NetApp公有雲與混合雲解決方案

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

目錄

NetApp公有雲與混合雲解決方案 1
NetApp公有雲和混合雲解決方案的新功能 2
NetApp混合多雲與 VMware 解決方案 3
VMware 的公有雲 3
NetApp與 VMware 的混合多雲概述 3
針對超大規模企業 VMware 的NetApp解決方案 6
NetApp混合多雲與 VMware 支援的配置 9
超大規模配置中的 VMware 9
公有雲中的NetApp存儲 33
總結與結論： NetApp為何選擇 VMware 作為混合多雲平台 128
VMware 混合雲端用例 129
NetApp與 VMware 混合多雲的用例 129
針對超大規模企業 VMware 的NetApp解決方案 130
適用於 Amazon VMware 託管雲端 (VMC) 的NetApp解決方案 131
適用於 Azure VMware 解決方案 (AVS) 的NetApp解決方案 131
適用於 Google Cloud VMware Engine (GCVE) 的NetApp解決方案 132
適用於 AWS/VMC 的NetApp 132
NetApp的 AWS VMC 功能 132
保護 AWS/VMC 上的工作負載 133
在 AWS/VMC 上遷移工作負載 243
適用於 AWS/EVS 的NetApp 256
將 FSx ONTAP掛載為 EVS 的外部資料存儲 256
保護 FSx ONTAP 資料存放區以用於 EVS 280
NetApp適用於 Azure/AVS 313
NetApp的 Azure AVS 功能 314
保護 Azure/AVS 上的工作負載 315
在 Azure/AVS 上遷移工作負載 379
NetApp適用於 GCP/GCVE 392
NetApp針對 Google Cloud Platform GCVE 的功能 392
保護 GCP/GCVE 上的工作負載 393
遷移 GCP/GCVE 上的工作負載 424
使用Google Cloud NetApp Volumes保護 Google Cloud 中的數據 441
NetApp Disaster Recovery 499
適用於 VMware 的 3-2-1 資料保護，搭配 SnapCenter 外掛程式與 NetApp Backup and Recovery，以保護 VMware 工作負載 499
NetApp Disaster Recovery 532
NetApp混合多雲與 Red Hat OpenShift 容器工作負載 572
開始 572
適用於 Red Hat OpenShift 容器工作負載的NetApp混合多雲解決方案 572

NetApp混合多雲解決方案針對 Red Hat OpenShift 容器工作負載的價值主張 574
NetApp混合多雲支援 Red Hat OpenShift 容器工作負載的解決方案 574
解決方案驗證中使用的各種組件的版本 578
支援NetApp Storage 與 Red Hat OpenShift Containers 的集成 579
其他文檔 583
Openshift 適用於本地 583
NetApp解決方案與 VMware 上的 Red Hat OpenShift Container 平台工作負載 583
在 VMware 上部署並設定 Red Hat OpenShift Container 平台 584
使用Trident Protect 進行資料保護 586
具有自管理元件的混合雲 587
NetApp解決方案與混合雲中的 Red Hat OpenShift 容器平台工作負載 587
在 AWS 上部署和設定 Red Hat OpenShift Container 平台 589
在 Google Cloud 上部署和設定 Red Hat OpenShift 容器平台 591
在 Azure 上部署並設定 Red Hat OpenShift 容器平台 593
使用Trident Protect 進行資料保護 595
具有提供者管理元件的混合雲 595
具有託管 Red Hat OpenShift 容器平台工作負載的NetApp解決方案 595
在 AWS 上部署和設定託管 Red Hat OpenShift 容器平台 596
使用Google Cloud NetApp Volumes在 Google Cloud 上部署和設定 OpenShift Dedicated 598
資料保護 600
適用於 Red Hat OpenShift 工作負載的其他NetApp混合多雲解決方案 600
使用Trident Protect 保護數據 601
使用 Trident Protect 為 OpenShift Container Platform 中的 Container Apps 提供資料保護 601
使用 Trident Protect 保護 Red Hat OpenShift Virtualization 中的虛擬機 612
使用第三方工具保護容器應用 633
使用 OpenShift API for Data Protection (OADP) 為 OpenShift Container Platform 中的容器應用程式提供資料保護 633
OpenShift API for Data Protection (OADP) Operator 的安裝 634
在 OpenShift Container Platform 中為應用程式建立按需備份 643
將應用程式從一個集群遷移到另一個集群 645
從備份還原應用程式 650
使用 Velero 刪除備份和恢復 656
觀看有關NetApp混合多雲解決方案的影片和演示 658
觀看有關使用NetApp的 Amazon Web Services 混合多雲解決方案的視頻 658
來賓連接存儲 658
TCO 和補充資料存儲 658
遷移工作流程 (HCX) 658
觀看有關使用NetApp的 Azure VMware 雲端的混合多雲解決方案的視頻 658
補充資料存儲 658
災難復原 658
遷移工作流程 (HCX) 658

觀看有關NetApp的 Red Hat OpenShift 混合多雲解決方案的視頻 . . . 659
快照和恢復 . . . 659
儲存集成 . . . 659
故障轉移和故障恢復 . . . 659
解決方案自動化 . . . 659
閱讀NetApp專家的雲端解決方案博客 . . . 660
VMware 與 AWS 和Amazon FSx for ONTAP 的集成 . . . 660
Azure VMware 解決方案 . . . 660
Google Cloud VMware 引擎 . . . 660
資料保護和管理 . . . 660
NetApp適用於 OpenShift 容器工作負載 . . . 660
VMware 主權雲 . . . 660
法律聲明 . . . 661
版權 . . . 661
商標 . . . 661
專利 . . . 661
隱私權政策 . . . 661

NetApp公有雲與混合雲解決方案

NetApp公有雲和混合雲解決方案的新功能

了解公有和混合雲解決方案的新功能。

[[18-august-2025]]
== 2025年8月18日

NetApp解決方案網站現在是"NetApp解決方案系列"，其中包括以下網站：

- "NetApp人工智慧解決方案"
- "NetApp容器解決方案"
- "NetApp資料管理解決方案"
- "NetApp資料庫解決方案"
- NetApp公有雲與混合雲解決方案
- "適用於 SAP 的NetApp解決方案"
- "NetApp虛擬化解決方案"

NetApp混合多雲與 VMware 解決方案

VMware 的公有雲

NetApp與 VMware 的混合多雲概述

大多數 IT 組織都遵循混合雲優先方法。這些組織正處於轉型階段，客戶正在評估其當前的 IT 環境，然後根據評估和發現練習將其工作負載遷移到雲端。

客戶遷移到雲端的因素可能包括彈性和爆發、資料中心退出、資料中心整合、生命週期終止場景、合併、收購等。遷移的原因可能因每個組織及其各自的業務優先順序而異。當遷移到混合雲時，選擇正確的雲端儲存對於釋放雲端部署和彈性的威力非常重要。

公有雲中的 VMware Cloud 選項

本節介紹每個雲端供應商如何在各自的公有雲產品中支援 VMware 軟體定義資料中心 (SDDC) 和/或 VMware Cloud Foundation (VCF) 堆疊。

Azure VMware 解決方案

Azure VMware 解決方案是一種混合雲端服務，可在 Microsoft Azure 公有雲中完全執行 VMware SDDC。Azure VMware 解決方案是完全由 Microsoft 管理和支援的第一方解決方案，並由 VMware 利用 Azure 基礎架構進行了驗證。這意味著，當部署 Azure VMware 解決方案時，客戶可以獲得 VMware 的 ESXi 用於計算虛擬化、vSAN 用於超融合儲存以及 NSX 用於網路和安全，同時利用 Microsoft Azure 的全球影響力、一流的資料中心設施以及靠近豐富的原生 Azure 服務和解決方案生態系統的優勢。

AWS 上的 VMware Cloud

VMware Cloud on AWS 將 VMware 的企業級 SDDC 軟體引入 AWS 雲，並優化了對原生 AWS 服務的存取。VMware Cloud on AWS 由 VMware Cloud Foundation 提供支持，整合了 VMware 的運算、儲存和網路虛擬化產品（VMware vSphere、VMware vSAN 和 VMware NSX）以及 VMware vCenter Server 管理，並針對專用、彈性、裸機 AWS 基礎架構上運行進行了最佳化。

Google Cloud VMware 引擎

Google Cloud VMware Engine 是一款基礎架構即服務 (IaaS) 產品，它是基於 Google Cloud 高效能可擴充基礎架構和 VMware Cloud Foundation 堆疊（VMware vSphere、vCenter、vSAN 和 NSX-T）建構。此服務可快速遷移至雲端，將現有 VMware 工作負載從本地環境無縫遷移或擴展到 Google Cloud Platform，無需承擔重構應用程式或重新調整運維的成本、精力或風險。這是一項由 Google 銷售和支援的服務，並與 VMware 密切合作。

SDDC 私有雲和NetApp Cloud Volumes 主機託管以最小的網路延遲提供最佳效能。

你可知道？

無論使用哪種雲，部署 VMware SDDC 時，初始叢集都包含以下產品：

- VMware ESXi 主機用於運算虛擬化，並使用 vCenter Server Appliance 進行管理
- VMware vSAN 超融合存儲，整合了每個 ESXi 主機的實體儲存資產

- VMware NSX 用於虛擬網路和安全，並使用 NSX Manager 叢集進行管理

儲存配置

對於規劃託管儲存密集型工作負載並在任何雲端託管 VMware 解決方案上進行擴充的客戶，預設的超融合基礎架構要求擴充應同時在運算和儲存資源上進行。

透過與NetApp Cloud Volumes（例如Azure NetApp Files、 Amazon FSx ONTAP、 Cloud Volumes ONTAP （適用於所有三大超大規模伺服器）以及適用於 Google Cloud 的Google Cloud NetApp Volumes ）集成，客戶現在可以選擇單獨擴展其存儲，並且僅根據需要向 SDDC 叢集添加計算節點。

筆記：

- VMware 不建議不平衡的叢集配置，因此擴充儲存意味著新增更多主機，這意味著更多的 TCO。
- 僅可實作一個 vSAN 環境。因此，所有儲存流量將直接與生產工作負載競爭。
- 沒有提供多個效能層來滿足應用程式要求、效能和成本的選項。
- 建立在叢集主機之上的 vSAN 的儲存容量很容易達到極限。使用NetApp Cloud Volumes 擴充儲存空間以託管活動資料集或將較冷的資料分層到持久性儲存。

Azure NetApp Files、 Amazon FSx ONTAP、 Cloud Volumes ONTAP （三大超大規模伺服器皆可使用）以及 Google Cloud 適用的Google Cloud NetApp Volumes可與來賓虛擬機器結合使用。這種混合式儲存架構由保存客戶作業系統和應用程式二進位資料的 vSAN 資料儲存組成。應用程式資料透過基於來賓的 iSCSI 啟動器或 NFS/SMB 掛載附加到虛擬機，這些掛載分別與Amazon FSx ONTAP、Cloud Volume ONTAP、 Azure NetApp Files和 Google Cloud 的Google Cloud NetApp Volumes直接通訊。這種配置可讓您輕鬆克服儲存容量方面的挑戰，就像使用 vSAN 一樣，可用的空閒空間取決於所使用的鬆弛空間和儲存策略。

讓我們考慮一下 VMware Cloud on AWS 上的三節點 SDDC 叢集：

- 三節點 SDDC 的總原始容量 = 31.1TB（每個節點約 10TB）。
- 在增加其他主機之前需要維護的鬆弛空間 = 25% = (.25 x 31.1TB) = 7.7TB。
- 扣除剩餘空間後的可用原始容量 = 23.4TB
- 可用的有效空閒空間取決於所應用的儲存策略。

  例如：

  - RAID 0 = 有效可用空間 = 23.4TB（可用原始容量/1）
  - RAID 1 = 有效可用空間 = 11.7TB（可用原始容量/2）
  - RAID 5 = 有效可用空間 = 17.5TB（可用原始容量/1.33）

因此，使用NetApp Cloud Volumes 作為客戶機連接儲存將有助於擴展儲存和最佳化 TCO，同時滿足效能和資料保護要求。



在撰寫本文檔時，客艙內儲存是唯一可用的選項。

需要記住的要點

- 在混合儲存模型中，將第 1 層或高優先級工作負載放置在 vSAN 資料儲存上，以滿足任何特定的延遲要求，因為它們是主機本身的一部分並且在附近。對於任何可以接受交易延遲的工作負載虛擬機，請使用客戶機內

機制。

- 使用 NetApp SnapMirror 技術將工作負載資料從內部部署 ONTAP 系統複寫到 Cloud Volumes ONTAP 或 Amazon FSx ONTAP，以使用區塊層級機制簡化移轉。這不適用於 Azure NetApp Files 和 Google Cloud NetApp Volumes。若要將資料移轉至 Azure NetApp Files 或 Google Cloud NetApp Volumes，請根據所使用的檔案協定，使用 NetApp XCP、NetApp Copy and Sync、rysnc 或 robocopy。
- 測試表明，從相應的 SDDC 存取儲存空間時會有 2-4ms 的額外延遲。在映射儲存時，將此額外的延遲考慮進應用程式要求中。
- 為了在測試故障轉移和實際故障轉移期間掛載來賓連接的存儲，請確保重新配置 iSCSI 啟動器、為 SMB 共享更新 DNS、並在 fstab 中更新 NFS 掛載點。
- 確保虛擬機器內部的 Microsoft 多路徑 I/O (MPIO)、防火牆和磁碟逾時登錄設定配置正確。



這僅適用於來賓連接的儲存。

NetApp雲端儲存的優勢

NetApp雲端儲存有以下優勢：

- 透過獨立於計算擴展存儲來提高計算到存儲的密度。
- 允許您減少主機數量，從而降低整體 TCO。
- 計算節點故障不會影響儲存效能。
- Azure NetApp Files的磁碟區重塑和動態服務等級功能可讓您透過調整穩定狀態工作負載的大小來最佳化成本，從而防止過度配置。
- Cloud Cloud Volumes ONTAP的儲存效率、雲端分層和實例類型修改功能允許以最佳方式新增和擴展儲存。
- 防止過度配置儲存資源，僅在需要時新增。
- 高效的 Snapshot 副本和克隆可讓您快速建立副本而不會對效能產生任何影響。
- 透過使用 Snapshot 副本的快速恢復來幫助應對勒索軟體攻擊。
- 提供高效的基於增量區塊傳輸的區域災難復原和跨區域的整合備份區塊級別，提供更好的 RPO 和 RTO。

假設

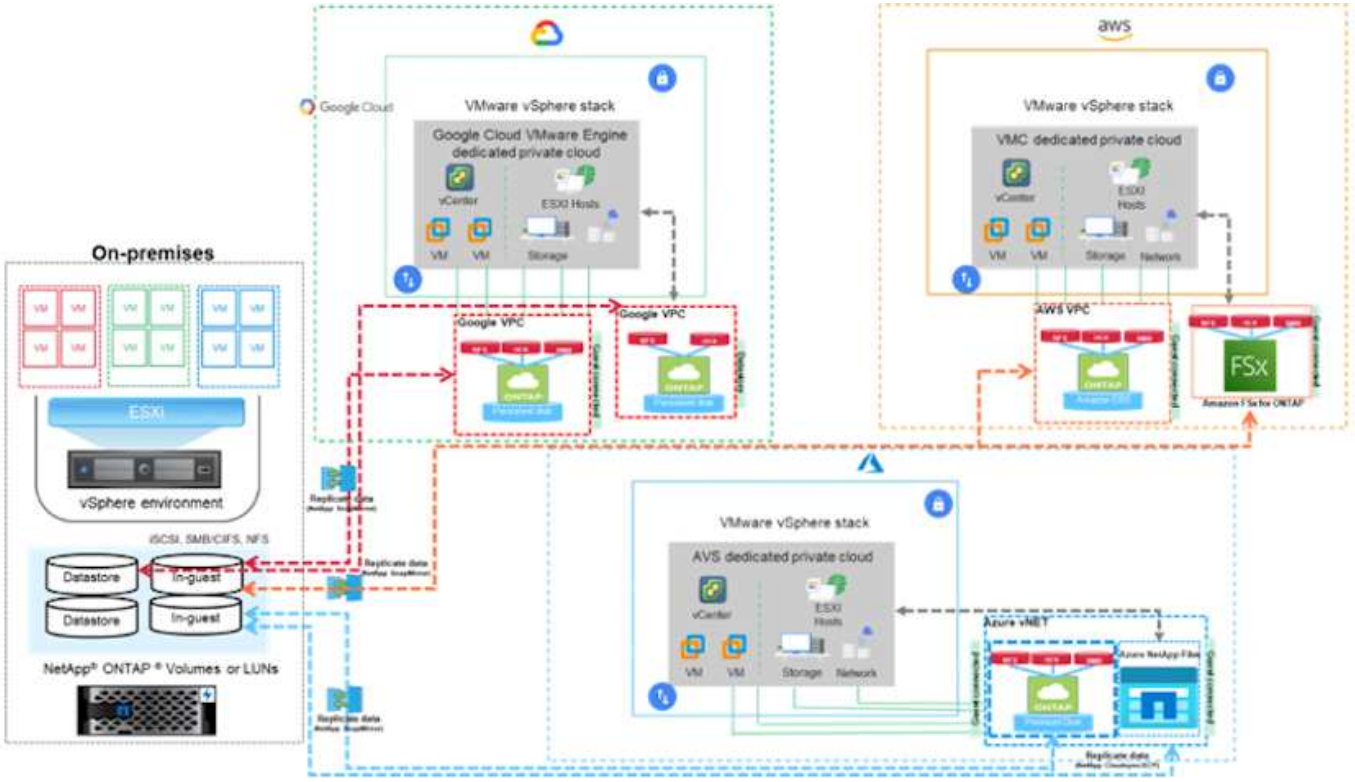
- 啟用SnapMirror技術或其他相關資料遷移機制。有許多連接選項，從本地到任何超大規模雲端。使用適當的路徑並與相關的網路團隊合作。
- 在撰寫本文檔時，客艙內儲存是唯一可用的選項。



與NetApp解決方案架構師和相應的超大規模雲端架構師合作，規劃和確定儲存空間以及所需的主機數量。 NetApp建議在使用Cloud Volumes ONTAP大小調整器之前先確定儲存效能需求，以確定儲存實例類型或具有正確吞吐量的適當服務等級。

詳細架構

從高層次的角度來看，該架構（如下圖所示）涵蓋如何使用NetApp Cloud Volumes ONTAP、 Google Cloud NetApp Volumes for Google Cloud 和Azure NetApp Files作為額外的客戶機儲存選項，實現跨多個雲端供應商的混合多雲連接和應用程式可移植性。



針對超大規模企業 **VMware** 的**NetApp**解決方案

進一步了解NetApp為三大 (3) 個主要超大規模企業帶來的功能 - 從NetApp作為來賓連接儲存設備或補充 NFS 資料儲存到遷移工作流程、擴展/爆發到雲端、備份/復原和災難復原。

選擇您的雲，讓NetApp完成剩下的工作！



若要查看特定超大規模器的功能，請按一下該超大規模器的對應標籤。

透過選擇以下選項跳到所需內容的部分：

- "超大規模配置中的 VMware"
- "NetApp儲存選項"
- "NetApp /VMware 雲端解決方案"

超大規模配置中的 **VMware**

與本地一樣，規劃基於雲端的虛擬化環境對於成功創建虛擬機器和遷移的生產就緒環境至關重要。

AWS/VMC

本節介紹如何設定和管理 VMware Cloud on AWS SDDC，並將其與可用於連接NetApp儲存的選項結合使用。

客戶機內儲存是將Cloud Volumes ONTAP連接到 AWS VMC 的唯一支援方法。

設定過程可分為以下步驟：

- 部署和配置 VMware Cloud for AWS
- 將 VMware Cloud 連接到 FSx ONTAP

查看詳細信息"VMC 的設定步驟"。

Azure/AVS

本部分介紹如何設定和管理 Azure VMware 解決方案，並將其與用於連接NetApp儲存裝置的可用選項結合使用。

來賓內儲存是將Cloud Volumes ONTAP連接到 Azure VMware 解決方案的唯一支援方法。

設定過程可分為以下步驟：

- 註冊資源提供者並建立私有雲
- 連接到新的或現有的 ExpressRoute 虛擬網路網關
- 驗證網路連線並存取私有雲

查看詳細信息"AVS設定步驟"。

良好操作規範/良好行為規範

本節介紹如何設定和管理 GCVE，以及如何將其與可用於連接NetApp儲存的選項結合使用。

客戶機內儲存是將Cloud Volumes ONTAP和Google Cloud NetApp Volumes連接到 GCVE 的唯一支援方法。

設定過程可分為以下步驟：

- 部署和配置 GCVE
- 啟用對 GCVE 的私人訪問

查看詳細信息"GCVE 的設定步驟"。

NetApp儲存選項

NetApp儲存可以在 3 個主要超大規模伺服器中以多種方式使用 - 既可以作為客戶機連接，也可以作為補充 NFS 資料儲存。

請訪問"支援的NetApp儲存選項"了解更多。

AWS/VMC

AWS 支援以下配置的NetApp儲存：

- FSx ONTAP作為來賓連接存儲
- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- FSx ONTAP作為補充 NFS 資料存儲

查看詳細信息"VMC 的用戶機連線儲存選項"。查看詳細信息"VMC 的補充 NFS 資料儲存選項"。

Azure/AVS

Azure 支援以下配置的NetApp儲存體：

- Azure NetApp Files(ANF) 作為來賓連接儲存
- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- Azure NetApp Files(ANF) 作為補充 NFS 資料存儲

查看詳細信息"AVS 的來賓連線儲存選項"。查看詳細信息"AVS 的補充 NFS 資料儲存選項"。

良好操作規範/良好行為規範

Google Cloud 支援以下配置的NetApp儲存：

- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- Google Cloud NetApp Volumes （NetApp Volumes）作為來賓連接存儲
- Google Cloud NetApp Volumes （NetApp Volumes）作為補充 NFS 資料存儲

查看詳細信息"GCVE 的來賓連接儲存選項"。查看詳細信息"GCVE 的補充 NFS 資料儲存選項"。

閱讀更多"Google Cloud NetApp Volumes資料儲存區支援 Google Cloud VMware Engine（NetApp部落格）"或者"如何將Google Cloud NetApp Volumes用作 Google Cloud VMware Engine 的資料儲存區（Google部落格）"

NetApp /VMware 雲端解決方案

透過NetApp和 VMware 雲端解決方案，許多用例都可以輕鬆部署在您選擇的超大規模中。 VMware 將主要的雲端工作負載用例定義為：

- 保護（包括災難復原和備份/還原）

- 遷移
- 延長

AWS/VMC

"瀏覽適用於 AWS/VMC 的NetApp解決方案"

Azure/AVS

"瀏覽適用於 Azure/AVS 的NetApp解決方案"

良好操作規範/良好行為規範

"瀏覽適用於 Google Cloud Platform (GCP)/GCVE 的NetApp解決方案"

NetApp混合多雲與 VMware 支援的配置

了解主要超大規模企業對NetApp儲存支援的組合。

	訪客已連線	補充 **NFS** 資料儲存
AWS	CVO FSx ONTAP"細節"	FSx ONTAP"細節"
蔚藍	CVO ANF"細節"	心鈉素"細節"
GCP	CVO NetApp區"細節"	NetApp區"細節"

超大規模配置中的 VMware

在雲端提供者中配置虛擬化環境

這裡介紹如何在每個受支援的超大規模器中配置虛擬化環境的詳細資訊。

AWS/VMC

本節介紹如何設定和管理 VMware Cloud on AWS SDDC，並將其與可用於連接NetApp儲存的選項結合使用。

客戶機內儲存是將Cloud Volumes ONTAP連接到 AWS VMC 的唯一支援方法。

設定過程可分為以下步驟：

- 部署和配置 VMware Cloud for AWS
- 將 VMware Cloud 連接到 FSx ONTAP

查看詳細信息"VMC 的設定步驟"。

Azure/AVS

本部分介紹如何設定和管理 Azure VMware 解決方案，並將其與用於連接NetApp儲存裝置的可用選項結合使用。

來賓內儲存是將Cloud Volumes ONTAP連接到 Azure VMware 解決方案的唯一支援方法。

設定過程可分為以下步驟：

- 註冊資源提供者並建立私有雲
- 連接到新的或現有的 ExpressRoute 虛擬網路網關
- 驗證網路連線並存取私有雲

查看詳細信息"AVS設定步驟"。

良好操作規範/良好行為規範

本節介紹如何設定和管理 GCVE，以及如何將其與可用於連接NetApp儲存的選項結合使用。

客戶機內儲存是將Cloud Volumes ONTAP和Google Cloud NetApp Volumes連接到 GCVE 的唯一支援方法。

設定過程可分為以下步驟：

- 部署和配置 GCVE
- 啟用對 GCVE 的私人訪問

查看詳細信息"GCVE 的設定步驟"。

在 **AWS** 上部署和配置虛擬化環境

與本地部署一樣，規劃 AWS 上的 VMware Cloud 對於成功建立虛擬機器和遷移的生產就緒環境至關重要。

本節介紹如何設定和管理 VMware Cloud on AWS SDDC，並將其與可用於連接NetApp儲存的選項結合使用。

目前，客戶機內儲存是將Cloud Volumes ONTAP (CVO) 連接到 AWS VMC 的唯一支援方法。

設定過程可分為以下步驟：

▼ 部署和配置 **VMware Cloud for AWS**

"AWS 上的 VMware Cloud"為 AWS 生態系統中基於 VMware 的工作負載提供雲端原生體驗。每個 VMware 軟體定義資料中心 (SDDC) 都在 Amazon 虛擬私有雲 (VPC) 中運行，並提供完整的 VMware 堆疊（包括 vCenter Server）、NSX-T 軟體定義網路、vSAN 軟體定義儲存以及一個或多個為您的工作負載提供運算和儲存資源的 ESXi 主機。

本節介紹如何設定和管理 VMware Cloud on AWS，以及如何將其與具有客戶機內儲存的 AWS 上的Amazon FSx ONTAP和/或Cloud Volumes ONTAP結合使用。

目前，客戶機內儲存是將Cloud Volumes ONTAP (CVO) 連接到 AWS VMC 的唯一支援方法。

設定過程可分為三個部分：

▼ 註冊 **AWS** 帳戶

註冊"亞馬遜網路服務帳戶"。

您需要一個 AWS 帳戶才能開始使用（假設尚未建立）。無論是新的還是現有的，您都需要帳戶的管理權限才能執行此過程中的許多步驟。看看這個"關聯"有關 AWS 憑證的詳細資訊。

▼ 註冊 **My VMware** 帳戶

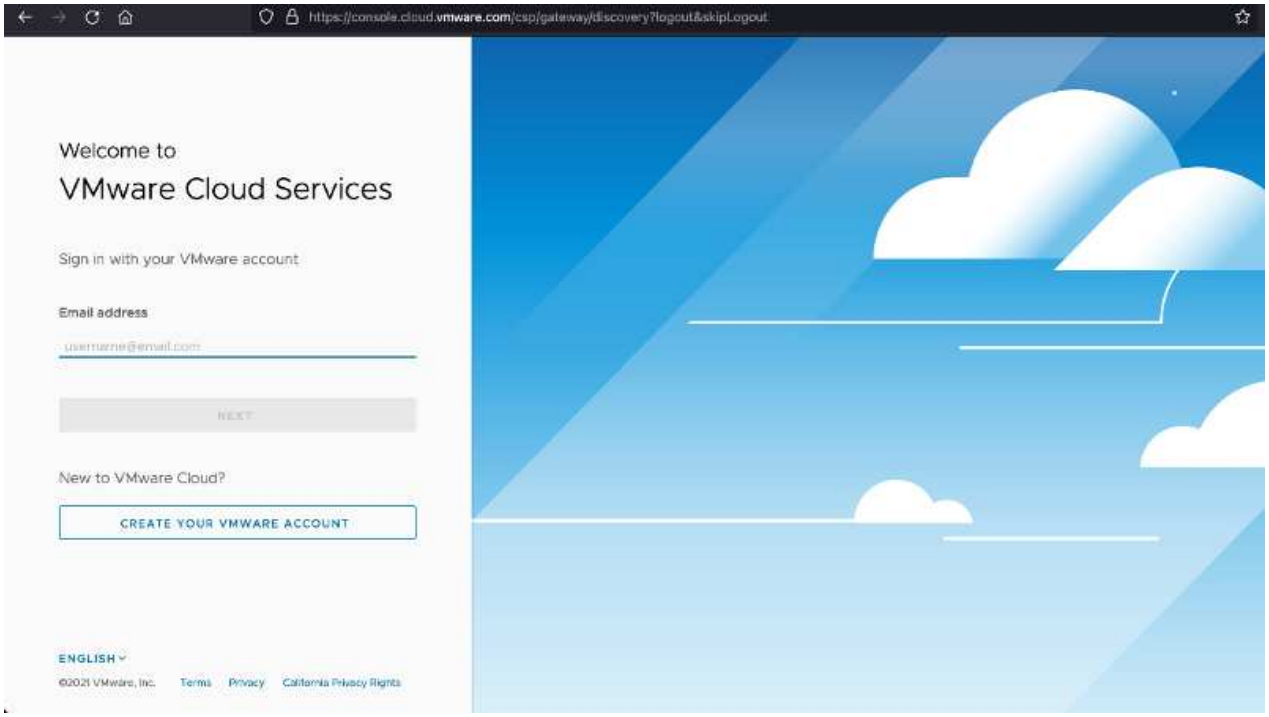
註冊"我的 VMware"帳戶。

若要存取 VMware 的雲端產品組合（包括 AWS 上的 VMware Cloud），您需要一個 VMware 客戶帳戶或 My VMware 帳戶。如果您尚未建立 VMware 帳戶，請建立一個"這裡"。

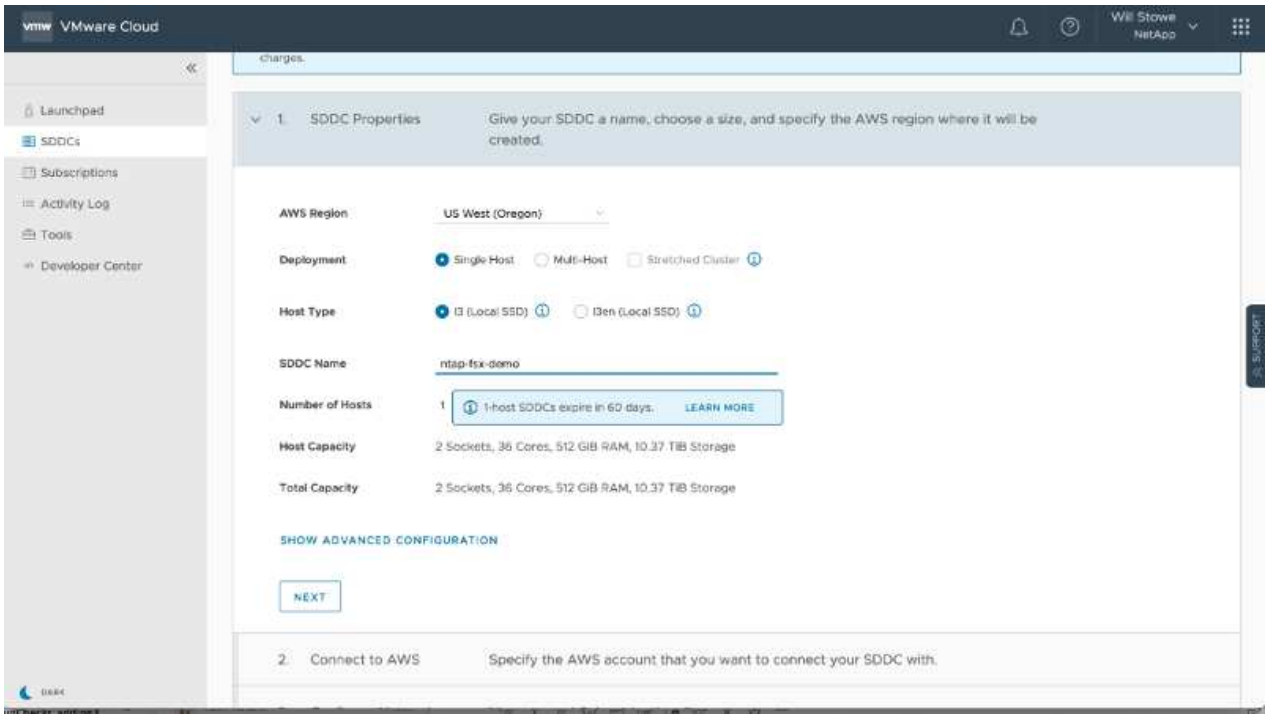
▼ 在 **VMware Cloud** 中調配 **SDDC**

配置 VMware 帳戶並執行適當的大小調整後，部署軟體定義資料中心是使用 VMware Cloud on AWS 服務的下一步。若要建立 SDDC，請選擇一個 AWS 區域來託管它，為 SDDC 命名，並指定您希望 SDDC 包含多少個 ESXi 主機。如果您還沒有 AWS 帳戶，您仍然可以建立包含單一 ESXi 主機的入門配置 SDDC。

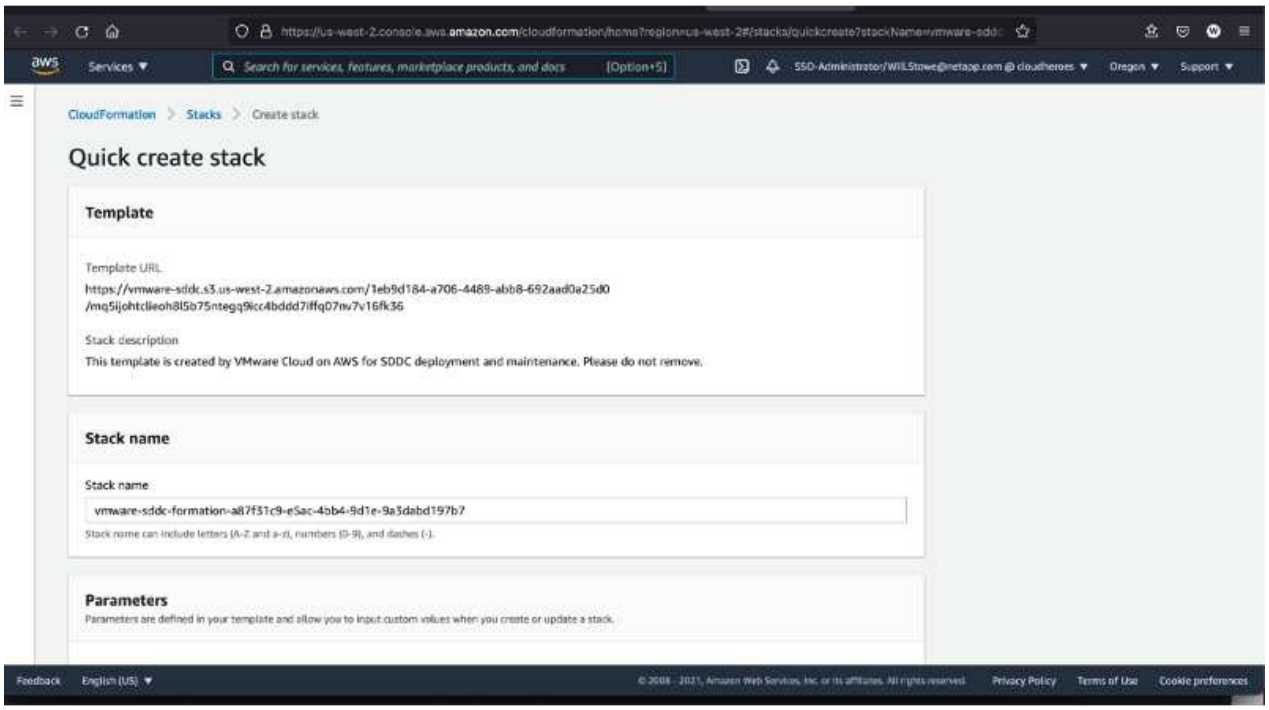
1. 使用現有或新建立的 VMware 憑證登入 VMware Cloud Console。

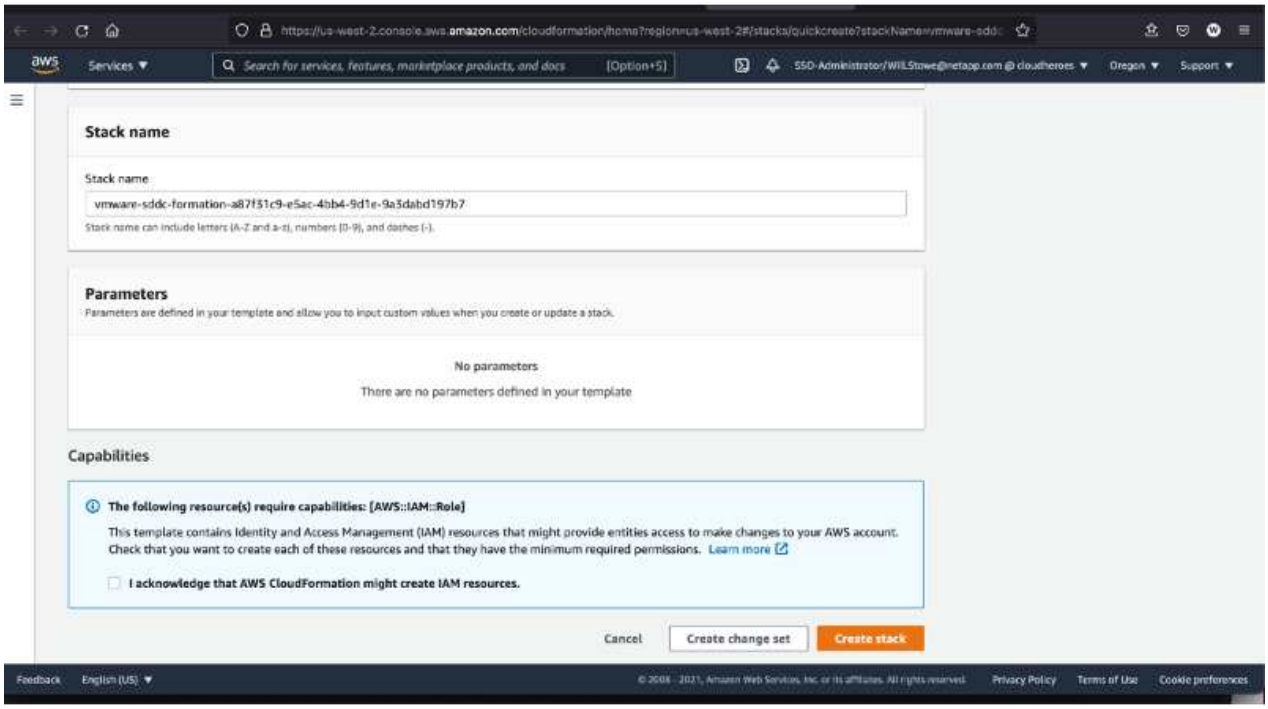


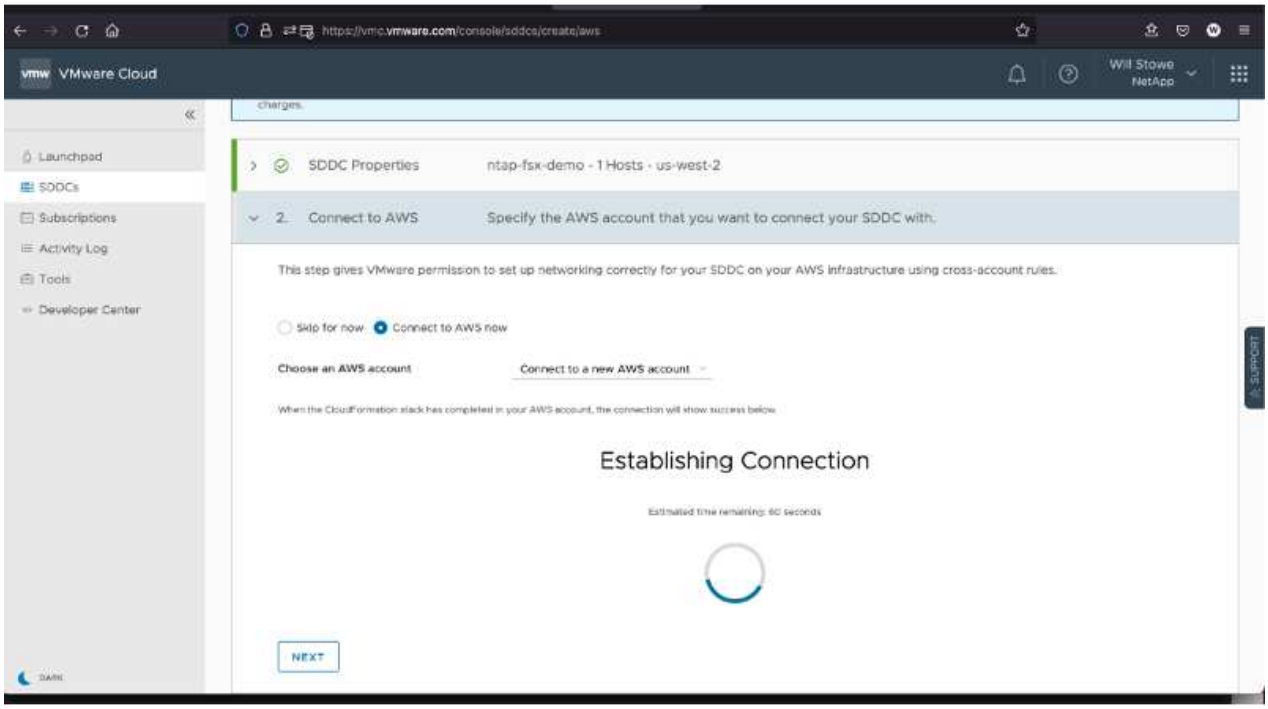
2. 配置 AWS 區域、部署、主機類型以及 SDDC 名稱：

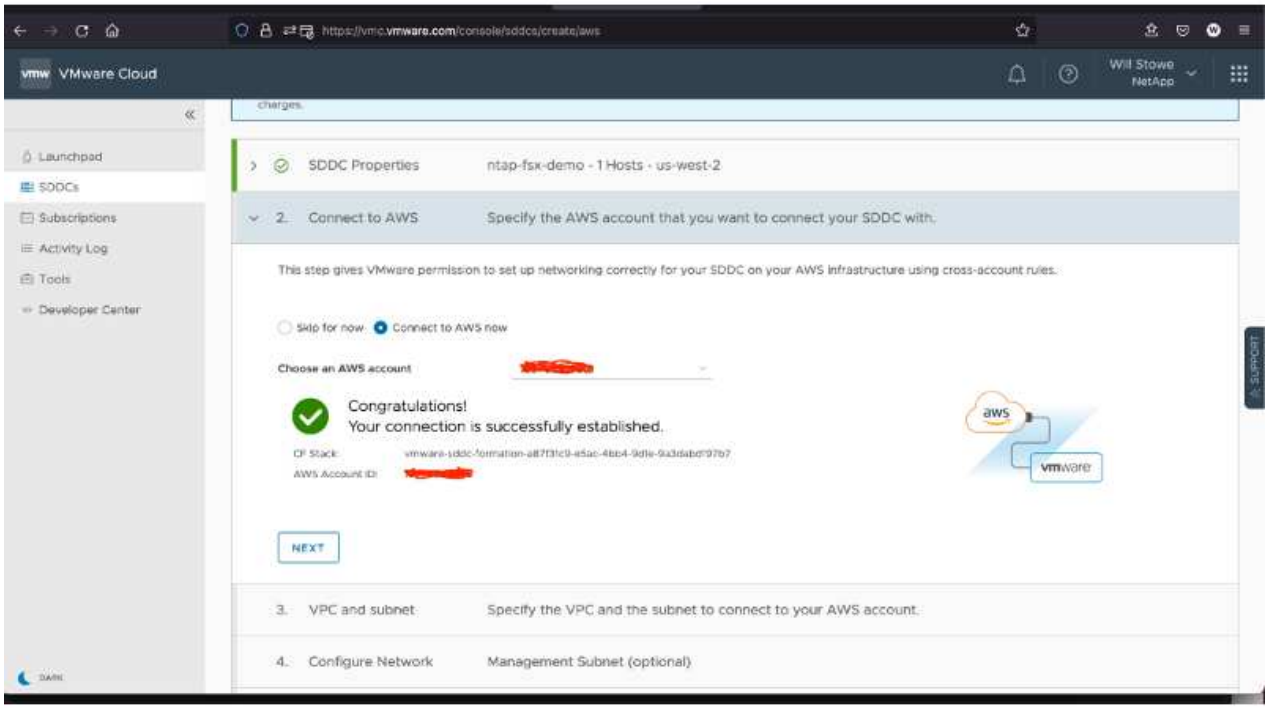


3. 連接到所需的 AWS 帳戶並執行 AWS Cloud Formation 堆疊。



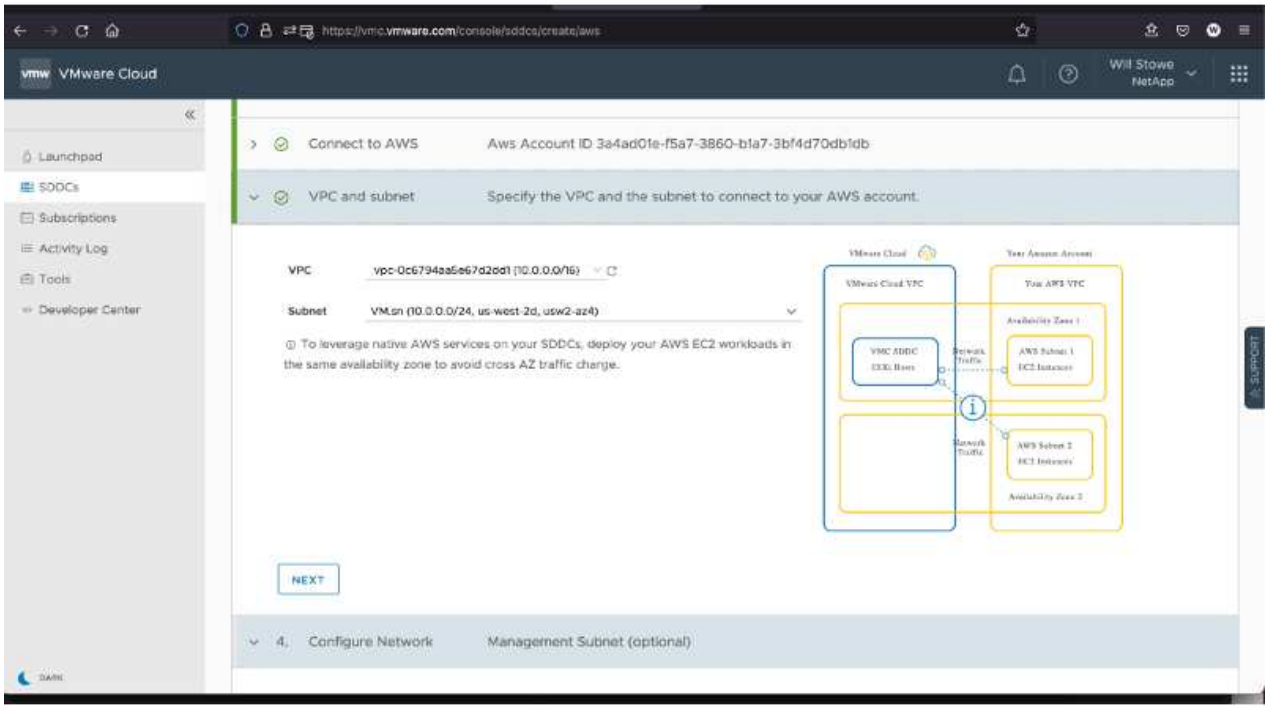

Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack


VMware Cloud
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
SDDC Properties
ntap-fsx-demo - 1 Hosts - us-west-2
2. Connect to AWS
Specify the AWS account that you want to connect your SDDC with.
This step gives VMware permission to set up networking correctly for your SDDC on your AWS infrastructure using cross-account rules.
Skip for now
Connect to AWS now
Choose an AWS account
Connect to a new AWS account
Establishing Connection
NEXT

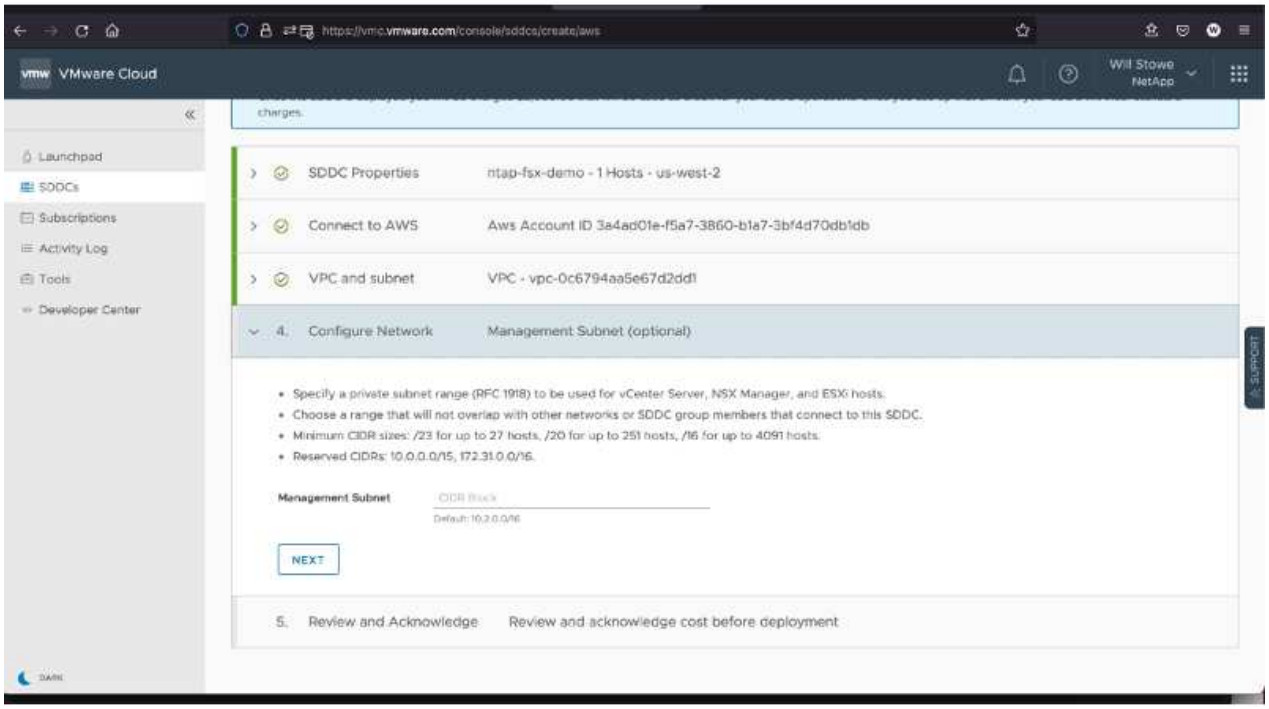


本次驗證採用單主機配置。

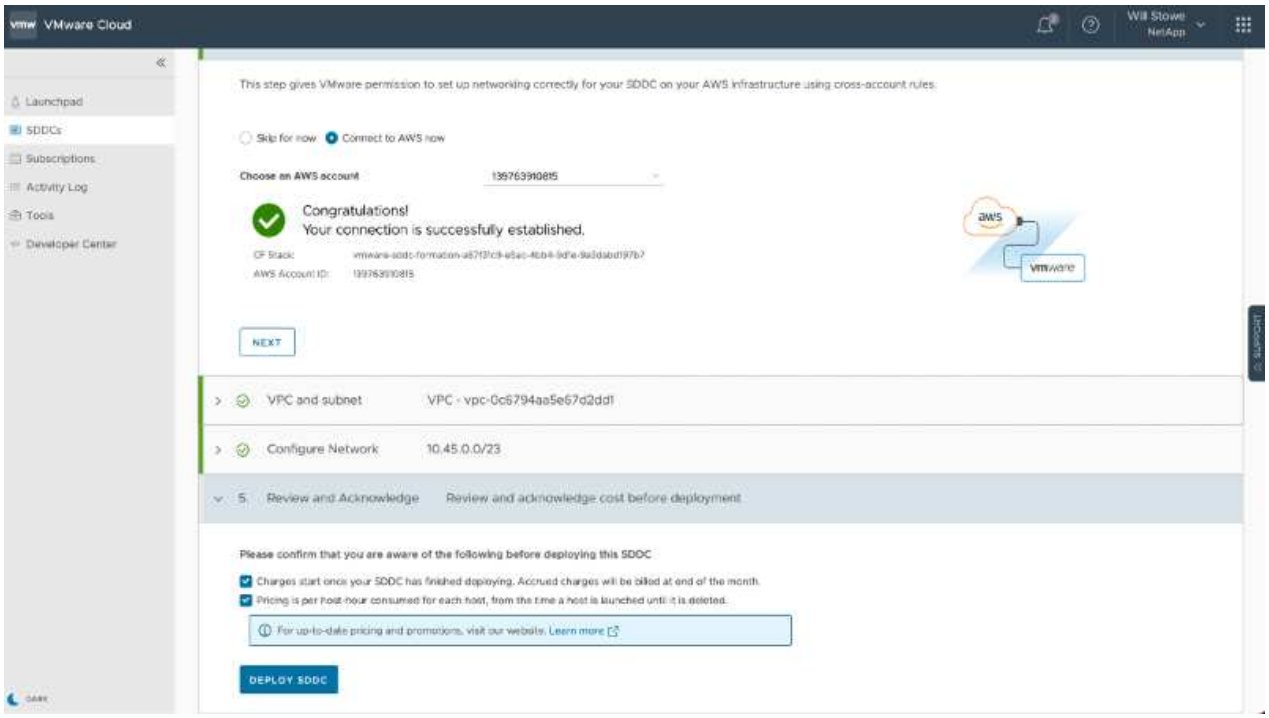
4. 選擇所需的 AWS VPC 來連接 VMC 環境。



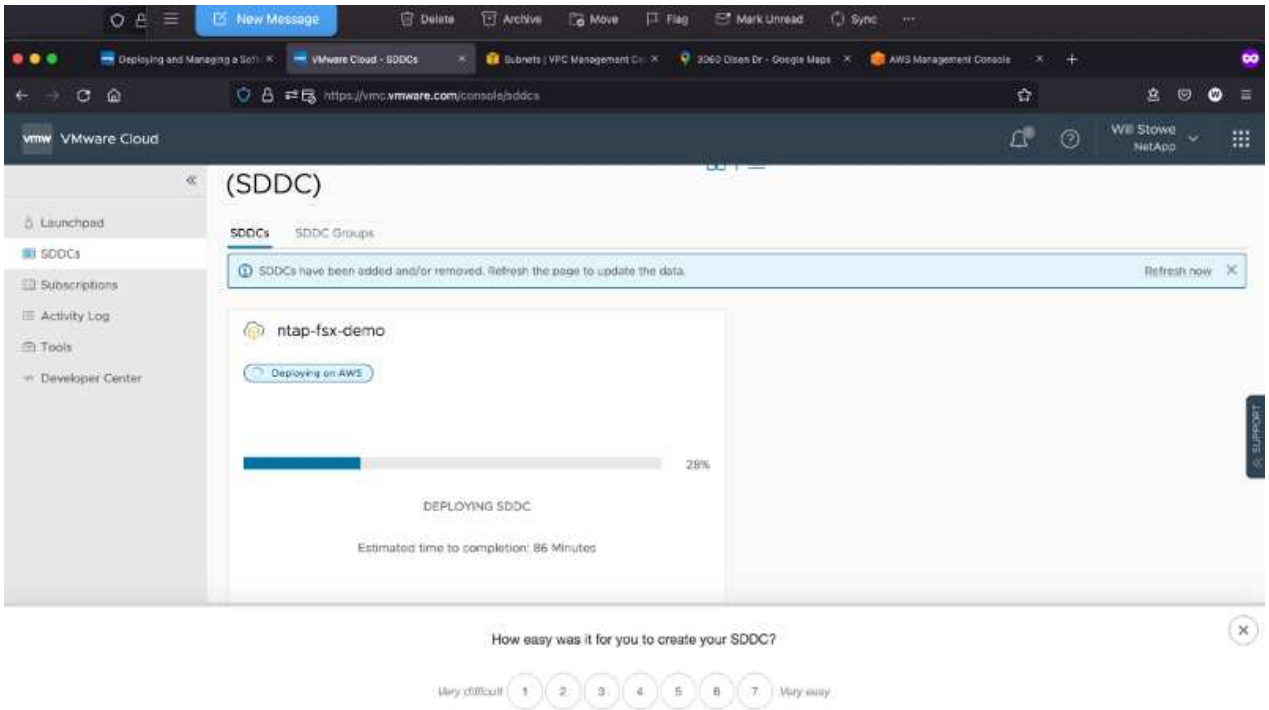
5. 設定 VMC 管理子網路；此子網路包含 VMC 管理的服務，如 vCenter、NSX 等。請勿選擇與任何其他需要連接到 SDDC 環境的網路重疊的位址空間。最後，請遵循下面註明的 CIDR 大小的建議。



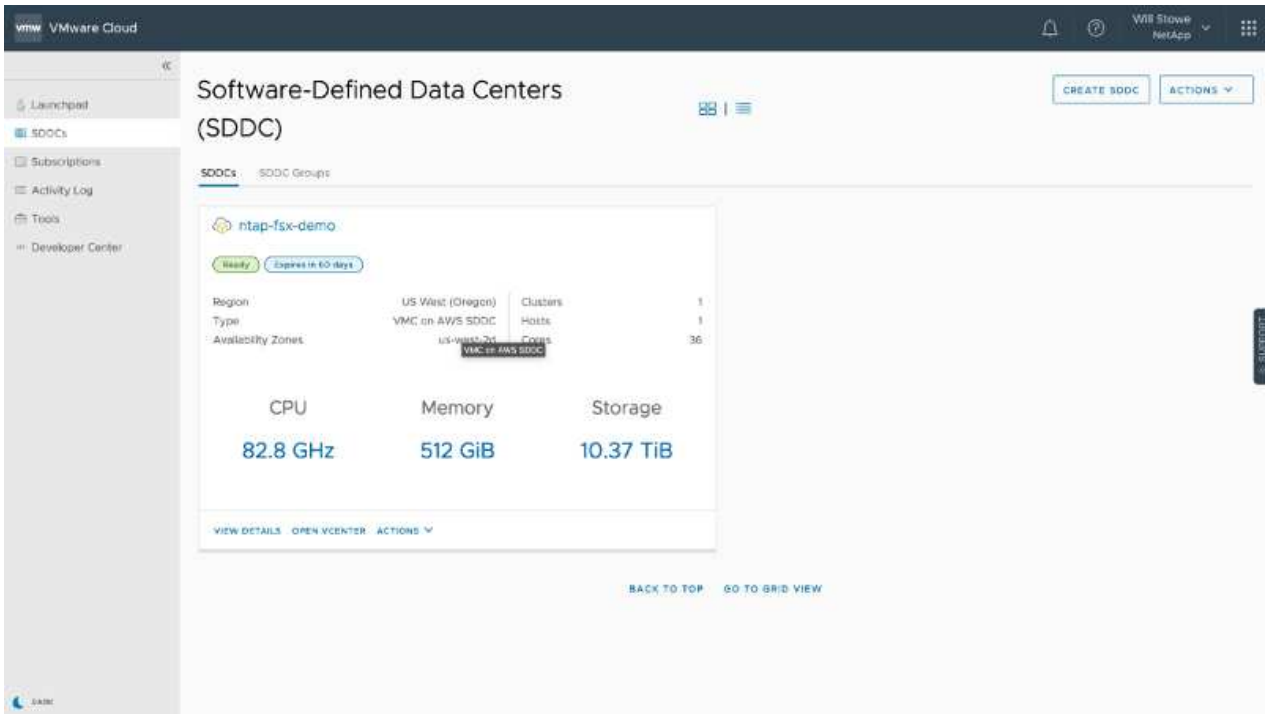
6. 查看並確認 SDDC 配置，然後按一下部署 SDDC。



部署過程通常需要大約兩個小時才能完成。



7. 完成後，SDDC 即可使用。

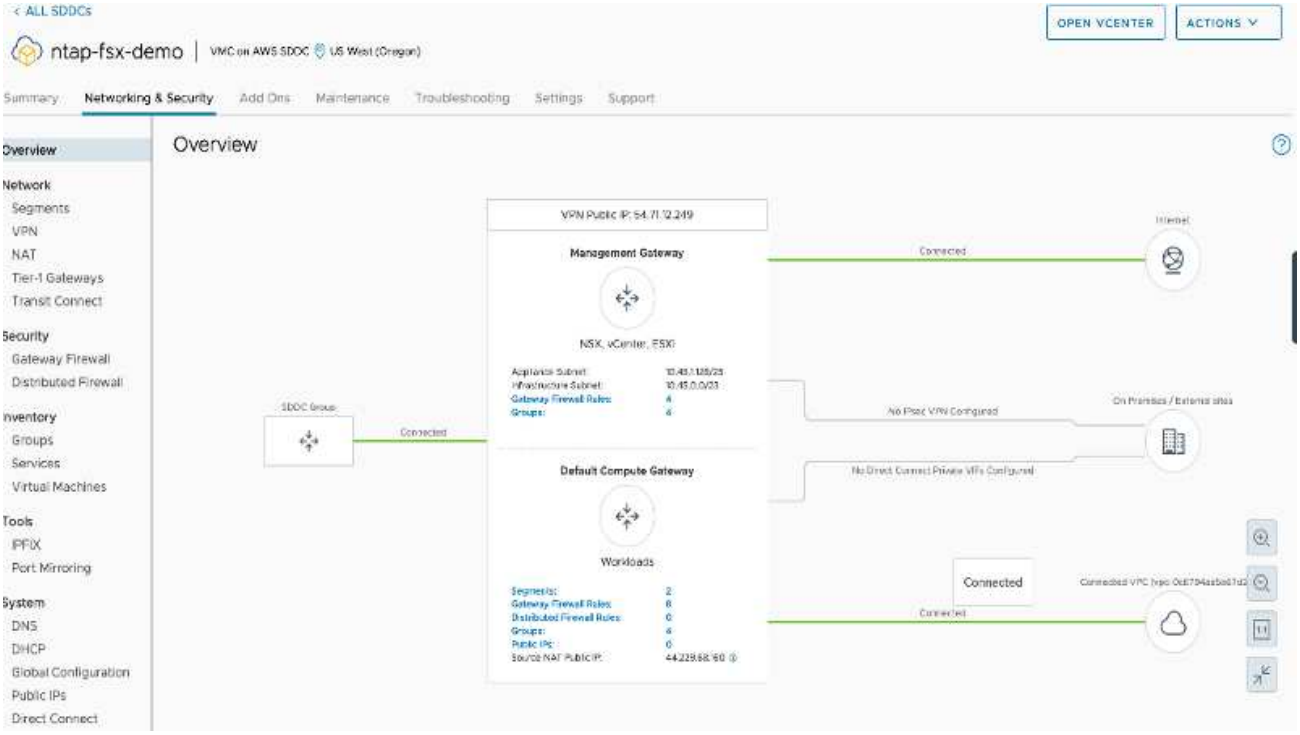


有關 SDDC 部署的逐步指南，請參閱"從 VMC 控制台部署 SDDC"。

▼ 將 **VMware Cloud** 連接到 **FSx ONTAP**

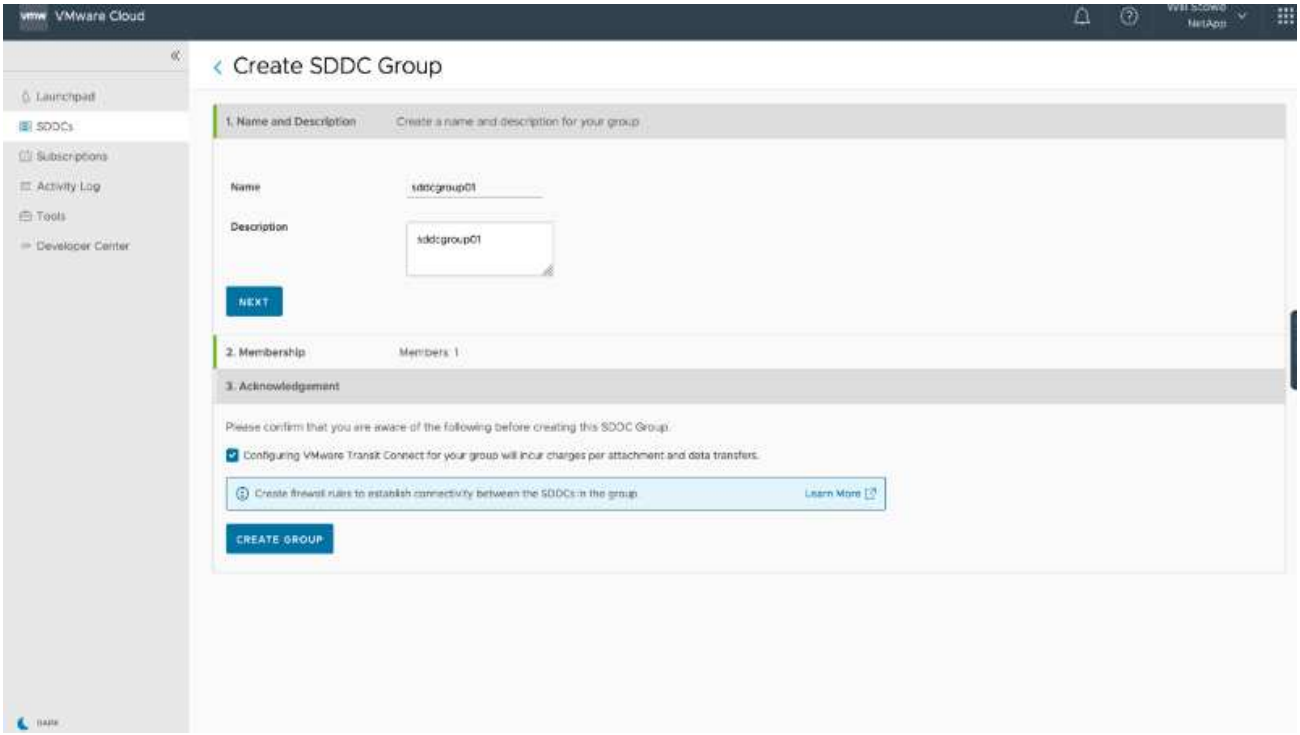
若要將 VMware Cloud 連線至 FSx ONTAP，請完成下列步驟：

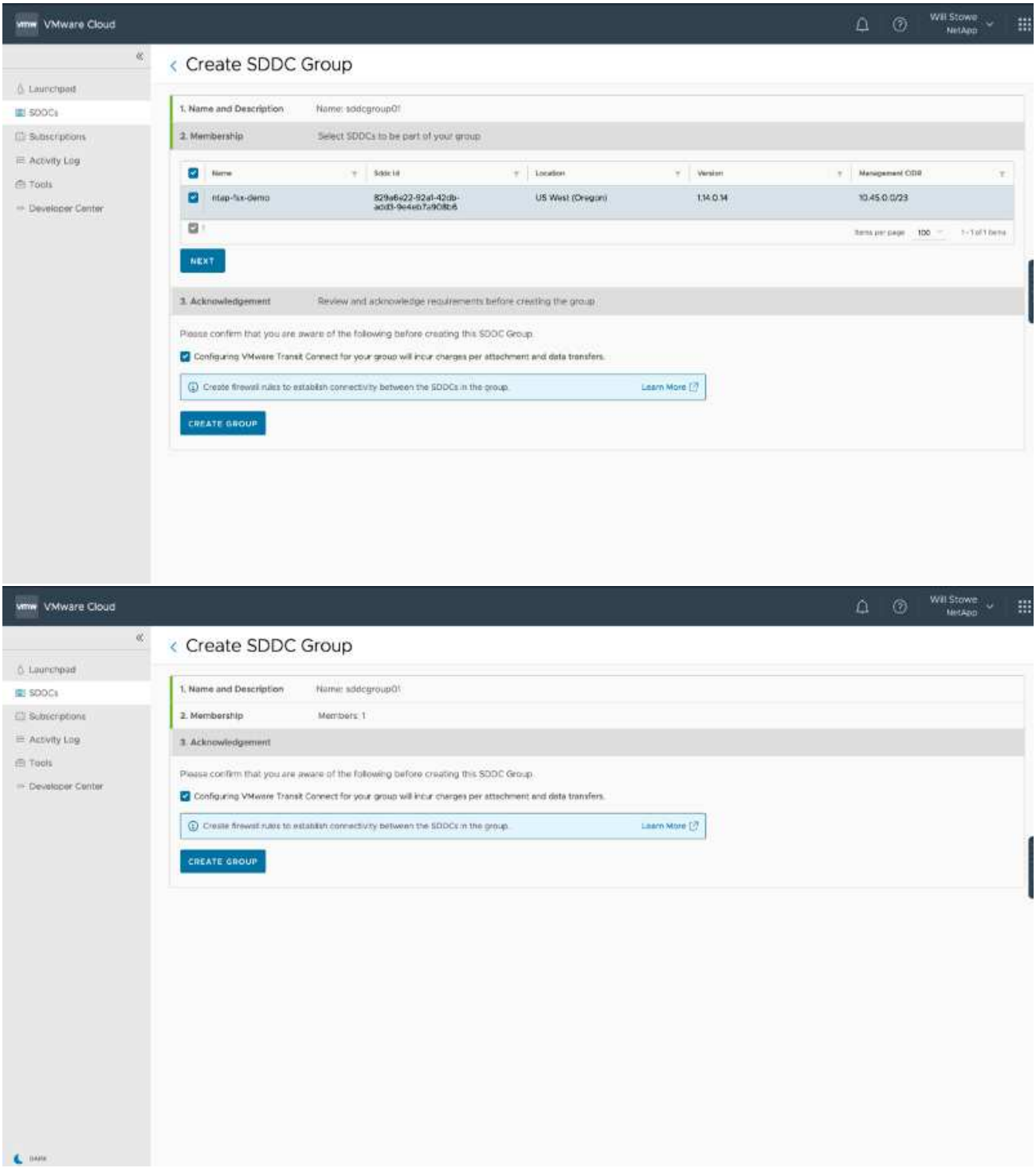
1. VMware Cloud 部署完成並連接到 AWS VPC 後，您必須將Amazon FSx ONTAP部署到新的 VPC 中，而不是原始連接的 VPC（請參閱下方的螢幕截圖）。如果 FSx（NFS 和 SMB 浮動 IP）部署在連接的 VPC 中，則無法存取。請記住，像Cloud Volumes ONTAP這樣的 ISCSI 端點在連接的 VPC 中可以正常運作。



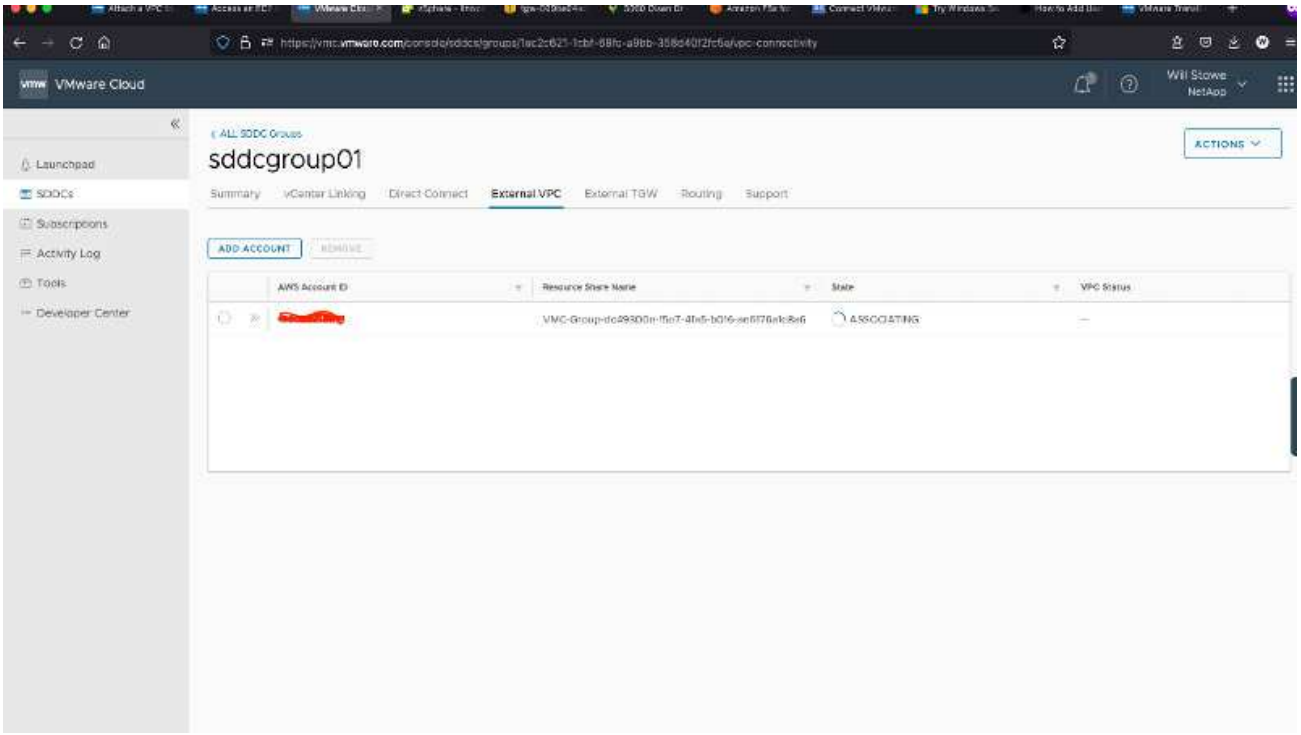
2. 在同一區域部署額外的 VPC，然後將Amazon FSx ONTAP部署到新的 VPC 中。

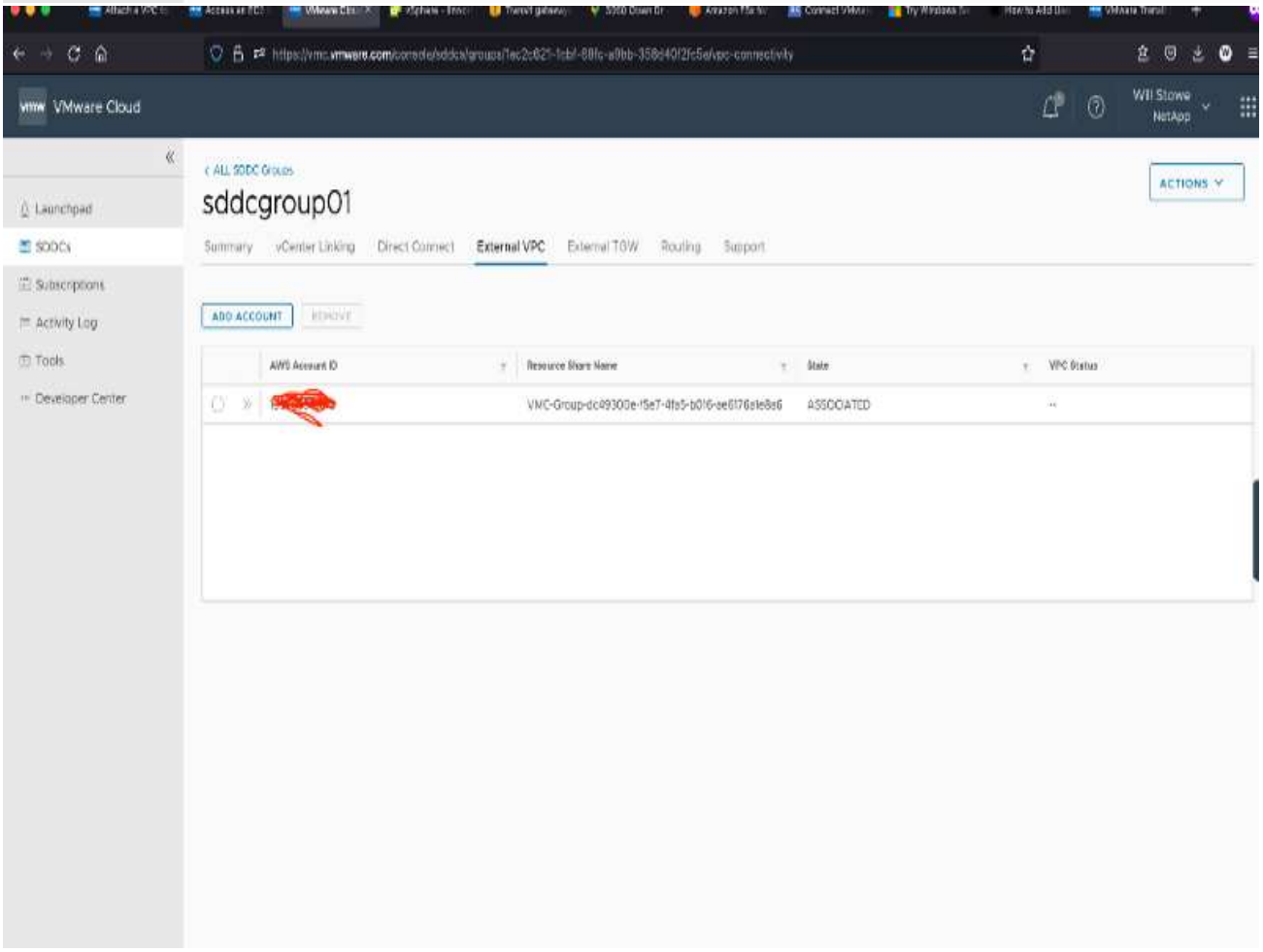
VMware Cloud 控制台中的 SDDC 群組配置啟用了連接到部署 FSx 的新 VPC 所需的網路設定選項。在步驟 3 中，驗證是否選取“為您的群組設定 VMware Transit Connect 將產生每個附件和資料傳輸的費用”，然後選擇“建立群組”。過程可能需要幾分鐘才能完成。



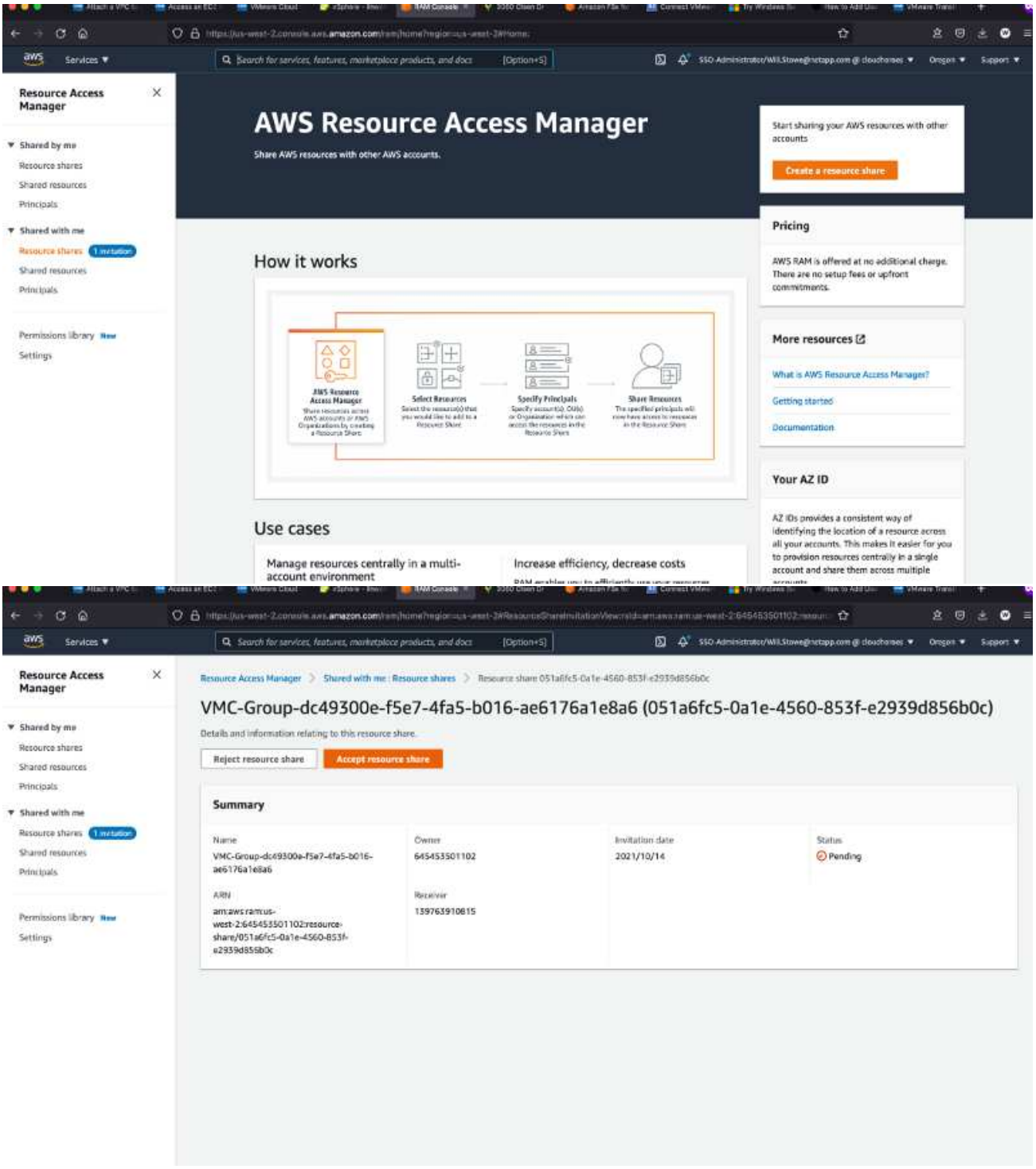


3. 將新建立的 VPC 附加到剛建立的 SDDC 群組。選擇外部 VPC 標籤並按照"連接外部 VPC 的說明"到群組。此過程可能需要 10 到 15 分鐘才能完成。



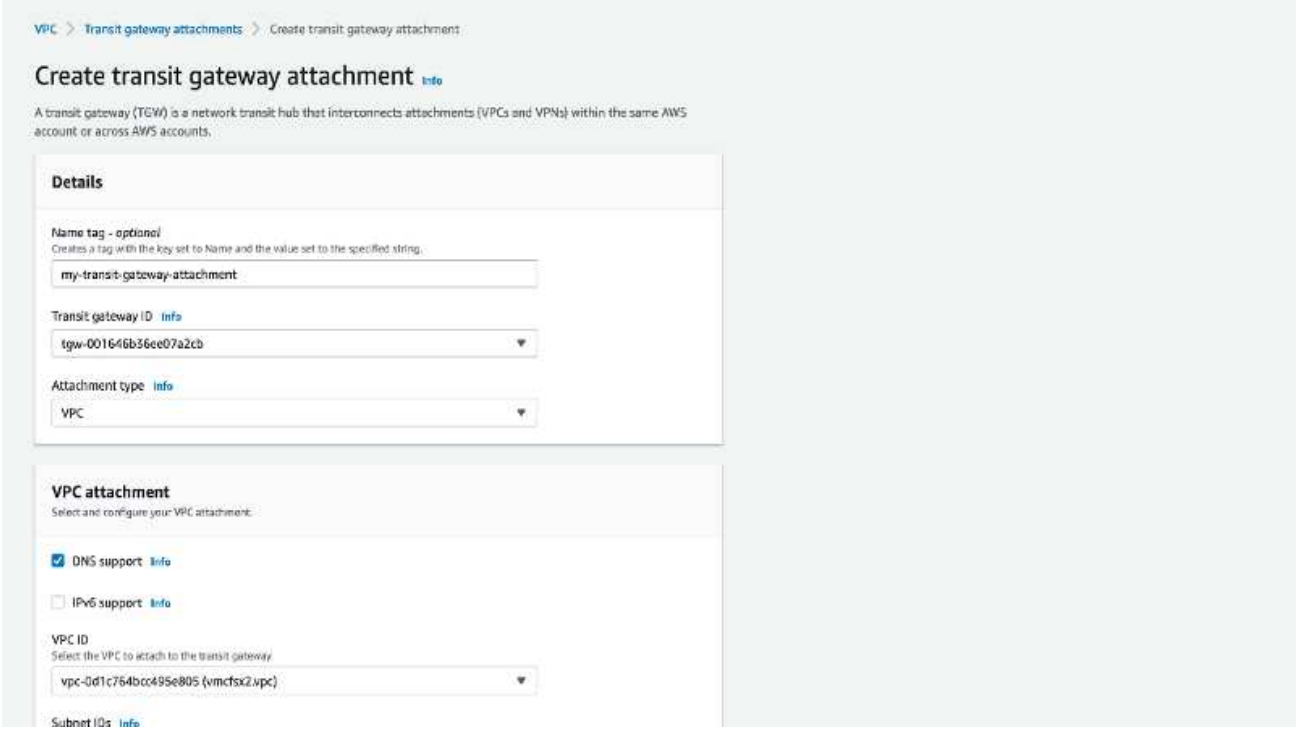


4. 作為外部 VPC 流程的一部分，您將透過 AWS 主控台透過資源存取管理員提示新的共用資源。共享資源是"AWS Transit Gateway"由 VMware Transit Connect 管理。

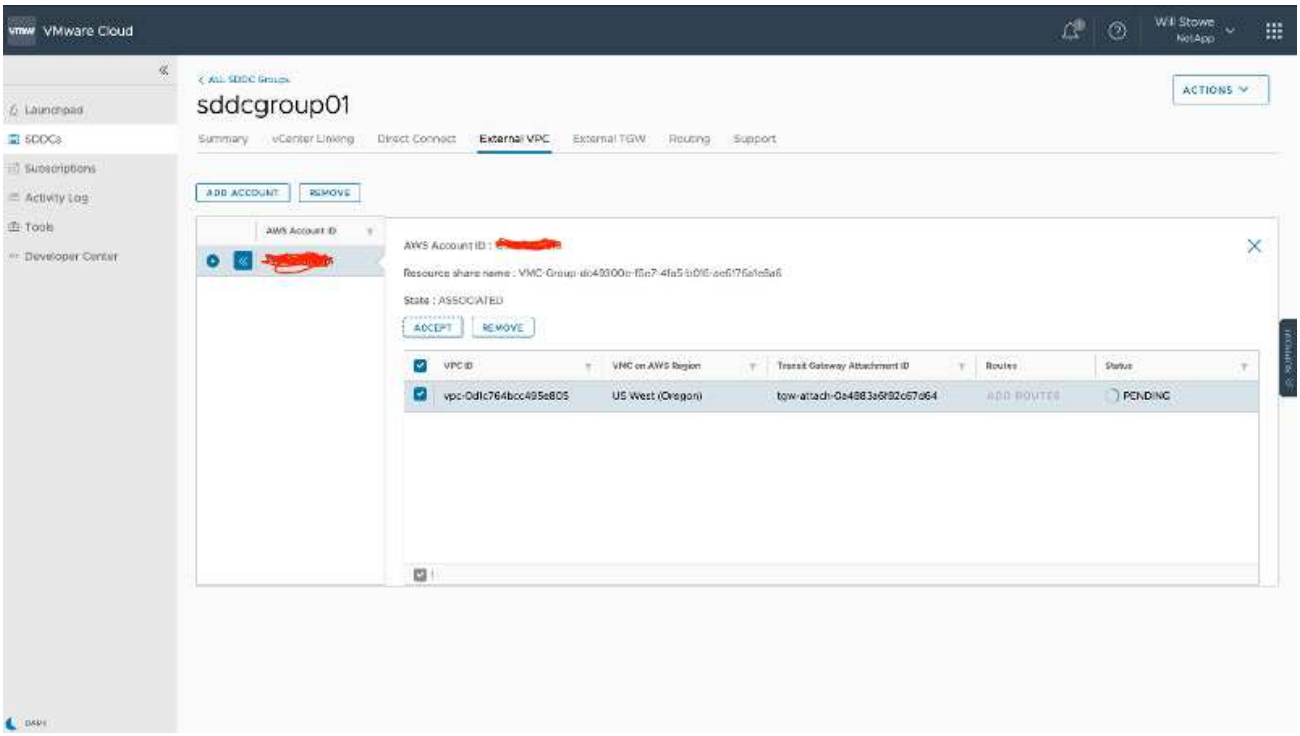

Resource Access Manager
Shared by me
Resource shares
Shared resources
Principals
Shared with me
Resource shares 1 invitation
Shared resources
Principals
Permissions library New
Settings
AWS Resource Access Manager
Share AWS resources with other AWS accounts.
Start sharing your AWS resources with other accounts
Create a resource share
How it works
Pricing
AWS RAM is offered at no additional charge. There are no setup fees or upfront commitments.
More resources
What is AWS Resource Access Manager?
Getting started
Documentation
Your AZ ID
AZ IDs provides a consistent way of identifying the location of a resource across all your accounts. This makes it easier for you to provision resources centrally in a single account and share them across multiple
Use cases
Manage resources centrally in a multi-account environment
Increase efficiency, decrease costs

Resource Access Manager
Shared by me
Resource shares
Shared resources
Principals
Shared with me
Resource shares 1 invitation
Shared resources
Principals
Permissions library New
Settings
Resource Access Manager > Shared with me : Resource shares > Resource share 051a6fc5-0a1e-4560-853f-e2939d856b0c
VMC-Group-dc49300e-f5e7-4fa5-b016-ae6176a1e8a6 (051a6fc5-0a1e-4560-853f-e2939d856b0c)
Details and information relating to this resource share.
Reject resource share
Accept resource share
Summary
Name
VMC-Group-dc49300e-f5e7-4fa5-b016-ae6176a1e8a6
Owner
645453501102
Invitation date
2021/10/14
Status
Pending
ARN
arn:aws:ram:us-west-2:645453501102:resource-share/051a6fc5-0a1e-4560-853f-e2939d856b0c
Receiver
139763910815

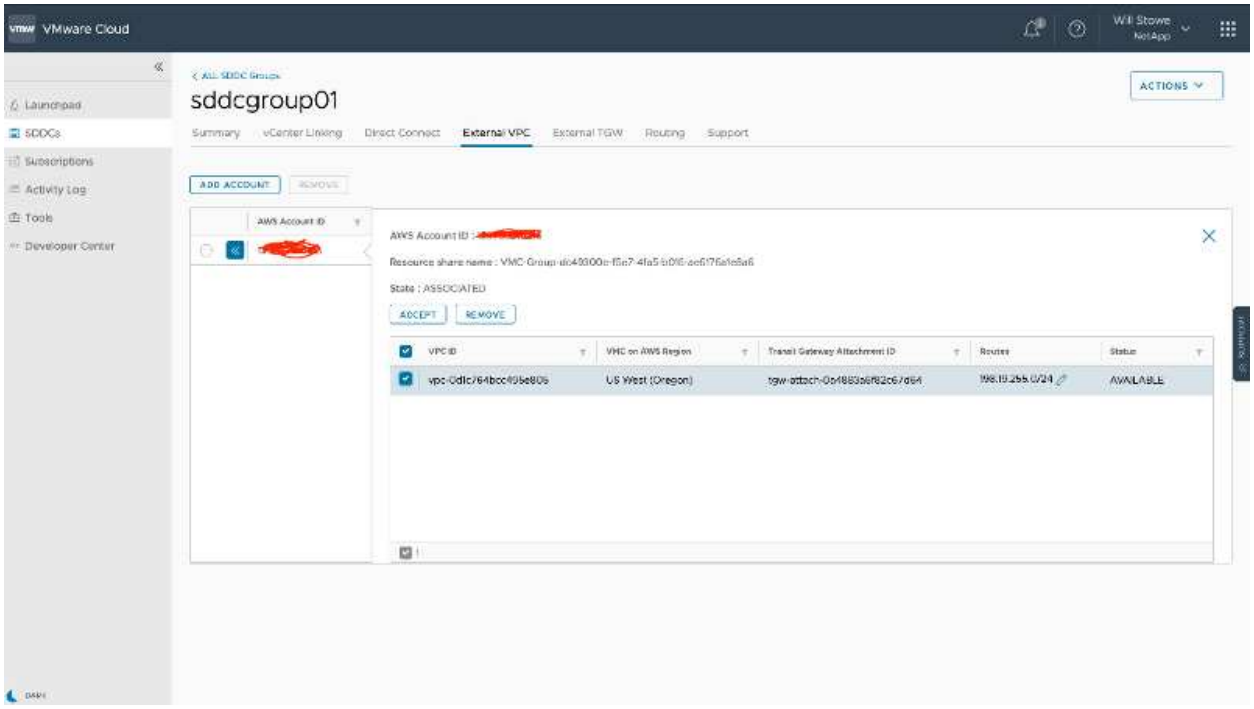
5. 建立傳輸網關附件。



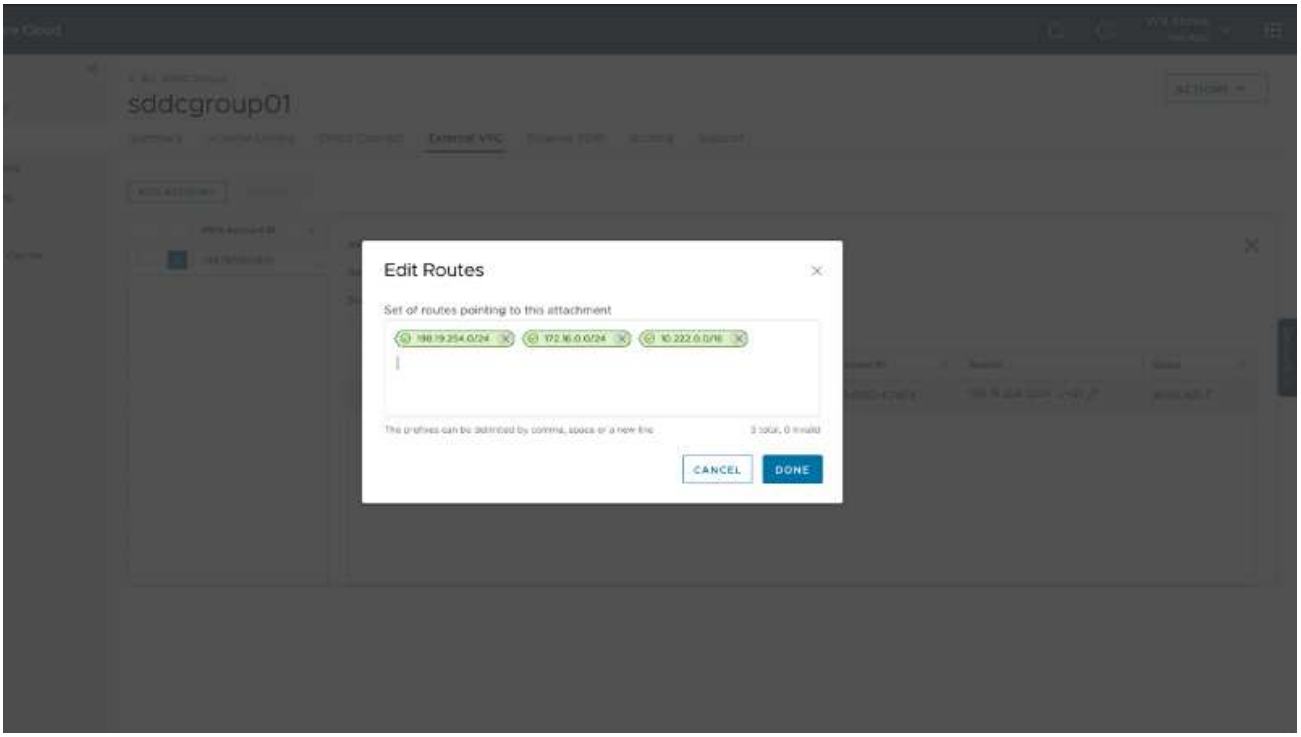
6. 返回 VMC 控制台，接受 VPC 附件。此過程大約需要 10 分鐘才能完成。



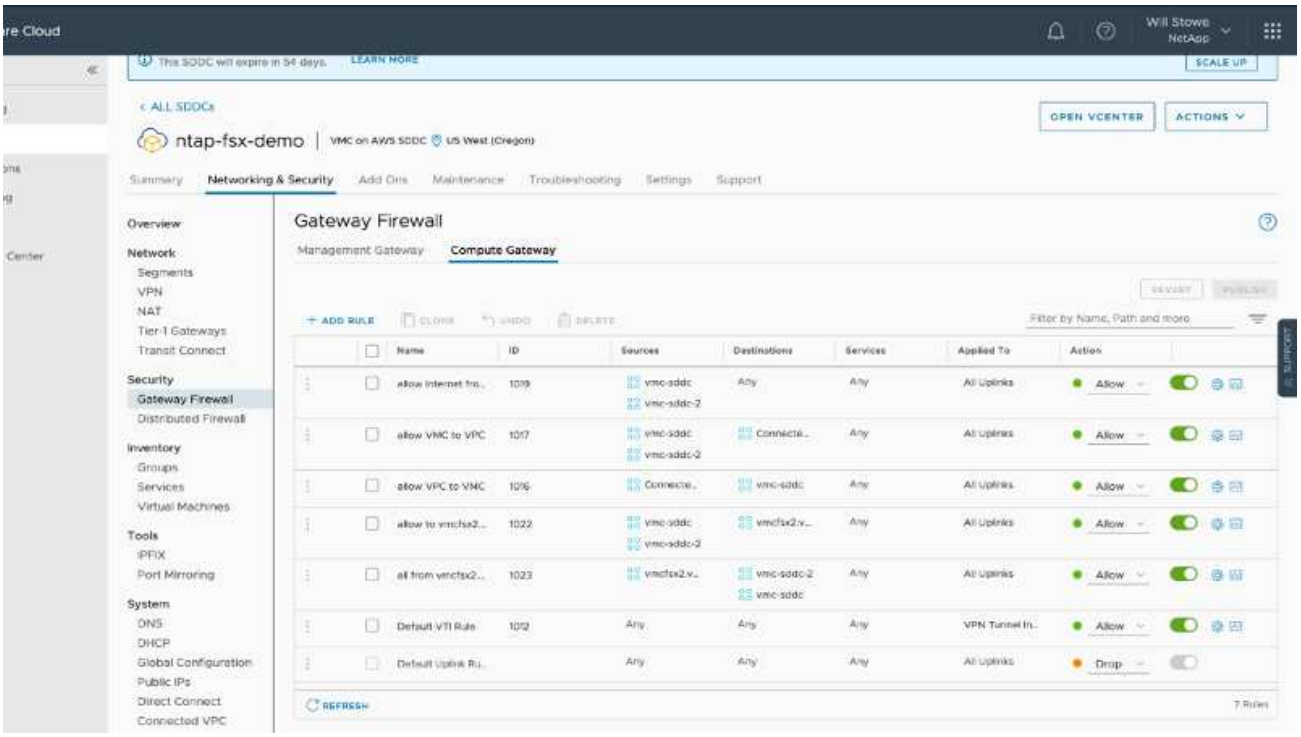
7. 在「外部 VPC」標籤中，按一下「路由」列中的編輯圖標，並新增以下所需路由：
   - Amazon FSx ONTAP浮動 IP 範圍的路由"浮動IP"。
   - Cloud Volumes ONTAP的浮動 IP 範圍的路由（如果適用）。
   - 新建立的外部 VPC 位址空間的路由。



8. 最後，允許雙向流量"防火牆規則"用於存取 FSx/CVO。遵循這些"詳細步驟"用於 SDDC 工作負載連線的運算網關防火牆規則。



9. 為管理和運算網關配置防火牆群組後，可以如下存取 vCenter：



下一步是驗證是否根據您的要求配置了Amazon FSx ONTAP或Cloud Volumes ONTAP ，以及是否配置了磁碟區以從 vSAN 卸載儲存元件以最佳化部署。

在 **Azure** 上部署並配置虛擬化環境

與本機一樣，規劃 Azure VMware 解決方案對於成功建立 VM 和遷移的生產就緒環境至關重要。

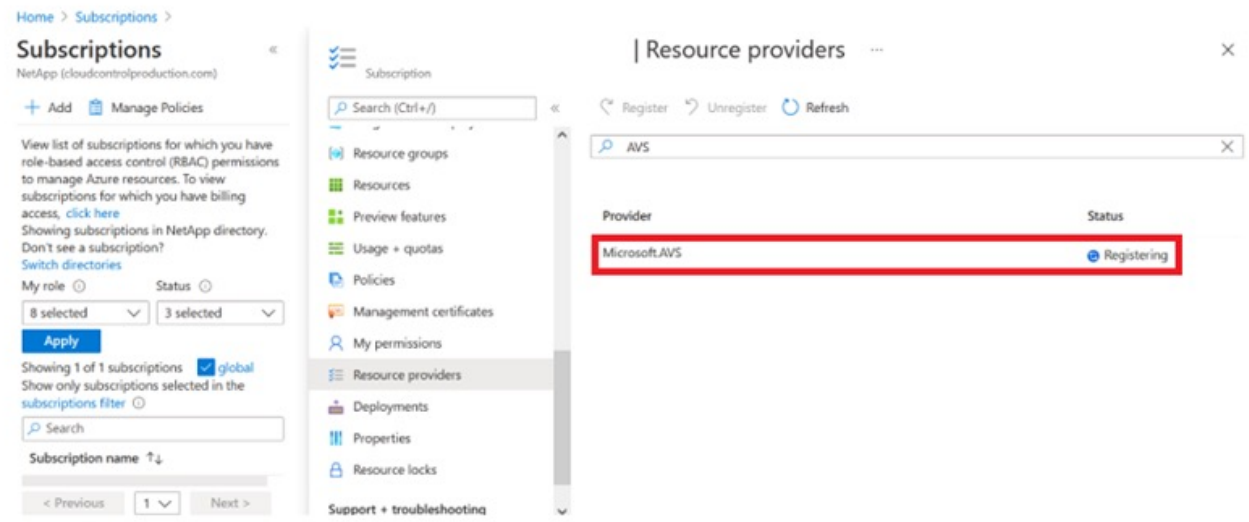
本部分介紹如何設定和管理 Azure VMware 解決方案，並將其與用於連接NetApp儲存裝置的可用選項結合使用。

設定過程可分為以下步驟：

▼ 註冊資源提供者並建立私有雲

若要使用 Azure VMware 解決方案，請先在已識別的訂閱中註冊資源提供者：

1. Sign inAzure 入口網站。
2. 在 Azure 入口網站功能表上，選擇「所有服務」。
3. 在「所有服務」對話方塊中，輸入訂閱，然後選擇「訂閱」。
4. 若要查看，請從訂閱清單中選擇訂閱。
5. 選擇資源提供者並在搜尋中輸入 Microsoft.AVS。
6. 如果資源提供者尚未註冊，請選擇註冊。

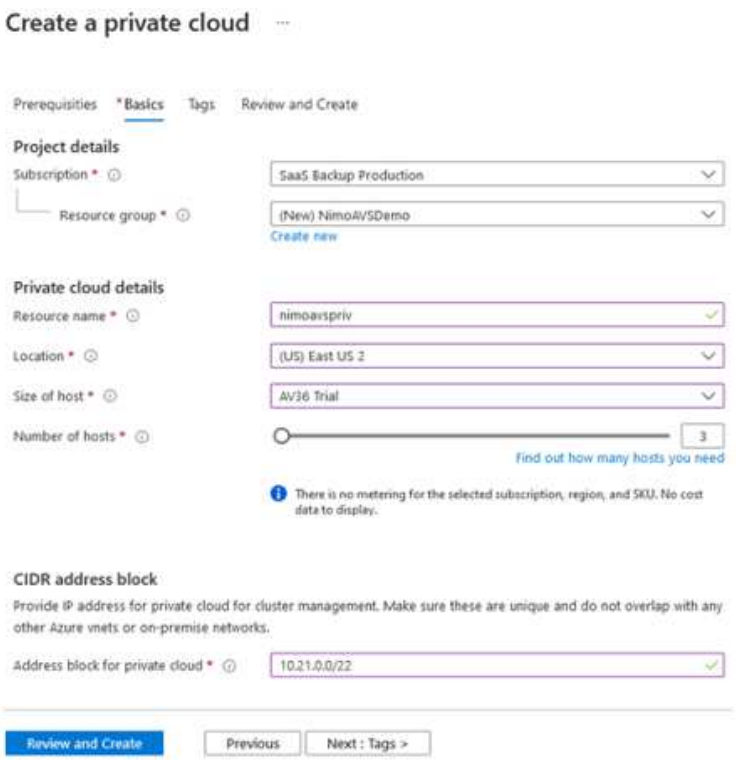




7. 註冊資源提供者後，使用 Azure 入口網站建立 Azure VMware 解決方案私有雲。
8. Sign inAzure 入口網站。
9. 選擇建立新資源。
10. 在「搜尋市場」文字方塊中，輸入「Azure VMware 解決方案」並從結果中選擇它。
11. 在 Azure VMware 解決方案頁面上，選擇「建立」。
12. 在「基本資訊」標籤中，輸入欄位中的值並選擇「審閱 + 建立」。

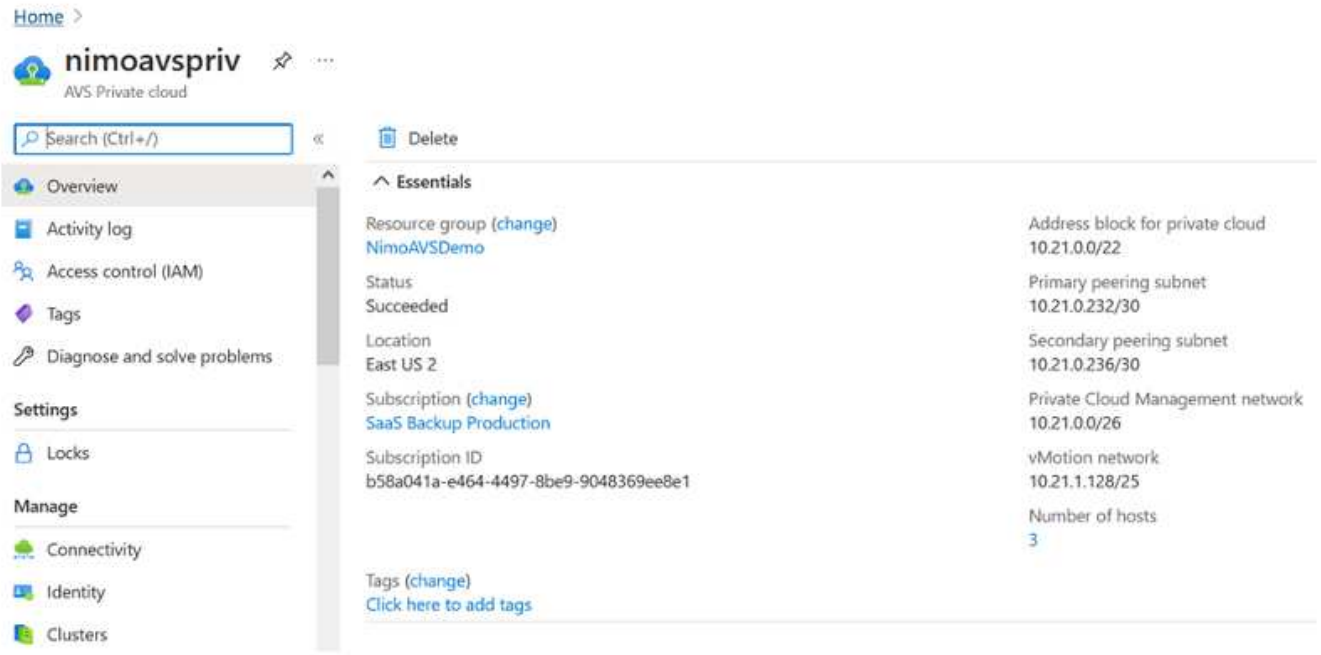
筆記：

- 為了快速啟動，請在規劃階段收集所需的資訊。
- 選擇現有資源群組或為私有雲建立新的資源群組。資源組是部署和管理 Azure 資源的邏輯容器。
- 確保 CIDR 位址是唯一的，並且不會與其他 Azure 虛擬網路或本機網路重疊。 CIDR 代表私有雲管理網絡，用於叢集管理服務，例如 vCenter Server 和 NSX-T Manager。 NetApp建議使用 /22 位址空間。在此範例中，使用 10.21.0.0/22。



配置過程大約需要 4 至 5 小時。流程完成後，透過從 Azure 入口網站存取私有雲來驗證部署是否成功。部署完成後將顯示「成功」狀態。

Azure VMware 解決方案私有雲需要 Azure 虛擬網路。由於 Azure VMware 解決方案不支援本機 vCenter，因此需要執行額外的步驟才能與現有的本機環境整合。還需要設定 ExpressRoute 線路和虛擬網路網關。在等待叢集預配完成時，建立一個新的虛擬網路或使用現有的虛擬網路連接到 Azure VMware 解決方案。



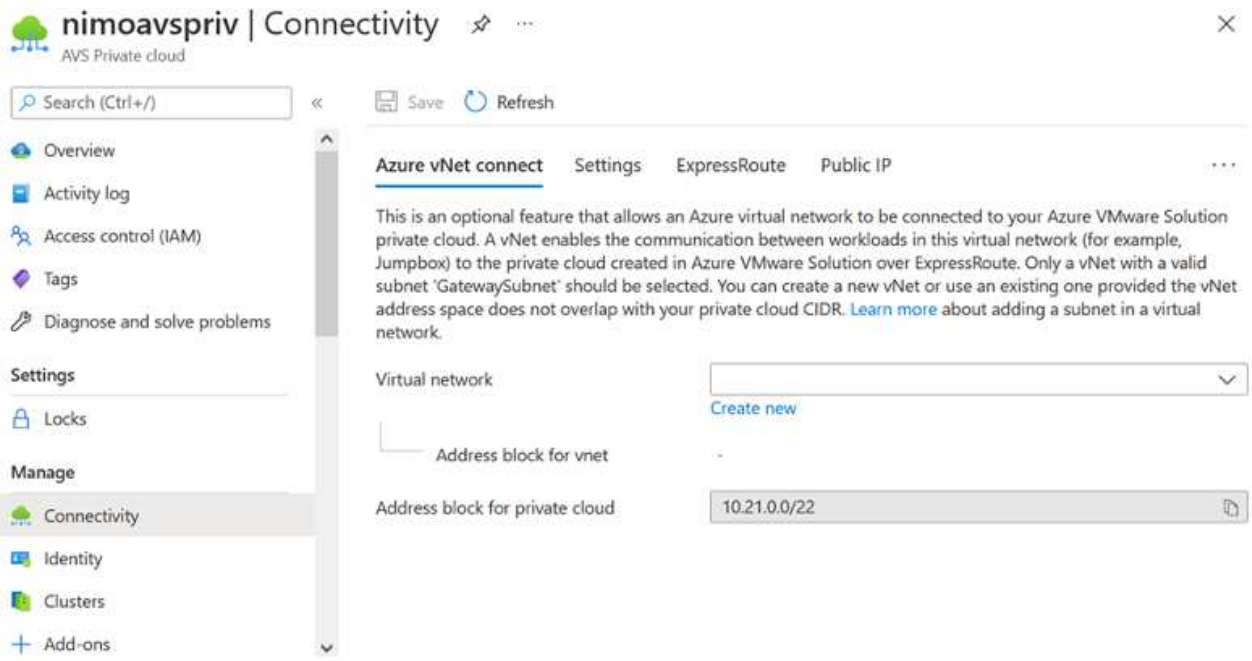
▼ 連接到新的或現有的 **ExpressRoute** 虛擬網路網關

若要建立新的 Azure 虛擬網路 (VNet)，請選擇 Azure VNet Connect 標籤。或者，您也可以使用建立虛擬網路精靈從 Azure 入口網站手動建立一個：

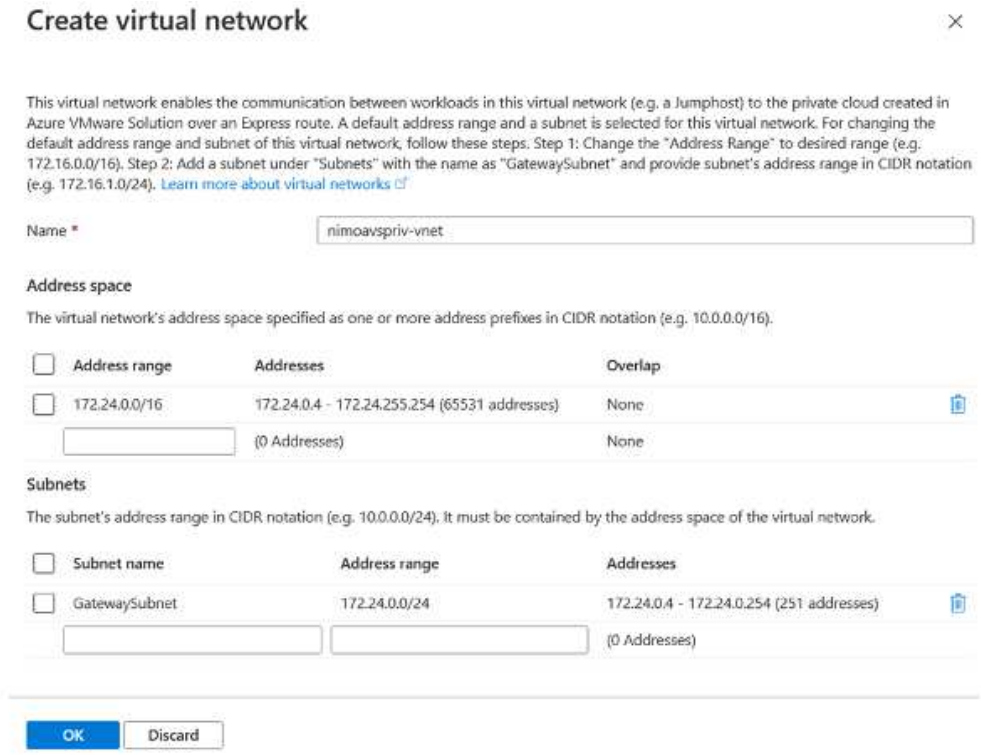
1. 前往 Azure VMware 解決方案私有雲並存取管理選項下的連線。
2. 選擇 Azure VNet Connect。
3. 若要建立新的 VNet，請選擇“新建”選項。

   此功能允許 VNet 連接到 Azure VMware 解決方案私有雲。 VNet 透過 ExpressRoute 自動為 Azure VMware 解決方案中建立的私有雲建立所需的元件（例如，跳躍框、共用服務（如Azure NetApp Files和 Cloud Volume ONTAP）），從而實現此虛擬網路中的工作負載之間的通訊。

   *注意：*VNet 位址空間不應與私有雲 CIDR 重疊。



4. 提供或更新新 VNet 的資訊並選擇「確定」。

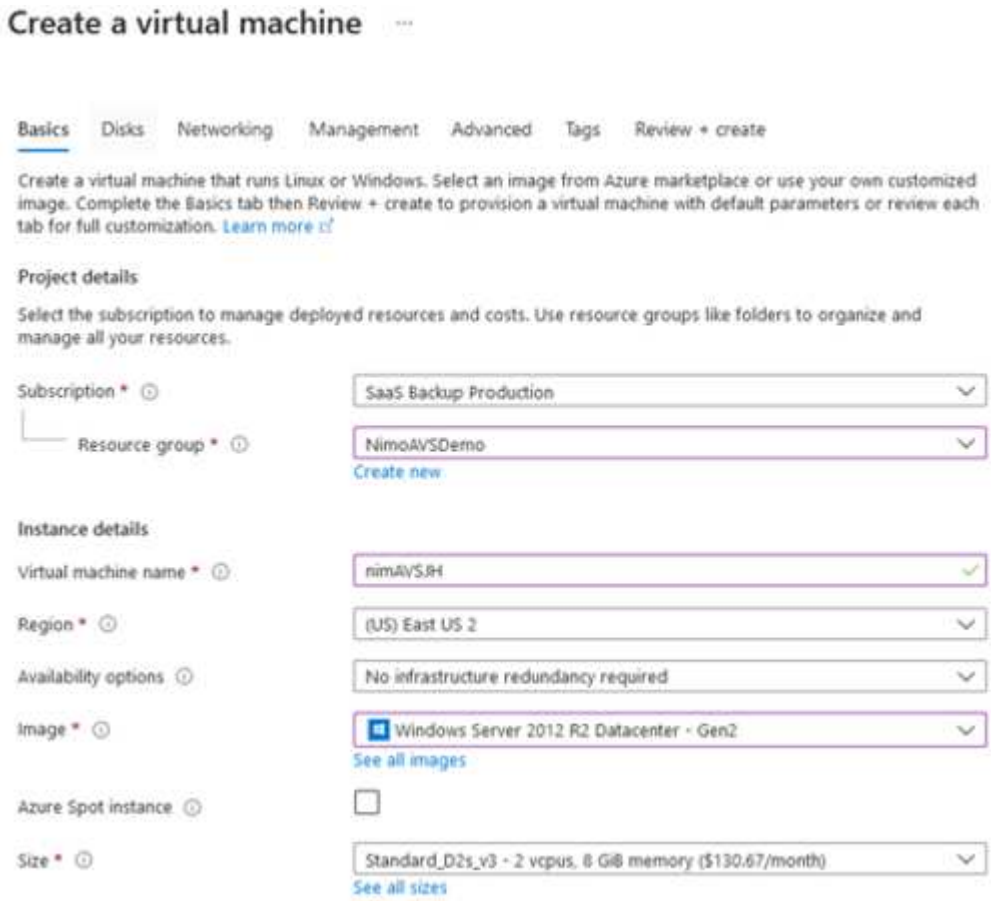


在指定的訂閱和資源群組中建立具有提供的位址範圍和網關子網路的 VNet。

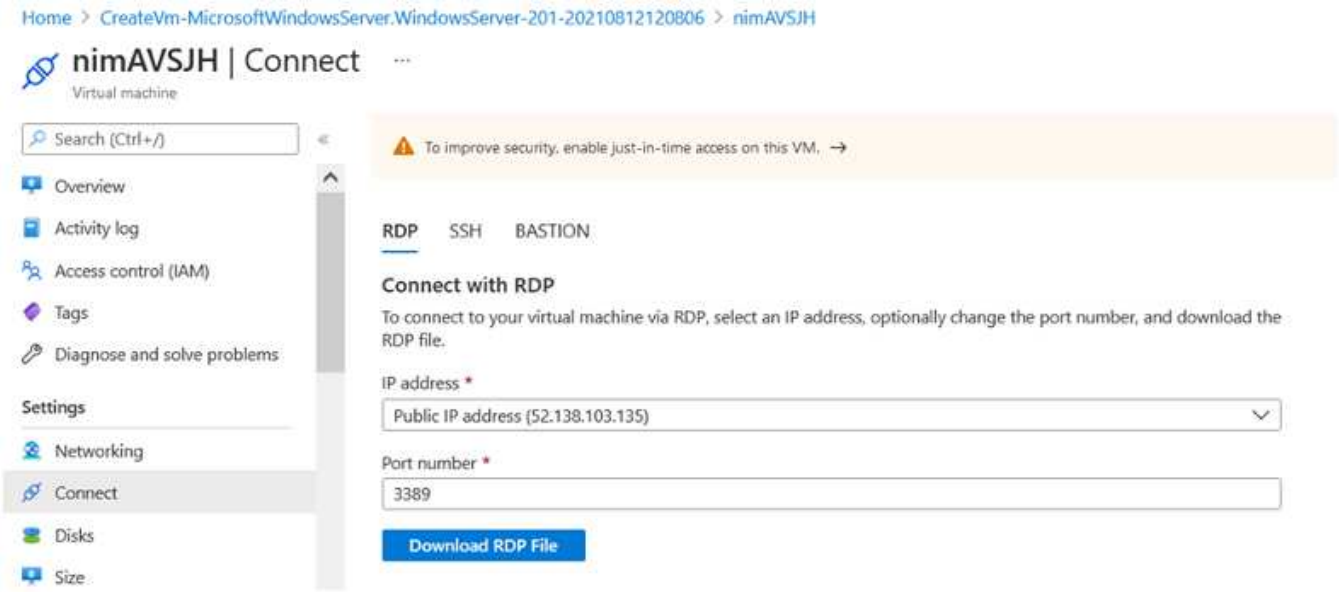
如果手動建立 VNet，請使用適當的 SKU 和 ExpressRoute 作為網關類型建立虛擬網路網關。部署完成後，使用授權金鑰將 ExpressRoute 連線連接到包含 Azure VMware 解決方案私有雲的虛擬網路閘道。有關更多信息，請參閱"在 Azure 中為 VMware 私有雲配置網絡" 。

▼ 驗證網路連線以及對 **Azure VMware** 解決方案私有雲的存取

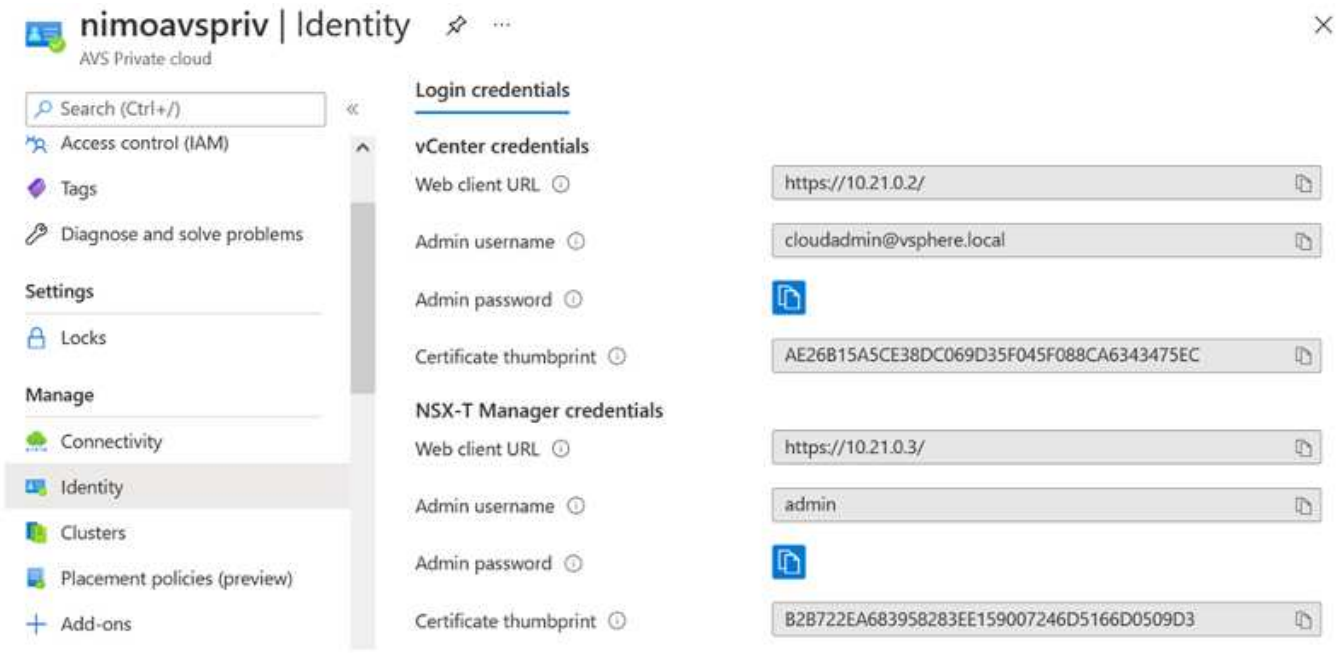
Azure VMware 解決方案不允許您使用本機 VMware vCenter 管理私有雲。相反，需要跳轉主機才能連線到 Azure VMware 解決方案 vCenter 執行個體。在指定的資源群組中建立跳轉主機並登入 Azure VMware 解決方案 vCenter。此跳轉主機應是為連線而建立的相同虛擬網路上的 Windows VM，並且應提供對 vCenter 和 NSX Manager 的存取權限。



配置虛擬機器後，使用「連線」選項存取 RDP。



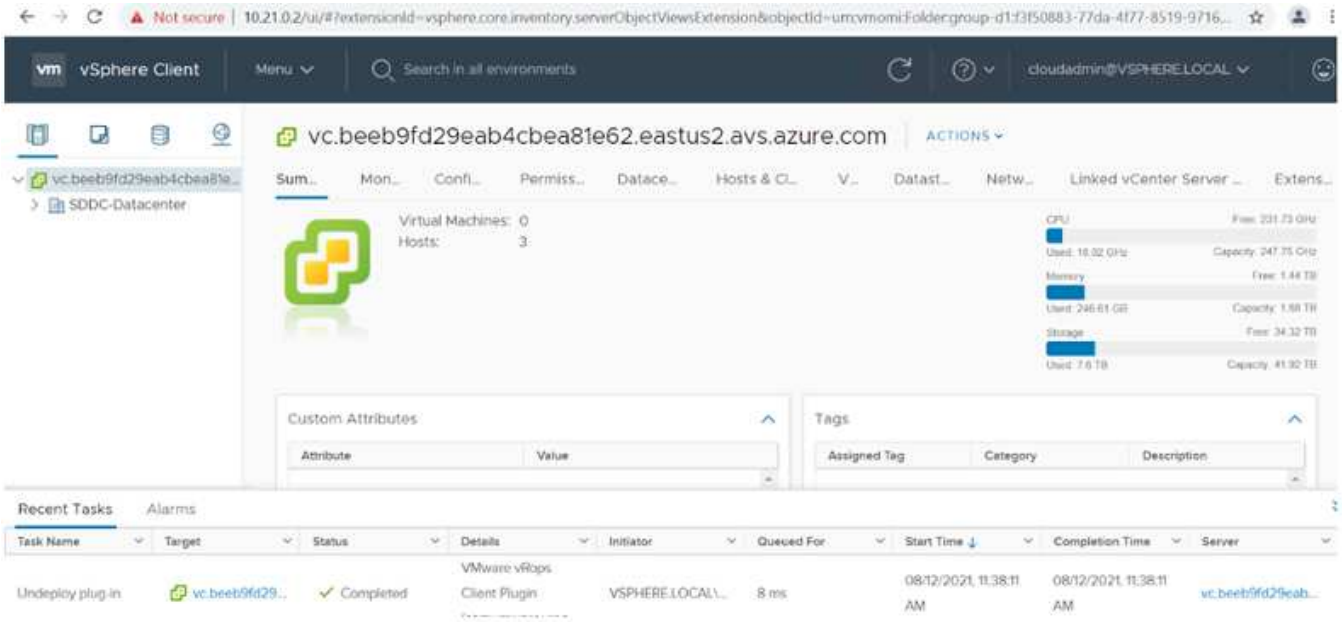
使用雲端管理員使用者從這個新建立的跳轉主機虛擬機器Sign invCenter。若要存取憑證，請前往 Azure 入口網站並導覽至「身分」（在私有雲中的「管理」選項下）。可以從這裡複製私有雲 vCenter 和 NSX-T 管理員的 URL 和使用者憑證。



在 Windows 虛擬機器中，開啟瀏覽器並導覽至 vCenter Web 用戶端 URL("`https://10.21.0.2/`") 並使用管理員使用者名稱為 **cloudadmin@vsphere.local** 並貼上複製的密碼。同樣，也可以使用 Web 用戶端 URL 存取 NSX-T 管理器("`https://10.21.0.3/`") 並使用管理員使用者名稱和貼上複製的密碼來建立新的段或修改現有的層網關。

對於每個配置的 SDDC，Web 用戶端 URL 都是不同的。





Azure VMware 解決方案 SDDC 現已部署並配置。利用 ExpressRoute Global Reach 將本機環境連接到 Azure VMware 解決方案私有雲。有關更多信息，請參閱"將本機環境與 Azure VMware 解決方案對等" 。

在 **Google Cloud Platform (GCP)** 上部署和配置虛擬化環境

與本地一樣，規劃 Google Cloud VMware Engine (GCVE) 對於成功建立虛擬機器和遷移的生產就緒環境至關重要。

本節介紹如何設定和管理 GCVE，以及如何將其與可用於連接NetApp儲存的選項結合使用。

設定過程可分為以下步驟：

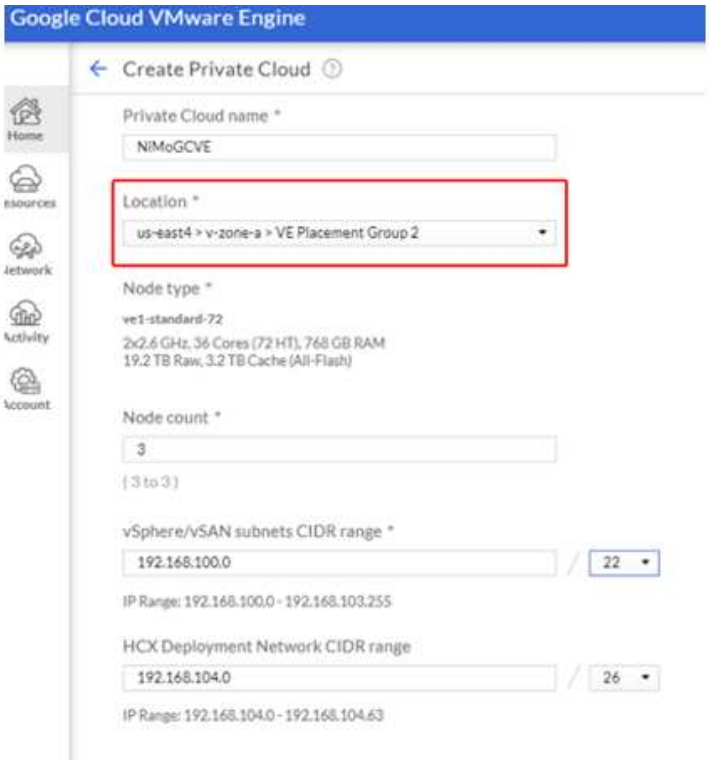
▼ 部署和配置 **GCVE**

若要在 GCP 上設定 GCVE 環境，請登入 GCP 控制台並存取 VMware Engine 入口網站。

點選「新建私有雲」按鈕，輸入GCVE私有雲所需的設定。在「位置」上，確保將私有雲部署在部署NetApp Volumes/CVO 的相同區域/區域中，以確保最佳效能和最低延遲。

先決條件：

- 設定 VMware Engine 服務管理員 IAM 角色
- "啟用 VMWare Engine API 存取和節點配額"
- 確保 CIDR 範圍不會與任何本地或雲端子網路重疊。 CIDR 範圍必須為 /27 或更高。



注意：私有雲建立可能需要 30 分鐘到 2 小時。

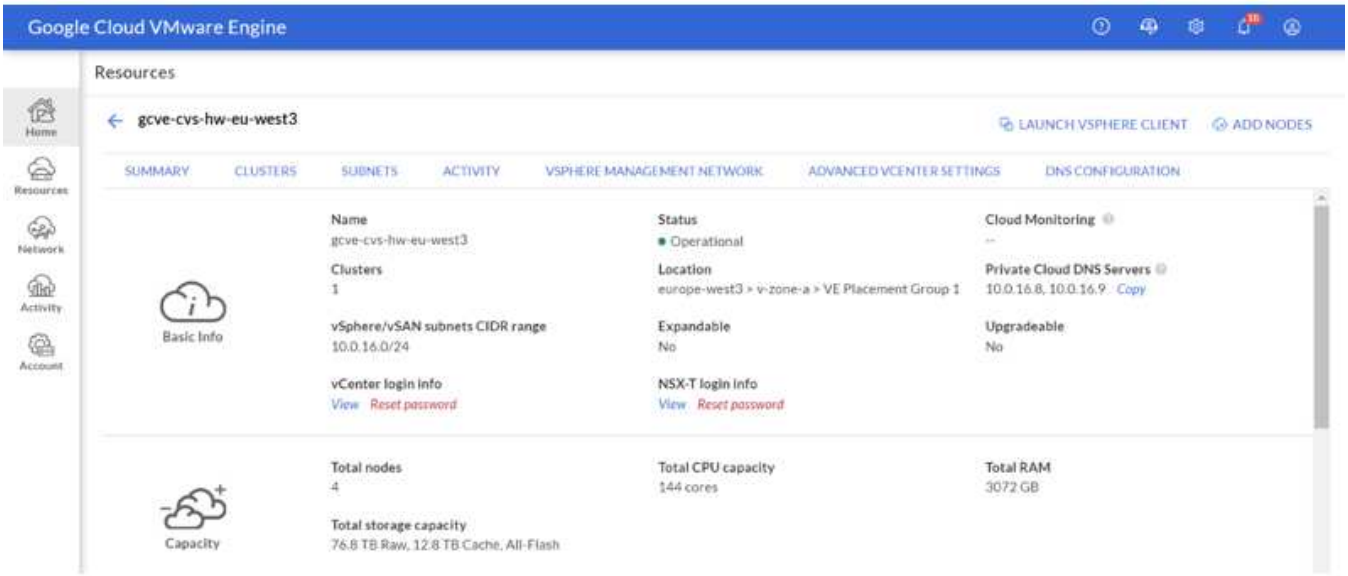
▼ 啟用對 **GCVE** 的私人訪問

一旦配置了私有雲，就配置對私有雲的私有訪問，以實現高吞吐量和低延遲的資料路徑連接。

這將確保執行 Cloud Volumes ONTAP 實例的 VPC 網路能夠與 GCVE 私有雲通訊。為此，請按照"GCP 文件"操作。對於 Cloud Volume Service，透過在租戶主機專案之間執行一次性對等關係，建立 VMware Engine 與 Google Cloud NetApp Volumes 之間的連線。如需詳細步驟，請參閱此"關聯"。

Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

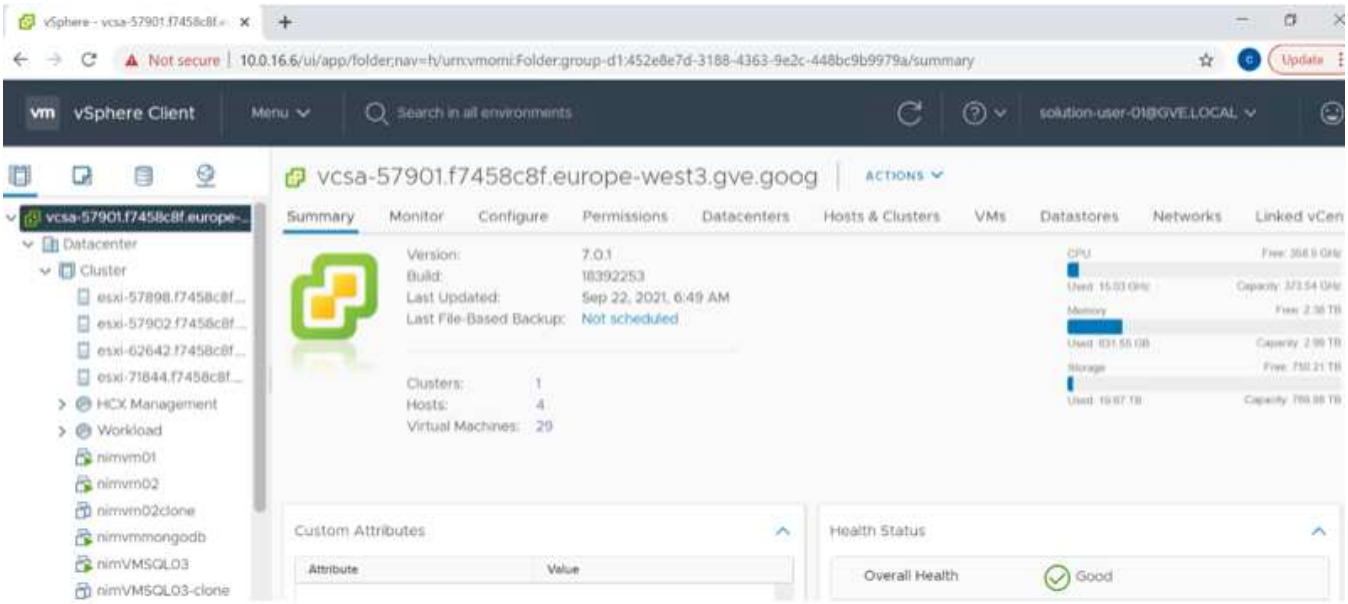
使用 CloudOwner@gve.local 使用者Sign invcenter。若要存取憑證，請前往 VMware Engine 門戶，前往資源，然後選擇適當的私有雲。在「基本資訊」部分中，按一下 vCenter 登入資訊（vCenter Server、HCX 管理員）或 NSX-T 登入資訊（NSX 管理員）的「檢視」連結。



在 Windows 虛擬機器中，開啟瀏覽器並導覽至 vCenter Web 用戶端 URL("`https://10.0.16.6/`") 並使用管理者使用者名稱作為 CloudOwner@gve.local 並貼上複製的密碼。同樣，也可以使用 Web 用戶端 URL 存取 NSX-T 管理器("`https://10.0.16.11/`") 並使用管理員使用者名稱和貼上複製的密碼來建立新的段或修改現有的層網關。

若要從本地網路連接到 VMware Engine 私有雲，請利用雲端 VPN 或 Cloud Interconnect 進行適當的連接，並確保所需的連接埠已開啟。有關詳細步驟，請依照"關聯"。





▼ 將**Google Cloud NetApp Volumes**補充資料儲存區部署到 **GCVE**

參考"使用NetApp磁碟區將補充 NFS 資料儲存部署到 GCVE 的過程"

公有雲中的**NetApp**存儲

面向公有雲提供者的**NetApp**儲存選項

探索NetApp在三大超大規模資料中心中作為儲存的選項。

AWS/VMC

AWS 支援以下配置的NetApp儲存：

- FSx ONTAP作為來賓連接存儲
- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- FSx ONTAP作為補充 NFS 資料存儲

查看詳細信息"VMC 的用戶機連線儲存選項"。查看詳細信息"VMC 的補充 NFS 資料儲存選項"。

Azure/AVS

Azure 支援以下配置的NetApp儲存體：

- Azure NetApp Files(ANF) 作為來賓連接儲存
- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- Azure NetApp Files(ANF) 作為補充 NFS 資料存儲

查看詳細信息"AVS 的來賓連線儲存選項"。查看詳細信息"AVS 的補充 NFS 資料儲存選項"。

良好操作規範/良好行為規範

Google Cloud 支援以下配置的NetApp儲存：

- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- Google Cloud NetApp Volumes （NetApp Volumes）作為來賓連接存儲
- Google Cloud NetApp Volumes （NetApp Volumes）作為補充 NFS 資料存儲

查看詳細信息"GCVE 的來賓連接儲存選項"。查看詳細信息"GCVE 的補充 NFS 資料儲存選項"。

閱讀更多"Google Cloud NetApp Volumes資料儲存區支援 Google Cloud VMware Engine（NetApp部落格）"或者"如何將Google Cloud NetApp Volumes用作 Google Cloud VMware Engine 的資料儲存區（Google部落格）"

Amazon Web Services：使用**NetApp**儲存的選項

NetApp儲存可以作為來賓連接儲存或補充儲存附加到 Amazon Web Services。

Amazon FSx for NetApp ONTAP (FSx ONTAP) 作為補充 NFS 資料存儲

Amazon FSx ONTAP提供了部署和管理應用程式工作負載以及檔案服務的絕佳選項，同時透過將資料需求無縫連接到應用程式層來降低 TCO。無論使用情況如何，選擇 VMware Cloud on AWS 以及Amazon FSx ONTAP都可以快速實現雲端優勢、一致的基礎架構和從本地到 AWS 的操作、工作負載的雙向可移植性以及企業級容量和效能。它與連接儲存所使用的過程和程序相同。

欲了解更多信息，請訪問：

- "FSx ONTAP作為補充 NFS 資料儲存：概述"
- "Amazon FSx for ONTAP作為補充資料存儲"

Amazon FSx for NetApp ONTAP作為來賓連接存儲

Amazon FSx ONTAP是一項完全託管的服務，它基於 NetApp 流行的ONTAP檔案系統構建，提供高度可靠、可擴展、高效且功能豐富的檔案儲存。 FSx ONTAP將NetApp檔案系統的熟悉功能、效能、功能和 API 操作與完全託管的 AWS 服務的靈活性、可擴充性和簡單性相結合。

FSx ONTAP提供功能豐富、快速且靈活的共享文件存儲，可從在 AWS 或本地運行的 Linux、Windows 和 macOS 計算實例廣泛存取。 FSx ONTAP提供具有亞毫秒延遲的高效能固態硬碟 (SSD) 儲存。借助 FSx ONTAP，您可以為您的工作負載實現 SSD 等級的效能，同時只需為一小部分資料支付 SSD 儲存費用。

使用 FSx ONTAP管理資料更容易，因為您只需點擊按鈕即可快照、複製和複製檔案。此外，FSx ONTAP會自動將您的資料分層到成本較低的彈性儲存中，從而減少您配置或管理容量的需要。

FSx ONTAP還提供高可用性和持久性存儲，具有完全託管的備份和跨區域災難復原支援。為了更輕鬆地保護和保護您的數據，FSx ONTAP支援流行的資料安全和防毒應用程式。

欲了解更多信息，請訪問"FSx ONTAP作為來賓連接存儲"

Cloud Volumes ONTAP (CVO) 作為來賓連接存儲

Cloud Volumes ONTAP（或稱 CVO）是基於 NetApp 的ONTAP儲存軟體所建置的業界領先的雲端資料管理解決方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的軟體定義版本，使用雲端原生存儲，允許您在雲端和本地使用相同的存儲軟體，從而無需重新培

訓 IT 人員採用全新方法來管理資料。

CVO 使客戶能夠無縫地將資料從邊緣移動到資料中心、雲端並返回，從而將您的混合雲整合在一起 - 所有這些都透過單一窗格管理控制台NetApp Cloud Manager 進行管理。

透過設計，CVO 可提供極高的效能和先進的資料管理功能，以滿足您在雲端中最嚴苛的應用程式的需求。

欲了解更多信息，請訪問"CVO 作為客戶連接存儲"。

TR-4938：使用 **VMware Cloud on AWS** 將**Amazon FSx ONTAP**掛載為 **NFS** 資料存儲

本文檔概述如何使用 VMware Cloud on AWS 將Amazon FSx ONTAP作為 NFS 資料儲存掛載。

介紹

每個成功的組織都走在轉型和現代化的道路上。作為此過程的一部分，公司通常使用其現有的 VMware 投資來利用雲端優勢並探索如何盡可能無縫地遷移、爆發、擴展和為流程提供災難復原。遷移到雲端的客戶必須評估彈性和爆發、資料中心退出、資料中心整合、生命週期終止場景、合併、收購等用例。

儘管 VMware Cloud on AWS 是大多數客戶的首選，因為它為客戶提供了獨特的混合功能，但有限的本機儲存選項限制了它對儲存工作負載繁重的組織的實用性。由於儲存直接與主機綁定，因此擴展儲存的唯一方法是添加更多主機，這可能會使儲存密集型工作負載的成本增加 35-40% 或更多。這些工作負載需要額外的儲存和隔離效能，而不是額外的馬力，但這意味著需要支付額外的主機費用。這就是 "最近的整合"FSx ONTAP對於使用 VMware Cloud on AWS 的儲存和效能密集型工作負載非常有用。

讓我們考慮以下場景：客戶需要八台主機來提供馬力（vCPU/vMem），但他們對儲存也有很大的需求。根據他們的評估，他們需要 16 台主機來滿足儲存需求。這會增加整體 TCO，因為他們必須購買所有額外的馬力，而他們真正需要的只是更多的儲存空間。這適用於任何用例，包括遷移、災難復原、爆發、開發/測試等等。

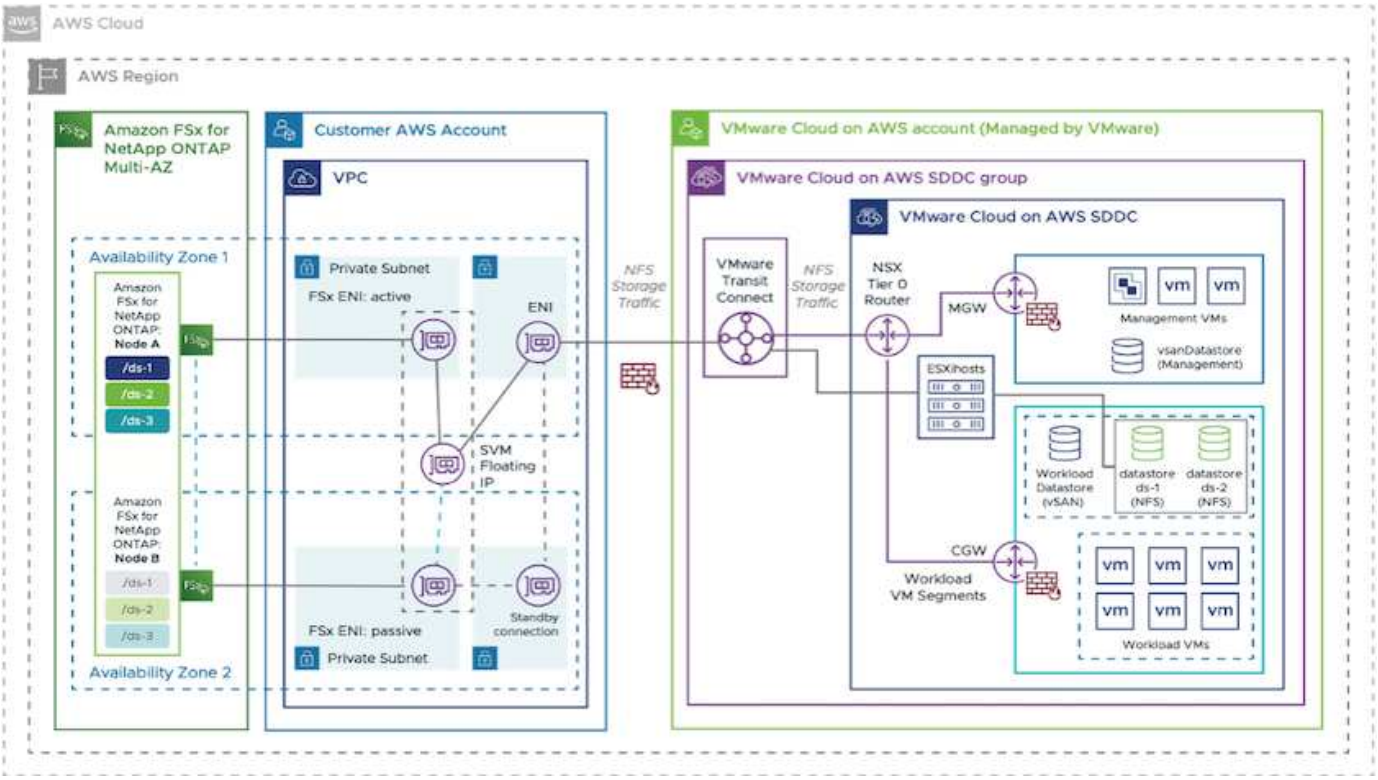
本文檔將引導您完成將 FSx ONTAP配置並連接為 VMware Cloud on AWS 的 NFS 資料儲存所需的步驟。

VMware 也提供此解決方案。請訪問"VMware Cloud on AWS 文檔"了解更多。

連線選項

VMware Cloud on AWS 支援 FSx ONTAP的多可用區和單一可用區部署。

本節介紹進階連接架構以及實施解決方案所需的步驟，以擴展 SDDC 叢集中的存儲，而無需添加其他主機。



進階部署步驟如下：

1. 在新的指定 VPC 中建立Amazon FSx ONTAP 。
2. 建立 SDDC 組。
3. 建立 VMware Transit Connect 和 TGW 附件。
4. 配置路由（AWS VPC 和 SDDC）和安全群組。
5. 將 NFS 磁碟區作為資料儲存附加到 SDDC 叢集。

在將 FSx ONTAP配置並連接為 NFS 資料儲存之前，您必須先設定 VMware on Cloud SDDC 環境或將現有 SDDC 升級至 v1.20 或更高版本。有關更多信息，請參閱"VMware Cloud on AWS 入門" 。

FSx ONTAP目前不支援延伸叢集。

結論

本文檔介紹了使用 AWS 上的 VMware 雲端配置Amazon FSx ONTAP所需的步驟。 Amazon FSx ONTAP提供了部署和管理應用程式工作負載以及檔案服務的絕佳選項，同時透過將資料需求無縫連接到應用程式層來降低 TCO。無論使用情況如何，選擇 VMware Cloud on AWS 以及Amazon FSx ONTAP都可以快速實現雲端優勢、一致的基礎架構和從本地到 AWS 的操作、工作負載的雙向可移植性以及企業級容量和效能。它與連接儲存所使用的過程和程序相同。請記住，只是資料的位置隨著新名稱而改變了；工具和流程都保持不變， Amazon FSx ONTAP有助於優化整體部署。

要了解有關此過程的更多信息，請隨意觀看詳細的演示視頻。

Amazon FSx ONTAP VMware 雲

VMware Cloud 準備好並連接到 AWS VPC 後，您必須將Amazon FSx ONTAP部署到新指定的 VPC 中，而不是原來連接的或現有的預設 VPC 中。

首先，在 SDDC 所在的相同區域和可用區中部署一個額外的 VPC，然後將Amazon FSx ONTAP部署到新的 VPC 中。 "VMware Cloud 中的 SDDC 群組的配置"控制台啟用連線到將部署 FSx ONTAP 的新指定的 VPC 所需的網路設定選項。

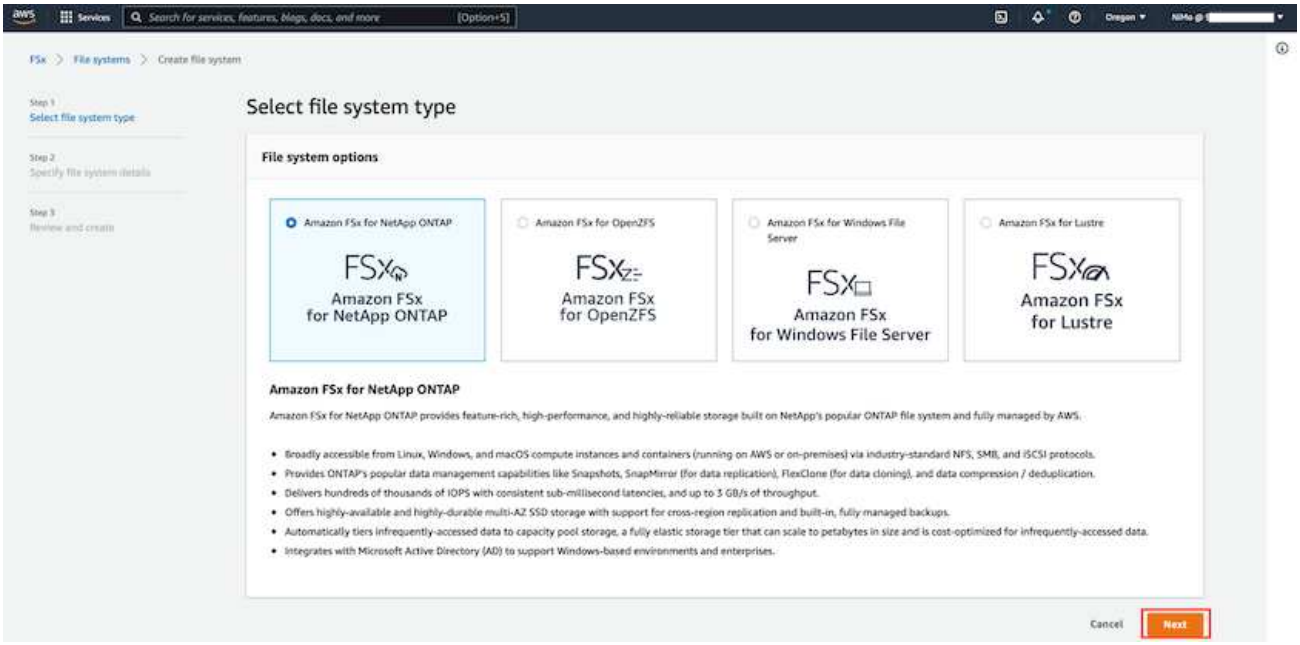
ⓘ 在與 VMware Cloud on AWS SDDC 相同的可用區域中部署 FSx ONTAP 。

ⓘ 您無法在已連線的 VPC 中部署 FSx ONTAP 。相反，您必須將其部署在新的指定 VPC 中，然後透過 SDDC 群組將 VPC 連接到 VMware Managed Transit Gateway (vTGW)。

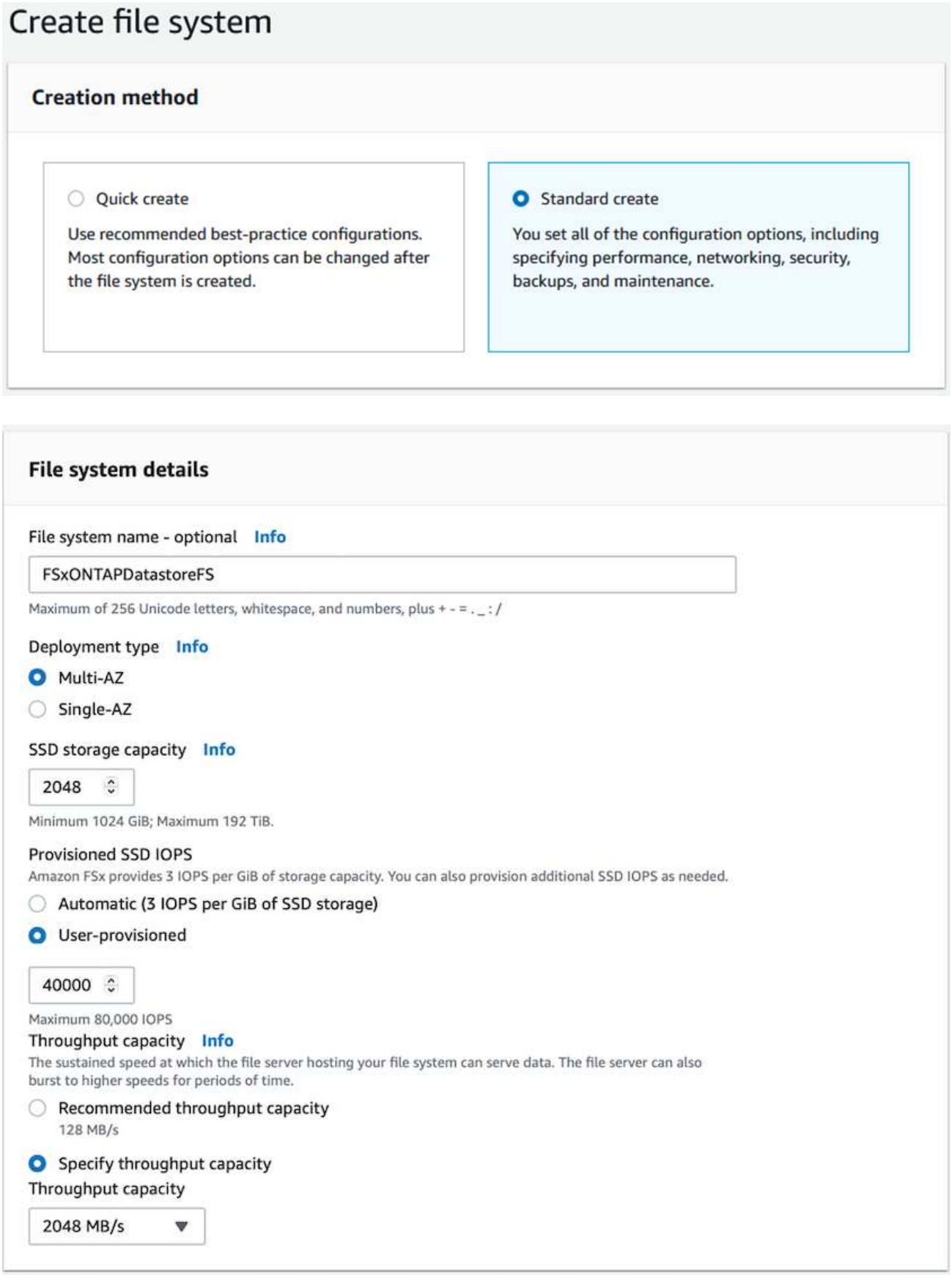
▼ 步驟 **1**：在新的指定 **VPC** 中建立**Amazon FSx ONTAP**

若要建立和掛載Amazon FSx ONTAP檔案系統，請完成下列步驟：

1. 開啟Amazon FSx控制台 `https://console.aws.amazon.com/fsx/`並選擇*建立檔案系統*來啟動*檔案系統建立*精靈。
2. 在選擇檔案系統類型頁面上，選擇 * Amazon FSx ONTAP*，然後按一下 下一步。出現「建立檔案系統」頁面。



3. 對於建立方法，選擇*標準建立*。



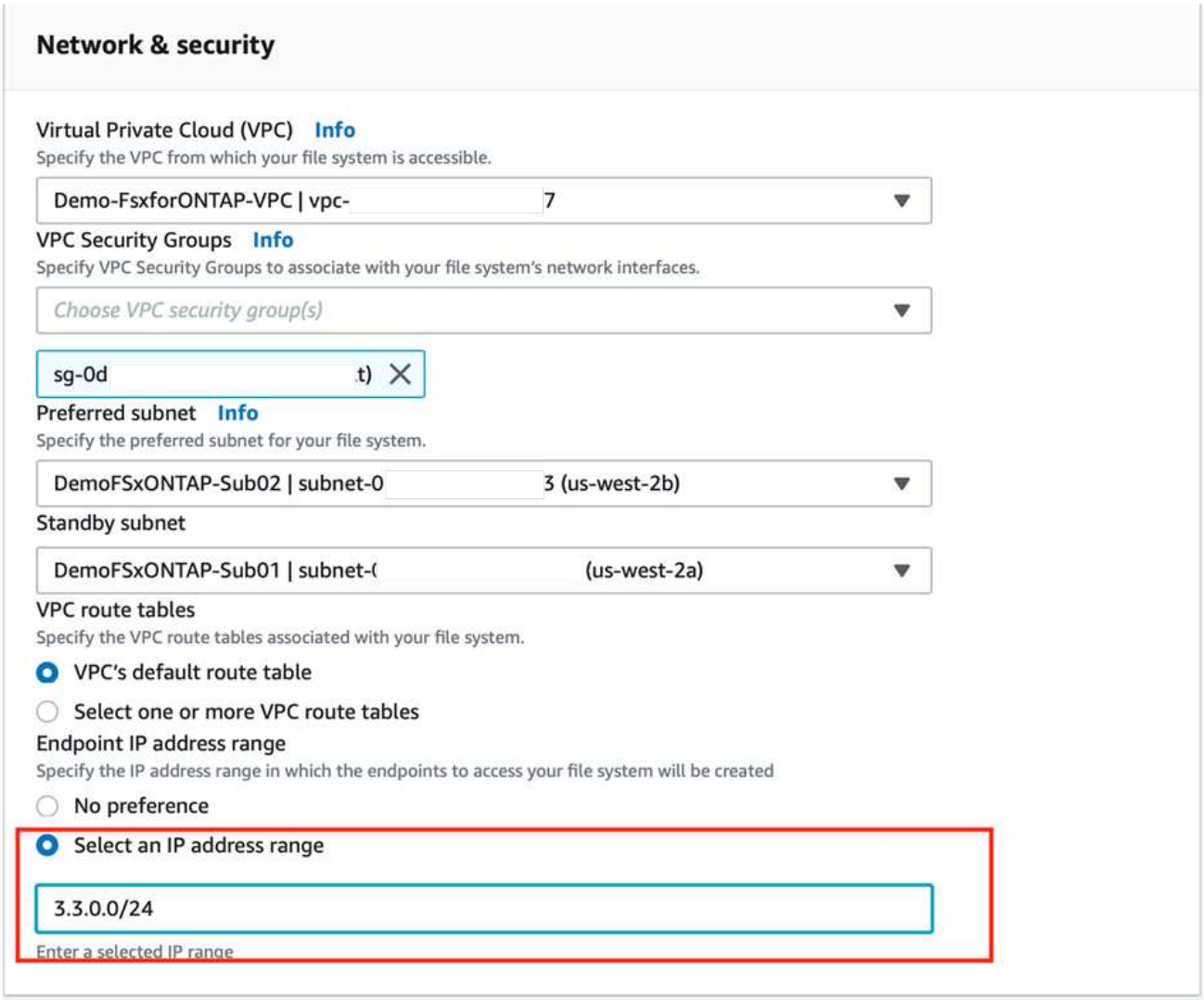
不同客戶的資料儲存大小差異很大。雖然每個 NFS 資料儲存區建議的虛擬機器數量是主觀的，但許多因素決定了可放置在每個資料儲存區上的虛擬機器的最佳數量。雖然大多數管

理員只考慮容量，但發送到 VMDK 的並發 I/O 量是影響整體效能的最重要因素之一。使用本地的效能統計資料來相應地調整資料儲存卷的大小。

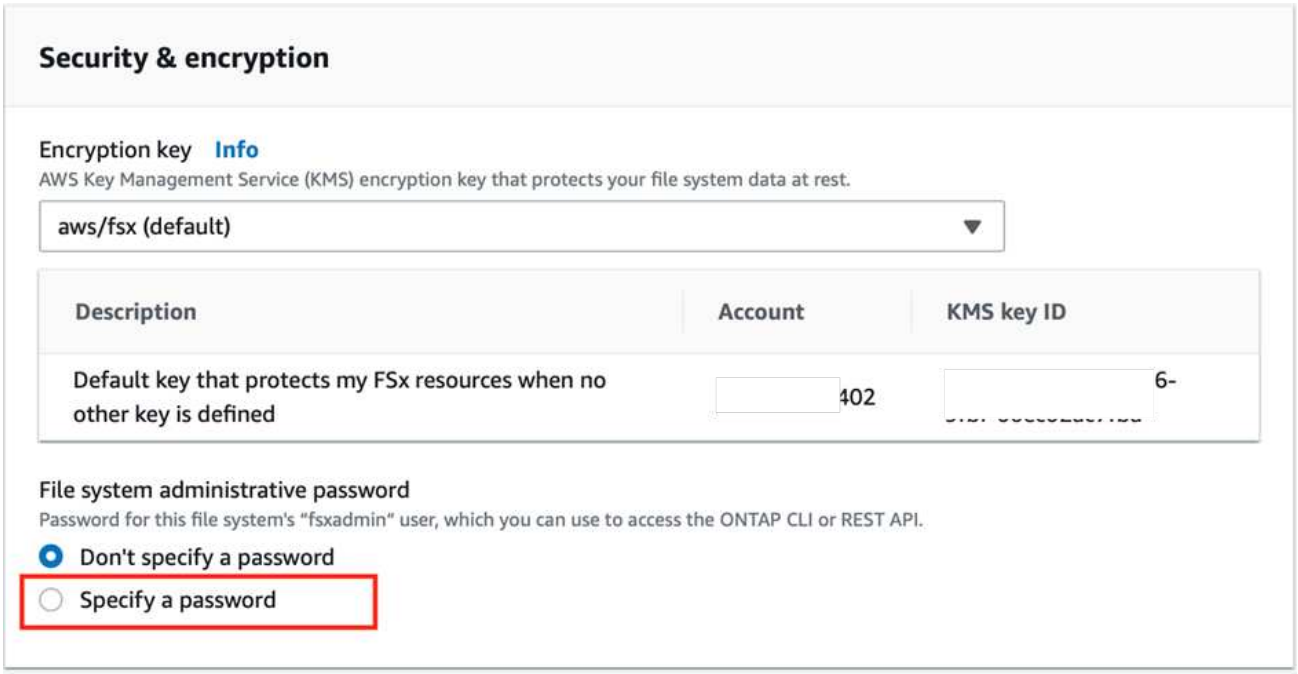
4. 在虛擬私有雲 (VPC) 的 網路 部分中，選擇適當的 VPC 和首選子網路以及路由表。在這種情況下，從下拉式選單中選擇 Demo-FSxforONTAP-VPC。

確保這是一個新的指定 VPC，而不是連接的 VPC。

預設情況下，FSx ONTAP使用 198.19.0.0/16 作為檔案系統的預設端點 IP 位址範圍。確保端點 IP 位址範圍與 AWS SDDC 上的 VMC、關聯的 VPC 子網路和本機基礎架構不衝突。如果您不確定，請使用沒有衝突的不重疊範圍。

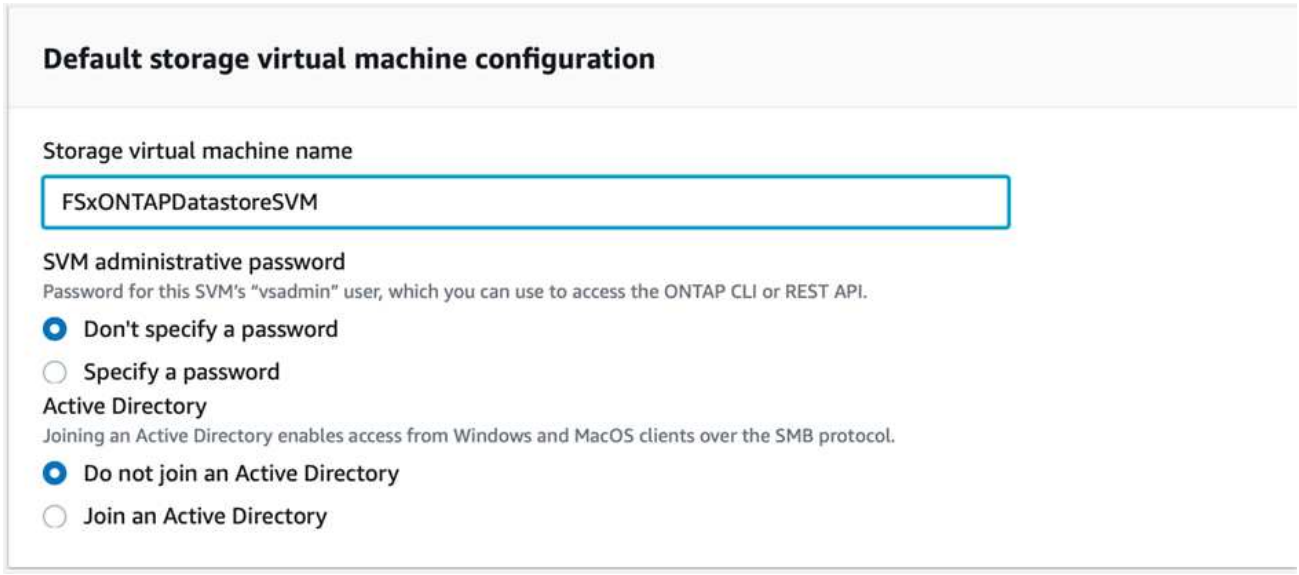


5. 在加密金鑰的「安全與加密」部分中，選擇保護檔案系統靜態資料的 AWS Key Management Service (AWS KMS) 加密金鑰。對於*檔案系統管理密碼*，請輸入 fsxadmin 使用者的安全密碼。



6. 在「預設儲存虛擬機器配置」部分中，指定 SVM 的名稱。

   從 GA 開始，支援四個 NFS 資料儲存。



7. 在「預設磁碟區配置」部分中，指定資料儲存所需的磁碟區名稱和大小，然後按一下「下一步」。這應該是一個 NFSv3 磁碟區。對於*儲存效率*，選擇*已啟用*以開啟ONTAP儲存效率功能（壓縮、重複資料刪除和壓縮）。建立完成後，使用shell使用*_volumemodify_*修改磁碟區參數，如下所示：

環境	配置
容量保證（空間保證方式）	無（精簡配置）– 預設設定
fractional_reserve（部分儲備）	0% – 預設設定
snap_reserve（快照空間百分比）	0%

環境	配置
自動調整大小（自動調整大小模式）	擴大_縮小
儲存效率	已啟用 – 預設設定
自動刪除	卷/oldest_first
卷分層策略	僅限快照 – 預設設定
嘗試先行	自動成長
快照策略	沒有任何

使用以下 SSH 命令建立和修改磁碟區：

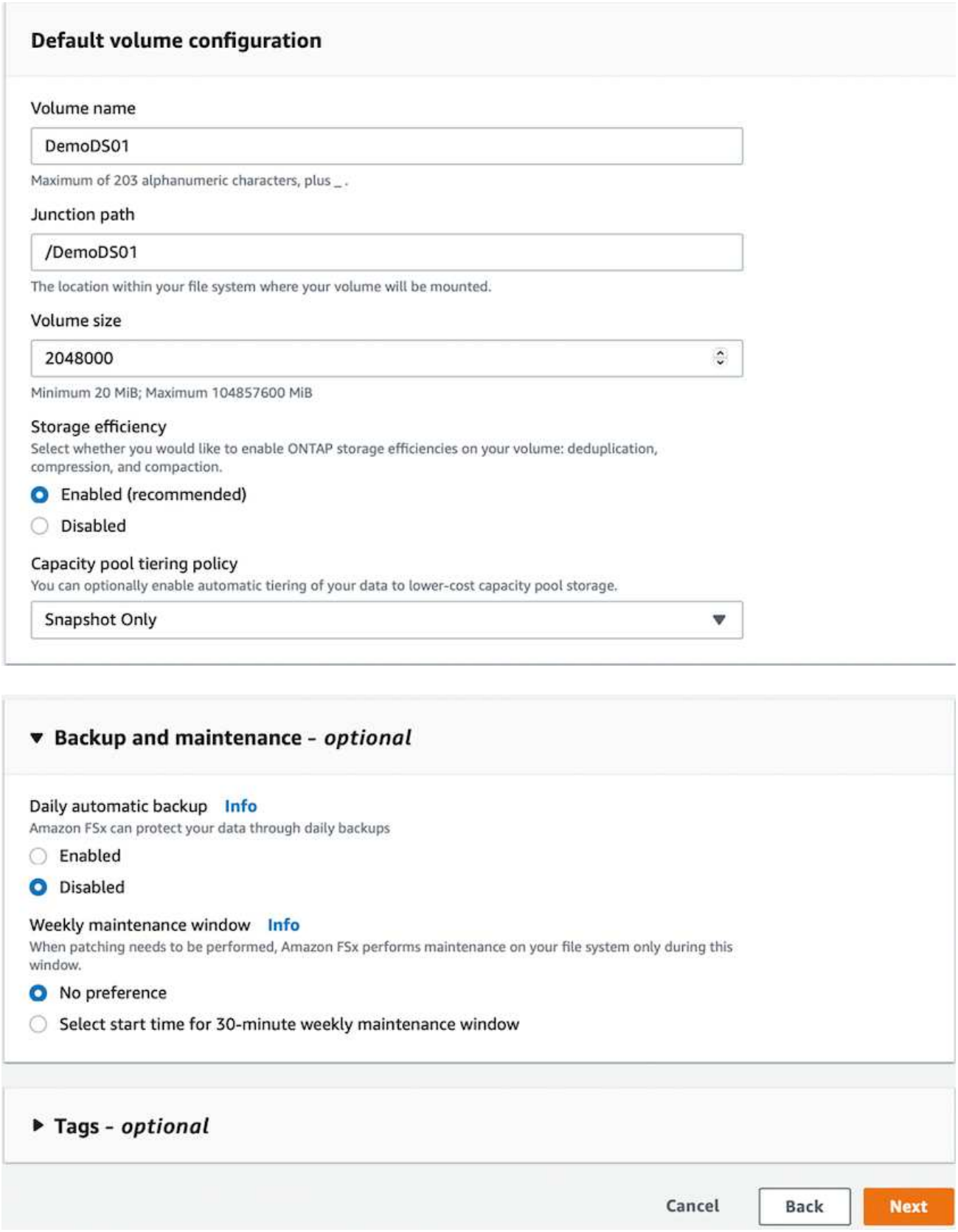
從 **shell** 建立新資料儲存卷的命令：

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy snapshot-
only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy
none -junction-path /DemoDS002
```

*注意：*透過 shell 建立的磁碟區將需要幾分鐘才能顯示在 AWS 控制台中。

修改預設未設定的音量參數的命令：

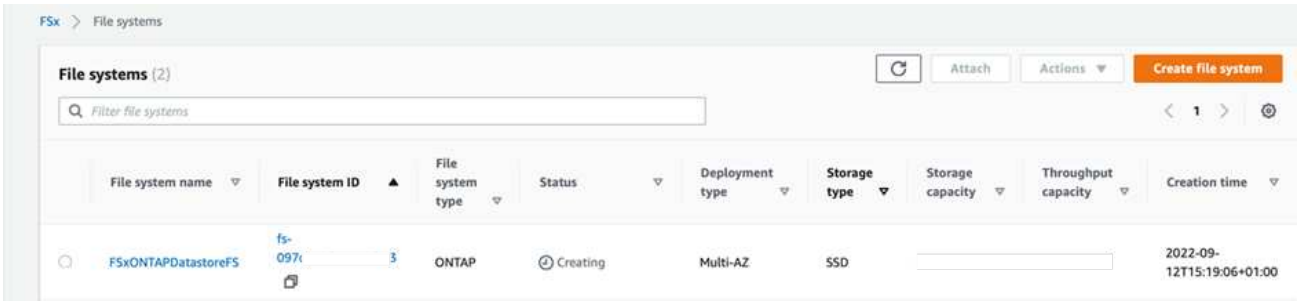
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```

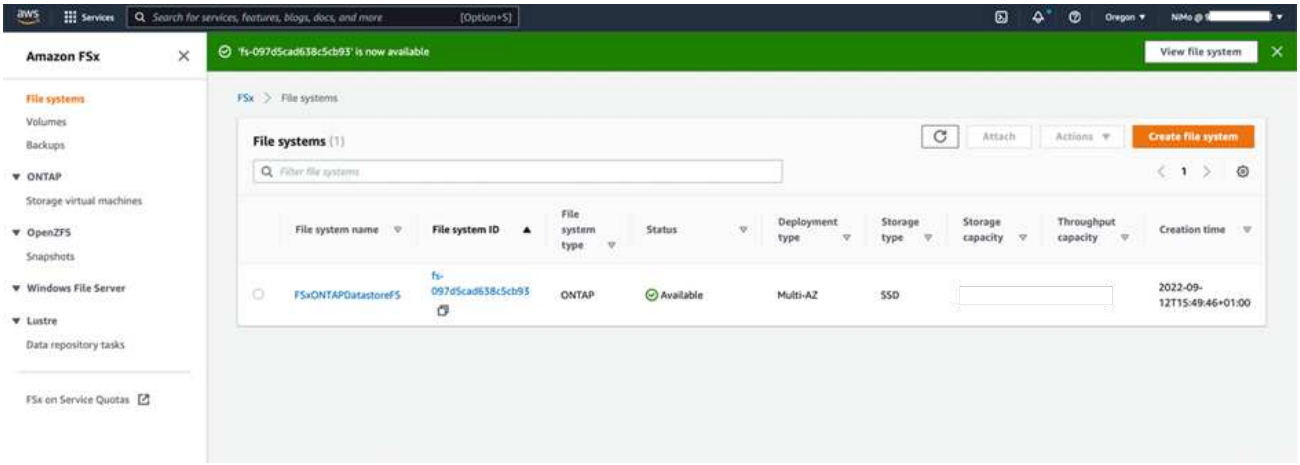


在初始遷移場景中，預設快照策略可能會導致資料儲存容量已滿的問題。為了克服這個問題，修改快照策略以滿足需求。

8. 查看「建立檔案系統」頁面上顯示的檔案系統配置。

9. 按一下“建立檔案系統”。





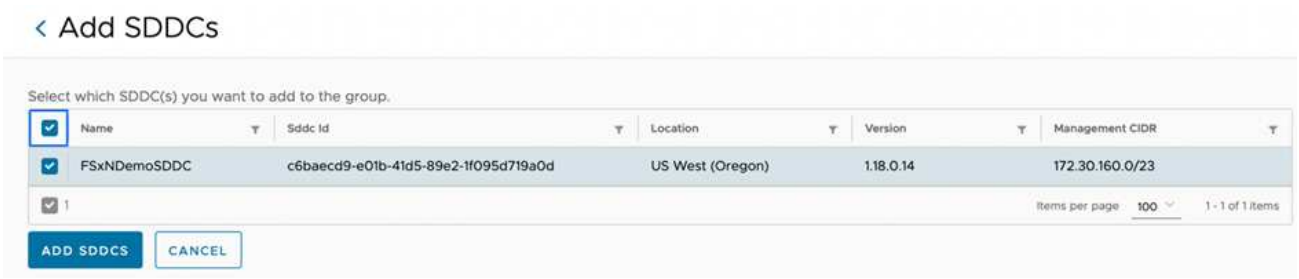
根據容量和效能要求重複上述步驟，建立更多儲存虛擬機器或檔案系統以及資料儲存磁碟區。

若要了解Amazon FSx ONTAP效能，請參閱 "Amazon FSx ONTAP效能"。

▼ 步驟 **2**：建立 **SDDC** 群組

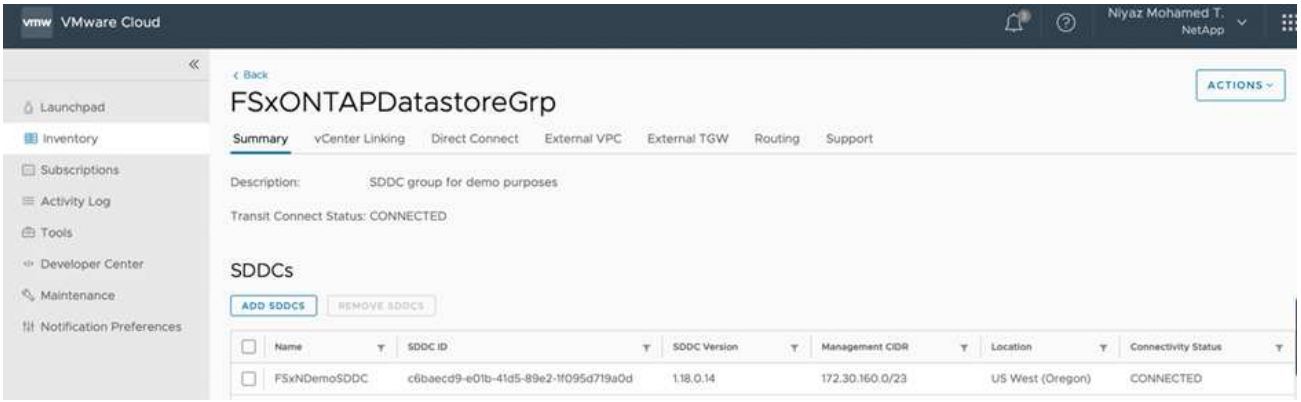
建立檔案系統和 SVM 後，使用 VMware Console 建立 SDDC 群組並設定 VMware Transit Connect。為此，請完成以下步驟，並記住必須在 VMware Cloud Console 和 AWS Console 之間導覽。

1. 登入 VMC 控制台 `https://vmc.vmware.com`。
2. 在「庫存」頁面上，按一下「**SDDC** 群組」。
3. 在 **SDDC Groups** 標籤上，按一下 **ACTIONS** 並選擇 **Create SDDC Group**。為了演示目的，SDDC 組被稱為 `FSxONTAPDatastoreGrp`。
4. 在成員資格網格上，選擇要作為群組成員包含的 SDDC。



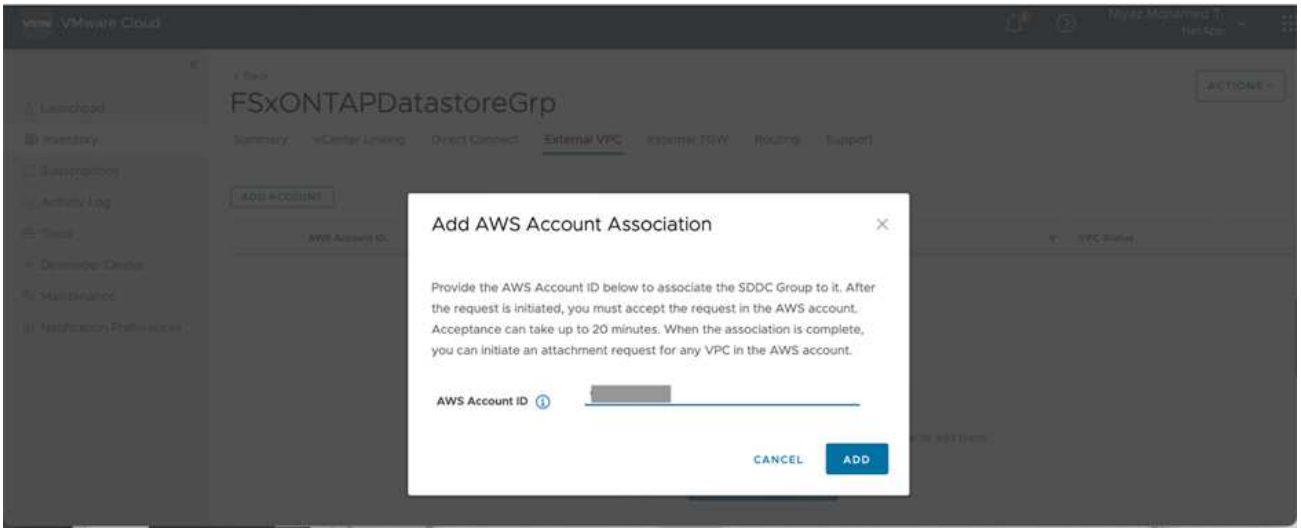
5. 驗證是否選取“為您的群組配置 VMware Transit Connect 將產生每個附件和資料傳輸的費用”，然後選擇*

建立群組*。過程可能需要幾分鐘才能完成。

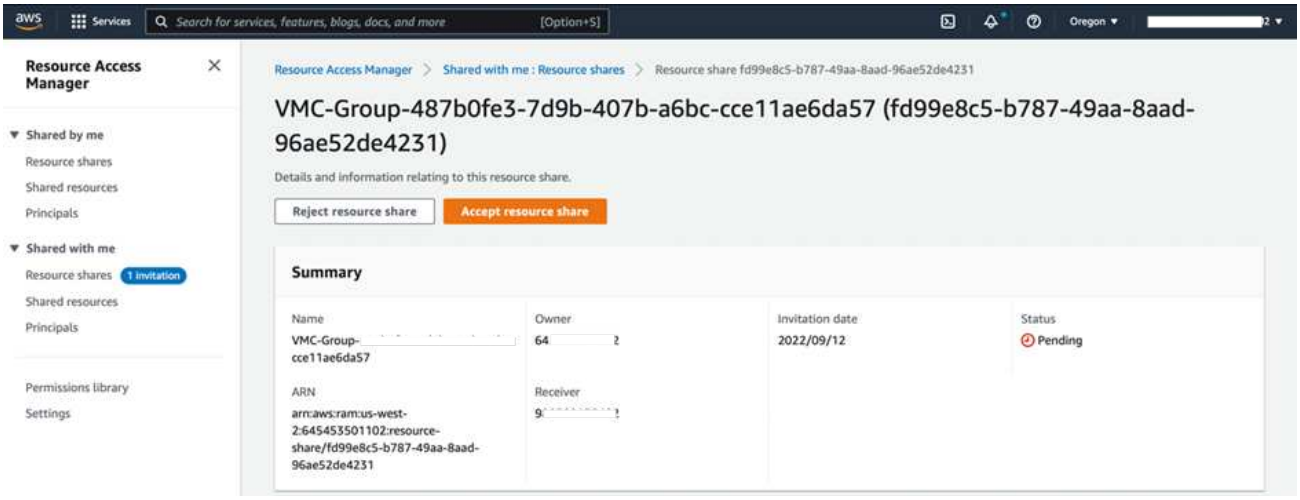


▼ 步驟 **3**：設定 **VMware Transit** 連接

1. 將新建立的指定 VPC 附加到 SDDC 群組。選擇“外部 VPC”標籤並按照 "將外部 VPC 附加到群組的說明 "。此過程可能需要 10-15 分鐘才能完成。

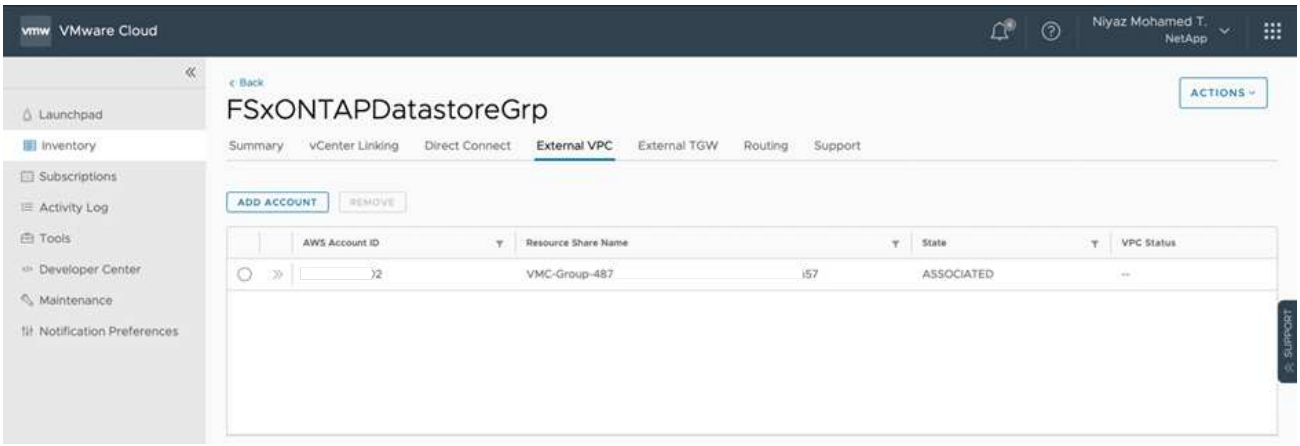


2. 按一下「新增帳戶」。
   a. 提供用於設定 FSx ONTAP檔案系統的 AWS 帳戶。
   b. 按一下“新增”。
3. 返回 AWS 控制台，登入同一個 AWS 帳戶並導覽至 資源存取管理器 服務頁面。有一個按鈕供您接受資源共享。



作為外部 VPC 流程的一部分，您將透過 AWS 主控台透過資源存取管理員提示新的共用資源。共享資源是由 VMware Transit Connect 管理的 AWS Transit Gateway。

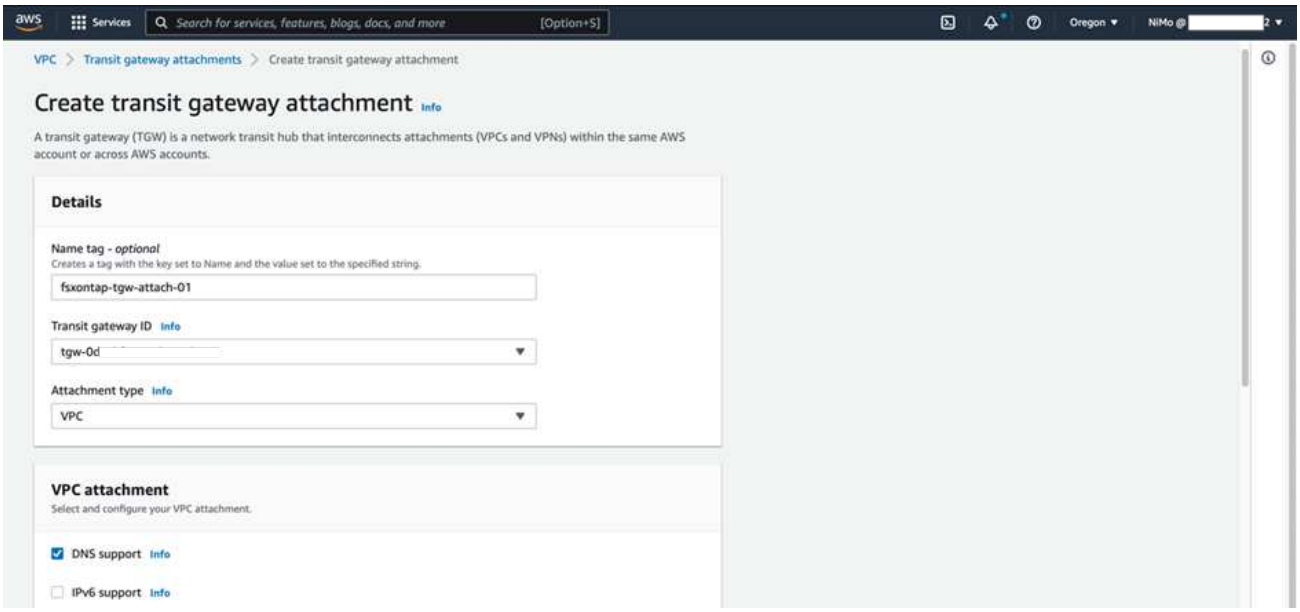
4. 點選*接受資源共享*。



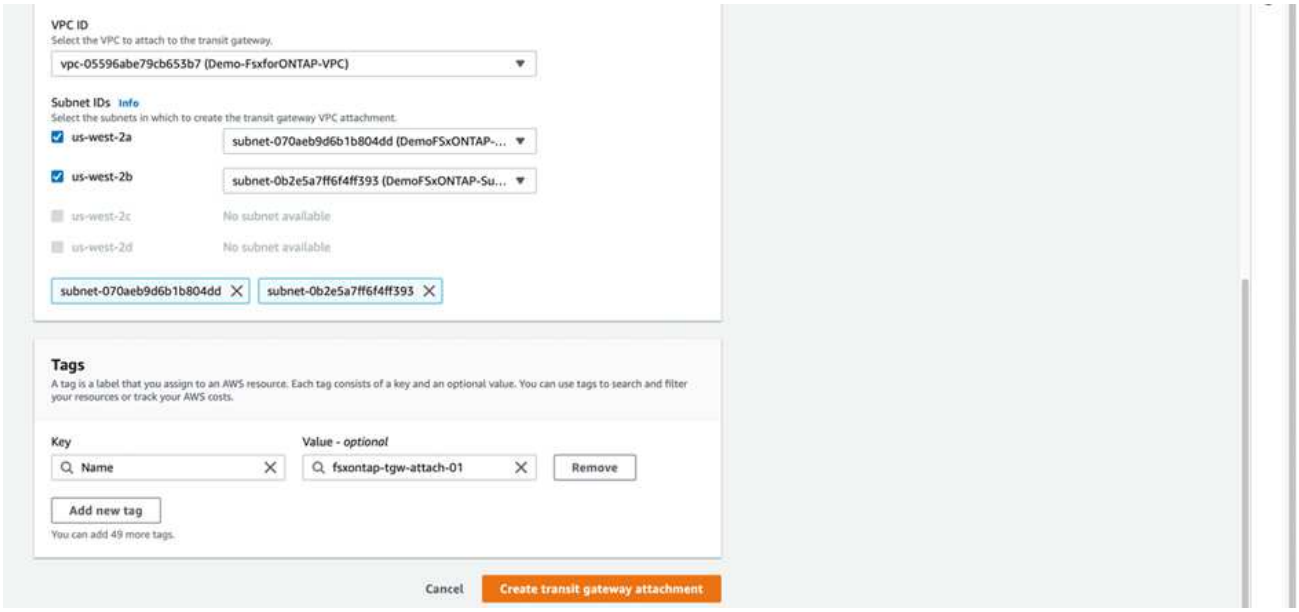
5. 回到 VMC 控制台，您現在看到外部 VPC 處於關聯狀態。這可能需要幾分鐘才能出現。

▼ 步驟 **4**：建立中轉網關連接

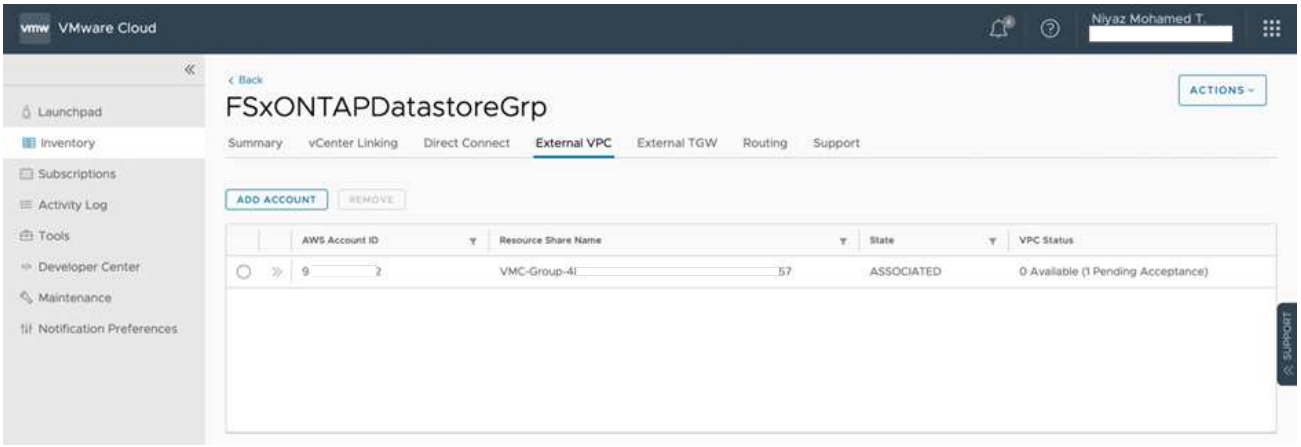
1. 在 AWS 控制台中，前往 VPC 服務頁面並導覽至用於設定 FSx 檔案系統的 VPC。在這裡，您可以透過點擊右側導覽窗格上的「**Transit Gateway Attachment**」來建立傳輸網關附件。
2. 在 **VPC** 附件 下，請確保選取 DNS 支援並選擇部署了 FSx ONTAP的 VPC。

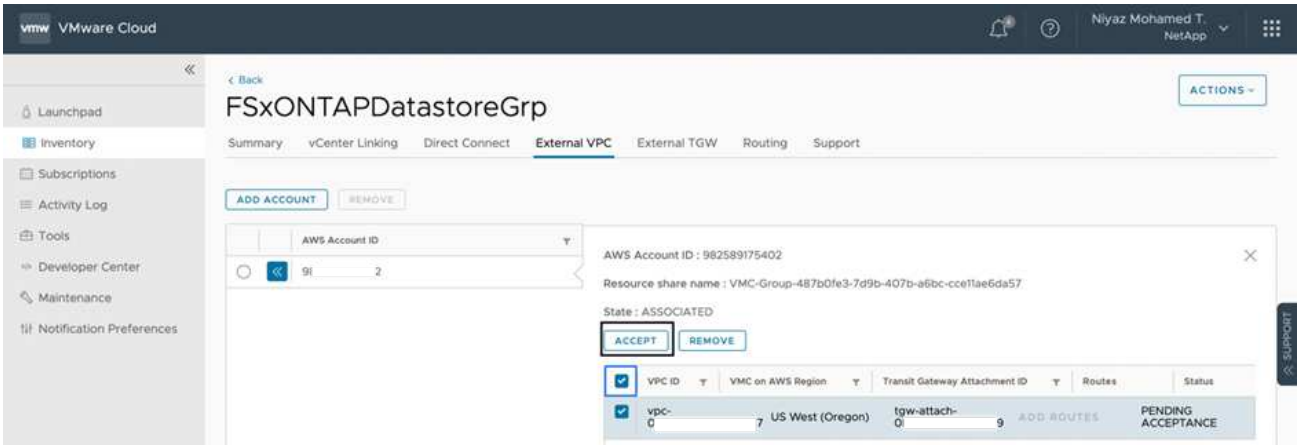


3. 按一下「建立」*「中轉網關附件」*。



4. 返回 VMware Cloud Console，導覽回 SDDC 群組 > 外部 VPC 標籤。選擇用於 FSx 的 AWS 帳戶 ID，按一下 VPC，然後按一下 接受。

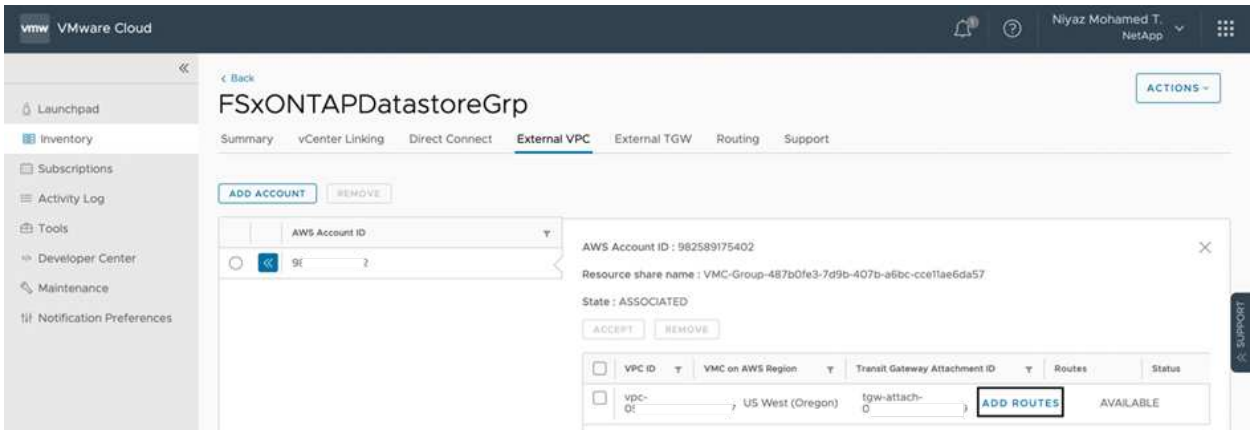


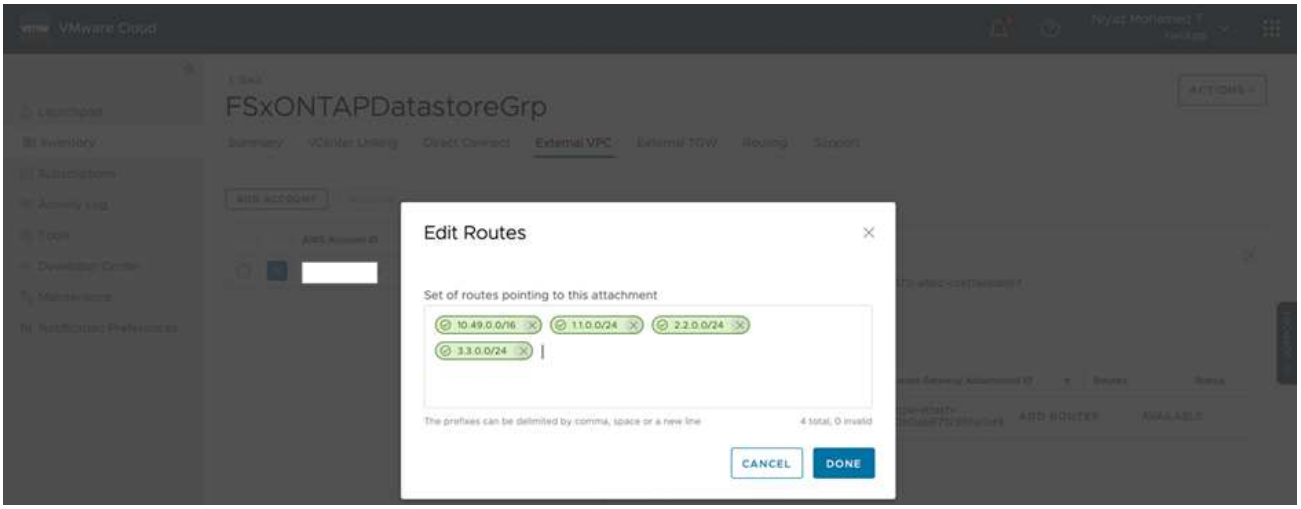


此選項可能需要幾分鐘才會出現。

5. 然後在 外部 **VPC** 標籤中的 路由 欄位中，按一下 新增路由 選項並新增所需的路由：

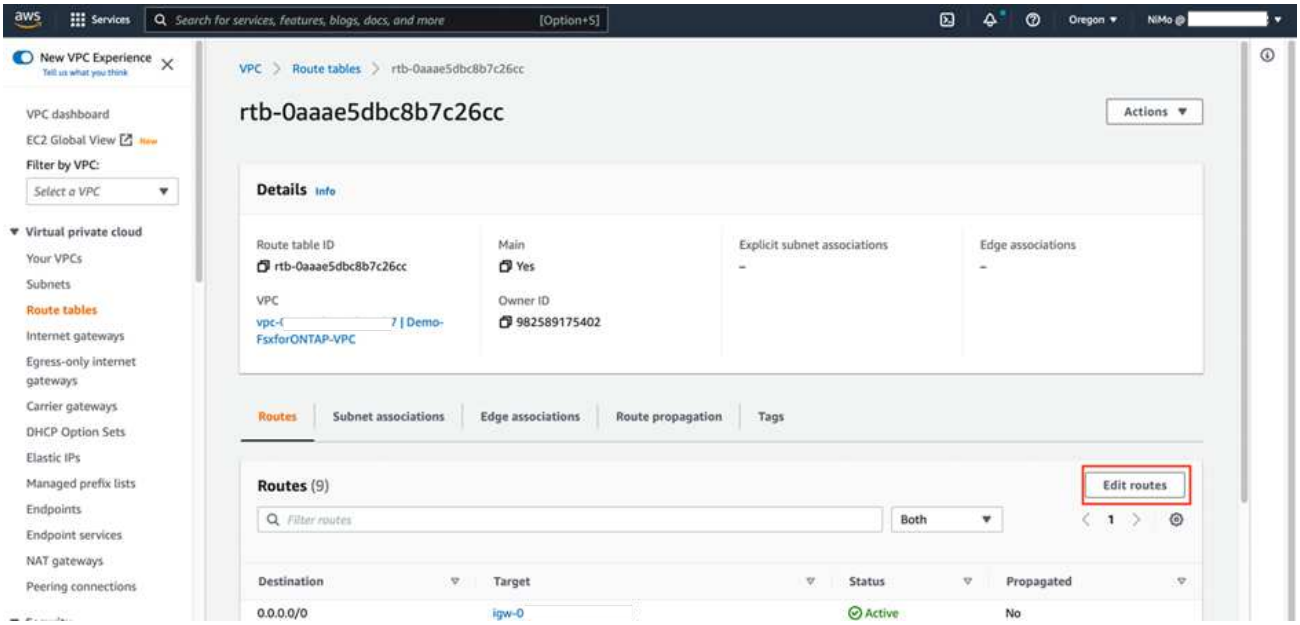
   - Amazon FSx ONTAP浮動 IP 的浮動 IP 範圍的路由。
   - 新建立的外部 VPC 位址空間的路由。



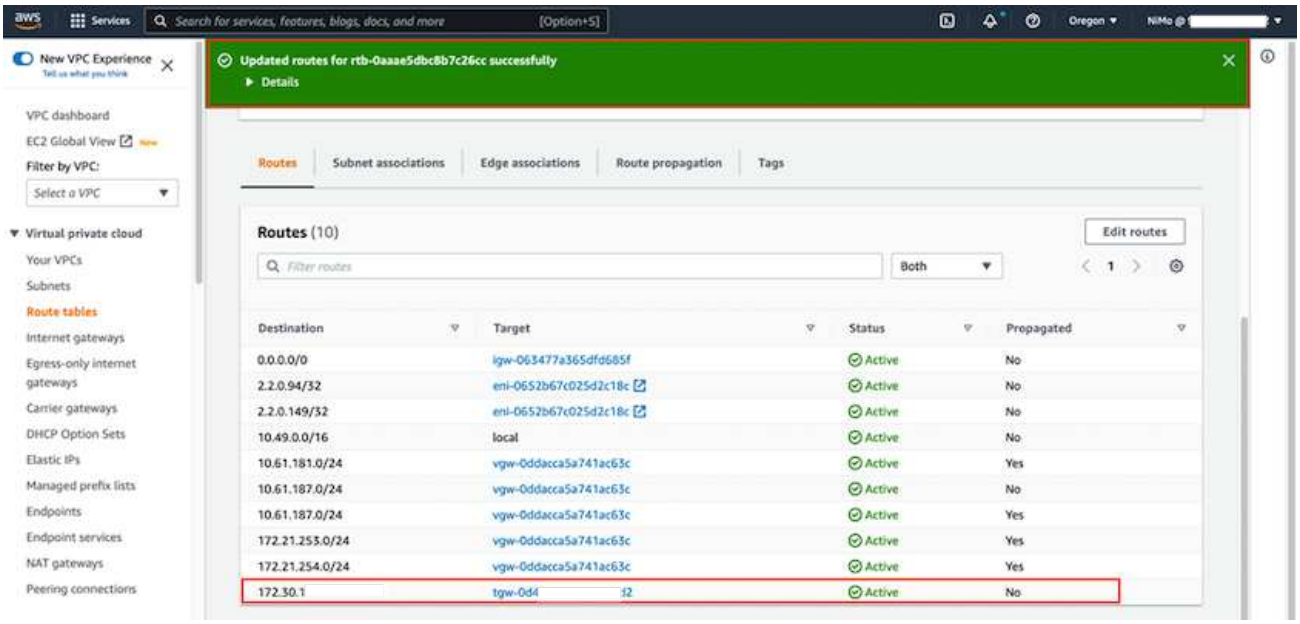


▼ 步驟 **5**：設定路由（**AWS VPC** 和 **SDDC**）和安全群組

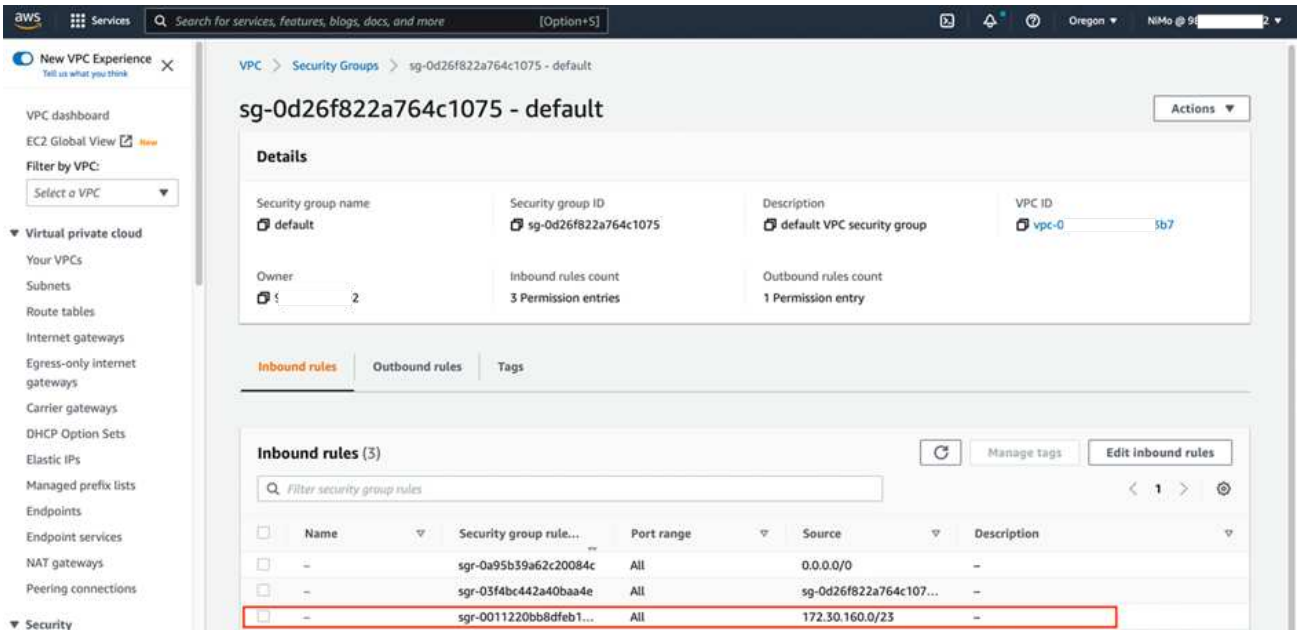
1. 在 AWS 控制台中，透過在 VPC 服務頁面中找到 VPC 並選擇 VPC 的 主 路由表來建立返回 SDDC 的路由。
2. 瀏覽到下方面板中的路線表，然後按一下「編輯路線」。



3. 在*編輯路由*面板中，按一下*新增路由*，然後選擇*Transit Gateway*和關聯的 TGW ID 輸入 SDDC 基礎架構的 CIDR。按一下“儲存變更”。



4. 下一步是驗證關聯 VPC 中的安全性群組是否使用 SDDC 群組 CIDR 的正確入站規則進行更新。
5. 使用 SDDC 基礎架構的 CIDR 區塊更新入站規則。



驗證 VPC（FSx ONTAP所在的位置）路由表是否已更新，以避免連線問題。

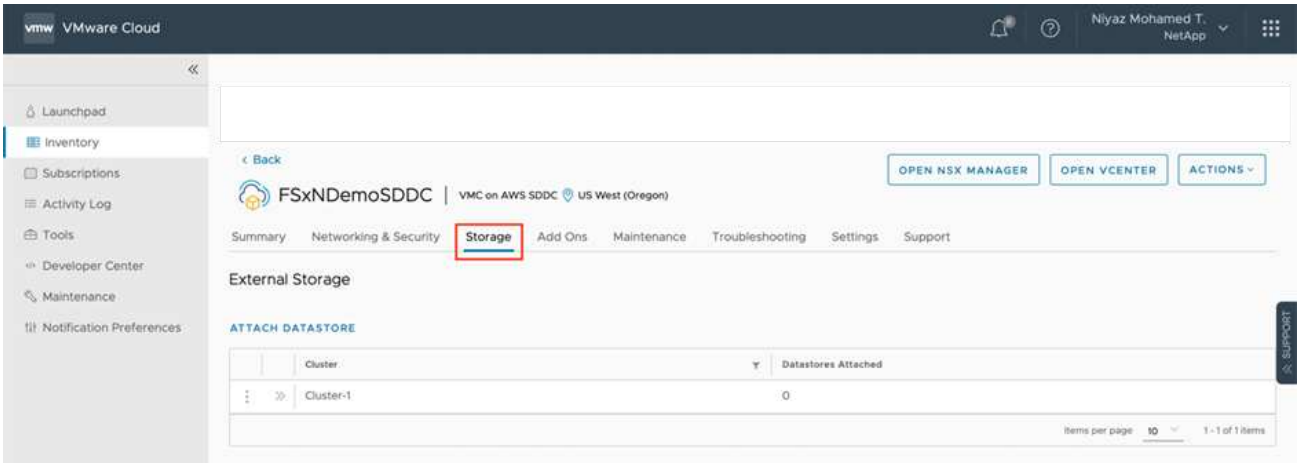
更新安全群組以接受 NFS 流量。

這是準備與適當的 SDDC 連線的最後一步。設定檔系統、新增路由並更新安全群組後，就可以掛載資料儲存了。

▼ 步驟 **6**：將 **NFS** 磁碟區作為資料儲存附加到 **SDDC** 集群

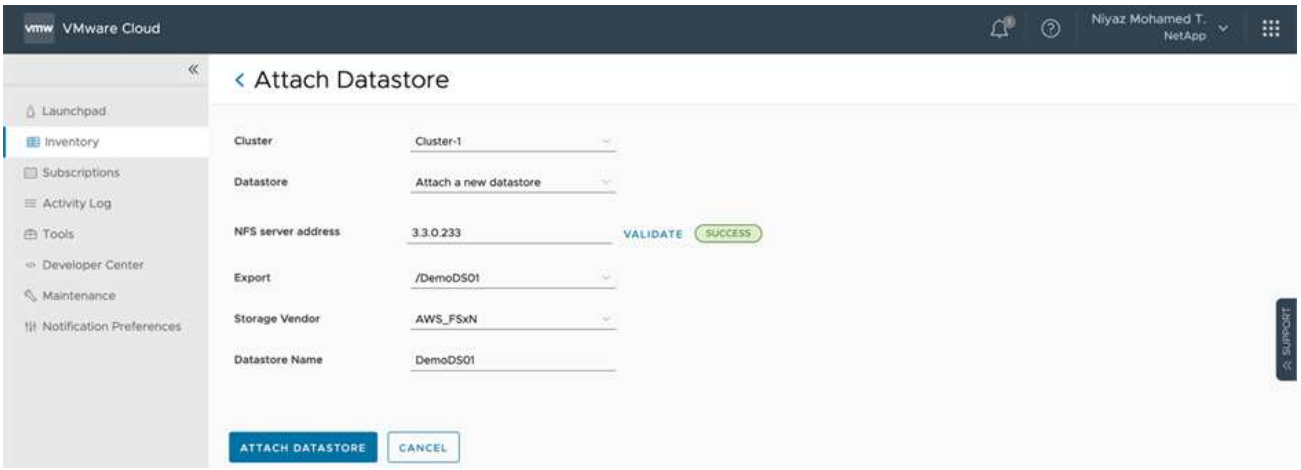
在設定檔系統並建立連線後，存取 VMware Cloud Console 來掛載 NFS 資料儲存。

1. 在 VMC 控制台中，開啟 SDDC 的 儲存 標籤。

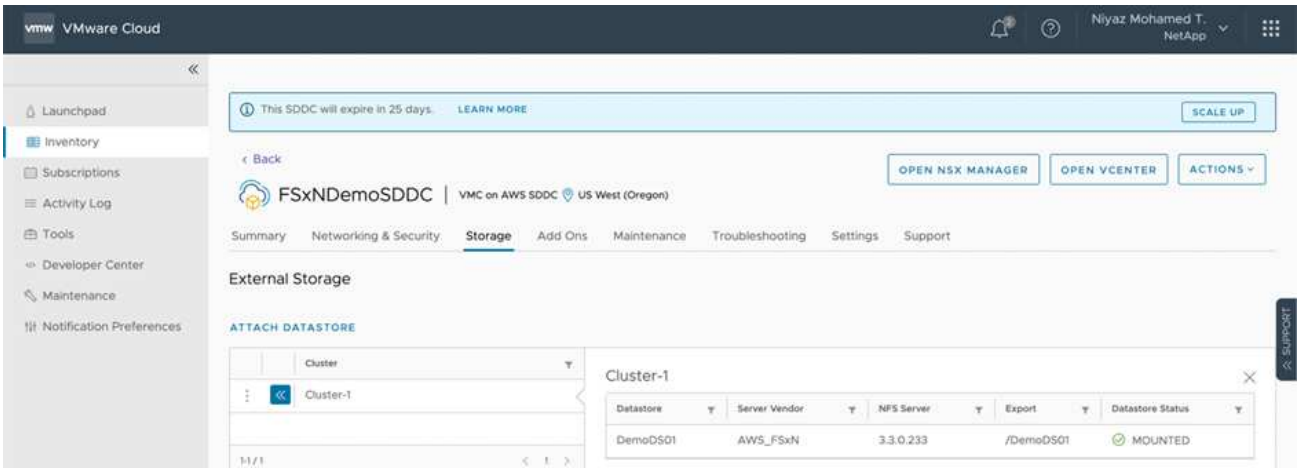


2. 點擊“附加資料儲存”並填寫所需的值。

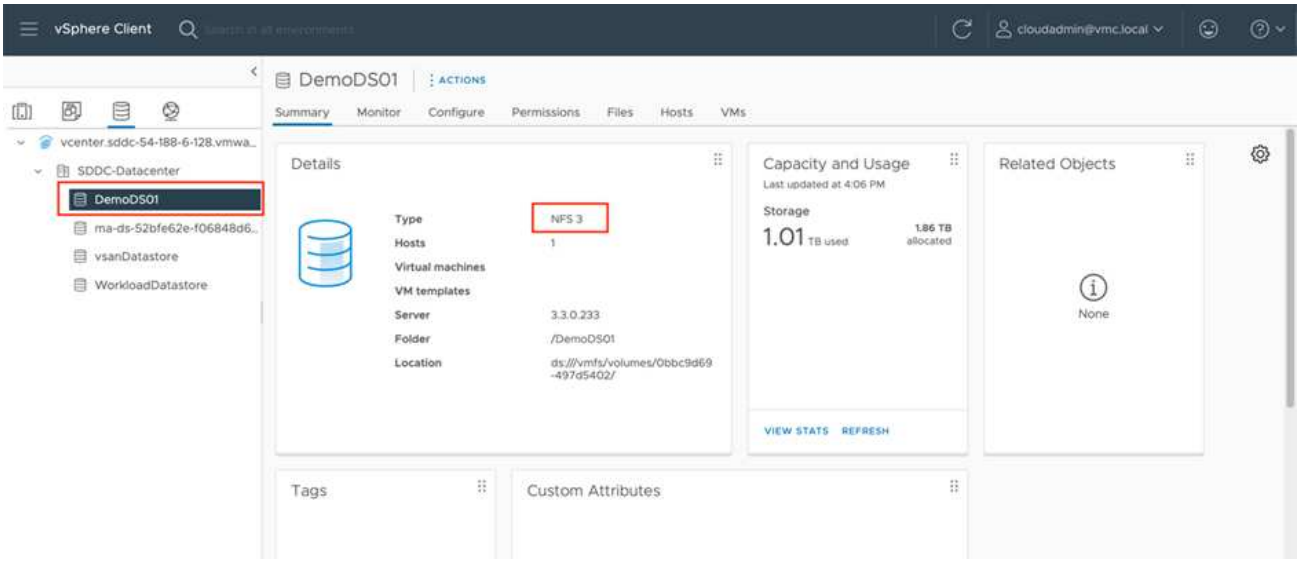
> NFS 伺服器位址是 NFS IP 位址，可以在 AWS 控制台中的 FSx > 儲存虛擬機器標籤 > 端點下找到。



3. 點擊“**ATTACH DATASTORE**”將資料儲存附加到叢集。



4. 透過存取 vCenter 來驗證 NFS 資料存儲，如下所示：



適用於 **AWS** 的**NetApp**來賓連線儲存選項

AWS 支援使用本機 FSx 服務 (FSx ONTAP) 或Cloud Volumes ONTAP (CVO) 連接來賓的NetApp儲存體。

FSx ONTAP

Amazon FSx ONTAP是一項完全託管的服務，它基於 NetApp 流行的ONTAP檔案系統構建，提供高度可靠、可擴展、高效且功能豐富的檔案儲存。 FSx ONTAP將NetApp檔案系統的熟悉功能、效能、功能和 API 操作與完全託管的 AWS 服務的靈活性、可擴充性和簡單性相結合。

FSx ONTAP提供功能豐富、快速且靈活的共享文件存儲，可從在 AWS 或本地運行的 Linux、Windows 和 macOS 計算實例廣泛存取。 FSx ONTAP提供具有亞毫秒延遲的高效能固態硬碟 (SSD) 儲存。借助 FSx ONTAP，您可以為您的工作負載實現 SSD 等級的效能，同時只需為一小部分資料支付 SSD 儲存費用。

使用 FSx ONTAP管理資料更容易，因為您只需點擊按鈕即可快照、複製和複製檔案。此外，FSx ONTAP會自動將您的資料分層到成本較低的彈性儲存中，從而減少您配置或管理容量的需要。

FSx ONTAP還提供高可用性和持久性存儲，具有完全託管的備份和跨區域災難復原支援。為了更輕鬆地保護和保護您的數據，FSx ONTAP支援流行的資料安全和防毒應用程式。

FSx ONTAP作為來賓連接存儲

▼ 使用 **VMware Cloud on AWS** 配置**Amazon FSx ONTAP**

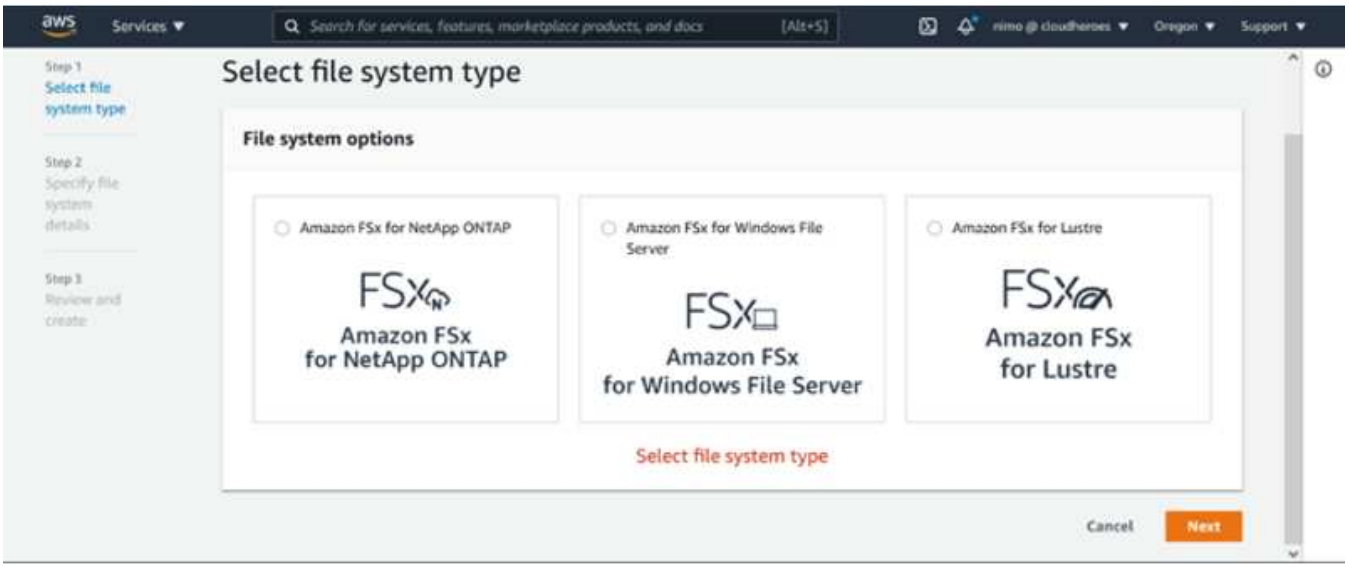
可以從在 AWS 的 VMware Cloud 上的 VMware SDDC 環境中建立的虛擬機器掛載Amazon FSx ONTAP檔案共用和 LUN。這些磁碟區也可以安裝在 Linux 用戶端上，並使用 NFS 或 SMB 協定對應到 Windows 用戶端上，並且透過 iSCSI 安裝時，可以在 Linux 或 Windows 用戶端上將 LUNS 作為區塊裝置進行存取。可依照下列步驟快速設定適用於NetApp ONTAP檔案系統的Amazon FSx 。

> Amazon FSx ONTAP和 VMware Cloud on AWS 必須位於相同可用區，以獲得更好的效能並避免可用區之間的資料傳輸費用。

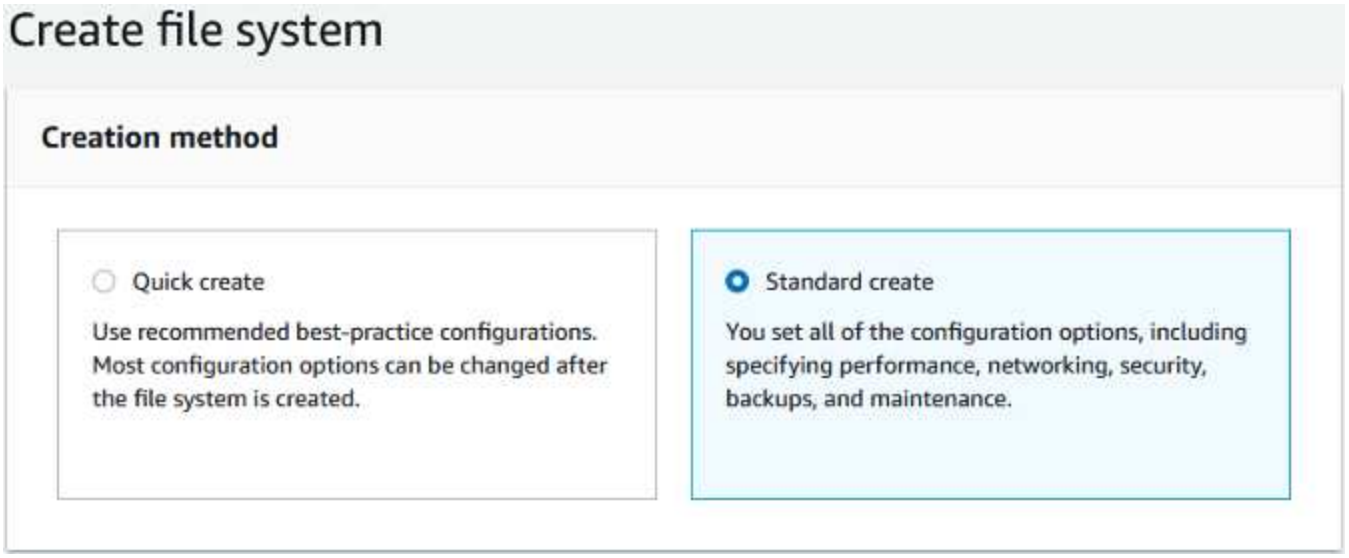
▼ 建立並掛載**Amazon FSx ONTAP**卷

若要建立和掛載Amazon FSx ONTAP檔案系統，請完成下列步驟：

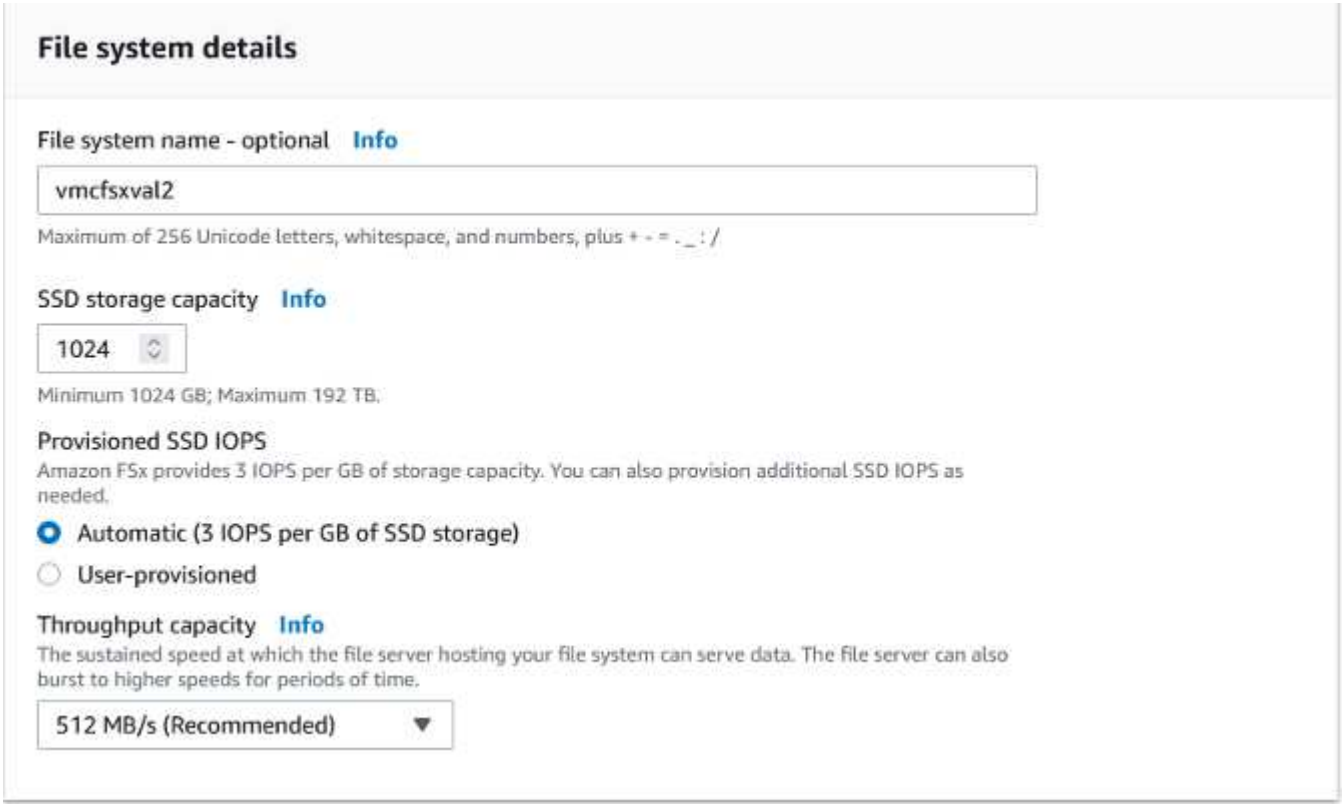
1. 打開"Amazon FSx控制台"並選擇建立檔案系統以啟動檔案系統建立精靈。
2. 在選擇檔案系統類型頁面上，選擇Amazon FSx ONTAP，然後選擇下一步。出現「建立檔案系統」頁面。



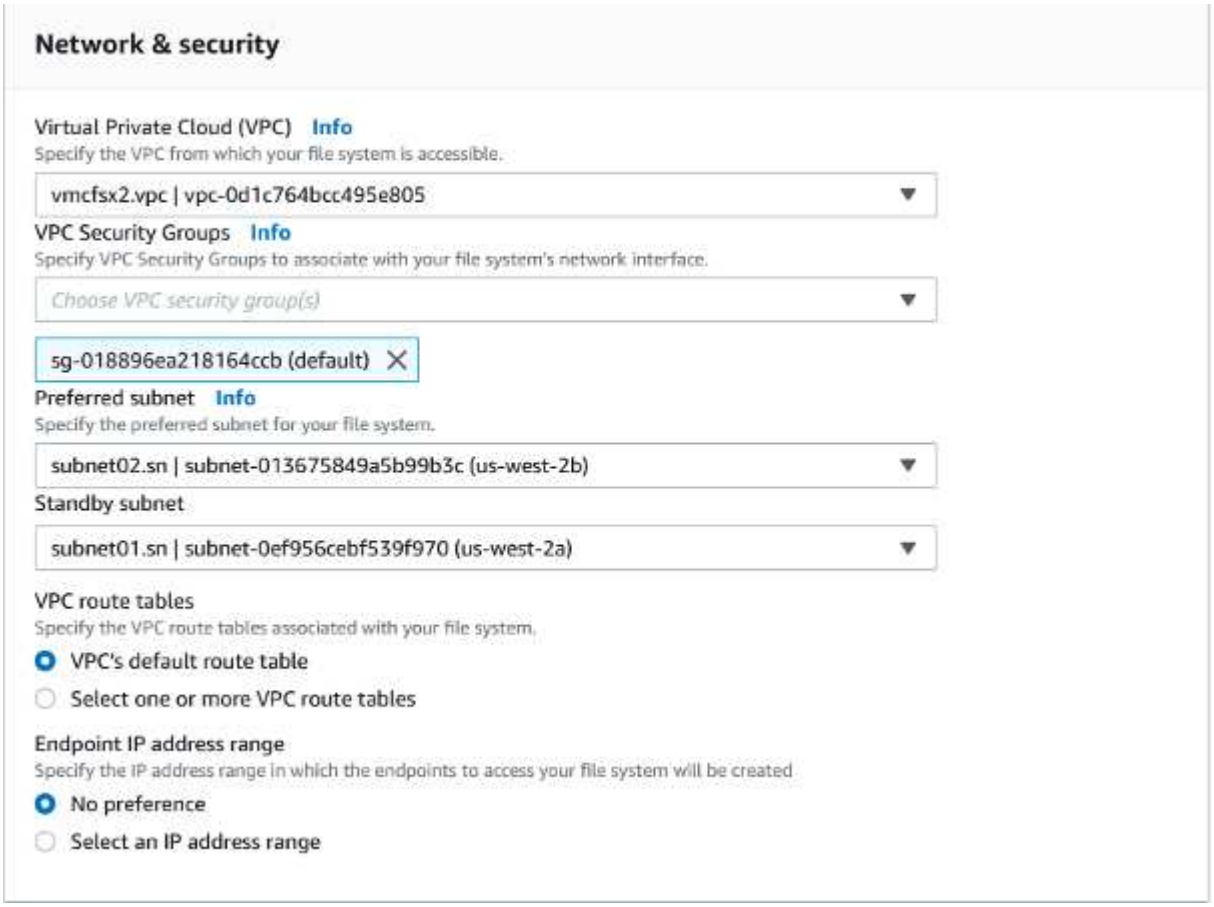
1. 在網路部分中，對於虛擬私有雲 (VPC)，選擇適當的 VPC 和首選子網路以及路由表。在這種情況下，從下拉式選單中選擇了 vmcfsx2.vpc。



1. 對於建立方法，請選擇標準建立。您也可以選擇“快速建立”，但本文檔使用“標準建立”選項。

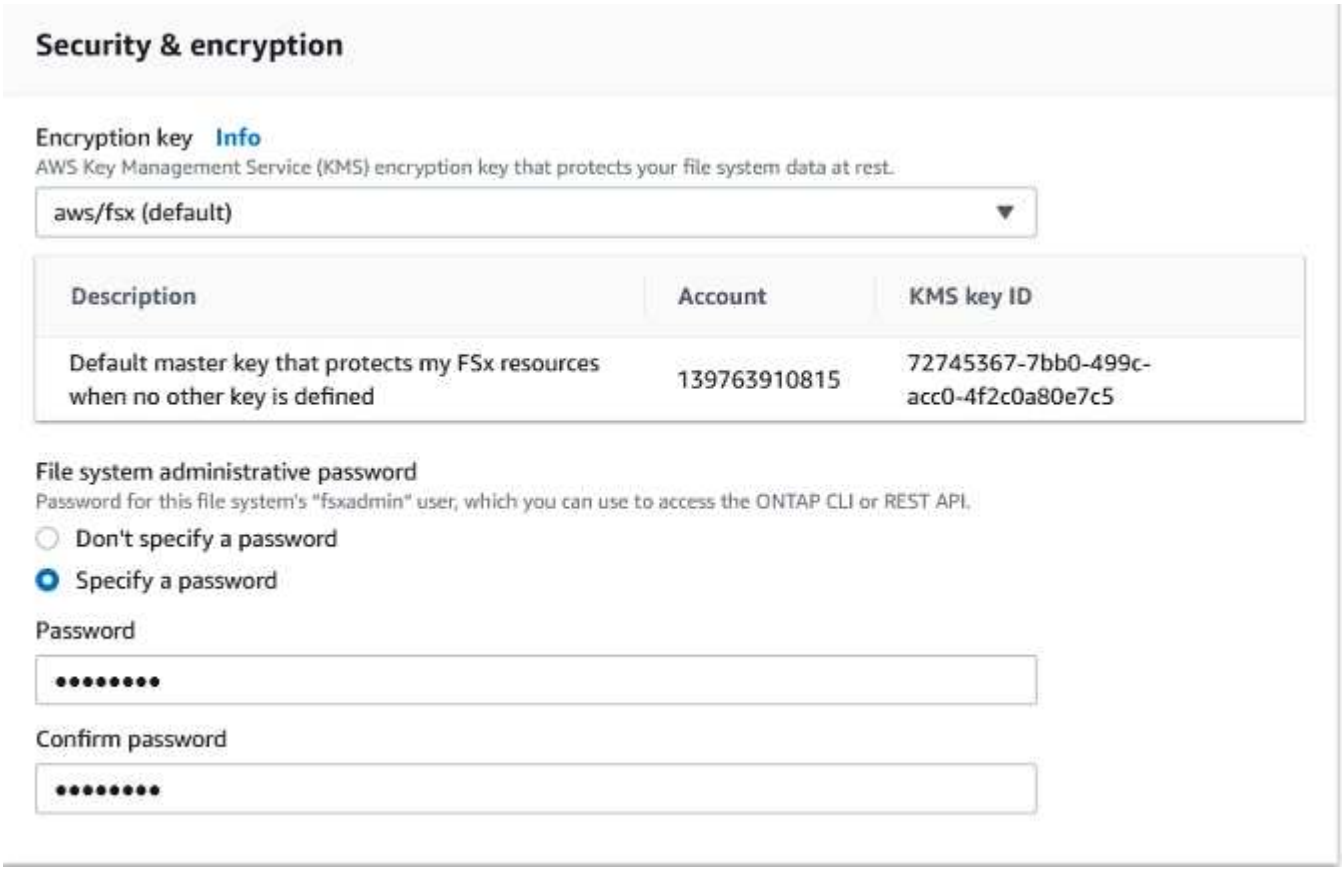


1. 在網路部分中，對於虛擬私有雲 (VPC)，選擇適當的 VPC 和首選子網路以及路由表。在這種情況下，從下拉式選單中選擇了 vmcfsx2.vpc。

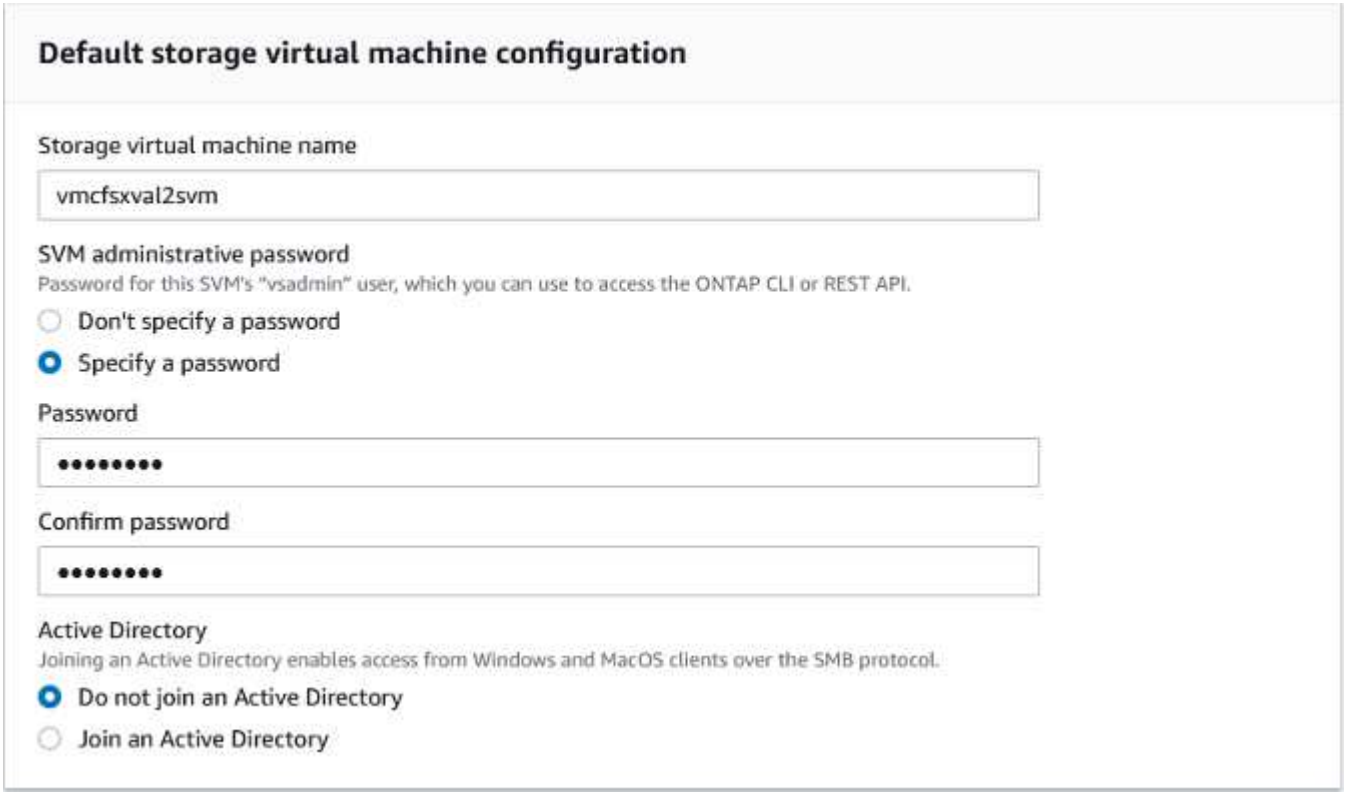


在網路部分中，對於虛擬私有雲 (VPC)，選擇適當的 VPC 和首選子網路以及路由表。在這種情況下，從下拉式選單中選擇了 vmcfsx2.vpc。

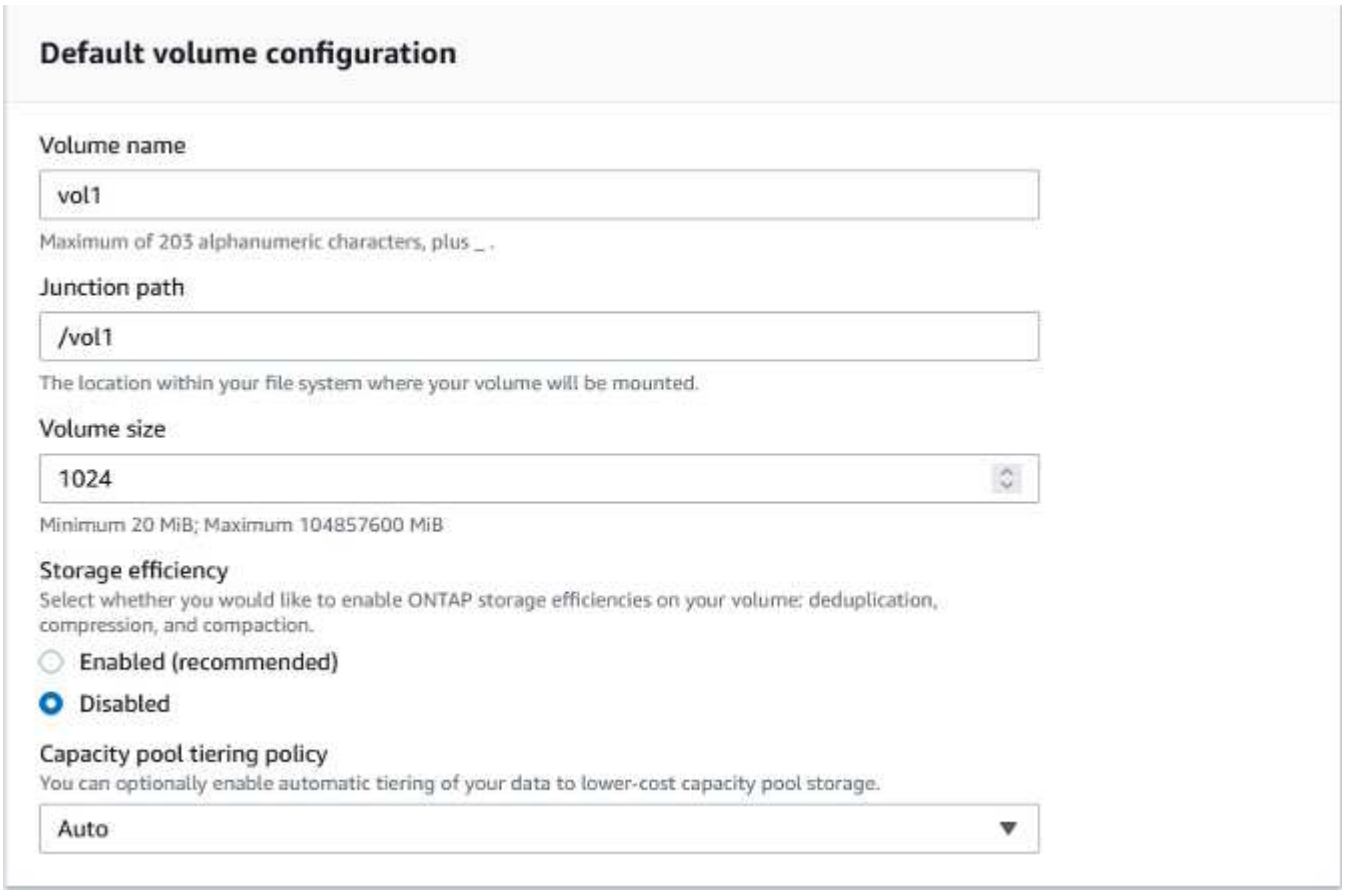
1. 在安全性和加密部分中，對於加密金鑰，選擇保護檔案系統靜態資料的 AWS Key Management Service (AWS KMS) 加密金鑰。對於檔案系統管理密碼，請輸入 fsxadmin 使用者的安全密碼。



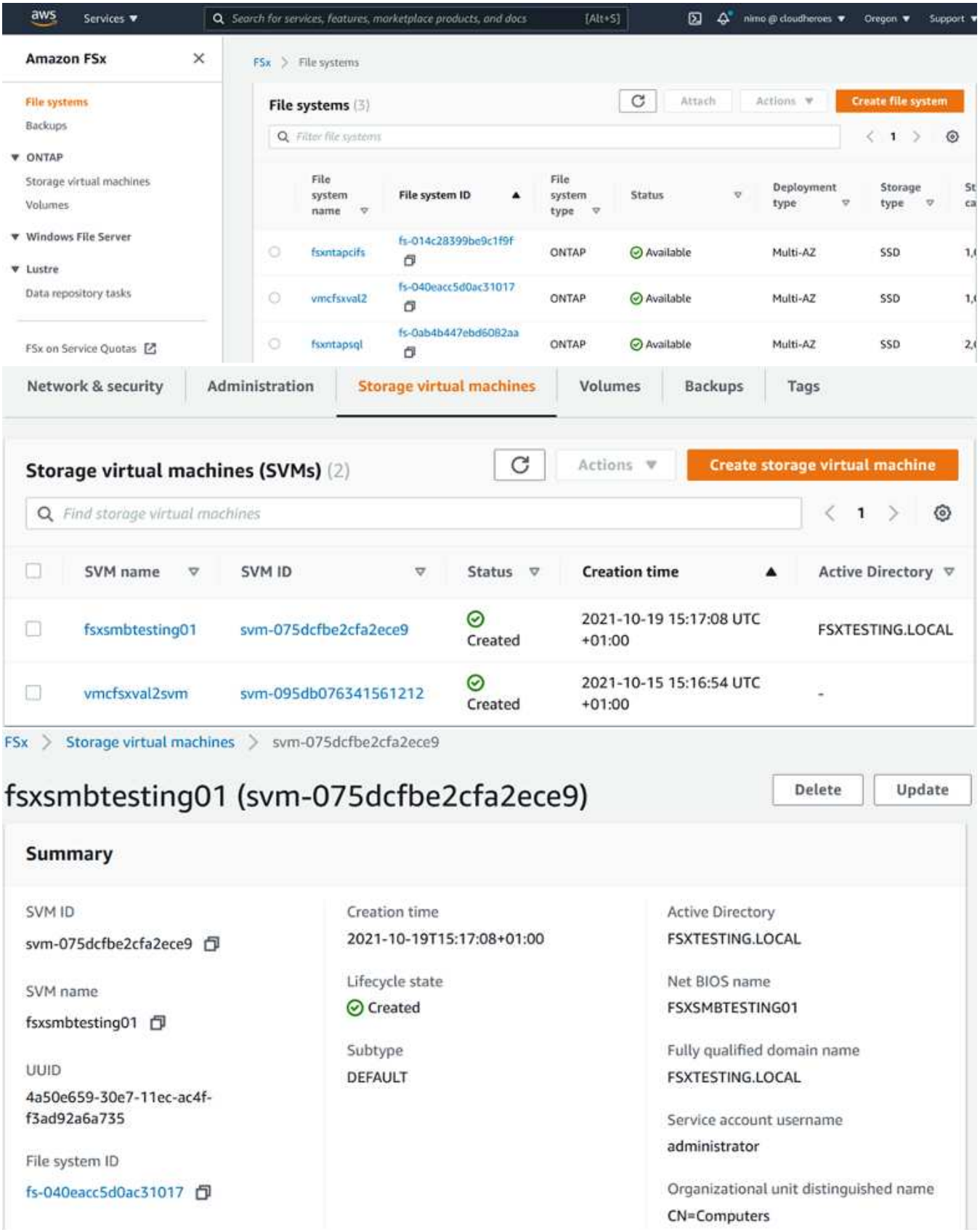
1. 在虛擬機器中指定與 vsadmin 一起使用的密碼，以便使用 REST API 或 CLI 管理ONTAP 。如果未指定密碼，則可以使用 fsxadmin 使用者來管理 SVM。在 Active Directory 部分中，請確保將 Active Directory 加入 SVM 以設定 SMB 共用。在預設儲存虛擬機器設定部分，為此驗證中的儲存提供一個名稱，SMB 共用是使用自管理 Active Directory 網域進行設定的。



1. 在預設磁碟區配置部分中，指定磁碟區名稱和大小。這是一個 NFS 磁碟區。對於儲存效率，選擇「啟用」以開啟ONTAP儲存效率功能（壓縮、重複資料刪除和壓縮）或選擇「停用」以關閉它們。



1. 查看「建立檔案系統」頁面上顯示的檔案系統配置。
2. 按一下“建立檔案系統”。



有關詳細信息，請參閱"Amazon FSx ONTAP入門"。

按照上述方法建立檔案系統後，建立具有所需大小和協定的磁碟區。

1. 打開"Amazon FSx控制台"。
2. 在左側導覽窗格中，選擇檔案系統，然後選擇要為其建立磁碟區的ONTAP檔案系統。
3. 選擇卷選項卡。
4. 選擇建立卷選項卡。
5. 出現「建立磁碟區」對話框。

出於演示目的，本節創建了一個 NFS 卷，可以輕鬆將其安裝在 AWS 上的 VMware 雲端上運行的虛擬機器上。 nfsdemovol01 的建立方式如下所示：



▼ 在 **Linux** 用戶端上掛載 **FSx ONTAP**磁碟區

若要掛載上一個步驟中建立的 FSx ONTAP磁碟區。從 AWS SDDC 上的 VMC 中的 Linux VM，請完成以下步驟：

1. 連接到指定的Linux實例。
2. 使用安全殼 (SSH) 在執行個體上開啟終端並使用適當的憑證登入。
3. 使用下列指令為磁碟區的掛載點建立目錄：

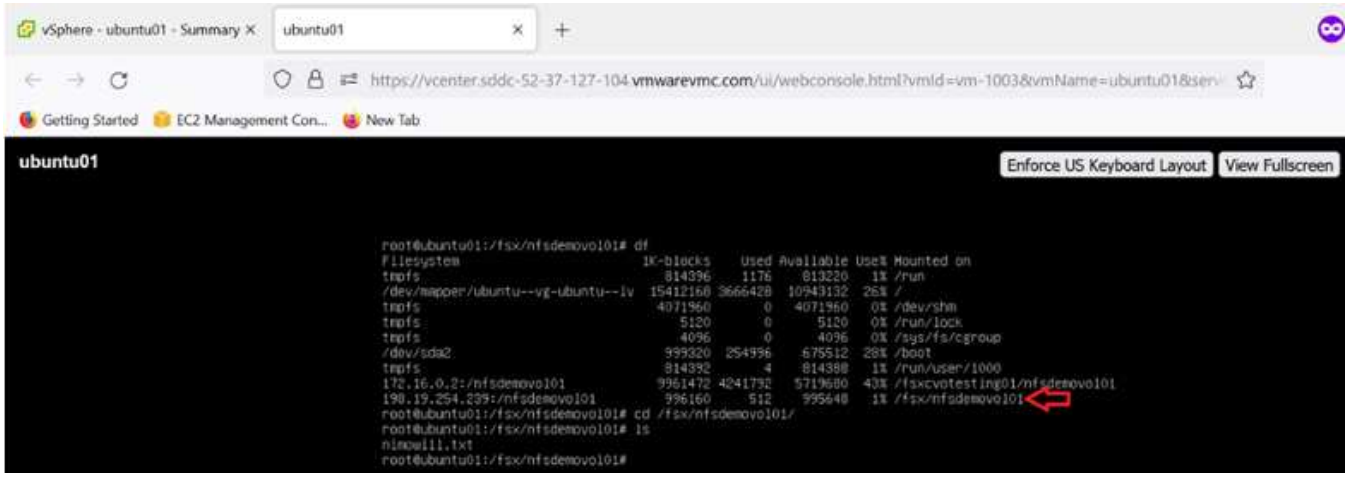
```
$ sudo mkdir /fsx/nfsdemovol01
```

. 將Amazon FSx ONTAP NFS 磁碟區掛載到上一個步驟所建立的目錄。

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. 執行後，執行 df 指令來驗證掛載。



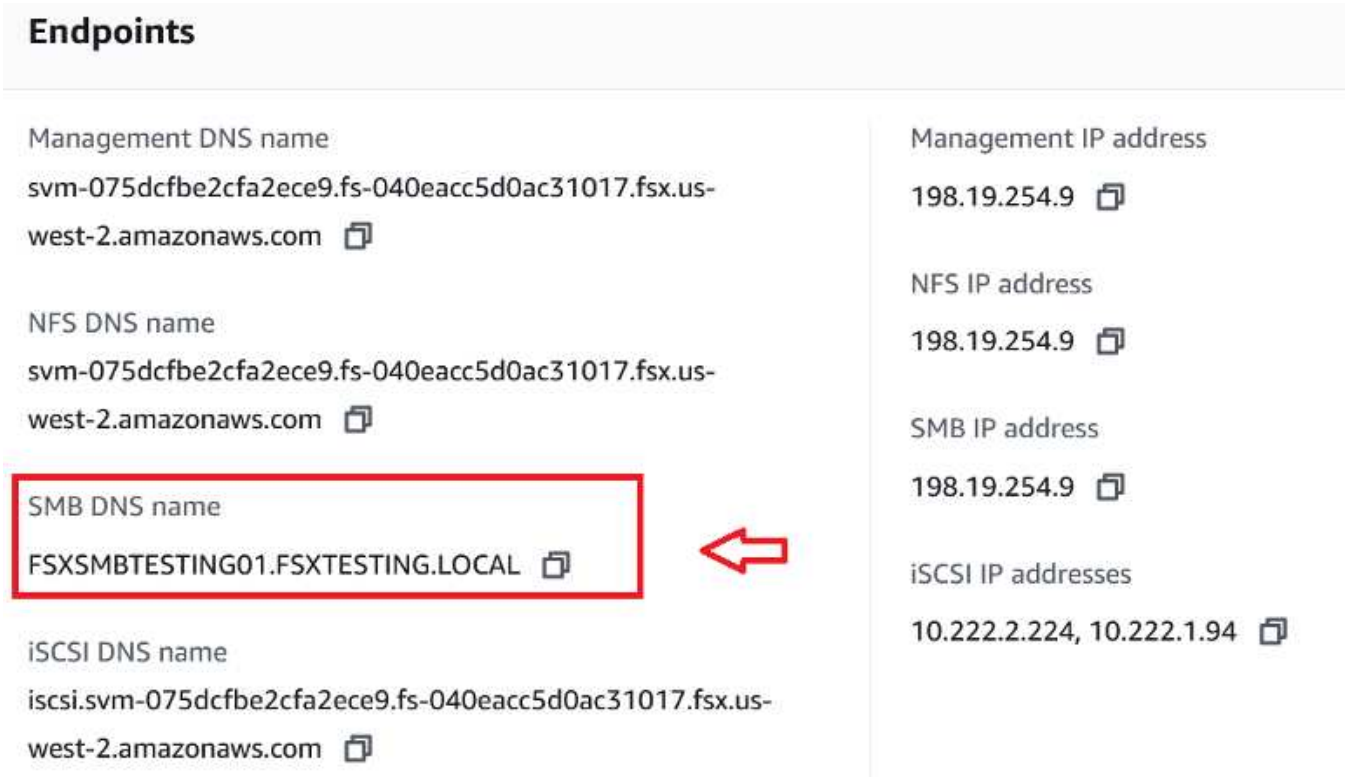
在 Linux 用戶端上掛載 FSx ONTAP磁碟區

▼ 將 **FSx ONTAP**磁碟區附加到 **Microsoft Windows** 用戶端

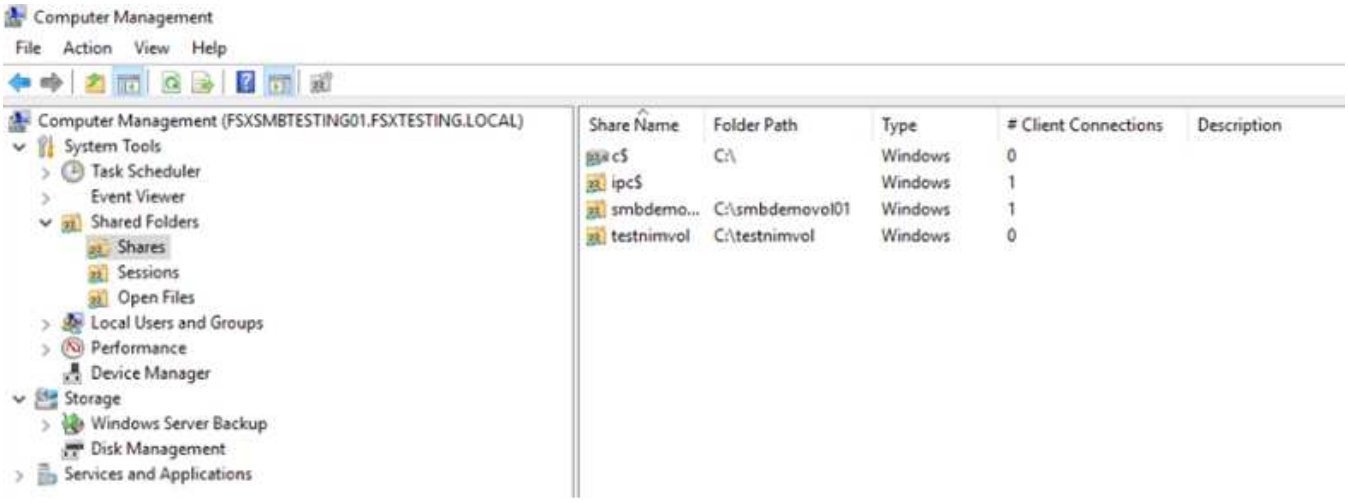
要管理和映射Amazon FSx檔案系統上的檔案共享，必須使用共享資料夾 GUI。

1. 開啟開始功能表並使用以管理員身分執行 fsmgmt.msc。執行此操作將開啟共用資料夾 GUI 工具。
2. 按一下操作 > 所有任務並選擇連接到另一台電腦。
3. 對於另一台計算機，輸入儲存虛擬機器 (SVM) 的 DNS 名稱。例如，本例中使用 FSXSMBTESTING01.FSXTESTING.LOCAL。

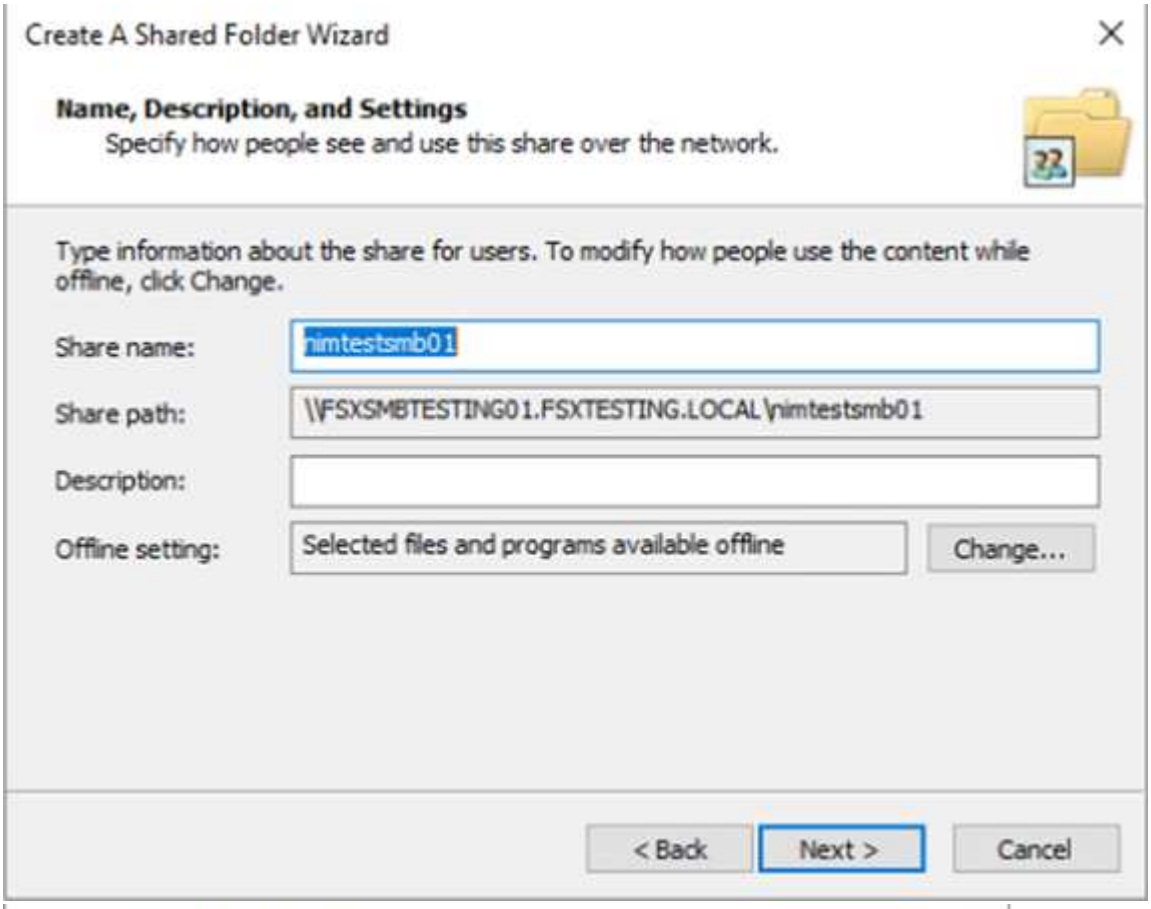
> ⓘ 在Amazon FSx控制台上找到 SVM 的 DNS 名稱，選擇儲存虛擬機，選擇 SVM，然後向下捲動到終端節點以找到 SMB DNS 名稱。按一下“確定”。 Amazon FSx檔案系統出現在共用資料夾清單中。



1. 在共用資料夾工具中，選擇左側窗格中的共用以查看Amazon FSx檔案系統的活動共用。



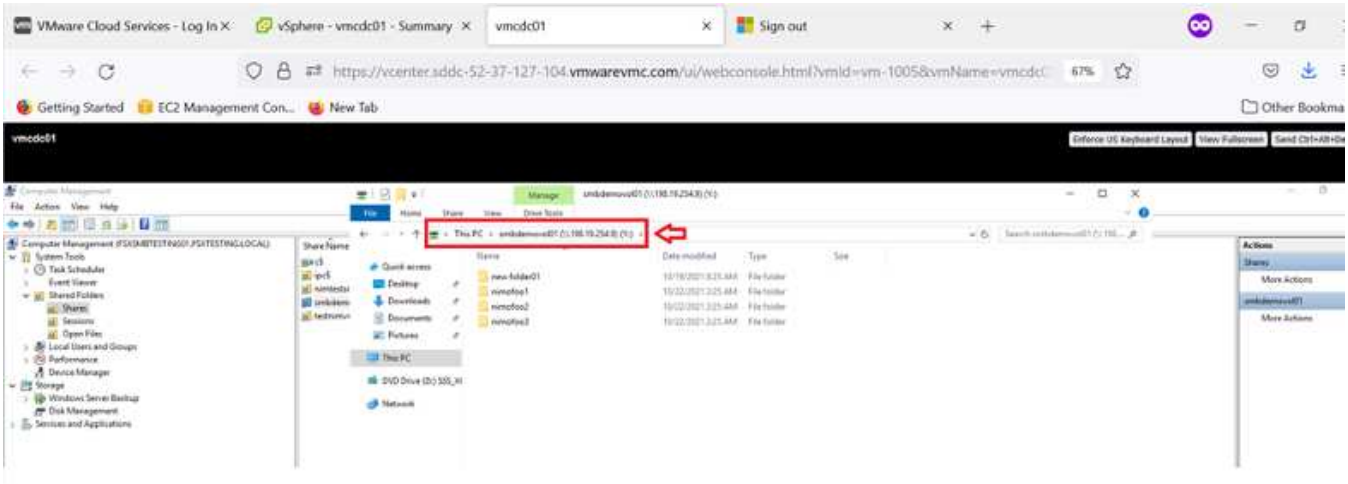
1. 現在選擇一個新的共用並完成建立共用資料夾精靈。





要了解有關在Amazon FSx檔案系統上建立和管理 SMB 共享的更多信息，請參閱"建立 SMB 共享"。

1. 連接建立後，即可連接 SMB 共享並用於應用程式資料。為此，複製共用路徑並使用映射網路磁碟機選項將磁碟區掛載到 AWS SDDC 上 VMware Cloud 上執行的虛擬機器上。



▼ 使用 **iSCSI** 將 **FSx ONTAP LUN** 連接到主機

使用 iSCSI 將 FSx ONTAP LUN 連接到主機

FSx 的 iSCSI 流量透過上一節提供的路由遍歷 VMware Transit Connect/AWS Transit Gateway。若要在Amazon FSx ONTAP中設定 LUN，請依照下列文件操作"這裡"。

在 Linux 用戶端上，確保 iSCSI 守護程序正在執行。配置 LUN 後，請參閱使用 Ubuntu 配置 iSCSI 的詳細指南（作為範例）"這裡"。

本文說明如何將 iSCSI LUN 連接到 Windows 主機：

▼ 在 **FSx ONTAP**中設定 **LUN**：

1. 使用 FSx for ONTAP檔案系統的管理連接埠存取NetApp ONTAP CLI。
2. 依照大小調整輸出的指示建立具有所需大小的 LUN。

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

在此範例中，我們建立了一個大小為 5g（5368709120）的 LUN。

1. 建立必要的 igroup 來控制哪些主機可以存取特定的 LUN。

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators

--------- ------------ -------- --------
------------------------------------
```

```
vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

顯示了兩個條目。

1. 使用以下命令將 LUN 對應到 igroup：

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------- ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

顯示了兩個條目。

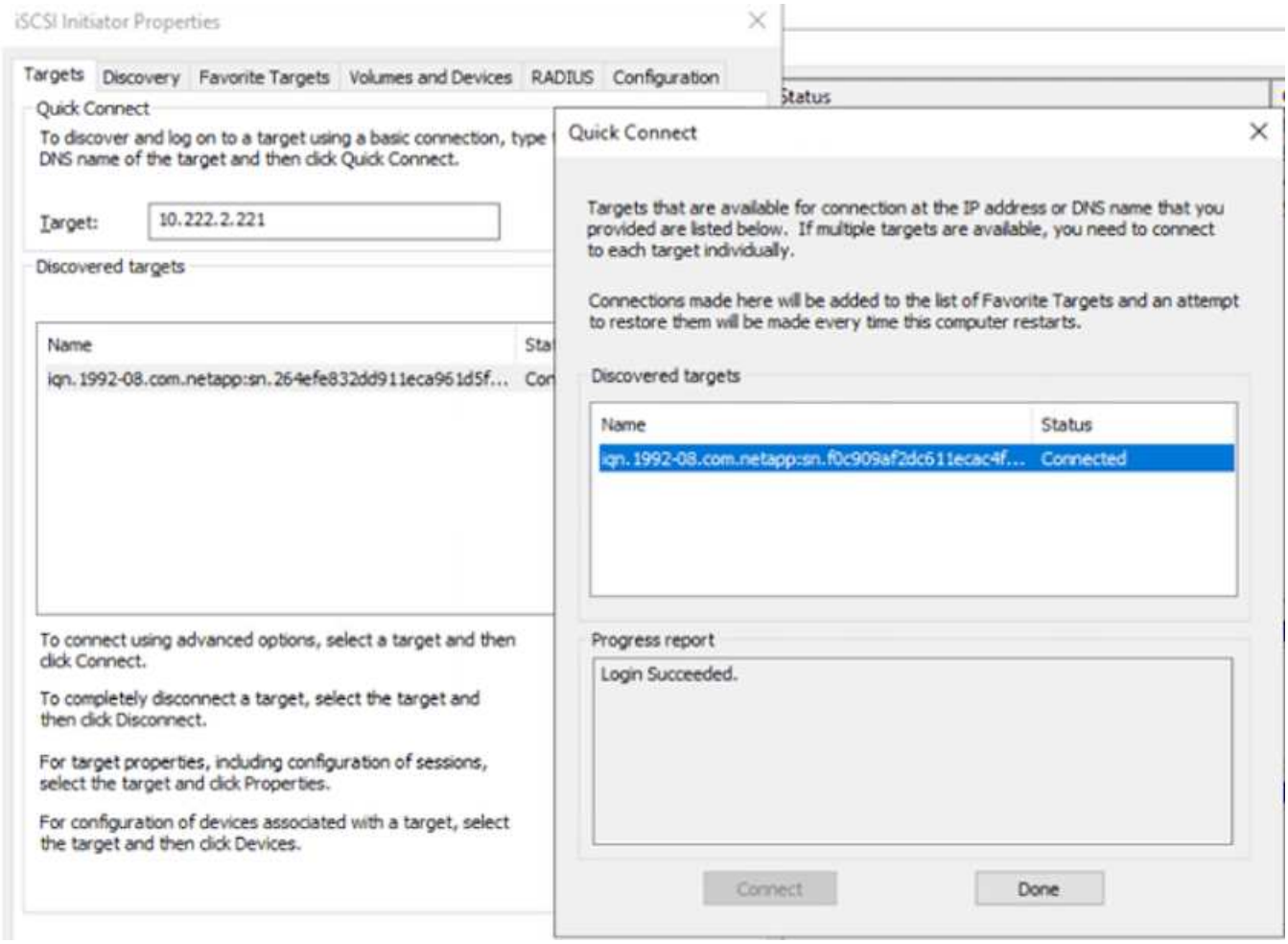
1. 將新設定的 LUN 連接到 Windows VM：

若要將新的 LUN 連接到位於 VMware cloud on AWS SDDC 上的 Windows 主機，請完成下列步驟：

1. 透過 RDP 連接到 VMware Cloud on AWS SDDC 上託管的 Windows VM。
2. 導覽至伺服器管理員 > 儀表板 > 工具 > iSCSI 啟動器以開啟 iSCSI 啟動器屬性對話方塊。
3. 在“發現”標籤中，按一下“發現入口網站”或“新增入口網站”，然後輸入 iSCSI 目標連接埠的 IP 位址。

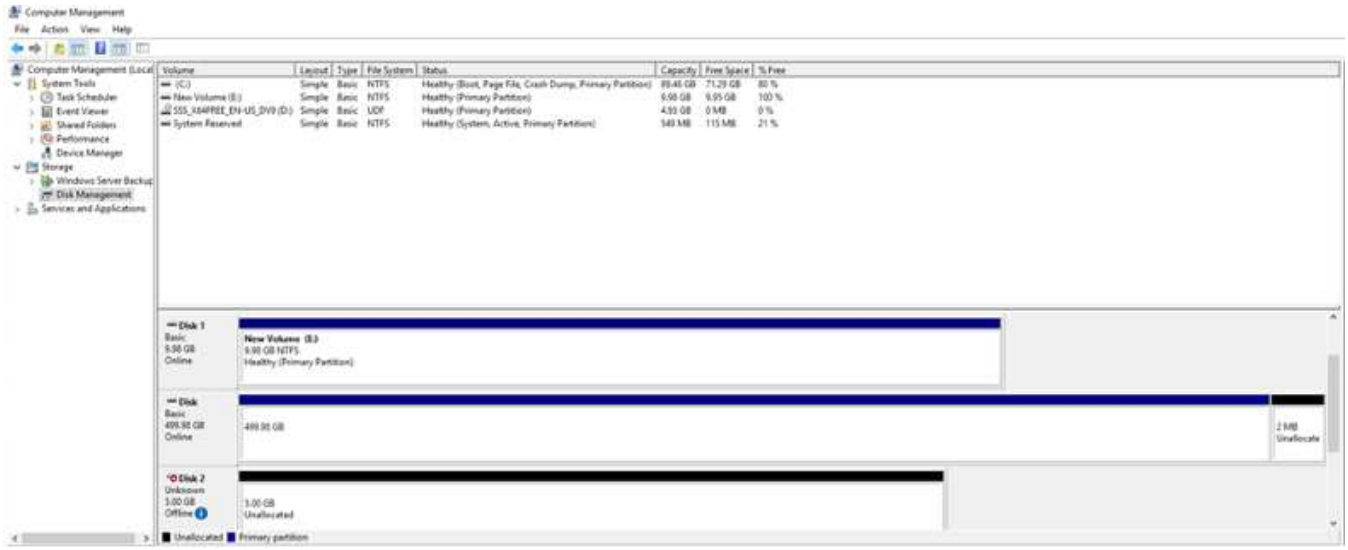
4. 從「目標」標籤中，選擇發現的目標，然後按一下「登入」或「連線」。
5. 選擇啟用多路徑，然後選擇「電腦啟動時自動恢復此連線」或「將此連線新增至收藏品目標清單」。按一下“進階”。

Windows 主機必須與群集中的每個節點建立 iSCSI 連線。本機 DSM 選擇要使用的最佳路徑。



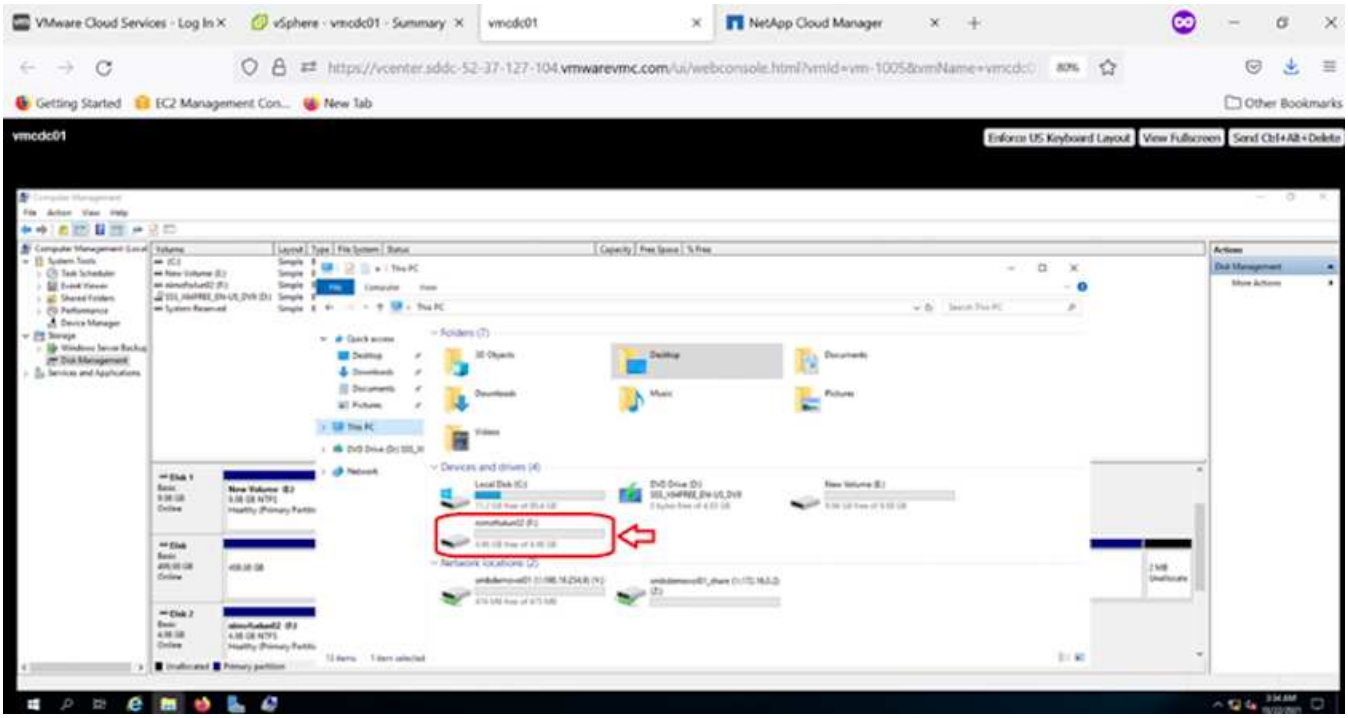
儲存虛擬機器 (SVM) 上的 LUN 對於 Windows 主機來說顯示為磁碟。主機不會自動發現任何新新增的磁碟。透過完成以下步驟觸發手動重新掃描以發現磁碟：

1. 開啟 Windows 電腦管理公用程式：開始 > 管理工具 > 電腦管理。
2. 在導航樹中展開儲存節點。
3. 按一下“磁碟管理”。
4. 按一下操作 > 重新掃描磁碟。



當 Windows 主機首次存取新的 LUN 時，它沒有分割區或檔案系統。透過完成以下步驟初始化 LUN，並（可選）使用檔案系統格式化 LUN：

1. 啟動 Windows 磁碟管理。
2. 右鍵單擊 LUN，然後選擇所需的磁碟或分割區類型。
3. 請按照精靈中的說明進行操作。在此範例中，已安裝磁碟機 F:。



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP（或稱 CVO）是基於 NetApp 的ONTAP儲存軟體所建置的業界領先的雲端資料管理解決方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的軟體定義版本，使用雲端原生存儲，允許您在雲端和本地使用相同的存儲軟體，從而無需重新培訓 IT 人員採用全新方法來管理資料。

CVO 使客戶能夠無縫地將資料從邊緣移動到資料中心、雲端並返回，從而將您的混合雲整合在一起 - 所有這些都透過單一窗格管理控制台NetApp Cloud Manager 進行管理。

CVO 的設計旨在提供極致的效能和先進的資料管理功能，以滿足您在雲端最嚴苛的應用程式

Cloud Volumes ONTAP (CVO) 作為來賓連接存儲

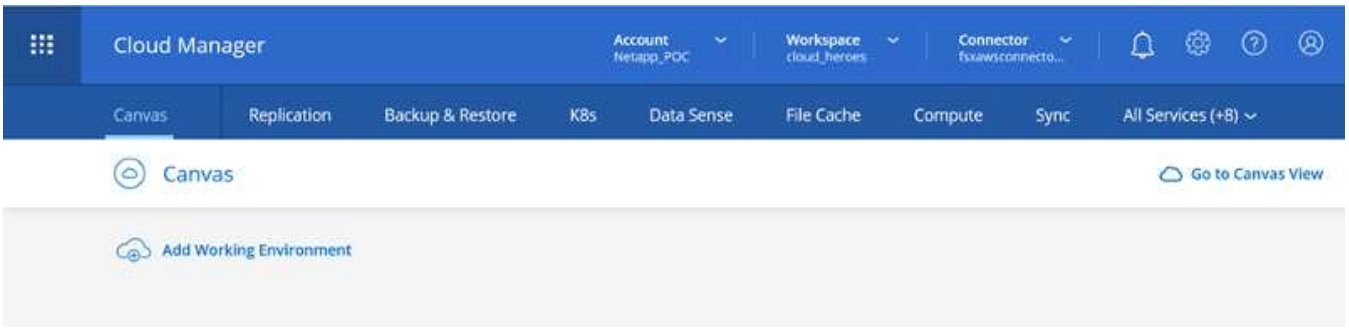
▼ 在 **AWS** 中部署新的**Cloud Volumes ONTAP**實例（自行部署）

可從在 VMware Cloud on AWS SDDC 環境中建立的虛擬機器掛載Cloud Volumes ONTAP共用和 LUN。這些磁碟區還可以安裝在本機 AWS VM Linux Windows 用戶端上，並且當透過 iSCSI 安裝時，可以在 Linux 或 Windows 用戶端上將 LUNS 作為區塊裝置訪問，因為Cloud Volumes ONTAP支援 iSCSI、SMB 和 NFS 協定。只需幾個簡單的步驟即可設定Cloud Volumes ONTAP磁碟區。

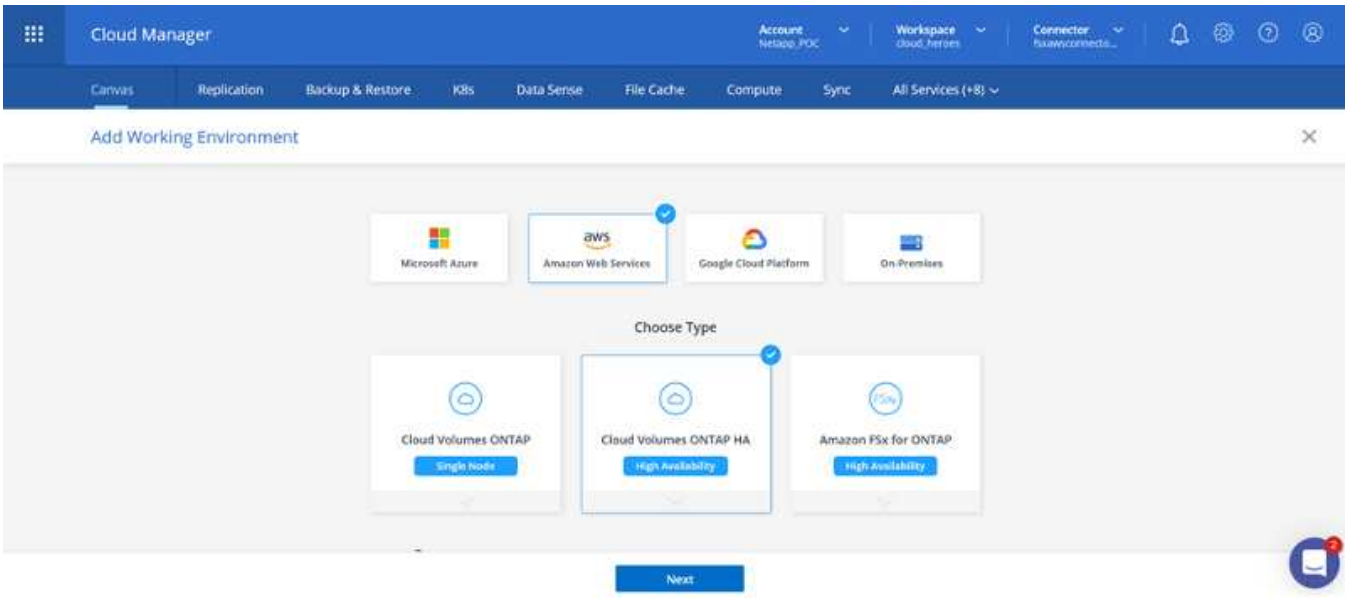
若要將磁碟區從本機環境複製到雲端以實現災難復原或遷移，請使用網站到網站 VPN 或 DirectConnect 建立與 AWS 的網路連線。將資料從本地複製到Cloud Volumes ONTAP超出了本文檔的範圍。若要在本機和Cloud Volumes ONTAP系統之間複製數據，請參閱"設定係統之間的資料複製"。

使用 "Cloud Volumes ONTAP大小調整器" 來精確調整 Cloud Volumes ONTAP 執行個體的大小。此外，監控內部部署效能，以作為 Cloud Volumes ONTAP 大小調整工具的輸入。

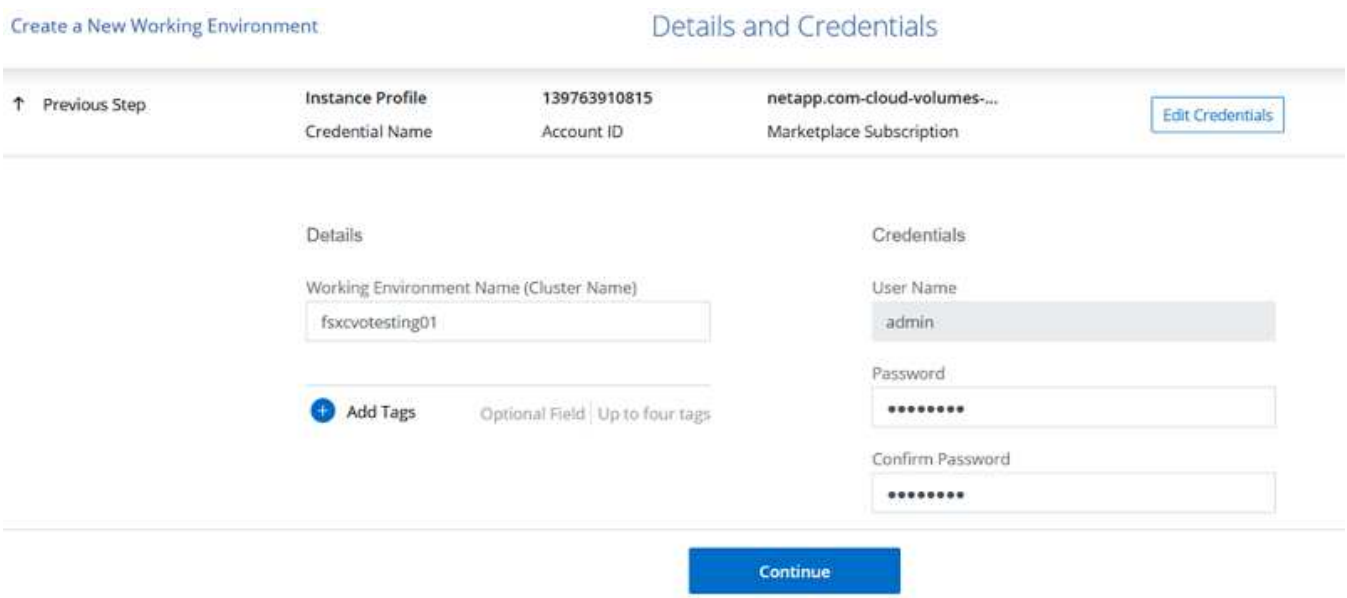
1. 登入NetApp Cloud Central；顯示 Fabric View 畫面。找到Cloud Volumes ONTAP標籤並選擇前往雲端管理員。登入後，將顯示 Canvas 畫面。



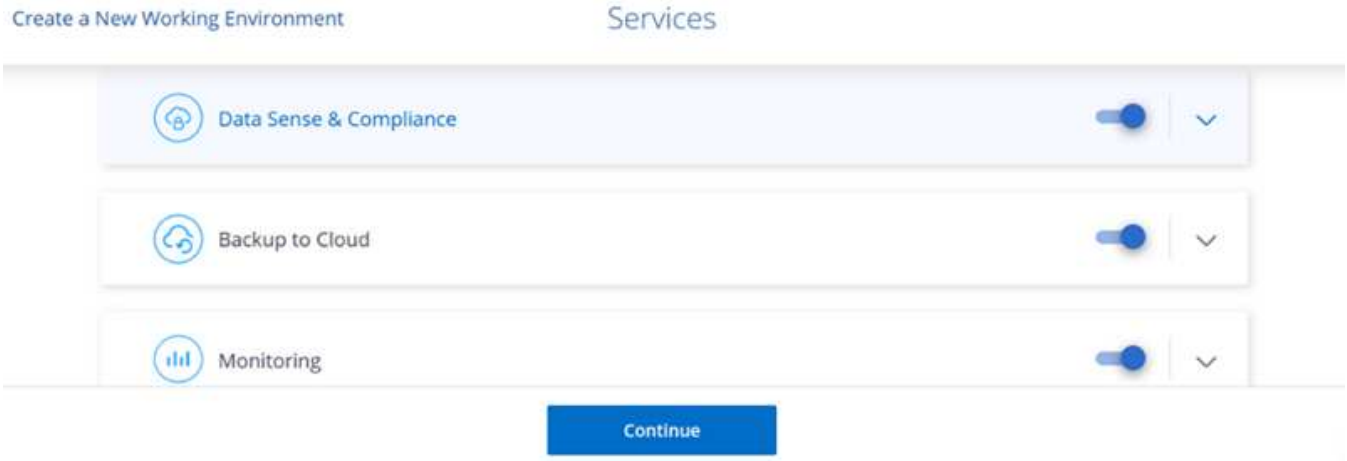
1. 在雲端管理器主頁上，按一下新增工作環境，然後選擇 AWS 作為雲端和系統配置類型。



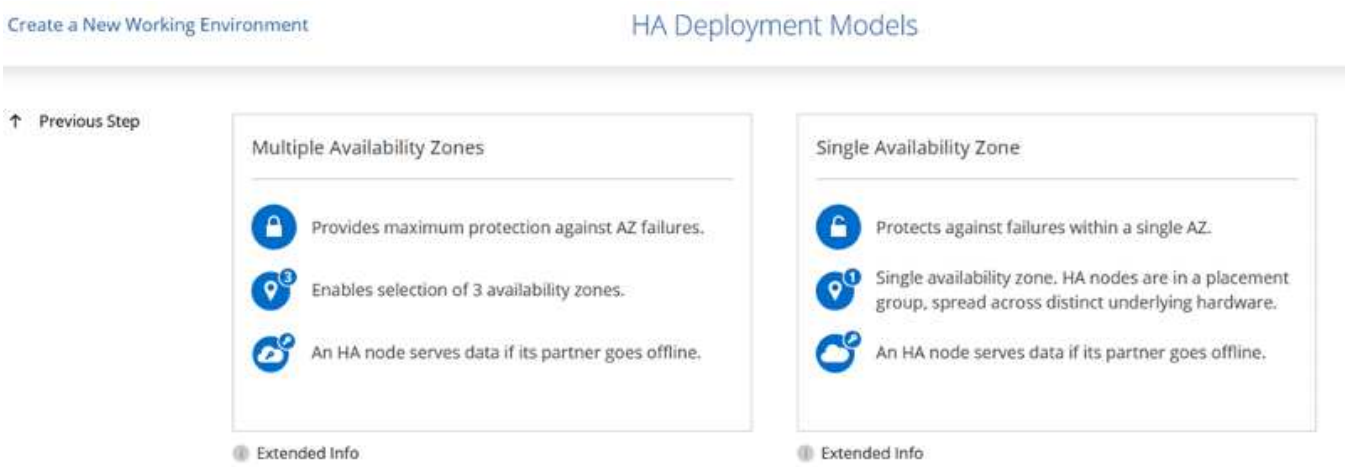
1. 提供要建立的環境的詳細信息，包括環境名稱和管理員憑證。按一下「Continue（繼續）」。



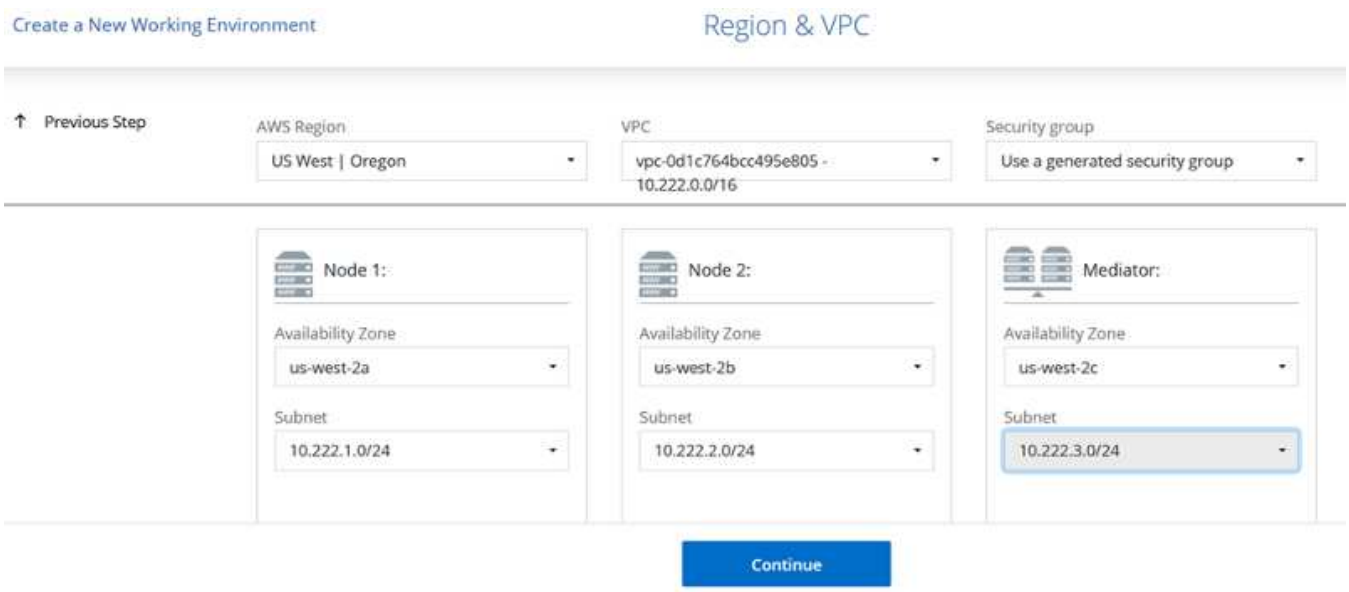
1. 選擇 Cloud Volumes ONTAP 部署的附加服務，包括 NetApp Data Classification、NetApp Backup and Recovery，以及 Data Infrastructure Insights。按一下繼續。



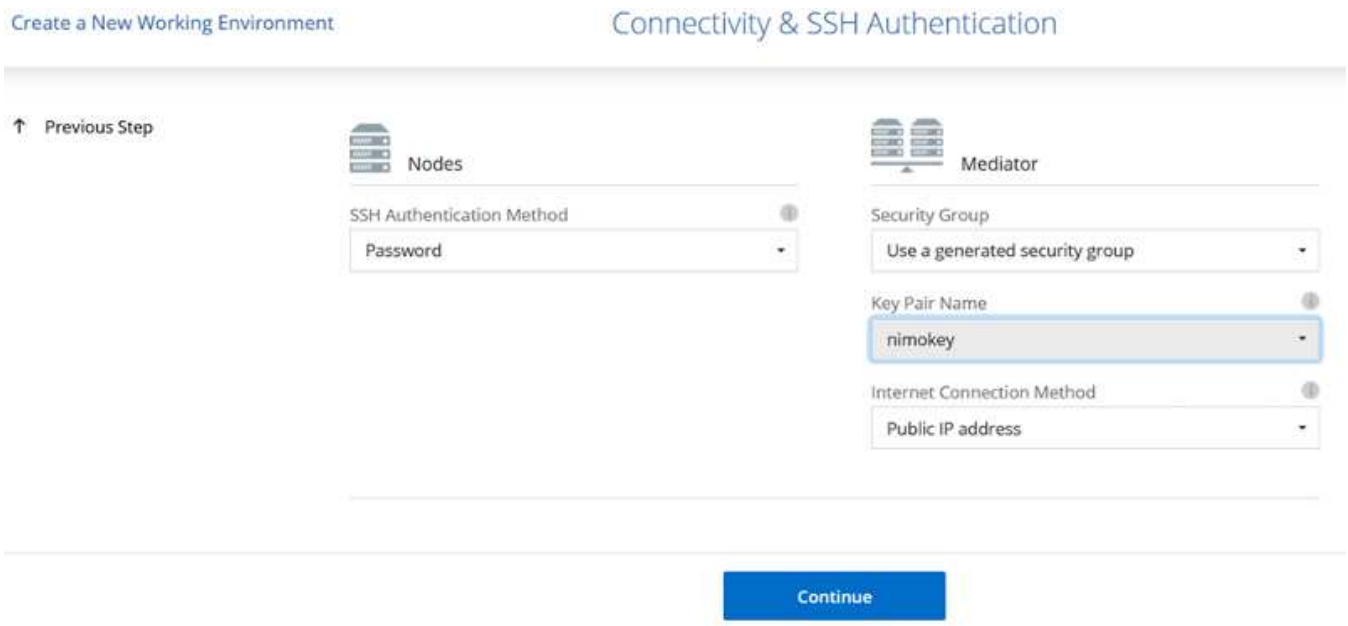
1. 在 HA 部署模型頁面上，選擇多可用區配置。



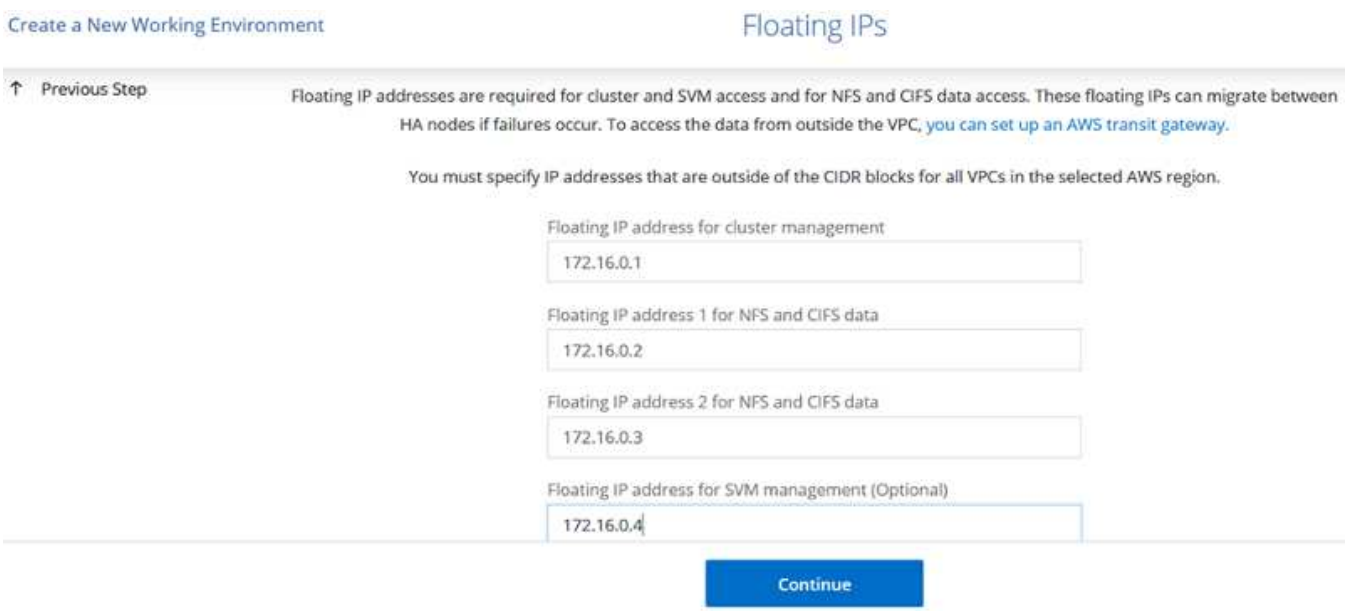
1. 在「區域和 VPC」頁面，輸入網路訊息，然後按一下「繼續」。



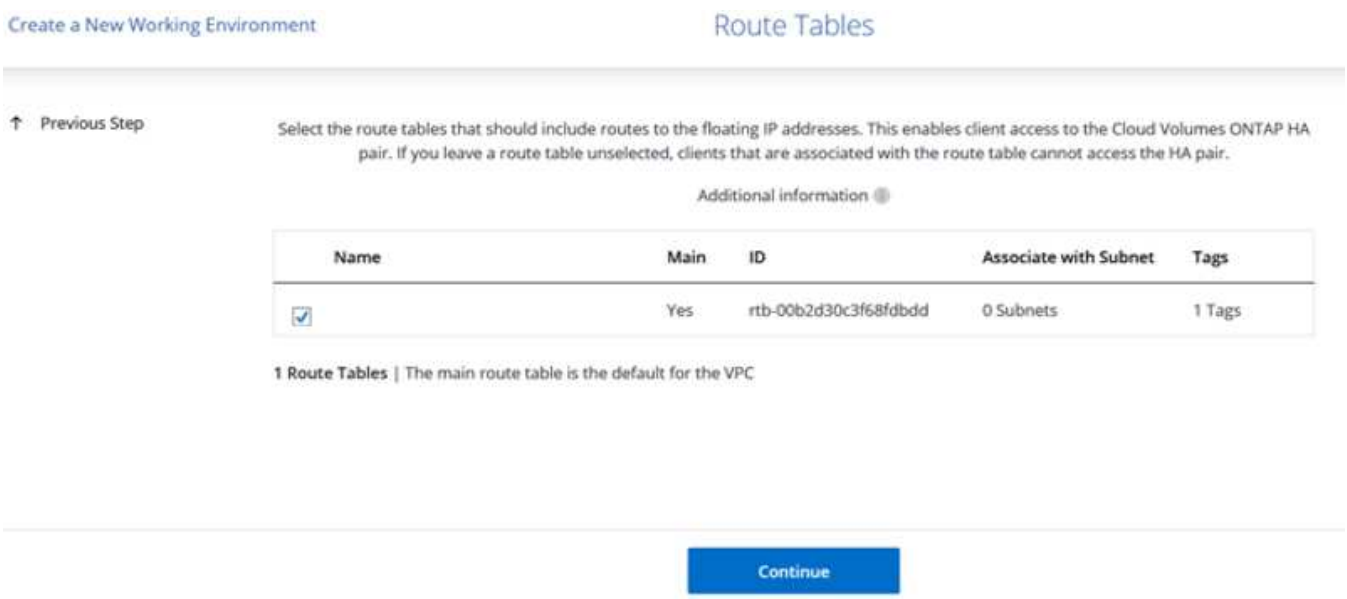
1. 在「連線和 SSH 驗證」頁面上，選擇 HA 對和中介的連線方法。



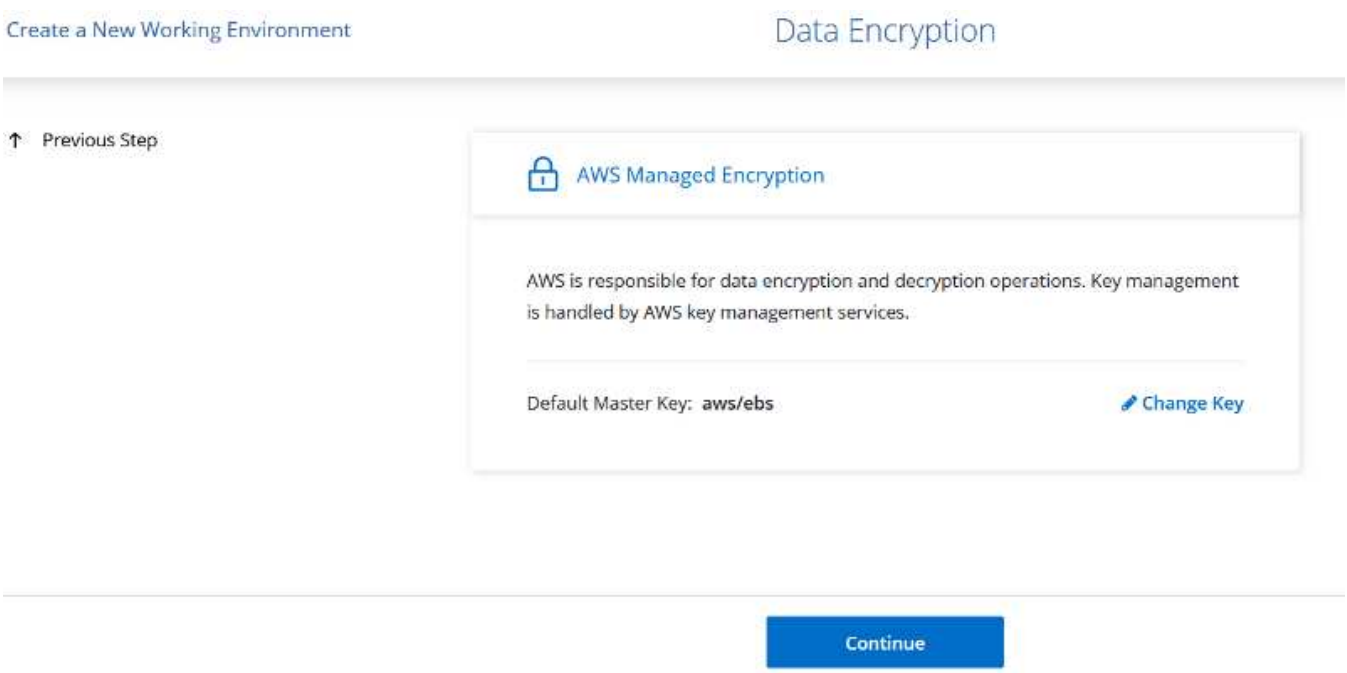
1. 指定浮動 IP 位址，然後按一下繼續。



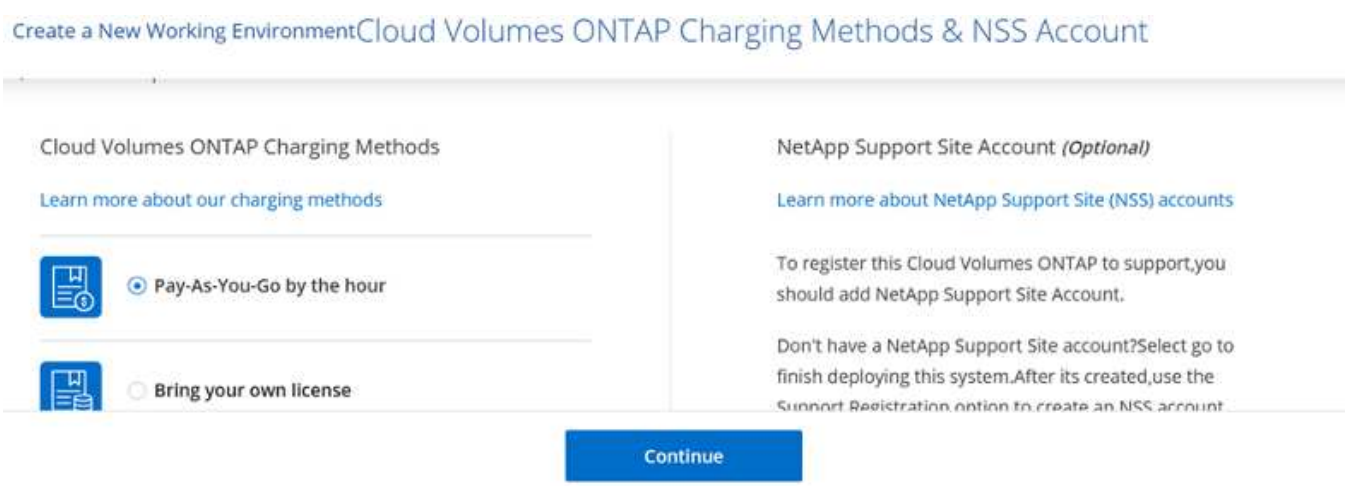
1. 選擇適當的路由表以包含到浮動 IP 位址的路由，然後按一下繼續。



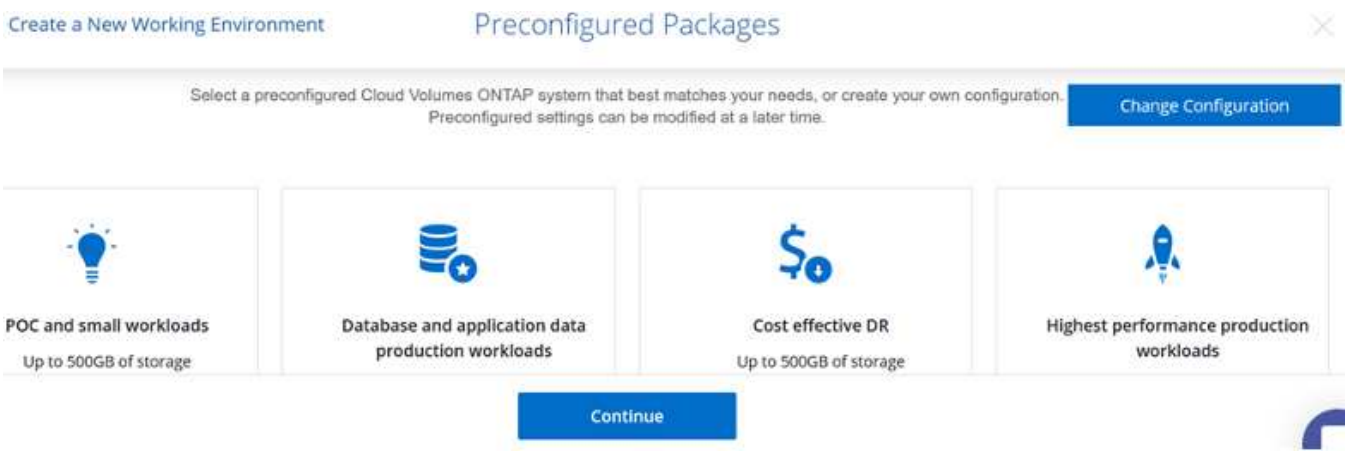
1. 在資料加密頁面上，選擇 AWS 託管加密。



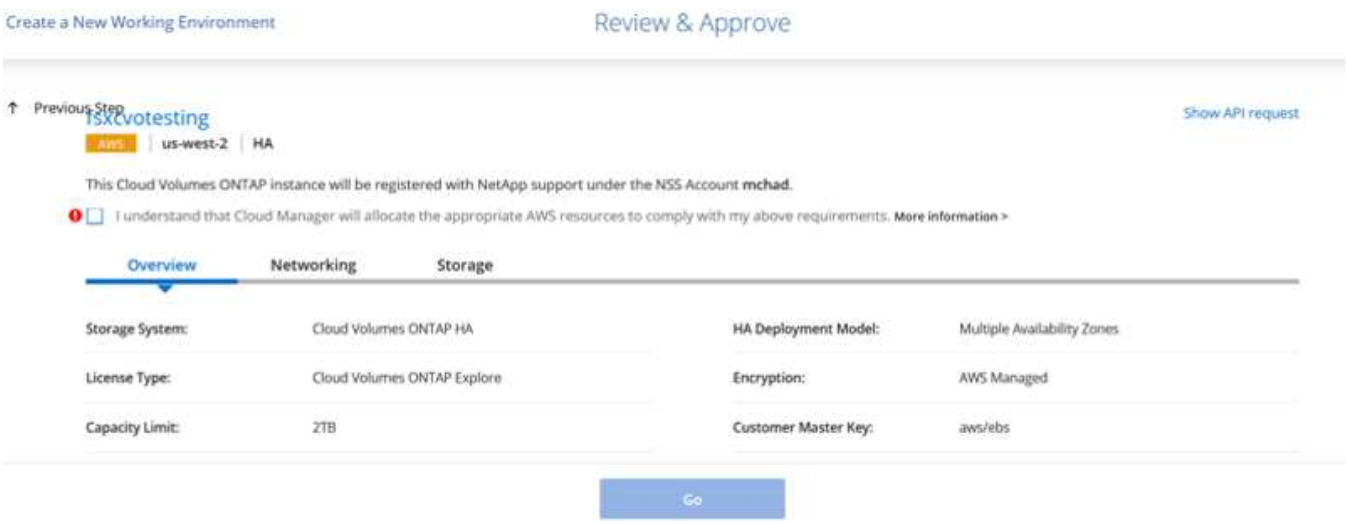
1. 選擇授權選項：按使用量付費或使用現有授權的 BYOL。在此範例中，使用了按使用量付費選項。



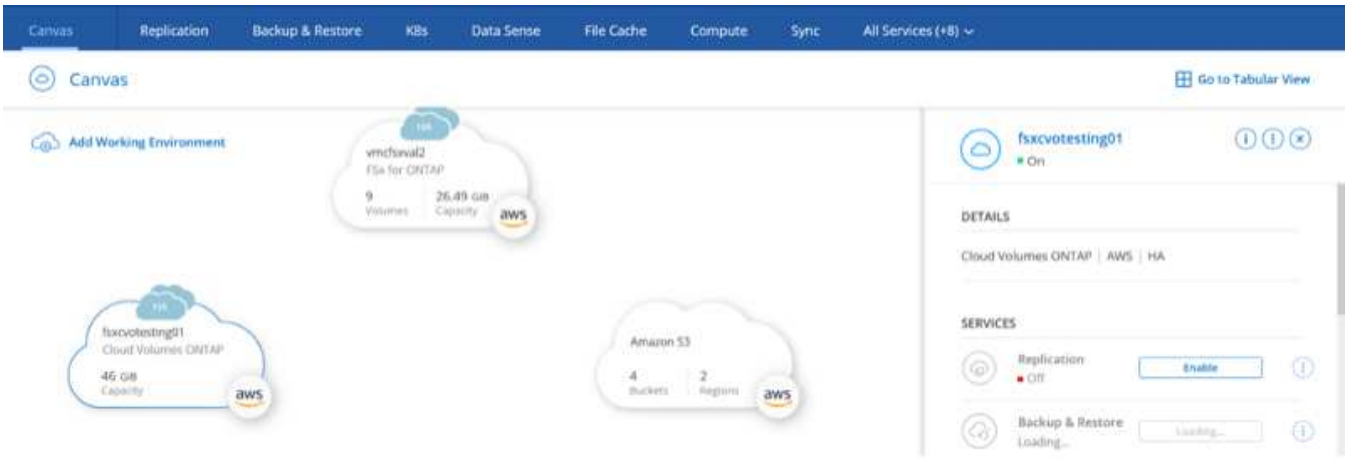
1. 根據要在 AWS SDDC 上的 VMware 雲端上執行的虛擬機器上部署的工作負載類型，在幾個可用的預先配置套件中進行選擇。



1. 在「審核並批准」頁面上，審核並確認選擇。若要建立Cloud Volumes ONTAP實例，請按一下「開始」。

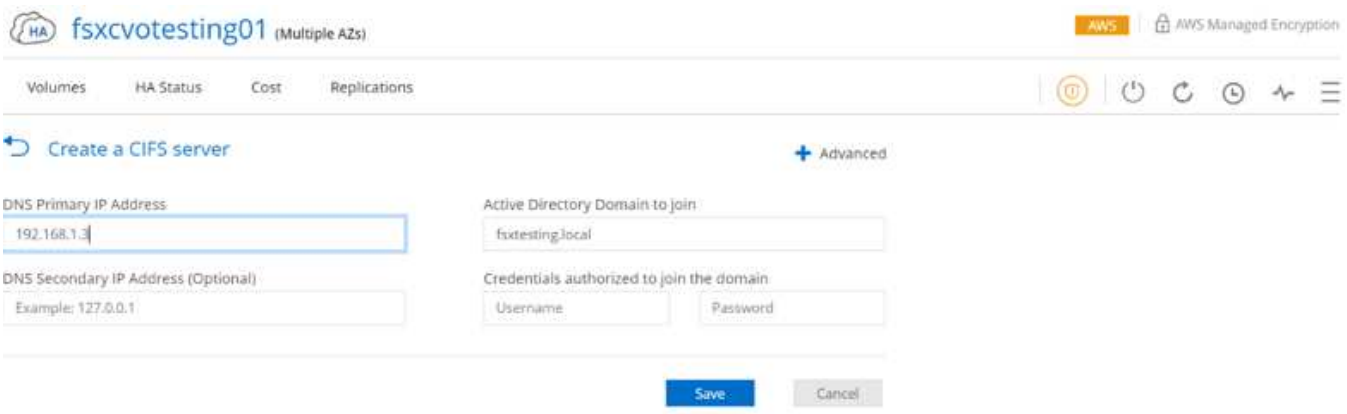


1. 配置Cloud Volumes ONTAP後，它會列在 Canvas 頁面上的工作環境中。



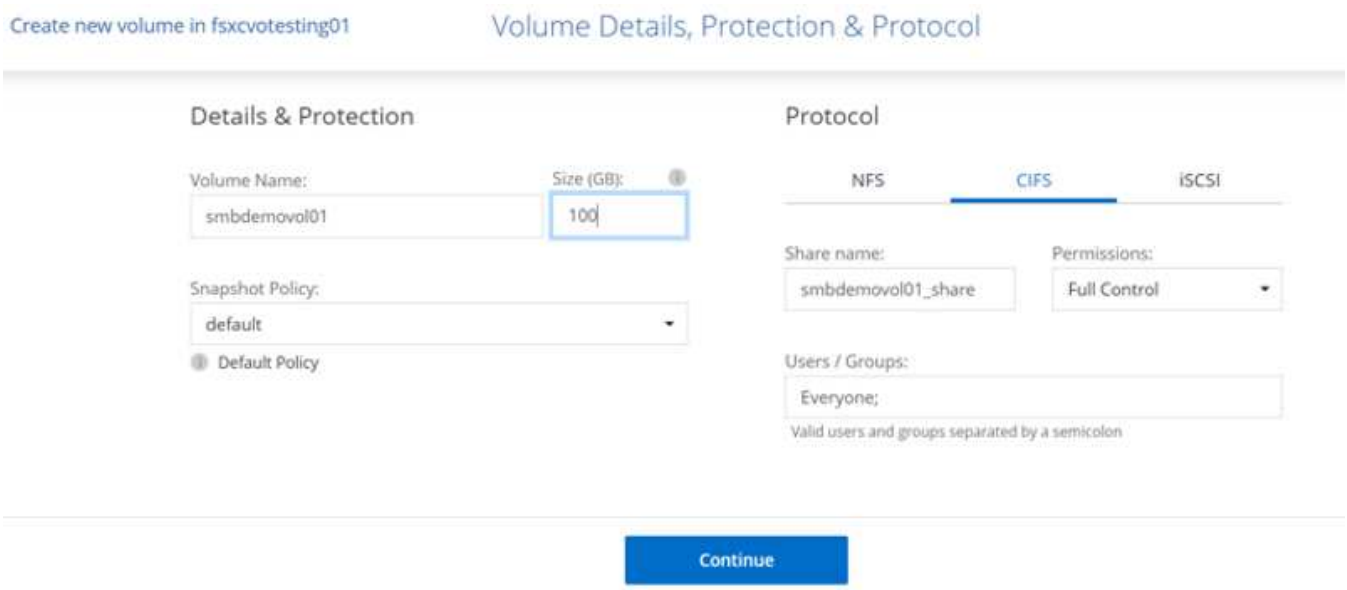
▼ **SMB** 磁碟區的附加配置

1. 工作環境準備好後，請確保 CIFS 伺服器配置了適當的 DNS 和 Active Directory 設定參數。在建立 SMB 磁碟區之前，需要執行此步驟。

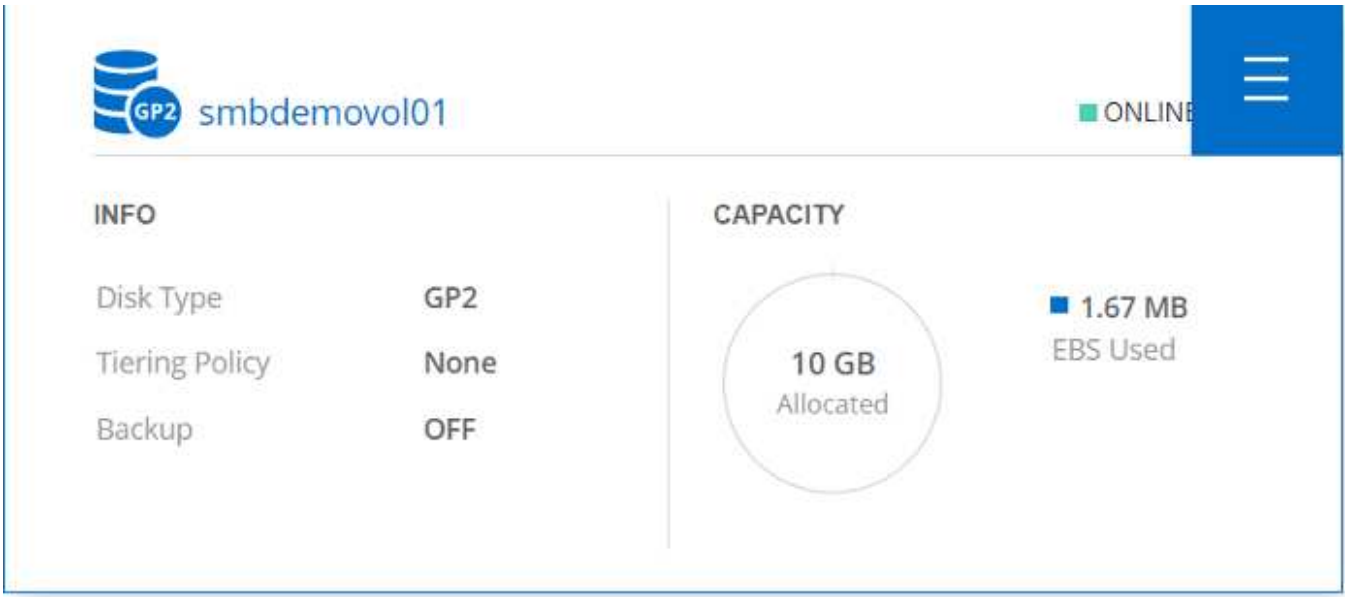


1. 選擇要建立磁碟區的 CVO 實例，然後按一下「建立磁碟區」選項。選擇適當的大小，雲端管理器選擇包

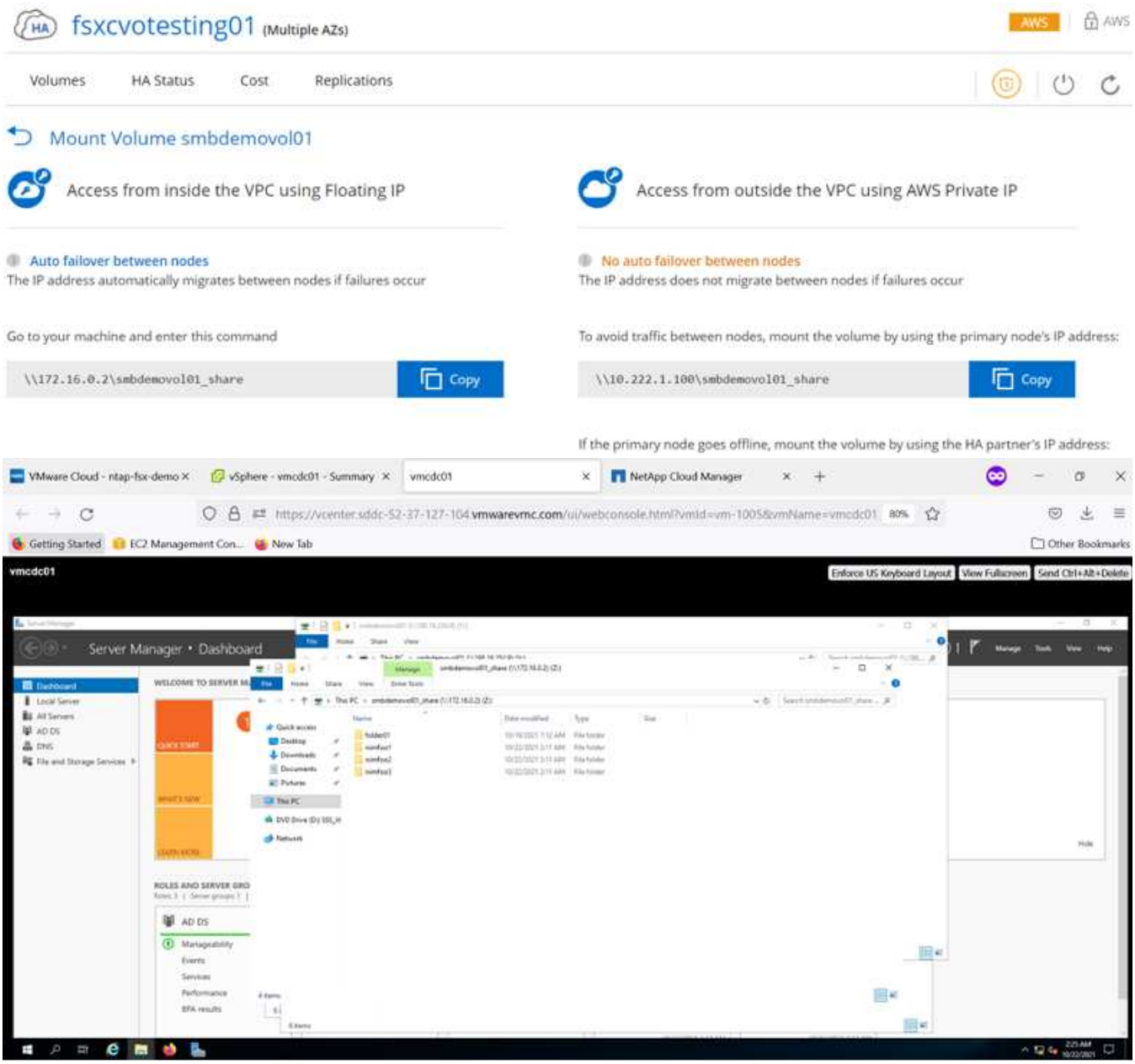
含的聚合或使用進階分配機制放置在特定的聚合上。對於此演示，選擇 SMB 作為協定。



1. 磁碟區配置完成後，可在「磁碟區」窗格下使用。由於已配置 CIFS 共享，因此您應該授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。



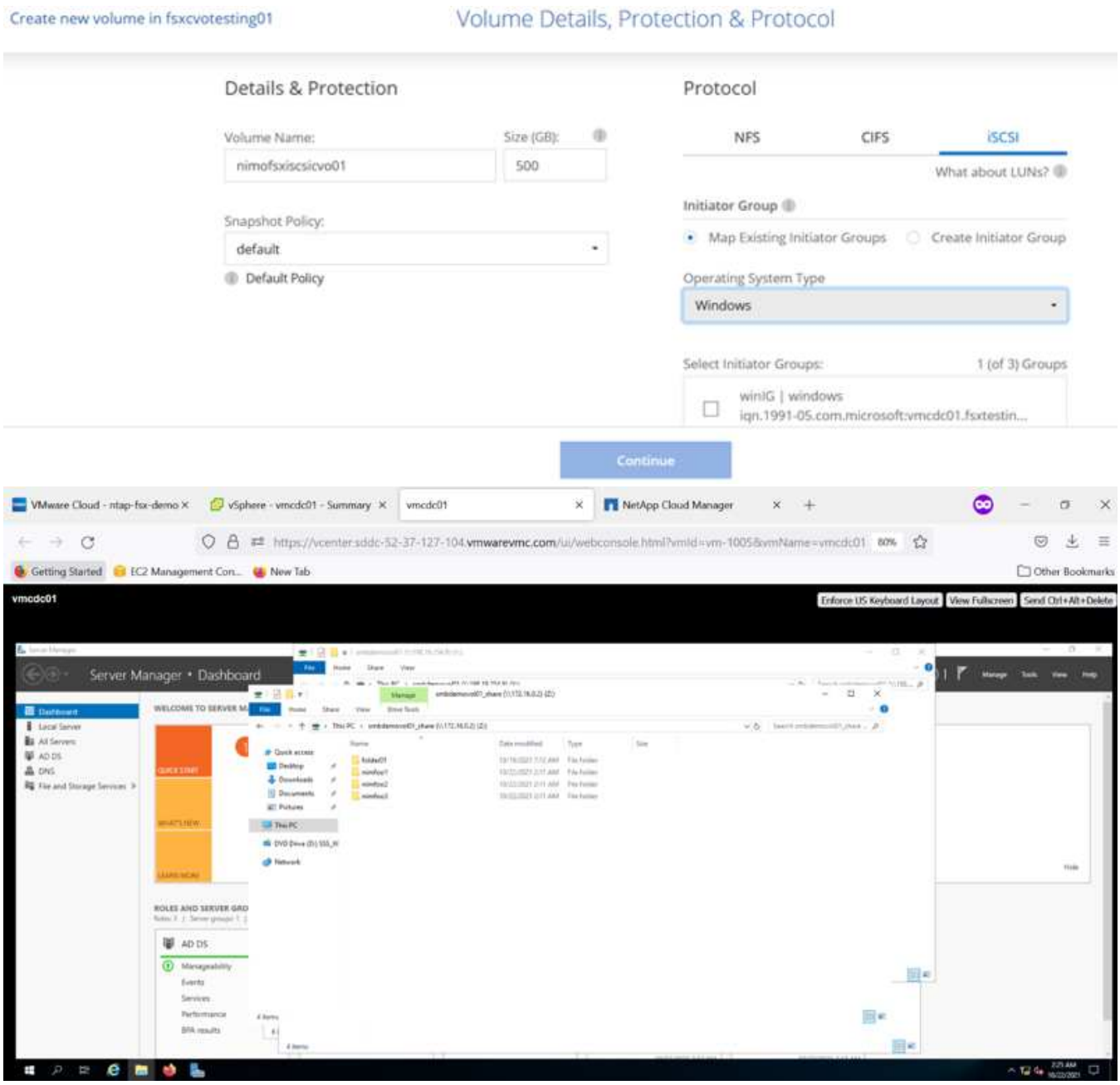
1. 建立磁碟區後，使用 mount 指令從 AWS SDDC 主機中 VMware Cloud 上執行的虛擬機器連接到共用。
2. 複製下列路徑並使用映射網路磁碟機選項將磁碟區掛載到 AWS SDDC 中 VMware Cloud 上執行的虛擬機器上。



▼ 將 **LUN** 連接到主機

若要將Cloud Volumes ONTAP LUN 連接到主機，請完成下列步驟：

1. 在 Cloud Manager Canvas 頁面上，雙擊Cloud Volumes ONTAP工作環境以建立和管理磁碟區。
2. 按一下新增磁碟區 > 新磁碟區，選擇 iSCSI，然後按一下建立啟動器群組。按一下「Continue（繼續）」。



1. 配置磁碟區後，選擇該磁碟區，然後按一下目標 IQN。若要複製 iSCSI 限定名稱 (IQN)，請按一下複製。建立從主機到 LUN 的 iSCSI 連線。

若要對位於 VMware Cloud on AWS SDDC 上的主機完成相同操作，請完成下列步驟：

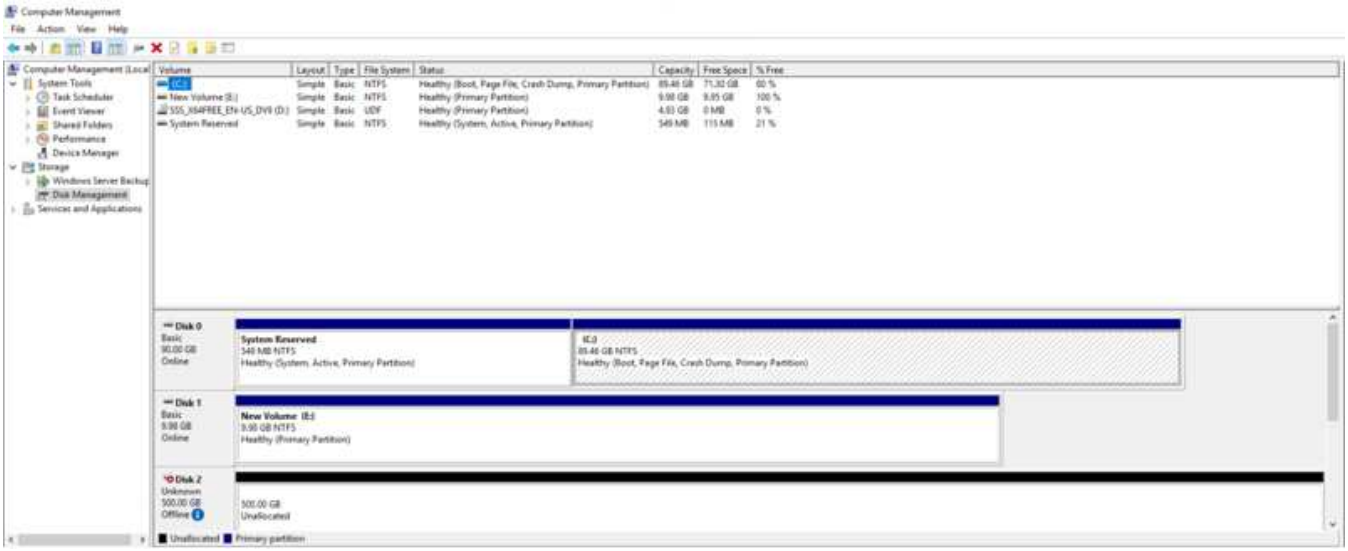
1. 透過 RDP 連接到 AWS 上的 VMware 雲端上託管的 VM。
2. 開啟 iSCSI 發起程式屬性對話方塊：伺服器管理員 > 儀表板 > 工具 > iSCSI 發起程式。
3. 在“發現”標籤中，按一下“發現入口網站”或“新增入口網站”，然後輸入 iSCSI 目標連接埠的 IP 位址。
4. 從「目標」標籤中，選擇發現的目標，然後按一下「登入」或「連線」。
5. 選擇啟用多路徑，然後選擇電腦啟動時自動恢復此連線或將此連線新增至收藏目標清單。按一下“進階”。

Windows 主機必須與群集中的每個節點建立 iSCSI 連線。本機 DSM 選擇要使用的最佳路徑。



SVM 中的 LUN 對 Windows 主機來說顯示為磁碟。主機不會自動發現任何新新增的磁碟。透過完成以下步驟觸發手動重新掃描以發現磁碟：

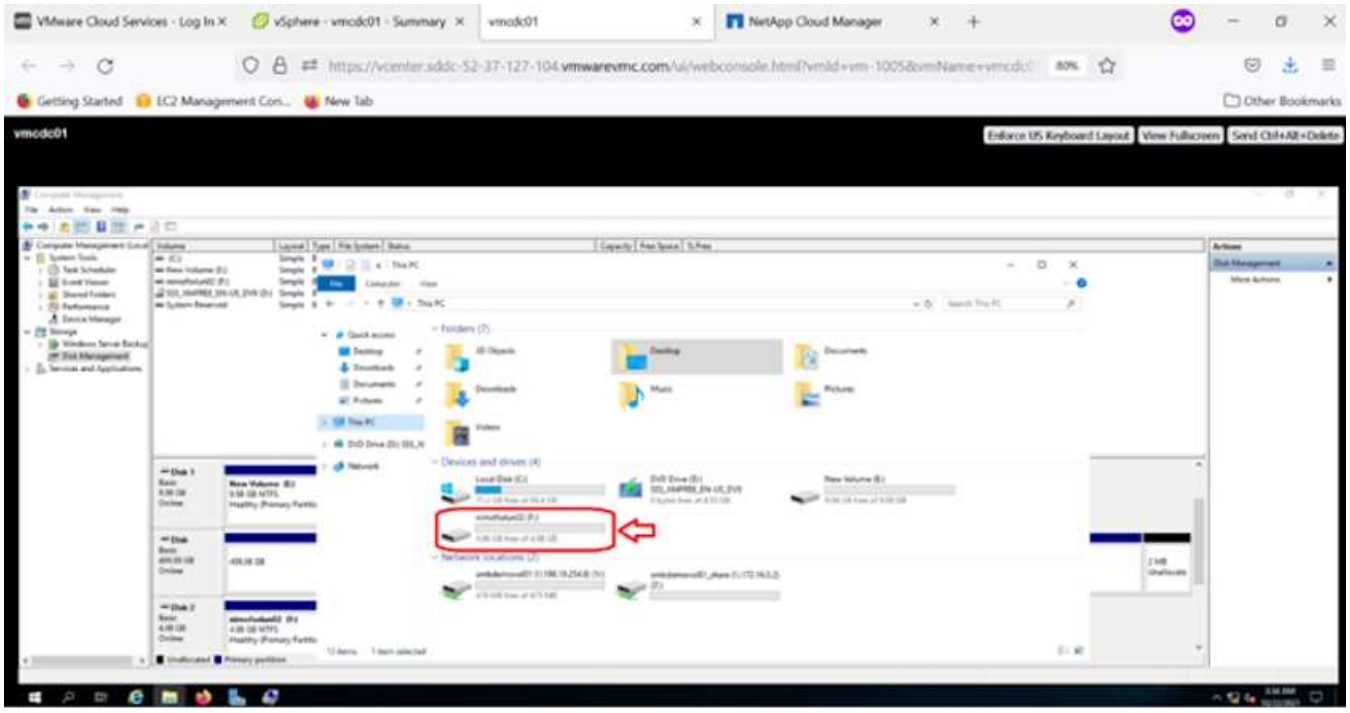
1. 開啟 Windows 電腦管理公用程式：開始 > 管理工具 > 電腦管理。
2. 在導航樹中展開儲存節點。
3. 按一下“磁碟管理”。
4. 按一下操作 > 重新掃描磁碟。



當 Windows 主機首次存取新的 LUN 時，它沒有分割區或檔案系統。初始化 LUN；並且（可選）透過完成以下步驟使用檔案系統格式化 LUN：

1. 啟動 Windows 磁碟管理。

2. 右鍵單擊 LUN，然後選擇所需的磁碟或分割區類型。
3. 請按照精靈中的說明進行操作。在此範例中，已安裝磁碟機 F:。



在 Linux 用戶端上，確保 iSCSI 守護程序正在執行。設定 LUN 後，請參閱有關 Linux 發行版的 iSCSI 設定的詳細指南。例如，Ubuntu iSCSI 配置可以找到"這裡"。要驗證，請從 shell 運行 lsblk cmd。

▼ 在 **Linux** 用戶端上掛載**Cloud Volumes ONTAP NFS** 卷

若要從 AWS SDDC 上的 VMC 內的虛擬機器掛載Cloud Volumes ONTAP (DIY) 檔案系統，請完成下列步驟：

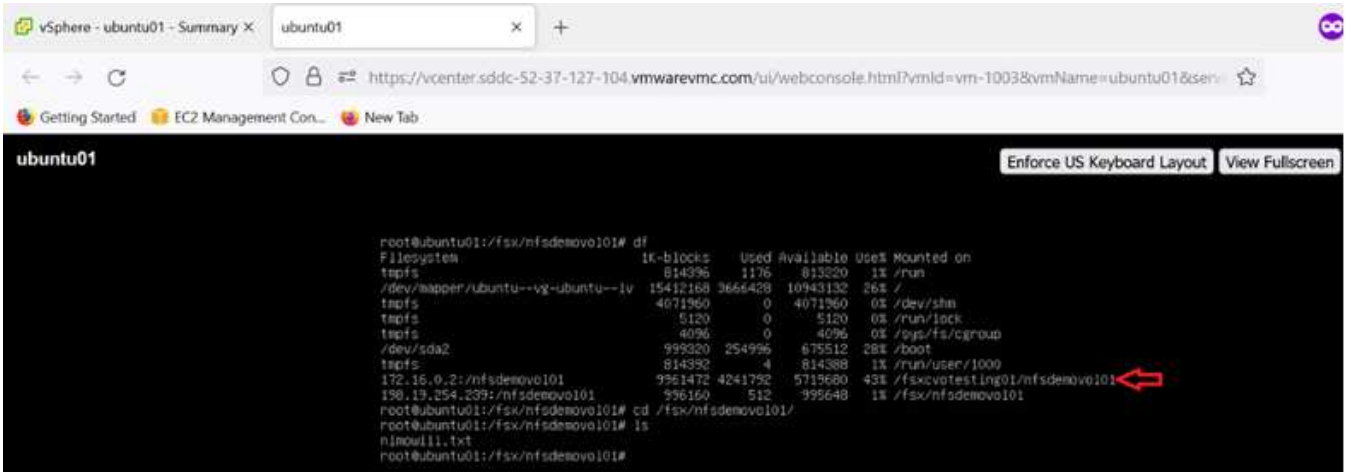
1. 連接到指定的Linux實例。
2. 使用安全殼 (SSH) 在執行個體上開啟終端並使用適當的憑證登入。
3. 使用下列指令為磁碟區的掛載點建立目錄。

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
```

. 將Amazon FSx ONTAP NFS 磁碟區掛載到上一個步驟所建立的目錄。

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```

```
root@ubuntu01:/fsx# mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdemovol01_
```



Azure 虛擬化服務：使用**NetApp**儲存裝置的選項

NetApp儲存可以作為來賓連接儲存或補充儲存附加到 Azure VMware 服務。

Azure NetApp Files(ANF) 作為補充 NFS 資料存儲

ESXi 版本 3 在本地部署中引入了 NFS 資料儲存支持，這極大地擴展了 vSphere 的儲存功能。

在 NFS 上執行 vSphere 是內部虛擬化部署廣泛採用的選項，因為它提供了強大的效能和穩定性。如果您在本機資料中心擁有大量網路附加儲存體 (NAS)，則應考慮使用 Azure NetApp File 資料儲存體在 Azure 中部署 Azure VMware 解決方案 SDDC，以克服容量和效能挑戰。

Azure NetApp Files是基於業界領先、高可用性的NetApp ONTAP資料管理軟體建置。 Microsoft Azure 服務分為三類：基礎、主流、專業。 Azure NetApp Files屬於專業類別，並由已在許多地區部署的硬體提供支援。透過內建的高可用性 (HA)， Azure NetApp Files可以保護您的資料免受大多數中斷的影響，並為您提供業界領先的 99.99%^ 正常運行時間的 SLA。

有關 ANF 作為補充 NFS 數據存儲的更多信息，請訪問：

- "ANF 作為補充 NFS 資料儲存：概述"
- "Azure 中的補充 NFS 資料儲存選項"

Azure NetApp Files(ANF) 作為來賓連接儲存

Azure NetApp Files為 Azure 帶來企業級資料管理和存儲，以便您可以輕鬆管理工作負載和應用程式。將您的工作負載遷移到雲端並運行它們，而不會犧牲效能。

Azure NetApp Files消除了障礙，因此您可以將所有基於檔案的應用程式遷移到雲端。這是第一次，您不必重新建立您的應用程序，並且您可以輕鬆獲得應用程式的持久性儲存。

由於該服務是透過 Microsoft Azure 入口網站提供的，因此使用者可以作為 Microsoft 企業協議的一部分體驗完全託管的服務。由 Microsoft 管理的世界級的支援讓您完全放心。此單一解決方案可讓您快速輕鬆地新增多協定工作負載。您可以建置和部署基於 Windows 和 Linux 檔案的應用程序，甚至對於傳統環境也是如此。

欲了解更多信息，請訪問"ANF 作為來賓連接存儲"。

Cloud Volumes ONTAP (CVO) 作為來賓連接存儲

Cloud Volumes ONTAP (CVO) 是基於 NetApp ONTAP儲存軟體所建置的業界領先的雲端資料管理解決方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的軟體定義版本，使用雲端原生存儲，允許您在雲端和本地使用相同的存儲軟體，從而無需重新培訓 IT 人員採用全新方法來管理資料。

CVO 使客戶能夠無縫地將資料從邊緣移動到資料中心、雲端並返回，從而將您的混合雲整合在一起 - 所有這些都透過單一窗格管理控制台NetApp Cloud Manager 進行管理。

CVO 的設計旨在提供極致的效能和先進的資料管理功能，以滿足您在雲端最嚴苛的應用程式

欲了解更多信息，請訪問"CVO 作為客戶連接存儲"。

ANF 資料儲存解決方案概述

每個成功的組織都走在轉型和現代化的道路上。作為此過程的一部分，公司通常會使用其現有的 VMware 投資，同時利用雲端優勢並探索如何盡可能使遷移、爆發、擴展和災難復原過程無縫。遷移到雲端的客戶必須評估彈性和爆發、資料中心退出、資料中心整合、生命週期終止場景、合併、收購等問題。每個組織所採用的方法可能因其各自的業務優先事項而異。在選擇基於雲端的操作時，選擇具有適當效能和最小阻礙的低成本模型是一個關鍵目標。除了選擇正確的平台之外，儲存和工作流程編排對於釋放雲端部署和彈性的力量也特別重要。

用例

儘管 Azure VMware 解決方案為客戶提供了獨特的混合功能，但有限的本機儲存選項限制了其對於儲存工作負載繁重的組織的實用性。由於儲存直接與主機綁定，因此擴展儲存的唯一方法是添加更多主機，這可能會使儲存密集型工作負載的成本增加 35-40% 或更多。這些工作負載需要額外的儲存空間，而不是額外的馬力，但這意味著需要支付額外的主機費用。

讓我們考慮以下場景；客戶需要六台主機來提供馬力（vCPU/vMem），但他們對儲存也有很大的需求。根據他們的評估，他們需要 12 台主機來滿足儲存需求。這會增加整體 TCO，因為他們必須購買所有額外的馬力，而他們真正需要的只是更多的儲存空間。這適用於任何用例，包括遷移、災難復原、爆發、開發/測試等等。

Azure VMware 解決方案的另一個常見用例是災難復原 (DR)。大多數組織都沒有萬無一失的 DR 策略，或者他們可能很難證明僅為了 DR 而運行幽靈資料中心是合理的。管理員可能會使用試點叢集或按需叢集來探索零佔用空間 DR 選項。然後他們可以擴展儲存而無需添加額外的主機，這可能是一個有吸引力的選擇。

總而言之，用例可以用兩種方式分類：

- 使用 ANF 資料儲存擴充儲存容量
- 使用 ANF 資料儲存作為災難復原目標，以便在軟體定義資料中心 (SDDC) 之間的本機或 Azure 區域內實現成本優化的復原工作流程。本指南深入介紹如何使用Azure NetApp Files為資料儲存提供最佳化儲存（目前處於公共預覽階段）以及 Azure VMware 解決方案中一流的資料保護和 DR 功能，使您能夠從 vSAN 儲存中卸載儲存容量。

有關使用 ANF 資料儲存的更多信息，請聯繫您所在地區的NetApp或 Microsoft 解決方案架構師。

Azure VMware 解決方案

Azure VMware 解決方案 (AVS) 是一種混合雲服務，可在 Microsoft Azure 公有雲中提供功能齊全的 VMware SDDC。 AVS 是使用 Azure 基礎架構、完全由 Microsoft 管理和支援並經過 VMware 驗證的第一方解決方案。因此，客戶可以獲得用於計算虛擬化的 VMware ESXi、用於超融合儲存的 vSAN 以及用於網路和安全的 NSX，同時利用 Microsoft Azure 的全球影響力、一流的資料中心設施以及與豐富的原生 Azure 服務和解決方案生態系統的接近性。 Azure VMware 解決方案 SDDC 和Azure NetApp Files的組合以最小的網路延遲提供了最佳效能。

無論使用哪種雲，部署 VMware SDDC 時，初始叢集都包含以下元件：

- VMware ESXi 主機用於計算虛擬化，並使用 vCenter 伺服器設備進行管理。
- VMware vSAN 超融合存儲，整合了每個 ESXi 主機的實體儲存資產。
- VMware NSX 用於虛擬網路和安全，並使用 NSX Manager 叢集進行管理。

結論

無論您的目標是全雲還是混合雲，Azure NetApp檔案都提供了出色的選項來部署和管理應用程式工作負載以及檔案服務，同時透過將資料需求無縫連接到應用程式層來降低 TCO。無論用例如何，選擇 Azure VMware 解決方案以及Azure NetApp Files都可以快速實現雲端優勢、跨本地和多個雲端的一致基礎架構和操作、工作負載的雙向可移植性以及企業級容量和效能。它與用於連接儲存的熟悉的過程和程序相同。請記住，只是資料的位置隨著新名稱而改變了；工具和流程都保持不變， Azure NetApp Files有助於優化整體部署。

總結

該文件的要點包括：

- 現在您可以將Azure NetApp Files用作 AVS SDDC 上的資料儲存。
- 提高應用程式回應時間並提供更高的可用性，以便在需要的時間和地點提供存取工作負載資料。
- 透過簡單、即時的調整大小功能簡化 vSAN 儲存的整體複雜性。
- 使用動態重塑功能保證關鍵任務工作負載的效能。
- 如果 Azure VMware 解決方案雲端是目標，Azure NetApp Files是最佳化部署的正確儲存解決方案。

在哪裡可以找到更多信息

要了解有關本文檔中描述的信息的更多信息，請參閱以下網站連結：

- Azure VMware 解決方案文檔

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

- Azure NetApp Files文檔

  "https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- 將Azure NetApp Files儲存體附加到 Azure VMware 解決方案主機（預覽版）

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-

hosts?tabs=azure-portal/

在 **Azure** 中建立補充 **NFS** 資料存儲

ESXi 版本 3 在本地部署中引入了 NFS 資料儲存支持，這極大地擴展了 vSphere 的儲存功能。

在 NFS 上執行 vSphere 是內部虛擬化部署廣泛採用的選項，因為它提供了強大的效能和穩定性。如果您在本機資料中心擁有大量網路附加儲存體 (NAS)，則應考慮使用 Azure NetApp File 資料儲存體在 Azure 中部署 Azure VMware 解決方案 SDDC，以克服容量和效能挑戰。

Azure NetApp Files是基於業界領先、高可用性的NetApp ONTAP資料管理軟體建置。 Microsoft Azure 服務分為三類：基礎、主流、專業。 Azure NetApp Files屬於專業類別，並由已在許多地區部署的硬體提供支援。憑藉內建的高可用性 (HA)， Azure NetApp Files可保護您的資料免受大多數中斷的影響，並為您提供業界領先的 SLA "99.99%"正常運轉時間。

在引入Azure NetApp Files資料儲存功能之前，規劃託管效能和儲存密集型工作負載的客戶的橫向擴展操作需要擴展運算和儲存。

請記住以下問題：

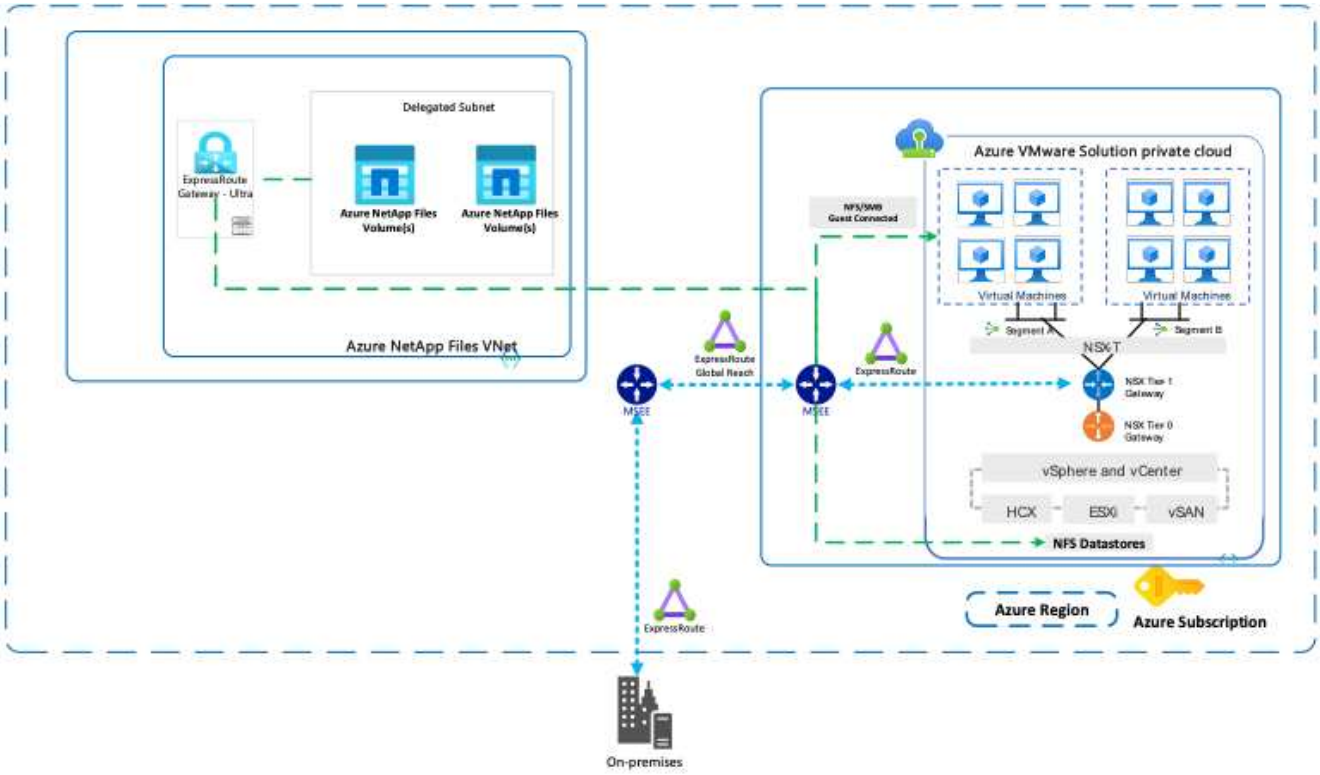
- 不建議在 SDDC 叢集中使用不平衡的叢集配置。因此，擴展儲存意味著添加更多主機，這意味著更多的 TCO。
- 僅可實作一個 vSAN 環境。因此，所有儲存流量都直接與生產工作負載競爭。
- 沒有提供多個效能層來滿足應用程式要求、效能和成本的選項。
- 在叢集主機之上建置的 vSAN 很容易達到儲存容量的極限。透過將 Azure 原生平台即服務 (PaaS) 產品（如Azure NetApp Files）集成為資料存儲，客戶可以選擇單獨擴展其存儲，並且僅根據需要向 SDDC 叢集新增運算節點。這種能力克服了上述挑戰。

Azure NetApp Files還允許您部署多個資料存儲，透過將虛擬機器放置在適當的資料儲存中並分配所需的服務等級以滿足工作負載效能要求，這有助於模擬本地部署模型。憑藉其獨特的多協定支援功能，客戶儲存成為 SQL 和 Oracle 等資料庫工作負載的附加選項，同時還可使用補充 NFS 資料儲存功能來容納剩餘的 VMDK。除此之外，本機快照功能可讓您執行快速備份和粒度復原。

> ⓘ 聯絡 Azure 和NetApp解決方案架構師來規劃和調整儲存大小並確定所需的主機數量。 NetApp建議在最終確定測試、POC 和生產部署的資料儲存佈局之前確定儲存效能要求。

詳細架構

從高層次的角度來看，該架構描述如何實現跨本地環境和 Azure 的混合雲連接和應用程式可移植性。它還描述如何使用Azure NetApp Files作為補充 NFS 資料儲存以及作為 Azure VMware 解決方案上託管的客戶虛擬機器的客戶端儲存選項。



漿紗

遷移或災難復原中最重要的方面是確定目標環境的正確規模。了解需要多少個節點才能完成從本機到 Azure VMware 解決方案的直接遷移練習非常重要。

對於大小調整，請使用 RVTools（首選）或其他工具（如 Live Optics 或 Azure Migrate）使用來自本機環境的歷史資料。 RVTools 是捕獲 vCPU、vMem、vDisk 和所有所需資訊（包括已開啟或關閉的虛擬機器）以表徵目標環境的理想工具。

若要執行 RVtools，請完成以下步驟：

1. 下載並安裝 RVTools。
2. 執行 RVTools，輸入連接到本機 vCenter Server 所需的信息，然後按「登入」。
3. 將庫存匯出到 Excel 電子表格。
4. 編輯電子表格並從 vInfo 標籤中刪除任何不理想的虛擬機器。此方法提供了有關儲存需求的清晰輸出，可用於根據所需數量的主機正確調整 Azure VMware SDDC 叢集的大小。

> 與來賓內儲存空間一起使用的來賓虛擬機器必須單獨計算；但是， Azure NetApp Files可以輕鬆覆蓋額外的儲存容量，從而保持較低的整體 TCO。

部署和配置 **Azure VMware** 解決方案

與本地一樣，規劃 Azure VMware 解決方案對於成功建立虛擬機器和遷移的生產就緒環境至關重要。

本節介紹如何設定和管理 AVS，以便將其與Azure NetApp Files結合使用，作為具有來賓內儲存的資料儲存。

設定過程可分為三個部分：

- 註冊資源提供者並建立私有雲。
- 連接到新的或現有的 ExpressRoute 虛擬網路閘道。
- 驗證網路連線並存取私有雲。參考這個"關聯"有關 Azure VMware 解決方案 SDDC 預配過程的逐步演練。

使用 **Azure VMware** 解決方案設定**Azure NetApp Files**

Azure NetApp Files之間的新整合使您能夠透過 Azure VMware 解決方案資源提供者 API/CLI 使用Azure NetApp Files磁碟區建立 NFS 資料存儲，並將資料儲存安裝在私有雲中您選擇的叢集上。除了容納 VM 和應用程式 VMDK 之外，Azure NetApp檔案磁碟區還可以從 Azure VMware 解決方案 SDDC 環境中建立的 VM 中裝載。由於Azure NetApp Files支援伺服器訊息區塊 (SMB) 和網路檔案系統 (NFS) 協議，因此磁碟區可以安裝在 Linux 用戶端上並對應到 Windows 用戶端上。

> 為了獲得最佳效能，請將Azure NetApp Files部署在與私有雲相同的可用區域中。與 Express 路由快速路徑共置可提供最佳效能，同時最大程度地減少網路延遲。

若要將 Azure NetApp檔案磁碟區附加為 Azure VMware 解決方案私有雲的 VMware 資料存儲，請確保滿足以下先決條件。

▼ 先決條件

1. 使用 az login 並驗證訂閱是否已註冊至 Microsoft.AVS 命名空間中的 CloudSanExperience 功能。

```
az login –tenant xcvxcvxc- vxcv- xcvx- cvxc- vxcvxcvxcv
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

1. 如果未註冊，則註冊。

```
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

> 註冊大約需要 15 分鐘才能完成。

1. 若要檢查註冊狀態，請執行以下命令。

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
--query properties.state
```

1. 如果註冊停留在中間狀態超過 15 分鐘，則取消註冊，然後重新註冊該標誌。

```
az feature unregister --name "CloudSanExperience" --namespace
"Microsoft.AVS"
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

1. 驗證訂閱是否已註冊至 Microsoft.AVS 命名空間中的 AnfDatastoreExperience 功能。

```
az feature show --name "AnfDatastoreExperience" --namespace
"Microsoft.AVS" --query properties.state
```

1. 驗證 vmware 擴充功能是否已安裝。

```
az extension show --name vmware
```

1. 如果擴充功能已安裝，請驗證版本是否為 3.0.0。如果安裝了舊版本，請更新擴充功能。

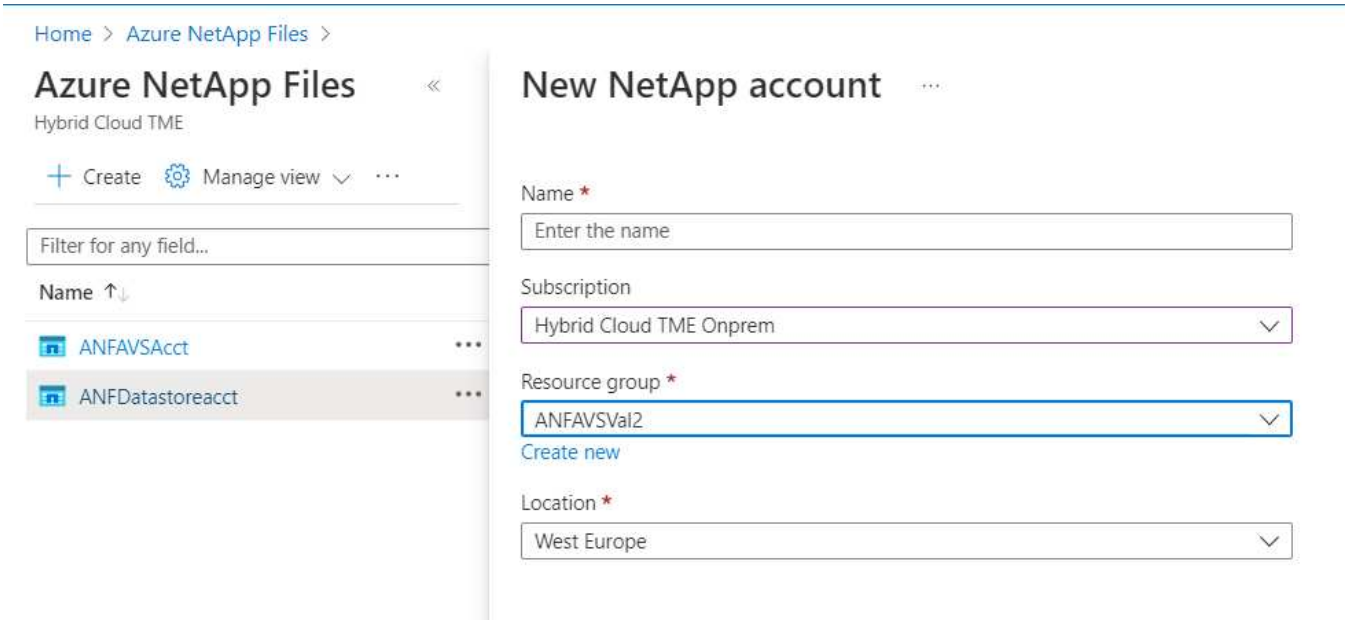
```
az extension update --name vmware
```

1. 如果尚未安裝該擴展，請安裝它。

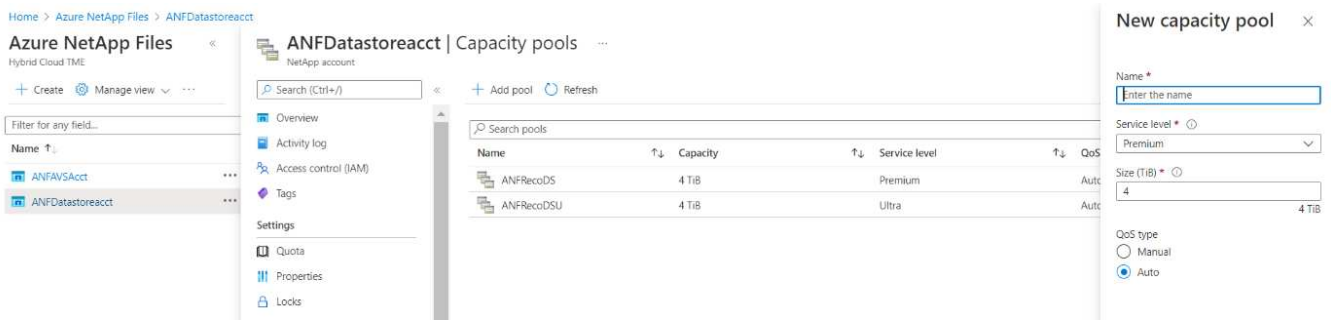
```
az extension add --name vmware
```

▼ 建立和裝載**Azure NetApp Files**卷

1. 登入 Azure 入口網站並存取Azure NetApp Files。驗證對Azure NetApp FilesAzure NetApp Files的存取權限，並使用 `az provider register `--namespace Microsoft.NetApp –wait`命令。註冊後，建立一個NetApp帳戶。參考這個 "關聯"了解詳細步驟。



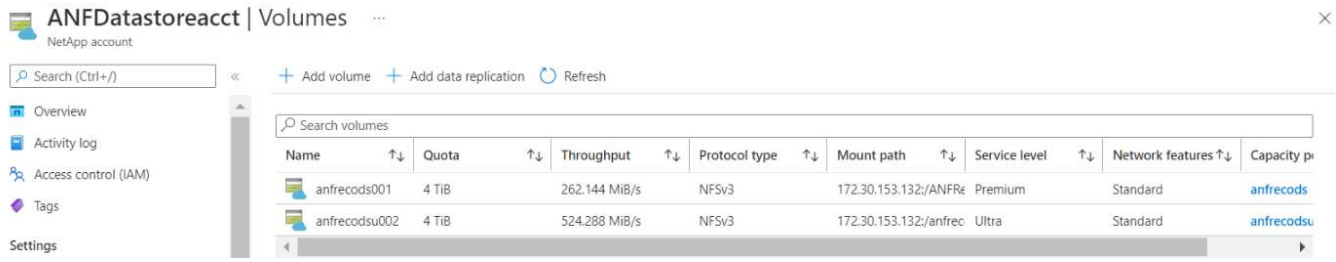
1. 建立NetApp帳戶後，設定具有所需服務等級和大小的容量池。有關詳細信息，請參閱此 "關聯"。



需要記住的要點

- Azure NetApp Files上的資料儲存支援 NFSv3。
- 在補充預設 vSAN 儲存的同時，根據需要對容量受限的工作負載使用進階或標準層，對效能受限的工作負載使用超級層。

1. 為Azure NetApp Files設定委託子網，並在建立磁碟區時指定此子網路。有關建立委託子網路的詳細步驟，請參閱此 "關聯"。
2. 使用容量池側邊欄標籤下的磁碟區側邊欄標籤為資料儲存區新增 NFS 磁碟區。



若要了解Azure NetApp Files磁碟區按大小或配額的效能，請參閱"Azure NetApp Files的效能注意事項"。

▼ 將 **Azure NetApp**檔案資料儲存新增至私有雲

可以使用 Azure 入口網站將Azure NetApp Files磁碟區附加到您的私有雲。關注此"來自微軟的連結"使用 Azure 入口網站逐步掛載 Azure NetApp檔案資料儲存體。

若要將 Azure NetApp檔案資料儲存體新增至私有雲，請完成下列步驟：

1. 註冊所需的功能後，透過執行適當的命令將 NFS 資料儲存附加到 Azure VMware 解決方案私有雲叢集。
2. 使用 Azure VMware 解決方案私有雲叢集中的現有 ANF 磁碟區建立資料儲存體。

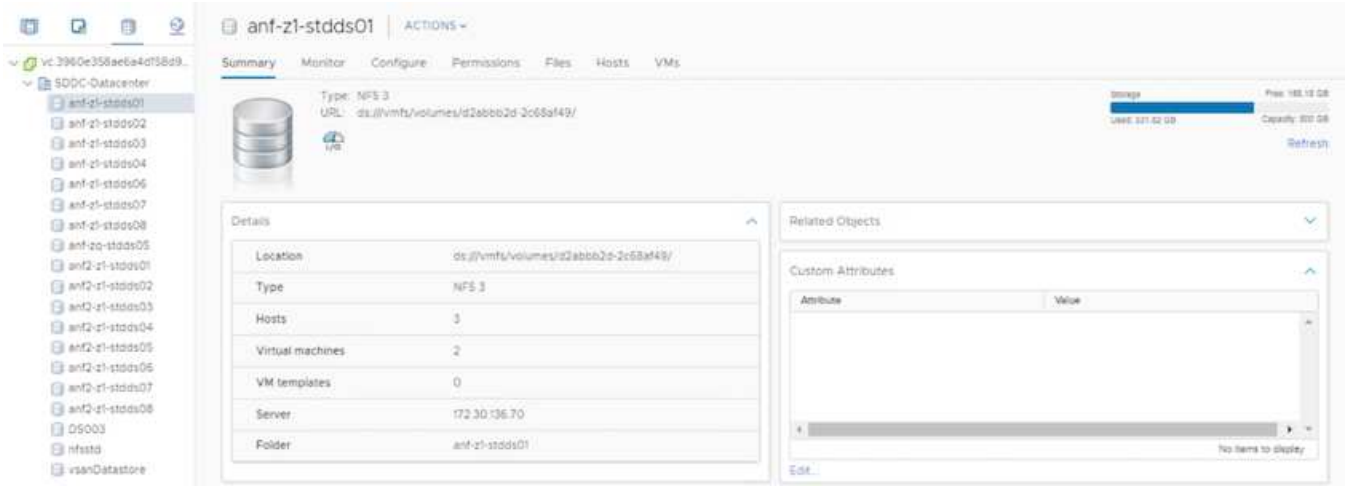
```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
```

```
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}

. List all the datastores in a private cloud cluster.
```

C:\Users\niyaz>az vmware 資料儲存清單 --resource-group anfavsval2 --cluster Cluster-1 --private-cloud ANFDataClus [{ 「diskPoolVolume」 ：null，「id」 ：「/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFuster/clusters/clusters/clusters/K105/cluster/cluster/cluster） “name”： “ANFRecoDS001”， “netAppVolume”：{ “id”：“/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/ NetApp./netAppAccounts/anfdatastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001”， “resourceGroup”：“anfavsval2”}，“provisioningState”：“成功”， “resourceGroup”：“anfavsvals”，anfwate” ：“成功”，“resourceGroup”：“anfavsvalvs”，gprivavsvalv.” “diskPoolVolume”：null， “id” ：“/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFusterC/clusters/cluster” “name”：“ANFRecoDSU002”， “netAppVolume”：{ “id”： “/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfod.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfododsu/volumes/fodm ””} ，“provisioningState”：“成功”， “resourceGroup”： “anfavsval2”， “type” ：“Microsoft.AVS/privateClouds/clusters/datastores”}]

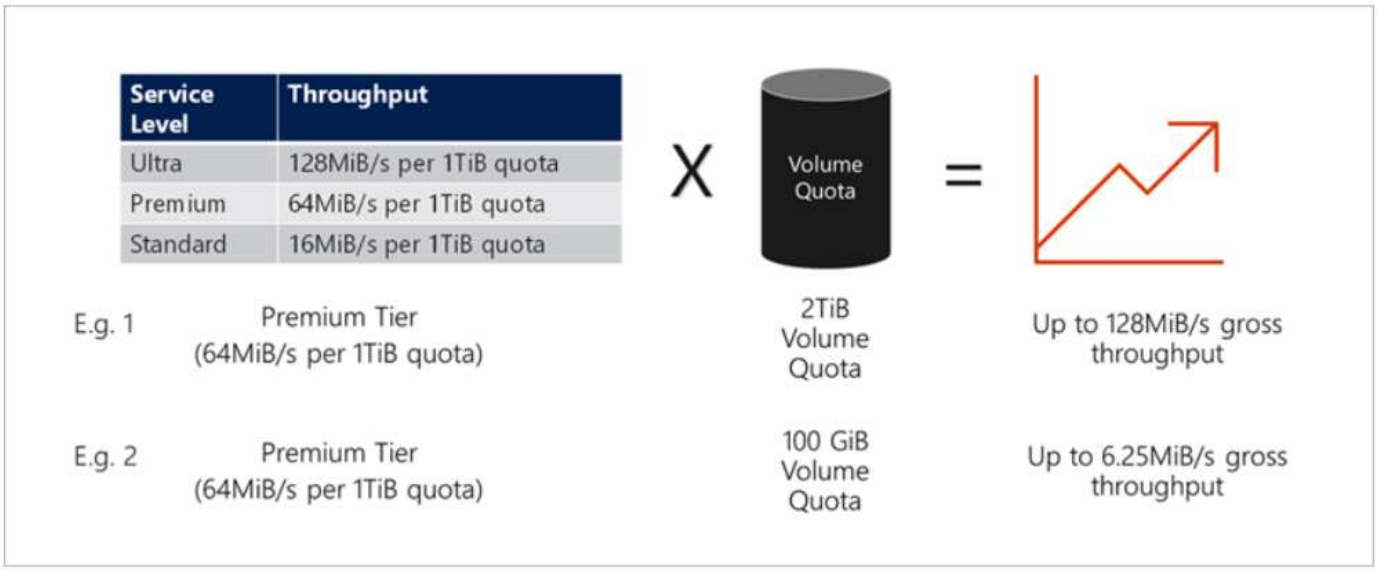
1. 在建立必要的連接後，磁碟區將作為資料儲存安裝。



尺寸和性能優化

Azure NetApp Files支援三種服務等級：標準等級（每 TB 16MBps）、進階（每 TB 64MBps）和超級等級（每 TB 128MBps）。配置正確的磁碟區大小對於資料庫工作負載的最佳效能非常重要。使用Azure NetApp Files，磁碟區效能和吞吐量限制根據以下因素決定：

- 卷所屬容量池的服務級別
- 分配給卷的配額
- 容量池的服務品質 (QoS) 類型（自動或手動）



有關更多信息，請參閱 "Azure NetApp Files的服務級別" 。

參考這個"來自微軟的連結"以獲得可在規模調整練習期間使用的詳細性能基準。

需要記住的要點

- 使用進階或標準層作為資料儲存卷，以獲得最佳容量和效能。如果需要效能，則可以使用超級層。
- 對於來賓掛載要求，請使用 Premium 或 Ultra 層；對於來賓虛擬機器的檔案共用要求，請使用 Standard 或 Premium 層磁碟區。

性能考慮

重要的是要理解，使用 NFS 版本 3 時，ESXi 主機和單一儲存目標之間的連接只有一個活動管道。這意味著儘管可能存在可用於故障轉移的備用連接，但單一資料儲存和底層儲存的頻寬僅限於單一連接所能提供的頻寬。

為了利用Azure NetApp Files磁碟區更多可用的頻寬，ESXi 主機必須與儲存目標建立多個連線。為了解決此問題，您可以設定多個資料儲存區，每個資料儲存區使用 ESXi 主機和儲存之間的單獨連線。

為了獲得更高的頻寬，最佳做法是使用多個 ANF 磁碟區建立多個資料儲存區，建立 VMDK，並在 VMDK 之間對邏輯磁碟區進行條帶化。

參考這個"來自微軟的連結"以獲得可在規模調整練習期間使用的詳細性能基準。

需要記住的要點

- Azure VMware 解決方案預設允許八個 NFS 資料儲存。這可以透過支援請求來增加。
- 利用 ER 快速路徑和 Ultra SKU 實現更高的頻寬和更低的延遲。更多資訊
- 透過 Azure NetApp檔案中的「基本」網路功能，來自 Azure VMware 解決方案的連接受 ExpressRoute 線路和 ExpressRoute 閘道的頻寬約束。
- 對於具有「標準」網路功能的Azure NetApp Files卷，支援 ExpressRoute FastPath。啟用後，FastPath 會將網路流量直接傳送到Azure NetApp Files卷，繞過網關，從而提供更高的頻寬和更低的延遲。

增加資料儲存的大小

磁碟區重塑和動態服務等級變化對於 SDDC 來說是完全透明的。在Azure NetApp Files中，這些功能可提供持續的效能、容量和成本最佳化。透過從 Azure 入口網站調整磁碟區大小或使用 CLI 來增加 NFS 資料儲存體的大小。完成後，存取 vCenter，轉到資料儲存選項卡，右鍵單擊相應的資料存儲，然後選擇刷新容量資訊。這種方法可用於增加資料儲存容量，並以動態方式提高資料儲存的效能，且無需停機。這個過程對於應用程式來說也是完全透明的。

需要記住的要點

- 磁碟區重塑和動態服務等級功能可讓您透過調整穩定狀態工作負載的大小來最佳化成本，從而避免過度配置。
- VAAI 未啟用。

工作負載

▼ 遷移

最常見的用例之一是遷移。使用 VMware HCX 或 vMotion 移動本機虛擬機器。或者，您可以使用 Rivermeadow 將虛擬機器遷移到Azure NetApp Files資料儲存。

▼ 資料保護

備份虛擬機器並快速恢復它們是 ANF 資料儲存的一大優勢。使用 Snapshot 副本快速複製您的 VM 或資料儲存而不影響效能，然後將它們傳送到 Azure 儲存體以實現長期資料保護，或使用跨區域複製將其發送到輔助區域以實現災難復原。這種方法僅儲存改變的訊息，從而最大限度地減少了儲存空間和網路頻寬。

使用Azure NetApp FilesSnapshot 副本進行常規保護，並使用應用程式工具保護駐留在來賓虛擬機器上的事務資料（例如 SQL Server 或 Oracle）。這些 Snapshot 副本與 VMware（一致性）快照不同，適合長期保護。

使用 ANF 資料存儲，「恢復到新磁碟區」選項可用於複製整個資料儲存卷，並且復原的磁碟區可以作為另一個資料儲存安裝到 AVS SDDC 內的主機。安裝資料儲存後，可以註冊、重新配置和自訂其中的虛擬機，就像單獨複製的虛擬機一樣。

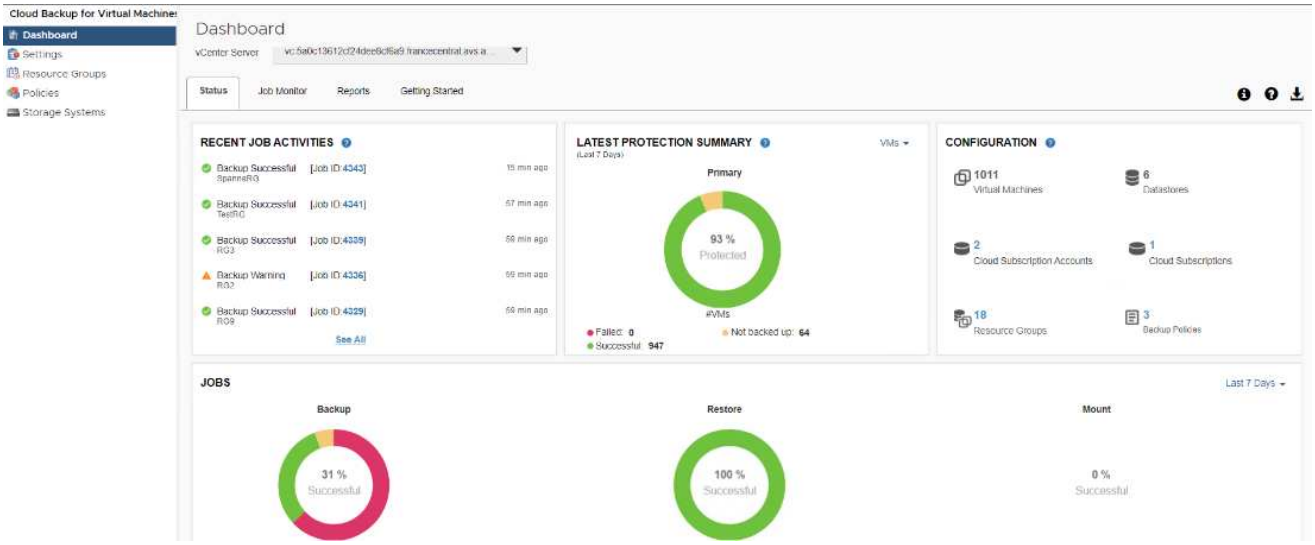
▼ **NetApp Backup and Recovery** 適用於虛擬機器

NetApp Backup and Recovery for Virtual Machines 在 vCenter 上提供 vSphere Web 用戶端 GUI，可透過備份原則保護 Azure VMware Solution 虛擬機器和 Azure NetApp Files 資料存放區。這些原則可定義排程、保留及其他功能。NetApp Backup and Recovery for Virtual Machine 的功能可使用 Run 命令進行部署。

可以透過完成以下步驟來安裝設定和保護策略：

1. 使用 Run 命令在 Azure VMware Solution 私有雲中安裝虛擬機器的 NetApp Backup and Recovery。
2. 新增雲端訂閱憑證（用戶端和金鑰值），然後新增包含您想要保護的資源的雲端訂閱帳戶（NetApp帳戶和相關資源群組）。
3. 建立一個或多個備份策略來管理資源組備份的保留、頻率和其他設定。
4. 建立一個容器來新增一個或多個需要使用備份策略保護的資源。
5. 如果發生故障，將整個 VM 或特定的單一 VMDK 恢復到相同位置。

透過Azure NetApp Files Snapshot 技術，備份和復原速度非常快。



▼ 使用**Azure NetApp Files**、**JetStream DR** 和 **Azure VMware** 解決方案進行災難復原

災難復原到雲端是一種具有彈性且經濟高效的方法，可以保護工作負載免受網站中斷和資料損壞事件（例如勒索軟體）的影響。使用 VMware VAIO 框架，可以將本機 VMware 工作負載複製到 Azure Blob 儲存體並進行恢復，從而實現最少或幾乎沒有資料遺失以及接近零的 RTO。 JetStream DR 可用於無縫恢復從本地複製到 AVS 以及特別是Azure NetApp Files 的工作負載。它透過使用災難復原站點的最少資源和經濟高效的雲端儲存來實現經濟高效的災難復原。 JetStream DR 透過 Azure Blob Storage 自動還原到 ANF 資料儲存。 JetStream DR 根據網路映射將獨立的虛擬機器或相關虛擬機器群組還原到復原站點基礎架構中，並提供時間點復原以進行勒索軟體保護。

"採用 ANF、JetStream 和 AVS 的 DR 解決方案" 。

適用於 **Azure** 的**NetApp**來賓連線儲存選項

Azure 支援透過本機Azure NetApp Files(ANF) 服務或Cloud Volumes ONTAP (CVO) 連接來賓的NetApp儲存體。

Azure NetApp Files(ANF)

Azure netApp Files 為 Azure 帶來企業級資料管理和存儲，以便您可以輕鬆管理工作負載和應用程式。將您的工作負載遷移到雲端並運行它們，而不會犧牲效能。

Azure netApp Files 消除了障礙，因此您可以將所有基於檔案的應用程式移轉到雲端。這是第一次，您不必重新建立您的應用程序，並且您可以輕鬆獲得應用程式的持久性儲存。

由於該服務是透過 Microsoft Azure 入口網站提供的，因此使用者可以作為 Microsoft 企業協議的一部分體驗完全託管的服務。由 Microsoft 管理的世界級的支援讓您完全放心。此單一解決方案可讓您快速輕鬆地新增多協定工作負載。您可以建置和部署基於 Windows 和 Linux 檔案的應用程序，甚至對於傳統環境也是如此。

Azure NetApp Files(ANF) 作為來賓連接儲存

▼ 使用 **Azure VMware** 解決方案 **(AVS)** 設定**Azure NetApp Files**

可以從 Azure VMware 解決方案 SDDC 環境中建立的 VM 裝載Azure NetApp Files共用。由於Azure NetApp Files支援 SMB 和 NFS 協議，因此磁碟區也可以安裝在 Linux 用戶端上並對應到 Windows 用戶端上。只需五個簡單的步驟即可設定Azure NetApp Files磁碟區。

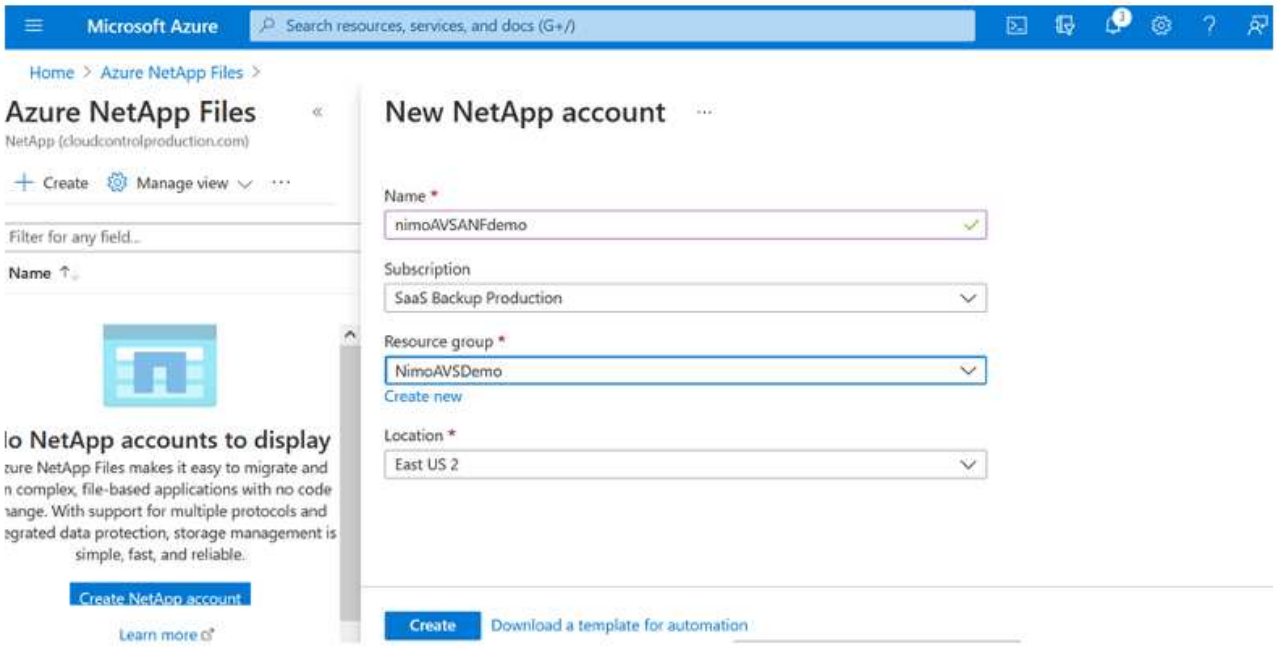
Azure NetApp Files和 Azure VMware 解決方案必須位於相同 Azure 區域。

▼ 建立和裝載**Azure NetApp Files**卷

若要建立和裝載Azure NetApp Files卷，請完成以下步驟：

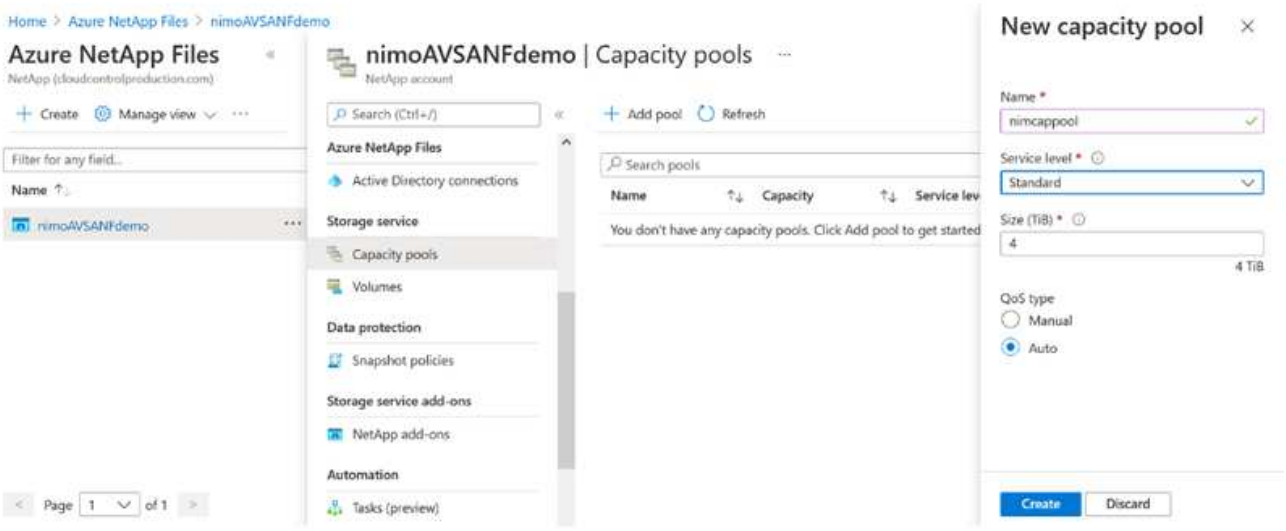
1. 登入 Azure 入口網站並存取Azure NetApp Files。驗證對Azure NetApp Files服務的訪問，並使用NetApp provider register --namespace Microsoft.NetApp –wait 命令註冊Azure NetApp Files資源提供者。註冊完成後，建立一個NetApp帳戶。

   詳細步驟請參見"Azure NetApp Files共享"。本頁將引導您完成逐步的過程。

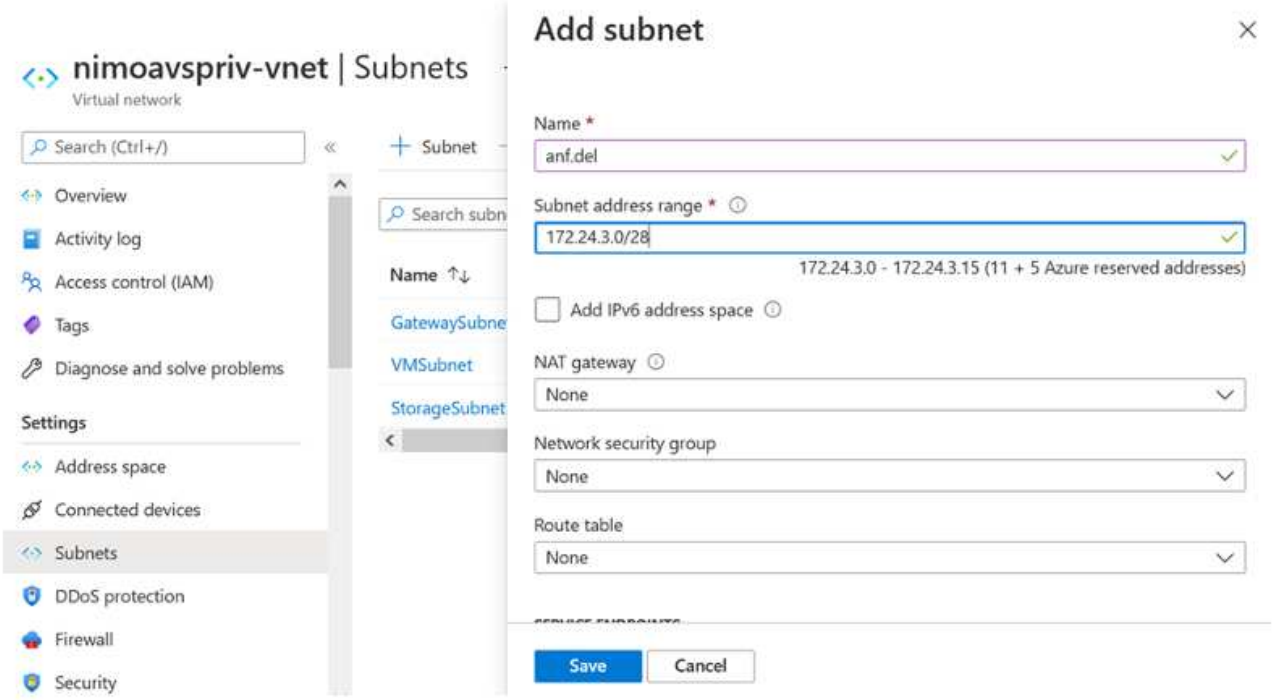


2. 建立NetApp帳戶後，設定具有所需服務等級和大小的容量池。

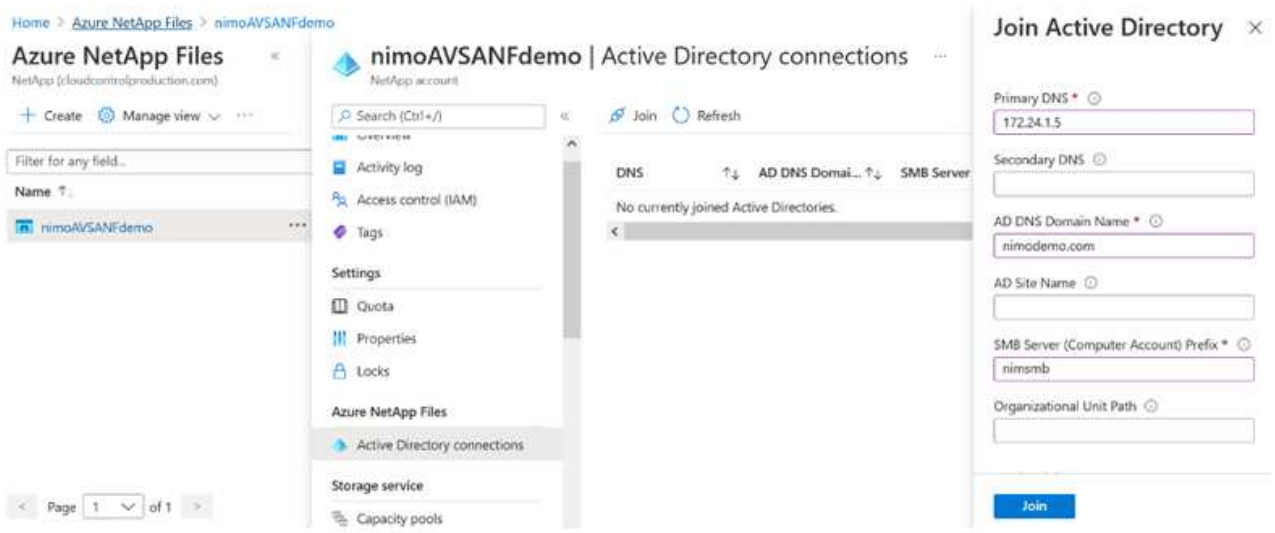
   有關更多信息，請參閱"設定容量池Set up a capacity pool" 。



3. 為Azure NetApp Files設定委派子網，並在建立磁碟區時指定此子網路。有關建立委託子網路的詳細步驟，請參閱"將子網路委託給Azure NetApp Files"。

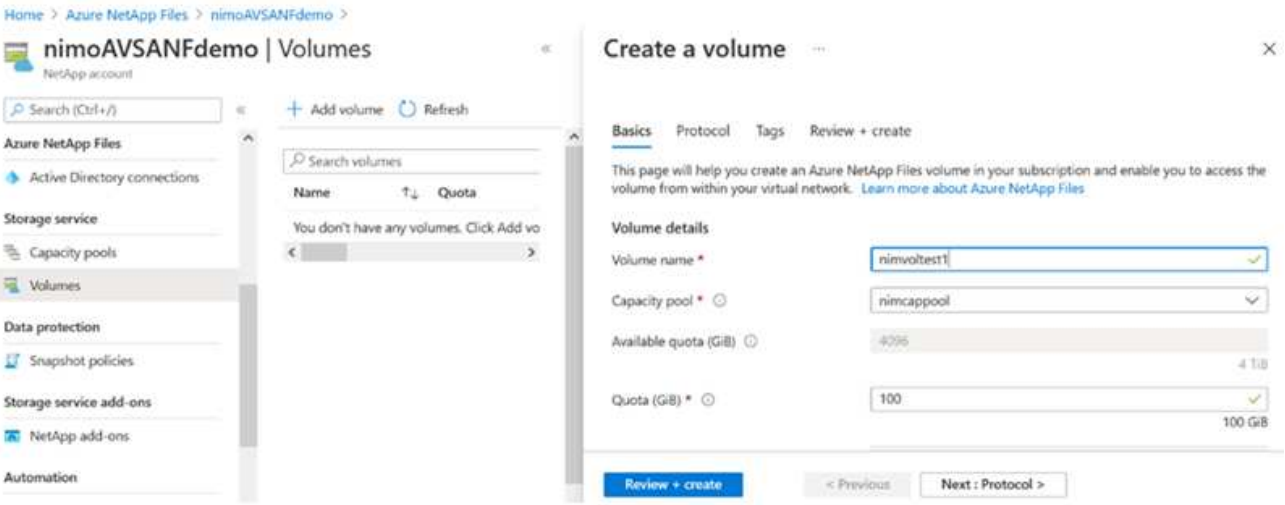


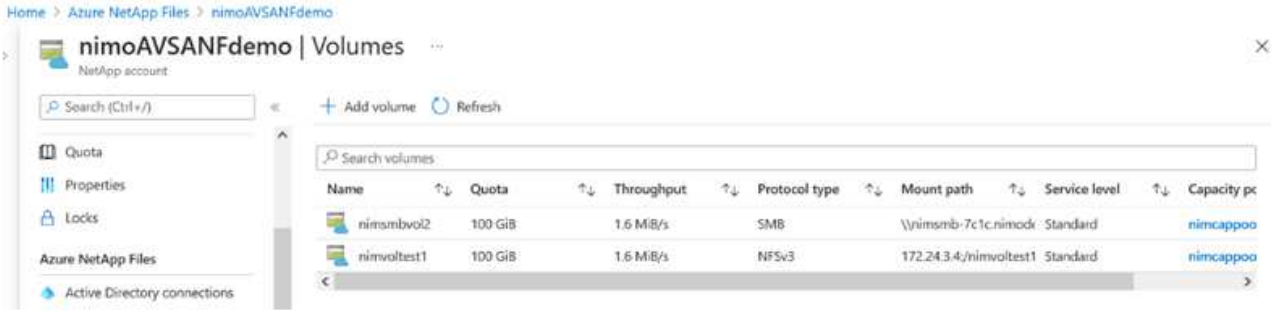
4. 使用「容量池」側邊欄標籤下的「磁碟區」側邊欄標籤新增 SMB 磁碟區。確保在建立 SMB 磁碟區之前配置了 Active Directory 連接器。



5. 按一下「檢視 + 建立」以建立 SMB 磁碟區。

   如果應用程式是 SQL Server，則啟用 SMB 持續可用性。

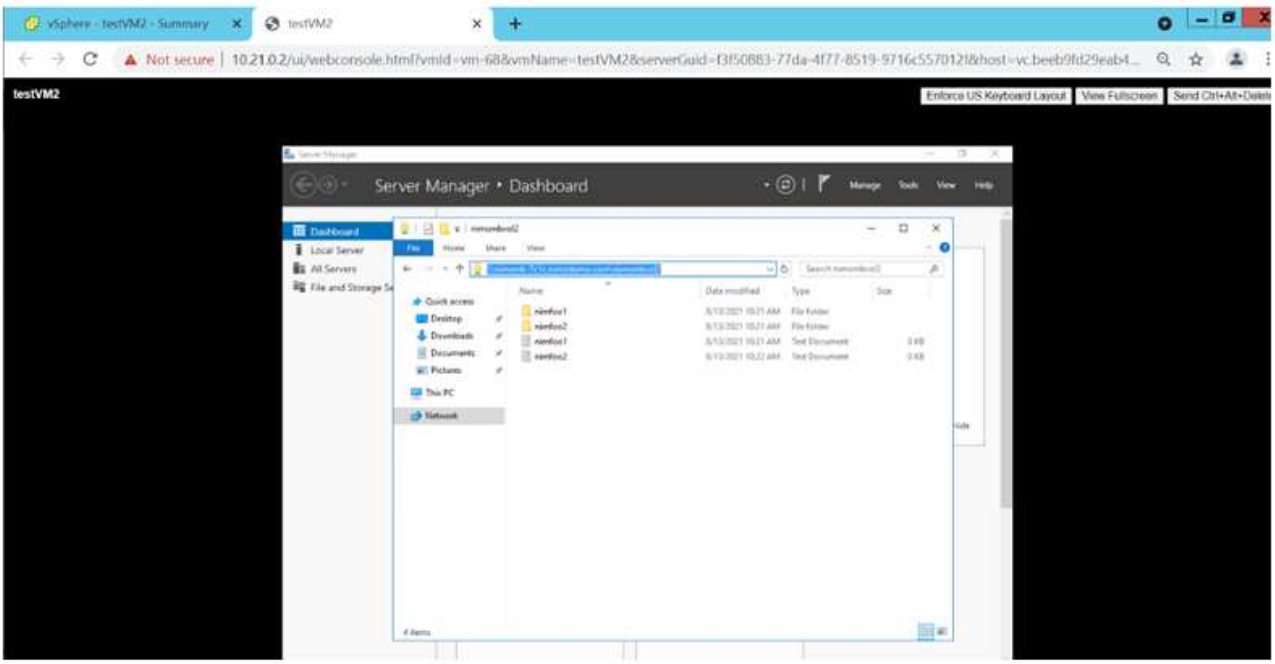


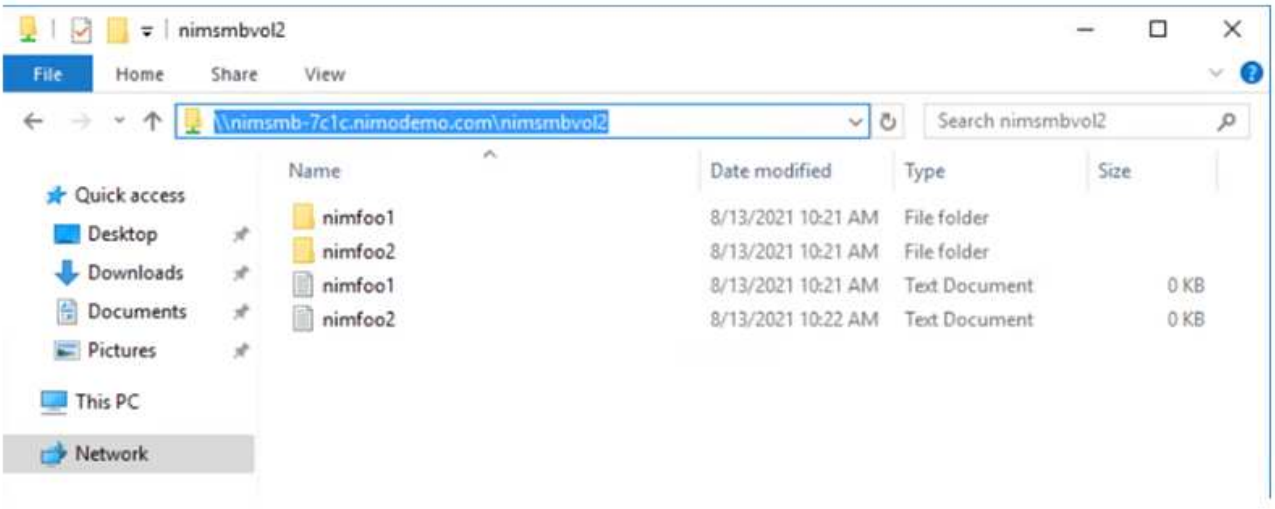


若要詳細了解Azure NetApp Files磁碟區按大小或配額的效能，請參閱"Azure NetApp Files的效能注意事項"。

6. 連接建立後，即可掛載該磁碟區並將其用於應用程式資料。

   為此，請在 Azure 入口網站中按一下「磁碟區」側邊欄選項卡，然後選擇要掛載的磁碟區並存取掛載說明。複製路徑並使用映射網路磁碟機選項將磁碟區載入到在 Azure VMware 解決方案 SDDC 上執行的 VM 上。





7. 若要在 Azure VMware 解決方案 SDDC 上執行的 Linux VM 上裝載 NFS 卷，請使用相同的程序。使用磁碟區重塑或動態服務等級功能來滿足工作負載需求。

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                   1K-blocks     Used Available Use% Mounted on
udev                           8168112        0   8168112   0% /dev
tmpfs                          1639548     1488   1638060   1% /run
/dev/sda5                     50824704  7902752  40310496  17% /
tmpfs                          8197728        0   8197728   0% /dev/shm
tmpfs                             5120        0      5120   0% /run/lock
tmpfs                          8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                       56832    56832         0 100% /snap/core18/2128
/dev/loop2                       66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                      224256   224256         0 100% /snap/gnome-3-34-180
4/72
/dev/loop3                       52224    52224         0 100% /snap/snap-store/547
/dev/loop4                       33152    33152         0 100% /snap/snapd/12704
/dev/sda1                       523248        4    523244   1% /boot/efi
tmpfs                          1639544       52   1639492   1% /run/user/1000
/dev/sr0                         54738    54738         0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

有關更多信息，請參閱"動態變更卷的服務級別" 。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP（或稱 CVO）是基於 NetApp 的ONTAP儲存軟體所建置的業界領先的雲端資料管理解決方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的軟體定義版本，使用雲端原生存儲，允許您在雲端和本地使用相同的存儲軟體，從而無需重新培訓 IT 人員採用全新方法來管理資料。

CVO 使客戶能夠無縫地將資料從邊緣移動到資料中心、雲端並返回，從而將您的混合雲整合在一起 - 所有這些

都透過單一窗格管理控制台NetApp Cloud Manager 進行管理。

CVO 的設計旨在提供極致的效能和先進的資料管理功能，以滿足您在雲端最嚴苛的應用程式

Cloud Volumes ONTAP (CVO) 作為來賓連接存儲

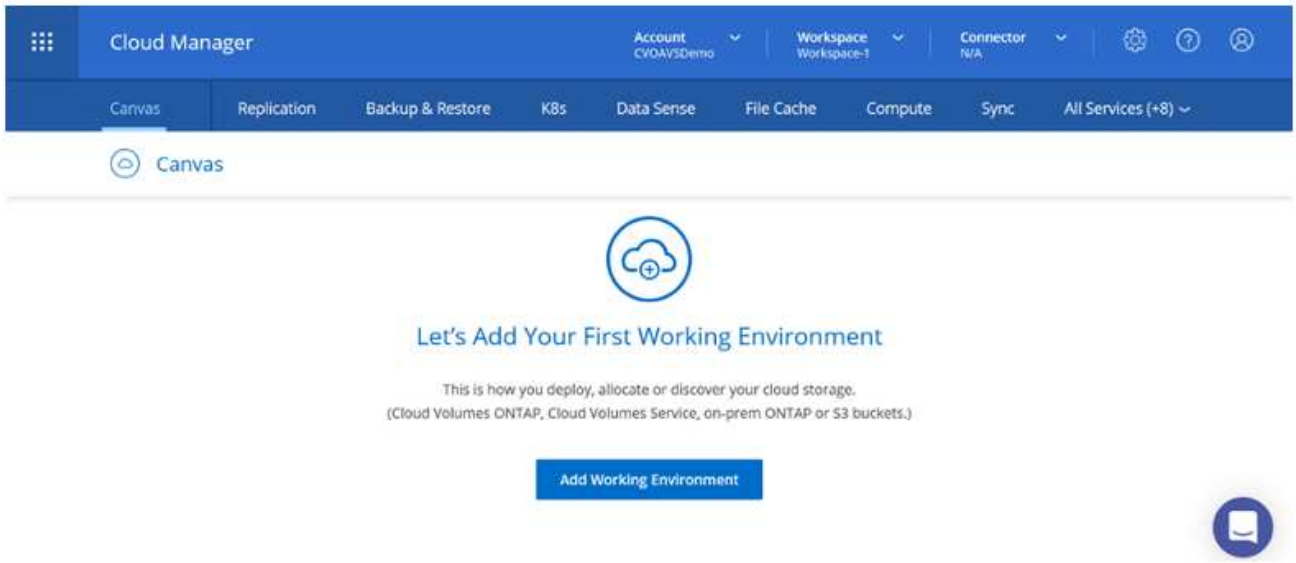
▼ 在 **Azure** 中部署新的**Cloud Volumes ONTAP**

可以從 Azure VMware 解決方案 SDDC 環境中建立的 VM 掛載Cloud Volumes ONTAP共用和 LUN。由於Cloud Volumes ONTAP支援 iSCSI、SMB 和 NFS 協議，因此磁碟區也可以安裝在 Linux 用戶端和 Windows 用戶端上。只需幾個簡單的步驟即可設定Cloud Volumes ONTAP磁碟區。

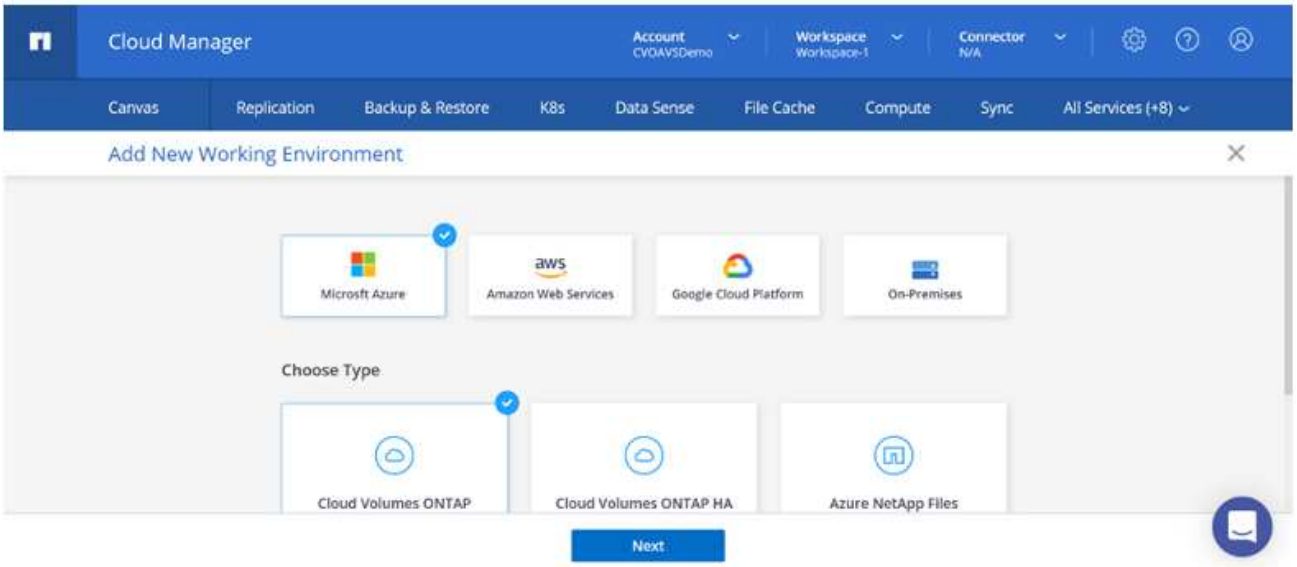
若要將磁碟區從本機環境複製到雲端以用於災難復原或遷移目的，請使用站台對站台 VPN 或 ExpressRoute 建立與 Azure 的網路連線。將資料從本地複製到Cloud Volumes ONTAP超出了本文檔的範圍。若要在本機和Cloud Volumes ONTAP系統之間複製數據，請參閱"設定係統之間的資料複製"。

使用 "Cloud Volumes ONTAP大小調整器" 來精確調整 Cloud Volumes ONTAP 執行個體的大小。同時監控內部部署效能，以作為 Cloud Volumes ONTAP 大小調整工具的輸入。

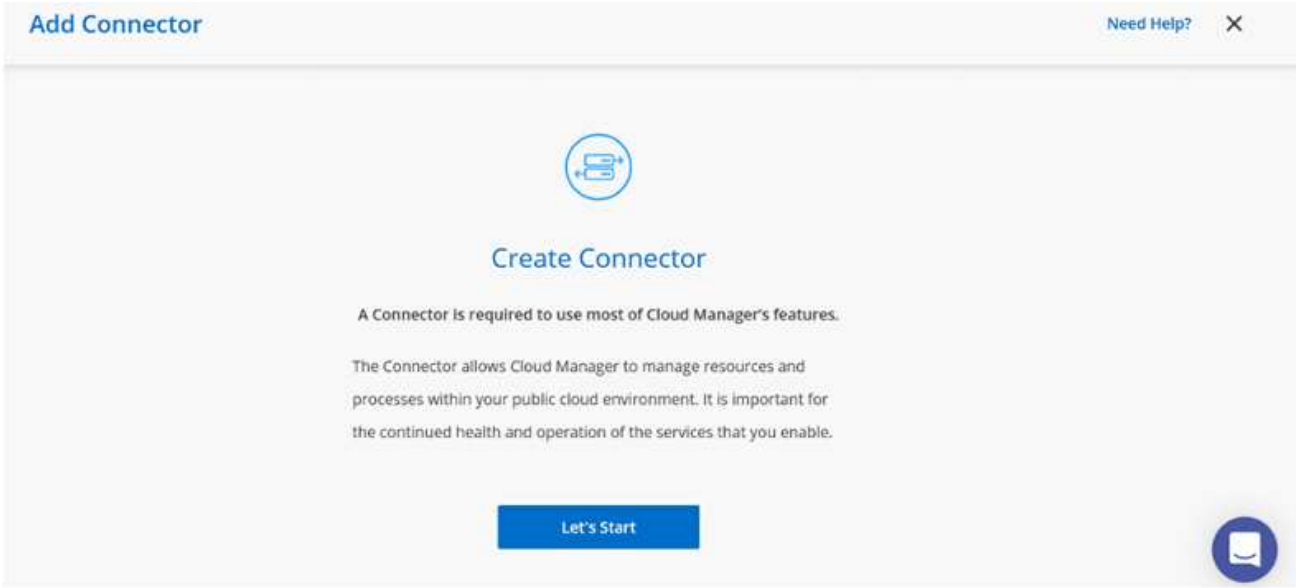
1. 登入NetApp Cloud Central — 顯示 Fabric View 畫面。找到Cloud Volumes ONTAP標籤並選擇前往雲端管理員。登入後，將顯示 Canvas 畫面。



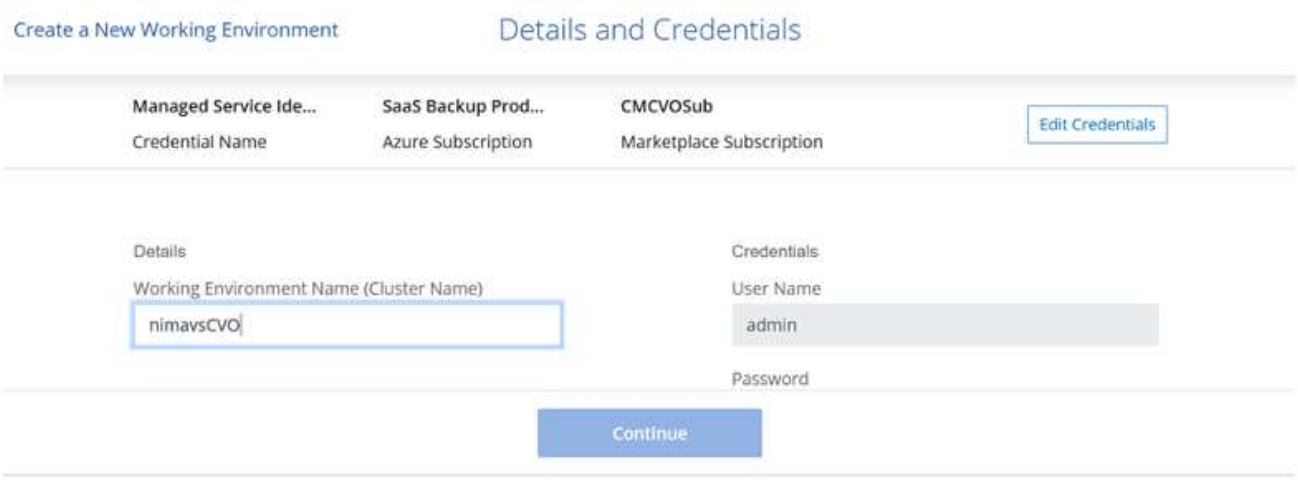
2. 在雲端管理器首頁上，按一下新增工作環境，然後選擇 Microsoft Azure 作為雲端和系統設定類型。



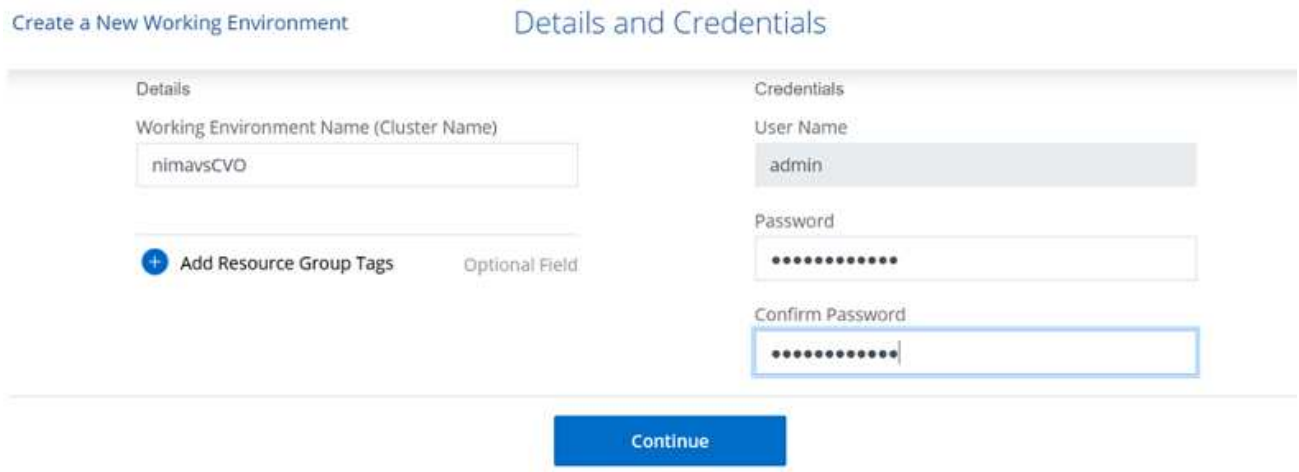
3. 建立第一個Cloud Volumes ONTAP工作環境時，Cloud Manager 會提示您部署連接器。



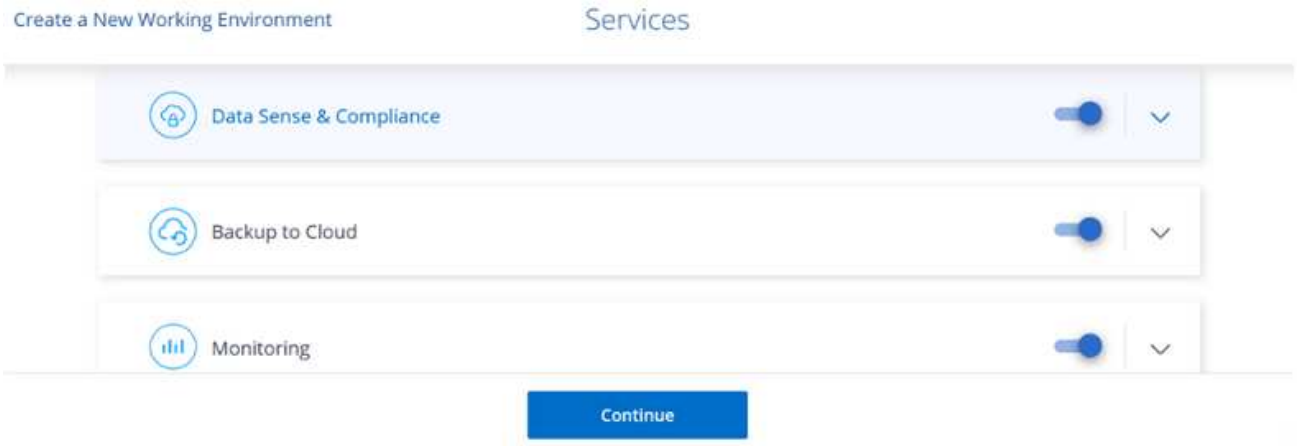
4. 建立連接器後，更新詳細資訊和憑證欄位。



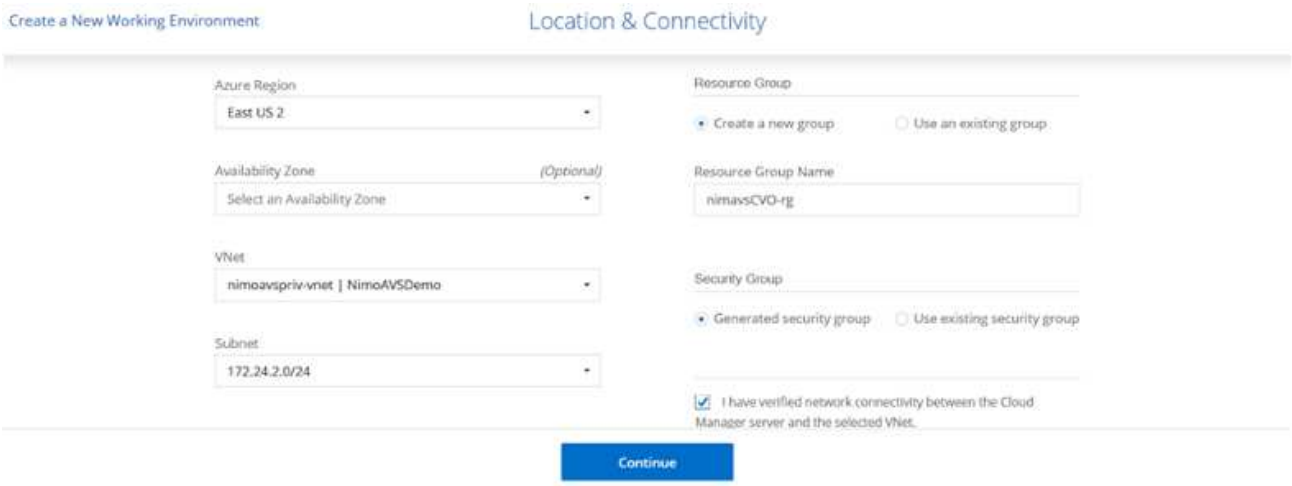
5. 提供要建立的環境的詳細信息，包括環境名稱和管理員憑證。新增 Azure 環境的資源組標籤作為可選參數。完成後，按一下“繼續”。



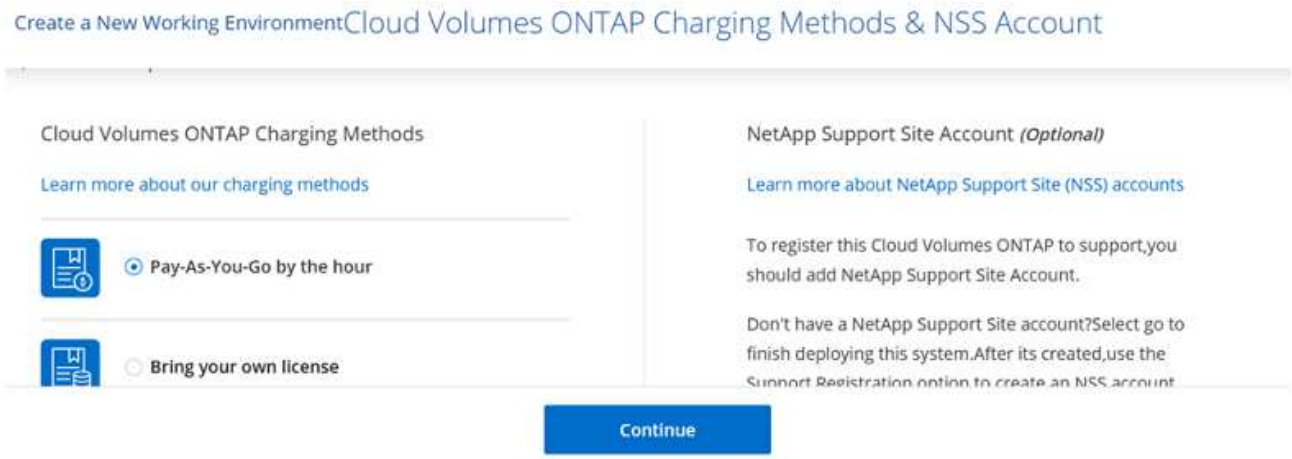
6. 選擇 Cloud Volumes ONTAP 部署的附加服務，包括 NetApp Data Classification、NetApp Backup and Recovery，以及 Data Infrastructure Insights。選擇服務，然後按一下「繼續」。



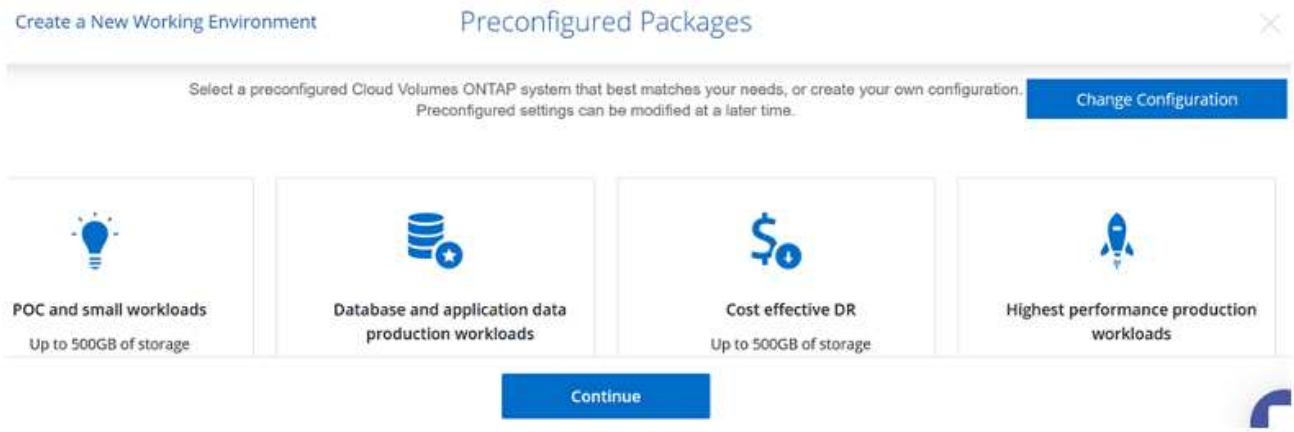
7. 配置 Azure 位置和連線。選擇要使用的 Azure 區域、資源群組、VNet 和子網路。



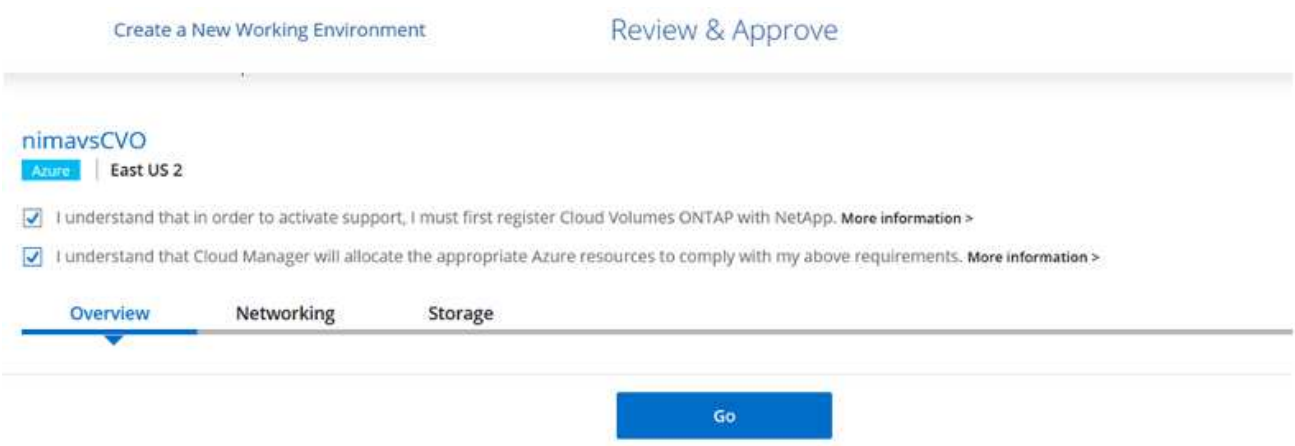
8. 選擇授權選項：按使用量付費或使用現有授權的 BYOL。在此範例中，使用了按使用量付費選項。



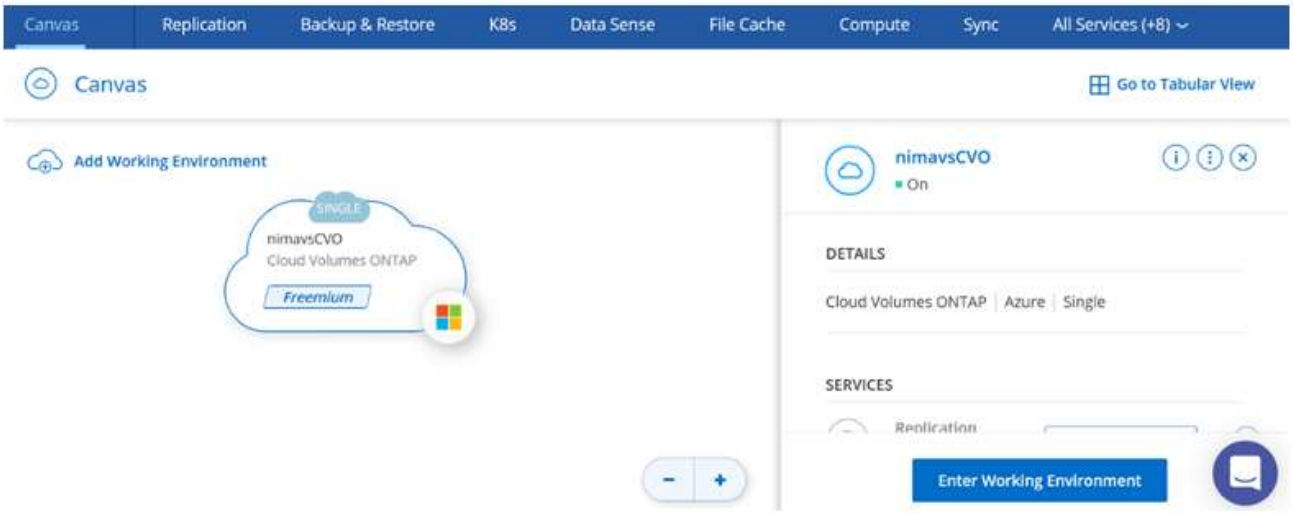
9. 在適用於各種類型工作負載的幾個預先配置套件中進行選擇。



10. 接受兩個關於啟動支援和分配 Azure 資源的協定。若要建立Cloud Volumes ONTAP實例，請按一下「Go」。

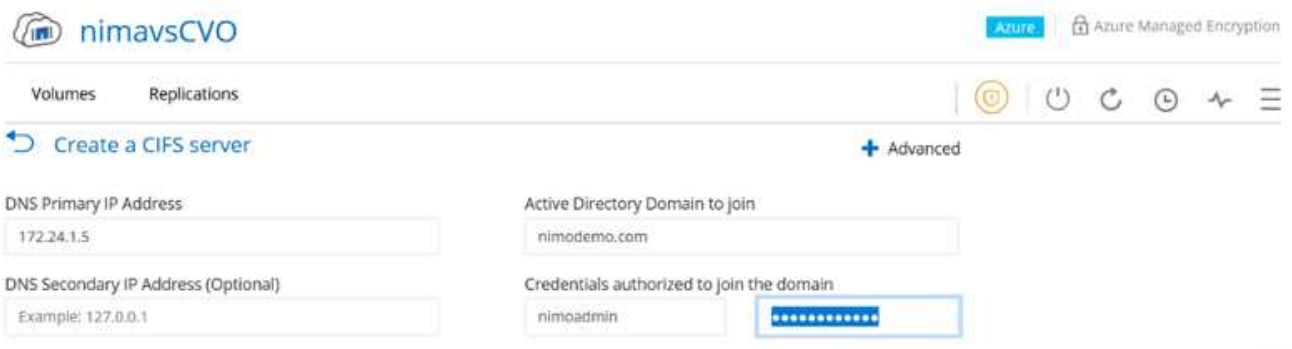


11. 配置Cloud Volumes ONTAP後，它會列在 Canvas 頁面上的工作環境中。

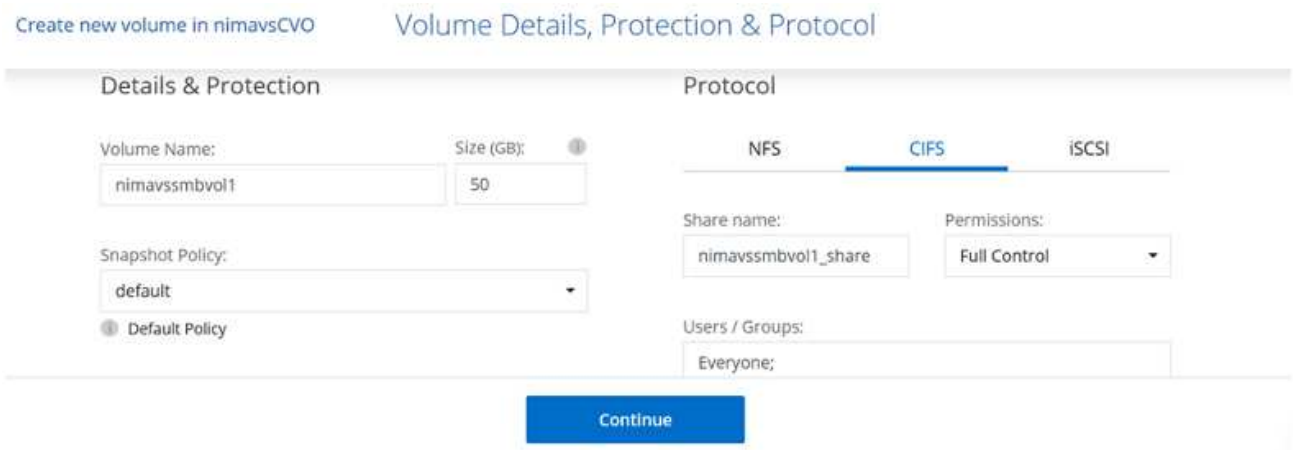


▼ **SMB** 磁碟區的附加配置

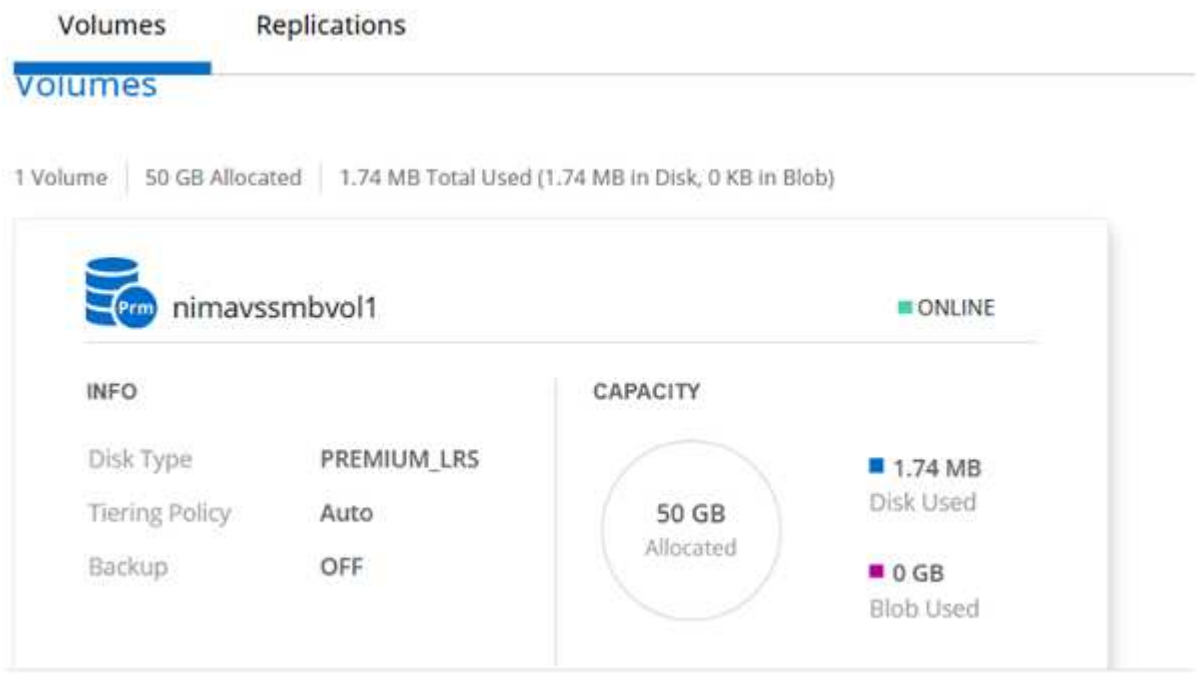
1. 工作環境準備好後，請確保 CIFS 伺服器配置了適當的 DNS 和 Active Directory 設定參數。在建立 SMB 磁碟區之前，需要執行此步驟。



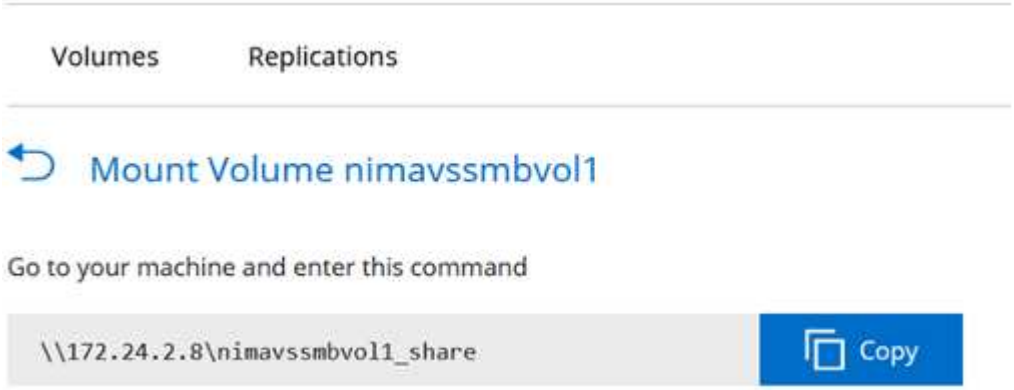
2. 建立 SMB 磁碟區是一個簡單的過程。選擇要建立磁碟區的 CVO 實例，然後按一下「建立磁碟區」選項。選擇適當的大小，雲端管理器選擇包含的聚合或使用進階分配機制放置在特定的聚合上。對於此演示，選擇 SMB 作為協定。

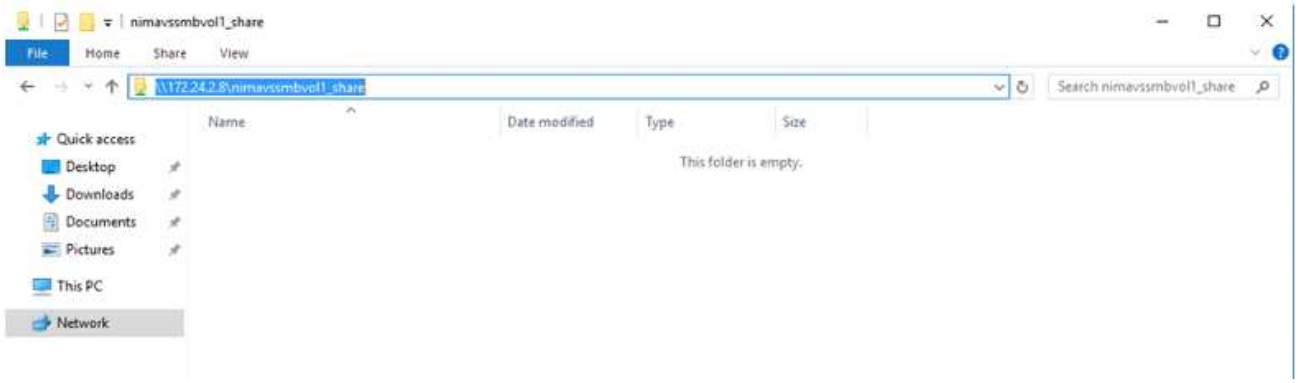


3. 磁碟區配置完成後，它將在「磁碟區」窗格下可用。由於已配置 CIFS 共享，請授予您的使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。如果從本機環境複製卷，則不需要此步驟，因為檔案和資料夾權限都將作為SnapMirror複製的一部分保留。



4. 建立磁碟區後，使用 mount 指令從 Azure VMware 解決方案 SDDC 主機上執行的 VM 連線到共用。
5. 複製以下路徑並使用映射網路磁碟機選項將磁碟區載入到在 Azure VMware 解決方案 SDDC 上執行的 VM 上。

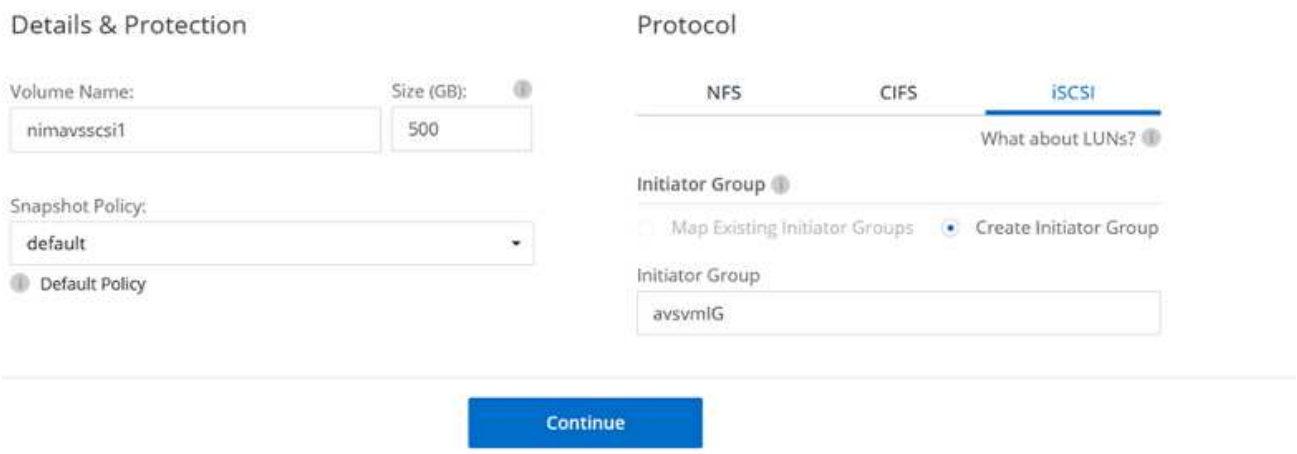




▼ 將 **LUN** 連接到主機

若要將 LUN 連接到主機，請完成下列步驟：

1. 在「畫布」頁面上，雙擊Cloud Volumes ONTAP工作環境以建立和管理磁碟區。
2. 按一下新增磁碟區 > 新磁碟區並選擇 iSCSI，然後按一下建立啟動器群組。按一下「Continue（繼續）」。



3. 配置磁碟區後，選擇該磁碟區，然後按一下目標 IQN。若要複製 iSCSI 限定名稱 (IQN)，請按一下複製。建立從主機到 LUN 的 iSCSI 連線。

   若要對駐留在 Azure VMware 解決方案 SDDC 上的主機完成相同操作，請執行下列操作：

   a. 透過 RDP 連接 Azure VMware 解決方案 SDDC 上託管的 VM。

b. 開啟 iSCSI 發起程式屬性對話方塊：伺服器管理員 > 儀表板 > 工具 > iSCSI 發起程式。

c. 在“發現”標籤中，按一下“發現入口網站”或“新增入口網站”，然後輸入 iSCSI 目標連接埠的 IP 位址。

d. 從「目標」標籤中，選擇發現的目標，然後按一下「登入」或「連線」。

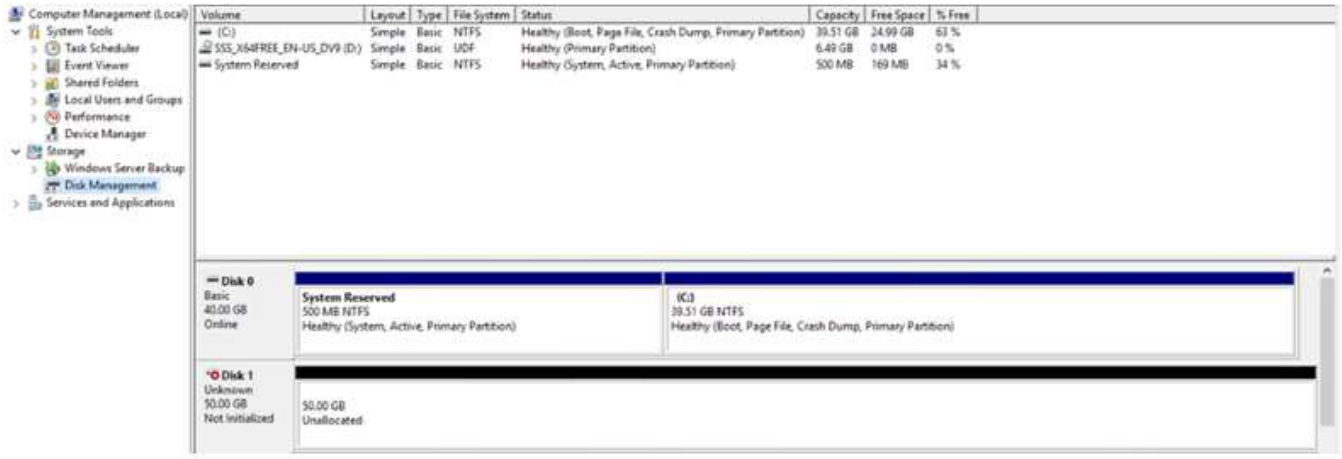
e. 選擇啟用多路徑，然後選擇電腦啟動時自動恢復此連線或將此連線新增至收藏目標清單。按一下“進階”。

*注意：*Windows 主機必須與叢集中的每個節點建立 iSCSI 連線。本機 DSM 選擇要使用的最佳路徑。



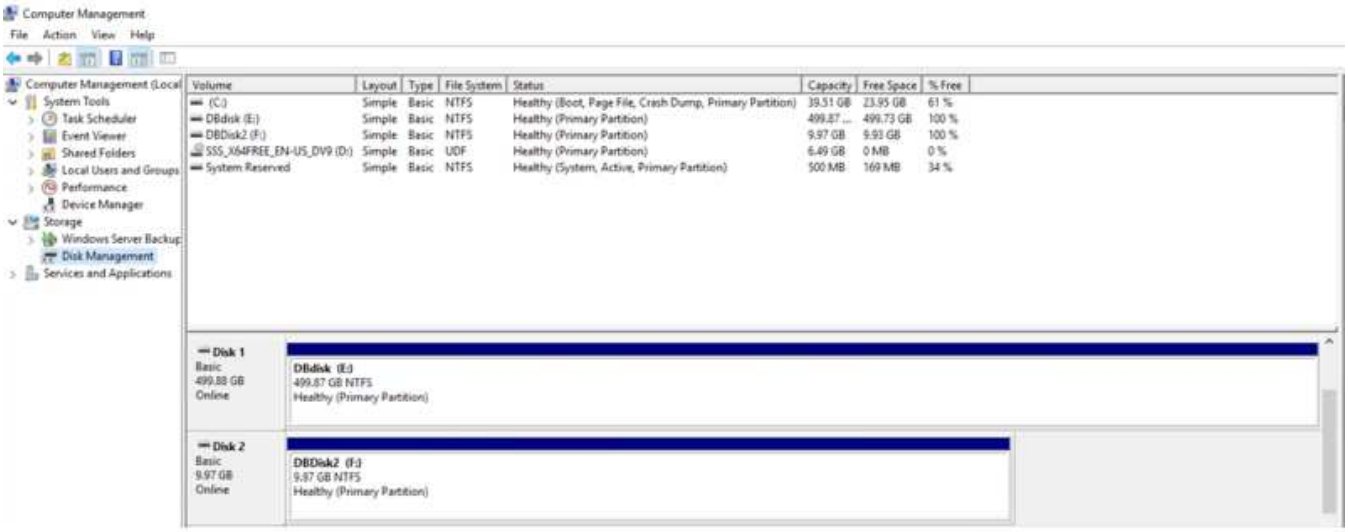
儲存虛擬機器 (SVM) 上的 LUN 對於 Windows 主機來說顯示為磁碟。主機不會自動發現任何新新增的磁碟。透過完成以下步驟觸發手動重新掃描以發現磁碟：

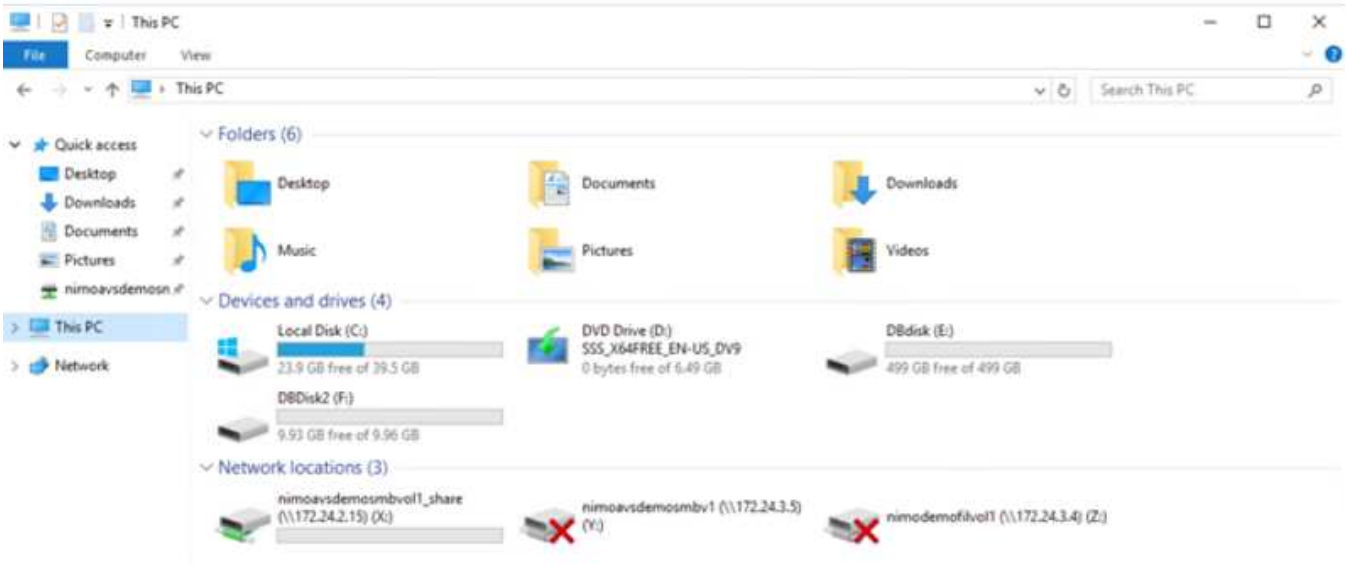
1. 開啟 Windows 電腦管理公用程式：開始 > 管理工具 > 電腦管理。
2. 在導航樹中展開儲存節點。
3. 按一下“磁碟管理”。
4. 按一下操作 > 重新掃描磁碟。



當 Windows 主機首次存取新的 LUN 時，它沒有分割區或檔案系統。初始化 LUN；並且（可選）透過完成以下步驟使用檔案系統格式化 LUN：

1. 啟動 Windows 磁碟管理。
2. 右鍵單擊 LUN，然後選擇所需的磁碟或分割區類型。
3. 請按照精靈中的說明進行操作。在此範例中，已安裝磁碟機 E:





Google Cloud VMware Engine：使用**NetApp**儲存的選項

NetApp儲存可以作為來賓連接儲存或補充儲存附加到 Google Cloud Virtualization Engine。

Google Cloud NetApp Volumes （NetApp Volumes）作為補充 NFS 資料儲存區

需要在 Google Cloud VMware Engine (GCVE) 環境中增加儲存容量的客戶可以利用Google Cloud NetApp Volumes作為補充 NFS 資料儲存進行掛載。將資料儲存在Google Cloud NetApp Volumes上允許客戶在區域之間進行複製以防止災難。

欲了解更多信息，請訪問"Google Cloud NetApp Volumes （NetApp Volumes）作為補充 NFS 資料儲存區"

NetApp CVO 作為客戶連接存儲

Cloud Volumes ONTAP（或稱 CVO）是基於 NetApp 的ONTAP儲存軟體所建置的業界領先的雲端資料管理解決方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的軟體定義版本，使用雲端原生存儲，允許您在雲端和本地使用相同的存儲軟體，從而無需重新培訓 IT 人員採用全新方法來管理資料。

CVO 使客戶能夠無縫地將資料從邊緣移動到資料中心、雲端並返回，從而將您的混合雲整合在一起 - 所有這些都透過單一窗格管理控制台NetApp Cloud Manager 進行管理。

透過設計，CVO 可提供極高的效能和先進的資料管理功能，以滿足您在雲端中最嚴苛的應用程式的需求。

欲了解更多信息，請訪問"NetApp CVO 作為客戶連接存儲"

Google Cloud NetApp Volumes （NetApp Volumes）作為來賓連接存儲

可從在 VMware Engine 環境中建立的虛擬機器掛載Google Cloud NetApp Volumes共用。由於Google Cloud NetApp Volumes支援 SMB 和 NFS 協議，因此這些磁碟區也可以安裝在 Linux 用戶端上並對應到 Windows 用戶端上。可以透過簡單的步驟來設定Google Cloud NetApp Volumes磁碟區。

Google Cloud NetApp Volumes和 Google Cloud VMware Engine 私有雲必須位於同一區域。

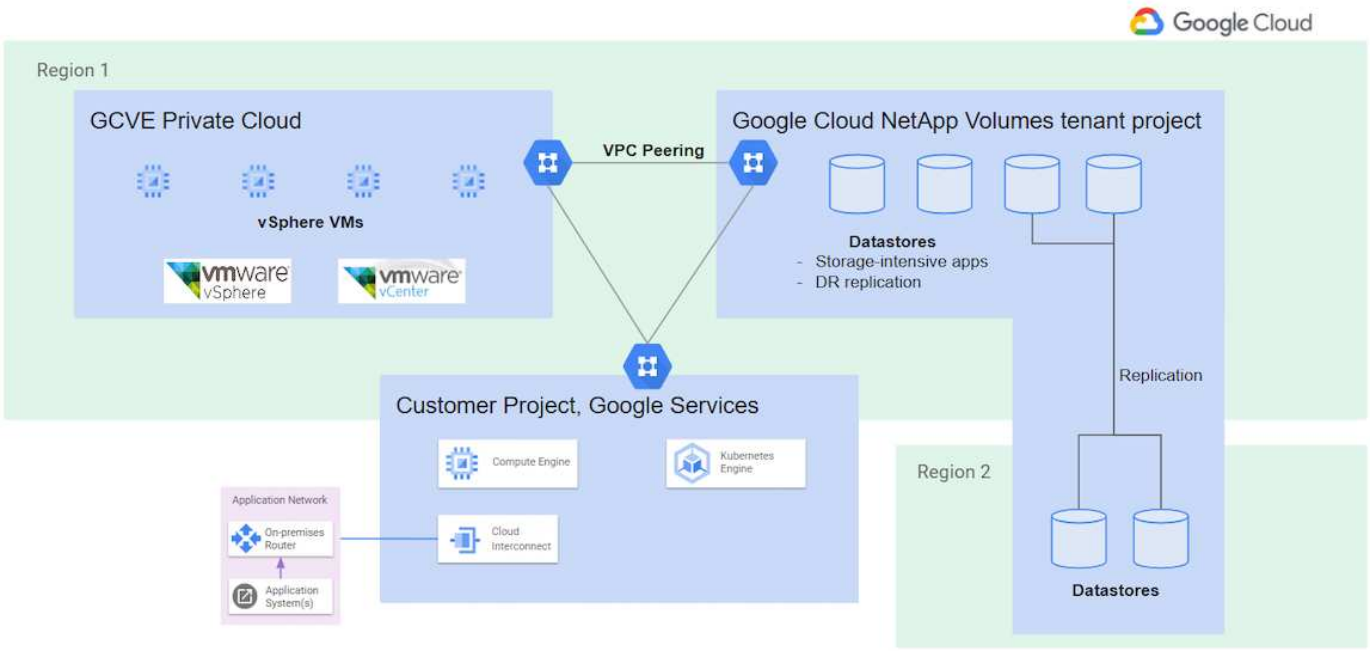
欲了解更多信息，請訪問"Google Cloud NetApp Volumes （NetApp Volumes）作為來賓連接存儲"

Google Cloud VMware Engine 補充 NFS 資料儲存與Google Cloud NetApp Volumes

客戶可以使用 NFS 補充資料儲存和Google Cloud NetApp Volumes擴充 Google Cloud VMware Engine 上的儲存容量。

概況

需要在 Google Cloud VMware Engine (GCVE) 環境上增加儲存容量的客戶可以利用 Netapp Cloud Volume Service 作為補充 NFS 資料儲存進行安裝。將資料儲存在Google Cloud NetApp Volumes上允許客戶在區域之間進行複製以防止災難。



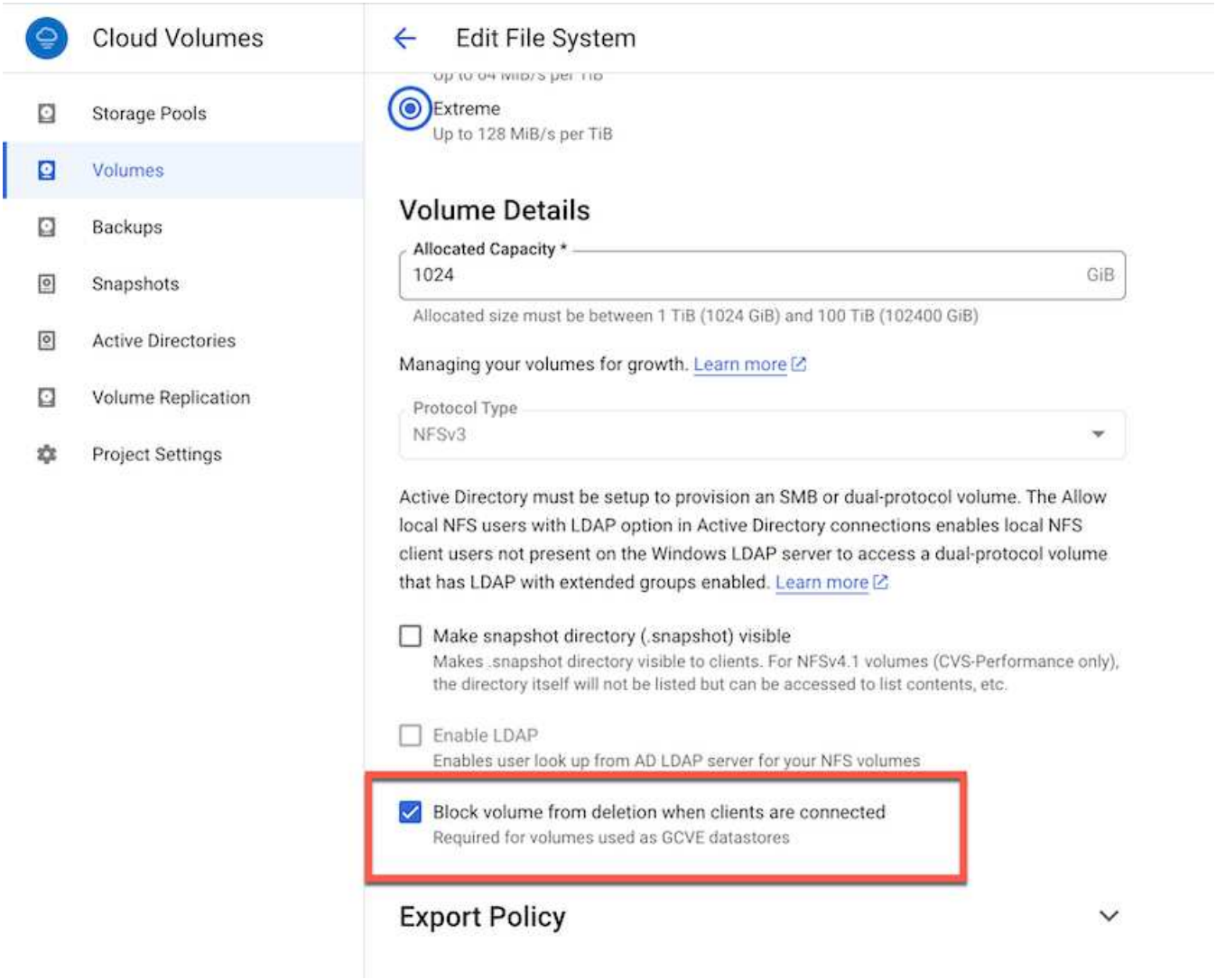
在 **GCVE** 上從**Google Cloud NetApp Volumes (NetApp Volumes)** 掛載 **NFS** 資料儲存區的部署步驟

▼ 配置**NetApp**卷 **-** 性能卷

Google Cloud NetApp Volumes Volume 可以透過 "使用 Google Cloud Console" "使用 Google Cloud CLI 或 API" 進行配置

▼ 將**NetApp Volumes** 磁碟區標記為不可刪除

為避免虛擬機器在執行時意外刪除 Volume，請確保將 Volume 標記為不可刪除，如下快照所示。



如需詳細資訊，請參閱 "建立 NFS 卷" 文件。

▼ 確保**NetApp Volumes Tenant VPC** 的 **GCVE** 上有專用連線。

要掛載 NFS 資料儲存區，GCVE 和NetApp Volumes 專案之間應該會有私有連線。欲了解更多信息，請參閱"如何設定私人服務訪問"

▼ 掛載 **NFS** 資料存儲

有關如何在 GCVE 上掛載 NFS 資料儲存的說明，請參閱"如何使用NetApp磁碟區建立 NFS 資料存儲"

由於 vSphere 主機由 Google 管理，因此您無權安裝 NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB)。如果您需要虛擬磁碟區 (vVol) 支持，請告知我們。如果您想使用巨型幀，請參閱"GCP 上支援的最大 MTU 大小"

使用**Google Cloud NetApp Volumes**節省成本

若要了解使用 Google Cloud NetApp Volumes 滿足您在 GCVE 上的儲存設備需求所帶來的潛力節省，請查看 "NetApp投資報酬率計算器"

參考連結

- "Google 部落格 - 如何使用NetApp Volumes 作為 Google Cloud VMware Engine 的資料儲存區"

- "NetApp部落格 - 將儲存豐富的應用程式遷移到 Google Cloud 的更好方法"

適用於 **GCP** 的**NetApp**儲存選項

GCP 支援透過Cloud Volumes ONTAP (CVO) 或Google Cloud NetApp Volumes (NetApp Volumes) 連接來賓的NetApp儲存。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP（或稱 CVO）是基於 NetApp 的ONTAP儲存軟體所建置的業界領先的雲端資料管理解決方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的軟體定義版本，使用雲端原生存儲，允許您在雲端和本地使用相同的存儲軟體，從而無需重新培訓 IT 人員採用全新方法來管理資料。

CVO 使客戶能夠無縫地將資料從邊緣移動到資料中心、雲端並返回，從而將您的混合雲整合在一起 - 所有這些都透過單一窗格管理控制台NetApp Cloud Manager 進行管理。

CVO 的設計旨在提供極致的效能和先進的資料管理功能，以滿足您在雲端最嚴苛的應用程式

Cloud Volumes ONTAP (CVO) 作為來賓連接存儲

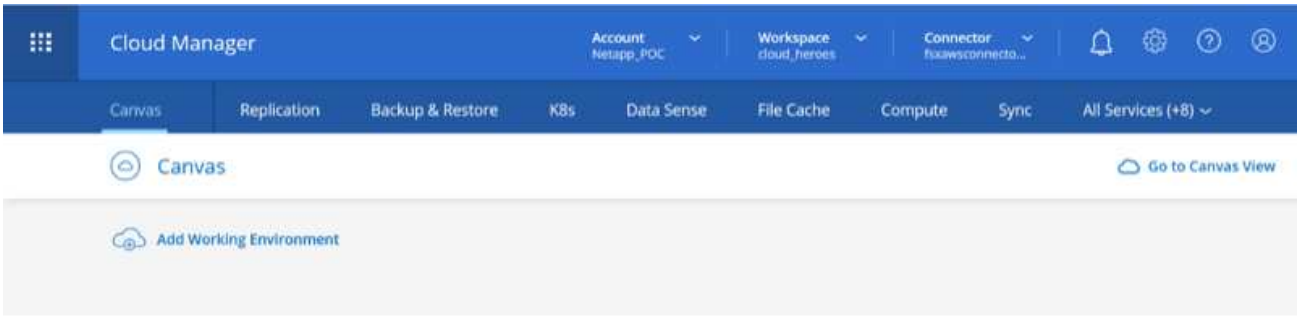
▼ 在 **Google Cloud** 中部署**Cloud Volumes ONTAP** （自行部署）

可從在 GCVE 私有雲環境中建立的虛擬機器掛載Cloud Volumes ONTAP共用和 LUN。這些磁碟區還可以安裝在 Linux 用戶端和 Windows 用戶端上，並且當透過 iSCSI 安裝時，可以在 Linux 或 Windows 用戶端上將 LUNS 作為區塊裝置進行訪問，因為Cloud Volumes ONTAP支援 iSCSI、SMB 和 NFS 協定。只需幾個簡單的步驟即可設定Cloud Volumes ONTAP磁碟區。

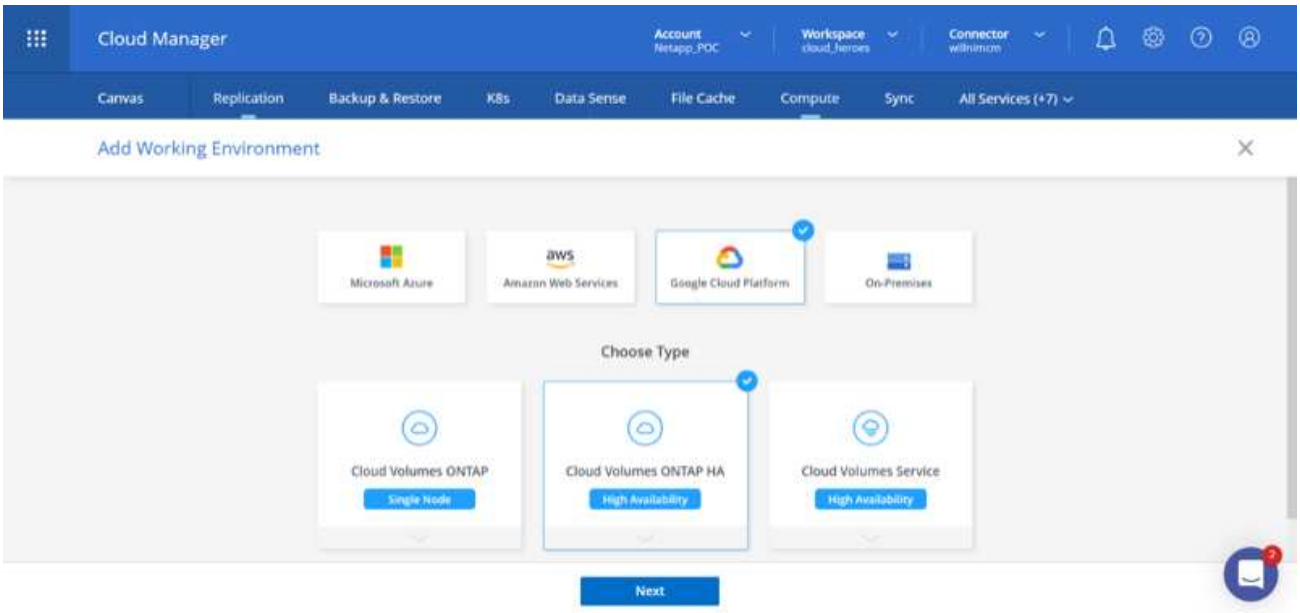
若要將磁碟區從本機環境複製到雲端以用於災難復原或遷移，請使用網站到網站 VPN 或 Cloud Interconnect 建立與 Google Cloud 的網路連線。將資料從本地複製到Cloud Volumes ONTAP超出了本文檔的範圍。若要在本機和Cloud Volumes ONTAP系統之間複製數據，請參閱"設定係統之間的資料複製"。

使用 "Cloud Volumes ONTAP大小調整器" 來精確調整 Cloud Volumes ONTAP 執行個體的大小。同時監控內部部署效能，以作為 Cloud Volumes ONTAP 大小調整工具的輸入。

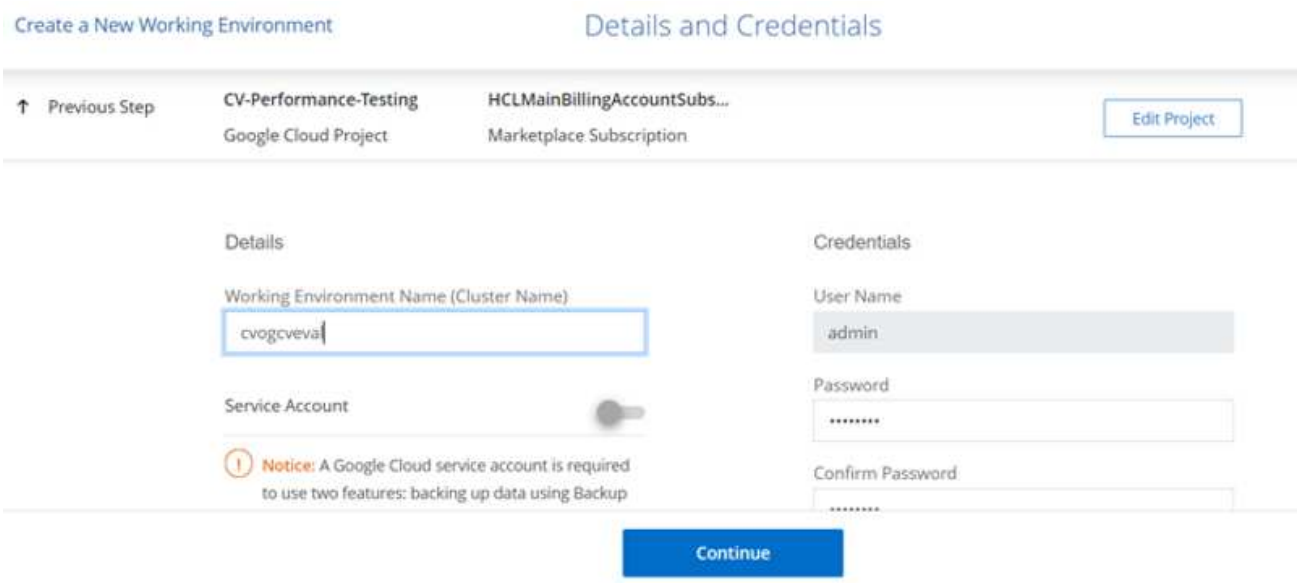
1. 登入NetApp Cloud Central — 顯示 Fabric View 畫面。找到Cloud Volumes ONTAP標籤並選擇前往雲端管理員。登入後，將顯示 Canvas 畫面。



2. 在 Cloud Manager Canvas 標籤上，按一下新增工作環境，然後選擇 Google Cloud Platform 作為雲端和系統配置類型。然後按一下“下一步”。

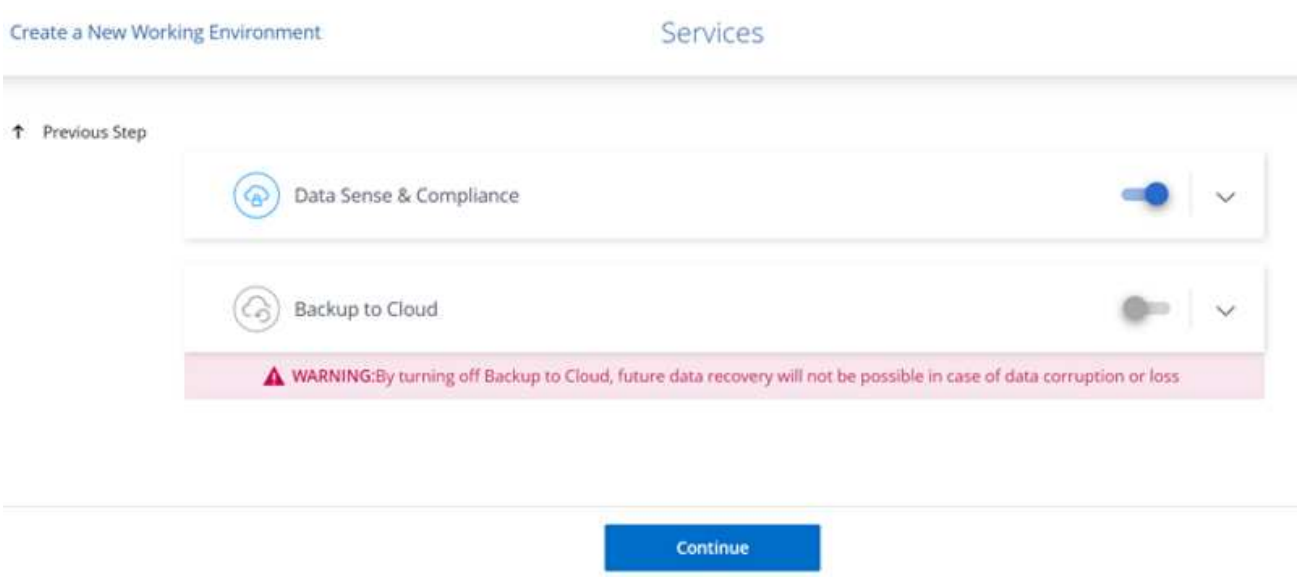


3. 提供要建立的環境的詳細信息，包括環境名稱和管理員憑證。完成後，按一下“繼續”。

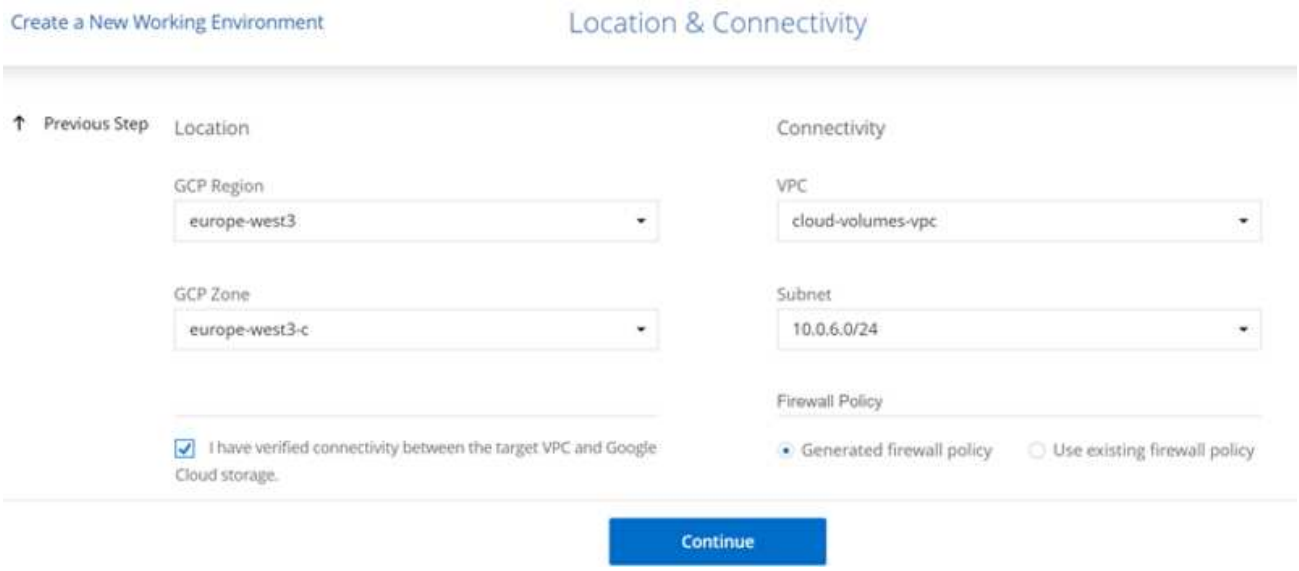


4. 選擇或取消選擇Cloud Volumes ONTAP部署的附加服務，包括資料感知與合規性或備份到雲端。然後，點擊“繼續”。

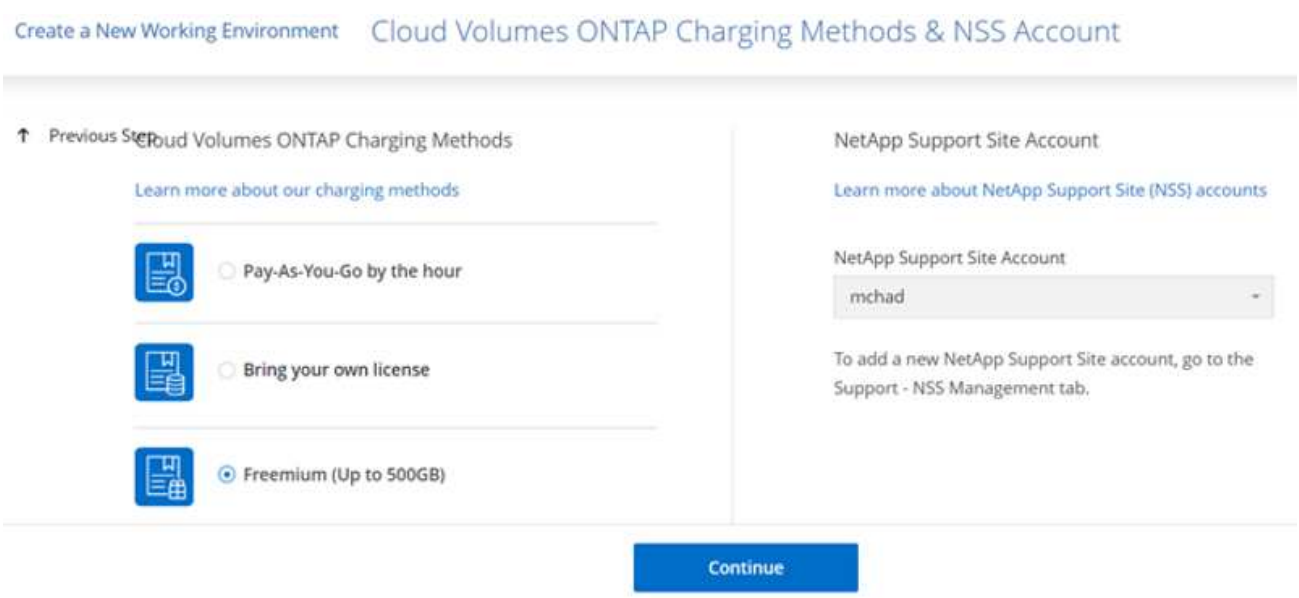
提示：停用附加服務時將顯示驗證彈出訊息。 CVO 部署後可以新增/刪除附加服務，如果從一開始就不需要，請考慮取消選擇它們以避免成本。



5. 選擇一個位置，選擇防火牆策略，然後選取核取方塊以確認與 Google Cloud 儲存的網路連線。

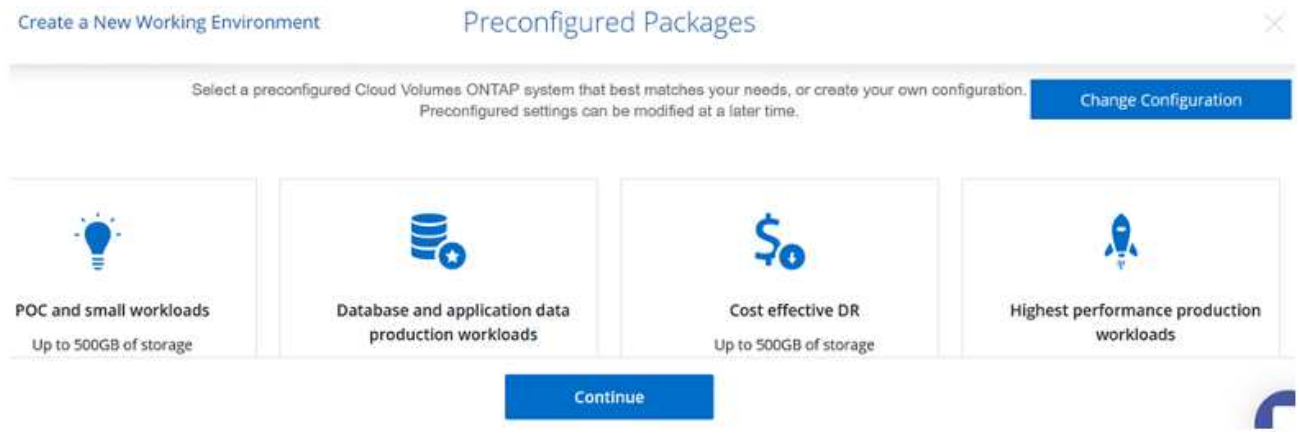


6. 選擇授權選項：按使用量付費或使用現有授權的 BYOL。在此範例中，使用了免費增值選項。然後，點擊繼續。

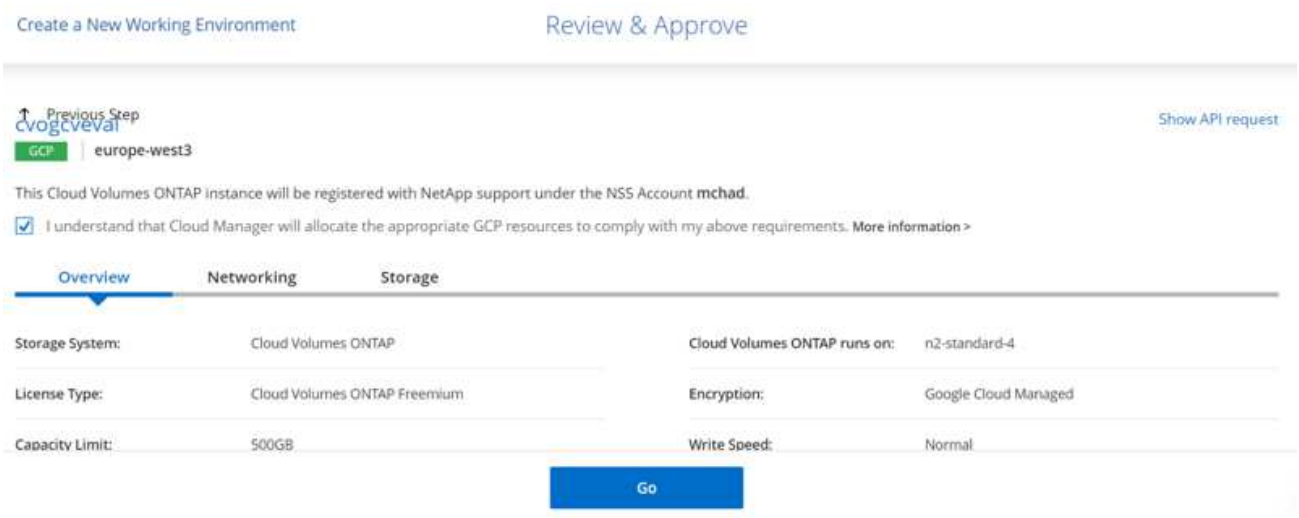


7. 根據將在 AWS SDDC 上的 VMware 雲端上執行的虛擬機器上部署的工作負載類型，在幾個可用的預先配置套件中進行選擇。

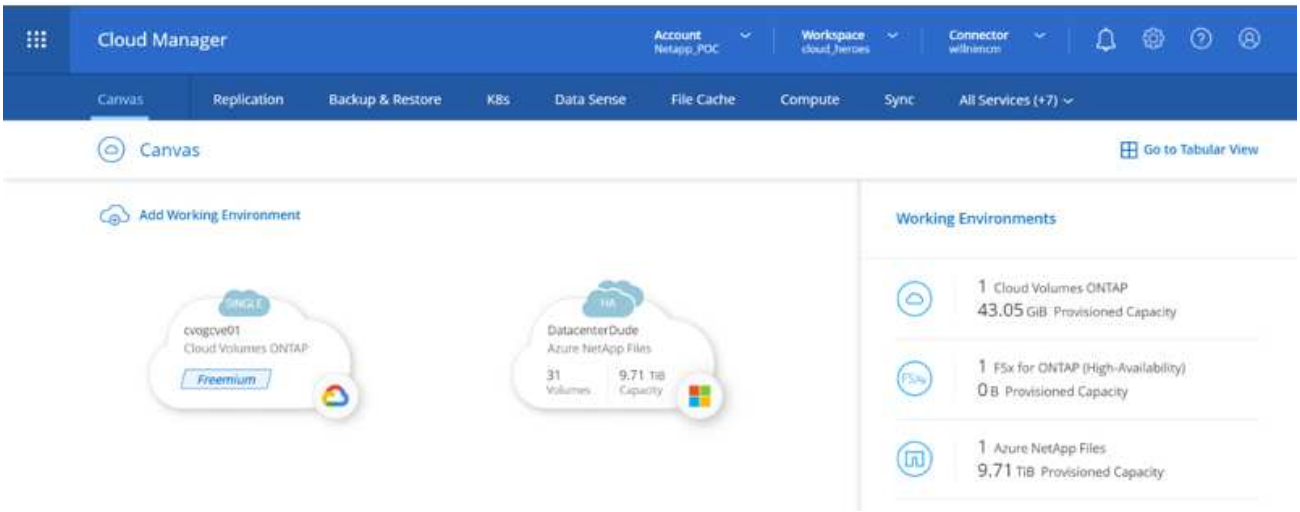
   提示：將滑鼠懸停在圖塊上以查看詳細信息，或按一下「更改配置」自訂 CVO 組件和ONTAP版本。



8. 在「審核並批准」頁面上，審核並確認選擇。若要建立Cloud Volumes ONTAP實例，請按一下「開始」。



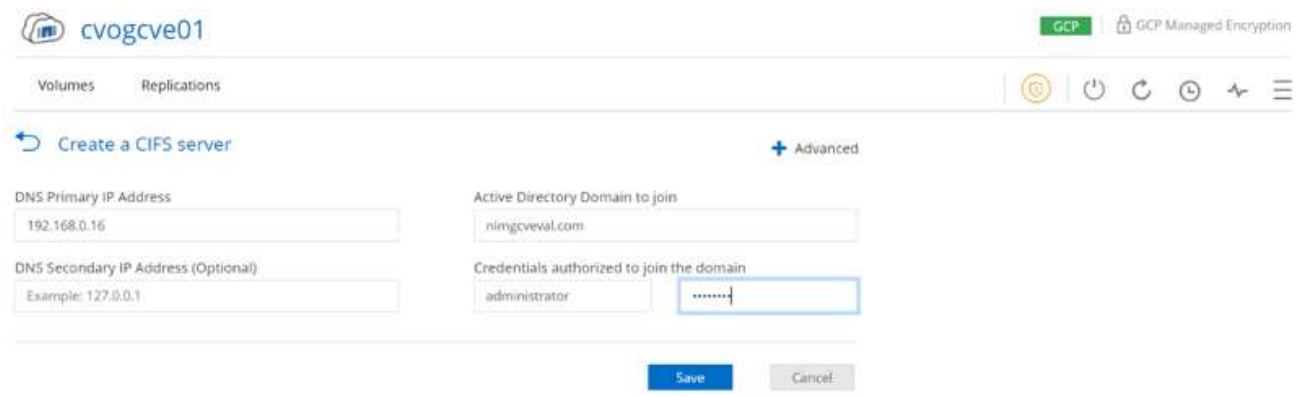
9. 配置Cloud Volumes ONTAP後，它會列在 Canvas 頁面上的工作環境中。



▼ **SMB** 磁碟區的附加配置

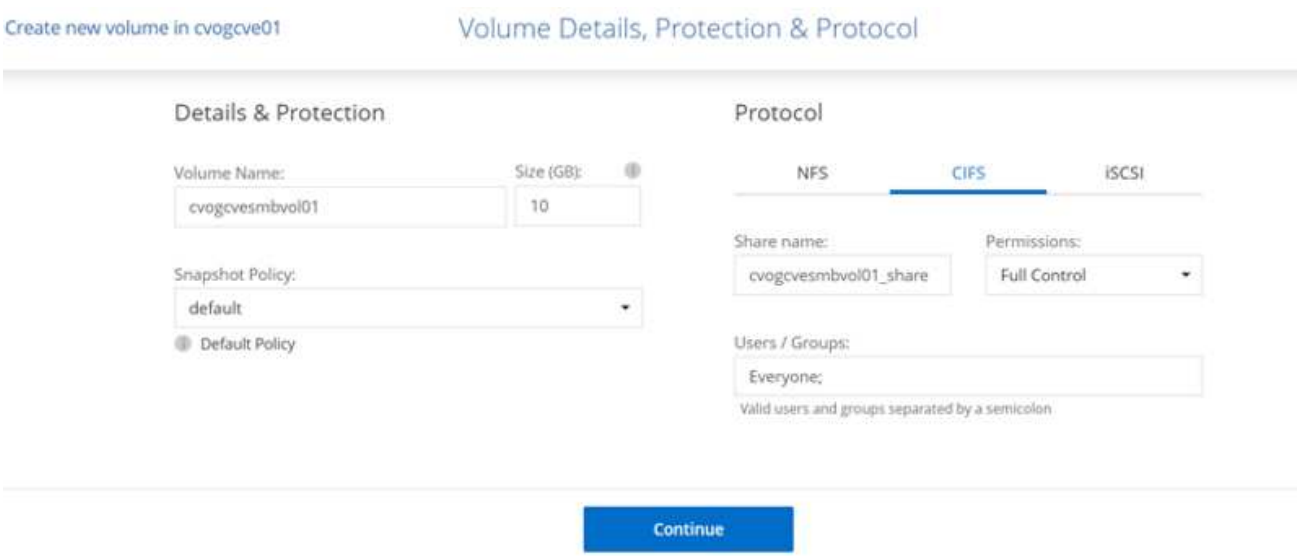
1. 工作環境準備好後，請確保 CIFS 伺服器配置了適當的 DNS 和 Active Directory 設定參數。在建立 SMB 磁碟區之前，需要執行此步驟。

   提示：按一下選單圖示 (º)，選擇進階以顯示更多選項並選擇 CIFS 設定。



2. 建立 SMB 磁碟區是一個簡單的過程。在 Canvas 中，雙擊Cloud Volumes ONTAP工作環境來建立和管理

卷，然後按一下建立卷選項。選擇適當的大小，雲端管理器選擇包含的聚合或使用進階分配機制放置在特定的聚合上。對於此演示，選擇 CIFS/SMB 作為協定。



3. 磁碟區配置完成後，它將在「磁碟區」窗格下可用。由於已配置 CIFS 共享，請授予您的使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。如果從本機環境複製卷，則不需要此步驟，因為檔案和資料夾權限都將作為SnapMirror複製的一部分保留。

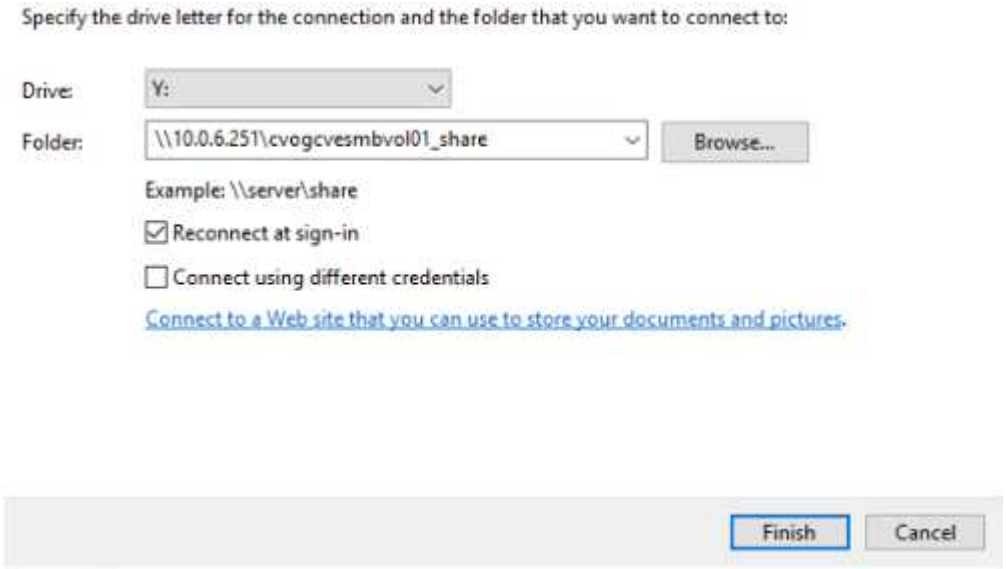
   提示：按一下音量選單 (º) 以顯示其選項。



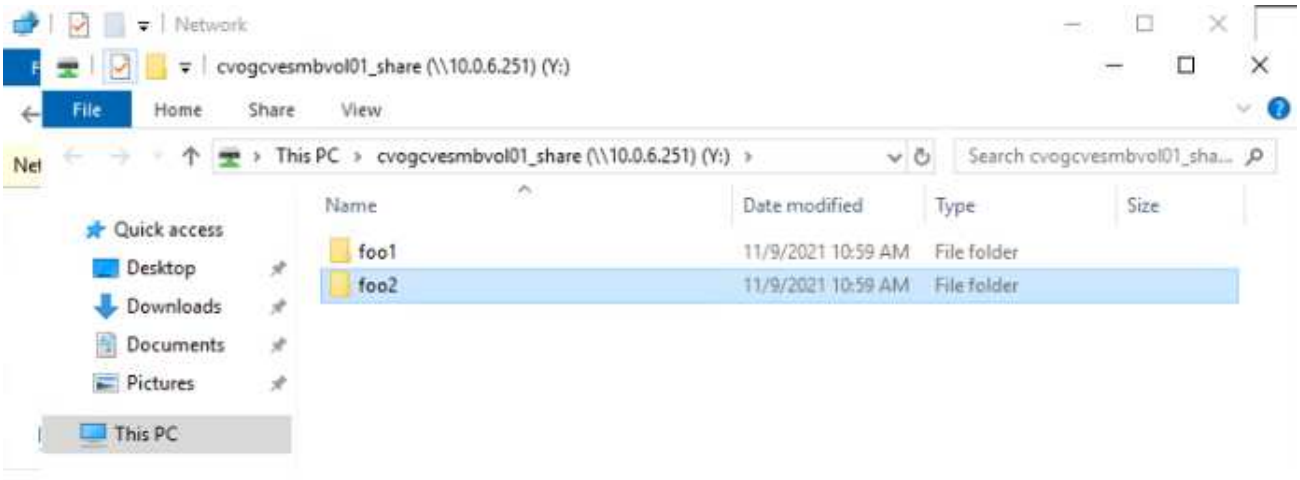
4. 建立磁碟區後，使用 mount 指令顯示磁碟區連線說明，然後從 Google Cloud VMware Engine 上的虛擬機器連線到共用。



5. 複製以下路徑並使用映射網路磁碟機選項將磁碟區掛載到在 Google Cloud VMware Engine 上執行的虛擬機器上。



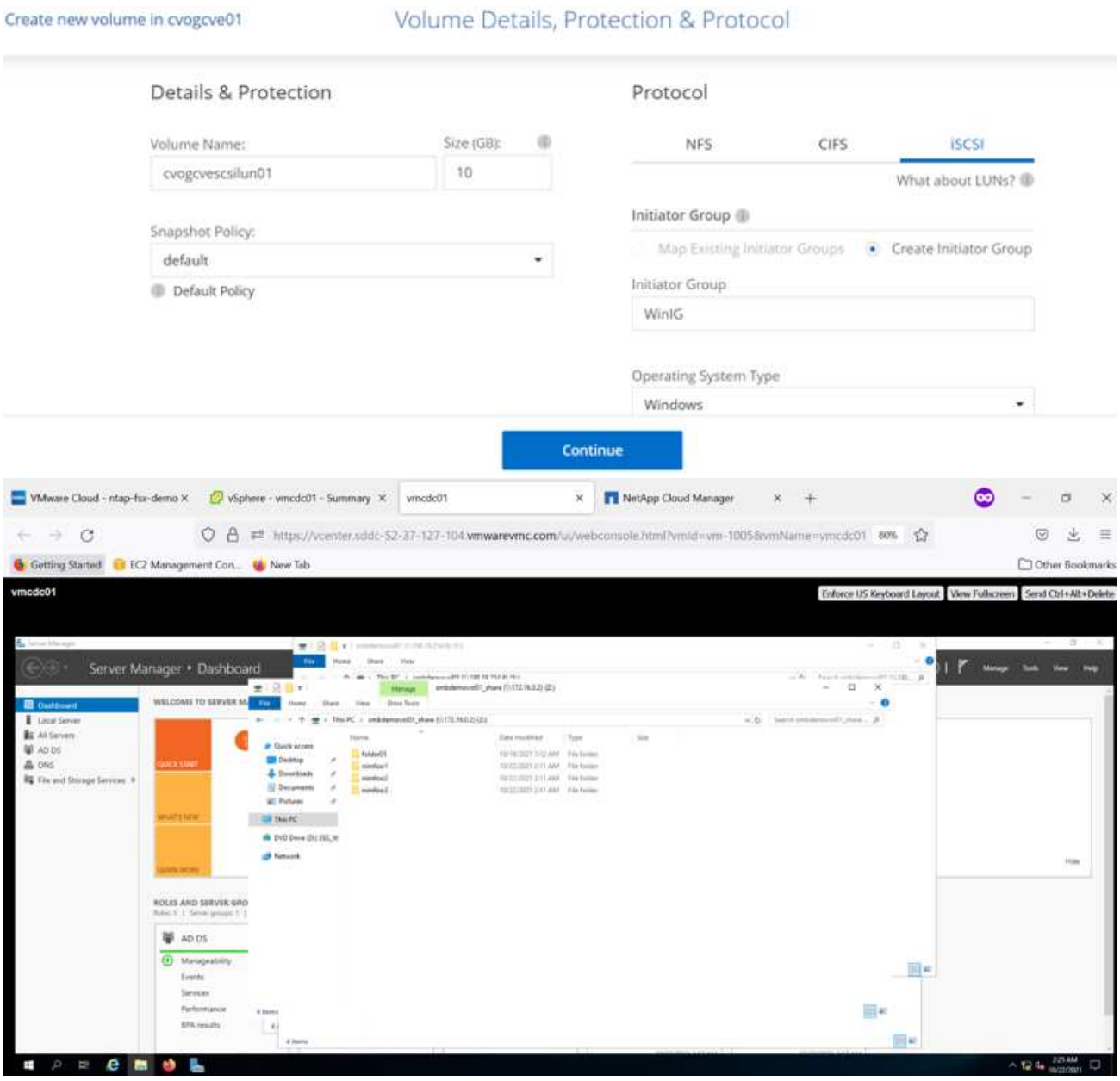
一旦映射，就可以輕鬆訪問，並且可以相應地設定 NTFS 權限。



▼ **Cloud Volumes ONTAP**上的 **LUN** 連接到主機

若要將雲端磁碟區ONTAP LUN 連接到主機，請完成下列步驟：

1. 在「畫布」頁面上，雙擊Cloud Volumes ONTAP工作環境以建立和管理磁碟區。
2. 按一下新增磁碟區 > 新磁碟區並選擇 iSCSI，然後按一下建立啟動器群組。按一下「Continue（繼續）」。



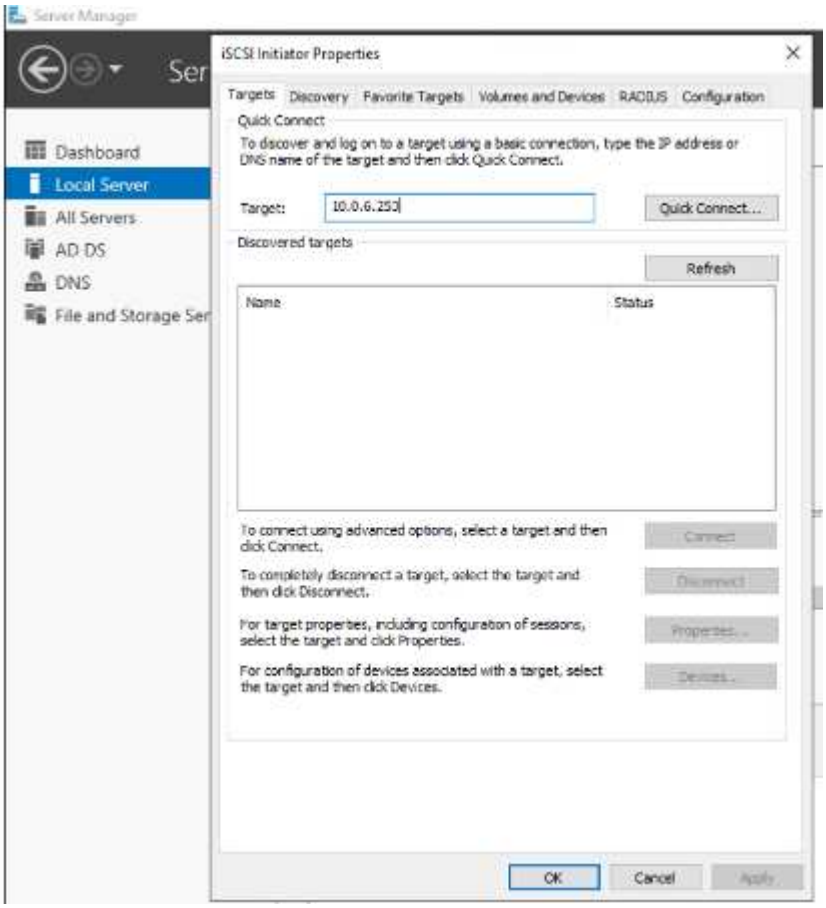
3. 配置磁碟區後，選擇磁碟區選單 (º)，然後按一下目標 iQN。若要複製 iSCSI 限定名稱 (iQN)，請按一下複製。建立從主機到 LUN 的 iSCSI 連線。

若要對駐留在 Google Cloud VMware Engine 上的主機完成相同操作：

1. 透過 RDP 連接到託管在 Google Cloud VMware Engine 上的虛擬機器。
2. 開啟 iSCSI 發起程式屬性對話方塊：伺服器管理員 > 儀表板 > 工具 > iSCSI 發起程式。
3. 在“發現”標籤中，按一下“發現入口網站”或“新增入口網站”，然後輸入 iSCSI 目標連接埠的 IP 位址。

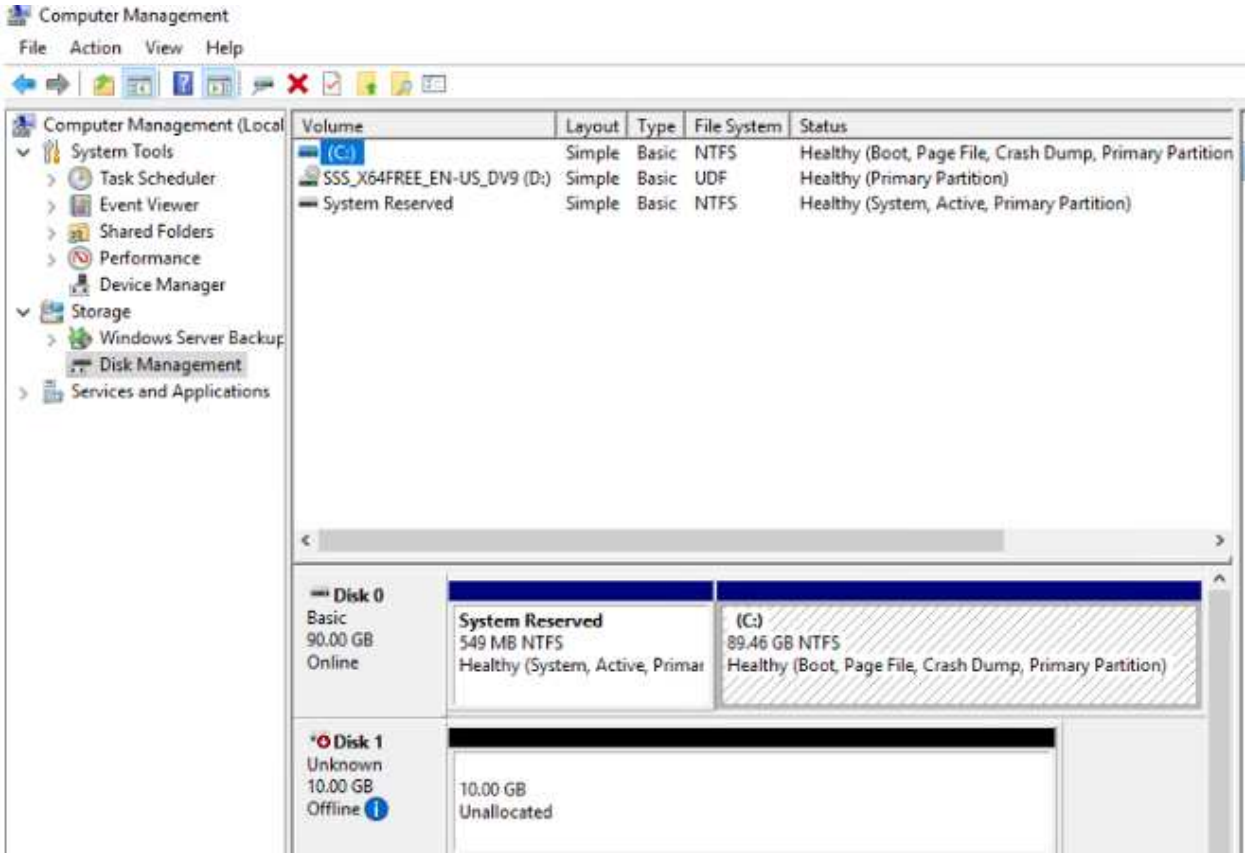
4. 從「目標」標籤中，選擇發現的目標，然後按一下「登入」或「連線」。
5. 選擇啟用多路徑，然後選擇電腦啟動時自動恢復此連線或將此連線新增至收藏目標清單。按一下“進階”。

> Windows 主機必須與群集中的每個節點建立 iSCSI 連線。本機 DSM 選擇要使用的最佳路徑。



儲存虛擬機器 (SVM) 上的 LUN 對於 Windows 主機來說顯示為磁碟。主機不會自動發現任何新新增的磁碟。透過完成以下步驟觸發手動重新掃描以發現磁碟：

a. 開啟 Windows 電腦管理公用程式：開始 > 管理工具 > 電腦管理。
b. 在導航樹中展開儲存節點。
c. 按一下“磁碟管理”。
d. 按一下操作 > 重新掃描磁碟。

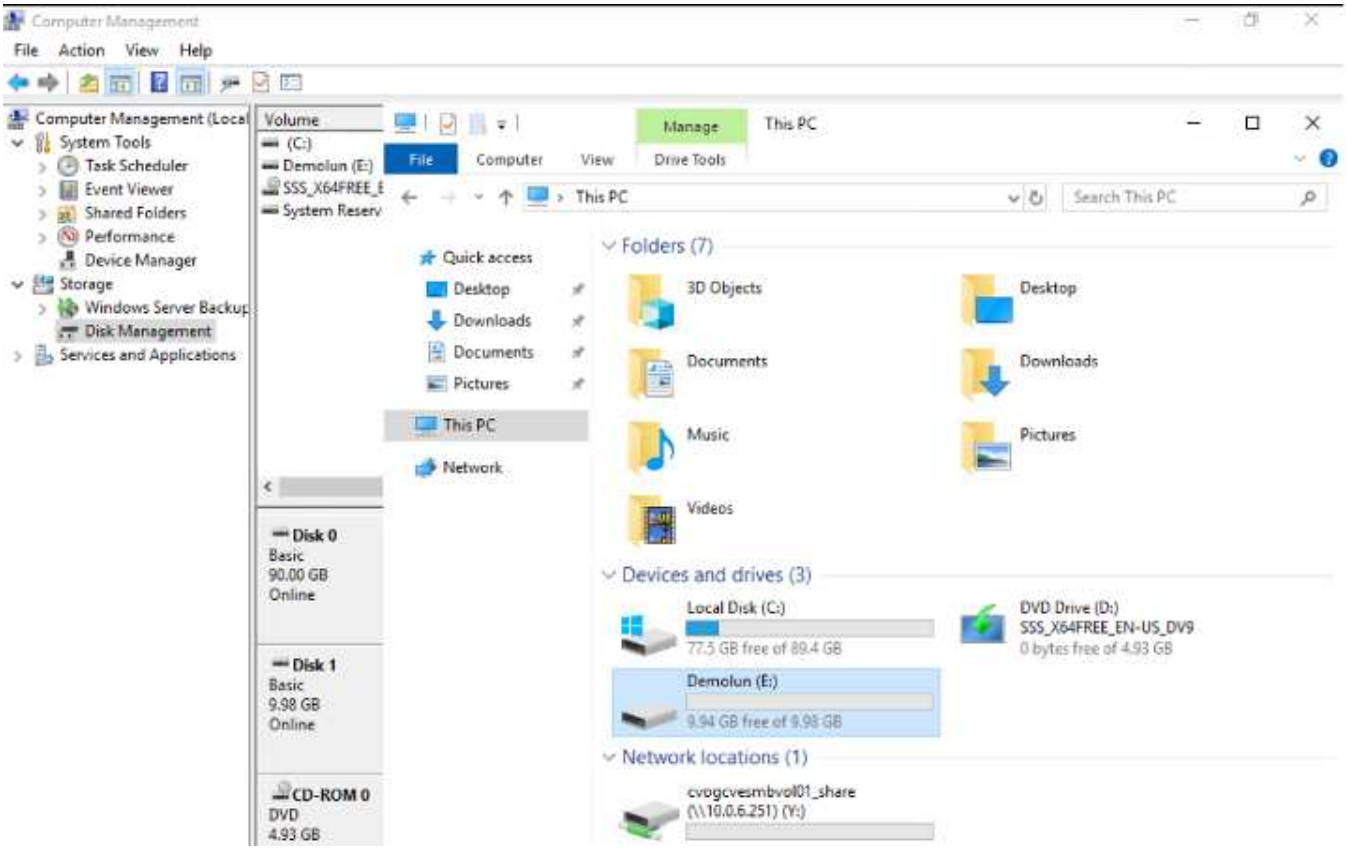


當 Windows 主機首次存取新的 LUN 時，它沒有分割區或檔案系統。初始化 LUN；並且（可選）透過完成以下步驟使用檔案系統格式化 LUN：

a. 啟動 Windows 磁碟管理。

b. 右鍵單擊 LUN，然後選擇所需的磁碟或分割區類型。

c. 請按照精靈中的說明進行操作。在此範例中，已安裝磁碟機 F:。



在 Linux 用戶端上，確保 iSCSI 守護程序正在執行。配置 LUN 後，請參閱此處以 Ubuntu 為例的 iSCSI 設定詳細指南。要驗證，請從 shell 運行 lsblk cmd。

```
nlyaz@nlmubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

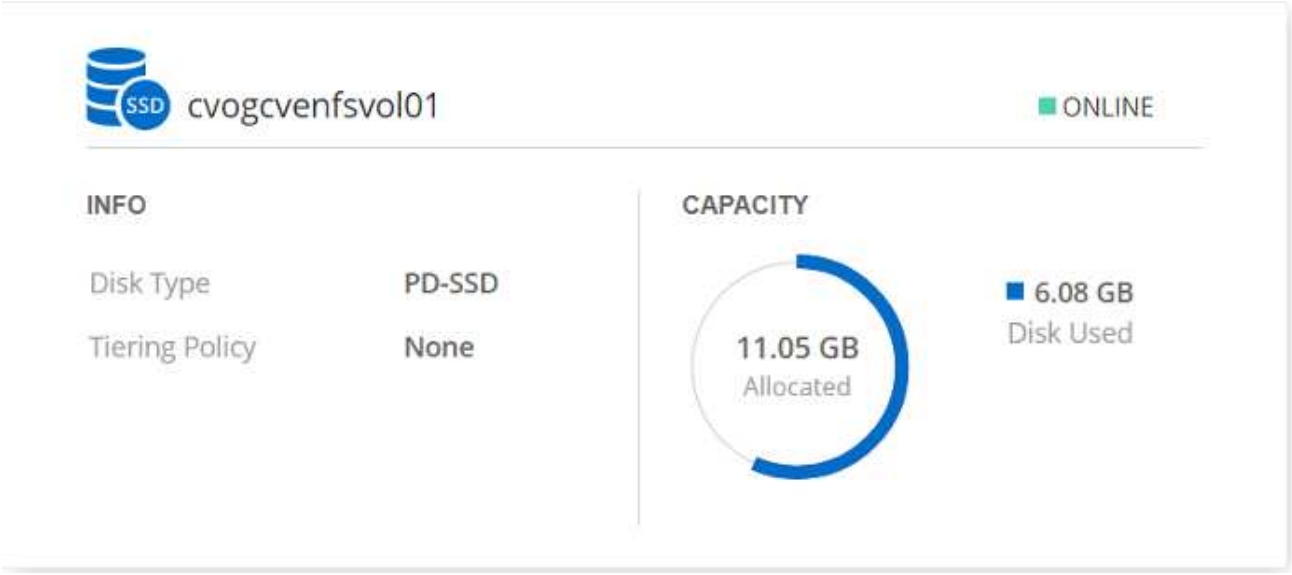
```
nlyaz@nlnubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M     0 100% /snap/snap-store/547
/dev/loop0       56M   56M     0 100% /snap/core18/2128
/dev/loop4       33M   33M     0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M   1% /boot/efi
tmpfs           394M   64K  394M   1% /run/user/1000
/dev/loop5       33M   33M     0 100% /snap/snapd/13640
/dev/loop6       56M   56M     0 100% /snap/core18/2246
/dev/loop7      128K  128K     0 100% /snap/bare/5
/dev/loop8       66M   66M     0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M   1% /mnt
```

▼ 在 **Linux** 用戶端上掛載**Cloud Volumes ONTAP NFS** 卷

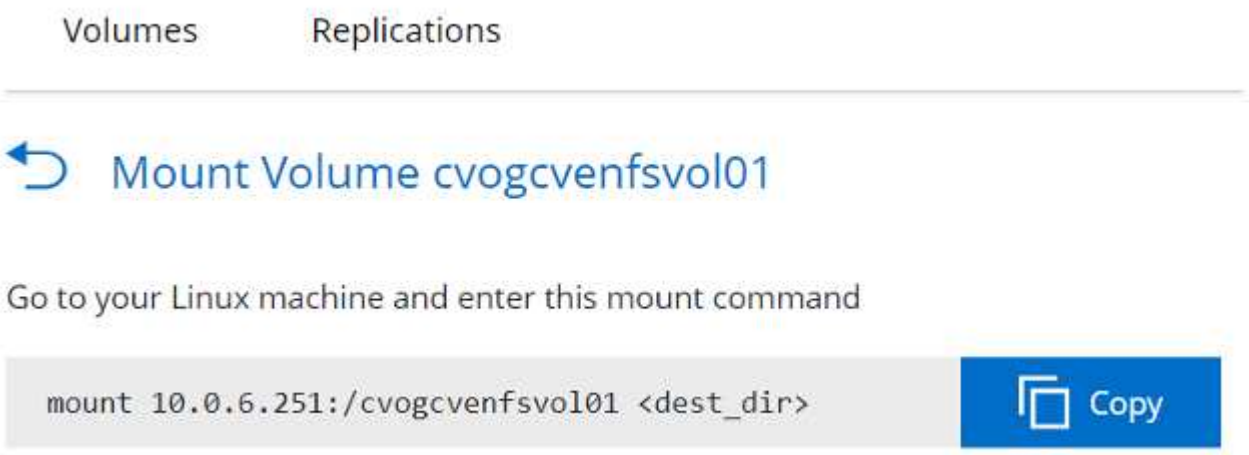
若要從 Google Cloud VMware Engine 中的虛擬機器掛載Cloud Volumes ONTAP (DIY) 檔案系統，請依照下列步驟操作：

請依照下列步驟配置磁碟區

1. 在磁碟區選項卡中，按一下建立新磁碟區。
2. 在「建立新磁碟區」頁面上，選擇磁碟區類型：



3. 在「磁碟區」標籤中，將滑鼠遊標放在磁碟區上，選擇選單圖示 (º)，然後按一下「掛載指令」。



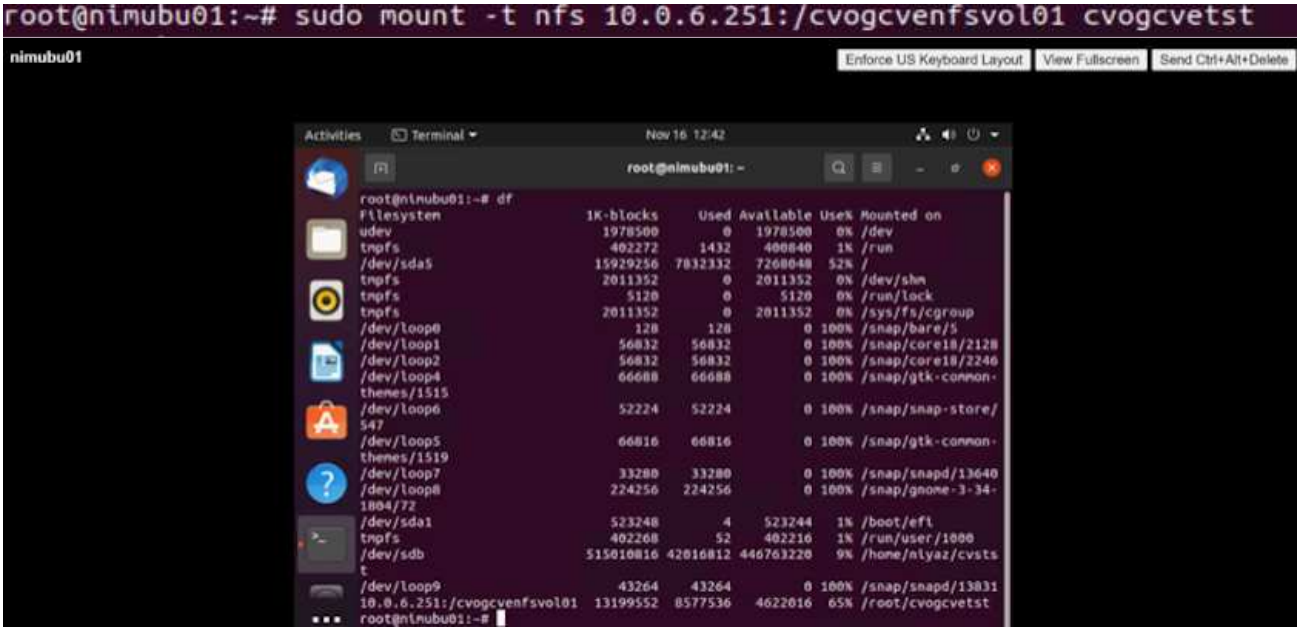
4. 按一下“複製”。
5. 連接到指定的Linux實例。
6. 使用安全殼 (SSH) 在執行個體上開啟終端並使用適當的憑證登入。
7. 使用下列指令為磁碟區的掛載點建立目錄。

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. 將Cloud Volumes ONTAP NFS 磁碟區掛載到上一個步驟所建立的目錄。

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



Google Cloud NetApp Volumes(NetApp區)

Google Cloud NetApp Volumes （NetApp Volumes）是一套完整的資料服務組合，可提供先進的雲端解決方案。 NetApp Volumes 支援主要雲端供應商的多種文件存取協定（NFS 和 SMB 支援）。

其他優點和功能包括：使用快照進行資料保護和復原；在本地或雲端複製、同步和遷移資料目的地的特殊功能；以及在專用快閃記憶體系統層級保持一致的高效能。

Google Cloud NetApp Volumes （NetApp Volumes）作為來賓連接存儲

▼ 使用 **VMware Engine** 設定**NetApp**區

可從在 VMware Engine 環境中建立的虛擬機器掛載Google Cloud NetApp Volumes共用。由於Google Cloud NetApp Volumes支援 SMB 和 NFS 協議，因此這些磁碟區也可以安裝在 Linux 用戶端上並對應到 Windows 用戶端上。可以透過簡單的步驟來設定Google Cloud NetApp Volumes磁碟區。

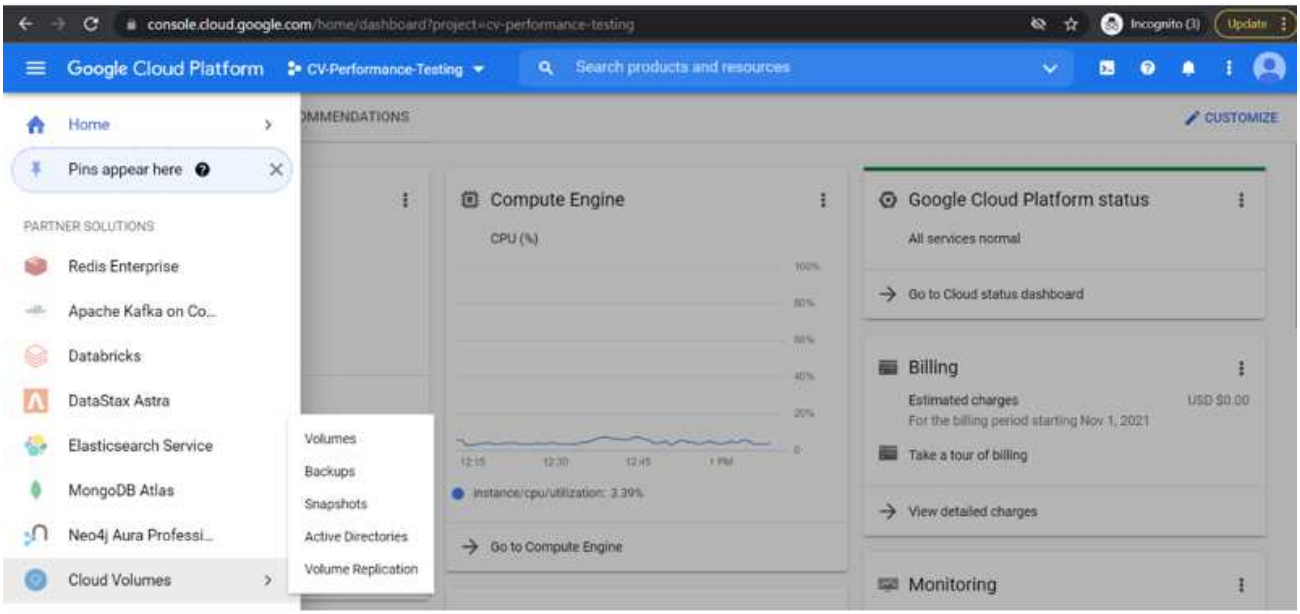
Google Cloud NetApp Volumes和 Google Cloud VMware Engine 私有雲必須位於同一區域。

若要從 Google Cloud Marketplace 購買、啟用和設定適用於 Google Cloud 的 Google Google Cloud NetApp Volumes ，請依照以下詳細說明操作"指導"。

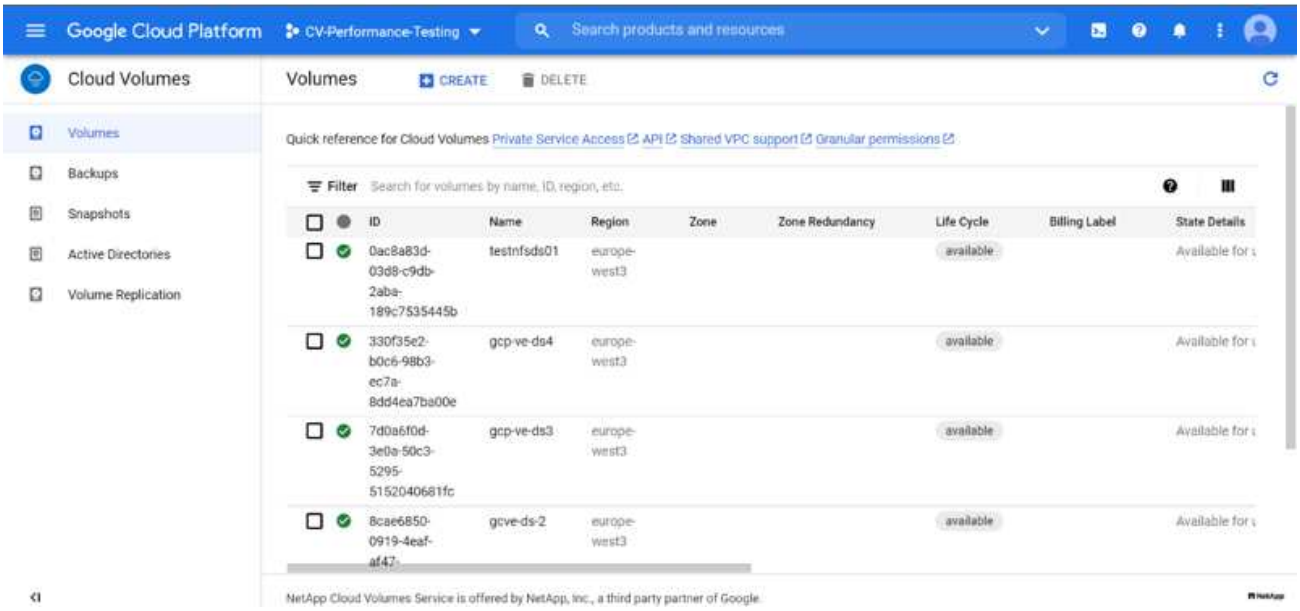
▼ 建立**NetApp Volumes NFS** 捲到 **GCVE** 私有雲

若要建立和掛載 NFS 卷，請完成下列步驟：

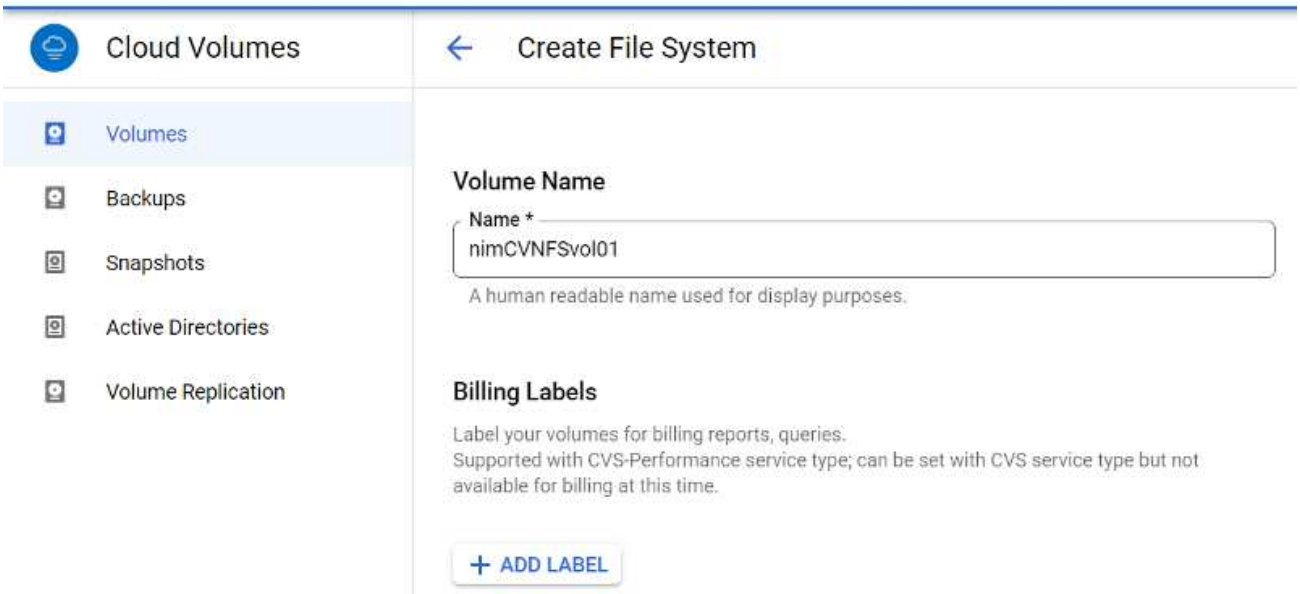
1. 從 Google 雲端控制台中的合作夥伴解決方案存取 Cloud Volumes。



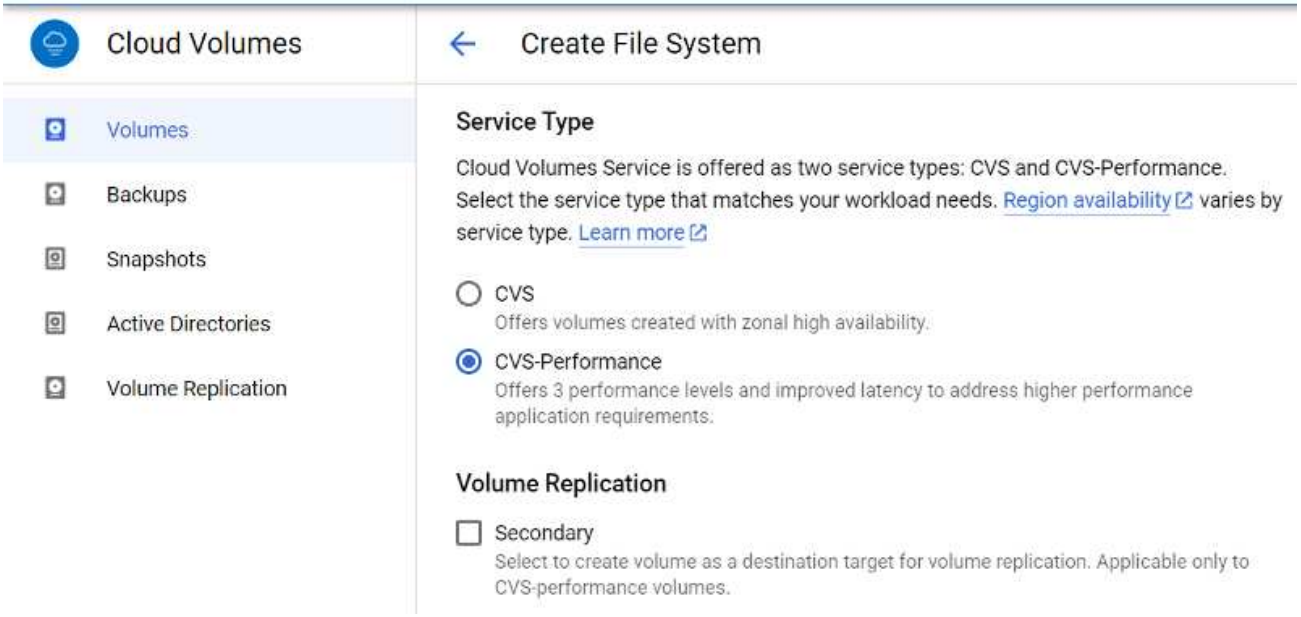
2. 在 Cloud Volumes 控制台中，前往磁碟區頁面並按一下建立。



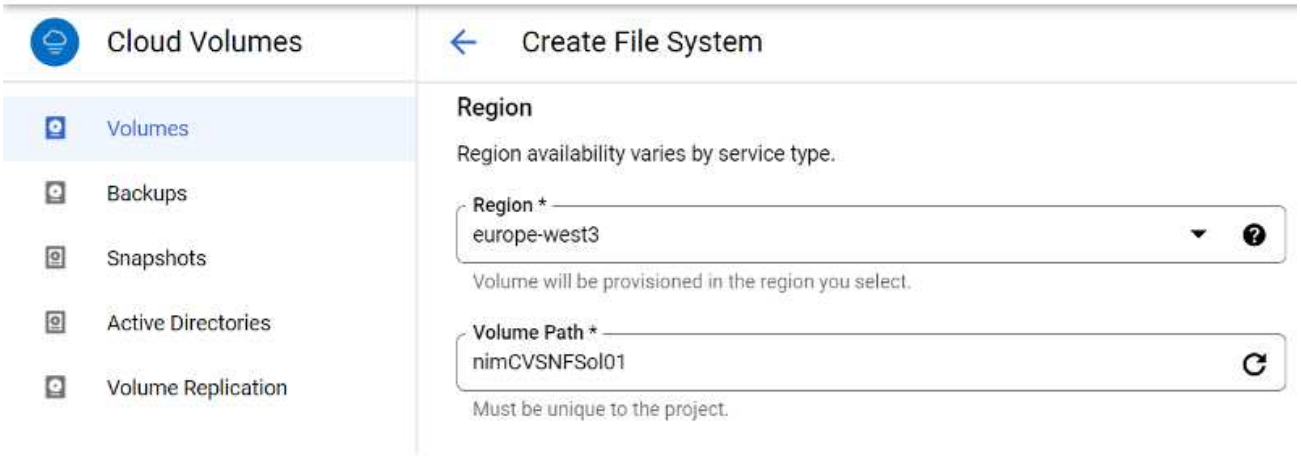
3. 在建立檔案系統頁面上，根據退款機制的需要指定磁碟區名稱和計費標籤。



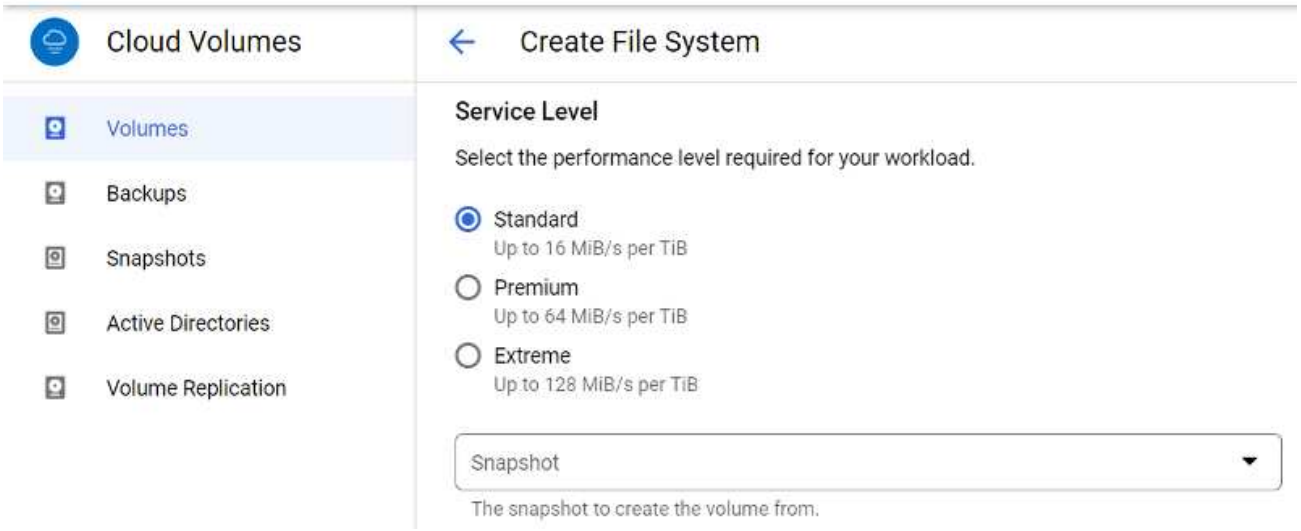
4. 選擇適當的服務。對於 GCVE，根據應用程式工作負載要求選擇NetApp Volumes-Performance 和所需的服務級別，以改善延遲並提高效能。



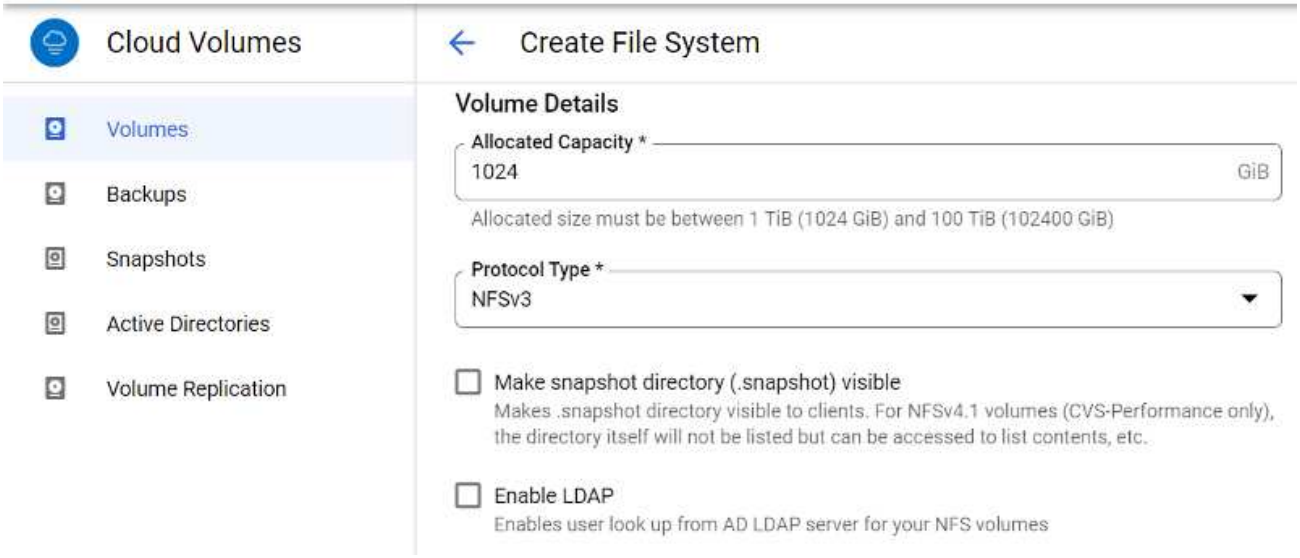
5. 指定磁碟區和磁碟區路徑的 Google Cloud 區域（磁碟區路徑在專案的所有雲端磁碟區中必須是唯一的）



6. 選擇磁碟區的效能等級。

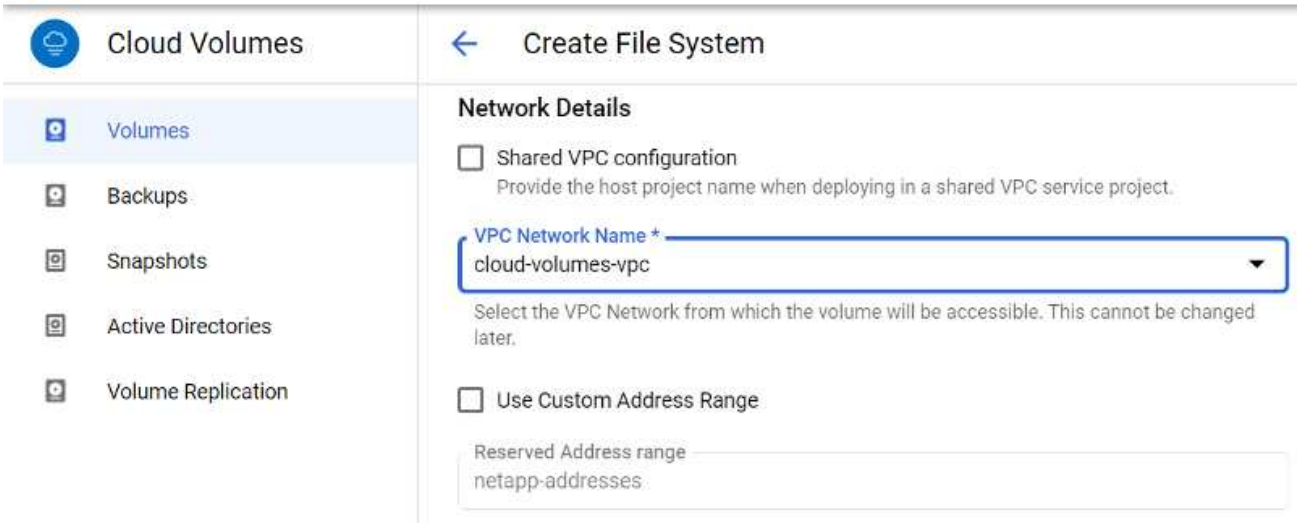


7. 指定磁碟區的大小和協定類型。本次測試採用的是NFSv3。



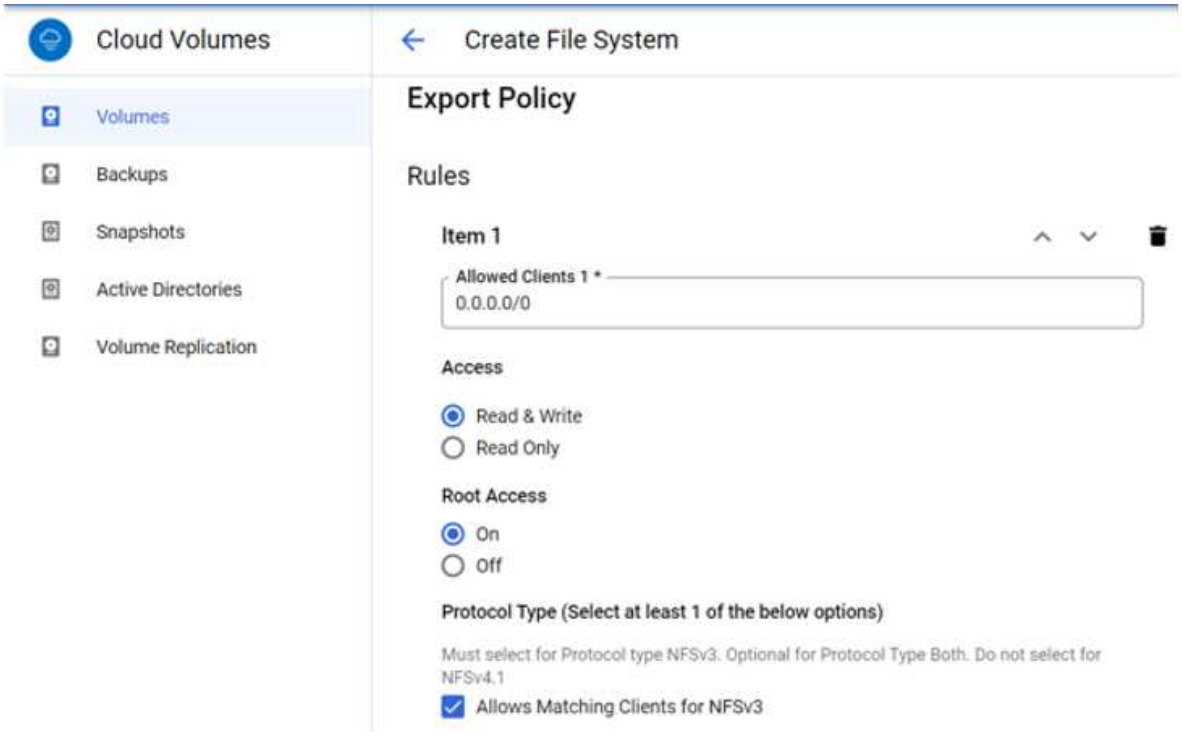
8. 在此步驟中，選擇可存取磁碟區的 VPC 網路。確保 VPC 對等連接已到位。

   提示：如果尚未完成 VPC 對等連接，則會顯示一個彈出按鈕來引導您完成對等連接命令。開啟 Cloud Shell 會話並執行適當的命令以將您的 VPC 與Google Cloud NetApp Volumes生產者對等連接。如果您決定提前準備 VPC 對等連接，請參閱這些說明。



9. 透過新增適當的規則來管理匯出策略規則並選取對應 NFS 版本的核取方塊。

   注意：除非新增匯出策略，否則無法存取 NFS 磁碟區。



10. 按一下「儲存」以建立磁碟區。



▼ 將 **NFS** 匯出掛載到在 **VMware Engine** 上執行的虛擬機

在準備掛載 NFS 磁碟區之前，請確保私有連線的對等狀態列為「活動」。一旦狀態為“活動”，請使用 mount 指令。

若要掛載 NFS 卷，請執行下列操作：

1. 在 Cloud Console 中，前往 Cloud Volumes > Volumes。
2. 前往卷頁面
3. 按一下要掛載 NFS 匯出的 NFS 磁碟區。
4. 捲動到右側，在“顯示更多”下按一下“安裝說明”。

若要從 VMware VM 的客戶作業系統執行安裝流程，請依照下列步驟操作：

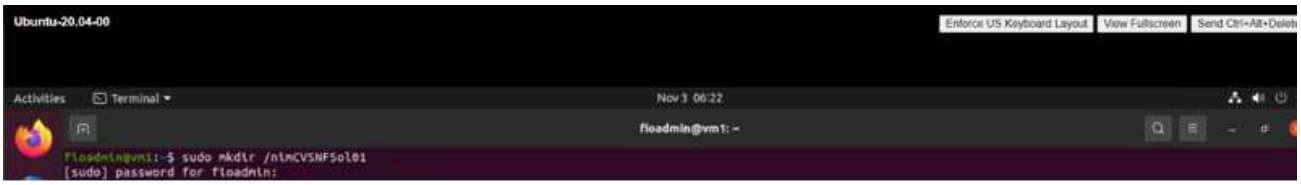
1. 使用 SSH 用戶端並透過 SSH 連接到虛擬機器。
2. 在實例上安裝 nfs 用戶端。
   a. 在 Red Hat Enterprise Linux 或 SuSE Linux 實例上：

```
 sudo yum install -y nfs-utils
.. 在 Ubuntu 或 Debian 實例上：
```

```
sudo apt-get install nfs-common
```

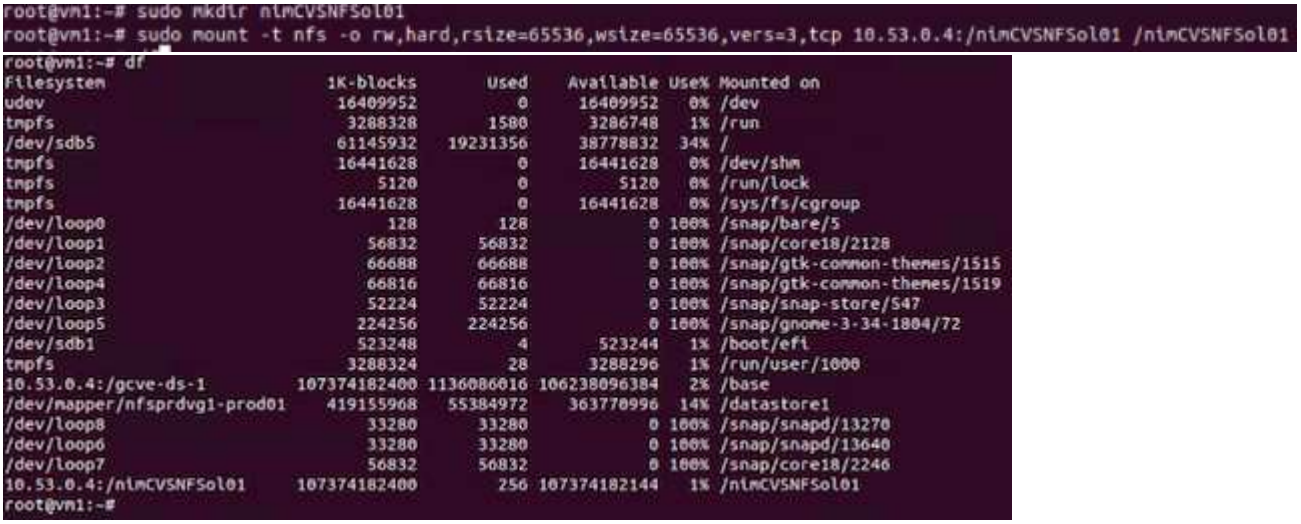
3. 在實例上建立一個新目錄，例如“/nimCVSNFSol01”：

```
sudo mkdir /nimCVSNFSol01
```



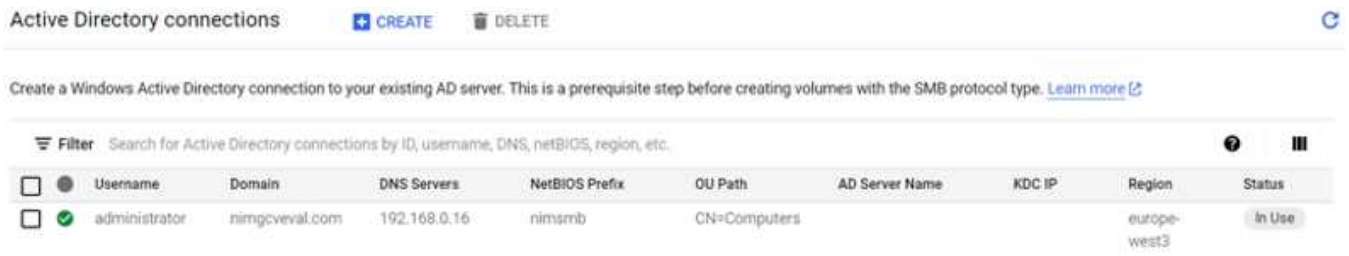
4. 使用適當的命令掛載卷。實驗室的範例命令如下：

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



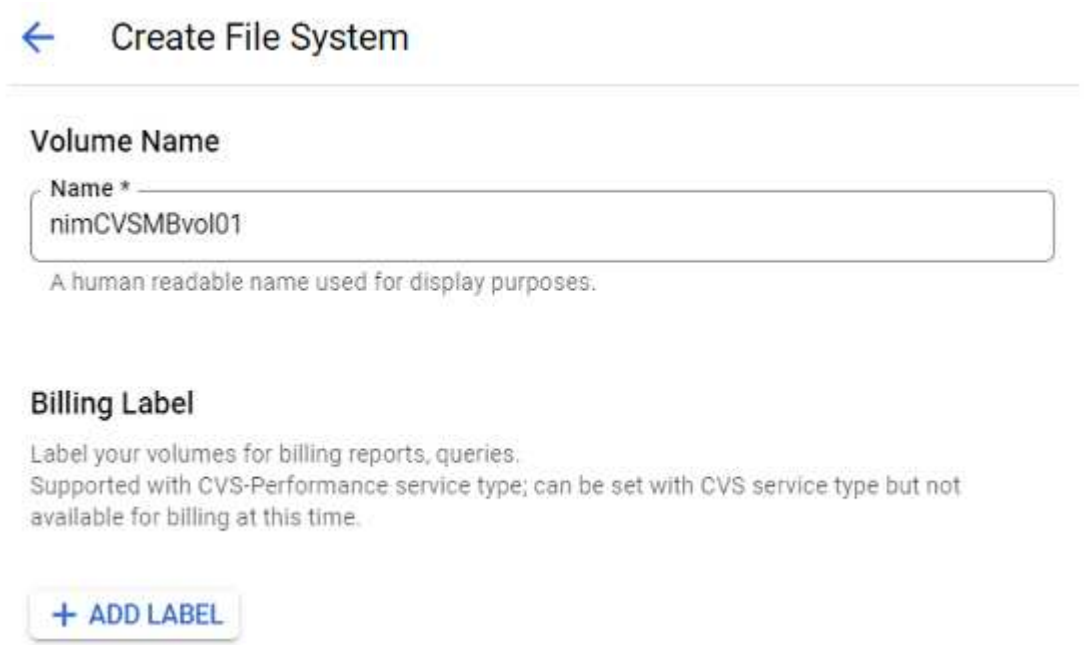
▼ 建立 **SMB** 共用並將其掛載到在 **VMware Engine** 上執行的虛擬機

對於 SMB 卷，請確保在建立 SMB 磁碟區之前已設定了 Active Directory 連線。

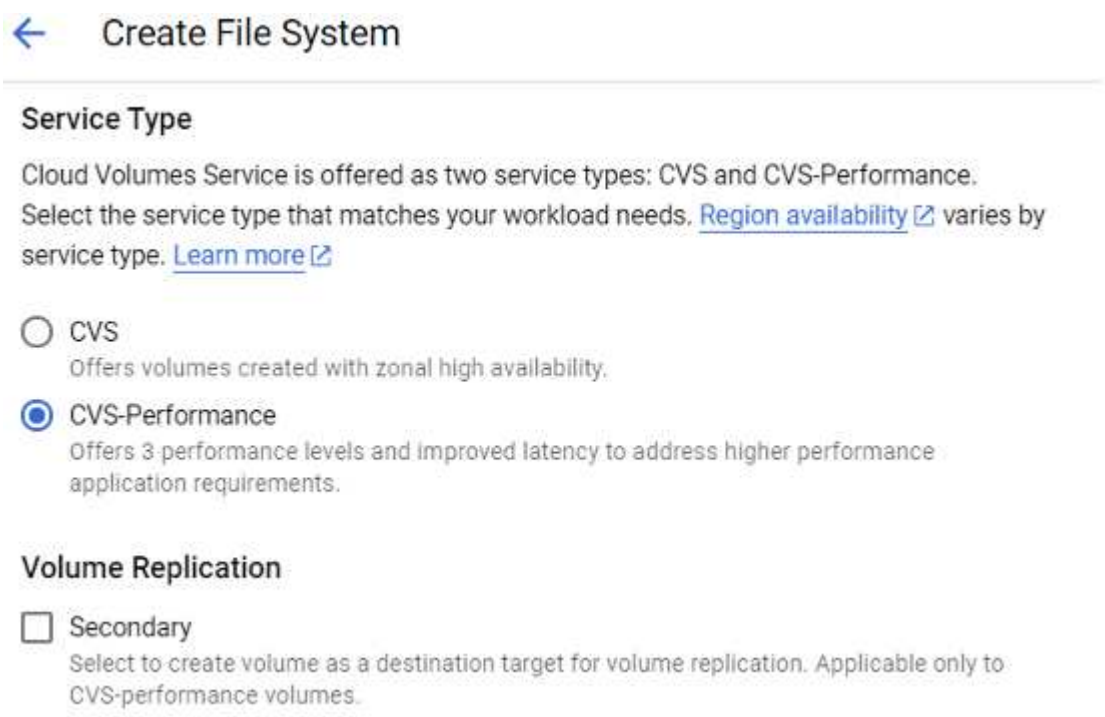


一旦 AD 連接到位，即可建立具有所需服務等級的磁碟區。除了選擇適當的協定外，步驟與建立 NFS 磁碟區類似。

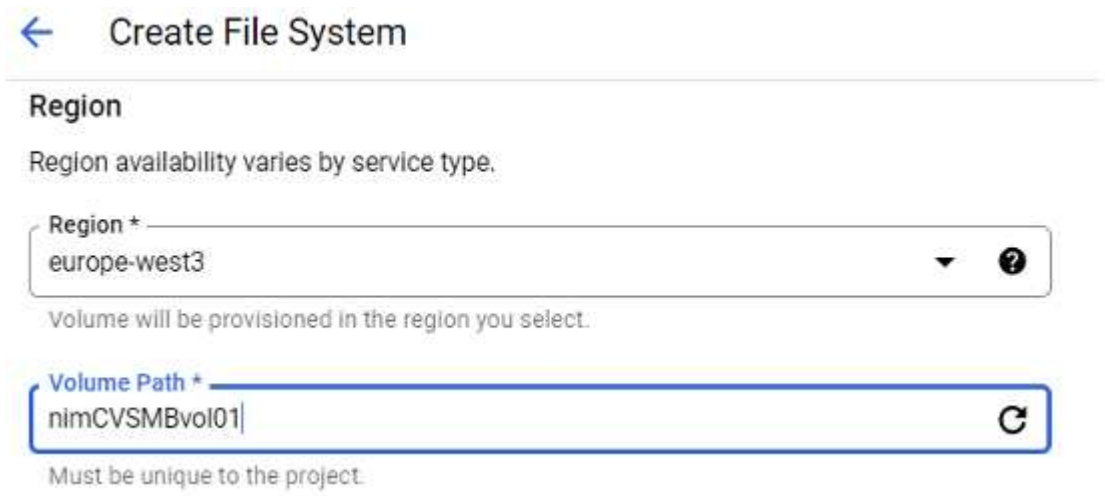
1. 在 Cloud Volumes 控制台中，前往磁碟區頁面並按一下建立。
2. 在建立檔案系統頁面上，根據退款機制的需要指定磁碟區名稱和計費標籤。



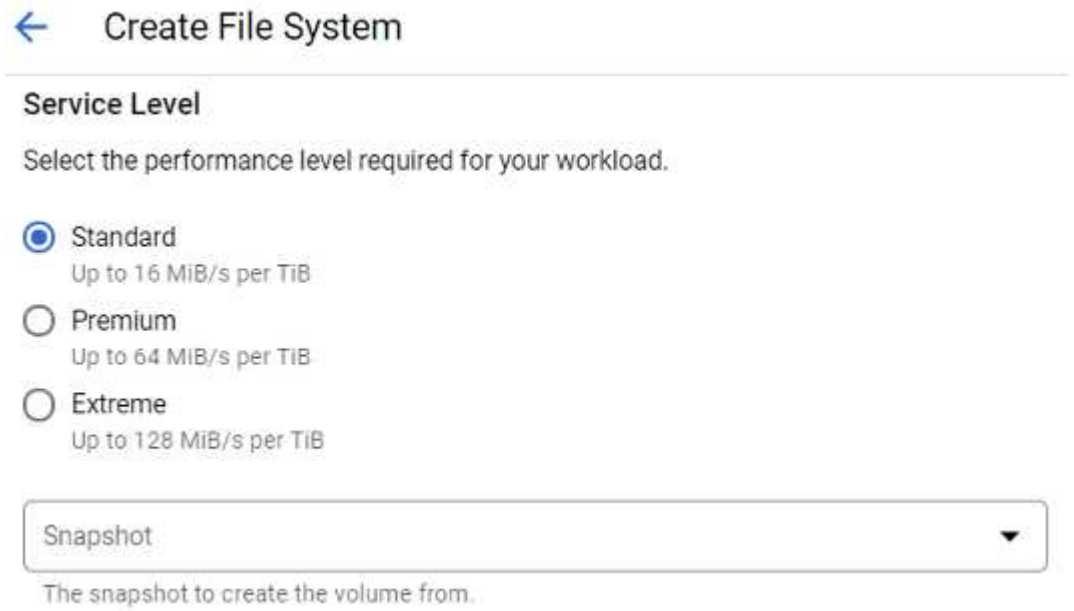
3. 選擇適當的服務。對於 GCVE，根據工作負載要求選擇NetApp Volumes-Performance 和所需的服務級別，以改善延遲並提高效能。



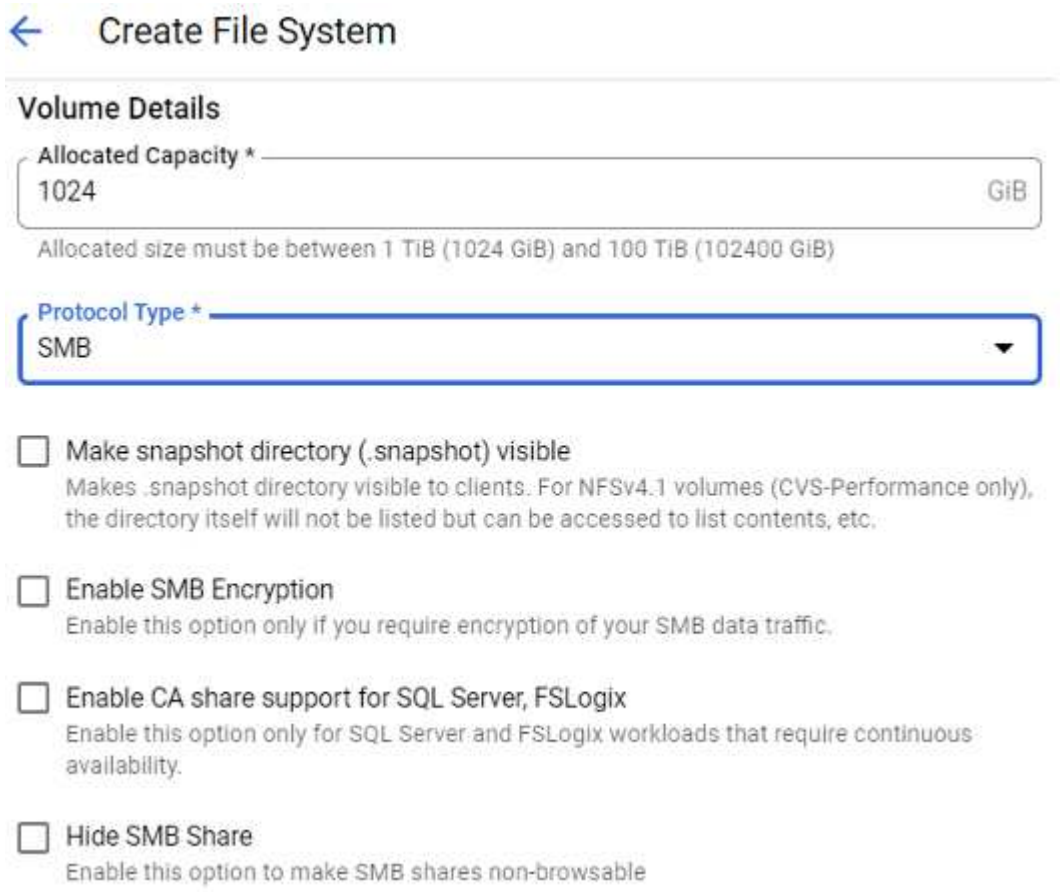
4. 指定磁碟區和磁碟區路徑的 Google Cloud 區域（磁碟區路徑在專案的所有雲端磁碟區中必須是唯一的）



5. 選擇磁碟區的效能等級。

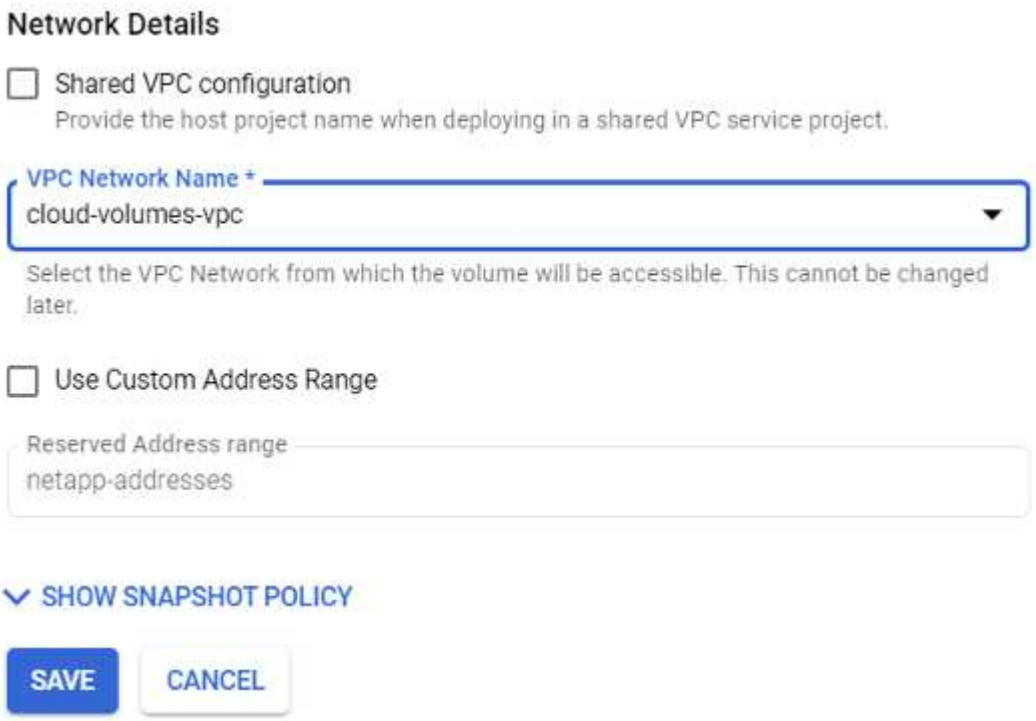


6. 指定磁碟區的大小和協定類型。本次測試中使用了 SMB。



7. 在此步驟中，選擇可存取磁碟區的 VPC 網路。確保 VPC 對等連接已到位。

   提示：如果尚未建立 VPC 對等關係，系統會顯示一個彈出按鈕，提供指南以協助您完成對等關係命令。開啟 Cloud Shell 工作階段，並執行相應的命令，將您的 VPC 與 Google Cloud NetApp Volumes 生產者建立對等關係。如果您決定預先準備 VPC 對等關係，請參閱這些 "指示"。



8. 按一下「儲存」以建立磁碟區。



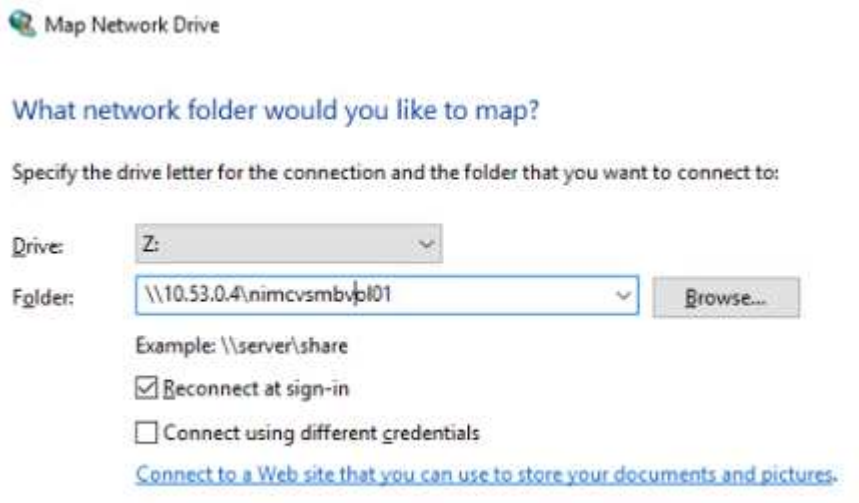
若要安裝 SMB 卷，請執行以下操作：

1. 在 Cloud Console 中，前往 Cloud Volumes > Volumes。
2. 前往卷頁面
3. 按一下要對應 SMB 共享的 SMB 磁碟區。
4. 捲動到右側，在“顯示更多”下按一下“安裝說明”。

若要從 VMware VM 的 Windows 用戶作業系統執行安裝流程，請依照下列步驟操作：

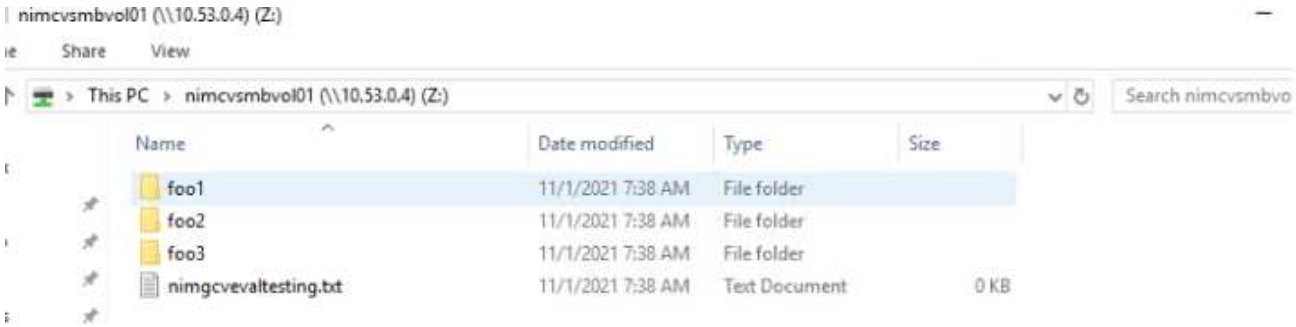
1. 按一下“開始”按鈕，然後按一下“電腦”。
2. 按一下「映射網路磁碟機」。
3. 在磁碟機清單中，按一下任何可用的磁碟機號。
4. 在資料夾框中，鍵入：

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



若要在每次登入電腦時進行連接，請勾選「登入時重新連接」複選框。

5. 按一下“完成”。



總結與結論： **NetApp**為何選擇 **VMware** 作為混合多雲平台

NetApp Cloud Volumes 與主要超大規模企業的 VMware 解決方案為希望利用混合雲的組織提供了巨大的潛力。本節的其餘部分提供了用例，表明整合NetApp Cloud Volumes 可以實現真正的混合多雲功能。

用例 **#1**：優化存儲

當使用 RVtools 輸出執行大小調整練習時，馬力（vCPU/vMem）比例與儲存平行是顯而易見的。很多時候，組織會發現他們所處的境地是，所需的儲存空間使叢集的規模遠遠超出了馬力所需的範圍。

透過整合NetApp Cloud Volumes，組織可以透過簡單的遷移方法實現基於 vSphere 的雲端解決方案，無需重新平台化、無需 IP 變更、無需架構變更。此外，透過此最佳化，您可以擴充儲存空間，同時將主機數量保持在 vSphere 所需的最少量，但不會改變儲存層次結構、安全性或可用的檔案。這使您可以優化部署並將總體 TCO 降低 35–45%。透過這種集成，您還可以在幾秒鐘內將儲存空間從熱儲存擴展到生產級效能。

用例**2**：雲端遷移

由於多種原因，組織面臨著將應用程式從本地資料中心遷移到公有雲的壓力：租約即將到期；財務指令要求從資本支出 (capex) 轉向營運支出 (opex)；或者僅僅是自上而下的命令要求將所有內容遷移到雲端。

當速度至關重要時，只有簡化的遷移方法是可行的，因為重新平台化和重構應用程式以適應雲端的特定 IaaS 平台既緩慢又昂貴，通常需要數月時間。透過將NetApp Cloud Volumes 與用於客戶端連接儲存的頻寬高效的SnapMirror複製（包括與應用程式一致的 Snapshot 副本和 HCX 結合的 RDM、特定於雲端的遷移（例如 Azure Migrate）或用於複製虛擬機器的第三方產品）相結合，這種轉變比依賴過濾機制更容易。

用例**3**：資料中心擴展

當資料中心因季節性需求高峰或僅僅是穩定的有機成長而達到容量限制時，遷移到雲端託管的 VMware 以及NetApp Cloud Volumes 是一個簡單的解決方案。利用NetApp Cloud Volumes，可以透過提供跨可用區域的高可用性和動態擴充功能，非常輕鬆地建立、複製和擴充儲存。利用NetApp Cloud Volumes 有助於克服對延伸叢集的需求，從而最大限度地減少主機叢集容量。

用例 **#4**：災難復原至雲端

在傳統方法中，如果發生災難，複製到雲端的虛擬機器需要轉換到雲端自己的虛擬機器管理程式平台才能恢復 - 這不是危機期間要處理的任務。

透過使用NetApp Cloud Volumes 進行來賓連接存儲，使用來自本地的SnapCenter和SnapMirror複製以及公共雲虛擬化解決方案，可以設計出一種更好的災難恢復方法，允許在完全一致的 VMware SDDC 基礎架構上恢復虛擬機副本以及特定於雲端的恢復工具（例如 Azure Site Recovery）或等效的第三方工具（如 Veeam）。這種方

法還使您能夠快速執行災難復原演習和勒索軟體復原。透過按需添加主機，您還可以擴展到全面生產以進行測試或在災難期間進行擴展。

用例 **#5**：應用程式現代化

應用程式進入公有雲後，組織將希望利用數百種強大的雲端服務來實現其現代化和擴展。透過使用NetApp Cloud Volumes，現代化是一個簡單的過程，因為應用程式資料不會被鎖定在 vSAN 中，並且允許在包括 Kubernetes 在內的廣泛用例中實現資料移動。

結論

無論您的目標是全雲還是混合雲， NetApp Cloud Volumes 都提供了出色的選項來部署和管理應用程式工作負載以及檔案服務和區塊協議，同時透過使資料需求無縫連接到應用程式層來降低 TCO。

無論使用情況如何，選擇您最喜歡的雲端/超大規模器以及NetApp Cloud Volumes，以快速實現雲端優勢、一致的基礎架構和跨本地和多個雲端的操作、工作負載的雙向可移植性以及企業級容量和效能。

它與用於連接儲存的熟悉的過程和程序相同。請記住，新名稱只是改變了資料的位置；工具和流程都保持不變，NetApp Cloud Volumes 有助於優化整體部署。

VMware 混合雲端用例

NetApp與 VMware 混合多雲的用例

概述在規劃混合雲或雲端優先部署時對 IT 組織重要的用例。

熱門用例

用例包括：

- 災難恢復，
- 在資料中心維護期間託管工作負載，* 快速爆發，需要超出本地資料中心配置的額外資源，
- VMware 站點擴展，
- 快速遷移到雲端，
- 開發/測試，以及
- 利用雲端補充技術實現應用程式的現代化。

在本文檔中，將使用 VMware 用例詳細說明雲端工作負載參考。這些用例是：

- 保護（包括災難復原和備份/還原）
- 遷移
- 延長

IT 之旅

大多數組織都處於轉型和現代化的旅程中。作為此過程的一部分，該公司正在嘗試利用其現有的 VMware 投資，同時利用雲端優勢並探索使遷移過程盡可能無縫的方法。由於資料已經在雲端，這種方法將使他們的現代化工

作變得非常容易。

對於這種情況最簡單的答案是每個超大規模企業都提供 VMware 產品。與NetApp Cloud Volumes 一樣，VMware 提供了一種將本機 VMware 環境移動或擴展到任何雲端的方法，使您能夠保留現有的本機資產、技能和工具，同時在雲端中本地運行工作負載。這降低了風險，因為不會出現服務中斷或需要更改 IP，並使 IT 團隊能夠使用現有技能和工具以在本地的方式進行操作。這可以加速雲端遷移並更順利地過渡到混合多雲架構。

了解補充 **NFS** 儲存選項的重要性

雖然任何雲端中的 VMware 都為每個客戶提供了獨特的混合功能，但有限的補充 NFS 儲存選項限制了其對於儲存工作負載繁重的組織的實用性。由於儲存直接與主機綁定，因此擴展儲存的唯一方法是添加更多主機 - 而這會使儲存密集型工作負載的成本增加 35-40% 或更多。這些工作負載只需要額外的儲存空間，而不是額外的馬力。但這意味著需要支付額外的主機費用。

讓我們考慮一下這種情況：

一個客戶只需要五台主機用於 CPU 和內存，但有大量的儲存需求，需要 12 台主機來滿足儲存需求。當他們只需要增加儲存空間時，這個要求最終會真正打破財務平衡，因為他們必須購買額外的馬力。

當您規劃雲端採用和遷移時，評估最佳方法並採取最簡單的途徑來減少總投資始終非常重要。對於任何應用程式遷移來說，最常見且最簡單的方法是重新託管（也稱為提升和轉移），其中不需要虛擬機器（VM）或資料轉換。將NetApp Cloud Volumes 與 VMware 軟體定義資料中心 (SDDC) 結合使用，在補充 vSAN 的同時，提供了簡單的提升和轉移選項。

針對超大規模企業 **VMware** 的**NetApp**解決方案

進一步了解NetApp為每個超大規模企業中的 VMware 環境提供的解決方案 - 從遷移工作流程、擴展/爆發到雲端、備份/還原到災難復原。

適用於 **VMware** 環境的**NetApp**解決方案

無論您採用混合雲模型還是「雲端優先」模型， NetApp都提供各種解決方案來滿足在雲端或混合雲模型中管理工作負載的最常見用例。

NetApp也為每個超大規模伺服器中的儲存提供解決方案，這些儲存可作為客戶機內（客戶機連接）儲存或補充 NFS 資料儲存。所有解決方案均依照 VMware 的雲端工作負載分類進行分類。這些分類包括：

- 保護（包括災難復原和備份/還原）
- 遷移
- 延長

有關每個超大規模企業可用解決方案的更多詳細信息，請訪問：

- "AWS/VMC 解決方案"
- "Azure/AVS 解決方案"
- "GCP/GCVE 解決方案"

適用於 **Amazon VMware** 託管雲端 **(VMC)** 的**NetApp**解決方案

詳細了解NetApp為 AWS 帶來的解決方案。

VMware 將雲端工作負載分為以下三類：

- 保護（包括災難復原和備份/還原）
- 遷移
- 延長

瀏覽以下部分中可用的解決方案。

保護

- "使用 AWS 上的 VMC 進行災難復原（來賓連線）"
- "使用 FSx ONTAP在 VMC 中備份和還原 Veeam"
- "使用 FSx ONTAP和 VMC 實現災難復原 (DRO)"
- "使用 Veeam Replication 和 FSx ONTAP實作 VMware Cloud on AWS 災難復原"

遷移

- "使用 VMware HCX 將工作負載遷移到 FSx ONTAP資料儲存區"

延長

即將推出！ ！

適用於 **Azure VMware** 解決方案 **(AVS)** 的**NetApp**解決方案

詳細了解NetApp為 Azure 帶來的解決方案。

VMware 將雲端工作負載分為以下三類：

- 保護（包括災難復原和備份/還原）
- 遷移
- 延長

瀏覽以下部分中可用的解決方案。

保護

- "使用 ANF 和 JetStream 進行災難復原（補充 NFS 資料儲存）"
- "使用 ANF 和 CVO（來賓連接儲存）進行災難復原"
- "使用 ANF 和 AVS 的災難復原 (DRO)"
- "使用 Veeam Replication 和Azure NetApp Files資料儲存區對 Azure VMware 解決方案進行災難復原"

遷移

- "使用 VMware HCX 將工作負載遷移到Azure NetApp Files資料存儲"

延長

即將推出！ ！

適用於 **Google Cloud VMware Engine (GCVE)** 的**NetApp**解決方案

詳細了解NetApp為 GCP 帶來的解決方案。

VMware 將雲端工作負載分為以下三類：

- 保護（包括災難復原和備份/還原）
- 遷移
- 延長

瀏覽以下部分中可用的解決方案。

保護

- "使用SnapCenter、 Cloud Volumes ONTAP和 Veeam Replication 實現應用程式災難復原"
- "使用NetApp SnapCenter和 Veeam Replication 實現應用程式一致性災難恢復，以在 GCVE 上複製NetApp卷"

遷移

- "使用 VMware HCX 將工作負載遷移到Google Cloud NetApp Volumes NFS 資料儲存區"
- "使用 Veeam 到Google Cloud NetApp Volumes NFS 資料儲存區的虛擬機器複製"

延長

即將推出！ ！

適用於 **AWS/VMC** 的**NetApp**

NetApp的 **AWS VMC** 功能

進一步了解NetApp為 AWS VMware Cloud (VMC) 帶來的功能 - 從NetApp作為來賓連接儲存裝置或補充 NFS 資料儲存到遷移工作流程、擴展/爆發到雲端、備份/復原和災難復原。

透過選擇以下選項跳到所需內容的部分：

- "在 AWS 中配置 VMC"
- "適用於 VMC 的NetApp儲存選項"
- "NetApp /VMware 雲端解決方案"

在 **AWS** 中配置 **VMC**

與本地一樣，規劃基於雲端的虛擬化環境對於成功創建虛擬機器和遷移的生產就緒環境至關重要。

本節介紹如何設定和管理 VMware Cloud on AWS SDDC，並將其與可用於連接NetApp儲存的選項結合使用。

客戶機內儲存是將Cloud Volumes ONTAP連接到 AWS VMC 的唯一支援方法。

設定過程可分為以下步驟：

- 部署和配置 VMware Cloud for AWS
- 將 VMware Cloud 連接到 FSx ONTAP

查看詳細信息"VMC 的設定步驟"。

適用於 **VMC** 的**NetApp**儲存選項

NetApp儲存在 AWS VMC 中可以以多種方式使用 - 既可以作為猜測連接，也可以作為補充 NFS 資料儲存。

請訪問"支援的NetApp儲存選項"了解更多。

AWS 支援以下配置的NetApp儲存：

- FSx ONTAP作為來賓連接存儲
- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- FSx ONTAP作為補充 NFS 資料存儲

查看詳細信息"VMC 的用戶機連線儲存選項"。查看詳細信息"VMC 的補充 NFS 資料儲存選項"。

解決方案用例

透過NetApp和 VMware 雲端解決方案，許多用例都可以輕鬆部署在您的 AWS VMC 中。針對 VMware 定義的每個雲端區域都定義了用例：

- 保護（包括災難復原和備份/還原）
- 延長
- 遷移

"瀏覽適用於 AWS VMC 的NetApp解決方案"

保護 **AWS/VMC** 上的工作負載

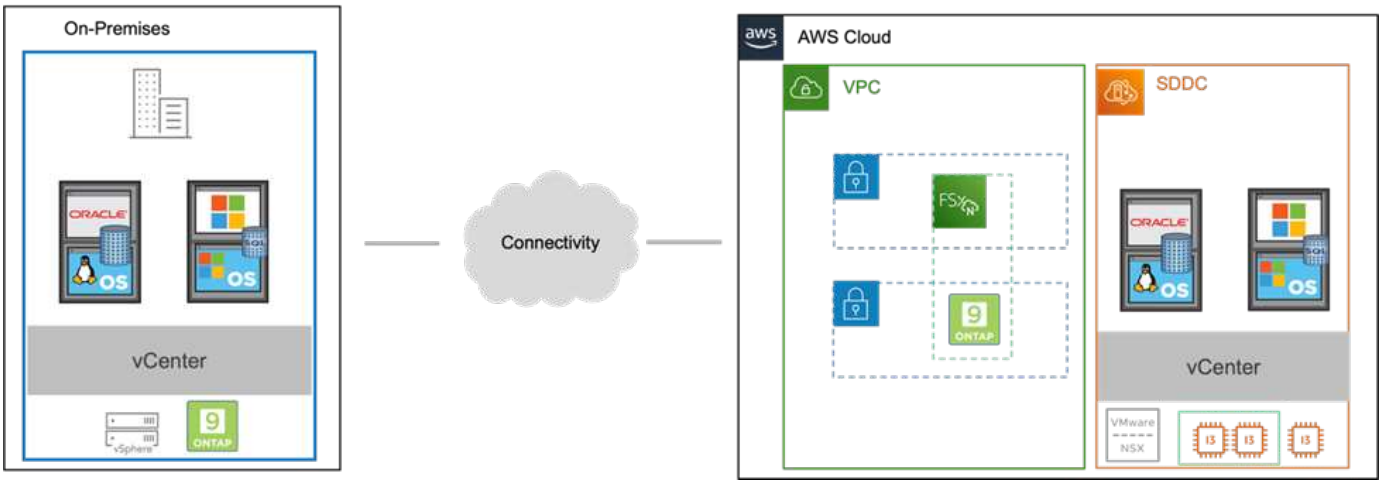
TR-4931：使用 **VMware Cloud on Amazon Web Services** 和 **Guest Connect** 進行災難復原

經過驗證的災難復原 (DR) 環境和計劃對於組織至關重要，以確保在發生重大中斷時能夠快速恢復關鍵業務應用程式。該解決方案專注於演示 DR 用例，重點關注 VMware 和NetApp技術，包括本地和 AWS 上的 VMware Cloud。

概況

NetApp與 VMware 的整合歷史悠久，數以萬計的客戶選擇NetApp作為其虛擬化環境的儲存合作夥伴，就證明了這一點。這種整合延續了雲端中的客戶連接選項以及最近與 NFS 資料儲存的整合。該解決方案專注於通常稱為客戶連接儲存的用例。

在來賓連接儲存中，來賓 VMDK 部署在 VMware 配置的資料儲存體上，應用程式資料存放在 iSCSI 或 NFS 上並直接對應到 VM。 Oracle 和 MS SQL 應用程式用於示範 DR 場景，如下圖所示。



假設、先決條件和組件概述

在部署此解決方案之前，請查看元件概述、部署此解決方案所需的先決條件以及記錄此解決方案時所做的假設。

"DR 解決方案需求、先決條件與規劃"

使用**SnapCenter**執行災難復原

在此解決方案中， SnapCenter為 SQL Server 和 Oracle 應用程式資料提供應用程式一致的快照。此配置與SnapMirror技術結合，可在我們的內部AFF和 FSx ONTAP叢集之間提供高速資料複製。此外，Veeam Backup & Replication 為我們的虛擬機器提供備份和復原功能。

在本節中，我們介紹SnapCenter、 SnapMirror和 Veeam 的備份和復原配置。

以下部分介紹在輔助站點完成故障轉移所需的設定和步驟：

配置**SnapMirror**關係和保留計劃

SnapCenter可以更新主儲存系統 (主 > 鏡像) 和二級儲存系統 (主 > 保險庫) 內的SnapMirror關係，以實現長期存檔和保留。為此，您必須使用SnapMirror在目標磁碟區和來源磁碟區之間建立並初始化資料複製關係。

來源 ONTAP 系統和目標ONTAP系統必須位於使用 Amazon VPC 對等連線、傳輸閘道、AWS Direct Connect 或 AWS VPN 進行對等連線的網路中。

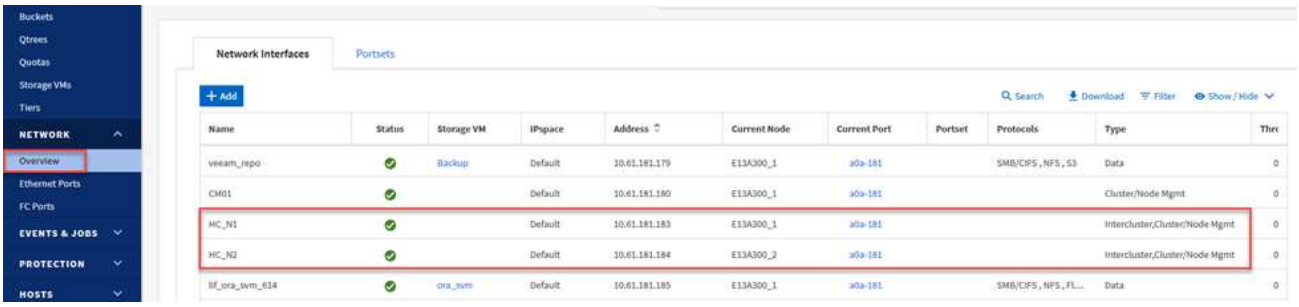
在本機ONTAP系統和 FSx ONTAP之間設定SnapMirror關係需要執行下列步驟：

請參閱 "FSx ONTAP – ONTAP使用者指南"有關使用 FSx 建立SnapMirror關係的詳細資訊。

▼ 記錄來源和目標集群間邏輯接口

對於位於本機的來源ONTAP系統，您可以從系統管理員或 CLI 檢索叢集間 LIF 資訊。

1. 在ONTAP系統管理員中，導覽至網路概覽頁面並擷取配置為與安裝了 FSx 的 AWS VPC 通訊的類型：叢集間的 IP 位址。



2. 若要擷取 FSx 的叢集間 IP 位址，請登入 CLI 並執行下列命令：

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

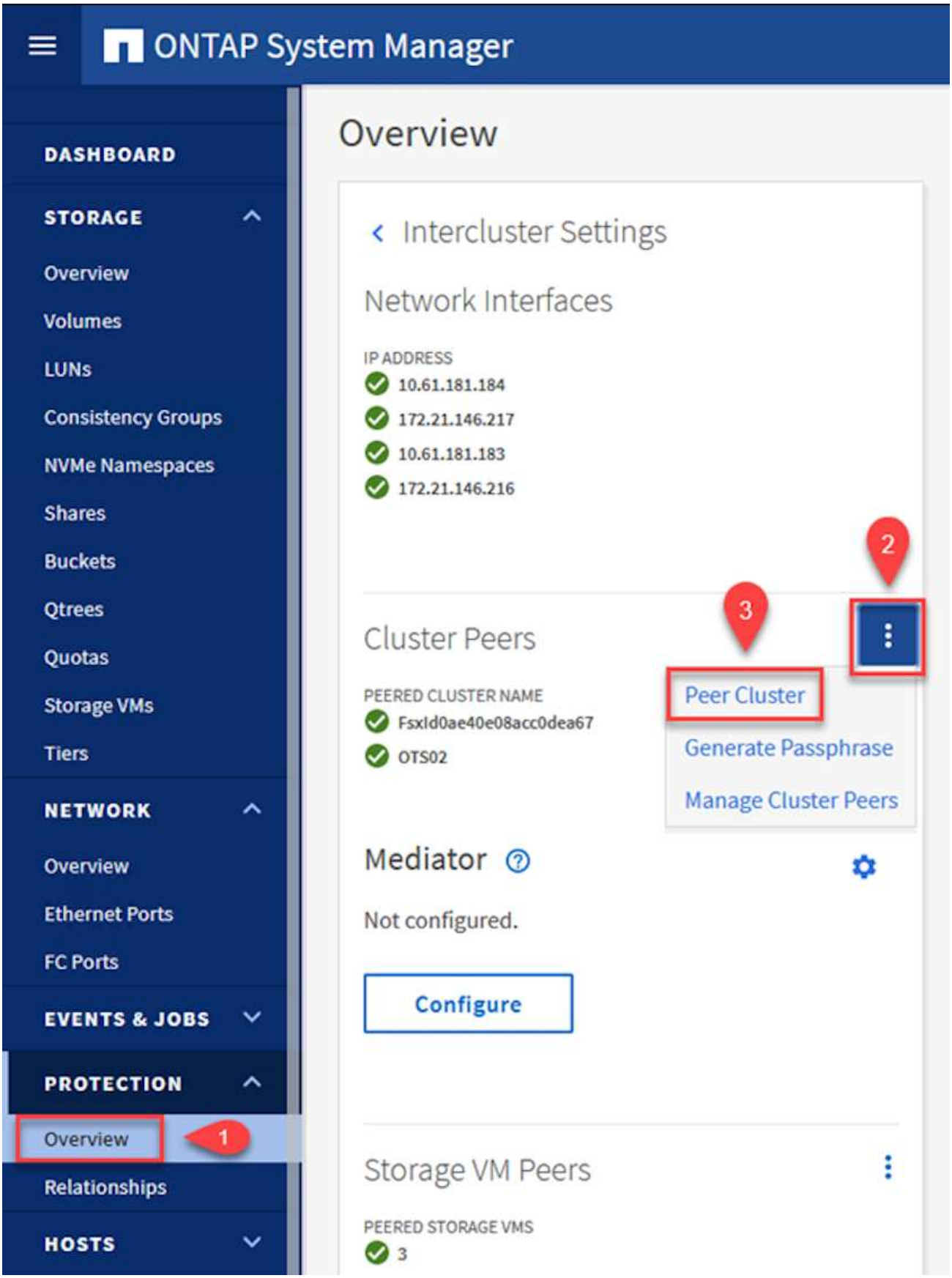
▼ 在**ONTAP**和 **FSx** 之間建立叢集對等連接

若要在ONTAP叢集之間建立叢集對等連接，必須在另一個對等叢集中確認在啟動ONTAP叢集中輸入的唯一密碼。

1. 使用以下方式在目標 FSx 叢集上設定對等連接 `cluster peer create`命令。出現提示時，請輸入稍後在來源叢集上使用的唯一密碼來完成建立程序。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. 在來源叢集中，您可以使用ONTAP系統管理員或 CLI 建立叢集對等關係。從ONTAP系統管理員中，導覽至“保護”>“概覽”，然後選擇“對等叢集”。

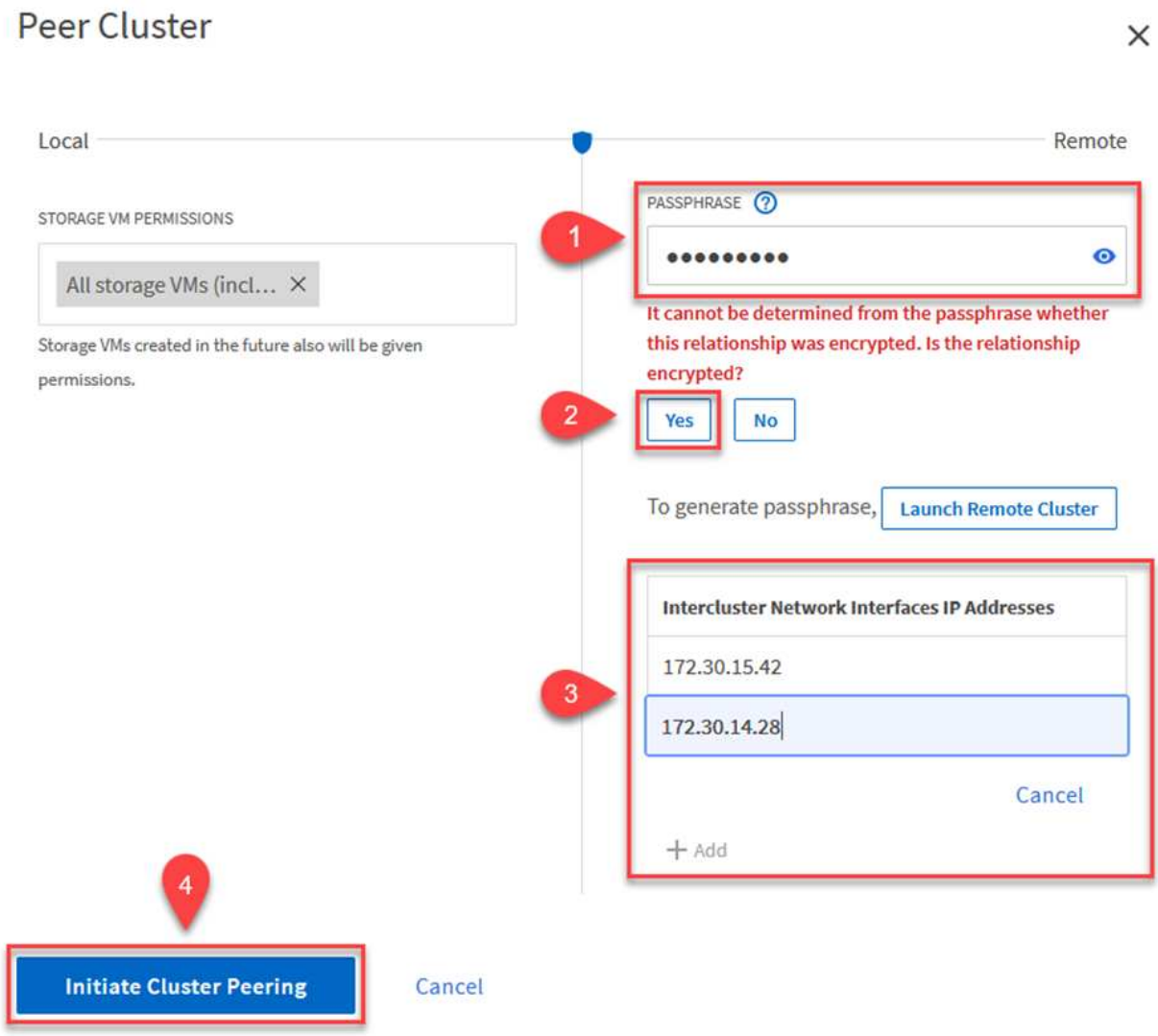


3. 在對等集群對話框中，填寫所需資訊：
   a. 輸入用於在目標 FSx 叢集上建立對等叢集關係的密碼。

b. 選擇 `Yes`建立加密關係。

c. 輸入目標 FSx 叢集的群集間 LIF IP 位址。

d. 按一下“啟動叢集對等”以完成該過程。



4. 使用下列命令從 FSx 叢集驗證叢集對等關係的狀態：

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

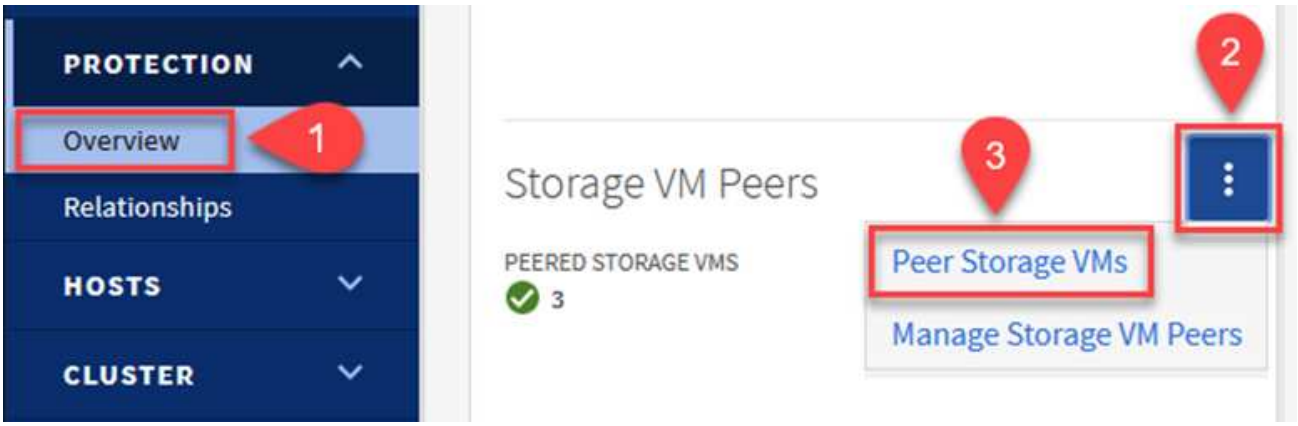
▼ 建立 **SVM** 對等關係

下一步是在包含將處於SnapMirror關係中的磁碟區的目標儲存虛擬機器和來源儲存虛擬機器之間建立 SVM 關係。

1. 從來源 FSx 集群，使用 CLI 中的下列命令建立 SVM 對等關係：

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup
-peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 從來源ONTAP集群，使用ONTAP系統管理器或 CLI 接受對等關係。
3. 從ONTAP系統管理員中，前往“保護”>“概覽”，然後選擇“儲存虛擬機器對等體”下的“對等儲存虛擬機器”。



4. 在對等儲存虛擬機器的對話方塊中，填寫必填欄位：
   - 源儲存虛擬機
   - 目標集群
   - 目標儲存虛擬機



5. 按一下「對等儲存虛擬機器」以完成 SVM 對等連線程序。

▼ 建立快照保留策略

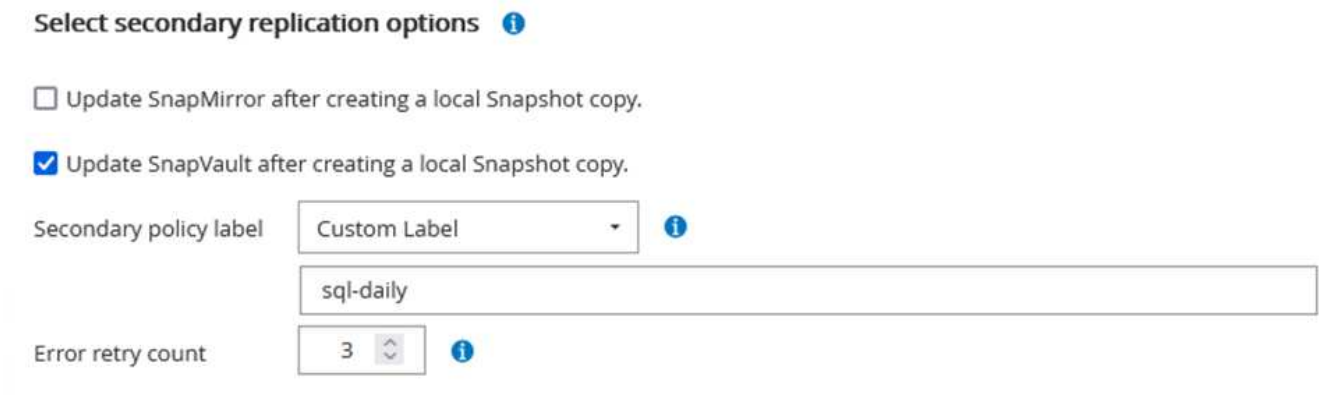
SnapCenter管理主儲存系統上作為快照副本存在的備份的保留計畫。這是在SnapCenter中建立策略時建立的。 SnapCenter不管理保留在二級儲存系統上的備份的保留策略。這些策略透過在輔助 FSx 叢集上建立

的SnapMirror策略單獨進行管理，並與與來源磁碟區具有SnapMirror關係的目標磁碟區相關聯。

建立SnapCenter策略時，您可以選擇指定一個輔助原則標籤，該標籤將會新增至執行SnapCenter備份時產生的每個快照的SnapMirror標籤。

在二級儲存上，這些標籤與目標磁碟區相關的策略規則相匹配，以強制保留快照。

以下範例顯示了一個SnapMirror標籤，該標籤存在於作為用於 SQL Server 資料庫和日誌卷的每日備份的政策的一部分所產生的所有快照上。



有關為 SQL Server 資料庫建立SnapCenter策略的更多信息，請參閱 "SnapCenter文檔"。

您必須先建立一個SnapMirror策略，其中包含規定要保留的快照副本數量的規則。

1. 在 FSx 叢集上建立SnapMirror策略。

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. 為具有與SnapCenter政策中指定的輔助策略標籤相符的SnapMirror標籤的政策新增規則。

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

以下腳本提供了可以新增到策略的規則範例：

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

為每個SnapMirror標籤和要保留的快照數量（保留期）建立附加規則。

▼ 建立目標磁碟區

若要在 FSx 上建立將作為來源磁碟區快照副本接收者的目標卷，請在 FSx ONTAP上執行下列命令：

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

▼ 在來源磁碟區和目標磁碟區之間建立**SnapMirror**關係

若要在來源磁碟區和目標磁碟區之間建立SnapMirror關係，請在 FSx ONTAP上執行下列命令：

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

▼ 初始化**SnapMirror**關係

初始化SnapMirror關係。此程序啟動從來源磁碟區產生的新快照並將其複製到目標磁碟區。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

在本機部署和設定 **Windows SnapCenter**伺服器。

▼ 在本機上部署 **Windows SnapCenter**伺服器

此解決方案使用NetApp SnapCenter對 SQL Server 和 Oracle 資料庫進行應用程式一致性備份。與 Veeam Backup & Replication 結合使用來備份虛擬機器 VMDK，這為本地和基於雲端的資料中心提供了全面的災難復原解決方案。

SnapCenter software可從NetApp支援網站取得，並可安裝在網域或工作群組中的 Microsoft Windows 系統上。詳細的規劃指南和安裝說明可以在 "NetApp文件中心"。

SnapCenter software可從以下網址取得 "此連結"。

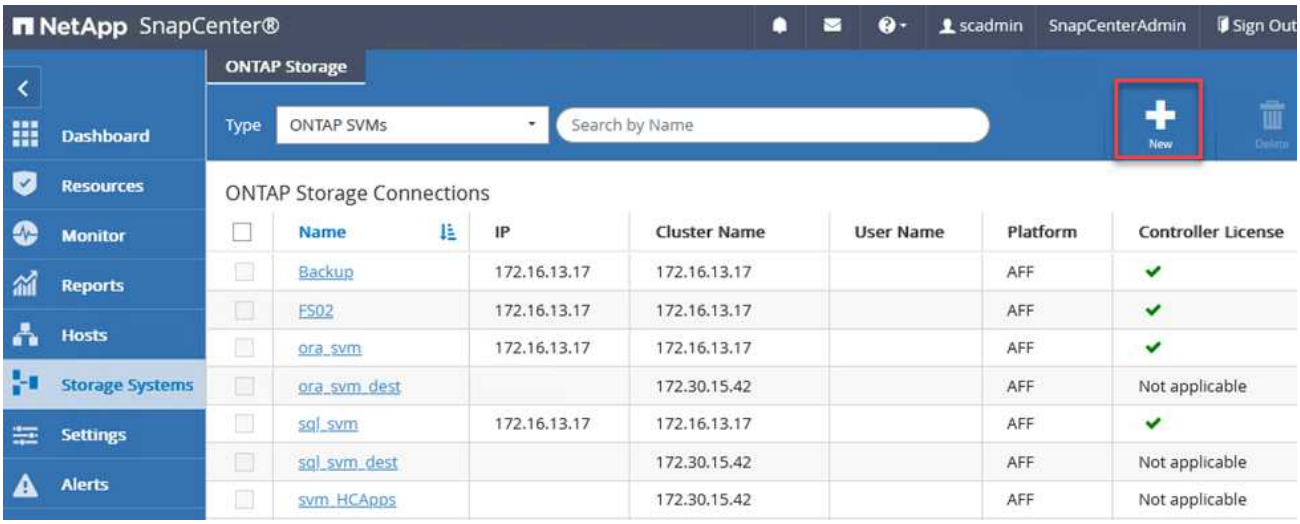
安裝完成後，您可以使用 *https://Virtual_Cluster_IP_or_FQDN:8146* 從 Web 瀏覽器存取SnapCenter控制台。

登入控制台後，您必須設定SnapCenter以備份 SQL Server 和 Oracle 資料庫。

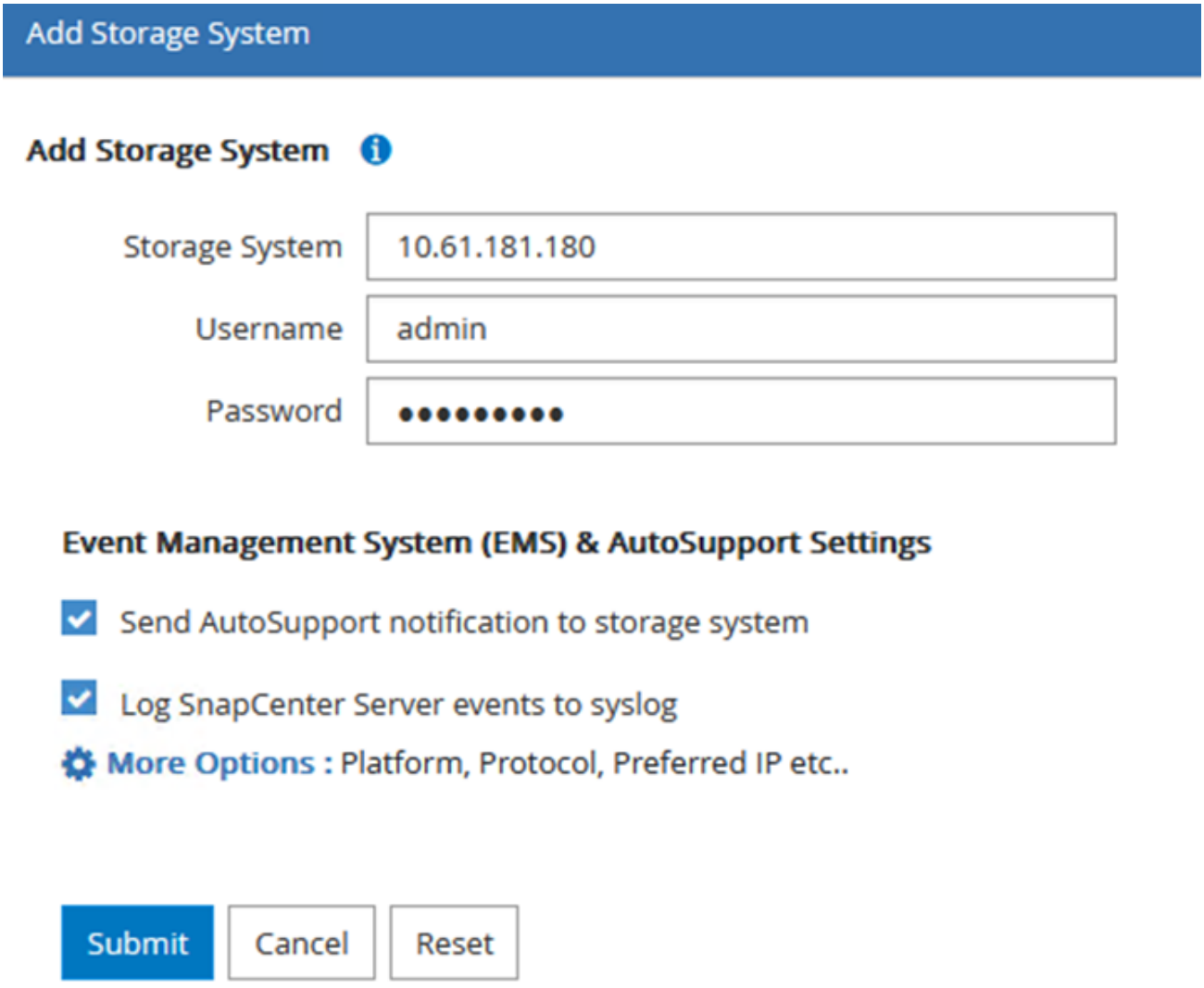
▼ 為**SnapCenter**新增儲存控制器

若要將儲存控制器新增至SnapCenter，請完成下列步驟：

1. 從左側選單中，選擇“儲存系統”，然後按一下“新建”開始將儲存控制器新增至SnapCenter的過程。

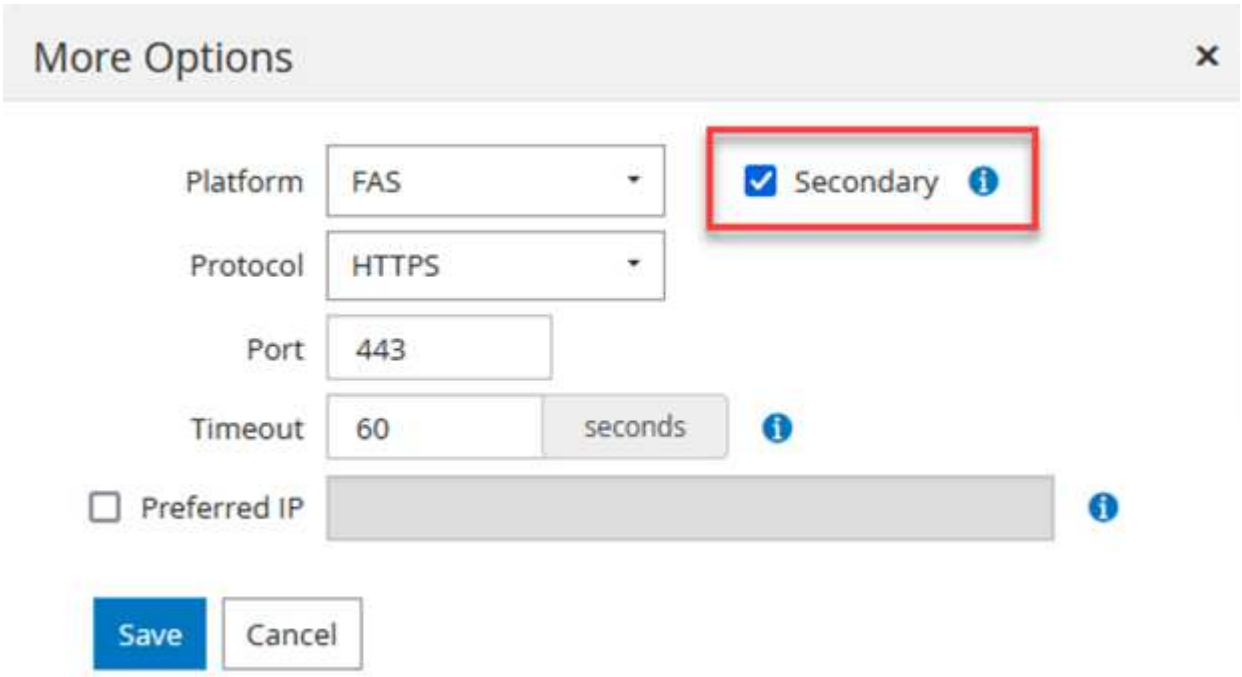


2. 在新增儲存系統對話方塊中，新增本機ONTAP叢集的管理 IP 位址以及使用者名稱和密碼。然後點擊“提交”開始發現儲存系統。



3. 重複此程序將 FSx ONTAP系統新增至SnapCenter。在這種情況下，選擇“新增儲存系統”視窗底部的“更多選項”，然後按一下“輔助”複選框，將 FSx 系統指定為使用SnapMirror副本或我們的主備份快照更新的輔

助儲存系統。

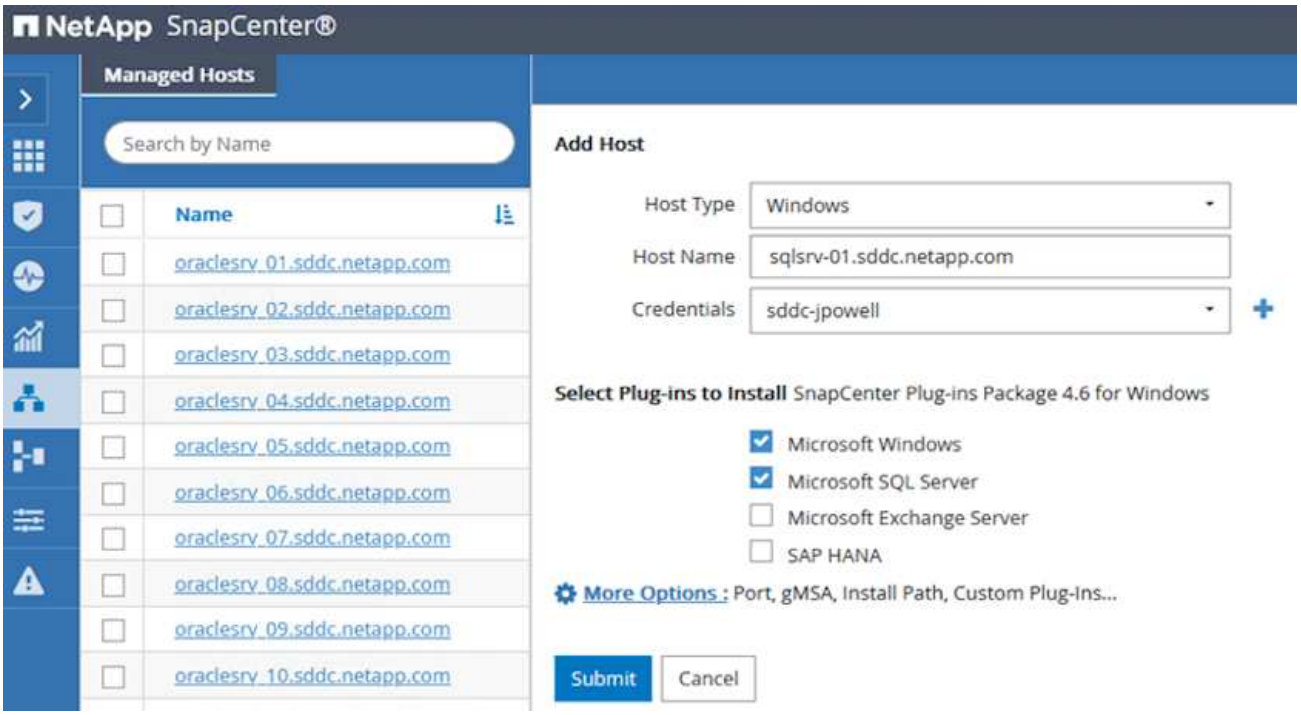


有關向SnapCenter添加儲存系統的更多信息，請參閱以下文件： "此連結" 。

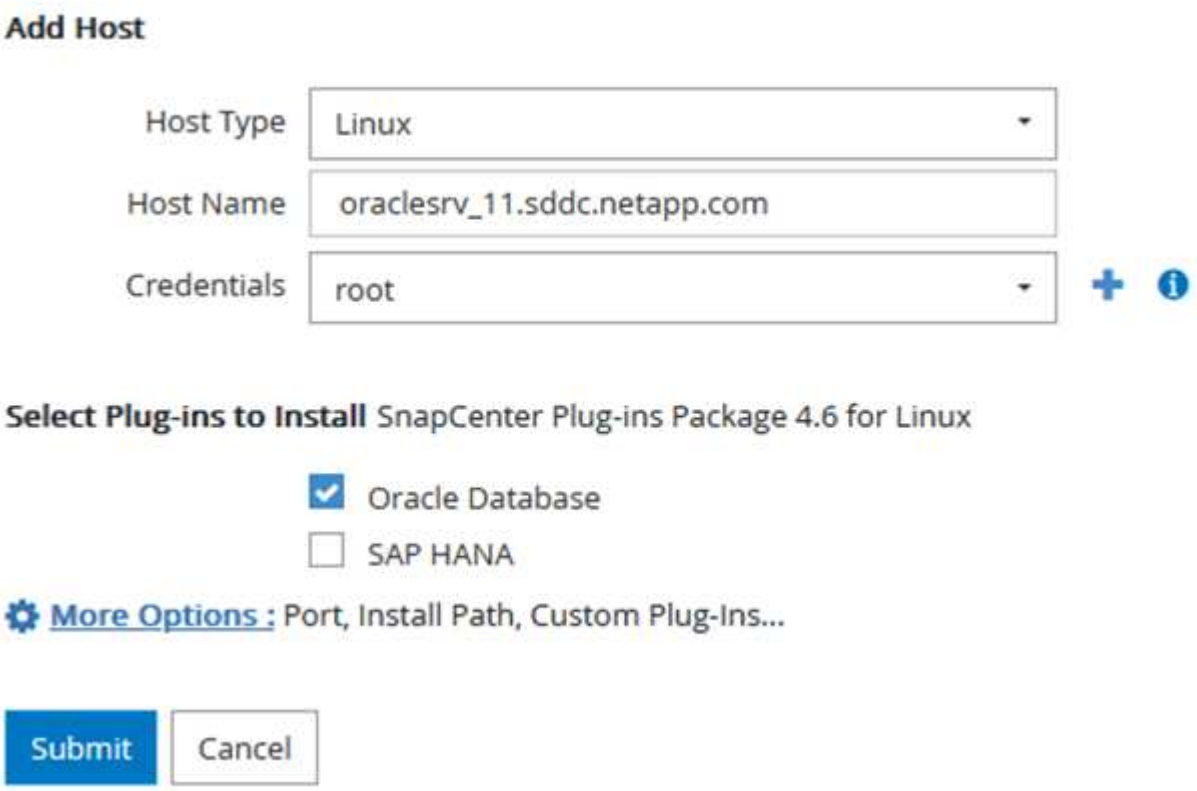
▼ 將主機加入**SnapCenter**

下一步是將主機應用程式伺服器新增至SnapCenter。 SQL Server 和 Oracle 的過程類似。

1. 從左側選單中，選擇“主機”，然後按一下“新增”以開始向SnapCenter新增儲存控制器的過程。
2. 在新增主機視窗中，新增主機類型、主機名稱和主機系統憑證。選擇插件類型。對於 SQL Server，選擇 Microsoft Windows 和 Microsoft SQL Server 外掛程式。



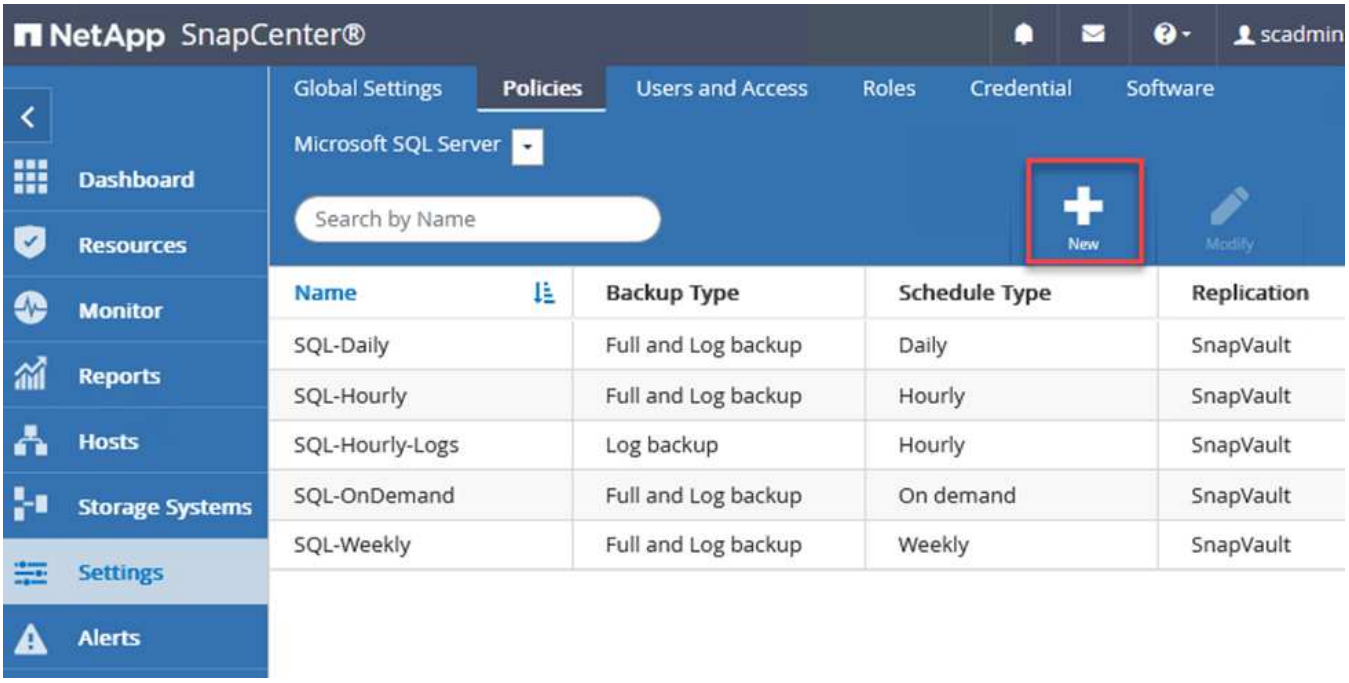
3. 對於 Oracle，請在「新增主機」對話方塊中填寫必填字段，並選取 Oracle 資料庫插件的核取方塊。然後按一下「提交」以開始發現程序並將主機新增至SnapCenter。



▼ 建立**SnapCenter**策略

策略制定了備份工作需要遵循的具體規則。它們包括但不限於備份計劃、複製類型以及SnapCenter如何處理備份和截斷交易日誌。

您可以在SnapCenter Web 用戶端的「設定」部分存取原則。



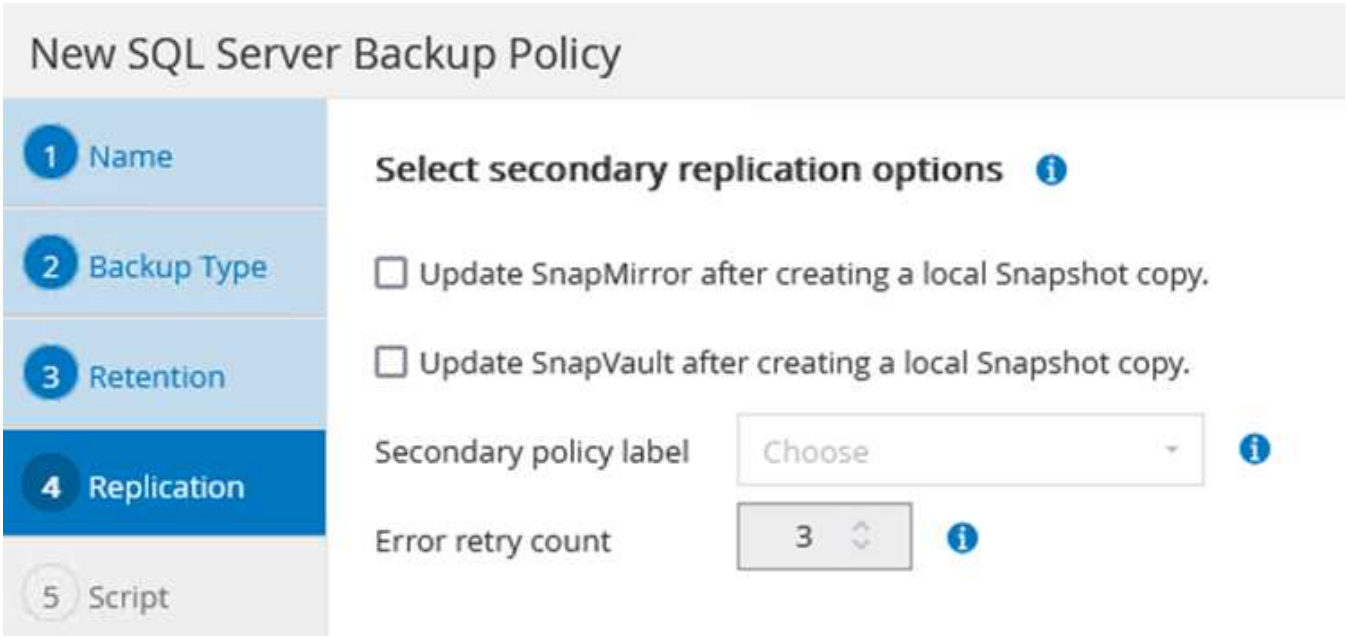
有關建立 SQL Server 備份策略的完整信息，請參閱 "SnapCenter文檔"。

有關建立 Oracle 備份策略的完整信息，請參閱 "SnapCenter文檔"。

筆記：

- 在您完成策略建立精靈的過程中，請特別注意複製部分。在本節中，您將規定在備份過程中要取得的輔助SnapMirror副本的類型。
- 「建立本機 Snapshot 副本後更新SnapMirror 」設定是指當位於同一叢集上的兩個儲存虛擬機器之間存在SnapMirror關係時更新該關係。
- 「建立本機 SnapShot 副本後更新SnapVault 」設定用於更新兩個獨立叢集之間以及本機ONTAP系統與Cloud Volumes ONTAP或 FSx ONTAP之間存在的SnapMirror關係。

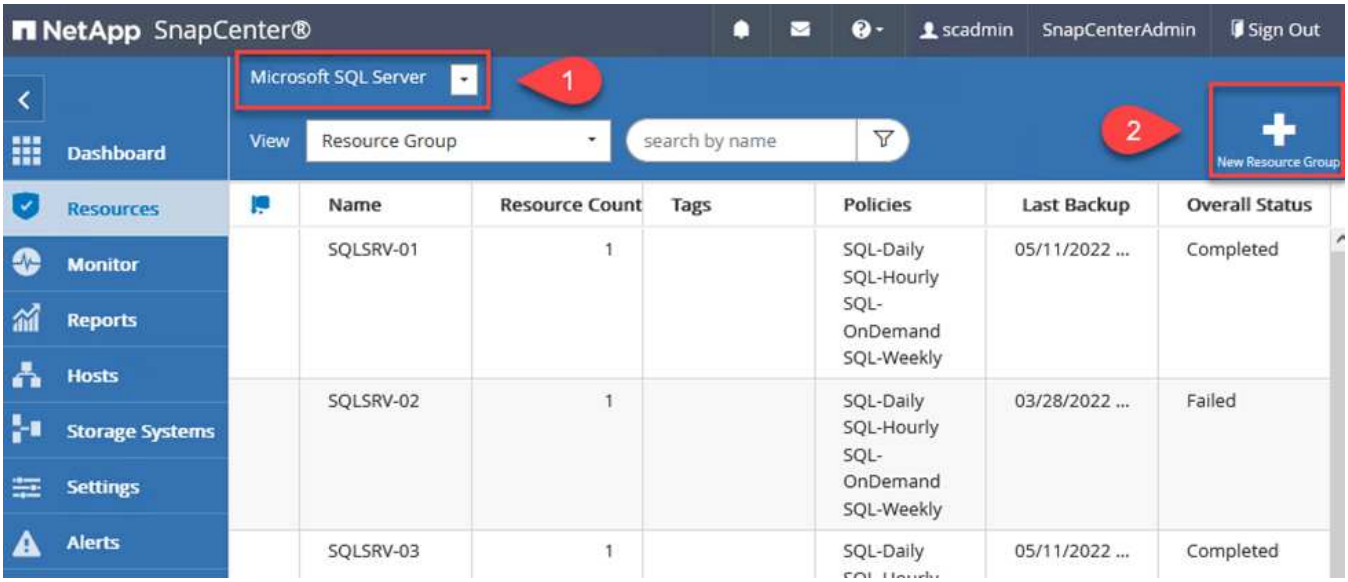
下圖顯示了上述選項以及它們在備份策略精靈中的外觀。



▼ 建立**SnapCenter**資源組

資源組可讓您選擇要包含在備份中的資料庫資源以及這些資源遵循的策略。

1. 轉到左側選單中的資源部分。
2. 在視窗頂部，選擇要使用的資源類型（在本例中為 Microsoft SQL Server），然後按一下新資源群組。



SnapCenter文件涵蓋了為 SQL Server 和 Oracle 資料庫建立資源群組的逐步詳細資訊。

若要備份 SQL 資源，請依照 "此連結"。

若要備份 Oracle 資源，請依照 "此連結"。

部署並設定 **Veeam** 備份伺服器

該解決方案使用 Veeam Backup & Replication 軟體來備份我們的應用程式虛擬機，並使用 Veeam 橫向擴展備份儲存庫 (SOBR) 將備份副本存檔到 Amazon S3 儲存桶。在本解決方案中，Veeam 部署在 Windows 伺服器上。部署 Veeam 的具體指導，請參閱 "Veeam 幫助中心 技術文檔"。

▼ 配置 **Veeam** 橫向擴充備份儲存庫

部署並取得軟體授權後，您可以建立橫向擴充備份儲存庫 (SOBR) 作為備份作業的目標儲存。您還應該包含一個 S3 儲存桶作為異地 VM 資料的備份，以實現災難復原。

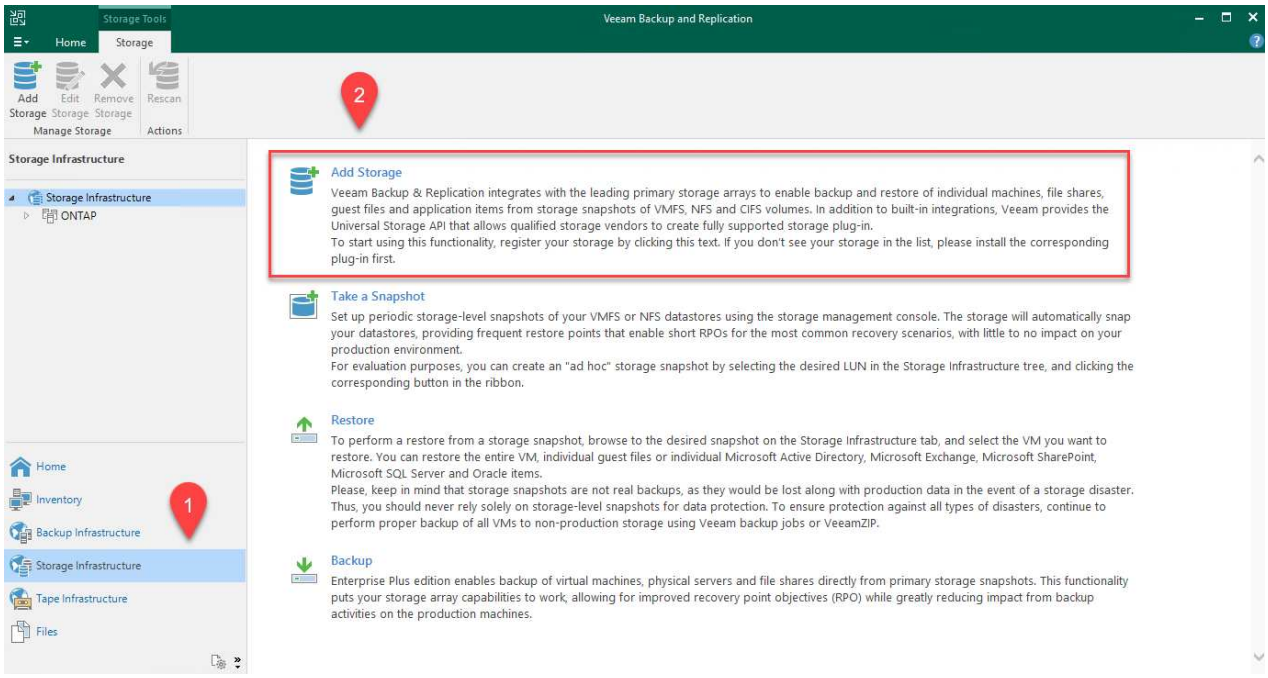
開始之前請參閱以下先決條件。

1. 在本機ONTAP系統上建立 SMB 檔案共享作為備份的目標儲存。
2. 建立一個 Amazon S3 儲存桶以包含在 SOBR 中。這是異地備份的儲存庫。

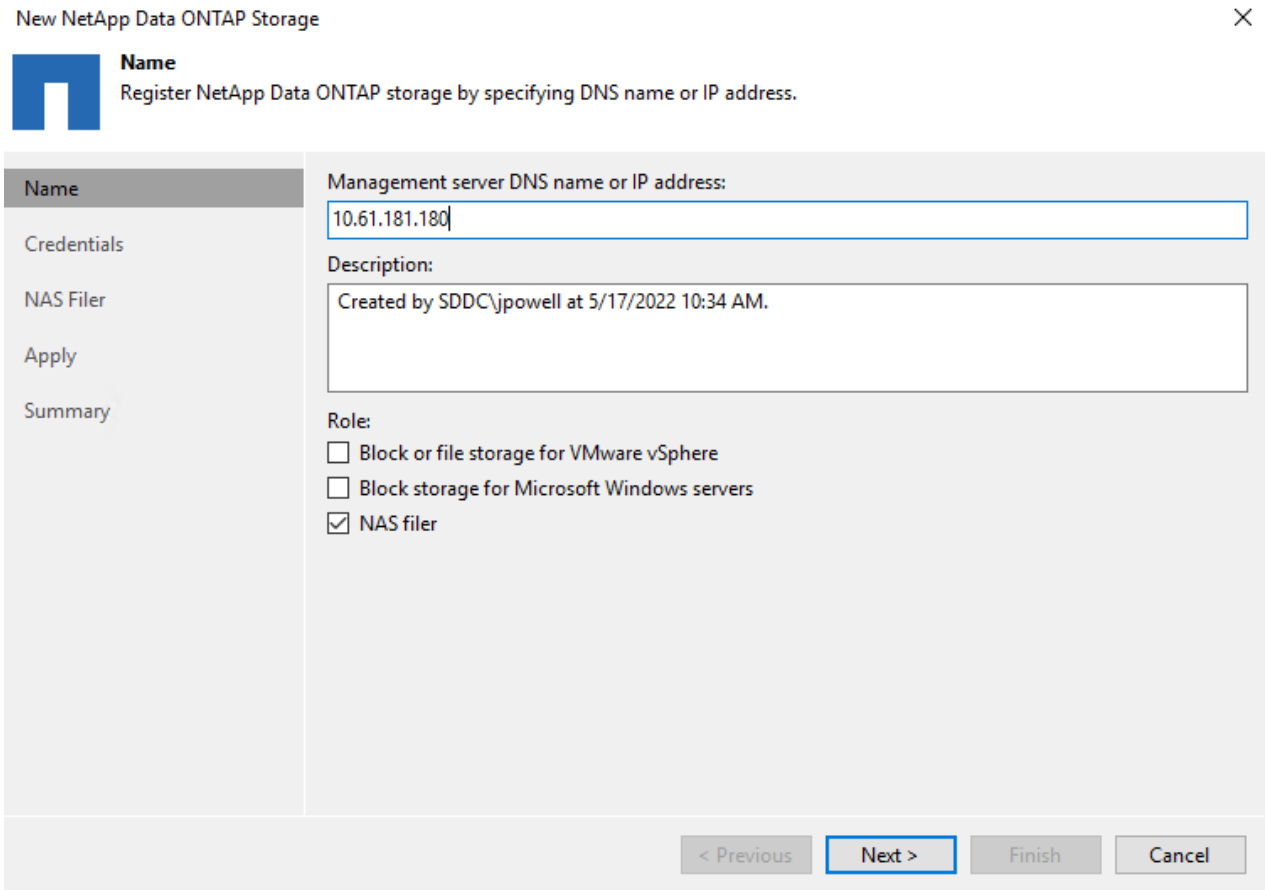
▼ 將**ONTAP**儲存加入到 **Veeam**

首先，在 Veeam 中新增ONTAP儲存叢集和相關的 SMB/NFS 檔案系統作為儲存基礎架構。

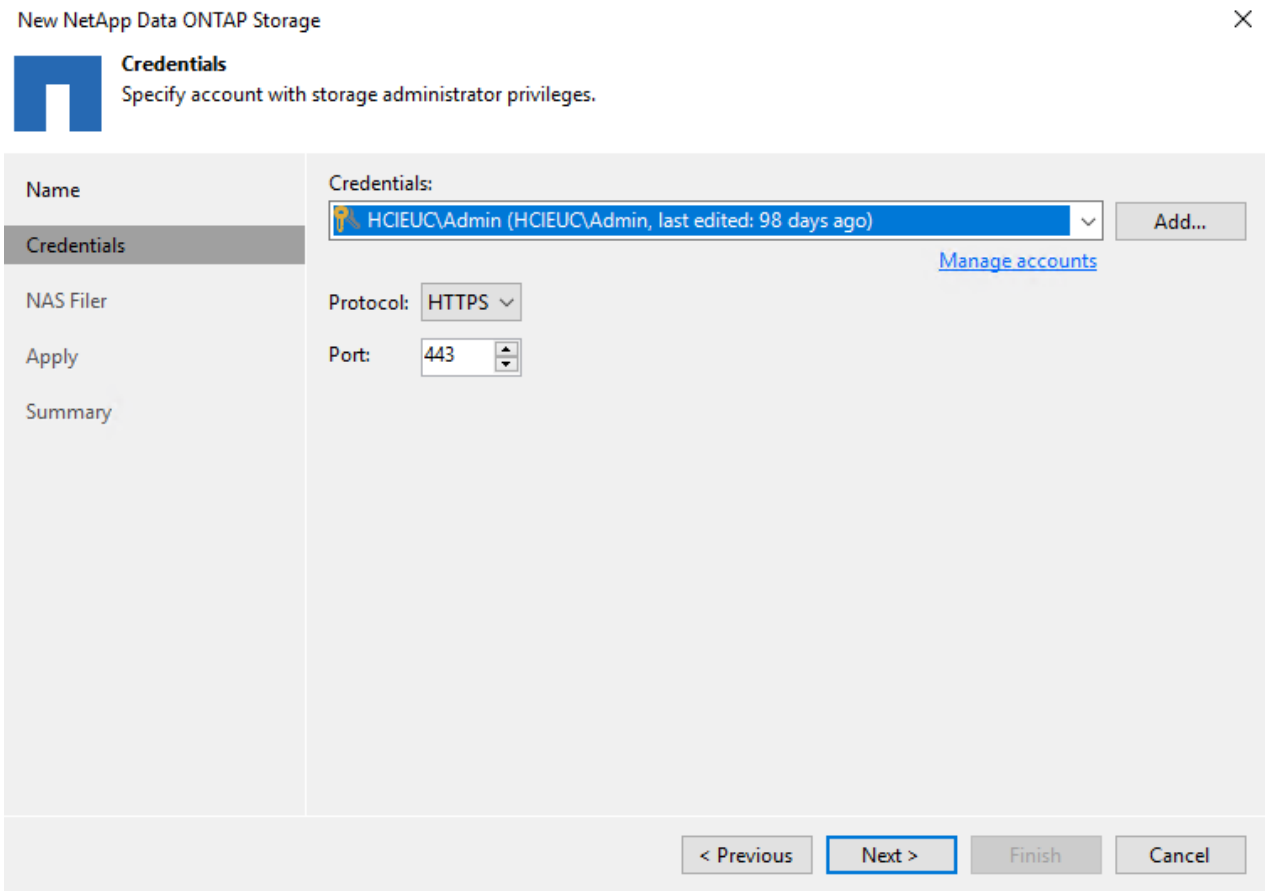
1. 開啟 Veeam 控制台並登入。導航至儲存基礎設施，然後選擇新增儲存。



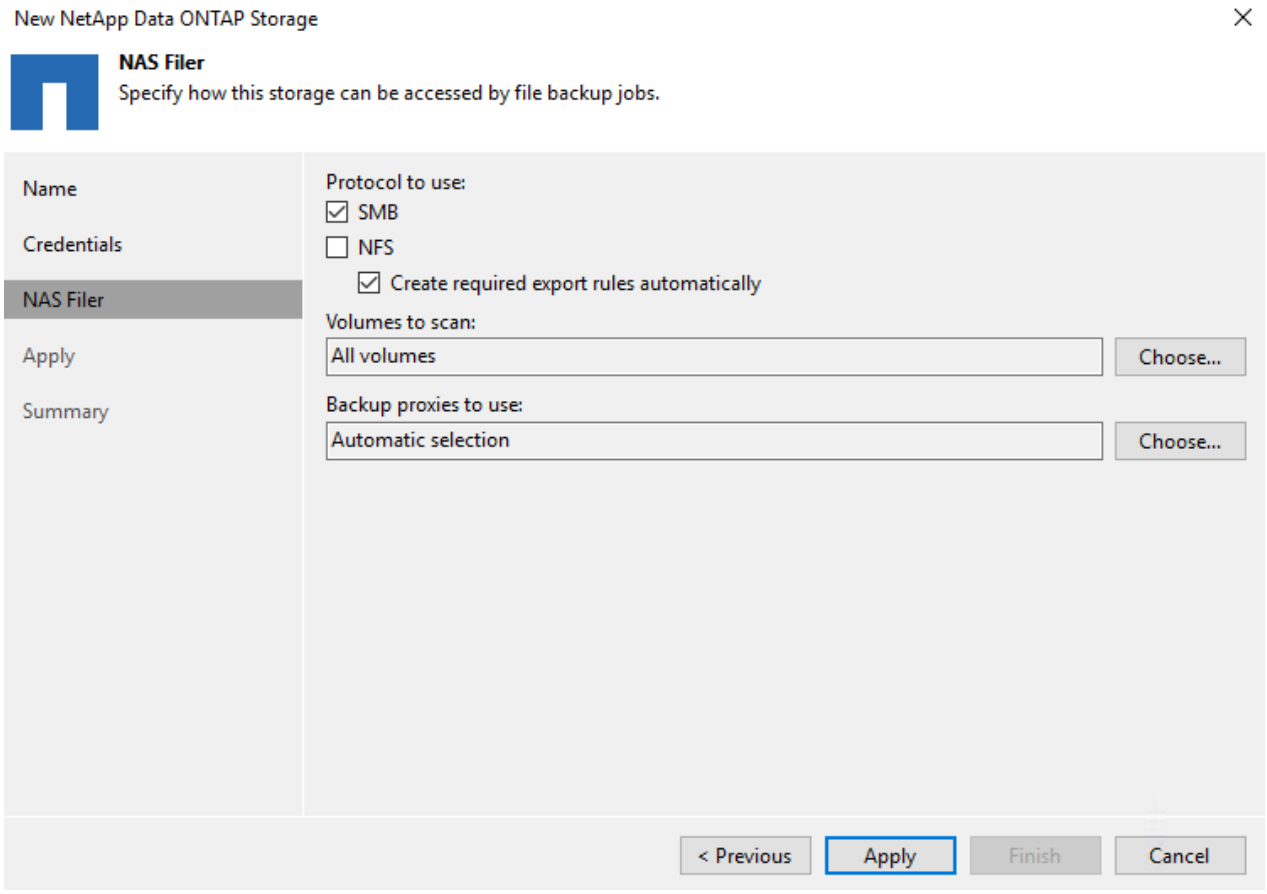
2. 在新增儲存精靈中，選擇NetApp作為儲存供應商，然後選擇Data ONTAP。
3. 輸入管理 IP 位址並選取 NAS Filer 方塊。按一下“下一步”。



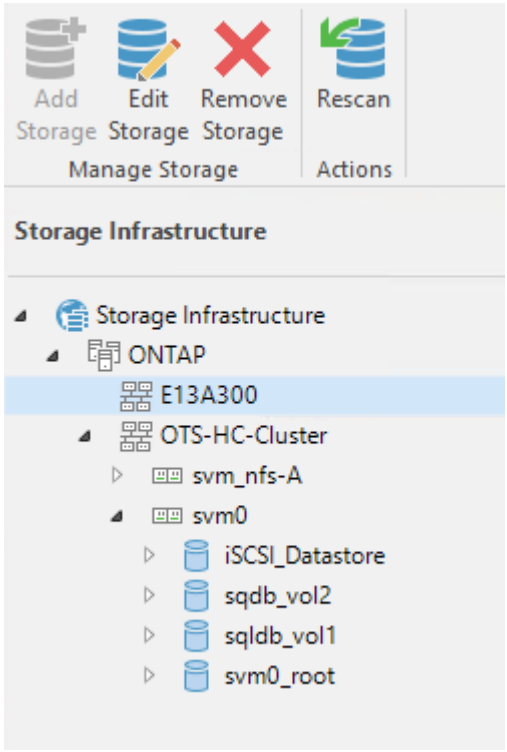
4. 新增您的憑證以存取ONTAP叢集。



5. 在 NAS Filer 頁面上，選擇要掃描的協議，然後選擇下一步。

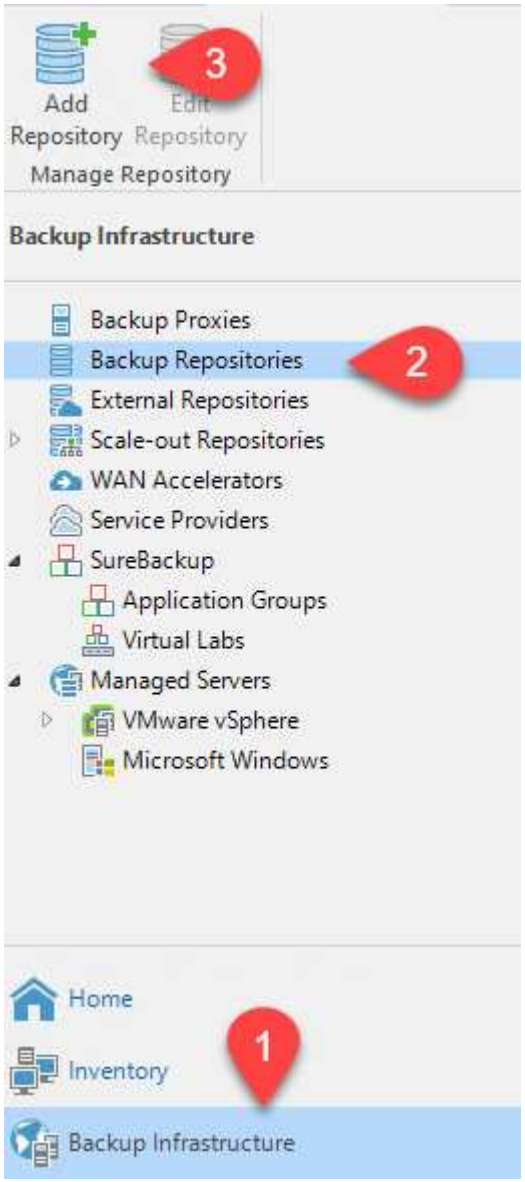


6. 完成精靈的「套用」和「摘要」頁面，然後按一下「完成」以開始儲存發現程序。掃描完成後，ONTAP叢集將與 NAS 檔案伺服器一起新增為可用資源。

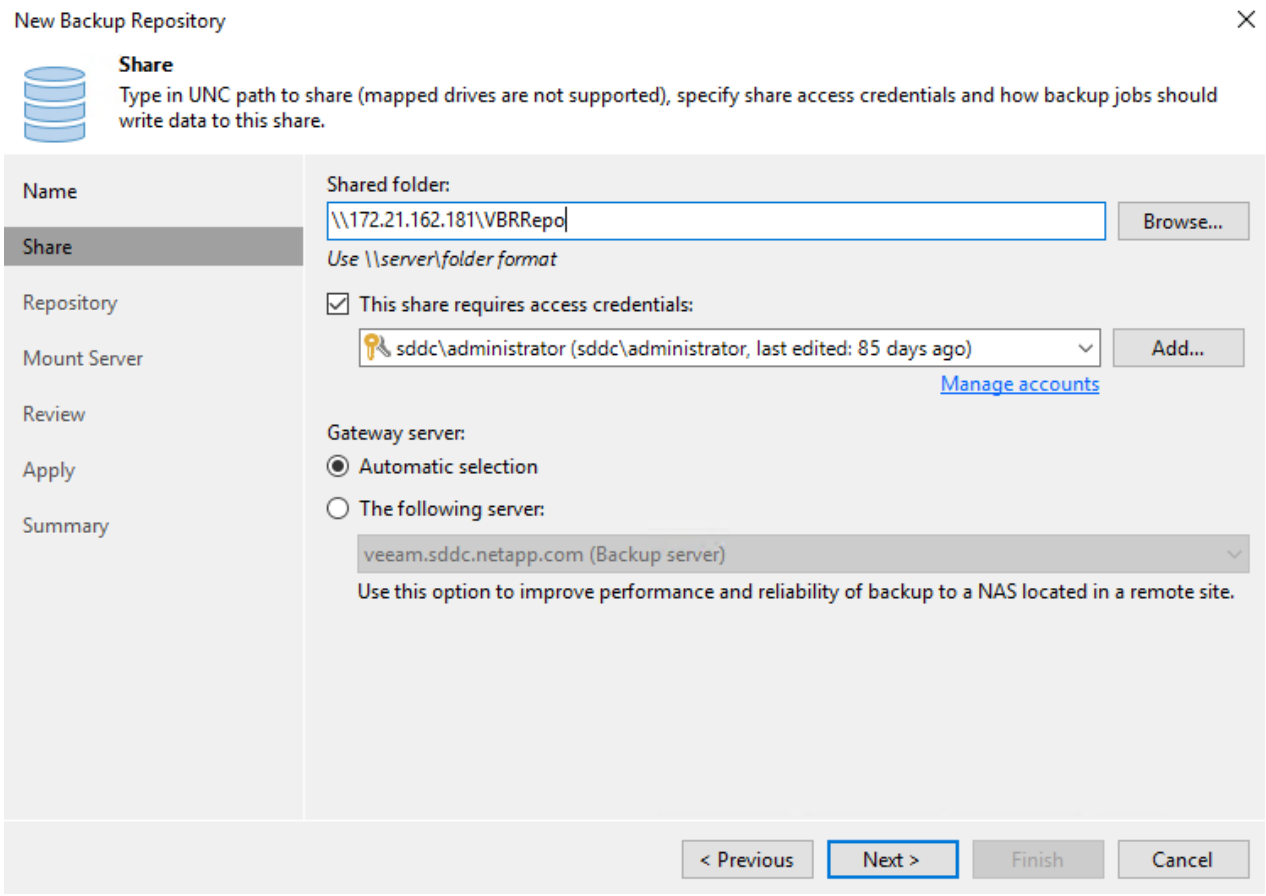


7. 使用新發現的 NAS 共用建立備份儲存庫。從備份基礎架構中，選擇備份儲存庫並點選新增儲存庫選單

項目。



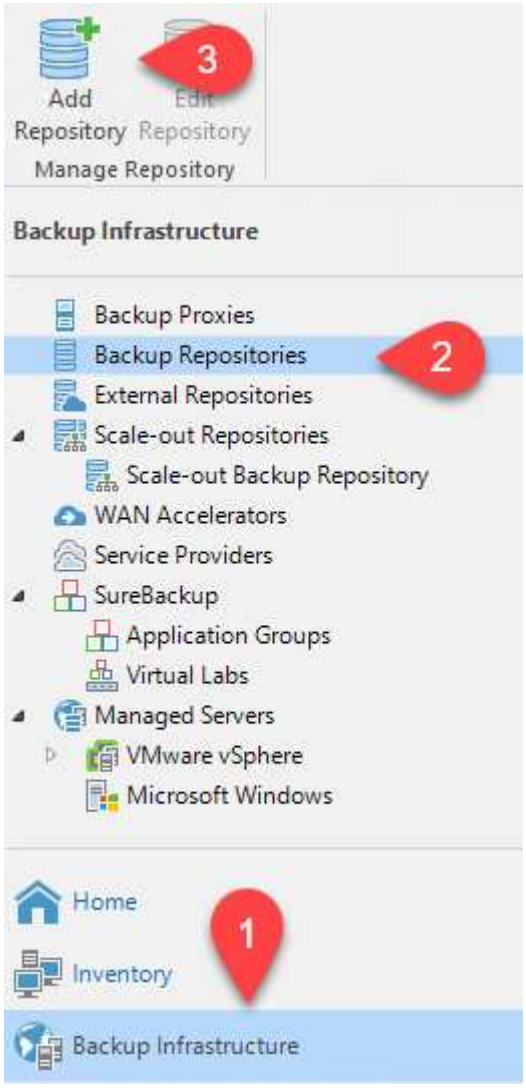
8. 請依照新備份儲存庫精靈中的所有步驟來建立儲存庫。有關建立 Veeam Backup 儲存庫的詳細信息，請參閱 "Veeam 文檔"。



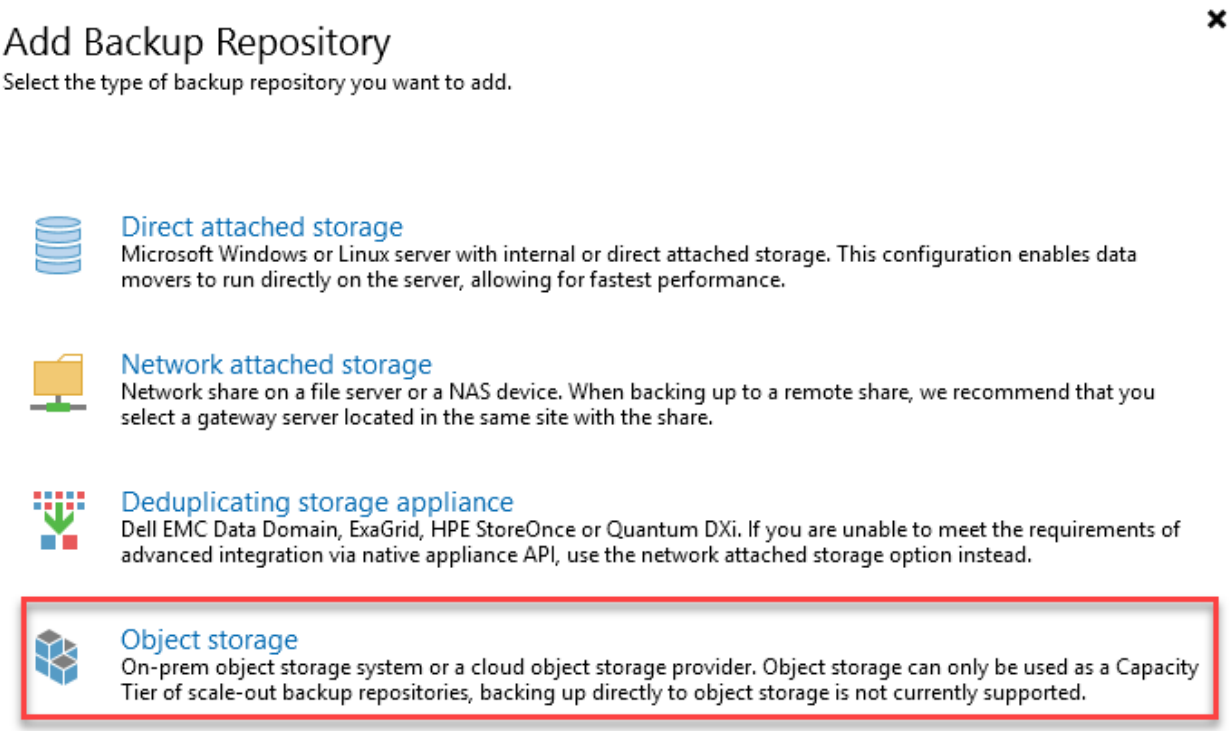
▼ 新增 **Amazon S3** 儲存桶作為備份儲存庫

下一步是新增 Amazon S3 儲存空間作為備份儲存庫。

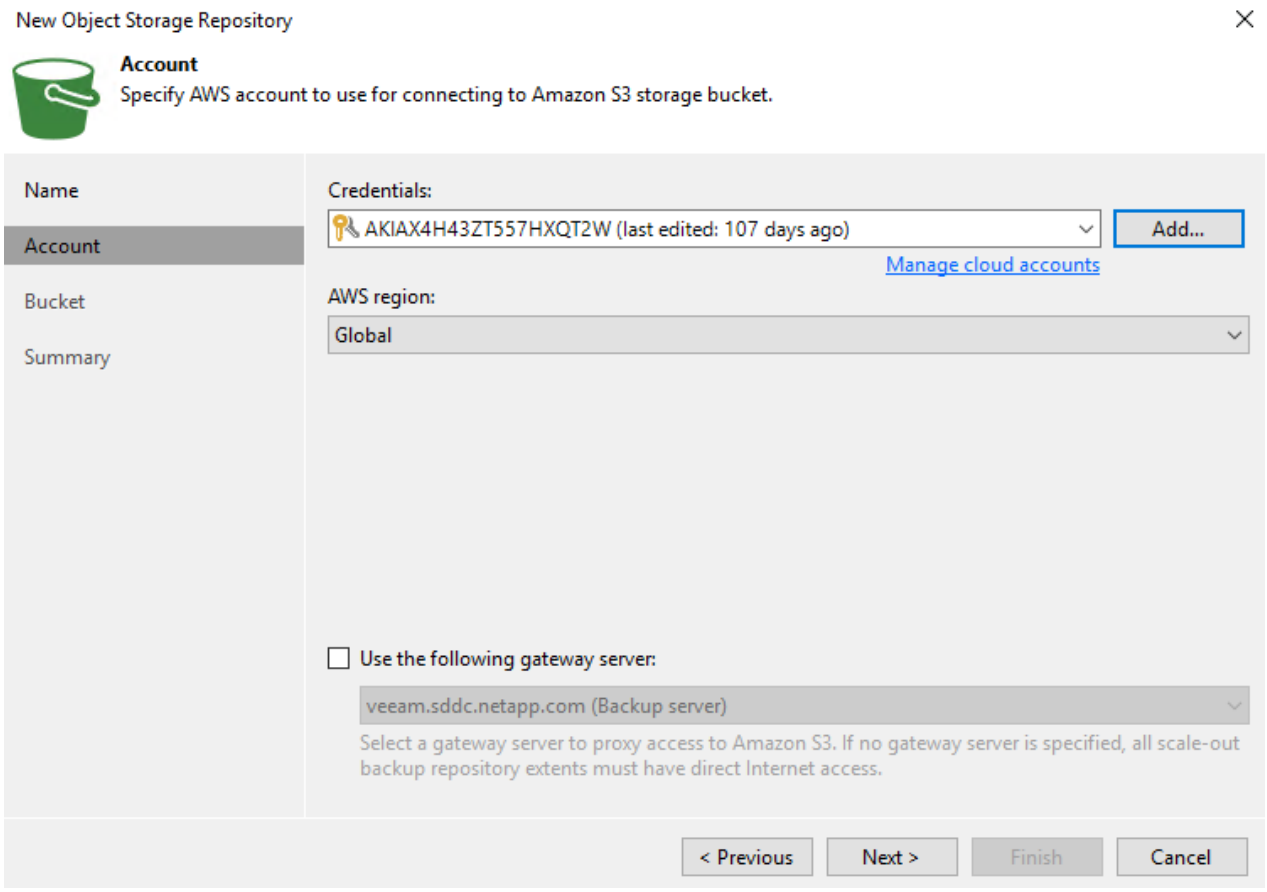
1. 導覽至備份基礎架構 > 備份儲存庫。按一下新增儲存庫。



2. 在新增備份儲存庫精靈中，選擇物件存儲，然後選擇 Amazon S3。這將啟動新物件儲存庫精靈。



3. 為您的物件儲存庫提供名稱，然後按一下下一步。
4. 在下一部分中，提供您的憑證。您需要一個 AWS 存取金鑰和金鑰。



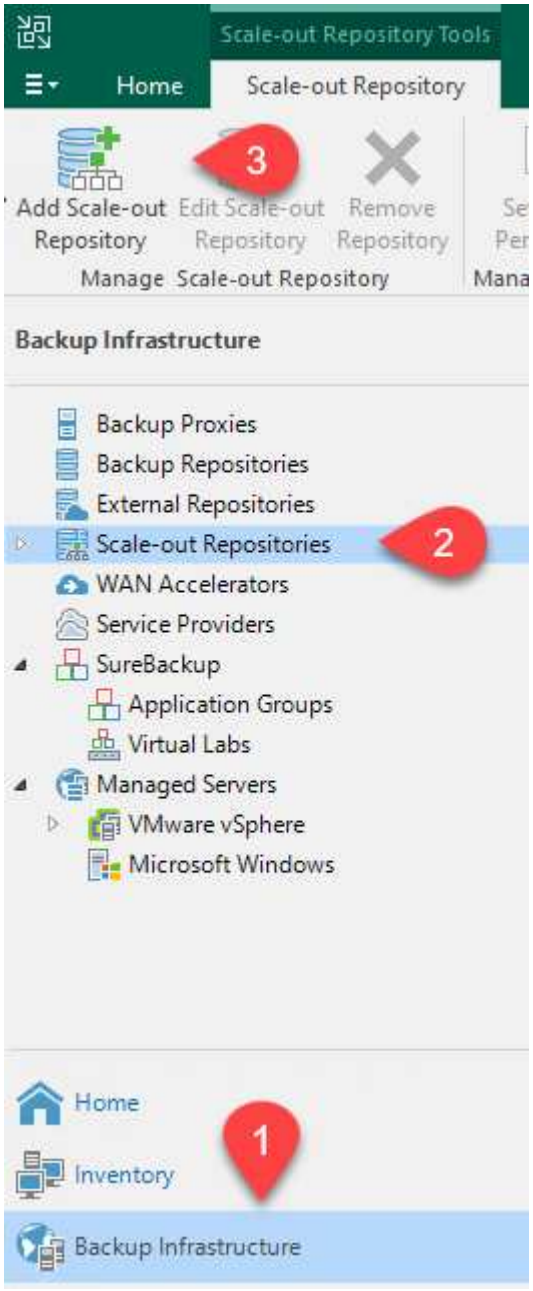
5. 載入 Amazon 配置後，選擇您的資料中心、儲存桶和資料夾，然後按一下「套用」。最後，按一下「

完成」關閉精靈。

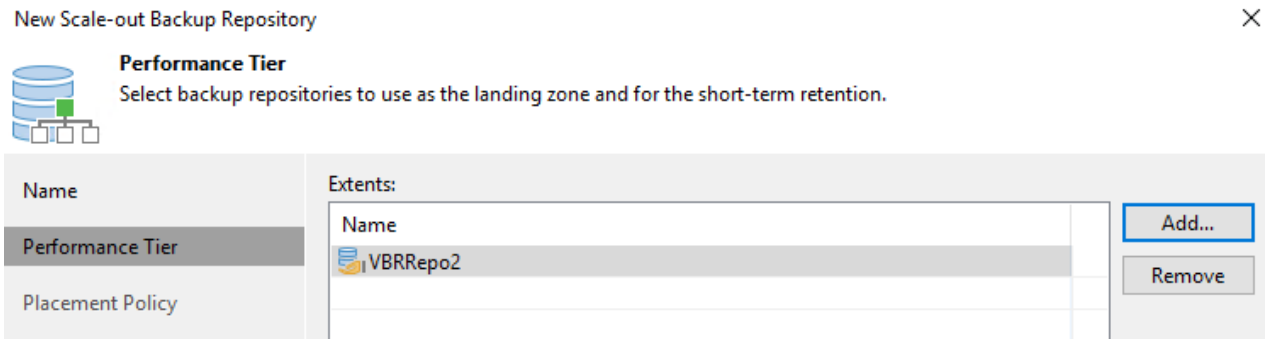
▼ 建立橫向擴充備份儲存庫

現在我們已經將儲存庫新增至 Veeam，我們可以建立 SOBR 來自動將備份副本分層到我們的異地 Amazon S3 物件儲存中，以實現災難復原。

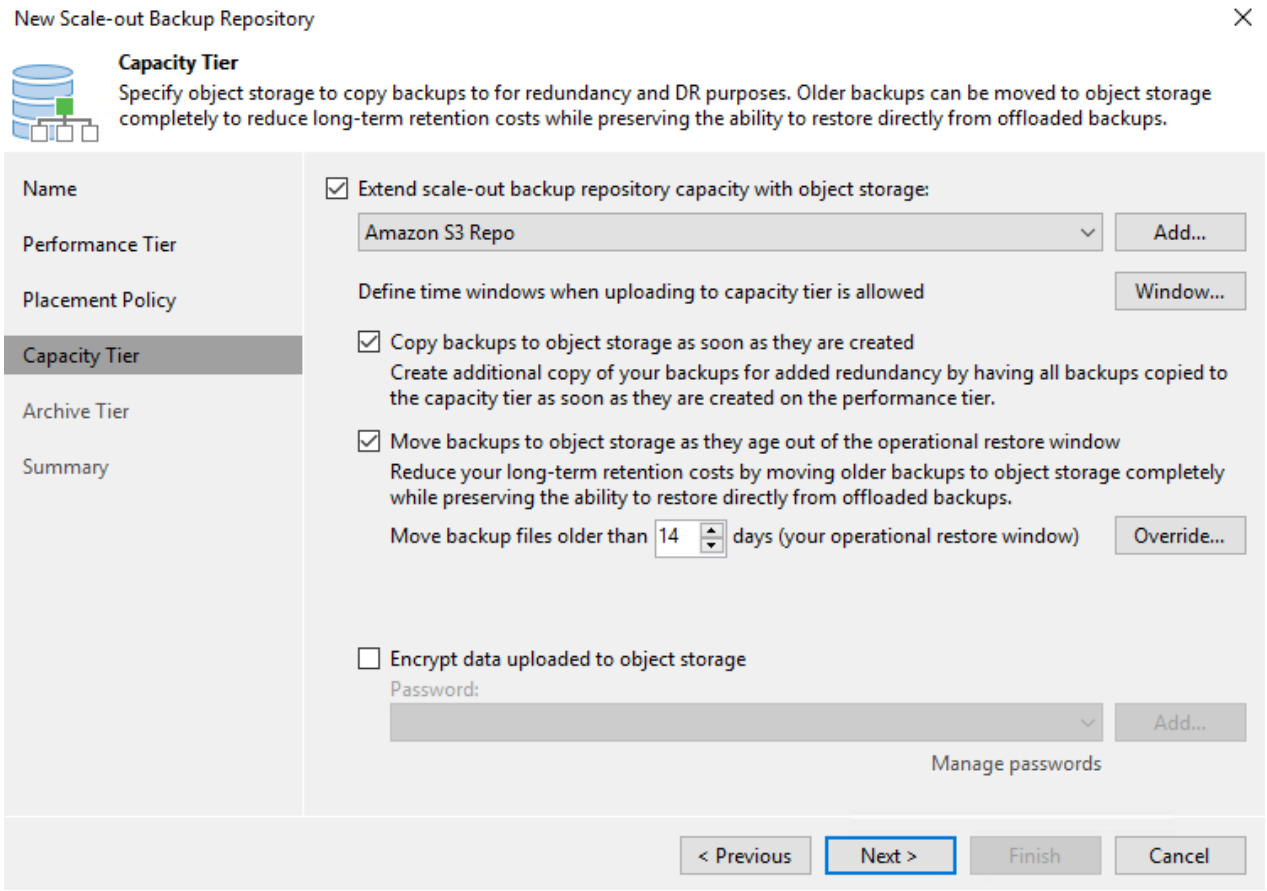
1. 從備份基礎架構中，選擇擴充儲存庫，然後按一下新增擴充儲存庫選單項目。



2. 在新的橫向擴充備份儲存庫中為 SOBR 提供一個名稱，然後按一下下一步。
3. 對於效能層，選擇包含位於本機ONTAP叢集上的 SMB 共用的備份儲存庫。



4. 對於放置策略，請根據您的要求選擇資料局部性或效能。選擇下一步。
5. 對於容量層，我們使用 Amazon S3 物件儲存來擴充 SOBR。為了實現災難恢復，請選擇“在創建備份後立即將其複製到物件儲存”，以確保及時交付我們的二次備份。



6. 最後，選擇「應用」和「完成」以完成 SOBR 的建立。

▼ 建立橫向擴充備份儲存庫作業

配置 Veeam 的最後一步是使用新建立的 SOBR 作為備份目標來建立備份作業。建立備份作業是任何儲存管理員的正常工作的一部分，我們在此不介紹詳細步驟。有關在 Veeam 中建立備份作業的更多完整信息，請參閱 "Veeam 幫助中心技術文檔"。

NetApp Backup and Recovery 工具與組態

若要將應用程式虛擬機器和資料庫磁碟區故障轉移到在 AWS 中執行的 VMware Cloud Volume 服務，您必須安裝並設定SnapCenter Server 和 Veeam Backup and Replication Server 的執行執行個體。故障轉移完成後，您

還必須設定這些工具以還原正常的備份作業，直到規劃並執行故障還原到內部資料中心。

▼ 部署輔助 **Windows SnapCenter**伺服器

SnapCenter Server 部署在 VMware Cloud SDDC 中，或安裝在與 VMware Cloud 環境具有網路連線的 VPC 中的 EC2 執行個體上。

SnapCenter software可從NetApp支援網站取得，並可安裝在網域或工作群組中的 Microsoft Windows 系統上。詳細的規劃指南和安裝說明可以在 "NetApp文件中心"。

您可以在以下位置找到SnapCenter software "此連結"。

▼ 設定輔助 **Windows SnapCenter**伺服器

若要執行鏡像到 FSx ONTAP 的應用程式資料還原，您必須先執行本機SnapCenter資料庫的完整還原。此過程完成後，將重新建立與虛擬機器的通信，並且現在可以使用 FSx ONTAP作為主儲存恢復應用程式備份。

為此，您必須在SnapCenter伺服器上完成以下項目：

1. 將電腦名稱配置為與原始本機SnapCenter伺服器相同。
2. 設定網路以與 VMware Cloud 和 FSx ONTAP實例通訊。
3. 完成恢復SnapCenter資料庫的過程。
4. 確認SnapCenter處於災難復原模式，以確保 FSx 現在是備份的主要儲存。
5. 確認已與復原的虛擬機器重新建立通訊。

▼ 部署輔助 **Veeam Backup & Replication** 伺服器

您可以在 AWS 上的 VMware Cloud 中的 Windows 伺服器或 EC2 執行個體上安裝 Veeam Backup & Replication 伺服器。有關詳細的實施指南，請參閱 "Veeam 幫助中心技術文檔"。

▼ 設定輔助 **Veeam Backup & Replication** 伺服器

若要對已備份至 Amazon S3 儲存空間的虛擬機器進行還原，必須在 Windows 伺服器上安裝 Veeam Server，並將其設定為與 VMware Cloud、FSx ONTAP和包含原始備份儲存庫的 S3 儲存桶通訊。它還必須在 FSx ONTAP上配置一個新的備份儲存庫，以便在虛擬機器復原後進行新的備份。

要執行此過程，必須完成以下項目：

1. 設定網路以與 VMware Cloud、FSx ONTAP和包含原始備份儲存庫的 S3 儲存桶通訊。
2. 將 FSx ONTAP上的 SMB 共用配置為新的備份儲存庫。
3. 安裝用作本機擴充備份儲存庫一部分的原始 S3 儲存桶。
4. 還原虛擬機器後，建立新的備份作業來保護 SQL 和 Oracle 虛擬機器。

有關使用 Veeam 恢復虛擬機的更多信息，請參閱"使用 Veeam Full Restore 復原應用程式虛擬機"。

SnapCenter資料庫備份用於災難復原

SnapCenter允許備份和恢復其底層 MySQL 資料庫和配置數據，以便在發生災難時恢復SnapCenter伺服器。對於我們的解決方案，我們恢復了位於我們的 VPC 中的 AWS EC2 執行個體上的SnapCenter資料庫和配置。有關SnapCenter災難復原的更多信息，請參閱 "此連結"。

▼ **SnapCenter**備份前提條件

SnapCenter備份需要符合以下先決條件：

- 在本機ONTAP系統上建立的磁碟區和 SMB 共享，用於定位備份資料庫和設定檔。
- 本機ONTAP系統與 AWS 帳戶中的 FSx 或 CVO 之間的SnapMirror關係。此關係用於傳輸包含備份的SnapCenter資料庫和設定檔的快照。
- 安裝在雲端帳戶中的 Windows Server，可以在 EC2 執行個體上，也可以在 VMware Cloud SDDC 中的 VM 上。
- SnapCenter安裝在 VMware Cloud 中的 Windows EC2 執行個體或 VM 上。

▼ **SnapCenter**備份與還原流程摘要

- 在本機ONTAP系統上建立一個卷，用於託管備份資料庫和設定檔。
- 在本地和 FSx/CVO 之間建立SnapMirror關係。
- 掛載 SMB 共享。
- 檢索用於執行 API 任務的 Swagger 授權令牌。
- 啟動資料庫復原程序。
- 使用 xcopy 公用程式將 db 和設定檔本機目錄複製到 SMB 共用。
- 在 FSx 上，建立ONTAP磁碟區的克隆（透過SnapMirror從本地複製）。
- 將 SMB 共用從 FSx 掛載到 EC2/VMware Cloud。
- 將復原目錄從 SMB 共用複製到本機目錄。
- 從 Swagger 執行 SQL Server 還原程序。

▼ 備份**SnapCenter**資料庫和配置

SnapCenter提供了一個用於執行 REST API 命令的 Web 用戶端介面。有關透過 Swagger 存取 REST API 的信息，請參閱SnapCenter文檔 "此連結"。

▼ 登入**Swagger**並取得授權令牌

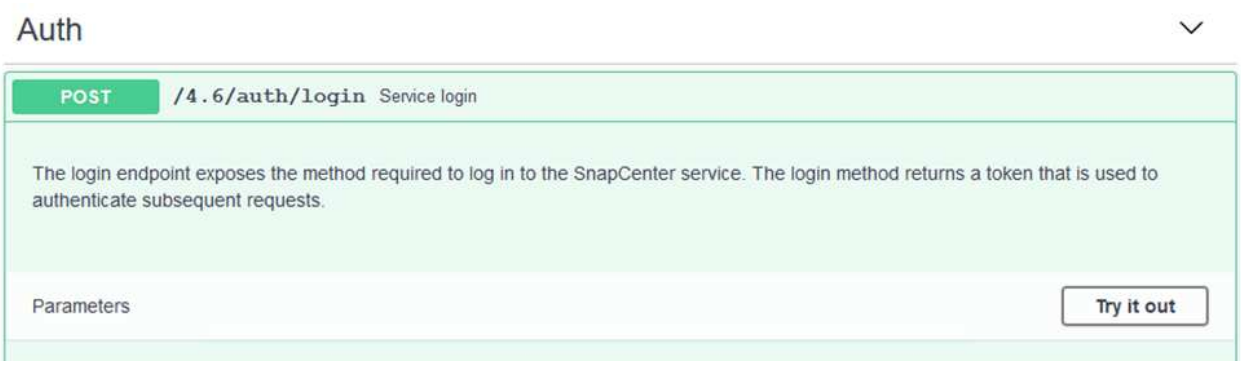
導覽至 Swagger 頁面後，您必須檢索授權令牌才能啟動資料庫復原程序。

1. 造訪SnapCenter Swagger API 網頁，位址為 *https://< SnapCenter*伺服器 *IP>:8146/swagger/*。

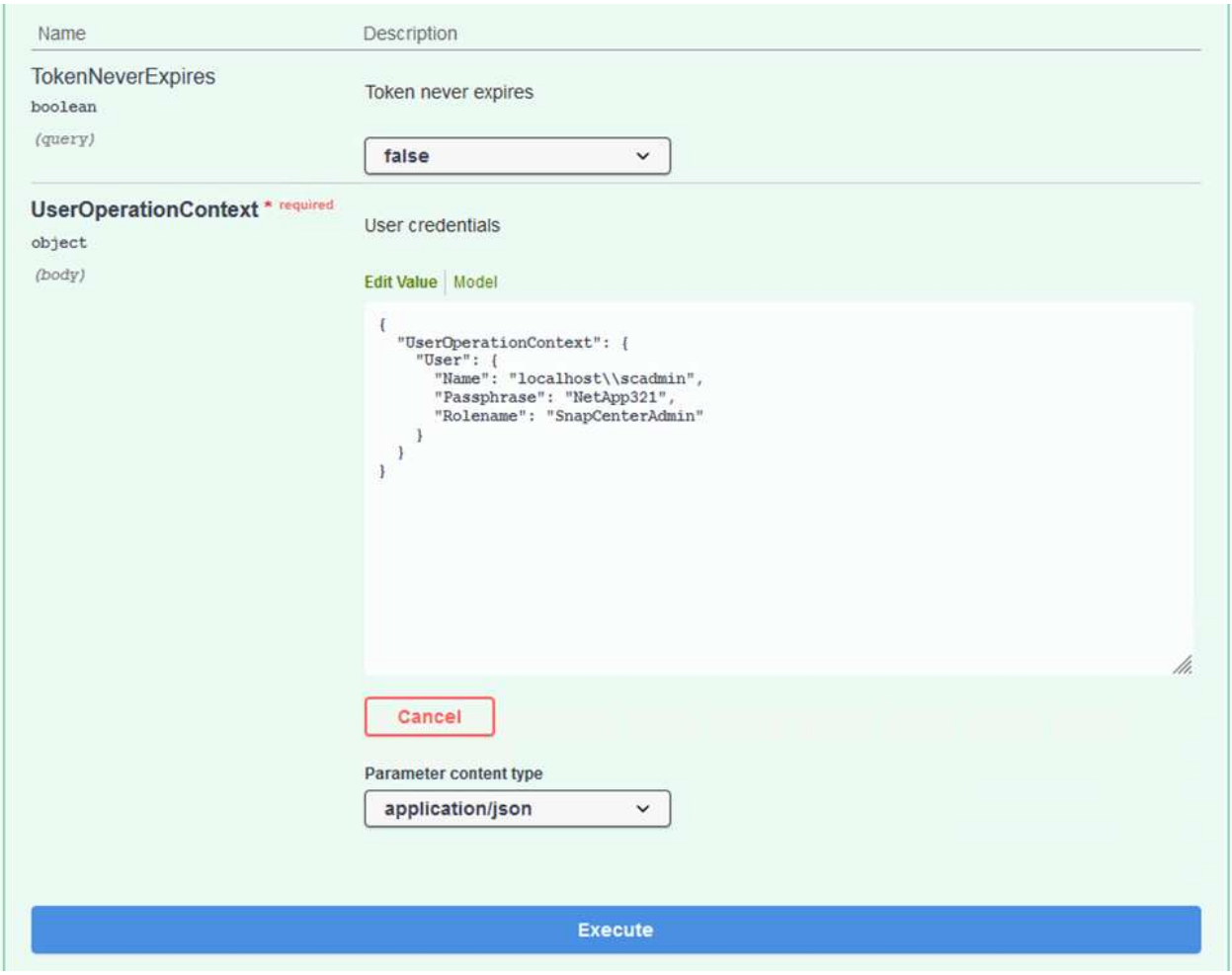




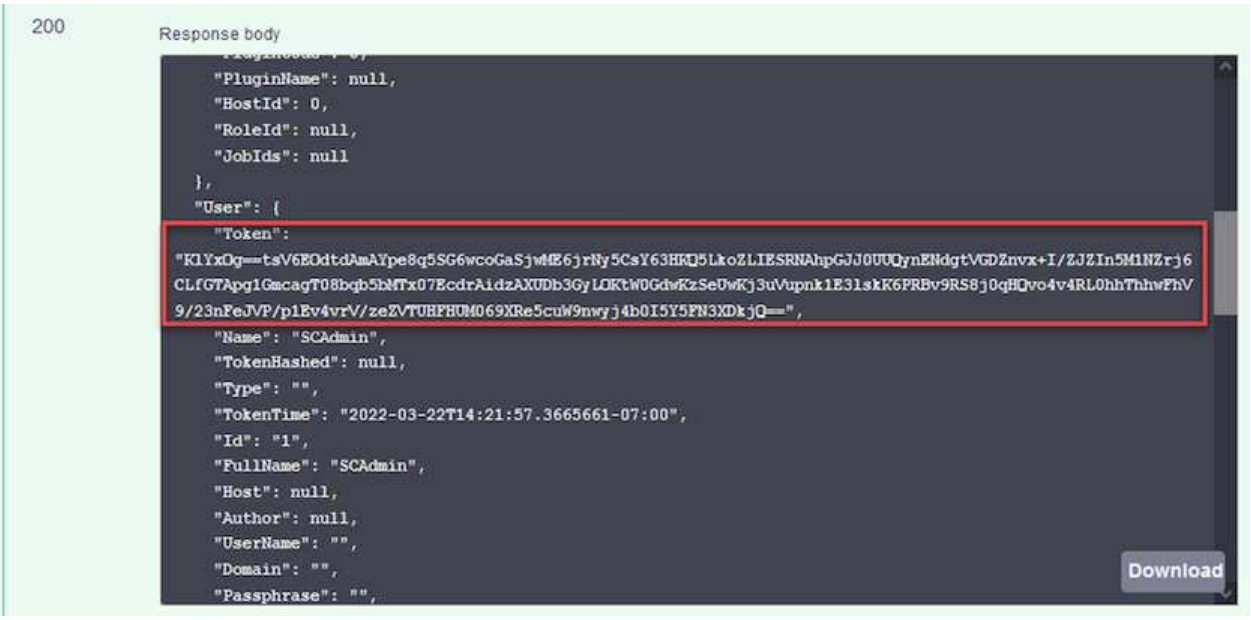
2. 展開“Auth”部分並點擊“Try it Out”。



3. 在 UserOperationContext 區域，填寫SnapCenter憑證和角色，然後按一下「執行」。



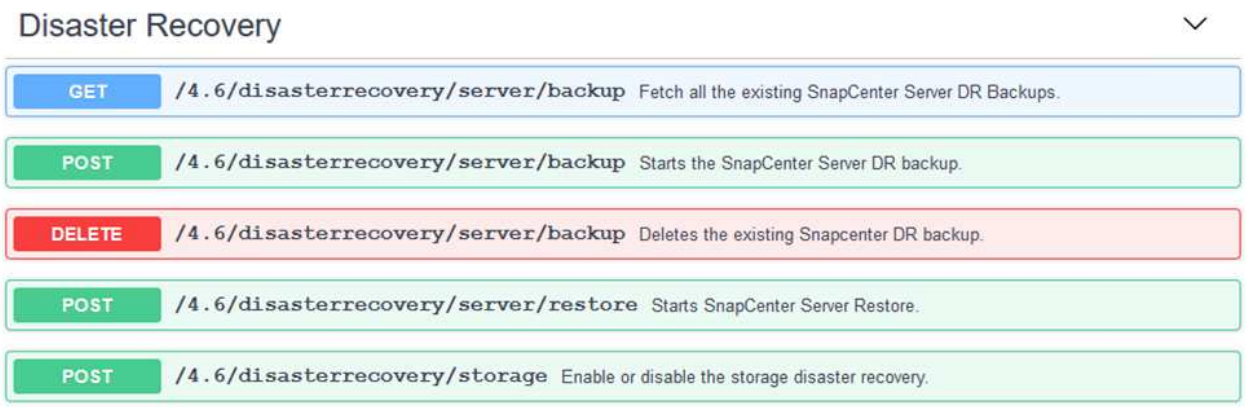
4. 在下面的回應主體中，您可以看到令牌。執行備份過程時複製令牌文字以進行身份驗證。



▼ 執行**SnapCenter**資料庫備份

接下來前往 Swagger 頁面上的災難復原區域以開始SnapCenter備份流程。

1. 按一下「災難復原」區域並將其展開。

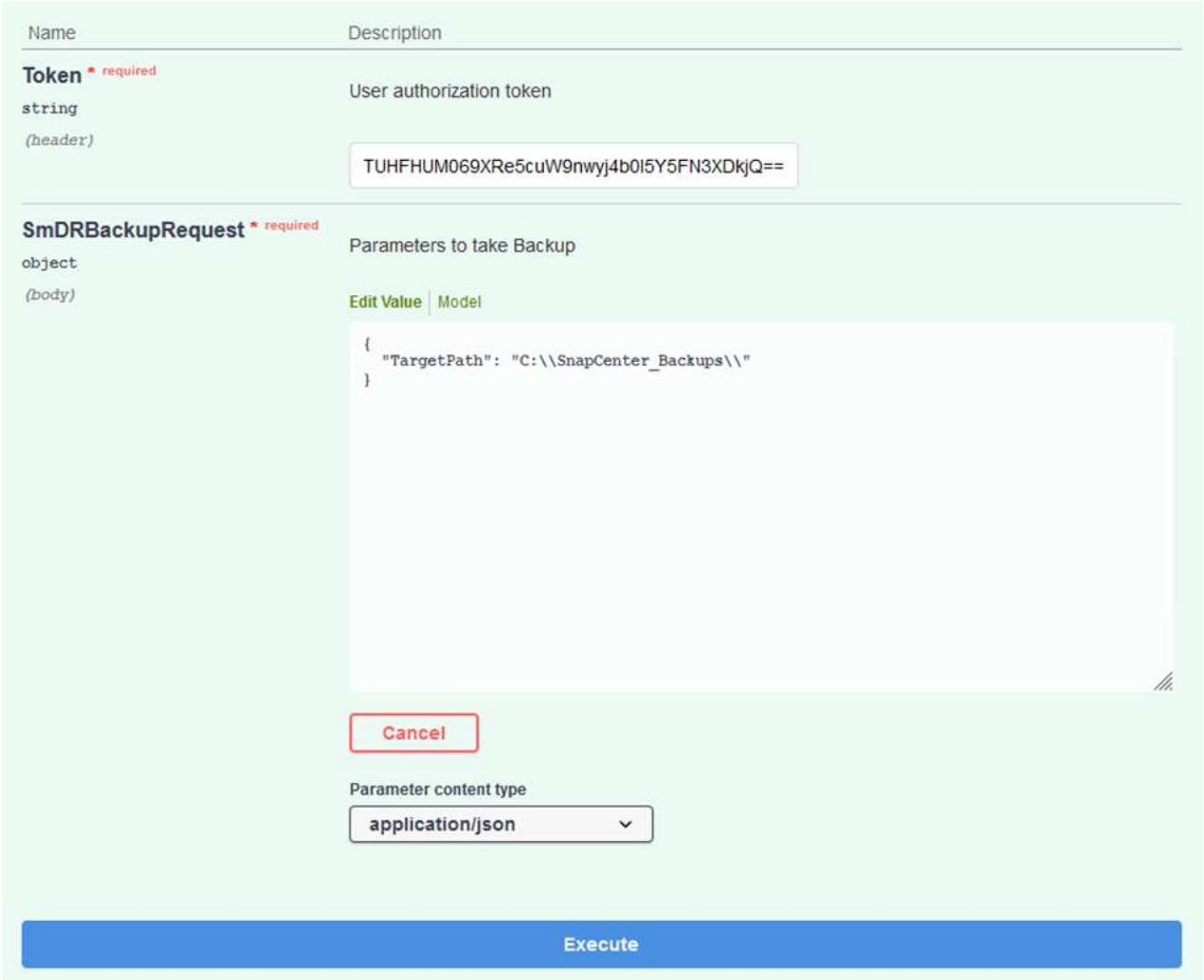


2. 展開 `/4.6/disasterrecovery/server/backup`部分並點擊“試用”。



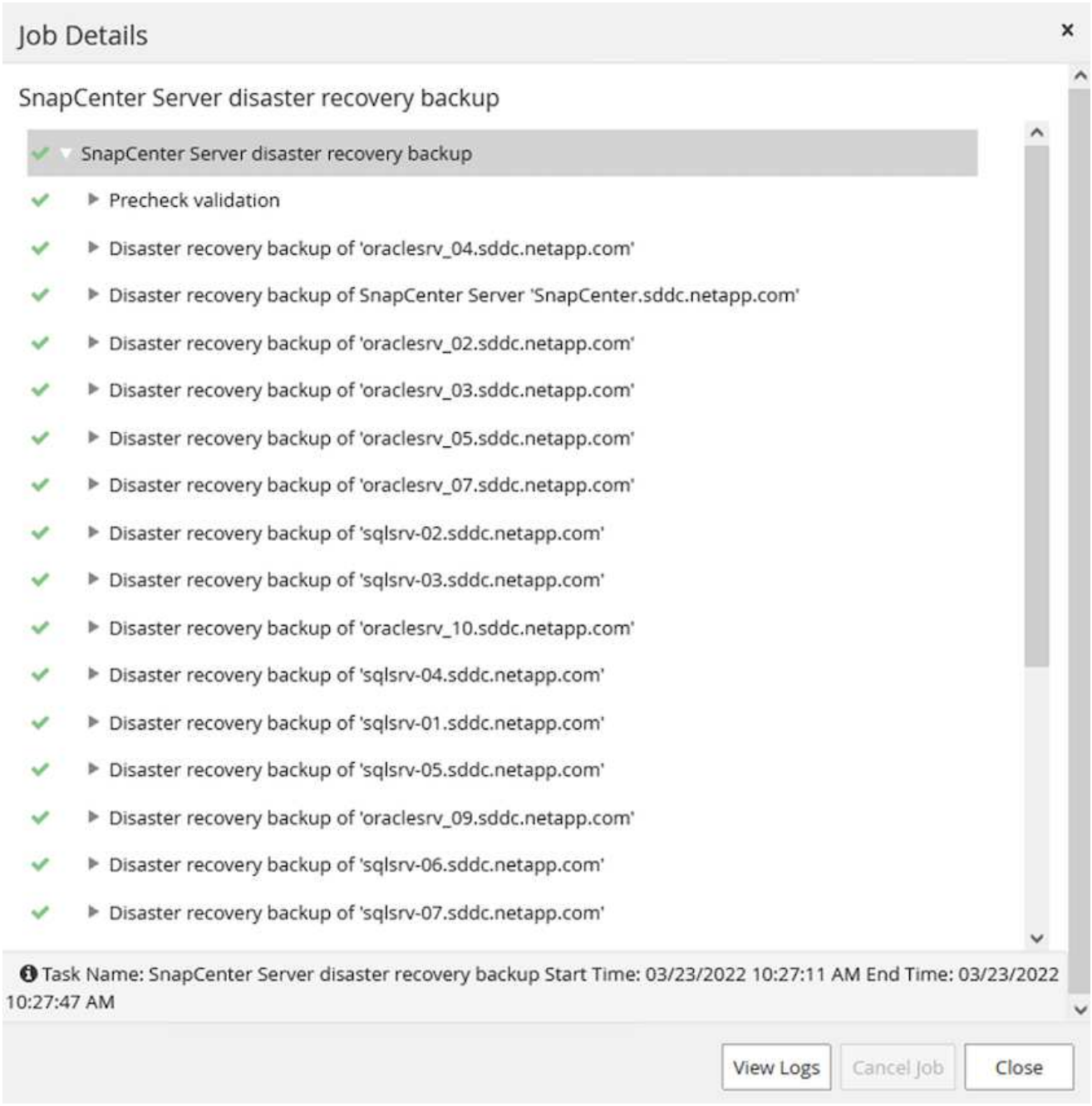
3. 在 SmDRBackupRequest 部分中，新增正確的本機目標路徑並選擇執行以啟動SnapCenter資料庫和配置的備份。

備份過程不允許直接備份到 NFS 或 CIFS 檔案共用。



▼ 從**SnapCenter**監控備份作業

在啟動資料庫還原程序時登入SnapCenter查看日誌檔案。在「監視」部分下，您可以查看SnapCenter伺服器災難復原備份的詳細資訊。



▼ 使用 **XCOPY** 實用程式將資料庫備份檔案複製到 **SMB** 共享

接下來，您必須將備份從SnapCenter伺服器上的本機磁碟機移至 CIFS 共用，該共用用於將資料透過SnapMirror複製到位於 AWS 中 FSx 執行個體上的輔助位置。使用具有特定選項的 xcopy 來保留檔案的權限。

以管理員身份開啟命令提示字元。在命令提示字元下，輸入以下命令：

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X /E
/H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O /X
/E /H /K
```

▼ 主站點發生災難

對於發生在主本機資料中心的災難，我們的場景包括使用 VMware Cloud on AWS 將故障轉移到位於 Amazon Web Services 基礎架構上的輔助站點。我們假設虛擬機器和我們的內部ONTAP叢集不再可存取。此外， SnapCenter和 Veeam 虛擬機都不再可訪問，必須在我們的輔助站點上重建。

本節討論將我們的基礎設施故障轉移到雲端，並涵蓋以下主題：

- SnapCenter資料庫還原。建立新的SnapCenter伺服器後，恢復 MySQL 資料庫和設定文件，並將資料庫切換到災難復原模式，以允許輔助 FSx 儲存成為主儲存設備。
- 使用 Veeam Backup & Replication 復原應用程式虛擬機器。連接包含 VM 備份的 S3 存儲，導入備份，然後將其還原到 VMware Cloud on AWS。
- 使用SnapCenter還原 SQL Server 應用程式資料。
- 使用SnapCenter恢復 Oracle 應用程式資料。

▼ **SnapCenter**資料庫還原過程

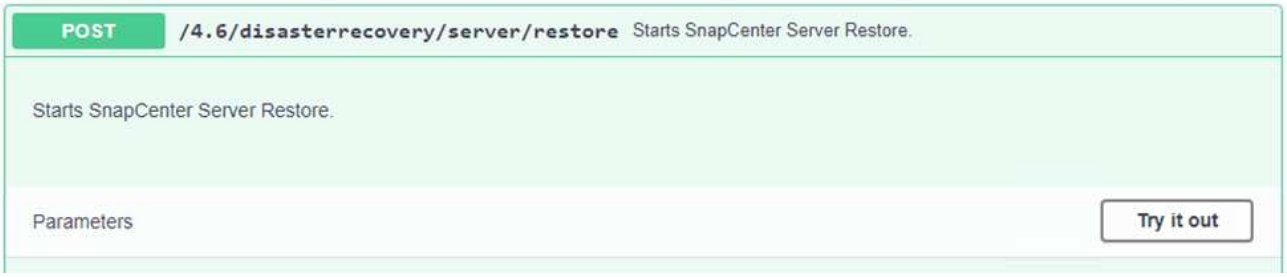
SnapCenter透過允許備份和還原其 MySQL 資料庫和設定檔來支援災難復原場景。這允許管理員在本地資料中心維護SnapCenter資料庫的定期備份，然後將該資料庫還原到輔助SnapCenter資料庫。

若要存取遠端SnapCenter伺服器上的SnapCenter備份文件，請完成下列步驟：

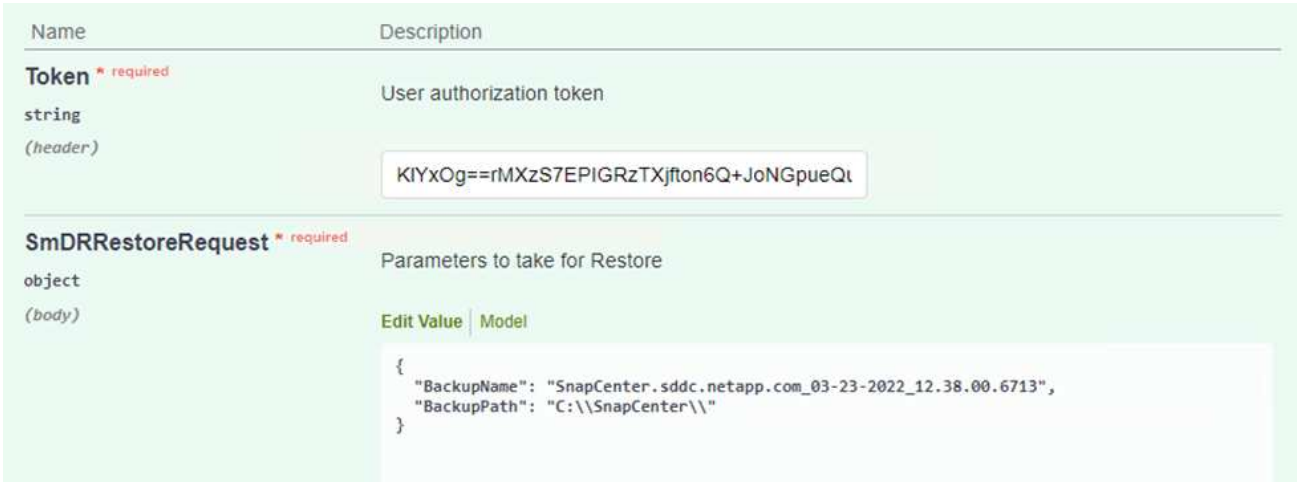
1. 斷開與 FSx 叢集的SnapMirror關係，這使得磁碟區可讀/寫入。
2. 建立 CIFS 伺服器（如有必要）並建立指向複製磁碟區連線路徑的 CIFS 共用。
3. 使用 xcopy 將備份檔案複製到輔助SnapCenter系統上的本機目錄。
4. 安裝SnapCenter v4.6。
5. 確保SnapCenter伺服器與原始伺服器具有相同的 FQDN。這是資料庫復原成功所必需的。

若要開始復原過程，請完成以下步驟：

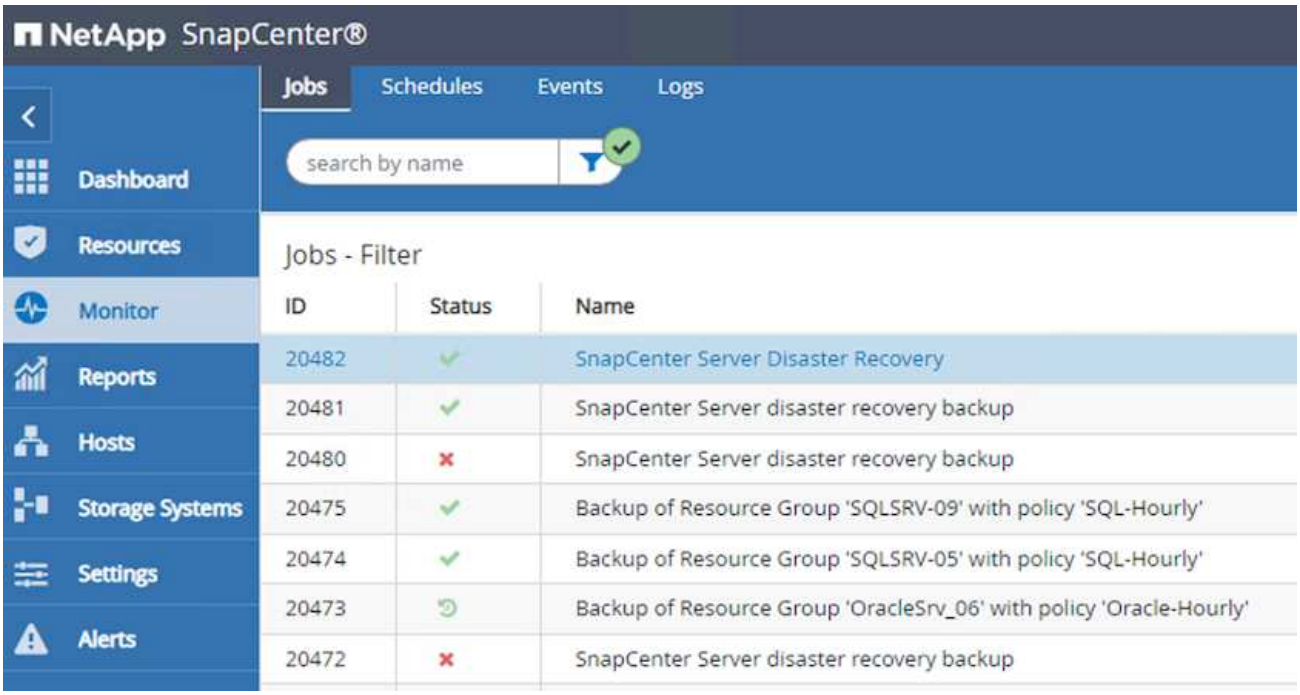
1. 導覽至輔助SnapCenter伺服器的 Swagger API 網頁，並依照前面的說明取得授權令牌。
2. 導航至 Swagger 頁面的災難復原部分，選擇 `/4.6/disasterrecovery/server/restore`，然後按一下「試用」。

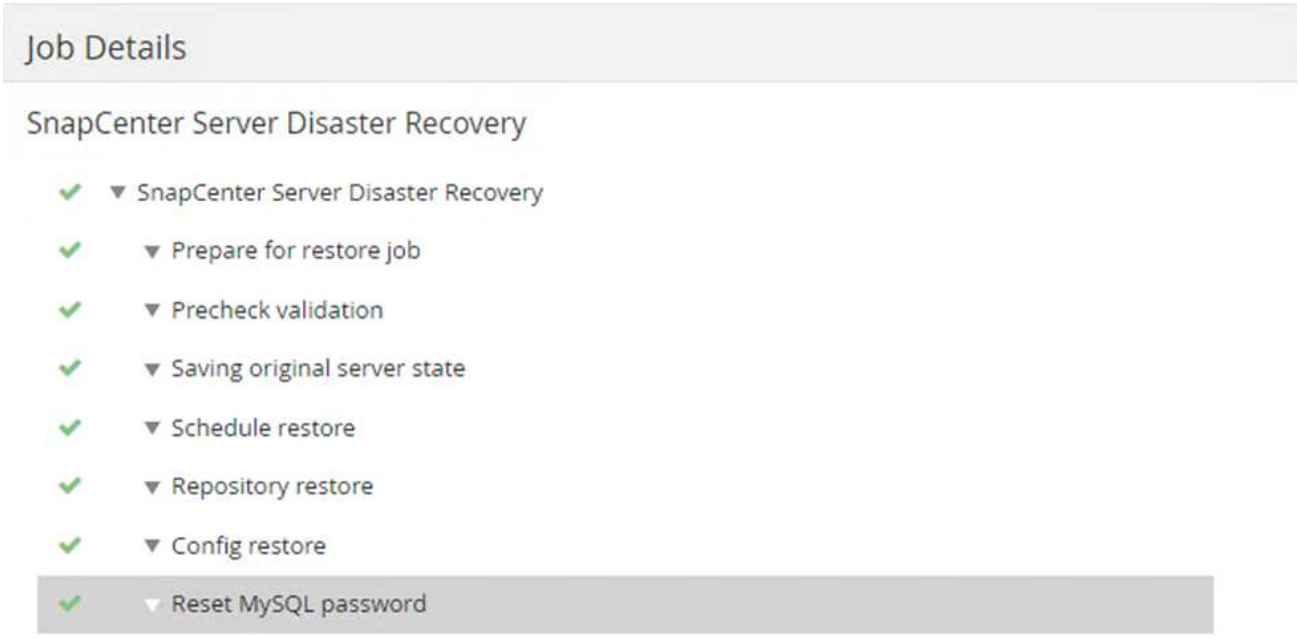


3. 貼上您的授權令牌，並在 SmDRResterRequest 部分貼上備份的名稱和輔助SnapCenter伺服器上的本機目錄。



4. 選擇“執行”按鈕開始恢復程序。
5. 從SnapCenter導航到「監視」部分以查看還原作業的進度。





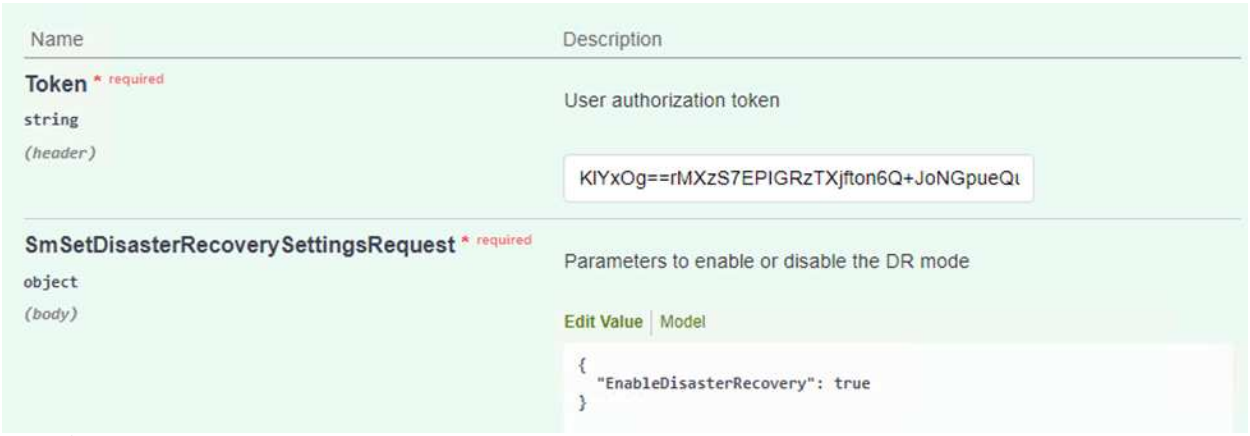
6. 若要從二級儲存啟用 SQL Server 還原，必須將SnapCenter資料庫切換到災難復原模式。這是作為單獨的操作執行的，並在 Swagger API 網頁上啟動。

   a. 導航至災難復原部分並點擊 `/4.6/disasterrecovery/storage`。

   b. 貼上使用者授權令牌。

   c. 在 SmSetDisasterRecoverySettingsRequest 部分中，更改 `EnableDisasterRecover`到 `true`。

   d. 按一下「執行」以啟用 SQL Server 的災難復原模式。



請參閱有關附加程序的評論。

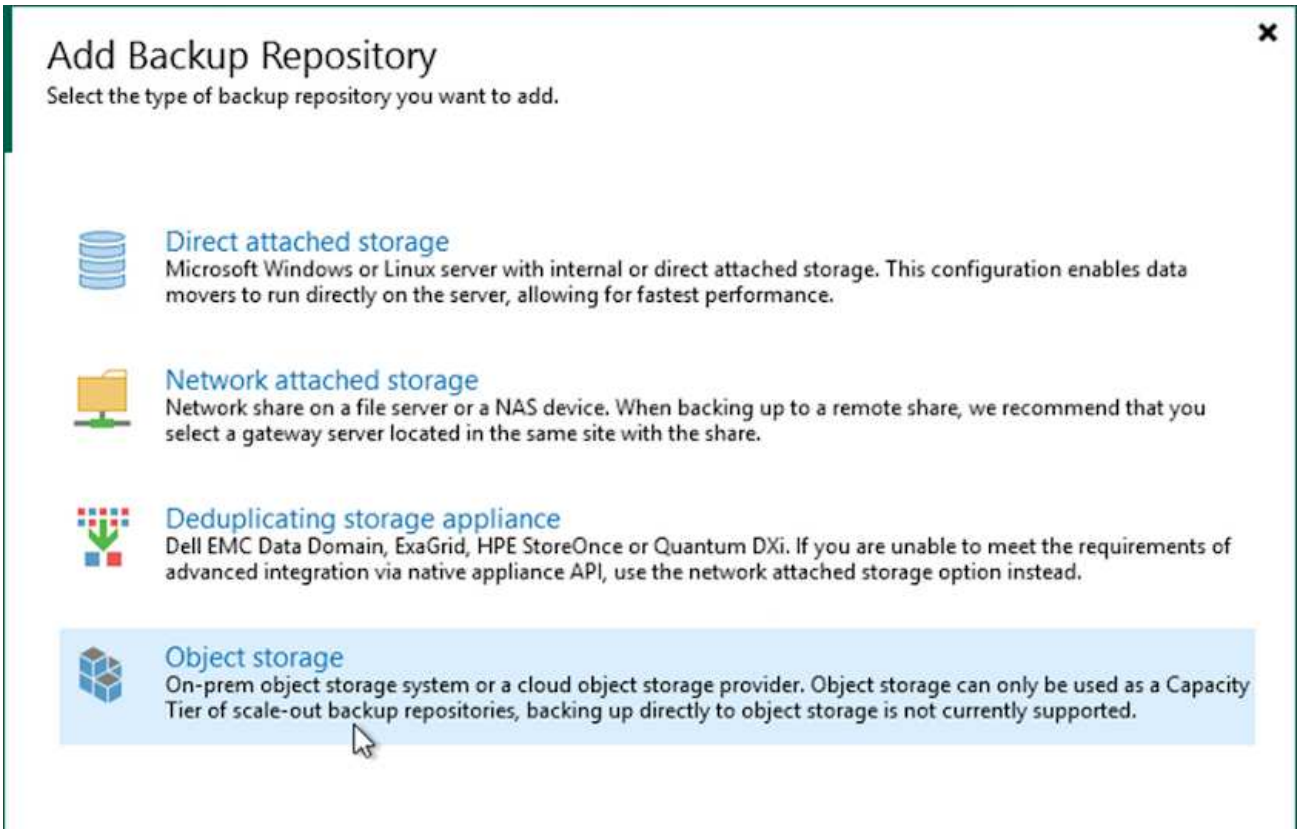
使用 **Veeam** 完整恢復功能恢復應用程式虛擬機

▼ 建立備份儲存庫並從 **S3** 匯入備份

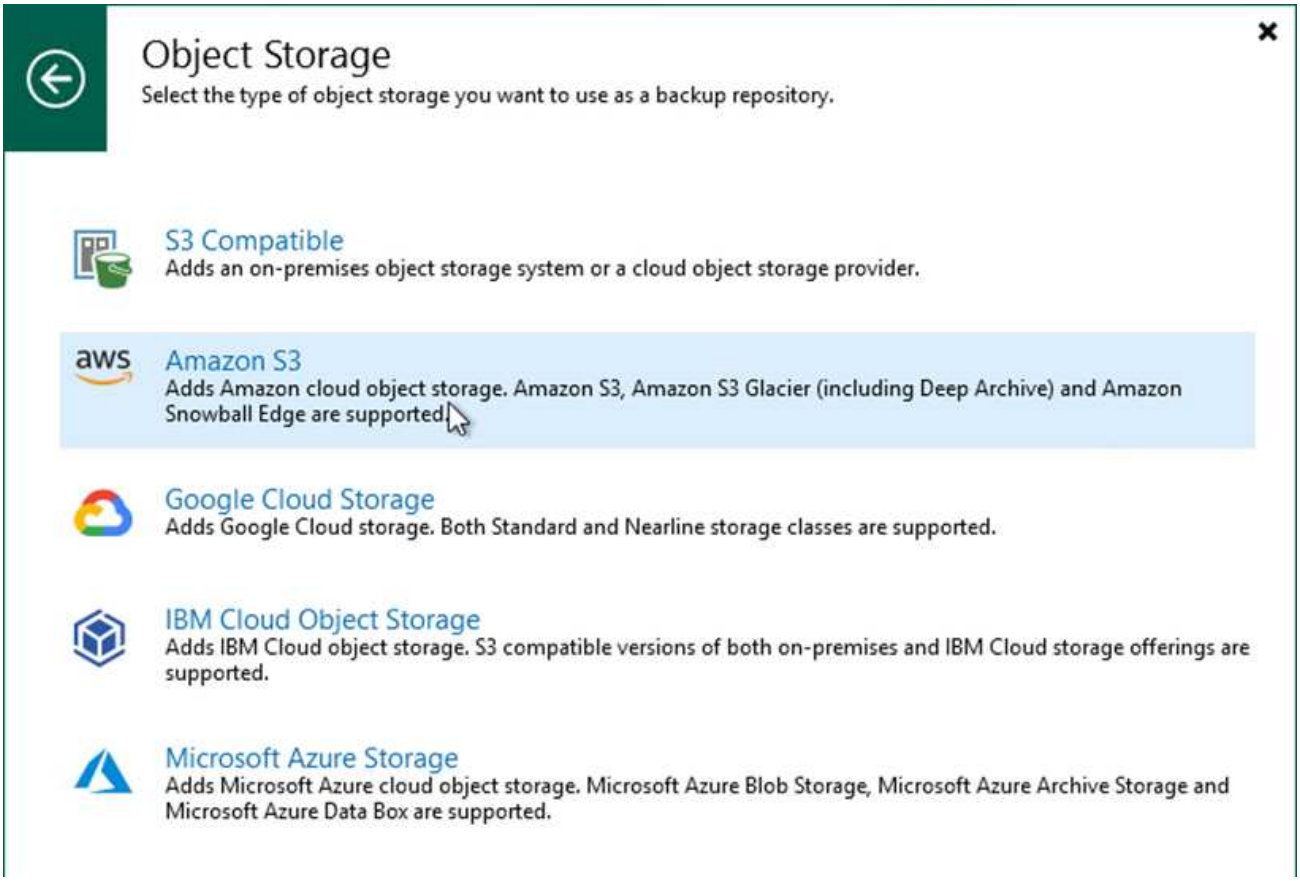
從輔助 Veeam 伺服器，從 S3 儲存匯入備份並將 SQL Server 和 Oracle VM 還原到您的 VMware Cloud 叢集。

若要從屬於本機擴充備份儲存庫的 S3 物件匯入備份，請完成下列步驟：

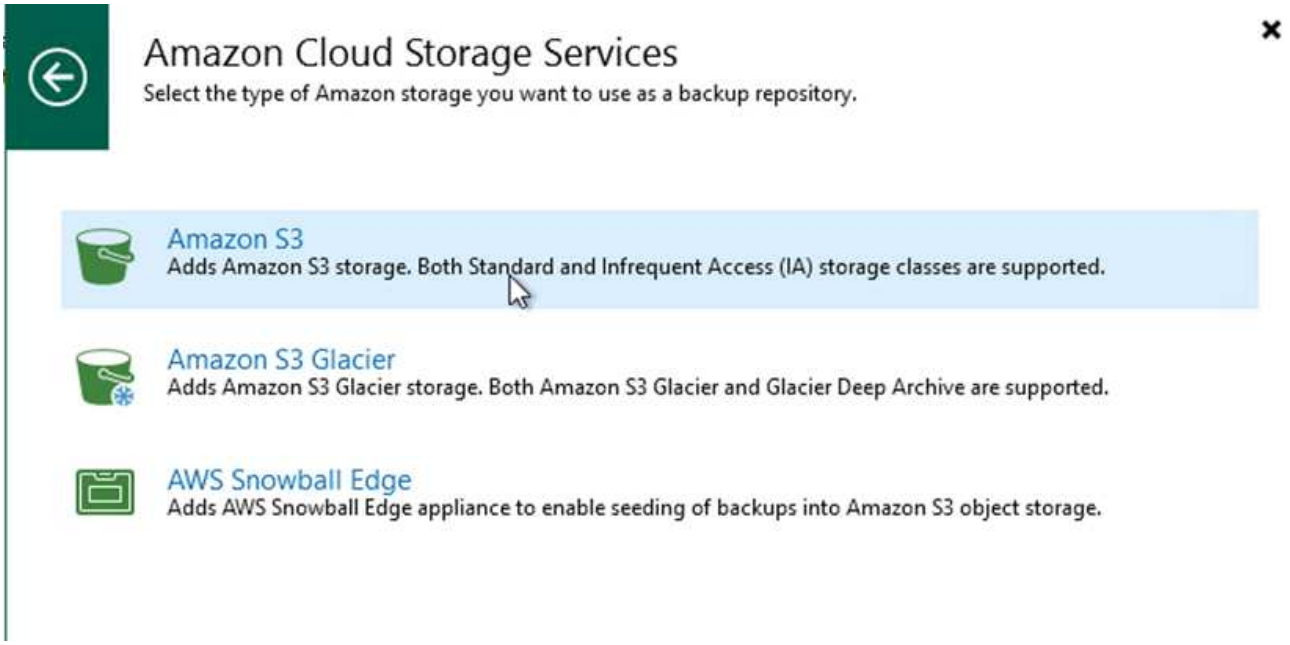
1. 前往備份儲存庫並點擊頂部選單中的新增儲存庫以啟動新增備份儲存庫精靈。在精靈的第一頁上，選擇物件儲存作為備份儲存庫類型。



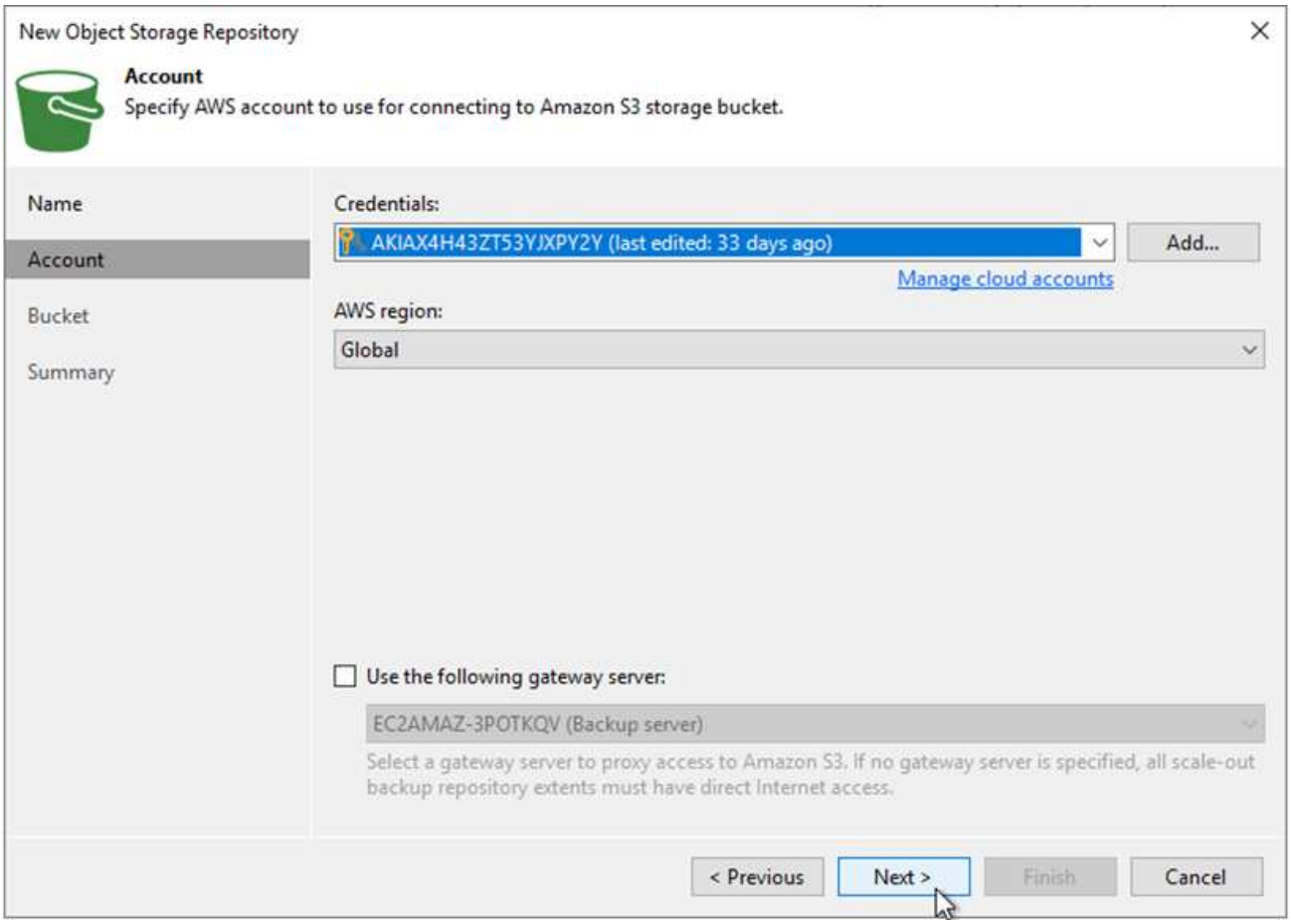
2. 選擇 Amazon S3 作為物件儲存類型。



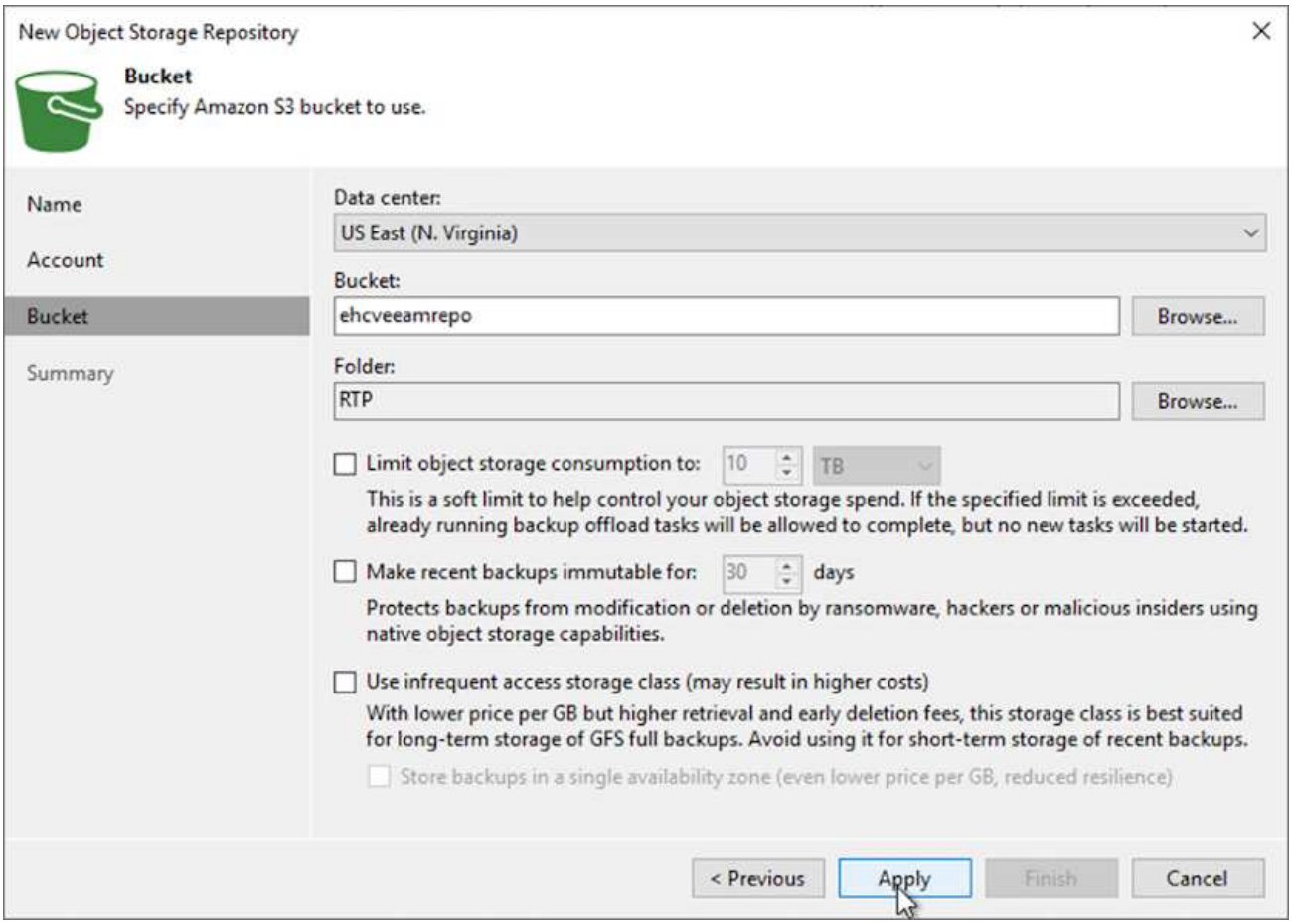
3. 從 Amazon 雲端儲存服務清單中，選擇 Amazon S3。



4. 從下拉清單中選擇您預先輸入的憑證或新增用於存取雲端儲存資源的新憑證。按一下“下一步”繼續。



5. 在 Bucket 頁面上，輸入資料中心、bucket、資料夾和任何所需選項。按一下“應用”。

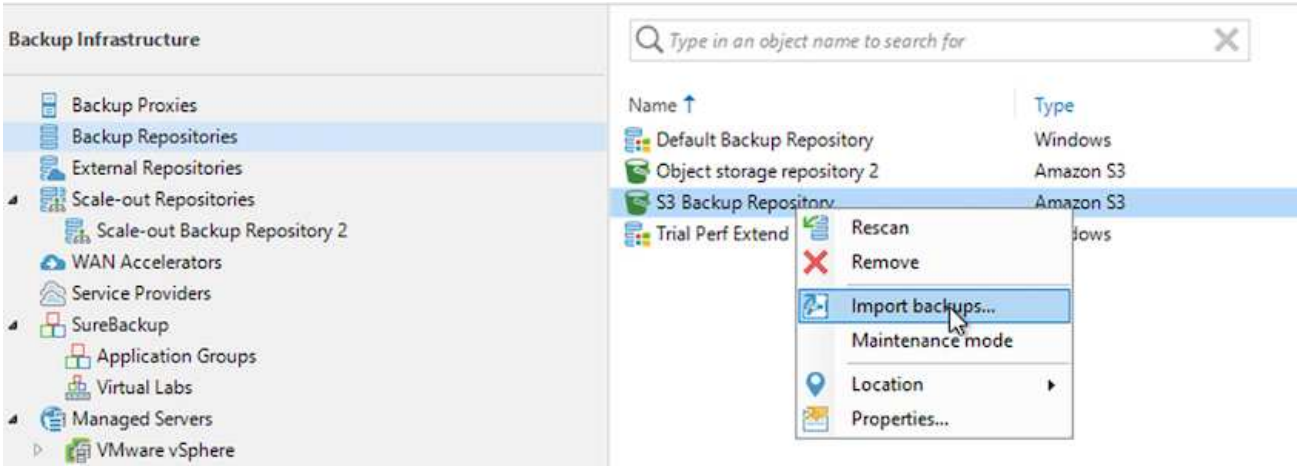


6. 最後，選擇“完成”以完成該過程並添加存儲庫。

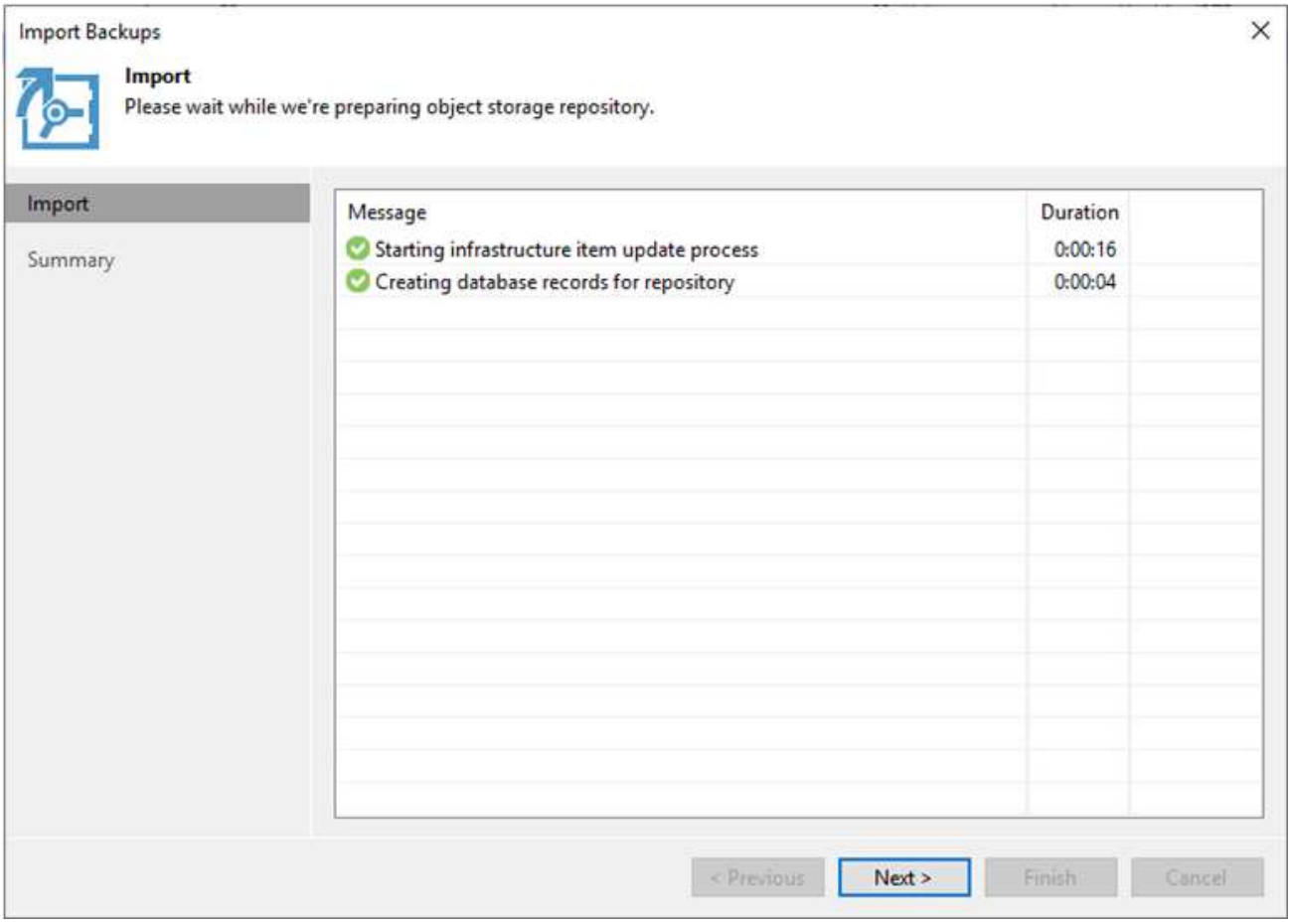
▼ 從 **S3** 物件儲存匯入備份

若要從上一節中新增的 S3 儲存庫匯入備份，請完成下列步驟。

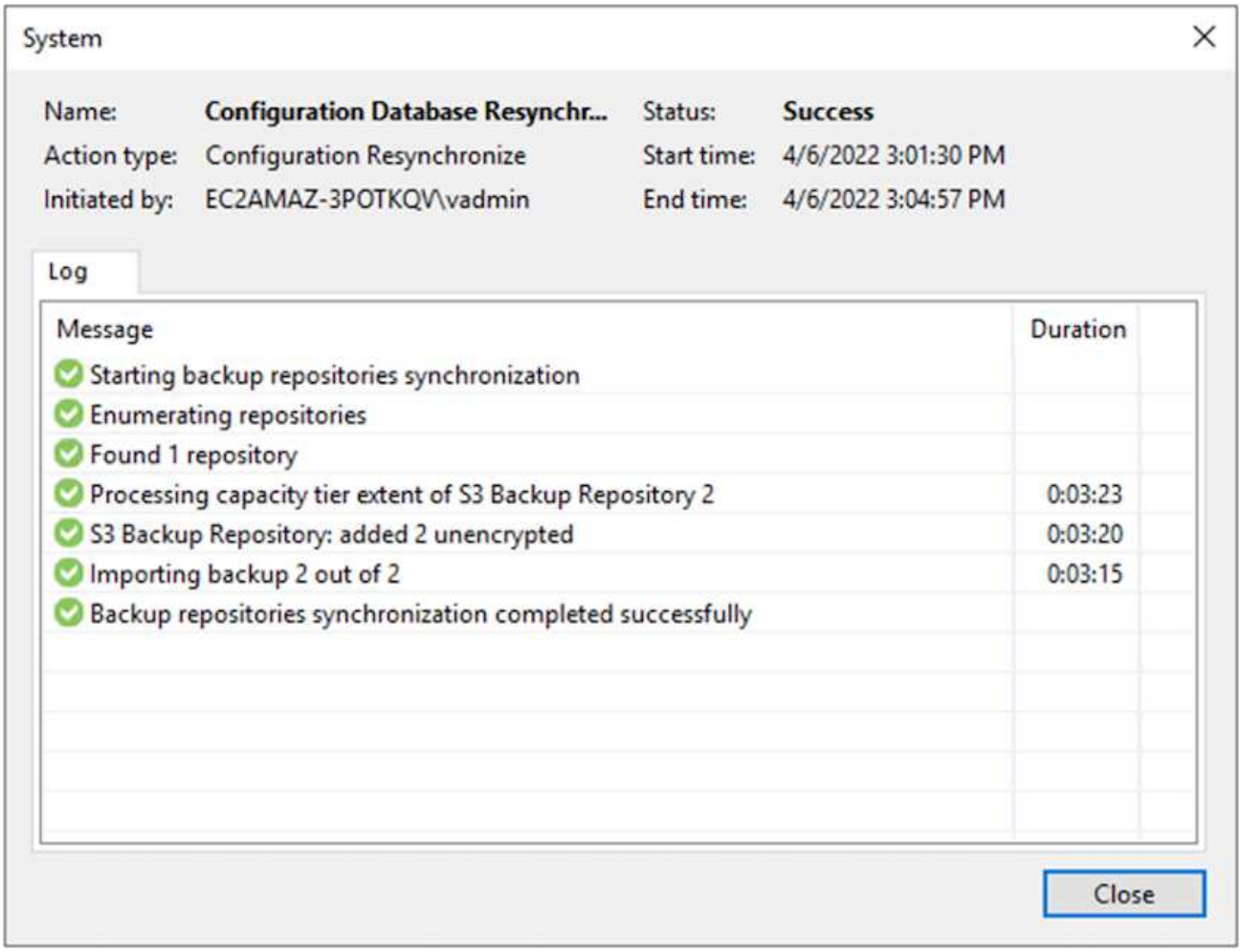
1. 從 S3 備份儲存庫中，選擇匯入備份以啟動匯入備份精靈。



2. 建立匯入的資料庫記錄後，選擇下一步，然後在摘要畫面上選擇完成以開始匯入程序。



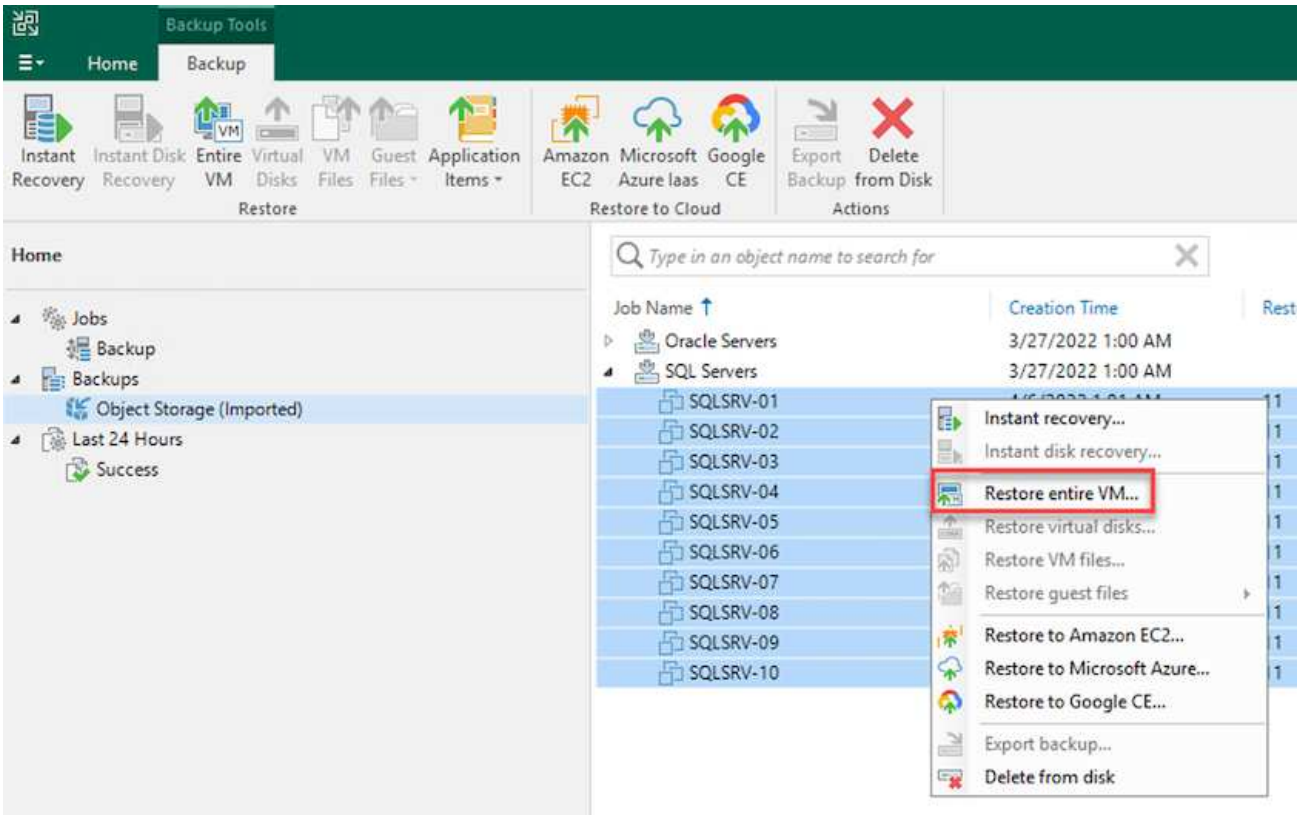
3. 匯入完成後，您可以將虛擬機器還原到 VMware Cloud 叢集。



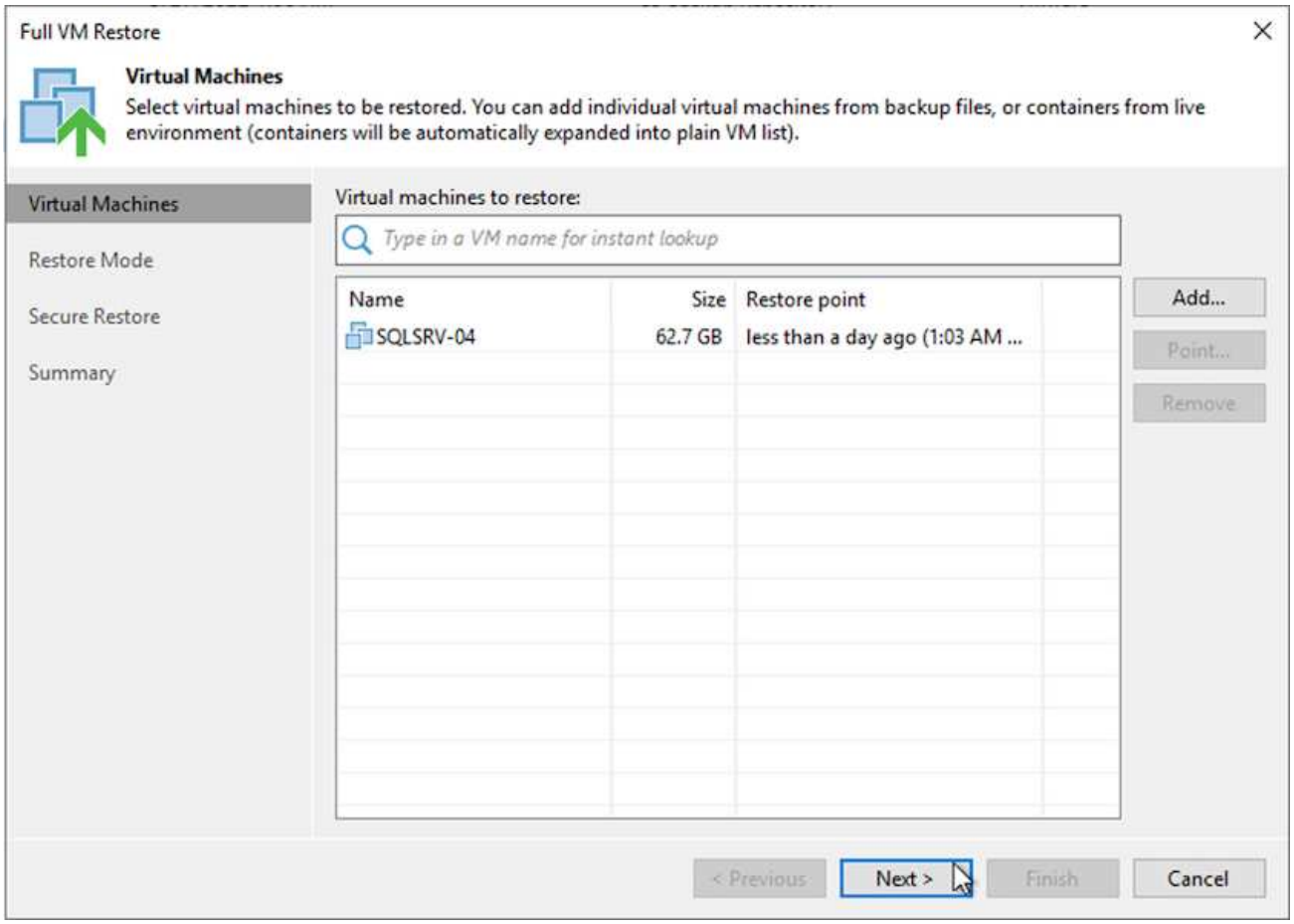
▼ 使用 **Veeam** 完整還原將應用程式虛擬機器還原到 **VMware Cloud**

若要將 SQL 和 Oracle 虛擬機器還原到 VMware Cloud on AWS 工作負載域/集群，請完成下列步驟。

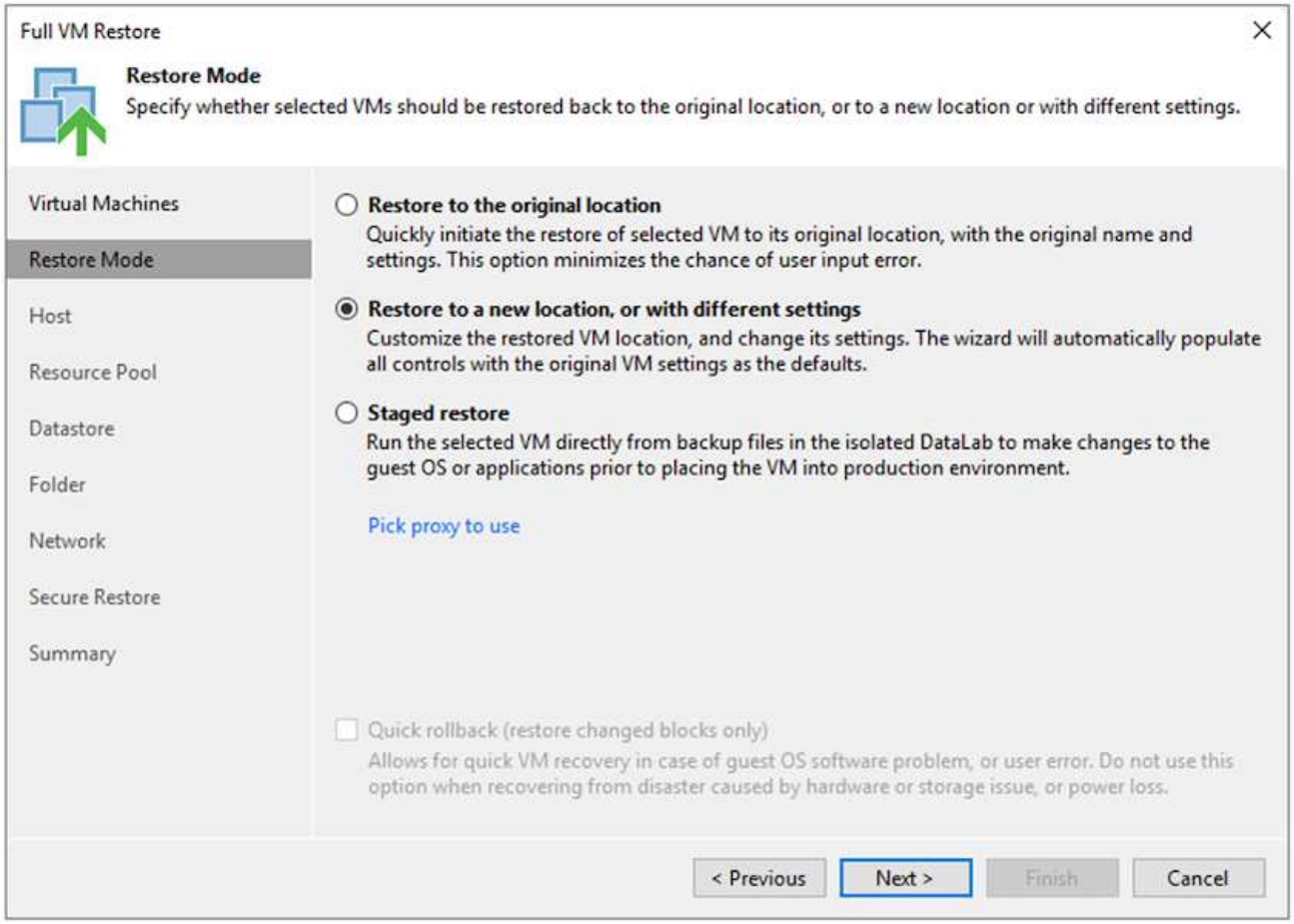
1. 從 Veeam 主頁中，選擇包含導入備份的對象存儲，選擇要恢復的虛擬機，然後右鍵單擊並選擇“恢復整個虛擬機”。



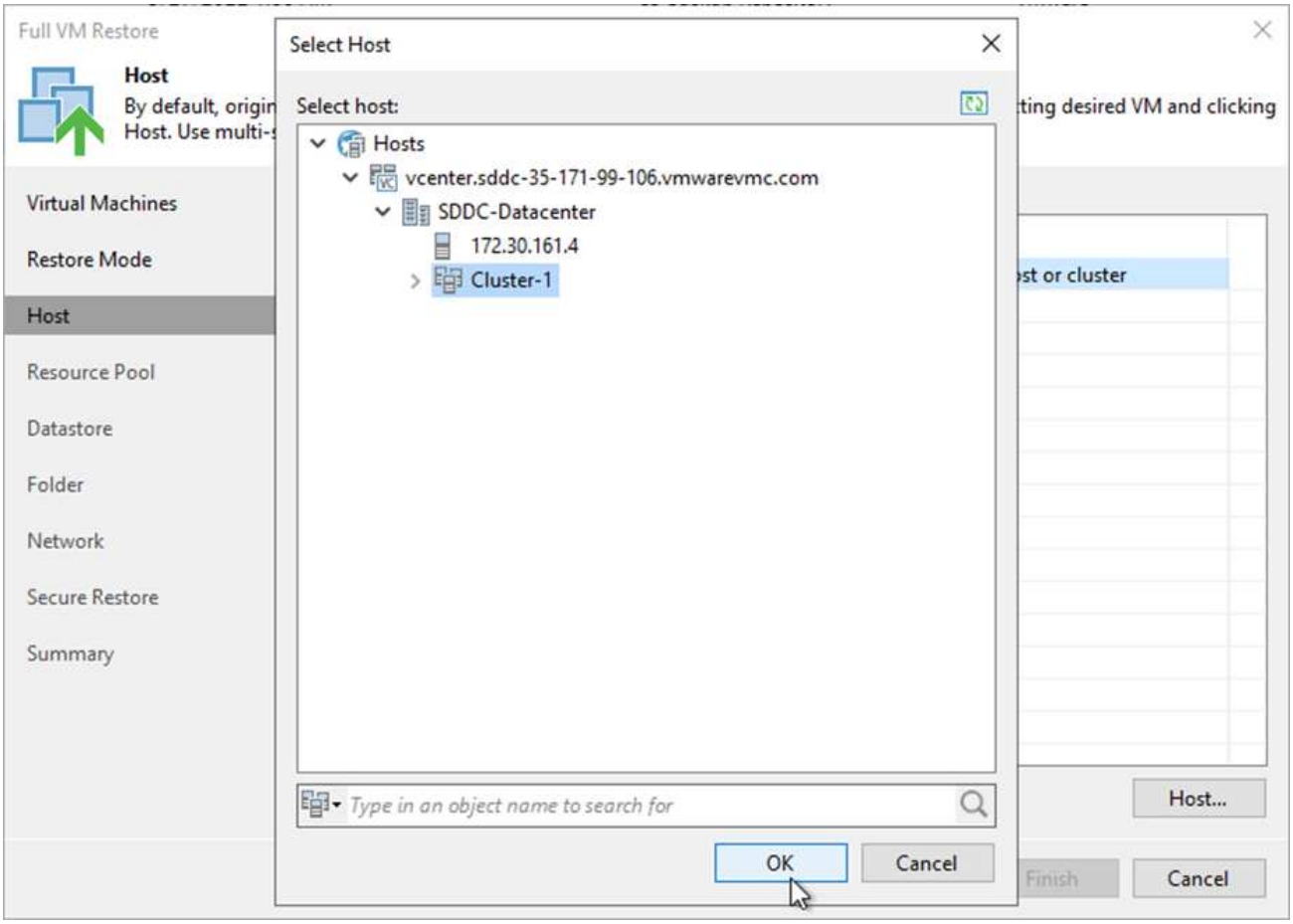
2. 在完整虛擬機還原精靈的第一頁上，根據需要修改要備份的虛擬機，然後選擇下一步。



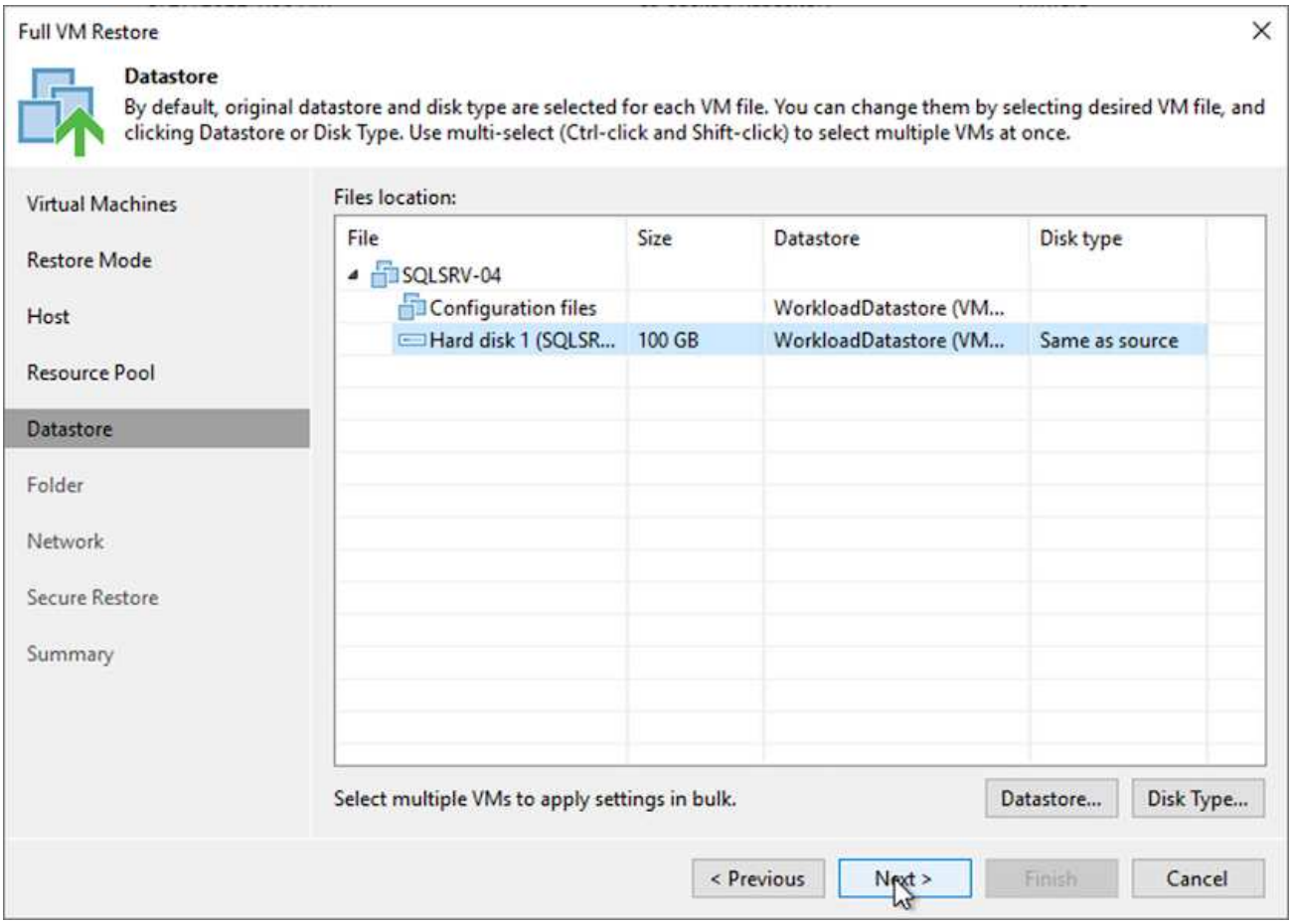
3. 在「恢復模式」頁面上，選擇「恢復到新位置」或「使用不同的設定」。



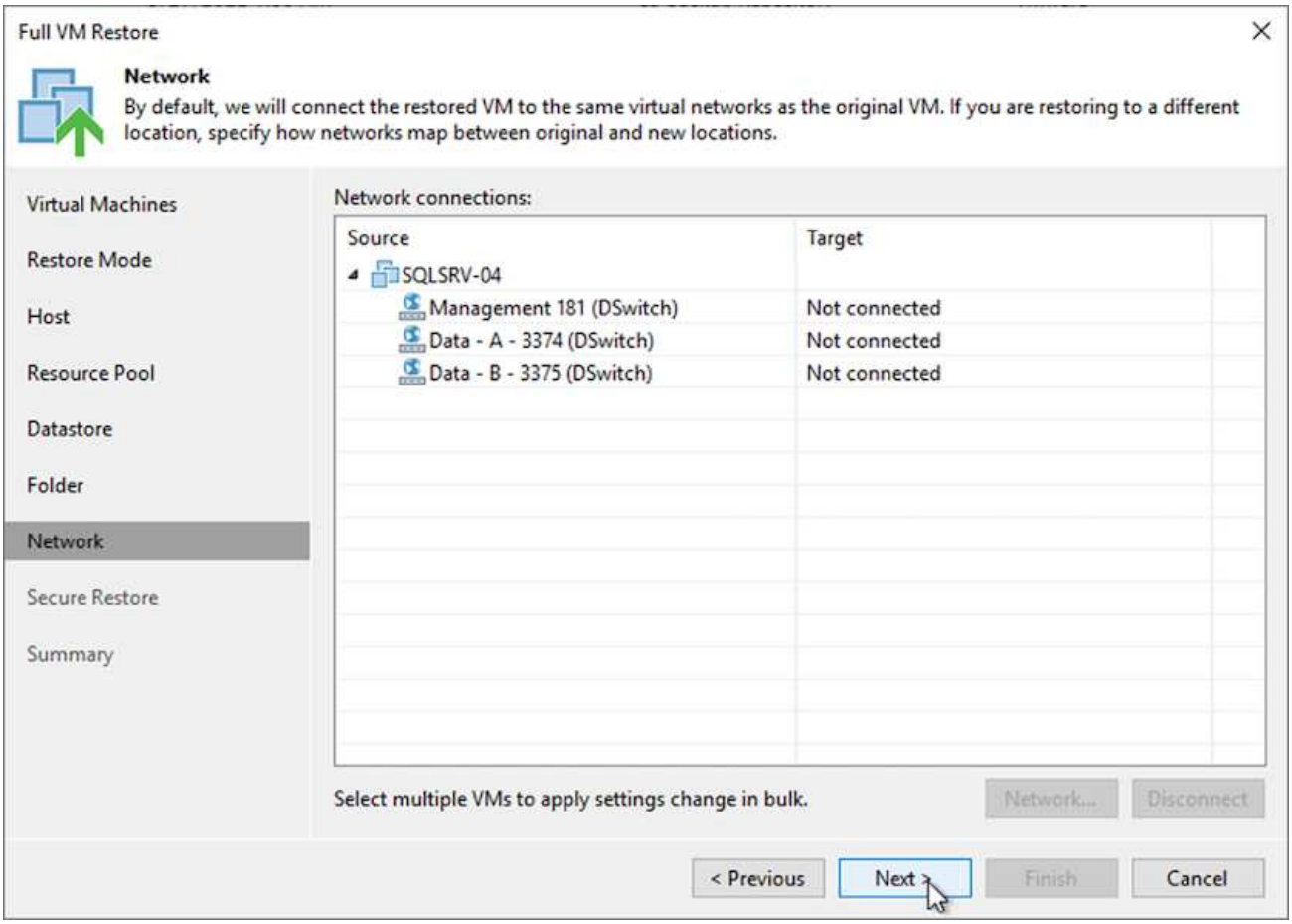
4. 在主機頁面上，選擇要將虛擬機器還原到的目標 ESXi 主機或叢集。

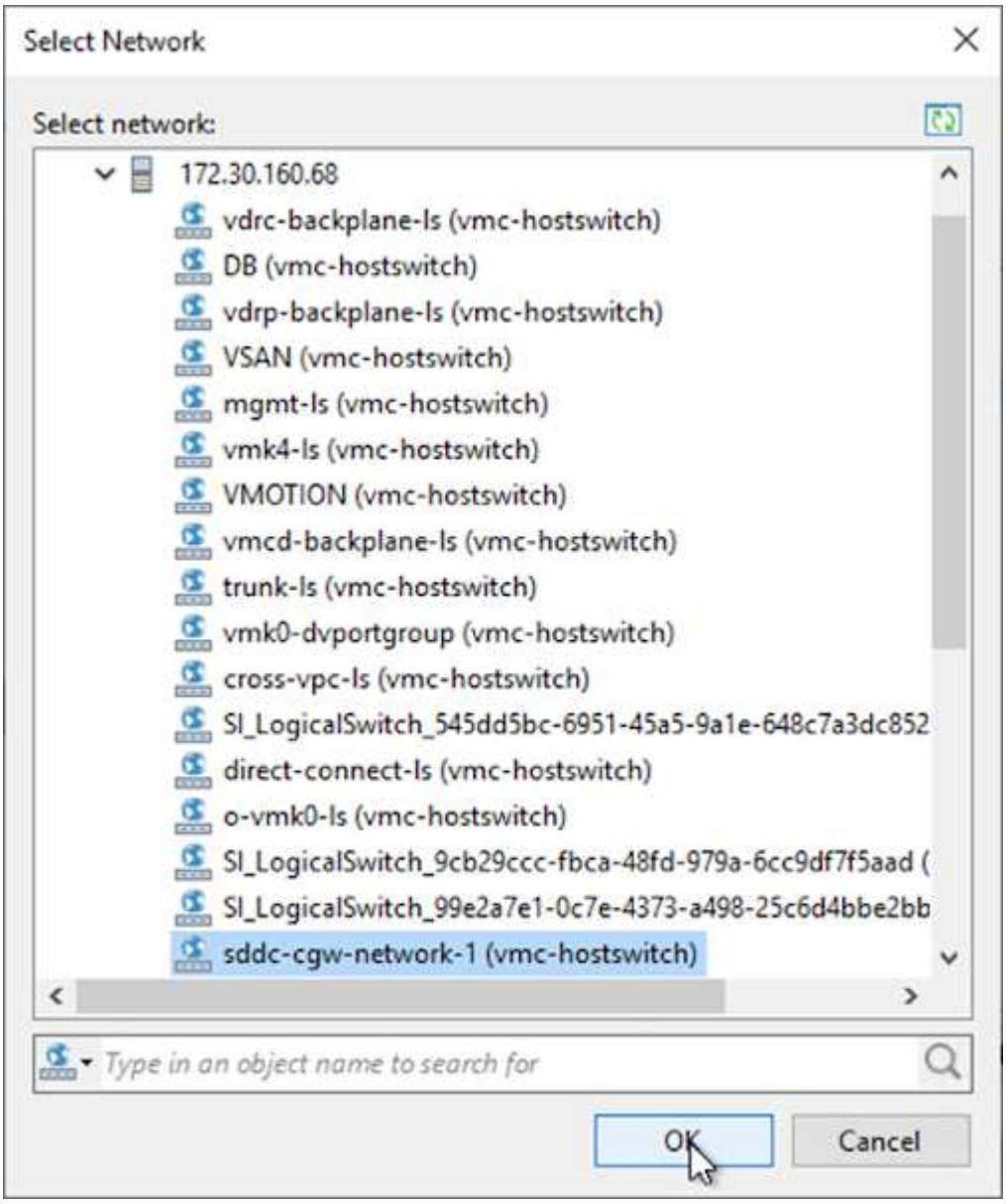


5. 在資料儲存頁面上，選擇設定檔和硬碟的目標資料儲存位置。



6. 在網路頁面，將虛擬機器上原有的網路對應到新目標位置的網路。


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. 選擇是否掃描已復原的虛擬機器中的惡意軟體，查看摘要頁面，然後按一下「完成」以開始復原。

還原 **SQL Server** 應用程式數據

以下程序提供了有關在發生導致本機網站無法執行的災難時如何在 AWS 中的 VMware Cloud Services 中還原 SQL Server 的說明。

為了繼續執行復原步驟，假定以下先決條件已完成：

1. Windows Server VM 已使用 Veeam Full Restore 還原至 VMware Cloud SDDC。
2. 已建立輔助SnapCenter伺服器，並已使用本節中概述的步驟完成SnapCenter資料庫還原和配置"SnapCenter備份和復原過程摘要。"

▼ **VM**：**SQL Server VM** 的復原後配置

虛擬機器還原完成後，您必須設定網路和其他項目，以準備在SnapCenter中重新發現主機虛擬機器。

1. 為管理和 iSCSI 或 NFS 指派新的 IP 位址。

2. 將主機加入 Windows 網域。
3. 將主機名稱新增至 DNS 或SnapCenter伺服器上的 hosts 檔案。

如果使用與目前網域不同的網域憑證部署SnapCenter插件，則必須變更 SQL Server VM 上 Windows 服務插件的登入帳戶。變更登入帳戶後，重新啟動SnapCenter SMCore、Windows 外掛程式和 SQL Server 外掛程式服務。

若要自動重新發現SnapCenter中還原的虛擬機，FQDN 必須與原先新增至本機SnapCenter 的虛擬機相同。

▼ 配置 **FSx** 儲存以進行 **SQL Server** 還原

要完成 SQL Server VM 的災難復原過程，您必須中斷與 FSx 叢集的現有SnapMirror關係並授予對該磁碟區的存取權。為此，請完成以下步驟。

1. 若要中斷 SQL Server 資料庫和日誌磁碟區的現有SnapMirror關係，請從 FSx CLI 執行下列命令：

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. 透過建立包含 SQL Server Windows VM 的 iSCSI IQN 的啟動器群組來授予對 LUN 的存取權限：

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

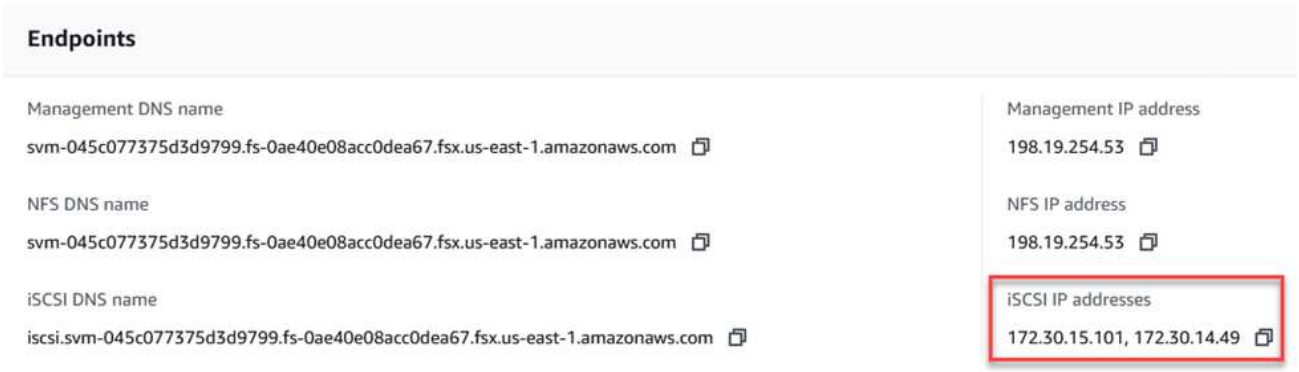
3. 最後，將 LUN 對應到剛剛建立的啟動器群組：

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

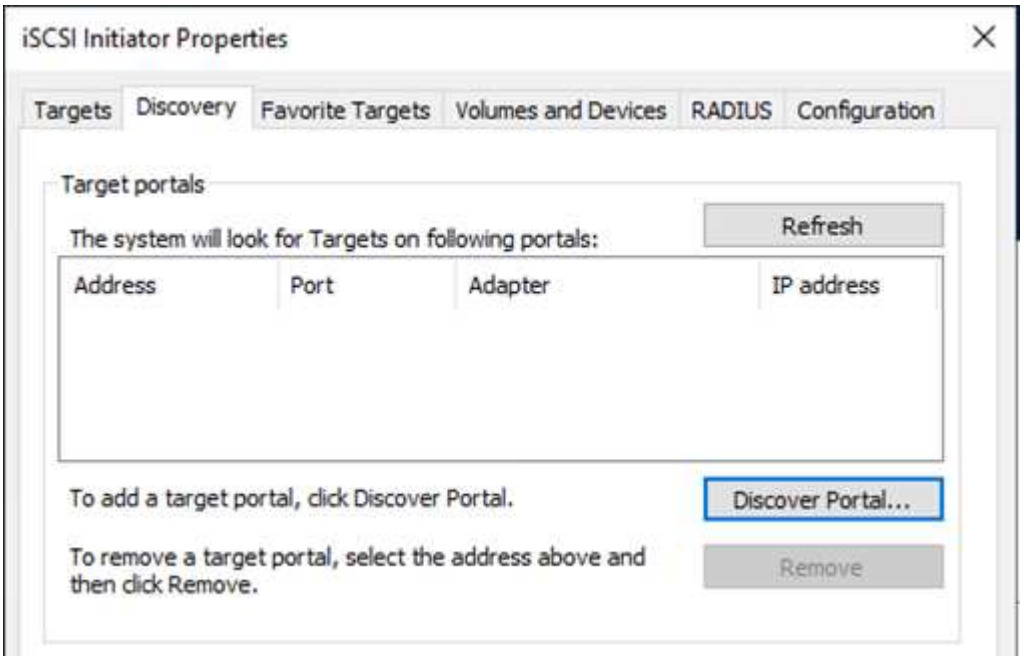
4. 若要尋找路徑名，請運行 `lun show`命令。

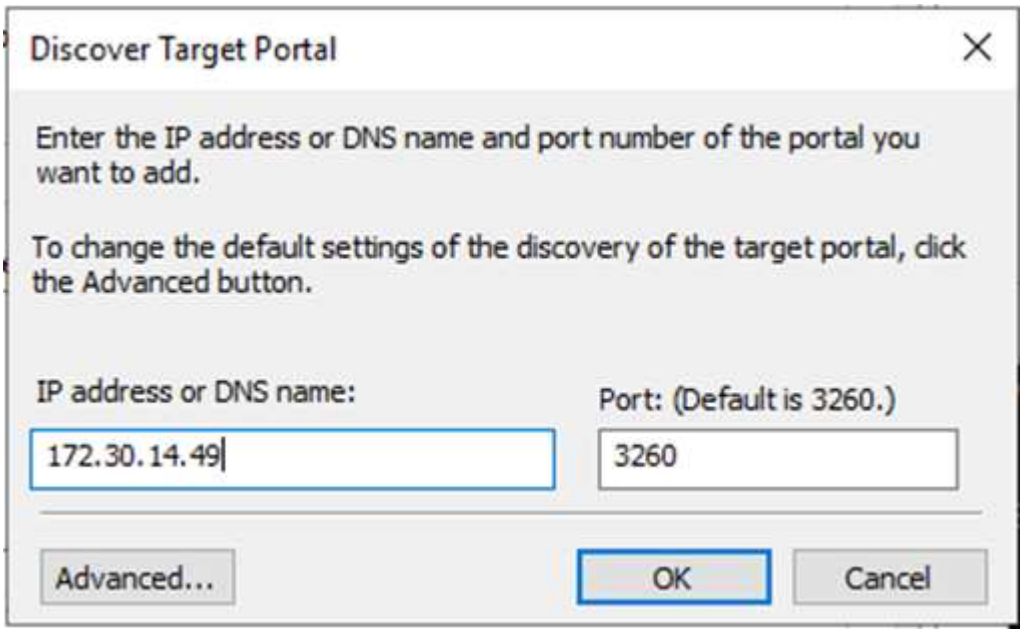
▼ 設定 **Windows VM** 以進行 **iSCSI** 存取並發現檔案系統

1. 從 SQL Server VM 中，設定您的 iSCSI 網路適配器，以便在已建立與 FSx 執行個體上的 iSCSI 目標介面連接的 VMware 連接埠群組上進行通訊。
2. 開啟 iSCSI 啟動器屬性公用程式並清除「發現」、「收藏目標」和「目標」標籤上的舊連線設定。
3. 尋找用於存取 FSx 實例/叢集上的 iSCSI 邏輯介面的 IP 位址。這可以在 AWS 控制台的Amazon FSx > ONTAP > Storage Virtual Machines 下找到。

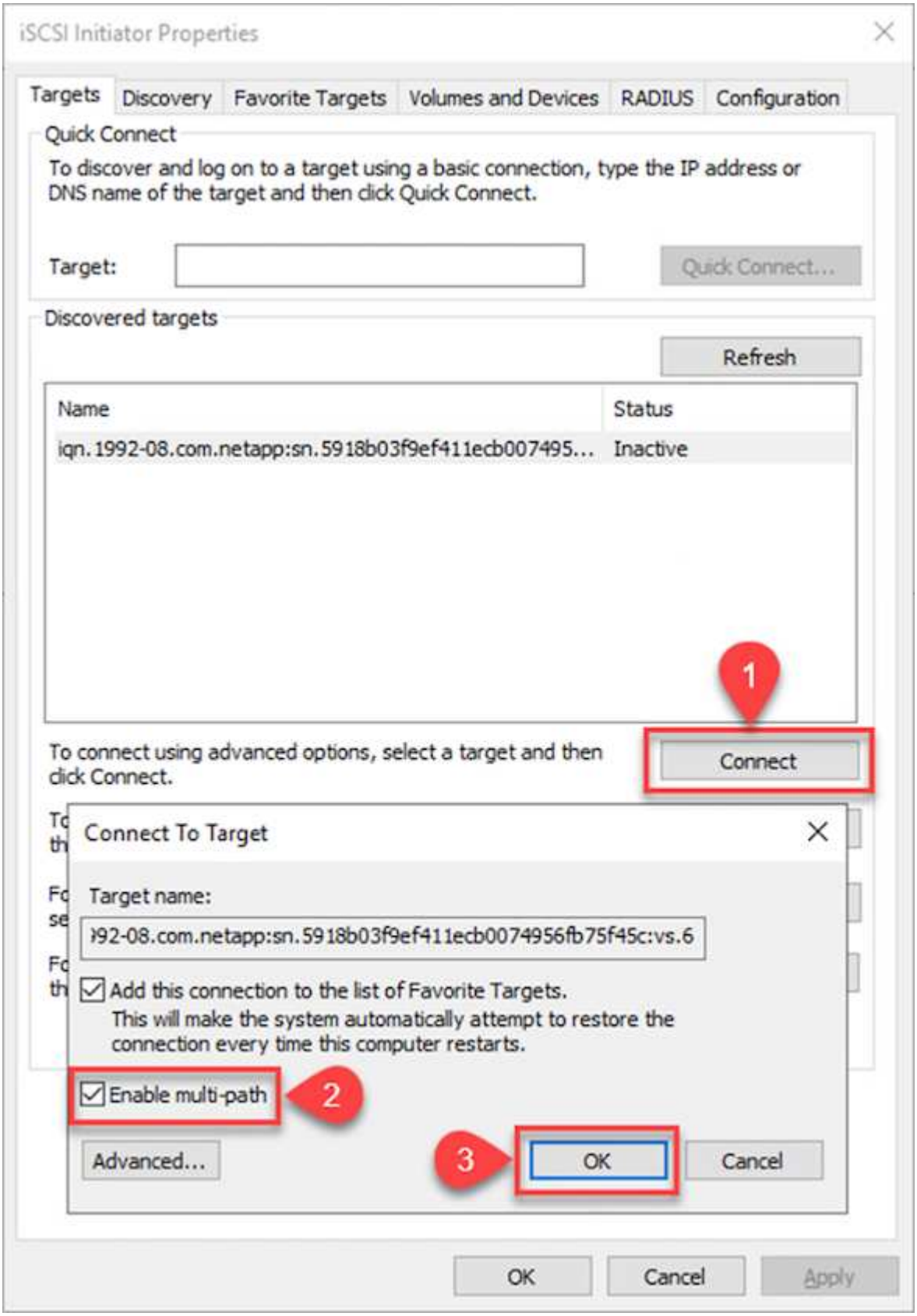


4. 在「發現」標籤中，按一下「發現入口網站」並輸入 FSx iSCSI 目標的 IP 位址。

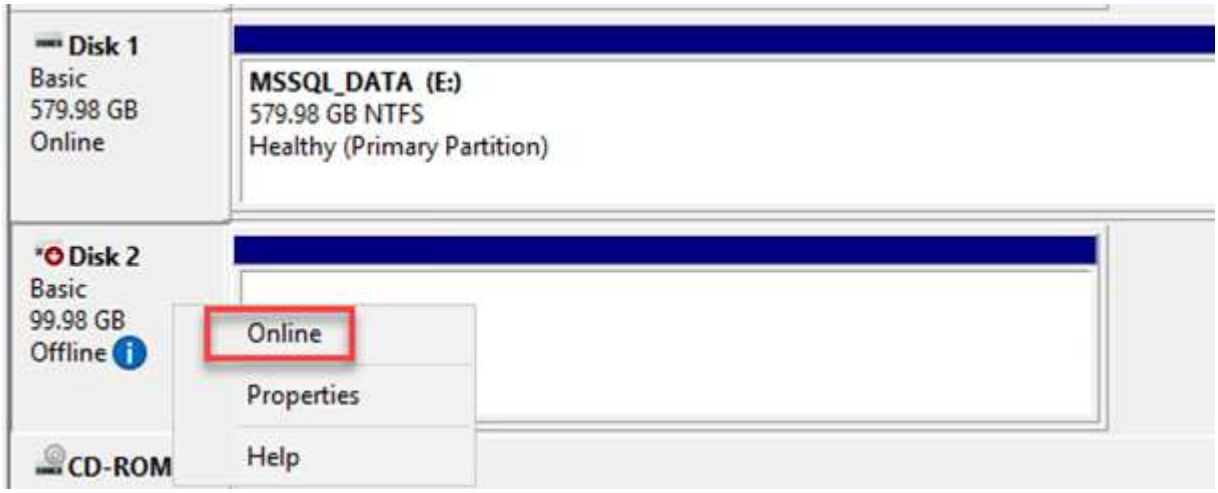




5. 在目標標籤上，按一下連接，如果適合您的配置，請選擇啟用多路徑，然後按一下確定以連接到目標。

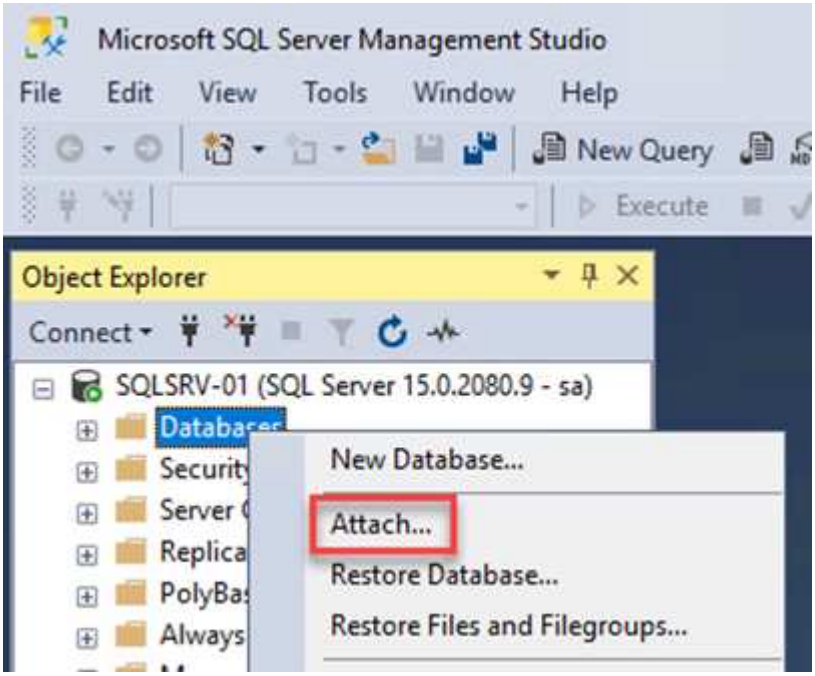


6. 開啟電腦管理公用程式並使磁碟連線。驗證它們是否保留了先前的相同磁碟機號。

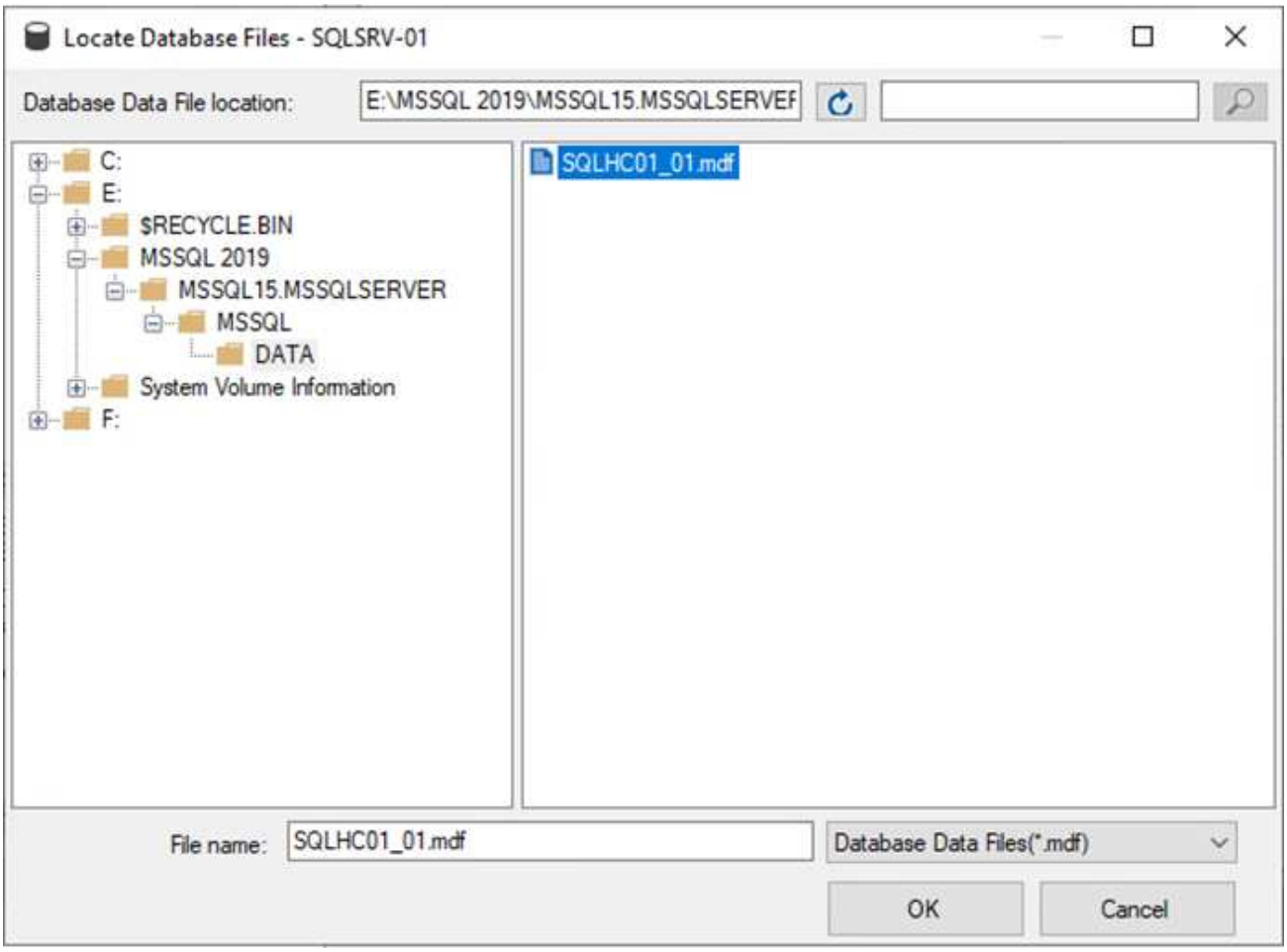


▼ 附加 **SQL Server** 資料庫

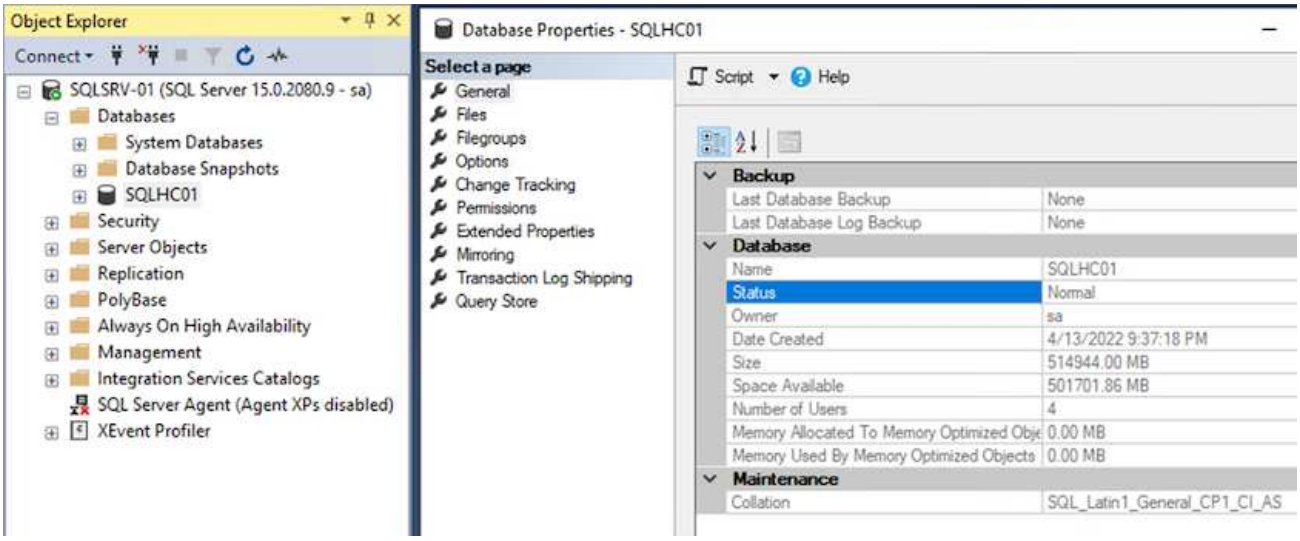
1. 從 SQL Server VM 中，開啟 Microsoft SQL Server Management Studio 並選擇「附加」以開始連接資料庫的程序。



2. 按一下「新增」並導覽至包含 SQL Server 主資料庫檔案的資料夾，選擇它，然後按一下「確定」。



3. 如果交易日誌位於單獨的磁碟機上，請選擇包含交易日誌的資料夾。
4. 完成後，按一下“確定”以附加資料庫。



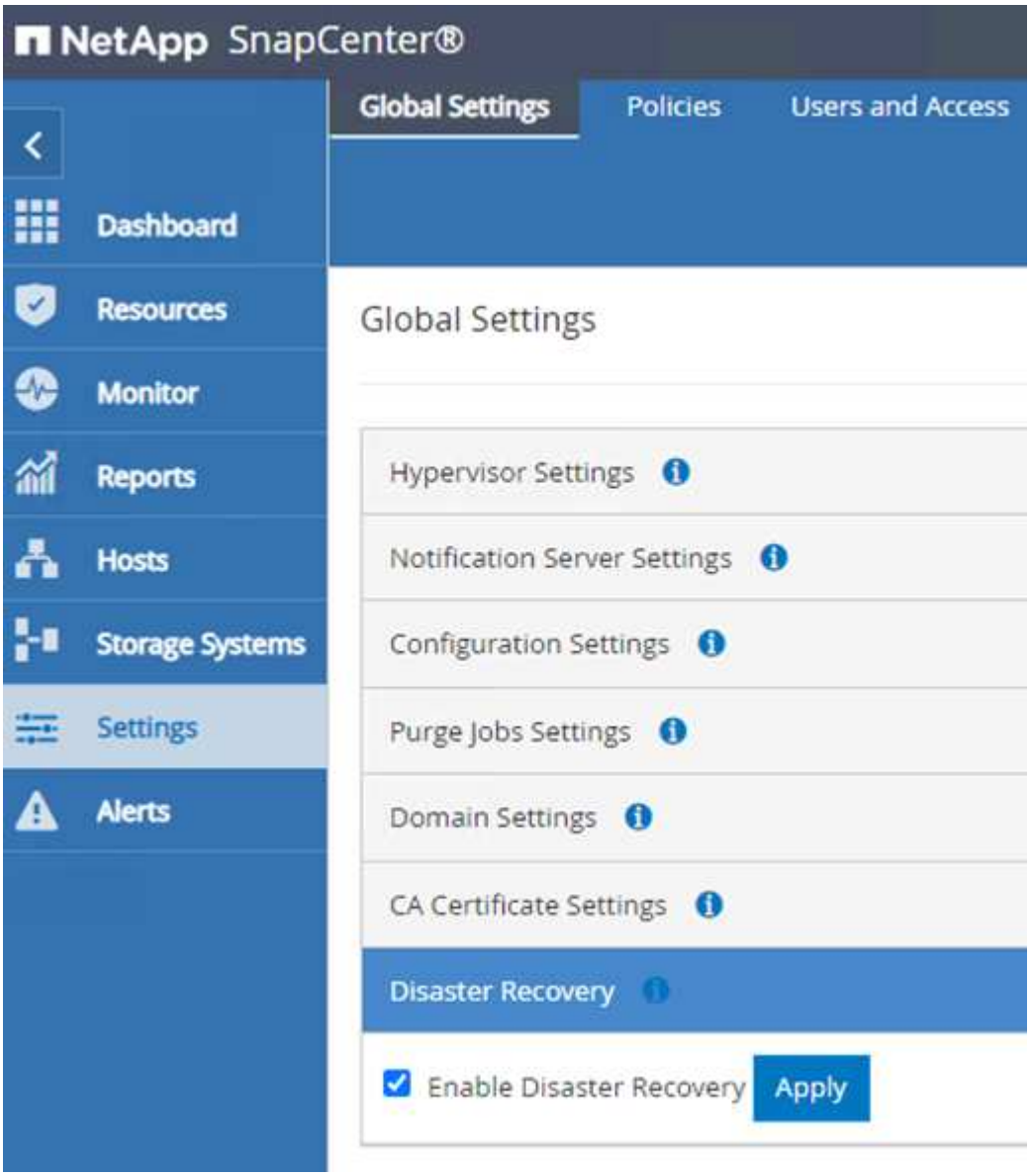
▼ 確認**SnapCenter**與 **SQL Server** 外掛程式的通信

當SnapCenter資料庫還原到先前的狀態時，它會自動重新發現 SQL Server 主機。為了使其正常工作，請記住以下先決條件：

- SnapCenter必須處於災難復原模式。這可以透過 Swagger API 或在災難復原下的全域設定中完成。

- SQL Server 的 FQDN 必須與在本機資料中心執行的執行個體相同。
- 必須破壞原始的SnapMirror關係。
- 必須將包含資料庫的 LUN 安裝到 SQL Server 執行個體並附加資料庫。

若要確認SnapCenter處於災難復原模式，請從SnapCenter Web 用戶端導覽至「設定」。轉到“全域設定”選項卡，然後按一下“災難復原”。確保啟用災難復原複選框已啟用。



恢復 **Oracle** 應用程式數據

以下流程提供了有關在發生導致本地站點無法運行的災難時如何在 AWS 中的 VMware Cloud Services 中還原 Oracle 應用程式資料的說明。

完成以下先決條件以繼續執行復原步驟：

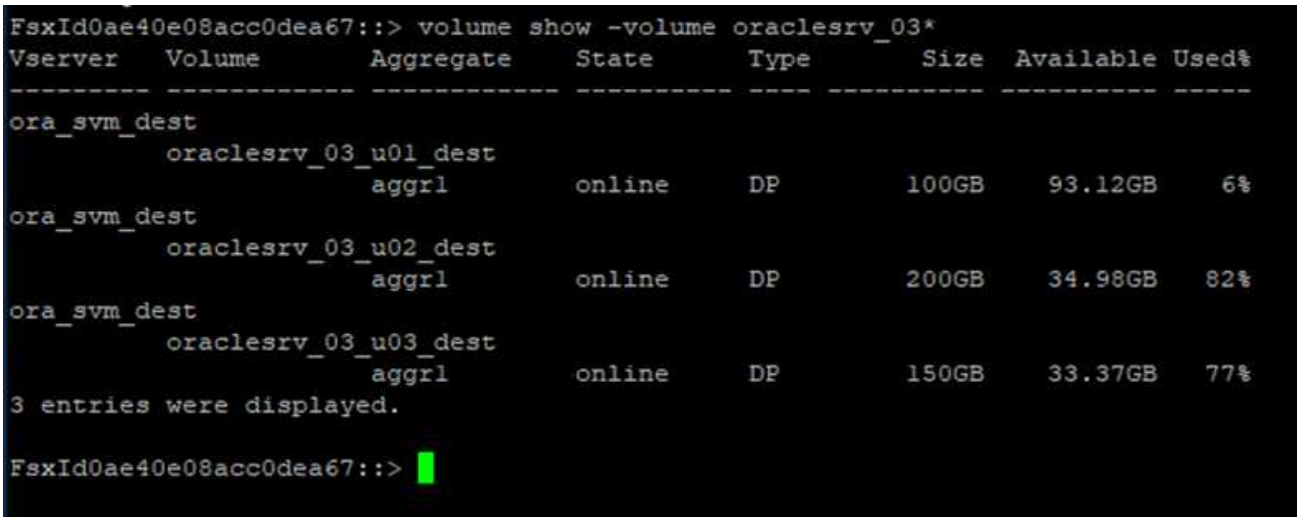
1. Oracle Linux 伺服器 VM 已使用 Veeam Full Restore 還原至 VMware Cloud SDDC。
2. 已建立輔助SnapCenter伺服器，並已使用本節概述的步驟恢復SnapCenter資料庫和設定文件"SnapCenter備份和復原過程摘要。"

▼ 設定 **FSx for Oracle** 還原 **–** 中斷**SnapMirror**關係

若要讓 Oracle 伺服器可以存取 FSx ONTAP執行個體上所託管的二級儲存卷，您必須先中斷現有的SnapMirror關係。

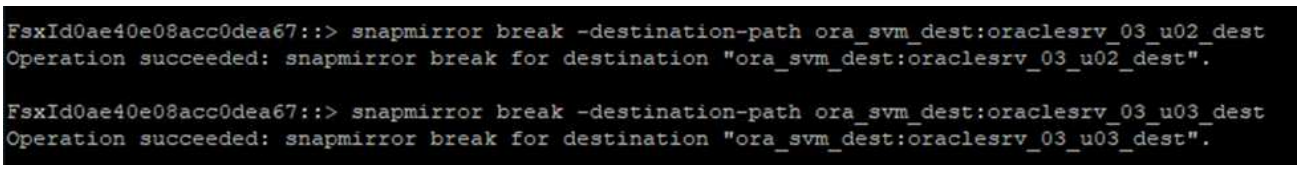
1. 登入 FSx CLI 後，執行以下命令以查看按正確名稱過濾的磁碟區。

```
FSx-Dest::> volume show -volume VolumeName*
```

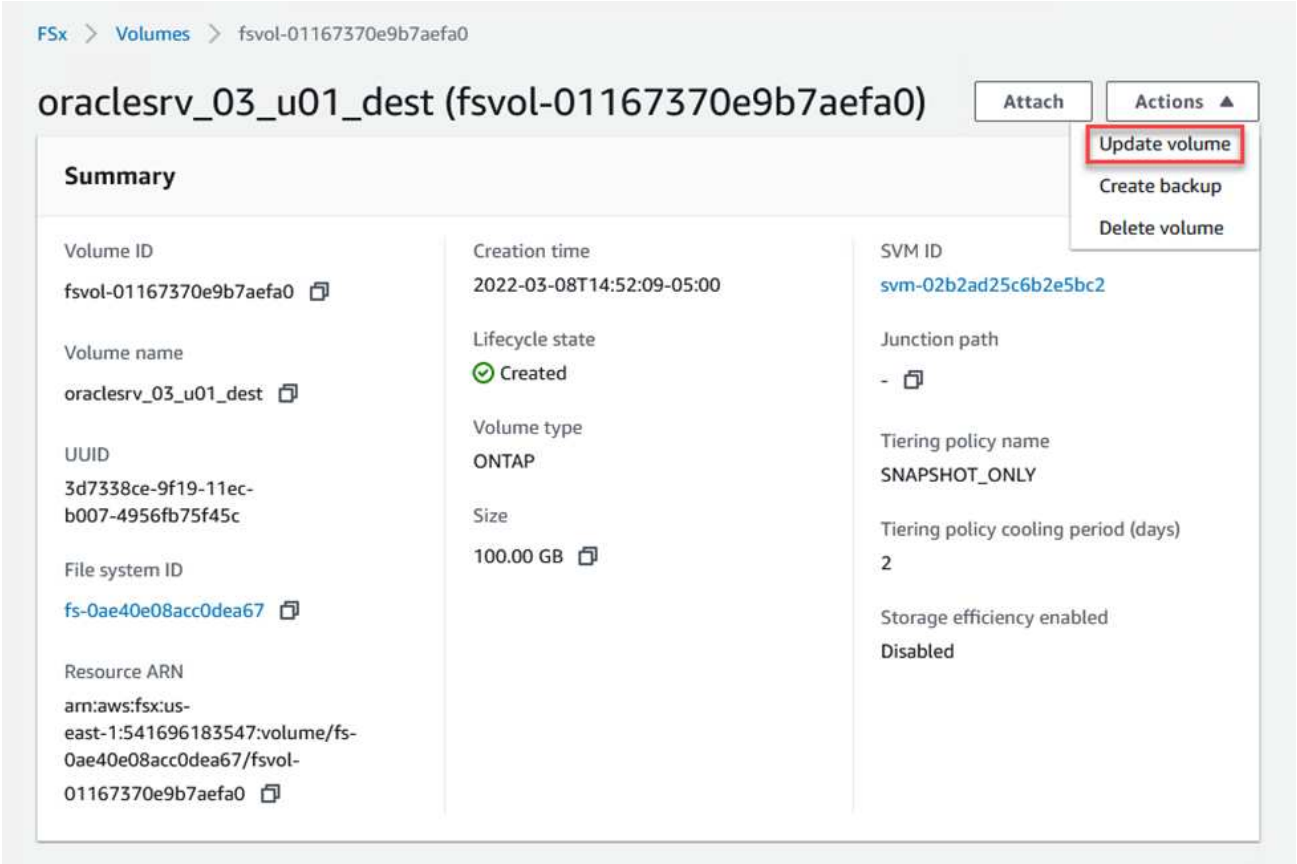


2. 執行以下命令來中斷現有的SnapMirror關係。

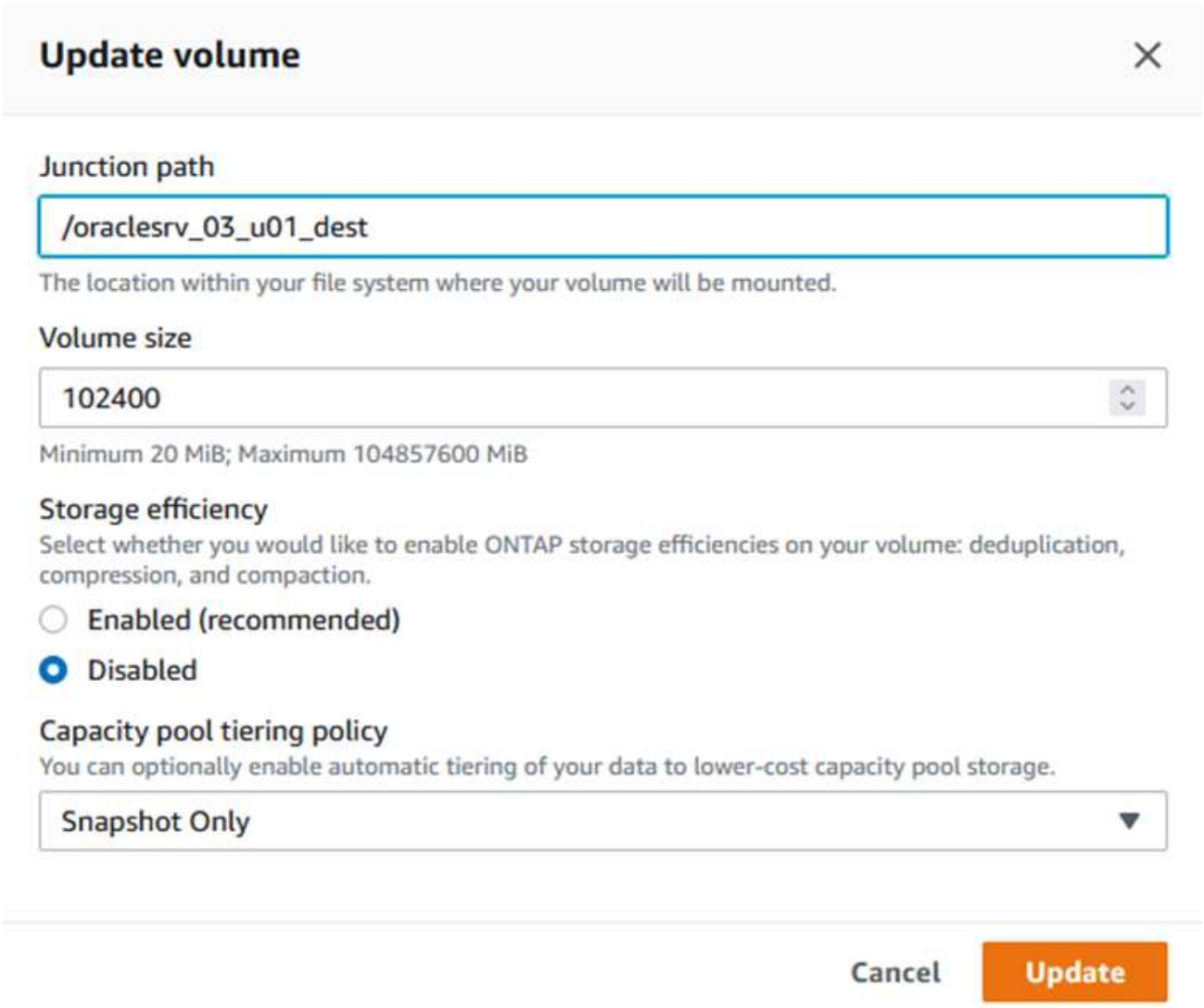
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```



3. 更新Amazon FSx Web 用戶端中的連線路徑：



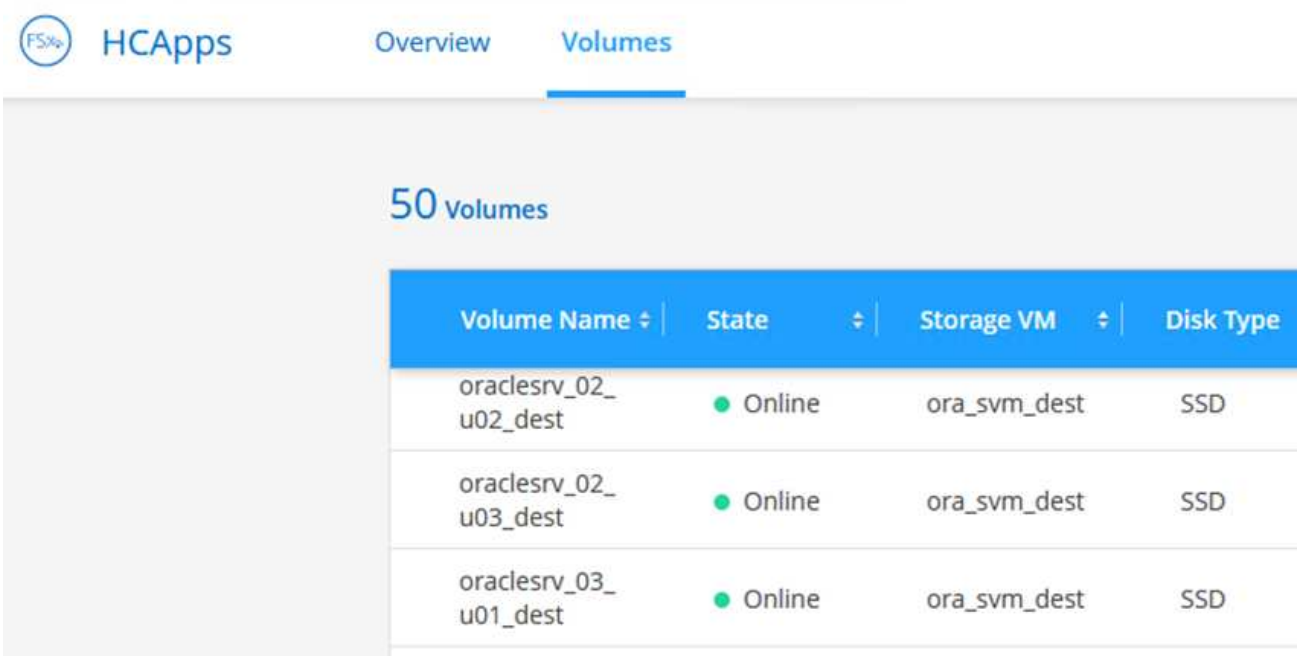
4. 新增連接路徑名稱並按一下更新。從 Oracle 伺服器掛載 NFS 磁碟區時指定此連線路徑。



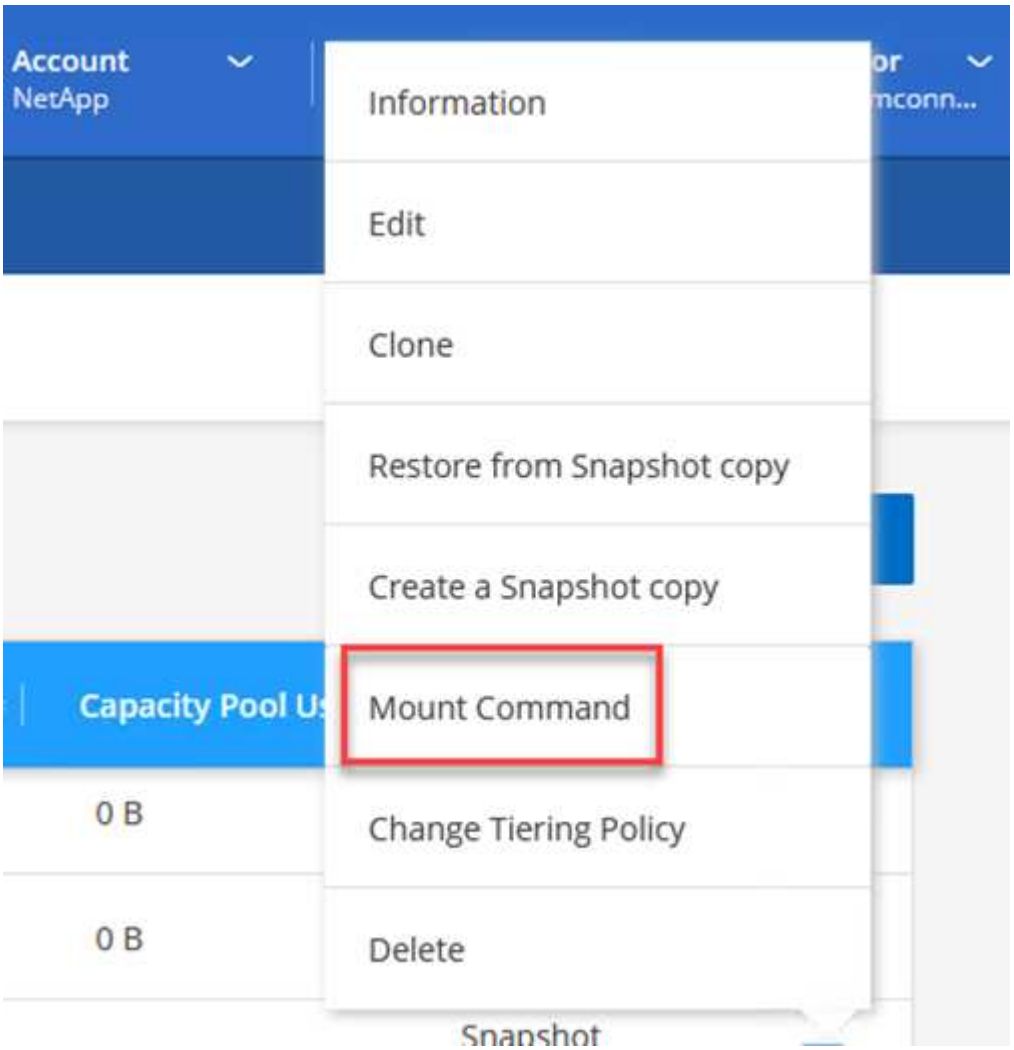
▼ 在 **Oracle** 伺服器上掛載 **NFS** 卷

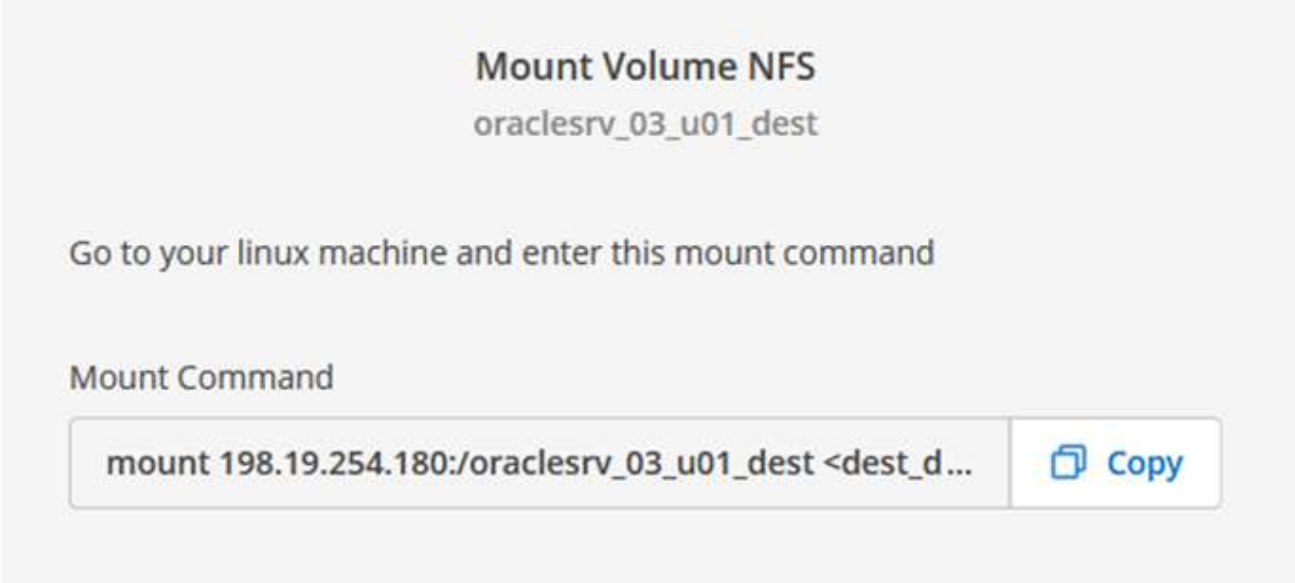
在 Cloud Manager 中，您可以取得具有正確 NFS LIF IP 位址的掛載命令，以掛載包含 Oracle 資料庫檔案和日誌的 NFS 磁碟區。

1. 在雲端管理器中，存取 FSx 叢集的磁碟區清單。



2. 從操作選單中，選擇「掛載命令」以查看和複製要在我們的 Oracle Linux 伺服器上使用的掛載命令。





3. 將 NFS 檔案系統掛載到 Oracle Linux 伺服器。用於掛載 NFS 共享的目錄已存在於 Oracle Linux 主機上。
4. 從 Oracle Linux 伺服器，使用 mount 指令掛載 NFS 磁碟區。

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

對與 Oracle 資料庫關聯的每個磁碟區重複此步驟。

若要讓 NFS 掛載在重新啟動後持久化，請編輯 `/etc/fstab`文件以包含掛載命令。

5. 重新啟動 Oracle 伺服器。 Oracle 資料庫應該會正常啟動並可供使用。

故障回覆

成功完成此解決方案中概述的故障轉移過程後， SnapCenter和 Veeam 將恢復在 AWS 中運行的備份功能，並且FSx ONTAP現在被指定為主存儲，與原始內部部署資料中心不存在現有的SnapMirror關係。在本機恢復正常功能後，您可以使用與本文檔中概述的流程相同的流程將資料鏡像回本機ONTAP儲存系統。

如本文檔中所概述的，您可以設定SnapCenter將應用程式資料磁碟區從 FSx ONTAP鏡像到位於本機的ONTAP儲存系統。類似地，您可以設定 Veeam 使用橫向擴充備份儲存庫將備份副本複製到 Amazon S3，以便位於本機資料中心的 Veeam 備份伺服器可以存取這些備份。

故障回復超出了本文檔的範圍，但故障回復與此處概述的詳細過程略有不同。

結論

本文檔中介紹的用例重點關注經過驗證的災難復原技術，突顯了NetApp和 VMware 之間的整合。 NetApp ONTAP儲存系統提供成熟的資料鏡像技術，使組織能夠設計涵蓋本地和領先雲端供應商所採用的ONTAP技術的災難復原解決方案。

AWS 上的 FSx ONTAP就是這樣一種解決方案，它允許與SnapCenter和SyncMirror無縫集成，以將應用程式資料複製到雲端。 Veeam Backup & Replication 是另一項知名技術，它與NetApp ONTAP儲存系統很好地集成，

並可以為 vSphere 原生儲存提供故障轉移。

該解決方案提供了一種災難復原解決方案，使用託管 SQL Server 和 Oracle 應用程式資料的ONTAP系統的客戶連接儲存。具有SnapMirror的SnapCenter提供了一個易於管理的解決方案，用於保護ONTAP系統上的應用程式磁碟區並將其複製到駐留在雲端中的 FSx 或 CVO。 SnapCenter是一種支援 DR 的解決方案，可將所有應用程式資料故障轉移到 AWS 上的 VMware Cloud。

VMware Cloud 中的 **Veeam** 備份與還原，搭配**Amazon FSx ONTAP**

Veeam Backup & Replication 是保護 VMware Cloud 中資料的有效且可靠的解決方案。此解決方案示範了使用 Veeam Backup and Replication 備份和還原 VMware Cloud 中 FSx ONTAP NFS 資料儲存區上的應用程式虛擬機器的正確設定和配置。

概況

VMware Cloud（在 AWS 中）支援使用 NFS 資料儲存作為補充存儲，而 FSx ONTAP對於需要為其雲端應用程式儲存大量資料的客戶來說是一種安全的解決方案，並且可以獨立於 SDDC 叢集中的 ESXi 主機數量進行擴展。此整合的 AWS 儲存服務提供高效率儲存以及所有傳統的NetApp ONTAP功能。

用例

此解決方案適用於以下用例：

- 使用 FSx ONTAP作為備份儲存庫，備份和還原 VMC 中託管的 Windows 和 Linux 虛擬機器。
- 使用 FSx ONTAP作為備份儲存庫備份和還原 Microsoft SQL Server 應用程式資料。
- 使用 FSx ONTAP作為備份儲存庫備份和還原 Oracle 應用程式資料。

使用**Amazon FSx ONTAP** 的**NFS** 資料存儲

此解決方案中的所有虛擬機器都駐留在 FSx ONTAP補充 NFS 資料儲存上。使用 FSx ONTAP作為補充 NFS 資料儲存有幾個好處。例如，它允許您：

- 在雲端中建立可擴展且高度可用的檔案系統，無需複雜的設定和管理。
- 與您現有的 VMware 環境集成，可讓您使用熟悉的工具和流程來管理您的雲端資源。
- 利用ONTAP提供的進階資料管理功能（例如快照和複製）來保護您的資料並確保其可用性。

▼ 解決方案部署概述

此清單提供了配置 Veeam Backup & Replication、使用 FSx ONTAP作為備份儲存庫執行備份和還原作業以及執行 SQL Server 和 Oracle VM 和資料庫還原所需的進階步驟：

1. 建立 FSx ONTAP檔案系統，用作 Veeam Backup & Replication 的 iSCSI 備份儲存庫。
2. 部署 Veeam Proxy 以指派備份工作負載並掛載 FSx ONTAP上託管的 iSCSI 備份儲存庫。
3. 設定 Veeam Backup Jobs 來備份 SQL Server、Oracle、Linux 和 Windows 虛擬機器。
4. 還原 SQL Server 虛擬機器和單一資料庫。
5. 復原 Oracle 虛擬機器和單一資料庫。

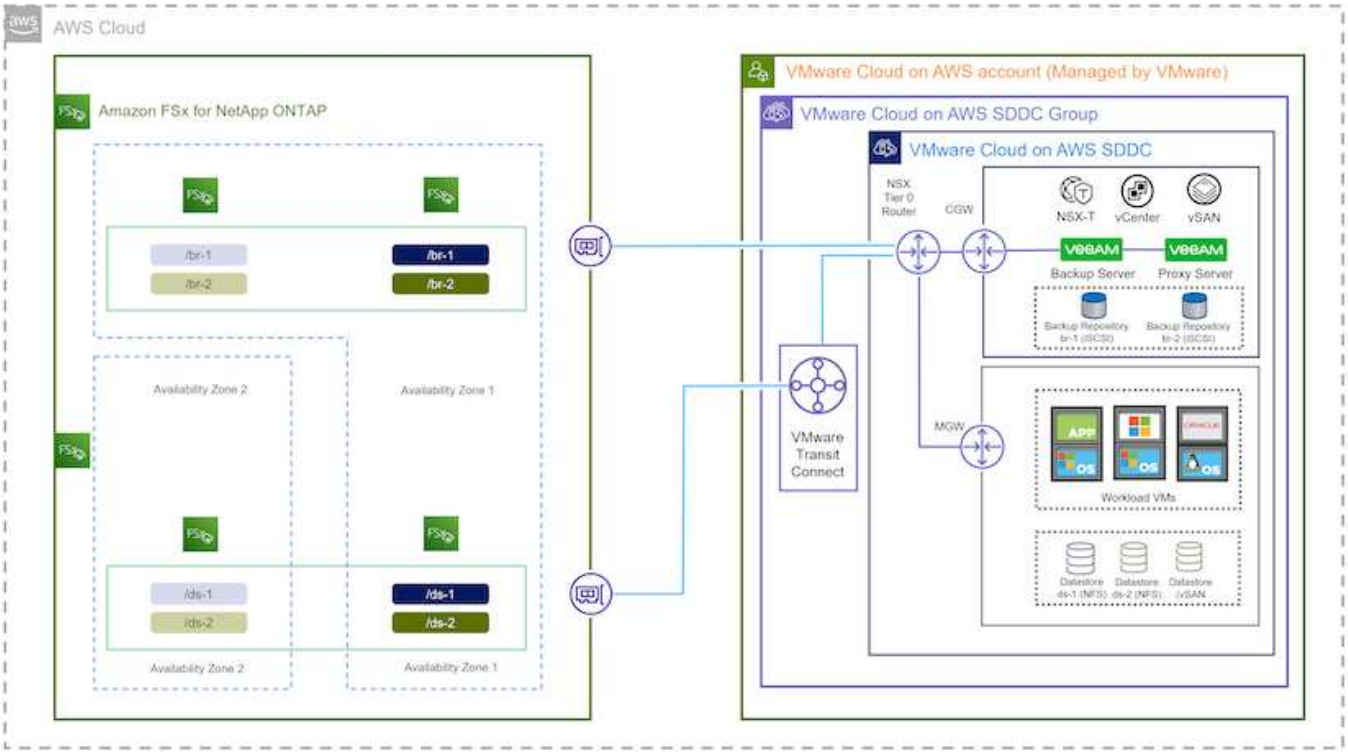
▼ 先決條件

此解決方案的目的是展示在 VMware Cloud 中運行並位於 FSx ONTAP託管的 NFS 資料儲存上的虛擬機器的資料保護。此解決方案假定以下組件已配置並可供使用：

1. 具有一個或多個連接到 VMware Cloud 的 NFS 資料儲存的 FSx ONTAP檔案系統。
2. 安裝了 Veeam Backup & Replication 軟體的 Microsoft Windows Server VM。
   - Veeam Backup & Replication 伺服器已使用其 IP 位址或完全限定網域名稱來發現 vCenter 伺服器。
3. 在解決方案部署期間，Microsoft Windows Server VM 將與 Veeam Backup Proxy 元件一起安裝。
4. 具有 VMDK 和應用程式資料的 Microsoft SQL Server VM 駐留在 FSx ONTAP NFS 資料儲存區上。對於此解決方案，我們在兩個獨立的 VMDK 上有兩個 SQL 資料庫。
   - 注意：最佳實踐是將資料庫和交易日誌檔案放在單獨的磁碟機上，因為這將提高效能和可靠性。部分原因是由於交易日誌是按順序寫入的，而資料庫檔案是隨機寫入的。
5. 具有 VMDK 和應用程式資料的 Oracle 資料庫虛擬機器駐留在 FSx ONTAP NFS 資料儲存區上。
6. 具有 VMDK 的 Linux 和 Windows 檔案伺服器虛擬機器駐留在 FSx ONTAP NFS 資料儲存區上。
7. Veeam 需要特定的 TCP 連接埠來實現備份環境中的伺服器和元件之間的通訊。在 Veeam 備份基礎架構元件上，會自動建立所需的防火牆規則。有關網路連接埠要求的完整列表，請參閱 "適用於 VMware vSphere 的 Veeam Backup and Replication 使用者指南"。

進階架構

該解決方案的測試/驗證是在實驗室中進行的，該實驗室可能與最終部署環境相匹配，也可能不匹配。欲了解更多信息，請參閱以下章節。



▼ 硬體/軟體組件

此解決方案的目的是展示在 VMware Cloud 中運行並位於 FSx ONTAP託管的 NFS 資料儲存上的虛擬機器的資料保護。此解決方案假定以下組件已配置並可供使用：

- 位於 FSx ONTAP NFS 資料儲存體上的 Microsoft Windows VM
- 位於 FSx ONTAP NFS 資料儲存上的 Linux (CentOS) VM
- 位於 FSx ONTAP NFS 資料儲存上的 Microsoft SQL Server VM
  - 兩個資料庫託管在不同的 VMDK 上
- 位於 FSx ONTAP NFS 資料儲存上的 Oracle VM

解決方案部署

在此解決方案中，我們提供了有關部署和驗證解決方案的詳細說明，該解決方案利用 Veeam Backup 和 Replication 軟體在 AWS 上的 VMware Cloud SDDC 中執行 SQL Server、Oracle 以及 Windows 和 Linux 檔案伺服器虛擬機器的備份和復原。此解決方案中的虛擬機器駐留在由 FSx ONTAP託管的補充 NFS 資料儲存上。此外，單獨的 FSx ONTAP檔案系統用於託管將用於 Veeam 備份儲存庫的 iSCSI 磁碟區。

我們將介紹 FSx ONTAP檔案系統的建立、掛載 iSCSI 磁碟區以用作備份儲存庫、建立和執行備份作業以及執行 VM 和資料庫復原。

有關 FSx ONTAP的詳細信息，請參閱 "FSx ONTAP使用者指南"。

有關 Veeam Backup and Replication 的詳細信息，請參閱 "Veeam 幫助中心技術文檔"地點。

有關在 VMware Cloud on AWS 上使用 Veeam Backup and Replication 時的注意事項與限制，請參閱 "VMware Cloud on AWS 和 VMware Cloud on Dell EMC 支援。注意事項和限制"。

部署 **Veeam** 代理伺服器

Veeam 代理伺服器是 Veeam Backup & Replication 軟體的一個元件，可作為來源和備份或複製目標之間的中介。代理伺服器透過在本機處理資料來協助最佳化和加速備份作業期間的資料傳輸，並且可以使用不同的傳輸模式透過 VMware vStorage API 進行資料保護或透過直接儲存存取來存取資料。

在選擇 Veeam 代理伺服器設計時，重要的是考慮並發任務的數量以及所需的傳輸模式或儲存存取類型。

有關代理伺服器數量及其係統需求，請參閱 "Veeam VMware vSphere 最佳實務指南"。

Veeam Data Mover 是 Veeam Proxy Server 的元件，它利用傳輸模式作為從來源取得 VM 資料並將其傳輸到目標的方法。傳輸模式是在備份作業配置期間指定的。透過使用直接儲存訪問，可以提高 NFS 資料儲存的備份效率。

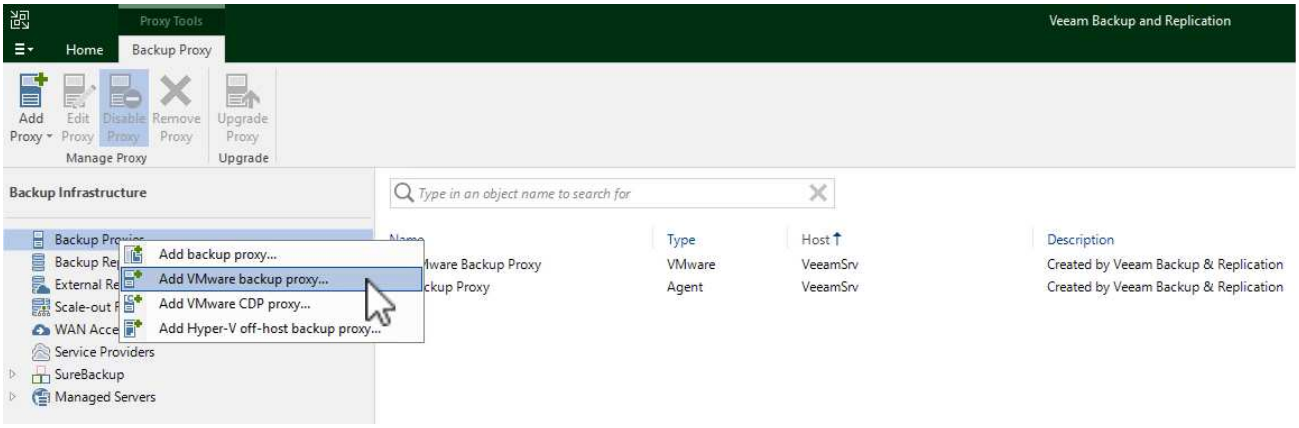
有關運輸方式的更多信息，請參閱 "適用於 VMware vSphere 的 Veeam Backup and Replication 使用者指南"。

在下一步中，我們將介紹在 VMware Cloud SDDC 中的 Windows VM 上部署 Veeam 代理伺服器。

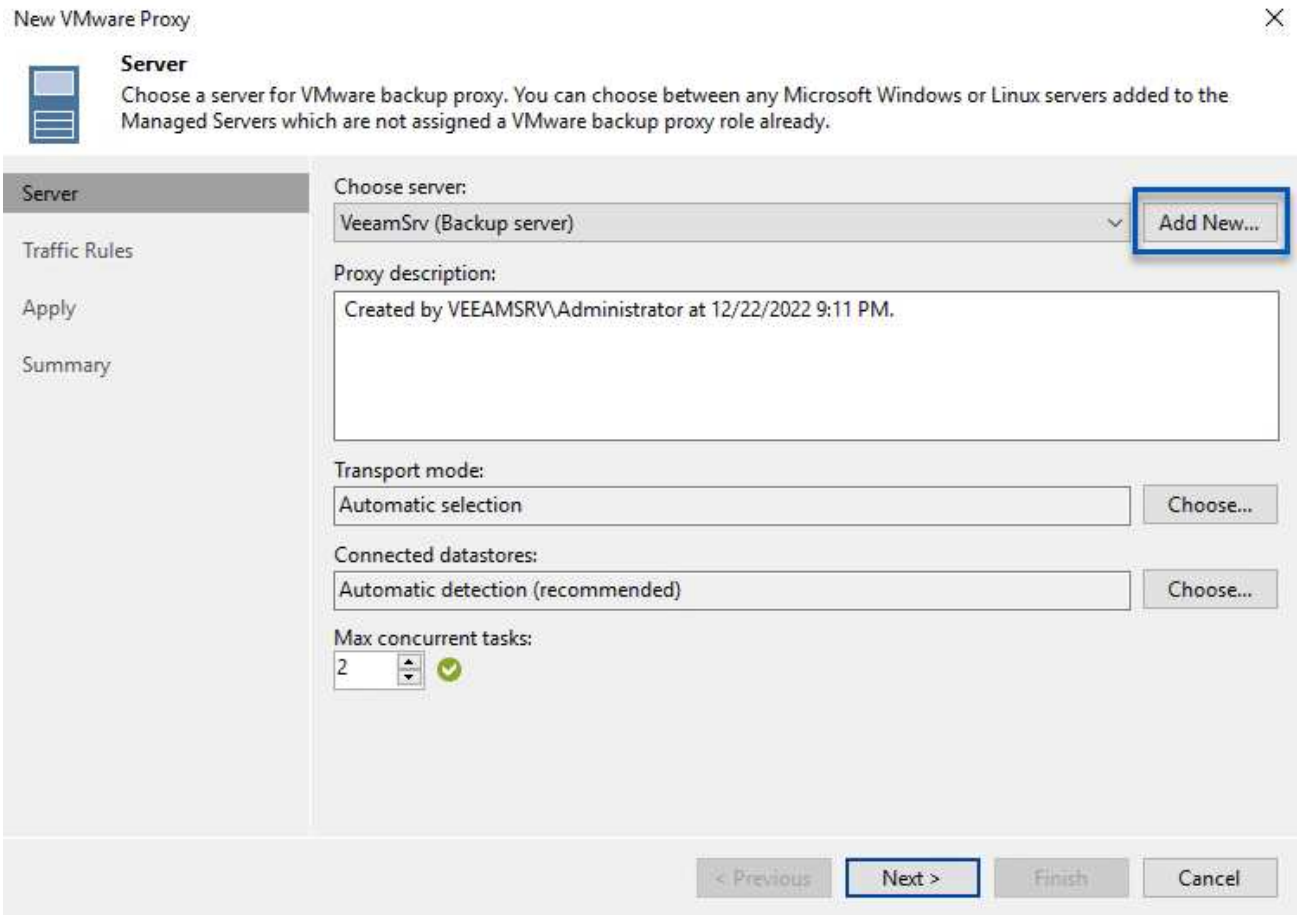
▼ 部署 **Veeam Proxy** 以分配備份工作負載

在此步驟中，Veeam Proxy 被部署到現有的 Windows VM。這允許備份作業在主 Veeam 備份伺服器和 Veeam 代理之間分配。

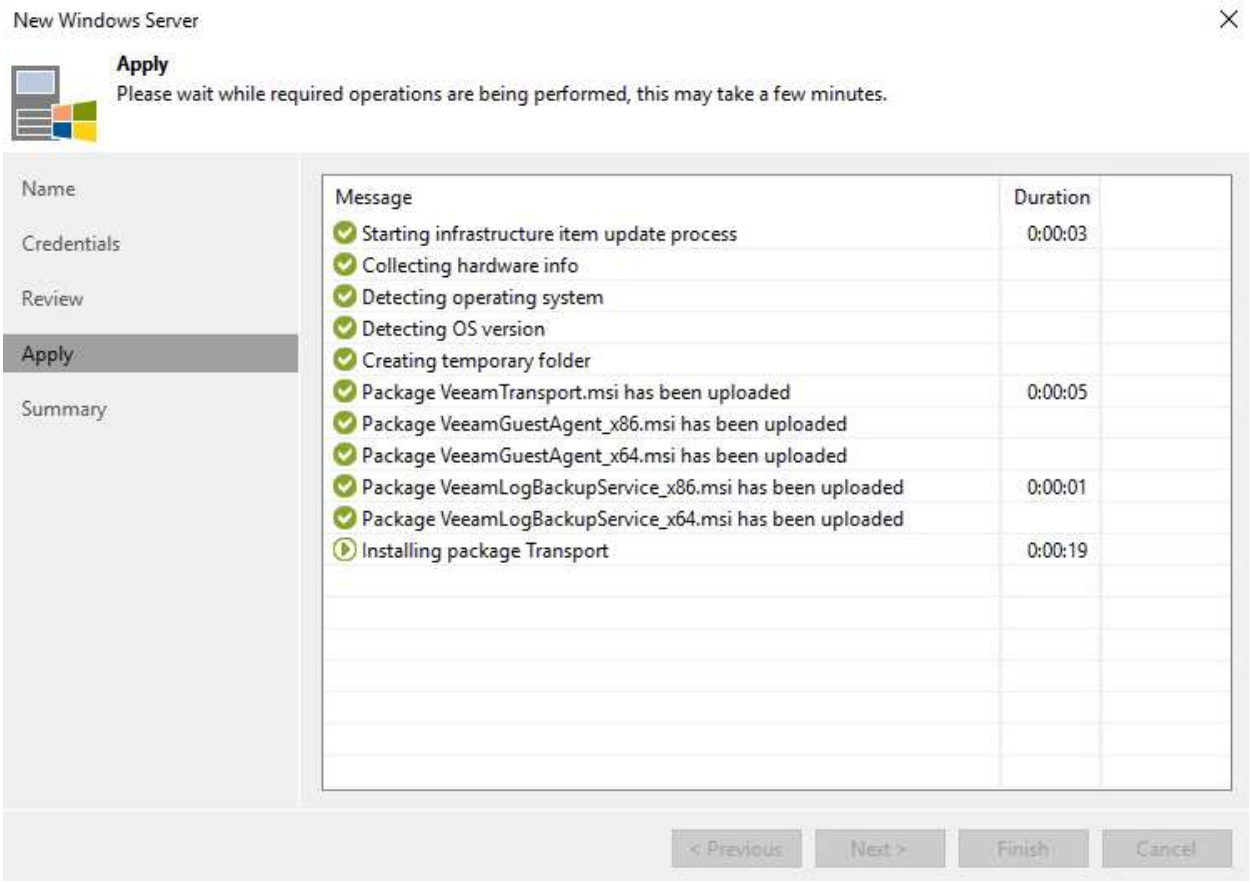
1. 在 Veeam Backup and Replication 伺服器上，開啟管理控制台並在左下角選單中選擇 **Backup Infrastructure**。
2. 右鍵單擊“備份代理”，然後按一下“新增 **VMware** 備份代理程式...”以開啟精靈。



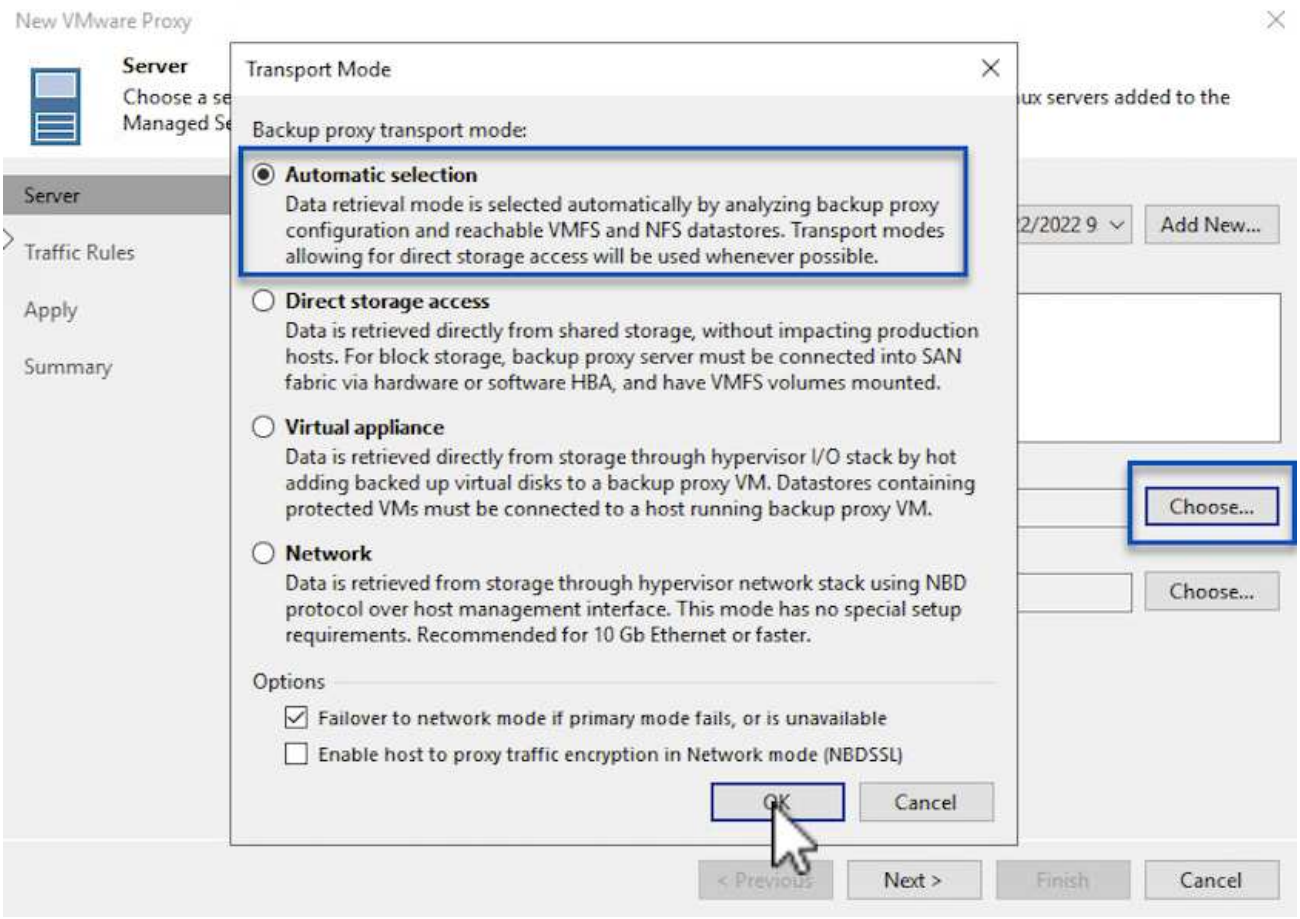
3. 在「新增 VMware 代理程式」精靈中，按一下「新增...」按鈕以新增新的代理伺服器。



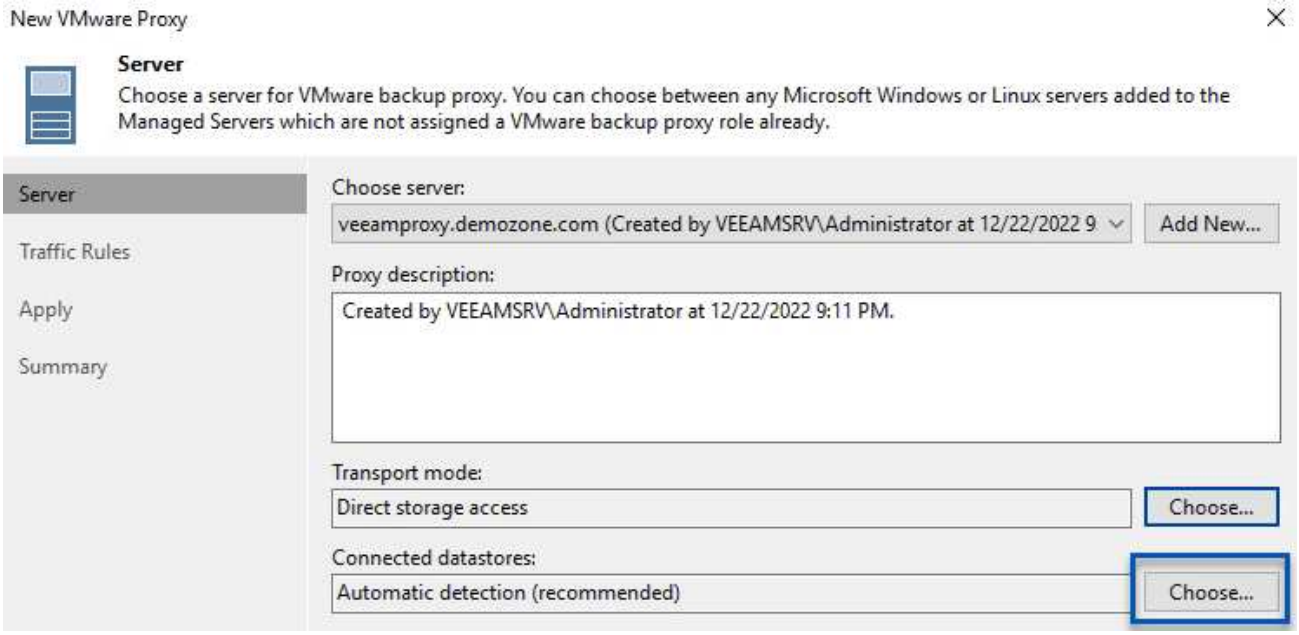
4. 選擇新增Microsoft Windows並依照指示新增伺服器：
   - 填寫DNS名稱或IP位址
   - 選擇新系統上用於憑證的帳戶或新增憑證
   - 檢查要安裝的元件，然後按一下「套用」開始部署

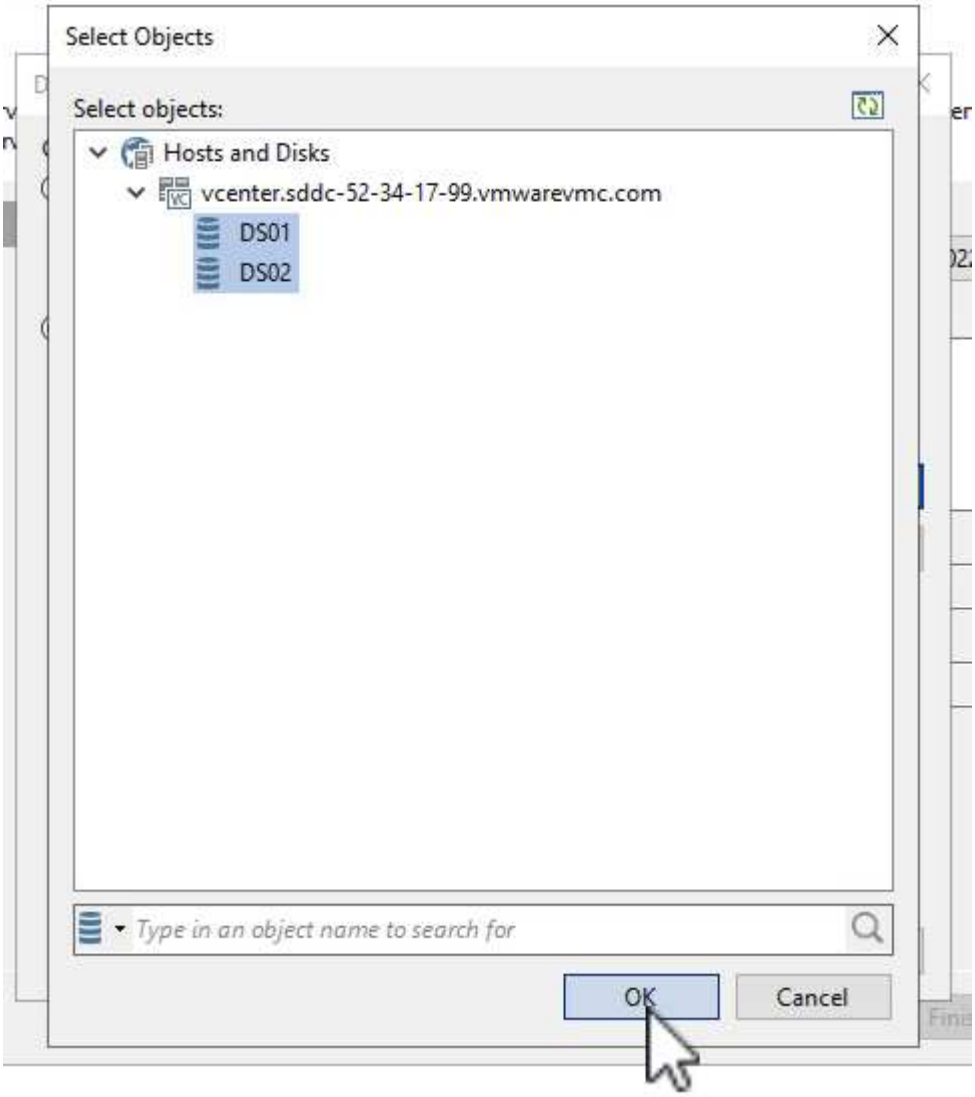


5. 返回「新 VMware 代理程式」精靈，選擇傳輸模式。在我們的例子中，我們選擇了*自動選擇*。

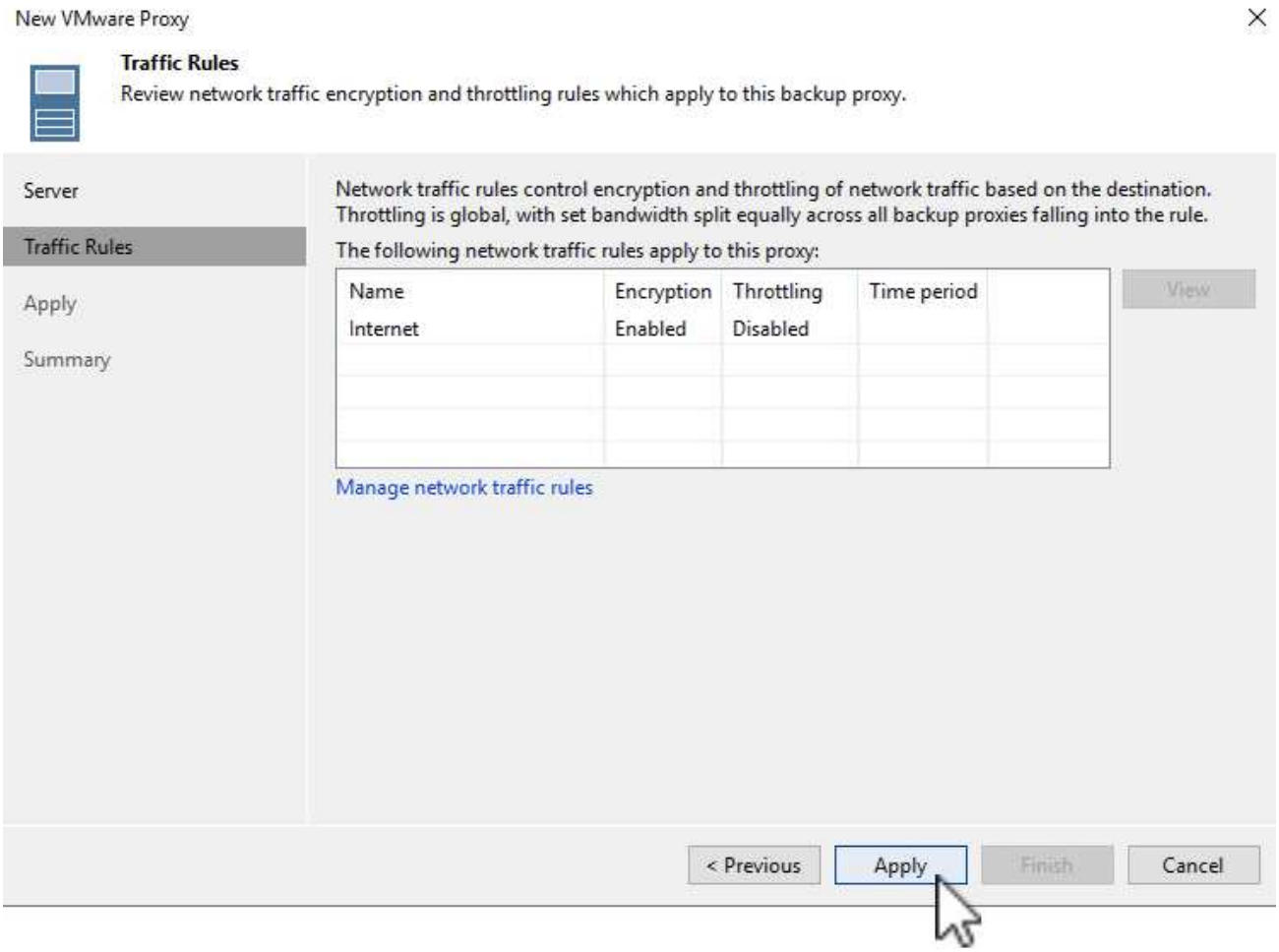


6. 選擇您希望 VMware 代理直接存取的已連接資料儲存。





7. 配置並套用所需的任何特定網路流量規則，例如加密或限制。完成後點選「應用」按鈕即可完成部署。



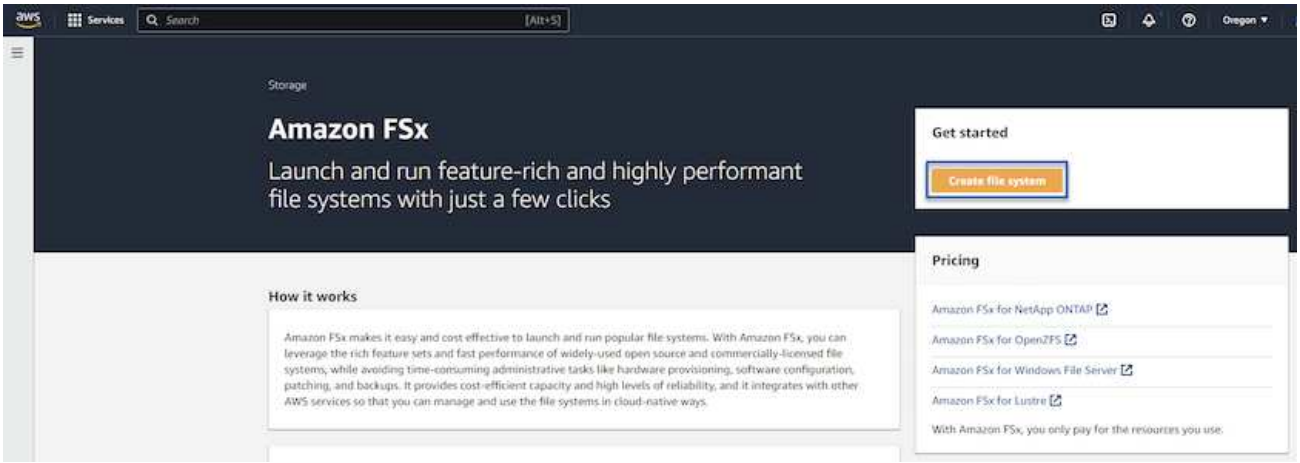
配置儲存和備份儲存庫

主 Veeam Backup 伺服器和 Veeam Proxy 伺服器可以以直接連接儲存空間的形式存取備份儲存庫。在本節中，我們介紹如何建立 FSx ONTAP檔案系統、將 iSCSI LUN 安裝到 Veeam 伺服器以及建立備份儲存庫。

▼ 建立 **FSx ONTAP**檔案系統

建立一個 FSx ONTAP檔案系統，用於託管 Veeam 備份儲存庫的 iSCSI 磁碟區。

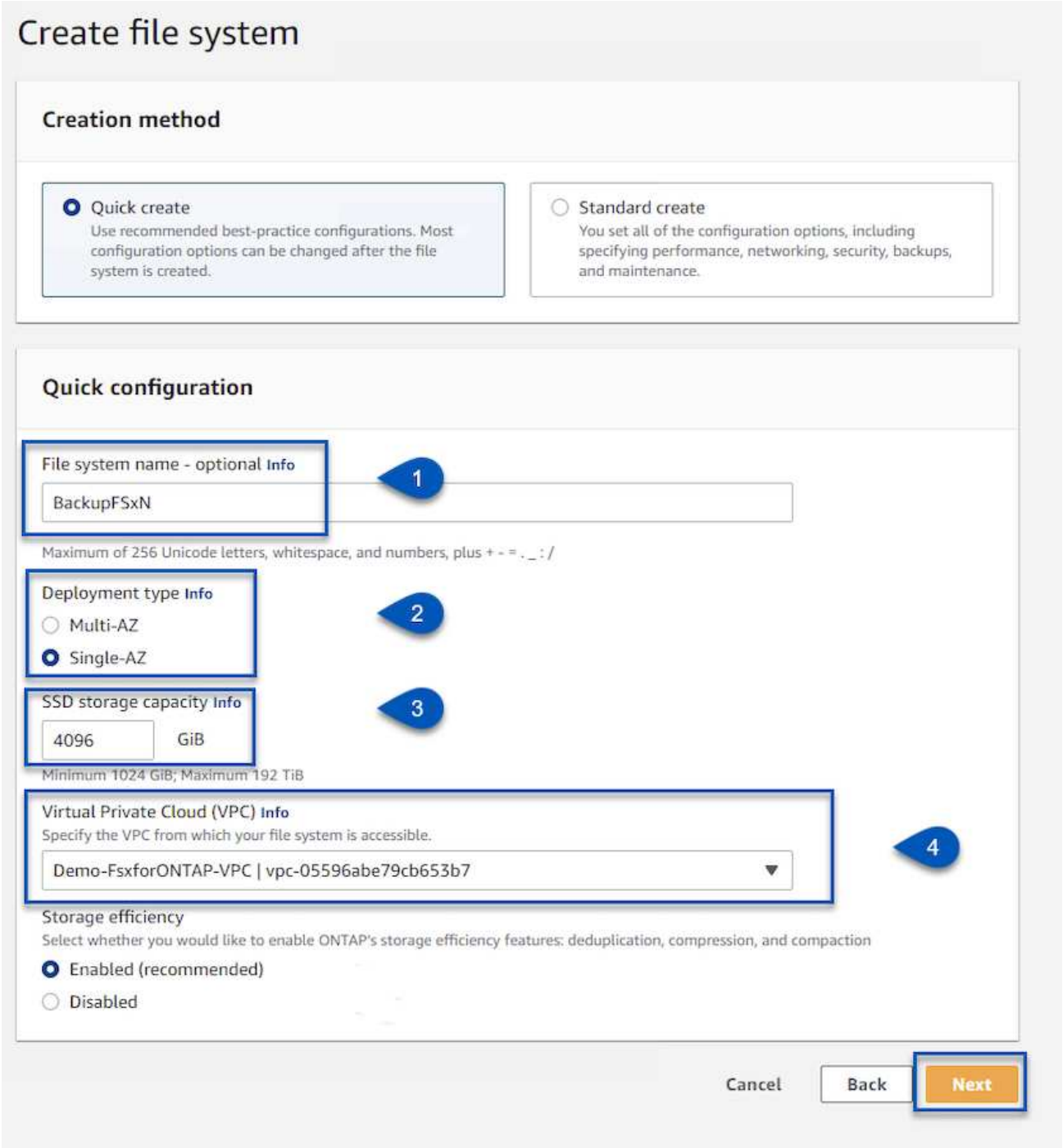
1. 在 AWS 控制台中，前往 FSx，然後 建立檔案系統



2. 選擇 * Amazon FSx ONTAP*，然後選擇 下一步 繼續。



3. 填寫檔案系統名稱、部署類型、SSD 儲存容量以及 FSx ONTAP叢集所在的 VPC。這必須是配置為與 VMware Cloud 中的虛擬機器網路通訊的 VPC。按一下“下一步”。



4. 查看部署步驟並點擊*建立檔案系統*開始檔案系統建立過程。

▼ 配置並掛載 **iSCSI LUN**

在 FSx ONTAP上建立和設定 iSCSI LUN 並安裝到 Veeam 備份和代理伺服器。這些 LUN 稍後將用於建立 Veeam 備份儲存庫。

在 FSx ONTAP上建立 iSCSI LUN 是一個多步驟的過程。建立磁碟區的第一步可以在Amazon FSx控制台或使用NetApp ONTAP CLI 完成。

有關使用 FSx ONTAP 的更多信息，請參閱 "FSx ONTAP使用者指南"。

1. 從NetApp ONTAP CLI 使用以下命令建立初始磁碟區：

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. 使用上一步建立的磁碟區建立 LUN：

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. 透過建立包含 Veeam 備份和代理伺服器的 iSCSI IQN 的啟動器群組來授予對 LUN 的存取權限：

```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

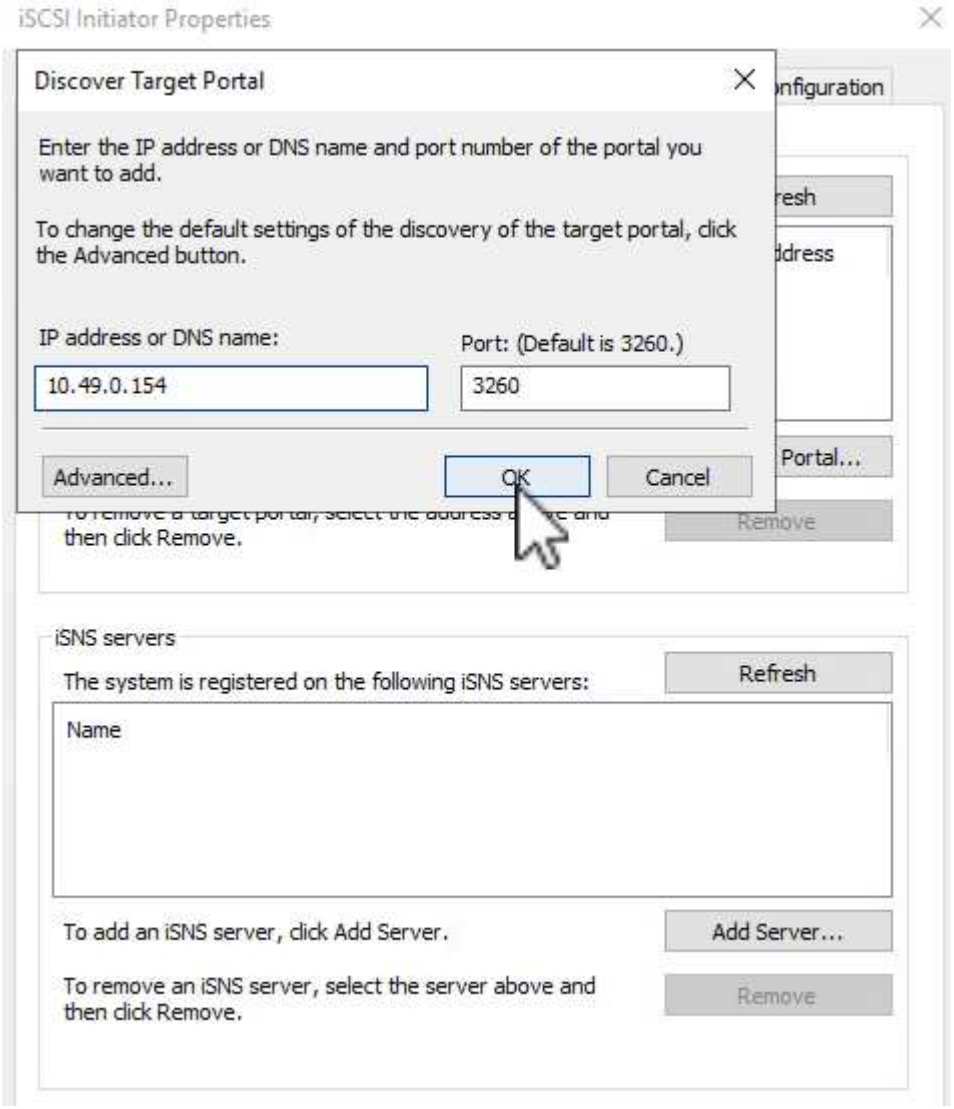


要完成前面的步驟，您需要先從 Windows 伺服器上的 iSCSI 啟動器屬性中擷取 IQN。

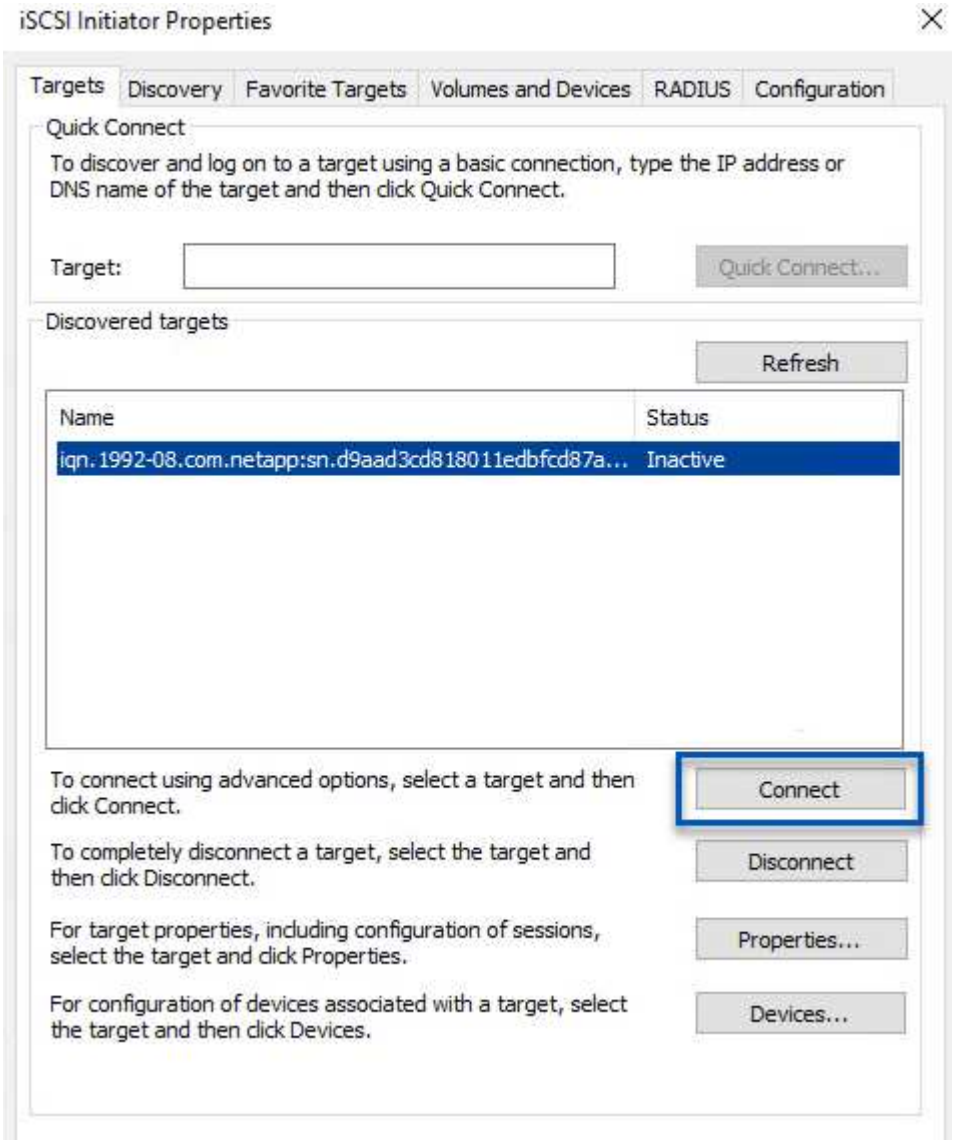
4. 最後，將 LUN 對應到剛剛建立的啟動器群組：

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

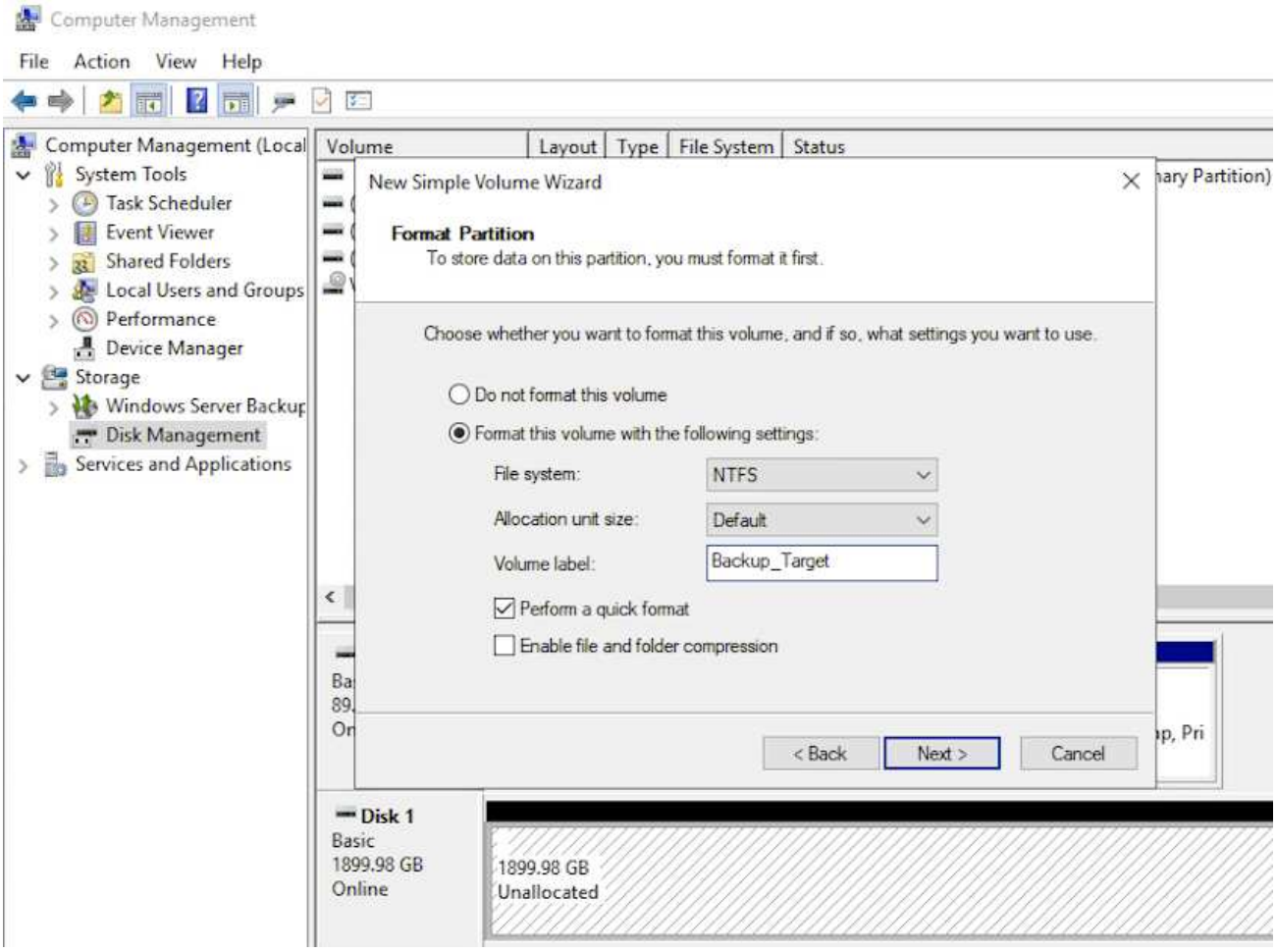
5. 若要安裝 iSCSI LUN，請登入 Veeam Backup & Replication Server 並開啟 iSCSI Initiator Properties。轉到“發現”標籤並輸入 iSCSI 目標 IP 位址。



6. 在「目標」標籤上，反白顯示非活動 LUN，然後按一下「連線」。勾選“啟用多路徑”方塊並點擊“確定”以連接到 LUN。



7. 在磁碟管理公用程式中初始化新的 LUN 並建立具有所需名稱和磁碟機號碼的磁碟區。勾選“啟用多路徑”方塊並點擊“確定”以連接到 LUN。

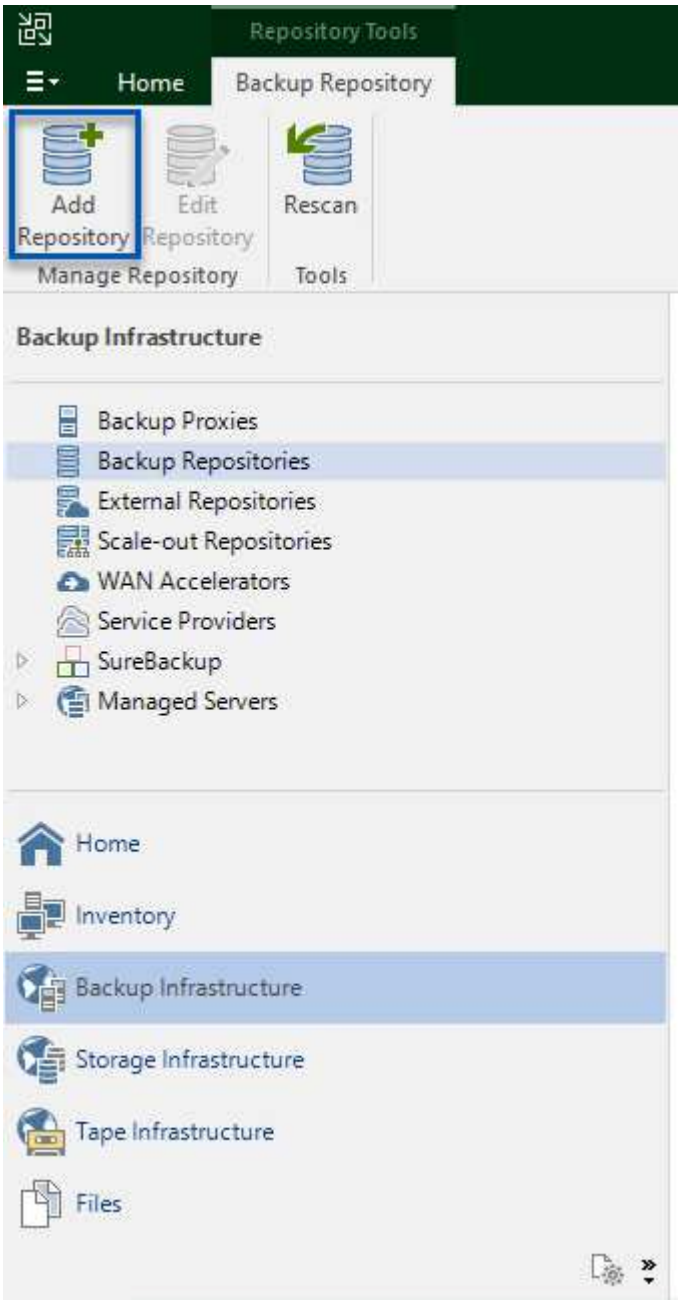


8. 重複這些步驟以在 Veeam 代理伺服器上掛載 iSCSI 磁碟區。

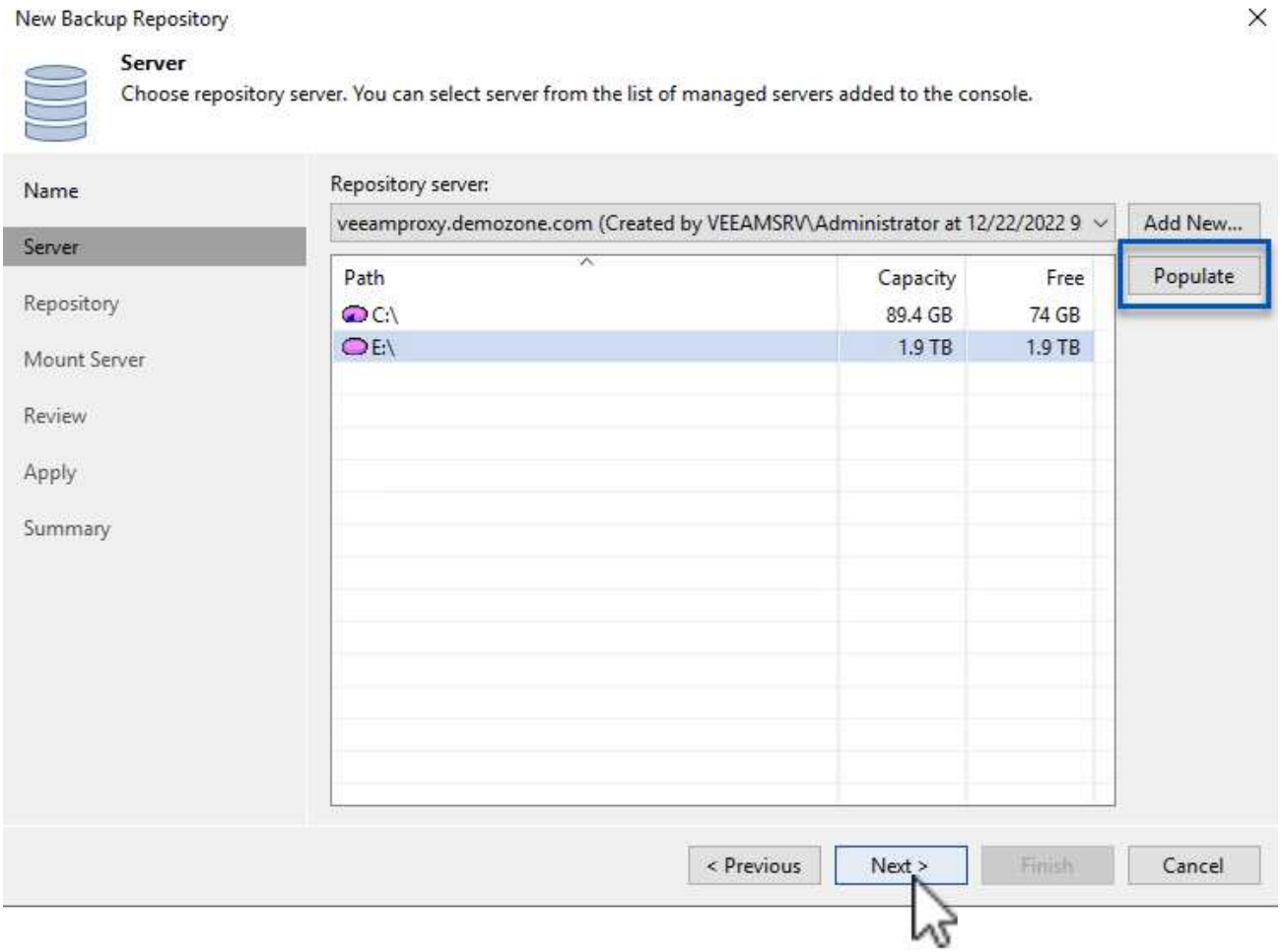
▼ 建立 **Veeam** 備份儲存庫

在 Veeam Backup and Replication 控制台中，為 Veeam Backup 和 Veeam Proxy 伺服器建立備份儲存庫。這些儲存庫將用作虛擬機器備份的備份目標。

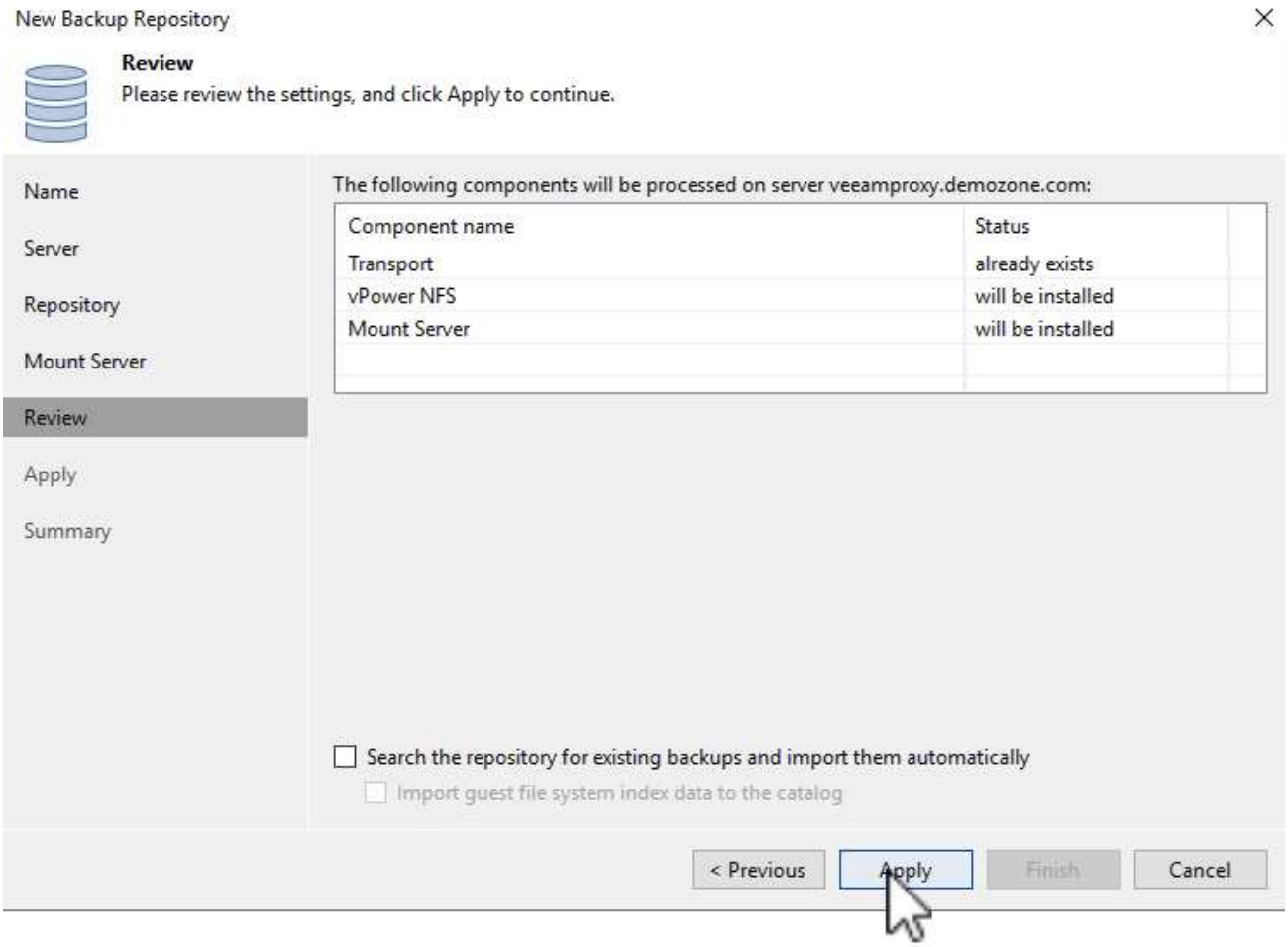
1. 在 Veeam Backup and Replication 控制台中，按一下左下角的“備份基礎架構”，然後選擇“新增儲存庫”



2. 在新備份儲存庫精靈中，輸入儲存庫的名稱，然後從下拉清單中選擇伺服器，並按一下*填入*按鈕以選擇將使用的 NTFS 磁碟區。



3. 在下一頁上，選擇執行進階復原時用於掛載備份的掛載伺服器。預設情況下，這是與儲存庫儲存連接的相同伺服器。
4. 檢查您的選擇並點擊"應用"開始建立備份儲存庫。



5. 對任何其他代理伺服器重複這些步驟。

設定 **Veeam** 備份作業

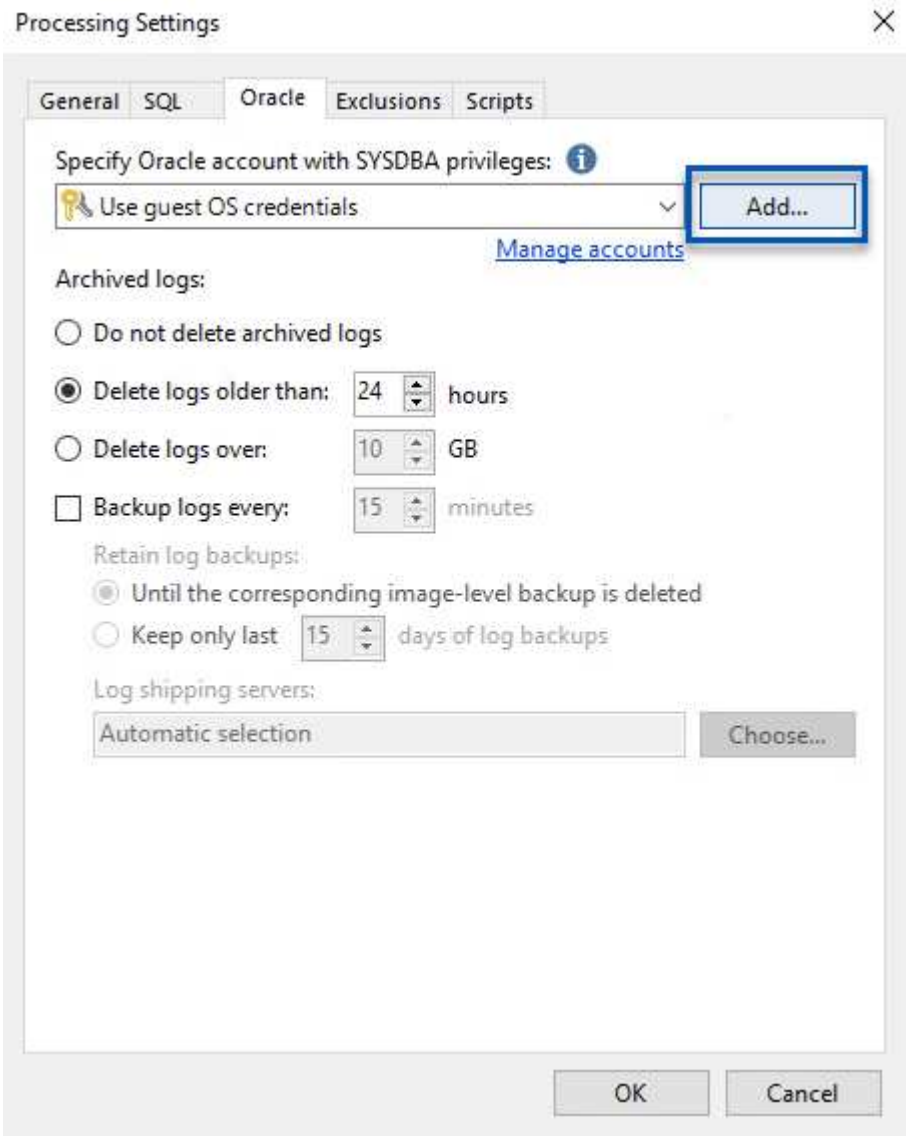
應利用上一節中的備份儲存庫建立備份作業。建立備份作業是任何儲存管理員的正常工作的一部分，我們不會在這裡介紹所有步驟。有關在 Veeam 中建立備份作業的更多完整信息，請參閱 "Veeam 幫助中心技術文檔"。

在此解決方案中，為以下內容建立了單獨的備份作業：

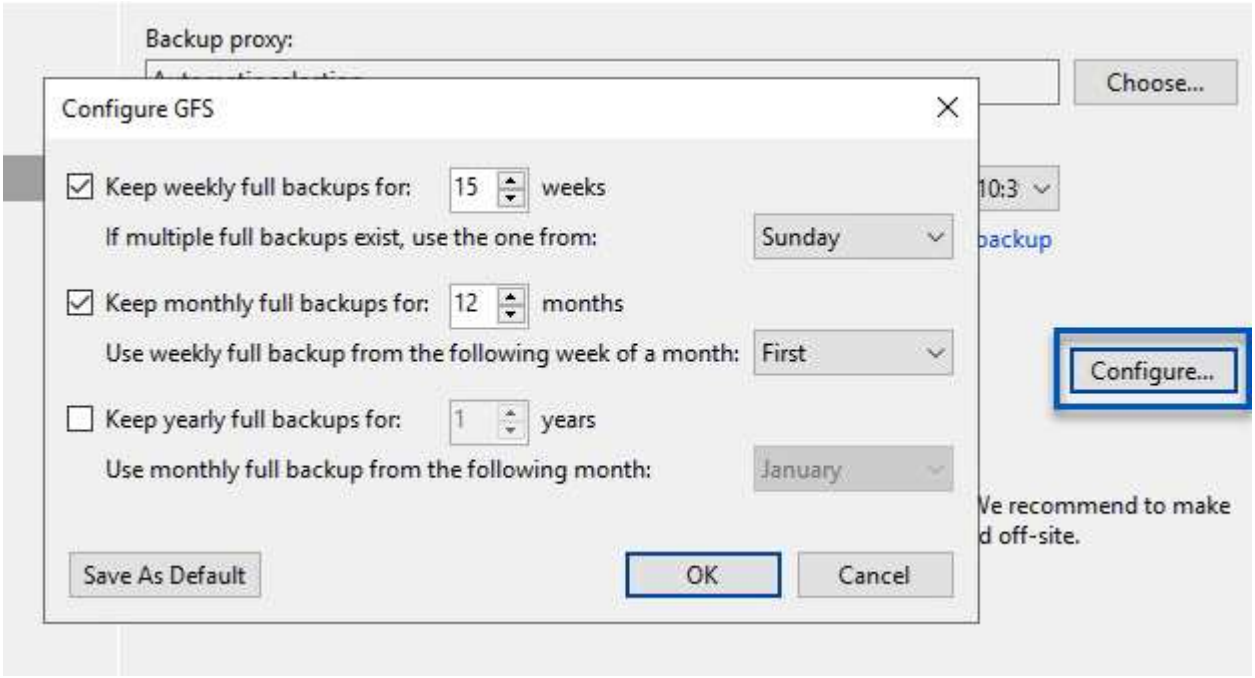
- Microsoft Windows SQL 伺服器
- Oracle 資料庫伺服器
- Windows 檔案伺服器
- Linux 檔案伺服器

▼ 設定 **Veeam** 備份作業時的一般注意事項

1. 啟用應用程式感知處理來建立一致的備份並執行交易日誌處理。
2. 啟用應用程式感知處理後，請向應用程式新增具有管理員權限的正確憑證，因為這可能與來賓作業系統憑證不同。



3. 若要管理備份的保留策略，請選取*將某些完整備份保留更長時間以用於存檔目的*，然後按一下*設定…*按鈕以設定策略。



使用 **Veeam** 完整恢復功能恢復應用程式虛擬機

使用 Veeam 執行完整復原是執行應用程式復原的第一步。我們驗證了虛擬機器的完全恢復已啟動並且所有服務均正常運作。

恢復伺服器是任何儲存管理員的正常工作的一部分，我們不會在這裡介紹所有步驟。有關在 Veeam 中執行完整恢復的更多完整信息，請參閱 "Veeam 幫助中心技術文檔"。

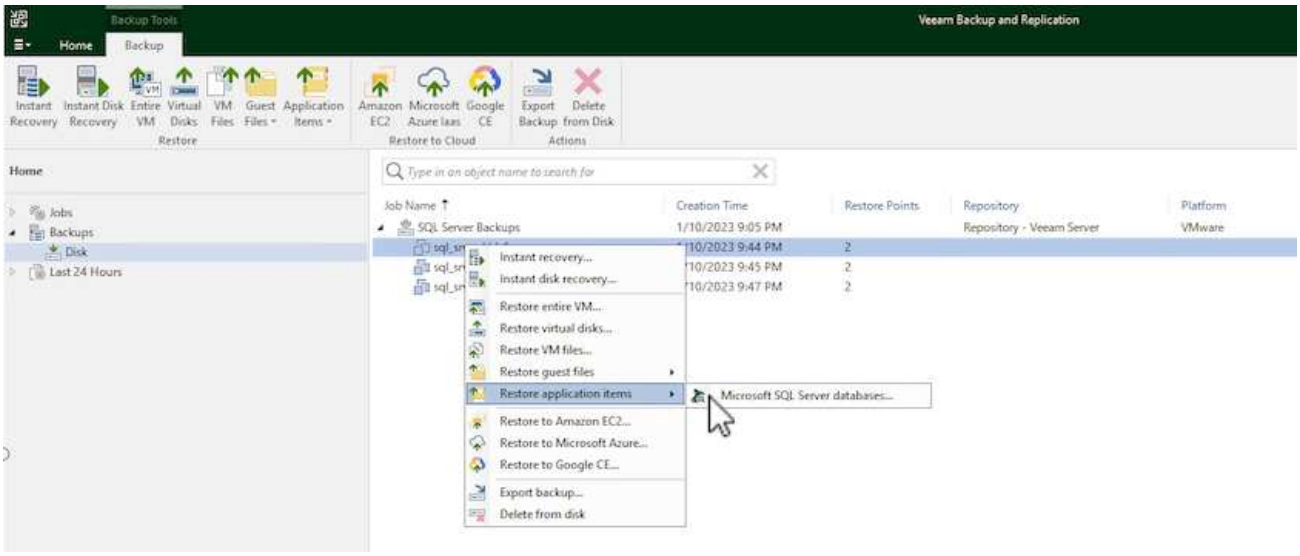
還原 **SQL Server** 資料庫

Veeam Backup & Replication 提供了多種還原 SQL Server 資料庫的選項。為了進行此驗證，我們使用具有即時復原功能的 Veeam Explorer for SQL Server 來執行 SQL Server 資料庫的復原。 SQL Server 即時復原功能可讓您快速還原 SQL Server 資料庫，而無需等待完整的資料庫還原。這種快速恢復過程可最大限度地減少停機時間並確保業務連續性。工作原理如下：

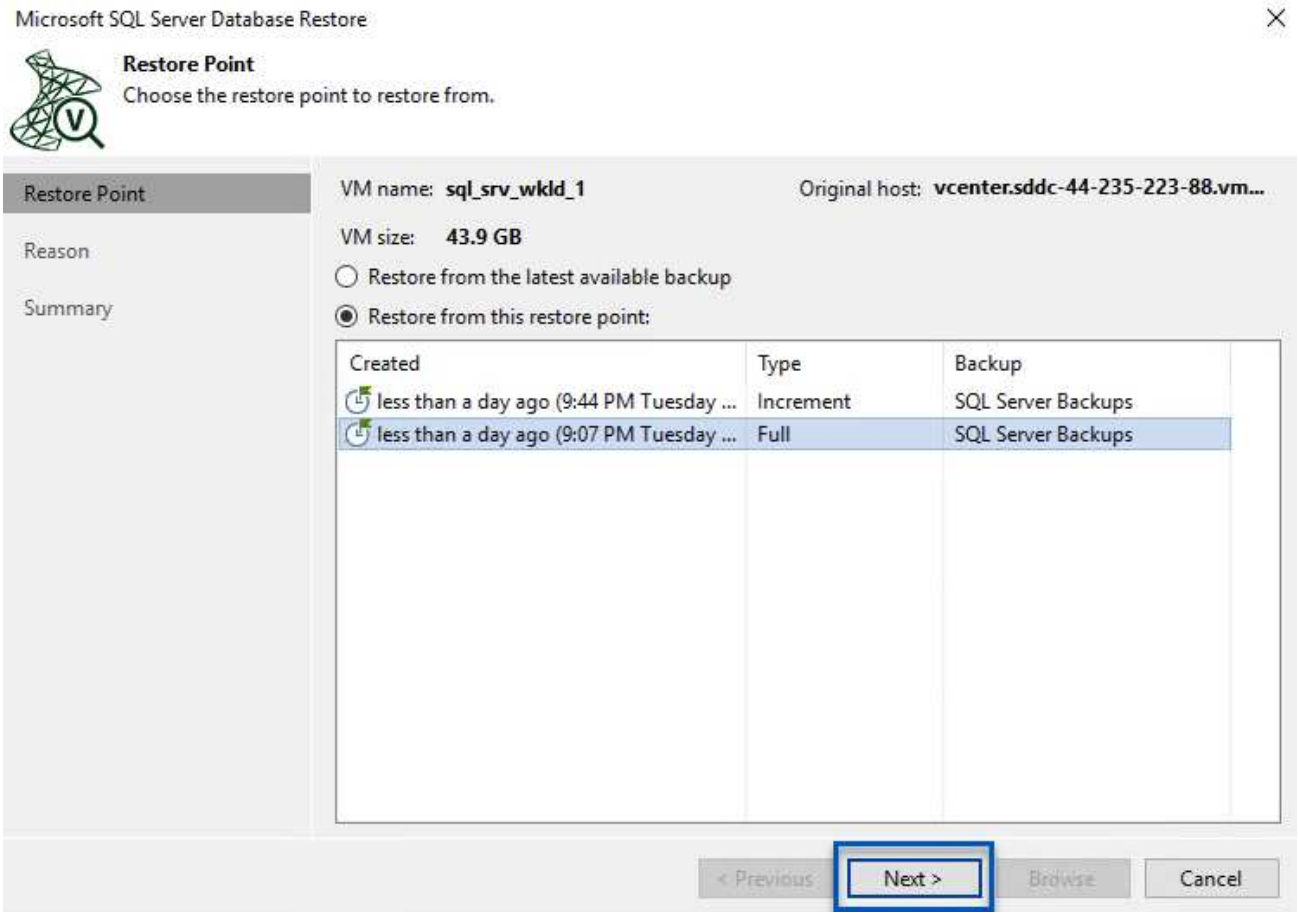
- Veeam Explorer 安裝包含要還原的 **SQL Server** 資料庫的備份。
- 軟體直接從已安裝的檔案*發佈資料庫*，使其可作為目標 SQL Server 執行個體上的臨時資料庫進行存取。
- 在使用臨時資料庫時，Veeam Explorer 會將使用者查詢重新導向至該資料庫，確保使用者可以繼續存取和使用資料。
- 在後台，Veeam 執行完整的資料庫復原，將資料從臨時資料庫傳輸到原始資料庫位置。
- 一旦完整資料庫恢復完成，Veeam Explorer 會將使用者查詢切換回原始*資料庫並刪除臨時資料庫。

▼ 使用 **Veeam Explorer Instant Recovery** 還原 **SQL Server** 資料庫

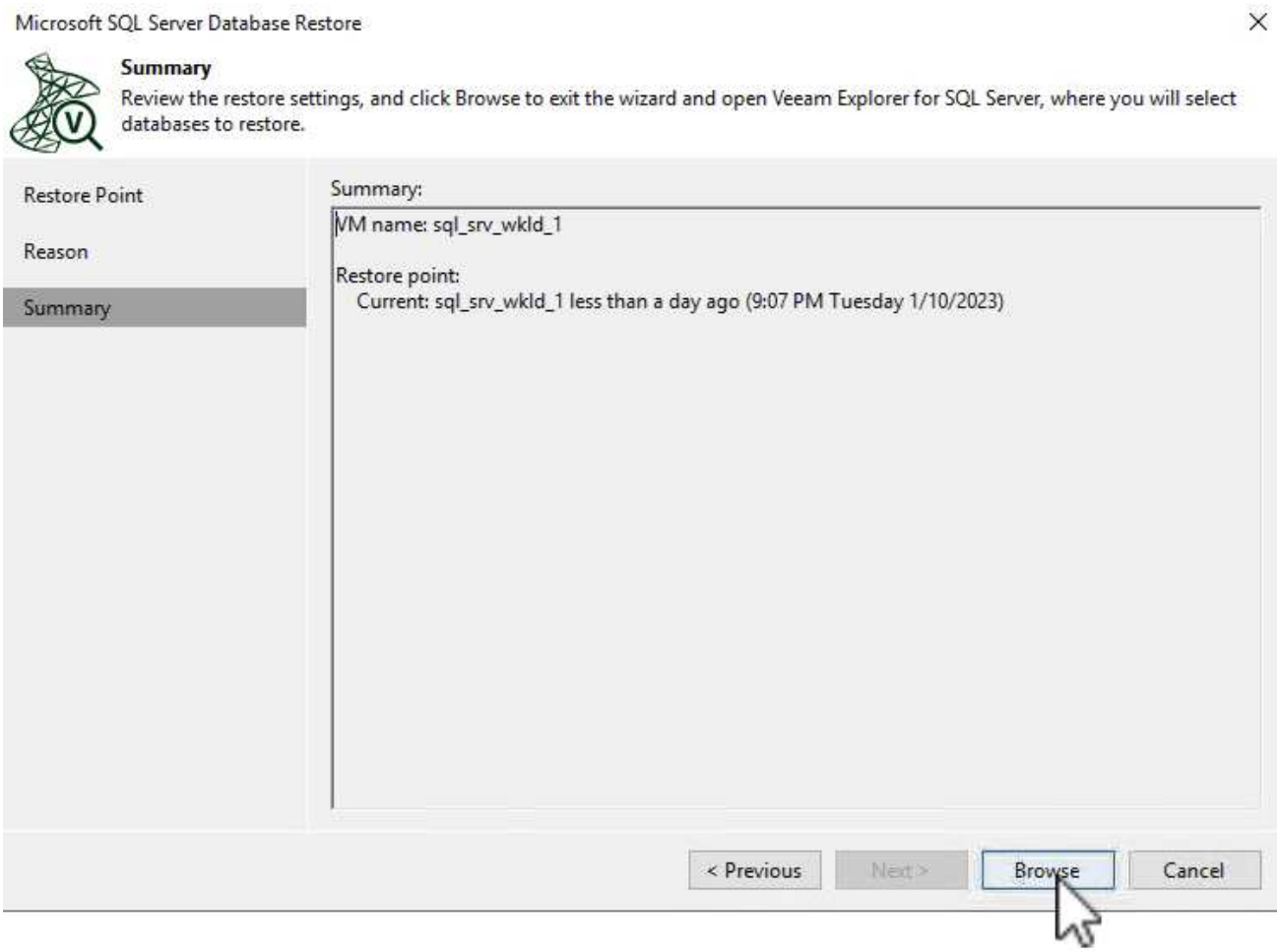
1. 在 Veeam Backup and Replication 控制台中，導覽至 SQL Server 備份列表，以滑鼠右鍵按一下伺服器並選擇 還原應用程式項目，然後選擇 **Microsoft SQL Server** 資料庫...。



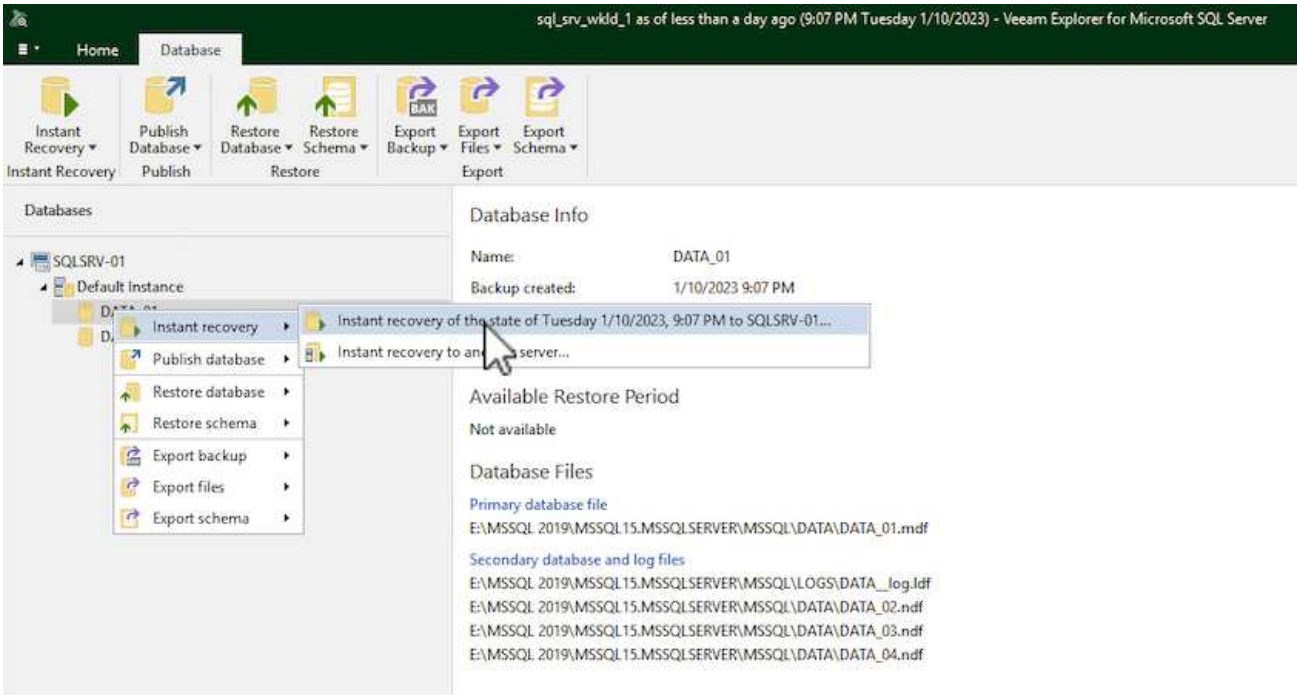
2. 在 Microsoft SQL Server 資料庫還原精靈中，從清單中選擇一個還原點，然後按一下「下一步」。



3. 如有需要，輸入*復原原因*，然後在摘要頁面上，按一下*瀏覽*按鈕啟動 Veeam Explorer for Microsoft SQL Server。

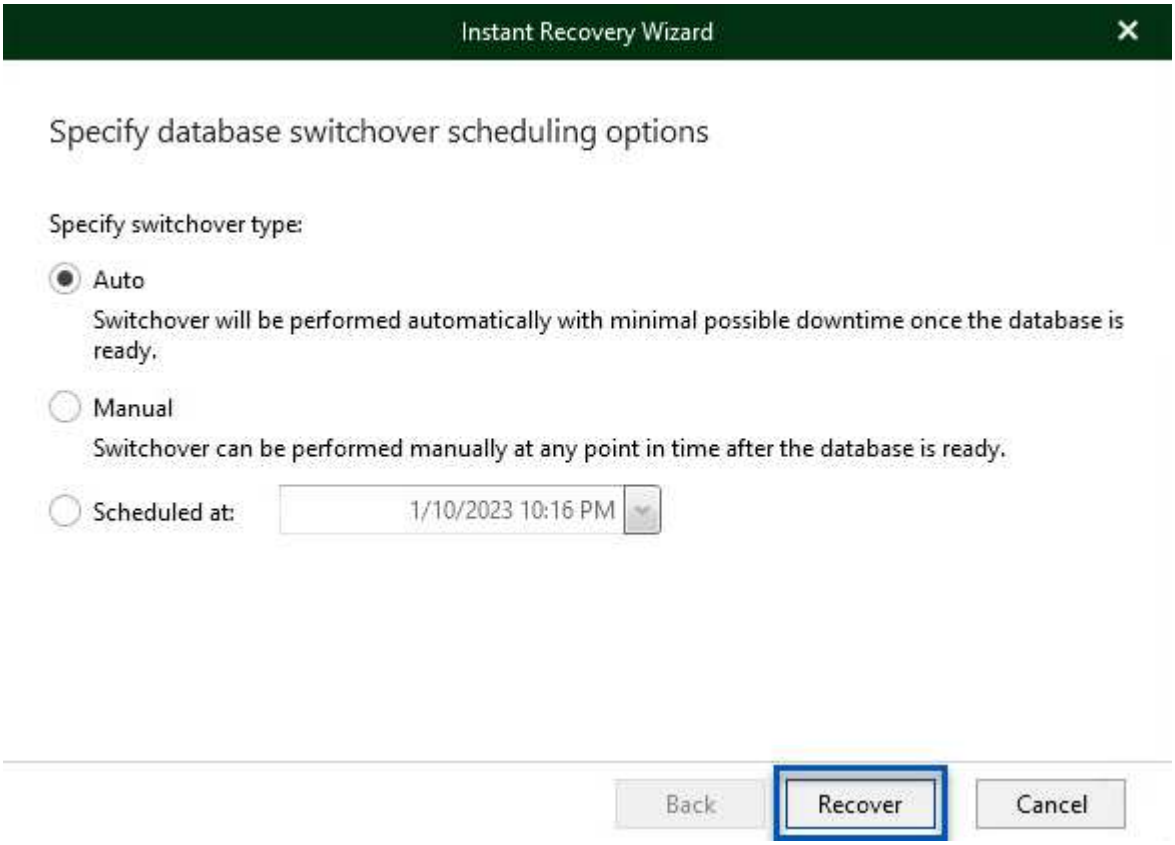


4. 在 Veeam Explorer 中展開資料庫實例列表，右鍵單擊並選擇 即時恢復，然後選擇要還原到的特定還原點。

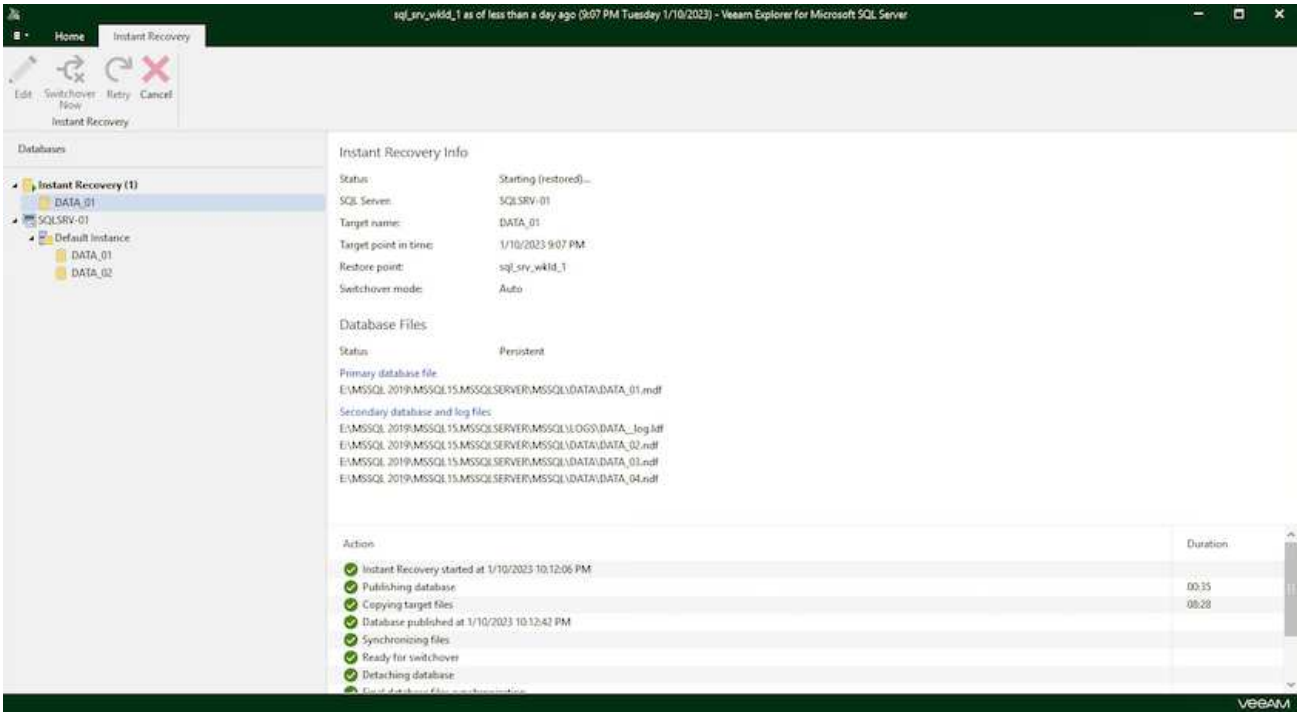


5. 在即時復原精靈中指定切換類型。這可以自動進行，停機時間最短，也可以手動進行，或在指定時間進

行。然後點選“恢復”按鈕開始恢復程序。



6. 可以從 Veeam Explorer 監控恢復過程。



有關使用 Veeam Explorer 執行 SQL Server 還原操作的更多詳細信息，請參閱 "Veeam Explorers 使用者指南 "。

使用 **Veeam Explorer** 還原 **Oracle** 資料庫

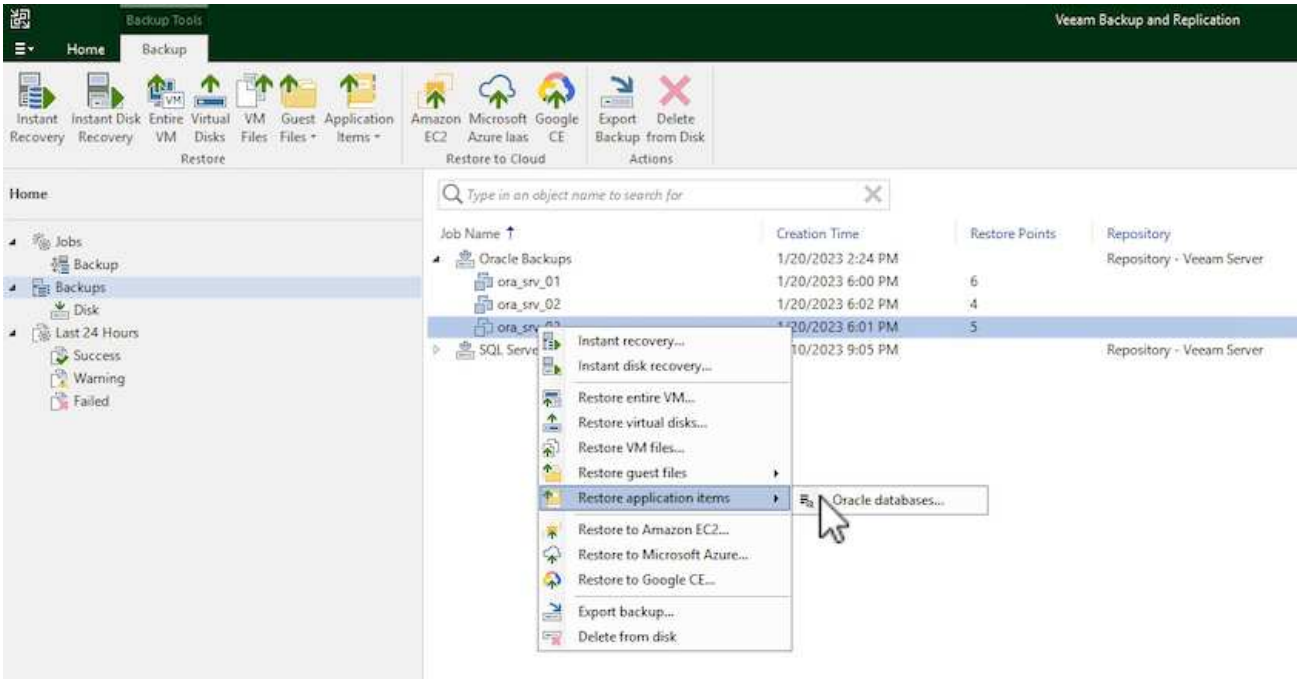
Veeam Explorer for Oracle 資料庫提供了執行標準 Oracle 資料庫還原或使用即時復原進行不間斷還原的能力。它還支援發布資料庫以實現快速存取、還原 Data Guard 資料庫以及從 RMAN 備份中復原。

有關使用 Veeam Explorer 執行 Oracle 資料庫還原作業的更多詳細信息，請參閱 "Veeam Explorers 使用者指南"。

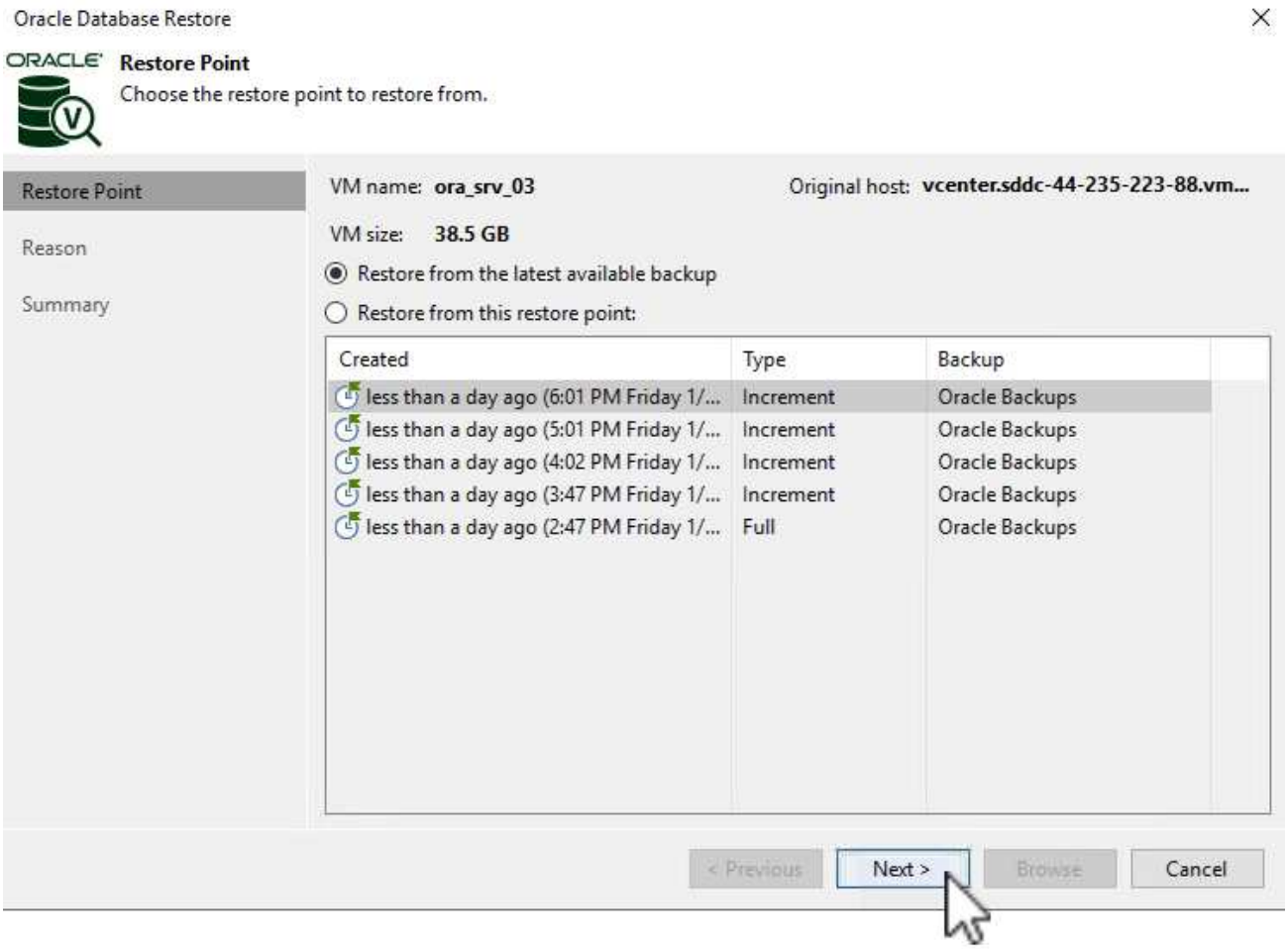
▼ 使用 **Veeam Explorer** 還原 **Oracle** 資料庫

本節介紹如何使用 Veeam Explorer 將 Oracle 資料庫還原到不同的伺服器。

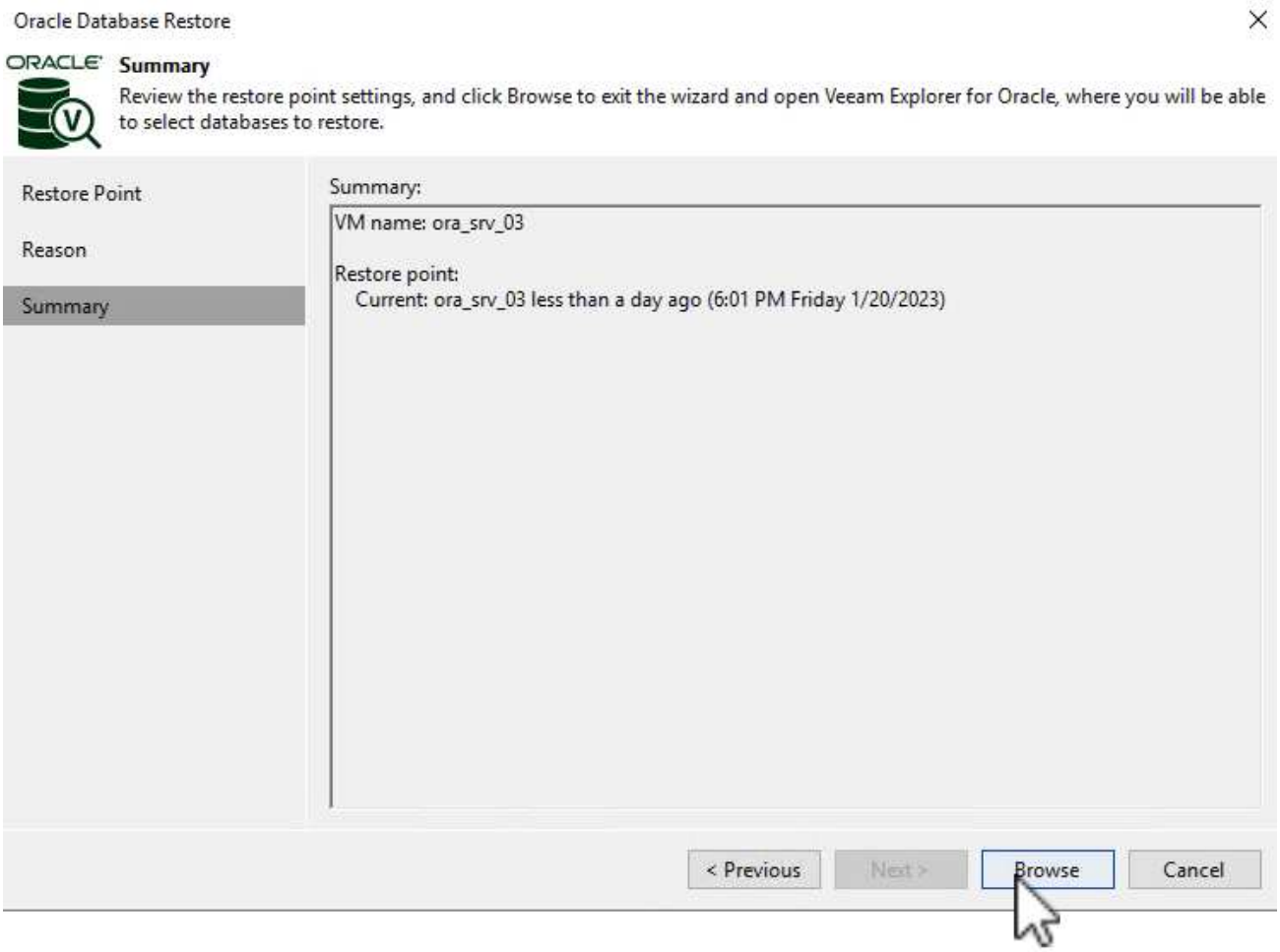
1. 在 Veeam Backup and Replication 控制台中，導覽至 Oracle 備份列表，右鍵點選伺服器並選擇 還原應用程式項目，然後選擇 **Oracle** 資料庫...。



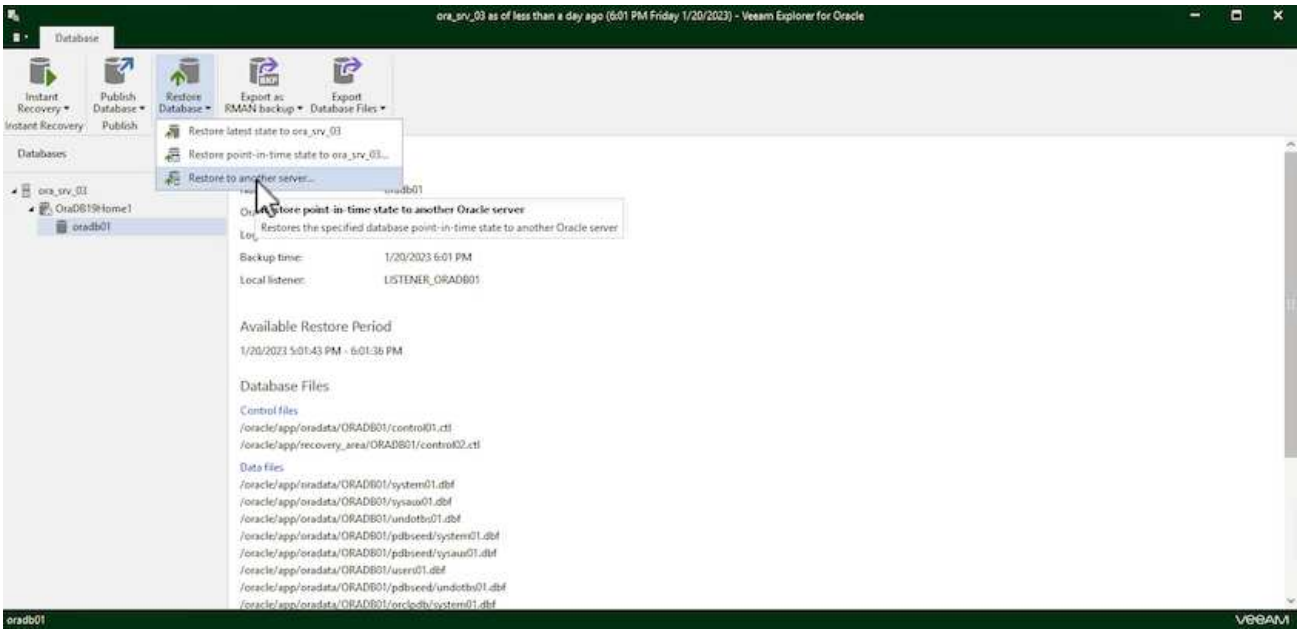
2. 在 Oracle 資料庫還原精靈中，從清單中選擇一個還原點，然後按一下「下一步」。



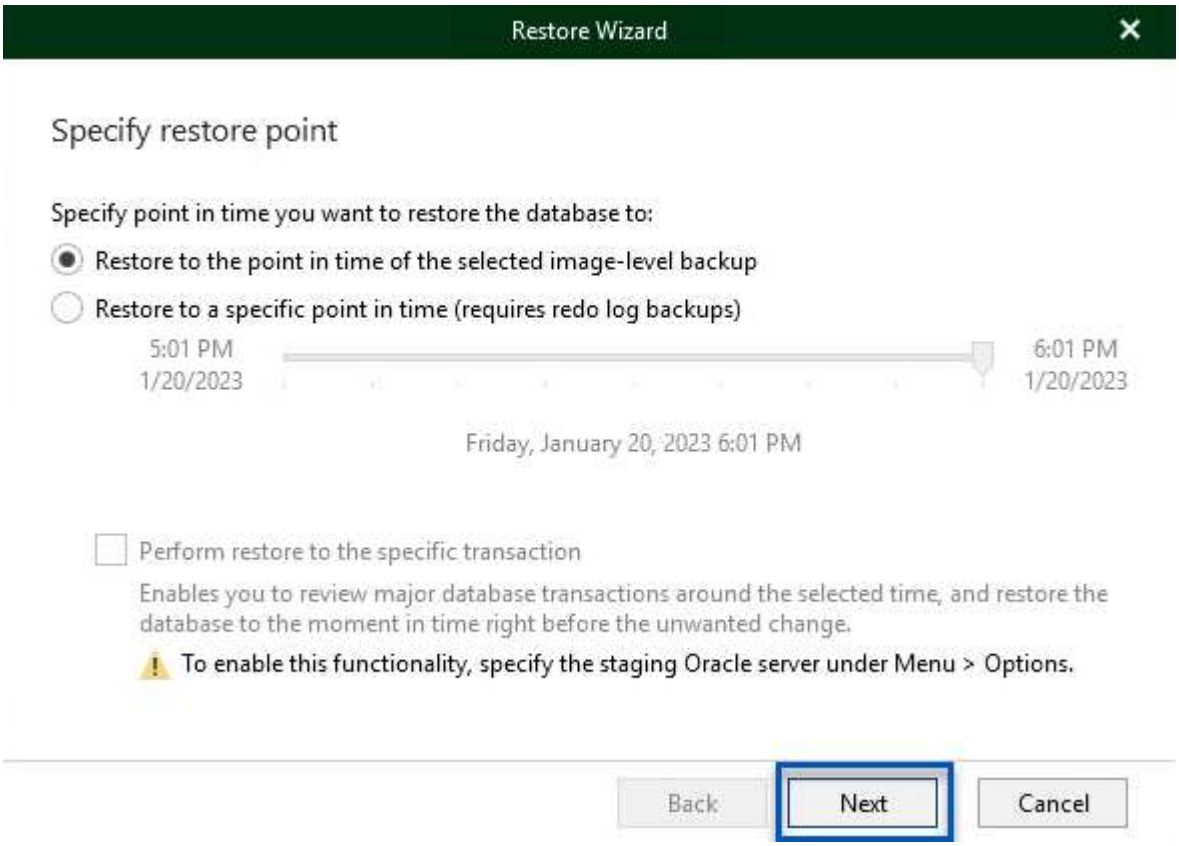
3. 如有需要，輸入*復原原因*，然後在摘要頁面上，按一下*瀏覽*按鈕啟動 Veeam Explorer for Oracle。



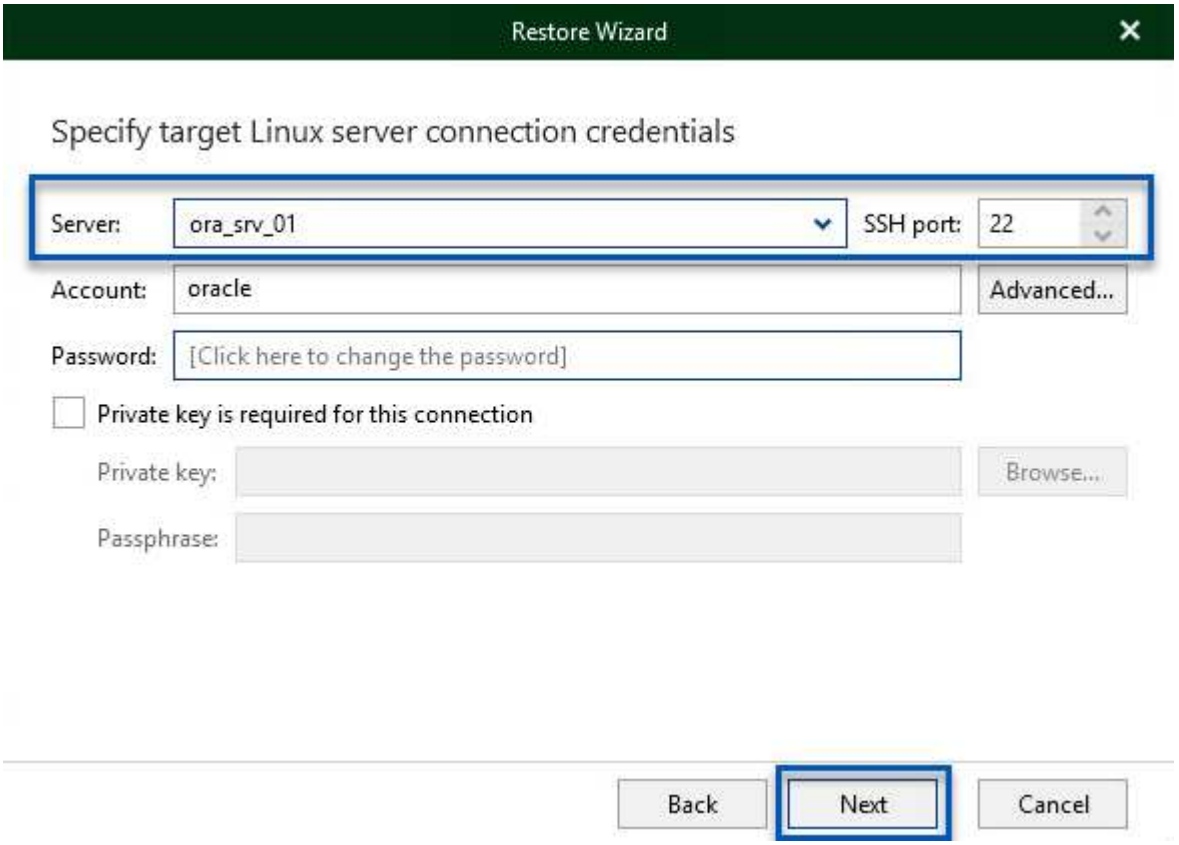
4. 在 Veeam Explorer 中展開資料庫實例列表，按一下要恢復的資料庫，然後從頂部的 恢復資料庫 下拉式選單中選擇 恢復到另一台伺服器...。



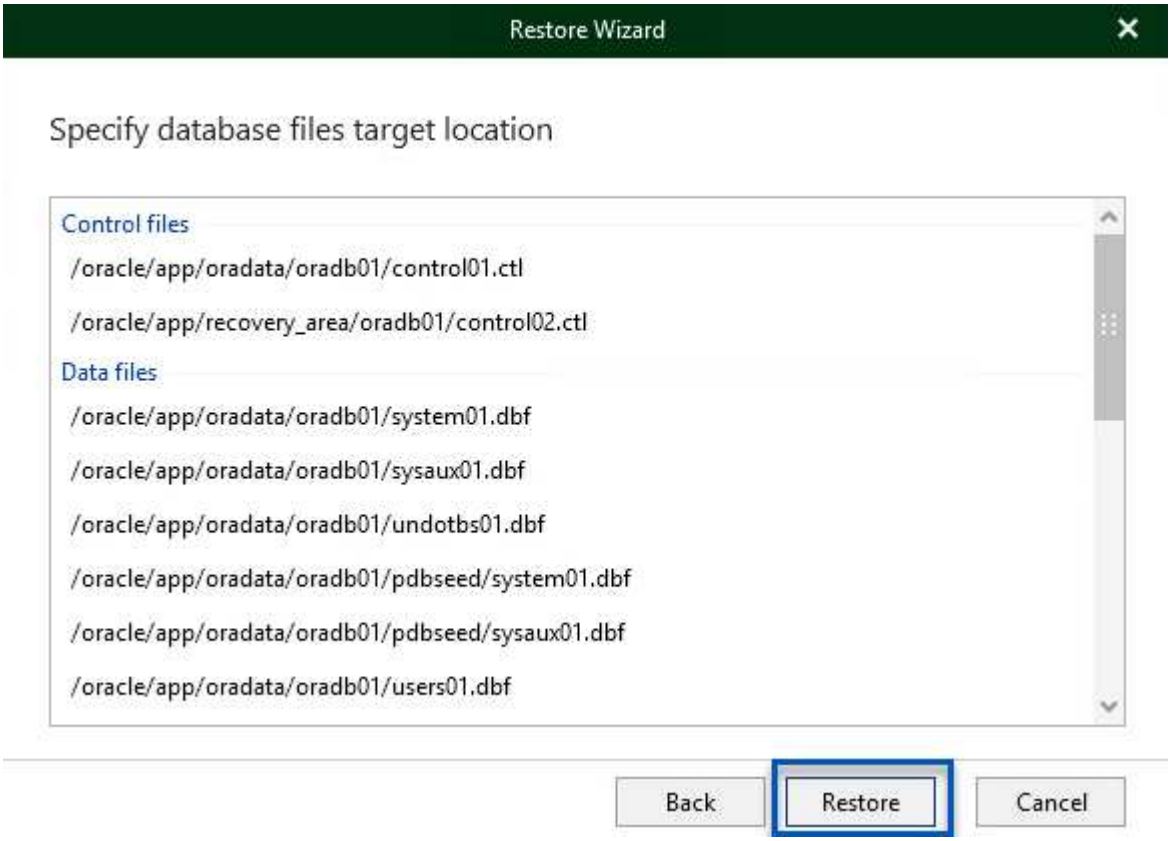
5. 在還原精靈中指定要還原的還原點，然後按一下「下一步」。



6. 指定資料庫將還原到的目標伺服器和帳戶憑證，然後按一下「下一步」。



7. 最後，指定資料庫檔案目標位置並點擊*恢復*按鈕開始復原程序。

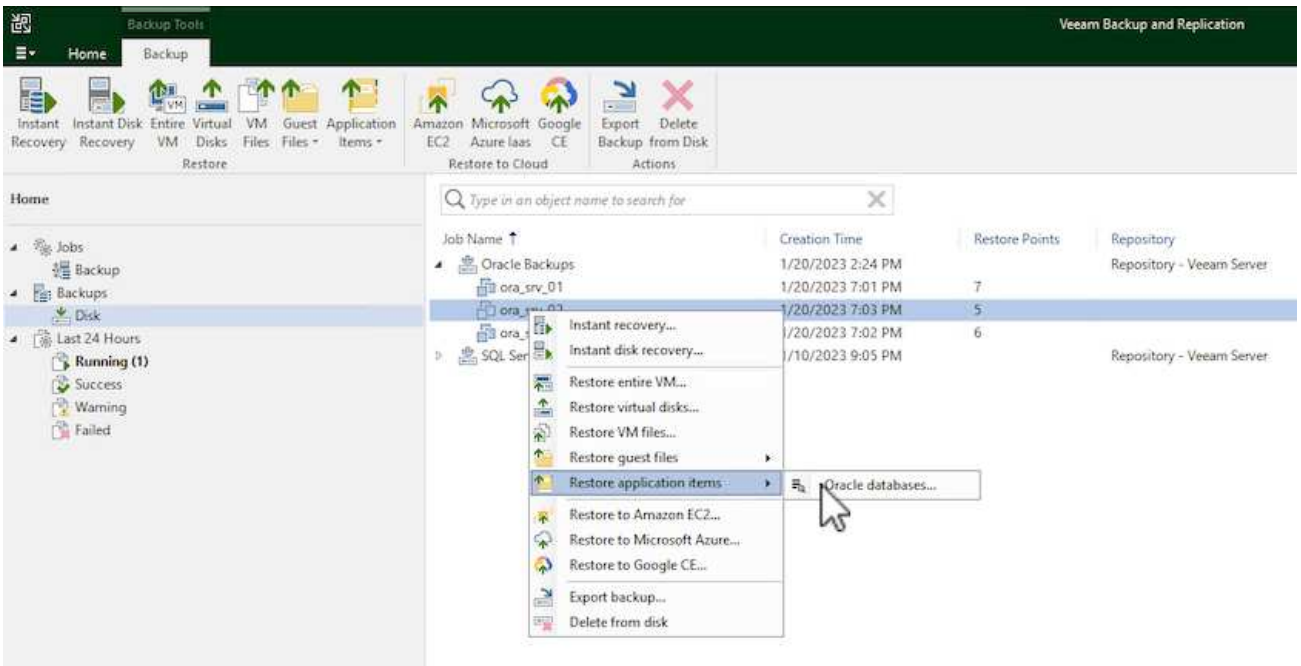


8. 資料庫復原完成後，檢查 Oracle 資料庫是否在伺服器上正常啟動。

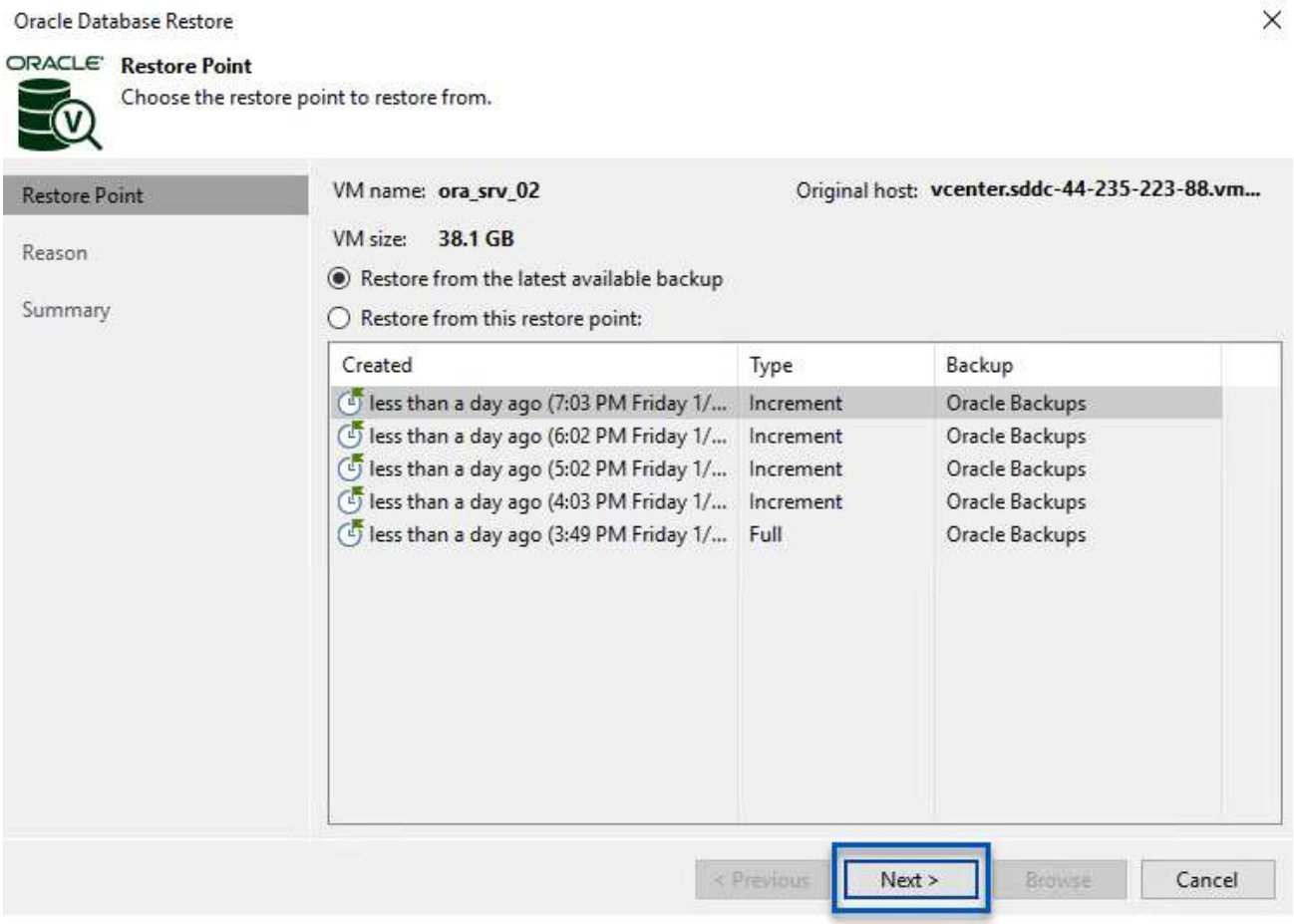
▼ 將 **Oracle** 資料庫發佈到備用伺服器

在本節中，資料庫發佈到備用伺服器，以便快速訪問，而無需啟動完整復原。

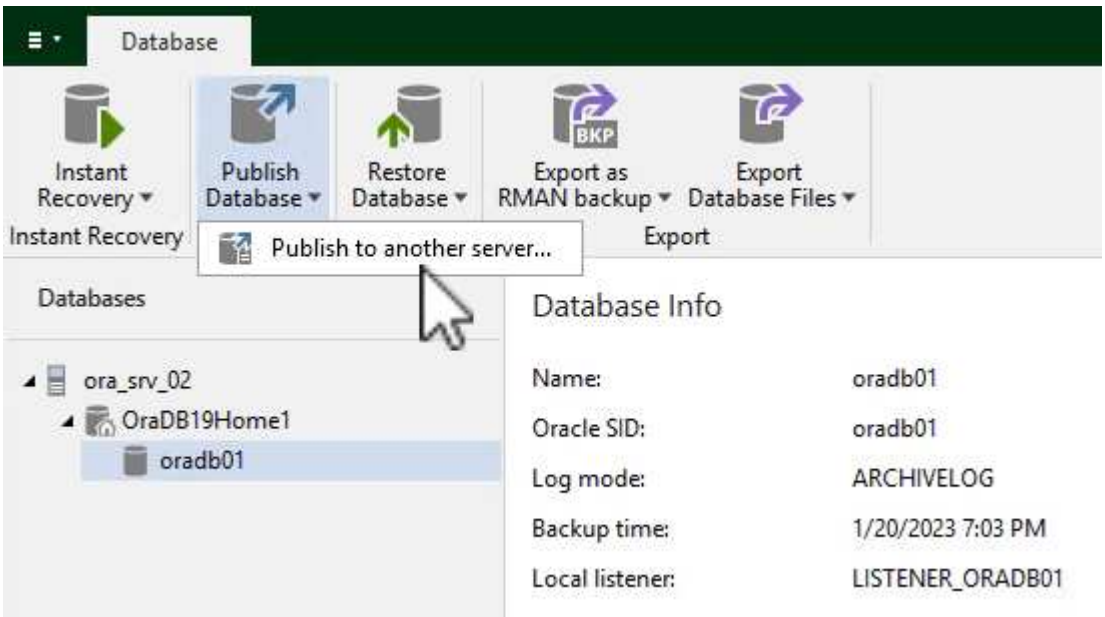
1. 在 Veeam Backup and Replication 控制台中，導覽至 Oracle 備份列表，右鍵點選伺服器並選擇 還原應用程式項目，然後選擇 **Oracle** 資料庫**...**。



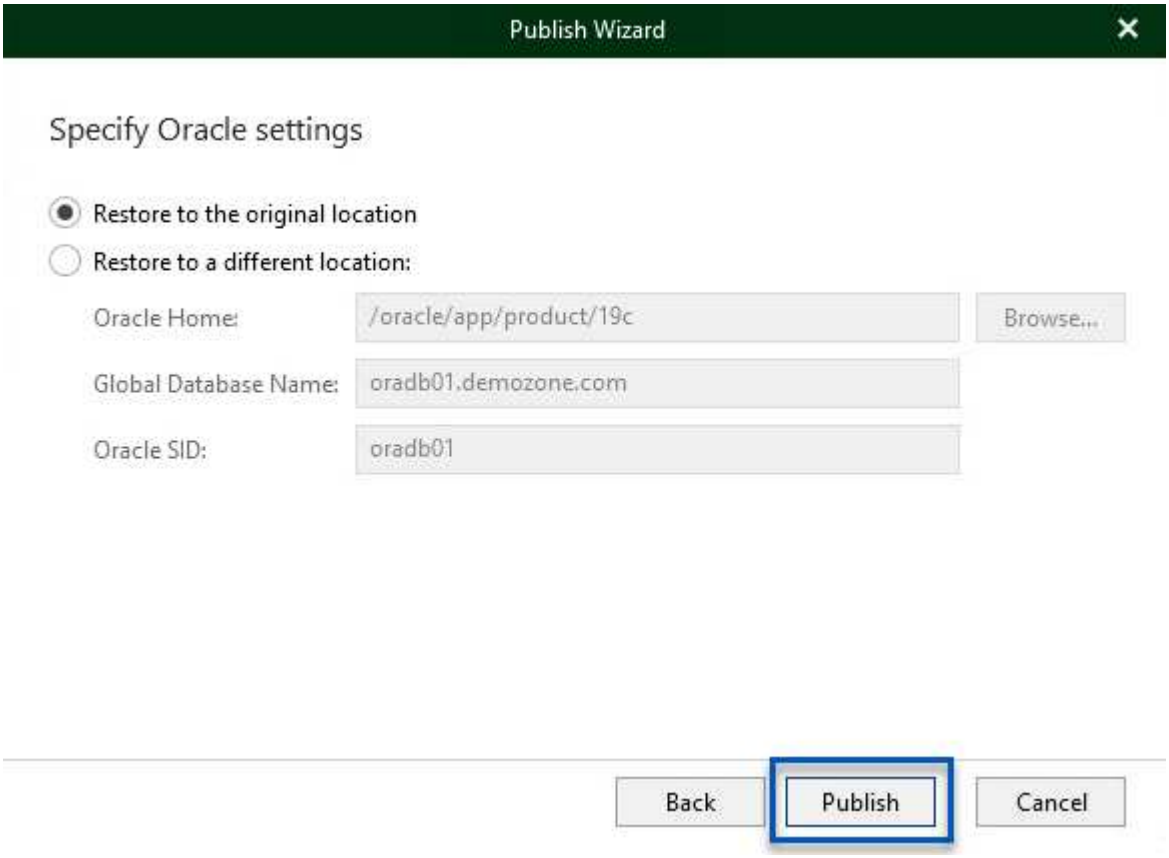
2. 在 Oracle 資料庫還原精靈中，從清單中選擇一個還原點，然後按一下「下一步」。



3. 如有需要，輸入*復原原因*，然後在摘要頁面上，按一下*瀏覽*按鈕啟動 Veeam Explorer for Oracle。
4. 在 Veeam Explorer 中展開資料庫實例列表，按一下要恢復的資料庫，然後從頂部的 發布資料庫 下拉式選單中選擇 發佈到另一台伺服器...。



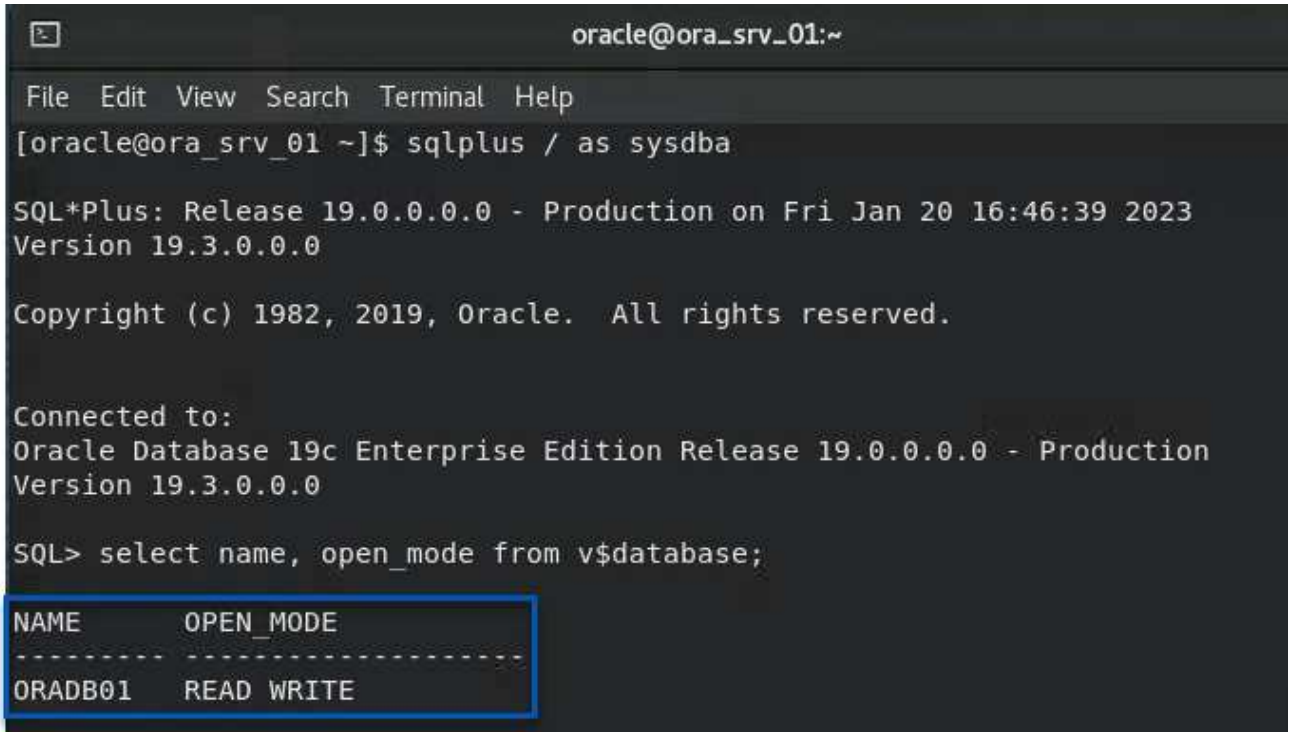
5. 在發佈精靈中，指定發佈資料庫的還原點，然後按一下「下一步」。
6. 最後，指定目標 Linux 檔案系統位置並點擊 發布 開始復原程序。



7. 發布完成後，登入目標伺服器並執行以下命令以確保資料庫正在執行：

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



結論

VMware Cloud 是一個強大的平台，用於運行關鍵業務應用程式和儲存敏感資料。對於依賴 VMware Cloud 來確保業務連續性並幫助防止網路威脅和資料遺失的企業來說，安全的資料保護解決方案至關重要。透過選擇可靠且強大的資料保護解決方案，企業可以確信無論如何其關鍵資料都是安全的。

本文檔中介紹的用例重點關注經過驗證的資料保護技術，突出了NetApp、VMware 和 Veeam 之間的整合。 FSx ONTAP作為 AWS 中 VMware Cloud 的補充 NFS 資料儲存區受支持，並用於所有虛擬機器和應用程式資料。 Veeam Backup & Replication 是一款全面的資料保護解決方案，旨在協助企業改善、自動化和簡化其備份和復原流程。 Veeam 與託管在 FSx ONTAP上的 iSCSI 備份目標磁碟區結合使用，為駐留在 VMware Cloud 中的應用程式資料提供安全且易於管理的資料保護解決方案。

附加資訊

要了解有關此解決方案中提出的技術的更多信息，請參閱以下附加資訊。

- "FSx ONTAP使用者指南"
- "Veeam 幫助中心技術文檔"
- "VMware Cloud on AWS 支援。注意事項和限制"

TR-4955：使用 **FSx ONTAP**和 **VMC** 進行災難復原 **(AWS VMware Cloud)**

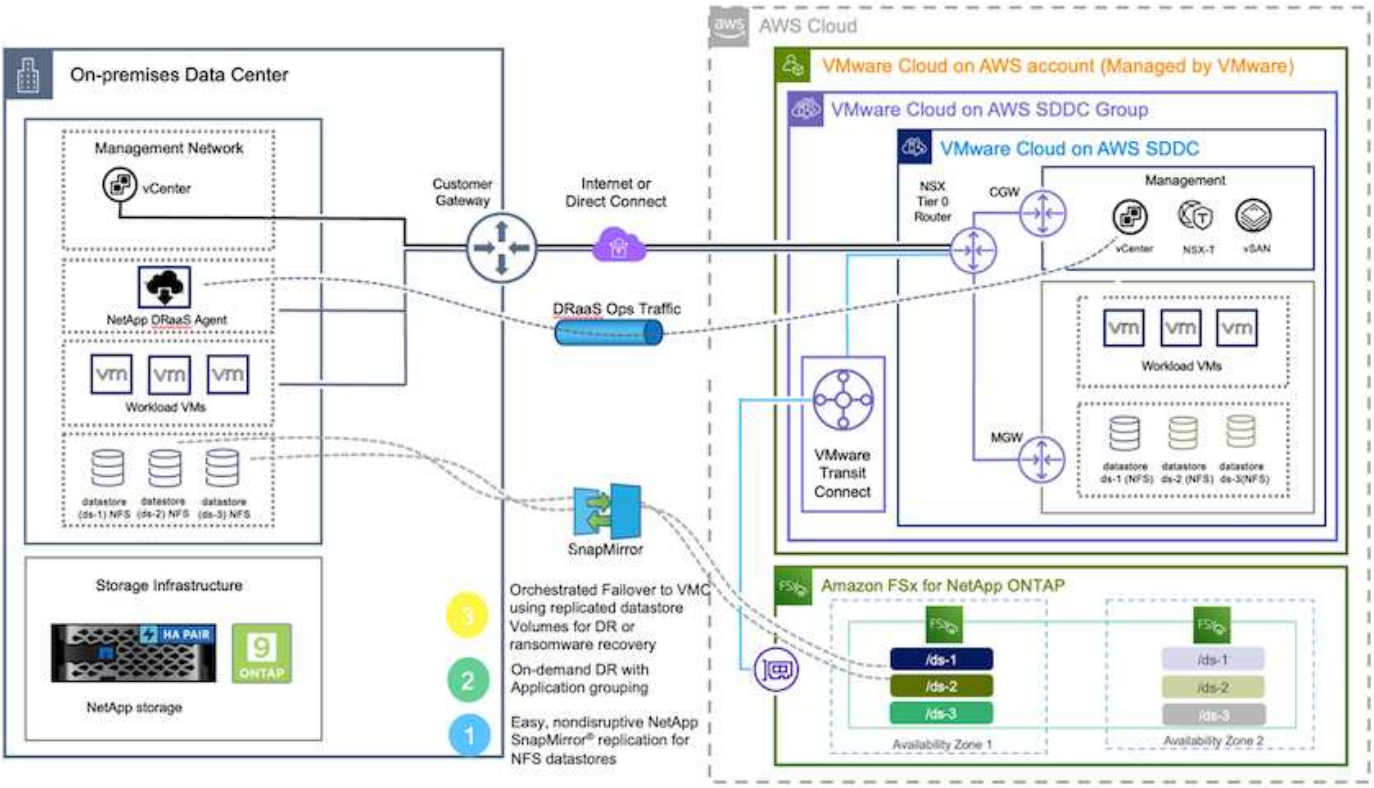
災難復原編排器（DRO；具有 UI 的腳本解決方案）可用於無縫復原從本機複製到 FSx ONTAP 的工作負載。 DRO 可自動執行從SnapMirror等級到 VM 註冊到 VMC 再到直接在 NSX-T 上進行網路對映的復原。所有 VMC 環境均包含此功能。

NetApp的 Niyaz Mohamed

概況

災難復原到雲端是一種具有彈性且經濟高效的方法，可以保護工作負載免受網站中斷和資料損壞事件（例如勒索軟體）的影響。透過NetApp SnapMirror技術，本機 VMware 工作負載可以複製到在 AWS 中執行的 FSx ONTAP 。

災難復原編排器（DRO；具有 UI 的腳本解決方案）可用於無縫復原從本機複製到 FSx ONTAP 的工作負載。DRO 可自動執行從SnapMirror等級到 VM 註冊到 VMC 再到直接在 NSX-T 上進行網路對映的復原。所有 VMC 環境均包含此功能。



入門

在 **AWS** 上部署並設定 **VMware Cloud**

"AWS 上的 VMware Cloud"為 AWS 生態系統中基於 VMware 的工作負載提供雲端原生體驗。每個 VMware 軟體定義資料中心 (SDDC) 都在 Amazon 虛擬私有雲 (VPC) 中運行，並提供完整的 VMware 堆疊（包括 vCenter Server）、NSX-T 軟體定義網路、vSAN 軟體定義儲存以及一個或多個為工作負載提供運算和儲存資源的 ESXi 主機。若要在 AWS 上設定 VMC 環境，請依照下列步驟操作"關聯"。指示燈組也可用於 DR 目的。

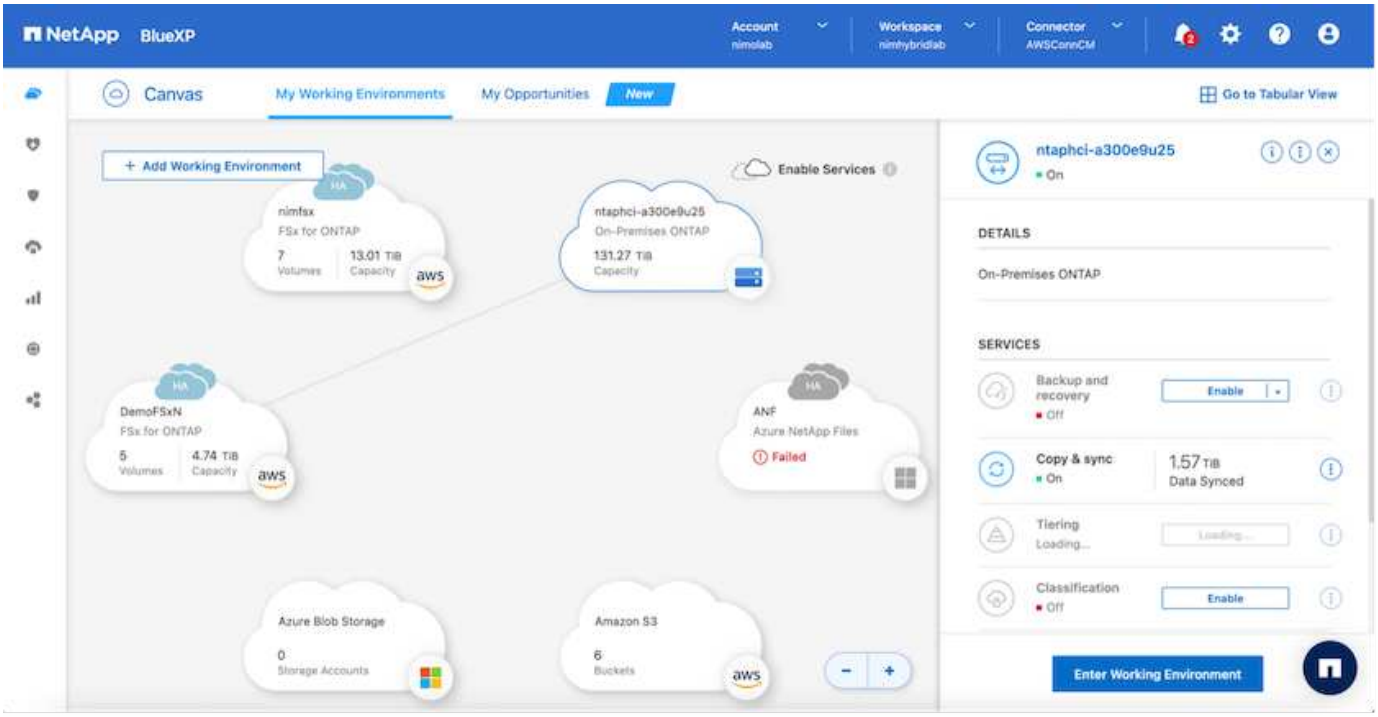
在初始版本中，DRO 支援現有的指示燈集群。按需 SDDC 創建功能將在即將發布的版本中提供。

配置 **FSx ONTAP**

Amazon FSx ONTAP是一項完全託管的服務，它基於流行的NetApp ONTAP檔案系統構建，提供高度可靠、可擴展、高效且功能豐富的文件儲存。請按照此處的步驟操作"關聯"配置和配置 FSx ONTAP。

部署並配置SnapMirror到 FSx ONTAP

下一步是使用 NetApp Console 發現已在 AWS 上配置的 FSx ONTAP 執行個體，並以適當的頻率和 NetApp Snapshot 複本保留，將所需的資料存放區 Volume 從內部部署環境複寫至 FSx ONTAP：



請按照此連結中的步驟設定 DRO。您也可以使用 NetApp ONTAP CLI，按照此連結中的步驟安排複寫。

SnapMirror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 EC2 執行個體或虛擬機器上使用 Ubuntu 作業系統，以確保您符合先決條件。然後安裝該套件。

先決條件

- 確保與來源和目標 vCenter 和儲存系統的連接存在。
- 如果您使用 DNS 名稱，則應該進行 DNS 解析。否則，您應該使用 vCenter 和儲存系統的 IP 位址。
- 建立具有root權限的使用者。您也可以將 sudo 與 EC2 執行個體一起使用。

OS 需求

- Ubuntu 20.04 (LTS)，最低配置 2GB 記憶體和 4 個 vCPU
- 必須在指定的代理虛擬機器上安裝以下軟體包：
  - Docker
  - Docker-compose
  - 傑

更改權限 `docker.sock`： `sudo chmod 666 /var/run/docker.sock` 。

這 `deploy.sh`腳本執行所有必要的先決條件。

安裝包

1. 在指定虛擬機器上下載安裝包：

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

此代理程式可以安裝在本機或 AWS VPC 內。

2. 解壓縮包，執行部署腳本，輸入主機IP（例如10.10.10.10）。

```
tar xvf DRO-prereq.tar
```

3. 導航至目錄並執行部署腳本，如下所示：

```
sudo sh deploy.sh
```

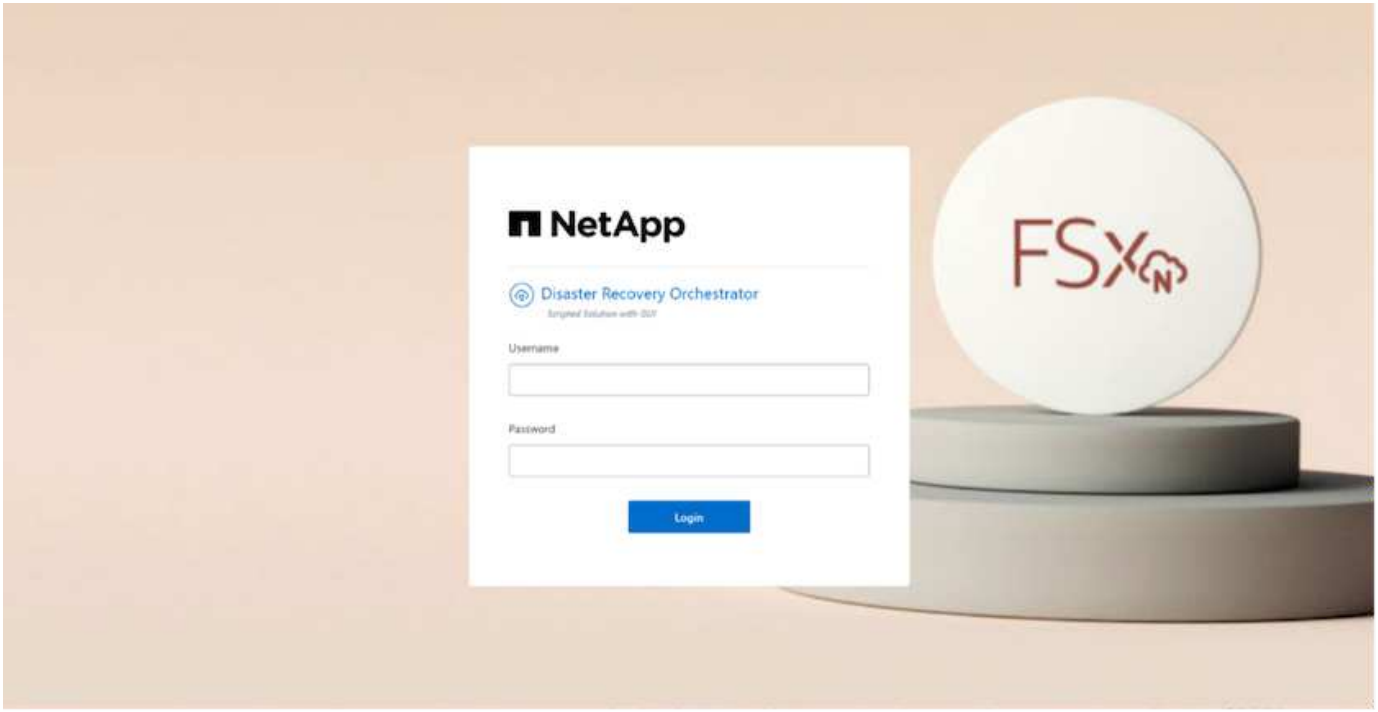
4. 使用以下方式存取 UI：

```
https://<host-ip-address>
```

使用以下預設憑證：

```
Username: admin
Password: admin
```

可以使用“更改密碼”選項來更改密碼。



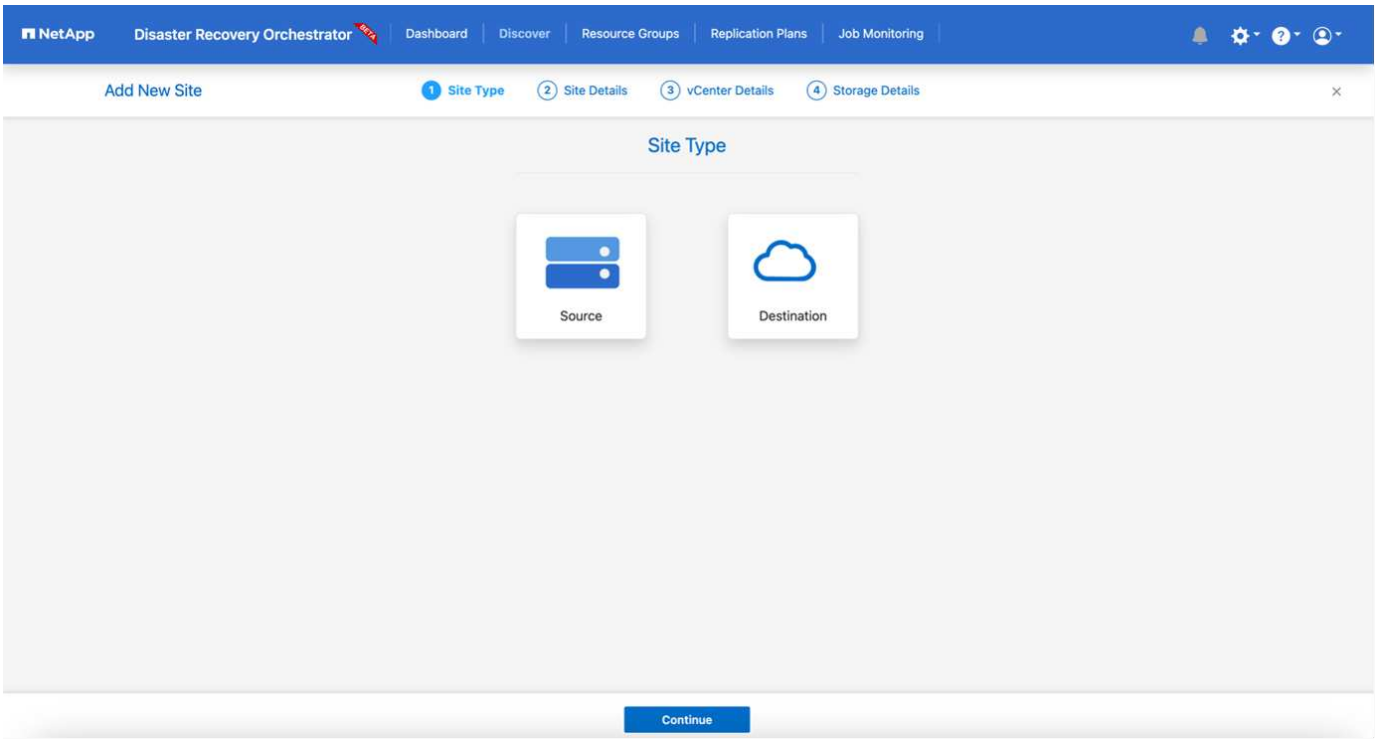
DRO 配置

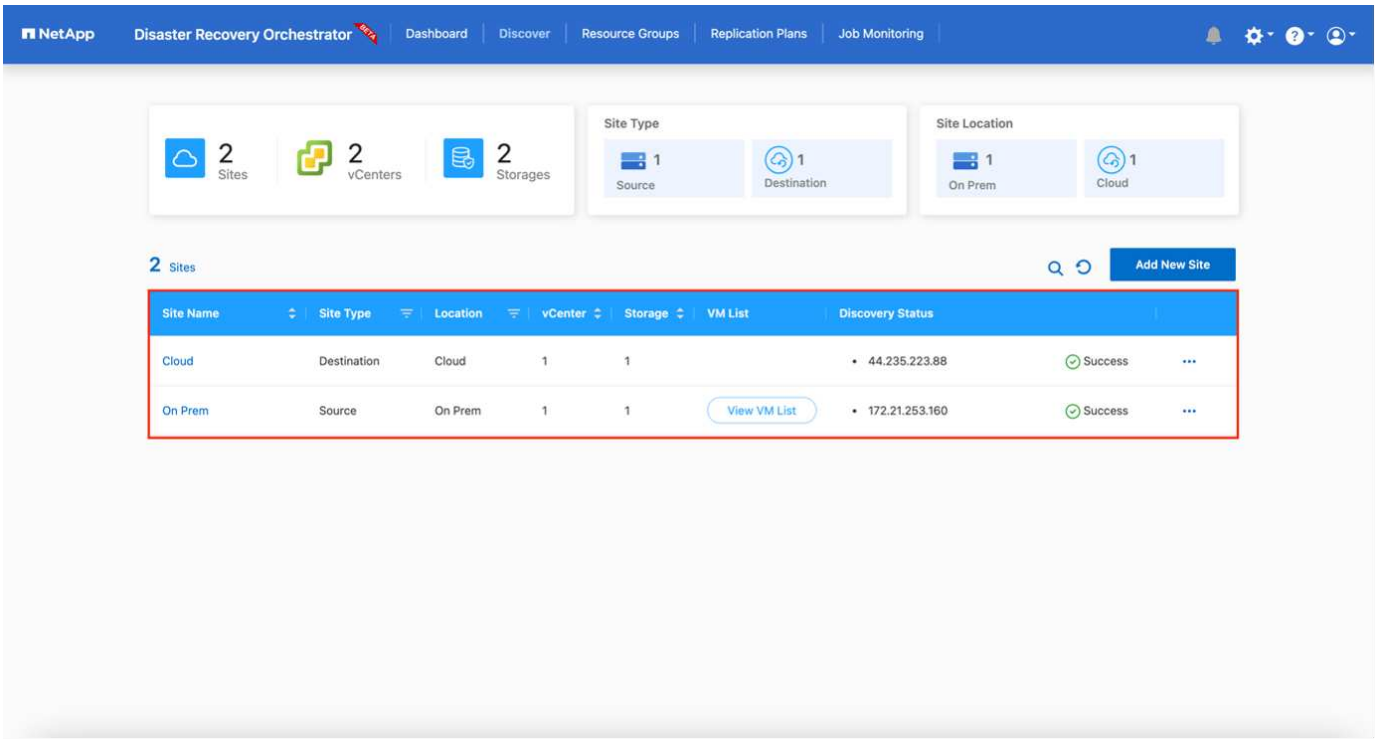
正確配置 FSx ONTAP和 VMC 後，您可以開始設定 DRO，以使用 FSx ONTAP上的唯讀SnapMirror副本自動將本機工作負載還原到 VMC。

NetApp建議在 AWS 中部署 DRO 代理，並將其部署到部署 FSx ONTAP 的相同 VPC（也可以對等連接），以便 DRO 代理可以透過網路與您的內部元件以及 FSx ONTAP和 VMC 資源進行通訊。

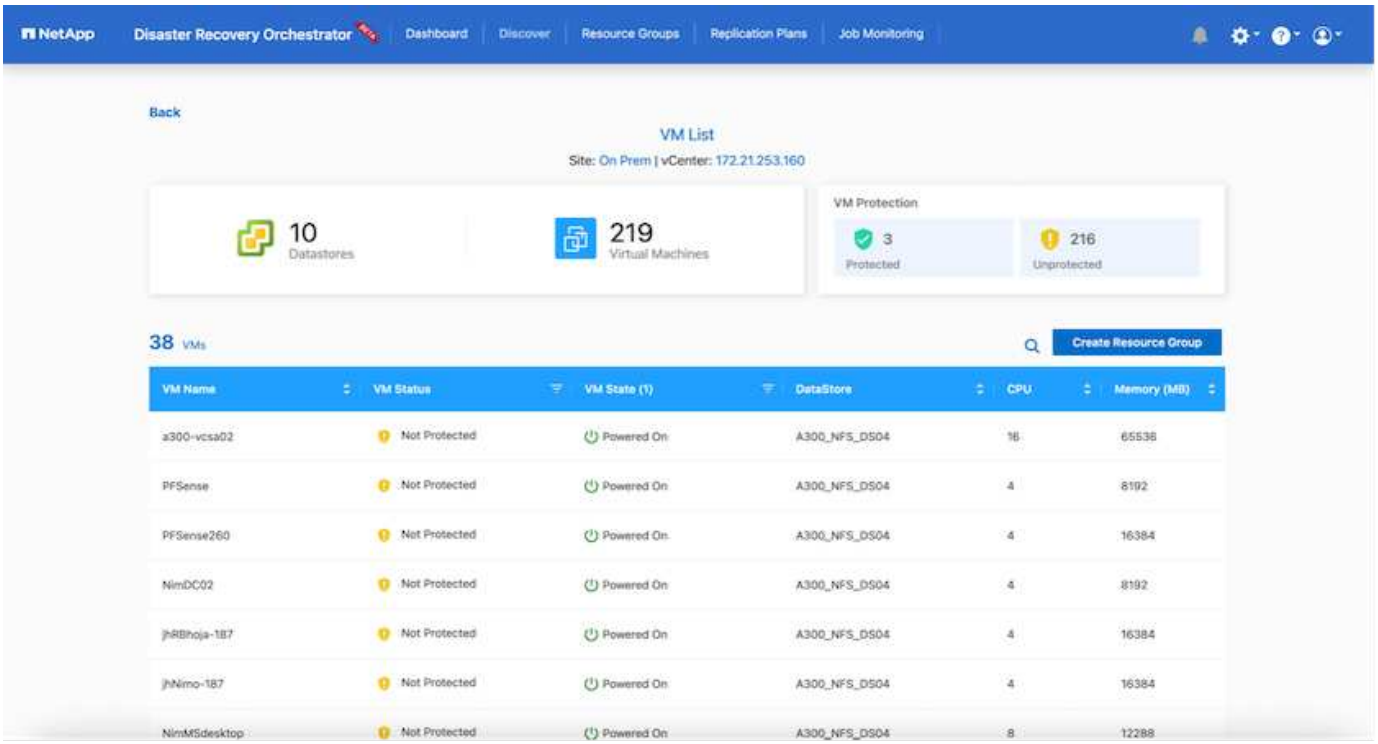
第一步是發現並將本機和雲端資源（vCenter 和儲存）新增至 DRO。在支援的瀏覽器中開啟 DRO 並使用預設使用者名稱和密碼（admin/admin）並新增網站。也可以使用「發現」選項新增網站。新增以下平台：

- 本地
  - 本機 vCenter
  - ONTAP儲存系統
- 雲端
  - VMC vCenter
  - FSx ONTAP





新增後，DRO 會執行自動發現並顯示從來源儲存到 FSx ONTAP具有對應SnapMirror副本的虛擬機器。 DRO 會自動偵測虛擬機器使用的網路和連接埠群組並填入它們。



下一步是將所需的虛擬機器分組到功能組中，作為資源組。

資源分組

新增平台後，您可以將要還原的虛擬機器分組到資源組中。 DRO 資源群組可讓您將一組從屬虛擬機器分組為邏輯群組，這些邏輯群組包含它們的啟動順序、啟動延遲以及可在復原時執行的選用應用程式驗證。

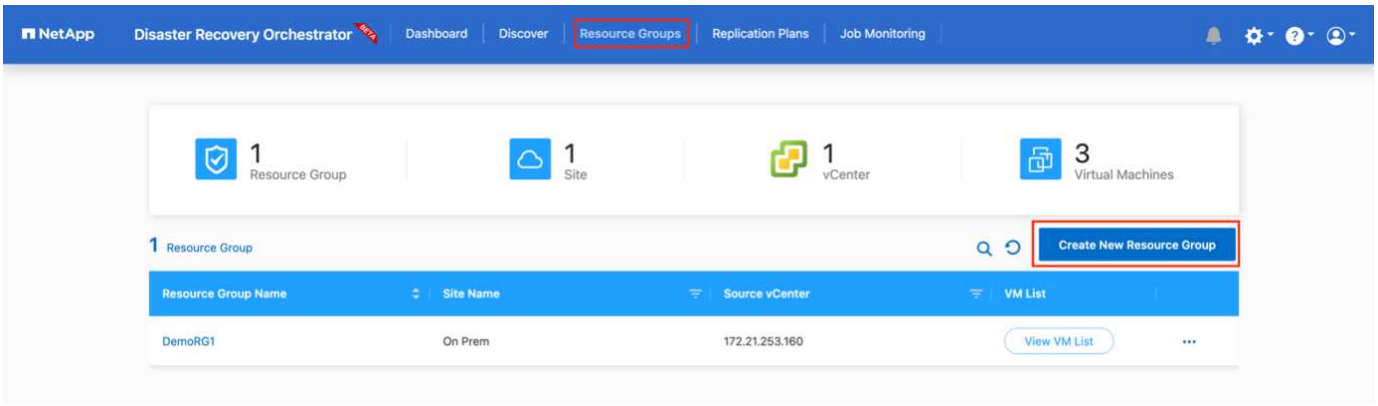
若要開始建立資源組，請完成以下步驟：

1. 存取*資源組*，然後按一下*建立新資源組*。
2. 在「新資源組」下，從下拉式選單中選擇來源站點，然後按一下「建立」。
3. 提供*資源組詳細資訊*並點選*繼續*。
4. 使用搜尋選項選擇適當的虛擬機器。
5. 為所選虛擬機器選擇啟動順序和啟動延遲（秒）。透過選擇每個虛擬機器並設定其優先順序來設定開機順序。所有虛擬機器的預設值都是三。

   選項如下：

   1 – 第一台啟動的虛擬機 3 – 預設 5 – 最後一個啟動的虛擬機

6. 按一下“建立資源組”。

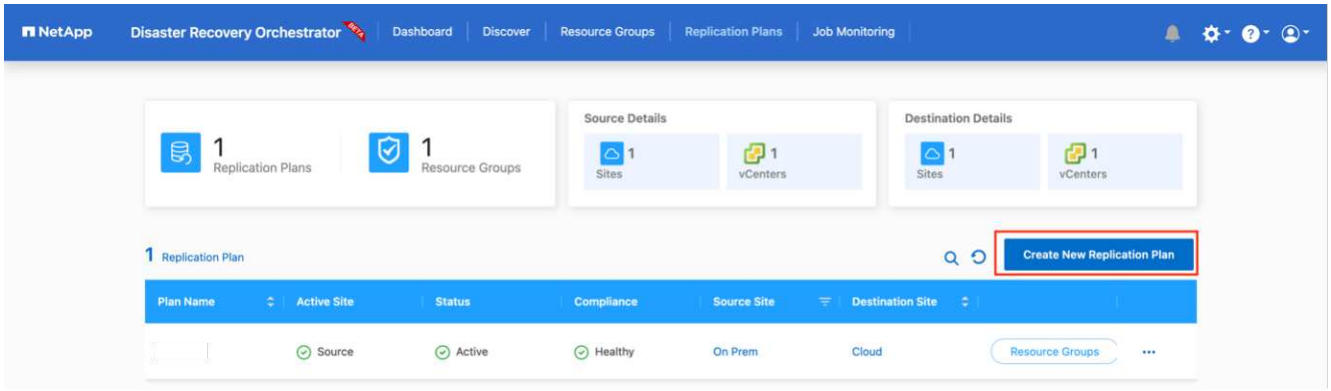


複製計劃

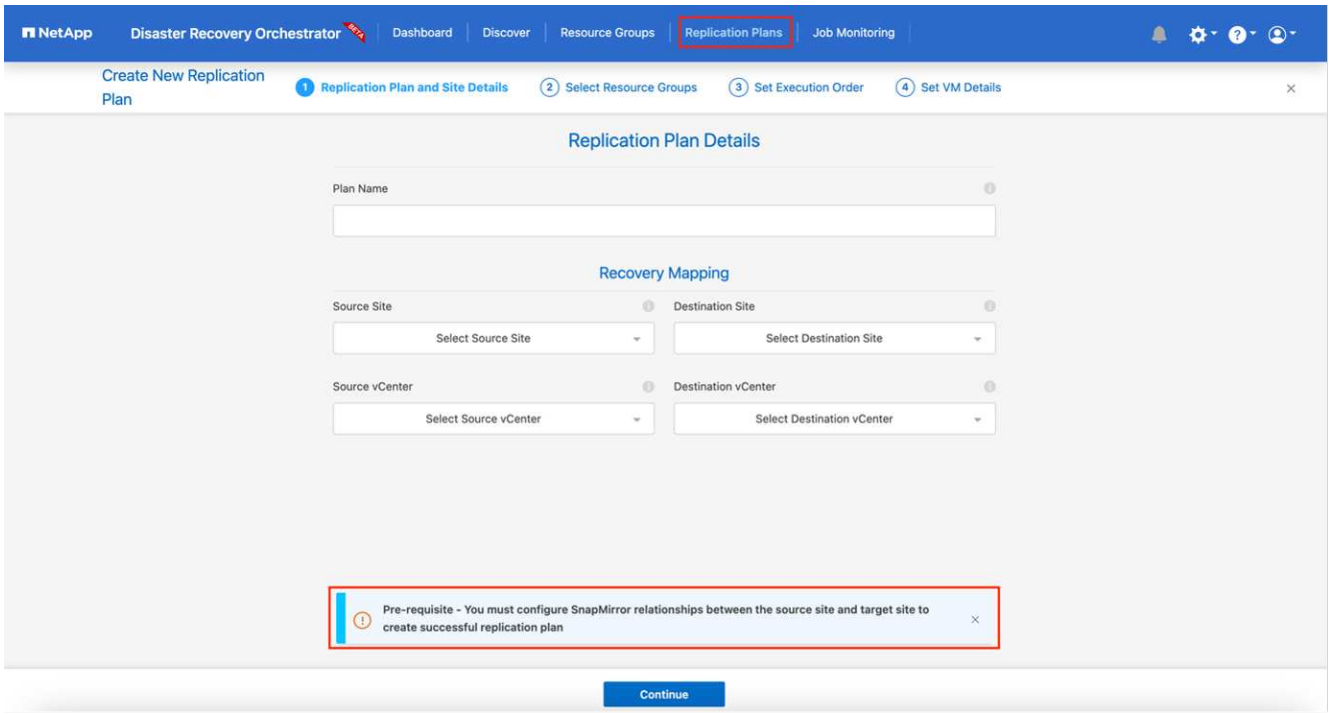
您需要一個在災難發生時恢復應用程式的計劃。從下拉式選單中選擇來源和目標 vCenter 平台，並選擇要包含在該計劃中的資源組，以及應用程式應如何恢復和啟動的分組（例如，網域控制器，然後是第 1 層，然後是第 2 層，等等）。這類計劃有時也稱為藍圖。若要定義復原計劃，請導覽至「複製計劃」標籤並按一下「新複製計劃」。

若要開始建立複製計劃，請完成以下步驟：

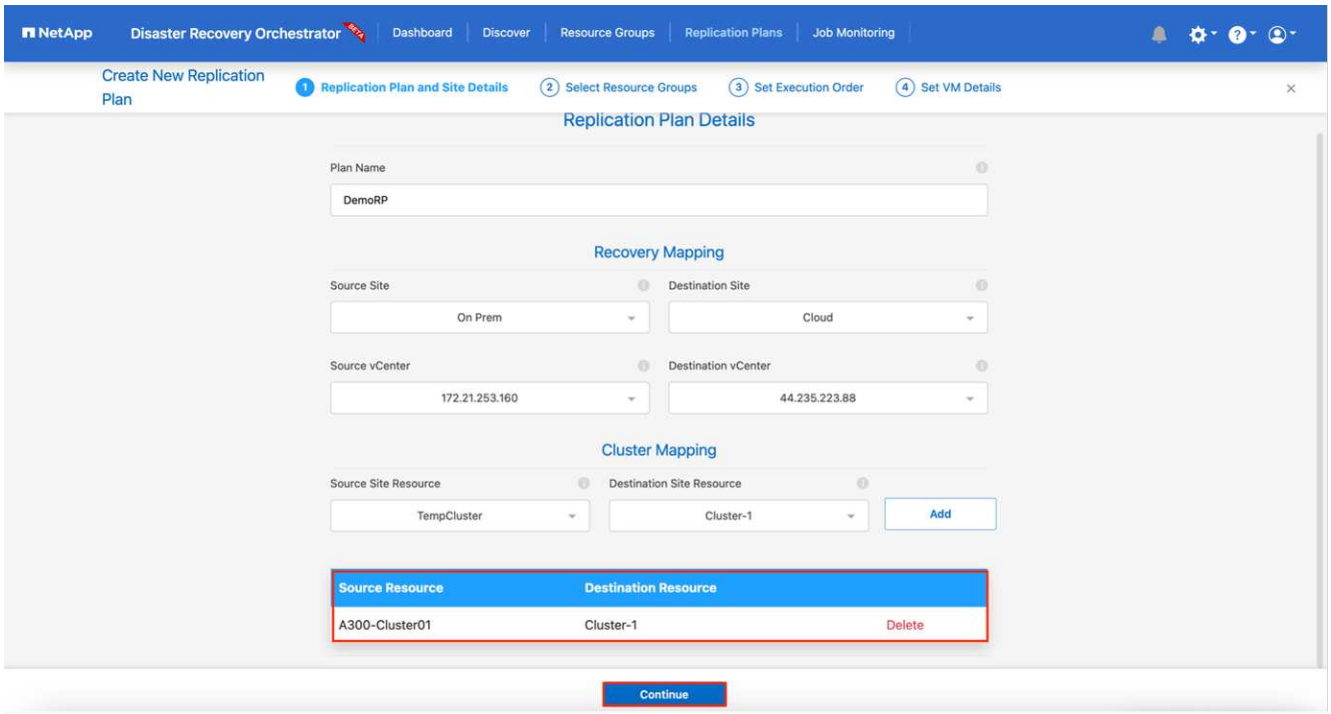
1. 存取*複製計劃*，然後按一下*建立新的複製計劃*。



2. 在「新複製計畫」下，提供計畫名稱並透過選擇來源網站、關聯 vCenter、目標網站和關聯 vCenter 新增復原對應。



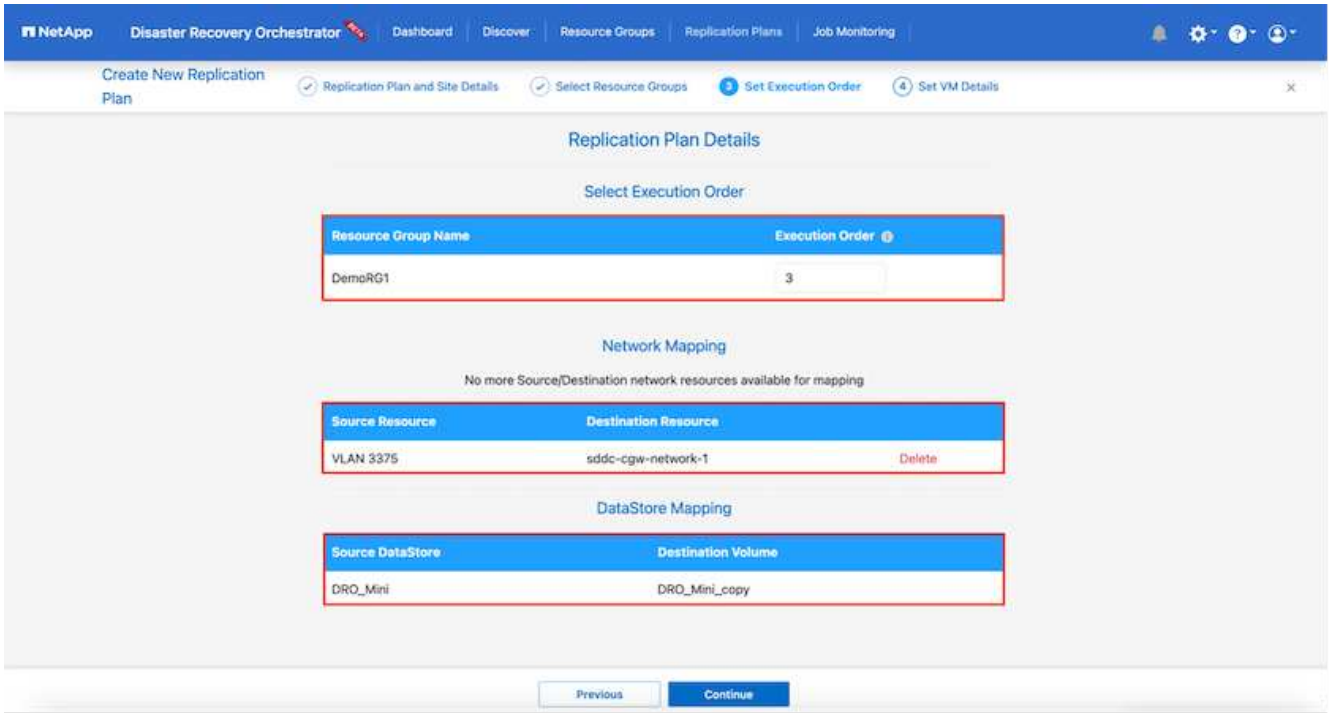
3. Recovery映射完成後，選擇叢集映射。



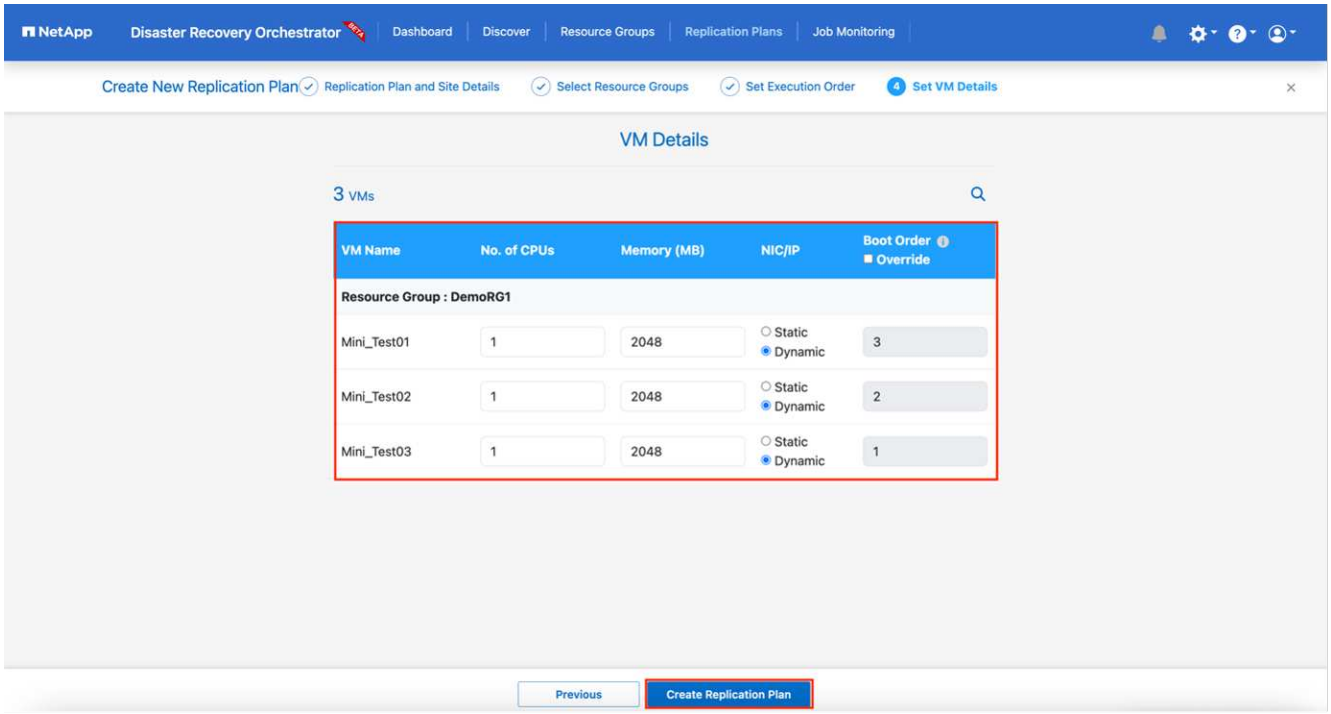
4. 選擇*資源組詳情*並點選*繼續*。
5. 設定資源組的執行順序。當存在多個資源組時，此選項可讓您選擇操作順序。
6. 完成後，選擇網路對應到適當的網段。這些段應該已經在 VMC 中配置，因此請選擇適當的段來對應 VM。
7. 根據虛擬機器的選擇，自動選擇資料儲存映射。

SnapMirror處於磁碟區層級。因此，所有虛擬機器都被複製到複製目標。確保選擇資料儲存

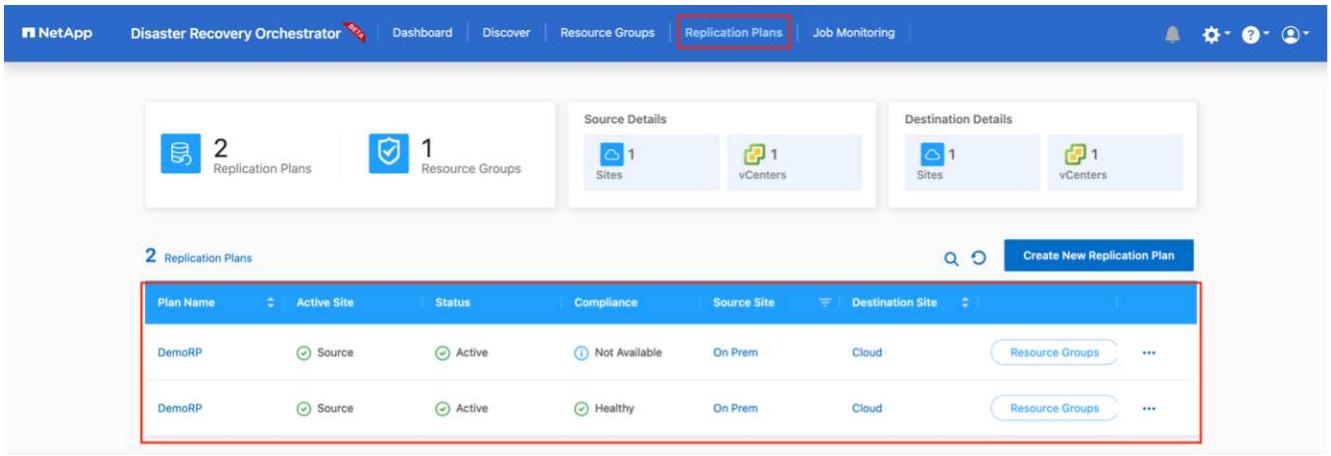
區中的所有虛擬機器。如果未選擇，則僅處理複製計劃中的虛擬機器。



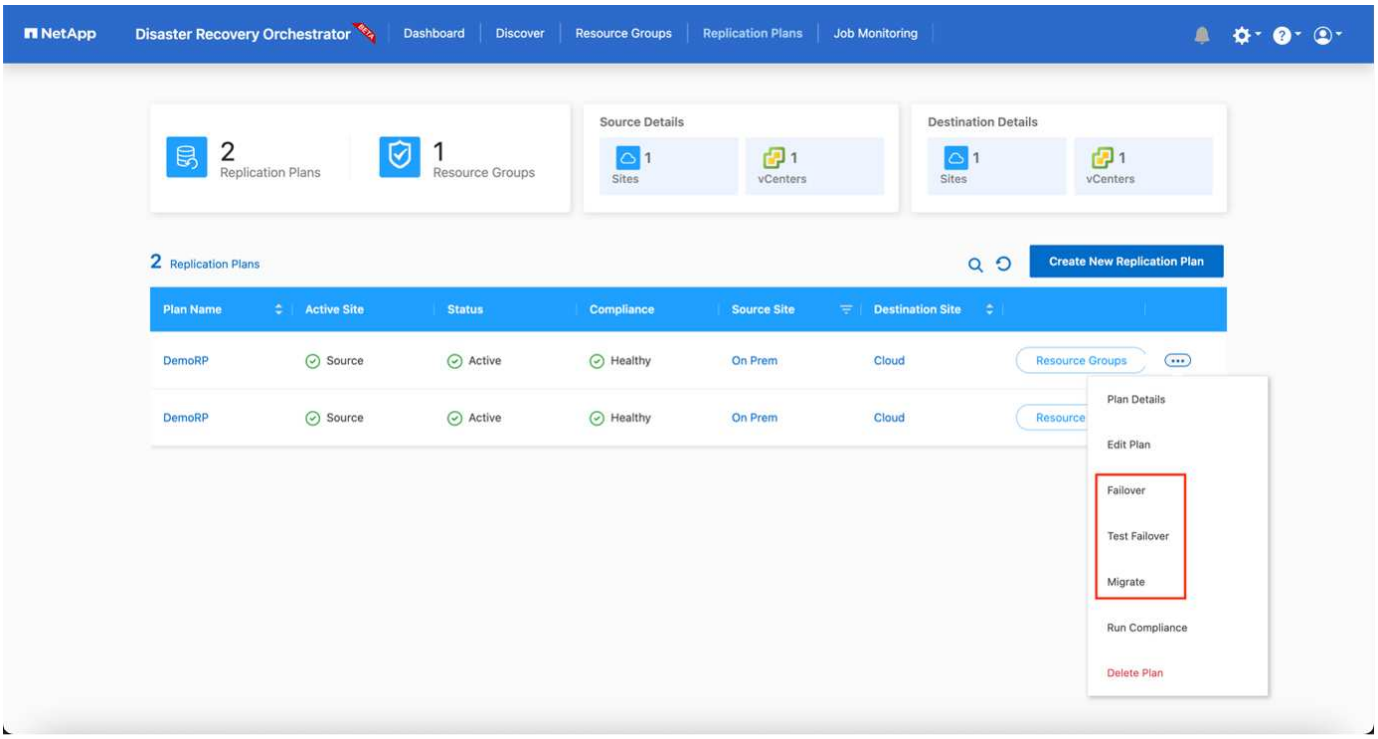
8. 在 VM 詳細資訊下，您可以選擇調整 VM 的 CPU 和 RAM 參數的大小；當將大型環境還原到較小的目標叢集或進行 DR 測試時，這非常有用，而無需配置一對一的實體 VMware 基礎架構。此外，您還可以修改資源組中所有選定虛擬機器的啟動順序和啟動延遲（秒）。如果需要對資源組啟動順序選擇期間選擇的順序進行任何更改，則可以選擇修改啟動順序。預設情況下，使用在資源組選擇期間選擇的啟動順序；但是，可以在此階段執行任何修改。

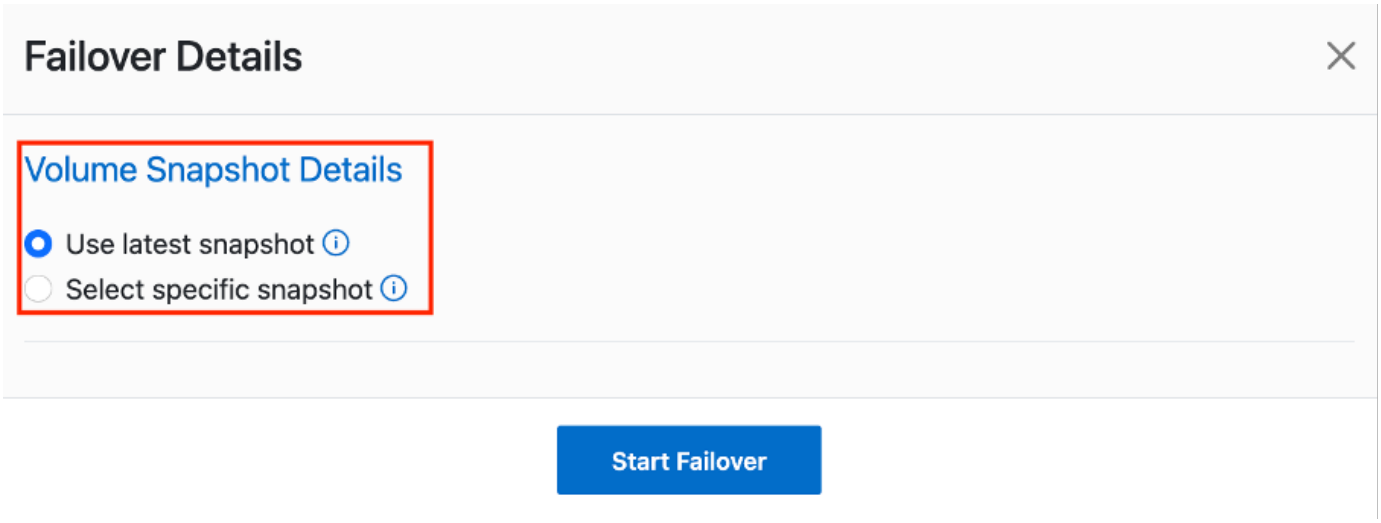


9. 按一下「建立複製計劃」。

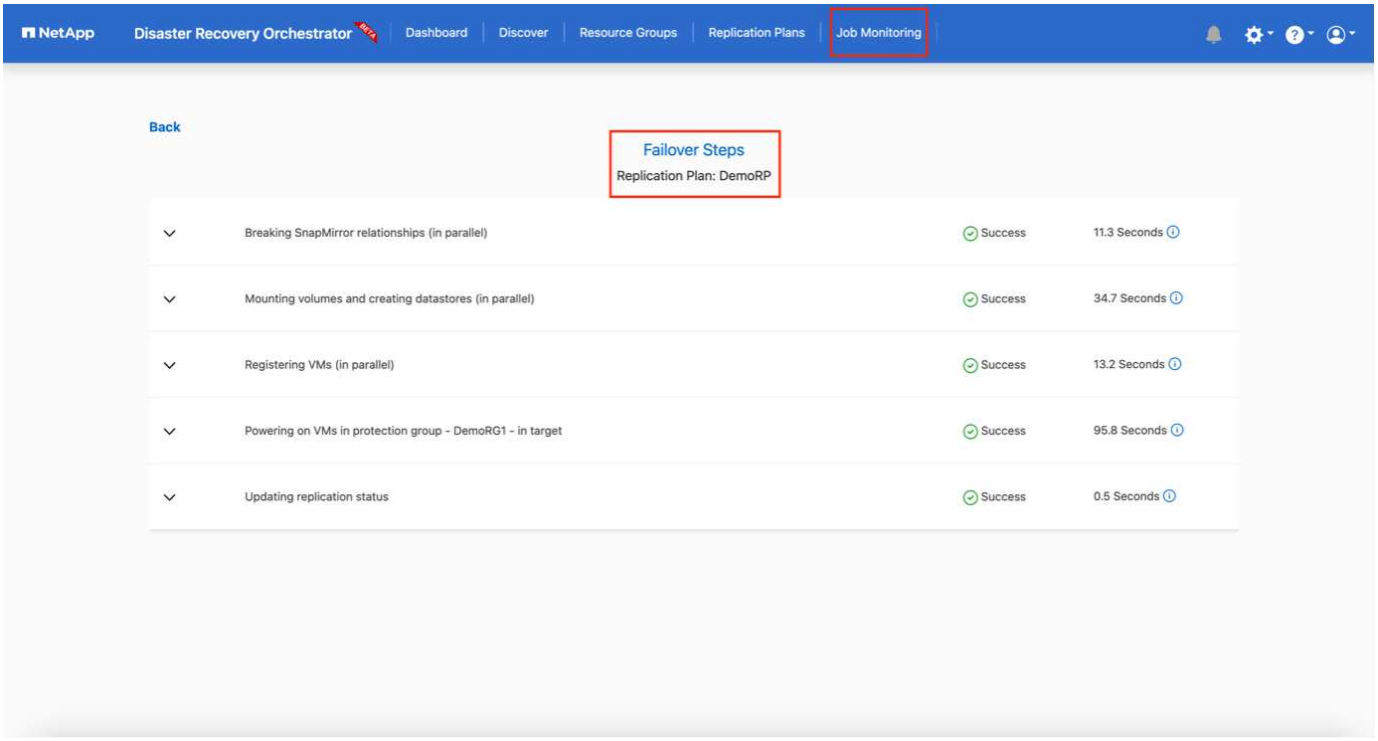


建立複製計劃後，可以根據需求執行故障轉移選項、測試故障轉移選項或遷移選項。在故障轉移和測試故障轉移選項期間，使用最新的SnapMirror Snapshot 副本，或可以從時間點 Snapshot 副本中選擇特定的 Snapshot 副本（根據SnapMirror的保留策略）。如果您面臨勒索軟體之類的損壞事件，則時間點選項可能非常有用，其中最新的副本已被破壞或加密。 DRO 顯示所有可用的時間點。若要使用複製計畫中指定的設定觸發故障轉移或測試故障轉移，您可以按一下「故障轉移」或「測試故障轉移」。

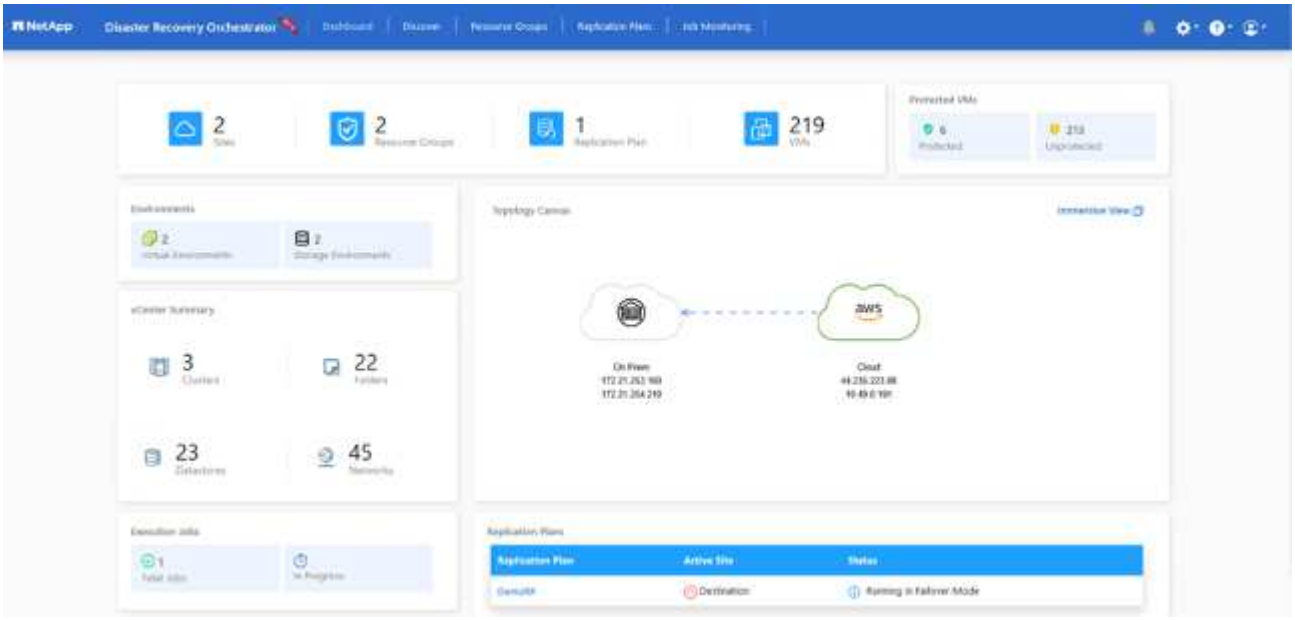




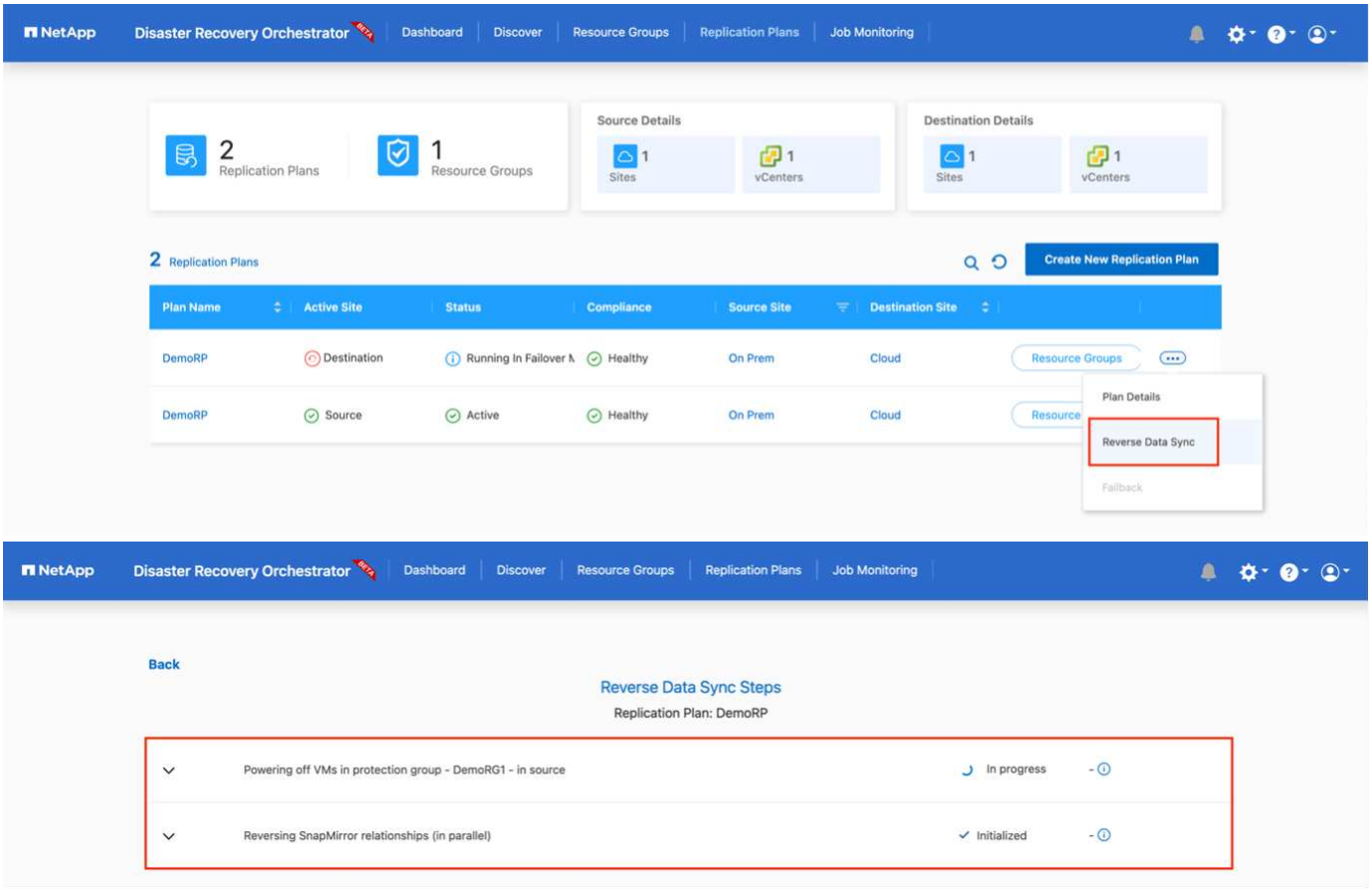
可以在任務選單中監控複製計劃：



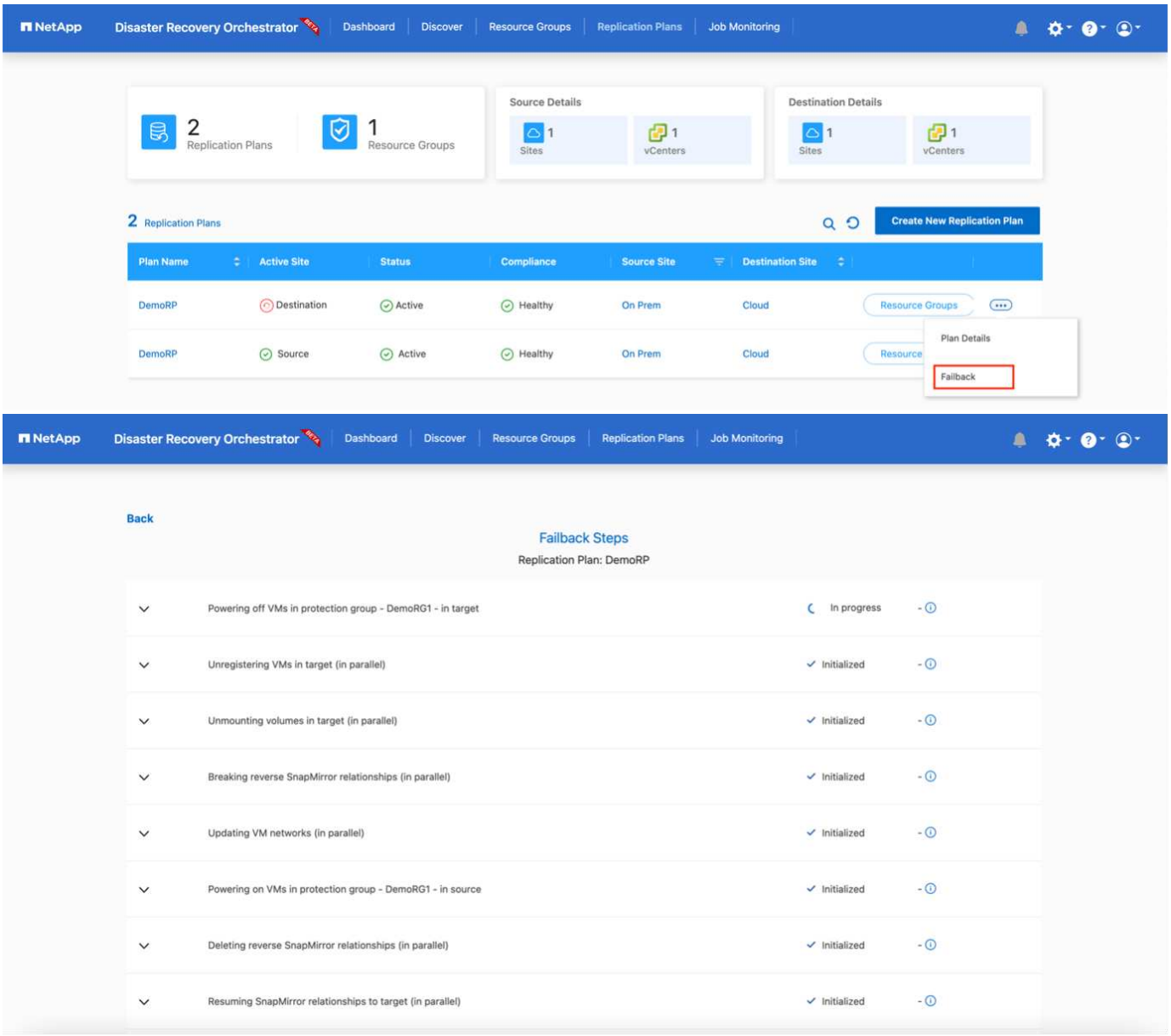
觸發故障轉移後，可以在 VMC vCenter（虛擬機器、網路、資料儲存）中看到復原的項目。預設情況下，虛擬機器將恢復到工作負載資料夾。



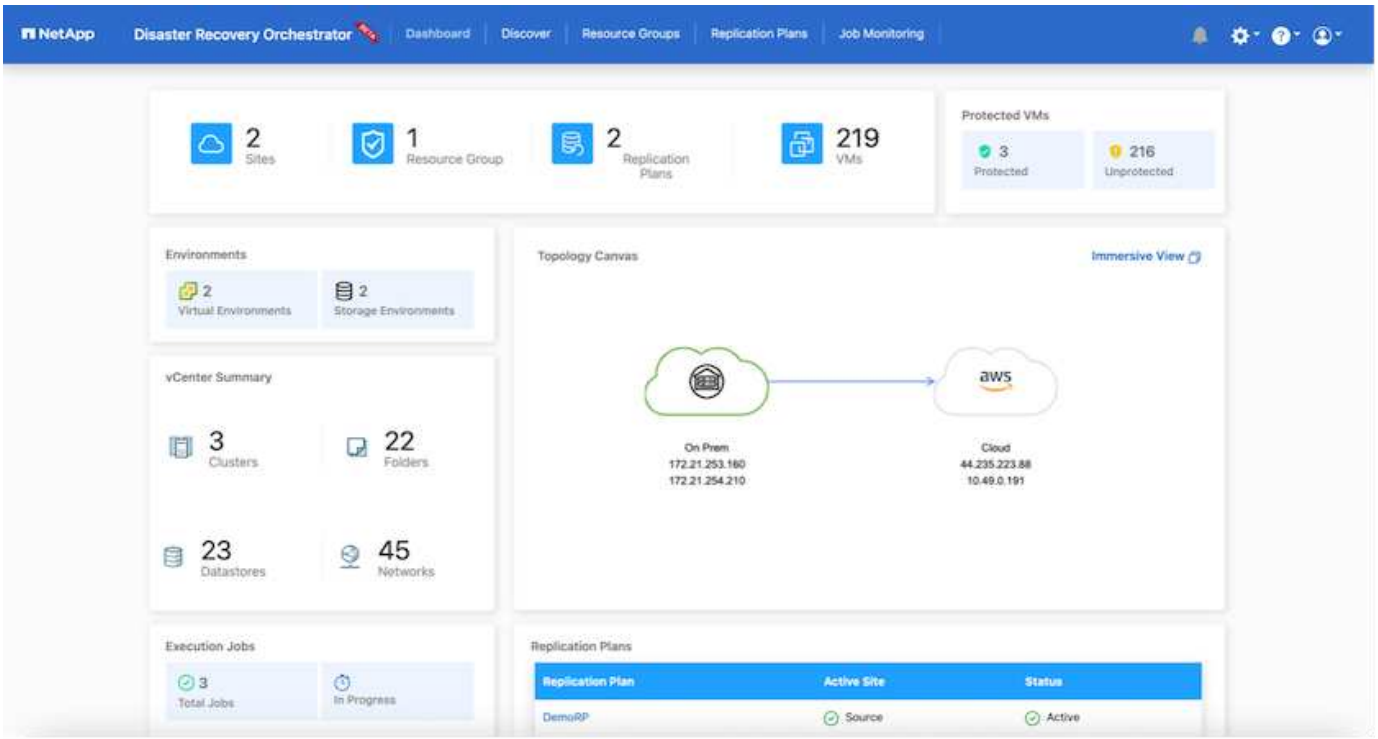
可以在複製計劃層級觸發故障恢復。對於測試故障轉移，可使用拆除選項來回變更並刪除FlexClone關係。與故障轉移相關的故障回復是一個兩步驟過程。選擇複製計劃並選擇*反向資料同步*。



一旦完成後，您可以觸發故障復原以返回原始生產網站。



在 NetApp Console 中，我們可以看到適當 Volume 的複寫健全狀況已中斷（即那些以讀寫 Volume 形式對應至 VMC 的 Volume）。在測試容錯移轉期間，DRO 不會對應目的地或複本 Volume。而是會建立所需 SnapMirror（或 Snapshot 快照技術）執行個體的 FlexClone® 複本，並公開 FlexClone® 執行個體，而不會為 FSx ONTAP 使用額外的實體容量。此程序可確保 Volume 不會遭到修改，且即使在 DR 測試或分類工作流程期間，複本工作也能持續執行。此外，此程序可確保在發生錯誤或恢復損毀資料的情況下，能夠清除恢復內容，而不會有複本遭到銷毀的風險。



勒索軟體恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體來說，IT 組織很難確定安全返回點在哪裡，而且一旦確定，就很難保護恢復的工作負載免受例如休眠惡意軟體或易受攻擊的應用程式的重複攻擊。

DRO 可讓您從任何可用時間點復原系統，從而解決這些問題。您還可以將工作負載恢復到功能正常但隔離的網路中，以便應用程式可以在不會暴露於南北流量的位置運行並相互通訊。這為您的安全團隊提供了一個安全的地方來進行取證，並確保沒有隱藏或休眠的惡意軟體。

好處

- 使用高效且有彈性的SnapMirror複製。
- 透過 Snapshot 副本保留恢復到任何可用的時間點。
- 完全自動化從儲存、運算、網路和應用程式驗證步驟中恢復數百到數千台虛擬機器所需的所有步驟。
- 使用ONTAP FlexClone技術進行工作負載恢復，採用的方法是不改變複製磁碟區。
  - 避免磁碟區或 Snapshot 副本的資料損壞風險。
  - 避免 DR 測試工作流程期間的複製中斷。
  - DR 資料與雲端運算資源的潛在用途，可用於 DR 以外的工作流程，例如開發測試、安全測試、修補程式或升級測試以及補救測試。
- 透過允許恢復到較小的運算集群，CPU 和 RAM 優化有助於降低雲端成本。

使用 **Veeam Replication** 和 **FSx ONTAP**實作 **VMware Cloud on AWS** 災難復原

Amazon FSx ONTAP與 VMware Cloud on AWS 的整合是一個 AWS 管理的外部 NFS 資料存儲，它建立在 NetApp 的ONTAP檔案系統上，可以連接到 SDDC 中的叢集。它為客戶提供靈活、高效能的虛擬化儲存基礎設施，可獨立於運算資源進行擴充。

概況

對於希望使用 VMware Cloud on AWS SDDC 作為災難復原目標的客戶，可以使用 FSx ONTAP資料儲存區透過任何經過驗證且提供 VM 複製功能的第三方解決方案從本機複製資料。透過新增 FSx ONTAP資料存儲，它將實現成本優化部署，而不是在 AWS SDDC 上建置 VMware 雲，並使用大量 ESXi 主機來容納儲存。

這種方法還可以幫助客戶使用 VMC 中的試點燈叢集以及 FSx ONTAP資料儲存來託管 VM 副本。透過優雅地故障轉移複製計劃，相同的流程還可以擴展為到 VMware Cloud on AWS 的遷移選項。

問題陳述

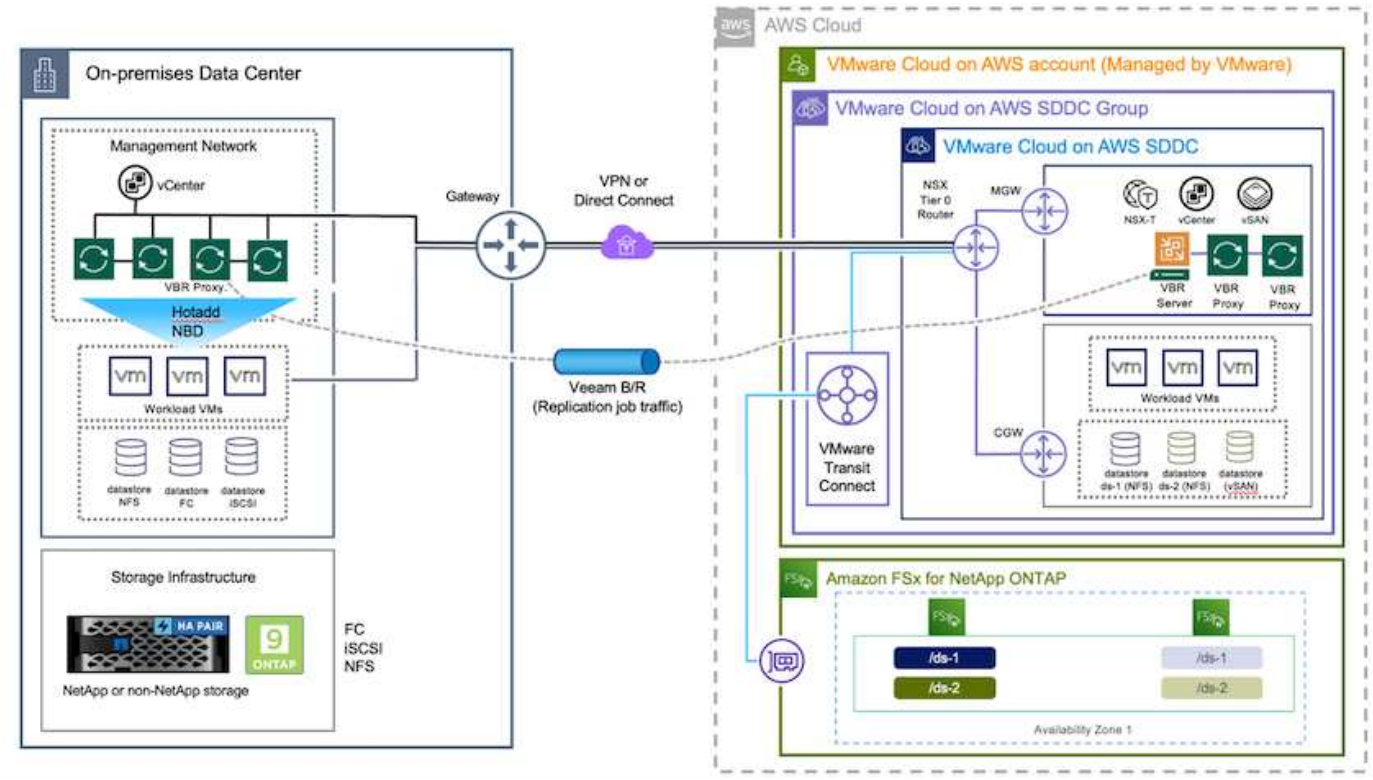
本文檔說明如何使用 FSx ONTAP資料儲存和 Veeam Backup 和複製，透過 VM 複製功能為本機 VMware VM 到 VMware Cloud on AWS 設定災難復原。

Veeam Backup & Replication 允許現場和遠端複製以實現災難復原 (DR)。當虛擬機器被複製時，Veeam Backup & Replication 會在目標 VMware Cloud on AWS SDDC 叢集上以原生 VMware vSphere 格式建立虛擬機器的精確副本，並使該副本與原始虛擬機器保持同步。

由於存在處於準備啟動狀態的 VM 副本，因此複製可提供最佳復原時間目標 (RTO) 值。此複製機制可確保在災難事件發生時工作負載能夠在 VMware Cloud on AWS SDDC 中快速啟動。 Veeam Backup & Replication 軟體也優化了透過 WAN 和慢速連線進行複製的流量傳輸。此外，它還過濾掉重複的資料塊、零資料塊、交換文件和排除的 VM 客戶作業系統文件，並壓縮副本流量。

為了防止複製作業消耗整個網路頻寬，可以實施 WAN 加速器和網路限制規則。 Veeam Backup & Replication 中的複製過程由作業驅動，這表示複製是透過設定複製作業來執行的。如果發生災難事件，可以觸發故障轉移，透過故障轉移到其副本來恢復虛擬機器。

當執行故障轉移時，複製的虛擬機器將接管原始虛擬機器的角色。可以將故障轉移到副本的最新狀態或任何已知的良好還原點。這使得勒索軟體恢復或隔離測試能夠根據需要進行。在 Veeam Backup & Replication 中，故障轉移和故障復原是臨時的中間步驟，需要進一步完成。 Veeam Backup & Replication 提供多種選項來處理不同的災難復原場景。



解決方案部署

進階步驟

1. Veeam Backup and Replication 軟體在具有適當網路連線的本機環境中運作。
2. 設定 VMware Cloud on AWS，請參閱 VMware Cloud Tech Zone 文章 "VMware Cloud on AWS 與Amazon FSx ONTAP整合部署指南" 以部署、設定 VMware Cloud on AWS SDDC 和 FSx ONTAP 作為 NFS 資料儲存。（可以使用設定為最低組態的試驗環境來進行災難復原。發生事件時，VMs 將容錯移轉至此叢集，並且可以新增額外的節點。）
3. 設定複製作業以使用 Veeam Backup and Replication 建立 VM 副本。
4. 建立故障轉移計劃並執行故障轉移。
5. 災難事件結束且主站點啟動後，切換回生產虛擬機器。

Veeam VM 複製到 **VMC** 和 **FSx ONTAP**資料儲存的先決條件

1. 確保 Veeam Backup & Replication 備份 VM 連線到來源 vCenter 以及 AWS SDDC 叢集上的目標 VMware 雲端。
2. 備份伺服器必須能夠解析短名稱並連接到來源 vCenter 和目標 vCenter。
3. 目標 FSx ONTAP資料儲存必須具有足夠的可用空間來儲存複製虛擬機器的 VMDK

有關更多信息，請參閱“注意事項和限制”"這裡" 。

部署詳情

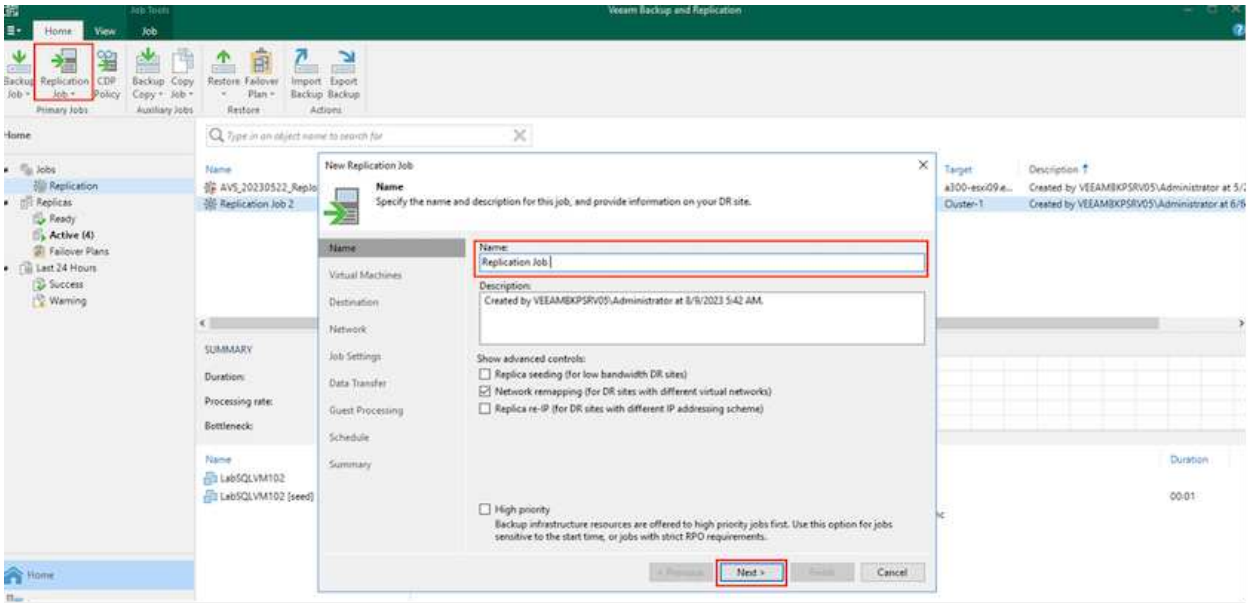
▼ 步驟 **1**：複製虛擬機

Veeam Backup & Replication 利用 VMware vSphere 快照功能，在複製期間，Veeam Backup & Replication

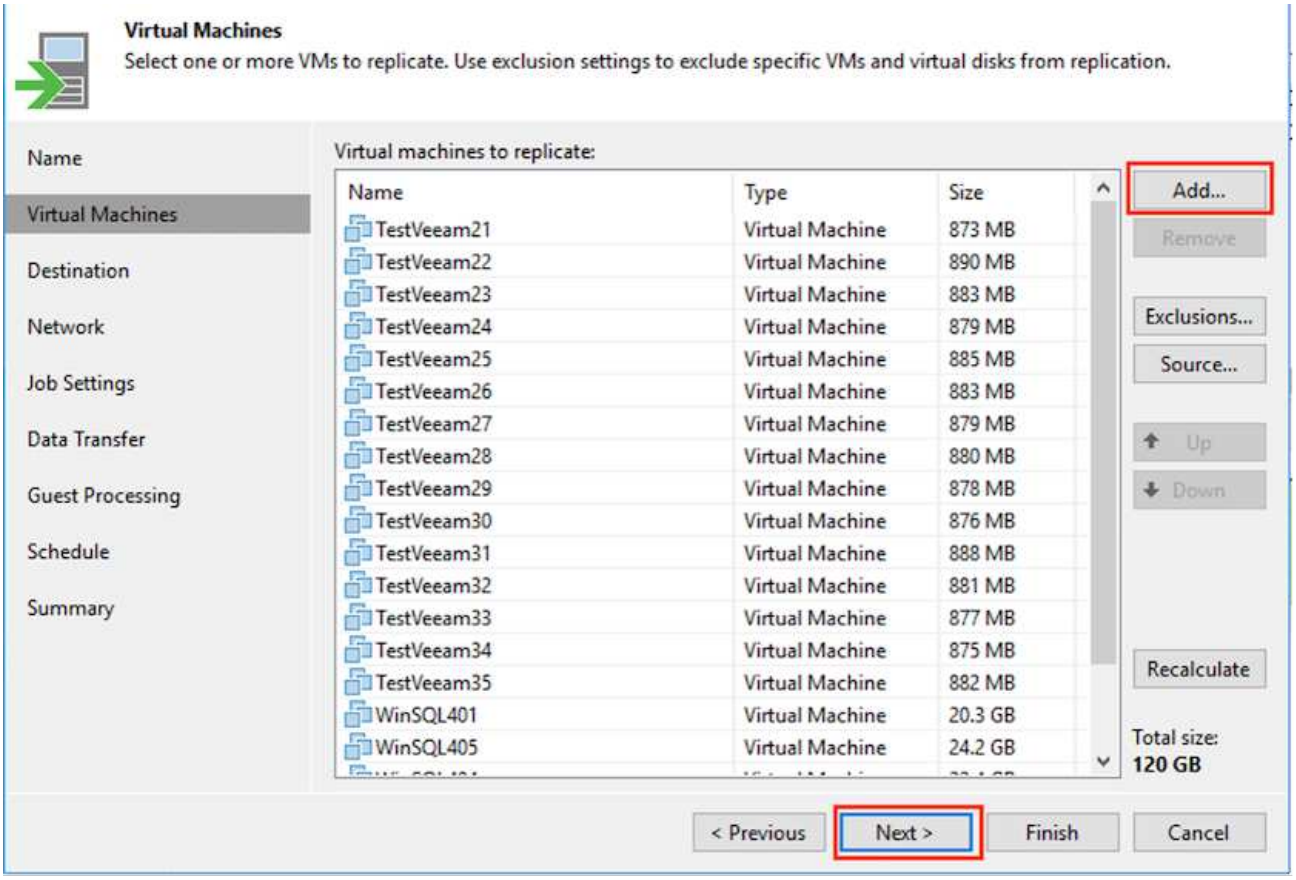
請求 VMware vSphere 建立 VM 快照。 VM 快照是 VM 的時間點副本，其中包含虛擬磁碟、系統狀態、配置等。 Veeam Backup & Replication 使用快照作為複製的資料來源。

若要複製虛擬機，請依照下列步驟操作：

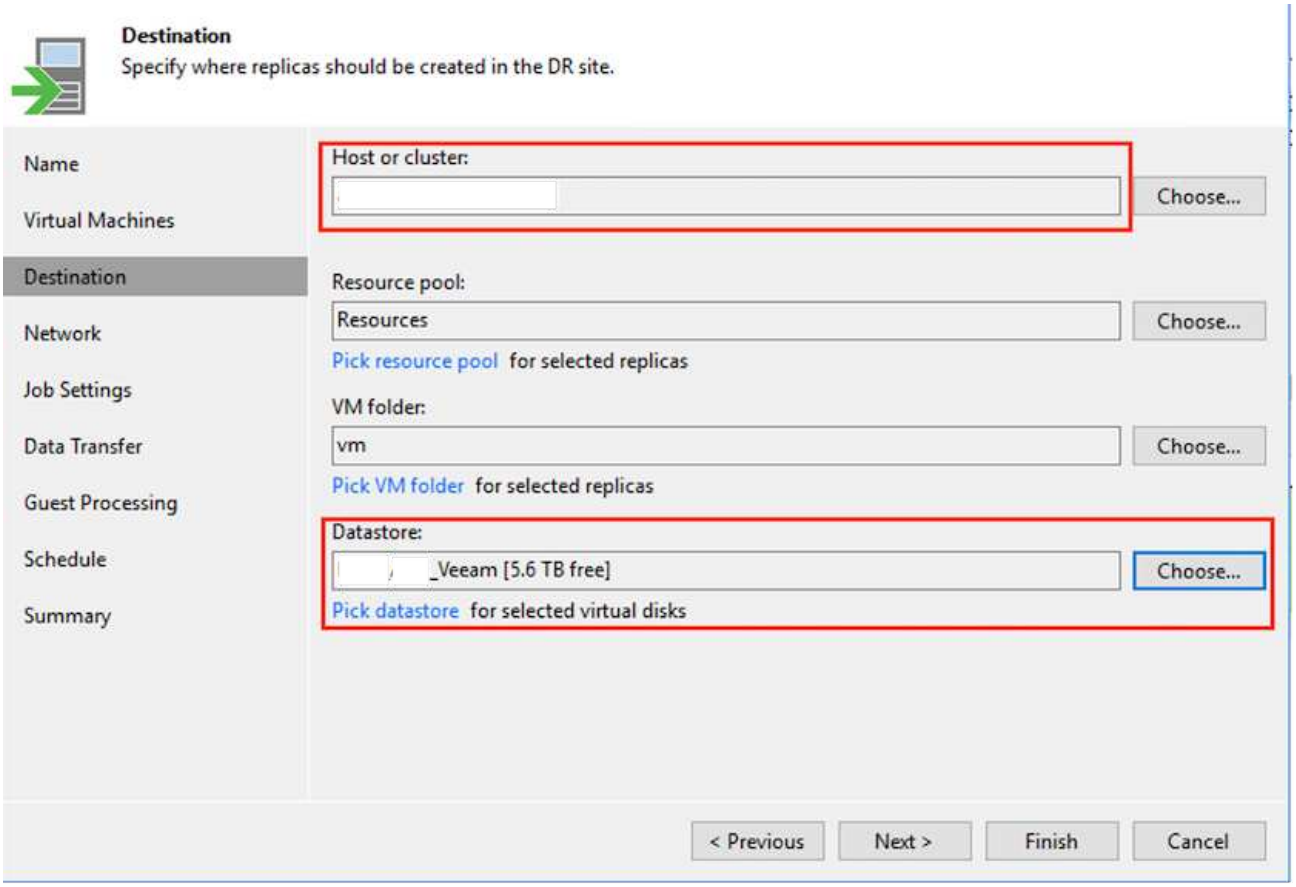
1. 開啟 Veeam 備份和複製控制台。
2. 在主頁檢視上，選擇複製作業 > 虛擬機器 > VMware vSphere。
3. 指定作業名稱並選擇適當的進階控制複選框。按一下“下一步”。
   - 如果本機和 AWS 之間的連線頻寬受限，請勾選「副本播種」複選框。
   - 如果 VMware Cloud on AWS SDDC 上的段與本機站點網路的段不匹配，請選取網路重新對應（針對具有不同網路的 AWS VMC 站點）複選框。
   - 如果本機生產站點中的 IP 位址方案與 AWS VMC 站點中的方案不同，請選取副本重新 IP（對於具有不同 IP 位址方案的 DR 站點）核取方塊。



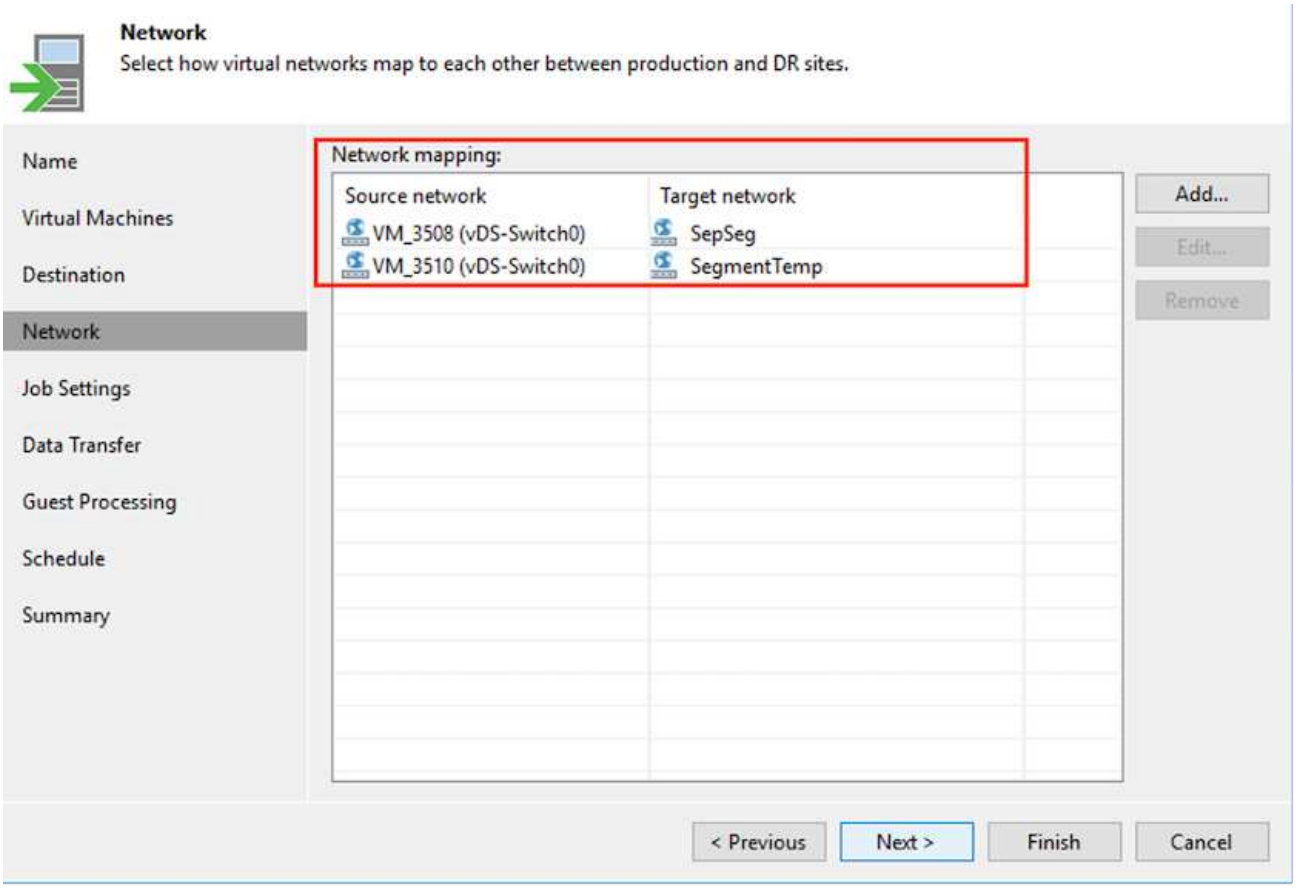
4. 在「虛擬機器」步驟中選擇需要複製到連接到 VMware Cloud on AWS SDDC 的 FSx ONTAP資料儲存的虛擬機器。可以將虛擬機器放置在 vSAN 上以填入可用的 vSAN 資料儲存容量。在試點叢集中，3 節點叢集的可用容量將受到限制。其餘資料可以複製到 FSx ONTAP資料儲存。按一下*新增*，然後在*新增物件*視窗中選擇必要的虛擬機器或虛擬機器容器，然後按一下*新增*。按一下“下一步”。



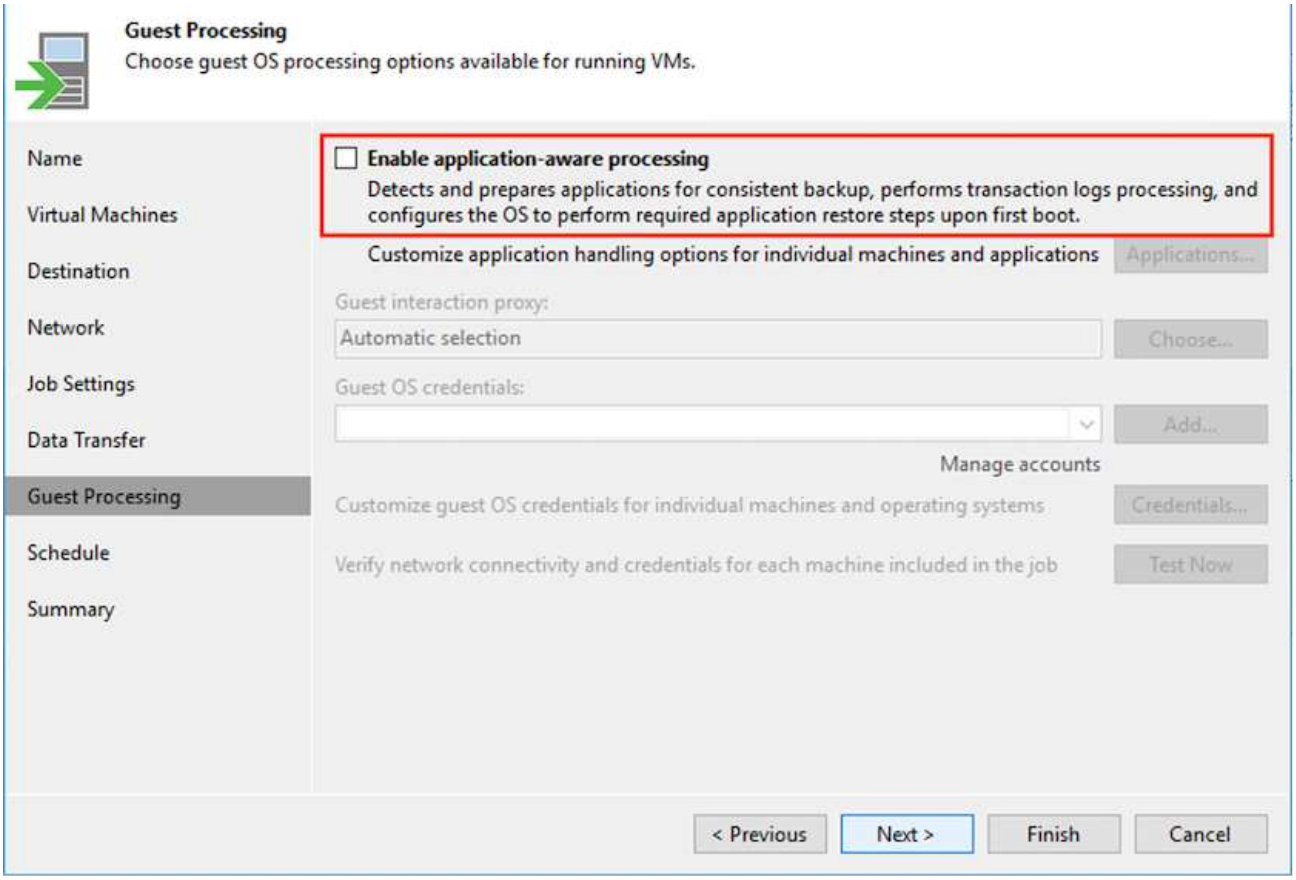
5. 之後，選擇目標為 VMware Cloud on AWS SDDC 叢集/主機，並選擇適當的資源池、VM 資料夾和 VM 副本的 FSx ONTAP資料儲存。然後按一下“下一步”。



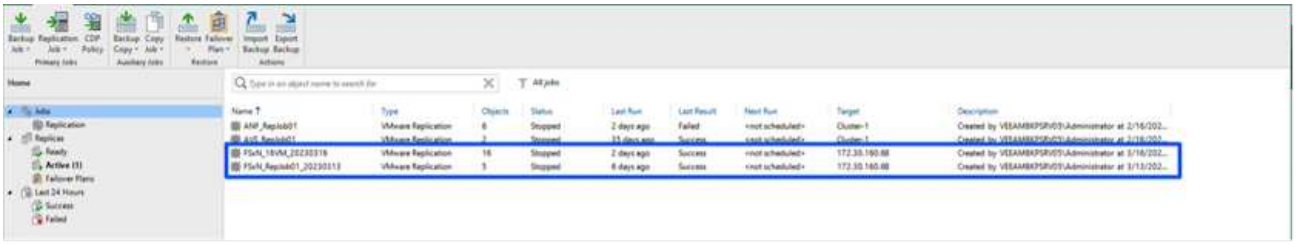
6. 下一步根據需要建立來源虛擬網路和目標虛擬網路之間的對應。



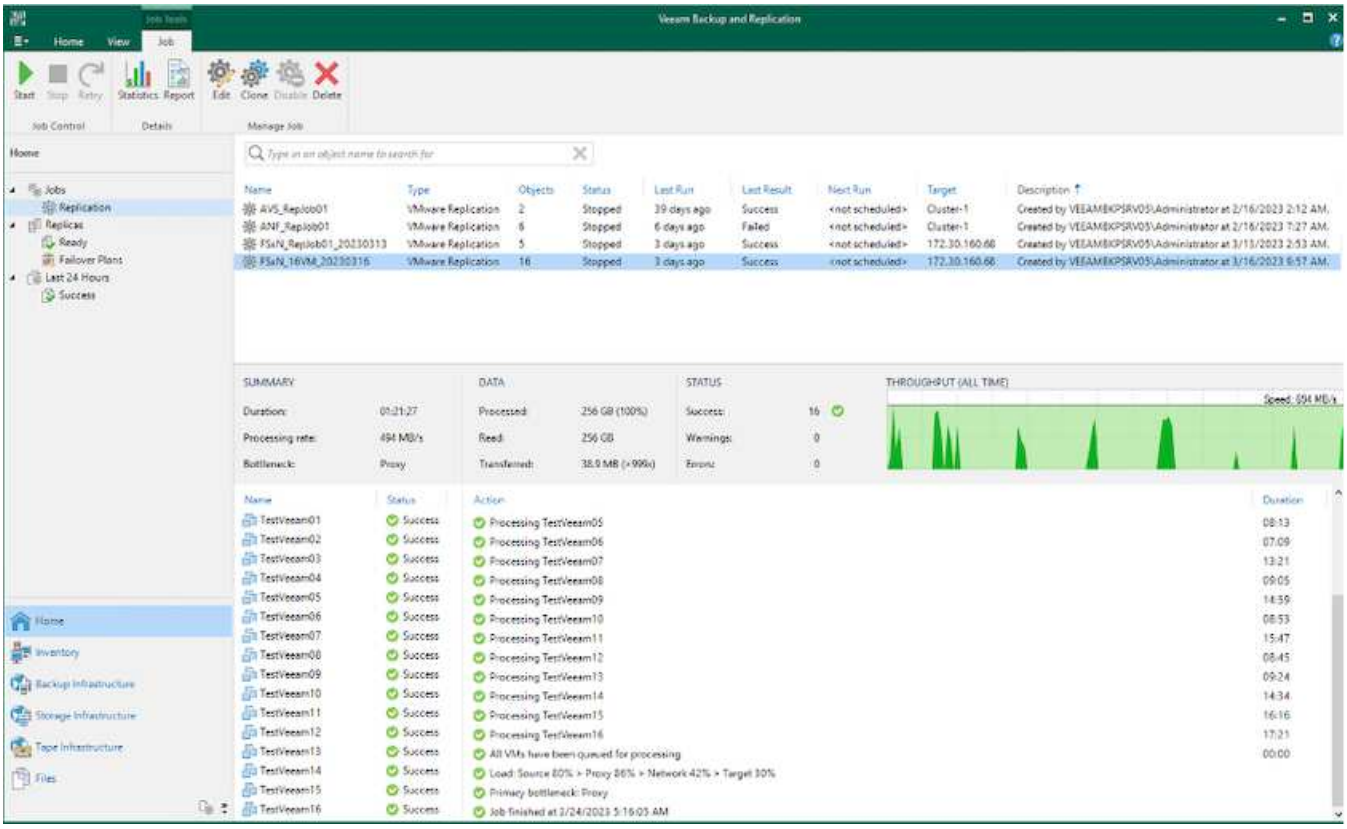
7. 在*作業設定*步驟中，指定將儲存 VM 副本、保留原則等元資料的備份儲存庫。
8. 在*資料傳輸*步驟中更新*來源*和*目標*代理伺服器，保留*自動*選擇（預設）並保持選擇*直接*選項，然後按一下*下一步*。
9. 在*Guest Processing*步驟中，依需求選擇*Enable application-aware processing*選項。按一下“下一步”。



10. 選擇複製計畫來定期執行複製作業。
11. 在精靈的*摘要*步驟中，查看複製作業的詳細資訊。若要在精靈關閉後立即啟動作業，請選取*按一下「完成」時執行作業*複選框，否則請不要選取該複選框。然後按一下「完成」關閉精靈。



複製作業啟動後，具有指定後綴的虛擬機器將填入目標 VMC SDDC 叢集/主機上。



有關 Veeam 複製的更多信息，請參閱"複製的工作原理"。

▼ 步驟 **2**：建立故障轉移計劃

初始複製或播種完成後，建立故障轉移計劃。故障轉移計畫有助於自動對從屬虛擬機器逐一或按群組執行故障轉移。故障轉移計劃是虛擬機器處理順序（包括啟動延遲）的藍圖。故障轉移計劃還有助於確保關鍵依賴的虛擬機器已經在運作。

若要建立計劃，請導覽至名為「副本」的新子部分並選擇「故障轉移計劃」。選擇適當的虛擬機器。 Veeam Backup & Replication 將尋找最接近此時間點的還原點並使用它們啟動 VM 副本。

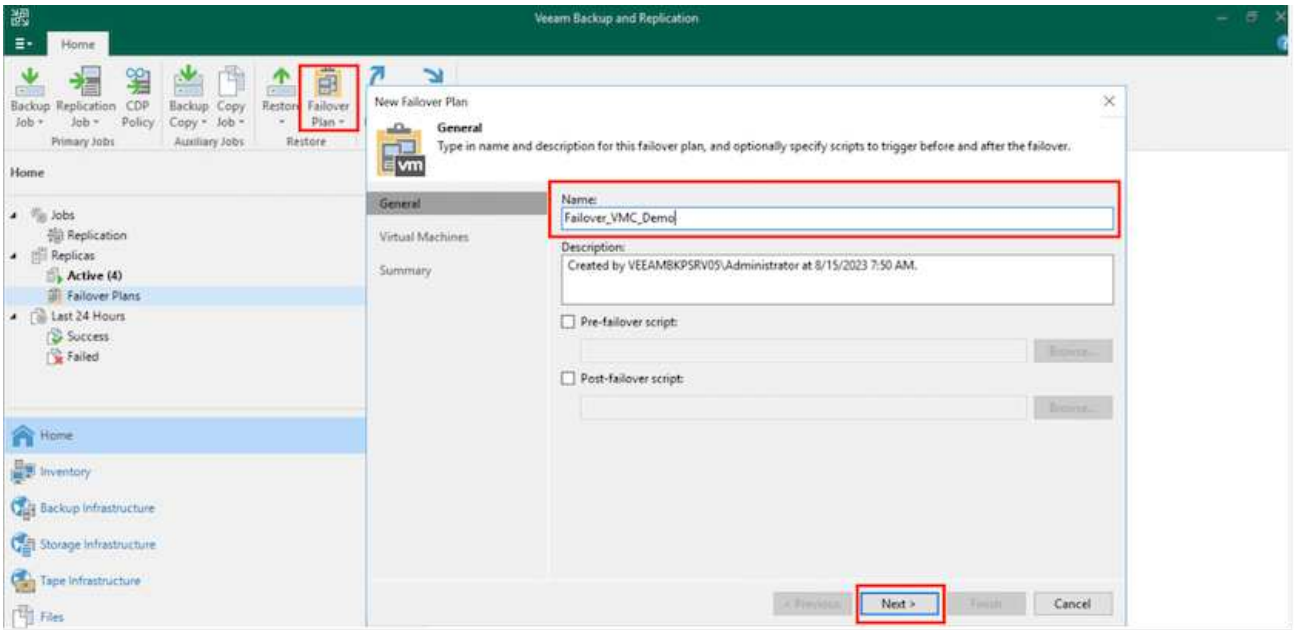
僅當初始複製完成且 VM 副本處於就緒狀態後，才能新增故障轉移計劃。

執行故障轉移計畫時可同時啟動的最大虛擬機器數量為 10 個。

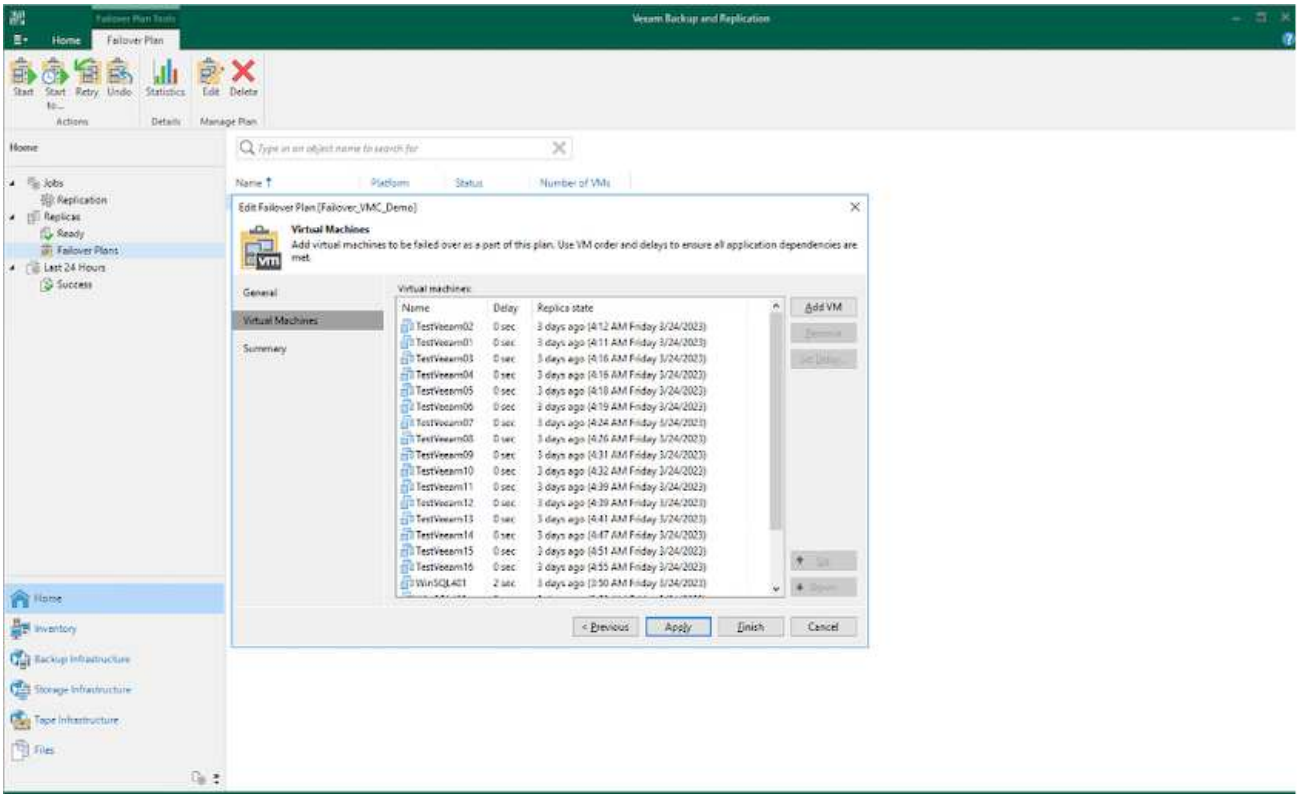
在故障轉移過程中，來源虛擬機器不會關閉。

若要建立*故障轉移計劃*，請執行下列操作：

1. 在主頁視圖上，選擇「故障轉移計畫」>「VMware vSphere」。
2. 接下來，為計劃提供名稱和描述。可根據需要新增故障轉移前和故障轉移後腳本。例如，在啟動複製的虛擬機器之前執行腳本來關閉虛擬機器。



3. 將虛擬機器新增至計畫中，並修改虛擬機器啟動順序和啟動延遲以滿足應用程式依賴關係。



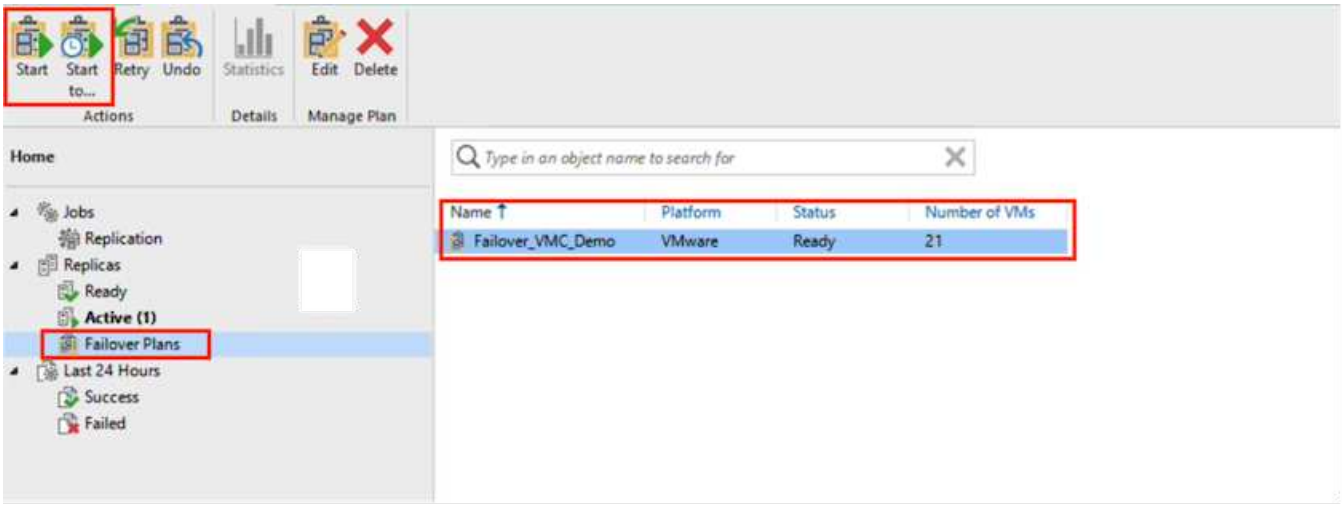
有關建立複製作業的其他信息，請參閱"建立複製作業"。

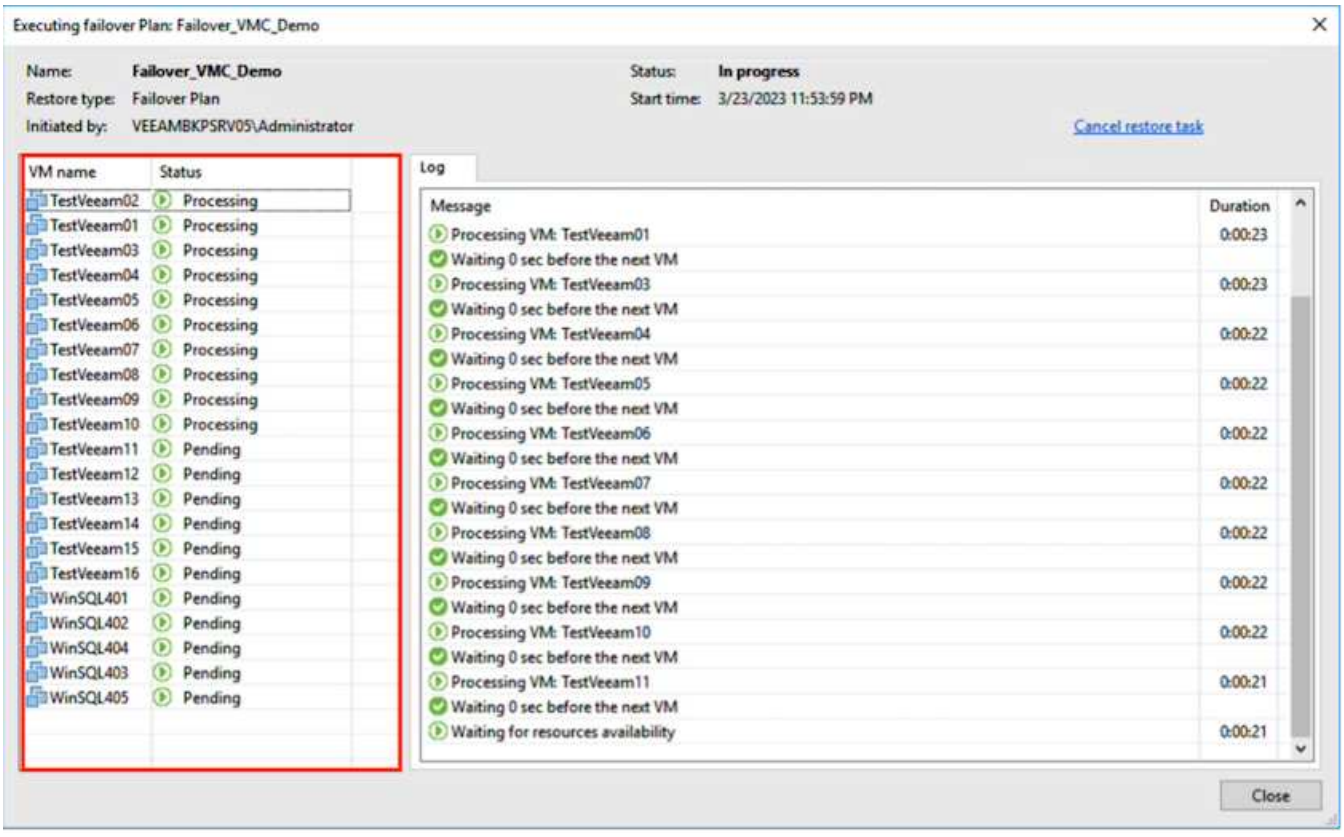
▼ 步驟 **3**：運行故障轉移計劃

在故障轉移期間，生產站點中的來源虛擬機器將切換到災難復原站點上的副本。作為故障轉移過程的一部分，Veeam Backup & Replication 將 VM 副本還原到所需的復原點，並將所有 I/O 活動從來源 VM 移至其副本。副本不僅可用於災難發生時，還可用於模擬災難復原演習。在故障轉移模擬期間，來源虛擬機器仍保持運作。一旦完成所有必要的測試，您就可以撤銷故障轉移並恢復正常操作。

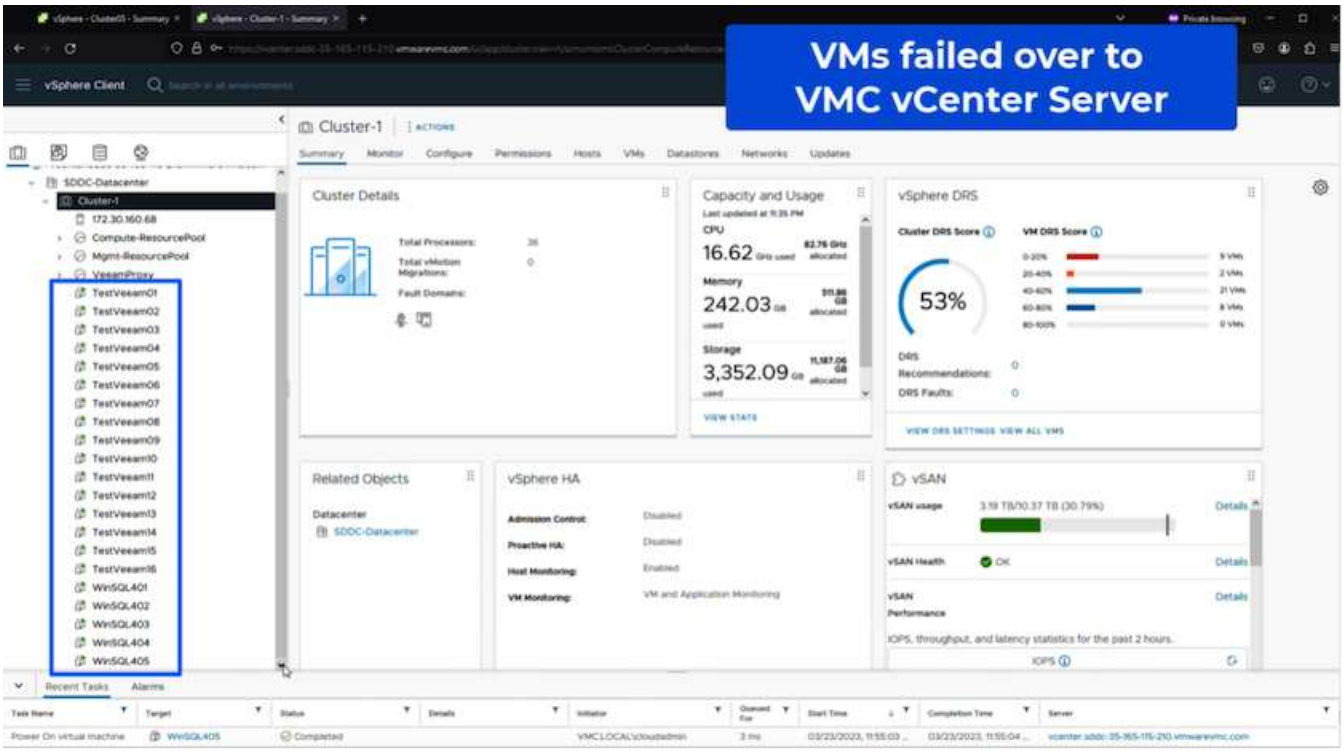
確保網路分段到位，以避免 DR 演習期間發生 IP 衝突。

要啟動故障轉移計劃，只需按一下「故障轉移計劃」選項卡，然後右鍵單擊故障轉移計劃。選擇“開始”。這將使用 VM 副本的最新還原點進行故障轉移。若要故障轉移到 VM 副本的特定還原點，請選擇*開始*。

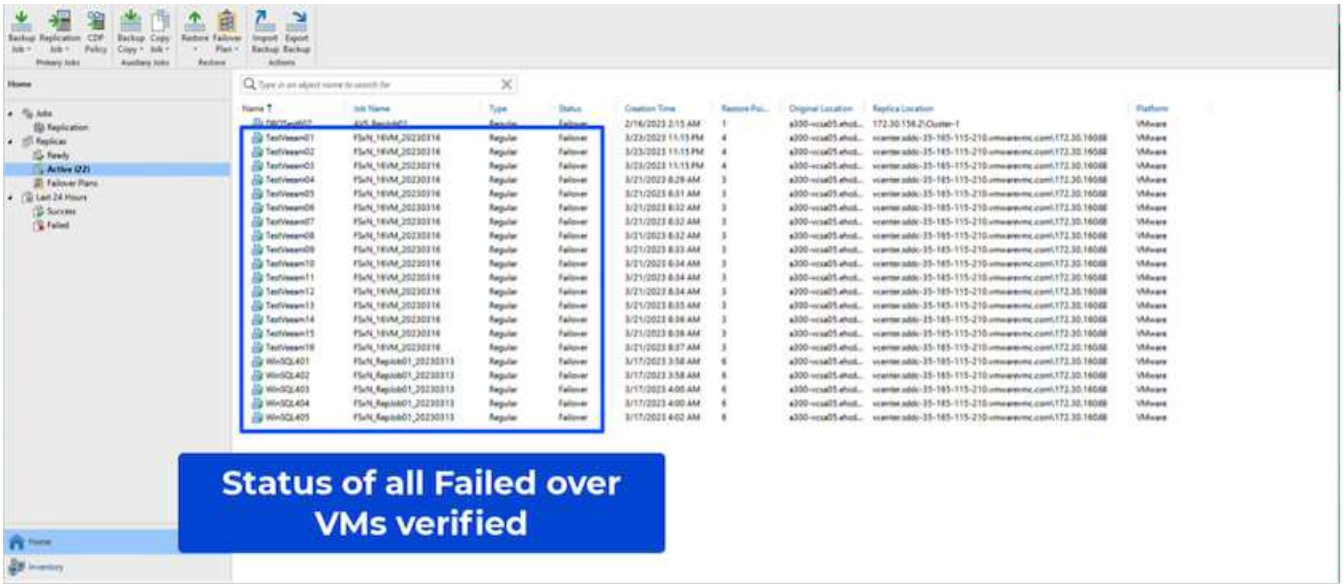




VM 副本的狀態從“就緒”變更為“故障轉移”，並且 VM 將在目標 VMware Cloud on AWS SDDC 叢集/主機上啟動。



故障轉移完成後，虛擬機器的狀態將變為「故障轉移」。



Veeam Backup & Replication 停止來源 VM 的所有複製活動，直到其副本返回就緒狀態。

有關故障轉移計劃的詳細信息，請參閱"故障轉移計劃"。

▼ 步驟 **4**：故障恢復到生產站點

當故障轉移計劃運行時，它被視為一個中間步驟，需要根據需求最終確定。選項包括以下內容：

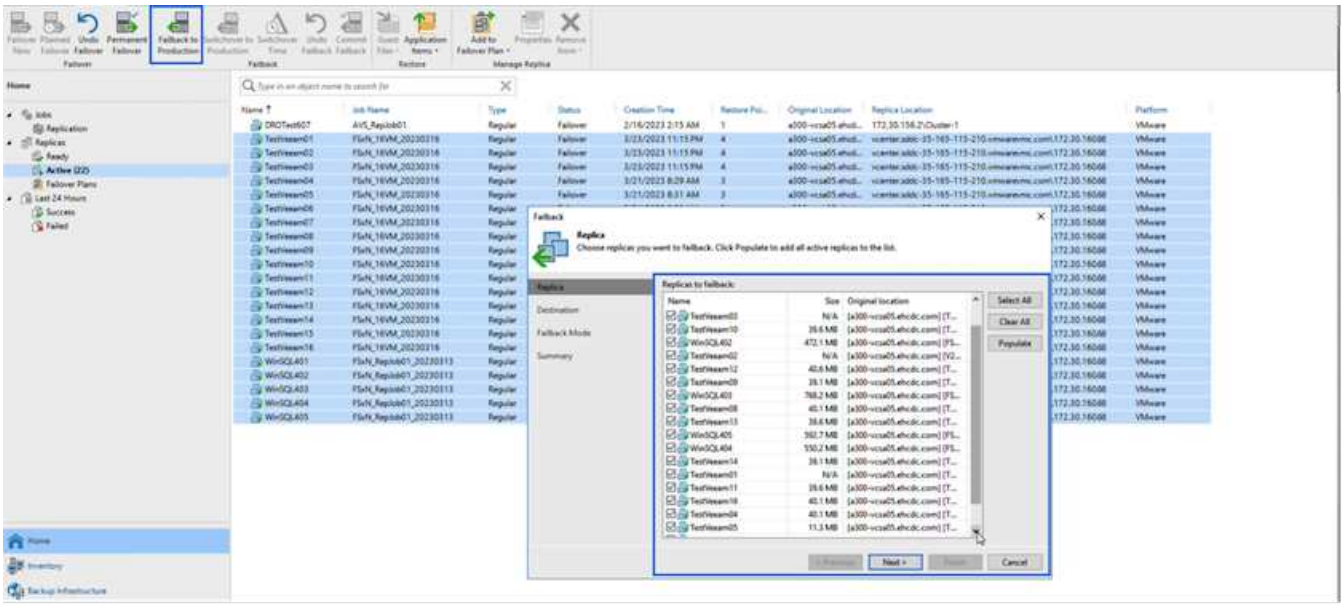
- 故障恢復到生產 - 切換回原始 VM，並將 VM 副本運行時發生的所有變更傳輸到原始 VM。

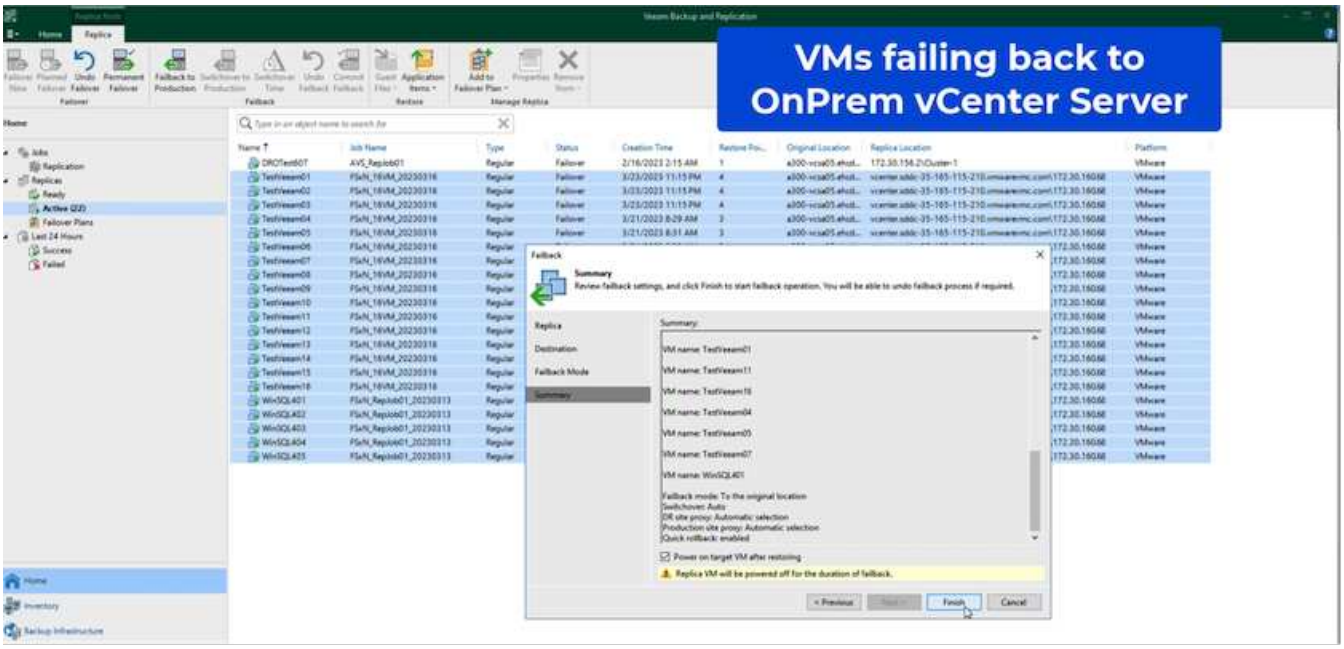
當您執行故障回應時，變更僅傳輸但不會被發布。如果原始 VM 未如預期運作，請選擇 提交故

障復原（一旦確認原始 VM 按預期運作）或 撤銷故障復原 以傳回 VM 副本。

- 撤銷故障轉移 - 切換回原始虛擬機器並放棄運行時對虛擬機器副本所做的所有變更。
- 永久故障轉移 - 從原始 VM 永久切換到 VM 副本，並使用此副本作為原始 VM。

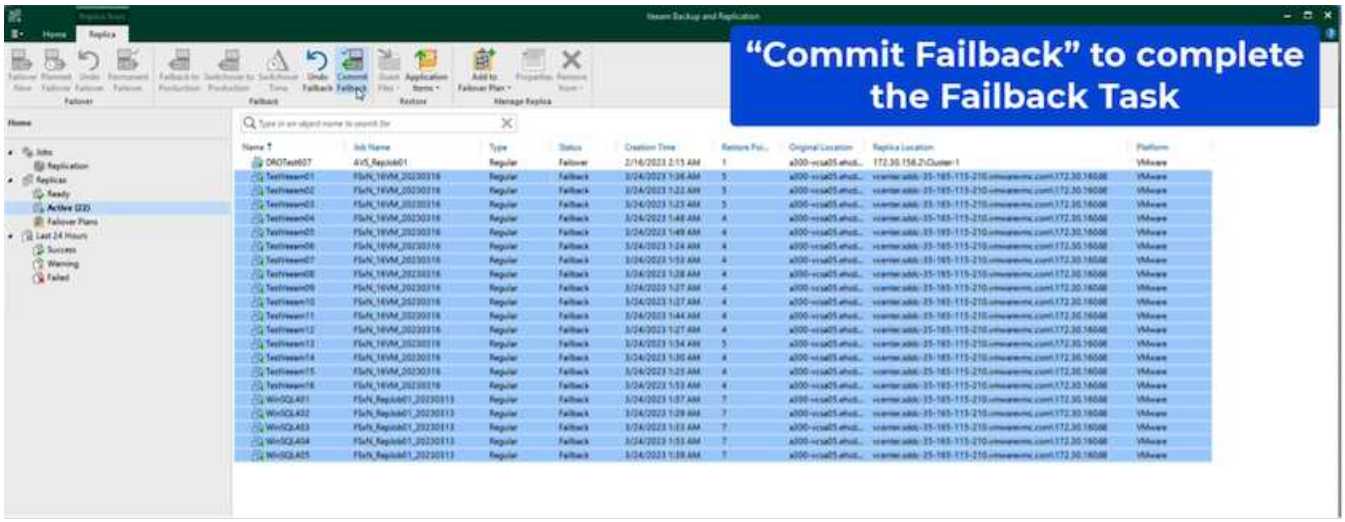
在這個演示中，選擇了故障恢復到生產。在精靈的目標步驟中選擇了故障回復到原始虛擬機，並且啟用了「恢復後啟動虛擬機」複選框。

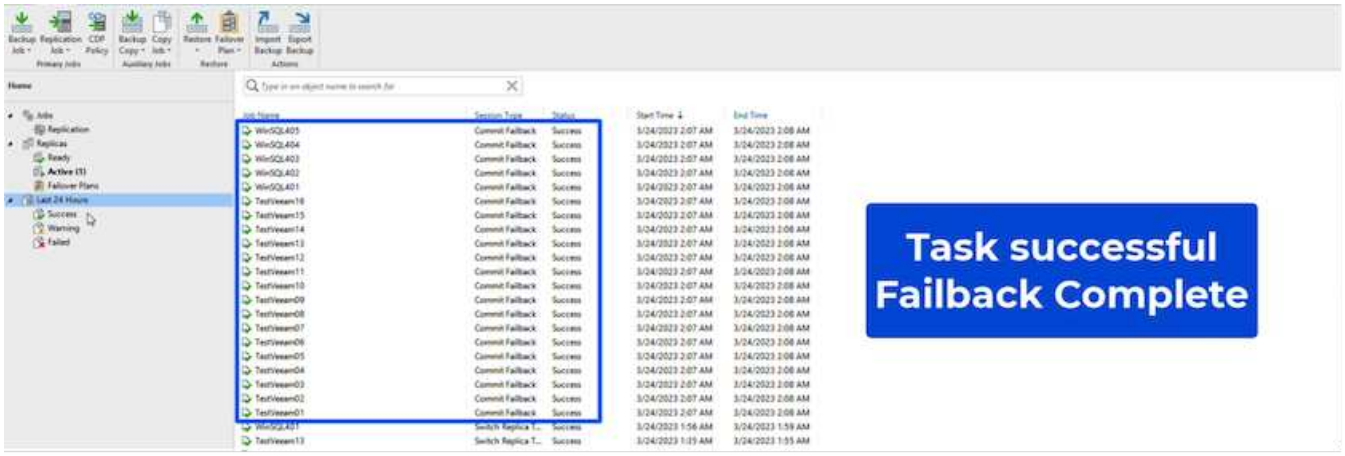




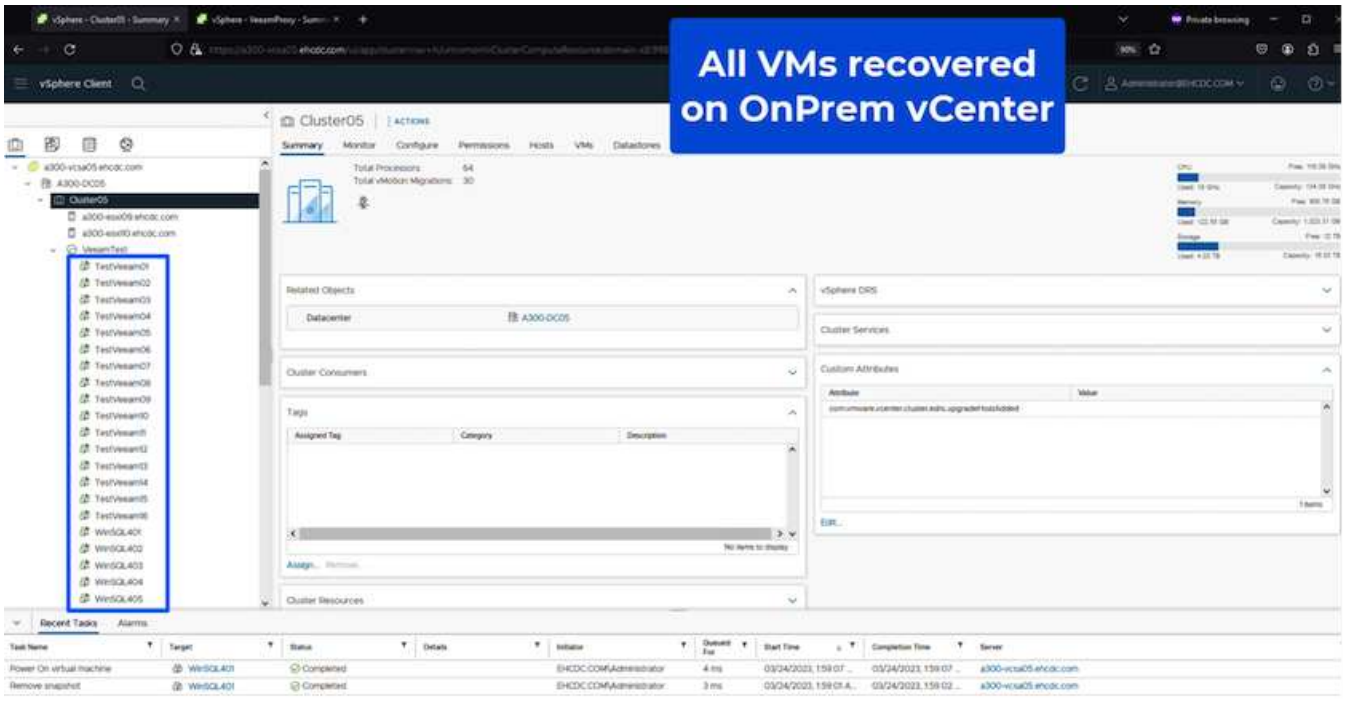
故障回復提交是完成故障回復操作的方法之一。當故障回復被提交時，它會確認發送到故障回復的虛擬機器（生產虛擬機器）的變更是否如預期般運作。提交操作後，Veeam Backup & Replication 將恢復生產虛擬機器的複製活動。

有關故障恢復過程的詳細信息，請參閱 Veeam 文檔"複製的故障轉移和故障恢復"。





故障復原生產成功後，所有虛擬機器都將恢復到原始生產站點。



結論

FSx ONTAP資料儲存功能可讓 Veeam 或任何經過驗證的第三方工具能夠使用 Pilot Light 叢集提供低成本的 DR 解決方案，而無需在叢集中建立大量主機以容納 VM 副本。這提供了一個強大的解決方案來處理量身定制的災難復原計劃，並且還允許重複使用內部現有的備份產品來滿足災難復原需求，從而透過退出內部災難復原資料中心實現基於雲端的災難復原。故障轉移可以按計劃進行，也可以在災難發生時點擊按鈕進行故障轉移，並決定啟動 DR 站點。

要了解有關此過程的更多信息，請隨意觀看詳細的演示視頻。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

在 **AWS/VMC** 上遷移工作負載

TR 4942：使用 **VMware HCX** 將工作負載遷移到 **FSx ONTAP**資料儲存區

Amazon Web Services (AWS) 上的 VMware Cloud (VMC) 及其在Amazon FSx ONTAP上的補充 NFS 資料儲存的常見用例是遷移 VMware 工作負載。 VMware HCX 是一種首選方案，它提供了各種遷移方法，將在任何 VMware 支援的資料儲存上運行的本機虛擬機 (VM) 及其資料移至 VMC 資料存儲，其中包括 FSx ONTAP上的補充 NFS 資料儲存。

概述：使用 **VMware HCX**、**FSx ONTAP**補充資料儲存區和 **VMware Cloud** 遷移虛擬機

VMware HCX 主要是一個行動平台，旨在簡化跨雲端的工作負載遷移、工作負載重新平衡和業務連續性。它是 AWS 上 VMware Cloud 的一部分，提供多種遷移工作負載的方法，並可用於災難復原 (DR) 操作。

本文檔提供了在本機和雲端資料中心端部署和配置 VMware HCX（包括其所有主要元件）的逐步指導，從而實現各種 VM 遷移機制。

有關詳細信息，請參閱 "VMware HCX 使用者指南"和 "安裝清單 B - 使用 VMware Cloud on AWS SDDC 目標環境的 HCX"。

▼ 摘要步驟

此清單提供了安裝和設定 VMware HCX 的進階步驟：

1. 透過 VMware Cloud Services Console 為 VMC 軟體定義資料中心 (SDDC) 啟動 HCX。
2. 在本機 vCenter Server 中下載並部署 HCX Connector OVA 安裝程式。
3. 使用許可證金鑰啟動 HCX。
4. 將本機 VMware HCX Connector 與 VMC HCX Cloud Manager 配對。
5. 設定網路設定檔、計算設定檔和服務網格。
6. （可選）執行網路擴展以擴展網路並避免重新 IP。
7. 驗證設備狀態並確保可以遷移。
8. 遷移虛擬機器工作負載。

▼ 先決條件

在開始之前，請確保滿足以下先決條件。有關更多信息，請參閱 "準備安裝" 。在滿足先決條件（包括連接性）後，透過從 VMC 的 VMware HCX 控制台產生許可證金鑰來設定和啟動 HCX。 HCX 啟動後，vCenter 外掛程式即部署，可透過 vCenter 控制台存取管理。

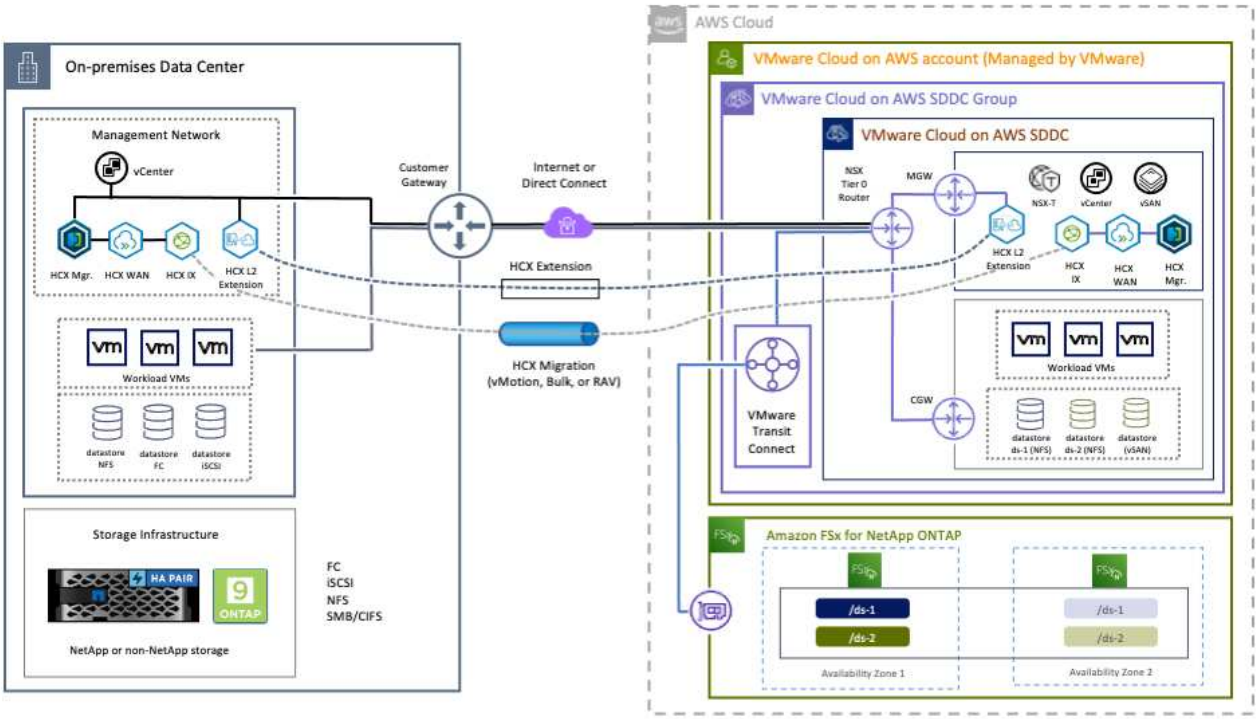
在繼續 HCX 啟動和部署之前，必須完成以下安裝步驟：

1. 使用現有的 VMC SDDC 或按照此步驟建立新的 SDDC"NetApp連結"或者這個 "VMware 連結"。
2. 從本機 vCenter 環境到 VMC SDDC 的網路路徑必須支援使用 vMotion 遷移虛擬機器。
3. 確保所需的 "防火牆規則和連接埠"允許在本機 vCenter Server 和 SDDC vCenter 之間進行 vMotion 流量。
4. FSx ONTAP NFS 磁碟區應作為補充資料儲存安裝在 VMC SDDC 中。若要將 NFS 資料儲存附加到適當的集群，請按照此處概述的步驟操作"NetApp連結"或者這個 "VMware 連結"。

▼ 進階架構

為了測試目的，用於此驗證的本機實驗室環境透過站點到站點 VPN 連接到 AWS VPC，從而允許透過外部傳輸網關在本地連接到 AWS 和 VMware 雲端 SDDC。 HCX 遷移和網路擴充流量透過網際網路在本地和 VMware 雲端目標 SDDC 之間流動。可以修改此架構以使用 Direct Connect 私有虛擬介面。

下圖描述了高階架構。



解決方案部署

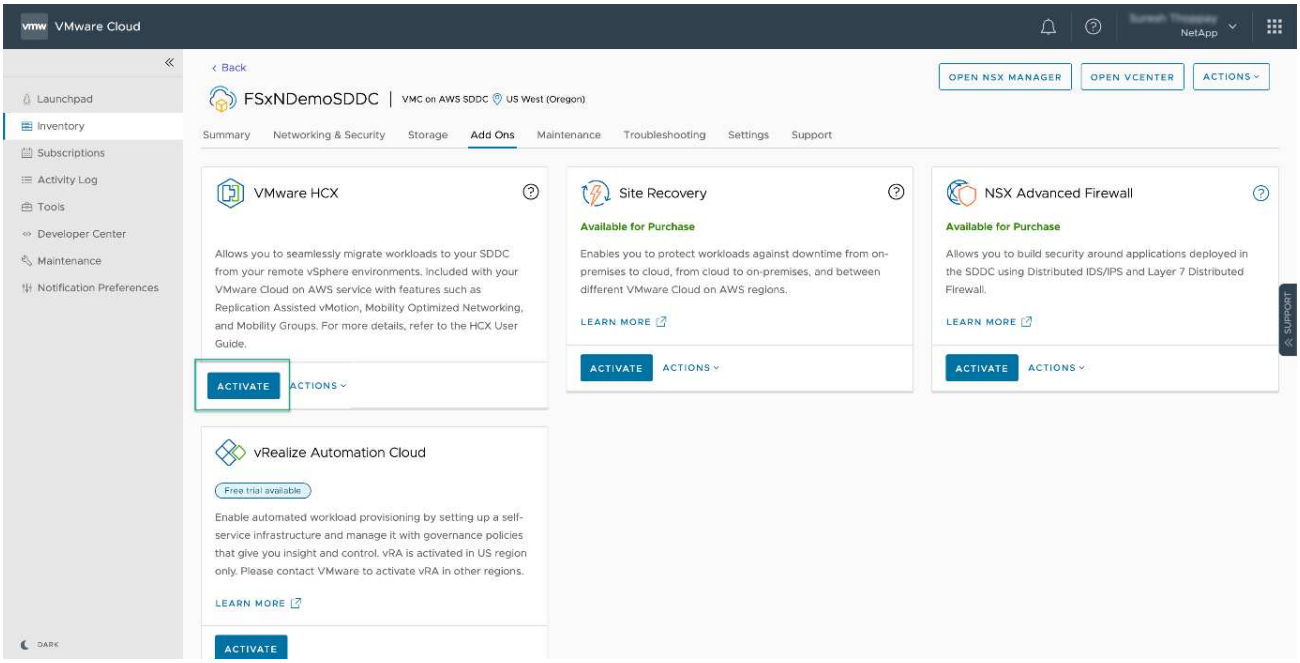
請按照一系列步驟完成此解決方案的部署：

▼ 步驟 **1**：使用附加組件選項透過 **VMC SDDC** 啟動 **HCX**

若要執行安裝，請完成以下步驟：

1. 登入 VMC 控制台 "vmc.vmware.com"並訪問庫存。
2. 若要選擇適當的 SDDC 並存取附加元件，請按一下 SDDC 上的「檢視詳細資料」並選擇「附加元件」標籤。
3. 按一下「啟動 VMware HCX」。

此步驟最多需要 25 分鐘才能完成。

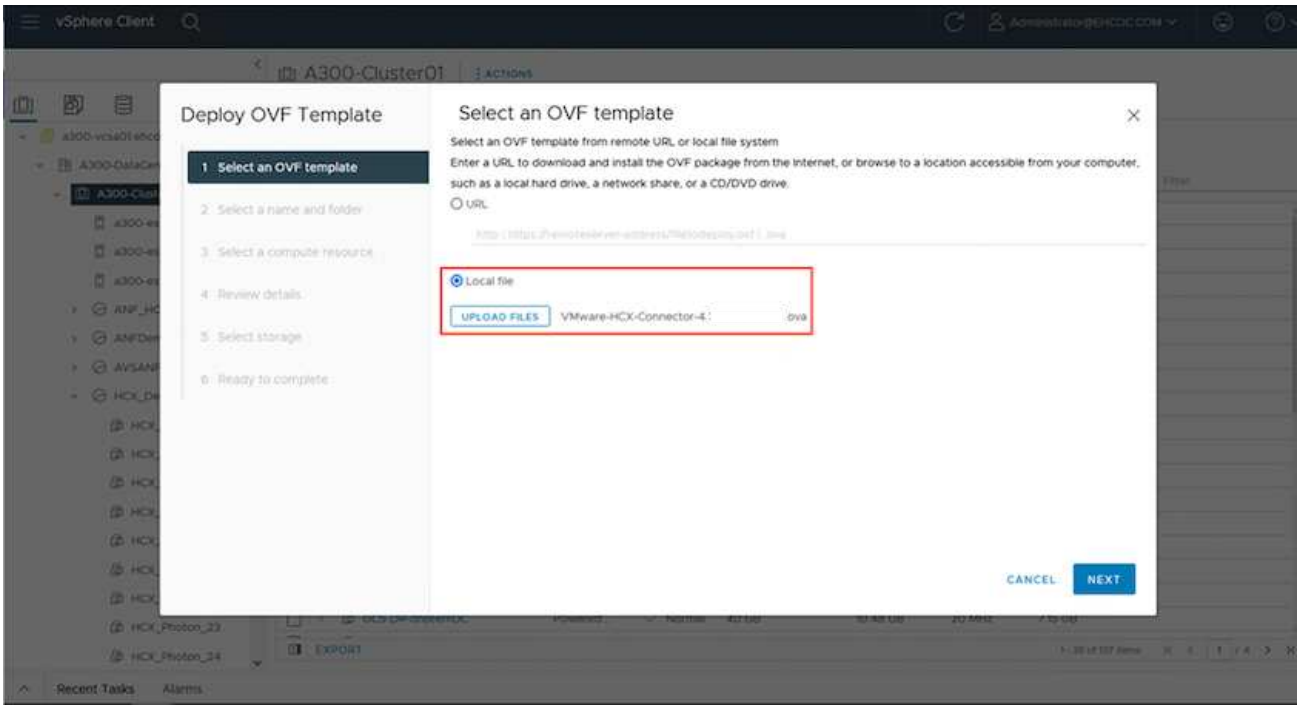


4. 部署完成後，透過確認 HCX Manager 及其相關外掛程式在 vCenter 控制台中可用於驗證部署。
5. 建立適當的管理網關防火牆以開啟存取 HCX 雲端管理器所需的連接埠。 HCX 雲端管理器現在已準備好進行 HCX 作業。

▼ 步驟 **2**：在本機 **vCenter Server** 中部署安裝程式 **OVA**

為了使本地連接器能夠與 VMC 中的 HCX 管理器通信，請確保在本地環境中開啟了相應的防火牆連接埠。

1. 從 VMC 控制台導覽至 HCX 儀表板，前往管理，然後選擇系統更新標籤。按一下「請求下載連結」以取得 HCX 連接器 OVA 映像。
2. 下載 HCX 連接器後，在本機 vCenter Server 中部署 OVA。右鍵點選 vSphere 叢集並選擇部署 OVF 範本選項。

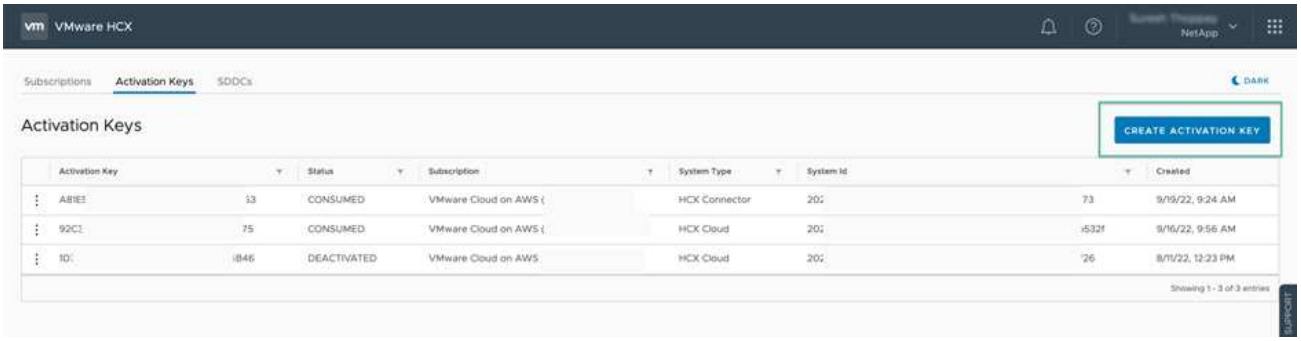


3. 在部署 OVF 範本精靈中輸入所需信息，按一下下一步，然後按一下完成以部署 VMware HCX 連接器 OVA。
4. 手動啟動虛擬設備。有關逐步說明，請轉至 "VMware HCX 使用者指南"。

▼ 步驟 **3**：使用許可證金鑰啟動 **HCX Connector**

在本機部署 VMware HCX Connector OVA 並啟動裝置後，請完成以下步驟以啟動 HCX Connector。從 VMC 的 VMware HCX 控制台產生許可證金鑰，並在 VMware HCX 連接器設定期間輸入許可證。

1. 從 VMware Cloud Console 中，前往“清單”，選擇 SDDC，然後按一下“查看詳細資料”。在「附加元件」標籤的 VMware HCX 磁貼中，按一下「開啟 HCX」。
2. 在「啟動金鑰」標籤中，按一下「建立啟動金鑰」。選擇系統類型為HCX連接器，然後按一下確認以產生金鑰。複製啟動密鑰。



每個在本地部署的 HCX 連接器都需要單獨的金鑰。

3. 登入本機 VMware HCX 連接器，網址為 `"https://hcxconnectorIP:9443"`使用管理員憑證。

使用 OVA 部署期間定義的密碼。

4. 在許可部分，輸入從步驟 2 複製的啟動金鑰，然後按一下啟動。

   本機 HCX 連接器必須具有 Internet 存取權限才能成功完成啟動。

5. 在資料中心位置下，提供在本機安裝 VMware HCX 管理器所需的位置。按一下「Continue（繼續）」。
6. 在系統名稱下，更新名稱並按一下繼續。
7. 選擇“是”，然後“繼續”。
8. 在「連接您的 vCenter」下，提供 vCenter Server 的 IP 位址或完全限定網域名稱 (FQDN) 和憑證，然後按一下「繼續」。

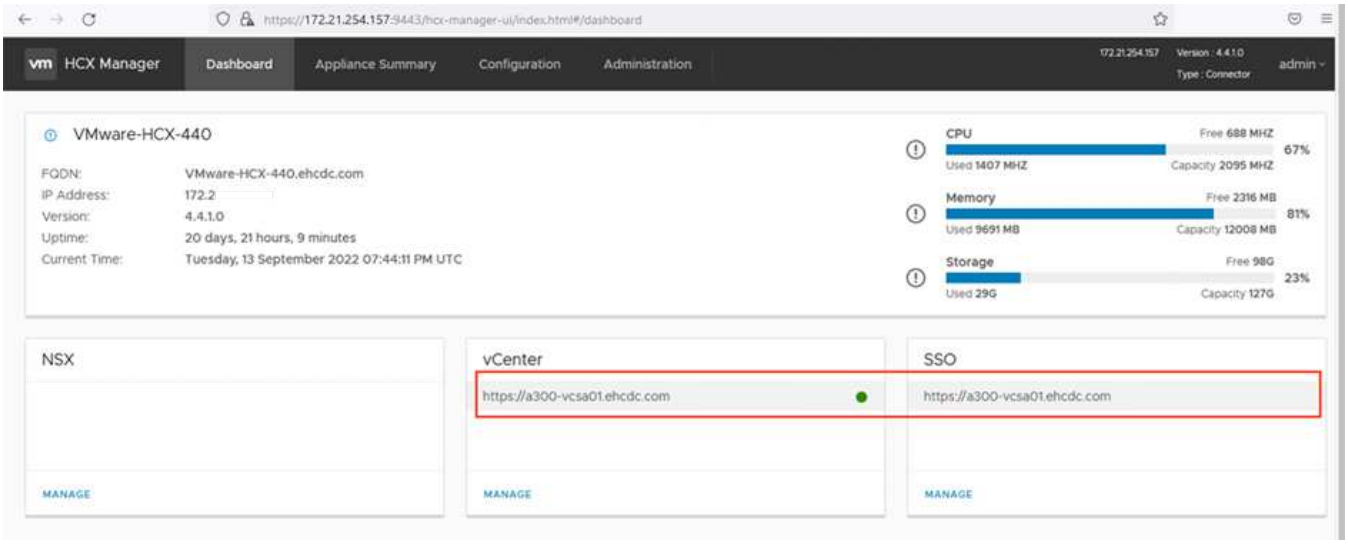
   使用 FQDN 以避免日後出現通訊問題。

9. 在設定 SSO/PSC 下，提供平台服務控制器的 FQDN 或 IP 位址，然後按一下繼續。

   輸入 vCenter Server 的 IP 位址或 FQDN。

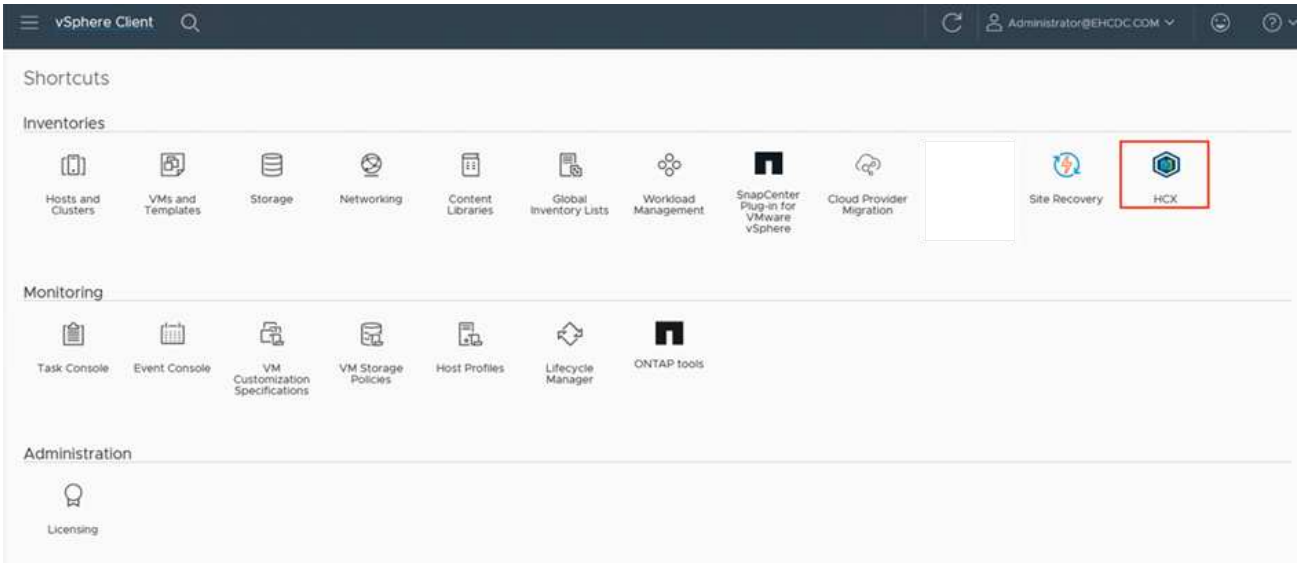
10. 驗證資訊輸入是否正確，然後按一下「重新啟動」。
11. 完成後，vCenter Server 顯示為綠色。 vCenter Server 和 SSO 都必須具有正確的設定參數，這些參數應與上一頁相同。

    此過程大約需要 10 到 20 分鐘，以便將插件新增至 vCenter Server。

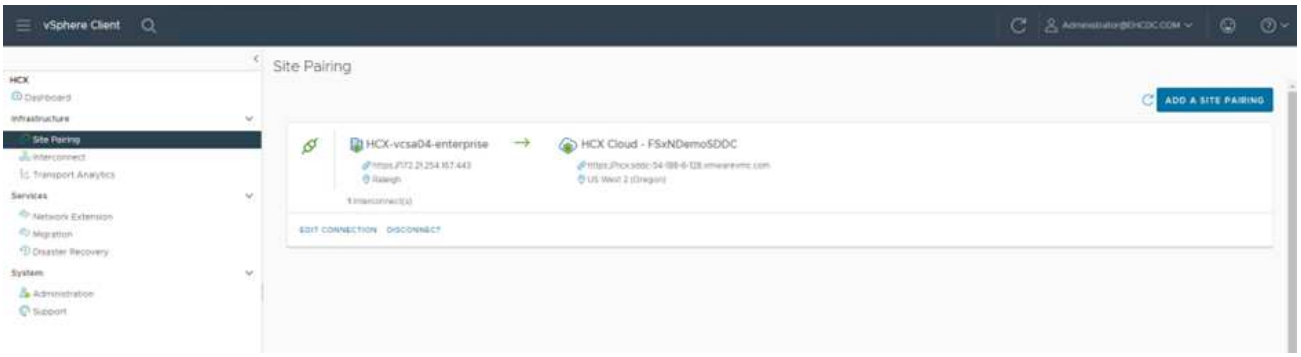


▼ 步驟 **4**：將本機 **VMware HCX Connector** 與 **VMC HCX Cloud Manager** 配對

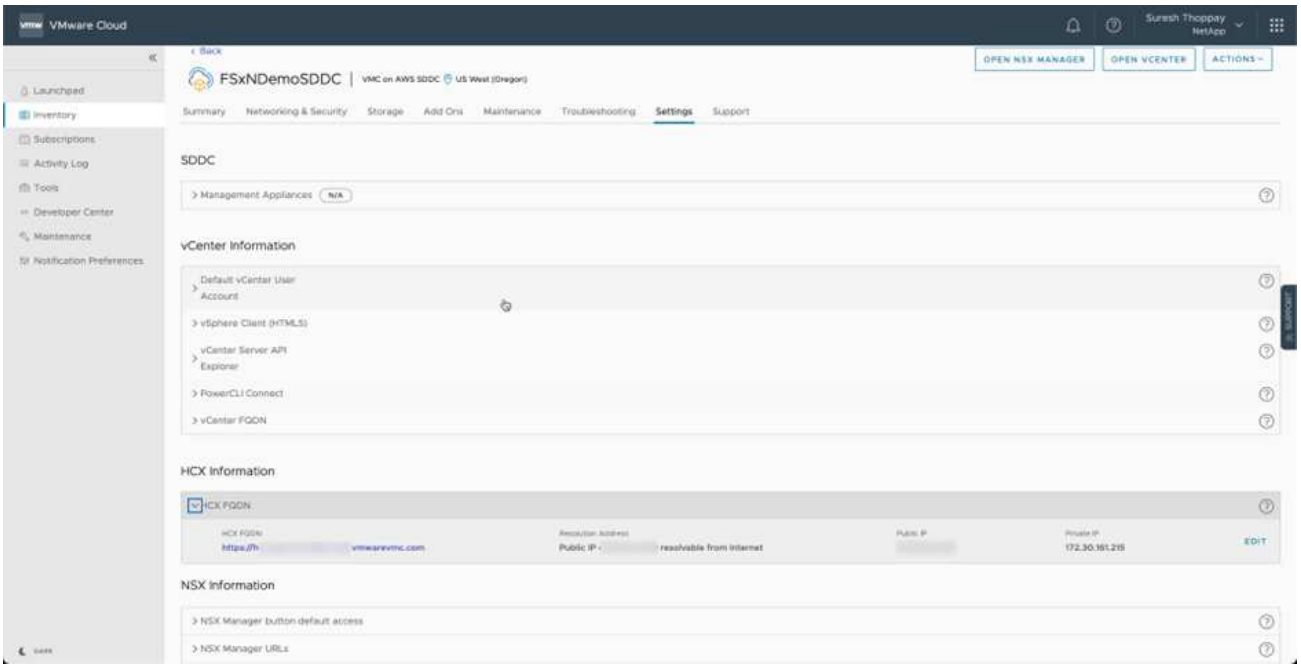
1. 若要在本機 vCenter Server 和 VMC SDDC 之間建立網站對，請登入本機 vCenter Server 並造訪 HCX vSphere Web Client 外掛程式。

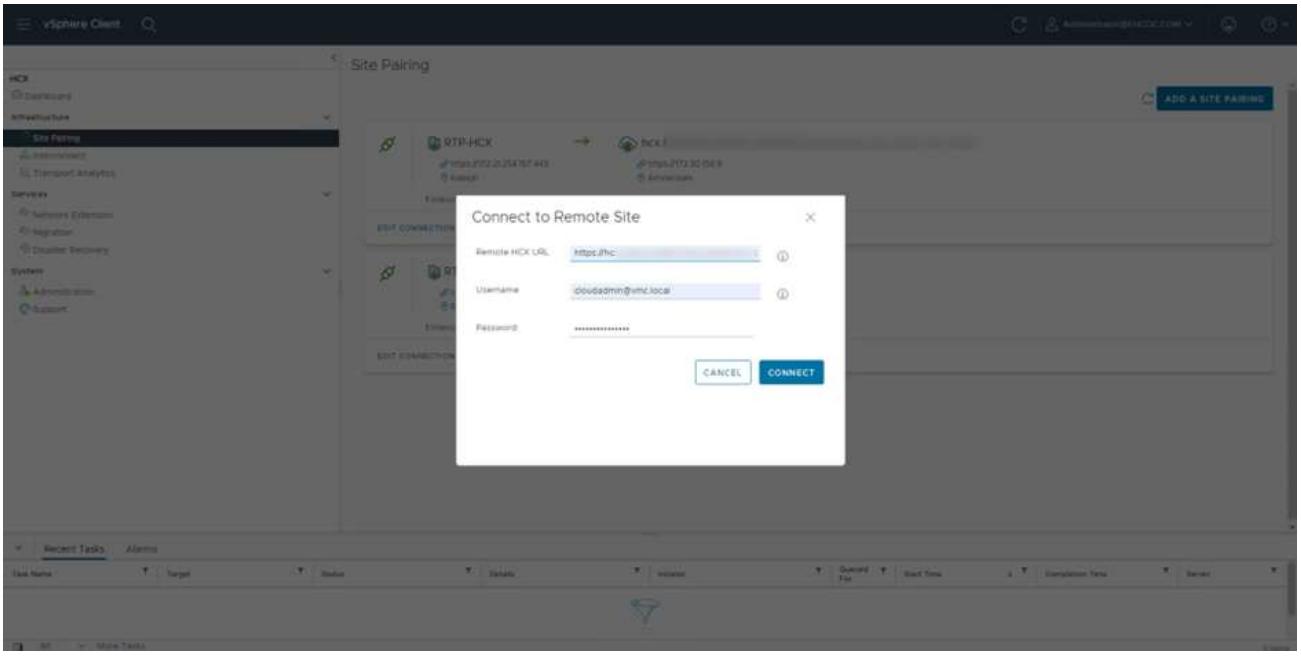


2. 在基礎架構下，按一下新增網站配對。若要對遠端網站進行驗證，請輸入 VMC HCX Cloud Manager URL 或 IP 位址以及 CloudAdmin 角色的憑證。



可以從 SDDC 設定頁面檢索 HCX 資訊。





3. 若要啟動網站配對，請按一下「連線」。

   VMware HCX Connector 必須能夠透過連接埠 443 與 HCX Cloud Manager IP 通訊。

4. 建立配對後，新配置的網站配對可在 HCX 儀表板上取得。

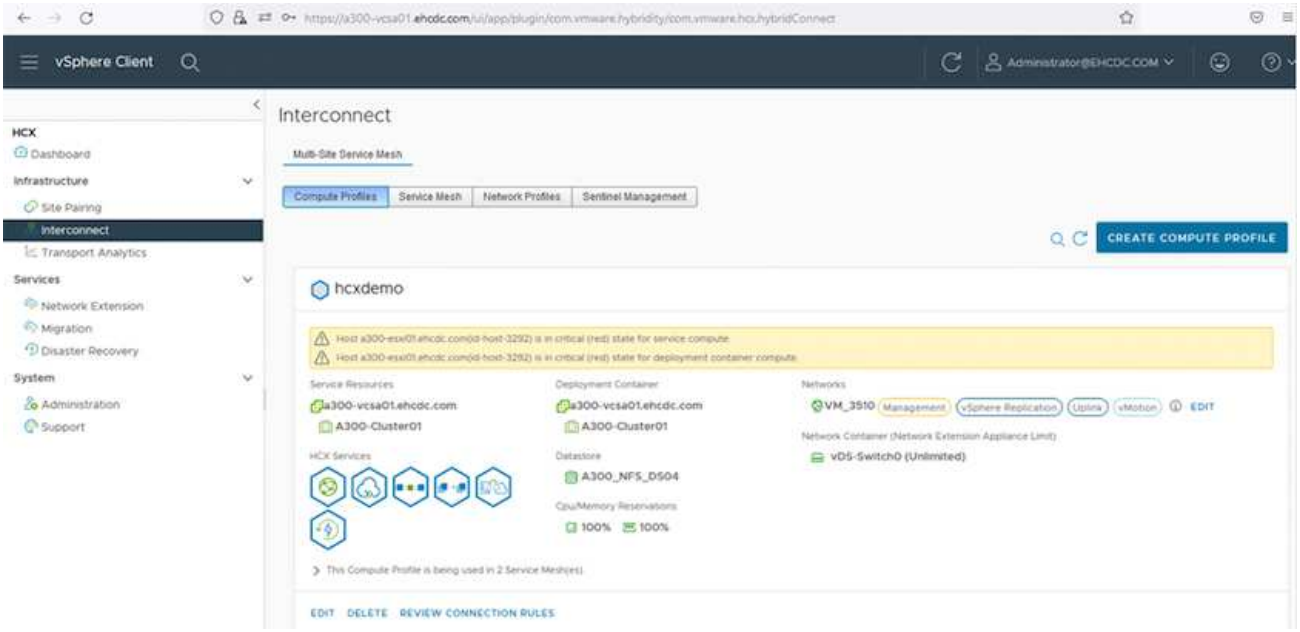
▼ 步驟 **5**：設定網路設定檔、計算設定檔和服務網格

VMware HCX Interconnect (HCX-IX) 裝置透過網際網路提供安全隧道功能以及與目標網站的專用連接，從而實現複製和基於 vMotion 的功能。互連提供加密、流量工程和 SD-WAN。若要建立 HCI-IX 互連設備，請完成下列步驟：

1. 在「基礎架構」下，選擇「互連」>「多站點服務網格」>「計算設定檔」>「建立計算設定檔」。

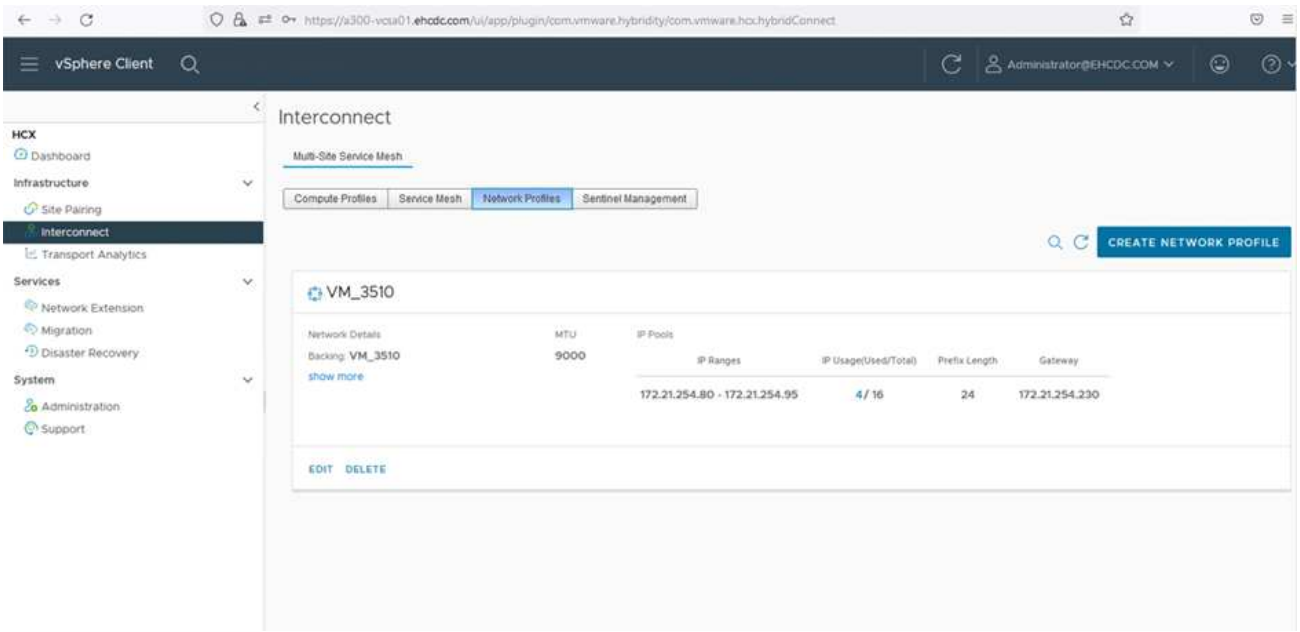
   計算設定檔包含部署互連虛擬設備所需的運算、儲存和網路部署參數。他們還指定 VMware 資料中心的哪些部分可供 HCX 服務存取。

有關詳細說明，請參閱 "建立計算配置檔案"。



2. 建立計算設定檔後，透過選擇多站點服務網格 > 網路設定檔 > 建立網路設定檔來建立網路設定檔。
3. 網路設定檔定義了 HCX 將用於其虛擬設備的一系列 IP 位址和網路。

   這將需要兩個或更多 IP 位址。這些 IP 位址將從管理網路指派給虛擬設備。

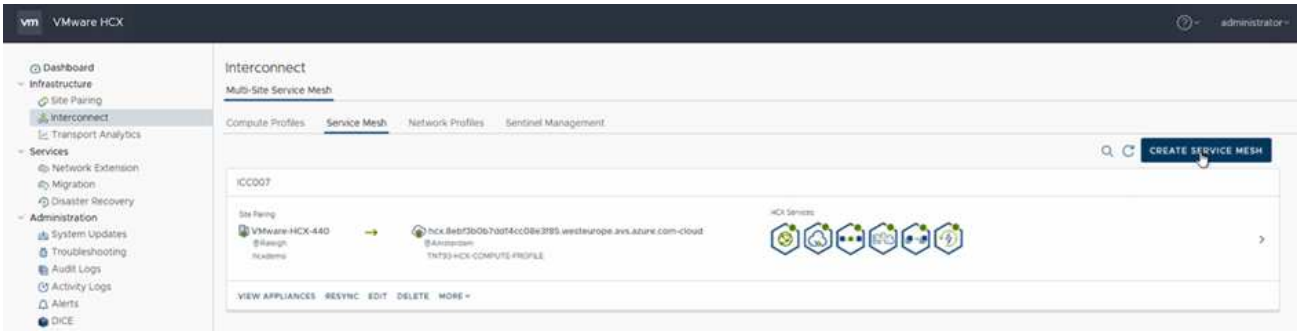


有關詳細說明，請參閱 "建立網路設定檔"。

如果您透過網際網路連接 SD-WAN，則必須在「網路和安全性」部分下保留公共 IP。

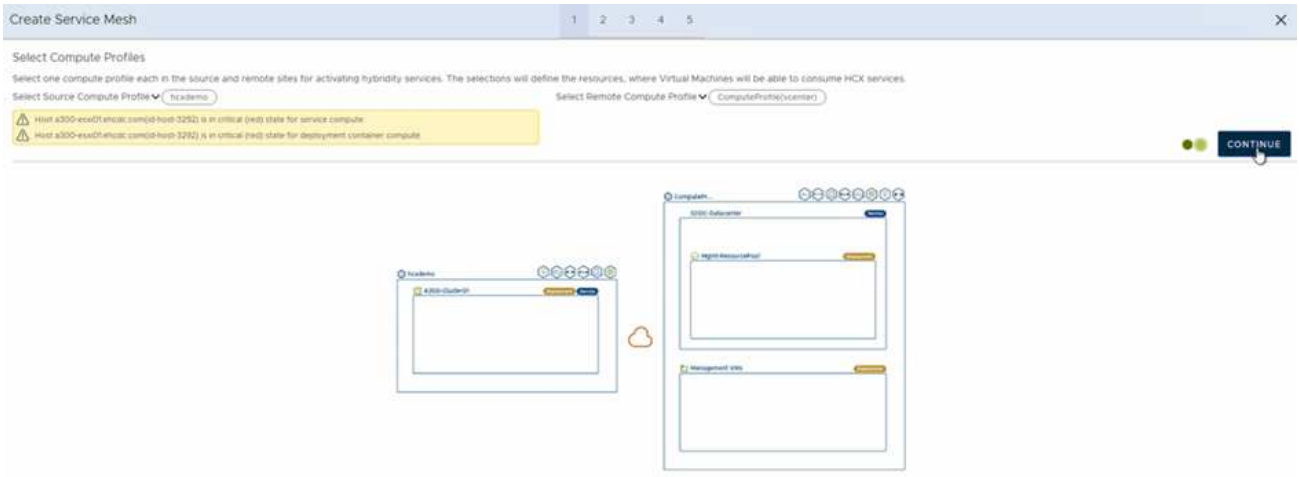
4. 若要建立服務網格，請選擇「互連」選項中的「服務網格」標籤，然後選擇本機和 VMC SDDC 網站。

   服務網格建立本地和遠端計算和網路設定檔對。

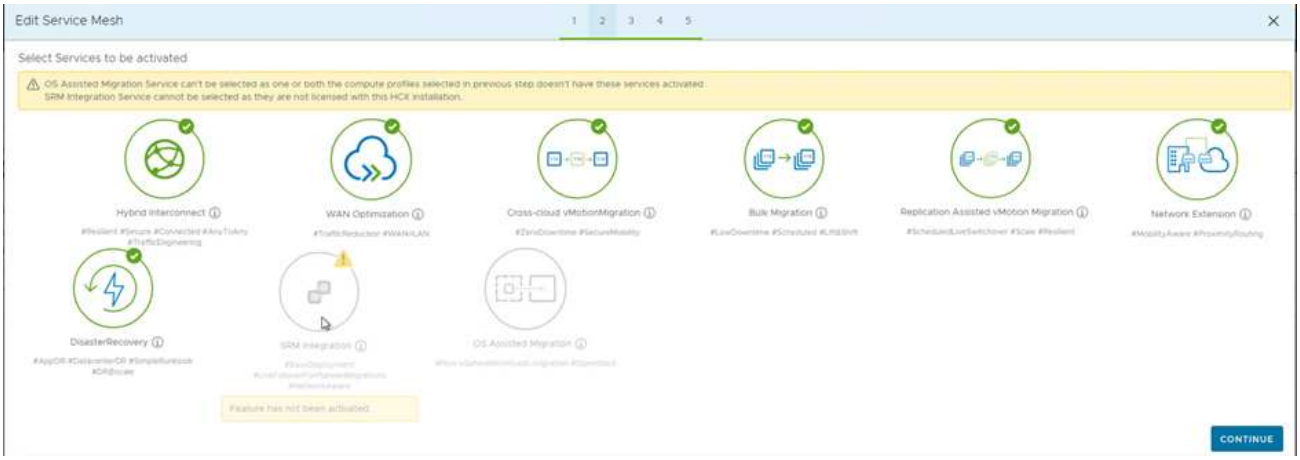


此過程的一部分涉及部署將在來源站點和目標站點上自動配置的 HCX 設備，從而建立安全的傳輸結構。

5. 選擇來源和遠端計算配置文件，然後按一下繼續。

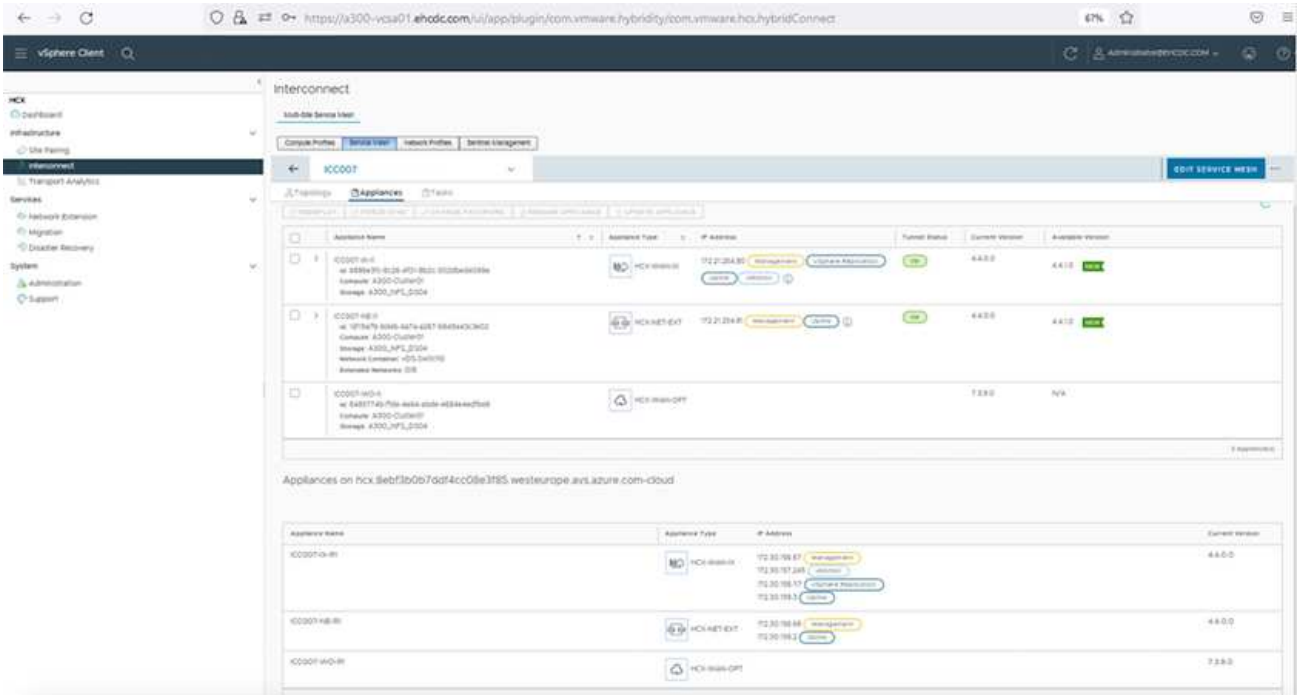


6. 選擇需要啟動的服務並點擊繼續。



複製輔助 vMotion 遷移、SRM 整合和 OS 輔助遷移需要 HCX Enterprise 授權。

7. 為服務網格建立名稱，然後按一下「完成」開始建立程序。部署大約需要 30 分鐘才能完成。配置服務網格後，遷移工作負載虛擬機器所需的虛擬基礎架構和網路已建立。



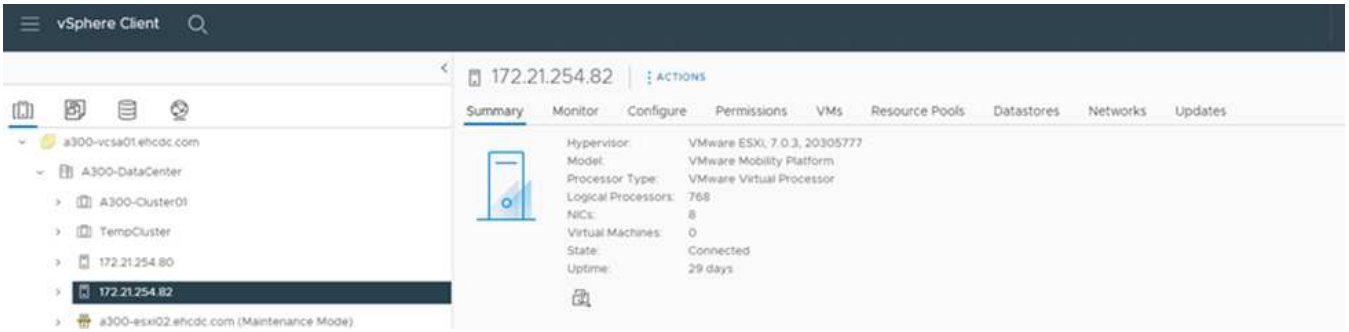
▼ 步驟 **6**：遷移工作負載

HCX 在兩個或多個不同的環境（例如本地和 VMC SDDC）之間提供雙向遷移服務。可以使用各種遷移技術將應用程式工作負載遷移到 HCX 激活站點和從 HCX 激活站點遷移，例如 HCX 批量遷移、HCX vMotion 、HCX 冷遷移、HCX 複製輔助 vMotion（HCX 企業版提供）和 HCX OS 輔助遷移（HCX 企業版提供）。

要了解有關可用的 HCX 遷移技術的更多信息，請參閱 "VMware HCX 遷移類型"

HCX-IX 設備使用行動代理服務執行 vMotion、Cold 和複製輔助 vMotion (RAV) 遷移。

HCX-IX 設備將行動代理服務新增為 vCenter Server 中的主機物件。此物件上顯示的處理器、記憶體、儲存和網路資源並不代表託管 IX 裝置的實體虛擬機器管理程式上的實際消耗。



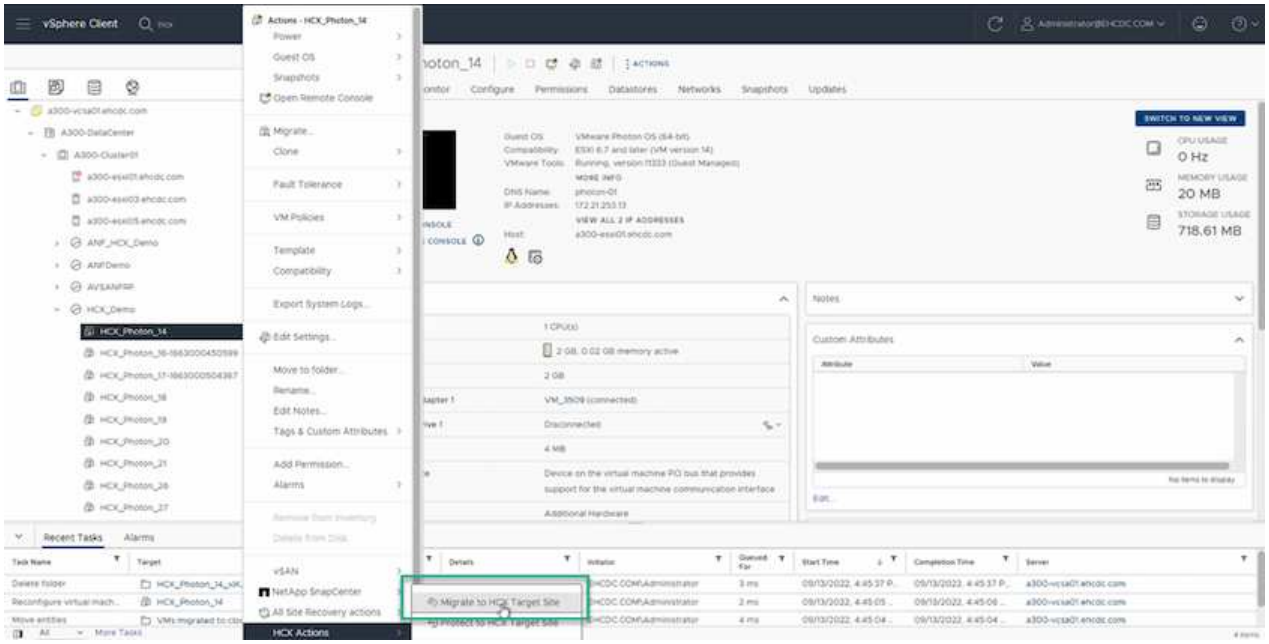
▼ **VMware HCX vMotion**

本節介紹 HCX vMotion 機制。此遷移技術使用 VMware vMotion 協定將虛擬機器遷移到 VMC SDDC。vMotion 遷移選項用於一次遷移單一 VM 的 VM 狀態。此遷移方法期間不會中斷服務。

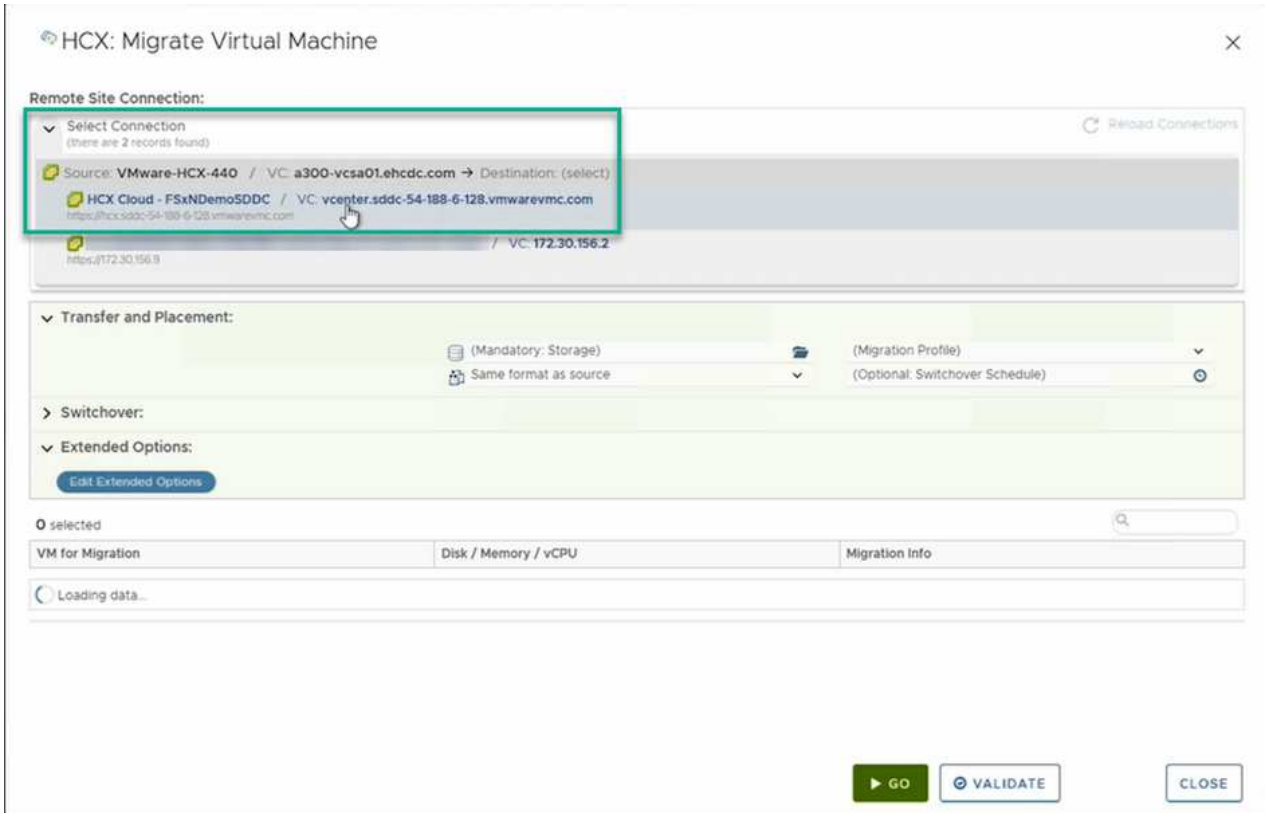
應該實施網路擴充（針對虛擬機器所連接的連接埠群組），以便遷移虛擬機器而無需更改 IP 位址。

1. 從本機 vSphere 用戶端，前往“清單”，右鍵點選要遷移的虛擬機，然後選擇“HCX 動作”>“遷移到 HCX

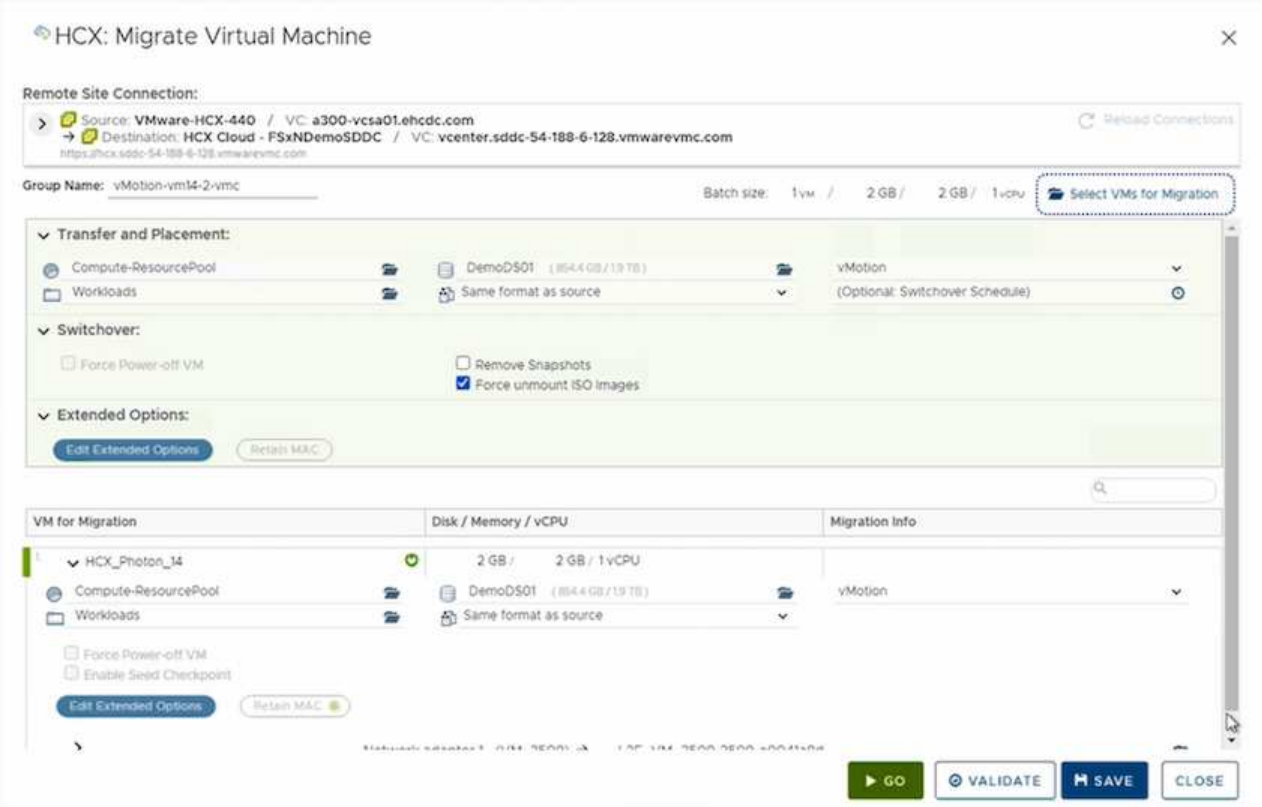
目標網站”。



2. 在遷移虛擬機器精靈中，選擇遠端站點連線（目標 VMC SDDC）。



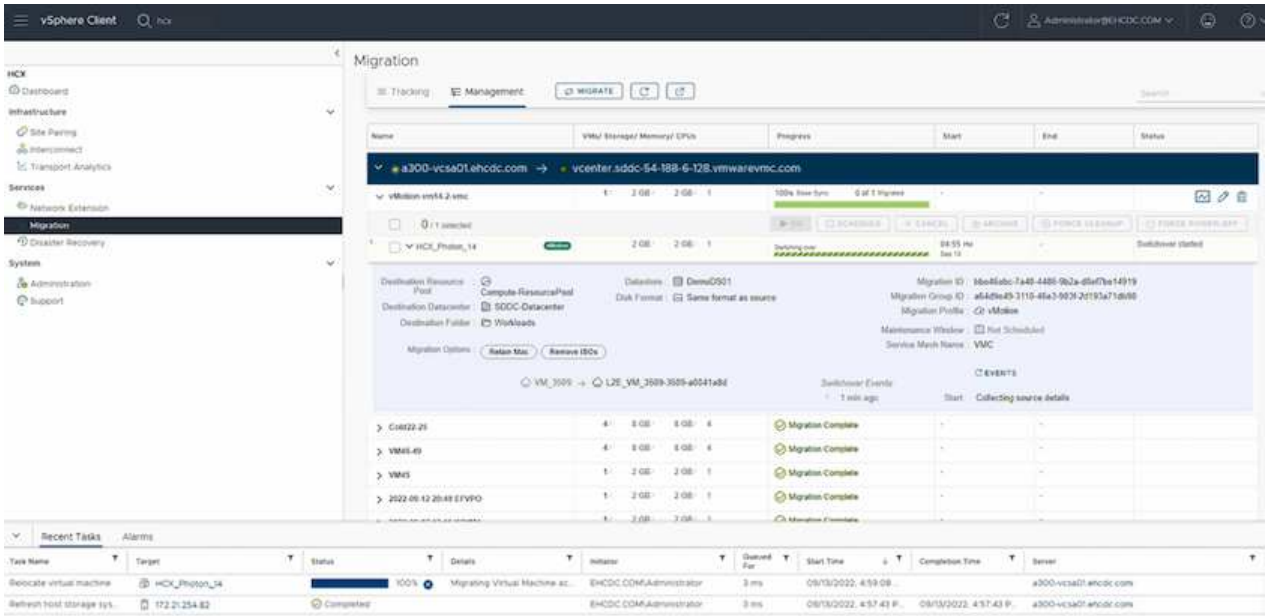
3. 新增群組名，並在傳輸和放置下更新必填欄位（叢集、儲存和目標網路），按一下驗證。



4. 驗證檢查完成後，按一下“Go”開始遷移。

> ⓘ vMotion 傳輸擷取 VM 活動記憶體、其執行狀態、其 IP 位址和其 MAC 位址。有關 HCX vMotion 的要求和限制的更多信息，請參閱 "了解 VMware HCX vMotion 和冷遷移"。

5. 您可以從 HCX > 遷移儀表板監控 vMotion 的進度和完成情況。

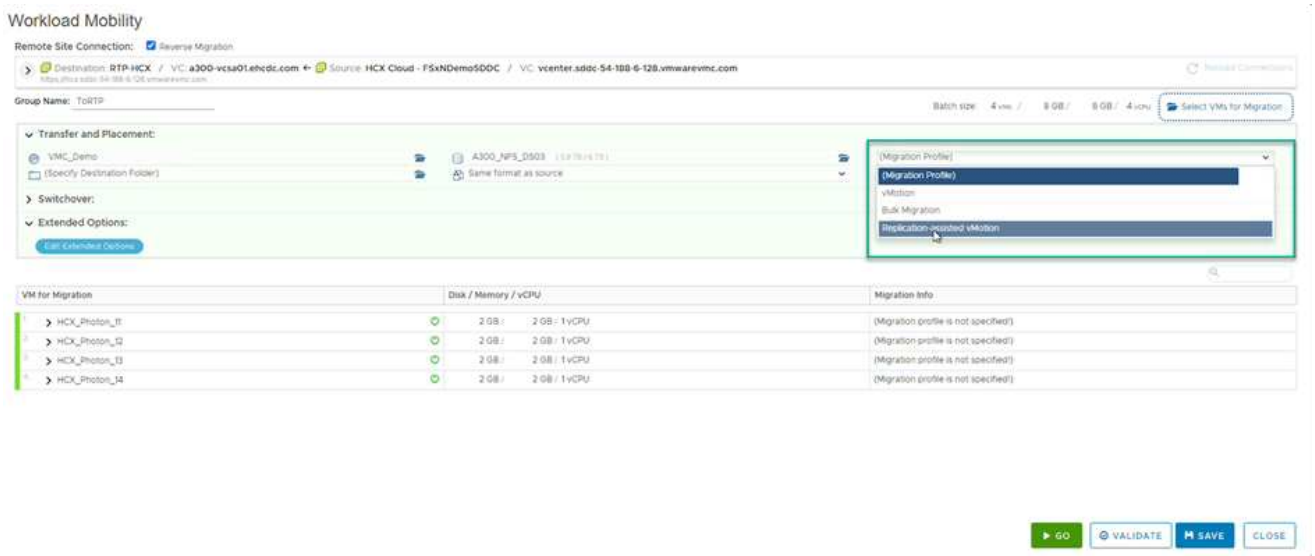


▼ **VMware 複製輔助 vMotion**

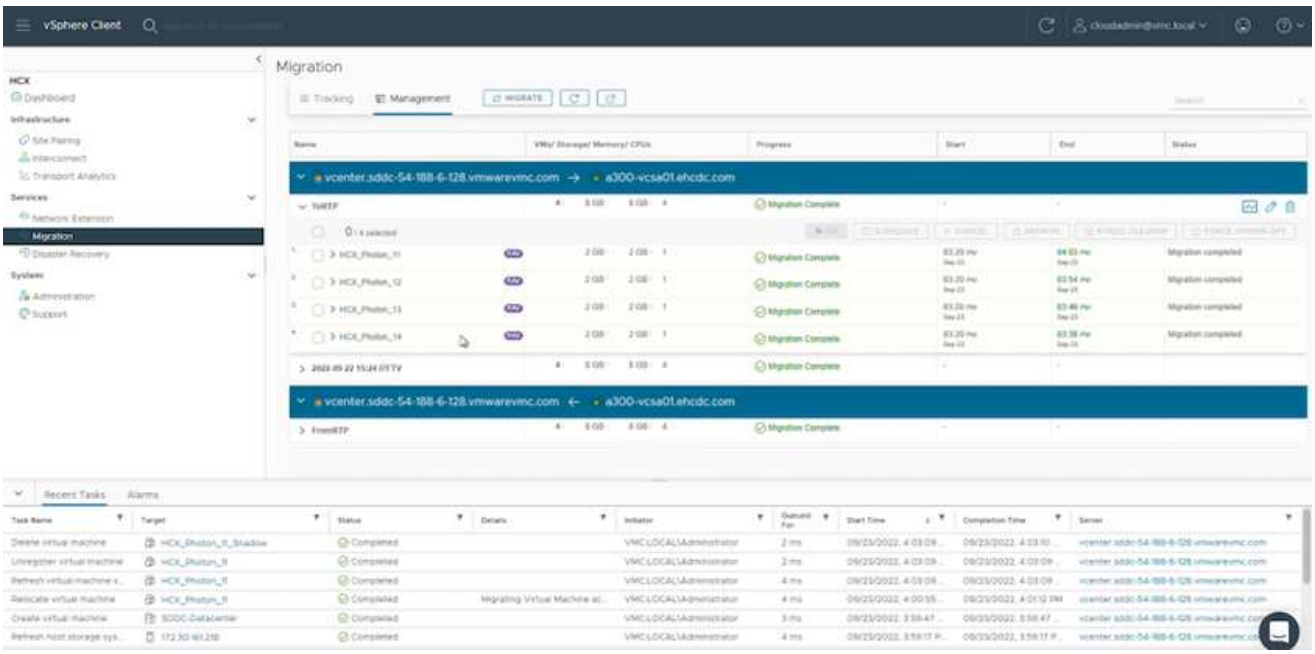
您可能從 VMware 文件中註意到，VMware HCX Replication Assisted vMotion (RAV) 結合了批量遷移和

vMotion 的優勢。批次遷移使用 vSphere Replication 並行遷移多個虛擬機器 - 虛擬機器在切換期間重新啟動。 HCX vMotion 遷移時無需停機，但它是在複製群組中一次一個虛擬機器地連續執行的。 RAV 並行複製虛擬機器並保持同步，直到切換視窗。在切換過程中，它一次遷移一個虛擬機，虛擬機不會停機。

以下螢幕截圖顯示了作為複製輔助 vMotion 的遷移設定檔。



與少量虛擬機器的 vMotion 相比，複製的持續時間可能會更長。使用 RAV，僅同步增量並包含記憶體內容。以下是遷移狀態的螢幕截圖 - 它顯示了遷移的開始時間對於每個虛擬機器都是相同的，而結束時間是不同的。



有關 HCX 遷移選項以及如何使用 HCX 將工作負載從本地遷移到 VMware Cloud on AWS 的更多信息，請參閱 "VMware HCX 使用者指南"。

VMware HCX vMotion 需要 100Mbps 或更高的吞吐量能力。

目標 VMC FSx ONTAP資料儲存必須有足夠的空間來容納遷移。

結論

無論您的目標是全雲還是混合雲，以及駐留在本地任何類型/供應商存儲上的數據， Amazon FSx ONTAP和 HCX 都提供了部署和遷移工作負載的絕佳選擇，同時通過使數據要求無縫連接到應用程序層來降低 TCO。無論用例如何，選擇 VMC 和 FSx ONTAP資料儲存都可以快速實現雲端優勢、跨本地和多個雲端的一致基礎架構和操作、工作負載的雙向可移植性以及企業級容量和效能。使用 VMware vSphere 複製、VMware vMotion 甚至 NFC 複製來連接儲存和遷移虛擬機器所採用的流程和程式相同。

總結

該文件的要點包括：

- 現在您可以將Amazon FSx ONTAP用作 VMC SDDC 的資料儲存。
- 您可以輕鬆地將資料從任何本地資料中心遷移到使用 FSx ONTAP資料儲存運行的 VMC
- 您可以輕鬆擴大或縮小 FSx ONTAP資料儲存以滿足遷移活動期間的容量和效能要求。

在哪裡可以找到更多信息

要了解有關本文檔中描述的信息的更多信息，請參閱以下網站連結：

- VMware Cloud 文件

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSx ONTAP文檔

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX 使用者指南

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

適用於 **AWS/EVS** 的**NetApp**

將 **FSx ONTAP**掛載為 **EVS** 的外部資料存儲

如何將**Amazon FSx for NetApp ONTAP**掛載為 **Amazon Elastic VMware Service** 的外部資料存儲

本文檔將介紹建立 FSx for ONTAP檔案系統並將其附加為互聯網小型電腦系統介面 (iSCSI) 或網路檔案系統 (NFS) 資料儲存以供 Amazon EVS 使用的具體步驟。

介紹

擁有現有本地 VMware 投資的組織正在尋求高效且經濟高效的方式，透過在 AWS 上遷移、爆發、擴展或保護（備份、災難復原）副本來實現其部署的現代化，但他們面臨著多項挑戰。隨著 Amazon Elastic VMware Service (Amazon EVS) 的發布，現在有了原生的 AWS 服務，可以直接在 Amazon Virtual Private Cloud (VPC) 中執行 VMware Cloud Foundation (VCF)。

Amazon EVS 可以將現有的 VCF 部署擴展到 AWS，在高峰使用期間爆發到 AWS 以擴展效能，並在 AWS 上完全執行 VCF 工作負載以促進現代化、資料中心退出、整合和其他使用案例。

儘管 Amazon EVS 提供了強大的優勢，但預設的超融合架構將運算和儲存結合在一起，從而阻止根據業務需求獨立擴展其中一個或另一個。在當今以資料為中心的世界中，許多組織的儲存需求高於運算需求。然而，在 VMware 超融合架構中，儲存資源與運算資源是結合在一起的。這意味著只能透過新增永遠不會使用的運算主機來實現儲存擴充。這種情況會大大增加成本，尤其是在儲存繁重的工作負載中。

為了解決這個問題，AWS 和NetApp提供Amazon FSx for NetApp ONTAP （FSx for ONTAP）作為 Amazon EVS 的外部儲存服務。 FSx for ONTAP是一種 AWS 原生儲存服務，可提供NetApp ONTAP軟體的高效能、資料彈性和成本效益功能。透過使用 FSx for ONTAP作為外部存儲，Amazon EVS 使用者可以獨立擴展運算和儲存資源，從而實現最佳總體擁有成本 (TCO)。

概況

本文檔將介紹建立 FSx for ONTAP檔案系統並將其附加為互聯網小型電腦系統介面 (iSCSI) 或網路檔案系統 (NFS) 資料儲存以供 Amazon EVS 使用的具體步驟。

本指南的目的

本指南提供了有關如何為 Amazon EVS 設定 FSx for ONTAP資料儲存的說明，以及最佳實踐、可支援性要求、大小考慮因素和其他信息，以幫助您規劃、設計和實施整合。

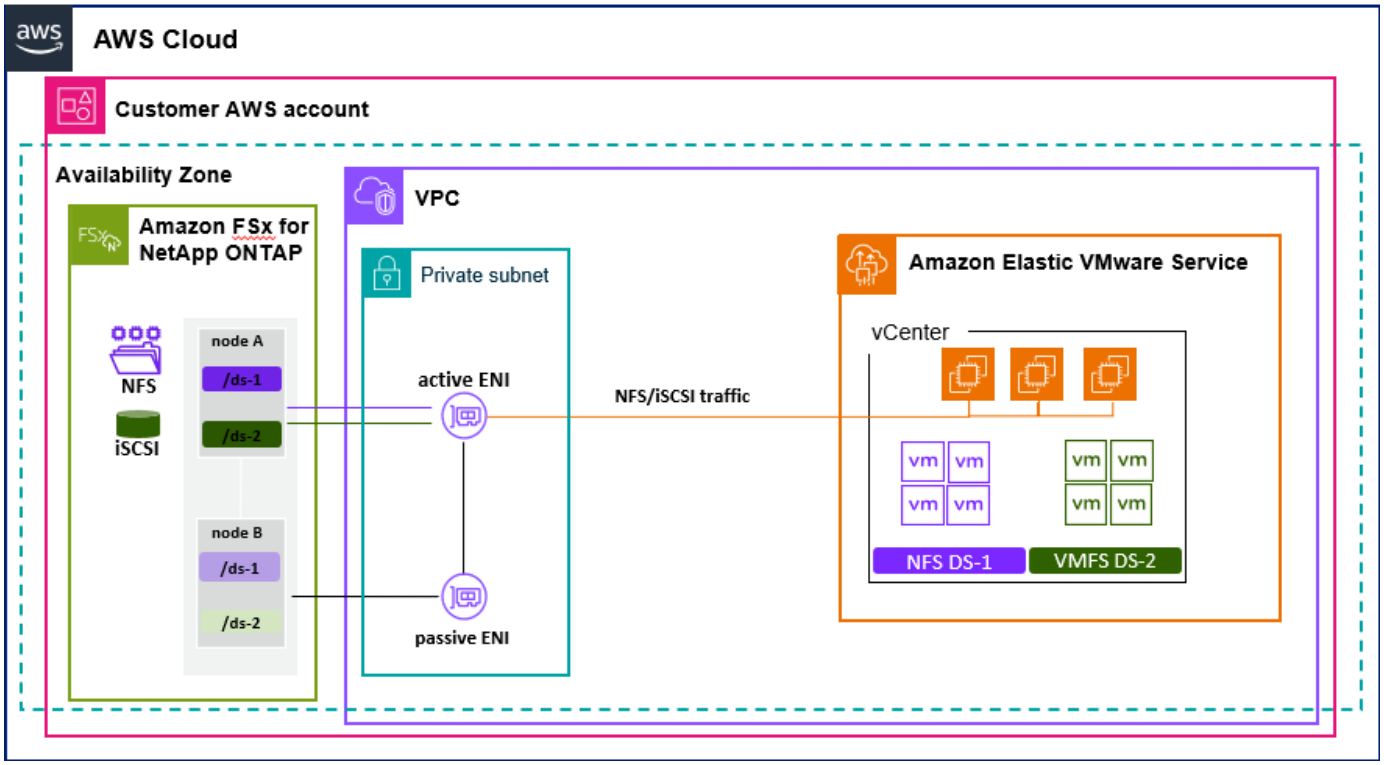
對象

本教學適用於熟悉 VMware vSphere、Amazon EVS、AWS 控制台和 FSx for ONTAP 的雲端架構師和雲端管理員。

進階架構

在本節中，我們將概述使用 FSx for ONTAP作為 Amazon EVS 資料儲存的解決方案架構。

下面您可以看到 AWS VPC 內具有 Amazon EVS 環境的 FSx for ONTAP資料儲存區的架構進階視圖。



使用 **FSx for ONTAP**作為 **NFS** 資料儲存庫的部署過程

本節將展示如何將 FSx for ONTAP部署為 NFS 資料儲存區的步驟。部署 iSCSI 資料儲存區的步驟將在下一節中詳細介紹。

進階部署步驟

部署 FSx for ONTAP檔案系統作為 Amazon EVS 的 NFS 資料儲存並在兩種服務之間建立連線將包含下列步驟：

- 在 Amazon EVS VCF 環境所在的相同 VPC 中設定 FSx for ONTAP檔案系統。
- 驗證安全群組和路由表。
- 連接 FSx for ONTAP儲存磁碟區以用作 Amazon EVS 的 NFS 資料儲存。

先決條件

在開始將 FSx for ONTAP設定為 Amazon EVS 的 NFS 資料儲存之前，應滿足以下先決條件：

- Amazon EVS 虛擬化環境。有關如何執行此操作的更多信息，請參閱"Amazon EVS 入門指南"。
- 使用適當的 SSD 儲存容量、預先配置的 IOPS 和吞吐量為ONTAP建立單一可用區 (AZ) FSx。
- 為了獲得最佳效能，請將 FSx for ONTAP檔案系統放置在與 Amazon EVS 執行個體相同的 VPC 內。請注意，當 FSx for ONTAP部署在不同 VPC 時，也支援 VPC Peering。
- 根據效能需求，選擇單可用區 FSx for ONTAP檔案系統所需的正確 IOPS 和吞吐量。看"FSx for ONTAP 的效能規格詳情"了解每個可用選項提供的吞吐量和 IOPS。

> 在本指南中，我們將在與服務存取子網路相同的子網路中部署 FSx for ONTAP檔案系統。

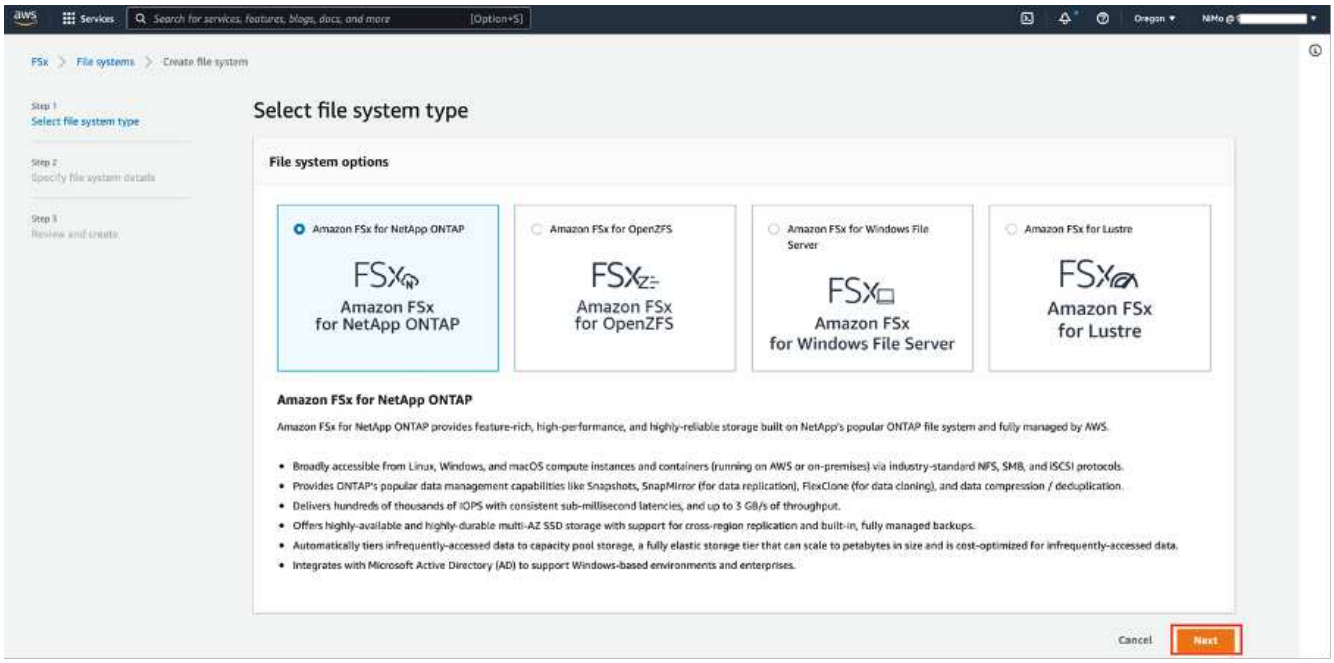
在 VPC 中部署 Amazon EVS 虛擬化環境後，您可以繼續設定將用作 NFS 資料儲存的單一可用區 FSx for ONTAP檔案系統。

> 您的 FSx for ONTAP檔案系統應部署在與 Amazon EVS SDDC 相同的 AZ 中。

建立 **FSx for ONTAP**檔案系統

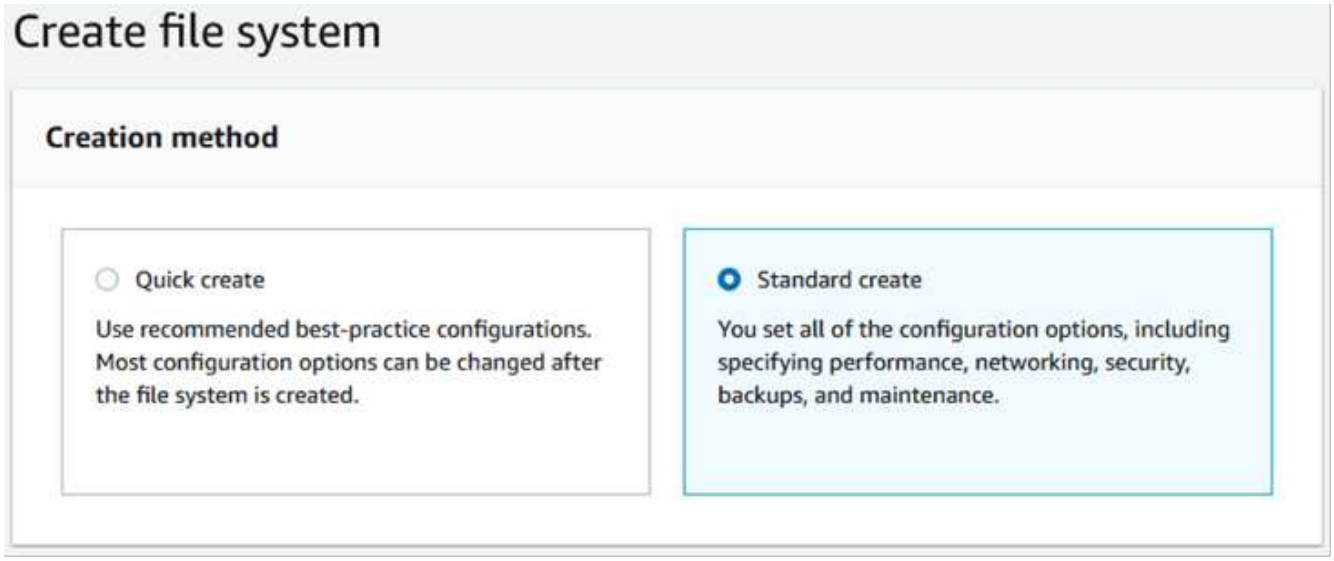
以下步驟將向您展示如何設定和掛載 FSx for ONTAP檔案系統：

1. 前往Amazon FSx控制台 `https://console.aws.amazon.com/fsx/`使用您的網際網路瀏覽器並使用您的憑證登入。
2. 在控制台中，選擇建立檔案系統。這將啟動安裝精靈來建立 FSx for ONTAP檔案系統。
3. 首先，選擇檔案系統類型。從可用的檔案系統選項中，選擇“Amazon FSx for NetApp ONTAP”，然後按一下“下一步”按鈕繼續。

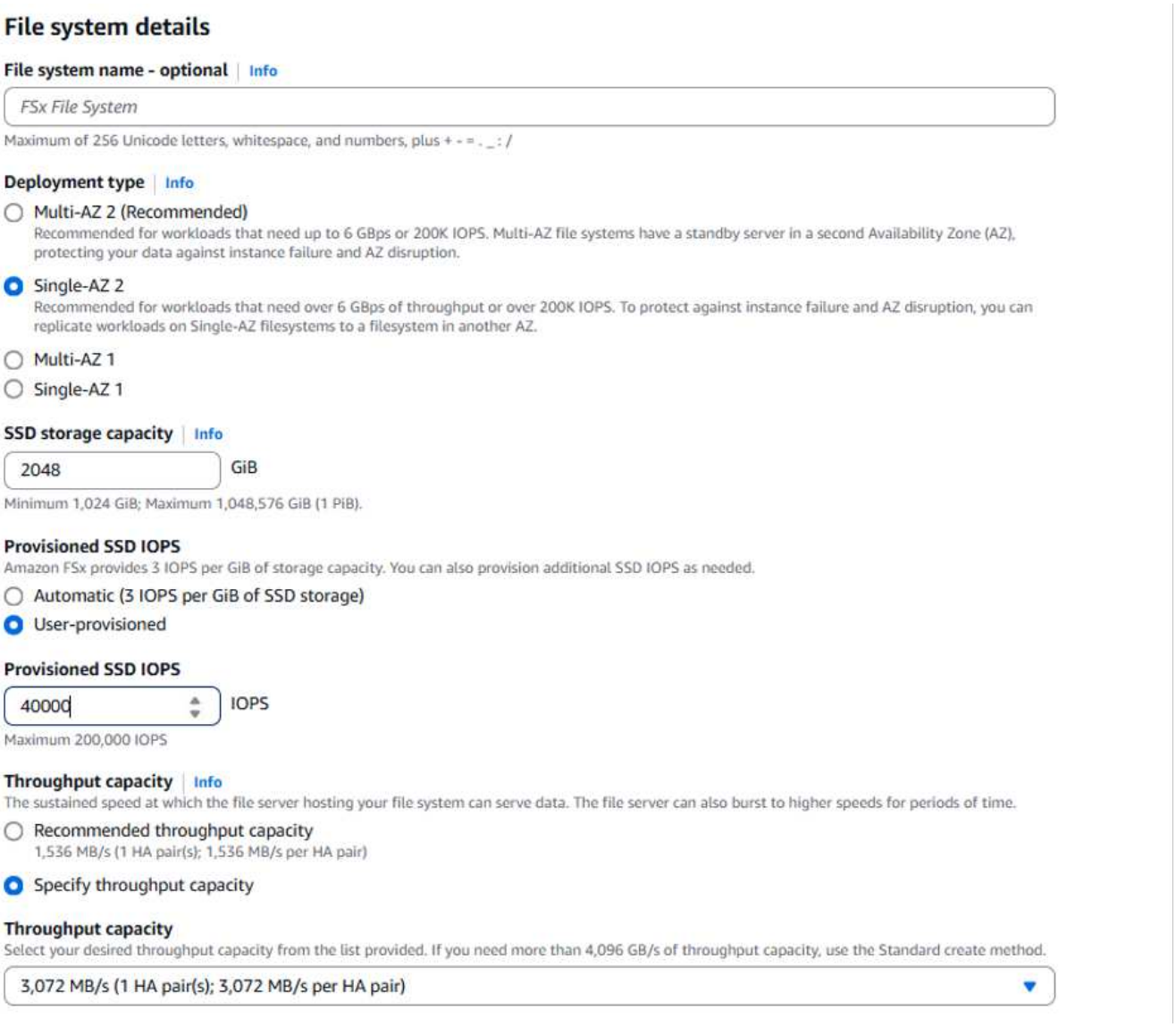


4. 您將可以在“快速建立”和“標準建立”選項之間進行選擇。快速建立提供預定義配置，標準建立允許您定義自己的配置。

   選擇“標準創建”選項。

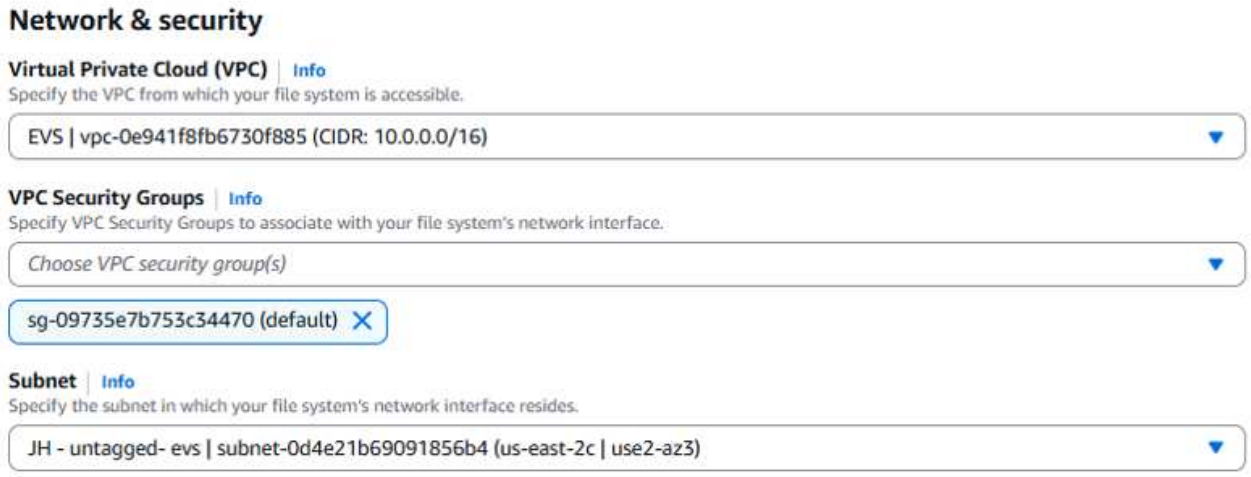


   現在您將進入標準建立檔案系統設定精靈。在檔案系統詳細資料頁面中，選擇並輸入如下圖所示的相同資訊：



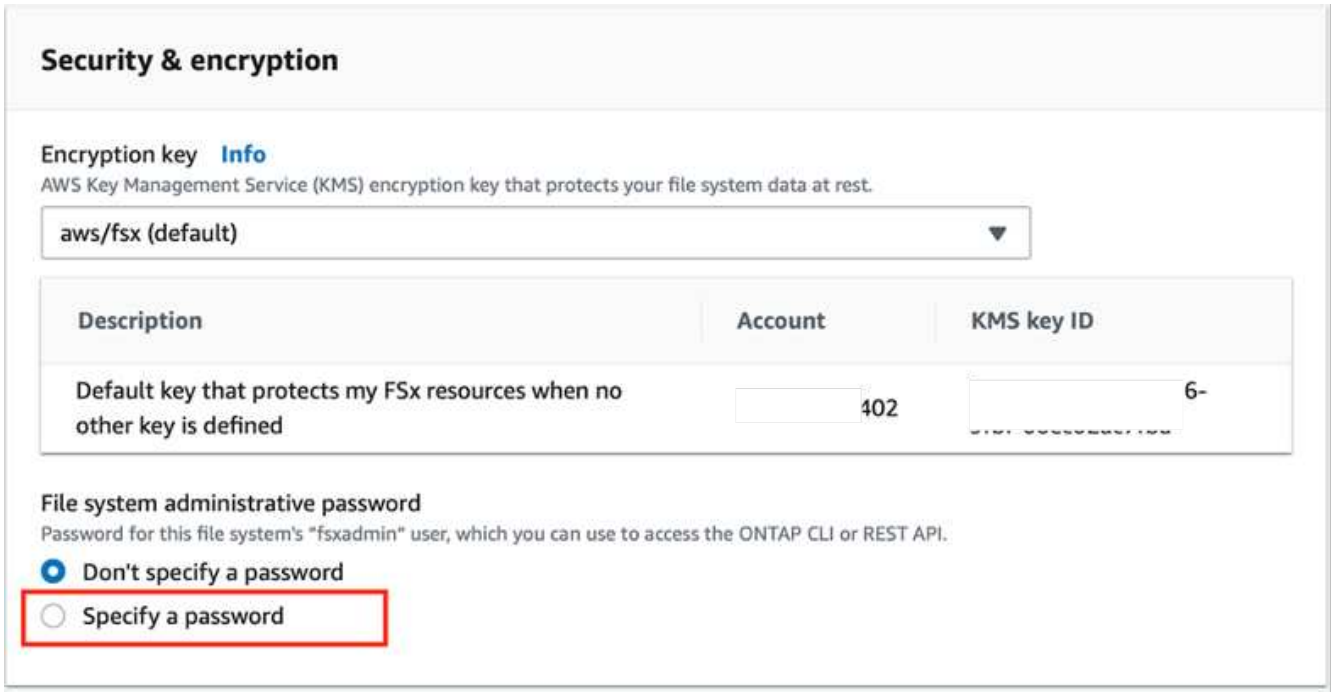
5. 向下捲動到標有“網路和安全”的部分。在本節中，您將設定子網路和 VPC 的詳細資訊。為了本指南的目的，我們從下拉式選單中選擇了“EVS-VPC”，並選擇服務存取子網路（未標記的 VLAN）作為 EVS 虛擬環境的子網路。

> ⓘ 此子網路可以是 VPC 中任何未標記的私有子網路。只要配置了正確的路由，它也可以位於透過 VPC Peering 連接的不同 VPC/子網路中。

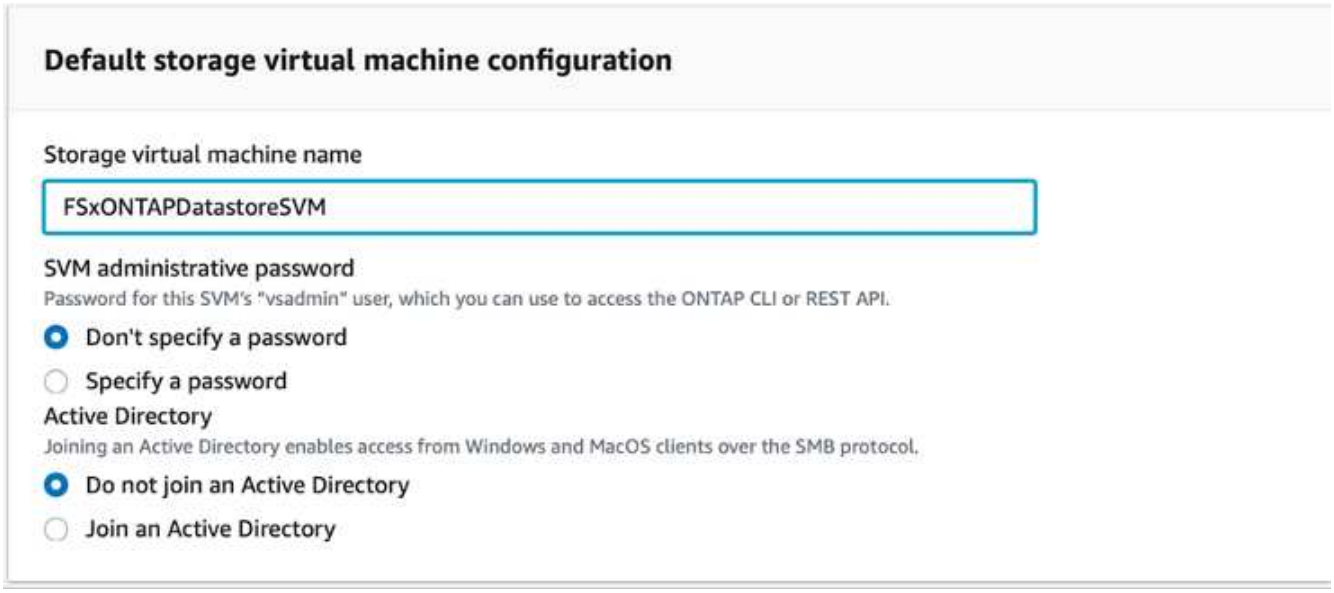


6. 向下捲動，您會找到“安全性和加密”部分。在這裡，從下拉式選單中選擇加密金鑰。這些金鑰由 AWS 金鑰管理服務 (AWS KMS) 提供，並將保護 FSx for ONTAP檔案系統中的靜態資料。

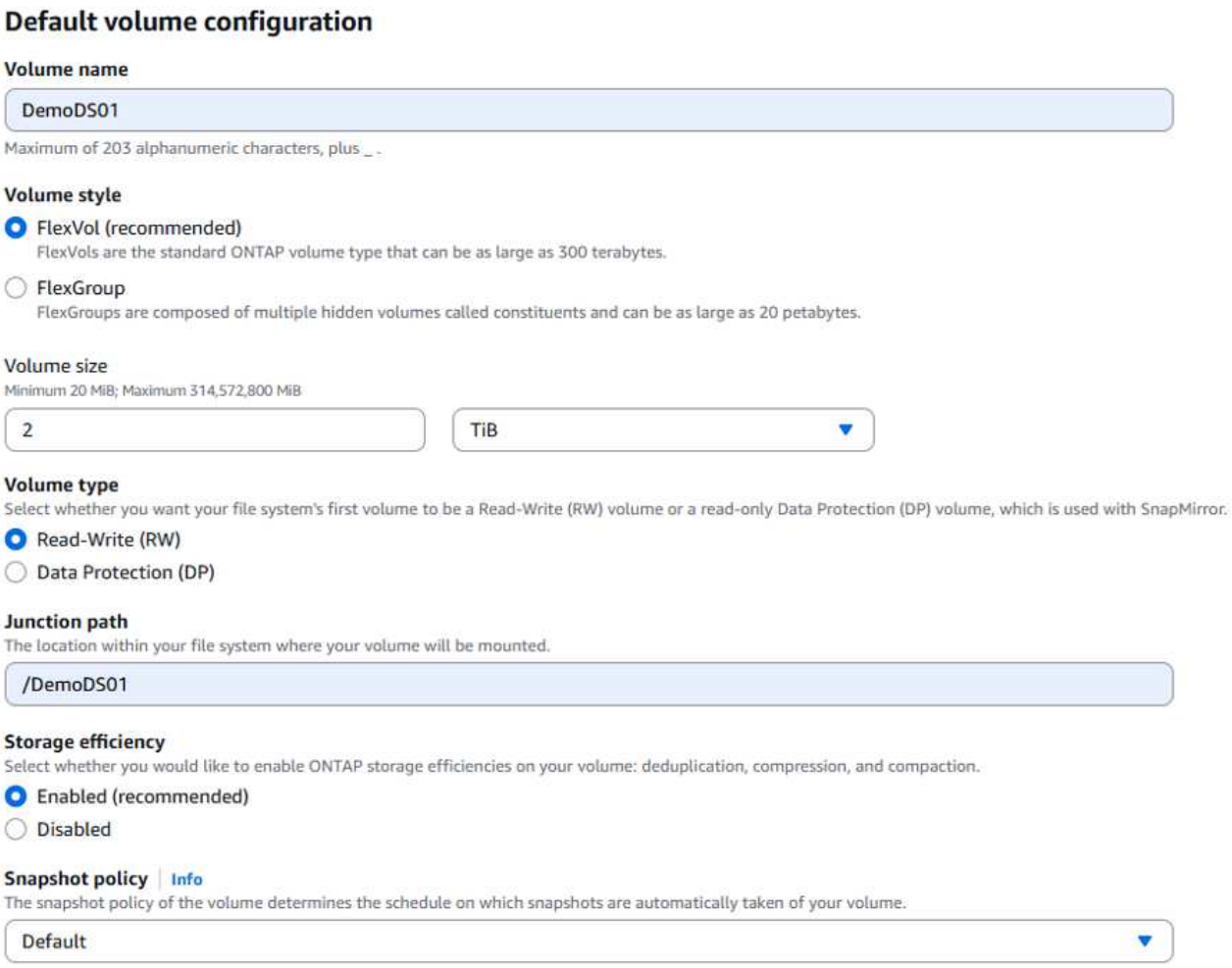
   接下來，在「檔案系統管理密碼」設定中，為將管理檔案系統的 fsxadmin 使用者指定一個唯一的密碼。



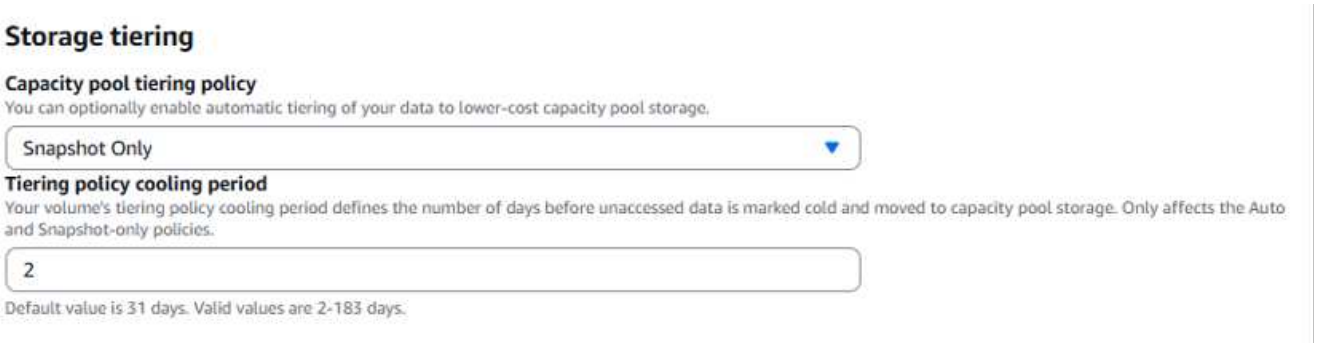
7. 接下來，您將向下捲動到標題為「預設儲存虛擬機器配置」的部分。在這裡，您需要為儲存虛擬機器 (SVM) 提供一個名稱。



8. 接下來，向下捲動到標題為「預設磁碟區配置」的部分。在這裡您將為磁碟區提供名稱並設定磁碟區大小。磁碟區協定應為 NFS v3（預設為啟用）。按一下此選項可啟用儲存效率功能（壓縮、重複資料刪除和壓縮），以減少整體儲存使用量和成本。



9. 對於儲存分層選項，從下拉式選單中選擇“僅快照”並設定分層策略冷卻期。預設值為 31 天，但對於此範例，我們設定了兩天的冷卻期。

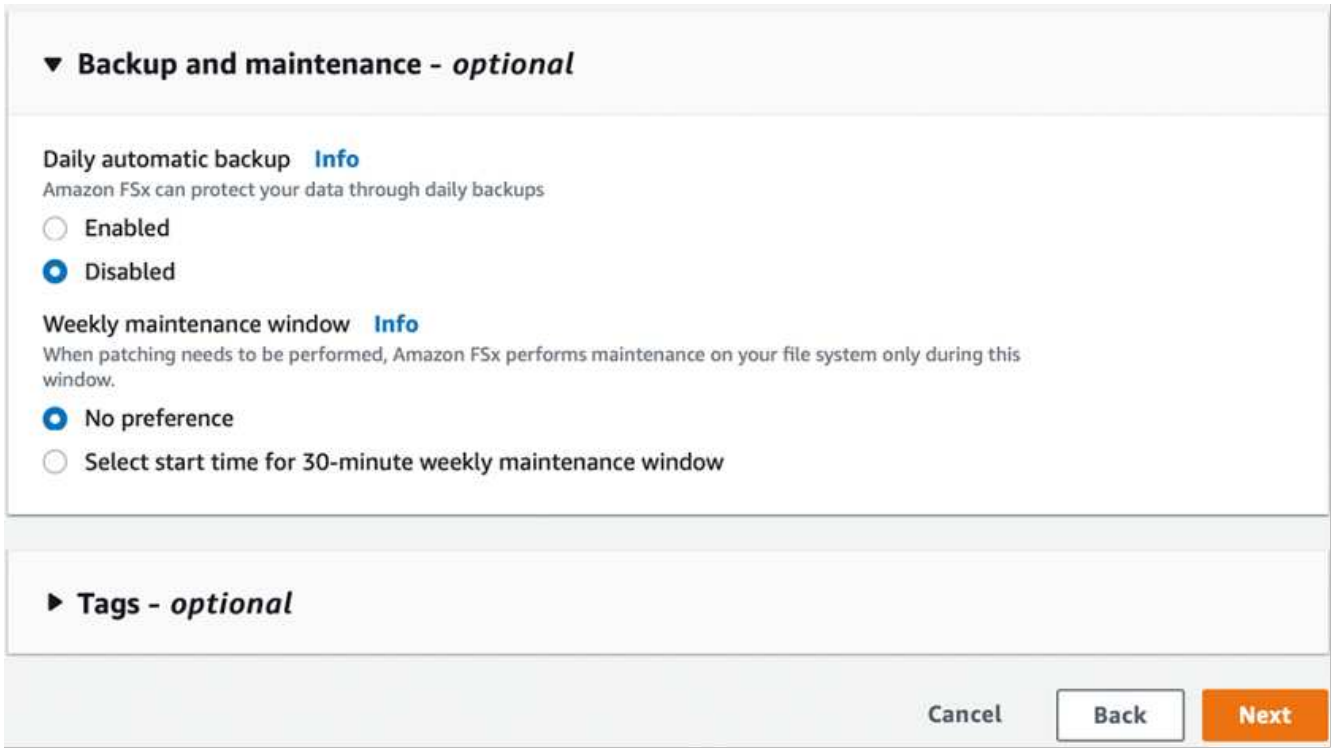


10. 建立磁碟區後，使用ONTAP命令列介面 (ONTAP CLI) 修改下列參數：

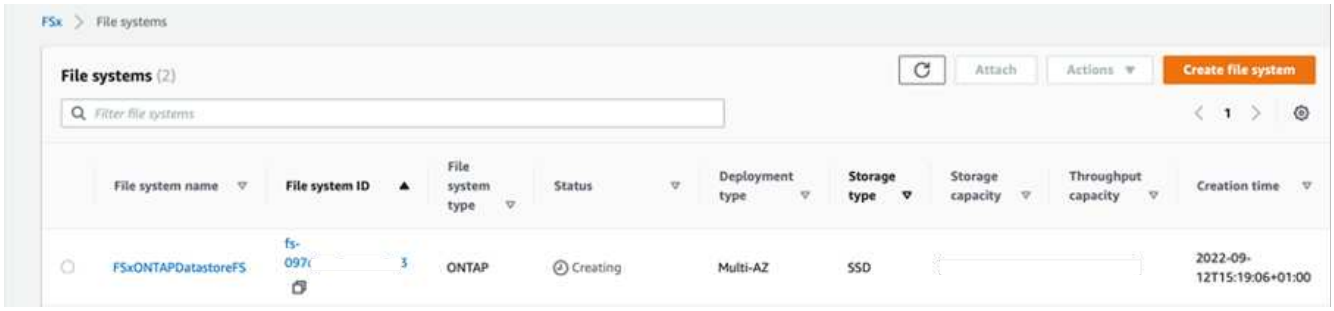
環境	配置
數量保證	無（精簡配置）
部分儲備	0%
snap_reserve	0%
自動調整大小	擴大_縮小
儲存效率	已啟用
卷分層策略	僅快照
訪問時間更新（-atime-update）	錯誤的
最小預讀（-min-readahead）	錯誤的
快照策略	沒有任何

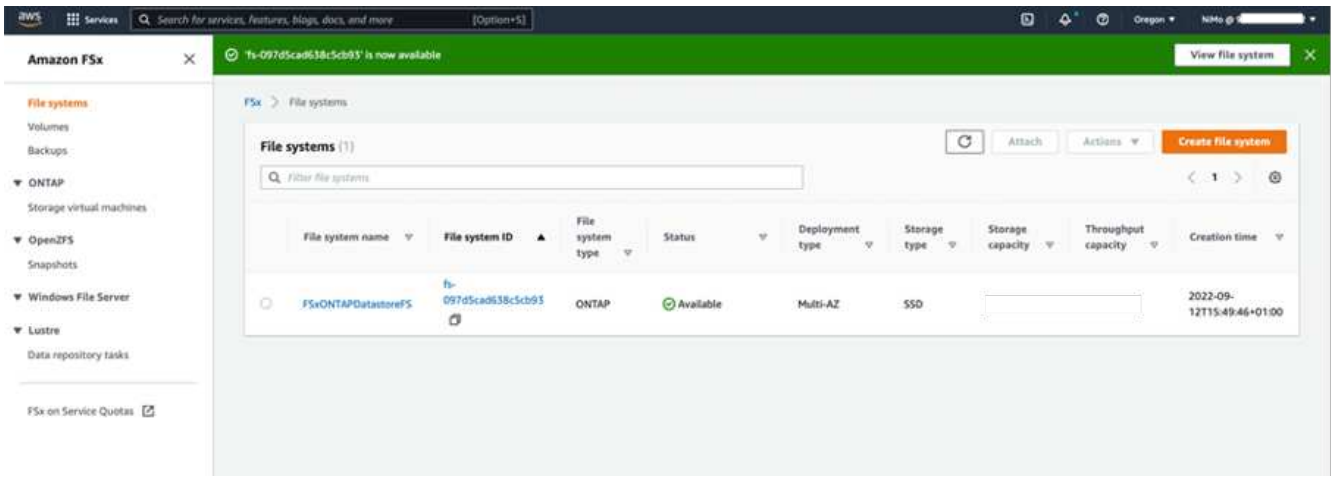
11. 在可選的「備份和維護」步驟中，停用每日自動備份並為每週維護視窗選擇「無首選項」。

    完成後按一下“下一步”。



12. 現在，您將獲得按照前面步驟設定的整個檔案系統配置的審查。檢查所有參數無誤後，點選「建立檔案系統」按鈕完成設定。

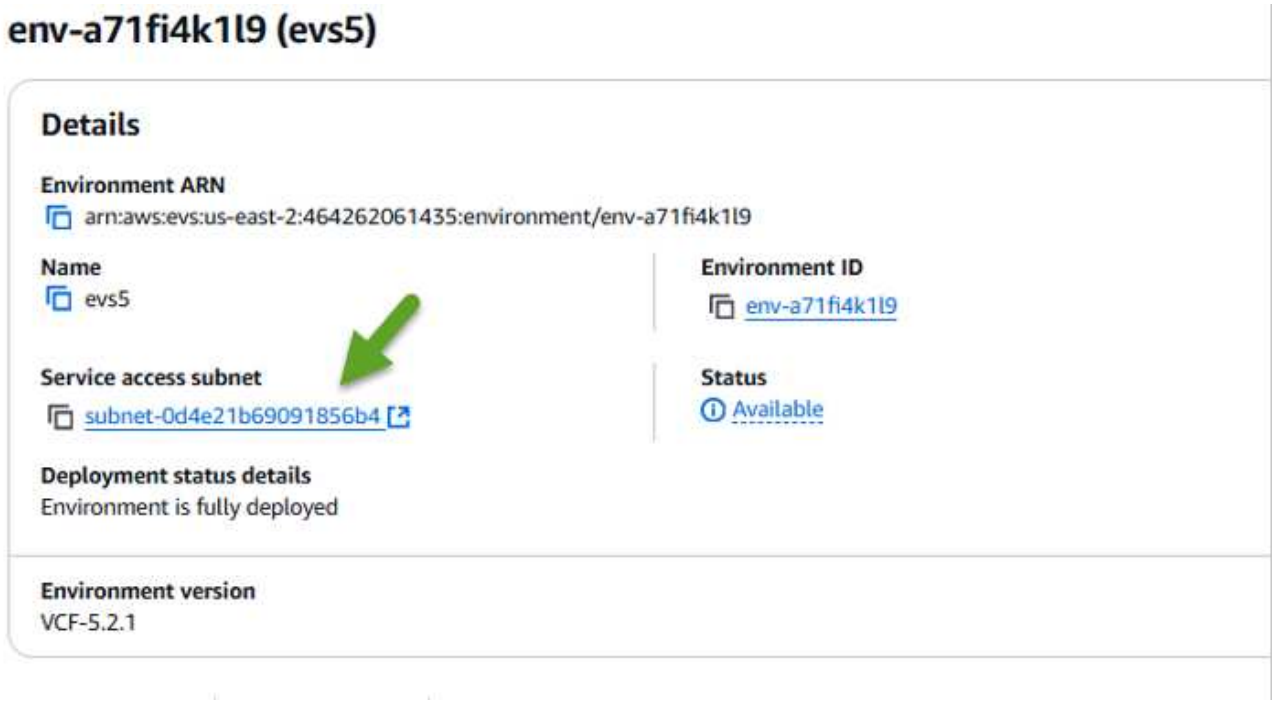




若要建立額外的 FSx for ONTAP檔案系統，您可以按照上面詳述的步驟操作，根據需要調整影響效能和磁碟容量的值。要了解有關 FSx for ONTAP效能選項的更多信息，請參閱"此文件頁面"。

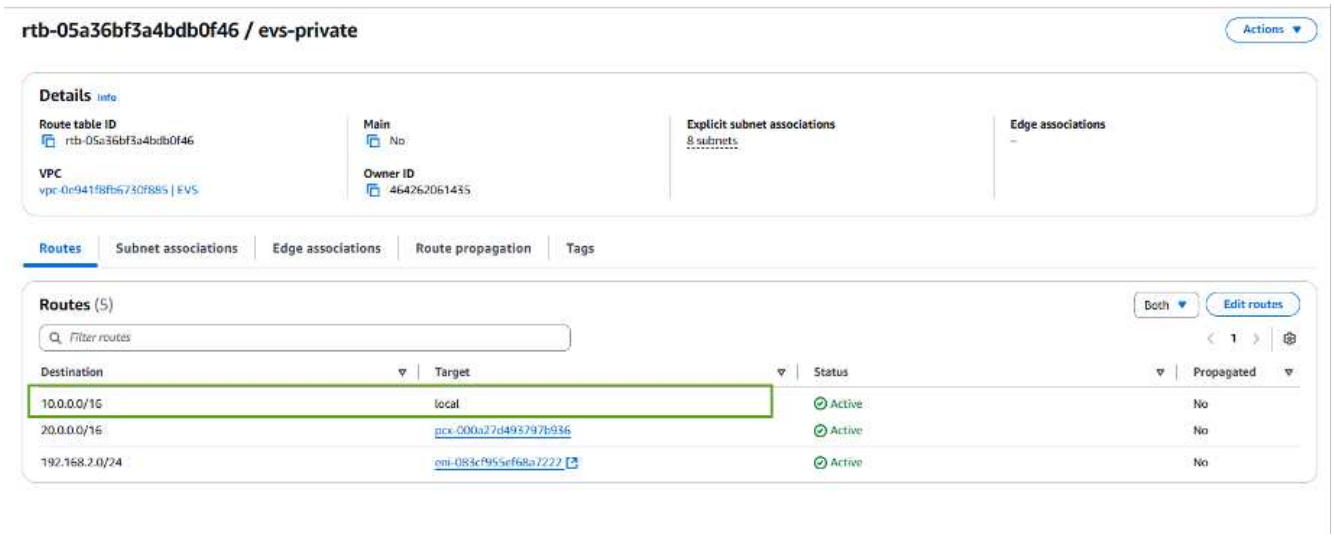
驗證 VPC 和 SDDC 路由和安全群組對於確保 Amazon EVS 虛擬化環境和 FSx for ONTAP檔案系統元件能夠正常協同工作非常重要。

1. 瀏覽至 Elastic VMware 服務 > 虛擬化環境 > [您的 Amazon EVS 環境] 並選擇服務存取子網，如下方綠色箭頭所示：

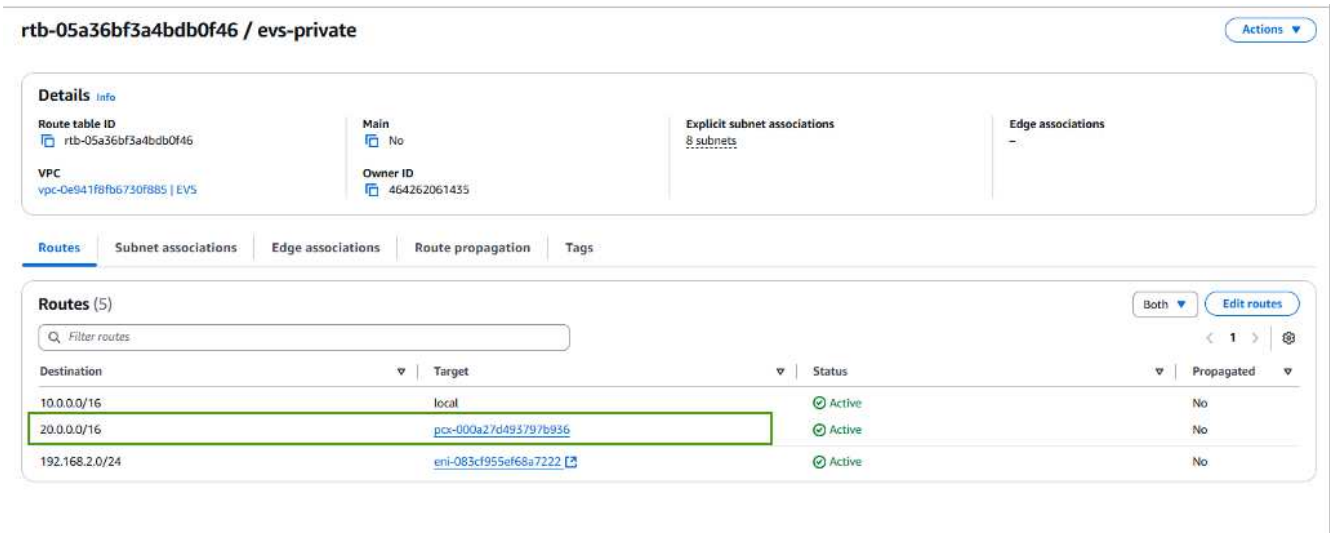


2. 這將打開子網面板。在此面板上找到路線表並點擊它。

   在此範例中，FSxN ONTAP檔案系統與 Amazon EVS VCF 環境位於相同 VPC 中，因此預設路由就足夠了。



   如果 FSx for ONTAP檔案系統位於不同的 VPC 中，則檢查是否已新增至該 VPC 的路由。在此範例中，已新增 VPC Peering 到 FSx for ONTAP系統所在 VPC 的路由。



3. 接下來，您需要檢查連接到 FSx for ONTAP檔案系統的安全性群組（即連接到彈性網路介面 (ENI) 的安全群組）是否允許存取 NFS 連接埠。

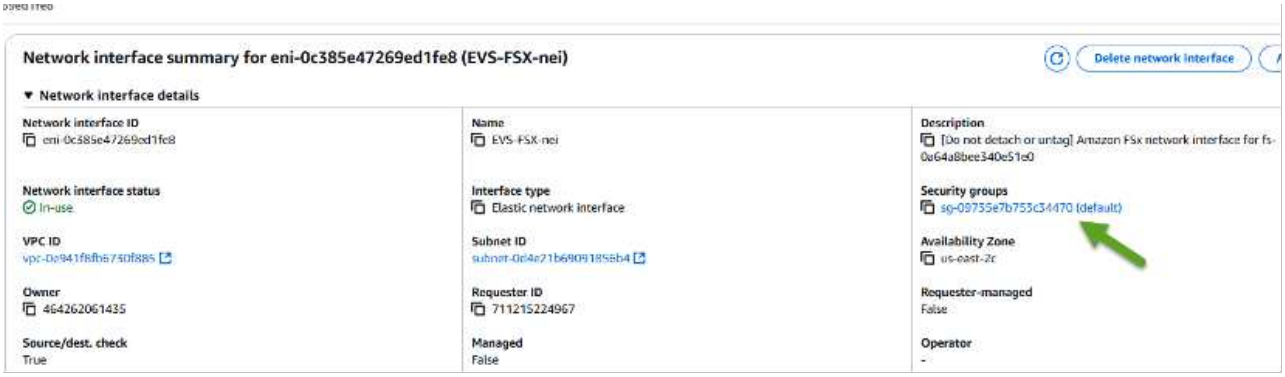
   有關 NFS 和 iSCSI 協定連接埠的完整列表，請參閱連結： https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html ://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]使用 Amazon VPC 文件進行檔案系統存取控制]。

   若要驗證您的 FSx for ONTAP檔案系統是否與安全性群組關聯：

   a. 在 AWS 控制台中，導覽至 FSx > 檔案系統 > [您的 FSx for ONTAP檔案系統]。

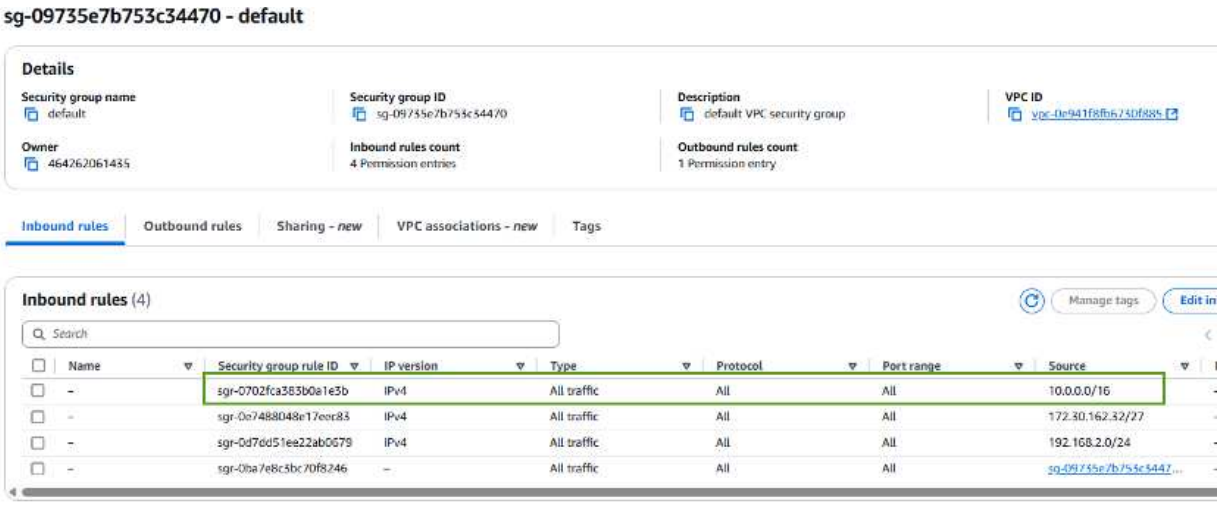
   b. 在網路和安全性標籤中，按一下 ENI。

   c. 找到網路介面詳細資訊下列出的與 ENI 關聯的安全群組（如下圖中的綠色箭頭所示）。



   d. 驗證連接埠。在以下畫面所示的範例中，所有流量都被允許。但是，您可以將其限制為僅限 NFS 連接埠。以下是連接埠清單：

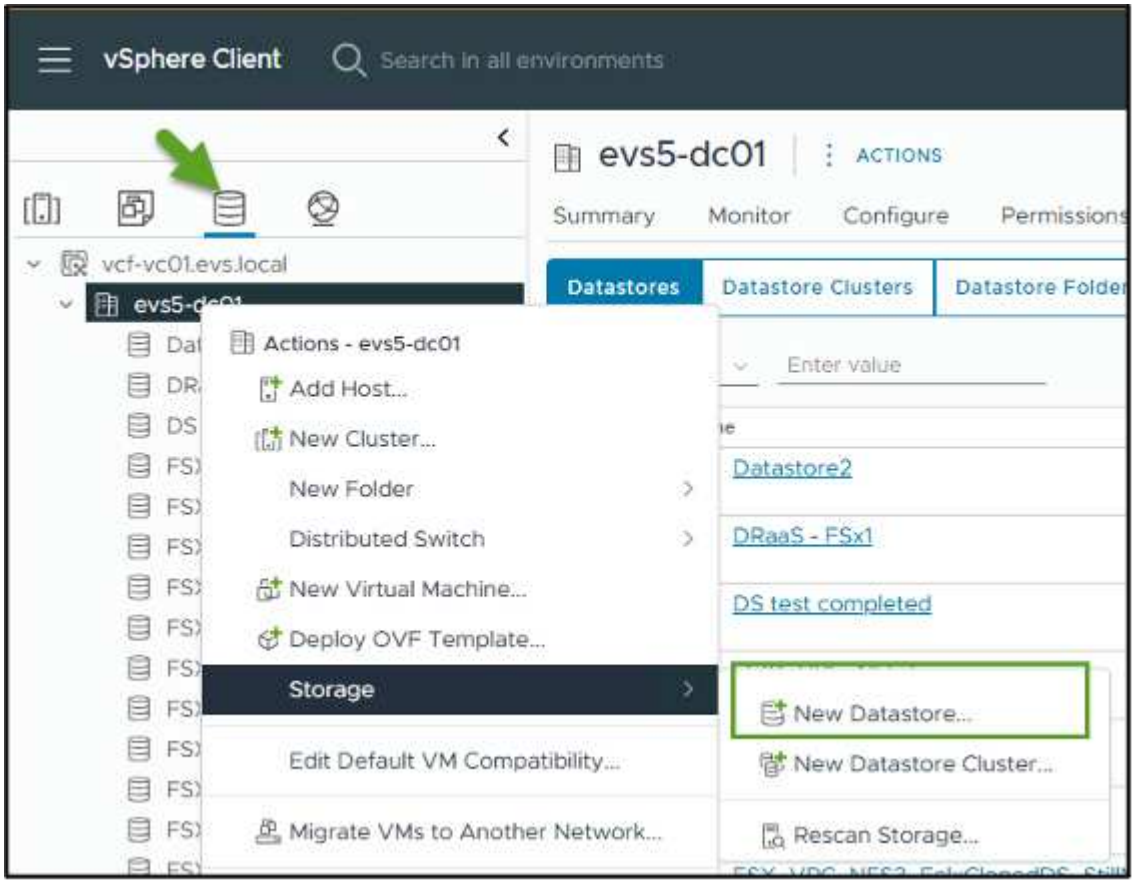
      - 連接埠 111 TCP：連接埠對映器，用於協商在 NFS 請求中使用哪些連接埠。
      - 連接埠 635 TCP：Mountd，用於接收傳入的掛載請求。
      - 連接埠 2049 TCP：NFS，用於處理 NFS 流量。
      - 連接埠 4045 TCP：網路鎖定管理器 (NLM)，處理鎖定請求。
      - 連接埠 4046 TCP：網路狀態監視器 (NSM)，當伺服器重新啟動以進行鎖定管理時，它會發送 NFS 用戶端通知。



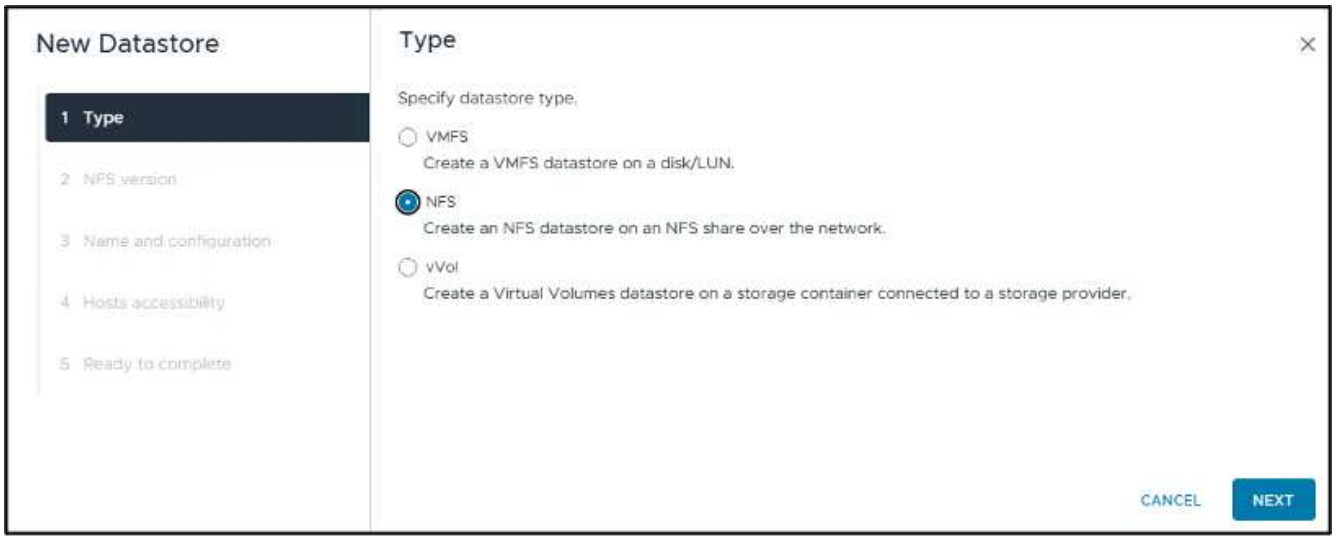
將 **FSx for ONTAP NFS** 磁碟區附加到 **Amazon EVS** 以用作資料存儲

現在您的 FSx for ONTAP檔案系統已設定完畢，並且所有正確的連線參數都已驗證，接下來就可以將 FSx for ONTAP儲存磁碟區附加到 Amazon EVS 了。以下步驟將展示如何存取 vCenter 並將 FSx for ONTAP磁碟區掛載為 NFS 資料儲存：

1. 在 vSphere 用戶端中，前往「資料儲存」標籤。找到資料中心，導航至存儲>新資料存儲，如下所示：

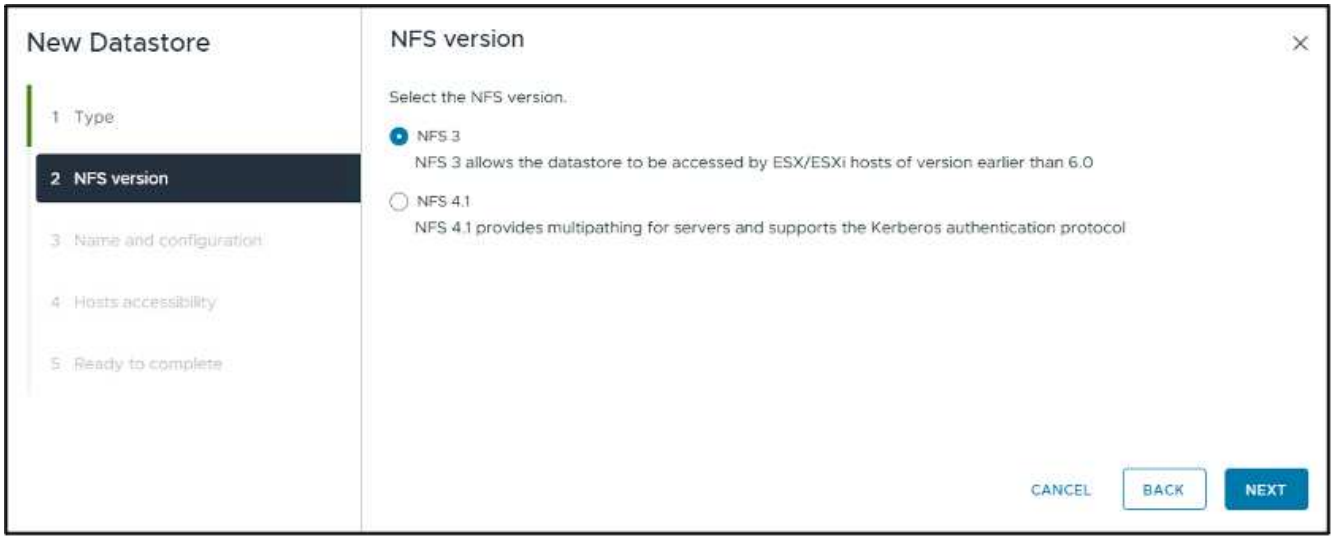


2. 您現在將進入新資料儲存精靈。在「類型」步驟中，您將選擇資料儲存類型。選擇“NFS”並點擊“下一步”繼續。



3. 在「NFS 版本」步驟中，您將選擇一個 NFS 版本。

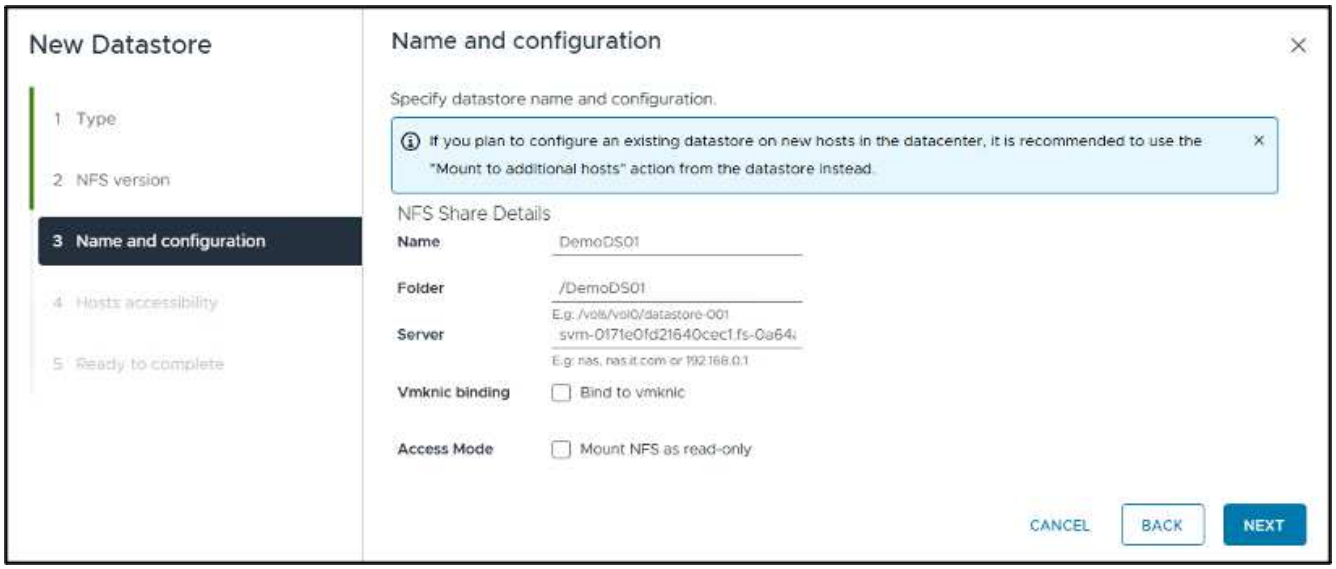
   為了本例的目的，我們將選擇“NFS 3”，但請注意，也可以使用 NFS v4.1。



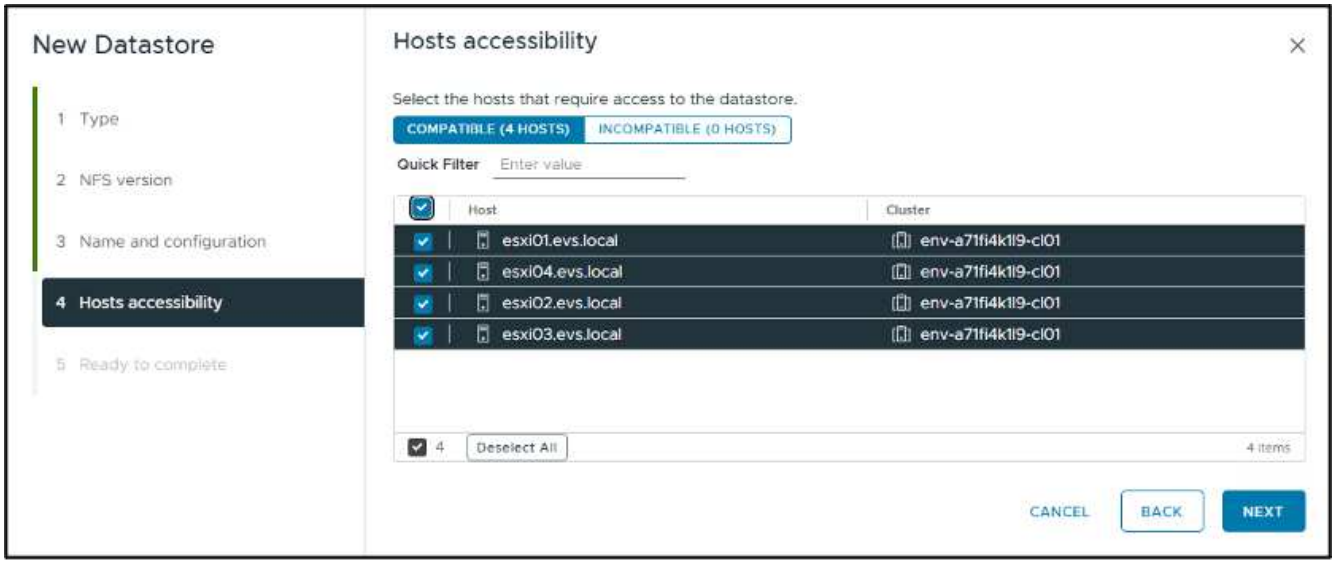
4. 在「名稱和配置」步驟中，您將：

   a. 命名資料儲存。
   b. 命名資料夾。使用 NFS 磁碟區的連接路徑。
   c. 命名伺服器。使用 SVM 的 NFS DNS 名稱或 NFS 的 IP 位址。

      按一下“下一步”繼續。



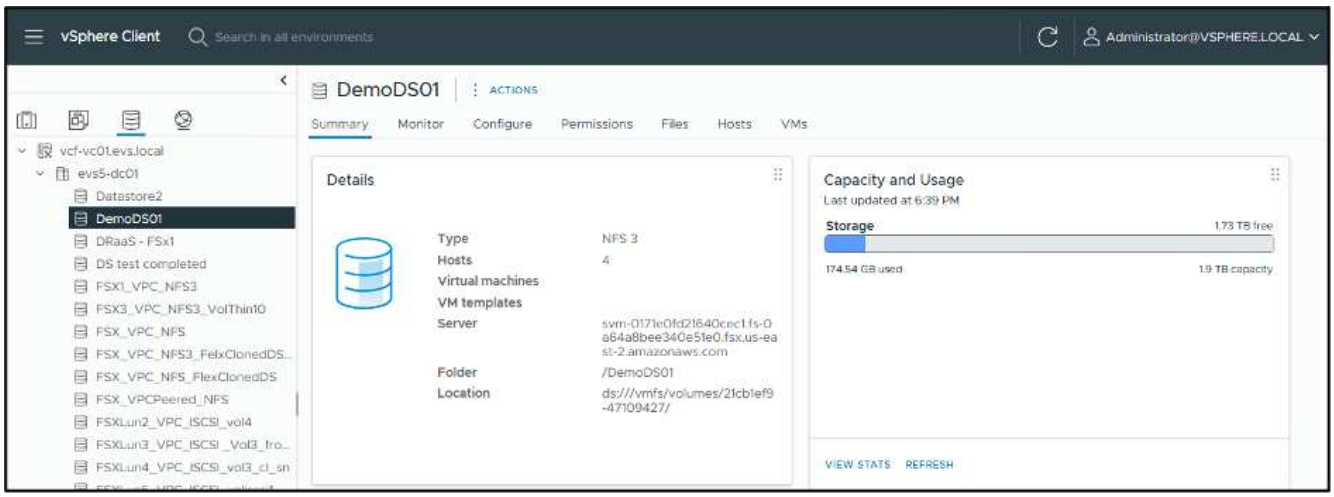
5. 在「主機可存取性」步驟中，選擇所有需要存取資料儲存的主機，然後按一下「下一步」繼續。



6. 在「準備完成」步驟中，檢查資料並按一下「完成」以完成設定。



7. 透過存取 vCenter 驗證 NFS 資料儲存是否已連接，如下所示：



使用 **FSx for ONTAP**作為 **iSCSI** 資料儲存庫的部署過程

本節介紹使用 FSx for ONTAP設定 iSCSI 資料儲存庫的步驟。

先決條件

在將 FSx for ONTAP配置並連線為 iSCSI 資料儲存之前，您必須先部署 Amazon EVS 虛擬化環境。有關更多信息，請參閱《Amazon EVS 入門指南》文件。本節也假設您已經部署了 FSx for ONTAP檔案系統，請參閱上面的詳細方法部分以了解適當的步驟。

進階部署步驟

部署 FSx for ONTAP檔案系統以用作 Amazon EVS 的 iSCSI 資料儲存並在兩項服務之間建立連線將包括下列步驟：

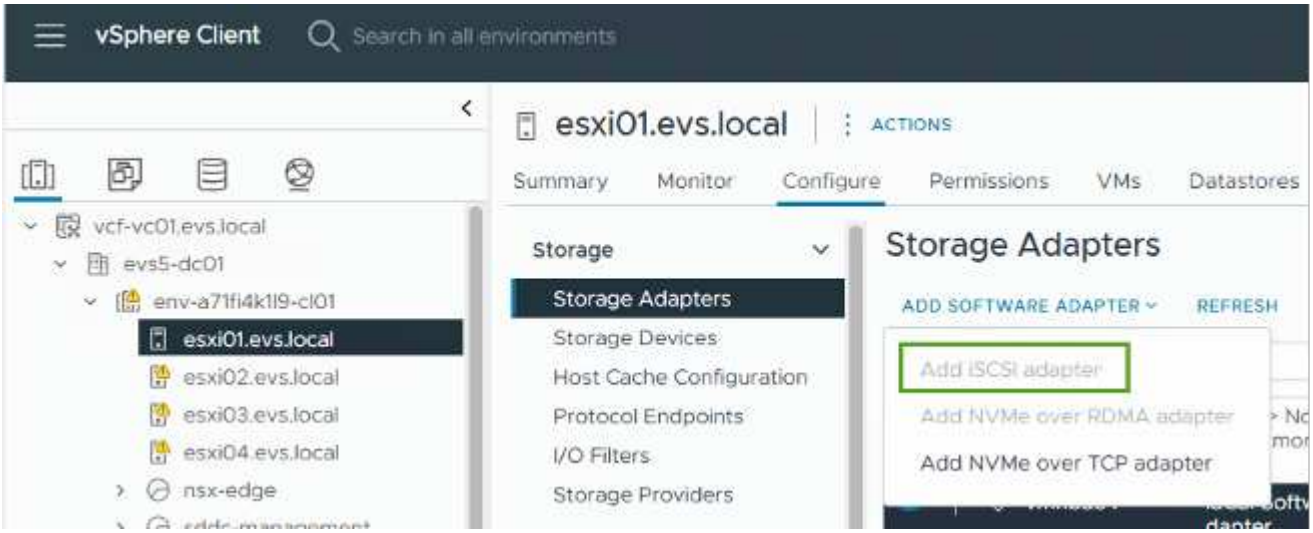
- 為每個 ESXi 主機設定一個 iSCSI 網路適配器。
- 建立並設定 FSx for ONTAP檔案系統、磁碟區、LUN 等。

- 將 ESXi 主機連接到 FSx for ONTAP檔案系統伺服器。
- 建立 iSCSI 資料儲存虛擬機器檔案系統 (VMFS)。

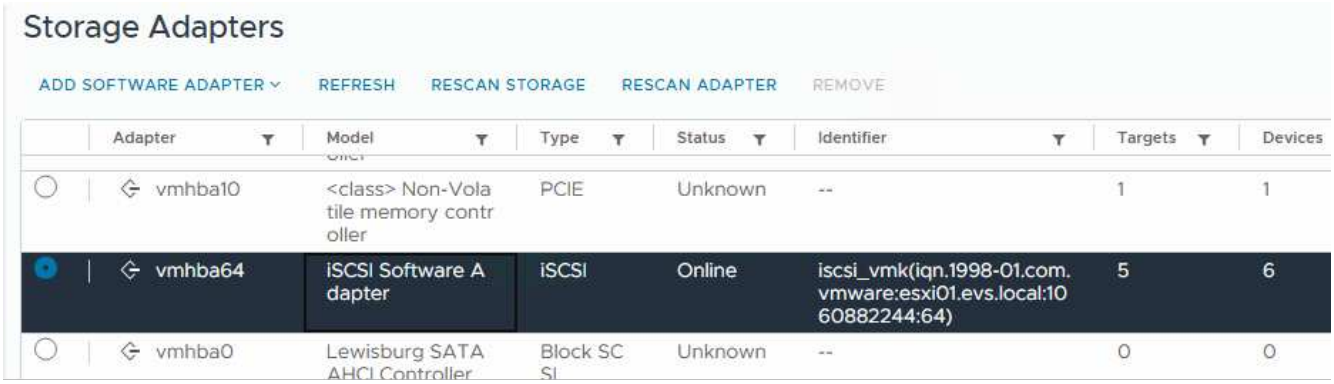
新增 **iSCSI** 網路介面卡

需要在您環境中的每個 ESXi 主機上執行下列步驟。

1. 進入vSphere客戶端，選擇ESXi主機。在配置標籤下，選擇“新增軟體適配器”，然後從下拉式選單中選擇“新增 iSCSI 適配器”，如下所示：

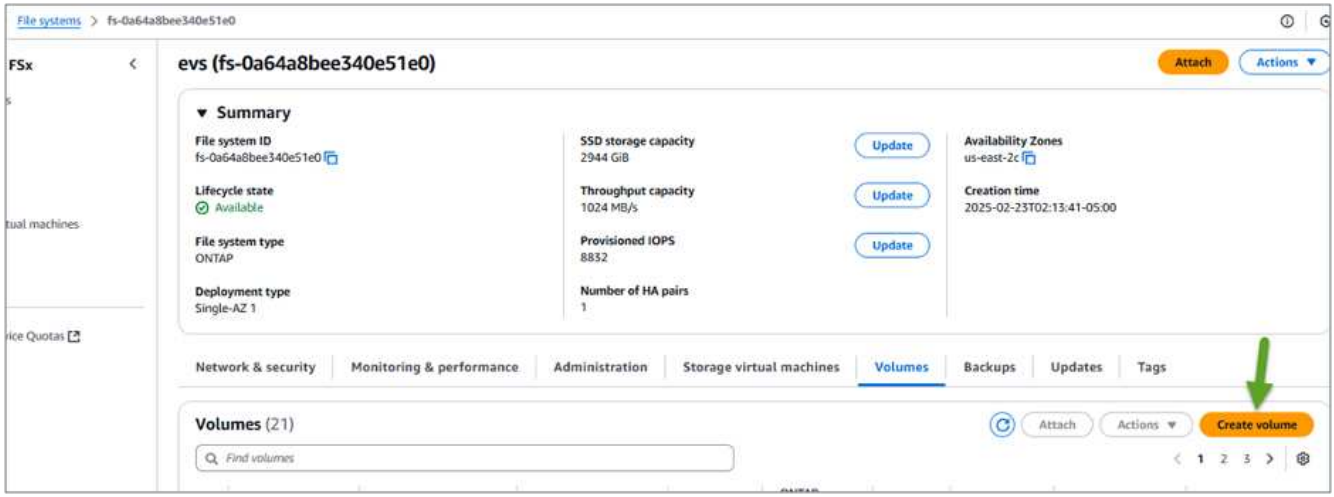


2. 安裝完成後，您將進入儲存適配器畫面。從功能表列中選擇“重新掃描適配器”。記錄 iSCSI 適配器的 IQN：iqn.xxxx。該值稍後將在 LUN 映射步驟中使用。



建立 **FSx for ONTAP**卷

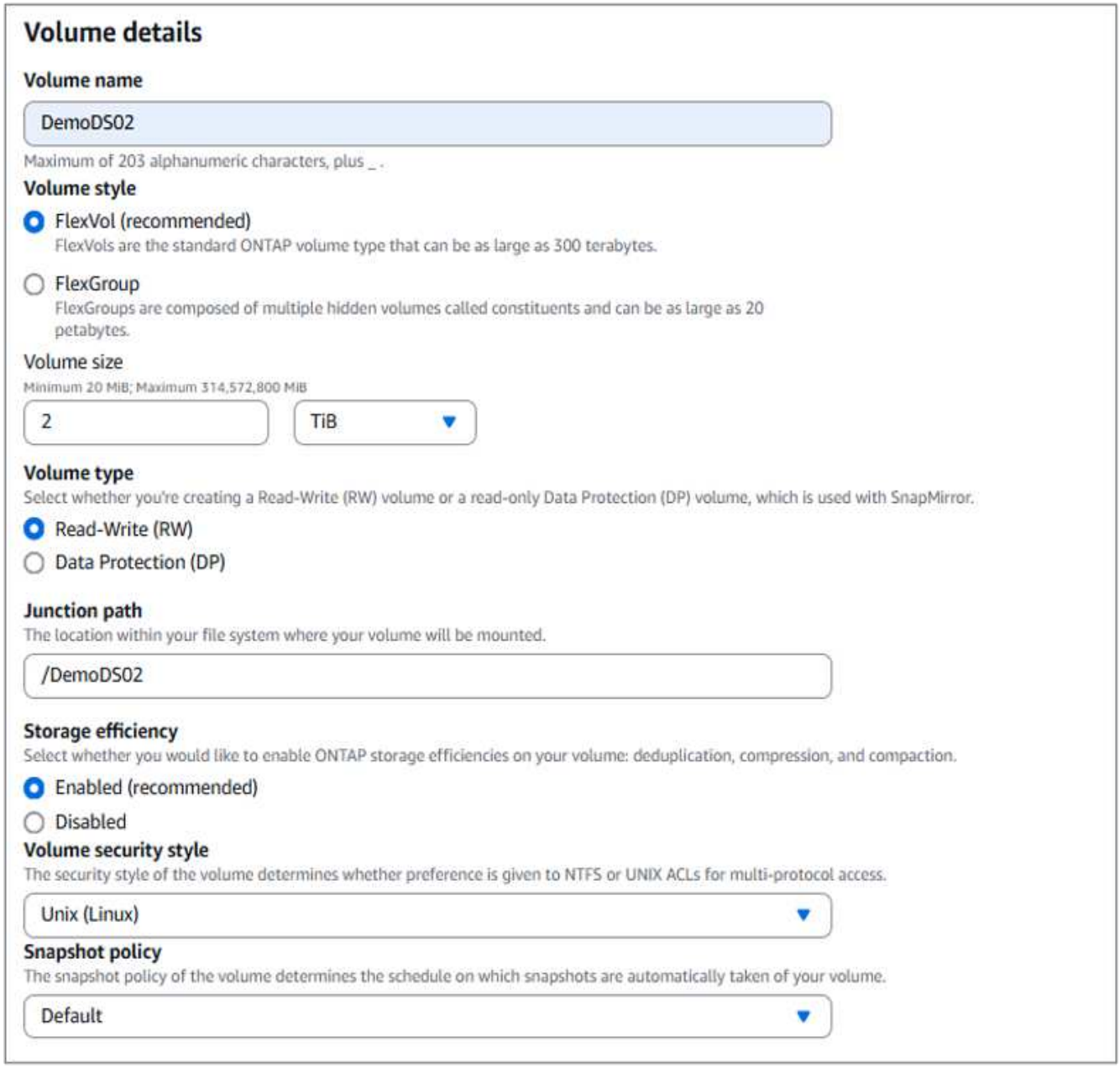
1. 前往 AWS 控制台並進入 FSx for ONTAP檔案系統的頁面，然後按一下「建立磁碟區」。



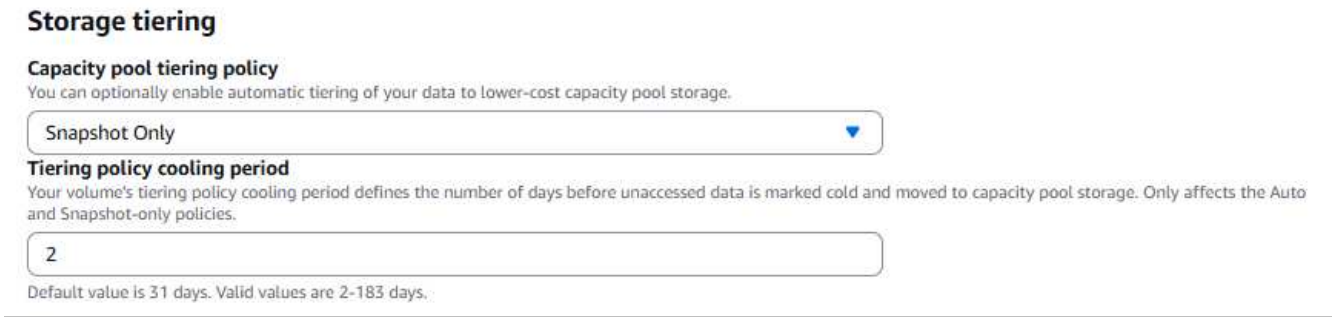
2. 選擇要建立磁碟區的 SVM。



3. 在「卷詳情」頁面，輸入如下圖所示的詳情。完成後，按一下「建立」來設定磁碟區。選擇「已啟用」以開啟ONTAP儲存效率功能（壓縮、重複資料刪除和壓縮）。



4. 對於儲存分層選項，從下拉式選單中選擇“僅快照”並設定分層策略冷卻期。預設值為 31 天，但對於此範例，我們設定了兩天的冷卻期。



5. 建立磁碟區後，使用ONTAP CLI 設定以下值：

環境	配置
數量保證	無（精簡配置）
部分儲備	0%
snap_reserve	0%
自動調整大小	擴大_縮小
儲存效率	已啟用
卷分層策略	僅快照
訪問時間更新（-atime-update）	錯誤的
最小預讀（-min-readahead）	錯誤的
快照策略	沒有任何
LUN 空間預留	已停用
LUN空間分配	已啟用

建立 **LUN**、**igroup** 和映射 **LUN**

在本節中，我們將展示如何建立將在 vSphere 中顯示為磁碟的 LUN。我們還將展示如何建立啟動器群組 (igroup)，它是可以存取 LUN 的啟動器的清單。 igroup 將允許從 vSphere ESXi 主機存取 LUN。最後，我們將展示如何將 igroup 對應到 LUN。

1. 若要存取ONTAP CLI，請透過執行下列命令在 FSx for ONTAP檔案系統或 SVM 的管理連接埠上建立 SSH 會話：

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. 建立 LUN。確保將空間分配和空間預留設定為啟用。該大小應達到卷大小的 90%：

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. 建立 igroup，並新增叢集內所有 ESXi 主機的 IQN。

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. 使用以下程式碼映射 LUN：

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. 檢查 LUN 對應並驗證狀態是否已變更為「已對應」。這是必要的雙重檢查，以確保 LUN 處於映射狀態：

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

從 **SVM** 取得 **iSCSI** 設定信息

1. 運行 iSCSI show 並記錄目標名稱。這將用於 FSx for ONTAP磁碟的 vSphere 發現（注意：此目標名稱對於您的 SVM 是唯一的）：

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. 記錄 iSCSI IP 位址：

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

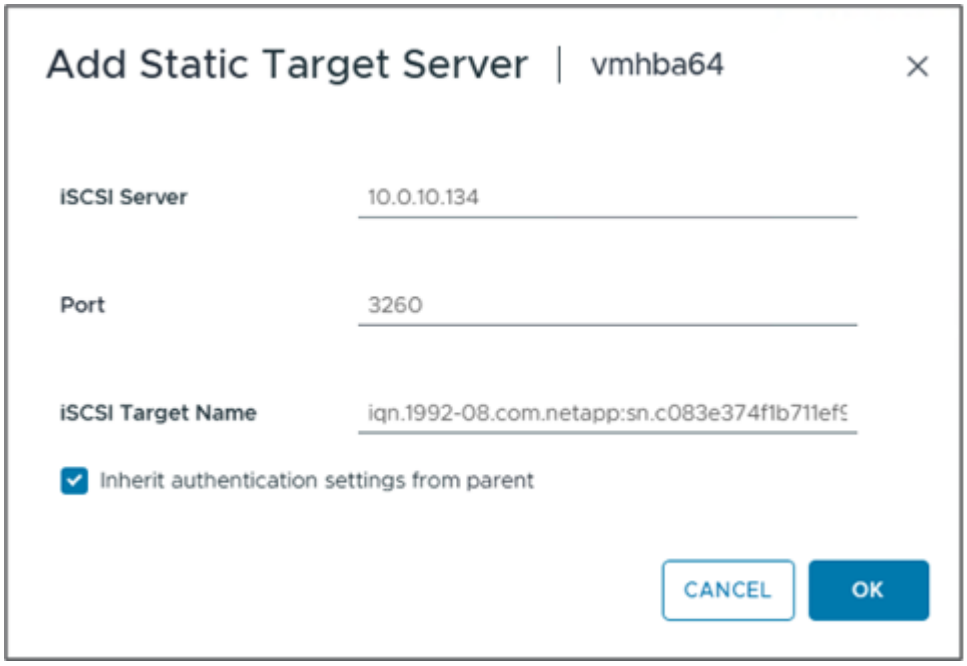
發現 **FSx for ONTAP iSCSI** 伺服器

現在我們已經映射了 LUN，我們可以發現 SVM 的 FSx for ONTAP iSCSI 伺服器。請注意，對於 SDDC 中存在的每個 ESXi 主機，您都需要重複此處列出的步驟。

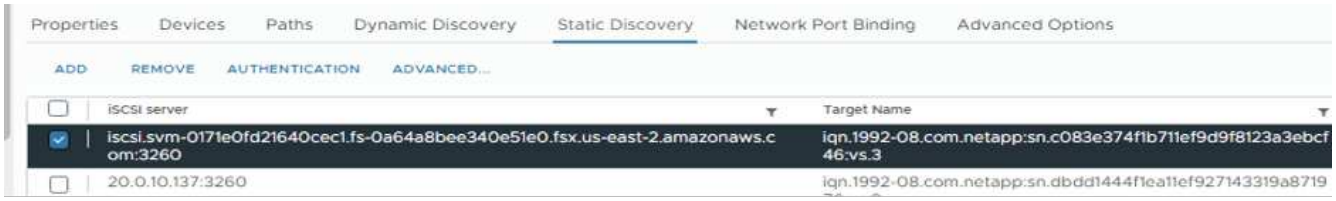
1. 首先，確保連結到 FSx for ONTAP檔案系統（即連接到 ENI 的安全群組）的安全群組允許 iSCSI 連接埠。

   有關 iSCSI 協定連接埠的完整清單以及如何應用它們，請參閱"使用 Amazon VPC 進行檔案系統存取控制"。

2. 在 vSphere Client 中，前往 ESXi 主機 > 儲存適配器 > 靜態發現，然後按一下「新增」。
3. 輸入上面的 iSCSI 伺服器 IP 位址（連接埠為 3260）。 iSCSI 目標名稱是來自 iSCSI show 指令的 IQN。按一下“確定”繼續。



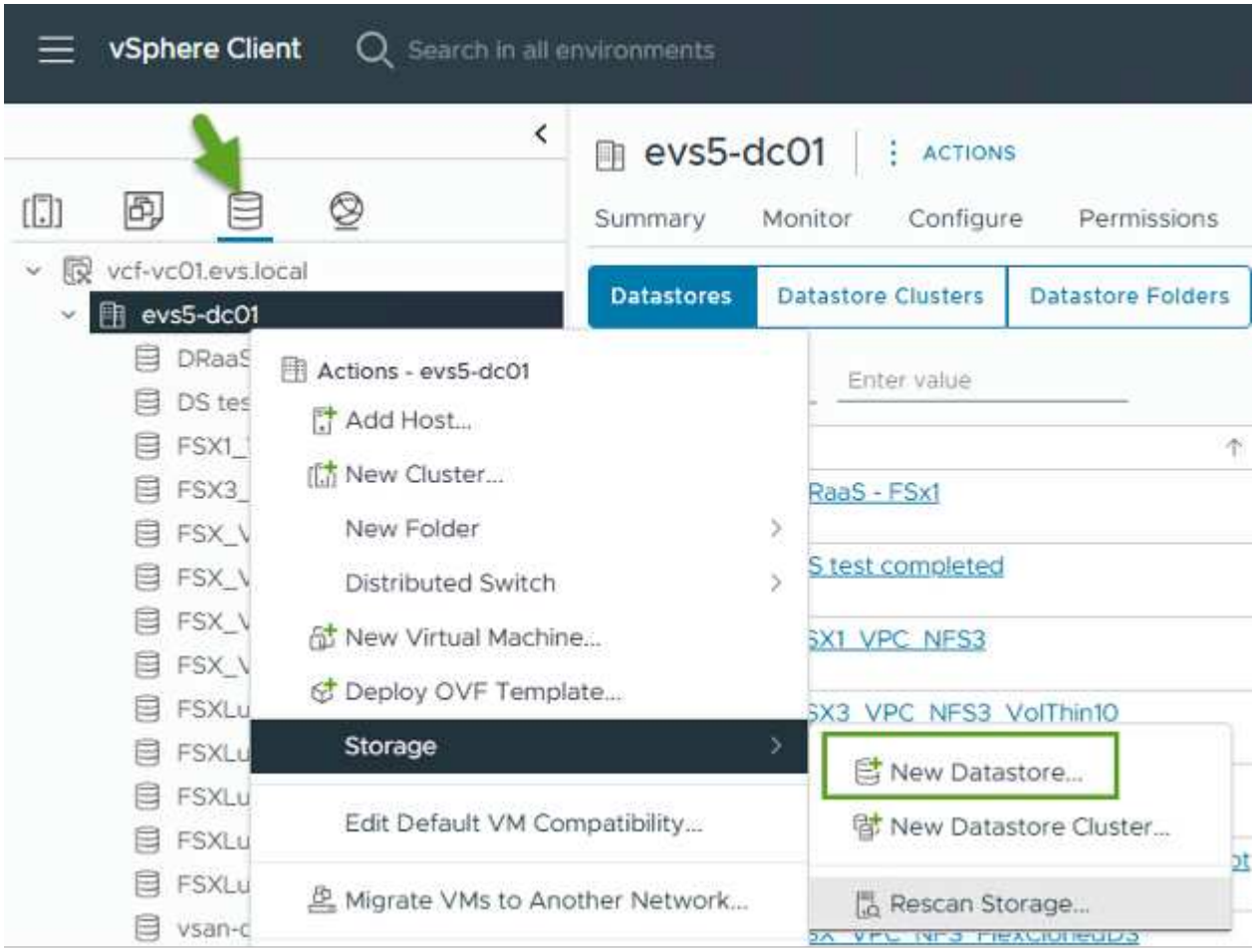
4. 精靈將關閉，您將進入資料儲存靜態發現畫面。在本頁的表格中，您將能夠驗證目標是否已被發現。



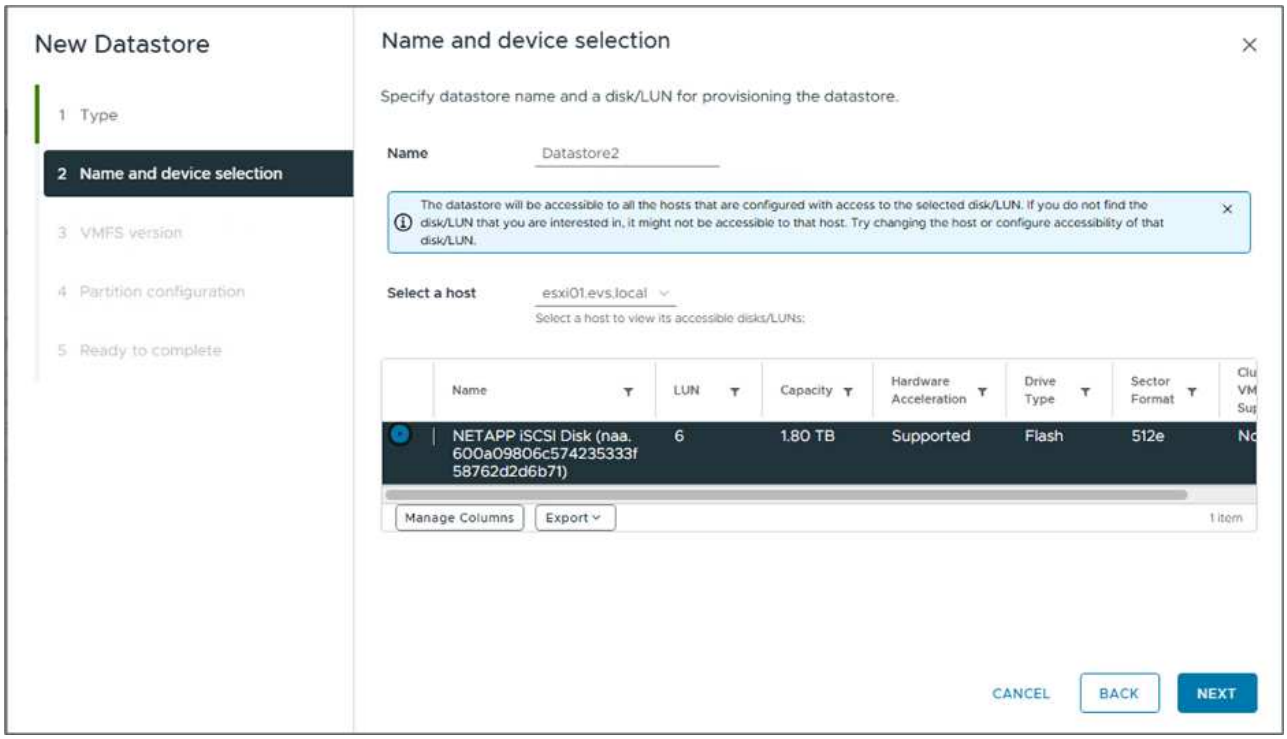
建立 **iSCSI** 資料存儲

現在我們已經發現了 iSCSI 伺服器，我們可以建立一個 iSCSI 資料儲存。

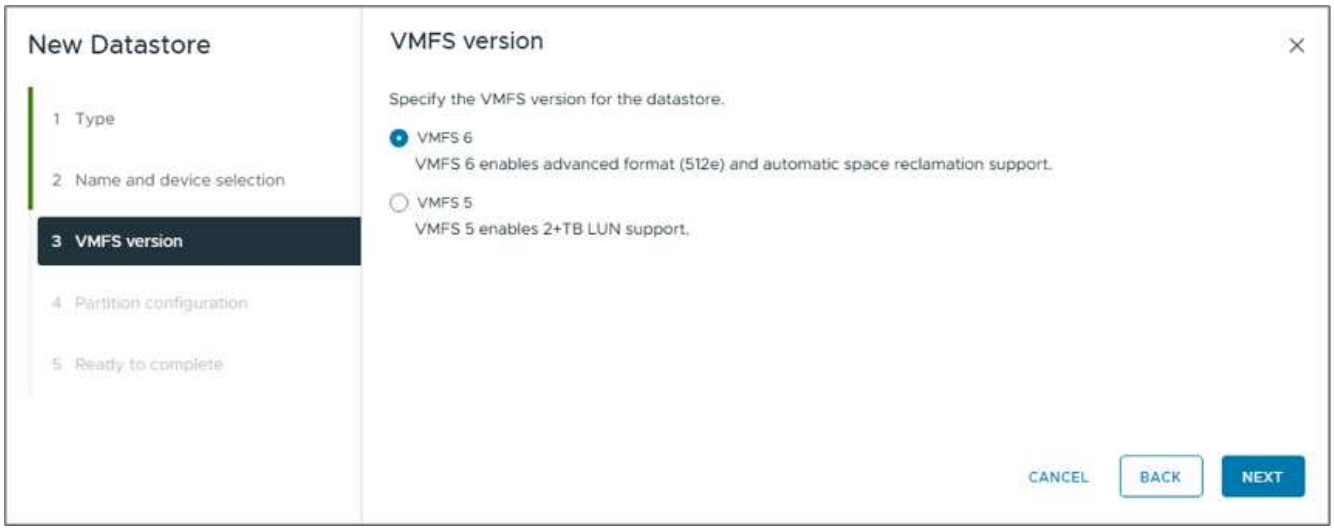
1. 在 vSphere 用戶端中，前往「資料儲存」選項卡，選擇要部署資料儲存的 SDDC。右鍵單擊並選擇儲存圖示（如下圖螢幕截圖中的綠色箭頭所示），然後從下拉式選單中選擇“新資料儲存”：



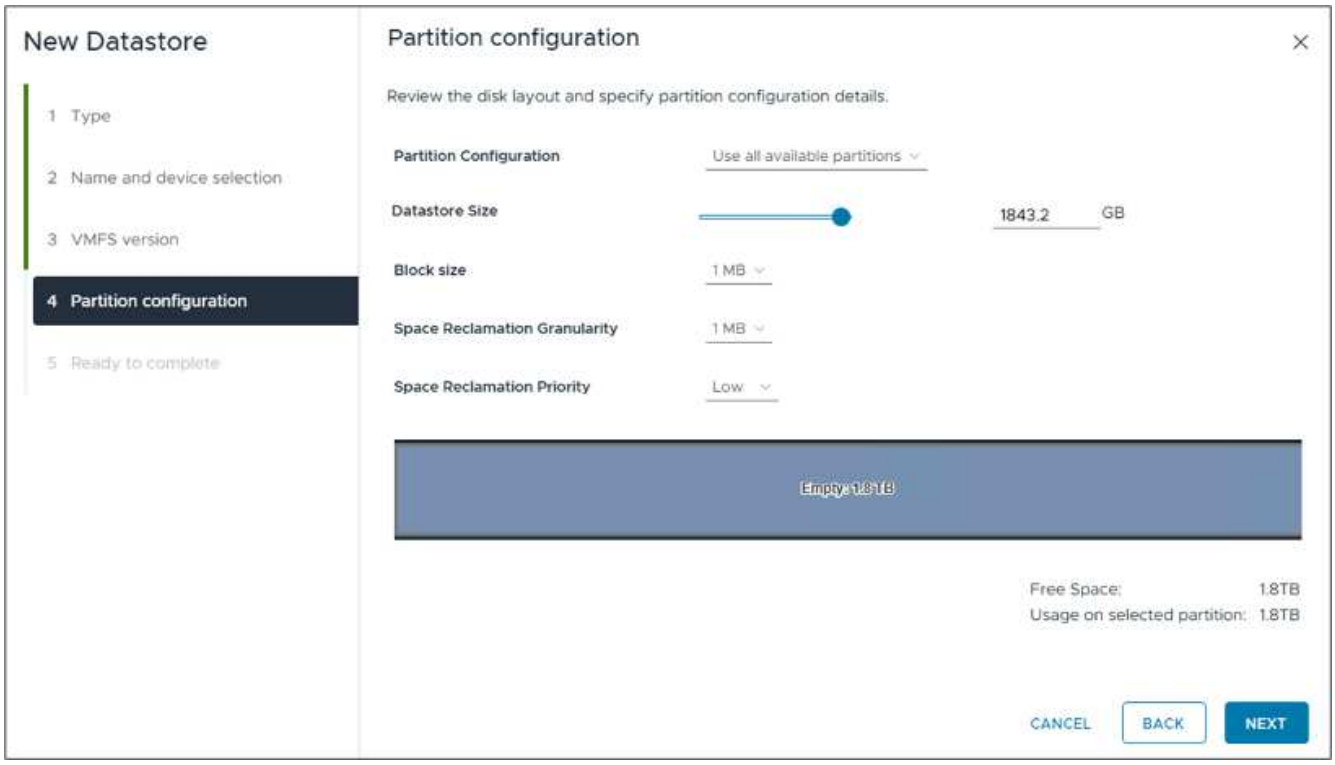
2. 您現在將進入新資料儲存精靈。在「類型」步驟中，選擇 VMFS 選項。
3. 在“名稱和設備選擇”步驟中：
   a. 為您的資料儲存提供一個名稱。
   b. 選擇要連接到資料儲存的 ESXi 主機。
   c. 選擇發現的磁碟（LUN），然後按一下「下一步」。



4. 在「VMFS 版本」步驟中，選擇「VMFS 6」。



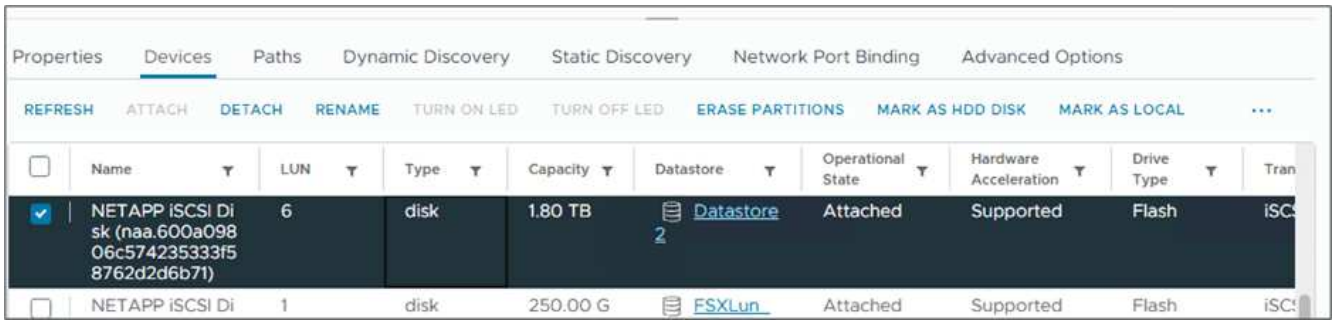
5. 在“分區配置”步驟中，保留預設設置，包括“使用所有可用分區”選項。按一下“下一步”繼續。



6. 在「準備完成」步驟中，確保設定正確。完成後，按一下"完成"以完成設定。



7. 返回「裝置」頁面並驗證資料儲存是否已連線。



結論

本文檔提供如何將 FSx for ONTAP設定為 Amazon EVS 的外部儲存以便與 NFS 和 iSCSI 協定一起使用的說明。

使用 FSx for ONTAP作為 Amazon EVS 的外部儲存可提供明確的營運和業務價值。它透過ONTAP技術提供更好的資料彈性、保護、複製和成本效率，並透過解耦 VMware 超融合架構保持 TCO 最佳化。借助 FSx for ONTAP，Amazon EVS 用戶無需添加計算資源即可擴展存儲，也不會增加成本。這充分發揮了 AWS 雲的彈性和規模潛力。

要了解更多信息，請閱讀亞馬遜新品公告："Amazon EVS 現已與 FSx for ONTAP集成"以及NetApp部落格："Amazon EVS 宣布支援 FSx for ONTAP" 。

保護 **FSx ONTAP** 資料存放區以用於 **EVS**

如何使用 **Amazon Elastic VMware Service** 及 **NetApp SnapCenter Plug-in for VMware** 保護 **Amazon FSx for NetApp ONTAP** 資料存放區

本指南將示範一種簡單的部署方法，用於使用 NetApp SnapCenter® Plug-in for VMware vSphere (SCV) 備份和復原解決方案來保護 FSx for ONTAP Network File System (NFS) 和 iSCSI Amazon EVS 資料儲存區以及相關的 VM。

介紹

基於 Amazon FSx for NetApp ONTAP（FSx for ONTAP）的 Amazon Elastic VMware Service（Amazon EVS）補充資料儲存區為執行對效能要求高的工作負載（例如運用 nConnect、Amazon Virtual Private Cloud（Amazon VPC）對等互連，以及每個資料儲存區掛載使用多個網路連線）和儲存密集型工作負載提供了絕佳的解決方案。

此功能使客戶能夠克服虛擬儲存區域網路 (vSAN) 提供的本機實例儲存的限制，實現儲存與運算資源的獨立擴展，並降低整體擁有成本。除了整體擁有成本 (TCO) 優勢之外，FSx for ONTAP 還為 Amazon EVS 提供企業級功能，這些功能是內部部署 ONTAP® 客戶所熟悉的，有助於優化和簡化部署。使用 FSx for ONTAP 可以存取 NetApp® Snapshot™、SnapMirror® 和 SnapVault® 技術，這些技術支援虛擬機器 (VM)、資料儲存區和虛擬機器磁碟 (VMDK) 的備份和還原作業。其中一項關鍵功能是基於 Snapshot 的保護。

概況

隨著企業規模的擴大和環境的整合，保護工作負載及其底層儲存的需求變得日益重要。SCV 可用於直接從 Amazon EVS vSphere 客戶端備份資料儲存和虛擬機器。

本指南的目的

本指南提供如何使用 SCV 保護 Amazon EVS 的 FSx for ONTAP 資料存放區的說明。指南中也提供了保護 VM 和資料庫的範例場景以及還原方法。

對象

本教學適用於熟悉 VMware vSphere、Amazon EVS、AWS 控制台和 FSx for ONTAP 的雲端架構師和雲端管理員。

部署和配置的高階步驟

以下是部署和配置 SCV 以保護 Amazon FSx for NetApp ONTAP 上的虛擬機器和資料儲存區的高階步驟：

1. 下載 SCV Open Virtual Appliance（OVA）。
2. 使用 vSphere Client 憑證登入 Amazon EVS。
3. 部署 Open Virtualization Format（OVF）範本以啟動 VMware 部署精靈。
4. 若要存取該插件，請從選單中選擇 SnapCenter Plug-in for VMware。
5. 新增儲存設備。
6. 建立備份原則。
7. 建立資源群組。
8. 備份資源群組。
9. 還原整個虛擬機器、特定虛擬磁碟或客體檔案。

SnapCenter Plug-in for VMware 的設定程序

本節介紹如何設定 SnapCenter Plug-in for VMware 的步驟。

先決條件

開始之前需要滿足以下先決條件：

1. 在部署 OVA 時註冊 vCenter 伺服器時，請指定 vCenter 的完全限定網域名稱（FQDN）或 IP 位址。
2. 對於 vCenter 憑證，請使用具有最低所需權限的帳戶
3. 為 vCenter Server 存取開放防火牆連接埠。
4. 更新執行 FSx for ONTAP 的 Amazon VPC 安全群組，以允許 SCV 存取 FSx for ONTAP。

SCV 可免費使用。

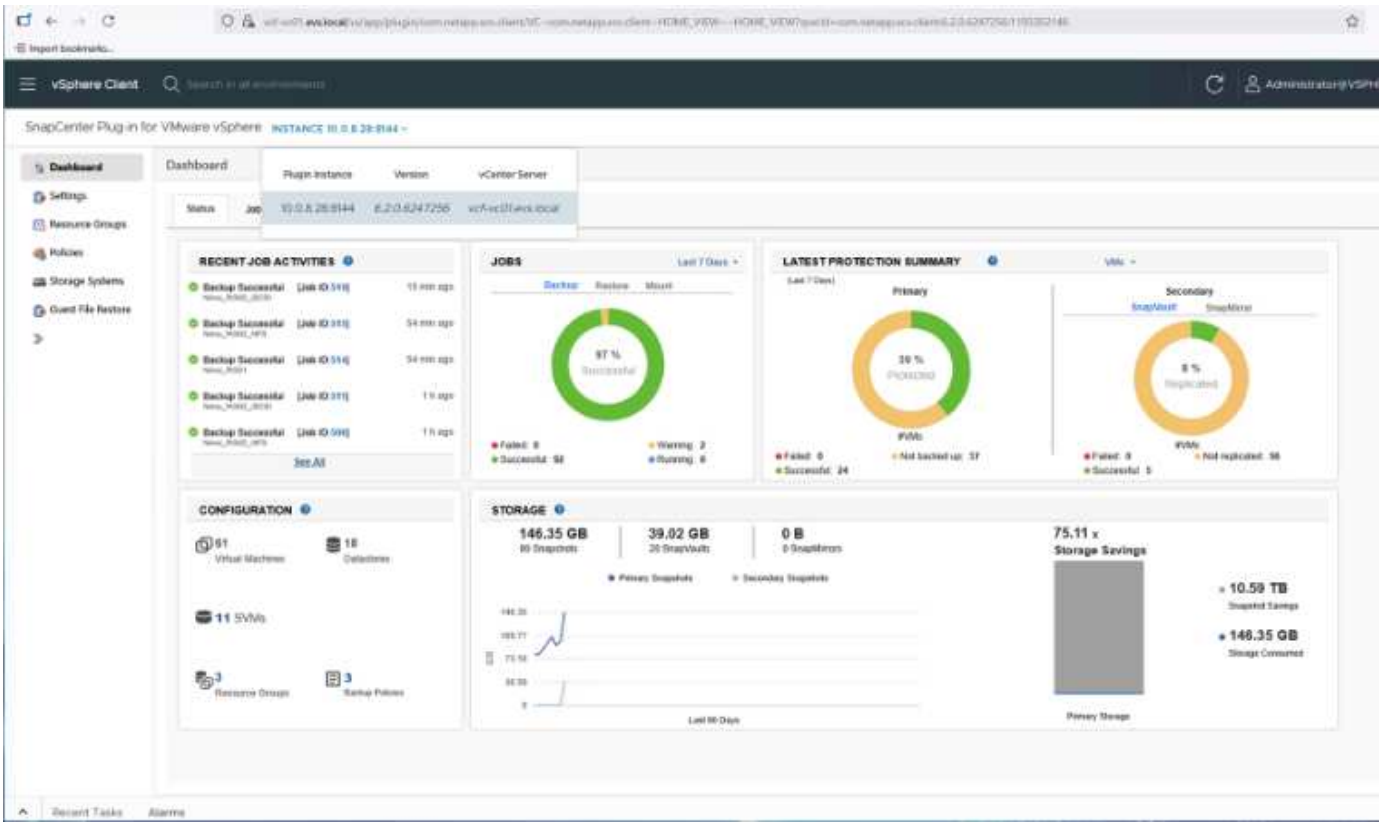
設定 SnapCenter Plug-in for VMware

為了保護 VM 及其託管的基於 NFS/iSCSI 的資料存儲，必須部署 SCV。這是一個簡單的 OVF 匯入。

部署步驟如下：

1. 從 "NetApp 支援網站" 下載 OVA。

2. 登入 Amazon EVS vCenter。
3. 在 vCenter 中，以滑鼠右鍵按一下任何目錄物件（例如資料中心、資料夾、叢集或主機），然後選取「部署 OVF 範本」。
4. 選擇正確的設定，包括儲存、區段，並自訂範本以更新 vCenter 及其認證資料、建立 SCV 認證資料和 IP 詳細資料。檢閱後，選取「完成」。
5. 等待 OVF 匯入和部署任務完成。
6. 成功部署 SCV 後，將在 vCenter 內註冊。
7. 若要存取插件，請導覽至 vCenter Web 用戶端頁面的左側邊欄，選擇「SnapCenter Plug-in for VMware」。



SnapCenter Plug-in for VMware 的組態程序

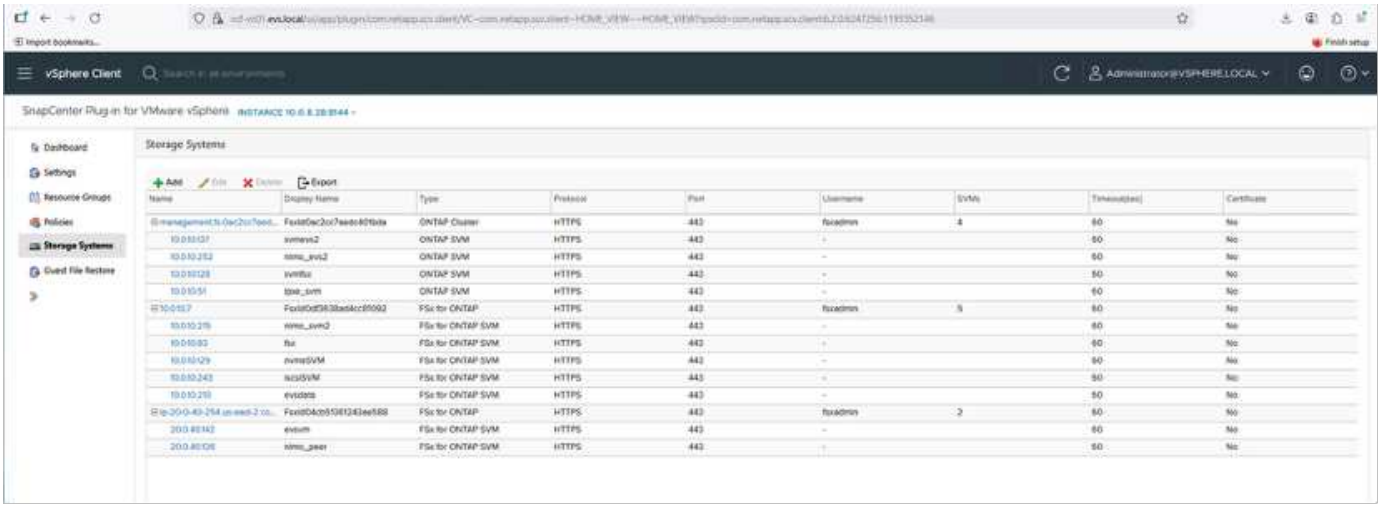
本節介紹配置 SnapCenter Plug-in for VMware vSphere 的步驟。後續章節將詳細介紹如何新增儲存空間、建立備份原則以及如何建立資源群組。

新增儲存系統

使用 SVC 保護工作負載的下一步是新增 "儲存系統"。新增儲存後，SCV 可以偵測和管理 vCenter 內的備份和還原作業。將 FSx for NetApp ONTAP 管理端點或儲存虛擬機器（SVM）管理端點 IP 作為儲存系統，以啟用 VM 備份和還原。

1. 從 EVS vCenter 的左側導覽選單中，選擇「SnapCenter Plug-in for VMware」。
2. 選擇「Storage System」。
3. 選擇「新增」以新增 FSx for ONTAP 詳細資料。

4. 使用「憑證作為驗證」方法，並輸入 FSxadmin 作為使用者名稱和密碼。然後選擇「新增」以儲存設定。



新增檔案系統時，所有 SVM 都會自動新增。

如果 SCV 版本為 6.2 、請前往 "SCV 支援頁面" 並下載 SCV 6.2P1 版本。

建立備份原則

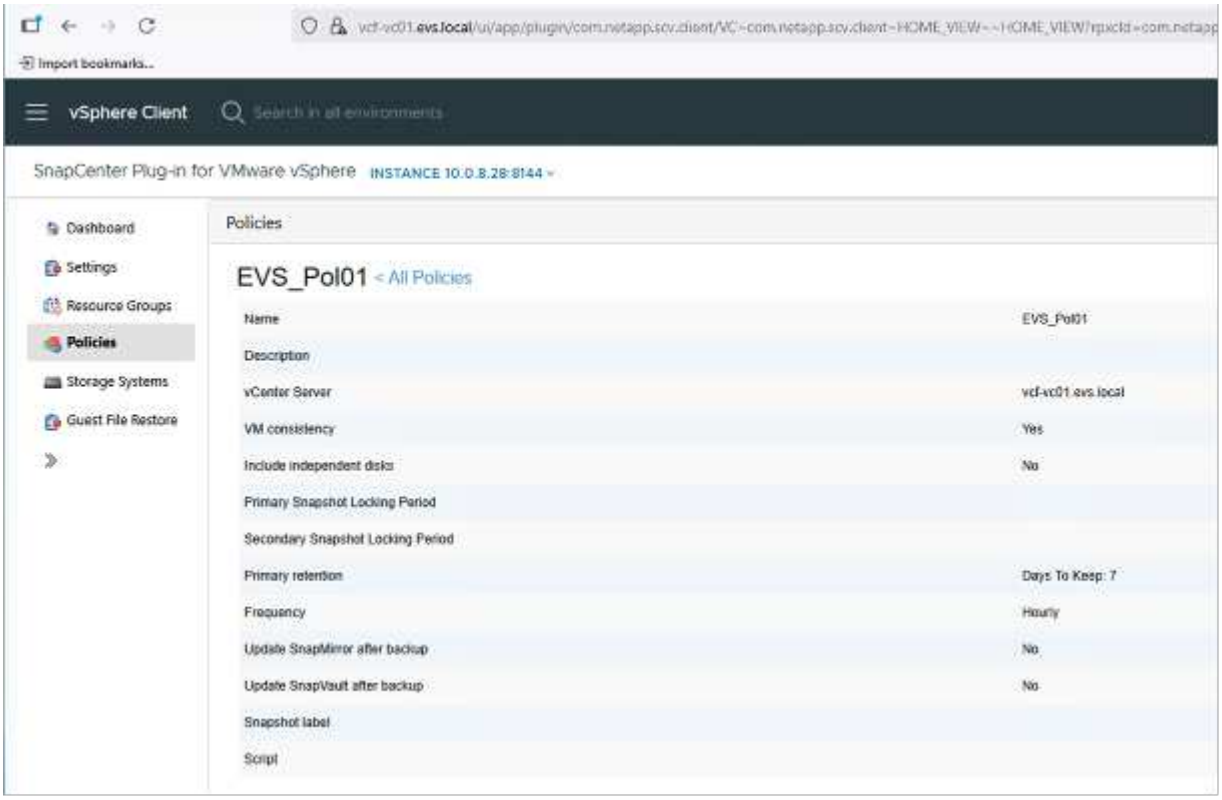
一個完善的備份策略應明確備份排程、待備份資料以及備份保留期限等關鍵因素。可以按小時或按天安排 Snapshot 複本，以保護整個資料存放區。這種備份排程方式不僅可以保護資料存放區，還支援對這些資料存放區中包含的 VM 和 VMDK 進行備份和還原作業。

在啟動 VM 和資料存放區的備份之前，請建立"備份原則"和資源群組。備份原則會指定備份排程和保留設定等參數。

以下是建立備份原則的步驟：

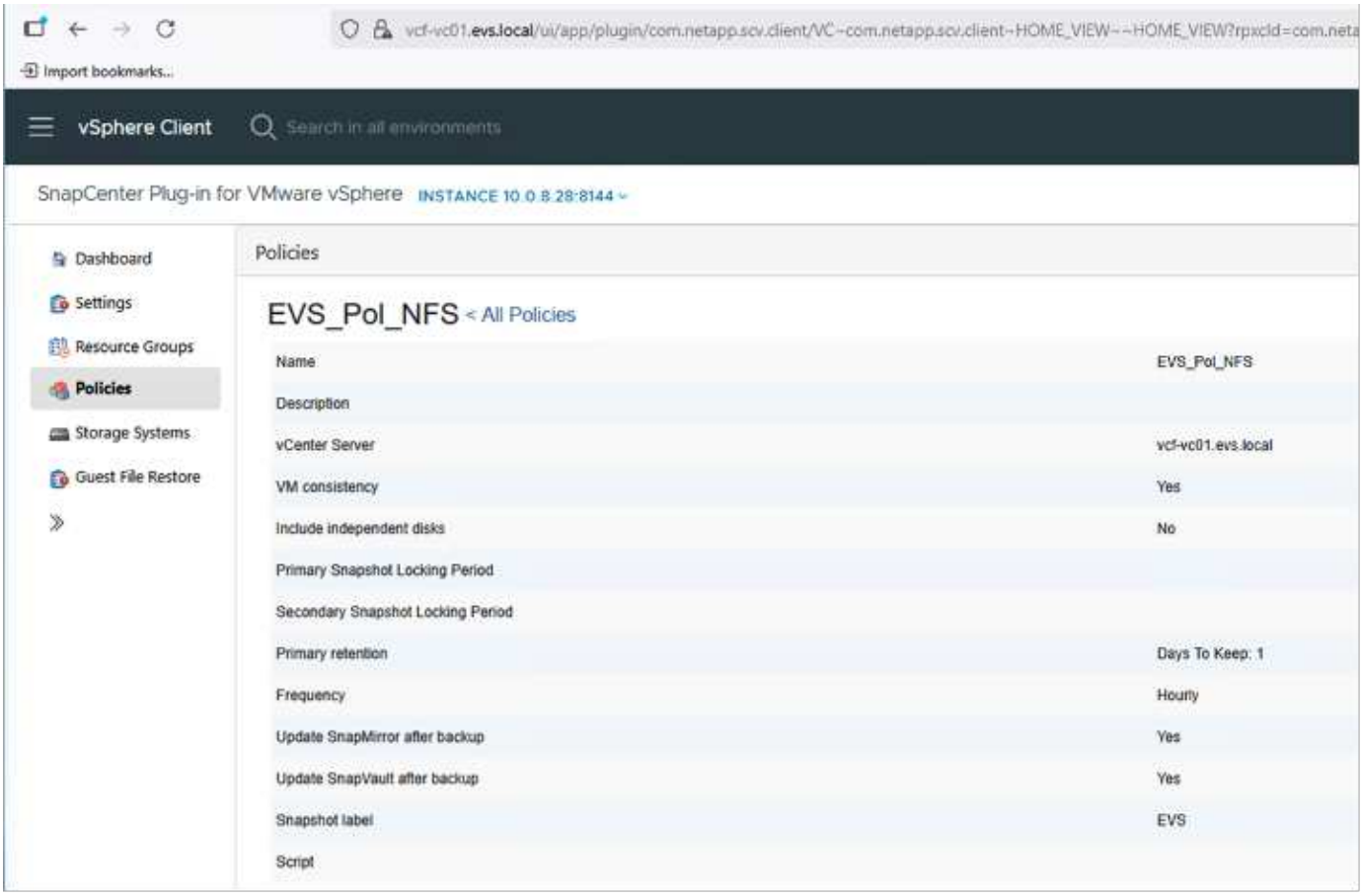
1. 前往 SCV 中的左側導覽選單，然後選取「原則」。
2. 在「策略」頁面上，選取「建立」以啟動精靈。
3. 在「新備份策略」頁面上，輸入策略名稱。
4. 指定保留期限、備份頻率和複寫設定。
5. 選取「鎖定週期」核取方塊以啟用 Snapshot 鎖定。您可以選擇主要和次要 Snapshot 鎖定週期，單位可以是天 / 月 / 年。

無論 SnapMirror 策略中定義的保留值為何，輔助 Snapshot 複本都會保持完整，直到指定的輔助 Snapshot 鎖定期到期為止。



若要啟用 VM 一致性備份，必須安裝並執行 VMware Tools。勾選「VM 一致性」複選框後，VM 會先進入靜默狀態，然後 VMware 執行 VM 一致性快照（不含記憶體），接著 SCV 執行備份作業，最後還原 VM 運作。

若要將 Snapshot 複本複寫到次要鏡射或資料保險箱檔案系統，必須事先設定關係。



建立原則後、下一步是建立資源群組、以定義應備份的適當 NFS 或 iSCSI 資料存放區和 VM 。

建立資源群組

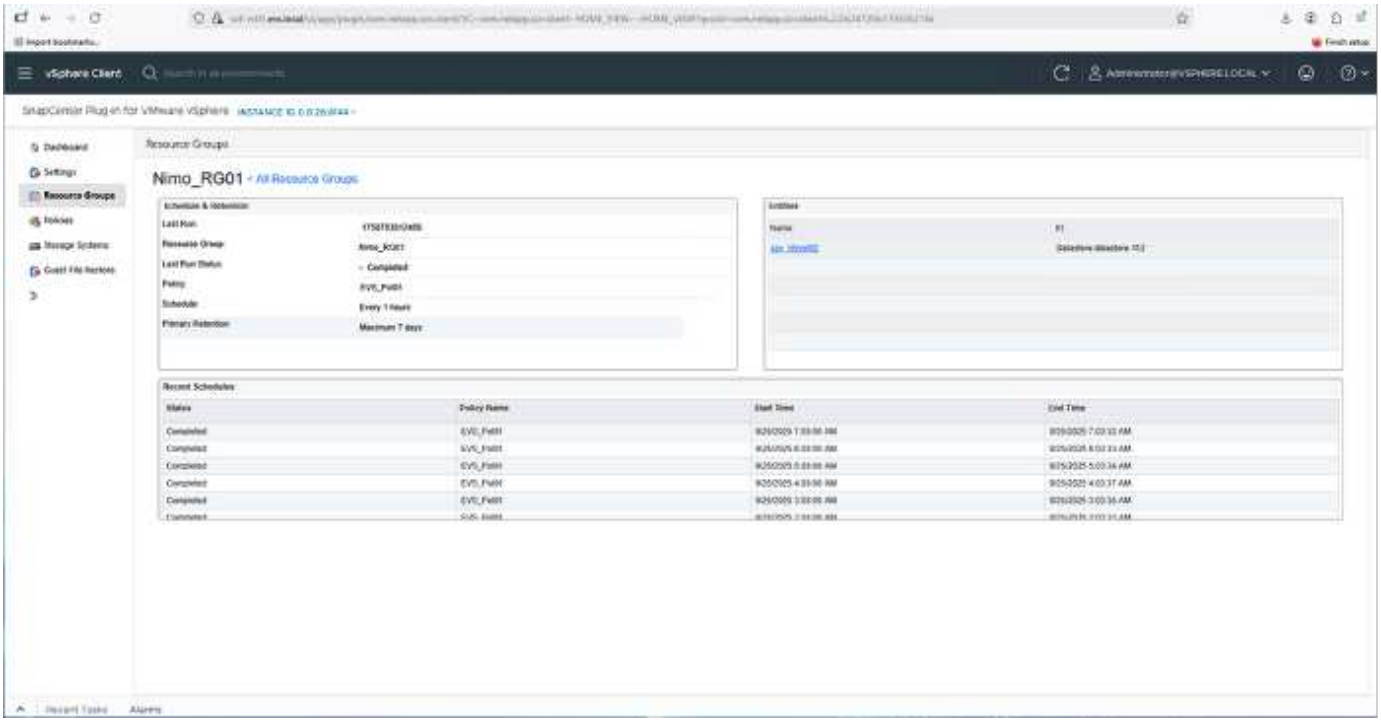
資源群組用作需要保護的 VM 和資料存放區的容器。可以隨時在資源群組中新增或移除資源，從而靈活地管理備份組態。

您可以使用以下步驟建立 "資源群組"：

1. 前往 SCV 左側導覽窗格，然後選擇「Resource Groups」。
2. 在「資源群組」頁面上，選取「建立」以啟動資源群組建立精靈。

> 建立資源群組的另一個選項是選取個別 VM 或資料存放區，並建立僅包含該資源的資源群組。

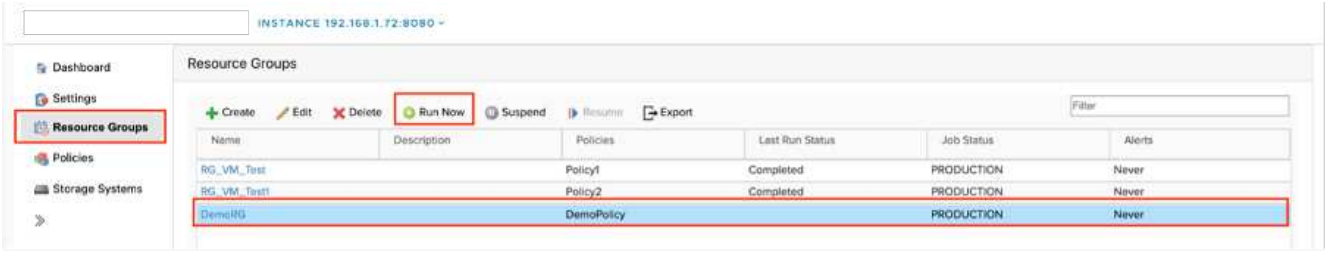
3. 在「資源」頁面上、選擇範圍（ VM 或資料存放區）和資料中心。
4. 在「跨磁碟」頁面上、選擇「跨多個資料儲存區的具有多個 VMDK 的虛擬機器」選項。
5. 接下來、建立備份原則的關聯。選取現有原則或建立新的備份原則。
6. 在「排程」頁面上，為每個選定的原則設定備份排程。
7. 完成相應選擇後，選擇「完成」。這將建立一個新的資源群組並將其新增至資源群組清單。



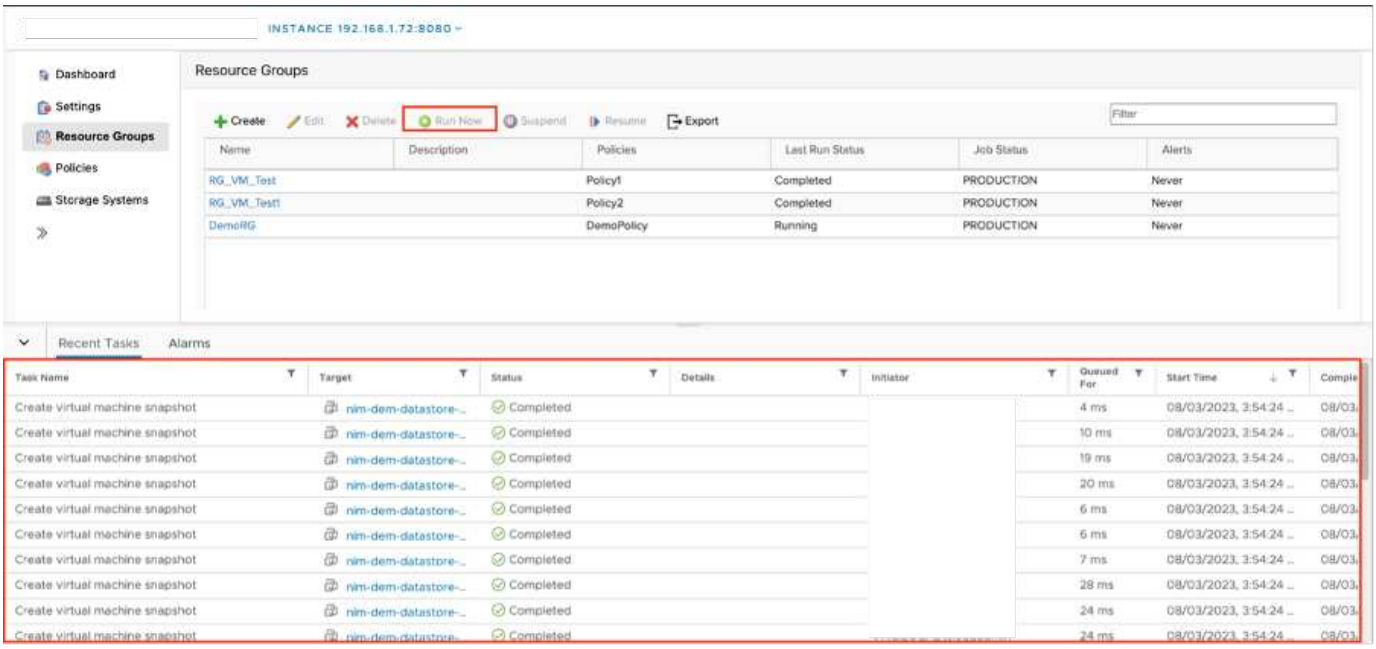
備份資源群組

備份作業會在資源群組內定義的所有資源上執行。如果資源群組已附加原則並設定了排程，則備份會根據排程自動進行。

1. 在 vCenter Web 用戶端頁面的左側導覽列中，選擇「SnapCenter Plug-in for VMware」，然後選擇「資源群組」。
2. 在「資源群組」頁面中，找到指定的資源群組，然後選取「立即執行」以啟動手動備份。



3. 如果資源群組配置了多個原則，請在「立即備份」對話方塊中選擇備份作業的原則。
4. 選擇「OK」以啟動備份。

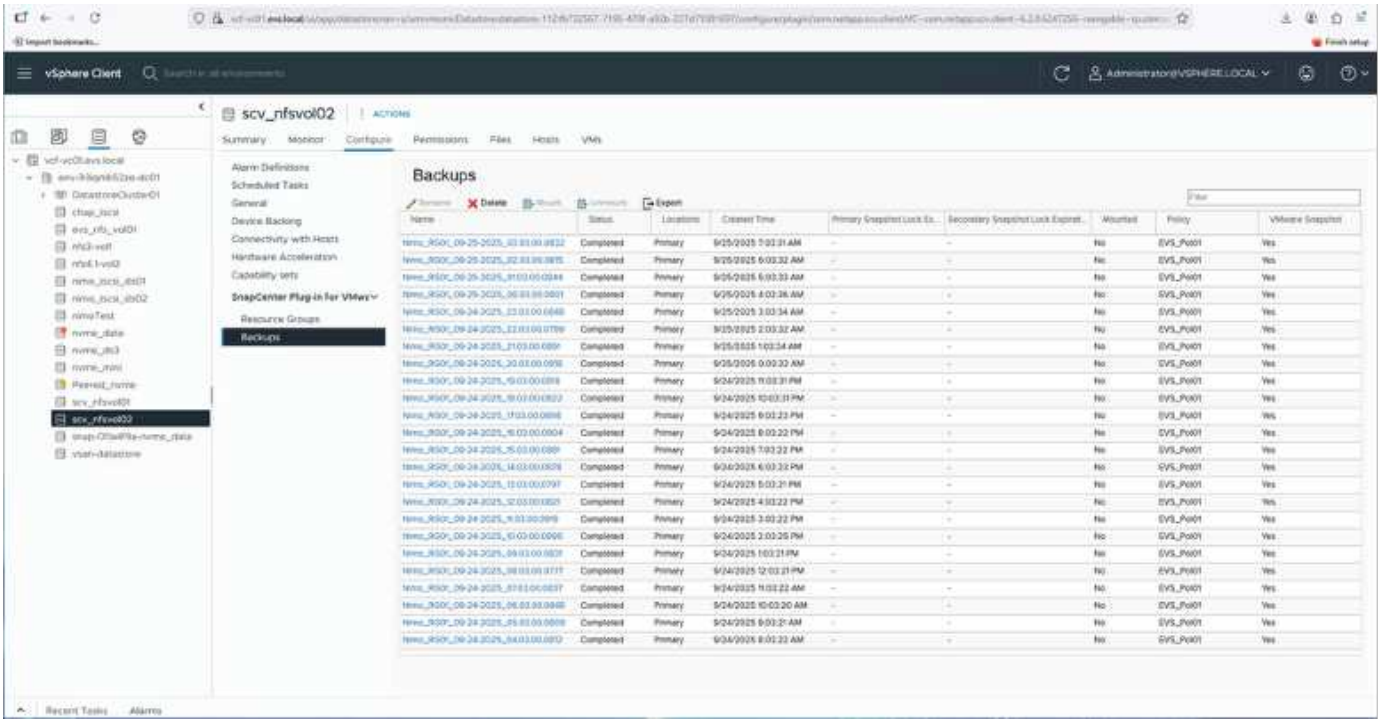


您可以透過選擇視窗底部的「最近任務」來監控操作進度，或者，要了解更多詳細資訊，請在儀表板上選擇「作業監控」。

建立備份原則、設定資源群組和執行備份作業的程序在不同的儲存傳輸協定（包括 NFS 和 iSCSI ）之間是一致的。

備份會根據原則中定義的排程執行。

備份完成後，可以透過從下拉清單中選擇「SnapCenter Plug-in for VMware vSphere」，然後選擇「還原」，在資料儲存層級或單一虛擬機器層級查看備份。



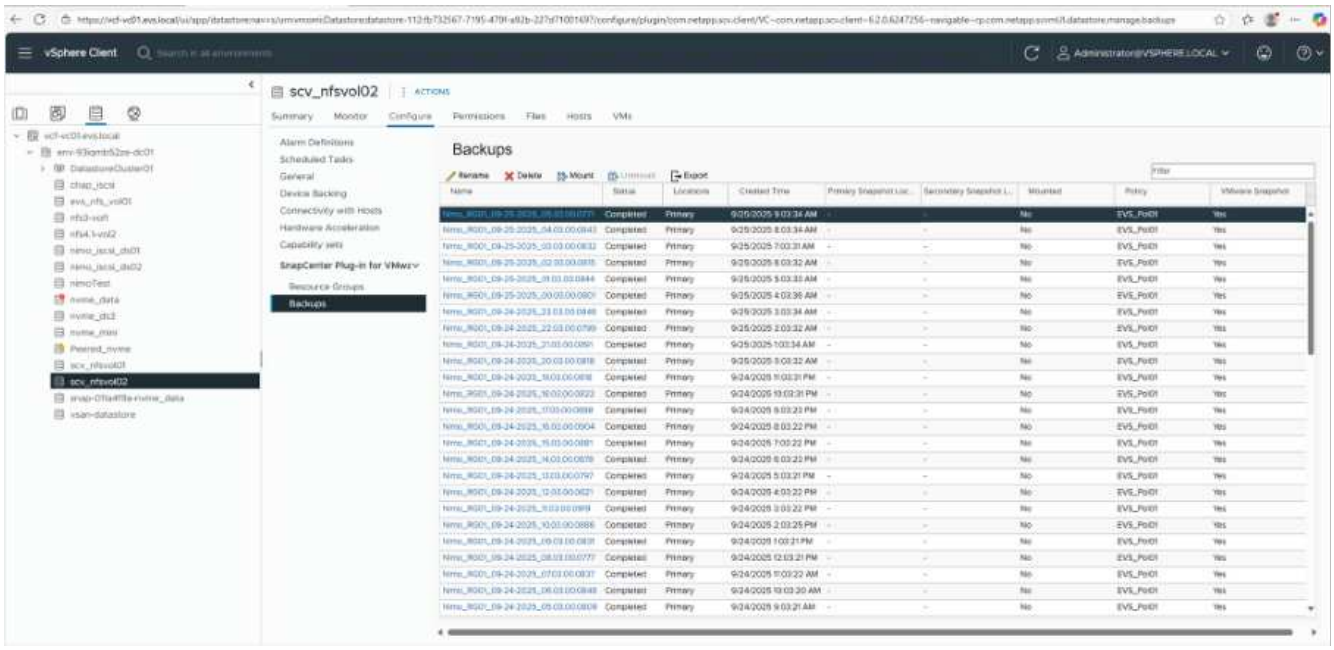
受 **SnapCenter Plug-in for VMware** 保護的虛擬機器的還原程序

本節介紹從備份還原 VM 的步驟。SCV 可用於還原 vCenter 內的 VM，允許將其還原到原始 ESXi 主機上的原始資料存放區（覆寫現有內容）、從備份副本還原已刪除或重新命名的 VM、還原到原始 ESXi 主機上的不同資料存放區、還原到由同一 vCenter 管理的不同 ESXi 主機上的原始資料存放區，或還原到同一 vCenter 環境中另一個 ESXi 主機上的不同資料存放區。

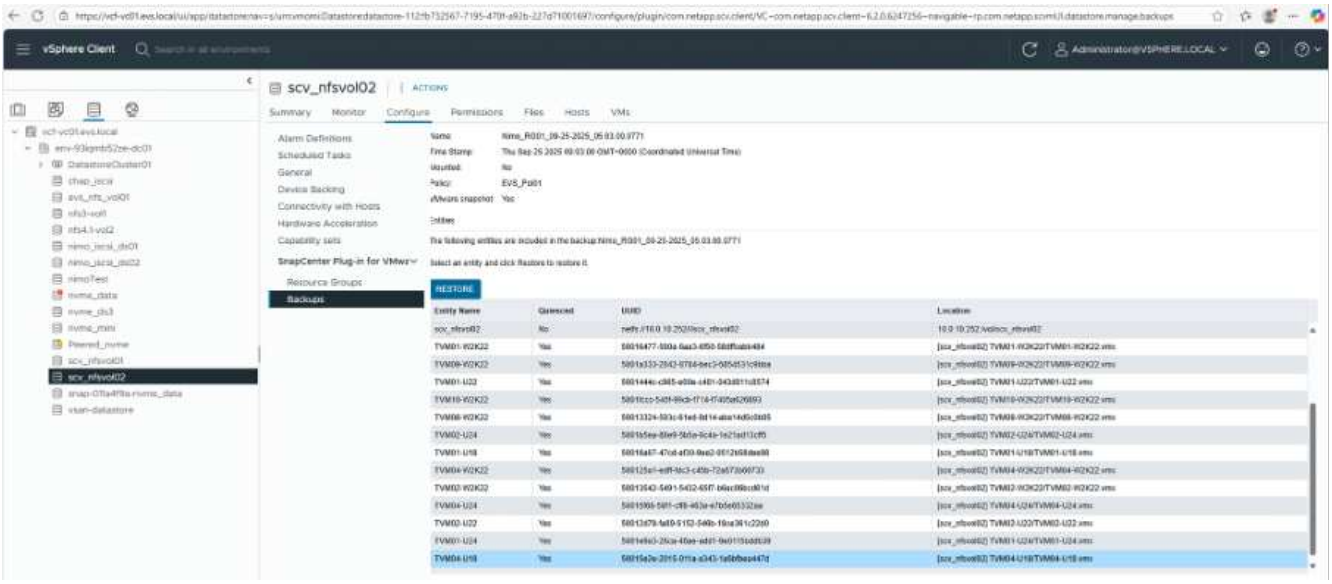
執行還原作業的步驟

若要執行還原作業，請依照下列步驟操作：

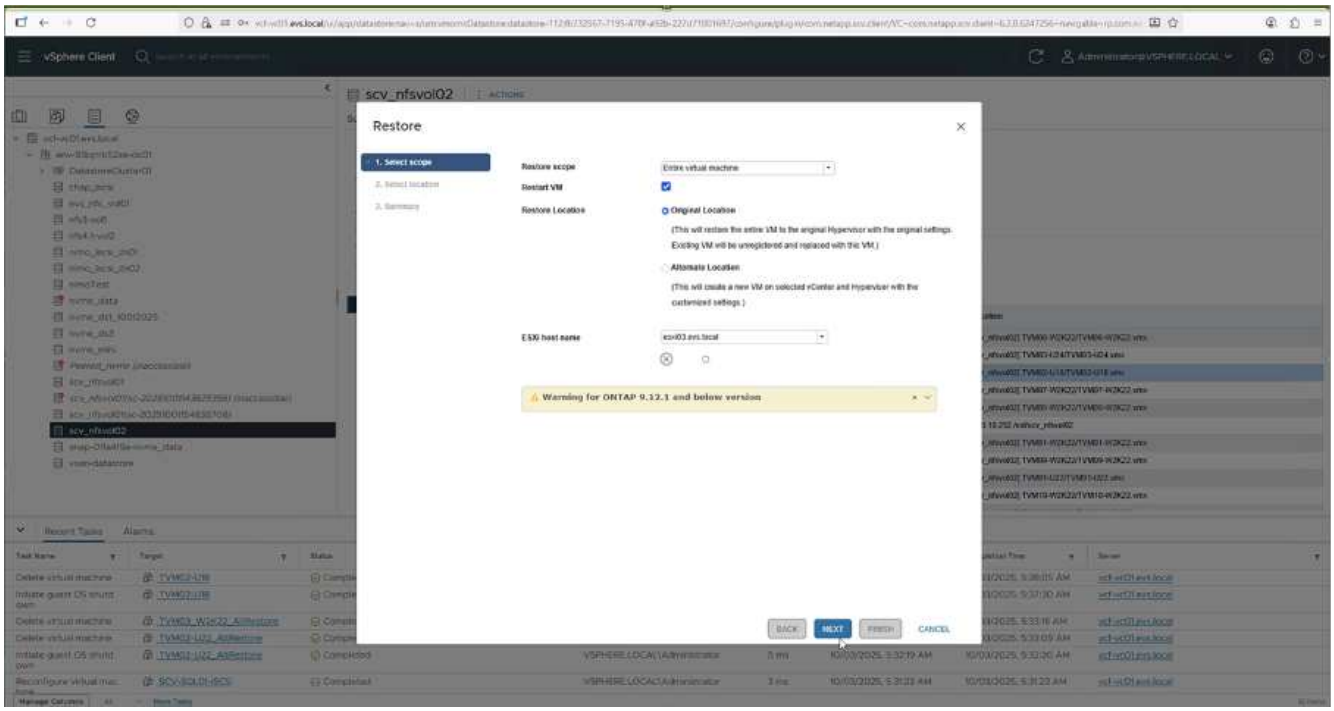
1. 在 EVS vSphere Web 用戶端 GUI 中，前往「清單 > 資料儲存區」，然後選擇所需的資料儲存區。接下來，導覽至「SnapCenter Plug-in for VMware vSphere」部分下的「設定 > 備份」。



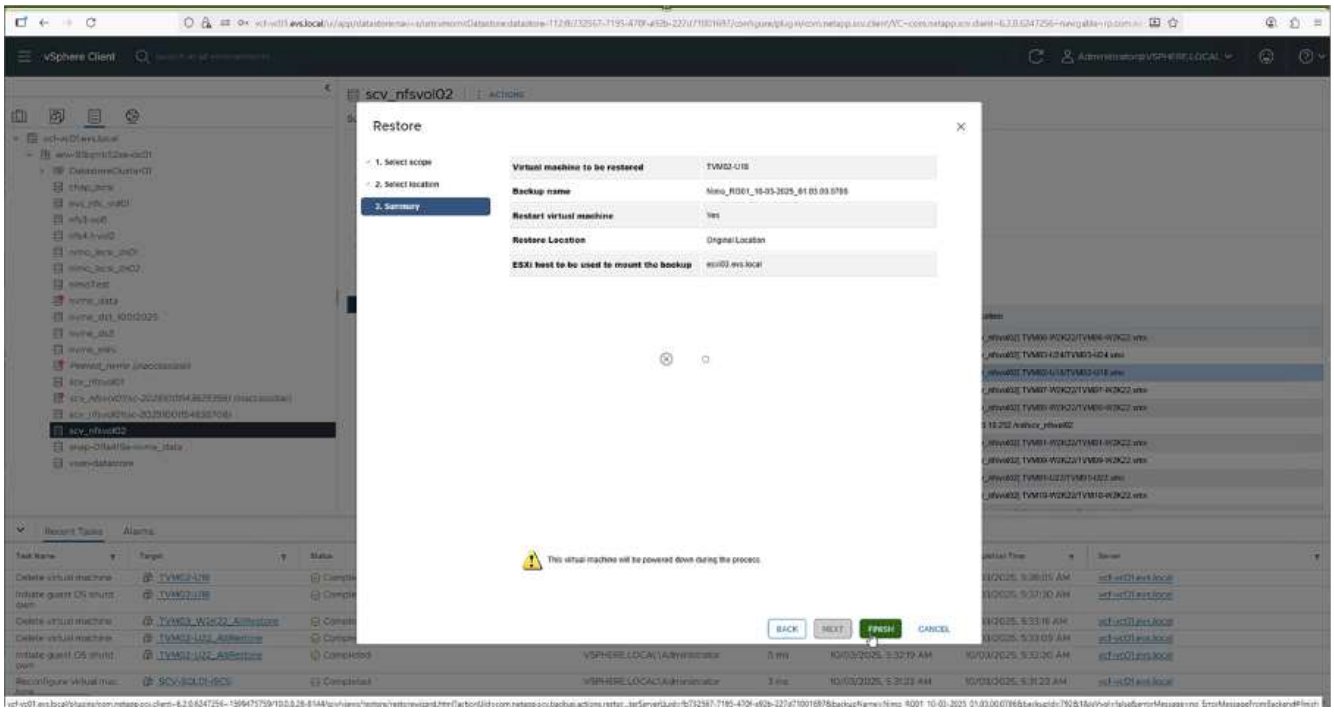
2. 雙擊備份檔案即可查看該備份中包含的所有 VM。在清單中找到要還原的 VM，然後選擇「還原」。



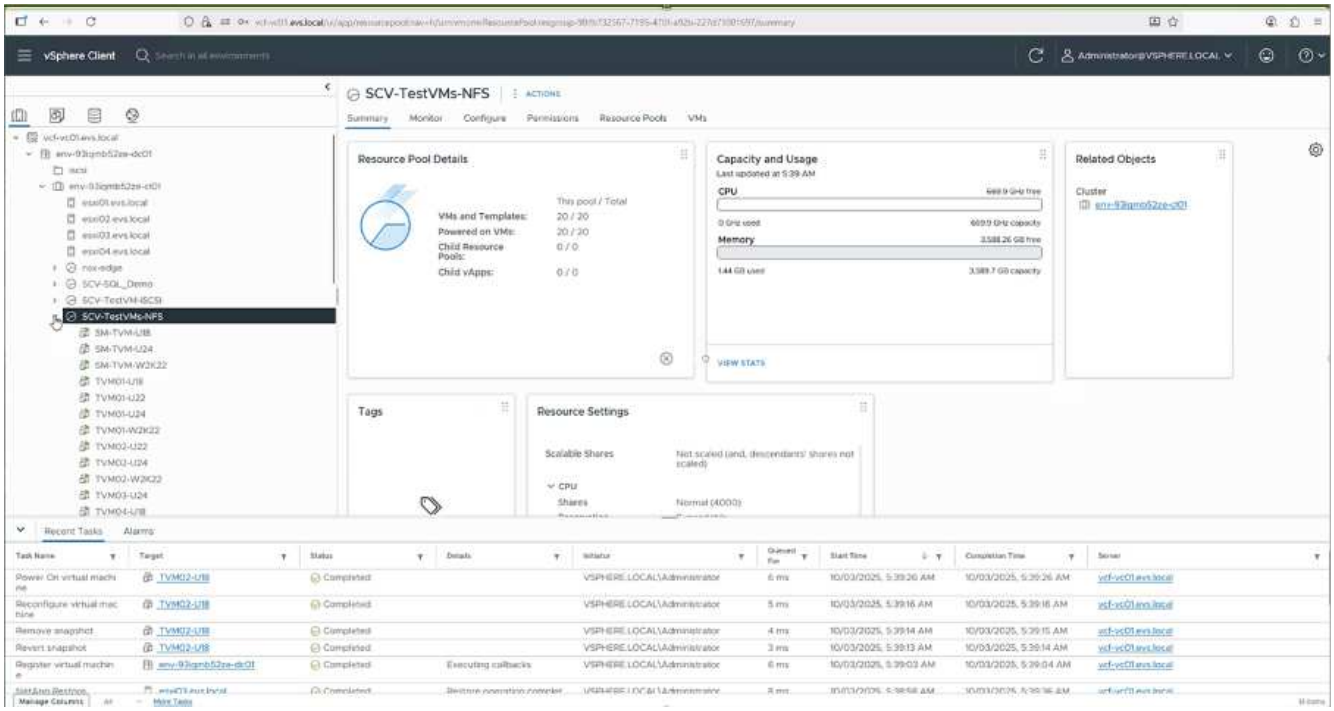
3. 在「選擇範圍」頁面上，在「還原範圍」欄位中選擇「整個虛擬機器」，然後選擇「還原位置」，並輸入備份應掛載的目標 ESXi 資訊。
4. 如果虛擬機需要在還原作業後開啟電源，請啟用「重新啟動 VM」核取方塊。
5. 在「選擇位置」頁面上，選擇主要位置。



6. 檢閱「摘要」頁面，然後選取「完成」。



7. 在螢幕底部選擇 "Recent Tasks"，即可監控操作進度。



雖然 VM 已還原，但不會自動新增至先前的資源群組。如果您想要保護這些 VM ，請手動將其新增至適當的資源群組。

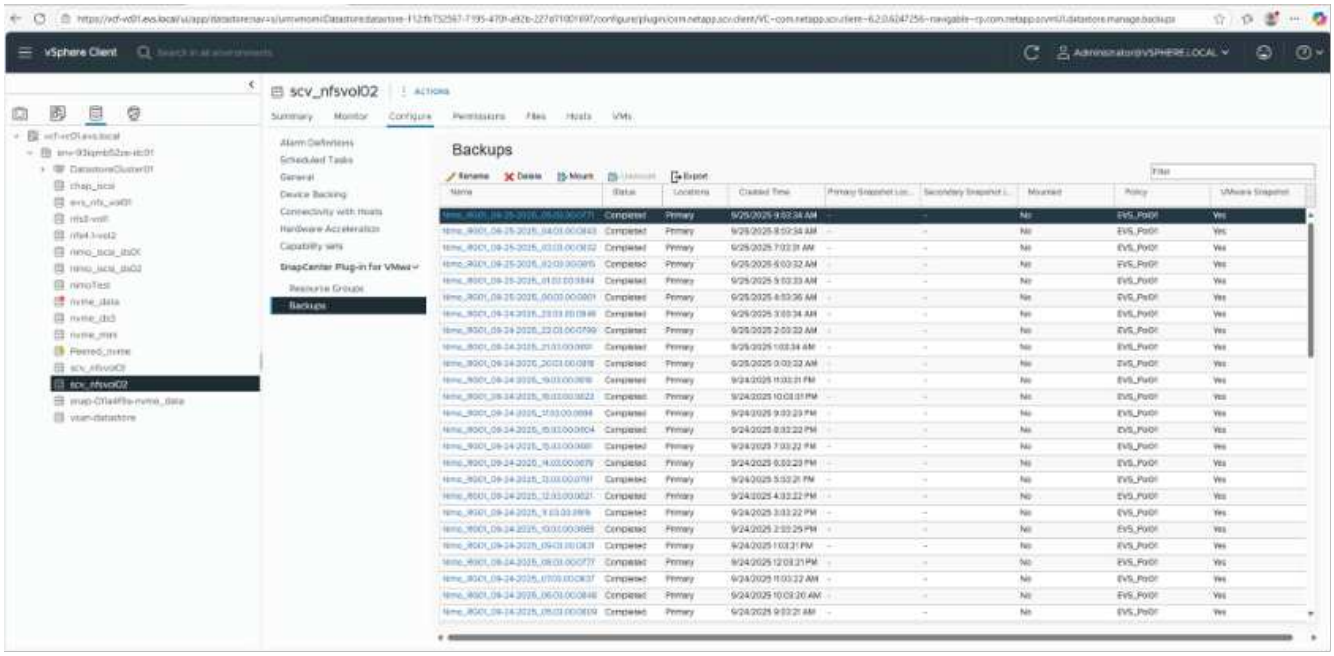
也可以從個別 VM 層級觸發還原作業。

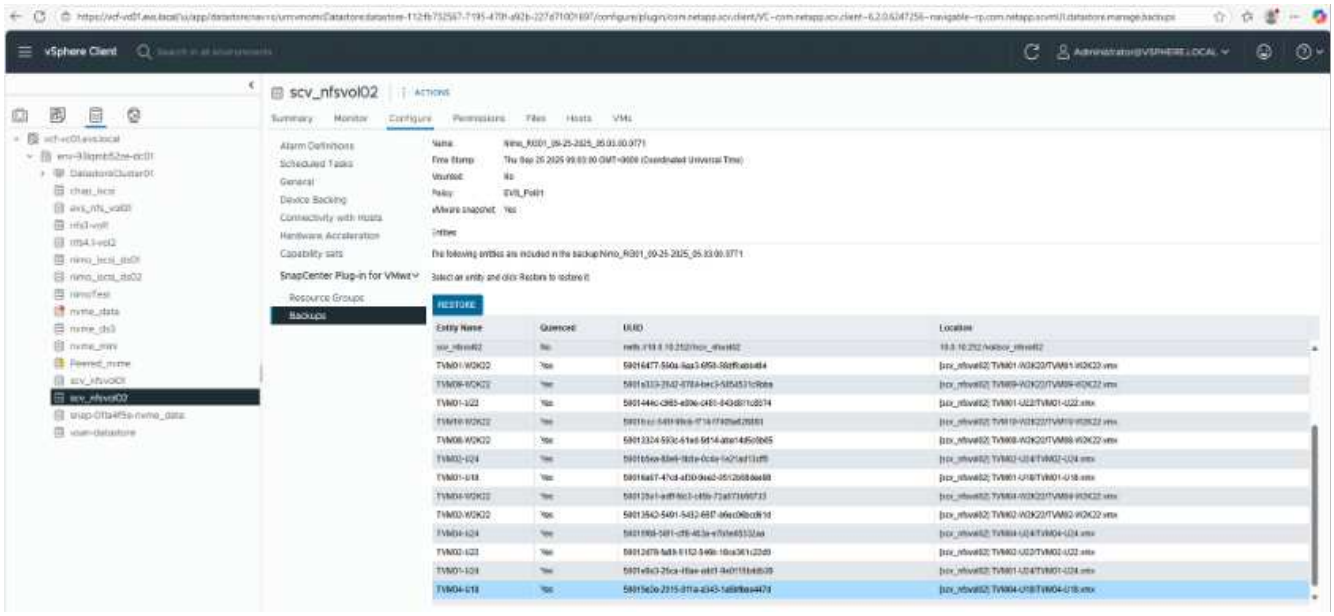
還原已刪除 **VM** 的步驟

使用 SCV 還原已刪除的 VM 是一個簡單的程序。

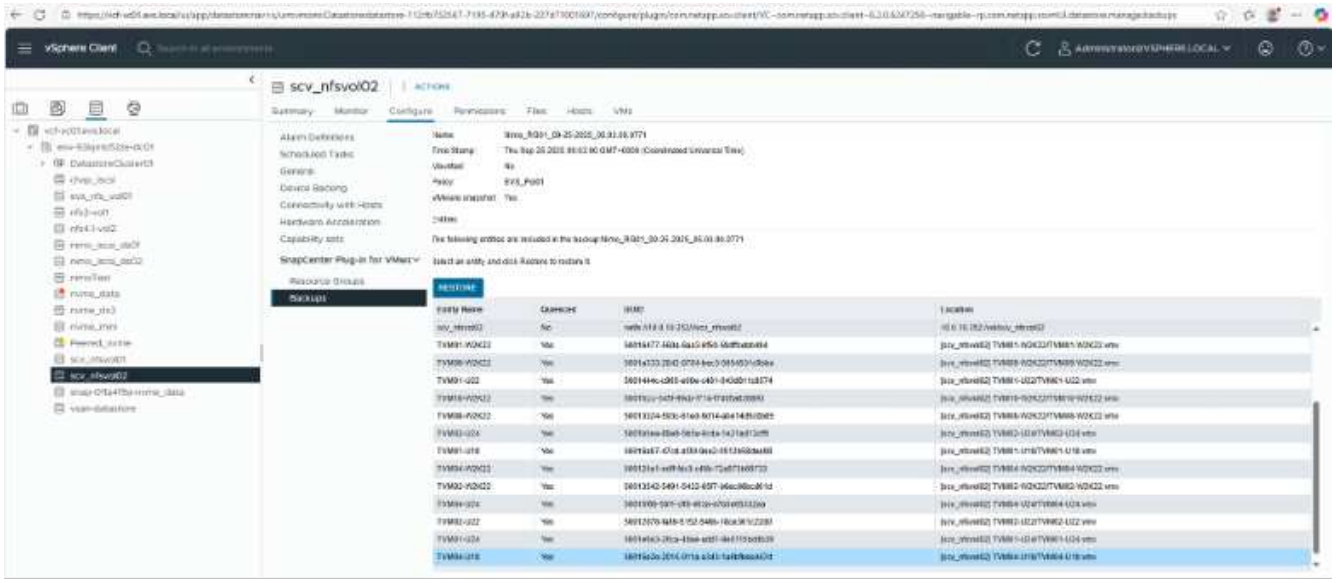
可以從資料儲存層級執行已刪除 VM 的還原作業。

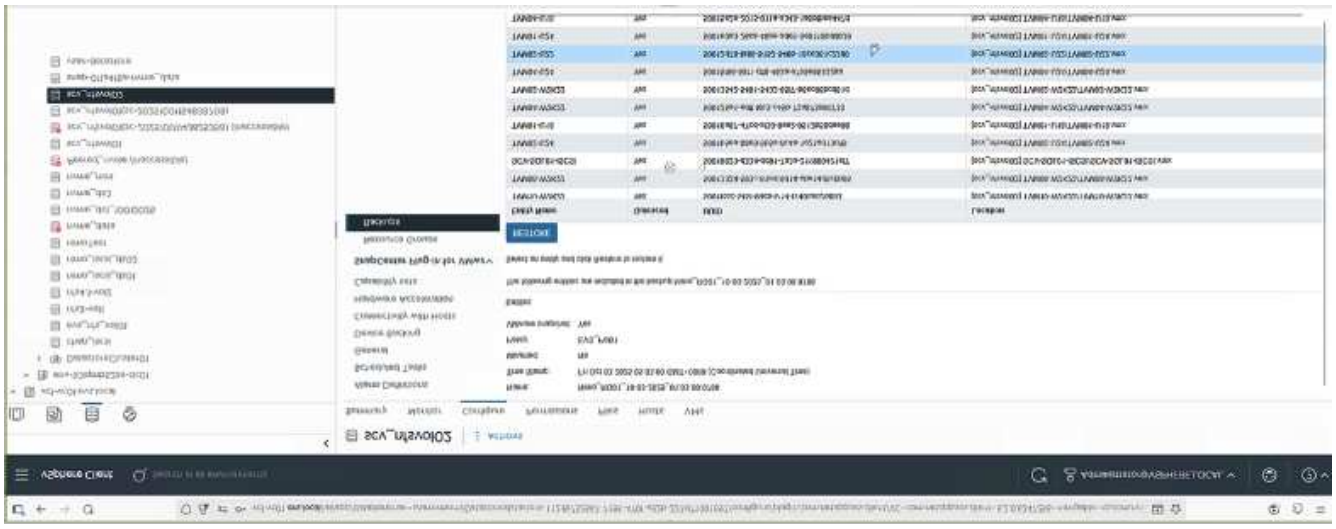
1. 前往對應的 Datastore > Configure > Backups。在那裡，選擇已刪除的 VM，然後選擇「Restore」。

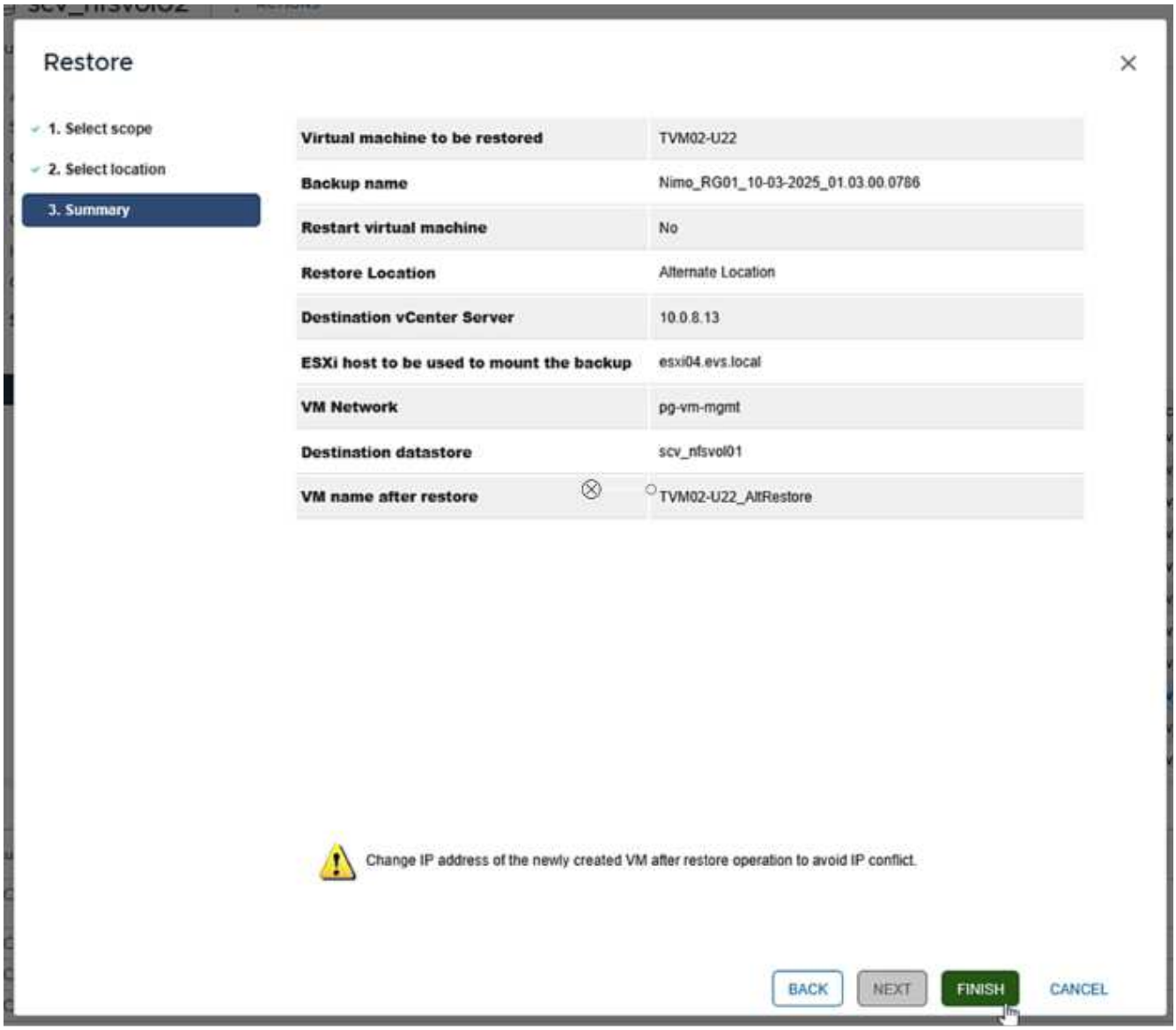


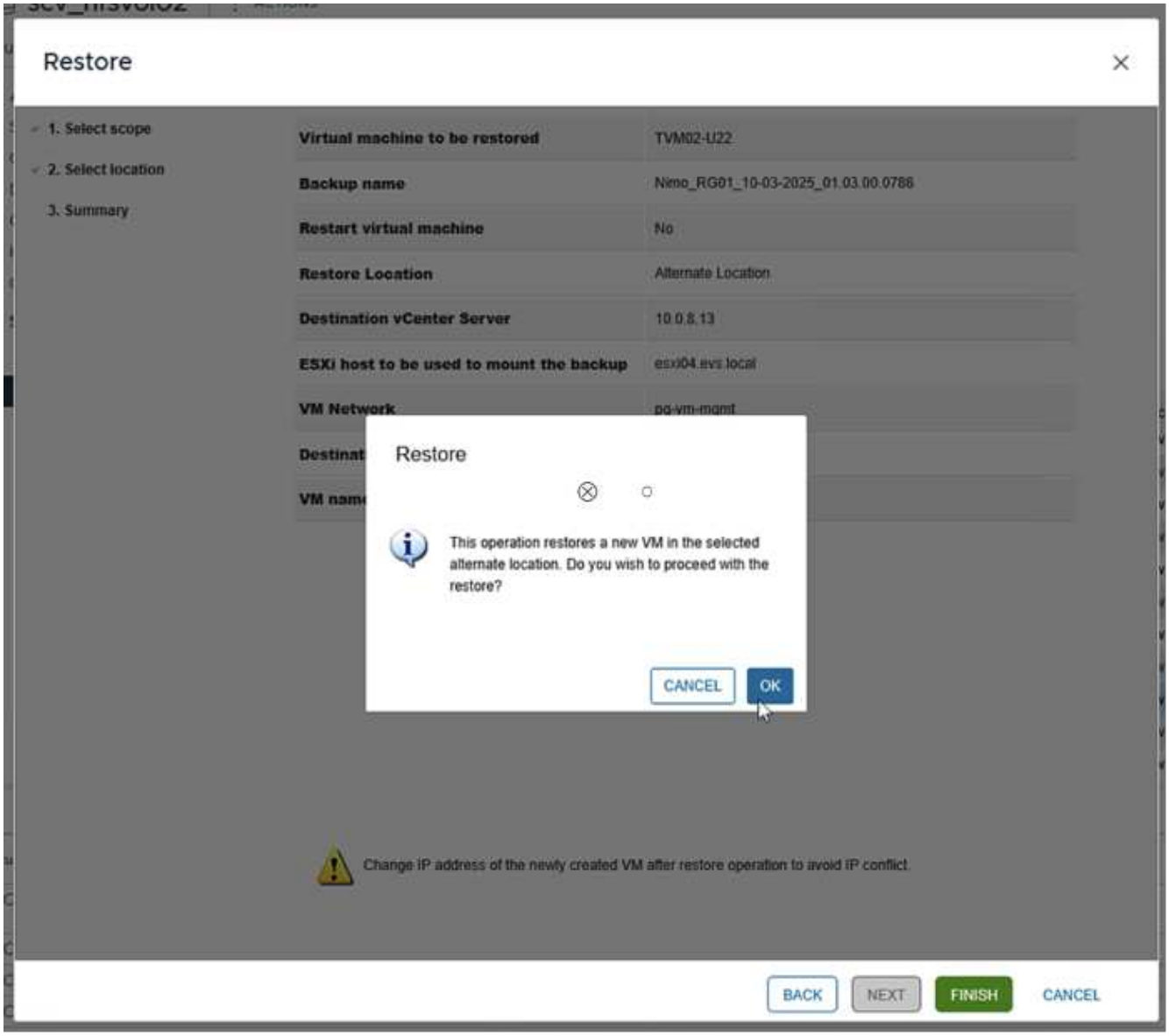


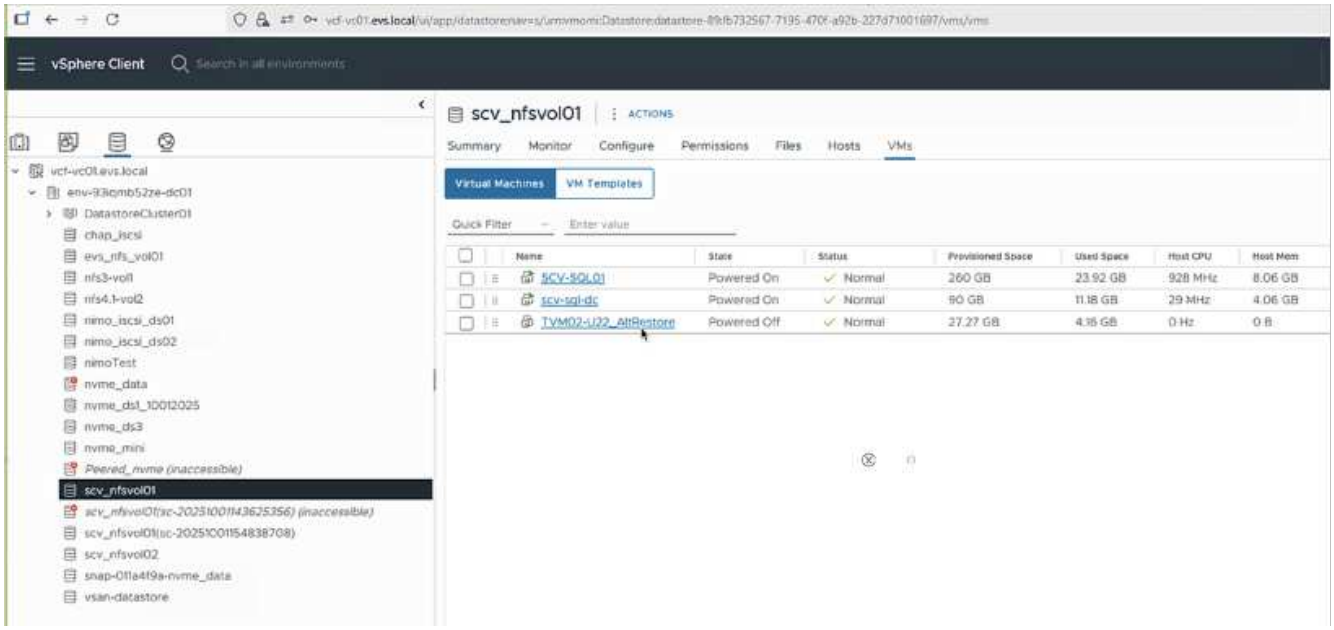
2. 接下來的螢幕截圖流程涵蓋了將 VM 還原到備用 ESXi 主機和不同資料儲存區的過程。


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE


vSphere Client
scv_nfsvol02
RESTORE


Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

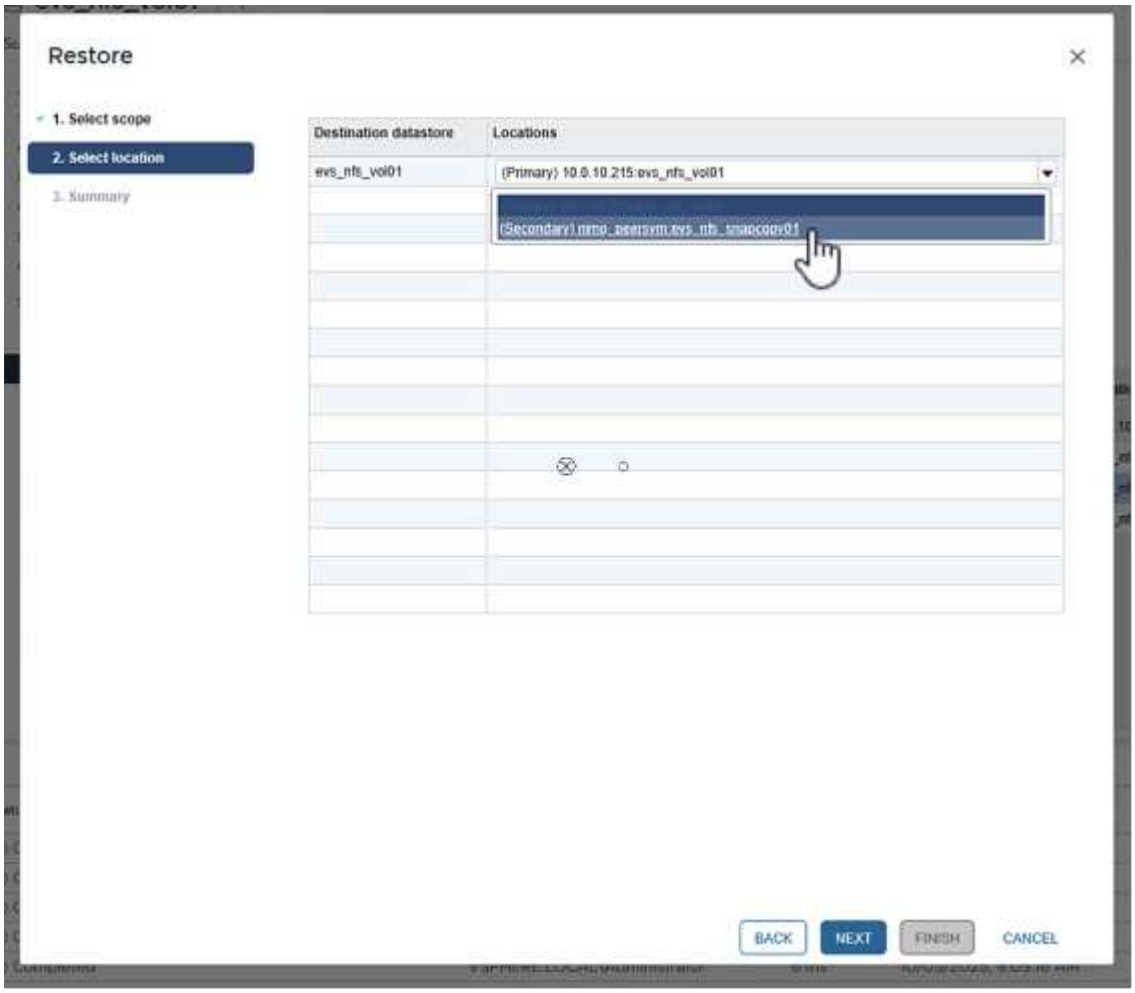

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

目標資料儲存區必須有足夠的可用空間，且在「還原到備用位置」欄位中指定的 vCenter 必須可透過 DNS 解析。

為了提高 NFS 環境中的還原效率，請開啟 VMware vStorage API for Array Integration （ VAAI ）。

也可以從次要位置（例如 SnapMirror 目的地）執行還原。



+

由 **SnapCenter Plug-in for VMware** 保護的客體檔案和資料夾的還原程序

以下部分展示如何從 VMDK 中還原客體檔案和資料夾。

SnapCenter 僅當客體作業系統為 Windows 時才支援從 VMDK 復原檔案和資料夾。

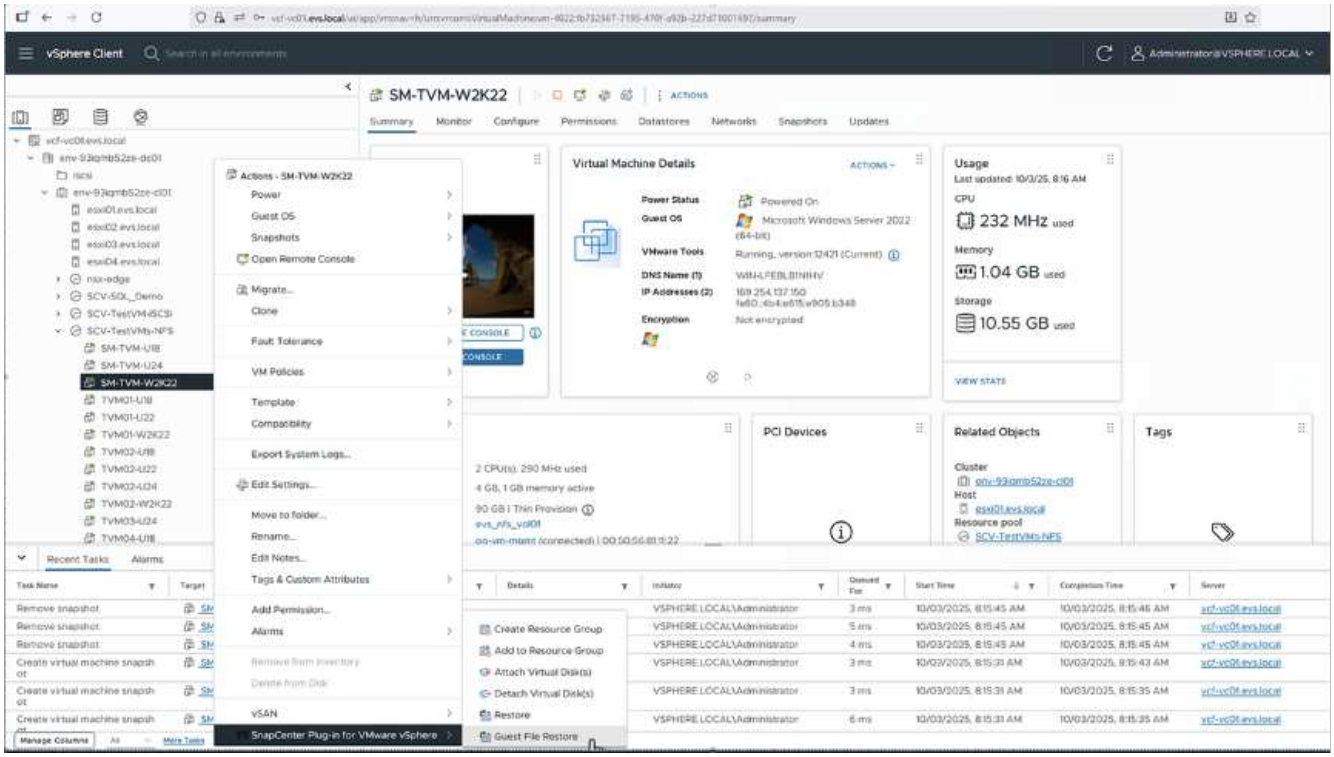
使用 SCV 還原客體檔案和資料夾的考量事項：

- 虛擬機器上必須執行 VMware 工具。
- 預設情況下，附加的 VMDK 可存取 24 小時。
- 一台虛擬機器一次只能執行一個還原或附加作業。

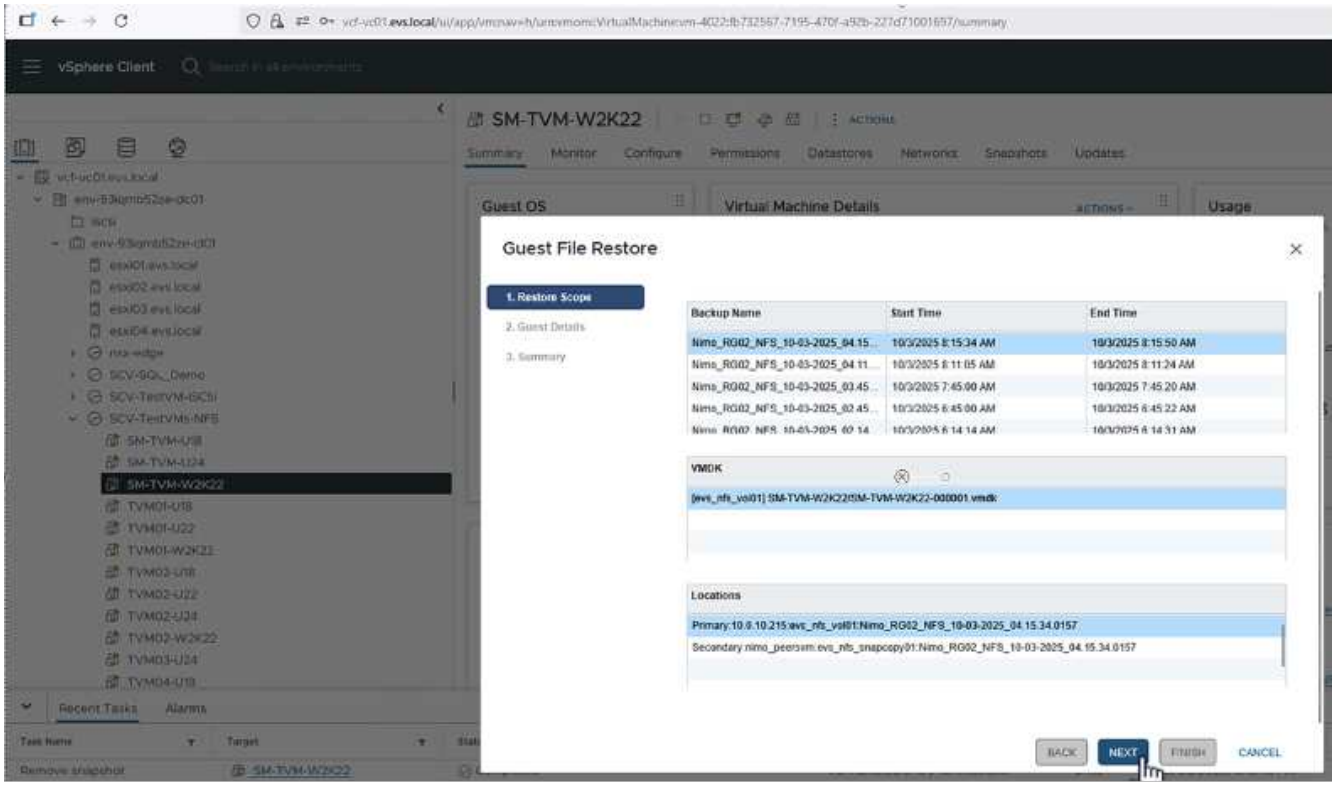
- 系統檔案、隱藏檔案和加密檔案可以還原；但是，它們的原始屬性將無法保留。
- 避免將加密檔案還原到加密資料夾或覆寫系統檔案。

恢復客體檔案和資料夾的步驟：

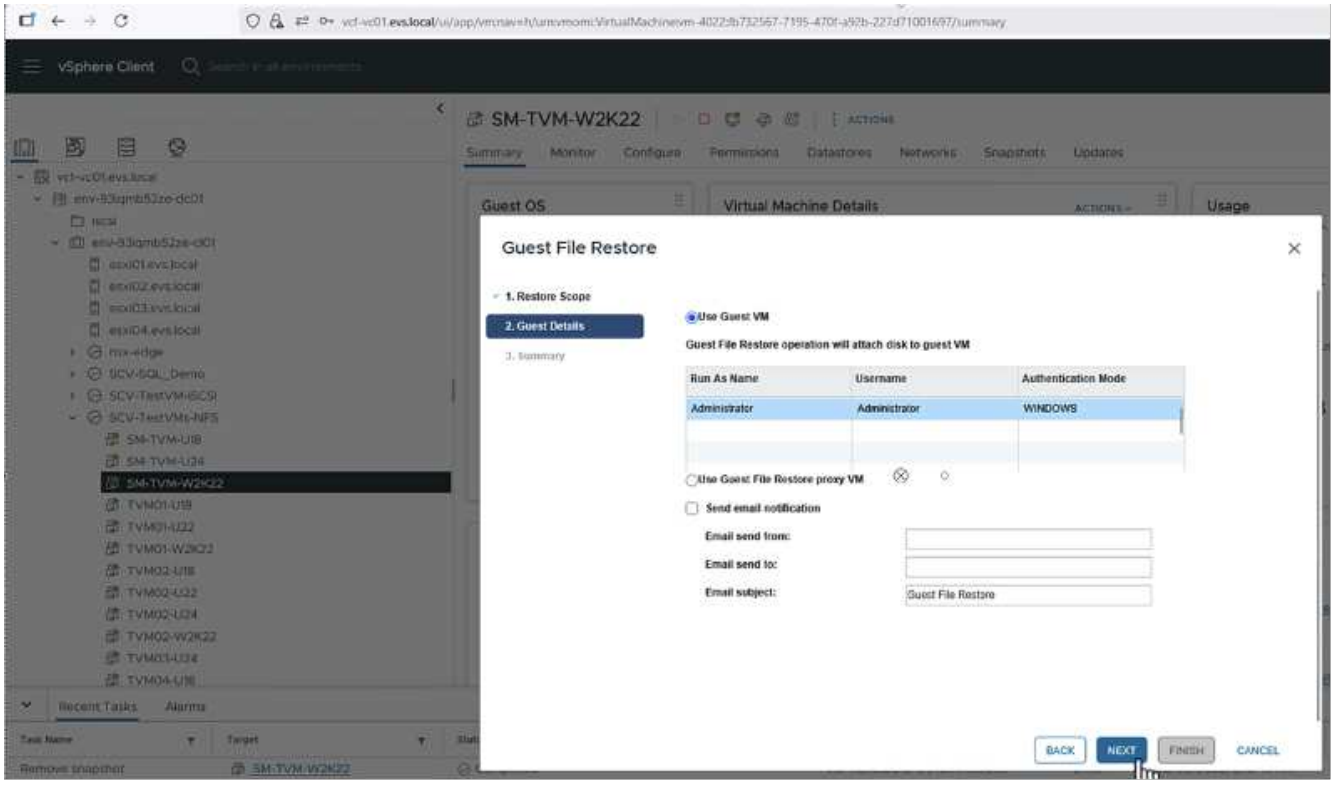
1. 右鍵點選目標虛擬機，然後選擇「NetApp SnapCenter > Guest File Restore」。



2. 選擇包含所需 VMDK 的備份。指定 VMDK 及其位置（主位置或次要位置）。

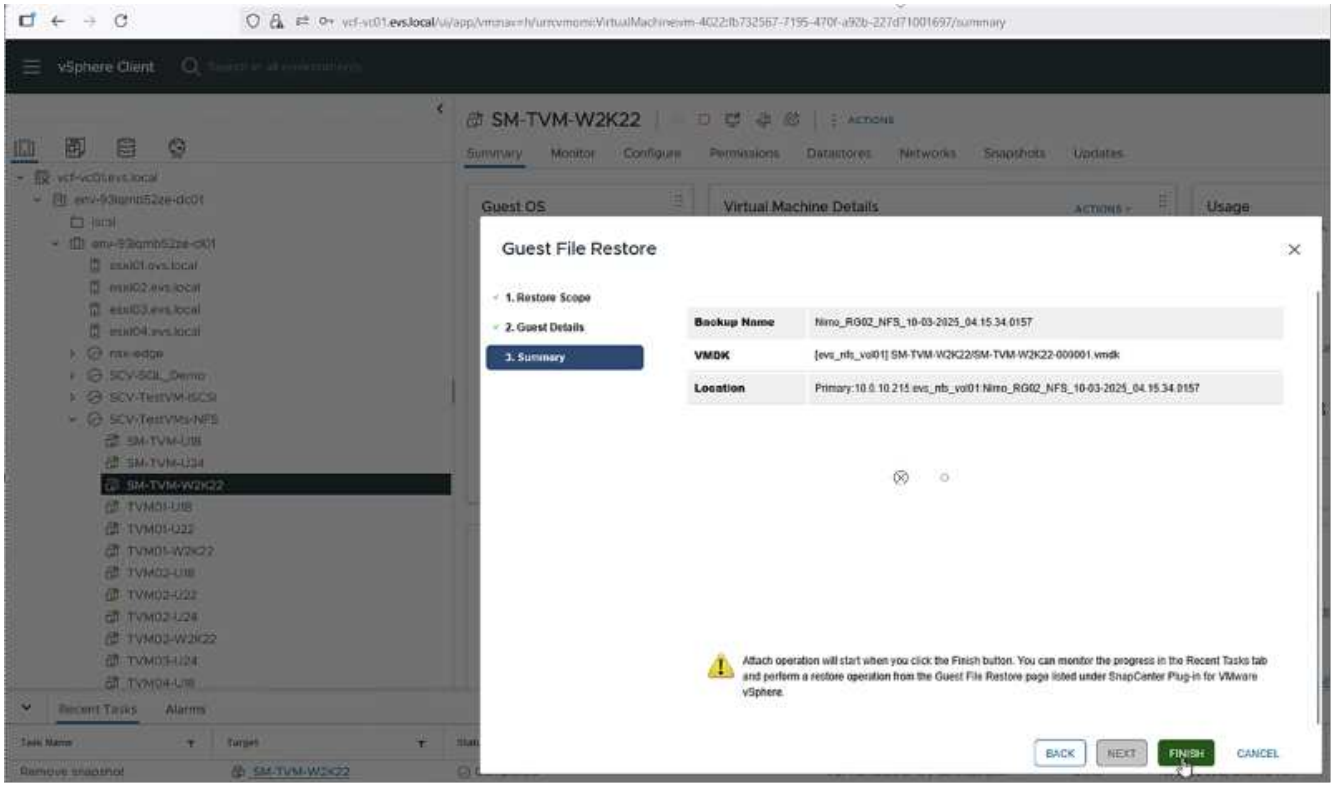


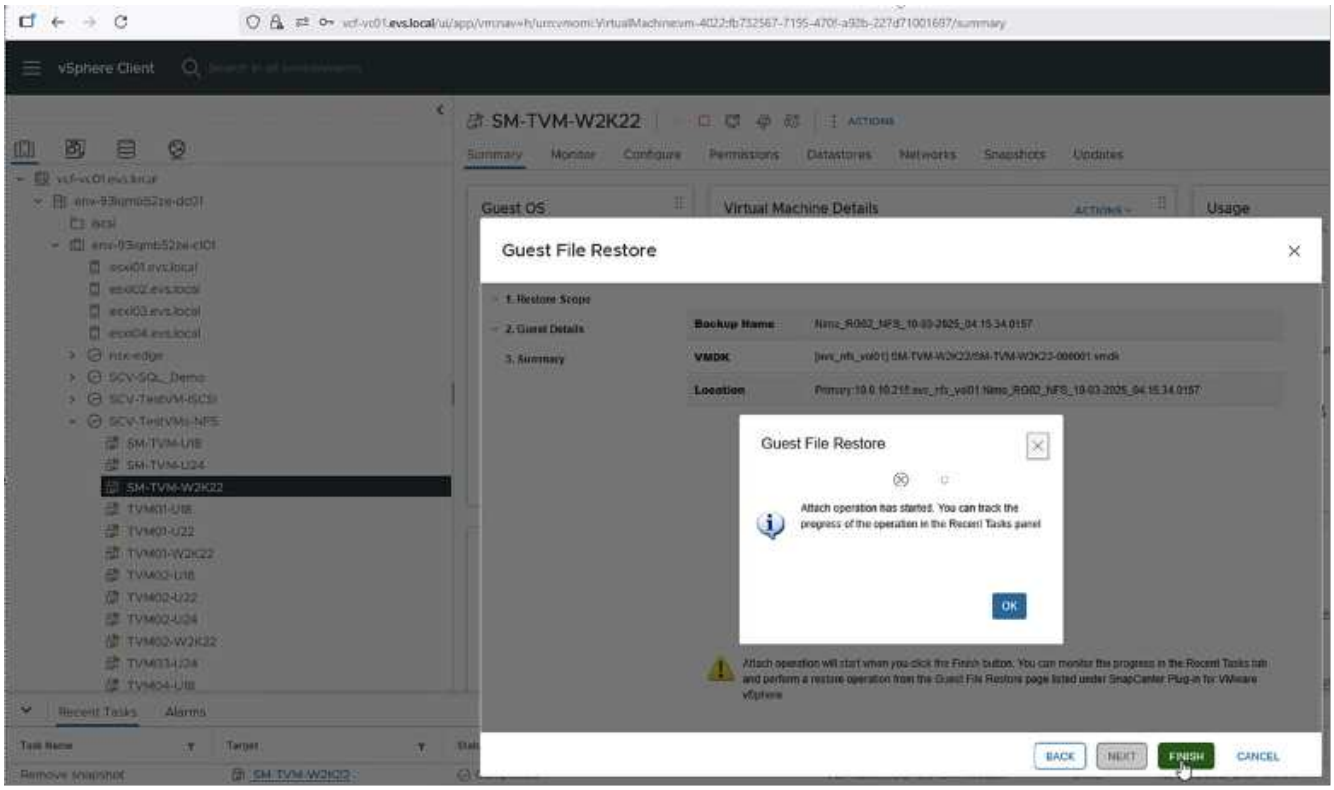
3. 選擇 "Disk Attachment Method"。



- 。客戶虛擬機器選項：將磁碟連接到原始虛擬機器（需要預先設定憑證）。本示範中使用的是此選項。
- 。Proxy VM 選項：將磁碟連接到指定的 Proxy VM（必須預先配置）。

4. 請等待附加操作完成後再瀏覽和還原檔案。操作完成後， SnapCenter 會自動建立訪客檔案還原工作階段。





5. 在客戶機檔案復原工作階段中瀏覽至 VMDK ，選擇所需的檔案或資料夾，然後將其還原至指定位置。

針對在 **VMware VMDK** 上執行的資料庫使用 **SnapCenter for SQL**（**SCSQL**）的保護程序

以下部分展示如何使用 SnapCenter for SQL（SCSQL）保護在 VMware VMDK 上執行的資料庫。

設定 **SCSQL**

使用 SCSQL 保護 VMDK 上資料庫的設定如下：

1. "安裝和配置" SnapCenter 伺服器。
2. 登入 SnapCenter。
3. 配置 SnapCenter 環境：
   - "新增或指派" 儲存系統連接。
   - "建立" 認證資料。
4. 對於 VMware VMDK 上的 Microsoft SQL Server 資料庫：
   - "部署 SCV"（已在設定部分介紹）。
   - 向 SnapCenter 註冊外掛程式。
5. 新增 "SQL Server 主機與安裝外掛程式"：
   - "設定 SQL 外掛程式"。
   - "設定資料庫和日誌的保護計畫和排程"。

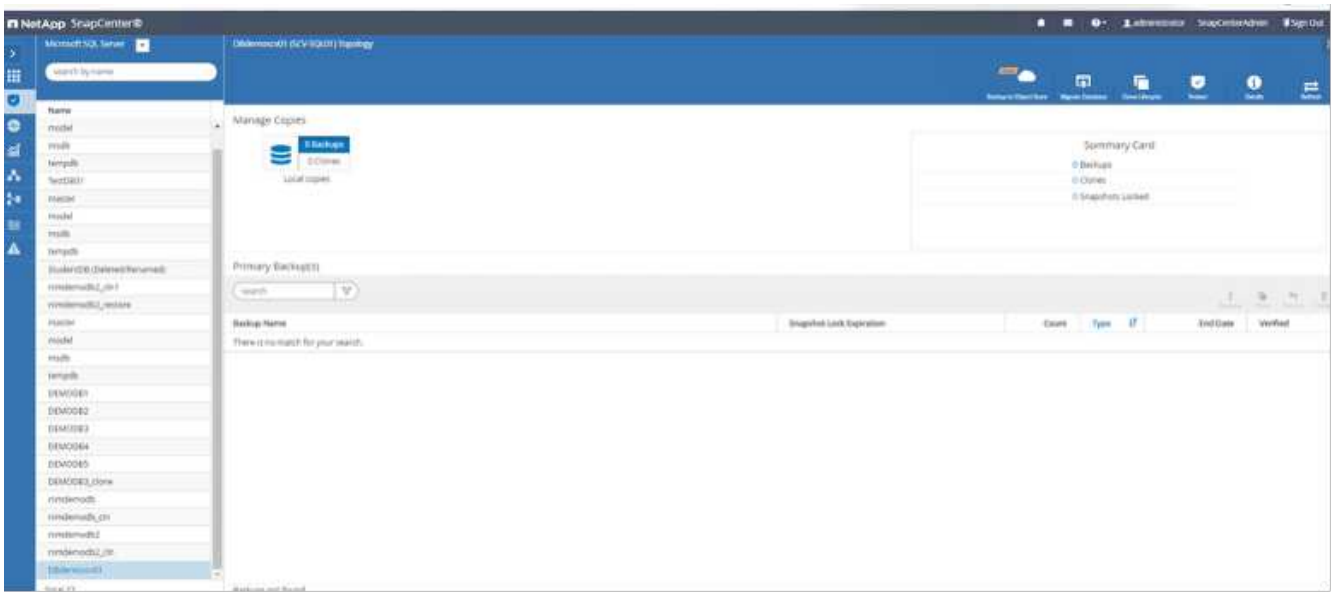


設定備份原則

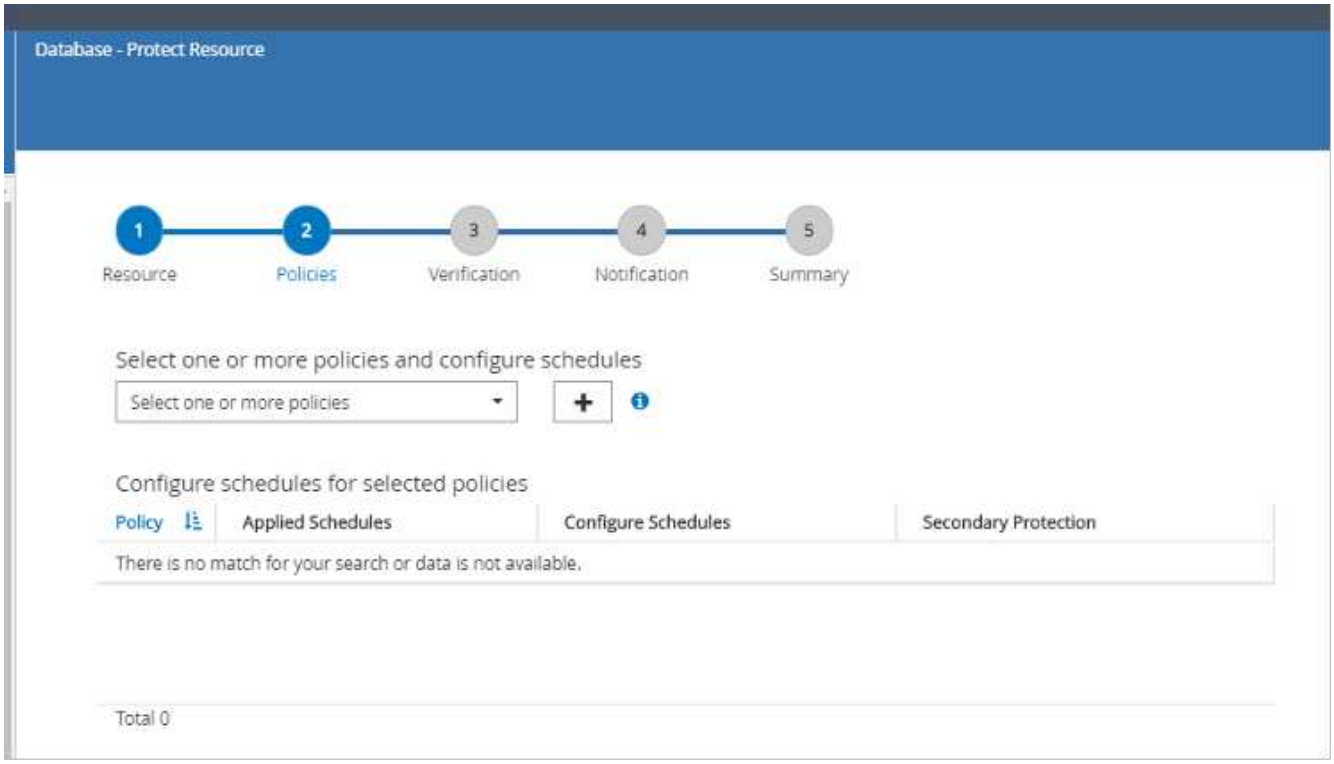
以下步驟將說明如何設定備份原則。

1. 從資源標籤中選擇資料庫，然後從右上角選擇「Protect」。

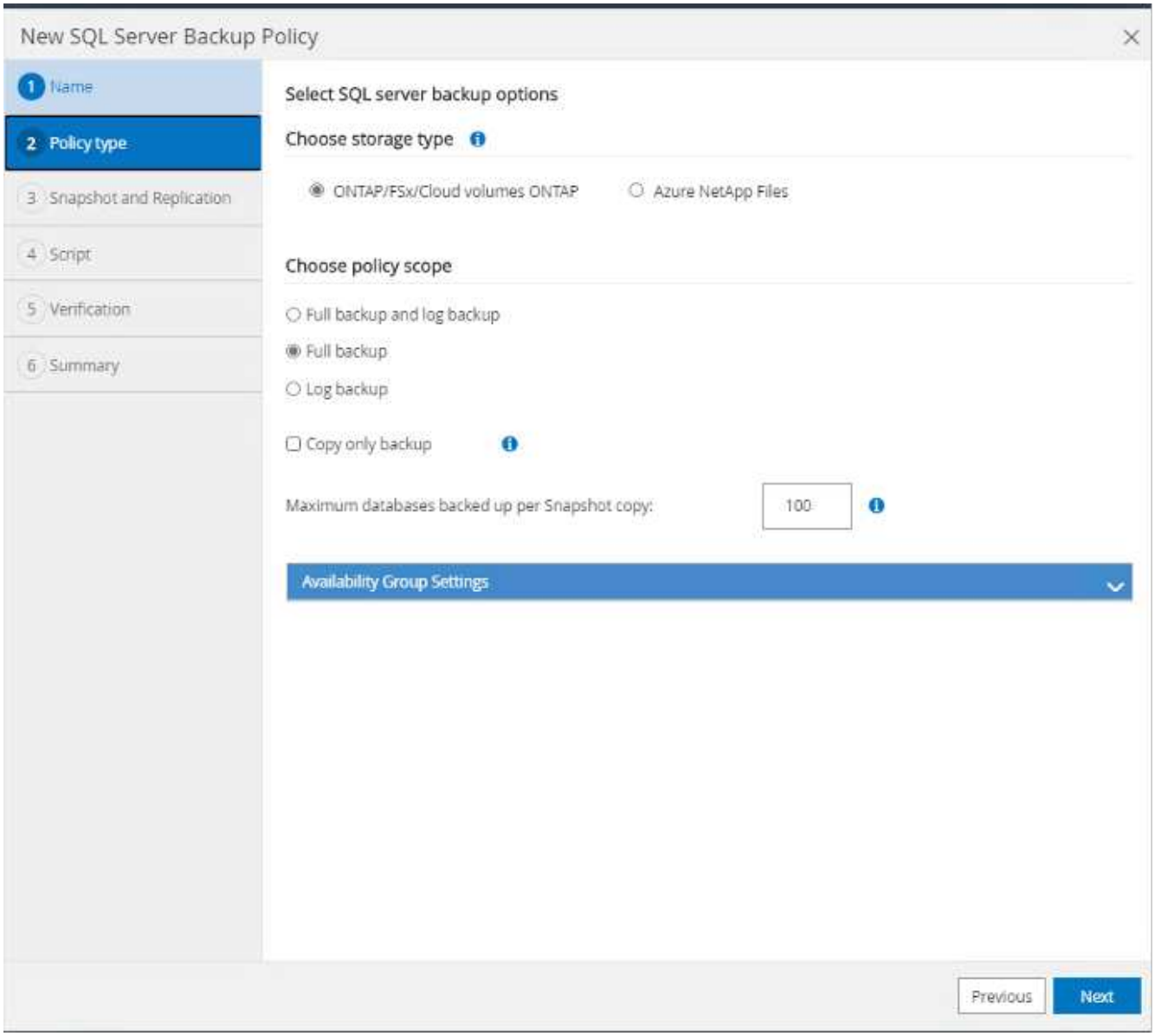
驗證是針對在客體虛擬機器上執行的 SQL Server 資料庫執行。



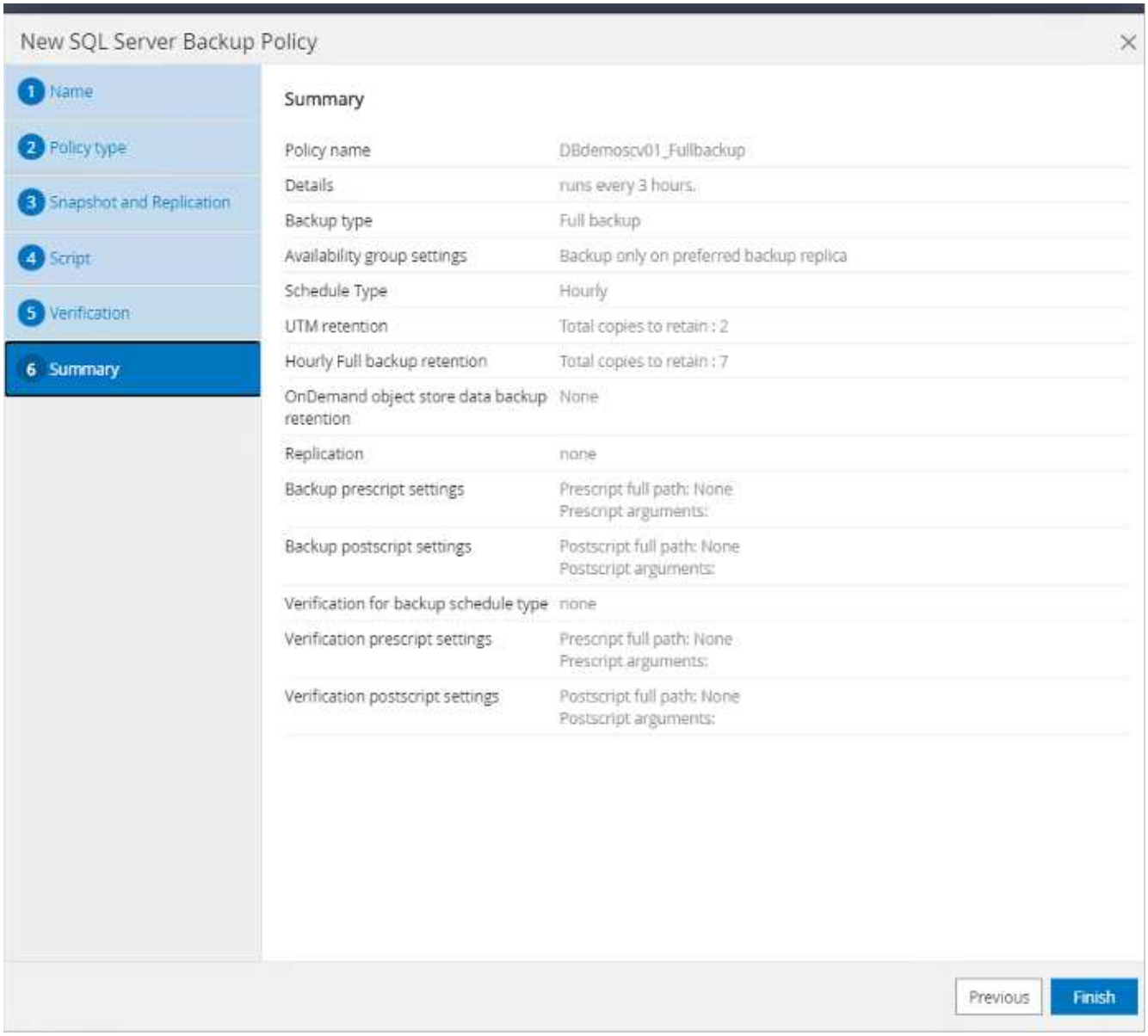
2. 點選加號圖示以配置 SQL Server 備份原則。



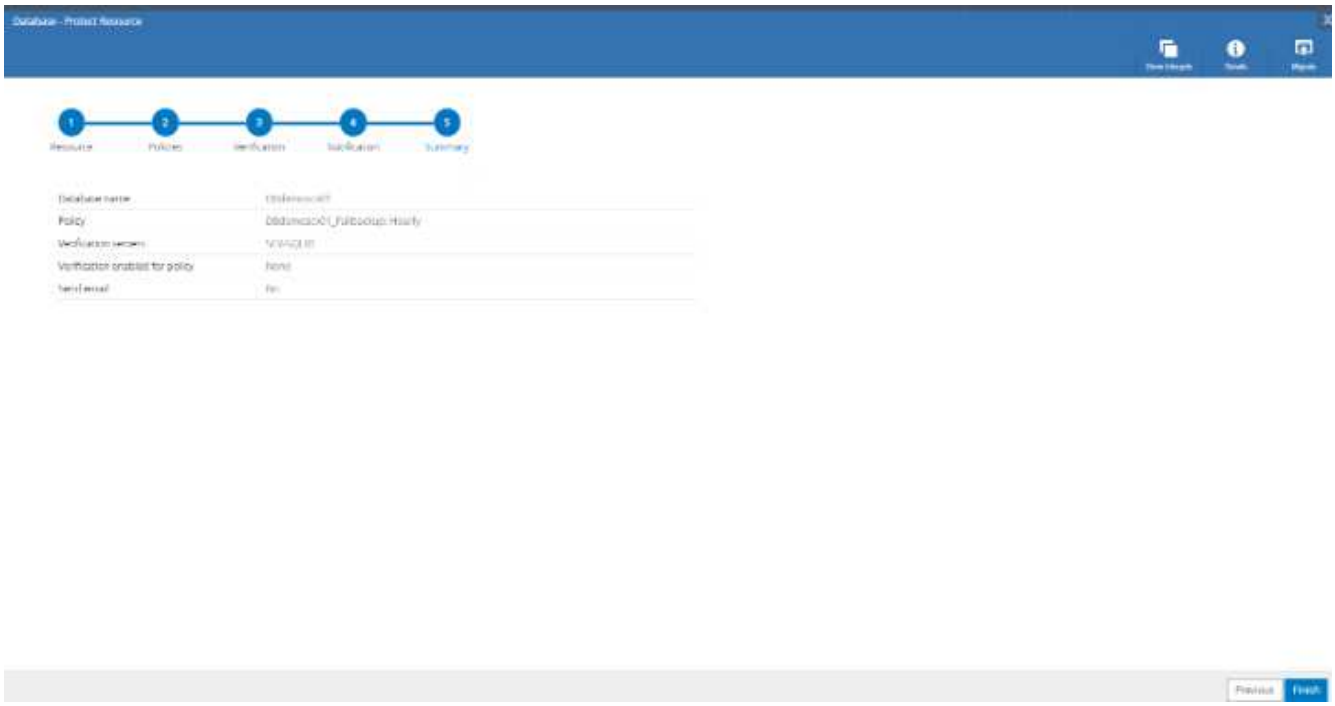
3. 在此演示中，已選擇「完整備份」。選擇「下一步」繼續。



4. 在「摘要」頁面上、選取「完成」。


New SQL Server Backup Policy
1 Name
2 Policy type
3 Snapshot and Replication
4 Script
5 Verification
6 Summary
Summary
Policy name
DBdemoscv01_Fullbackup
Details
runs every 3 hours.
Backup type
Full backup
Availability group settings
Backup only on preferred backup replica
Schedule Type
Hourly
UTM retention
Total copies to retain : 2
Hourly Full backup retention
Total copies to retain : 7
OnDemand object store data backup retention
None
Replication
none
Backup prescript settings
Prescript full path: None
Prescript arguments:
Backup postscript settings
Postscript full path: None
Postscript arguments:
Verification for backup schedule type
none
Verification prescript settings
Prescript full path: None
Prescript arguments:
Verification postscript settings
Postscript full path: None
Postscript arguments:
Previous
Finish

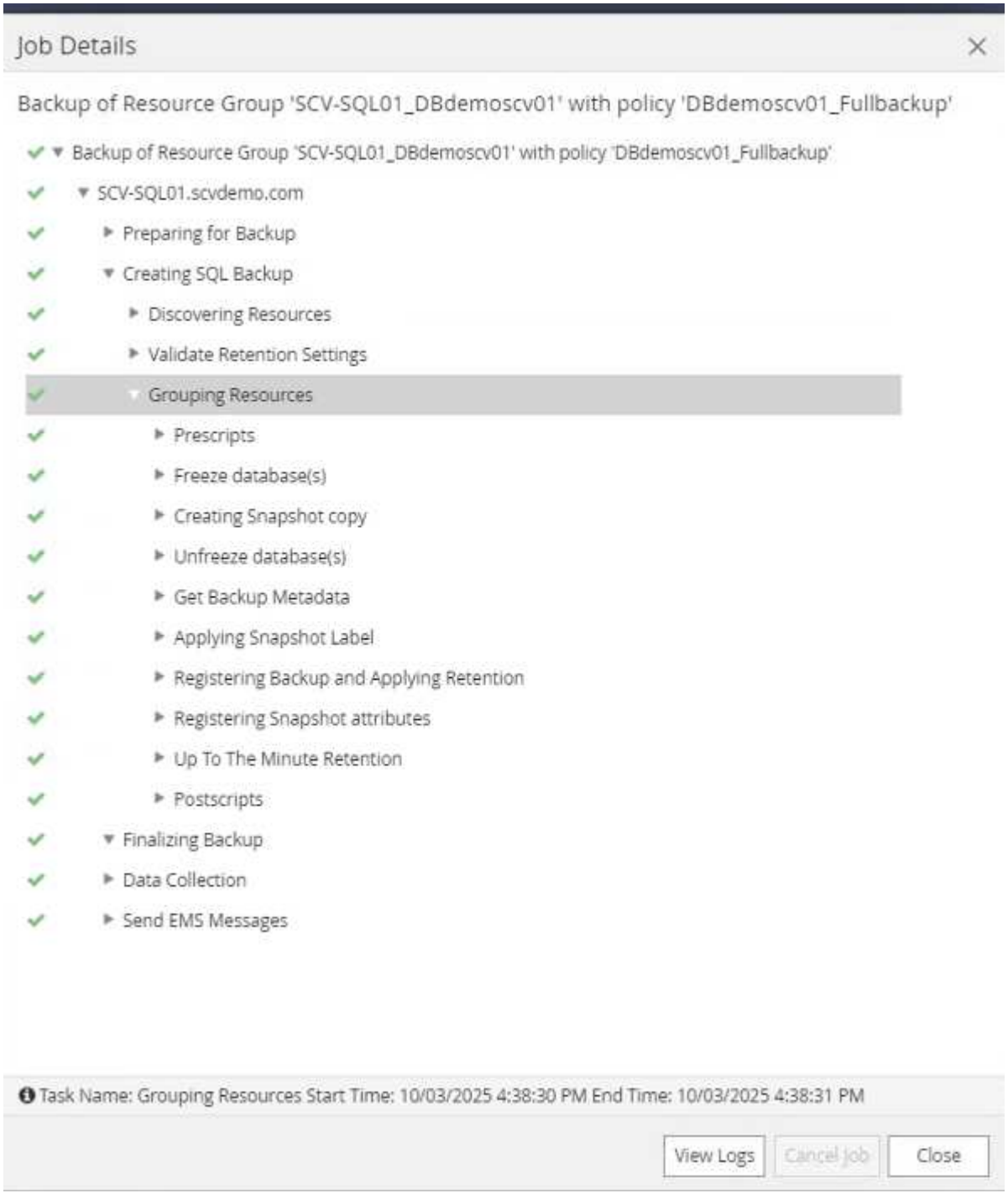
5. 繼續執行「完成」操作。



監控備份

設定備份策略後，您可以即時監控備份操作。您可以點擊 Backup now 觸發按需備份操作，也可以等待預定的備份策略生效。

1. 使用「監控 > 作業」監控作業進度。
2. 選擇備份作業，然後按一下「Details」以查看如下所示的作業詳細資訊。

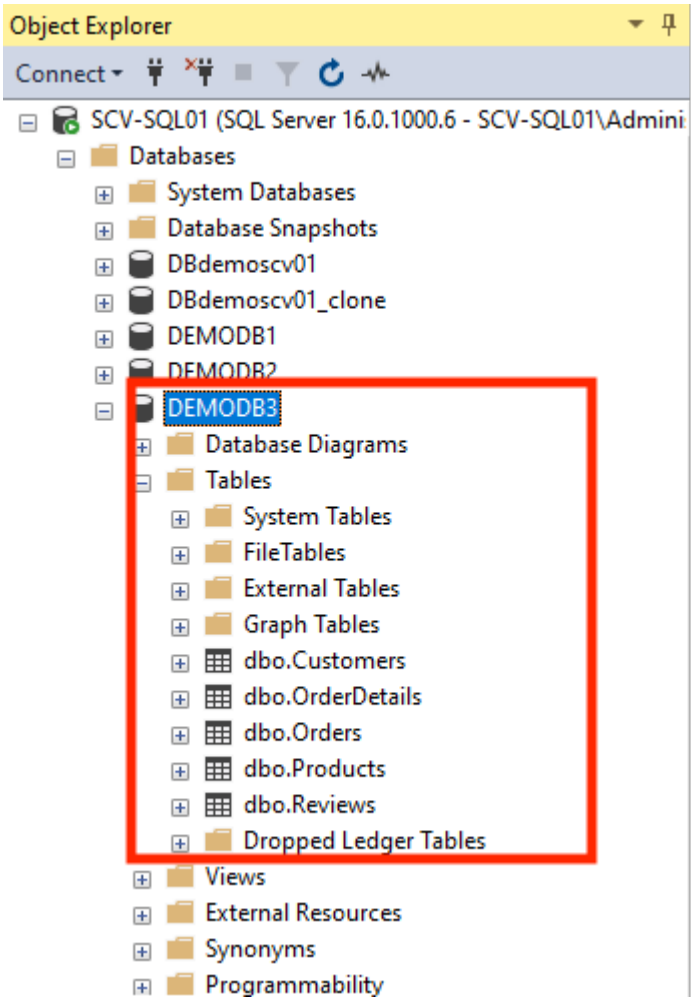


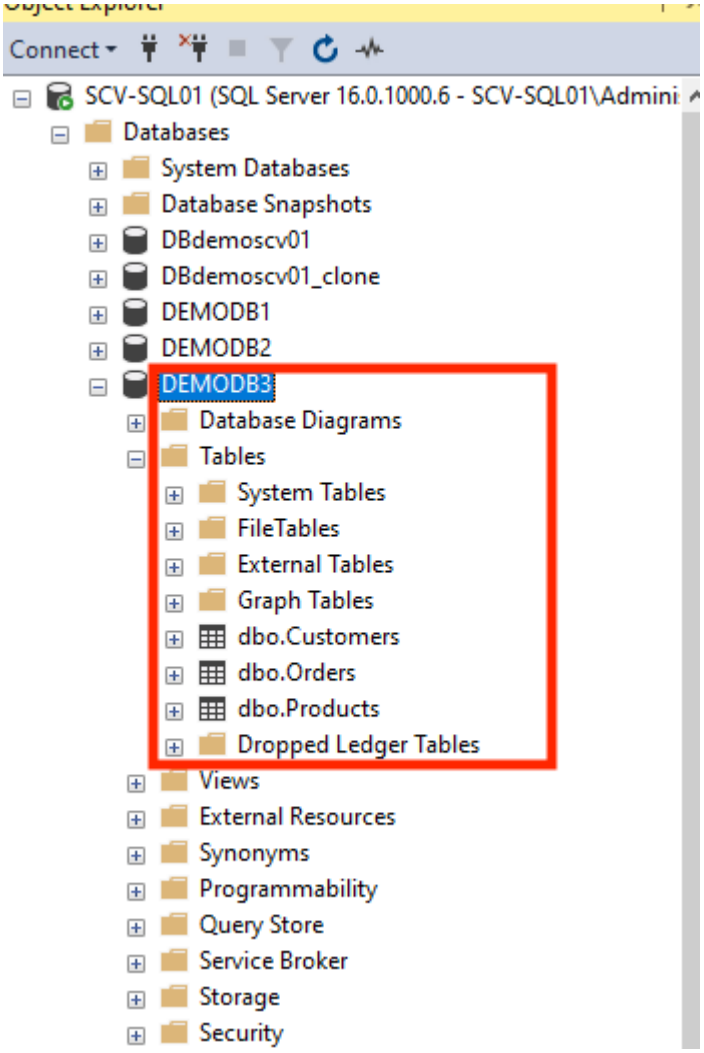
還原駐留在 **VMDK** 上的資料庫

VMDK 上的資料庫可以還原到特定的時間點。

我們可以透過刪除資料庫中的一些表格來模擬此操作的重要性，然後透過執行時間點還原來修正。

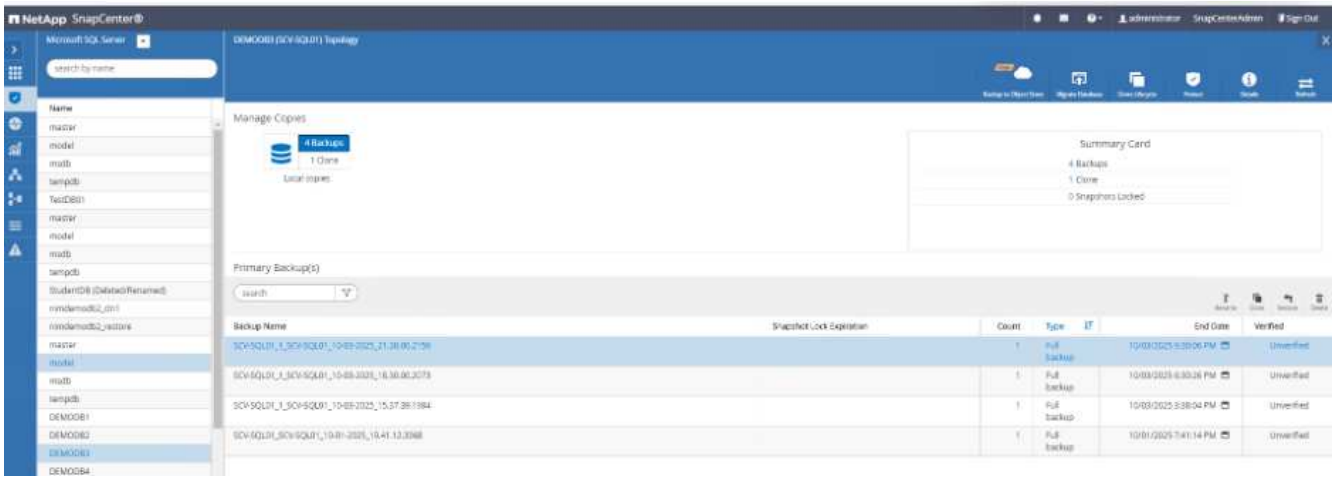
從下面的截圖中可以看出，第一張截圖中顯示的資料庫中的幾個表格在第二張截圖中已被刪除：


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

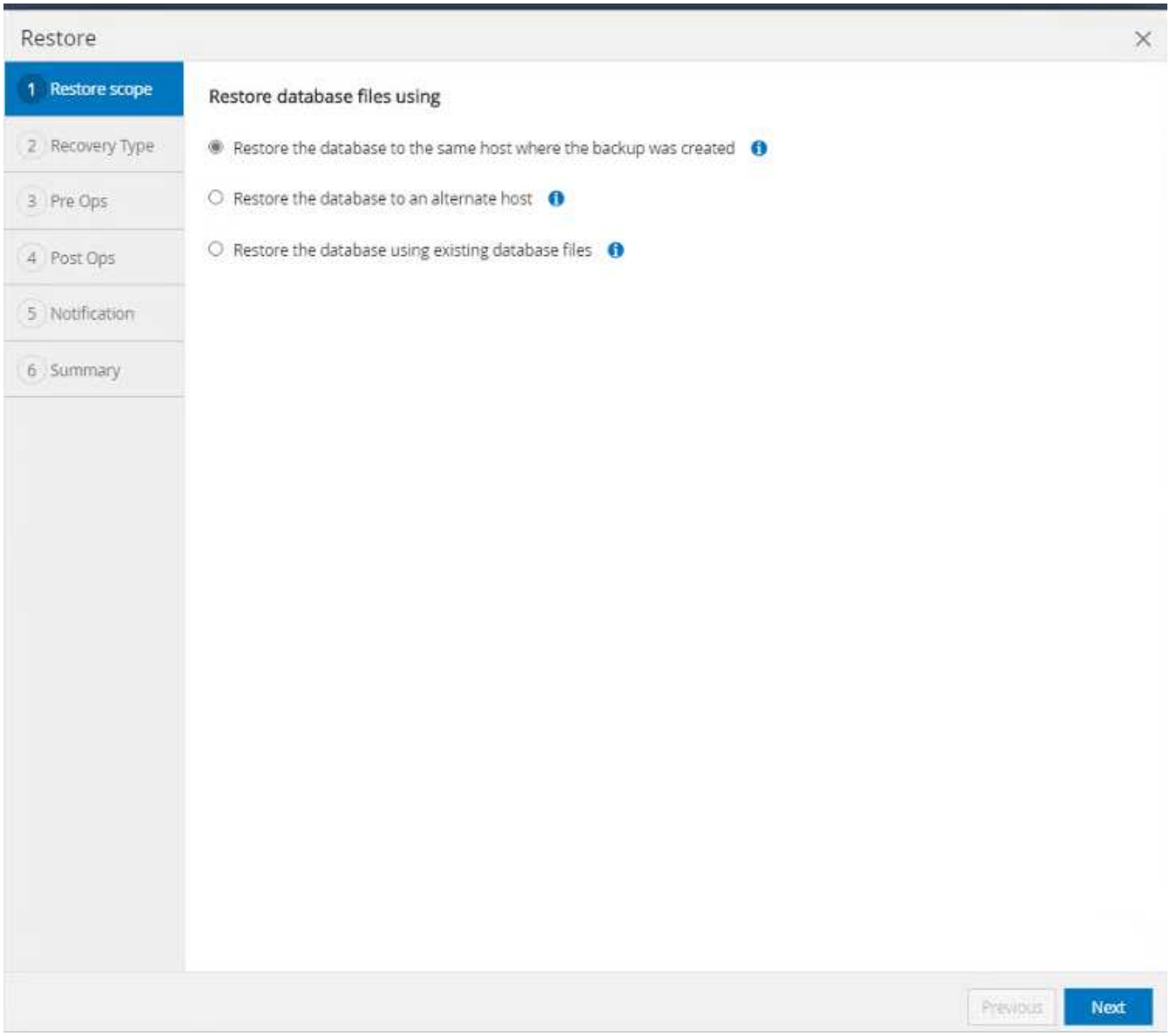


以下步驟顯示如何執行還原以復原已刪除的表格：

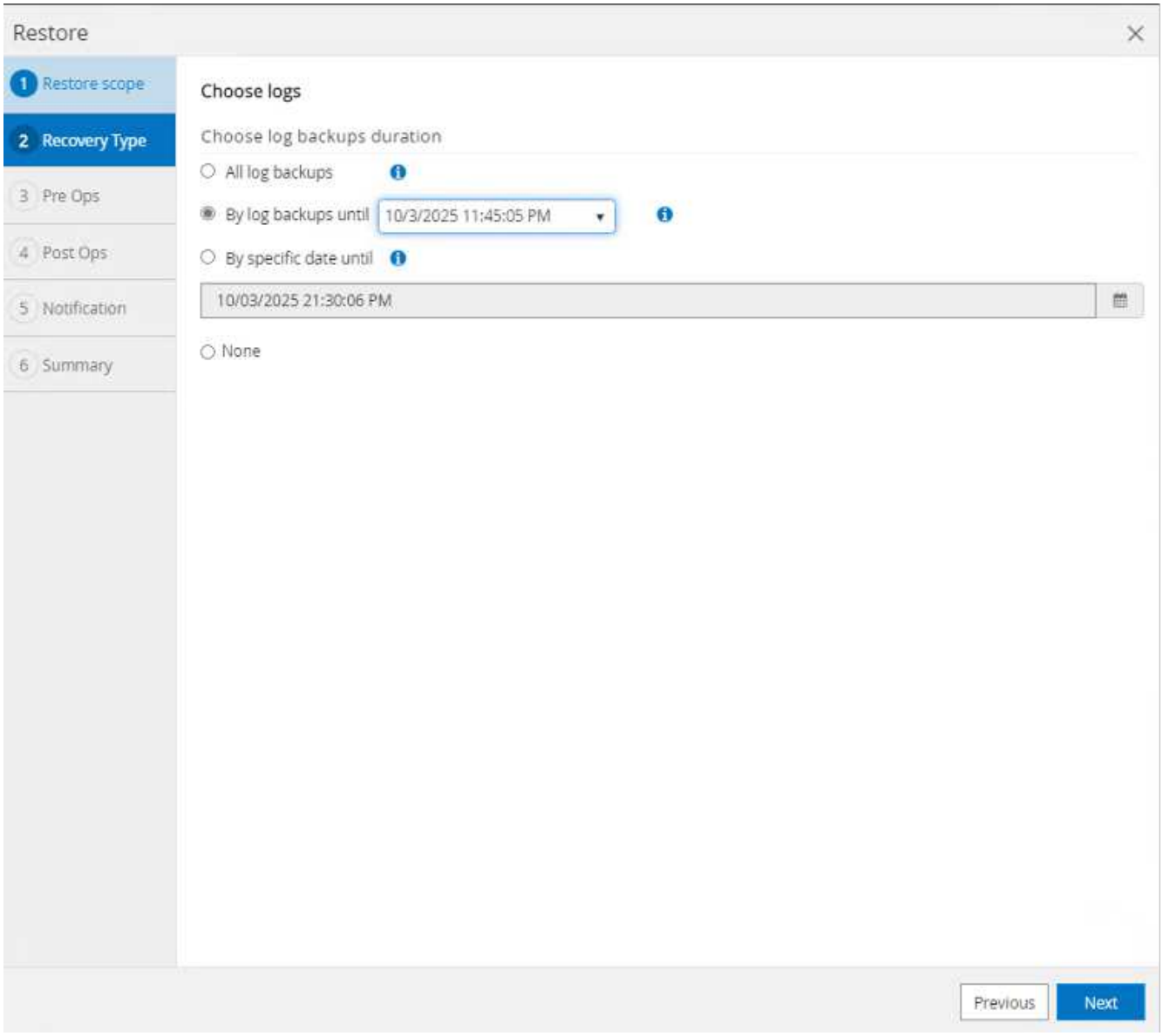
1. 從資源群組中選取資料庫。



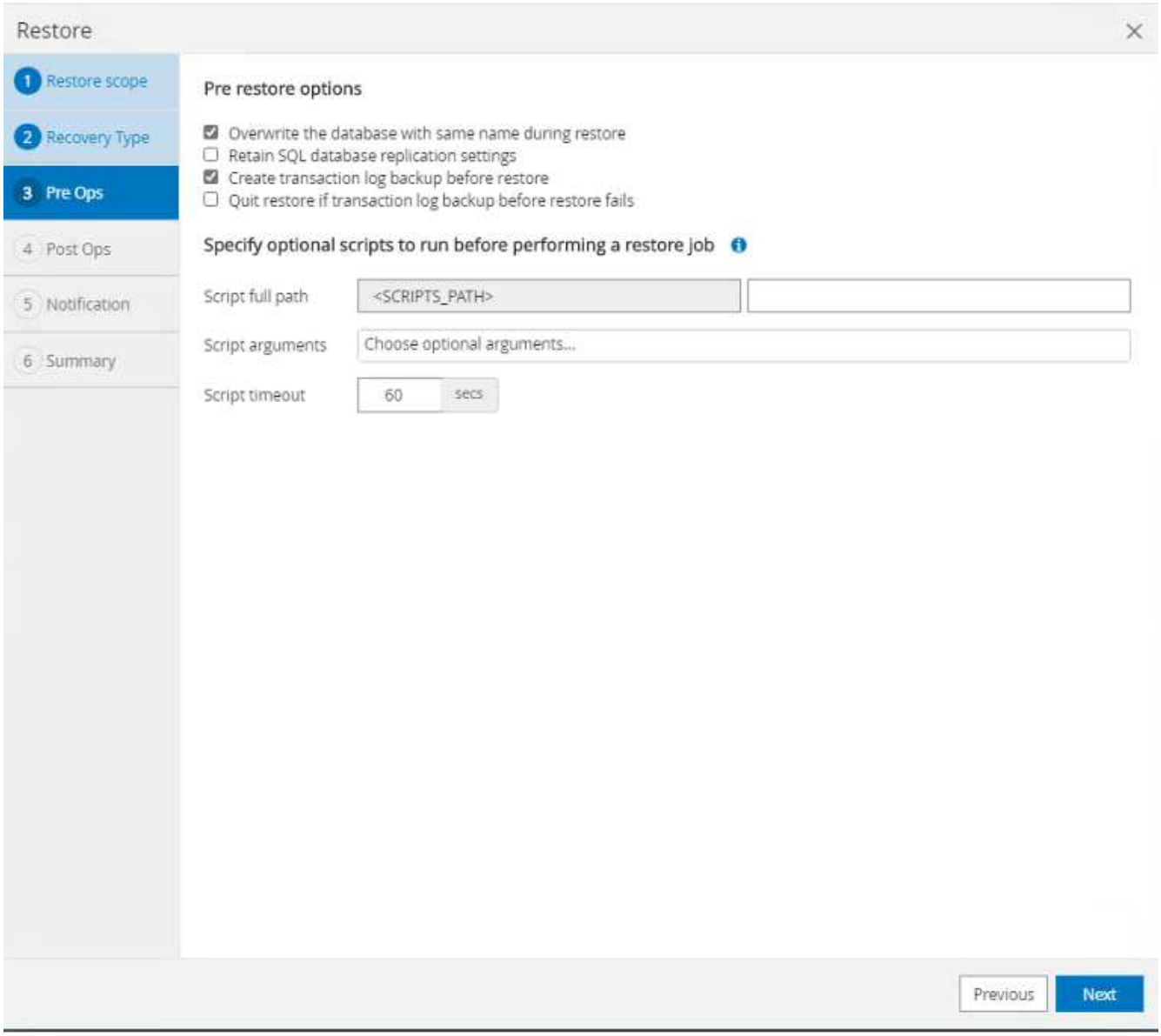
2. 在「復原」頁面中、選取「將資料庫還原至建立備份的相同主機」選項。



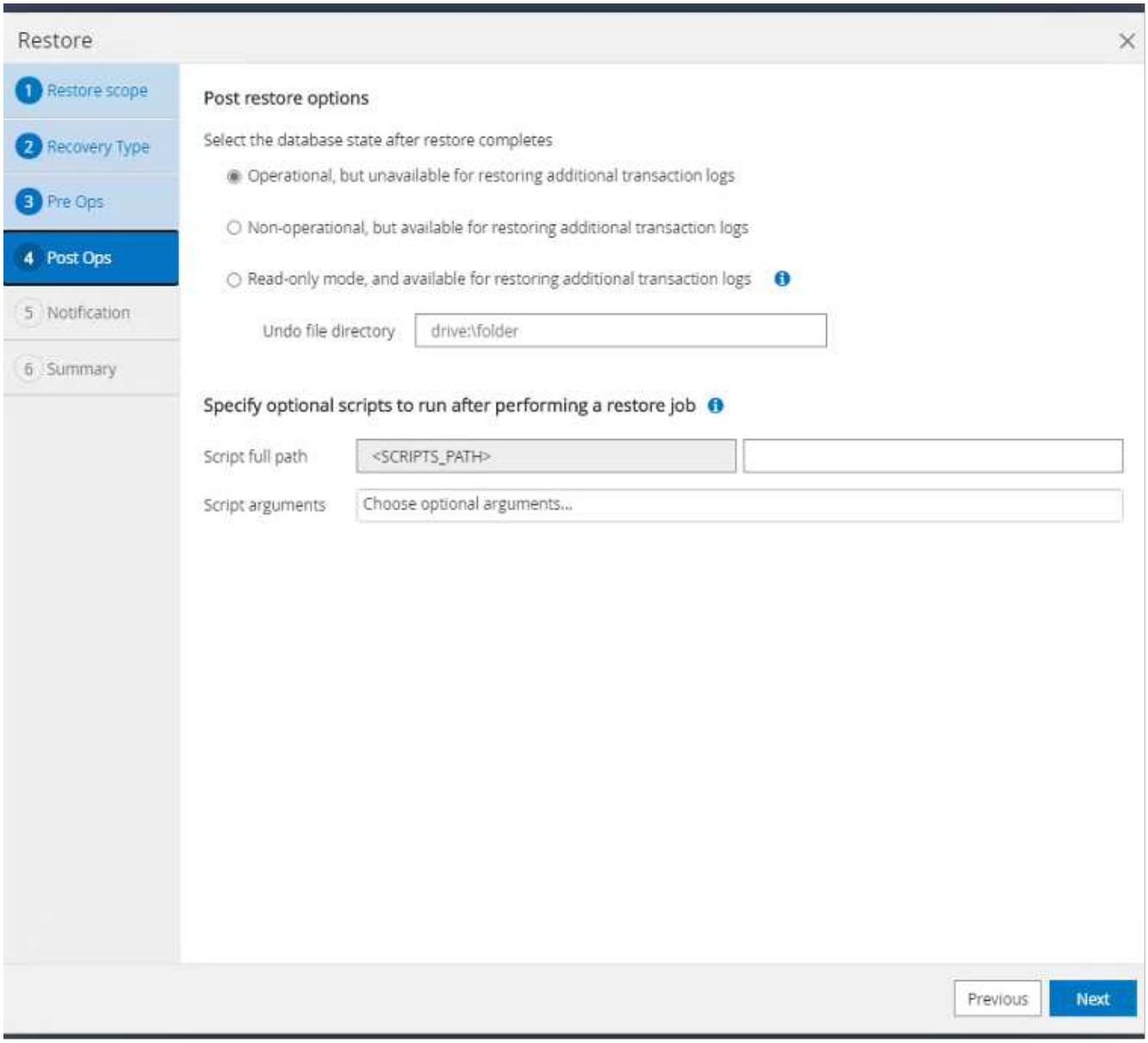
3. 選擇使用日誌備份到特定時間點的選項。



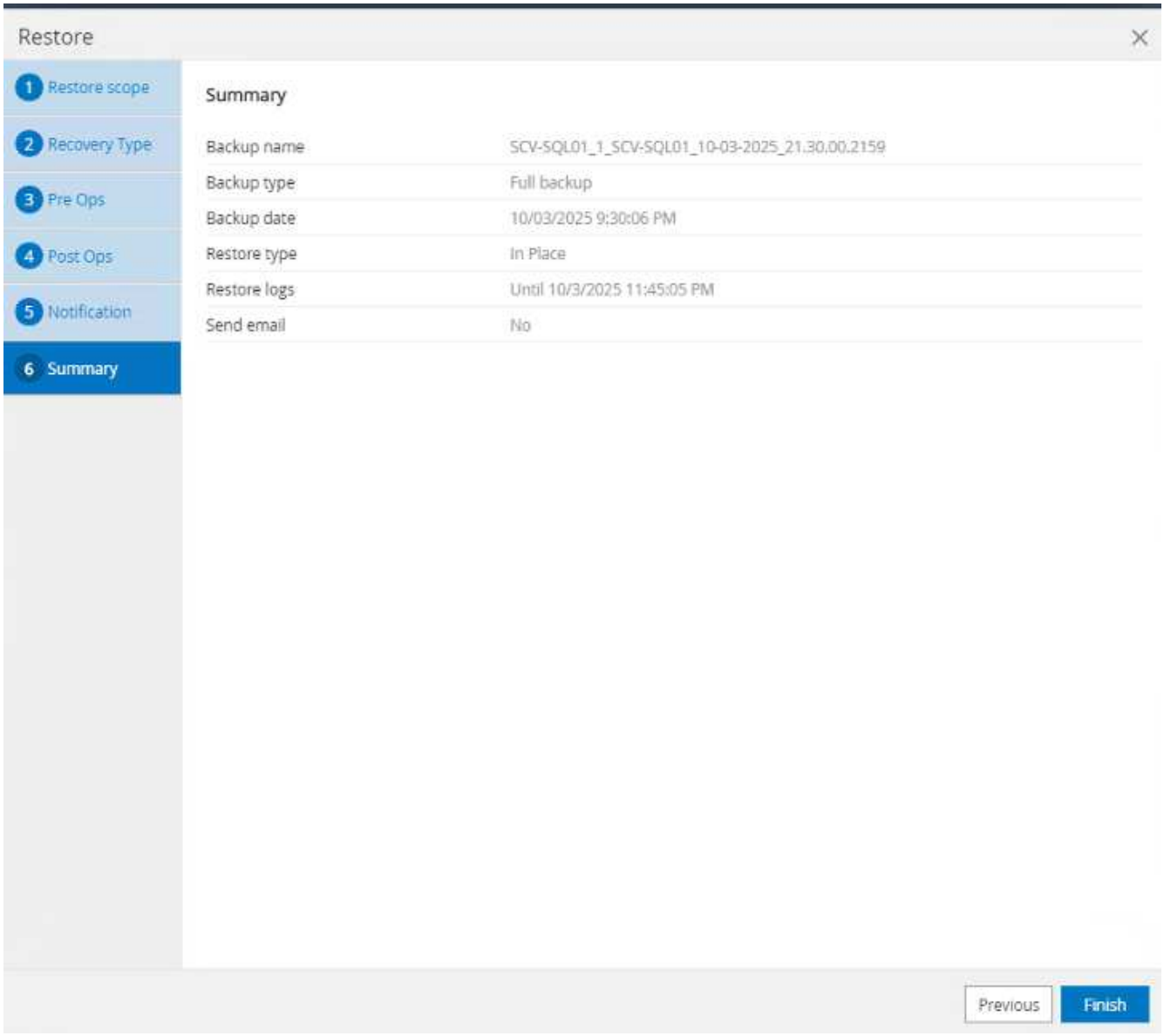
4. 選擇「還原時覆寫同名資料庫、還原前建立交易記錄備份」，然後選擇「下一步」。



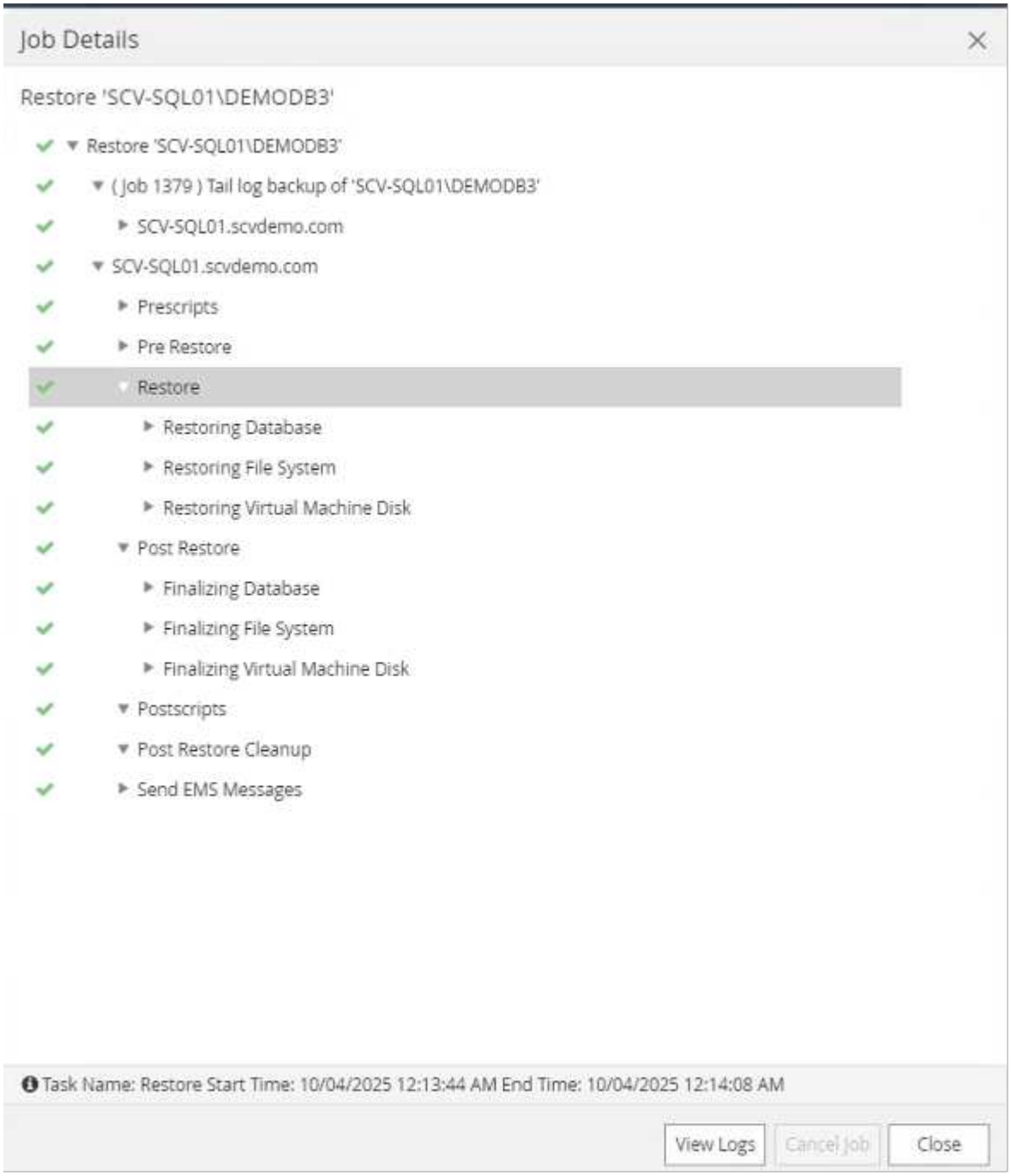
5. 從清單選項中選擇您希望資料庫在還原後達到的狀態，然後選擇「下一步」。



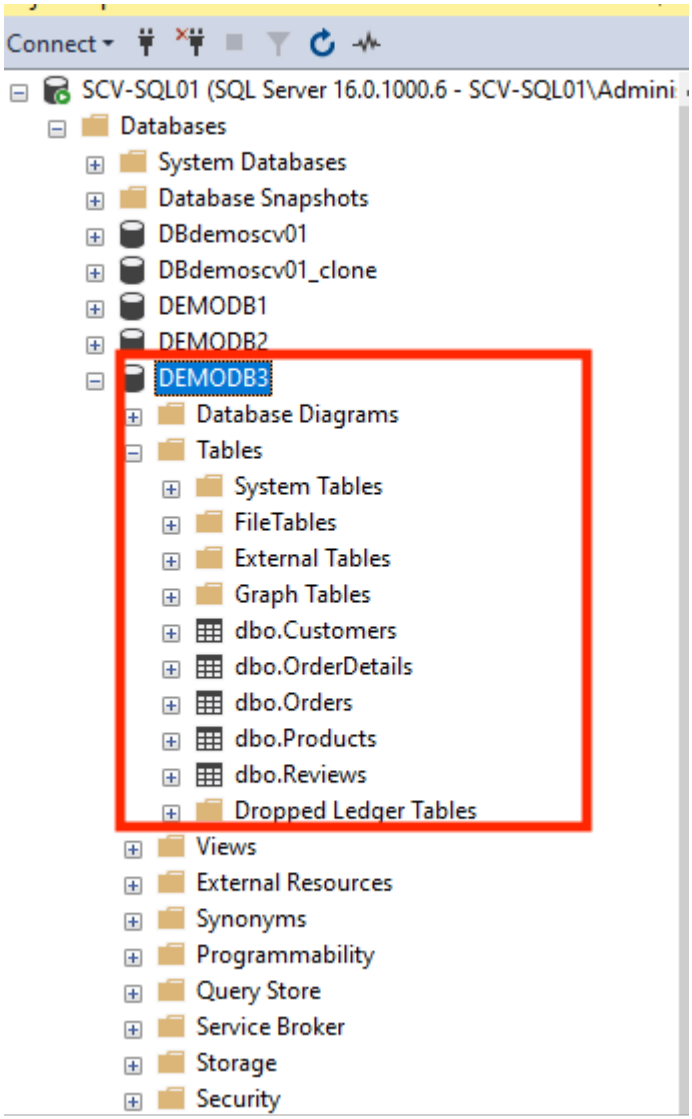
6. 在摘要頁面上，選取「完成」。


Restore
1 Restore scope
2 Recovery Type
3 Pre Ops
4 Post Ops
5 Notification
6 Summary
Summary
Backup name
SCV-SQL01_1_SCV-SQL01_10-03-2025_21.30.00.2159
Backup type
Full backup
Backup date
10/03/2025 9:30:06 PM
Restore type
In Place
Restore logs
Until 10/3/2025 11:45:05 PM
Send email
No
Previous
Finish

7. 监控工作直至完成。



8. 確認已刪除的表已成功還原。



結論

在本文件中，我們提供了詳細的逐步指導，說明如何部署、配置和使用 SCV 和"SnapCenter Plug-in for SQL Server（SCSQL）"，同時使用 FSx for ONTAP 作為 Amazon EVS 叢集的補充資料存放區。

結論

總而言之，當使用 FSx for ONTAP 來最佳化 Amazon EVS 部署的 TCO 時，SCV 提供了一種簡單且有效率的虛擬機器備份方法。由於它依賴 Snapshot 複本，因此可以無縫快速地備份和還原虛擬機器，而 Snapshot 複本的建立只需幾秒鐘即可完成。

"立即免費試用適用於 VMware 的 SnapCenter 插件"。

NetApp適用於 Azure/AVS

NetApp的 Azure AVS 功能

進一步了解NetApp為 Azure VMware 解決方案 (AVS) 帶來的功能 - 從NetApp作為來賓連接儲存裝置或補充 NFS 資料儲存到遷移工作流程、擴展/爆發到雲端、備份/還原和災難復原。

透過選擇以下選項跳到所需內容的部分：

- "在 Azure 中設定 AVS"
- "NetApp的 AVS 儲存選項"
- "NetApp /VMware 雲端解決方案"

在 Azure 中設定 AVS

與本地一樣，規劃基於雲端的虛擬化環境對於成功創建虛擬機器和遷移的生產就緒環境至關重要。

本部分介紹如何設定和管理 Azure VMware 解決方案，並將其與用於連接NetApp儲存裝置的可用選項結合使用。

來賓內儲存是將Cloud Volumes ONTAP連接到 Azure VMware 解決方案的唯一支援方法。

設定過程可分為以下步驟：

- 註冊資源提供者並建立私有雲
- 連接到新的或現有的 ExpressRoute 虛擬網路網關
- 驗證網路連線並存取私有雲

查看詳細信息"AVS設定步驟"。

NetApp的 AVS 儲存選項

NetApp儲存可以在 Azure AVS 中以多種方式使用 - 既可以作為猜測連接，也可以作為補充 NFS 資料儲存。

請訪問"支援的NetApp儲存選項"了解更多。

Azure 支援以下配置的NetApp儲存體：

- Azure NetApp Files(ANF) 作為來賓連接儲存
- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- Azure NetApp Files(ANF) 作為補充 NFS 資料存儲

查看詳細信息"AVS 的來賓連線儲存選項"。查看詳細信息"AVS 的補充 NFS 資料儲存選項"。

解決方案用例

透過NetApp和 VMware 雲端解決方案，許多用例都可以在 Azure AVS 中輕鬆部署。針對 VMware 定義的每個雲端區域都定義了這些用例：

- 保護（包括災難復原和備份/還原）
- 延長
- 遷移

"瀏覽適用於 Azure AVS 的NetApp解決方案"

保護 **Azure/AVS** 上的工作負載

使用 **ANF** 和 **JetStream** 進行災難復原

災難復原到雲端是一種具有彈性且經濟高效的方法，可以保護工作負載免受網站中斷和資料損壞事件（例如勒索軟體）的影響。使用 VMware VAIO 框架，可以將本機 VMware 工作負載複製到 Azure Blob 儲存體並進行恢復，從而實現最少或幾乎沒有資料遺失以及接近零的 RTO。

JetStream DR 可用於無縫恢復從本地複製到 AVS 以及特別是Azure NetApp Files 的工作負載。它透過使用災難復原站點的最少資源和經濟高效的雲端儲存來實現經濟高效的災難復原。 JetStream DR 透過 Azure Blob Storage 自動還原到 ANF 資料儲存。 JetStream DR 根據網路映射將獨立的虛擬機器或相關虛擬機器群組還原到復原站點基礎架構中，並提供時間點復原以進行勒索軟體保護。

本文檔可協助您了解 JetStream DR 的操作原理及其主要組件。

▼ 解決方案部署概述

1. 在本地資料中心安裝 JetStream DR 軟體。
    a. 從 Azure 市場 (ZIP) 下載 JetStream DR 軟體包，並在指定叢集中部署 JetStream DR MSA (OVA)。
    b. 使用 I/O 過濾器包配置叢集（安裝 JetStream VIB）。
    c. 在與 DR AVS 叢集相同的區域中設定 Azure Blob（Azure 儲存帳戶）。
    d. 部署 DRVA 設備並分配複製日誌磁碟區（來自現有資料儲存或共用 iSCSI 儲存的 VMDK）。
    e. 建立受保護的網域（相關 VM 群組）並指派 DRVA 和 Azure Blob 儲存體/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. 使用運行命令安裝和設定 JetStream DR。
    b. 新增相同的 Azure Blob 容器並使用掃描網域選項發現網域。
    c. 部署所需的 DRVA 設備。
    d. 使用可用的 vSAN 或 ANF 資料儲存建立複製日誌卷。
    e. 導入受保護的網域並配置 RocVA（恢復 VA）以使用 ANF 資料儲存進行 VM 放置。
    f. 選擇適當的故障轉移選項並開始對接近零 RTO 域或虛擬機器進行持續補水。
3. 在災難事件發生期間，觸發故障轉移到指定 AVS DR 站點中的Azure NetApp Files資料儲存。
4. 在受保護站點恢復後，呼叫故障回復到受保護站點。在開始之前，請確保滿足本 "關聯"並執行 JetStream Software 提供的頻寬測試工具 (BWT) 來評估與 JetStream DR 軟體一起使用時 Azure Blob 儲存體及其複製頻寬的潛在效能。滿足先決條件（包括連接性）後，設定並訂閱 JetStream DR for AVS "Azure 市場"。下載軟體包後，繼續執行上面所述的安裝過程。

在規劃和啟動對大量虛擬機器（例如 100 多個）的保護時，請使用 JetStream DR 自動化工具包中的容量規劃工具 (CPT)。提供要保護的虛擬機器清單及其 RTO 和復原群組首選項，然後執行 CPT。

CPT 執行以下功能：

- 根據 RTO 將虛擬機器組合到保護域。
- 定義 DRVA 及其資源的最佳數量。
- 估計所需的複製頻寬。
- 識別複製日誌卷特徵（容量、頻寬等）。
- 估算所需的物件儲存容量等等。

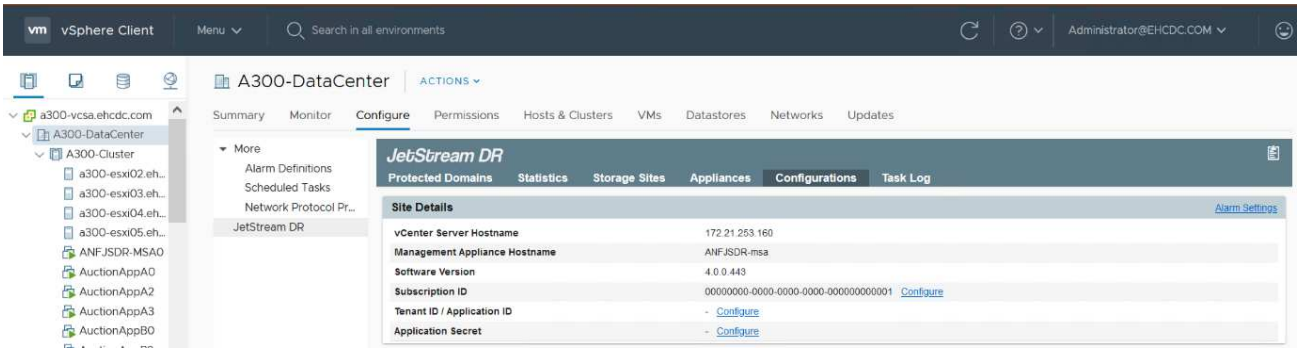
規定的域的數量和內容取決於各種 VM 特性，例如平均 IOPS、總容量、優先順序（定義故障轉移順序）、RTO 等。

在本地資料中心安裝 **JetStream DR**

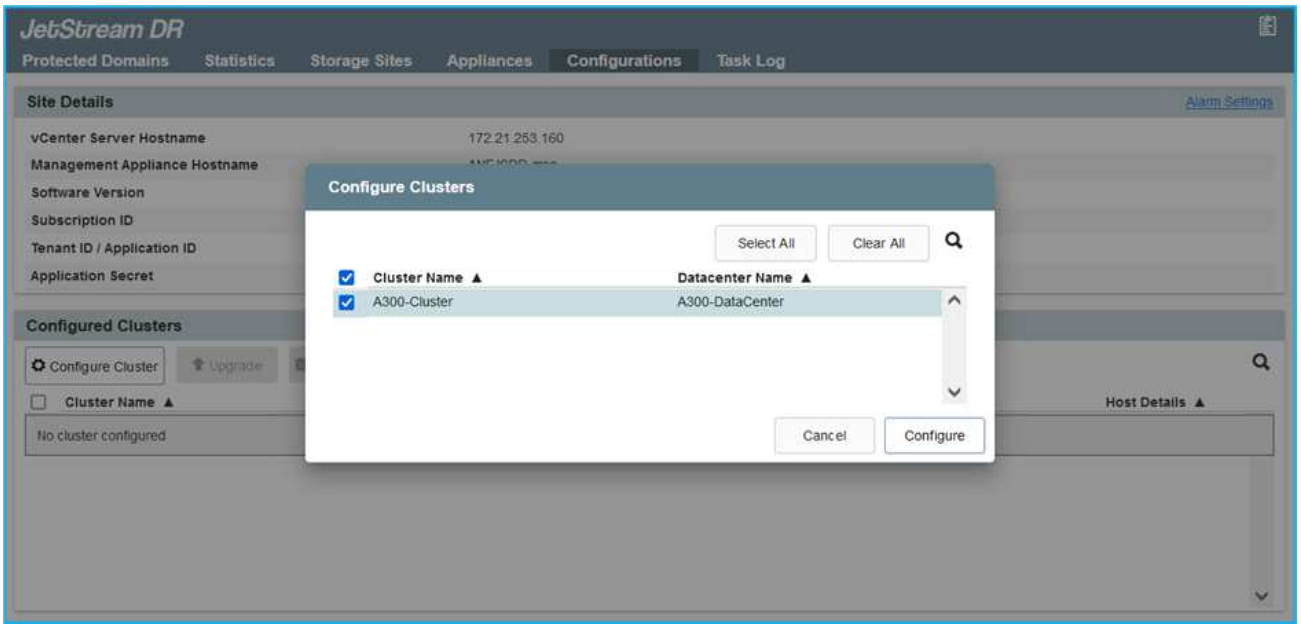
JetStream DR 軟體由三個主要元件組成：JetStream DR 管理伺服器虛擬裝置 (MSA)、DR 虛擬裝置 (DRVA) 和主機元件（I/O 篩選器套件）。 MSA 用於在運算叢集上安裝和設定主機元件，然後管理 JetStream DR 軟體。以下列表提供了安裝過程的高級描述：

▼ 如何為本地安裝 **JetStream DR**

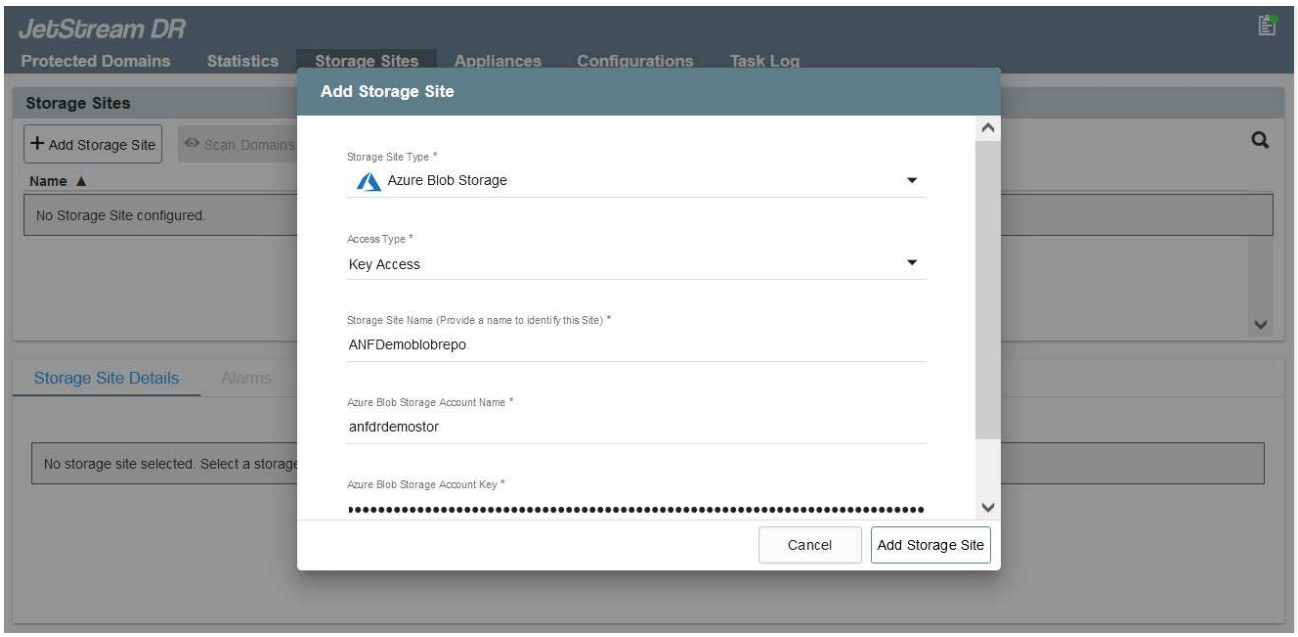
1. 檢查先決條件。
2. 運行容量規劃工具可取得資源和配置建議（可選，但建議用於概念驗證試驗）。
3. 將 JetStream DR MSA 部署到指定叢集中的 vSphere 主機。
4. 在瀏覽器中使用其 DNS 名稱啟動 MSA。
5. 向 MSA 註冊 vCenter 伺服器。若要執行安裝，請完成以下詳細步驟：
6. 部署 JetStream DR MSA 並註冊 vCenter Server 後，使用 vSphere Web Client 存取 JetStream DR 外掛程式。這可以透過導覽至資料中心 > 配置 > JetStream DR 來完成。



7. 從 JetStream DR 介面中，選擇適當的叢集。



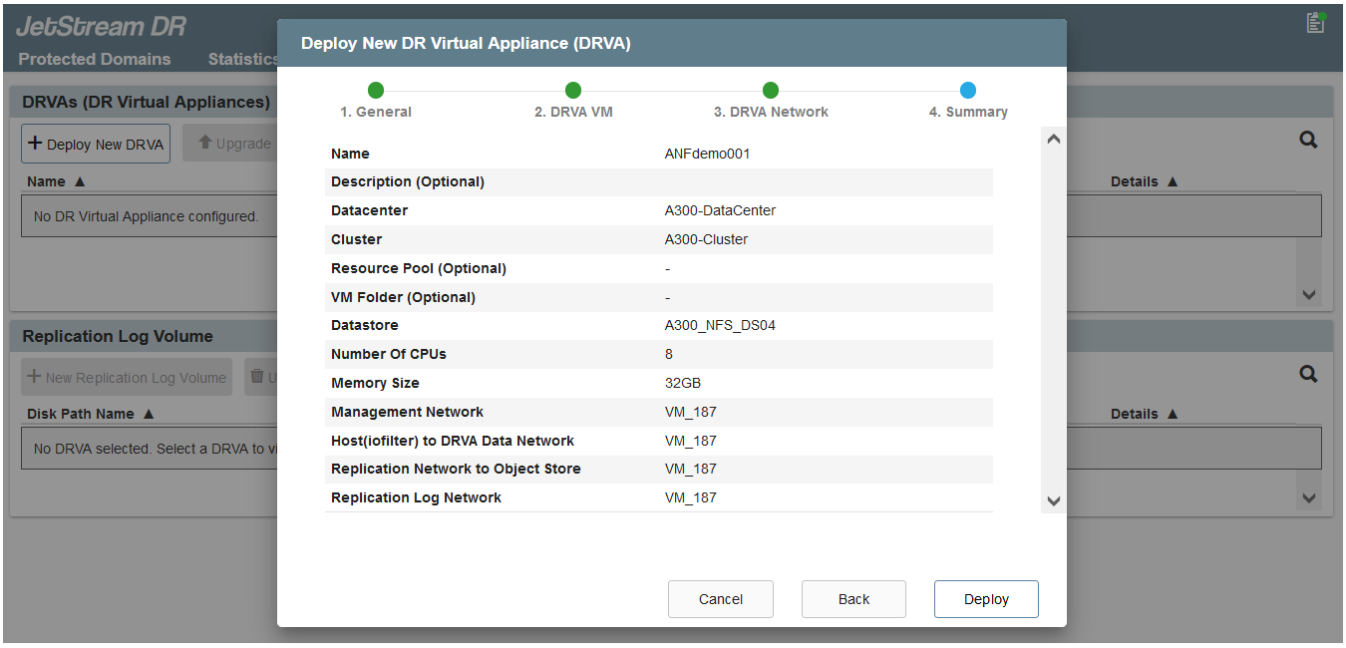
8. 使用 I/O 篩選器包配置叢集。



9. 新增位於復原站台的 Azure Blob 儲存體。
10. 從設備選項卡部署 DR 虛擬設備 (DRVA)。

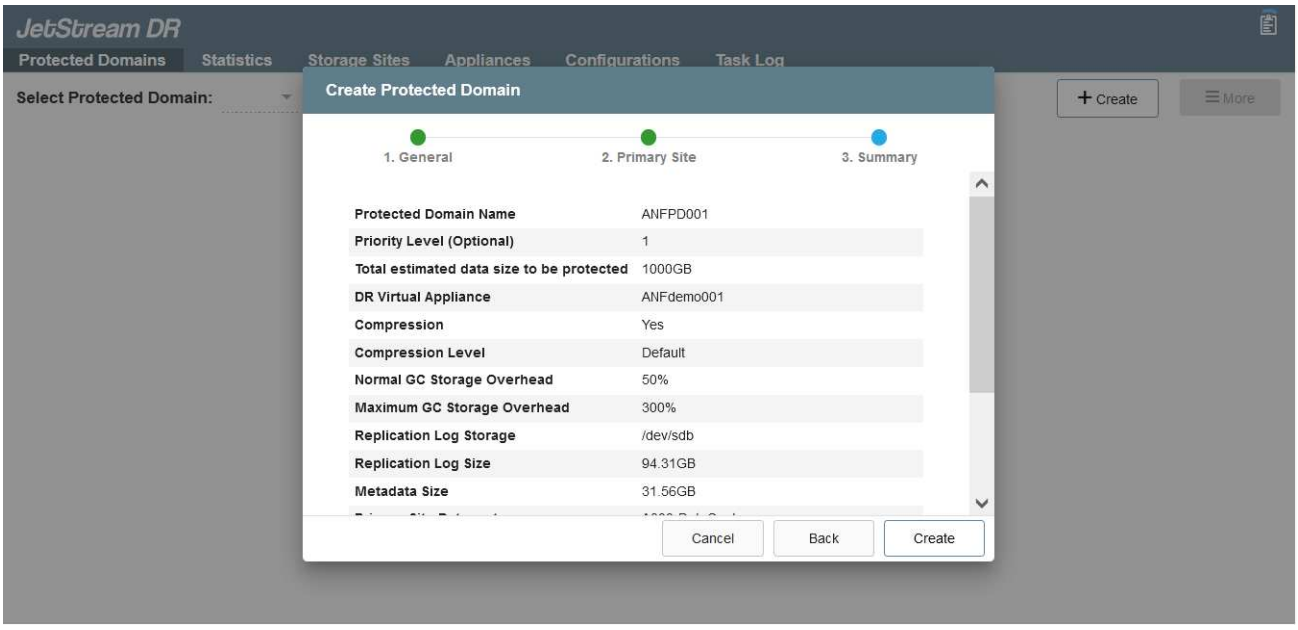
> DRVA 可以由 CPT 自動創建，但對於 POC 試驗，我們建議手動配置和運行 DR 週期（啟動保護 > 故障轉移 > 故障恢復）。

JetStream DRVA 是一種虛擬設備，可促進資料複製過程中的關鍵功能。受保護的叢集必須至少包含一個 DRVA，並且通常每個主機配置一個 DRVA。每個 DRVA 可以管理多個受保護域。



在此範例中，為 80 台虛擬機器建立了 4 個 DRVA。

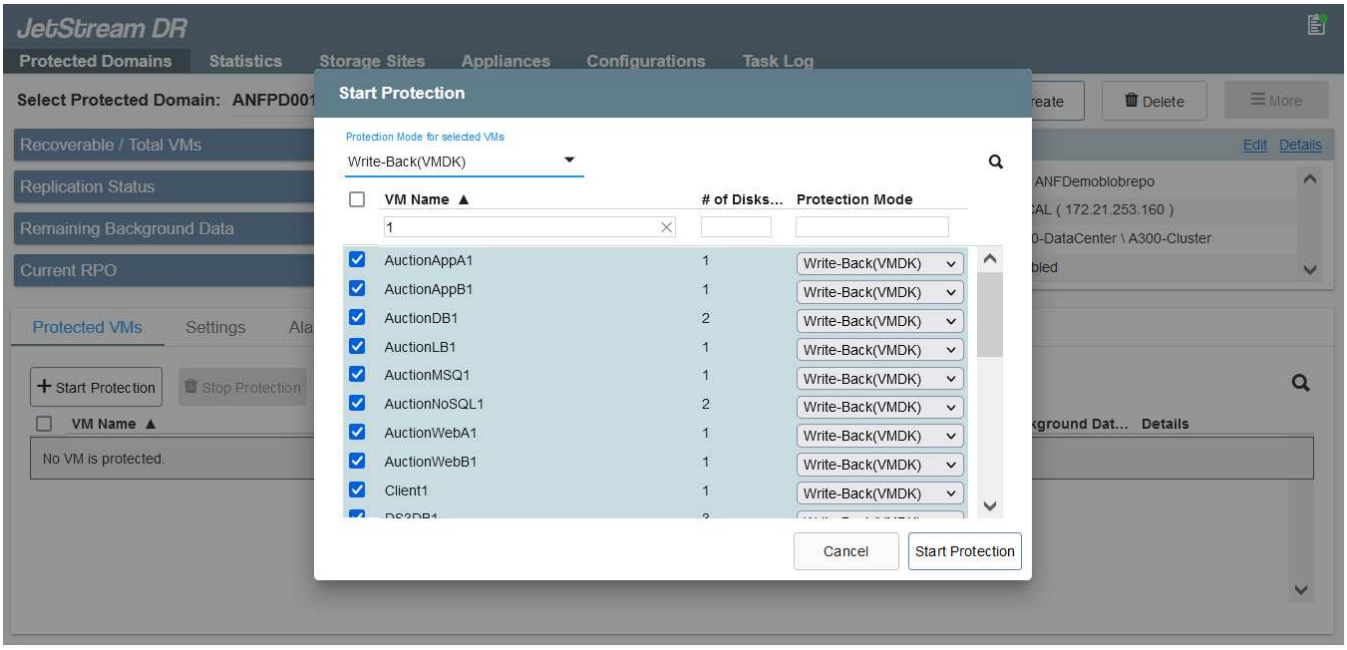
1. 使用來自可用資料儲存或獨立共用 iSCSI 儲存池的 VMDK 為每個 DRVA 建立複製日誌磁碟區。
2. 在「受保護的網域」標籤中，使用有關 Azure Blob 儲存站台、DRVA 執行個體和複製日誌的資訊建立所需數量的受保護網域。受保護域定義了叢集內的特定虛擬機或一組虛擬機，這些虛擬機受到共同保護，並分配了故障轉移/故障回復操作的優先順序。



3. 選擇需要保護的虛擬機，啟動受保護域的虛擬機保護。這將開始將資料複製到指定的 Blob 儲存。

驗證受保護域中的所有虛擬機器是否使用相同的保護模式。

寫回（VMDK）模式可以提供更高的效能。



驗證複製日誌卷是否放置在高效能儲存上。

> 可以設定故障轉移運作手冊來對虛擬機器進行分組（稱為復原群組）、設定啟動順序以及修改 CPU/記憶體設定以及 IP 配置。

使用運行命令在 **Azure VMware** 解決方案私有雲中安裝 **JetStream DR for AVS**

恢復站點 (AVS) 的最佳實踐是提前創建一個三節點的試點燈叢集。這允許預先配置恢復站點基礎設施，包括以下項目：

- 目標網路段、防火牆、DHCP 和 DNS 等服務等等。
- 為 AVS 安裝 JetStream DR
- 將 ANF 卷配置為資料存儲，並且更多 JetStream DR 支援關鍵任務域的近零 RTO 模式。對於這些網域，應該預先安裝目標儲存。在這種情況下，ANF 是建議的儲存類型。

> 應在 AVS 叢集上配置包括段創建在內的網路配置以滿足本機要求。

根據 SLA 和 RTO 要求，可以使用連續故障轉移或常規（標準）故障轉移模式。對於接近零的 RTO，應在恢復站點開始持續補液。

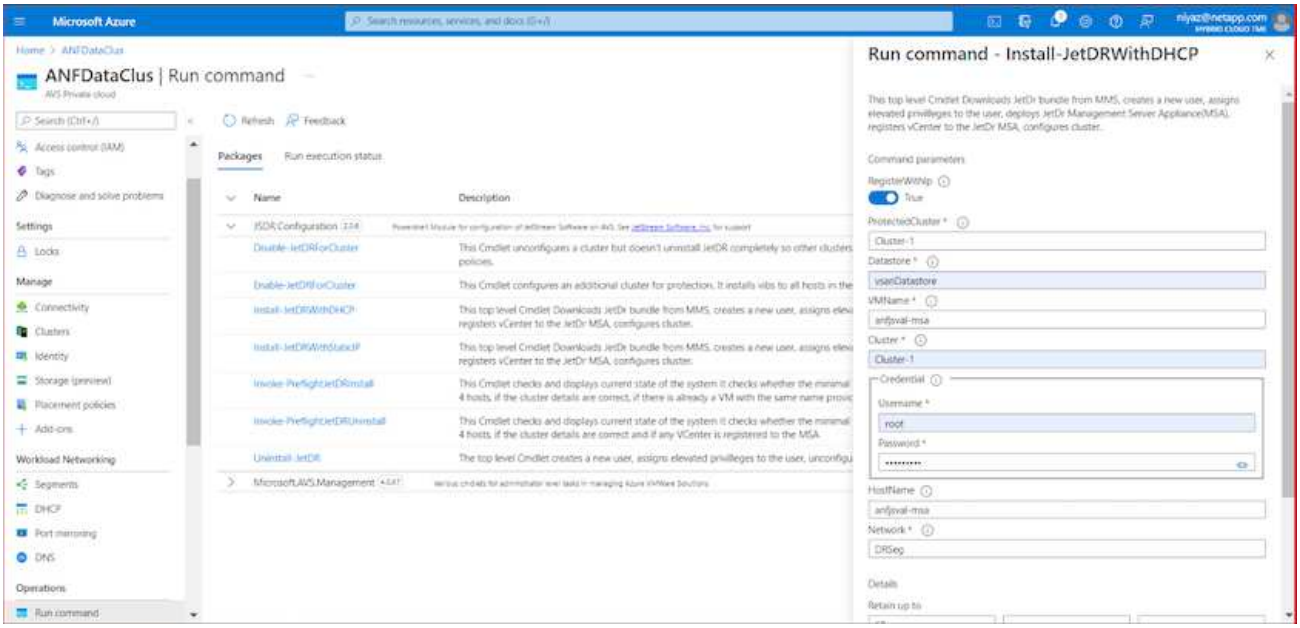
▼ 如何在私有雲中安裝 **JetStream DR for AVS**

若要在 Azure VMware 解決方案私有雲上安裝 JetStream DR for AVS，請完成下列步驟：

1. 從 Azure 入口網站前往 Azure VMware 解決方案，選擇私有雲，然後選擇執行命令> 套件> JSDR.Configuration。

> Azure VMware 解決方案中的預設 CloudAdmin 使用者沒有足夠的權限來為 AVS 安裝 JetStream DR。 Azure VMware 解決方案透過呼叫 JetStream DR 的 Azure VMware 解決方案來執行指令，實現了 JetStream DR 的簡化和自動化安裝。

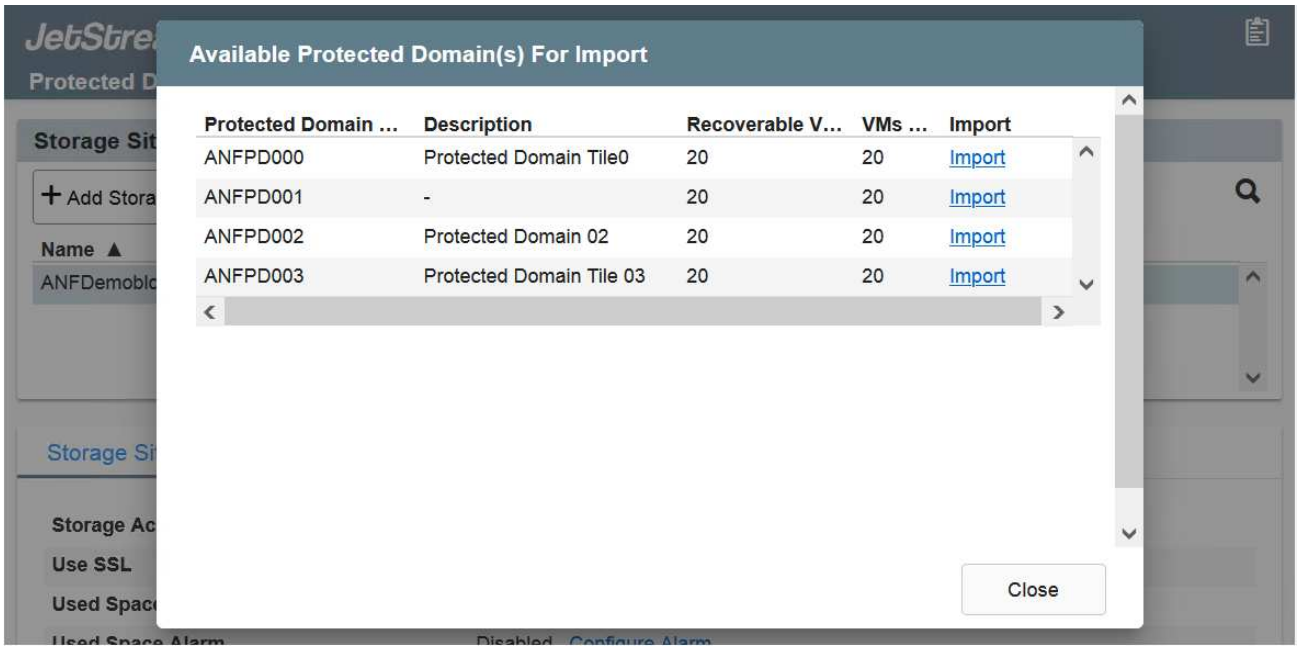
以下螢幕截圖顯示了使用基於 DHCP 的 IP 位址的安裝。



2. JetStream DR for AVS 安裝完成後，刷新瀏覽器。若要存取 JetStream DR UI，請前往 SDDC 資料中心 > 設定 > JetStream DR。



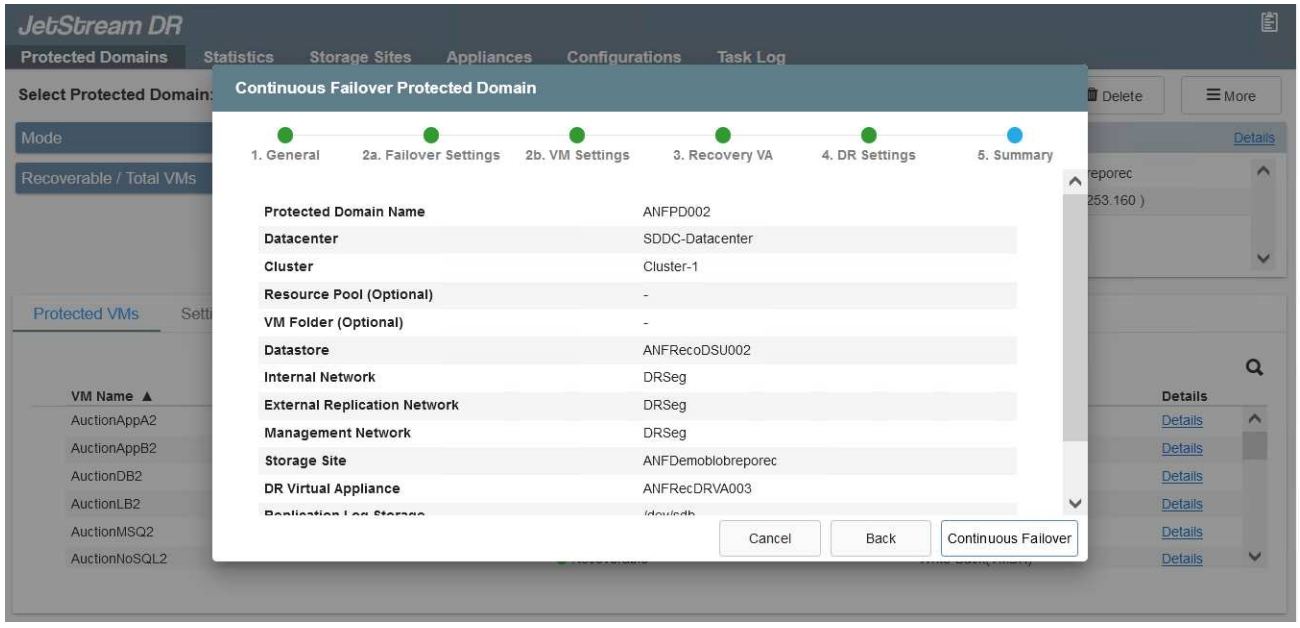
3. 從 JetStream DR 介面，新增用於保護本機叢集的 Azure Blob 儲存帳戶作為儲存站點，然後執行掃描網域選項。



4. 導入受保護域後，部署 DRVA 設備。在此範例中，使用 JetStream DR UI 從復原站台手動啟動連續補水。

> 這些步驟也可以使用 CPT 建立的計劃自動執行。

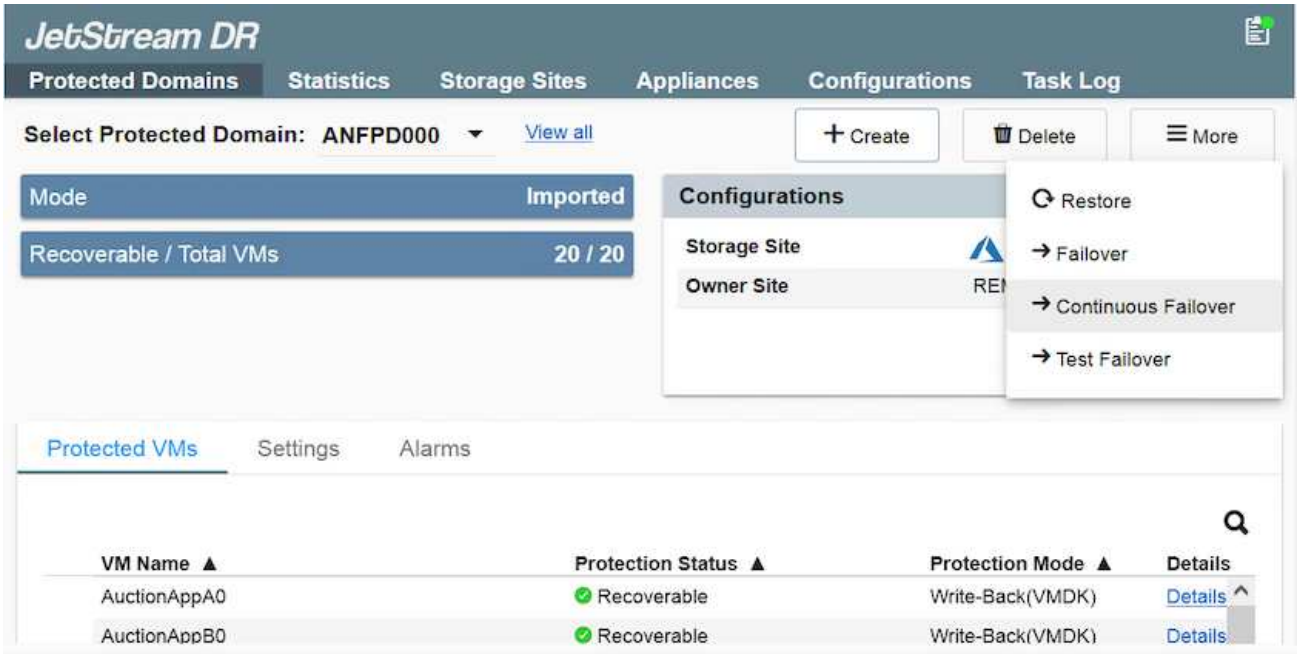
5. 使用可用的 vSAN 或 ANF 資料儲存建立複製日誌卷。
6. 導入受保護的網域並配置恢復 VA 以使用 ANF 資料儲存進行 VM 放置。



> 確保所選網段上啟用了 DHCP 並且有足夠的可用 IP。在網域名稱恢復期間，暫時使用動態 IP。每個復原的虛擬機器（包括持續補水）都需要一個單獨的動態 IP。恢復完成後，IP 被釋放並可重複使用。

7. 選擇適當的故障轉移選項（連續故障轉移或故障轉移）。在這個例子中，選擇了持續補水（持續故障轉移

）。



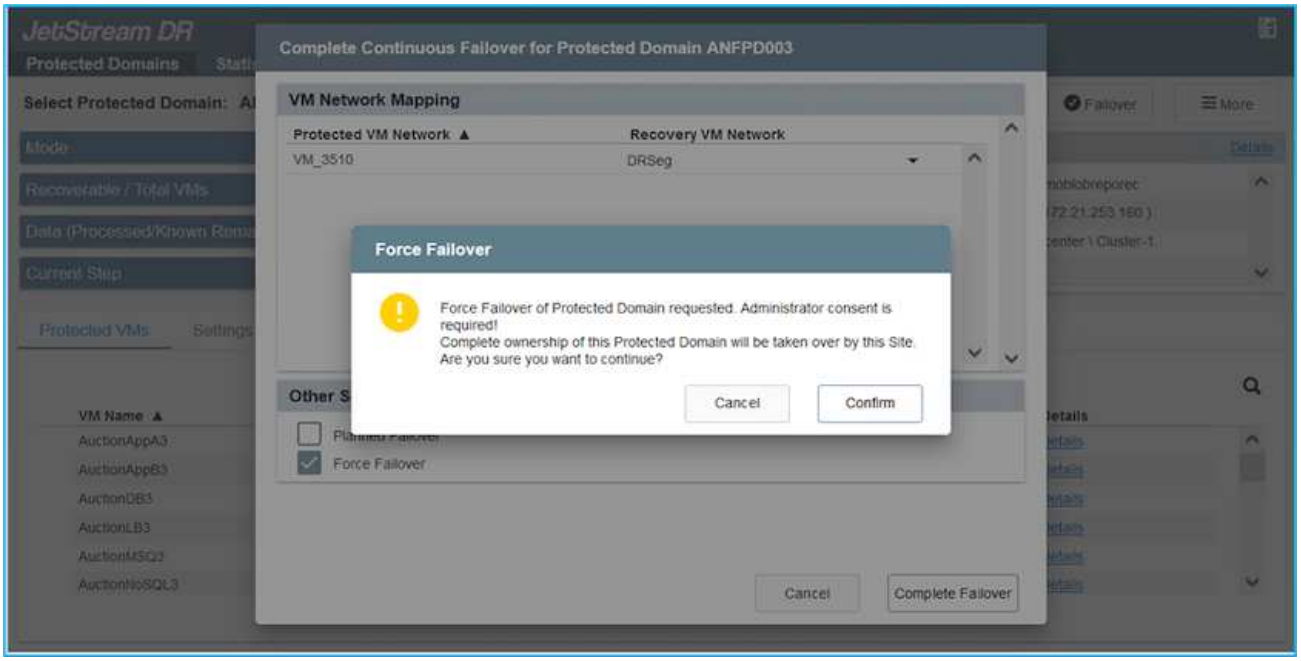
執行故障轉移/故障回復

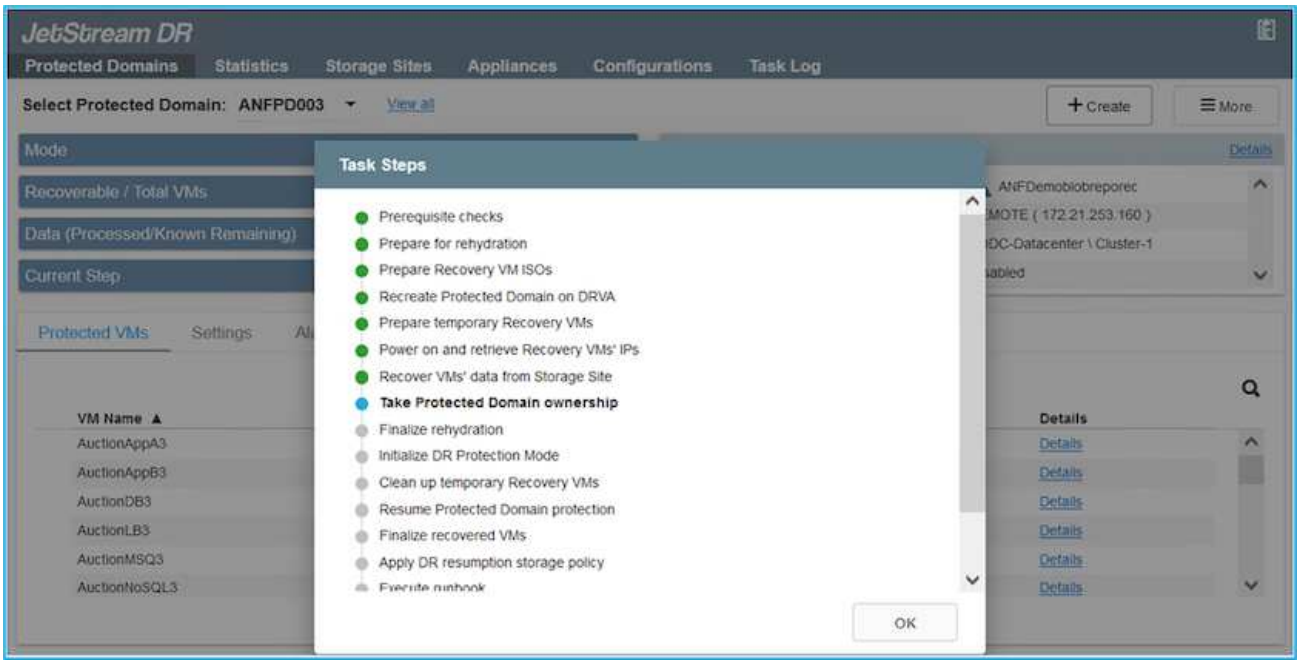
▼ 如何執行故障轉移/故障復原

1. 當本地環境受保護叢集發生災難（部分或全部故障）後，觸發故障轉移。

CPT 可用於執行故障轉移計劃，將虛擬機器從 Azure Blob 儲存體還原至 AVS 叢集復原站台。

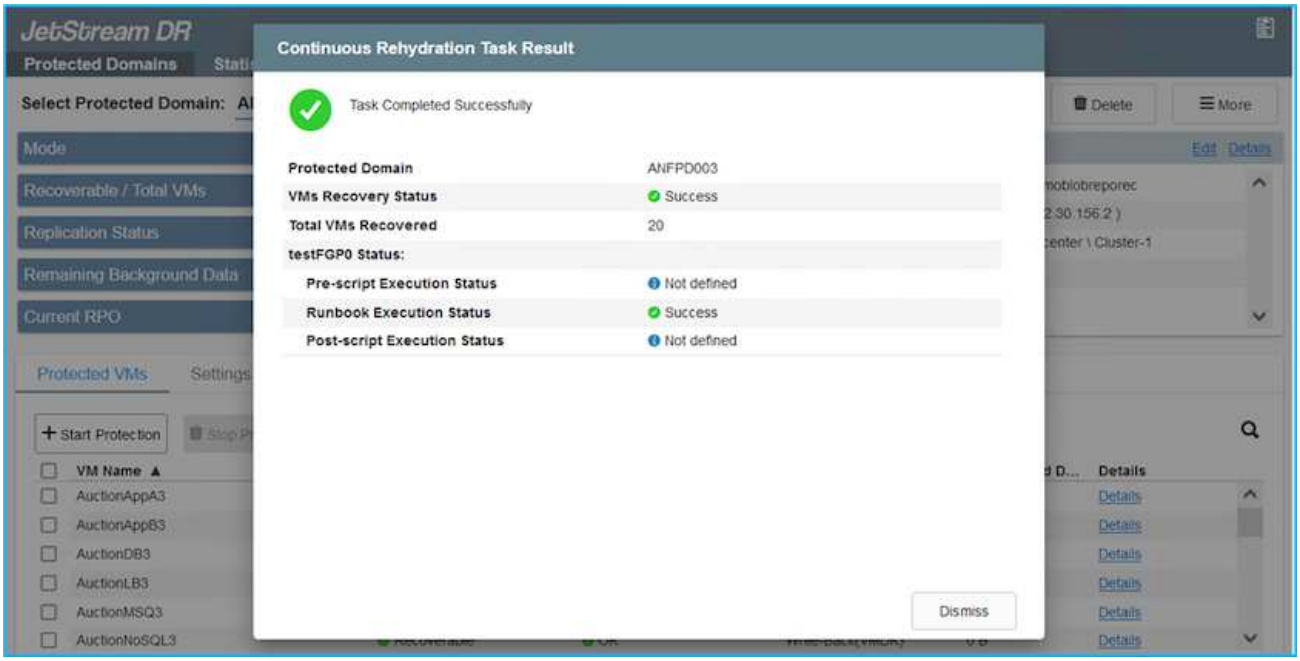
在 AVS 中啟動受保護的虛擬機器後進行故障轉移（用於連續或標準補水），保護將自動恢復，並且 JetStream DR 將繼續將其資料複製到 Azure Blob 儲存體中的相應/原始容器中。





工作列顯示故障轉移活動的進度。

2. 任務完成後，存取恢復的虛擬機，業務繼續正常進行。



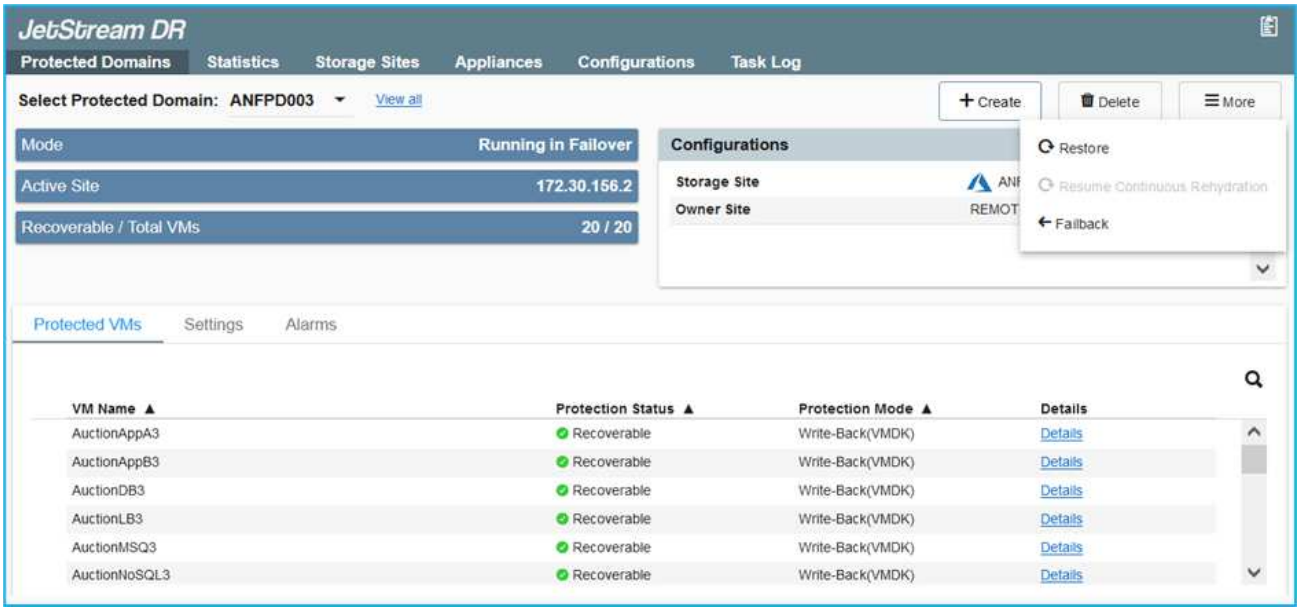
主站點重新啟動並運行後，即可執行故障復原。 VM 保護已恢復，應檢查資料一致性。

3. 恢復本地環境。根據災難事件的類型，可能需要復原和/或驗證受保護叢集的配置。如有必要，可能需要重新安裝 JetStream DR 軟體。

> 注意： `recovery_utility_prepare_failback`自動化工具包中提供的腳本可用於協助清理原始受保護網站中的任何過時的虛擬機器、網域資訊等。

4. 存取復原的本機環境，前往 Jetstream DR UI，然後選擇適當的受保護網域。受保護網站準備好故障復原

後，在 UI 中選擇故障復原選項。



CPT 產生的故障復原計畫也可用於啟動虛擬機器及其資料從物件儲存返回原始 VMware 環境。

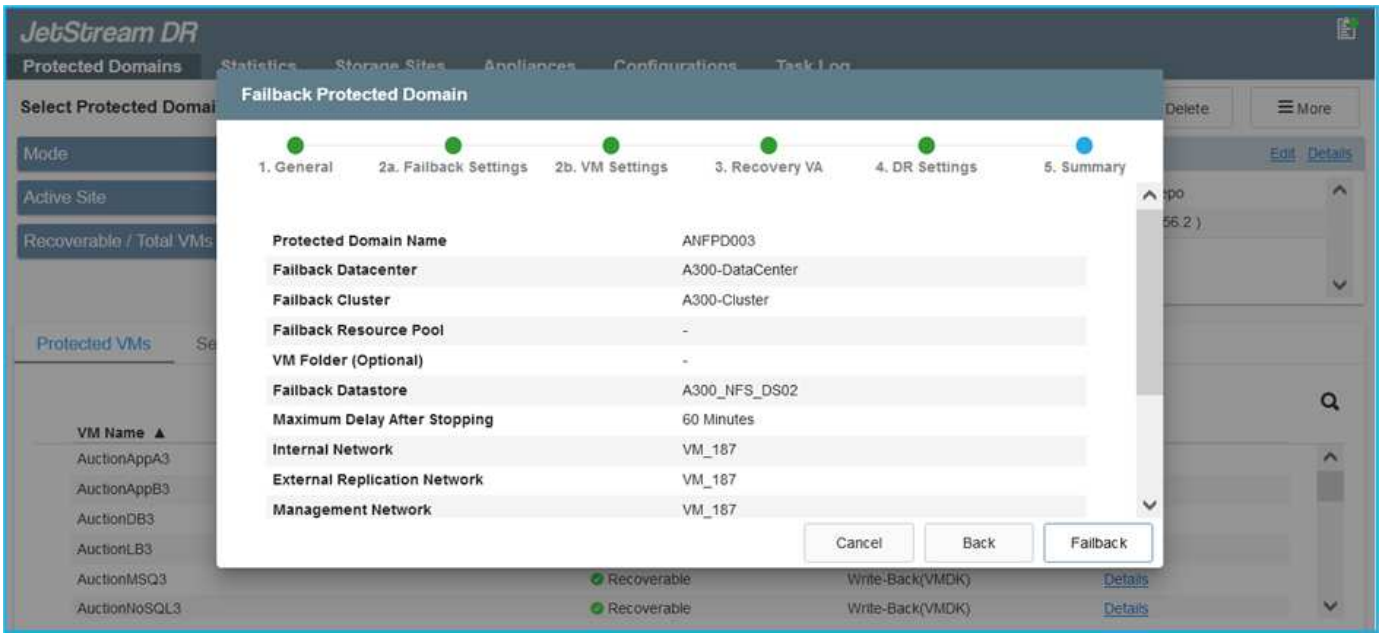
指定在復原站點中暫停虛擬機器並在受保護站點中重新啟動後的最大延遲。此時間包括停止故障轉移虛擬機器後完成複製的時間、清理復原站點的時間以及在受保護站點中重新建立虛擬機器的時間。 NetApp建議值為 10 分鐘。

完成故障復原流程，然後確認復原虛擬機器保護和資料一致性。

勒索軟體恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體來說，IT 組織很難確定安全的返回點，而且一旦確定，如何確保恢復的工作負載免受再次發生的攻擊（來自休眠惡意軟體或透過易受攻擊的應用程式）。

JetStream DR for AVS 與Azure NetApp Files資料儲存結合，可解決這些問題，讓組織可以從可用的時間點恢復，以便在需要時將工作負載恢復到功能齊全的隔離網路。恢復允許應用程式運行並相互通信，同時不會將它們暴露在南北流量中，從而為安全團隊提供一個安全的地方來執行取證和其他必要的補救措施。



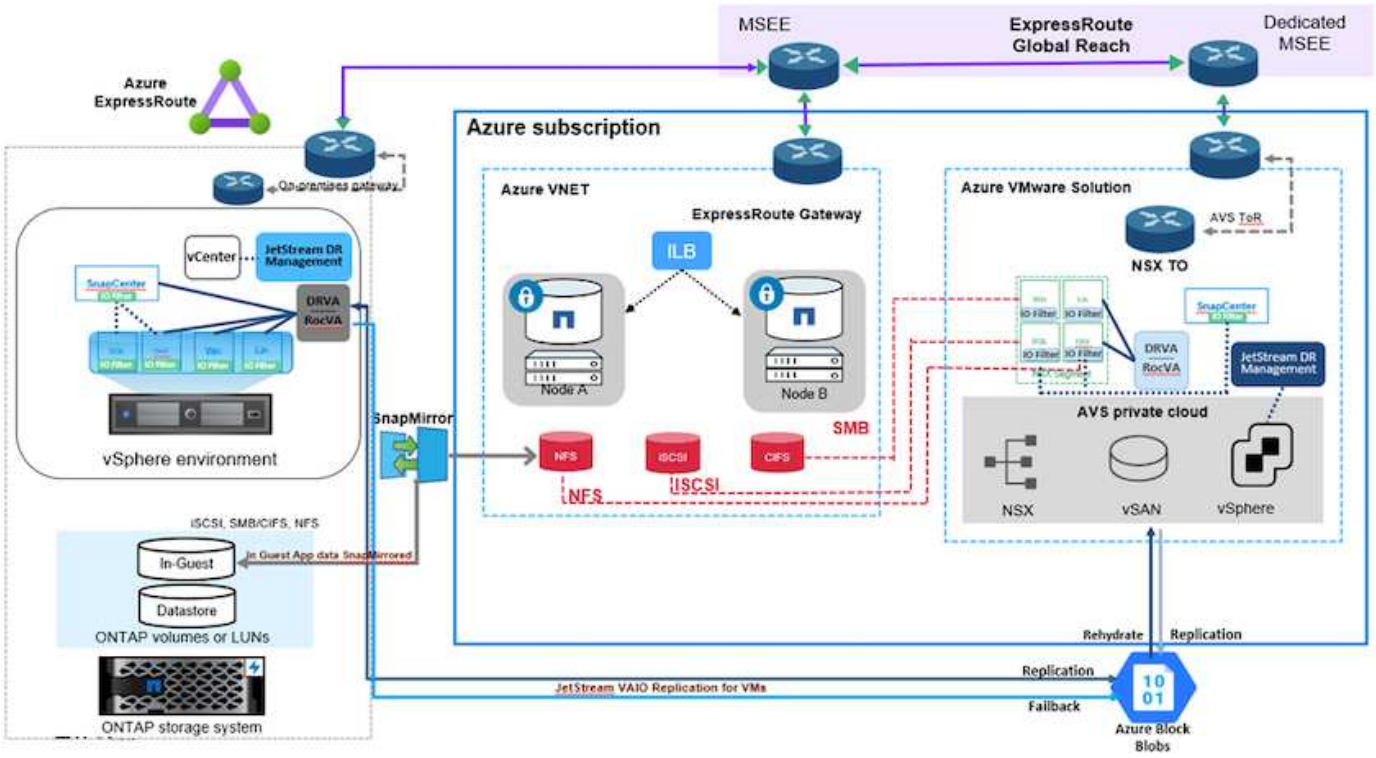
使用 **CVO** 和 **AVS**（來賓連接儲存）進行災難復原

雲端災難復原是一種具有彈性且經濟高效的方法，可保護工作負載免受網站中斷和勒索軟體等資料損壞事件的影響。透過NetApp SnapMirror，使用來賓連接儲存的本機 VMware 工作負載可以複製到在 Azure 中執行的NetApp Cloud Volumes ONTAP 。

概況

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
```

本文檔提供了使用NetApp SnapMirror、JetStream 和 Azure VMware 解決方案 (AVS) 設定和執行災難復原的逐步方法。



假設

本文檔重點介紹應用程式資料的客戶機內儲存（也稱為客戶機連線），我們假設本機環境使用SnapCenter進行應用程式一致性備份。

本文檔適用於任何第三方備份或復原解決方案。根據環境中使用的解決方案，遵循最佳實務來建立符合組織 SLA 的備份策略。

對於本機環境和 Azure 虛擬網路之間的連接，請使用快速路由全球覆蓋或具有 VPN 閘道的虛擬 WAN。應根據內部部署 vLAN 設計建立段。

將本機資料中心連接到 Azure 有多種選擇，因此我們無法在本文檔中概述特定的工作流程。請參閱 Azure 文檔，以了解適當的本地到 Azure 連線方法。

部署災難復原解決方案

解決方案部署概述

1. 確保使用SnapCenter備份應用程式資料並滿足必要的 RPO 要求。
2. 使用適當的訂閱和虛擬網路中的雲端管理器為Cloud Volumes ONTAP配置正確的執行個體大小。
   a. 為相關應用程式磁碟區設定SnapMirror 。
   b. 更新SnapCenter中的備份策略以在排程的作業之後觸發SnapMirror更新。
3. 在本地資料中心安裝 JetStream DR 軟體並啟動對虛擬機器的保護。
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，使用 Cloud Manager 中斷SnapMirror關係並觸發虛擬機器到Azure NetApp Files或指定 AVS DR 站點中的 vSAN 資料儲存的故障轉移。
    a. 重新連接應用程式虛擬機器的 ISCSI LUN 和 NFS 掛載。
6. 主站點恢復後，透過反向重新同步SnapMirror呼叫故障回復到受保護站點。

部署詳情

▼ 在 **Azure** 上設定 **CVO** 並將磁碟區複製到 **CVO**

第一步是在 Azure 上設定Cloud Volumes ONTAP （"關聯") 並以所需的頻率和快照保留將所需的磁碟區複製到Cloud Volumes ONTAP 。

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

▼ 配置 **AVS** 主機和 **CVO** 資料存取

部署 SDDC 時需要考慮的兩個重要因素是 Azure VMware 解決方案中 SDDC 叢集的大小以及保持 SDDC 服務的時間。災難復原解決方案的這兩個關鍵考慮因素有助於降低整體營運成本。 SDDC 最小可以只有三台主機，最大可以達到全面部署的多主機叢集。

部署 AVS 叢集的決定主要基於 RPO/RTO 要求。透過 Azure VMware 解決方案，可以及時配置 SDDC，為測試或實際災難事件做好準備。當您不處理災難時，及時部署的 SDDC 可以節省 ESXi 主機成本。然而，這種部署形式會在配置 SDDC 時影響 RTO 數小時。

最常見的部署選項是讓 SDDC 以始終開啟、指示燈亮起的操作模式運作。此選項佔用空間較小，僅需三個始終可用的主機，同時還透過為模擬活動和合規性檢查提供運行基線來加快恢復操作，從而避免生產站點和 DR 站點之間出現操作偏差的風險。當需要處理實際 DR 事件時，指示燈群集可以快速擴展到所需的等級。

若要設定 AVS SDDC（按需模式或指示燈模式），請參閱"在 Azure 上部署並配置虛擬化環境"。作為先決條件，請驗證在建立連線後，駐留在 AVS 主機上的客戶虛擬機器是否能夠使用來自Cloud Volumes ONTAP的資料。

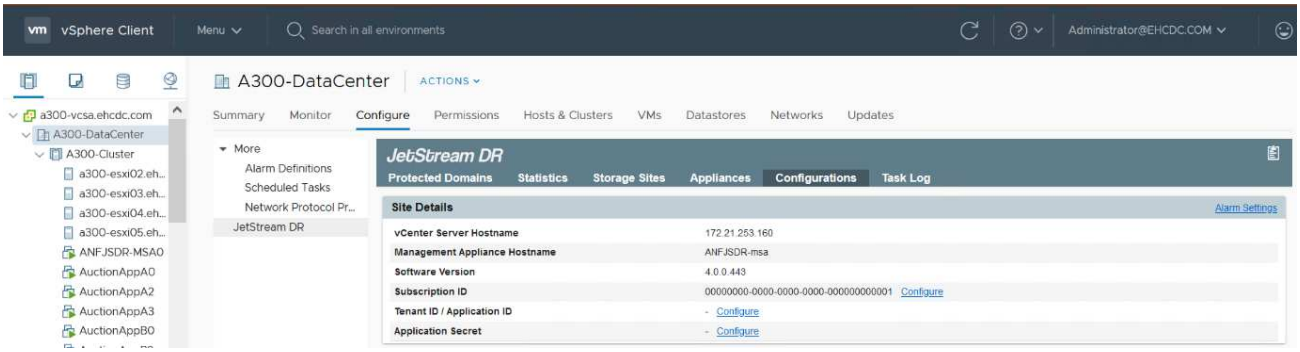
正確配置Cloud Volumes ONTAP和 AVS 後，開始設定 Jetstream，透過使用 VAIO 機制並利用SnapMirror將應用程式磁碟區複製到Cloud Volumes ONTAP，自動將本機工作負載還原到 AVS（具有應用程式 VMDK 的虛擬機器和具有客戶機內儲存的虛擬機器）。

▼ 在本地資料中心安裝 **JetStream DR**

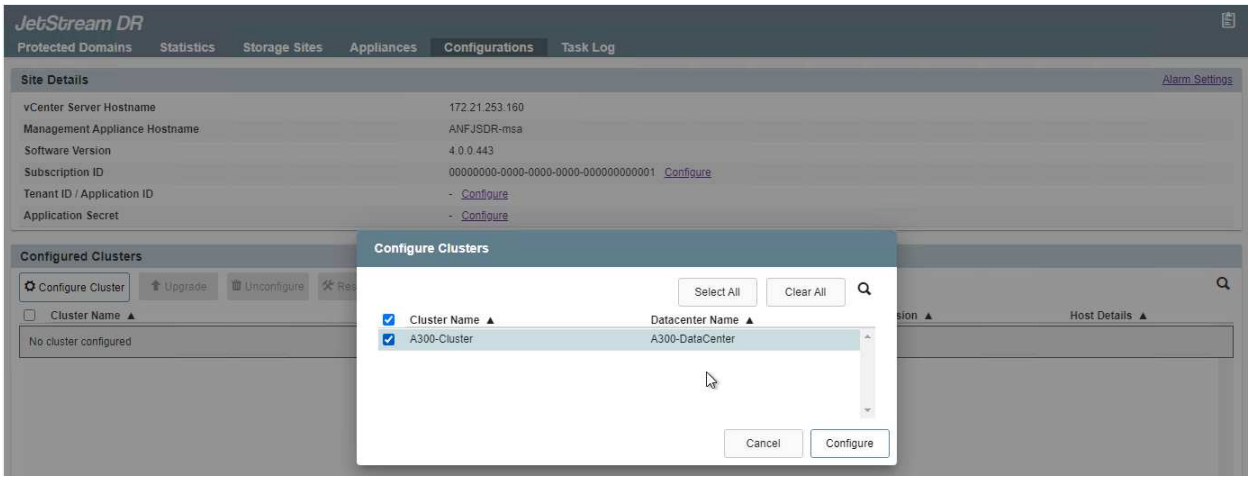
JetStream DR 軟體由三個主要元件組成：JetStream DR 管理伺服器虛擬設備 (MSA)、DR 虛擬設備 (DRVA) 和主機元件（I/O 過濾套件）。 MSA 用於在運算叢集上安裝和設定主機元件，然後管理 JetStream DR 軟體。安裝過程如下：

1. 檢查先決條件。
2. 運作容量規劃工具取得資源和配置建議。
3. 將 JetStream DR MSA 部署到指定叢集中的每個 vSphere 主機。

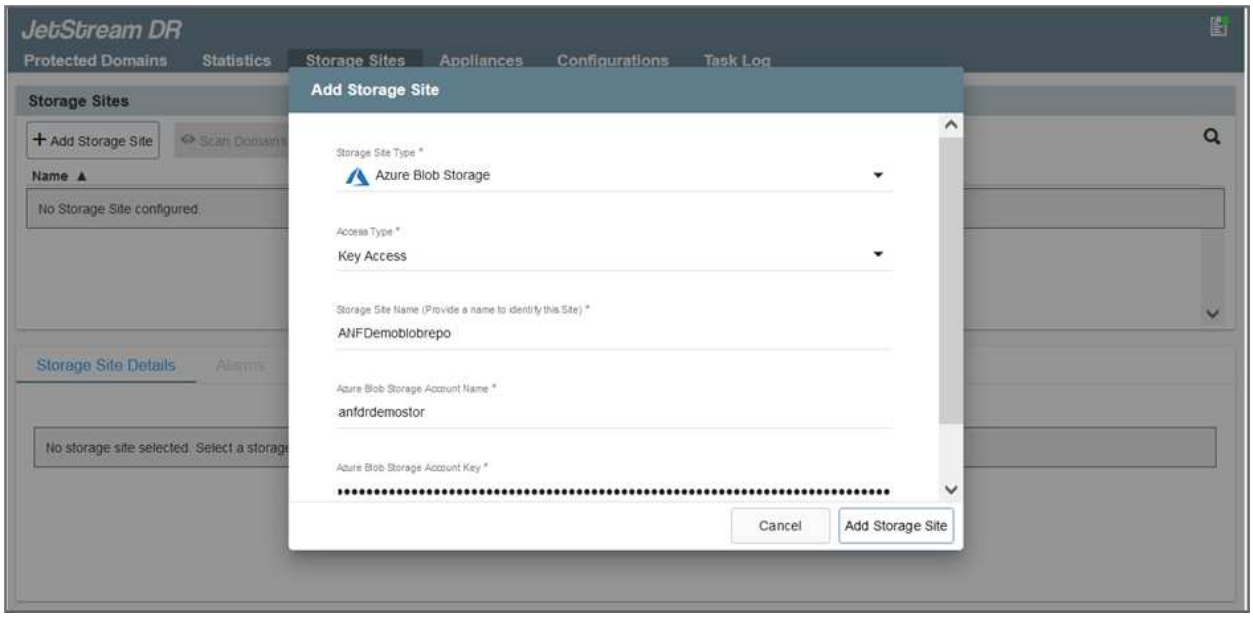
4. 在瀏覽器中使用其 DNS 名稱啟動 MSA。
5. 向 MSA 註冊 vCenter 伺服器。
6. 部署 JetStream DR MSA 並註冊 vCenter Server 後，使用 vSphere Web Client 導覽至 JetStream DR 外掛程式。這可以透過導覽至資料中心 > 配置 > JetStream DR 來完成。



7. 從 JetStream DR 介面完成以下任務：
   a. 使用 I/O 篩選器包配置叢集。

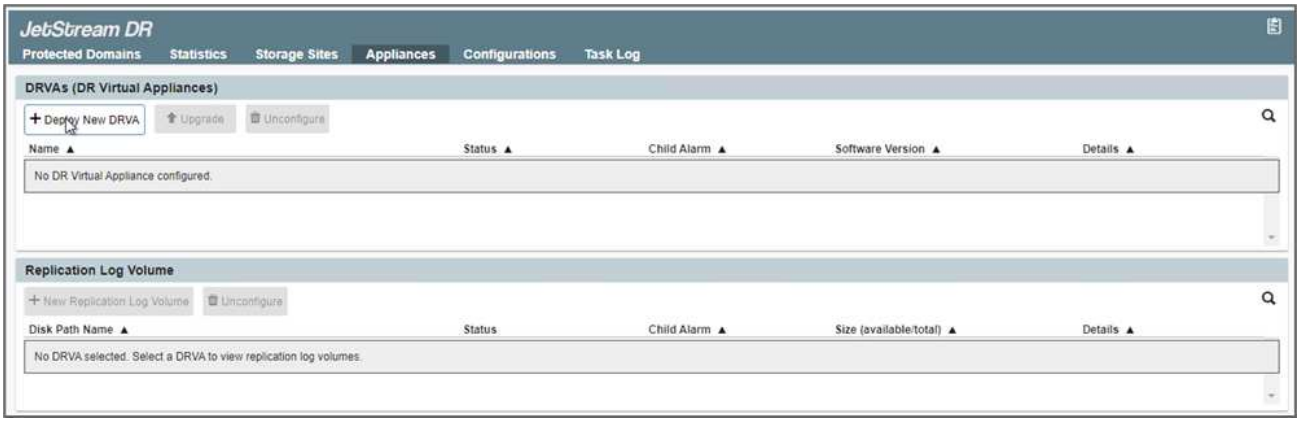


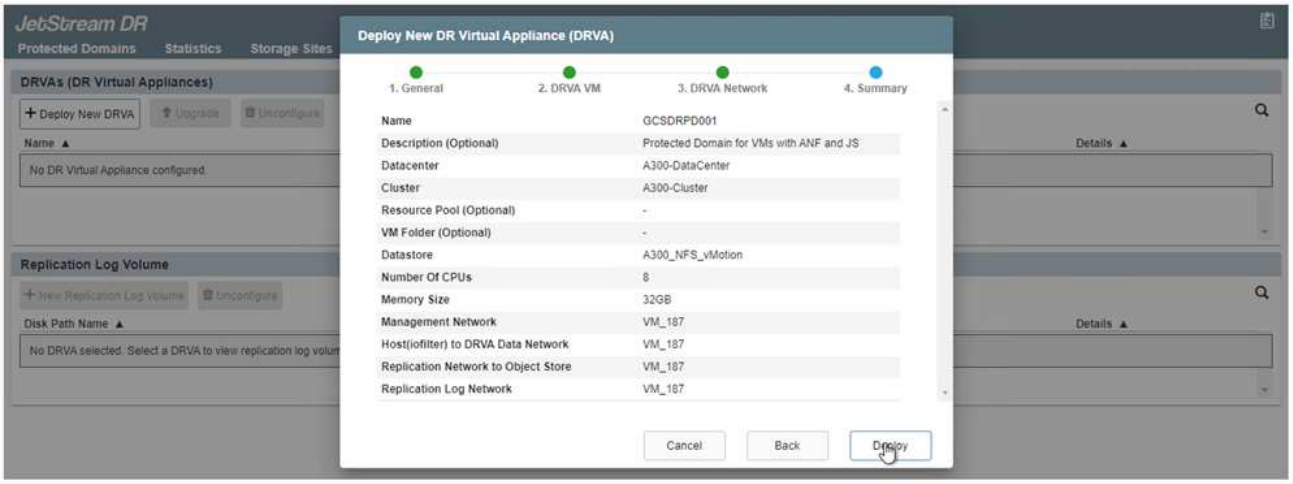
   b. 新增位於復原站台的 Azure Blob 儲存體。



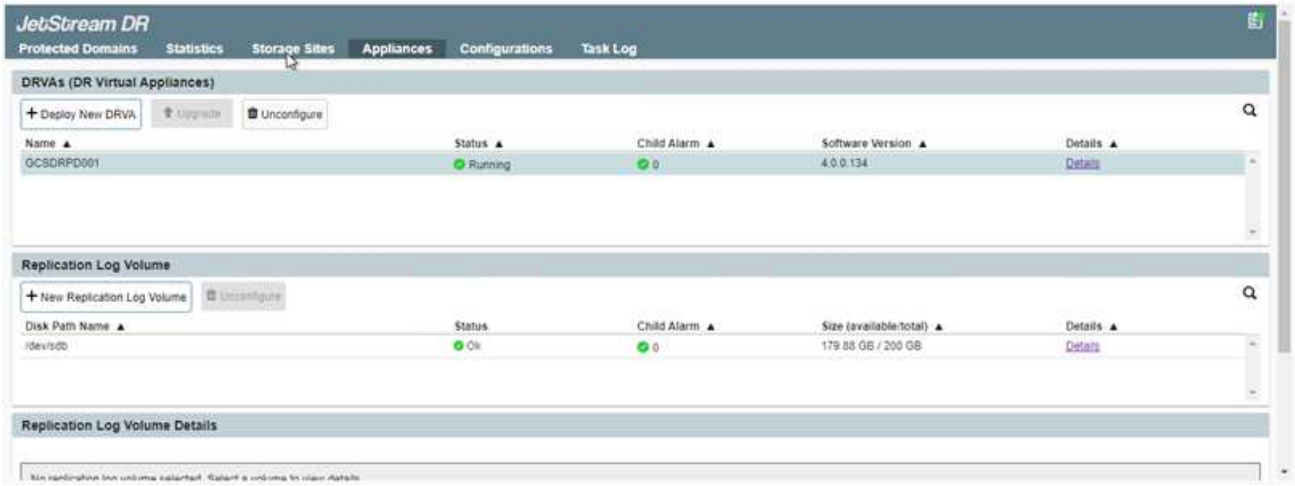
8. 從設備標籤部署所需數量的 DR 虛擬設備 (DRVA)。

   使用容量規劃工具來估計所需的 DRVA 數量。

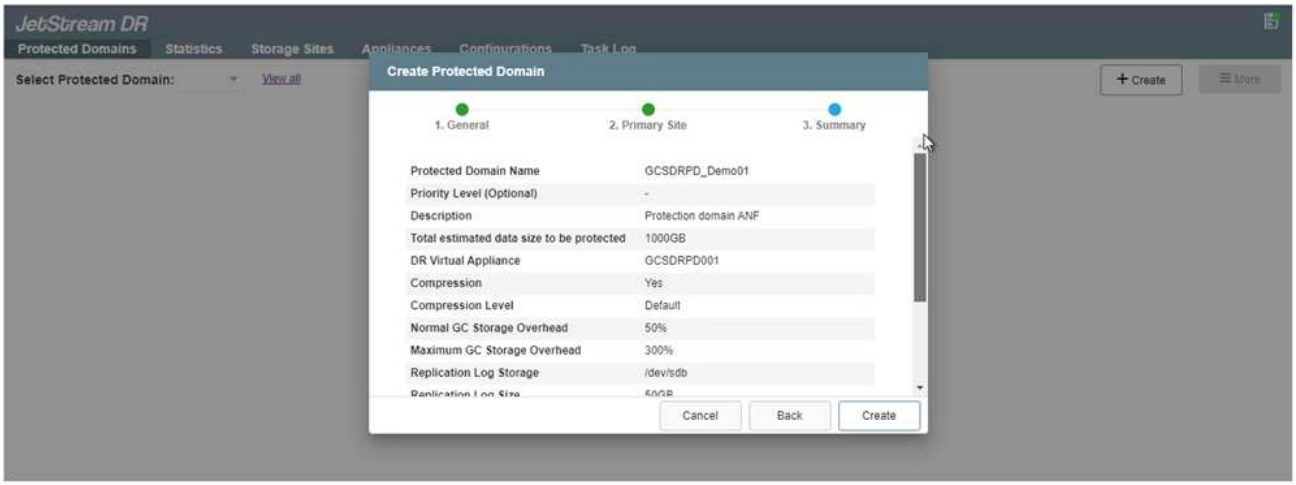


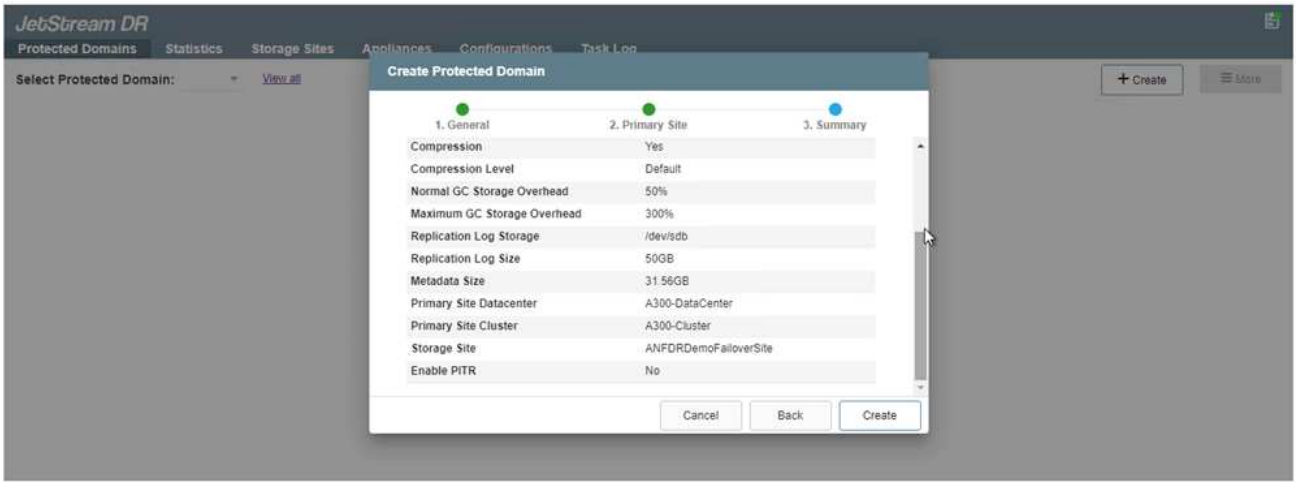


9. 使用來自可用資料儲存或獨立共用 iSCSI 儲存池的 VMDK 為每個 DRVA 建立複製日誌磁碟區。



10. 在「受保護的網域」標籤中，使用有關 Azure Blob 儲存站台、DRVA 執行個體和複製日誌的資訊建立所需數量的受保護網域。受保護域定義叢集內的特定虛擬機或一組應用程式虛擬機，這些虛擬機受到一起保護，並分配了故障轉移/故障回復操作的優先順序。

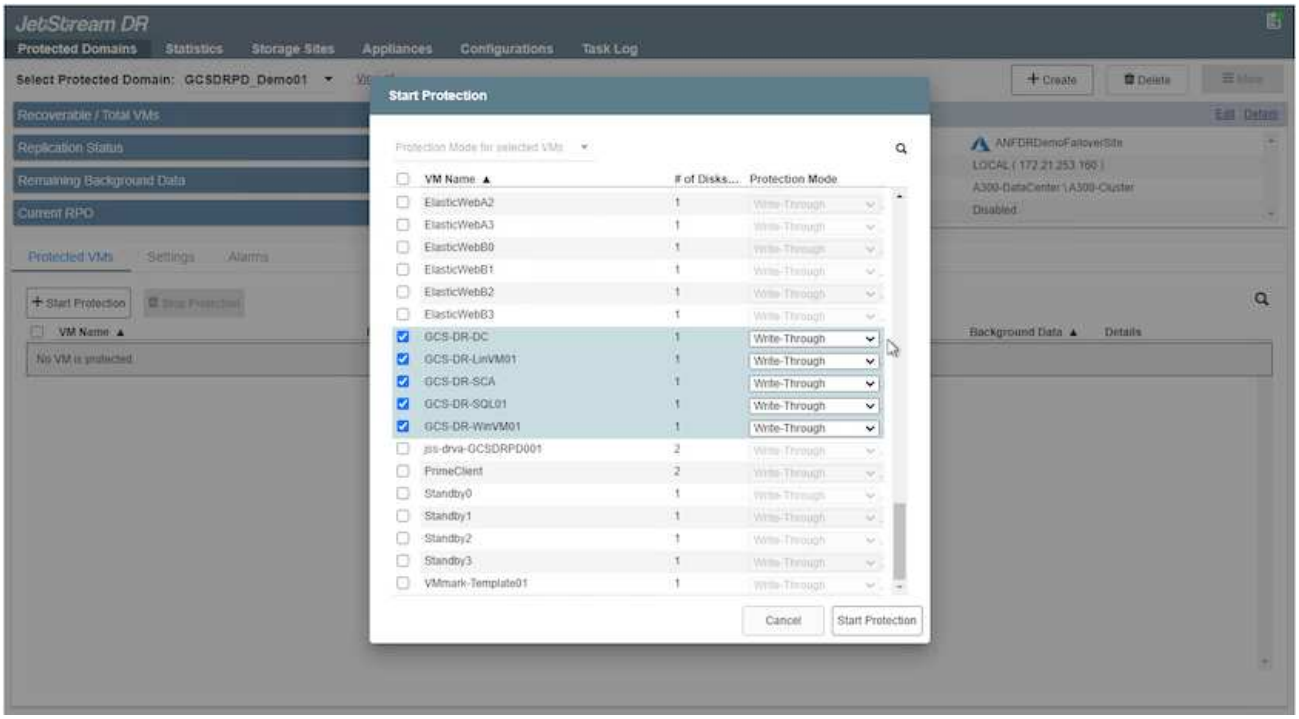




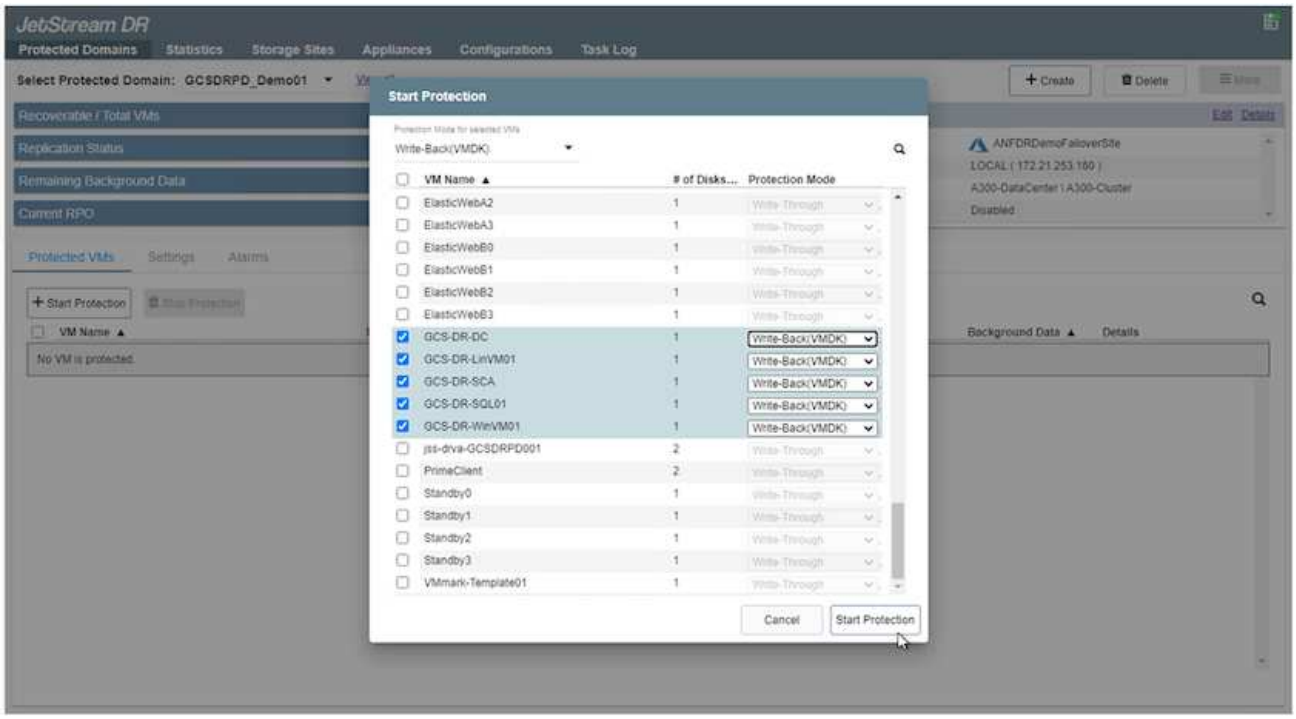
11. 選擇要保護的虛擬機，並根據依賴關係將虛擬機分組到應用程式群組中。應用程式定義可讓您將虛擬機器集分組為邏輯群組，其中包含其啟動順序、啟動延遲以及可在復原時執行的選用應用程式驗證。

確保受保護域內的所有虛擬機器使用相同的保護模式。

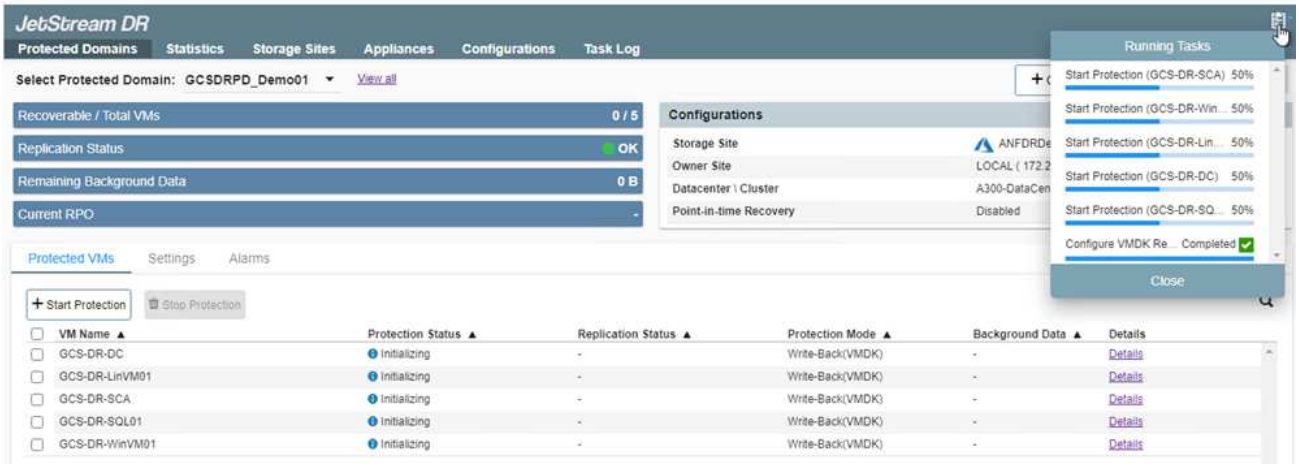
回寫（VMDK）模式提供更高的效能。



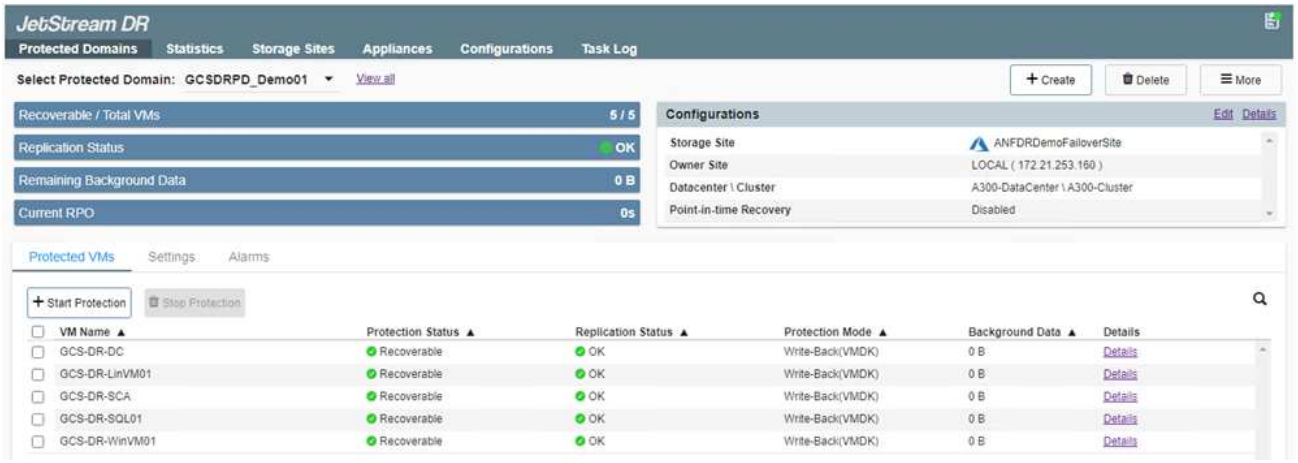
12. 確保複製日誌卷放置在高效能儲存上。



13. 完成後，按一下「開始保護」以保護受保護的網域。這將開始將選定虛擬機器的資料複製到指定的 Blob 儲存體。



14. 複製完成後，虛擬機器保護狀態標記為可恢復。



可以設定故障轉移運作手冊來對虛擬機器進行分組（稱為復原群組）、設定啟動順序以及修改 CPU/記憶體設定以及 IP 配置。

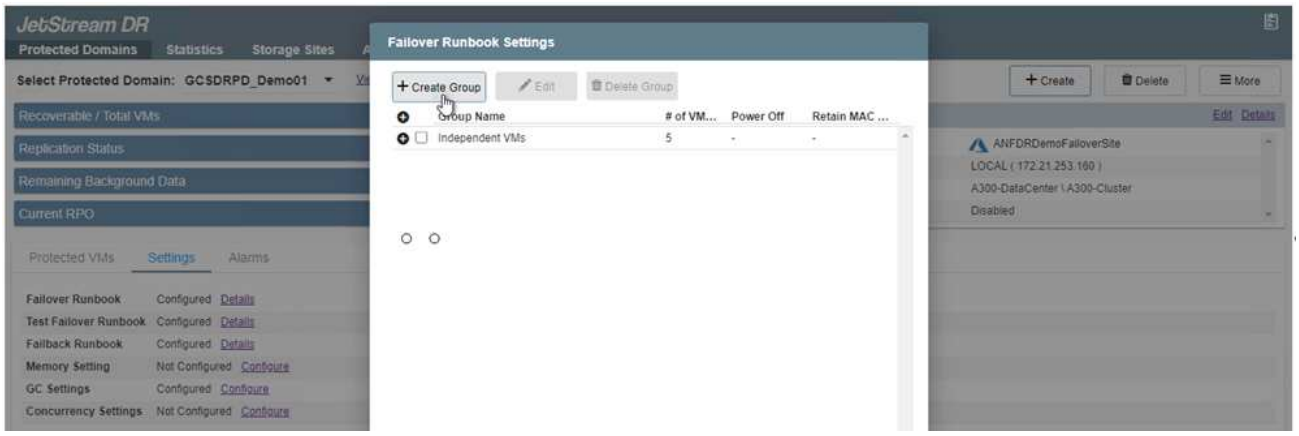
15. 按一下“設定”，然後按一下“執行手冊設定”連結來設定執行手冊群組。



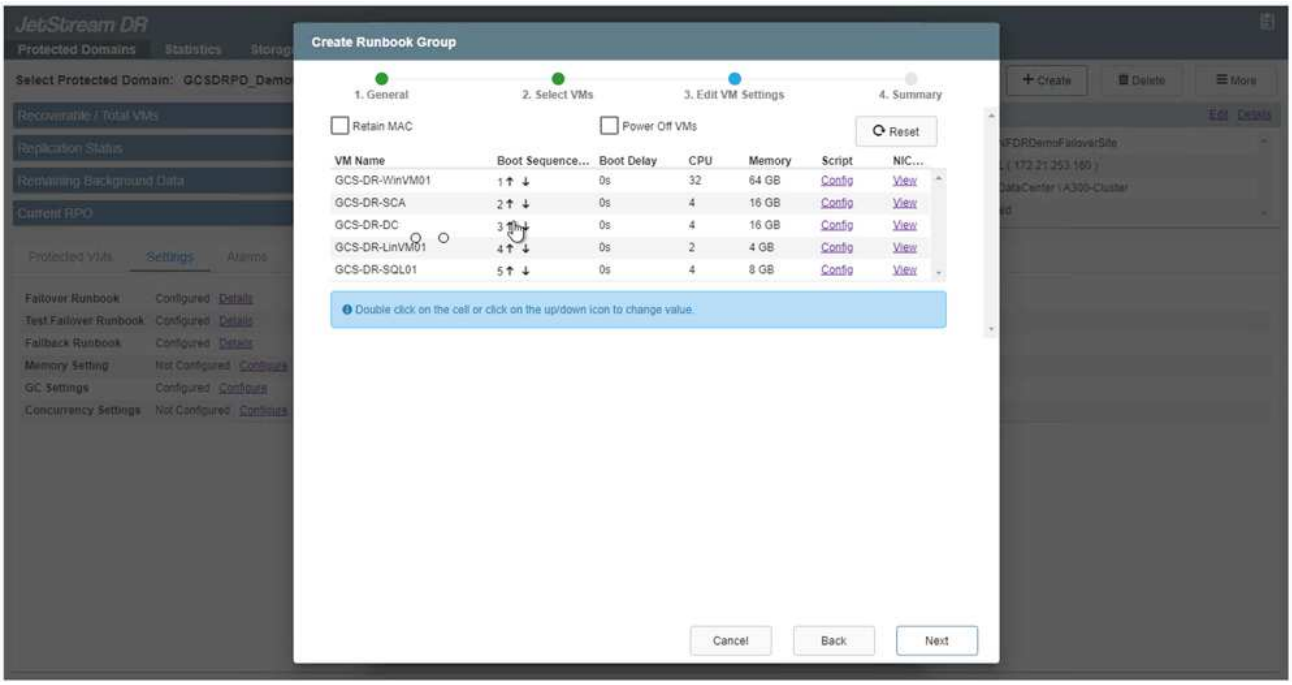
16. 點選「建立群組」按鈕開始建立新的運作手冊群組。

如果需要，在螢幕的下部，套用自訂前腳本和後腳本，以便在執行手冊組操作之前和之後

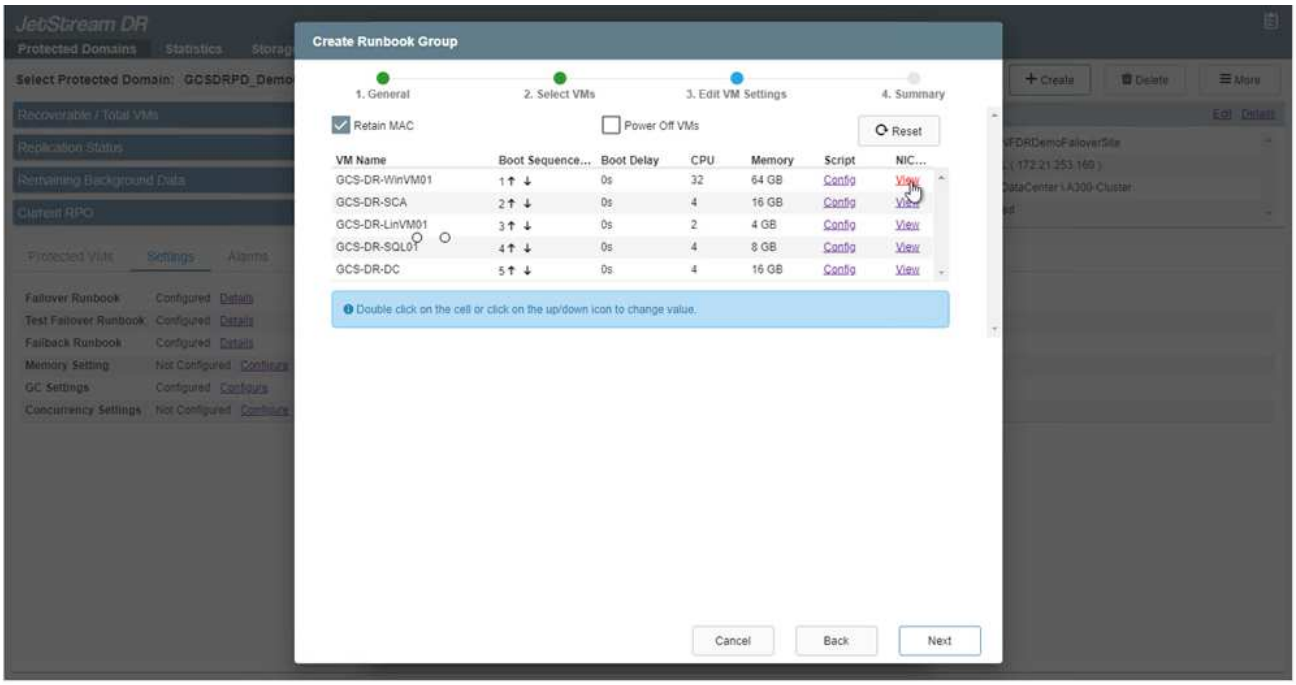
自動執行。確保 Runbook 腳本駐留在管理伺服器上。



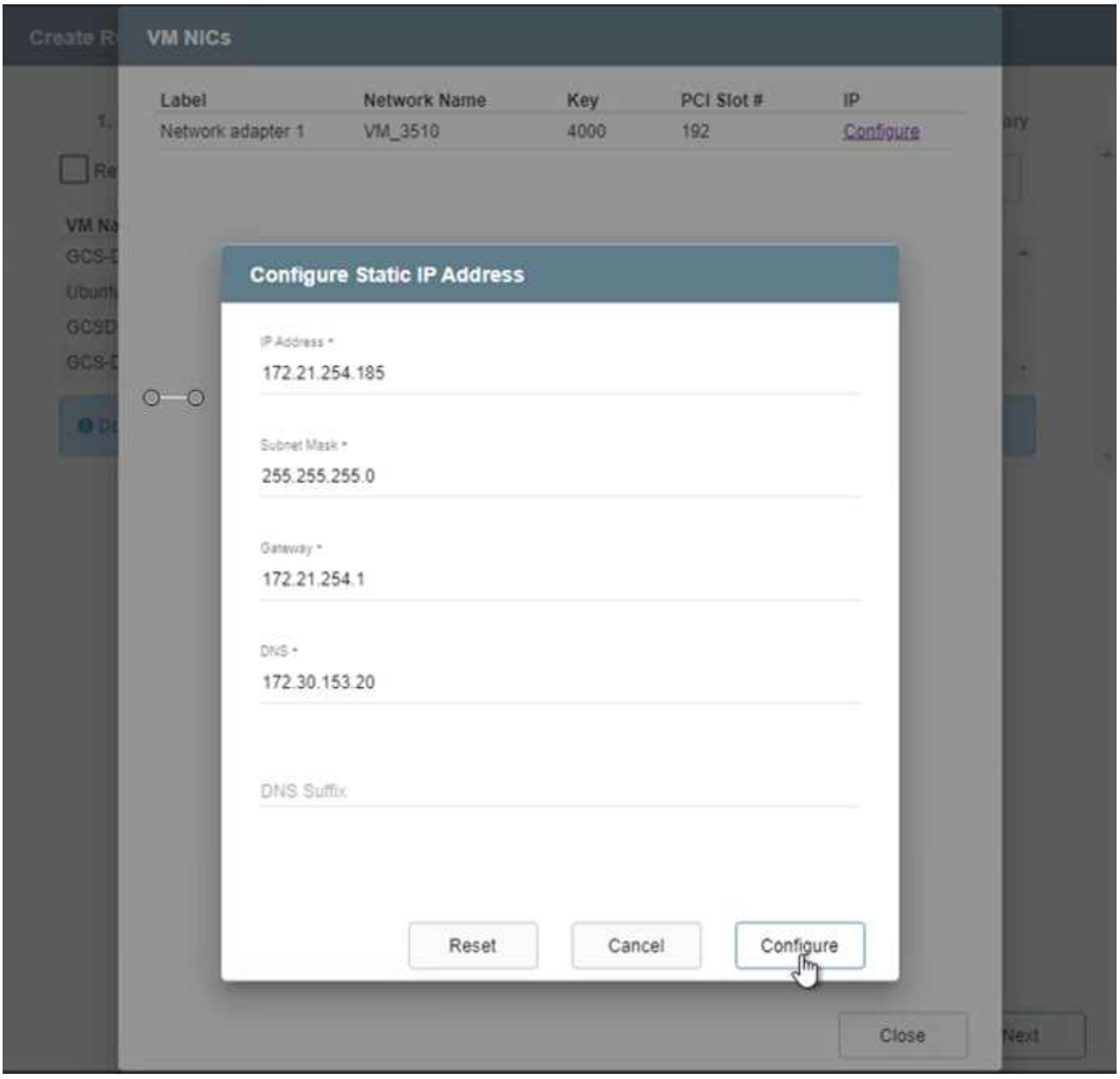
17. 根據需要編輯 VM 設定。指定恢復虛擬機器的參數，包括啟動順序、啟動延遲（以秒為單位）、CPU 數量以及要分配的記憶體量。按一下向上或向下箭頭以變更虛擬機器的啟動順序。也提供了保留 MAC 的選項。

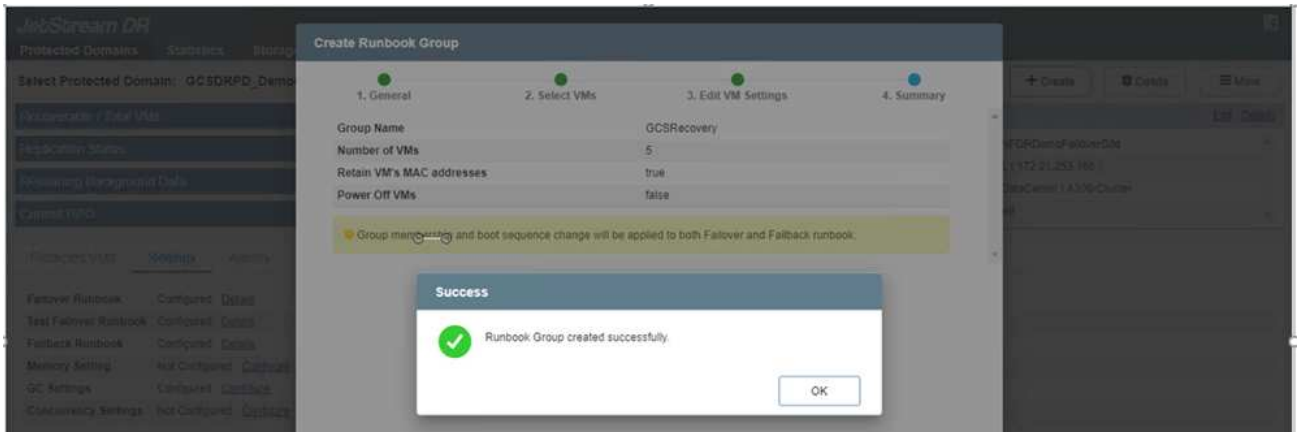


18. 可以為群組中的個別虛擬機器手動配置靜態 IP 位址。按一下虛擬機器的 NIC 視圖連結以手動配置其 IP 位址設定。



19. 點選配置按鈕儲存各個虛擬機器的 NIC 設定。





故障轉移和故障回復運作手冊的狀態現在均列為「已設定」。故障轉移和故障回應運作手冊群組是使用相同的初始虛擬機器群組和設定成對建立的。如果需要，可以透過點擊其各自的「詳細資料」連結並進行更改來單獨自訂任何運行手冊組的設定。

▼ 在私有雲中為 **AVS** 安裝 **JetStream DR**

恢復站點 (AVS) 的最佳實踐是提前創建一個三節點的試點燈叢集。這允許預先配置恢復站點基礎設施，包括以下內容：

- 目標網路段、防火牆、DHCP 和 DNS 等服務等
- 為 AVS 安裝 JetStream DR
- 將 ANF 卷配置為資料儲存等

JetStream DR 支援關鍵任務域的接近零 RTO 模式。對於這些網域，應該預先安裝目標儲存。在這種情況下，ANF 是建議的儲存類型。

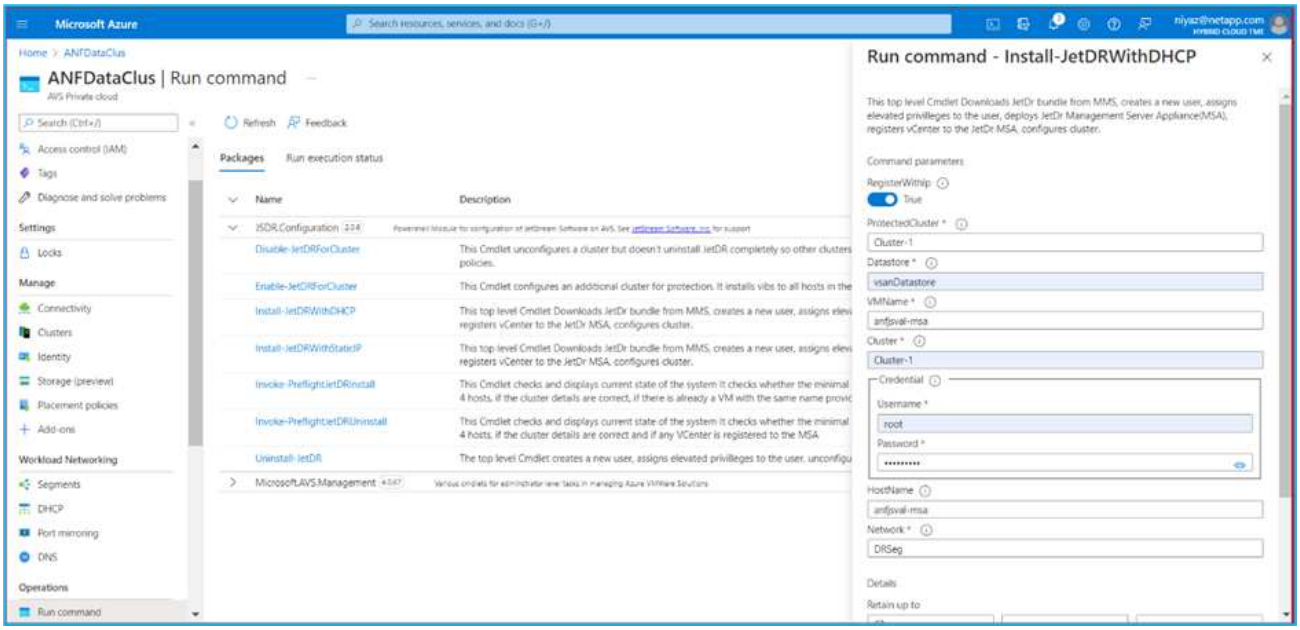
ⓘ 應在 AVS 叢集上配置包括段創建在內的網路配置以滿足本機要求。

ⓘ 根據 SLA 和 RTO 要求，您可以使用連續故障轉移或常規（標準）故障轉移模式。對於接近零的 RTO，您應該在復原站點開始持續補水。

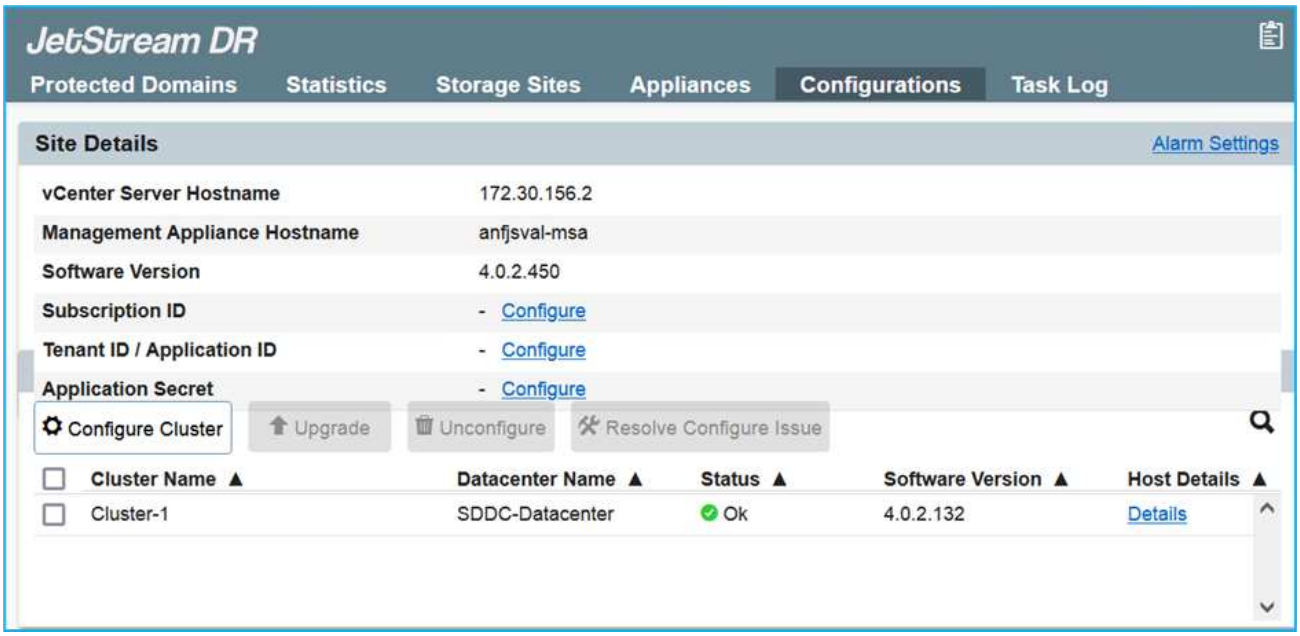
1. 若要在 Azure VMware 解決方案私有雲上安裝 JetStream DR for AVS，請使用執行指令。從 Azure 入口網站前往 Azure VMware 解決方案，選擇私有雲，然後選擇執行命令> 套件> JSDR.Configuration。

   ⓘ Azure VMware 解決方案的預設 CloudAdmin 使用者沒有足夠的權限來為 AVS 安裝 JetStream DR。 Azure VMware 解決方案透過呼叫 JetStream DR 的 Azure VMware 解決方案來執行指令，實現了 JetStream DR 的簡化和自動化安裝。

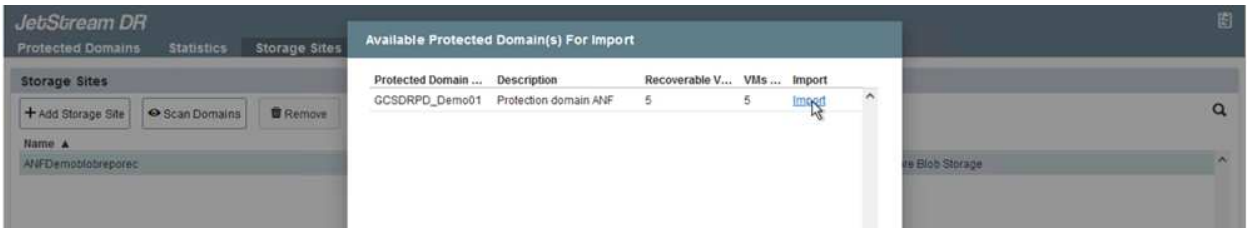
   以下螢幕截圖顯示了使用基於 DHCP 的 IP 位址的安裝。



2. JetStream DR for AVS 安裝完成後，刷新瀏覽器。若要存取 JetStream DR UI，請前往 SDDC 資料中心 > 設定 > JetStream DR。



3. 從 JetStream DR 介面完成以下任務：
   a. 新增用於保護本機叢集的 Azure Blob 儲存帳戶作為儲存站點，然後執行掃描網域選項。
   b. 在出現的彈出對話方塊視窗中，選擇要匯入的受保護網域，然後按一下其匯入連結。



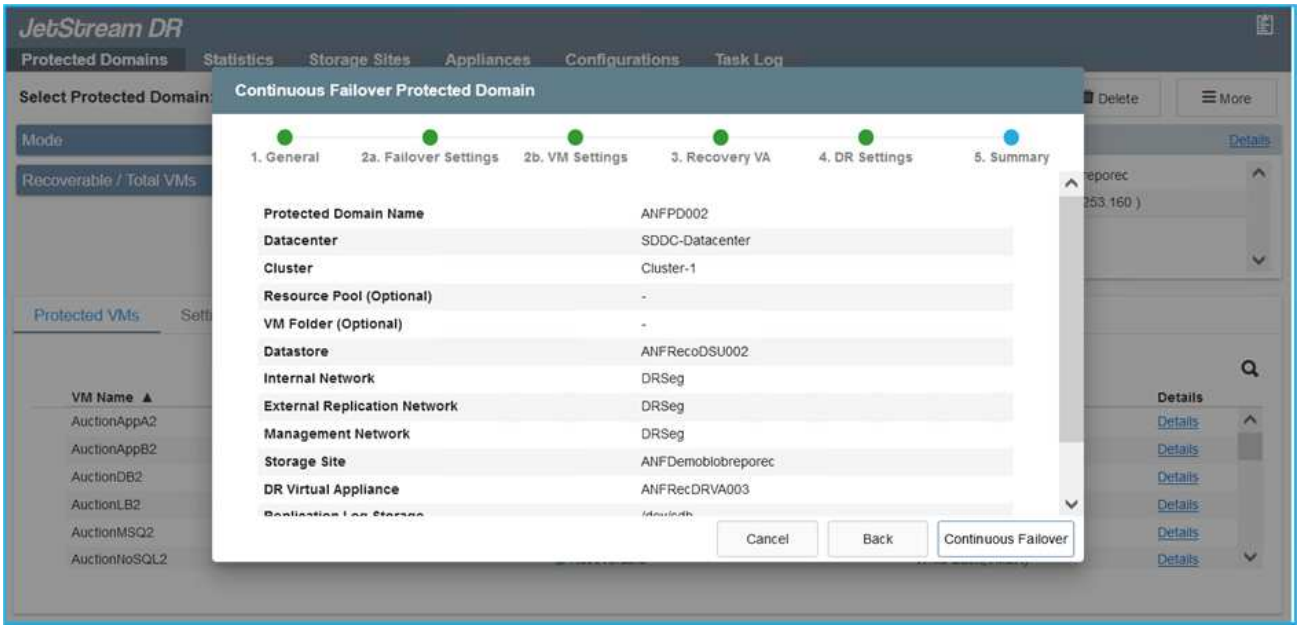
4. 該域名已導入以進行恢復。前往「受保護的網域」標籤並驗證是否已選擇目標網域，或從「選擇受保護的網域」功能表中選擇所需的網域。顯示受保護域中可復原的虛擬機器清單。



5. 導入受保護域後，部署 DRVA 設備。

> 這些步驟也可以使用 CPT 建立的計劃自動執行。

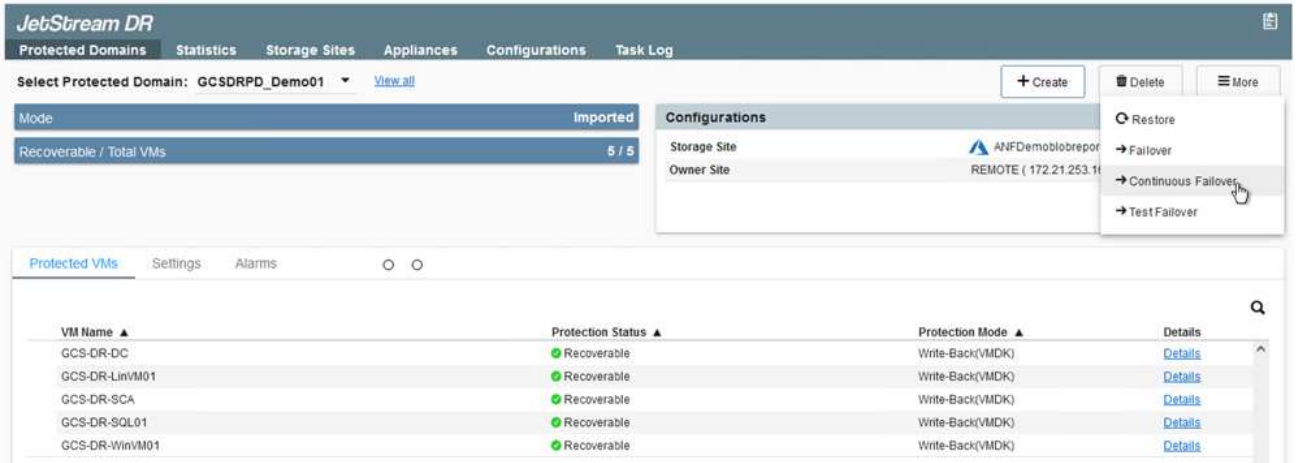
6. 使用可用的 vSAN 或 ANF 資料儲存建立複製日誌卷。
7. 導入受保護的網域並配置恢復 VA 以使用 ANF 資料儲存進行 VM 放置。



確保所選網段上啟用了 DHCP，並且有足夠的可用 IP。在網域名稱恢復期間，暫時使用動態 IP。每個復原的虛擬機器（包括持續補水）都需要一個單獨的動態 IP。恢復完成後，IP 被釋放並可重複使用。

8. 選擇適當的故障轉移選項（連續故障轉移或故障轉移）。在這個例子中，選擇了持續補水（持續故障轉移）。

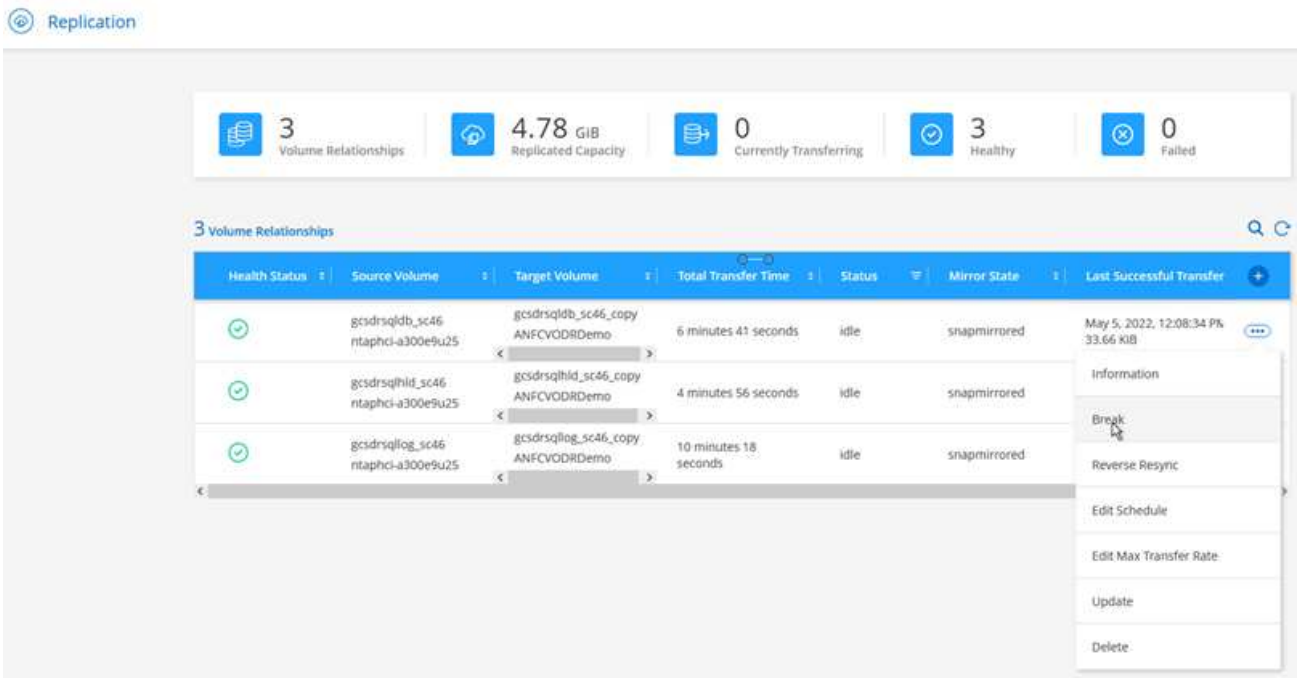
儘管連續故障轉移和故障轉移模式在執行配置時有所不同，但兩種故障轉移模式都使用相同的步驟進行設定。故障轉移步驟是一起配置和執行的，以應對災難事件。可以隨時配置連續故障轉移，然後允許其在正常系統運作期間在背景運作。災難事件發生後，完成持續故障轉移，立即將受保護虛擬機器的所有權轉移到復原站點（接近零 RTO）。

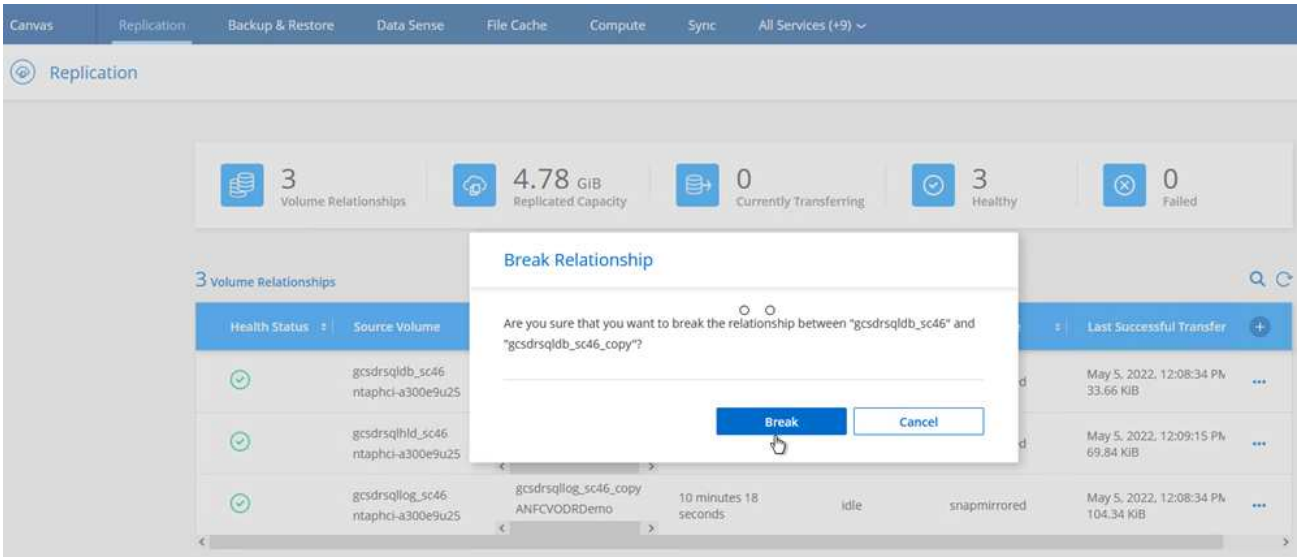


持續故障轉移程序開始，並且可以從 UI 監控其進度。點擊「目前步驟」部分中的藍色圖示將開啟一個彈出窗口，其中顯示故障轉移過程當前步驟的詳細資訊。

▼ 故障轉移和故障恢復

1. 當本地環境的受保護叢集發生災難（部分或全部故障）後，您可以在中斷各個應用程式磁碟區的SnapMirror關係後，使用 Jetstream 觸發虛擬機器的故障轉移。

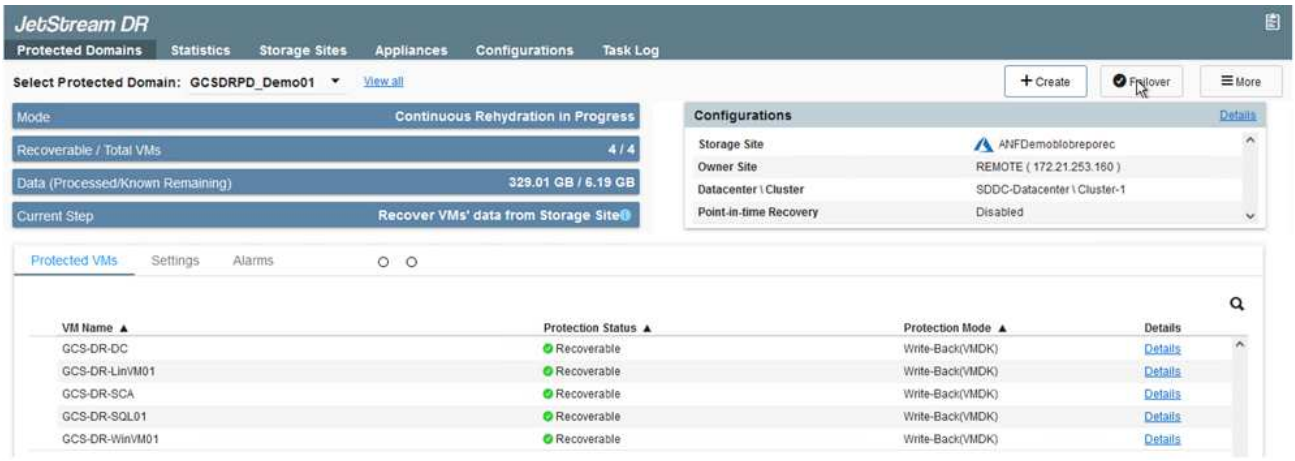


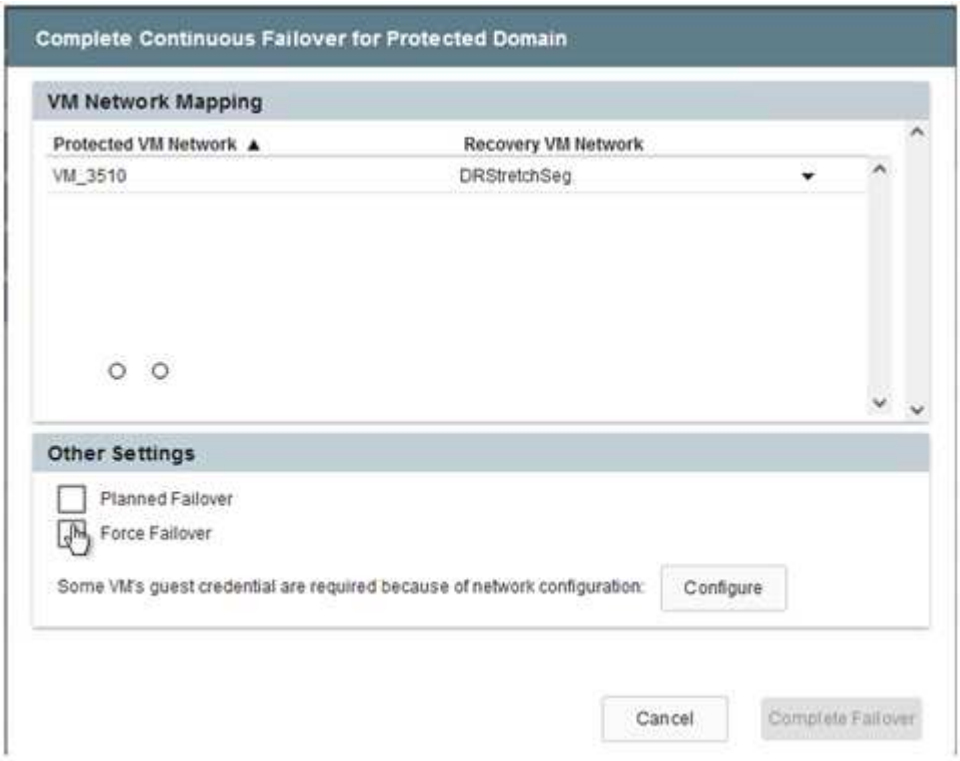


此步驟可以輕鬆實現自動化，以促進恢復過程。

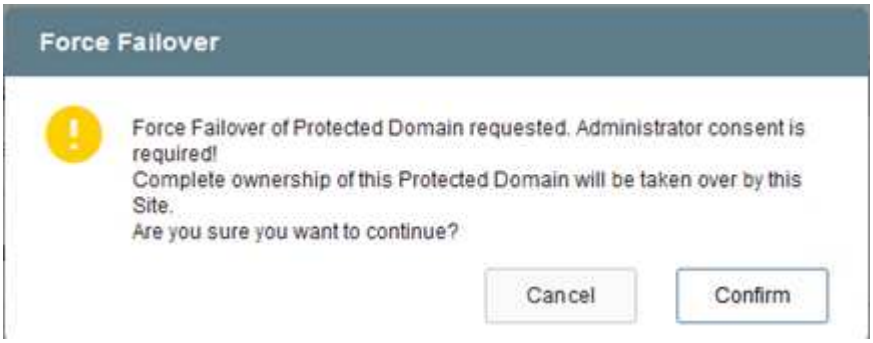
2. 存取 AVS SDDC（目標端）上的 Jetstream UI 並觸發故障轉移選項以完成故障轉移。工作列顯示故障轉移活動的進度。

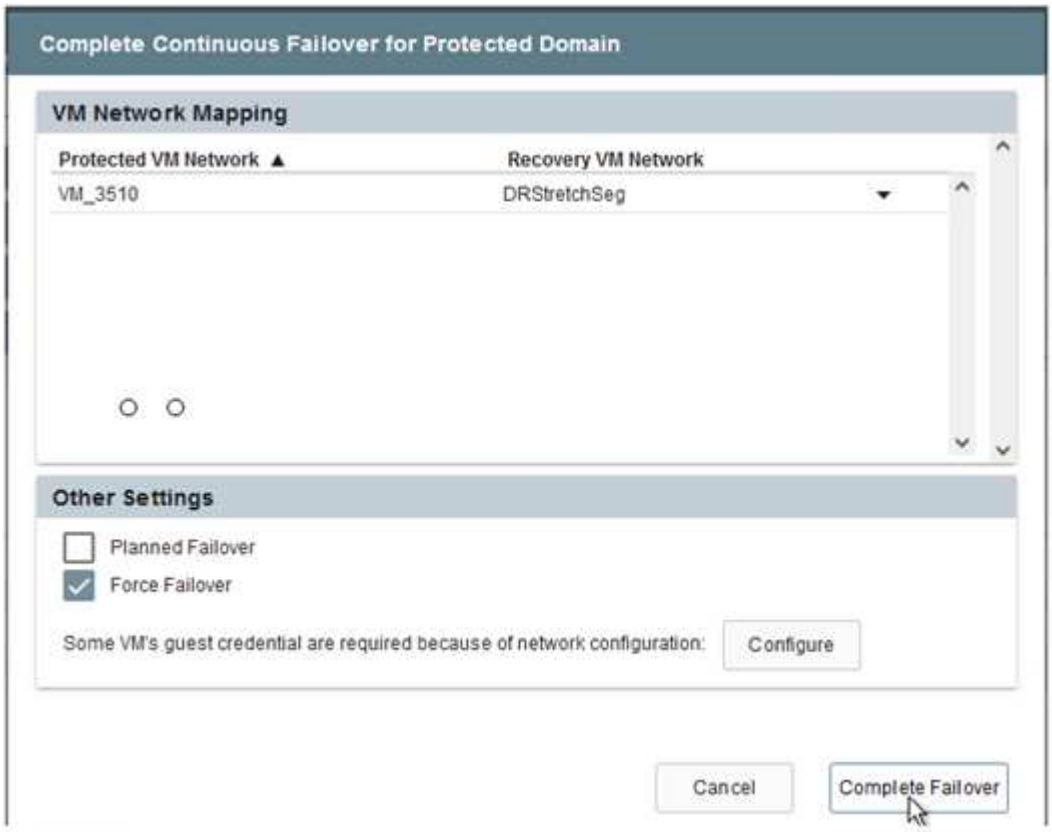
   在完成故障轉移時出現的對話視窗中，可以將故障轉移任務指定為計劃的或假定為強制的。





強制故障轉移假定主站點不再可訪問，受保護域的所有權應由復原站點直接承擔。





3. 連續故障轉移完成後，會出現一則訊息確認任務完成。任務完成後，存取復原的虛擬機器以設定 ISCSI 或 NFS 會話。

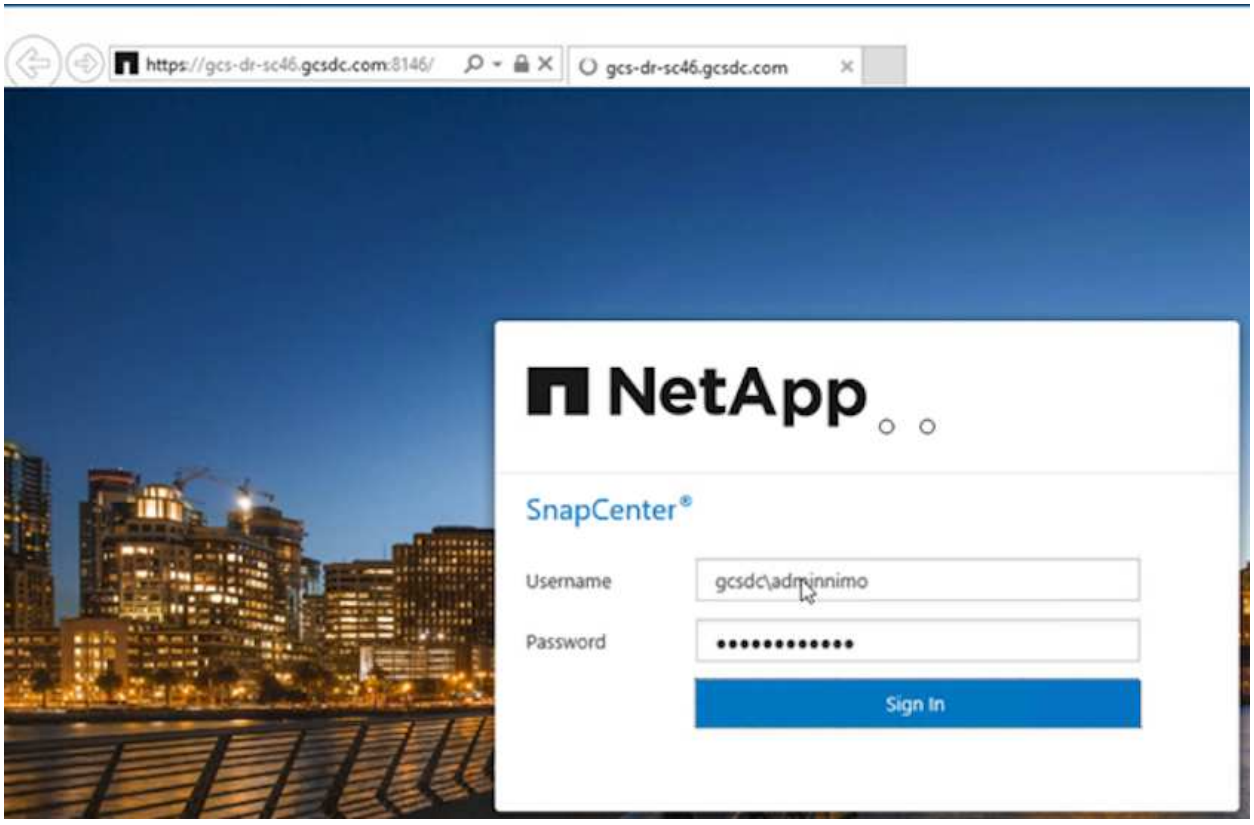
故障轉移模式變為“故障轉移中正在運行”，虛擬機器狀態變為“可恢復”。受保護域的所有虛擬機器現在都在復原站點上執行，狀態依照故障轉移運作手冊設定指定。

為了驗證故障轉移配置和基礎設施，JetStream DR 可以在測試模式下運作（測試故障轉移選項），以觀察虛擬機器及其資料從物件儲存到測試復原環境的復原情況。當在測試模式下執行故障轉移過程時，其操作類似於實際的故障轉移過程。

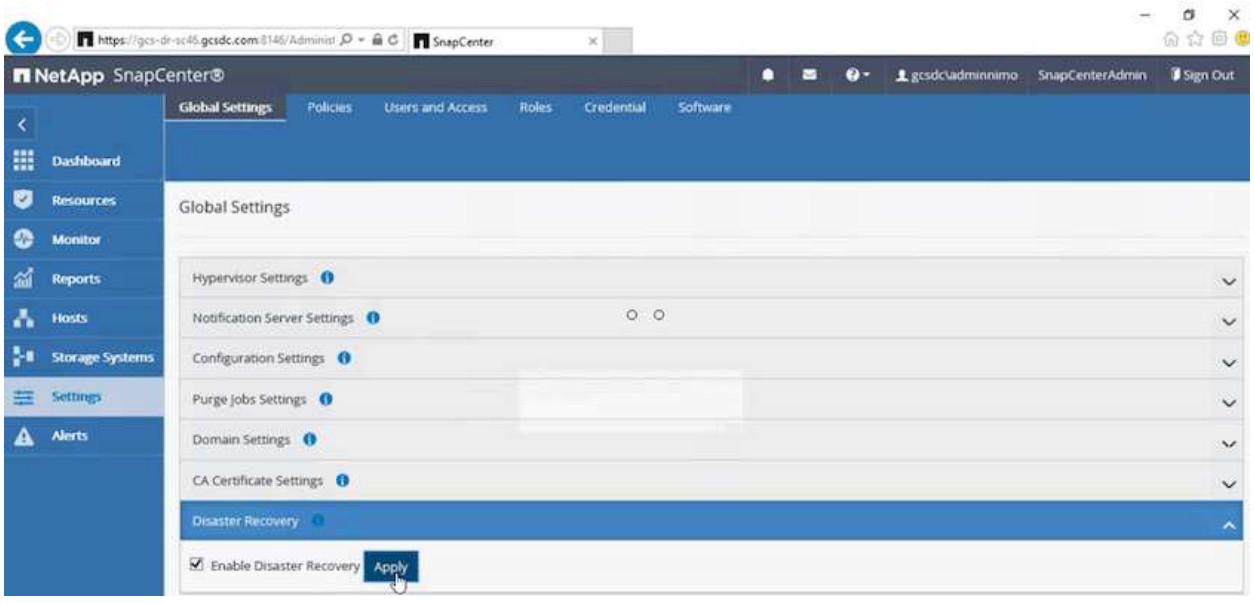


4. 虛擬機器復原後，使用儲存災難復原進行來賓儲存。為了示範此過程，本例中使用了 SQL 伺服器。

5. 登入 AVS SDDC 上復原的SnapCenter VM 並啟用 DR 模式。
   a. 使用瀏覽器存取SnapCenter UI。



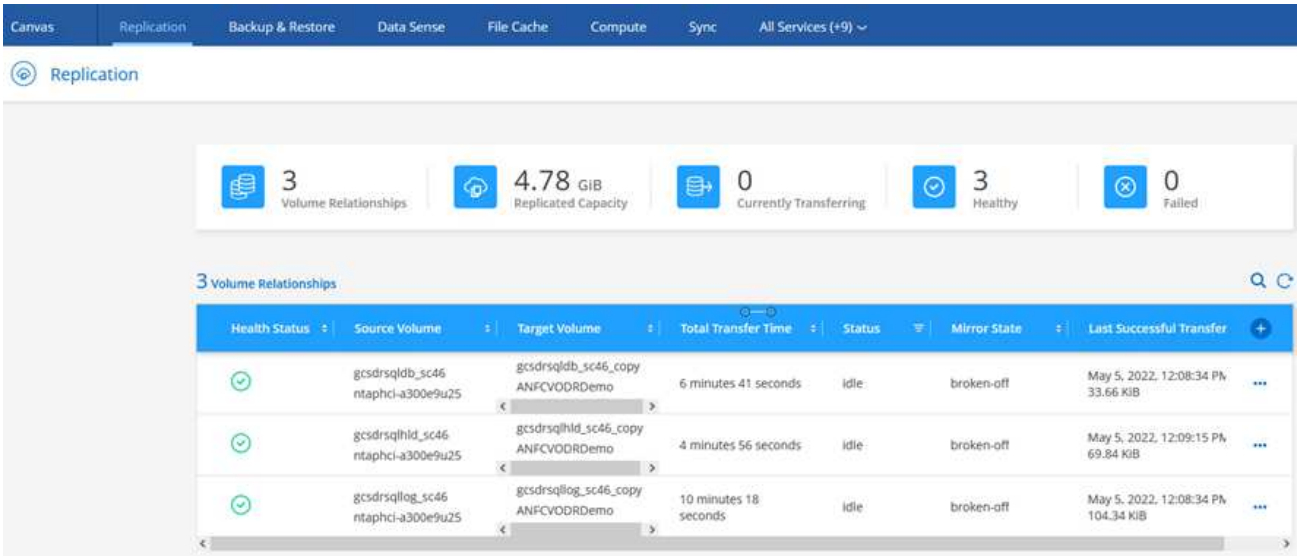
   b. 在設定頁面中，導覽至設定> 全域設定> 災難復原。
   c. 選擇啟用災難復原。
   d. 按一下“應用”。



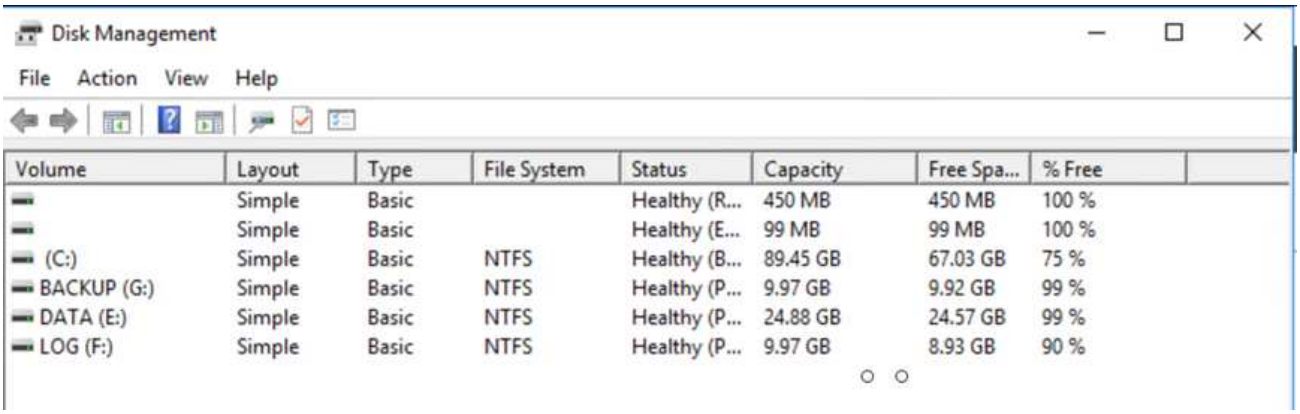
   e. 按一下「監視」>「作業」來驗證 DR 作業是否已啟用。

應使用NetApp SnapCenter 4.6 或更高版本進行儲存災難復原。對於先前的版本，應使用應用程式一致性快照（使用SnapMirror複製），並且應執行手動恢復，以防必須在災難恢復站點恢復先前的備份。

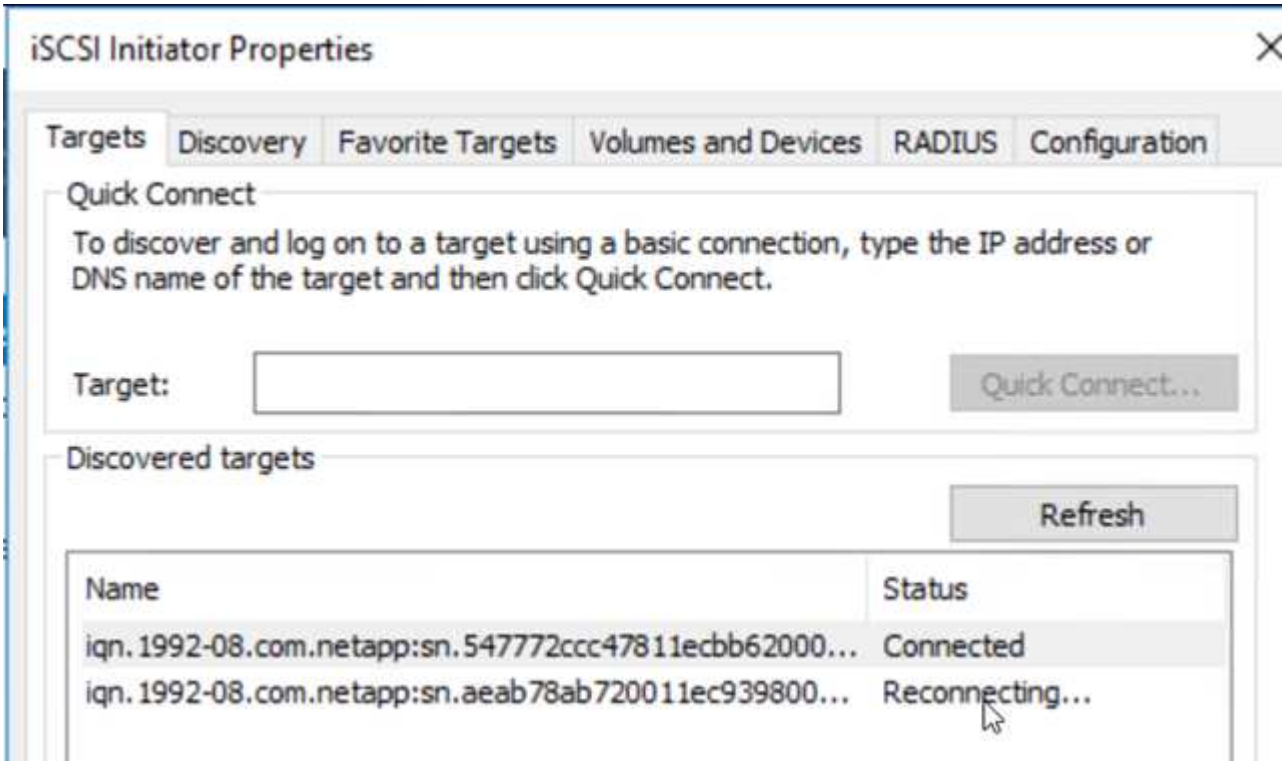
6. 確保SnapMirror關係已中斷。



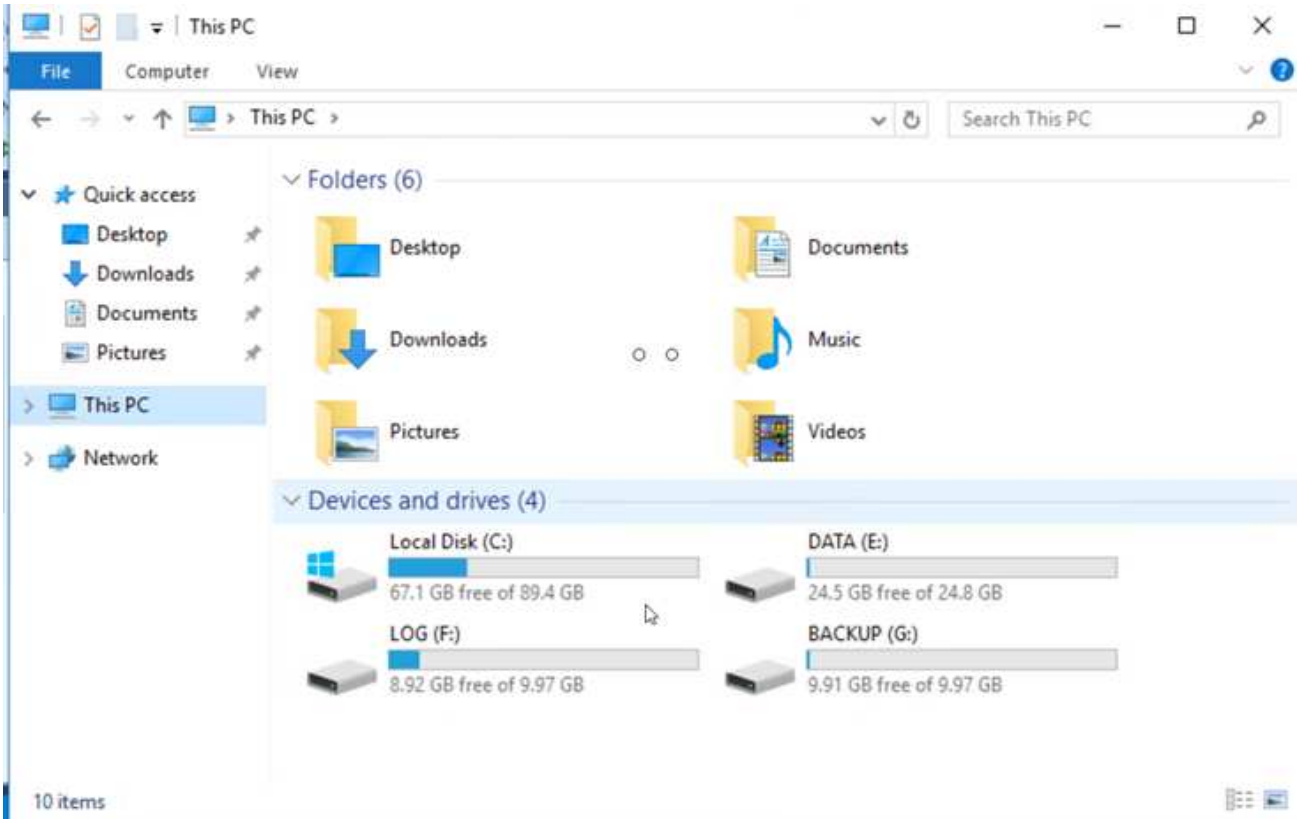
7. 將Cloud Volumes ONTAP中的 LUN 連接到具有相同磁碟機號碼的復原的 SQL 客戶虛擬機器。



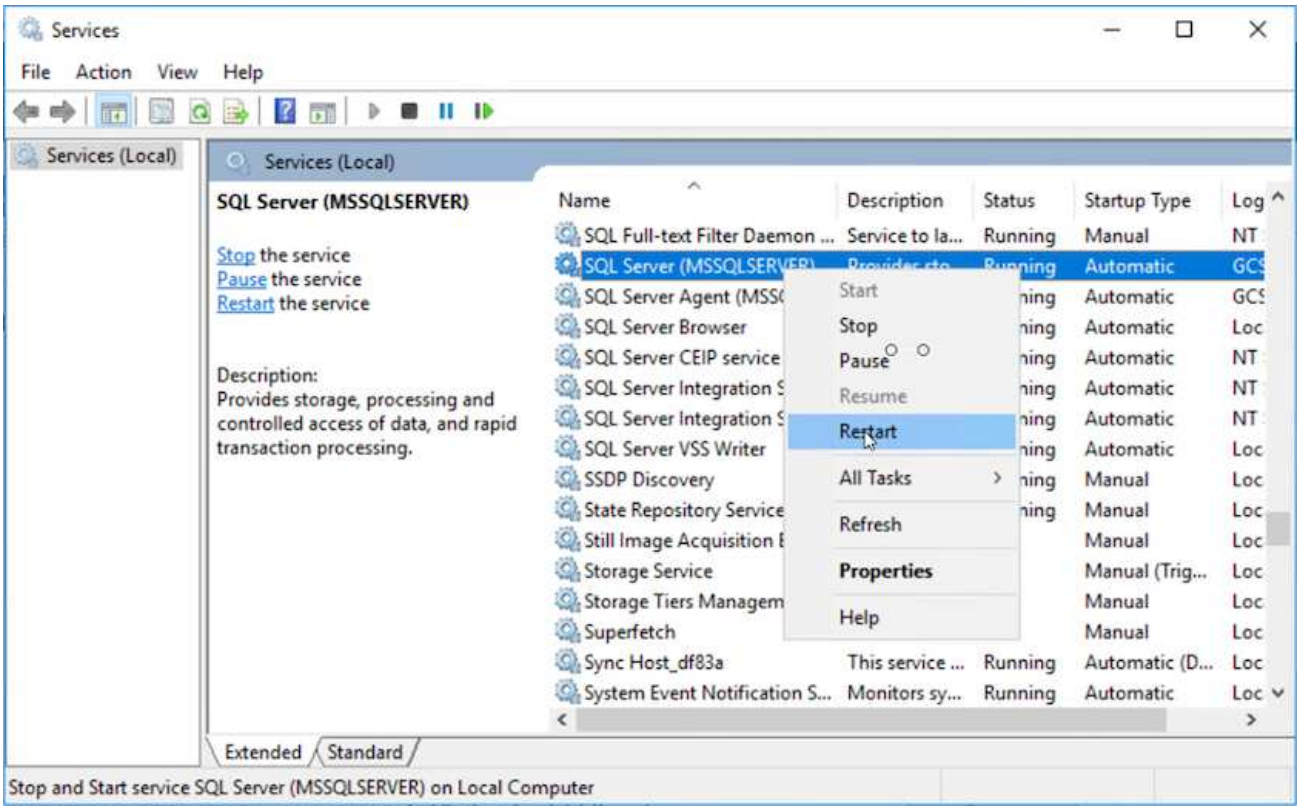
8. 開啟 iSCSI 啟動器，清除先前已中斷的會話，並為複製的Cloud Volumes ONTAP磁碟區新增目標以及多路徑。



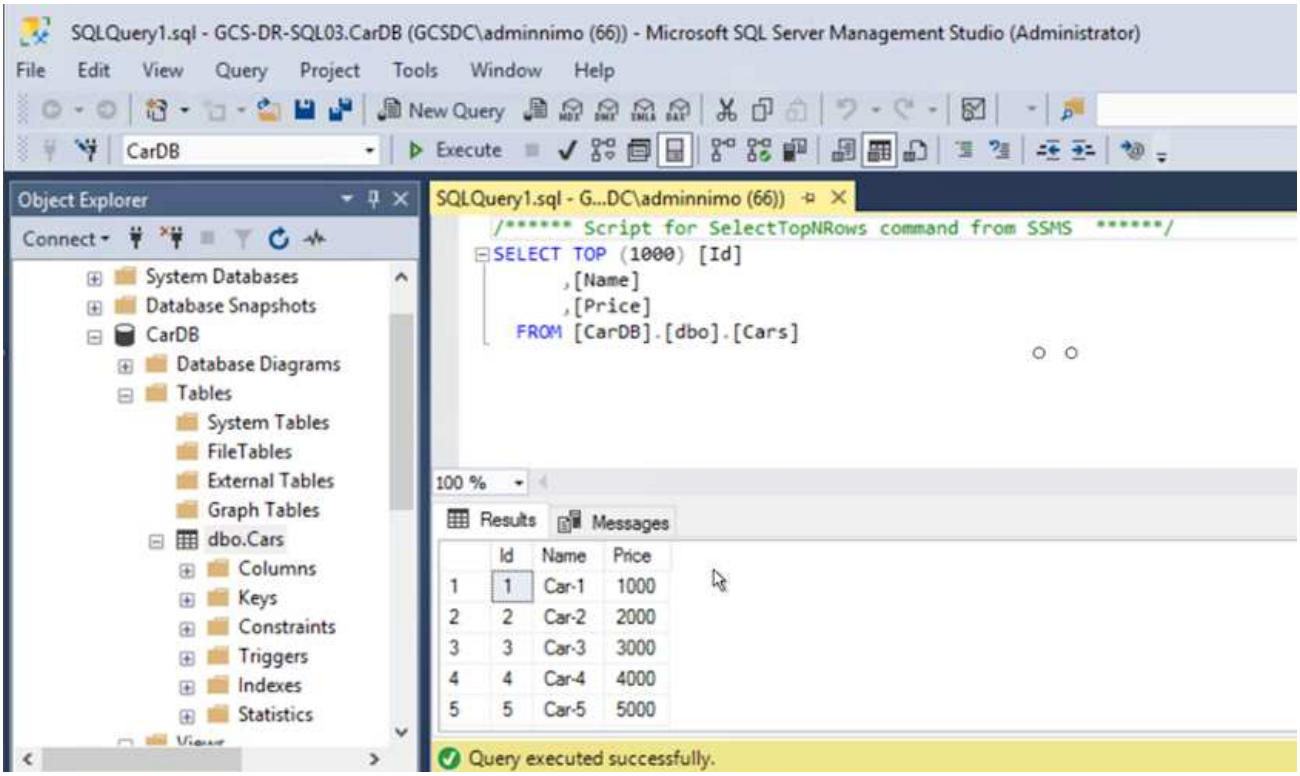
9. 確保所有磁碟都使用 DR 之前使用的相同磁碟機號碼進行連接。



10. 重新啟動 MSSQL 伺服器服務。



11. 確保 SQL 資源已恢復上線。



對於 NFS，使用 mount 指令附加磁碟區並更新 `/etc/fstab`條目。

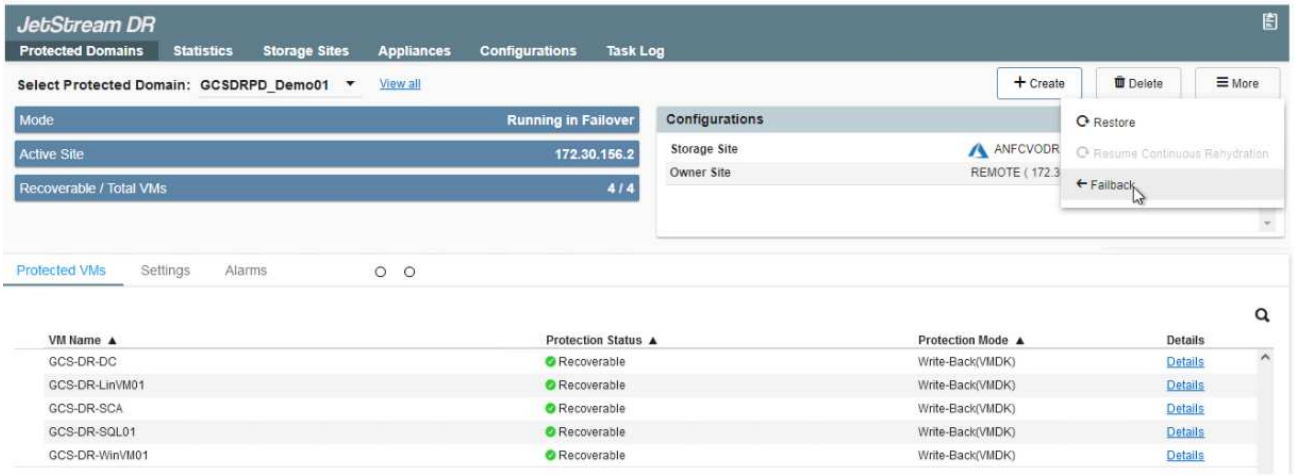
此時，操作可以運作且業務可以繼續正常進行。

在 NSX-T 端，可以建立單獨的專用第 1 層閘道來模擬故障轉移場景。這可確保所有工作負載可以相互通信，但不會有任何流量可以路由進出環境，從而可以執行任何分類、遏製或強化任務而不會有交叉污染的風險。此操作超出了本文檔的範圍，但可以輕鬆實現模擬隔離。

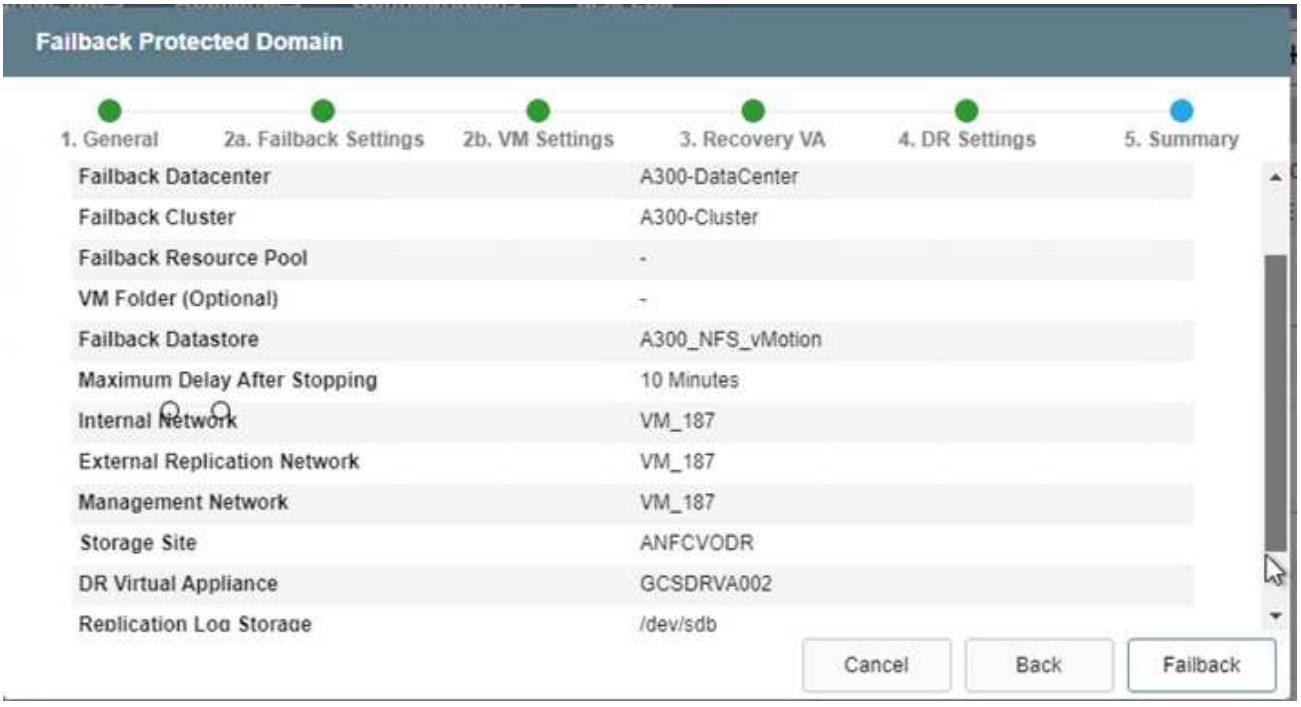
主站點重新啟動並運行後，您可以執行故障復原。 VM 保護由 Jetstream 恢復，並且必須逆轉SnapMirror關係。

1. 恢復本地環境。根據災難事件的類型，可能需要復原和/或驗證受保護叢集的配置。如有必要，可能需要重新安裝 JetStream DR 軟體。
2. 存取復原的本機環境，前往 Jetstream DR UI，然後選擇適當的受保護網域。受保護網站準備好故障復原後，在 UI 中選擇故障復原選項。

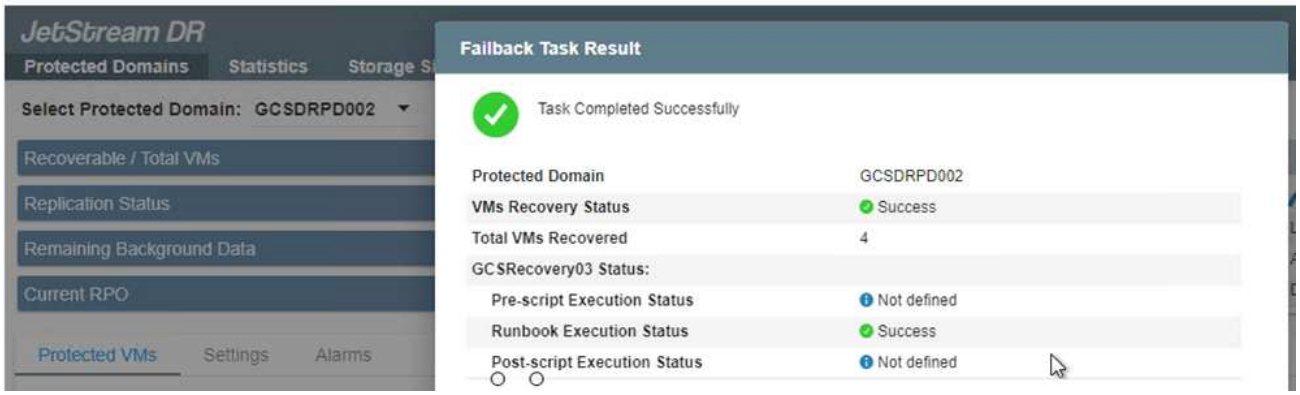
CPT 產生的故障復原計畫也可用於啟動虛擬機器及其資料從物件儲存返回原始 VMware 環境。



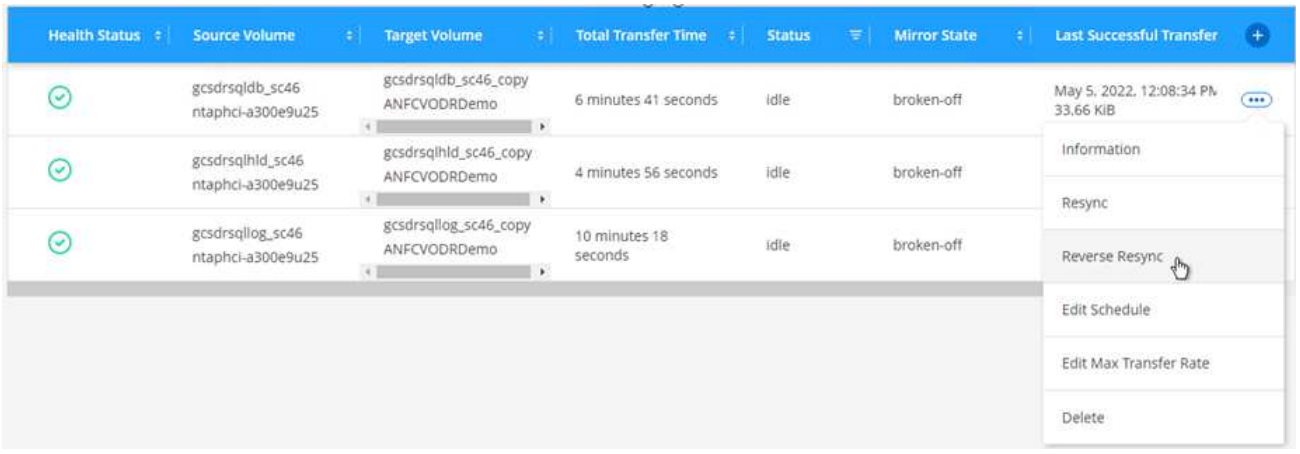
指定在復原站點中暫停虛擬機器並在受保護站點中重新啟動虛擬機器後的最大延遲。完成此程序所需的時間包括停止故障轉移虛擬機器後完成複製的時間、清理復原站點所需的時間以及在受保護站點中重新建立虛擬機器所需的時間。 NetApp建議 10 分鐘。

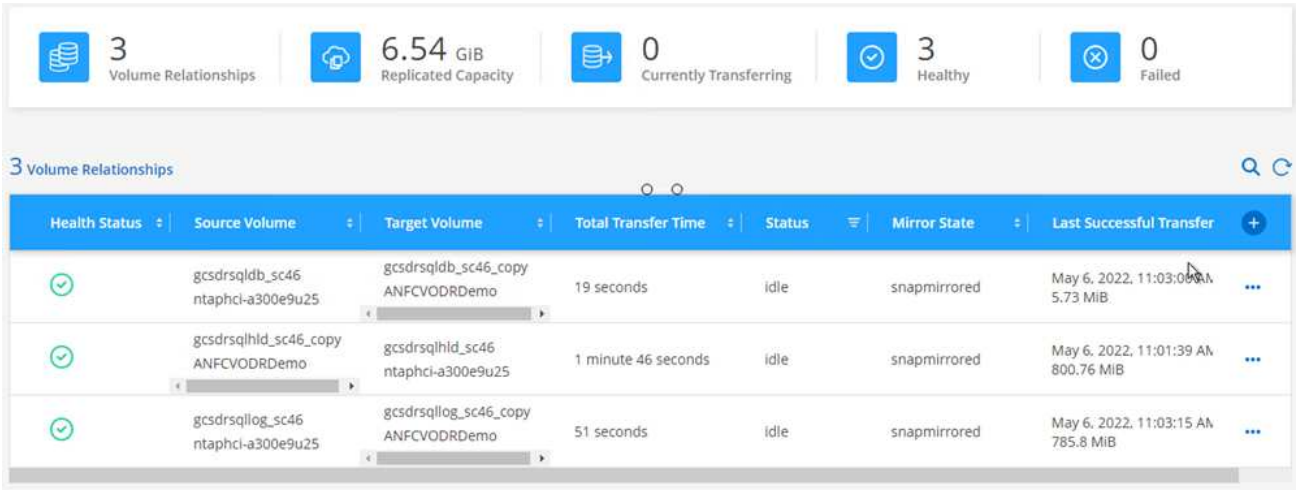


3. 完成故障復原流程，然後確認復原虛擬機器保護和資料一致性。

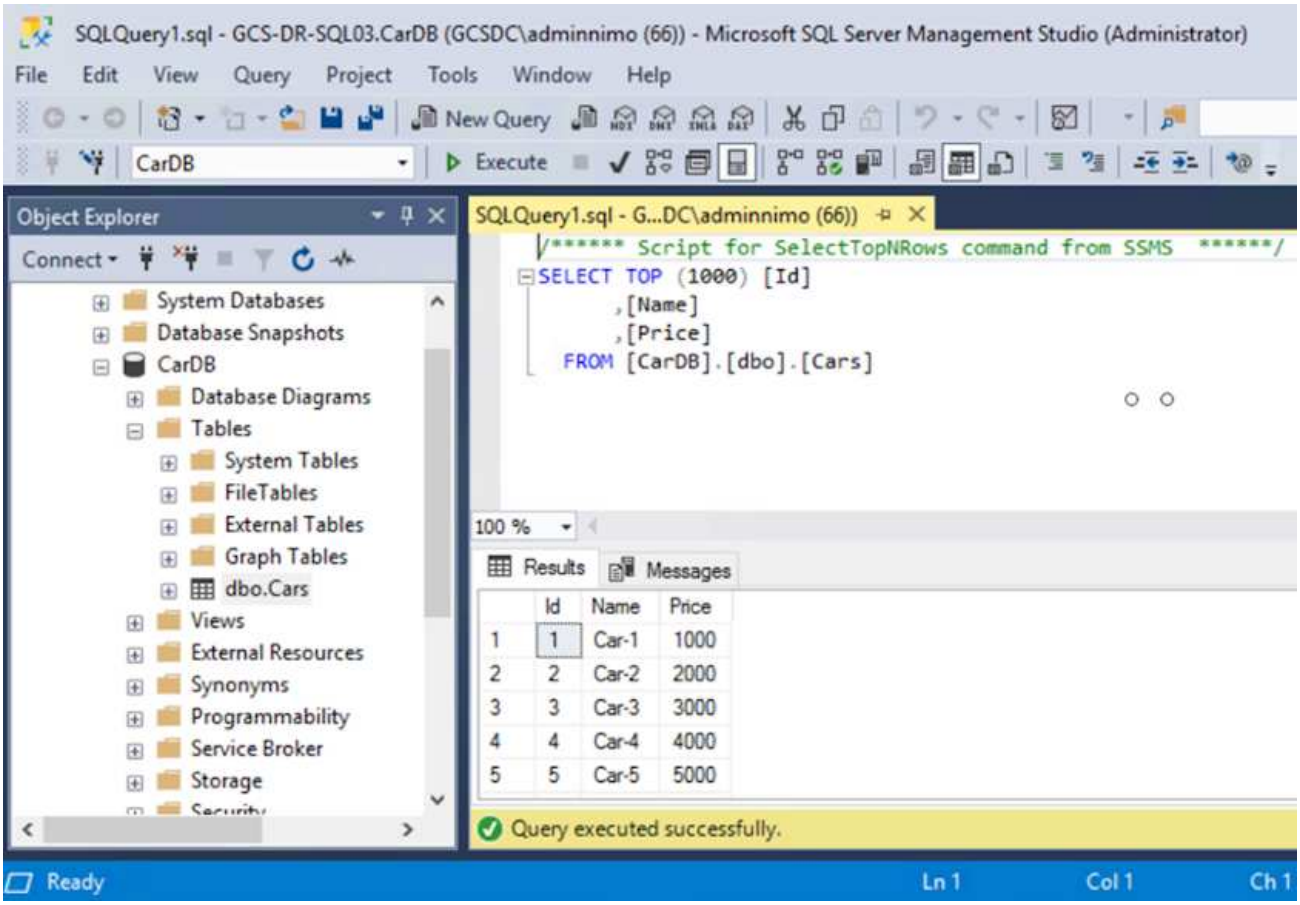


4. 虛擬機器恢復後，斷開輔助儲存與主機的連接並連接到主儲存。





5. 重新啟動 MSSQL 伺服器服務。
6. 驗證 SQL 資源是否已恢復連線。



若要故障恢復到主存儲，請透過執行反向重新同步操作確保關係方向與故障轉移之前保持相同。

為了在反向重新同步操作後保留主儲存和輔助儲存的角色，請再次執行反向重新同步操作。

此過程適用於其他應用程序，如 Oracle、類似的資料庫類型以及任何其他使用來賓連接儲存的應用程式。

與往常一樣，在將關鍵工作負載轉移到生產環境之前，請先測試復原所涉及的步驟。

此解決方案的優勢

- 使用SnapMirror的高效且有彈性的複製。
- 透過ONTAP快照保留還原到任何可用的時間點。
- 從儲存、運算、網路和應用程式驗證步驟，恢復數百到數千台虛擬機器所需的所有步驟均可完全自動化。
- SnapCenter使用不會改變複製磁碟區的克隆機制。
  - 這避免了磁碟區和快照資料損壞的風險。
  - 避免 DR 測試工作流程期間的複製中斷。
  - 利用 DR 資料進行 DR 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 最佳化可以透過恢復到較小的運算叢集來幫助降低雲端成本。

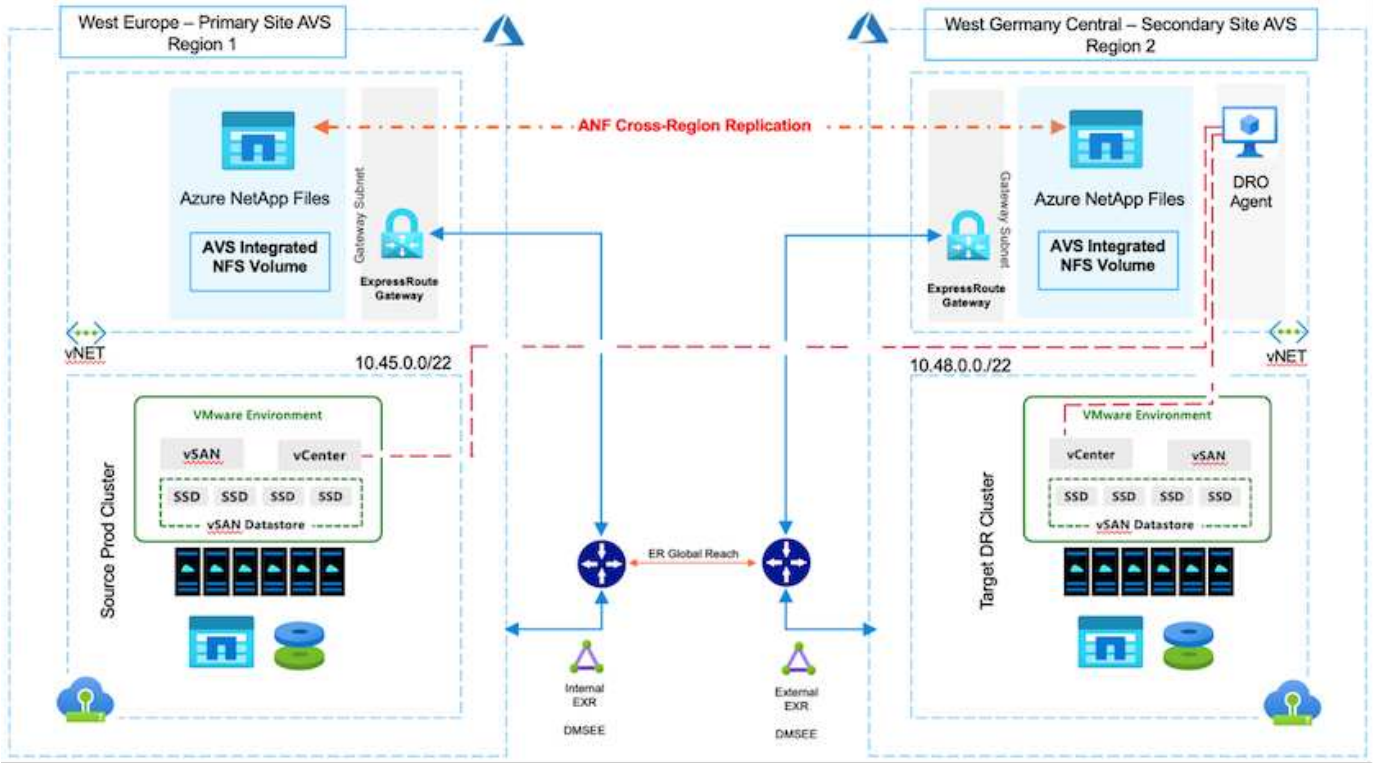
TR-4955：使用**Azure NetApp Files(ANF)** 和 **Azure VMware** 解決方案 **(AVS)** 進行災難復原

使用雲端內區域之間的區塊級複製進行災難復原是一種有彈性且經濟高效的方法，可保護工作負載免受網站中斷和資料損壞事件（例如勒索軟體）的影響。

概況

使用 Azure NetApp檔案 (ANF) 跨區域磁碟區複製，在 Azure VMware 解決方案 (AVS) SDDC 網站上執行的 VMware 工作負載（使用 Azure NetApp檔案磁碟區作為主 AVS 網站上的 NFS 資料儲存）可以複製到目標復原區域中的指定輔助 AVS 網站。

災難復原編排器 (DRO)（具有 UI 的腳本解決方案）可用於無縫復原從一個 AVS SDDC 複製到另一個 AVS SDDC 的工作負載。 DRO 透過中斷複製對等，然後將目標磁碟區作為資料儲存安裝，透過 VM 註冊到 AVS，再到 NSX-T 上的網路對應（包含在所有 AVS 私有雲中）來實現自動復原。



先決條件和一般建議

- 透過建立複製對等連線來驗證您是否已啟用跨區域複製。看 "為Azure NetApp Files建立磁碟區複製"。
- 必須在來源和目標 Azure VMware 解決方案私有雲之間設定 ExpressRoute Global Reach。
- 您必須擁有可以存取資源的服務主體。
- 支援以下拓撲：主 AVS 站點到輔助 AVS 站點。
- 配置 "複製"根據業務需求和資料變化率適當地安排每個卷。

不支援級聯和扇入扇出拓撲。

入門

部署 **Azure VMware** 解決方案

這 "Azure VMware 解決方案"(AVS) 是一種混合雲服務，可在 Microsoft Azure 公有雲中提供功能齊全的 VMware SDDC。 AVS 是使用 Azure 基礎架構、完全由 Microsoft 管理和支援並經過 VMware 驗證的第一方解決方案。因此，客戶可以獲得用於計算虛擬化的 VMware ESXi、用於超融合儲存的 vSAN 以及用於網路和安全的 NSX，同時利用 Microsoft Azure 的全球影響力、一流的資料中心設施以及與豐富的原生 Azure 服務和解決方案生態系統的接近性。 Azure VMware 解決方案 SDDC 和Azure NetApp Files的組合以最小的網路延遲提供了最佳效能。

若要在 Azure 上設定 AVS 私有雲，請依照下列步驟操作"關聯"請參閱NetApp文件以及 "關聯"用於 Microsoft 文件。可以使用以最小配置設定的指示燈環境來實現 DR 目的。此設定僅包含支援關鍵應用程式的核心元件，如果發生故障轉移，它可以擴展並產生更多主機來承擔大部分負載。

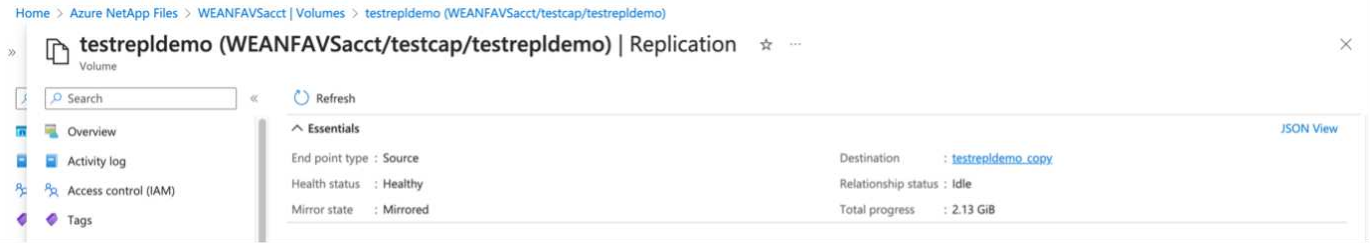
在初始版本中，DRO 支援現有的 AVS SDDC 叢集。按需 SDDC 創建功能將在即將發布的版本中提供。

預配並設定Azure NetApp Files

"Azure NetApp Files"是一種高效能、企業級、計量文件儲存服務。請依照以下步驟操作 "關聯"將Azure NetApp Files配置為 NFS 資料存儲，以最佳化 AVS 私有雲部署。

為Azure NetApp Files支援的資料儲存磁碟區建立磁碟區複製

第一步是設定所需資料儲存磁碟區從 AVS 主站點到 AVS 輔助站點的跨區域複製，並採用適當的頻率和保留。



請依照以下步驟操作 "關聯"透過建立複製對等來設定跨區域複製。目標容量池的服務等級可以與來源容量池的服務等級相符。但是，對於這個特定的用例，您可以選擇標準服務級別，然後 "修改服務級別"當發生真實災難或 DR 模擬時。

跨區域複製關係是先決條件，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 作業系統並確保滿足先決條件。然後安裝該套件。

先決條件：

- 可以存取資源的服務主體。
- 確保來源和目標 SDDC 以及Azure NetApp Files實例之間存在適當的連線。
- 如果您使用 DNS 名稱，則應該進行 DNS 解析。否則，請使用 vCenter 的 IP 位址。

作業系統需求：

- Ubuntu Focal 20.04 (LTS)必須在指定的代理虛擬機器上安裝以下軟體包：
- Docker
- Docker-Compose
- JqChange `docker.sock`對於這個新權限： `sudo chmod 666 /var/run/docker.sock` 。

這 `deploy.sh`腳本執行所有必要的先決條件。

步驟如下：

1. 在指定虛擬機器上下載安裝包：

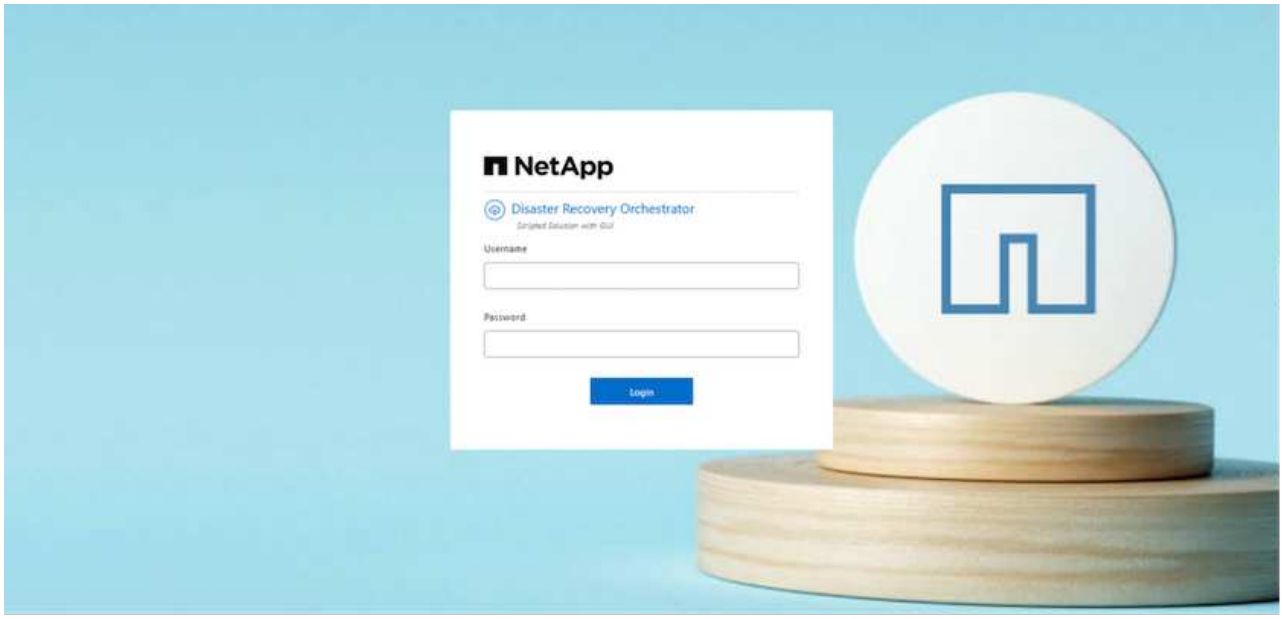
```
git clone https://github.com/NetApp/DRO-Azure.git
```

此代理程式必須安裝在輔助 AVS 站點區域或與 SDDC 不同的 AZ 中的主 AVS 站點區域。

2. 解壓縮安裝包，執行部署腳本，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. 使用以下憑證存取 UI：
   - 使用者名稱: `admin`
   - 密碼： `admin`



DRO 配置

正確配置Azure NetApp Files和 AVS 後，您可以開始設定 DRO 以自動將工作負載從主 AVS 站點還原到輔助 AVS 站點。 NetApp建議在輔助 AVS 站點部署 DRO 代理程式並配置 ExpressRoute 閘道連接，以便 DRO 代理程式可以透過網路與適當的 AVS 和Azure NetApp Files元件進行通訊。

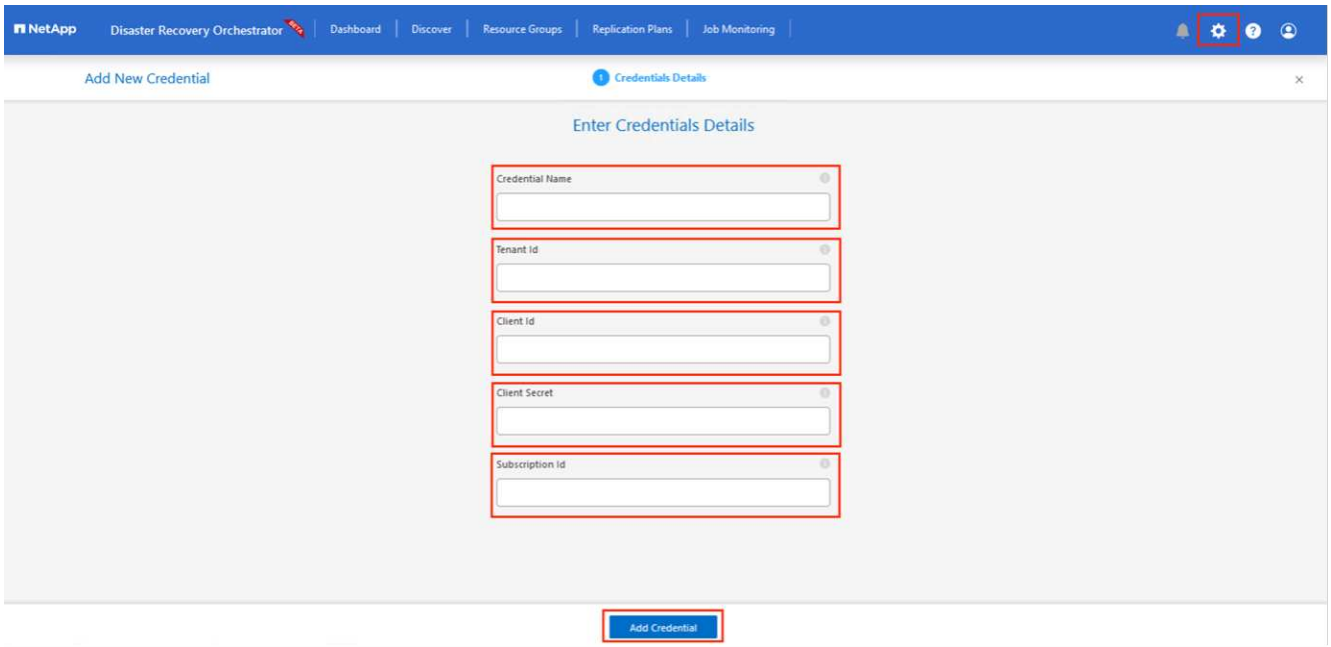
第一步是新增憑證。 DRO 需要權限才能發現Azure NetApp Files和 Azure VMware 解決方案。您可以透過建立和設定 Azure Active Directory (AD) 應用程式並取得 DRO 所需的 Azure 憑證來授予 Azure 帳戶所需的權限。您必須將服務主體綁定至您的 Azure 訂閱，並為其指派具有相關所需權限的自訂角色。新增來源環境和目標環境時，系統會提示您選擇與服務主體關聯的憑證。您需要將這些憑證新增至 DRO，然後才能按一下「新增網站」。

若要執行此操作，請完成以下步驟：

1. 在支援的瀏覽器中開啟 DRO 並使用預設使用者名稱和密碼(`admin/admin`）。首次登入後可以使用「更改密碼」選項重設密碼。
2. 在 DRO 控制台的右上角，按一下 設定 圖標，然後選擇 憑證。
3. 按一下「新增憑證」並按照精靈中的步驟進行操作。

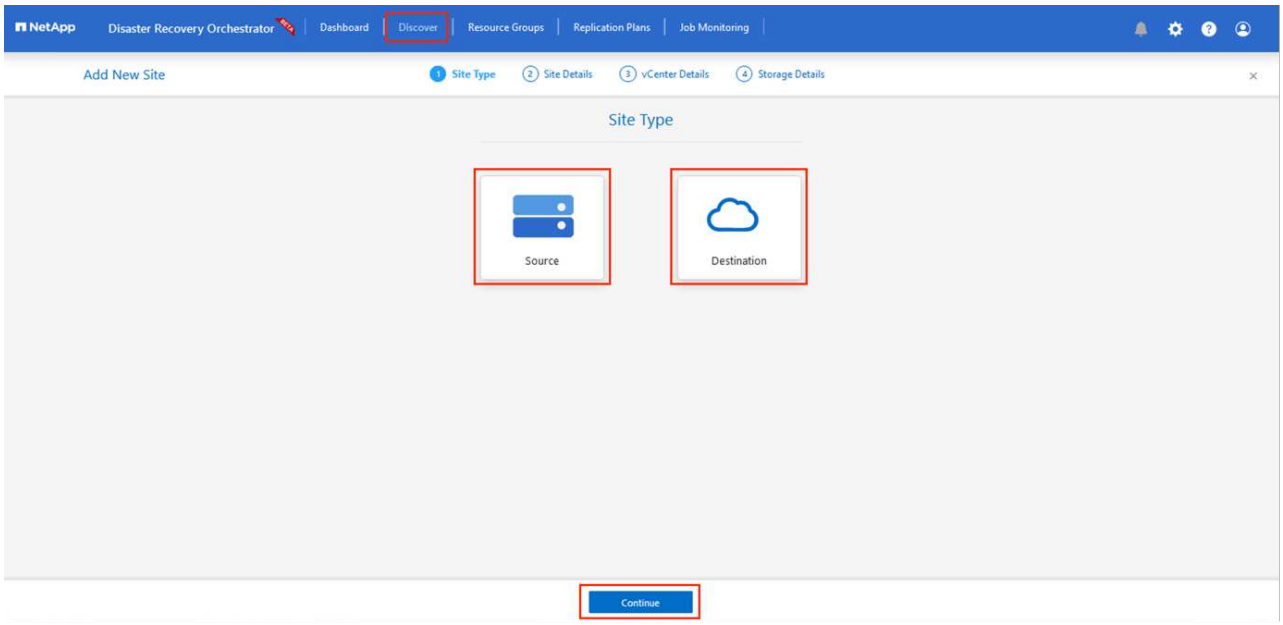
4. 若要定義憑證，請輸入有關授予所需權限的 Azure Active Directory 服務主體的資訊：
   - 憑證名稱
   - 租戶 ID
   - 客戶端 ID
   - 客戶端機密
   - 訂閱 ID

     您應該在建立 AD 應用程式時捕獲此資訊。
5. 確認有關新憑證的詳細信息，然後按一下「新增憑證」。



新增憑證後，就可以發現並將主 AVS 網站和輔助 AVS 網站（vCenter 和 Azure NetApp檔案儲存帳戶）新增至 DRO。若要新增來源站點和目標站點，請完成以下步驟：

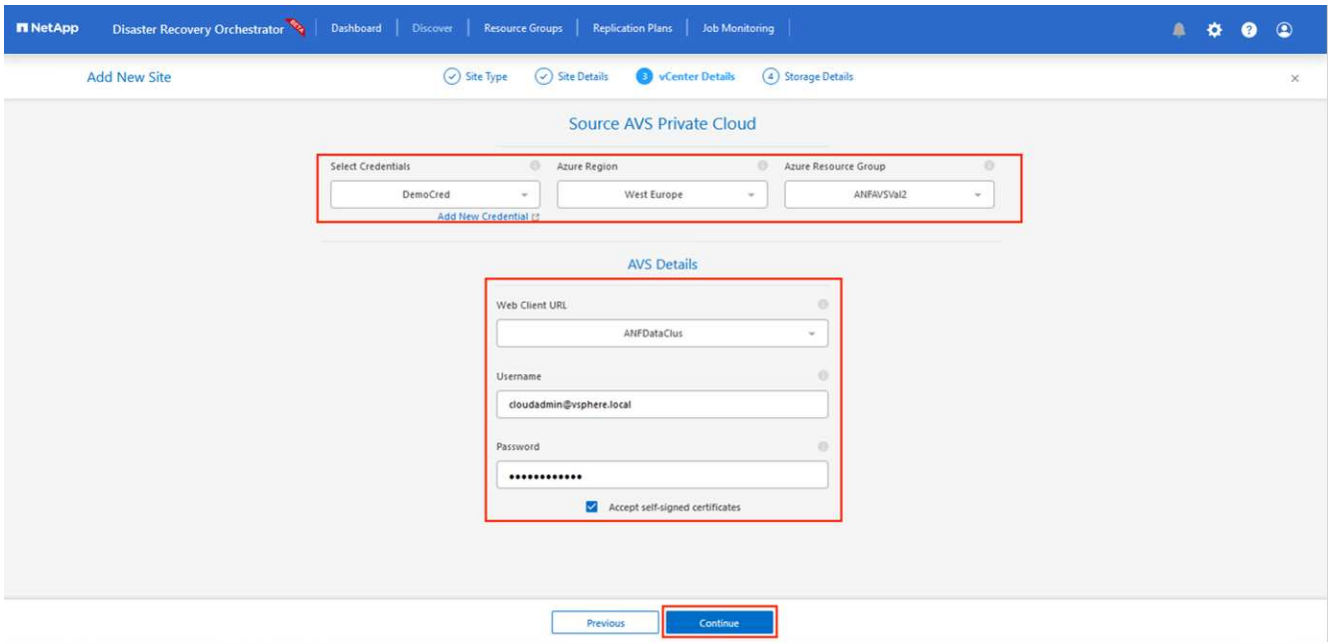
6. 轉到“發現”標籤。
7. 按一下“新增網站”。
8. 新增下列主要 AVS 網站（在控制台中指定為 來源）。
   - SDDC vCenter
   - Azure NetApp Files儲存帳戶
9. 新增下列輔助 AVS 網站（在控制台中指定為 目標）。
   - SDDC vCenter
   - Azure NetApp Files儲存帳戶



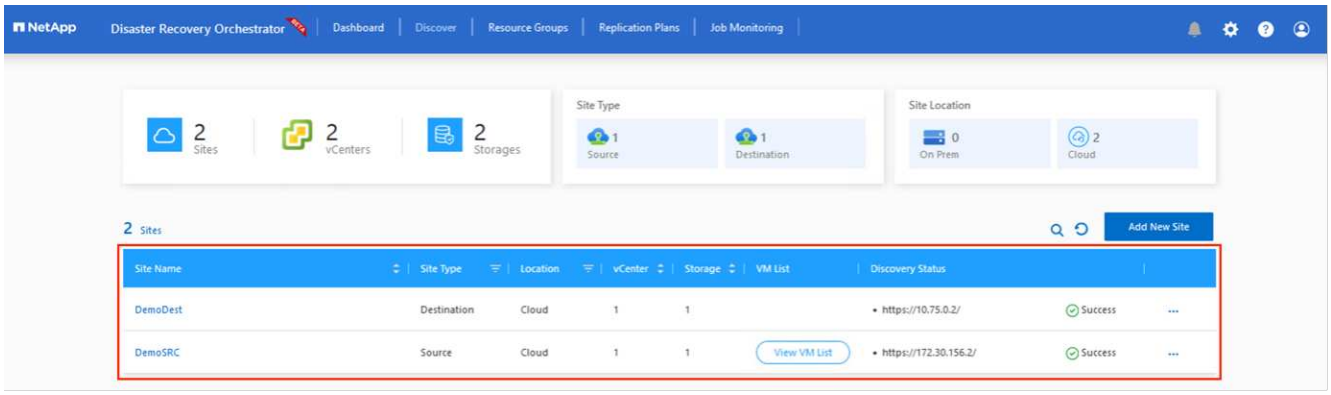
10. 透過點擊“來源”，輸入友善的網站名稱並選擇連接器來新增網站詳細資訊。然後點選“繼續”。

> 為了演示目的，本文檔涵蓋了新增來源網站的內容。

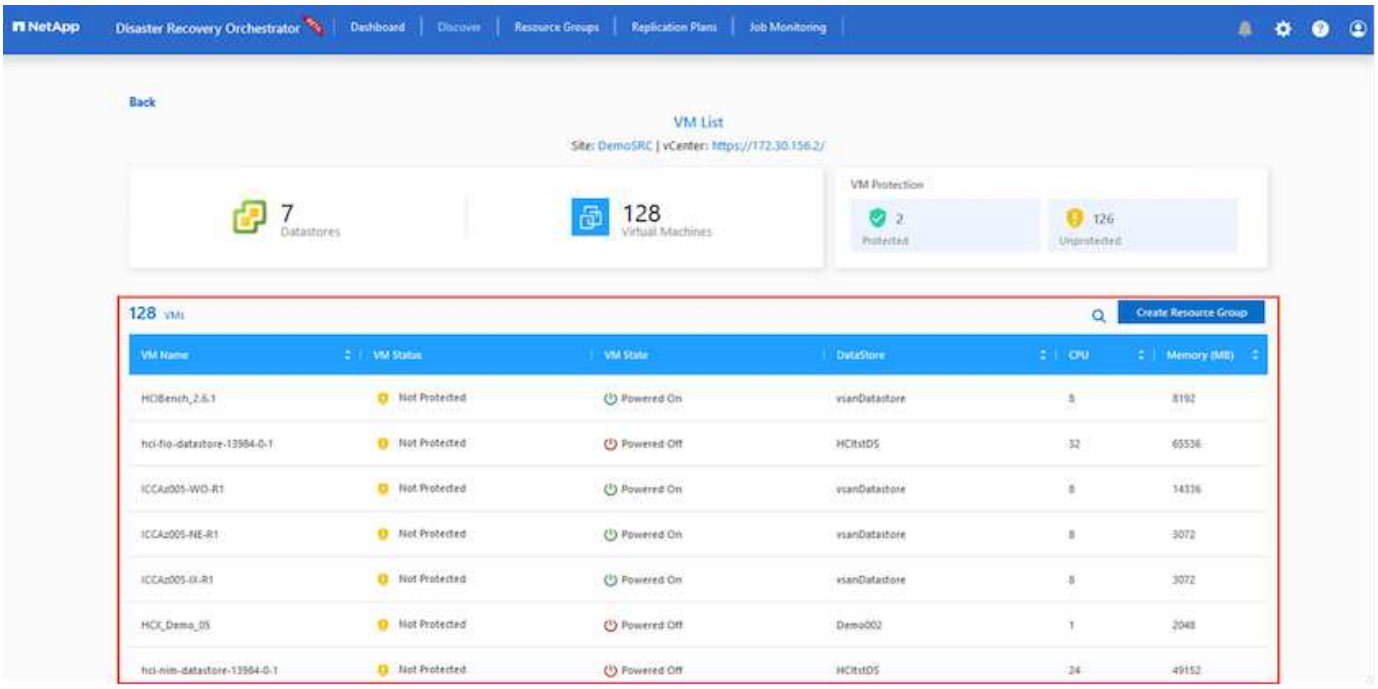
11. 更新 vCenter 詳細資訊。為此，請從主 AVS SDDC 的下拉清單中選擇憑證、Azure 區域和資源群組。
12. DRO 列出了該地區所有可用的 SDDC。從下拉式選單中選擇指定的私有雲 URL。
13. 輸入 `cloudadmin@vsphere.local`用戶憑證。可以從 Azure 入口網站存取。按照本文提到的步驟 "關聯"。完成後，按一下“繼續”。



14. 透過選擇 Azure 資源群組和NetApp帳戶來選擇來源儲存詳細資料 (ANF)。
15. 按一下“建立網站”。



新增後，DRO 會執行自動發現並顯示從來源站點到目標站點具有相應跨區域副本的虛擬機器。 DRO 會自動偵測虛擬機器使用的網路和區段並填滿它們。



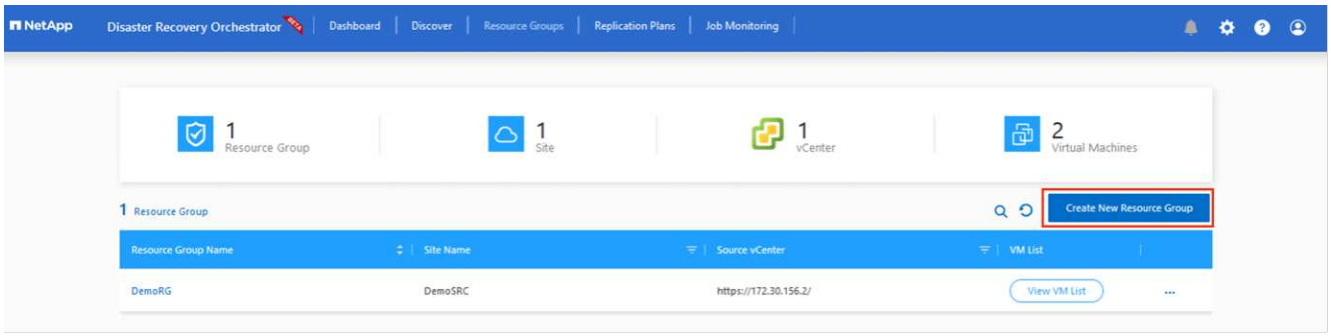
下一步是將所需的虛擬機器分組到其功能組中作為資源組。

資源分組

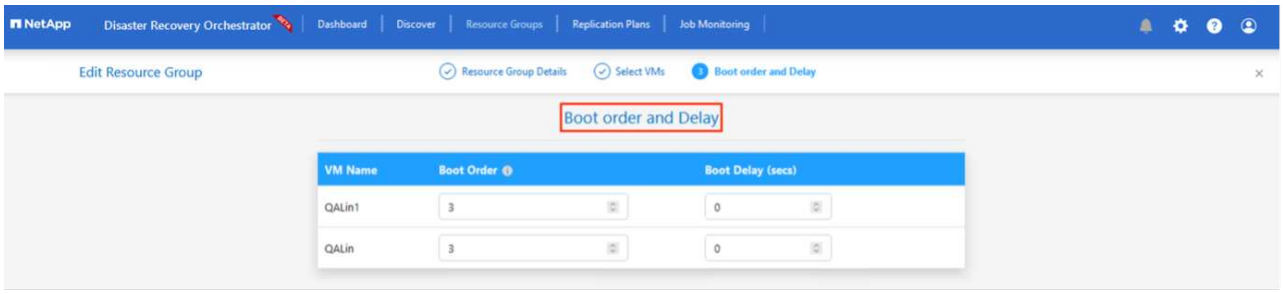
新增平台後，將要復原的虛擬機器分組到資源組。 DRO 資源群組可讓您將一組從屬虛擬機器分組為邏輯群組，這些邏輯群組包含它們的啟動順序、啟動延遲以及可在復原時執行的選用應用程式驗證。

若要開始建立資源組，請按一下「建立新資源組」功能表項目。

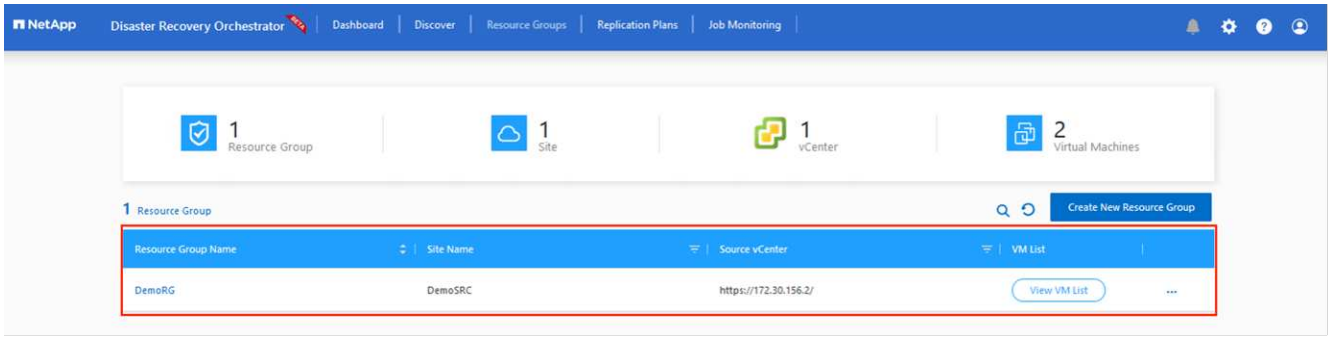
1. 訪問“資源組”並點擊“建立新資源組”。



2. 在新資源組下，從下拉式選單中選擇來源站點，然後按一下*建立*。
3. 提供資源組詳細信息，然後按一下“繼續”。
4. 使用搜尋選項選擇合適的虛擬機器。
5. 為所有選定的虛擬機器選擇*啟動順序*和*啟動延遲*（秒）。透過選擇每個虛擬機器並設定其優先順序來設定開機順序。所有虛擬機器的預設值為 3。選項如下：
   - 第一個啟動的虛擬機
   - 預設
   - 最後啟動的虛擬機



6. 按一下“建立資源組”。

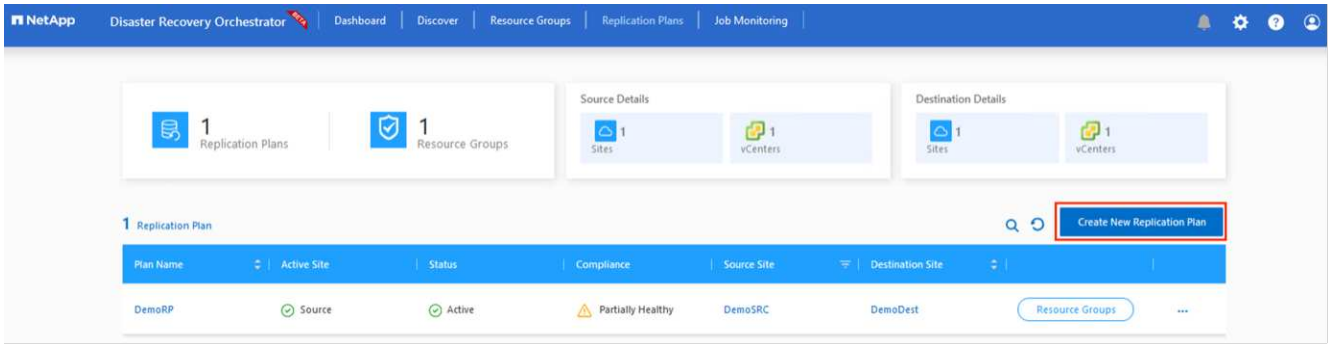


複製計劃

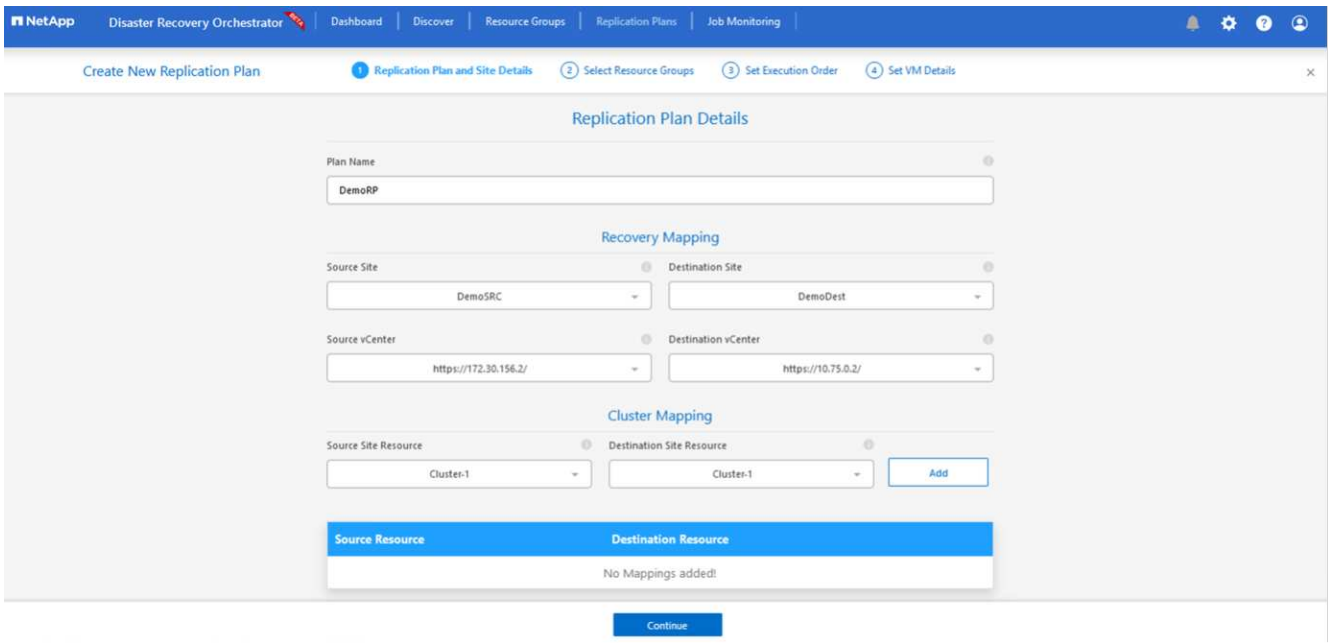
您必須制定一個在災難發生時恢復應用程式的計劃。從下拉式選單中選擇來源和目標 vCenter 平台，選擇要包含在此計畫中的資源群組，還包括應用程式應如何復原和啟動的分組（例如，網域控制站、第 1 層、第 2 層等）。計劃通常也被稱為藍圖。若要定義復原計劃，請導覽至「複製計劃」選項卡，然後按一下「新複製計劃」。

若要開始建立複製計劃，請完成以下步驟：

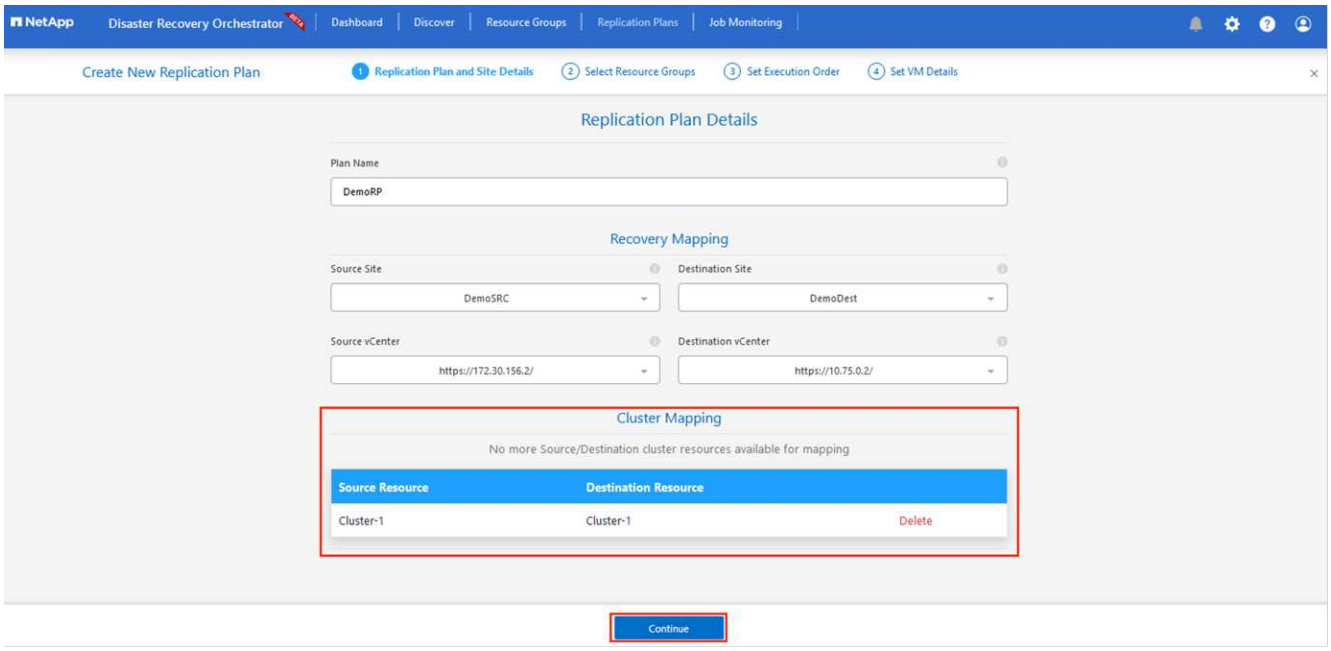
1. 導航至*複製計劃*並點擊*建立新複製計劃*。



2. 在*新複製計劃*上，提供計劃名稱並透過選擇來源網站、關聯 vCenter、目標網站和關聯 vCenter 來新增復原對應。

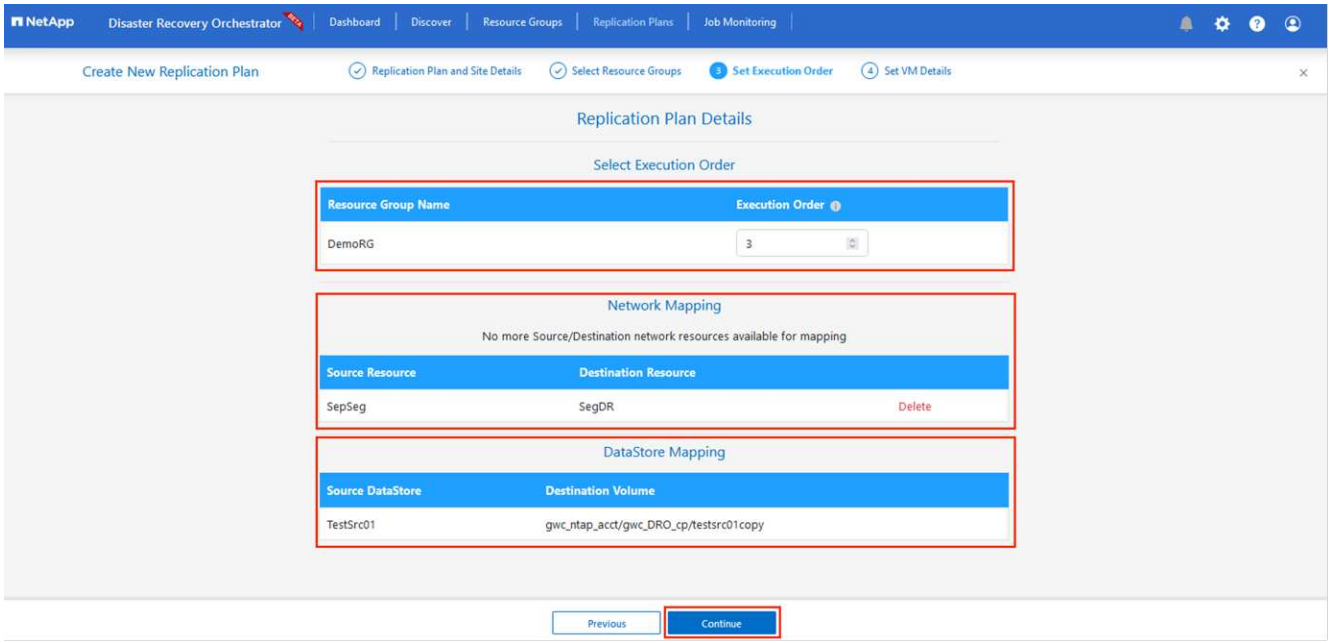


3. 恢復映射完成後，選擇*集群映射*。



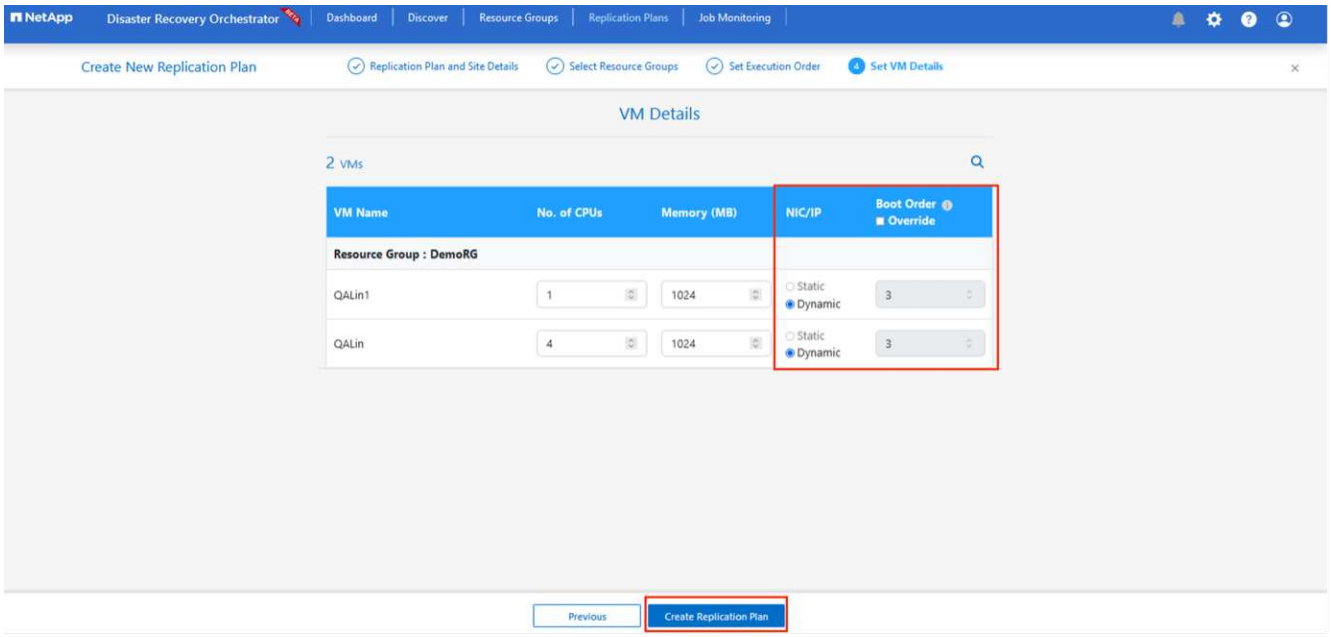
4. 選擇*資源組詳情*並點選*繼續*。
5. 設定資源組的執行順序。當存在多個資源組時，此選項可讓您選擇操作順序。
6. 完成後，將網路映射設定到適當的段。這些段應該已經在輔助 AVS 叢集上配置，並且要將虛擬機器對應到這些段，請選擇適當的段。
7. 根據虛擬機器的選擇自動選擇資料儲存映射。

跨區域複製（CRR）處於磁碟區層級。因此，駐留在對應磁碟區上的所有虛擬機器都會複製到 CRR 目標。確保選擇資料儲存區中的所有虛擬機，因為只有複製計畫中的虛擬機才會被處理。

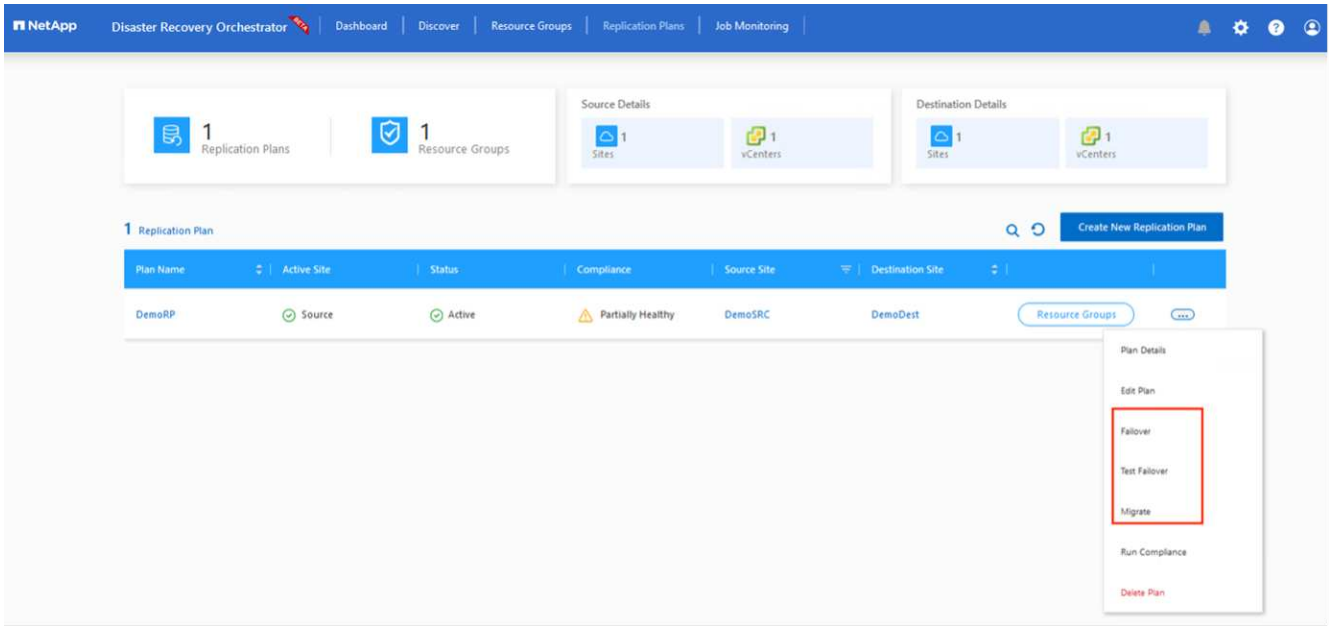


8. 在 VM 詳細資料下，您可以選擇調整 VM 的 CPU 和 RAM 參數。當您將大型環境還原到較小的目標叢集或進行 DR 測試而無需配置一對一的實體 VMware 基礎架構時，這會非常有用。另外，修改資源組中所有選定

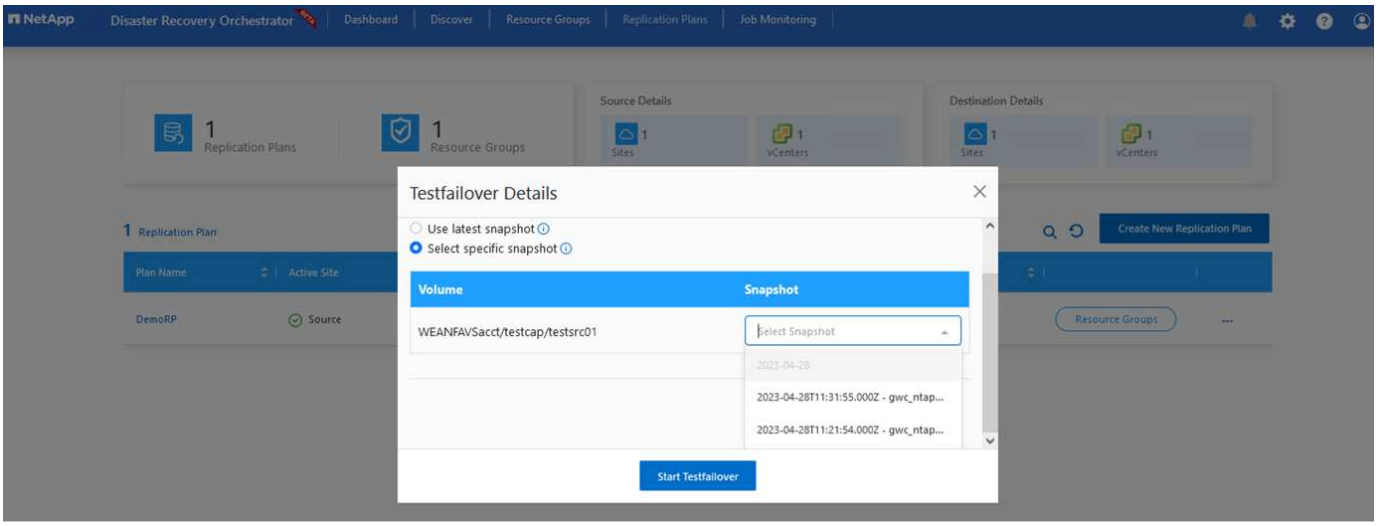
虛擬機器的啟動順序和啟動延遲（秒）。如果需要對資源組啟動順序選擇過程中選擇的內容進行任何更改，則可以使用附加選項來修改啟動順序。預設情況下，使用資源組選擇期間選擇的啟動順序，但可以在此階段執行任何修改。



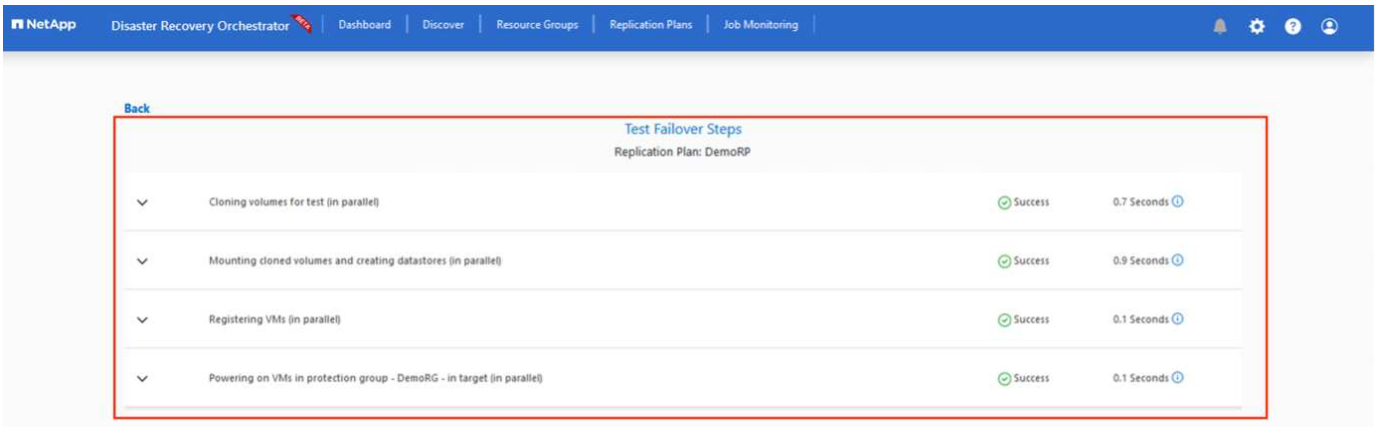
9. 按一下*建立複製計劃*。建立複製計劃後，您可以根據需要執行故障轉移、測試故障轉移或遷移選項。



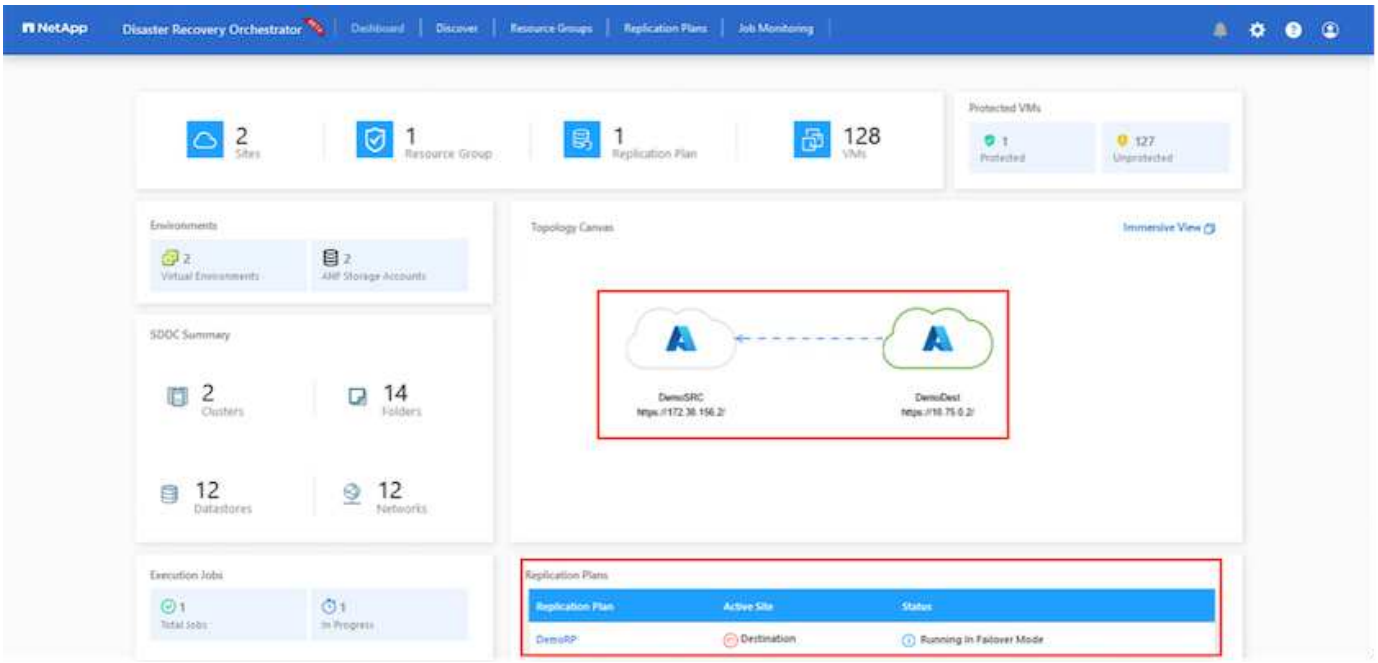
在故障轉移和測試故障轉移選項期間，使用最新的快照，或者可以從時間點快照中選擇特定快照。如果您面臨勒索軟體之類的損壞事件，則時間點選項可能非常有用，其中最新的副本已被破壞或加密。 DRO 顯示所有可用的時間點。



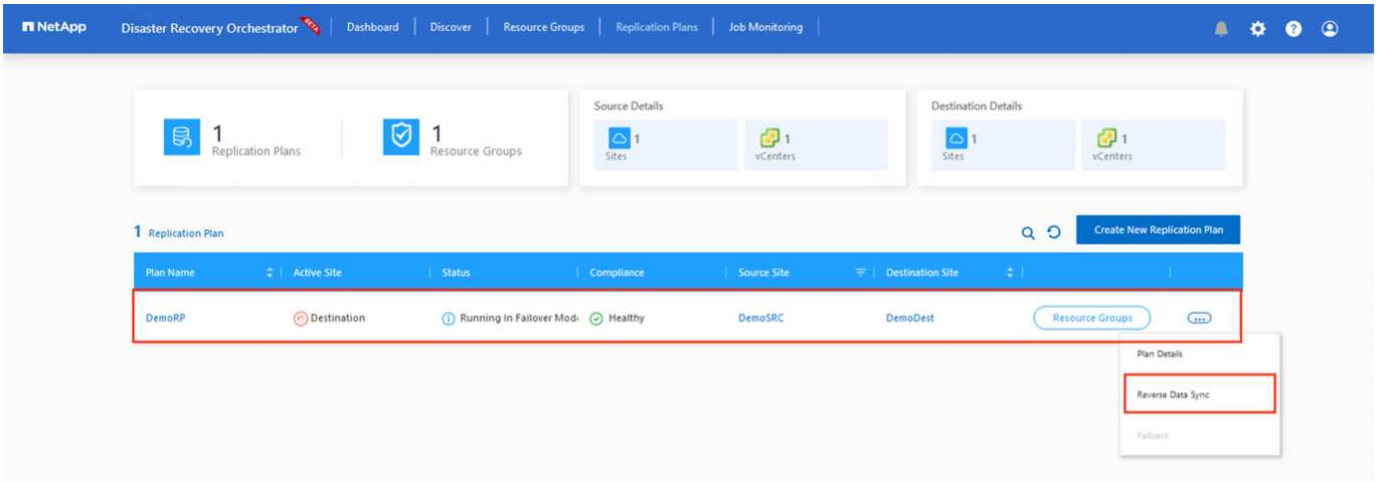
若要使用複製計畫中指定的配置觸發故障轉移或測試故障轉移，您可以按一下*故障轉移*或*測試故障轉移*。您可以在任務選單中監控複製計劃。



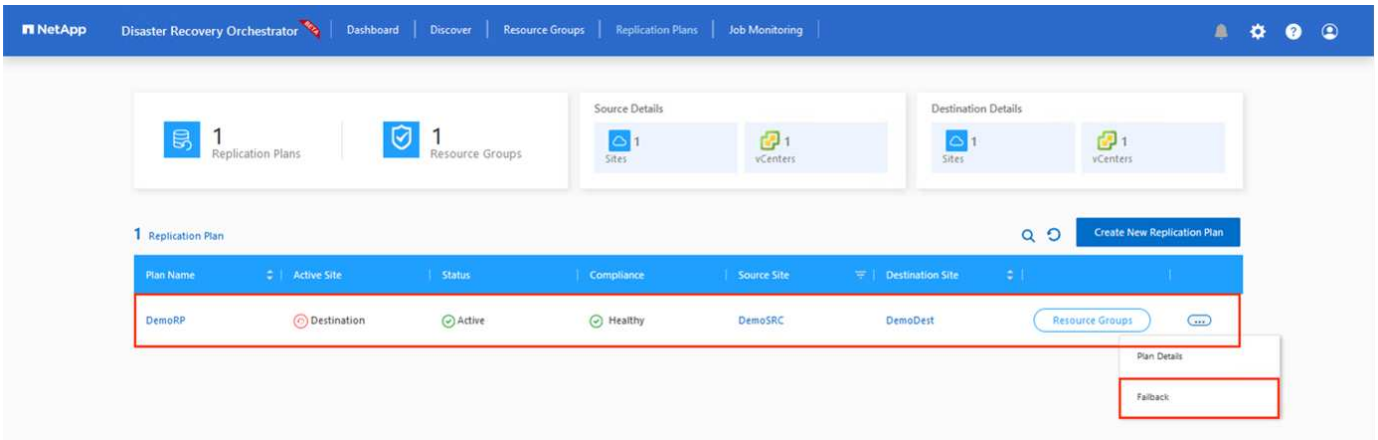
觸發故障轉移後，可以在輔助站點 AVS SDDC vCenter（虛擬機器、網路和資料儲存區）中看到復原的項目。預設情況下，虛擬機器將恢復到工作負載資料夾。

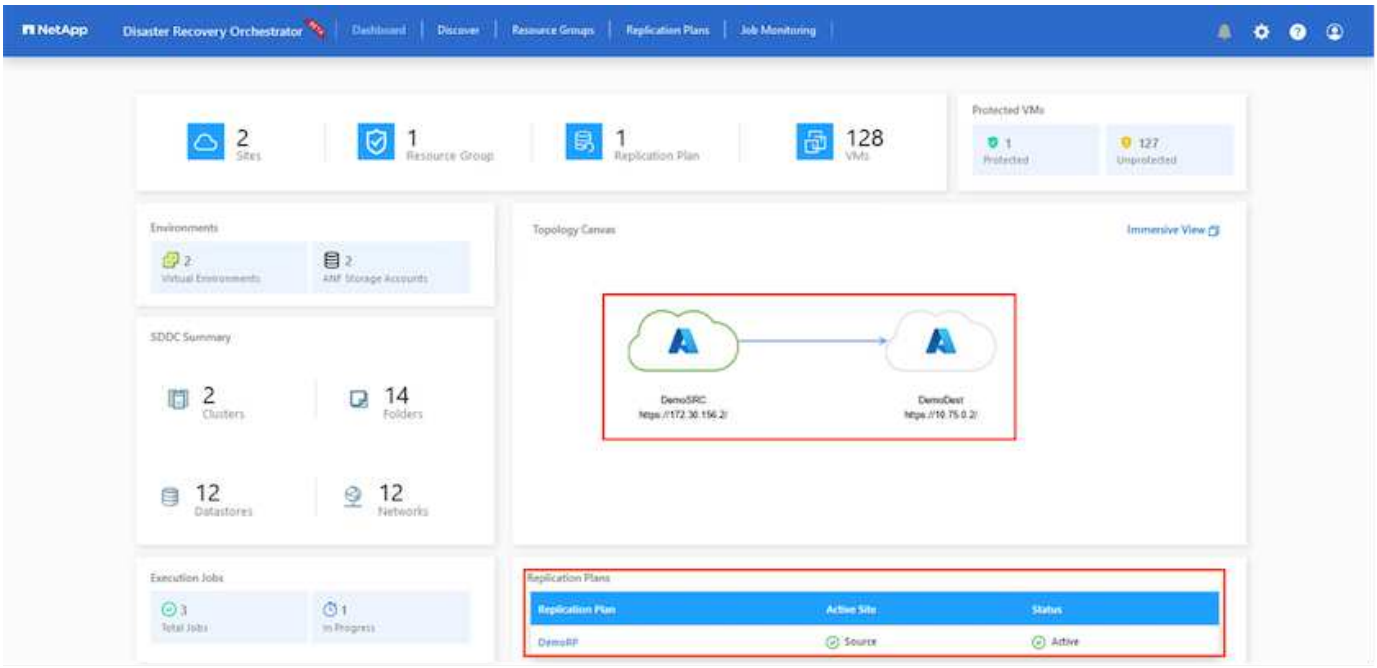


可以在複製計劃層級觸發故障恢復。如果發生測試故障轉移，可以使用拆除選項來回變更並刪除新建立的磁碟區。與故障轉移相關的故障回復是一個兩步驟過程。選擇複製計劃並選擇*反向資料同步*。



此步驟完成後，觸發故障復原以移回主 AVS 站點。





從 Azure 入口網站中，我們可以看到，對於作為讀取/寫入磁碟區對應到輔助網站 AVS SDDC 的對應磁碟區，複製運作狀況已中斷。在測試故障轉移期間，DRO 不會對應目標磁碟區或副本磁碟區。相反，它會創建所需的跨區域複製快照的新卷，並將該卷公開為數據存儲，這會消耗容量池中的額外物理容量並確保源卷不會被修改。值得注意的是，複製作業可以在 DR 測試或分類工作流程期間繼續進行。此外，此過程可確保可以清理恢復，而不會在發生錯誤或恢復損壞的資料時存在副本被破壞的風險。

勒索軟體恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體來說，IT 組織很難確定安全的返回點，而且，一旦確定，如何確保恢復的工作負載免受再次發生的攻擊（例如，來自休眠惡意軟體或透過易受攻擊的應用程式）。

DRO 透過允許組織從任何可用的時間點恢復來解決這些問題。然後將工作負載恢復到功能齊全但隔離的網路中，以便應用程式可以運行並相互通信，但不會暴露於任何南北流量。此過程為安全團隊提供了一個安全的地方來進行取證並識別任何隱藏或休眠的惡意軟體。

結論

Azure NetApp Files和 Azure VMware 災難復原解決方案為您提供以下優勢：

- 利用高效且有彈性的Azure NetApp Files跨區域複製。
- 透過快照保留還原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到數千台虛擬機器。
- 工作負載復原利用「從最新的快照建立新磁碟區」流程，該過程不會操作複製的磁碟區。
- 避免磁碟區或快照上的任何資料損壞風險。
- 避免 DR 測試工作流程期間的複製中斷。
- 利用 DR 資料和雲端運算資源進行 DR 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 最佳化可以透過允許恢復到較小的運算叢集來幫助降低雲端成本。

在哪裡可以找到更多信息

要了解有關本文檔中描述的信息的更多信息，請查看以下文檔和/或網站：

- 為Azure NetApp Files建立磁碟區複製

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

- Azure NetApp Files磁碟區的跨區域複製

  "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 上部署並配置虛擬化環境

  "在 Azure 上設定 AVS"

- 部署和配置 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**資料儲存區對 **Azure VMware** 解決方案進行災難復原

Azure NetApp Files (ANF) 資料儲存體將儲存體與運算分離，並釋放了任何組織將其工作負載轉移到雲端所需的靈活性。它為客戶提供靈活、高效能的儲存基礎設施，可獨立於運算資源進行擴充。 Azure NetApp Files資料儲存簡化並最佳化了與 Azure VMware 解決方案 (AVS) 一起的部署，作為本地 VMWare 環境的災難復原站點。

概況

基於Azure NetApp Files(ANF) 磁碟區的 NFS 資料儲存可用於使用任何經過驗證的提供 VM 複製功能的第三方解決方案從本機複製資料。透過新增Azure NetApp Files資料存儲，它將實現成本優化部署，而不是建立具有大量 ESXi 主機來容納儲存的 Azure VMware 解決方案 SDDC。這種方法被稱為「Pilot Light Cluster」。試點燈叢集是最小 AVS 主機配置（3 x AVS 節點）以及Azure NetApp Files資料儲存容量。

目標是維護一個擁有所有核心組件的低成本基礎設施來處理故障轉移。如果發生故障轉移，指示燈叢集可以擴展並提供更多的 AVS 主機。一旦故障轉移完成並且恢復正常操作，指示燈叢集就可以縮減到低成本的運作模式。

本文件的目的

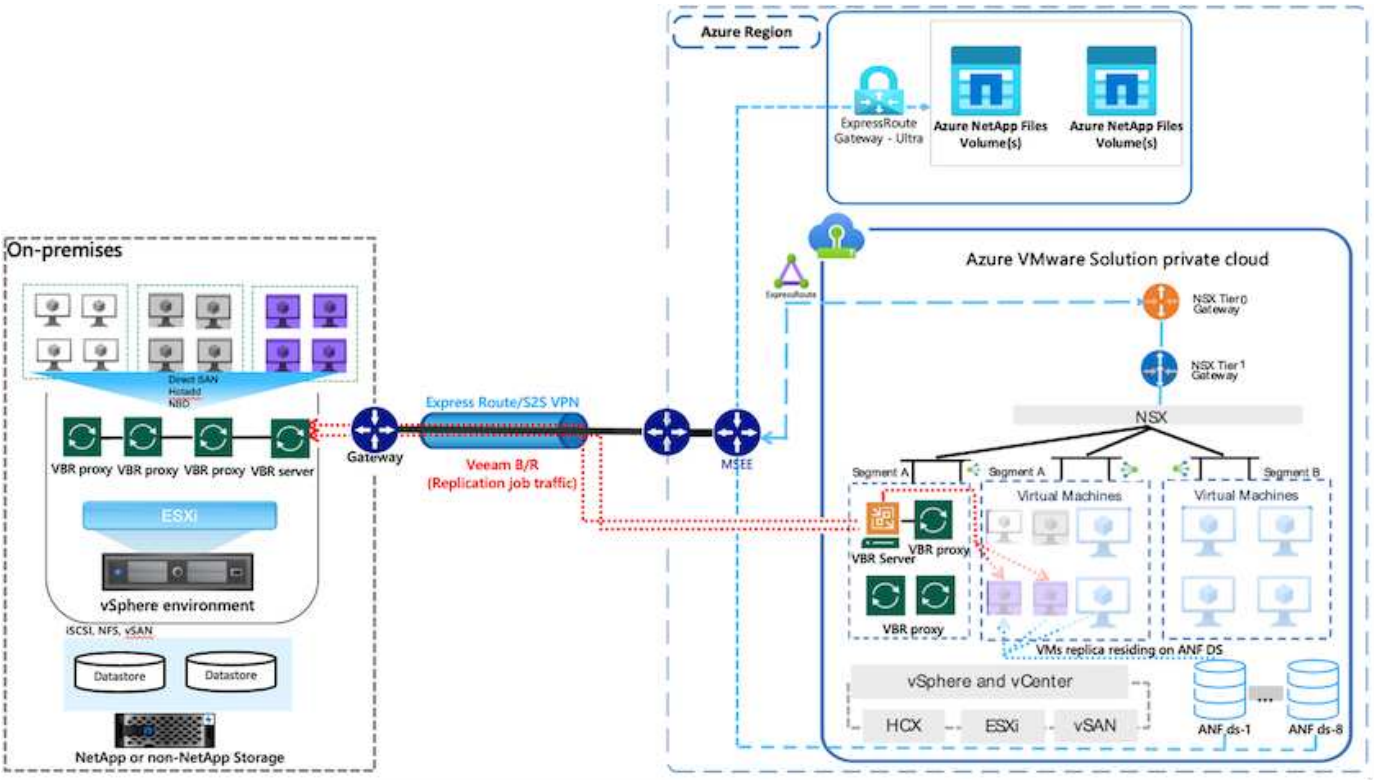
本文介紹如何將Azure NetApp Files資料儲存與 Veeam Backup 和複製結合使用，以使用 Veeam VM 複製軟體功能為本機 VMware VM 到 (AVS) 設定災難復原。

Veeam Backup & Replication 是一款用於虛擬環境的備份和複製應用程式。當虛擬機器被複製時，Veeam Backup & Replication 會從 AVS 上複製，該軟體將在目標 AVS SDDC 叢集上以原生 VMware vSphere 格式建立虛擬機器的精確副本。 Veeam Backup & Replication 將使副本與原始 VM 保持同步。複製提供了最佳的復原時間目標 (RTO)，因為 DR 站點上有一個處於準備啟動狀態的 VM 的安裝副本。

這種複製機制可確保在災難事件發生時工作負載能夠在 AVS SDDC 中快速啟動。 Veeam Backup & Replication

軟體也優化了透過 WAN 和慢速連線進行複製的流量傳輸。此外，它還過濾掉重複的資料區塊、零資料區塊、交換檔案和「排除的 VM 客戶作業系統檔案」。該軟體還將壓縮副本流量。為了防止複製作業消耗整個網路頻寬，可以利用 WAN 加速器和網路限制規則。

Veeam Backup & Replication 中的複製過程由作業驅動，這表示複製是透過設定複製作業來執行的。如果發生災難事件，可以觸發故障轉移，透過故障轉移到其副本來恢復虛擬機器。當執行故障轉移時，複製的虛擬機器將接管原始虛擬機器的角色。可以執行故障轉移至副本的最新狀態或任何已知的良好還原點。這使得勒索軟體恢復或隔離測試能夠根據需要進行。 Veeam Backup & Replication 提供多種選項來處理不同的災難復原場景。



解決方案部署

進階步驟

1. Veeam Backup and Replication 軟體在具有適當網路連線的本機環境中運作。
2. "部署 Azure VMware 解決方案 (AVS)"私有雲和"附加Azure NetApp Files資料存儲"到 Azure VMware 解決方案主機。

   可以使用以最小配置設定的指示燈環境來實現 DR 目的。一旦發生事故，虛擬機器將故障轉移到該集群，並且可以添加其他節點）。

3. 設定複製作業以使用 Veeam Backup and Replication 建立 VM 副本。
4. 建立故障轉移計劃並執行故障轉移。
5. 災難事件結束且主站點啟動後，切換回生產虛擬機器。

Veeam VM 複製到 **AVS** 和 **ANF** 資料儲存區的先決條件

1. 確保 Veeam Backup & Replication 備份 VM 連線到來源以及目標 AVS SDDC 叢集。

2. 備份伺服器必須能夠解析短名稱並連接到來源 vCenter 和目標 vCenter。
3. 目標Azure NetApp Files資料儲存必須有足夠的可用空間來儲存複製的 VM 的 VMDK。

有關更多信息，請參閱“注意事項和限制”"這裡" 。

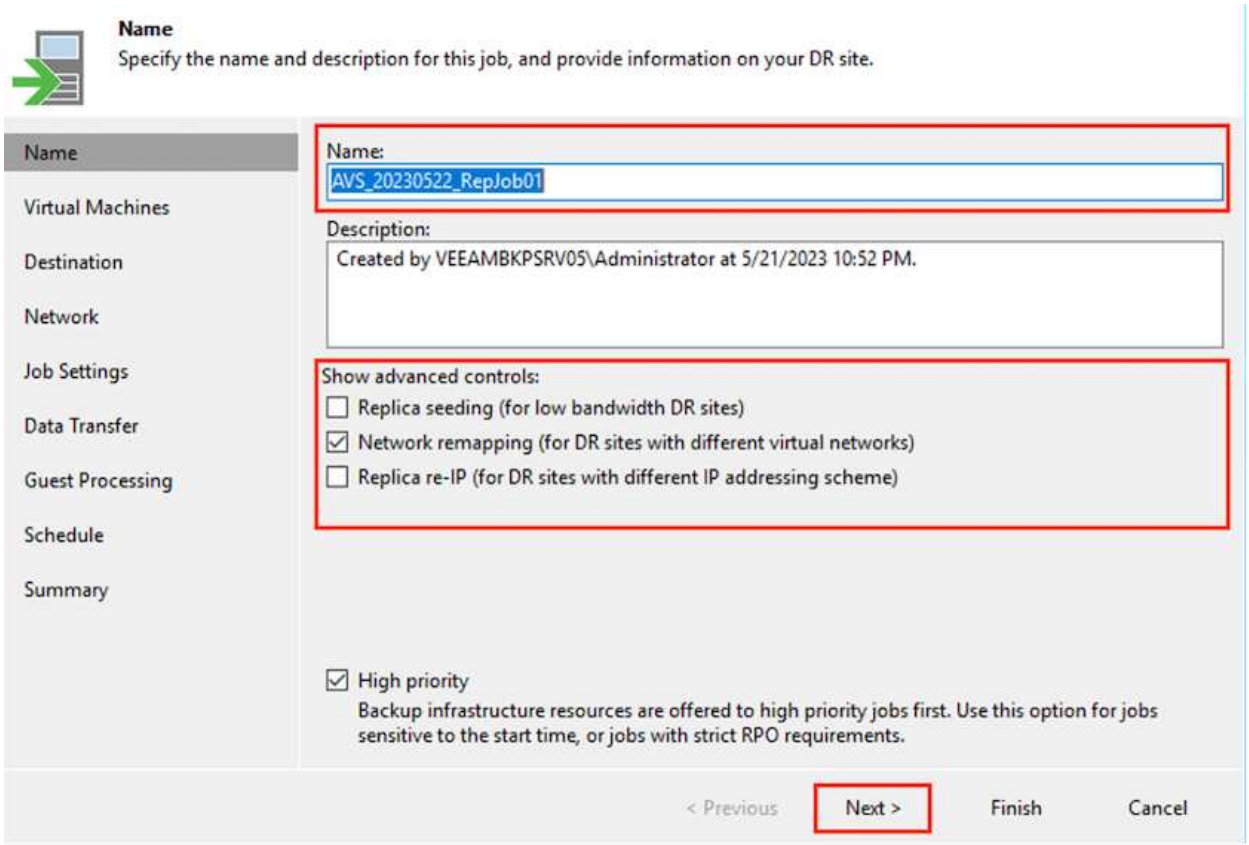
部署詳情

▼ 步驟 **1**：複製虛擬機

Veeam Backup & Replication 利用 VMware vSphere 快照功能/在複製期間，Veeam Backup & Replication 請求 VMware vSphere 建立 VM 快照。 VM 快照是 VM 的時間點副本，其中包括虛擬磁碟、系統狀態、配置和元資料。 Veeam Backup & Replication 使用快照作為複製的資料來源。

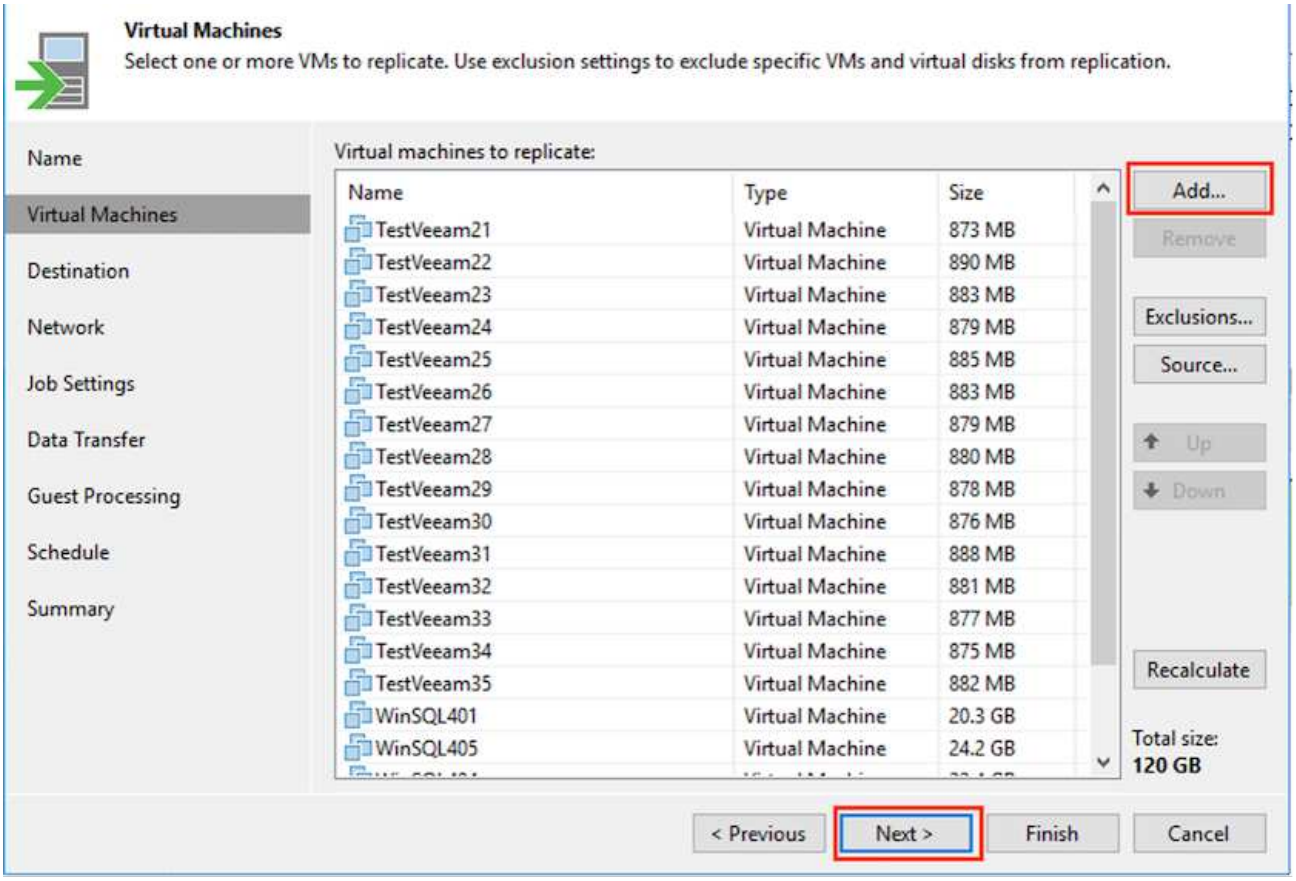
若要複製虛擬機，請依照下列步驟操作：

1. 開啟 Veeam 備份和複製控制台。
2. 在主頁視圖上。右鍵點選作業節點並選擇複製作業>虛擬機器。
3. 指定作業名稱並選擇適當的進階控制複選框。按一下“下一步”。
   - 如果本機和 Azure 之間的連線頻寬受限，請勾選「副本種子」複選框。 *如果 Azure VMware 解決方案 SDDC 上的段與本機站台網路的段不匹配，請勾選「網路重新對應（針對具有不同網路的 AVS SDDC 站台）」複選框。
   - 如果本機生產站點中的 IP 位址方案與目標 AVS 站點中的方案不同，請勾選「副本重新 IP（適用於具有不同 IP 位址方案的 DR 站點）」複選框。

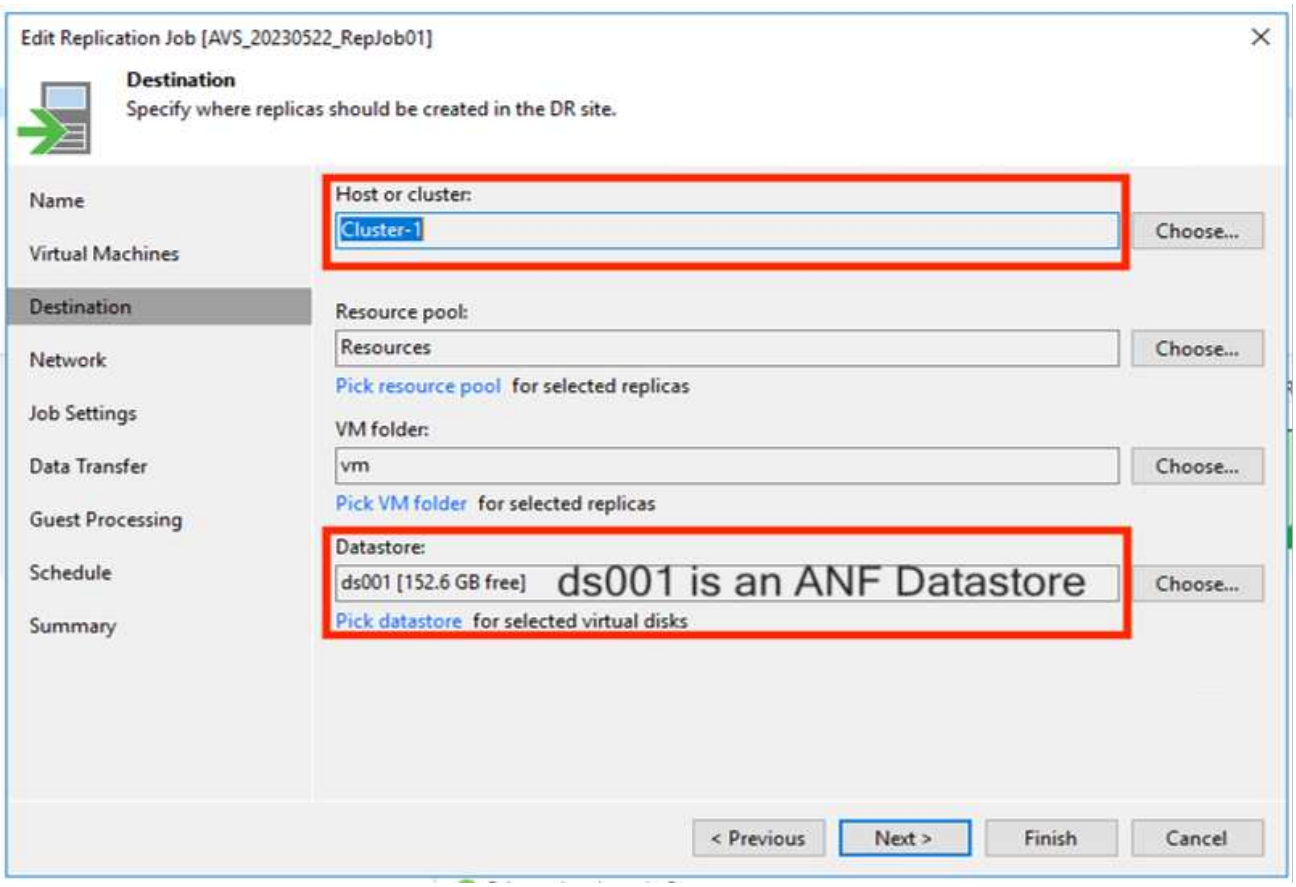


4. 在「虛擬」電腦*步驟中選擇要複製到附加到 **Azure VMware** 解決方案 **SDDC**的 **Azure NetApp Files**資料儲存的 **VM**。可以將虛擬機器放置在 **vSAN** 上以填入可用的 **vSAN** 資料儲存容量。在試點叢集中，**3** 節

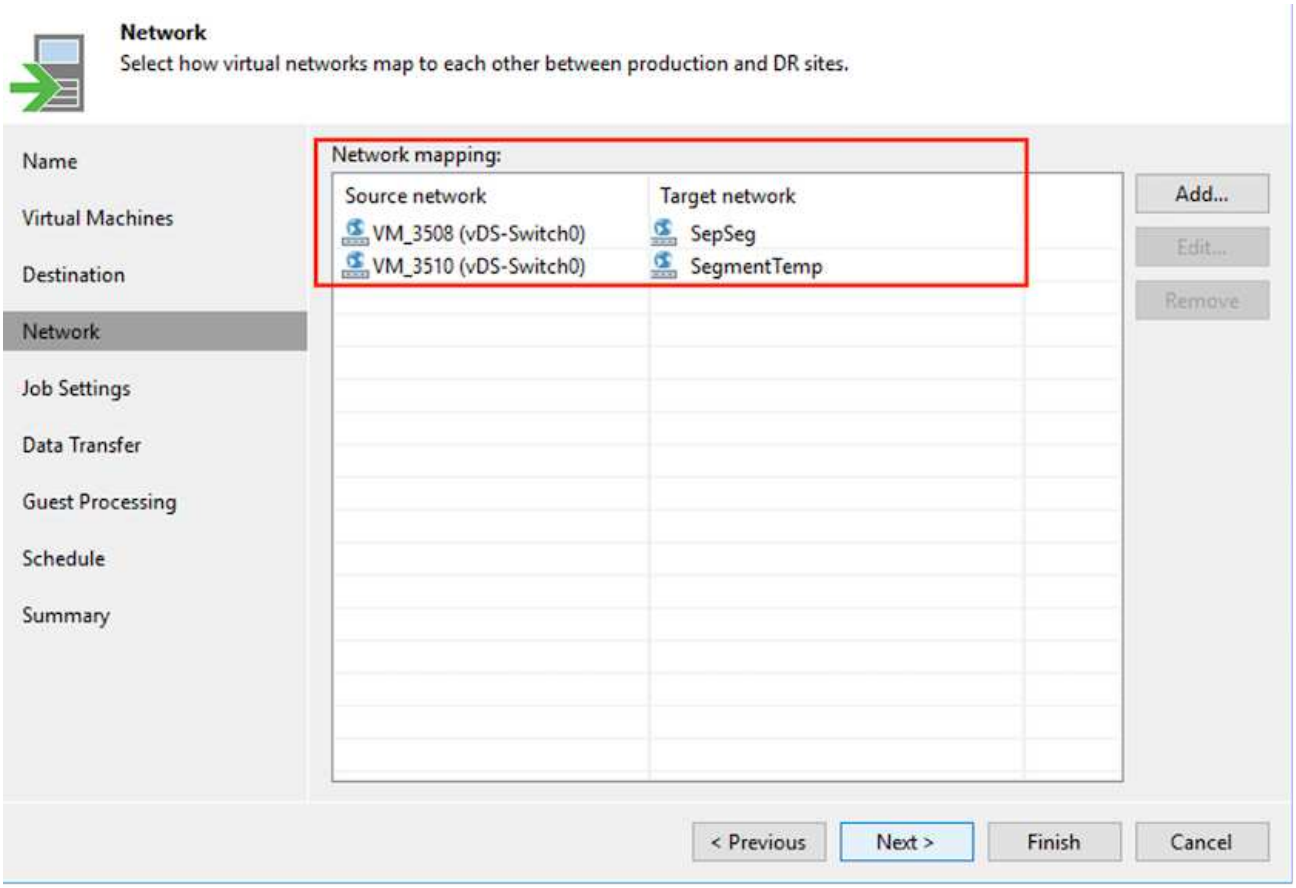
點叢集的可用容量將受到限制。其餘資料可輕鬆放置在**Azure NetApp Files**資料儲存中，以便可以恢復虛擬機，並且擴展叢集以滿足 **CPU**/記憶體需求。按一下*新增，然後在*新增物件*視窗中選擇必要的虛擬機器或虛擬機器容器，然後按一下*新增*。按一下“下一步”。



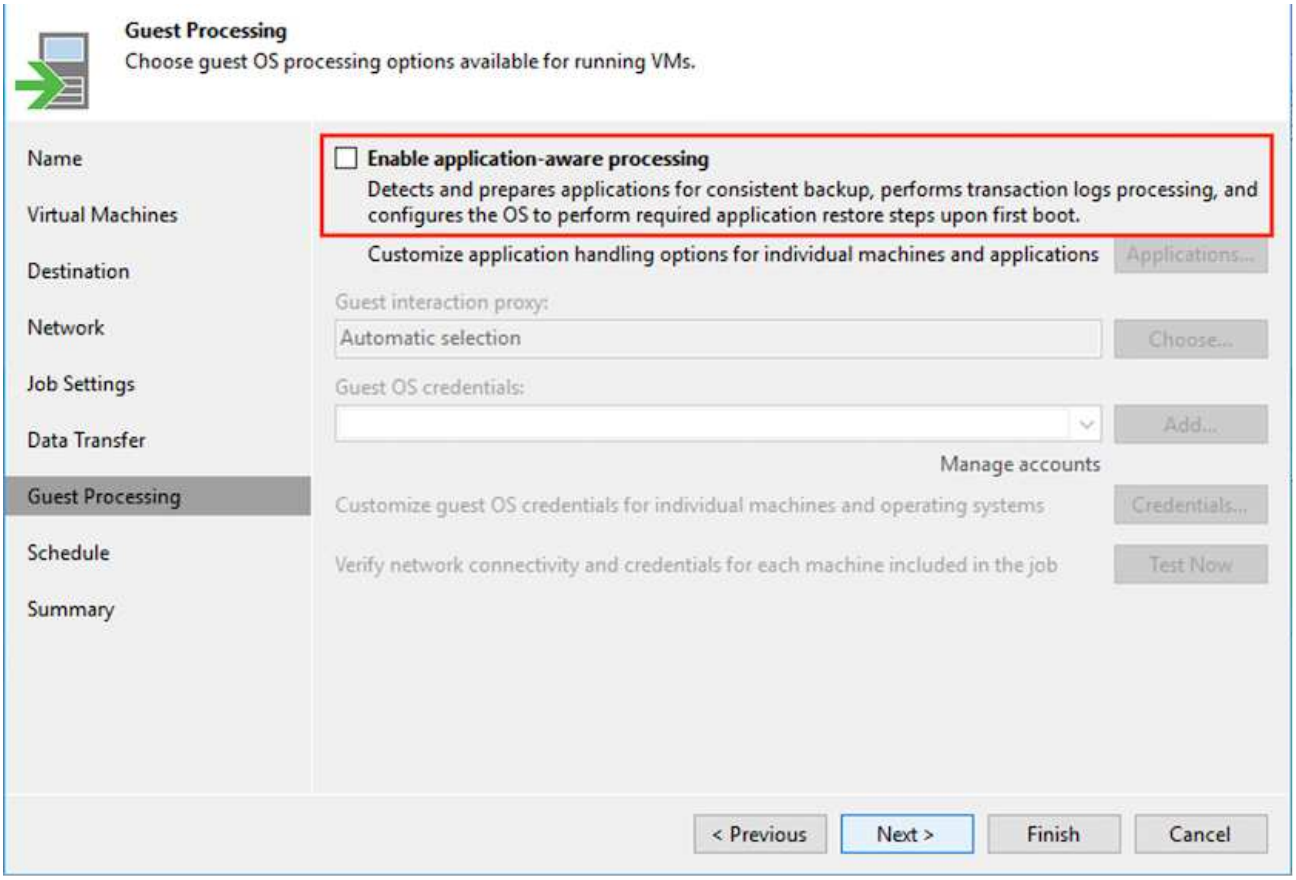
5. 之後，選擇目標作為 Azure VMware 解決方案 SDDC 叢集/主機，並選擇適當的資源池、VM 資料夾和 VM 副本的 FSx ONTAP資料儲存。然後按一下“下一步”。



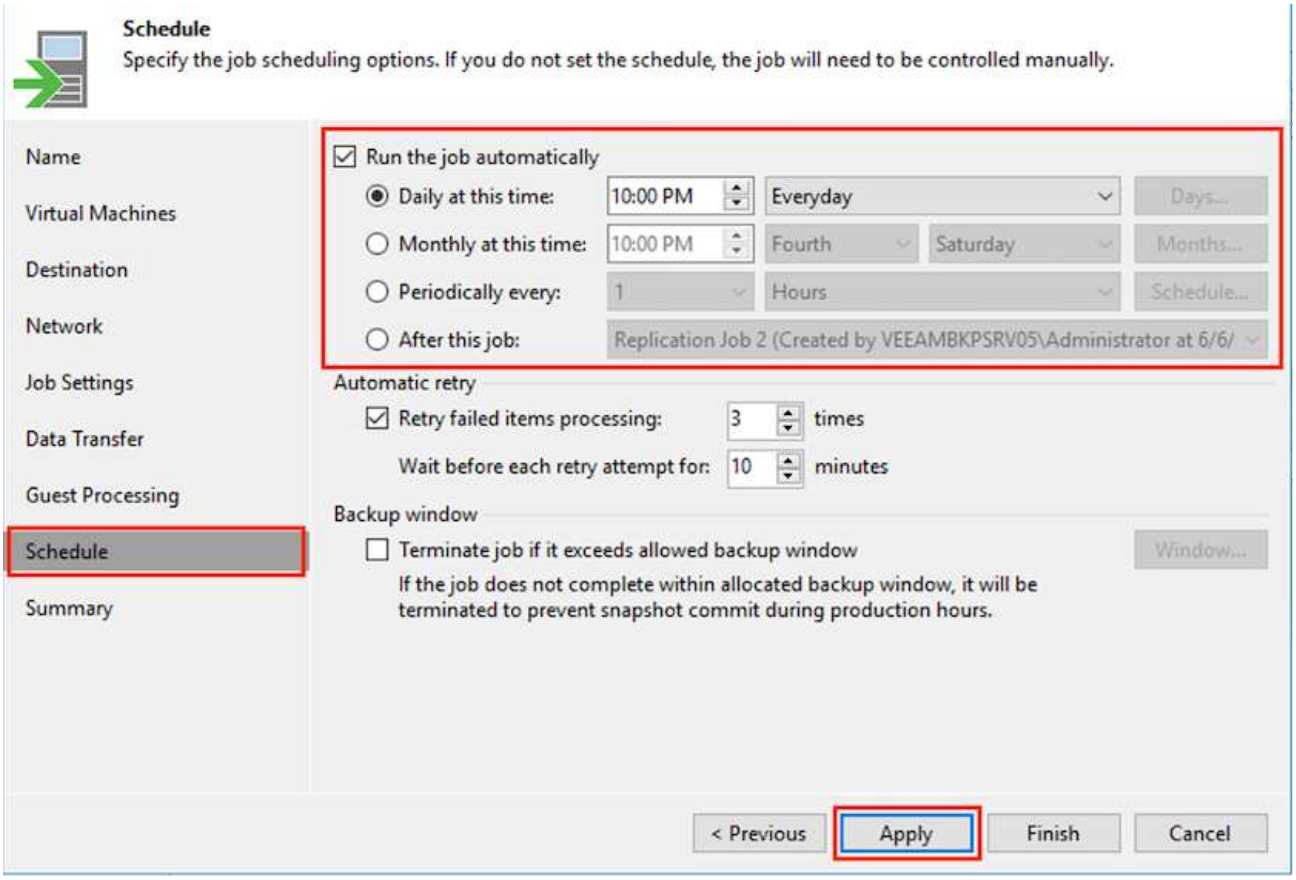
6. 下一步根據需要建立來源虛擬網路和目標虛擬網路之間的對應。



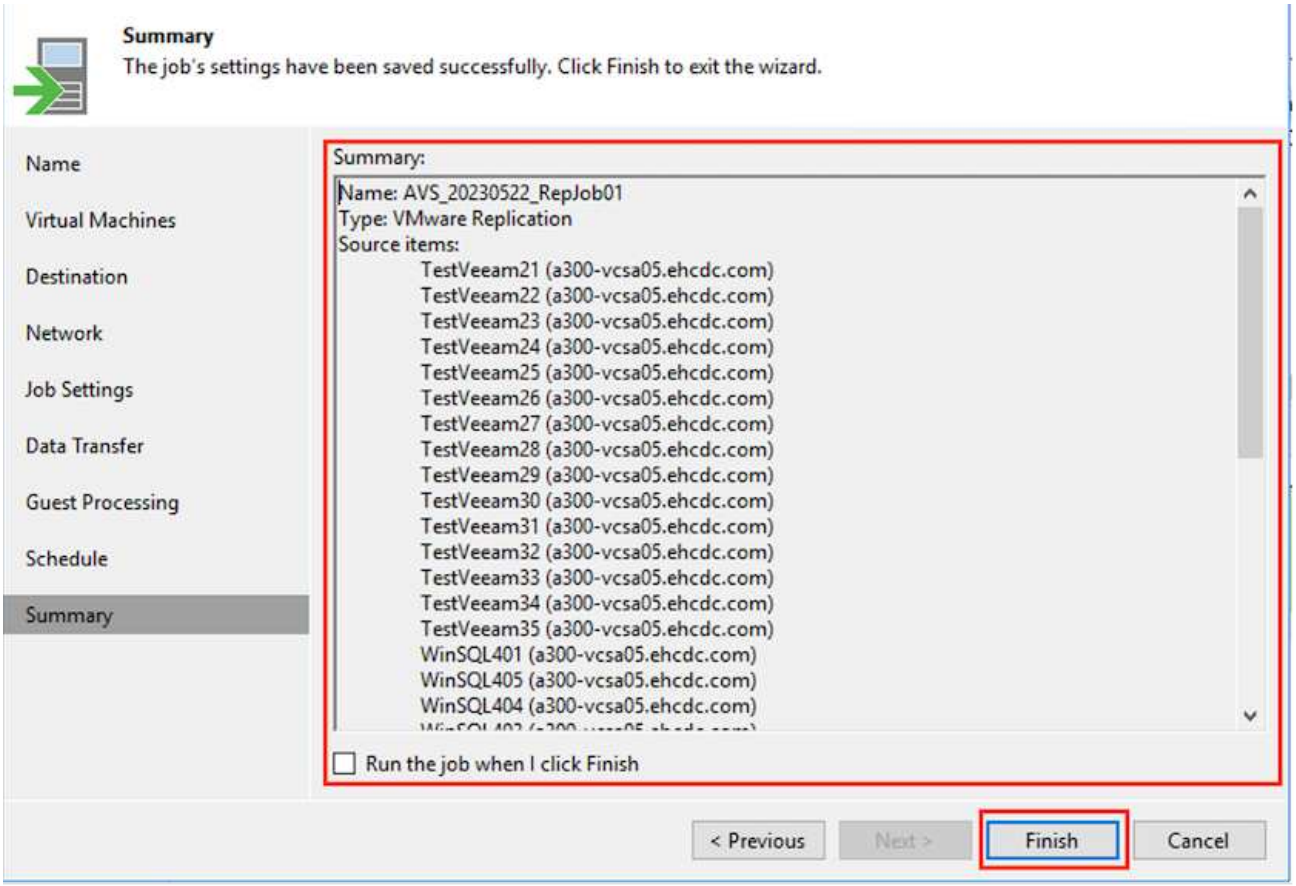
7. 在*作業設定*步驟中，指定將儲存 VM 副本、保留原則等元資料的備份儲存庫。
8. 在*資料傳輸*步驟中更新*來源*和*目標*代理伺服器，保留*自動*選擇（預設）並保持選擇*直接*選項，然後按一下*下一步*。
9. 在*Guest Processing*步驟中，依需求選擇*Enable application-aware processing*選項。按一下“下一步”。



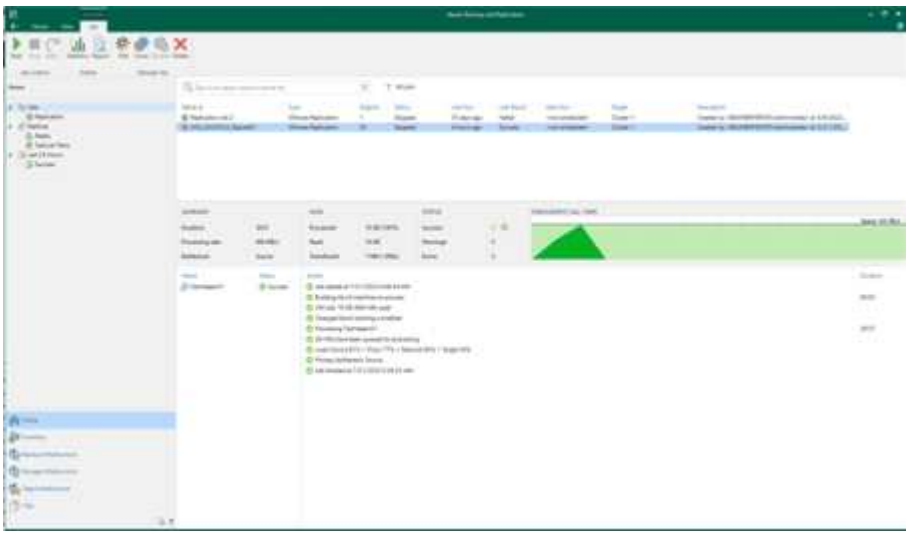
10. 選擇複製計畫來定期執行複製作業。



11. 在精靈的*摘要*步驟中，查看複製作業的詳細資訊。若要在精靈關閉後立即啟動作業，請選取*按一下「完成」時執行作業*複選框，否則請不要選取該複選框。然後按一下「完成」關閉精靈。



複製作業啟動後，具有指定後綴的虛擬機器將填入目標 AVS SDDC 叢集/主機上。



有關 Veeam 複製的更多信息，請參閱"複製的工作原理"

▼ 步驟 **2**：建立故障轉移計劃

初始複製或播種完成後，建立故障轉移計劃。故障轉移計畫有助於自動對從屬虛擬機器逐一或按群組執行故障轉移。故障轉移計劃是虛擬機器處理順序（包括啟動延遲）的藍圖。故障轉移計劃還有助於確保關鍵依賴的虛擬機器已經在運作。

若要建立計劃，請導覽至名為「副本」的新子部分並選擇「故障轉移計劃」。選擇適當的虛擬機器。 Veeam Backup & Replication 將尋找最接近此時間點的還原點並使用它們啟動 VM 副本。

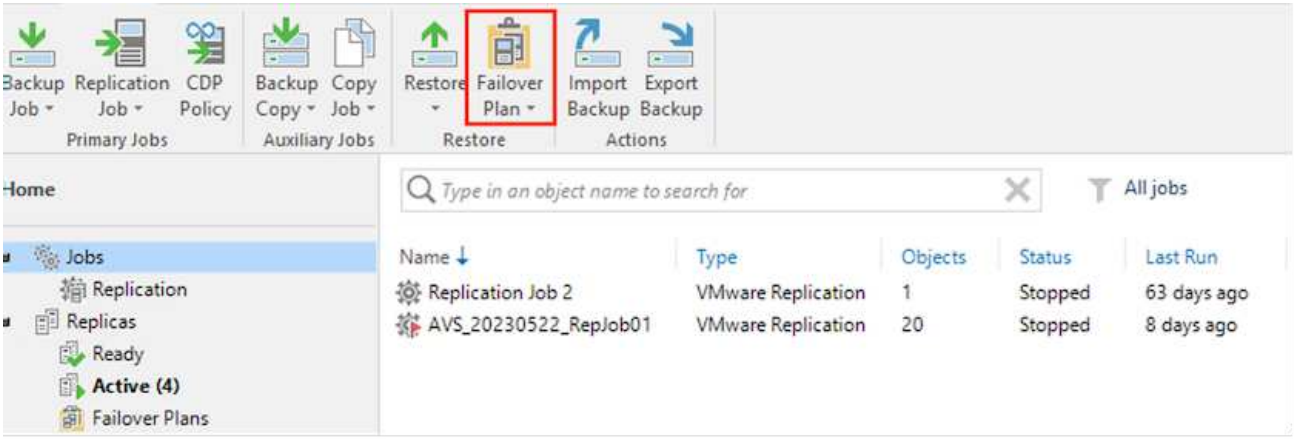
僅當初始複製完成且 VM 副本處於就緒狀態後，才能新增故障轉移計劃。

執行故障轉移計畫時可同時啟動的虛擬機器數量上限為 10

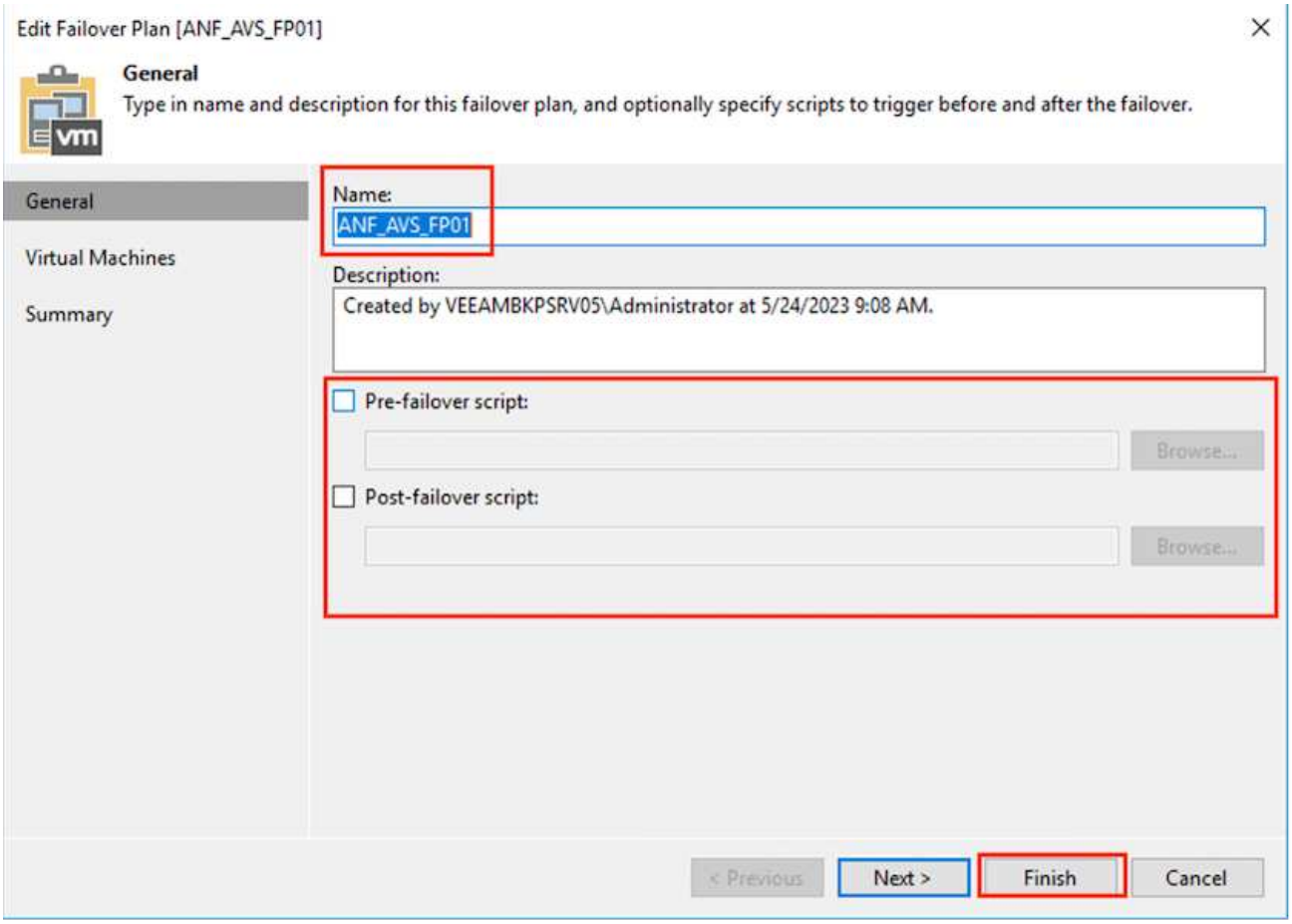
在故障轉移過程中，來源虛擬機器不會關閉

若要建立*故障轉移計劃*，請執行下列操作：

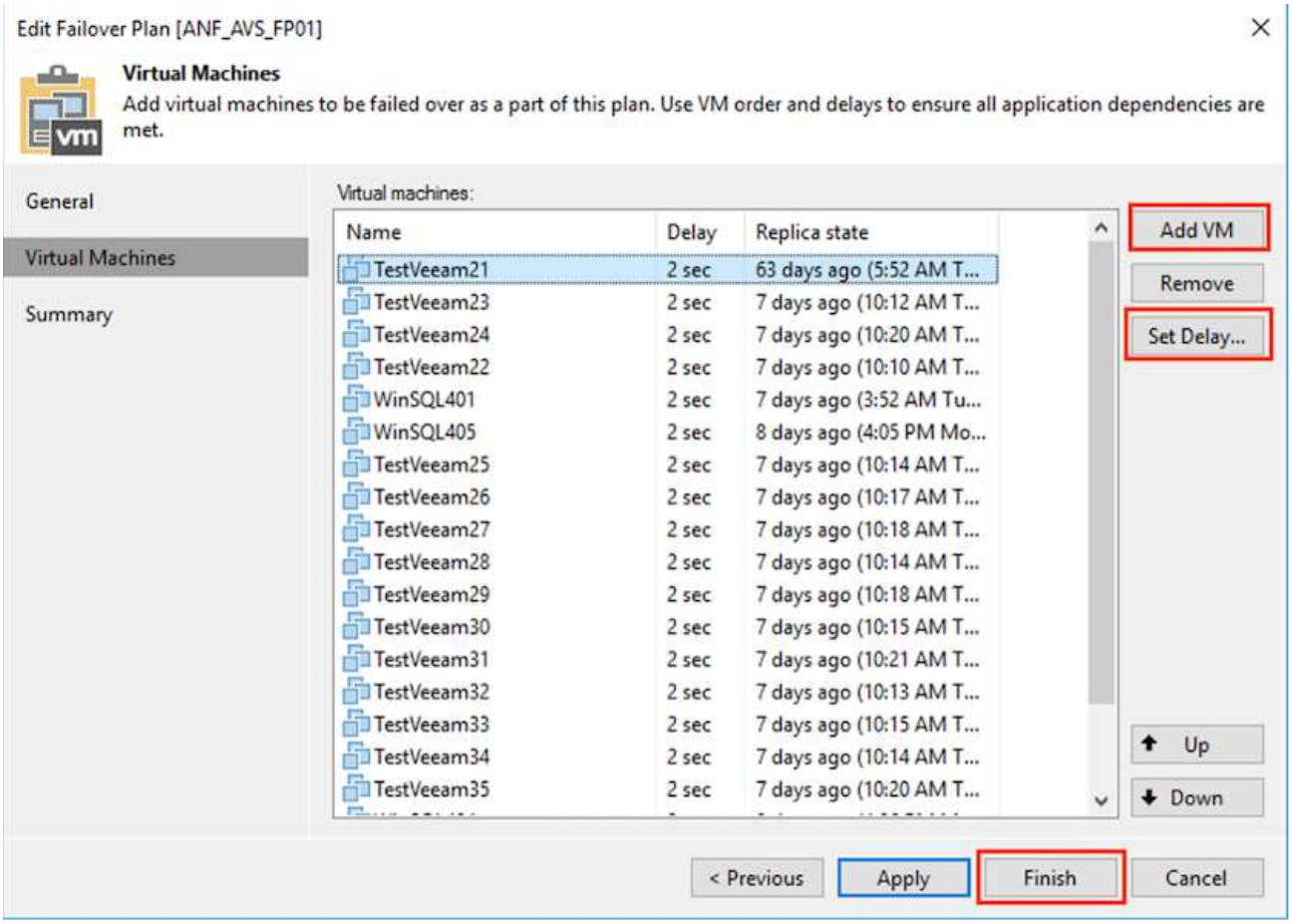
1. 在主頁視圖上。右鍵點選「副本」節點並選擇「故障轉移計畫」>「故障轉移計畫」>「VMware vSphere」。



2. 接下來為計劃提供名稱和描述。可根據需要新增故障轉移前和故障轉移後腳本。例如，在啟動複製的虛擬機器之前執行腳本來關閉虛擬機器。



3. 將虛擬機器新增至計畫中，並修改虛擬機器啟動順序和啟動延遲以滿足應用程式依賴關係。



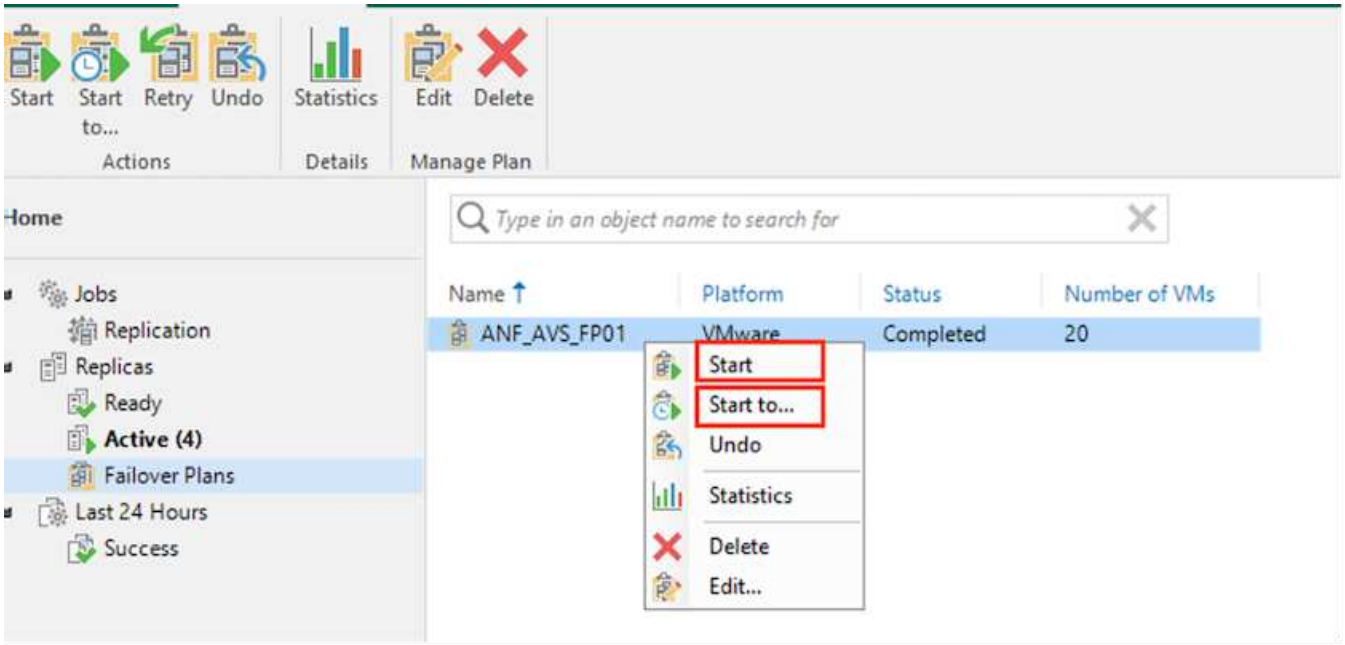
有關建立複製作業的其他信息，請參閱"建立複製作業"。

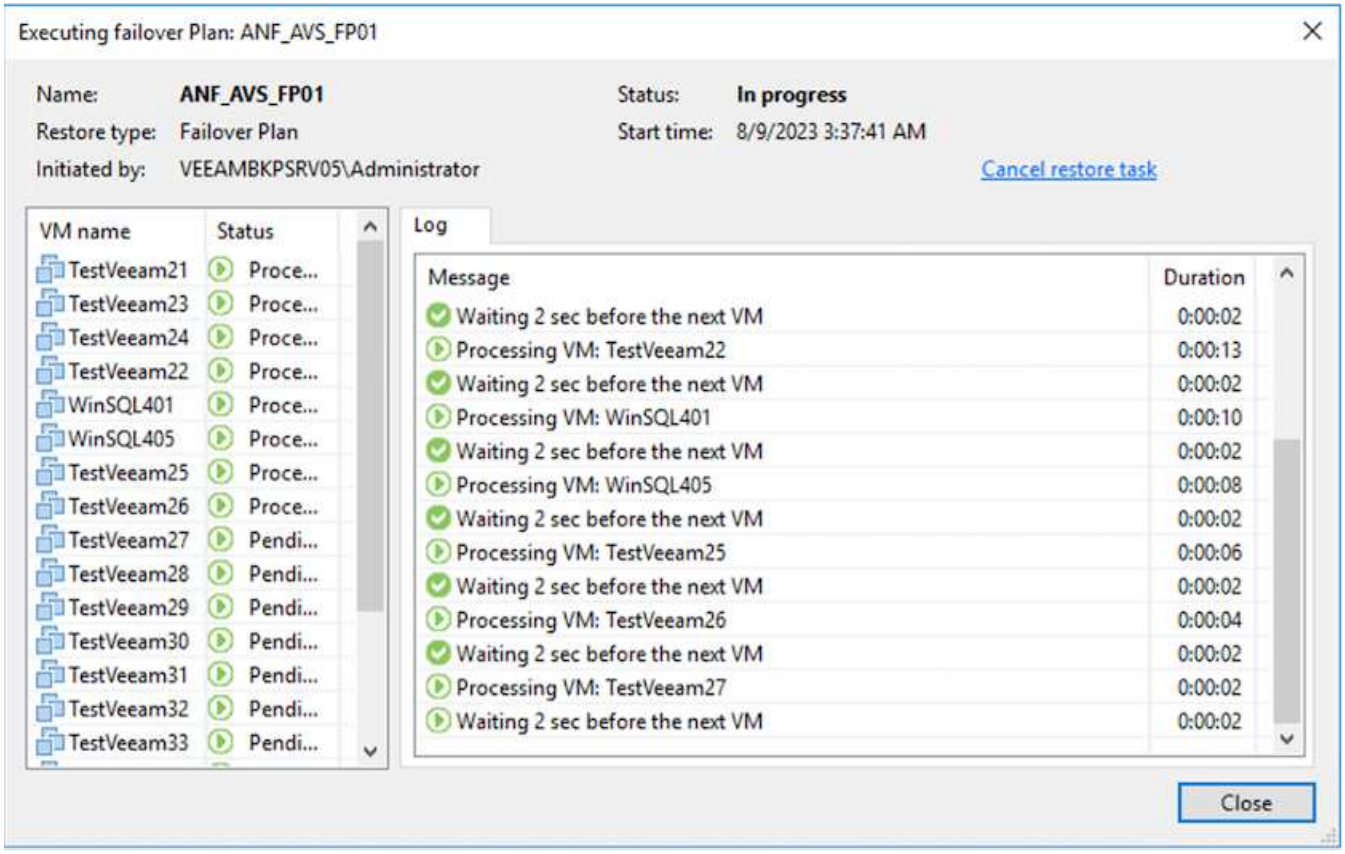
▼ 步驟 **3**：運行故障轉移計劃

在故障轉移期間，生產站點中的來源虛擬機器將切換到災難復原站點上的副本。作為故障轉移過程的一部分，Veeam Backup & Replication 將 VM 副本還原到所需的復原點，並將所有 I/O 活動從來源 VM 移至其副本。副本不僅可用於災難發生時，還可用於模擬災難復原演習。在故障轉移模擬期間，來源虛擬機器仍保持運作。一旦完成所有必要的測試，您就可以撤銷故障轉移並恢復正常操作。

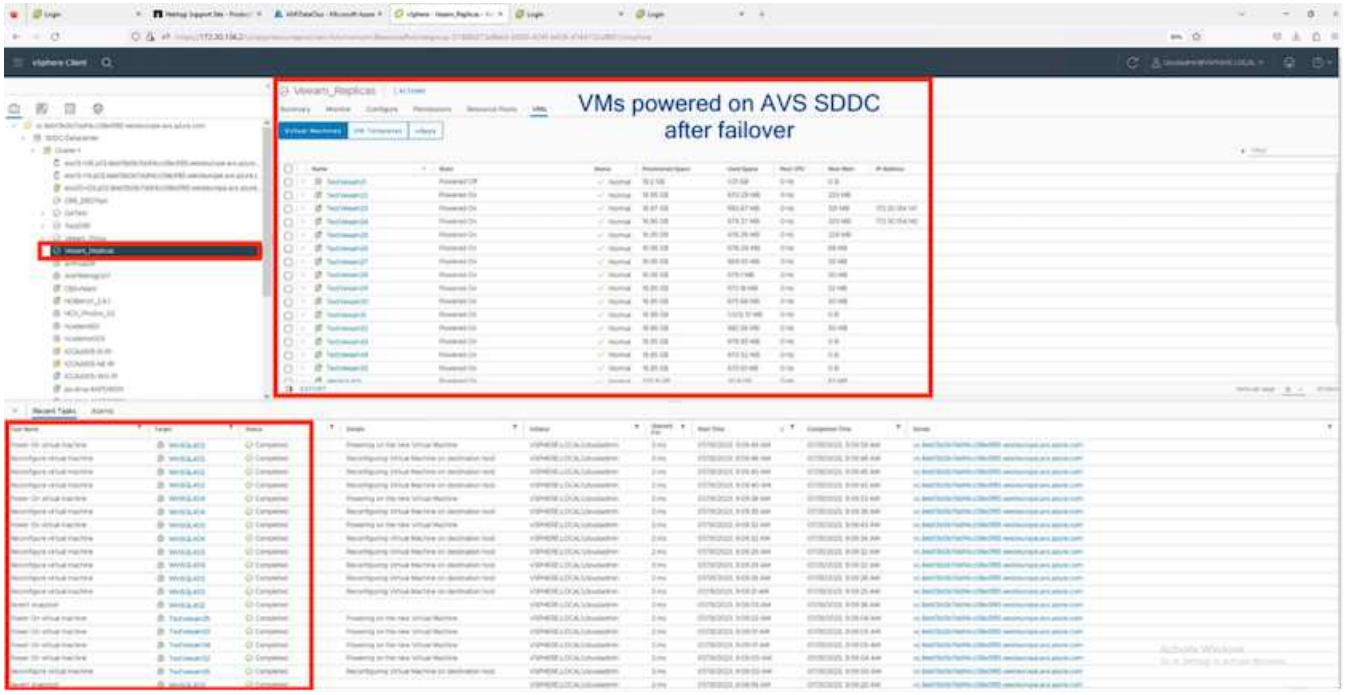
確保網路分段到位，以避免故障轉移期間發生 IP 衝突。

要啟動故障轉移計劃，只需按一下「故障轉移計劃」選項卡，然後右鍵單擊您的故障轉移計劃。選擇“開始”。這將使用 VM 副本的最新還原點進行故障轉移。若要故障轉移到 VM 副本的特定還原點，請選擇*開始*。

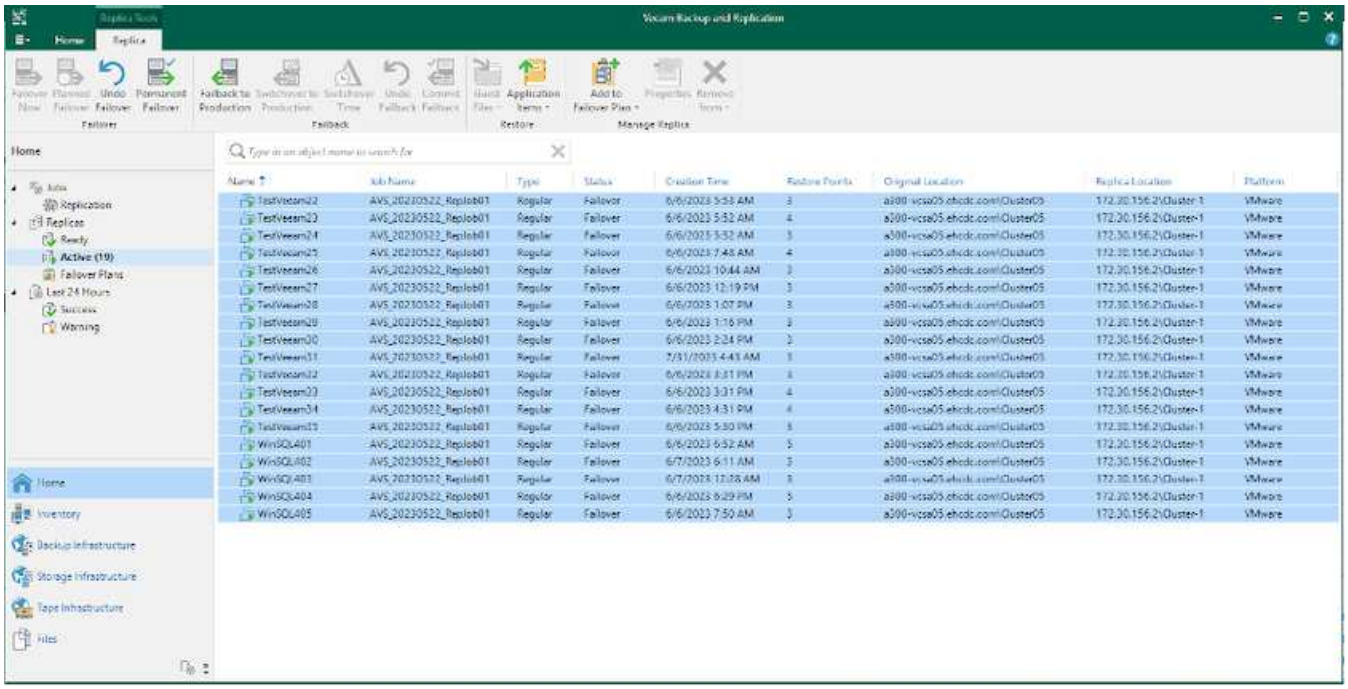




VM 副本的狀態從“就緒”變更為“故障轉移”，並且 VM 將在目標 Azure VMware 解決方案 (AVS) SDDC 叢集/主機上啟動。



故障轉移完成後，虛擬機器的狀態將變為「故障轉移」。



Veeam Backup & Replication 停止來源 VM 的所有複製活動，直到其副本返回就緒狀態。

有關故障轉移計劃的詳細信息，請參閱"故障轉移計劃"。

▼ 步驟 **4**：故障恢復到生產站點

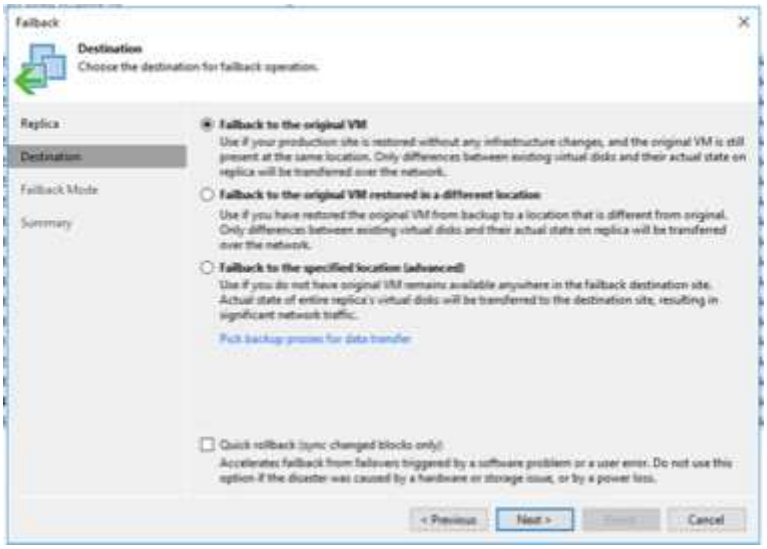
當故障轉移計劃運行時，它被視為一個中間步驟，需要根據需求最終確定。選項包括以下內容：

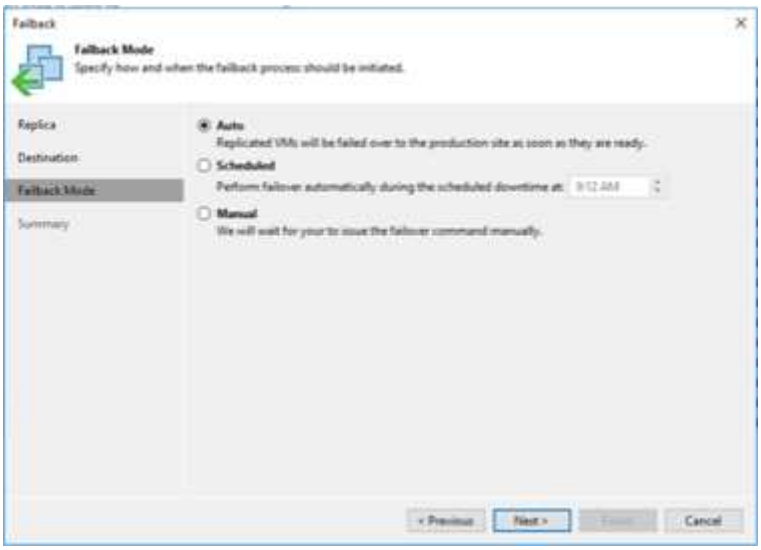
- 故障恢復到生產 - 切換回原始 VM，並將 VM 副本運行時發生的所有變更傳輸到原始 VM。

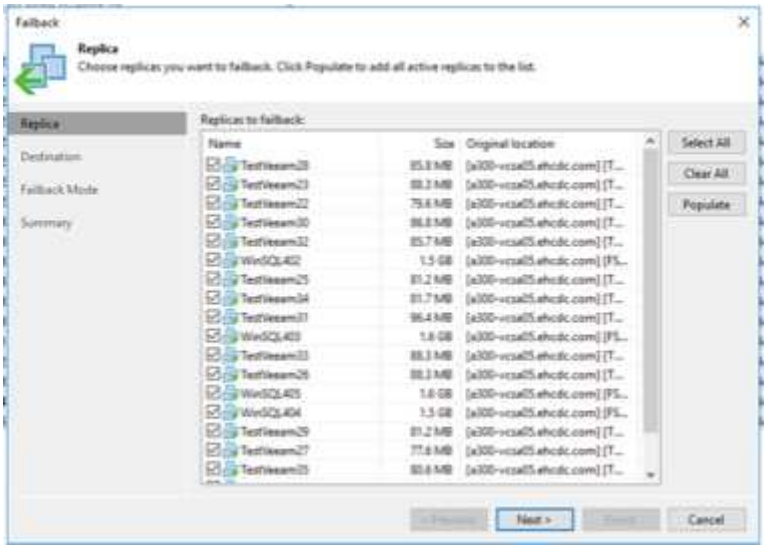
當您執行故障回應時，變更僅傳輸但不會被發布。如果原始虛擬機器未如預期運作，請選擇*提交故障復原*（一旦確認原始虛擬機器按預期工作）或撤銷故障復原以傳回虛擬機器副本。

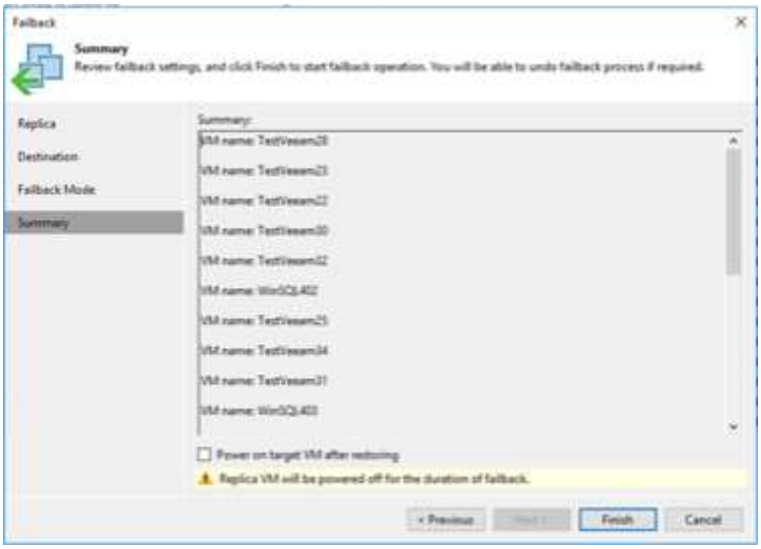
- 撤銷故障轉移 - 切換回原始虛擬機器並放棄運行時對虛擬機器副本所做的所有變更。
- 永久故障轉移 - 從原始 VM 永久切換到 VM 副本，並使用此副本作為原始 VM。

在這個演示中，選擇了故障恢復到生產。在精靈的目標步驟中選擇了故障回復到原始虛擬機，並且啟用了「恢復後啟動虛擬機」複選框。



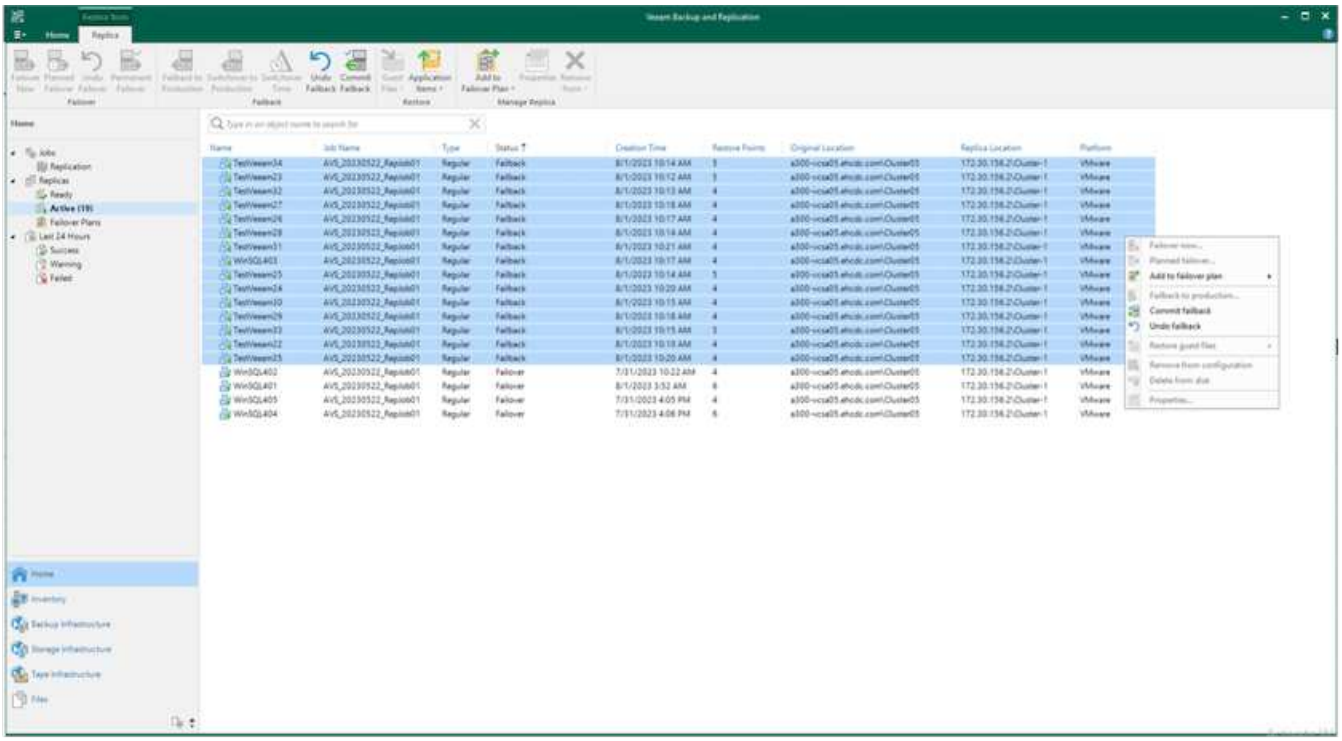




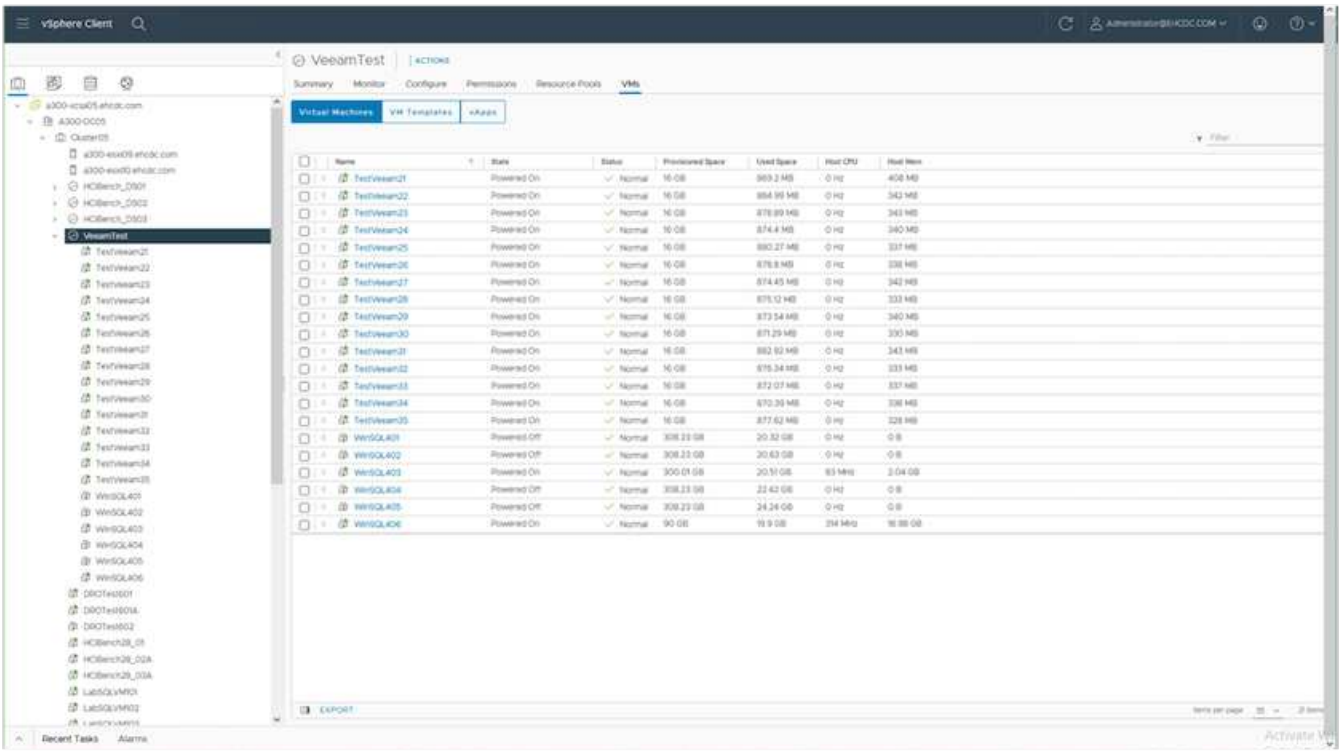


故障回復提交是完成故障回復操作的方法之一。當故障回復被提交時，它會確認發送到故障回復的虛擬機器（生產虛擬機器）的變更是否如預期般運作。提交操作後，Veeam Backup & Replication 將恢復生產虛擬機器的複製活動。

有關故障恢復過程的詳細信息，請參閱 Veeam 文檔"複製的故障轉移和故障恢復"。



故障復原生產成功後，所有虛擬機器都將恢復到原始生產站點。



結論

Azure NetApp Files資料儲存功能使 Veeam 或任何經過驗證的第三方工具能夠利用 Pilot light 叢集來提供低成本的 DR 解決方案，而不是僅僅為了容納 VM 副本而建立大型叢集。這提供了一種有效的方法來處理量身定制的災難復原計劃，並重複使用內部現有的備份產品進行災難恢復，透過退出內部災難復原資料中心實現基於雲端的災難復原。發生災難時，可以透過點擊按鈕進行故障轉移，或在發生災難時自動進行故障轉移。

要了解有關此過程的更多信息，請隨意觀看詳細的演示視頻。

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

在 **Azure/AVS** 上遷移工作負載

TR-4940：使用 **VMware HCX** 將工作負載移轉到**Azure NetApp Files**資料儲存 **-** 快速入門指南

Azure VMware 解決方案和Azure NetApp Files儲存最常見的用例之一是遷移 VMware 工作負載。 VMware HCX 是首選方案，它提供了各種遷移機制，可將本機虛擬機器 (VM) 及其資料移至Azure NetApp Files資料儲存。

概述：使用 **VMware HCX**、 **Azure NetApp Files**資料儲存和 **Azure VMware** 解決方案遷移虛擬機

VMware HCX 主要是一個遷移平台，旨在簡化應用程式遷移、工作負載重新平衡甚至跨雲端的業務連續性。它是 Azure VMware 解決方案私有雲的一部分，提供了多種遷移工作負載的方法，可用於災難復原 (DR) 作業。

本文檔提供了配置Azure NetApp Files資料儲存以及下載、部署和配置 VMware HCX 的逐步指導，包括本地和 Azure VMware 解決方案端的所有主要元件（包括互連、網路擴展和 WAN 最佳化），以啟用各種 VM 遷移機制。

> VMware HCX 適用於任何資料儲存類型，因為遷移是在 VM 層級進行的。因此，本文檔適用於現有NetApp客戶和計畫使用 Azure VMware 解決方案部署Azure NetApp Files以實現經濟高效的 VMware 雲端部署的非NetApp客戶。

▼ 摘要步驟

此清單提供了在 Azure 雲端安裝和設定 HCX Cloud Manager 以及在本機安裝 HCX Connector 所需的進階步驟：

1. 透過 Azure 入口網站安裝 HCX。
2. 在本機 VMware vCenter Server 中下載並部署 HCX Connector Open Virtualization Appliance (OVA) 安裝程式。
3. 使用許可證金鑰啟動 HCX。
4. 將本機 VMware HCX 連接器與 Azure VMware 解決方案 HCX 雲端管理器配對。
5. 設定網路設定檔、計算設定檔和服務網格。
6. （可選）執行網路擴展以避免在遷移期間重新分配 IP。
7. 驗證設備狀態並確保可以遷移。
8. 遷移虛擬機器工作負載。

▼ 先決條件

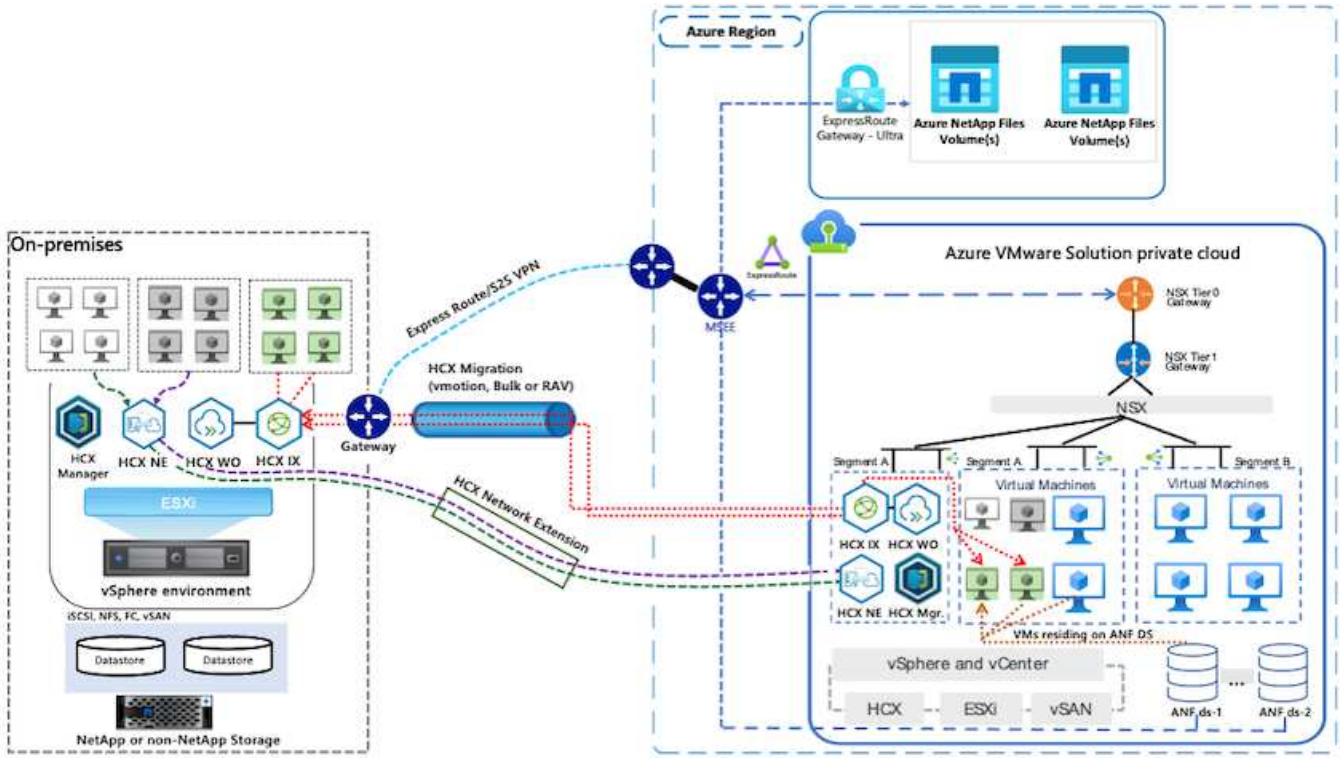
在開始之前，請確保滿足以下先決條件。有關詳細信息，請參閱 "關聯"。滿足先決條件（包括連接性）後，透過從 Azure VMware 解決方案入口網站產生許可證金鑰來設定和啟動 HCX。下載 OVA 安裝程式後，請依照如下所述進行安裝程序。

> HCX 高級版是預設選項，VMware HCX 企業版也可透過支援票獲得，且無需額外付費即可獲得支援。

- 使用現有的 Azure VMware 解決方案軟體定義資料中心 (SDDC) 或使用此解決方案建立私有雲"NetApp連結"或者這個 "微軟連結"。
- 從支援 VMware vSphere 的內部部署資料中心遷移虛擬機器和相關資料需要從資料中心到 SDDC 環境的網路連線。在遷移工作負載之前， "設定站台到站台 VPN 或 Express 路由 Global Access 連接"在本地環境和對應的私有雲之間。
- 從本機 VMware vCenter Server 環境到 Azure VMware 解決方案私有雲的網路路徑必須支援使用 vMotion 遷移 VM。
- 確保所需的 "防火牆規則和連接埠"允許在本機 vCenter Server 和 SDDC vCenter 之間進行 vMotion 流量。在私有雲上，預設配置vMotion網路上的路由。
- Azure NetApp FilesNFS 磁碟區應會作為資料儲存體裝載在 Azure VMware 解決方案中。請按照本文中詳細說明的步驟操作 "關聯"將Azure NetApp Files資料儲存附加到 Azure VMware 解決方案主機。

▼ 進階架構

出於測試目的，用於此驗證的本機實驗室環境會透過站點對站點 VPN 連接，這允許本機連接到 Azure VMware 解決方案。



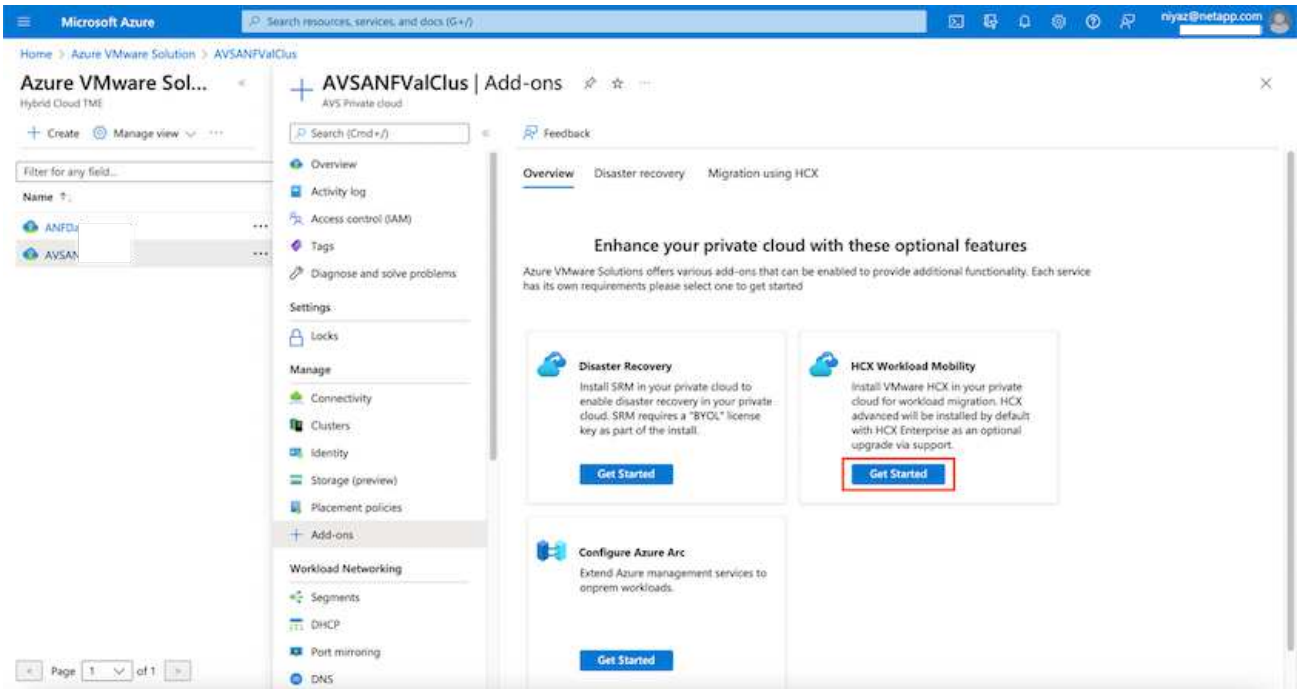
解決方案部署

請按照一系列步驟完成此解決方案的部署：

▼ 步驟 **1**：使用附加元件選項透過 **Azure** 入口網站安裝 **HCX**

若要執行安裝，請完成以下步驟：

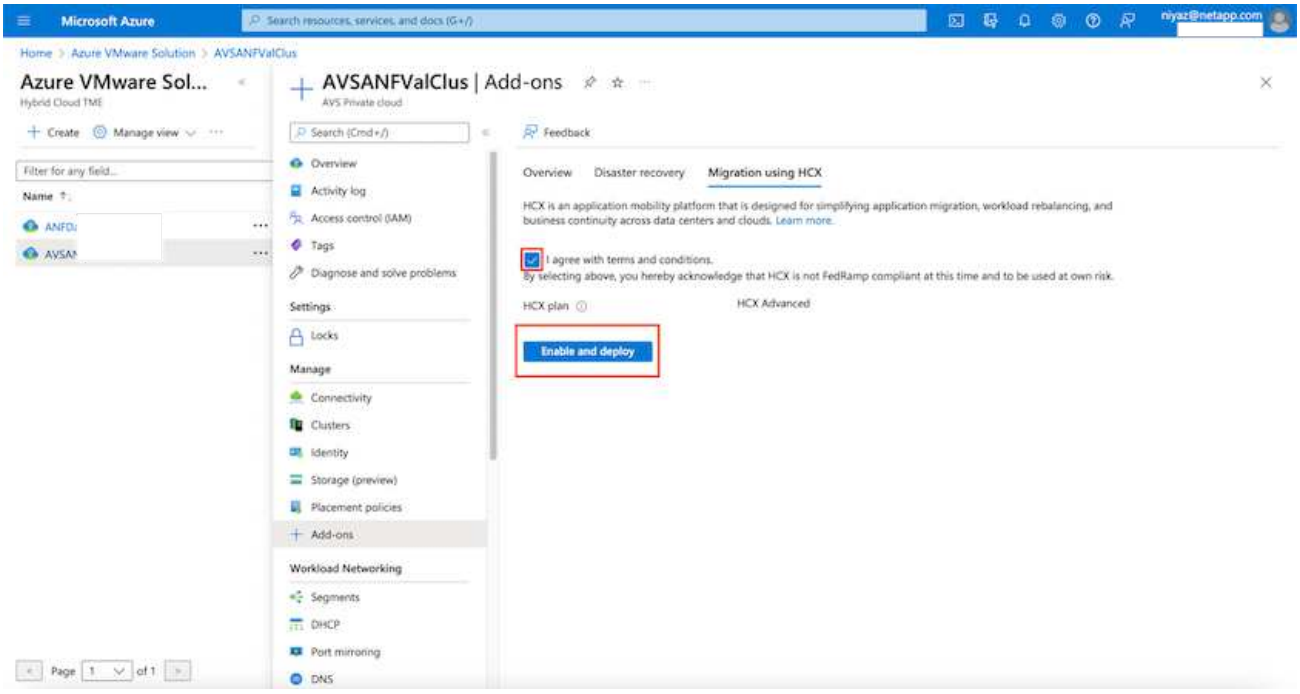
1. 登入 Azure 入口網站並存取 Azure VMware 解決方案私有雲。
2. 選擇適當的私有雲並存取附加元件。這可以透過導航到*管理>附加元件*來完成。
3. 在 HCX Workload Mobility 部分，按一下 開始。



4. 選擇*我同意條款和條件*選項，然後點擊*啟用和部署*。

預設部署是 HCX Advanced。開啟支援請求以啟用企業版。

部署大約需要 25 到 30 分鐘。



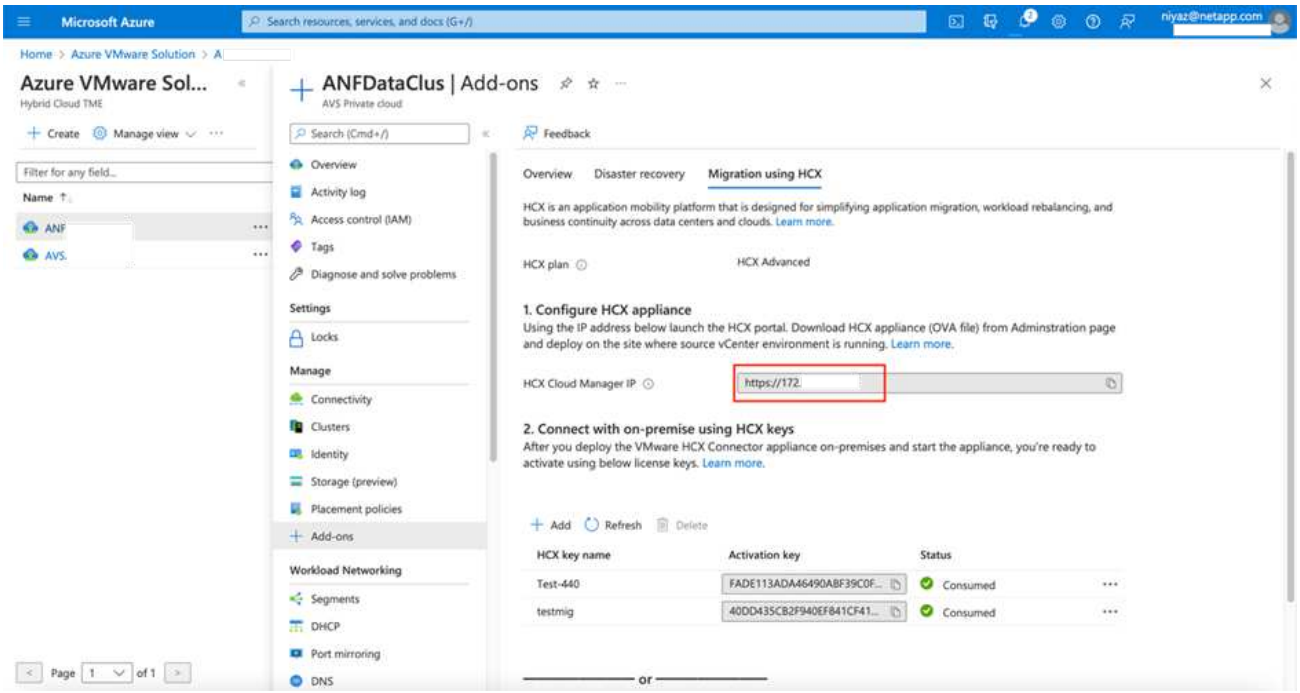
▼ 步驟 **2**：在本機 **vCenter Server** 中部署安裝程式 **OVA**

為了讓本機連接器連接到 Azure VMware 解決方案中的 HCX 管理器，請確保在本機環境中開啟了對應的防火牆連接埠。

若要在本機 vCenter Server 中下載並安裝 HCX Connector，請完成下列步驟：

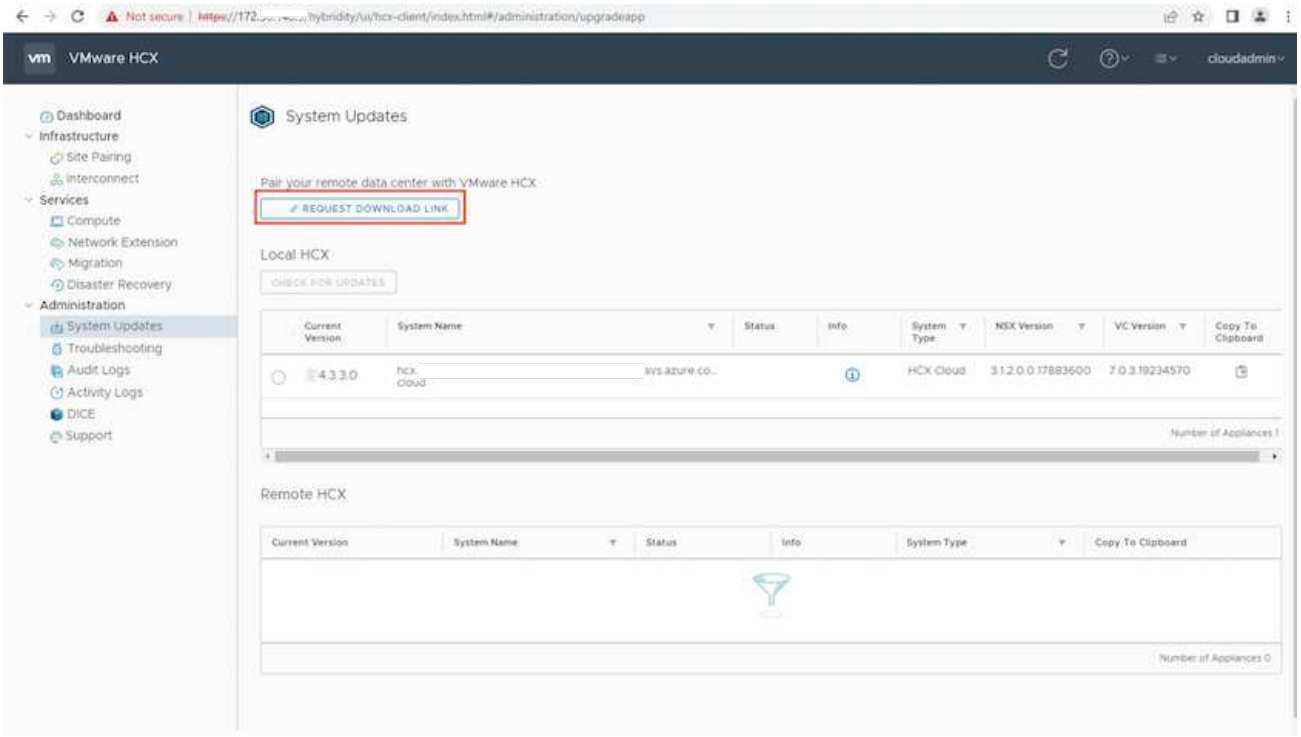
1. 從 Azure 入口網站前往 Azure VMware 解決方案，選擇私有雲，然後使用 HCX 選擇 管理 > 附加元件 > 遷移，並複製 HCX 雲端管理器入口網站以下載 OVA 檔案。

   使用預設 CloudAdmin 使用者憑證存取 HCX 入口網站。

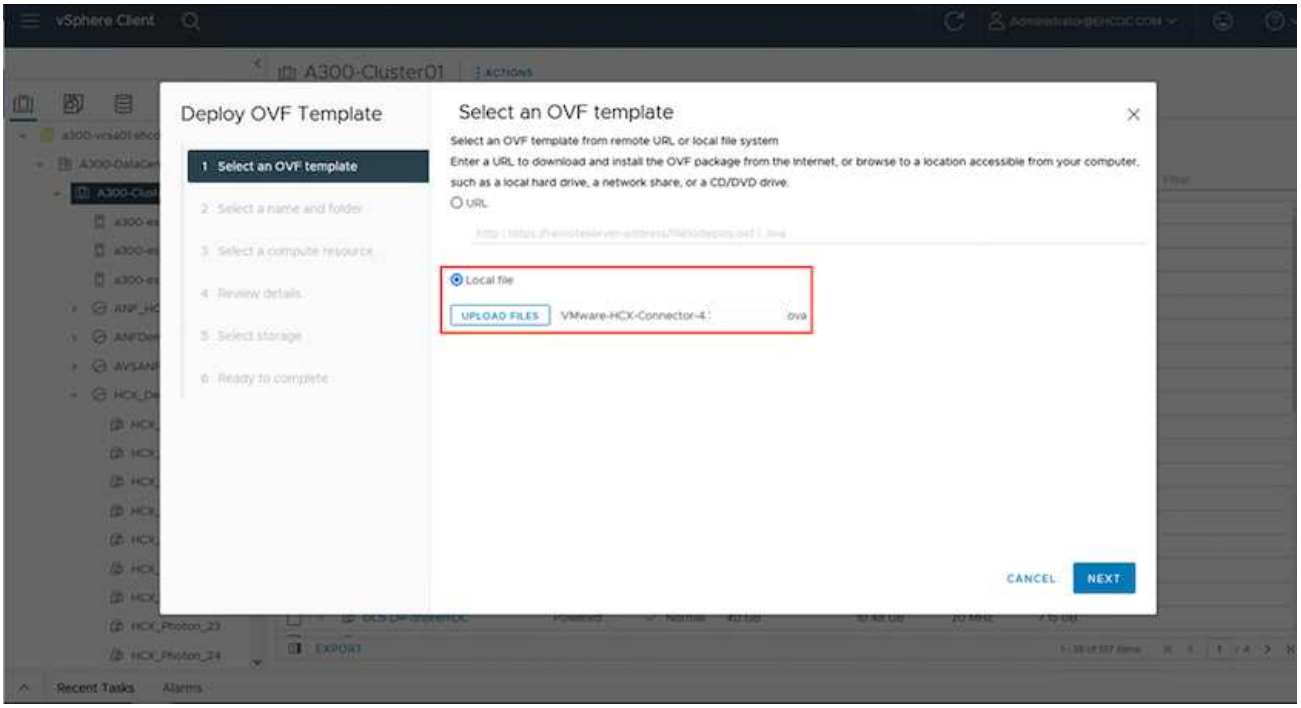


2. 使用 jumphost 透過 cloudadmin@vsphere.local 存取 HCX 入口網站後，導覽至 管理 > 系統更新，然後按 要求下載連結。

   下載或複製 OVA 連結並將其貼上到瀏覽器中，開始下載 VMware HCX Connector OVA 檔案以部署在本機 vCenter Server 上。



3. 下載 OVA 後，使用 部署 **OVF** 範本 選項將其部署到本機 VMware vSphere 環境。



4. 輸入 OVA 部署所需的所有信息，按一下“下一步”，然後按一下“完成”以部署 VMware HCX 連接器 OVA。

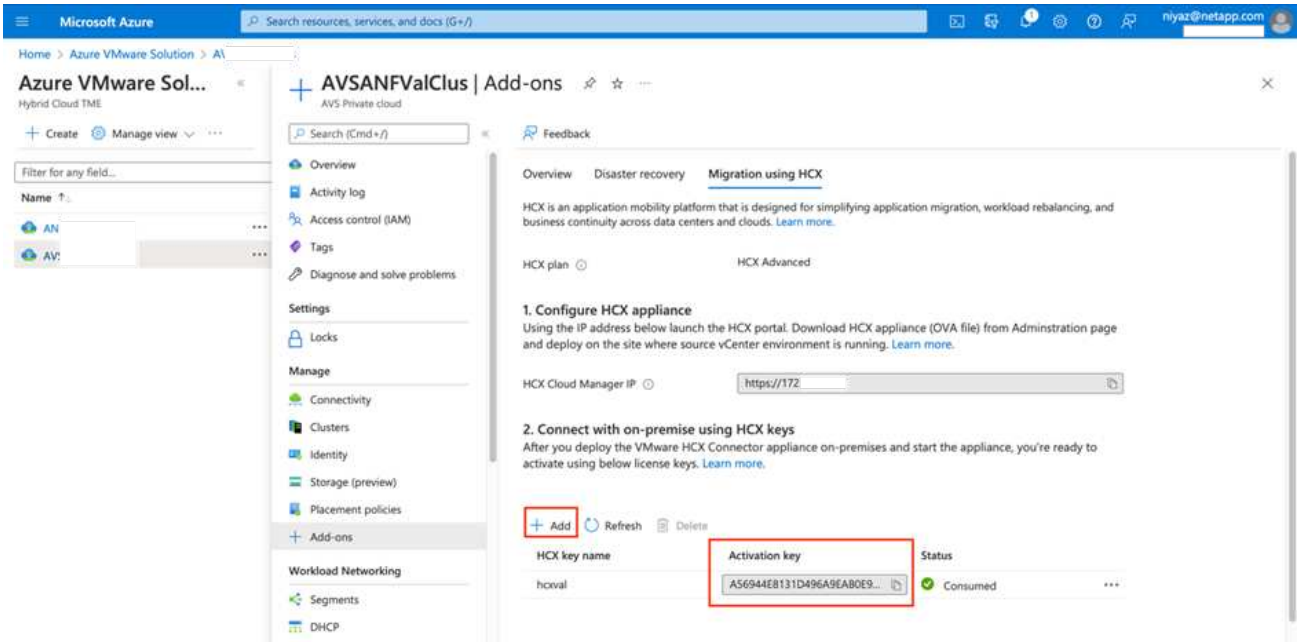
手動啟動虛擬設備。

有關逐步說明，請參閱 "VMware HCX 使用者指南"。

▼ 步驟 **3**：使用許可證金鑰啟動 **HCX Connector**

在本機部署 VMware HCX Connector OVA 並啟動裝置後，請完成以下步驟以啟動 HCX Connector。從 Azure VMware 解決方案入口網站產生授權金鑰，並在 VMware HCX 管理器中啟動它。

1. 從 Azure 入口網站前往 Azure VMware 解決方案，選擇私有雲，然後選擇「管理」>「附加元件」>「使用 HCX 遷移」。
2. 在*使用 HCX 金鑰連接本機*下，按一下*新增*並複製啟動金鑰。



部署的每個本機 HCX 連接器都需要單獨的金鑰。

3. 登入本機 VMware HCX 管理器 `"https://hcxmanagerIP:9443"`使用管理員憑證。

使用 OVA 部署期間定義的密碼。

4. 在許可中，輸入從步驟 3 複製的金鑰，然後按一下 啟動。

本地 HCX 連接器應該具有網路存取權限。

5. 在「資料中心位置」下，提供在本機安裝 VMware HCX 管理器的最近位置。按一下“繼續”。
6. 在“系統名稱”下，更新名稱並按一下“繼續”。
7. 點擊“是，繼續”。
8. 在「連接您的 vCenter」下，提供 vCenter Server 的完全限定網域名稱 (FQDN) 或 IP 位址以及對應的憑證，然後按一下「繼續」。

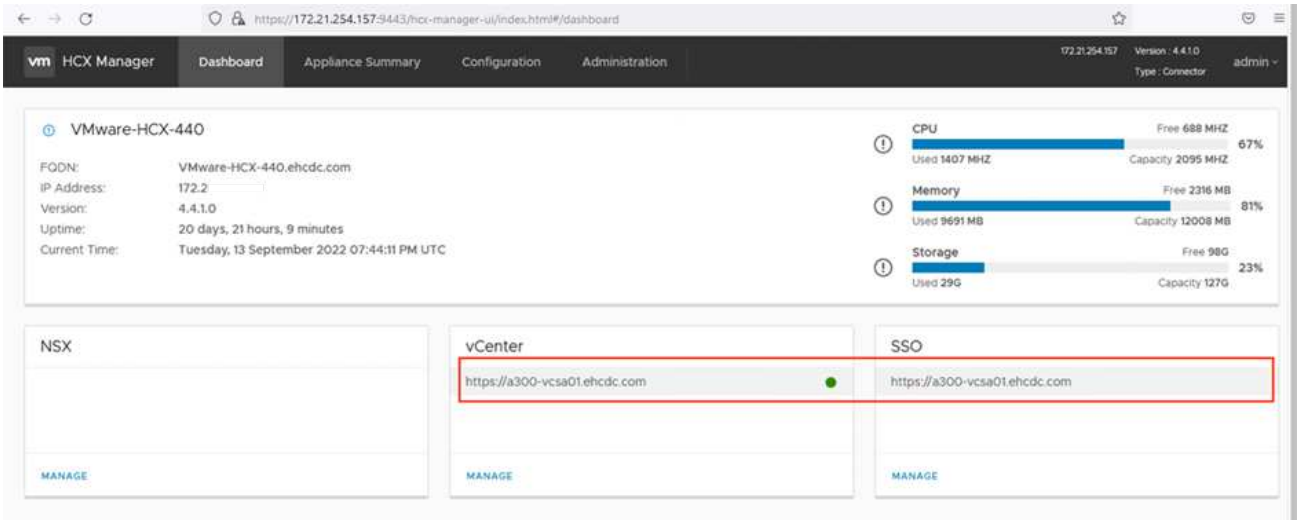
使用 FQDN 以避免日後出現連線問題。

9. 在「設定 SSO/PSC」下，提供平台服務控制器的 FQDN 或 IP 位址，然後按一下「繼續」。

輸入 VMware vCenter Server FQDN 或 IP 位址。

10. 驗證輸入的資訊是否正確，然後按一下「重新啟動」。
11. 服務重新啟動後，vCenter Server 在出現的頁面上顯示為綠色。 vCenter Server 和 SSO 都必須具有適當的設定參數，這些參數應與上一頁相同。

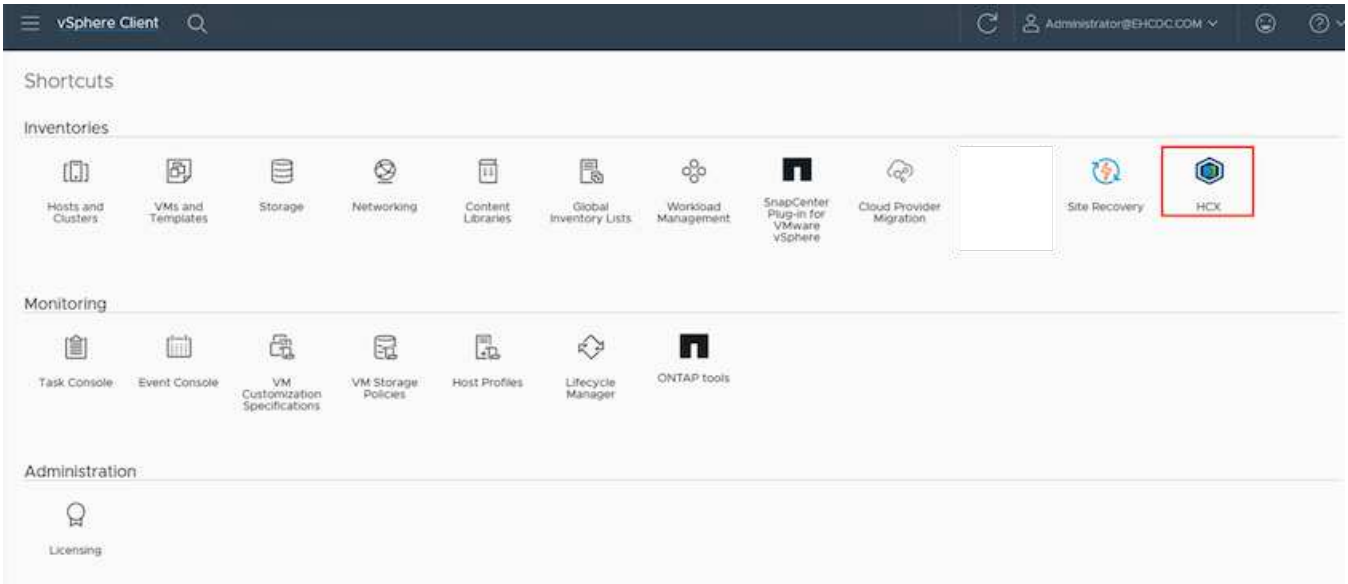
> 此過程大約需要 10 到 20 分鐘，以便將插件新增至 vCenter Server。



▼ 步驟 **4**：將本機 **VMware HCX** 連接器與 **Azure VMware** 解決方案 **HCX** 雲端管理器配對

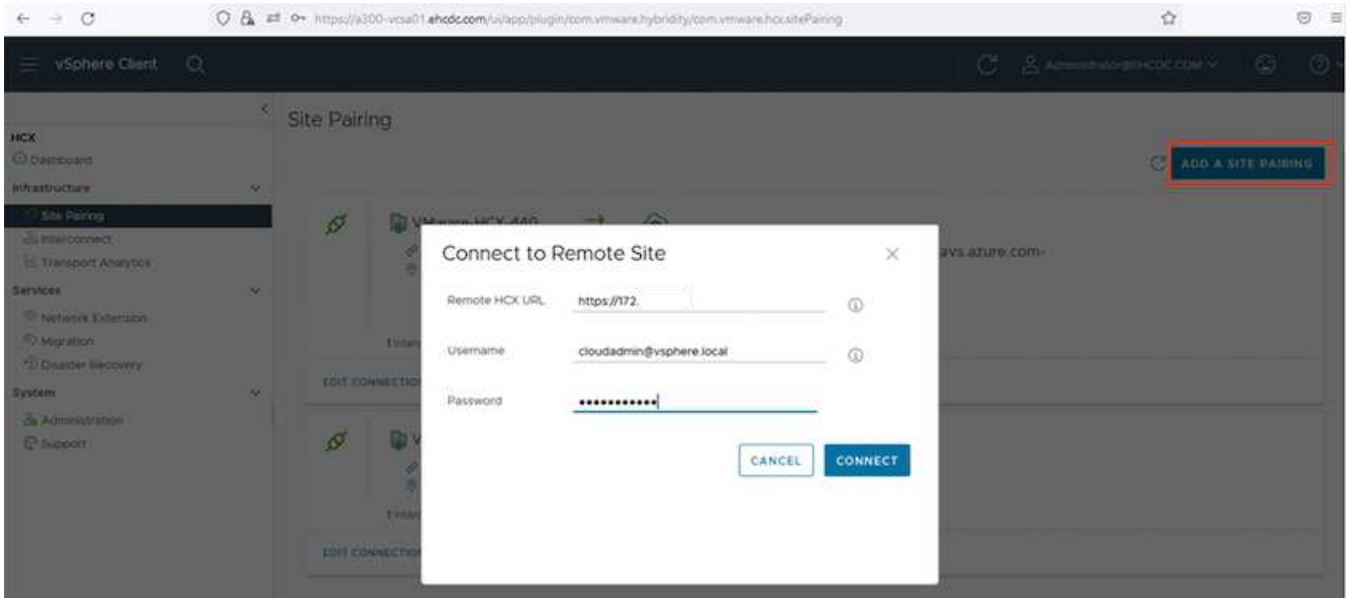
在本機和 Azure VMware 解決方案中安裝 HCX 連接器後，透過新增配對為 Azure VMware 解決方案私有雲配置本機 VMware HCX 連接器。若要設定網站配對，請完成以下步驟：

1. 若要在本機 vCenter 環境和 Azure VMware 解決方案 SDDC 之間建立網站對，請登入本機 vCenter Server 並造訪新的 HCX vSphere Web Client 外掛程式。



1. 在基礎架構下，按一下*新增網站配對*。

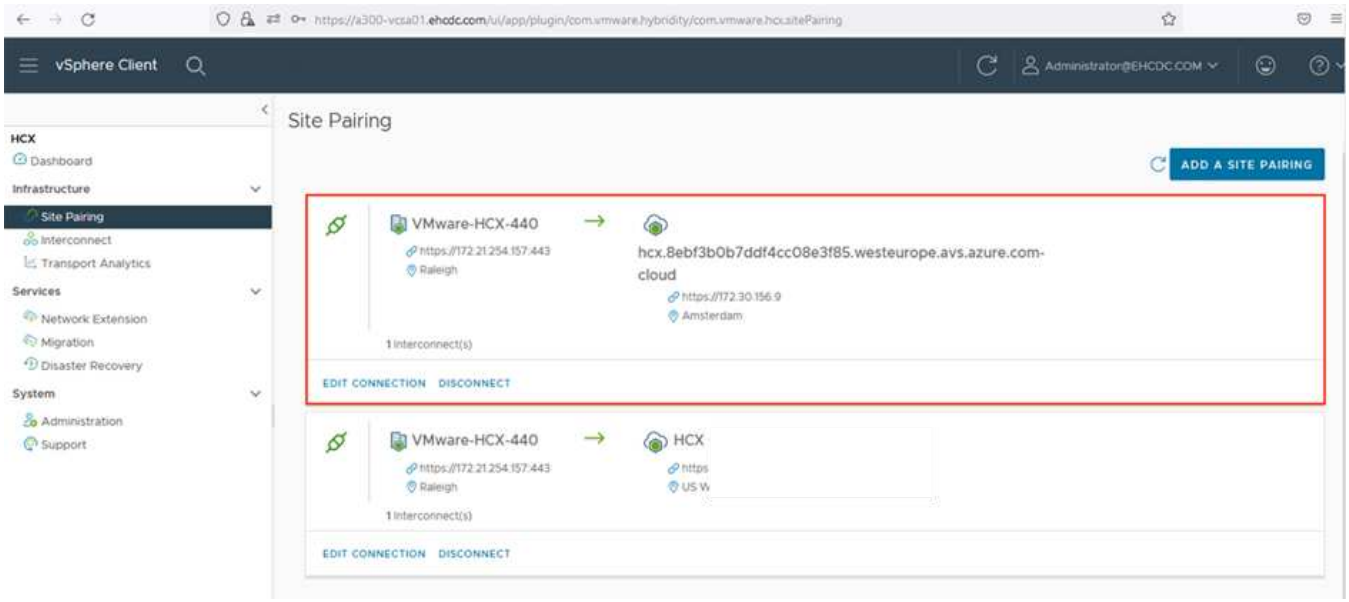
> 輸入 Azure VMware 解決方案 HCX 雲端管理器 URL 或 IP 位址以及用於存取私有雲的 CloudAdmin 角色的憑證。



1. 按一下“連接”。

VMware HCX Connector 必須能夠透過連接埠 443 路由至 HCX Cloud Manager IP。

1. 建立配對後，新配置的網站配對可在 HCX 儀表板上取得。

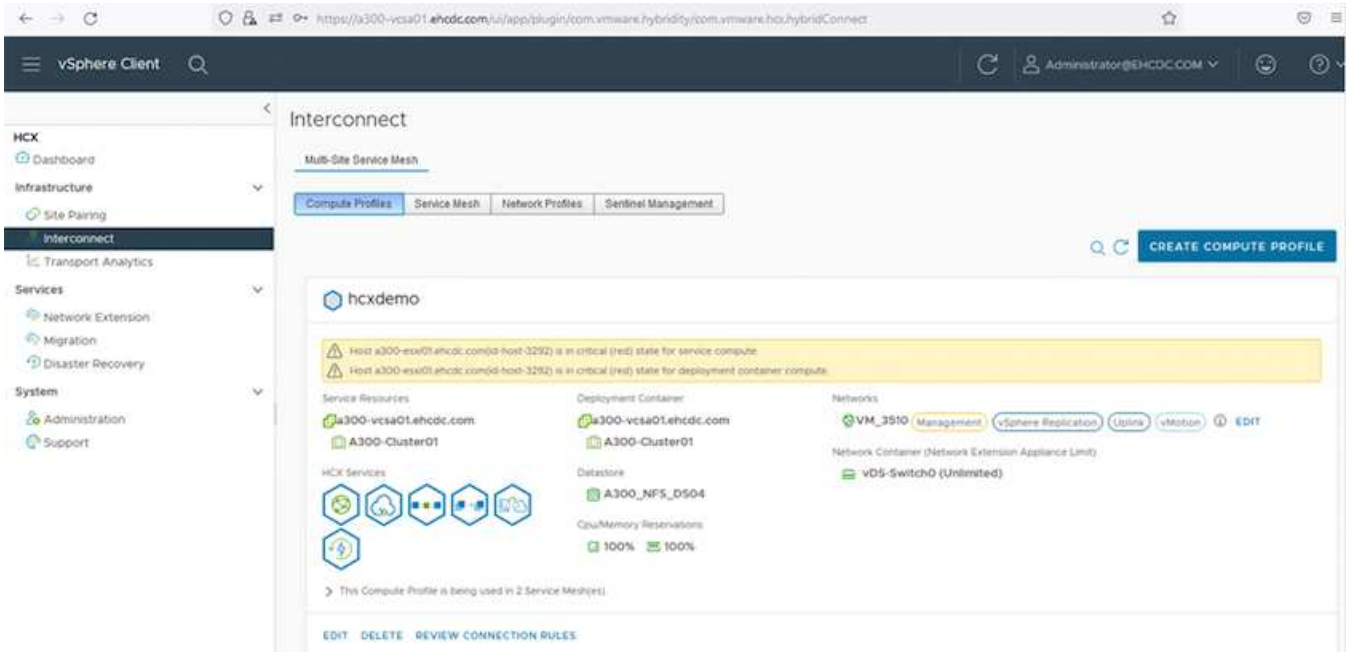


▼ 步驟 **5**：設定網路設定檔、計算設定檔和服務網格

VMware HCX Interconnect 服務設備透過網際網路和與目標網站的專用連線提供複製和基於 vMotion 的遷移功能。互連提供加密、流量工程和 VM 移動性。若要建立互連服務設備，請完成以下步驟：

1. 在基礎架構下，選擇*互連>多站點服務網格>計算設定檔>建立計算設定檔*。

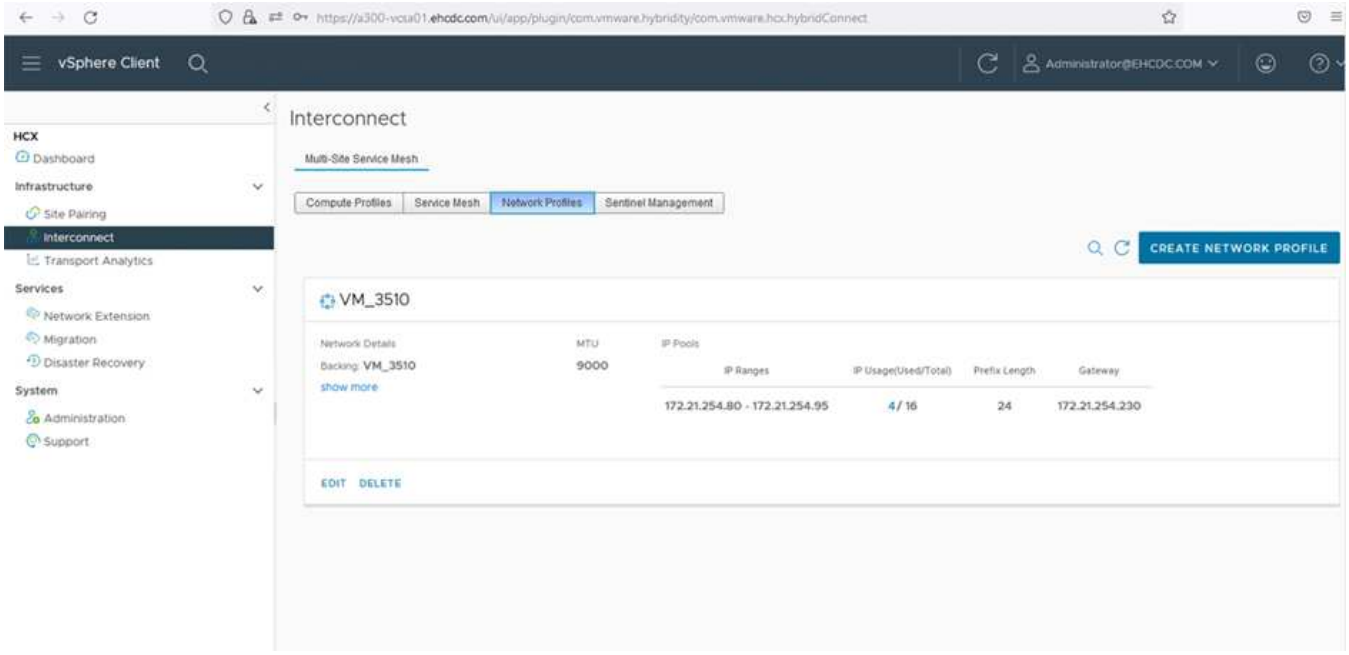
計算設定檔定義部署參數，包括部署的設備以及 VMware 資料中心的哪些部分可供 HCX 服務存取。



1. 建立計算設定檔後，透過選擇「多站點服務網格」>「網路設定檔」>「建立網路設定檔」來建立網路設定檔。

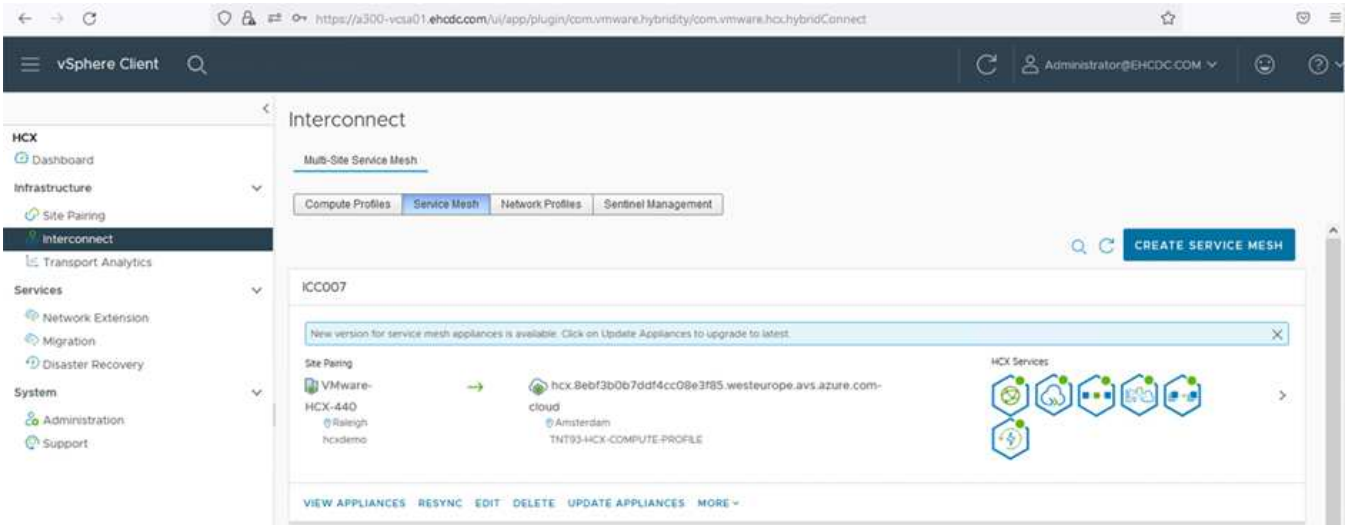
網路設定檔定義了 HCX 用於其虛擬設備的一系列 IP 位址和網路。

此步驟需要兩個或更多 IP 位址。這些 IP 位址由管理網路指派給互連設備。

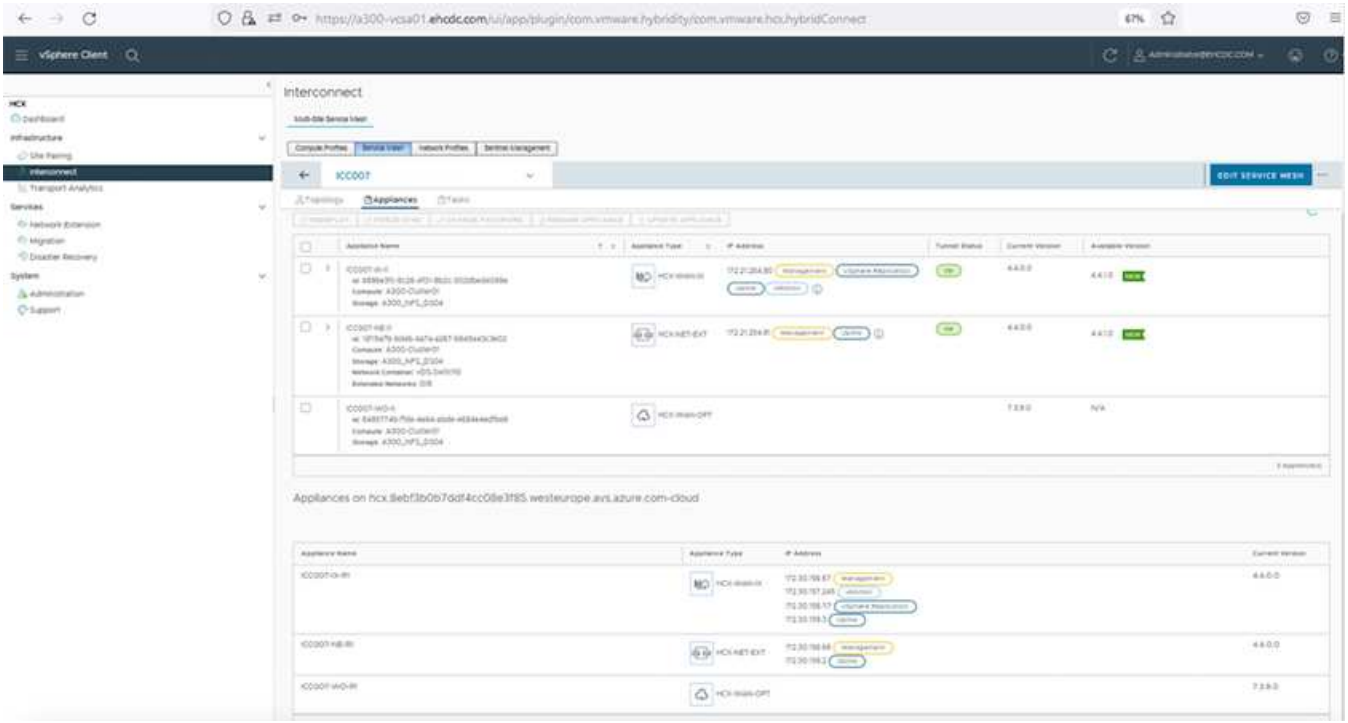


1. 此時，計算和網路設定檔已成功建立。
2. 透過選擇「**Interconnect**」選項中的「**Service Mesh**」標籤並選擇本機和 Azure SDDC 網站來建立服務網格。
3. 服務網格指定本地和遠端計算和網路設定檔對。

作為此流程的一部分，HCX 裝置在來源網站和目標網站上部署並自動配置，以建立安全的傳輸結構。



1. 這是配置的最後一步。完成部署大約需要 30 分鐘。配置服務網格後，環境已準備就緒，並已成功建立 IPsec 隧道來遷移工作負載虛擬機器。



▼ 步驟 **6**：遷移工作負載

可使用各種 VMware HCX 遷移技術在本機和 Azure SDDC 之間雙向遷移工作負載。可以使用多種遷移技術將虛擬機器移至 VMware HCX 啟動的實體或從中移出，例如 HCX 批量遷移、HCX vMotion、HCX 冷遷移、HCX 複製輔助 vMotion（HCX 企業版提供）和 HCX OS 輔助遷移（HCX 企業版提供）。

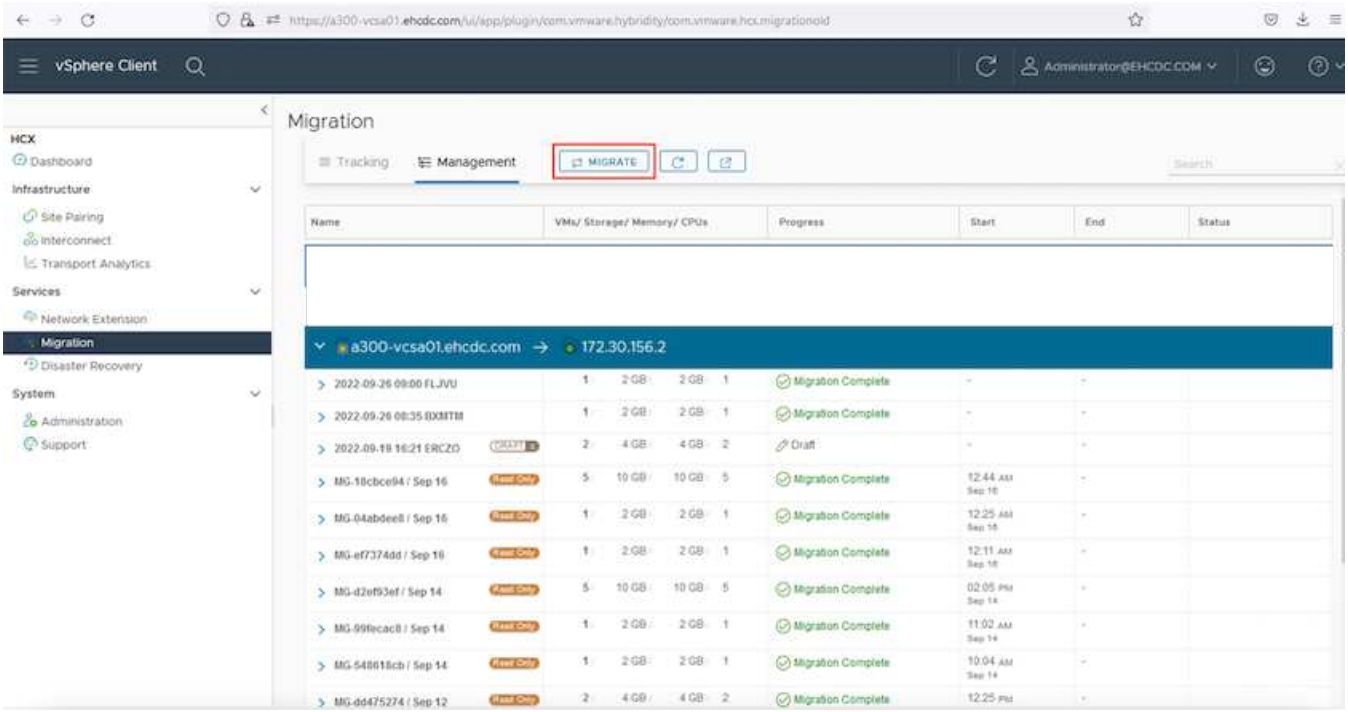
要了解有關各種 HCX 遷移機制的更多信息，請參閱 "VMware HCX 遷移類型"。

大量遷移

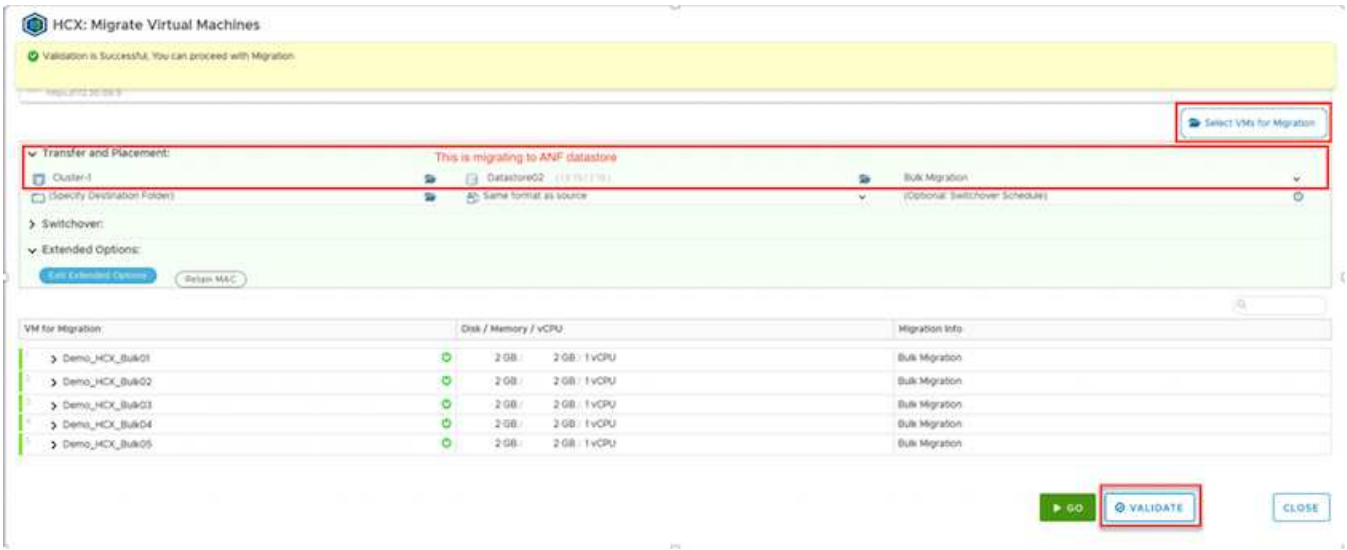
本節詳細介紹批量遷移機制。在批次遷移期間，HCX 的批次遷移功能使用 vSphere Replication 遷移磁碟文件，同時在目標 vSphere HCX 實例上重新建立虛擬機器。

若要啟動批次虛擬機器遷移，請完成以下步驟：

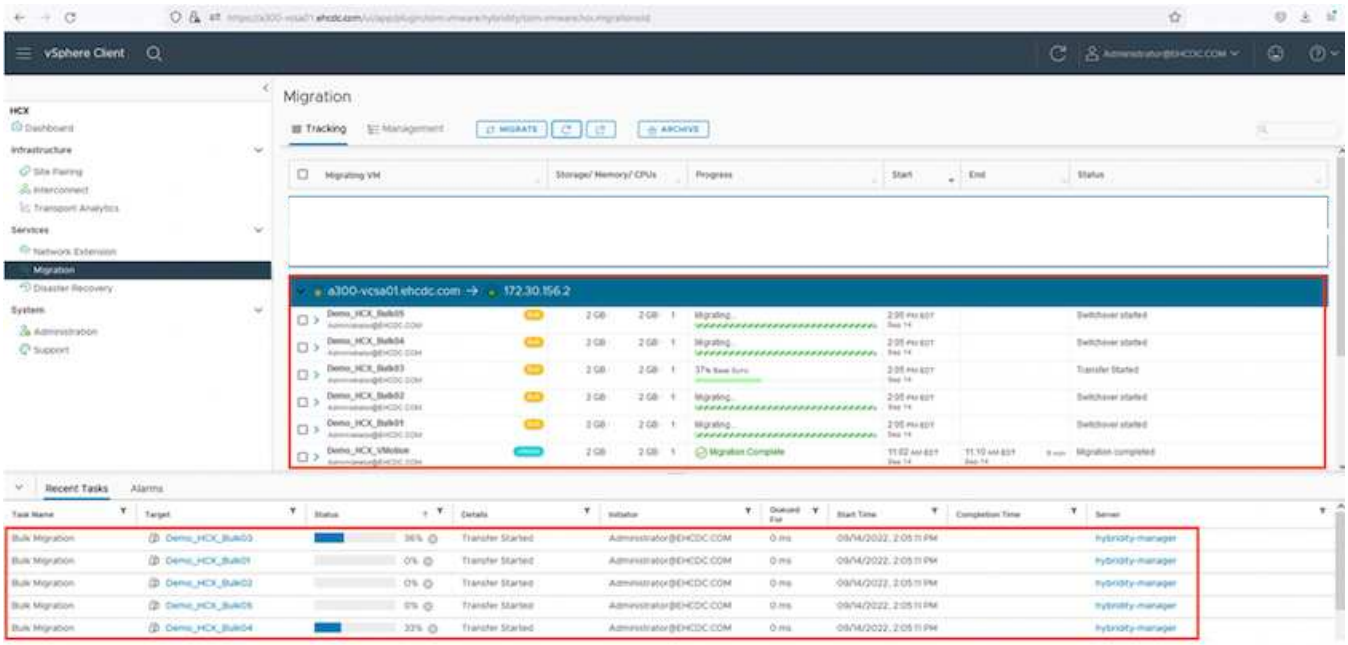
1. 存取「服務 > 遷移」下的「遷移」標籤。



1. 在*遠端站點連線*下，選擇遠端站點連線並選擇來源和目標。在此範例中，目標是 Azure VMware 解決方案 SDDC HCX 終點。
2. 按一下“選擇要遷移的虛擬機器”。這提供了所有本地虛擬機器的清單。根據匹配：值表達式選擇虛擬機，然後按一下*新增*。
3. 在「傳輸和放置」部分中，更新必填欄位（「叢集*」、「儲存*」、「目標*」和「網路*」），包括遷移設定文件，然後按一下「驗證」。

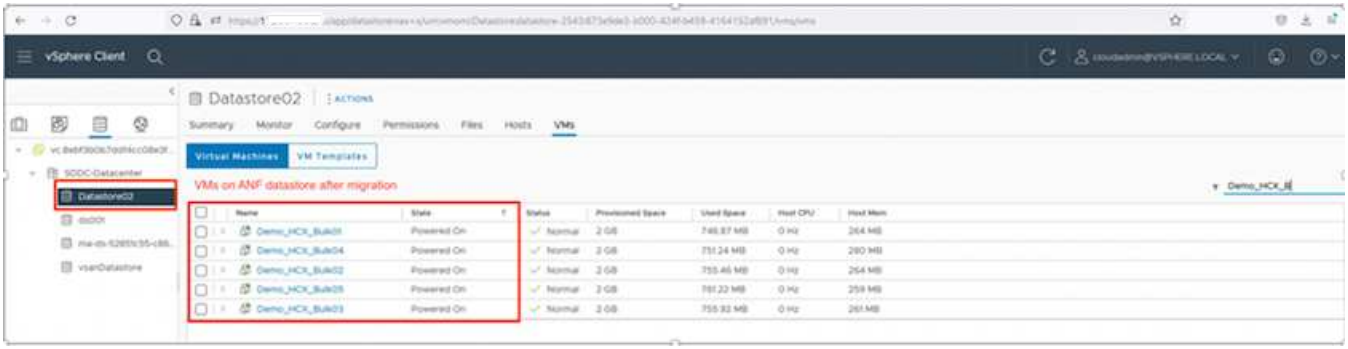


1. 驗證檢查完成後，按一下“開始”以啟動遷移。



在此遷移期間，將在目標 vCenter 內的指定Azure NetApp Files資料儲存體上建立佔位磁碟，以便將來源 VM 磁碟的資料複製到佔位磁碟。 HBR 觸發與目標的完全同步，在基準完成後，根據復原點目標 (RPO) 週期執行增量同步。全量/增量同步完成後，除非設定特定的計劃，否則會自動觸發切換。

1. 遷移完成後，透過存取目標 SDDC vCenter 進行驗證。

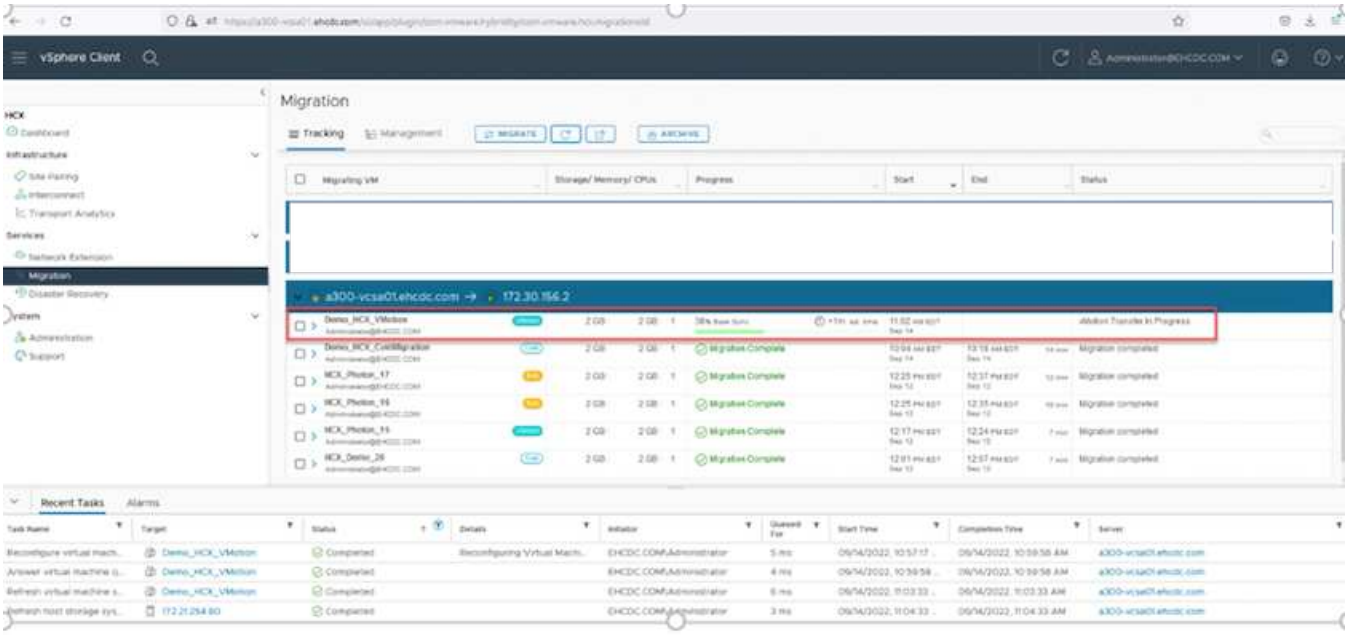


有關各種遷移選項以及如何使用 HCX 將工作負載從本地遷移到 Azure VMware 解決方案的更多詳細信息，請參閱 "VMware HCX 遷移注意事項"。

要了解有關此過程的更多信息，請觀看以下視頻：

使用 HCX 進行工作負載遷移

這是 HCX vMotion 選項的螢幕截圖。



要了解有關此過程的更多信息，請觀看以下視頻：

HCX vMotion

確保有足夠的頻寬來處理遷移。

目標 ANF 資料儲存應具有足夠的空間來處理遷移。

結論

無論您的目標是全雲還是混合雲，以及駐留在本地任何類型/供應商儲存上的數據， Azure NetApp Files和 HCX 都提供了部署和遷移應用程式工作負載的絕佳選擇，同時透過使資料需求無縫連接到應用程式層來降低 TCO。無論用例如何，選擇 Azure VMware 解決方案以及Azure NetApp Files都可以快速實現雲端優勢、跨本地和多個雲端的一致基礎架構和操作、工作負載的雙向可移植性以及企業級容量和效能。使用 VMware vSphere Replication、VMware vMotion 甚至網路檔案複製 (NFC) 連接儲存和遷移虛擬機器所使用的流程和程式相同。

總結

該文件的要點包括：

- 現在可以將Azure NetApp Files用作 Azure VMware 解決方案 SDDC 上的資料儲存。
- 您可以輕鬆地將資料從本機遷移到Azure NetApp Files資料儲存。
- 您可以輕鬆擴大或縮小Azure NetApp Files資料儲存以滿足遷移活動期間的容量和效能要求。

在哪裡可以找到更多信息

要了解有關本文檔中描述的信息的更多信息，請參閱以下網站連結：

- Azure VMware 解決方案文檔

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

- Azure NetApp Files文檔

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- VMware HCX 遷移注意事項

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

NetApp適用於 GCP/GCVE

NetApp針對 Google Cloud Platform GCVE 的功能

詳細了解NetApp為 Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) 帶來的功能 - 從NetApp作為來賓連接儲存裝置或補充 NFS 資料儲存到遷移工作流程、擴展/爆發到雲端、備份/復原和災難復原。

透過選擇以下選項跳到所需內容的部分：

- "在 GCP 中配置 GCVE"
- "NetApp的 GCVE 儲存選項"
- "NetApp /VMware 雲端解決方案"

在 GCP 中配置 GCVE

與本地一樣，規劃基於雲端的虛擬化環境對於成功創建虛擬機器和遷移的生產就緒環境至關重要。

本節介紹如何設定和管理 GCVE，以及如何將其與可用於連接NetApp儲存的選項結合使用。

> 客戶機內儲存是將Cloud Volumes ONTAP和Google Cloud NetApp Volumes連接到 GCVE 的唯一支援方法。

設定過程可分為以下步驟：

- 部署和配置 GCVE
- 啟用對 GCVE 的私人訪問

查看詳細信息"GCVE 的設定步驟"。

NetApp的 GCVE 儲存選項

NetApp儲存在 GCP GCVE 中可以以多種方式使用 - 既可以作為猜測連接，也可以作為補充 NFS 資料儲存。

請訪問"支援的NetApp儲存選項"了解更多。

Google Cloud 支援以下配置的NetApp儲存：

- Cloud Volumes ONTAP (CVO) 作為來賓連接存儲
- Google Cloud NetApp Volumes （NetApp Volumes）作為來賓連接存儲

- Google Cloud NetApp Volumes （NetApp Volumes）作為補充 NFS 資料存儲

查看詳細信息"GCVE 的來賓連接儲存選項"。查看詳細信息"GCVE 的補充 NFS 資料儲存選項"。

閱讀更多"Google Cloud NetApp Volumes資料儲存區支援 Google Cloud VMware Engine（NetApp部落格）"或者"如何將Google Cloud NetApp Volumes用作 Google Cloud VMware Engine 的資料儲存區（Google 部落格）"

解決方案用例

透過NetApp和 VMware 雲端解決方案，許多用例都可以在 Azure AVS 中輕鬆部署。針對 VMware 定義的每個雲端區域都定義了這些用例：

- 保護（包括災難復原和備份/還原）
- 延長
- 遷移

"瀏覽適用於 Google Cloud GCVE 的NetApp解決方案"

保護 **GCP/GCVE** 上的工作負載

使用**NetApp SnapCenter**和 **Veeam Replication** 實現應用程式一致性災難復原

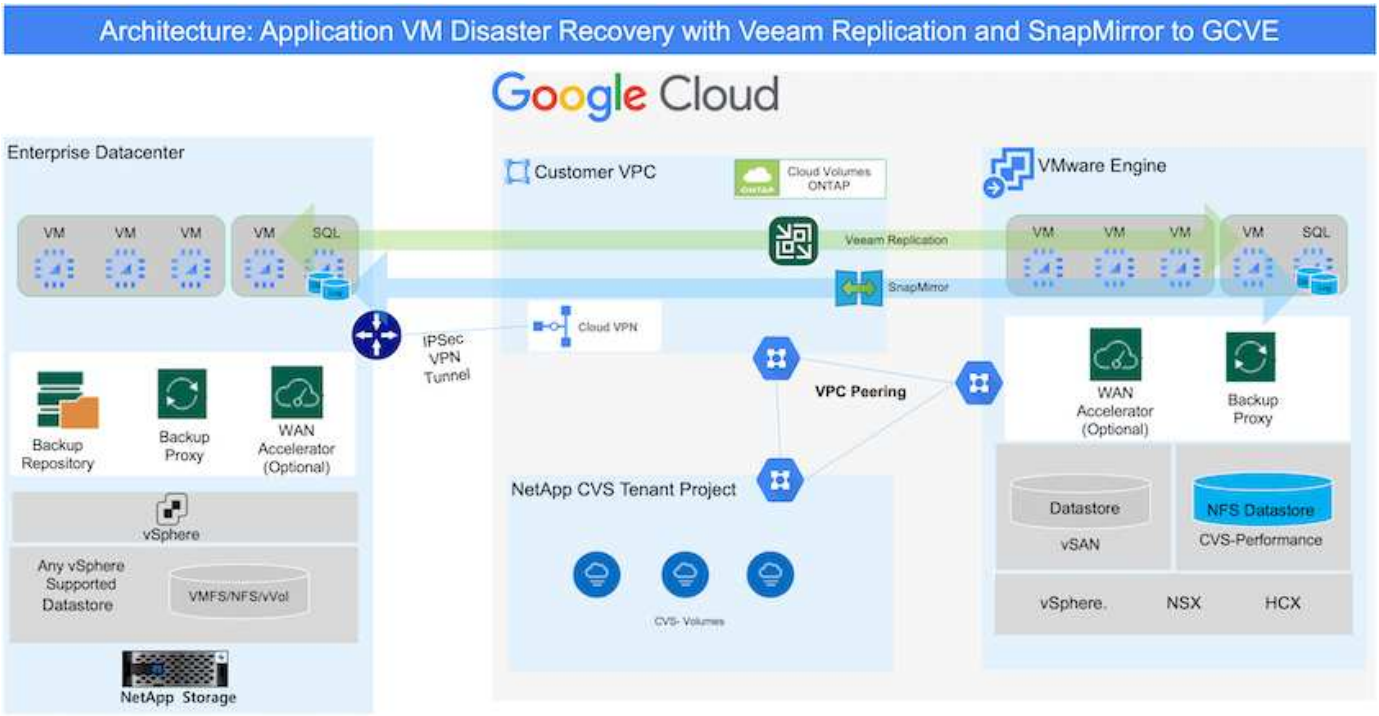
雲端災難復原是一種具有彈性且經濟高效的方法，可保護工作負載免受網站中斷和勒索軟體等資料損壞事件的影響。透過NetApp SnapMirror，使用來賓連接儲存的本機 VMware 工作負載可以複製到在 Google Cloud 中執行的NetApp Cloud Volumes ONTAP 。

概況

許多客戶正在為託管在 VMware vSphere 上的應用程式虛擬機器尋找有效的災難復原解決方案。他們中的許多人使用現有的備份解決方案在災難期間進行復原。很多時候，該解決方案會增加 RTO 並且無法滿足他們的期望。為了減少 RPO 和 RTO，只要有網路連線和具有適當權限的環境，就可以利用 Veeam VM 複製，甚至可以從本地到 GCVE。注意：Veeam VM Replication 不會保護 VM 用戶機連接的儲存設備，例如客戶機 VM 內的 iSCSI 或 NFS 掛載。需要單獨保護它們。

為了實現 SQL VM 的應用程式一致性複製並減少 RTO，我們使用SnapCenter來協調 SQL 資料庫和日誌磁碟區的 SnapMirror 操作。

本文檔提供了使用NetApp SnapMirror、Veeam 和 Google Cloud VMware Engine (GCVE) 設定和執行災難復原的逐步方法。



假設

本文檔重點介紹應用程式資料的客戶機內儲存（也稱為客戶機連線），我們假設本機環境使用SnapCenter進行應用程式一致性備份。

本文檔適用於任何第三方備份或復原解決方案。根據環境中使用的解決方案，遵循最佳實務來建立符合組織 SLA 的備份策略。

對於本地環境和 Google Cloud 網路之間的連接，請使用專用互連或 Cloud VPN 等連接選項。應根據內部部署 VLAN 設計來建立段。

將本機資料中心連接到 Google Cloud 有多種選擇，因此我們無法在本文檔中概述特定的工作流程。請參閱 Google Cloud 文檔，以了解適當的本地到 Google 連接方法。

部署災難復原解決方案

解決方案部署概述

1. 確保使用SnapCenter備份應用程式資料並滿足必要的 RPO 要求。
2. 使用 NetApp Console 在適當的訂閱和虛擬網路中配置具有正確執行個體大小的 Cloud Volumes ONTAP。
   a. 為相關應用程式磁碟區設定SnapMirror 。
   b. 更新SnapCenter中的備份策略以在排程的作業之後觸發SnapMirror更新。
3. 安裝 Veeam 軟體並開始將虛擬機器複製到 Google Cloud VMware Engine 執行個體。
4. 在災難事件期間，將 SnapMirror 關係透過 NetApp Console 中斷，並使用 Veeam 觸發虛擬機器的容錯移轉。
   a. 重新連接應用程式虛擬機器的 ISCSI LUN 和 NFS 掛載。

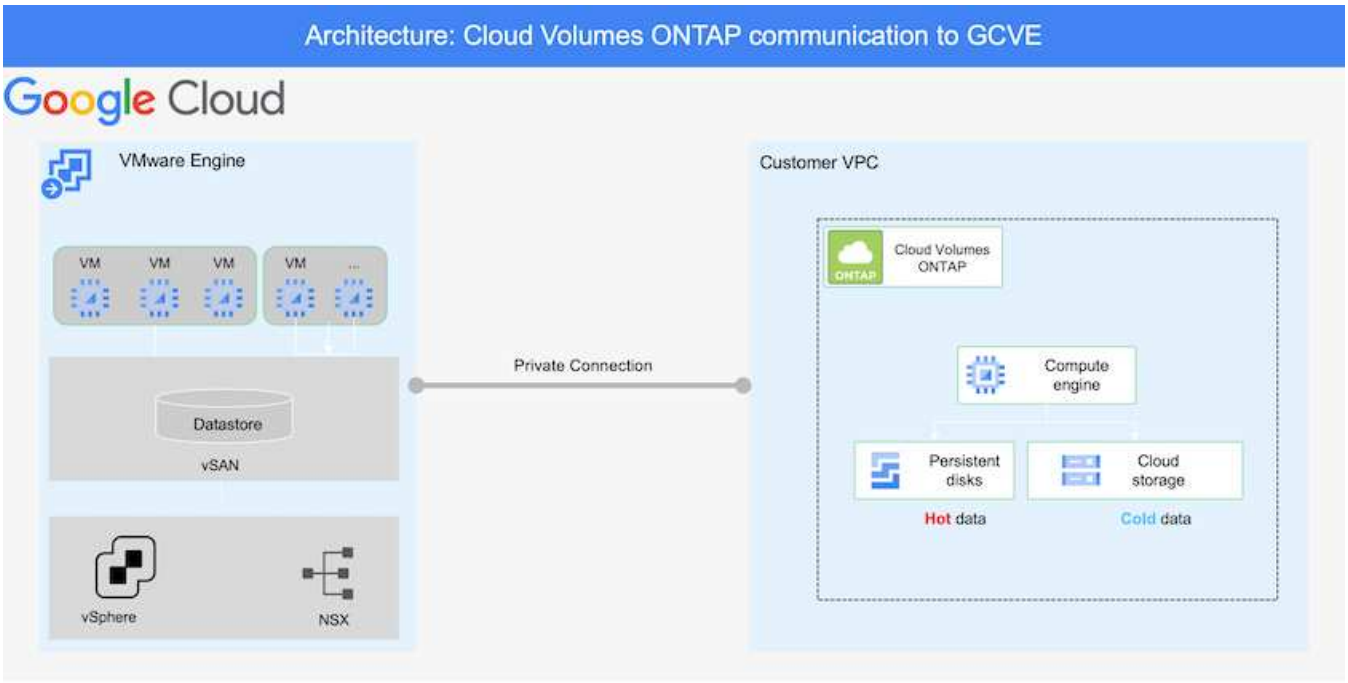
b. 在網路上啟動應用程式。

5. 主站點恢復後，透過反向重新同步SnapMirror呼叫故障回復到受保護站點。

部署詳情

▼ 在 **Google Cloud** 上設定 **CVO** 並將磁碟區複製到 **CVO**

第一步是在 Google Cloud 上設定Cloud Volumes ONTAP （"克沃") 並以所需的頻率和快照保留將所需的磁碟區複製到Cloud Volumes ONTAP 。



有關設定SnapCenter和複製資料的範例逐步說明，請參閱"使用SnapCenter設定複製"

使用SnapCenter審查 SQL VM 保護

▼ 配置 **GCVE** 主機和 **CVO** 資料存取

部署 SDDC 時需要考慮的兩個重要因素是 GCVE 解決方案中 SDDC 叢集的大小以及保持 SDDC 服務的時間。災難復原解決方案的這兩個關鍵考慮因素有助於降低整體營運成本。 SDDC 最小可以只有三台主機，最大可以達到全面部署的多主機叢集。

Google Cloud NetApp Volumes for NFS 資料儲存區和Cloud Volumes ONTAP for SQL 資料庫和日誌可以部署到任何 VPC，並且 GCVE 應該具有與該 VPC 的私有連接以掛載 NFS 資料儲存區並讓 VM 連接到 iSCSI LUN。

若要設定 GCVE SDDC，請參閱"在 Google Cloud Platform (GCP) 上部署和配置虛擬化環境"。作為先決條件，請驗證在建立連線後，駐留在 GCVE 主機上的客戶虛擬機器是否能夠使用來自Cloud Volumes ONTAP的資料。

正確配置Cloud Volumes ONTAP和 GCVE 後，開始設定 Veeam，使用 Veeam 複製功能自動將本機工作負載恢復到 GCVE（具有應用程式 VMDK 的虛擬機器和具有來賓內儲存的虛擬機器），並利用SnapMirror將應用程式磁碟區複製到Cloud Volumes ONTAP。

▼ 安裝 **Veeam** 組件

根據部署場景，需要部署Veeam備份伺服器、備份儲存庫和備份代理程式。對於這種用例，不需要為 Veeam 部署物件存儲，也不需要 Scale-out 儲存庫。https://helpcenter.veeam.com/docs/backup/vsphere/replication_components.html?ver=120["有關安裝過程，請參閱 Veeam 文檔"]欲了解更多信息，請參閱"使用 Veeam Replication 進行遷移"

▼ 使用 **Veeam** 設定虛擬機器複製

本機 vCenter 和 GCVE vCenter 都需要在 Veeam 中註冊。 "設定 vSphere VM 複製作業"在精靈的客戶機處理步驟中，選擇停用應用程式處理，因為我們將利用SnapCenter進行應用程式感知備份和復原。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

▼ **Microsoft SQL Server VM** 的故障轉移

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

此解決方案的優勢

- 使用SnapMirror的高效且有彈性的複製。
- 透過ONTAP快照保留還原到任何可用的時間點。
- 從儲存、運算、網路和應用程式驗證步驟，恢復數百到數千台虛擬機器所需的所有步驟均可完全自動化。
- SnapCenter使用不會改變複製磁碟區的克隆機制。
  - 這避免了磁碟區和快照資料損壞的風險。
  - 避免 DR 測試工作流程期間的複製中斷。
  - 利用 DR 資料進行 DR 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。
- Veeam Replication 允許在 DR 站點上變更 VM IP 位址。

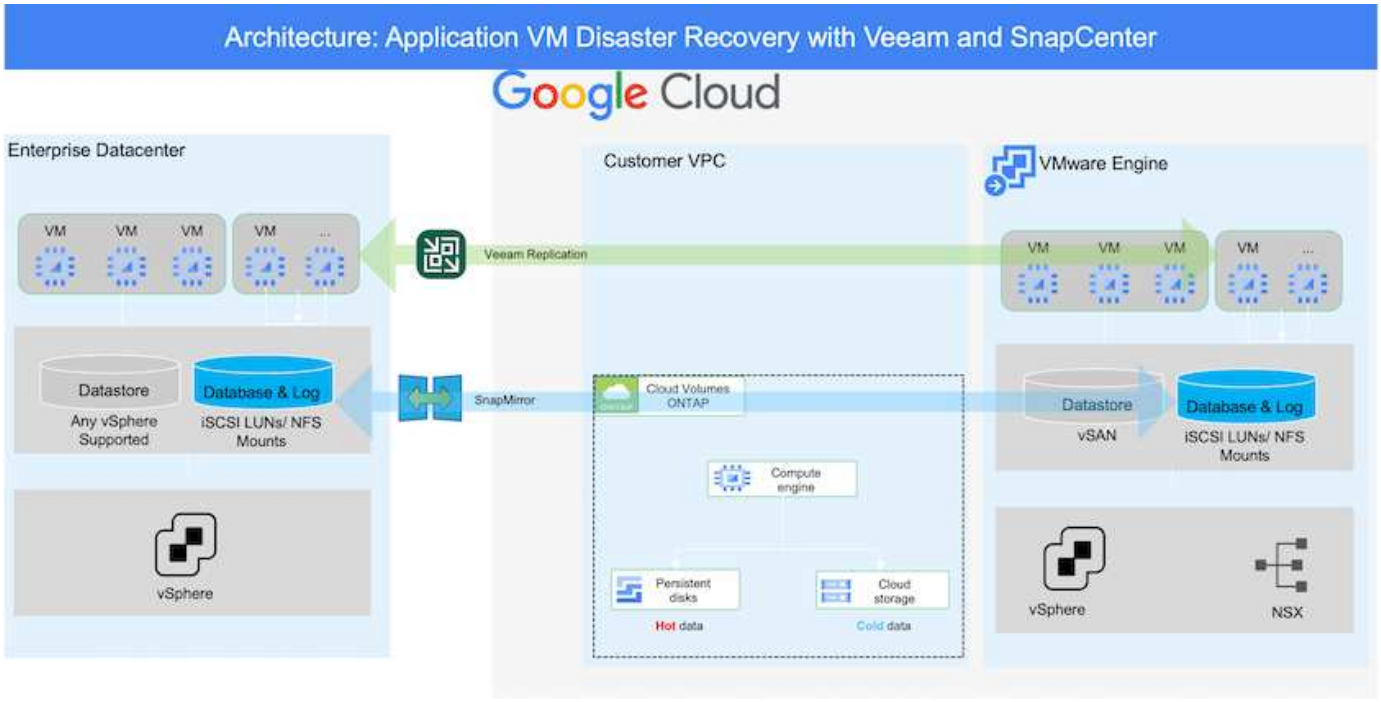
使用**SnapCenter**、 **Cloud Volumes ONTAP**和 **Veeam Replication** 實現應用程式災難復原

雲端災難復原是一種具有彈性且經濟高效的方法，可保護工作負載免受網站中斷和勒索軟體等資料損壞事件的影響。透過NetApp SnapMirror，使用來賓連接儲存的本機 VMware 工作負載可以複製到在 Google Cloud 中執行的NetApp Cloud Volumes ONTAP 。

概況

這涵蓋了應用程式資料；但是，實際的虛擬機器本身又如何呢？災難復原應涵蓋所有相關元件，包括虛擬機器、VMDK、應用程式資料等。為了實現此目的，可以使用SnapMirror和 Veeam 無縫恢復從本地複製到Cloud Volumes ONTAP 的工作負載，同時使用 vSAN 儲存作為 VM VMDK。

本文檔提供了使用NetApp SnapMirror、Veeam 和 Google Cloud VMware Engine (GCVE) 設定和執行災難復原的逐步方法。



假設

本文檔重點介紹應用程式資料的客戶機內儲存（也稱為客戶機連線），我們假設本機環境使用SnapCenter進行應用程式一致性備份。

本文檔適用於任何第三方備份或復原解決方案。根據環境中使用的解決方案，遵循最佳實務來建立符合組織 SLA 的備份策略。

對於本地環境和 Google Cloud 網路之間的連接，請使用專用互連或 Cloud VPN 等連接選項。應根據內部部署 VLAN 設計來建立段。

將本機資料中心連接到 Google Cloud 有多種選擇，因此我們無法在本文檔中概述特定的工作流程。請參閱 Google Cloud 文檔，以了解適當的本地到 Google 連接方法。

部署災難復原解決方案

解決方案部署概述

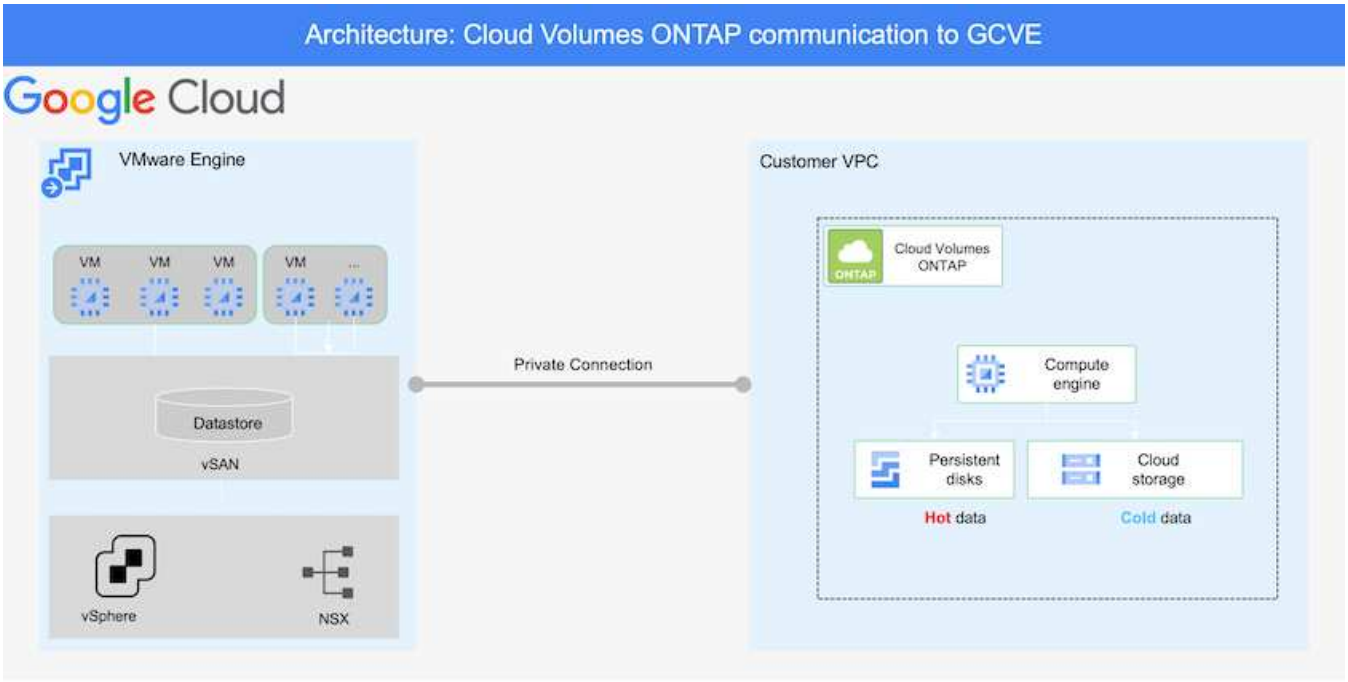
1. 確保使用SnapCenter備份應用程式資料並滿足必要的 RPO 要求。
2. 使用適當的訂閱和虛擬網路中的雲端管理器為Cloud Volumes ONTAP配置正確的執行個體大小。
   a. 為相關應用程式磁碟區設定SnapMirror 。
   b. 更新SnapCenter中的備份策略以在排程的作業之後觸發SnapMirror更新。
3. 安裝 Veeam 軟體並開始將虛擬機器複製到 Google Cloud VMware Engine 執行個體。
4. 在災難事件期間，使用 Cloud Manager 中斷SnapMirror關係並使用 Veeam 觸發虛擬機器故障轉移。
   a. 重新連接應用程式虛擬機器的 ISCSI LUN 和 NFS 掛載。
   b. 在網路上啟動應用程式。

5. 主站點恢復後，透過反向重新同步SnapMirror呼叫故障回復到受保護站點。

部署詳情

▼ 在 **Google Cloud** 上設定 **CVO** 並將磁碟區複製到 **CVO**

第一步是在 Google Cloud 上設定Cloud Volumes ONTAP （"克沃") 並以所需的頻率和快照保留將所需的磁碟區複製到Cloud Volumes ONTAP 。



有關設定SnapCenter和複製資料的範例逐步說明，請參閱"使用SnapCenter設定複製"

使用SnapCenter設定複製

▼ 配置 **GCVE** 主機和 **CVO** 資料存取

部署 SDDC 時需要考慮的兩個重要因素是 GCVE 解決方案中 SDDC 叢集的大小以及保持 SDDC 服務的時間。災難復原解決方案的這兩個關鍵考慮因素有助於降低整體營運成本。 SDDC 最小可以只有三台主機，最大可以達到全面部署的多主機叢集。

Cloud Volumes ONTAP可以部署到任何 VPC，並且 GCVE 應該與該 VPC 建立私有連接，以使 VM 連接到 iSCSI LUN。

若要設定 GCVE SDDC，請參閱"在 Google Cloud Platform (GCP) 上部署和配置虛擬化環境"。作為先決條件，請驗證在建立連線後，駐留在 GCVE 主機上的客戶虛擬機器是否能夠使用來自Cloud Volumes ONTAP的資料。

正確配置Cloud Volumes ONTAP和 GCVE 後，開始設定 Veeam，使用 Veeam 複製功能自動將本機工作負載恢復到 GCVE（具有應用程式 VMDK 的虛擬機器和具有來賓內儲存的虛擬機器），並利用SnapMirror將應用程式磁碟區複製到Cloud Volumes ONTAP。

▼ 安裝 **Veeam** 組件

根據部署場景，需要部署Veeam備份伺服器、備份儲存庫和備份代理程式。對於這種用例，不需要為 Veeam 部署物件存儲，也不需要 Scale-out 儲存
庫。https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["有關安裝過程，

請參閱 Veeam 文檔"]

▼ 使用 **Veeam** 設定虛擬機器複製

本機 vCenter 和 GCVE vCenter 都需要在 Veeam 中註冊。 "設定 vSphere VM 複製作業"在精靈的客戶機處理步驟中，選擇停用應用程式處理，因為我們將利用SnapCenter進行應用程式感知備份和復原。

設定 vSphere VM 複製作業

▼ **Microsoft SQL Server VM** 的故障轉移

Microsoft SQL Server VM 的故障轉移

此解決方案的優勢

- 使用SnapMirror的高效且有彈性的複製。
- 透過ONTAP快照保留還原到任何可用的時間點。
- 從儲存、運算、網路和應用程式驗證步驟，恢復數百到數千台虛擬機器所需的所有步驟均可完全自動化。
- SnapCenter使用不會改變複製磁碟區的克隆機制。
  - 這避免了磁碟區和快照資料損壞的風險。
  - 避免 DR 測試工作流程期間的複製中斷。
  - 利用 DR 資料進行 DR 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。
- Veeam Replication 允許在 DR 站點上變更 VM IP 位址。

使用 **Veeam Replication** 和**Google Cloud NetApp Volumes**資料儲存區實現 **Google Cloud VMware Engine** 的災難復原

在危機時刻，全面的災難復原計畫對企業來說至關重要。許多組織利用雲端運算進行日常營運和災難復原。這種主動的方法可以減少或消除昂貴的業務中斷。

本文介紹如何使用 Veeam Backup & Replication 設定本機 VMware VM 到具有Google Cloud NetApp Volumes (NetApp Volumes) 的 Google Cloud VMware Engine (GCVE) 的災難復原。

概況

Google Cloud NetApp Volumes是 Google 和NetApp推出的儲存服務，可用於 Google Cloud。 NetApp Volumes 服務提供高效能 NFS/SMB 儲存。 VMware 認證的NetApp Volumes NFS 儲存可用作 GCVE 中 ESXi 主機的外部資料儲存。使用者需要在其 GCVE 私有雲和NetApp Volumes 專案之間建立對等連線。區域內的儲存存取不會產生任何網路費用。使用者可以在 Google Cloud 控制台中建立NetApp Volumes 卷，並在將磁碟區作為資料儲存區掛載到其 ESXi 主機之前啟用刪除保護。

基於NetApp Volumes 的 NFS 資料儲存區可用於使用任何經過驗證且提供 VM 複製功能的第三方解決方案從本機複製資料。透過新增NetApp Volumes 資料存儲，可以實現成本優化部署，而無需建立基於 Google Cloud VMware Engine (GCVE) 的 SDDC 並使用大量 ESXi 主機來容納儲存。這種方法被稱為「Pilot Light Cluster」。試點燈叢集是最小 GCVE 主機配置（3 x GCVE ESXi 主機）以及NetApp Volumes 資料儲存容量，以允許獨立擴展以滿足容量需求。

目標是僅使用管理故障轉移的核心組件來維持具有成本效益的基礎設施。在發生故障轉移時，指示燈叢集可以擴展並新增更多 GCVE 主機。一旦故障轉移得到解決並且正常運作恢復，指示燈叢集就可以縮小規模，回到低成

本的運作模式。

本文件的目的

本文介紹如何使用Google Cloud NetApp Volumes資料儲存和 Veeam Backup & Replication 來設定本地 VMware VM 到 GCVE 的災難復原（使用 Veeam VM 複製軟體功能）。

Veeam Backup & Replication 是一款用於虛擬環境的備份和複製應用程式。當虛擬機器被複製時，Veeam Backup & Replication 會在目標 GCVE SDDC 叢集上以原生 VMware vSphere 格式建立虛擬機器的精確副本。Veeam Backup & Replication 將使副本與原始 VM 保持同步。複製提供了最佳的復原時間目標 (RTO)，因為 DR 站點上有一個處於準備啟動狀態的 VM 的安裝副本。

這種複製機制確保在災難事件發生時工作負載能夠在 GCVE 中快速啟動。 Veeam Backup & Replication 軟體也優化了透過 WAN 和慢速連線進行複製的流量傳輸。此外，它還過濾掉重複的資料區塊、零資料區塊、交換檔案和「排除的 VM 客戶作業系統檔案」。該軟體還將壓縮副本流量。為了防止複製作業消耗整個網路頻寬，可以利用 WAN 加速器和網路限制規則。

Veeam Backup & Replication 中的複製過程由作業驅動，這表示複製是透過設定複製作業來執行的。如果發生災難事件，可以觸發故障轉移，透過故障轉移到其副本來恢復虛擬機器。當執行故障轉移時，複製的虛擬機器將接管原始虛擬機器的角色。可以執行故障轉移至副本的最新狀態或任何已知的良好還原點。這使得勒索軟體恢復或隔離測試能夠根據需要進行。 Veeam Backup & Replication 提供多種選項來處理不同的災難復原場景。

解決方案概述

此解決方案涵蓋以下進階步驟：

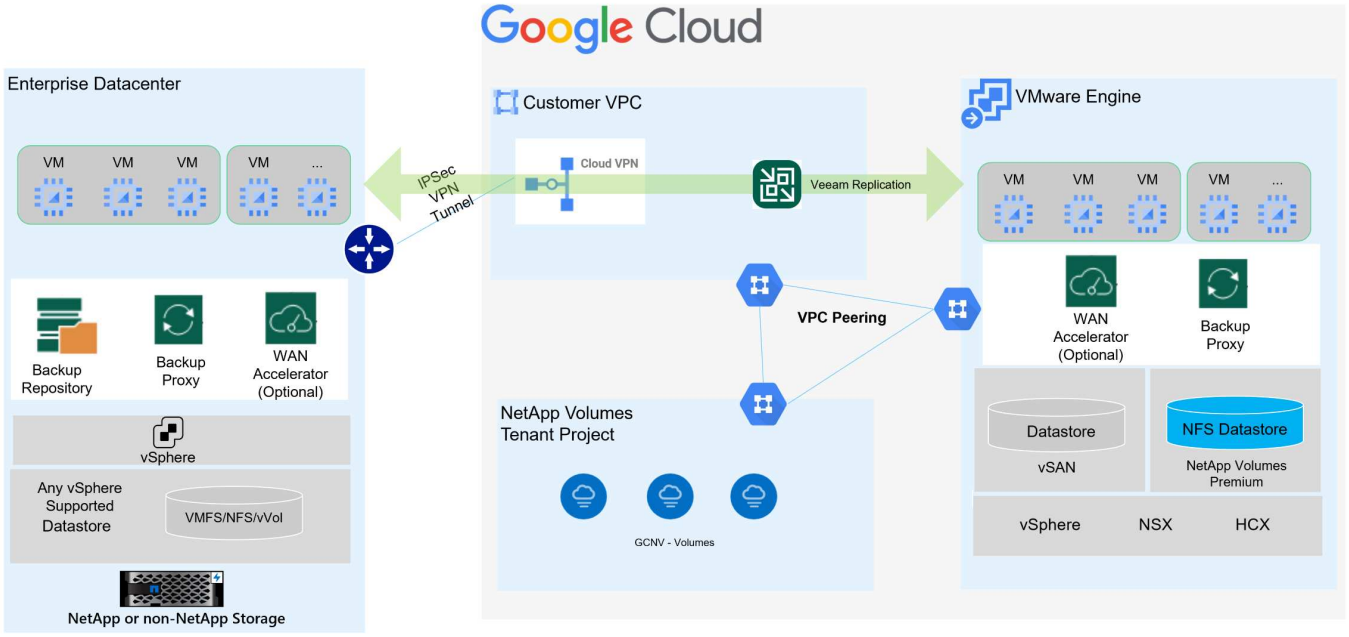
1. 使用Google Cloud NetApp Volumes建立 NFS 卷
2. 依照 GCP 流程從NetApp Volumes NFS 磁碟區建立 GCVE 資料儲存。
3. 設定複製作業以使用 Veeam Backup & Replication 建立 VM 副本。
4. 建立故障轉移計劃並執行故障轉移。
5. 災難事件結束且主站點啟動後，切換回生產虛擬機器。

> ⓘ 在NetApp Volumes 中建立磁碟區作為 GCVE 資料儲存時，僅支援 NFS v3。

有關使用NetApp Volumes NFS 磁碟區作為 GCVE 資料儲存的更多信息，請查看 "使用 NFS 磁碟區作為由Google Cloud NetApp Volumes託管的 vSphere 資料存儲"。

架構

下圖顯示了本文檔中提出的解決方案的架構。建議的最佳實踐是在本機站點和 GCVE SDDC 中都安裝一個 Veeam Backup & Replication 伺服器。備份和復原由內部部署的 Veeam 伺服器執行和管理，複製由 GCVE SDDC 中的 Veeam 伺服器管理。當主資料中心發生故障時，此架構可提供最高的可用性。



Veeam 複製到 **GCVE** 和**NetApp Volumes** 資料儲存區的先決條件

此解決方案需要以下元件和配置：

1. NetApp Volumes 有一個可用的儲存池，具有足夠的可用容量來容納要建立的 NFS 磁碟區。
2. Veeam Backup and Replication 軟體在具有適當網路連線的本機環境中運作。
3. 確保 Veeam Backup & Replication 備份 VM 連線到來源以及目標 GCVE SDDC 叢集。
4. 確保 Veeam Backup & Replication 備份 VM 連線到來源和目標 GCVE 叢集上的 Veeam 代理伺服器 VM。
5. 備份伺服器必須能夠解析短名稱並連接到來源 vCenter 和目標 vCenter。

使用者需要使用 VMware Engine Cloud 控制台 UI 中的 VPC 網路對等或私有連線頁面在其 GCVE 私有雲和NetApp Volumes 專案之間建立對等連線。

> 將 GCVE vCenter 伺服器新增至 Veeam Backup and Replication 清單時，Veeam 需要具有提升權限的 GCVE 解決方案使用者帳戶。如需詳細資訊，請參閱 Google Cloud Platform （GCP） 文件 "提升 VMware Engine 權限"。

有關更多信息，請參閱 "注意事項和限制"在 Veeam Backup & Replication 文件中。

部署步驟

以下部分概述了使用Google Cloud NetApp Volumes建立和掛載 NFS 資料儲存的部署步驟，以及使用 Veeam Backup and Replication 在本機資料中心和 Google Cloud VMware Engine 之間實施完整災難復原解決方案的步驟。

為 **GCVE** 建立**NetApp Volumes NFS** 捲和資料存儲

參考 "使用 NFS 磁碟區作為由Google Cloud NetApp Volumes託管的 vSphere 資料存儲"了解如何將Google Cloud NetApp Volumes作為 GCVE 的資料儲存的概述。

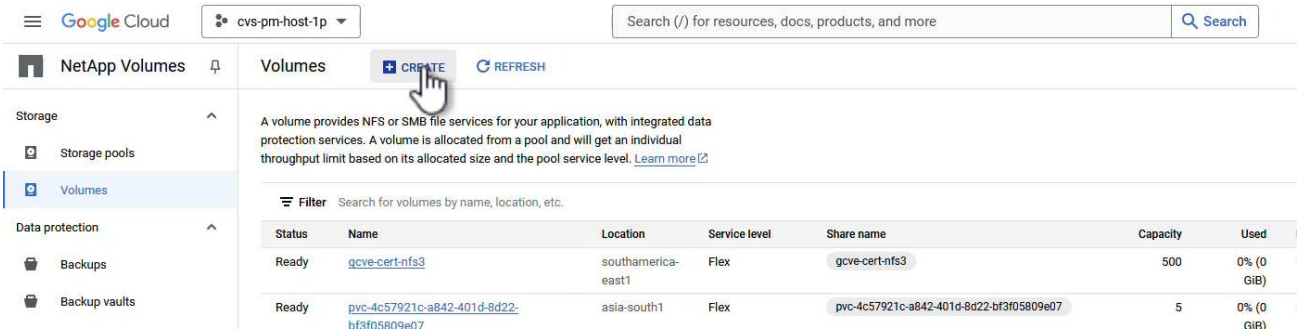
完成以下步驟以使用NetApp Volumes 為 GCVE 建立和使用 NFS 資料儲存：

▼ 建立**NetApp Volumes NFS** 卷

可從 Google Cloud Platform (GCP) 控制台存取Google Cloud NetApp Volumes 。

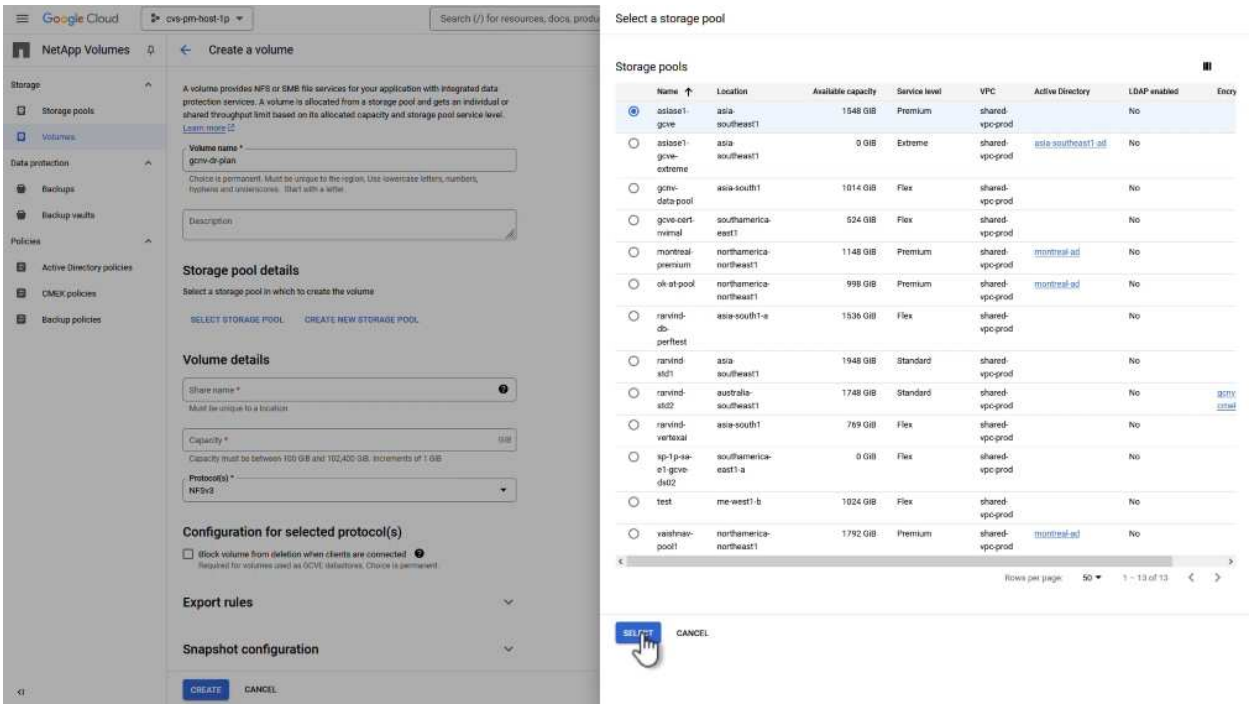
參考 "創建卷"有關此步驟的詳細信息，請參閱Google Cloud NetApp Volumes文件。

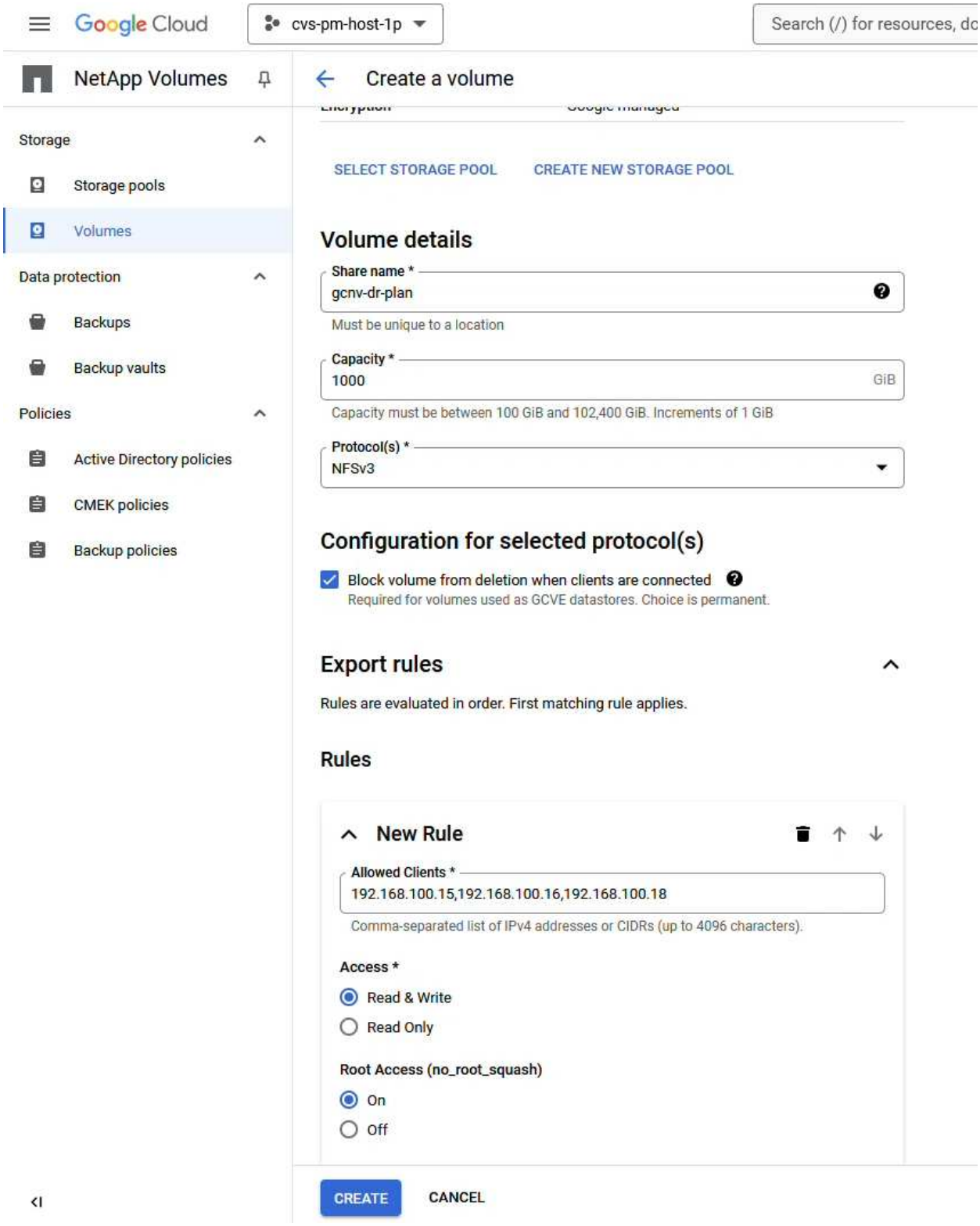
1. 在 Web 瀏覽器中，導覽至 https://console.cloud.google.com/並登入您的 GCP 控制台。搜尋 * NetApp Volumes* 開始。
2. 在* NetApp Volumes* 管理介面中，按一下* Create* 開始建立 NFS 磁碟區。



3. 在「建立磁碟區」精靈中，填寫所有必需的資訊：
   - 卷的名稱。
   - 建立磁碟區的儲存池。
   - 掛載 NFS 磁碟區時使用的共用名稱。
   - 卷的容量（以 GiB 為單位）。
   - 要使用的儲存協定。
   - 勾選此方塊以*客戶端連線時阻止刪除磁碟區*（GCVE 作為資料儲存安裝時需要）。
   - 訪問卷的導出規則。這是 NFS 網路上 ESXi 適配器的 IP 位址。
   - 用於使用本機快照保護磁碟區的快照計劃。
   - 或者，選擇備份磁碟區和/或為磁碟區建立標籤。

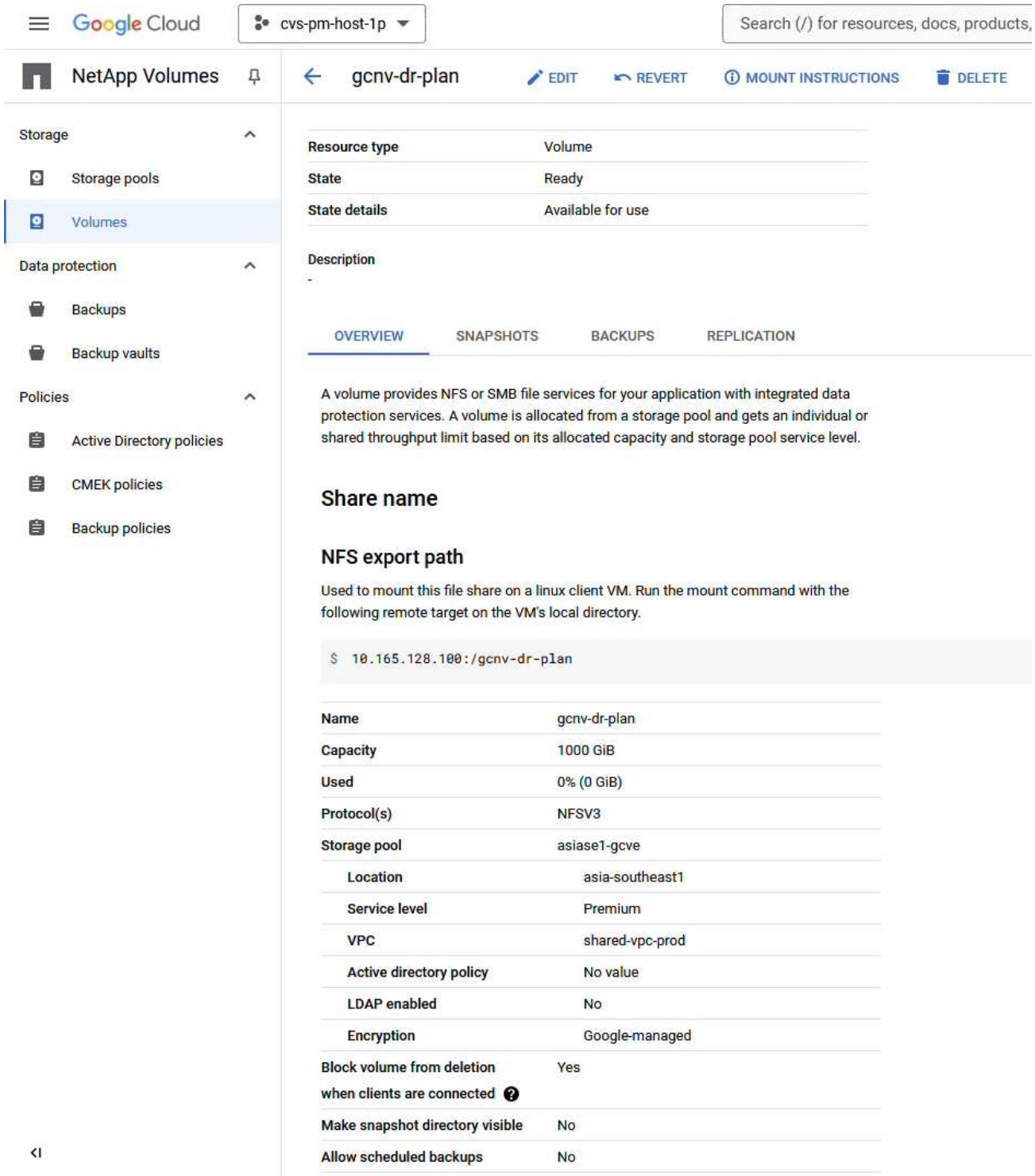
   在NetApp Volumes 中建立磁碟區作為 GCVE 資料儲存時，僅支援 NFS v3。


Google Cloud
cvs-pm-host-1p
Search (/) for resources, docs, produ
NetApp Volumes
Create a volume
Storage
Storage pools
Volumes
Data protection
Backups
Backup vaults
Policies
Active Directory policies
CMEK policies
Backup policies
A volume provides NFS or SMB file services for your application with integrated data protection services. A volume is allocated from a storage pool and gets an individual or shared throughput limit based on its allocated capacity and storage pool service level.
Learn more
Volume name *
gcnv-dr-plan
Choice is permanent. Must be unique to the region. Use lowercase letters, numbers, hyphens and underscores. Start with a letter.
Description
Storage pool details
Select a storage pool in which to create the volume
SELECT STORAGE POOL
CREATE NEW STORAGE POOL
Volume details
Share name *
Must be unique to a location
Capacity *
GiB
Capacity must be between 100 GiB and 102,400 GiB. Increments of 1 GiB
Protocol(s) *
NFSv3
Configuration for selected protocol(s)
Block volume from deletion when clients are connected
Required for volumes used as GCVE datastores. Choice is permanent.
Export rules
Snapshot configuration
CREATE
CANCEL
Select a storage pool
Storage pools
Name
Location
Available capacity
Service level
VPC
Active Directory
LDAP enabled
Encry
asiase1-gcve
asia-southeast1
1548 GiB
Premium
shared-vpc-prod
No
asiase1-gcve-extreme
asia-southeast1
0 GiB
Extreme
shared-vpc-prod
asia-southeast1-ad
No
gcnv-data-pool
asia-south1
1014 GiB
Flex
shared-vpc-prod
No
gcve-cert-nvmal
southamerica-east1
524 GiB
Flex
shared-vpc-prod
No
montreal-premium
northamerica-northeast1
1148 GiB
Premium
shared-vpc-prod
montreal-ad
No
ok-at-pool
northamerica-northeast1
998 GiB
Premium
shared-vpc-prod
montreal-ad
No
ranvind-db-perftest
asia-south1-a
1536 GiB
Flex
shared-vpc-prod
No
ranvind-std1
asia-southeast1
1948 GiB
Standard
shared-vpc-prod
No
ranvind-std2
australia-southeast1
1748 GiB
Standard
shared-vpc-prod
No
gcnv cmek
ranvind-vertexai
asia-south1
769 GiB
Flex
shared-vpc-prod
No
sp-1p-sa-e1-gcve-ds02
southamerica-east1-a
0 GiB
Flex
shared-vpc-prod
No
test
me-west1-b
1024 GiB
Flex
shared-vpc-prod
No
vaishnav-pool1
northamerica-northeast1
1792 GiB
Premium
shared-vpc-prod
montreal-ad
No
Rows per page: 50
1 – 13 of 13
SELECT
CANCEL



按一下「建立」以完成磁碟區的建立。

4. 一旦建立了磁碟區，就可以從磁碟區的屬性頁面查看掛載磁碟區所需的 NFS 匯出路徑。



▼ 在 **GCVE** 中掛載 **NFS** 資料存儲

在撰寫本文時，在 GCVE 中掛載資料儲存的過程需要開啟 GCP 支援票證才能將磁碟區掛載為 NFS 資料儲存。

參考 "使用 NFS 磁碟區作為由Google Cloud NetApp Volumes託管的 vSphere 資料存儲"了解更多。

將虛擬機器複製到 **GCVE** 並執行故障轉移計劃和故障回復

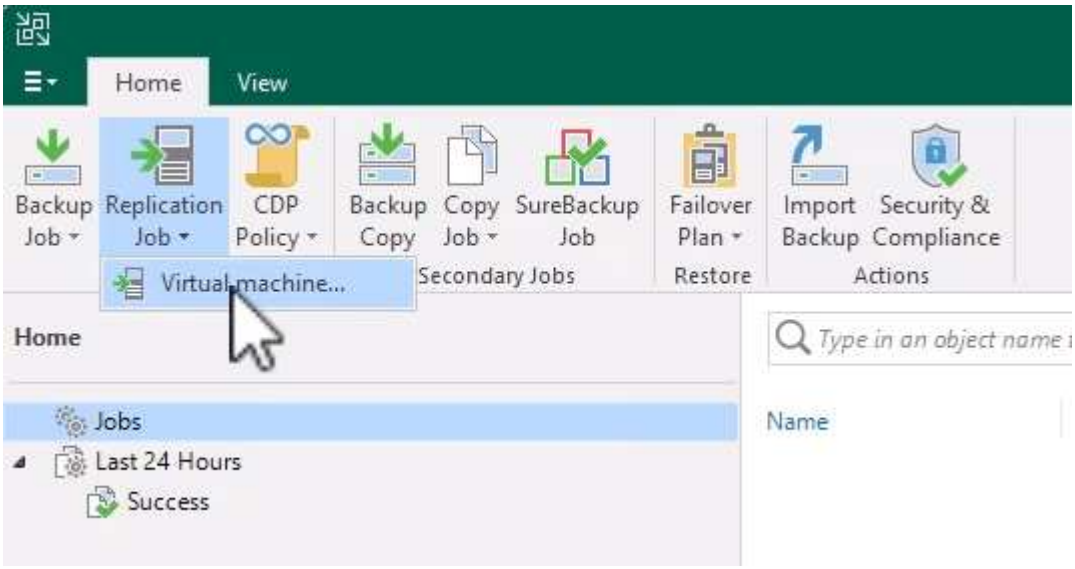
▼ 將虛擬機器複製到 **GCVE** 中的 **NFS** 資料存儲

Veeam Backup & Replication 在複製期間利用 VMware vSphere 快照功能，Veeam Backup & Replication 請

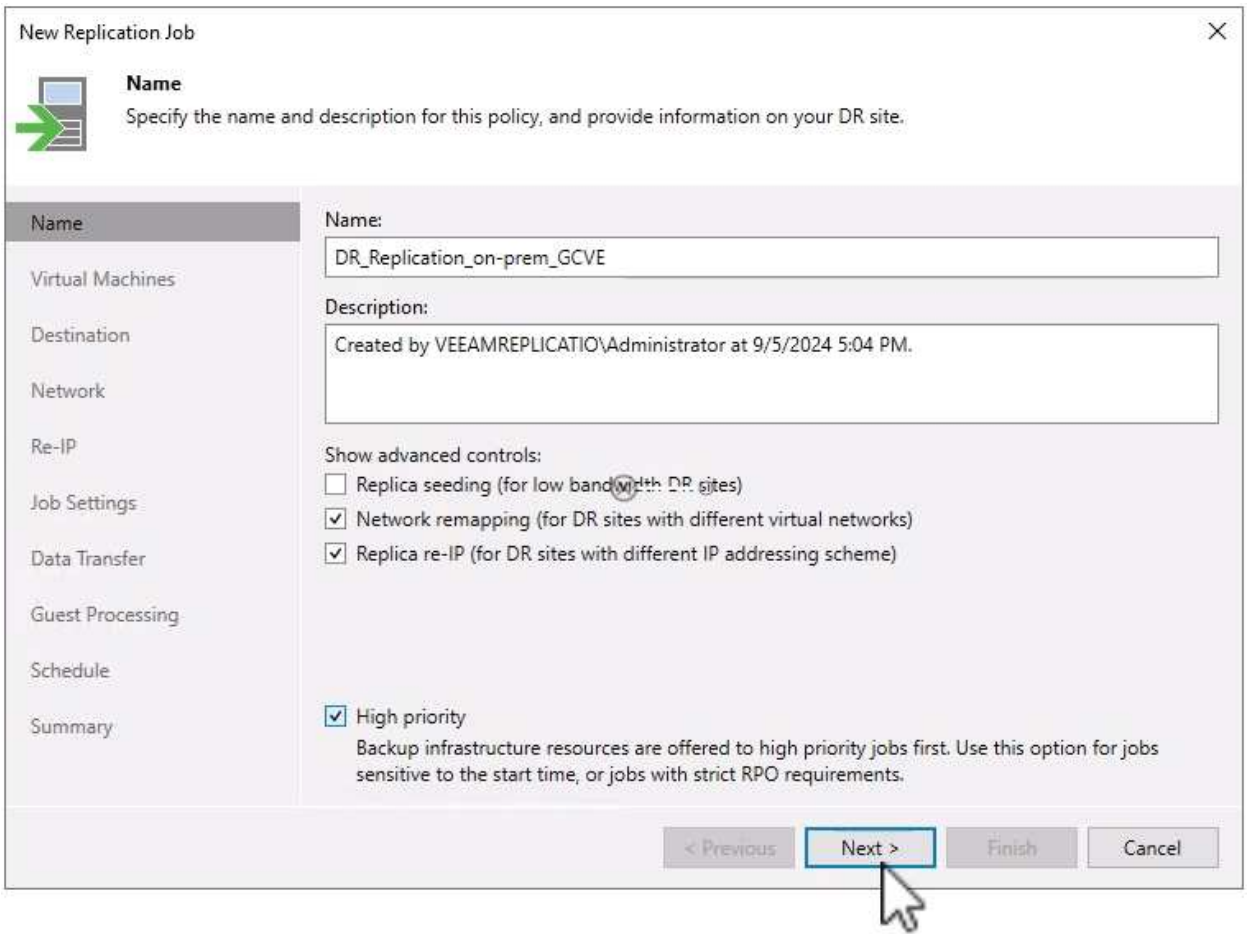
求 VMware vSphere 建立 VM 快照。 VM 快照是 VM 的時間點副本，其中包括虛擬磁碟、系統狀態、配置和元資料。 Veeam Backup & Replication 使用快照作為複製的資料來源。

若要複製虛擬機，請完成以下步驟：

1. 開啟 Veeam 備份和複製控制台。
2. 在“主頁”標籤上，按一下“複製作業”>“虛擬機器…”

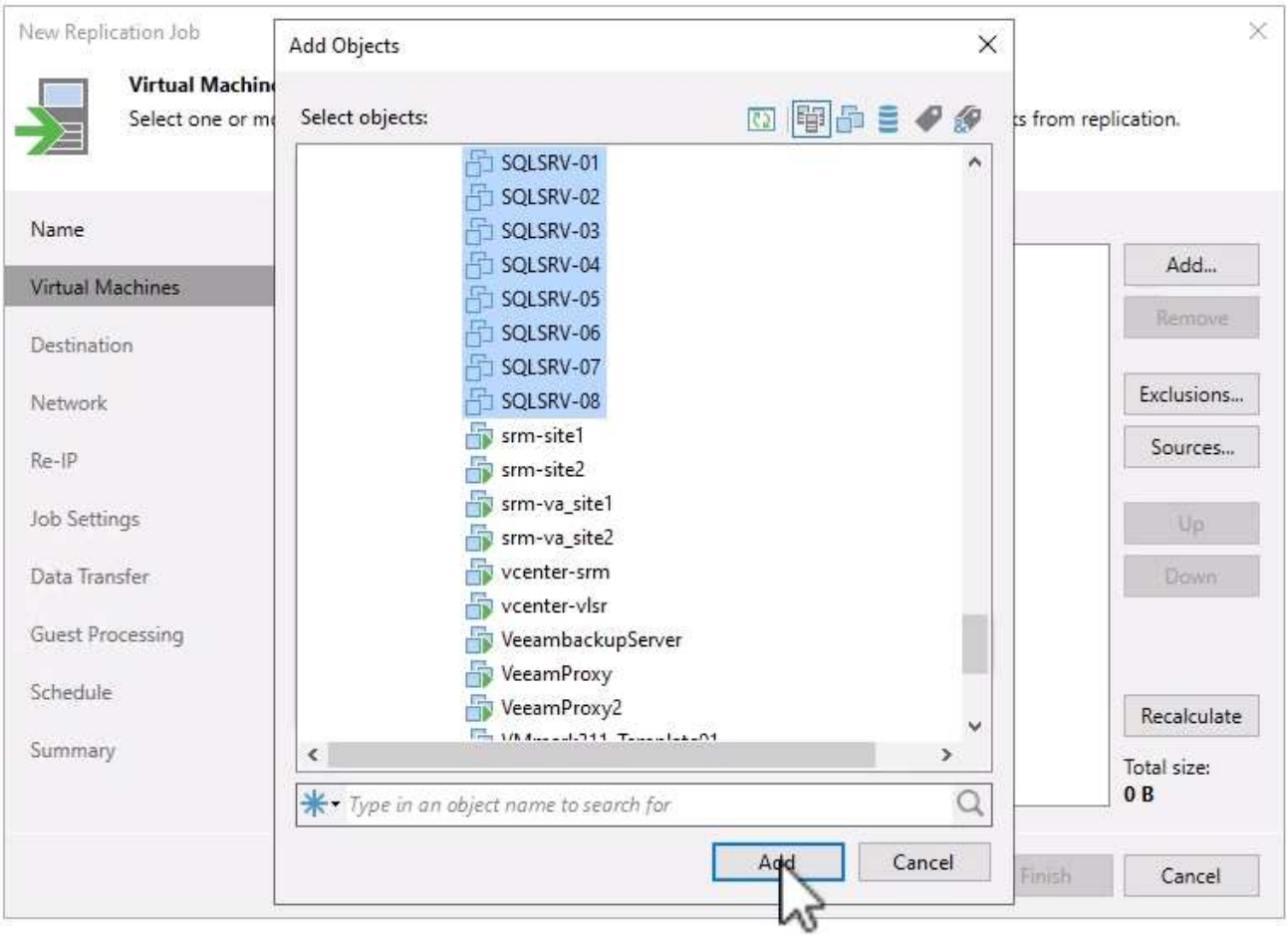


3. 在「新複製作業」精靈的「名稱」頁面上，指定作業名稱並選擇適當的進階控制複選框。
   - 如果本機和 GCP 之間的連線頻寬受限，請勾選「副本播種」複選框。
   - 如果 GCVE SDDC 上的段與本機站點網路的段不匹配，請選取網路重新對應（針對具有不同網路的 GCVE SDDC 站點）複選框。
   - 如果本機生產站點中的 IP 位址方案與目標 GCVE 站點中的方案不同，請選取副本重新 IP（適用於具有不同 IP 位址方案的 DR 站點）核取方塊。

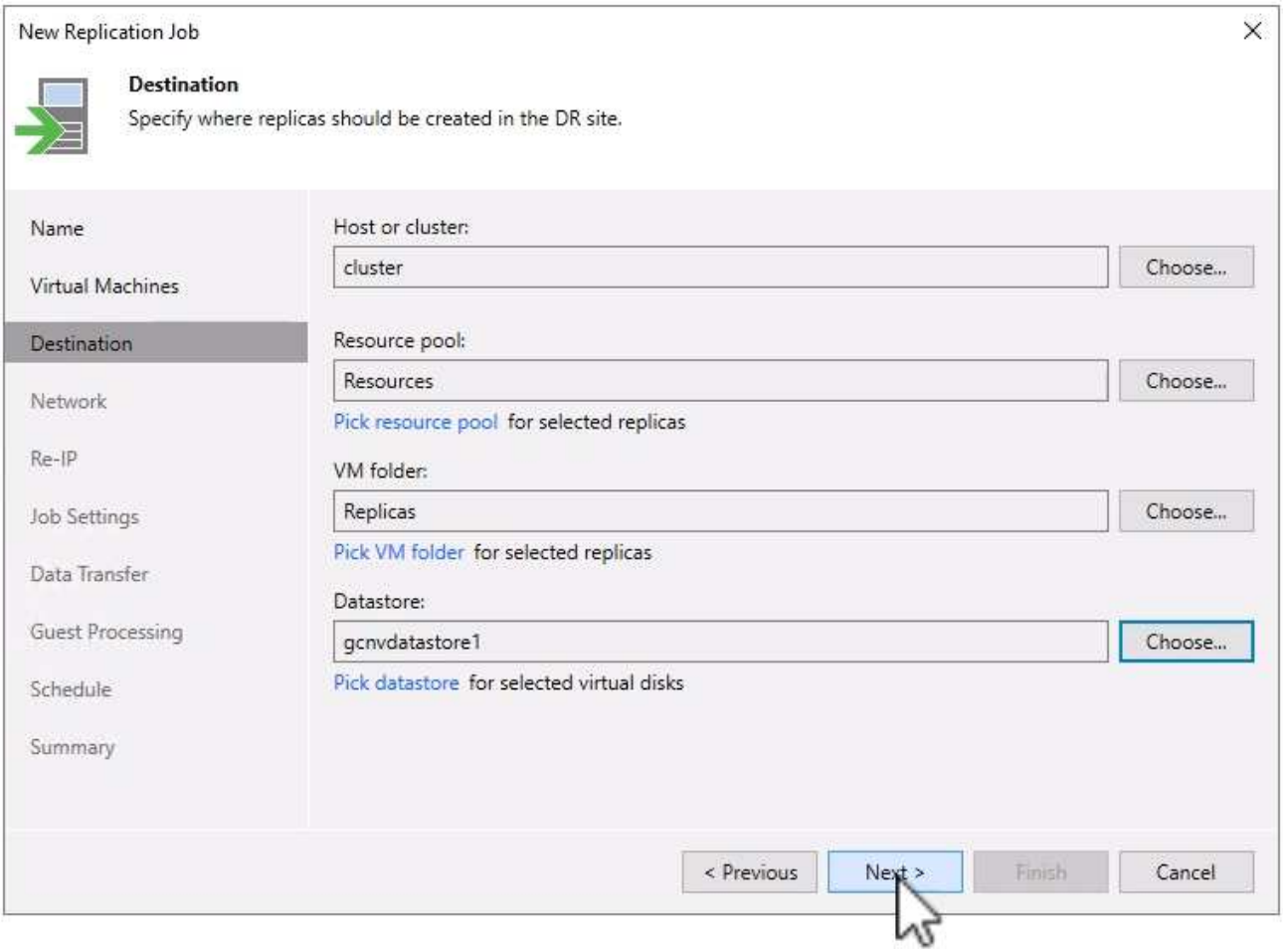


4. 在「虛擬機器」頁面上，選擇要複製到連接到 GCVE SDDC 的NetApp磁碟區資料儲存區的虛擬機器。按一下*新增*，然後在*新增物件*視窗中選擇必要的虛擬機器或虛擬機器容器，然後按一下*新增*。按一下“下一步”。

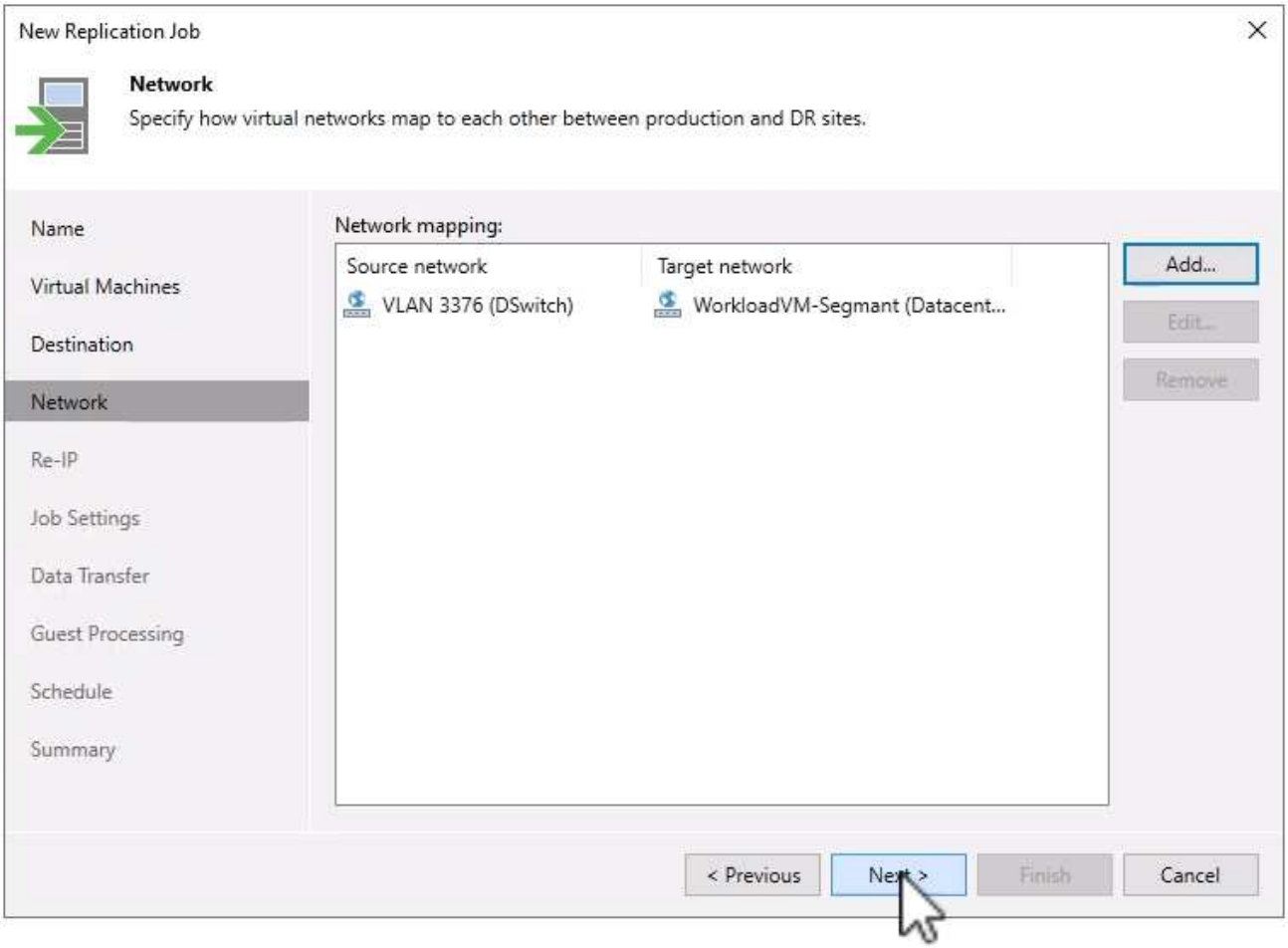
> 可以將虛擬機器放置在 vSAN 上以填入可用的 vSAN 資料儲存容量。在試點叢集中，3 節點 vSAN 叢集的可用容量將受到限制。其餘資料可以輕鬆放置在Google Cloud NetApp Volumes資料儲存中，以便可以恢復虛擬機，並且可以稍後擴展叢集以滿足 CPU/記憶體需求。



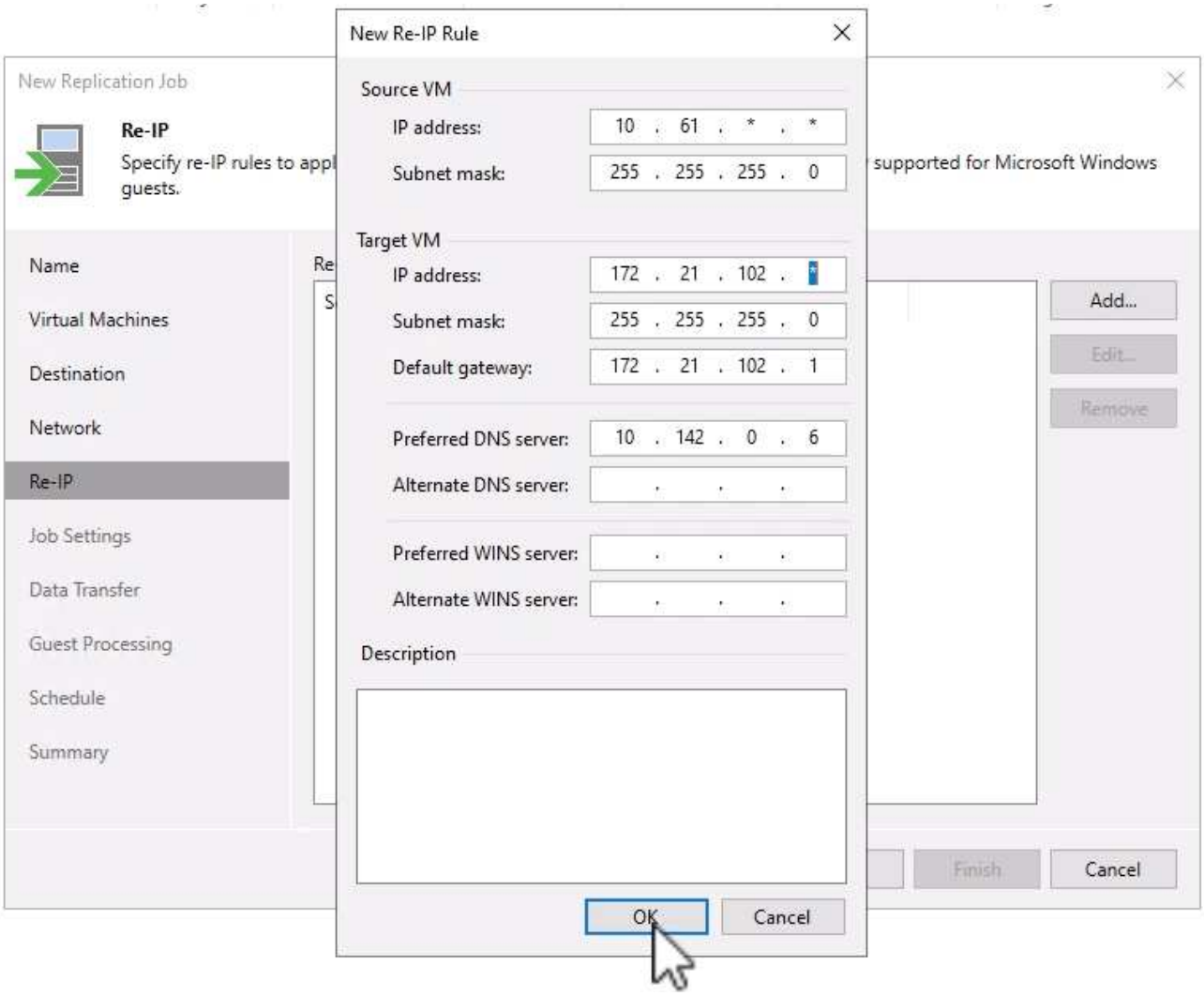
5. 在*目標*頁面上，選擇目標作為 GCVE SDDC 叢集/主機，並為 VM 副本選擇適當的資源池、VM 資料夾和NetApp Volumes 資料儲存。按一下“下一步”繼續。



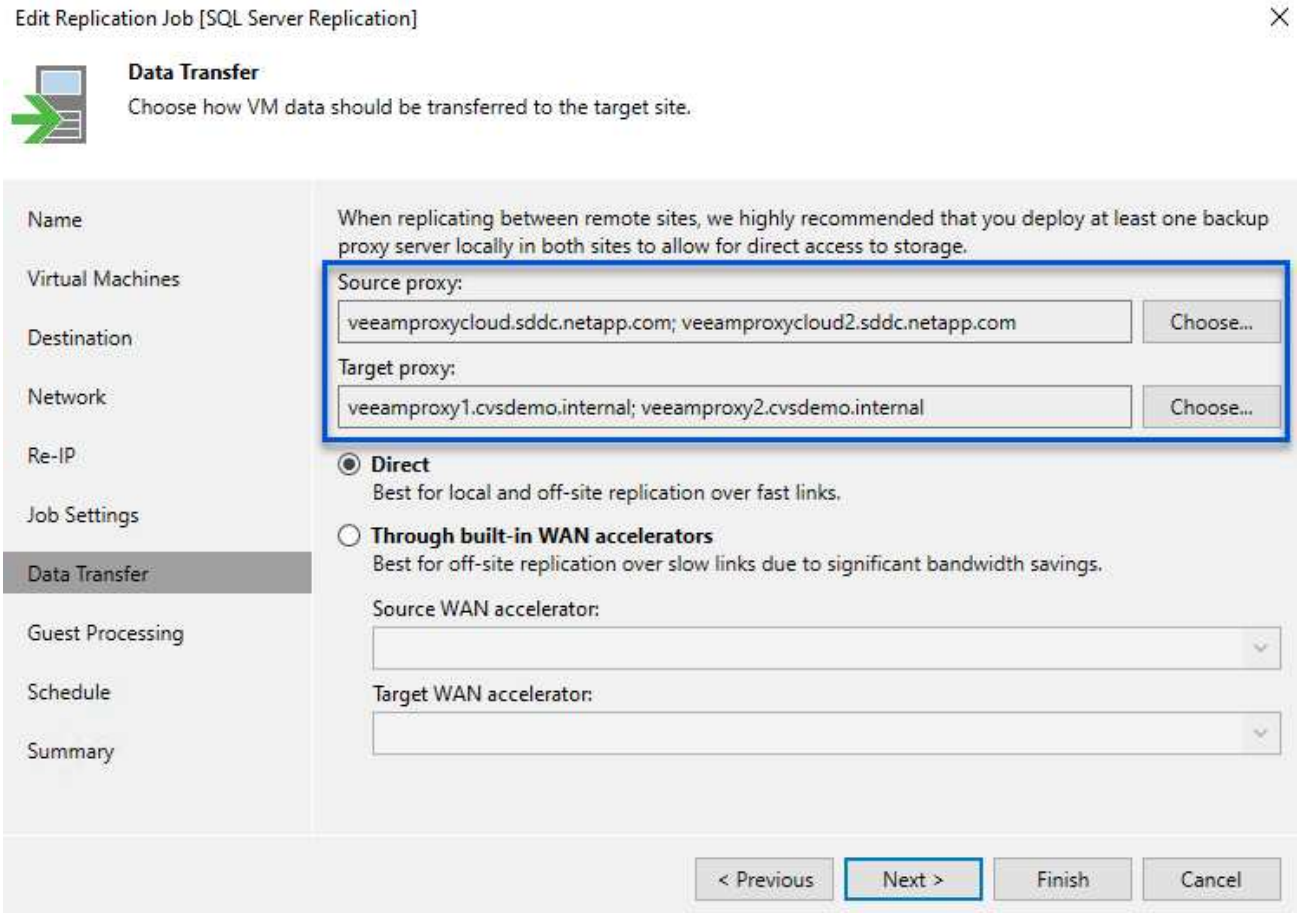
6. 在「網路」頁面上，根據需要建立來源虛擬網路和目標虛擬網路之間的對應。按一下“下一步”繼續。



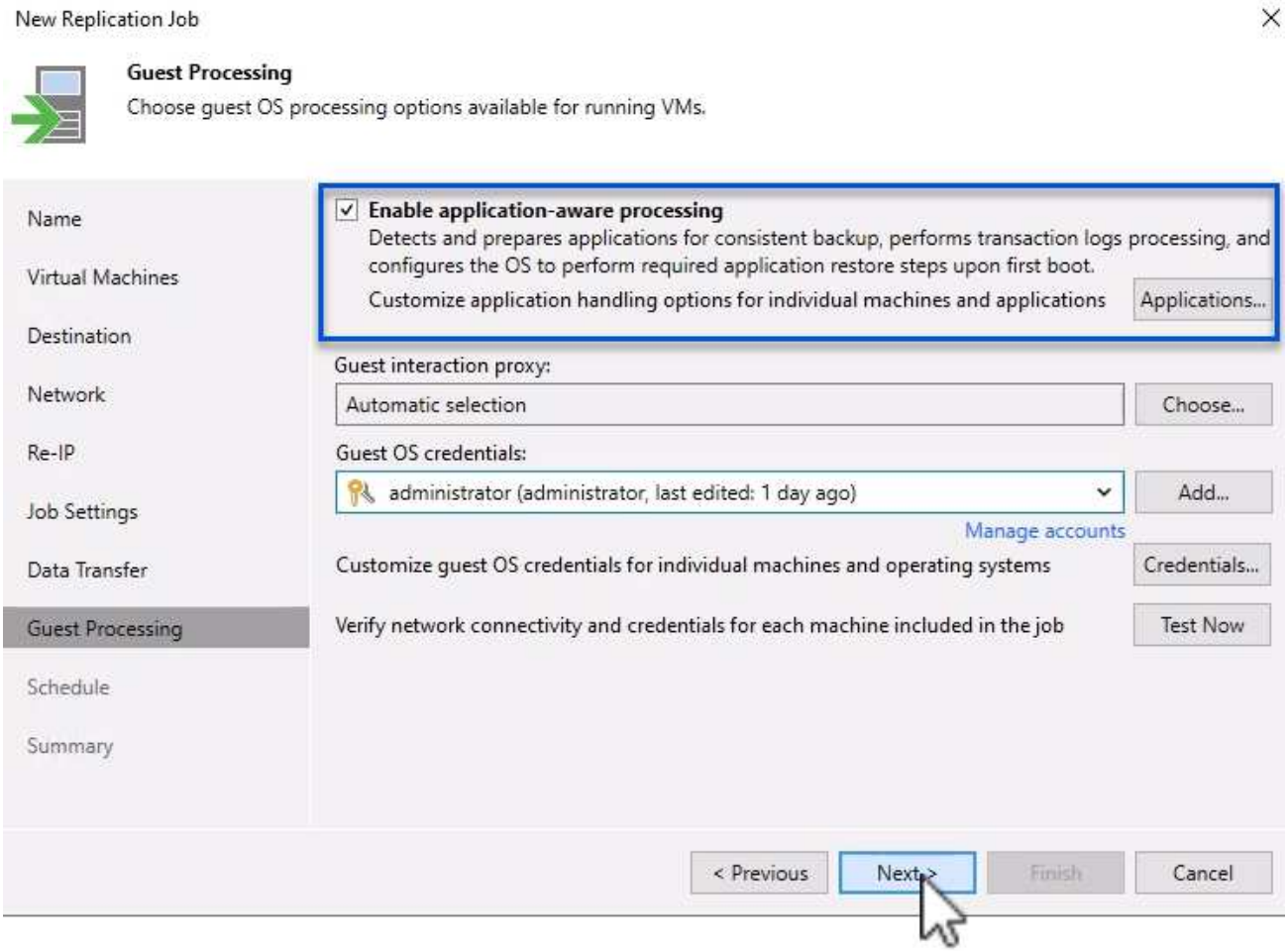
7. 在*Re-IP*頁面上，按一下*Add…按鈕新增新的**re-ip**規則。填寫來源和目標虛擬機器 **IP** 範圍以指定在故障轉移時將套用於來源虛擬機器的網路。使用星號來指定該八位元組的位址範圍。按一下“*下一步”繼續。



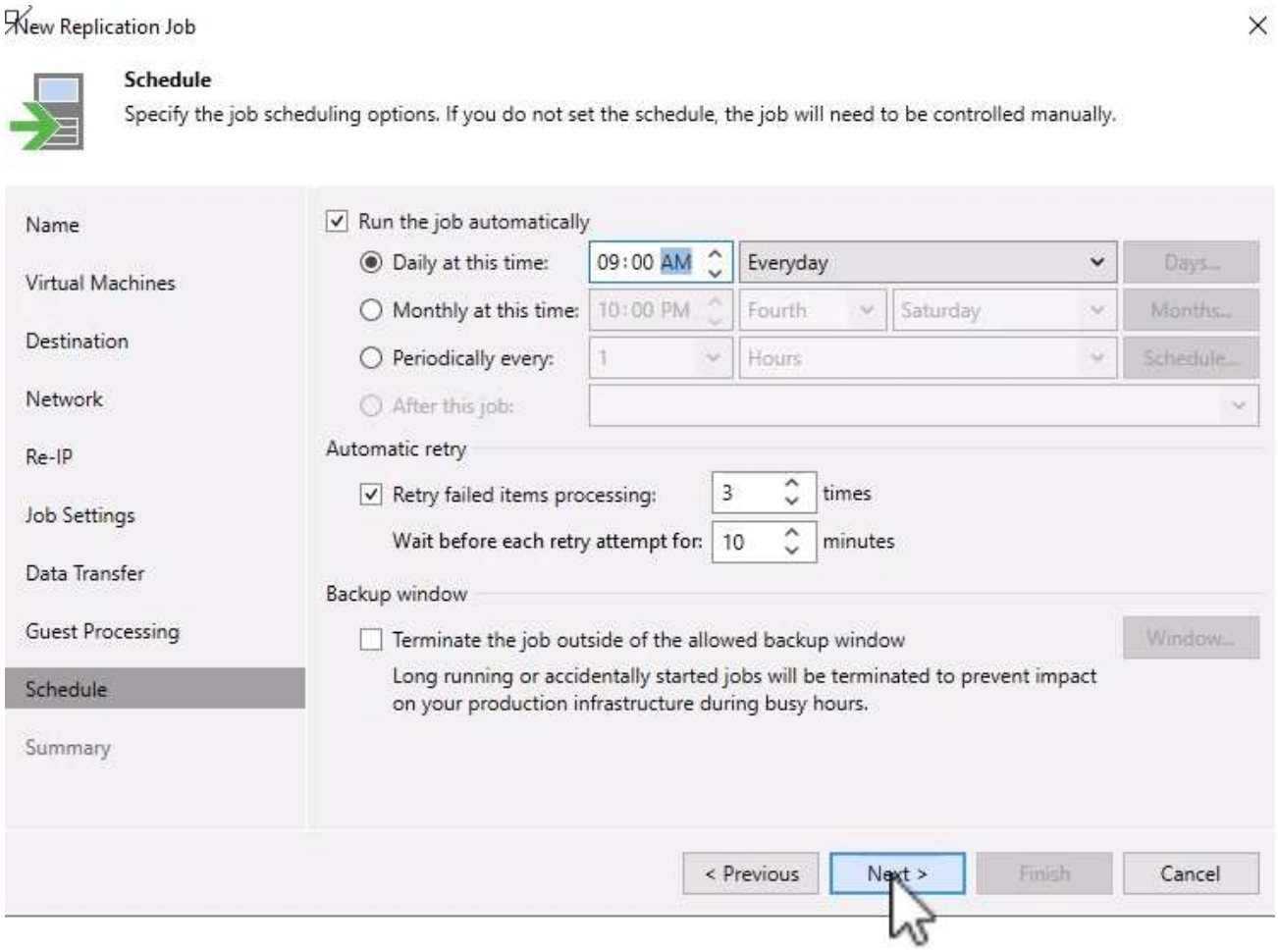
8. 在「作業設定」頁面上，指定將儲存 VM 副本元資料的備份儲存庫、保留策略，然後選擇底部的「進階...」按鈕以進行其他作業設定。按一下"下一步"繼續。
9. 在*資料傳輸*上，選擇位於來源網站和目標網站的代理伺服器，並保持選擇直接選項。如果配置了 WAN 加速器，也可以在這裡選擇。按一下"下一步"繼續。



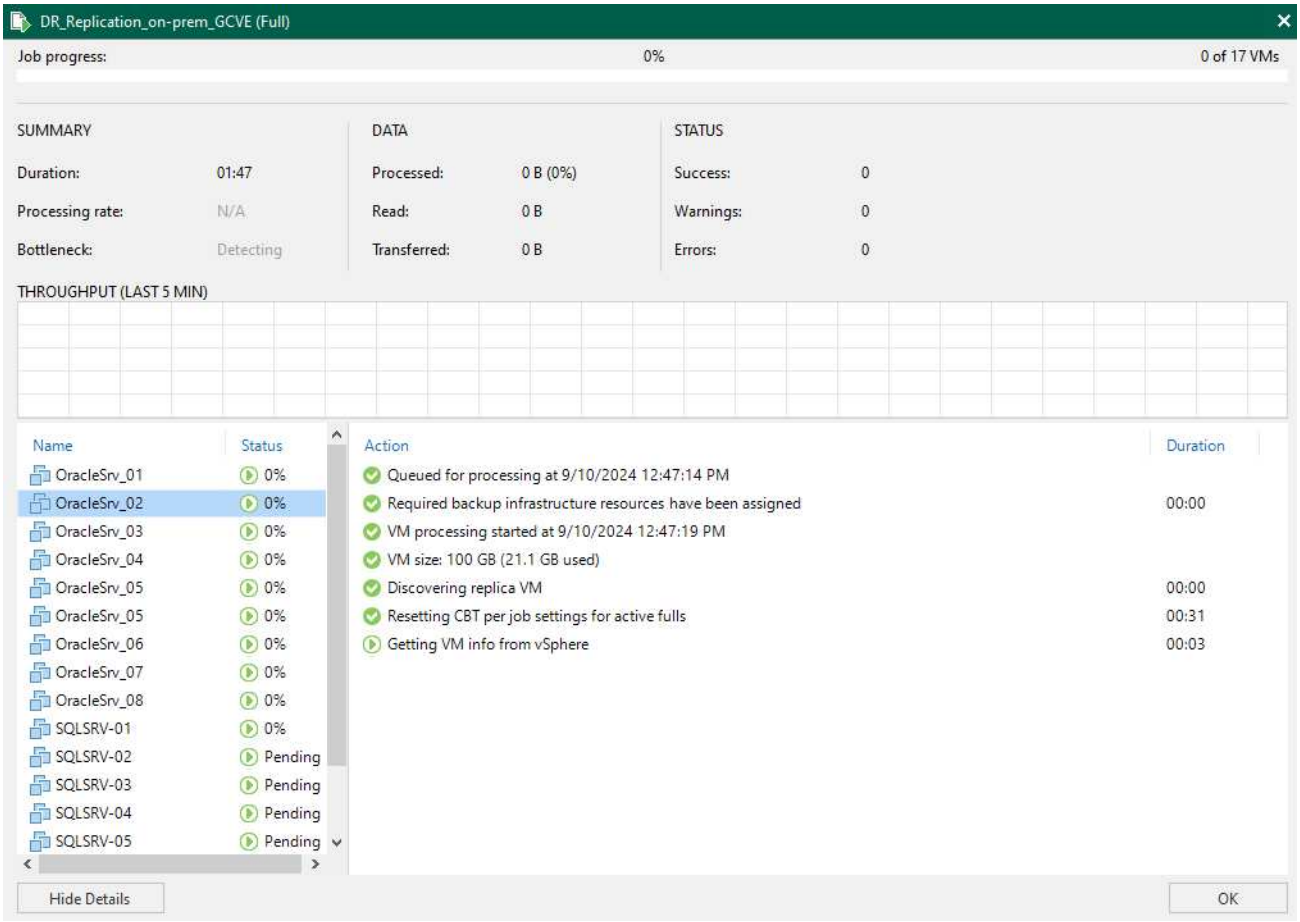
10. 在*Guest Processing*頁面上，根據需要選取*Enable application-aware processing*複選框，並選擇*Guest OS credentials*。按一下“下一步”繼續。



11. 在「計畫」頁面上，定義複製作業運作的時間和頻率。按一下“下一步”繼續。



12. 最後，在*摘要*頁面上檢查作業設定。勾選「按一下完成時執行該作業」複選框，然後按一下「完成」即可完成建立複製作業。
13. 一旦運行，就可以在作業狀態視窗中查看複製作業。



有關 Veeam 複製的更多信息，請參閱"複製的工作原理"

▼ 建立故障轉移計劃

初始複製或播種完成後，建立故障轉移計劃。故障轉移計畫有助於自動對從屬虛擬機器逐一或按群組執行故障轉移。故障轉移計劃是虛擬機器處理順序（包括啟動延遲）的藍圖。故障轉移計劃還有助於確保關鍵依賴的虛擬機器已經在運作。

完成初始複製或播種後，建立故障轉移計劃。該計劃可作為協調依賴虛擬機器（單獨或作為一個群組）故障轉移的策略藍圖。它定義了虛擬機器的處理順序，包含了必要的啟動延遲，並確保關鍵的依賴虛擬機器在其他虛擬機器之前運行。透過實施結構良好的故障轉移計劃，組織可以簡化其災難復原流程，最大限度地減少停機時間並在故障轉移事件期間維護相互依賴系統的完整性。

建立計劃時，Veeam Backup & Replication 會自動識別並使用最新的還原點來啟動 VM 副本。

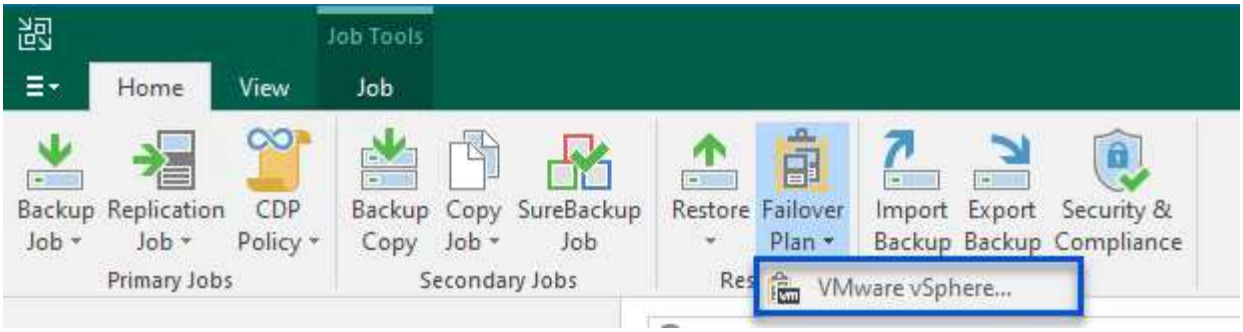
僅當初始複製完成且 VM 副本處於就緒狀態時，才能建立故障轉移計劃。

執行故障轉移計畫時可同時啟動的最大虛擬機器數量為 10 個。

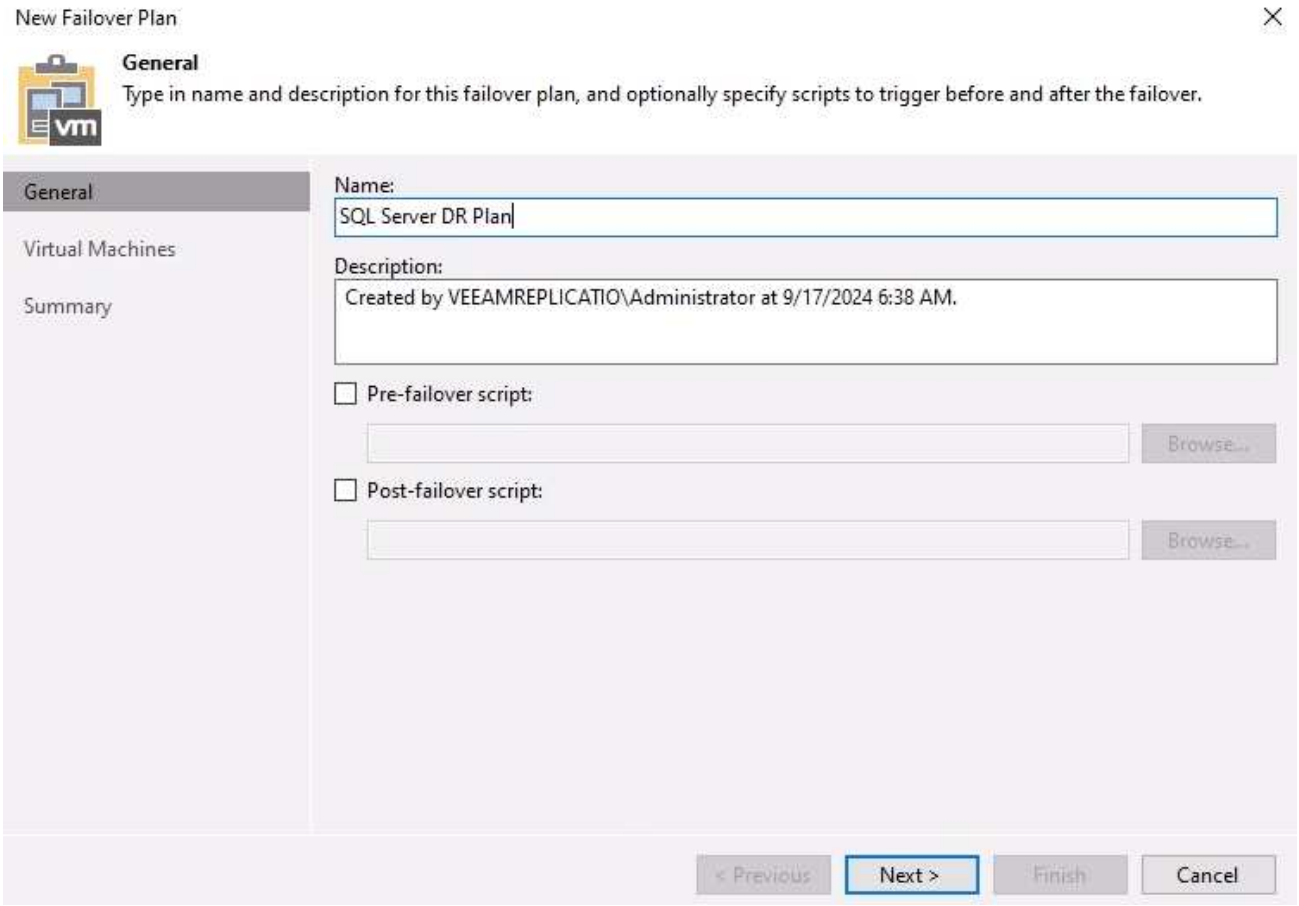
在故障轉移過程中，來源虛擬機器不會關閉。

若要建立*故障轉移計劃*，請完成以下步驟：

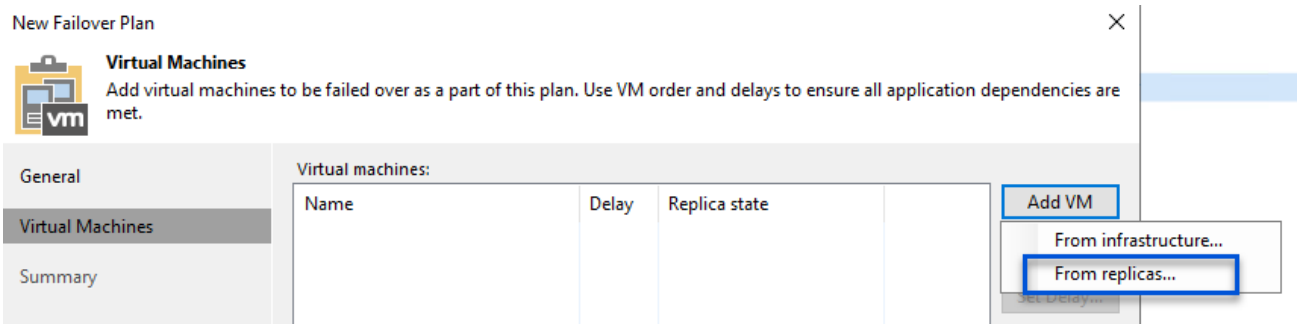
1. 在*主頁*視圖上，按一下*恢復*部分中的*故障轉移計劃*按鈕。在下拉式選單中，選擇 **VMware vSphere...**

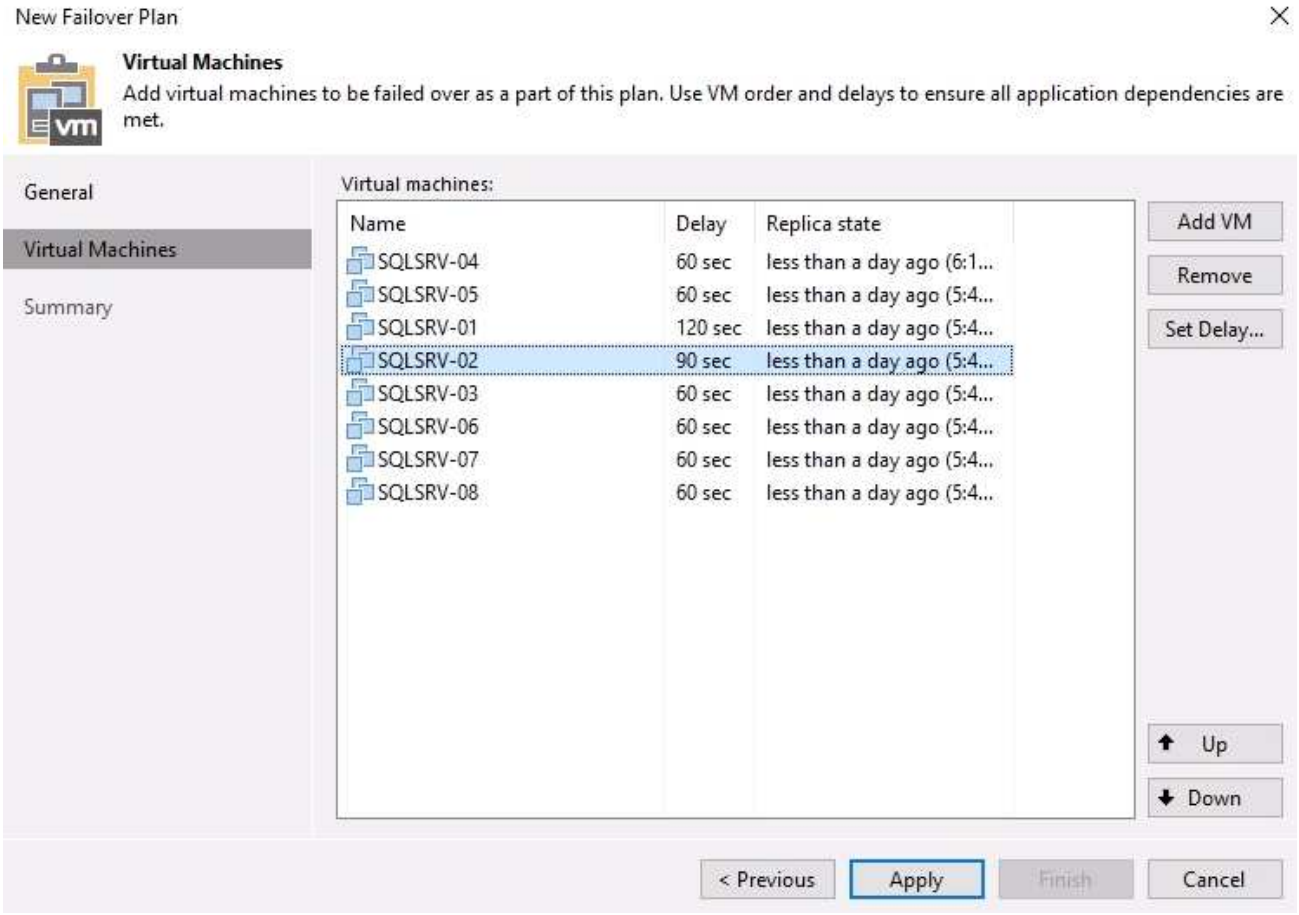


2. 在「新故障轉移計畫」精靈的「常規」頁面上，提供計畫的名稱和說明。可根據需要新增故障轉移前和故障轉移後腳本。例如，在啟動複製的虛擬機器之前執行腳本來關閉虛擬機器。



3. 在“虛擬機器”頁面上，按一下“新增虛擬機器”按鈕並選擇“從副本…”。選擇作為故障轉移計畫一部分的虛擬機，然後修改虛擬機啟動順序和任何所需的啟動延遲以滿足應用程式依賴關係。





點選“應用”繼續。

4. 最後檢查所有故障轉移計劃設置，然後按一下「完成」以建立故障轉移計劃。

有關建立複製作業的其他信息，請參閱"建立複製作業"。

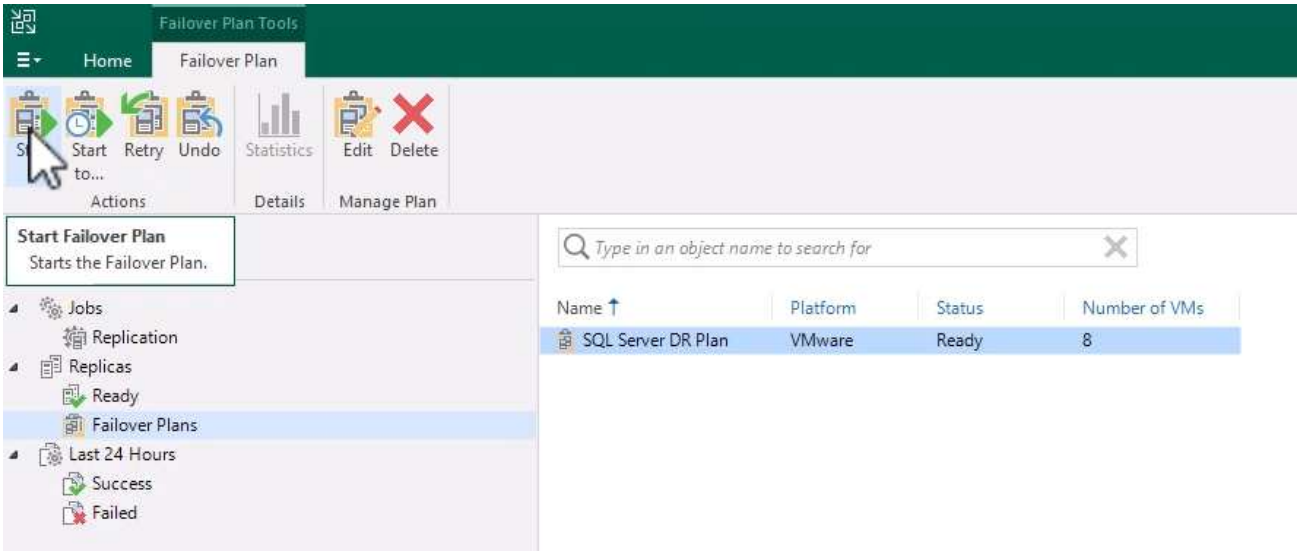
▼ 運行故障轉移計劃

在故障轉移期間，生產站點中的來源虛擬機器將切換到災難復原站點上的副本。作為該過程的一部分，Veeam Backup & Replication 將 VM 副本還原到所需的復原點，並將所有 I/O 活動從來源 VM 傳輸到其副本。複製品不僅可用於實際災難，還可用於模擬災難復原演習。在故障轉移模擬中，來源虛擬機器繼續運作。完成必要的測試後，可以撤銷故障轉移，恢復正常操作。

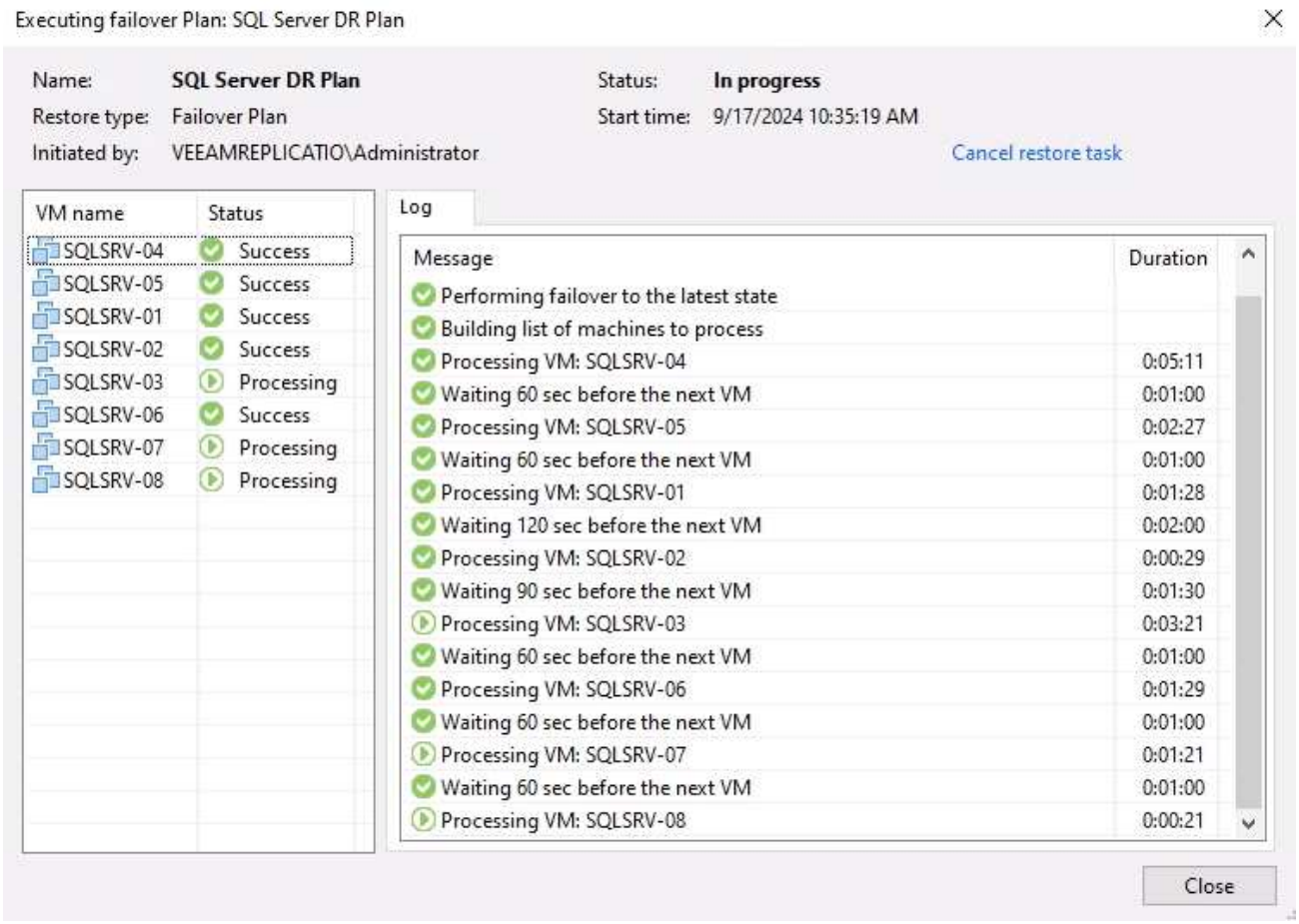
確保網路分段到位，以避免故障轉移期間發生 IP 衝突。

完成以下步驟以啟動故障轉移計畫：

1. 首先，在*主頁*視圖中，按一下左側功能表中的*副本 > 故障轉移計劃*，然後按一下*開始*按鈕。或者，可以使用「開始到...」按鈕將故障轉移到先前的還原點。



2. 在*執行故障轉移計劃*視窗中監控故障轉移的進度。



Veeam Backup & Replication 停止來源 VM 的所有複製活動，直到其副本返回就緒狀態。

有關故障轉移計劃的詳細信息，請參閱"故障轉移計劃"。

▼ 故障恢復到生產站點

進行故障轉移被視為中間步驟，需要根據要求最終確定。選項包括以下內容：

- 故障恢復到生產 - 恢復到原始虛擬機器並將副本活動期間所做的所有修改同步回來源虛擬機器。

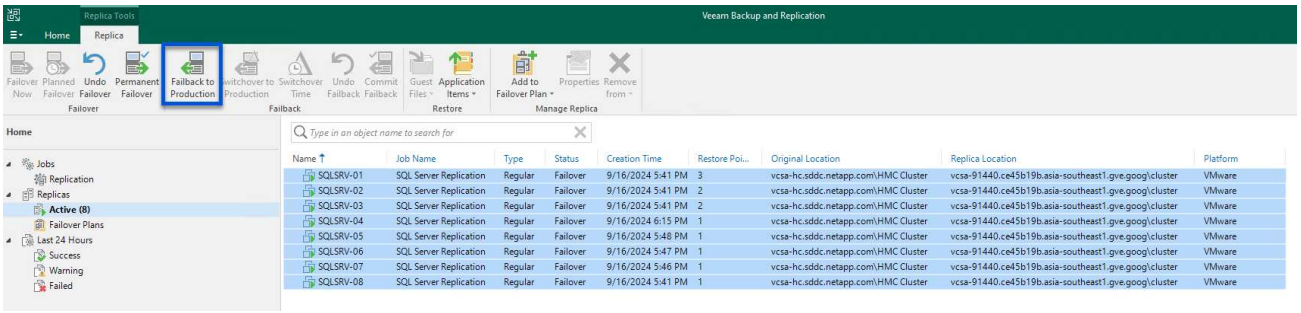
在故障復原期間，變更會被傳輸但不會立即套用。驗證原始虛擬機器的功能後，選擇「提交故障復原」。或者，如果原始虛擬機器表現出意外行為，請選擇「撤銷故障回應」以還原至虛擬機器副本。

- 撤銷故障轉移 - 恢復到原始 VM，丟棄在運行期間對 VM 副本所做的所有變更。
- 永久故障轉移 - 從原始虛擬機器永久切換到其副本，並將副本建立為正在進行的操作的新主虛擬機器。

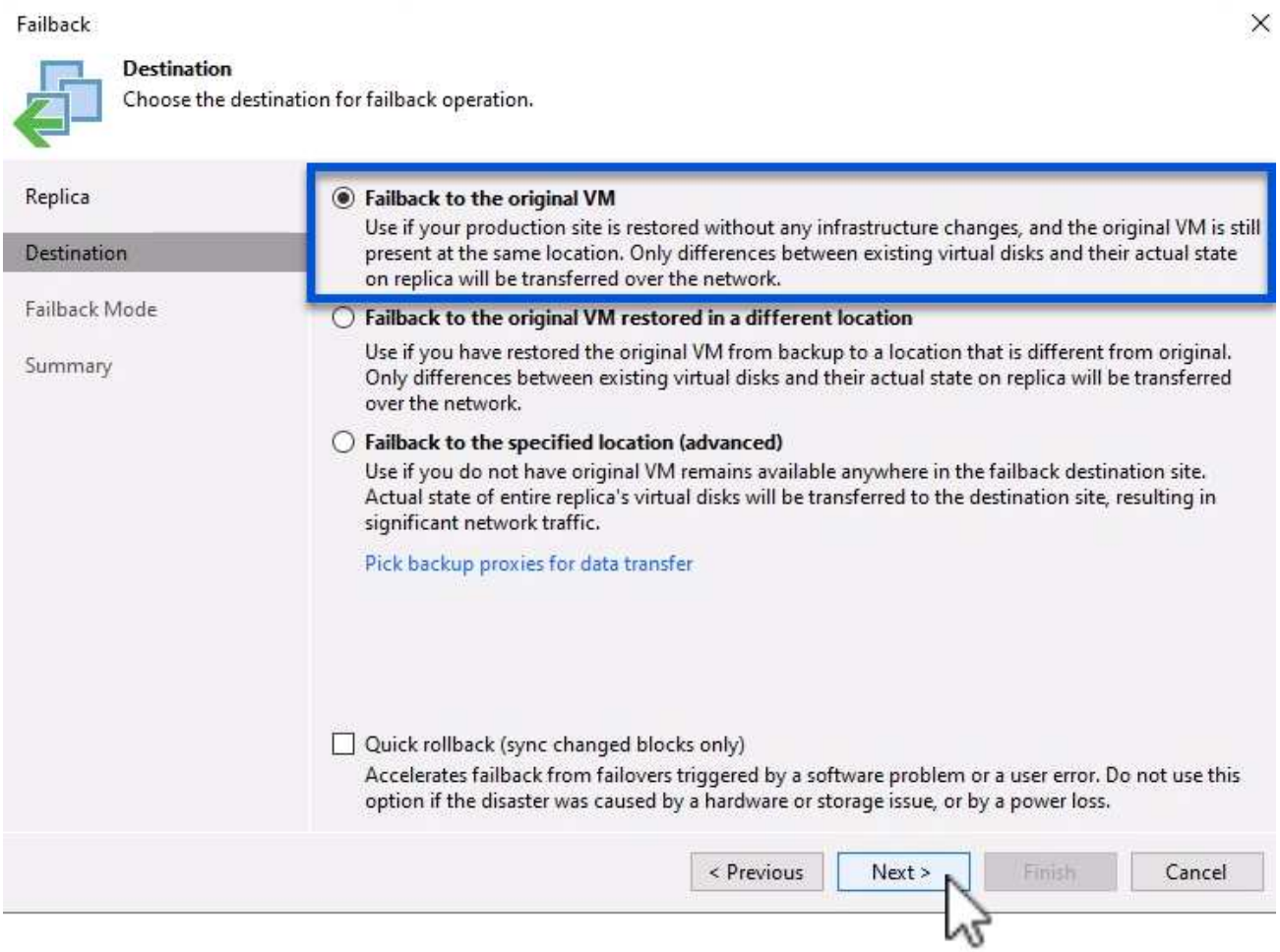
在這種情況下，選擇了“故障恢復到生產”選項。

完成以下步驟以故障還原為生產站點：

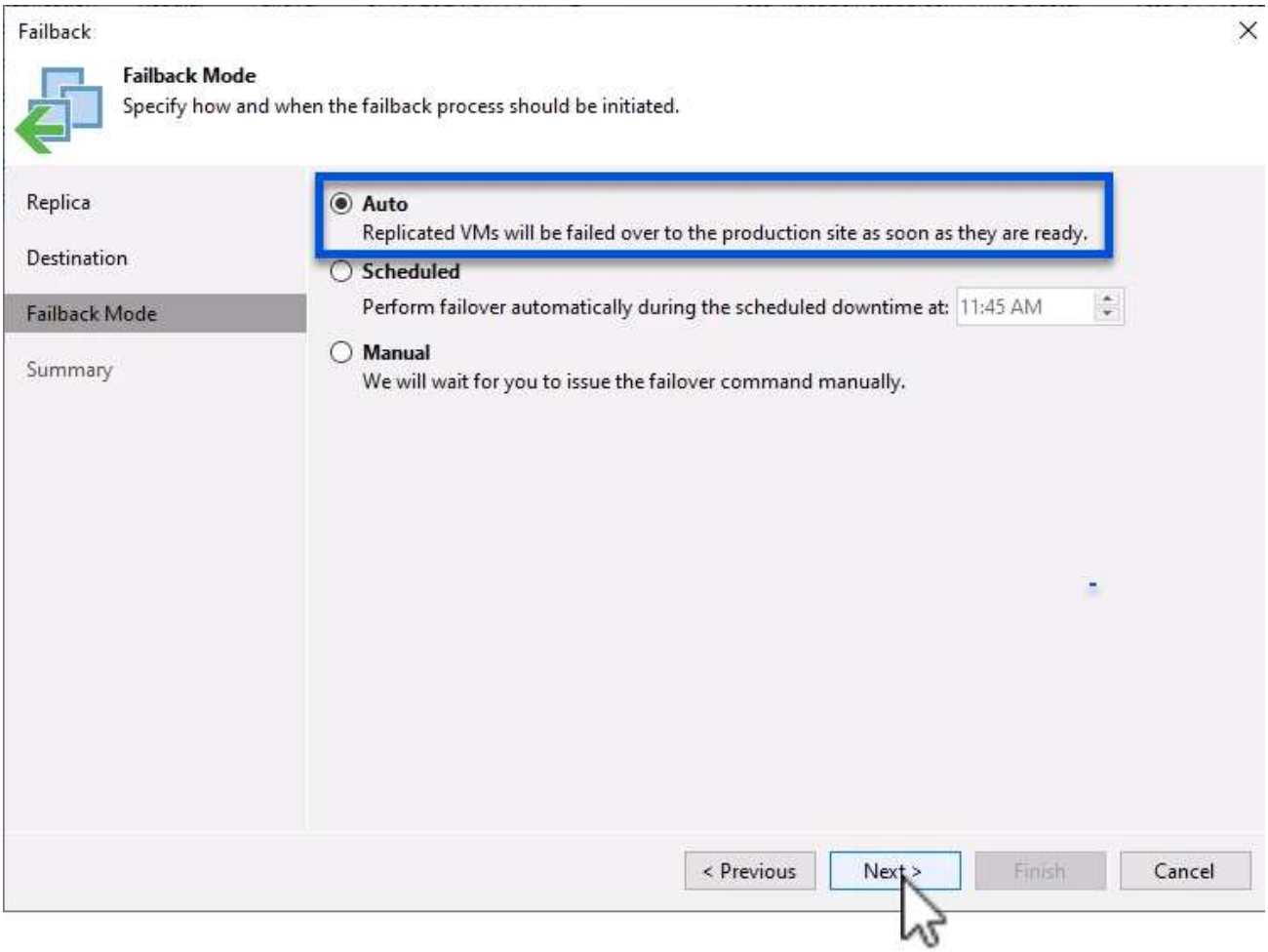
1. 從*主頁*視圖中，按一下左側選單中的*副本>活動*。選擇要包含的虛擬機，然後點擊頂部選單中的「故障恢復到生產」按鈕。



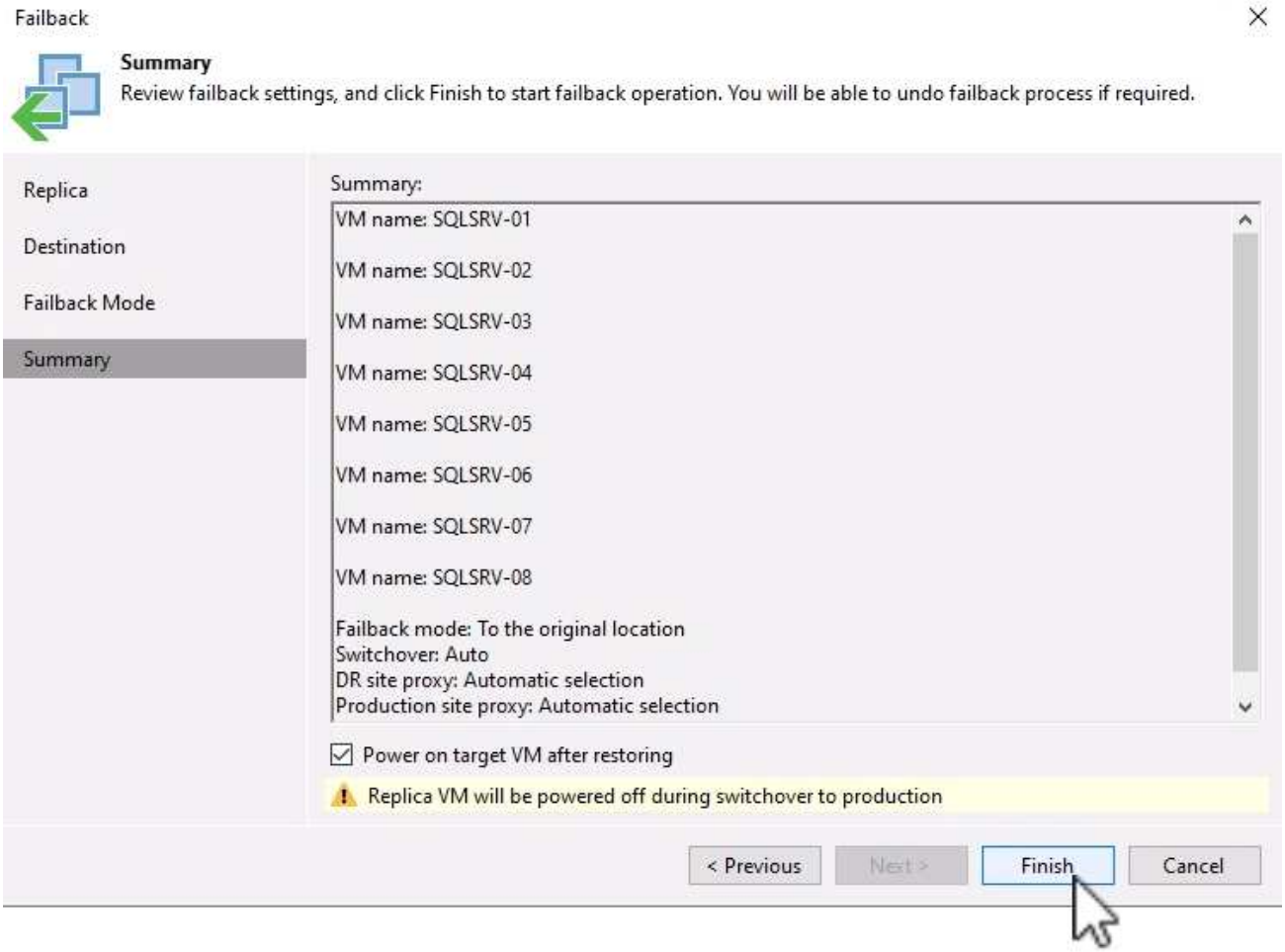
2. 在「故障回覆」精靈的「副本」頁面上，選擇要包含在故障回復作業中的副本。
3. 在*目標*頁面上，選擇*故障還原到原始虛擬機器*，然後按一下*下一步*繼續。



4. 在「故障復原模式」頁面上，選擇「自動」以盡快啟動故障復原。

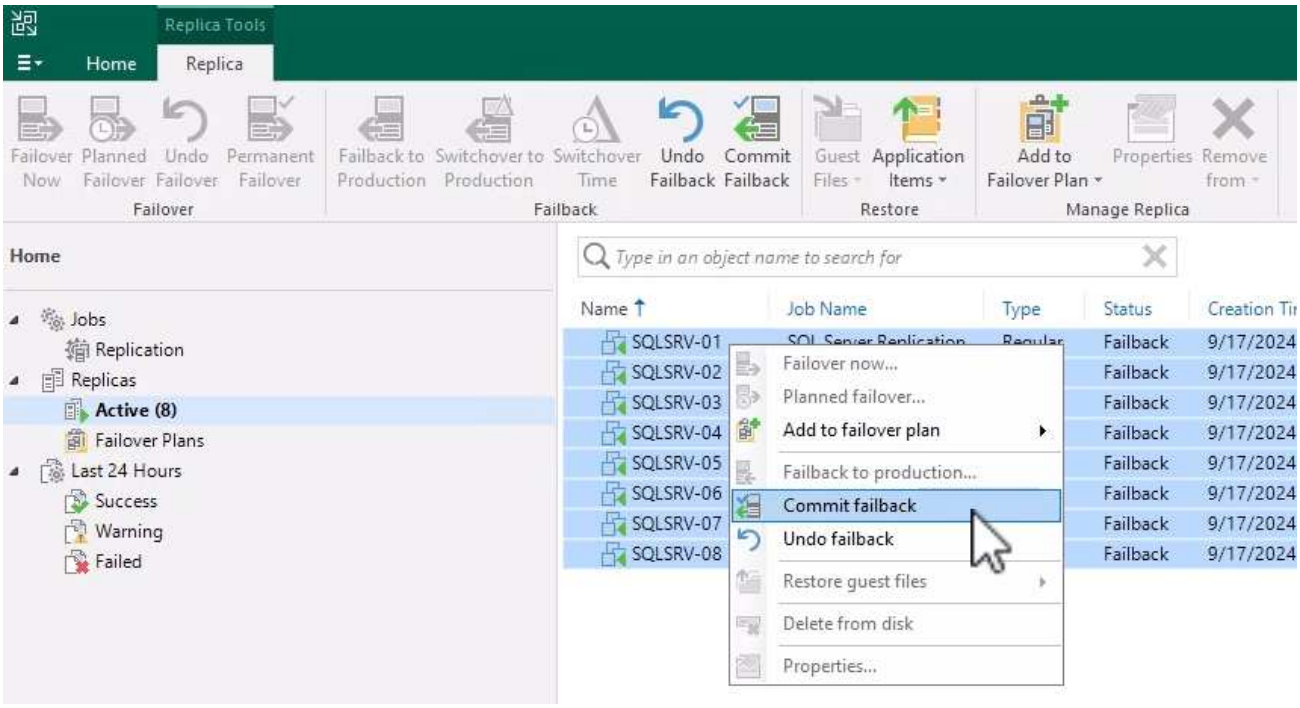


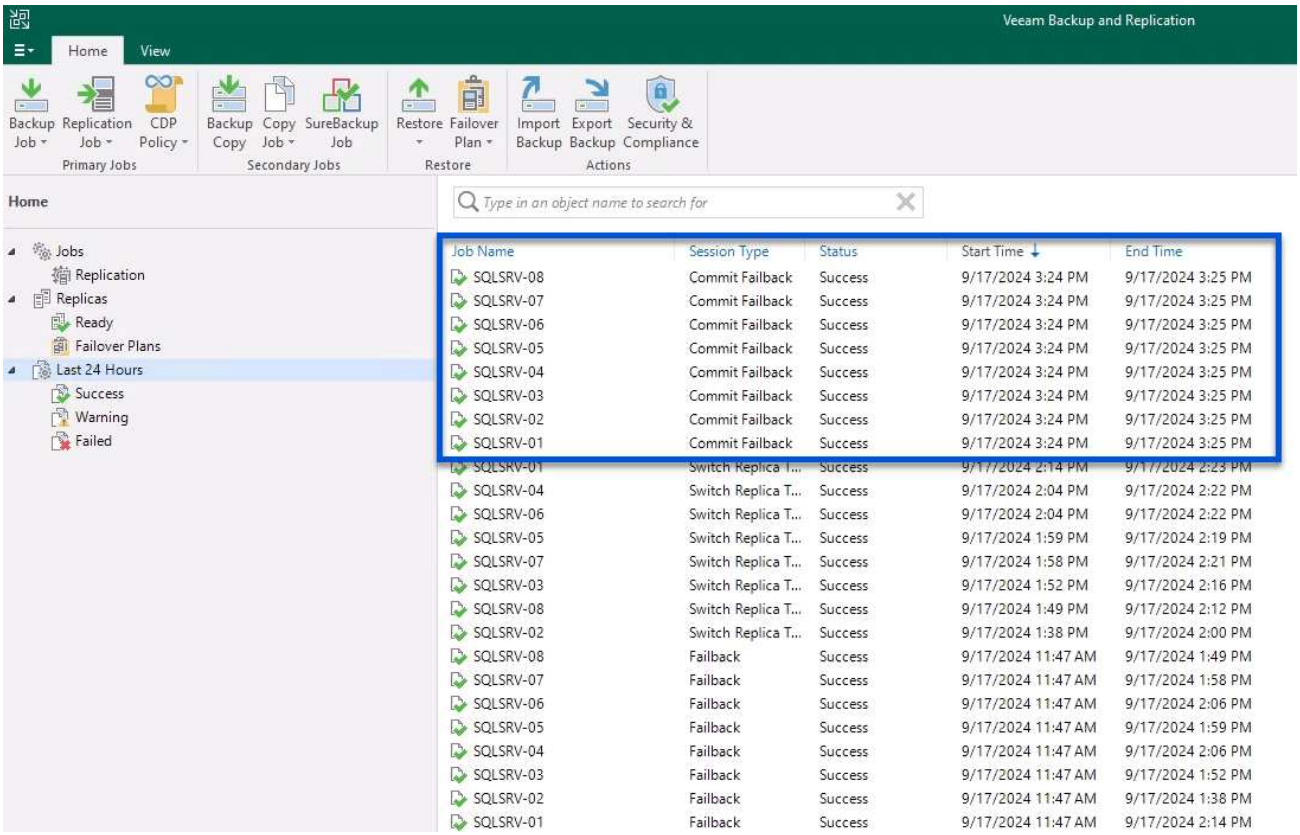
5. 在“摘要”頁面上，選擇是否“恢復後啟動目標虛擬機器”，然後按一下“完成”以啟動故障復原作業。



故障回復提交完成故障回復操作，確認變更已成功整合至生產虛擬機器。提交後，Veeam Backup & Replication 將恢復已復原的生產虛擬機器的常規複製活動。這會將恢復的副本的狀態從_故障回復_更改為_就緒_。

1. 若要提交故障回復，請導航至 **Replicas > Active**，選擇要提交的虛擬機，右鍵單擊並選擇 **Commit failback**。





故障恢復到生產環境成功後，所有虛擬機器都將恢復到原始生產站點。

有關故障恢復過程的詳細信息，請參閱 Veeam 文檔"複製的故障轉移和故障恢復"。

結論

Google Cloud NetApp Volumes資料儲存功能可讓 Veeam 和其他經過驗證的第三方工具提供經濟高效的災難復原 (DR) 解決方案。透過利用 Pilot Light 集群而不是用於 VM 副本的大型專用集群，組織可以顯著降低開支。這種方法可以實現客製化的 DR 策略，利用現有的內部備份解決方案進行基於雲端的災難恢復，從而無需額外的內部資料中心。如果發生災難，只需按一下即可啟動故障轉移或配置為自動發生故障轉移，從而確保業務連續性並將停機時間降至最低。

要了解有關此過程的更多信息，請隨意觀看詳細的演示視頻。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

遷移 GCP/GCVE 上的工作負載

使用 **VMware HCX** 將工作負載遷移到**Google Cloud NetApp Volumes**資料儲存區 **-** 快速入門指南

Google Cloud VMware Engine 和 Cloud Volume Service 資料儲存最常見的用例之一是遷移 VMware 工作負載。 VMware HCX 是首選方案，它提供了各種遷移機制，可將本機虛擬機器 (VM) 及其資料移至 Cloud Volume Service NFS 資料儲存。

概述：使用 **VMware HCX**、 **Google Cloud NetApp Volumes**資料儲存區和 **Google Cloud VMware Engine (GCVE)** 遷移虛擬機

VMware HCX 主要是一個遷移平台，旨在簡化應用程式遷移、工作負載重新平衡甚至跨雲端的業務連續性。它是 Google Cloud VMware Engine Private Cloud 的一部分，提供了多種遷移工作負載的方法，並可用於災難復原 (DR) 作業。

本文檔提供了配置 Cloud Volume Service 資料儲存區的逐步指導，隨後下載、部署和配置 VMware HCX，包括其在本地和 Google Cloud VMware Engine 端的所有主要元件（包括互連、網路擴展和 WAN 最佳化），以支援各種 VM 遷移機制。

> VMware HCX 適用於任何資料儲存類型，因為遷移是在 VM 層級進行的。因此，本文檔適用於現有NetApp客戶和計畫使用 Google Cloud VMware Engine 部署 Cloud Volume Service 以實現經濟高效的 VMware 雲端部署的非NetApp客戶。

▼ 摘要步驟

此清單提供了將虛擬機器從本機 HCX Connector 配對並遷移到 Google Cloud VMware Engine 端的 HCX Cloud Manager 所需的進階步驟：

1. 透過 Google VMware Engine 入口網站準備 HCX。
2. 在本機 VMware vCenter Server 中下載並部署 HCX Connector Open Virtualization Appliance (OVA) 安裝程式。
3. 使用許可證金鑰啟動 HCX。
4. 將本機 VMware HCX Connector 與 Google Cloud VMware Engine HCX Cloud Manager 配對。
5. 設定網路設定檔、計算設定檔和服務網格。
6. （可選）執行網路擴展以避免在遷移期間重新分配 IP。
7. 驗證設備狀態並確保可以遷移。
8. 遷移虛擬機器工作負載。

▼ 先決條件

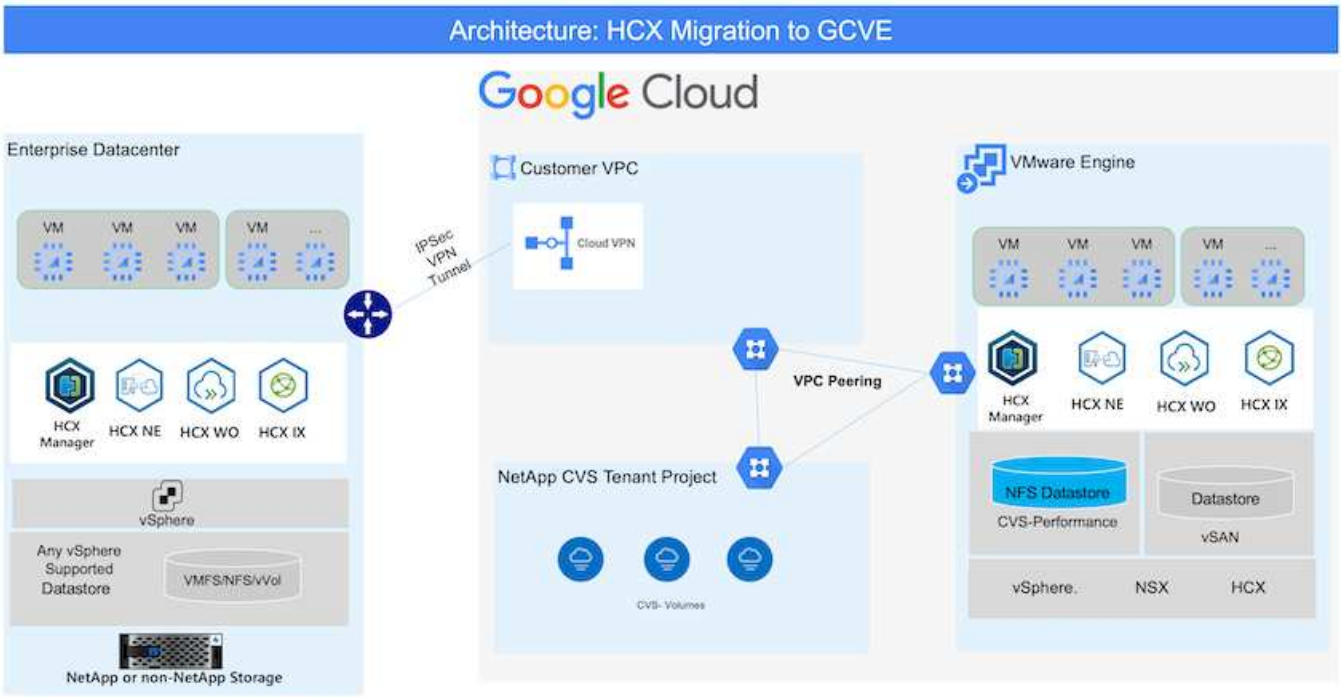
在開始之前，請確保滿足以下先決條件。有關詳細信息，請參閱 "關聯"。滿足連線等先決條件後，從 Google Cloud VMware Engine 入口網站下載 HCX 授權金鑰。下載 OVA 安裝程式後，請依照如下所述進行安裝程序。

> HCX 高級版是預設選項，VMware HCX 企業版也可透過支援票獲得，且無需額外付費即可獲得支援。參考 "此連結"

- 使用現有的 Google Cloud VMware Engine 軟體定義資料中心 (SDDC) 或使用此"NetApp連結"或者這個"Google連結"。
- 從支援 VMware vSphere 的內部部署資料中心遷移虛擬機器和相關資料需要從資料中心到 SDDC 環境的網路連線。在遷移工作負載之前， "設定 Cloud VPN 或 Cloud Interconnect 連接"在本地環境和對應的私有雲之間。
- 從本機 VMware vCenter Server 環境到 Google Cloud VMware Engine 私有雲的網路路徑必須支援使用 vMotion 遷移虛擬機器。
- 確保所需的 "防火牆規則和連接埠"允許在本機 vCenter Server 和 SDDC vCenter 之間進行 vMotion 流量。
- Cloud Volume Service NFS 磁碟區應作為資料儲存安裝在 Google Cloud VMware Engine 中。請按照本文中詳細說明的步驟操作 "關聯"將 Cloud Volume Service 資料儲存附加到 Google Cloud VMware Engines 主機。

▼ 進階架構

為了測試目的，用於此驗證的本地實驗室環境透過 Cloud VPN 連接，這允許本地連接到 Google Cloud VPC。



有關將 VMware HCX 與 Google 結合使用的更多詳細信息，請參閱 "VMware 連結"

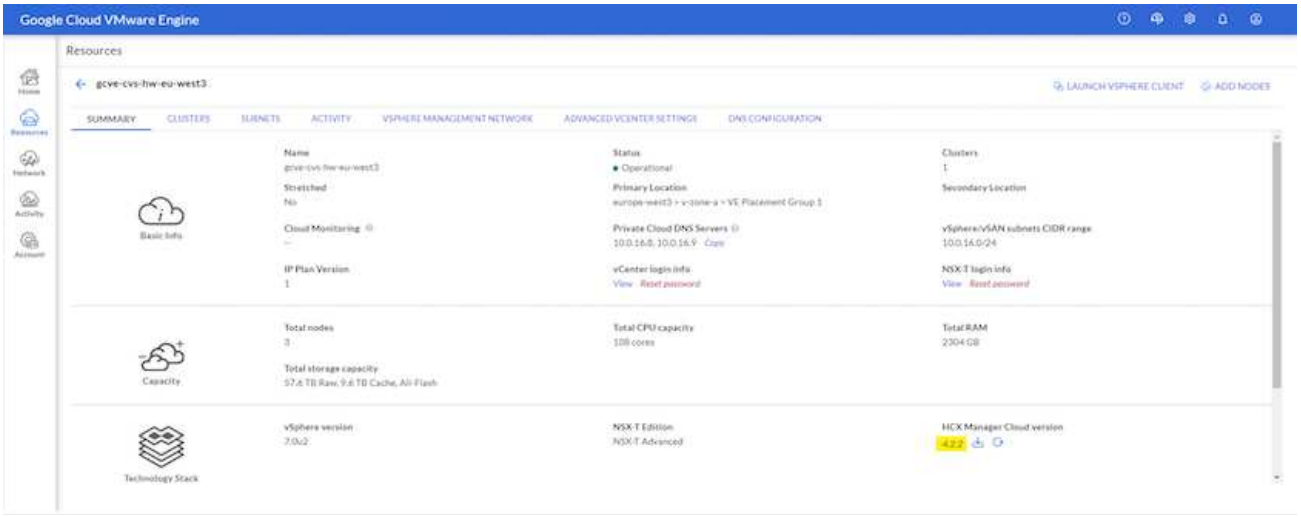
請按照一系列步驟完成此解決方案的部署：

▼ 步驟 **1**：透過 **Google VMware Engine** 入口網站準備 **HCX**

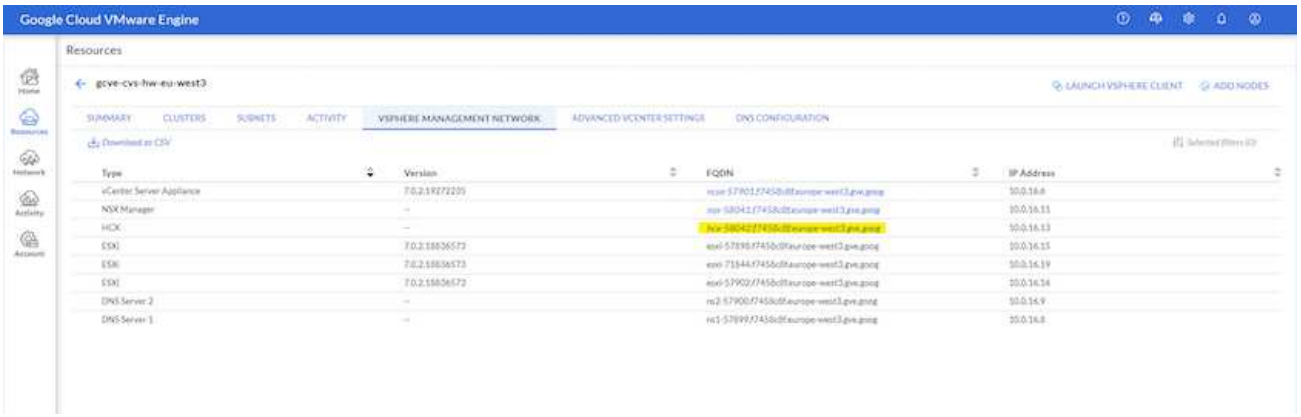
當您使用 VMware Engine 設定私有雲時，HCX Cloud Manager 元件會自動安裝。若要準備網站配對，請完成以下步驟：

1. 登入 Google VMware Engine 入口網站並登入 HCX Cloud Manager。

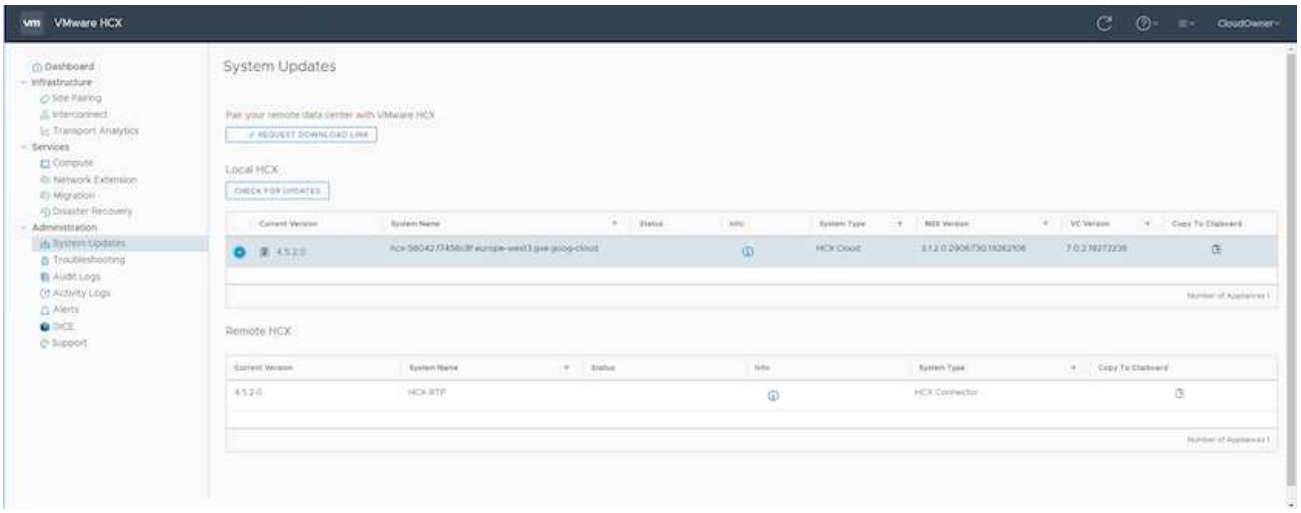
   您可以透過點擊 HCX 版本連結登入 HCX 控制台



   或點選 vSphere 管理網路標籤下的 HCX FQDN。



2. 在 HCX 雲端管理器中，前往「管理」>「系統更新」。
3. 點擊*請求下載連結*並下載 OVA 檔案。



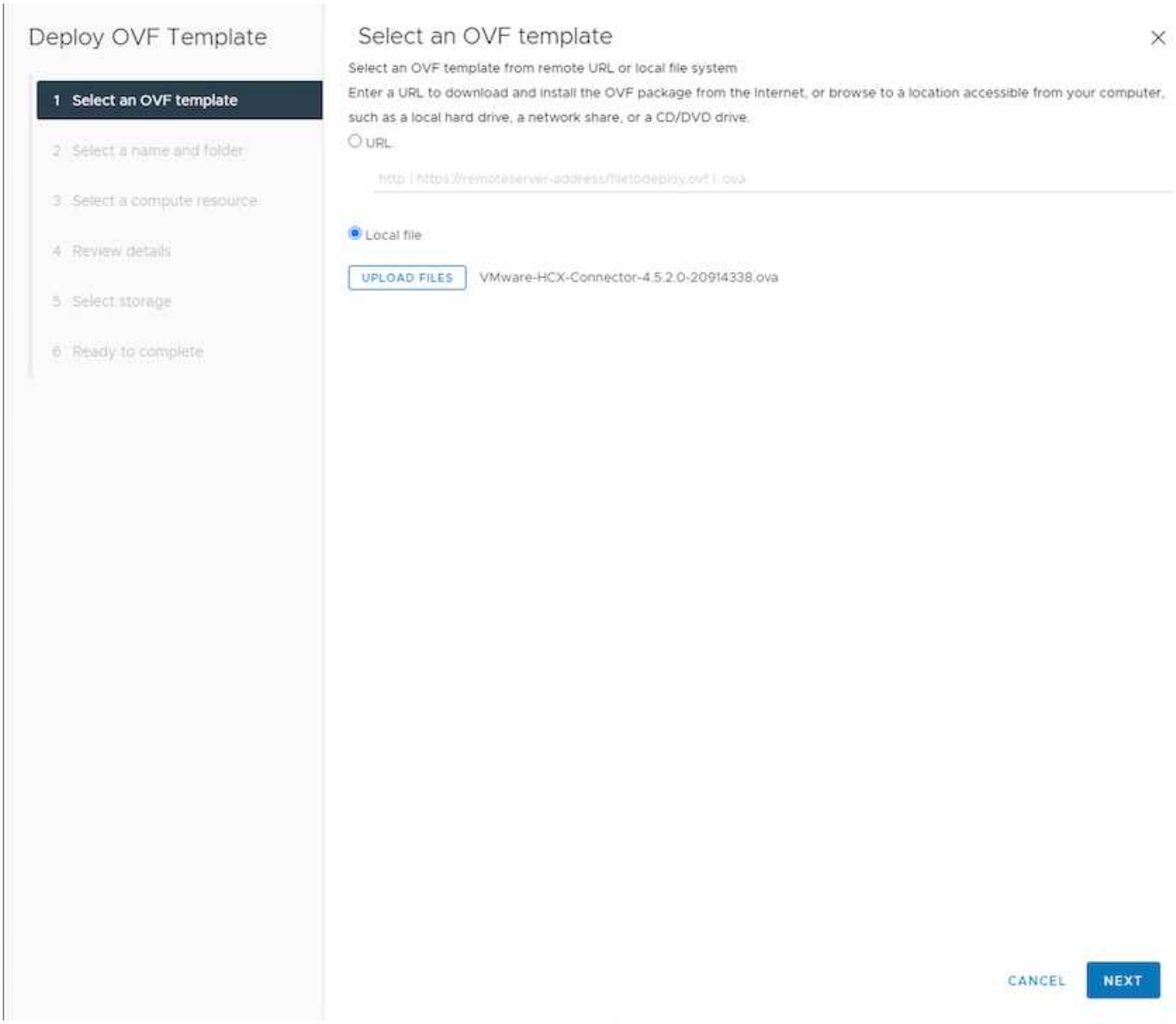
4. 將 HCX Cloud Manager 更新至 HCX Cloud Manager UI 提供的最新版本。

▼ 步驟 **2**：在本機 **vCenter Server** 中部署安裝程式 **OVA**

若要將本機連接器連接至 Google Cloud VMware Engine 中的 HCX 管理器，請確保在本機環境中開啟了對應的防火牆連接埠。

若要在本機 vCenter Server 中下載並安裝 HCX Connector，請完成下列步驟：

1. 按照上一步所述，從 Google Cloud VMware Engine 上的 HCX 控制台下載 ova。
2. 下載 OVA 後，使用 部署 **OVF** 範本 選項將其部署到本機 VMware vSphere 環境。



3. 輸入 OVA 部署所需的所有信息，按一下“下一步”，然後按一下“完成”以部署 VMware HCX 連接器 OVA。

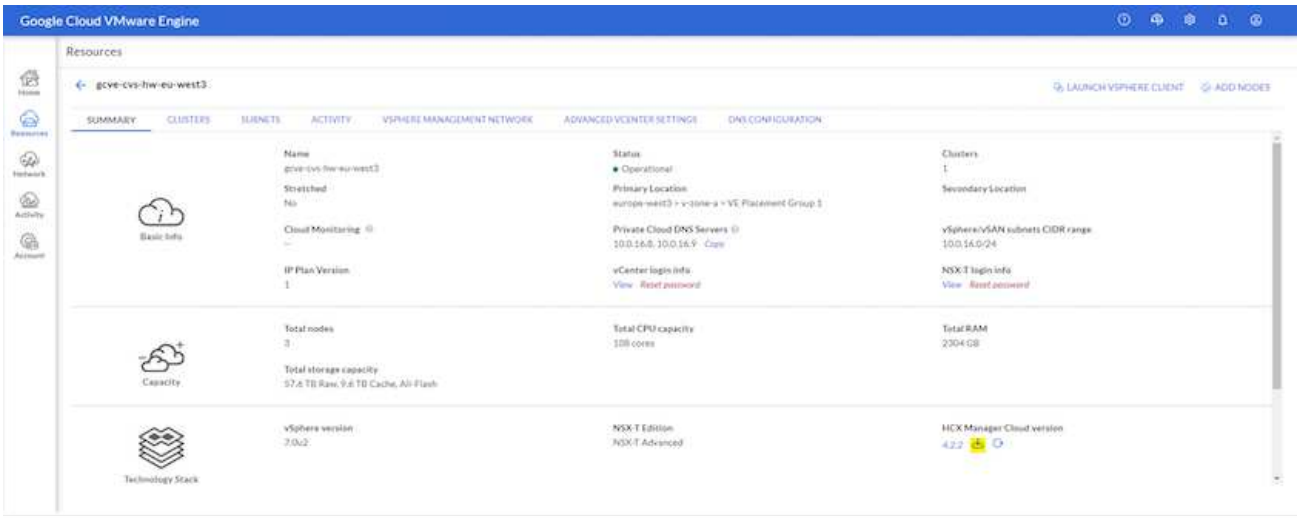
   手動啟動虛擬設備。

有關逐步說明，請參閱 "Google HCX 文件"。

▼ 步驟 **3**：使用許可證金鑰啟動 **HCX Connector**

在本機部署 VMware HCX Connector OVA 並啟動裝置後，請完成以下步驟以啟動 HCX Connector。從 Google Cloud VMware Engine 入口網站產生許可證金鑰並在 VMware HCX Manager 中啟動它。

1. 在 VMware Engine 入口網站中，按一下“資源”，選擇私有雲，然後*按一下“HCX Manager 雲端版本”下的下載圖示*
   。



開啟下載的檔案並複製許可證金鑰字串。

2. 登入本機 VMware HCX 管理器 `"https://hcxmanagerIP:9443"`使用管理員憑證。

   使用 OVA 部署期間定義的 hcxmanagerIP 和密碼。

3. 在許可中，輸入從步驟 3 複製的金鑰，然後按一下 啟動。

   本地 HCX 連接器應該具有網路存取權限。

4. 在「資料中心位置」下，提供在本機安裝 VMware HCX 管理器的最近位置。按一下“繼續”。
5. 在“系統名稱”下，更新名稱並按一下“繼續”。
6. 點擊“是，繼續”。
7. 在「連接您的 vCenter」下，提供 vCenter Server 的完全限定網域名稱 (FQDN) 或 IP 位址以及對應的憑證，然後按一下「繼續」。

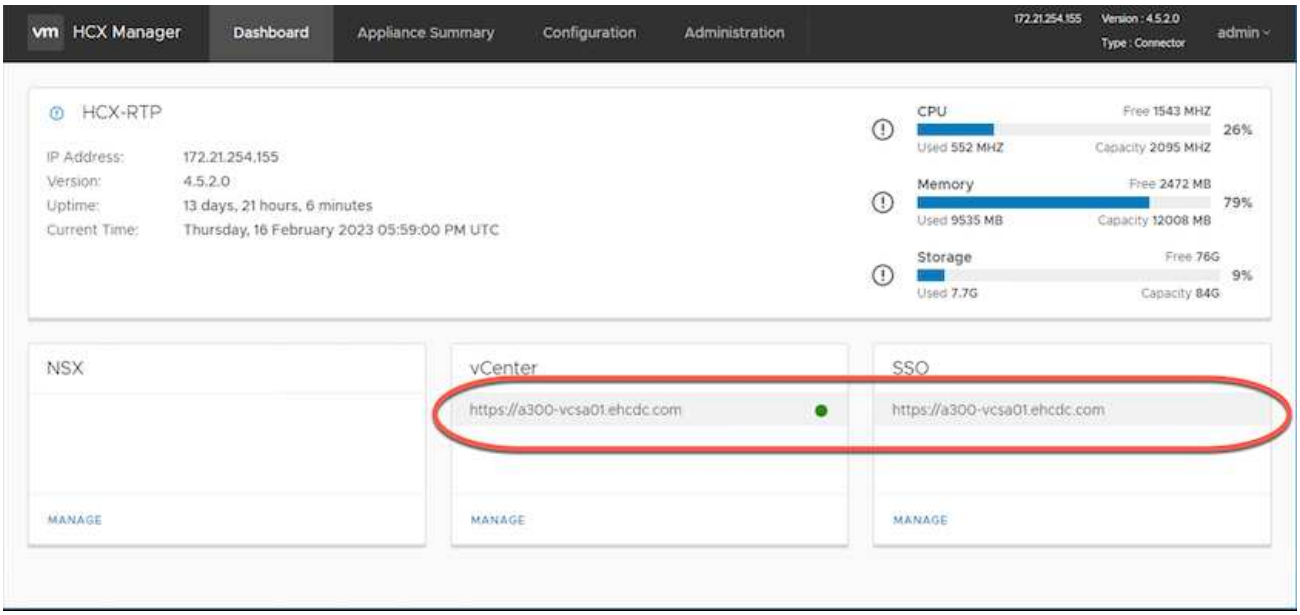
   使用 FQDN 以避免日後出現連線問題。

8. 在「設定 SSO/PSC」下，提供平台服務控制器 (PSC) 的 FQDN 或 IP 位址，然後按一下「繼續」。

   對於嵌入式 PSC，輸入 VMware vCenter Server FQDN 或 IP 位址。

9. 驗證輸入的資訊是否正確，然後按一下「重新啟動」。
10. 服務重新啟動後，vCenter Server 在出現的頁面上顯示為綠色。 vCenter Server 和 SSO 都必須具有適當的設定參數，這些參數應與上一頁相同。

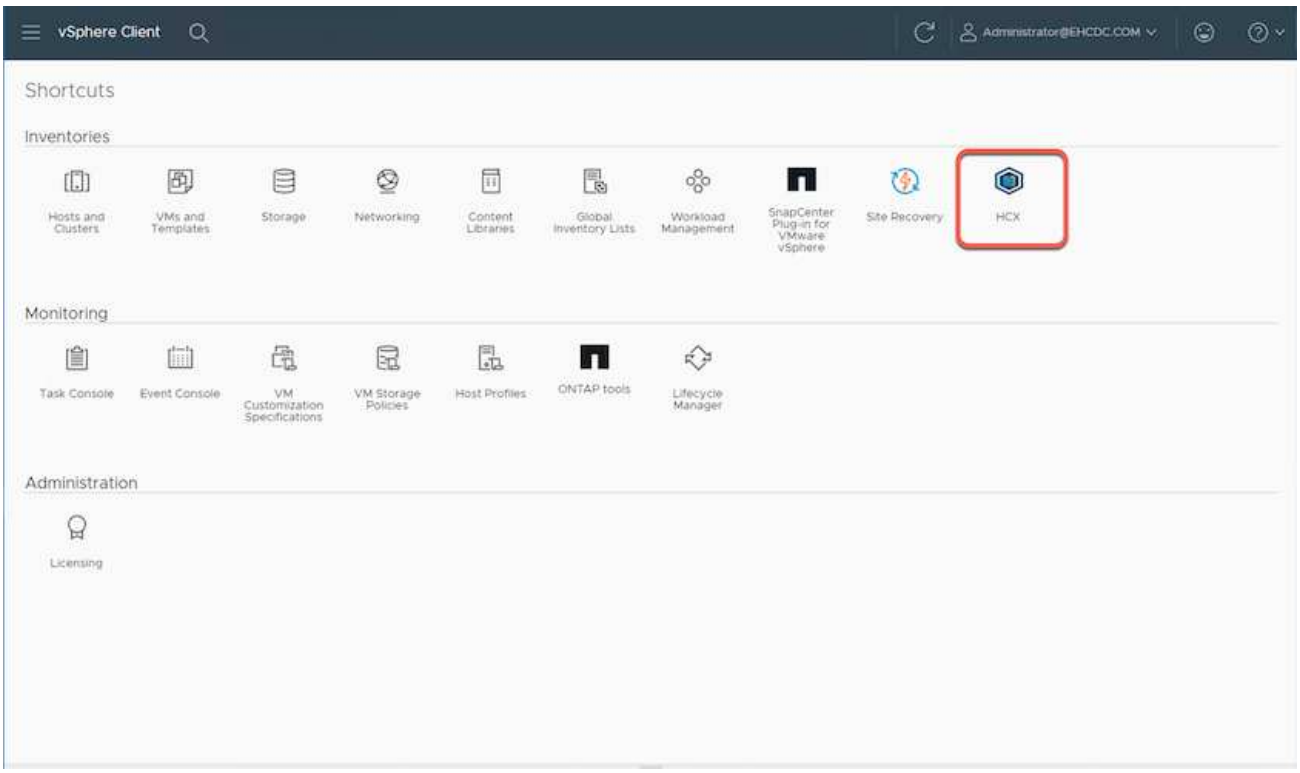
    此過程大約需要 10 到 20 分鐘，以便將插件新增至 vCenter Server。



▼ 步驟 **4**：將本機 **VMware HCX** 連接器與 **Google Cloud VMware Engine HCX Cloud Manager** 配對

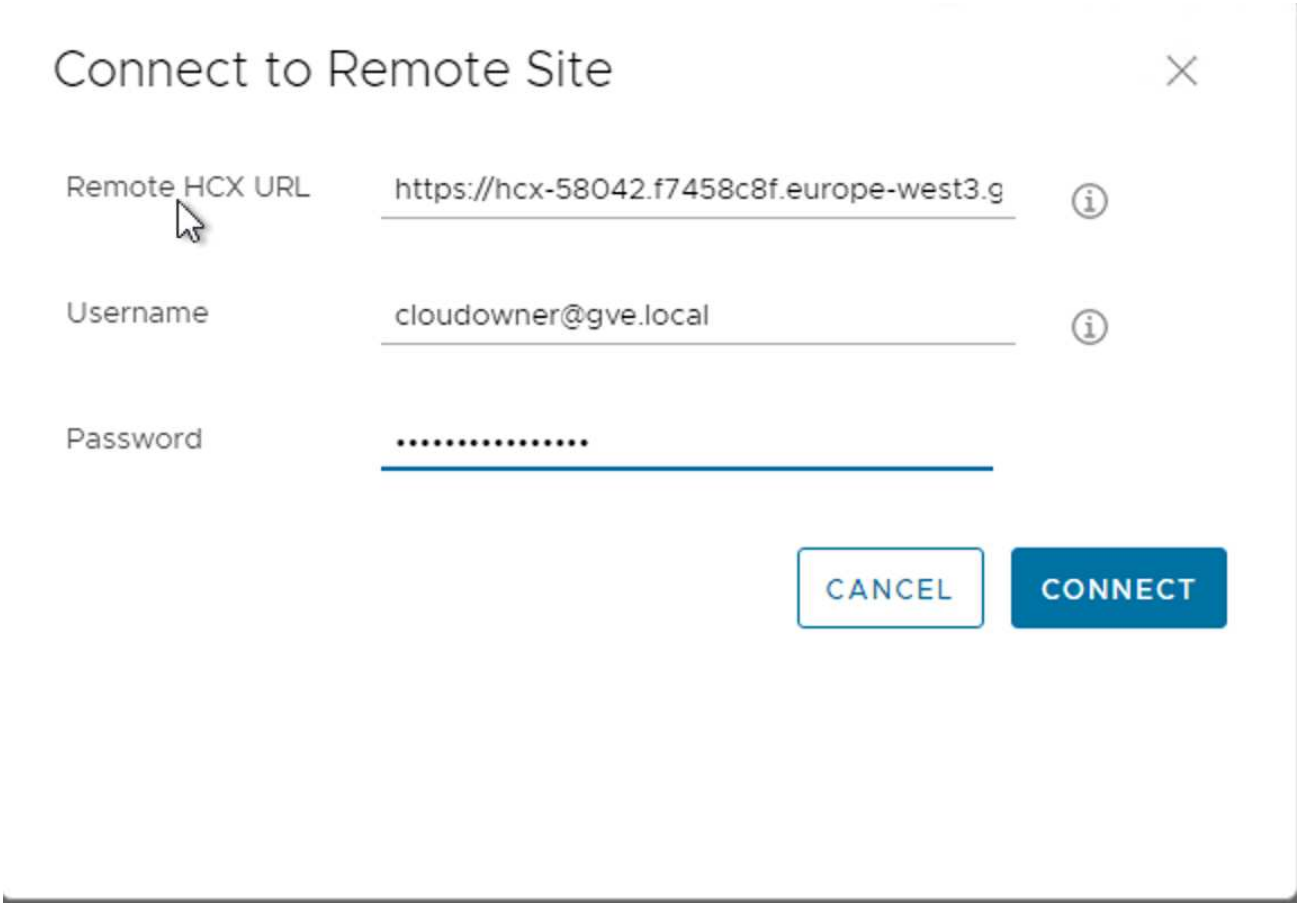
在本機 vCenter 上部署和設定 HCX Connector 後，透過新增配對建立與 Cloud Manager 的連線。若要設定網站配對，請完成以下步驟：

1. 若要在本機 vCenter 環境和 Google Cloud VMware Engine SDDC 之間建立網站對，請登入本機 vCenter Server 並造訪新的 HCX vSphere Web Client 外掛程式。



2. 在基礎架構下，按一下*新增網站配對*。

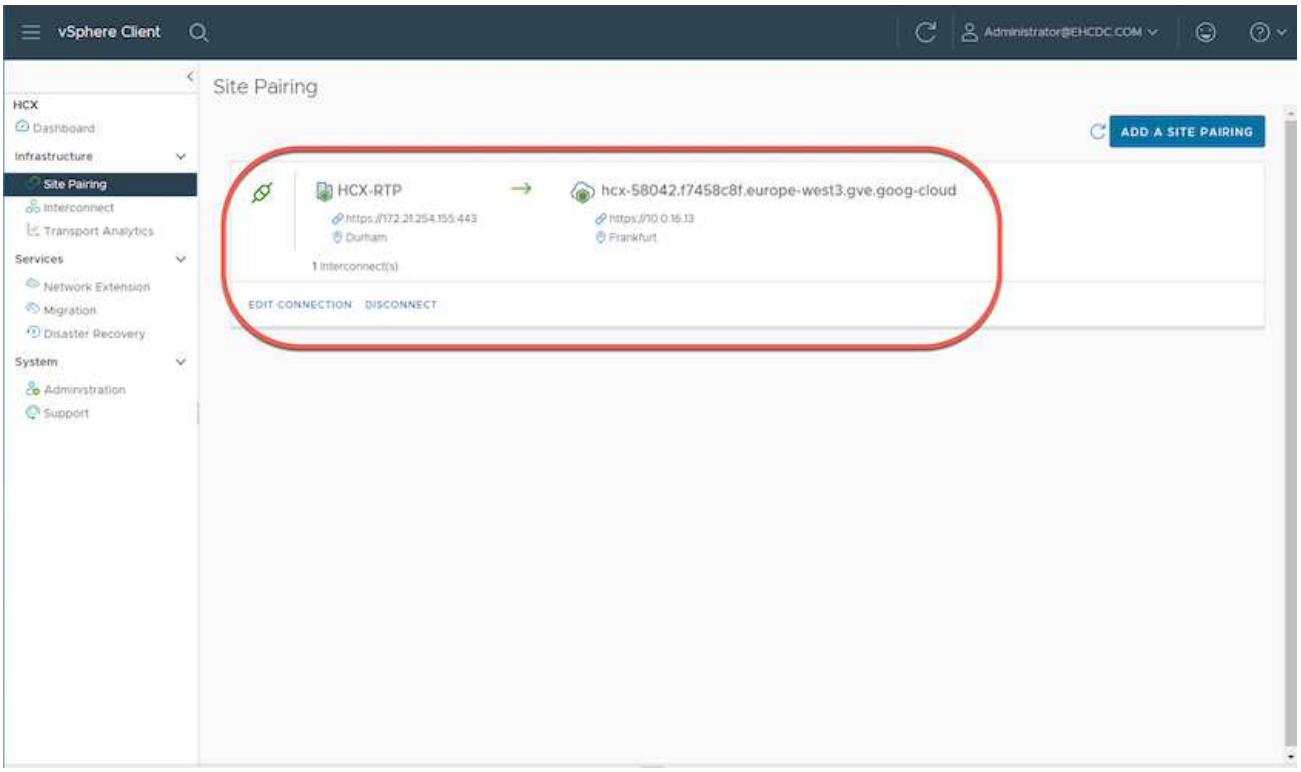
輸入 Google Cloud VMware Engine HCX Cloud Manager URL 或 IP 位址以及具有 CloudOwner-Role 權限的使用者存取私有雲的憑證。



3. 按一下“連接”。

   VMware HCX Connector 必須能夠透過連接埠 443 路由至 HCX Cloud Manager IP。

4. 建立配對後，新配置的網站配對可在 HCX 儀表板上取得。

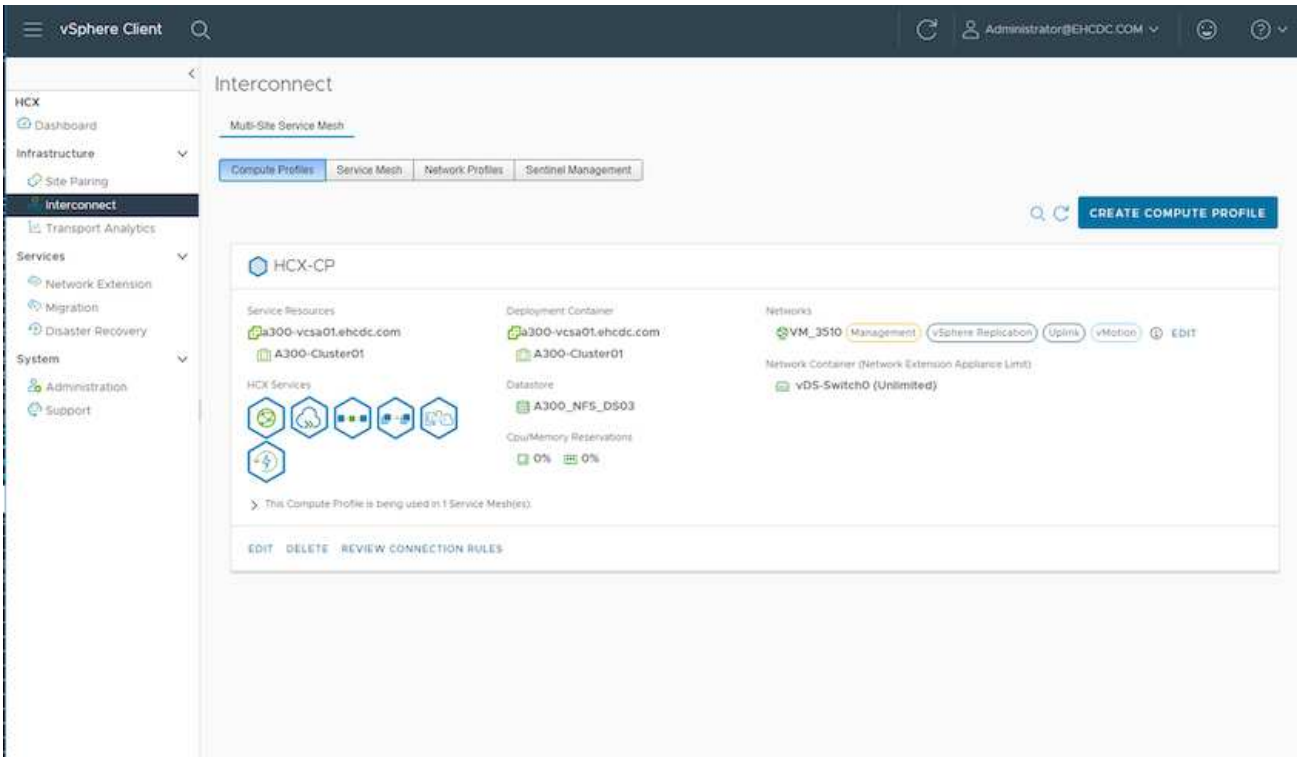


▼ 步驟 **5**：設定網路設定檔、計算設定檔和服務網格

VMware HCX Interconnect 服務設備透過網際網路和與目標網站的專用連線提供複製和基於 vMotion 的遷移功能。互連提供加密、流量工程和 VM 移動性。若要建立互連服務設備，請完成以下步驟：

1. 在基礎架構下，選擇*互連>多站點服務網格>計算設定檔>建立計算設定檔*。

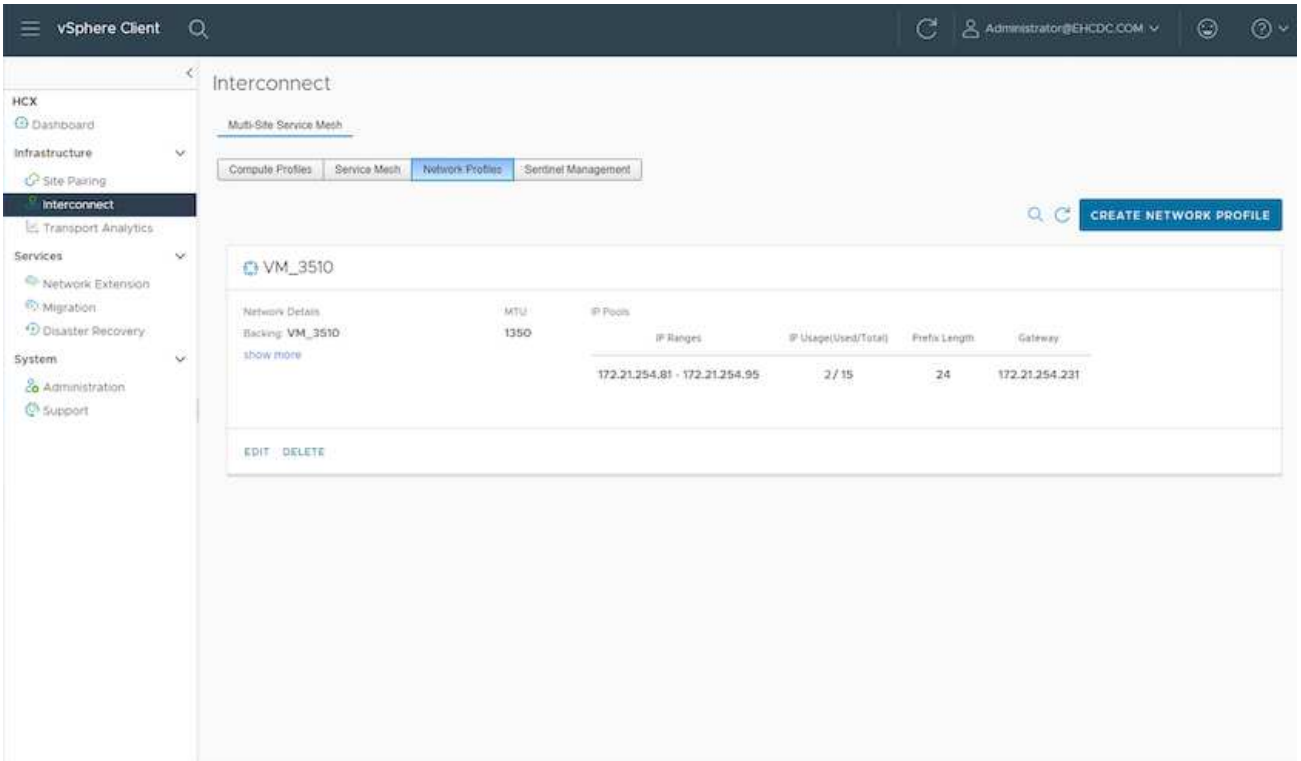
> ⓘ 計算設定檔定義部署參數，包括部署的設備以及 VMware 資料中心的哪些部分可供 HCX 服務存取。



2. 建立計算設定檔後，透過選擇「多站點服務網格」>「網路設定檔」>「建立網路設定檔」來建立網路設定檔。

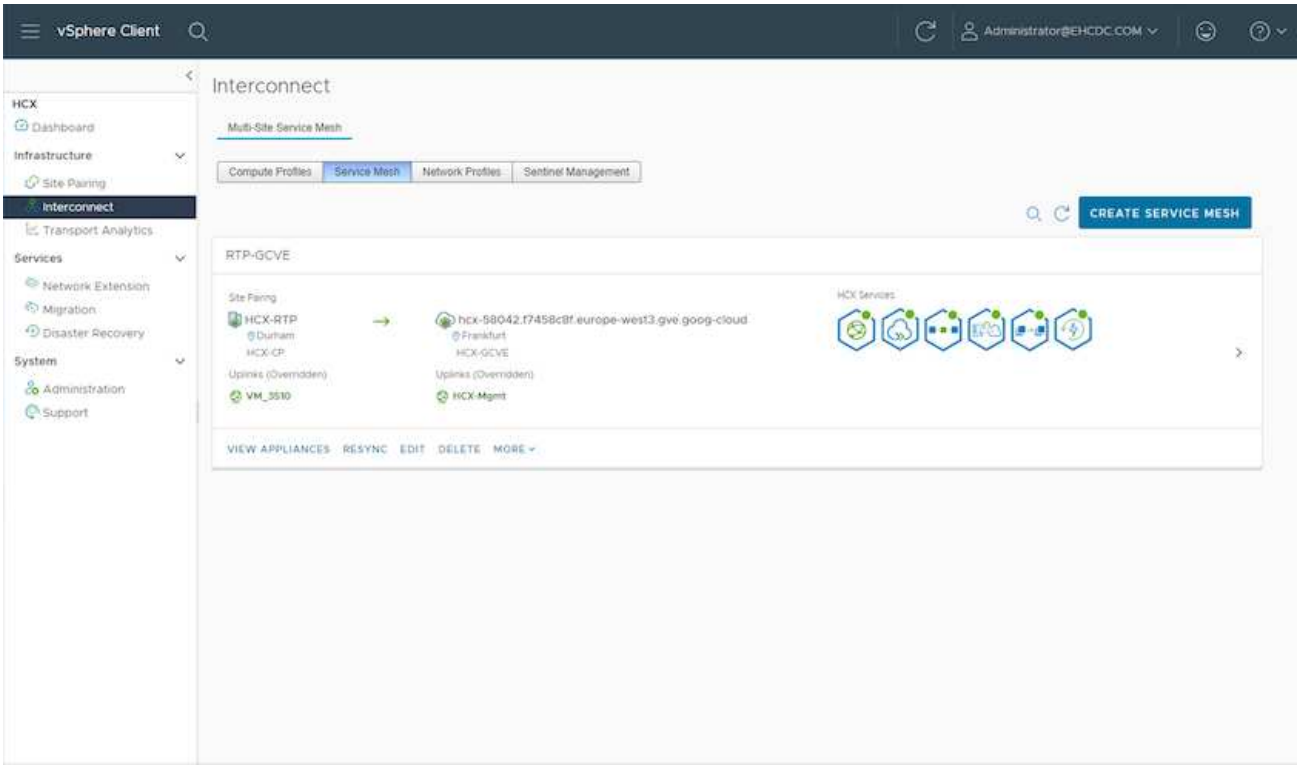
   網路設定檔定義了 HCX 用於其虛擬設備的一系列 IP 位址和網路。

   此步驟需要兩個或更多 IP 位址。這些 IP 位址由管理網路指派給互連設備。

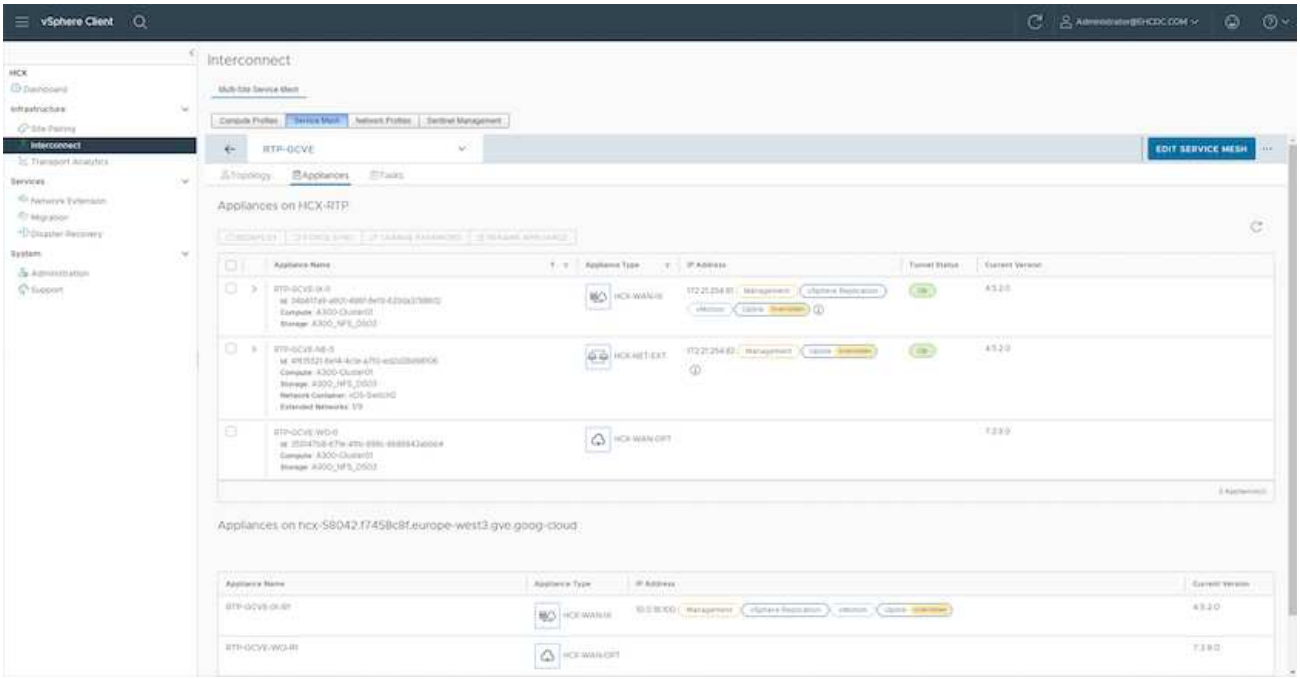


3. 此時，計算和網路設定檔已成功建立。
4. 透過選擇「**Interconnect**」選項中的「**Service Mesh**」標籤來建立服務網格，並選擇本地和 GCVE SDDC 網站。
5. 服務網格指定本地和遠端計算和網路設定檔對。

> 作為此流程的一部分，HCX 裝置在來源網站和目標網站上部署並自動配置，以建立安全的傳輸結構。



6. 這是配置的最後一步。完成部署大約需要 30 分鐘。配置服務網格後，環境已準備就緒，並已成功建立 IPsec 隧道來遷移工作負載虛擬機器。



▼ 步驟 **6**：遷移工作負載

可以使用各種 VMware HCX 遷移技術在本地和 GCVE SDDC 之間雙向遷移工作負載。可以使用多種遷移技術將虛擬機器移至 VMware HCX 啟動的實體或從中移出，例如 HCX 批量遷移、HCX vMotion、HCX 冷遷移、HCX 複製輔助 vMotion（HCX 企業版提供）和 HCX OS 輔助遷移（HCX 企業版提供）。

要了解有關各種 HCX 遷移機制的更多信息，請參閱 "使用 VMware HCX 文件遷移 VMware VM"。

HCX-IX 設備使用行動代理服務執行 vMotion、Cold 和複製輔助 vMotion (RAV) 遷移。

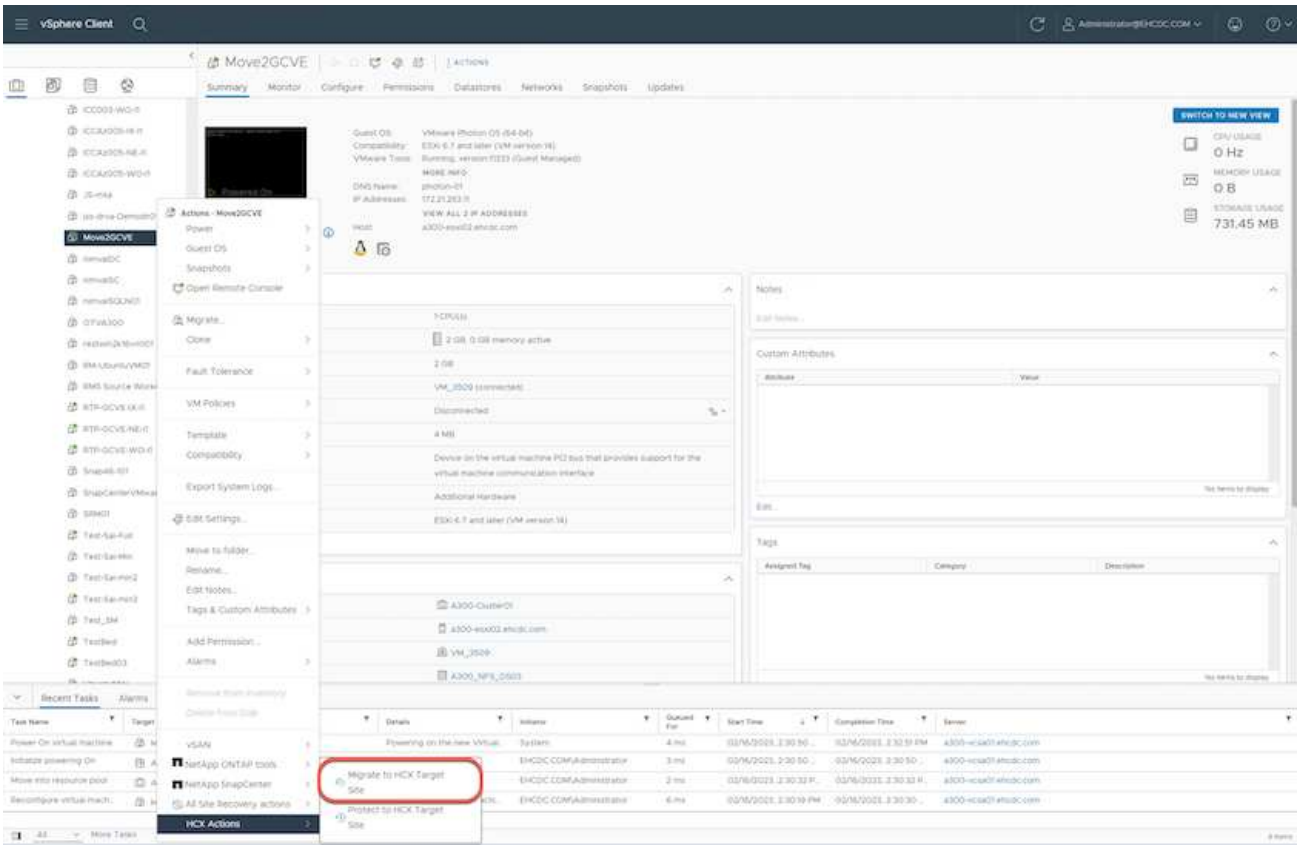
ⓘ HCX-IX 設備將行動代理服務新增為 vCenter Server 中的主機物件。此物件上顯示的處理器、記憶體、儲存和網路資源並不代表託管 IX 裝置的實體虛擬機器管理程式上的實際消耗。

HCX vMotion

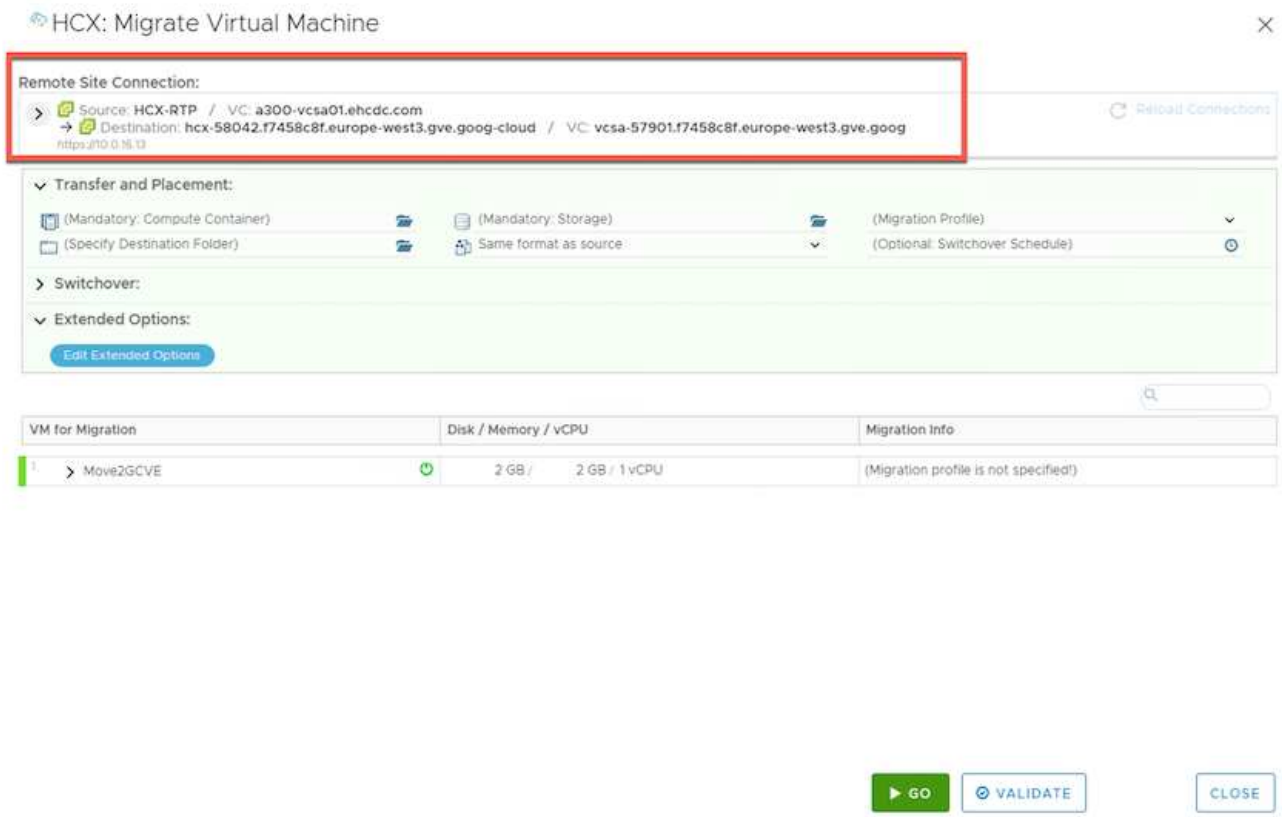
本節介紹 HCX vMotion 機制。此遷移技術使用 VMware vMotion 協定將虛擬機器遷移到 GCVE。 vMotion 遷移選項用於一次遷移單一 VM 的 VM 狀態。此遷移方法期間不會中斷服務。

ⓘ 應該實施網路擴充（針對虛擬機器所連接的連接埠群組），以便遷移虛擬機器而無需更改 IP 位址。

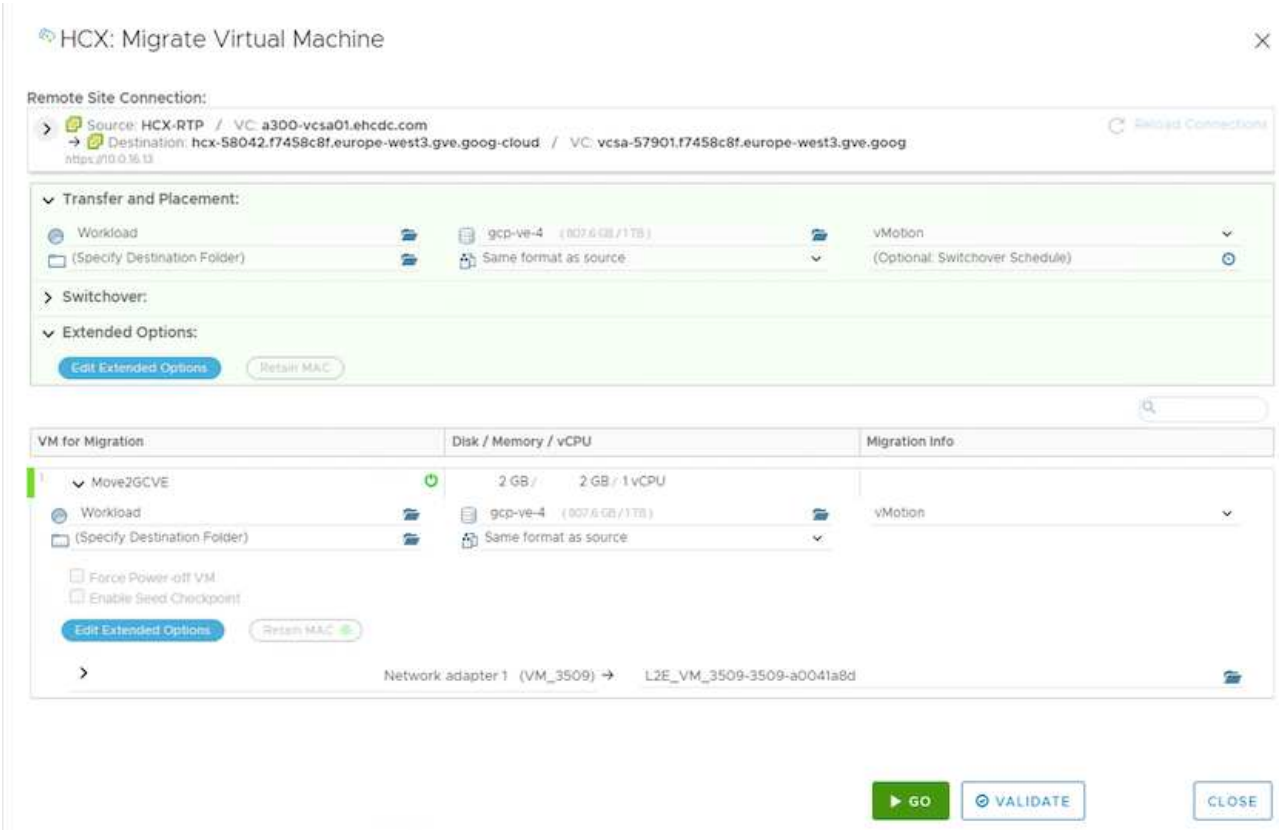
1. 從本機 vSphere 用戶端，前往“清單”，右鍵點選要遷移的虛擬機，然後選擇“HCX 動作”>“遷移到 HCX 目標網站”。



2. 在遷移虛擬機器精靈中，選擇遠端站台連線（目標 GCVE）。



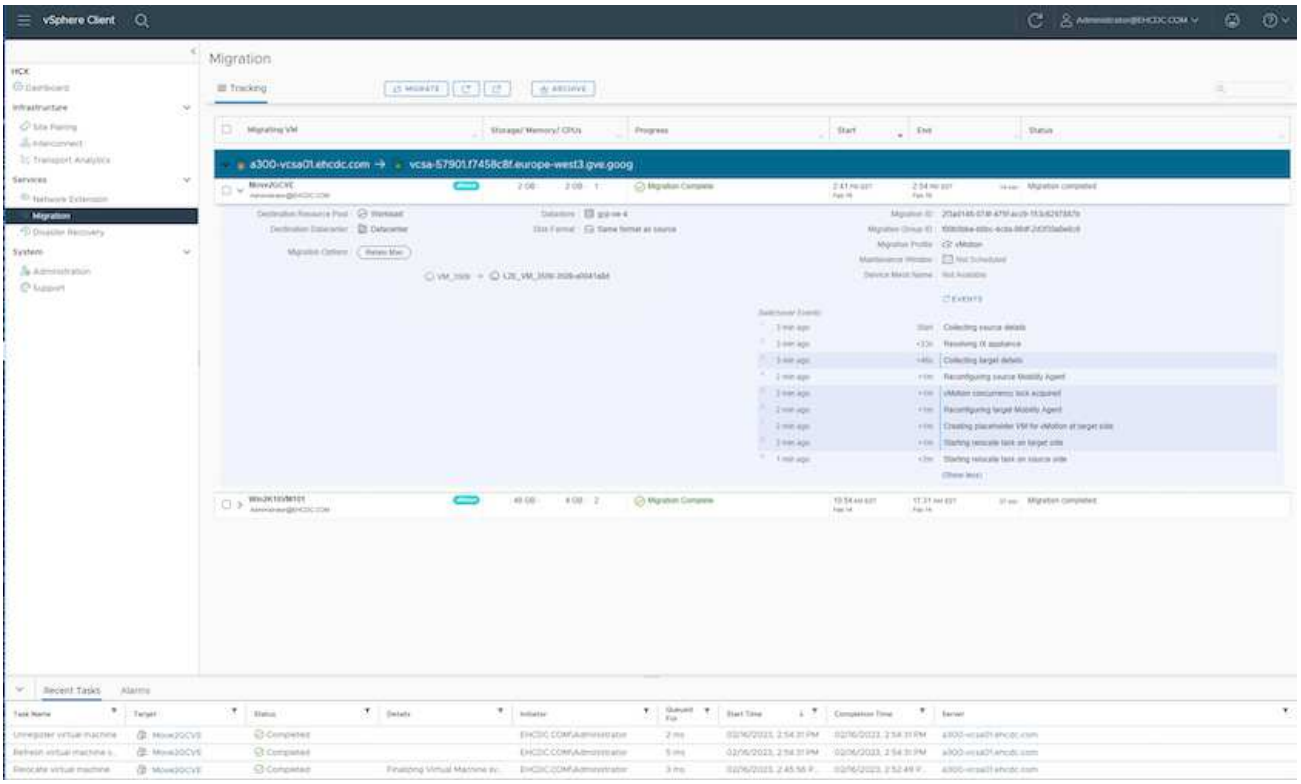
3. 更新必填欄位（叢集、儲存和目標網路），按一下驗證。



4. 驗證檢查完成後，按一下“Go”開始遷移。

> vMotion 傳輸擷取 VM 活動記憶體、其執行狀態、其 IP 位址和其 MAC 位址。有關 HCX vMotion 的要求和限制的更多信息，請參閱 "了解 VMware HCX vMotion 和冷遷移"。

5. 您可以從 HCX > 遷移儀表板監控 vMotion 的進度和完成情況。



目標Google Cloud NetApp Volumes （NetApp Volumes）NFS 資料儲存應具有足夠的空間來處理遷移。

結論

無論您的目標是全雲還是混合雲，以及駐留在本地任何類型/供應商存儲上的數據，Cloud Volume Service 和 HCX 都提供了部署和遷移應用程式工作負載的絕佳選擇，同時透過使數據需求無縫連接到應用程式層來降低 TCO。無論用例如何，選擇 Google Cloud VMware Engine 以及 Cloud Volume Service 都可以快速實現雲端優勢、跨本地和多雲的一致基礎架構和操作、工作負載的雙向可移植性以及企業級容量和效能。使用 VMware vSphere Replication、VMware vMotion 甚至網路檔案複製 (NFC) 連接儲存和遷移虛擬機器所使用的流程和程式相同。

總結

該文件的要點包括：

- 現在您可以將 Cloud Volume Service 用作 Google Cloud VMware Engine SDDC 上的資料儲存。
- 您可以輕鬆地將資料從本地遷移到 Cloud Volume Service 資料儲存區。
- 您可以輕鬆擴大或縮小 Cloud Volume Service 資料儲存以滿足遷移活動期間的容量和效能要求。

參考 **Google** 和 **VMware** 的視頻

▼ 來自**Google**

- "使用 GCVE 部署 HCX 連接器"
- "使用 GCVE 配置 HCX ServiceMesh"
- "將帶有 HCX 的虛擬機器遷移到 GCVE"

▼ 來自 **VMware**

- "適用於 GCVE 的 HCX 連接器部署"
- "GCVE 的 HCX ServiceMesh 配置"
- "HCX 工作負載遷移至 GCVE"

在哪裡可以找到更多信息

要了解有關本文檔中描述的信息的更多信息，請參閱以下網站連結：

- Google Cloud VMware Engine 文件

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service 文檔

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- VMware HCX 使用者指南

  "https://docs.vmware.com/en/VMware-HCX/index.html"

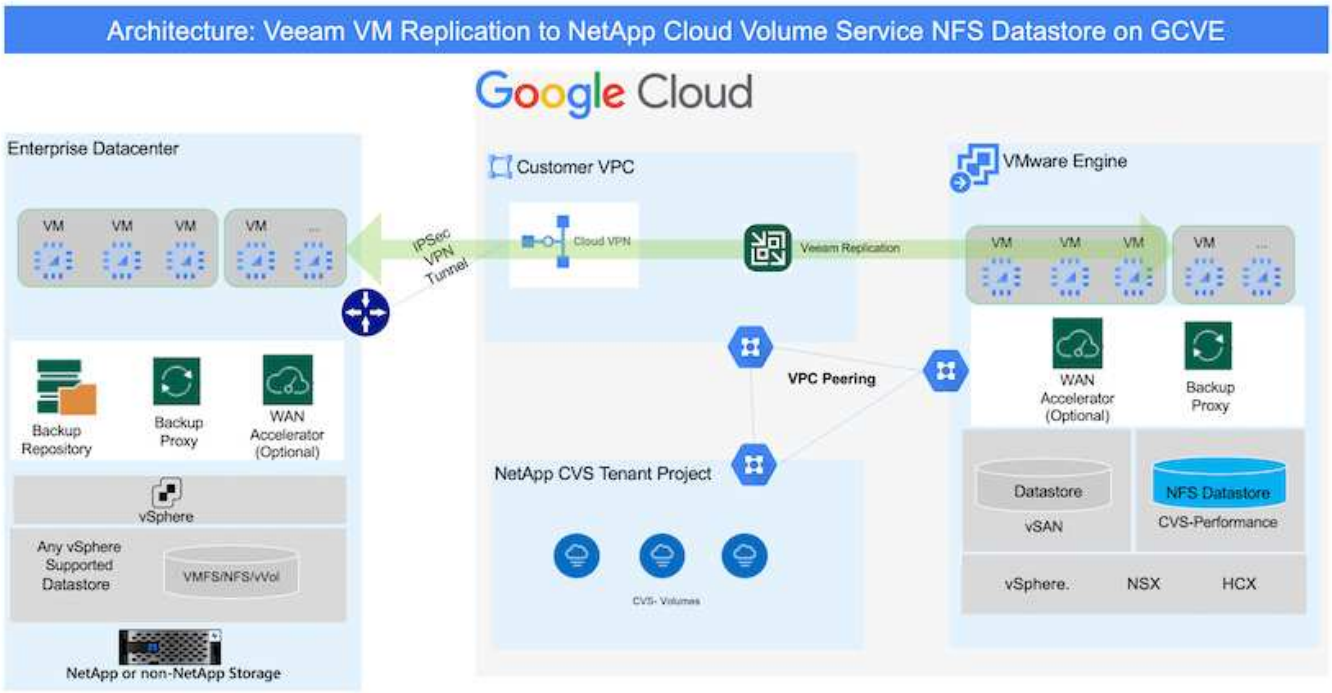
使用 **Veeam Replication** 功能將虛擬機器遷移到 **Google Cloud VMware Engine** 上的**Google Cloud NetApp Volumes NFS** 資料儲存區

目前使用 Veeam 滿足資料保護需求的客戶可以繼續使用該解決方案將工作負載遷移到 GCVE，並享受Google Cloud NetApp Volumes NFS 資料儲存區帶來的好處。

概況

利用 Veeam Replication 功能可以將 VMware vSphere 上執行的虛擬機器工作負載遷移到 Google Cloud VMware Engine (GCVE)。

本文檔提供了使用Google Cloud NetApp Volumes、Veeam 和 Google Cloud VMware Engine (GCVE) 設定和執行 VM 遷移的逐步方法。



假設

本文檔假設您已安裝 Google Cloud VPN 或 Cloud Interconnect 或其他網路選項，以建立從現有 vSphere 伺服器到 Google Cloud VMware Engine 的網路連線。

> 將本機資料中心連接到 Google Cloud 有多種選擇，因此我們無法在本文檔中概述特定的工作流程。請參閱"Google Cloud 文件"以找到適當的本地到 Google 連線方法。

部署遷移解決方案

解決方案部署概述

1. 確保Google Cloud NetApp Volumes的 NFS 資料儲存已安裝在 GCVE vCenter 上。
2. 確保 Veeam Backup Recovery 部署在現有 VMware vSphere 環境中
3. 建立複製作業以開始將虛擬機器複製到 Google Cloud VMware Engine 執行個體。
4. 執行 Veeam 複製作業的故障轉移。
5. 在 Veeam 上執行永久故障轉移。

部署詳情

確保**Google Cloud NetApp Volumes**中的 **NFS** 資料儲存已安裝在 **GCVE vCenter** 上

登入 GCVE vCenter 並確保有足夠空間的 NFS 資料儲存可用。如果沒有，請參閱"將NetApp磁碟區掛載為 GCVE 上的 NFS 資料存儲"

確保 **Veeam Backup Recovery** 部署在現有 **VMware vSphere** 環境中

請參考"Veeam 複製元件"安裝所需組件的文件。

建立複製作業以開始將虛擬機器複製到 **Google Cloud VMware Engine** 執行個體。

本機 vCenter 和 GCVE vCenter 都需要在 Veeam 中註冊。"設定 vSphere VM 複製作業"這是一個解釋如何"配置複製作業"。

副本虛擬機器可以具有與來源虛擬機器不同的 IP，也可以連接到不同的連接埠群組。欲了解更多詳情，請查看上面的影片。

執行 **Veeam** 複製作業的故障轉移

若要遷移虛擬機，請執行"執行故障轉移"

在 **Veeam** 上執行永久故障轉移。

若要將 GCVE 視為新的來源環境，請執行"永久故障轉移"

此解決方案的優勢

- 現有的 Veeam 備份基礎架構可用於遷移。
- Veeam Replication 允許變更目標站台上的 VM IP 位址。
- 能夠重新對應在 Veeam 外部複寫的現有資料（例如來自 NetApp 系統的複寫資料）
- 能夠在目標站點上指定不同的網路連接埠群組。
- 可以指定虛擬機器的啟動順序。
- 利用 VMware 變更塊追蹤來最大限度地減少透過 WAN 發送的資料量。
- 能夠執行複製的前腳本和後腳本。
- 能夠執行快照的前腳本和後腳本。

使用Google Cloud NetApp Volumes保護 Google Cloud 中的數據

TR-4918：安全概覽 **- Google Cloud** 中的**Google Cloud NetApp Volumes**

Oliver Krause、Justin Parisi、 NetApp

安全性，尤其是在基礎架構不受儲存設備系統管理員控制的雲端環境中，對於將您的資料託付給雲端供應商所提供的服務而言，至關重要。本文件是安全性服務的總覽，這些服務"Google Cloud NetApp Volumes在 Google Cloud 提供"。

目標受眾

本文檔的目標受眾包括但不限於以下角色：

- 雲端提供者
- 儲存管理員
- 儲存架構師
- 現場資源

- 商業決策者

如果您對本技術報告的內容有任何疑問，請參閱"聯繫我們。"

縮寫	定義
NetApp卷-SW	Google Cloud NetApp Volumes，服務類型NetApp Volumes
NetApp磁碟區效能	雲端磁碟區服務，服務類型NetApp磁碟區 - 效能
變壓吸附	

Google Cloud 中的**Google Cloud NetApp Volumes**如何保護您的數據

Google Cloud 中的Google Cloud NetApp Volumes提供了多種方式來原生保護您的資料。

安全架構和租賃模型

Google Cloud NetApp Volumes透過將服務管理（控制平面）和資料存取（資料平面）劃分到不同的端點，從而彼此之間不會產生影響，從而在 Google Cloud 中提供安全架構（請參閱"Google Cloud NetApp Volumes架構"）。它使用谷歌的 "私人服務訪問"（PSA）框架來提供服務。此框架區分了服務生產者（由NetApp提供和營運）和服務消費者（客戶專案中的虛擬私有雲 (VPC)，用於託管想要存取Google Cloud NetApp Volumes檔案共用的用戶端）。

在此架構中，租用戶（參見"租賃模型"）被定義為除非使用者明確連接，否則彼此完全隔離的 Google Cloud 專案。租用戶可以使用Google Cloud NetApp Volumes磁碟區平台將資料磁碟區、外部名稱服務以及解決方案的其他重要部分與其他租用戶完全隔離。由於Google Cloud NetApp Volumes平台透過 VPC 對等連接，因此這種隔離也適用於它。您可以使用共用 VPC 在多個專案之間共用Google Cloud NetApp Volumes磁碟區（請參閱"共享VPC"）。您可以對 SMB 共用和 NFS 匯出套用存取控制，以限制誰或什麼可以檢視或修改資料集。

控制平面的強大身分管理

在進行Google Cloud NetApp Volumes配置的控制平面中，身分識別管理透過使用 "身分存取管理 (IAM)"。 IAM 是一項標準服務，可讓您控制對 Google Cloud 專案執行個體的驗證（登入）和授權（權限）。所有設定均透過使用 TLS 1.2 加密的安全 HTTPS 傳輸使用Google Cloud NetApp Volumes API 執行，並使用 JWT 令牌執行驗證以增強安全性。 Google Cloud NetApp Volumes的 Google 控制台 UI 將使用者輸入轉換為Google Cloud NetApp Volumes API 呼叫。

安全強化－限制攻擊面

有效安全的一部分是限制服務中可用的攻擊面數量。攻擊面可以包括各種各樣的東西，包括靜態資料、動態傳輸資料、登入資料和資料集本身。

託管服務消除了其設計中固有的一些攻擊面。基礎設施管理，如本節所述"服務運營，"由專門的團隊處理並實現自動化，以減少人工實際接觸配置的次數，有助於減少有意和無意的錯誤。網路被隔離，以便只有必要的服務才能相互存取。加密已融入資料儲存中，只有資料平面需要Google Cloud NetApp Volumes管理員的安全關注。透過將大部分管理隱藏在 API 介面後面，可以透過限制攻擊面來實現安全性。

零信任模型

從歷史上看，IT 安全理念一直是信任但要驗證，並表現為僅依靠外部機制（如防火牆和入侵偵測系統）來減輕威脅。然而，攻擊和入侵已經演變成透過網路釣魚、社會工程、內部威脅和其他提供驗證的方法來繞過環境中的驗證，從而進入網路並造成破壞。

零信任已成為安全領域的一種新方法，其當前的口號是「不信任任何事物，但仍然驗證一切」。因此，預設情況下不允許任何內容存取。這一口號透過多種方式執行，包括標準防火牆和入侵偵測系統 (IDS)，以及以下方法：

- 強式驗證方法（例如 AES 加密的 Kerberos 或 JWT 令牌）
- 單一強大的身分來源（例如 Windows Active Directory、輕量級目錄存取協定 (LDAP) 和 Google IAM）
- 網路分段和安全多租戶（預設只允許租戶存取）
- 使用最小特權存取策略進行細粒度存取控制
- 擁有專門的、值得信賴的管理員的小型獨家名單，具有數位審計和紙本記錄

在 Google Cloud 中運行的Google Cloud NetApp Volumes透過實施「不信任任何事物，驗證一切」的立場來遵循零信任模型。

加密

加密靜態資料（請參閱"靜態資料加密") 透過使用 XTS-AES-256 密碼與NetApp卷加密 (NVE) 以及"SMB 加密"或 NFS Kerberos 5p 支援。請放心，跨區域複製傳輸受到 TLS 1.2 加密的保護（請參閱部分連結：gcp-gcnv-security-considerations.html#Detection, Prevention and mitigation of ransomware, Malware, and viral#cross-region-replication["Cross-region replication"]）。此外，Google 網路也提供加密通訊（請參閱"傳輸中的資料加密") 來增加一層防禦攻擊的保護。有關傳輸加密的更多信息，請參閱"Google Cloud 網路"。

資料保護和備份

安全不僅僅意味著預防攻擊。它還涉及我們如何在攻擊發生時恢復。該策略包括資料保護和備份。 Google Cloud NetApp Volumes提供了在發生中斷時複製到其他區域的方法（請參閱"跨區域複製"）或資料集是否受到勒索軟體攻擊的影響。它還可以透過以下方式將資料非同步備份到Google Cloud NetApp Volumes實例之外的位置："Google Cloud NetApp Volumes備份" 。透過定期備份，緩解安全事件可以花費更少的時間，並為管理員節省金錢和精力。

利用業界領先的 **Snapshot** 副本快速緩解勒索軟體

除了資料保護和備份之外， Google Cloud NetApp Volumes還支援不可變的 Snapshot 副本（請參閱"不可變的 Snapshot 副本"）允許從勒索軟體攻擊中恢復的捲（請參閱"服務營運") 在發現問題後的幾秒鐘內就能解決問題，並且幹擾最小。恢復時間和效果取決於 Snapshot 計劃，但您可以建立在勒索軟體攻擊中提供僅一小時增量的 Snapshot 副本。快照副本對效能和容量使用的影響可以忽略不計，並且是一種保護資料集的低風險、高回報的方法。

安全考慮和攻擊面

了解如何保護資料的第一步是識別風險和潛在的攻擊面。

這些包括（但不限於）以下內容：

- 管理和登入
- 靜態數據
- 飛行中的數據
- 網路和防火牆
- 勒索軟體、惡意軟體和病毒

了解攻擊面可以幫助您更好地保護您的環境。 Google Cloud 中的Google Cloud NetApp Volumes已經考慮了許多此類主題，並預設實現了安全功能，無需任何管理互動。

確保安全登入

在保護關鍵基礎設施元件時，必須確保只有經過批准的使用者才能登入和管理您的環境。如果不法分子破壞了您的管理憑證，那麼他們就擁有了城堡的鑰匙，可以做任何他們想做的事情 - 更改配置、刪除捲和備份、創建後門或禁用快照計劃。

Google Cloud NetApp Volumes for Google Cloud 透過混淆儲存即服務 (StaaS) 來防止未經授權的管理登入。 Google Cloud NetApp Volumes完全由雲端供應商維護，無法從外部登入。所有設定和配置操作都是完全自動化的，因此除了極少數情況外，人工管理員無需與系統進行互動。

如果需要登入，Google Cloud 中的Google Cloud NetApp Volumes透過維護一個有權登入系統的受信任管理員的極短列表來確保登入安全。這種把關有助於減少有存取權限的潛在不良行為者的數量。此外，Google Cloud 網路將系統隱藏在多層網路安全之後，只向外界公開所需的內容。有關 Google Cloud、 Google Cloud NetApp Volumes架構的信息，請參閱"Google Cloud NetApp Volumes架構。"

叢集管理和升級

存在潛在安全風險的兩個領域包括叢集管理（如果不良行為者擁有管理員存取權限會發生什麼情況）和升級（如果軟體映像外洩會發生什麼情況）。

儲存管理保護

作為服務提供的儲存空間透過刪除雲端資料中心以外的最終使用者的存取權限，消除了管理員面臨的額外風險。相反，唯一完成的配置是針對客戶的資料存取平面。每個租用戶管理自己的捲，並且沒有租戶可以存取其他Google Cloud NetApp Volumes實例。該服務由自動化管理，只有極少數受信任的管理員可以透過本節介紹的流程存取系統"服務運作。"

NetApp Volumes-Performance 服務類型提供跨區域複製選項，以便在發生區域故障時為不同區域提供資料保護。在這些情況下， Google Cloud NetApp Volumes可以故障轉移到未受影響的區域以維持資料存取。

服務升級

更新有助於保護易受攻擊的系統。每次更新都提供安全性增強和錯誤修復，以最大限度地減少攻擊面。軟體更新從集中式儲存庫下載，並在允許更新之前進行驗證，以驗證是否使用了官方映像以及升級是否未被不良行為者破壞。

使用Google Cloud NetApp Volumes，更新由雲端提供者團隊處理，透過提供精通配置和升級的專家（這些專家已經對流程進行了自動化和全面測試），從而消除了管理員團隊的風險敞口。升級不會造成中斷， Google Cloud NetApp Volumes會維護最新更新以獲得最佳整體效果。

有關執行這些服務升級的管理員團隊的信息，請參閱"服務運作。"

保護靜態數據

當磁碟被盜、被退回或被重新利用時，靜態資料加密對於保護敏感資料非常重要。 Google Cloud NetApp Volumes中的資料透過使用基於軟體的加密進行靜態保護。

- Google 產生的金鑰用於NetApp Volumes-SW。
- 對於NetApp Volumes-Performance，每個磁碟區的金鑰都儲存在Google Cloud NetApp Volumes內建的金鑰管理器中，該管理員使用NetApp ONTAP CryptoMod 產生 AES-256 加密金鑰。 CryptoMod 列在 CMVP

FIPS 140-2 驗證模組清單中。看 "FIPS 140-2 憑證 #4144"。

從 2021 年 11 月開始，預覽版客戶管理加密 (CMEK) 功能已為NetApp Volumes-Performance 提供。此功能可讓您使用託管在 Google 金鑰管理服務 (KMS) 中的每個項目、每個區域的主金鑰加密每個磁碟區的金鑰。 KMS 可讓您附加外部金鑰管理員。

如需如何為 NetApp Volumes-Performance 設定 KMS 的詳細資訊， "請參閱Google Cloud NetApp Volumes文檔"。

有關架構的更多信息，請參閱"Google Cloud NetApp Volumes架構。"

確保傳輸中的資料安全

除了保護靜態資料之外，您還必須能夠保護在Google Cloud NetApp Volumes實例和用戶端或複製目標之間傳輸的資料。 Google Cloud NetApp Volumes使用加密方法（例如使用 Kerberos 的 SMB 加密、封包的簽署/密封以及用於資料傳輸端對端加密的 NFS Kerberos 5p）為透過 NAS 協定傳輸的資料提供加密。

Google Cloud NetApp Volumes磁碟區的複製使用 TLS 1.2，它利用了 AES-GCM 加密方法。

大多數不安全的運行中協定（如 telnet、NDMP 等）預設都是禁用的。但是，DNS 並非由Google Cloud NetApp Volumes加密（不支援 DNS Sec），因此應盡可能使用外部網路加密進行加密。請參閱"傳輸中的資料加密"有關保護傳輸中資料的詳細資訊。

有關 NAS 協定加密的信息，請參閱"NAS 協定。"

NAS 權限的使用者和群組

保護雲端中資料安全的一部分涉及正確的用戶和群組身份驗證，其中存取資料的用戶被驗證為環境中的真實用戶，且群組包含有效用戶。這些使用者和群組提供初始共用和匯出存取權限，以及儲存系統中檔案和資料夾的權限驗證。

Google Cloud NetApp Volumes使用基於標準 Active Directory 的 Windows 使用者和群組驗證來實現 SMB 共用和 Windows 風格的權限。該服務還可以利用 UNIX 身分提供程序，例如用於 UNIX 使用者和群組的 LDAP，以進行 NFS 匯出、NFSv4 ID 驗證、Kerberos 驗證和 NFSv4 ACL。

目前， Google Cloud NetApp Volumes僅支援 Active Directory LDAP 的 LDAP 功能。

偵測、預防和緩解勒索軟體、惡意軟體和病毒

勒索軟體、惡意軟體和病毒對管理員來說是一個持續的威脅，偵測、預防和緩解這些威脅始終是企業組織的首要任務。針對關鍵資料集的一次勒索軟體事件就可能造成數百萬美元的損失，因此盡最大努力將風險降至最低是有益的。

儘管 Google Cloud NetApp Volumes 目前不包含原生偵測或預防措施（例如防毒保護或 "自動勒索軟體偵測"），但您可以透過啟用定期 Snapshot 快照技術排程來快速從勒索軟體事件中恢復。Snapshot 快照技術副本是不可變的，並且是指向檔案系統中變更的區塊的唯讀指標，幾乎是瞬時的，對效能的影響極小，並且僅在資料變更或刪除時才佔用空間。您可以設定 Snapshot 快照技術副本的排程，以符合您所需的可接受恢復點目標（RPO）/ 恢復時間目標（RTO），每個 Volume 最多可保留 1,024 個 Snapshot 快照技術副本。

Google Cloud NetApp Volumes提供免費的快照支援（除了 Snapshot 副本保留的更改區塊/資料的資料儲存費用之外），並且在發生勒索軟體攻擊時，可用於回滾到攻擊發生之前的 Snapshot 副本。快照恢復只需幾秒鐘即可完成，然後您就可以恢復正常提供資料。有關更多信息，請參閱 "NetApp勒索軟體解決方案" 。

防止勒索軟體影響您的業務需要採取多層次的方法，包括以下一項或多項措施：

- 端點保護
- 透過網路防火牆防禦外部威脅
- 數據異常檢測
- 關鍵資料集的多重備份（現場和異地）
- 定期對備份進行復原測試
- 不可變的唯讀NetApp Snapshot 副本
- 關鍵基礎設施的多因素身份驗證
- 系統登入安全審計

此列表遠非詳盡無遺，但在處理潛在的勒索軟體攻擊時，它是一個很好的藍圖。 Google Cloud 中的Google Cloud NetApp Volumes提供了多種方法來防範勒索軟體事件並減少其影響。

不可變的 **Snapshot** 副本

Google Cloud NetApp Volumes本身提供不可變的唯讀 Snapshot 副本，這些副本按照可自訂的時間表進行，以便在資料刪除或整個磁碟區受到勒索軟體攻擊時快速進行時間點恢復。 Snapshot 恢復到以前的良好 Snapshot 副本速度很快，並且可以根據 Snapshot 計劃和 RTO/RPO 的保留期最大限度地減少資料遺失。採用Snapshot技術對效能的影響微乎其微。

由於Google Cloud NetApp Volumes中的 Snapshot 副本是唯讀的，因此它們不會被勒索軟體感染，除非勒索軟體在不知不覺中擴散到資料集中，並且已經從受勒索軟體感染的資料中獲取了 Snapshot 副本。這就是為什麼您還必須考慮基於資料異常的勒索軟體偵測。 Google Cloud NetApp Volumes目前不提供原生偵測，但您可以使用外部監控軟體。

備份和復原

Google Cloud NetApp Volumes提供標準 NAS 用戶端備份功能（例如透過 NFS 或 SMB 進行備份）。

- NetApp Volumes-Performance 提供跨區域 Volume 複寫至其他 NetApp Volumes-Performance Volume。如需詳細資訊，請參閱 Google Cloud NetApp Volumes 文件中的 "卷複製"。
- NetApp Volumes-SW 提供服務原生的 Volume 備份/還原功能。如需詳細資訊，請參閱 Google Cloud NetApp Volumes 文件中的 "雲端備份"。

卷複製提供了來源磁碟區的精確副本，以便在發生災難（包括勒索軟體事件）時實現快速故障轉移。

跨區域複製

NetApp Volumes-Performance 可讓您在NetApp控制的後端服務網路上使用 TLS1.2 AES 256 GCM 加密，使用在 Google 網路上執行的用於複製的特定接口，安全地跨 Google Cloud 區域複製磁碟區以進行資料保護和存檔用例。主（來源）磁碟區包含活動生產數據，並複製到輔助（目標）磁碟區以提供主資料集的精確副本。

初始複製傳輸所有區塊，但更新僅傳輸主磁碟區中變更的區塊。例如，如果將位於主磁碟區上的 1TB 資料庫複製到輔助磁碟區，則在初始複製時會傳送 1TB 的空間。如果資料庫在初始化和下次更新之間有數百行（假設幾 MB）發生變化，則只有包含已更改行的區塊才會複製到輔助資料庫（幾 MB）。這有助於確保傳輸時間保持較低水平並降低複製費用。

檔案和資料夾的所有權限都會複製到輔助磁碟區，但共用存取權限（例如匯出原則和規則或 SMB 共用和共用 ACL）必須單獨處理。在發生網站故障轉移的情況下，目標網站應利用相同的名稱服務和 Active Directory 網域連線來提供對使用者和群組身分和權限的一致處理。您可以透過中斷複製關係（將輔助磁碟區轉換為讀寫關係）在災難發生時將輔助磁碟區用作故障轉移目標。

卷副本是唯讀的，它提供了異地資料的不可變副本，以便在病毒感染資料或勒索軟體加密主資料集的情況下快速恢復資料。只讀資料不會被加密，但是，如果主磁碟區受到影響並發生複製，則受感染的區塊也會複製。您可以使用較舊的、未受影響的 Snapshot 副本進行恢復，但根據偵測到攻擊的速度，SLA 可能會超出承諾的 RTO/RPO 範圍。

此外，借助 Google Cloud 中的跨區域複寫（CRR）管理，您可以防止惡意管理操作，例如刪除 Volume、刪除 Snapshot 快照技術或變更 Snapshot 排程。這可以透過建立自訂角色來實現，將 Volume 系統管理員（可以刪除來源 Volume 但不能破壞鏡像，因此無法刪除目的地 Volume）與 CRR 系統管理員（不能執行任何 Volume 操作）分隔開來。有關每個系統管理員群組允許的權限，請參閱 Google Cloud NetApp Volumes 文件中的 "安全注意事項"。

Google Cloud NetApp Volumes備份

儘管Google Cloud NetApp Volumes提供了高資料持久性，但外部事件可能會導致資料遺失。如果發生病毒或勒索軟體等安全事件，備份和復原對於及時恢復資料存取至關重要。管理員可能會意外刪除Google Cloud NetApp Volumes磁碟區。或者用戶只是想將其資料的備份版本保留數月，而保留卷內的額外 Snapshot 副本空間則成為一項成本挑戰。儘管 Snapshot 副本應該是保留過去幾週的備份版本以從中恢復遺失資料的首選方式，但它們位於磁碟區內，如果磁碟區消失，它們也會遺失。

基於上述所有原因，Google Cloud NetApp Volumes 透過 "Google Cloud NetApp Volumes備份"提供備份服務。

Google Cloud NetApp Volumes備份會在 Google Cloud Storage (GCS) 上產生該磁碟區的副本。它僅備份卷內儲存的實際數據，而不是可用空間。它永遠以增量方式工作，這意味著它傳輸一次卷內容，然後從那時起繼續僅備份更改的資料。與具有多次完整備份的傳統備份概念相比，它節省了大量的備份存儲，從而降低了成本。由於備份空間的月費與磁碟區相比較低，因此它是長期保存備份版本的理想場所。

使用者可以使用Google Cloud NetApp Volumes備份將任何備份版本還原到同一區域內的相同或不同磁碟區。如果刪除來源卷，備份資料將保留，並且需要單獨管理（例如，刪除）。

Google Cloud NetApp Volumes 備份是以選項形式內建於 Google Cloud NetApp Volumes 中。使用者可透過以每個 Volume 為單位啟用 Google Cloud NetApp Volumes 備份，來決定要保護哪些 Volume。請參閱 "Google Cloud NetApp Volumes備份文檔"以取得有關備份、 "支援的最大備份版本數量"、排程及 "定價"的相關資訊。

專案的所有備份資料都儲存在 GCS 儲存桶中，該儲存桶由服務管理，使用者不可見。每個項目使用不同的儲存桶。目前，這些儲存桶與Google Cloud NetApp Volumes磁碟區位於同一區域，但正在討論更多選項。查閱文件以了解最新狀態。

從Google Cloud NetApp Volumes儲存桶到 GCS 的資料傳輸使用具有 HTTPS 和 TLS1.2 的服務內部 Google 網路。資料使用 Google 管理的金鑰進行靜態加密。

若要管理 Google Cloud NetApp Volumes 備份（建立、刪除和還原備份），使用者必須具有 "roles/netapp.admin" 角色。

概況

信任雲端解決方案的一部分是了解其架構及其安全性方式。本節介紹了 Google 中Google Cloud NetApp Volumes架構的不同方面，以幫助緩解有關資料安全方式的潛在擔憂，並指出可能需要額外配置步驟才能獲得最安全部署的區域。

Google Cloud NetApp Volumes的整體架構可分為兩個主要元件：控制平面和資料平面。

控制平面

Google Cloud NetApp Volumes中的控制平面是由Google Cloud NetApp Volumes管理員和NetApp原生自動化軟體管理的後端基礎架構。此平面對最終用戶完全透明，包括網路、儲存硬體、軟體更新等，以協助為Google Cloud NetApp Volumes等雲端駐留解決方案提供價值。

數據平面

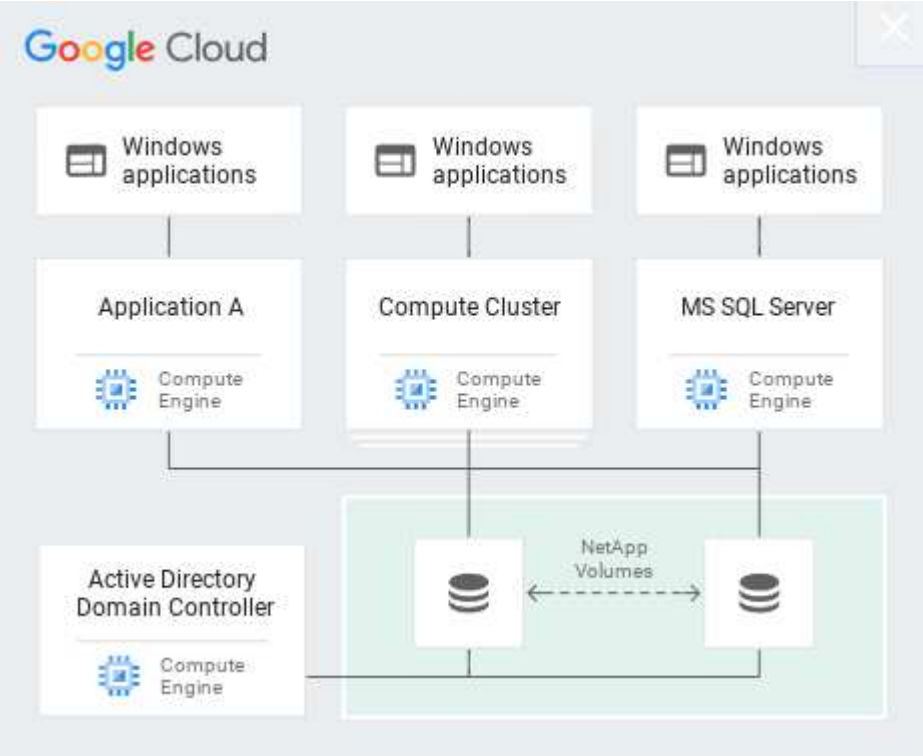
Google Cloud NetApp Volumes中的資料平麵包括實際資料磁碟區和整體Google Cloud NetApp Volumes設定（例如存取控制、Kerberos 驗證等）。資料平面完全由Google Cloud NetApp Volumes平台的最終使用者和消費者控制。

每架飛機的安全和管理方式都有明顯差異。以下部分將介紹這些差異，首先介紹Google Cloud NetApp Volumes架構概述。

Google Cloud NetApp Volumes架構

與 CloudSQL、Google Cloud VMware Engine (GCVE) 和 FileStore 等其他 Google Cloud 原生服務類似， Google Cloud NetApp Volumes使用 "谷歌公益廣告"來提供服務。在 PSA 中，服務是在服務生產者專案內部建構的，該專案使用 "VPC 網路對等連接"連接到服務消費者。服務生產者由NetApp提供和經營，服務消費者是客戶專案中的 VPC，託管想要存取Google Cloud NetApp Volumes檔案共享的用戶端。

下圖參考自 "Google Cloud NetApp Volumes 說明文件"，概述了高層次的視圖。



虛線上方部分顯示了服務的控制平面，它控制著卷的生命週期。虛線以下部分錶示資料平面。左邊藍色框表示使用者VPC（服務消費者），右邊藍色框表示NetApp提供的服務生產者。兩者透過 VPC 對等連接。

在Google Cloud NetApp Volumes中，單一專案被視為唯一的租用戶。這意味著對磁碟區、Snapshot 副本等的操作都是基於每個專案執行的。換句話說，所有磁碟區都歸創建它們的專案所有，並且預設只有該專案可以管理和存取其中的資料。這被認為是服務的控制平面視圖。

共享 **VPC**

在資料平面視圖上， Google Cloud NetApp Volumes可以連接到共用 VPC。您可以在託管專案或連接到共用 VPC 的某個服務專案中建立磁碟區。連接到該共用 VPC 的所有項目（主機或服務）都能夠存取網路層（TCP/IP）的磁碟區。由於共用 VPC 上具有網路連線的所有用戶端都可以透過 NAS 協定存取數據，因此必須使用單一磁碟區上的存取控制（例如使用者/群組存取控制清單 (ACL) 和 NFS 匯出的主機名稱/IP 位址）來控制誰可以存取資料。

每個客戶專案最多可以將Google Cloud NetApp Volumes連接到五個 VPC。在控制平面上，該專案使您能夠管理所有建立的捲，無論它們連接到哪個 VPC。在資料平面上，VPC之間相互隔離，每個磁碟區只能連接到一個VPC。

對各個磁碟區的存取由特定協定（NFS/SMB）存取控制機制控制。

換句話說，在網路層，所有連接到共享 VPC 的項目都能夠看到該卷，而在管理端，控制平面只允許所有者專案看到該卷。

VPC 服務控制

VPC 服務控制在連接到網際網路且可在全球範圍內存取的 Google Cloud 服務周圍建立存取控制邊界。這些服務透過使用者身分提供存取控制，但無法限制請求來自哪個網路位置。 VPC 服務控制透過引入限制對定義網路的存取的功能來彌補這一差距。

Google Cloud NetApp Volumes資料平面並未連接到外部互聯網，而是連接到具有明確定義的網路邊界（週邊）的私人 VPC。在該網路中，每個磁碟區都使用特定於協定的存取控制。任何外部網路連線均由 Google Cloud 專案管理員明確建立。然而，控制平面不提供與資料平面相同的保護，任何人都可以從任何地方透過有效憑證進行存取（ "JWT 令牌" ）。

簡而言之， Google Cloud NetApp Volumes資料平面提供了網路存取控制功能，而無需支援 VPC Service Controls，也不明確使用 VPC Service Controls。

資料包嗅探/追蹤注意事項

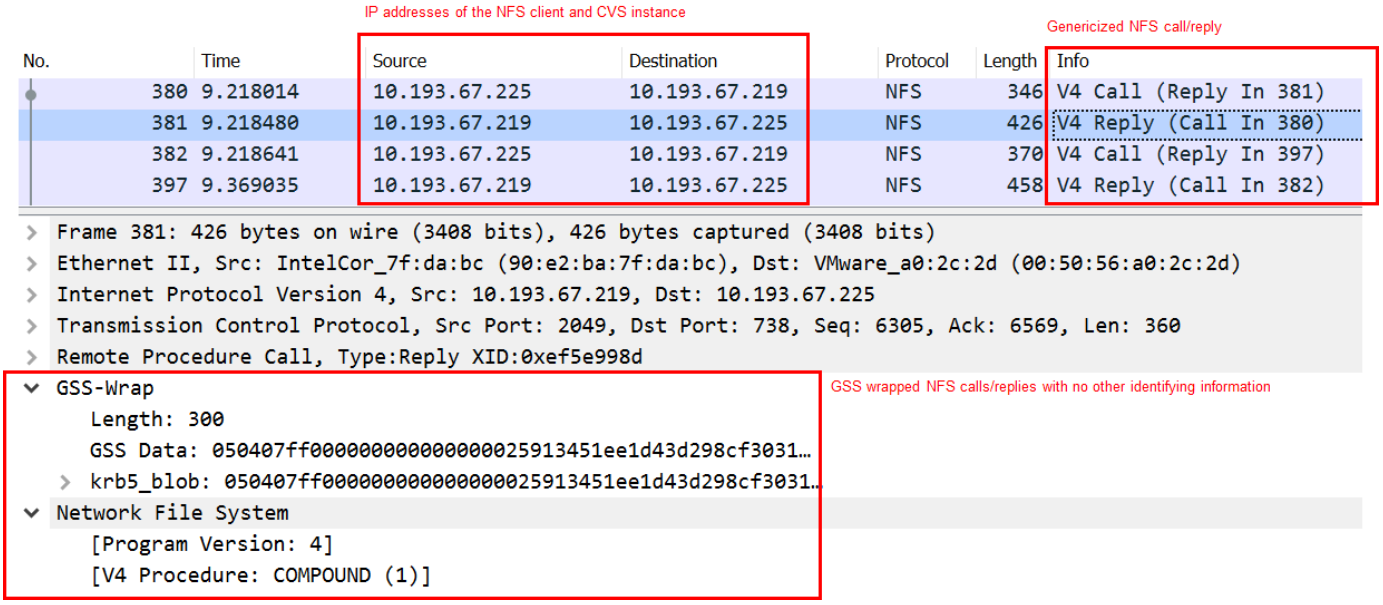
封包擷取可用於解決網路問題或其他問題（例如 NAS 權限、LDAP 連線等），但也可能被惡意用於取得有關網路 IP 位址、MAC 位址、使用者和群組名稱以及端點上使用的安全等級的資訊。由於 Google Cloud 網路、VPC 和防火牆規則的配置方式，如果沒有使用者登入憑證或"JWT 令牌"進入雲端實例。封包擷取僅可在端點（例如虛擬機器 (VM)）上進行，並且僅可在 VPC 內部的端點上進行，除非使用共用 VPC 和/或外部網路隧道/IP 轉送明確允許外部流量到端點。沒有辦法嗅探客戶端以外的流量。

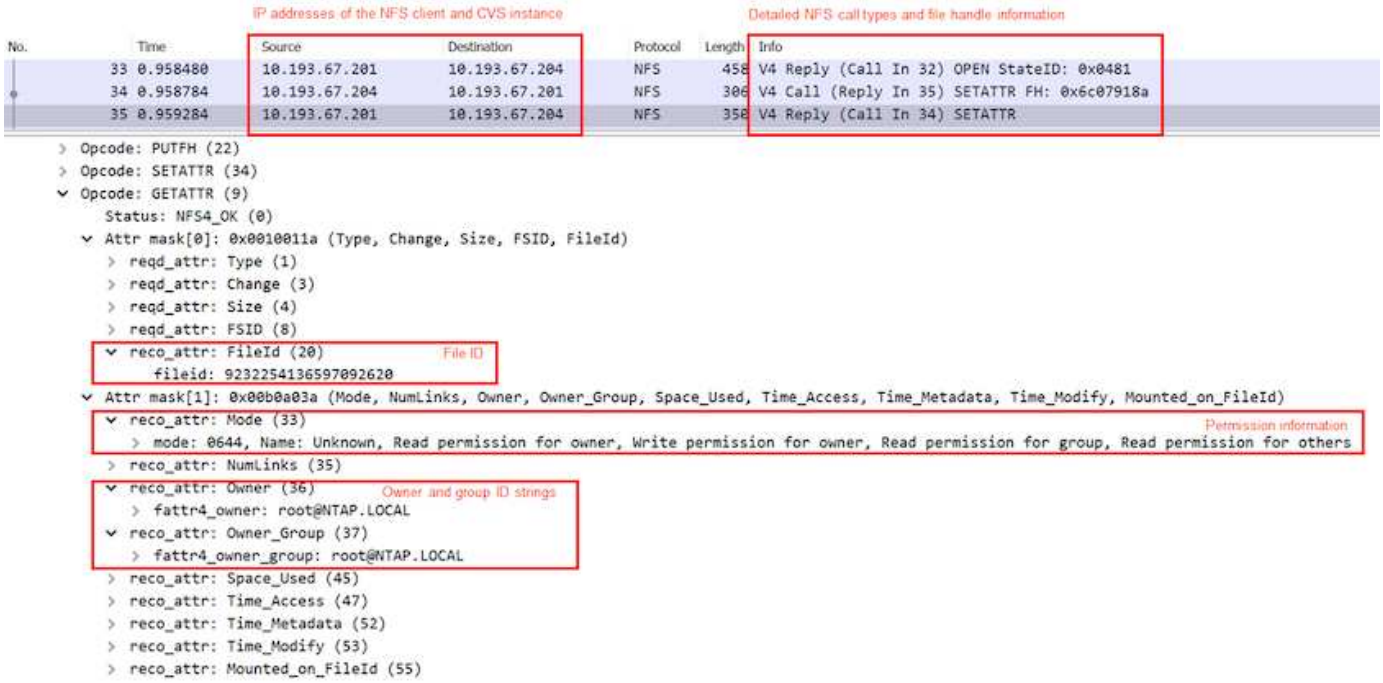
使用共用 VPC 時，使用 NFS Kerberos 和/或"SMB 加密"可以掩蓋從痕跡中收集到的大量資訊。然而，有些流量仍然以明文形式發送，例如"DNS"和"LDAP 查詢"。下圖顯示了來自Google Cloud NetApp Volumes的純文字 LDAP 查詢的封包擷取以及可能暴露的識別資訊。 Google Cloud NetApp Volumes中的 LDAP 查詢目前不支援加密或 LDAP over SSL。如果 Active Directory 要求， NetApp Volumes-Performance 支援 LDAP 簽章。 NetApp Volumes-SW 不支援 LDAP 簽章。



unixUserPassword 由 LDAP 查詢，並且不是以純文字形式發送，而是以加鹽哈希形式發送。預設情況下，Windows LDAP 不會填入 unixUserPassword 欄位。只有當您需要利用 Windows LDAP 透過 LDAP 互動式登入用戶端時才需要此欄位。 Google Cloud NetApp Volumes不支援實例的互動式 LDAP 登入。

下圖顯示了從 NFS Kerberos 對話擷取的封包以及透過 AUTH_SYS 擷取的 NFS 封包。請注意兩者之間追蹤中可用的資訊有何不同，以及啟用飛行中加密如何為 NAS 流量提供更高的整體安全性。





虛擬機器網路介面

攻擊者可能會嘗試的一個技巧是向虛擬機器新增新的網路介面卡 (NIC) "混雜模式" （連接埠鏡像）或在現有 NIC 上啟用混雜模式以嗅探所有流量。在 Google Cloud 中，新增新的 NIC 需要完全關閉 VM，這會建立警報，因此攻擊者無法不被注意地執行此操作。

此外，NIC 根本無法設定為混雜模式，否則會在 Google Cloud 中觸發警報。

控制平面架構

對Google Cloud NetApp Volumes 的所有管理作業均透過 API 完成。整合到 GCP Cloud Console 中的Google Cloud NetApp Volumes管理也使用Google Cloud NetApp Volumes API。

身分和存取管理

身分和存取管理("我是") 是一項標準服務，可讓您控制對 Google Cloud 專案執行個體的驗證（登入）和授權（權限）。 Google IAM 提供權限授權和刪除的完整稽核追蹤。目前， Google Cloud NetApp Volumes不提供控制平面稽核。

授權/許可概述

IAM 為 Google Cloud NetApp Volumes 提供內建的精細權限。您可以找到 "此處有詳細的權限完整列表"。

IAM 還提供了兩個預定義角色，稱為 `netappcloudvolumes.admin`和 `netappcloudvolumes.viewer`。這些角色可以指派給特定使用者或服務帳戶。

指派適當的角色和權限以允許 IAM 使用者管理Google Cloud NetApp Volumes。

使用細粒度權限的範例包括：

- 建置僅具有取得/列出/建立/更新權限的自訂角色，以便使用者無法刪除磁碟區。
- 使用僅具有 `snapshot.*`建立用於建立應用程式一致的快照整合的服務帳戶的權限。
- 建立自訂角色以進行委派 `volumereplication.*`針對特定用戶。

服務帳戶

透過腳本Google Cloud NetApp Volumes "地形"，您必須建立一個服務帳戶 `roles/netappcloudvolumes.admin` 角色。您可以使用此服務帳戶以兩種不同的方式產生驗證Google Cloud NetApp Volumes API 請求所需的 JWT 令牌：

- 產生 JSON 金鑰並使用 Google API 從中派生出 JWT 令牌。這是最簡單的方法，但它涉及手動機密（JSON 金鑰）管理。
- 使用 "服務帳戶模擬"和 `roles/iam.serviceAccountTokenCreator`。程式碼（腳本、Terraform 等）運行 "應用程式預設憑證"並模擬服務帳戶以取得其權限。這種方法體現了 Google 安全最佳實踐。

如需詳細資訊，請參閱 Google Cloud 文件中的 "建立您的服務帳戶和私鑰"。

Google Cloud NetApp VolumesAPI

Google Cloud NetApp Volumes API 使用基於 REST 的 API，並以 HTTPS（TLSv1.2）作為底層網路傳輸。您可以在 "Google 雲端文件中的 Cloud Volumes API"找到最新的 API 定義與如何使用 API 的資訊。

NetApp使用標準 HTTPS（TLSv1.2）功能來操作和保護 API 端點。

JWT 令牌

使用 JWT 承載令牌執行 API 驗證("RFC-7519"）。必須使用 Google Cloud IAM 驗證來取得有效的 JWT 令牌。這必須透過提供服務帳戶 JSON 金鑰從 IAM 取得令牌來完成。

審計日誌

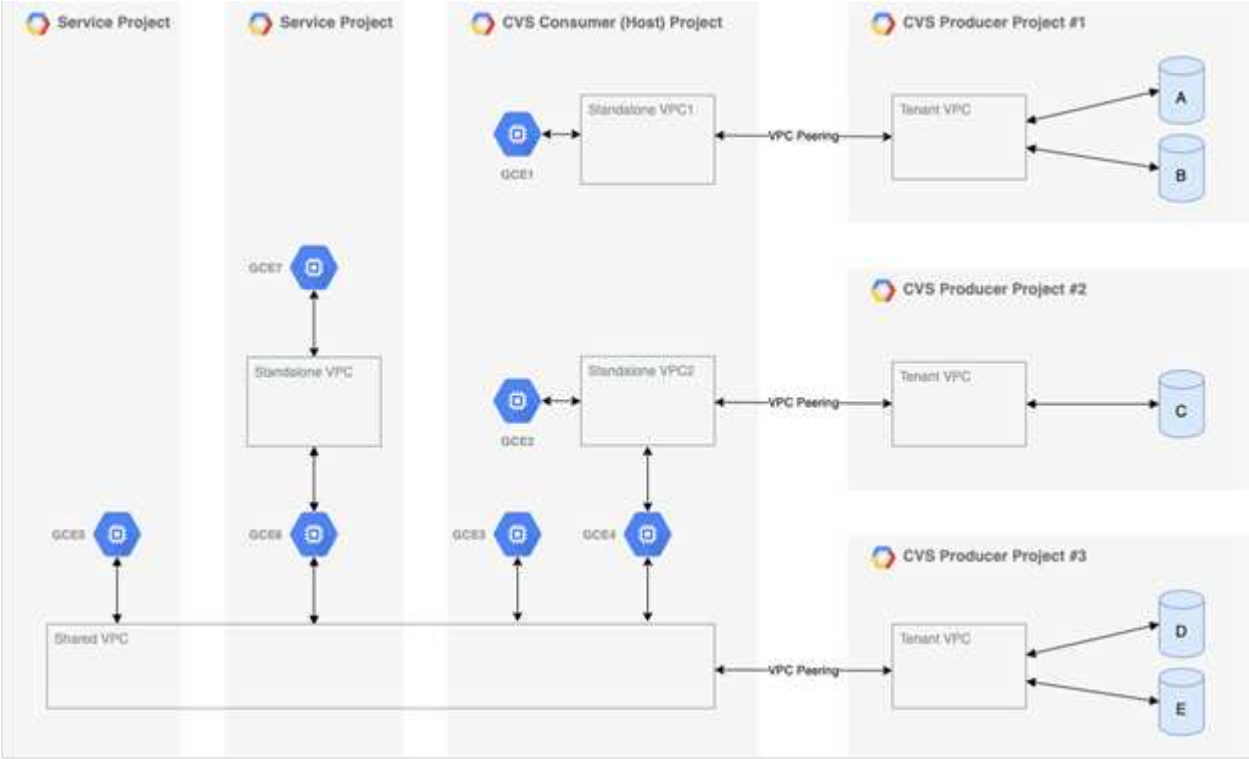
目前，沒有可供使用者存取的控制平面稽核日誌。

資料平面架構

Google Cloud NetApp Volumes for Google Cloud 利用 Google Cloud "私人服務訪問"框架。在這個框架中，使用者可以連接到Google Cloud NetApp Volumes。該框架像其他 Google Cloud 服務一樣使用服務網路和 VPC 對等結構，確保租戶之間的完全隔離。

如需 Google Cloud NetApp Volumes for Google Cloud 的架構總覽，請參閱 "Google Cloud NetApp Volumes的架構"。

使用者 VPC（獨立或共用）與託管磁碟區的Google Cloud NetApp Volumes管理租用戶專案內的 VPC 對等。



上圖展示了一個專案（中間的NetApp Volumes 消費者專案），其中有三個 VPC 網路連接到Google Cloud NetApp Volumes ，並且多個 Compute Engine VM（GCE1-7）共用磁碟區：

- VPC1 允許 GCE1 存取卷 A 和 B。
- VPC2 允許 GCE2 和 GCE4 存取卷 C。
- 第三個VPC網路是共享VPC，由兩個服務項目共享。它允許 GCE3、GCE4、GCE5 和 GCE6 訪問卷 D 和 E。共享 VPC 網路僅支援NetApp Volumes-Performance 服務類型的磁碟區。

GCE7 無法存取任何磁碟區。

資料可以在Google Cloud NetApp Volumes中傳輸（使用 Kerberos 和/或 SMB 加密）和靜止時加密。

傳輸中的資料加密

傳輸中的資料可以在 NAS 協定層加密，而 Google Cloud 網路本身也經過加密，如以下部分所述。

Google Cloud 網路

Google Cloud 在網路層級加密流量，具體說明如下 "傳輸中加密"在 Google 文件中。正如「Google Cloud NetApp Volumes架構」部分所述， Google Cloud NetApp Volumes是由NetApp控制的 PSA 生產商專案提供的。

對於NetApp Volumes-SW，生產者租用戶執行 Google VM 來提供服務。用戶虛擬機器和Google Cloud NetApp Volumes虛擬機器之間的流量由 Google 自動加密。

儘管NetApp Volumes-Performance 的資料路徑在網路層上並未完全加密，但NetApp和 Google 結合使用 "IEEE 802.1AE 加密 (MACSec)"， "封裝" （資料加密）和實體受限的網路來保護Google Cloud NetApp Volumes

NetApp Volumes-Performance 服務類型和 Google Cloud 之間傳輸的資料。

NAS 協定

NFS 和 SMB NAS 協定在協定層提供可選的傳輸加密。

SMB 加密

"SMB 加密"提供 SMB 資料的端對端加密，並保護資料免受不受信任網路上的竊聽。您可以為用戶端/伺服器資料連線（僅適用於支援 SMB3.x 的用戶端）和伺服器/網域控制站驗證啟用加密。

啟用 SMB 加密後，不支援加密的用戶端無法存取共用。

Google Cloud NetApp Volumes支援 SMB 加密的 RC4-HMAC、AES-128-CTS-HMAC-SHA1 和 AES-256-CTS-HMAC-SHA1 安全密碼。 SMB 協商伺服器支援的最高加密類型。

NFSv4.1 Kerberos

對於 NFSv4.1， NetApp Volumes-Performance 提供 Kerberos 驗證，如 "RFC7530"。您可以按磁碟區啟用 Kerberos。

Kerberos 目前最強大的加密類型是 AES-256-CTS-HMAC-SHA1。 Google Cloud NetApp Volumes支援 NFS 的 AES-256-CTS-HMAC-SHA1、AES-128-CTS-HMAC-SHA1、DES3 和 DES。它也支援用於 CIFS/SMB 流量的 ARCFOUR-HMAC (RC4)，但不支援用於 NFS。

Kerberos 為 NFS 掛載提供了三種不同的安全級別，可供您選擇 Kerberos 安全性的強度。

根據 RedHat 的 "常見安裝選項"文件:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

一般來說，Kerberos 安全等級要做的工作越多，效能就越差，因為客戶端和伺服器要花時間對發送的每個資料包進行加密和解密 NFS 操作。許多用戶端和 NFS 伺服器都支援將 AES-NI 卸載到 CPU 以獲得更好的整體體驗，但 Kerberos 5p（完全端對端加密）對效能的影響明顯大於 Kerberos 5（用戶身份驗證）的影響。

下表顯示了每個等級在安全性和效能方面的差異。

安全等級	安全	表現
NFSv3—系統	• 最不安全；帶有數位使用者 ID/群組 ID 的純文字 • 能夠在封包擷取中查看UID 、GID、客戶端IP位址、匯出路徑、檔案名稱、權限	• 最適合大多數情況
NFSv4.x—系統	• 比 NFSv3 更安全（客戶端 ID、名稱字串/域字串匹配），但仍然是純文本 • 能夠查看封包擷取中的 UID 、GID、客戶端 IP 位址、名稱字串、網域 ID、匯出路徑、檔案名稱、權限	• 適用於順序工作負載（例如虛擬機器、資料庫、大型檔案） • 文件數量多/元資料多時效果不佳（差 30-50%）
NFS—krb5	• 對每個 NFS 封包中的憑證進行 Kerberos 加密 - 在 GSS 包裝器中包裝 RPC 呼叫中使用者/群組的 UID/GID • 請求訪問掛載的使用者需要有效的 Kerberos 票證（透過使用者名稱/密碼或手動金鑰標籤交換）；票證在指定時間段後過期，使用者必須重新進行身份驗證才能存取 • NFS 操作或輔助協定（如 mount/portmapper/nlm）沒有加密（可在封包擷取中查看匯出路徑、IP 位址、檔案句柄、權限、檔案名稱、atime/mtime）	• 在大多數情況下，Kerberos 是最佳選擇；但比 AUTH_SYS 差
NFS—krb5i	• 對每個 NFS 封包中的憑證進行 Kerberos 加密 - 在 GSS 包裝器中包裝 RPC 呼叫中使用者/群組的 UID/GID • 請求訪問掛載的使用者需要有效的 Kerberos 票證（透過使用者名稱/密碼或手動金鑰標籤交換）；票證在指定時間段後過期，使用者必須重新進行身份驗證才能存取 • NFS 操作或輔助協定（如 mount/portmapper/nlm）沒有加密（可在封包擷取中查看匯出路徑、IP 位址、檔案句柄、權限、檔案名稱、atime/mtime） • 每個資料包都新增了 Kerberos GSS 校驗和，以確保沒有任何東西攔截資料包。如果校驗和匹配，則允許對話。	• 比 krb5p 更好，因為 NFS 有效負載未加密；與 krb5 相比唯一增加的開銷是完整性校驗和。krb5i 的表現不會比 krb5 差太多，但會有一些下降。

安全等級	安全	表現
NFS – krb5p	• 對每個 NFS 封包中的憑證進行 Kerberos 加密 - 在 GSS 包裝器中包裝 RPC 呼叫中使用者/群組的 UID/GID • 請求訪問掛載的使用者需要有效的 Kerberos 票證（透過使用者名稱/密碼或手動金鑰表交換）；票證在指定時間段後過期，使用者必須重新進行身份驗證才能存取 • 所有 NFS 封包有效負載都使用 GSS 包裝器加密（在封包擷取中看不到檔案句柄、權限、檔案名稱、atime/mtime）。 • 包括完整性檢查。 • NFS 操作類型可見（FSINFO、ACCESS、GETATTR 等）。 • 輔助協定（mount、portmap、nlm 等）未加密 - （可以看到匯出路徑、IP 位址）	• 安全等級效能最差；krb5p 必須進行更多加密/解密。 • 對於高檔案數工作負載，效能比使用 NFSv4.x 的 krb5p 更好。

在Google Cloud NetApp Volumes中，設定的 Active Directory 伺服器用作 Kerberos 伺服器和 LDAP 伺服器（從 RFC2307 相容模式中尋找使用者身分）。不支援其他 Kerberos 或 LDAP 伺服器。 NetApp強烈建議您在Google Cloud NetApp Volumes中使用 LDAP 進行身分識別管理。有關 NFS Kerberos 在封包擷取中如何顯示的信息，請參閱部分 "Packet sniffing/trace considers."

靜態資料加密

Google Cloud NetApp Volumes中的所有磁碟區均使用 AES-256 加密進行靜態加密，這表示寫入媒體的所有使用者資料都經過加密，並且只能使用每個磁碟區的金鑰解密。

- 對於NetApp Volumes-SW，使用 Google 產生的金鑰。
- 對於NetApp Volumes-Performance，每個磁碟區的金鑰都儲存在Google Cloud NetApp Volumes內建的金鑰管理器中。

從 2021 年 11 月開始，預覽客戶管理加密金鑰 (CMEK) 功能已推出。這使得您可以使用託管在以下位置的每個項目、每個區域的主密鑰來加密每個卷密鑰： "Google 金鑰管理服務 (KMS)。" KMS 可讓您附加外部金鑰管理員。

有關設定 NetApp Volumes-Performance 的 KMS 資訊，請參閱 "設定客戶管理的加密金鑰"。

防火牆

Google Cloud NetApp Volumes公開多個 TCP 連接埠來為 NFS 和 SMB 共用提供服務：

- "NFS 存取所需的連接埠"
- "SMB 存取所需的連接埠"

此外，SMB、包含 Kerberos 的 LDAP 的 NFS 以及雙協定組態需要存取 Windows Active Directory 網域。Active Directory 連線必須 "配置"以每個區域為基礎。Active Directory 網域控制站（DC）是使用 "基於 DNS 的 DC 發現"透過指定的 DNS 伺服器來識別。系統會使用傳回的任何 DC。可以透過指定 Active Directory 站台來限制符合條件的 DC 清單。

Google Cloud NetApp Volumes 使用透過 `gcloud compute address`命令指派的 CIDR 範圍內的 IP 位址進行通訊 "加入Google Cloud NetApp Volumes"。您可以將此 CIDR 用作來源位址，為 Active Directory 網域控制站設定傳入防火牆。

Active Directory 網域控制站必須 "如這裡所述，將連接埠暴露給Google Cloud NetApp Volumes CIDR"。

NAS 協定概述

NAS 協定包括 NFS（v3 和 v4.1）和 SMB/CIFS（2.x 和 3.x）。這些協定是NetApp Volumes 允許跨多個 NAS 用戶端共用存取資料的方式。此外， Google Cloud NetApp Volumes可以同時提供對 NFS 和 SMB/CIFS 用戶端的存取（雙協定），同時遵守 NAS 共用中檔案和資料夾的所有身分和權限設定。為了維持最高的資料傳輸安全性， Google Cloud NetApp Volumes支援使用 SMB 加密和 NFS Kerberos 5p 進行飛行中的協定加密。

雙協定僅適用於NetApp Volumes-Performance。

NAS 協定基礎知識

NAS 協定是網路上的多個用戶端存取儲存系統上的相同資料的方式，例如 GCP 上的Google Cloud NetApp Volumes 。 NFS 和 SMB 是定義的 NAS 協議，在客戶端/伺服器基礎上運行，其中Google Cloud NetApp Volumes充當伺服器。客戶端向伺服器發送存取、讀取和寫入請求，伺服器負責協調文件的鎖定機制、儲存權限以及處理身份和身份驗證請求。

例如，如果 NAS 用戶端想要在資料夾中建立新文件，請遵循以下一般流程。

1. 客戶端向伺服器詢問有關目錄的資訊（權限、擁有者、群組、文件 ID、可用空間等）；如果請求的客戶端和使用者對父資料夾具有必要的權限，則伺服器會回應該資訊。
2. 如果目錄的權限允許訪問，客戶端就會詢問伺服器正在建立的檔案名稱是否已經存在於檔案系統中。如果檔案名稱已被使用，則建立失敗。如果檔案名稱不存在，伺服器會讓客戶端知道可以繼續。
3. 客戶端向伺服器發出調用，使用目錄句柄和文件名建立文件，並設定存取和修改時間。伺服器為文件發出唯一的文件 ID，以確保沒有其他文件使用相同的文件 ID 建立。
4. 客戶端在 WRITE 操作之前傳送呼叫來檢查檔案屬性。如果權限允許，客戶端就會寫入新檔案。如果協定/應用程式使用了鎖定，用戶端會向伺服器請求鎖定，以防止其他用戶端在鎖定時存取文件，從而防止資料損壞。

NFS

NFS 是一種分散式檔案系統協議，它是請求評論 (RFC) 中定義的開放 IETF 標準，允許任何人實現該協議。

Google Cloud NetApp Volumes中的磁碟區透過匯出用戶端或一組用戶端可存取的路徑共用給 NFS 用戶端。安裝這些匯出的權限由匯出原則和規則定義，可由Google Cloud NetApp Volumes管理員設定。

NetApp NFS 實施被認為是該協議的黃金標準，並應用於無數企業 NAS 環境。以下部分介紹Google Cloud NetApp Volumes中提供的 NFS 和特定安全功能及其實作方式。

預設本機 UNIX 使用者和群組

Google Cloud NetApp Volumes包含幾個用於各種基本功能的預設 UNIX 使用者和群組。目前無法修改或刪除這些使用者和群組。目前無法將新的本機使用者和群組新增至Google Cloud NetApp Volumes。預設使用者和群組以外的 UNIX 使用者和群組需要由外部 LDAP 名稱服務提供。

下表顯示了預設使用者和群組及其對應的數字 ID。 NetApp建議不要在 LDAP 中或重複使用這些數位 ID 的本機用戶端上建立新的使用者或群組。

預設用戶：數字 **ID**	預設群組：數字 **ID**
• 根：0 • pcuser：65534 • 無人：65535	• 根：0 • 守護程式：1 • pcuser：65534 • 無人：65535

使用 NFSv4.1 時，root 使用者在 NFS 用戶端上執行目錄清單指令時可能會顯示為 nobody。這是由於客戶端的ID域映射配置造成的。請參閱名為NFSv4.1 和 nobody 使用者/群組有關此問題及其解決方法的詳細資訊。

根用戶

在 Linux 中，root 帳號可以存取基於 Linux 的檔案系統中所有指令、檔案和資料夾。由於此帳戶的強大功能，安全最佳實踐通常要求以某種方式停用或限制根用戶。在 NFS 匯出中，可以透過匯出策略和規則以及稱為 root squash 的概念在Google Cloud NetApp Volumes中控制 root 使用者對檔案和資料夾的權限。

Root 壓縮確保存取 NFS 掛載的 root 使用者被壓縮為匿名數位使用者 65534（請參閱“[匿名用戶] "），目前僅在使用NetApp Volumes-Performance 時可用，方法是在建立匯出策略規則期間選擇關閉 root 存取權。如果 root 用戶被壓縮為匿名用戶，則它不再具有運行 chown 或 "setuid/setgid 指令（黏滯位）"在 NFS 掛載中的檔案或資料夾上，以及由 root 使用者建立的檔案或資料夾顯示匿名 UID 作為擁有者/群組。此外，root 使用者無法修改 NFSv4 ACL。但是，root 使用者仍然可以存取 chmod 並刪除其沒有明確權限的檔案。如果要限制對 root 使用者的檔案和資料夾權限的訪問，請考慮使用具有 NTFS ACL 的捲，建立名為 `root`並將所需的權限套用到檔案或資料夾。

匿名用戶

匿名 (anon) 使用者 ID 指定對應到沒有有效 NFS 憑證的用戶端請求的 UNIX 使用者 ID 或使用者名稱。當使用 root 壓縮時，這可以包括 root 使用者。 Google Cloud NetApp Volumes的匿名使用者是 65534。

此 UID 通常與使用者名稱相關聯 `nobody`或者 `nfsnobody`在 Linux 環境中。 Google Cloud NetApp Volumes也使用 65534 作為本機 UNIX 使用者 `pcuser`（請參閱“預設本機 UNIX 使用者和群組 "），當在 LDAP 中找不到有效符合的 UNIX 使用者時，它也是 Windows 到 UNIX 名稱對應的預設後備使用者。

由於 Linux 和Google Cloud NetApp Volumes中 UID 65534 的使用者名稱有差異，因此使用 NFSv4.1 時對應到 65534 的使用者的名稱字串可能不符。因此，你可能會看到 `nobody`作為某些文件和資料夾的使用者。請參閱 “NFSv4.1 和 nobody 使用者/群組 「以獲取有關此問題及其解決方法的資訊。

存取控制/導出

NFS 掛載的初始導出/共享存取透過導出策略中包含的基於主機的導出策略規則進行控制。定義主機 IP、主機名稱、子網路、網路群組或網域以允許存取掛載 NFS 共用以及允許對主機的存取等級。匯出策略規則設定選項取決於Google Cloud NetApp Volumes等級。

對於NetApp Volumes-SW，以下選項可用於匯出策略配置：

- *客戶匹配。 *以逗號分隔的 IP 位址清單、以逗號分隔的主機名稱、子網路、網路群組、網域名稱清單。
- *RO/RW 存取規則。 *選擇讀取/寫入或唯讀來控制導出的存取等級。 NetApp NetApp -Performance 提供以下選項：
- *客戶匹配。 *以逗號分隔的 IP 位址清單、以逗號分隔的主機名稱、子網路、網路群組、網域名稱清單。
- *RO/RW 存取規則。 *選擇讀取/寫入或唯讀來控制導出的存取等級。
- *Root 存取權限（開/關）。 *配置根壁球（請參閱“[根用戶] 」以了解詳情）。
- *協定類型。 *這會將對 NFS 掛載的存取限製到特定的協定版本。當為磁碟區同時指定 NFSv3 和 NFSv4.1 時，請將兩者留空或選取兩個方塊。
- *Kerberos 安全性等級（選擇「啟用 Kerberos」時）。 *提供 krb5、krb5i 和/或 krb5p 選項以進行唯讀或讀寫存取。

更改所有權（**chown**）和更改組（**chgrp**）

Google Cloud NetApp Volumes上的 NFS 僅允許 root 使用者對檔案和資料夾執行 chown/chgrp。其他用戶看到 `Operation not permitted`錯誤——即使是他們自己的文件。如果你使用根南瓜（如“[根用戶] "），root 被壓縮為非 root 用戶，不允許存取 chown 和 chgrp。目前， Google Cloud NetApp Volumes中沒有允許非 root 使用者使用 chown 和 chgrp 的解決方法。如果需要變更所有權，請考慮使用雙協定磁碟區並將安全樣式設定為 NTFS 以從 Windows 端控制權限。

權限管理

Google Cloud NetApp Volumes支援模式位元（例如 rwx 的 644、777 等）和 NFSv4.1 ACL，以控制使用 UNIX 安全樣式的磁碟區的 NFS 用戶端權限。這些使用標準權限管理（例如 chmod、chown 或 nfs4_setfacl）並可與任何支援它們的 Linux 用戶端一起使用。

此外，當使用設定為 NTFS 的雙協定磁碟區時，NFS 用戶端可以利用Google Cloud NetApp Volumes名稱對應到 Windows 用戶，然後用於解析 NTFS 權限。這需要與Google Cloud NetApp Volumes建立 LDAP 連線以提供數位 ID 到使用者名稱的轉換，因為Google Cloud NetApp Volumes需要有效的 UNIX 使用者名稱才能正確對應到 Windows 使用者名稱。

為 **NFSv3** 提供細粒度的 **ACL**

模式位元權限在語義上僅涵蓋擁有者、群組和其他所有人 - 這意味著基本 NFSv3 沒有細粒度的使用者存取控制。 Google Cloud NetApp Volumes不支援 POSIX ACL 和擴充屬性（例如 chattr），因此細粒度 ACL 僅在以下使用 NFSv3 的場景中可用：

- 具有有效 UNIX 到 Windows 使用者對應的 NTFS 安全樣式磁碟區（需要 CIFS 伺服器）。
- 使用安裝 NFSv4.1 的管理用戶端套用 NFSv4.1 ACL 來套用 ACL。

兩種方法都需要 LDAP 連線來進行 UNIX 身分識別管理，並填入有效的 UNIX 使用者和群組資訊（請參閱"LDAP") 並且僅適用於NetApp Volumes-Performance 實例。若要將 NTFS 安全樣式磁碟區與 NFS 一起使用，您必須使用雙協定（SMB 和 NFSv3）或雙協定（SMB 和 NFSv4.1），即使沒有建立 SMB 連線。若要將

NFSv4.1 ACL 與 NFSv3 掛載一起使用，您必須選擇 `Both (NFSv3/NFSv4.1)`作為協定類型。

常規 UNIX 模式位元不提供與 NTFS 或 NFSv4.x ACL 相同的權限粒度。下表比較了 NFSv3 模式位元和 NFSv4.1 ACL 之間的權限粒度。有關 NFSv4.1 ACL 的信息，請參閱 "nfs4_acl - NFSv4 存取控制列表"。

NFSv3 模式位	**NFSv4.1 ACL**
• 執行時設定使用者 ID • 執行時設定群組 ID • 儲存交換的文字（POSIX 中未定義） • 所有者的讀取權限 • 所有者的寫入權限 • 執行檔案擁有者的權限；或在目錄中尋找（搜尋）擁有者的權限 • 群組的讀取權限 • 群組的寫入權限 • 執行檔案上的群組的權限；或在目錄中尋找（搜尋）群組的權限 • 其他人的閱讀權限 • 授予他人寫入權限 • 為其他人在文件上執行權限；或在目錄中尋找（搜尋）其他人的權限	存取控制條目 (ACE) 類型（允許/拒絕/審核）* 繼承標誌* 目錄繼承* 檔案繼承* 不傳播繼承* 僅繼承 ACL * 讀取資料（檔案）/列出目錄（目錄） * 寫入資料（檔案）/建立檔案（目錄） * 附加資料（檔案）/建立子目錄（目錄） * 執行（檔案）/變更目錄（目錄） * 刪除 * 刪除子項目 * 讀取屬性權限 *寫入屬性 * 讀取命名屬性 * 寫入屬性 * 刪除 * 刪除子項目 * 讀取屬性權限 *寫入屬性 * 讀取命名屬性 * 寫入屬性 * 命名屬性 *

最後，根據 RPC 封包限制，NFS 群組成員資格（在 NFSv3 和 NFSV4.x 中）對於 AUTH_SYS 的預設最大值限制為 16。 NFS Kerberos 提供最多 32 個群組，NFSv4 ACL 透過細粒度的使用者和群組 ACL（每個 ACE 最多 1024 個條目）消除了限制。

此外，Google Cloud NetApp Volumes 提供擴充群組支援，可將支援的最大群組數擴充至 32 個。這需要與包含有效 UNIX 使用者和群組身分的 LDAP 伺服器建立 LDAP 連線。如需設定此功能的詳細資訊，請參閱 Google 文件中的 "建立和管理 NFS 卷"。

NFSv3 使用者和群組 **ID**

NFSv3 使用者和群組 ID 以數字 ID 而非名稱的形式透過網路傳輸。 Google Cloud NetApp Volumes不會透過 NFSv3 對這些數位 ID 進行使用者名稱解析，而 UNIX 安全樣式磁碟區僅使用模式位元。當存在 NFSv4.1 ACL 時，需要進行數字 ID 查找和/或名稱字串查找才能正確解析 ACL - 即使使用 NFSv3。對於 NTFS 安全樣式捲，Google Cloud NetApp Volumes必須將數位 ID 解析為有效的 UNIX 用戶，然後對應到有效的 Windows 用戶以協商存取權限。

NFSv3 使用者和群組 **ID** 的安全限制

使用 NFSv3，客戶端和伺服器永遠不必確認嘗試使用數位 ID 進行讀取或寫入的使用者是否是有效使用者；它只是隱式地受到信任。只需偽造任何數字 ID，檔案系統就有可能受到破壞。為了防止此類安全漏洞， Google Cloud NetApp Volumes提供了一些選項。

- 為 NFS 實作 Kerberos 強制使用者使用使用者名稱和密碼或金鑰表檔案進行驗證，以取得 Kerberos 票證以允許存取掛載。 Kerberos 適用於NetApp Volumes-Performance 實例，且僅適用於 NFSv4.1。

- 限制匯出政策規則中的主機清單會限制哪些 NFSv3 用戶端可以存取Google Cloud NetApp Volumes區。
- 使用雙協定磁碟區並將 NTFS ACL 套用至磁碟區會強制 NFSv3 用戶端將數字 ID 解析為有效的 UNIX 使用者名，以正確驗證存取掛載。這需要啟用 LDAP 並配置 UNIX 使用者和群組身分。
- 壓縮 root 使用者可以限制 root 使用者對 NFS 掛載造成的損害，但並不能完全消除風險。有關詳細信息，請參閱“[根用戶] “

最終，NFS 安全性受限於您所使用的協定版本所提供的功能。 NFSv3 雖然整體上比 NFSv4.1 效能更好，但卻無法提供相同等級的安全性。

NFSv4.1

與 NFSv3 相比，NFSv4.1 提供了更高的安全性和可靠性，原因如下：

- 透過基於租賃的機制整合鎖定
- 有狀態會話
- 所有 NFS 功能均透過單一連接埠 (2049)
- 僅 TCP
- ID域對映
- Kerberos 整合（NFSv3 可以使用 Kerberos，但僅限於 NFS，不適用於 NLM 等輔助協定）

NFSv4.1 依賴項

由於 NFSv4.1 中增加了安全功能，因此涉及一些使用 NFSv3 時不需要的外部相依性（類似於 SMB 需要 Active Directory 等相依性）。

NFSv4.1 ACL

Google Cloud NetApp Volumes提供對 NFSv4.x ACL 的支持，與普通 POSIX 樣式權限相比，它具有明顯的優勢，例如：

- 精細控制使用者對文件和目錄的訪問
- 更好的 NFS 安全性
- 改進了與 CIFS/SMB 的互通性
- 取消了使用 AUTH_SYS 安全性的 NFS 每個使用者 16 個群組的限制
- ACL 繞過了群組 ID (GID) 解析的需要，從而有效地消除了 GID 限制。 NFSv4.1 ACL 由 NFS 用戶端控制，而不是由Google Cloud NetApp Volumes控制。若要使用 NFSv4.1 ACL，請確保您的用戶端的軟體版本支援它們並且安裝了正確的 NFS 實用程式。

NFSv4.1 ACL 與 SMB 用戶端之間的相容性

NFSv4 ACL 與 Windows 檔案級 ACL（NTFS ACL）不同，但具有類似的功能。但是，在多協定 NAS 環境中，如果存在 NFSv4.1 ACL 並且您使用雙協定存取（同一資料集上的 NFS 和 SMB），則使用 SMB2.0 及更高版本的用戶端將無法從 Windows 安全性標籤檢視或管理 ACL。

NFSv4.1 ACL 的工作原理

為供參考，定義以下名詞：

- 存取控制清單 (ACL)。權限條目清單。
- 門禁入口 (ACE)。清單中的權限條目。

當用戶端在 SETATTR 作業期間在檔案上設定 NFSv4.1 ACL 時， Google Cloud NetApp Volumes會在物件上設定該 ACL，取代任何現有的 ACL。如果檔案上沒有 ACL，則檔案的模式權限將根據 OWNER@、GROUP@ 和 EVERYONE@ 計算。如果文件上存在任何現有的 SUID/SGID/STICKY 位，則它們不受影響。

當客戶端在 GETATTR 作業過程中取得檔案上的 NFSv4.1 ACL 時， Google Cloud NetApp Volumes會讀取與該物件關聯的 NFSv4.1 ACL，建立 ACE 列表，並將該列表傳回給客戶端。如果檔案具有 NT ACL 或模式位，則由模式位建構 ACL 並傳回給用戶端。

如果 ACL 中存在 DENY ACE，則拒絕存取；如果存在 ALLOW ACE，則允許存取。但是，如果 ACL 中不存在任何 ACE，存取也會被拒絕。

安全描述符由安全性 ACL (SACL) 和自由 ACL (DACL) 組成。 NFSv4.1與CIFS/SMB互通時，DACL與NFSv4、CIFS是一一映射的。 DACL 由 ALLOW ACE 和 DENY ACE 組成。

如果一個基本的 `chmod`在設定了 NFSv4.1 ACL 的檔案或資料夾上執行，現有使用者和群組 ACL 將被保留，但預設的 OWNER@、GROUP@、EVERYONE@ ACL 將被修改。

使用 NFSv4.1 ACL 的客戶端可以設定和檢視系統上檔案和目錄的 ACL。當在具有 ACL 的目錄中建立新檔案或子目錄時，該物件將繼承 ACL 中所有已使用適當標記的 ACE "繼承標誌" 。

如果檔案或目錄具有 NFSv4.1 ACL，則無論使用哪種協定存取該檔案或目錄，都會使用該 ACL 來控制存取。

只要 ACE 標有正確的繼承標誌，檔案和目錄就會從父目錄上的 NFSv4 ACL 繼承 ACE（可能經過適當的修改）。

當根據 NFSv4 請求建立檔案或目錄時，產生的檔案或目錄上的 ACL 取決於檔案建立請求是否包含 ACL 或僅包含標準 UNIX 檔案存取權限。 ACL 也取決於父目錄是否有 ACL。

- 如果請求包含 ACL，則使用該 ACL。
- 如果請求僅包含標準 UNIX 檔案存取權限，且父目錄沒有 ACL，則使用用戶端檔案模式設定標準 UNIX 檔案存取權限。
- 如果請求僅包含標準 UNIX 檔案存取權限，且父目錄具有不可繼承的 ACL，則會在新物件上設定基於傳遞到請求中的模式位元的預設 ACL。
- 如果請求僅包含標準 UNIX 檔案存取權限，但父目錄具有 ACL，則只要 ACE 已使用適當的繼承標誌進行標記，父目錄的 ACL 中的 ACE 就會被新檔案或目錄繼承。

ACE 權限

NFSv4.1 ACL 權限使用一系列大寫和小寫字母值（例如 `rxtncy`) 來控制存取。有關這些字母值的更多信息，請參閱 "如何使用 NFSv4 ACL"。

具有 umask 和 ACL 繼承的 NFSv4.1 ACL 行為

"NFSv4 ACL 提供 ACL 繼承功能" 。ACL 繼承意味著在設定了 NFSv4.1 ACL 的物件下建立的檔案或資料夾可以

根據 "ACL 繼承標誌"。

"烏馬斯克"用於控制無需管理員互動即可在目錄中建立檔案和資料夾的權限等級。預設情況下， Google Cloud NetApp Volumes允許 umask 覆寫繼承的 ACL，這是根據 "RFC 5661"。

ACL 格式

NFSv4.1 ACL 具有特定的格式。以下範例是文件上的 ACE 設定：

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上述範例遵循以下 ACL 格式準則：

```
type:flags:principal:permissions
```

一種 `A`意思是「允許」。在這種情況下，不會設定繼承標誌，因為主體不是一個群組並且不包括繼承。此外，由於 ACE 不是 AUDIT 條目，因此無需設定審計標誌。有關 NFSv4.1 ACL 的更多信息，請參閱 "http://linux.die.net/man/5/nfs4_acl"。

如果 NFSv4.1 ACL 設定不正確（或用戶端和伺服器無法解析名稱字串），ACL 可能不會如預期執行，或者 ACL 變更可能無法套用並引發錯誤。

範例錯誤包括：

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

明確拒絕

NFSv4.1 權限可以包括 OWNER、GROUP 和 EVERYONE 的明確 DENY 屬性。這是因為 NFSv4.1 ACL 是預設拒絕的，這表示如果 ACE 未明確授予 ACL，則會被拒絕。明確的 DENY 屬性將覆蓋任何 ACCESS ACE，無論是否明確。

DENY ACE 的屬性標籤為 `D`。

在下面的範例中，GROUP@ 被允許所有讀取和執行權限，但被拒絕所有寫入存取權限。

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

應盡可能避免使用 DENY ACE，因為它們可能令人困惑且複雜；未明確定義的 ALLOW ACL 將被隱式拒絕。當設定了 DENY ACE 時，使用者在期望獲得存取權限時可能會被拒絕存取。

上述一組 ACE 相當於模式位元中的 755，這表示：

- 所有者擁有充分的權利。
- 群組具有唯讀權限。
- 其他人只讀。

但是，即使將權限調整為 775，由於 EVERYONE 上明確設定了 DENY，存取也可能會被拒絕。

NFSv4.1 ID 域對映依賴關係

NFSv4.1 利用 ID 網域對映邏輯作為安全層，幫助驗證嘗試存取 NFSv4.1 掛載的使用者確實是他們所聲稱的使用者。在這些情況下，來自 NFSv4.1 用戶端的使用者名稱和群組名稱會附加一個名稱字串並將其傳送到Google Cloud NetApp Volumes實例。如果使用者名稱/群組名稱和 ID 字串組合不匹配，則該使用者和/或群組將被壓縮為 `/etc/idmapd.conf`客戶端上的文件。

此 ID 字串是遵守正確權限的必要條件，尤其是在使用 NFSv4.1 ACL 和/或 Kerberos 時。因此，需要名稱服務伺服器相依性（例如 LDAP 伺服器）來確保客戶端和Google Cloud NetApp Volumes之間的一致性，以便正確解析使用者和群組名稱身分。

Google Cloud NetApp Volumes使用靜態預設 ID 網域值 `defaultv4iddomain.com`。 NFS 用戶端預設使用 DNS 網域名稱作為其 ID 網域名稱設置，但您可以在 `/etc/idmapd.conf`。

如果在Google Cloud NetApp Volumes中啟用了 LDAP，則Google Cloud NetApp Volumes會自動將 NFS ID 網域變更為 DNS 中搜尋網域的配置，且用戶端無需修改，除非它們使用不同的 DNS 網域搜尋名稱。

當Google Cloud NetApp Volumes可以解析本機檔案或 LDAP 中的使用者名稱或群組名稱時，將使用網域字串，而不符合的網域 ID 將被壓縮為 nobody。如果Google Cloud NetApp Volumes在本機檔案或 LDAP 中找不到使用者名稱或群組名，則使用數字 ID 值，且 NFS 用戶端會正確解析該名稱（這類似於 NFSv3 行為）。

如果不變更客戶端的 NFSv4.1 ID 網域以符合Google Cloud NetApp Volumes磁碟區正在使用的網域，您會看到下列行為：

- Google Cloud NetApp Volumes中具有本機條目的 UNIX 使用者和群組（例如 root，如本機 UNIX 使用者和群組中所定義）被壓縮為 nobody 值。
- 如果 NFS 用戶端和Google Cloud NetApp Volumes Google Cloud NetApp Volumes配置為使用 LDAP）將被壓縮為 nobody。
- 沒有本機條目或 LDAP 條目的 UNIX 使用者和群組使用數字 ID 值並解析為 NFS 用戶端上指定的名稱。如果用戶端上不存在名稱，則僅顯示數字 ID。

下面顯示了上述場景的結果：

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
```

```
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

當客戶端和伺服器 ID 網域相符時，相同的檔案清單如下所示：

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

有關此問題及其解決方法的更多信息，請參閱“NFSv4.1 和 nobody 使用者/群組 “

Kerberos 依賴項

如果您打算將 Kerberos 與 NFS 結合使用，則必須具備以下Google Cloud NetApp Volumes：

- Kerberos 分發中心服務 (KDC) 的 Active Directory 網域
- 具有使用者和群組屬性的 Active Directory 網域，其中填充了用於 LDAP 功能的 UNIX 資訊（ Google Cloud NetApp Volumes中的 NFS Kerberos 需要使用者 SPN 到 UNIX 使用者對應才能正常運作。）
- Google Cloud NetApp Volumes實例上啟用了 LDAP
- DNS 服務的 Active Directory 網域

NFSv4.1 和 **nobody** 使用者/群組

NFSv4.1 配置中最常見的問題之一是當檔案或資料夾顯示在清單中時使用 `ls`歸 `user:group`組合 `nobody:nobody`。

例如：

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

數位 ID 是 `99`。

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

在某些情況下，文件可能會顯示正確的所有者，但 `nobody`作為團體。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

誰是沒人？

這 `nobody`NFSv4.1 中的使用者與 `nfsnobody`用戶。您可以透過執行以下命令來查看 NFS 用戶端如何查看每個用戶 `id`命令：

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

使用 NFSv4.1， `nobody`用戶是 `idmapd.conf`文件，可以定義為您想要使用的任何使用者。

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

為什麼會發生這種情況？

因為透過名稱字串映射實現的安全性是 NFSv4.1 操作的關鍵原則，所以當名稱字串無法正確匹配時，預設行為是將該使用者壓縮為通常無法存取使用者和群組所擁有的檔案和資料夾的使用者。

當你看到 `nobody`對於檔案清單中的使用者和/或群組，這通常意味著 NFSv4.1 中的某些內容配置錯誤。這裡需要區分大小寫。

例如，如果 user1@CVSDEMO.LOCAL (uid 1234, gid 1234) 正在存取匯出， Google Cloud NetApp Volumes必須能夠找到 user1@CVSDEMO.LOCAL (uid 1234, gid 1234)。如果Google Cloud NetApp Volumes中的使用者是 USER1@CVSDEMO.LOCAL，則不會相符（大寫 USER1 與小寫 user1）。在許多情況下，您可以在客戶端的訊息檔案中看到以下內容：

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

客戶端和伺服器必須都同意用戶確實是他們所聲稱的用戶，因此您必須檢查以下內容以確保客戶端看到的用戶與Google Cloud NetApp Volumes看到的用戶具有相同的資訊。

- NFSv4.x ID 域。客戶： `idmapd.conf`文件； Google Cloud NetApp Volumes使用 `defaultv4iddomain.com`並且無法手動更改。如果將 LDAP 與 NFSv4.1 一起使用， Google Cloud NetApp Volumes會將 ID 網域變更為 DNS 搜尋網域正在使用的網域，該網域與 AD 網域相同。
- *用戶名和數字 ID。 *這確定了客戶端在哪裡尋找用戶名，並利用名稱服務交換器來設定客戶端：

`nsswitch.conf`和/或本機密碼和群組檔案； Google Cloud NetApp Volumes不允許對此進行修改，但在啟用時會自動將 LDAP 新增至設定。

- *組名和數字 ID。 *這確定了客戶端在哪裡尋找群組名，並利用名稱服務交換器來設定客戶端：`nsswitch.conf`和/或本機密碼和群組檔案； Google Cloud NetApp Volumes不允許對此進行修改，但在啟用時會自動將 LDAP 新增至設定。

在幾乎所有情況下，如果你看到 `nobody`在客戶端的使用者和群組清單中，問題是Google Cloud NetApp Volumes和 NFS 用戶端之間的使用者或群組名稱 ID 轉換。為避免這種情況，請使用 LDAP 解析客戶端和Google Cloud NetApp Volumes之間的使用者和群組資訊。

在客戶端上查看 **NFSv4.1** 的名稱 **ID** 字串

如果您使用的是 NFSv4.1，則在 NFS 操作期間會發生名稱字串映射，如前所述。

除了使用 `/var/log/messages`要查找 NFSv4 ID 的問題，您可以使用 "nfsidmap -l"在 NFS 用戶端上執行命令以查看哪些使用者名稱已正確對應到 NFSv4 網域。

例如，這是客戶端和Google Cloud NetApp Volumes可以找到的使用者存取 NFSv4.x 掛載後命令的輸出：

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

當使用者沒有正確地對應到 NFSv4.1 ID 網域時（在這種情況下， `netapp-user`) 嘗試存取相同的掛載並接觸文件，它們被分配 `nobody:nobody`，正如預期的那樣。

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

這 `nfsidmap -l`輸出顯示用戶 `pcuser`在顯示幕上，但沒有 `netapp-user`；這是我們的導出策略規則中的匿名用戶(65534）。

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

中小企業

"中小企業" 是由 Microsoft 開發的網路檔案共享協定，可透過乙太網路為多個 SMB 用戶端提供集中式的使用者/群組驗證、權限、鎖定及檔案共享。檔案與資料夾透過共享的方式呈現給用戶端，這些共享可設定各種共享屬性，並透過共享層級的權限提供存取控制。SMB 可呈現給任何提供該協定支援的用戶端，包括 Windows 、 Apple 及 Linux 用戶端。

Google Cloud NetApp Volumes為此協定的 SMB 2.1 和 3.x 版本提供支援。

存取控制/**SMB** 共享

- 當 Windows 使用者名稱要求存取Google Cloud NetApp Volumes磁碟區時， Google Cloud NetApp Volumes會使用Google Cloud NetApp Volumes管理員設定的方法來尋找 UNIX 使用者名稱。
- 如果設定了外部 UNIX 身分提供者 (LDAP) 且 Windows/UNIX 使用者名稱相同，則 Windows 使用者名稱將 1:1 對應到 UNIX 使用者名，而無需任何其他設定。啟用 LDAP 後，Active Directory 用於託管使用者和群組物件的 UNIX 屬性。
- 如果 Windows 名稱和 UNIX 名稱不完全匹配，則必須設定 LDAP 以允許Google Cloud NetApp Volumes使用 LDAP 名稱對映配置（請參閱"使用 LDAP 進行非對稱名稱映射"）。
- 如果未使用 LDAP，則 Windows SMB 使用者將會對應到名為 `pcuser`在Google Cloud NetApp Volumes。這意味著用戶在 Windows 中編寫的檔案映射到 `pcuser`將 UNIX 所有權顯示為 `pcuser`在多協定 NAS 環境中。 `pcuser`這實際上是 `nobody`Linux 環境中的使用者（UID 65534）。

在僅使用 SMB 的部署中， `pcuser`映射仍然會發生，但這並不重要，因為 Windows 使用者和群組所有權已正確顯示，並且不允許 NFS 存取僅 SMB 磁碟區。此外，僅 SMB 磁碟區在建立後不支援轉換為 NFS 或雙協定磁碟區。

Windows 利用 Kerberos 與 Active Directory 網域控制站進行使用者名稱驗證，這需要與 AD DC 交換使用者名稱/密碼，而 AD DC 位於Google Cloud NetApp Volumes實例外部。當 `\\SERVERNAME`SMB 用戶端使用 UNC 路徑，且以下列情況為屬實：

- SERVERNAME 存在 DNS A/AAAA 條目
- SERVERNAME 存在用於 SMB/CIFS 存取的有效 SPN

建立Google Cloud NetApp Volumes SMB 磁碟區時，將依照本節中的定義建立機器帳戶名稱"Google Cloud NetApp Volumes如何在 Active Directory 中顯示。"這個機器帳戶名稱也成為 SMB 共享存取路徑，因為Google Cloud NetApp Volumes利用動態 DNS (DDNS) 在 DNS 中建立必要的 A/AAAA 和 PTR 項目，並在機器帳戶主體上建立必要的 SPN 項目。

若要建立 PTR 條目，DNS 伺服器上必須存在Google Cloud NetApp Volumes實例 IP 位址的反向查找區域。

例如，此Google Cloud NetApp Volumes磁碟區使用下列 UNC 共用路徑： `\\cvs-east-433d.cvsdemo.local` 。

在 Active Directory 中，這些是Google Cloud NetApp Volumes產生的 SPN 項目：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

這是 DNS 正向/反向查找結果：

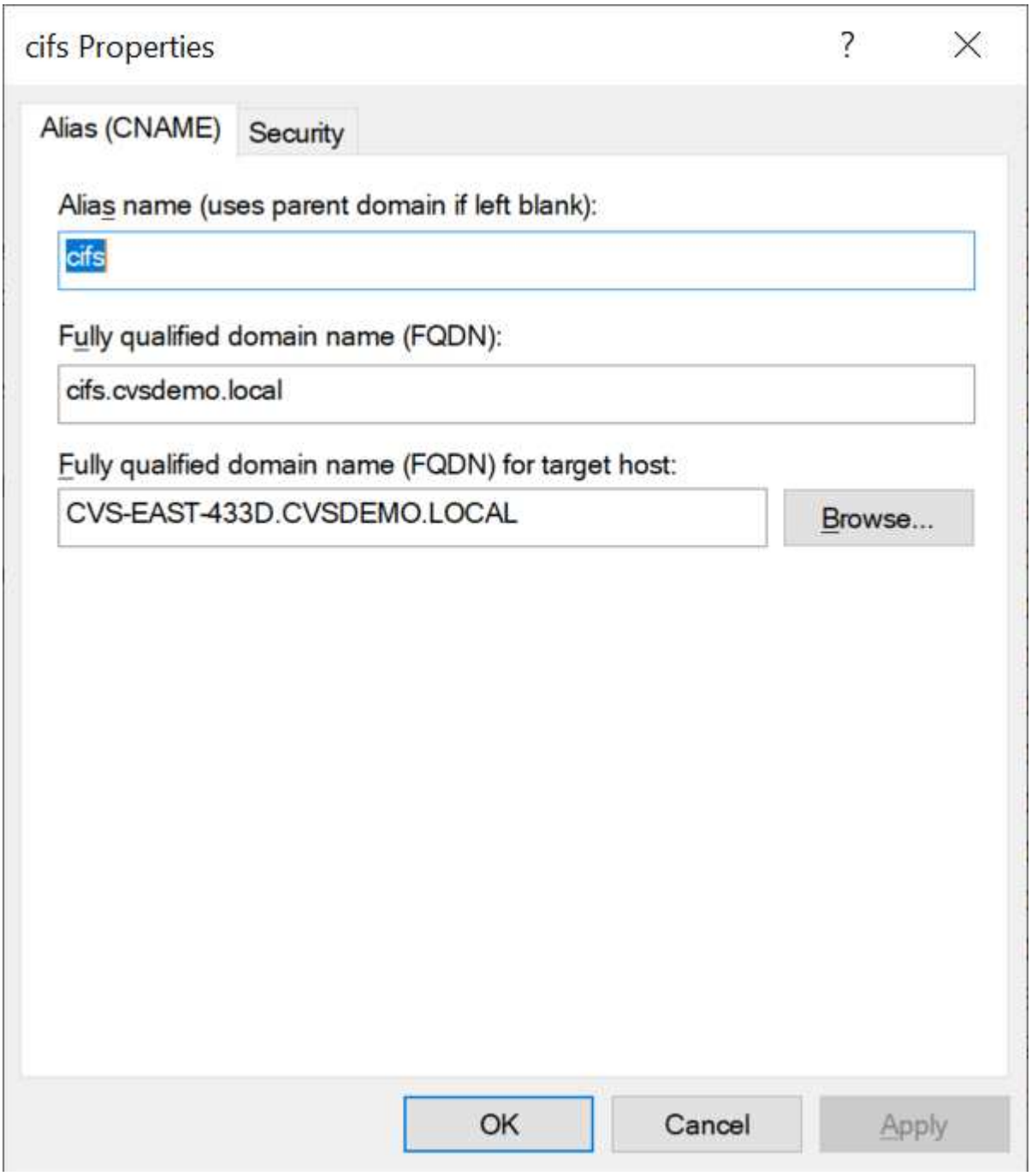
```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

或者，可以透過在Google Cloud NetApp Volumes中啟用/要求 SMB 共享的 SMB 加密來應用更多存取控制。如果其中一個端點不支援 SMB 加密，則不允許存取。

使用 **SMB** 名稱別名

在某些情況下，讓最終使用者知道Google Cloud NetApp Volumes所使用的機器帳戶名稱可能會帶來安全隱患。在其他情況下，您可能只是想為最終用戶提供更簡單的存取路徑。在這些情況下，您可以建立 SMB 別名。

如果您想要為 SMB 共用路徑建立別名，您可以利用 DNS 中所謂的 CNAME 記錄。例如，如果你想使用名稱 `\\CIFS`存取共享而不是 `\\cvs-east- 433d.cvsdemo.local`，但您仍然想使用 Kerberos 驗證，DNS 中指向現有 A/AAAA 記錄的 CNAME 和新增至現有機器帳戶的附加 SPN 可提供 Kerberos 存取。



這是新增 CNAME 之後的 DNS 正向查找結果：

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

這是新增 SPN 後產生的 SPN 查詢：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

在封包擷取中，我們可以看到使用與 CNAME 綁定的 SPN 的會話設定請求。

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB 身份驗證方言

Google Cloud NetApp Volumes支援以下 "方言"對於 SMB 身份驗證：

- LM
- NTLM
- NTLMv2
- Kerberos

SMB 共用存取的 Kerberos 驗證是您可以使用的最安全的驗證等級。啟用AES和SMB加密後，安全等級進一步提高。

Google Cloud NetApp Volumes也支援 LM 和 NTLM 驗證的向後相容性。當 Kerberos 設定錯誤時（例如建立 SMB 別名時），共用存取將回退到較弱的驗證方法（例如 NTLMv2）。由於這些機制不太安全，因此在某些 Active Directory 環境中它們被停用。如果停用較弱的驗證方法且未正確配置 Kerberos，則共用存取將會失敗，因為沒有有效的驗證方法可以回退。

有關在 Active Directory 中配置/查看支援的身份驗證等級的信息，請參閱 "網路安全: LAN Manager 驗證級別"。

權限模型

NTFS/檔案權限

NTFS 權限是遵循 NTFS 邏輯對檔案系統中的檔案和資料夾套用的權限。您可以在 `Basic`或者 `Advanced`並可設定為 `Allow`或者 `Deny`用於存取控制。

基本權限包括以下內容：

- 完全控制

- 調整
- 讀取並執行
- 讀
- 寫

當您為使用者或群組設定權限（稱為 ACE）時，它位於 ACL 中。 NTFS 權限使用與 UNIX 模式位元相同的讀取/寫入/執行基礎，但它們還可以擴展到更細粒度和擴展的存取控制（也稱為特殊權限），例如取得所有權、建立資料夾/附加資料、寫入屬性等。

標準 UNIX 模式位元不提供與 NTFS 權限相同等級的粒度（例如，能夠在 ACL 中為單一使用者和群組物件設定權限或設定擴充屬性）。但是，NFSv4.1 ACL 確實提供了與 NTFS ACL 相同的功能。

NTFS 權限比共用權限更具體，可以與共用權限結合使用。對於 NTFS 權限結構，適用最嚴格的限制。因此，在定義存取權限時，對使用者或群組的明確拒絕甚至會覆蓋完全控制。

NTFS 權限由 Windows SMB 用戶端控制。

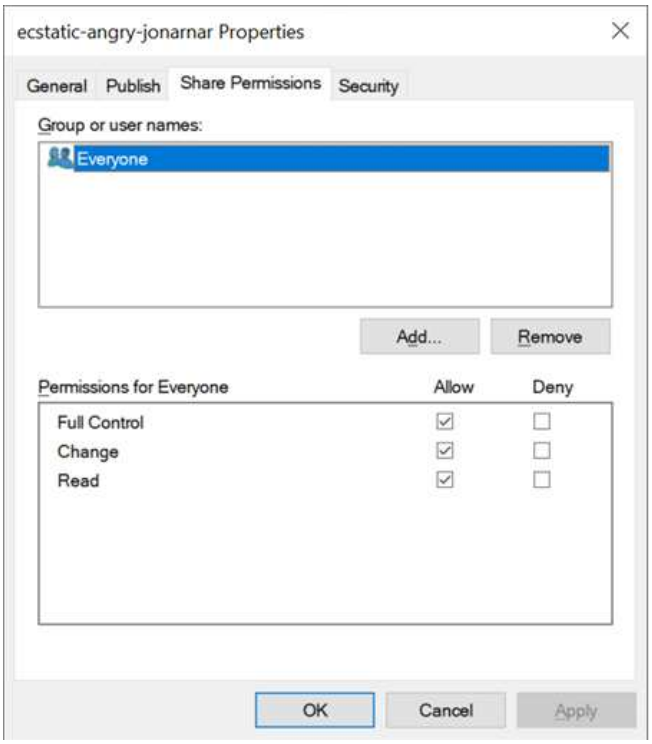
共享權限

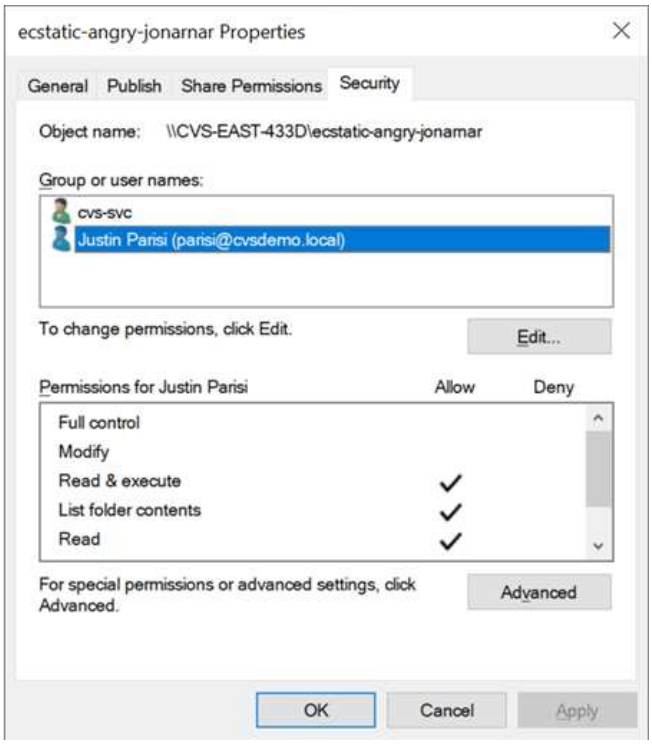
共享權限比 NTFS 權限（僅讀取/更改/完全控制）更通用，並控制進入 SMB 共享的初始條目 - 類似於 NFS 導出策略規則的工作方式。

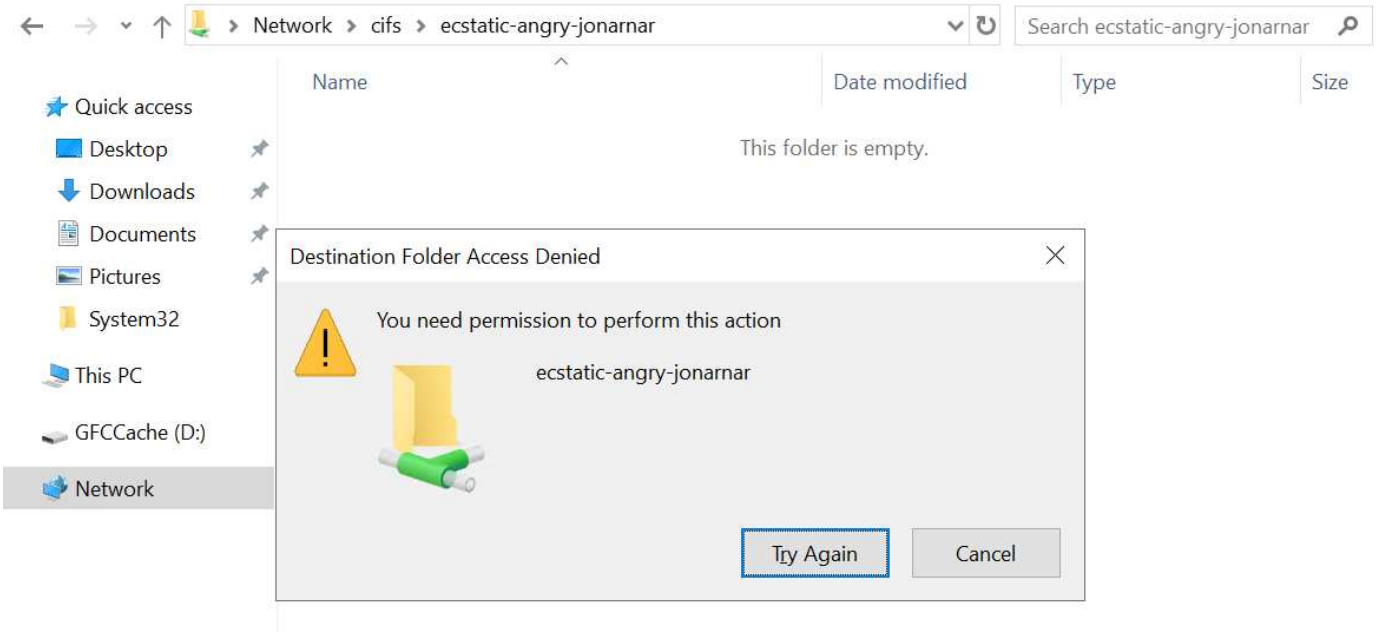
儘管 NFS 匯出策略規則透過基於主機的資訊（例如 IP 位址或主機名稱）控制訪問，但 SMB 共用權限可以透過使用共用 ACL 中的使用者和群組 ACE 來控制存取。您可以從 Windows 用戶端或Google Cloud NetApp Volumes管理 UI 設定共用 ACL。

預設情況下，共用 ACL 和初始磁碟區 ACL 包括具有完全控制權的所有人。應該更改檔案 ACL，但共用權限被共用中物件的檔案權限所取代。

例如，如果使用者僅被允許對Google Cloud NetApp Volumes磁碟區檔案 ACL 進行讀取訪問，則即使共用 ACL 設定為“具有完全控制權的所有人”，他們也將被拒絕建立檔案和資料夾，如下圖所示。







為了獲得最佳安全效果，請執行以下操作：

- 從共用和檔案 ACL 中刪除所有人，並為使用者或群組設定共用存取權限。
- 使用群組而不是單一使用者進行存取控制，以便於管理，並可以透過群組管理更快地刪除/新增使用者以共用 ACL。
- 允許對共享權限的 ACE 進行限制較少、更通用的共享訪問，並鎖定具有文件權限的用戶和群組的訪問，以實現更精細的訪問控制。
- 避免普遍使用明確拒絕 ACL，因為它們會覆蓋允許 ACL。對於需要快速限制存取檔案系統的使用者或群組，限制使用明確拒絕 ACL。
- 確保你注意到 "ACL 繼承"修改權限時的設定；在具有大量檔案數的目錄或磁碟區的頂層設定繼承標誌意味著

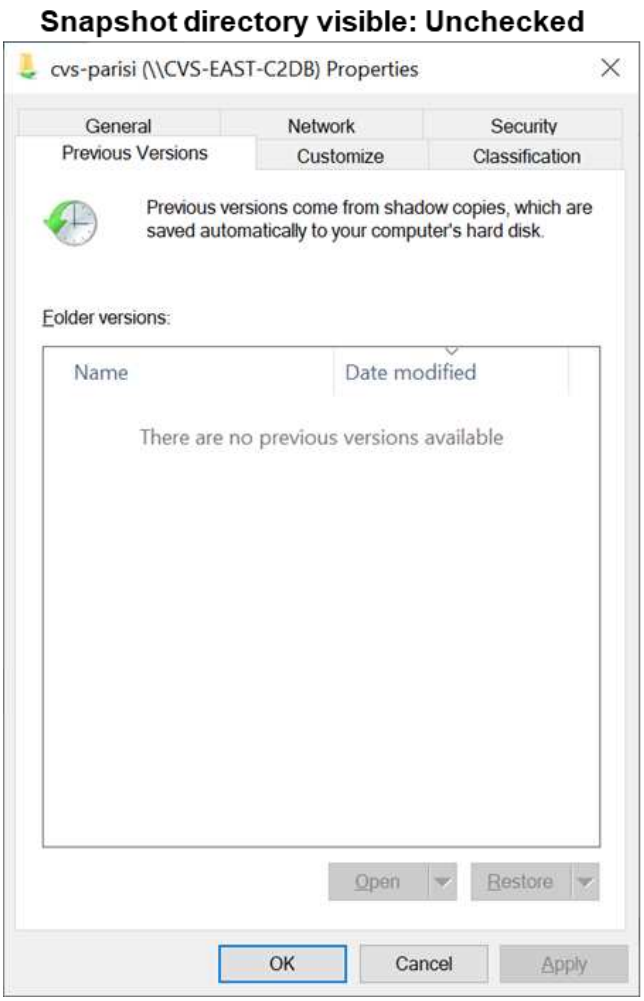
該目錄或磁碟區下的每個檔案都新增了繼承的權限，這可能會產生不必要的行為，例如意外的存取/拒絕以及在調整每個檔案時長時間修改權限。

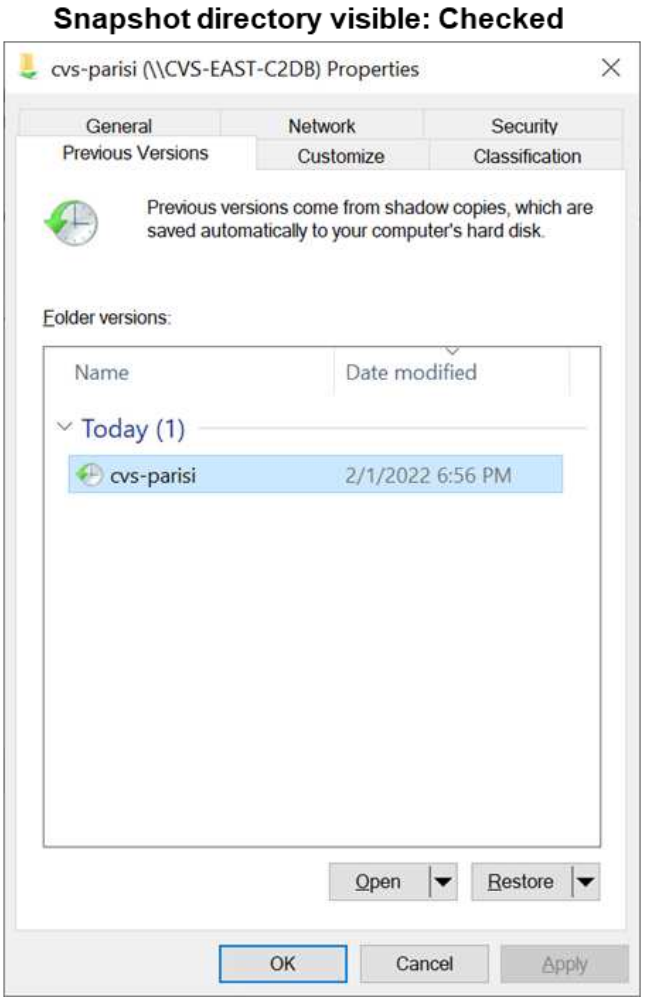
SMB 共享安全功能

當您首次在Google Cloud NetApp Volumes中建立具有 SMB 存取權限的磁碟區時，系統會向您提供一系列用於保護該磁碟區的選擇。

其中一些選擇取決於Google Cloud NetApp Volumes等級（效能或軟體），選擇包括：

- *讓快照目錄可見（適用於NetApp Volumes-Performance 和NetApp Volumes-SW）。 *此選項控制 SMB 用戶端是否可以存取 SMB 共用中的快照目錄(`\\server\share\~snapshot`和/或“先前版本”選項卡）。預設為“未選取”，這表示磁碟區預設為隱藏並禁止訪問 `~snapshot`目錄，並且磁碟區的「先前版本」標籤中不會顯示任何 Snapshot 副本。





出於安全原因、效能原因（隱藏這些資料夾以防 AV 掃描）或偏好，可能需要對最終使用者隱藏 Snapshot 副本。 Google Cloud NetApp Volumes快照是唯讀的，因此即使這些快照可見，最終使用者也無法刪除或修改快照目錄中的檔案。拍攝 Snapshot 副本時的檔案或資料夾的檔案權限適用。如果檔案或資料夾的權限在 Snapshot 副本之間發生變化，則這些變更也會套用至 Snapshot 目錄中的檔案或資料夾。使用者和群組可以根據權限存取這些文件或資料夾。雖然無法刪除或修改快照目錄中的文件，但可以將文件或資料夾複製出快照目錄。

- *啟用 SMB 加密（適用於NetApp Volumes-Performance 和NetApp Volumes-SW）。 *預設情況下，SMB 加密在 SMB 共用上是停用的（未選取）。勾選此方塊可啟用 SMB 加密，這表示 SMB 用戶端和伺服器之間的

流量在傳輸過程中進行加密，並使用協商的最高支援加密等級。 Google Cloud NetApp Volumes支援對 SMB 進行高達 AES-256 的加密。啟用 SMB 加密確實會帶來效能損失，您的 SMB 用戶端可能會或可能不會注意到這一點 - 大約在 10-20% 的範圍內。 NetApp強烈建議進行測試，以了解效能損失是否可以接受。

- *隱藏 SMB 共享（適用於NetApp Volumes-Performance 和NetApp Volumes-SW）。 *設定此選項會隱藏正常瀏覽中的 SMB 共用路徑。這意味著不知道共享路徑的客戶端在存取預設 UNC 路徑（例如 `\\NetApp Volumes-SMB`）。選取該複選框後，只有明確知道 SMB 共用路徑或具有由群組原則物件定義的共用路徑的用戶端才能存取它（透過混淆實現安全性）。
- *啟用基於存取的枚舉 (ABE)（僅限NetApp Volumes-SW）。 *這類似於隱藏 SMB 共享，不同之處在於共享或檔案僅對沒有權限存取物件的使用者或群組隱藏。例如，如果 Windows 用戶 `joe`不允許至少透過權限讀取存取權限，那麼 Windows 用戶 `joe`根本看不到 SMB 共享或文件。預設情況下，此功能是停用的，您可以透過選取核取方塊來啟用它。有關 ABE 的更多信息，請參閱NetApp知識庫文章 "基於訪問的枚舉（ABE）如何運作？"
- *啟用持續可用 (CA) 共享支援（僅限NetApp Volumes-Performance）。 * "持續可用的 SMB 共享"透過在Google Cloud NetApp Volumes後端系統中的節點之間複製鎖定狀態，提供一種在故障轉移事件期間最大限度地減少應用程式中斷的方法。這不是一個安全功能，但它確實提供了更好的整體彈性。目前，只有 SQL Server 和 FSLogix 應用程式支援此功能。

預設隱藏共享

在Google Cloud NetApp Volumes中建立 SMB 伺服器時， "隱藏的管理共享" （使用 $ 命名約定）除了資料磁碟區 SMB 共用之外所建立的。這些包括 C$（命名空間存取）和 IPC$（共用命名管道以用於程式之間的通信，例如用於 Microsoft 管理控制台 (MMC) 存取的遠端程序呼叫 (RPC)）。

IPC$ 共用不包含共用 ACL，且無法修改 - 它嚴格用於 RPC 呼叫和 "Windows 預設不允許匿名存取這些共用"。

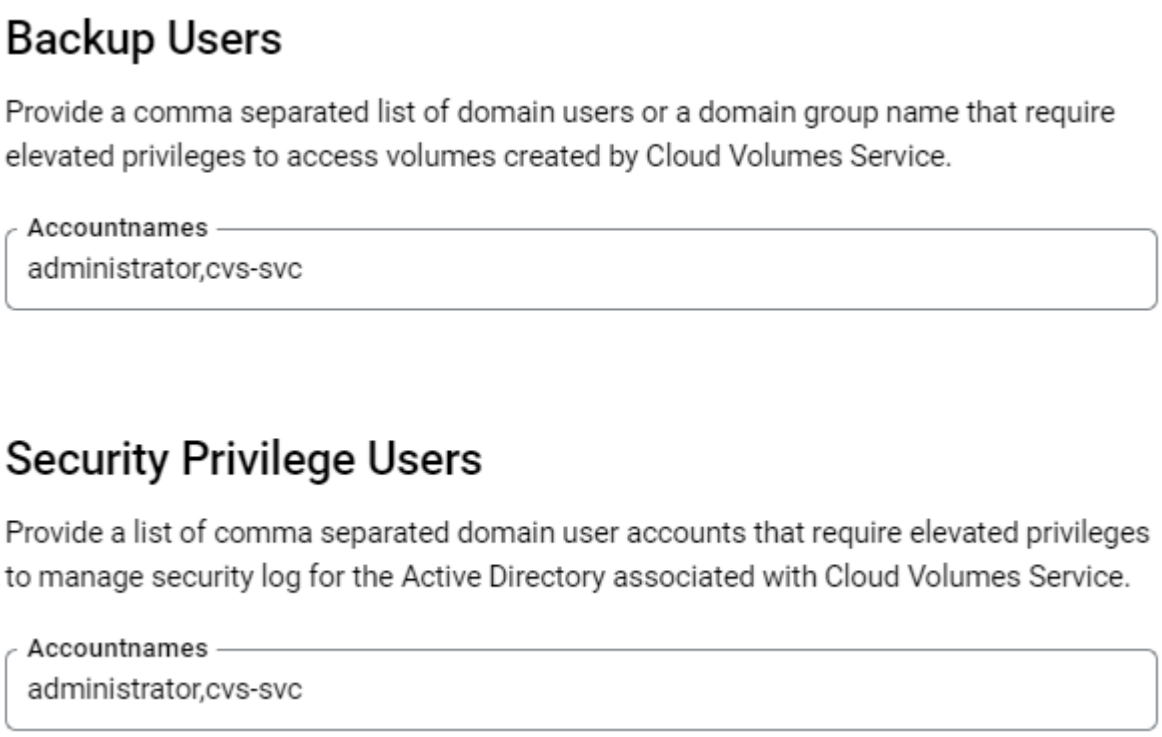
C$ 共用預設允許 BUILTIN/Administrators 訪問，但Google Cloud NetApp Volumes自動化會刪除共用 ACL 並且不允許任何人訪問，因為訪問 C$ 共用可以查看Google Cloud NetApp Volumes檔案系統中所有已安裝的磁碟區。因此，嘗試導航至 `\\SERVER\C$`失敗。

具有本機/內建管理員/備份權限的帳戶

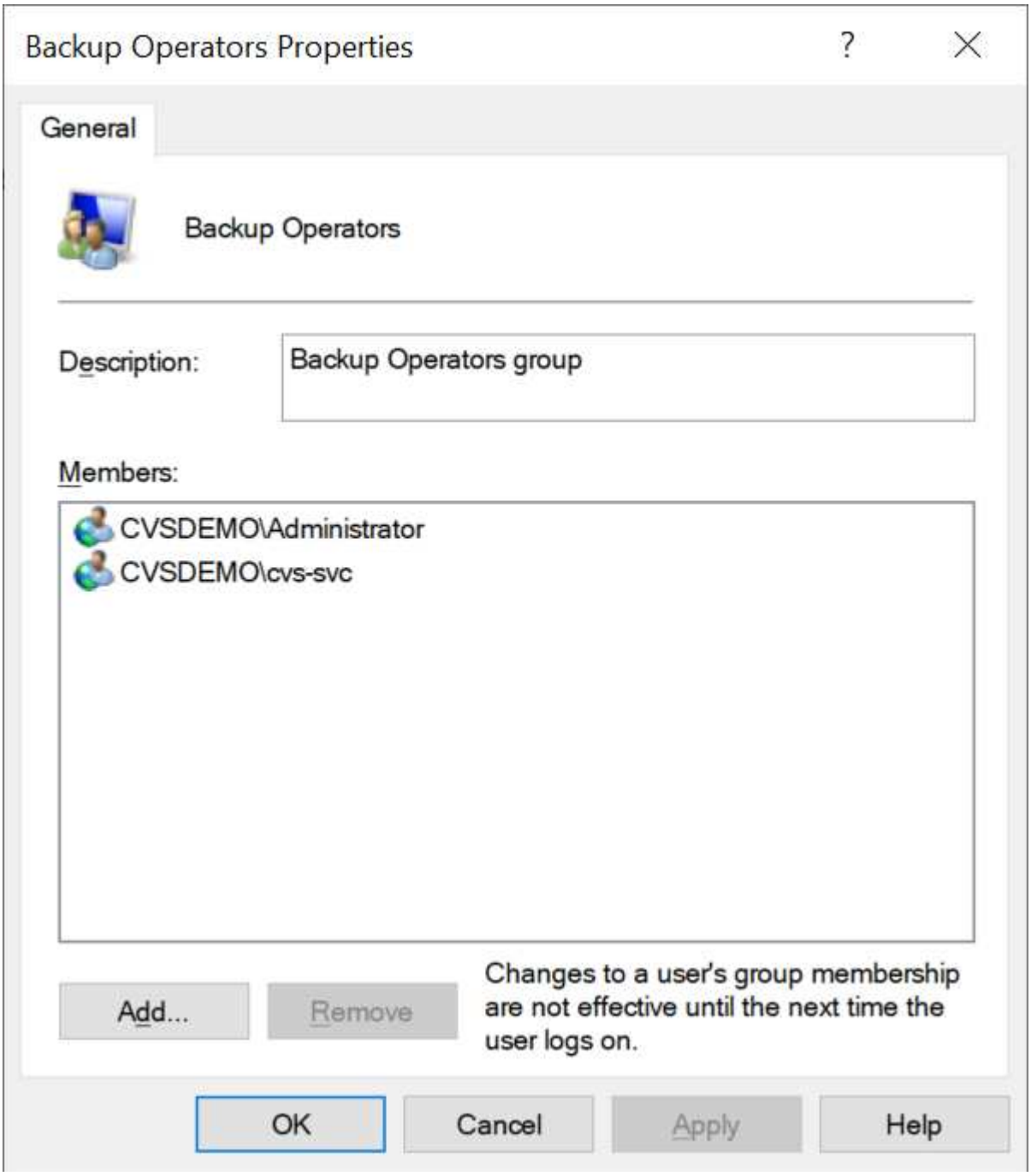
Google Cloud NetApp Volumes SMB 伺服器保持與常規 Windows SMB 伺服器類似的功能，即存在將存取權限套用至選定網域使用者和群組的本機群組（例如 BUILTIN\Administrators）。

當您指定要新增至備份使用者中的使用者時，該使用者將被新增至使用該 Active Directory 連線的Google Cloud NetApp Volumes實例中的 BUILTIN\Backup Operators 群組中，然後該執行個體將會取得 "SeBackupPrivilege 和 SeRestorePrivilege"。

當您將使用者新增至「安全權限使用者」時，該使用者將被賦予 SeSecurityPrivilege，這在某些應用程式用例中很有用，例如 "SMB 共用上的 SQL Server"。



您可以透過 MMC 以適當的權限查看Google Cloud NetApp Volumes本機群組成員資格。下圖顯示了使用Google Cloud NetApp Volumes控制台新增的使用者。

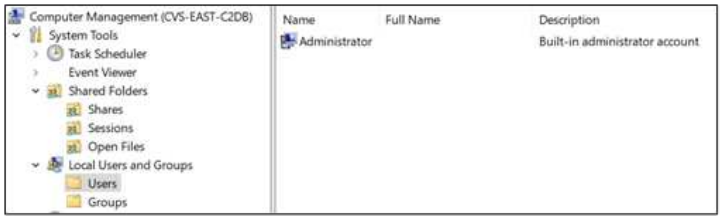


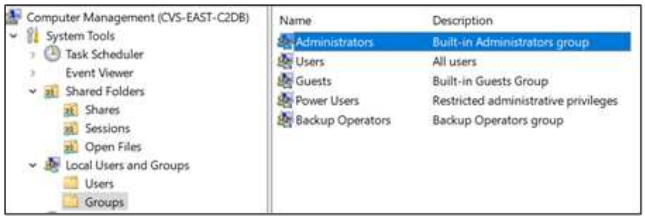
下表顯示了預設的 BUILTIN 群組的清單以及預設新增的使用者/群組。

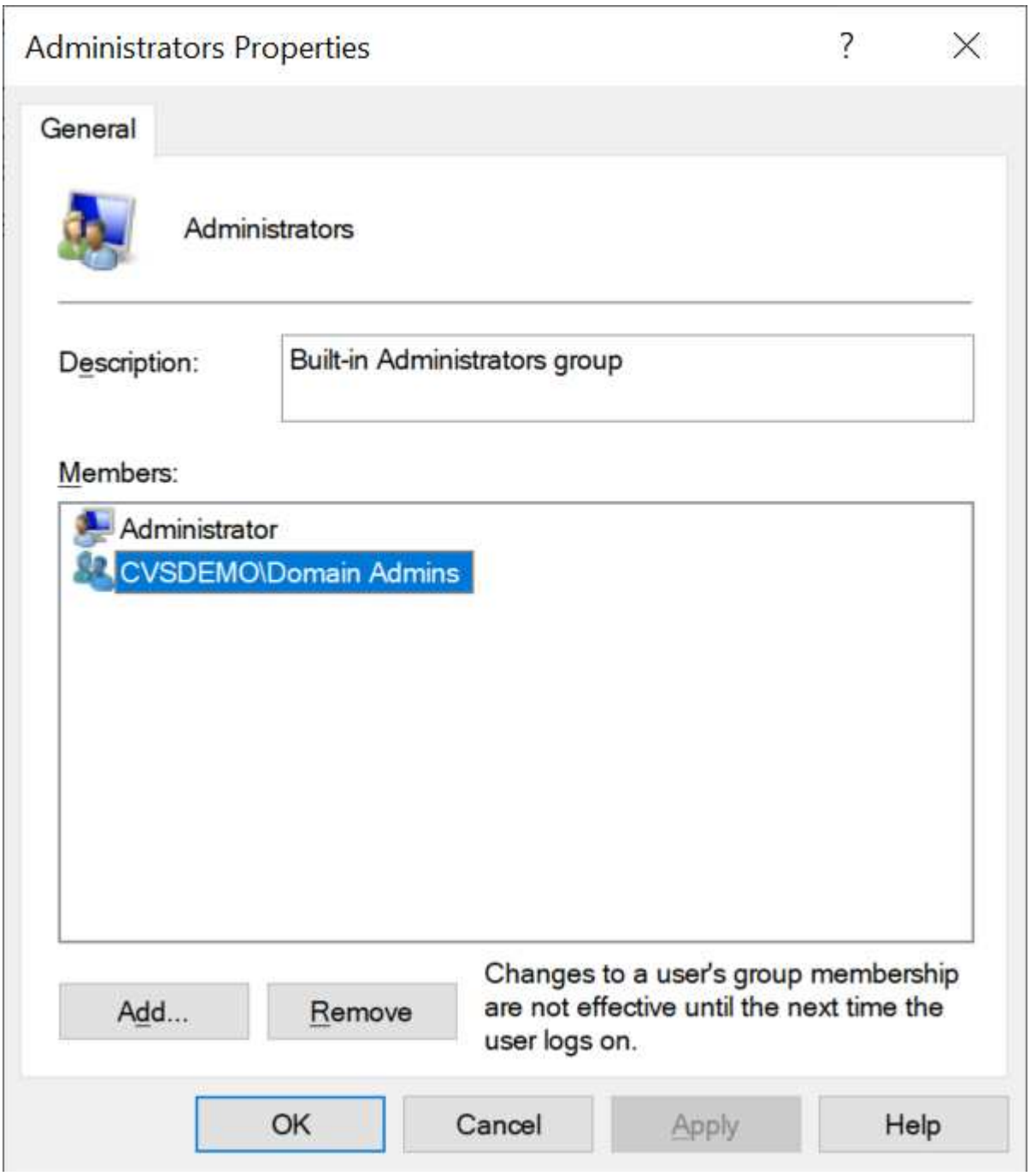
本地/內建群組	預設成員
內建管理員*	網域\網域管理員
內建\備份操作員*	沒有任何
內置\來賓	域\域來賓
內建\進階用戶	沒有任何
BUILTIN\網域用戶	網域\網域用戶

- Google Cloud NetApp Volumes Active Directory 連線配置中控制的群組成員資格。

您可以在 MMC 視窗中查看本機使用者和群組（以及群組成員），但無法從此控制台新增或刪除物件或變更群組成員資格。預設情況下，只有網域管理員群組和管理員會加入到Google Cloud NetApp Volumes中的 BUILTIN\Administrators 群組。目前，您無法修改此設定。







MMC/電腦管理訪問

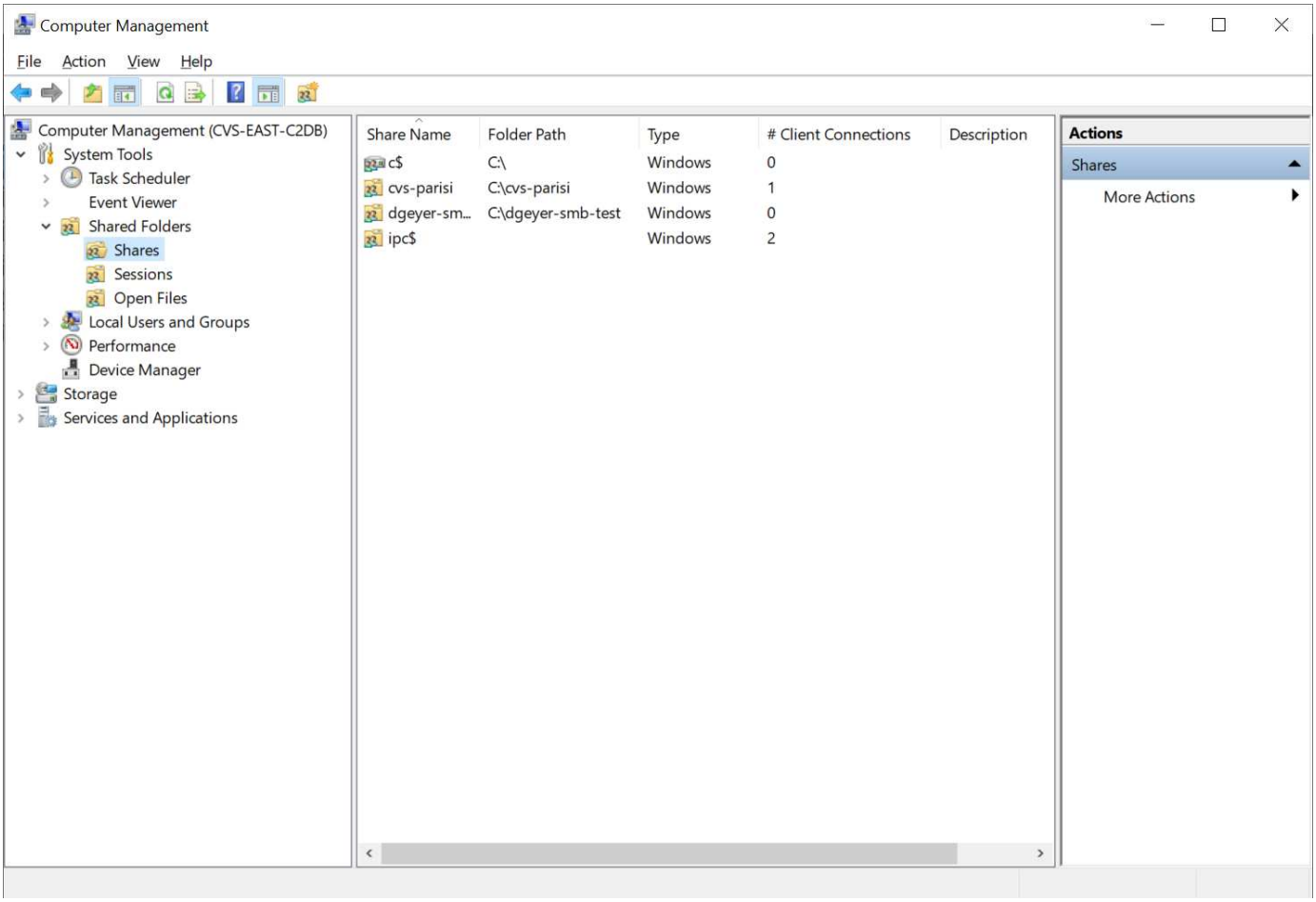
Google Cloud NetApp Volumes中的 SMB 存取提供與電腦管理 MMC 的連接，可讓您查看共用、管理共用 ACL 以及檢視/管理 SMB 會話和開啟檔案。

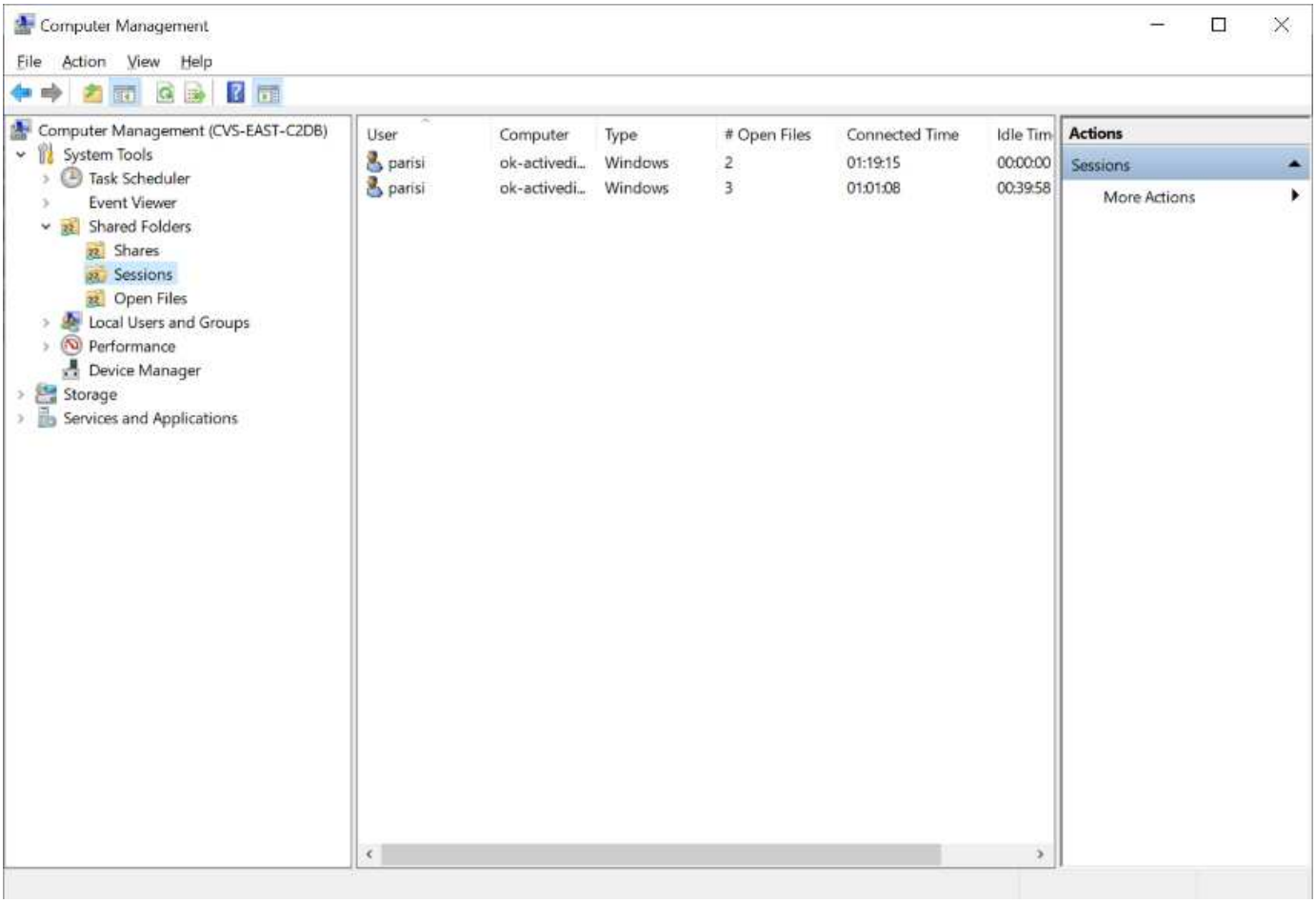
若要使用 MMC 查看Google Cloud NetApp Volumes中的 SMB 共用和會話，目前登入的使用者必須是網域管理員。其他使用者可以從 MMC 存取以查看或管理 SMB 伺服器，並在嘗試查看Google Cloud NetApp Volumes SMB 實例上的共用或會話時收到「您沒有權限」對話方塊。

若要連接到 SMB 伺服器，請開啟“電腦管理”，右鍵單擊“電腦管理”，然後選擇“連接到另一台電腦”。這將開啟「選擇電腦」對話框，您可以在其中輸入 SMB 伺服器名稱（可在Google Cloud NetApp Volumes磁碟區資訊中找到）。

當您查看具有適當權限的 SMB 共用時，您會看到Google Cloud NetApp Volumes實例中共用 Active Directory 連線的所有可用共用。若要控制此行為，請在Google Cloud NetApp Volumes磁碟區實例上設定隱藏 SMB 共用選項。

請記住，每個區域只允許一個 Active Directory 連線。





下表顯示了 MMC 支援/不支援的功能清單。

支援的功能	不支援的功能
• 查看分享 • 查看活動的 SMB 會話 • 查看開啟的文件 • 查看本機使用者和群組 • 查看本地群組成員資格 • 枚舉系統中的會話、檔案和樹連接列表 • 關閉系統中開啟的文件 • 關閉開放會議 • 建立/管理共享	• 建立新的本機使用者/群組 • 管理/查看現有的本機使用者/群組 • 查看事件或效能日誌 • 管理儲存 • 管理服務和應用程式

SMB 伺服器安全訊息

Google Cloud NetApp Volumes中的 SMB 伺服器使用一系列選項定義 SMB 連線的安全性策略，包括 Kerberos 時鐘偏差、票證年齡、加密等。

下表包含這些選項的清單、它們的作用、預設配置以及是否可以使用Google Cloud NetApp Volumes進行修改。某些選項不適用於Google Cloud NetApp Volumes。

安全選項	它的作用	預設值	可以改嗎？
最大 Kerberos 時鐘偏差（分鐘）	Google Cloud NetApp Volumes與網域控制站之間的最大時間偏差。如果時間偏差超過 5 分鐘，Kerberos 身份驗證將會失敗。這被設定為 Active Directory 預設值。	5	不
Kerberos 票證有效期限（小時）	Kerberos 票證在需要續訂之前保持有效的最長時間。如果 10 小時之前沒有續訂，則必須取得新票。Google Cloud NetApp Volumes會自動執行這些續訂。 10 小時是 Active Directory 的預設值。	10	不
最大 Kerberos 票證更新時間（天）	在需要新的授權請求之前，Kerberos 票證可以續訂的最長天數。 Google Cloud NetApp Volumes會自動更新 SMB 連線的票證。七天是 Active Directory 的預設值。	7	不
Kerberos KDC 連線逾時（秒）	KDC 連線逾時前的秒數。	3	不
要求對傳入的 SMB 流量進行簽名	設定為要求對 SMB 流量進行簽署。如果設定為 true，則不支援簽署的用戶端將無法連線。	錯誤的	
要求本地用戶帳戶的密碼複雜性	用於本機 SMB 使用者的密碼。 Google Cloud NetApp Volumes不支援本機使用者創建，因此此選項不適用於Google Cloud NetApp Volumes。	真的	不
使用 start_tls 進行 Active Directory LDAP 連接	用於啟用 Active Directory LDAP 的啟動 TLS 連線。Google Cloud NetApp Volumes目前不支援啟用此功能。	錯誤的	不
是否啟用 Kerberos 的 AES-128 和 AES-256 加密	這控制是否對 Active Directory 連線使用 AES 加密，並在建立/修改 Active Directory 連線時透過「為 Active Directory 驗證啟用 AES 加密」選項進行控制。	錯誤的	是的

安全選項	它的作用	預設值	可以改嗎？
LM 相容級別	Active Directory 連線支援的身份驗證方言層級。請參閱“SMB 身份驗證方言 ”獲取更多資訊。	ntlmv2-krb	不
要求對傳入的 CIFS 流量進行 SMB 加密	要求所有共享都進行 SMB 加密。 Google Cloud NetApp Volumes不使用此方法；而是根據每個磁碟區設定加密（請參閱“SMB 共享安全功能 "）。	錯誤的	不
客戶端會話安全	為 LDAP 通訊設定簽章和/或密封。目前， Google Cloud NetApp Volumes尚未設定該問題，但在未來的版本中可能需要解決。本節介紹了由於 Windows 修補程式導致的 LDAP 驗證問題的補救措施"LDAP 頻道綁定。"。	沒有任何	不
SMB2 啟用 DC 連接	使用 SMB2 進行 DC 連線。預設啟用。	系統預設	不
LDAP 推薦追蹤	當使用多個 LDAP 伺服器時，如果在第一個伺服器中找不到條目，則引用追蹤允許客戶端引用清單中的其他 LDAP 伺服器。 Google Cloud NetApp Volumes目前不支援此功能。	錯誤的	不
使用 LDAPS 實現安全的 Active Directory 連接	允許使用 LDAP over SSL。目前不受Google Cloud NetApp Volumes支援。	錯誤的	不
直流連線需要加密	需要加密才能成功連接 DC。在Google Cloud NetApp Volumes中預設為停用。	錯誤的	不

雙協議/多協議

Google Cloud NetApp Volumes 提供將相同資料集共享給 SMB 和 NFS 用戶端的能力，同時維持適當的存取權限 ("雙協議") 。這是透過協調通訊協定之間的身分對應，並使用集中式後端 LDAP 伺服器向 Google Cloud NetApp Volumes 提供 UNIX 身分來完成。為了方便使用，您可以使用 Windows Active Directory 同時提供 Windows 和 UNIX 使用者。

存取控制

- *共享存取控制。 *確定哪些客戶端和/或使用者和群組可以存取 NAS 共用。對於 NFS，導出策略和規則控制用戶端對導出的存取。 NFS 匯出由Google Cloud NetApp Volumes實例管理。 SMB 利用 CIFS/SMB 共用和共用 ACL 在使用者和群組層級提供更精細的控制。您只能透過使用https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html [MMC/Computer Management^] 和在Google Cloud NetApp Volumes實例上具有共享管理員的帳戶權限ACL（請參閱部分連結：gcp-gcnv-smb.html#Accounts with local/BUILTIN administrator/backup rights["Accounts with local/BUILTIN administrator/backup rights."]）。
- *檔案存取控制。 *控製檔案或資料夾層級的權限，並始終從 NAS 用戶端進行管理。 NFS 用戶端可以使用傳統模式位元 (rwx) 或 NFSv4 ACL。 SMB 用戶端利用 NTFS 權限。

向 NFS 和 SMB 提供資料的磁碟區的存取控制取決於所使用的協定。有關雙協議權限的信息，請參閱“[權限模型] “

使用者映射

當用戶端存取磁碟區時， Google Cloud NetApp Volumes會嘗試將傳入使用者對應到相反方向的有效使用者。這對於跨協定確定正確的存取權限以及確保請求存取的使用者確實是他們所聲稱的使用者來說是必要的。

例如，如果 Windows 使用者名稱為 `joe`嘗試透過 SMB 存取具有 UNIX 權限的捲，然後Google Cloud NetApp Volumes執行搜尋以尋找名為 `joe`。如果存在，則以 Windows 使用者身分寫入 SMB 共用的文件 `joe`顯示為 UNIX 用戶 `joe`來自 NFS 客戶端。

或者，如果 UNIX 使用者名稱為 `joe`嘗試使用 Windows 權限存取Google Cloud NetApp Volumes卷，則 UNIX 使用者必須能夠對應到有效的 Windows 使用者。否則，將拒絕存取該磁碟區。

目前，使用 LDAP 的外部 UNIX 身分識別管理僅支援 Active Directory。有關設定此服務存取的更多資訊，請參閱 "建立 AD 連接"。

權限模型

使用雙協定設定時， Google Cloud NetApp Volumes會利用磁碟區的安全樣式來決定 ACL 的類型。這些安全樣式是根據指定的 NAS 協定設定的，或者在雙協定的情況下，是在建立Google Cloud NetApp Volumes區時所做的選擇。

- 如果您僅使用 NFS， Google Cloud NetApp Volumes磁碟區將使用 UNIX 權限。
- 如果您只使用 SMB， Google Cloud NetApp Volumes磁碟區將使用 NTFS 權限。

如果您正在建立雙協定卷，則可以在建立磁碟區時選擇 ACL 樣式。此決定應根據所需的權限管理做出。如果您的使用者從 Windows/SMB 用戶端管理權限，請選擇 NTFS。如果您的使用者喜歡使用 NFS 用戶端和 chmod/chown，請使用 UNIX 安全樣式。

建立 **Active Directory** 連線的注意事項

Google Cloud NetApp Volumes可以將您的Google Cloud NetApp Volumes執行個體連接到外部 Active Directory 伺服器，以便為 SMB 和 UNIX 使用者進行身分識別管理。需要建立 Active Directory 連線才能在Google Cloud NetApp Volumes中使用 SMB。

此配置提供了幾個需要考慮安全性的選項。外部 Active Directory 伺服器可以是本機實例或雲端原生實例。如果您使用的是本機 Active Directory 伺服器，請不要將網域暴露給外部網路（例如使用 DMZ 或外部 IP 位址）。相反，使用安全的私人隧道或 VPN、單向林信任或專用網路連接到本地網路 "私人 Google 存取權限"。有關更多信

息，請參閱 Google Cloud 文檔 "在 Google Cloud 中使用 Active Directory 的最佳實踐"。

NetApp Volumes-SW 要求 Active Directory 伺服器位於相同區域。如果在NetApp Volumes-SW 中嘗試建立到另一個區域的 DC 連接，則嘗試會失敗。使用NetApp Volumes-SW 時，請確保建立包含 Active Directory DC 的 Active Directory 站點，然後在Google Cloud NetApp Volumes中指定站點，以避免跨區域 DC 連線嘗試。

Active Directory 憑證

啟用 SMB 或 LDAP for NFS 後， Google Cloud NetApp Volumes會與 Active Directory 控制器互動以建立用於驗證的機器帳戶物件。這與 Windows SMB 用戶端加入網域並需要對 Active Directory 中的組織單位 (OU) 具有相同的存取權限的方式沒有什麼不同。

在許多情況下，安全群組不允許在外部伺服器（例如Google Cloud NetApp Volumes）上使用 Windows 管理員帳戶。在某些情況下，為了確保最佳安全措施，Windows 管理員使用者會被完全停用。

建立 **SMB** 機器帳戶所需的權限

要將Google Cloud NetApp Volumes機器物件新增至 Active Directory，需要具有網域管理權限或具有 "委派建立和修改機器帳戶物件的權限"需要指定 OU。您可以使用 Active Directory 中的控制委派精靈來執行此操作，方法是建立自訂任務，該任務為使用者提供建立/刪除電腦物件的權限，並提供下列存取權限：

- 讀/寫
- 建立/刪除所有子對象
- 讀/寫所有屬性
- 更改/重置密碼

這樣做會自動將定義的使用者的安全 ACL 新增至 Active Directory 中的 OU，並最大限度地減少對 Active Directory 環境的存取。委派使用者後，可在此視窗中提供該使用者名稱和密碼作為 Active Directory 憑證。

傳遞給 Active Directory 網域的使用者名稱和密碼在機器帳戶物件查詢和建立期間利用 Kerberos 加密來增強安全性。

Active Directory 連接詳細信息

```
https://docs.cloud.google.com/netapp/volumes/docs/configure-and-
use/active-directory/about-ad["Active Directory 連接詳細信息
"^]為管理員提供指導，以便提供用於放置電腦帳戶的特定 Active Directory 架構資訊，例如：
```

- Active Directory 連線類型。用於指定區域中的 Active Directory 連線是否用於Google Cloud NetApp Volumes或NetApp Volumes-Performance 服務類型的磁碟區。如果在現有連線上設定不正確，使用或編輯時可能無法正常運作。
- *領域。 * Active Directory 網域。
- *站台。*將 Active Directory 伺服器限制在特定站台，以提升安全性與效能 "注意事項"。當多個 Active Directory 伺服器橫跨多個區域時，這是必要的，因為 Google Cloud NetApp Volumes 目前不支援允許 Active Directory 驗證請求發送至與 Google Cloud NetApp Volumes 實例不同區域的 Active Directory 伺服器。（例如，Active Directory 網域控制器位於僅支援 NetApp Volumes-Performance 的區域，但您希望在

NetApp Volumes-SW 實例中建立 SMB 共用。）

- DNS 伺服器。用於名稱查找的 DNS 伺服器。
- NetBIOS 名稱（可選）。如果需要，伺服器的 NetBIOS 名稱。這是使用 Active Directory 連線建立新機器帳戶時所使用的內容。例如，如果 NetBIOS 名稱設定為NetApp Volumes-EAST，則機器帳戶名稱將為NetApp Volumes-EAST-{1234}。請參閱"Google Cloud NetApp Volumes如何在 Active Directory 中顯示"了解更多。
- 組織單位 (OU)。建立計算機帳戶的特定 OU。如果您將機器帳戶的控制權委託給特定 OU 的用戶，這將非常有用。
- AES 加密。您也可以選取或取消選取「為 AD 身份驗證啟用 AES 加密」複選框。為 Active Directory 驗證啟用 AES 加密可為使用者和群組查找期間Google Cloud NetApp Volumes與 Active Directory 的通訊提供額外的安全性。啟用此選項之前，請先與網域管理員核實，以確認 Active Directory 網域控制器支援 AES 驗證。

> 預設情況下，大多數 Windows 伺服器不會停用較弱的密碼（例如 DES 或 RC4-HMAC），但如果您選擇停用較弱的密碼，請確認Google Cloud NetApp Volumes Active Directory 連線已設定為啟用 AES。否則，身份驗證將會失敗。啟用 AES 加密不會停用較弱的密碼，而是在Google Cloud NetApp Volumes SMB 機器帳戶中新增對 AES 密碼的支援。

Kerberos 領域詳細信息

此選項不適用於 SMB 伺服器。相反，它用於為Google Cloud NetApp Volumes系統配置 NFS Kerberos。填入這些詳細資訊後，將設定 NFS Kerberos 領域（類似於 Linux 上的 krb5.conf 檔案），並在Google Cloud NetApp Volumes磁碟區建立上指定 NFS Kerberos 時使用，因為 Active Directory 連線充當 NFS Kerberos 分發中心 (KDC)。

> 非 Windows KDC 目前不支援與Google Cloud NetApp Volumes一起使用。

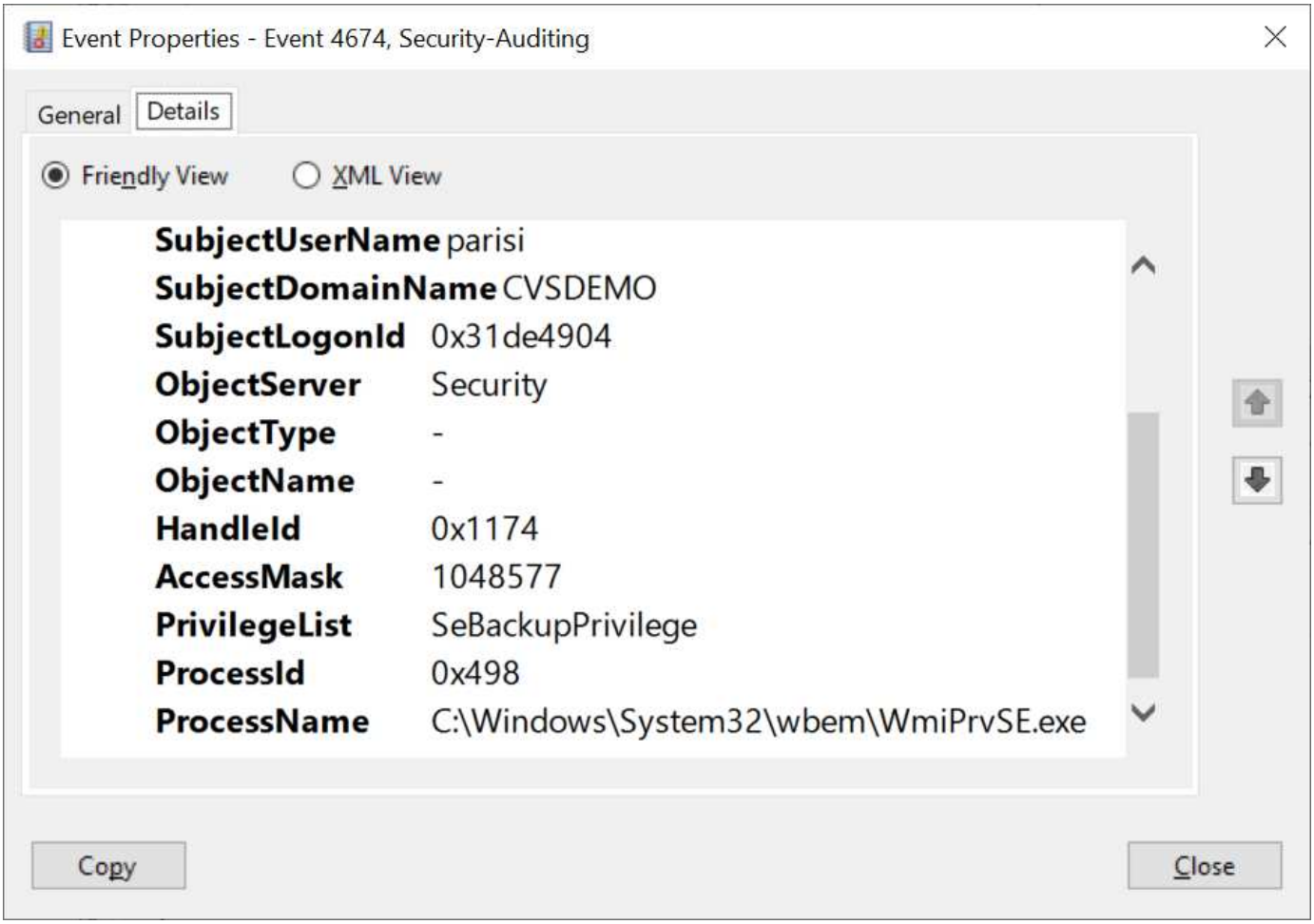
地區

透過區域，您可以指定 Active Directory 連線所在的位置。該區域必須與Google Cloud NetApp Volumes磁碟區位於同一區域。

- *具有 LDAP 的本機 NFS 使用者。 *在本節中，還有一個選項允許本機 NFS 使用者使用 LDAP。如果您想要擴展 UNIX 使用者群組成員資格支持，使其超出 NFS（擴展群組）的 16 個群組限制，則必須取消選擇此選項。但是，使用擴充組需要為 UNIX 身分配置 LDAP 伺服器。如果您沒有 LDAP 伺服器，請不要選擇此選項。如果您有 LDAP 伺服器並且還想使用本機 UNIX 使用者（例如 root），請選擇此選項。

備份用戶

此選項可讓您指定對Google Cloud NetApp Volumes磁碟區具有備份權限的 Windows 使用者。某些應用程式需要備份權限（SeBackupPrivilege）才能正確備份和還原 NAS 磁碟區中的資料。此使用者對磁碟區中的資料具有高層級存取權限，因此您應該考慮 "啟用該使用者存取的審計"。啟用後，稽核事件將顯示在事件檢視器 > Windows 日誌 > 安全性中。



安全特權用戶

透過此選項，您可以指定對Google Cloud NetApp Volumes磁碟區具有安全修改權限的 Windows 使用者。某些應用程式需要安全權限（SeSecurityPrivilege）("例如 SQL Server") 在安裝過程中正確設定權限。管理安全日誌需要此權限。雖然此權限不如 SeBackupPrivilege 強大，NetApp建議 "審計用戶的用戶訪問"如果需要的話，可以使用此權限等級。

有關更多信息，請參閱 "指派給新登入的特殊權限" 。

Google Cloud NetApp Volumes如何在 **Active Directory** 中顯示

Google Cloud NetApp Volumes在 Active Directory 中顯示為一般機器帳戶物件。命名約定如下。

- CIFS/SMB 和 NFS Kerberos 建立單獨的機器帳戶物件。
- 啟用 LDAP 的 NFS 在 Active Directory 中為 Kerberos LDAP 綁定建立一個機器帳戶。
- 具有 LDAP 的雙協定磁碟區共用 LDAP 和 SMB 的 CIFS/SMB 機器帳戶。
- CIFS/SMB 機器帳戶使用 NAME-1234 的命名約定（隨機四位元 ID，在 <10 個字元的名稱後附加連字號）。您可以透過 Active Directory 連線上的 NetBIOS 名稱設定來定義 NAME（請參閱「Active Directory 連接詳細信息 "）。
- NFS Kerberos 使用 NFS-NAME-1234 作為命名約定（最多 15 個字元）。如果使用超過 15 個字符，則名稱為 NFS-TRUNCATED-NAME-1234。
- 啟用 LDAP 的僅 NFS NetApp Volumes-Performance 實例會建立一個 SMB 機器帳戶，以與 CIFS/SMB 實

例具有相同的命名約定來綁定到 LDAP 伺服器。

- 建立 SMB 機器帳戶時，預設隱藏的管理共用（請參閱"預設隱藏共享") 也被建立（c$、admin$、ipc$），但這些共用沒有分配 ACL，因此無法存取。
- 預設情況下，機器帳戶物件放在 CN=Computers 中，但您可以在必要時指定不同的 OU。請參閱“建立 SMB 機器帳戶所需的權限 「有關新增/刪除Google Cloud NetApp Volumes的機器帳戶物件所需的存取權限的資訊。

當Google Cloud NetApp Volumes將 SMB 機器帳戶新增至 Active Directory 時，將填入下列欄位：

- cn（帶有指定的 SMB 伺服器名稱）
- dNSHostName（使用 SMBserver.domain.com）
- msDS-SupportedEncryptionTypes（如果未啟用 AES 加密，則允許使用 DES_CBC_MD5、RC4_HMAC_MD5；如果啟用了 AES 加密，則允許使用 DES_CBC_MD5、RC4_HMAC_MD5、AES128_CTS_HMAC_SHA1_96、AES256_CTS_HMAC_SHA1_96 與 SMB 的機器帳戶進行 Kerberos 票證交換）
- 名稱（使用 SMB 伺服器名稱）
- sAMAccountName（附 SMBserver$）
- servicePrincipalName（對於 Kerberos，使用 host/smbserver.domain.com 和 host/smbserver SPN）

如果您想要在電腦帳戶上停用較弱的 Kerberos 加密類型 (enctype)，您可以將電腦帳戶上的 msDS-SupportedEncryptionTypes 值變更為下表中的值之一，以僅允許 AES。

msDS-SupportedEncryptionTypes 值	已啟用 **Enctype**
2	DES_CBC_MD5
4	RC4_HMAC
8	僅限 AES128_CTS_HMAC_SHA1_96
16	僅限 AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 和 AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5、RC4_HMAC、AES128_CTS_HMAC_SHA1_96 和 AES256_CTS_HMAC_SHA1_96

若要為 SMB 機器帳戶啟用 AES 加密，請在建立 Active Directory 連線時按一下為 AD 驗證啟用 AES 加密。

若要為 NFS Kerberos 啟用 AES 加密， "請參閱Google Cloud NetApp Volumes文檔"

其他 **NAS** 基礎架構服務相依性（**KDC**、**LDAP** 和 **DNS**）

當使用Google Cloud NetApp Volumes進行 NAS 共用時，可能需要外部相依性才能正常發揮作用。這些依賴關係在特定情況下發揮作用。下表顯示了各種配置選項以及所需的依賴項（如果有）。

配置	所需依賴項
僅限 NFSv3	沒有任何

配置	所需依賴項
僅限 NFSv3 Kerberos	Windows 活動目錄：* KDC * DNS * LDAP
僅限 NFSv4.1	客戶端 ID 映射配置（/etc/idmap.conf）
僅限 NFSv4.1 Kerberos	• 客戶端 ID 映射配置（/etc/idmap.conf） • Windows 活動目錄：KDC DNS LDAP
僅限 SMB	活動目錄：* KDC * DNS
多協定 NAS（NFS 和 SMB）	• 客戶端 ID 映射配置（僅限 NFSv4.1；/etc/idmap.conf） • Windows 活動目錄：KDC DNS LDAP

機器帳戶物件的 **Kerberos** 金鑰表輪換/密碼重置

使用 SMB 機器帳戶， Google Cloud NetApp Volumes會為 SMB 機器帳戶安排定期重設密碼。這些密碼重設使用 Kerberos 加密進行，並按照每月第四個星期日晚上 11 點到凌晨 1 點之間的隨機時間進行。這些密碼重設會變更 Kerberos 金鑰版本，輪換儲存在Google Cloud NetApp Volumes系統上的金鑰表，並協助為在Google Cloud NetApp Volumes中執行的 SMB 伺服器維持更高層級的安全性。機器帳戶密碼是隨機的，管理員不知道。

對於 NFS Kerberos 機器帳戶，僅當建立/與 KDC 交換新的金鑰表時才會重設密碼。目前，在Google Cloud NetApp Volumes中無法執行此操作。

用於 **LDAP** 和 **Kerberos** 的網路連接埠

使用 LDAP 和 Kerberos 時，您應該確定這些服務所使用的網路連接埠。您可以在 "Google Cloud NetApp Volumes有關安全注意事項的文檔"中找到 Google Cloud NetApp Volumes 所使用的完整連接埠清單。

LDAP

Google Cloud NetApp Volumes可作為 LDAP 用戶端，並使用標準 LDAP 搜尋查詢來尋找 UNIX 身分的使用者和群組。如果您打算使用Google Cloud NetApp Volumes提供的標準預設使用者以外的使用者和群組，則 LDAP 是必要的。如果您打算將 NFS Kerberos 與使用者主體（例如 user1@domain.com）一起使用，則 LDAP 也是必要的。目前僅支援使用 Microsoft Active Directory 的 LDAP。

若要將 Active Directory 用作 UNIX LDAP 伺服器，您必須在要用於 UNIX 身分的使用者和群組上填入必要的 UNIX 屬性。 Google Cloud NetApp Volumes使用預設 LDAP 模式模板，該模板根據以下資訊查詢屬性 "RFC-2307-bis"。因此，下表顯示了使用者和群組需要填入的最低限度的 Active Directory 屬性以及每個屬性的用途。

如需在 Active Directory 中設定 LDAP 屬性的詳細資訊，請參閱 "管理雙協定存取。"

屬性	它的作用
uid*	指定 UNIX 使用者名稱
uid編號*	指定 UNIX 使用者的數字 ID
gid編號*	指定 UNIX 使用者的主要群組數字 ID
物件類別*	指定正在使用的物件類型； Google Cloud NetApp Volumes要求將「使用者」包含在物件類別清單中（預設包含在大多數 Active Directory 部署中）。

屬性	它的作用
姓名	有關帳戶的一般資訊（真實姓名、電話號碼等 - 也稱為 gecos）
unix用戶密碼	無需設定此項；不用於 NAS 驗證的 UNIX 身份查找。設定此項目將會將配置的 unixUserPassword 值以純文字形式放置。
unix主目錄	當使用者從 Linux 用戶端針對 LDAP 進行身份驗證時，定義 UNIX 主目錄的路徑。如果您想要使用 LDAP 實作 UNIX 主目錄功能，請設定此項目。
登入外殼	當使用者透過 LDAP 進行身份驗證時，定義 Linux 用戶端的 bash/profile shell 的路徑。

*表示該屬性是Google Cloud NetApp Volumes正常功能所必需的。其餘屬性僅供客戶端使用。

屬性	它的作用
cn*	指定 UNIX 組名。當使用 Active Directory 進行 LDAP 時，這是在首次建立物件時設定的，但以後可以變更。此名稱不能與其他物件相同。例如，如果您的 UNIX 使用者 user1 屬於 Linux 用戶端上名為 user1 的群組，則 Windows 不允許兩個物件具有相同 cn 屬性。若要解決此問題，請將 Windows 使用者重新命名為唯一名稱（例如 user1-UNIX）； Google Cloud NetApp Volumes 中的 LDAP 使用 uid 屬性作為 UNIX 使用者名稱。
gid編號*	指定 UNIX 群組數字 ID。
物件類別*	指定正在使用的物件類型； Google Cloud NetApp Volumes要求將群組包含在物件類別清單中（預設情況下，此屬性包含在大多數 Active Directory 部署中）。
會員ID	指定哪些 UNIX 使用者是 UNIX 群組的成員。使用Google Cloud NetApp Volumes中的 Active Directory LDAP，此欄位不是必要的。 Google Cloud NetApp Volumes LDAP 模式使用成員欄位來表示群組成員資格。
成員*	對於群組成員身分/次要 UNIX 群組是必需的。透過將 Windows 使用者新增至 Windows 群組來填入此欄位。但是，如果 Windows 群組沒有填入 UNIX 屬性，則它們不會包含在 UNIX 使用者的群組成員資格清單中。任何需要在 NFS 中可用的群組都必須填入此表中列出的所需 UNIX 群組屬性。

*表示該屬性是Google Cloud NetApp Volumes正常功能所必需的。其餘屬性僅供客戶端使用。

LDAP 綁定資訊

若要查詢 LDAP 中的用戶， Google Cloud NetApp Volumes必須綁定（登入）到 LDAP 服務。此登入具有唯讀權限，用於查詢 LDAP UNIX 屬性以進行目錄查找。目前，只有使用 SMB 機器帳戶才可以進行 LDAP 綁定。

只能為以下物件啟用 LDAP `NetApp Volumes-Performance`實例並將其用於 NFSv3、NFSv4.1 或雙重協定磁碟區。必須在與Google Cloud NetApp Volumes磁碟區相同的區域建立 Active Directory 連線才能成功部署啟用

LDAP 的磁碟區。

啟用LDAP後，在特定場景下會出現以下情況。

- 如果Google Cloud NetApp Volumes專案僅使用 NFSv3 或 NFSv4.1，則會在 Active Directory 網域控制站中建立新的機器帳戶，而Google Cloud NetApp Volumes中的 LDAP 用戶端會使用該機器帳戶憑證綁定至 Active Directory。沒有為 NFS 磁碟區建立 SMB 共用，且預設為隱藏管理共用（請參閱"預設隱藏共享") 已刪除共用 ACL。
- 如果Google Cloud NetApp Volumes專案使用雙協定卷，則僅使用為 SMB 存取權建立的單一機器帳戶將Google Cloud NetApp Volumes中的 LDAP 用戶端綁定到 Active Directory。不建立額外的機器帳戶。
- 如果單獨建立專用的 SMB 磁碟區（在啟用具有 LDAP 的 NFS 磁碟區之前或之後），則 LDAP 綁定的機器帳戶將與 SMB 機器帳戶共用。
- 如果也啟用了 NFS Kerberos，則會建立兩個機器帳戶 - 一個用於 SMB 共用和/或 LDAP 綁定，一個用於 NFS Kerberos 驗證。

LDAP 查詢

儘管 LDAP 綁定是加密的，但 LDAP 查詢是透過使用通用 LDAP 連接埠 389 以純文字形式透過網路傳遞的。目前無法在Google Cloud NetApp Volumes中變更此知名連接埠。因此，有權在網路中嗅探資料包的人可以看到使用者和群組名稱、數字 ID 和群組成員身分。

但是，Google Cloud VM 無法嗅探其他 VM 的單播流量。只有主動參與 LDAP 流量（即能夠綁定）的虛擬機器才能看到來自 LDAP 伺服器的流量。有關Google Cloud NetApp Volumes中的資料包嗅探的更多信息，請參閱"資料包嗅探/追蹤注意事項。"

LDAP 用戶端配置預設設定

在Google Cloud NetApp Volumes實例中啟用 LDAP 時，預設會使用特定的設定詳細資訊建立 LDAP 用戶端設定。在某些情況下，選項不適用於Google Cloud NetApp Volumes （不受支援）或不可設定。

LDAP 用戶端選項	它的作用	預設值	可以改嗎？
LDAP 伺服器列表	設定用於查詢的 LDAP 伺服器名稱或 IP 位址。這不適用於Google Cloud NetApp Volumes。相反，Active Directory 網域用於定義 LDAP 伺服器。	未設定	不
Active Directory 網域	設定用於 LDAP 查詢的 Active Directory 網域。Google Cloud NetApp Volumes利用 DNS 中 LDAP 的 SRV 記錄來尋找網域中的 LDAP 伺服器。	設定為 Active Directory 連線中指定的 Active Directory 網域。	不
首選 Active Directory 伺服器	設定用於 LDAP 的首選 Active Directory 伺服器。不受Google Cloud NetApp Volumes支援。相反，使用 Active Directory 網站來控制 LDAP 伺服器選擇。	未設定。	不

LDAP 用戶端選項	它的作用	預設值	可以改嗎？
使用 SMB 伺服器憑證綁定	使用 SMB 機器帳戶綁定到 LDAP。目前， Google Cloud NetApp Volumes中唯一支援的 LDAP 綁定方法。	真的	不
架構模板	用於 LDAP 查詢的架構模板。	MS-AD-BIS	不
LDAP 伺服器連接埠	用於 LDAP 查詢的連接埠號碼。 Google Cloud NetApp Volumes目前僅使用標準 LDAP 連接埠 389。 LDAPS/連接埠 636 目前不受支援。	389	不
LDAPS 是否已啟用	控制是否使用安全通訊端層 (SSL) 上的 LDAP 進行查詢和綁定。目前不受Google Cloud NetApp Volumes支援。	錯誤的	不
查詢超時（秒）	查詢超時。如果查詢時間超過指定值，則查詢失敗。	3	不
最低綁定身份驗證級別	支援的最低綁定等級。由於Google Cloud NetApp Volumes使用機器帳戶進行 LDAP 綁定，而 Active Directory 預設不支援匿名綁定，因此此選項對於安全性不起作用。	匿名的	不
綁定 DN	使用簡單綁定時用於綁定的使用者/專有名稱 (DN)。Google Cloud NetApp Volumes使用機器帳戶進行 LDAP 綁定，目前不支援簡單綁定驗證。	未設定	不
基本 DN	用於 LDAP 搜尋的基本 DN。	用於 Active Directory 連線的 Windows 網域，採用 DN 格式（即 DC=domain、DC=local ）。	不
基本搜尋範圍	基本 DN 搜尋的搜尋範圍。值可以包括 base 、onelevel 或 subtree。Google Cloud NetApp Volumes僅支援子樹搜尋。	子樹	不

LDAP 用戶端選項	它的作用	預設值	可以改嗎？
用戶 DN	定義使用者開始搜尋 LDAP 查詢的 DN。目前不支援Google Cloud NetApp Volumes，因此所有使用者搜尋都從基本 DN 開始。	未設定	不
用戶搜尋範圍	用戶 DN 搜尋的搜尋範圍。值可以包括 base、onelevel 或 subtree。Google Cloud NetApp Volumes不支援設定使用者搜尋範圍。	子樹	不
群組 DN	定義 LDAP 查詢的群組搜尋開始的 DN。目前不支援Google Cloud NetApp Volumes，因此所有群組搜尋都從基本 DN 開始。	未設定	不
群組搜尋範圍	群組 DN 搜尋的搜尋範圍。值可以包括 base、onelevel 或 subtree。Google Cloud NetApp Volumes不支援設定群組搜尋範圍。	子樹	不
網路群組 DN	定義網路群組搜尋 LDAP 查詢的起始 DN。目前不支援Google Cloud NetApp Volumes，因此所有網路群組搜尋都從基本 DN 開始。	未設定	不
網路組搜尋範圍	網路群組 DN 搜尋的搜尋範圍。值可以包括 base、onelevel 或 subtree。Google Cloud NetApp Volumes不支援設定網路群組搜尋範圍。	子樹	不
透過 LDAP 使用 start_tls	利用 Start TLS 透過連接埠 389 建立基於憑證的 LDAP 連線。目前不受Google Cloud NetApp Volumes支援。	錯誤的	不
啟用按主機尋找網路群組	啟用按主機名稱尋找網路群組，而不是擴充網路群組來列出所有成員。目前不受Google Cloud NetApp Volumes支援。	錯誤的	不

LDAP 用戶端選項	它的作用	預設值	可以改嗎？
按主機 DN 劃分的網路群組	定義 LDAP 查詢的 netgroup-by-host 搜尋開始的 DN。 Google Cloud NetApp Volumes目前不支援 Netgroup-by-host。	未設定	不
Netgroup-by-host 搜尋範圍	依主機 DN 搜尋的網路群組搜尋範圍。值可以包括 base、onelevel 或 subtree。 Google Cloud NetApp Volumes目前不支援 Netgroup-by-host。	子樹	不
客戶端會話安全	定義 LDAP 使用的會話安全等級（簽章、印章或無）。如果 Active Directory 提出請求， NetApp Volumes-Performance 將支援 LDAP 簽章。 NetApp Volumes-SW 不支援 LDAP 簽章。對於這兩種服務類型，目前不支援密封。	沒有任何	不
LDAP 引用追蹤	當使用多個 LDAP 伺服器時，如果在第一個伺服器中找不到條目，則引用追蹤允許客戶端引用清單中的其他 LDAP 伺服器。 Google Cloud NetApp Volumes目前不支援此功能。	錯誤的	不
群組成員資格過濾器	提供自訂 LDAP 搜尋過濾器，用於從 LDAP 伺服器尋找群組成員身分。目前不支援Google Cloud NetApp Volumes。	未設定	不

使用 **LDAP** 進行非對稱名稱映射

預設情況下， Google Cloud NetApp Volumes會雙向對應具有相同使用者名稱的 Windows 用戶和 UNIX 用戶，無需特殊配置。只要Google Cloud NetApp Volumes可以找到有效的 UNIX 使用者（使用 LDAP），就會發生 1:1 名稱對映。例如，如果 Windows 用戶 `johnsmith`然後，如果Google Cloud NetApp Volumes可以找到名為 `johnsmith`在 LDAP 中，該使用者的名稱對應成功，由該使用者建立的所有檔案/資料夾 `johnsmith`顯示正確的使用者所有權，以及所有影響的 ACL `johnsmith`無論使用何種 NAS 協議，都將受到尊重。這被稱為對稱名稱映射。

非對稱名稱對映是指 Windows 使用者和 UNIX 使用者身分不符的情況。例如，如果 Windows 用戶 `johnsmith`具有 `UNIX 身份 `jsmith`， Google Cloud NetApp Volumes需要一種方法來獲知該變化。由於Google Cloud NetApp Volumes目前不支援建立靜態名稱對應規則，因此必須使用 LDAP 來尋找 Windows 和 UNIX 身份的使用者身份，以確保檔案和資料夾的正確所有權和預期權限。

預設情況下， Google Cloud NetApp Volumes包含 `LDAP`在名稱對映資料庫執行個體的 ns-switch 中，以便透

過使用 LDAP 為非對稱名稱提供名稱對映功能，您只需修改一些使用者/群組屬性以反映Google Cloud NetApp Volumes所尋找的內容。

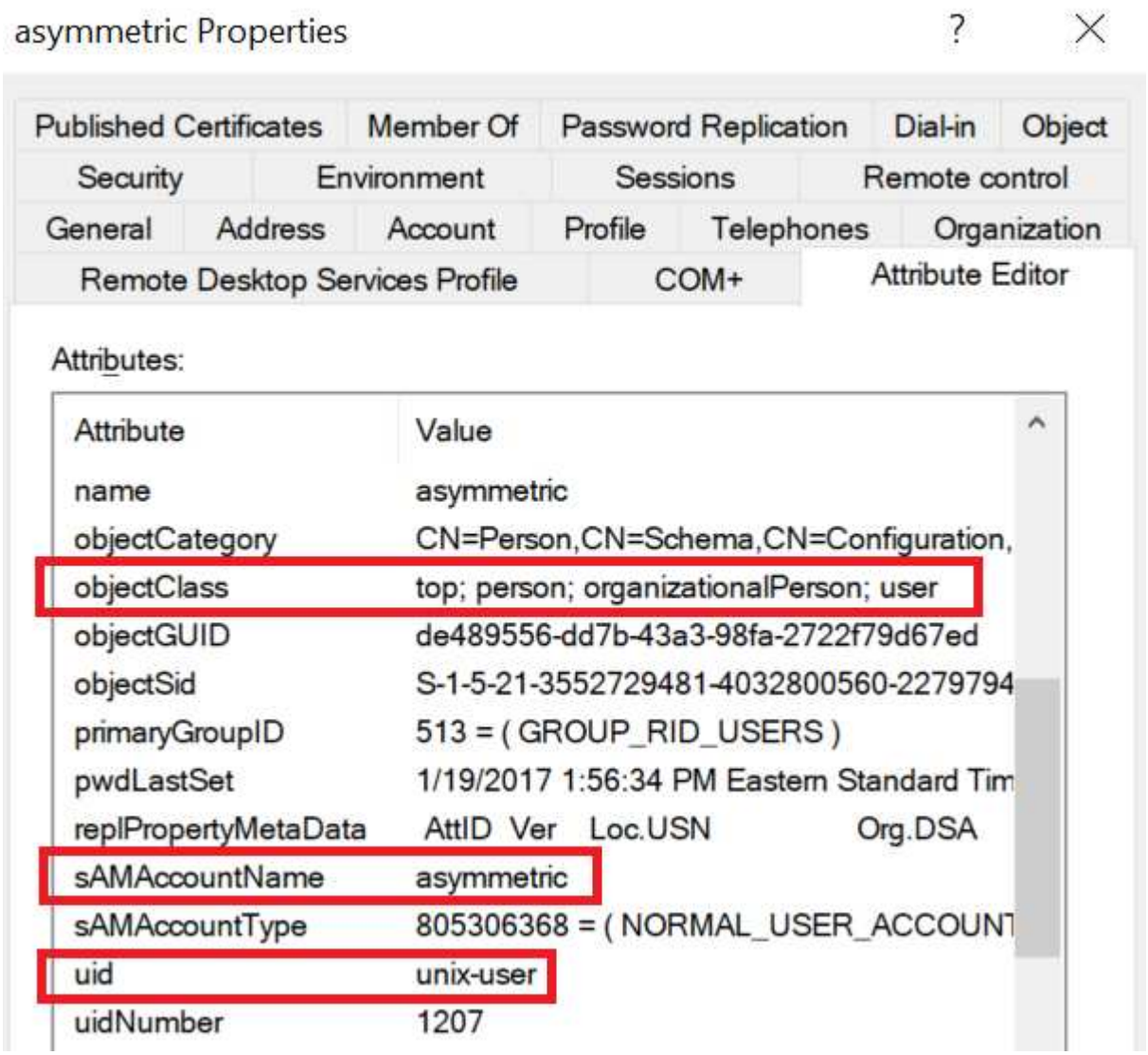
下表顯示了 LDAP 中必須填入哪些屬性才能實現非對稱名稱對應功能。在大多數情況下，Active Directory 已經設定為執行此操作。

Google Cloud NetApp Volumes屬性	它的作用	**Google Cloud NetApp Volumes**用於名稱對映的值
Windows 到 UNIX 物件類	指定正在使用的物件的類型。 （即使用者、群組、posixAccount 等）	必須包含使用者（如果需要，可以包含多個其他值。）
Windows 到 UNIX 屬性	在建立時定義 Windows 使用者名稱。 Google Cloud NetApp Volumes使用它來進行 Windows 到 UNIX 的查找。	這裡不需要更改；sAMAccountName 與 Windows 登入相同。
唯一識別符	定義 UNIX 使用者名稱。	所需的 UNIX 使用者名稱。

Google Cloud NetApp Volumes目前在 LDAP 尋找中不使用網域前綴，因此多網域 LDAP 環境無法正常進行 LDAP 名稱對應查找。

以下範例顯示了具有 Windows 名稱的用戶 `asymmetric`，UNIX 名稱 `unix-user`，以及從 SMB 和 NFS 寫入檔案時所遵循的行為。

下圖顯示了 LDAP 屬性在 Windows 伺服器上的樣子。



從 NFS 用戶端，您可以查詢 UNIX 名稱，但不能查詢 Windows 名稱：

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

當檔案從 NFS 寫入時 `unix-user`，以下是來自 NFS 客戶端的結果：

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

從 Windows 用戶端，您可以看到檔案的擁有者已設定為正確的 Windows 用戶：

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

相反，Windows 用戶建立的文件 `asymmetric`從 SMB 用戶端顯示正確的 UNIX 擁有者，如下文所示。

中小企業：

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS：

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user          sharedgroup    14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP 通道綁定

由於 Windows Active Directory 網域控制站存在漏洞， "Microsoft 安全公告 ADV190023"改變 DC 允許 LDAP 綁定的方式。

對Google Cloud NetApp Volumes的影響與對任何 LDAP 用戶端的影響相同。 Google Cloud NetApp Volumes目前不支援通道綁定。由於Google Cloud NetApp Volumes透過協商預設支援 LDAP 簽名，因此 LDAP 通道綁定應該不是問題。如果您在啟用通道綁定的情況下確實遇到 LDAP 綁定問題，請按照 ADV190023 中的修復步驟操作，以允許Google Cloud NetApp Volumes的 LDAP 綁定成功。

DNS

Active Directory 和 Kerberos 都依賴 DNS 來實作主機名稱到 IP/IP 到主機名稱的解析。 DNS 要求連接埠 53 處於開啟狀態。 Google Cloud NetApp Volumes不會對 DNS 記錄進行任何修改，目前也不支援使用 "動態 DNS"在網路介面上。

您可以設定 Active Directory DNS 來限制哪些伺服器可以更新 DNS 記錄。有關更多信息，請參閱 "安全性 Windows DNS" 。

請注意，Google 專案內的資源預設使用 Google Cloud DNS，它與 Active Directory DNS 無關。使用 Cloud DNS 的用戶端無法解析Google Cloud NetApp Volumes傳回的 UNC 路徑。加入 Active Directory 網域的 Windows 用戶端配置為使用 Active Directory DNS，並且可以解析此類 UNC 路徑。

若要將用戶端參加 Active Directory，您必須設定其 DNS 組態為使用 Active Directory DNS。您也可以選擇設定 Cloud DNS 將要求轉送至 Active Directory DNS。如需詳細資訊，請參閱 "為什麼我的客戶端無法解析 SMB NetBIOS 名稱？"。

Google Cloud NetApp Volumes目前不支援 DNSSEC，DNS 查詢以純文字形式執行。

文件存取審計

目前不支援Google Cloud NetApp Volumes。

防毒保護

您必須在 NAS 共用用戶端的Google Cloud NetApp Volumes中執行防毒掃描。目前， Google Cloud NetApp Volumes尚未實現本機防毒整合。

服務營運

Google Cloud NetApp Volumes團隊管理 Google Cloud 中的後端服務，並使用多種策略來保護平台安全並防止不必要的存取。

每個客戶都有自己獨特的子網，預設情況下，該子網路的存取權限與其他客戶隔離，而Google Cloud NetApp Volumes中的每個租用戶都有自己的命名空間和 VLAN，以實現完全的資料隔離。使用者通過身份驗證後，服務交付引擎 (SDE) 只能讀取特定於該租用戶的設定資料。

實體安全

經過適當的預先批准，只有現場工程師和帶有NetApp標誌的現場支援工程師 (FSE) 才能進入籠子和機架進行實體工作。不允許儲存和網路管理。只有這些現場資源能夠執行硬體維護任務。

對於現場工程師，將提出工作說明書 (SOW) 的票證，其中包括機架 ID 和設備位置 (RU)，所有其他詳細資訊都包含在票證中。對於NetApp FSE，必須向 COLO 提出現場訪問票，票上應包含訪客的詳細資料、日期和時間，以供審計。 FSE 的 SOW 在內部傳達給NetApp。

營運團隊

Google Cloud NetApp Volumes的營運團隊由Google Cloud NetApp Volumes的生產工程和站點可靠性工程師 (SRE) 以及硬體的NetApp現場支援工程師和合作夥伴組成。所有營運團隊成員均已獲得在 Google Cloud 工作的認證，每張提出的工單都會保留詳細的工作記錄。此外，還制定了嚴格的變更控制和批准流程，以確保每個決策都經過適當的審查。

SRE 團隊管理控制平面以及如何將資料從 UI 請求路由到Google Cloud NetApp Volumes中的後端硬體和軟體。 SRE 團隊也管理系統資源，例如磁碟區和 inode 最大值。 SRE 不得與客戶資料互動或存取客戶資料。 SRE 還提供與退貨授權 (RMA) 的協調，例如後端硬體的新磁碟或記憶體更換要求。

客戶責任

Google Cloud NetApp Volumes的客戶管理其組織的 Active Directory 和使用者角色管理以及磁碟區和資料操作。客戶可以擁有管理角色，並且可以使用NetApp和 Google Cloud 提供的兩個預先定義角色（管理員和檢視者）將權限委託給同一 Google Cloud 專案內的其他最終使用者。

管理員可以將客戶專案中的任何 VPC 與客戶認為合適的Google Cloud NetApp Volumes對等連接。客戶有責任管理對其 Google Cloud 市場訂閱的存取以及管理有權存取資料平面的 VPC。

惡意 **SRE** 保護

可能出現的一個問題是， Google Cloud NetApp Volumes如何防範惡意 SRE 或 SRE 憑證外洩的情況？

只有有限數量的 SRE 個人可以存取生產環境。管理權限進一步限制於少數經驗豐富的管理員。 Google Cloud NetApp Volumes生產環境中任何人執行的所有操作都會被記錄下來，我們的安全資訊和事件管理 (SIEM) 威脅情報平台會偵測到基準異常或可疑活動。因此，可以在對Google Cloud NetApp Volumes後端造成太大損害之前追蹤和緩解惡意行為。

卷生命週期

Google Cloud NetApp Volumes僅管理服務內的對象，而非磁碟區內的資料。只有存取卷的客戶端才能管理資料、ACL、文件擁有者等。這些磁碟區中的資料在靜止時是加密的，且存取權限僅限於Google Cloud NetApp Volumes實例的租用戶。

Google Cloud NetApp Volumes的磁碟區生命週期是建立-更新-刪除。磁碟區會保留磁碟區的 Snapshot 副本，直到磁碟區被刪除，並且只有經過驗證的Google Cloud NetApp Volumes管理員才能刪除Google Cloud NetApp Volumes中的磁碟區。當管理員要求刪除磁碟區時，需要額外輸入磁碟區名稱來驗證刪除。磁碟區被刪除後，該磁碟區將消失並且無法復原。

如果Google Cloud NetApp Volumes合約終止， NetApp會在特定時段後將磁碟區標記為刪除。在該時間段到期之前，您可以根據客戶的要求恢復卷。

認證

Google Cloud NetApp Volumes for Google Cloud 目前已通過 ISO/IEC 27001:2013 和 ISO/IEC 27018:2019 標準認證。該服務最近還收到了 SOC2 Type I 認證報告。有關NetApp對資料安全和隱私的承諾，請參閱 "合規性：資料安全和資料隱私"。

GDPR

我們對隱私權和法規遵循 GDPR 的承諾可見於我們的多項 "客戶合約"中，例如我們的 "客戶Data Processing附錄"，其中包含歐盟委員會提供的 "標準合約條款"。我們也在隱私權政策中做出這些承諾，並以我們公司行為準則中規定的核心價值為後盾。

附加資訊和聯絡資訊

要了解有關本文檔中描述的信息的更多信息，請查看以下文檔和/或網站：

- Google Google Cloud NetApp Volumes Cloud 文件

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Google 私人服務訪問

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp產品文檔

  "https://www.netapp.com/support-and-training/documentation/"

- 加密驗證模組程式 - NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- NetApp勒索軟體解決方案

https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616： ONTAP中的 NFS Kerberos

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

聯絡我們

讓我們知道如何改進這份技術報告。

請透過 doccomments@netapp.com 與我們聯絡。在主題行中包含技術報告 4918。

NetApp Disaster Recovery

適用於 **VMware** 的 **3-2-1** 資料保護，搭配 **SnapCenter** 外掛程式與 **NetApp Backup and Recovery**，以保護 **VMware** 工作負載

3-2-1 備份策略是業界認可的資料保護方法，它提供了一種全面的方法來保護寶貴的資料。這種策略是可靠的，並確保即使發生一些意外的災難，仍然可以提供資料的副本。

概況

此策略由三個基本規則組成：

1. 至少保留三份資料副本。這樣可以確保即使一個副本遺失或損壞，您仍然至少有兩個副本可以依靠。
2. 將兩個備份儲存在不同的儲存媒體或裝置上。多樣化的儲存媒體有助於防止特定於設備或特定於媒體的故障。如果一個設備損壞或一種媒體發生故障，另一個備份副本不會受到影響。
3. 最後，確保至少有一個備份副本位於異地。異地儲存可以作為防止火災或洪水等局部災害的故障保護措施，因為這些災害可能會導致現場副本無法使用。

本解決方案文件涵蓋 3-2-1 備份解決方案，使用 SnapCenter Plug-in for VMware vSphere (SCV) 建立內部部署虛擬機器的主要與次要備份，並使用虛擬機器專用的 NetApp Backup and Recovery 將資料複本備份至雲端儲存或 StorageGRID。

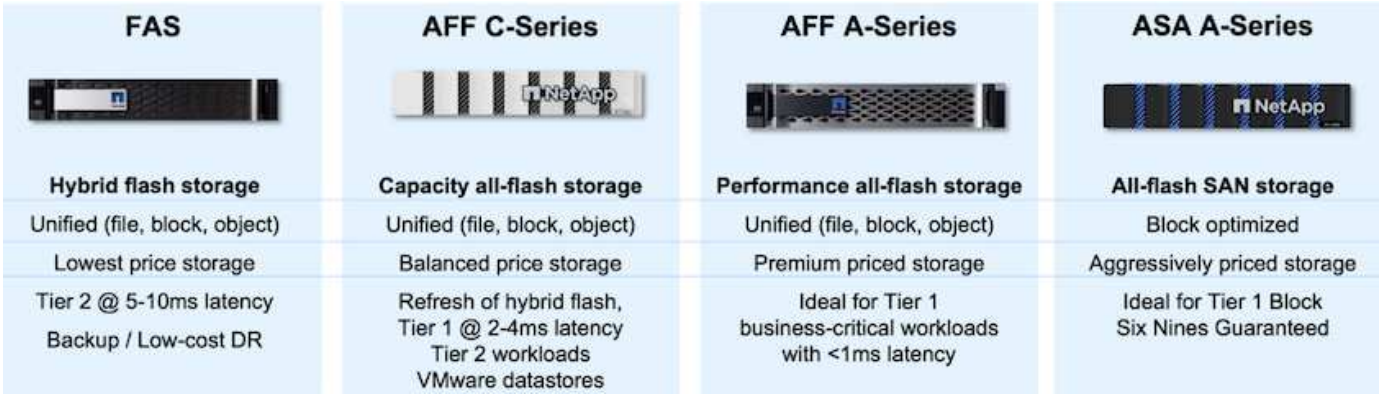
用例

此解決方案適用於以下用例：

- 使用適用於SnapCenter Plug-in for VMware vSphere備份和還原本機虛擬機器和資料儲存區。
- 備份與還原內部部署虛擬機器與資料存放區，其託管於 ONTAP 叢集，並使用適用於虛擬機器的 NetApp Backup and Recovery 備份至物件儲存。

NetApp ONTAP資料存儲

ONTAP是 NetApp 業界領先的儲存解決方案，無論您透過 SAN 還是 NAS 協定訪問，它都能提供統一儲存。 3-2-1 備份策略可確保本地資料在多種媒體類型上受到保護，並且NetApp提供從高速快閃記憶體到低成本媒體的平台。



有關 NetApp 所有硬體平台的更多信息，請查看 "NetApp資料儲存"。

SnapCenter Plug-in for VMware vSphere

VMware vSphere 的SnapCenter插件是一種資料保護產品，它與 VMware vSphere 緊密整合，可輕鬆管理虛擬機器的備份和復原。作為此解決方案的一部分， SnapMirror提供了一種快速可靠的方法，可在二級ONTAP儲存叢集上建立虛擬機器資料的第二個不可變備份副本。有了這個架構，就可以從主備份位置或輔助備份位置輕鬆啟動虛擬機器復原作業。

SCV 使用 OVA 檔案部署為 Linux 虛擬裝置。該插件現在使用遠端插件架構。遠端插件在 vCenter 伺服器之外運行，並託管在 SCV 虛擬設備上。

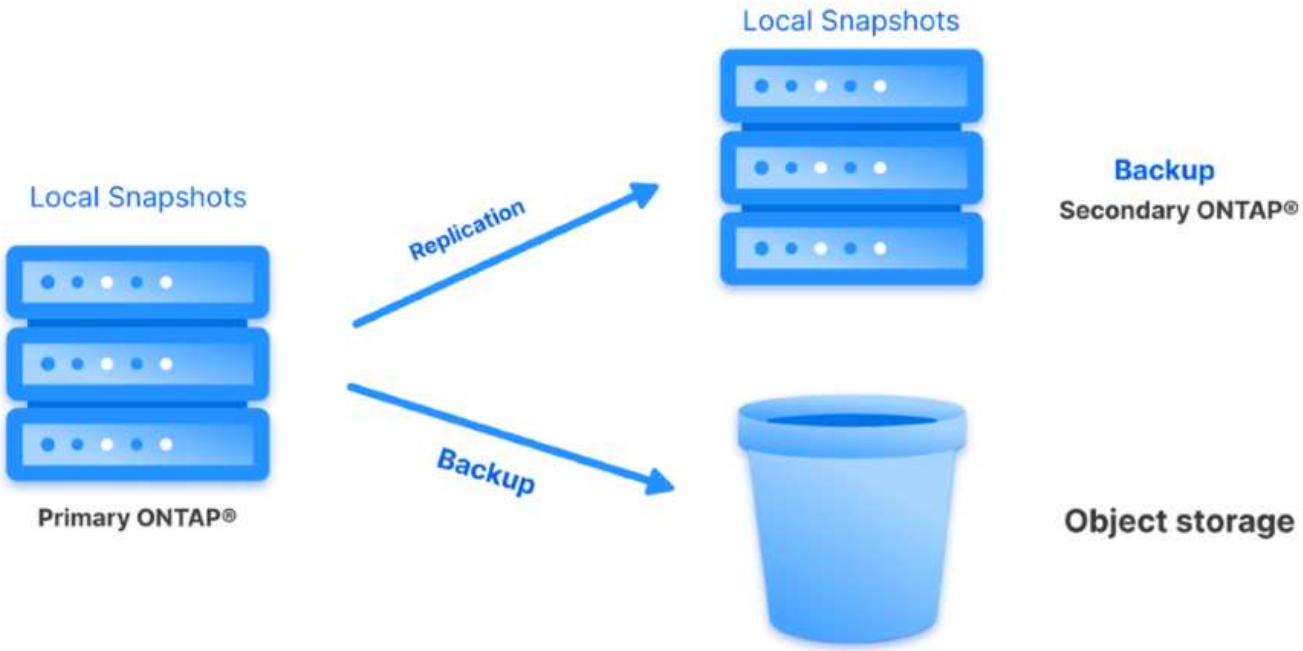
有關 SCV 的詳細信息，請參閱 "SnapCenter Plug-in for VMware vSphere文檔"。

NetApp Backup and Recovery 以保護 VMware 工作負載

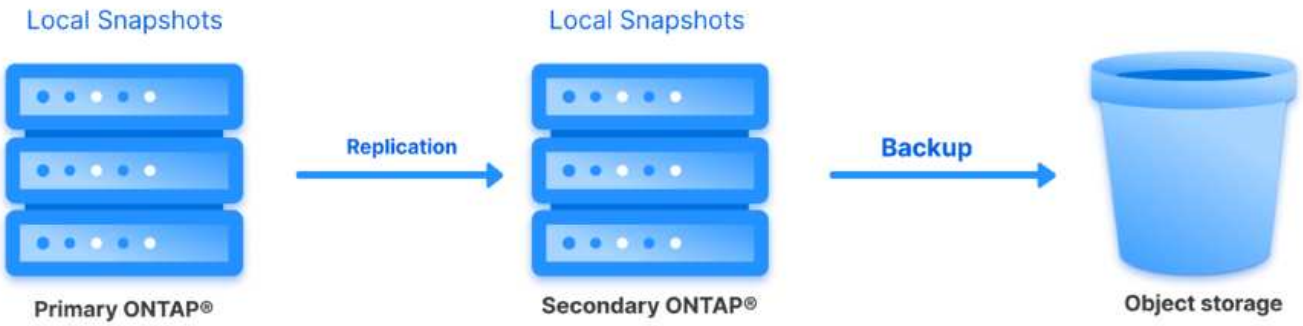
NetApp Backup and Recovery 是一款雲端型資料管理員工具，可為內部部署與雲端環境中的各種備份與還原作業提供單一控制層。NetApp Backup and Recovery for VM 套件包含一項功能，可與 SnapCenter 外掛程式（適用於 VMware vSphere ，內部部署）整合，將資料複本延伸至雲端的物件儲存。這會建立第三份異地資料複本，其來源為主儲存設備或次要儲存設備備份。NetApp Backup and Recovery for VMs 可讓您輕鬆設定儲存設備原則，從這兩個內部部署位置的任一個傳輸資料複本。

在 NetApp Backup and Recovery 中選擇主要或次要備份作為來源，將會實作兩種拓撲的其中一種：

連出拓撲 – 當 SnapCenter Plug-in for VMware vSphere 啟動備份時，會立即建立本機快照。然後，SCV 會啟動 SnapMirror 作業，將最新的快照複寫到次要 ONTAP 叢集。在 NetApp Backup and Recovery 中，原則會將主要 ONTAP 叢集指定為要傳輸至您所選雲端供應商之物件儲存的資料 Snapshot 複本來源。



級聯拓撲 – 使用 SCV 建立主要和次要資料複本與上述連出拓撲相同。不過，這次會在 NetApp Backup and Recovery 中建立一項原則，指定備份至物件儲存的作業將源自次要 ONTAP 叢集。



NetApp Backup and Recovery 可將內部部署 ONTAP 快照的備份複本建立至 AWS Glacier、Azure Blob 與 GCP Archive 儲存設備。







AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

此外，您可以使用NetApp StorageGRID作為物件儲存備份目標。有關StorageGRID 的更多信息，請參閱 "StorageGRID登入頁面"。

▼ 解決方案部署概述

此清單提供設定此解決方案，以及從 SCV 和 NetApp Console 執行備份與還原作業所需的高階步驟：

1. 配置ONTAP叢集之間的SnapMirror關係以用於主資料和輔助資料副本。
2. 為 VMware vSphere 配置SnapCenter插件。
   a. 新增儲存系統
   b. 建立備份策略
   c. 建立資源組
   d. 執行備份第一個備份作業
3. 為虛擬機器設定 NetApp Backup and Recovery
   a. 新增工作環境
   b. 發現 SCV 和 vCenter 設備
   c. 建立備份策略
   d. 啟動備份
4. 使用 SCV 從主儲存和輔助儲存還原虛擬機器。
5. 使用 NetApp Console 從物件儲存還原虛擬機器。

▼ 先決條件

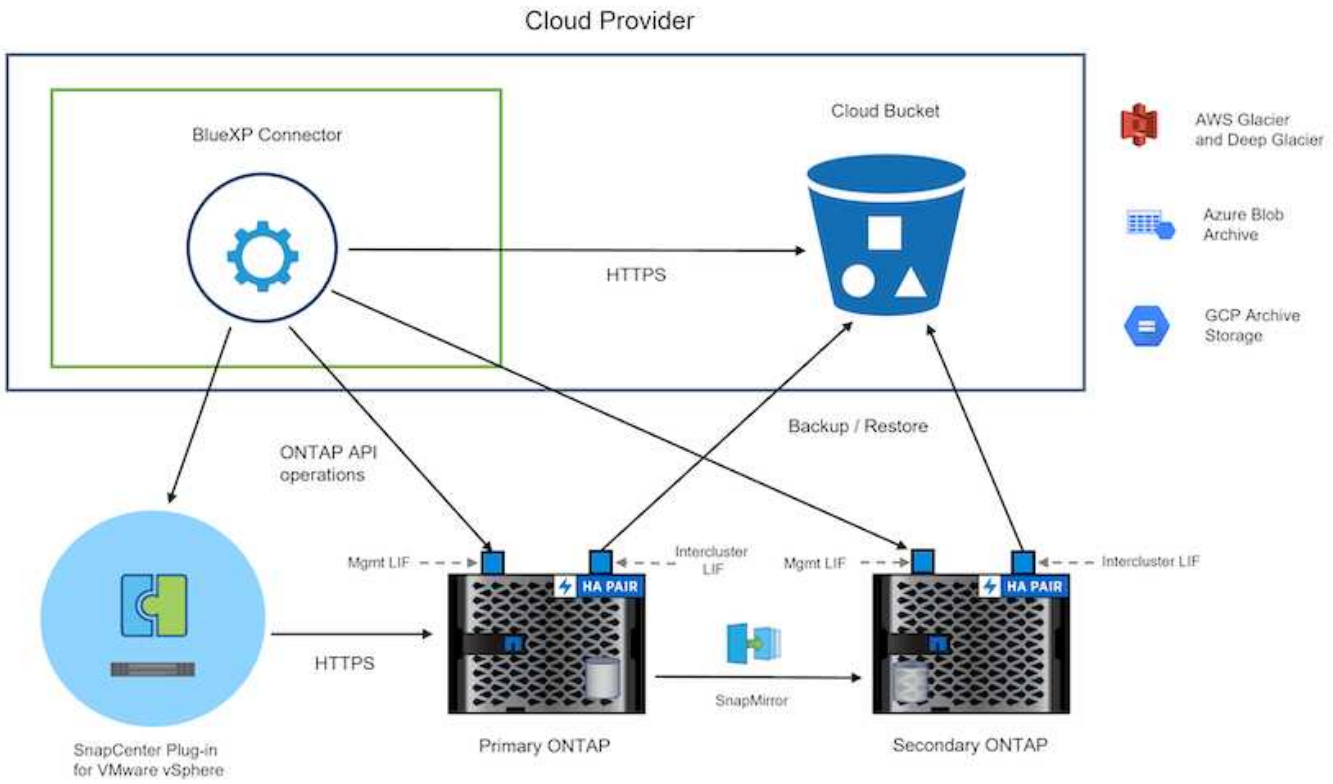
此解決方案的目的是展示在 VMware vSphere 中運行並位於NetApp ONTAP託管的 NFS 資料儲存上的虛擬機器的資料保護。此解決方案假定以下組件已配置並可供使用：

1. 具有連接到 VMware vSphere 的 NFS 或 VMFS 資料儲存的ONTAP儲存叢集。 NFS 和 VMFS 資料儲存均支援。此解決方案採用了 NFS 資料儲存。
2. 為用於 NFS 資料儲存庫的磁碟區建立了具有SnapMirror關係的輔助ONTAP儲存叢集。
3. 已為用於物件儲存備份的雲端供應商安裝主控台代理程式。
4. 要支援的虛擬機器位於主ONTAP儲存叢集上的 NFS 資料儲存庫上。

5. Console 代理程式與內部部署 ONTAP 儲存設備叢集管理介面之間的網路連線。
6. 主控台代理程式與內部部署 SCV 應用裝置 VM 之間，以及主控台代理程式與 vCenter 之間的網路連線。
7. 本機ONTAP叢集間 LIF 與物件儲存服務之間的網路連線。
8. 為主ONTAP儲存叢集和輔助 ONTAP 儲存叢集上的管理 SVM 配置的 DNS。更多資訊請參閱 "配置 DNS 以進行主機名稱解析"。

進階架構

該解決方案的測試/驗證是在實驗室中進行的，該實驗室可能與最終部署環境相匹配，也可能不匹配。



解決方案部署

在此解決方案中，我們提供詳細指示，說明如何部署與驗證利用 SnapCenter Plug-in for VMware vSphere 以及備份與還原的解決方案，以執行位於內部部署資料中心的 VMware vSphere 叢集內 Windows 和 Linux 虛擬機器的備份與還原。此設定中的虛擬機器儲存在由 ONTAP A300 儲存設備叢集所託管的 NFS 資料存放區上。此外，一個分隔的 ONTAP A300 儲存設備叢集可作為使用 SnapMirror 複寫之 Volume 的次要目的地。此外，託管在 Amazon Web Services 和 Azure Blob 上的物件儲存被用作第三個資料複本的目標。

我們將介紹為 SCV 代管的備份次要複本建立 SnapMirror 關係，以及在 SCV 和 NetApp Console 中組態備份作業。

有關適用SnapCenter Plug-in for VMware vSphere的詳細信息，請參閱 "SnapCenter Plug-in for VMware vSphere文檔"。

有關備份與還原的詳細資訊，請參閱 "備份與還原文件"。

SnapCenter Plug-in for VMware vSphere使用ONTAP SnapMirror技術來管理二級SnapMirror和/或SnapVault副本到二級ONTAP叢集的傳輸。

SCV 備份策略可以選擇使用SnapMirror或SnapVault關係式。主要區別在於，當使用SnapMirror選項時，策略中為備份配置的保留計劃在主位置和輔助位置將是相同的。 SnapVault專為歸檔而設計，使用此選項時，可以使用SnapMirror關係為二級ONTAP儲存叢集上的快照副本建立單獨的保留計畫。

設定 SnapMirror 關係可以在 NetApp Console 中完成（其中許多步驟已自動化），也可以使用 System Manager 和 ONTAP CLI 來完成。以下將討論所有這些方法。

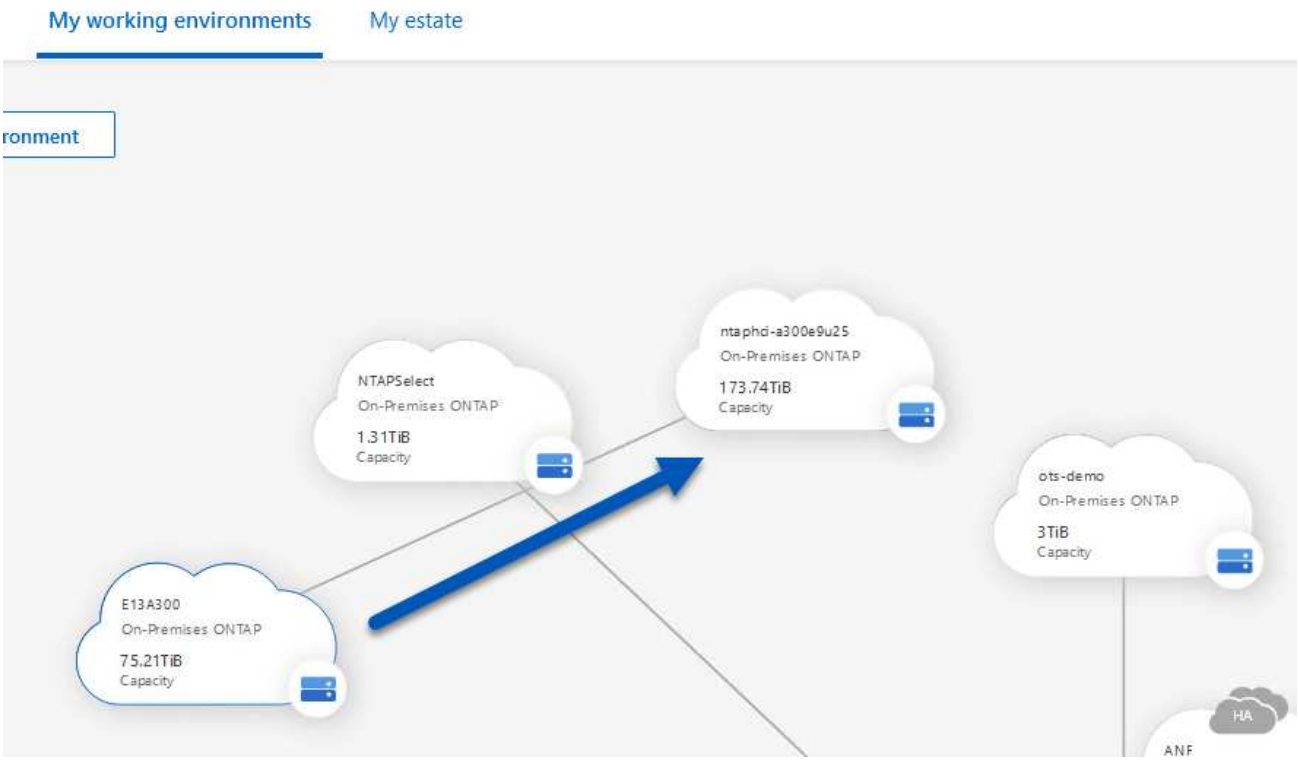
透過 **NetApp Console** 建立 **SnapMirror** 關係

以下步驟必須在 NetApp Console 中完成：

▼ 主 **ONTAP** 儲存系統和輔助**ONTAP**儲存系統的複製設置

首先登入 NetApp Console 並導覽至系統。

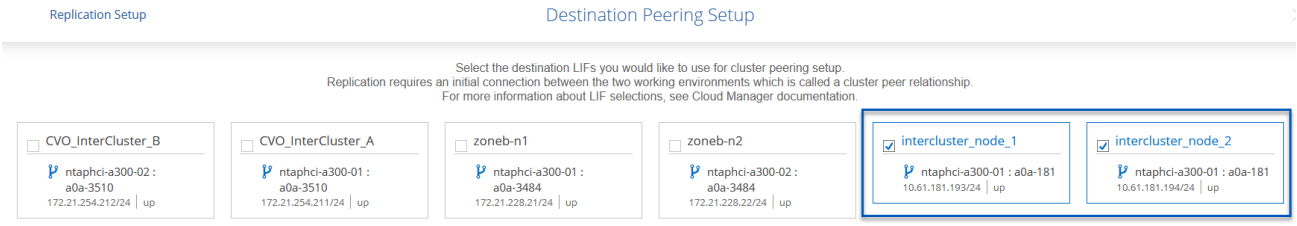
1. 將來源（主） ONTAP儲存系統拖曳到目標（輔助） ONTAP儲存系統上。



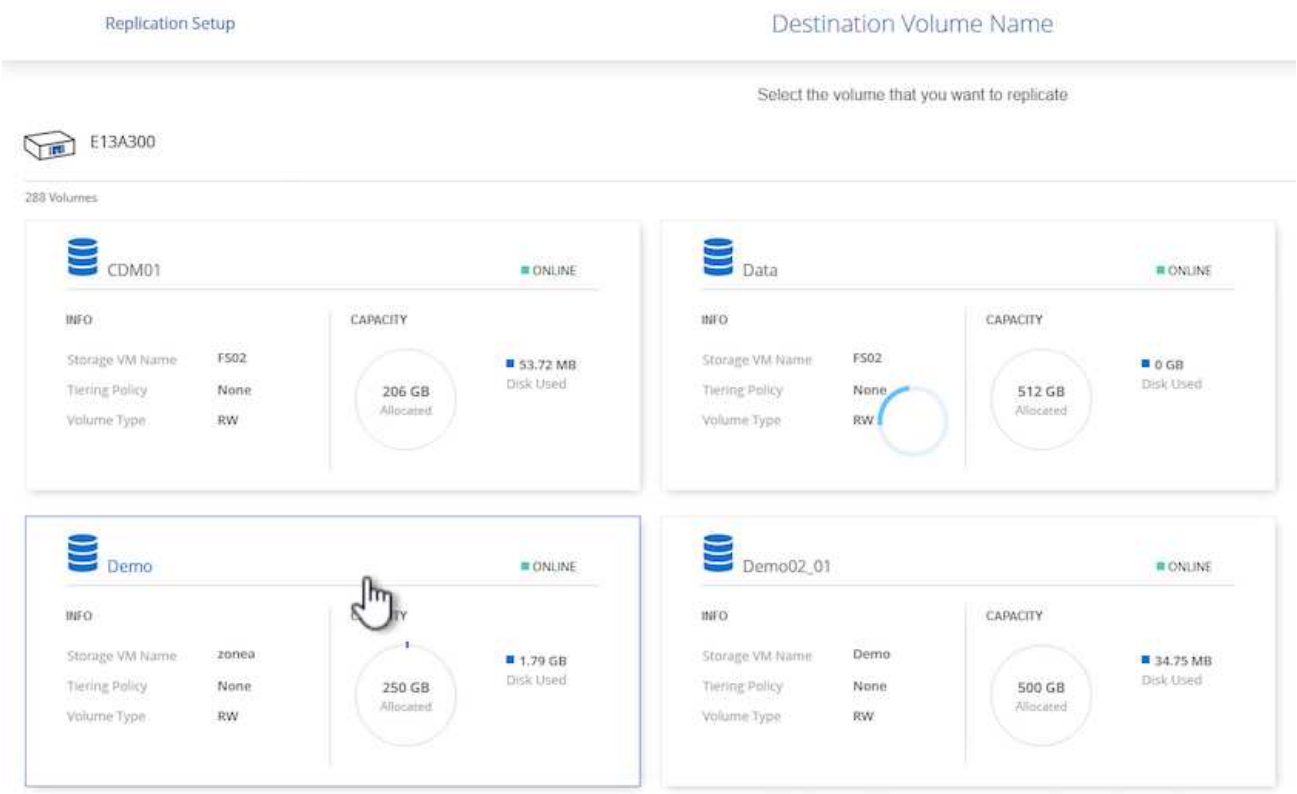
2. 從出現的選單中選擇*複製*。



3. 在「目標對等設定」頁面上，選擇用於儲存系統之間連接的目標群集間 LIF。

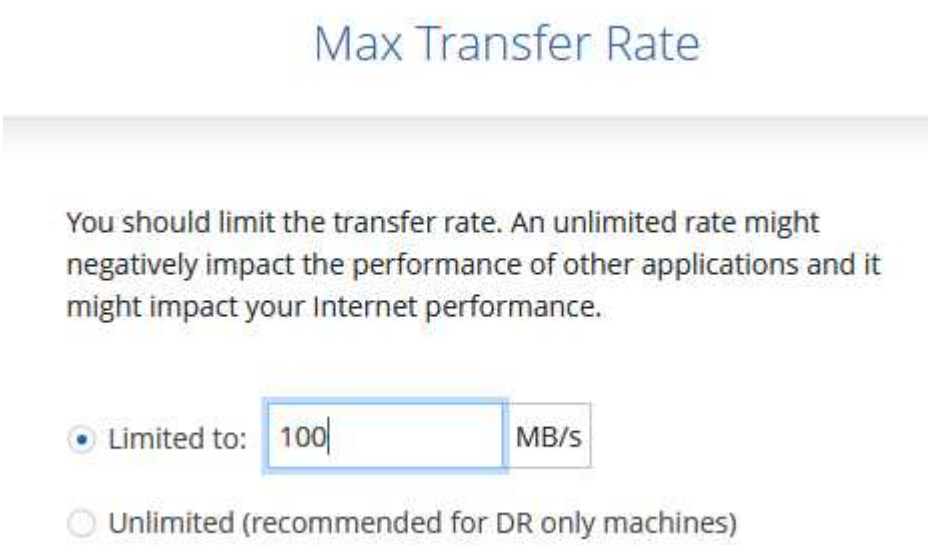


4. 在「目標卷名稱」頁面上，首先選擇來源卷，然後填寫目標卷名稱並選擇目標 SVM 和聚合。按一下“下一步”繼續。

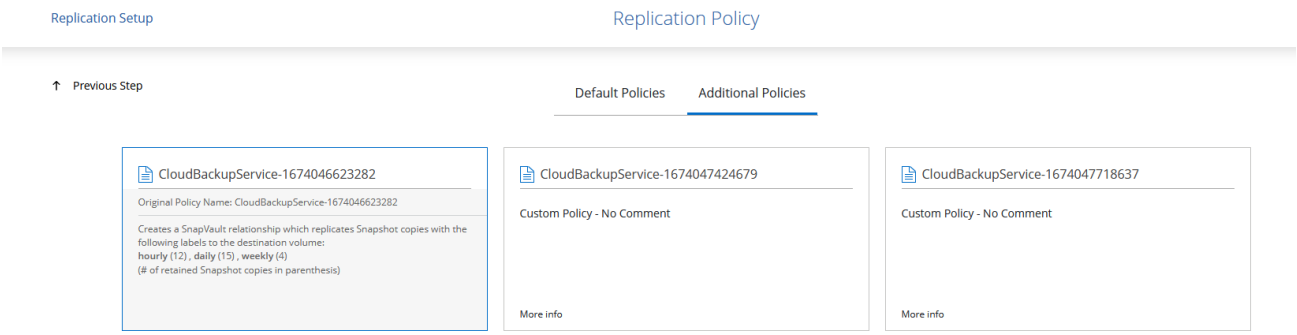




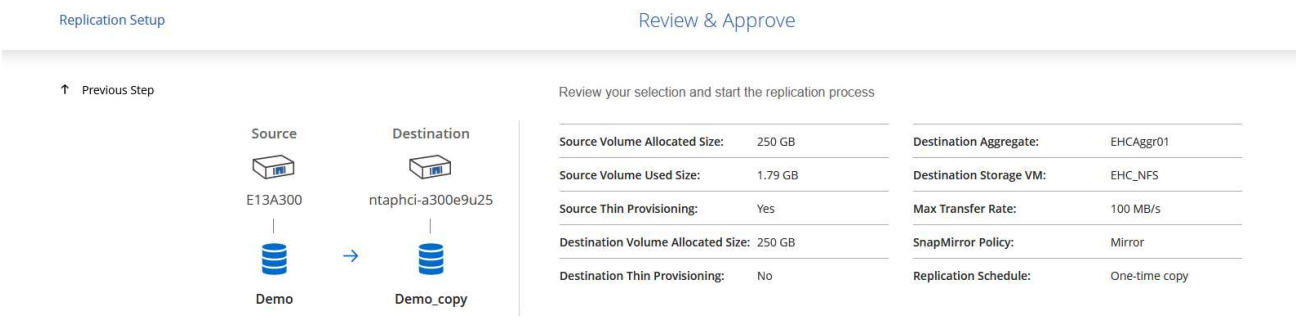
5. 選擇進行複製的最大傳輸速率。



6. 選擇確定二次備份保留計畫的策略。此策略可以預先建立（請參閱下方*建立快照保留策略*步驟中的手動程序），也可以在需要時在事後進行變更。



7. 最後，檢查所有資訊並點擊“**Go**”按鈕開始複製設定過程。



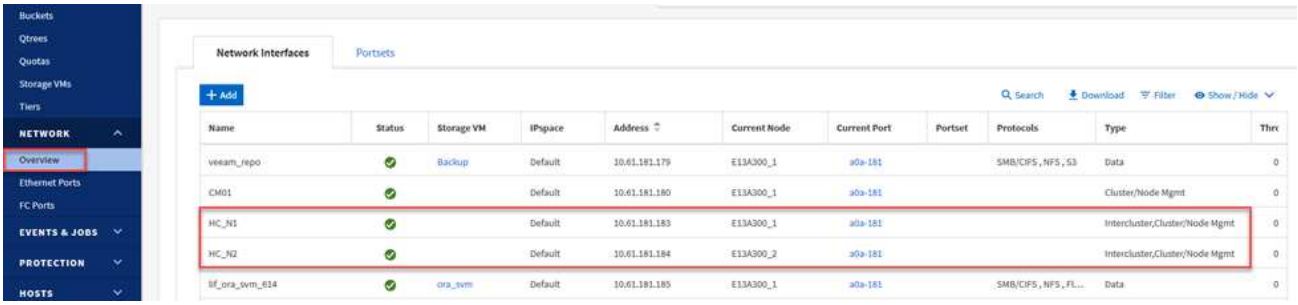
使用 **System Manager** 和**ONTAP CLI** 建立**SnapMirror**關係

建立SnapMirror關係所需的所有步驟都可以透過 System Manager 或ONTAP CLI 完成。以下部分提供了這兩種方法的詳細資訊：

▼ 記錄來源和目標集群間邏輯接口

對於來源和目標ONTAP集群，您可以從系統管理器或 CLI 檢索集群間 LIF 資訊。

1. 在ONTAP系統管理員中，導覽至網路概覽頁面並擷取配置為與安裝了 FSx 的 AWS VPC 通訊的類型：叢集間的 IP 位址。



2. 若要使用 CLI 檢索叢集間 IP 位址，請執行下列命令：

```
ONTAP-Dest::> network interface show -role intercluster
```

▼ 在**ONTAP**集群之間建立集群對等連接

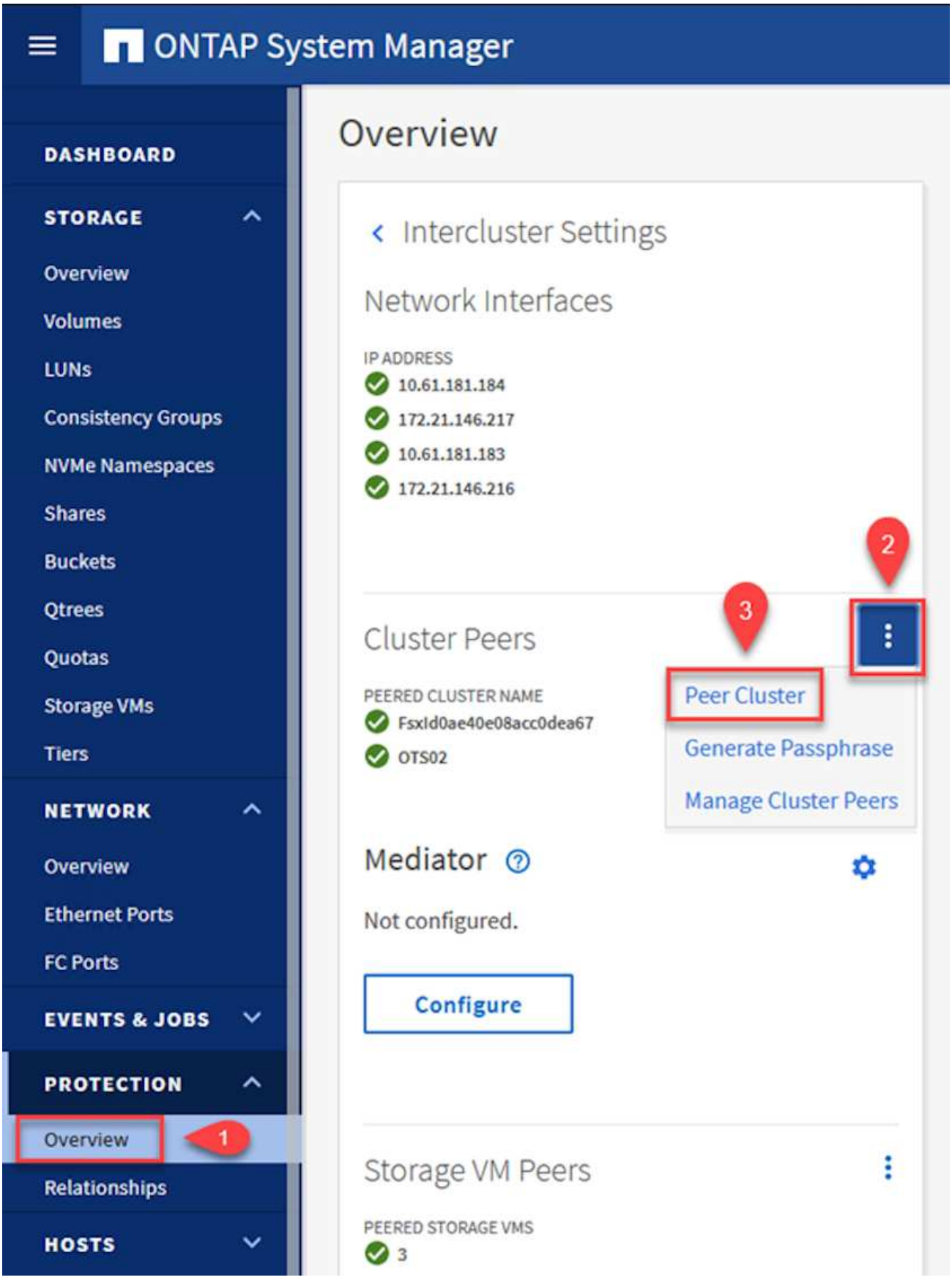
若要在ONTAP叢集之間建立叢集對等連接，必須在另一個對等叢集中確認在啟動ONTAP叢集中輸入的唯一密

碼。

1. ONTAP `cluster peer create`命令。出現提示時，請輸入稍後在來源叢集上使用的唯一密碼來完成建立程序。

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. 在來源叢集中，您可以使用ONTAP系統管理員或 CLI 建立叢集對等關係。從ONTAP系統管理員中，導覽至“保護”>“概覽”，然後選擇“對等叢集”。

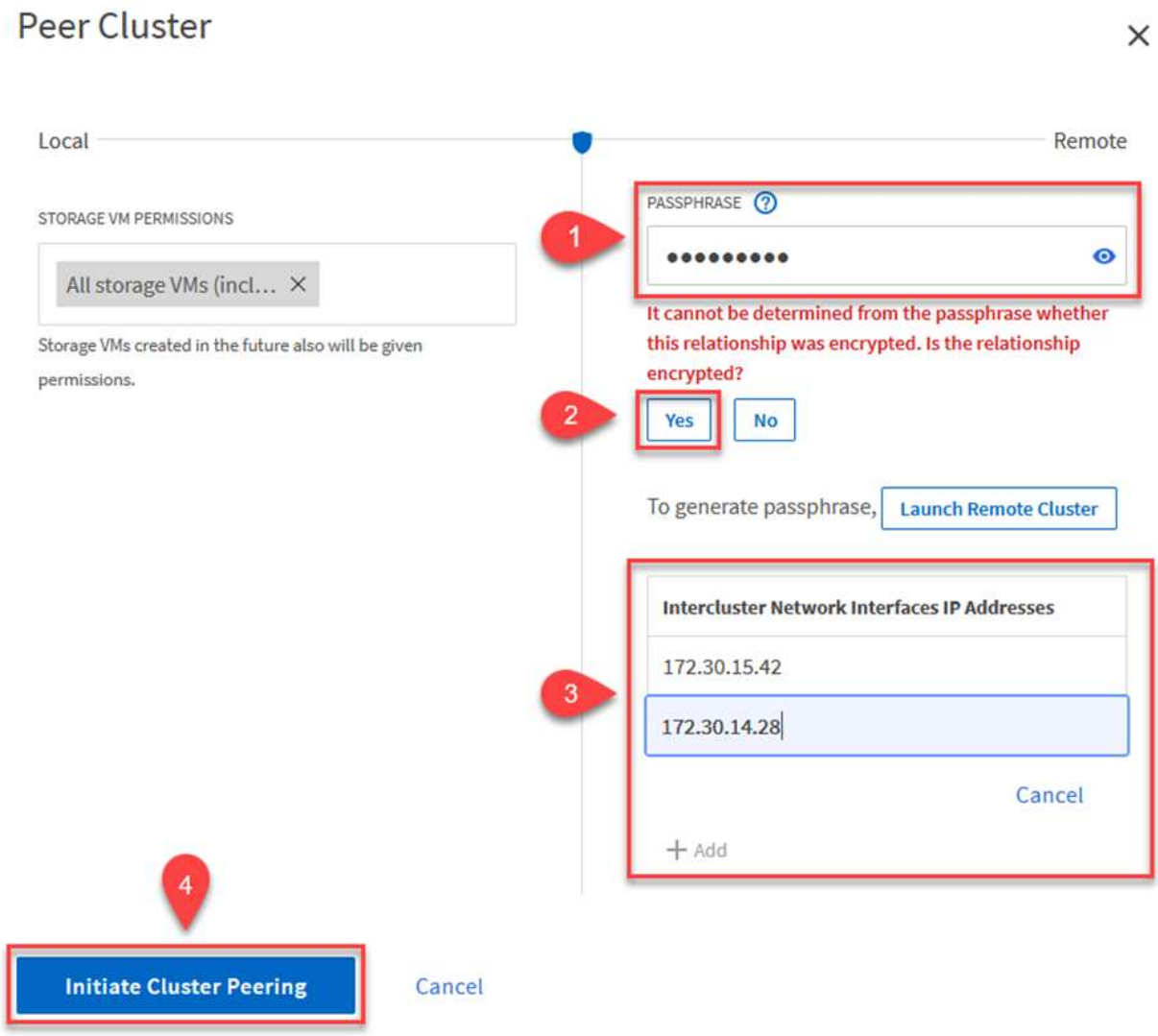


3. 在對等集群對話框中，填寫所需資訊：
   a. 輸入用於在目標ONTAP叢集上建立對等叢集關係的密碼。

b. 選擇 `Yes`建立加密關係。

c. 輸入目標ONTAP叢集的群集間 LIF IP 位址。

d. 按一下“啟動叢集對等”以完成該過程。



4. 使用以下命令從目標ONTAP叢集驗證叢集對等關係的狀態：

```
ONTAP-Dest::> cluster peer show
```

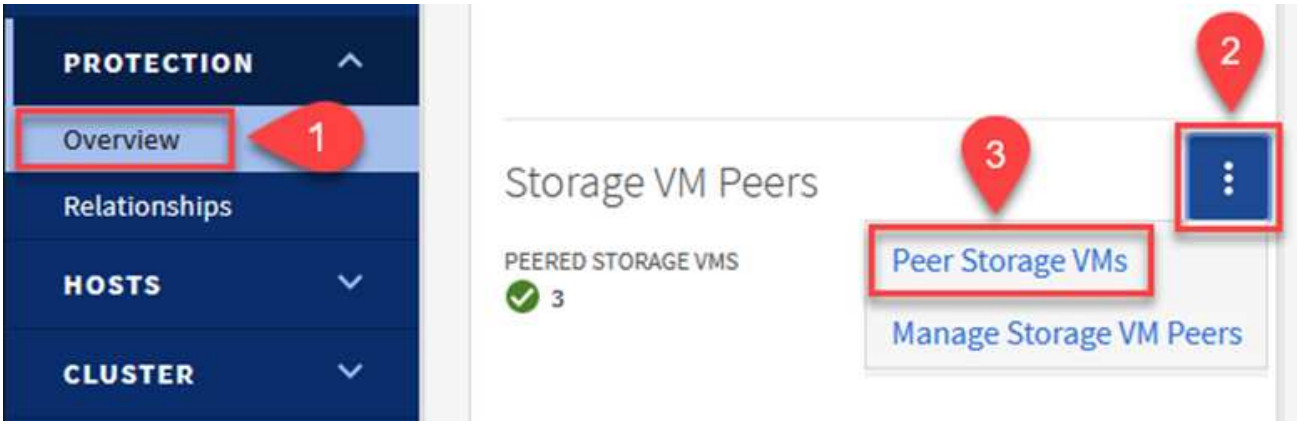
▼ 建立 **SVM** 對等關係

下一步是在包含將處於SnapMirror關係中的磁碟區的目標儲存虛擬機器和來源儲存虛擬機器之間建立 SVM 關係。

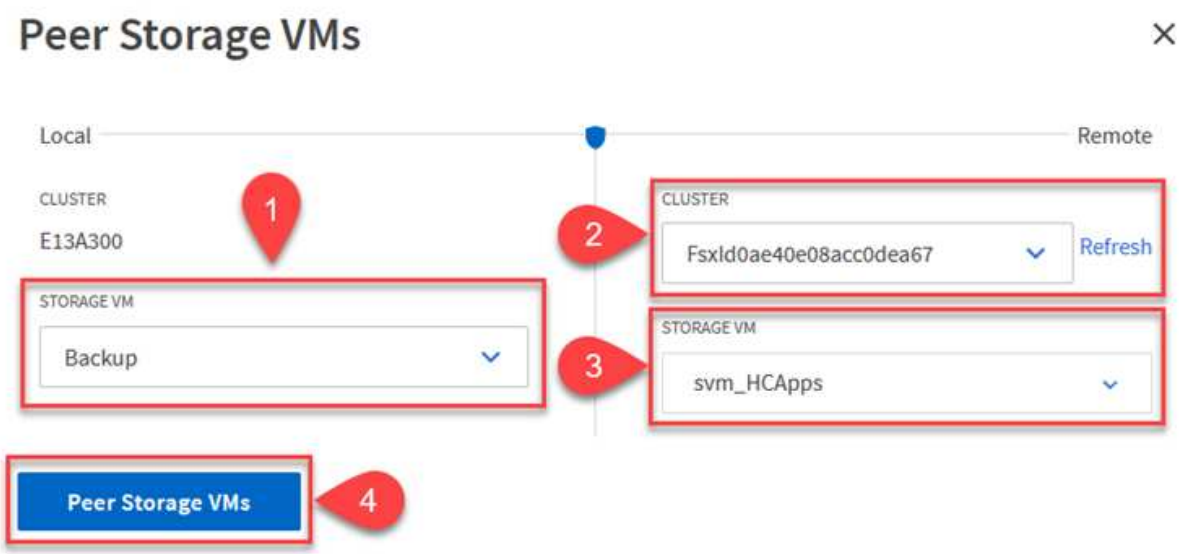
1. 從目標ONTAP集群，使用 CLI 中的以下命令建立 SVM 對等關係：

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 從來源ONTAP集群，使用ONTAP系統管理器或 CLI 接受對等關係。
3. 從ONTAP系統管理員中，前往“保護”>“概覽”，然後選擇“儲存虛擬機器對等體”下的“對等儲存虛擬機器”。



4. 在對等儲存虛擬機器的對話方塊中，填寫必填欄位：
   - 源儲存虛擬機
   - 目標集群
   - 目標儲存虛擬機



5. 按一下「對等儲存虛擬機器」以完成 SVM 對等連線程序。

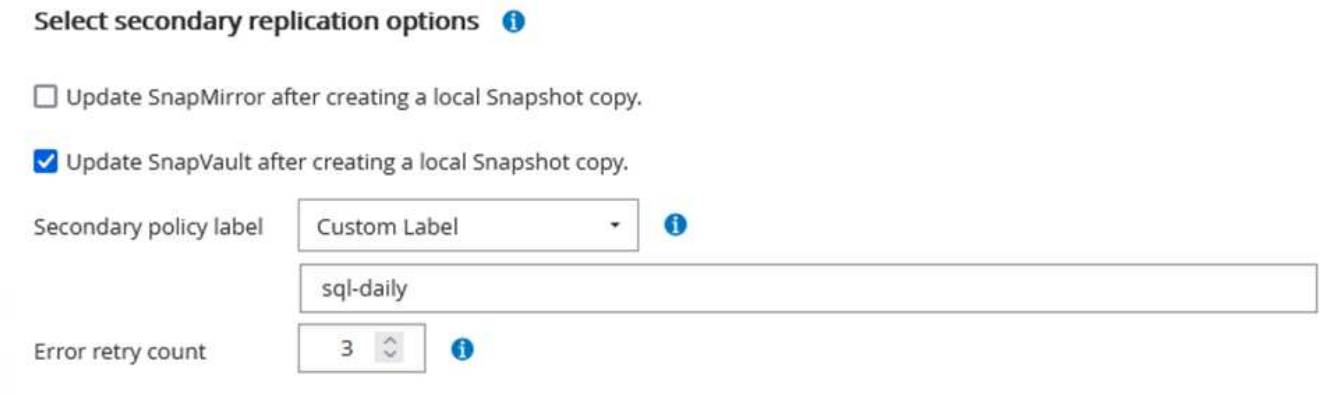
▼ 建立快照保留策略

SnapCenter管理主儲存系統上作為快照副本存在的備份的保留計畫。這是在SnapCenter中建立策略時建立的。 SnapCenter不管理保留在二級儲存系統上的備份的保留策略。這些策略透過在輔助 FSx 叢集上建立的SnapMirror策略單獨進行管理，並與與來源磁碟區具有SnapMirror關係的目標磁碟區相關聯。

建立SnapCenter策略時，您可以選擇指定一個輔助原則標籤，該標籤將會新增至執行SnapCenter備份時產生的每個快照的SnapMirror標籤。

ⓘ 在二級儲存上，這些標籤與目標磁碟區相關的策略規則相匹配，以強制保留快照。

以下範例顯示了一個SnapMirror標籤，該標籤存在於作為用於 SQL Server 資料庫和日誌卷的每日備份的政策的一部分所產生的所有快照上。



有關為 SQL Server 資料庫建立SnapCenter策略的更多信息，請參閱 "SnapCenter文檔"。

您必須先建立一個SnapMirror策略，其中包含規定要保留的快照副本數量的規則。

1. 在 FSx 叢集上建立SnapMirror策略。

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. 為具有與SnapCenter政策中指定的輔助策略標籤相符的SnapMirror標籤的政策新增規則。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

以下腳本提供了可以新增到策略的規則範例：

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

ⓘ 為每個SnapMirror標籤和要保留的快照數量（保留期）建立附加規則。

▼ 建立目標磁碟區

若要在ONTAP上建立將作為來源磁碟區快照副本接收者的目標卷，請在目標ONTAP叢集上執行下列命令：

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

▼ 在來源磁碟區和目標磁碟區之間建立**SnapMirror**關係

若要在來源磁碟區和目標磁碟區之間建立SnapMirror關係，請在目標ONTAP叢集上執行下列命令：

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

▼ 初始化**SnapMirror**關係

初始化SnapMirror關係。此程序啟動從來源磁碟區產生的新快照並將其複製到目標磁碟區。

若要建立卷，請在目標ONTAP叢集上執行以下命令：

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

SnapCenter Plug-in for VMware vSphere

安裝後，可以從 vCenter Server Appliance 管理介面存取SnapCenter Plug-in for VMware vSphere。 SCV 將管理安裝到 ESXi 主機並包含 Windows 和 Linux VM 的 NFS 資料儲存的備份。

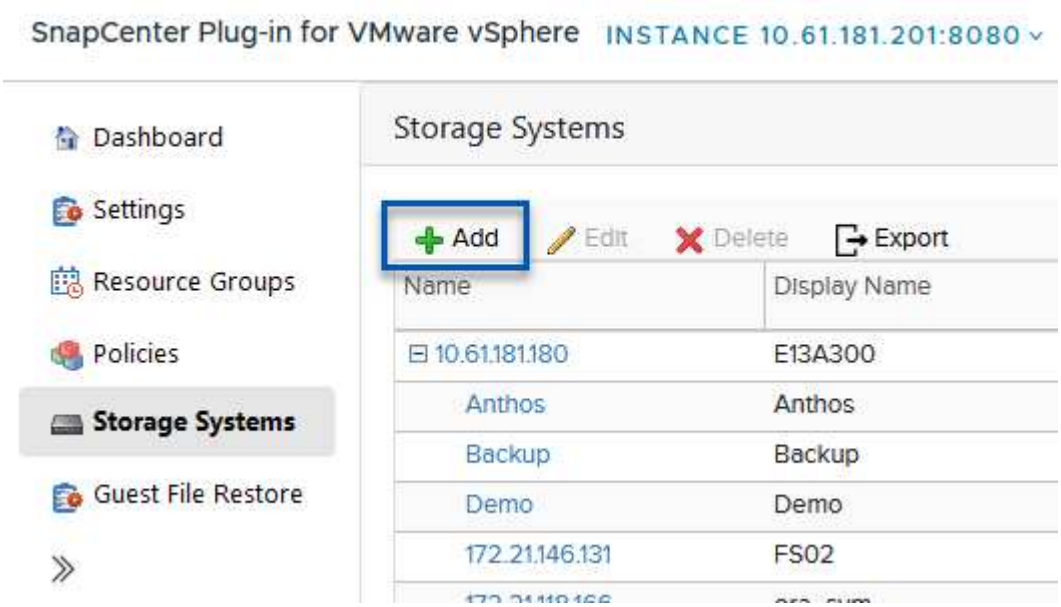
回顧 "資料保護工作流程"有關配置備份所涉及的步驟的更多信息，請參閱 SCV 文件的部分。

要設定虛擬機器和資料儲存的備份，需要從插件介面完成以下步驟。

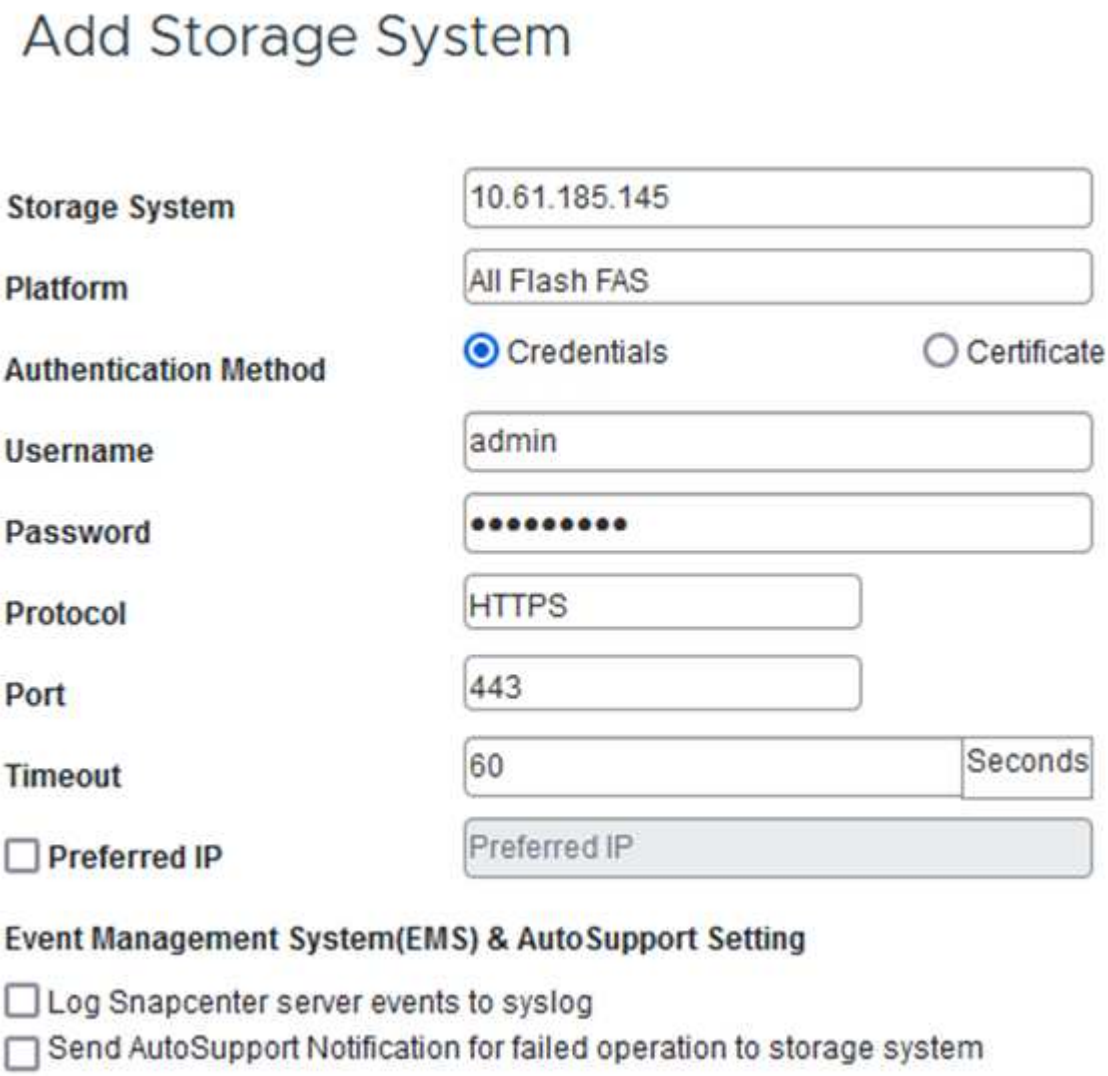
▼ **Discovery ONTAP**儲存系統

發現用於主備份和輔助備份的ONTAP儲存叢集。

1. 在SnapCenter Plug-in for VMware vSphere中，導覽至左側選單中的“儲存系統”，然後按一下“新增”按鈕。



2. 填寫主ONTAP儲存系統的憑證和平台類型，然後按一下「新增」。



3. 對輔助ONTAP儲存系統重複此程序。

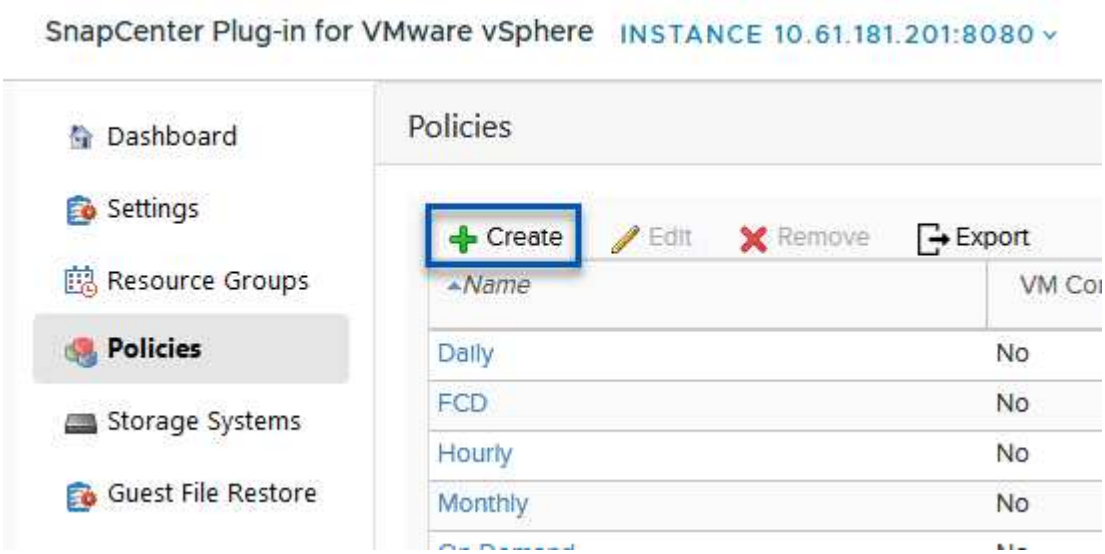
▼ 建立 **SCV** 備份策略

策略指定 SCV 管理的備份的保留期、頻率和複製選項。

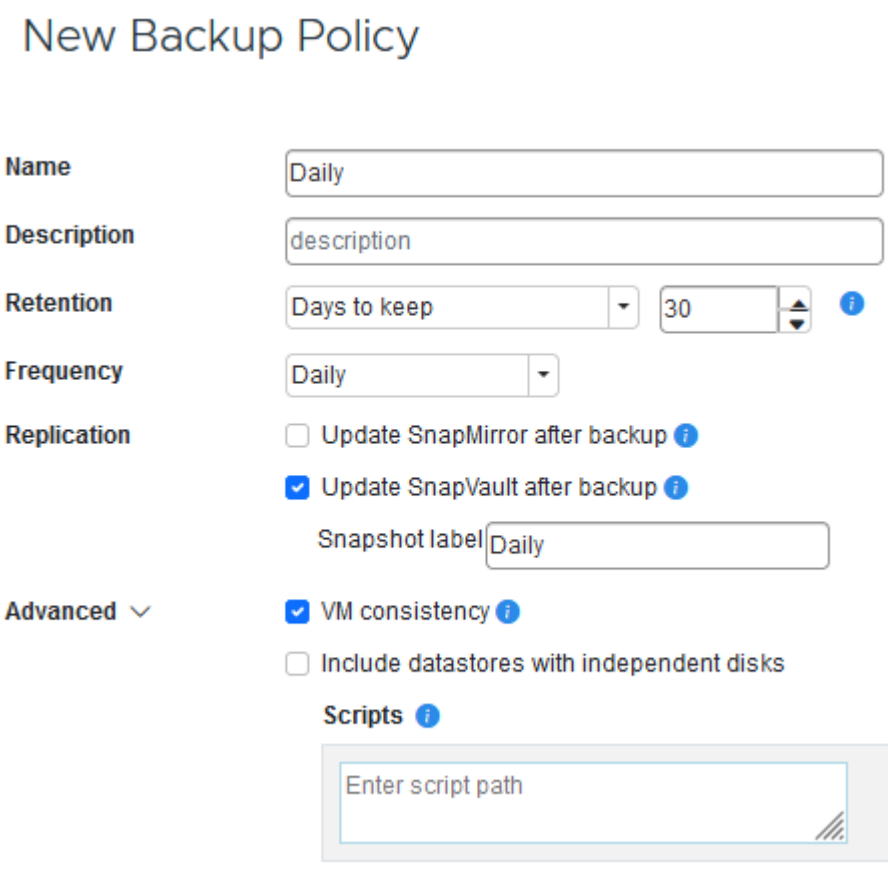
回顧 "為虛擬機器和資料儲存建立備份策略"請參閱文件部分以取得更多資訊。

若要建立備份策略，請完成以下步驟：

1. 在SnapCenter Plug-in for VMware vSphere中，導覽至左側選單中的“策略”，然後按一下“建立”按鈕。



2. 指定策略的名稱、保留期、頻率和複製選項以及快照標籤。



在SnapCenter插件中建立策略時，您將看到SnapMirror和SnapVault的選項。如果您選擇SnapMirror，則政策中指定的保留計畫對於主快照和輔助快照將相同。如果您選擇SnapVault，則輔助快照的保留計畫將基於使用SnapMirror關係實施的單獨計畫。當您希望延長二次備份的保留期時，這很有用。

Snapshot 快照技術標籤非常有用，因為它們可用於對複寫至次要 ONTAP 叢集的 SnapVault 複本，實施具有特定保留期間的原則。當 SCV 與 NetApp Data Services 搭配

使用時，Snapshot 快照技術標籤欄位必須為空白，或與備份原則中指定的標籤 相符。

3. 對每個所需的策略重複此過程。例如，針對每日、每周和每月備份制定單獨的策略。

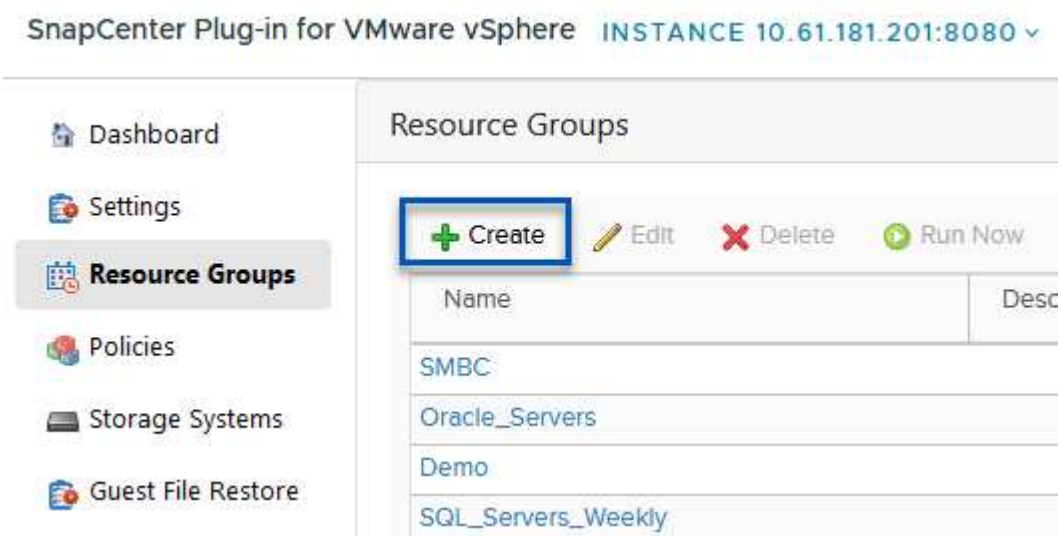
▼ 建立資源組

資源組包含要包含在備份作業中的資料儲存區和虛擬機，以及相關的策略和備份計畫。

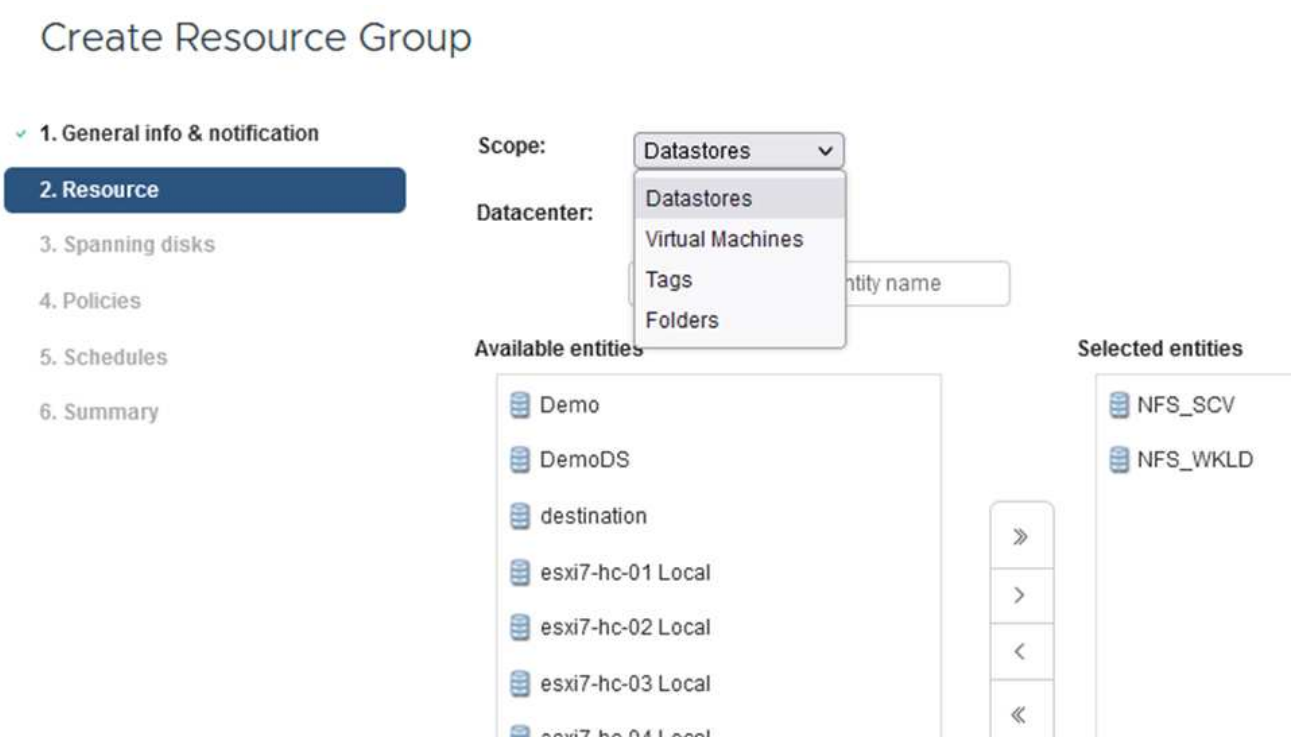
回顧 "建立資源組"請參閱文件部分以取得更多資訊。

若要建立資源組，請完成以下步驟。

1. 在SnapCenter Plug-in for VMware vSphere中，導覽至左側選單中的“資源組”，然後按一下“建立”按鈕。

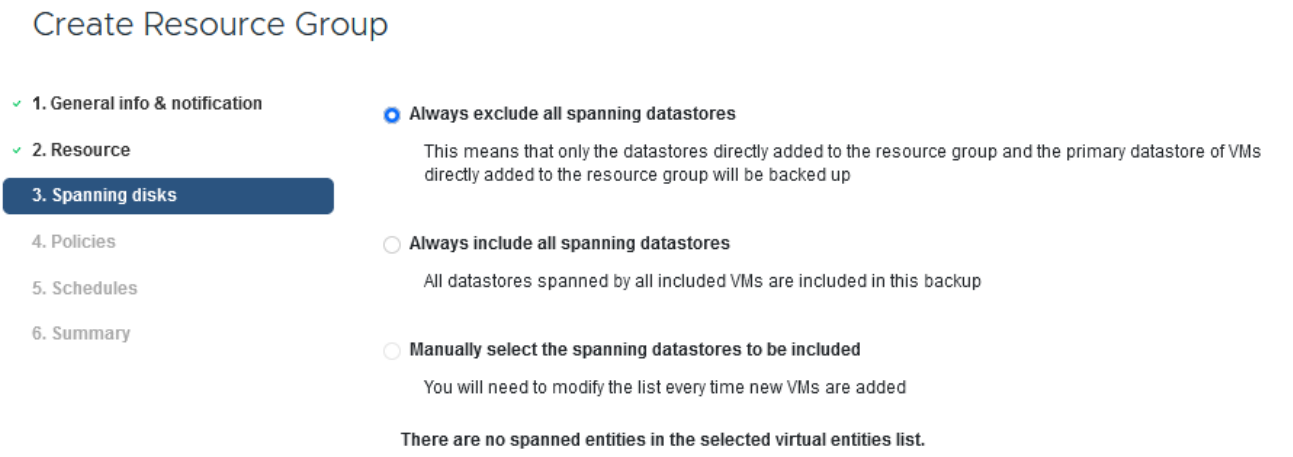


2. 在建立資源群組精靈中，輸入群組的名稱和描述，以及接收通知所需的資訊。點擊“下一步”
3. 在下一頁上，選擇希望包含在備份作業中的資料儲存和虛擬機，然後按一下「下一步」。



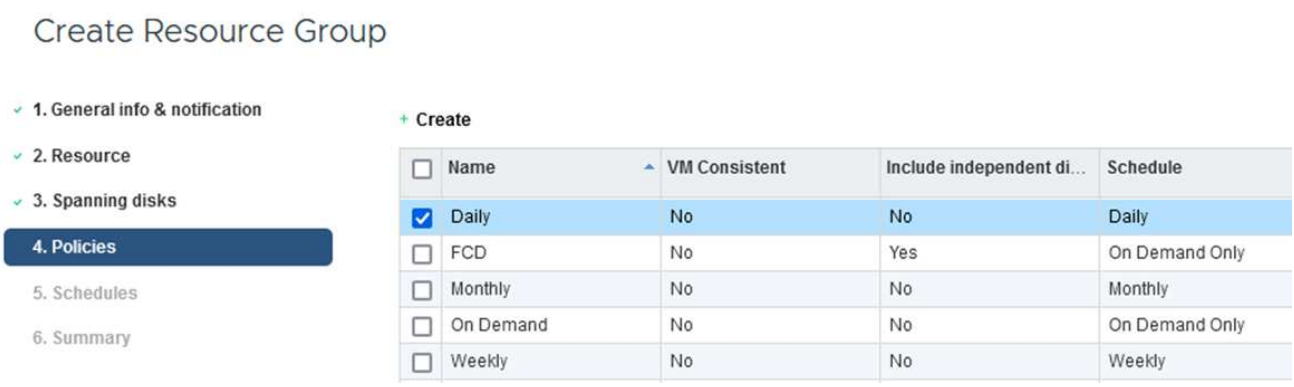
您可以選擇特定的虛擬機器或整個資料儲存。無論您選擇哪種方式，整個磁碟區（和資料儲存）都會備份，因為備份是拍攝底層磁碟區快照的結果。在大多數情況下，選擇整個資料儲存是最簡單的。但是，如果您希望在復原時限制可用虛擬機器的列表，則可以只選擇一部分虛擬機器進行備份。

4. 選擇跨位於多個資料儲存體上的 VMDK 的虛擬機器的資料儲存選項，然後按一下「下一步」。



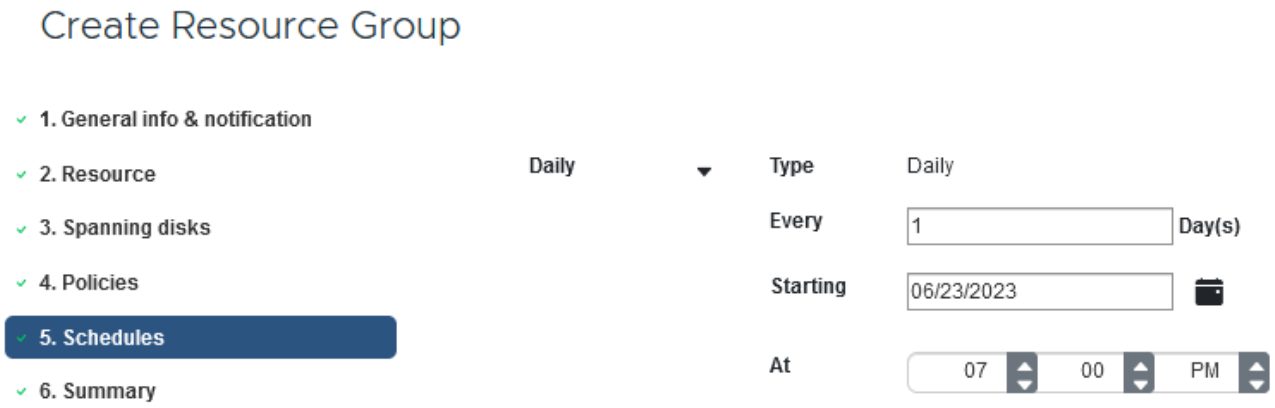
目前，用於保護 VMware 工作負載的備份與還原不支援備份具有跨越多個資料存放區之 VMDK 的虛擬機器。

5. 在下一頁上，選擇與資源群組關聯的策略，然後按一下「下一步」。



使用備份與還原將 SCV 代管的快照備份到物件儲存時，每個資源群組只能與單一原則關聯。

6. 選擇一個計劃來確定備份的運行時間。按一下“下一步”。

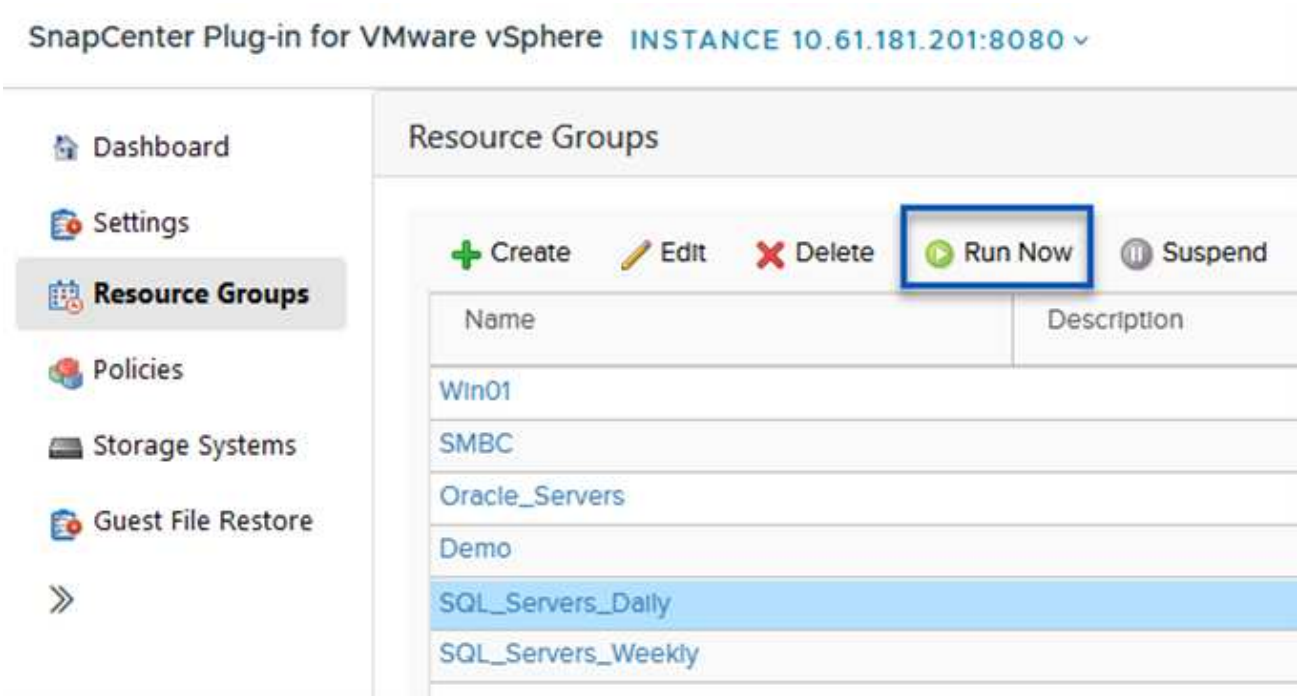


7. 最後，查看摘要頁面，然後按一下「完成」以完成資源組建立。

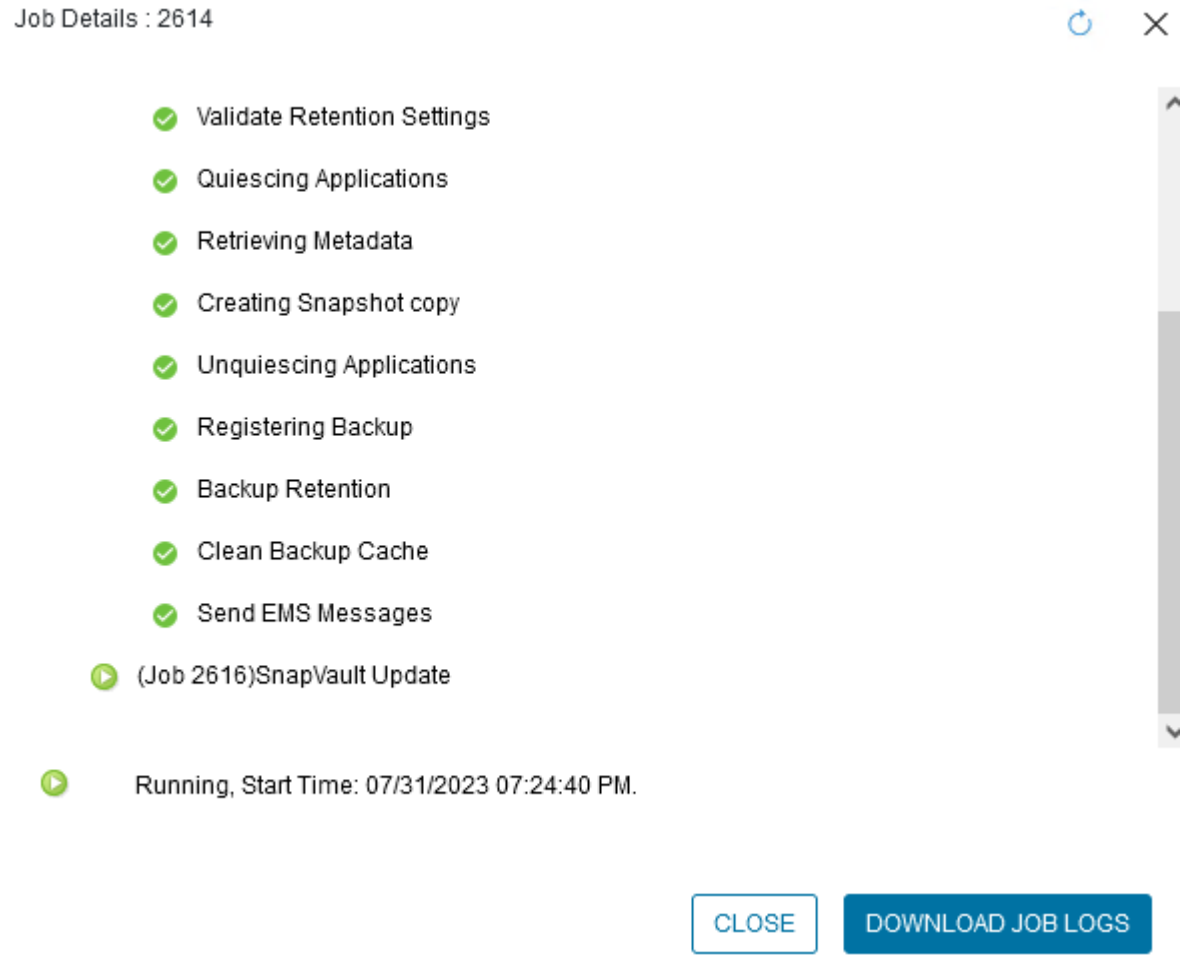
▼ 執行備份作業

最後一步，執行備份作業並監控其進度。至少必須在 SCV 中成功完成一個備份作業，才能從 NetApp Console 發現資源。

1. 在SnapCenter Plug-in for VMware vSphere中，導覽至左側選單中的「資源組」。
2. 若要啟動備份作業，請選擇所需的資源群組並按一下*立即執行*按鈕。



3. 若要監控備份作業，請導覽至左側選單上的「儀表板」。在「最近的工作活動」下點選工作 ID 號碼來監控工作進度。



為了讓 NetApp Console 有效地管理資料基礎架構，需要預先安裝 Console 代理程式。Console 代理程式會執行與探索資源和管理資料作業相關的動作。

如需有關 Console 代理程式的詳細資訊，請參閱 NetApp Console 文件中的 "了解 Console 代理程式"。

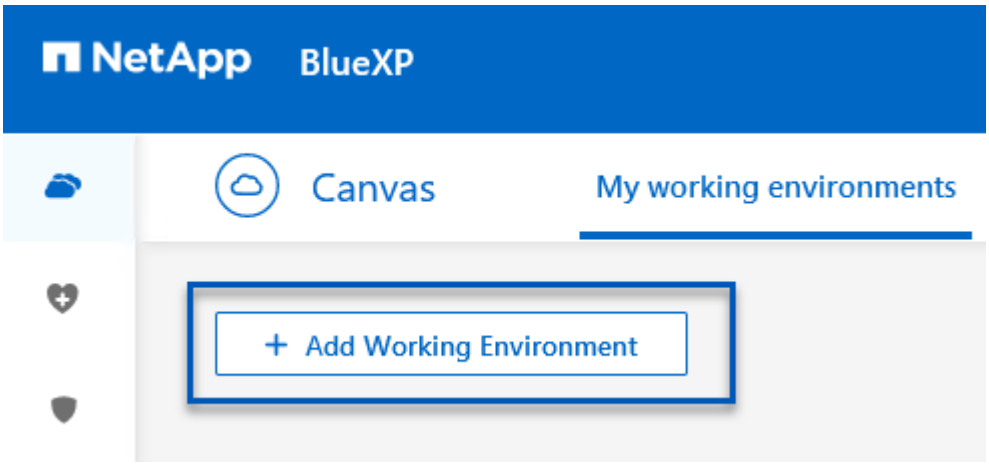
一旦為所使用的雲端供應商安裝了代理程式，即可從系統中查看物件儲存的圖形表示。

若要設定備份與還原以備份 SCV 在內部部署代管的資料，請完成下列步驟：

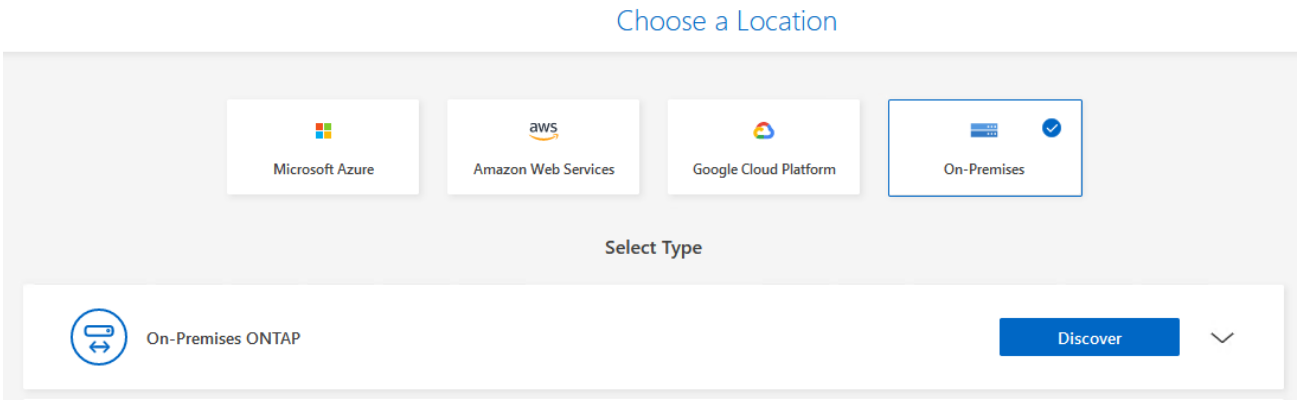
▼ 將 **ONTAP** 儲存系統新增至系統

第一步是將內部部署的 ONTAP 儲存系統新增至 NetApp Console。

1. 從「系統」中，按一下 **+** 新增 以開始。



2. 從位置選擇中選擇*On-Premises*，然後按一下*Discover*按鈕。



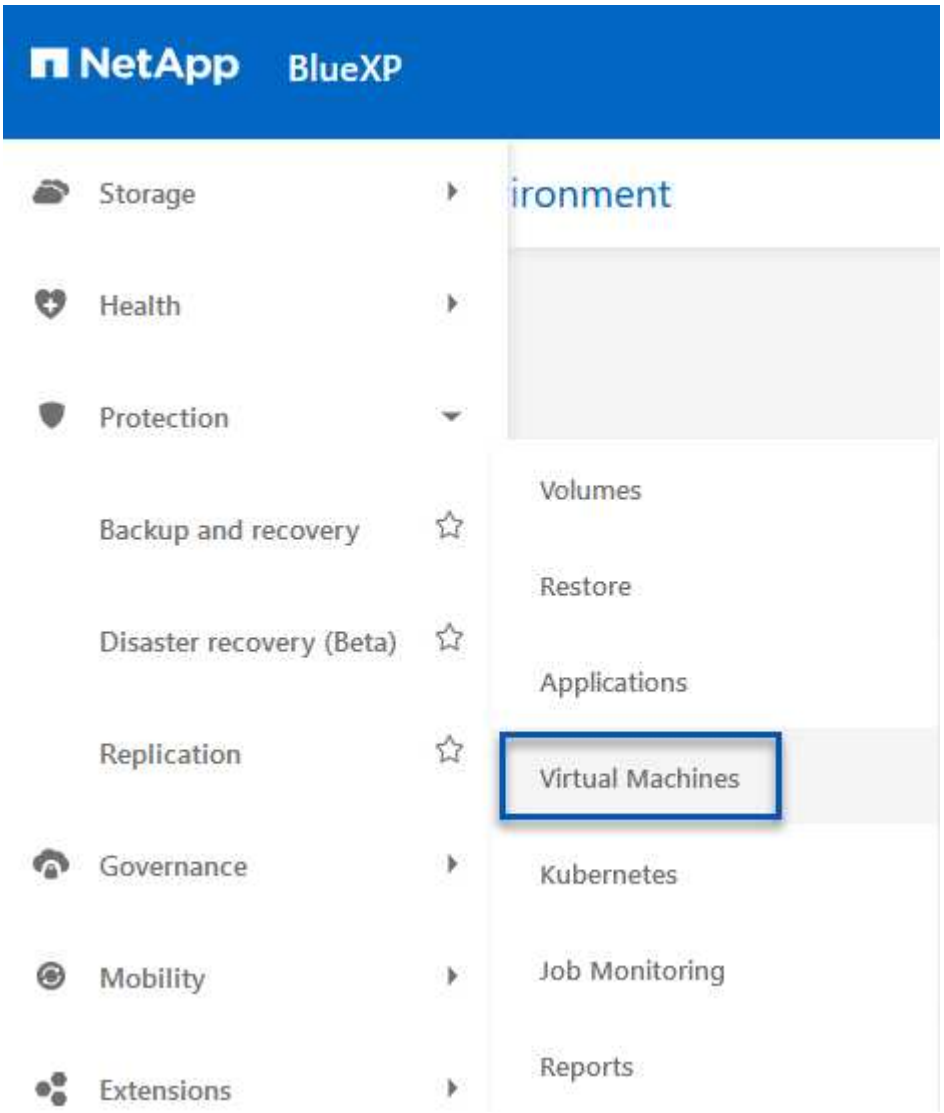
3. 填寫ONTAP儲存系統的憑證，然後點選 發現 按鈕新增工作環境。



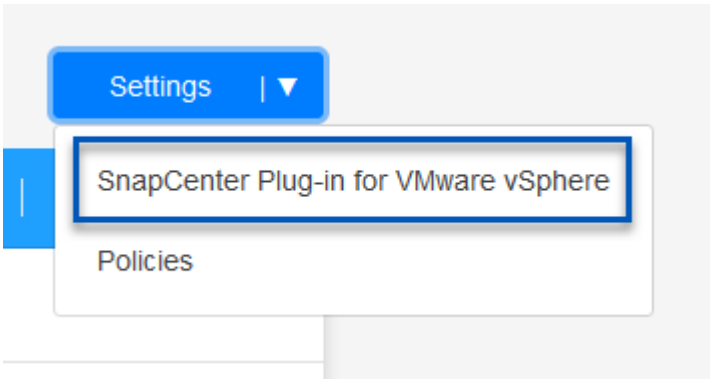
▼ 發現本地 **SCV** 設備和 **vCenter**

若要發現本機資料儲存和虛擬機器資源，請新增 SCV 資料代理程式的資訊和 vCenter 管理設備的憑證。

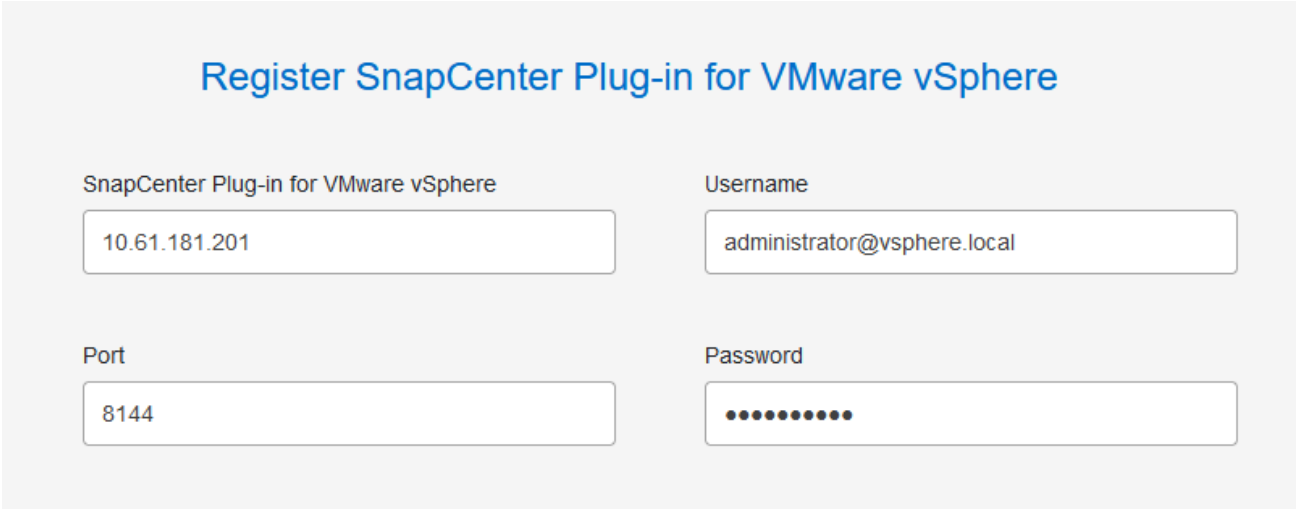
1. 從 NetApp Console 左側選單中選擇 保護 **>** 備份與還原 **>** 工作負載 **> VMware**



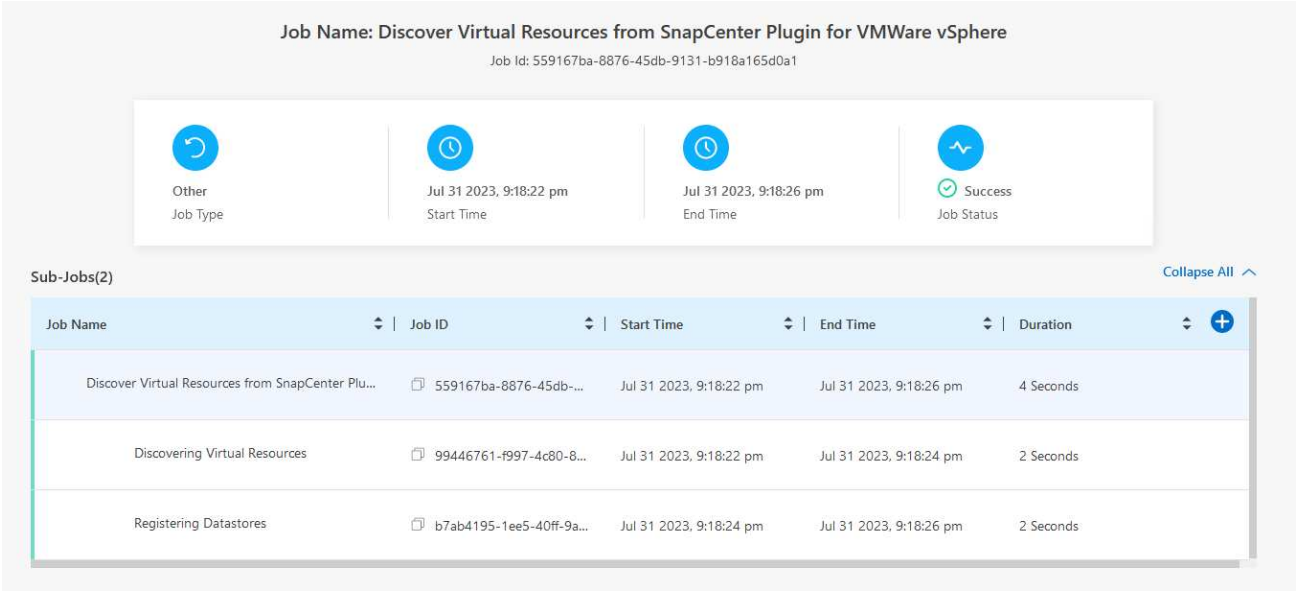
2. 從虛擬機器主畫面存取*設定*下拉選單並選擇*SnapCenter Plug-in for VMware vSphere*。



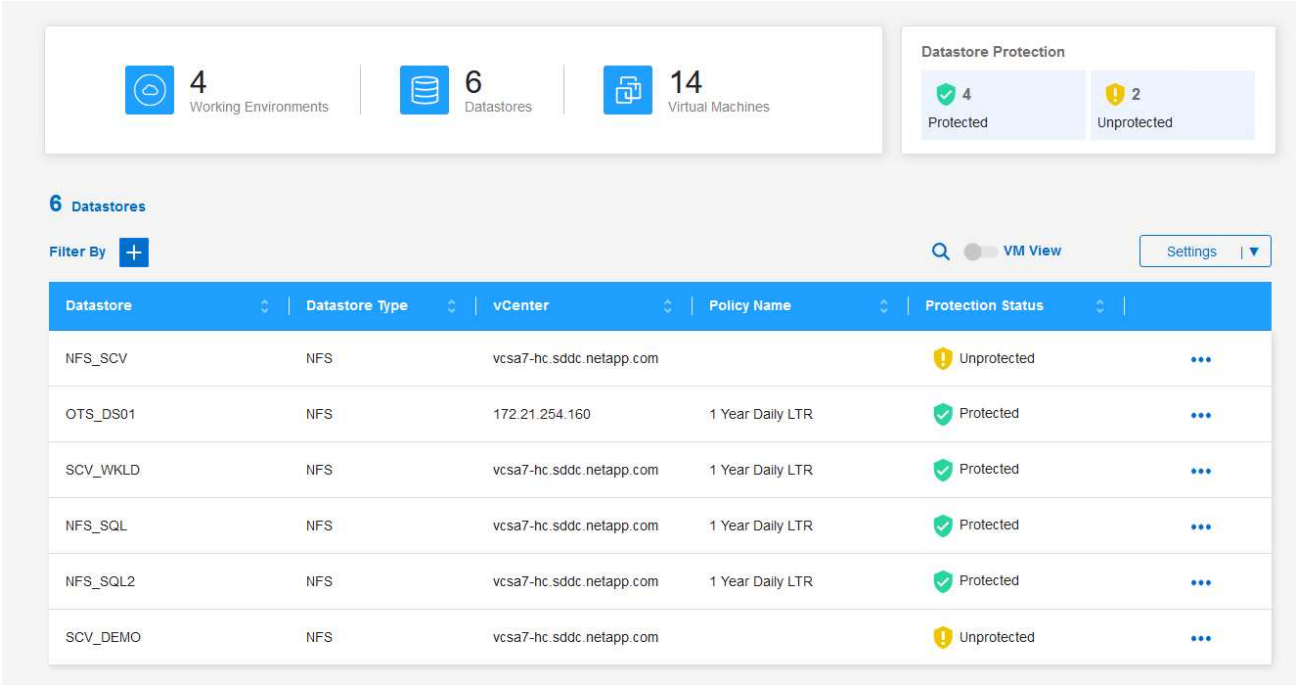
3. 點擊*註冊*按鈕，然後輸入SnapCenter插件設備的 IP 位址和連接埠號碼以及 vCenter 管理設備的使用者名稱和密碼。點擊“註冊”按鈕開始發現過程。



4. 您可以從「作業監控」標籤監控作業的進度。



5. 一旦發現完成，您將能夠查看所有已發現的 SCV 裝置上的資料儲存和虛擬機器。

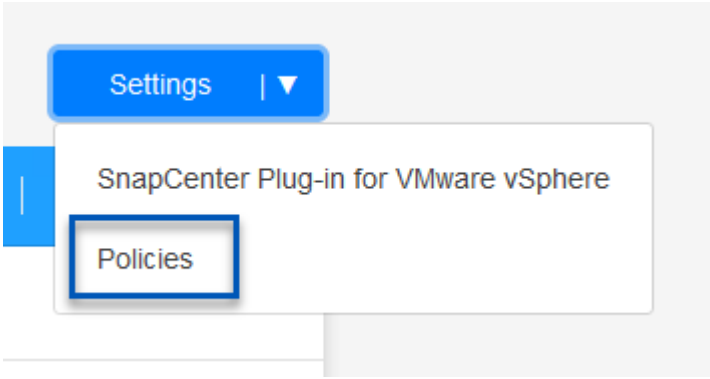


▼ 建立備份策略

在虛擬機器的 NetApp Backup and Recovery 中，建立原則以指定保留期間、備份來源和歸檔原則。

如需建立保護群組的詳細資訊，請參閱 "建立保護群組"。

1. 從適用於虛擬機器的 NetApp Backup and Recovery 主頁，存取 設定 下拉式選單，然後選擇 原則。



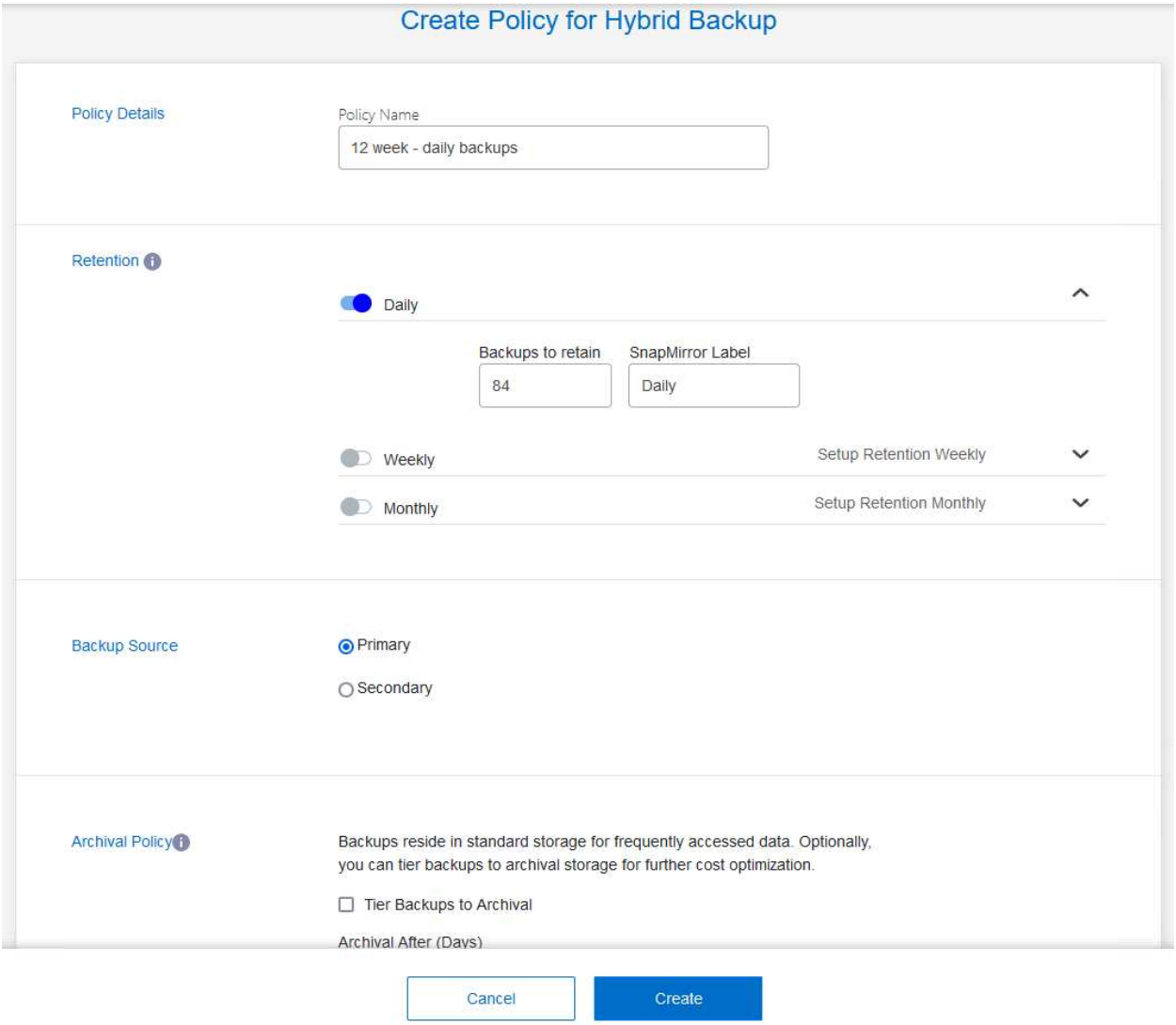
2. 按一下「建立策略」以存取「建立混合備份策略」視窗。

   a. 新增策略名稱

   b. 選擇所需的保留期限

   c. 選擇備份是否來自主或輔助本機ONTAP儲存系統

   d. 或者，指定在多長時間後將備份分層到檔案儲存以節省更多成本。



此處輸入的SnapMirror標籤用於識別要套用該策略的備份。標籤名稱必須與對應的本地 SCV 策略中的標籤名稱相符。

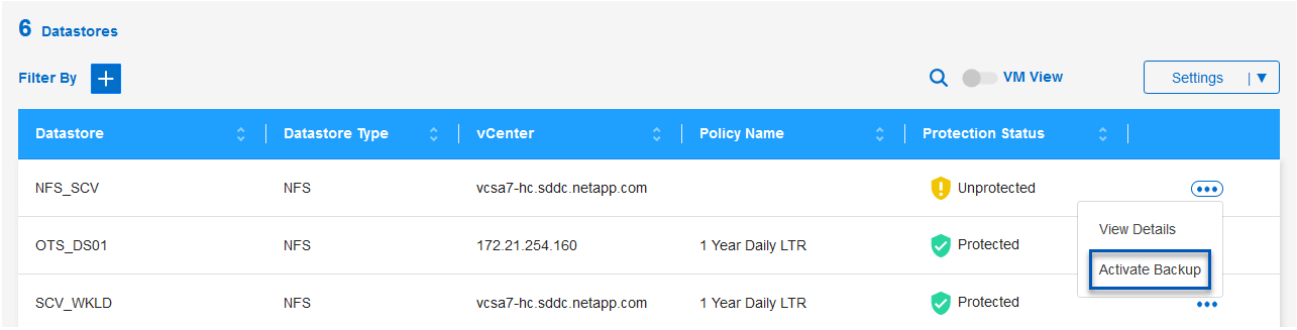
3. 按一下「建立」完成策略建立。

▼ 將資料儲存備份到 **Amazon Web Services**

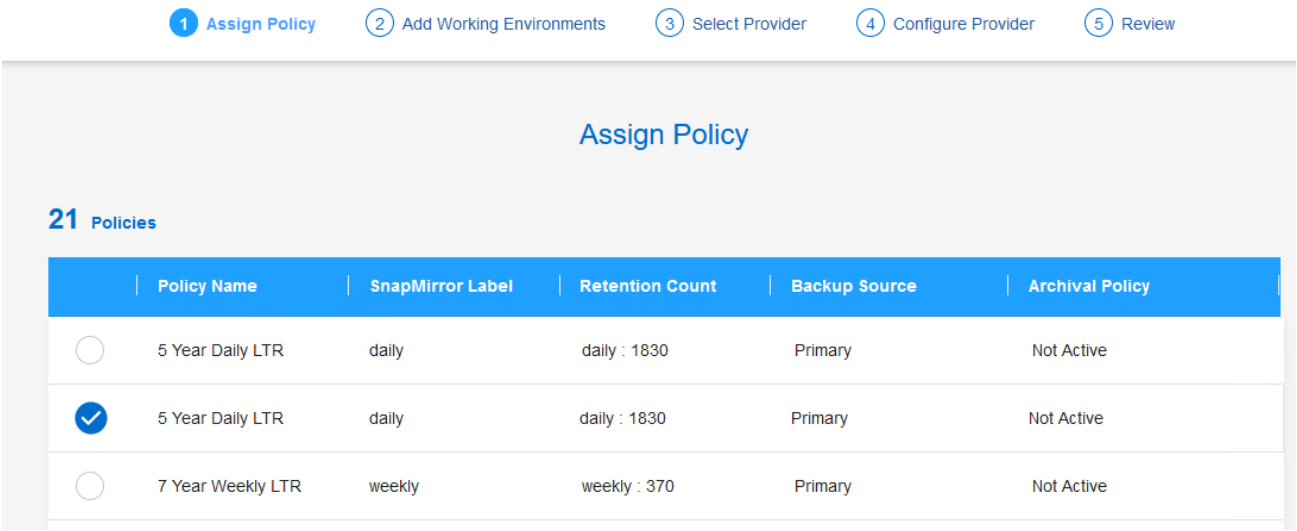
最後一步是啟動各個資料儲存區和虛擬機器的資料保護。以下步驟概述如何啟動 AWS 備份。

更多資訊請參閱 "備份 VMware 工作負載"。

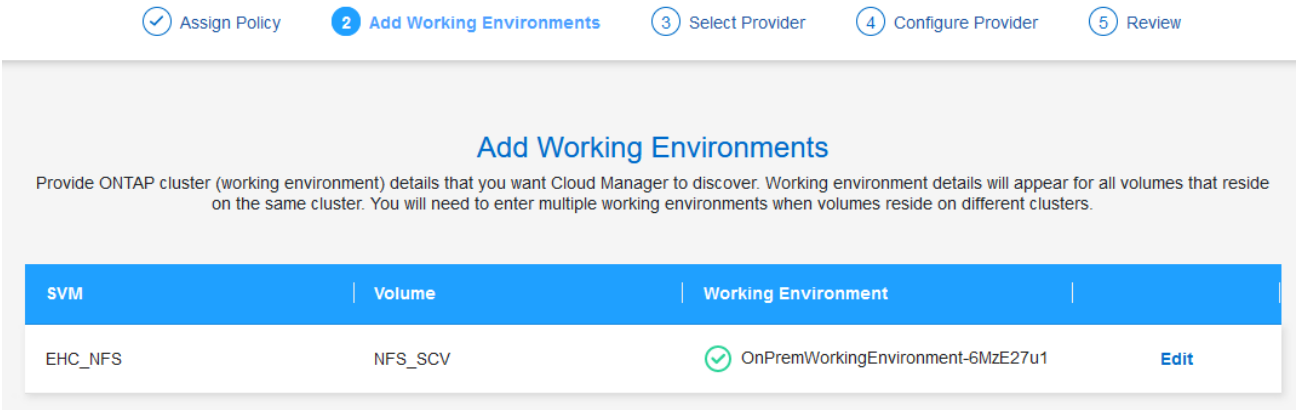
1. 從 NetApp Backup and Recovery for Virtual Machines 主頁，存取要備份的資料存放區的設定下拉式選單，然後選取 啟動備份。



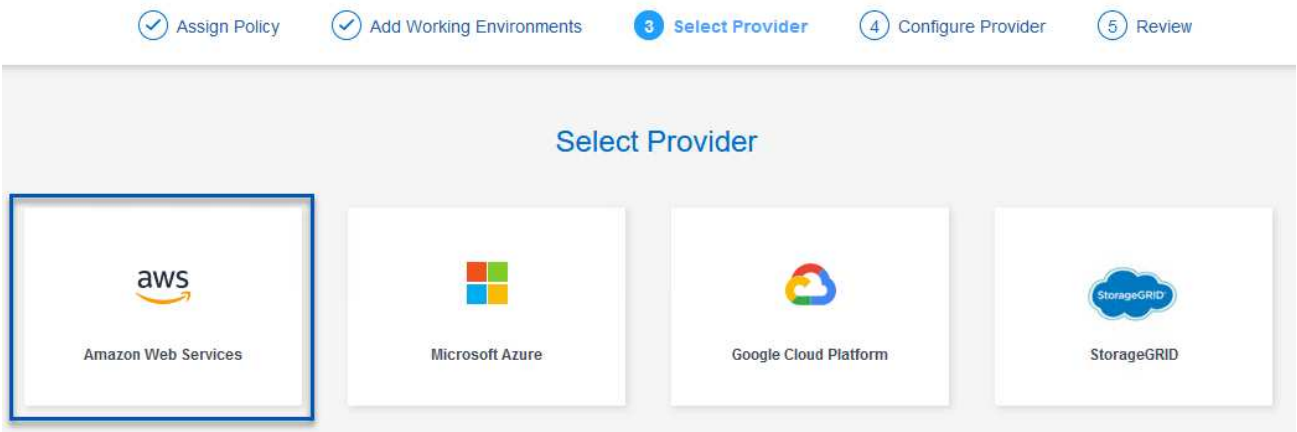
2. 指派用於資料保護操作的策略，然後按一下「下一步」。



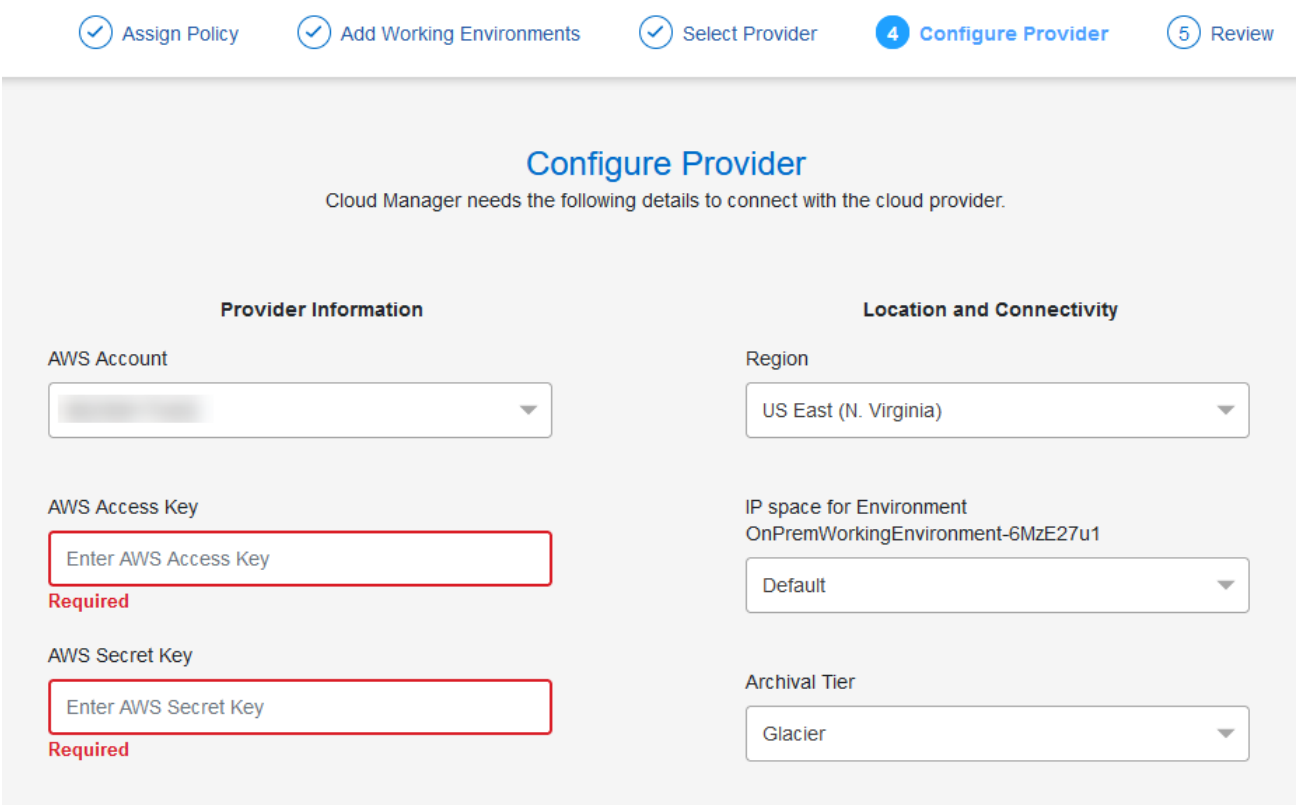
3. 如果之前已經發現了工作環境，則在「新增工作環境」頁面上應該會出現帶有複選標記的資料儲存和工作環境。如果之前沒有發現工作環境，您可以在這裡添加它。按一下"下一步"繼續。



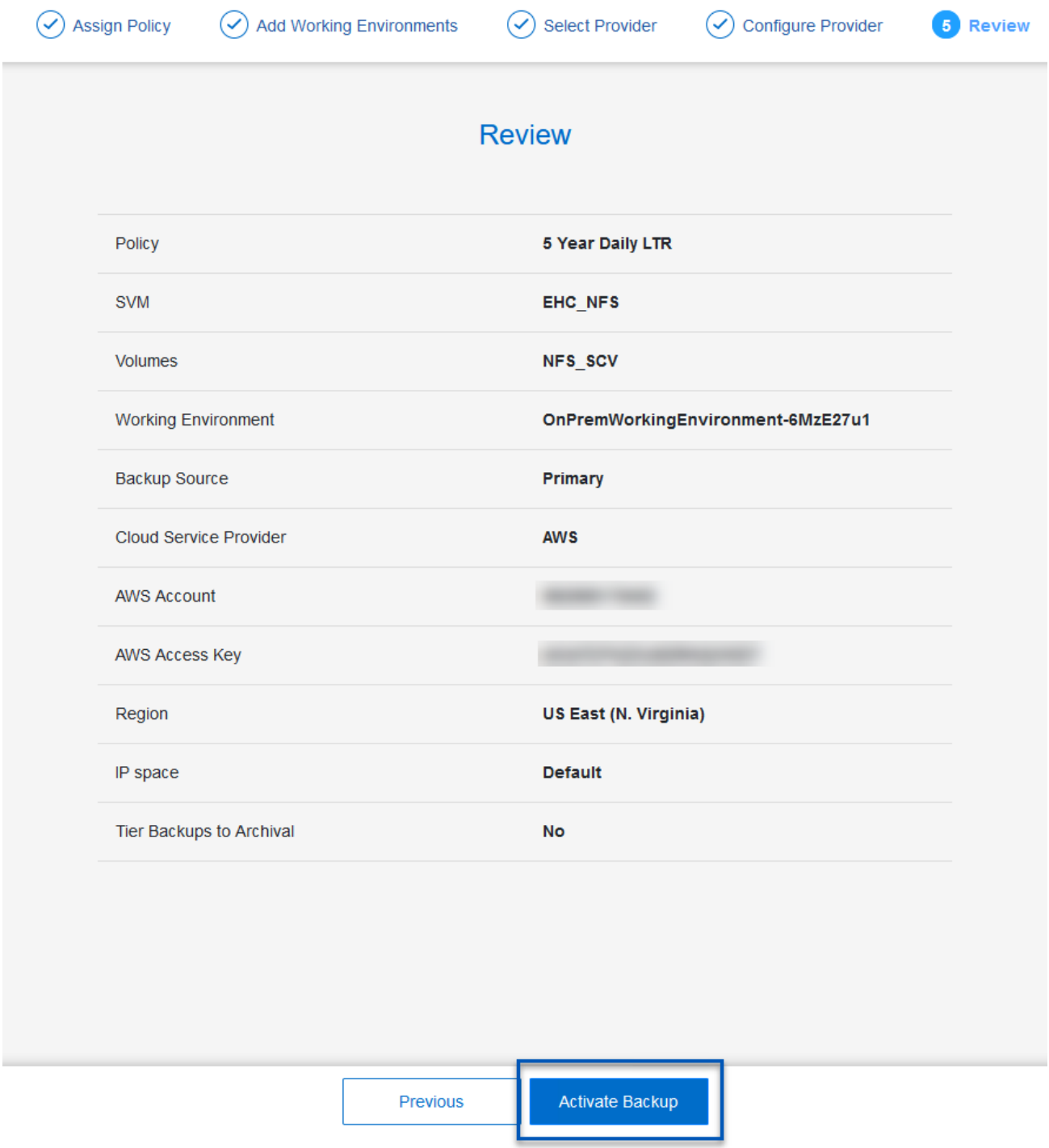
4. 在*選擇提供者*頁面上按一下 AWS，然後按一下*下一步*按鈕繼續。



5. 填寫 AWS 提供者特定的憑證訊息，包括要使用的 AWS 存取金鑰和金鑰、區域和存檔層。此外，也要為本機ONTAP儲存系統選擇ONTAP IP 空間。按一下“下一步”。



6. 最後，查看備份作業詳細信息，然後按一下「啟動備份」按鈕以啟動資料儲存的資料保護。



此時資料傳輸可能不會立即開始。NetApp Backup and Recovery 每小時掃描一次任何未完成的 Snapshot 複本，然後將其傳輸至物件儲存。

資料遺失時恢復虛擬機

確保資料的安全只是全面資料保護的一個面向。同樣重要的是，在發生資料遺失或勒索軟體攻擊時能夠從任何位置迅速恢復資料。此功能對於維持無縫業務營運和滿足復原點目標至關重要。

NetApp提供高度適應性的 3-2-1 策略，可對主儲存、輔助儲存和物件儲存位置的保留計畫進行客製化控制。該策略提供了靈活性，可以根據特定需求自訂資料保護方法。

本節提供從 SnapCenter Plug-in for VMware vSphere 和虛擬機器的 NetApp Backup and Recovery 還原資料程序的總覽。

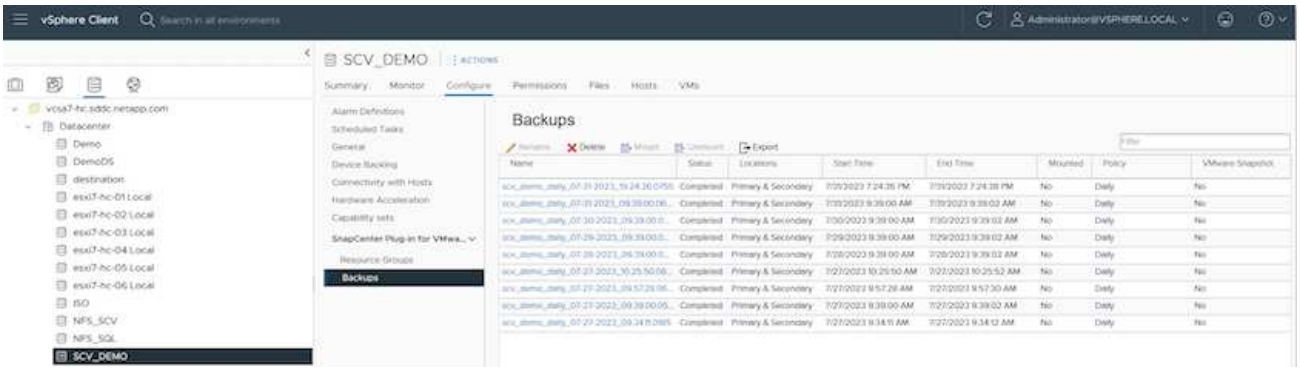
從**SnapCenter Plug-in for VMware vSphere**還原虛擬機

對於此解決方案，虛擬機器被恢復到原始位置和備用位置。該解決方案並未涵蓋 SCV 資料復原功能的所有面向。有關 SCV 提供的所有服務的詳細信息，請參閱 "從備份還原虛擬機"在產品文件中。

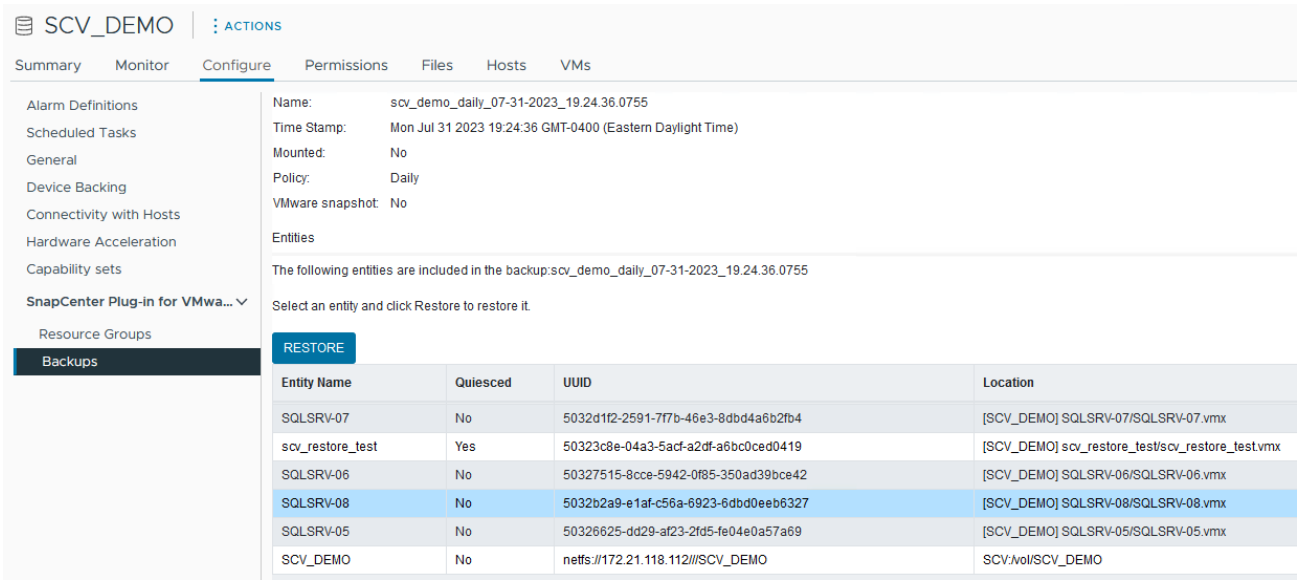
▼ 從 **SCV** 還原虛擬機

完成以下步驟以從主儲存或輔助儲存還原虛擬機器。

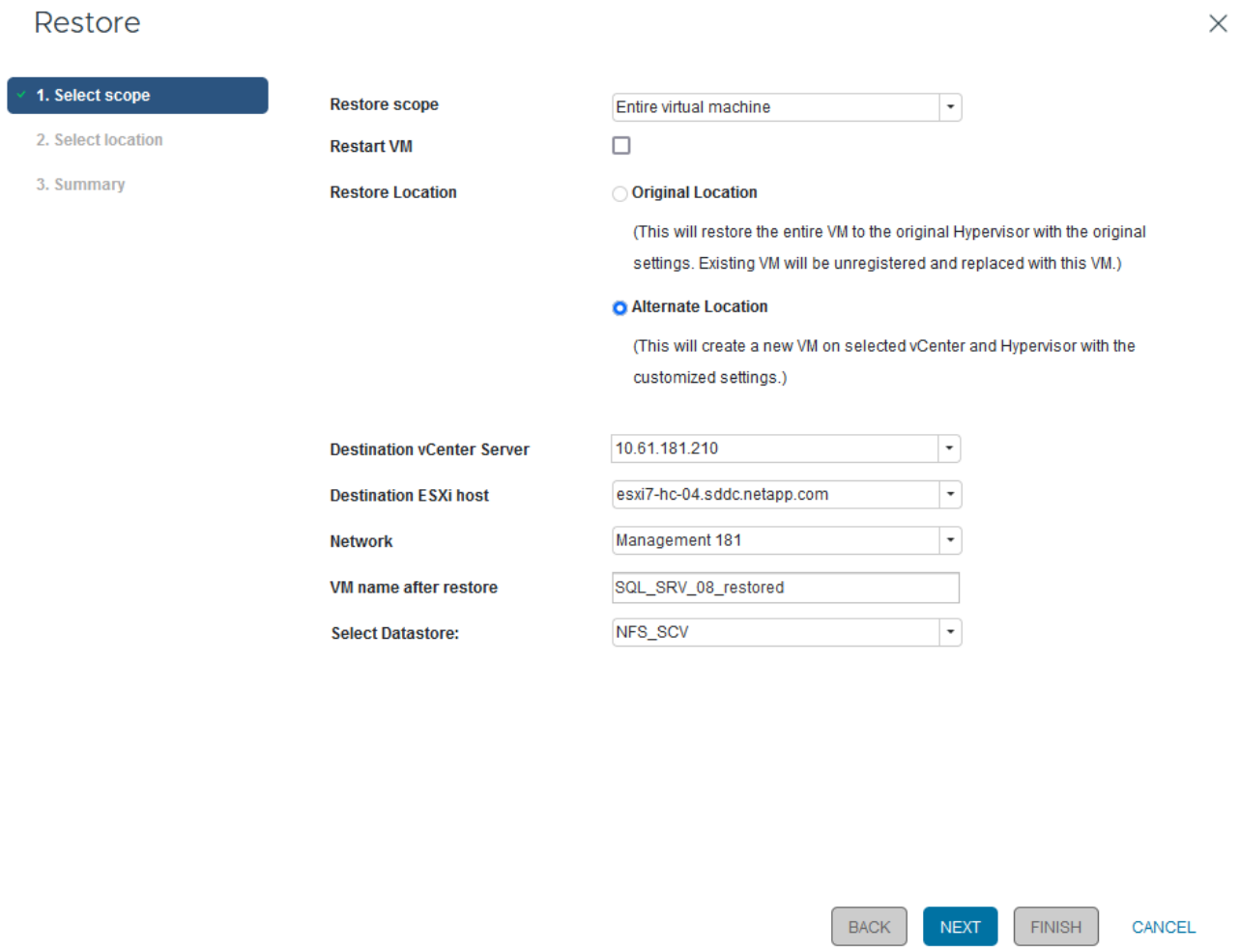
1. 從 vCenter 用戶端導覽至 **Inventory > Storage**，然後按一下包含要還原的虛擬機器的資料儲存體。
2. 從「配置」標籤按一下「備份」以存取可用備份清單。



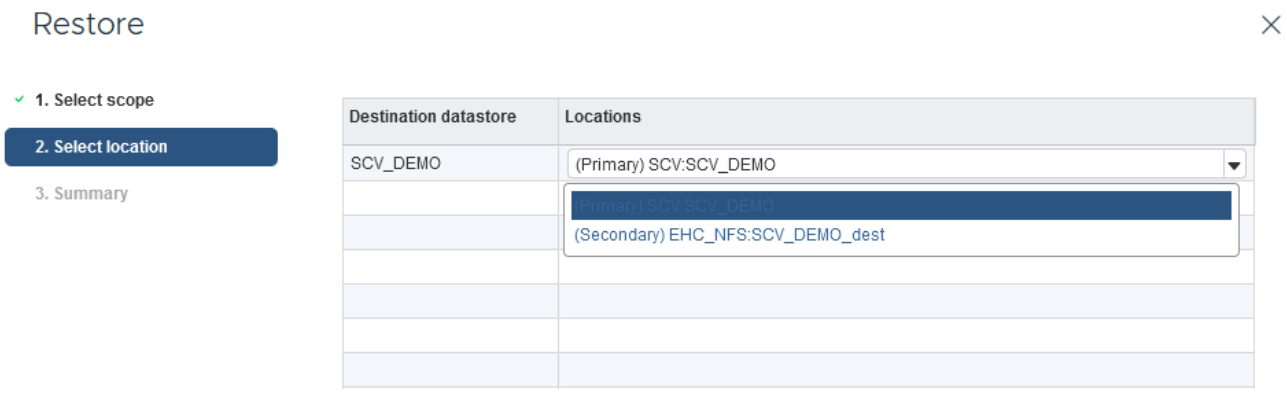
3. 按一下備份以存取虛擬機器列表，然後選擇要恢復的虛擬機器。點選*恢復*。



4. 從還原精靈中選擇還原整個虛擬機器或特定的 VMDK。選擇安裝到原始位置或備用位置，提供復原後的虛擬機器名稱和目標資料儲存。按一下“下一步”。



5. 選擇從主儲存位置或輔助儲存位置備份。



6. 最後，查看備份作業的摘要並按一下「完成」以開始復原程序。

從適用於虛擬機器的 **NetApp Backup and Recovery** 還原虛擬機器

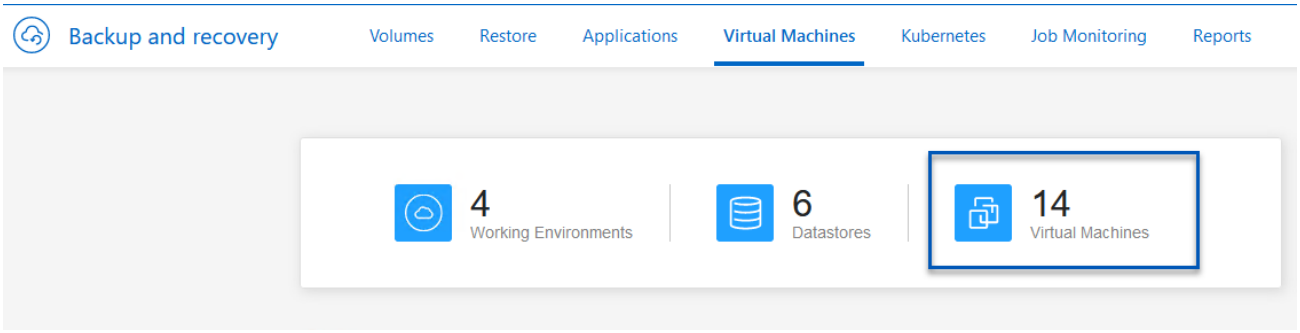
適用於虛擬機器的 NetApp Backup and Recovery 可將虛擬機器還原至其原始位置。還原功能可透過 NetApp Backup and Recovery 網頁主控台進行存取。

更多資訊請參閱 "從雲端恢復虛擬機器數據"。

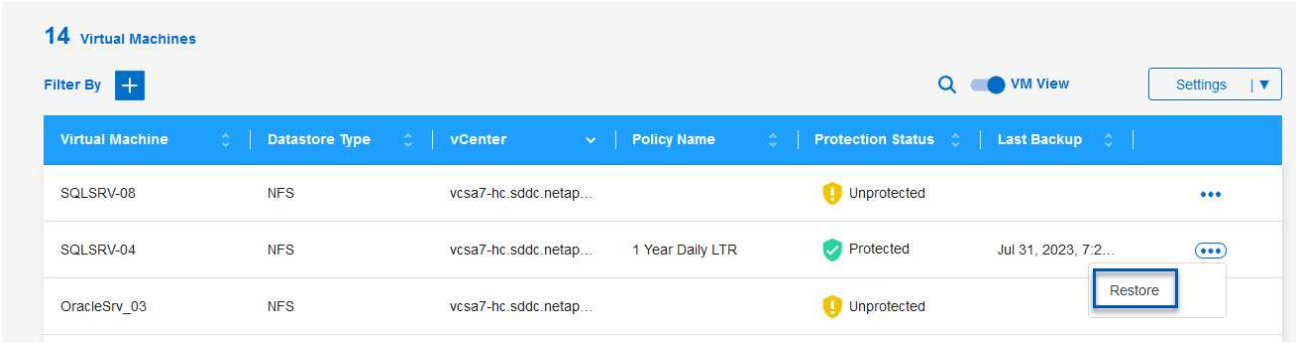
▼ 從 **NetApp Backup and Recovery** 還原虛擬機器

若要從 NetApp Backup and Recovery 還原虛擬機器，請完成下列步驟。

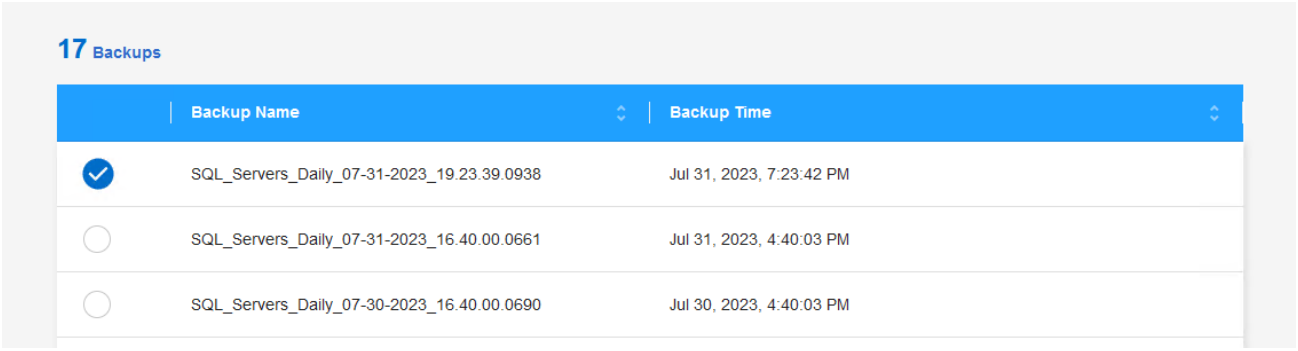
1. 導航至*保護>備份和還原>虛擬機器*，然後按一下虛擬機器以查看可還原的虛擬機器清單。



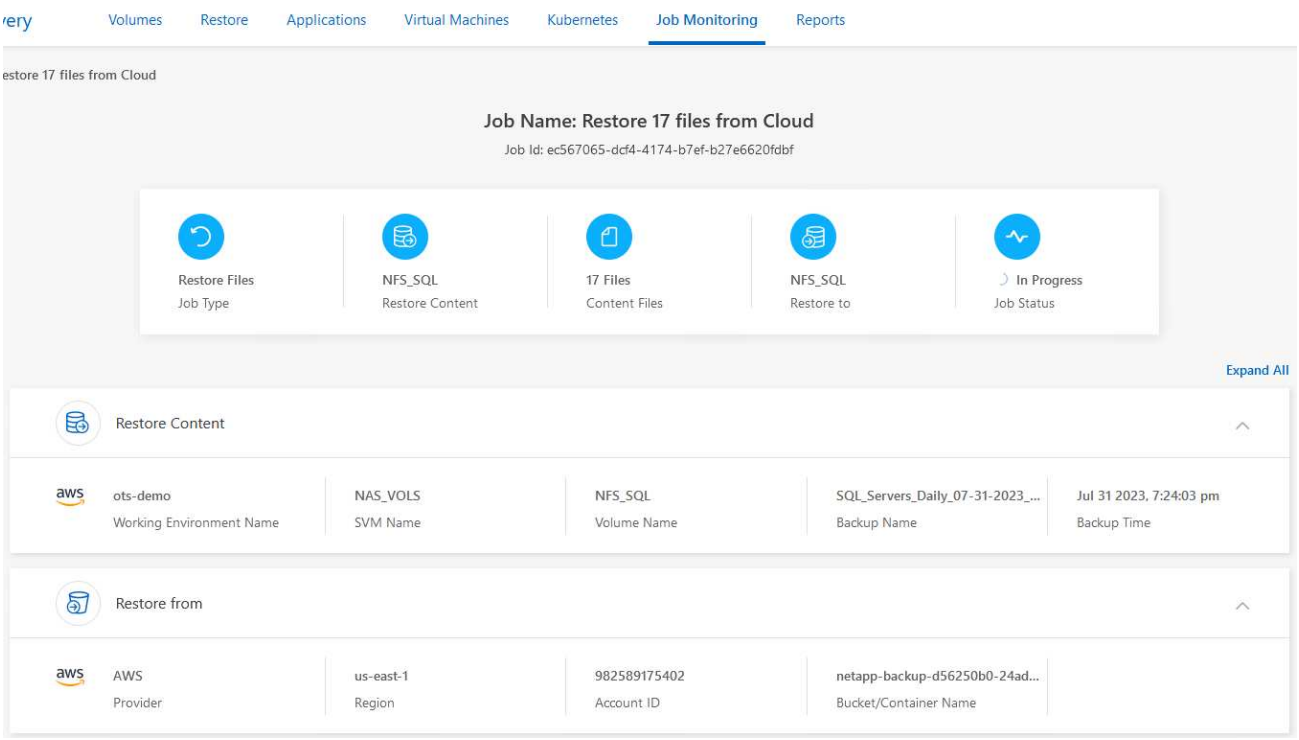
2. 存取要復原的虛擬機器的設定下拉式選單並選擇



3. 選擇要還原的備份，然後按一下「下一步」。



4. 查看備份作業的摘要，然後按一下「復原」開始復原程序。
5. 從「作業監控」標籤監控恢復作業的進度。



結論

當 3-2-1 備份策略與 SnapCenter Plug-in for VMware vSphere 和適用於虛擬機器的 NetApp Backup and Recovery 搭配實作時，可為資料保護提供強大、可靠且具成本效益的解決方案。此策略不僅確保資料備援和存取能力，還提供從任何位置，以及從內部部署 ONTAP 儲存系統和雲端物件儲存還原資料的靈活度。

本文件介紹的使用案例重點在於獲證實的資料保護技術，這些技術重點摘要了 NetApp、VMware 與領先業界的雲端供應商之間的整合。SnapCenter Plug-in for VMware vSphere 可與 VMware vSphere 無縫整合，進而實現高效且集中的資料保護作業管理。此整合簡化了虛擬機器的備份與還原流程，能夠在 VMware 生態系統內輕鬆進行排程、監控和靈活的還原作業。針對虛擬機器的 NetApp Backup and Recovery 透過將虛擬機器資料安全、實體隔離地備份到雲端物件儲存，提供了 3-2-1 中的一 (1)。直覺式的介面和邏輯清晰的工作流程為關鍵資料的長期歸檔提供了一個安全的平台。

附加資訊

要了解有關此解決方案中提出的技術的更多信息，請參閱以下附加資訊。

- "SnapCenter Plug-in for VMware vSphere文檔"
- "NetApp Console 文件"

NetApp Disaster Recovery

概況

災難恢復是每位 VMware 系統管理員最為關注的問題。由於 VMware 將整個伺服器封裝成一系列構成虛擬機器的檔案，系統管理員會利用複製、快照和複本等區塊儲存設備技術來保護這些虛擬機器。ONTAP 陣列提供內建複寫，可將 Volume 資料（以及駐留在指定資料儲存區 LUN 上的虛擬機器）從一個站台傳輸到另一個站台。NetApp Disaster Recovery 整合 vSphere 並自動化整個工作流程，以便在發生災難時實現無縫容錯移轉與容錯回復。透

過將儲存設備複寫與至能自動化相結合，系統管理員現在不僅能夠以可管理的方式設定、自動化和測試災難恢復計畫，而且還能夠在災難發生時輕鬆執行這些計畫。

VMware vSphere 環境中 DR 故障轉移最耗時的部分是在 DR 站點執行清點、註冊、重新配置和啟動虛擬機器所需的步驟。理想的解決方案既具有低 RPO（以分鐘為單位），又具有低 RTO（以分鐘到小時為單位）。 DR 解決方案中經常被忽略的一個因素是定期有效地測試 DR 解決方案的能力。

要建立 DR 解決方案，請牢記以下因素：

- 恢復時間目標 (RTO)。 RTO 是指企業從災難中復原的速度，或者更具體地說，是執行復原過程以使業務服務再次可用所需的時間。
- 恢復點目標 (RPO)。 RPO 是指復原的資料相對於災難發生的時間而言，可供使用的時間。
- 可擴展性和適應性。此因素包括隨著需求的增加而逐步增加儲存資源的能力。

有關可用解決方案的更多技術信息，請參閱：

- "適用於 NFS 資料存放區的 NetApp Disaster Recovery"
- "適用於 VMFS 資料儲存的 NetApp Disaster Recovery"

適用於 **NFS** 資料存放區的 **NetApp Disaster Recovery**

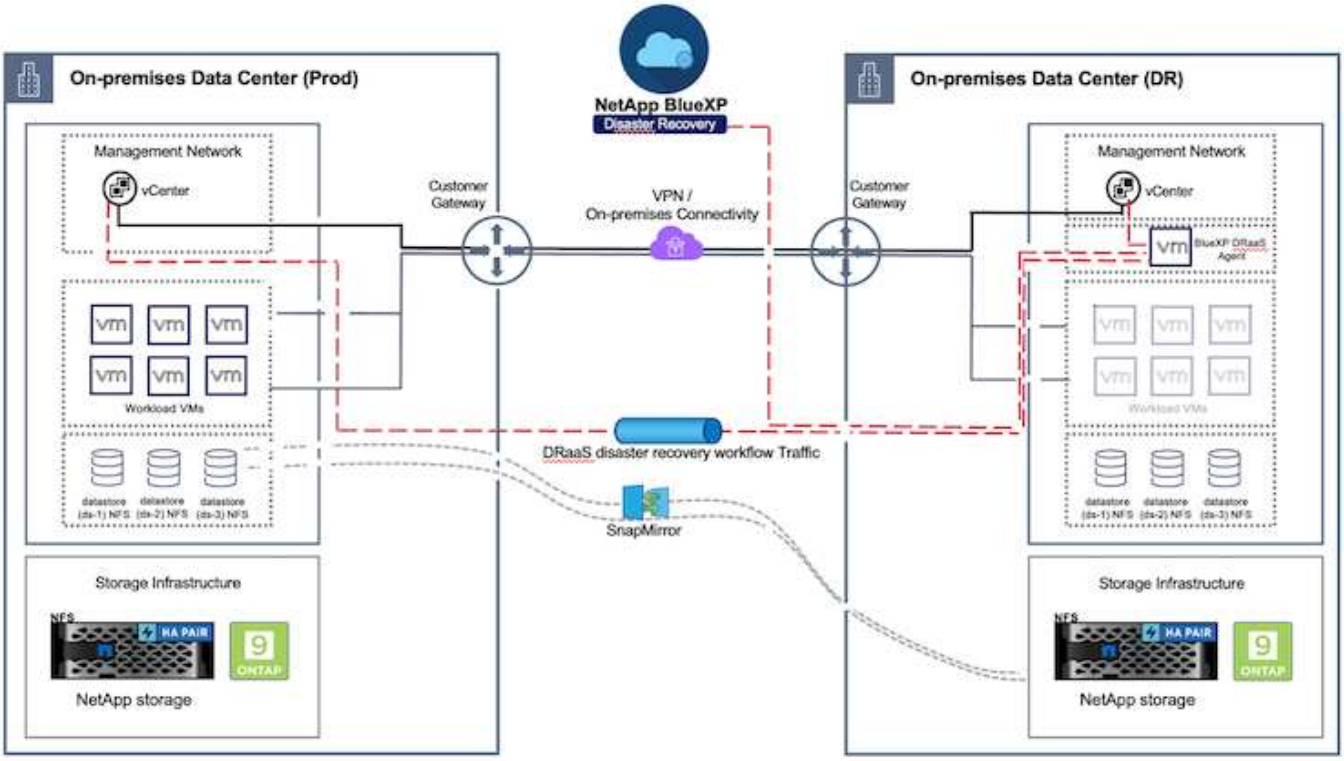
適用於 **NFS** 資料存放區的 **NetApp Disaster Recovery**

透過從生產站點到災難復原站點的區塊級複製來實現災難復原是一種具有彈性且經濟高效的方法，可保護工作負載免受網站中斷和資料損壞事件（例如勒索軟體攻擊）的影響。使用NetApp SnapMirror複製，在具有 NFS 資料儲存的本機ONTAP系統上執行的 VMware 工作負載可以複製到位於指定復原資料中心的另一個ONTAP儲存系統，該資料中心也部署了 VMware。

本文件的這一節說明 NetApp Disaster Recovery 的組態，以便為內部部署 VMware VM 設定至另一個指定站台的災難恢復。作為此設定的一部分，包括 Console 代理程式、將 ONTAP 陣列上線、定義站台以及關聯 VMware vCenter。此外，本文件詳細說明如何設定站台之間的複寫，以及如何設定與測試恢復計畫。最後一節提供執行完整站台容錯移轉的指示，以及在主要站台恢復並處於線上狀態時如何進行容錯回復。

利用 NetApp Data Services 中的災難恢復功能，企業可以輕鬆探索其內部部署的 VMware vCenters 和 ONTAP 儲存設備。然後，組織可以建立資源群組、建立災難恢復計畫、將其與資源群組建立關聯，並測試或執行容錯移轉與容錯回復。SnapMirror 提供儲存層級的區塊複寫，透過遞增變更讓兩個站台保持最新狀態，進而達成最多 5 分鐘的復原點目標（RPO）。此外，還可以模擬災難恢復程序，而不會影響正式作業或產生額外儲存容量成本。

災難恢復利用 ONTAP 的 FlexClone 技術，從災難恢復站台上最後一次複寫的 Snapshot 快照技術建立 NFS 資料儲存的極具空間效率複本。完成災難恢復測試後，客戶可以輕鬆刪除測試環境，而不會影響實際複寫的生產資源。如果發生實際容錯移轉，災難恢復會協調所有必要步驟，只需按幾下即可在指定的災難恢復站台上自動啟動受保護的虛擬機器。該服務也會在需要時反轉與主站台的 SnapMirror 關係，並將次要站台的任何變更複寫到主站台，以執行回復作業。與其他知名替代方案相比，所有這些功能的成本都低得多。

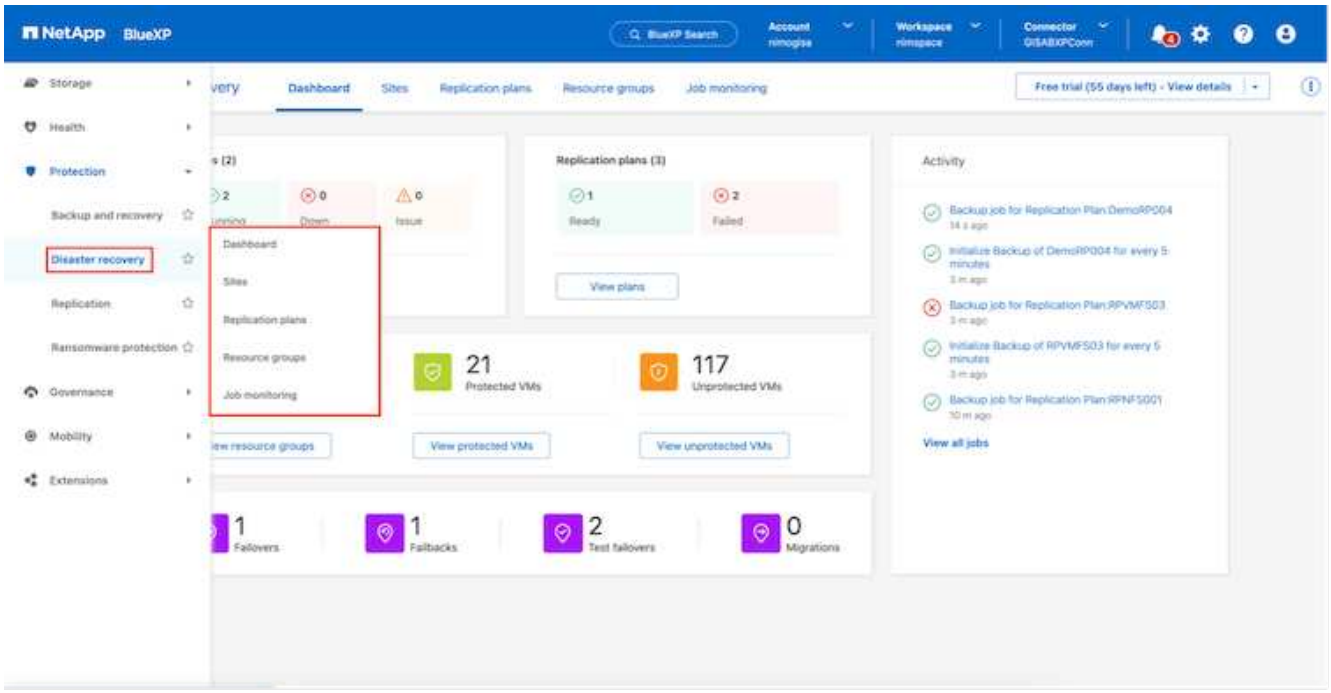


如需用於災難恢復的 vCenter Server、ESXi 和 ONTAP 的最新資訊與支援版本，請參閱 "災難恢復支援的組態"。

入門

若要開始使用 NetApp 災難恢復，請使用 NetApp 控制台，然後存取服務。

1. 登入控制台。
2. 從主控台左側導覽中，選擇 保護 > 災難恢復。
3. 災難恢復儀表板隨即顯示。

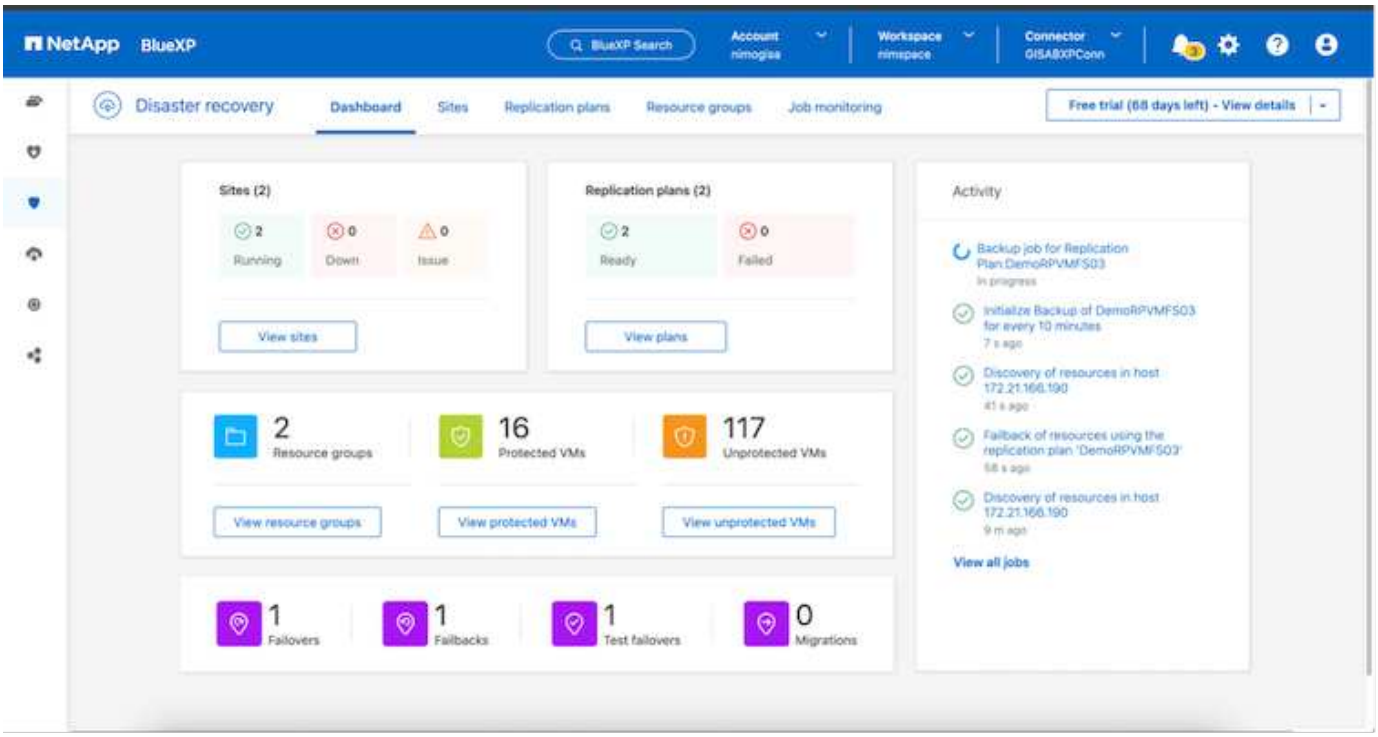


在設定災難恢復計畫之前，請確保滿足以下先決條件：

- 主控台代理程式已部署。
- 代理程式可連線至來源和目的地 vCenter 與儲存系統。
- 已啟用 NFS 服務的 ONTAP 叢集 SVM 可用。
- 託管 VMware NFS 資料存放區的內部部署 NetApp 儲存系統已在 Console 中新增。
- 使用 DNS 名稱時應該進行 DNS 解析。否則，請使用 vCenter 的 IP 位址。
- SnapMirror複製是為指定的基於 NFS 的資料儲存庫磁碟區配置的。
- 確保環境具有支援的 vCenter Server 和 ESXi 伺服器版本。

一旦來源站點和目標站點之間建立了連接，請繼續執行設定步驟，這需要幾次點擊和大約 3 到 5 分鐘的時間。

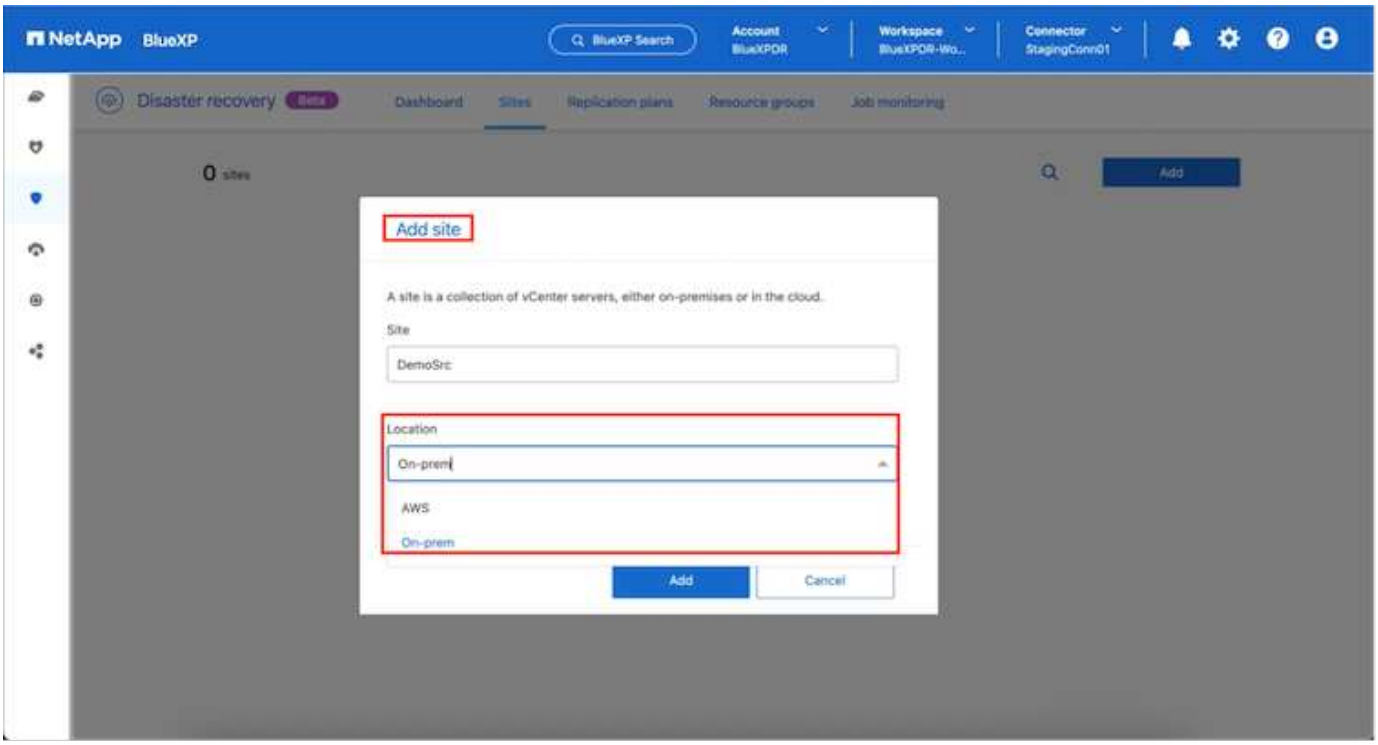
NetApp 建議將 Console 代理程式部署在目的地站台或第三個站台，以便 Console 代理程式可以透過網路與來源和目的地資源進行通訊。



NetApp 災難恢復組態

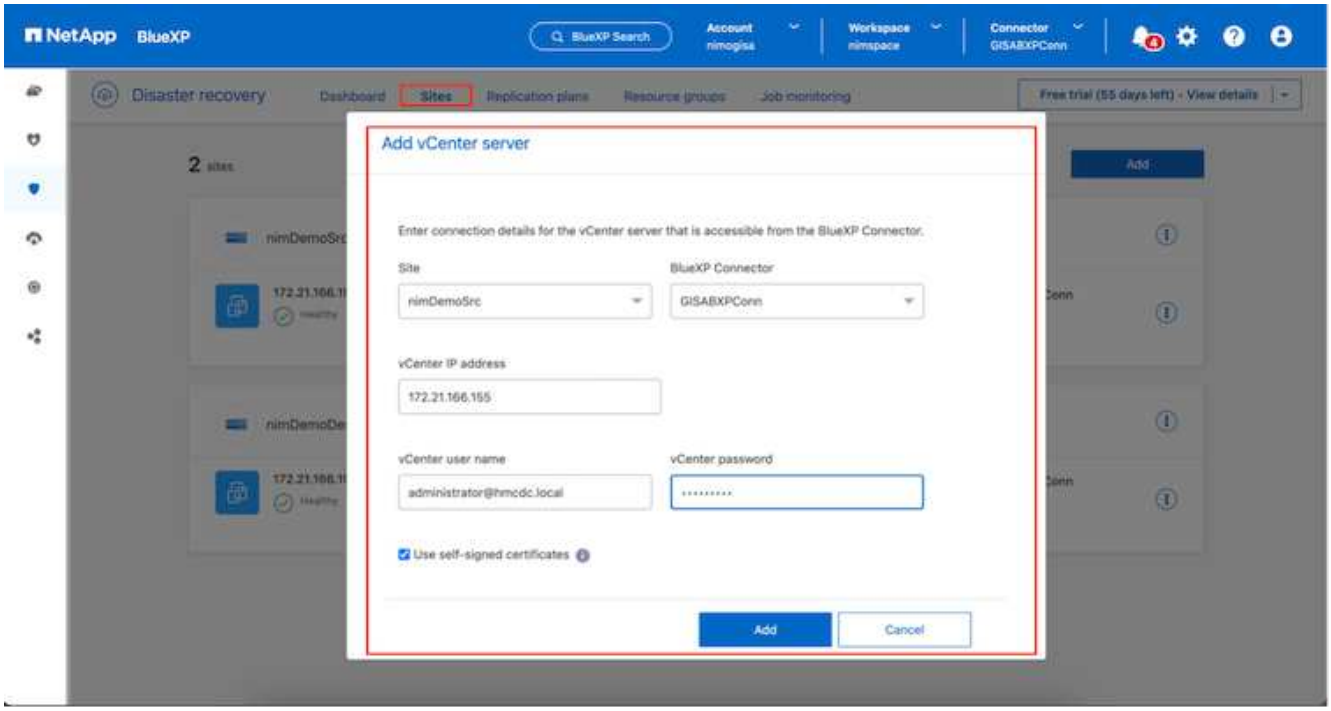
準備災難恢復的第一步是探索並將內部部署的 vCenter 和儲存資源新增至 NetApp Disaster Recovery。

開啟主控台，從左側導覽列選擇 保護 **>** 災難恢復。按一下 站台，提供名稱並選擇位置類型。然後，按一下 新增 **vCenter** 按鈕。

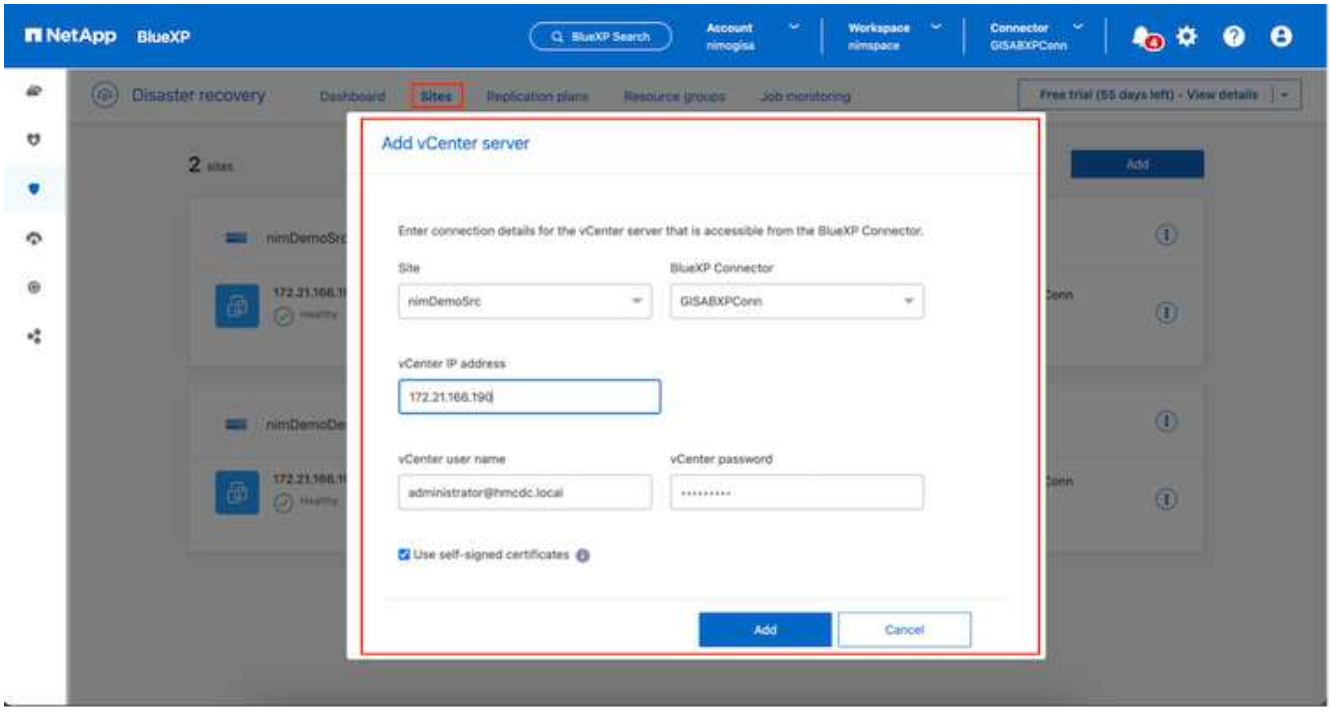


新增以下平台：

- 來源。本機 vCenter。



- 目的地。 VMC SDDC vCenter。



一旦新增了 vCenter，就會觸發自動發現。

配置來源站點陣列和目標站點陣列之間的儲存複製

SnapMirror 在 NetApp 環境中提供資料複寫功能。SnapMirror 複寫以 NetApp Snapshot 快照技術為基礎，效率極高，因為它只複寫自上次更新以來已變更或新增的區塊。SnapMirror 可透過 NetApp OnCommand System Manager 或 ONTAP CLI 輕鬆設定。NetApp Data Services 也可建立 SnapMirror 關係，前提是事先設定叢集與

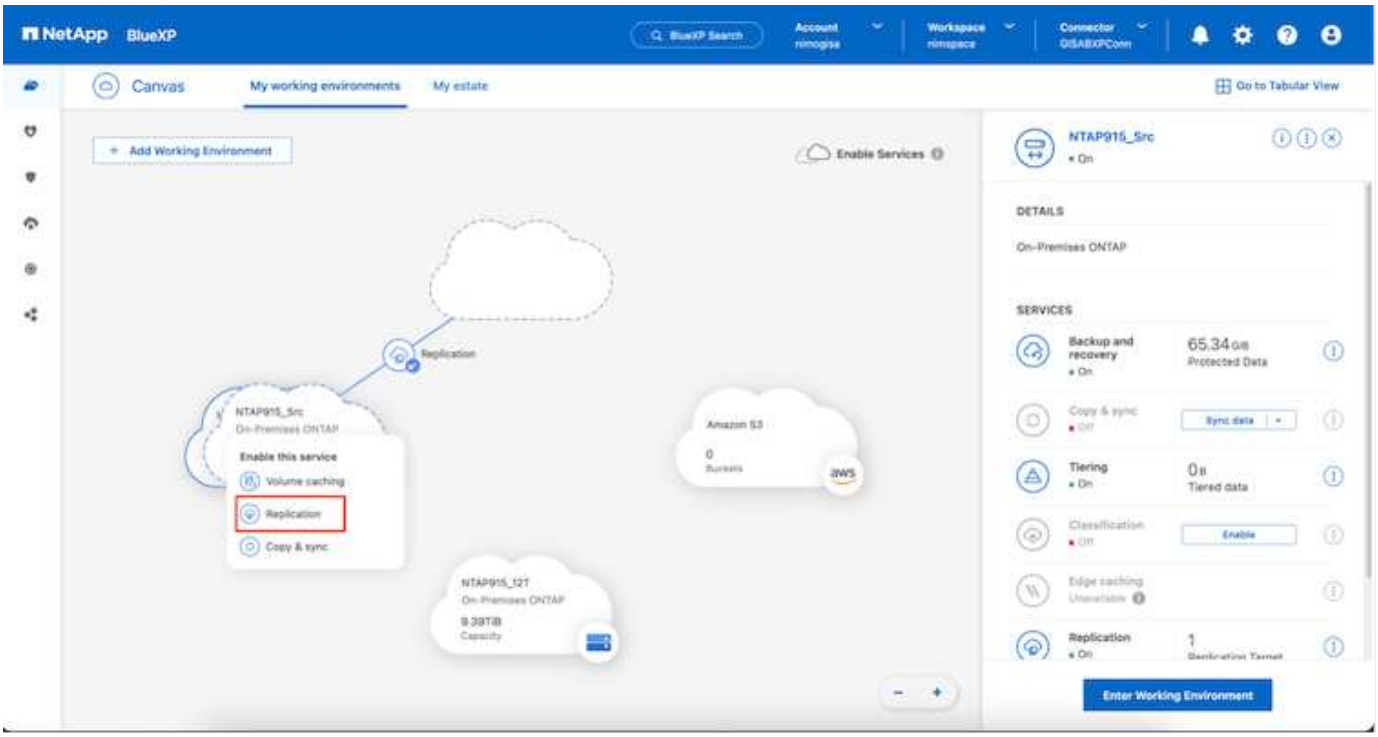
SVM 對等關係。

對於主儲存設備未完全遺失的情況，SnapMirror 提供了一種重新同步主站台和災難恢復站台的高效方法。SnapMirror 可以重新同步這兩個站台，只需反轉 SnapMirror 關係，即可僅將變更或新增的資料從災難恢復站台傳回主站台。這意味著在災難恢復中，容錯移轉後可以雙向重新同步複寫計畫，而無需重新複製整個 Volume。如果以相反方向重新同步關係，則只會將自上次成功同步 Snapshot 複本以來寫入的新資料傳回目的地。

如果已透過 CLI 或 System Manager 為 Volume 設定 SnapMirror 關係，NetApp Data Services 會取得該關係，並繼續執行其餘的工作流程作業。

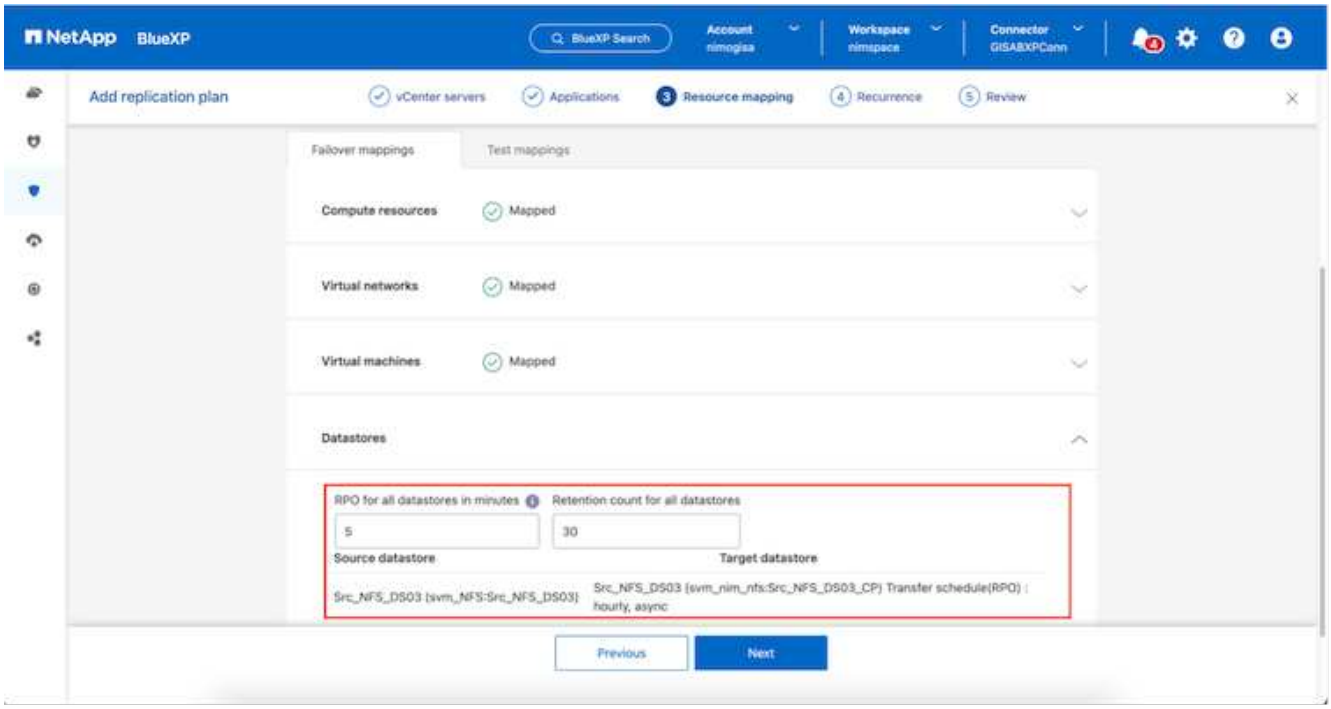
如何設定 **VMware** 災難復原

建立 SnapMirror 複寫的過程對於任何指定的應用程式皆相同。過程可以是手冊或自動化的。最簡單的方法是運用 NetApp Console 來設定 SnapMirror 複寫，只需在環境中將來源 ONTAP 系統拖放至目的地，即可觸發精靈以引導完成剩餘的過程。



如果滿足以下兩個條件，災難恢復也可以自動化相同的作業：

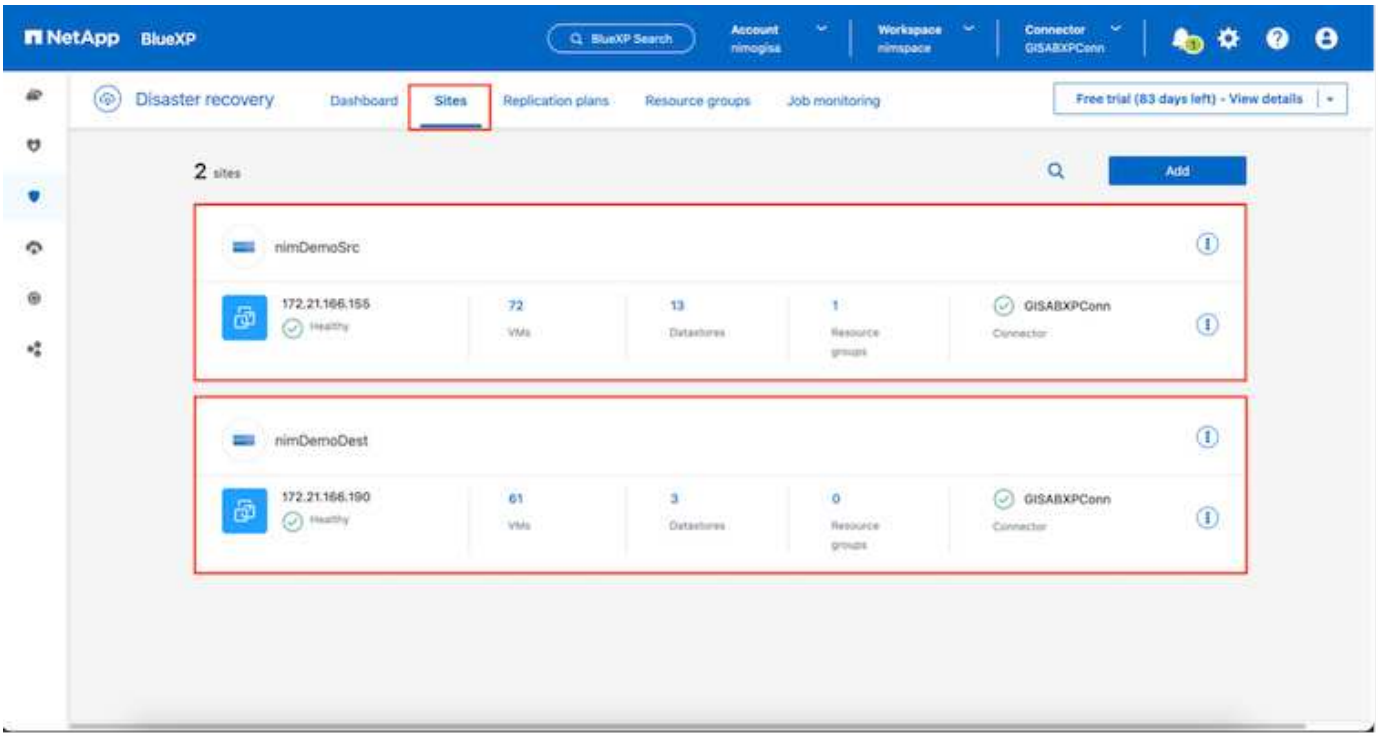
- 源集群和目標集群具有對等關係。
- 源 SVM 和目標 SVM 具有對等關係。



如果已透過 CLI 為 Volume 設定 SnapMirror 關係，則災難恢復會取得該關係並繼續執行其餘的工作流程操作。

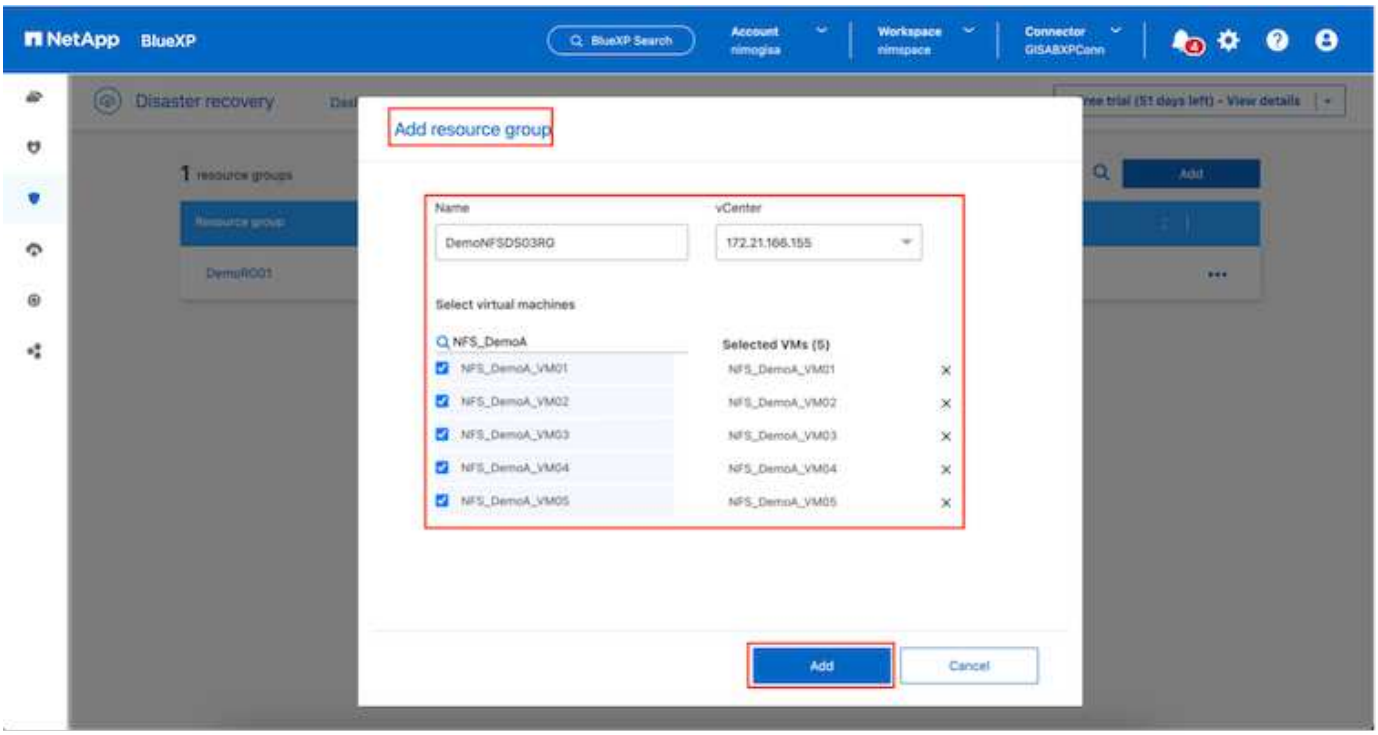
災難恢復能為您帶來什麼好處？

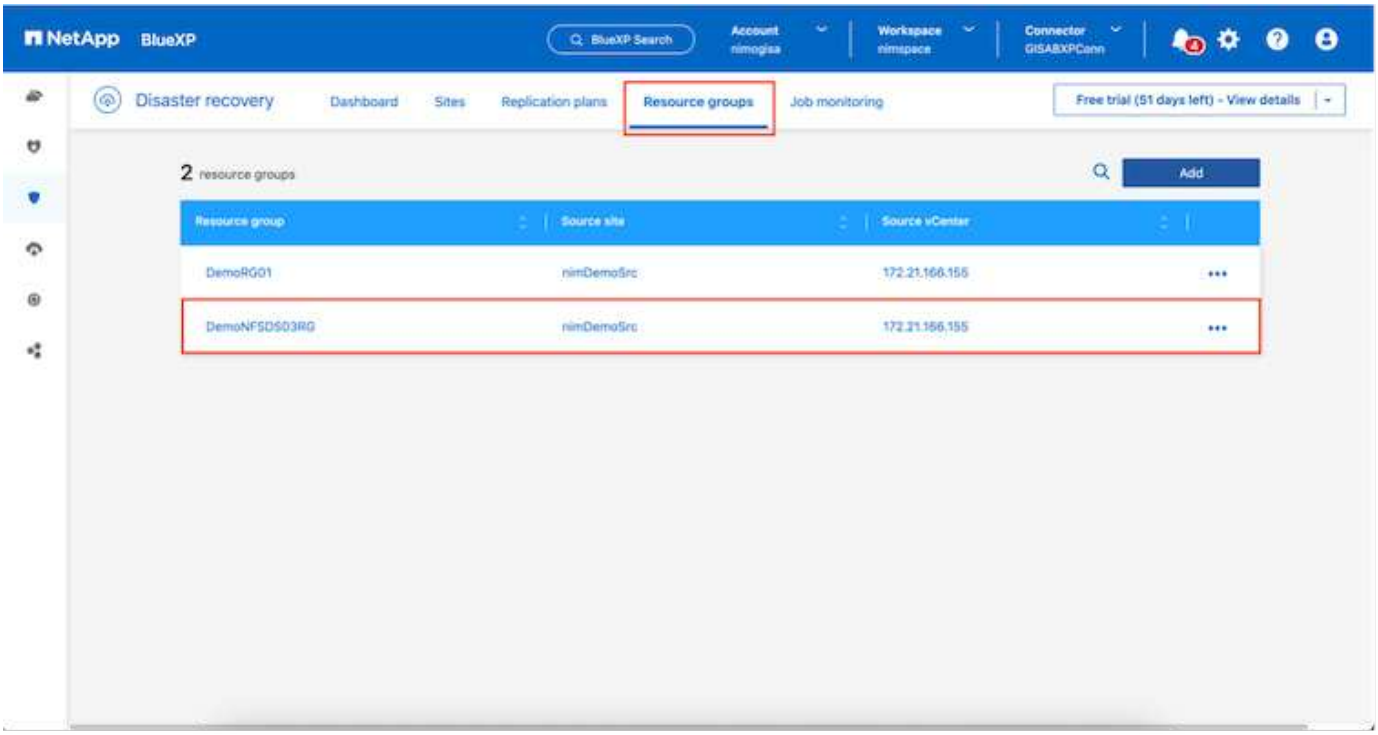
新增來源和目的地站台後，災難恢復會自動執行深度探索，並顯示虛擬機器及其關聯的中繼資料。災難恢復也會自動偵測虛擬機器使用的網路和連接埠群組，並將其填入。



新增站台後，即可將虛擬機器分組到資源群組。災難恢復資源群組可讓您將一組相依的虛擬機器分組到邏輯群組

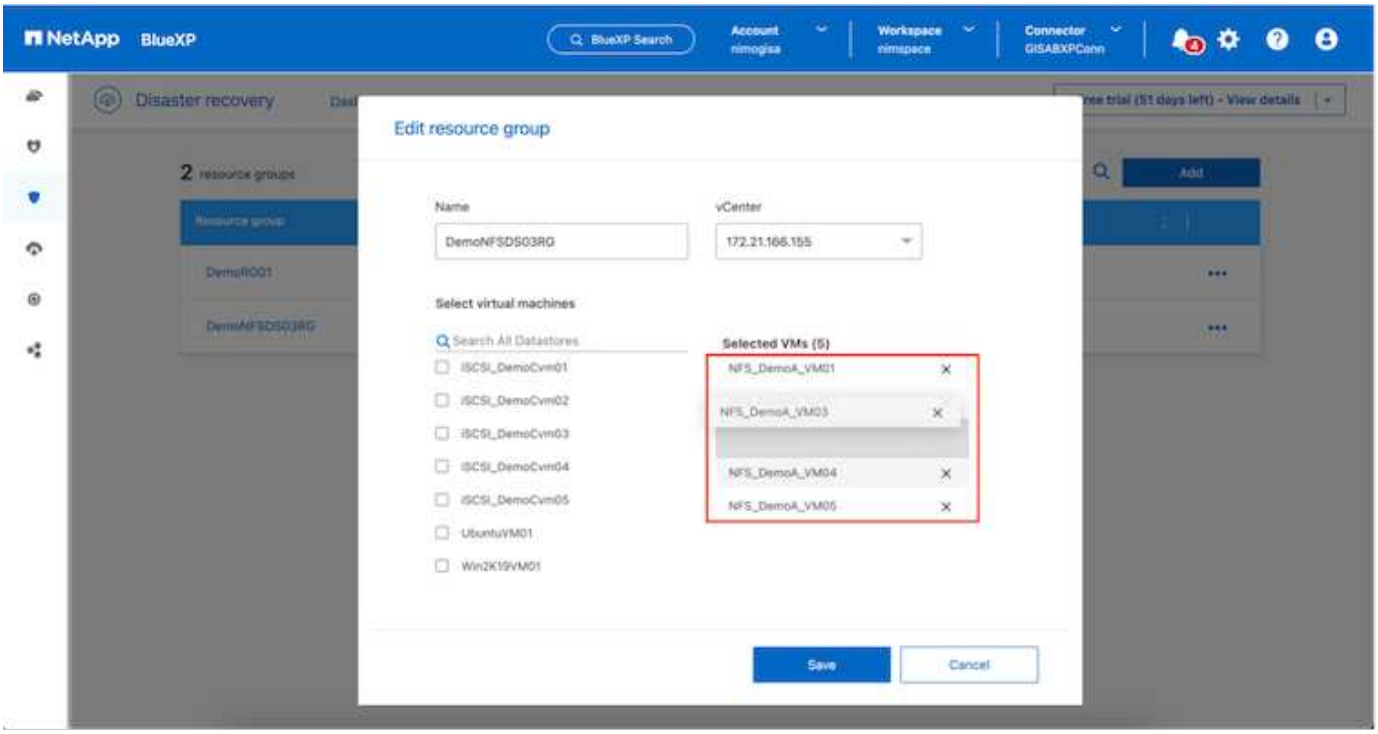
中，這些邏輯群組包含其開機順序和開機延遲，以便在恢復時執行。若要開始建立資源群組，請導覽至 資源群組 ，然後按一下 建立新資源群組 。



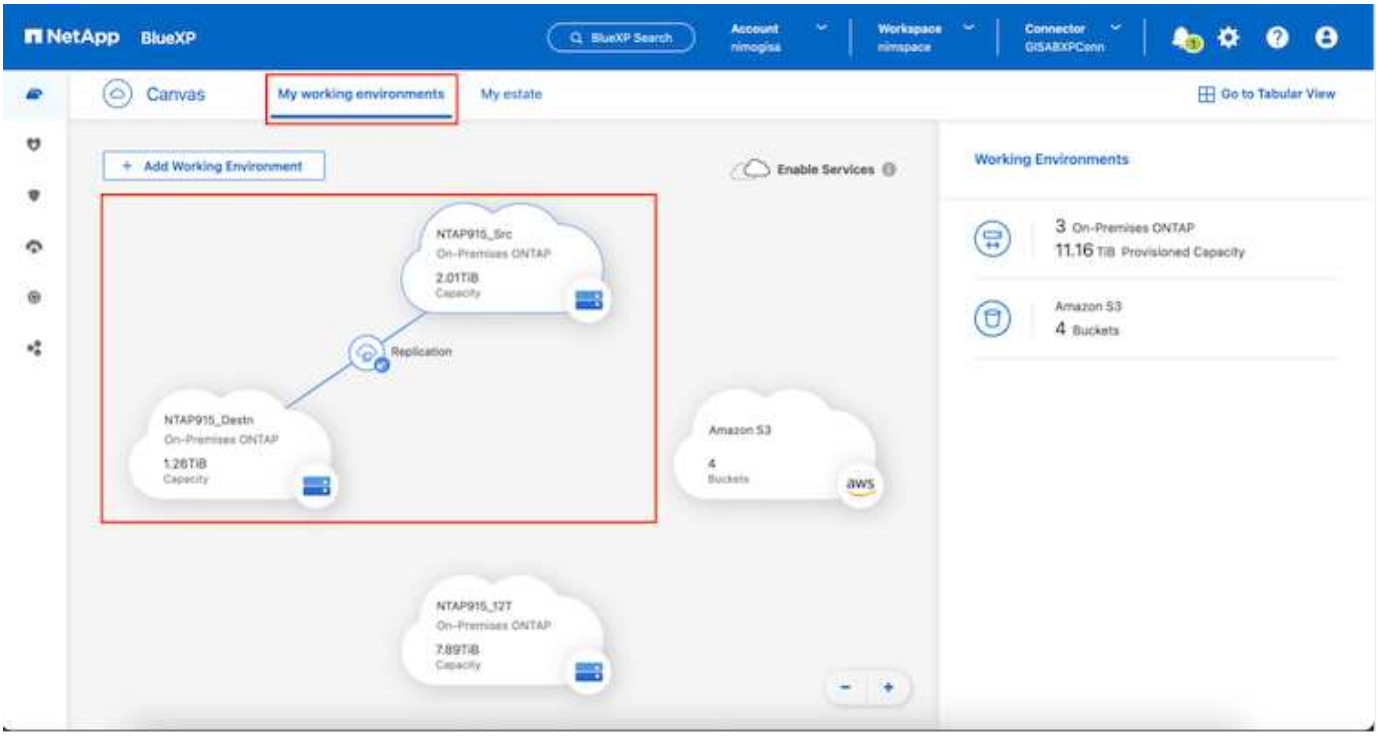


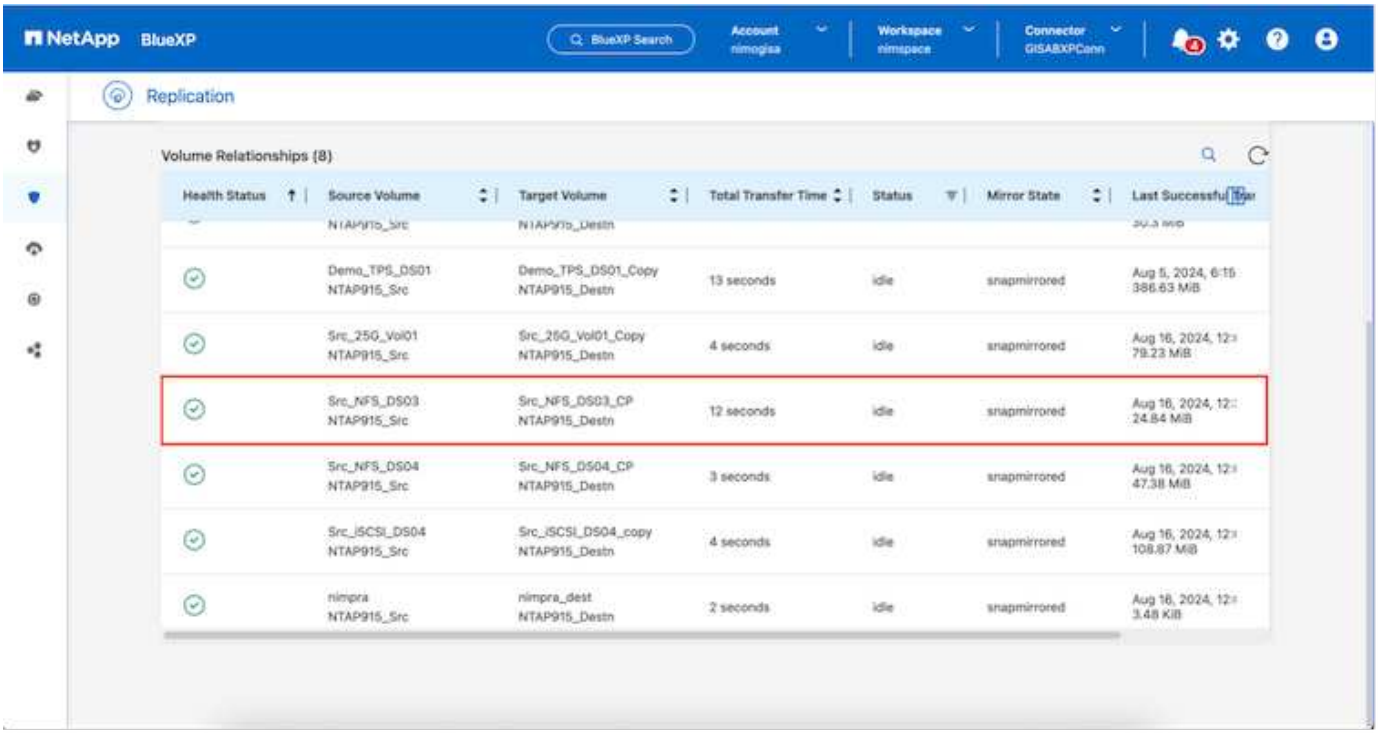
在建立複製計劃時也可以建立資源組。

可以透過簡單的拖放機制在建立資源群組期間定義或修改虛擬機器的啟動順序。



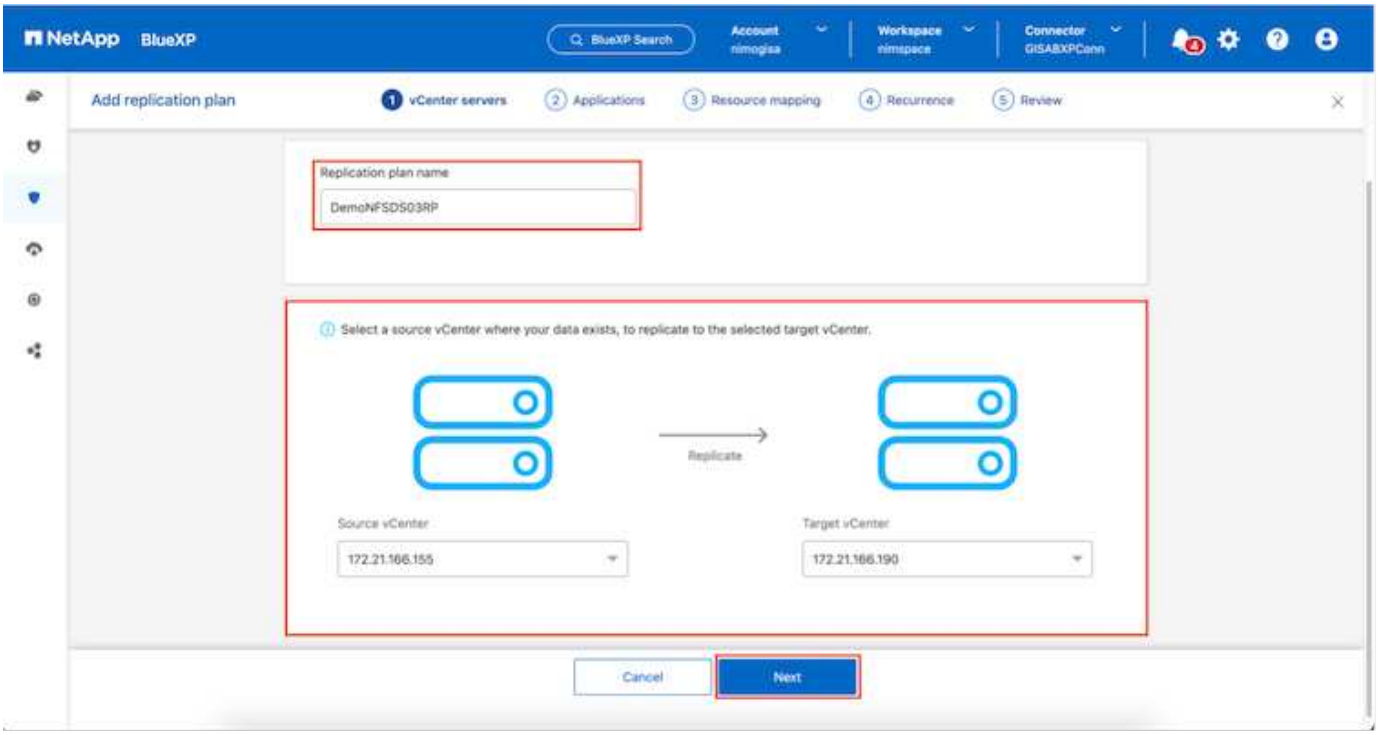
建立資源群組後，下一步是建立執行藍圖或在災難發生時復原虛擬機器和應用程式的計畫。如先決條件中所述，可以預先配置SnapMirror複製，或者 DRaaS 可以使用在建立複製計劃期間指定的 RPO 和保留計數來配置它。



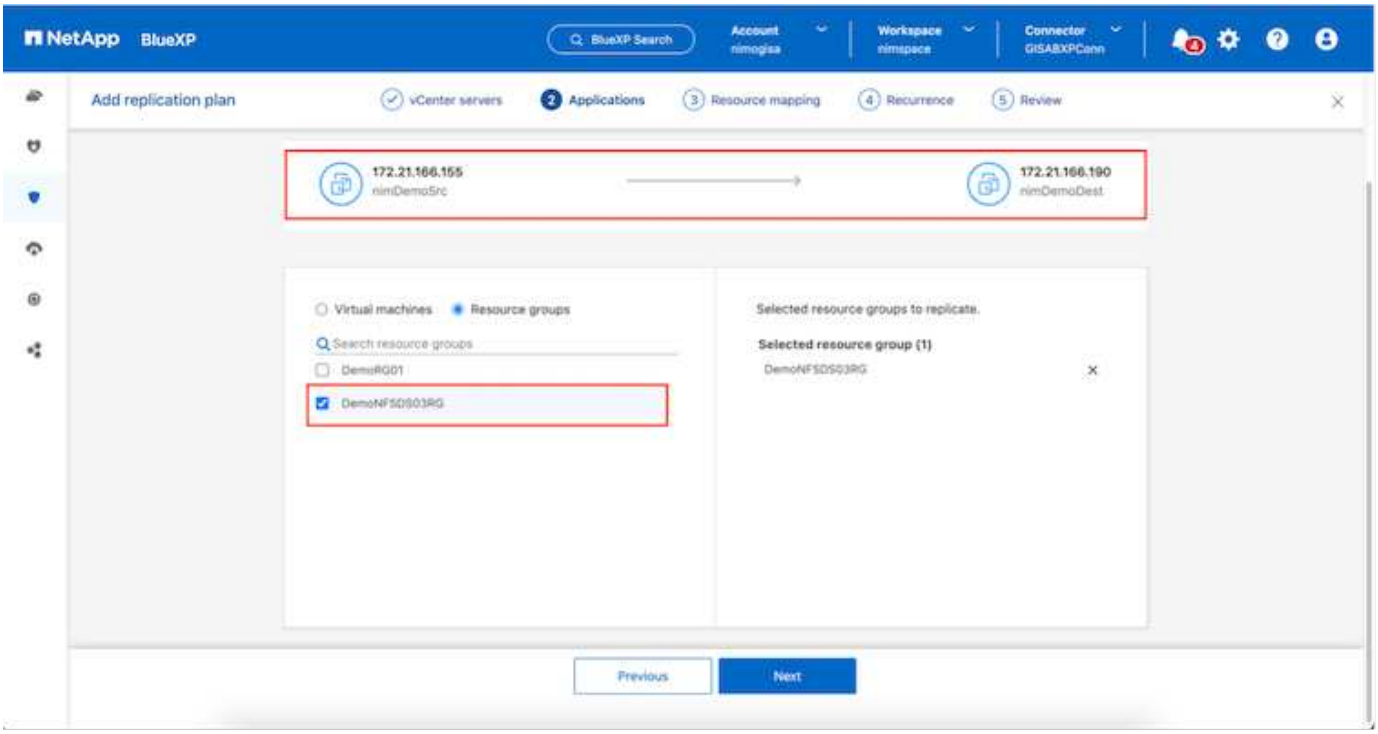


透過從下拉式選單中選擇來源和目標 vCenter 平台來設定複製計劃，並選擇要包含在計劃中的資源群組，以及如何復原和啟動應用程式的分組以及叢集和網路的對應。若要定義復原計劃，請導覽至「複製計劃」標籤並按一下「新增計劃」。

首先，選擇來源 vCenter，然後選擇目標 vCenter。



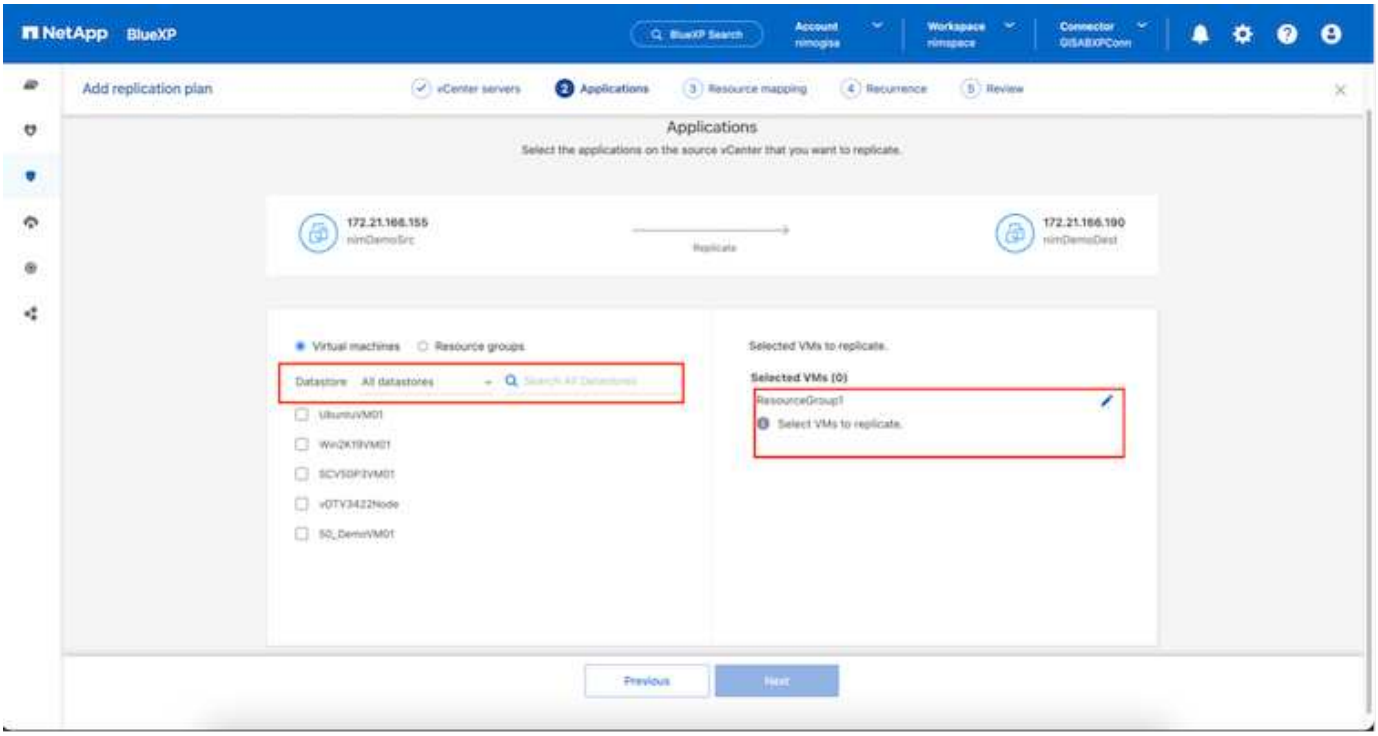
下一步是選擇現有的資源組。如果沒有建立資源組，則精靈將協助根據復原目標對所需的虛擬機器進行分組（基本上建立功能資源組）。這也有助於定義如何恢復應用程式虛擬機器的操作順序。



資源組允許使用拖放功能設定啟動順序。它可用於輕鬆修改復原過程中虛擬機器的啟動順序。

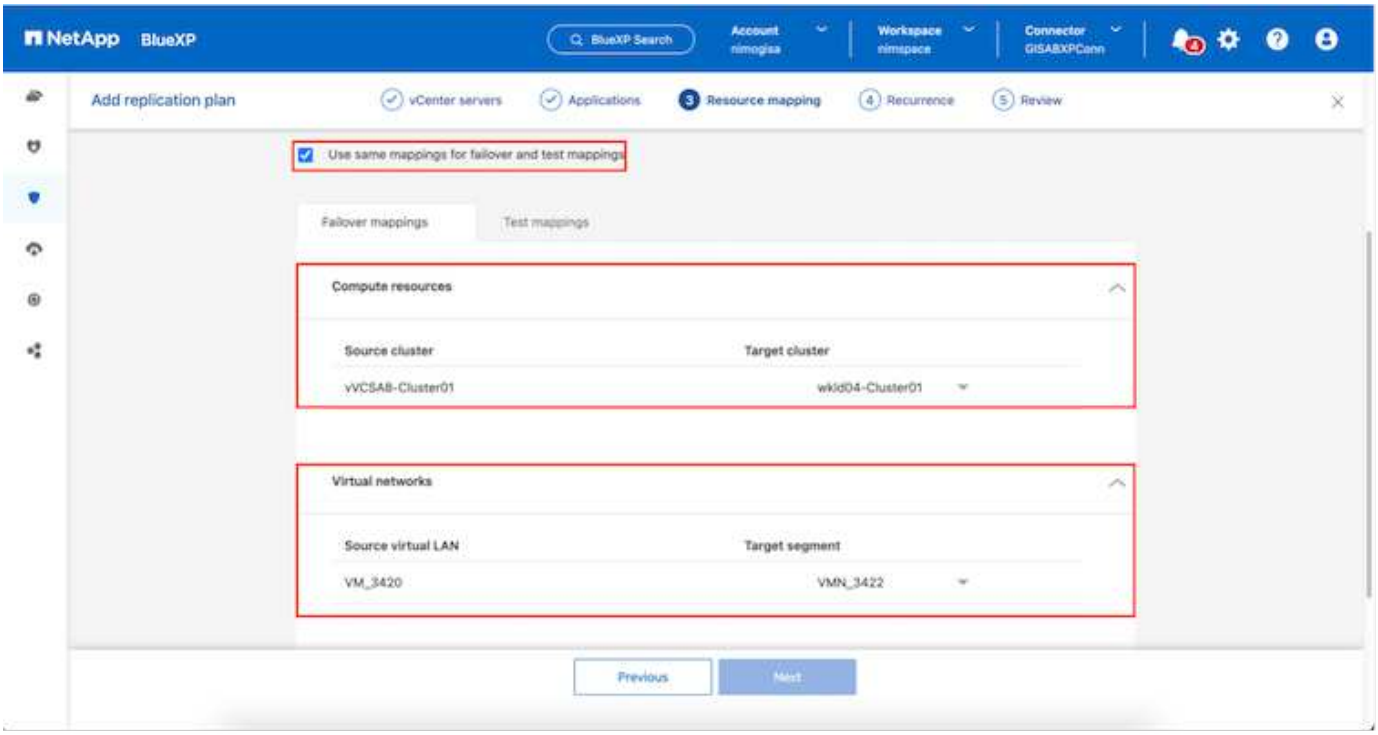
資源組內的各個虛擬機器依序依序啟動。兩個資源組並行啟動。

如果未事先建立資源群組，則下列螢幕截圖顯示了根據組織要求過濾虛擬機器或特定資料儲存的選項。

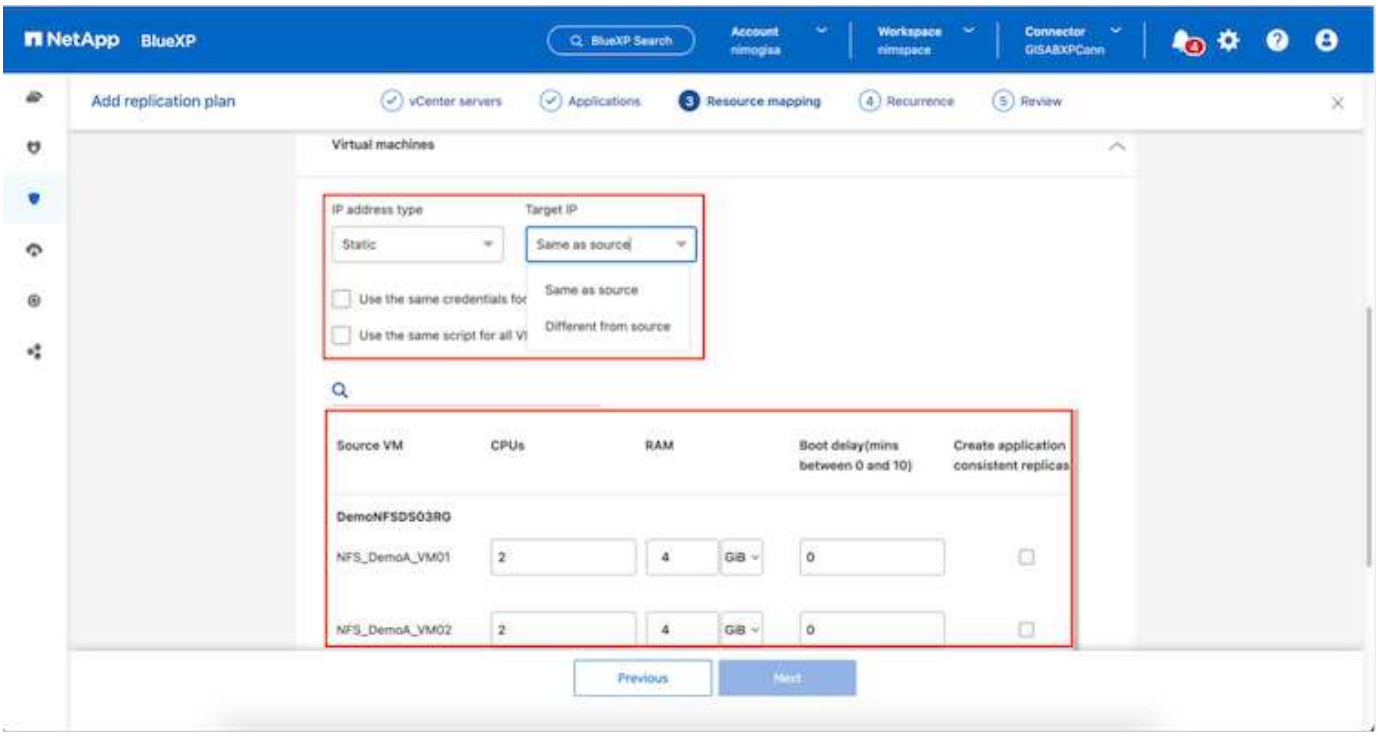


選取資源群組後，建立容錯移轉對應。在此步驟中，指定來源環境中的資源如何對應至目的地。這包括運算資源、虛擬網路。IP 自訂、執行前與執行後指令碼、開機延遲、應用程式一致性等等。如需詳細資訊，請參閱 "建

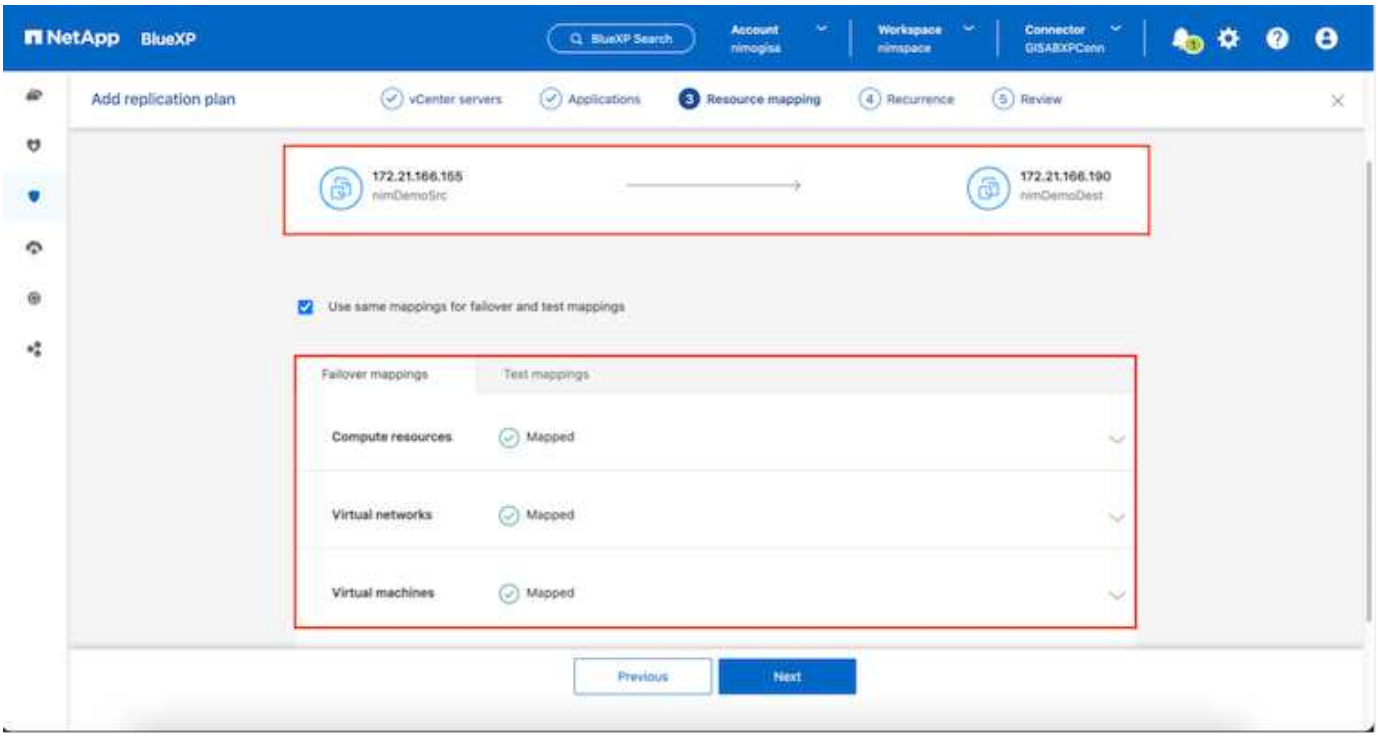
立複製計劃"。



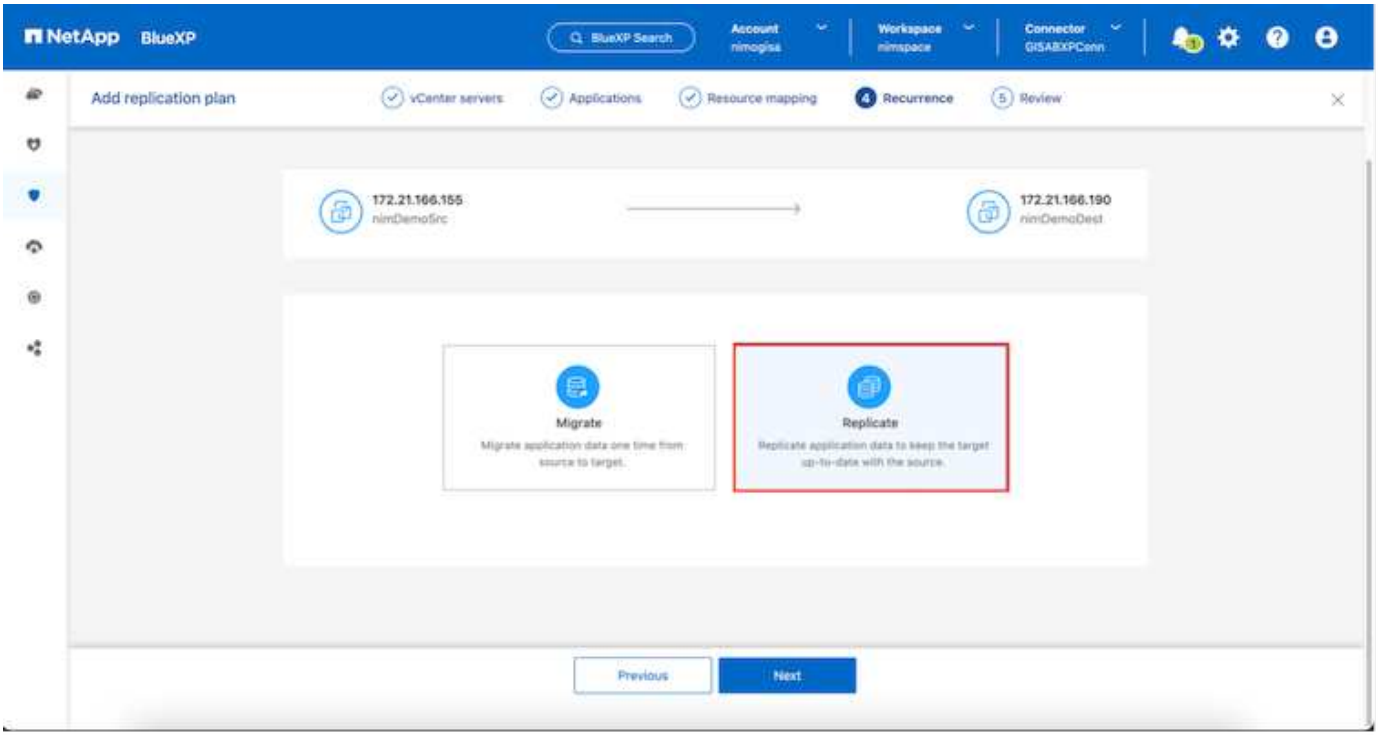
預設情況下，測試和故障轉移操作使用相同的映射參數。若要為測試環境設定不同的映射，請取消勾選方塊後選擇測試映射選項，如下所示：



資源映射完成後，按一下下一步。

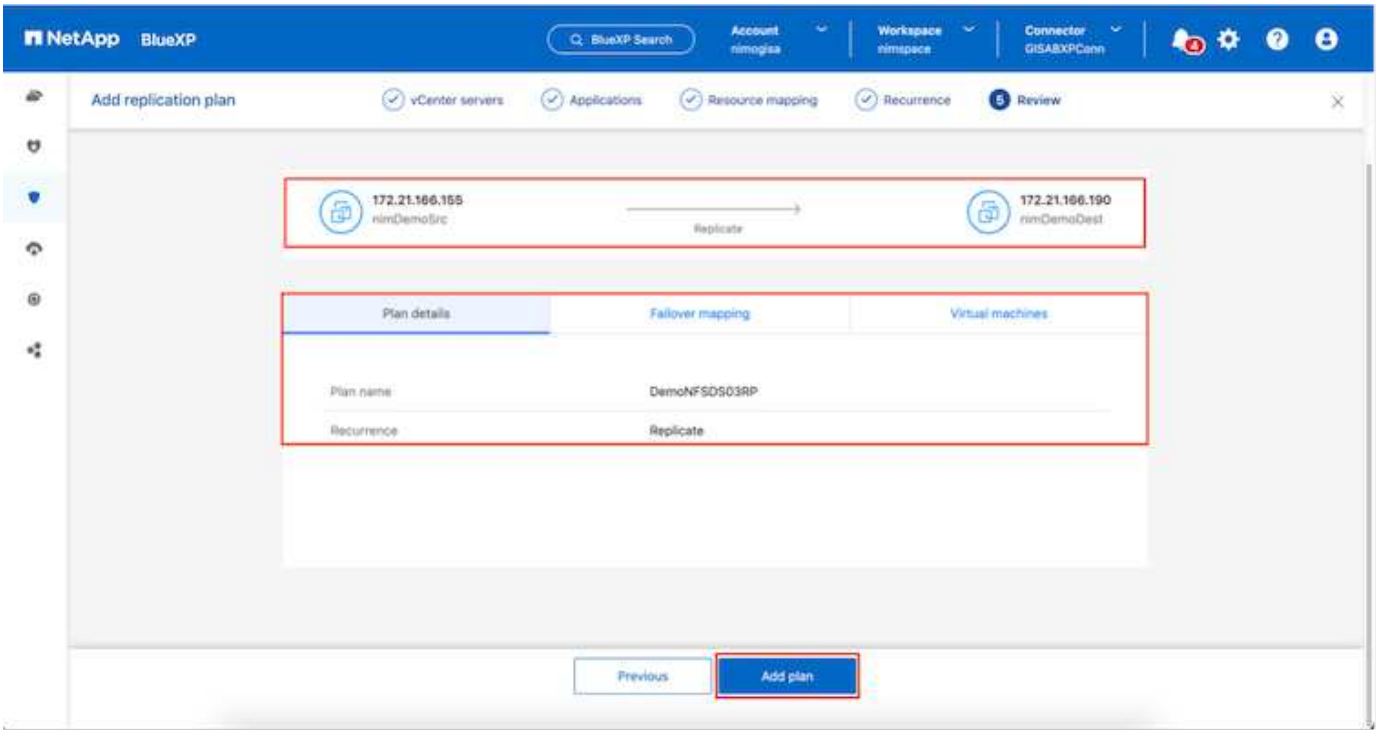


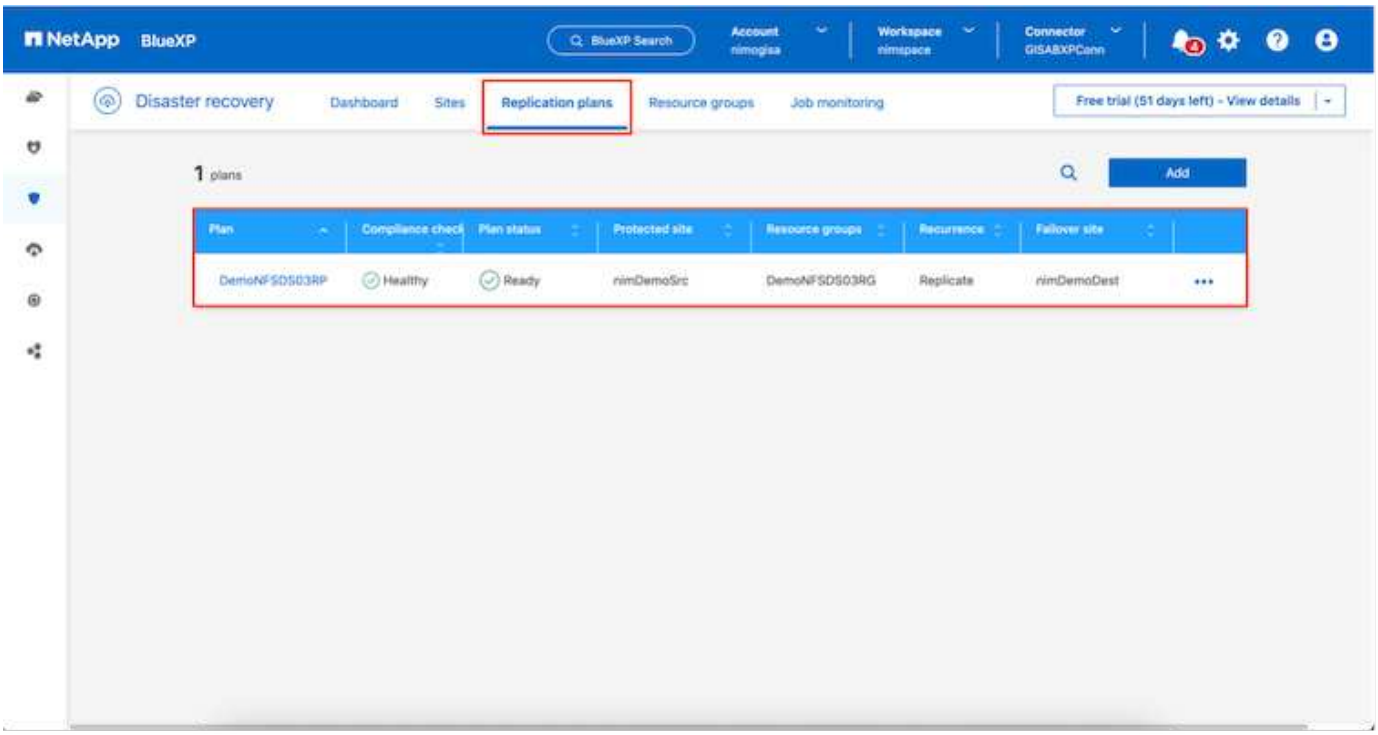
選擇重複類型。簡單來說，選擇遷移（使用故障轉移的一次性遷移）或重複連續複製選項。在本演練中，選擇了「複製」選項。



完成後，檢查已建立的映射，然後按一下*新增計劃*。

來自不同 Volume 和 SVM 的虛擬機器可以包含在複寫計畫中。根據虛擬機器的放置位置（無論是在同一 Volume 上、同一 SVM 內的分隔 Volume 上，或是不同 SVM 上的分隔 Volume 上），災難恢復會建立一致性群組 Snapshot 快照技術。



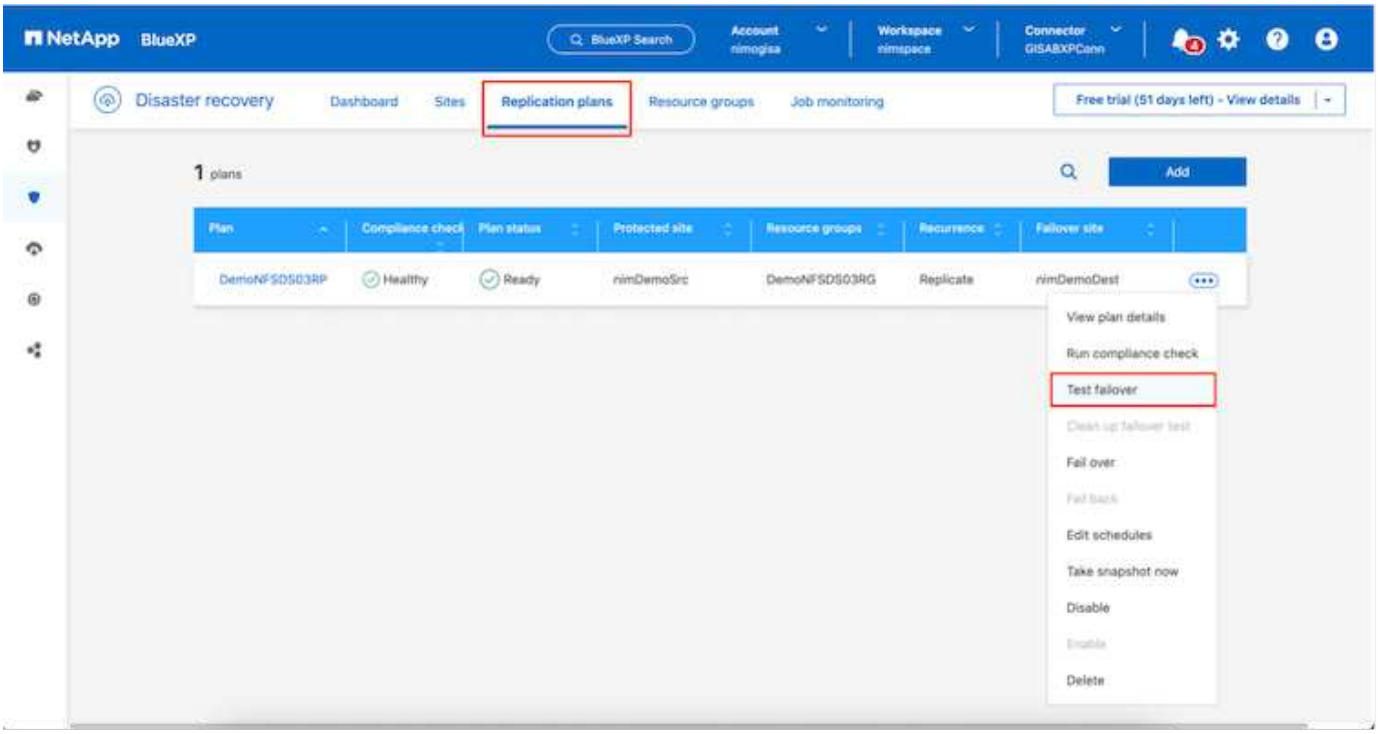


災難恢復包括以下工作流程：

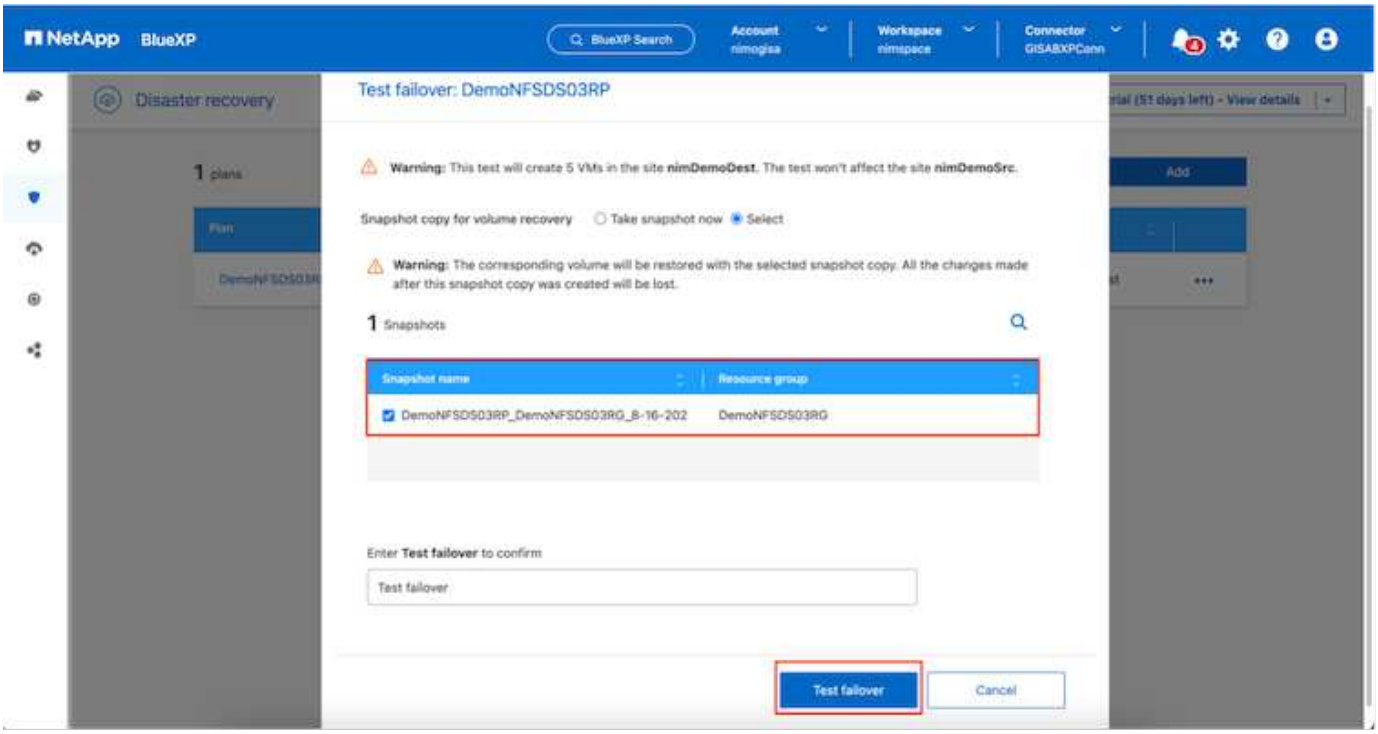
- 測試故障轉移（包括定期自動模擬）
- 清理故障轉移測試
- 故障轉移
- 故障回覆

測試故障轉移

災難恢復中的測試容錯移轉是一項操作程序，可讓 VMware 系統管理員在不中斷生產環境的情況下，全面驗證其恢復計畫。在測試容錯移轉期間，災難恢復會在災難恢復儲存系統上，建立複寫的 NFS 資料存放區 Volume 的極具空間效率 NetApp FlexClone 複本。然後，這些 FlexClone Volume 會掛載到災難恢復站台的 ESXi 主機，並在隔離的測試網路中將虛擬機器開機。此程序可讓系統管理員驗證其災難恢復計畫在發生實際災難時，是否能如預期運作。

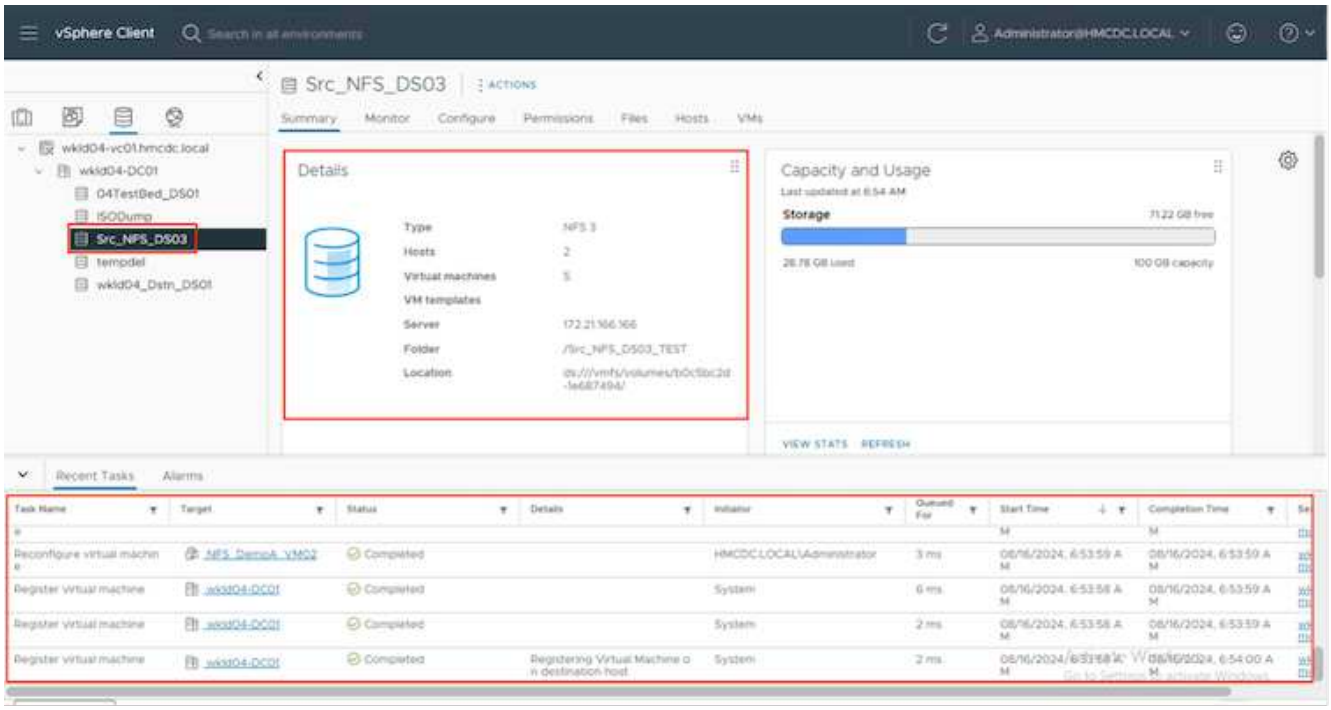


災難恢復包含在測試容錯移轉作業中選擇 Snapshot 複本做為選用功能的能力。此功能可讓 VMware 系統管理員驗證環境中最近所做的任何變更是否已複寫到目的地站台，從而在測試期間呈現。此類變更包括虛擬機器客體作業系統的修補程式



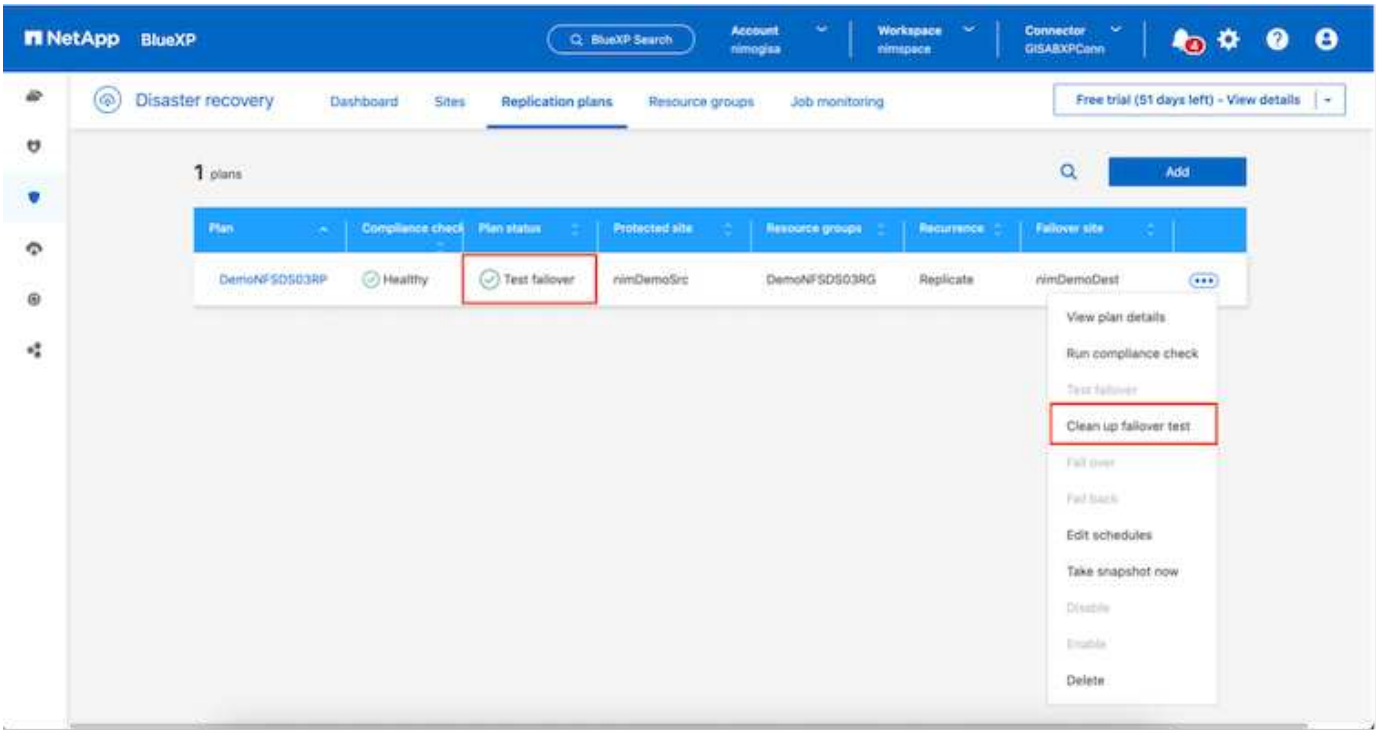
當 VMware 系統管理員執行測試容錯移轉作業時，災難恢復會自動化下列工作：

- 觸發SnapMirror關係，使用生產網站上所做的任何最新變更來更新目標網站上的儲存空間。
- 在 DR 儲存陣列上建立FlexVol磁碟區的NetApp FlexClone磁碟區。
- 將FlexClone磁碟區中的 NFS 資料儲存庫連接到 DR 站點的 ESXi 主機。
- 將虛擬機器網路介面卡連接到映射期間指定的測試網路。
- 依照 DR 站點的網路定義重新配置 VM 客戶作業系統網路設定。
- 執行複製計劃中儲存的任何自訂命令。
- 依照複製計畫中定義的順序啟動虛擬機器。



清理故障轉移測試操作

清理故障轉移測試操作在複製計劃測試完成並且 VMware 管理員回應清理提示後發生。



此操作將虛擬機器 (VM) 和複製計劃的狀態重設為就緒狀態。

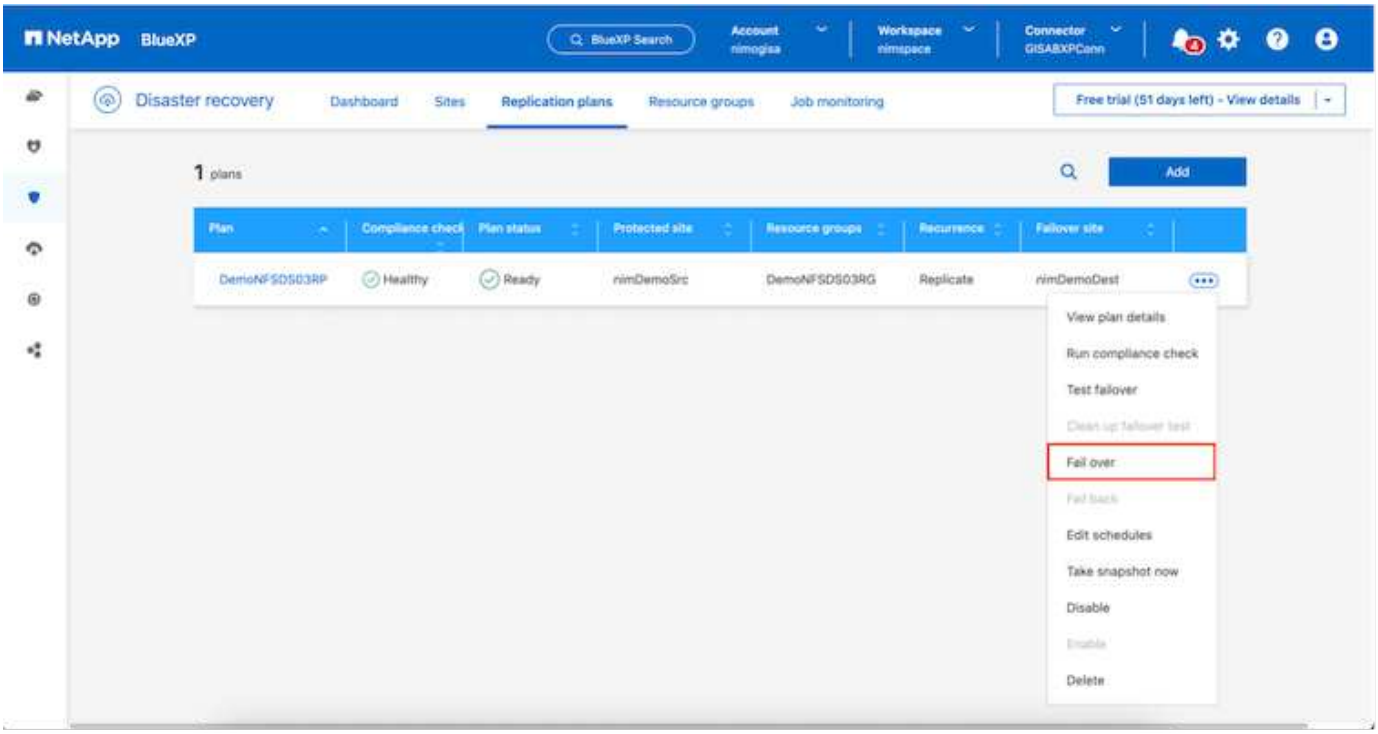
當 VMware 系統管理員執行恢復作業時，災難恢復會完成下列程序：

1. 它關閉用於測試的FlexClone副本中的每個恢復的虛擬機器。

2. 它會刪除在測試期間用於呈現復原的虛擬機器的 FlexClone磁碟區。

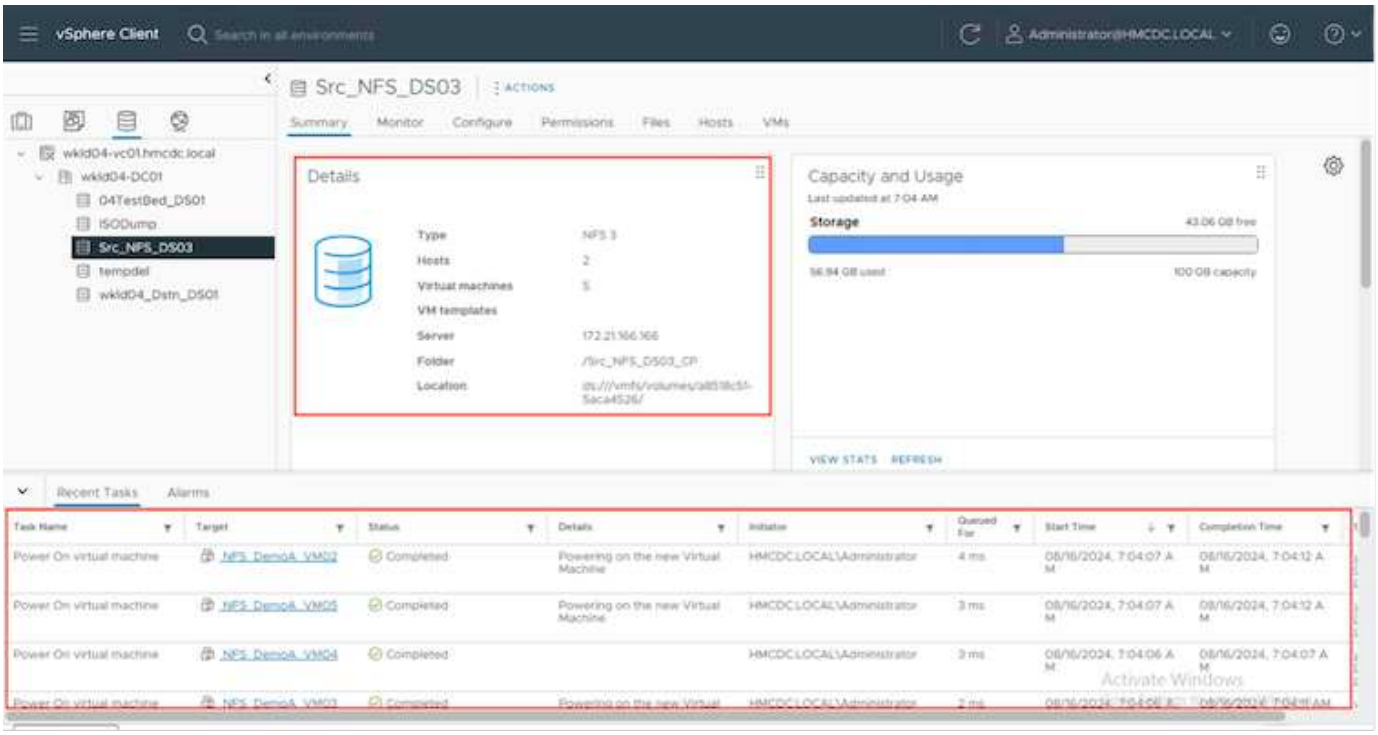
計劃遷移和故障轉移

災難恢復有兩種執行真正容錯移轉的方法：計畫性移轉和容錯移轉。第一種方法是計畫性移轉，將虛擬機器關機和儲存設備複寫同步整合到流程中，以恢復或有效地將虛擬機器移轉到目的地站台。計畫性移轉需要存取來源站台。第二種方法是容錯移轉，這是一種計畫性/非計畫性的容錯移轉，其中虛擬機器會在目的地站台，從上一次成功完成的儲存設備複寫間隔中恢復。根據解決方案中設計的 RPO，在災難恢復情境中可能會出現一定程度的資料遺失。



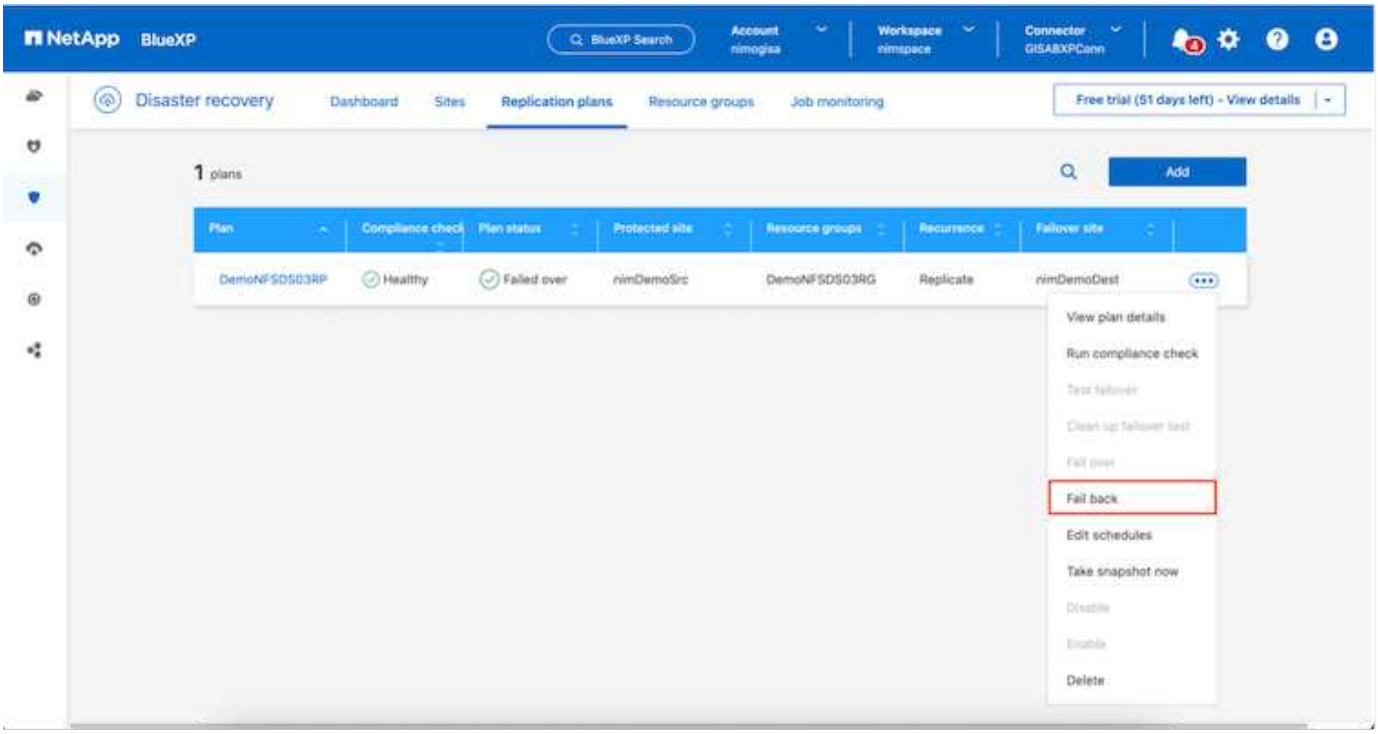
當 VMware 系統管理員執行容錯移轉作業時，災難恢復會自動化下列任務：

- 中斷並故障轉移NetApp SnapMirror關係。
- 將複製的 NFS 資料儲存連接到 DR 站點的 ESXi 主機。
- 將 VM 網路介面卡連接到適當的目標站點網路。
- 依照目標站點的網路定義重新配置 VM 客戶作業系統網路設定。
- 執行複製計劃中儲存的任何自訂命令（如果有）。
- 依照複製計畫中定義的順序啟動虛擬機器。



故障回覆

故障回復是一種選用過程，可在復原後還原來源站台和目標站台的原始設定。



當 VMware 管理員準備將服務還原到原始來源網站時，他們可以設定並執行故障回應程式。

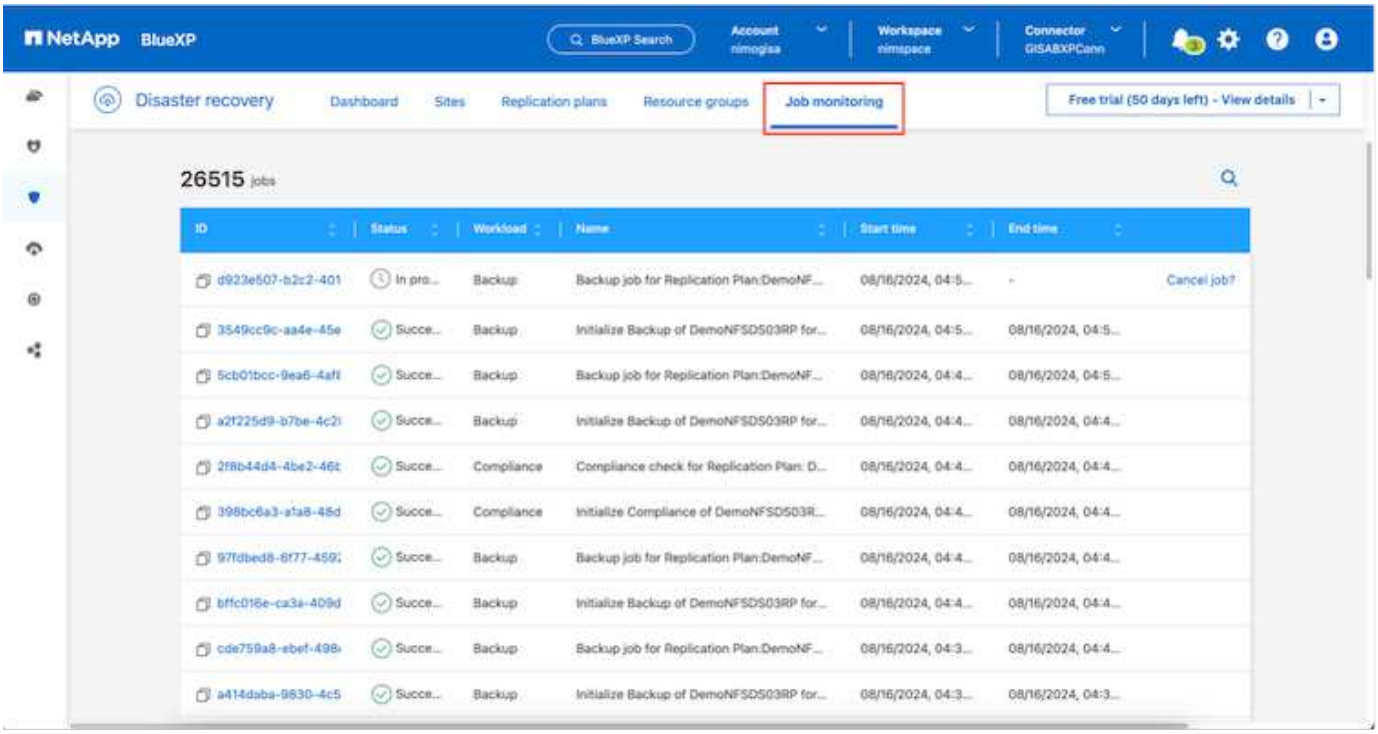
*注意：*災難恢復會在反轉複寫方向之前，將任何變更複寫（重新同步）回原始來源虛擬機器。此程序從已完成容錯移轉至目標的關係開始，並包含下列步驟：

- 關閉並取消註冊虛擬機，並卸載目標網站上的磁碟區。
- 打破原始來源上的SnapMirror關係，使其變成讀/寫。
- 重新同步SnapMirror關係以逆轉複製。
- 在來源上安裝卷，啟動並註冊來源虛擬機器。

如需存取與設定災難恢復的詳細資訊，請參閱"了解適用於 VMware 的 NetApp Disaster Recovery"。

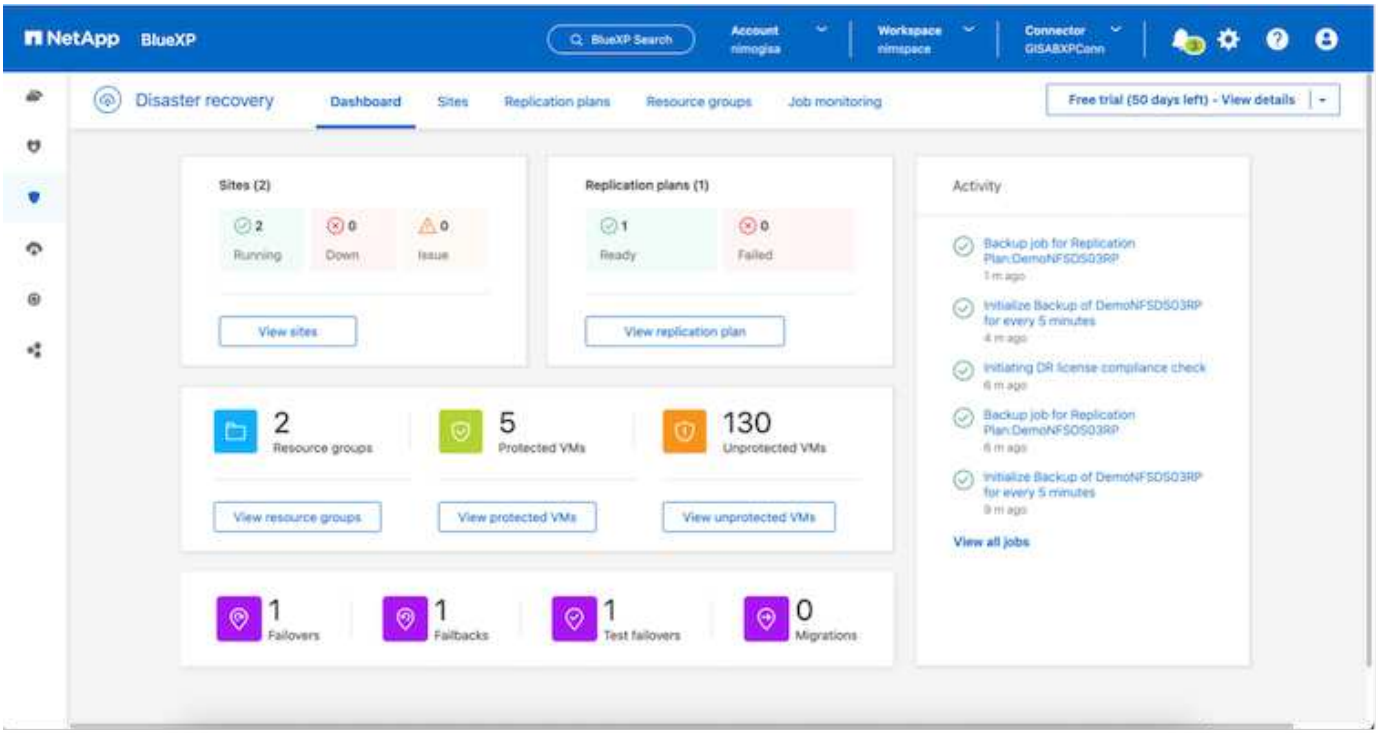
監控和儀表板

從 Console 或 ONTAP CLI，您可以監控適當資料存放區 Volume 的複寫健全狀況，並可透過作業監控來追蹤容錯移轉或測試容錯移轉的狀態。



如果某項工作目前正在進行或排隊，而您希望停止它，則可以選擇取消它。

透過災難恢復儀表板，您可以自信地評估災難恢復站台與複寫計畫的狀態。這可讓系統管理員迅速識別健全、已斷線或降級的站台與計畫。



這為處理量身定制的災難復原計劃提供了強大的解決方案。當發生災難並決定啟動 DR 站點時，可以按計劃進行故障轉移或單擊按鈕進行故障轉移。

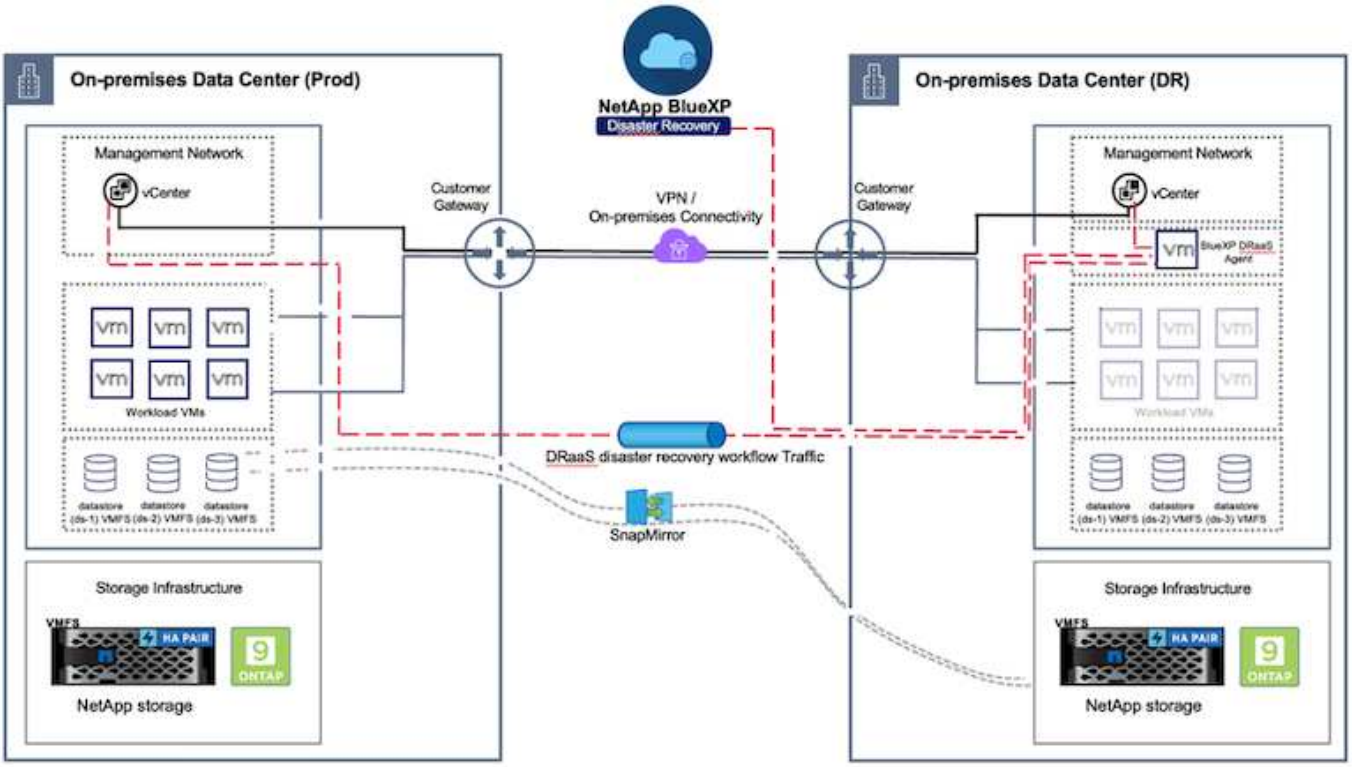
要了解有關此過程的更多信息，請隨意觀看詳細的演示視頻或使用"解決方案模擬器"。

適用於 **VMFS** 資料儲存的 **NetApp Disaster Recovery**

使用從生產站點到災難復原站點的區塊級複製進行災難復原是一種有彈性且經濟高效的方法，可保護工作負載免受網站中斷和資料損壞事件（如勒索軟體攻擊）的影響。透過NetApp SnapMirror複製，使用 VMFS 資料儲存區運行本地ONTAP系統的 VMware 工作負載可以複製到 VMware 所在的指定復原資料中心的另一個ONTAP儲存系統

本文件的此節說明 NetApp Disaster Recovery 的組態，以為內部部署 VMware VM 設定災難恢復至另一個指定站台。做為此設定的一部分，包括 Console 代理程式、上線 ONTAP 陣列、定義站台以及關聯 VMware vCenter。此外，本文件詳細說明如何設定站台之間的複寫，以及如何設定與測試恢復計畫。最後一節提供執行完整站台容錯移轉的指示，以及在主站台恢復並上線時如何進行容錯回復。

運用 NetApp Data Services 的災難恢復功能，客戶可以探索其內部部署的 VMware vCenters 以及 ONTAP 儲存設備，建立資源群組，建立災難恢復計畫，將其與資源群組建立關聯，並測試或執行容錯移轉與容錯回復。SnapMirror 提供儲存層級的區塊複寫，透過遞增變更讓兩個站台保持最新狀態，進而達成最短 5 分鐘的 RPO。此外，也可以將 DR 程序模擬為常規演練，而不會影響生產環境與複寫的資料存放區，也不會產生額外儲存容量成本。NetApp Data Services 運用 ONTAP 的 FlexClone 技術，從 DR 站台上最後一次複寫的 Snapshot 快照技術，建立 VMFS 資料存放區極具空間效率的複本。DR 測試完成後，客戶只需刪除測試環境即可，同樣不會對實際複寫的生產資源造成任何影響。當需要（計畫內或計畫外）進行實際容錯移轉時，只需按幾下，災難恢復功能即可協調所有必要步驟，自動在指定的災難恢復站台上啟動受保護的虛擬機器。該服務也會反轉與主要站台的 SnapMirror 關係，並在需要時將任何變更從次要站台複寫到主要站台，以進行容錯回復作業。與其他知名替代方案相比，只需極低的成本即可達成所有這些目標。

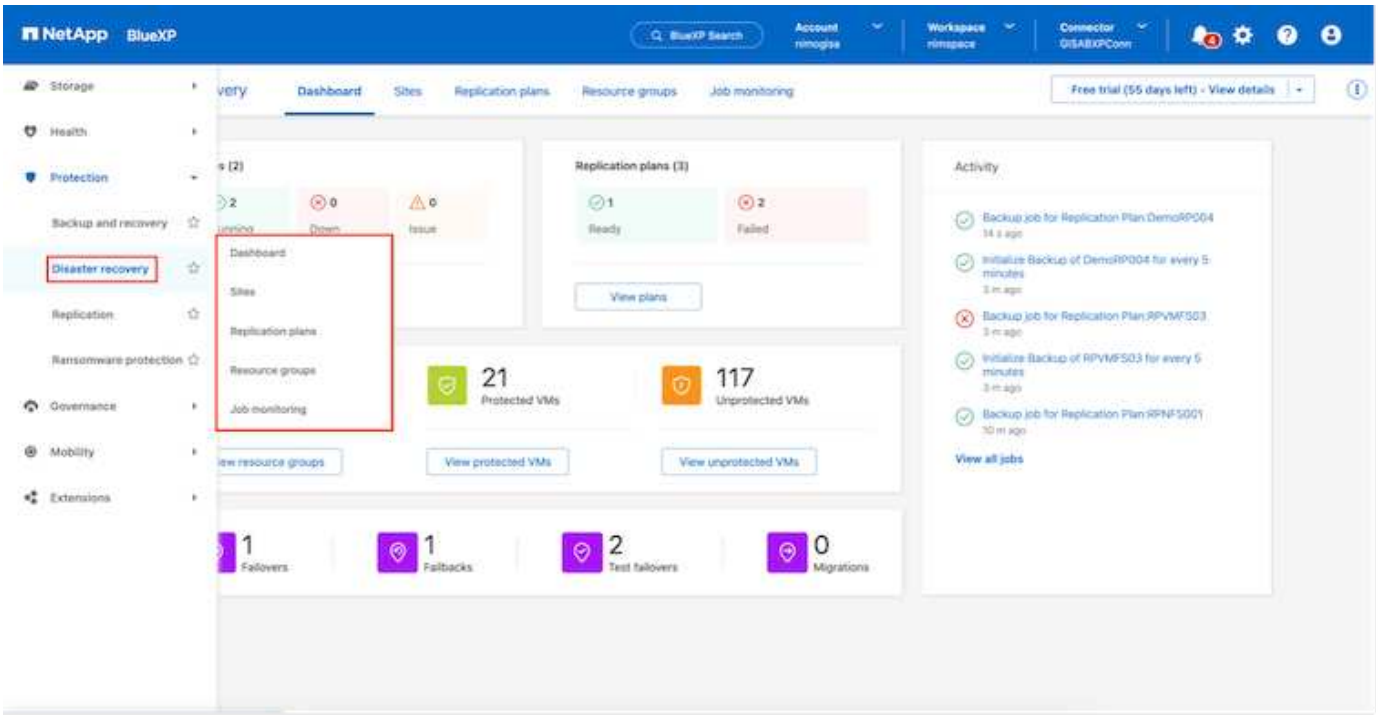


如需用於災難恢復的 vCenter Server、ESXi 和 ONTAP 的最新資訊與支援版本，請參閱 "災難恢復支援的組態"。

入門

若要開始使用災難恢復，請使用 NetApp Console，然後存取服務。

1. 登入控制台。
2. 從主控台左側導覽中，選取「保護」>「災難恢復」。
3. 災難恢復儀表板隨即顯示。

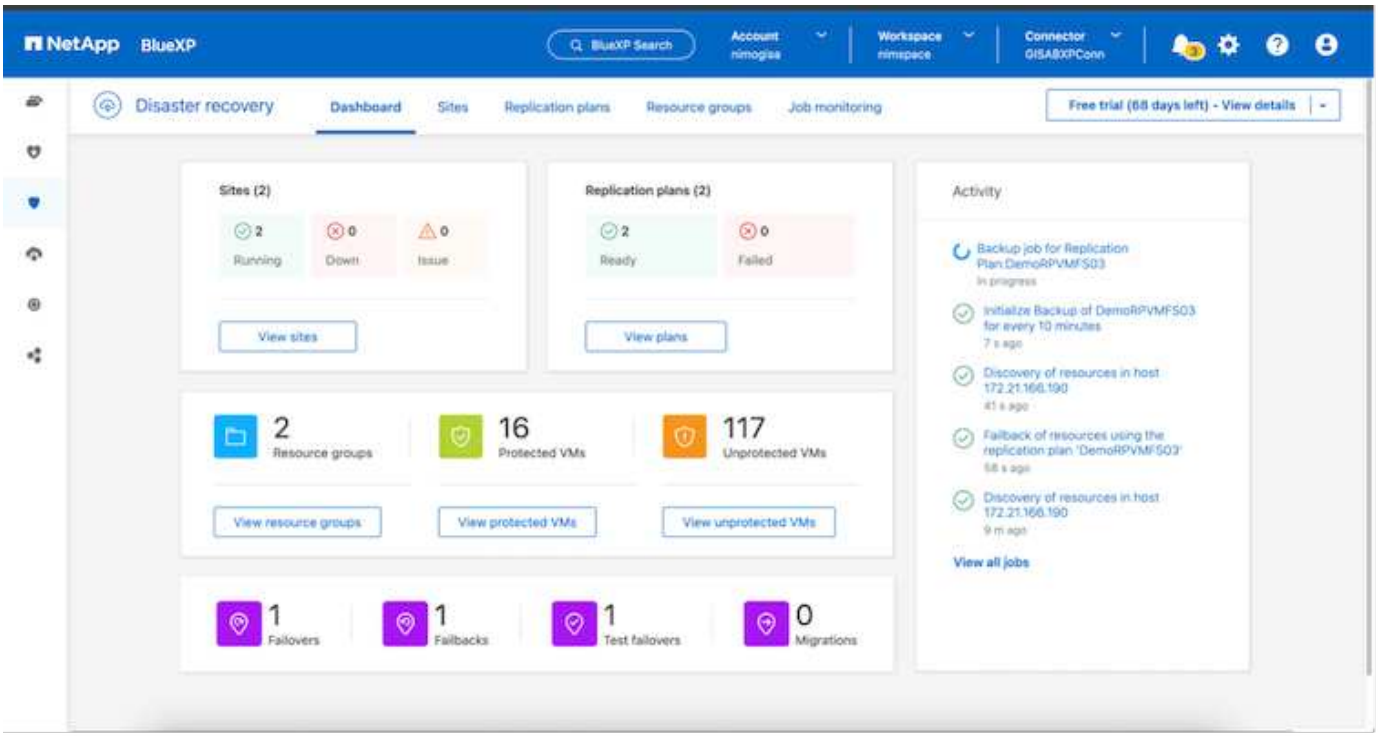


在配置災難復原計畫之前，請確保滿足以下先決條件：

- 控制台代理程式已部署在 AWS VPC 中。
- 控制台代理程式執行個體與來源和目的地 vCenter 及儲存系統具有連線能力。
- 為 VMware 託管 VMFS 資料存放區的內部部署 NetApp 儲存系統已新增至 Console。
- 使用 DNS 名稱時應該進行 DNS 解析。否則，請使用 vCenter 的 IP 位址。
- SnapMirror複製是為指定的基於 VMFS 的資料儲存磁碟區配置的。

一旦來源站點和目標站點之間建立連接，請繼續執行設定步驟，這大約需要 3 到 5 分鐘。

NetApp 建議將主控台代理程式部署在災難恢復站台或第三個站台，以便主控台代理程式在實際中斷或自然災害期間，可以透過網路與來源和目的地資源進行通訊。

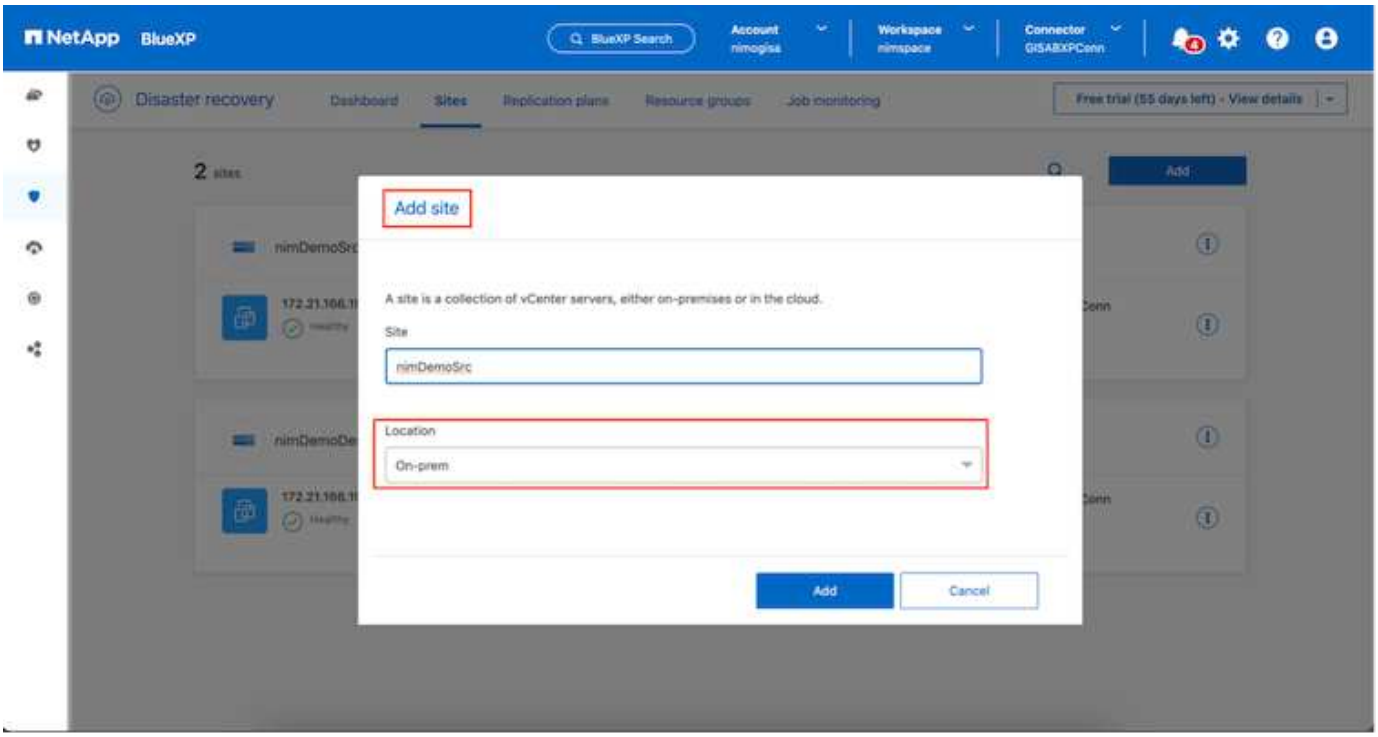


在撰寫本文檔時，對本地到本機 VMFS 資料儲存的支援處於技術預覽階段。基於 FC 和 ISCSI 協定的 VMFS 資料儲存均支援此功能。

災難恢復組態

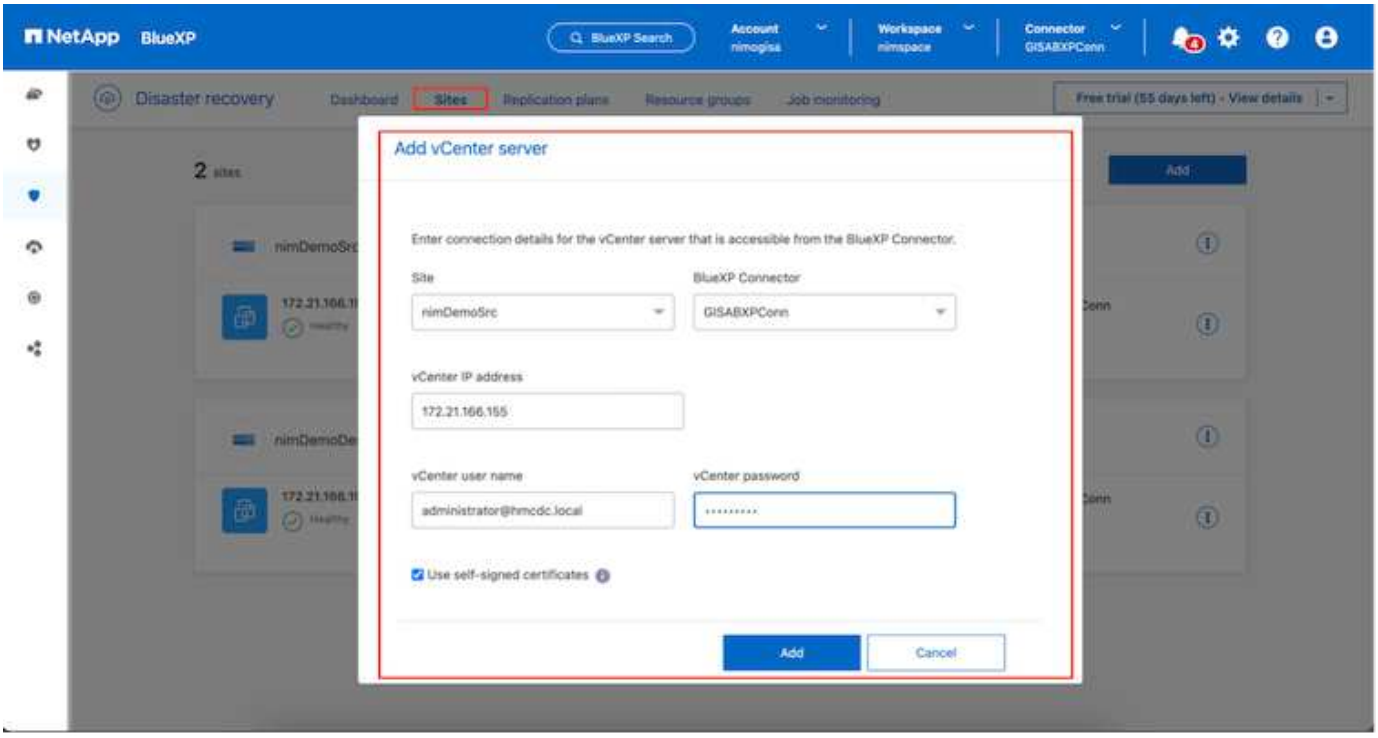
準備災難恢復的第一步是探索並將內部部署的 vCenter 和儲存資源新增至災難恢復。

確保已將 ONTAP 儲存系統新增至畫布中的工作環境。開啟主控台，並從左側導覽列選擇 保護 > 災難恢復。選擇 探索 **vCenter** 伺服器 或使用頂部選單，選擇 站台 > 新增 > 新增 **vCenter**。

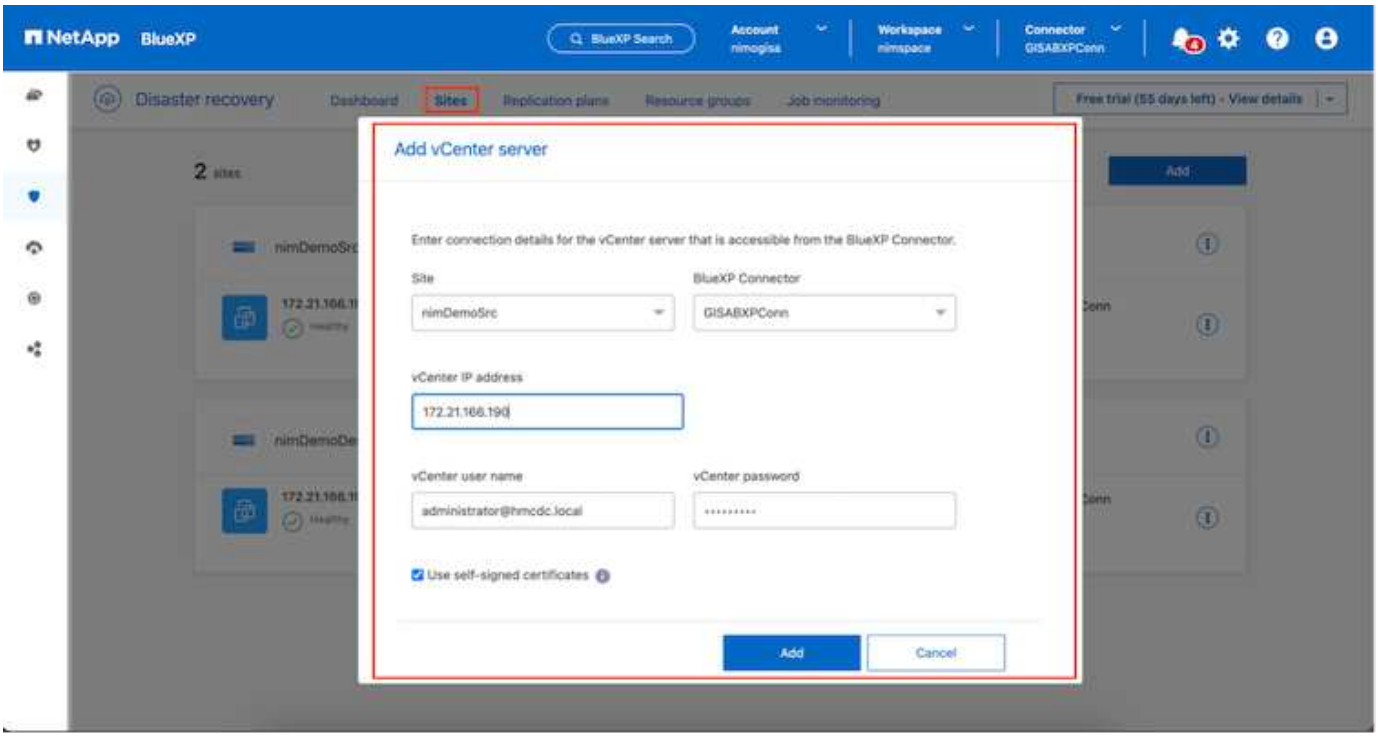


新增以下平台：

- 來源。本機 vCenter。



- 目的地。 VMC SDDC vCenter。



一旦新增了 vCenter，就會觸發自動發現。

配置來源站點和目標站點之間的儲存複製

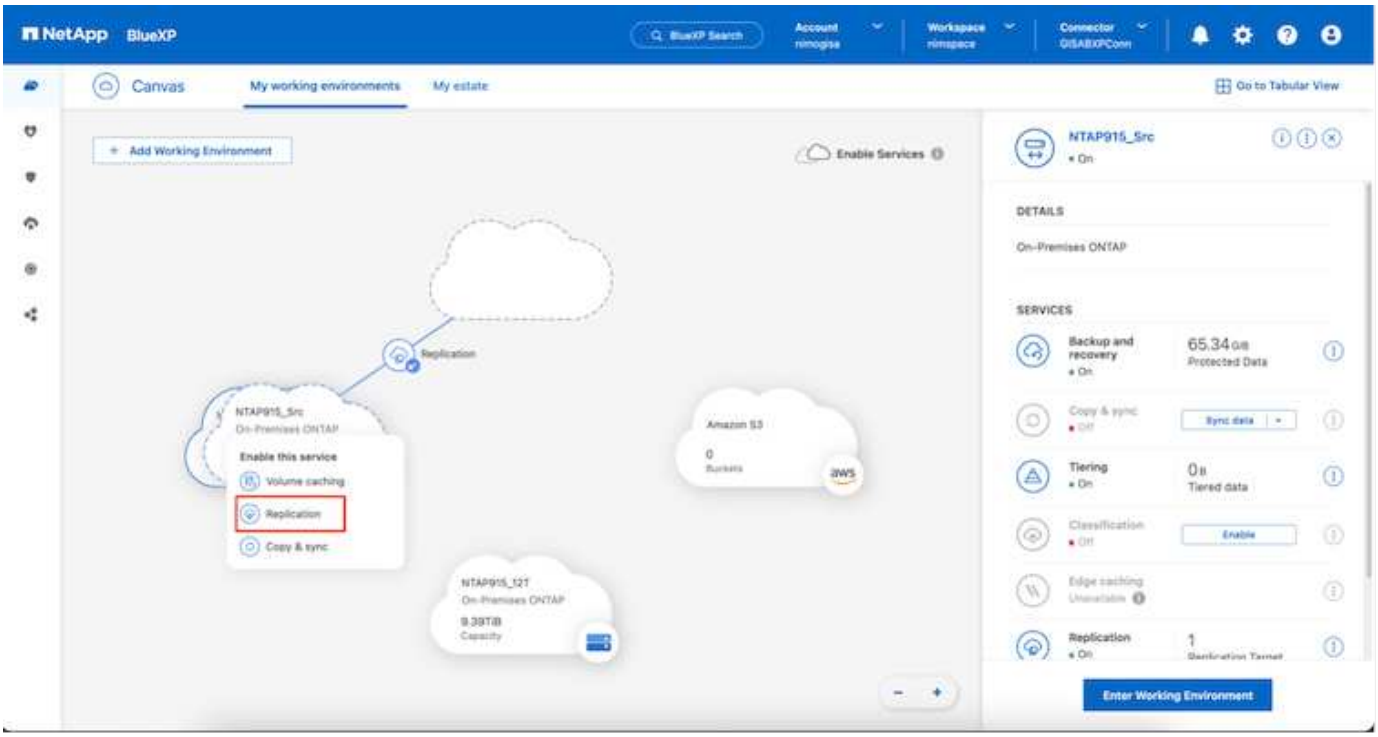
SnapMirror利用ONTAP快照來管理從一個位置到另一個位置的資料傳輸。首先，基於來源磁碟區快照的完整副本被複製到目標位置以執行基線同步。當來源處發生資料變更時，會建立一個新的快照並將其與基準快照進行比較。然後將發現已更改的區塊複製到目標位置，其中較新的快照成為當前基線或最新的公共快照。這使得該過程可以重複，並且可以將增量更新發送到目的地。

建立SnapMirror關係後，目標磁碟區處於線上唯讀狀態，因此仍可存取。 SnapMirror與實體儲存區塊一起工作，而不是在檔案或其他邏輯層級上工作。這意味著目標磁碟區是來源的相同副本，包括快照、磁碟區設定等。如果來源磁碟區正在使用ONTAP空間效率功能（例如資料壓縮和重複資料刪除），則複製的磁碟區將保留這些最佳化。

中斷SnapMirror關係會使目標磁碟區變得可寫，並且通常在使用SnapMirror將資料同步到 DR 環境時用於執行故障轉移。 SnapMirror足夠複雜，可以允許故障轉移網站上更改的資料有效地重新同步回主系統（如果主系統稍後恢復上線），然後允許重新建立原始的SnapMirror關係。

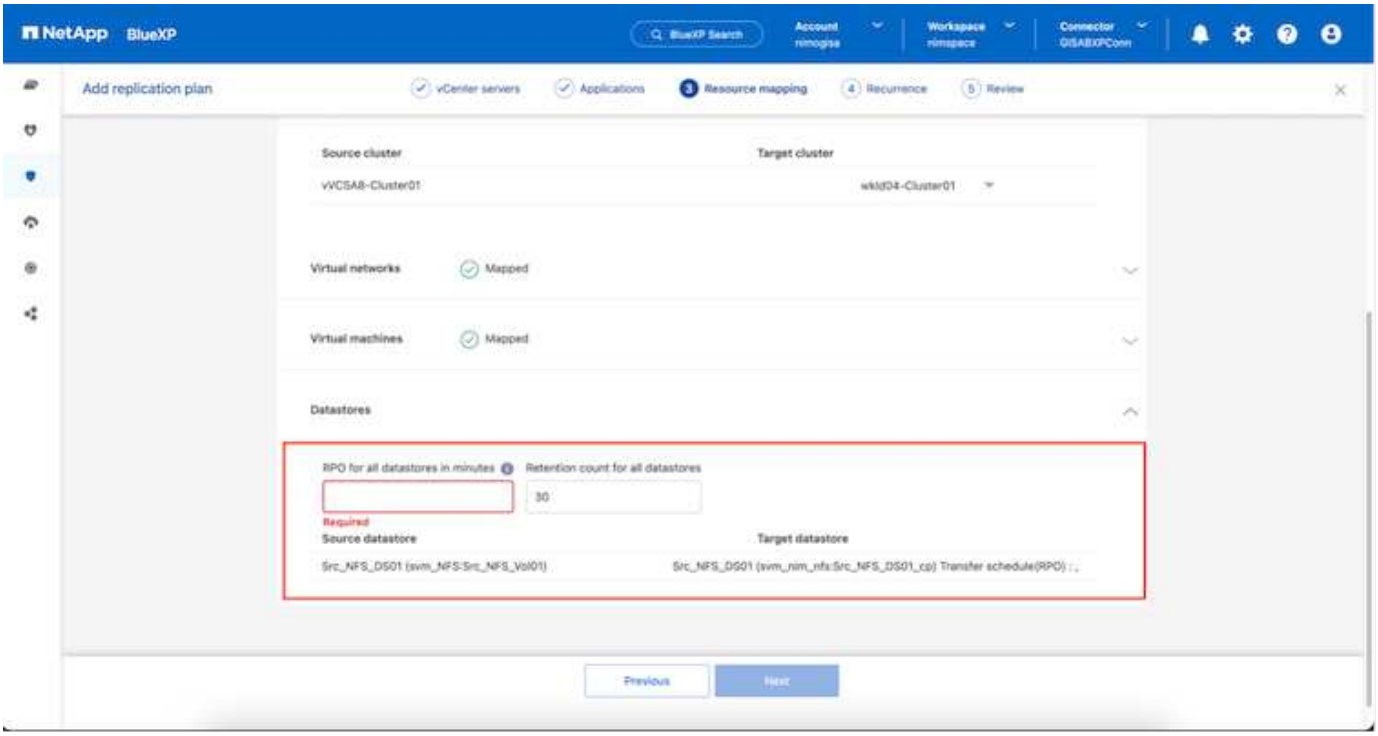
如何設定 **VMware** 災難復原

建立 SnapMirror 複寫的程序對於任何指定的應用程式皆相同。此程序可以是手冊或自動化。最簡單的方法是運用 Console 來設定 SnapMirror 複寫，只需將環境中的來源 ONTAP 系統拖放至目的地，即可觸發精靈來引導完成其餘程序。



NetApp Data Services 也可以自動化相同的作業，前提是符合下列兩個條件：

- 源集群和目標集群具有對等關係。
- 源 SVM 和目標 SVM 具有對等關係。

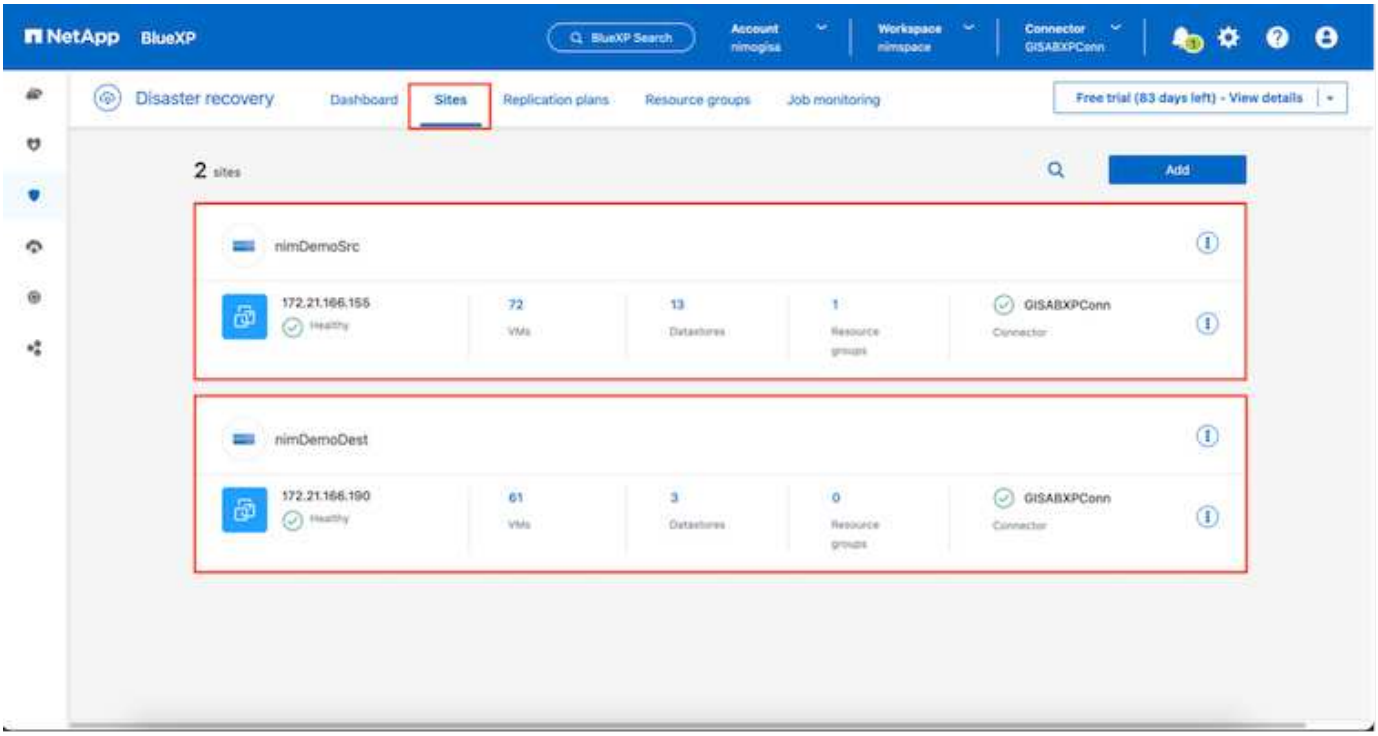


如果已透過 CLI 為 Volume 設定 SnapMirror 關係，Console 會取得該關係並繼續執行其餘的工作流程操作。

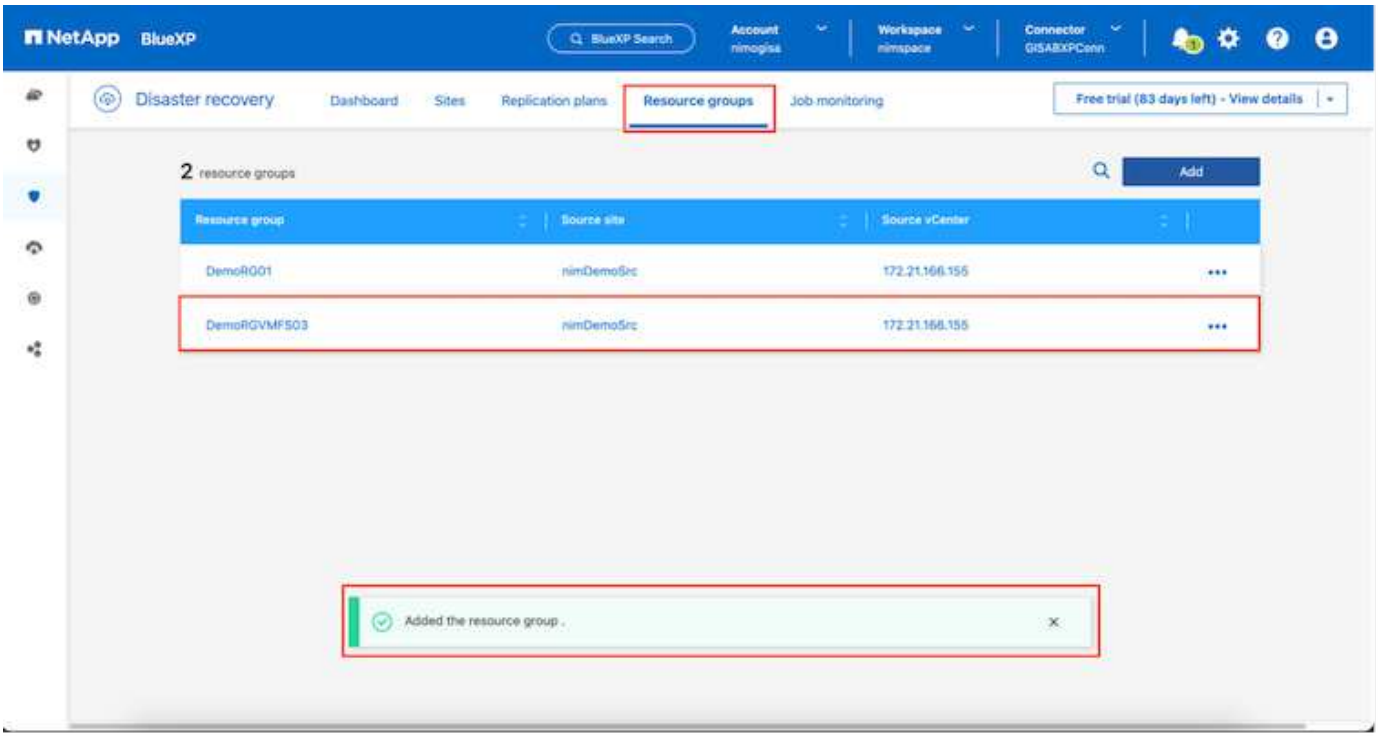
除了上述方法外，也可以透過 ONTAP CLI 或 System Manager 建立 SnapMirror 複寫。無論採用何種方法使用 SnapMirror 同步資料，災難恢復都會協調工作流程，以實現無縫且有效率的災難恢復作業。

災難恢復能為您帶來什麼好處？

新增來源和目的地站台後，災難恢復會自動執行深度探索，並顯示虛擬機器及其關聯的中繼資料。災難恢復也會自動偵測虛擬機器使用的網路和連接埠群組，並將其填入。

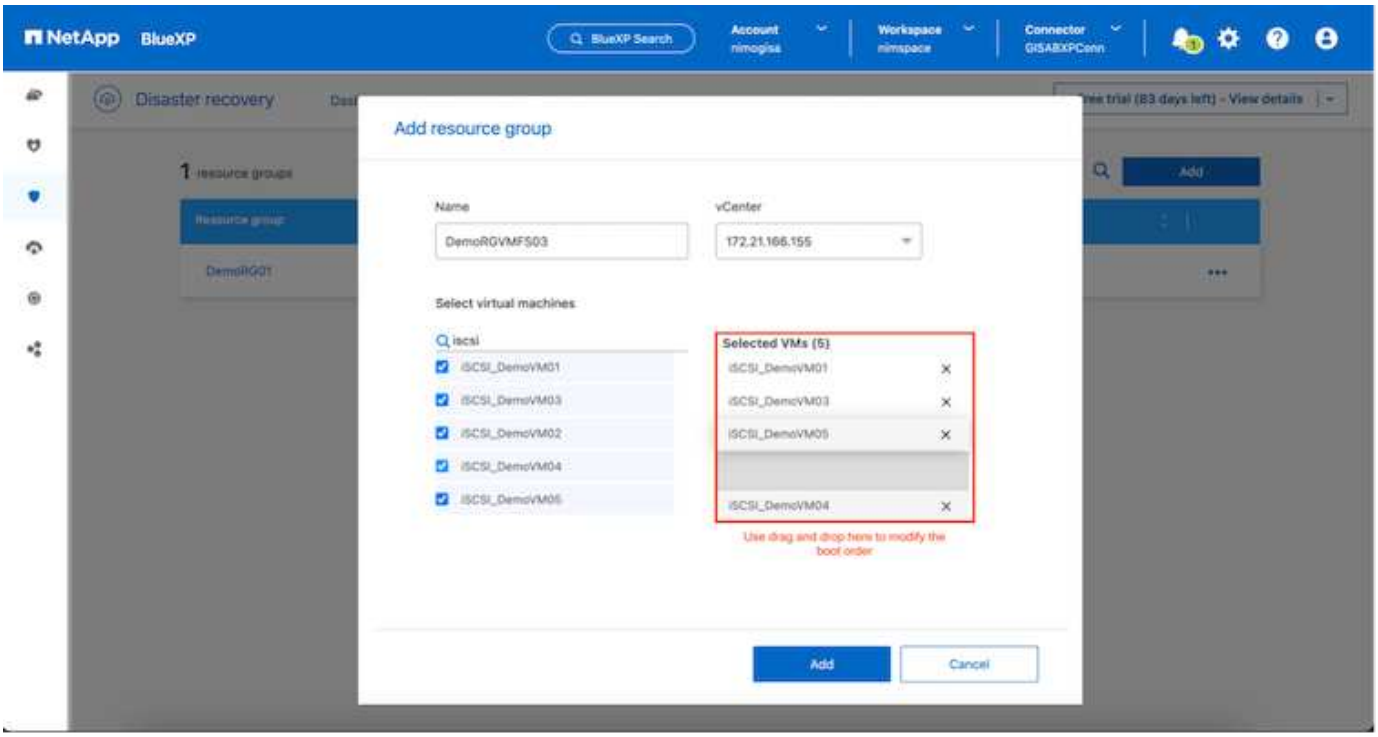


新增站台後，即可將虛擬機器分組到資源群組。災難恢復資源群組可讓您將一組相依的虛擬機器分組到邏輯群組中，這些邏輯群組包含其開機順序和開機延遲，以便在恢復時執行。若要開始建立資源群組，請導覽至 資源群組 ，然後按一下 建立新資源群組 。

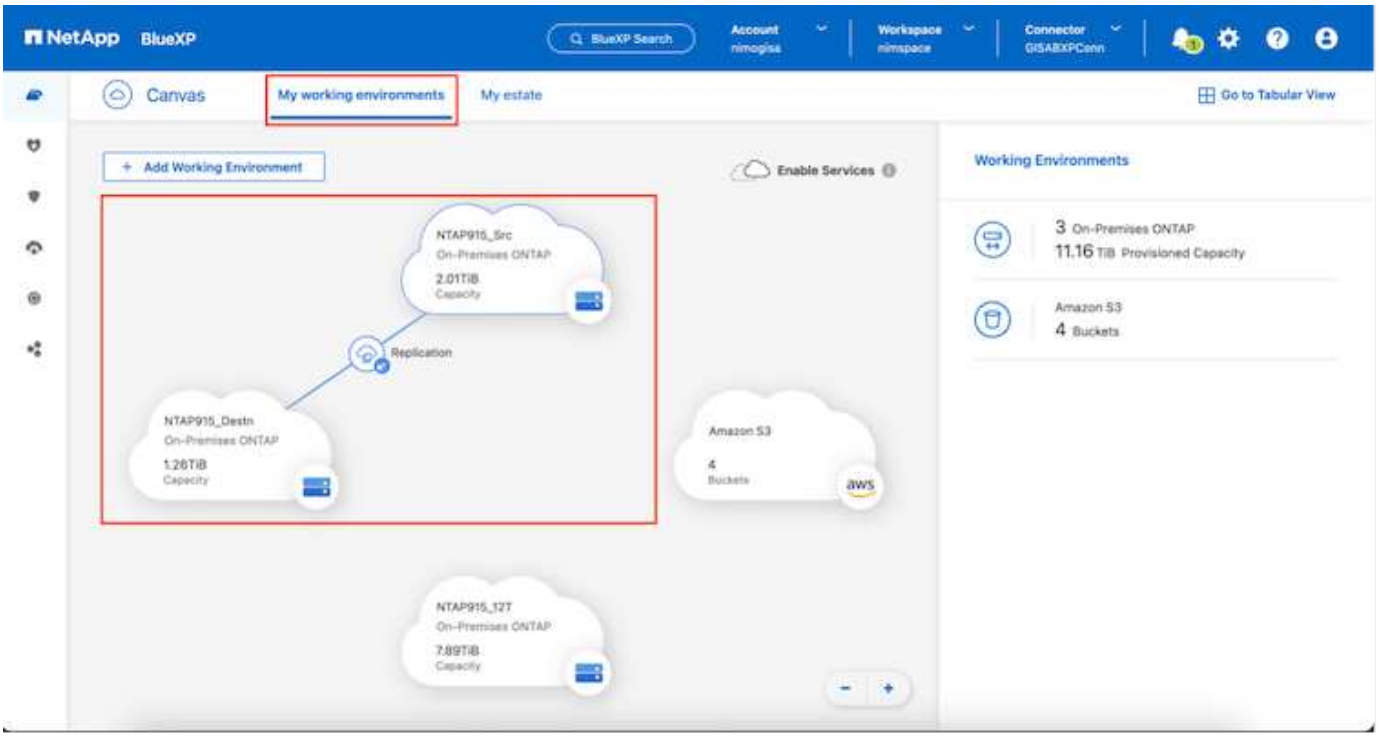


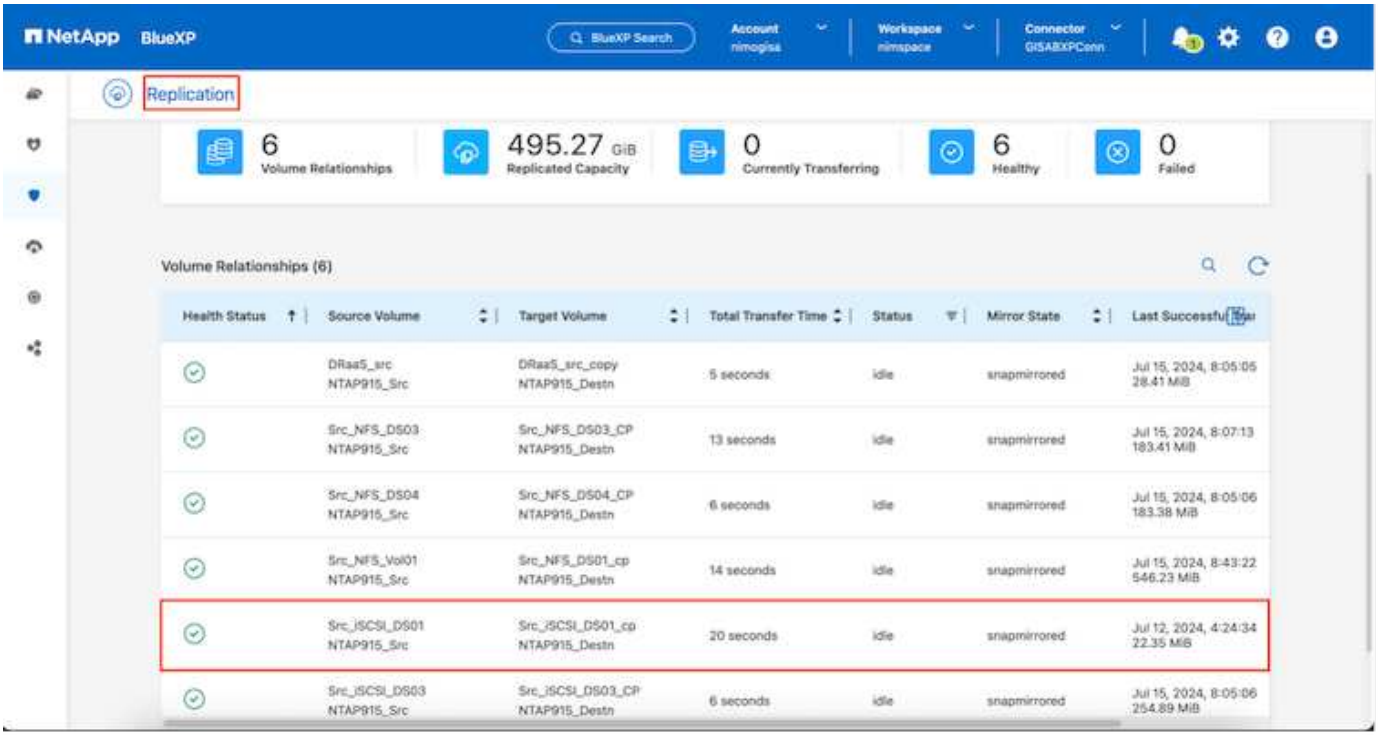
在建立複製計劃時也可以建立資源組。

可以透過簡單的拖放機制在建立資源群組期間定義或修改虛擬機器的啟動順序。



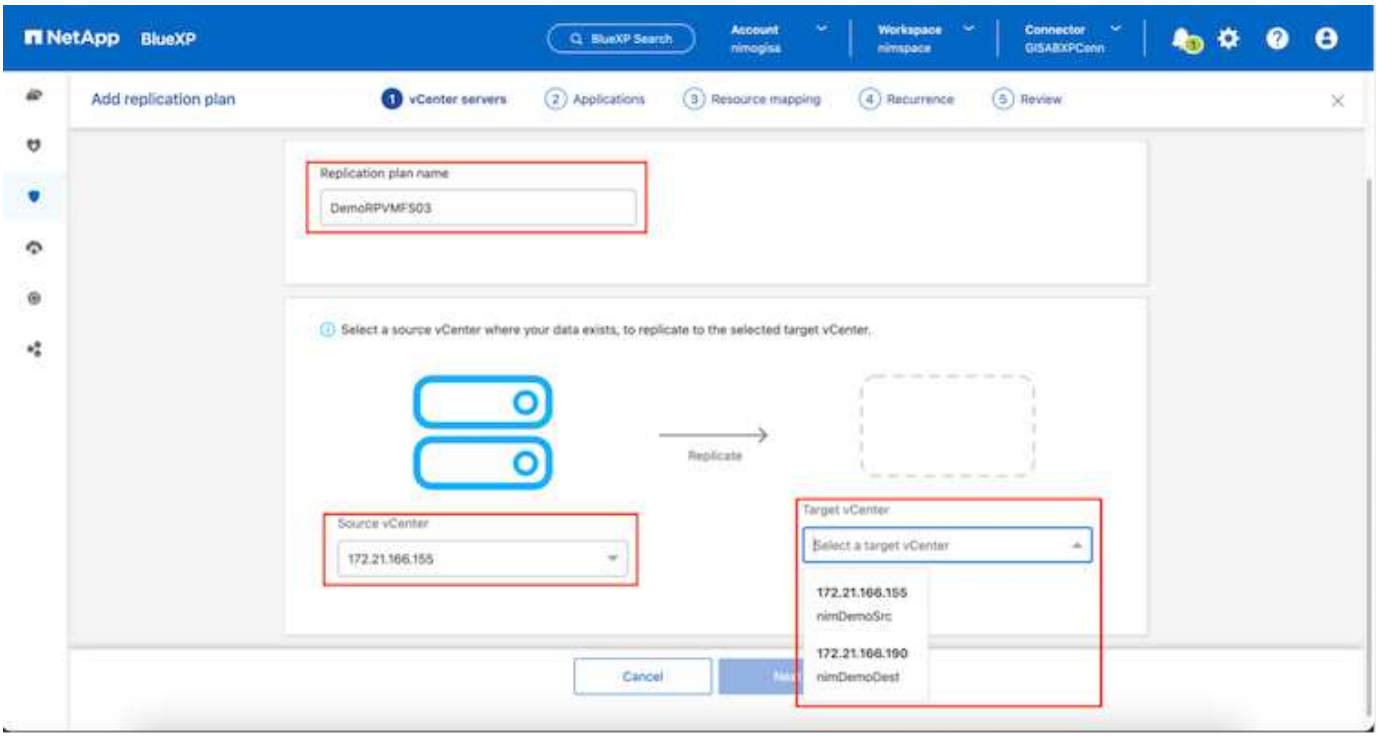
建立資源群組後，下一步是建立執行藍圖或在災難發生時復原虛擬機器和應用程式的計畫。如先決條件中所述，可以預先配置SnapMirror複製，或者 DRaaS 可以使用在建立複製計劃期間指定的 RPO 和保留計數來配置它。



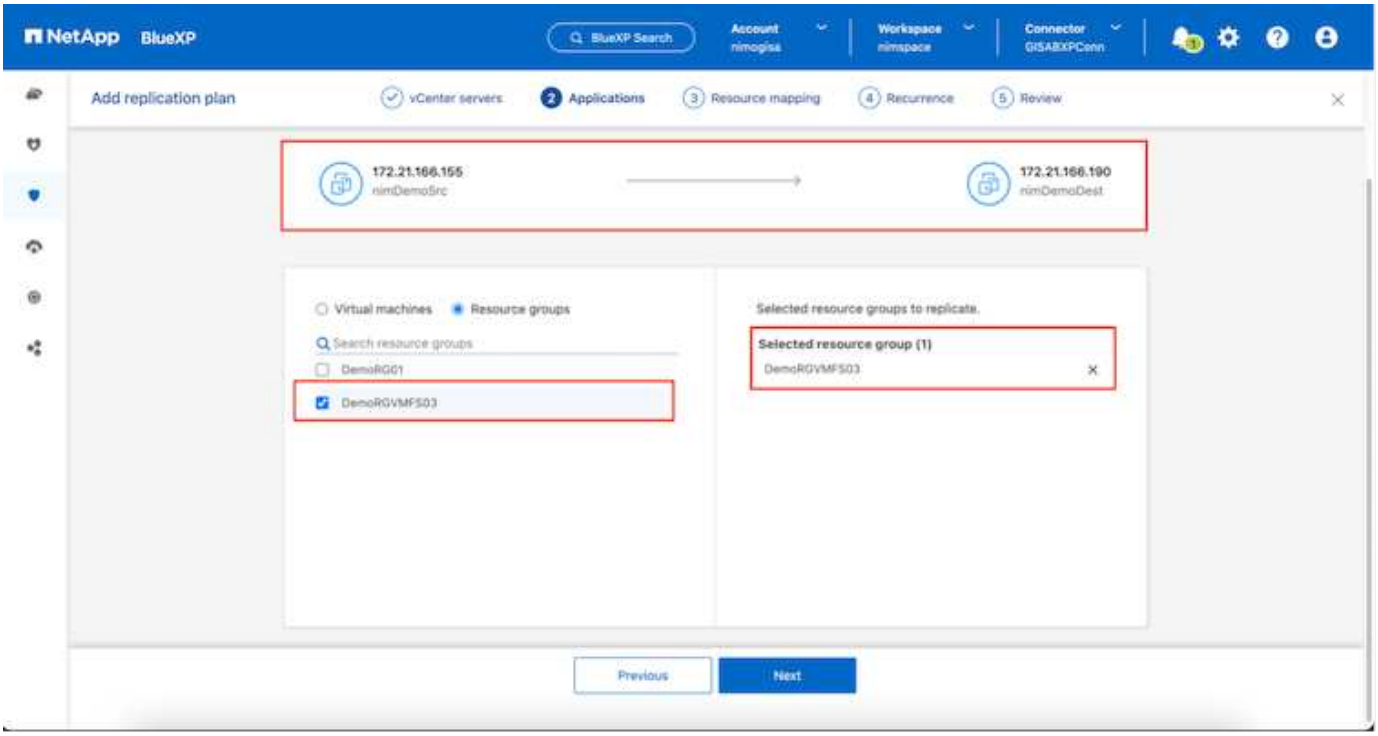


透過從下拉式選單中選擇來源和目標 vCenter 平台來設定複製計劃，並選擇要包含在計劃中的資源群組，以及如何復原和啟動應用程式的分組以及叢集和網路的對應。若要定義復原計劃，請導覽至「複製計劃」標籤並按一下「新增計劃」。

首先，選擇來源 vCenter，然後選擇目標 vCenter。



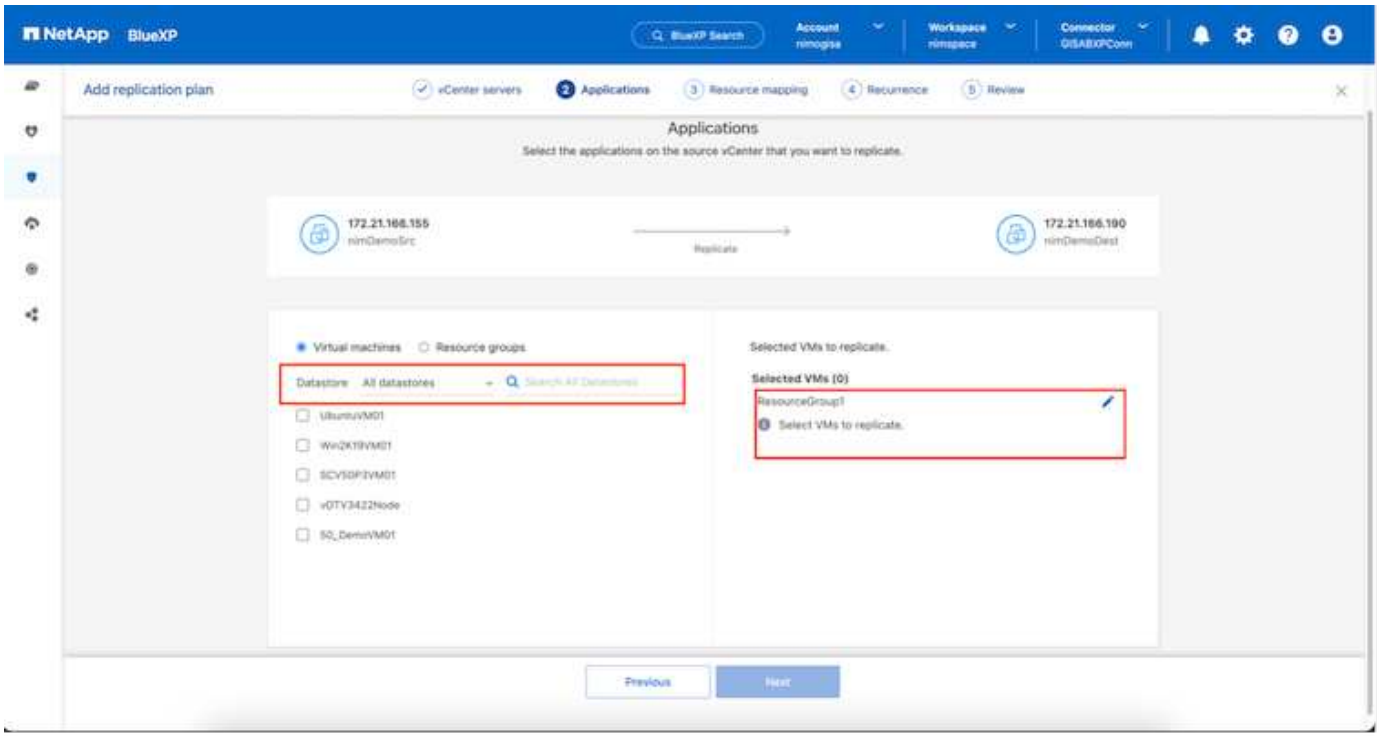
下一步是選擇現有的資源組。如果沒有建立資源組，則精靈將協助根據復原目標對所需的虛擬機器進行分組（基本上建立功能資源組）。這也有助於定義如何恢復應用程式虛擬機器的操作順序。



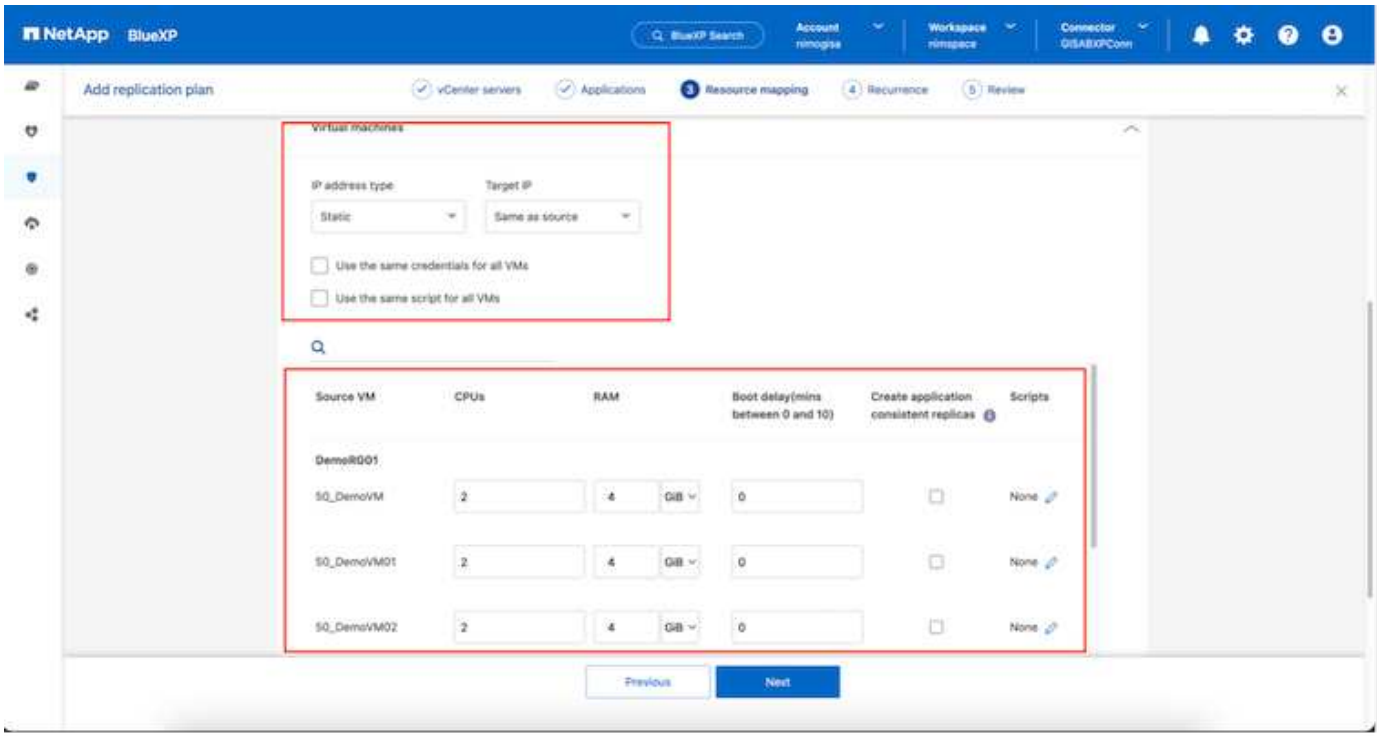
資源組允許使用拖放功能設定啟動順序。它可用於輕鬆修改復原過程中虛擬機器的啟動順序。

資源組內的各個虛擬機器依序依序啟動。兩個資源組並行啟動。

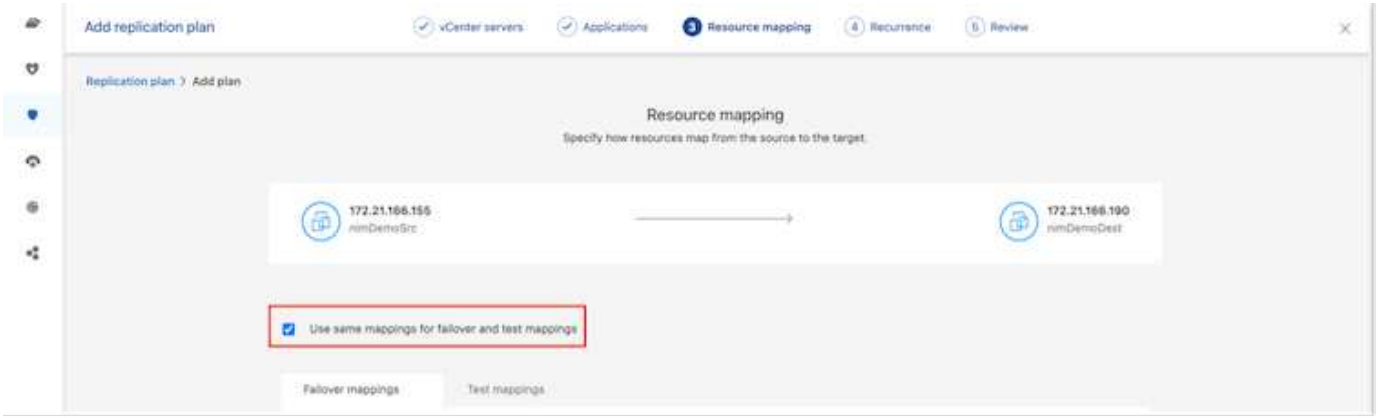
如果未事先建立資源群組，則下列螢幕截圖顯示了根據組織要求過濾虛擬機器或特定資料儲存的選項。



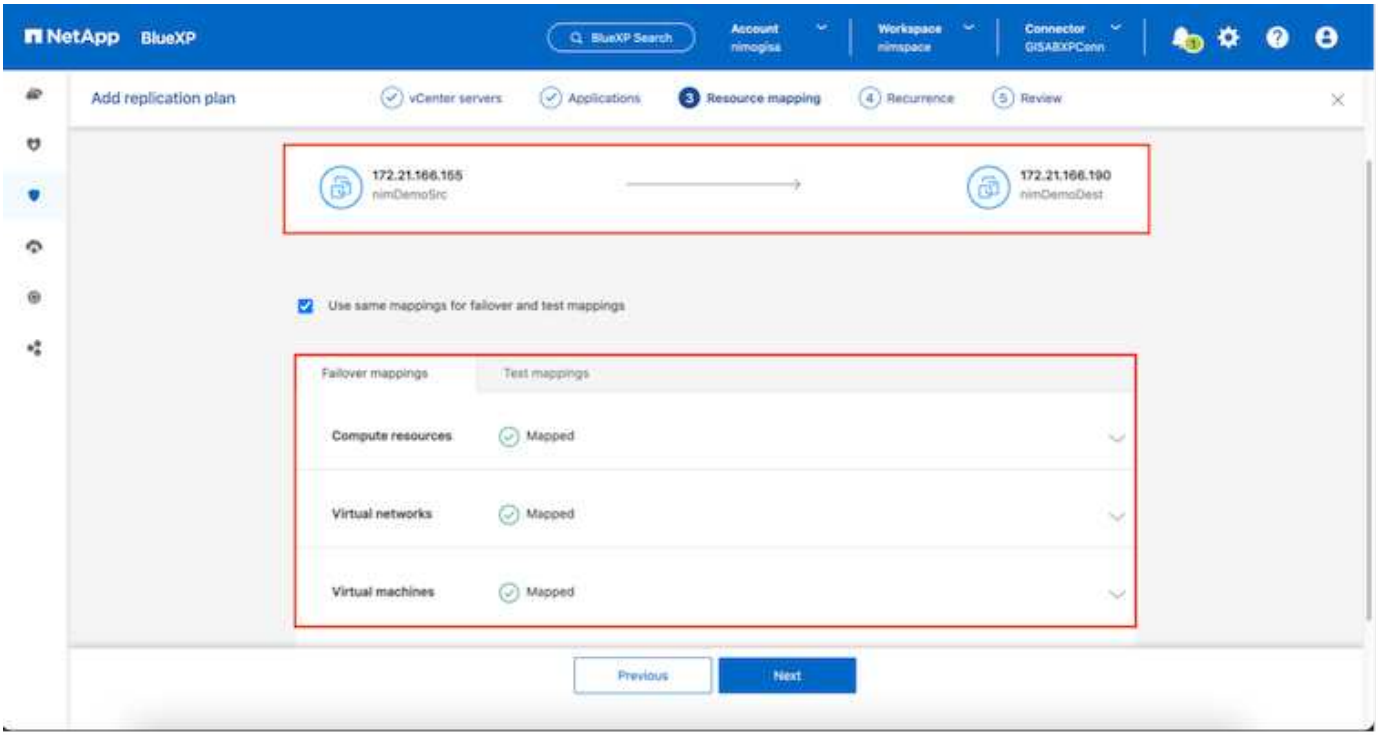
選取資源群組後，請建立容錯移轉對應。在此步驟中，請指定來源環境中的資源如何對應至目的地。這包括運算資源、虛擬網路。IP 自訂、前置與後置指令碼、開機延遲、應用程式一致性等。如需詳細資訊，請參閱 "建立複製計劃"。



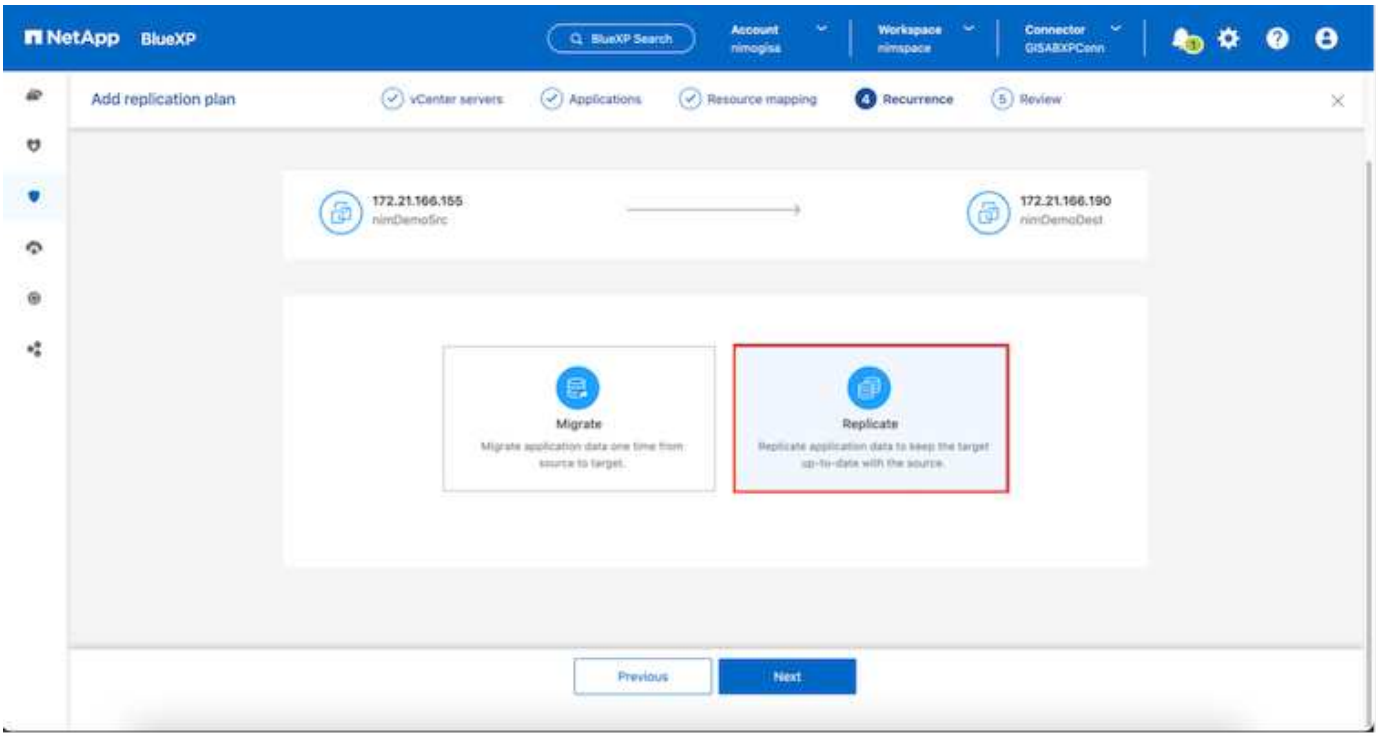
預設情況下，測試和故障轉移操作使用相同的映射參數。若要對測試環境套用不同的映射，請取消選取複選框後選擇測試映射選項，如下所示：



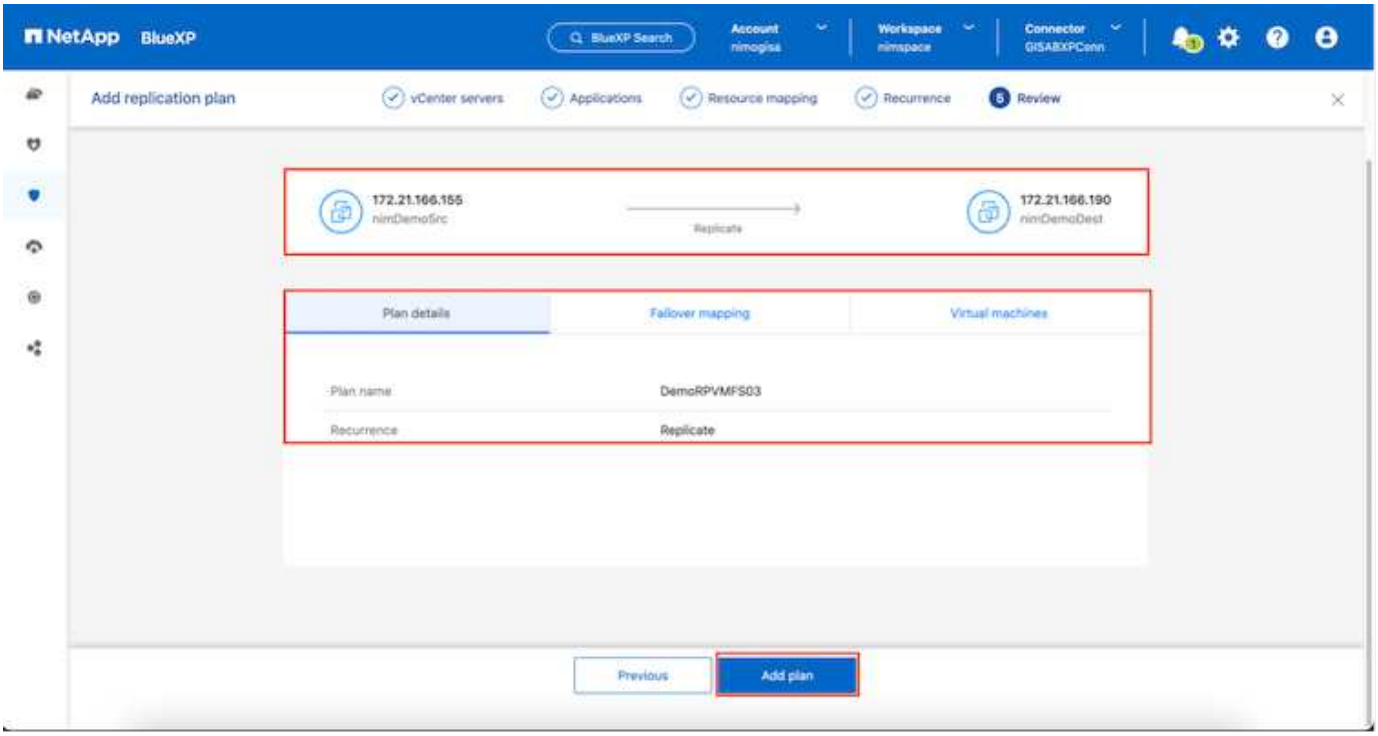
資源映射完成後，按一下下一步。

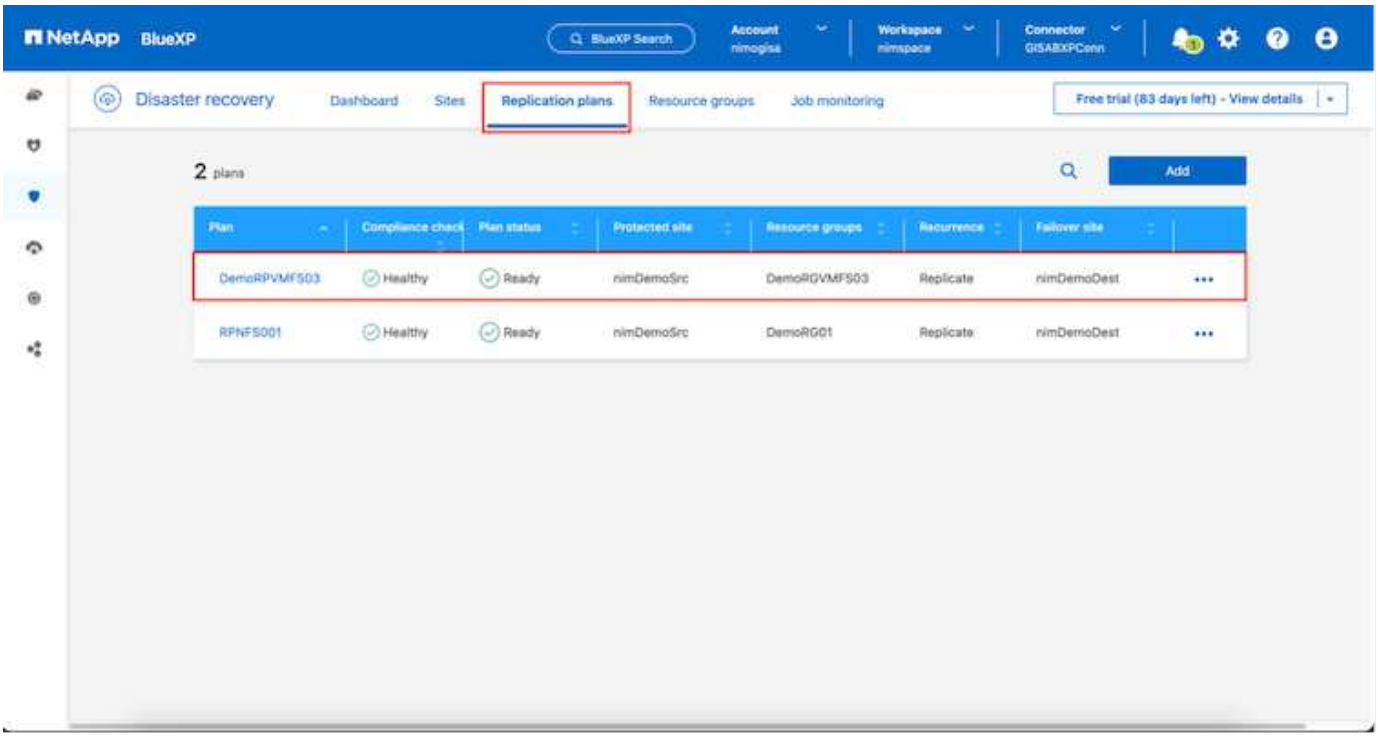


選擇重複類型。簡單來說，選擇遷移（使用故障轉移的一次性遷移）或重複連續複製選項。在本演練中，選擇了「複製」選項。

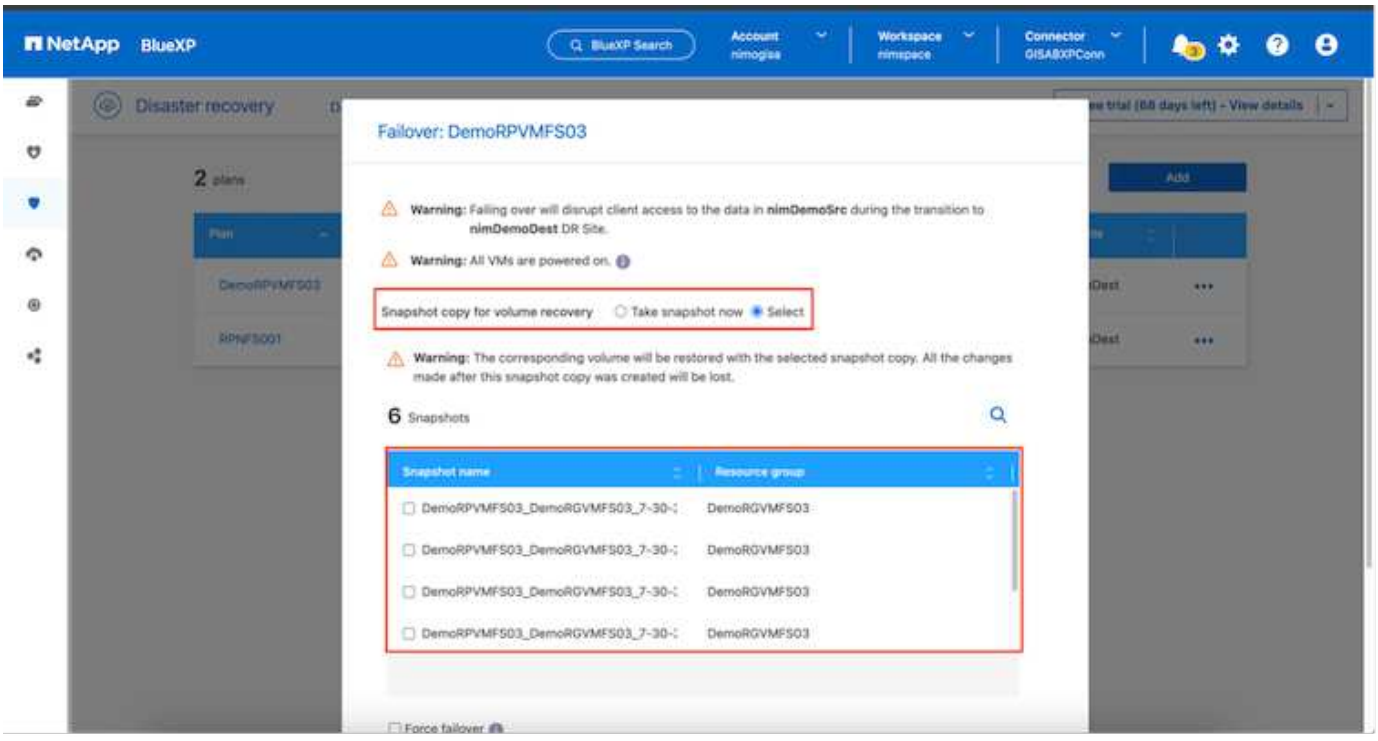


完成後，檢查建立的映射，然後按一下新增計劃。

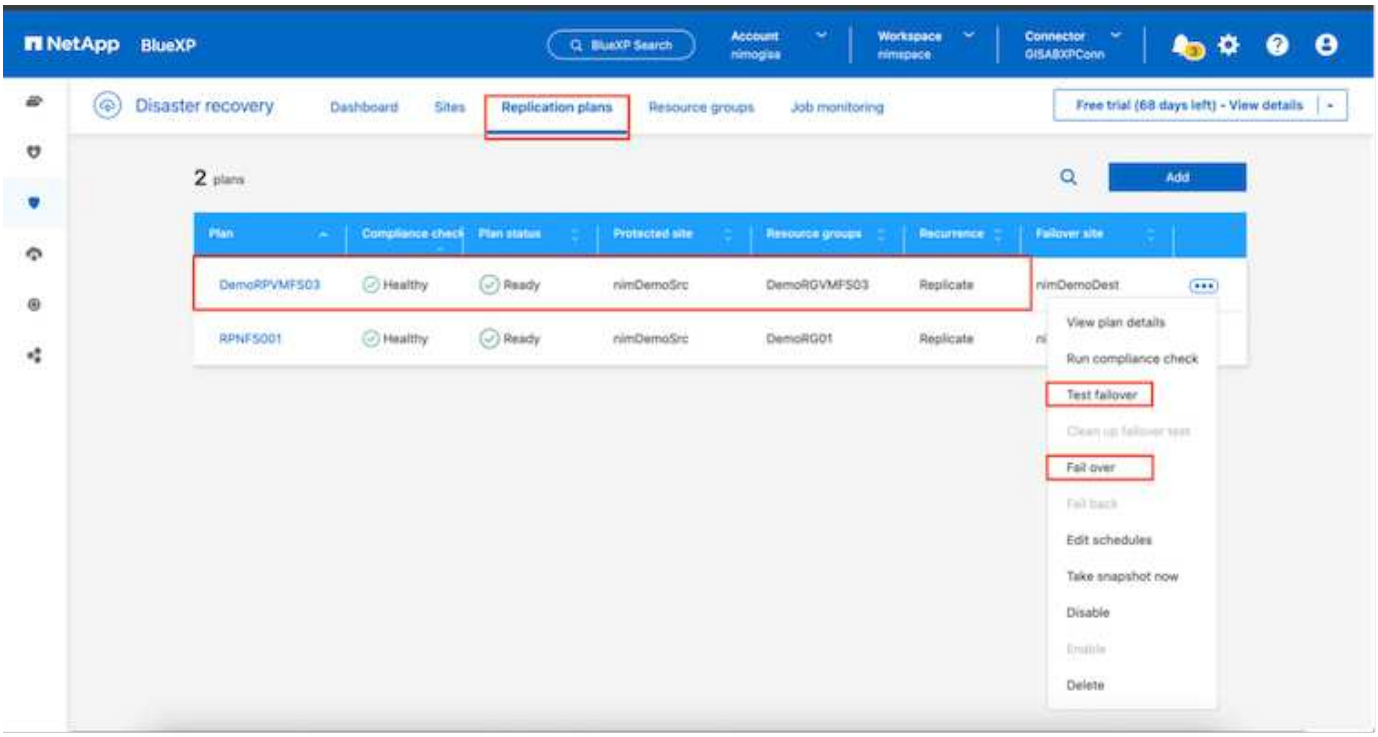




建立複寫計畫後，可以根據需求選擇容錯移轉選項、測試容錯移轉選項或移轉選項來執行容錯移轉。災難恢復確保複寫程序每 30 分鐘按照計畫執行一次。在容錯移轉和測試容錯移轉選項期間，您可以使用最新的 SnapMirror Snapshot 複本，也可以從時間點 Snapshot 複本中選擇特定的 Snapshot 複本（根據 SnapMirror 的保留政策）。如果發生勒索軟體等毀損事件，導致最新的複本已被破壞或加密，時間點選項會非常有用。災難恢復會顯示所有可用的恢復點。



若要使用複製計畫中指定的配置觸發故障轉移或測試故障轉移，請按一下「故障轉移」或「測試故障轉移」。

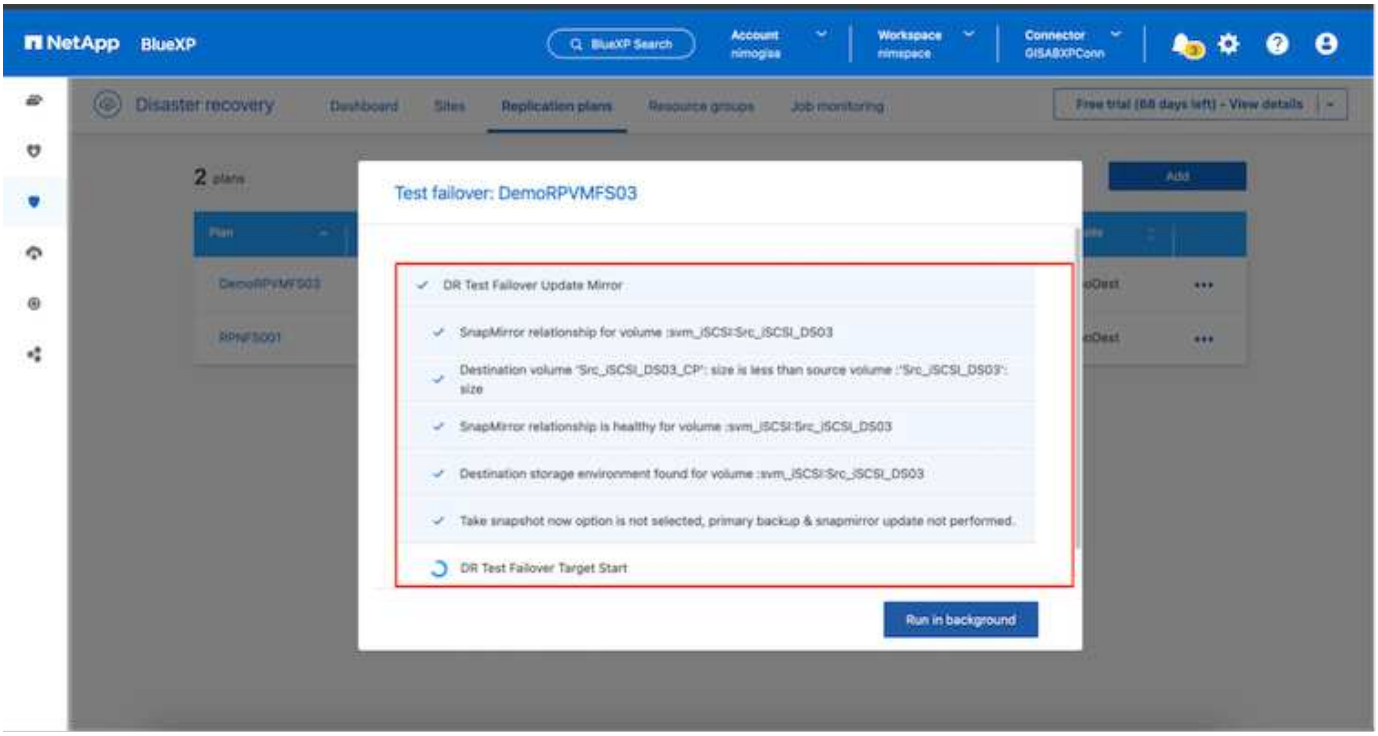


故障轉移或測試故障轉移操作期間會發生什麼？

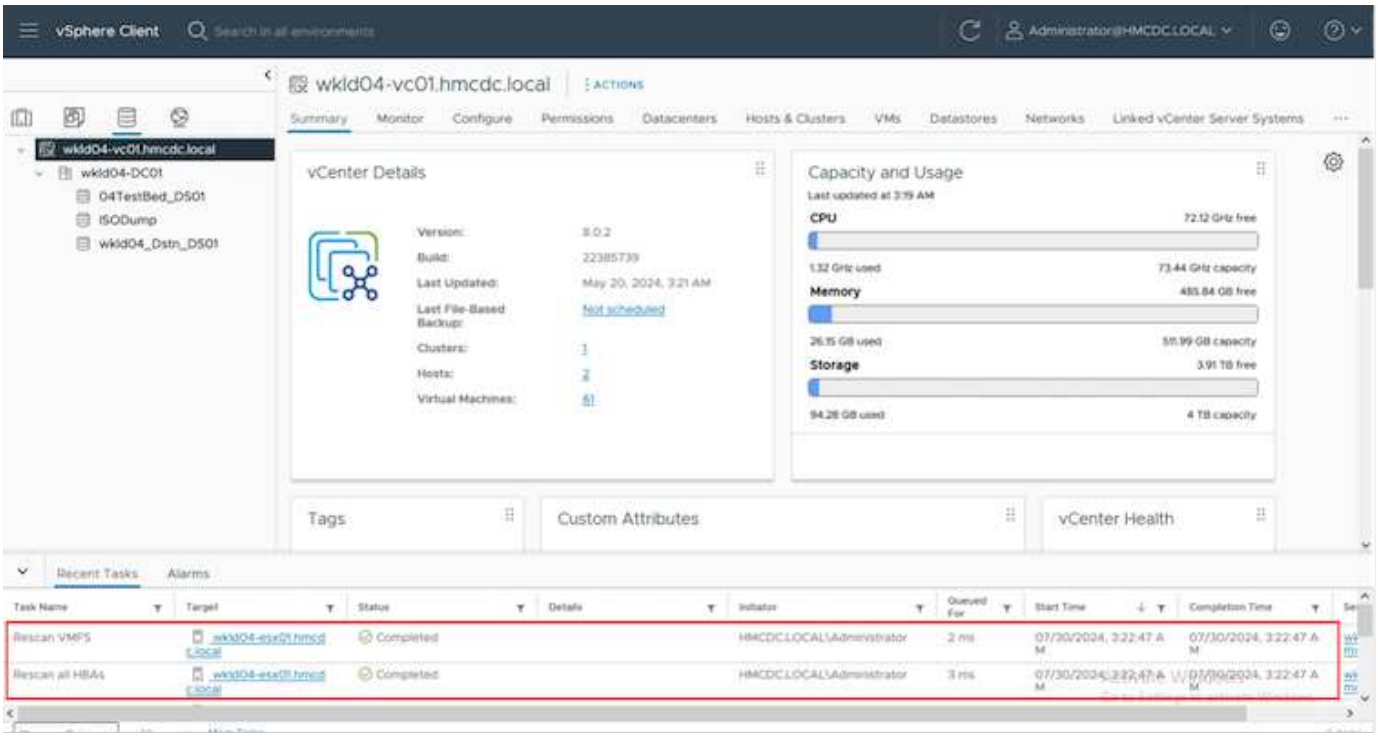
在測試容錯移轉作業期間，災難恢復會使用目的地 Volume 的最新 Snapshot 複本或選定的快照，在目的地 ONTAP 儲存系統上建立 FlexClone Volume。

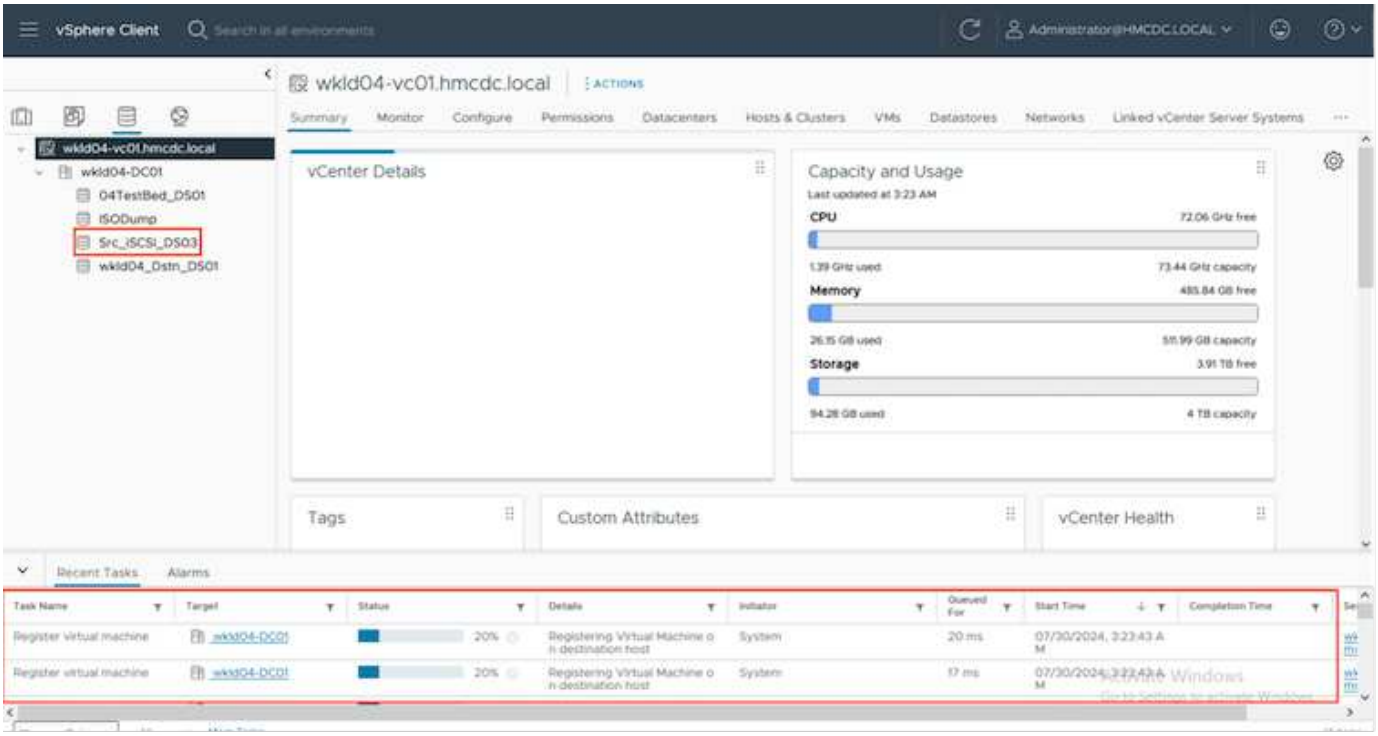
測試故障轉移操作會在目標ONTAP儲存系統上建立複製磁碟區。

執行測試恢復操作不會影響SnapMirror複製。



在此過程中，災難恢復不會對應原始目標 Volume。相反地，它會從選定的 Snapshot 快照技術建立一個新的 FlexClone Volume，並將支援該 FlexClone Volume 的暫存資料存放區對應至 ESXi 主機。



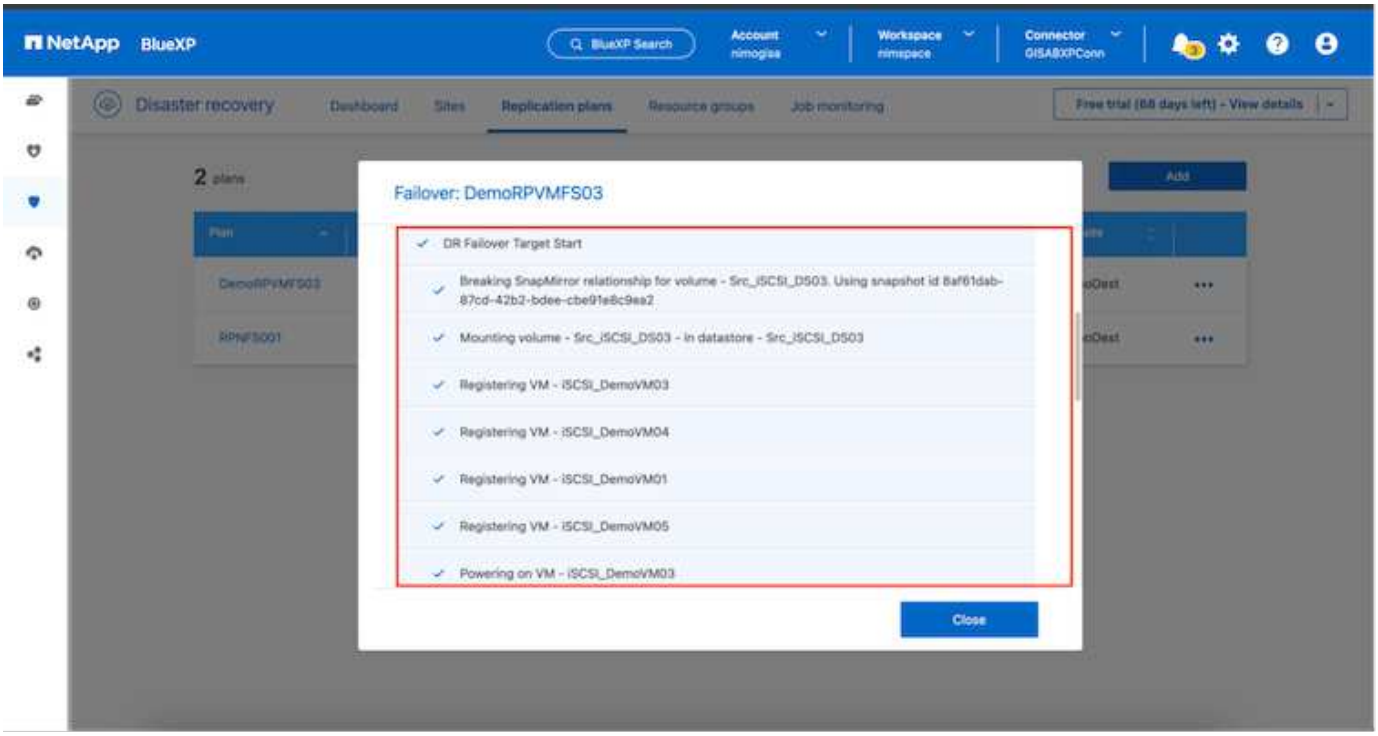


當測試容錯移轉作業完成時，可以使用 **"Clean Up failover test"** 觸發清理作業。在此作業期間，災難恢復會銷毀在作業中使用的 FlexClone Volume。

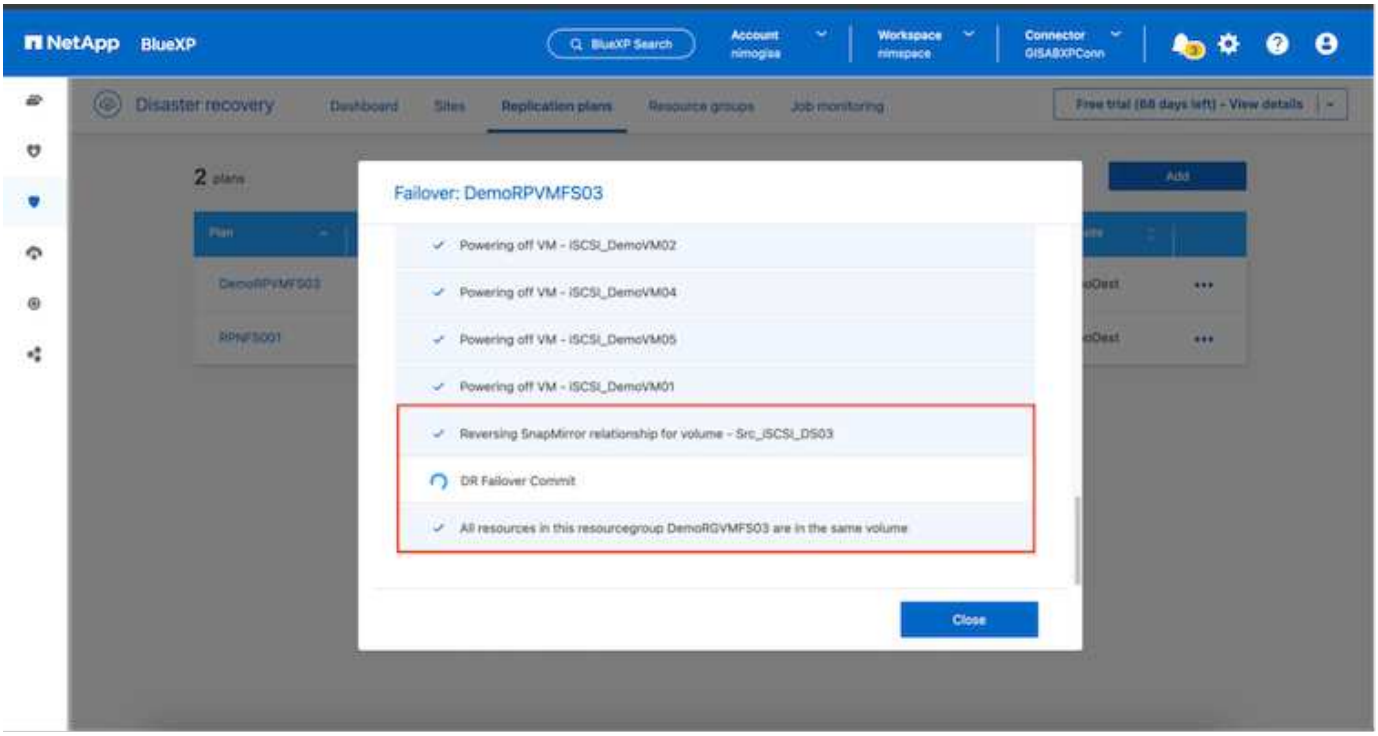
若發生真實的災難事件，災難恢復會執行下列步驟：

1. 中斷站點之間的SnapMirror關係。

2. 重新簽署後掛載 VMFS 資料儲存磁碟區以供立即使用。
3. 註冊虛擬機
4. 啟動虛擬機



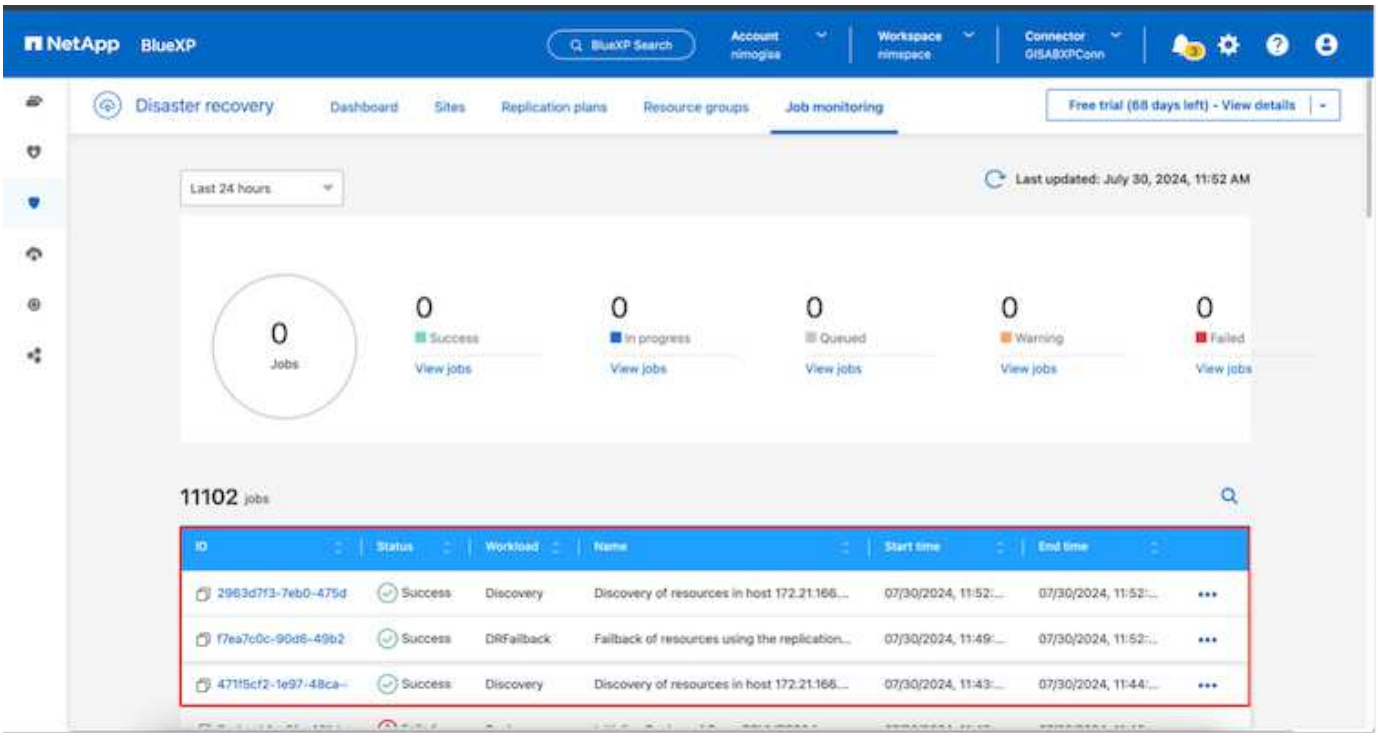
主站台啟動並運作後，災難恢復可為 SnapMirror 啟用反向重新同步並啟用容錯回復，同樣只需按一下按鈕即可執行。



如果選擇遷移選項，則它將被視為計劃內的故障轉移事件。在這種情況下，將觸發額外的步驟，即關閉來源站點

的虛擬機器。其餘步驟與故障轉移事件相同。

從 Console 或 ONTAP CLI，您可以監控適當資料存放區 Volume 的複寫健全狀況，並可透過作業監控來追蹤容錯移轉或測試容錯移轉的狀態。



這為處理量身定制的災難復原計劃提供了強大的解決方案。當發生災難並決定啟動 DR 站點時，可以按計劃進行故障轉移或單擊按鈕進行故障轉移。

要了解有關此過程的更多信息，請隨意觀看詳細的演示視頻或使用"解決方案模擬器"。

NetApp混合多雲與 Red Hat OpenShift 容器工作負載

開始

適用於 **Red Hat OpenShift** 容器工作負載的**NetApp**混合多雲解決方案

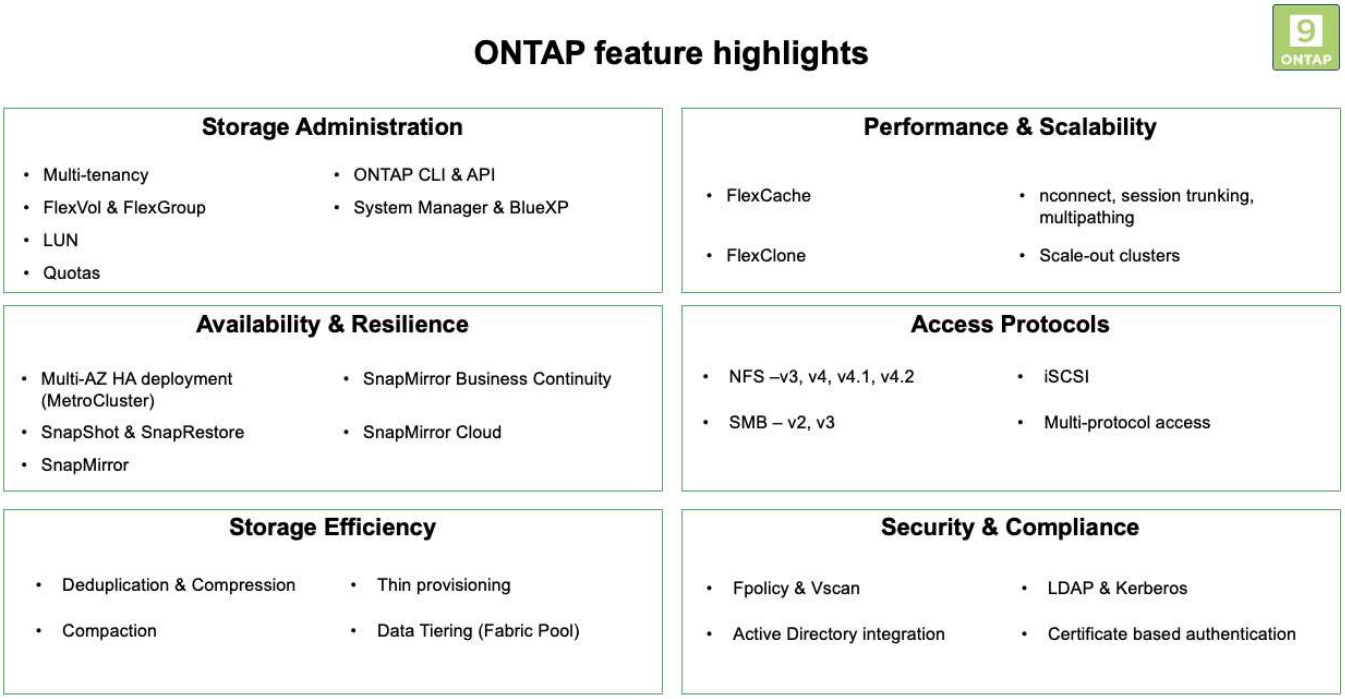
NetApp發現，越來越多的客戶正在對其傳統企業應用程式進行現代化改造，並使用圍繞 Kubernetes 構建的容器和編排平台來建立新的應用程式。 Red Hat OpenShift Container Platform 就是我們看到許多客戶採用的一個例子。

概況

隨著越來越多的客戶開始在其企業內採用容器， NetApp完全有能力幫助滿足其有狀態應用程式的持久儲存需求以及資料保護、資料安全和資料遷移等經典資料管理需求。然而，這些需求可以透過不同的策略、工具和方法來滿足。

以下列出的基於 **NetApp ONTAP** 的儲存選項為容器和 Kubernetes 部署提供安全性、資料保護、可靠性和靈活性。

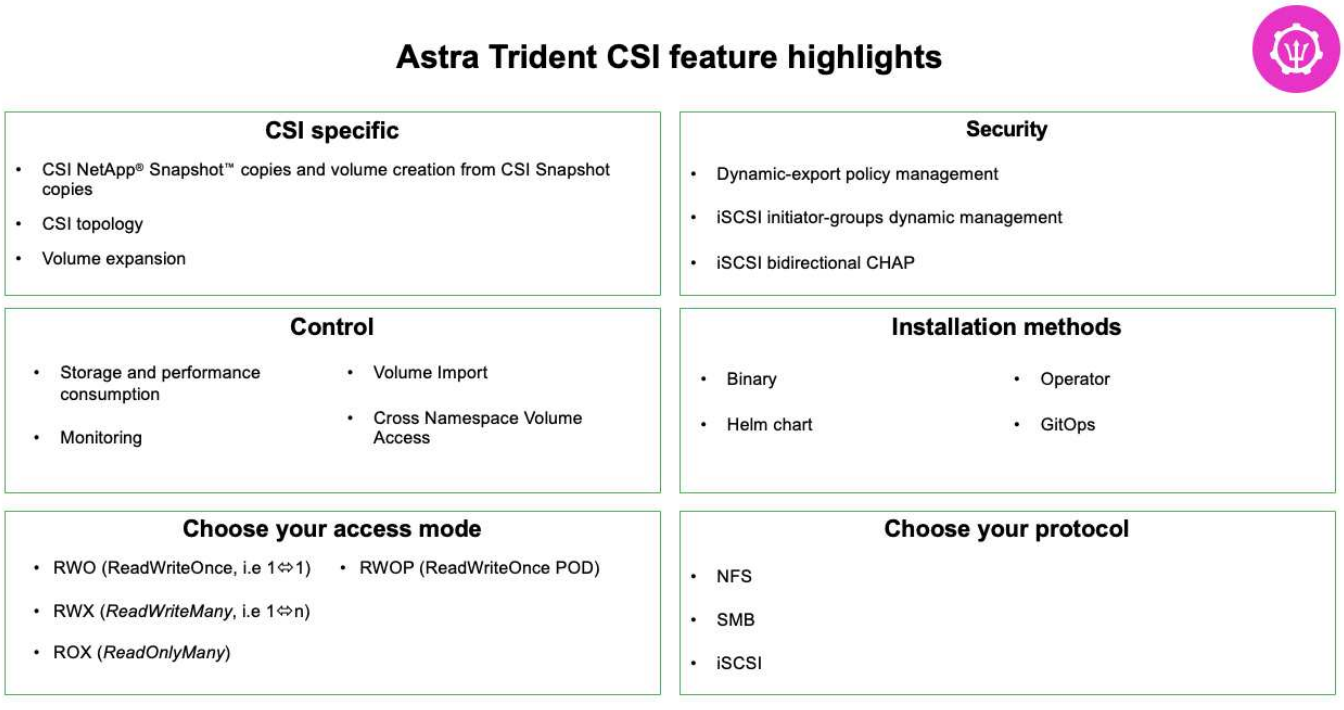
- 本地自我管理儲存：
  - NetApp光纖連接儲存 (FAS)、 NetApp全快閃FAS陣列 (AFF)、 NetApp全 SAN 陣列 (ASA) 和ONTAP Select
- 本機提供者管理的儲存：
  - NetApp Keystone提供儲存即服務 (STaaS)
- 雲端自我管理儲存：
  - NetApp Cloud Volumes ONTAP（CVO）在超大規模資料中心中提供自管理儲存
- 雲端中的提供者管理儲存：
  - Amazon FSx for NetApp ONTAP、 Azure NetApp Files和Google Cloud NetApp Volumes在雲端提供基於檔案的儲存。



NetApp Console 可讓您透過單一控制平面/介面管理所有儲存設備和資料資產。

您可以使用 NetApp Console 建立和管理雲端儲存（例如 Cloud Volumes ONTAP 和 Azure NetApp Files），移動、保護和分析資料，以及控制許多內部部署和邊緣儲存設備。

- NetApp Trident** 是符合 CSI 標準的儲存編排器，可快速輕鬆地使用由上述各種NetApp儲存選項支援的持久性儲存。它是由NetApp維護和支援的開源軟體。



業務關鍵型容器工作負載需要的不僅僅是持久卷。他們的資料管理要求也需要保護和遷移應用程式 Kubernetes 物件。

應用程式資料除了使用者資料之外，還包括 kubernetes 對象：以下是一些範例： - kubernetes 對象，例如 pod 規範、PVC、部署、服務 - 自訂配置對象，例如配置映射和機密 - 持久性數據，例如 Snapshot 副本、備份、克隆 - 自訂資源，例如 CR 和 CRD

NetApp Trident Protect 是 NetApp Trident 的免費附加元件，提供進階應用程式資料管理功能，可增強由 NetApp ONTAP 儲存系統支援的有狀態 Kubernetes 應用程式的功能和可用性。Trident Protect 簡化了跨公有雲和內部部署環境的容器化工作負載的管理、保護和移動。它還透過其 API 和 CLI 提供強大的自動化功能。

此參考文件提供了使用Trident Protect 在 RedHat OpenShift 平台上部署的基於容器的應用程式的資料保護驗證。此外，該解決方案還提供了部署和使用 Red Hat Advanced Cluster Management (ACM) 管理容器平台的高階詳細資訊。該文件還重點介紹了使用Trident CSI 配置器將NetApp儲存與 Red Hat OpenShift 容器平台整合的細節。

NetApp混合多雲解決方案針對 Red Hat OpenShift 容器工作負載的價值主張

大多數客戶不會在沒有任何現有基礎設施的情況下開始建立基於 Kubernetes 的環境。也許他們是一家傳統的 IT 商店，在虛擬機器上運行大多數企業應用程式（例如在大型 VMware 環境中）。然後，他們開始建立基於小型容器的環境來滿足現代應用程式開發團隊的需求。這些措施通常從小處開始，隨著團隊學習這些新技術和技能並開始認識到採用它們的許多好處，它們開始變得更加普遍。對客戶來說，好消息是NetApp可以滿足這兩種環境的需求。這套採用 Red Hat OpenShift 的混合多雲解決方案將使NetApp客戶能夠採用現代雲端技術和服務，而無需徹底改造其整個基礎架構和組織。無論客戶應用程式和資料託管在本機、雲端、虛擬機器上運作或容器上， NetApp都能提供一致的資料管理、保護、安全性和可攜性。借助這些新解決方案， NetApp數十年來在本地資料中心環境中提供的相同價值將在整個企業資料範圍內提供，而無需進行大量投資來重新裝備、獲取新技能或組建新團隊。無論客戶處於雲端之旅的哪個階段， NetApp都能夠協助客戶解決這些業務挑戰。

NetApp混合多雲與 Red Hat Openshift：

- 為客戶提供經過驗證的設計和實踐，展示客戶在使用基於NetApp 的Red Hat OpenShift 儲存解決方案時管理、保護、保護和遷移其資料和應用程式的最佳方法。
- 為在 VMware 環境、裸機基礎架構或兩者結合中運行 Red Hat OpenShift 和NetApp儲存的客戶提供最佳實務。
- 展示本地和雲端環境以及兩者混合環境的策略和選項。

NetApp混合多雲支援 Red Hat OpenShift 容器工作負載的解決方案

此解決方案測試並驗證使用 OpenShift 容器平台 (OCP)、OpenShift 進階叢集管理員 (ACM)、NetApp ONTAP、NetApp Console 和 NetApp Trident Protect 進行的移轉與集中式資料保護。

對於此解決方案， NetApp已測試並驗證了以下場景。此解決方案根據以下特點分為多個場景：

- 本地
- 雲

- 自我管理的 OpenShift 叢集和自我管理的NetApp存儲
- 由供應商管理的 OpenShift 叢集和供應商管理的NetApp存儲

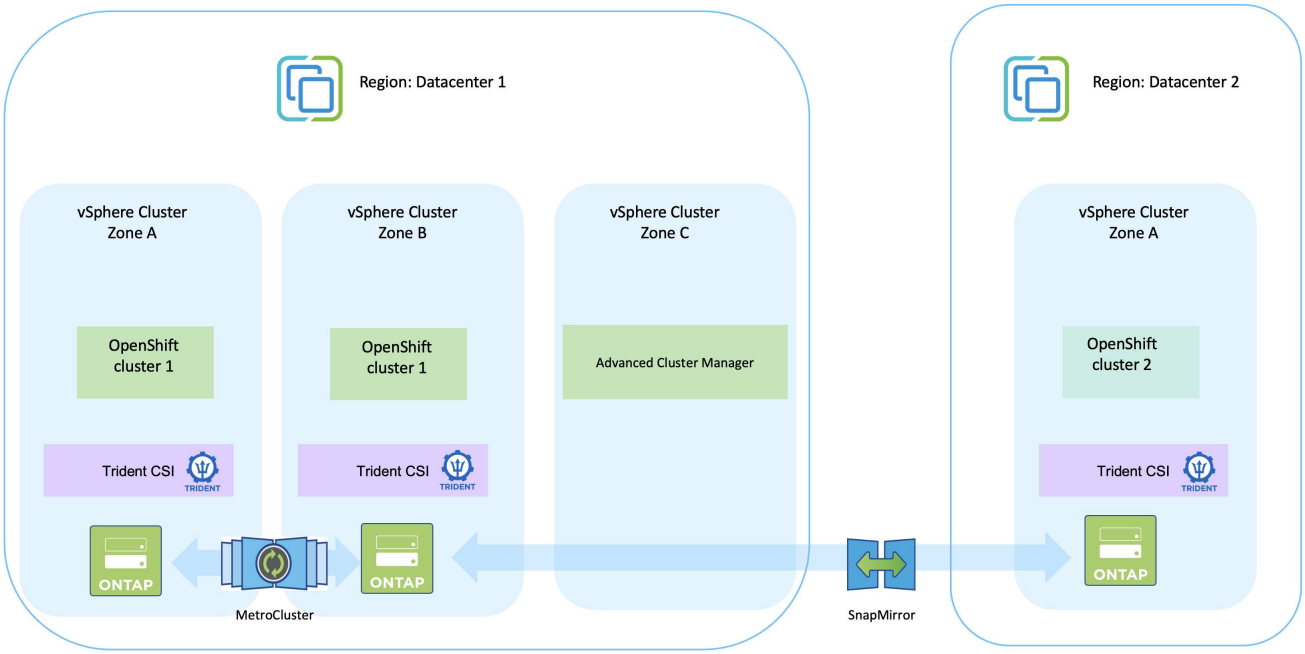
我們將在未來建立更多解決方案和用例。

情境 **1**：使用**Trident Protect** 在本機環境中進行資料保護和遷移

本地：自我管理的 **OpenShift** 叢集和自我管理的**NetApp**儲存

- 使用 Trident Protect 保護應用程式並支援內部部署叢集之間的遷移。

場景 **1**

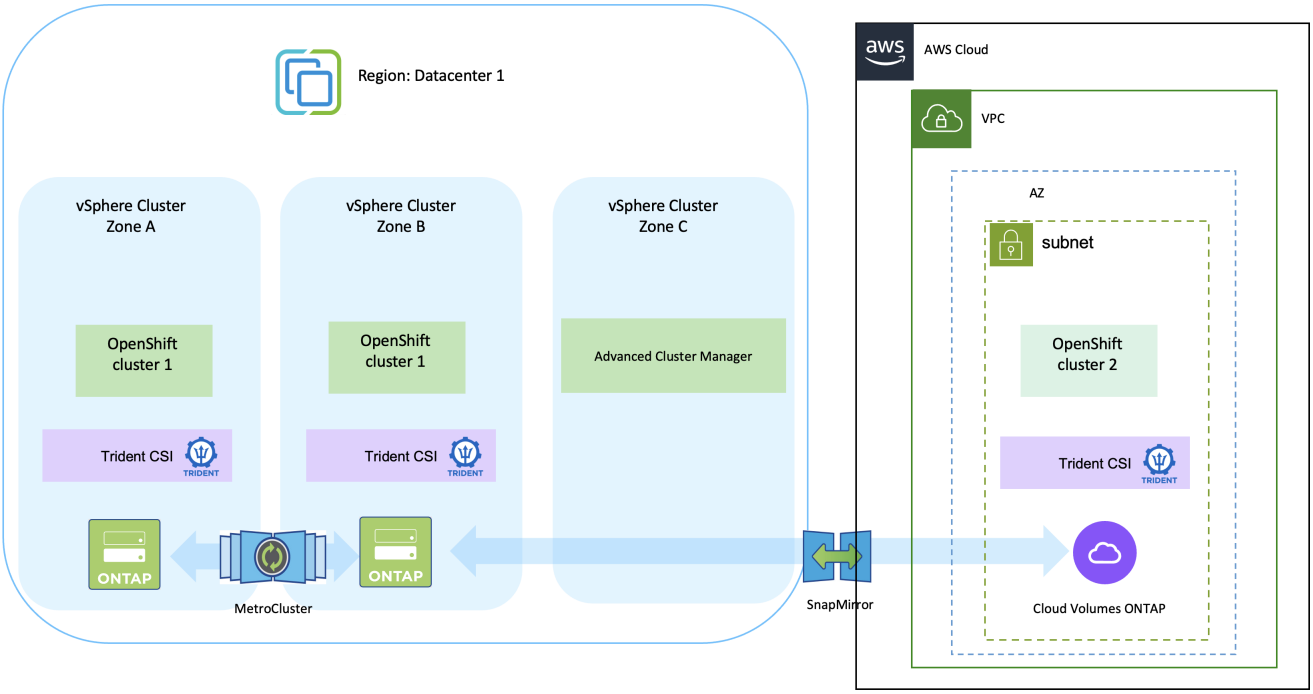


情境 **2**：使用**Trident Protect** 進行資料保護以及從本機環境到 **AWS** 環境的遷移

本機：自管理 **OpenShift** 叢集和自管理儲存 **AWS** 雲端：自管理 **OpenShift** 叢集和自管理儲存

- 使用 Trident Protect 保護應用程式，並支援在本機叢集和 AWS 中的自管理 OpenShift 叢集之間進行遷移。

場景 **2**

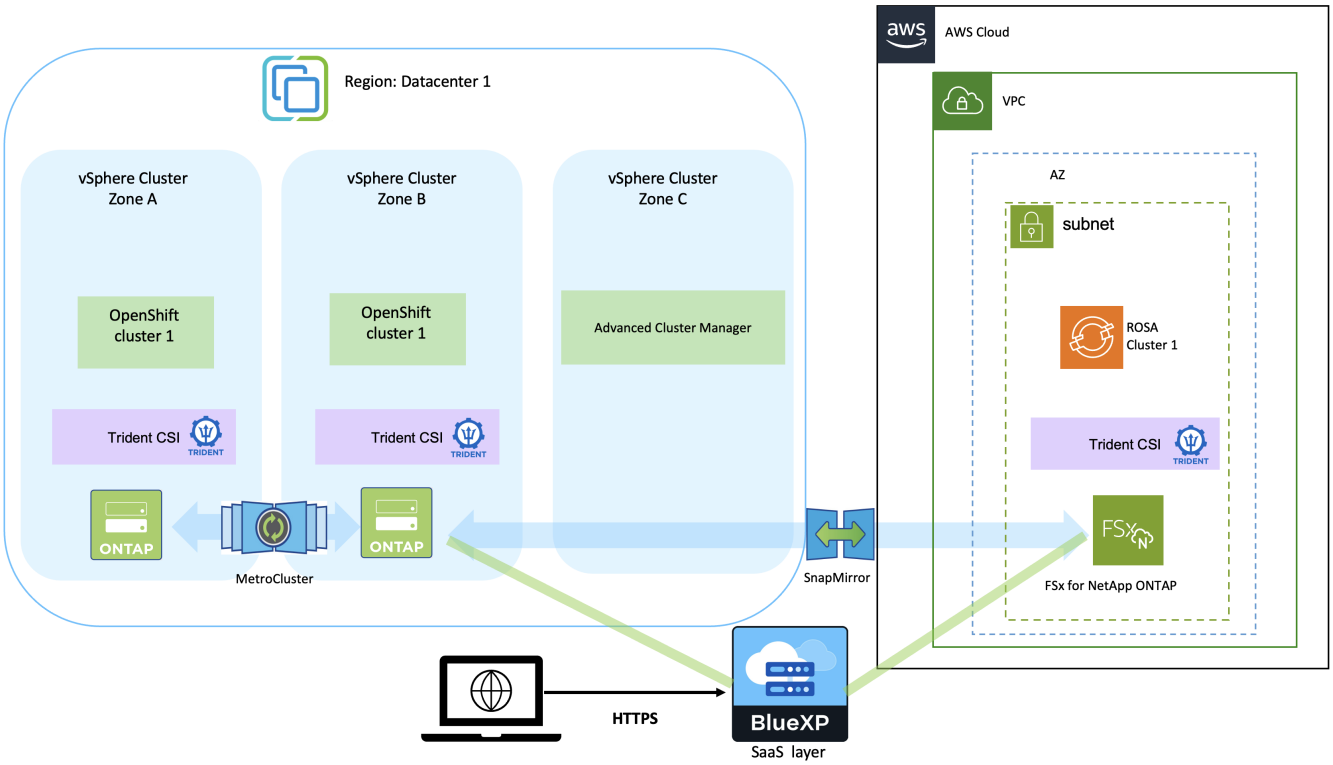


情境 **3**：資料保護以及從本機環境到 **AWS** 環境的遷移

本機：自管理 **OpenShift** 叢集和自管理儲存 **AWS** 雲端：供應商管理的 **OpenShift** 叢集 **(ROSA)** 和供應商管理的儲存 **(FSx ONTAP)**

- 使用 NetApp Console，執行持續性 Volume（FSx ONTAP）的複寫。
- 使用 OpenShift GitOps 重新建立應用程式元資料。

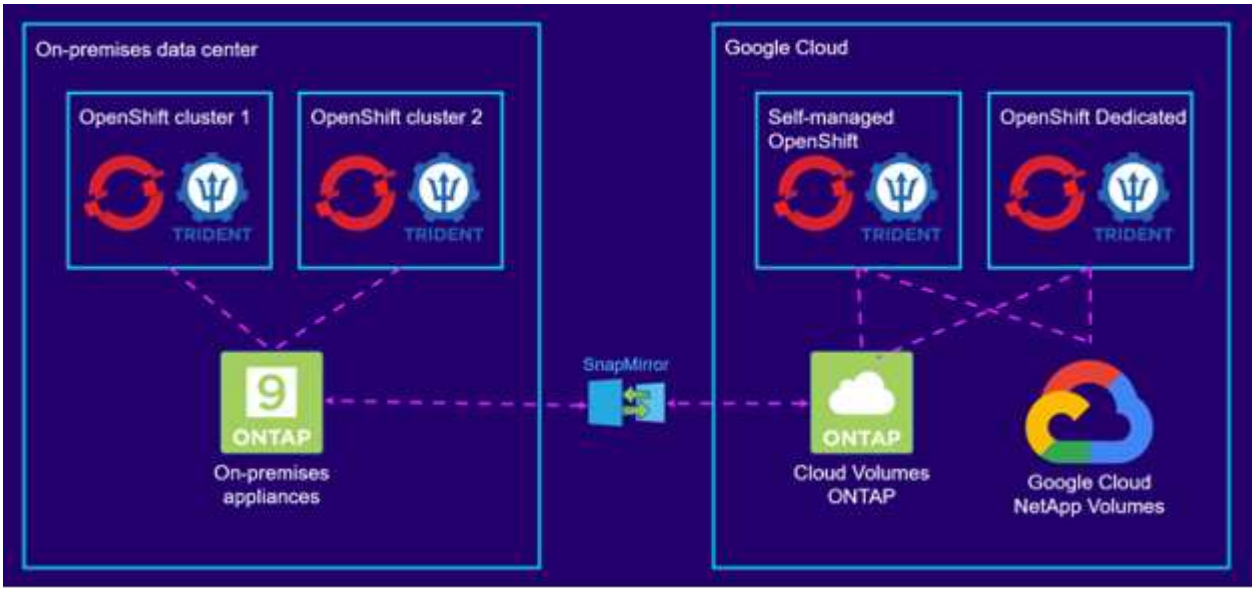
場景 **3**



情境 **4**：使用**Trident Protect** 進行資料保護以及從本地環境到 **GCP** 環境的遷移

本地：自管理 **OpenShift** 叢集和自管理儲存 **Google Cloud**：自管理 **OpenShift** 叢集和自管理儲存

- 使用 Trident Protect 保護應用程式，並支援在本地叢集和 Google Cloud OpenShift 叢集之間進行遷移。

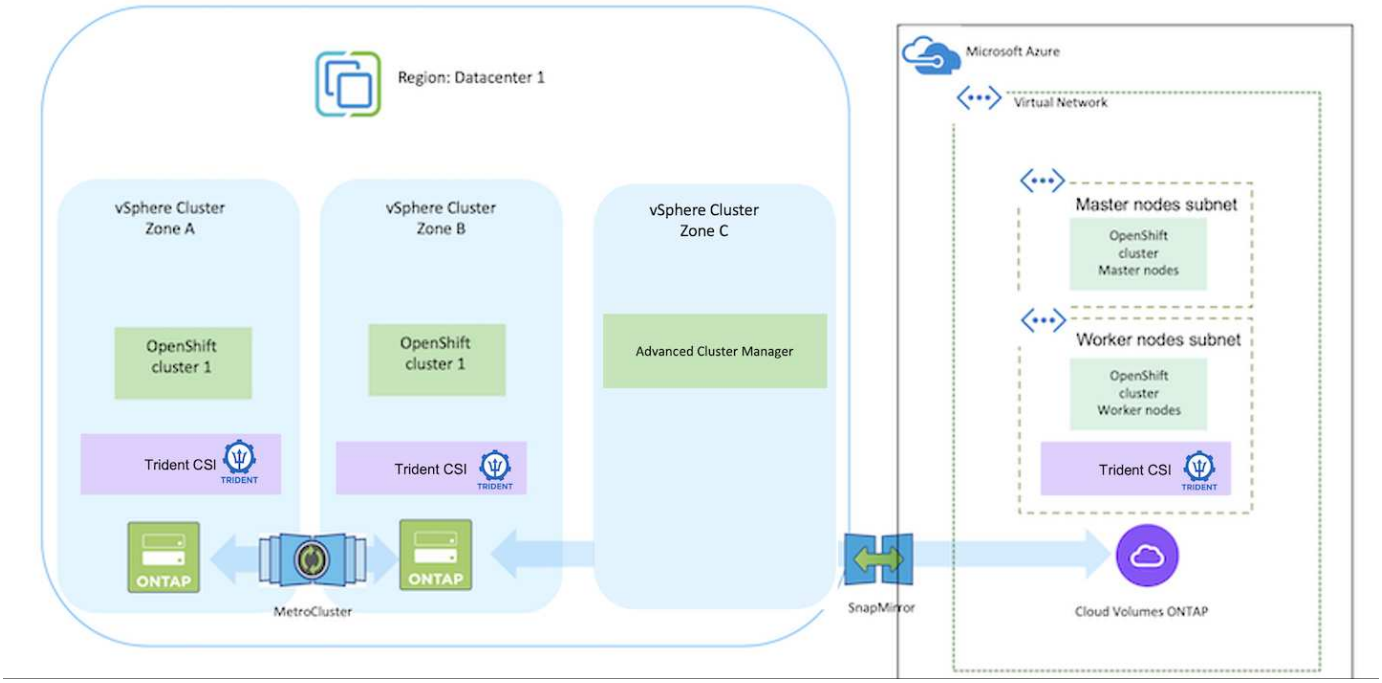


有關在MetroCluster配置中使用ONTAP時的注意事項，請參閱"這裡"。

情境 **5**：使用**Trident Protect** 進行資料保護以及從本機環境到 **Azure** 環境的遷移

本機：自管理 **OpenShift** 叢集和自管理儲存 **Azure** 雲端：自管理 **OpenShift** 叢集和自管理儲存

- 使用 Trident Protect 保護應用程式，並支援在內部部署與 Azure 中的 OpenShift 叢集之間進行移轉。



有關在MetroCluster配置中使用ONTAP時的注意事項，請參閱"這裡"。

解決方案驗證中使用的各種組件的版本

此解決方案使用 OpenShift 容器平台、OpenShift Advanced Cluster Manager、 NetApp ONTAP和NetApp Trident Protect 測試並驗證遷移和集中資料保護。

解決方案的場景 1、2 和 3 使用下表所示的版本進行驗證：

成分	版本
VMware	vSphere Client 版本 8.0.0.10200 VMware ESXi，8.0.0，20842819
樞紐集群	OpenShift 4.11.34
來源集群和目標集群	OpenShift 4.12.9 本機和 AWS
NetApp Trident	Trident伺服器和客戶端 23.04.0
* NetApp Trident保護*	Trident Protect 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1
AWS FSx ONTAP	單一可用區

解決方案的場景 4 使用下表所示的版本進行了驗證：

成分	版本
VMware	vSphere Client 版本 8.0.2.00000 VMware ESXi，8.0.2，22380479

樞紐集群	OpenShift 4.13.13
來源集群和目標集群	OpenShift 4.13.12 本地與 Google Cloud 中
NetApp Trident	Trident伺服器和客戶端 23.07.0
NetApp ONTAP	ONTAP 9.12.1
* Cloud Volumes ONTAP*	單可用區，單節點，9.14.0

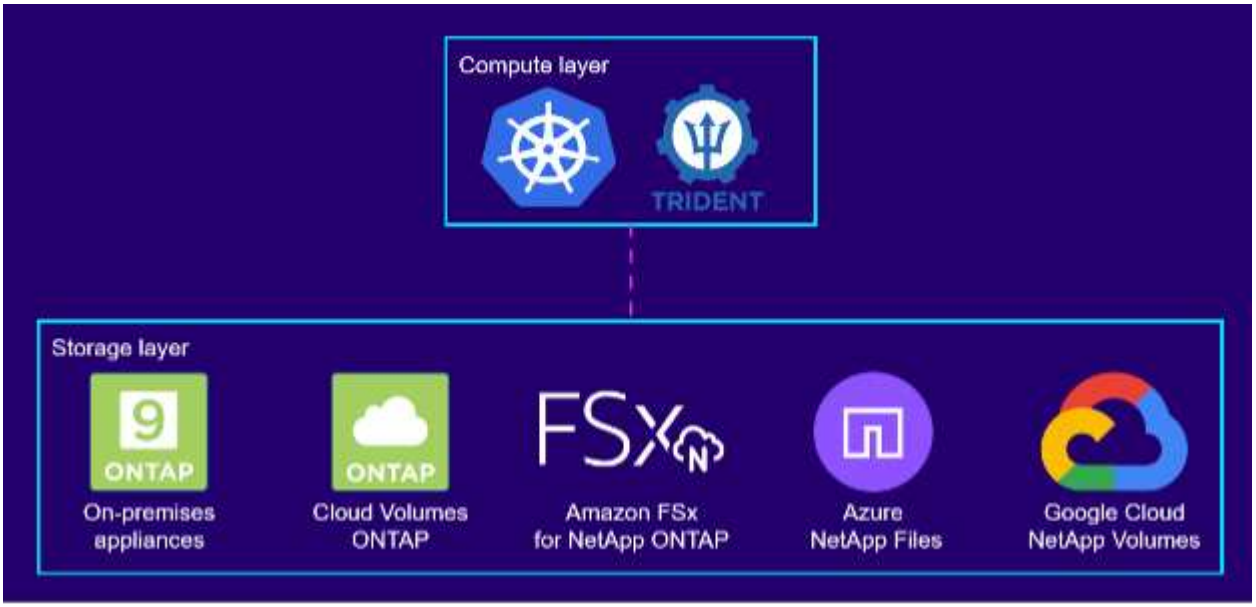
解決方案的場景 5 使用下表所示的版本進行了驗證：

成分	版本
VMware	vSphere Client 版本 8.0.2.00000 VMware ESXi，8.0.2，22380479
來源集群和目標集群	OpenShift 4.13.25 本機和 Azure
NetApp Trident	Trident 伺服器和用戶端 23.10.0
* NetApp Trident保護*	Trident Protect 23.10
NetApp ONTAP	ONTAP 9.12.1
* Cloud Volumes ONTAP*	單可用區，單節點，9.14.0

支援**NetApp Storage** 與 **Red Hat OpenShift Containers** 的集成

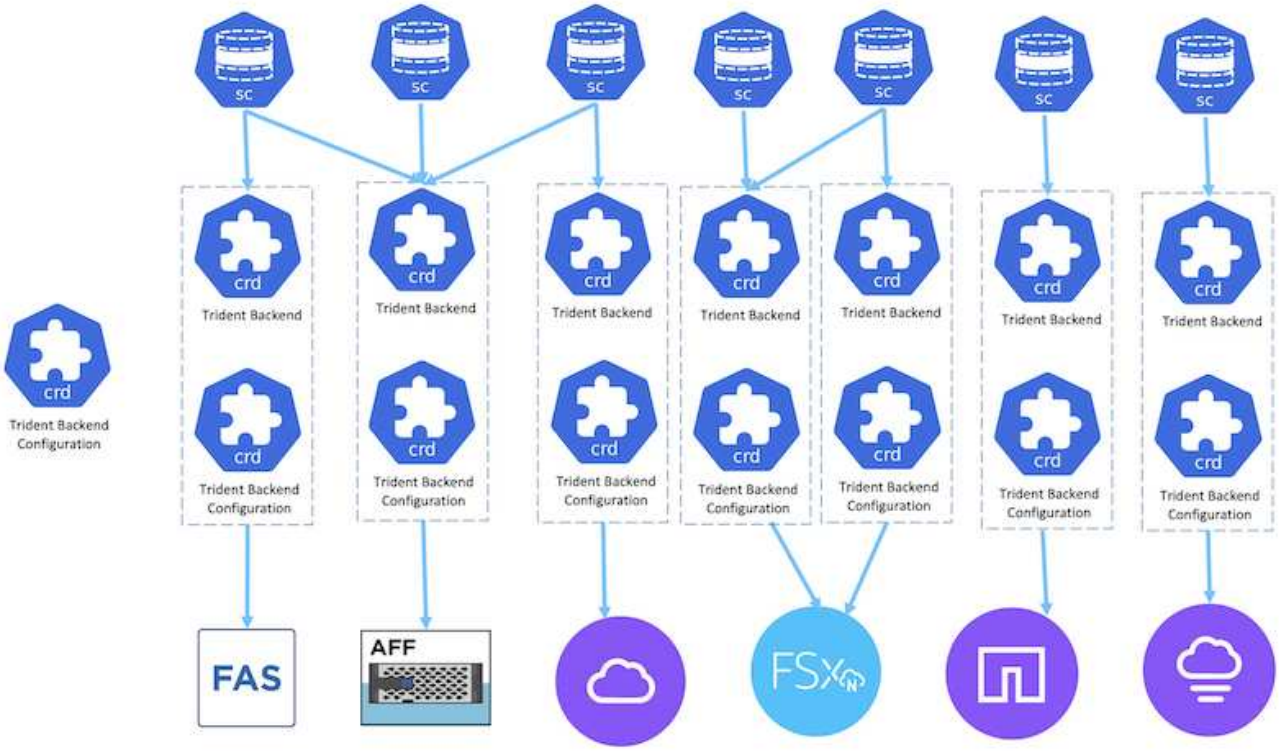
無論 Red Hat OpenShift 容器是在 VMware 上運行還是在超大規模環境中運行， NetApp Trident都可以用作其支援的各種類型的後端NetApp儲存的 CSI 配置器。

下圖描述了可使用NetApp Trident與 OpenShift 叢集整合的各種後端NetApp儲存。



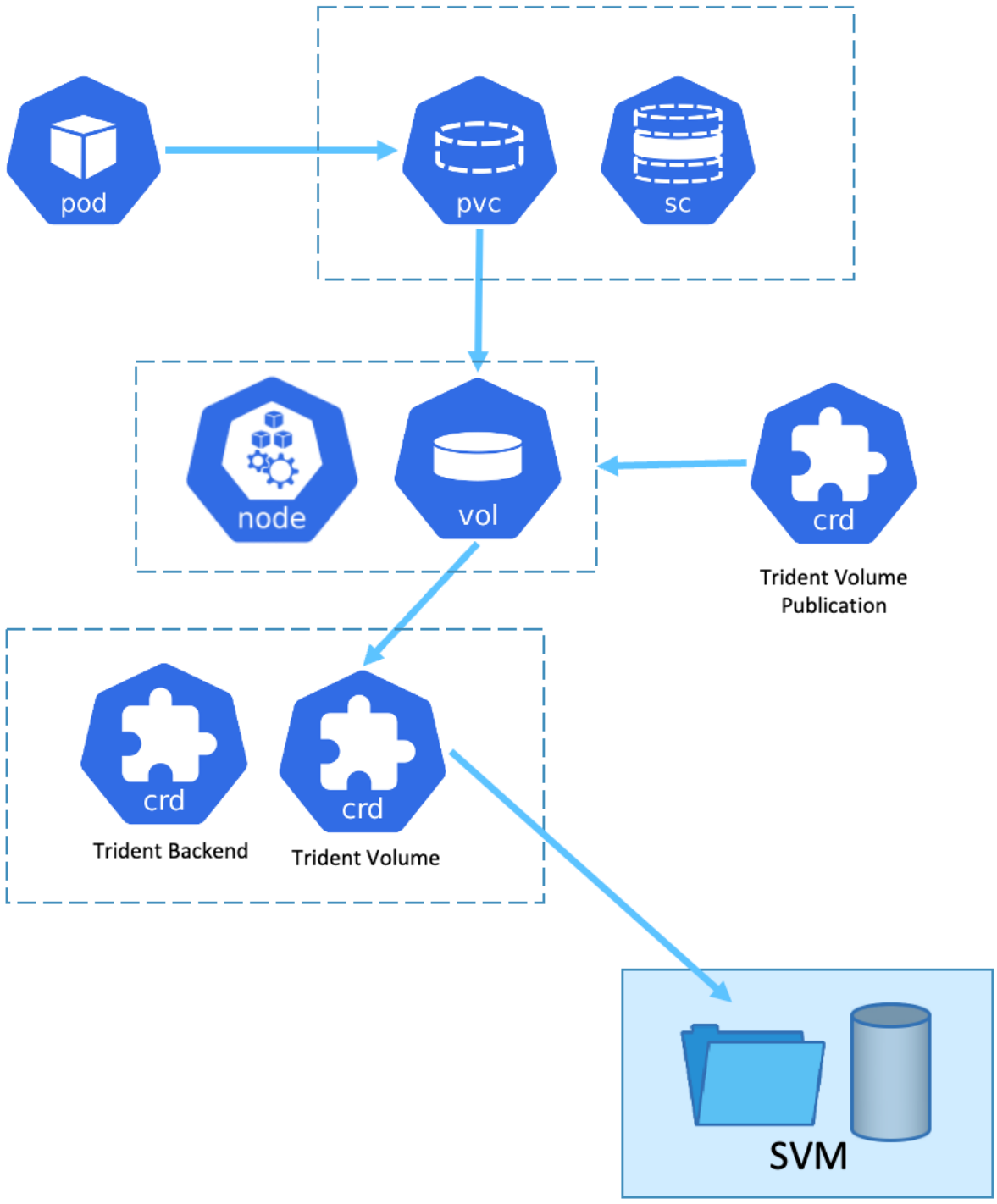
ONTAP儲存虛擬機器 (SVM) 提供安全的多租戶。單一 OpenShift 叢集可以連接到單一 SVM 或多個 SVM，甚至多個ONTAP叢集。儲存類別根據參數或標籤過濾後端儲存。儲存管理員使用 trident 後端設定定義連接到儲存系統的參數。成功建立連線後，它會建立 trident 後端並填入儲存類別可以過濾的資訊。

storageclass和backend的關係如下圖所示。



應用程式擁有者請求使用儲存類別的持久性磁碟區。儲存類別過濾後端儲存。

pod與後端儲存的關係如下圖所示。



容器儲存介面 **(CSI)** 選項

在 vSphere 環境中，客戶可以選擇 VMware CSI 驅動程式和/或Trident CSI 與ONTAP整合。使用 VMware CSI 時，持久性磁碟區將作為本機 SCSI 磁碟使用，而使用Trident時，它將與網路一起使用。

由於 VMware CSI 不支援ONTAP的 RWX 存取模式，因此如果需要 RWX 模式，應用程式需要使用Trident CSI。對於基於 FC 的部署，VMware CSI 是首選，而SnapMirror業務連續性 (SMBC) 可提供區域層級的高可用性。

VMware CSI 支援

- 基於核心區塊的資料儲存（FC、FCoE、iSCSI、NVMeoF）
- 基於核心檔案的資料儲存（NFS v3、v4）
- vVol 資料儲存（區塊和檔案）

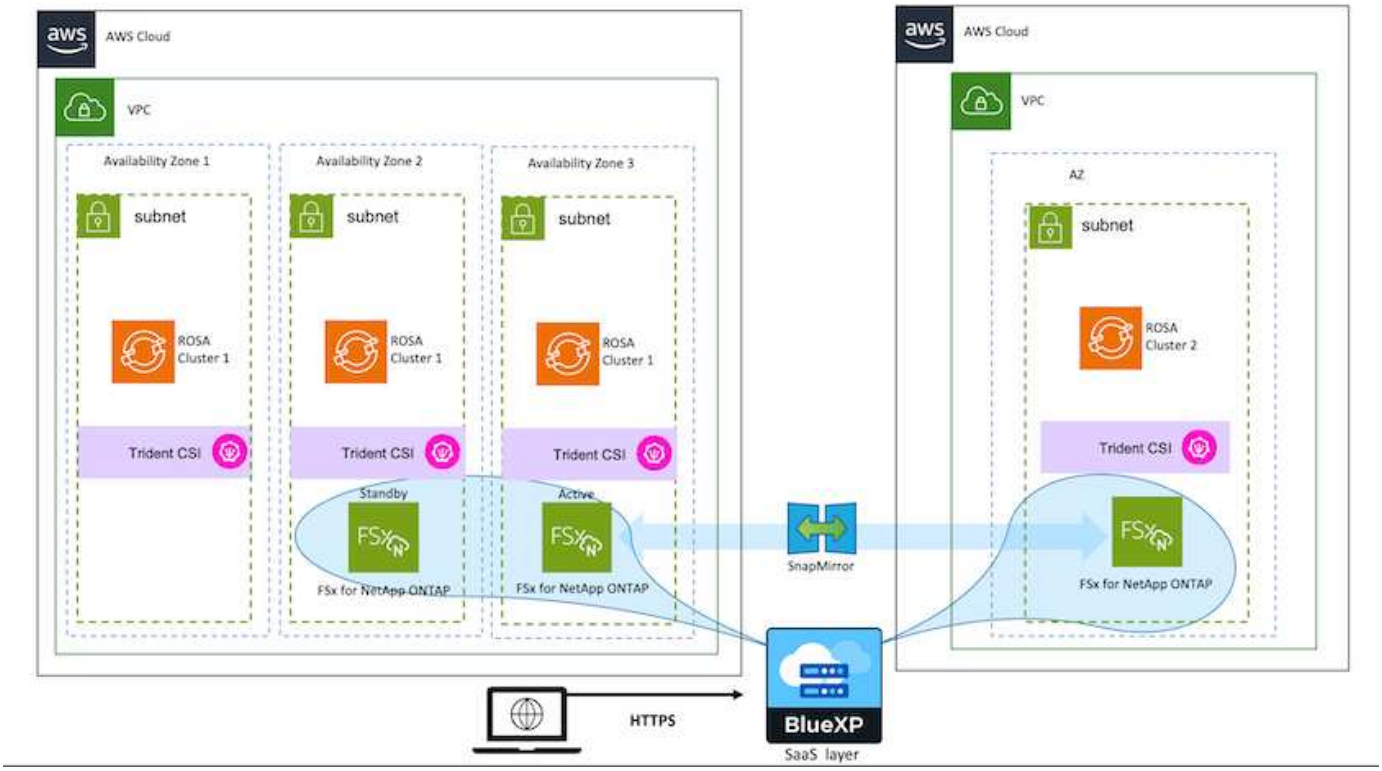
Trident有以下驅動程式支援ONTAP

- ontap-san（專用卷）
- ontap-san-economy（共享卷）
- ontap-nas（專用卷）
- ontap-nas-economy（共享卷）
- ontap-nas-flexgroup（專用大規模卷）

對於 VMware CSI 和Trident CSI， ONTAP支援 NFS 的 nconnect、會話中繼、kerberos 等以及區塊協定的多路徑、chap 驗證等。

在 AWS 中， Amazon FSx for NetApp ONTAP （FSx ONTAP）可以部署在單一可用區（AZ）或多可用區中。對於需要高可用性的生產工作負載，與單可用區相比，多可用區提供區域級容錯能力並具有更好的 NVMe 讀取快取。欲了解更多信息，請查看"AWS 效能指南"。

為了節省災難復原站點的成本，可以使用單一 AZ FSx ONTAP
。



有關 FSx ONTAP支援的 SVM 數量，請參閱"管理 FSx ONTAP儲存虛擬機"

其他文檔

以下是一些可供參考的附加文件：

1. "VMware vSphere"
2. "OpenShift 容器平台產品文檔"
3. "安裝 OpenShift 容器平台集群"
4. "高階叢集管理產品文檔"
5. "使用 ACM 建立集群"
6. "在 OpenShift 上部署 Red Hat Quay"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda" - Verda（開源）提供了一系列適用於熱門雲端原生資料密集型應用程式的參考執行掛鉤
10. "NetApp 資料服務"
11. "Red Hat OpenShift Service on AWS 經典架構"
12. "Amazon FSx ONTAP"
13. "在 GCP 上安裝 OpenShift 集群"
14. "在 Azure 上安裝 OpenShift 集群"

Openshift 適用於本地

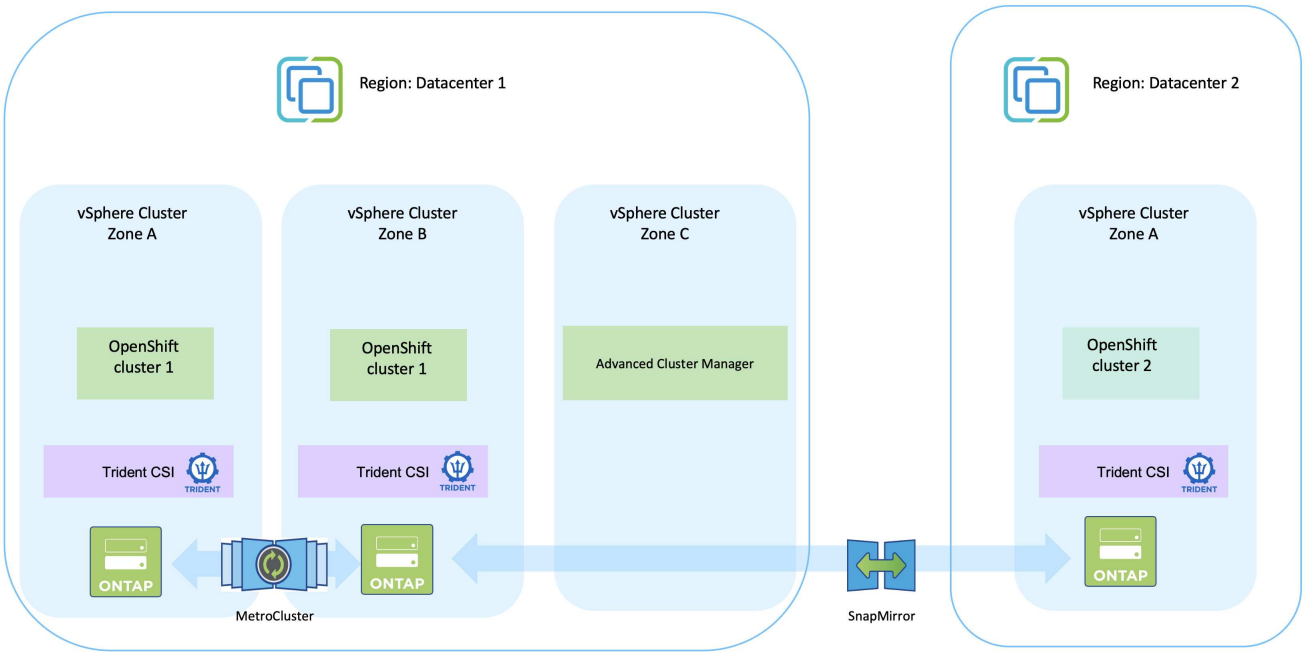
NetApp解決方案與 VMware 上的 Red Hat OpenShift Container 平台工作負載

如果客戶需要在其私人資料中心的基礎設施上運行現代容器化應用程序，他們可以這樣做。他們應該規劃和部署 Red Hat OpenShift 容器平台 (OCP)，以便成功建構可用於生產的環境來部署他們的容器工作負載。他們的 OCP 叢集可以部署在 VMware 或裸機上。

NetApp ONTAP儲存為容器部署提供資料保護、可靠性和靈活性。 Trident作為動態儲存配置器，為客戶的有狀態應用程式使用持久性ONTAP儲存。 NetApp Trident Protect 可用於滿足有狀態應用程式的多種資料管理需求，例如資料保護、遷移和業務連續性。

透過 VMware vSphere， NetApp ONTAP工具提供了可用於設定資料儲存區的 vCenter 外掛程式。應用標籤並將其與 OpenShift 一起使用來儲存節點配置和資料。基於 NVMe 的儲存提供更低的延遲和高效能。

使用**Trident Protect** 為 **OpenShift Container** 工作負載提供資料保護和遷移解決方案

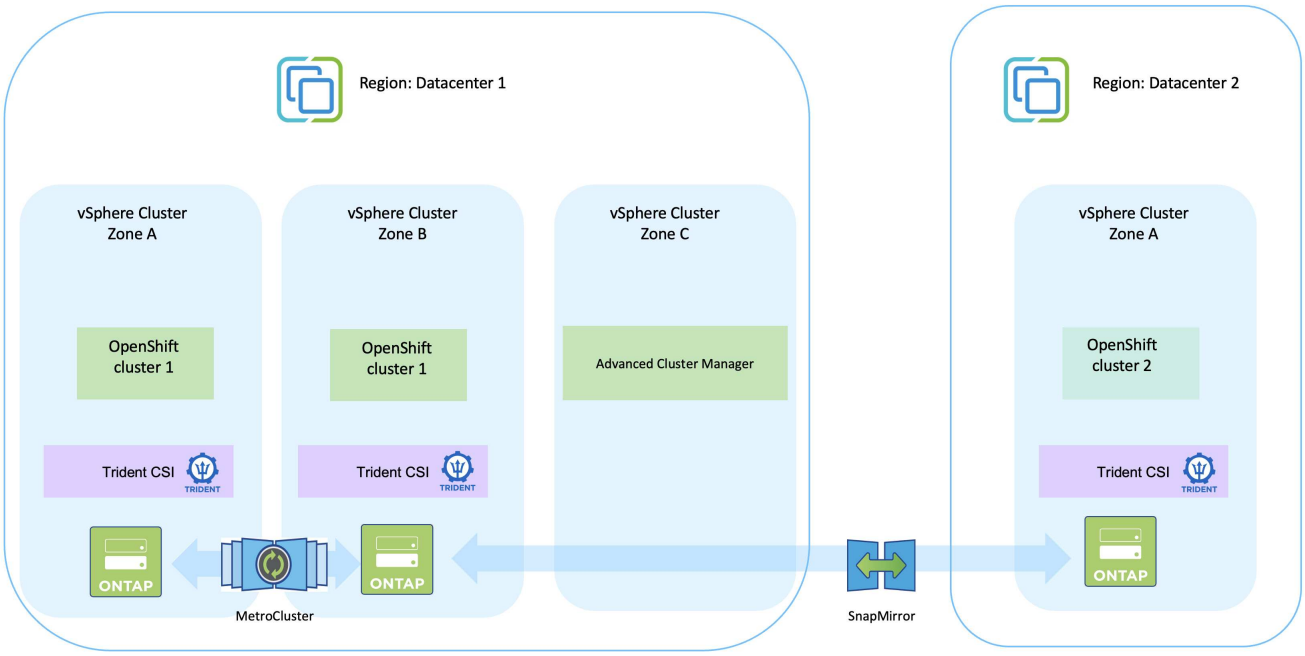


在 **VMware** 上部署並設定 **Red Hat OpenShift Container** 平台

本節介紹如何設定和管理 OpenShift 叢集以及管理其上的有狀態應用程式的高階工作流程。它展示瞭如何使用NetApp ONTAP儲存陣列借助Trident來提供持久性磁碟區。

部署 Red Hat OpenShift Container 平台叢集有多種方法。此設定的高級描述提供了所使用的特定方法的文檔連結。您可以參考"資源部分"。

下面是描述資料中心內 VMware 上部署的叢集的圖表。



設定過程可分為以下步驟：

▼ 部署並配置 **CentOS VM**

- 它部署在VMware vSphere環境中。
- 此虛擬機器用於為解決方案部署一些元件，例如NetApp Trident和NetApp Trident Protect。
- 安裝期間，此虛擬機器上配置了一個 root 使用者。

▼ 在 **VMware vSphere**（**Hub Cluster**）上部署和設定 **OpenShift Container Platform** 叢集

請參閱 "協助部署" 方法的說明以部署 OCP 叢集。

請記住以下內容： - 建立 ssh 公鑰和私鑰以提供給安裝程式。如果需要，這些金鑰將用於登入主節點和工作節點。 - 從輔助安裝程式下載安裝程式。此程式用於啟動您在 VMware vSphere 環境中為主節點和工作節點所建立的虛擬機器。 - 虛擬機器應具備最低 CPU、記憶體和硬碟需求。 （請參閱 vm create 命令"這"提供此資訊的主節點和工作節點的頁面） - 應在所有虛擬機器上啟用 diskUUID。 - 為 master 建立至少 3 個節點，為 worker 建立至少 3 個節點。 - 一旦安裝程式發現它們，請開啟 VMware vSphere 整合切換按鈕。

▼ 在 **Hub** 叢集上安裝進階叢集管理

這是使用 Hub 叢集上的高級叢集管理操作員安裝的。參考說明"這裡"。

▼ 安裝兩個額外的 **OCP** 叢集（來源和目標）

- 可以使用 Hub 叢集上的 ACM 部署附加叢集。
- 請參閱說明"這裡"。

▼ 配置**NetApp ONTAP**存儲

- 在 VMWare 環境中安裝與 OCP VM 連線的ONTAP叢集。

- 建立 SVM。
- 配置 NAS 資料生命週期以存取 SVM 中的儲存。

▼ 在 **OCP** 叢集上安裝**NetApp Trident**

- 在所有三個叢集上安裝NetApp Trident ：中心叢集、來源叢集和目標集群
- 請參閱說明"這裡"。
- 為 ontap-nas 建立儲存後端。
- 為 ontap-nas 建立儲存類別。
- 參考說明"這裡"。

▼ 在來源集群上部署應用程式

使用 OpenShift GitOps 部署應用程式。 （例如 Postgres、Ghost）

下一步是使用Trident Protect 進行資料保護和從來源叢集到目標叢集的資料遷移。參考"這裡"以取得說明。

使用**Trident Protect** 進行資料保護

本頁顯示使用 Trident Protect 在 VMware vSphere 上執行的 Red Hat OpenShift Container 應用程式的資料保護選項。

使用者在使用 Red Hat OpenShift 進行應用程式現代化改造的過程中，應制定資料保護策略，以防止意外刪除或其他人為錯誤導致的資料遺失。此外，出於監管或合規性要求，還需要製定資料保護策略，以防資料在災難中遺失。

資料保護的要求多種多樣，從恢復到某個時間點的副本到無需任何人工幹預即可自動故障轉移到不同的故障域。許多客戶選擇ONTAP作為其 Kubernetes 應用程式的首選儲存平台，因為它具有豐富的功能，例如多租戶、多協定、高效能和容量產品、多站點位置的複製和快取、安全性和靈活性。

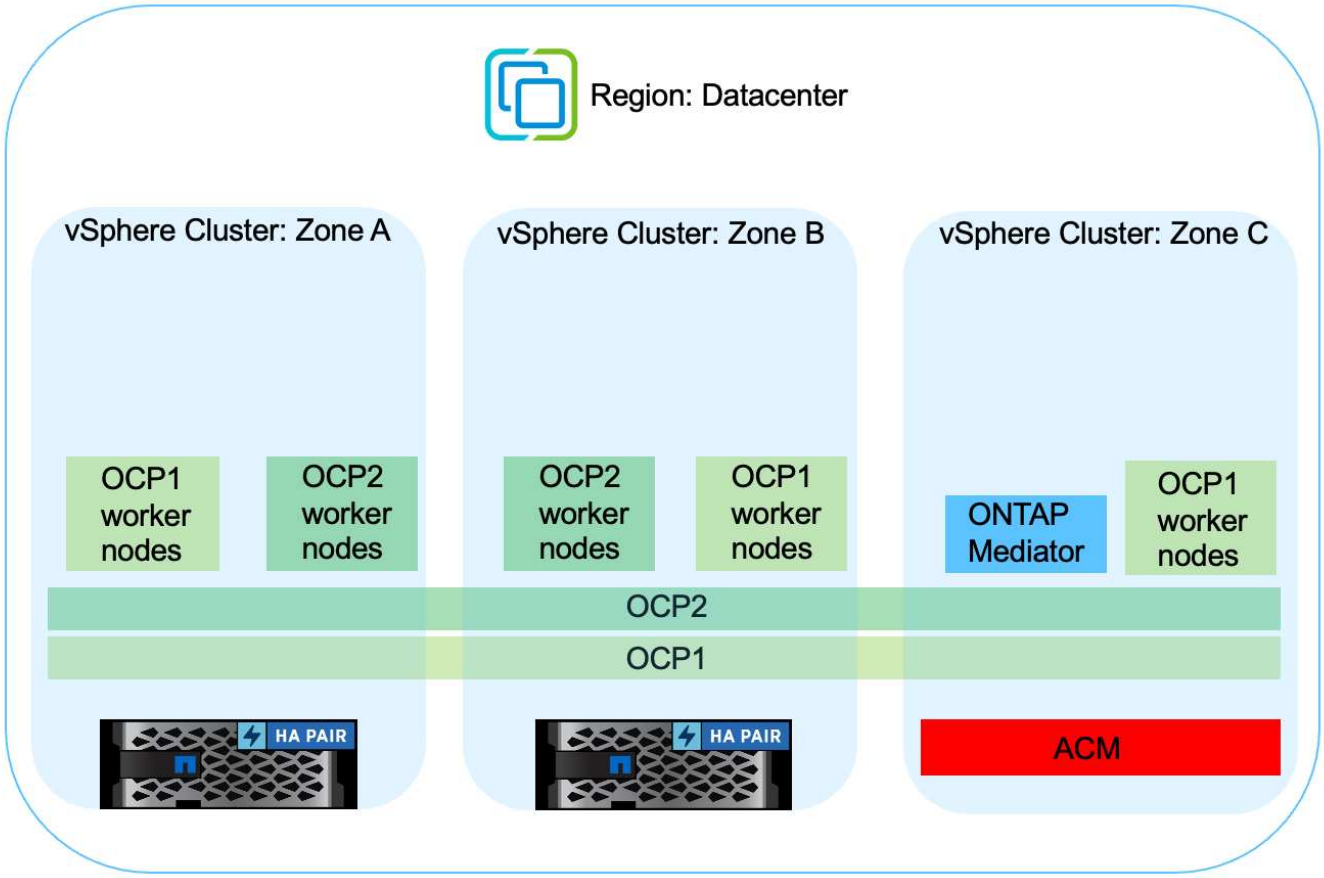
有關使用 Trident Protect 保護和遷移容器工作負載的詳細資訊，請參閱以下章節：- "使用 Trident Protect 保護和遷移容器應用程式"

利用**MetroCluster**實現業務連續性

我們的大多數ONTAP硬體平台都具有高可用性功能，可防止設備故障，避免執行災難復原。但為了防止火災或任何其他災難，並以零 RPO 和低 RTO 繼續開展業務，通常會使用MetroCluster解決方案。

目前擁有ONTAP系統的客戶可以透過在距離限制內添加支援的ONTAP系統來擴展到MetroCluster ，以提供區域級災難復原。 Trident，CSI（容器儲存介面）支援NetApp ONTAP，ONTAPMetroCluster配置以及其他選項，如Cloud Volumes ONTAP、 Azure NetApp Files、AWS FSx ONTAP等。 Trident 為Trident提供了五種儲存驅動程式選項，並且所有選項都支援MetroCluster配置。參考"這裡"有關Trident支援的ONTAP儲存驅動程式的更多詳細資訊。

MetroCluster解決方案需要第 2 層網路擴展或從兩個故障域存取相同網路位址的能力。一旦MetroCluster配置到位，該解決方案對於應用程式擁有者來說是透明的，因為MetroCluster svm 中的所有磁碟區都受到保護並獲得SyncMirror （零 RPO）的好處。



對於Trident後端設定 (TBC)，使用MetroCluster設定時請勿指定 dataLIF 和 SVM。為 managementLIF 指定 SVM 管理 IP 並使用 vsadmin 角色憑證。

有關 Trident Protect 資料保護功能的詳細資訊，請參閱"這裡"。

具有自管理元件的混合雲

NetApp解決方案與混合雲中的 Red Hat OpenShift 容器平台工作負載

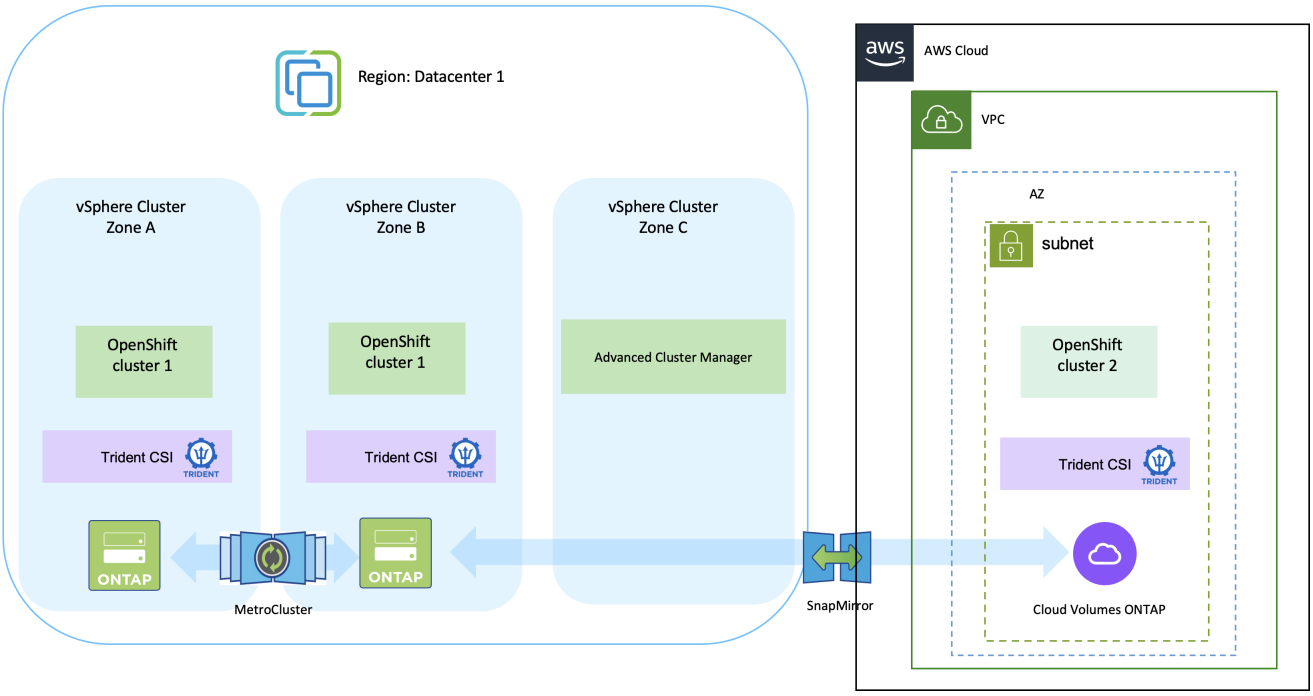
當客戶準備將部分選定的工作負載或所有工作負載從資料中心遷移到雲端時，他們可能正處於現代化轉型的某個階段。他們可能會出於各種原因選擇在雲端中使用自管理的 OpenShift 容器和自管理的NetApp儲存。他們應該在雲端中規劃和部署 Red Hat OpenShift 容器平台 (OCP)，以便成功建構一個可用於生產的環境，以便從資料中心遷移容器工作負載。他們的 OCP 叢集可以在其資料中心部署在 VMware 或 Bare Metal 上，也可以在雲端環境中部署在 AWS、Azure 或 Google Cloud 上。

NetApp Cloud Volumes ONTAP 儲存為 AWS、Azure 和 Google Cloud 中的容器部署提供資料保護、可靠性和靈活性。Trident 作為動態儲存配置器，為客戶的有狀態應用程式使用持久的 Cloud Volumes ONTAP 儲存。Trident Protect 可用於滿足有狀態應用程式的資料管理需求，例如資料保護、遷移和業務連續性。

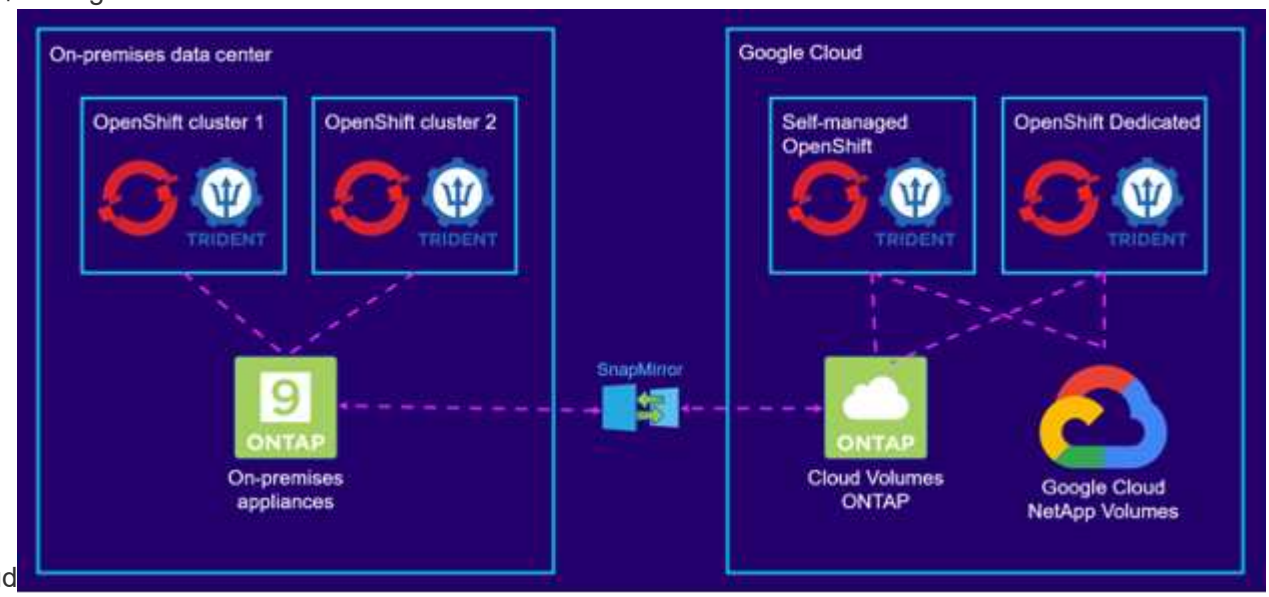
使用**Trident Protect** 為混合雲中的 **OpenShift Container** 工作負載提供資料保護和遷移解決方案

本地和

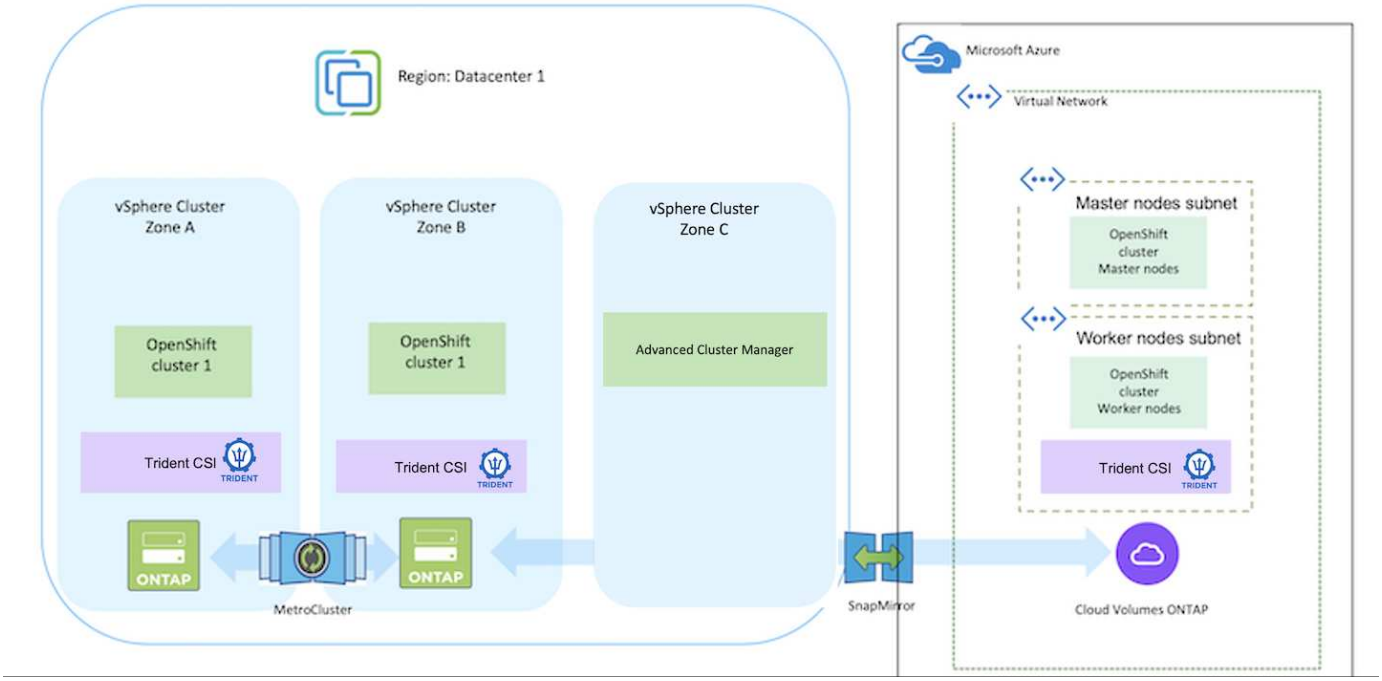
AWS



本地和 Google Cloud



本地和 Azure 云端

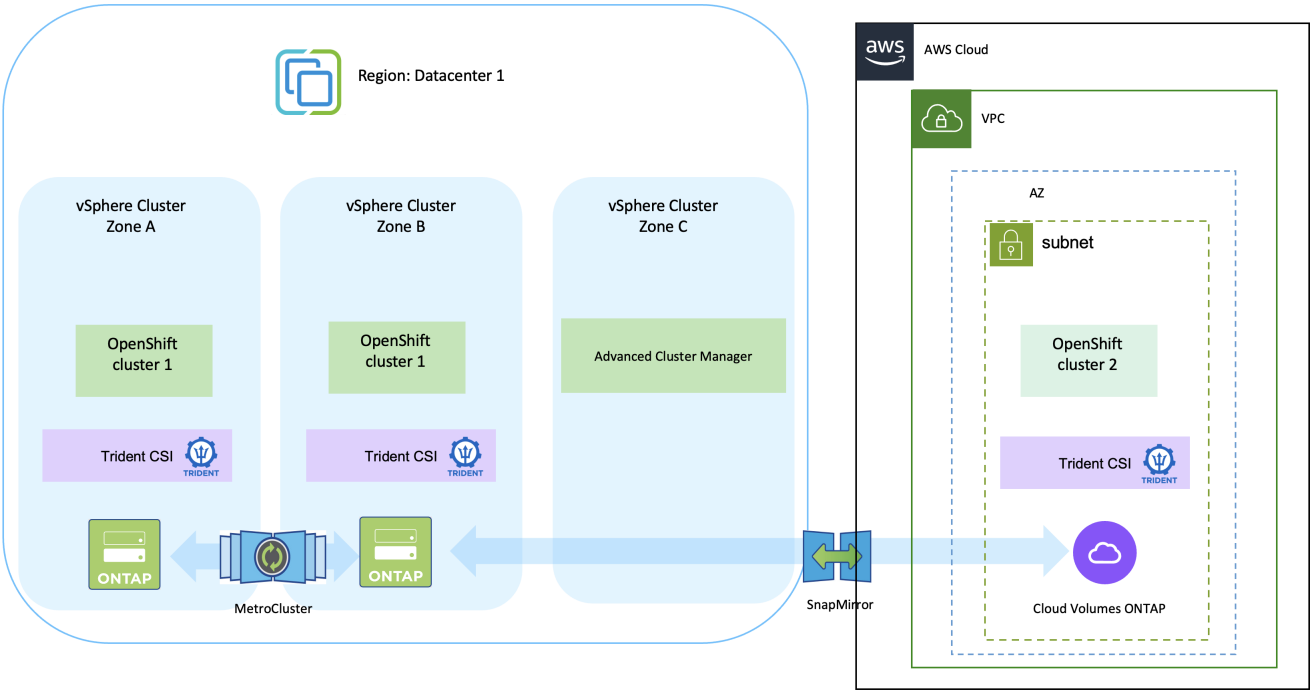


在 **AWS** 上部署和設定 **Red Hat OpenShift Container** 平台

本節介紹如何在 AWS 中設定和管理 OpenShift 叢集並在其上部署有狀態應用程式的進階工作流程。它展示瞭如何使用NetApp Cloud Volumes ONTAP儲存在Trident的幫助下提供持久卷。提供了有關使用Trident Protect 為有狀態應用程式執行資料保護和遷移活動的詳細資訊。

有幾種方法可以在 AWS 上部署 Red Hat OpenShift Container 平台叢集。此設定的高級描述提供了所使用的特定方法的文檔連結。您可以參考"資源部分"。

下圖描述了部署在 AWS 上並使用 VPN 連接到資料中心的叢集。



設定過程可分為以下步驟：

▼ 從進階叢集管理在 **AWS** 上安裝 **OCP** 叢集。

- 建立具有網站到網站 VPN 連線（使用 pfSense）的 VPC 以連接到本機網路。
- 內部網路具有網路連線。
- 在 3 個不同的 AZ 中建立 3 個私有子網路。
- 為 VPC 建立 Route 53 私人託管區域和 DNS 解析器。

從 Advanced Cluster Management（ACM）精靈在 AWS 上建立 OpenShift 叢集。請參閱指示 "這裡"。

您也可以透過 OpenShift 混合雲主控台在 AWS 中建立叢集。請參閱 "這裡" 相關說明。

使用 ACM 建立叢集時，您可以在表單檢視中填寫詳細資料後透過編輯 yaml 檔案來自訂安裝。叢集建立完成後，可以透過ssh登入叢集的節點進行故障排除或額外的手動設定。使用您在安裝過程中提供的 ssh 金鑰和使用者名稱 core 登入。

▼ 使用 **NetApp Console** 在 **AWS** 中部署 **Cloud Volumes ONTAP**。

- 在本機 VMware 環境中安裝連接器。參考說明"這裡"。
- 使用連接器在 AWS 中部署 CVO 執行個體。參考說明"這裡"。

此連接器也可以安裝在雲端環境中。參考"這裡"了解更多。

▼ 在 **OCP** 叢集中安裝**Trident**

- 使用 Helm 部署 Trident Operator。請參閱指示 "這裡"

- 建立後端和儲存類別。參考說明"這裡"。

使用**Trident**的 **CSI** 拓樸功能實現多區域架構

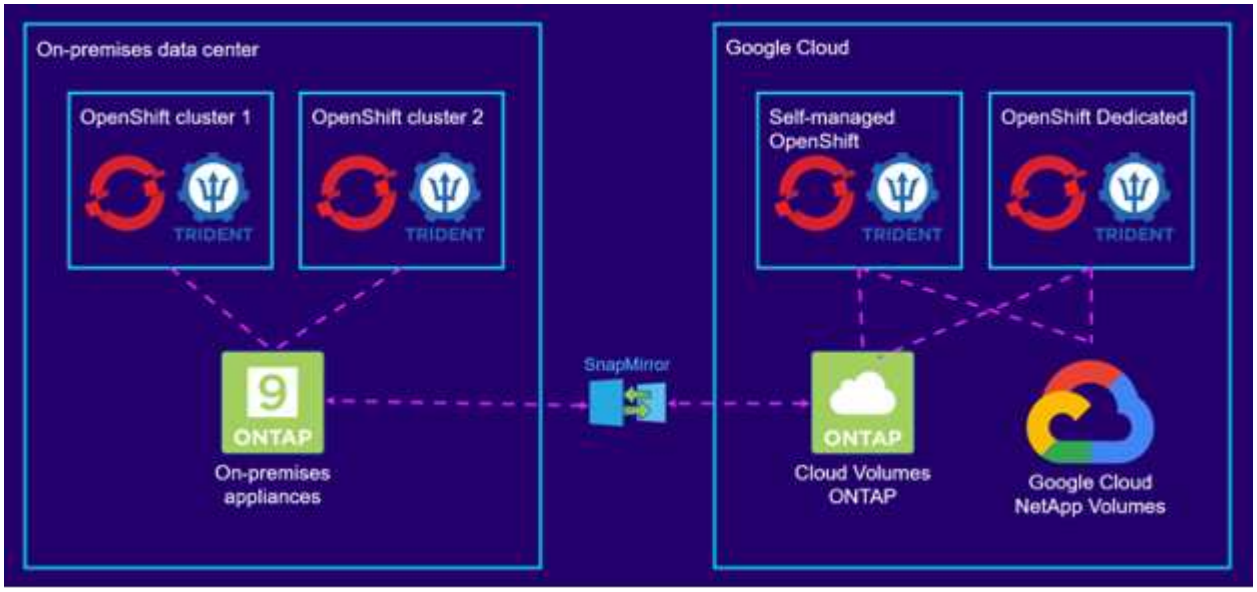
如今，雲端提供者使 Kubernetes/OpenShift 叢集管理員能夠產生基於區域的叢集節點。節點可以位於一個區域內的不同可用區，也可以跨越多個區域。為了方便在多區域架構中為工作負載配置卷， Trident使用了 CSI 拓撲。使用 CSI 拓撲功能，可以根據區域和可用區域將對磁碟區的存取限製到節點子集。參考"這裡"了解更多詳細資訊。

> Kubernetes 支援兩種磁碟區綁定模式： - 當 ***VolumeBindingMode*** 設定為 ***Immediate***（預設）時， Trident會在沒有任何拓樸感知的情況下建立磁碟區。持久性卷的建立不依賴請求 pod 的調度要求。 - 當 ***VolumeBindingMode*** 設定為 ***WaitForFirstConsumer*** 時，PVC 的持久卷的建立和綁定將被延遲，直到使用該 PVC 的 pod 被調度和建立。這樣，就可以建立磁碟區來滿足拓樸要求所強制執行的調度約束。 Trident儲存後端可設計為根據可用區域（拓撲感知後端）選擇性地配置磁碟區。對於使用此類後端的 StorageClasses，只有在受支援的區域/區域中調度的應用程式請求時才會建立磁碟區。 （拓樸感知 StorageClass）參考"這裡"了解更多詳細資訊。

在 **Google Cloud** 上部署和設定 **Red Hat OpenShift** 容器平台

本節介紹如何在 GCP 中設定和管理 OpenShift 叢集以及在其上部署有狀態應用程式的進階工作流程。它展示瞭如何使用Google Cloud NetApp Volumes和NetApp Cloud Volumes ONTAP儲存在Trident的幫助下提供持久卷。

下圖顯示了在 GCP 上部署並使用 VPN 連接到資料中心的叢集。



> 在 GCP 中部署 Red Hat OpenShift Container 平台叢集有多種方法。此設定的高級描述提供了所使用的特定方法的文檔連結。您可以參考"資源部分"。

設定過程可分為以下步驟：

從 **CLI** 在 **GCP** 上安裝 **OCP** 集群

- 請確保您已滿足所有規定的先決條件"這裡"。
- 為了實現本地和 GCP 之間的 VPN 連接，我們建立並配置了一個 pfSense VM。有關說明，請參閱 "這裡"。

- 只有在 Google Cloud Platform 中建立 VPN 閘道後，才能設定 pfSense 中的遠端網關位址。
- 只有在 OpenShift 叢集安裝程式執行並建立叢集的基礎架構元件後，才能設定第 2 階段的遠端網路 IP 位址。
- 只有在安裝程式建立叢集的基礎架構元件後，才能設定 Google Cloud 中的 VPN。

- 現在在 GCP 上安裝 OpenShift 叢集。
  - 取得安裝方案和拉取金鑰，並按照文件中提供的步驟部署叢集 "這裡"。
  - 安裝在 Google Cloud Platform 中建立 VPC 網路。它還在 Cloud DNS 中建立私有區域並新增 A 記錄。
    - 使用VPC網路的CIDR塊位址配置pfSense並建立VPN連線。確保防火牆設定正確。
    - 使用 Google Cloud DNS 的 A 記錄中的 IP 位址在本機環境的 DNS 中新增 A 記錄。
  - 叢集安裝完成，會提供一個kubeconfig檔案以及登入叢集控制台的使用者名稱和密碼。

部署**Google Cloud NetApp Volumes**

- 可以按照概述將Google Cloud NetApp Volumes新增至您的專案中"這裡"。

使用 **NetApp Console** 在 **GCP** 中部署 **Cloud Volumes ONTAP**

- 在 Google Cloud 中安裝主控台代理程式。請參閱指示 "這裡"。
- 使用代理程式在 Google Cloud 中部署 CVO 執行個體。請參閱相關說明 "這裡"。

在 **GCP** 中的 **OCP** 叢集中安裝**Trident**

- 部署 Trident 的方法有很多種，如圖所示 "這裡"。
- 在本專案中，Trident 是透過依照指示手動部署 Trident Operator 來安裝的 "這裡"。
- 建立後端和儲存類別。參考說明"這裡"。

使用**Trident**的 **CSI** 拓樸功能實現多區域架構

如今，雲端提供者使 Kubernetes/OpenShift 叢集管理員能夠產生基於區域的叢集節點。節點可以位於一個區域內的不同可用區，也可以跨越多個區域。為了方便在多區域架構中為工作負載配置卷， Trident使用了 CSI 拓撲。使用 CSI 拓撲功能，可以根據區域和可用區域將對磁碟區的存取限製到節點子集。參考"這裡"了解更多詳細資訊。

> Kubernetes 支援兩種磁碟區綁定模式： - 當 ***VolumeBindingMode*** 設定為 ***Immediate***（預設）時， Trident會在沒有任何拓樸感知的情況下建立磁碟區。持久性卷的建立不依賴請求 pod 的調度要求。 - 當 ***VolumeBindingMode*** 設定為 ***WaitForFirstConsumer*** 時，PVC 的持久卷的建立和綁定將被延遲，直到使用該 PVC 的 pod 被調度和建立。這樣，就可以建立磁碟區來滿足拓樸要求所強制執行的調度約束。 Trident儲存後端可設計為根據可用區域（拓撲感知後端）選擇性地配置磁碟區。對於使用此類後端的 StorageClasses，只有在受支援的區域/區域中調度的應用程式請求時才會建立磁碟區。 （拓樸感知 StorageClass）參考"這裡"了解更多詳細資訊。

示範影片

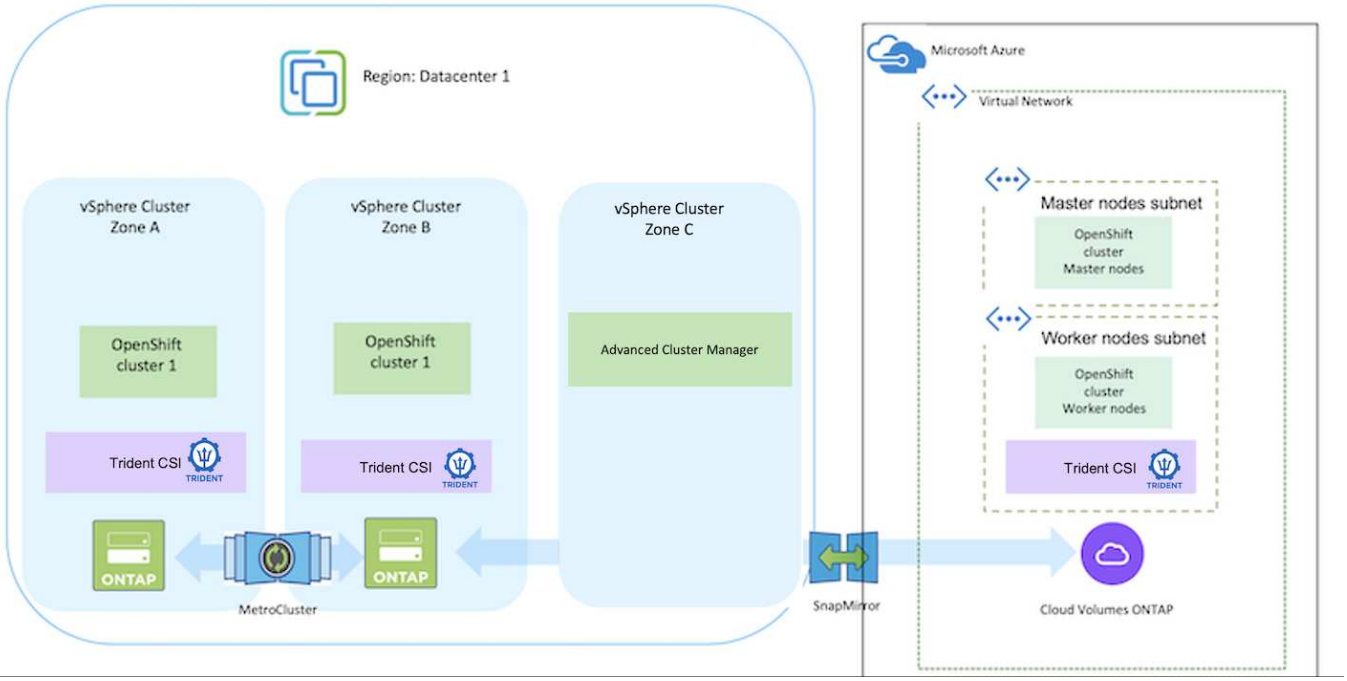
在 Google Cloud Platform 上安裝 OpenShift 集群

將 OpenShift 叢集導入Trident Protect

在 **Azure** 上部署並設定 **Red Hat OpenShift** 容器平台

本節介紹如何在 Azure 中設定和管理 OpenShift 叢集以及在其上部署有狀態應用程式的進階工作流程。它展示瞭如何使用NetApp Cloud Volumes ONTAP儲存在Trident的幫助下提供持久卷。提供了有關使用Trident Protect 為有狀態應用程式執行資料保護和遷移活動的詳細資訊。

下圖顯示了在 Azure 上部署並使用 VPN 連接到資料中心的叢集。



有幾種方法可以在 Azure 中部署 Red Hat OpenShift Container 平台叢集。此設定的高級描述提供了所使用的特定方法的文檔連結。您可以參考"資源部分"。

設定過程可分為以下步驟：

▼ 從 **CLI** 在 **Azure** 上安裝 **OCP** 叢集。

- 請確保您已滿足所有規定的先決條件"這裡"。
- 建立 VPN、子網路和網路安全群組以及私人 DNS 區域。建立 VPN 閘道和網站到站台 VPN 連線。
- 為了實現本地和 Azure 之間的 VPN 連接，我們建立並配置了一個 pfSense VM。有關說明，請參閱"這裡"。
- 取得安裝方案和拉取機密，並按照文件中提供的步驟部署叢集 "這裡"。
- 叢集安裝完成，會提供一個kubeconfig檔案以及登入叢集控制台的使用者名稱和密碼。

下面給了一個範例 install-config.yaml 檔案。

```
apiVersion: v1
baseDomain: sddc.netapp.com
```

```
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
```

```
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

▼ 使用 **NetApp Console** 在 **Azure** 中部署 **Cloud Volumes ONTAP**。

- 在 Azure 中安裝 NetApp Console 代理程式。請參閱說明 "這裡"。
- 使用代理程式在 Azure 中部署 CVO 執行個體。請參閱指示 "這裡"。

使用**Trident**的 **CSI** 拓樸功能實現多區域架構

如今，雲端提供者使 Kubernetes/OpenShift 叢集管理員能夠產生基於區域的叢集節點。節點可以位於一個區域內的不同可用區，也可以跨越多個區域。為了方便在多區域架構中為工作負載配置卷， Trident使用了 CSI 拓撲。使用 CSI 拓撲功能，可以根據區域和可用區域將對磁碟區的存取限製到節點子集。參考"這裡"了解更多詳細資訊。

> Kubernetes 支援兩種磁碟區綁定模式： - 當 ***VolumeBindingMode*** 設定為 ***Immediate***（預設）時， Trident會在沒有任何拓樸感知的情況下建立磁碟區。持久性卷的建立不依賴請求 pod 的調度要求。 - 當 ***VolumeBindingMode*** 設定為 ***WaitForFirstConsumer*** 時，PVC 的持久卷的建立和綁定將被延遲，直到使用該 PVC 的 pod 被調度和建立。這樣，就可以建立磁碟區來滿足拓樸要求所強制執行的調度約束。 Trident儲存後端可設計為根據可用區域（拓撲感知後端）選擇性地配置磁碟區。對於使用此類後端的 StorageClasses，只有在受支援的區域/區域中調度的應用程式請求時才會建立磁碟區。 （拓樸感知 StorageClass）參考"這裡"了解更多詳細資訊。

使用**Trident Protect** 進行資料保護

有關使用 Trident Protect 保護和遷移容器工作負載的詳細資訊，請參閱以下章節：- "使用 Trident Protect 保護和遷移容器應用程式"

具有提供者管理元件的混合雲

具有託管 **Red Hat OpenShift** 容器平台工作負載的**NetApp**解決方案

客戶可能“誕生於雲端”，或正處於現代化歷程的某個階段，準備將部分選定的工作負載或所有工作負載從資料中心遷移到雲端。他們可以選擇在雲端中使用供應商管理的 OpenShift 容器和供應商管理的NetApp儲存體來運行他們的工作負載。他們應該在雲端中

規劃和部署託管的 Red Hat OpenShift 容器集群，以便為他們的容器工作負載提供成功的生產就緒環境。 NetApp為三大領先公有雲中的託管 Red Hat 解決方案提供完全託管的儲存產品。

Amazon FSx for NetApp ONTAP (FSx ONTAP)

FSx ONTAP為 AWS 中的容器部署提供資料保護、可靠性和靈活性。 Trident作為動態儲存供應器，為客戶的有狀態應用程式使用持久性 FSx ONTAP儲存。

由於 ROSA 可以在 HA 模式下部署，並且控制平面節點分佈在多個可用區域，因此 FSx ONTAP還可以配置多可用區選項，以提供高可用性並防止可用區故障。

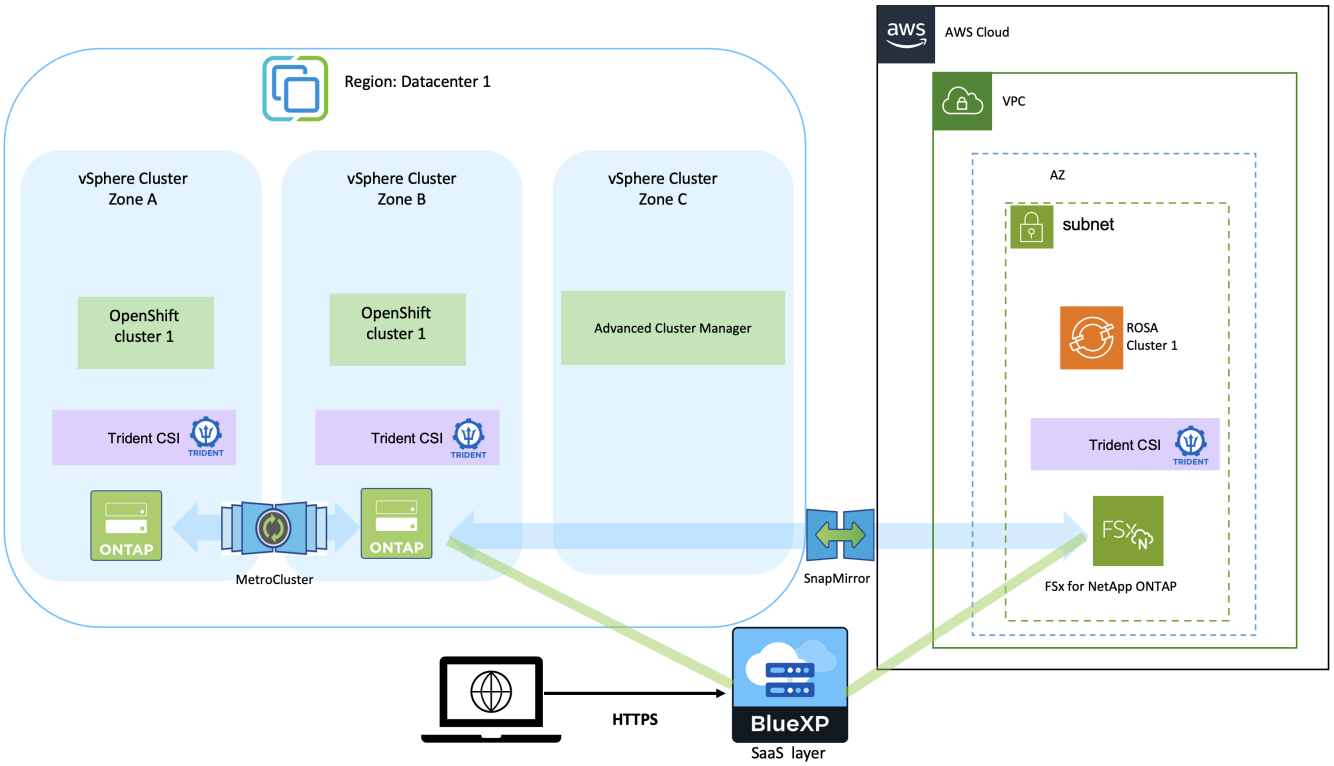
- Google Cloud NetApp Volumes*

Red Hat OpenShift Dedicated 是一個完全託管的應用程式平台，可讓您在混合雲中快速建置、部署和擴展應用程式。 Google Cloud NetApp Volumes提供持久性卷，將 ONTAP 的全套企業資料管理功能帶入 Google Cloud 中的 OpenShift 部署。

在 **AWS** 上部署和設定託管 **Red Hat OpenShift** 容器平台

本節說明在 AWS （ROSA） 上設定代管 Red Hat OpenShift 叢集的高階工作流程。它展示了 Trident 如何使用代管的 Amazon FSx for NetApp ONTAP （FSx ONTAP） 作為儲存設備後端，以提供持續性 Volume。其中提供了有關使用 NetApp Console 在 AWS 上部署 FSx ONTAP 的詳細資料。此外，也提供了有關使用 NetApp Console 和 OpenShift GitOps （Argo CD） 對 ROSA 叢集上的有狀態應用程式執行資料保護和移轉活動的詳細資料。

下圖描述了部署在 AWS 上並使用 FSx ONTAP作為後端儲存的 ROSA 叢集。



該解決方案透過在AWS的兩個VPC中使用兩個ROSA集群進行了驗證。每個 ROSA 叢集都使用Trident與 FSx ONTAP整合。在 AWS 中部署 ROSA 叢集和 FSx ONTAP有幾種方法。此設定的高級描述提供了所使用的特定方法的文檔連結。您可以參考"資源部分"。

設定過程可分為以下步驟：

安裝**ROSA**集群

- 建立兩個 VPC 並在 VPC 之間建立 VPC 對等連線。
- 請參閱"這裡"以取得安裝 ROSA 叢集的說明。

安裝 **FSx ONTAP**

- 從 NetApp Console 在 VPC 上安裝 FSx ONTAP。請參閱 "這裡" 以建立 NetApp Console 帳戶並開始使用。請參閱 "這裡" 以安裝 FSx ONTAP。請參閱 "這裡" 以在 AWS 中建立連接器來管理 FSx ONTAP。
- 使用 AWS 部署 FSx ONTAP 。參考"這裡"使用 AWS 控制台進行部署。

在 **ROSA** 叢集上安裝**Trident** （使用 **Helm** 圖表）

- 使用 Helm chart 在 ROSA 叢集上安裝 Trident。請參閱文件連結：https://docs.netapp.com/us-en/trident/trident-install/kubernetes-deploy-helm.html[此處^]。

FSx ONTAP與Trident整合用於 ROSA 集群

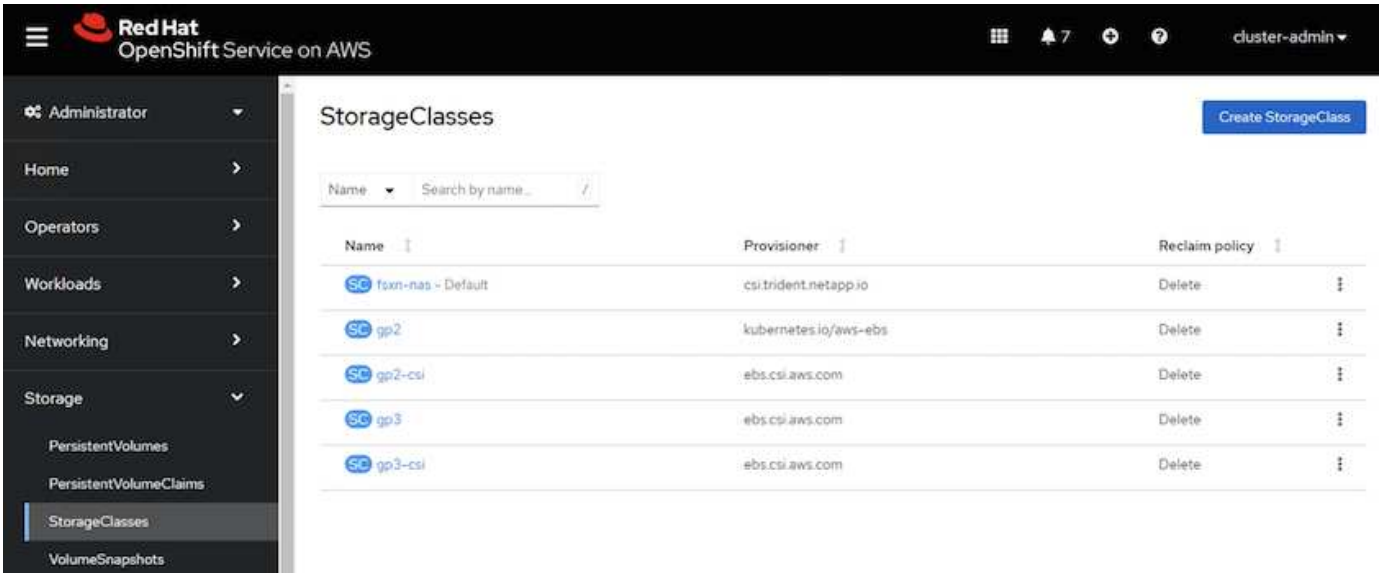
OpenShift GitOps 可用於將Trident CSI 部署到所有託管集群，因為它們使用 ApplicationSet 註冊到 ArgoCD。

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```



使用**Trident**建立後端和儲存類別（適用於 **FSx ONTAP**）

- 參考"這裡"有關建立後端和儲存類別的詳細資訊。
- 從 OpenShift 控制台將使用Trident CSI 為 FsxN 建立的儲存類別設為預設。請參閱下面的截圖：



使用 **OpenShift GitOps**（**Argo CD**）部署應用程式

- 在叢集上安裝 OpenShift GitOps 營運者。請參閱說明 "這裡"。
- SetUp 為叢集建立一個新的 Argo CD 執行個體。請參閱說明 "這裡"。

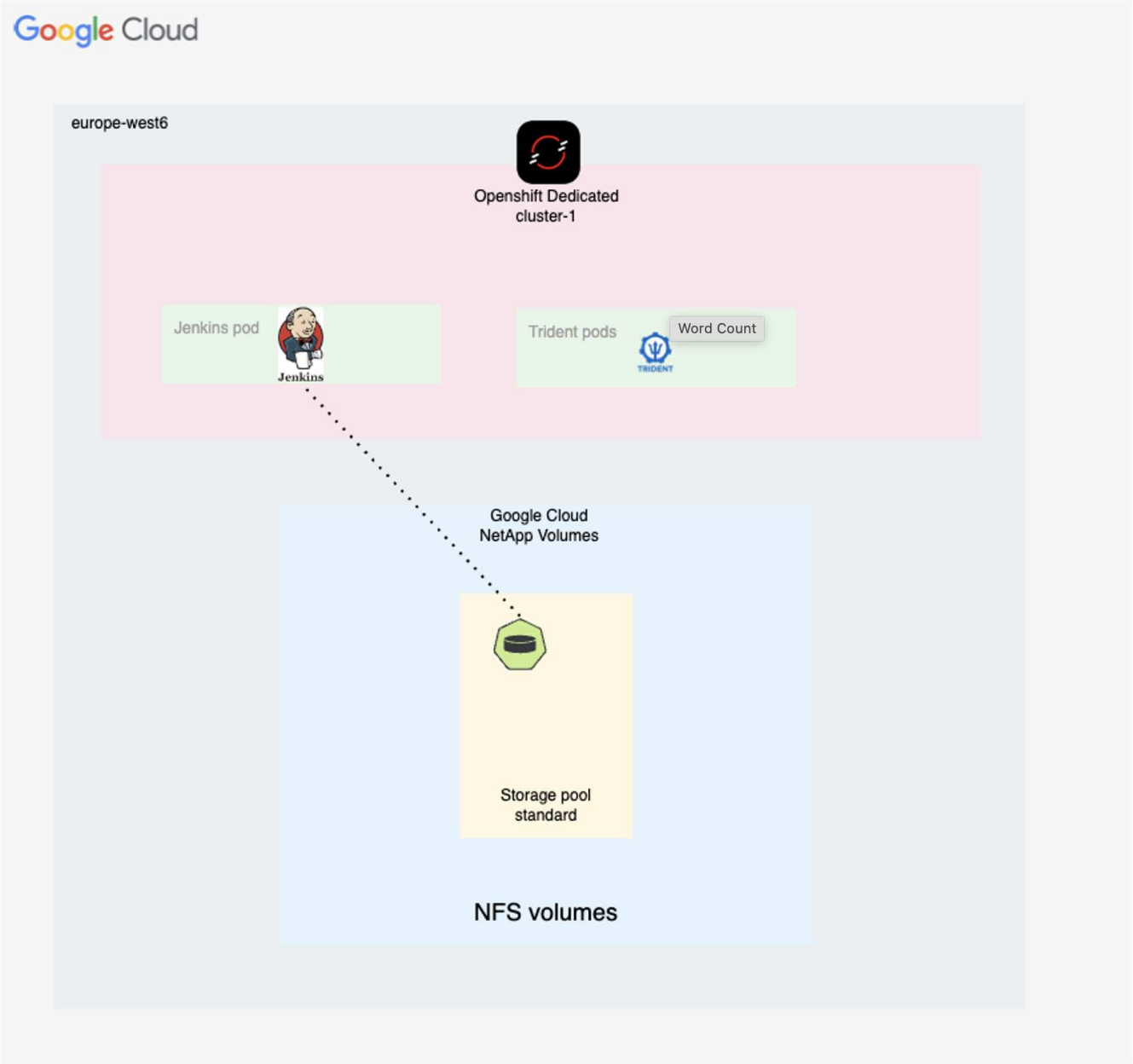
開啟 Argo CD 控制台並部署應用程式。例如，您可以使用 Argo CD 和 Helm Chart 部署 Jenkins 應用程式。建立應用程式時，提供了以下詳細資訊：專案：default；叢集：'https://kubernetes.default.svc'[]（不含引號）；命名空間：Jenkins；Helm Chart 的 URL：'https://charts.bitnami.com/bitnami'[]（不含引號）

Helm 參數：global.storageClass: fsxn-nas

使用**Google Cloud NetApp Volumes**在 **Google Cloud** 上部署和設定 **OpenShift Dedicated**

本節介紹在 Google Cloud 平台上設定 OpenShift Dedicated (OSD) 叢集的高階工作流程。它顯示NetApp Trident使用Google Cloud NetApp Volumes作為儲存後端，為使用 Kubernetes 運行的有狀態應用程式提供持久性磁碟區。

下圖描述了部署在 Google Cloud 上並使用NetApp Volumes 作為後端儲存的 OSD 叢集。



設定過程可分為以下步驟：

在 **Google Cloud** 中安裝 **OSD** 集群

- 如果您希望為叢集使用現有的 VPC，則必須為 OSD 叢集建立 VPC、兩個子網路、一個雲端路由器和兩個 GCP 雲端 NAT。參考"這裡"以取得說明。
- 請參閱 "這裡" 以取得有關使用客戶雲端訂閱（CCS）計費模式在 GCP 上安裝 OSD 叢集的指示。OSD 也已在 Google Cloud Marketplace 上架。示範如何使用 Google Cloud Marketplace 解決方案安裝 OSD 的影片位於 "這裡"。

啟用**Google Cloud NetApp Volumes**

- 參考"這裡"有關設定對Google Cloud NetApp Volumes 的存取權限的資訊。遵循所有步驟，包括
- 建立儲存池。參考"這裡"有關如何在Google Cloud NetApp Volumes上設定儲存池的資訊。將在儲存池內建立在 OSD 上執行的有狀態 Kubernetes 應用程式的磁碟區。

在 **OSD** 叢集上安裝**Trident** （使用 **Helm** 圖表）

- 使用 Helm Chart 在 OSD 叢集上安裝 Trident。請參閱"這裡"以取得如何安裝 Helm Chart 的說明。

將**NetApp Volumes** 與**NetApp Trident**整合用於 **OSD** 集群

使用Trident建立後端和儲存類別（適用於Google Cloud NetApp Volumes）

- 有關創建後端的詳細信息，請參閱此處。
- 如果 kubernetes 中的任何目前儲存類別被標記為默認，請透過編輯儲存類別來刪除該註釋。
- 使用Trident CSI 設定程式為NetApp磁碟區建立至少一個儲存類別。使用註解將其中一個儲存類別設為預設儲存類別。當 PVC 清單中未明確呼叫時，這將允許 PVC 使用此儲存類別。下面顯示了一個帶有註釋的範例。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

使用 **OpenShift GitOps**（**Argo CD**）部署應用程式

- 在叢集上安裝 OpenShift GitOps 營運者。請參閱說明 "這裡"。
- SetUp 為叢集建立一個新的 Argo CD 執行個體。請參閱說明 "這裡"。

開啟 Argo CD 控制台並部署應用程式。例如，您可以使用 Argo CD 和 Helm Chart 部署 Jenkins 應用程式。建立應用程式時，提供了以下詳細資訊：專案：default；叢集：'https://kubernetes.default.svc'[]（不含引號）；命名空間：Jenkins；Helm Chart 的 URL：'https://charts.bitnami.com/bitnami'[]（不含引號）

資料保護

有關使用 Trident Protect 保護和遷移容器工作負載的詳細資訊，請參閱以下章節：- "使用 Trident Protect 保護和遷移容器應用程式"

適用於 **Red Hat OpenShift** 工作負載的其他**NetApp**混合多雲解決方案

請參閱以下其他解決方案：

- "Red Hat OpenShift 容器解決方案（本地部署）"
- "Red Hat OpenShift Service on AWS Container 解決方案"
- "本地部署的 Red Hat OpenShift 虛擬化解決方案"

- "Red Hat OpenShift Service on AWS 虛擬化解決方案"

使用Trident Protect 保護數據

使用 Trident Protect 為 OpenShift Container Platform 中的 Container Apps 提供資料保護

本參考文件的這一部分詳細介紹如何使用 Trident Protect 建立 Container Apps 的快照和備份。NetApp Trident Protect 提供進階應用程式資料管理功能，可增強由 NetApp ONTAP 儲存系統和 NetApp Trident CSI 儲存設定器支援的有狀態 Kubernetes 應用程式的功能和可用性。Trident Protect 會建立應用程式快照和備份。這意味著，它不僅會為持久性磁碟區中的應用程式資料建立快照和備份，還會為應用程式元資料建立快照和備份。Trident Protect 建立的快照和備份可以儲存在以下任何物件儲存中，並可在以後從中還原。

- AWS S3
- Azure Blob 儲存
- Google 雲端儲存
- ONTAP S3
- 儲存網格
- 任何其他與 S3 相容的儲存設備

Trident Protect 使用 Kubernetes 的角色型存取控制（RBAC）模型。預設情況下，Trident Protect 提供一個名為 trident-protect 的系統命名空間及其關聯的預設服務帳戶。如果您的組織擁有眾多使用者或有特定的安全需求，則可以使用 Trident Protect 的 RBAC 功能來更精細地控制對資源和命名空間的存取。

有關 Trident Protect 中 RBAC 的其他資訊、請參閱"Trident Protect 說明文件"

> 叢集管理員可以存取預設的 trident-protect 命名空間中的資源，也可以存取所有其他命名空間中的資源。使用者無法在 trident-protect 命名空間中建立應用程式資料管理自訂資源 (CR)，如快照和備份 CR。作為最佳實踐，使用者需要在應用程式命名空間中建立這些 CR。

Trident Protect 可使用文件中提供的說明安裝"這裡"。本節將介紹使用 Trident Protect 對容器應用程式進行資料保護和復原的工作流程。1.建立快照（按需或排程）2.從快照還原（還原到相同或不同的命名空間）3.建立備份 4.從備份還原

▼ 先決條件

在為應用程式建立快照和備份之前，必須在 Trident Protect 中配置物件儲存以儲存快照和備份。此配置透過儲存桶 CR 完成。只有管理員才能建立和配置儲存桶 CR。在 Trident Protect 中，儲存桶 CR 稱為 AppVault。AppVault 物件是儲存桶的聲明式 Kubernetes 工作流程表示。AppVault CR 包含儲存桶在保護作業（例如備份、快照、復原作業和 SnapMirror 複製）中所需的設定。

在本範例中，我們將展示如何使用 ONTAP S3 作為物件儲存。以下是為 ONTAP S3 建立 AppVault CR 的工作流程：1.在 ONTAP 叢集的 SVM 中建立 S3 物件儲存伺服器。2.在物件儲存伺服器中建立儲存桶。3.在 SVM 中建立 S3 使用者。將存取金鑰和私密金鑰保存在安全的位置。4.在 OpenShift 中，建立密鑰來儲存 ONTAP S3 憑證。5.為 ONTAP S3 建立 AppVault 物件

為 **ONTAP S3** 設定 **Trident Protect AppVault**

用於設定 **Trident Protect** 與 **ONTAP S3** 作為 **AppVault** 的範例 **YAML** 檔案

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
```

```
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

用於安裝 **postgresql** 應用程式的範例 **yaml** 檔案

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
```

```
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ 建立快照

建立按需快照

```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+----------------+--------------+-----------+-----+-------+
|      NAME      |   APP REF    |   STATE   | AGE | ERROR |
+----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```

```
[root@localhost DataProtection]# oc get all,pvc,volumesnapshot -n postgres
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
Warning: kubevirt.io/v1 VirtualMachineInstancePresets is now deprecated and will be removed in v2.
NAME                            READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-jfx49     1/1     Running   0          3h47m

NAME               TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/postgres   ClusterIP   172.30.132.112   <none>        5432/TCP   3h47m

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/postgres   1/1     1            1           3h47m

NAME                                  DESIRED   CURRENT   READY   AGE
replicaset.apps/postgres-cd9d6ccb     1         1         1       3h47m

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAG
ECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   8Gi        RWO            sc-zon
ea-nas   <unset>                 4h40m
persistentvolumeclaim/postgres-pvc                 Bound    pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   5Gi        RWO            sc-zon
ea-nas   <unset>                 3h47m

NAME                                                                                                                                READYTO
USE   SOURCEPVC                   SOURCESNAPSHOTCONTENT   RESTORESIZE   SNAPSHOTCLASS           SNAPSHOTCONTENT
            CREATIONTIME   AGE
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true
      postgres-pvc                                          53676Ki       trident-snapshotclass   snapcontent-796ea7f8-59a0-493e-bbd8-3a
e76fe9036c   13m            13m
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true
      data-postgres-postgresql-0                            368Ki         trident-snapshotclass   snapcontent-86a464d4-ffd8-4279-9cf7-88
88a097c001   13m            13m
```

建立計畫 使用以下命令，將每天 15:33 建立快照，並保留兩個快照和備份。

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+-----+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE | ERROR |
+-----------+--------------+----------------------+---------+-------+-----+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 17s |       |
+-----------+--------------+----------------------+---------+-------+-----+-------+
[root@localhost DataProtection]#
```

使用 **yaml** 建立計劃

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
```

```
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

您可以看到按照此計劃建立的快照。

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

也創建了磁碟區快照。

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                  READYTOUSE   SOURCEPVC
                                CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ 刪除應用程式以模擬應用程式遺失

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ 從快照還原到相同命名空間

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

應用程式及其 PVC 恢復到同一個命名空間。

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                     READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                 Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ 從快照還原到不同的命名空間

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-
3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n
postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |      APPVAULT      |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

您可以看到應用程式已還原到新的命名空間。

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                  Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ 建立備份

建立按需備份

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+-----------------------------+--------------+-----------+--------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+-----------------------------+--------------+-----------+--------+-------+
| backup1                     | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300  | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300  | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1            | postgres-app | Completed | 6m19s  |       |
+-----------------------------+--------------+-----------+--------+-------+
```

建立備份計畫

上面列表中的每日和每小時備份是根據先前設定的計劃建立的。

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily --hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ 從備份中恢復

刪除應用程式和 **PVC** 以模擬資料遺失。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

恢復到相同的命名空間 #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir" created。

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

應用程式和 PVC 在同一個命名空間中恢復。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w     1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                  Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

恢復到不同的命名空間 建立一個新的命名空間。從備份還原到新的命名空間。

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                      READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p   1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                 Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ 遷移應用程式

若要將應用程式複製或遷移到不同的叢集（執行跨叢集克隆），請在來源叢集上建立備份，然後將備份還原到不同的叢集。請確保目標叢集上已安裝 Trident Protect。

在來源叢集上，執行下圖所示的步驟：

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

從來源集群，將上下文切換到目標集群。然後，確保可以從目標群集上下文存取 AppVault，並從目標群集取得 AppVault 內容。

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+---------------+--------------+--------+----------------------------+--------------------------+-----------------------------------
-----------------------------------------------------------------------------------------------+
|    CLUSTER    |     APP      |  TYPE  |            NAME            |        TIMESTAMP         |
                      PATH                                                                     |
+---------------+--------------+--------+----------------------------+--------------------------+-----------------------------------
-----------------------------------------------------------------------------------------------+
| ocp-cluster11 | bbox         | backup | bboxbackup1                | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                                  |
| ocp-cluster11 | postgres-app | backup | backup1                    | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3                              |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300 | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd           |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300 | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d           |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc           |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031           |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1   | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3             |
```

使用清單中的備份路徑並建立備份還原 CR 對象，如下面的命令所示。

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|           NAME           |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

現在您可以看到應用程式 pod 和 PVC 已在目標叢集中建立。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                    READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                  Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

使用 **Trident Protect** 保護 **Red Hat OpenShift Virtualization** 中的虛擬機

使用快照和備份保護 OpenShift Virtualization 中的 VM。此程序包括使用 ONTAP S3 物件

儲存建立 AppVault、配置 Trident Protect 以擷取 VM 資料（包括 Kubernetes 資源物件、持續性磁碟區和內部映像），並在必要時還原資料。

OpenShift 虛擬化環境中的虛擬機器是在 OpenShift 容器平台的工作節點中執行的容器化應用程式。保護虛擬機器元資料以及虛擬機器的持久性磁碟非常重要，以便在它們遺失或損壞時可以還原它們。

OpenShift Virtualization VM 的持續磁碟可由使用 "Trident犯罪現場調查" 整合至 OpenShift 叢集的 ONTAP 儲存設備提供支援。在本節中、我們使用 "Trident Protect" 建立 VM 的快照和備份、包括其資料磁碟區至 ONTAP 物件儲存設備。

然後，我們在需要時從快照或備份中還原。

Trident Protect 支援對 OpenShift 叢集上的應用程式和虛擬機器進行快照、備份、還原和災難復原。對於 OpenShift Virtualization 虛擬機器，Trident Protect 可保護的資料包括與虛擬機器關聯的 Kubernetes 資源物件、持久磁碟區和內部鏡像。

以下是本節範例所使用的各個元件的版本

- "OpenShift 叢集 4.17"
- "透過 Red Hat 提供的 OpenShift Virtualization Operator 安裝 OpenShift Virtualization"
- "Trident25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

建立物件儲存的 **AppVault**

▼ 建立 **AppVault**

在為應用程式或虛擬機器建立快照和備份之前，必須在 Trident Protect 中配置物件儲存以儲存快照和備份。此配置透過儲存桶 CR 完成。只有管理員才能建立和配置儲存桶 CR。在 Trident Protect 中，儲存桶 CR 稱為 AppVault。AppVault 物件是儲存桶的聲明式 Kubernetes 工作流程表示。AppVault CR 包含儲存桶在保護作業（例如備份、快照、復原作業和 SnapMirror 複製）中所需的設定。

在本範例中、我們將展示如何使用 ONTAP S3 作為物件儲存設備。以下是為 ONTAP S3 建立 AppVault CR 的工作流程：1.在 ONTAP 叢集的 SVM 中建立 S3 物件存放區伺服器。2.在物件存放區伺服器中建立儲存區。3.在 SVM 中建立 S3 使用者。將存取金鑰和秘密金鑰保存在安全的位置。4.在 OpenShift 中、建立密碼以儲存 ONTAP S3 認證資料。5.為 ONTAP S3 建立 AppVault 物件

為 **ONTAP S3** 設定 **Trident Protect AppVault**

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
```

```
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+--------------------+----------+-----------+-------+---------+-------+
|        NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+--------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault  | OntapS3  | Available |       |         | 8d17h |
+--------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

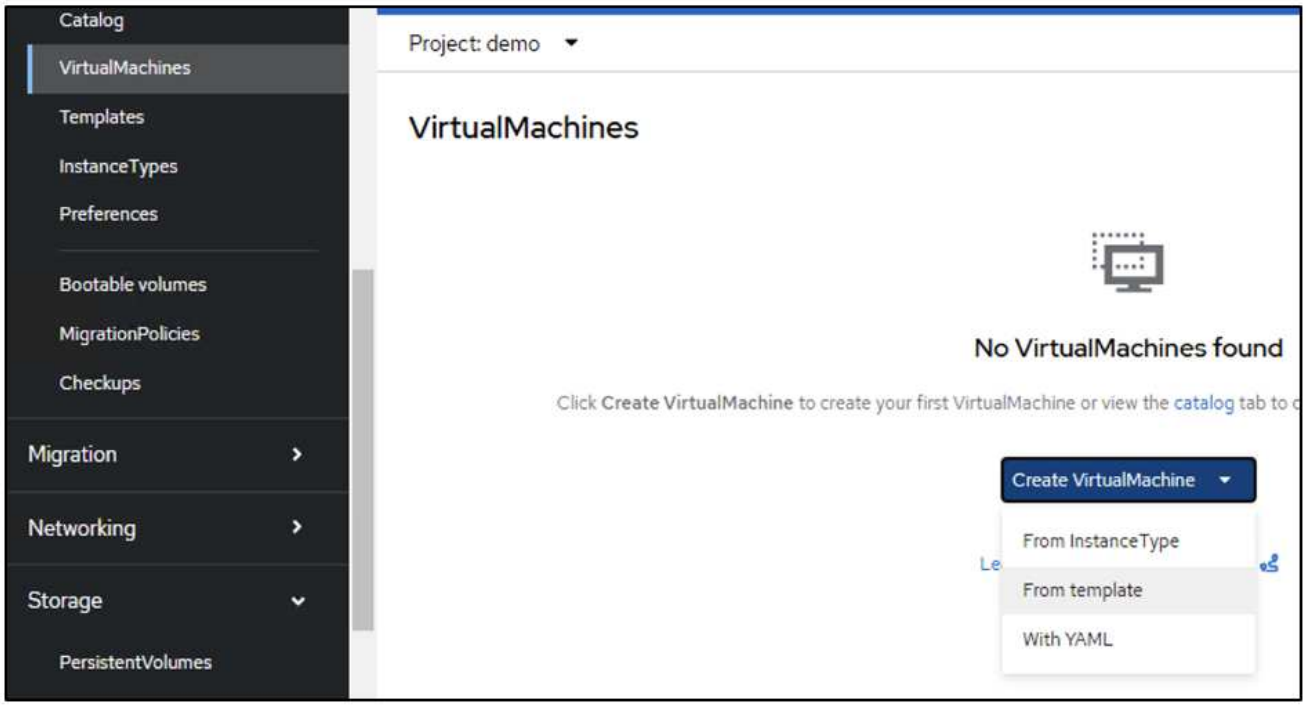
在 **OpenShift Virtualization** 中建立 **VM**

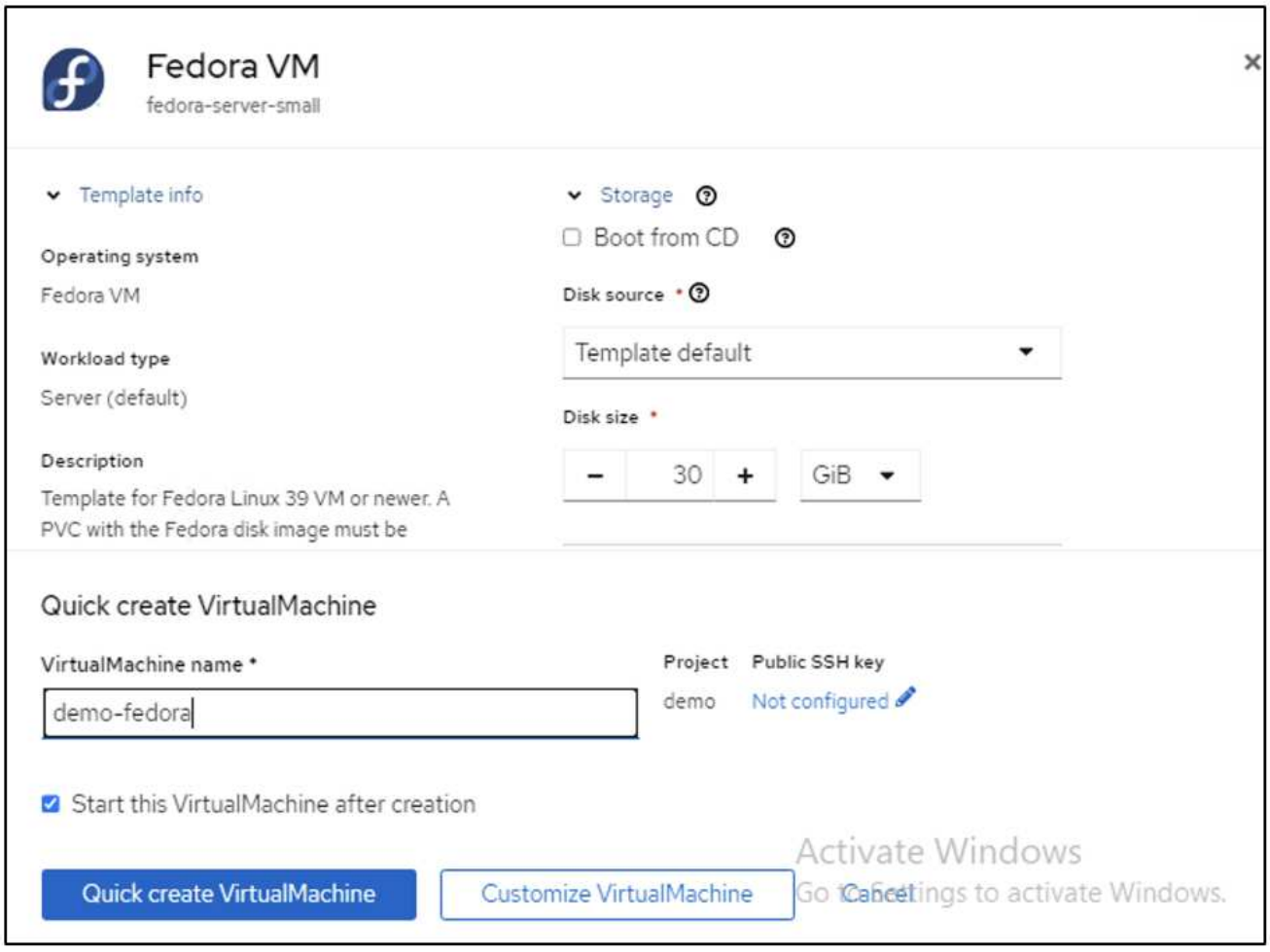
▼ 在 **OpenShift Virtualization** 中建立 **VM**

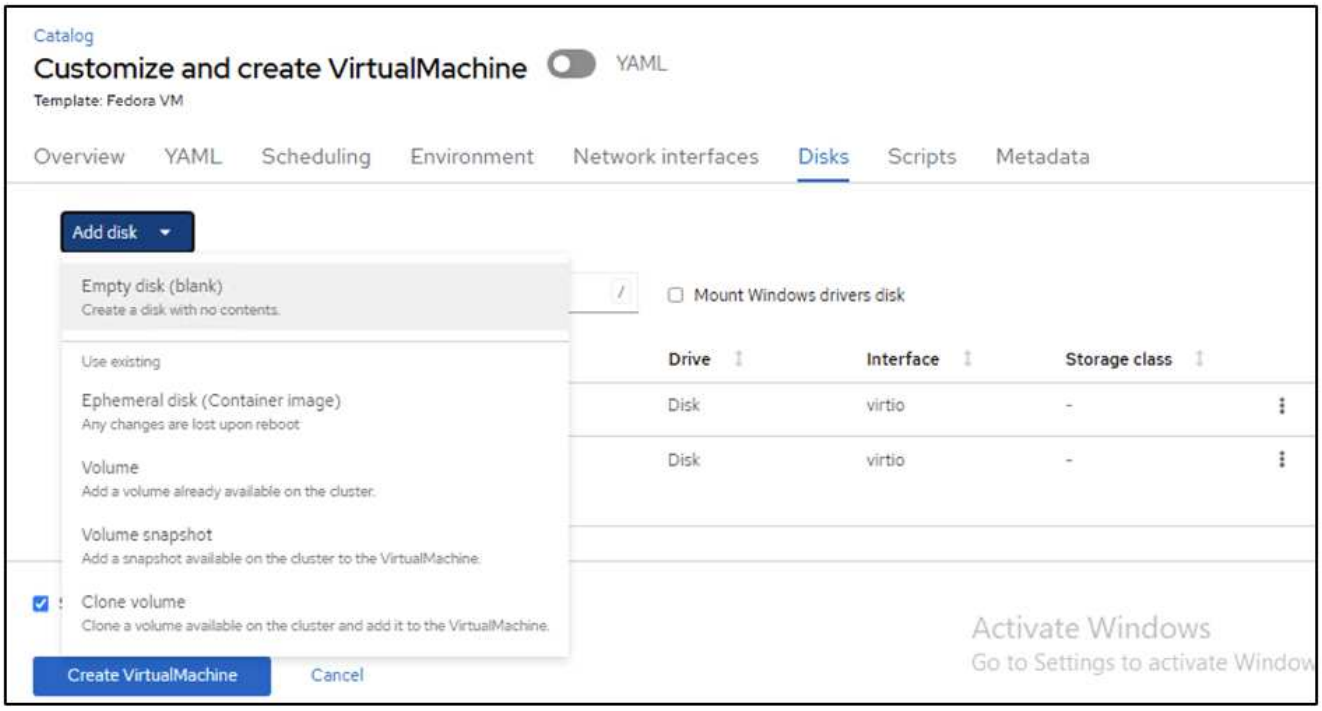
以下螢幕截圖顯示了使用模板從控制台建立 VM（命名空間 demo 中的 demo-fedora）。根磁碟會自動選擇預設儲存類別，因此，請驗證預設儲存類別是否設定得當。在此設定中，預設儲存類別是**sc-zonea-san**。確保在建立附加磁碟時選擇儲存類別 sc-zonea-san 並選取「應用最佳化儲存設定」複選框。這會將存取模式設為 RWX，將磁碟區模式設為封鎖。

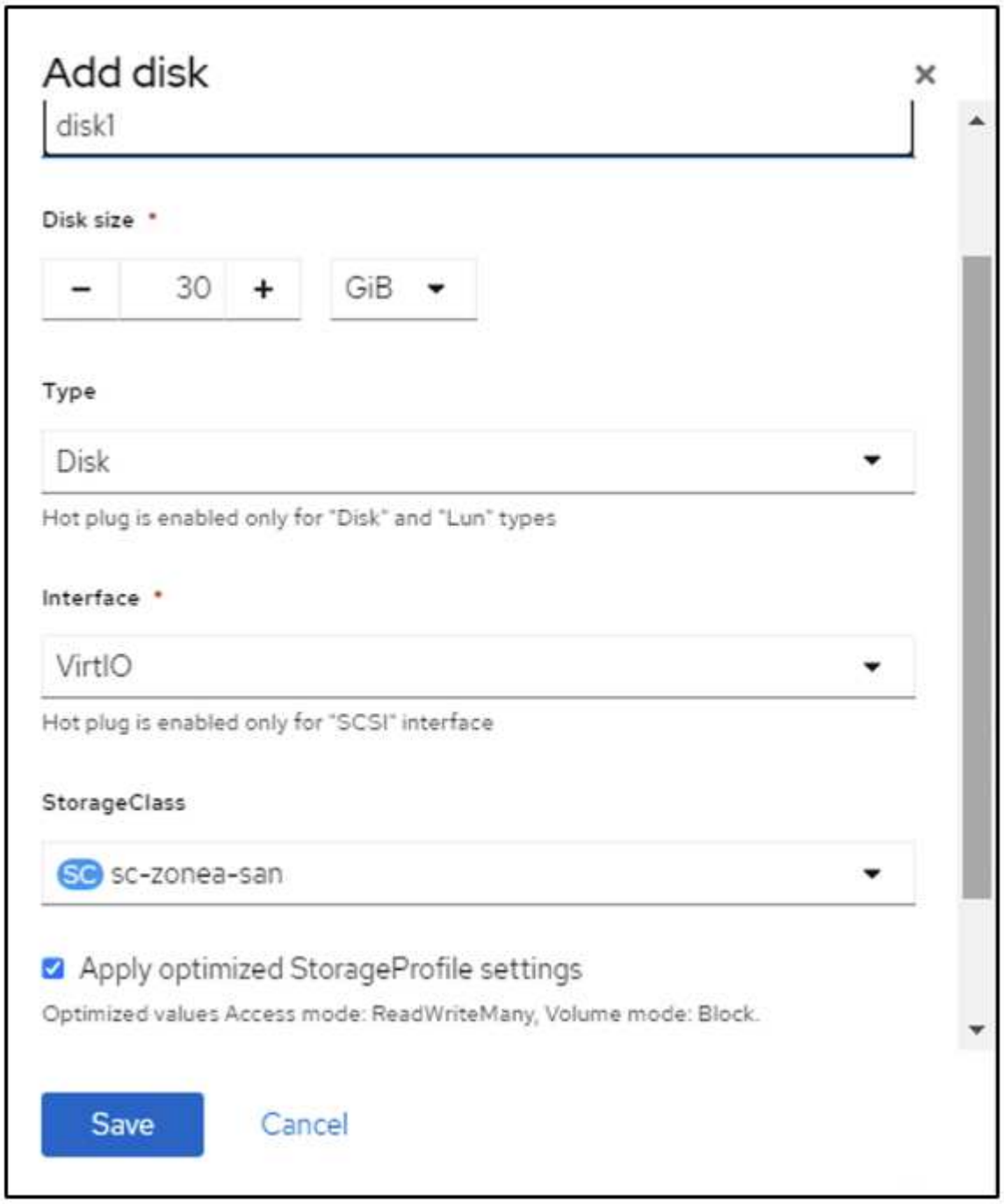
> Trident支援 SAN（iSCSI、NVMe/TCP 和 FC）區塊磁碟區模式下的 RWX 存取模式。 （這是NAS的預設存取模式）。如果您稍後需要對虛擬機器進行即時遷移，則需要 RWX 存取模式。

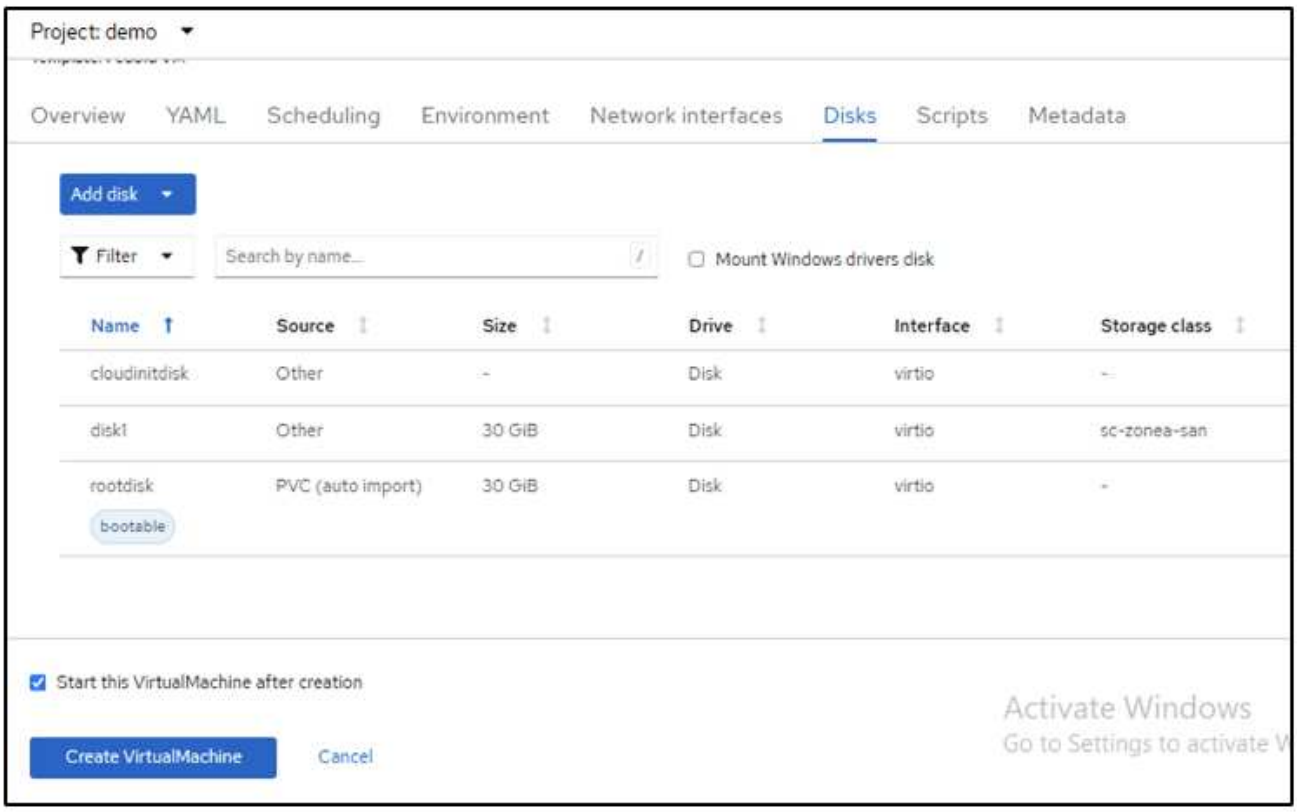



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Quick create VirtualMachine
Customize VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows.


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

創建應用程式

▼ 創建應用程式

為虛擬機器建立 **Trident Protect** 應用程式

在此範例中、demo 命名空間有一個 VM、建立應用程式時會包含該命名空間的所有資源。

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
  namespace: demo
```

```
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

透過建立備份來保護應用程式

▼ 建立備份

建立按需備份

為先前建立的應用程式（demo-vm）建立一個備份，其中包括 demo 命名空間中的所有資源。提供將儲存備份的 appvault 名稱。

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

按計畫建立備份

建立備份計劃，指定要保留的備份粒度和數量。

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

從備份還原

▼ 從備份還原

將虛擬機器還原到相同的命名空間

在範例中，備份 demo-vm-backup-on-demand 包含 fedora VM 的 demo-app 備份。

首先，刪除虛擬機，並確保 PVC、pod 和虛擬機物件從命名空間「demo」中刪除

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                 STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

現在，建立一個就地備份還原物件。

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

驗證虛擬機器、Pod 和 PVC 是否已恢復

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

將虛擬機器還原到不同的命名空間

首先建立一個要將應用程式還原到的新命名空間，在本例中為 demo2。然後建立備份還原對象

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  conditions: null
```

```
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

驗證是否在新命名空間 demo2 中建立了 VM、pod 和 pvc。

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

使用快照保護應用程式

▼ 建立快照

建立按需快照 為應用程式建立快照並指定需要儲存它的 appvault。

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
```

```
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

為快照建立計劃 為快照建立計劃。指定粒度和要保留的快照數量。

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-------------------------------------------+---------+----------------+-----------+-------+--------+
|                   NAME                    |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand                 | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000               | demo-vm | Delete         | Completed |       | 1m29s  |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

從快照還原

▼ 從快照還原

將虛擬機器從快照還原到同一個命名空間 從 demo2 命名空間中刪除虛擬機器 demo-fedora。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

從虛擬機器的快照建立快照就地還原物件。

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
```

```
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+-----------------------------------+-------------------+-----------+-------+--------+
|               NAME                |     APPVAULT      |   STATE   | ERROR |  AGE   |
+-----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+-----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

驗證虛擬機器及其 PVC 是否在 demo 命名空間中建立。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                  STATUS   VOLUME
persistentvolumeclaim/demo-fedora                     Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

將虛擬機器從快照還原到不同的命名空間

刪除先前從備份中還原的 demo2 命名空間中的虛擬機器。

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                     Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                     Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

從快照建立快照還原物件並提供命名空間映射。

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-----------------------------------+------------------+-----------+-------+--------+
|                NAME               |     APPVAULT     |   STATE   | ERROR |  AGE   |
+-----------------------------------+------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-----------------------------------+------------------+-----------+-------+--------+
```

驗證虛擬機器及其 PVC 是否在新的命名空間 demo2 中復原。

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                      STATUS   VOLUME
STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                         Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san     <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87     Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san     <unset>                 29h
[root@localhost RedHat]#
```

恢復特定虛擬機

▼ 選擇命名空間中的特定虛擬機器來建立快照/備份和還原

在前面的例子中，我們在命名空間內有一個虛擬機器。透過將整個命名空間包含在備份中，可以擷取與該虛擬機器相關的所有資源。在下面的範例中，我們將另一個 VM 新增到同一個命名空間，並使用標籤選擇器為這個新 VM 建立一個應用程式。

在 **demo** 命名空間中建立一個新的虛擬機器（**demo-centos vm**）

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora    81m     Running   True

NAME                                  READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g   1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          81m

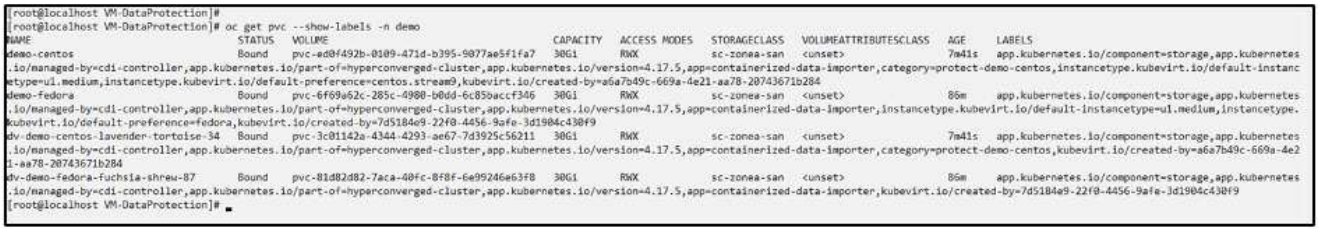
NAME                                                      STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                         Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                         Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87     Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

標記 **demo-centos vm** 及其相關資源

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

驗證 **demo-centos vm** 和 **pvcs** 是否已取得標籤

```
[root@localhost VM-DataProtection]# oc get vm --show-labels -n demo
NAME          AGE     STATUS    READY   LABELS
demo-centos   6m31s   Running   True    app=demo-centos,category=protect-demo-centos,kubevirt.io/dynamic-credentials-support=true,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=centos-stream9-server-small
demo-fedora   85m     Running   True    app=demo-fedora,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=fedora-server-small
[root@localhost VM-DataProtection]#
```



使用標籤選擇器僅為特定虛擬機器（**demo-centos**）建立應用程式

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+-----------------+------------+-------+------+
|      NAME       | NAMESPACES | STATE | AGE  |
+-----------------+------------+-------+------+
| demo-centos-app | demo       | Ready | 56s  |
| demo-vm         | demo       | Ready | 4h6m |
+-----------------+------------+-------+------+
```

按需和按計劃建立備份和快照的方法與前面所示的相同。由於用於建立快照或備份的 trident-protect 應用程式僅包含來自命名空間的特定 VM，因此從它們還原只會還原特定的 VM。下面顯示了一個備份/復原作業的範例。

使用其對應的應用程式建立命名空間中特定虛擬機器的備份

在前面的步驟中，使用標籤選擇器建立了一個應用程序，以僅包含演示命名空間中的 centos vm。為此應用程式建立備份（在本例中為按需備份）。

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+------------------------------+-----------------+----------------+-----------+-------+--------+
|             NAME             |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand     | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500  | demo-vm         | Retain         | Completed |       | 56m17s |
+------------------------------+-----------------+----------------+-----------+-------+--------+
```

將特定的 **VM** 還原到同一個命名空間 使用對應的應用程式建立了特定的 VM（centos）的備份。如果從此建立了備份就地恢復或備份恢復，則僅還原此特定的 VM。刪除 Centos VM。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora    4m27s   Running   True

NAME                                                        STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                           Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                           Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    5m17s   Running   True

NAME                                                        STATUS   VOLUME
persistentvolumeclaim/demo-fedora                           Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

從 demo-centos-backup-on-demand 建立備份就地還原並驗證 centos VM 是否已重新建立。

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-
demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore  | ontap-s3-appvault  | Completed |       | 57m9s |
| demo-fedora-restore  | ontap-s3-appvault  | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

將特定的 **VM** 還原到不同的命名空間 從 demo-centos-backup-on-demand 建立到不同命名空間 (demo3) 的備份恢復，並驗證 centos VM 是否已重新建立。

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-
demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault  | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

影片示範

以下影片示範如何使用快照保護虛擬機

保護虛擬機

使用第三方工具保護容器應用

使用 **OpenShift API for Data Protection (OADP)** 為 **OpenShift Container Platform** 中的容器應用程式提供資料保護

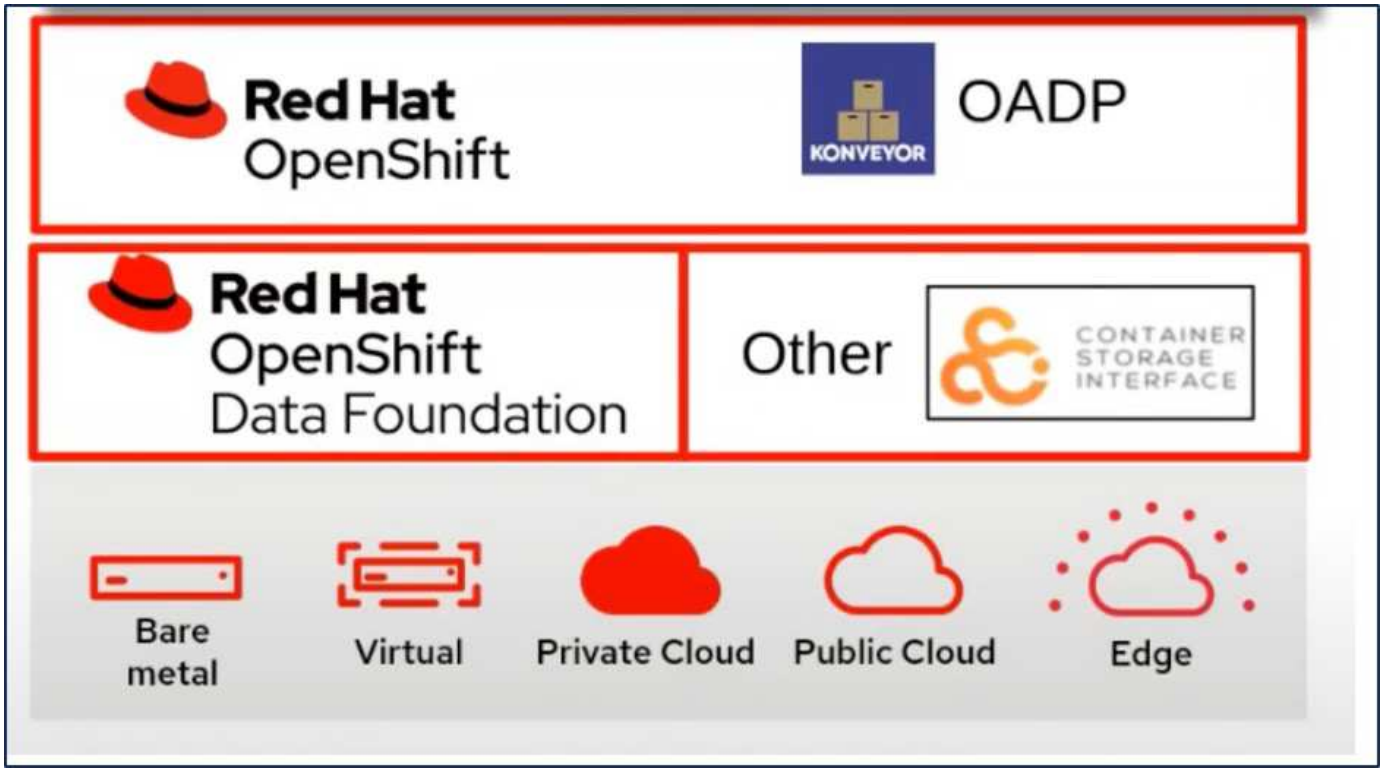
參考文件的此部分提供了在NetApp ONTAP S3 或NetApp StorageGRID S3 上使用 Velero 的 OpenShift API for Data Protection (OADP) 建立容器應用程式備份的詳細資訊。使用 CSI Trident Snapshots 建立應用程式的命名空間範圍資源（包括持久性磁碟區 (PV)）的備份。

Container 應用程式的持續儲存可由使用 "Trident犯罪現場調查" 整合至 OpenShift 叢集的 ONTAP 儲存設備提供支援。在本節中，我們使用 "OpenShift 資料保護 API (OADP)" 將應用程式（包括其資料磁碟區）備份至

- ONTAP物件存儲
- 儲存網格

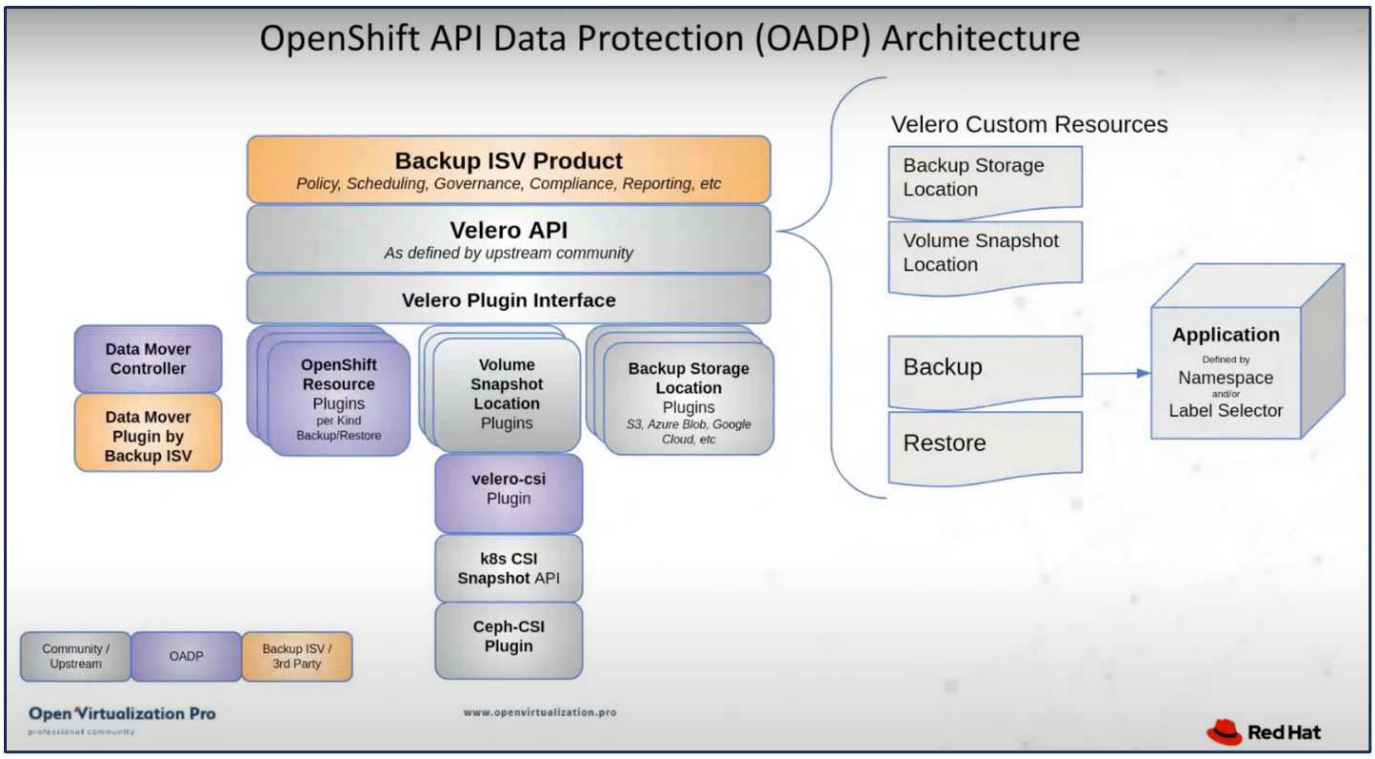
然後我們在需要時從備份中恢復。請注意，應用程式只能還原到已建立備份的叢集。

OADP 支援 OpenShift 叢集上應用程式的備份、還原和災難復原。可以使用 OADP 保護的資料包括 Kubernetes 資源物件、持久磁碟區和內部映像。



Red Hat OpenShift 利用開源社群開發的解決方案來保護資料。"維萊羅"是一個開源工具，用於安全地備份和復

原、執行災難復原以及遷移 Kubernetes 叢集資源和持久磁碟區。為了輕鬆使用 Velero，OpenShift 開發了 OADP 操作符和 Velero 插件以與 CSI 儲存驅動程式整合。所公開的 OADP API 的核心是基於 Velero API。安裝 OADP 操作器並配置後，可以執行的備份/復原作業是基於 Velero API 公開的操作。



OADP 1.3 可從 OpenShift 叢集 4.12 及更高版本的操作員中心取得。它有一個內建的資料移動器，可以將 CSI 磁碟區快照移至遠端物件儲存。透過在備份期間將快照移至物件儲存位置，這提供了可移植性和耐用性。災難發生後，快照可用於復原。

以下是本節範例所使用的各個元件的版本

- OpenShift 叢集 4.14
- Red Hat 提供的 OADP Operator 1.13
- 適用於 Linux 的 Velero CLI 1.13
- Trident24.02
- ONTAP 9.12
- 使用 helm 安裝 postgresql。

"Trident犯罪現場調查" "OpenShift 資料保護 API (OADP)" "維萊羅"

OpenShift API for Data Protection (OADP) Operator 的安裝

本節概述了 OpenShift API for Data Protection (OADP) Operator 的安裝。

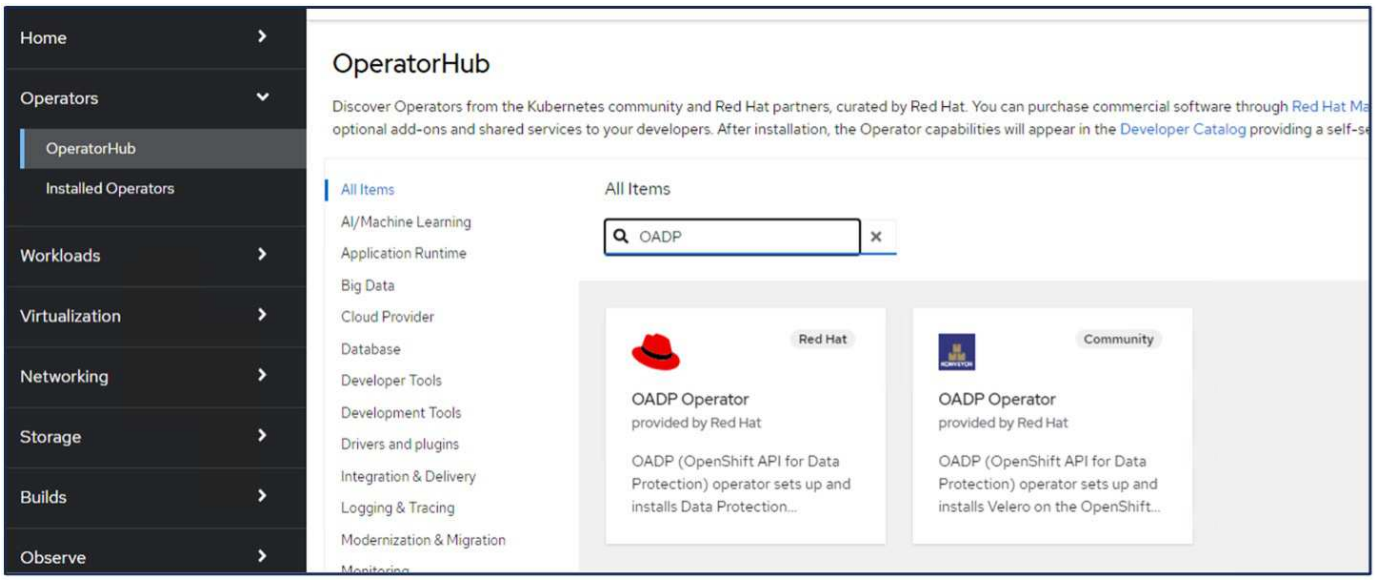
先決條件

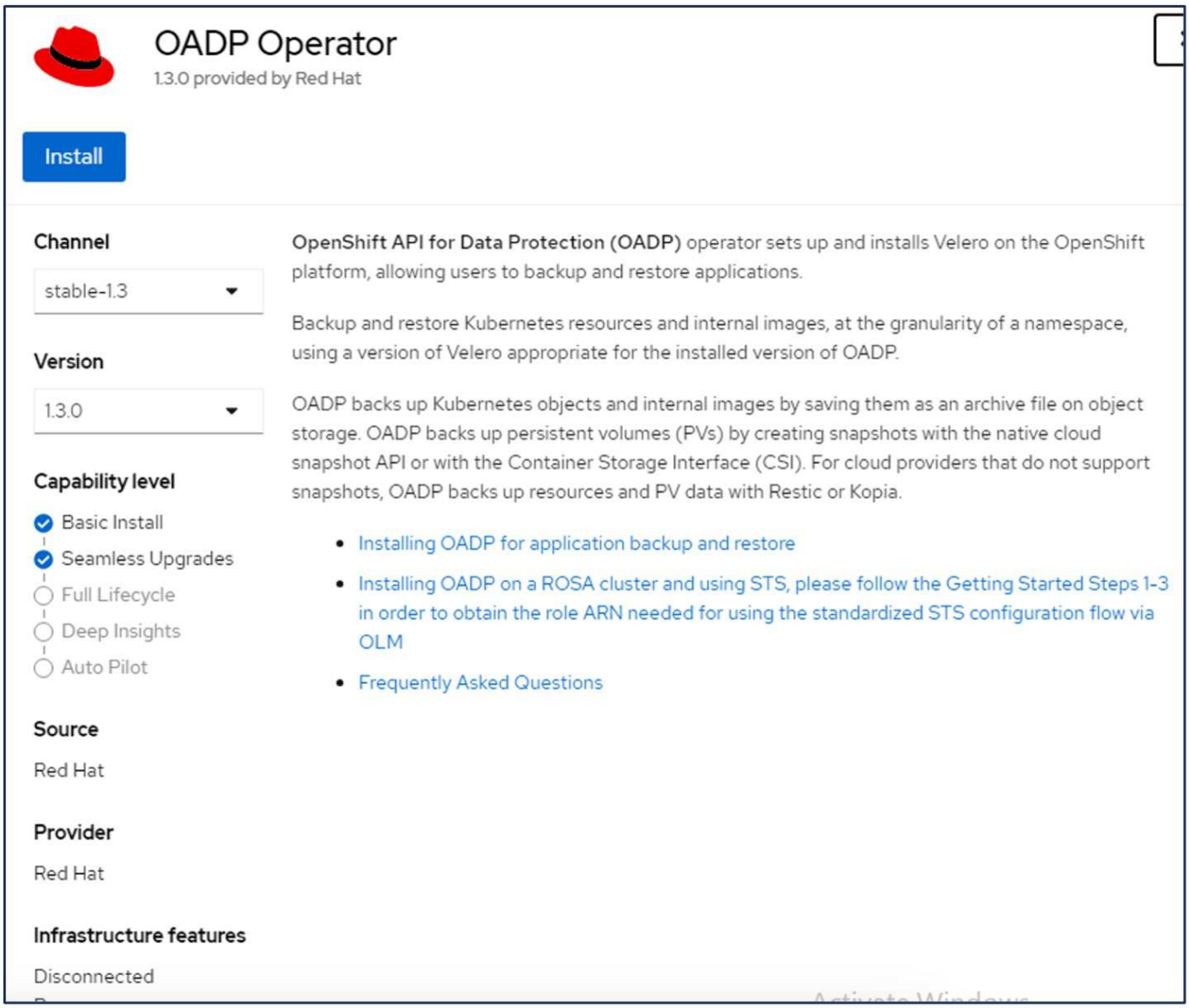
- 安裝在裸機基礎架構上並帶有 RHCOS 工作節點的 Red Hat OpenShift 叢集（高於 4.12 版本）
- 使用Trident與叢集整合的NetApp ONTAP叢集

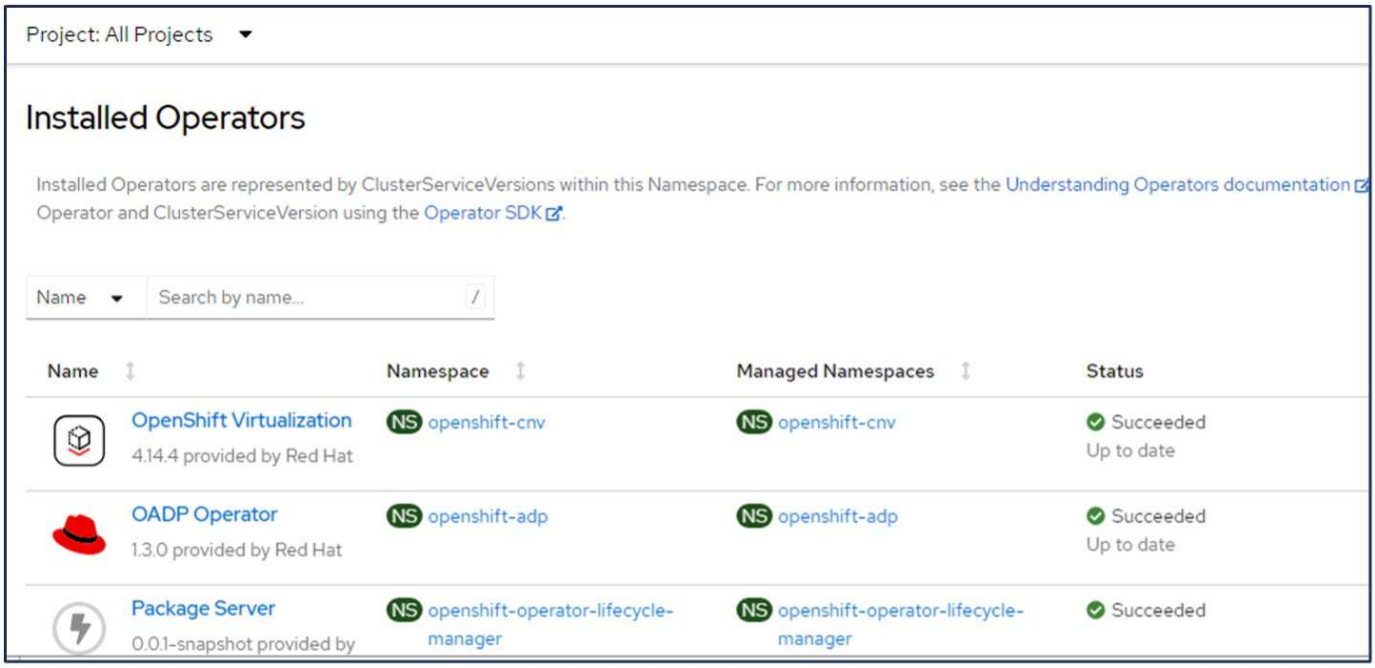
- 在ONTAP叢集上設定了 SVM 的Trident後端
- 在 OpenShift 叢集上設定 StorageClass，並使用Trident作為配置器
- 在叢集上建立的Trident Snapshot 類
- 叢集管理員存取 Red Hat OpenShift 叢集
- NetApp ONTAP叢集的管理員存取權限
- 部署在叢集上的應用程序，例如 postgresql
- 安裝了 tridentctl 和 oc 工具並新增至 $PATH 的管理員工作站

安裝 **OADP Operator** 的步驟

1. 進入叢集的 Operator Hub，選擇 Red Hat OADP 操作員。在安裝頁面中，使用所有預設選擇並按一下安裝。在下一頁上，再次使用所有預設設定並點擊“安裝”。 OADP 操作員將安裝在命名空間 openshift-adp 中。




OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions


Project: All Projects
Installed Operators
Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation
Operator and ClusterServiceVersion using the Operator SDK
Name
Search by name...
Name
Namespace
Managed Namespaces
Status
OpenShift Virtualization
4.14.4 provided by Red Hat
openshift-cnv
openshift-cnv
Succeeded
Up to date
OADP Operator
1.3.0 provided by Red Hat
openshift-adp
openshift-adp
Succeeded
Up to date
Package Server
0.0.1-snapshot provided by
openshift-operator-lifecycle-manager
openshift-operator-lifecycle-manager
Succeeded

使用 **Ontap S3** 詳細資訊進行 **Velero** 配置的先決條件

操作員安裝成功後，配置Velero的實例。 Velero 可以配置為使用 S3 相容的物件儲存。使用所示步驟設定ONTAP S3"ONTAP文件的物件儲存管理部分" 。您將需要ONTAP S3 配置中的以下資訊才能與 Velero 整合。

- 可用於存取 S3 的邏輯介面 (LIF)
- 存取 S3 的使用者憑證，包括存取金鑰和秘密存取金鑰
- S3 中用於備份的儲存桶名稱，具有使用者存取權限
- 為了安全存取物件存儲，應在物件儲存伺服器上安裝 TLS 憑證。

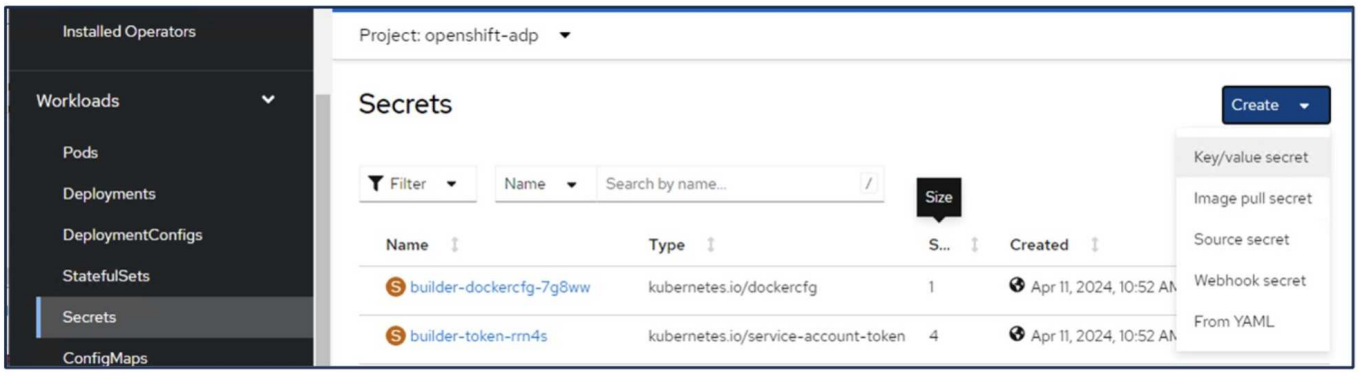
使用 **StorageGrid S3** 詳細資訊進行 **Velero** 配置的先決條件

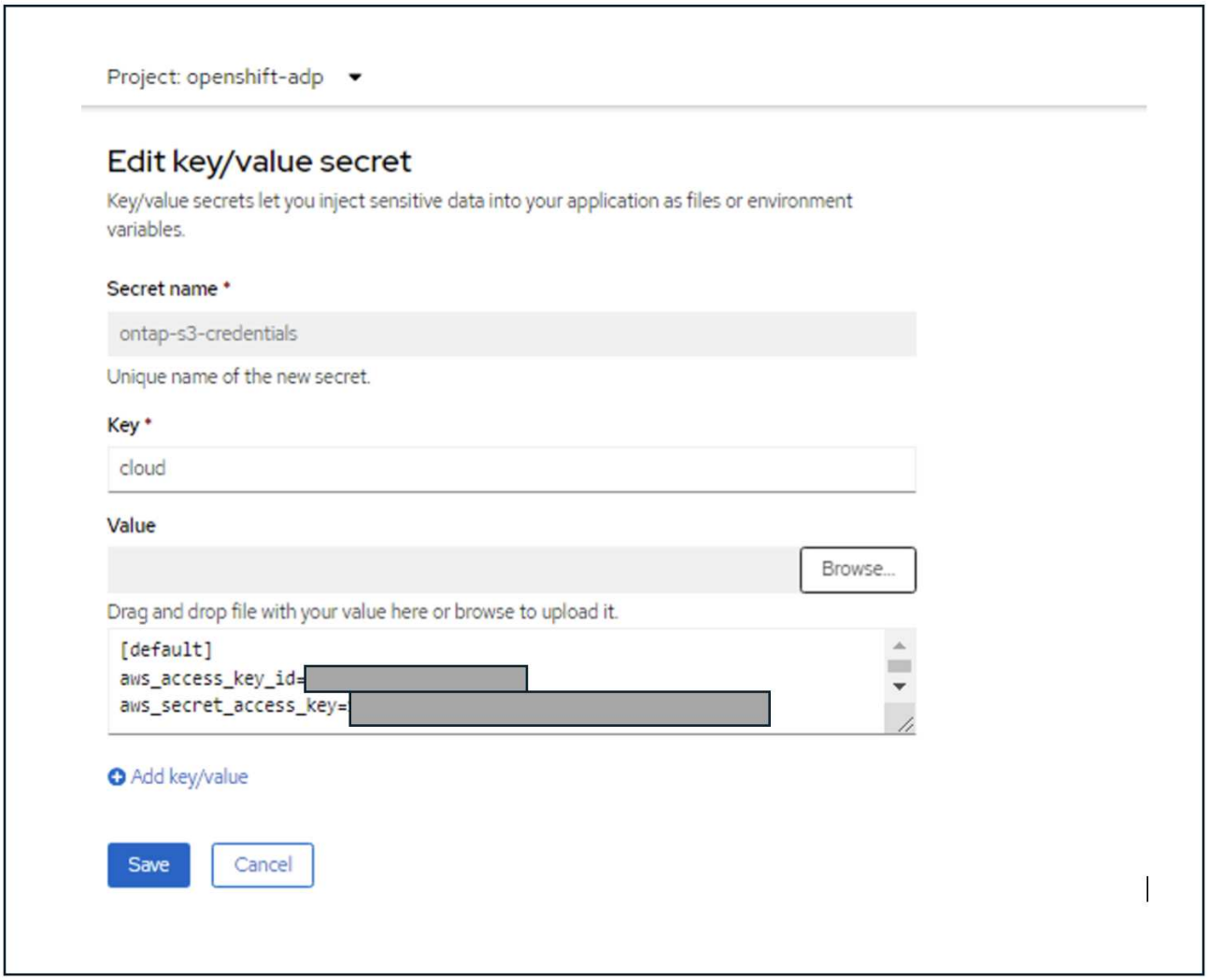
Velero 可以配置為使用 S3 相容的物件儲存。您可以使用以下所示的步驟來配置 StorageGrid S3"StorageGrid 文檔" 。您將需要 StorageGrid S3 配置中的以下資訊才能與 Velero 整合。

- 可用於存取 S3 的端點
- 存取 S3 的使用者憑證，包括存取金鑰和秘密存取金鑰
- S3 中用於備份的儲存桶名稱，具有使用者存取權限
- 為了安全存取物件存儲，應在物件儲存伺服器上安裝 TLS 憑證。

配置 **Velero** 的步驟

- 首先，為ONTAP S3 使用者憑證或 StorageGrid Tenant 使用者憑證建立一個金鑰。這將用於稍後配置 Velero。您可以從 CLI 或 Web 控制台建立機密。若要從 Web 控制台建立金鑰，請選擇“金鑰”，然後按一下“鍵/值金鑰”。提供憑證名稱、金鑰和值的值，如下所示。請務必使用您的 S3 使用者的存取金鑰 ID 和秘密存取金鑰。為秘密指定一個合適的名稱。在下面的範例中，建立了一個名為 ontap-s3-credentials 的具有ONTAP S3 使用者憑證的金鑰。





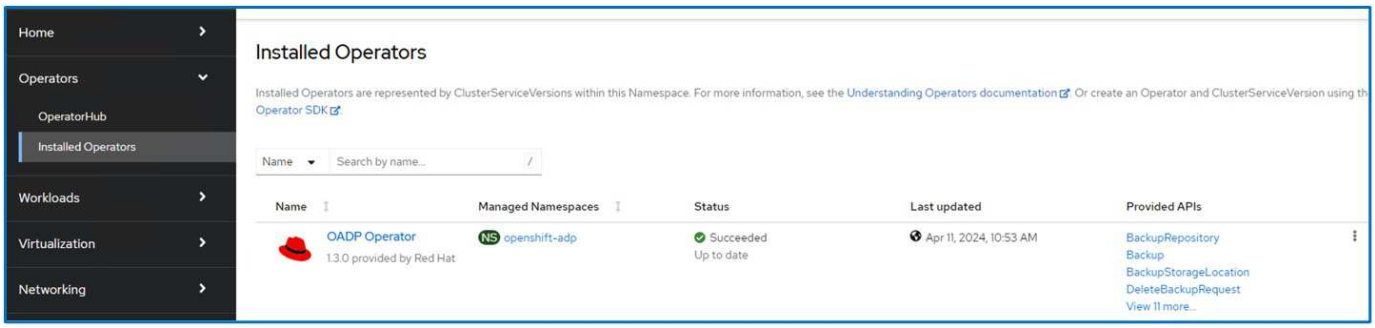
若要從 CLI 建立名為 sg-s3-credentials 的金鑰，您可以使用下列命令。

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

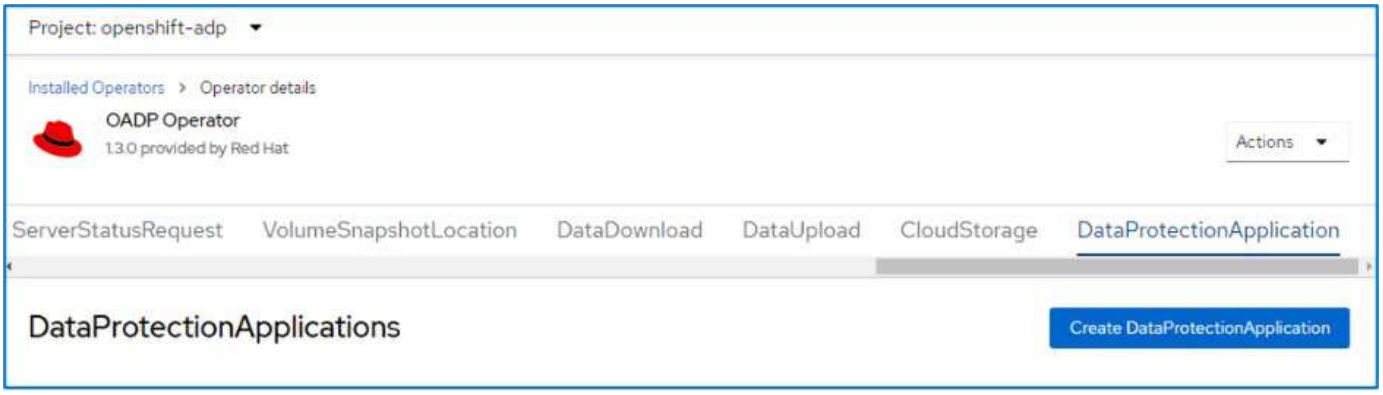
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- 接下來，要設定 Velero，請從 Operators 下的選單項目中選擇 Installed Operators，按一下 OADP 操作員，然後選擇 **DataProtectionApplication** 標籤。



按一下建立 DataProtectionApplication。在表單檢視中，為資料保護應用程式提供一個名稱或使用預設名稱。



現在轉到 YAML 視圖並取代規範訊息，如下面的 yaml 檔案範例所示。

使用**ONTAP S3** 作為備份位置配置 **Velero** 的範例 **yaml** 檔案

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
```

```
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

使用 **StorageGrid S3** 作為備份位置來配置 **Velero** 的範例 **yaml** 檔案

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

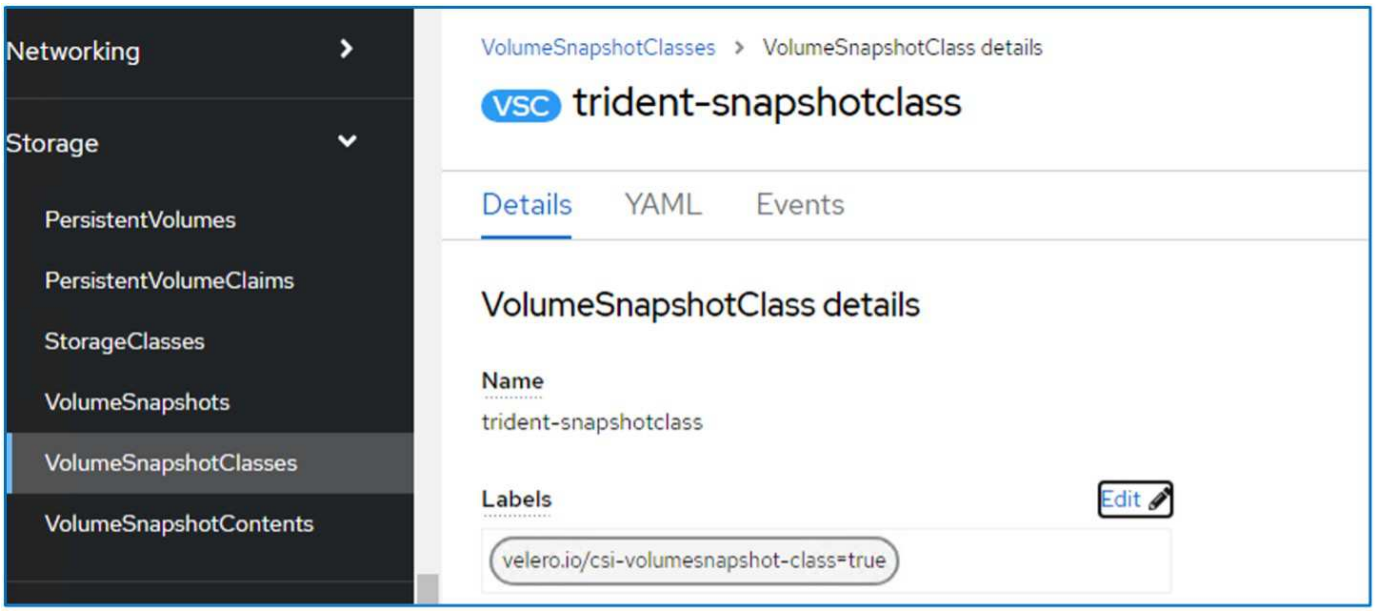
yaml 檔案中的 spec 部分應針對類似上述範例的下列參數進行適當配置

backupLocations ONTAP S3 或 StorageGrid S3（其憑證和其他資訊如 yaml 所示）配置為 velero 的預設 BackupLocation。

snapshotLocations 如果您使用容器儲存介面 (CSI) 快照，則無需指定快照位置，因為您將建立 VolumeSnapshotClass CR 來註冊 CSI 驅動程式。在我們的範例中，您使用Trident CSI，並且先前已使用Trident CSI 驅動程式建立了 VolumeSnapShotClass CR。

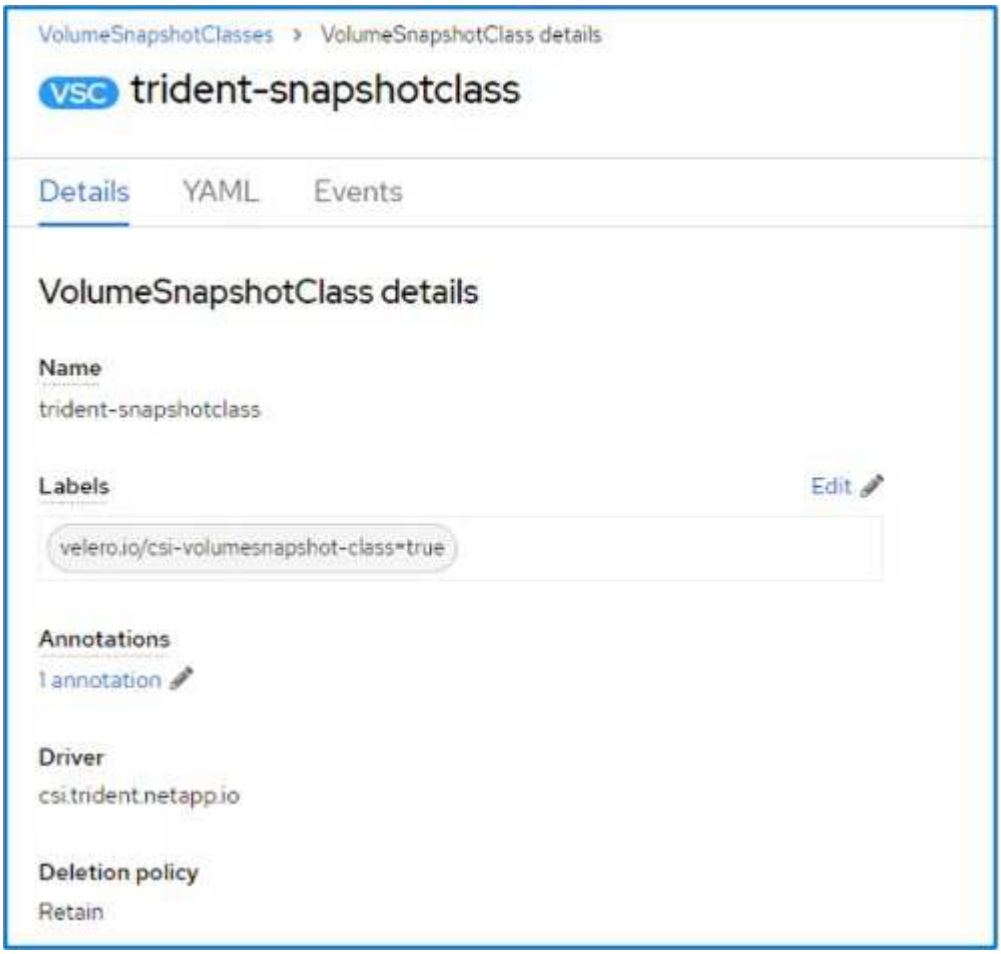
啟用 **CSI** 插件 將 csi 新增至 Velero 的預設插件中，以使用 CSI 快照備份持久性磁碟區。 Velero CSI 外掛程式用於備份 CSI 支援的 PVC，它將選擇叢集中設定了 **velero.io/csi-volumesnapshot-class** 標籤的 VolumeSnapshotClass。為了這

- 您必須建立 trident VolumeSnapshotClass。
- 編輯 trident-snapshotclass 的標籤，並將其設定為 **velero.io/csi-volumesnapshot-class=true**，如下所示。

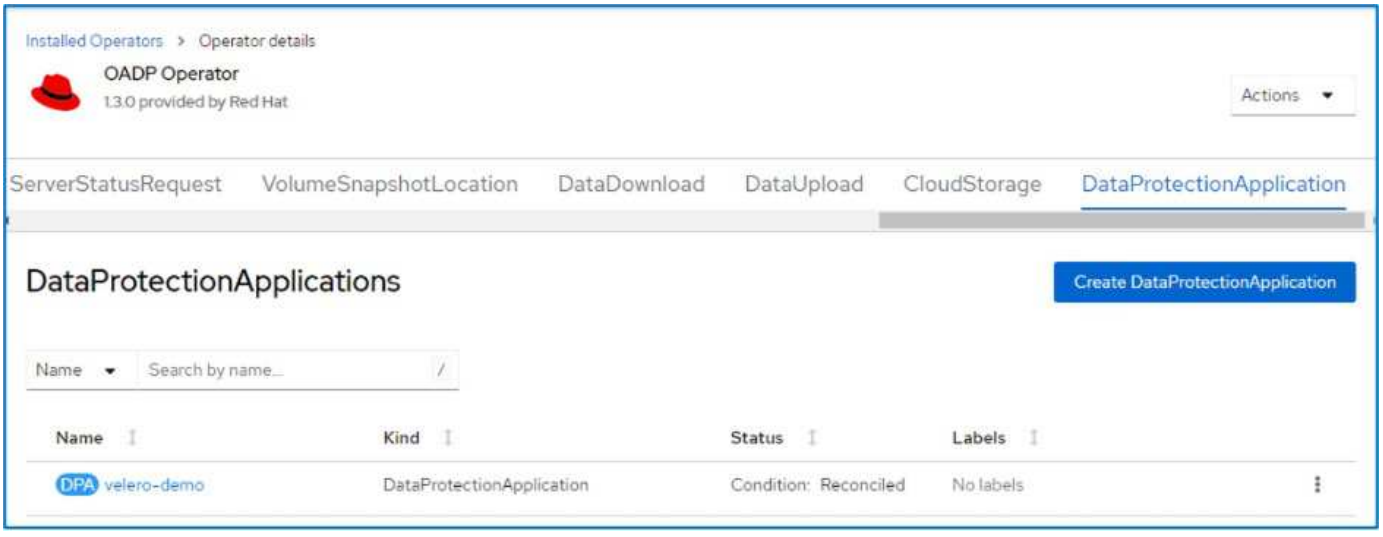


確保即使 VolumeSnapshot 物件被刪除，快照也能保留。這可以透過將 **deletionPolicy** 設為 Retain 來實現。如果不是，刪除命名空間將完全遺失其中備份的所有 PVC。

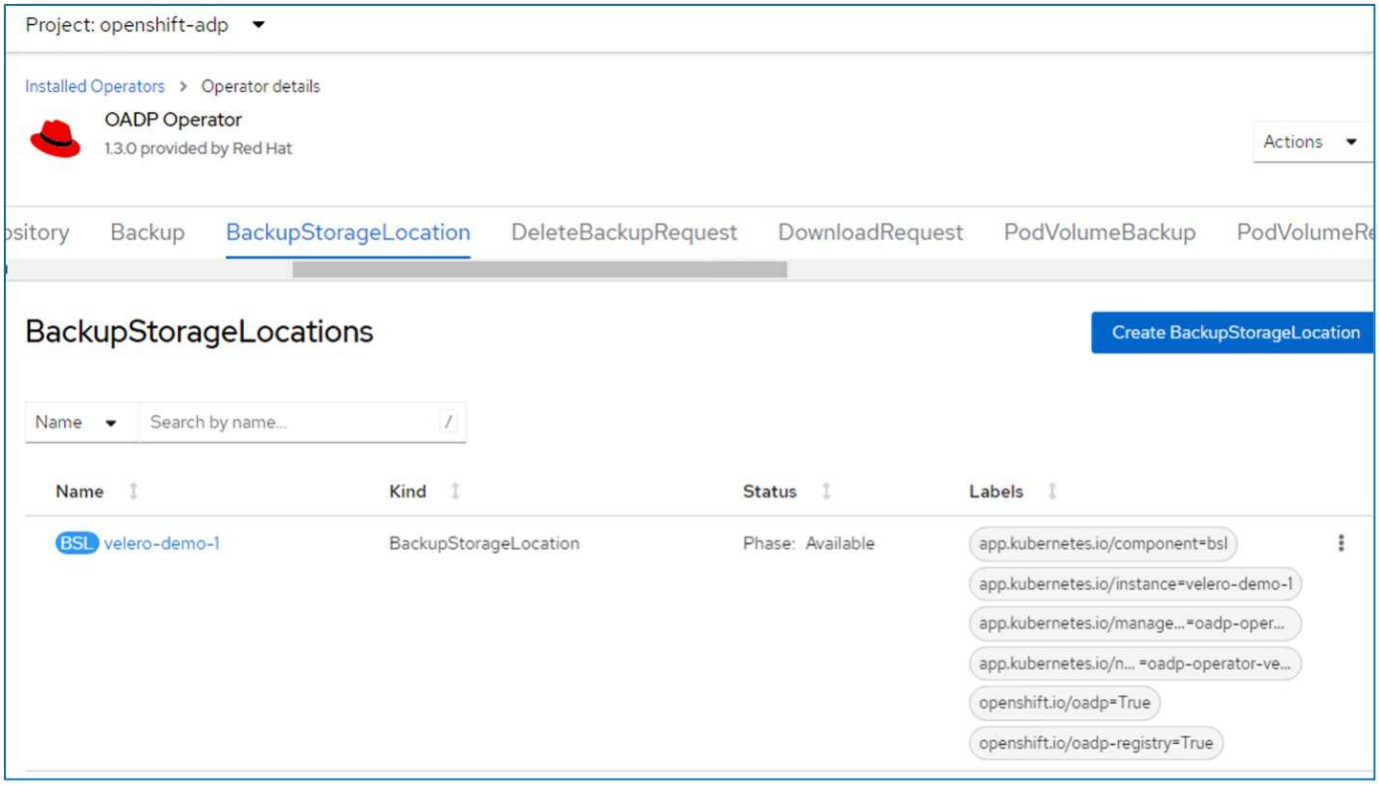
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



確保 DataProtectionApplication 已建立並且處於「狀態：Reconciled」。



OADP 操作員將建立對應的 BackupStorageLocation。這將在建立備份時使用。



在 **OpenShift Container Platform** 中為應用程式建立按需備份

本節概述如何在 OpenShift Virtualization 中為虛擬機器建立按需備份。

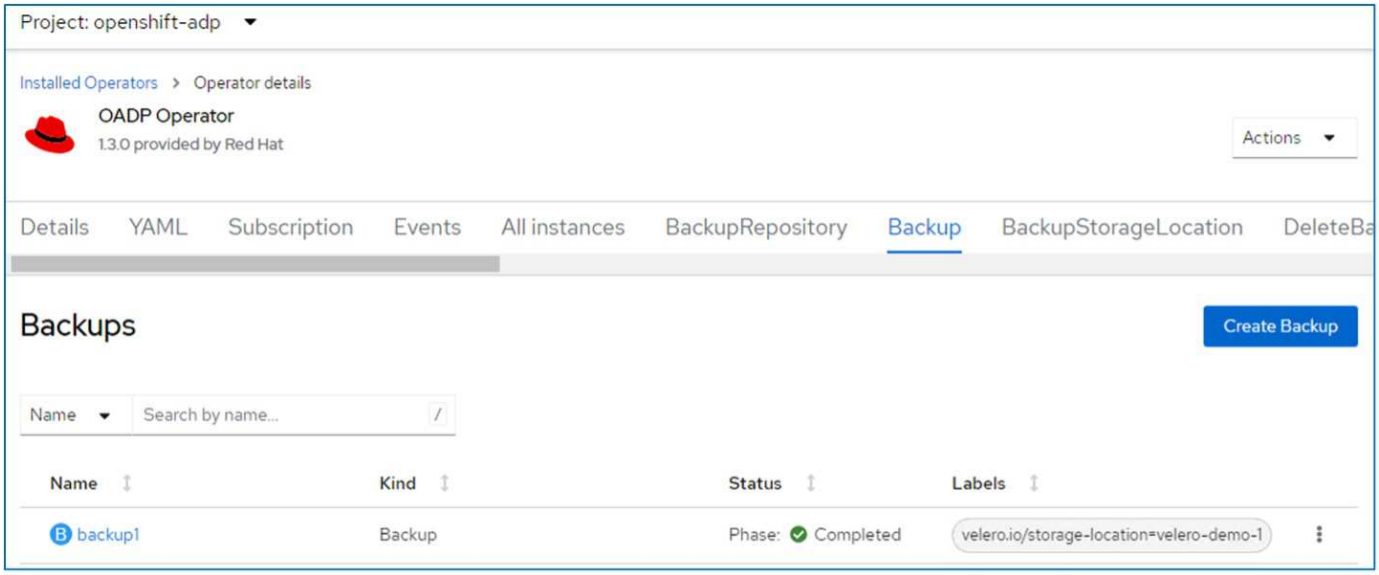
建立應用程式備份的步驟

若要建立應用程式（應用程式中繼資料和應用程式的持續性磁碟區）的隨選備份，請按一下 備份 索引標籤以建立備份自訂資源（CR）。系統提供了一個範例 yaml 來建立備份 CR。使用此 yaml，將會備份指定命名空間中的應用程式及其持續儲存。可以設定其他參數，如 "文件" 所示。

CSI 將建立指定命名空間中的持久磁碟區和應用程式資源的快照。此快照將儲存在 yaml 中指定的備份位置。備份將按照 ttl 的規定在系統中保留 30 天。

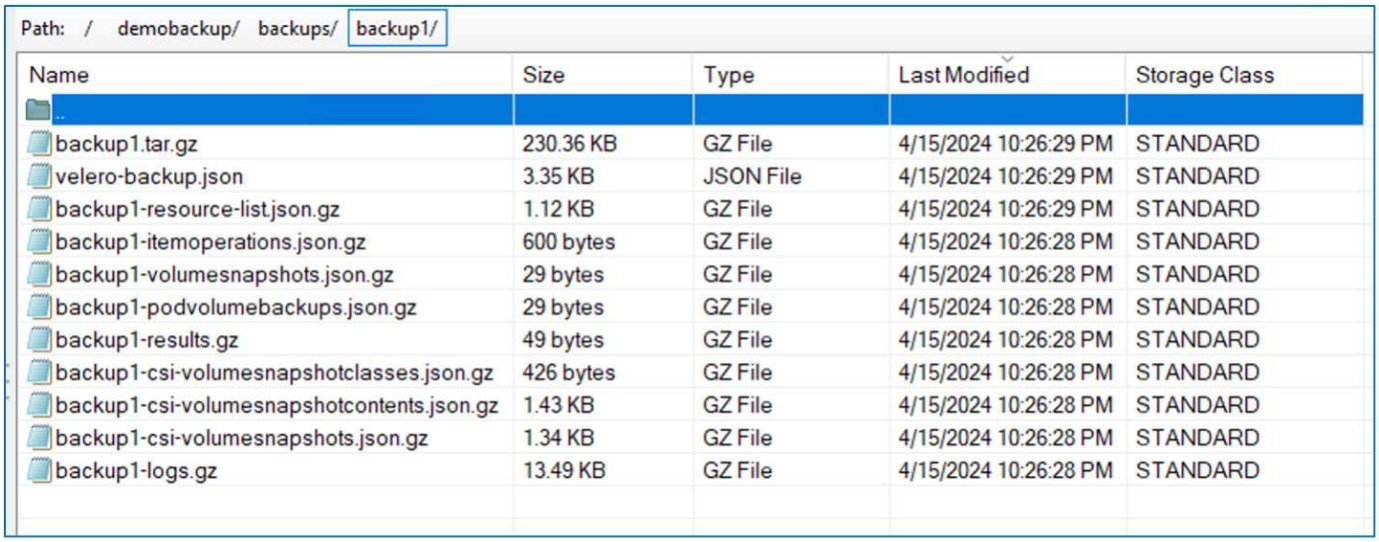
```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
  ttl: 720h0m0s
```

備份完成後，其階段將顯示為已完成。



您可以使用 S3 瀏覽器應用程式檢查物件儲存中的備份。備份路徑顯示在配置的儲存桶中，前綴名稱為（velero/container-demo-backup）。您可以看到備份的內容包括磁碟區快照、日誌和應用程式的其他元資料。

在 StorageGrid 中，您也可以使用租用戶管理器提供的 S3 控制台來檢視備份物件。



為應用程式建立排程備份

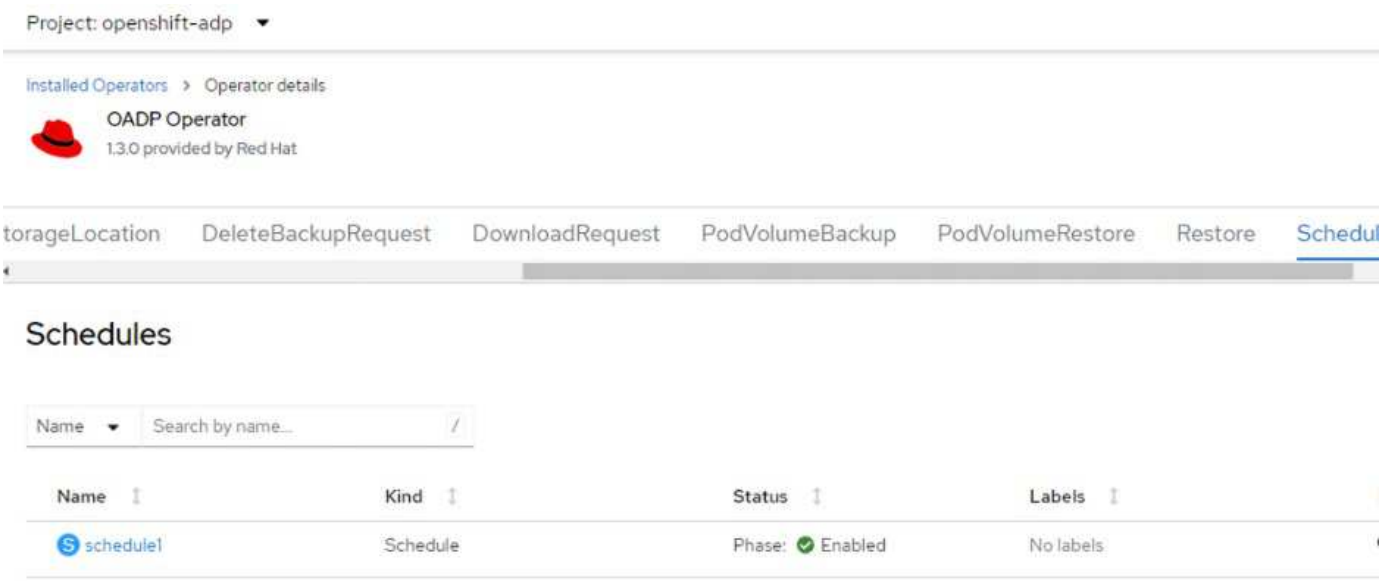
若要按排程建立備份，您需要建立計劃 CR。該計劃只是一個 Cron 表達式，可讓您指定要建立備份的時間。下面顯示了建立 Schedule CR 的範例 yaml。

```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
```

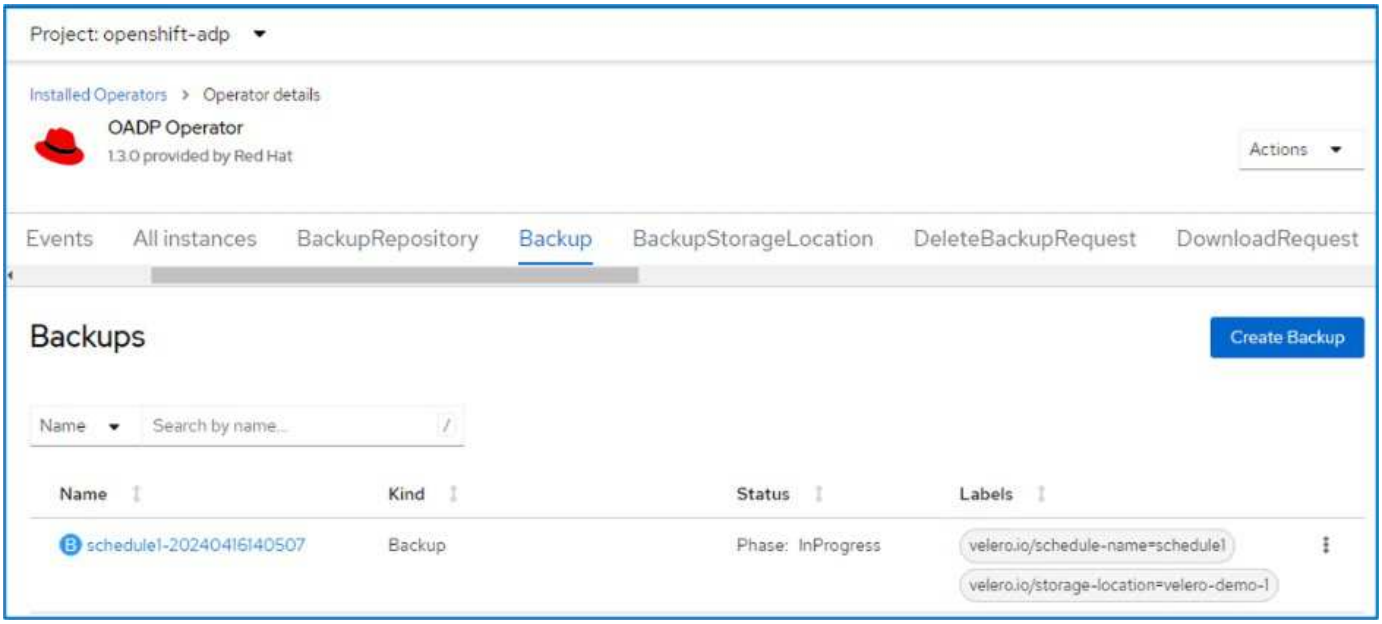
```
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

Cron表達式 0 7 * * * 表示每天7:00建立備份。也指定了要包含在備份中的命名空間和備份的儲存位置。因此，不是使用備份 CR，而是使用計劃 CR 在指定的時間和頻率建立備份。

一旦創建了計劃，它將被啟用。



備份將根據此計劃創建，並可從「備份」標籤中查看。



將應用程式從一個集群遷移到另一個集群

Velero 的備份和復原功能使其成為在叢集之間遷移資料的有價值的工具。本節介紹如何將

應用程式從一個集群遷移到另一個集群，方法是在一個集群的物件儲存中建立應用程式的備份，然後將應用程式從相同物件儲存還原到另一個集群。。

▼ 從第一個叢集備份

集群 **1** 的先決條件

- 必須在叢集上安裝Trident 。
- 必須建立 trident 後端和儲存類別。
- 必須在叢集上安裝 OADP 操作員。
- 應該要配置 DataProtectionApplication。

使用以下規格來配置 DataProtectionApplication 物件。

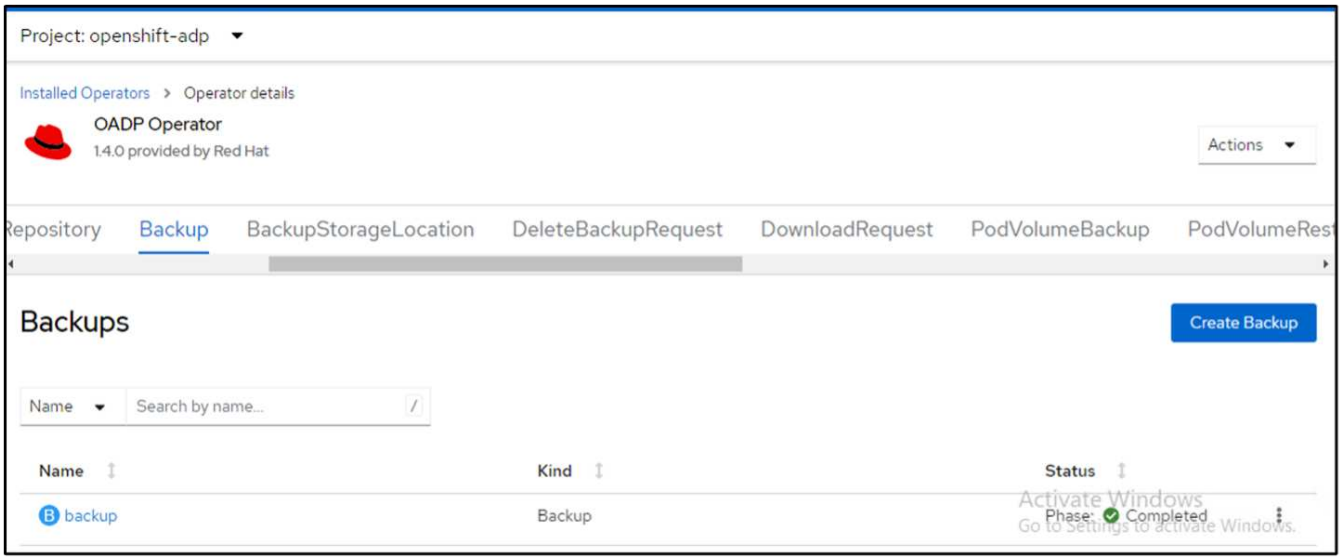
```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

- 在叢集上建立一個應用程式並備份該應用程式。例如，安裝一個 postgres 應用程式。

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE     VERSION
ocp6-master1   Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-master2   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-master3   Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-worker1   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker2   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker3   Ready    control-plane,master   3d12h   v1.27.15+6147456
[root@localhost ~]# helm install postgresql bitnami/postgresql -n postgresql --create namespace^C
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          4h53m
[root@localhost ~]# oc get pvc -n postgresql
NAME              STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            ontap-nas      4h53m
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                      STORAGECLASS
REASON   AGE
pvc-2e9e982f-54a4-4e7b-8eae-a589e0d9d819   1Gi        RWO            Delete           Bound    trident/basic              ontap-nas
         4h55m
pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         4h53m
[root@localhost ~]#
```

- 對備份 CR 使用以下規格：

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



您可以點擊所有實例選項卡以查看正在建立的不同對象，它們經過不同的階段，最終進入備份完成階段。

命名空間 postgresql 中的資源備份將儲存在 OADP 規範中的 backupLocation 中指定的物件儲存位置 (ONTAP S3) 中。

▼ 恢復到第二個集群

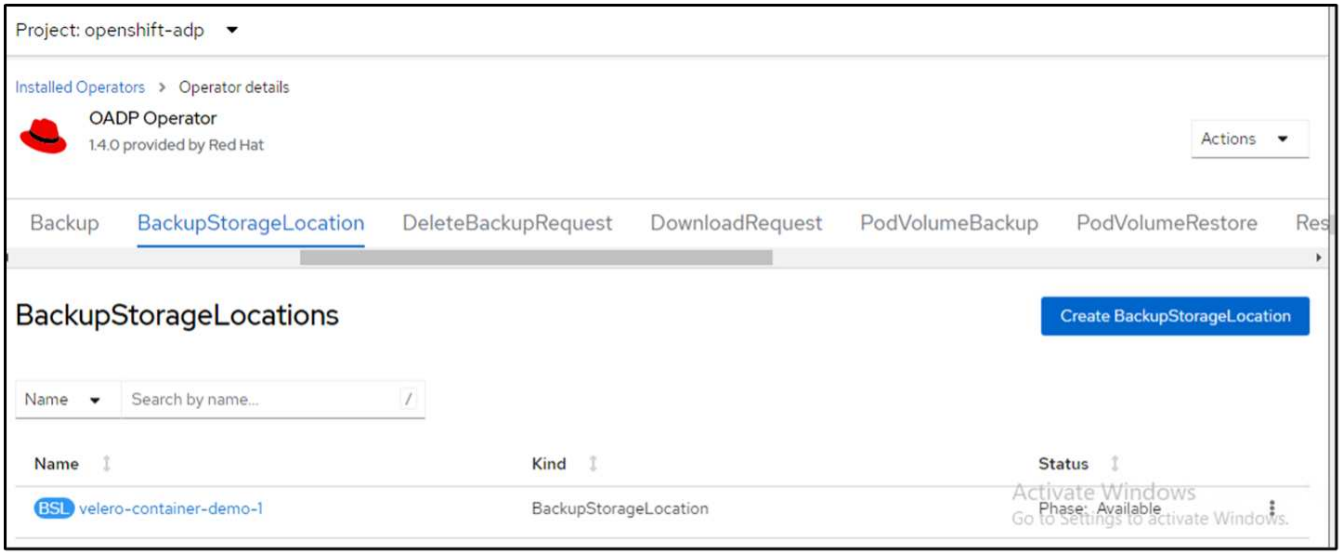
集群 **2** 的先決條件

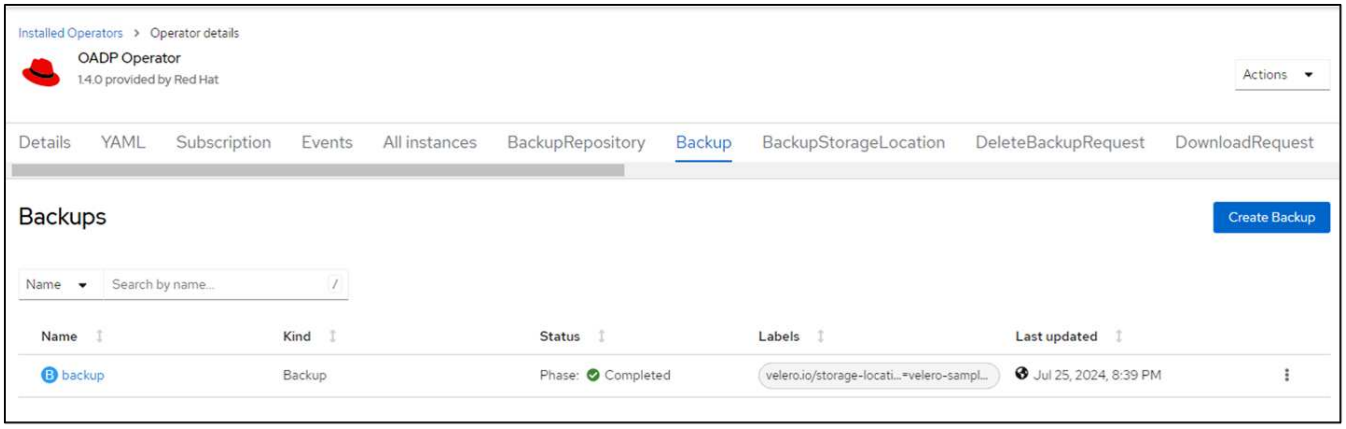
- 必須在叢集 2 上安裝Trident 。
- postgresql 應用程式一定不能已經安裝在 postgresql 命名空間中。
- OADP 操作員必須安裝在叢集 2 上，且 BackupStorage Location 必須指向儲存第一個叢集的備份的相同物件儲存位置。
- 備份 CR 必須對第二個叢集可見。

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker               3d    v1.27.15+6147456
ocp7-worker2   Ready    worker               3d    v1.27.15+6147456
ocp7-worker3   Ready    worker               3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM              STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic      ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc   vsphere-sc              2d7
h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

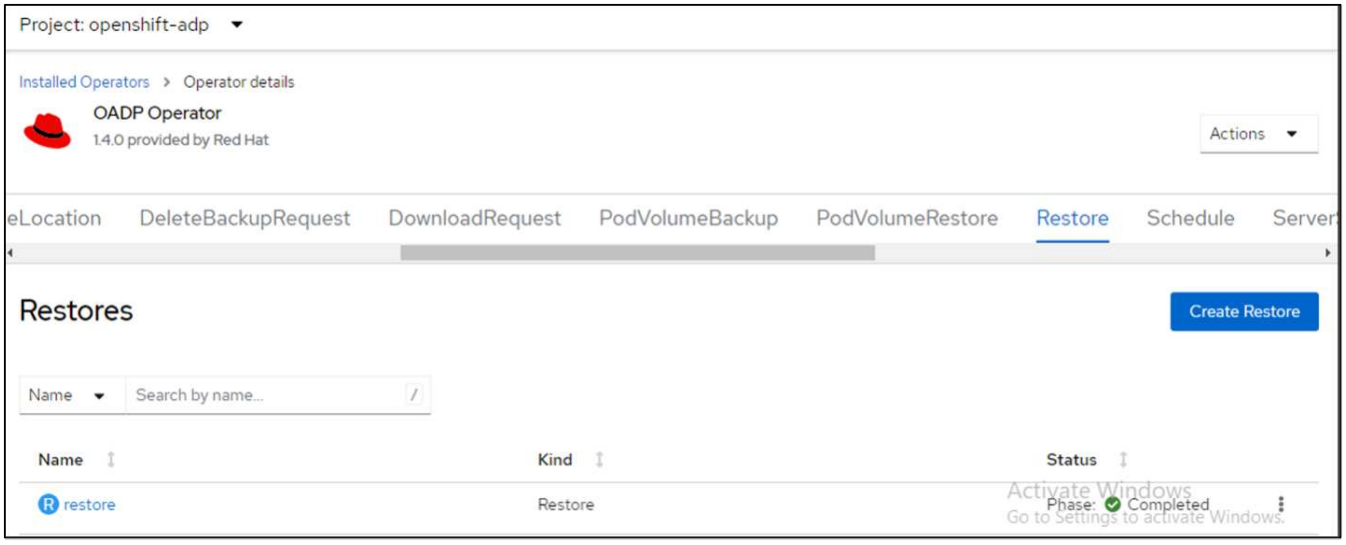




從備份還原此叢集上的應用程式。使用以下 yaml 建立 Restore CR。

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
```

恢復完成後，您將看到 postgresql 應用程式正在此叢集上運行，並與 pvc 和對應的 pv 相關聯。應用程式的狀態與備份時的狀態相同。



```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                  AGE    VERSION
ocp7-master1  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3  Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME               STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0  Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                          STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                  ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc               vsphere-sc
         2d10h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

從備份還原應用程式

本節介紹如何從備份還原應用程式。

先決條件

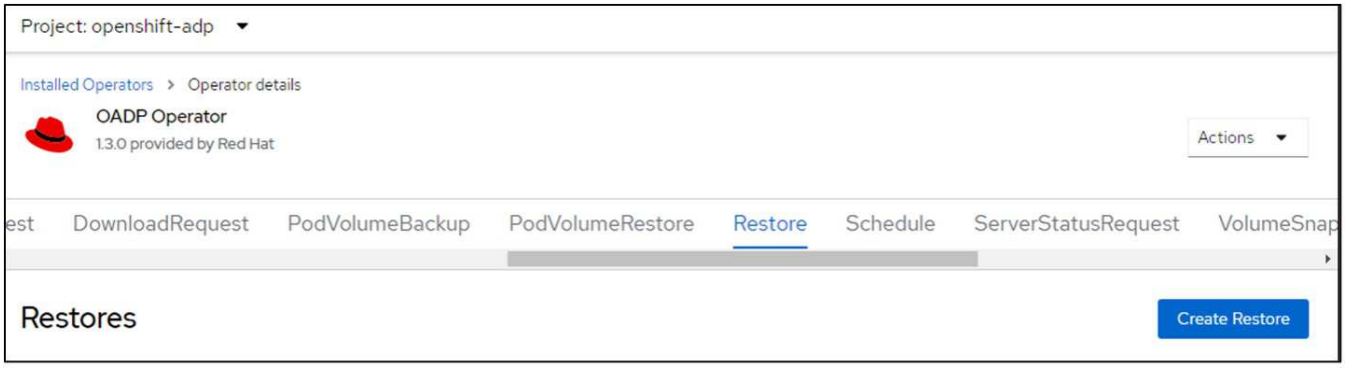
為了從備份中恢復，我們假設應用程式所在的命名空間被意外刪除了。

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

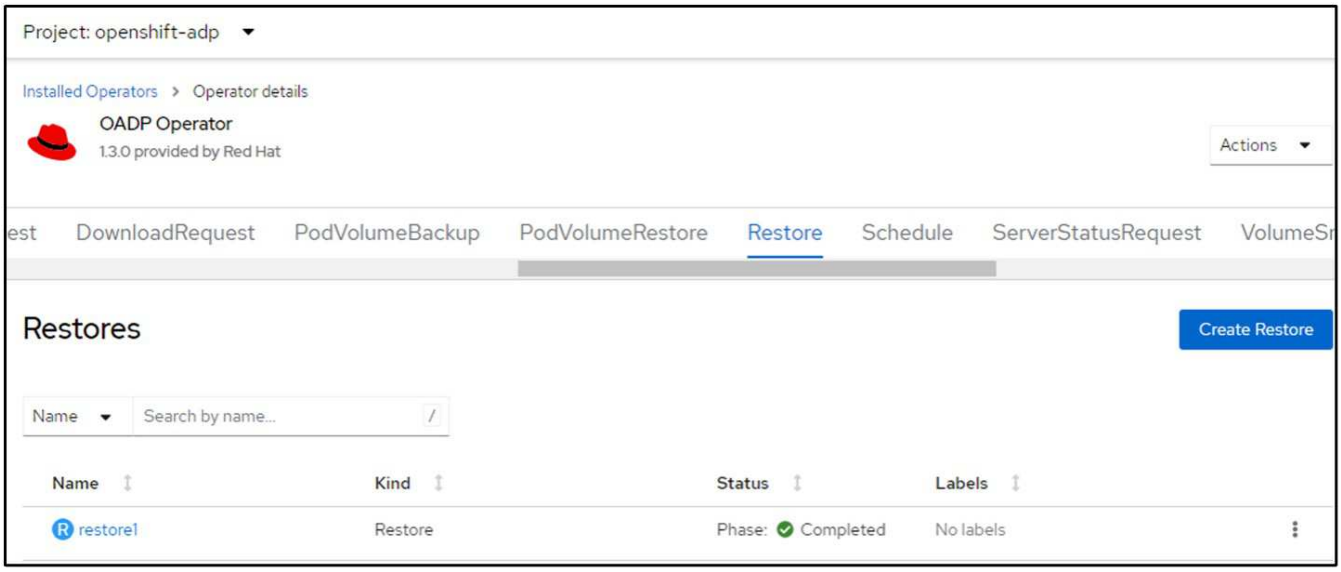
▼ 還原到同一命名空間

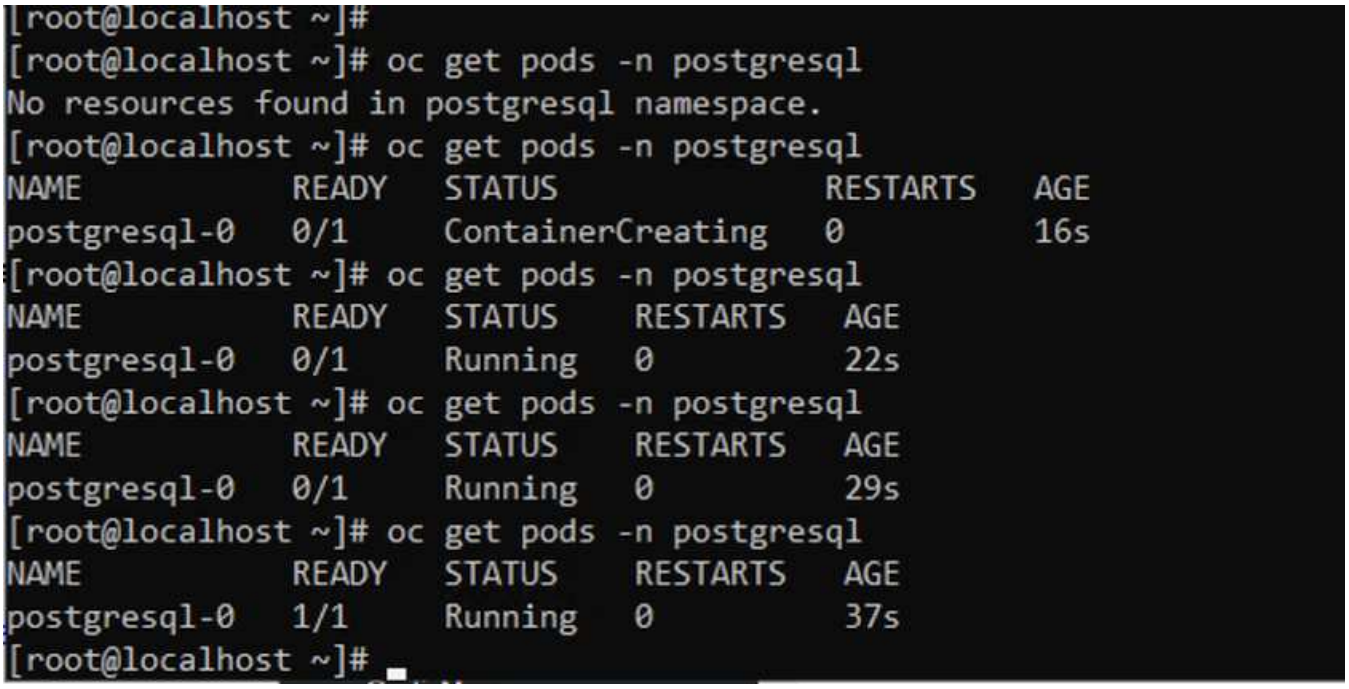
若要從我們剛剛建立的備份還原，我們需要建立一個還原自訂資源（CR）。我們需要為其命名，提供要從中還原的備份名稱，並將 restorePVs 設為 true。其他參數可以如 "文件" 所示進行設定。按一下「建立」按鈕。




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

當階段顯示完成時，您可以看到應用程式已恢復到拍攝快照時的狀態。應用程式恢復到相同的命名空間。





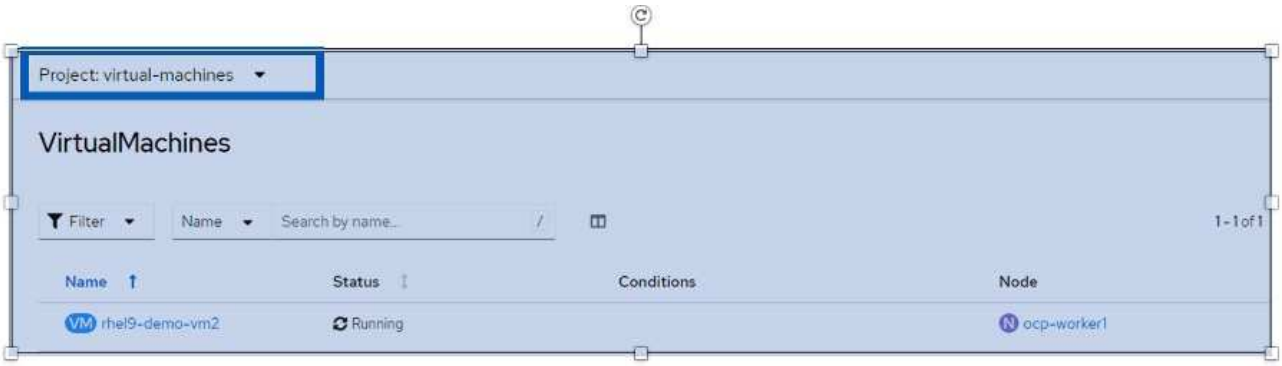
▼ 還原到不同的命名空間

若要將應用程式還原到不同的命名空間，您可以在 Restore CR 的 yaml 定義中提供 namespaceMapping。

以下範例 yaml 檔案建立一個 Restore CR，以將應用程式及其持久性儲存從 postgresql 命名空間還原到新的命名空間 postgresql-restored。

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

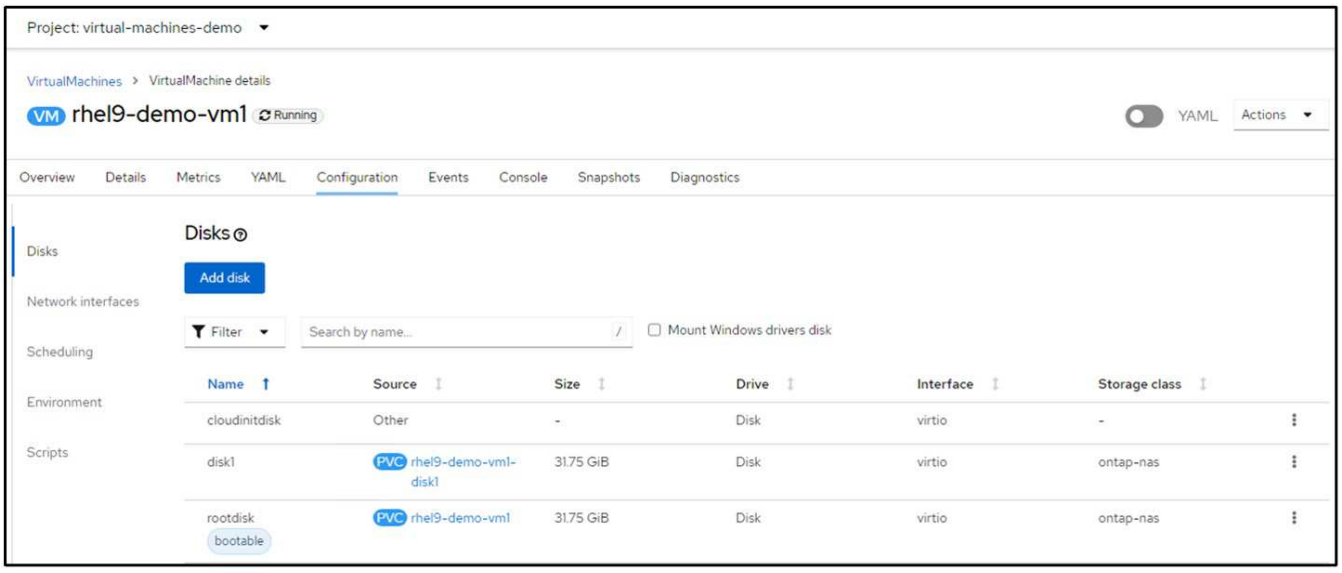
當階段顯示完成時，您可以看到應用程式已恢復到拍攝快照時的狀態。應用程式將恢復到 yaml 中指定的不同命名空間。

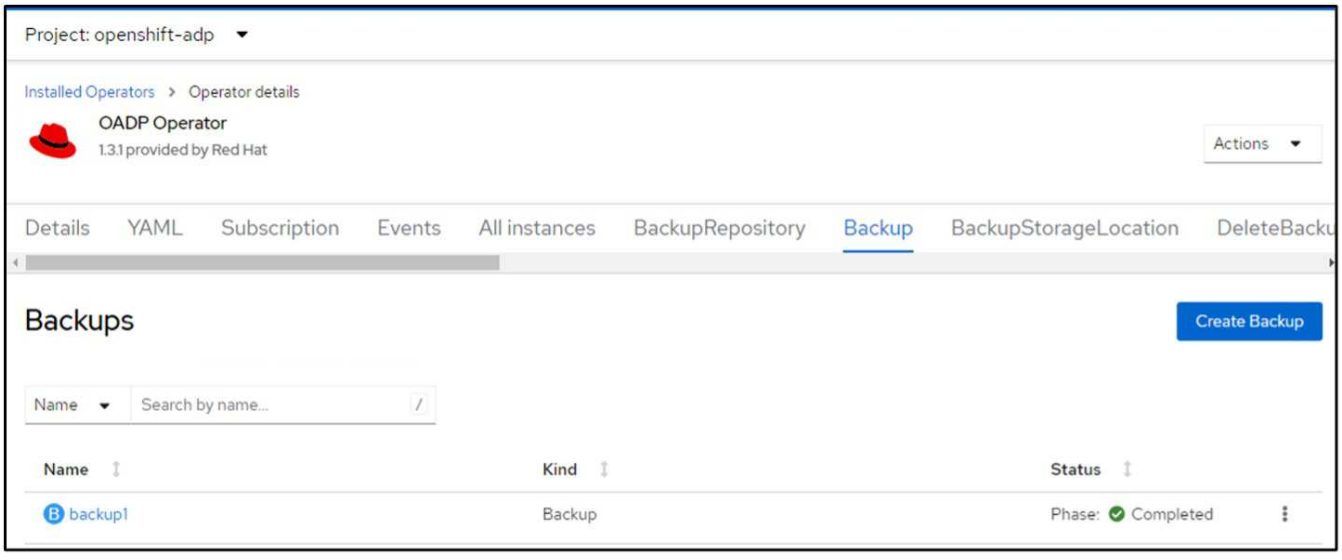


▼ 還原到不同的儲存類別

Velero 提供了透過指定 json 補丁來修改復原期間資源的通用功能。在恢復資源之前，json 補丁會套用到資源上。 json 補丁在 configmap 中指定，並在 restore 命令中引用該 configmap。此功能使您能夠使用不同的儲存類別進行復原。

在下面的範例中，應用程式在部署期間使用 ontap-nas 作為其持久卷的儲存類別。創建了名為backup-postgresql-ontaps3的應用程式備份。





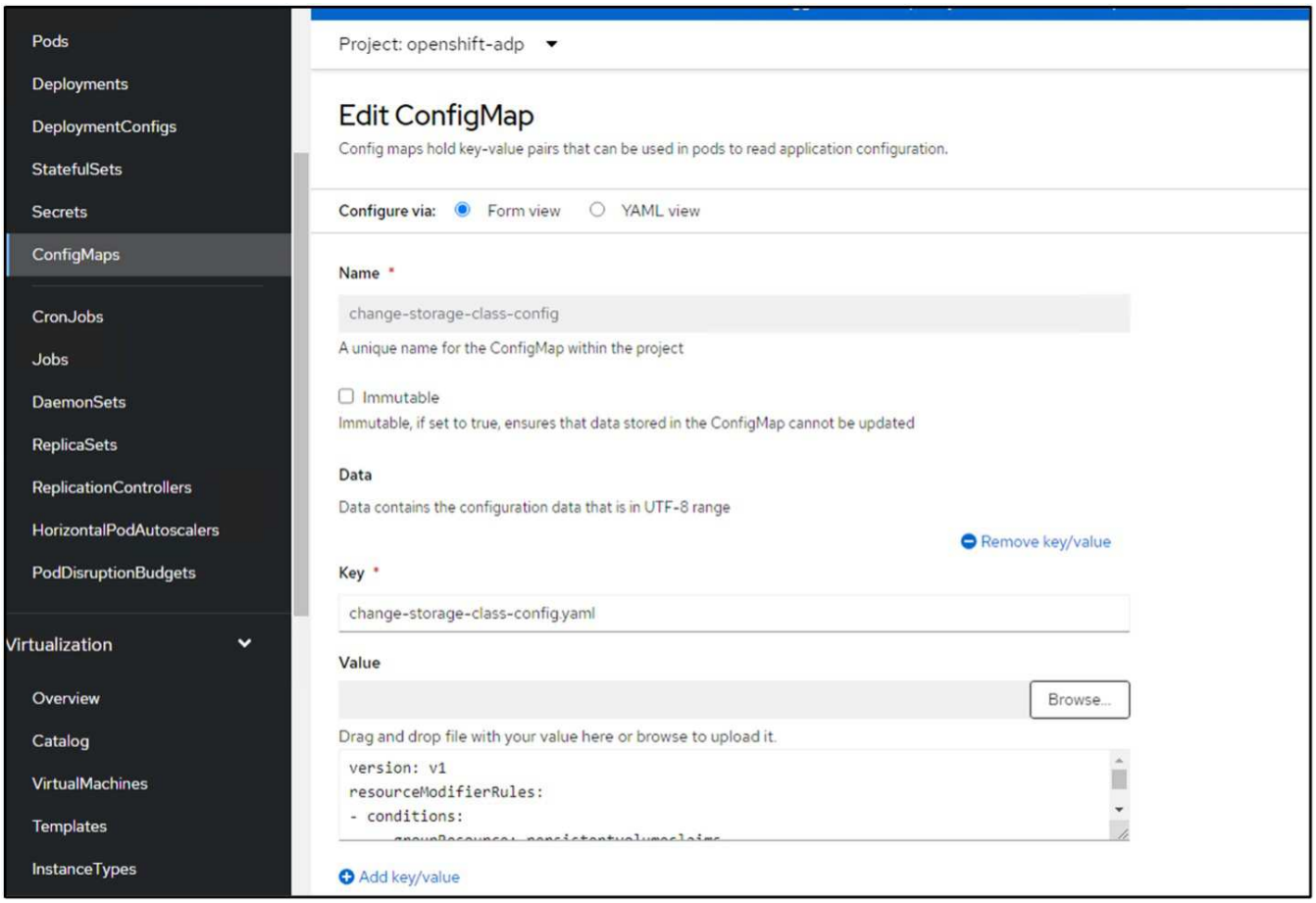
透過卸載應用程式來模擬應用程式的遺失。

要使用不同的儲存類別（例如 ontap-nas-eco 儲存類別）還原虛擬機，您需要執行以下兩個步驟：

步驟 **1**

在 openshift-adp 命名空間中建立一個配置映射（控制台），如下所示： 填寫螢幕截圖中顯示的詳細資訊：選擇命名空間：openshift-adp 名稱：change-ontap-sc（可以是任意名稱） 鍵：change-ontap-sc-config.yaml ： 值：

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



產生的配置映射物件應如下所示（CLI）：

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"



BinaryData
====

Events:  <none>
```

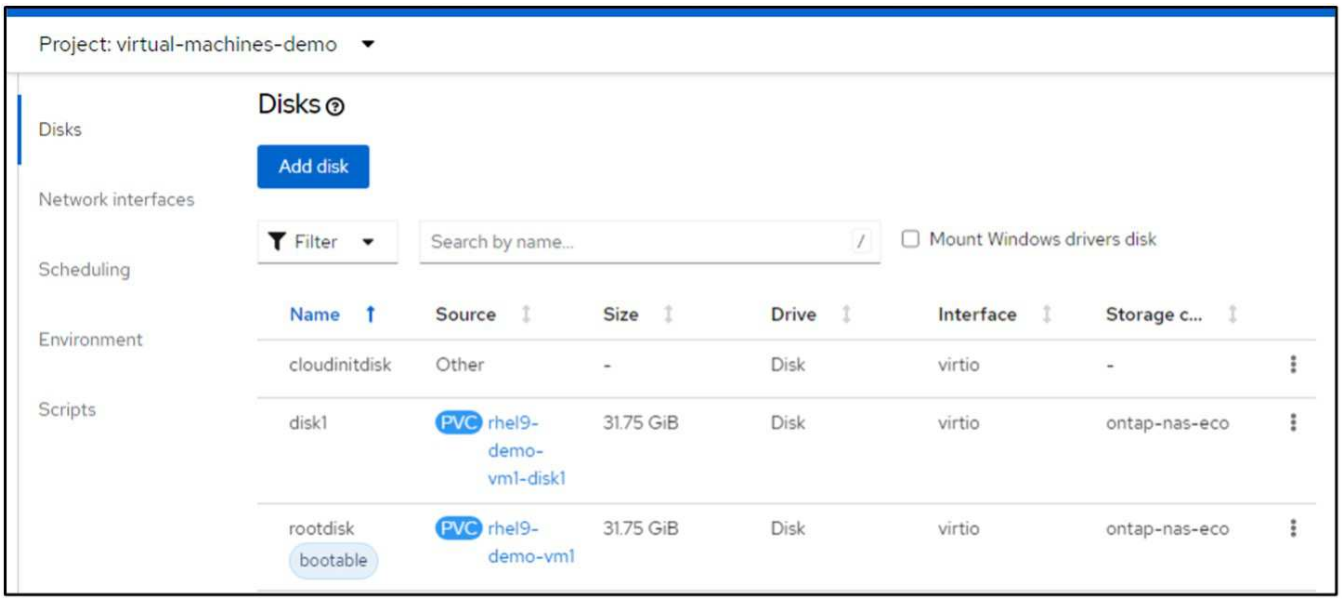
此配置圖將在建立復原時套用資源修改規則。將應用程式補丁將以 rhel 開頭的所有持久化卷聲明的儲存類別名稱替換為 ontap-nas-eco。

步驟 **2**

若要復原虛擬機，請使用 Velero CLI 中的下列命令：

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

該應用程式在使用儲存類別 ontap-nas-eco 創建的持久卷聲明的相同命名空間中恢復。



使用 **Velero** 刪除備份和恢復

本節概述如何使用 Velero 刪除 OpenShift 容器平台中應用程式的備份和還原。

列出所有備份

您可以使用 OC CLI 工具或 Velero CLI 工具列出所有備份 CR。按照說明下載 Velero CLI"Velero 文檔" 。

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

刪除備份

您可以使用 OC CLI 工具刪除備份 CR，而不刪除物件儲存資料。備份將從 CLI/控制台輸出中刪除。但是，由於相應的備份沒有從物件儲存中刪除，它將重新出現在 CLI/控制台輸出中。

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

如果您想刪除備份 **CR** 和相關的物件儲存數據，您可以使用 **Velero CLI** 工具來執行此操作。

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                       Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

刪除還原

您可以使用 OC CLI 或 Velero CLI 刪除恢復 CR 對象

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

觀看有關NetApp混合多雲解決方案的影片和演示

觀看有關使用NetApp的 Amazon Web Services 混合多雲解決方案的視頻

探索 NetApp 的綜合影片庫，其中包含NetApp為 AWS 提供的混合多雲解決方案。觀看有關 VMware Cloud on AWS 和Amazon FSx for ONTAP的客戶機連接存儲、TCO 節省、補充資料存儲和遷移工作流程的視頻，包括 Windows 和 Linux 場景。

來賓連接存儲

使用 iSCSI 的 Windows 用戶端連線儲存與 FSx ONTAP

使用 NFS 連接 Linux 用戶端和 FSx ONTAP 的存儲

TCO 和補充資料存儲

VMware Cloud on AWS 使用Amazon FSx ONTAP節省 TCO

VMware Cloud on AWS 補充資料儲存（附Amazon FSx ONTAP）

遷移工作流程 (HCX)

VMC 的 VMware HCX 部署與設定

使用 VMware HCX for VMC 和 FSx ONTAP進行 vMotion 遷移演示

使用 VMware HCX for VMC 和 FSx ONTAP進行冷遷移演示

觀看有關使用NetApp的 Azure VMware 雲端的混合多雲解決方案的視頻

探索 NetApp 的綜合影片庫，其中包含NetApp針對 Azure VMware 解決方案 (AVS) 的混合多雲解決方案。該系列包括有關補充資料儲存、災難復原和遷移工作流程的影片。

補充資料存儲

Azure VMware 解決方案補充資料儲存概述（包含Azure NetApp Files）

災難復原

帶有Cloud Volumes ONTAP、 SnapCenter和 JetStream 的 Azure VMware 解決方案 DR

遷移工作流程 (HCX)

使用 VMware HCX 進行 AVS 和 ANF 冷遷移演示

使用 VMware HCX 進行 AVS 和 ANF 的 vMotion 演示

使用 VMware HCX 進行 AVS 和 ANF 批量遷移演示

觀看有關NetApp的 Red Hat OpenShift 混合多雲解決方案的視頻

探索 NetApp 的綜合影片庫，其中包含NetApp為 Red Hat OpenShift 提供的混合多雲解決方案。該集合包括使用 FSx ONTAP對 AWS 上的 OpenShift (ROSA) 進行快照和復原、與Trident 的整合、應用程式的故障轉移和故障復原以及使用 Ansible 在FlexPod上自動部署 Oracle RAC 的示範。

快照和恢復

使用Amazon FSx ONTAP儲存為 AWS (ROSA) 叢集上的 Red Hat OpenShift Service 應用程式進行快照/還原

儲存集成

FSx ONTAP與Trident的集成

故障轉移和故障恢復

使用 FSx ONTAP在 ROSA 上實現應用程式的故障轉移和故障復原

解決方案自動化



使用 **Ansible** 在**FlexPod**上自動部署 **Oracle 19c RAC**

閱讀NetApp專家的雲端解決方案博客

閱讀博客，了解有關將ONTAP儲存與NetApp雲解決方案整合的實用指導和最佳實踐。

VMware 與 AWS 和Amazon FSx for ONTAP 的集成

- "使用 Amazon EC2 和Amazon FSx ONTAP iSCSI 協定將 VMware VM 移轉到 AWS"
- "Amazon EVS 現已與 FSx for ONTAP集成"
- "Amazon EVS 宣布支援 FSx for ONTAP"
- "使用 VMware HCX 配置具有 FSx ONTAP和 VMware Cloud on AWS SDDC 的混合雲"

Azure VMware 解決方案

- "在任何雲端環境中最佳化儲存和資料密集型 VMware 工作負載"
- "將 VMware 工作負載遷移到 Azure VMware Solution ？請先閱讀本文。"

Google Cloud VMware 引擎

- "Google Cloud NetApp Volumes資料儲存區支援 Google Cloud VMware Engine (NetApp)"
- "如何將NetApp Volumes 用作 Google Cloud VMware Engine 的資料儲存區（Google）"
- "NetApp部落格 - 將儲存豐富的應用程式遷移到 Google Cloud 的更好方法"

資料保護和管理

- "搭配 SnapCenter 外掛程式與虛擬機器的 NetApp Backup and Recovery 的 VMware 3-2-1 資料保護"
- "利用NetApp Cloud Insights實現現代資料中心的可觀察性"

NetApp適用於 OpenShift 容器工作負載

- "NetApp ONTAP兼作 Red Hat OpenShift 容器平台中的日誌存儲"

VMware 主權雲

- "推出全新主權雲端計劃"

法律聲明

法律聲明提供對版權聲明、商標、專利等的存取。

版權

"https://www.netapp.com/company/legal/copyright/"

商標

NETAPP、NETAPP 標誌和NetApp商標頁面上列出的標誌是NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

"https://www.netapp.com/company/legal/trademarks/"

專利

NetApp擁有的專利的最新清單可在以下位置找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隱私權政策

"https://www.netapp.com/company/legal/privacy-policy/"

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。