保護 Azure / AVS 上的工作負載

NetApp Solutions

NetApp
April 12, 2024

目錄

保護 Azure / AVS 上的工作負載

使用ANF和Jetstream進行災難恢復

災難恢復至雲端是一種彈性且具成本效益的方法、可保護工作負載免受站台停機和資料毀損事件（例如勒索軟體）的影響。使用VMware VAIO架構、內部部署的VMware工作負載可複寫至Azure Blob儲存設備並進行還原、使資料遺失率降至最低或接近零、RTO接近零。

可以使用Jetstream DR無縫恢復從內部部署複製到AVS的工作負載、特別是Azure NetApp Files 到還原的工作負載。它能在災難恢復站台使用最少的資源、並以具成本效益的雲端儲存設備、實現具成本效益的災難恢復。透過Azure Blob Storage、在Anf資料存放區中自動恢復、根據網路對應、Jetstream DR會將獨立的VM或相關VM群組恢復至恢復站台基礎架構、並提供時間點還原功能以保護勒索軟體。

本文件提供對Jetstream災難恢復作業原則及其主要元件的瞭解。

解決方案部署總覽

1. 在內部部署資料中心安裝Jetstream DR軟體。
   a. 從Azure Marketplace（ZIP）下載Jetstream DR軟體套裝組合、並在指定的叢集中部署Jetstream DR MSA（OVA）。
   b. 使用I/O篩選套件設定叢集（安裝Jetstream VIB）。
   c. 在災難恢復AVS叢集所在的相同地區配置Azure Blob（Azure儲存帳戶）。
   d. 部署DRVA設備並指派複寫記錄磁碟區（來自現有資料存放區或共享iSCSI儲存設備的VMDK）。
   e. 建立受保護的網域（相關VM群組）、並指派DRVA和Azure Blob Storage/anf。
   f. 開始保護。
2. 在Azure VMware解決方案私有雲中安裝Jetstream DR軟體。
   a. 使用Run命令安裝及設定Jetstream DR。
   b. 使用「掃描網域」選項新增相同的Azure Blob容器並探索網域。
   c. 部署所需的DRVA設備。
   d. 使用可用的vSAN或ANF資料存放區建立複寫記錄磁碟區。
   e. 匯入受保護的網域、並將RockVA（恢復VA）設定為使用ANF資料存放區來放置VM。
   f. 選取適當的容錯移轉選項、並針對接近零的RTO網域或VM開始持續重新補充。
3. 在災難事件期間、觸發容錯移轉至Azure NetApp Files 指定AVS DR站台中的各個資料存放區。
4. 在受保護的站台恢復之後、呼叫容錯回復至受保護的站台。在啟動之前、請確定符合本說明所述的先決條件 "連結" 此外、您也可以執行所提供的「頻寬測試工具」（BWT）、評估Azure Blob儲存設備在與Jetstream DR軟體搭配使用時的潛在效能及其複寫頻寬。完成先決條件（包括連線）之後、請從設定並訂閱適用於AVS的Jetstream DR "Azure Marketplace"。軟體套裝軟體下載完成後、請繼續執行上述安裝程序。

規劃及啟動大量VM的保護（例如、超過100個）時、請使用位於Jetstream DR Automation Toolkit的容量規劃工

具（CPt）。提供要保護的VM清單、以及其RTO和恢復群組偏好設定、然後執行CPt。

執行下列功能：

- 根據虛擬機器的RTO、將虛擬機器整合至保護網域。
- 定義最理想的DRVA數量及其資源。
- 預估必要的複寫頻寬。
- 識別複寫記錄磁碟區的特性（容量、頻寬等）。
- 估計所需的物件儲存容量等。

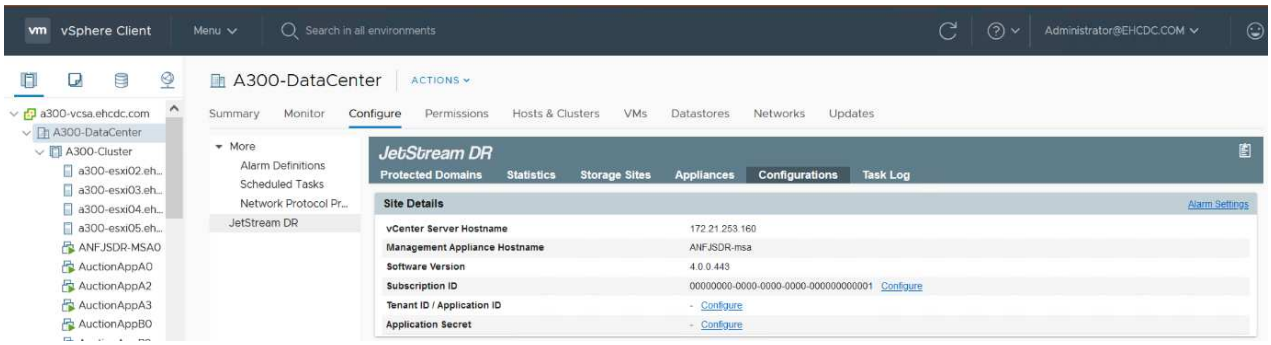
> 指定的網域數量和內容取決於各種VM特性、例如平均IOPS、總容量、優先順序（定義容錯移轉順序）、RTO及其他特性。

在內部部署資料中心安裝**Jetstream DR**

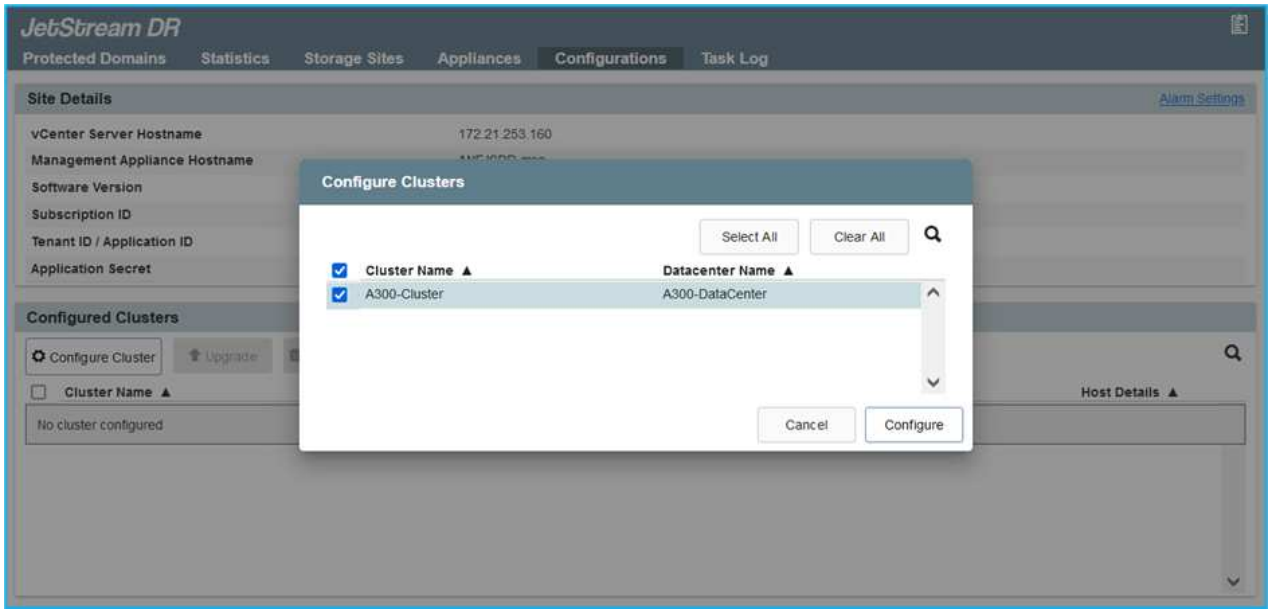
Jetstream DR軟體包含三個主要元件：「Jetstream DR管理伺服器虛擬應用裝置（MSA）」、「DR虛擬應用裝置（DRVA）」和「主機元件（I/O篩選套件）」。MSA用於在運算叢集上安裝及設定主機元件、然後管理Jetstream DR軟體。下列清單提供安裝程序的詳細說明：

如何為內部部署安裝**Jetstream DR**

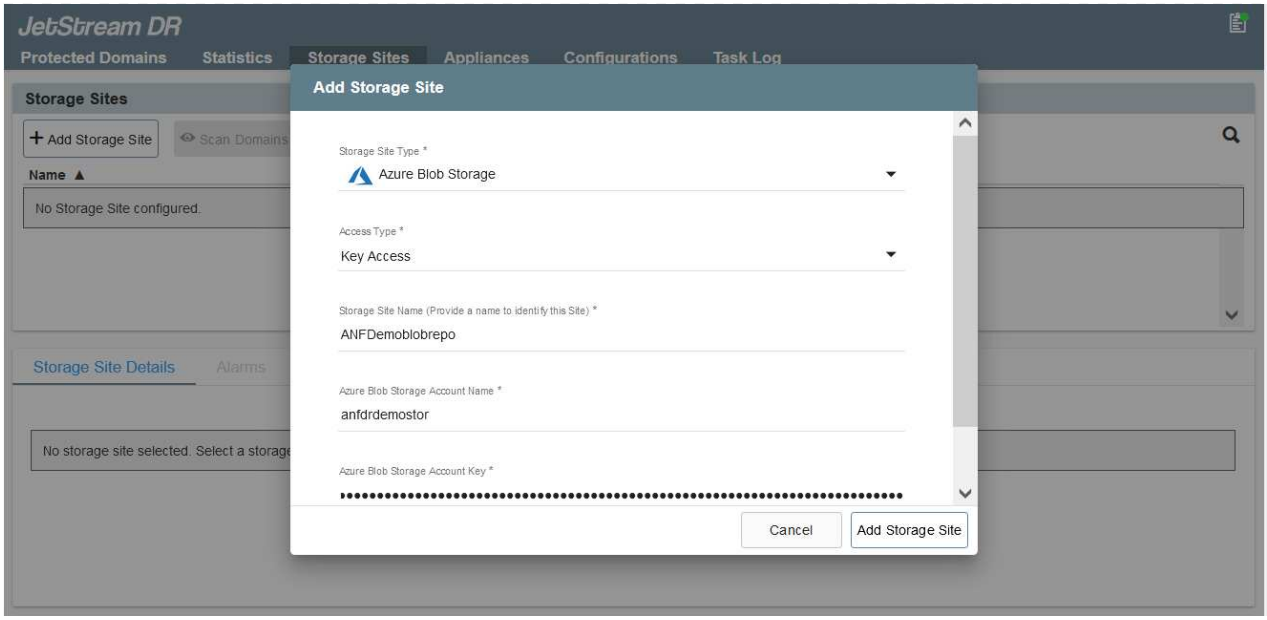
1. 檢查先決條件。
2. 執行容量規劃工具以取得資源和組態建議（可選、但建議用於概念驗證試用）。
3. 將Jetstream DR MSA部署至指定叢集內的vSphere主機。
4. 在瀏覽器中使用其DNS名稱啟動MSA。
5. 向MSA登錄vCenter伺服器。若要執行安裝、請完成下列詳細步驟：
6. 部署了Jetstream DR MSA並註冊vCenter Server之後、請使用vSphere Web Client存取Jetstream DR外掛程式。您可以瀏覽至「資料中心」>「設定」>「Jetstream DR」來完成此作業。



7. 在Jetstream DR介面中、選取適當的叢集。



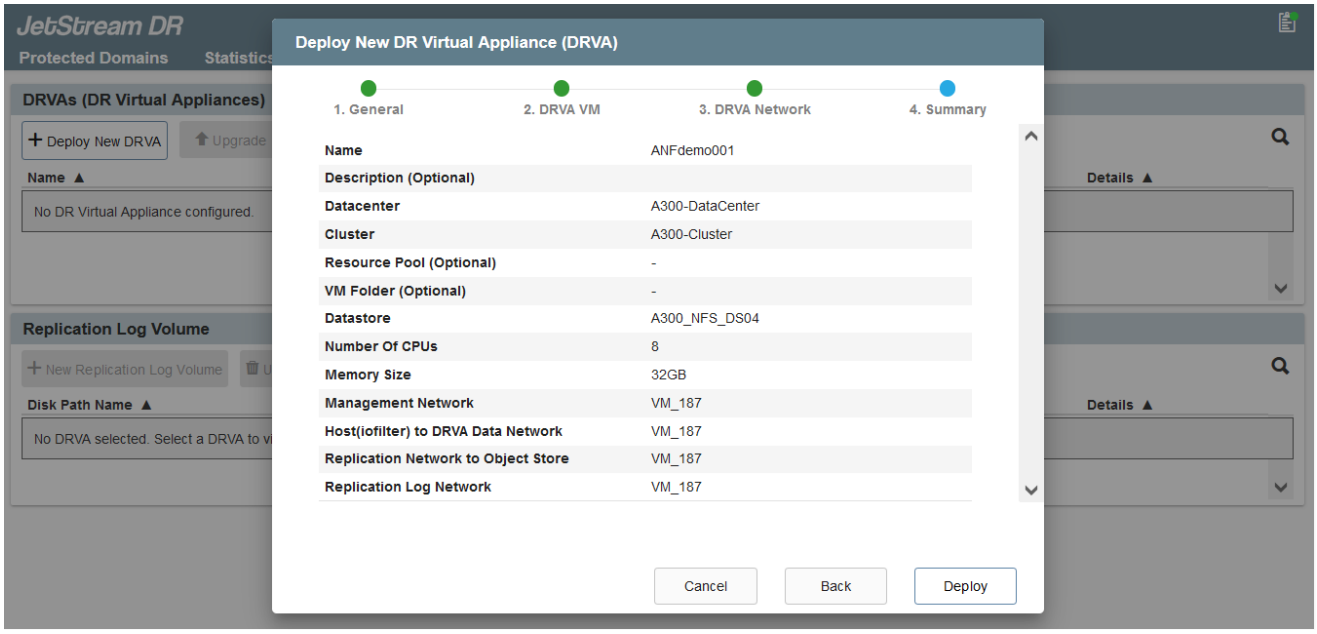
8. 使用I/O篩選套件設定叢集。



9. 新增位於恢復站台的Azure Blob儲存設備。
10. 從「應用裝置」索引標籤部署DR虛擬應用裝置（DRVA）。

> DRVA可由CPt自動建立、但對於POC試用、我們建議手動設定及執行DR週期（「start protection」（開始保護）>「Failover」（容錯移轉）>「Failover」（容錯回復））。

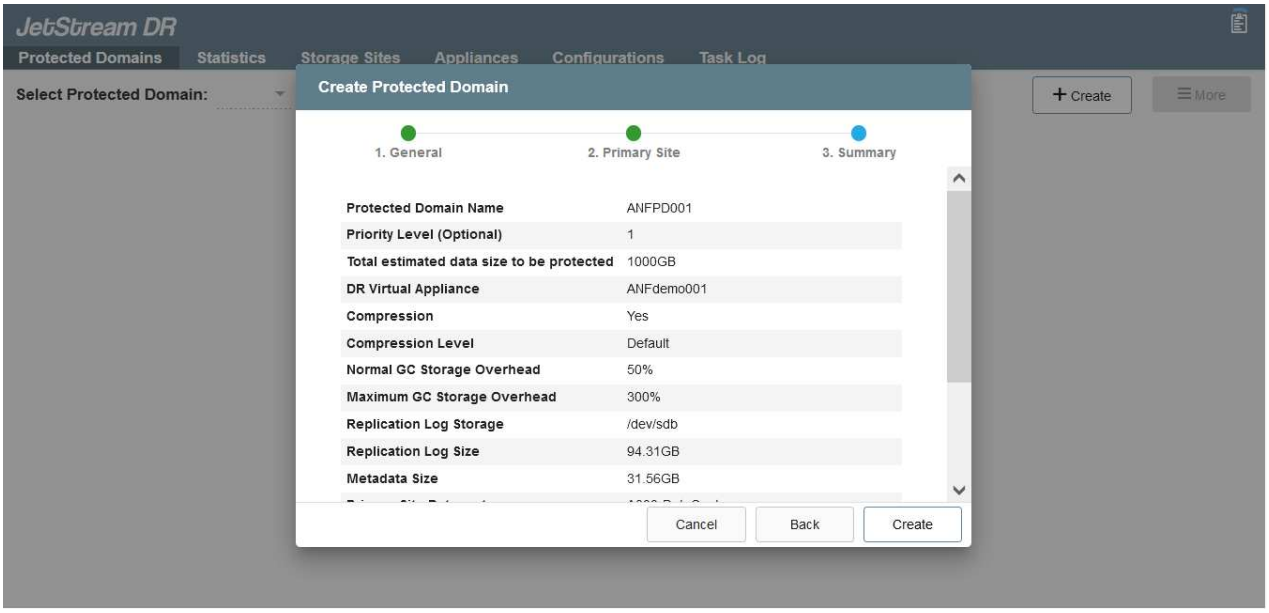
Jetstream DRVA是一種虛擬應用裝置、有助於在資料複寫程序中發揮關鍵功能。受保護的叢集必須至少包含一個DRVA、而且每個主機通常會設定一個DRVA。每個DRVA都能管理多個受保護的網域。



在此範例中、我們為80部虛擬機器建立了四部DRVA。

1. 使用VMDK從可用的資料存放區或獨立的共享iSCSI儲存集區、為每個DRVA建立複寫記錄磁碟區。
2. 從「受保護的網域」索引標籤、使用Azure Blob儲存站台、DRVA執行個體和複寫記錄的相關資訊、建立所需數量的受保護網域。受保護的網域會定義叢集中的特定VM或VM組、這些VM會一起受到保護、

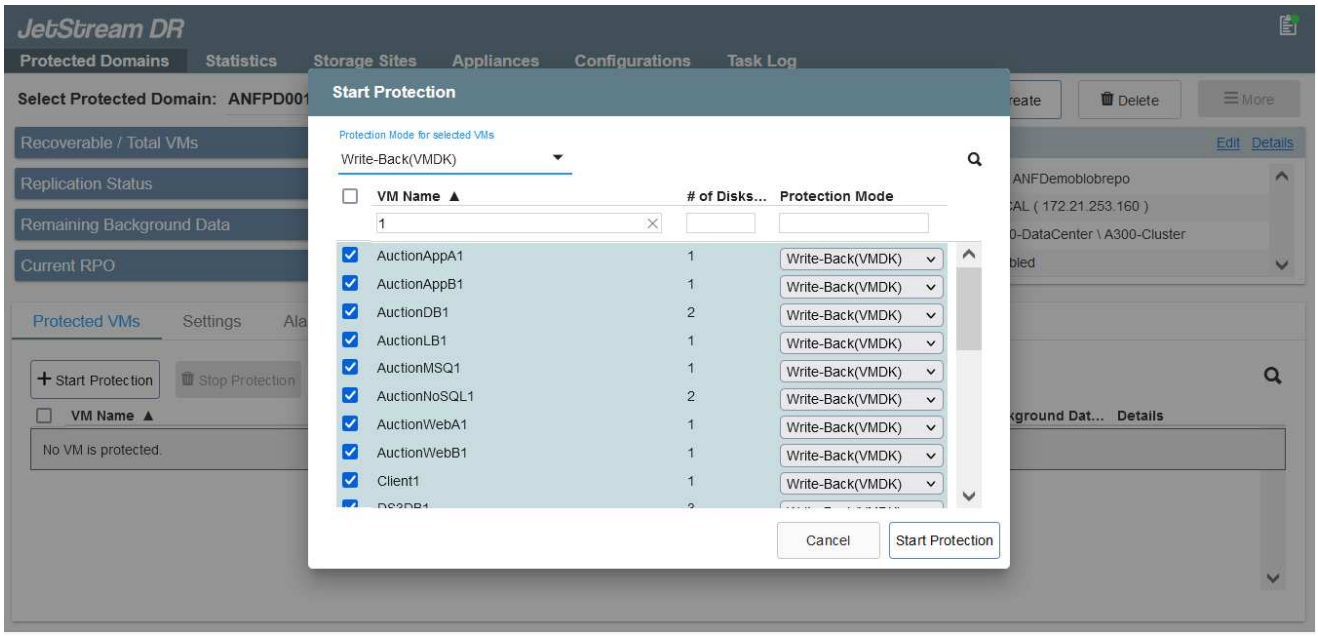
並指派容錯移轉/容錯回復作業的優先順序。



3. 選取您要保護的VM、並啟動受保護網域的VM保護。這會開始將資料複寫到指定的Blob Store。

ⓘ 確認受保護網域中的所有VM都使用相同的保護模式。

ⓘ 回寫（VMDK）模式可提供更高的效能。



驗證複寫記錄磁碟區是否放置在高效能儲存設備上。

ⓘ 容錯移轉執行手冊可設定為群組VM（稱為「恢復群組」）、設定開機順序、以及修改CPU / 記憶體設定和IP組態。

使用Run命令、在Azure VMware解決方案私有雲中安裝AVS的Jetstream DR

恢復站台（AVS）的最佳實務做法是事先建立三節點的指示燈式叢集。如此可預先設定恢復站台基礎架構、包括下列項目：

- 目的地網路區段、防火牆、DHCP和DNS等服務。
- 安裝AVS的Jetstream DR
- 將ANF磁碟區組態為資料存放區、而moreJetStream DR則支援接近零的RTO模式、適用於關鍵任務網域。對於這些網域、應該預先安裝目的地儲存設備。在此情況下、建議使用ANF儲存類型。

> 應在AVS叢集上設定網路組態（包括區段建立）、以符合內部部署需求。

視SLA和RTO需求而定、您可以使用持續容錯移轉或一般（標準）容錯移轉模式。對於接近零的RTO、應在恢復站台開始持續重新補充。

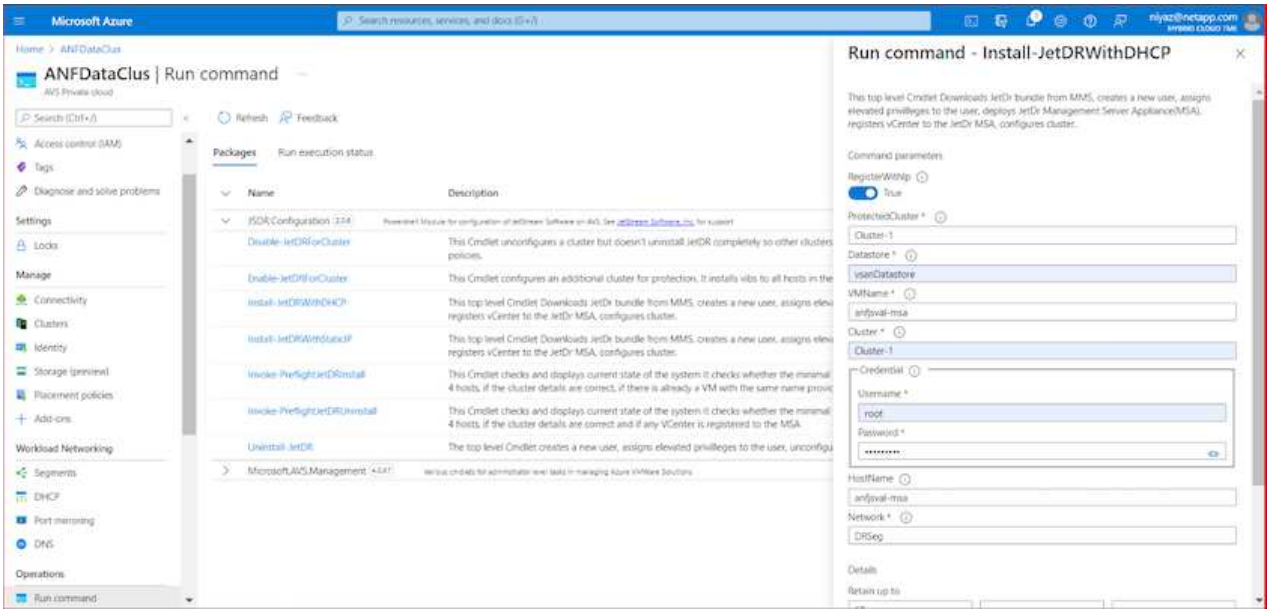
如何在私有雲中安裝**AVS**的**Jetstream DR**

若要在Azure VMware解決方案私有雲上安裝適用於AVS的Jetstream DR、請完成下列步驟：

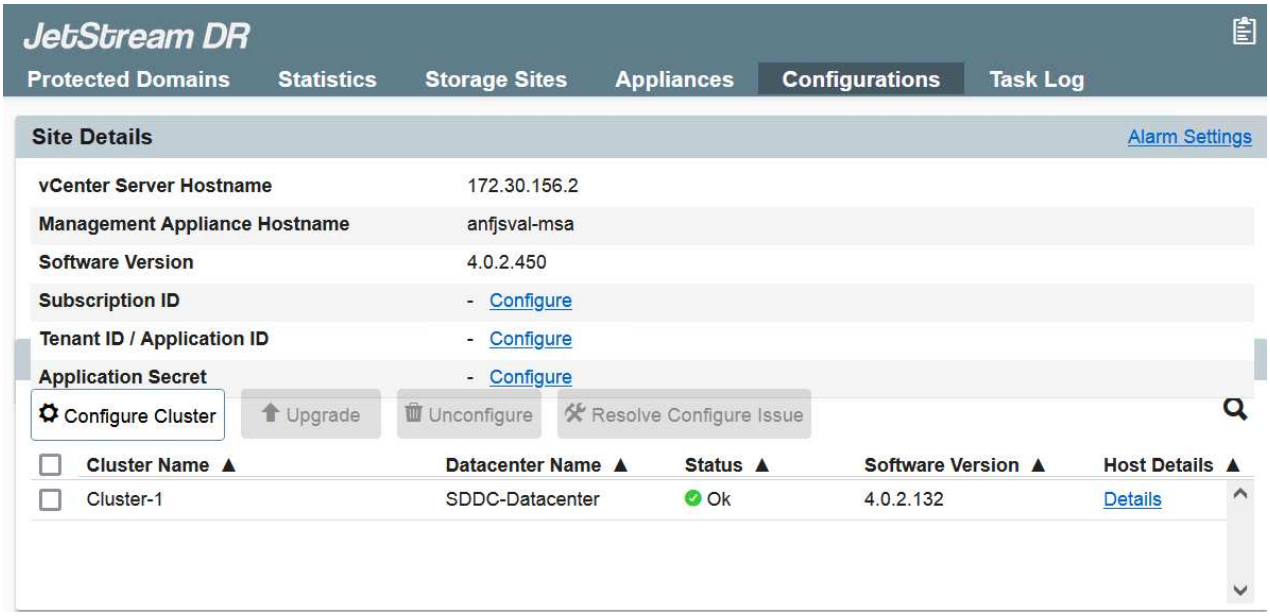
1. 從Azure入口網站移至Azure VMware解決方案、選取私有雲、然後選取執行命令>套件> JSDR.Configuration。

> Azure VMware解決方案中的預設CloudAdmin使用者沒有足夠權限可安裝AVS的Jetstream DR。Azure VMware解決方案可針對Jetstream DR叫用Azure VMware Solution Run命令、以簡化及自動化方式安裝Jetstream DR。

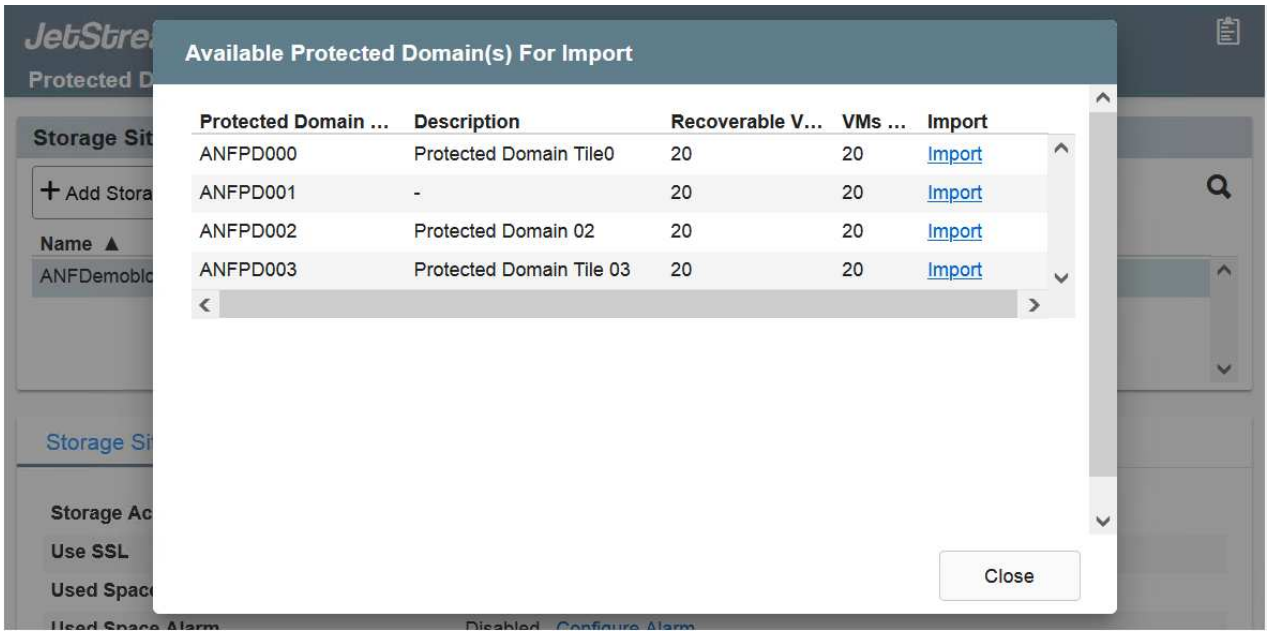
下列螢幕快照顯示使用DHCP型IP位址進行安裝。



2. 在安裝AVS的Jetstream DR完成後、請重新整理瀏覽器。若要存取Jetstream DR UI、請前往SDDC資料中心>組態> Jetstream DR。



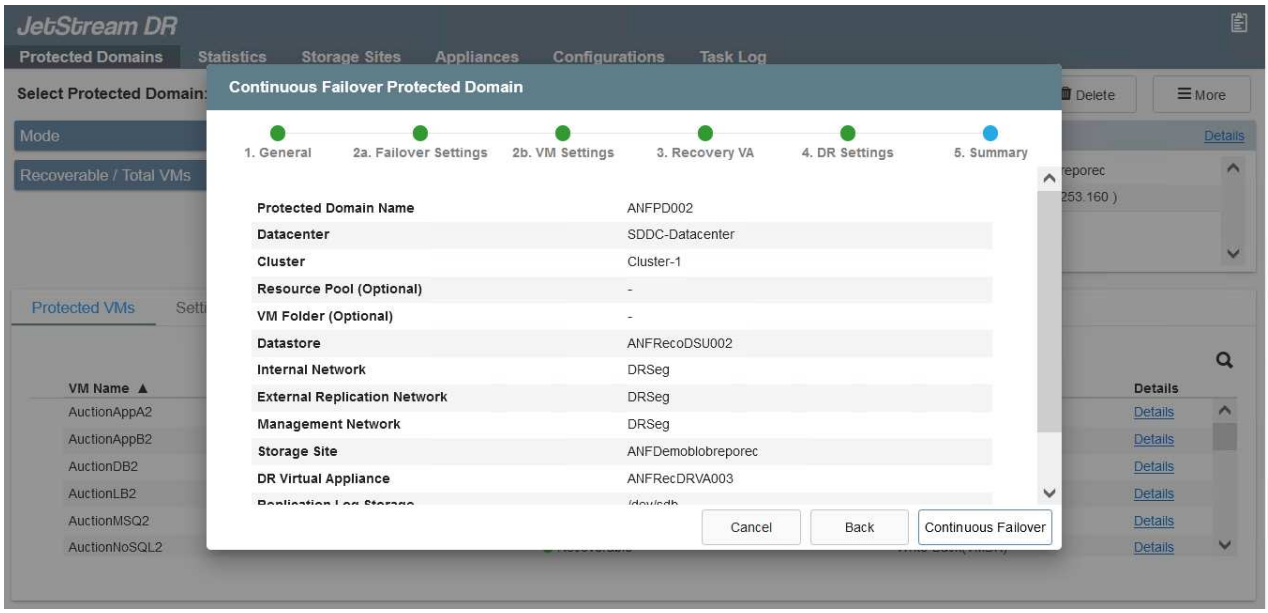
3. 從Jetstream DR介面新增Azure Blob Storage帳戶、以保護內部部署叢集做為儲存站台、然後執行「掃描網域」選項。



4. 匯入受保護的網域之後、請部署DRVA設備。在此範例中、會使用Jetstream DR UI從恢復站台手動啟動持續重新補充。

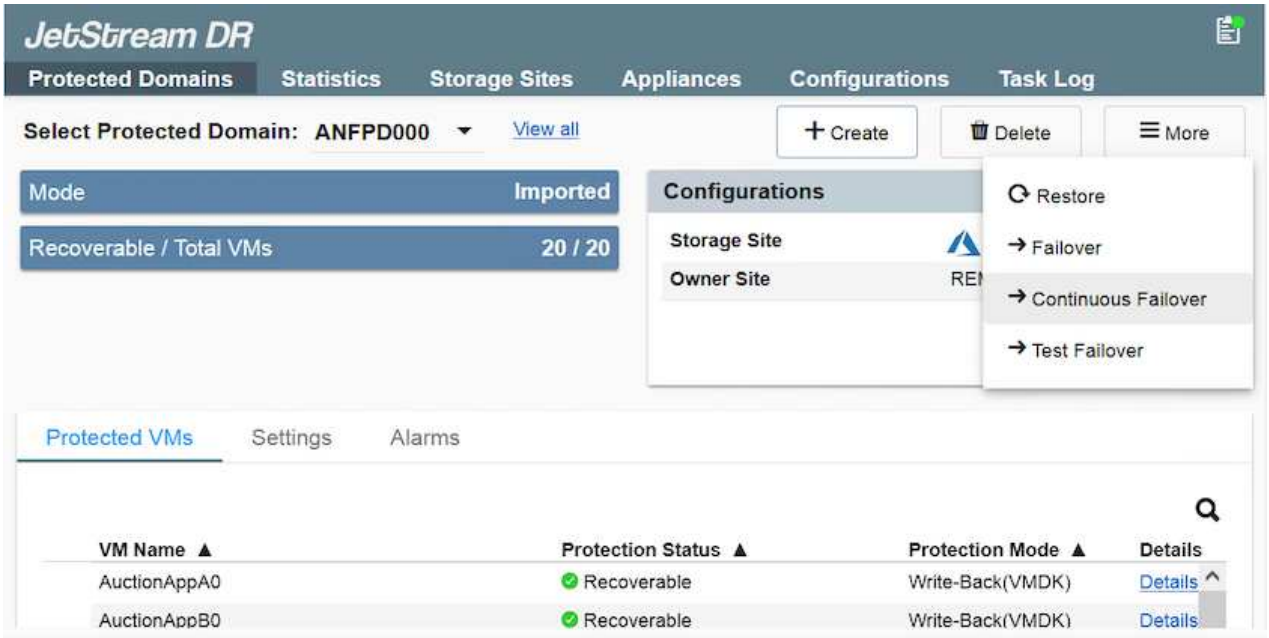
> 您也可以使用已建立的CPT計畫來自動化這些步驟。

5. 使用可用的vSAN或ANF資料存放區建立複寫記錄磁碟區。
6. 匯入受保護的網域、並將恢復VA設定為使用ANF資料存放區來放置VM。



> 請確定選取的區段已啟用DHCP、而且有足夠的IP可用。在網域還原期間、會暫時使用動態IP。每個恢復中的VM（包括持續重新補充）都需要個別的動態IP。恢復完成後、IP便會釋出、並可重複使用。

7. 選取適當的容錯移轉選項（持續容錯移轉或容錯移轉）。在此範例中、會選取持續還原（持續容錯移轉）。



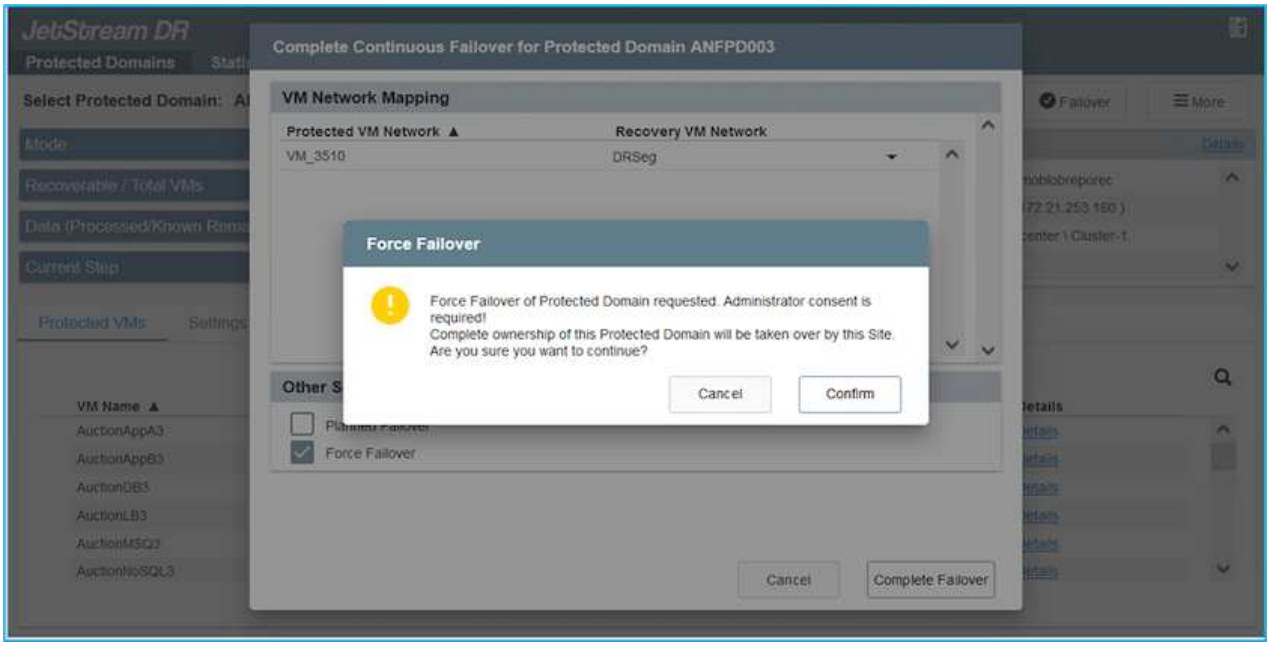
執行容錯移轉/容錯回復

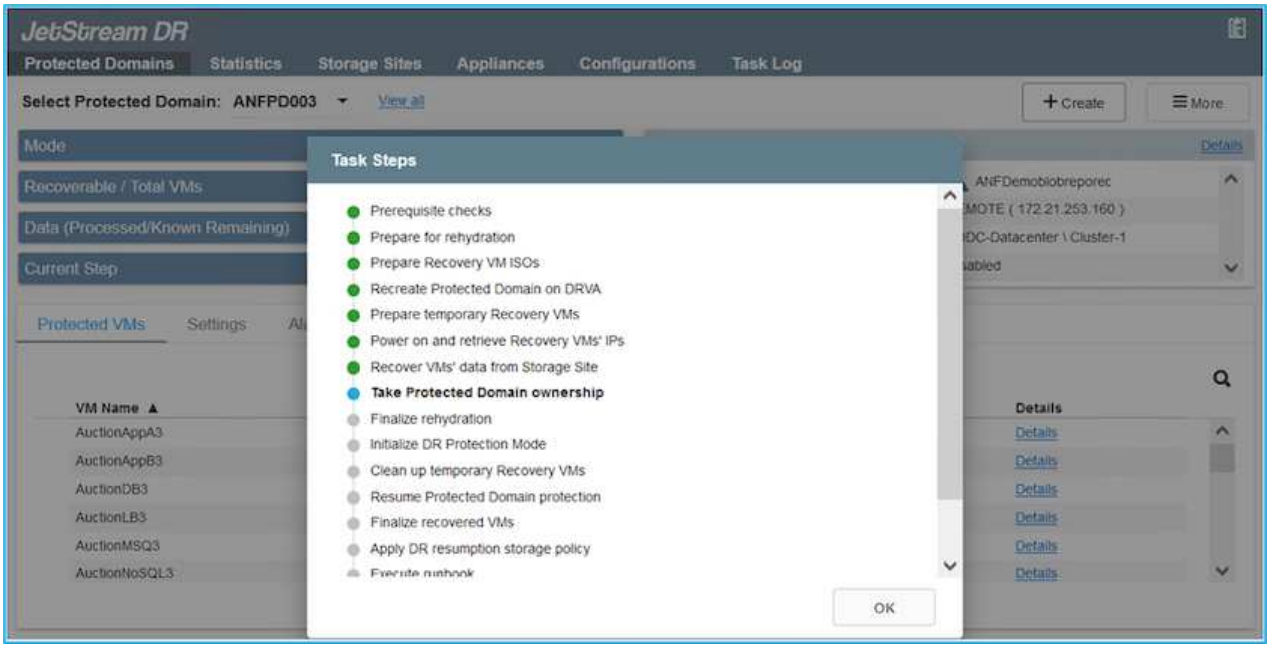
如何執行容錯移轉/容錯回復

1. 在內部部署環境的受保護叢集發生災難（部分或完整故障）之後、觸發容錯移轉。

> ⓘ 您可以使用CPt執行容錯移轉計畫、將VM從Azure Blob Storage恢復到AVS叢集還原站台。

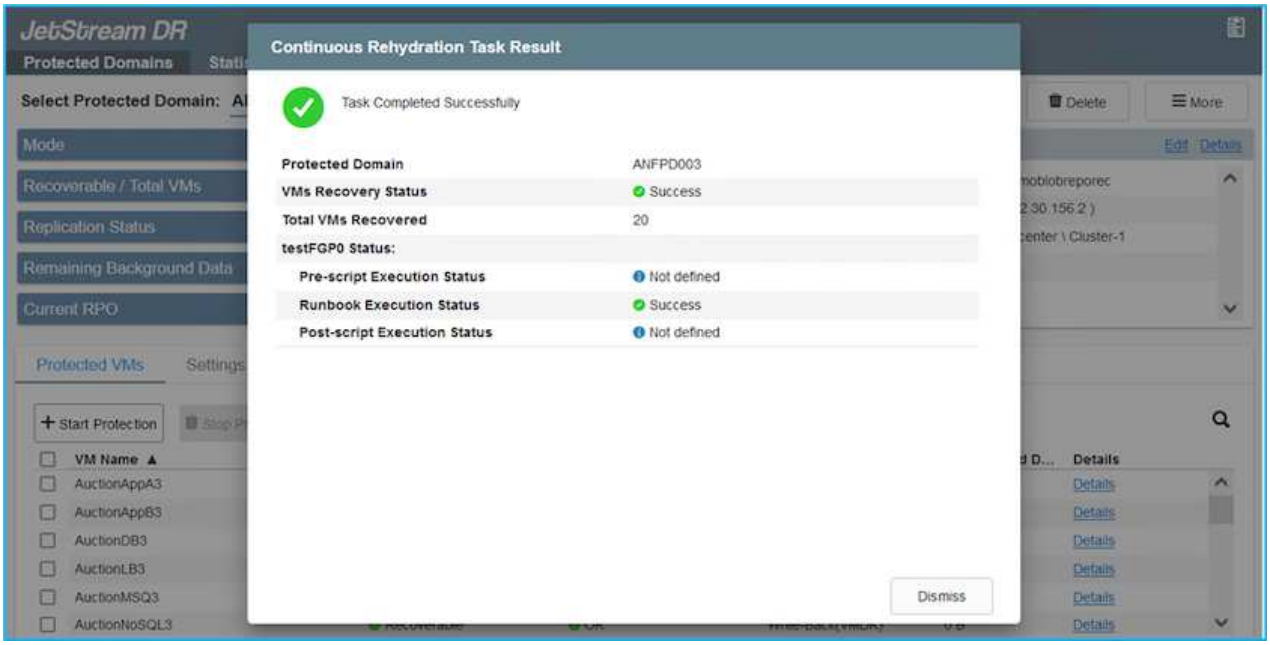
> ⓘ 在AVS中啟動受保護的VM後、容錯移轉（持續或標準還原）會自動恢復保護、而在Azure Blob Storage中、則會繼續將資料複寫到適當/原始的容器中。





工作列會顯示容錯移轉活動的進度。

2. 當工作完成時、存取恢復的VM並維持正常營運。

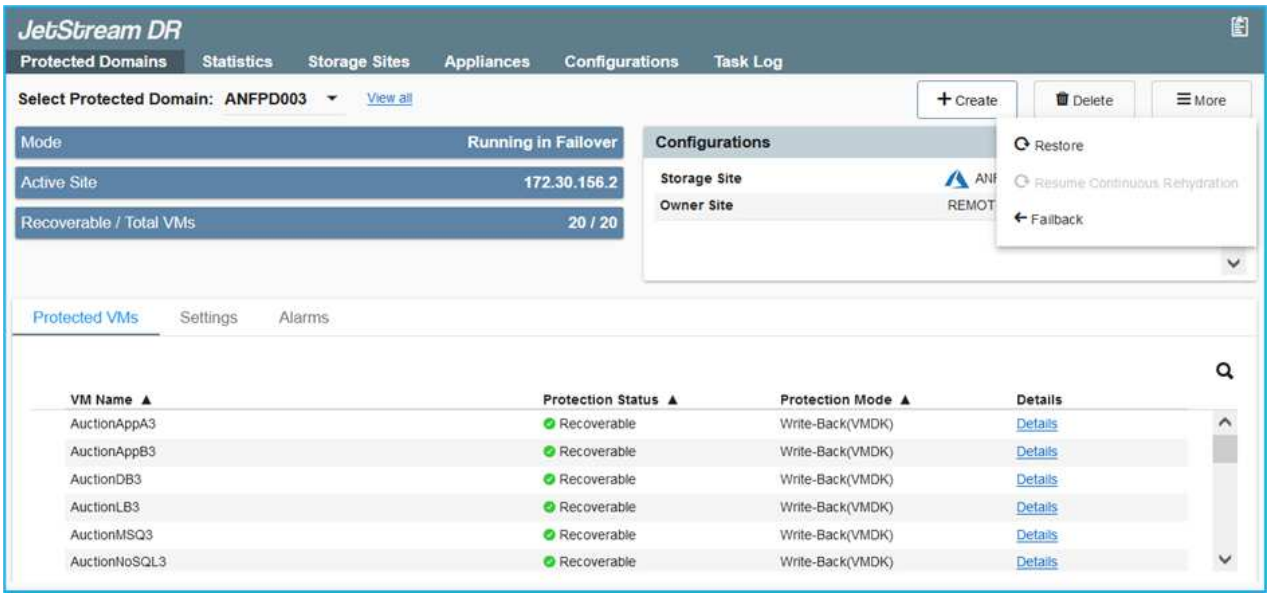


在主站台啟動並再次執行之後、即可執行容錯回復。恢復VM保護、並檢查資料一致性。

3. 還原內部部署環境。視災難事件類型而定、可能需要還原及/或驗證受保護叢集的組態。如有必要、可能需要重新安裝Jetstream DR軟體。

> 附註：Automation Toolkit提供的「恢復公用程式準備回復」指令碼、可用來協助清除任何過時VM、網域資訊等的原始受保護網站。

4. 存取還原的內部部署環境、前往Jetstream DR UI、然後選取適當的受保護網域。受保護的站台準備好進行容錯回復之後、請在UI中選取「容錯回復」選項。



> 此外、也可使用由CPT產生的容錯回復計畫、將VM及其資料從物件存放區傳回原始的VMware環境。

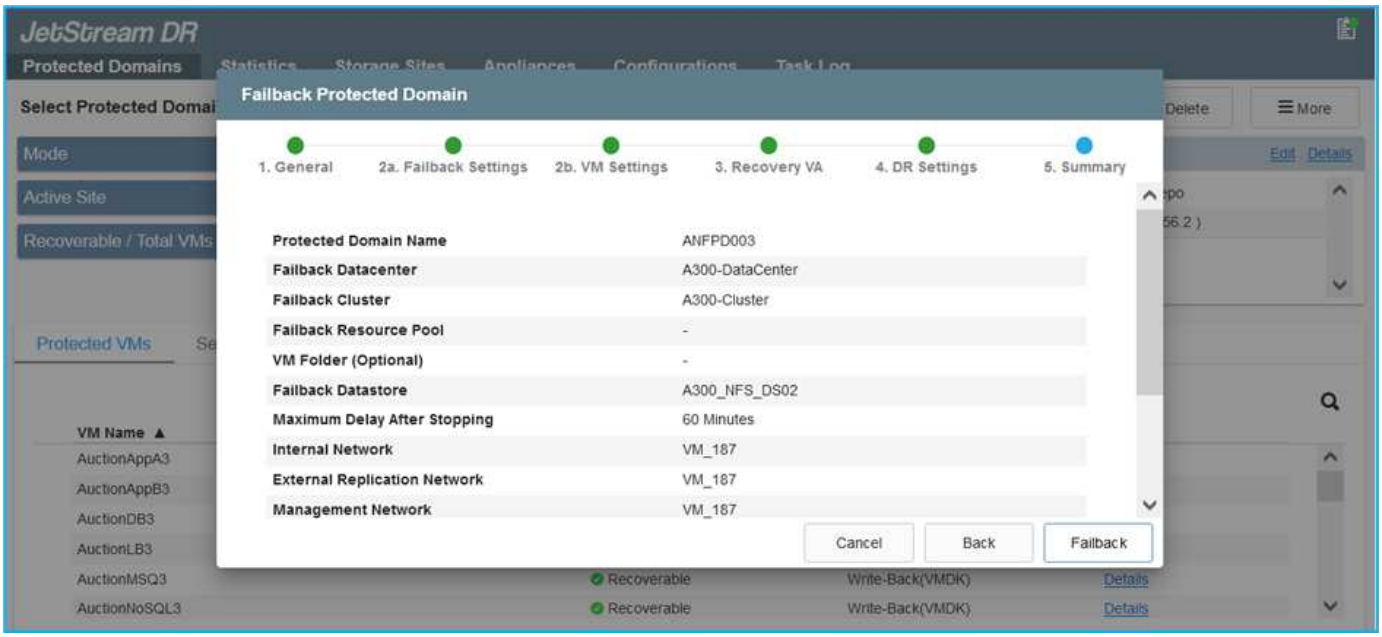
> 指定在恢復站台暫停VM並在受保護站台重新啟動之後的最大延遲。這次包括在停止容錯移轉虛擬機器之後完成複寫、清理恢復站台的時間、以及在受保護站台重新建立虛擬機器的時間。NetApp建議的值為10分鐘。

完成容錯回復程序、然後確認恢復VM保護和資料一致性。

Ransomware恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體而言、IT組織很難判斷安全的回報點、一旦確定、如何確保恢復的工作負載受到保護、避免再度發生攻擊（從休眠的惡意軟體或透過易受影響的應用程式）。

針對AVS的Jetstream DR搭配Azure NetApp Files 支援功能資料存放區、可讓組織從可用時間點恢復、以便在需要時將工作負載恢復至功能性隔離的網路、藉此解決這些問題。恢復功能可讓應用程式彼此運作和通訊、但不會讓它們暴露在北南流量中、因此安全團隊可以安全地執行鑑識和其他必要的補救措施。



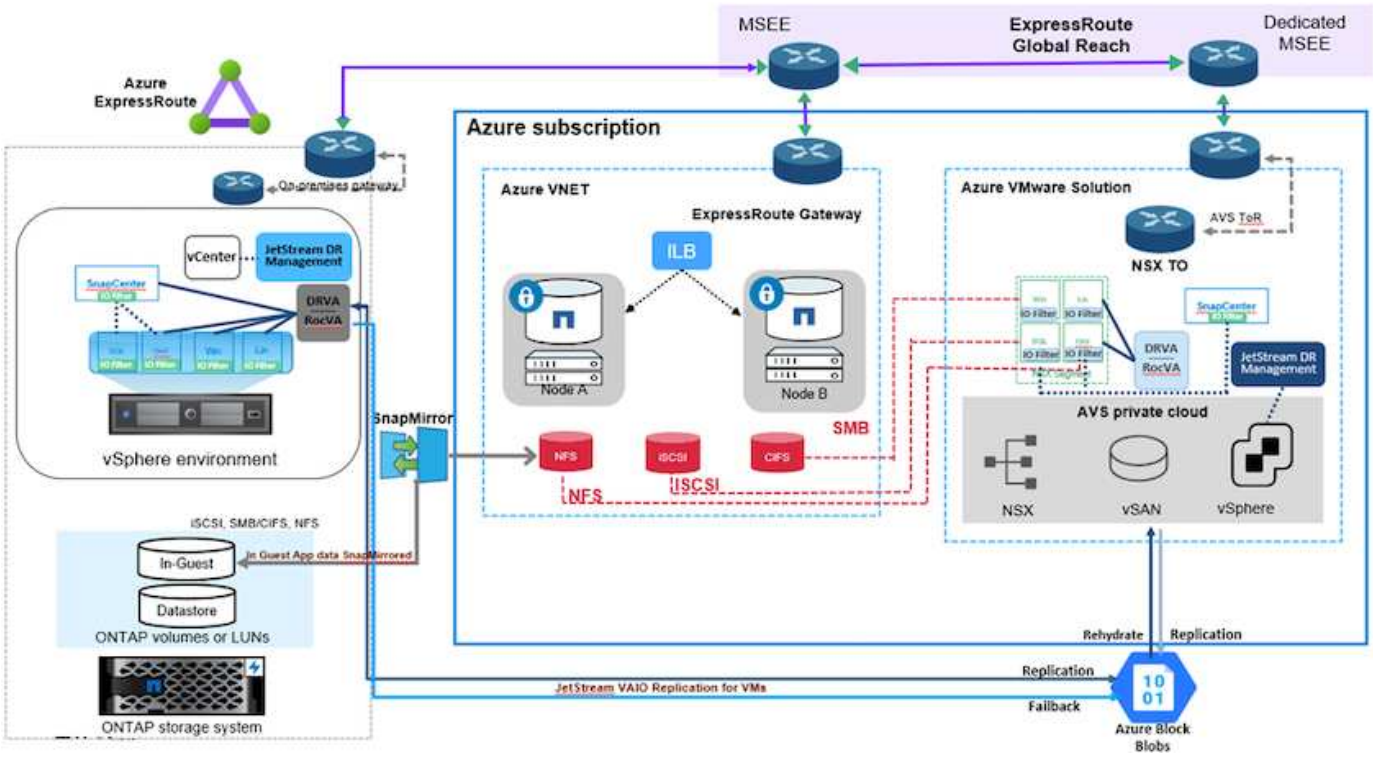
使用CVO和AVS（與來賓連線的儲存設備）進行災難恢復

總覽

作者：Ravi BCB和Niyazz Mohamed, NetApp

災難恢復至雲端是一種彈性且具成本效益的方法、可保護工作負載、避免站台中斷運作、以及勒索軟體等資料毀損事件。有了NetApp SnapMirror、使用來賓連線儲存設備的內部部署VMware工作負載可複寫至Cloud Volumes ONTAP Azure上執行的NetApp VMware。這涵蓋應用程式資料、但實際VM本身的情況如何。災難恢復應涵蓋所有相依元件、包括虛擬機器、VMDK、應用程式資料等。為達成此目標、SnapMirror與Jetstream一起可用來無縫恢復從內部部署複寫至Cloud Volumes ONTAP VMware的工作負載、同時使用vSAN儲存設備來執行VM VMDK。

本文件提供逐步的方法來設定及執行使用NetApp SnapMirror、Jetstream及Azure VMware解決方案（AVS）的災難恢復。



假設

本文件著重於客體內儲存應用程式資料（也稱為來賓連線）、我們假設內部環境使用SnapCenter 的是應用程式一致的備份。

> 本文件適用於任何第三方備份或還原解決方案。視環境中使用的解決方案而定、請遵循最佳實務做法來建立符合組織SLA的備份原則。

若要在內部部署環境與Azure虛擬網路之間建立連線、請使用Express Route Global Reach或虛擬WAN搭配VPN閘道。應根據內部部署的VLAN設計來建立區段。

> 將內部部署資料中心連線至Azure的選項有多種、因此我們無法在此文件中概述特定的工作流程。如需適當的內部部署至Azure連線方法、請參閱Azure文件。

部署災難恢復解決方案

解決方案部署總覽

1. 確保應用程式資料是以SnapCenter 不必要的RPO要求使用支援功能進行備份。
2. 在Cloud Volumes ONTAP 適當的訂購和虛擬網路中使用Cloud Manager、以正確的執行個體大小進行配置。
   a. 為相關的應用程式磁碟區設定SnapMirror。
   b. 更新SnapCenter 中的備份原則、以便在排程工作之後觸發SnapMirror更新。
3. 在內部部署資料中心安裝Jetstream DR軟體、並開始保護虛擬機器。

4. 在Azure VMware解決方案私有雲中安裝Jetstream DR軟體。
5. 在災難事件期間、請使用Cloud Manager中斷SnapMirror關係、並觸發將虛擬機器容錯移轉至Azure NetApp Files 指定AVS DR站台中的VMware資料存放區或vSAN資料存放區。
    a. 重新連接應用程式VM的iSCSI LUN和NFS掛載。
6. 在主站台恢復後、透過反向重新同步SnapMirror來叫用容錯回復至受保護站台。

部署詳細資料

在**Azure**上設定**CVO**、並將磁碟區複寫至**CVO**

第一步是在Cloud Volumes ONTAP Azure上設定功能 ("連結"）並以Cloud Volumes ONTAP 所需的頻率和快照保留量、將所需的Volume複製到不間斷的地方。

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB
	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB
	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB

設定**AVS**主機和**CVO**資料存取

部署SDDC時、需要考量的兩個重要因素是Azure VMware解決方案中SDDC叢集的大小、以及SDDC持續服務的時間。這兩項災難恢復解決方案的關鍵考量、有助於降低整體營運成本。SDDC可只有三部主機、在全規模部署中、一直到多主機叢集為止。

部署AVS叢集的決定主要取決於RPO / RTO需求。有了Azure VMware解決方案、SDDC就能準時配置、以準備測試或實際的災難事件。即時部署的SDDC可在不處理災難時節省ESXi主機成本。不過、這種部署方式會在部署SDDC時、影響RTO數小時。

最常見的部署選項是讓SDDC以一律開啟的操作前導指示燈模式執行。此選項可提供三部隨時可用的主機的小型佔用空間、並提供執行中的基準來執行模擬活動和法規遵循檢查、藉此加速恢復作業、避免在正式作業站台和災難恢復站台之間發生作業移位的風險。當需要處理實際的DR事件時、可以將指示燈叢集快速擴充至所需的層級。

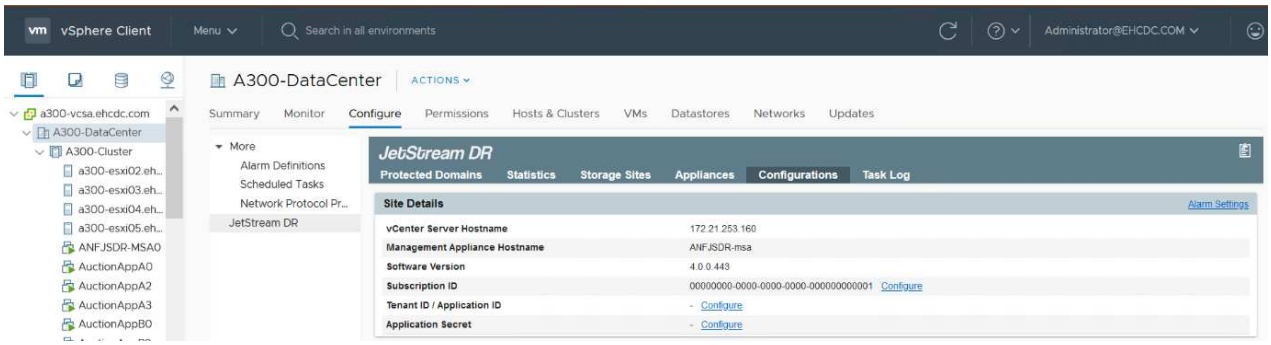
若要設定AVS SDDC（無論是隨需或是以指示燈模式）、請參閱 "在Azure上部署及設定虛擬化環境"。先決條件是確認位於AVS主機上的客體VM能夠在Cloud Volumes ONTAP 建立連線之後、從支援中心使用資料。

正確設定好VMware及AVS之後Cloud Volumes ONTAP 、請開始設定Jetstream、使用VAIO機制、並利用SnapMirror將應用程式磁碟區複本複製到Cloud Volumes ONTAP 物件上、將內部部署工作負載自動還原至AVS（使用應用程式VMDK的VM及使用客體內建儲存設備的VM）。

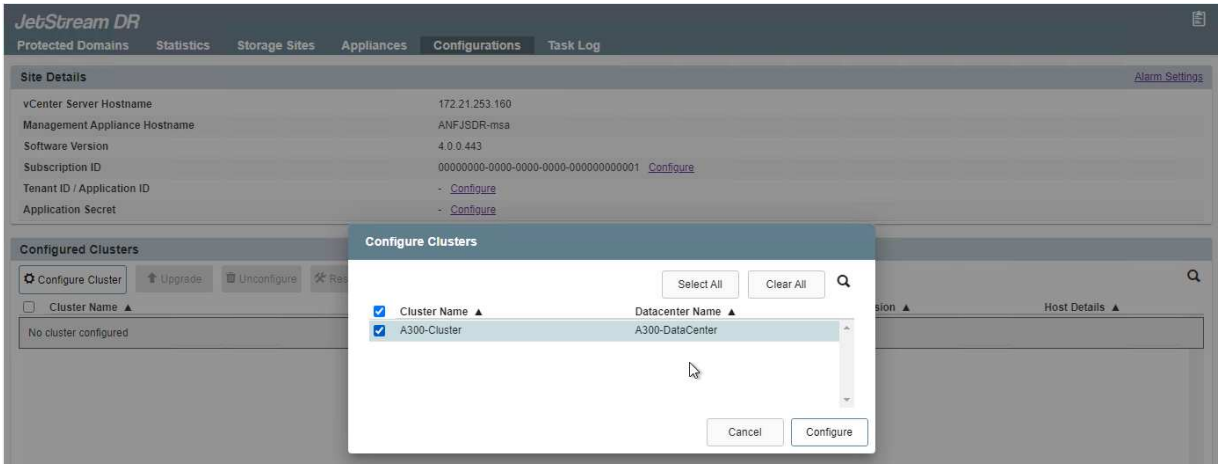
在內部部署資料中心安裝**Jetstream DR**

Jetstream DR軟體包含三個主要元件：Jetstream DR管理伺服器虛擬設備（MSA）、DR虛擬設備（DRVA）和主機元件（I/O篩選套件）。MSA用於在運算叢集上安裝及設定主機元件、然後管理Jetstream DR軟體。安裝程序如下：

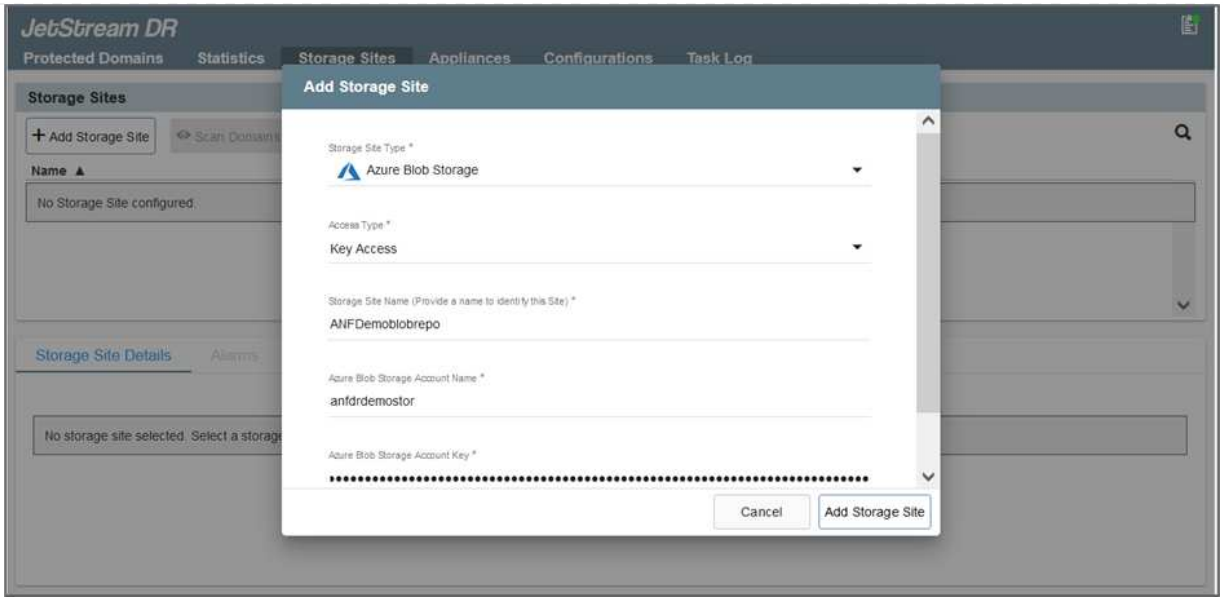
1. 檢查先決條件。
2. 執行容量規劃工具以取得資源和組態建議。
3. 將Jetstream DR MSA部署至指定叢集中的每個vSphere主機。
4. 在瀏覽器中使用其DNS名稱啟動MSA。
5. 向MSA登錄vCenter伺服器。
6. 部署了Jetstream DR MSA並註冊vCenter Server之後、請使用vSphere Web Client瀏覽至Jetstream DR外掛程式。您可以瀏覽至「資料中心」>「設定」>「Jetstream DR」來完成此作業。



7. 在Jetstream DR介面中、完成下列工作：
   a. 使用I/O篩選套件設定叢集。

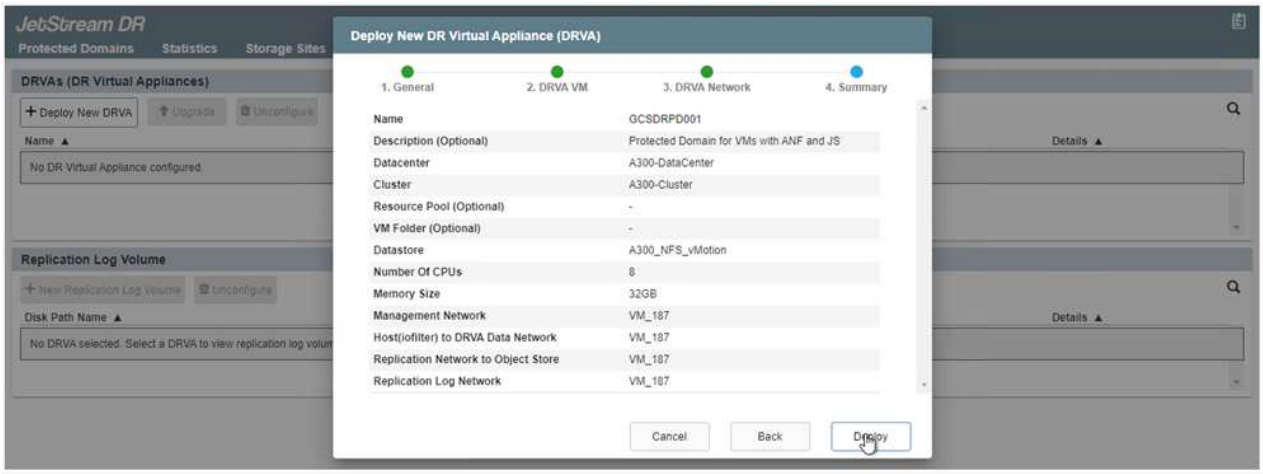


   b. 新增位於恢復站台的Azure Blob儲存設備。

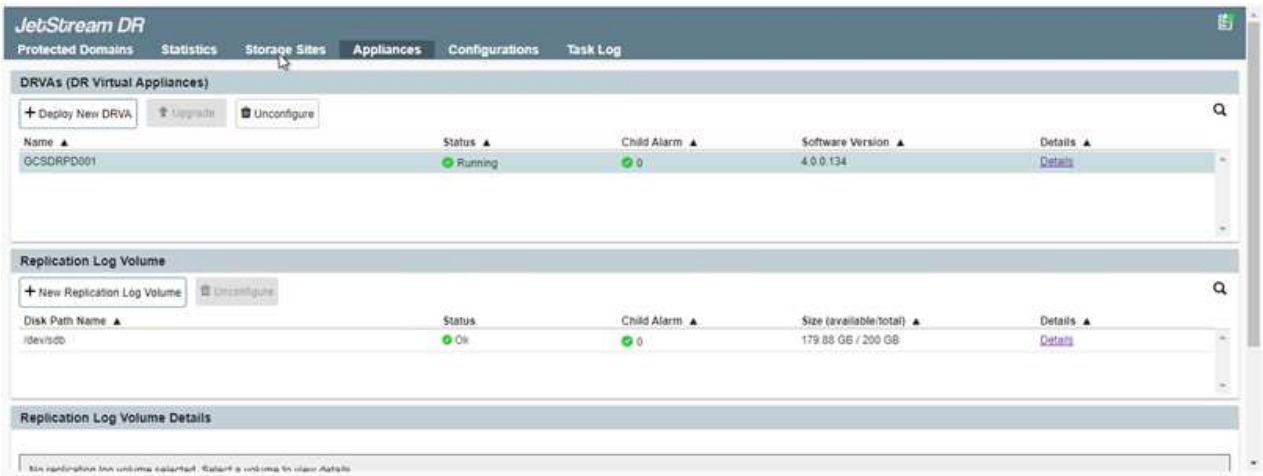


8. 從「應用裝置」索引標籤部署所需數量的DR虛擬應用裝置（DRVA）。

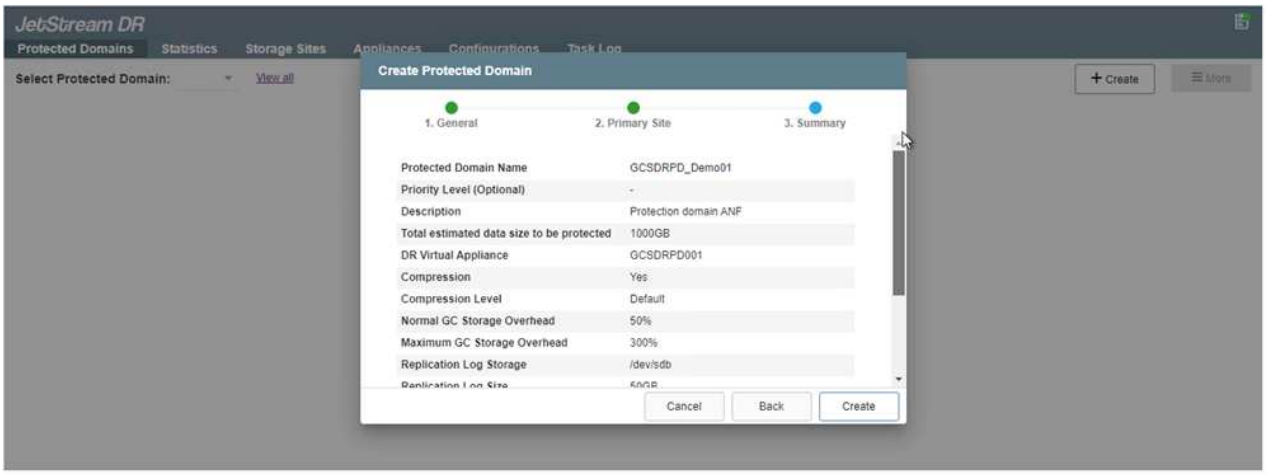
> ⓘ 使用容量規劃工具來預估所需的DRVA數量。

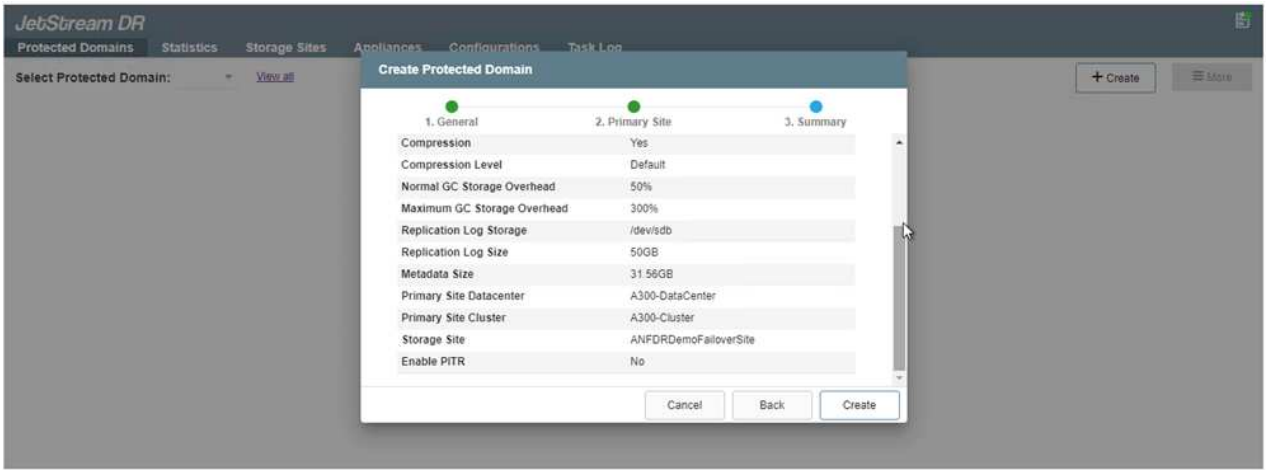


9. 使用可用的資料存放區或獨立的共享iSCSI儲存池中的VMDK、為每個DRVA建立複寫記錄磁碟區。



10. 從「受保護的網域」索引標籤、使用Azure Blob儲存站台、DRVA執行個體和複寫記錄的相關資訊、建立所需數量的受保護網域。受保護的網域會定義叢集中的特定VM或一組應用程式VM、這些VM會一起受到保護、並指派容錯移轉/容錯回復作業的優先順序。

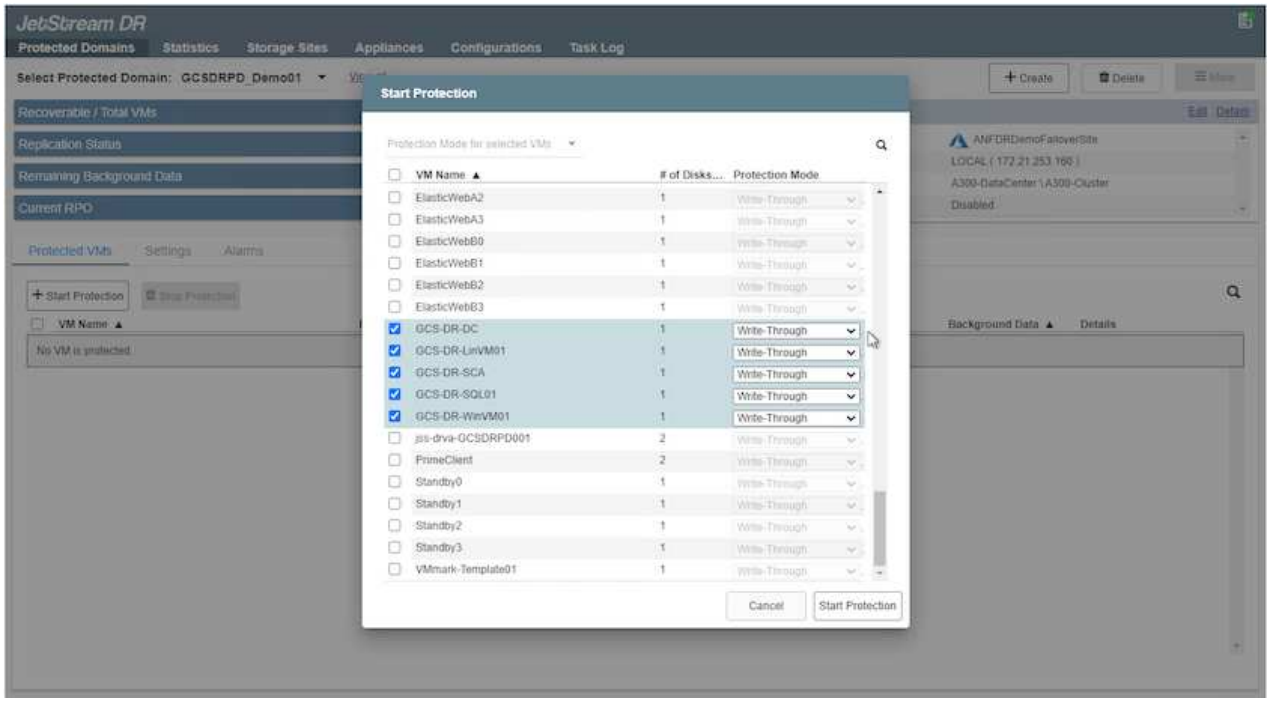




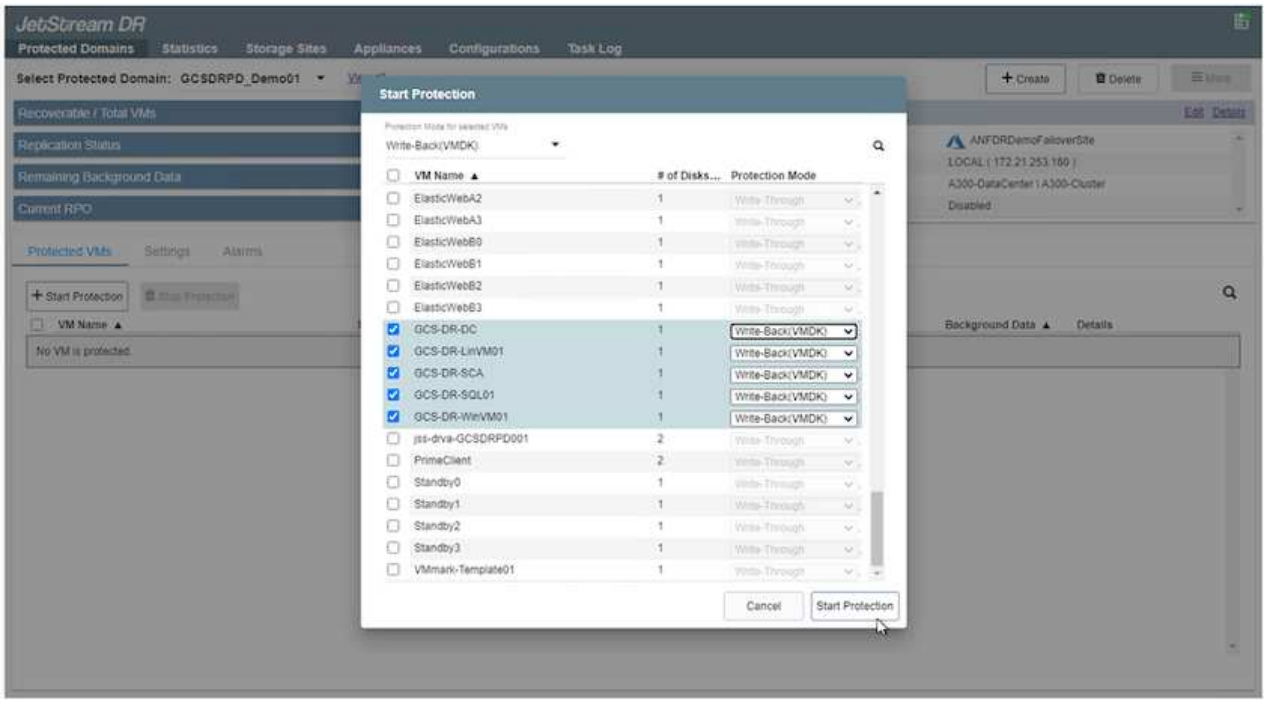
11. 選取要保護的VM、並根據相依性將VM分組為應用程式群組。應用程式定義可讓您將一組VM分組為邏輯群組、其中包含開機順序、開機延遲、以及可在恢復時執行的選用應用程式驗證。

> ⓘ 請確定保護網域中的所有VM都使用相同的保護模式。

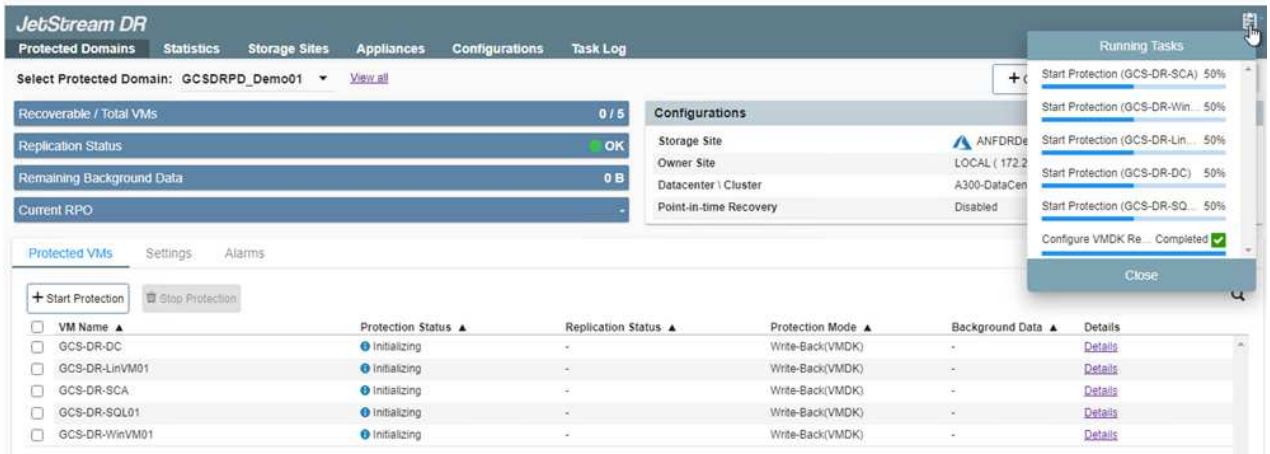
回寫（VMDK）模式可提供更高的效能。



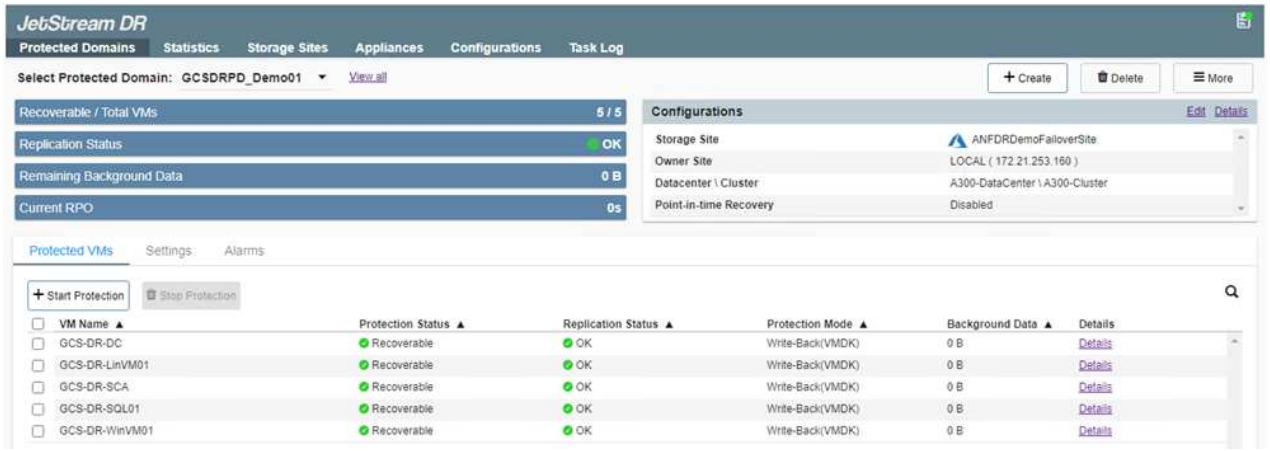
12. 請確定複寫記錄磁碟區放置在高效能儲存設備上。



13. 完成後、按一下「開始保護受保護網域」。這會開始將所選VM的資料複寫到指定的Blob存放區。



14. 複寫完成後、VM保護狀態會標示為可恢復。

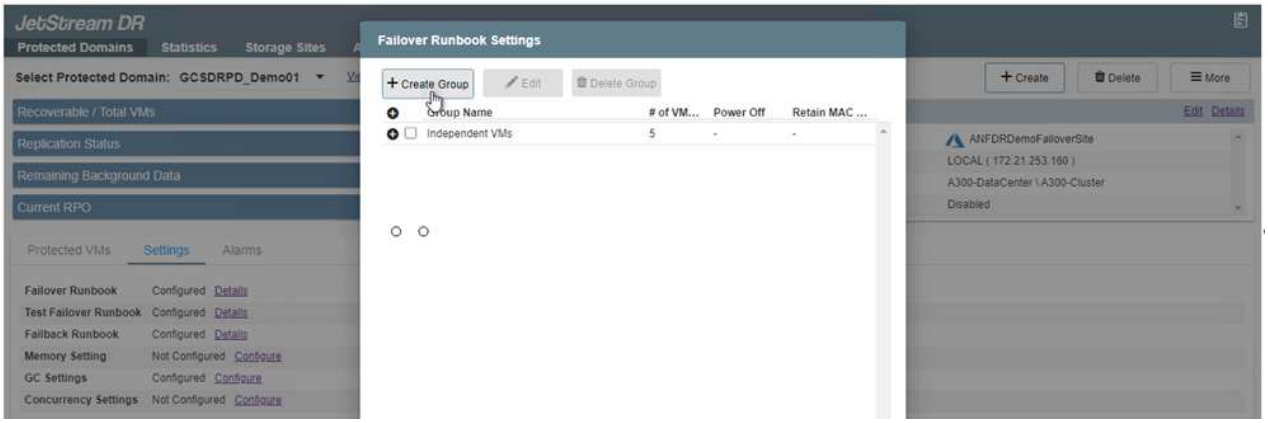


> 容錯移轉Runbook可設定為群組VM（稱為恢復群組）、設定開機順序、以及修改CPU / 記憶體設定和IP組態。

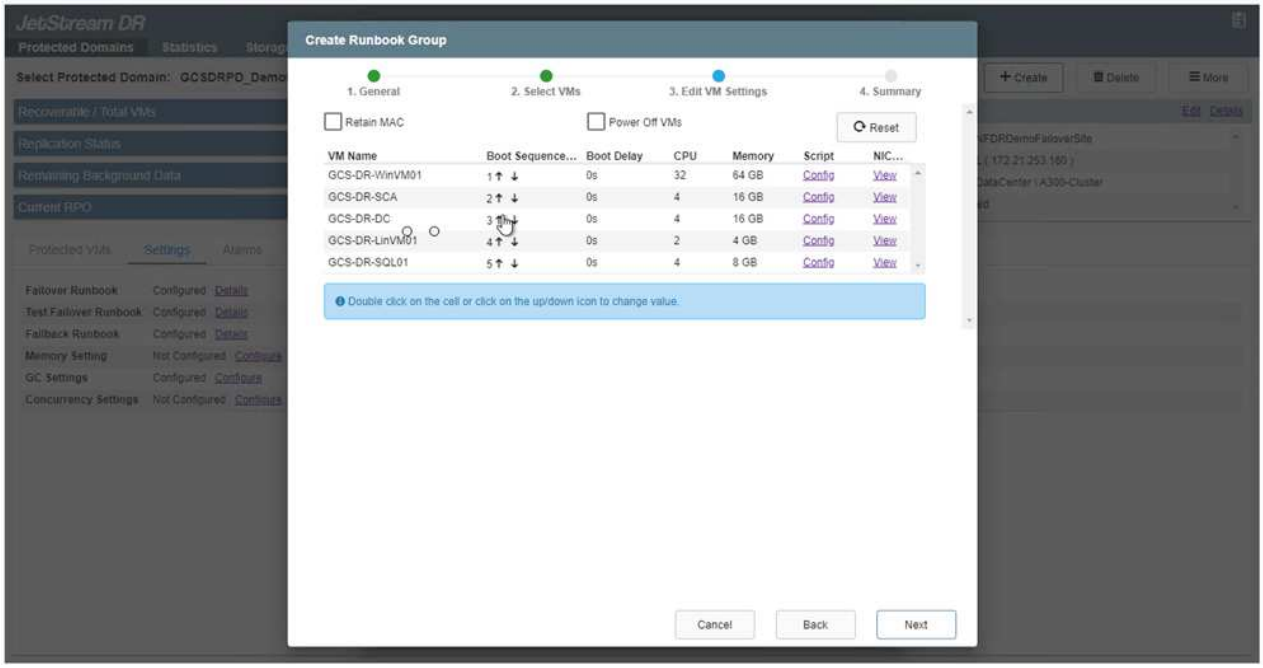
15. 按一下「設定」、然後按一下Runbook「設定」連結以設定Runbook群組。

16. 按一下「Create Group（建立群組）」按鈕、開始建立新的Runbook群組。

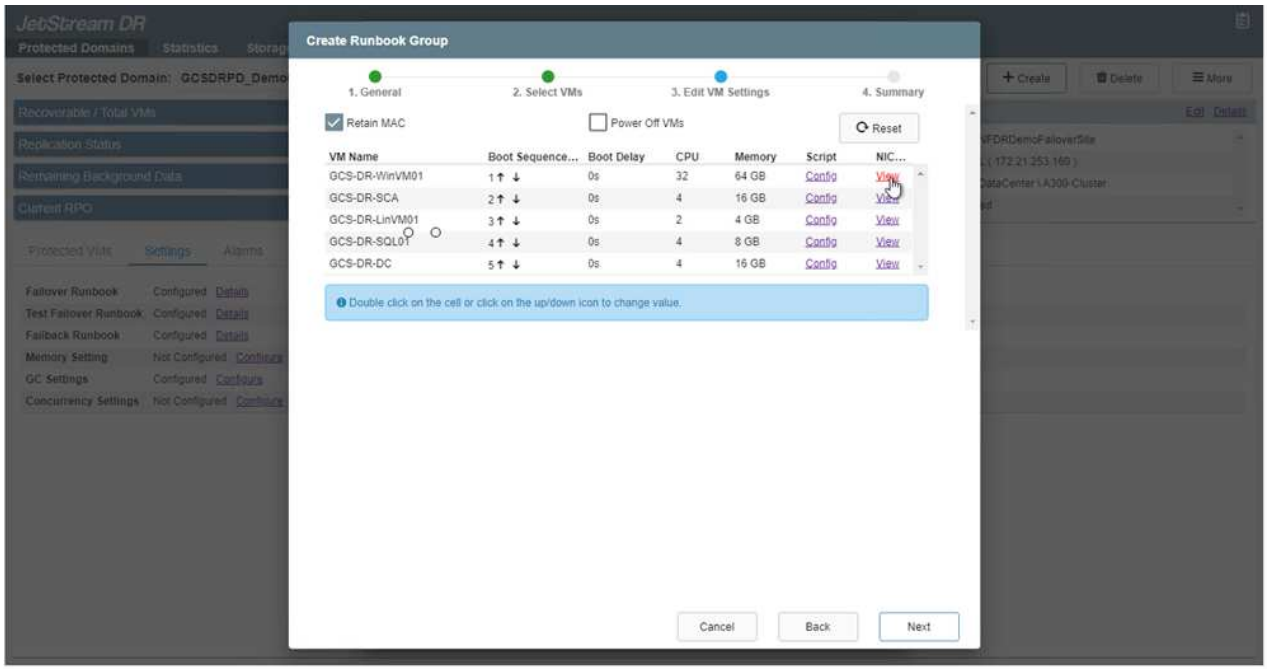
> 如有需要、請在畫面下方套用自訂的預先指令碼和後置指令碼、以便在執行手冊群組作業之前和之後自動執行。確定Runbook指令碼位於管理伺服器上。



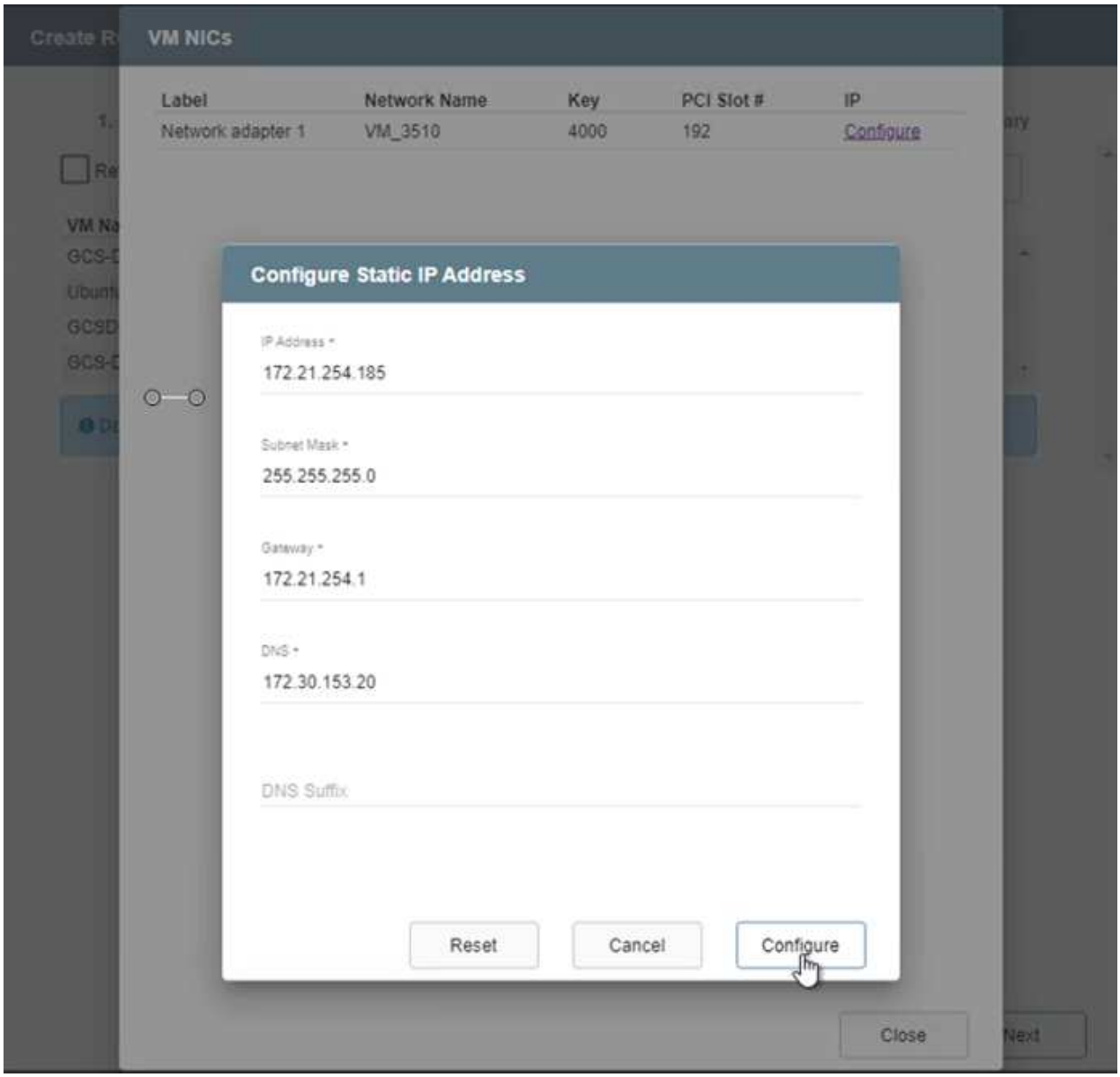
17. 視需要編輯VM設定。指定用於恢復VM的參數、包括開機順序、開機延遲（以秒為單位）、CPU數量、以及要分配的記憶體容量。按一下向上或向下箭頭、變更VM的開機順序。也提供了用於保留MAC的選項。

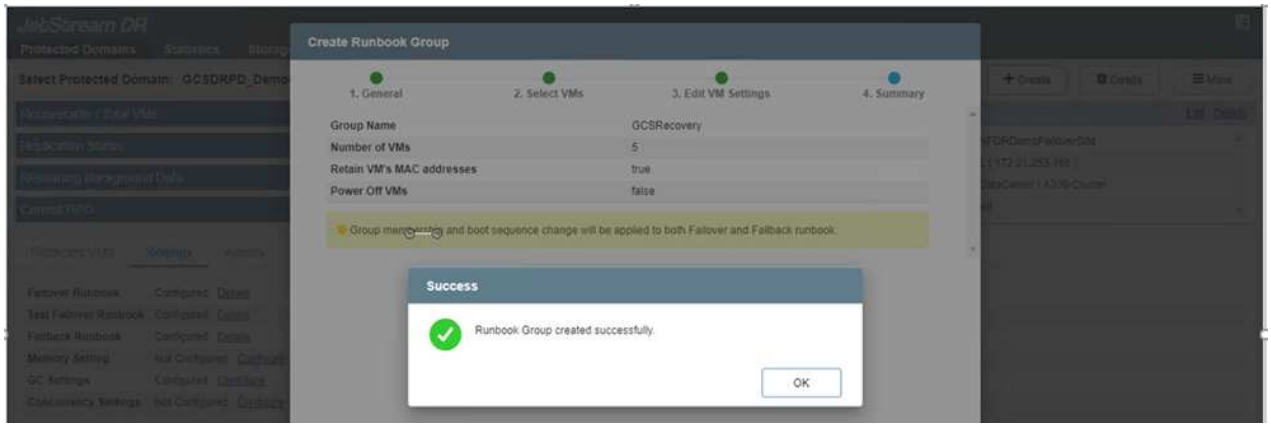


18. 靜態IP位址可針對群組中的個別VM手動設定。按一下VM的NIC View連結、手動設定其IP位址設定。



19. 按一下「Configure（設定）」按鈕以儲存個別VM的NIC設定。





容錯移轉和容錯回復執行工作簿的狀態現在會列為「已設定」。容錯移轉和容錯回復執行手冊群組是以相同的初始VM群組和設定成對建立。如有必要、您可以按一下各自的詳細資料連結並進行變更、個別自訂任何Runbook群組的設定。

在私有雲中安裝**AVS**的**Jetstream DR**

恢復站台（AVS）的最佳實務做法是事先建立三節點的指示燈式叢集。如此可預先設定恢復站台基礎架構、包括下列項目：

- 目的地網路區段、防火牆、DHCP和DNS等服務
- 安裝AVS的Jetstream DR
- 將anf磁碟區設定為資料存放區等

對於任務關鍵型網域、Jetstream DR支援的RTO模式接近零。對於這些網域、應該預先安裝目的地儲存設備。在此情況下、建議使用ANF儲存類型。

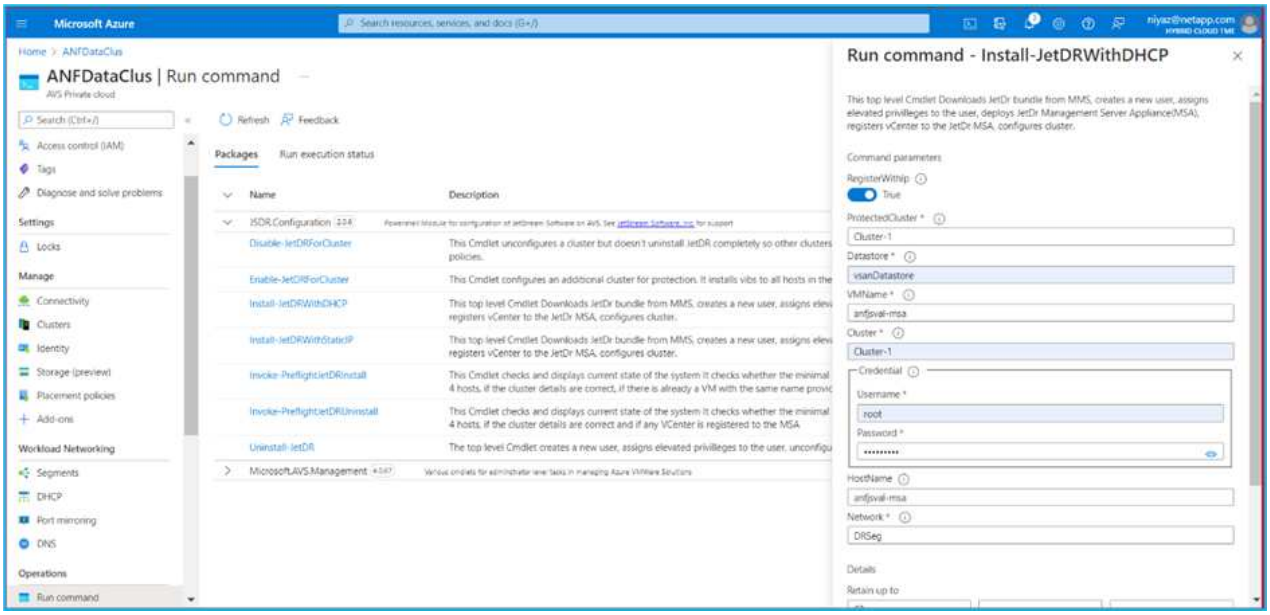
> ⓘ 應在AVS叢集上設定網路組態（包括區段建立）、以符合內部部署需求。

> ⓘ 視SLA和RTO需求而定、您可以使用持續容錯移轉或一般（標準）容錯移轉模式。對於接近零的RTO、您應該在恢復站台開始持續重新補充。

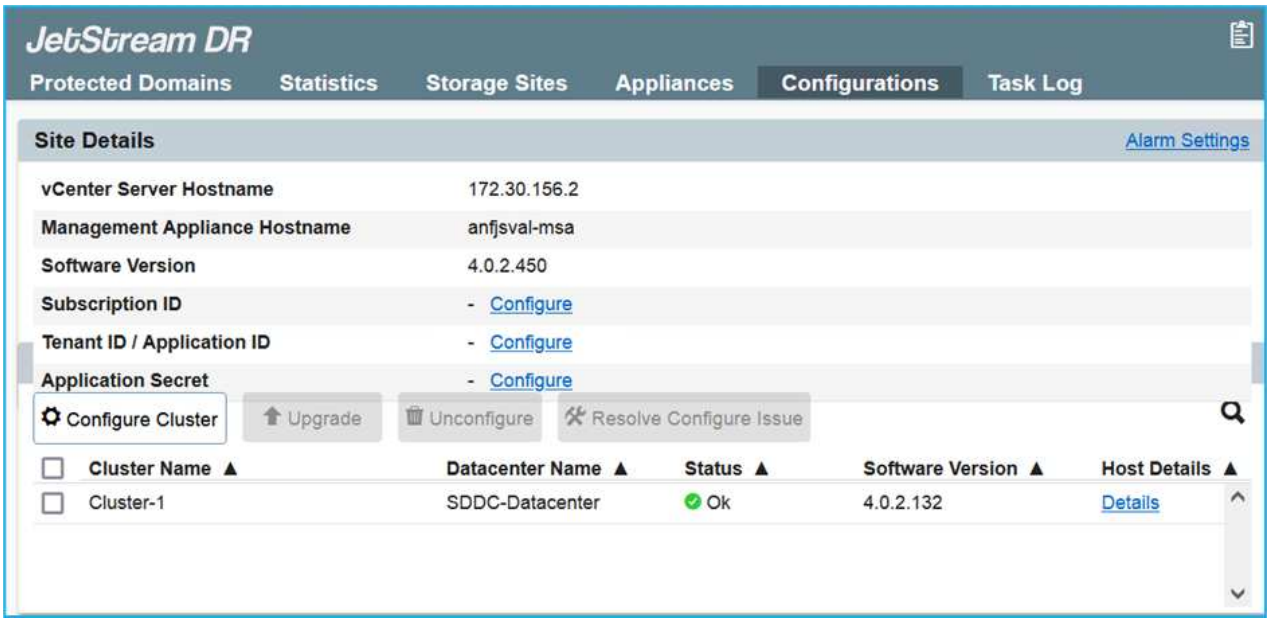
1. 若要在Azure VMware解決方案私有雲上安裝適用於AVS的Jetstream DR、請使用Run命令。從Azure入口網站移至Azure VMware解決方案、選取私有雲、然後選取執行命令>套件> JSDR.Configuration。

   > ⓘ Azure VMware解決方案的預設CloudAdmin使用者沒有足夠的權限可安裝適用於AVS的Jetstream DR。Azure VMware解決方案可針對Jetstream DR叫用Azure VMware Solution Run命令、以簡化及自動化方式安裝Jetstream DR。

   下列螢幕快照顯示使用DHCP型IP位址進行安裝。

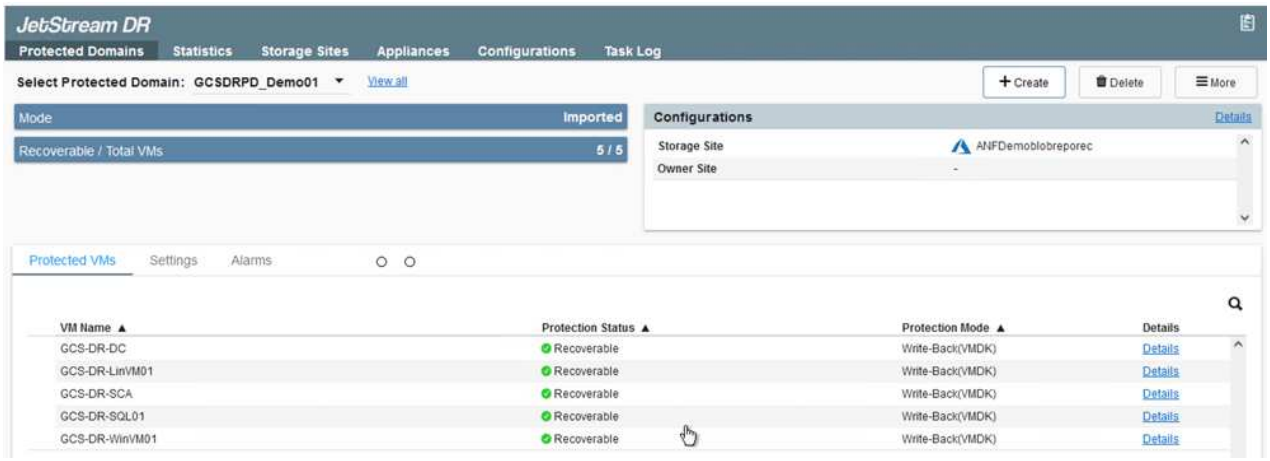


2. 在安裝AVS的Jetstream DR完成後、請重新整理瀏覽器。若要存取Jetstream DR UI、請前往SDDC資料中心>組態> Jetstream DR。



3. 在Jetstream DR介面中、完成下列工作：
   a. 新增Azure Blob儲存設備帳戶、以保護內部部署叢集做為儲存站台、然後執行「掃描網域」選項。
   b. 在出現的快顯對話方塊視窗中、選取要匯入的受保護網域、然後按一下其匯入連結。

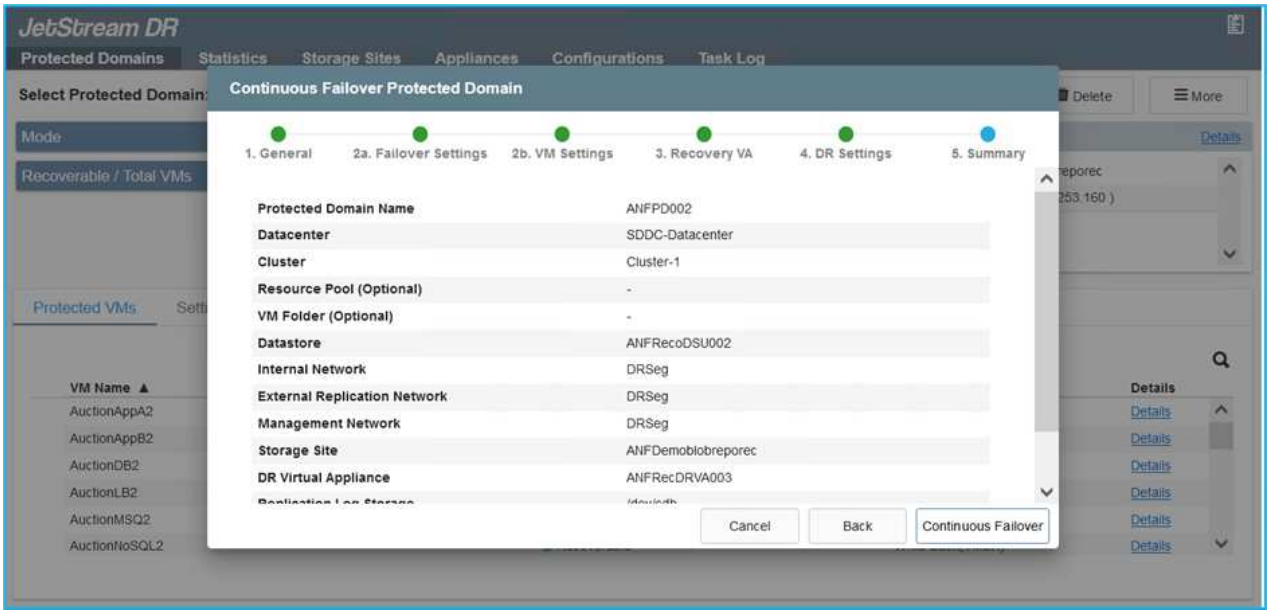
4. 網域已匯入以供還原。移至「受保護的網域」索引標籤、確認已選取所需的網域、或從「選取受保護的網域」功能表中選擇所需的網域。隨即顯示受保護網域中可恢復的VM清單。



5. 匯入受保護的網域之後、請部署DRVA設備。

> 您也可以使用由CPt建立的計畫來自動化這些步驟。

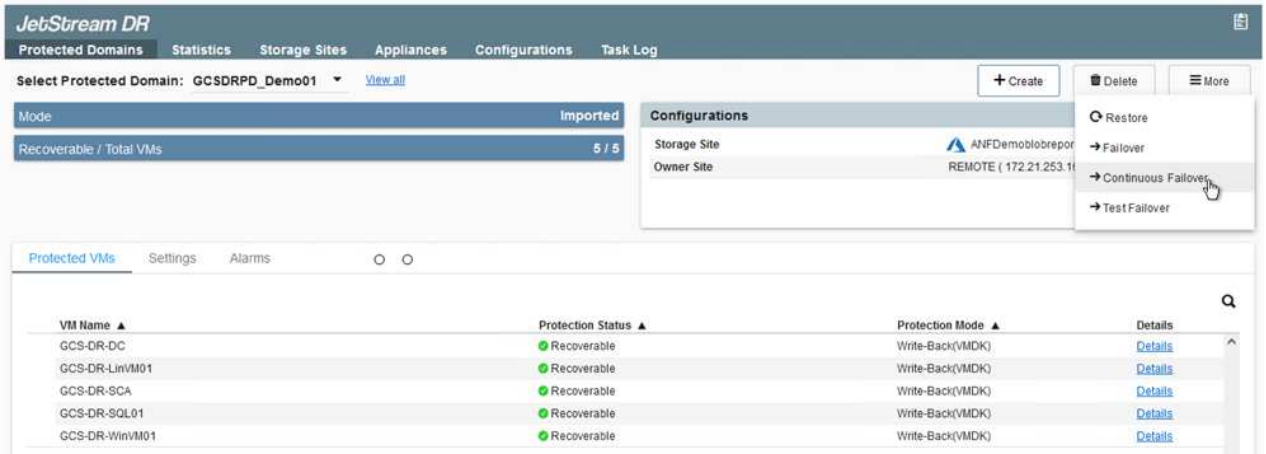
6. 使用可用的vSAN或ANF資料存放區建立複寫記錄磁碟區。
7. 匯入受保護的網域、並將恢復VA設定為使用ANF資料存放區來放置VM。



請確定選取的區段已啟用DHCP、而且有足夠的IP可用。在網域還原期間、會暫時使用動態IP。每個恢復中的VM（包括持續重新補充）都需要個別的動態IP。恢復完成後、IP便會釋出、並可重複使用。

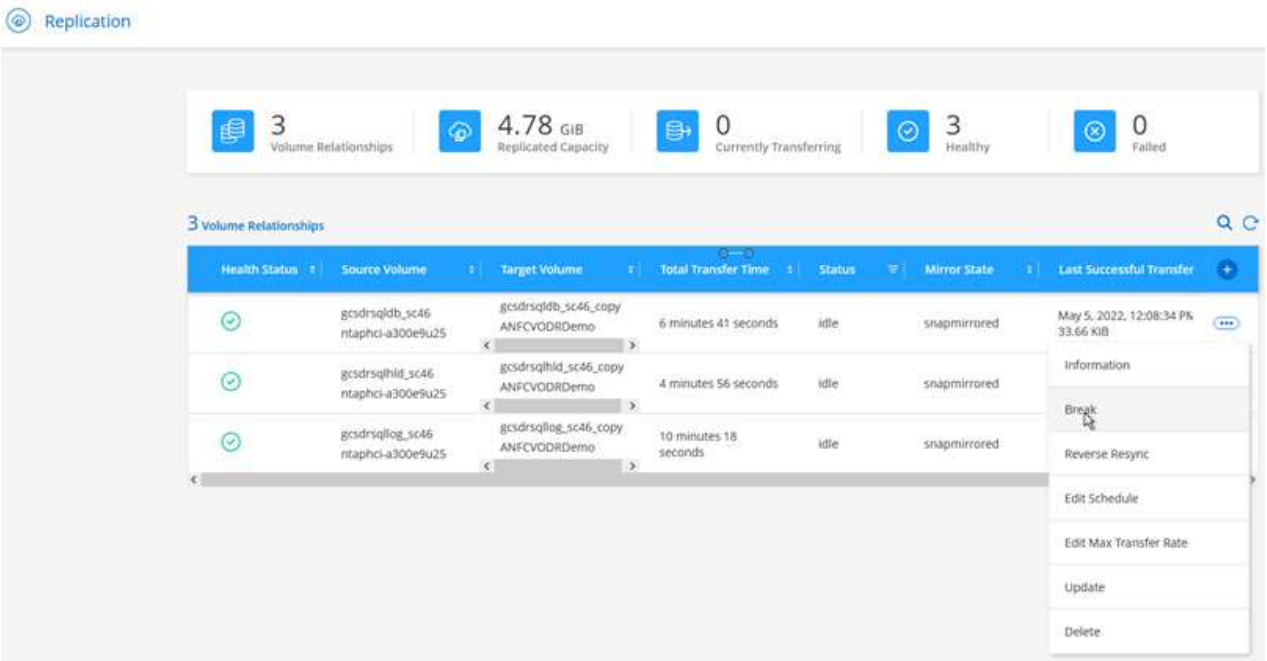
8. 選取適當的容錯移轉選項（持續容錯移轉或容錯移轉）。在此範例中、會選取持續還原（持續容錯移轉）。

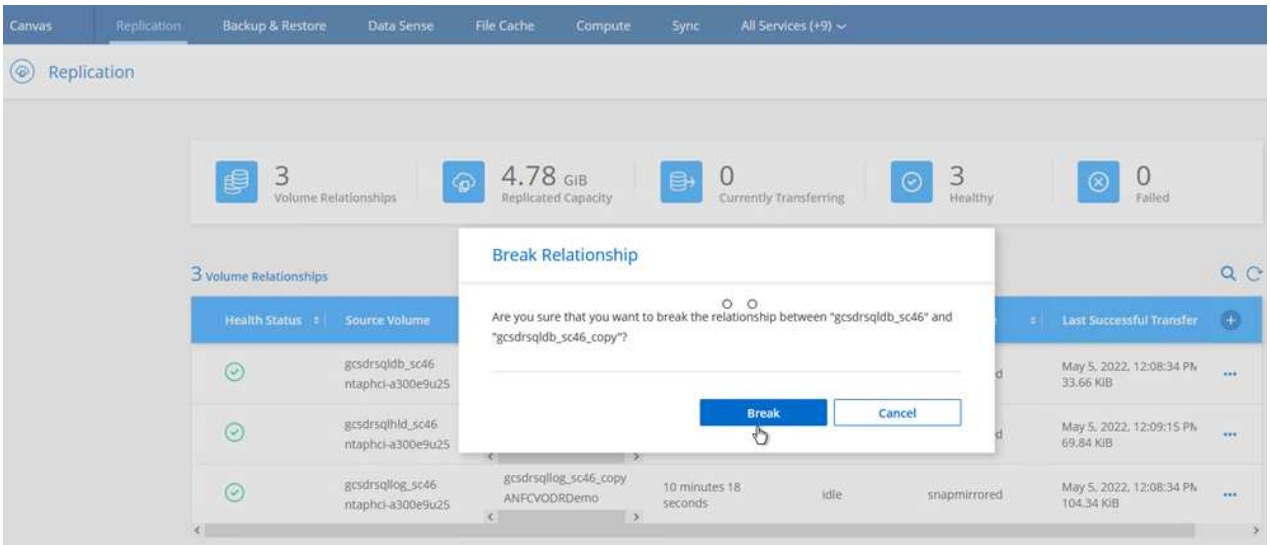
雖然執行組態時、「持續容錯移轉」和「容錯移轉」模式各有不同、但兩種容錯移轉模式的設定步驟相同。容錯移轉步驟會一起設定及執行、以回應災難事件。您可以隨時設定持續容錯移轉、然後在正常系統作業期間、允許在背景執行。發生災難事件之後、持續容錯移轉作業便會完成、以便立即將受保護VM的擁有權轉移到恢復站台（RTO接近零）。



持續容錯移轉程序隨即開始、其進度可從UI監控。按一下「目前步驟」區段中的藍色圖示、會顯示快顯視窗、顯示容錯移轉程序目前步驟的詳細資料。

1. 在內部部署環境的受保護叢集發生災難（部分或完整故障）之後、您可以在中斷個別應用程式磁碟區的SnapMirror關係之後、使用Jetstream來觸發VM的容錯移轉。

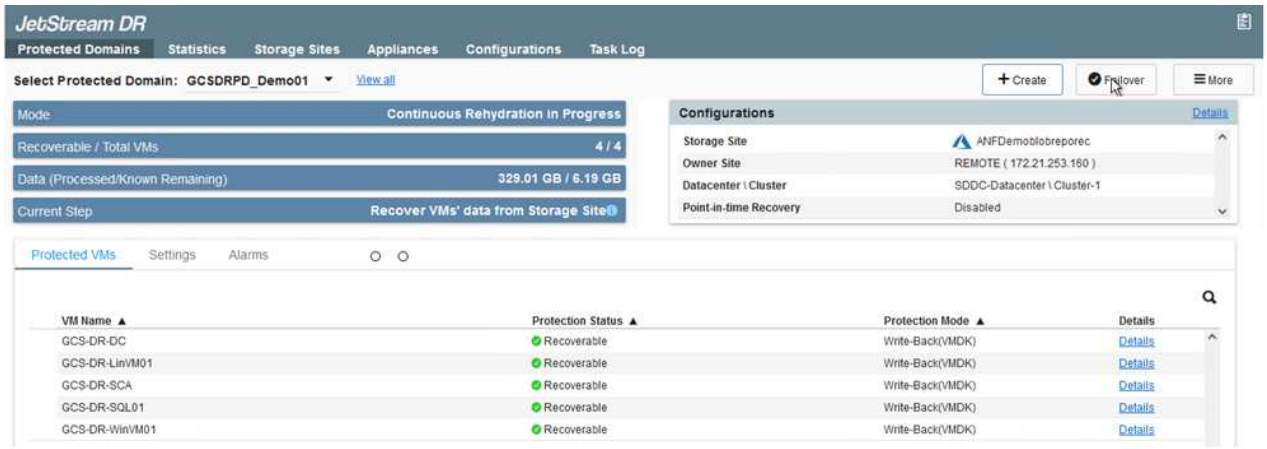


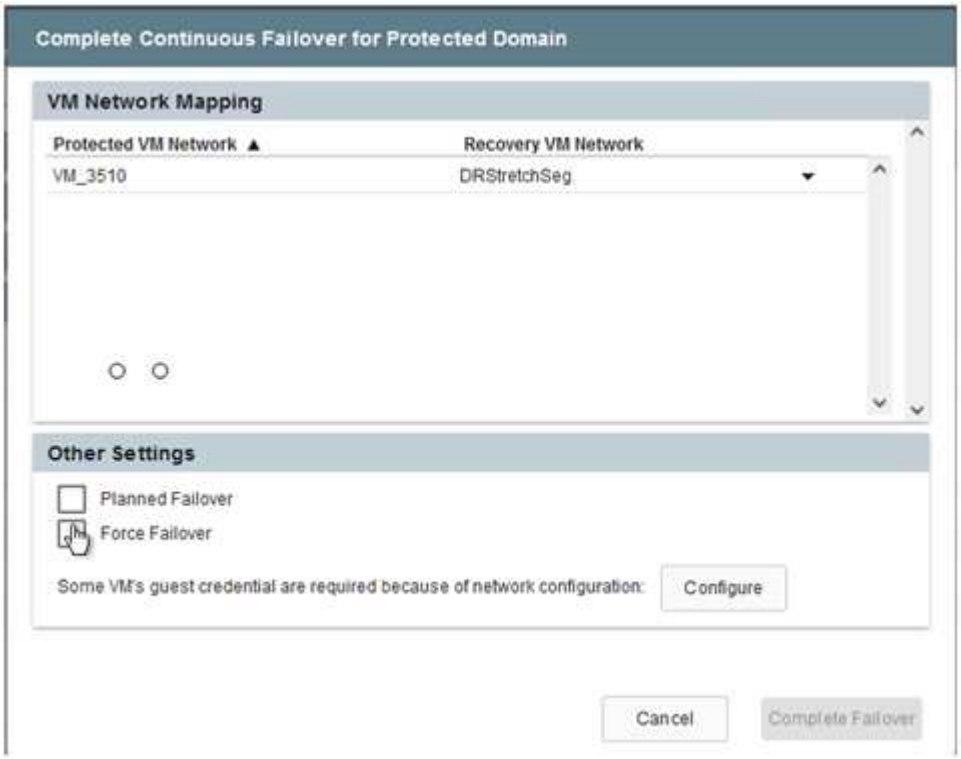


> 此步驟可輕鬆自動化、以利恢復程序。

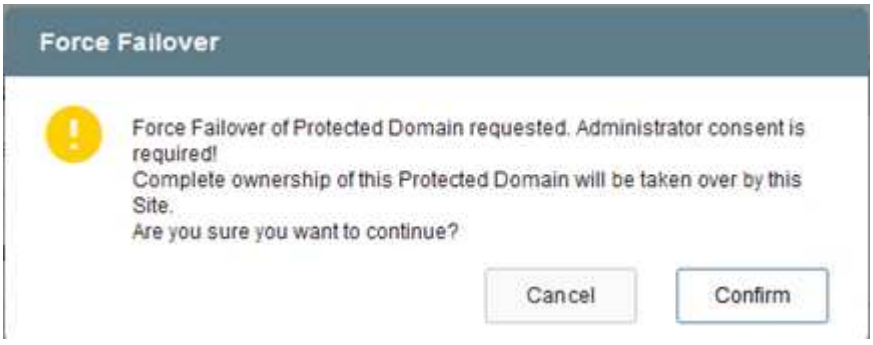
2. 存取AVS SDDC（目的地端）上的Jetstream UI、然後觸發容錯移轉選項以完成容錯移轉。工作列會顯示容錯移轉活動的進度。

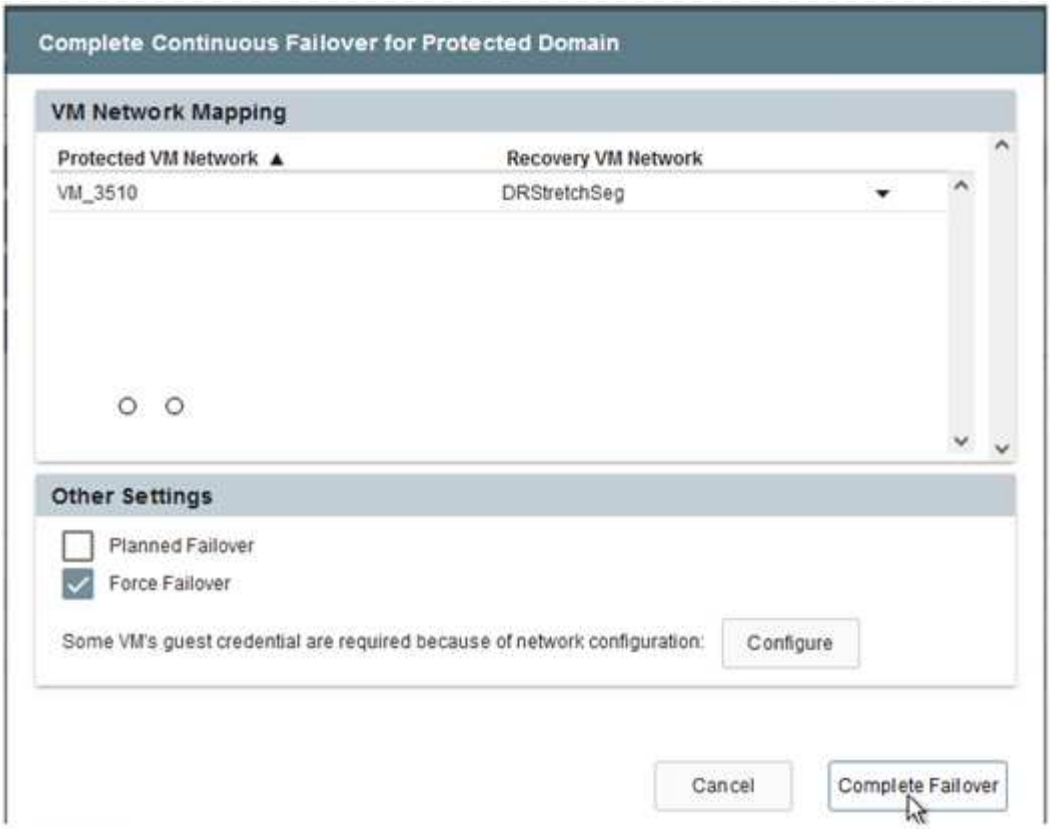
   在完成容錯移轉時所出現的對話視窗中、容錯移轉工作可以指定為已規劃或假設為強制進行。





強制容錯移轉假設主站台已無法再存取、且受保護網域的擁有權應由還原站台直接承擔。





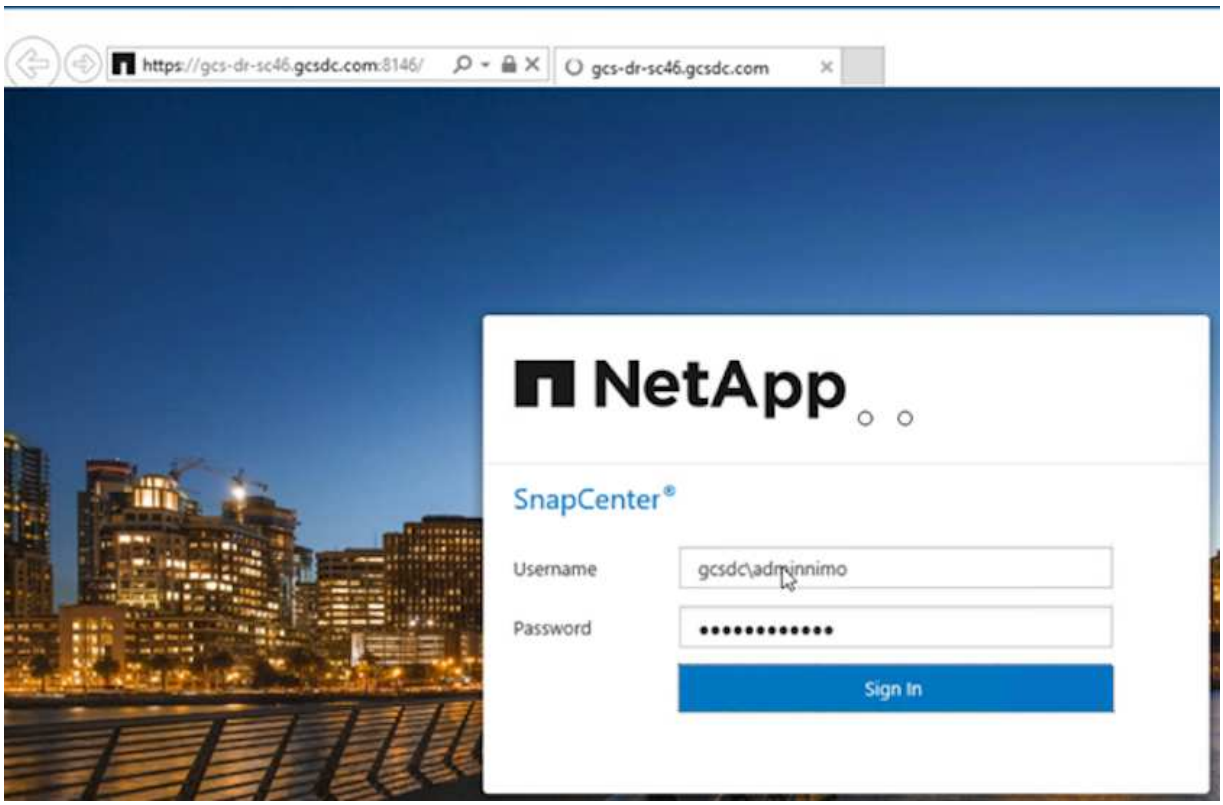
3. 持續容錯移轉完成後、會出現一則訊息、確認工作已完成。當工作完成時、請存取恢復的VM來設定iSCSI或NFS工作階段。

> 容錯移轉模式會變更為在容錯移轉中執行、而VM狀態會恢復。受保護網域的所有VM現在都在容錯移轉執行手冊設定所指定的狀態下、於還原站台執行。

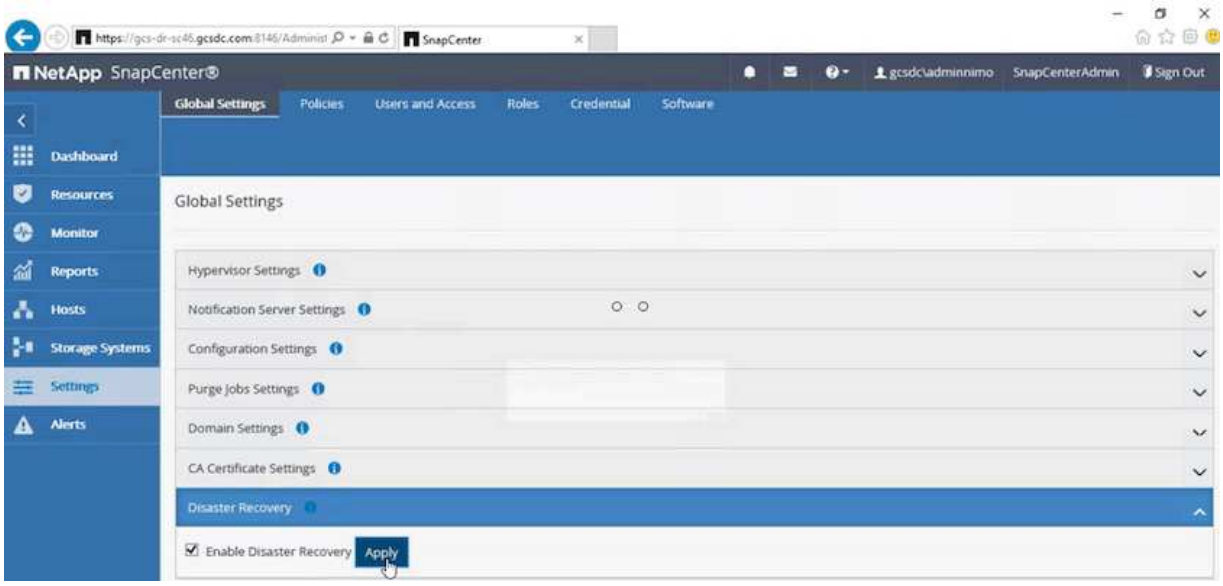
> 為了驗證容錯移轉組態和基礎架構、可以在測試模式（測試容錯移轉選項）下操作、觀察虛擬機器及其資料從物件存放區恢復到測試還原環境的過程。在測試模式下執行容錯移轉程序時、其運作方式類似於實際的容錯移轉程序。

4. 虛擬機器恢復後、請使用儲存災難恢復功能來進行客體內儲存設備。為了示範此程序、本範例使用SQL Server。

5. 在SnapCenter AVS SDDC上登入恢復的S振 向虛擬機器、並啟用DR模式。
   a. 使用瀏覽器N存取SnapCenter 這個功能。



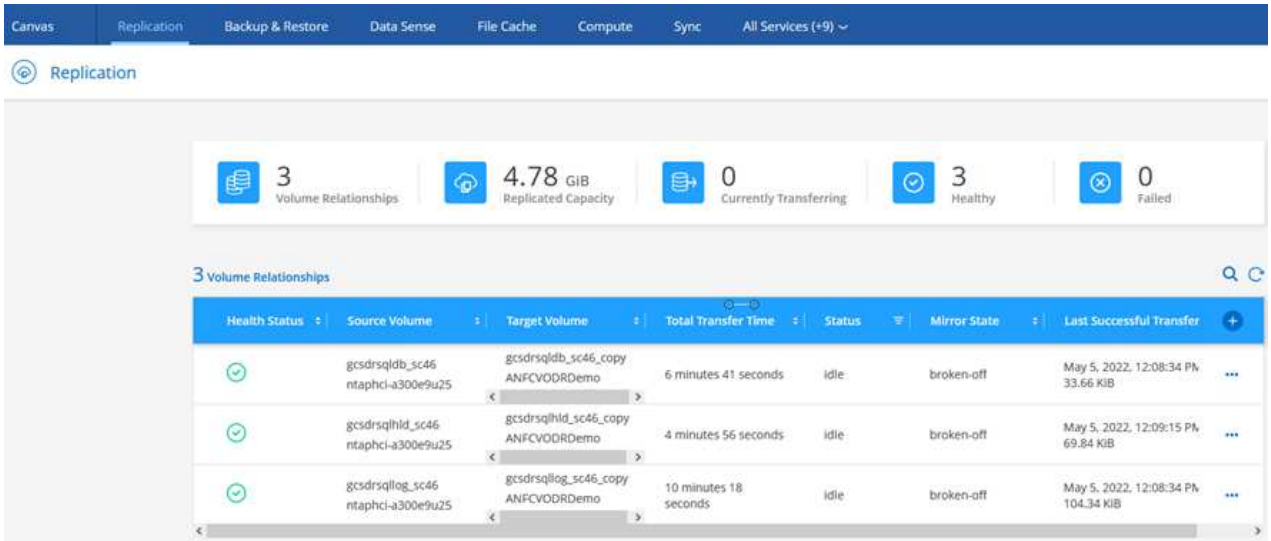
   b. 在「設定」頁面中、瀏覽至「設定」>「全域設定」>「災難恢復」。
   c. 選取「啟用災難恢復」。
   d. 按一下套用。



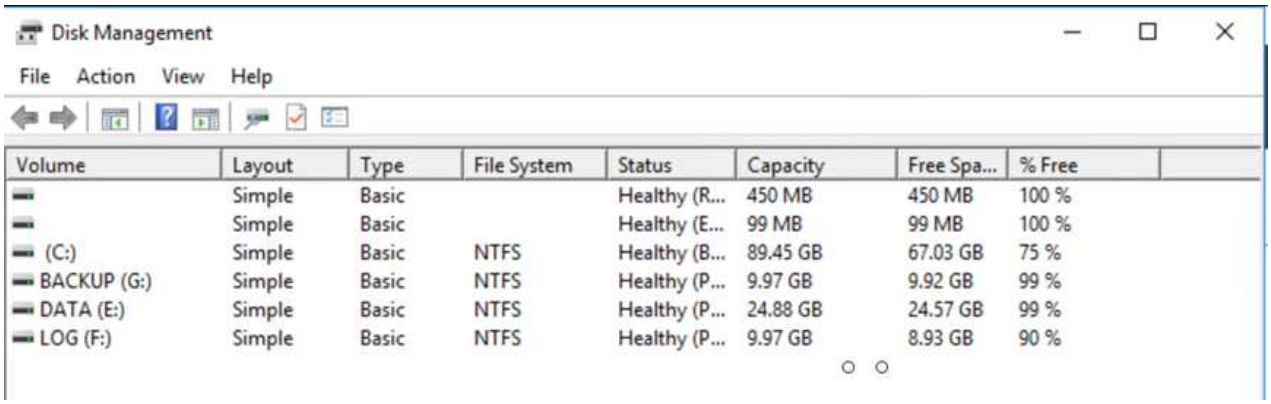
   e. 按一下「監控」>「工作」、確認DR工作是否已啟用。

NetApp SnapCenter 支援區4.6或更新版本應用於儲存災難恢復。對於舊版、應使用應用程式一致的快照（使用SnapMirror複寫）、如果必須在災難恢復站台中恢復先前的備份、則應執行手動恢復。

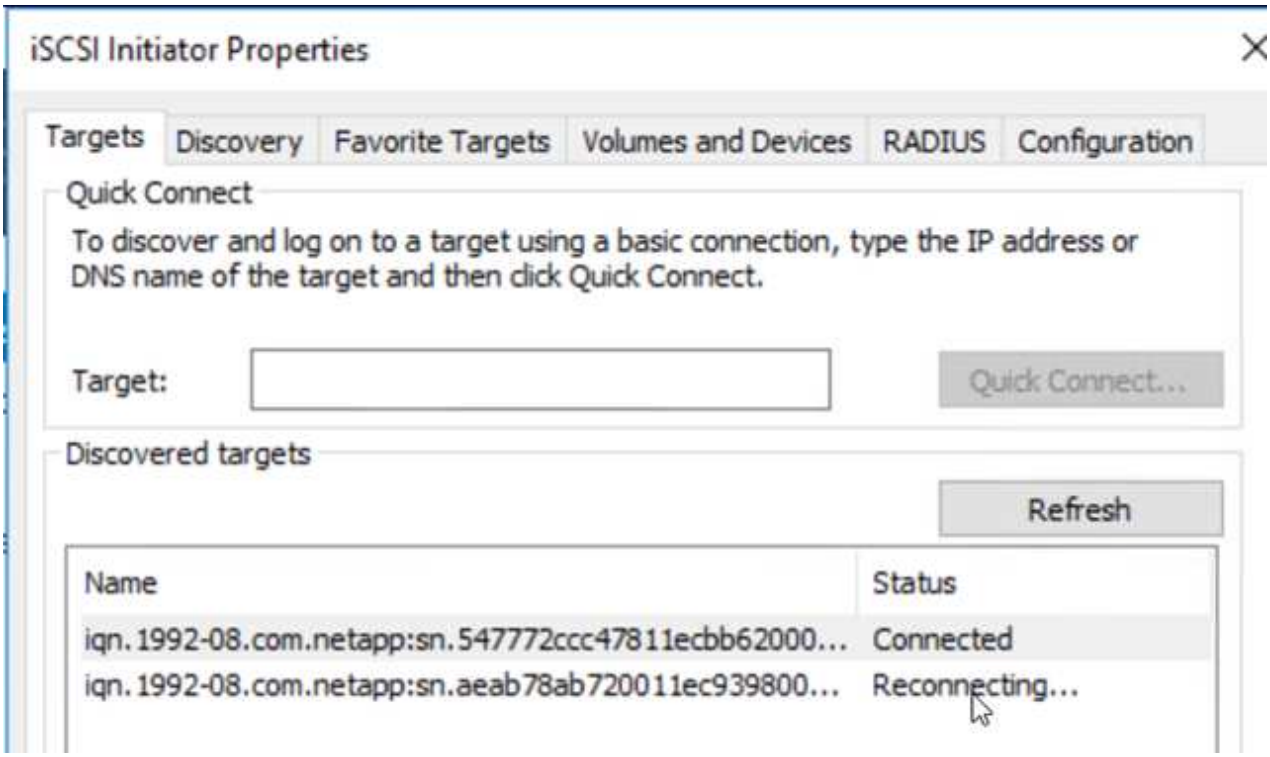
6. 確定SnapMirror關係已中斷。



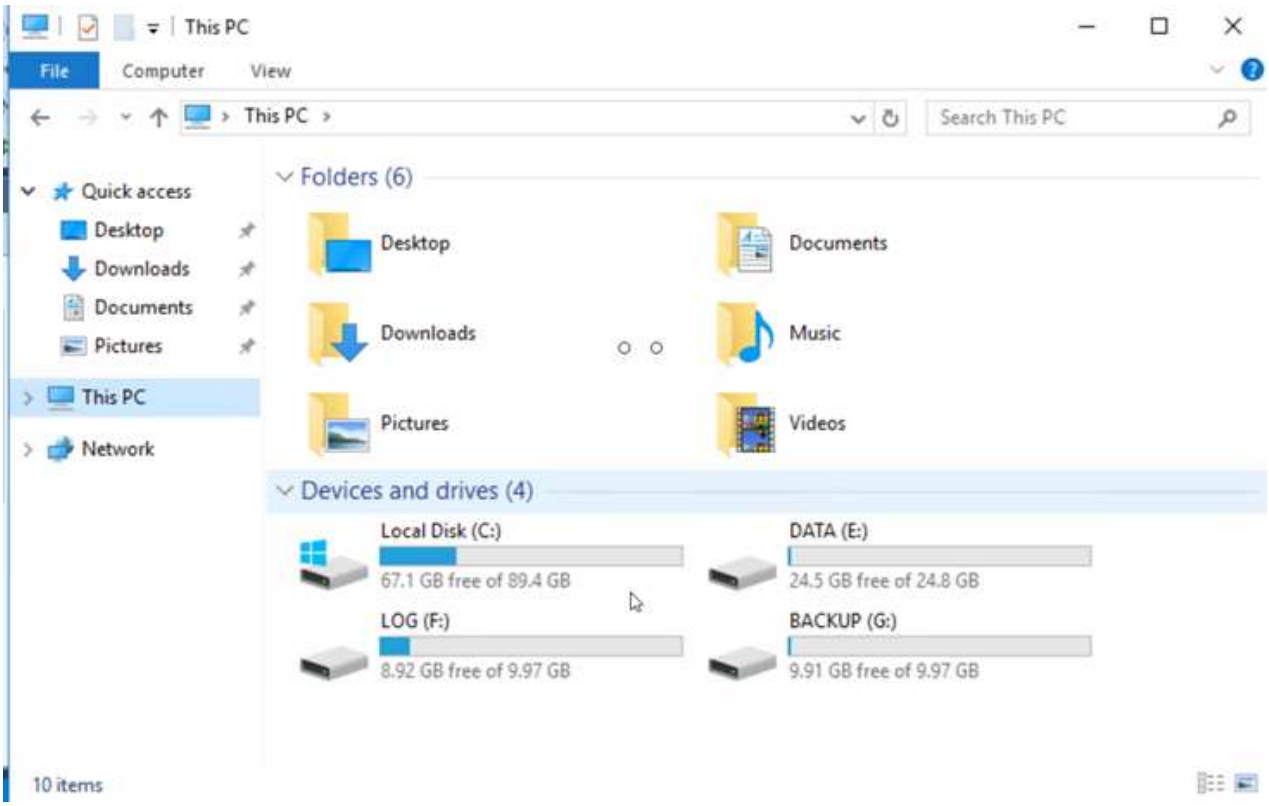
7. 使用Cloud Volumes ONTAP 相同的磁碟機代號、將LUN從支援系統連接到已恢復的SQL客體VM。



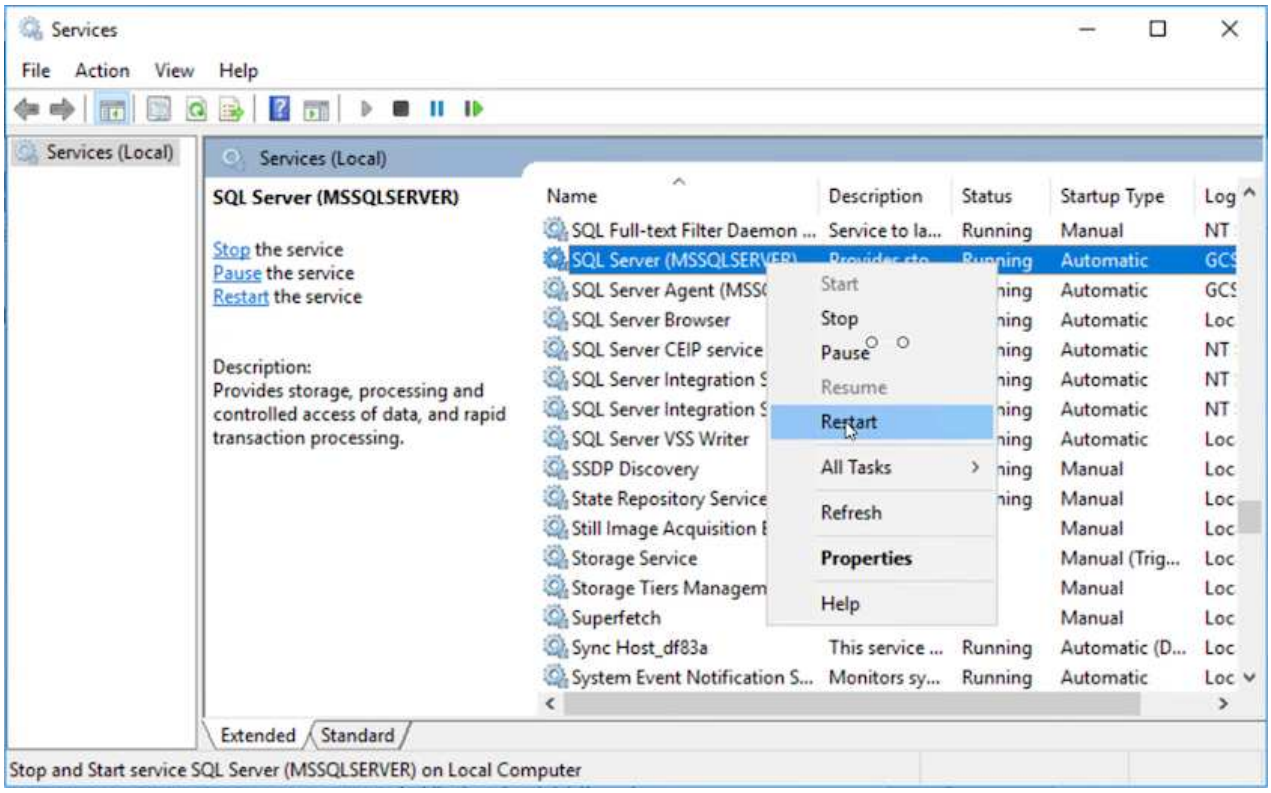
8. 開啟iSCSI啟動器、清除先前中斷連線的工作階段、並新增新目標及複寫Cloud Volumes ONTAP 的支援區的多重路徑。



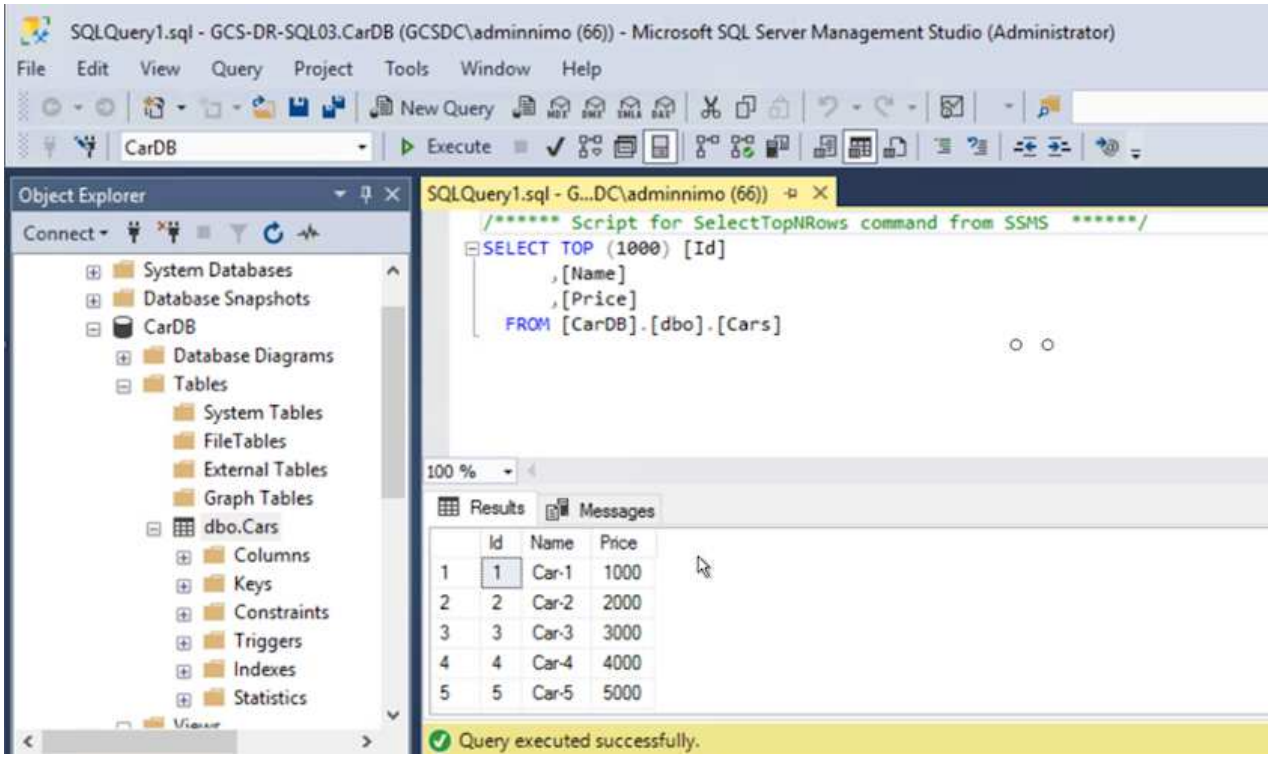
9. 請確定所有磁碟均使用與DR之前相同的磁碟機代號進行連線。



10. 重新啟動MSSQL伺服器服務。



11. 請確定SQL資源重新連線。



> ⓘ 如果是NFS、請使用mount命令附加磁碟區、然後更新「etc/fstab'」項目。

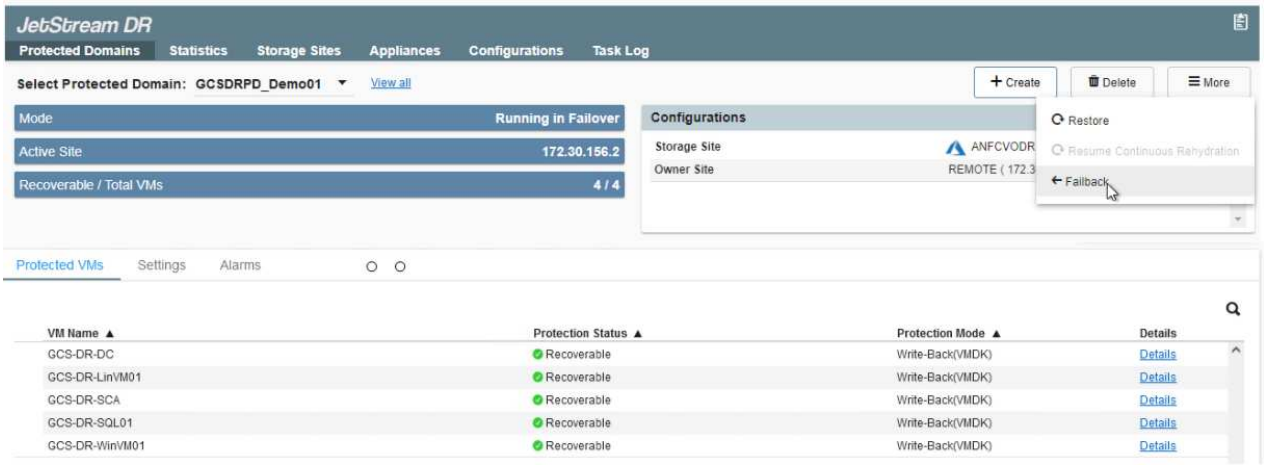
此時、您可以執行作業並正常營運。

> 在NSxT-T端點上、可建立獨立的專屬層級1閘道、以模擬容錯移轉案例。如此可確保所有工作負載彼此通訊、但不會有流量進入或離開環境、如此一來、就能執行任何分類、控制或強化工作、而不會產生交叉污染的風險。此作業不在本文件的範圍之內、但可輕鬆模擬隔離。

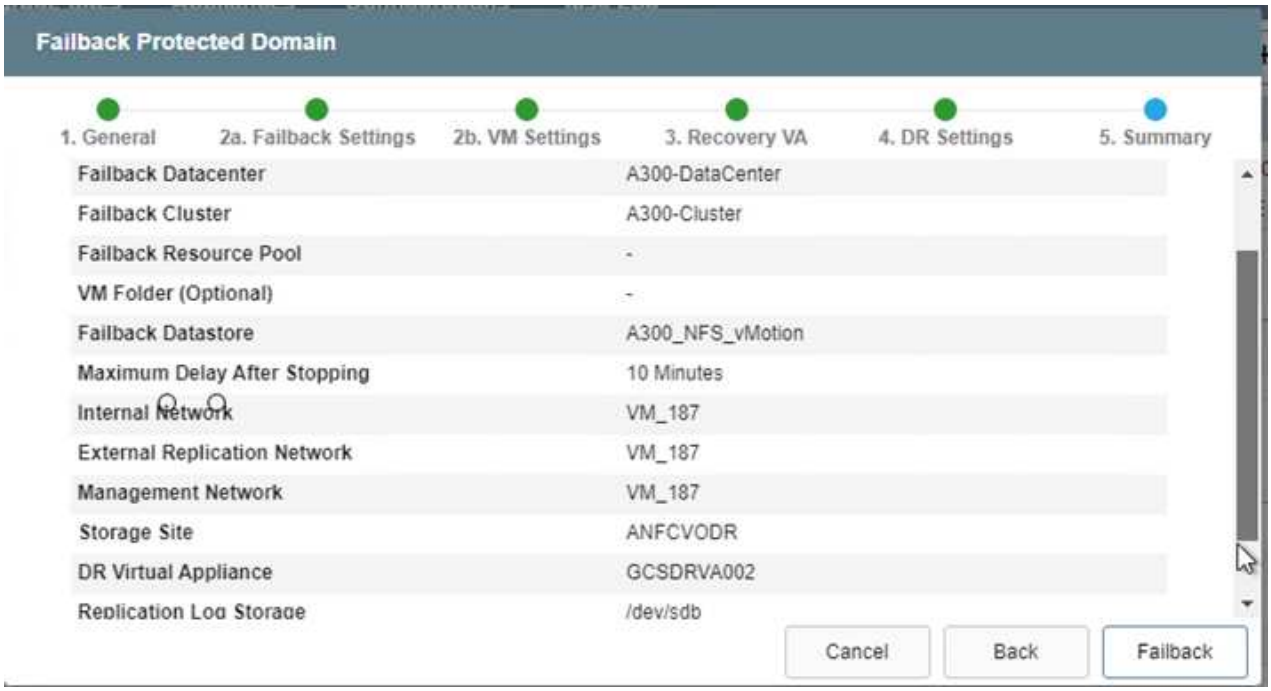
當主要站台重新啟動並執行之後、您就可以執行容錯回復。系統會由Jetstream恢復VM保護、且SnapMirror關係必須回復。

1. 還原內部部署環境。視災難事件類型而定、可能需要還原及/或驗證受保護叢集的組態。如有必要、可能需要重新安裝Jetstream DR軟體。
2. 存取還原的內部部署環境、前往Jetstream DR UI、然後選取適當的受保護網域。受保護的站台準備好進行容錯回復之後、請在UI中選取「容錯回復」選項。

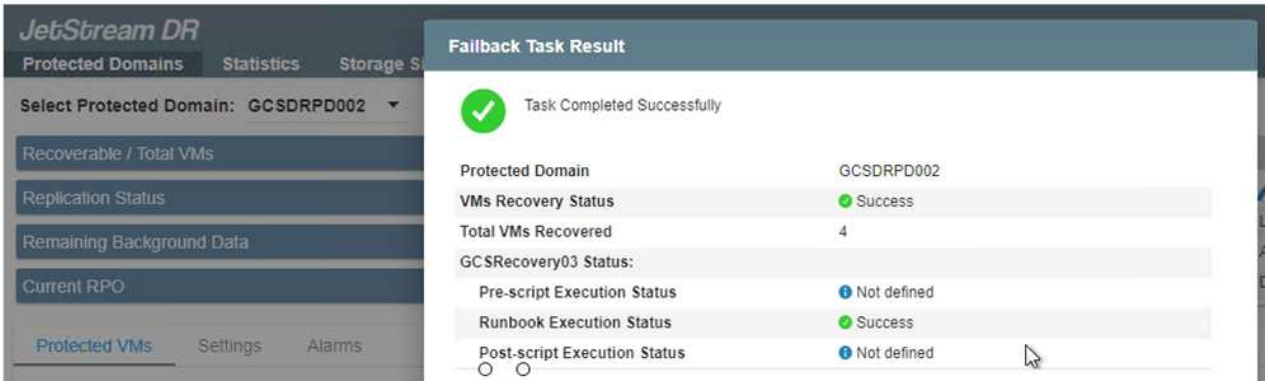
> 此外、也可使用由程式管理產生的容錯回復計畫、將VM及其資料從物件存放區傳回原始的VMware環境。



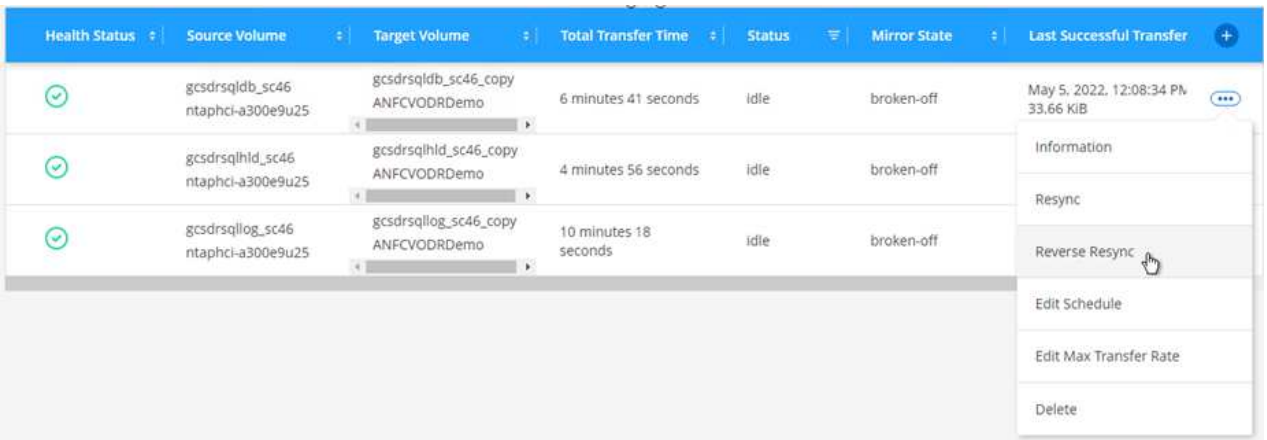
> 在恢復站台中暫停VM並在受保護站台重新啟動VM之後、請指定最大延遲。完成此程序所需的時間包括：停止容錯移轉VM後完成複寫、清理恢復站台所需的時間、以及在受保護站台重新建立VM所需的時間。NetApp建議使用10分鐘。

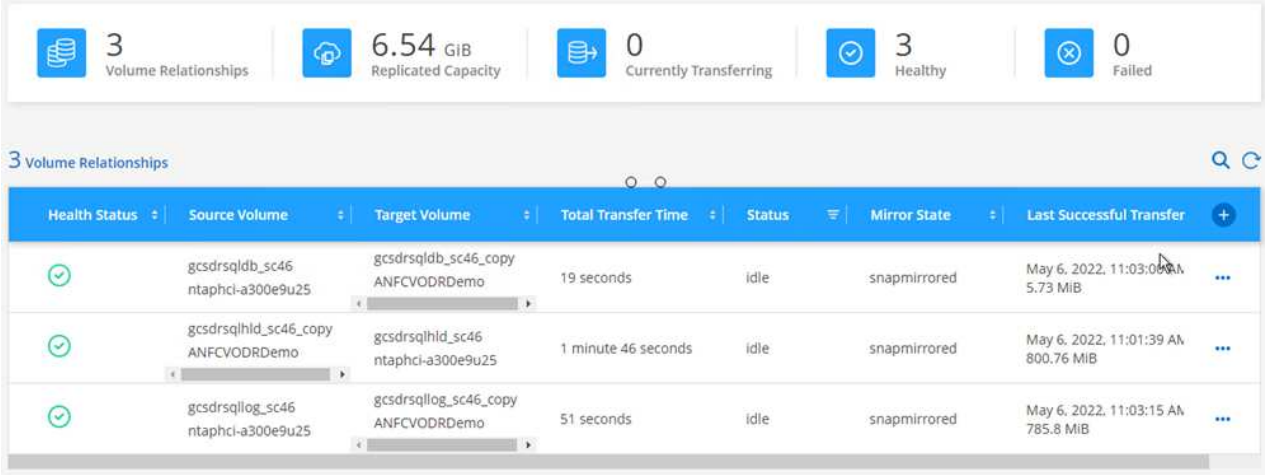


3. 完成容錯回復程序、然後確認恢復VM保護和資料一致性。

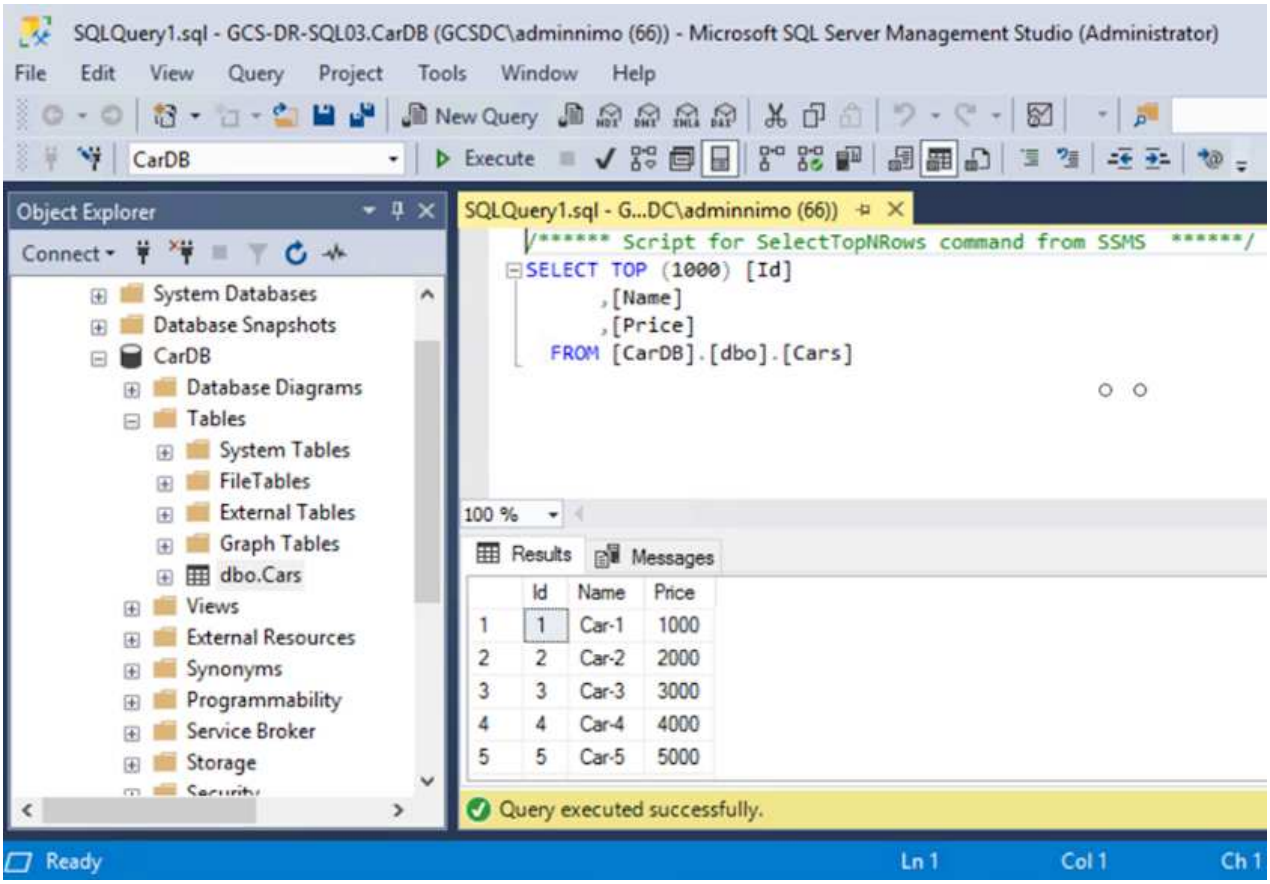


4. 恢復虛擬機器後、請中斷次要儲存設備與主機的連線、並連線至主要儲存設備。





5. 重新啟動MSSQL伺服器服務。
6. 驗證SQL資源是否重新連線。



> ⓘ 若要容錯回復至主要儲存設備、請執行反向重新同步作業、確保關係方向與容錯移轉之前的方向相同。

> ⓘ 若要在反向重新同步作業之後保留主要和次要儲存設備的角色、請再次執行反轉重新同步作業。

此程序適用於其他應用程式、例如Oracle、類似的資料庫類型、以及使用客體連線儲存設備的任何其他應

用程式。

如同往常一樣、在將關鍵工作負載移轉至正式作業之前、請先測試相關步驟、以恢復這些工作負載。

本解決方案的優點

- 使用SnapMirror的高效率和彈性複寫。
- 利用不含資料的快照保留功能、可即時恢復至任何可用點ONTAP 。
- 從儲存、運算、網路和應用程式驗證步驟、將數百個VM恢復到數千個VM所需的所有步驟均可完全自動化。
- 使用不會變更複寫磁碟區的複製機制。SnapCenter
  - 如此可避免磁碟區和快照發生資料毀損的風險。
  - 避免災難恢復測試工作流程期間的複寫中斷。
  - 利用DR資料處理DR以外的工作流程、例如開發/測試、安全性測試、修補程式與升級測試、以及補救測試。
- CPU與RAM最佳化可讓您恢復至較小的運算叢集、進而降低雲端成本。

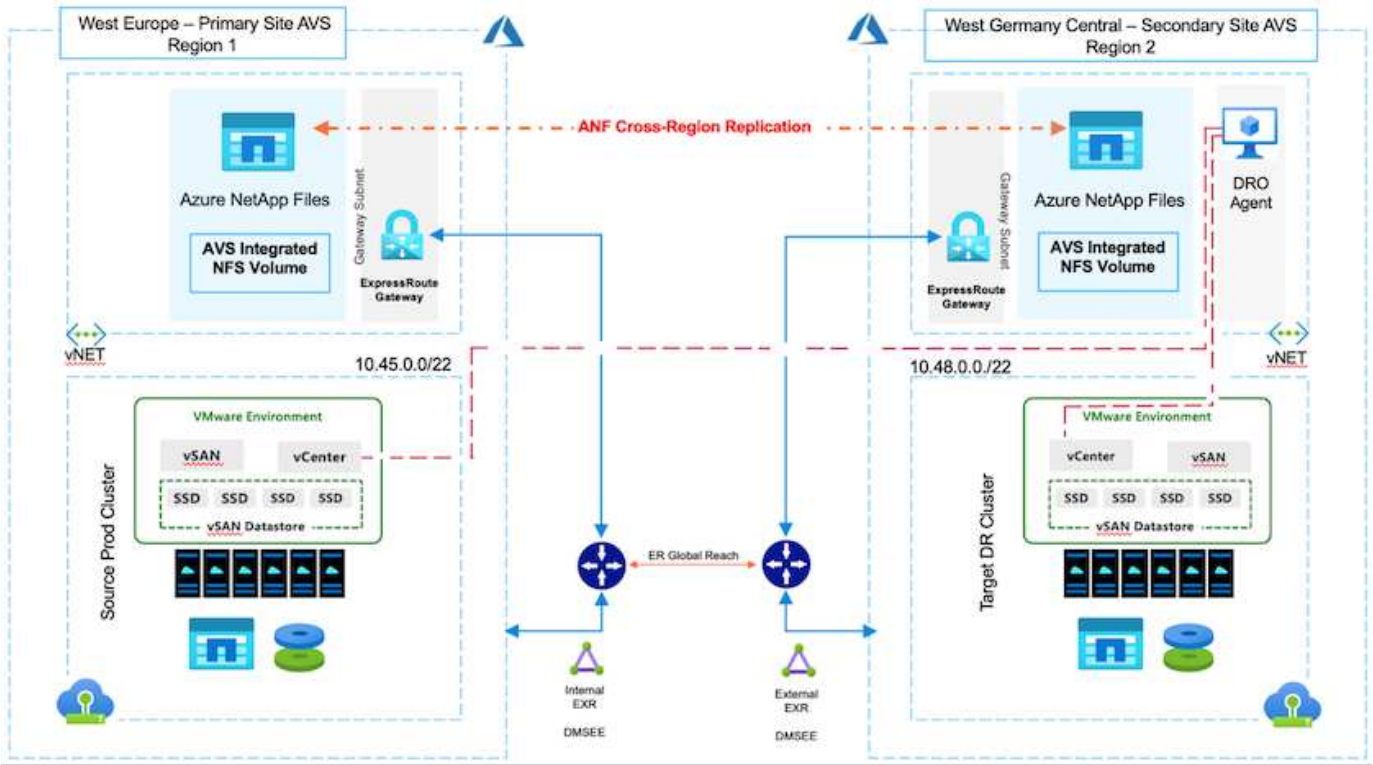
TR-4755 ：使用 Azure NetApp Files （ anf ）和 Azure VMware 解決方案（ AVS ）進行災難恢復

作者： NetApp 解決方案工程公司 Niyaz Mohamed

總覽

在雲端區域之間使用區塊層級複寫進行災難恢復、是一種彈性且具成本效益的方法、可保護工作負載免受站台中斷和資料毀損事件（例如勒索軟體）的影響。透過 Azure NetApp Files （ anf ）跨區域磁碟區複寫、在 Azure VMware 解決方案（ AVS ） SDDC 站台上執行的 VMware 工作負載、使用 Azure NetApp Files 磁碟區做為主要 AVS 站台上的 NFS 資料存放區、可複寫至目標恢復區域中的指定次要 AVS 站台。

災難恢復協調器（ DRO ）（一種具有 UI 的指令碼化解決方案）可用於無縫恢復從一個 AVS SDDC 複製到另一個 AVS SDDC 的工作負載。DRO 會中斷複寫對等關係、然後將目的地磁碟區掛載為資料存放區、透過 VM 註冊至 AVS 、將其自動還原至 NSS-T 上的網路對應（包含在所有 AVS 私有雲中）。



先決條件和一般建議

- 建立複寫對等關係、確認您已啟用跨區域複寫。請參閱 "為 Azure NetApp Files 建立 Volume 複寫"。
- 您必須在來源與目標 Azure VMware 解決方案私有雲之間設定 ExpressRoute Global Reach 。
- 您必須擁有可存取資源的服務主體。
- 支援下列拓撲：主要 AVS 站台到次要 AVS 站台。
- 設定 "複寫" 根據業務需求和資料變更率、適當排程每個 Volume 。

> ⓘ 不支援串聯和扇入及扇出拓撲。

快速入門

部署 **Azure VMware** 解決方案

。 "Azure VMware解決方案" （AVS）是混合雲服務、可在 Microsoft Azure 公有雲中提供功能完整的 VMware SDDC 。AVS是第一方的解決方案、由Microsoft完全管理及支援、並由VMware驗證、使用Azure基礎架構。因此、客戶可取得 VMware ESXi 來進行運算虛擬化、 vSAN 用於超融合式儲存設備、而 NSX 則用於網路和安全性、同時還能充分利用 Microsoft Azure 的全球知名度、領先同級的資料中心設施、以及鄰近豐富的原生 Azure 服務與解決方案生態系統。Azure VMware解決方案SDDC與Azure NetApp Files VMware解決方案的結合、可提供最佳效能、並將網路延遲降至最低。

若要在 Azure 上設定 AVS 私有雲、請遵循本中的步驟 "連結" 適用於 NetApp 文件及本文件 "連結" 適用於 Microsoft 文件。 以最小組態設定的導向照明環境可用於 DR 用途。 此設定僅包含支援關鍵應用程式的核心元件、而且在發生容錯移轉時、它可以橫向擴充和啟動更多主機來承受大量負載。

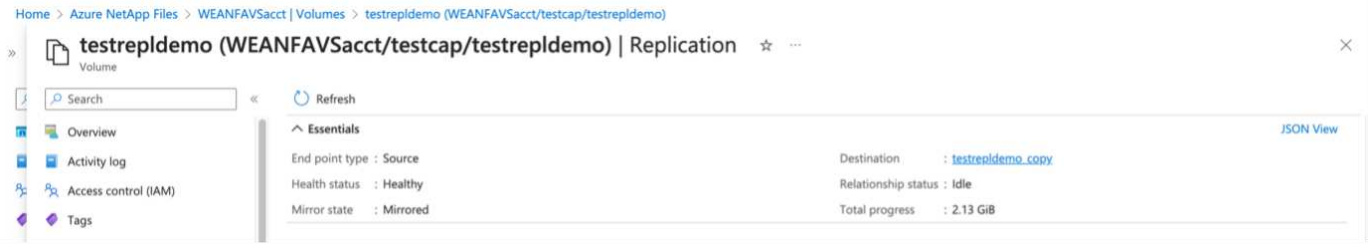
在初始版本中、 DRO 支援現有的 AVS SDDC 叢集。隨需建立SDDC將於即將推出的版本中提供。

配置和配置 **Azure NetApp Files**

"Azure NetApp Files" 是一項高效能、企業級的計量檔案儲存服務。請依照本文件中的步驟進行 "連結" 將 Azure NetApp Files 配置為 NFS 資料存放區、以最佳化 AVS 私有雲部署。

為 **Azure NetApp Files** 資料存放區磁碟區建立 **Volume** 複寫

第一步是設定所需資料存放區磁碟區的跨區域複寫、從 AVS 主要站台到 AVS 次要站台、並提供適當的頻率和保留。



請依照本文件中的步驟進行 "連結" 建立複寫對等關係來設定跨區域複寫。目的地容量集區的服務層級可與來源容量集區的服務層級相符。不過、在這種特定的使用案例中、您可以選擇標準服務層級、然後再選擇 "修改服務層級" 發生真正的災難或災難恢復模擬時。

跨區域複寫關係是先決條件、必須事先建立。

DRO安裝

若要開始使用 DRO 、請在指定的 Azure 虛擬機器上使用 Ubuntu 作業系統、並確保您符合先決條件。然後安裝套件。

- 先決條件： *
- 可存取資源的服務主體。
- 請確定來源和目的地 SDDC 和 Azure NetApp Files 執行個體有適當的連線。
- 如果您使用DNS名稱、則應該已有DNS解析。否則、請使用 vCenter 的 IP 位址。
- 作業系統需求： *
- Ubuntu 焦點 20.04 （ LTS ） 下列套件必須安裝在指定的代理程式虛擬機器上：
- Docker
- Docker - 撰寫
- JqChange `docker.sock` 此新權限： `sudo chmod 666 /var/run/docker.sock`。

。 `deploy.sh` 指令碼會執行所有必要的先決條件。

步驟如下：

1. 在指定的虛擬機器上下載安裝套件：

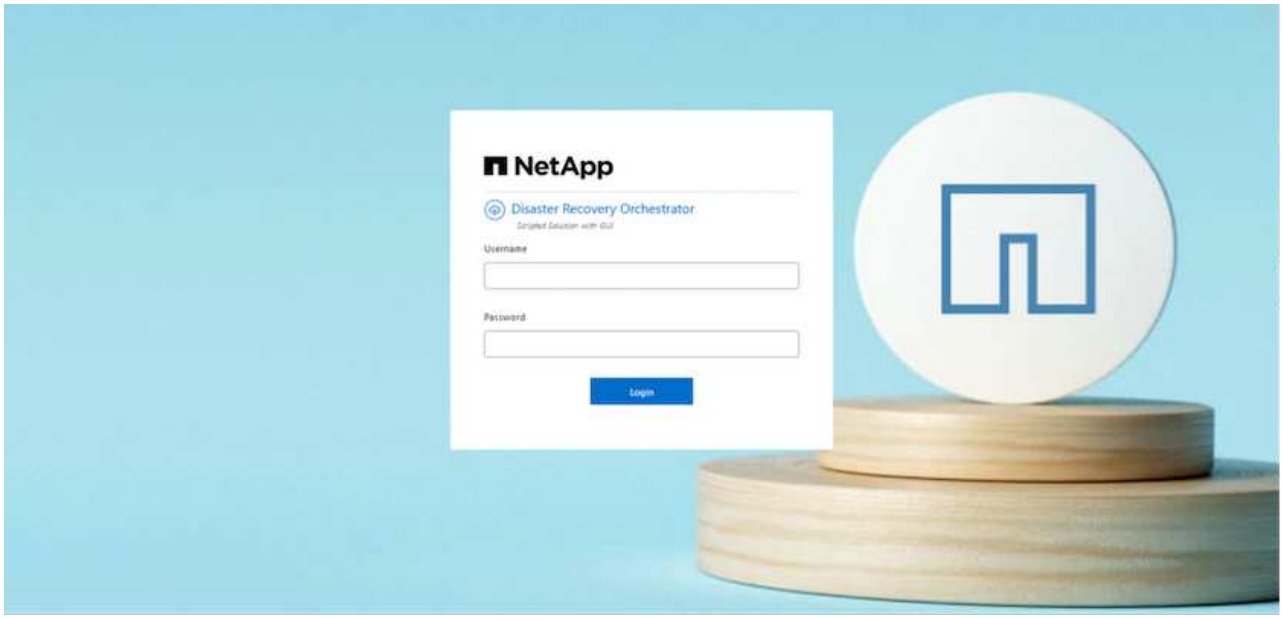
```
git clone https://github.com/NetApp/DRO-Azure.git
```

> 代理程式必須安裝在次要 AVS 站台區域、或安裝在主要 AVS 站台區域、但必須安裝在 SDDC 以外的另一個 AZ 。

2. 解壓縮套件、執行部署指令碼、然後輸入主機 IP （例如、 `10.10.10.10`）。

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. 使用下列認證存取 UI ：
   - 使用者名稱： `admin`
   - 密碼： `admin`



DRO組態

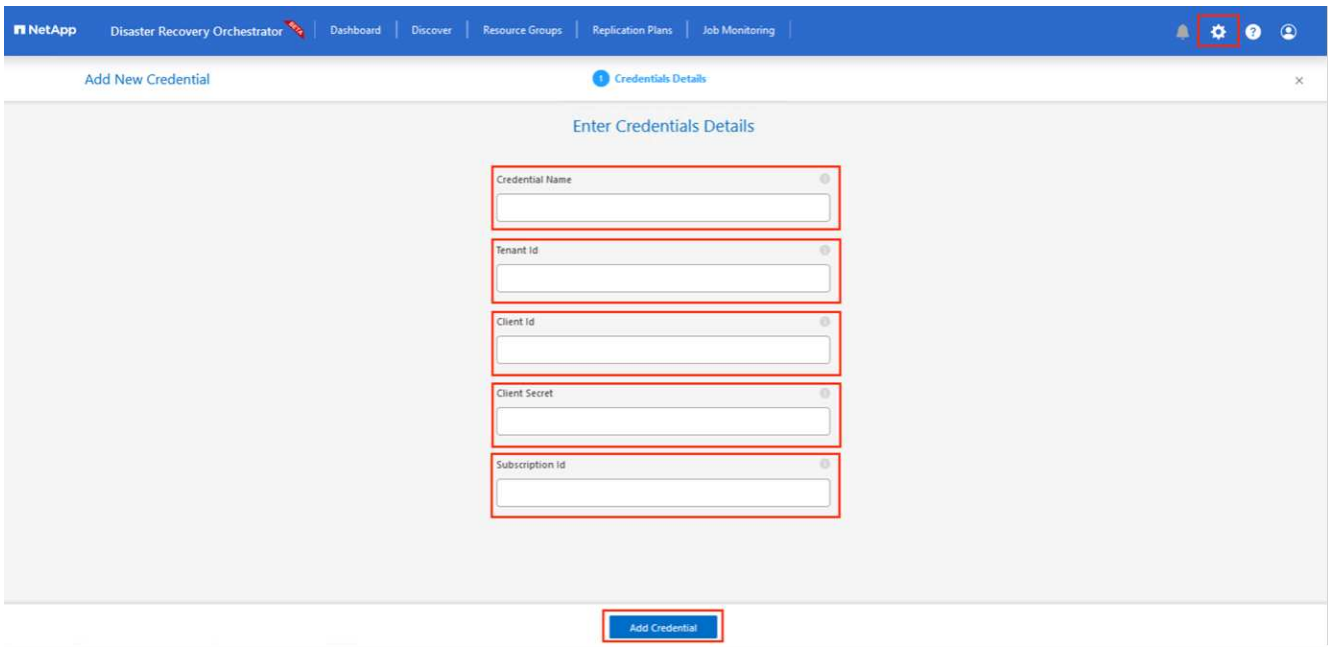
正確設定 Azure NetApp Files 和 AVS 之後、您可以開始設定 DRO 、將工作負載從主要 AVS 站台自動恢復到次要 AVS 站台。NetApp 建議在次要 AVS 站台部署 DRO 代理程式、並設定 ExpressRoute 閘道連線、以便 DRO 代理程式能透過網路與適當的 AVS 和 Azure NetApp Files 元件進行通訊。

第一步是新增認證。DRO 需要權限才能探索 Azure NetApp Files 和 Azure VMware 解決方案。您可以建立和設定 Azure Active Directory （ AD ）應用程式、並取得 DRO 所需的 Azure 認證、將必要的權限授予 Azure 帳戶。您必須將服務主體繫結至 Azure 訂閱、並指派具有相關必要權限的自訂角色。當您新增來源和目的地環境時、系統會提示您選取與服務主體相關的認證。您必須先將這些認證新增至 DRO 、才能按一下新增站台。

若要執行此作業、請完成下列步驟：

1. 在支援的瀏覽器中開啟 DRO 、並使用預設的使用者名稱和密碼 /admin/admin）。您可以使用變更密碼選項、在第一次登入後重設密碼。
2. 在 DRO 主控台的右上角、按一下 * 設定 * 圖示、然後選取 * 認證 * 。
3. 按一下新增認證、然後依照精靈中的步驟進行。
4. 若要定義認證、請輸入有關授與必要權限的 Azure Active Directory 服務主體的資訊：
   - 認證名稱
   - 租戶 ID
   - 用戶端ID
   - 用戶端機密
   - 訂閱 ID

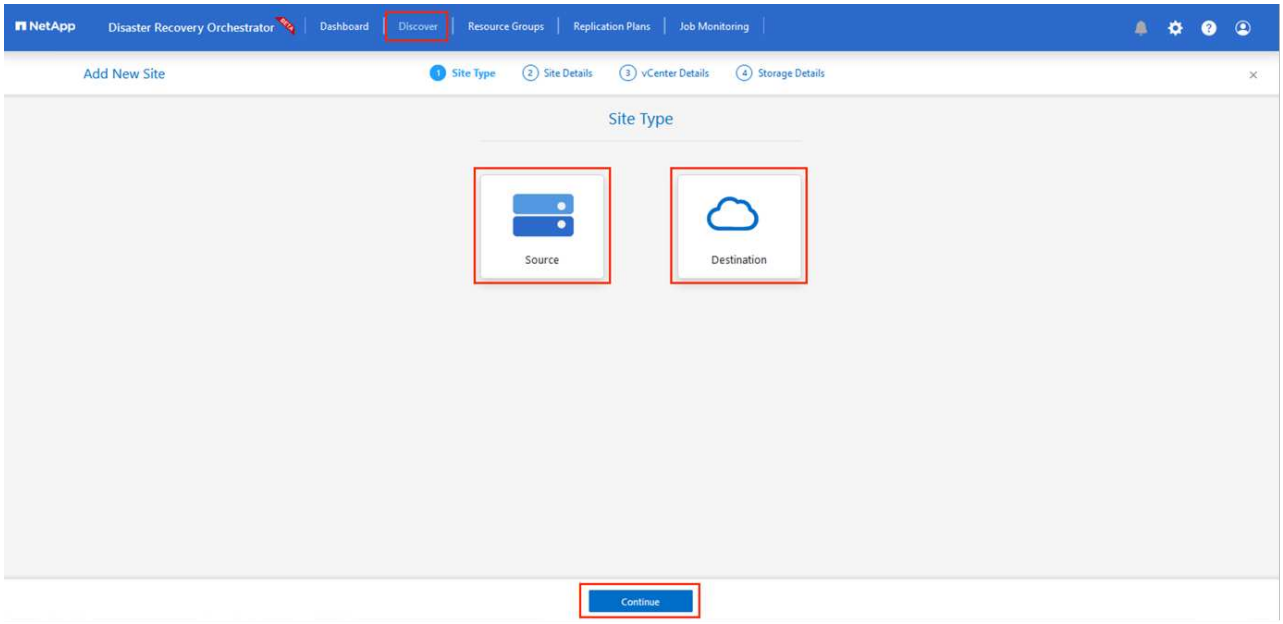
     建立 AD 應用程式時、您應該已擷取此資訊。
5. 確認新認證的詳細資料、然後按一下新增認證。



新增認證之後、現在是探索主要和次要 AVS 站台（ vCenter 和 Azure NetApp Files 儲存帳戶）並將其新增至 DRO 的時候了。若要新增來源和目的地站台、請完成下列步驟：

6. 移至 * 探索 * 標籤。
7. 按一下 * 新增站台 * 。
8. 新增下列主要 AVS 站台（在主控台中指定為 * 來源 * ）。
   - SDDC vCenter
   - Azure NetApp Files 儲存帳戶
9. 新增下列次要 AVS 站台（在主控台中指定為 * 目的地 * ）。

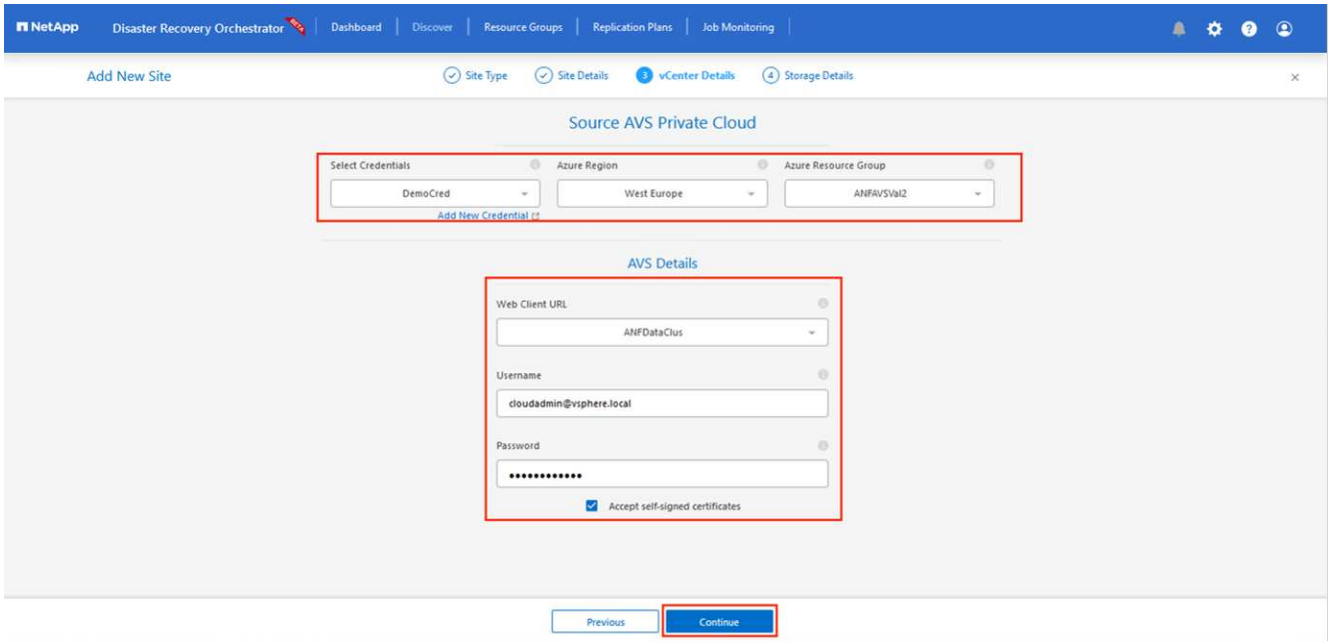
- SDDC vCenter
- Azure NetApp Files 儲存帳戶



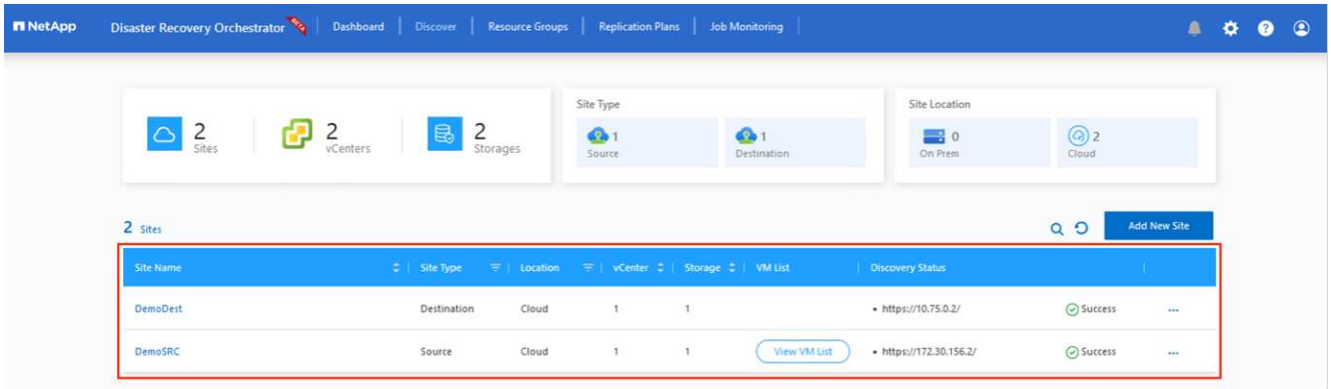
10. 按一下 * 來源 * 、 * 輸入易記的網站名稱、然後選取連接器、即可新增網站詳細資料。然後按一下 * 繼續 * 。

> 為了進行示範、本文件涵蓋新增來源網站。

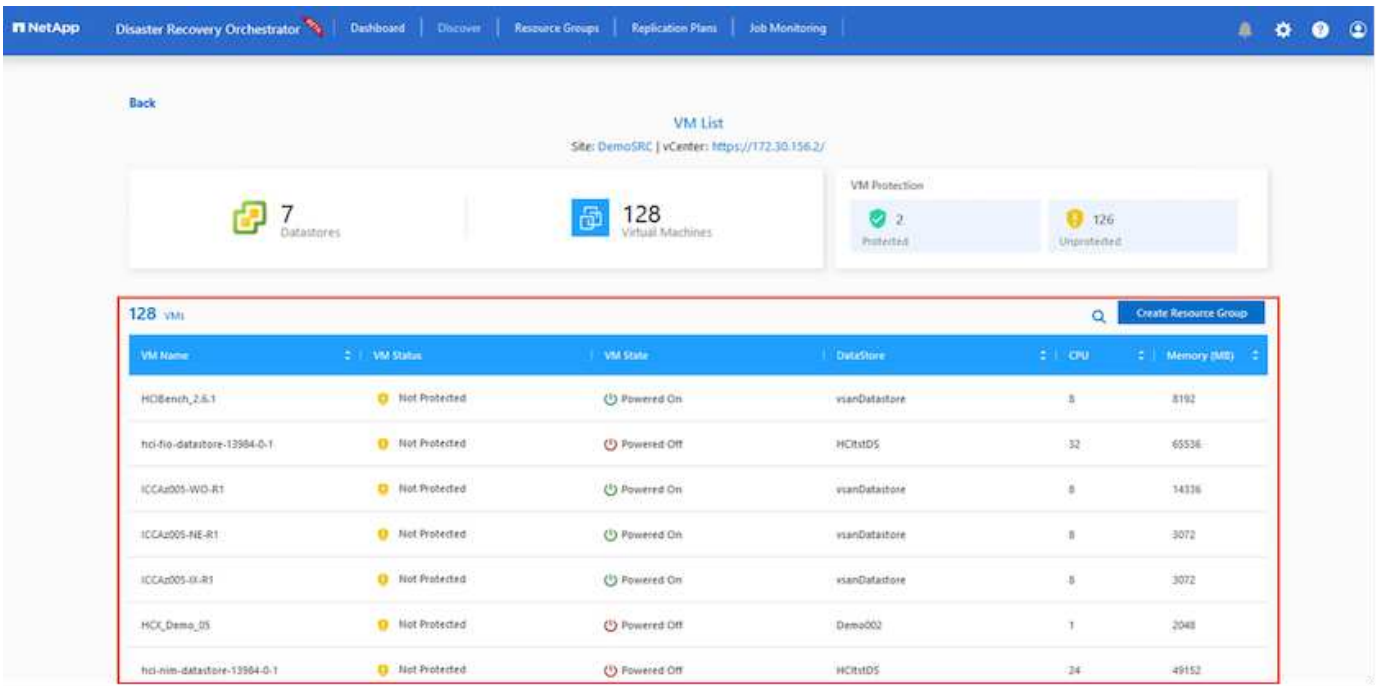
11. 更新 vCenter 詳細資料。若要這麼做、請從主 AVS SDDC 的下拉式清單中選取認證、 Azure 區域和資源群組。
12. DRO 會列出區域內所有可用的 SDDC 。從下拉式清單中選取指定的私有雲 URL 。
13. 輸入 `cloudadmin@vsphere.local` 使用者認證。您可以從 Azure Portal 存取此功能。請遵循本文件中所述的步驟 "連結"。完成後、按一下 * 繼續 * 。



14. 選取 Azure 資源群組和 NetApp 帳戶、以選取來源儲存詳細資料（anf）。
15. 按一下 * 建立站台 * 。



一旦新增、 DRO 會執行自動探索、並顯示從來源站台到目的地站台的具有對應跨區域複本的 VM 。DRO 會自動偵測虛擬機器所使用的網路和區段、並填入這些網路和區段。



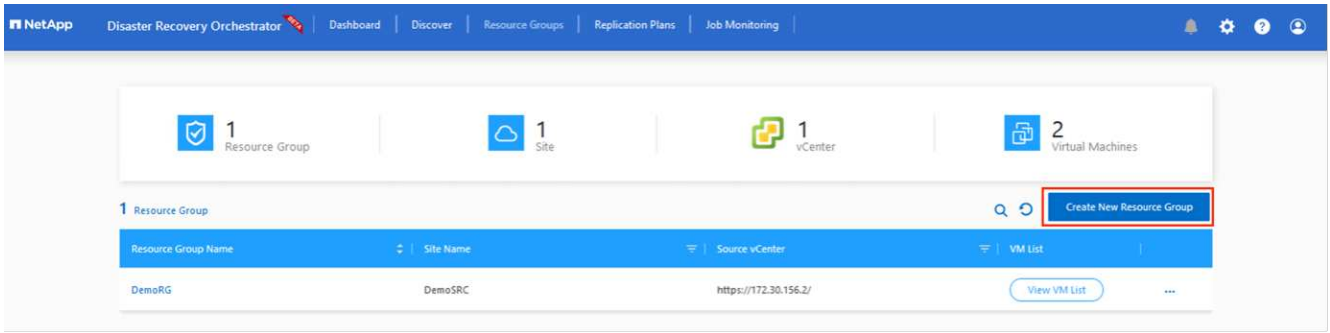
下一步是將所需的虛擬機器分組為其功能群組、做為資源群組。

資源群組

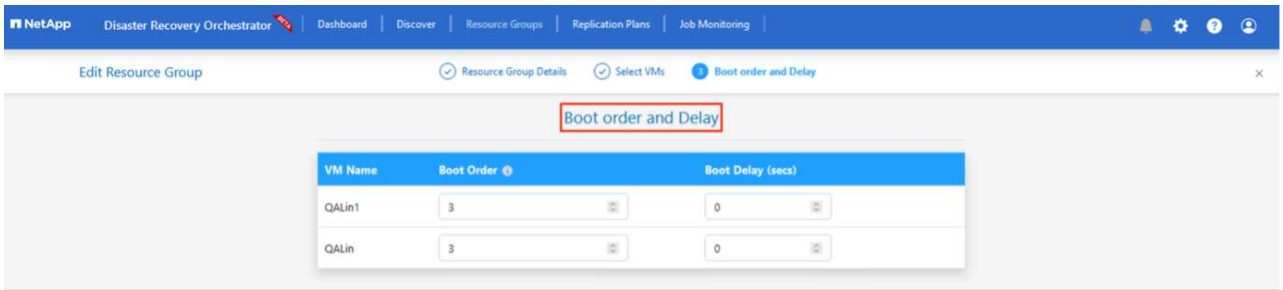
新增平台之後、將您要恢復的虛擬機器分組到資源群組中。DRO資源群組可讓您將一組相依的虛擬機器分組至邏輯群組、其中包含開機順序、開機延遲、以及可在恢復時執行的選用應用程式驗證。

若要開始建立資源群組、請按一下 * 建立新資源群組 * 功能表項目。

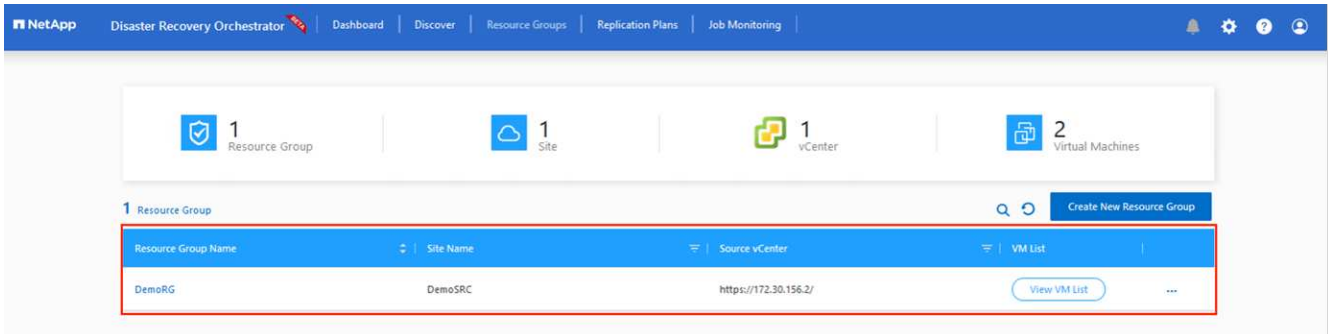
1. 存取 * 資源群組 * 、然後按一下 * 建立新資源群組 * 。



2. 在 [新資源群組] 下，從下拉式清單中選取來源網站，然後按一下 [建立] 。
3. 提供資源群組詳細資料、然後按一下 * 繼續 * 。
4. 使用搜尋選項選取適當的 VM 。
5. 為所有選取的 VM 選取 * 開機順序 * 和 * 開機延遲 * （秒）。選取每個虛擬機器並設定其優先順序、以設定開機順序的順序。所有虛擬機器的預設值為 3 。選項如下：
   - 第一部要開機的虛擬機器
   - 預設
   - 最後一部要開機的虛擬機器



6. 按一下「建立資源群組」。

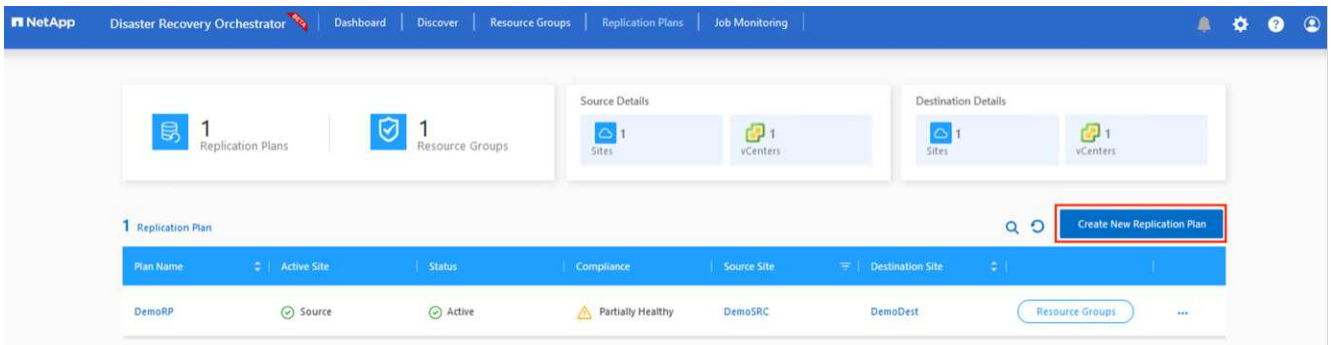


複寫計畫

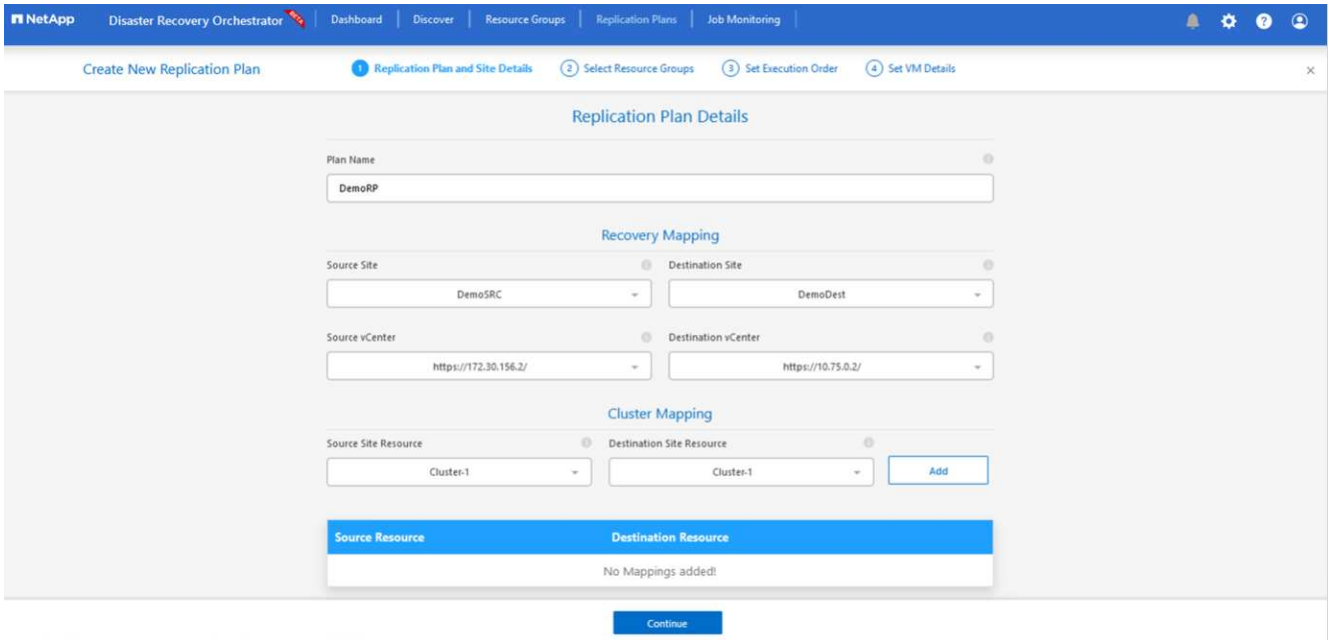
您必須制定計畫、以便在發生災難時恢復應用程式。從下拉式清單中選取來源和目的地 vCenter 平台、選擇要納入此計畫的資源群組、並包含應用程式還原和開機方式的分組（例如、網域控制站、層級 1 、層級 2 等）。計畫通常也稱為藍圖。若要定義恢復計畫、請瀏覽至複寫計畫索引標籤、然後按一下 * 新增複寫計畫 * 。

若要開始建立複寫計畫、請完成下列步驟：

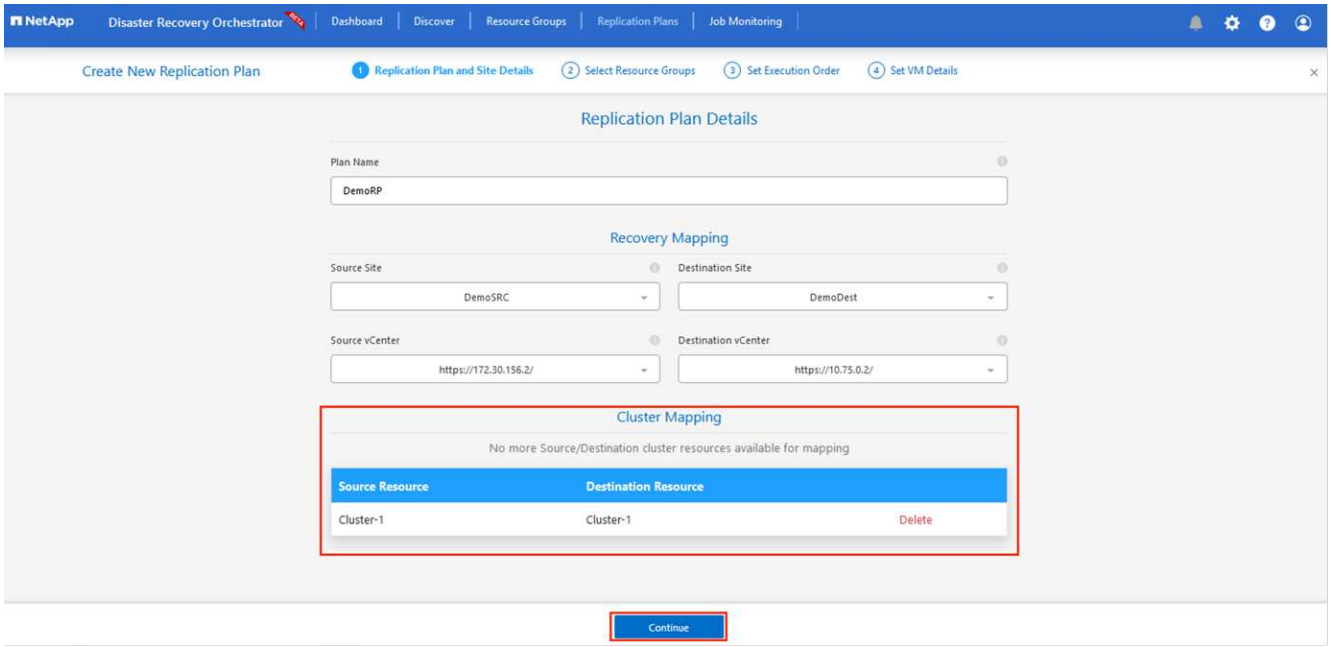
1. 瀏覽至 * 複寫計畫 * 、然後按一下 * 建立新複寫計畫 * 。



2. 在 * 新的複寫計畫 * 上、選取來源站台、相關的 vCenter 、目的地站台及相關的 vCenter 、以提供計畫名稱並新增還原對應。

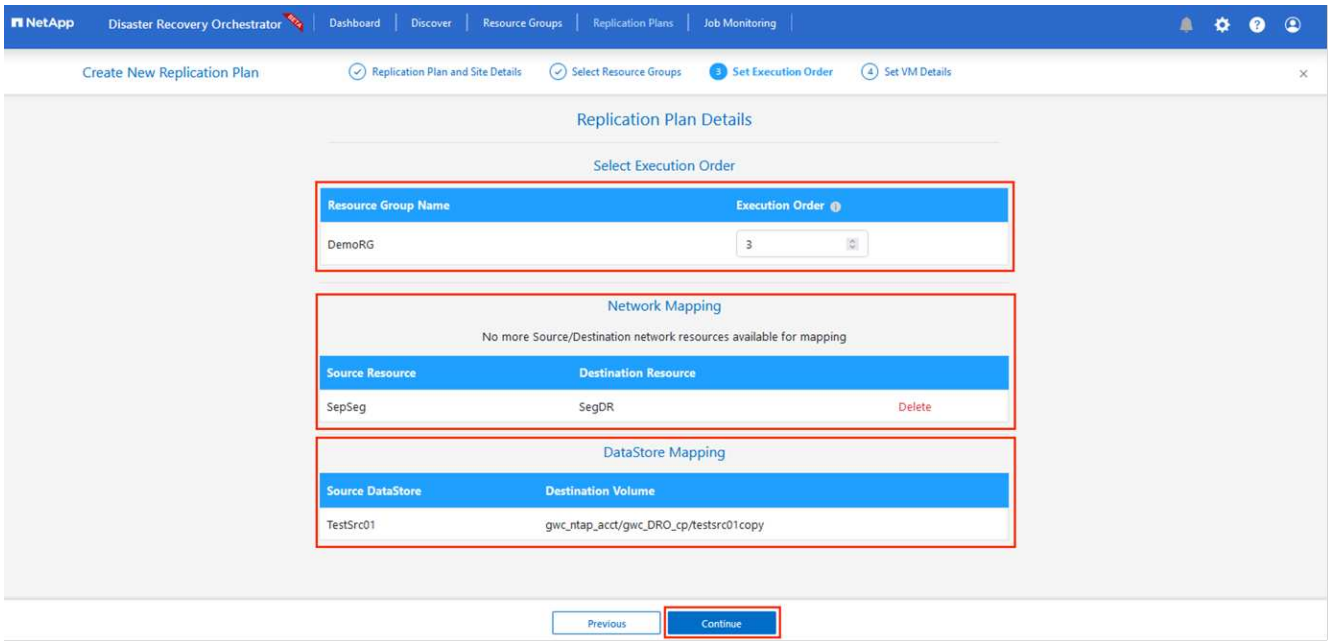


3. 恢復對應完成後、選取 * 叢集對應 * 。



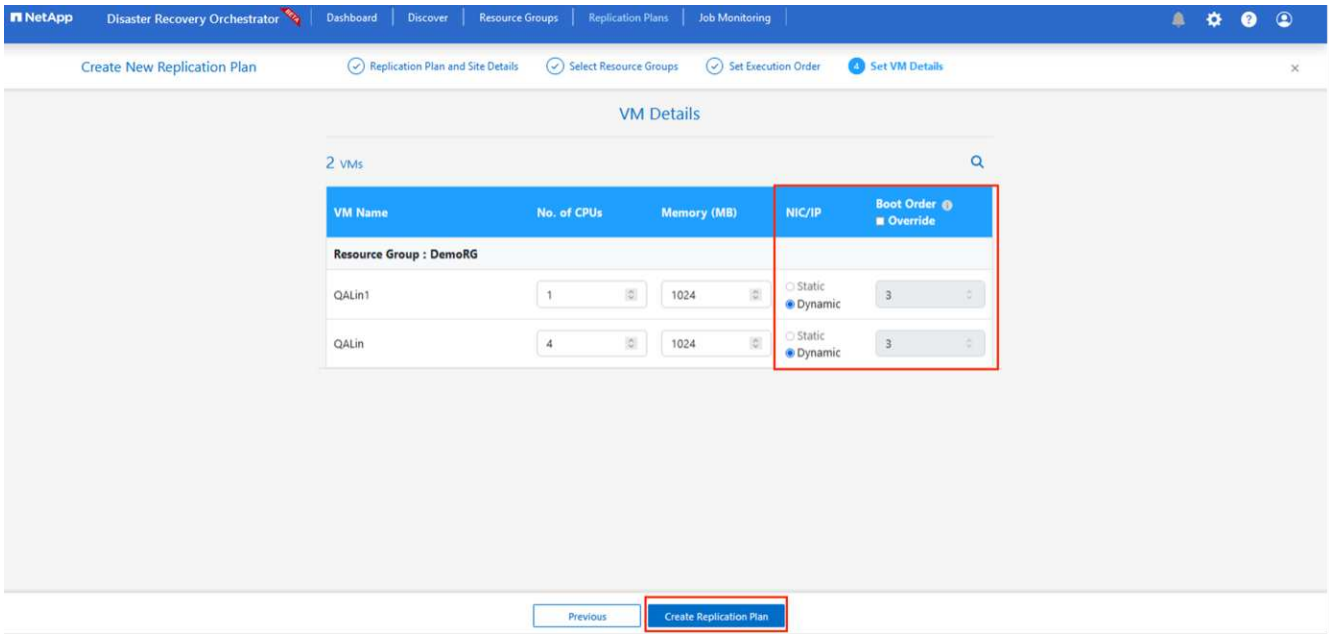
4. 選擇*資源群組詳細資料*、然後按一下*繼續*。
5. 設定資源群組的執行順序。此選項可讓您在存在多個資源群組時、選取作業順序。
6. 完成後、請將網路對應設定為適當的區段。這些區段應已在次要 AVS 叢集上進行佈建、若要將 VM 對應至這些區段、請選取適當的區段。
7. 資料存放區對應會根據虛擬機器的選擇自動選取。

> ⓘ 跨區域複寫（CRR）位於磁碟區層級。因此、位於各自磁碟區上的所有 VM 都會複寫到 CRR 目的地。請務必選取屬於資料存放區一部分的所有 VM 、因為只會處理屬於複寫計畫一部分的虛擬機器。

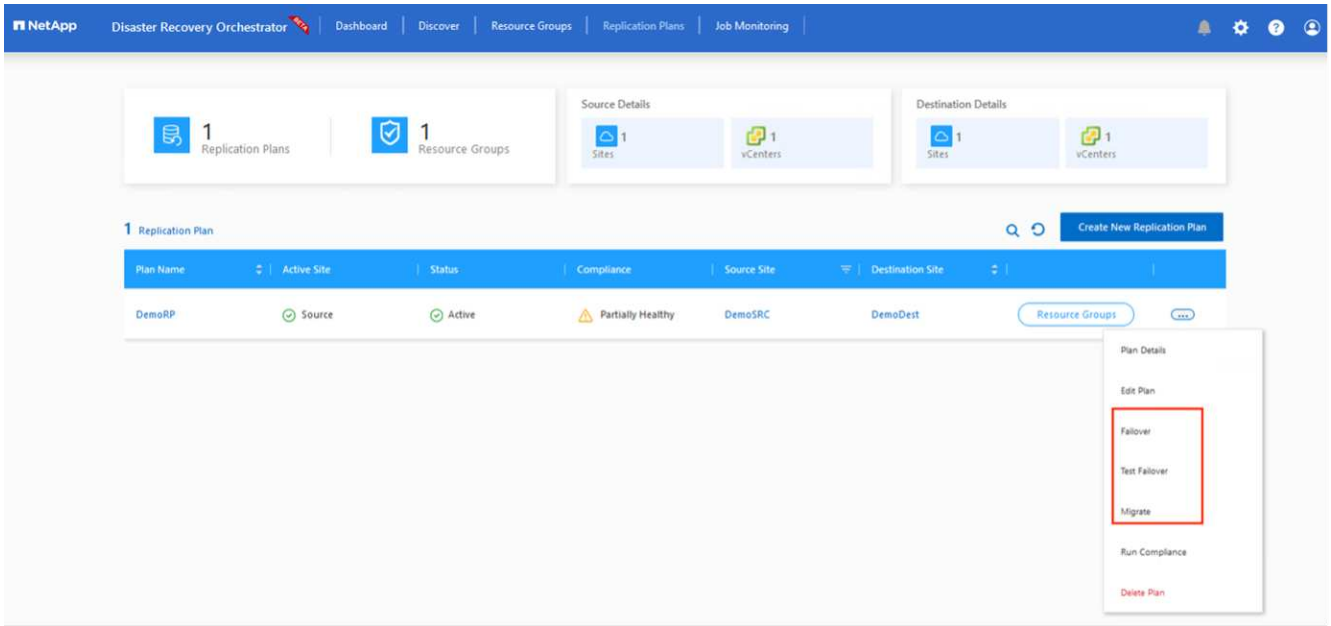


8. 在 VM 詳細資料下、您可以選擇性地調整 VM CPU 和 RAM 參數的大小。當您將大型環境恢復到較小的目標叢集、或是在執行災難恢復測試時、而不需要佈建一對一實體 VMware 基礎架構、這項功能將會非常有幫

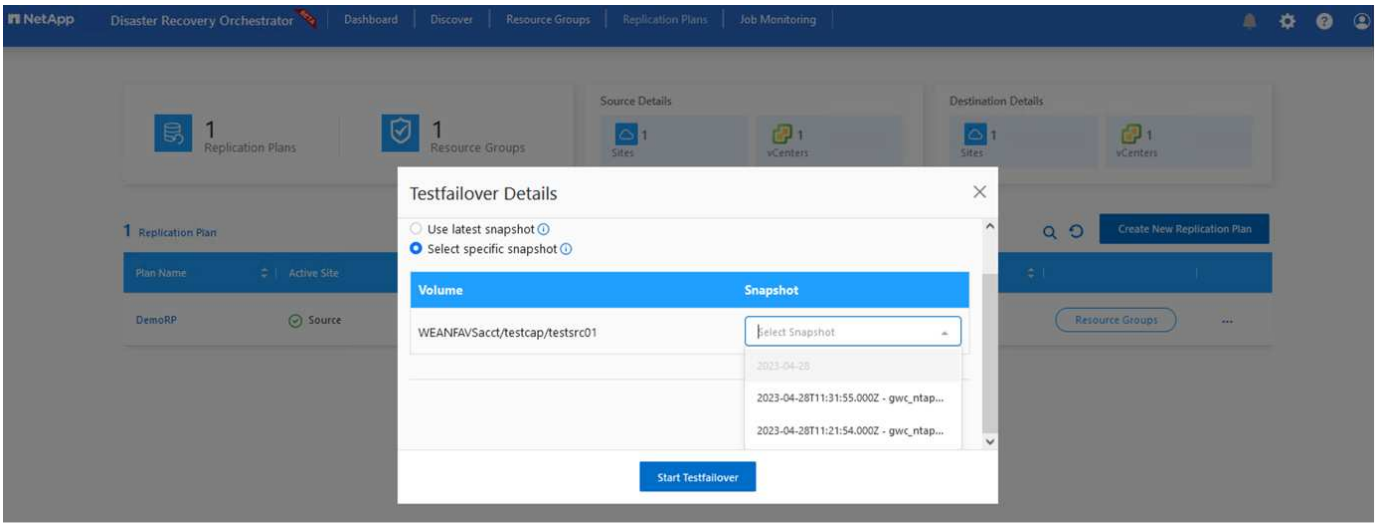
助。此外、也可修改資源群組中所有選定虛擬機器的開機順序和開機延遲（秒）。如果您在資源群組開機順序選擇期間所選取的項目需要任何變更、則還有其他選項可修改開機順序。根據預設、會使用在資源群組選擇期間所選的開機順序、但在此階段可以執行任何修改。



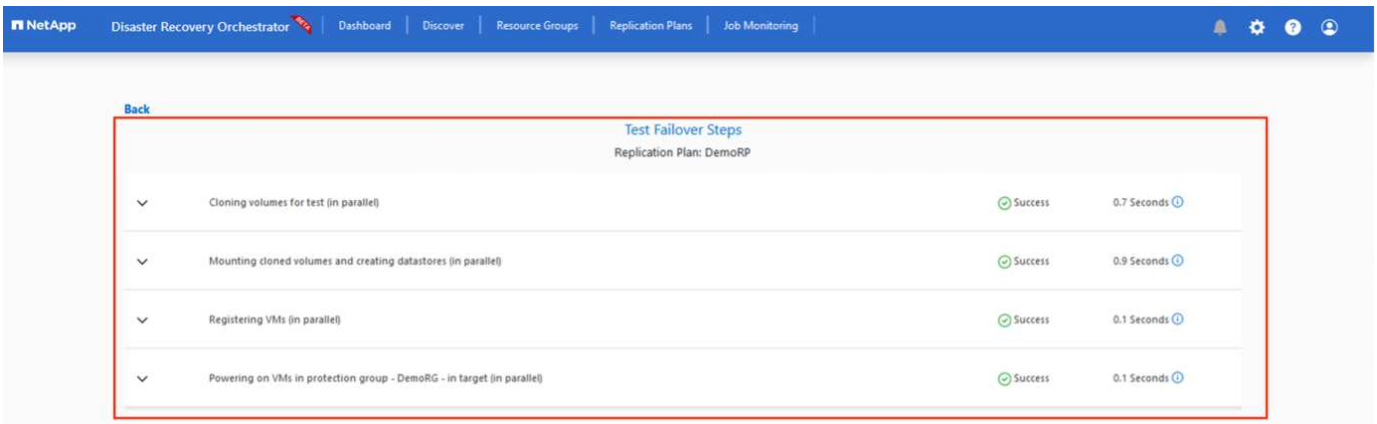
9. 按一下 * 建立複寫計畫 * 。建立複寫計畫之後、您可以根據需求來執行容錯移轉、測試容錯移轉或移轉選項。



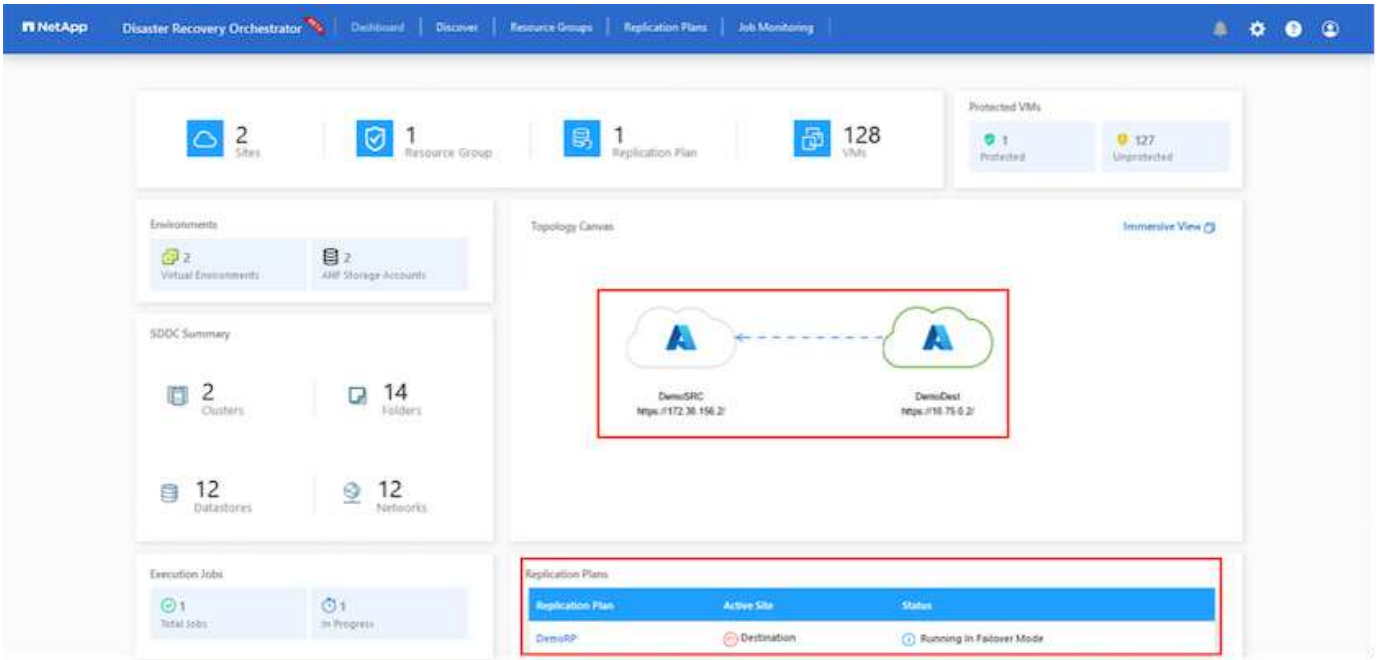
在容錯移轉和測試容錯移轉選項期間、會使用最新的快照、或是從時間點快照中選取特定的快照。如果您面臨勒索軟體等毀損事件、而最近的複本已經遭到入侵或加密、則時間點選項可能非常有用。DRO 會顯示所有可用的時間點。



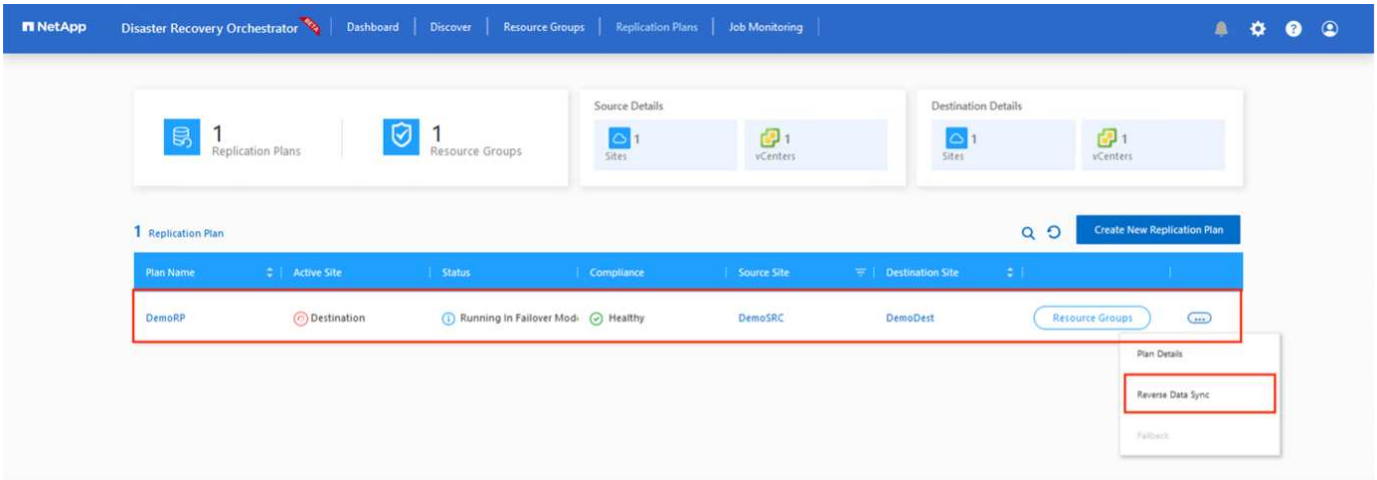
若要使用複寫計畫中指定的組態觸發容錯移轉或測試容錯移轉，您可以按一下 * 容錯移轉 * 或 * 測試容錯移轉 * 。您可以在工作功能表中監控複寫計畫。



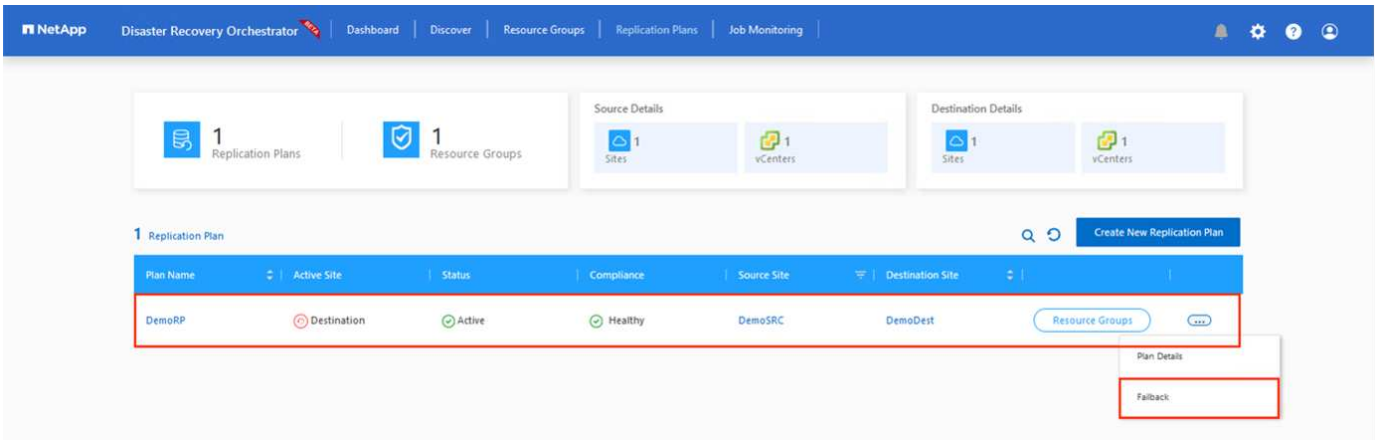
觸發容錯移轉後、可在次要站台 AVS SDDC vCenter （ VM 、網路和資料存放區）中看到復原的項目。依預設、 VM 會還原至 Workload 資料夾。

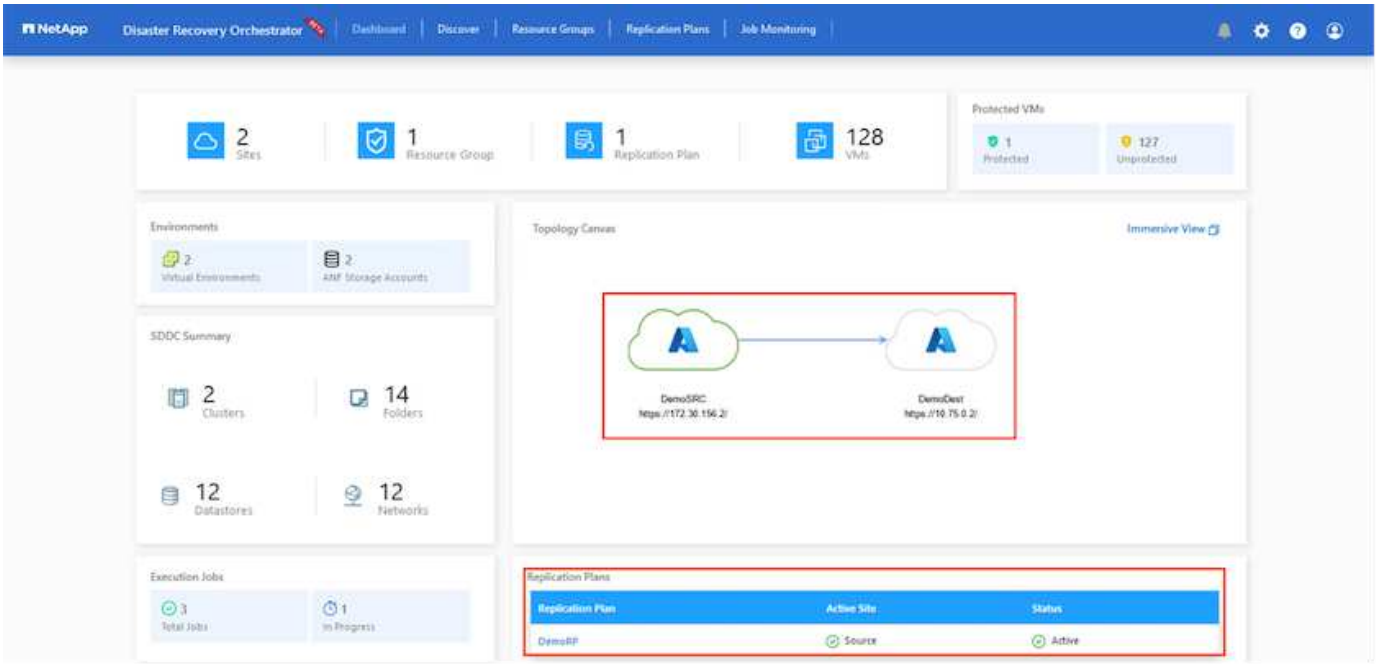


可在複寫計畫層級觸發容錯回復。在測試容錯移轉時、可使用「切紙」選項來回復變更並移除新建立的磁碟區。與容錯移轉相關的容錯回復是兩個步驟的程序。選取複寫計畫、然後選取 * 反轉資料同步 * 。



完成此步驟後、觸發容錯回復、以移回主要 AVS 站台。





從 Azure 入口網站、我們可以看到對應至次要站台 AVS SDDC 的適當磁碟區、其複寫健全狀況已中斷、成為讀取 / 寫入磁碟區。在測試容錯移轉期間、DRO不會對應目的地或複本磁碟區。相反地、它會建立所需跨區域複寫快照的新磁碟區、並將該磁碟區公開為資料存放區、這會消耗容量集區的額外實體容量、並確保來源磁碟區不會遭到修改。值得注意的是、複寫工作可在災難恢復測試或分類工作流程期間繼續進行。此外、此程序可確保在發生錯誤或恢復毀損的資料時、能夠清除恢復作業、而不會有銷毀複本的風險。

勒索軟體恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體而言、 IT 組織可能很難找出安全的回報點、一旦確定、如何確保恢復的工作負載受到保護、免受重複發生的攻擊（例如、睡眠惡意軟體或易受攻擊的應用程式）。

DRO 可讓組織從任何可用的時間點恢復、藉此解決這些疑慮。然後工作負載會恢復至功能正常且隔離的網路、以便應用程式能夠彼此運作並進行通訊、但不會暴露於任何南北流量中。此程序可讓安全團隊安全地進行鑑識、並識別任何隱藏或睡眠中的惡意軟體。

結論

Azure NetApp Files 與 Azure VMware 災難恢復解決方案提供下列優點：

- 運用高效且靈活的 Azure NetApp Files 跨區域複寫功能。
- 利用快照保留功能、恢復到任何可用的時間點。
- 完全自動化所有必要步驟、從儲存、運算、網路和應用程式驗證步驟中恢復數百至數千個 VM 。
- 工作負載恢復採用「從最近的快照建立新磁碟區」程序、不會操控複寫的磁碟區。
- 避免磁碟區或快照上的資料毀損風險。
- 避免災難恢復測試工作流程中的複寫中斷。
- 利用災難恢復資料和雲端運算資源來執行災難恢復以外的工作流程、例如開發 / 測試、安全測試、修補程式和升級測試、以及補救測試。
- CPU 和 RAM 最佳化可讓您恢復至較小的運算叢集、進而降低雲端成本。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- 為 Azure NetApp Files 建立 Volume 複寫

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Azure NetApp Files 磁碟區的跨區域複寫

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Azure VMware解決方案"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- 在Azure上部署及設定虛擬化環境

  "https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html"

- 部署及設定 Azure VMware 解決方案

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

使用 Veeam Replication 和 Azure NetApp Files 資料存放區、將災難恢復至 Azure VMware 解決方案

作者： Niyaz Mohamed - NetApp 解決方案工程

總覽

Azure NetApp Files （ anf ）資料存放區可將儲存設備與運算分離、並釋放任何組織將工作負載移轉至雲端所需的靈活度。它為客戶提供靈活、高效能的儲存基礎架構、可在運算資源之外進行擴充。Azure NetApp Files 資料存放區可簡化並最佳化部署、並將 Azure VMware 解決方案（ AVS ）作為內部部署 VMware 環境的災難恢復站台。

Azure NetApp Files （ anf） Volume 型 NFS 資料存放區可用於從內部部署複寫資料、使用任何可提供 VM 複寫功能的驗證協力廠商解決方案。透過新增 Azure NetApp Files 資料存放區、相較於使用大量 ESXi 主機來建置 Azure VMware 解決方案 SDDC 來容納儲存設備、它將可實現成本最佳化的部署。這種方法稱為「試驗燈叢集」。試驗性光叢集是一種最低的 AVS 主機組態（ 3 個 AVS 節點）、以及 Azure NetApp Files 資料存放區容量。

其目標是維持低成本的基礎架構、讓所有核心元件都能處理容錯移轉。如果發生容錯移轉、先導光叢集可以橫向擴充並配置更多 AVS 主機。當容錯移轉完成且正常作業恢復後、試驗性光叢集即可向下擴充至低成本作業模式。

本文檔的用途

本文說明如何搭配 Veeam 備份和複寫使用 Azure NetApp Files 資料存放區、以使用 Veeam VM 複寫軟體功能、為內部部署的 VMware VM 設定災難恢復（ AVS ）。

Veeam 備份與複寫是適用於虛擬環境的備份與複寫應用程式。複寫虛擬機器時、 Veeam 備份與複寫會從 AVS 複寫、軟體會在目標 AVS SDDC 叢集上以原生 VMware vSphere 格式建立 VM 的精確複本。 Veeam 備份與複寫會將複本與原始 VM 保持同步。複寫可提供最佳的恢復時間目標（RTO）、因為災難恢復站台上有已掛載的 VM 複本處於就緒啟動狀態。

這種複寫機制可確保工作負載在發生災難事件時、能在 AVS SDDC 中快速啟動。Veeam 備份與複寫軟體也能最佳化流量傳輸、以便透過 WAN 進行複寫、並降低連線速度。此外、它也會篩選出重複的資料區塊、零資料區塊、交換檔案和「排除的 VM 來賓作業系統檔案」。軟體也會壓縮複本流量。為了避免複寫工作佔用整個網路頻寬、可使用 WAN 加速器和網路節流規則。

Veeam Backup & Replication 中的複寫程序是由工作所驅動、這表示複寫是透過設定複寫工作來執行。發生災難事件時、可觸發容錯移轉、藉由容錯移轉至複本來恢復 VM 。執行容錯移轉時、複寫的 VM 會接管原始 VM 的角色。容錯移轉可以執行至複本的最新狀態、或是任何已知的還原點。如此一來、就能視需要進行勒索軟體恢復或隔離測試。Veeam 備份與複寫提供多種選項來處理不同的災難恢復案例。

[]

解決方案部署

高階步驟

1. Veeam 備份與複寫軟體是在內部環境中執行、並具備適當的網路連線能力。
2. "部署 Azure VMware 解決方案（AVS）" 私有雲和 "附加 Azure NetApp Files 資料存放區" 至 Azure VMware 解決方案主機。

   以最小組態設定的試驗環境可用於災難恢復。發生事件時、 VM 會容錯移轉至此叢集、並可新增其他節點）。

3. 設定複寫工作、以使用 Veeam 備份與複寫建立 VM 複本。
4. 建立容錯移轉計畫並執行容錯移轉。
5. 災難事件完成且主站台正常運作後、切換回正式作業的 VM 。

Veeam VM 複寫至 **AVS** 和 **anf** 資料存放區的先決條件

1. 確保 Veeam 備份與複寫備份 VM 已連線至來源叢集和目標 AVS SDDC 叢集。
2. 備份伺服器必須能夠解析簡短名稱、並連線至來源和目標 vCenter 。
3. 目標 Azure NetApp Files 資料存放區必須有足夠的可用空間來儲存複寫 VM 的 VMDK 。

如需其他資訊、請參閱涵蓋的「考量與限制」 "請按這裡"。

部署詳細資料

步驟 **1** ：複寫 **VM**

Veeam 備份與複寫利用 VMware vSphere 快照功能 / 在複寫期間、 Veeam 備份與複寫要求 VMware vSphere 建立 VM 快照。VM 快照是 VM 的時間點複本、其中包含虛擬磁碟、系統狀態、組態和中繼資料。Veeam 備份與複寫會使用快照做為複寫資料來源。

若要複寫 VM 、請依照下列步驟進行：

1. 開啟 Veeam 備份與複寫主控台。
2. 在主畫面上。在工作節點上按一下滑鼠右鍵、然後選取複寫工作 > 虛擬機器。
3. 指定工作名稱並選取適當的進階控制核取方塊。按一下「下一步」
   - 如果內部部署與 Azure 之間的連線頻寬有限、請選取複本植入核取方塊。
     - 如果 Azure VMware 解決方案 SDDC 上的區段與內部部署站台網路不相符、請選取「網路重新對應（適用於具有不同網路的 AVS SDDC 站台）」核取方塊。
   - 如果內部生產站台的 IP 定址方案與目標 AVS 站台的配置不同、請選取複本重新 IP （適用於具有不同 IP 定址方案的 DR 站台）核取方塊。

     []
4. 在「 * 虛擬 * 機器 * 」步驟中、選取要複寫到連接至 Azure VMware 解決方案 SDDC 的 Azure NetApp Files 資料存放區的虛擬機器。虛擬機器可放置在 vSAN 上、以填滿可用的 vSAN 資料存放區容量。在試驗性光叢集中、 3 節點叢集的可用容量將會受到限制。其餘資料可輕鬆置於 Azure NetApp Files 資料存放區、以便恢復 VM 、並可擴充叢集以符合 CPU/ 記憶體需求。按一下 * 新增 * 、然後在 * 新增物件 * 視窗中選取必要的 VM 或 VM 容器、然後按一下 * 新增 * 。單擊 * 下一步 * 。

   []
5. 之後、請將目的地選取為 Azure VMware 解決方案 SDDC 叢集 / 主機、以及適當的資源集區、 VM 資料夾、以及適用於 VM 複本的 ONTAP 資料存放區的 FSX 。然後單擊*下一步*。

   []
6. 在下一個步驟中、視需要在來源和目的地虛擬網路之間建立對應。

   []
7. 在 * 工作設定 * 步驟中、指定將儲存 VM 複本中繼資料、保留原則等的備份儲存庫。
8. 在 **Data Transfer** 步驟中更新 **Source** 和 **Target** 代理服務器，並保留 **Automatic** 選擇（默認）並保持 **Direct** 選項，然後單擊 **Next** （下一步）。
9. 在 * 來賓處理 * 步驟中、視需要選取 * 啟用應用程式感知處理 * 選項。單擊 * 下一步 * 。

   []
10. 選擇複寫排程以定期執行複寫工作。

    []
11. 在精靈的 * 摘要 * 步驟中、檢閱複寫工作的詳細資料。若要在精靈關閉後立即啟動工作、請選取 * 按一下「完成」時執行工作 * 核取方塊、否則請取消選取核取方塊。然後按一下 * 完成 * 以關閉精靈。

[]

複寫工作啟動後、會在目的地 AVS SDDC 叢集 / 主機上填入具有指定尾碼的 VM 。

[]

如需 Veeam 複寫的其他資訊、請參閱 "複寫的運作方式"

步驟 **2** ：建立容錯移轉計畫

當初始複寫或植入完成時、請建立容錯移轉計畫。容錯移轉計畫有助於自動逐一或以群組的方式、為相關的 VM 執行容錯移轉。容錯移轉計畫是 VM 處理順序的藍圖、包括開機延遲。容錯移轉計畫也有助於確保關鍵相依的 VM 已經在執行中。

若要建立計畫、請瀏覽至新的子區段 * 複本 * 、然後選取 * 容錯移轉計畫 * 。選擇適當的 VM 。Veeam 備份與複寫會尋找最接近此時間點的還原點、並使用它們來啟動 VM 複本。

> 只有在初始複寫完成且 VM 複本處於就緒狀態時、才能新增容錯移轉計畫。

> 執行容錯移轉計畫時可同時啟動的虛擬機器數量上限為 10 個

> 在容錯移轉過程中、來源 VM 將不會關閉

若要建立 * 容錯移轉計畫 * 、請執行下列步驟：

1. 在主畫面上。在複本節點上按一下滑鼠右鍵、然後選取容錯移轉計畫 > 容錯移轉計畫 > VMware vSphere 。

   []

2. 接著提供計畫的名稱和說明。可視需要新增容錯移轉前後指令碼。例如、在啟動複寫的虛擬機器之前、請先執行指令碼來關閉虛擬機器。

   []

3. 將 VM 新增至計畫、並修改 VM 開機順序和開機延遲、以符合應用程式相依性。

   []

如需建立複寫工作的其他資訊、請參閱 "建立複寫工作"。

步驟 **3** ：執行容錯移轉計畫

在容錯移轉期間、正式作業站台中的來源 VM 會切換至災難恢復站台上的複本。在容錯移轉程序中、Veeam 備份與複寫會將 VM 複本還原至所需的還原點、並將所有 I/O 活動從來源 VM 移至複本。複本不僅可在發生災難時使用、也可用於模擬災難恢復訓練。在容錯移轉模擬期間、來源 VM 仍在執行中。完成所有必要的測試後、即可復原容錯移轉並恢復正常作業。

> 請確定已建立網路區段、以避免容錯移轉期間發生 IP 衝突。

若要開始進行容錯移轉計畫、只要按一下 * 容錯移轉計畫 * 索引標籤、然後在容錯移轉計畫上按一下滑鼠右鍵即可。選擇 ** 開始 * 。這會使用最新的 VM 複本還原點進行容錯移轉。若要容錯移轉至虛擬機器複本的特定還原點、請選取 * 開始至 * 。

[]

[]

VM 複本的狀態會從「 Ready （就緒）」變更為「 Failover （容錯移轉）」、而 VM 會從目的地 Azure VMware Solution （ AVS） SDDC 叢集 / 主機啟動。

[]

容錯移轉完成後、 VM 的狀態會變更為「容錯移轉」。

[]

> Veeam 備份與複寫會停止來源 VM 的所有複寫活動、直到其複本回到「就緒」狀態為止。

如需容錯移轉計畫的詳細資訊、請參閱 "容錯移轉計畫"。

步驟 **4** ：容錯回復至正式作業網站

當容錯移轉計畫執行時、它會被視為中間步驟、需要根據需求完成。選項包括：

- * 容錯回復至正式作業 * ：切換回原始 VM 、並將 VM 複本執行時發生的所有變更傳輸至原始 VM 。

> 當您執行容錯回復時、變更只會傳輸但不會發佈。選擇 * 提交容錯回復 * （一旦原始 VM 確認正常運作）或復原容錯回復、以在原始 VM 未如預期運作時返回 VM 複本。

- * 復原容錯移轉 * ：切換回原始 VM 、並在 VM 複本執行時捨棄對其所做的所有變更。
- * 永久容錯移轉 * ：從原始 VM 永久切換至 VM 複本、並將此複本作為原始 VM 使用。

在本示範中、選擇了「容錯回復至正式作業」。在精靈的「目的地」步驟中選取容錯回復至原始 VM 、並啟用「還原後開啟 VM 」核取方塊。

[]

[]

[]

[]

容錯回復認可是完成容錯回復作業的方法之一。提交容錯回復時、會確認傳送至容錯回復的 VM （正式作業 VM ）所做的變更、均如預期運作。提交作業完成後、 Veeam 備份與複寫會恢復正式作業 VM 的複寫活動。

如需容錯回復程序的詳細資訊、請參閱的 Veeam 文件 "容錯移轉和容錯回復以進行複寫"。

[]

在容錯回復至正式作業後、虛擬機器都會還原回原始正式作業站台。

[]

結論

Azure NetApp Files 資料存放區功能可讓 Veeam 或任何經過驗證的協力廠商工具、利用 Pilot Light 叢集來提供低成本的災難恢復解決方案、而非只為了容納 VM 複本而站在大型叢集上。這可有效處理量身打造的自訂災難恢復計畫、並可重複使用內部現有的備份產品進行災難恢復、透過結束內部部署的災難恢復資料中心來實現雲端型災難恢復。在發生災難時按一下按鈕即可進行容錯移轉、或在發生災難時自動進行容錯移轉。

若要深入瞭解此程序、歡迎觀看詳細的逐步解說影片。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278