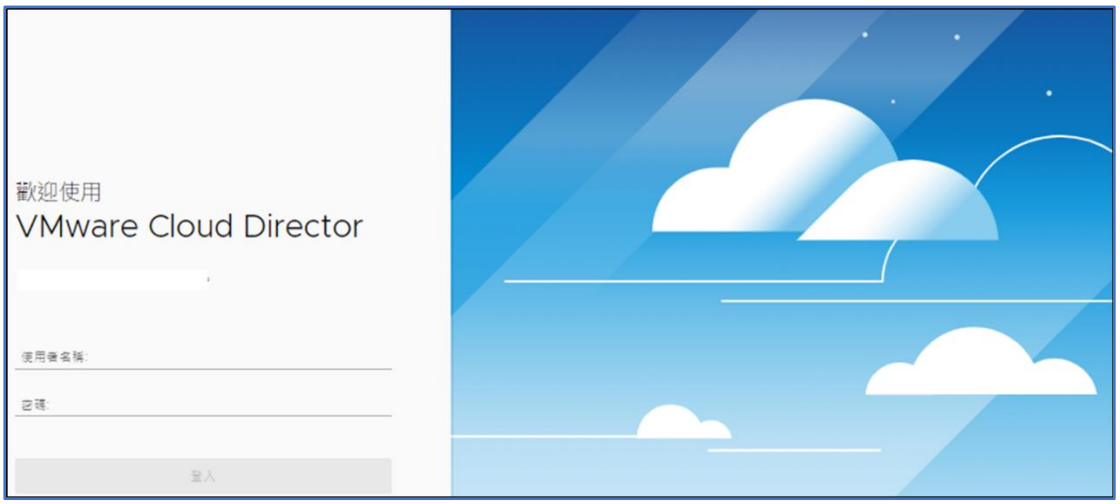
程序步驟 1：

登入管理平台

輸入 https://portal.akcloud.fetnet.net/tenant/您的用戶編號

或https://fetvmware.vmcloud.fetnet.net/tenant/您的用戶編號

輸入帳號與密碼

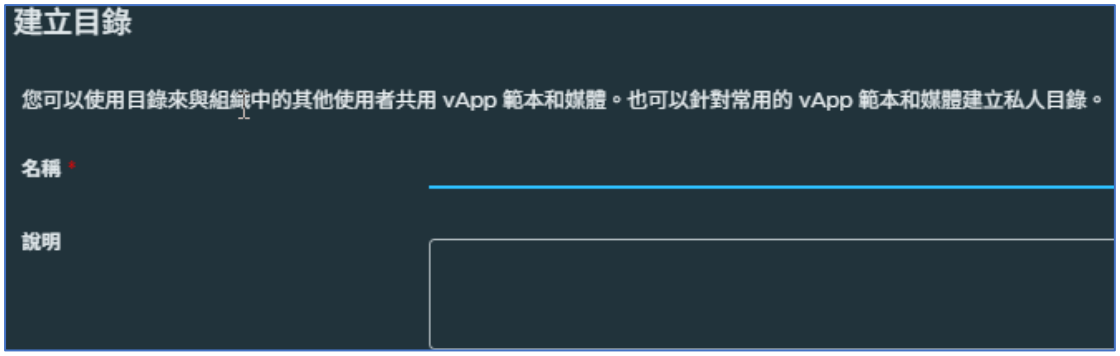



程序步驟 2：

登入管理平台點選【內容中樞】

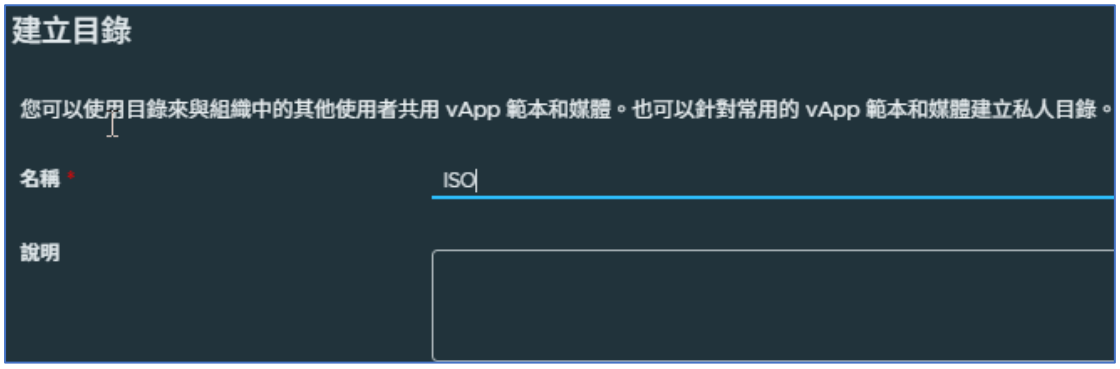
程序步驟 3:

首先須增加新的目錄，按【目錄】，再按【新增目錄】




程序步驟 4：

輸入目錄名稱後按【確定】

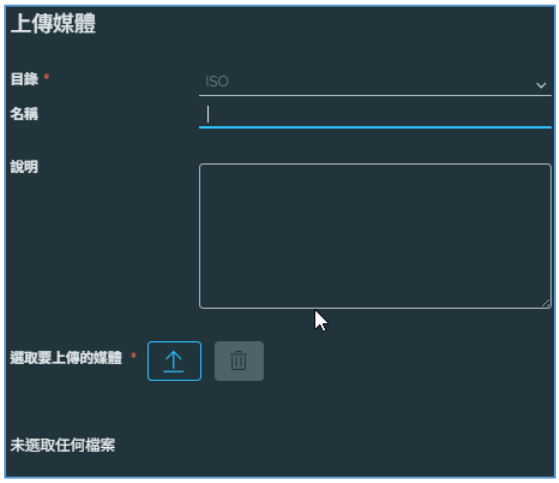



程序步驟 5：

點選【目錄】，選取新增目錄名稱，點選【媒體】，按【新增】

程序步驟 6：

選擇之前新增的目錄，點取【選取要上傳的媒體】Upload



程序步驟 7：

選擇右下角的【所有檔案】，找到之前的 ISO 檔或是 OVA 檔，按【開啟】確定

程序步驟 8：

確定要上載 Upload 的檔案後，按【確定】

程序步驟 9：

確認 ISO 檔案或 OVA 檔已經放置到目錄後即完成 **Upload 媒體影像檔**

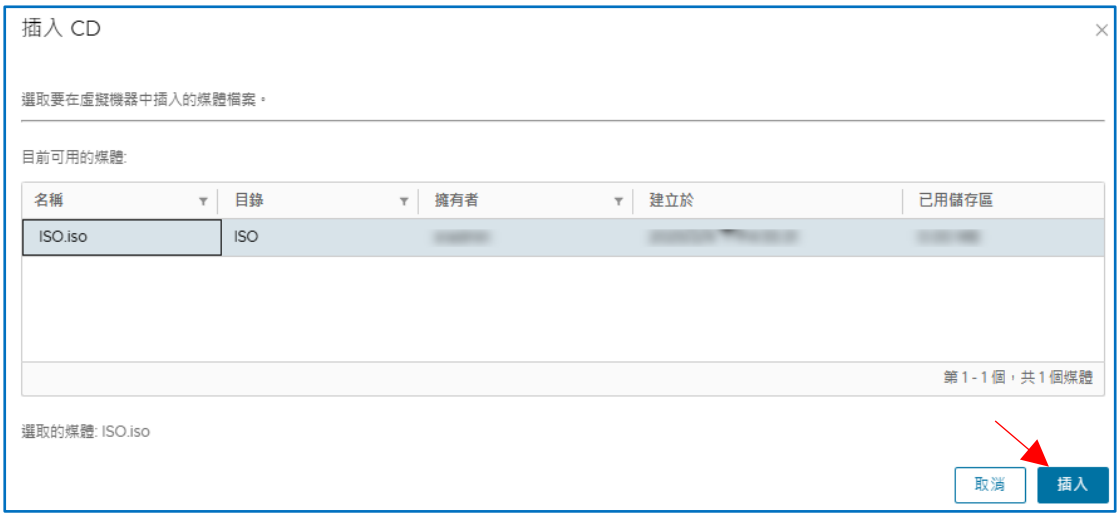
## 6. 掛載 ISO檔或OVA檔

程序步驟 1：

在虛擬機器上按【 ⋮ 】，再選【插入媒體】

程序步驟 2：

選取 ISO 檔或是 OVA 檔的媒體，然後按【插入】

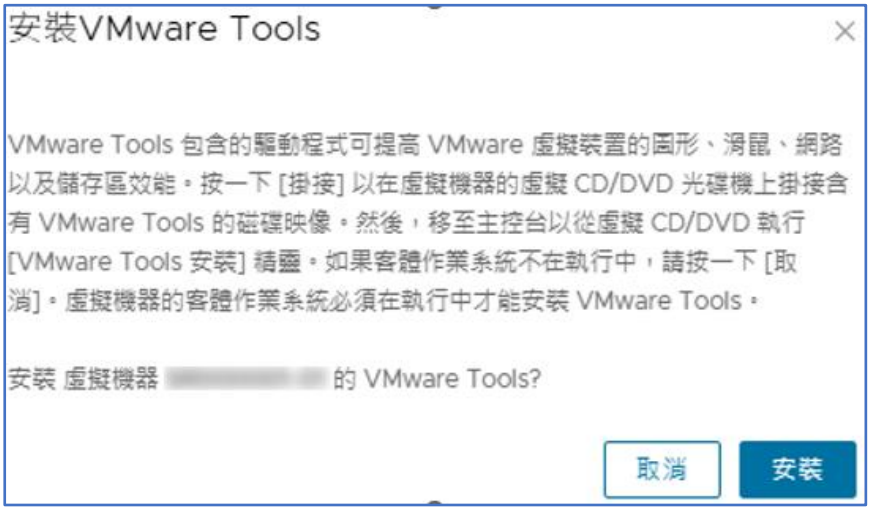


## 7. 安裝 VMware Tools 工具

**VMware Tools** 是一項模組，提供多項功能來進行客體作業系統管理，以及提供順暢的使用體驗讓使用者與客體作業系統互動。

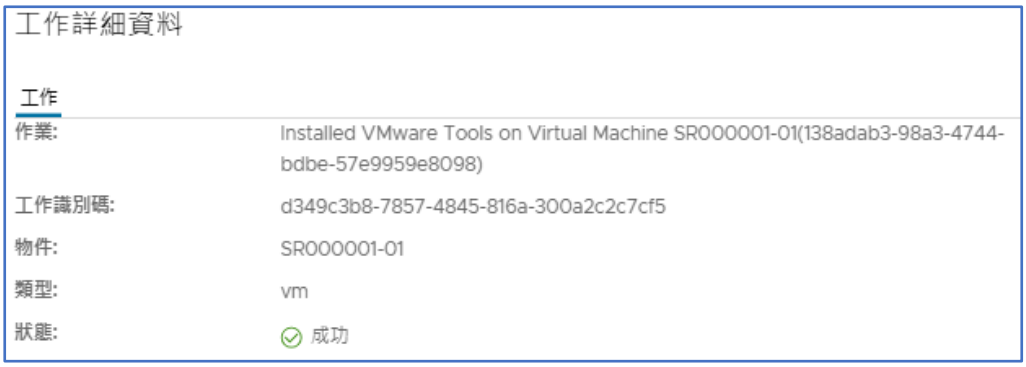
PS:遠傳雲端運算VM預設為已安裝VMware Tools 工具，
使用者可視需求選擇自行移除或重新安裝VMware Tools 工具。

程序步驟 1：
選取虛擬機器上【 ⋮ 】，然後選擇【安裝VMware Tools】



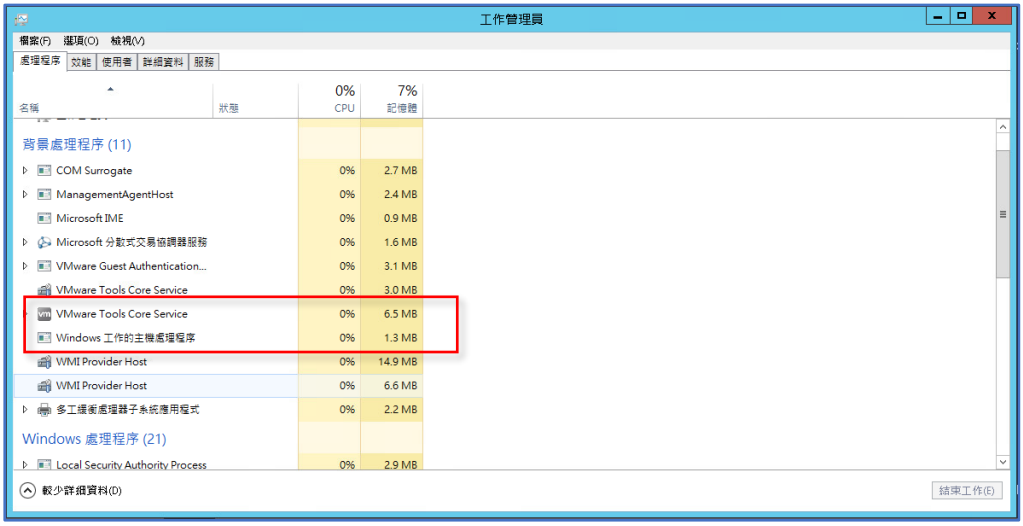
程序步驟 2：

確認VMware Tools安裝是否順利完成




程序步驟 3：

虛擬機登入後，開啟【工作管理員】，確定VMware Tools已經安裝成功運行中



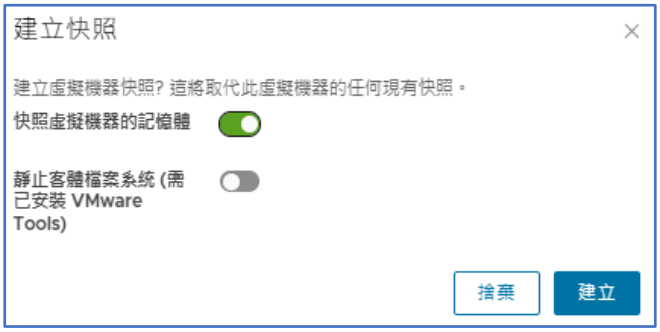
# 8. 建立虛擬機快照 (Snapshot)

在一個特定的時間點，使用快照保留了虛擬機的狀態和數據
使用者可建立多次快照，但系統僅保留最後一次快照

## *8.1* 建立快照

程序步驟 1：
在虛擬機器上點【 ⋮ 】，然後選擇【建立快照】

程序步驟 2：
按【建立】




備註: 視需求選取是否快照虛擬機記憶體及選取靜止客體檔案系統

## 8.2 還原快照

程序步驟 1：

在虛擬機器上點【 ⋮ 】，然後選擇【還原至快照】

程序步驟 2：按【還原】

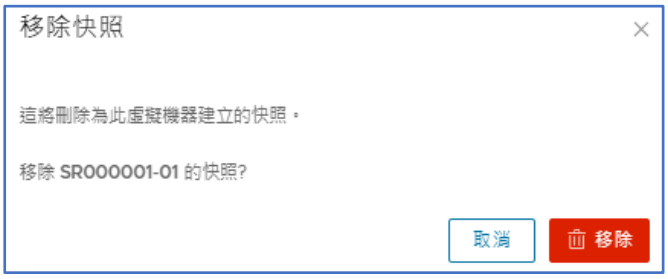
## 8.3 移除快照

程序步驟 1：

在虛擬機器上點【 ⋮ 】，然後選擇【移除快照】

程序步驟 2：

按【移除】



# 9. VM效能監控( vCloud Director )

## 雲端用戶可使用 Web 主控台 (Console) 觀察 VM 使用狀態

### 登入Web主控台(Console)

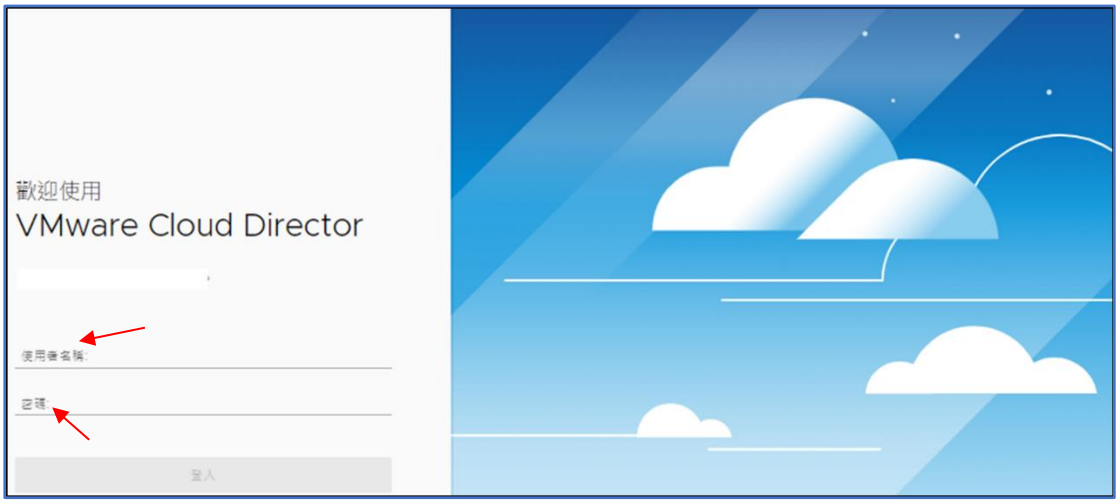
程序步驟 **1 :**

A. 在瀏覽器中，輸入組織的URL，並按 Enter 鍵。

輸入https://portal.akcloud.fetnet.net/tenant/台北用戶編號

輸入https://fetvmware.vmcloud.fetnet.net/tenant/台中用戶編號

輸入帳號 密碼




程序步驟 **2 :**

點選 Operations Manager

程序步驟 **3**：

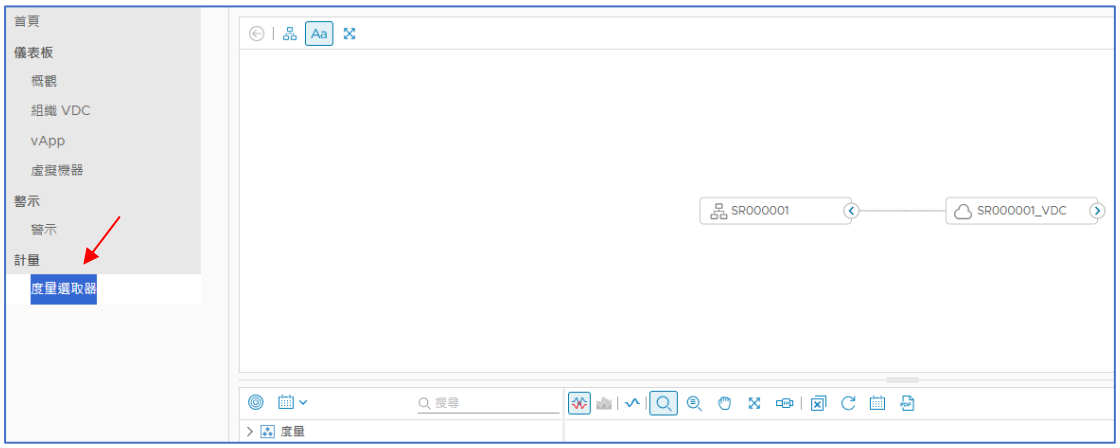
儀表板 概觀

程序步驟 **4**：

虛擬機器資訊: CPU、 記憶體 、 儲存區

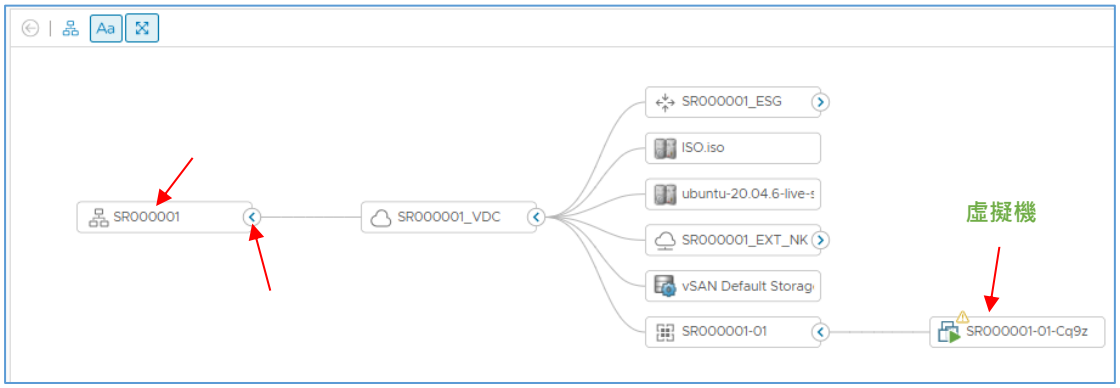
程序步驟 **5**：

選取計量 中的【度量選取器】



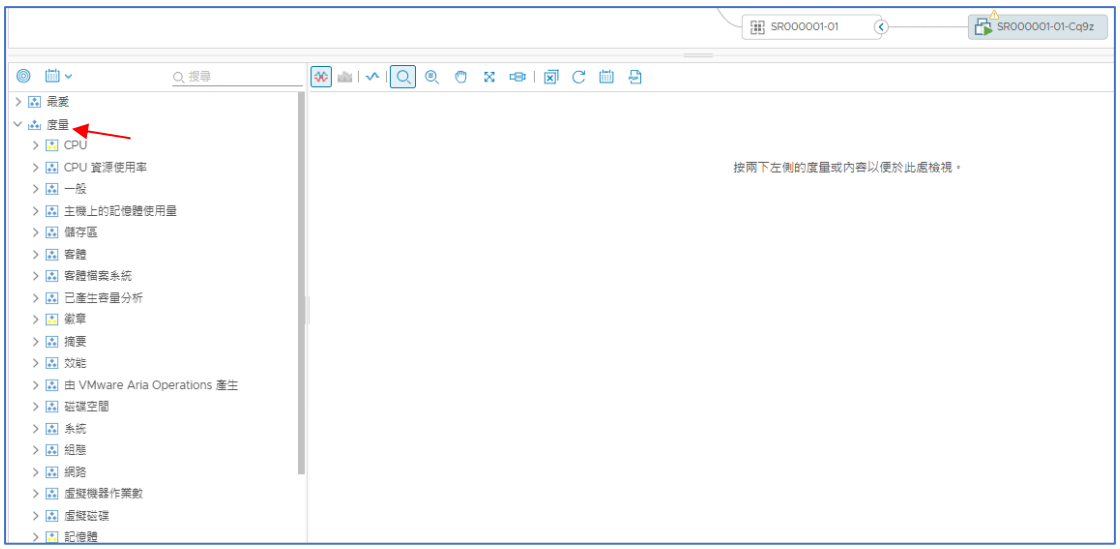

程序步驟 **6**：

選租戶 VM 展開如下圖示選取預計查詢虛擬機



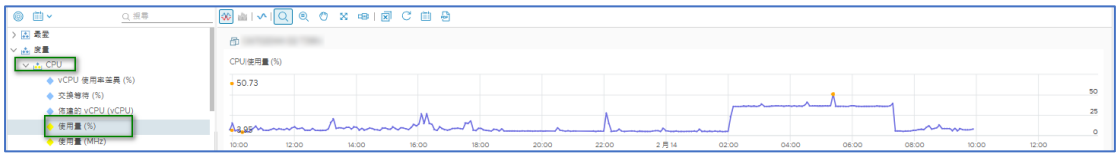
## 程序步驟 7：

## 虛擬機度量資訊




## 程序步驟 8：

## 虛擬機 CPU 效能資訊

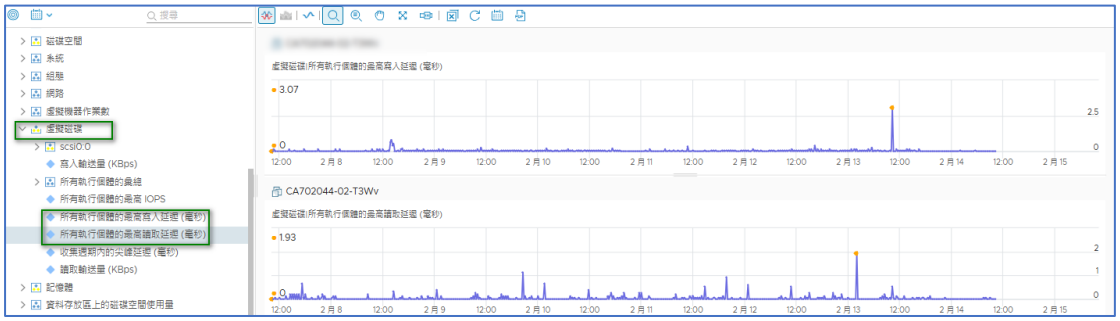



## 程序步驟 9：

## 虛擬機 記憶體效能資訊

## 程序步驟 10：

## 虛擬機 網路資訊



## 10.新增虛擬機

(此項目 Pools 規格客戶)

**登入管理平台**

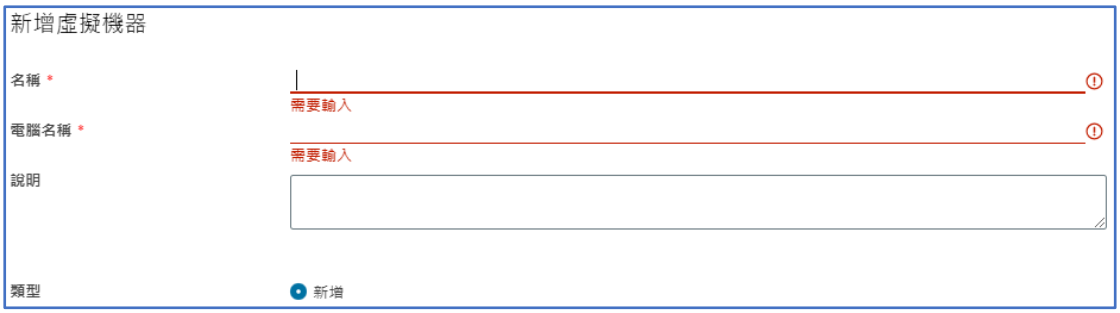
程序步驟 1：

由Web主控台 (Console)選取【vApp】，依照服務需求輸入【名稱】點選

輸入【名稱】點選新增虛擬機器

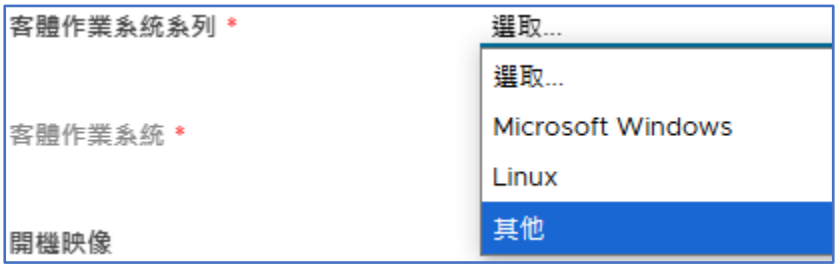
程序步驟 2：

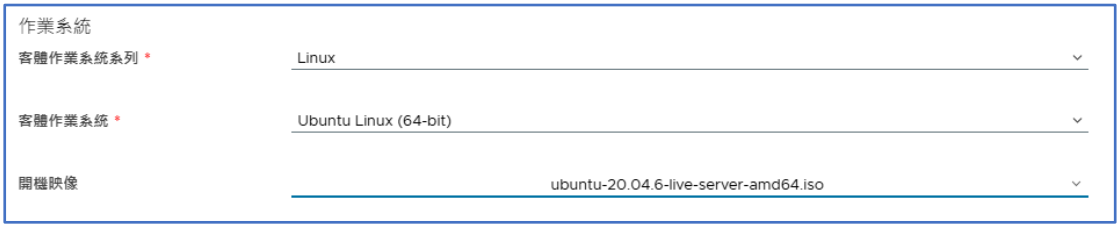
輸入【名稱】及【電腦名稱】點選【新增】




程序步驟 3：

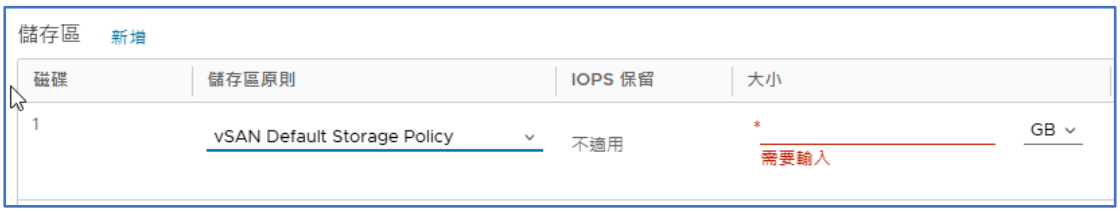
依照系統需求選取【客體作業系統系列】，開機映像選取用戶自行上傳 ISO 檔



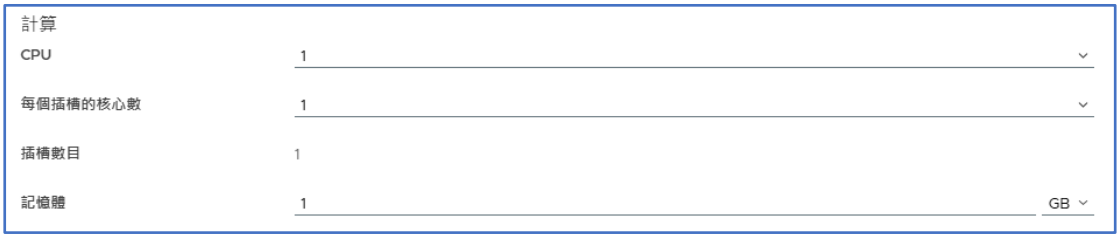

程序步驟 4:

設定儲存空間原則為【vSAN Default Storage Policy】並輸入磁碟空間大小




程序步驟 5：

設定運算原則 CPU/MEMORY



程序步驟 6：

網路設定 輸入【IP 位址】範例 第一台主機 輸入 10.10.0.101 依此類推

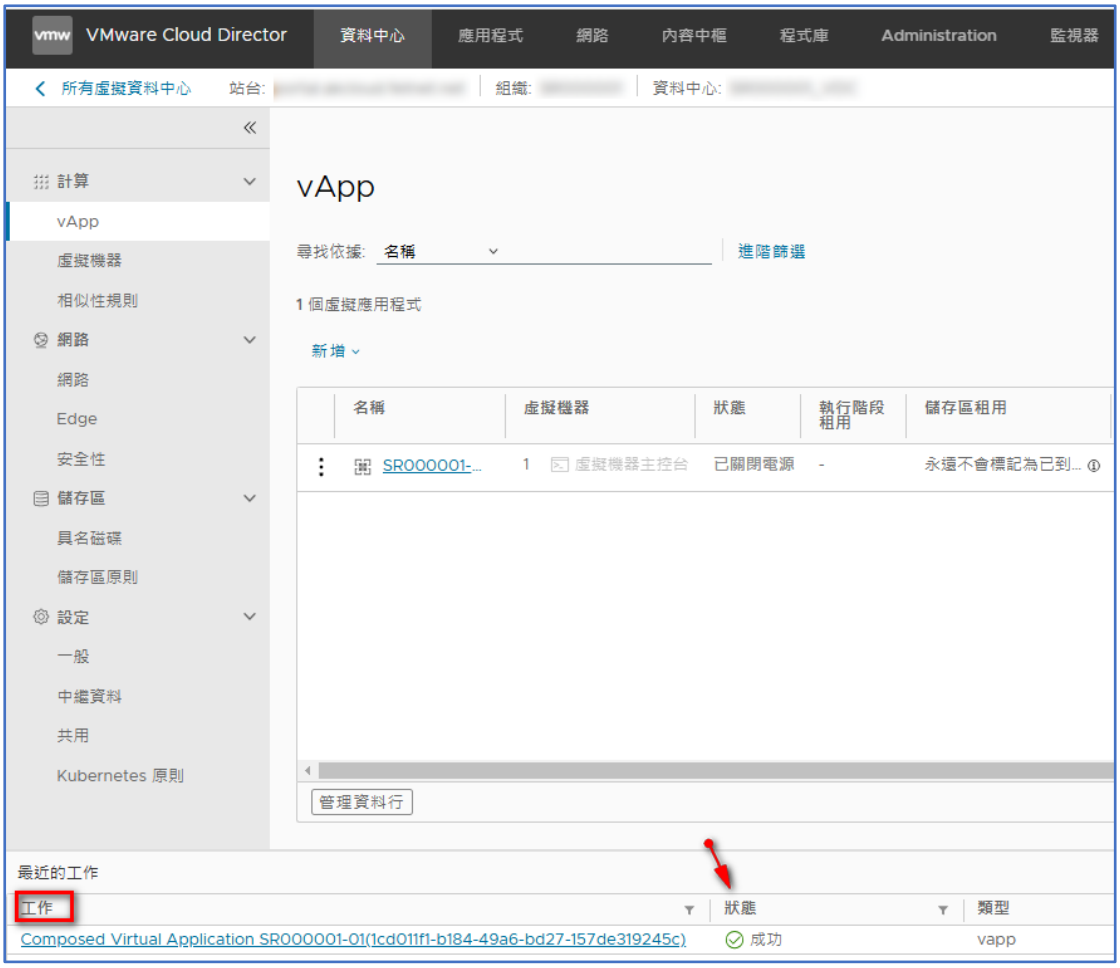
點選【確定】

程序步驟 7:

確認無誤後點選【建立】

程序步驟 8:

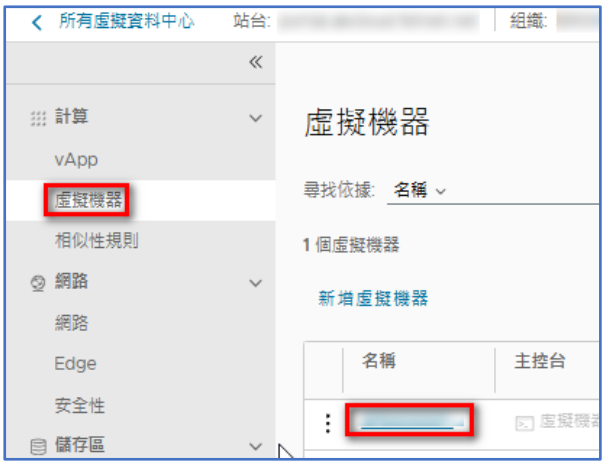
可以從視窗最下方【最近的工作】查閱佈建的狀態




VM 佈建完成

程序步驟 9：

選取【虛擬機器】展開 VM 機器




確認硬碟空間

確認網卡設定

## *10.1* 配置NAT設定

程序步驟 1：

點選【網路】

程序步驟 2：

點選【Edge 閘道】

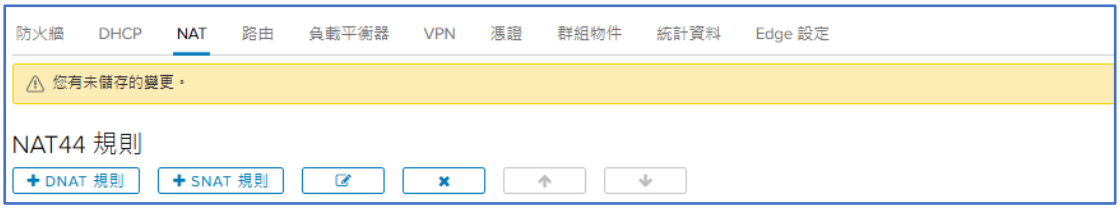
點選【服務】

程序步驟 3：

選擇【NAT】頁籤

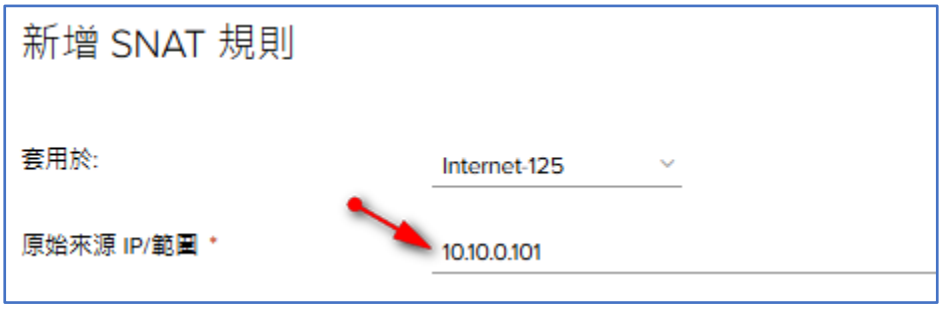
程序步驟 4：

點選【+SNAT 規則】頁籤



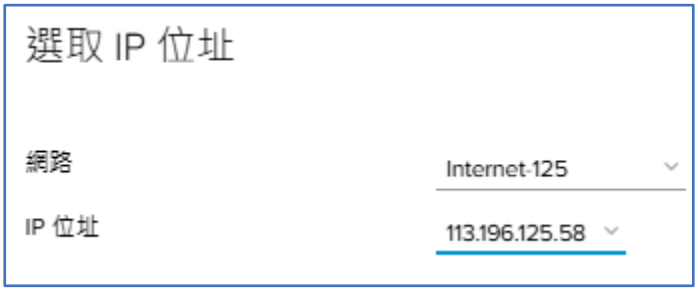

程序步驟 5：

原始來源 IP/範圍 輸入 VM IP



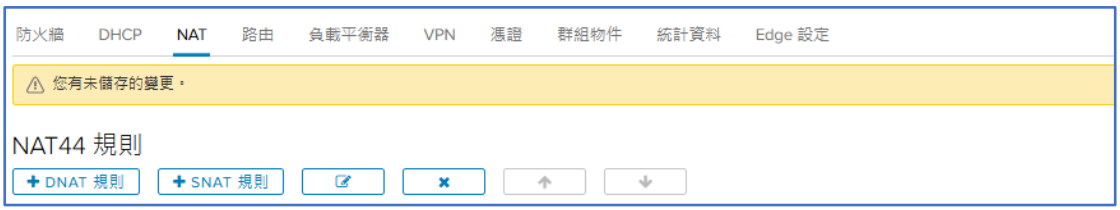

點選【選取】

IP 位址下拉選取配置 IP 後點選保留

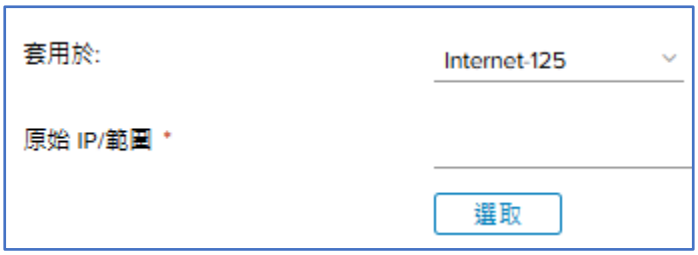



程序步驟 6：

點選【+ DNAT 規則】

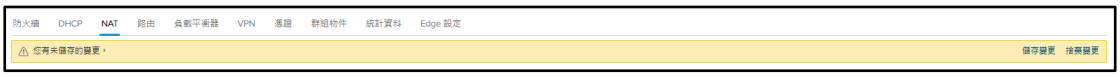


原始來源 IP/範圍 點選【選取】




轉譯的 IP/範圍輸入 VM IP 後點選保留

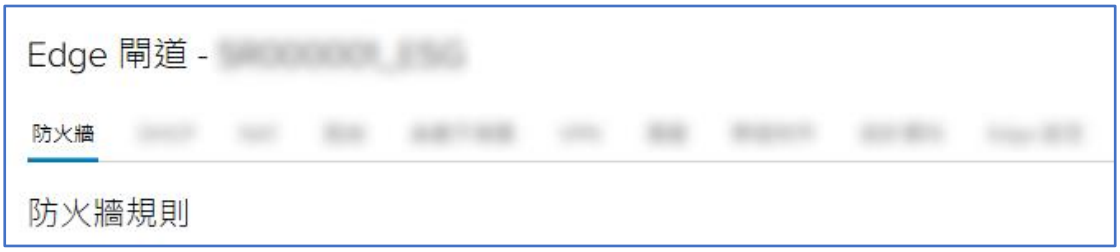
最後點選【儲存變更】



## 10.2 配置防火牆設定

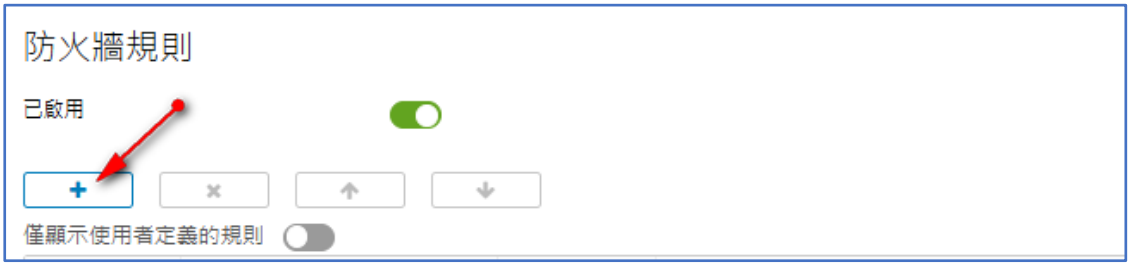
程序步驟 1：

點選【網路】



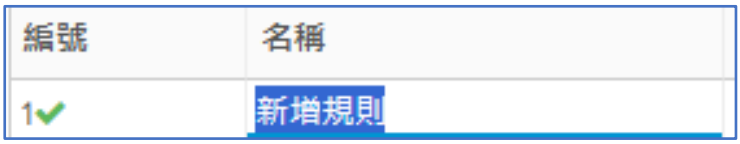

程序步驟 2：

點選【+】



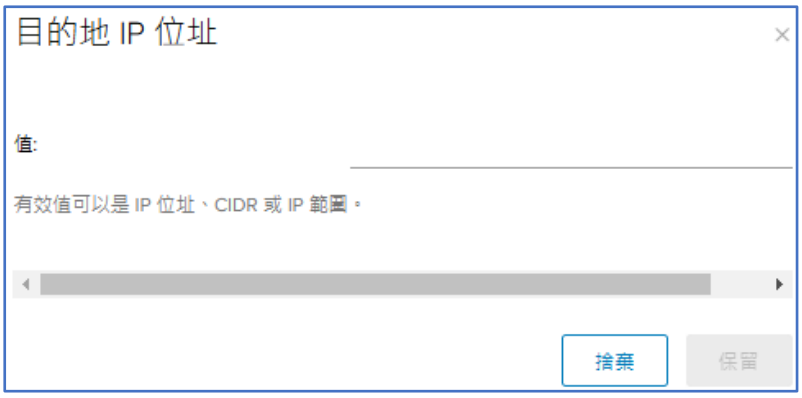

程序步驟 3：

填入服務名稱

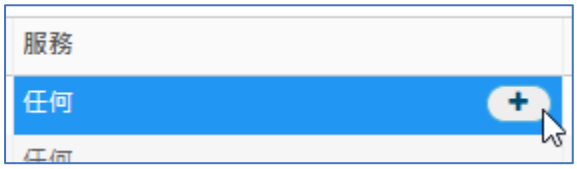



填入來源 IP

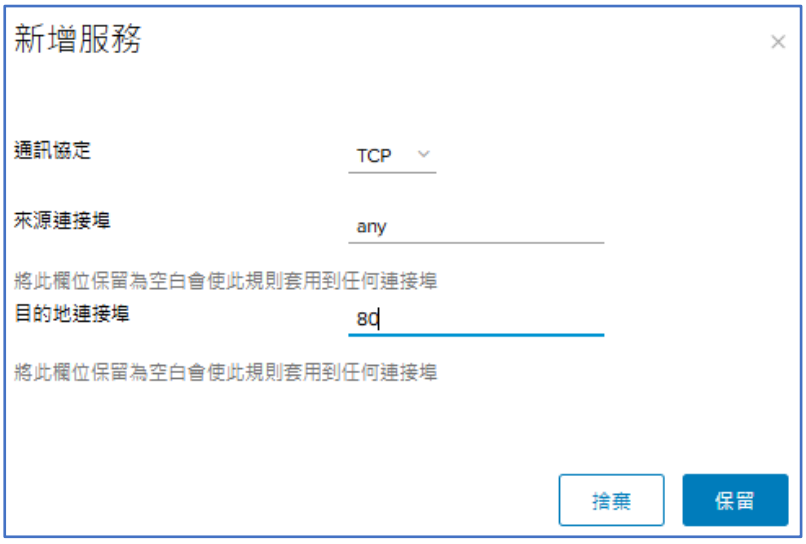
輸入目的 IP (指 VM NAT IP)




點選【服務】

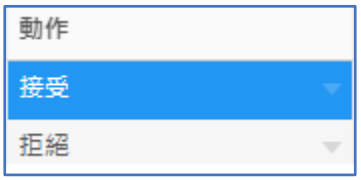



填入【通訊協定】【來源連接埠】【目的連接埠】




程序步驟 4：

於【動作】欄位上依需求選取【接受(Allow)/拒絕(Deny)】




程序步驟 5：

點擊【儲存變更】

## *10.3* 配置防火牆設定(新版)

程序步驟 1

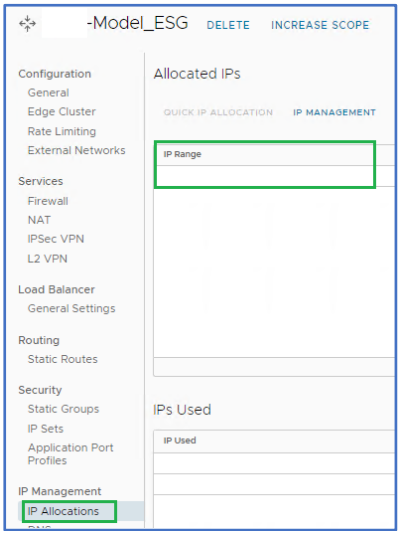
選擇您的虛擬資料中心

程序步驟 2

在「**網路**」部分下，按一下「**Edge**」。然後，點擊您的 Edge

程序步驟 3

按一下 **IP 分配**，然後找到您分配的 IP



程序步驟 4

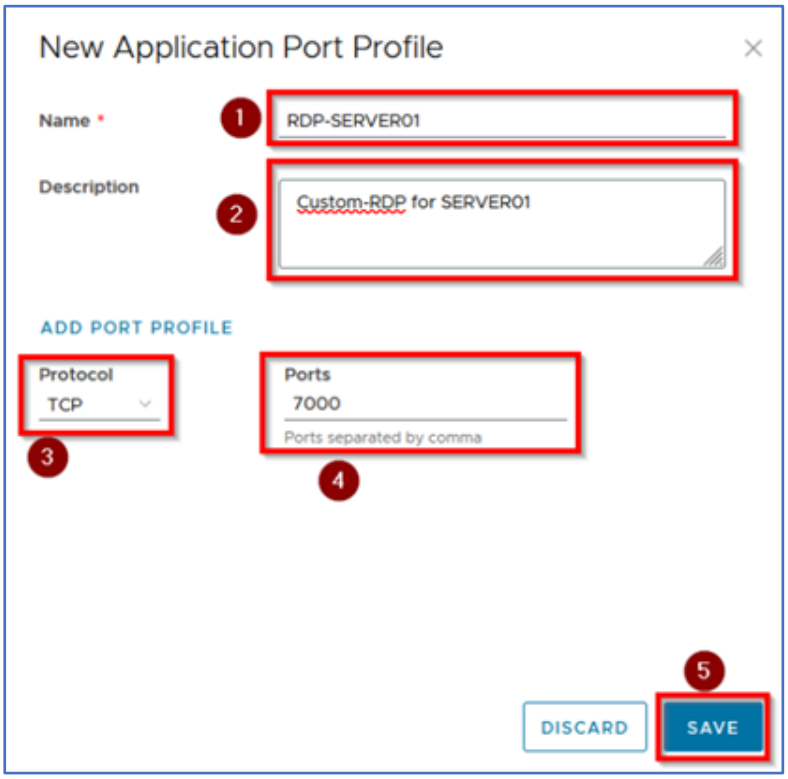
定義自訂應用程式，Edge 閘道內已有內建應用程式。

您也可以建立自訂應用程式。Edge 設定中，轉到名為**“應用程式連接埠設定檔”**的部分，然後按一下**“新增”**

程序步驟 5

輸入應用程式名稱和描述。選擇協定並輸入所需的連接埠。然後，按一下「**儲存**」

本範例 為 TCP Ports 7000



下面範例 為單一 IP 位址開啟自訂 HTTP 服務

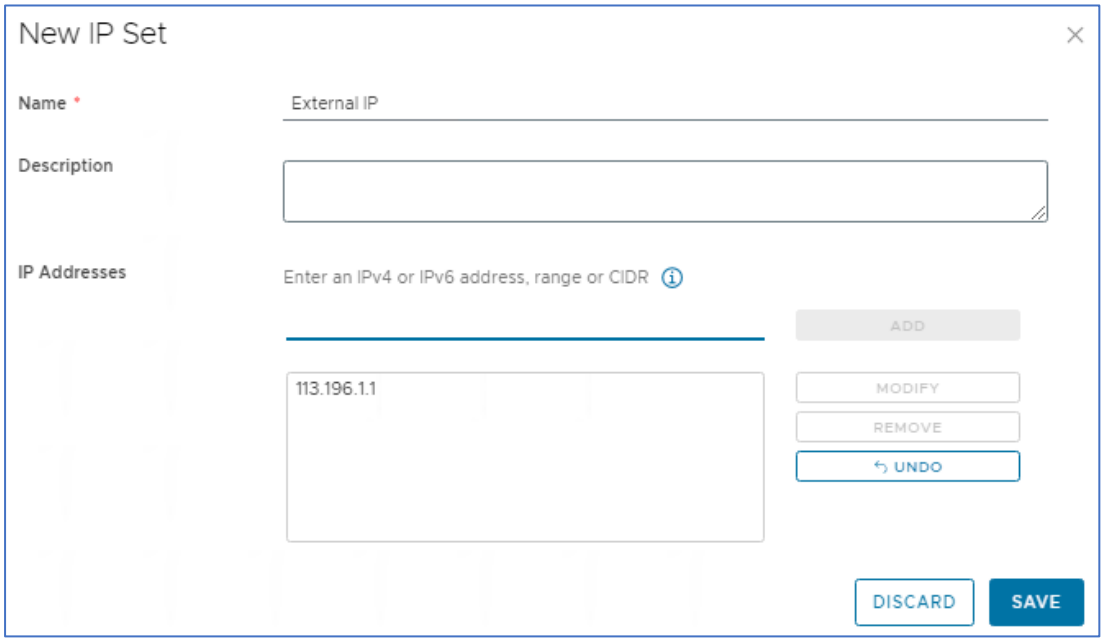
程序步驟 6

定義 IP ，然後按一下**“新增”**

程序步驟 7

建立 External IP

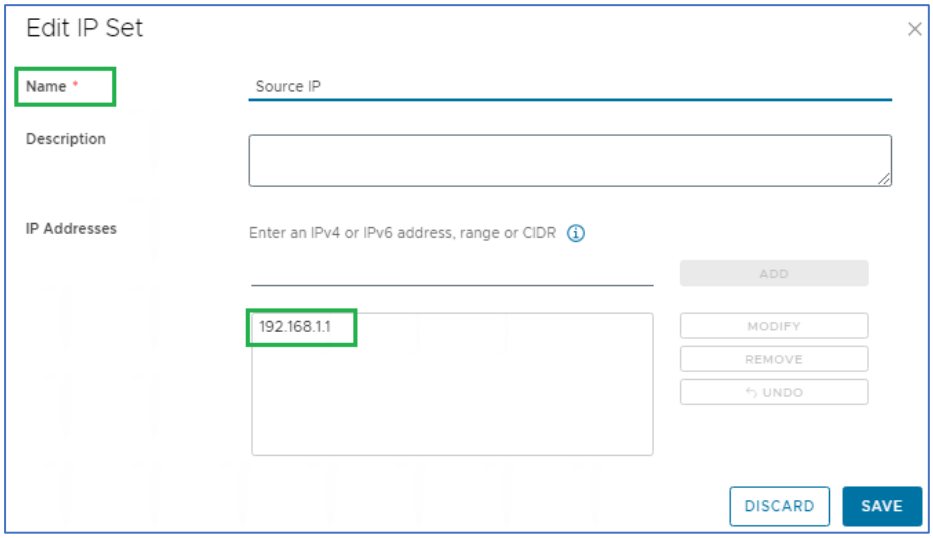
Name: 輸入所需的規則名稱 IP: 參考 Allocated Ips 內容 (程序步驟 3)



程序步驟 8

建立 **Source IP**

Name: 輸入所需的規則名稱 IP: 輸入外部來源 IP




程序步驟 9

配置防火牆規則，前往**防火牆** 部分並點擊**編輯規則**

程序步驟 10

名稱：為您的防火牆規則命名

應用程式：按一下鉛筆為此防火牆規則選擇應用程式。然後，按一下「**儲存**」

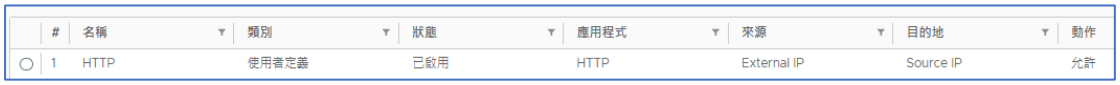
在此範例中，選擇了 HTTP 應用程式

程序步驟 11

來源 IP 勾選 External IP

程序步驟 12

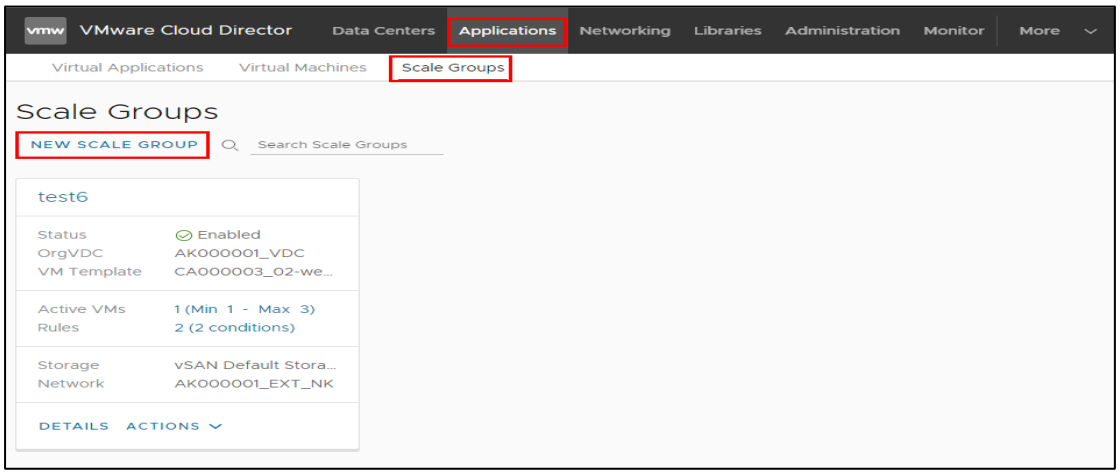
目的: 此範例中，為「遠端辦公室」的 IP




## 11. VM自動擴展功能

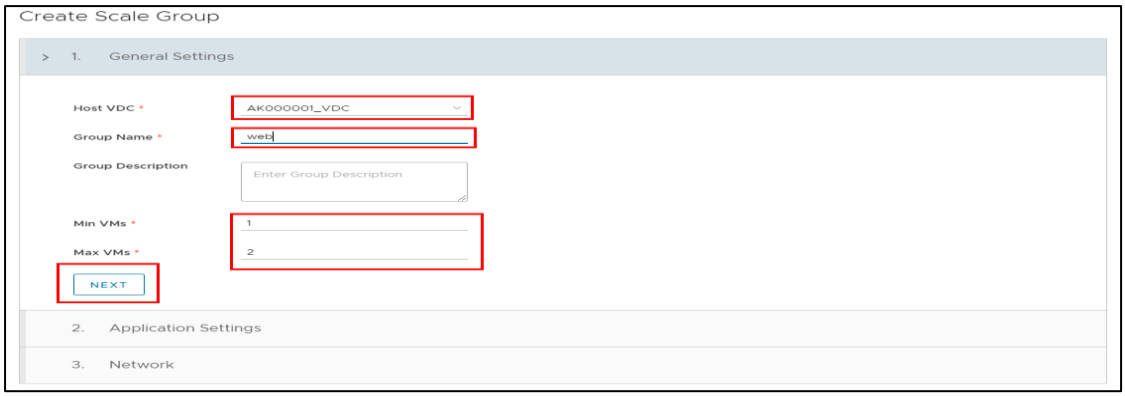
程序步驟 1:

點選應用程式，選取比例組



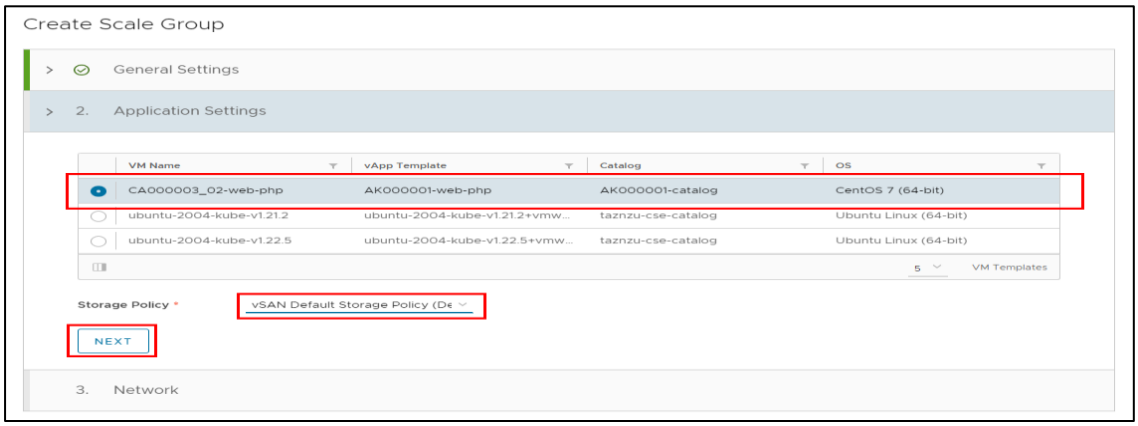
程序步驟 2:

選取 Host VDC(客戶編號)，輸入群組名稱，選取最小虛擬機及最大虛擬機



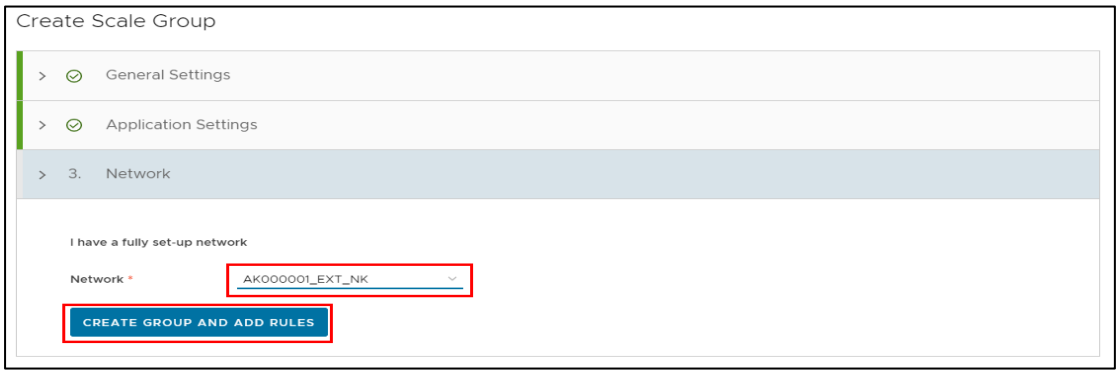

程序步驟 3:

選取範本 VM，儲存設備政策選取預設



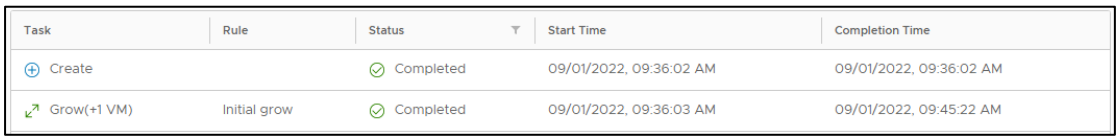

程序步驟 4:

Network 選取對外網卡 XXXX_EXT_NK，點選建立

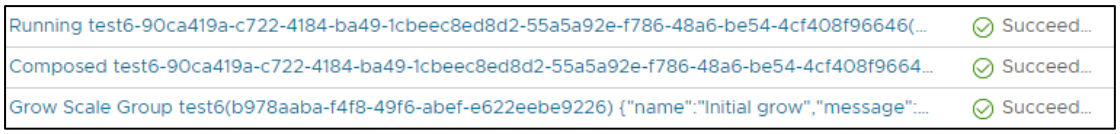



程序步驟 5:

建立中

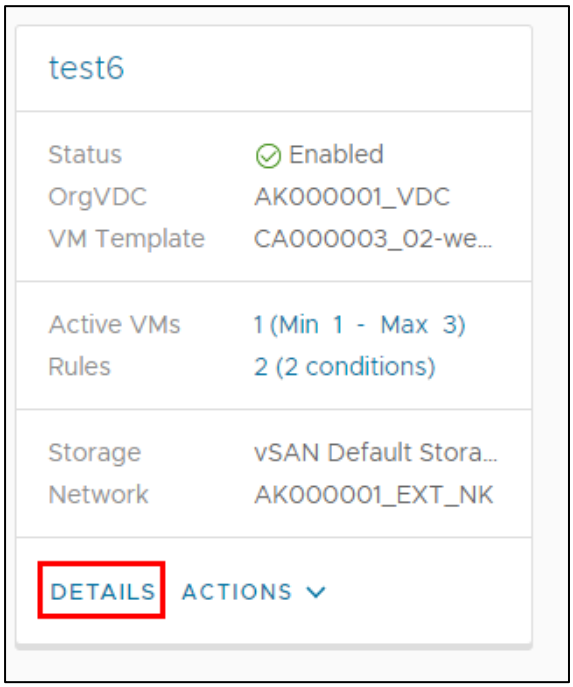


| Task | Rule | Status | Start Time | Completion Time |
|---|---|---|---|---|
| Create | | Completed | 09/01/2022, 09:36:02 AM | 09/01/2022, 09:36:02 AM |
| Grow(+1 VM) | Initial grow | Completed | 09/01/2022, 09:36:03 AM | 09/01/2022, 09:45:22 AM |



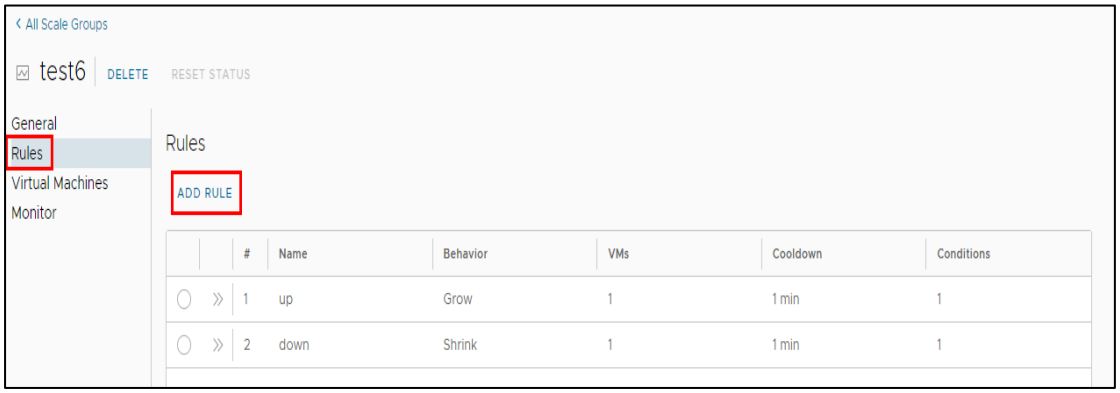

程序步驟 6:

建立完成，點選細項



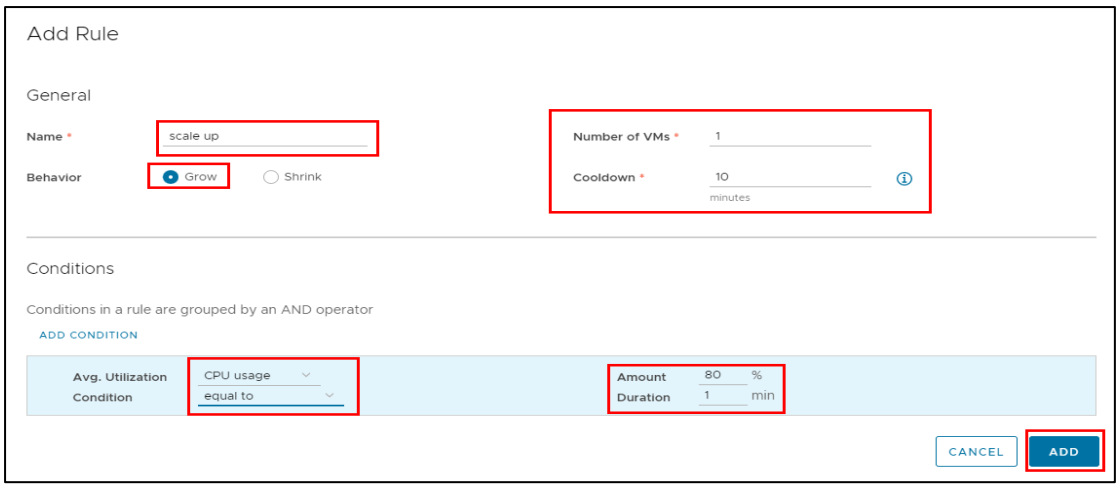

程序步驟 7:

點選規則，添加規格



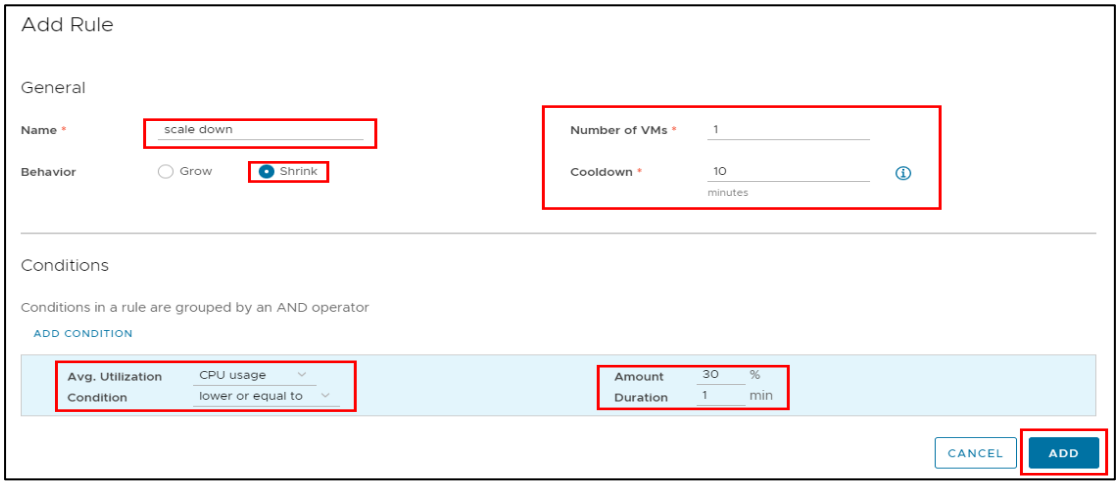

程序步驟 8:

依需求輸入辯示名稱，勾選佈署，VM 數量，狀況欄位輸入當 CPU 使用率達到制定數值維持多久就開始佈建 VM



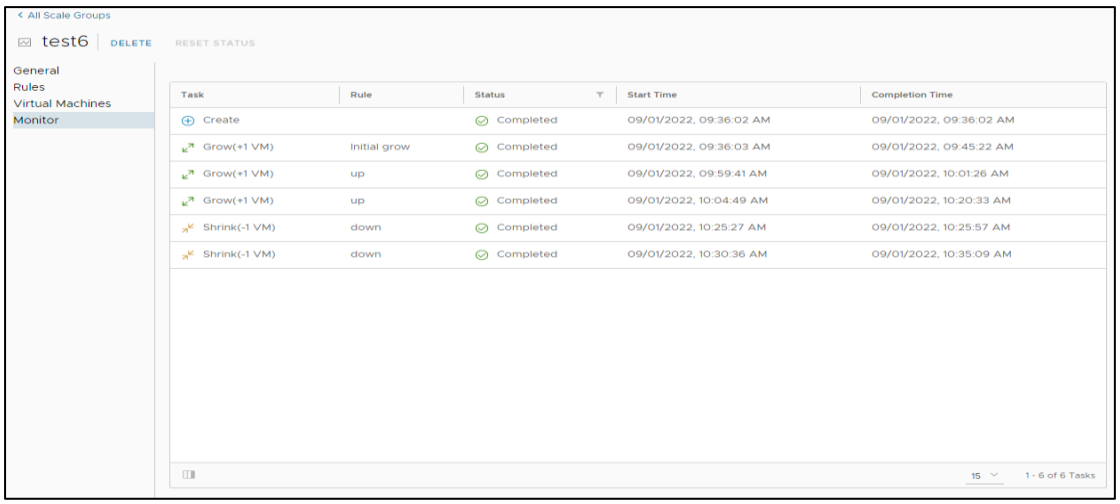

程序步驟 9:

依需求輸入辯示名稱，勾選佈署，VM 數量，狀況欄位輸入當 CPU 使用率達到制定數值維持多久，VM 就開始回收



程序步驟 10:

監視器

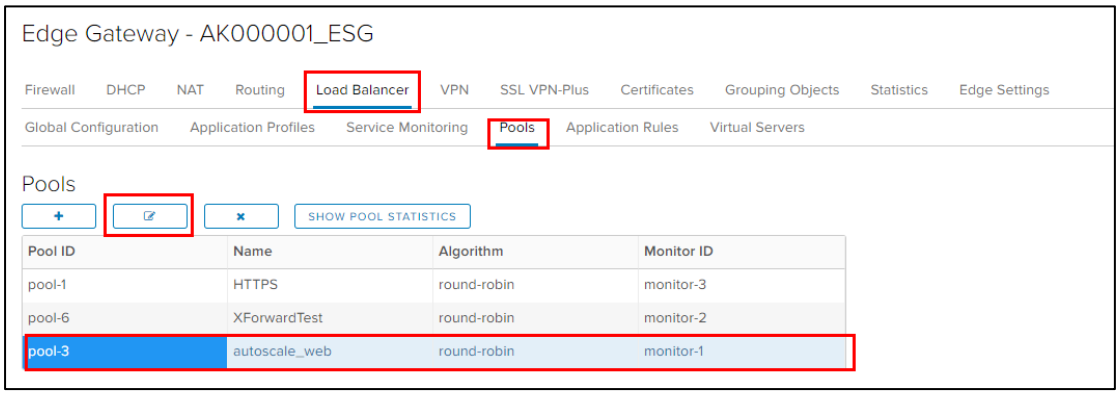



程序步驟 11:

如有申請 SLB 服務設定

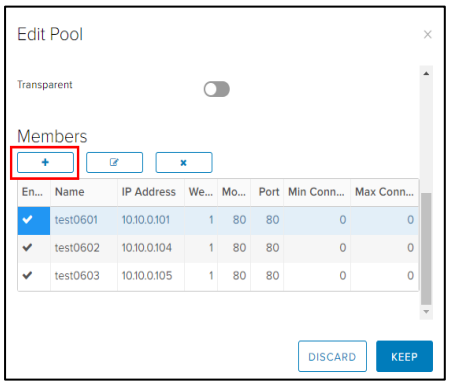
申請 SLB 服務

Edit SLB pools to add auto scale member



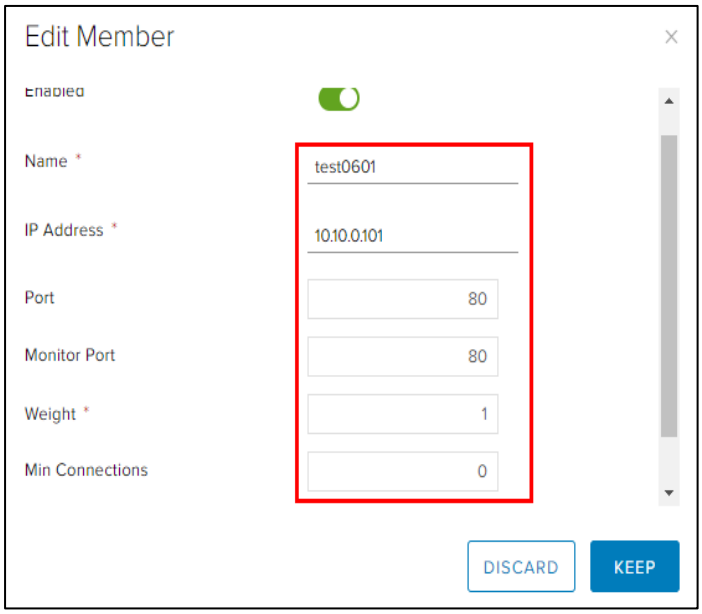

程序步驟 13:

Edit pool to add members



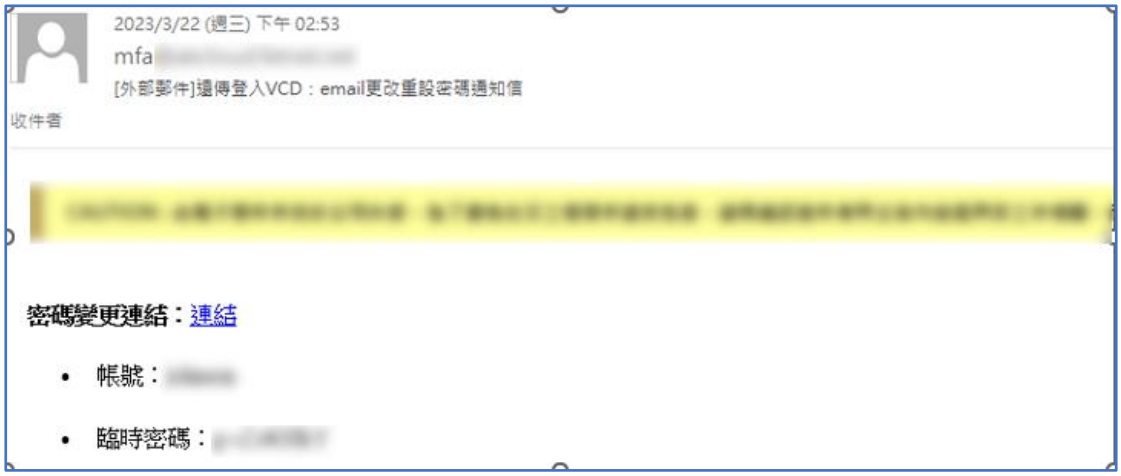
程序步驟 14:

add members name and IP, port



## 12. MFA 登入操作

系統會發送重設密碼通知信，用戶需依照通知信內容點選密碼變更連結輸入臨時帳號 密碼進行變更。



依照 email 內容填入臨時帳密

用戶需要自行安裝 Authenticator AP，依照 App 產出資訊填入一次性驗證碼欄位。Device Name :輸入用戶編號

用戶輸入新密碼

## 即可登入用戶 tenant

## 登出重新登入驗證

輸入新的帳號 密碼

輸入 Authenticator AP 產出一次性驗證密碼

即可登入

VMware Cloud Director
資料中心
應用程式
網路
程式庫
管理
監視器
更多
虛擬資料中心
環境
站台: 1
組織: 1
虛擬資料中心: 2
執行中應用程式
虛擬機器: 2
vApp: 2
應用程式
CPU
記憶體
儲存區
1
vApp
2 GHz
2 GB
287.24 GB

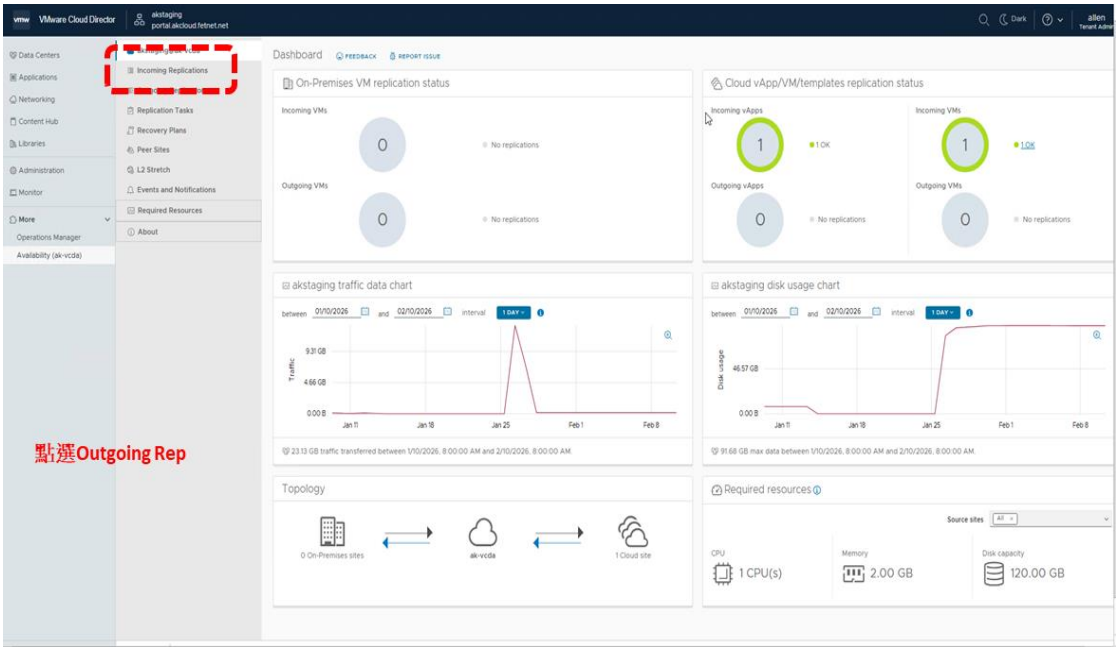
## 13. VCDA 操作說明

A. 由 Portal 介面選取 VMWare VCDA 功能(申請 VCDA 功能需有於另一 SITE 帳號，範例主 SITE 為台中，DR SITE 為台北，故由 DR SITE 登入並開啟 VCDA)

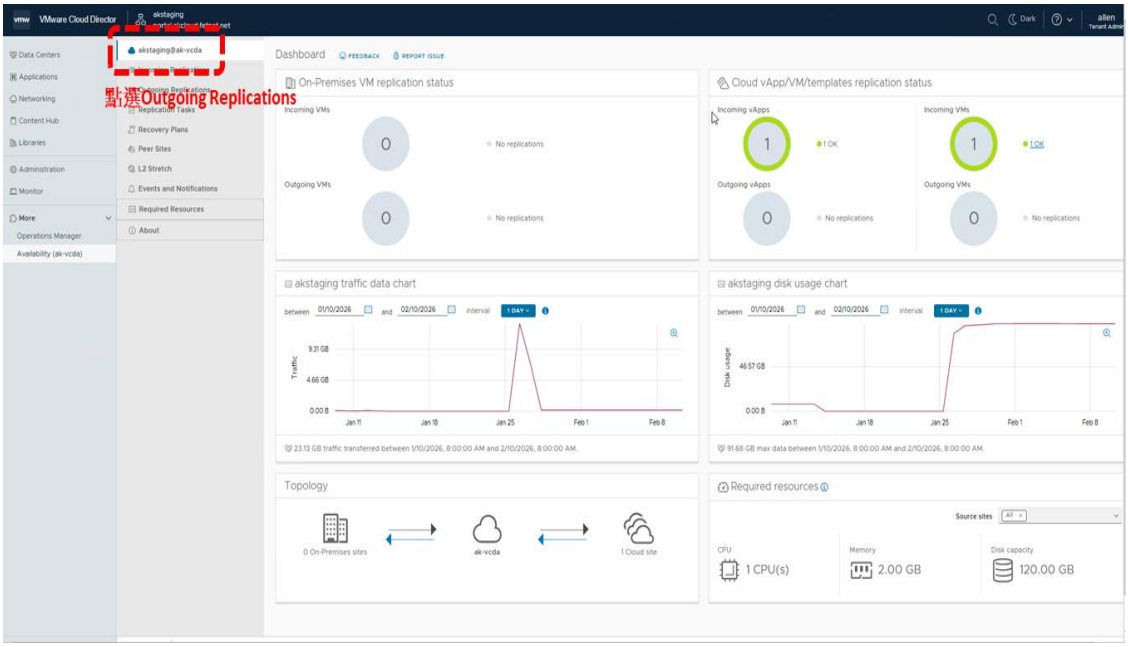
台中 site 網址: https://FETVMWARE.VMCLOUD.FETNET.NET

台北 site 網址: https://PORTAL.AKCLOUD.FETNET.NET

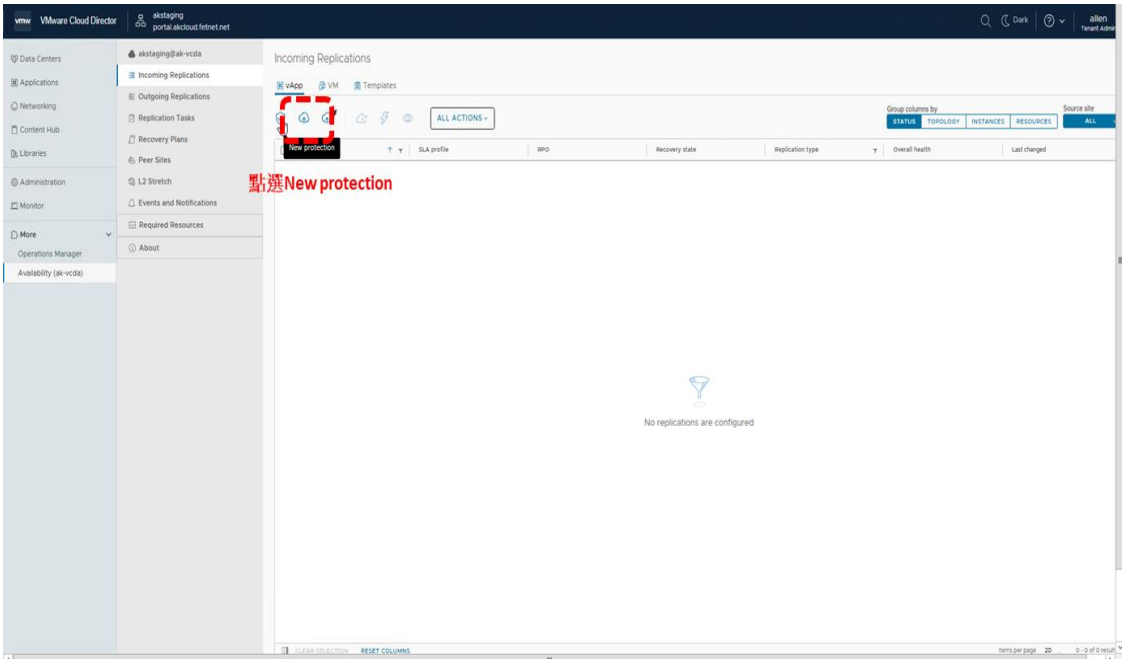
B. 登入 VMWare VCDA 介面操作 ，依需求選取 Incoming Replications 傳入抄寫或 Outgoing Replications 傳出抄寫及 FAILOVER 切換(TEST)功能。



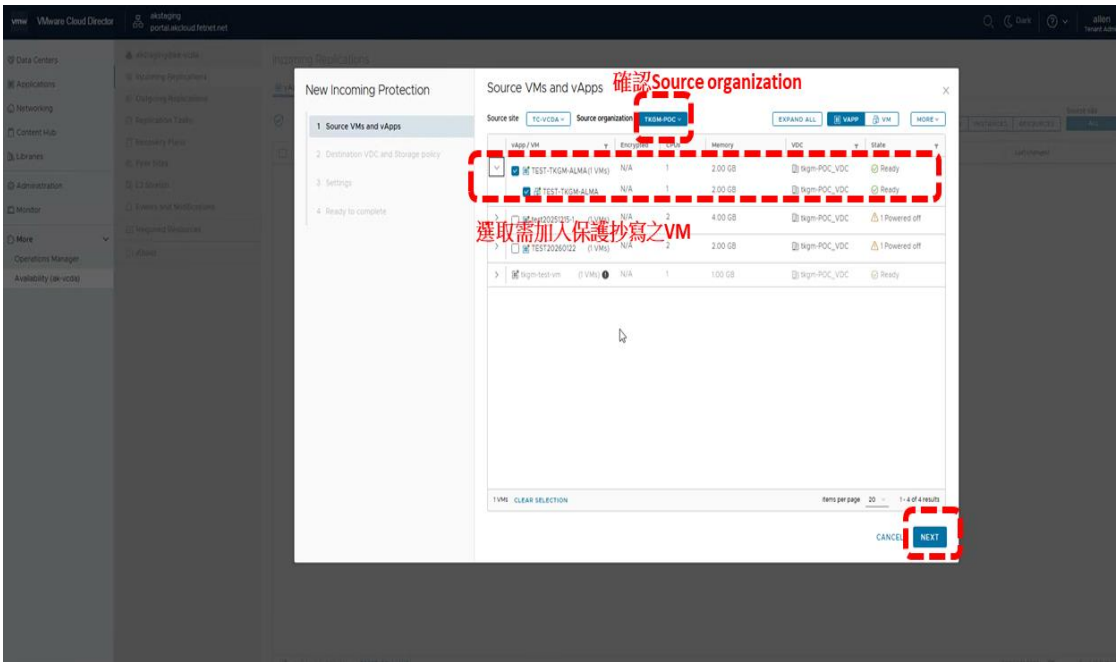
C. 執行新增保護抄寫至 DR SITE 操作 ，選取 Incoming Replications 傳入抄寫。



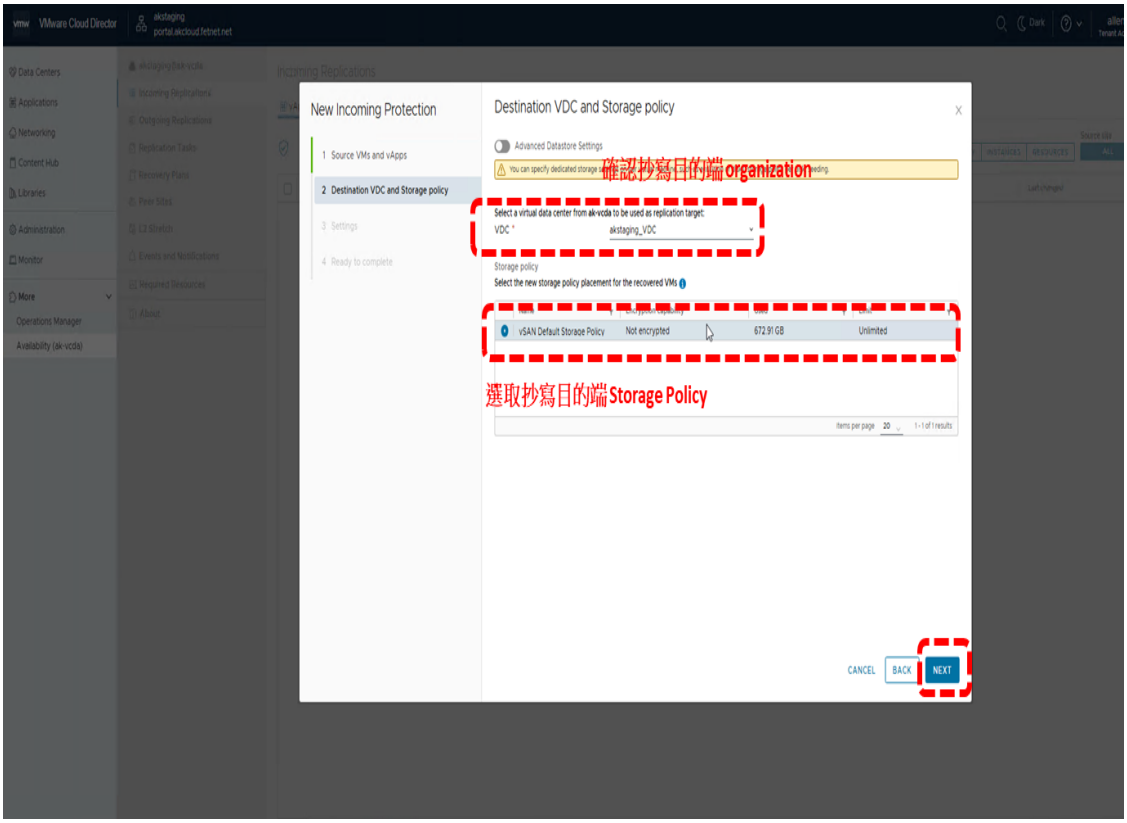

D. 選取 New protection 新增 VM 保護抄寫。



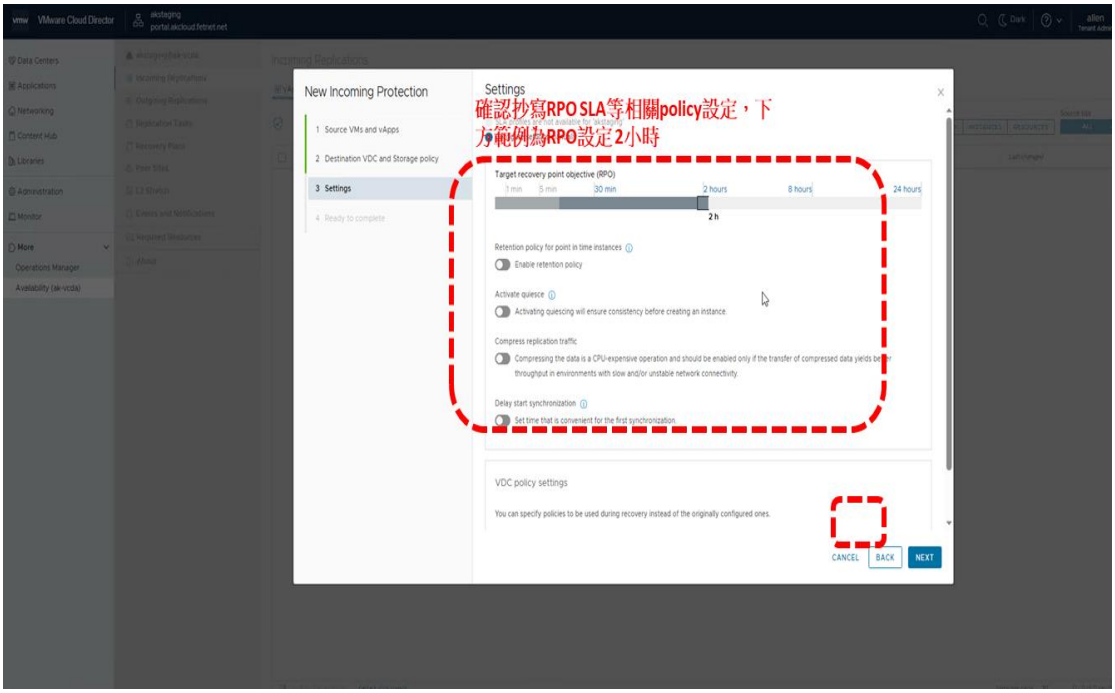

E. 確認 Source organization，選取需加入保護抄寫之 VM，選取 NEXT。



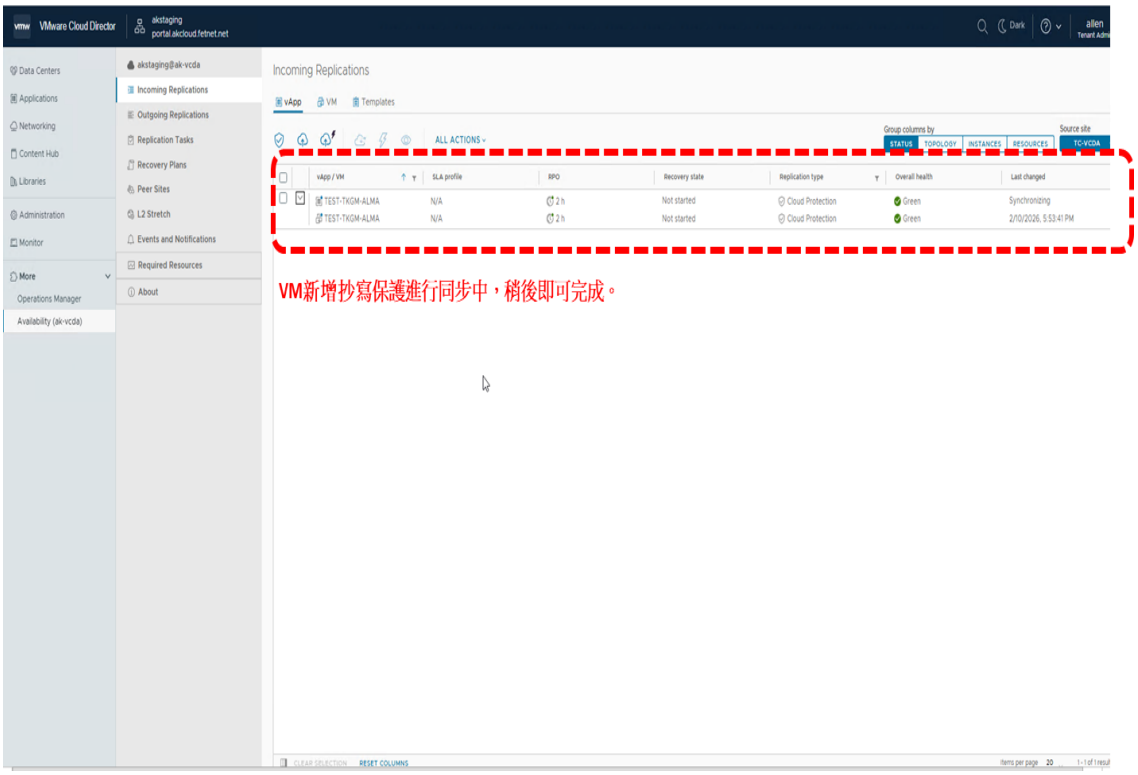

F. 確認抄寫目的端 organization，選取抄寫目的端 Storage Policy，選取 NEXT。



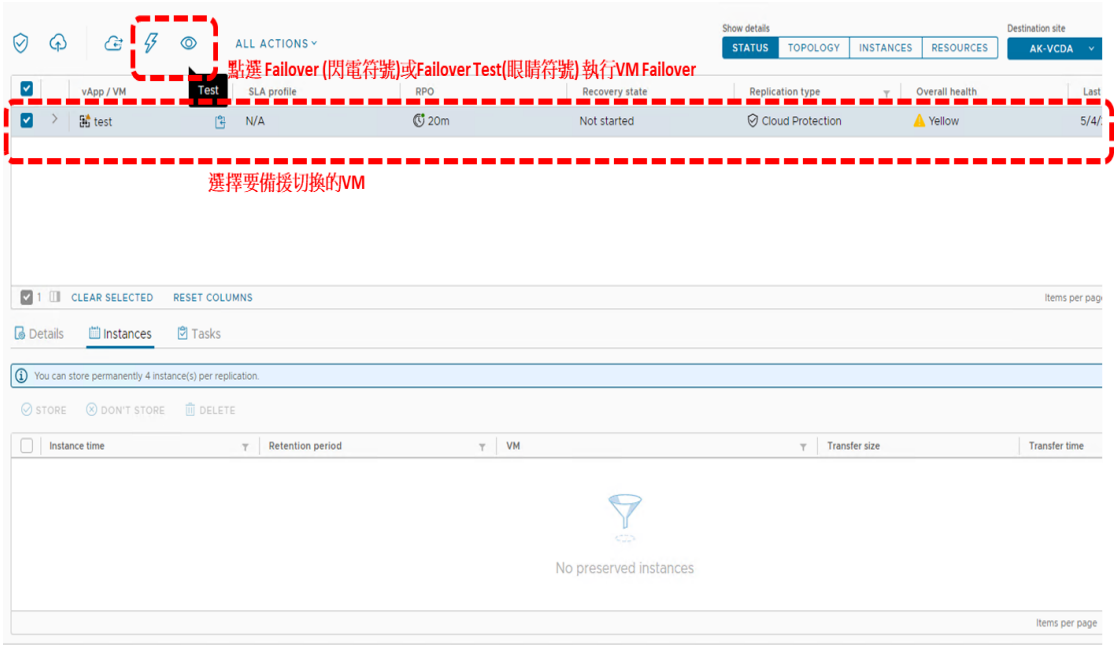

G. 確認抄寫 RPO SLA 等相關 policy 設定，下方範例為 RPO 設定 2 小時，選取 NEXT。



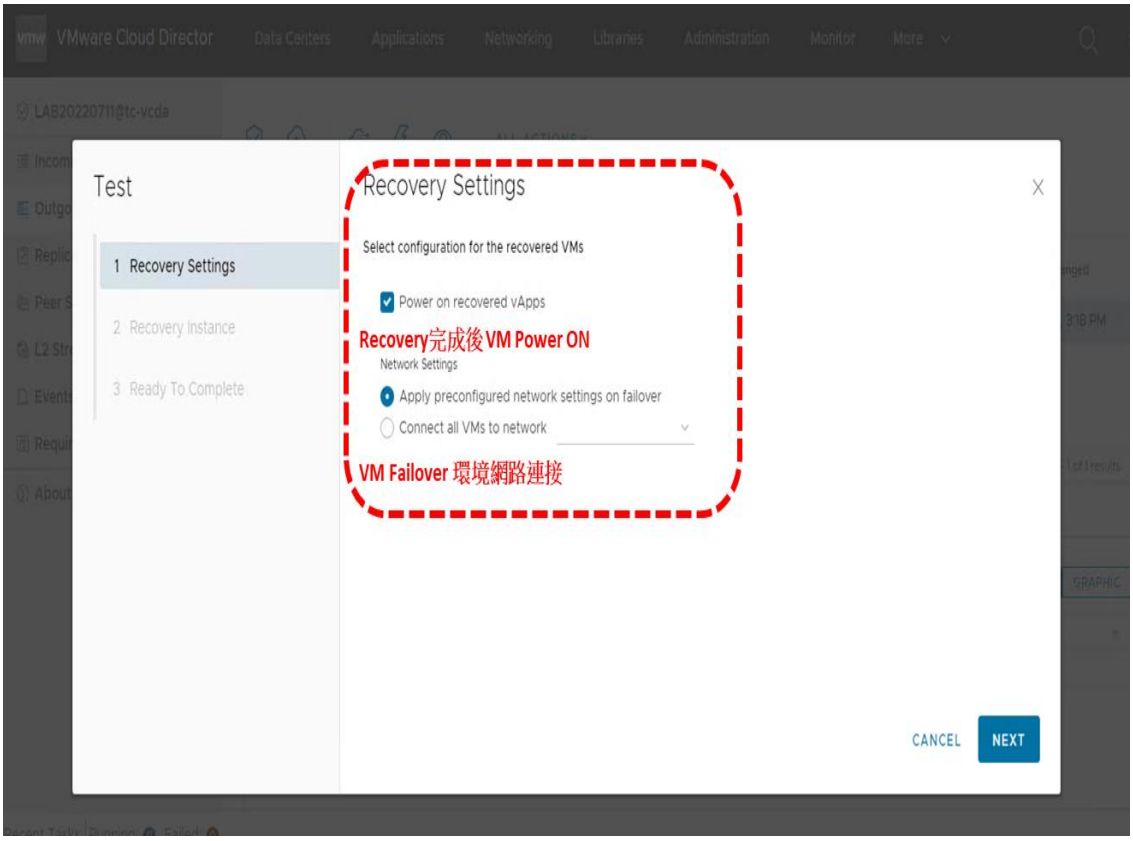

## H. VM 新增抄寫保護進行同步中，稍後即可完成。



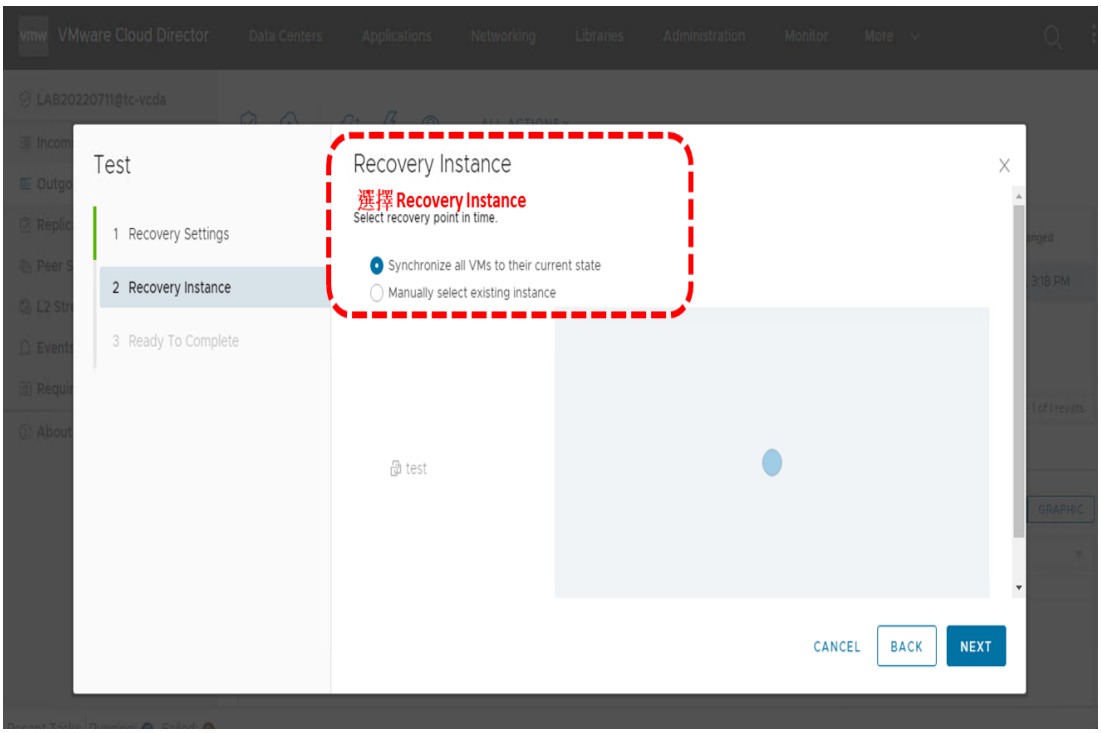

## I. 操作 VCDA 的 Failover(或 TEST)功能步驟，過程選擇要備援切換的 VM，點選 Failover (閃電符號)或 Failover Test(眼睛符號) 執行 VM Failover 驗證



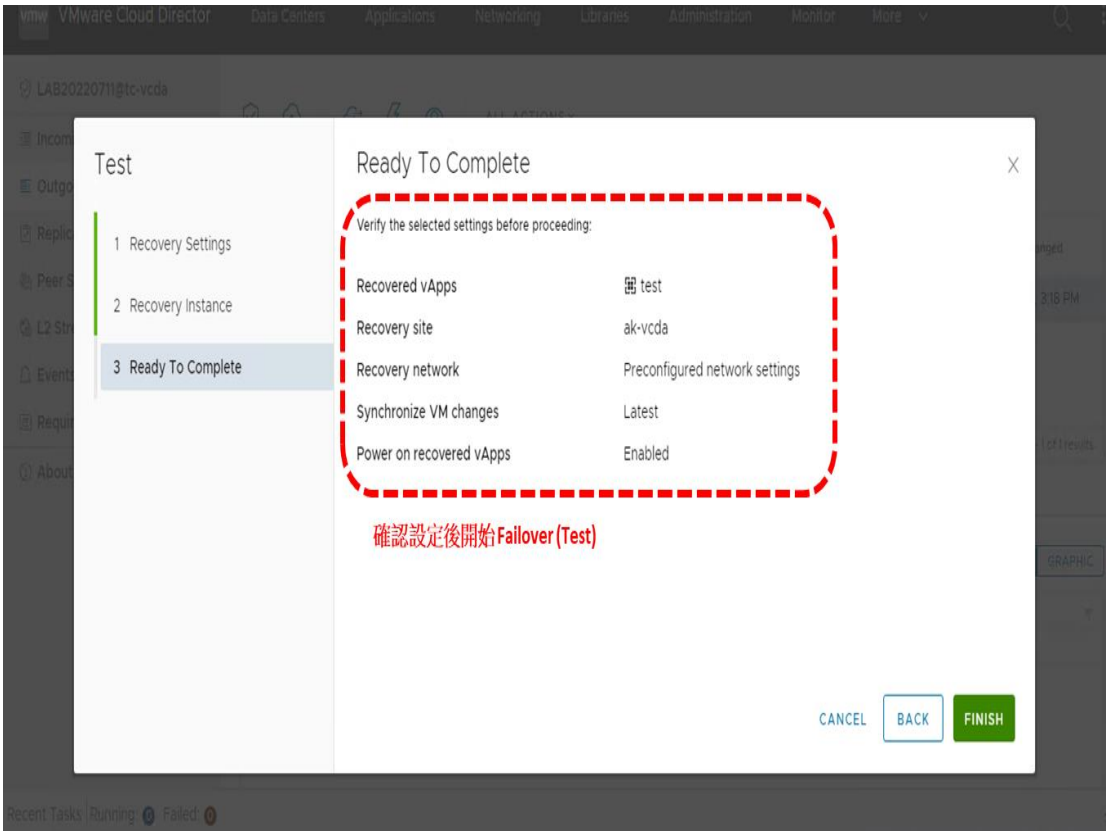

J. 選擇 Failover Recovery Settings，選擇 Recovery 完成後 VM Power ON 及 Failover Recovered 環境網路連接。



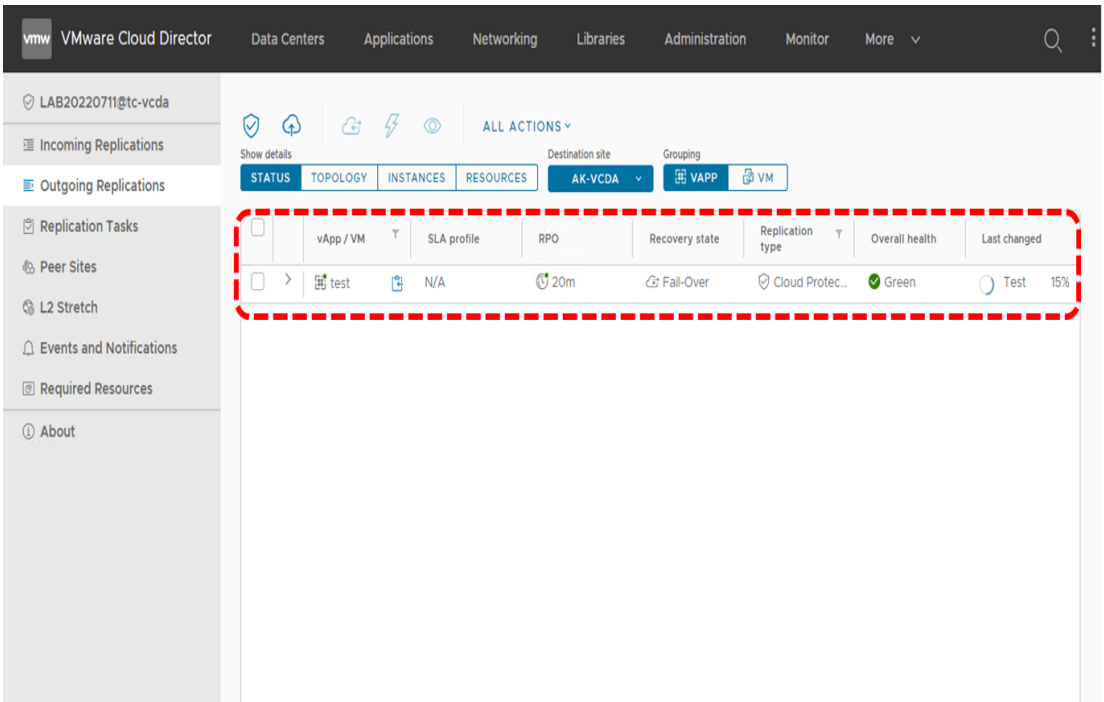

K. 選擇 Failover 相關還原點(Recovery Instance)。



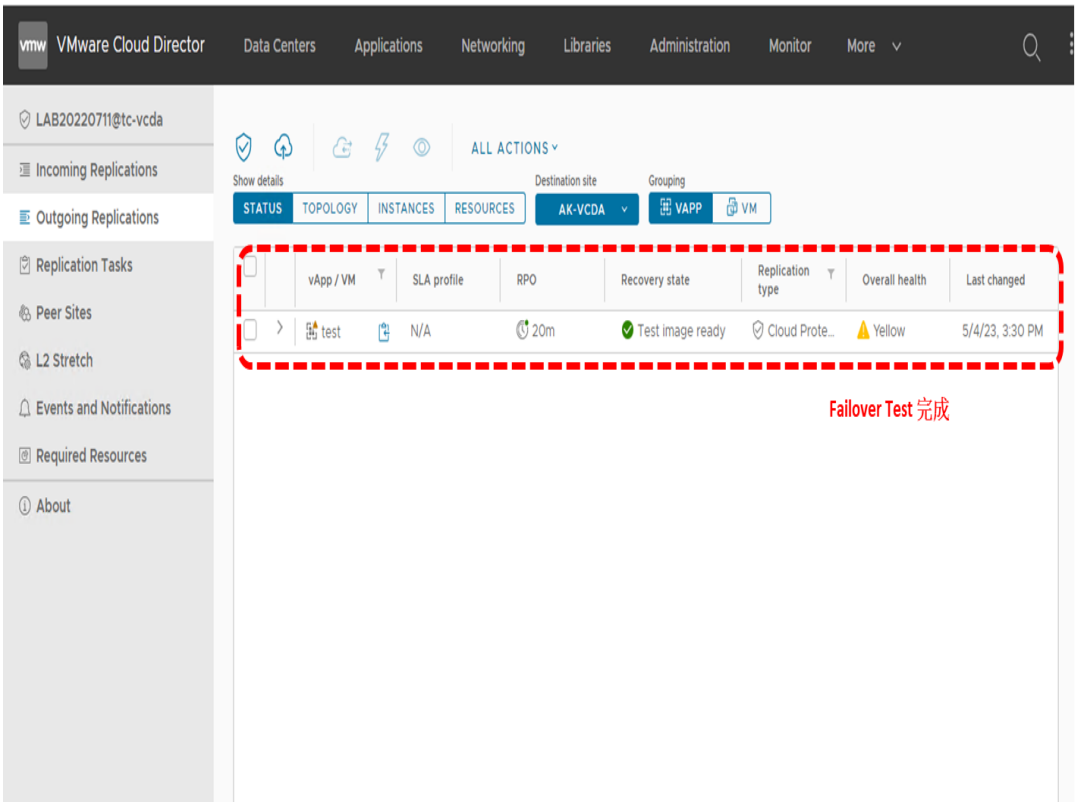

L. **確認 Failover (Test)相關設定，點選 FINISH 開始 Failover (Test)。**



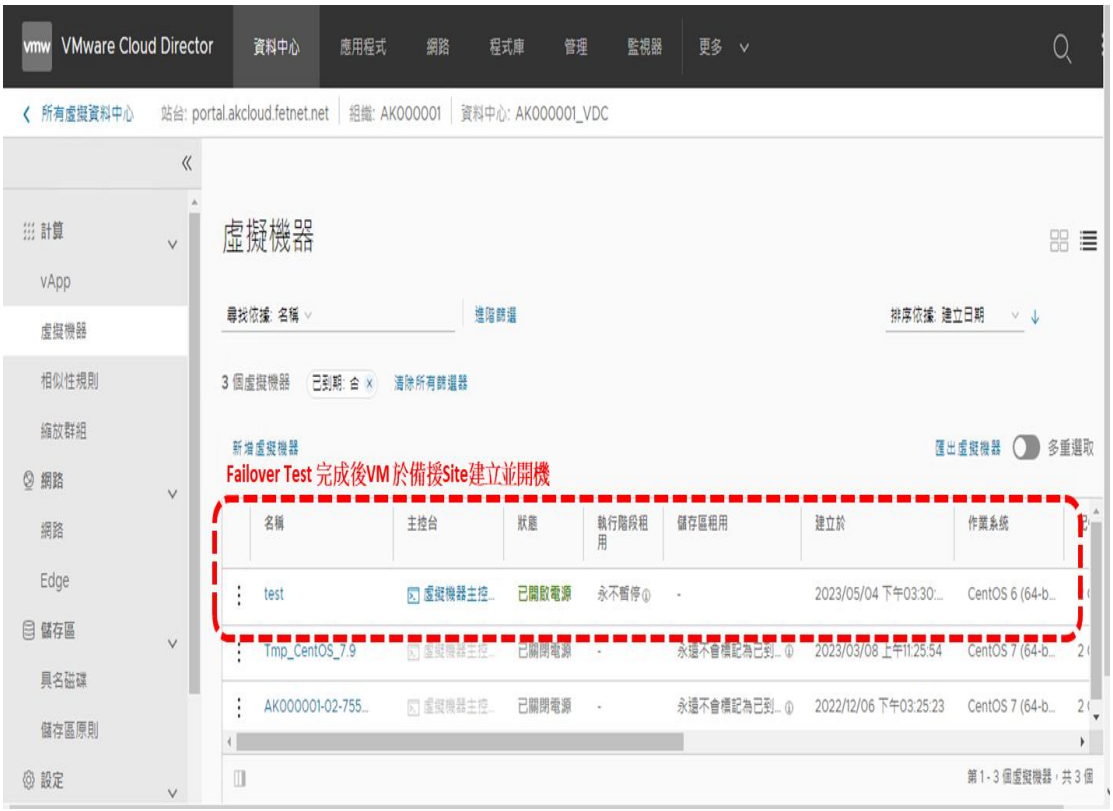

M. **Failover TEST 執行中，Recovery state 狀態顯示為 Fail-Over。**



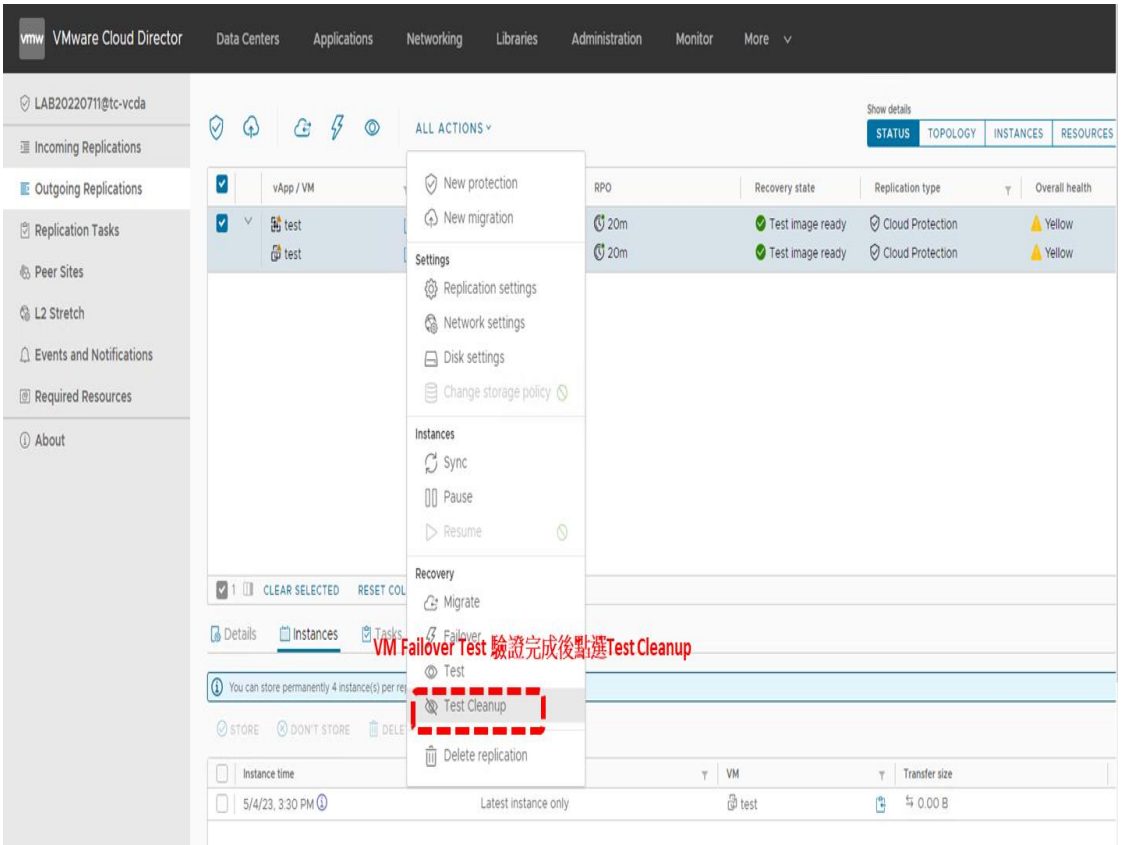

N. **Failover TEST 執行完成，Recovery state 狀態顯示為 Test image ready。**



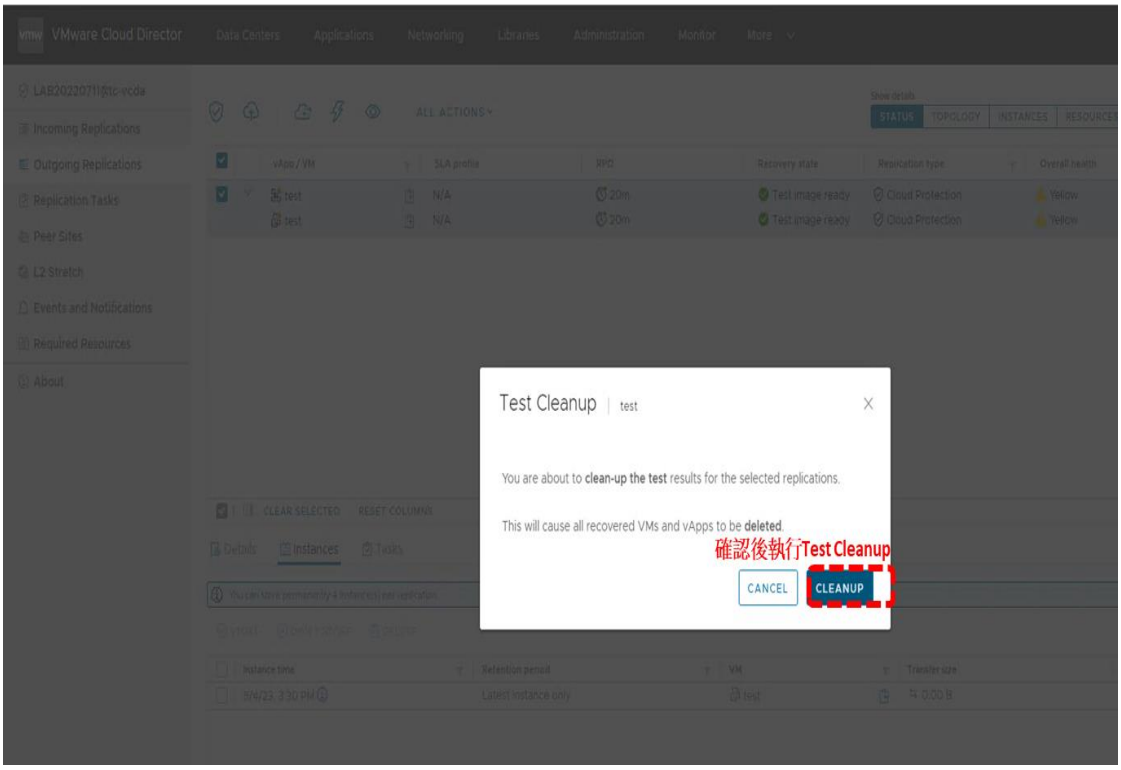

O. **Failover TEST 執行完成後，Failover Recovered VM 於備援 DR Site 建立並開機。**



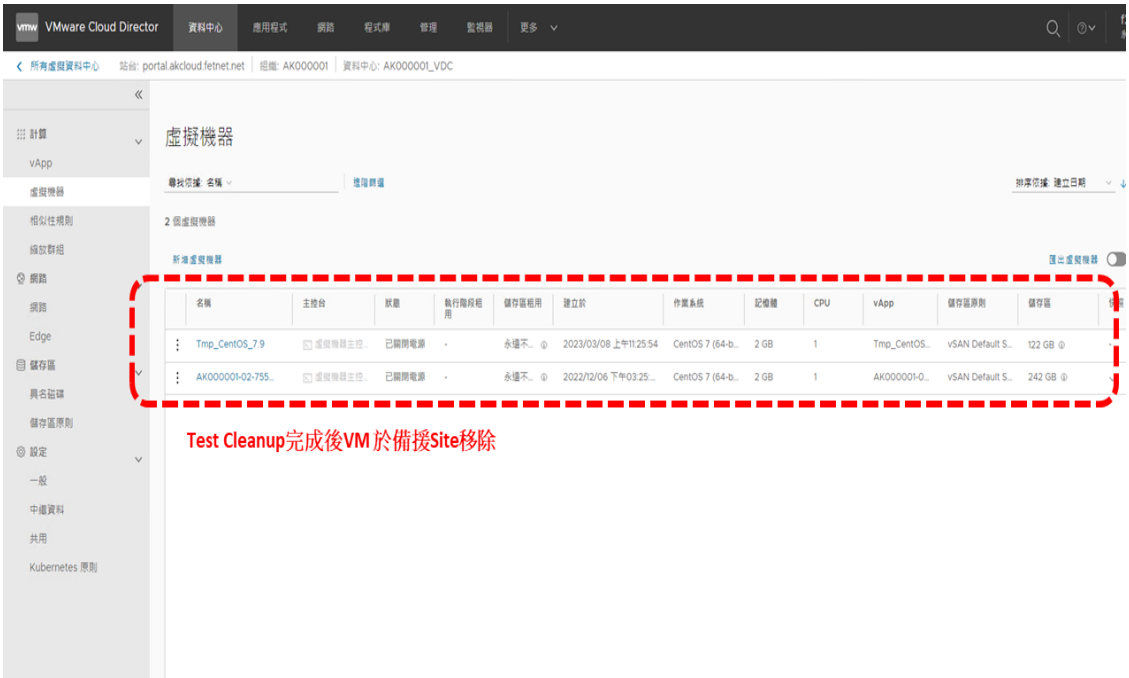

## P. VM Failover TEST 驗證完成後，可再點選 Test Cleanup 。



Q. **確認後點選 Test Cleanup，此動作將會把步驟 14 於備援 Site 建立之 Failover Recovered VM 刪除 。**

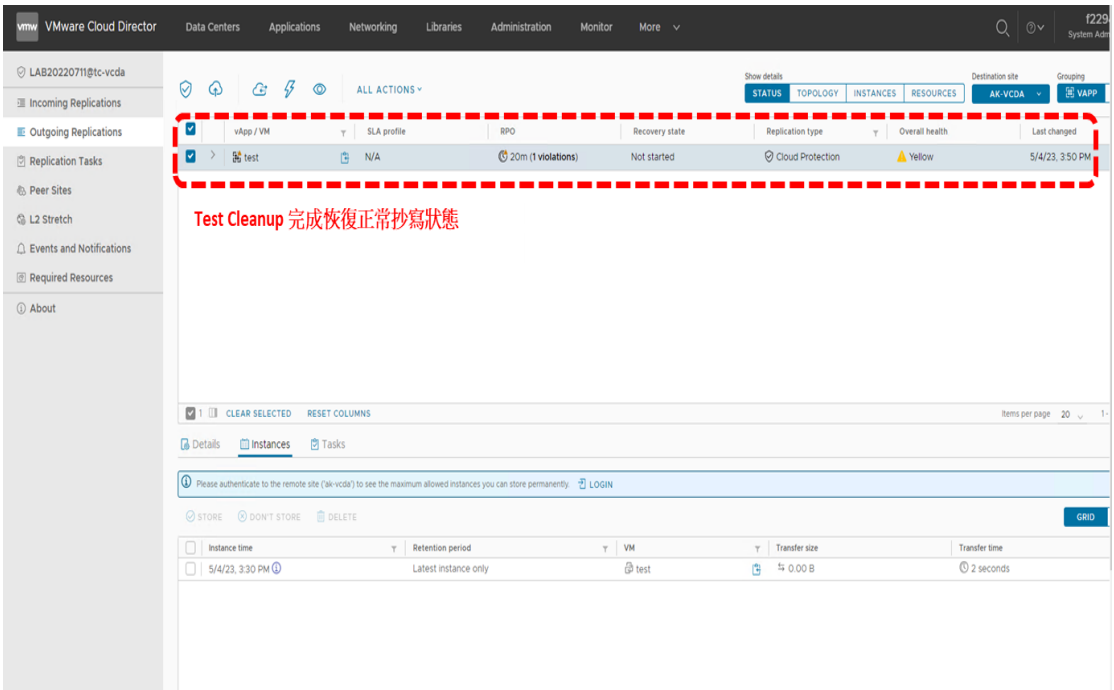



R. **Test Cleanup 執行完成，可於備援 Site 發現 Failover RecoveredVM 已被移除。**



S. **Test Cleanup 執行完成後，VM 恢復正常保護及抄寫狀態**

**(RPO 20m 既有每 20 分鐘完成 1 份抄寫任務)。**




## 14. VM 資料防止外洩操作說明

**客戶在退租後可執行以下命令進行資料抹除或加密以防外洩**

Linux OS :

1. 用 Linux Live ISO 開機。
2. 執行 shred -v -n 1 /dev/sda (針對該 VM 的主要硬碟)。
3. 跑完後關機。

Windows OS :

1. Windows VM，開啟 BitLocker 對 C 槽（以及所有資料槽）進行全磁碟加密。
2. 不要備份修復金鑰！加密完成後，直接重新啟動 VM。

## *Appendix 附錄:*

### *A. 無法顯示遠端操控台 Remote Console (VMRC)*

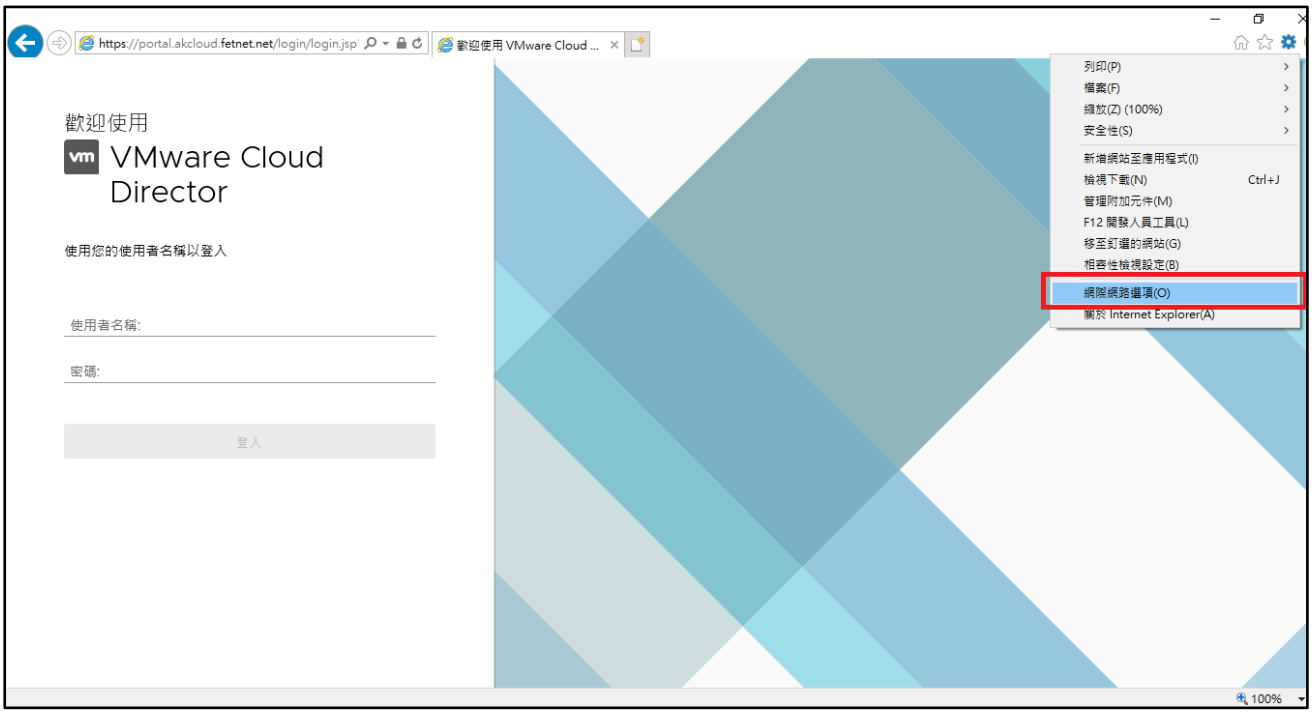
**Internet Explorer:**

增加 https://portal.akcloud.fetnet.net/tenant/ 您的用戶編號

或 https://fetvmware.vmcloud.fetnet.net/tenant/您的用戶編號 在信任的網站內

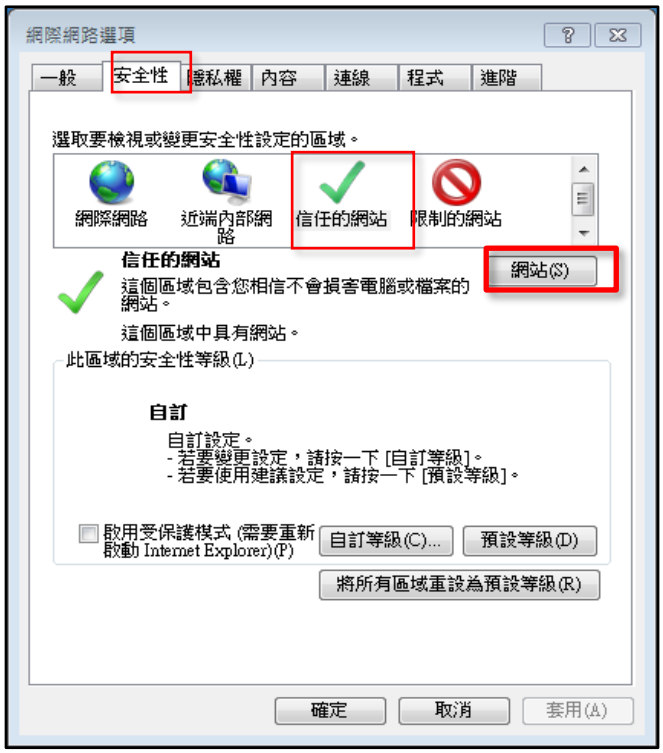
程序步驟 1:

按【工具】，再點選【網際網路選項】



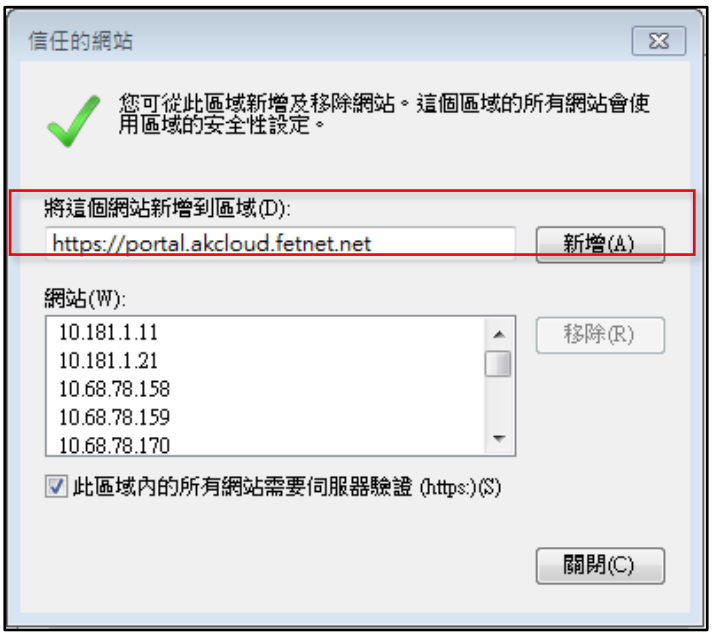
程序步驟 2：

按【安全性】，點選【信任的網站】，再按【網站】




程序步驟 3:

輸入 https://portal.akcloud.fetnet.net 或 https://fetvmware.vmcloud.fetnet.net，然後按【新增】



### *B. 虛擬機NTP時間校時方法*

**建議使用**[國家時間與頻率標準實驗室](#)**提供之NTP主機進行校時**

tock.stdtime.gov.tw
watch.stdtime.gov.tw
time.stdtime.gov.tw
clock.stdtime.gov.tw
tick.stdtime.gov.tw

**NTP校時操作參閱如下說明:**

**A.Windows:**

**以系統管理員使用命令列模式(CMD)執行下列指令**

1.設定同步之 NTP Server

w32tm /config /update /manualpeerlist:stdtime.gov.tw

2.進行同步

w32tm /resync

**B.Linux:**

**CentOS**

**先行安裝 ntp 套件:**

**CentOS:**

```
$ sudo yum install ntp -y
```

**Ubuntu:**

```
$ sudo apt-get install ntp ntpdate
```

**使用 ntpdate 指令連接 ntp 伺服器同步時間**

```
$ sudo ntpdate time.stdtime.gov.tw
```

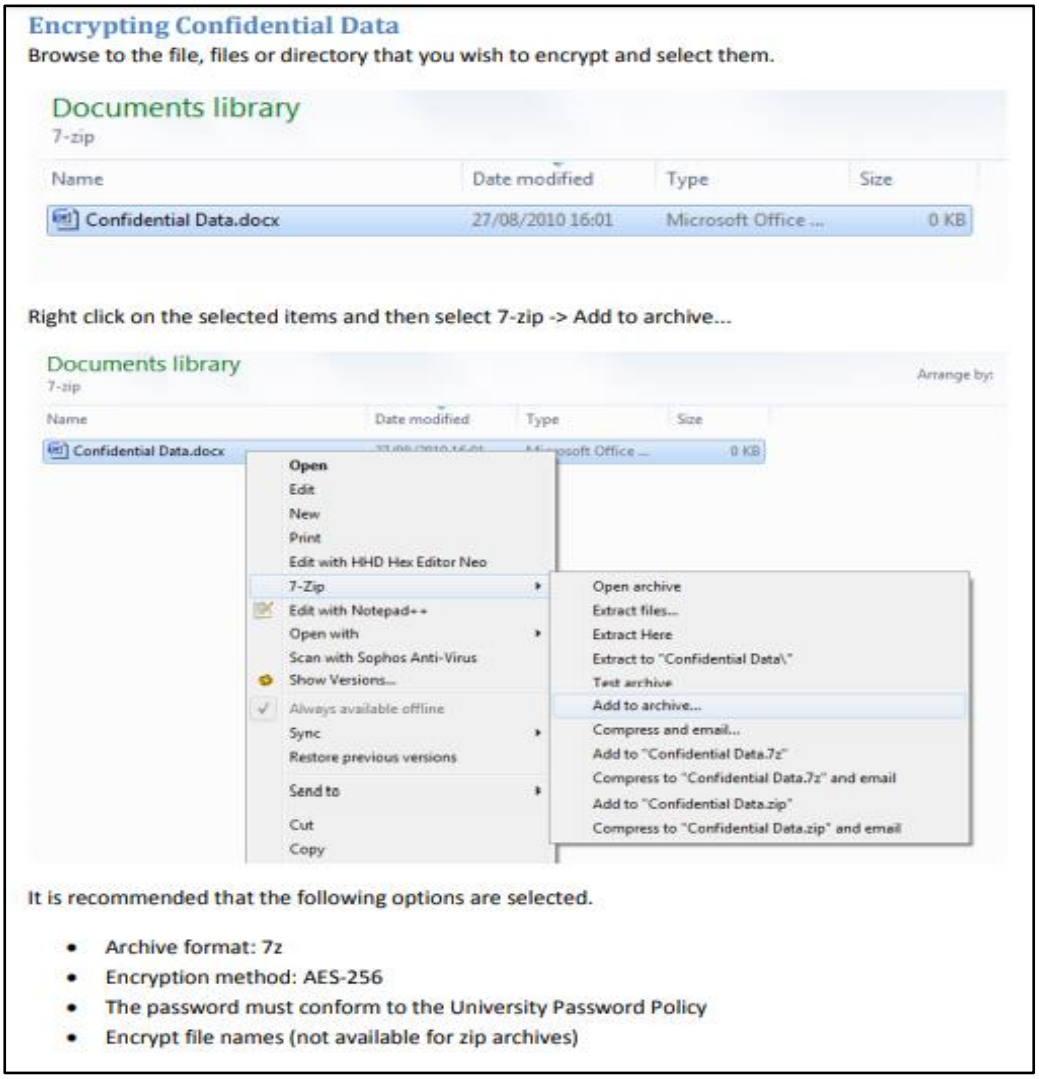
## *C. 如何保護虛擬機內的機敏資料*

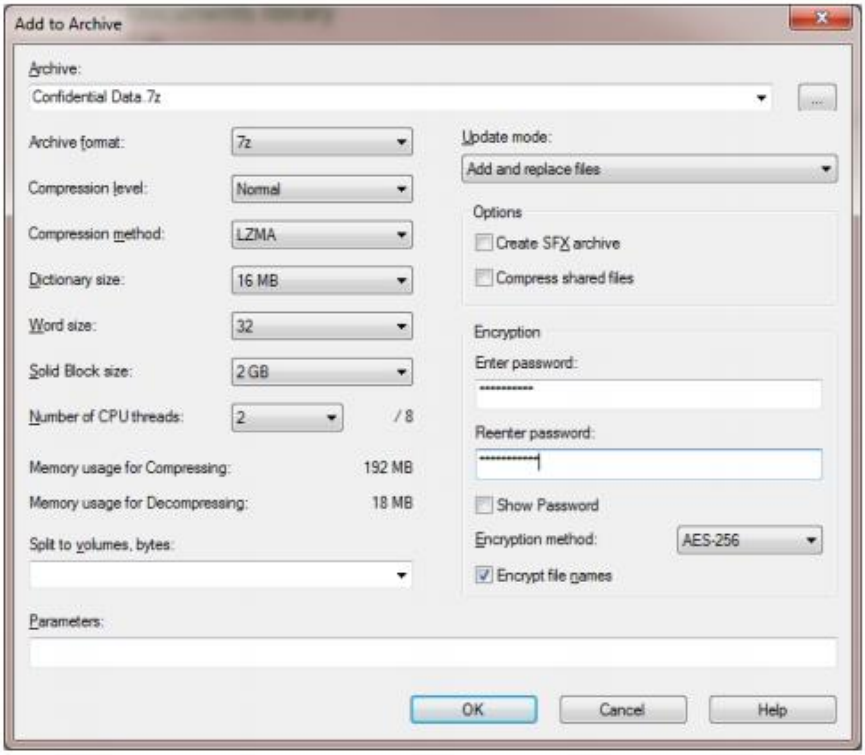
參考下列方式:

**7-zip為一般常用的Freeware**

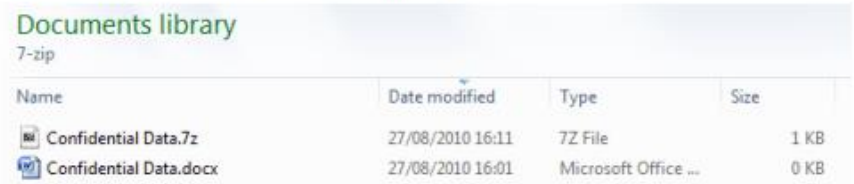
下載官網:https://www.developershome.com/7-zip/

加密操作範例:






You should then have a compressed and encrypted archive of your data.



## *D. 如何保護虛擬機的資訊安全*

基於IaaS服務的特性，遠傳會致力於雲端服務平台的資訊安全，然而客戶也要負起其虛擬機的資安管理及其中資料的安全保護責任，包含但不限於：惡意軟體防禦、備份、加密控制措施、弱點管理、日常維護及補丁(patch)、事件管理、合規檢測、安全測試、稽核、證據(包含日誌及稽核軌跡之蒐集、維護及保護)、當服務協議終止時的資料取回、身分認證及存取控制、客戶自身須遵循之法令規範等。

對於技術脆弱性風險的因應，建議客戶定期至相關網站查詢公告的弱點資訊，如：
N-ISAC：https://www.nics.nat.gov.tw/VulnerabilityNews.htm?lang=zh
TWCERT/CC：https://www.twcert.org.tw/tw/lp-132-1.html
微軟官網：https://portal.msrc.microsoft.com/en-us/security-guidance
資安趨勢部落格：https://blog.trendmicro.com.tw/
iThome資安：https://www.ithome.com.tw/security

## *E. 業務關係和提供服務的範圍、特點和位置(Scope, characteristics and location of business relationship and services offered)*

遠傳雲端運算服務是遠傳建置大規模的資料儲存中心，運用虛擬運算的技術，提供接近實體伺服器的虛擬運算環境，可以讓企業客戶在多種的作業系統上操作運用（**Windows**、**Linux**），如同本地連線般的呈現，提供企業客戶佈署自己所需要的軟體及應用項目，讓企業客戶在系統安全的基礎上使用雲端服務所帶來的可靠環境。

遠傳電信帶來強大的基礎設施即服務**(IaaS)**，為滿足企業客戶在雲端運算上的需求，特別針對本身雲端機房的維運管理、電力設施、網路品質及資訊安全皆投入龐大的資源，目前已於台北內湖及台中太平設置雲端機房，確保您的雲端資料僅存放於這兩處安全可靠的地點。此外，遠傳電信推出雲端運算服務包含了三種類型，經濟型、進階型及專業型，滿足企業在運算資源上的考量，打造您不論是資料的備援、測試服務的環境或多媒體網頁伺服器的應用，建構屬於您自己的雲端運算服務。

## *F. 雲端資訊安全要求(Information Security Requirement)*

a. 遠傳雲端運算服務建構在遠傳專業機房，擁有實體機房、實體設備及虛擬主機多層次的安全防禦機制。
b. 雲端運算服務之平台皆定期施作安全性檢核、安全漏洞的系統 Patch 以及作弱點掃描，遠傳提供客戶在網路防禦中，提供資安保全防火牆及入侵防禦系統和 Firewall 的保護，阻擋可能透過網路或系統漏洞，並監測連線協定，以減少系統無法作業服務的問題，定期更新 IPS 定義碼，運用複雜的演算引擎，保護您的服務不受攻擊。
c. 通過 ISO/IEC 27017 在 ISO 27001 基礎上，針對雲端服務客戶及供應商的作業規範，以優化雲端服務的安全性。
d. 通過 ISO/IEC 27018 在 ISO 27001 基礎上，針對公有雲個人可識別資訊(PII)處理者的作業規範，以保護個人資料。
e. 通過 CSA STAR 在 ISO 27001 基礎上，強化雲端服務安全的技術管控。
f. 通過 ISO 20000 (IT Service Management，ITSM) IT 服務管理系統要求的標準，著重用 IT 服務標準化確保服務的品質。

## *G. 雲端資訊安全責任共擔模型(Shared Security Responsibility Model, SSRM)*

**雲端資訊安全責任共擔模型的定義可能因不同的雲端服務而異，下面係以遠傳雲端運算服務(IaaS)之服務型態進行說明。**

| 項目 | 維運類型 | 維運責任方 |
|---|---|---|
| 1 | 資訊與資料 | 客戶 |
| 2 | 設備(手機和個人電腦) | 客戶 |
| 3 | 帳戶與身分 | 客戶 |
| 4 | 身分與目錄基礎設施 | 客戶 |
| 5 | 應用程式 | 客戶 |
| 6 | 作業系統 | 客戶 |
| 7 | 網路控制 | 客戶 |
| 8 | 虛擬機監視器 | 遠傳電信 |
| 9 | 實體主機 | 遠傳電信 |
| 10 | 實體網路 | 遠傳電信 |
| 11 | 實體資料中心 | 遠傳電信 |

針對各維運類型細部涉及的範圍，依照各別客戶合約可能有所不同，若想進一步確認權責劃分，請諮詢負責業務人員。

## *H. 雲端客戶變更需求程序(Cloud Customer Change Management Process)*

為提供更穩定雲端服務，若客戶使用上有任何變更需求，可經由業務或專案經理提出需求，若變更需求過大，需要專業人員規劃則需進行額外費用付費要求，經由評估和主管授權，並取得客戶同意，依照需求執行變更或拒絕申請，以下是變更流程：

a. 客戶向業務或專案經理提出變更申請
b. 雲端維運團隊評估變更
c. 雲端維運團隊主管授權/拒絕變更要求
d. 取得客戶同意變更授權
e. 雲端維運團隊協調變更執行
f. 客戶檢視變更結果
g. 結束變更程序

因應遠傳雲端運算服務為 IaaS 服務，若客戶有需要委託遠傳電信代為操作作業系統層以上之變更或設定，請洽業務或專案經理，遠傳電信將視需求酌收不等費用，作業系統層以上之變更或設定包含但不限於以下項目：

a. 虛擬機網路架構異動
b. 作業系統密碼變更
c. 作業系統問題處理
d. 作業系統弱點修正
e. 映像檔製作或提供
f. 備份和還原作業
g. 虛擬機移轉或升級
h. 備援切換演練
i. 本機防火牆規則新增，刪除，異動
j. 伺服器負載平衡新增，刪除，異動
k. 憑證更換
l. 弱點掃描
m. 複製虛擬機
n. 匯出虛擬機映像檔
o. 虛擬機先建後拆需求
p. 部署新的虛擬機
q. 刪除有問題或異常的虛擬機

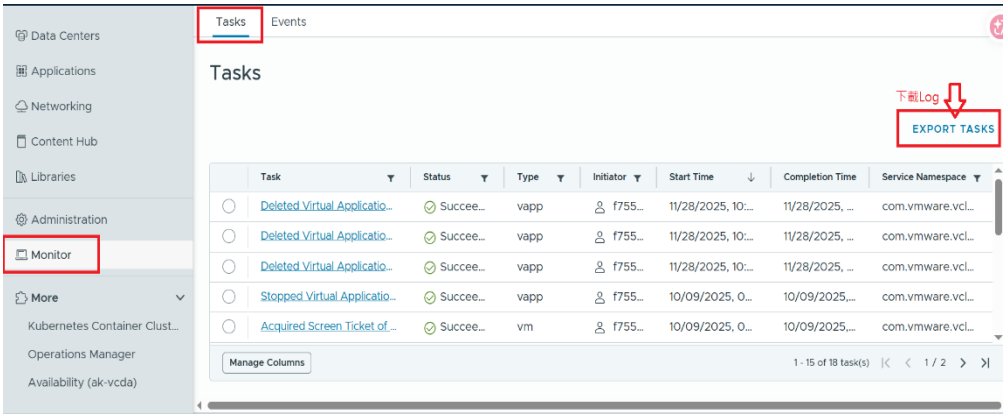
## I. *日誌記錄和監視能力(Logging and monitoring capability)*

a. 遠傳雲端運算服務提供完備的日誌記錄功能，具體操作步驟詳見前述章節【檢視使用紀錄】。

b. 遠傳雲端運算服務提供完備的監視功能，具體操作步驟詳見前述章節【VM 效能監控( vCloud Director )】。

c. 雲端客戶日誌保留時間:半年

d. 雲端客戶日誌下載:



## *J. 資安事件的通報與溝通處理(Incident management and communication procedures)*

若發現本服務可能的資安事件，我們將透過以下方式聯繫您：

a. 透過業務窗口。
b. 透過24小時機房值班人員(OP)。
c. 透過Email或電話。

客戶若發現有關本服務的資安事件，可透過客服專線 (02) 4499-365 進行通報，遠傳得視必要情形通知相關客戶處理事宜，包含但不限於資訊安全事故的範圍、發生的時間、處理聯絡資訊及補救措施。

## *K. 稽核權利(Audit rights)*

遠傳雲端運算服務在不影響商業機密或有條件的情況下，可配合客戶要求進行稽核，稽核範圍僅以遠傳雲端運算服務為限，且需依照相關需求進行收費。

## *L. 第三方評鑑(Third party assessment)*

**遠傳雲端運算服務每年都有進行內部稽核，並經過第三方認證機構驗證，取得 ISO 27001、ISO 27017、ISO 27018、 ISO 27701 與 CSA STAR 的認證，且證書持續有效，若客戶對於遠傳雲端運算服務有進一步的問題，可洽詢業務。**

## *M. 服務終止(Service termination)*

**a.** 客戶如欲終止本服務時，應自親向遠傳電信或委託代理人辦理書面終止租用手續，並繳清所有費用。

**b.** 客戶申請終止租用本業務時，應於預定終止租用之日前一個月以前提出申請。

c. 客戶申請暫停租用、違反法令或因欠費致被暫停租用者，其停止租用期間，租費仍應照繳。

d. 客戶申請終止租用者，其相關軟體、程式、資料內容應於預定服務終止日前取回，逾期未取回時，客戶視同放棄資料保留之權利，原則將於終止日次月底前進行系統資料之刪除，如客戶有特殊要求，可立即刪除或特別保留額外議定時間。

e. 遠傳電信因服務所掌握之客戶相關資料，新增、過戶及異動服務之申請書將永久保存，終止服務之申請書於租用終止後保留一年，並於到期後定期銷毀刪除；前述內容如遠傳電信資料保存等相關作業流程內容異動調整時，則依調整後之內容為之，除非依法需保留更長者不在此限。

f. 前述服務終止作業如有更改，請以最新版服務契約為準，或可洽業務窗口進行確認。

## *N. 互操作性和可攜性要求(Interoperability and portability requirements)*

遠傳雲端運算服務提供客戶匯入及匯出映像檔的功能：

a. 匯入映像檔具體操作步驟詳見前述章節【掛載 ISO檔或OVA檔】。
b. 匯出映像檔請洽業務窗口，將由專人協助您作業。

## *O. 資料隱私(Data privacy)*

在遠傳雲端運算服務中，依照雲端資安責任共擔模型(SSRM)，資料保護係由客戶自行負責。客戶需確保在雲端基礎設施中存儲的資料受到適當的加密、儲存安全、存取控制和備份。客戶應自行依照適用的法令法規如個人資料保護法、GDPR、HIPAA等，並對資料安全性和合規性進行評估和管理。雖然遠傳雲端運算服務已提供基本資安安全功能與步驟，但客戶仍需承擔最終保護責任。