公有雲和混合雲

NetApp Solutions

NetApp
May 10, 2024

目錄

公有雲和混合雲

NetApp混合式多雲端搭配VMware解決方案

適用於公有雲的VMware

NetApp混合式多雲端與VMware的總覽

大多數IT組織都採用混合式雲端優先方法。這些組織正處於轉型階段、客戶正在評估其目前的IT環境、然後根據評估與探索練習、將工作負載移轉至雲端。

客戶移轉至雲端的因素包括彈性與爆發、資料中心結束、資料中心整合、生命週期結束案例、合併、 併購等。此移轉的原因可能因組織及其各自的業務優先順序而異。移轉至混合雲時、在雲端中選擇適當的儲存設備、對於釋放雲端部署和彈性的威力十分重要。

公有雲的VMware Cloud選項

本節說明各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服務、可在Microsoft Azure公有雲中提供功能完整的VMware SDDC。Azure VMware解決方案是第一方的解決方案、由Microsoft完全管理及支援、並由VMware運用Azure基礎架構進行驗證。這表示當部署Azure VMware解決方案時、客戶會獲得VMware的ESXi用於運算虛擬化、vSAN用於超融合式儲存設備、 以及NSX的網路與安全功能、同時充分利用Microsoft Azure的全球知名度、領先同級的資料中心設施、以及接近豐富的原生Azure服務與解決方案生態系統。

AWS上的VMware Cloud

AWS上的VMware Cloud可將VMware企業級SDDC軟體導入AWS Cloud、並針對原生AWS服務進行最佳化存取。以VMware Cloud Foundation為後盾、AWS上的VMware Cloud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管理功能、經過最佳化、可在專屬、靈活、裸機的AWS基礎架構上執行。

Google Cloud VMware Engine

Google Cloud VMware Engine是基礎架構即服務（IaaS）、以Google Cloud高效能的可擴充基礎架構和VMware Cloud Foundation堆疊（VMware vSphere、vCenter、vSAN和NSX T）為基礎這項服務可讓您快速移轉至雲端、從內部部署環境無縫移轉或延伸現有的VMware工作負載至Google Cloud Platform、而不需重新建構應用程式或重組作業的成本、心力或風險。這項服務是由Google銷售及支援的服務、與VMware密切合作。

SDDC私有雲和NetApp Cloud Volumes共置可提供最佳效能、並將網路延遲降至最低。

您知道嗎？

無論使用何種雲端、部署VMware SDDC時、初始叢集都包含下列產品：

- 使用vCenter Server應用裝置進行運算虛擬化的VMware ESXi主機進行管理
- VMware vSAN超融合式儲存設備整合了每個ESXi主機的實體儲存資產
- VMware NSX提供虛擬網路與安全性、並搭配NSX Manager叢集進行管理

儲存組態

對於計畫裝載儲存密集工作負載並在任何雲端代管VMware解決方案上橫向擴充的客戶、預設的超融合式基礎架構要求擴充時必須同時使用運算與儲存資源。

透過與Azure NetApp Files NetApp Cloud Volumes整合、例如：《關於NetApp ONTAP 的Amazon FSX 》、Cloud Volumes ONTAP 《關於NetApp的支援》、《關於所有三大大型超大規模系統的支援》和Cloud Volumes Service 《關於Google Cloud的支援》、客戶現在可以選擇獨立擴充儲存設備、 而且只能視需要將運算節點新增至SDDC叢集。

附註：

- VMware不建議使用不平衡的叢集組態、因此擴充儲存設備意味著增加更多主機、這意味著擁有更高的TCO。
- 只能有一個vSAN環境。因此、所有的儲存流量都會直接與正式作業工作負載競爭。
- 您無法選擇提供多個效能層級來調整應用程式需求、效能和成本。
- 輕鬆達到叢集主機上建置的vSAN儲存容量限制。使用NetApp Cloud Volumes將儲存設備擴充至裝載作用中資料集、或將層級較低的資料擴充至持續儲存設備。

適用於NetApp的Amazon FSX、功能齊全的功能、包括所有三大大型超大規模擴充系統、以及適用於Google Cloud的功能、均可搭配訪客VM一起使用。Azure NetApp Files ONTAP Cloud Volumes ONTAP Cloud Volumes Service這種混合式儲存架構是由vSAN資料存放區所組成、其中包含客體作業系統和應用程式二進位資料。應用程式資料會透過來賓型iSCSI啟動器附加至VM、或是透過NFS/SMB掛載直接與Amazon FSX for NetApp ONTAP 、Cloud Volume ONTAP Sfor Azure NetApp Files Google Cloud進行通訊Cloud Volumes Service 。此組態可讓您輕鬆克服vSAN儲存容量所帶來的挑戰、可用空間取決於所使用的閒置空間和儲存原則。

讓我們來考慮在AWS上的VMware Cloud上使用三節點SDDC叢集：

- 三節點SDDC的總原始容量= 31.1TB（每個節點約10TB）。
- 新增額外主機之前所需保留的寬限空間= 25%=（.25 x 31.1TB）= 7.7TB。
- 閒餘空間減除後的可用原始容量= 23.4TB
- 可用的有效可用空間取決於套用的儲存原則。

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做為與來賓連線的儲存設備、有助於擴充儲存設備並最佳化TCO、同時滿足效能與資料保護需求。

在寫入本文檔時、來賓儲存設備是唯一可用的選項。 隨著補充NFS資料存放區支援的推出、我們也會提供額外的文件 "請按這裡"。

值得記住的重點

- 在混合式儲存模式中、將層級1或高優先順序的工作負載放在vSAN資料存放區上、以因應任何特定的延遲需求、因為它們是主機本身的一部分、而且位於鄰近範圍內。針對可接受交易延遲的任何工作負載VM、使用來賓機制。
- 使用NetApp SnapMirror®技術、將工作負載資料從內部部署ONTAP 的SnapMirror系統複寫到Cloud Volumes ONTAP 適用於NetApp ONTAP 的Sf2或Amazon FSX、以便使用區塊層級機制輕鬆移轉。這不適用於Azure NetApp Files 「不適用於」和「Cloud Volumes服務」。若要將資料移轉至 Azure NetApp Files 或雲端 Volume Services 、請根據使用的檔案傳輸協定、使用 NetApp XCP 、 BlueXP 複製與同步、 rysnc 或 Robocopy 。
- 測試顯示、從個別SDDC存取儲存設備時、會有2至4毫秒的額外延遲。在對應儲存設備時、請將額外延遲因素納入應用程式需求。
- 若要在測試容錯移轉和實際容錯移轉期間掛載與來賓連線的儲存設備、請確認iSCSI啟動器已重新設定、SMB共用的DNS已更新、而且Fstab中的NFS掛載點已更新。
- 請確定已在VM內部正確設定來賓Microsoft多重路徑I/O（MPIO）、防火牆及磁碟逾時登錄設定。

這僅適用於來賓連線的儲存設備。

NetApp雲端儲存設備的優點

NetApp雲端儲存設備具備下列優點：

- 透過獨立擴充運算儲存設備、改善運算對儲存設備的密度。
- 可讓您減少主機數、進而降低整體TCO。
- 運算節點故障不會影響儲存效能。
- 藉由Azure NetApp Files 利用功能強大的功能來調整磁碟區大小、以調整穩定狀態工作負載的規模、進而避免資源過度配置、進而達到最佳成本效益。
- 利用NetApp的儲存效率、雲端分層和執行個體類型修改功能Cloud Volumes ONTAP 、您可以以最佳方式新增及擴充儲存設備。
- 避免只在需要時才新增過度資源配置。
- 高效率的Snapshot複本與複本可讓您快速建立複本、而不會對效能造成任何影響。
- 使用Snapshot複本的快速恢復功能、協助解決勒索軟體攻擊。

- 跨區域提供有效率的遞增區塊傳輸型區域性災難恢復和整合式備份區塊層級、可提供更好的RPO和RTO。

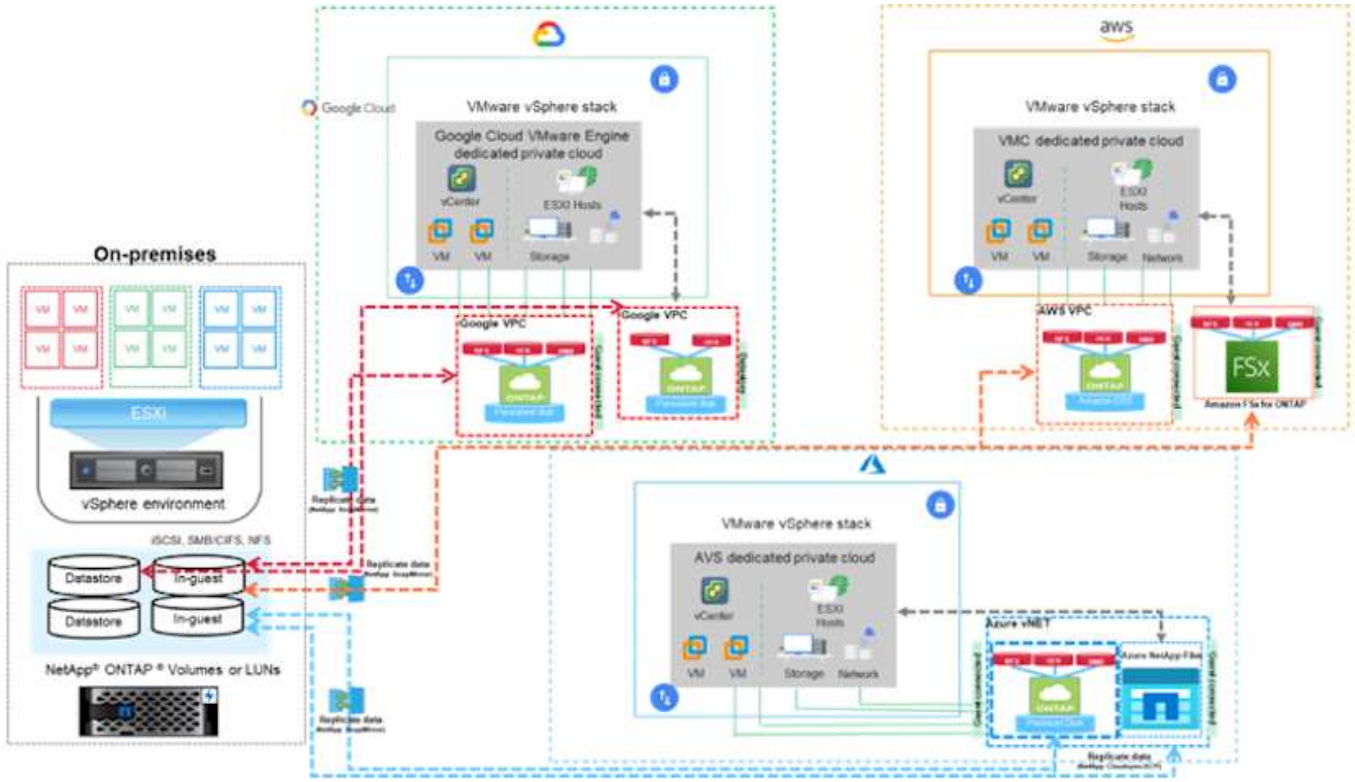
假設

- SnapMirror技術或其他相關的資料移轉機制已啟用。從內部部署到任何超大規模雲端、都有許多連線選項可供選擇。使用適當的途徑、並與相關的網路團隊合作。
- 在寫入本文檔時、來賓儲存設備是唯一可用的選項。 隨著補充NFS資料存放區支援的推出、我們也會提供額外的文件 "請按這裡"。

> 請與NetApp解決方案架構設計師及各自的超大規模雲端架構設計師接洽、以規劃及調整儲存設備規模、以及所需的主機數量。NetApp建議您先找出儲存效能需求、再使用Cloud Volumes ONTAP VMware解決方案、以適當的處理量來完成儲存執行個體類型或適當的服務層級。

詳細架構

從高層面來看、此架構（如下圖所示）涵蓋如何使用NetApp Cloud Volumes ONTAP 解決方案、Cloud Volumes Service 以供Google Cloud使用的支援、以及Azure NetApp Files 以客戶儲存選項形式、在多家雲端供應商之間實現混合式多雲連線和應用程式可攜性。



適用於**VMware**的**NetApp**解決方案

深入瞭解NetApp為三（3）個主要超大規模擴充系統帶來的功能、包括NetApp作為來賓連線儲存設備或輔助NFS資料存放區、移轉工作流程、延伸/突增至雲端、備份/還原及災難恢復。

挑選您的雲端、讓NetApp為您提供更多優勢！

若要查看特定超大規模擴充程式的功能、請按一下該超大規模擴充程式的適當索引標籤。

從下列選項中選取、跳至所需內容的區段：

- "超大規模擴充組態中的VMware"
- "NetApp儲存選項"
- "NetApp / VMware雲端解決方案"

超大規模擴充組態中的**VMware**

如同內部部署、規劃雲端型虛擬化環境對於成功建立虛擬機器和移轉的正式作業就緒環境來說、是非常重要的。

AWS / VMC

本節說明如何在AWS SDDC上設定及管理VMware Cloud、並搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的將Cloud Volumes ONTAP 功能連接到AWS VMC的方法。

設定程序可分為下列步驟：

- 部署及設定適用於AWS的VMware Cloud
- 將VMware Cloud連接至FSX ONTAP VMware

檢視詳細資訊 "VMC的組態步驟"。

Azure / AVS

本節說明如何設定及管理Azure VMware解決方案、以及如何搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的連線Cloud Volumes ONTAP 至Azure VMware解決方案的方法。

設定程序可分為下列步驟：

- 註冊資源供應商並建立私有雲
- 連線至新的或現有的ExpressRoute虛擬網路閘道
- 驗證網路連線能力並存取私有雲端

檢視詳細資訊 "AVS的組態步驟"。

GCP / GCV

本節說明如何設定及管理GCVE,並搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的方法、可將Cloud Volumes ONTAP 「效益」和「雲端Volume服務」連線至GCVE.

設定程序可分為下列步驟：

- 部署及設定GCVE
- 啟用對GCVE的私有存取

檢視詳細資訊 "GCVE.的組態步驟"。

NetApp儲存選項

NetApp 儲存設備可在三個主要的大型超大型超大型超大型擴充器中、以多種方式使用、無論是以來賓連線或作為補充 NFS 資料存放區。

請造訪 "支援的NetApp儲存選項" 以取得更多資訊。

AWS / VMC

AWS支援下列組態的NetApp儲存設備：

- FSX ONTAP 支援以客為本的連線儲存設備
- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- FSX ONTAP 不只是NFS的補充資料存放區

檢視詳細資訊 "VMC的來賓連線儲存選項"。檢視詳細資訊 "VMC的補充NFS資料存放區選項"。

Azure / AVS

Azure以下列組態支援NetApp儲存設備：

- 以客體連線儲存設備的形式提供Azure NetApp Files
- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- 作爲NFS補充資料存放區的能力（ANF Azure NetApp Files ）

檢視詳細資訊 "AVS的來賓連線儲存選項"。檢視詳細資訊 "AVS的補充NFS資料存放區選項"。

GCP / GCV

Google Cloud支援下列組態的NetApp儲存設備：

- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- 以客體連線儲存設備的形式提供資訊（CVS）Cloud Volumes Service
- 作爲NFS補充資料存放區的CVS Cloud Volumes Service

檢視詳細資訊 "GCVE的來賓連線儲存選項"。

深入瞭解 "NetApp Cloud Volumes Service 支援Google Cloud VMware Engine的資料儲存區（NetApp部落格）" 或 "如何使用NetApp CVS做為Google Cloud VMware Engine的資料存放區（Google部落格）"

NetApp / VMware雲端解決方案

有了NetApp和VMware雲端解決方案、許多使用案例都能輕鬆部署到您選擇的超大規模環境中。VMware將主要雲端工作負載使用案例定義為：

- 保護（包括災難恢復和備份/還原）
- 移轉
- 延伸

AWS / VMC

"瀏覽NetApp的AWS / VMC解決方案"

Azure / AVS

"瀏覽適用於Azure / AVS的NetApp解決方案"

GCP / GCV

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

NetApp混合式多雲端搭配**VMware**的支援組態

瞭解NetApp儲存設備在主要大型大型大型大型大型擴充系統中的支援組合。

	來賓連線	補充**NFS Datastor**
* AWS *	CVO FSX ONTAP"詳細資料"	FSX ONTAP"詳細資料"
* Azure *	CVO ANF"詳細資料"	ANF"詳細資料"
* GCP*	CVO CVS"詳細資料"	CVS"詳細資料"

在雲端供應商中設定虛擬化環境

如需如何在每個受支援的超大規模擴充系統中設定虛擬化環境的詳細資訊、請參閱此處。

AWS / VMC

本節說明如何在AWS SDDC上設定及管理VMware Cloud、並搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的將Cloud Volumes ONTAP 功能連接到AWS VMC的方法。

設定程序可分為下列步驟：

- 部署及設定適用於AWS的VMware Cloud
- 將VMware Cloud連接至FSX ONTAP VMware

檢視詳細資訊 "VMC的組態步驟"。

Azure / AVS

本節說明如何設定及管理Azure VMware解決方案、以及如何搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的連線Cloud Volumes ONTAP 至Azure VMware解決方案的方法。

設定程序可分為下列步驟：

- 註冊資源供應商並建立私有雲
- 連線至新的或現有的ExpressRoute虛擬網路閘道
- 驗證網路連線能力並存取私有雲端

檢視詳細資訊 "AVS的組態步驟"。

GCP / GCV

本節說明如何設定及管理GCVE,並搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的方法、可將Cloud Volumes ONTAP 「效益」和「雲端Volume服務」連線至GCVE.

設定程序可分為下列步驟：

- 部署及設定GCVE
- 啟用對GCVE的私有存取

檢視詳細資訊 "GCVE.的組態步驟"。

在**AWS**上部署及設定虛擬化環境

如同內部部署、在AWS上規劃VMware Cloud對於成功建立虛擬機器和移轉的正式作業就緒環境而言、是非常重要的。

本節說明如何在AWS SDDC上設定及管理VMware Cloud、並搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是目前唯一支援的連線Cloud Volumes ONTAP 功能、可將VMware（CVO）連線至AWS VMC。

設定程序可分為下列步驟：

部署及設定適用於**AWS**的**VMware Cloud**

"AWS上的VMware Cloud" 在AWS生態系統中為VMware工作負載提供雲端原生體驗。每個VMware軟體定義資料中心（SDDC）都會在Amazon Virtual Private Cloud（VPC）上執行、並提供完整的VMware堆疊（包括vCenter Server）、NSX-T軟體定義網路、vSAN軟體定義儲存設備、以及一或多個ESXi主機、為您的工作負載提供運算與儲存資源。

本節說明如何在AWS上設定及管理VMware Cloud、並搭配Amazon FSX for NetApp ONTAP 時使用Cloud Volumes ONTAP 、以及/或在AWS上搭配來賓儲存設備使用VMware Cloud。

客體內儲存設備是目前唯一支援的連線Cloud Volumes ONTAP 功能、可將VMware（CVO）連線至AWS VMC。

設定程序可分為三個部分：

註冊**AWS**帳戶

註冊以取得 "Amazon Web Services帳戶"。

假設尚未建立AWS帳戶、您就需要AWS帳戶才能開始使用。無論是新的或現有的、您都需要在帳戶中擁有管理權限、才能執行此程序中的許多步驟。請參閱 "連結" 如需AWS認證資料的詳細資訊、

註冊**My VMware**帳戶

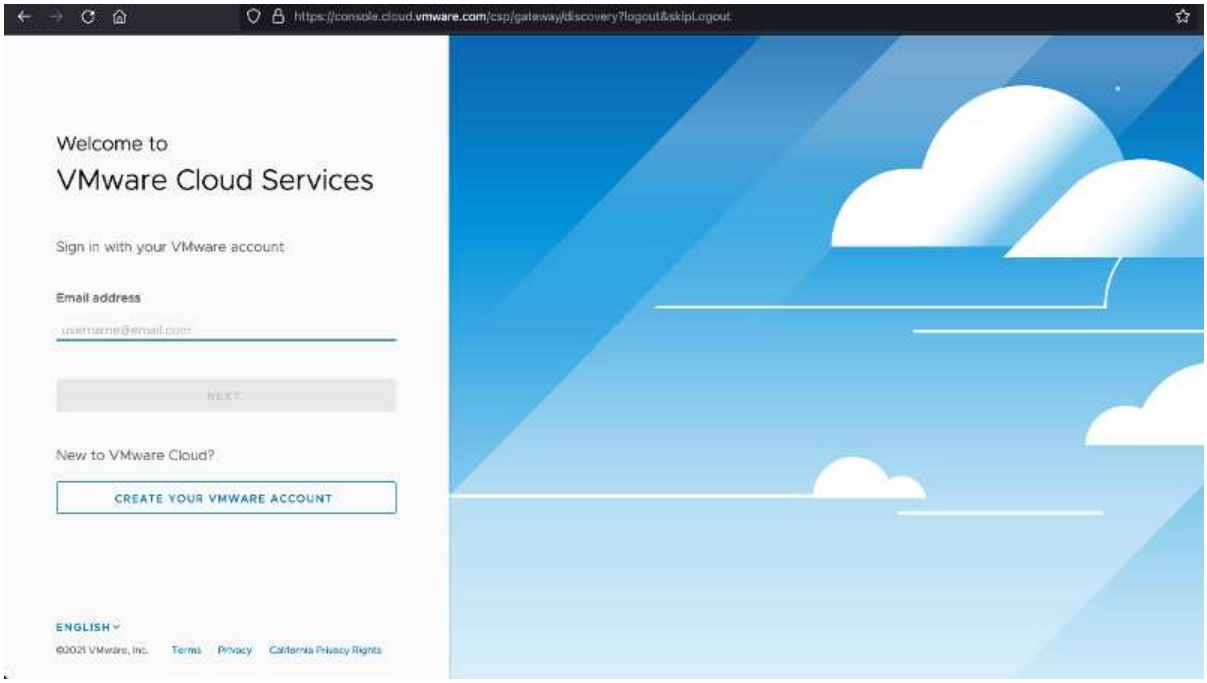
註冊以取得 "我的VMware" 帳戶。

若要存取VMware的雲端產品組合（包括AWS上的VMware Cloud）、您需要VMware客戶帳戶或My VMware帳戶。如果您尚未建立VMware帳戶、請建立該帳戶 "請按這裡"。

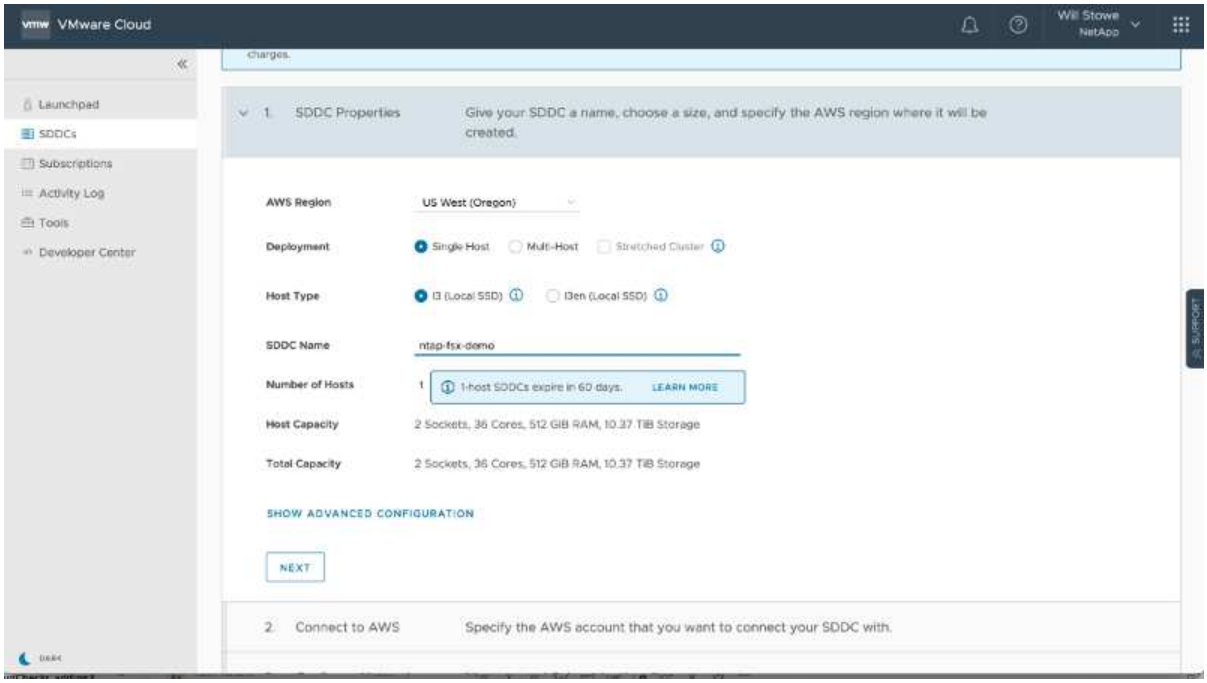
在**VMware Cloud**中配置**SDDC**

設定VMware帳戶並執行適當規模調整之後、部署軟體定義的資料中心是在AWS服務上使用VMware Cloud的下一步。若要建立SDDC、請挑選一個AWS區域來裝載它、為SDDC命名、然後指定您希望SDDC包含多少ESXi主機。如果您尚未擁有AWS帳戶、您仍可建立包含單一ESXi主機的入門組態SDDC。

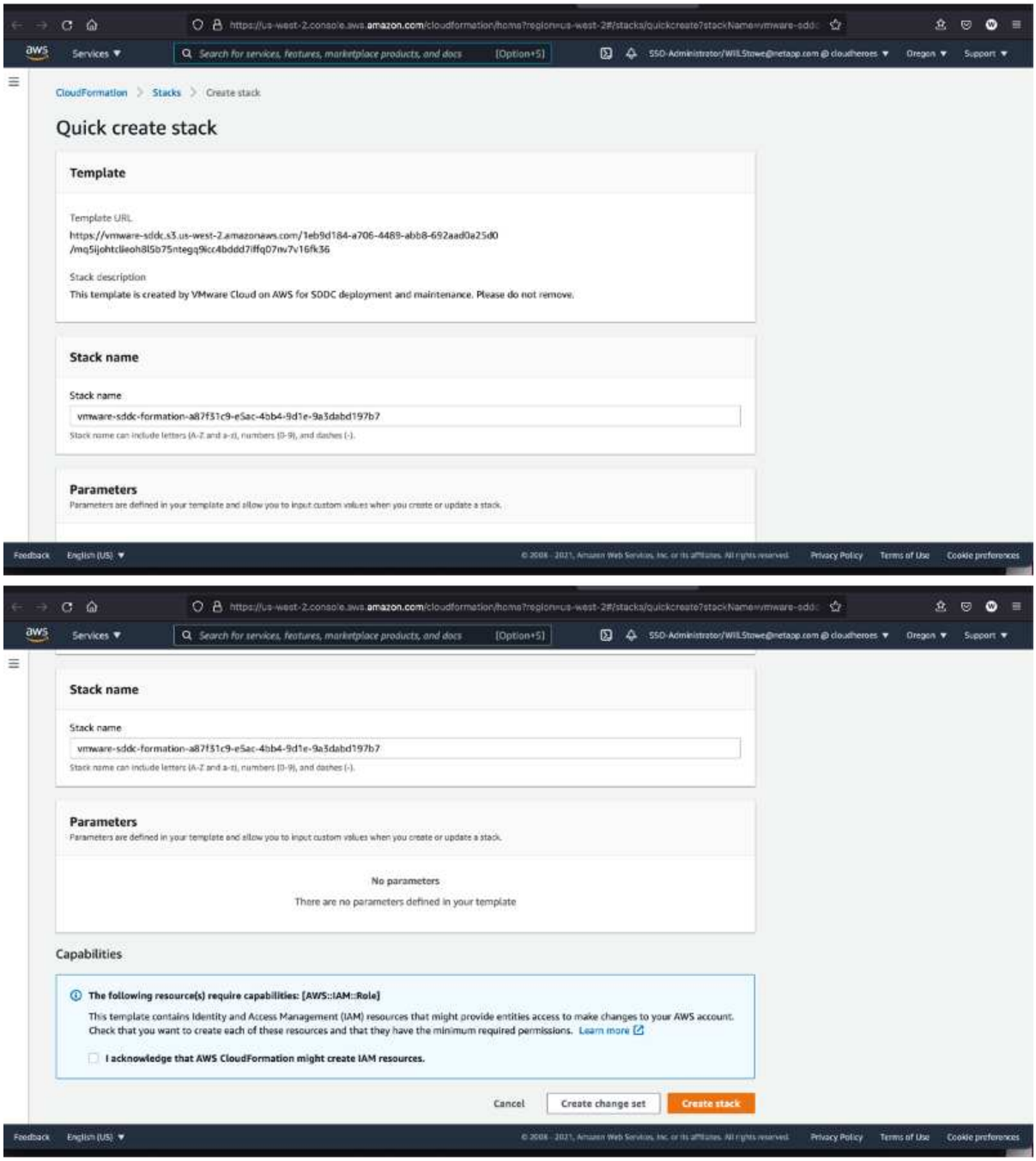
1. 使用現有或新建立的VMware認證資料登入VMware Cloud Console。



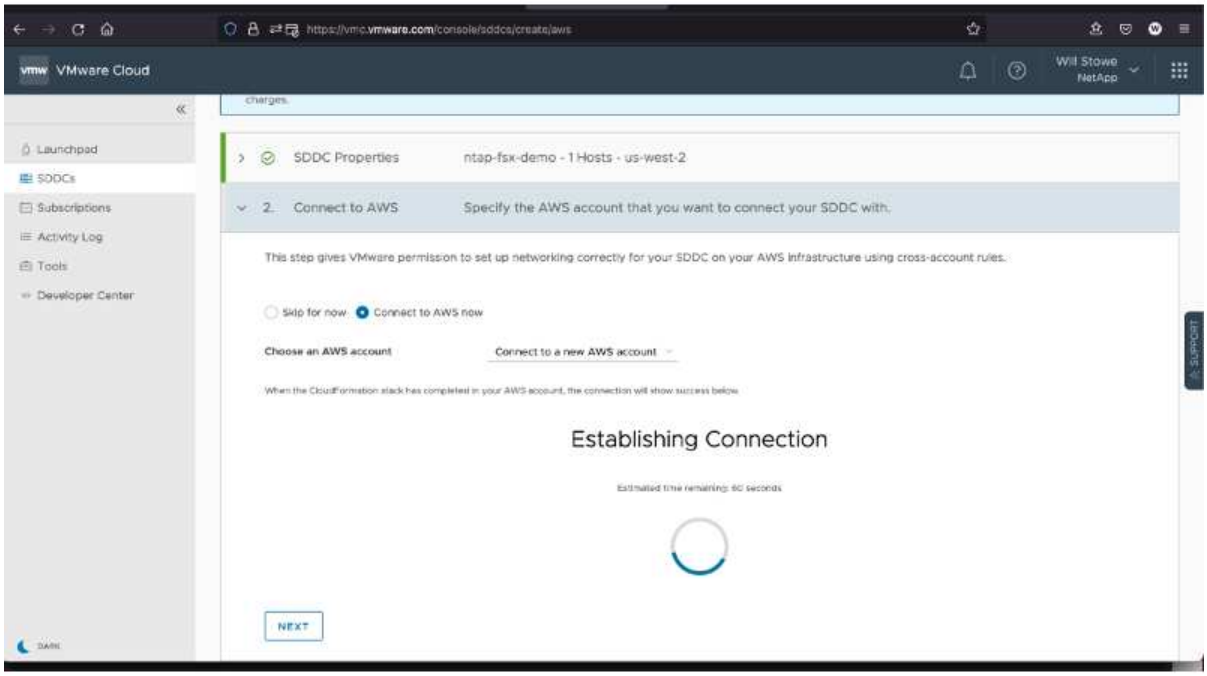
2. 設定AWS區域、部署和主機類型、以及SDDC名稱：

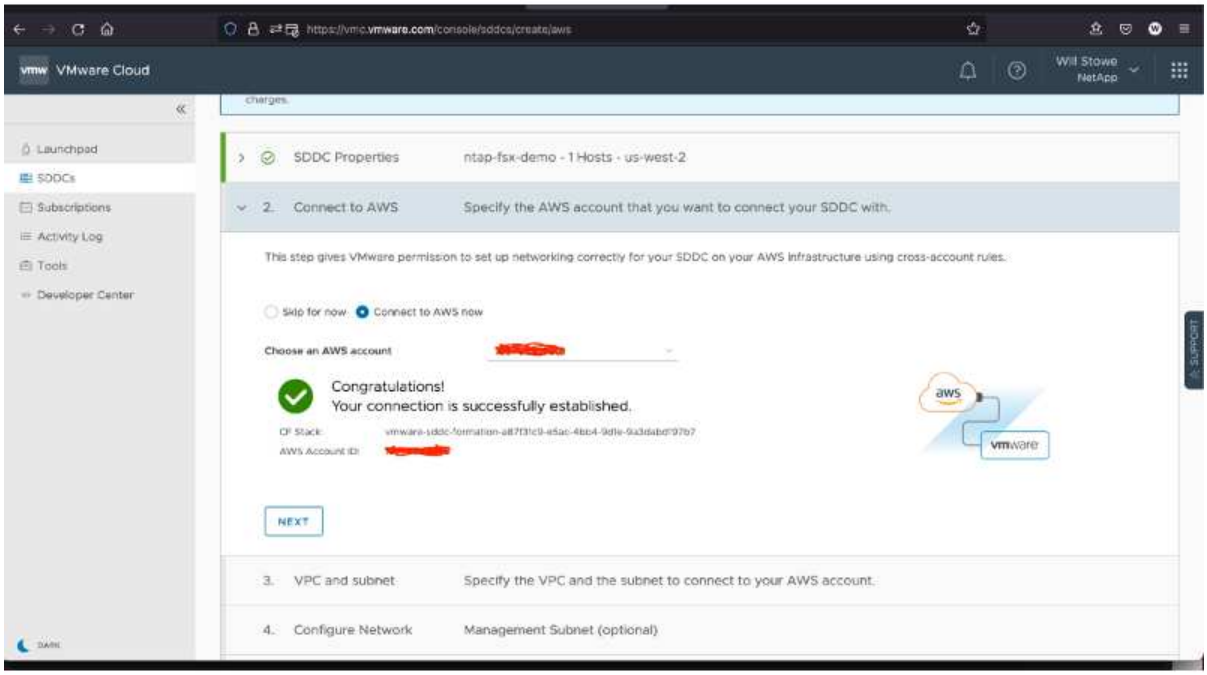


3. 連線至所需的AWS帳戶、然後執行AWS Cloud formation堆疊。


CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ijohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences

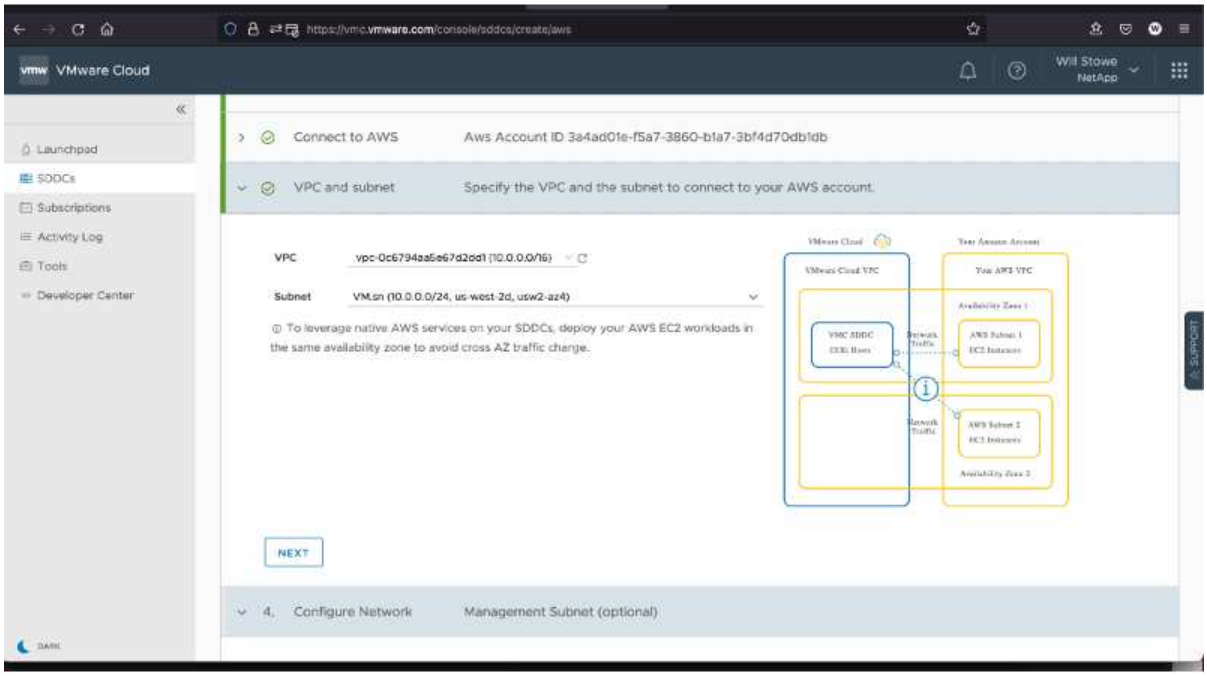
Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There 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
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences



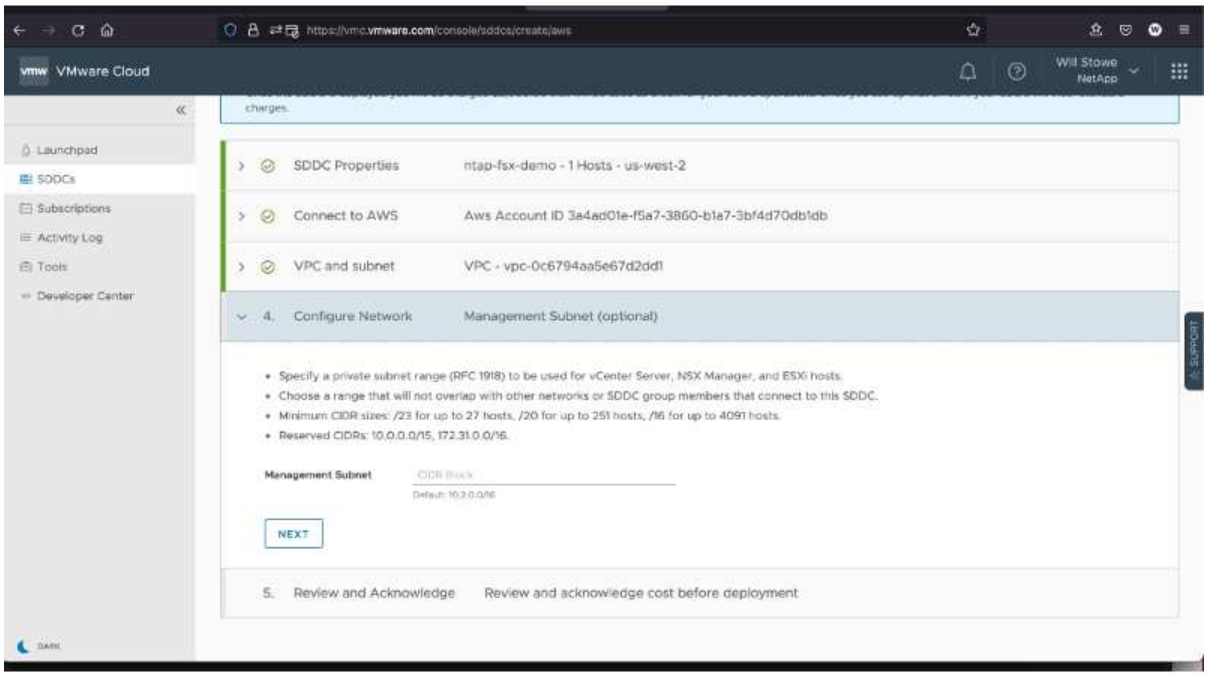


此驗證使用單一主機組態。

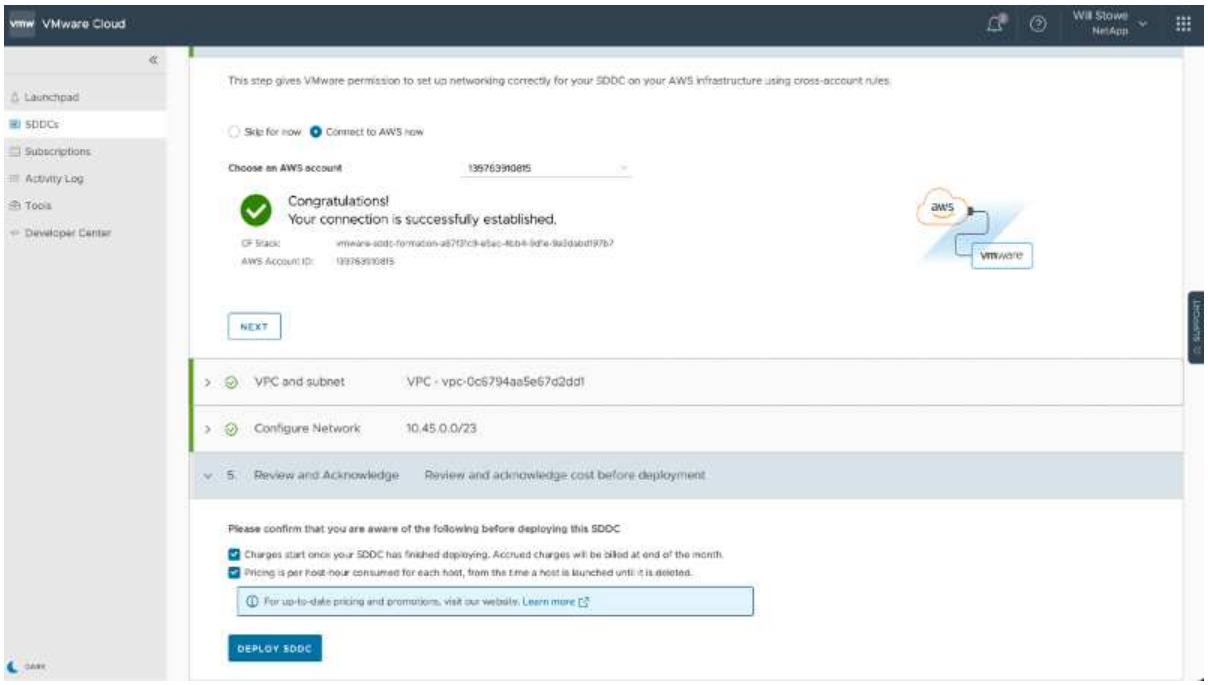
4. 選取所需的AWS VPC、以連接VMC環境。



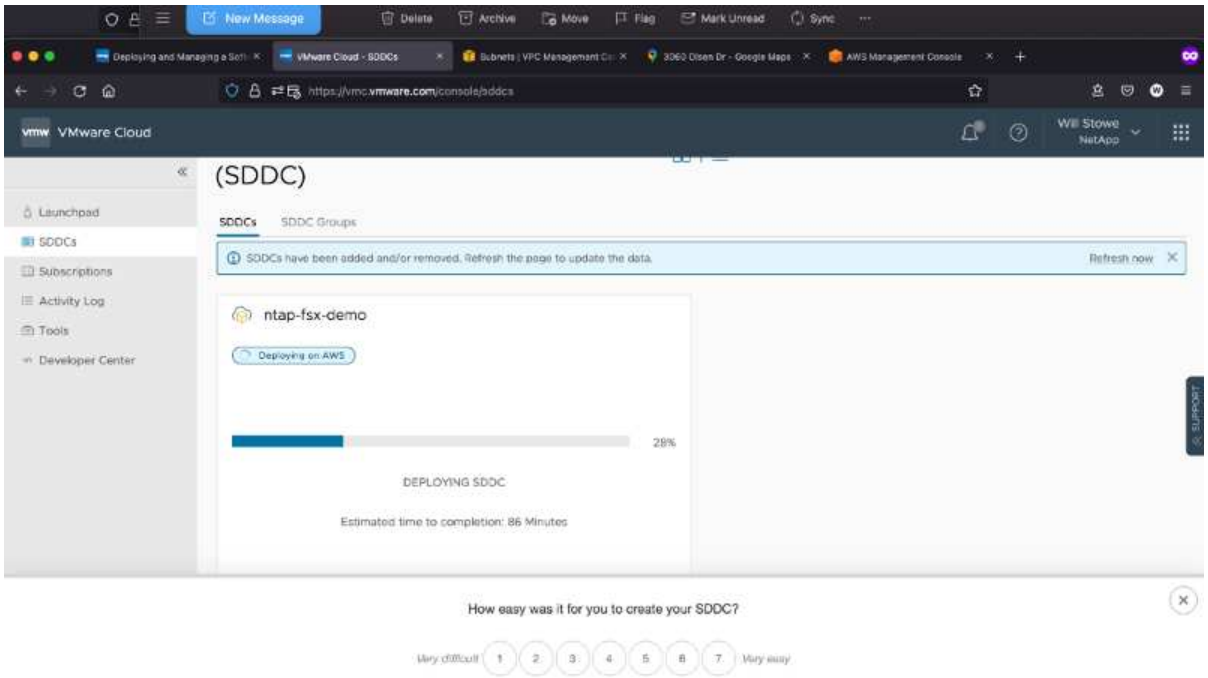
5. 設定VMC管理子網路；此子網路包含vCenter、NSX等VMC託管服務。請勿選擇與任何其他需要連線至SDDC環境的網路重疊的位址空間。最後、請遵循以下所述的CIDR大小建議。



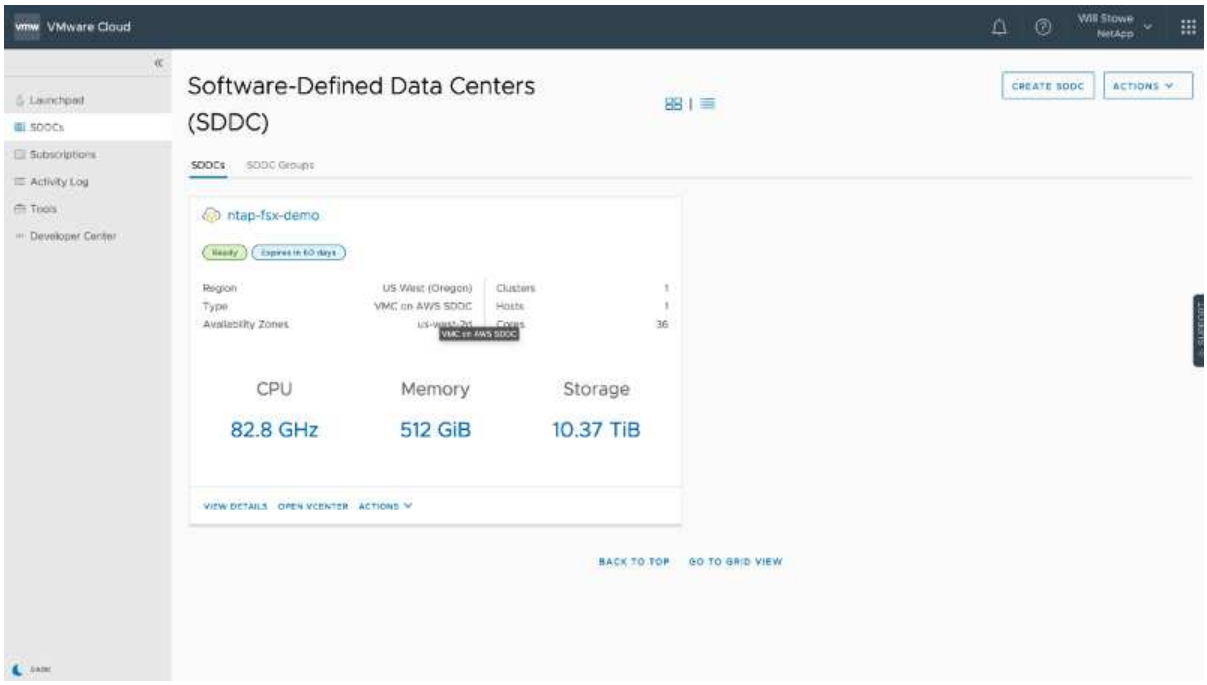
6. 檢閱並確認SDDC組態、然後按一下「部署SDDC」。



部署程序通常需要約兩小時才能完成。



7. 完成後、SDDC即可開始使用。

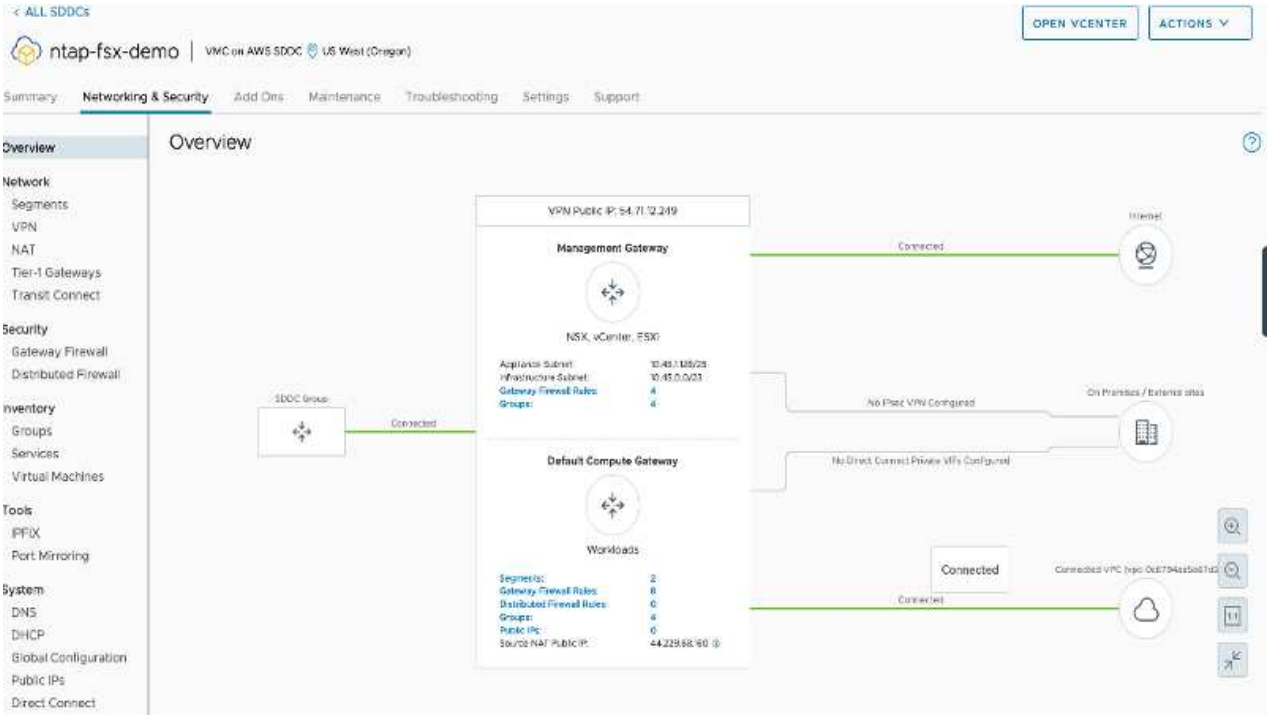


如需SDDC部署的逐步指南、請參閱 "從VMC主控台部署SDDC"。

將**VMware Cloud**連接至**FSX ONTAP VMware**

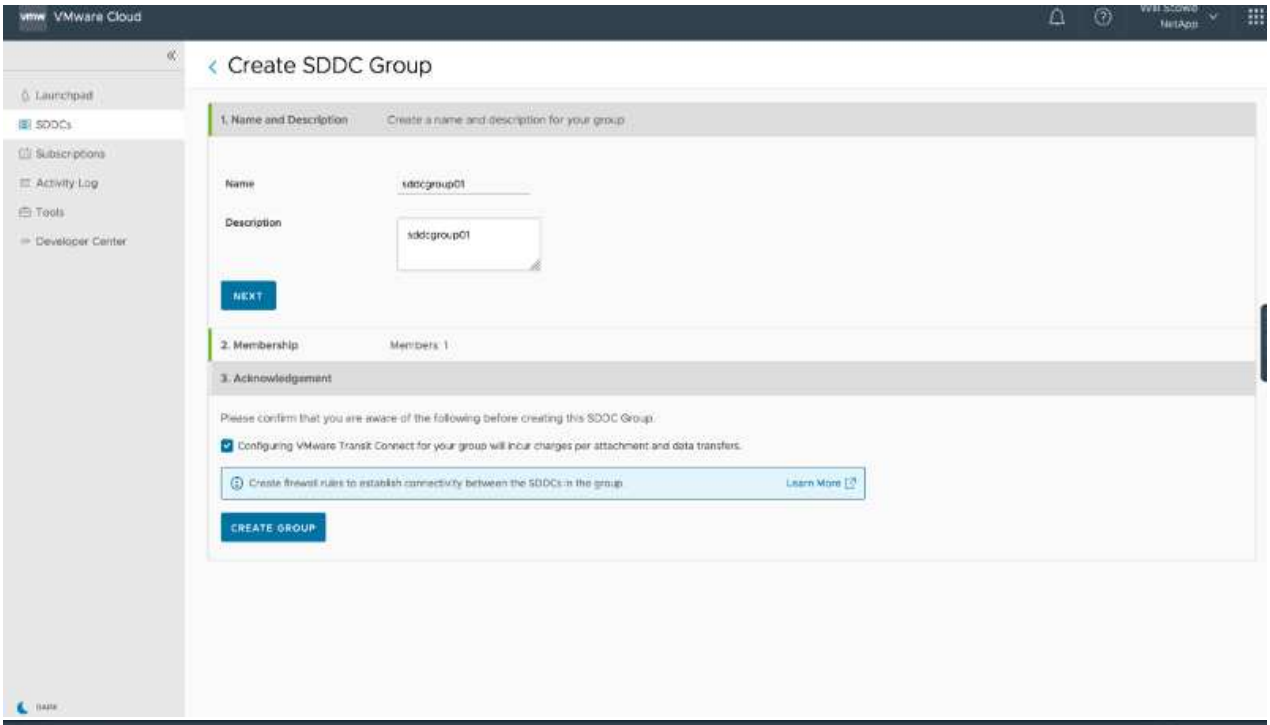
若要將VMware Cloud連接至FSXVMware ONTAP 、請完成下列步驟：

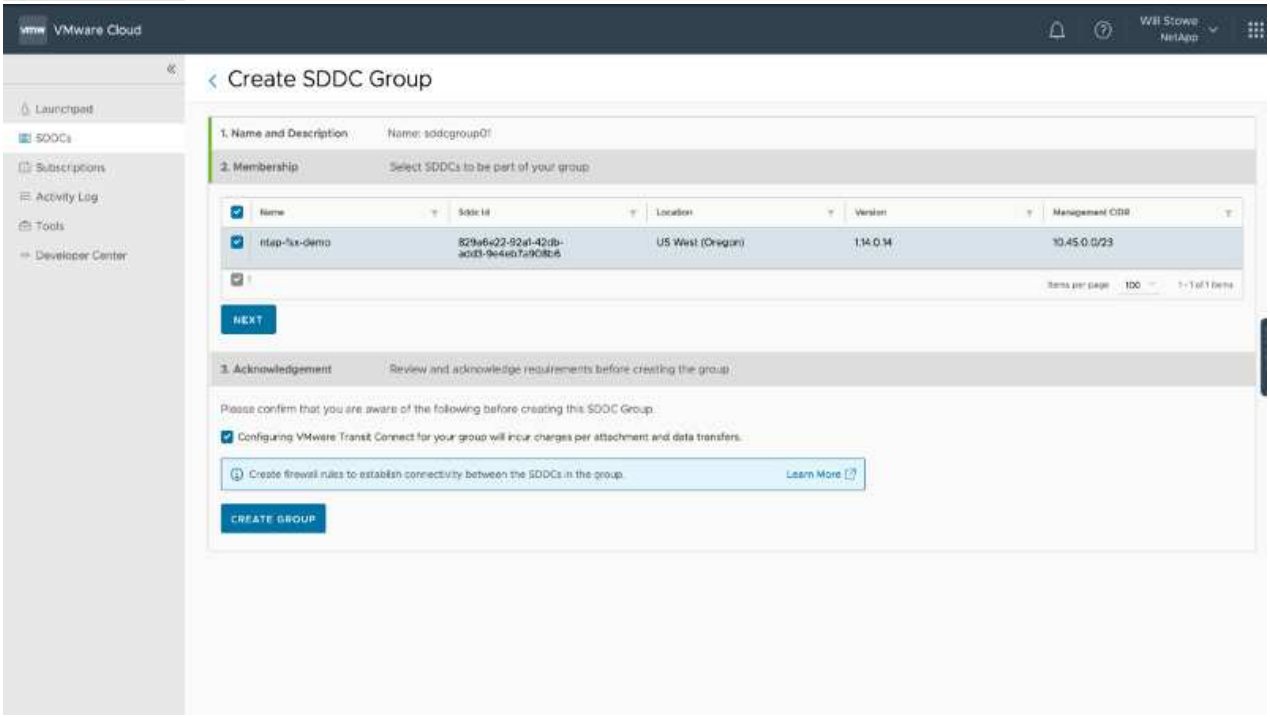
1. 完成VMware Cloud部署並連線至AWS VPC後、您必須將Amazon FSX for NetApp ONTAP 支援部署至新的VPC、而非原始連線的VPC（請參閱下方螢幕快照）。如果FSX（NFS和SMB浮動IP）部署在連線的VPC上、則無法存取。請記住Cloud Volumes ONTAP 、像是支援的iSCSI端點、在連線的VPC上運作正常。

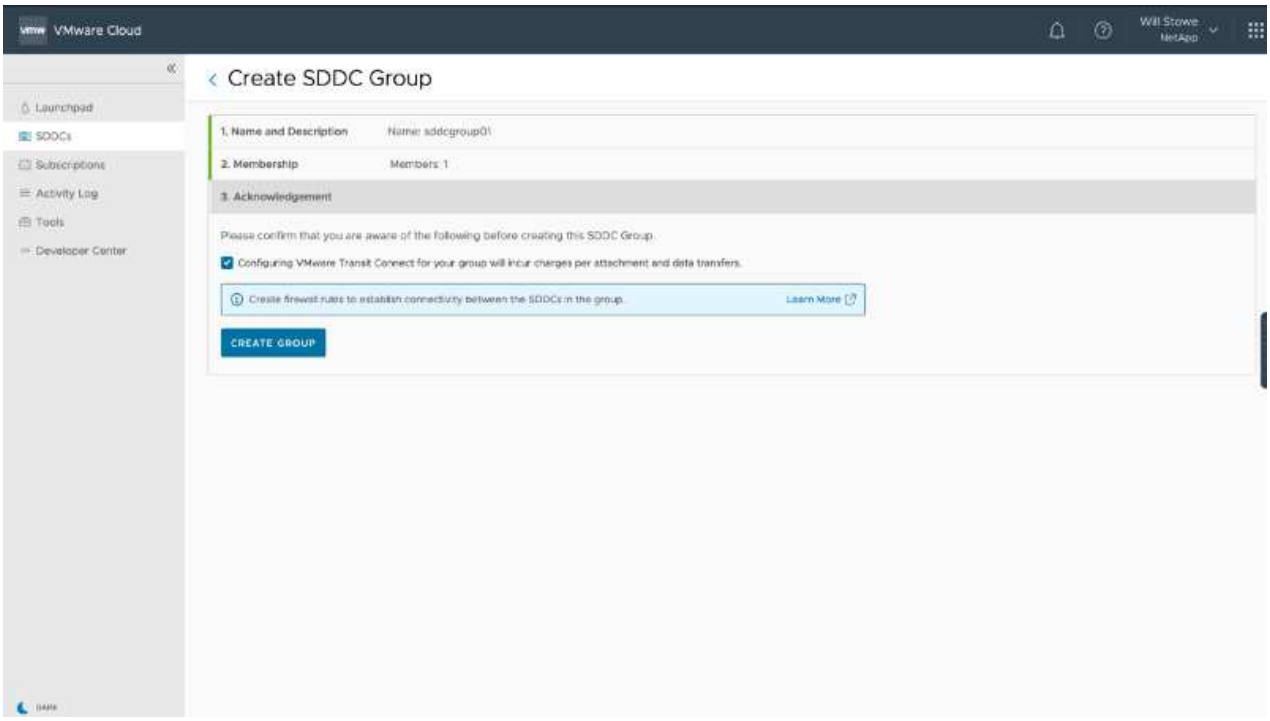


2. 在同一個地區部署額外的VPC、然後將Amazon FSX for NetApp ONTAP 支援VPC部署到新的VPC。

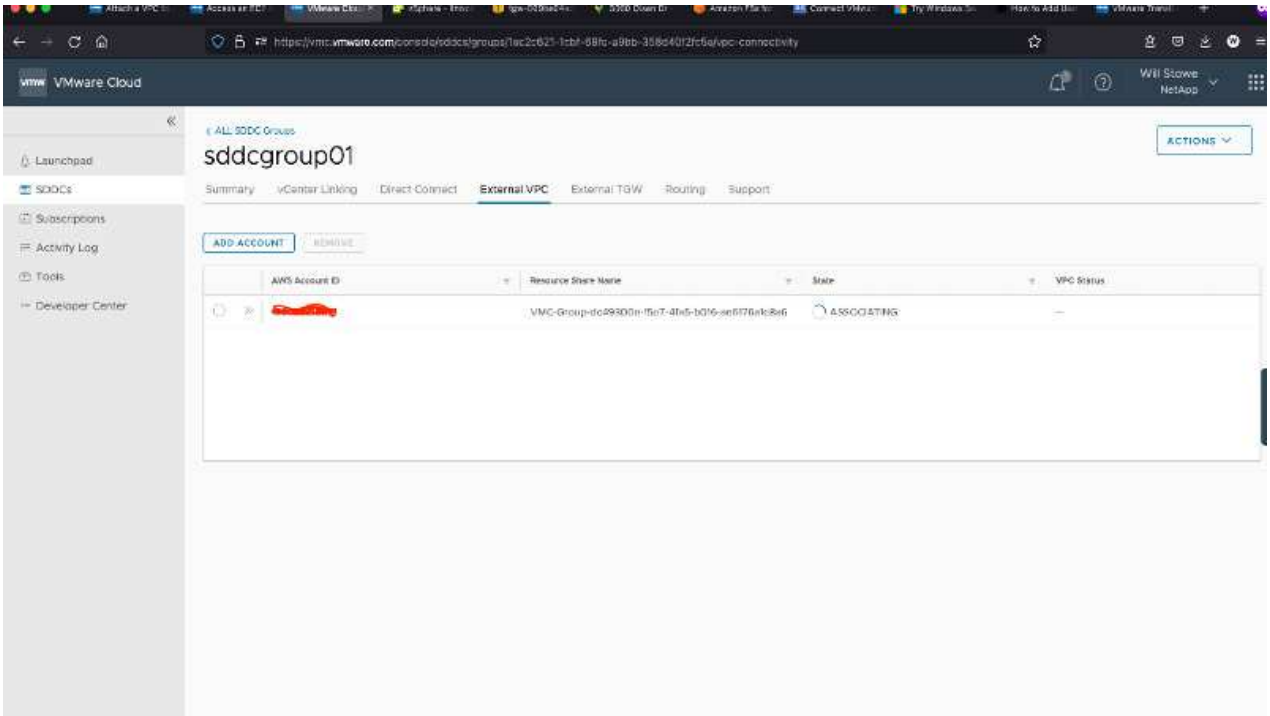
   在VMware Cloud主控台中設定SDDC群組、可提供連線至部署FSx的新VPC所需的網路組態選項。在步驟3中、確認已勾選「為您的群組設定VMware Transit Connect將會產生每個附件和資料傳輸的費用」、然後選擇「建立群組」。此程序可能需要幾分鐘的時間才能完成。

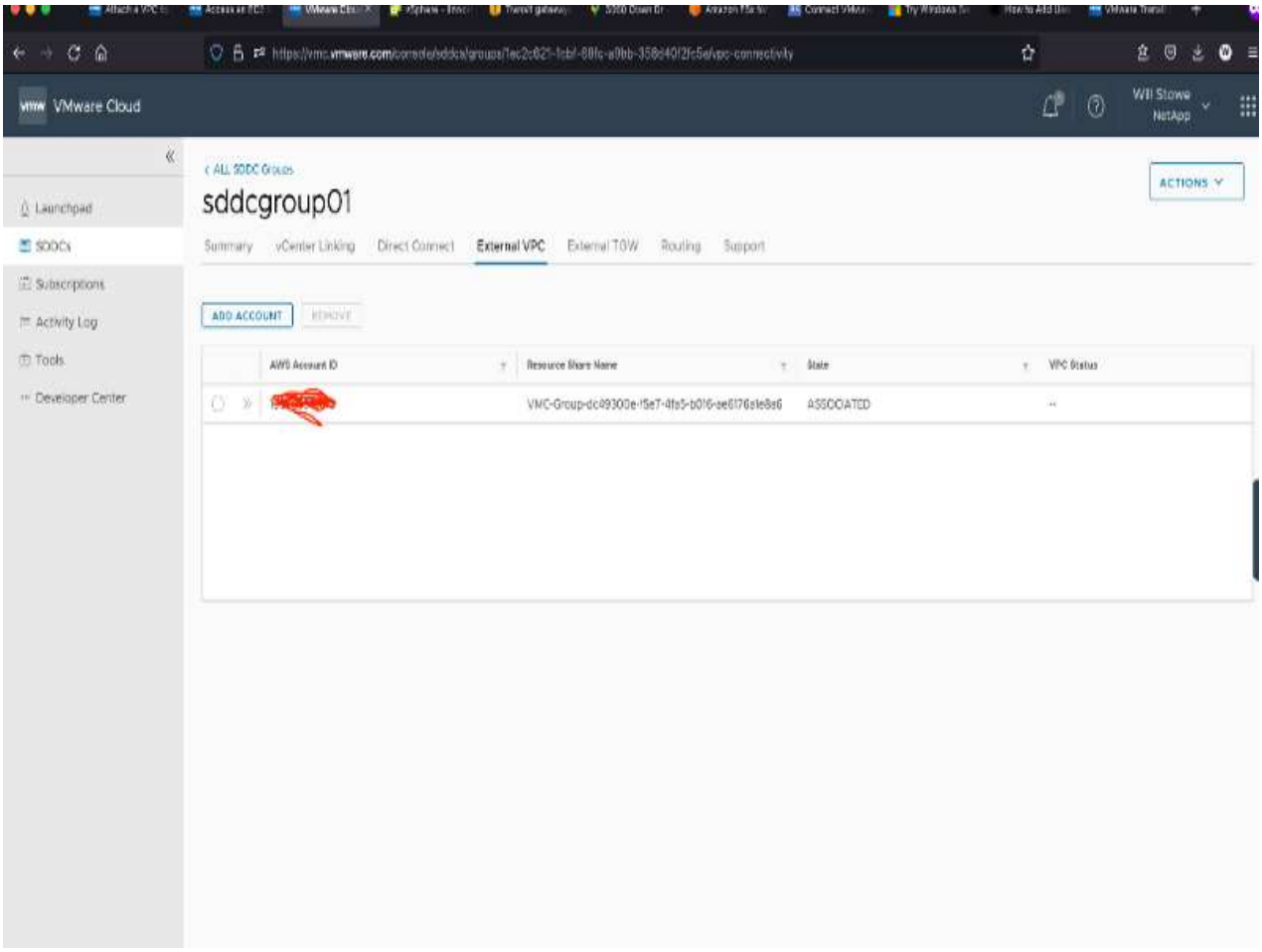

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP


VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6e22-92a1-42db-
acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page
100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

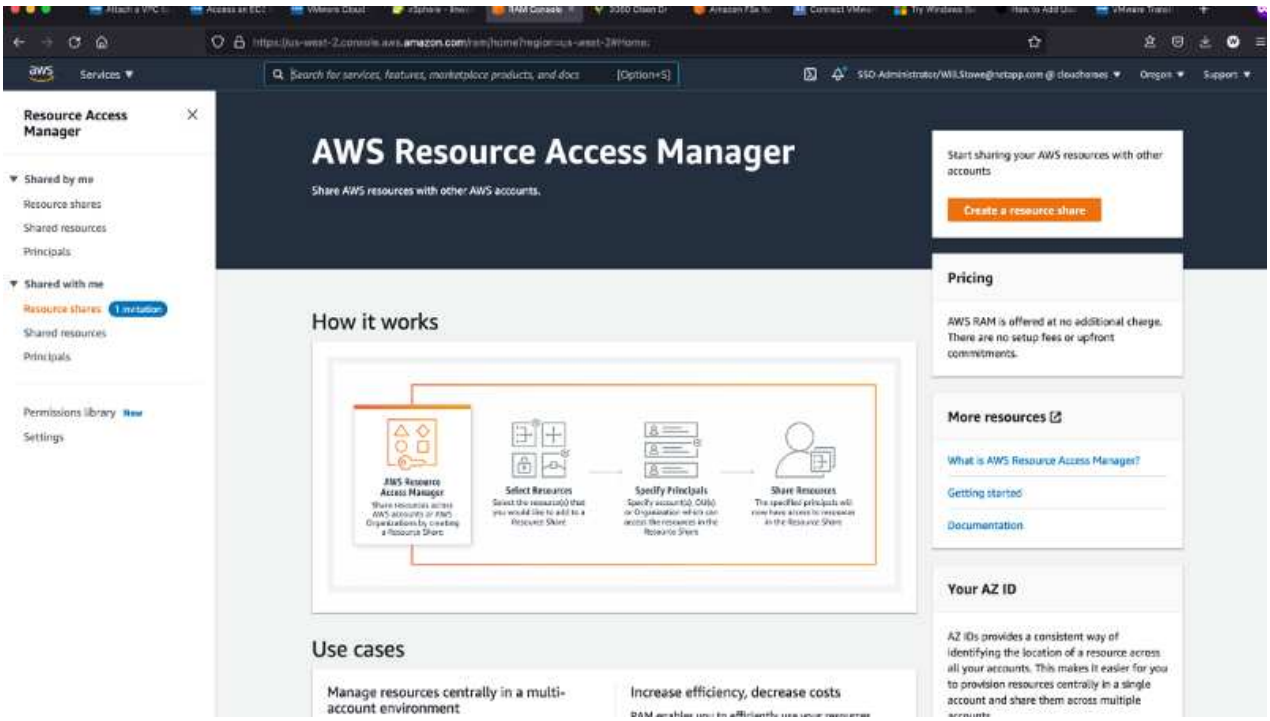


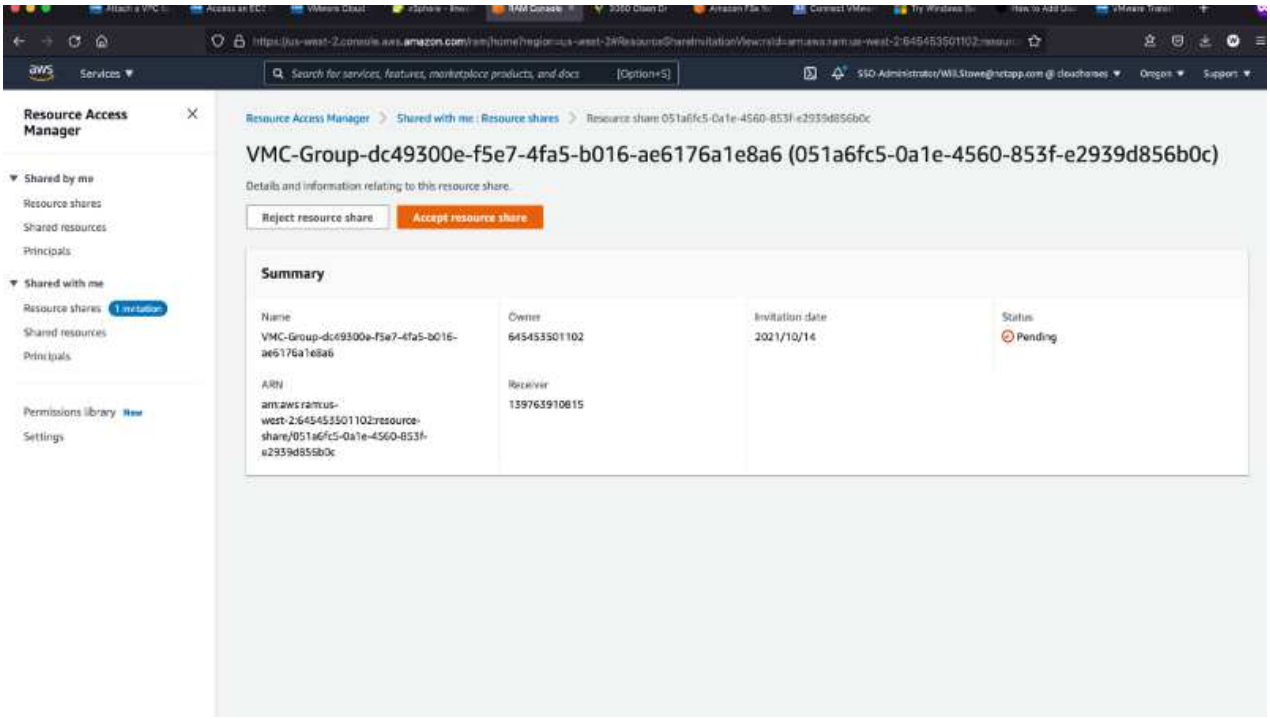
3. 將新建立的VPC附加至剛建立的SDDC群組。選取「外部VPC」索引標籤、然後遵循 "連接外部VPC的說明" 給群組。此程序可能需要10至15分鐘才能完成。



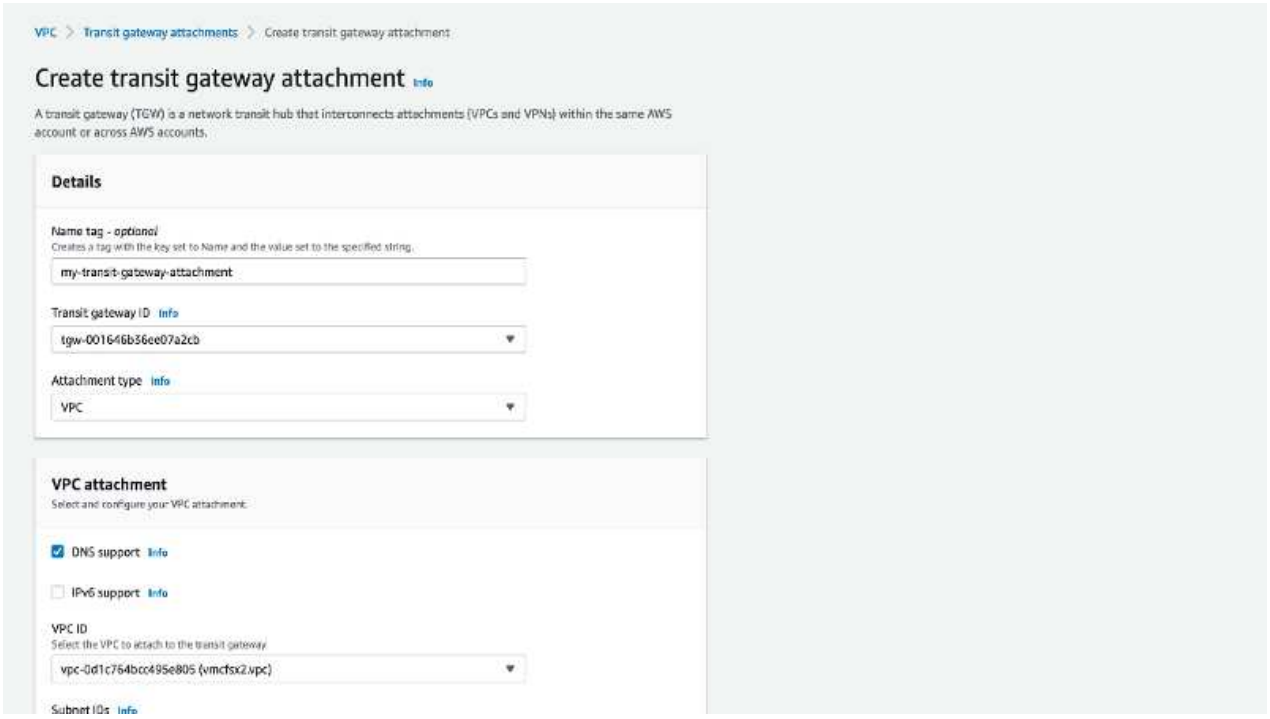


4. 在外部VPC程序中、系統會透過AWS主控台、透過資源存取管理程式提示您移至新的共用資源。共享資源是 "AWS Transit閘道" 由VMware Transit Connect管理。

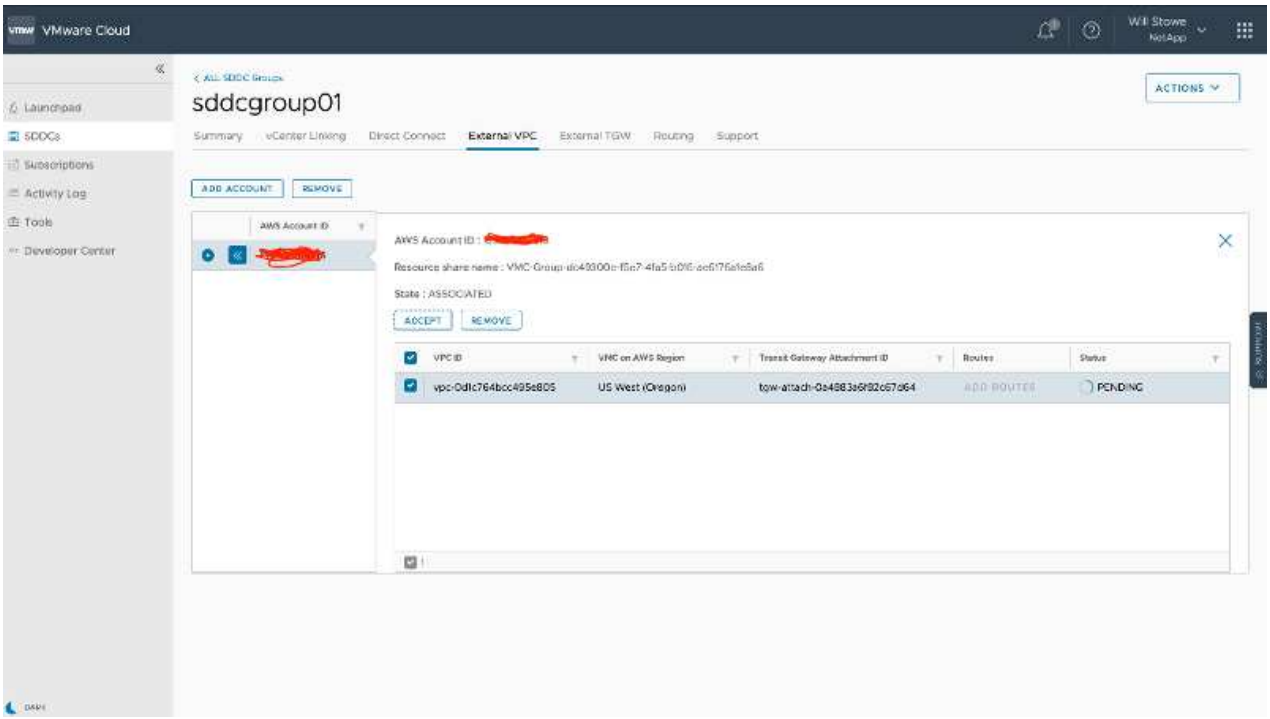




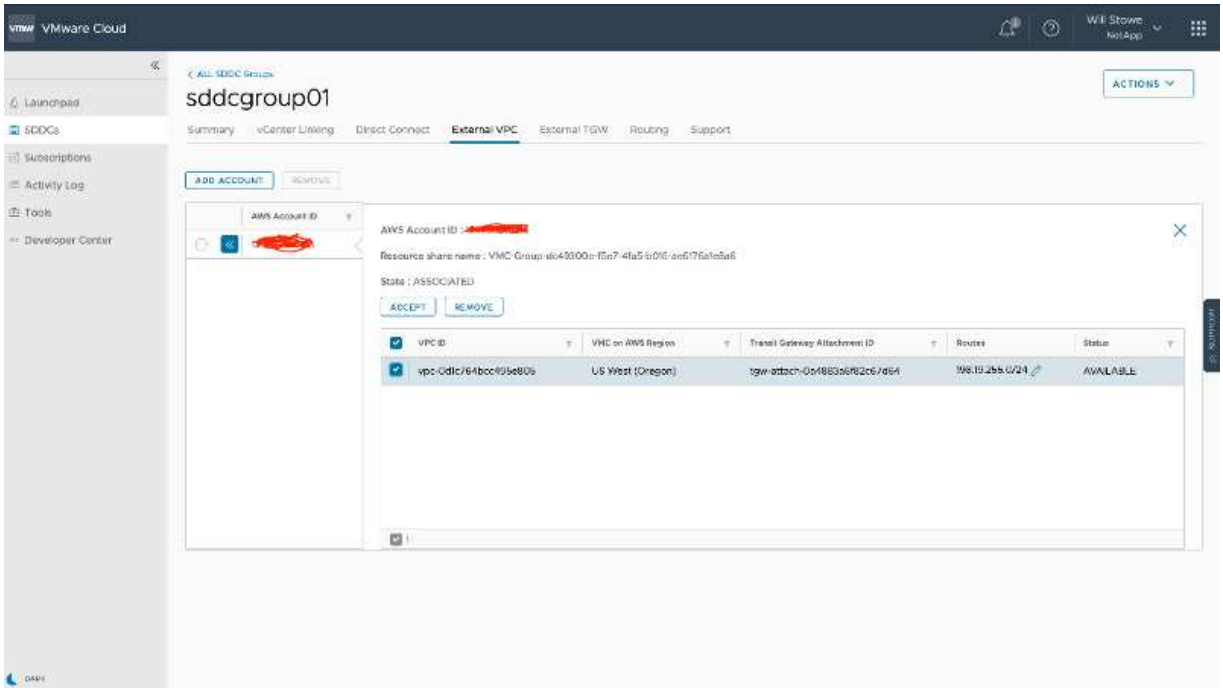
5. 建立Transit Gateway附件。



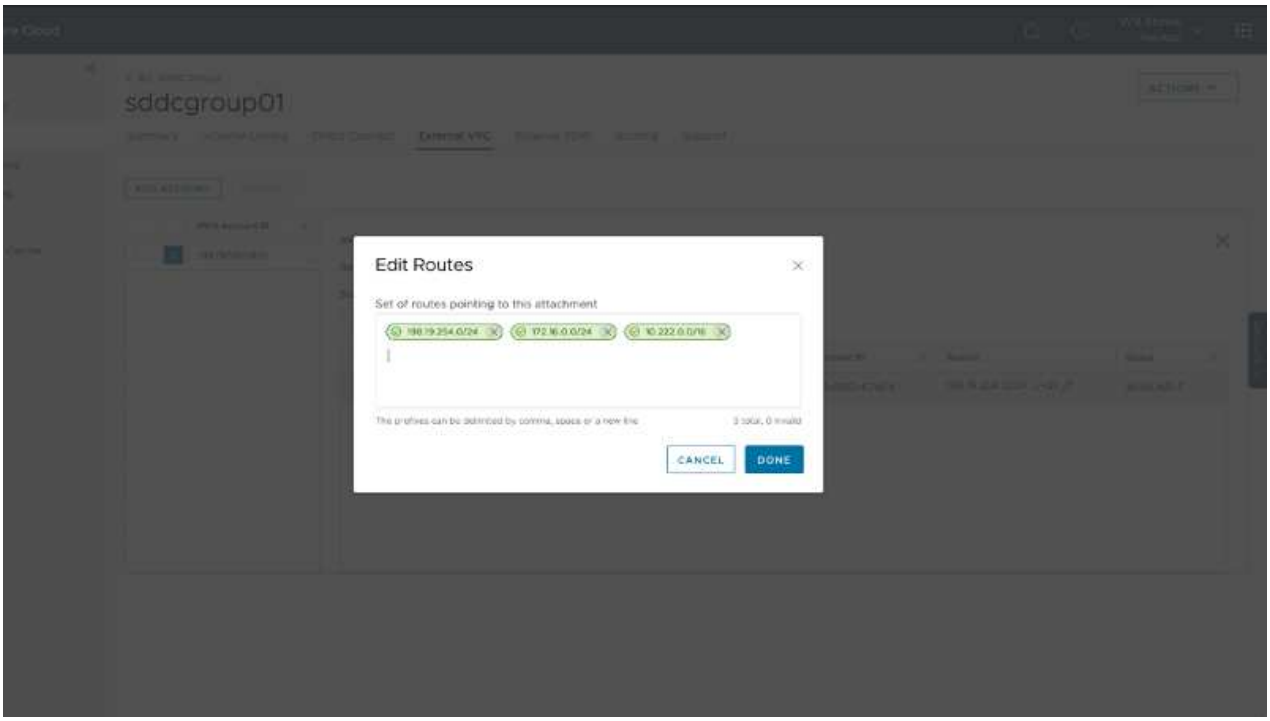
6. 回到VMC主控台、接受VPC附件。完成此程序大約需要10分鐘。



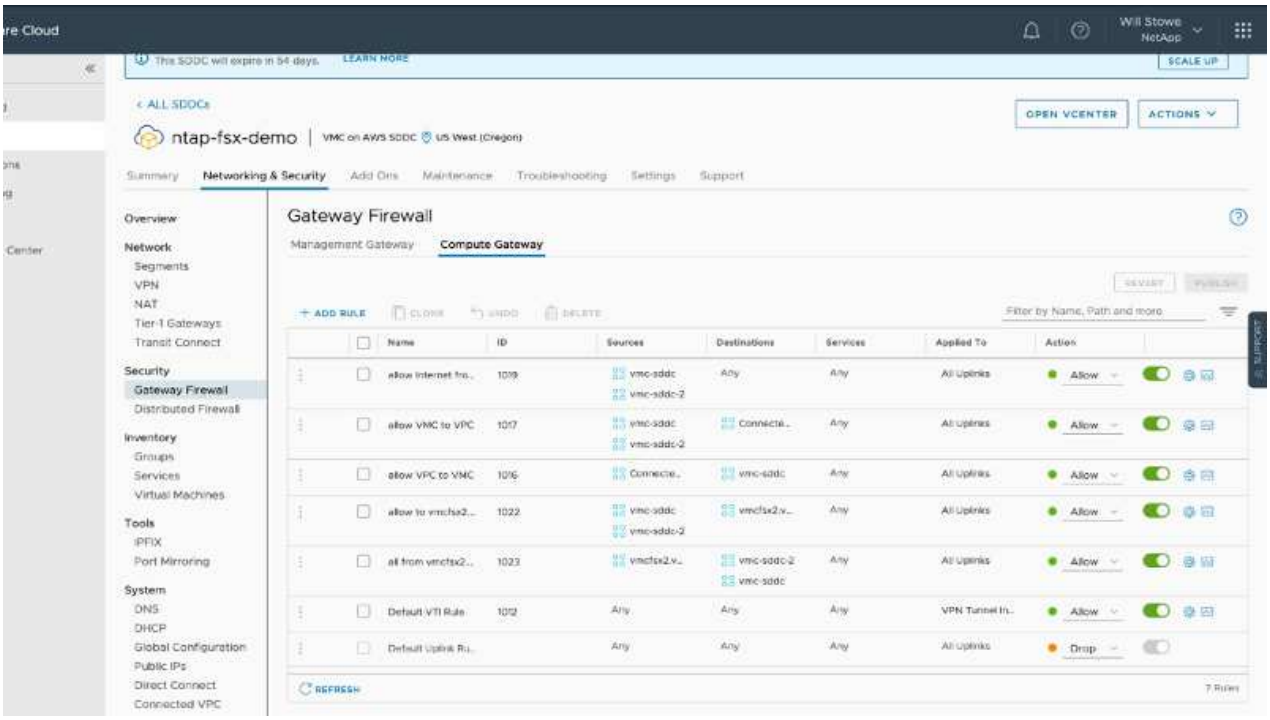
7. 在「外部VPC」索引標籤中、按一下「路由」欄中的編輯圖示、然後新增下列必要路由：
   - Amazon FSX for NetApp ONTAP 的浮動IP範圍路由 "浮動IP"。
   - 適用於靜態的浮動IP範圍路由Cloud Volumes ONTAP （若適用）。
   - 新建立外部VPC位址空間的路由。



8. 最後、允許雙向流量 "防火牆規則" 以存取FSx/CVO。請依照下列步驟操作 "詳細步驟" 適用於SDDC工作負載連線的運算閘道防火牆規則。



9. 為管理和運算閘道設定防火牆群組之後、即可存取vCenter、如下所示：



下一步是根據ONTAP 您的需求、確認Amazon FSX Sfor Cloud Volumes ONTAP 支援功能已設定完成、而且已配置磁碟區以卸載vSAN的儲存元件、以最佳化部署。

在**Azure**上部署及設定虛擬化環境

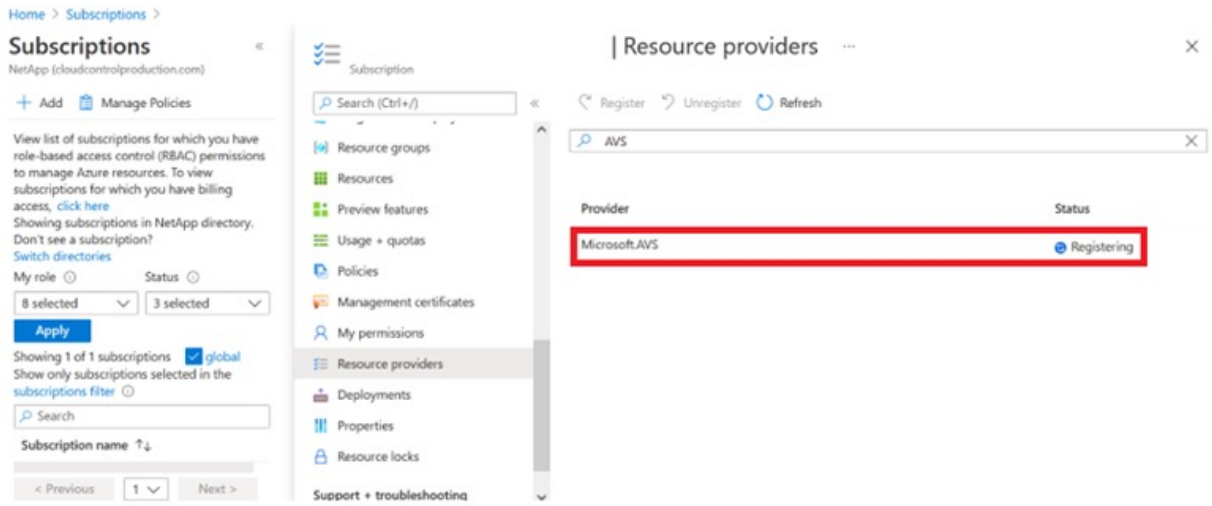
如同內部部署、規劃Azure VMware解決方案對於成功建立虛擬機器和移轉的正式作業就緒環境而言、是非常重要的。

本節說明如何設定及管理Azure VMware解決方案、以及如何搭配可用的選項來連接NetApp儲存設備。

設定程序可分為下列步驟：

若要使用Azure VMware解決方案、請先在指定的訂閱中註冊資源供應商：

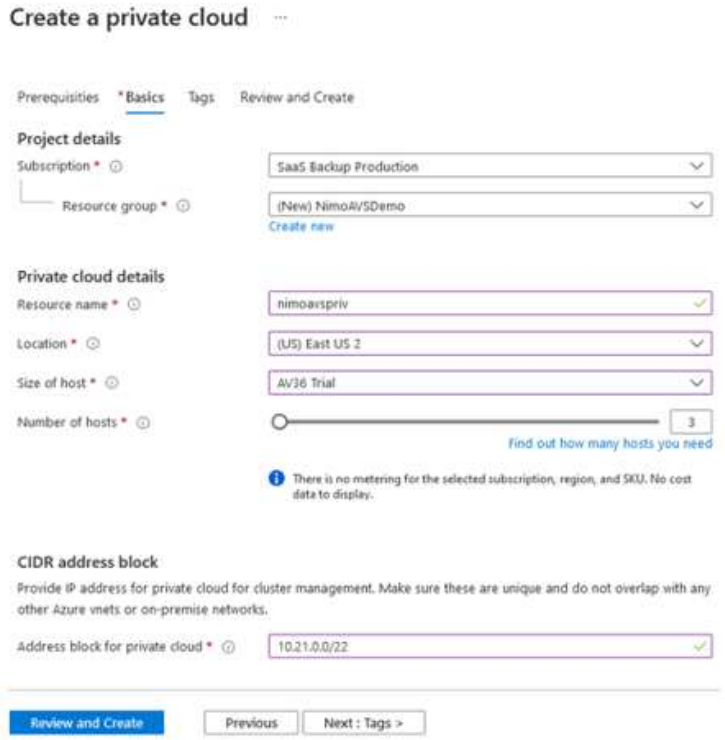
1. 登入Azure入口網站。
2. 在Azure入口網站功能表上、選取All Services（所有服務）。
3. 在「所有服務」對話方塊中、輸入訂閱內容、然後選取「訂閱」。
4. 若要檢視、請從訂閱清單中選取訂閱。
5. 選取資源供應商、然後在搜尋中輸入microsoft.AVS。
6. 如果資源供應商尚未登錄、請選取「註冊」。



7. 在資源供應商註冊之後、請使用Azure入口網站建立Azure VMware解決方案私有雲。
8. 登入Azure入口網站。
9. 選取「Create a New Resource（建立新資源）」。
10. 在「搜尋市場」文字方塊中、輸入Azure VMware解決方案、然後從結果中選取。
11. 在Azure VMware解決方案頁面上、選取建立。
12. 從「基礎」索引標籤、在欄位中輸入值、然後選取「檢閱」+「建立」。

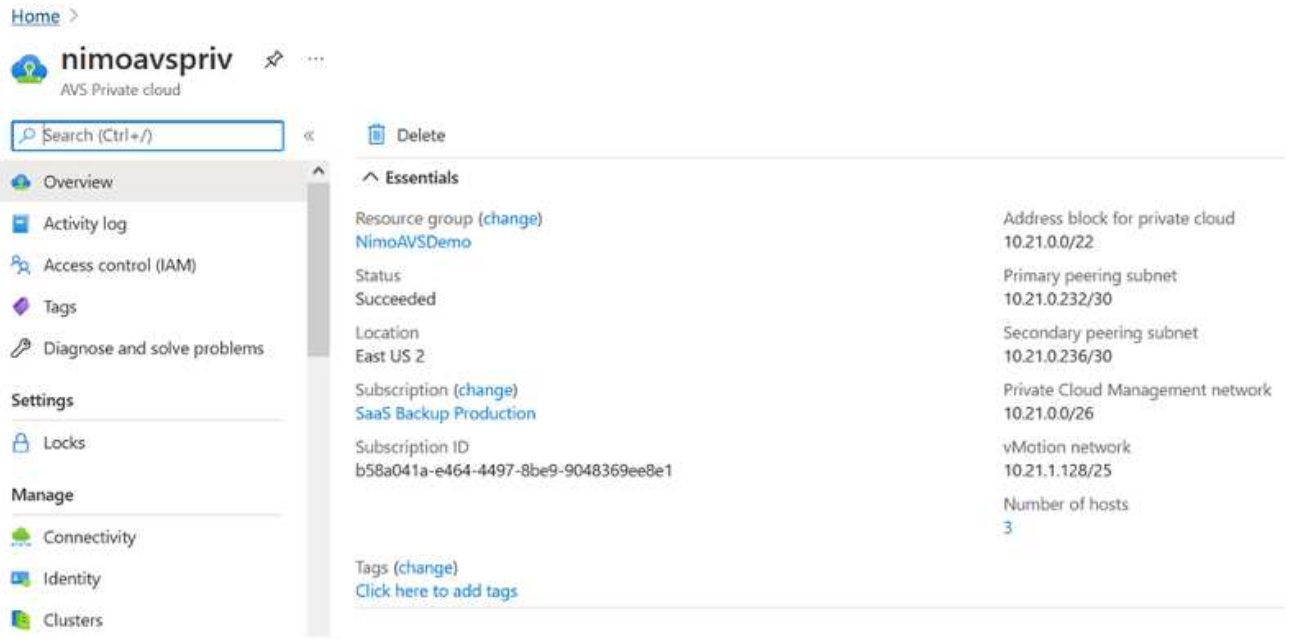
附註：

- 若要快速入門、請在規劃階段收集所需資訊。
- 選取現有的資源群組、或為私有雲建立新的資源群組。資源群組是部署及管理Azure資源的邏輯容器。
- 請確定CIDR位址是唯一的、且不會與其他Azure虛擬網路或內部部署網路重疊。CIDR代表私有雲端管理網路、用於叢集管理服務、例如vCenter Server和NSxT-T Manager。NetApp建議使用/22位址空間。在此範例中、使用10.21.0/22。



資源配置程序約需4至5小時。程序完成後、請從Azure入口網站存取私有雲、確認部署是否成功。部署完成時、會顯示「成功」狀態。

Azure VMware解決方案私有雲需要Azure虛擬網路。由於Azure VMware解決方案不支援內部部署vCenter、因此需要採取其他步驟、才能與現有的內部部署環境整合。也需要設定ExpressRoute電路和虛擬網路閘道。等待叢集資源配置完成時、請建立新的虛擬網路、或使用現有的網路來連線至Azure VMware解決方案。



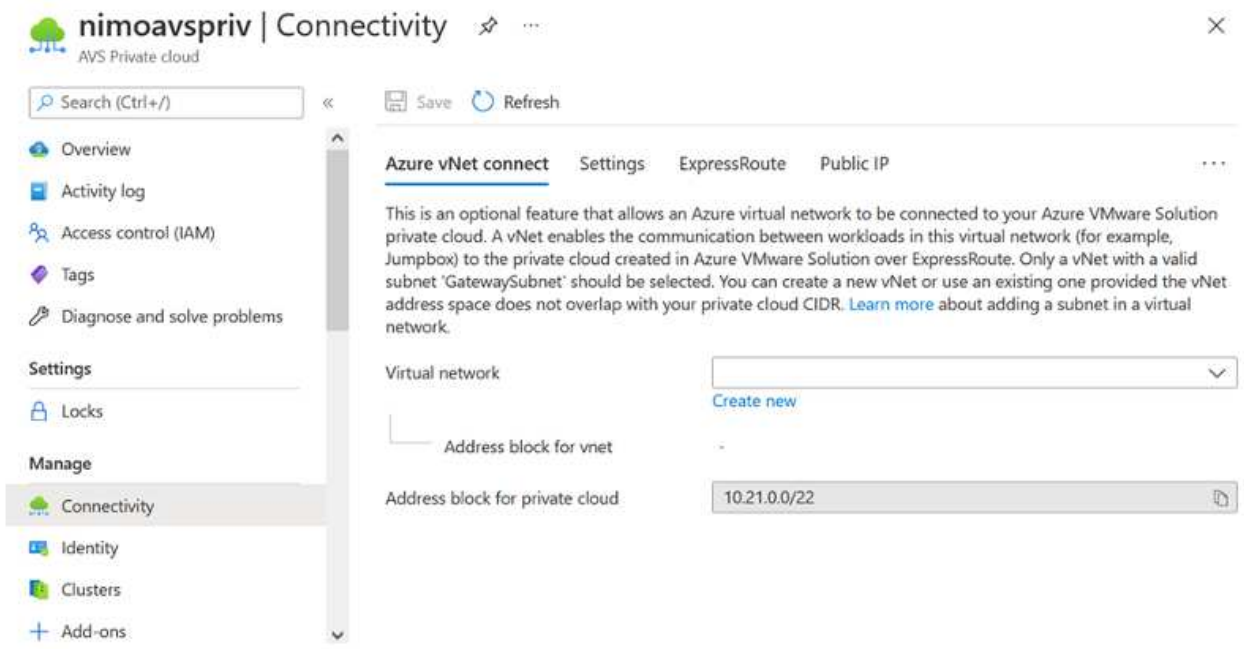
連線至新的或現有的**ExpressRoute**虛擬網路閘道

若要建立新的Azure虛擬網路（vnet）、請選取Azure vnet Connect索引標籤。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：

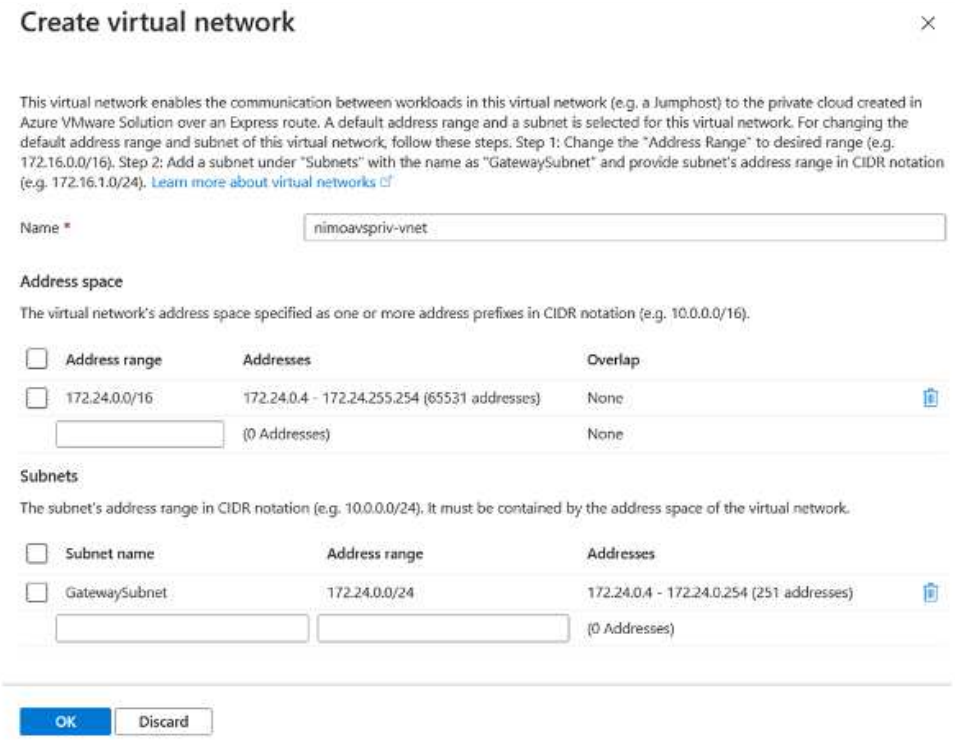
1. 前往Azure VMware解決方案私有雲、並在「Manage（管理）」選項下存取「Connectivity（連線能力）」。
2. 選取Azure Vnet Connect。
3. 若要建立新的vnet、請選取「Create New」（建立新的）選項。

   此功能可讓Vnet連線至Azure VMware解決方案私有雲。vnet可自動建立所需元件（例如跳接箱、Azure NetApp Files 共享服務（例如：VMware、VMware、Cloud Volume ONTAP 等）、並透過ExpressRoute建立在Azure VMware解決方案中的私有雲、藉此在虛擬網路中的工作負載之間進行通訊。

   附註： vnet位址空間不應與私有雲端CIDR重疊。



4. 提供或更新新vnet的資訊、然後選取「確定」。

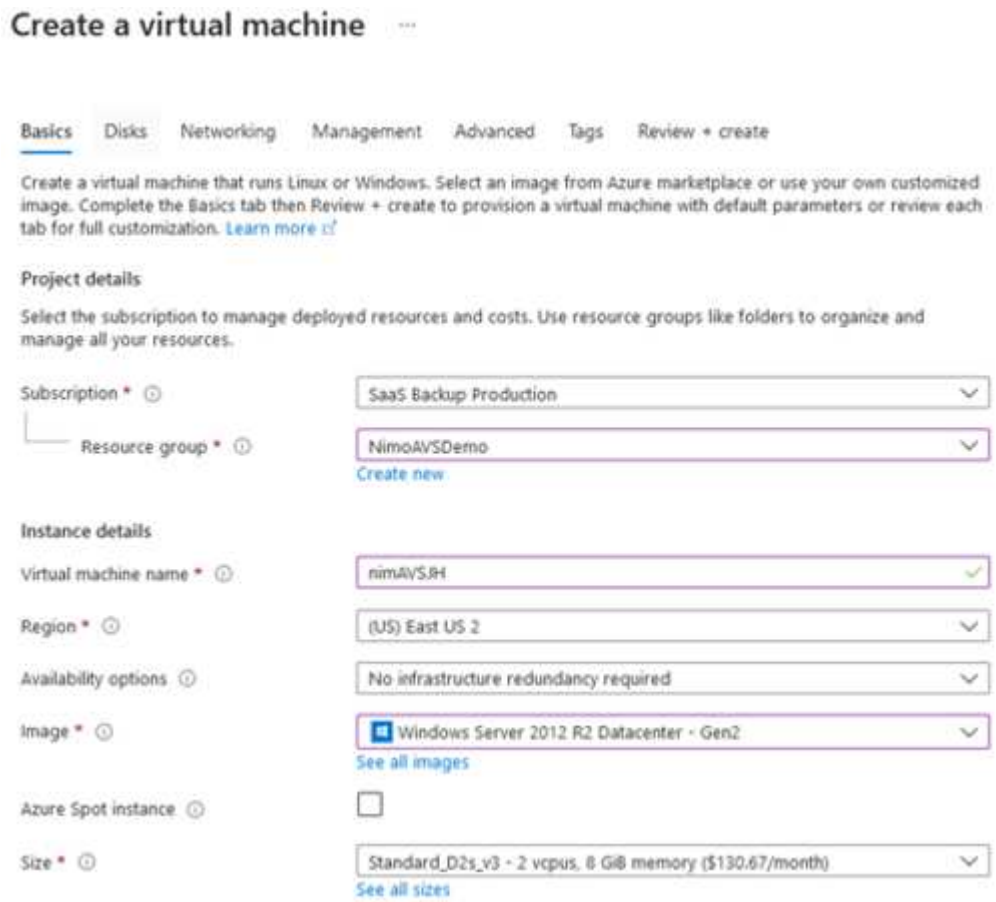


提供位址範圍和閘道子網路的vnet會建立在指定的訂閱和資源群組中。

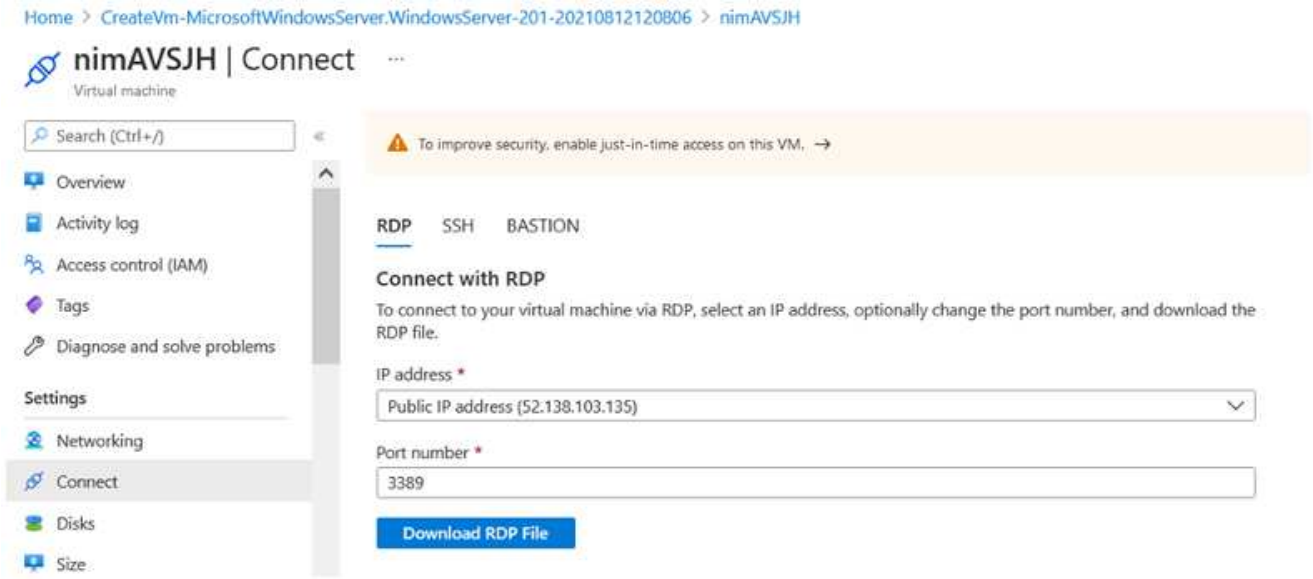
如果您手動建立vnet、請建立一個虛擬網路閘道、並以適當的SKU和ExpressRoute做為閘道類型。部署完成後、請使用授權金鑰、將ExpressRoute連線連接至內含Azure VMware Solution私有雲的虛擬網路閘道。如需詳細資訊、請參閱 "在Azure中設定VMware私有雲端的網路功能"。

驗證網路連線及存取**Azure VMware**解決方案私有雲的能力

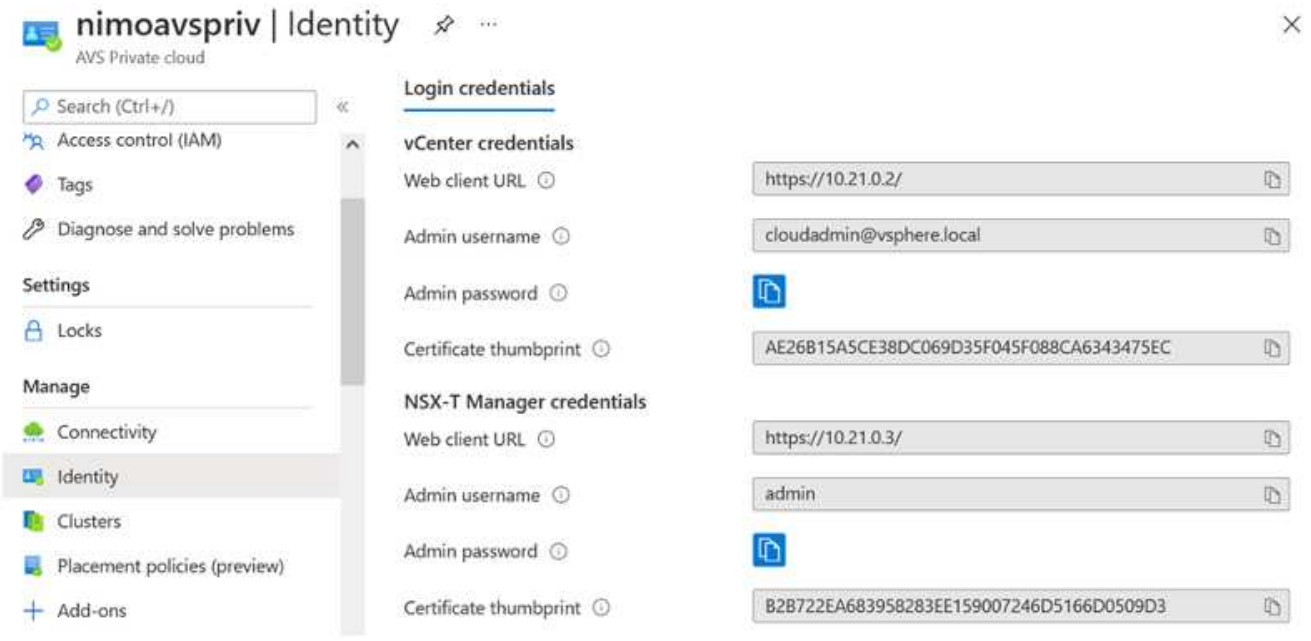
Azure VMware解決方案不允許您使用內部部署的VMware vCenter來管理私有雲。而是需要跨接主機才能連線至Azure VMware Solution vCenter執行個體。在指定的資源群組中建立跳接主機、然後登入Azure VMware Solution vCenter。這台跨接主機應該是在為連線所建立的同一個虛擬網路上的Windows VM、並應提供vCenter和NSX Manager的存取權。



虛擬機器佈建完成後、請使用「Connect（連線）」選項來存取RDP。

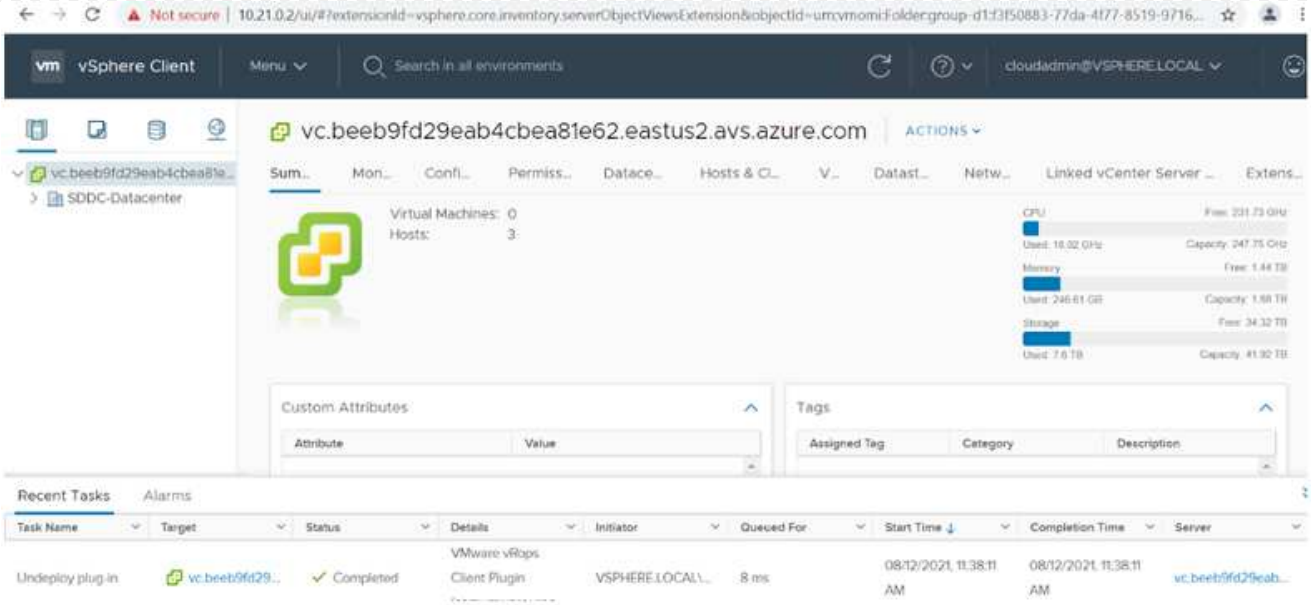


使用Cloud admin使用者、從這個新建立的跨接主機虛擬機器登入vCenter。若要存取認證資料、請前往Azure入口網站並瀏覽至Identity（位於私有雲端的「Manage（管理）」選項下）。您可以從這裡複製私有雲端vCenter和NSX T Manager的URL和使用者認證資料。



在Windows虛擬機器中、開啟瀏覽器並瀏覽至vCenter Web用戶端URL 並使用管理使用者名稱* cloudadmin@vple.1l*、然後貼上複製的密碼。同樣地、您也可以使用Web用戶端URL來存取NSxT-T Manager 並使用管理使用者名稱貼上複製的密碼、以建立新區段或修改現有的層級閘道。

每個已配置SDDC的Web用戶端URL各不相同。



Azure VMware解決方案SDDC現在已完成部署與設定。善用ExpressRoute Global Reach、將內部部署環境連接至Azure VMware解決方案私有雲。如需詳細資訊、請參閱 "Azure VMware解決方案的對等內部部署環境"。

在**Google Cloud Platform**（**GCP**）上部署及設定虛擬化環境

如同內部部署、規劃Google Cloud VMware Engine（GCVM）對於成功建立虛擬機器和移轉的正式作業就緒環境而言、是非常重要的。

本節說明如何設定及管理GCVE,並搭配可用的選項來連接NetApp儲存設備。

設定程序可分為下列步驟：

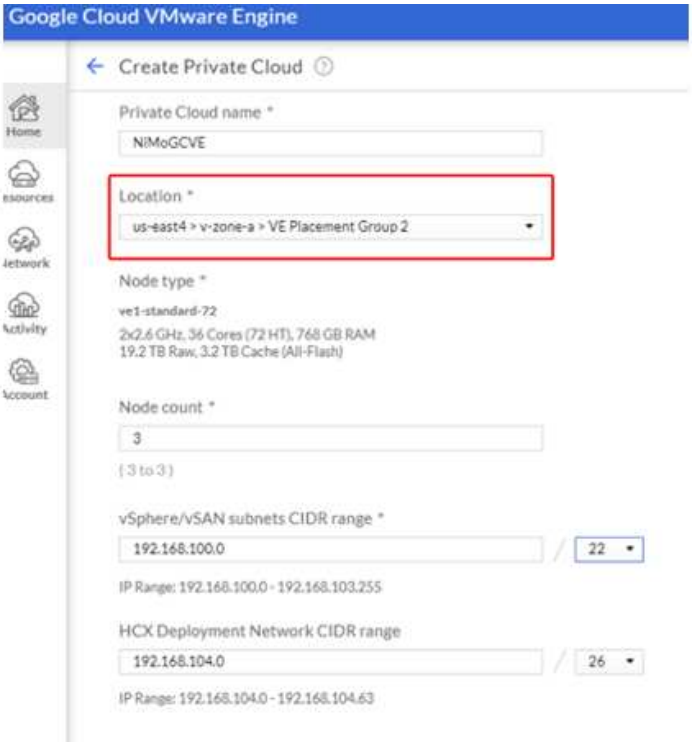
部署及設定**GCVE**

若要在GCP上設定GCVE環境、請登入GCP主控台、然後存取VMware Engine入口網站。

按一下「New Private Cloud」（新私有雲端）按鈕、然後輸入所需的GCVM私有雲端組態。在「位置」上、請務必在部署CVS/CVO的相同地區/區域中部署私有雲端、以確保最佳效能和最低延遲。

先決條件：

- 設定VMware引擎服務管理IAM角色
- "啟用VMware Engine API存取和節點配額"
- 請確定CIDR範圍不會與任何內部部署或雲端子網路重疊。CIDR範圍必須為/27或更高。



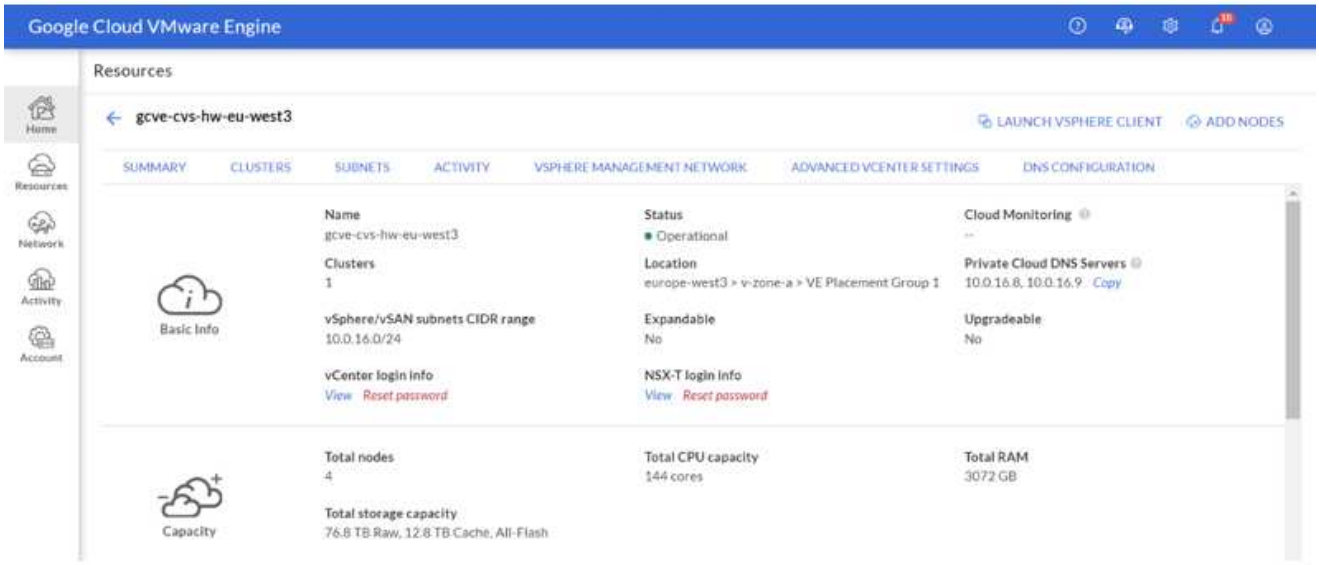
附註：建立私有雲端可能需要30分鐘到2小時的時間。

一旦私有雲端資源配置完成、請設定私有雲端存取、以實現高處理量和低延遲的資料路徑連線。

如此可確保Cloud Volumes ONTAP 執行了某些執行個體的VPC網路能夠與GCVR私有雲端通訊。若要這麼做、請遵循 "GCP文件"。對於Cloud Volume Service、請Cloud Volumes Service 在租戶主機專案之間執行一次對等、以建立VMware Engine與VMware Infrastructure之間的連線。如需詳細步驟、請遵循此步驟 "連結"。

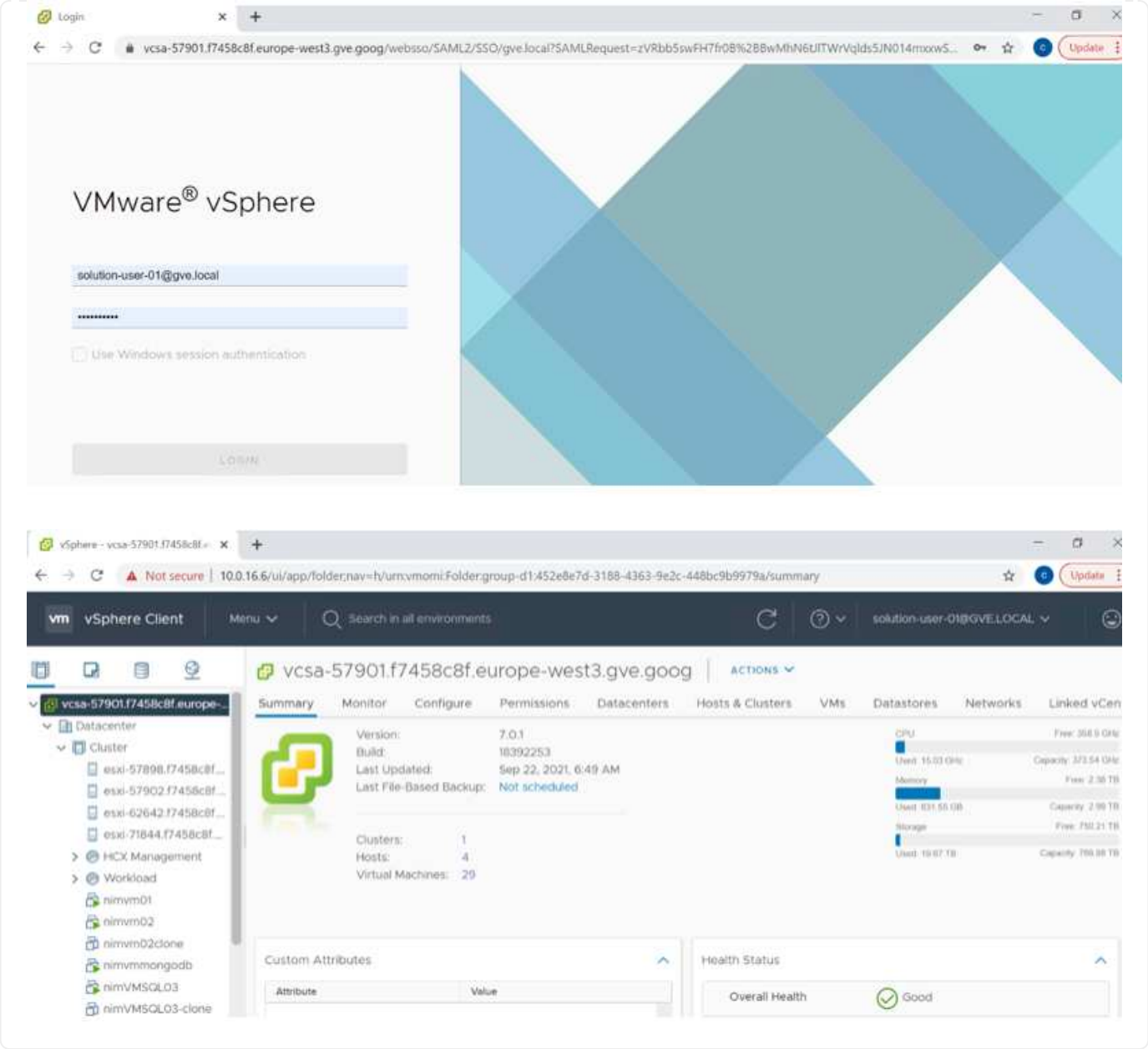
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

使用CloudOwner@gve.estil使用者登入vCenter。若要存取認證資料、請前往VMware Engine入口網站、前往資源、然後選取適當的私有雲。在基本資訊區段中、按一下vCenter登入資訊（vCenter Server、HCX Manager）或NSX-T登入資訊（NSX Manager）的檢視連結。



在Windows虛擬機器中、開啟瀏覽器並瀏覽至vCenter Web用戶端URL 並將管理使用者名稱用作CloudOwner@gve.erl、然後貼上複製的密碼。同樣地、您也可以使用Web用戶端URL來存取NSxT-T Manager 並使用管理使用者名稱貼上複製的密碼、以建立新區段或修改現有的層級閘道。

若要從內部部署網路連線至VMware Engine私有雲、請善用雲端VPN或雲端互連來進行適當的連線、並確保所需的連接埠是開放的。如需詳細步驟、請遵循此步驟 "連結"。



將 **NetApp Cloud Volume Service** 補充資料存放區部署至 **GCVE**

請參閱 "使用 NetApp CVS 將補充 NFS 資料存放區部署至 GCVE 的程序"

適用於公有雲供應商的**NetApp**儲存選項

在三大大型超大規模擴充系統中探索NetApp儲存設備的選項。

AWS / VMC

AWS支援下列組態的NetApp儲存設備：

- FSX ONTAP 支援以客為本的連線儲存設備
- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- FSX ONTAP 不只是NFS的補充資料存放區

檢視詳細資訊 "VMC的來賓連線儲存選項"。檢視詳細資訊 "VMC的補充NFS資料存放區選項"。

Azure / AVS

Azure以下列組態支援NetApp儲存設備：

- 以客體連線儲存設備的形式提供Azure NetApp Files
- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- 作爲NFS補充資料存放區的能力（ANF Azure NetApp Files ）

檢視詳細資訊 "AVS的來賓連線儲存選項"。檢視詳細資訊 "AVS的補充NFS資料存放區選項"。

GCP / GCV

Google Cloud支援下列組態的NetApp儲存設備：

- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- 以客體連線儲存設備的形式提供資訊（CVS）Cloud Volumes Service
- 作爲NFS補充資料存放區的CVS Cloud Volumes Service

檢視詳細資訊 "GCVE的來賓連線儲存選項"。

深入瞭解 "NetApp Cloud Volumes Service 支援Google Cloud VMware Engine的資料儲存區（NetApp部落格）" 或 "如何使用NetApp CVS做為Google Cloud VMware Engine的資料存放區（Google部落格）"

TR-4938：在**ONTAP AWS**上安裝**VMware Cloud**、將**Amazon FSX for VMware**當作**NFS**資料存放區

NetApp公司Niyazz Mohamed

簡介

每個成功的組織都走上轉型與現代化的道路。在這項流程中、公司通常會利用現有的VMware投資來充分發揮雲端效益、並探索如何移轉、突發、擴充及提供災難恢復功能、使流程盡可能順暢無礙。移轉至雲端的客戶必須評估使用案例的彈性與爆發、資料中心結束、資料中心整合、生命週期結束案例、合併、 併購等。

雖然AWS上的VMware Cloud是大多數客戶偏好的選擇、因為它能為客戶提供獨特的混合式功能、但有限的原生儲存選項限制了它對於具有大量儲存工作負載的組織的效用。由於儲存設備直接與主機相連、因此擴充儲存設備的唯一方法是新增更多主機、如此一來、儲存密集工作負載的成本就會增加35%至40%以上。這些工作負載需要額外的儲存設備和隔離效能、而非額外的馬力、但這表示需要支付額外的主機費用。這就是 "最近整合" 使用ONTAP VMware Cloud on AWS、即可輕鬆處理儲存與效能密集的工作負載。

讓我們來思考下列案例：客戶需要八部主機來處理馬力（vcpU/vMem）、但他們也需要大量的儲存設備。根據

評估結果、他們需要16台主機來滿足儲存需求。如此一來、整體TCO就會增加、因為他們必須在真正需要更多儲存設備的情況下、購買所有額外的馬力。這適用於任何使用案例、包括移轉、災難恢復、突發、開發/測試、等等。

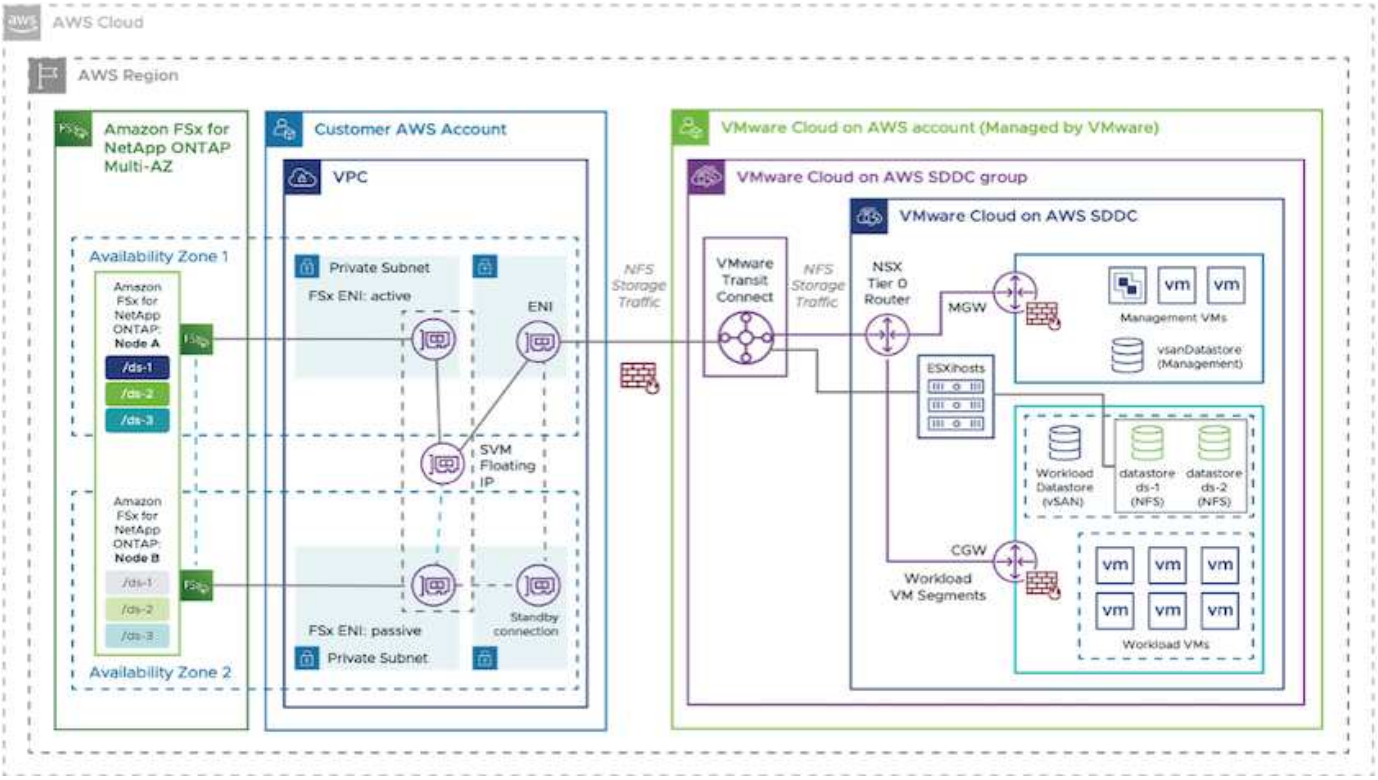
本文件將引導您完成在ONTAP AWS上配置和附加FSXfor VMware做為VMware Cloud的NFS資料存放區所需的步驟。

此解決方案也可從VMware取得。請造訪 "VMware Cloud技術區" 以取得更多資訊。

連線選項

AWS上的VMware Cloud可同時支援針對ONTAP VMware的多AZ和單一AZ部署FSX。

本節說明高層連線架構、以及實作解決方案以擴充SDDC叢集儲存設備所需的步驟、而不需要新增其他主機。



高階部署步驟如下：

1. 在ONTAP 新指定的VPC中建立Amazon FSX以供支援。
2. 建立SDDC群組。
3. 建立VMware Transit Connect和TGW附件。
4. 設定路由（AWS VPC和SDDC）和安全群組。
5. 將NFS磁碟區作為資料存放區附加至SDDC叢集。

在您配置及附加FSXfor ONTAP VMware做為NFS資料存放區之前、您必須先在Cloud SDDC環境上設定VMware、或是將現有SDDC升級至v1.20或更新版本。如需詳細資訊、請參閱 "開始使用AWS上的VMware Cloud"。

目前、延伸叢集不支援FSX ONTAP for Sfor Sf2。

結論

本文件說明在ONTAP AWS上設定Amazon FSX for VMware Cloud搭配VMware Cloud的必要步驟。Amazon FSX ONTAP for Sfor Sfor Sfor Sfor功能提供絕佳的選項、可部署及管理應用程式工作負載及檔案服務、同時將資料需求無縫地移至應用程式層、進而降低TCO。無論使用案例為何、請選擇AWS上的VMware Cloud搭配Amazon FSX ONTAP for VMware for VMware、以快速實現雲端效益、一致的基礎架構、以及從內部部署到AWS的作業、工作負載的雙向可攜性、以及企業級容量與效能。這是用來連接儲存設備的熟悉程序和程序。請記住、這只是資料的變更位置、加上新名稱；工具和程序都維持不變、Amazon FSX for ONTAP VMware有助於最佳化整體部署。

若要深入瞭解此程序、歡迎觀看詳細的逐步解說影片。

Amazon FSX for ONTAP VMware Cloud

適用於**AWS**的**NetApp**來賓連線儲存選項

AWS支援以原生FSX服務（FSX0 ONTAP ）或Cloud Volumes ONTAP 透過Sfor（CVO）連接來賓的NetApp儲存設備。

FSX ONTAP

Amazon FSX for NetApp ONTAP Sfing是一項完全託管的服務、以NetApp廣受歡迎ONTAP 的Sfing檔案系統為基礎、提供高度可靠、可擴充、高效能且功能豐富的檔案儲存設備。FSX for ONTAP VMware將NetApp檔案系統熟悉的功能、效能、功能和API作業、以及完全託管的AWS服務的敏捷度、擴充性和簡易性結合在一起。

FSX for ONTAP FSfor支援功能豐富、快速且靈活的共享檔案儲存設備、可從在AWS或內部部署環境中執行的Linux、Windows及MacOS運算執行個體進行廣泛存取。FSX for ONTAP VMware提供高效能固態硬碟（SSD）儲存設備、延遲低於毫秒。使用FSXfor ONTAP Sfor Sf0、您可以為工作負載達到SSD等級的效能、同時只需支付一小部分資料的SSD儲存設備費用。

只ONTAP 要按一下按鈕、就能輕鬆使用FSXfor Sfor Sfor功能來管理資料、快照、複製及複寫檔案。此外ONTAP 、FSX for Sfor Sfor Sfor Sfor Elfed會自動將您的資料分層、以降低成本、靈活儲存、減少您配置或管理容量的需求。

FSX for ONTAP Sfor Sfor支援跨區域災難恢復、提供高度可用且持久的儲存設備、並具備完整的備份管理功能。為了讓資料更容易保護和保護、FSXfor ONTAP Sfor支援熱門的資料安全和防毒應用程式。

FSX ONTAP 支援以客為本的連線儲存設備

使用**ONTAP AWS**上的**VMware Cloud**設定**Amazon FSX for NetApp**功能

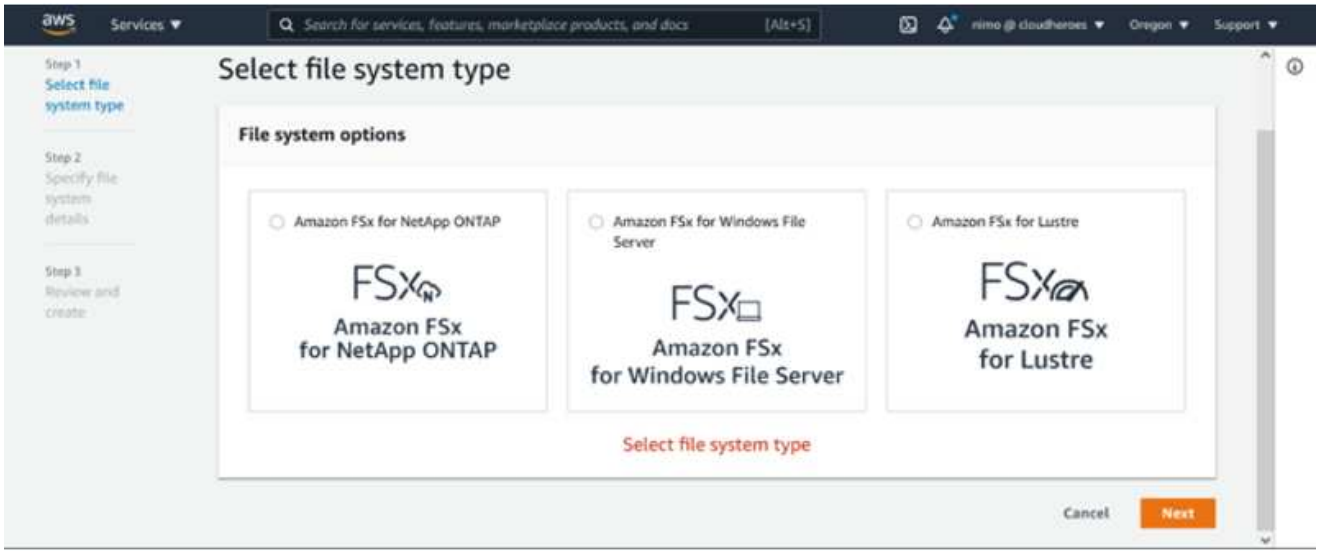
Amazon FSx for NetApp ONTAP 的支援文件共享和LUN可從在VMware Cloud AWS上的VMware SDDC環境中建立的VM掛載。這些磁碟區也可以安裝在Linux用戶端上、並使用NFS或SMB傳輸協定對應到Windows用戶端、而LUN則可在透過iSCSI掛載時、以區塊裝置的形式在Linux或Windows用戶端上存取。可ONTAP 透過下列步驟快速設定適用於NetApp的Amazon FSX。

Amazon FSX for NetApp ONTAP 的VMware解決方案和AWS上的VMware Cloud必須位於相同的可用度區域、才能達到更好的效能、並避免在可用度區域之間傳輸資料。

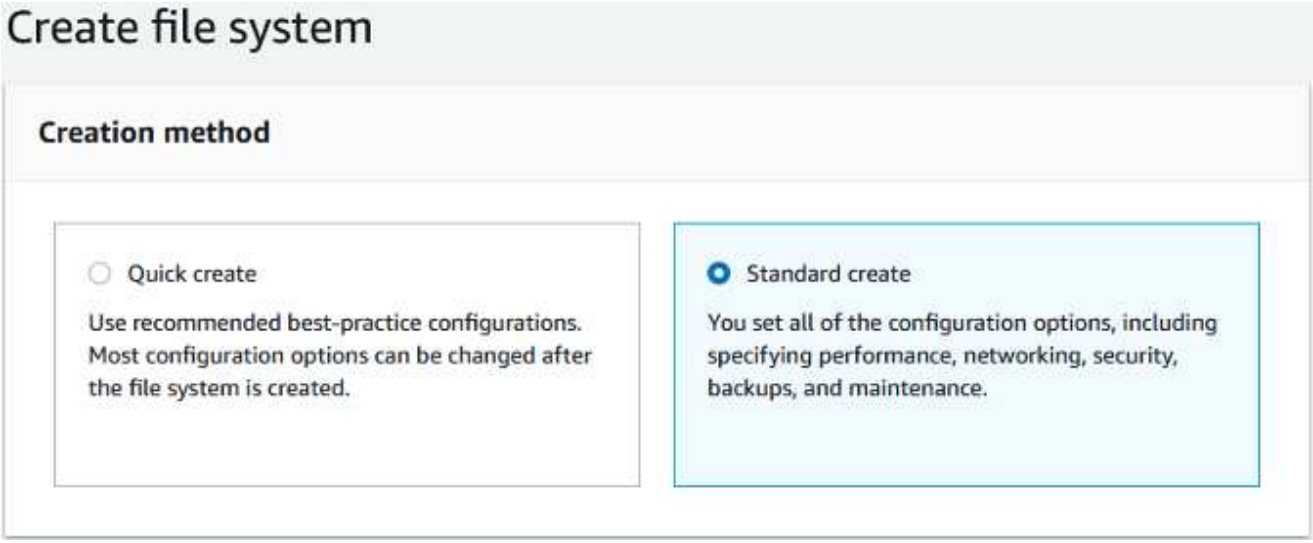
建立及掛載**Amazon FSX for ONTAP Sf6 Volume**

若要建立及掛載適用於NetApp ONTAP 的Amazon FSX for NetApp Sfor the File System、請完成下列步驟：

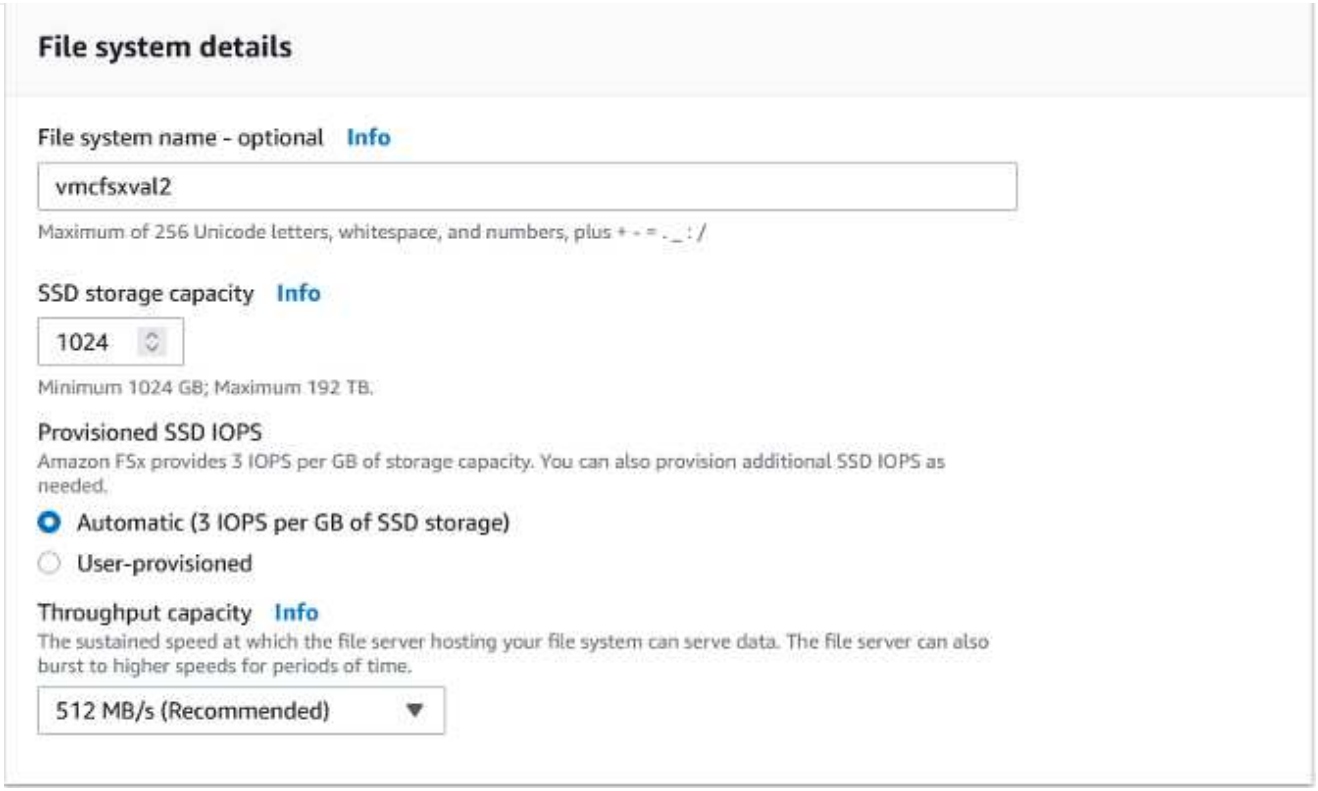
1. 開啟 "Amazon FSX主控台" 然後選擇Create file system（建立檔案系統）以啟動檔案系統建立精靈。
2. 在「Select File System Type」（選取檔案系統類型）頁面上、選擇Amazon FSX for NetApp ONTAP解決方案、然後選擇「Next」（下一步）。此時將顯示Create File System（創建文件系統）頁面。



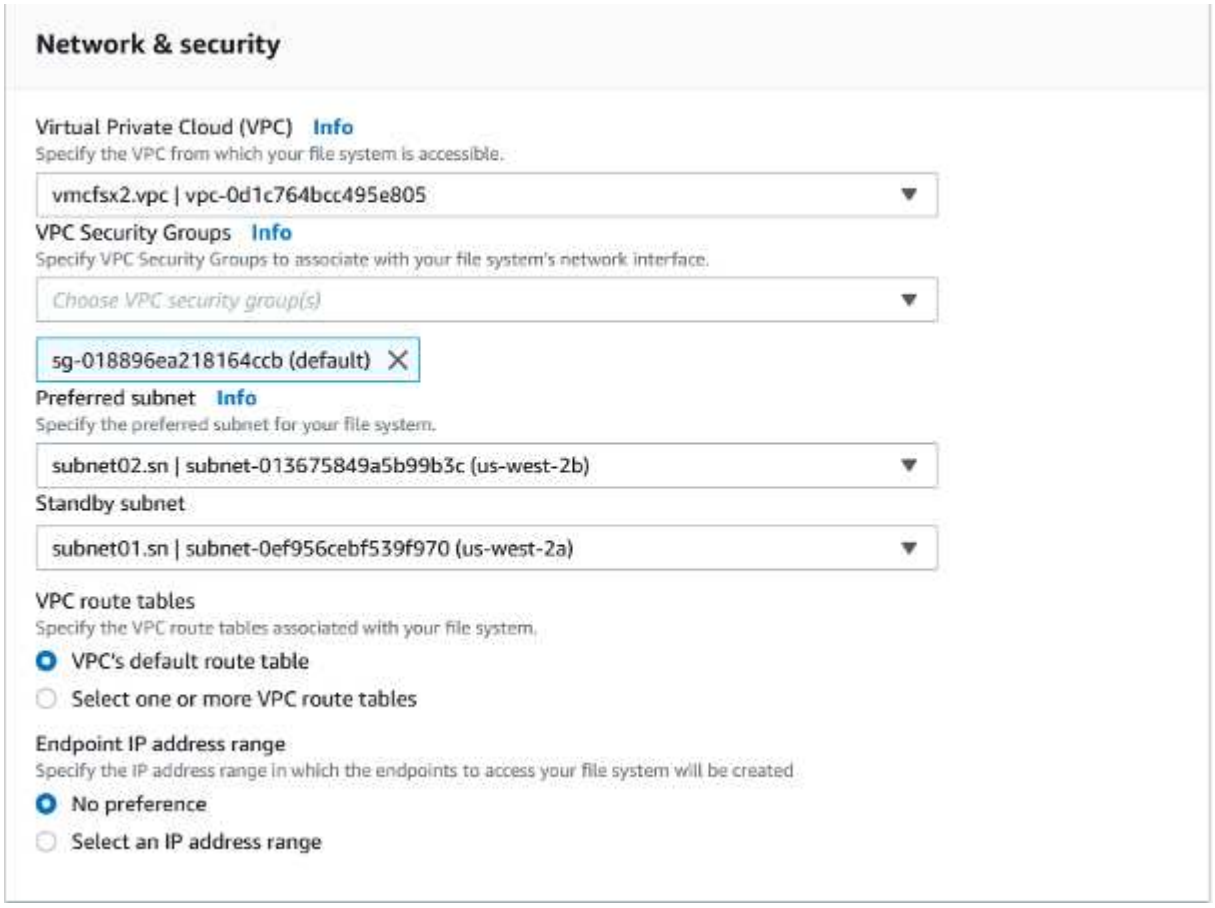
1. 在「Networking（網路）」區段中、針對Virtual Private Cloud（VPC）選擇適當的VPC和偏好的子網路、以及路由表。在此情況下、會從下拉式清單中選取vmcfsx2.VPC。



1. 對於建立方法、請選擇「標準建立」。您也可以選擇「快速建立」、但本文件使用「標準建立」選項。

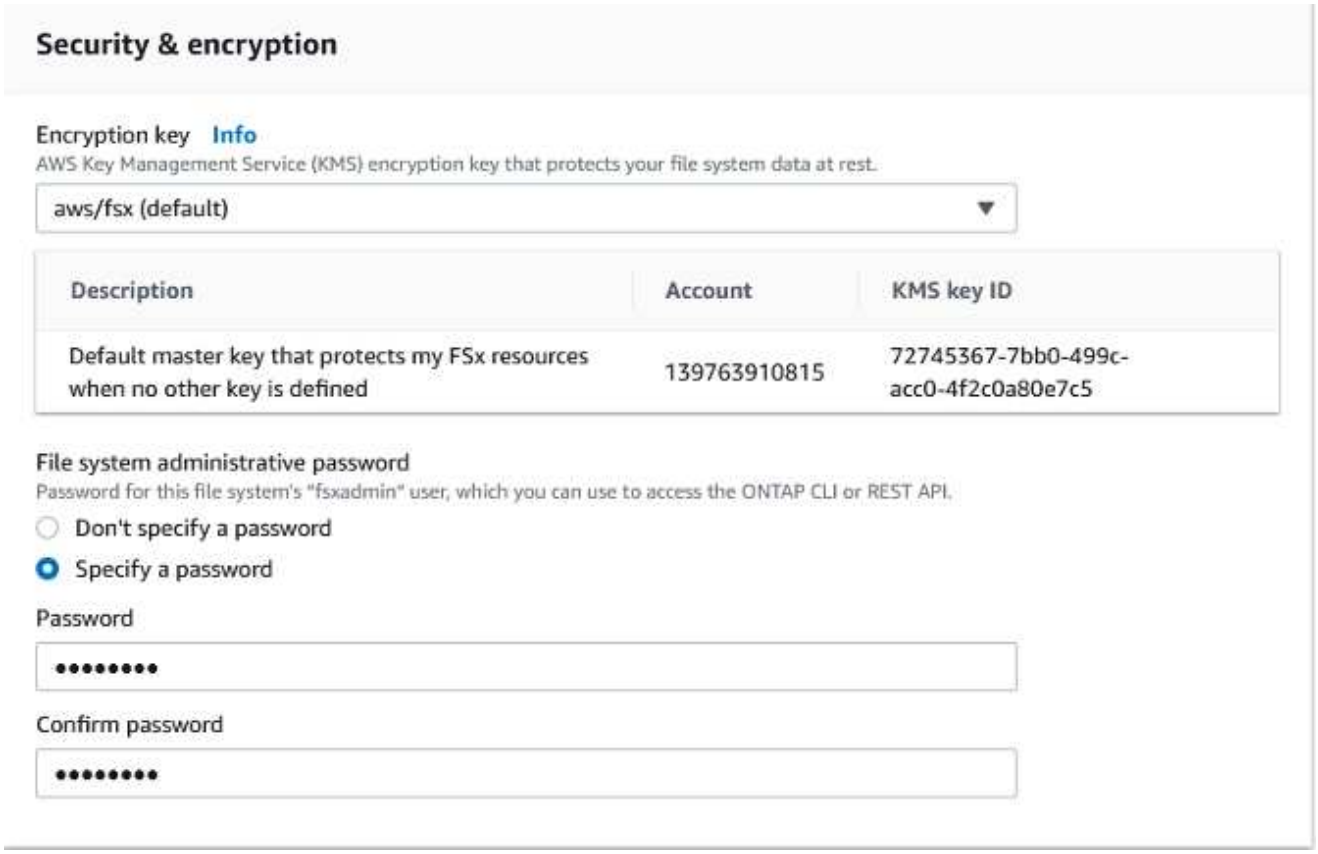


1. 在「Networking（網路）」區段中、針對Virtual Private Cloud（VPC）選擇適當的VPC和偏好的子網路、以及路由表。在此情況下、會從下拉式清單中選取vmcfsx2.VPC。

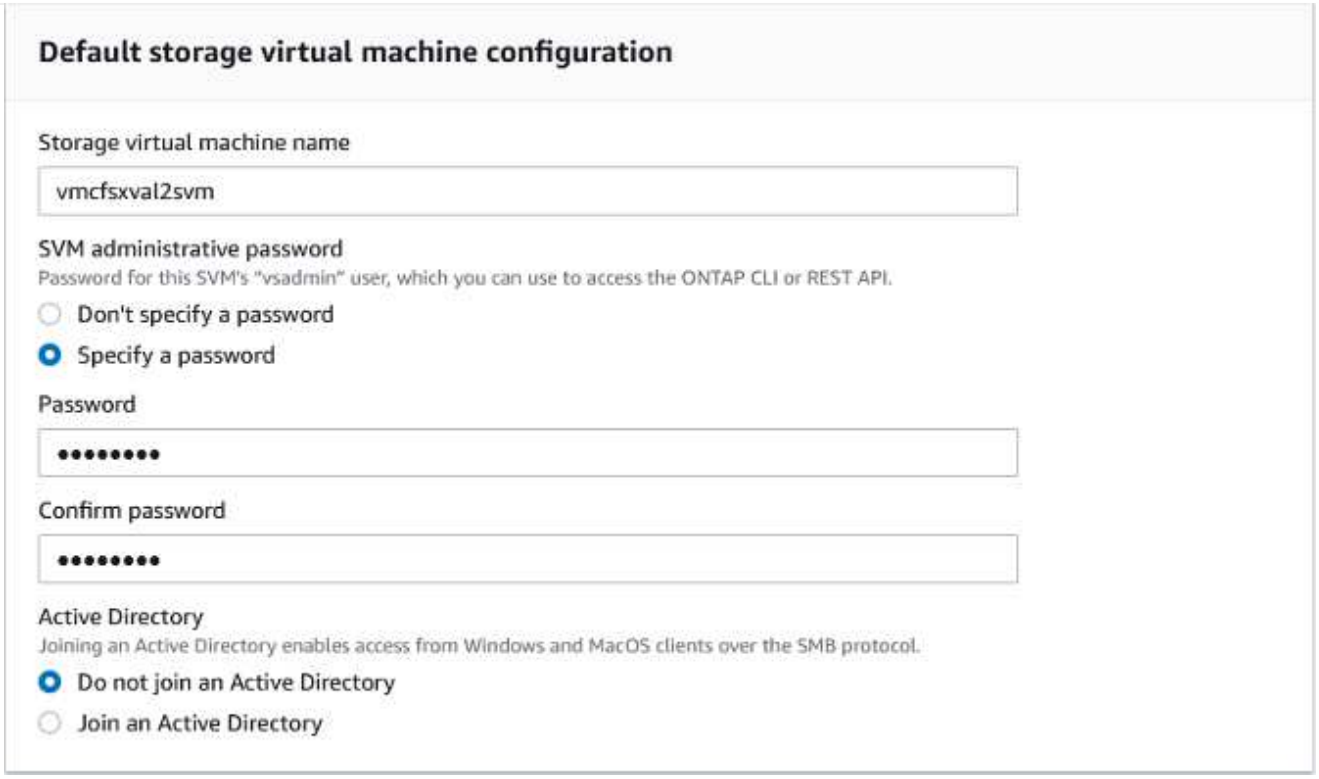


在「Networking（網路）」區段中、針對Virtual Private Cloud（VPC）選擇適當的VPC和偏好的子網路、以及路由表。在此情況下、會從下拉式清單中選取vmcfsx2.VPC。

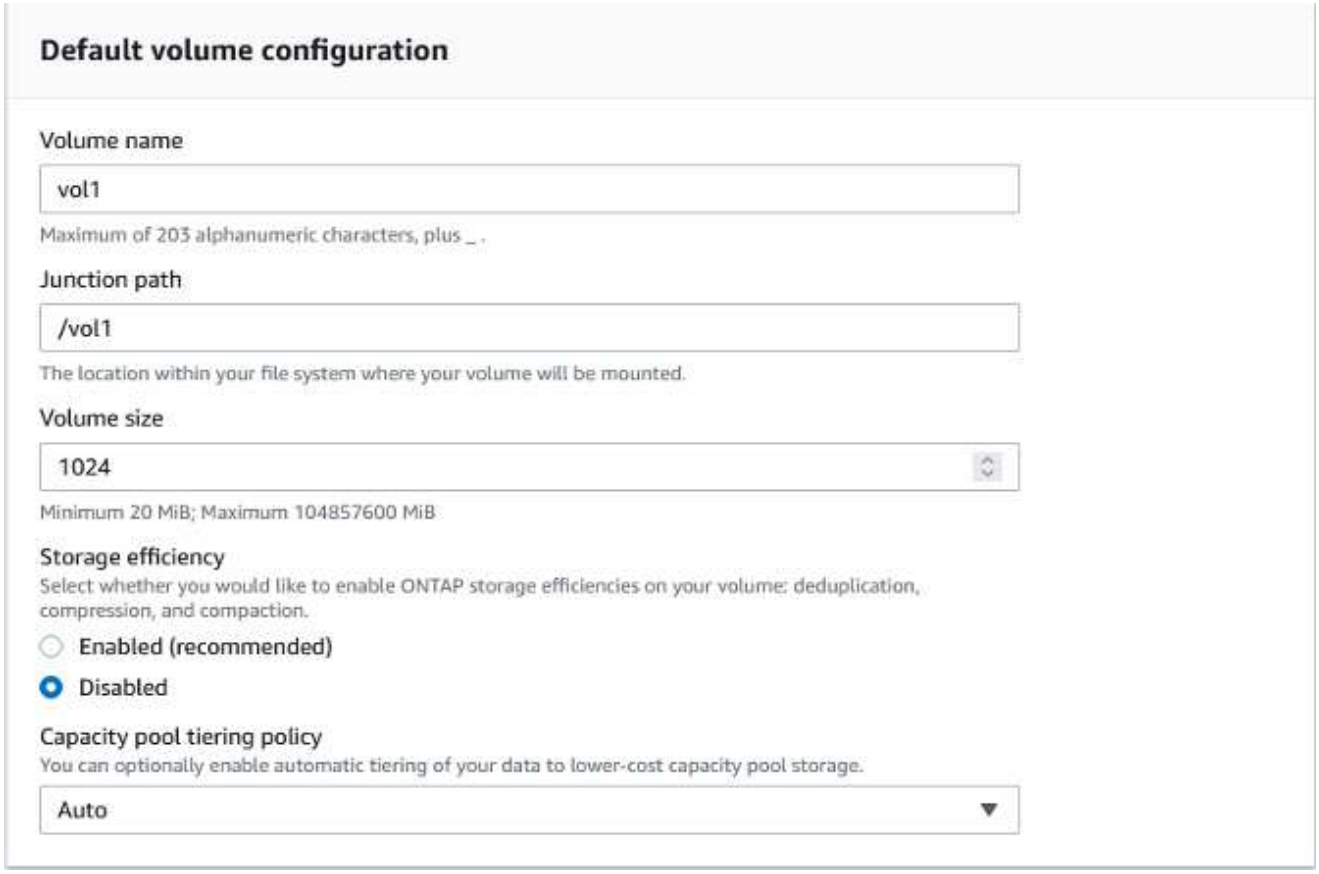
1. 在「安全性與加密」區段中、針對加密金鑰選擇AWS金鑰管理服務（AWS KMS）加密金鑰、以保護檔案系統閒置的資料。在「檔案系統管理密碼」中、輸入fsxadmin使用者的安全密碼。



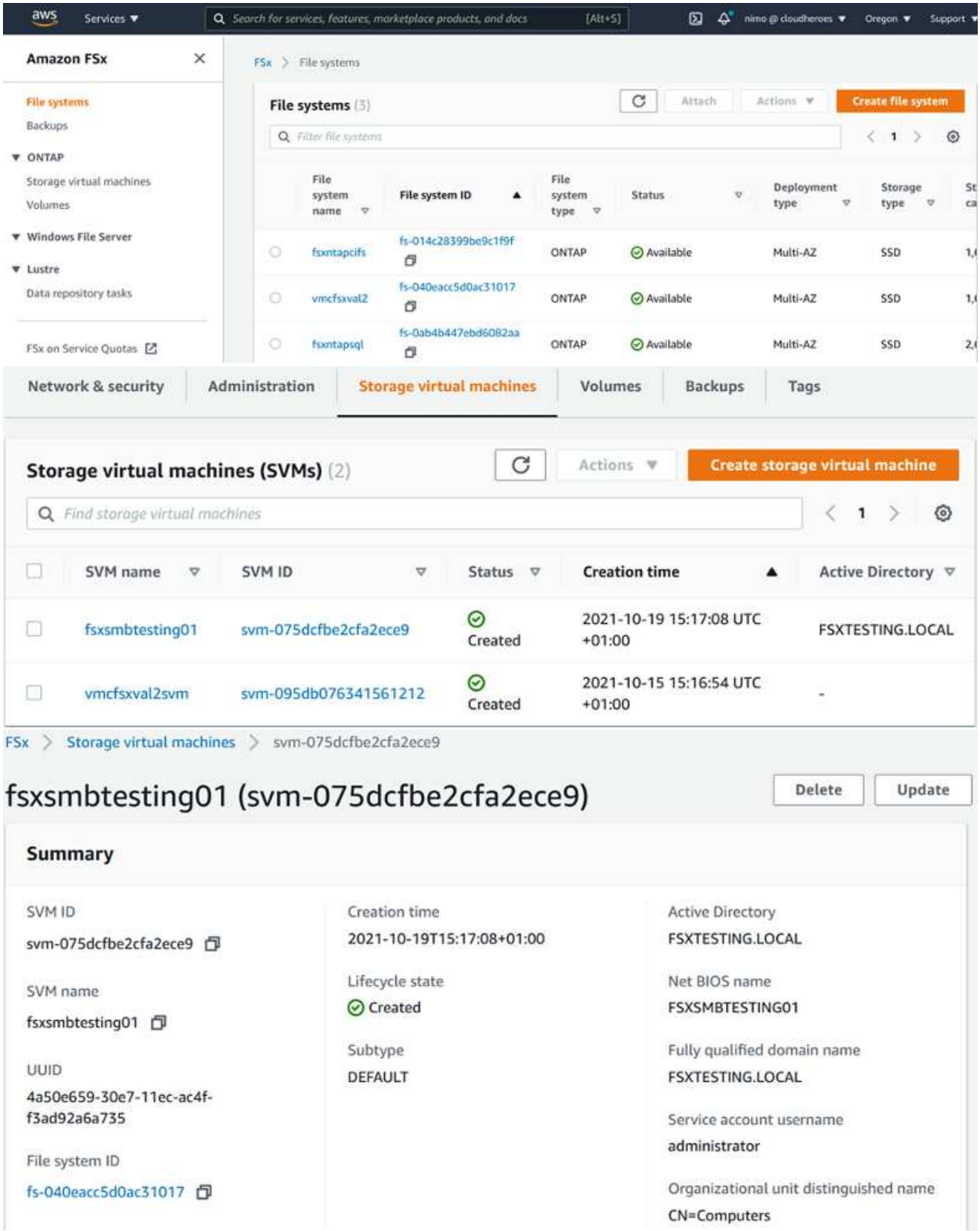
1. 在虛ONTAP 擬機器中、指定與vsadmin搭配使用的密碼、以便使用REST API或CLI來管理功能。如果未指定密碼、則可使用fsxadmin使用者來管理SVM。在Active Directory區段中、請務必將Active Directory加入SVM、以進行SMB共用資源的資源配置。在「預設儲存虛擬機器組態」區段中、提供此驗證中儲存設備的名稱、即使用自我管理的Active Directory網域來配置SMB共用。



1. 在「預設Volume組態」區段中、指定Volume名稱和大小。這是NFS Volume。若要提升儲存效率、請選擇「啟用」以開啟ONTAP 「不支援的儲存效率」功能（壓縮、重複資料刪除和壓縮）、或選擇「停用」以關閉這些功能。



1. 檢閱「Create File System（建立檔案系統）」頁面上顯示的檔案系統組態。
2. 按一下建立檔案系統。

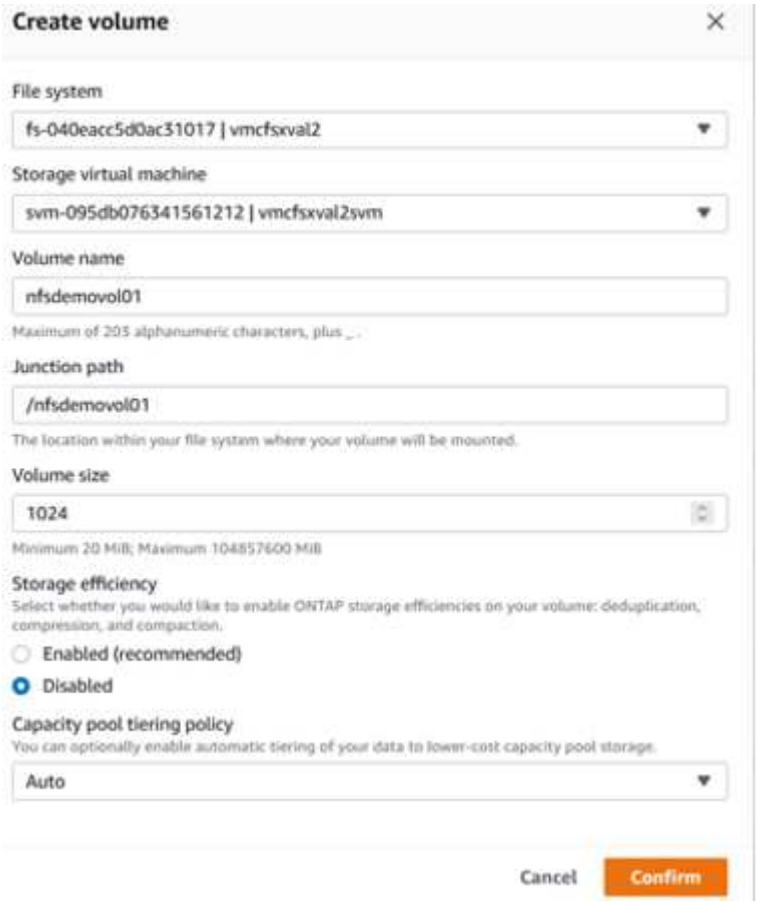


如需詳細資訊、請參閱 "Amazon FSX for NetApp ONTAP 功能入門"。

依照上述方式建立檔案系統之後、請使用所需的大小和傳輸協定來建立磁碟區。

1. 開啟 "Amazon FSX主控台"。
2. 在左側導覽窗格中、選擇「檔案系統」、然後選擇ONTAP 您要建立Volume的作業系統。
3. 選取Volume（磁碟區）索引標籤。
4. 選取「Create Volume（建立Volume）」索引標籤。
5. 此時將出現Create Volume（創建Volume）對話框。

為了進行示範、本節會建立NFS磁碟區、以便輕鬆掛載於AWS上VMware雲端上執行的VM。nfsdemov01的建立方式如下所示：



在**ONTAP Linux**用戶端上掛載**FSX***

以掛載ONTAP 上一步建立的FSXSf問題Volume。在AWS SDDC上VMC內的Linux VM中、完成下列步驟：

1. 連線至指定的Linux執行個體。
2. 使用Secure Shell（SSH）在執行個體上開啟終端機、然後以適當的認證登入。
3. 使用下列命令建立磁碟區掛載點的目錄：

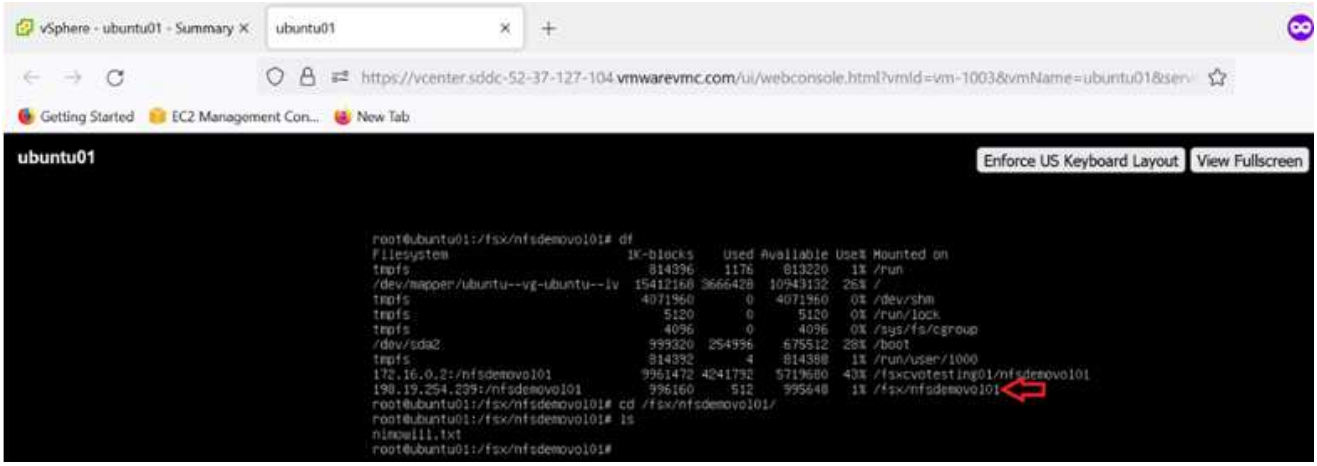
```
 $ sudo mkdir /fsx/nfsdemovol01
```

. 將Amazon FSX for NetApp ONTAP SfNFS Volume掛載到上一步建立的目錄。

```
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、請執行df命令來驗證掛載。

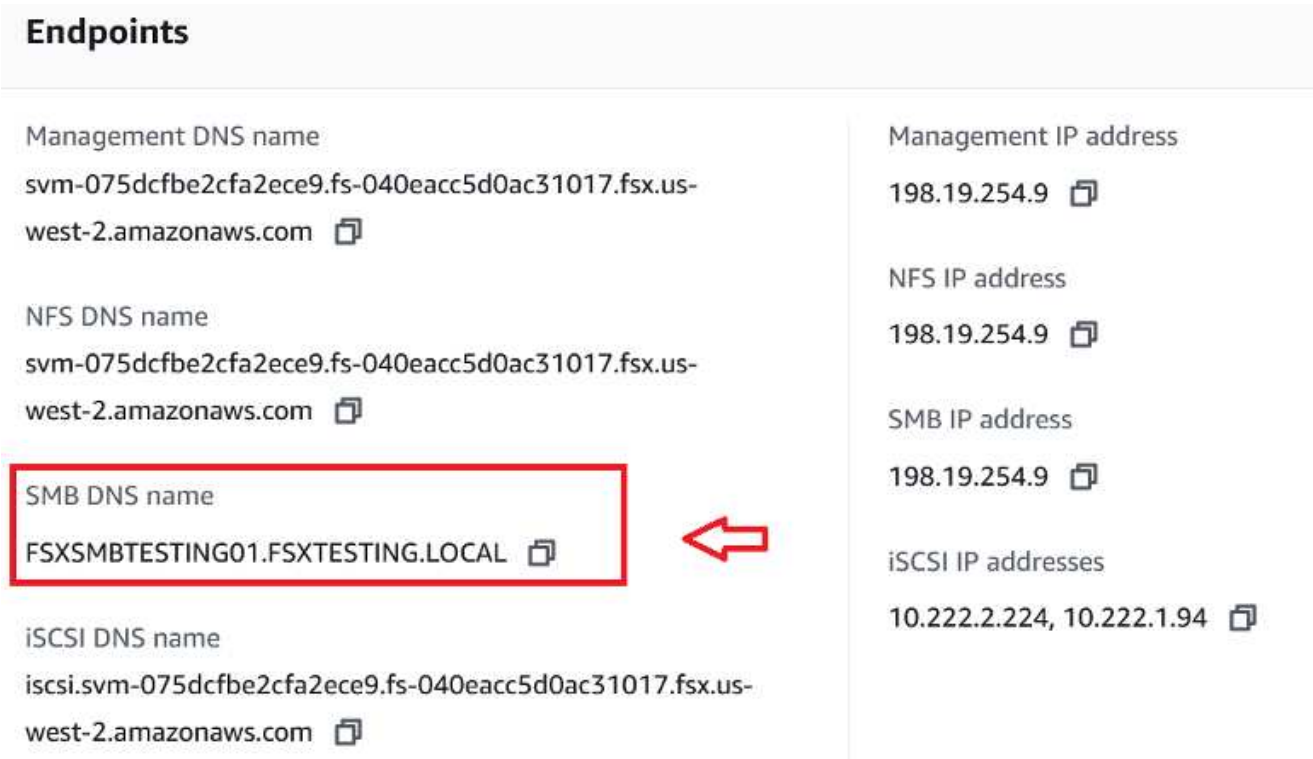


在ONTAP Linux用戶端上掛載FSX*

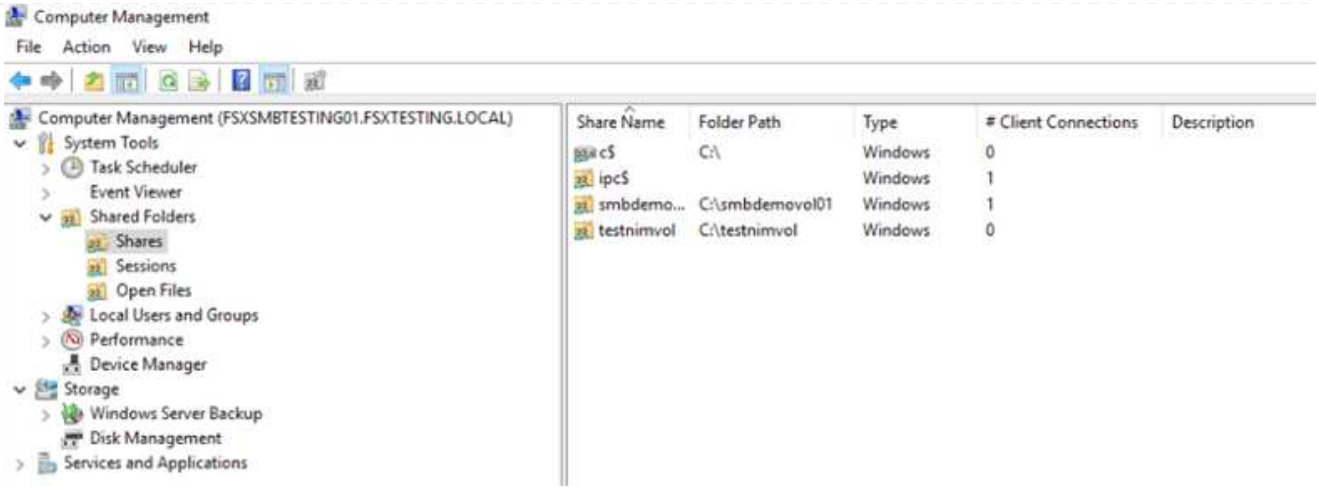
若要管理及對應Amazon FSX檔案系統上的檔案共用、必須使用共用資料夾GUI。

1. 開啟「開始」功能表、然後使用「以系統管理員身分執行」執行fsmgmt・msc。這樣做會開啟「共用資料夾GUI」工具。
2. 按一下「行動」>「所有工作」、然後選擇「連線至其他電腦」。
3. 對於另一台電腦、請輸入儲存虛擬機器（SVM）的DNS名稱。例如、本範例使用FSXSMBTESTIN01.FSXTESTIN.local。

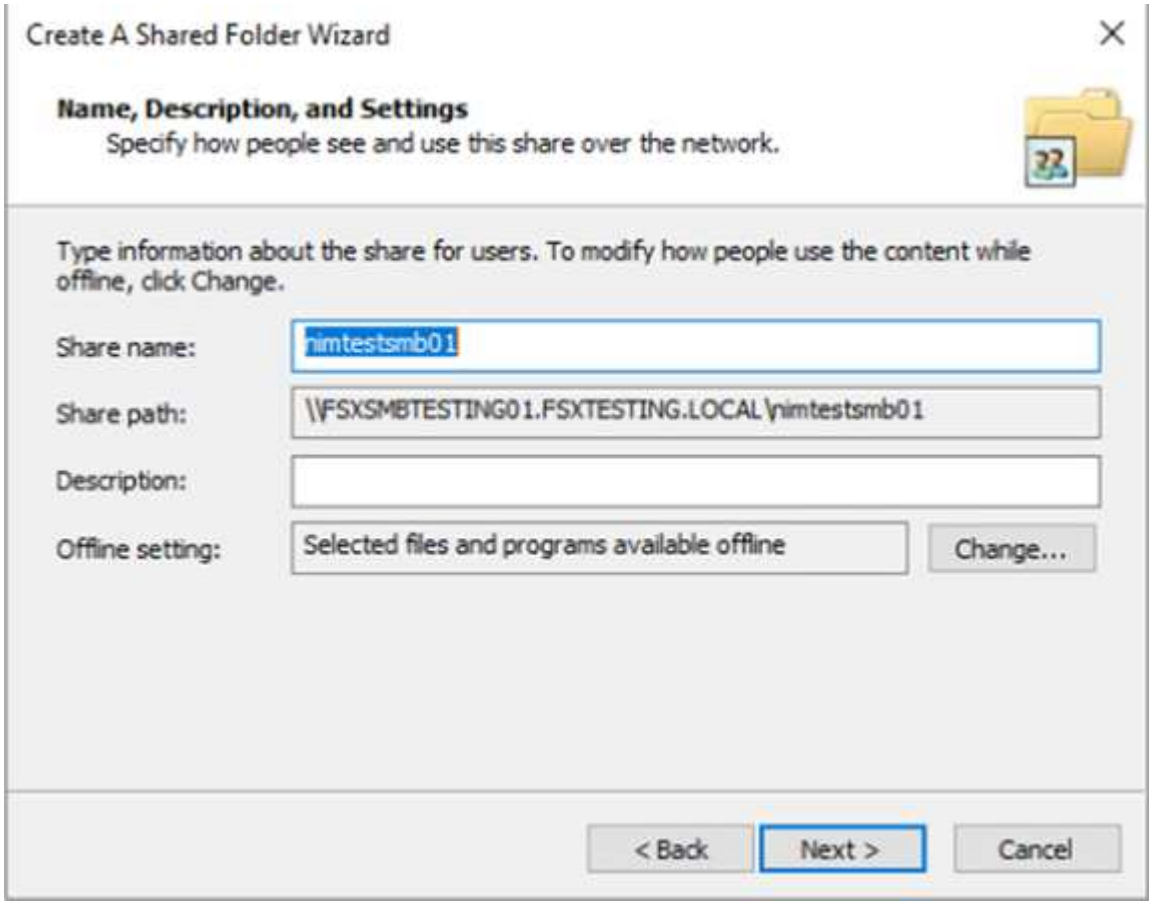
若要在Amazon FSX主控台找到SVM的DNS名稱、請選擇「儲存虛擬機器」、選擇「SVM」、然後向下捲動至「端點」以尋找SMB DNS名稱。按一下「確定」。Amazon FSX檔案系統會出現在共用資料夾的清單中。



1. 在「共享資料夾」工具中、選擇左窗格中的「共享」、即可查看Amazon FSX檔案系統的作用中共用。

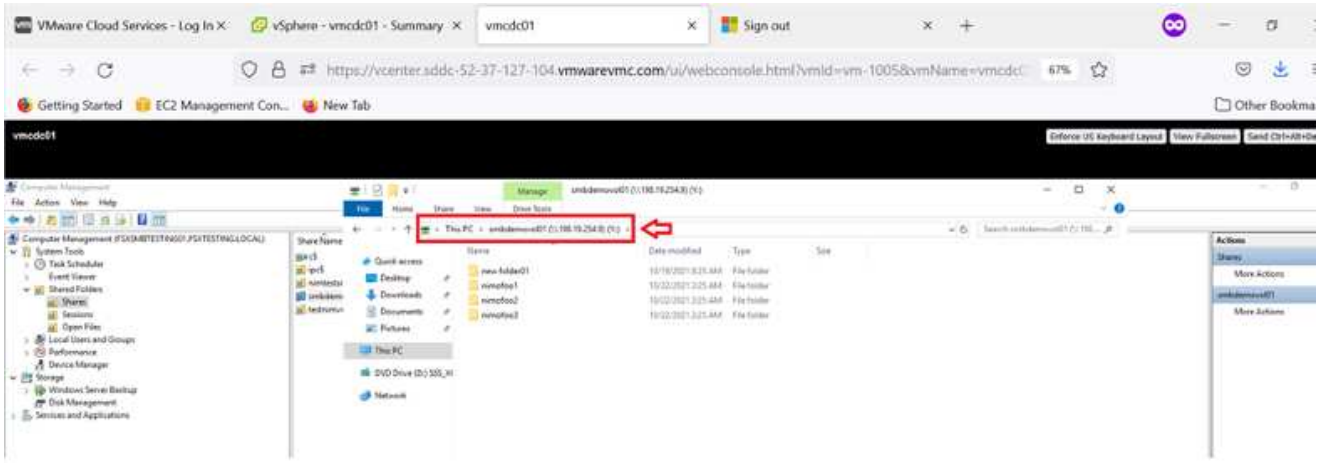


1. 現在請選擇新的共用區、然後完成「建立共用資料夾」精靈。



若要深入瞭解如何在Amazon FSX檔案系統上建立及管理SMB共用區、請參閱 "建立SMB共用"。

1. 連線到位後、即可附加SMB共用區並用於應用程式資料。若要完成此作業、請複製共用路徑、然後使用「對應網路磁碟機」選項、將磁碟區掛載到AWS SDDC上VMware Cloud上執行的VM上。



使用ONTAP iSCSI將FSX for NetApp的LUN連接至主機

FSX的iSCSI流量會透過上一節所提供的路由、通過VMware Transit Connect/AWS Transit Gateway傳輸。若要在Amazon FSX for NetApp ONTAP 支援中設定LUN、請遵循所找到的文件 "請按這裡"。

在Linux用戶端上、請確定iSCSI精靈正在執行。配置LUN後、請參閱有關使用Ubuntu進行iSCSI組態的詳細指南（範例）。 "請按這裡"。

本文將說明如何將iSCSI LUN連接至Windows主機：

在**FSX**中配置**LUN**以供**NetApp ONTAP** 使用：

1. 使用ONTAP FSX的管理連接埠存取NetApp Sfor ONTAP the Sfor the Sfof the文件系統。
2. 依照規模調整輸出所示、以所需大小建立LUN。

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

在此範例中、我們建立的LUN大小為5g（5368709120）。

1. 建立必要的igroup來控制哪些主機可以存取特定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
```

顯示兩個項目。

1. 使用下列命令將LUN對應至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
```

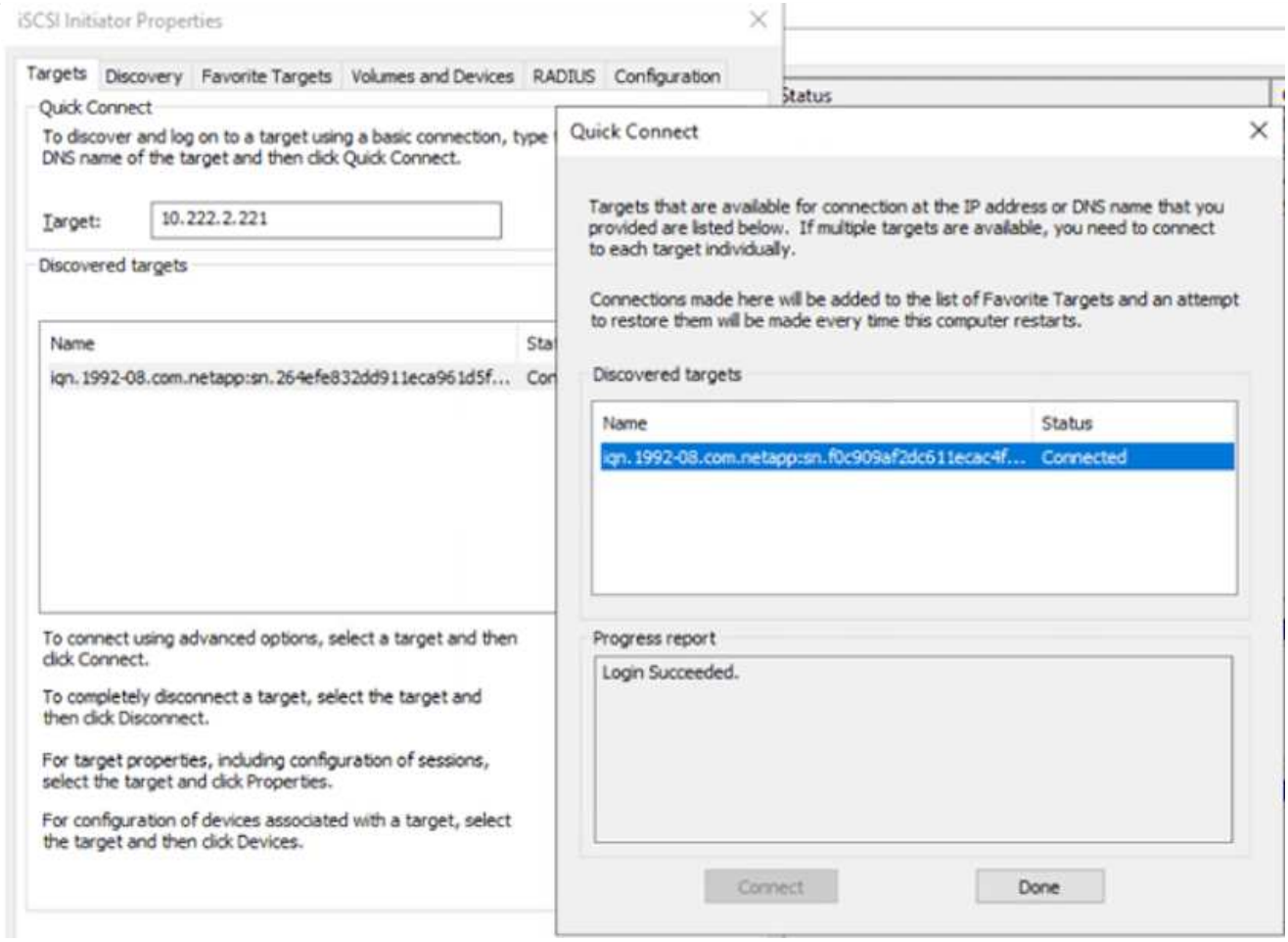
顯示兩個項目。

1. 將新配置的LUN連接至Windows VM：

若要在AWS SDDC上連接位於VMware雲端上的Windows主機、請完成下列步驟：

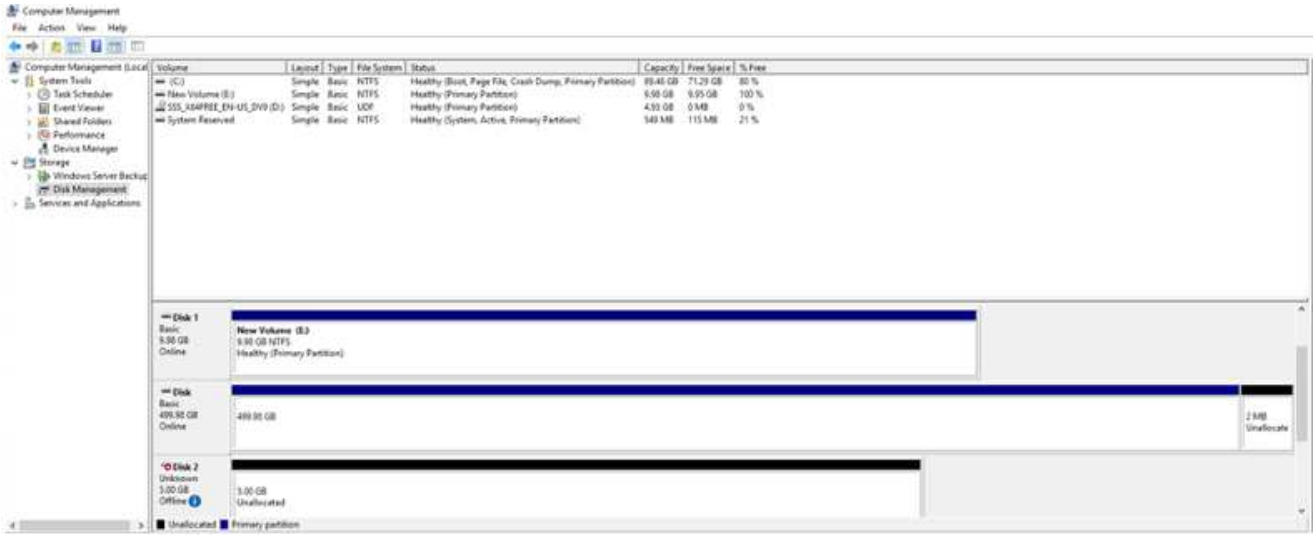
1. 將RDP移至AWS SDDC上VMware Cloud上的Windows VM。
2. 瀏覽至「伺服器管理員」>「儀表板」>「工具」>「iSCSI啟動器」、以開啟「iSCSI啟動器內容」對話方塊。
3. 在「Discovery（探索）」索引標籤中、按一下「Discover Portal（探索入口網站）」或「Add Portal（新增入口網站）」、然後輸入iSCSI目標連接埠的IP位
4. 從「目標」索引標籤中選取探索到的目標、然後按一下「登入」或「連線」。
5. 選取「啟用多重路徑」、然後選取「電腦啟動時自動還原此連線」或「將此連線新增至最愛目標清單」。按一下進階。

Windows主機必須與叢集中的每個節點建立iSCSI連線。原生DSM會選取最佳路徑。



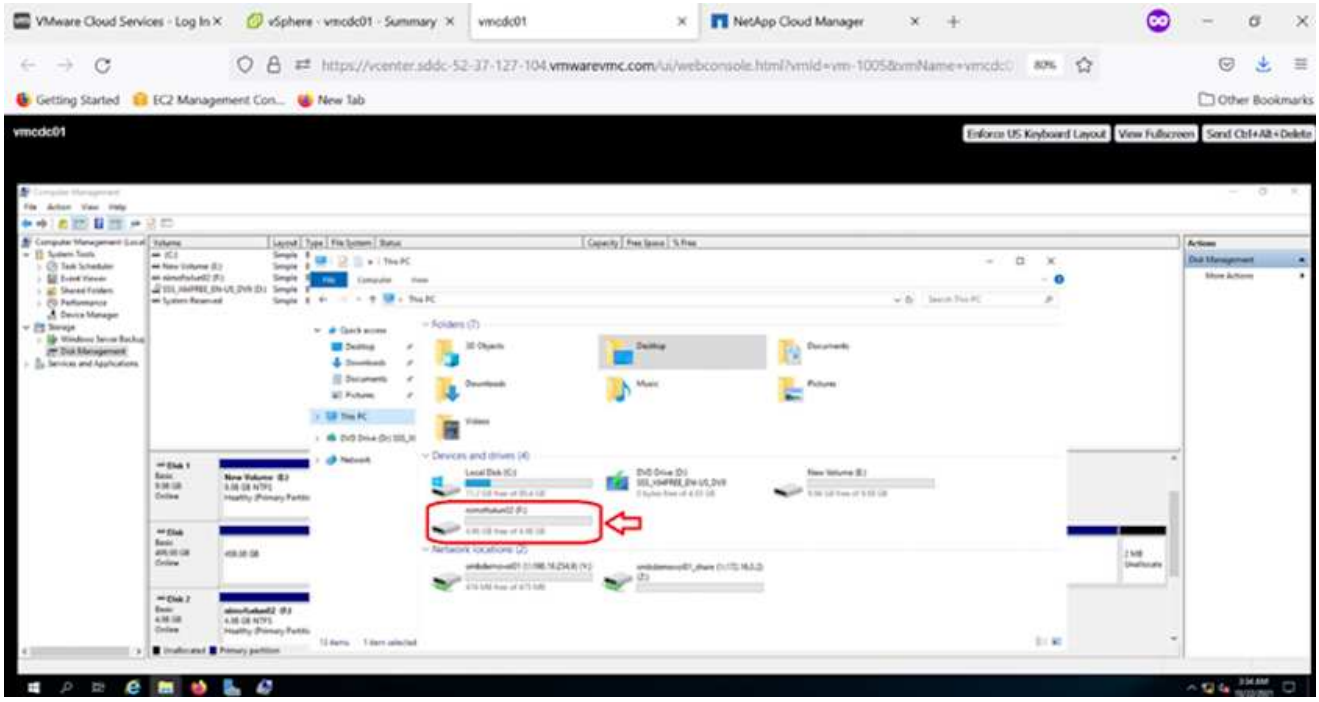
儲存虛擬機器（SVM）上的LUN會在Windows主機上顯示為磁碟。主機不會自動探索任何新增的磁碟。完成下列步驟、觸發手動重新掃描以探索磁碟：

1. 開啟Windows電腦管理公用程式：「開始」>「系統管理工具」>「電腦管理」。
2. 展開導覽樹狀結構中的「Storage（儲存）」節點。
3. 按一下「磁碟管理」。
4. 按一下「行動」>「重新掃描磁碟」。



當Windows主機首次存取新LUN時、它沒有分割區或檔案系統。完成下列步驟、即可初始化LUN、並選擇性地使用檔案系統格式化LUN：

1. 啟動Windows磁碟管理。
2. 以滑鼠右鍵按一下LUN、然後選取所需的磁碟或磁碟分割類型。
3. 依照精靈中的指示進行。在此範例中、磁碟機F：已掛載。



驗證（CVO）Cloud Volumes ONTAP

NetApp以NetApp的整套儲存軟體為基礎、是領先業界的雲端資料管理解決方案、原生可在Amazon Web Services（AWS）、Microsoft Azure和Google Cloud Platform（GCP）上使用。Cloud Volumes ONTAP ONTAP

這是ONTAP 由軟體定義的版本、會消耗雲端原生儲存設備、讓您在雲端和內部環境中擁有相同的儲存軟體、減少重新訓練IT人員以全新方法管理資料的需求。

CVO讓客戶能夠無縫地將資料從邊緣移至資料中心、移至雲端和移回、將混合式雲端整合在一起、所有這些都是透過單一窗格管理主控台NetApp Cloud Manager進行管理。

根據設計、CVO提供極致效能和進階資料管理功能、即使是雲端最嚴苛的應用程式、也能輕鬆滿足需求

以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP

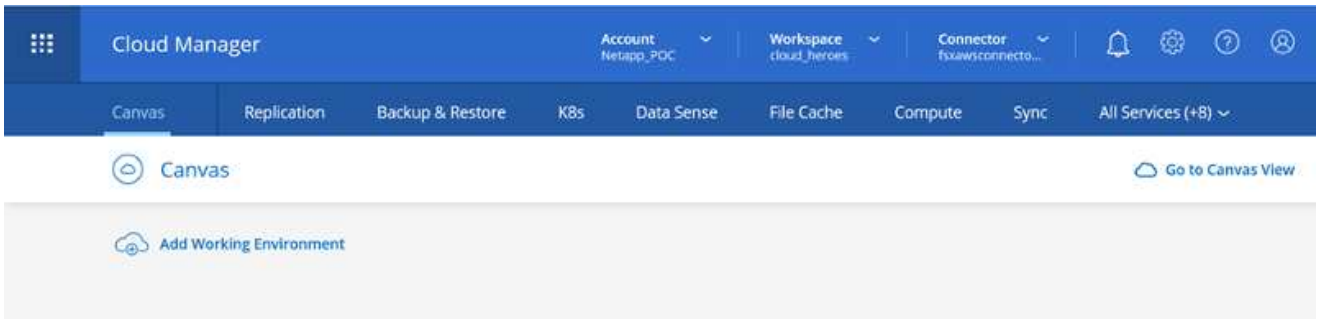
在Cloud Volumes ONTAP AWS中部署新的執行個體（自行執行）

您可以從在AWS SDDC環境的VMware Cloud上建立的VM掛載支援資源和LUN。Cloud Volumes ONTAP這些磁碟區也可掛載於原生AWS VM Linux Windows用戶端、而LUN Cloud Volumes ONTAP 則可在透過iSCSI掛載時、以區塊裝置的形式在Linux或Windows用戶端上存取、因為它支援iSCSI、SMB及NFS傳輸協定。只需幾個簡單步驟、即可設定各個資料區。Cloud Volumes ONTAP

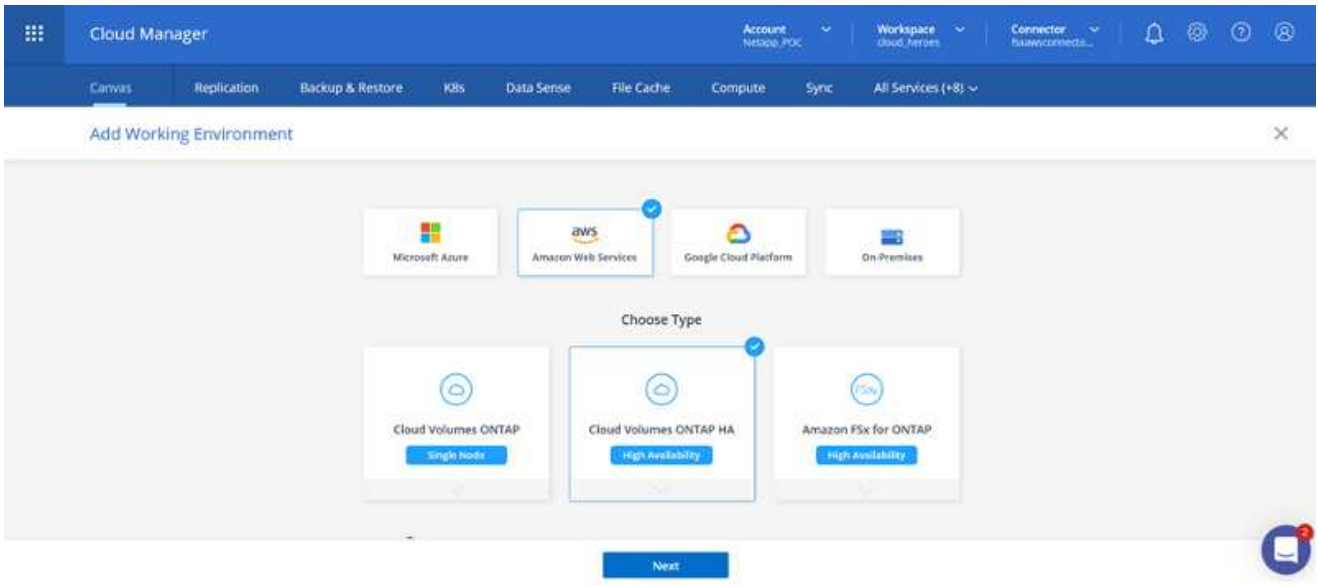
若要將磁碟區從內部部署環境複寫到雲端以進行災難恢復或移轉、請使用站台對站台VPN或DirectConnect、建立與AWS的網路連線。將內部部署的資料複寫到Cloud Volumes ONTAP 內部部署的不適用範圍。若要在內部部署Cloud Volumes ONTAP 和不間斷系統之間複寫資料、請參閱 "設定系統之間的資料複寫"。

使用 "Szizer Cloud Volumes ONTAP" 以準確調整Cloud Volumes ONTAP 實體執行個體的大小。此外、也要監控內部部署效能、以作為Cloud Volumes ONTAP 參考資料的輸入。

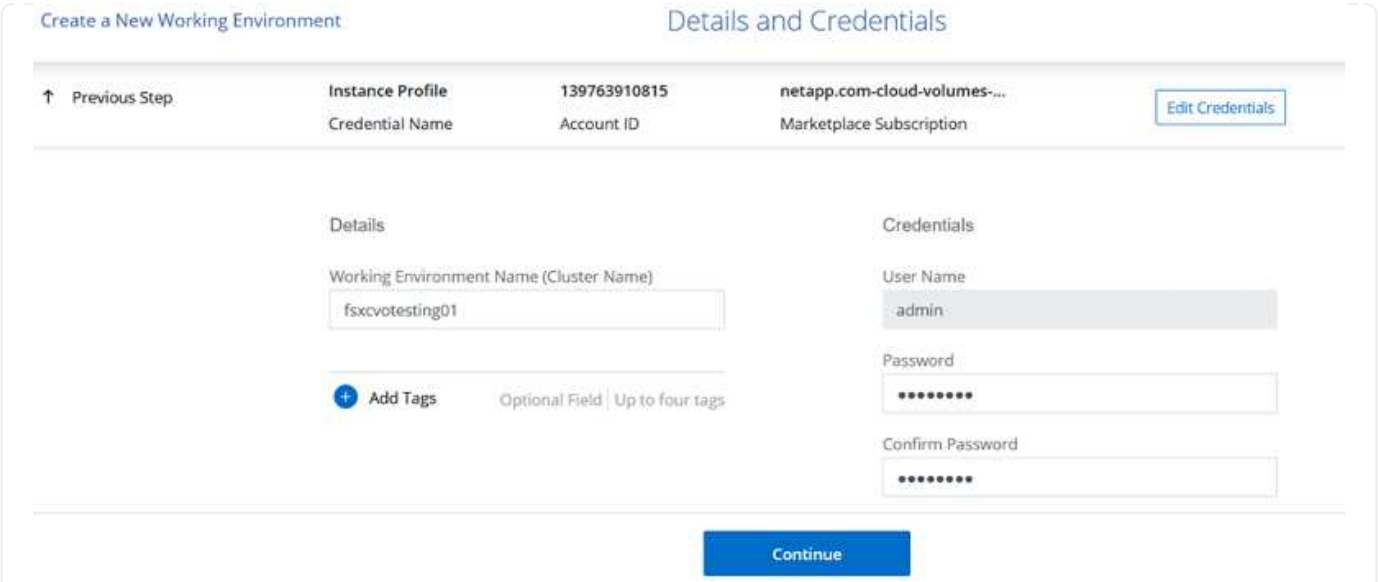
1. 登入NetApp Cloud Central；「Fabric View（架構檢視）」畫面隨即顯示。找到Cloud Volumes ONTAP 「解決方案」索引標籤、然後選取「前往Cloud Manager」。登入之後、便會顯示「畫版」畫面。



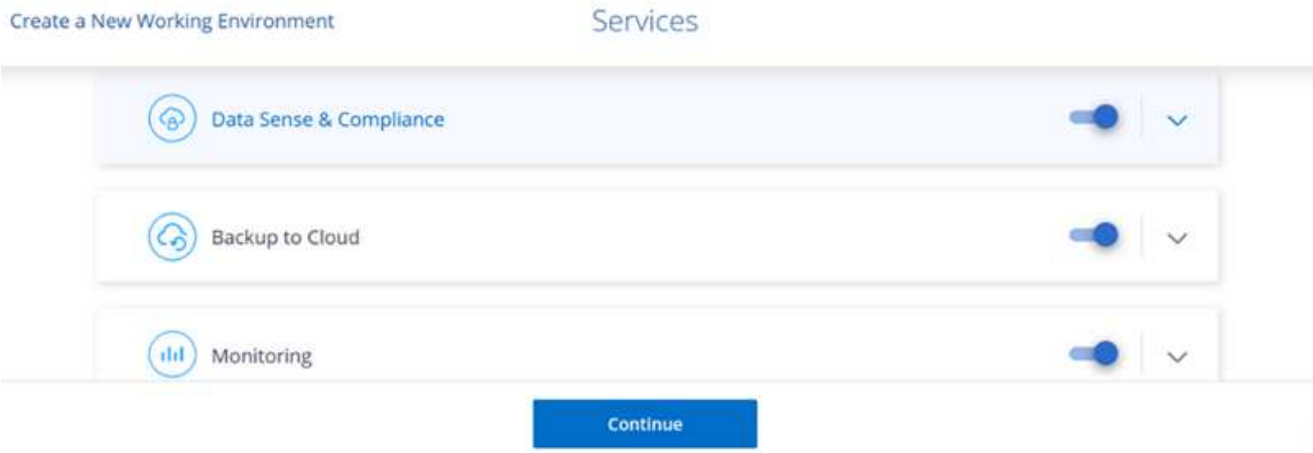
1. 在Cloud Manager首頁上、按一下「Add a Working Environment（新增工作環境）」、然後選取AWS做為雲端和系統組態類型。



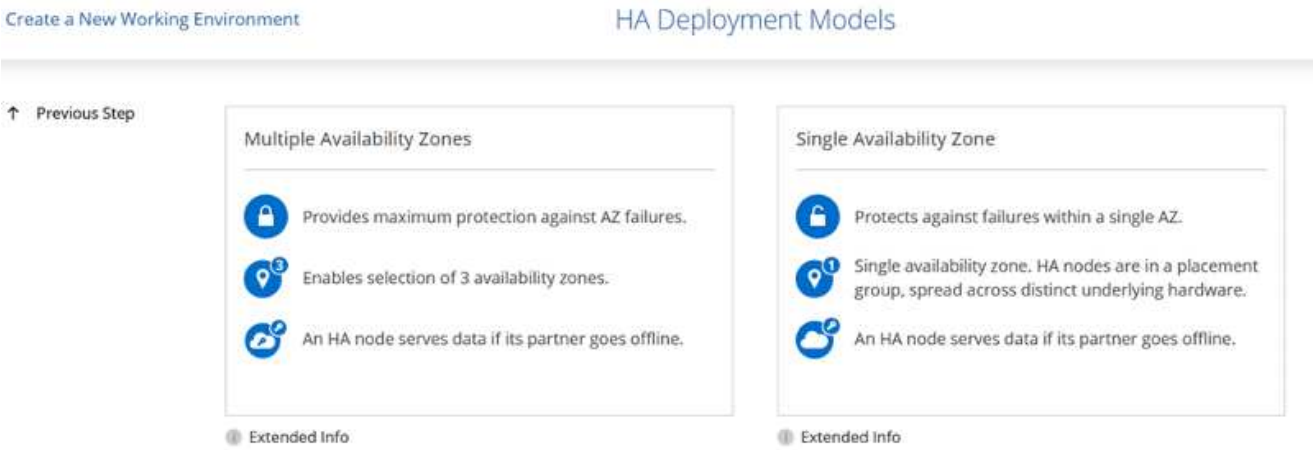
1. 提供要建立的環境詳細資料、包括環境名稱和管理員認證資料。按一下「繼續」。



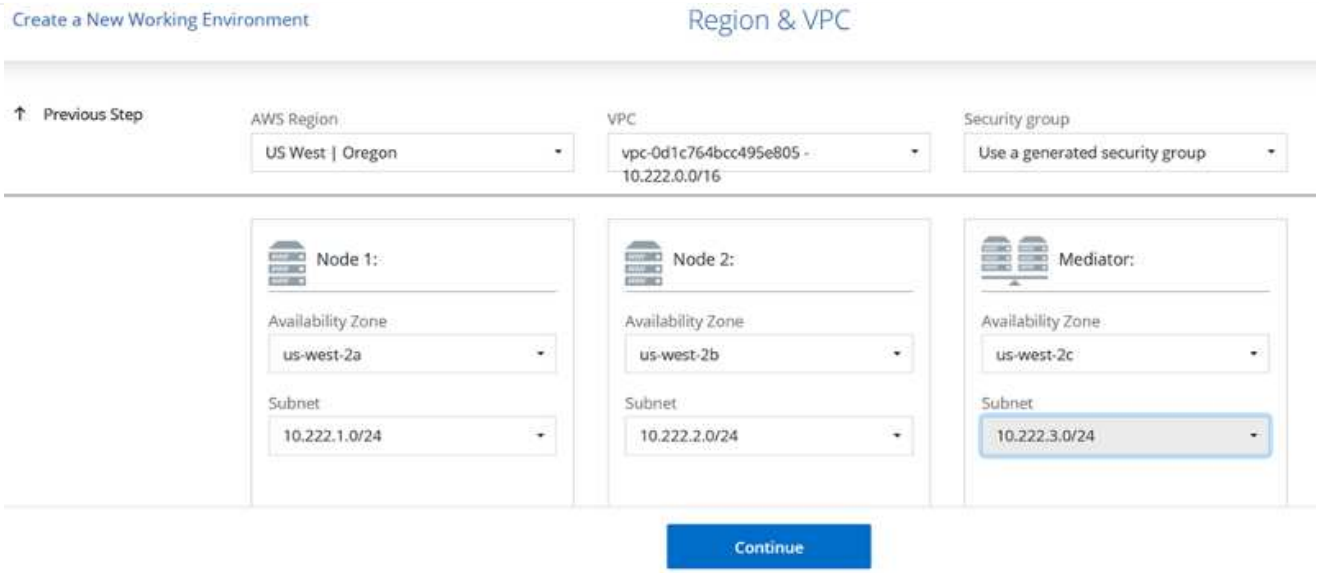
1. 選取 Cloud Volumes ONTAP 部署的附加服務、包括 BlueXP 分類、 BlueXP 備份與還原、以及 Cloud Insights 。按一下「繼續」。



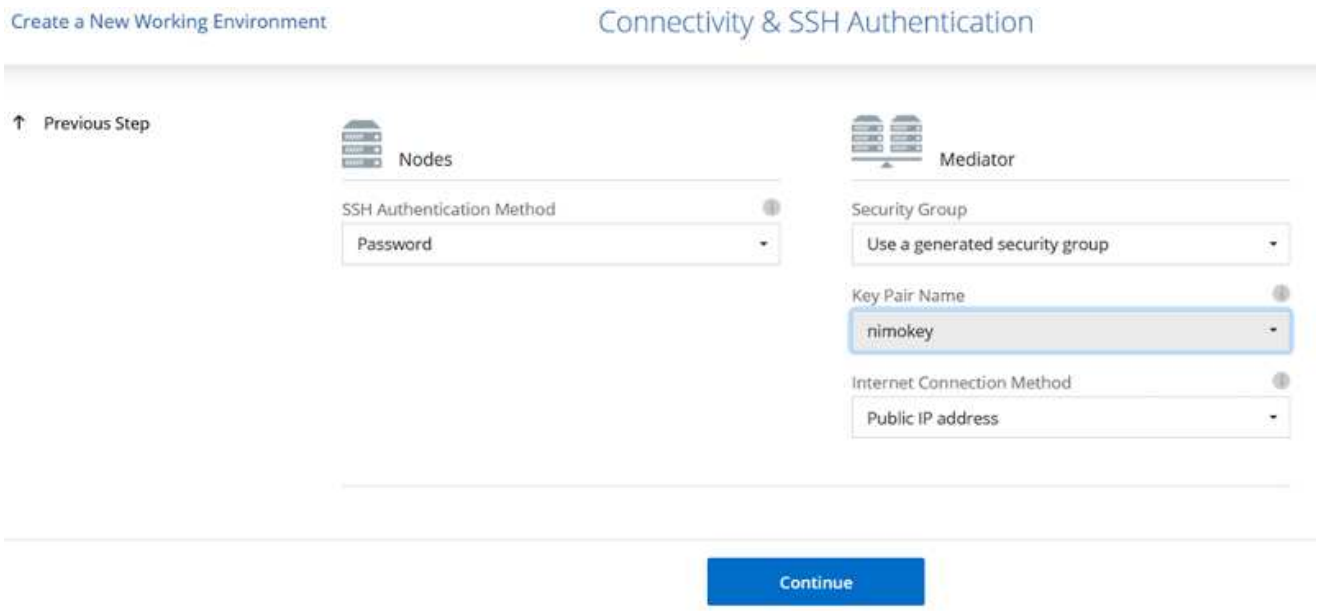
1. 在「HA部署模型」頁面上、選擇「多可用度區域」組態。



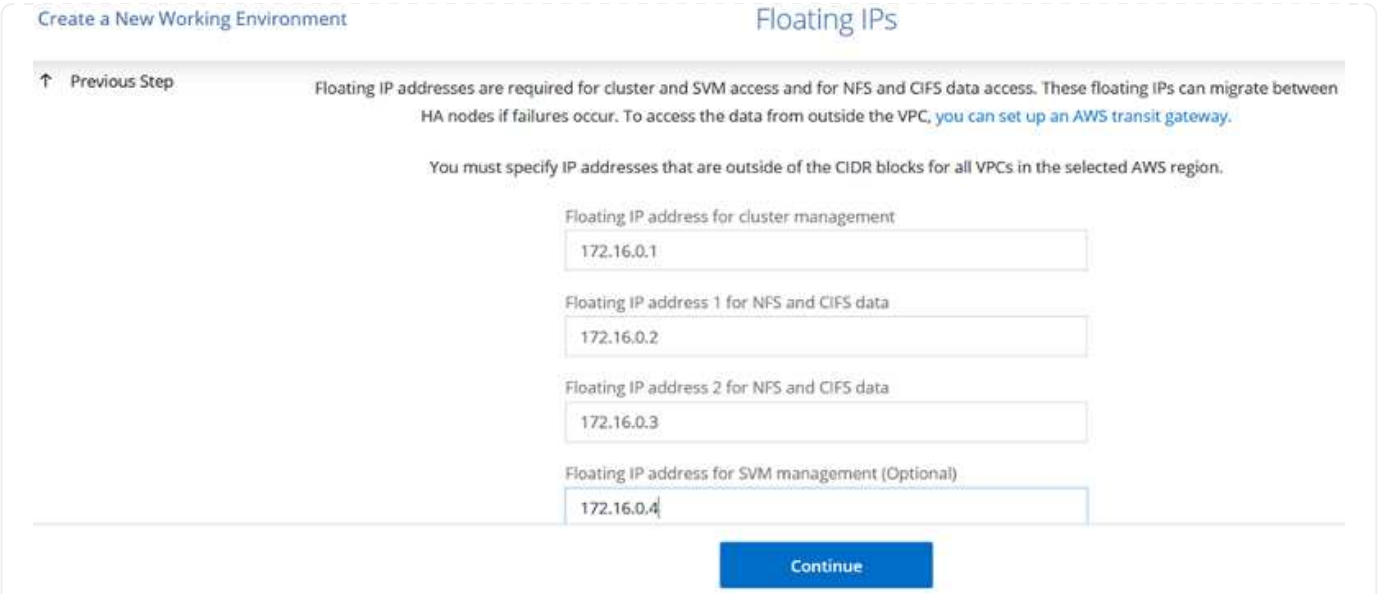
1. 在「Region & VPC（地區與VPC）」頁面上、輸入網路資訊、然後按一下「Continue（繼續）」。



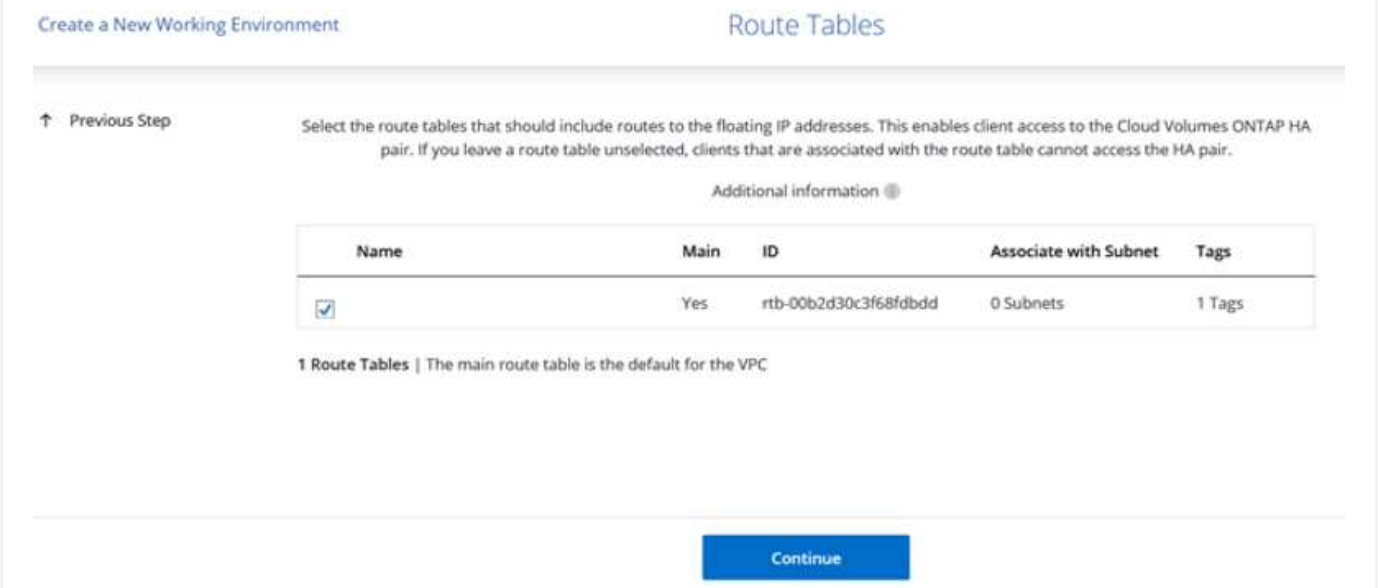
1. 在「連線能力與SSH驗證」頁面上、選擇HA配對與中介器的連線方法。



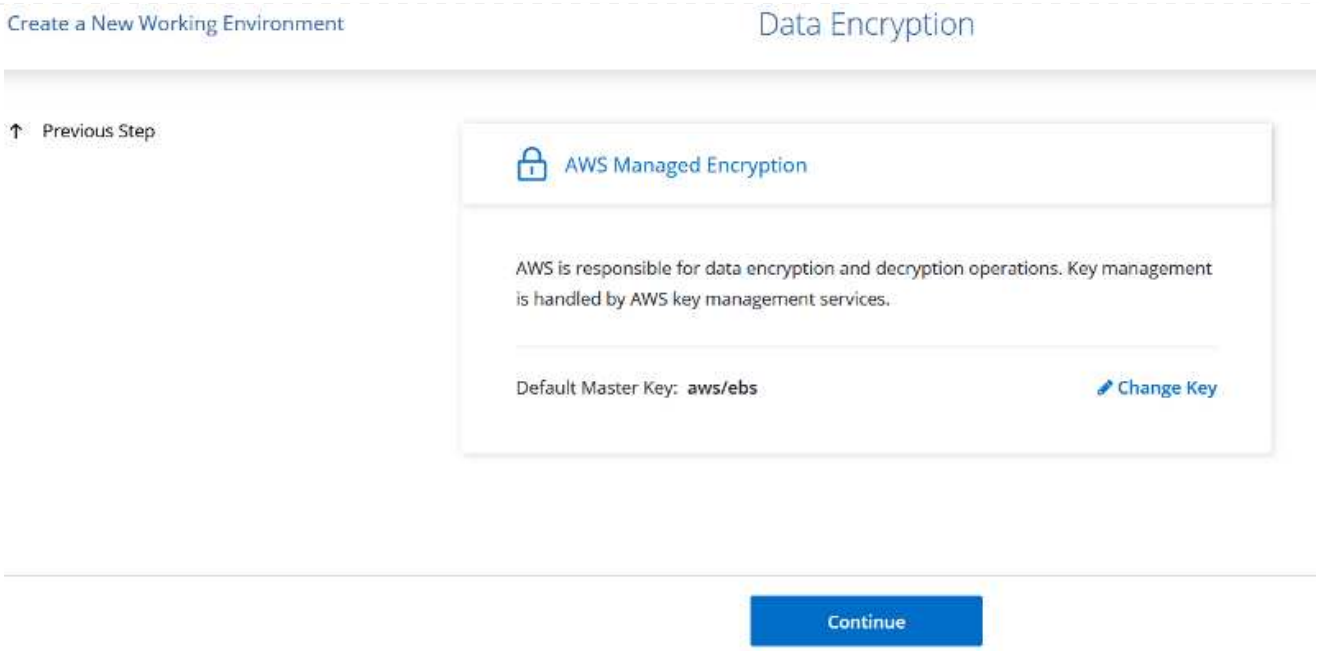
1. 指定浮動IP位址、然後按一下「Continue（繼續）」。



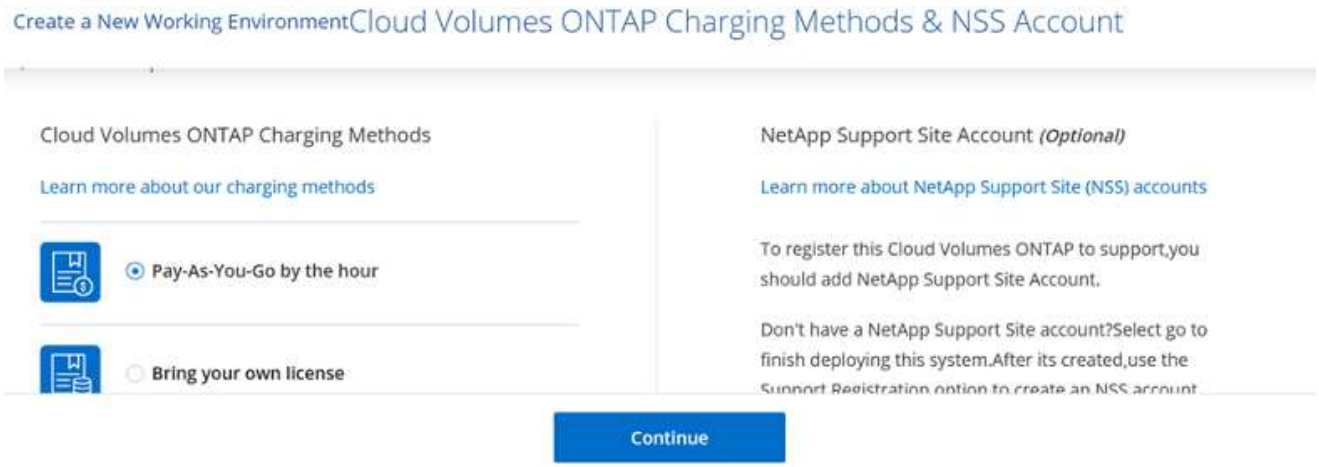
1. 選取適當的路由表以納入通往浮動IP位址的路由、然後按一下「Continue（繼續）」。



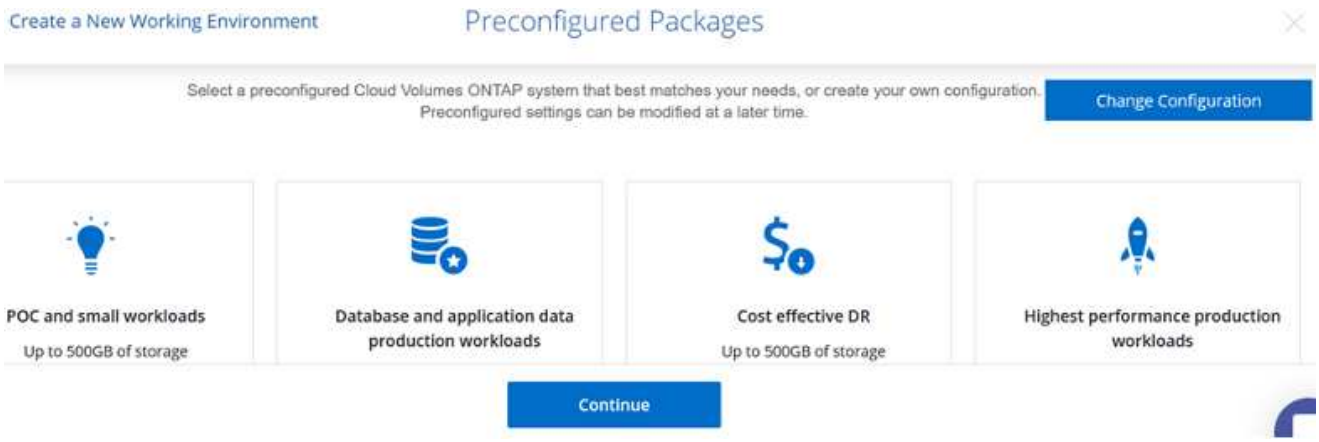
1. 在「Data Encryption（資料加密）」頁面上、選擇「AWS託管加密」。



1. 選取使用許可選項：「隨用隨付」或「BYOL」以使用現有的授權。在此範例中、會使用隨用隨付選項。

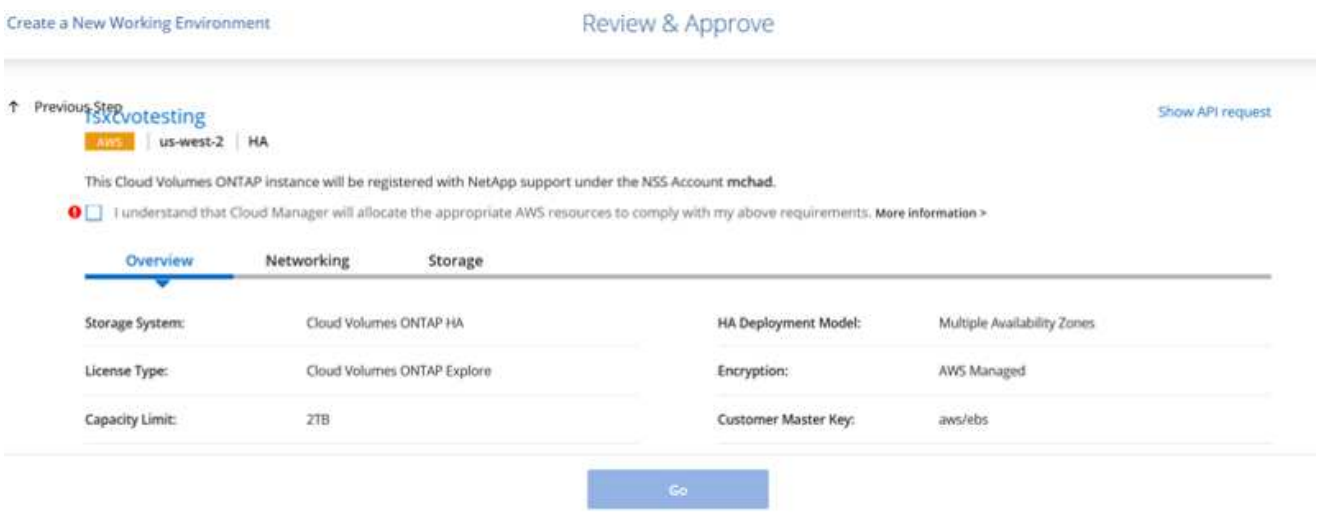


1. 根據要部署在AWS SDDC上VMware雲端上執行的VM上的工作負載類型、選擇幾個預先設定的套件。

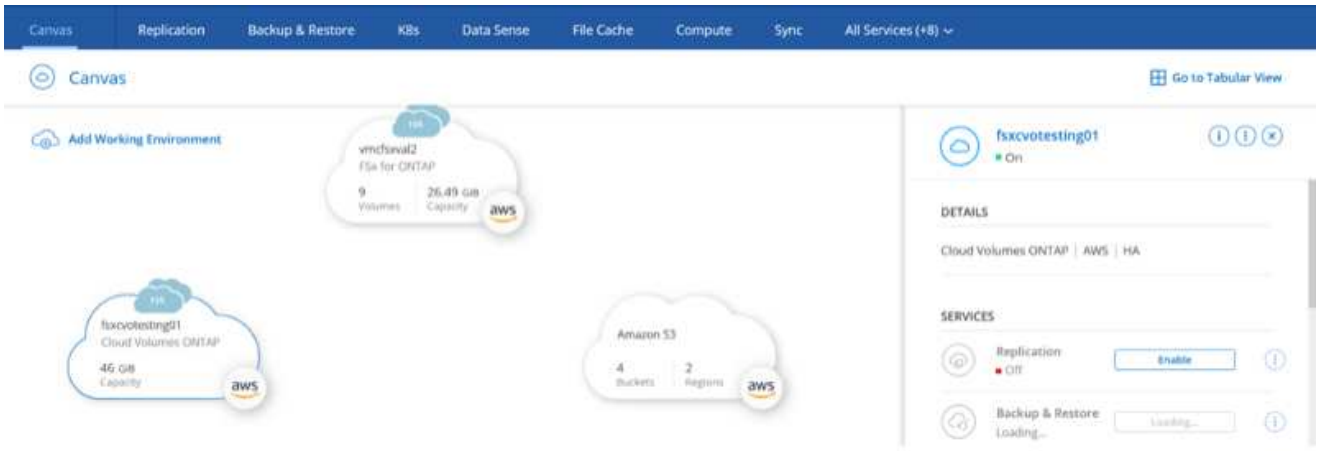


1. 在「Review & Approve（檢閱與核准）」頁面上、檢閱並確認所做的選擇。若要建立Cloud Volumes

ONTAP 此實例、請按一下「Go（執行）」。

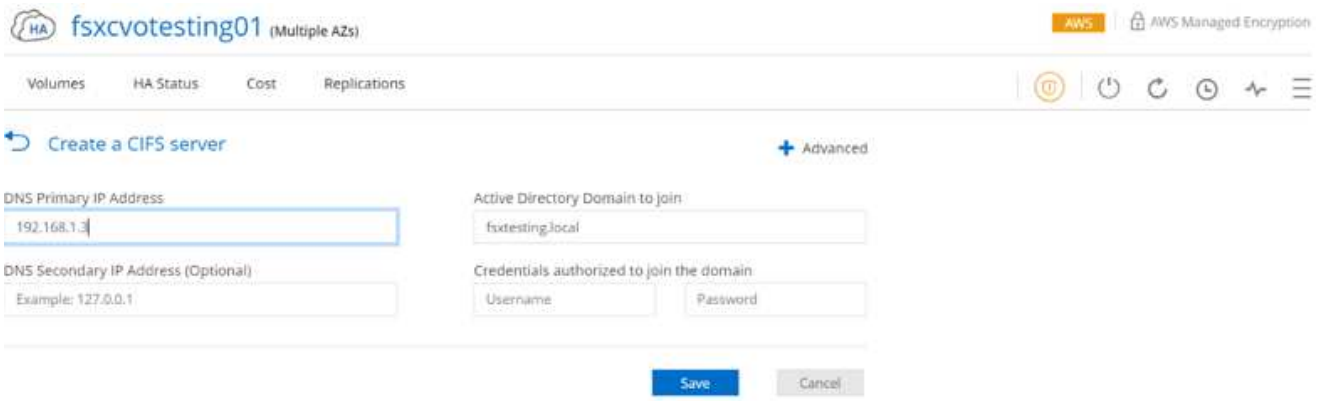


1. 完成供應後、此功能會列在「畫版」頁面上的工作環境中。Cloud Volumes ONTAP

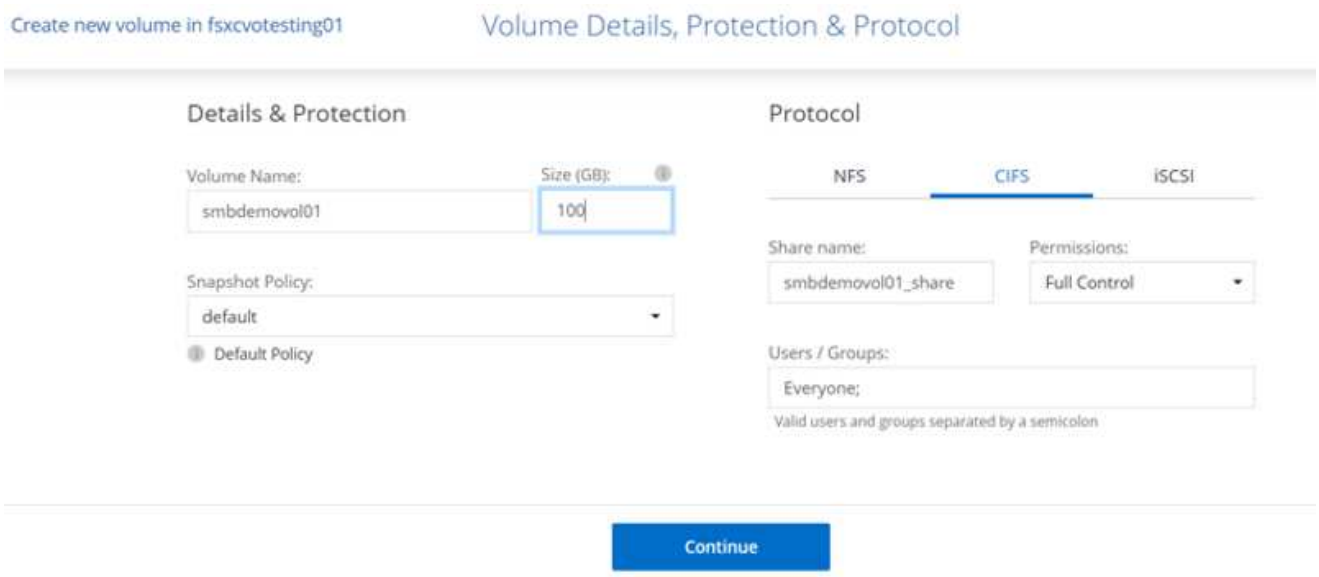


SMB Volume的其他組態

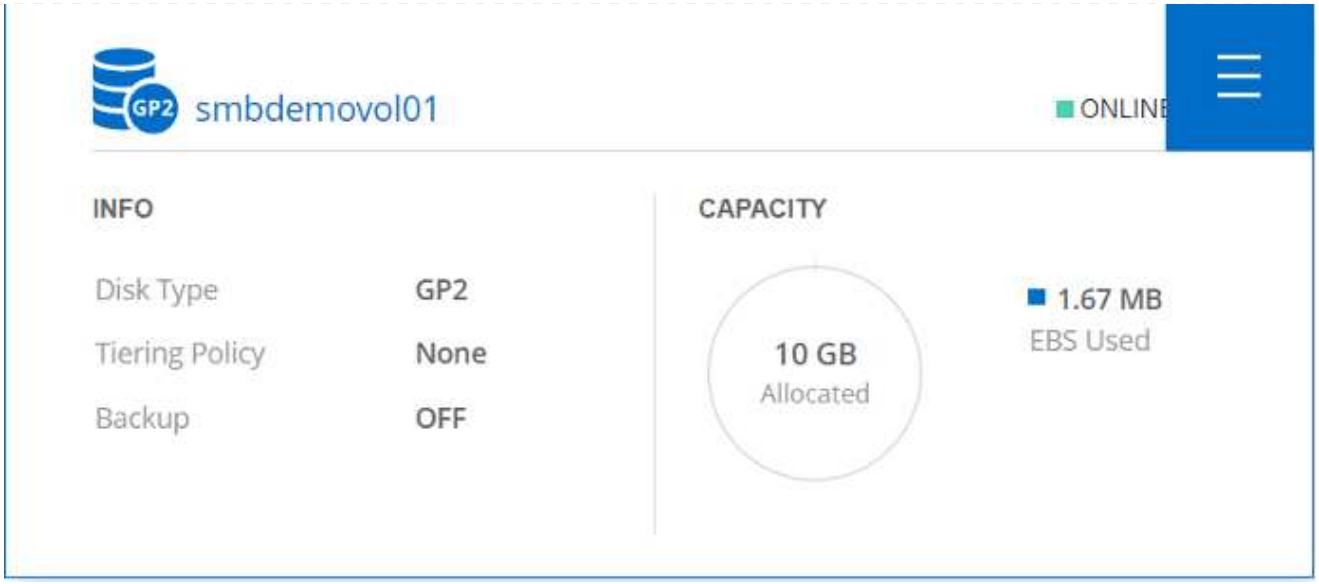
1. 工作環境準備好之後、請確定CIFS伺服器已設定適當的DNS和Active Directory組態參數。您必須先執行此步驟、才能建立SMB Volume。



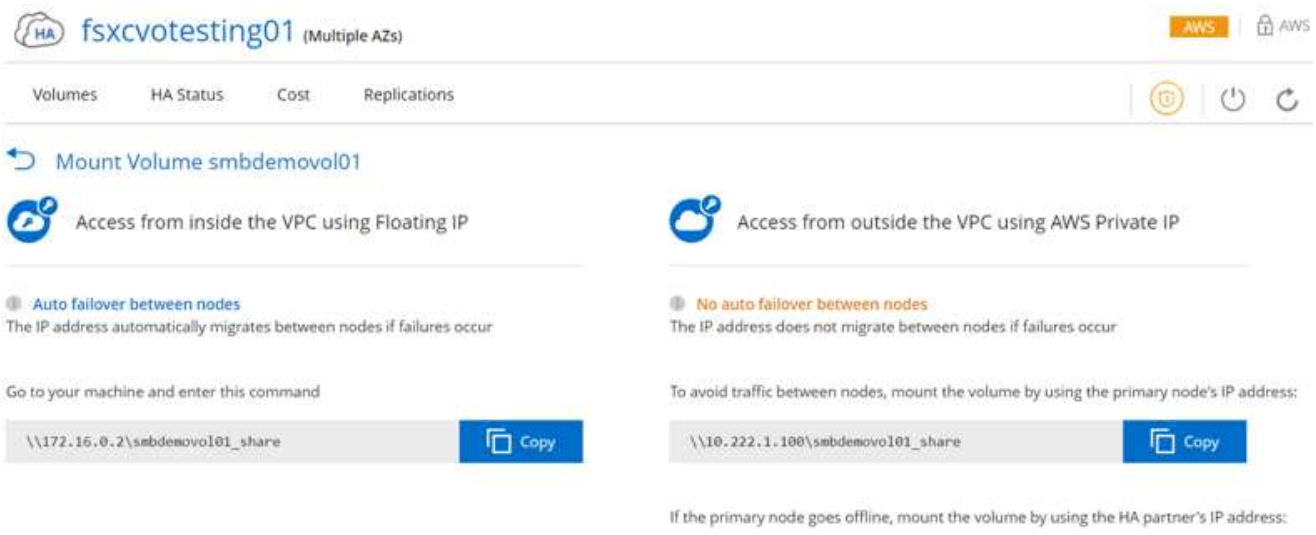
1. 選取CVO執行個體以建立磁碟區、然後按一下Create Volume（建立磁碟區）選項。選擇適當的大小、然後由Cloud Manager選擇內含的Aggregate、或使用進階分配機制將其放置在特定的Aggregate上。在此示範中、SMB被選取為傳輸協定。

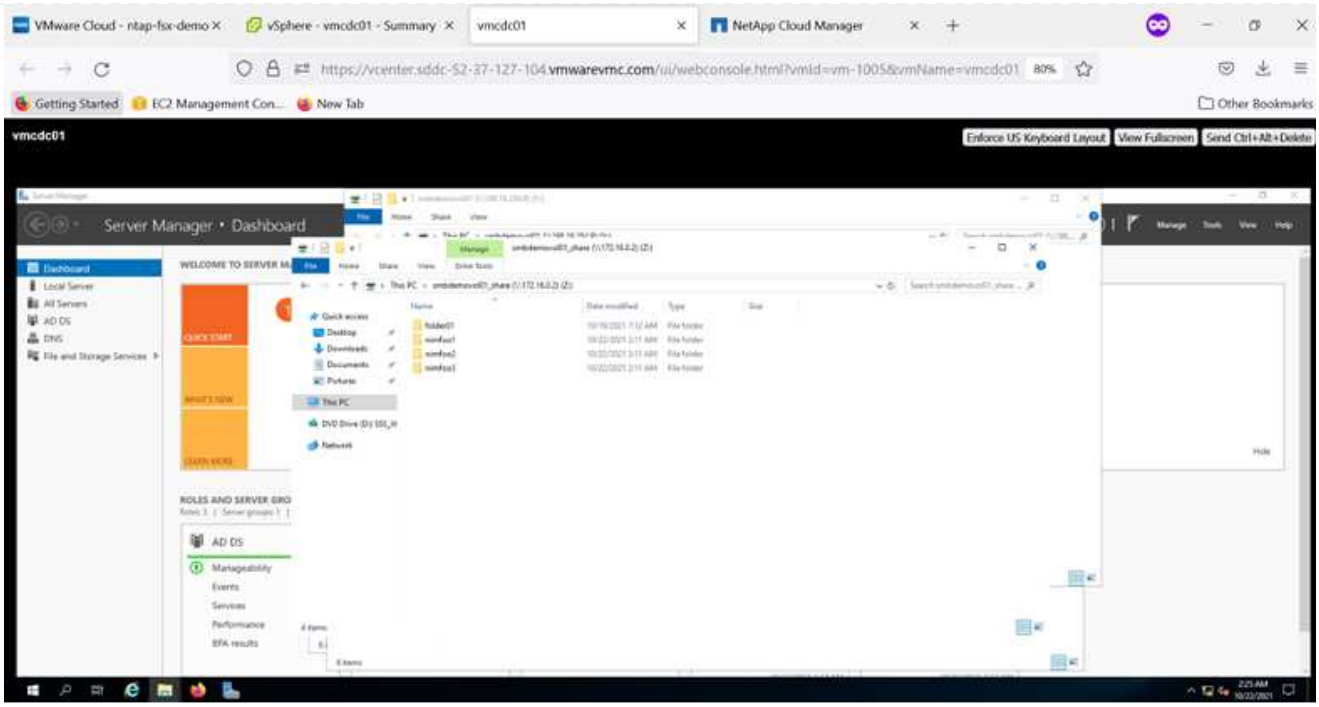


1. 在配置磁碟區之後、磁碟區會出現在「Volumes（磁碟區）」窗格下方。由於CIFS共用區已配置完成、因此您應授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。



1. 建立磁碟區之後、請使用mount命令、從AWS SDDC主機上VMware Cloud上執行的VM連線至共用區。
2. 複製下列路徑、然後使用「對應網路磁碟機」選項、將磁碟區掛載到AWS SDDC中VMware Cloud上執行的VM上。

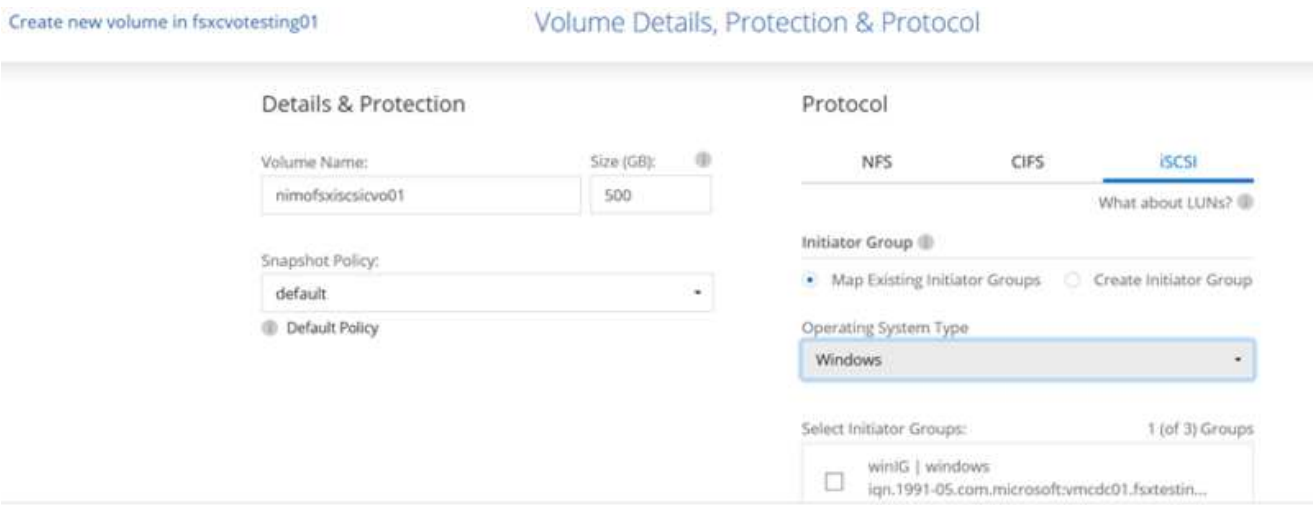


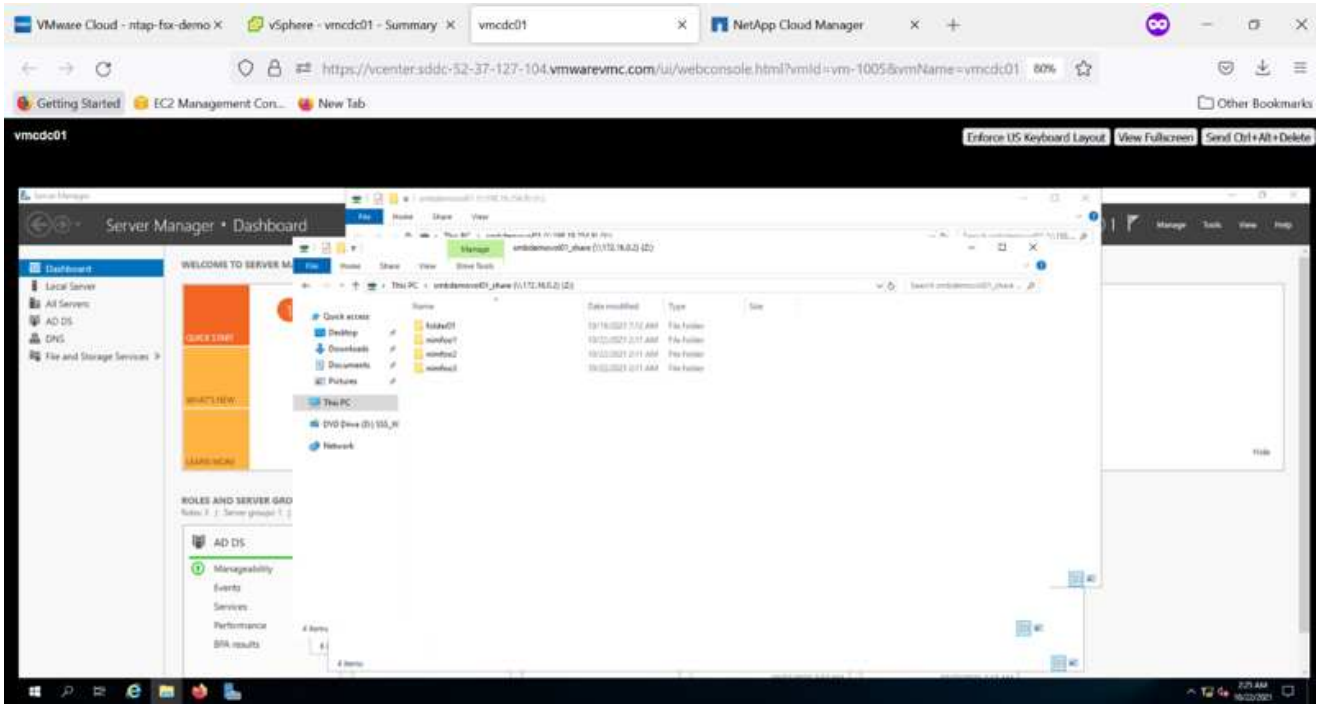

VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Dashboard
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER GROUPS
AD DS
Manageability
Events
Services
Performance
BPA results
This PC
Network
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_X
Manage
Tools
View
Help
Hide

將LUN連接至主機

若要將Cloud Volumes ONTAP LUN連接至主機、請完成下列步驟：

1. 在Cloud Manager的「Canvases」頁面上、按兩下Cloud Volumes ONTAP 「功能性環境」以建立及管理Volume。
2. 按一下「Add Volume（新增Volume）」>「New Volume（新Volume）」、選取「iSCSI（iSCSI）」、然後按一按一下「繼續」。





1. 配置磁碟區之後、選取磁碟區、然後按一下「Target IQN」。若要複製iSCSI合格名稱（IQN）、請按一下複製。設定從主機到 LUN 的 iSCSI 連線。

若要針對位於AWS SDDC上VMware Cloud上的主機完成相同的作業、請完成下列步驟：

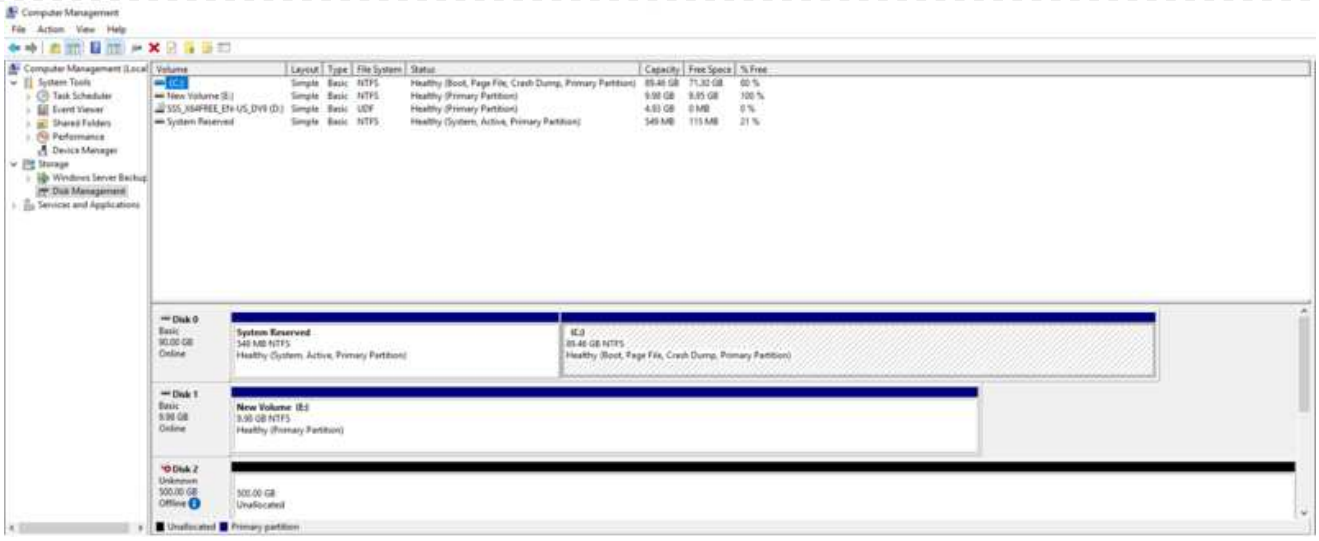
1. 將RDP移至AWS上VMware雲端上的VM。

2. 開啟「iSCSI啟動器內容」對話方塊：「伺服器管理員」>「儀表板」>「工具」>「iSCSI啟動器」。
3. 在「Discovery（探索）」索引標籤中、按一下「Discover Portal（探索入口網站）」或「Add Portal（新增入口網站）」、然後輸入iSCSI目標連接埠的IP位
4. 從「目標」索引標籤中選取探索到的目標、然後按一下「登入」或「連線」。
5. 選取「啟用多重路徑」、然後選取「電腦啟動時自動還原此連線」或「將此連線新增至最愛目標清單」。按一下進階。

Windows主機必須與叢集中的每個節點建立iSCSI連線。原生DSM會選取最佳路徑。

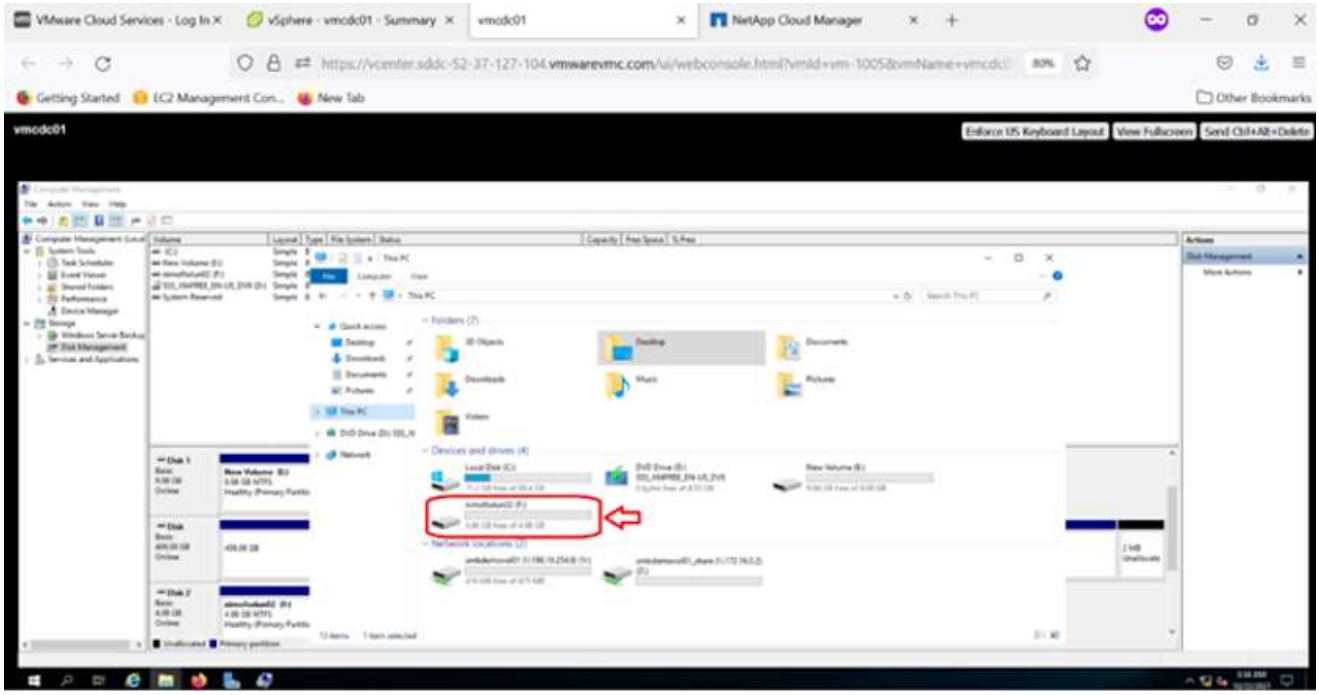
SVM的LUN會顯示為Windows主機的磁碟。主機不會自動探索任何新增的磁碟。完成下列步驟、觸發手動重新掃描以探索磁碟：

1. 開啟Windows電腦管理公用程式：「開始」>「系統管理工具」>「電腦管理」。
2. 展開導覽樹狀結構中的「Storage（儲存）」節點。
3. 按一下「磁碟管理」。
4. 按一下「行動」>「重新掃描磁碟」。



當Windows主機首次存取新LUN時、它沒有分割區或檔案系統。初始化LUN；並可選擇完成下列步驟、以檔案系統格式化LUN：

1. 啟動Windows磁碟管理。
2. 以滑鼠右鍵按一下LUN、然後選取所需的磁碟或磁碟分割類型。
3. 依照精靈中的指示進行。在此範例中、磁碟機F：已掛載。



在Linux用戶端上、確定iSCSI精靈正在執行。配置LUN之後、請參閱Linux套裝作業系統的iSCSI組態詳細指南。例如、可以找到Ubuntu iSCSI組態 "請按這裡"。若要驗證、請從Shell執行lsblk cmd。

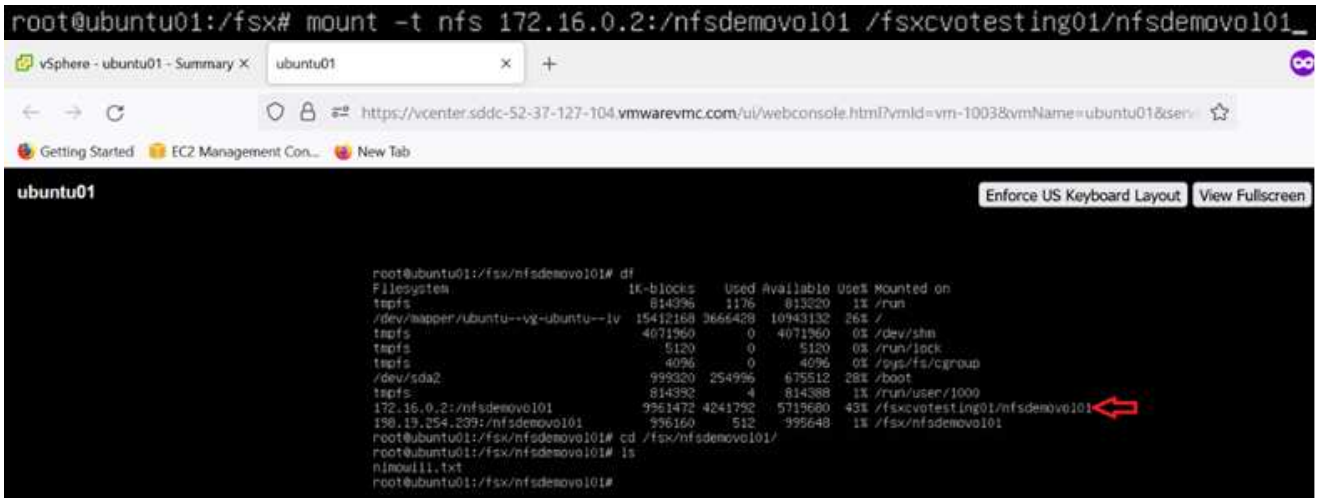
在**Cloud Volumes ONTAP Linux**用戶端上掛載不只是**NFS**磁碟區

若要從Cloud Volumes ONTAP AWS SDDC上VMC內的VM掛載支援功能（DIY）檔案系統、請完成下列步驟：

1. 連線至指定的Linux執行個體。
2. 使用安全Shell（SSH）開啟執行個體上的終端機、然後以適當的認證登入。
3. 使用下列命令建立磁碟區掛載點的目錄。

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. 將Amazon FSX for NetApp ONTAP SfNFS Volume掛載到上一步建立的目錄。
```

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



ANF資料存放區解決方案總覽

每個成功的組織都走上轉型與現代化的道路。在這項流程中、企業通常會使用現有的VMware投資、同時善用雲端效益、並探索如何使移轉、突發、擴充及災難恢復程序盡可能順暢無礙。移轉至雲端的客戶必須評估彈性與爆發、資料中心結束、資料中心整合、生命週期結束案例、併購等問題。每個組織採用的方法可能會因其各自的業務優先順序而有所不同。選擇雲端型作業時、選擇效能適當且障礙最小的低成本模式、是關鍵目標。除了選擇適當的平台、儲存設備和工作流程協調對於釋放雲端部署和彈性的強大威力而言、更是極為重要。

使用案例

雖然Azure VMware解決方案為客戶提供獨特的混合式功能、但有限的原生儲存選項限制了其對於具有大量儲存工作負載的組織的使用效益。由於儲存設備直接與主機相連、因此擴充儲存設備的唯一方法是新增更多主機、如此一來、儲存密集工作負載的成本就會增加35%至40%以上。這些工作負載需要額外的儲存容量、而非額外的馬

力、但這表示需要支付額外的主機費用。

讓我們來思考下列案例：客戶需要六台主機來處理馬力（vcpU/vMem）、但他們也需要大量的儲存設備。根據評估結果、他們需要12台主機來滿足儲存需求。如此一來、整體TCO就會增加、因為他們必須在真正需要更多儲存設備的情況下、購買所有額外的馬力。這適用於任何使用案例、包括移轉、災難恢復、突發、開發/測試、等等。

Azure VMware解決方案的另一個常見使用案例是災難恢復（DR）。大多數組織都沒有防礙災難恢復策略、或是難以證明只是為了災難恢復而執行重影資料中心的理由。系統管理員可能會透過試運行式叢集或隨需叢集來探索零佔用空間的災難恢復選項。然後、他們可以擴充儲存設備、而不需要新增額外的主機、這可能是一個吸引人的選項。

因此、總的來說、使用案例可分為兩種類別：

- 使用ANF資料存放區擴充儲存容量
- 使用ANF資料存放區做為災難恢復目標、在軟體定義的資料中心（SDDC）之間、從內部部署或Azure區域內進行成本最佳化的恢復工作流程。本指南深入探討如何使用Azure NetApp Files NetApp為資料存放區提供最佳化的儲存（目前為公開預覽） 搭配Azure VMware解決方案中同級最佳的資料保護與DR功能、可讓您從vSAN儲存設備卸載儲存容量。

> 如需使用ANF資料存放區的其他資訊、請聯絡您所在地區的NetApp或Microsoft解決方案架構設計師。

Azure中的**VMware Cloud**選項

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

無論使用何種雲端、部署VMware SDDC時、初始叢集都包含下列元件：

- 使用vCenter伺服器應用裝置進行運算虛擬化的VMware ESXi主機進行管理。
- VMware vSAN超融合式儲存設備整合了每個ESXi主機的實體儲存資產。
- VMware NSX提供虛擬網路與安全性、並搭配NSX Manager叢集進行管理。

結論

無論您的目標是全雲端或混合雲、Azure NetApp Files 透過無縫接軌的應用程式層資料需求、提供絕佳的選項來部署及管理應用程式工作負載及檔案服務、同時降低TCO。無論使用案例為何、請選擇Azure VMware解決方案搭配Azure NetApp Files VMware解決方案、以快速實現雲端效益、一致的基礎架構、以及跨內部部署和多個雲端的作業、工作負載的雙向可攜性、以及企業級容量和效能。這是用來連接儲存設備的熟悉程序和程序。請記住、這只是資料的變更位置、加上新名稱；工具和程序都維持不變、Azure NetApp Files 而VMware協助最佳化整體部署。

重點摘要

本文件的重點包括：

- 現在、您可以在Azure NetApp Files AVS SDDC上使用效能不實的資料存放區。
- 縮短應用程式回應時間、提供更高的可用度、以便在需要時隨時隨地存取工作負載資料。
- 透過簡單且即時的調整大小功能、簡化vSAN儲存設備的整體複雜度。
- 利用動態重新塑造功能、保證關鍵任務工作負載的效能。
- 如果您的目的地是Azure VMware Solution Cloud、Azure NetApp Files 那麼針對最佳化部署而言、最佳化的儲存解決方案就是理想選擇。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請參閱下列網站連結：

- Azure VMware解決方案文件

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

- 本文檔 Azure NetApp Files

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

- 將Azure NetApp Files 物件資料存放區附加至Azure VMware解決方案主機（預覽）

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

適用於**Azure**的**NetApp**來賓連線儲存設備選項

Azure可透過原生Azure NetApp Files 的不穩定（anf）服務或Cloud Volumes ONTAP 使用支援以客體連線的NetApp儲存設備（CVO）。

產品統計（ **ANF** ） **Azure NetApp Files**

支援Azure的企業級資料管理與儲存、讓您輕鬆管理工作負載與應用程式。Azure NetApp Files將工作負載移轉至雲端、然後在不犧牲效能的情況下執行。

解決障礙、讓您將所有檔案型應用程式移至雲端。Azure NetApp Files第一次、您不需要重新建構應用程式、也能在不複雜的情況下、持續為應用程式提供儲存設備。

由於此服務是透過Microsoft Azure Portal提供、因此使用者在Microsoft企業協議中享有完整的託管服務。由Microsoft管理的世界級支援、讓您完全安心。此單一解決方案可讓您快速輕鬆地新增多重傳輸協定工作負載。您可以建置及部署Windows和Linux檔案型應用程式、即使是舊有環境也沒問題。

以客體連線儲存設備的形式提供**Azure NetApp Files**

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

您可以從Azure VMware解決方案SDDC環境中建立的VM掛載支援資料共享。Azure NetApp Files由於Azure NetApp Files 支援SMB和NFS傳輸協定、因此也可以在Linux用戶端上掛載磁碟區並對應至Windows用戶端。只需五個簡單步驟即可設定各個資料區。Azure NetApp Files

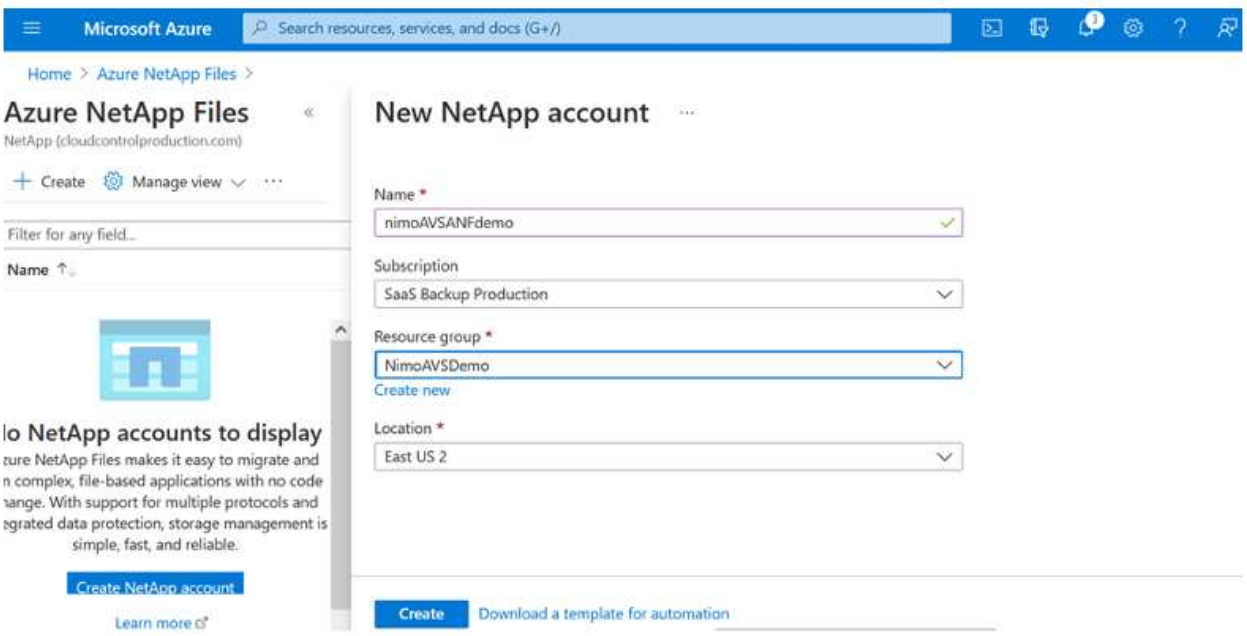
VMware解決方案的VMware解決方案必須位於同一個Azure地區。Azure NetApp Files

建立及掛載**Azure NetApp Files** 功能

若要建立及掛載Azure NetApp Files 此功能、請完成下列步驟：

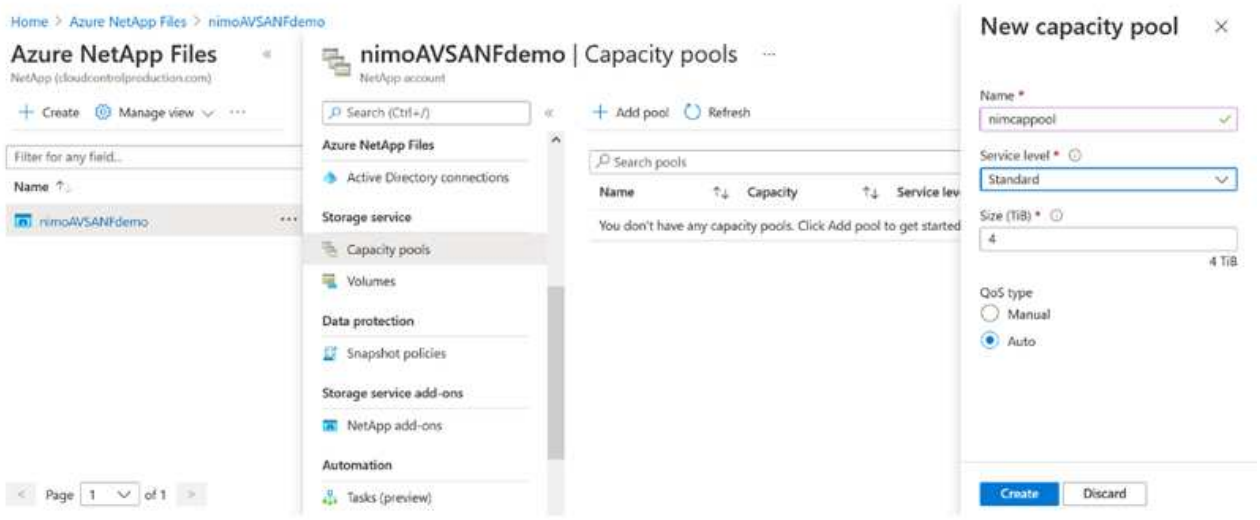
1. 登入Azure Portal並存取Azure NetApp Files 功能。使用Azure NetApp Files *AZ*供應商*Register --namespace*–wait_命令來驗證對該服務的存取權、並登錄Azure NetApp Files 該資源供應商。Microsoft.NetApp註冊完成後、請建立NetApp帳戶。

   如需詳細步驟、請參閱 "共享Azure NetApp Files"。本頁將引導您逐步完成程序。

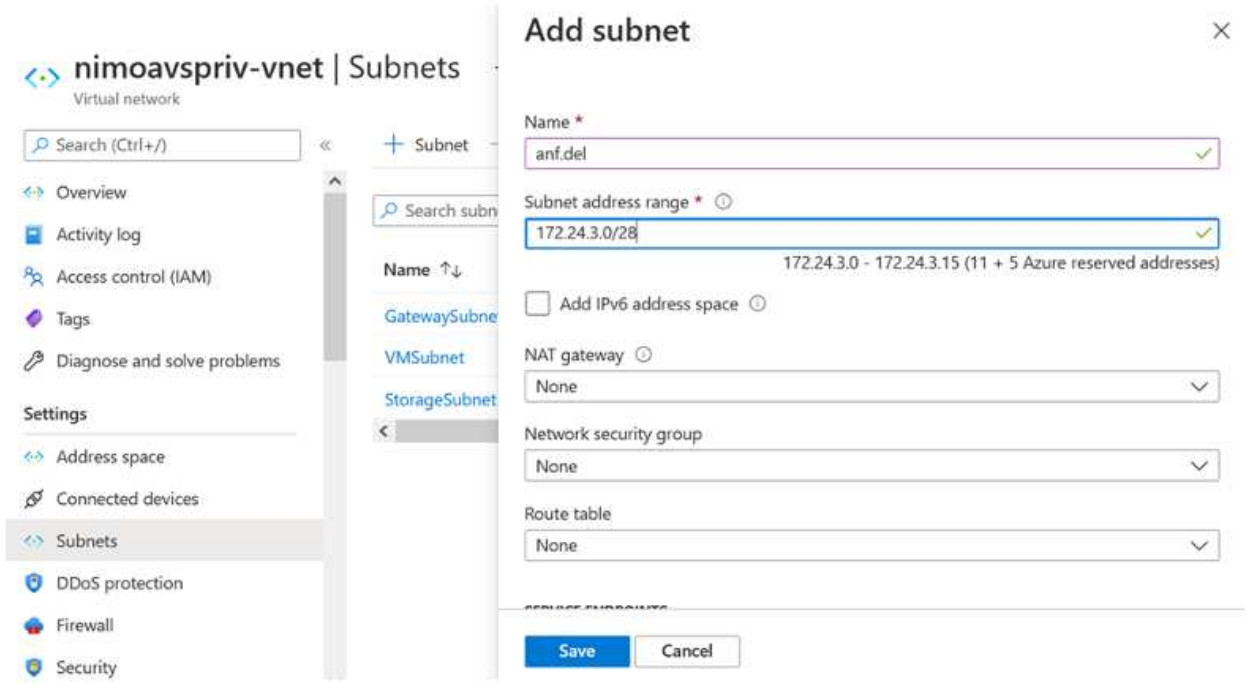


2. 建立NetApp帳戶之後、請使用所需的服務層級和大小來設定容量資源池。

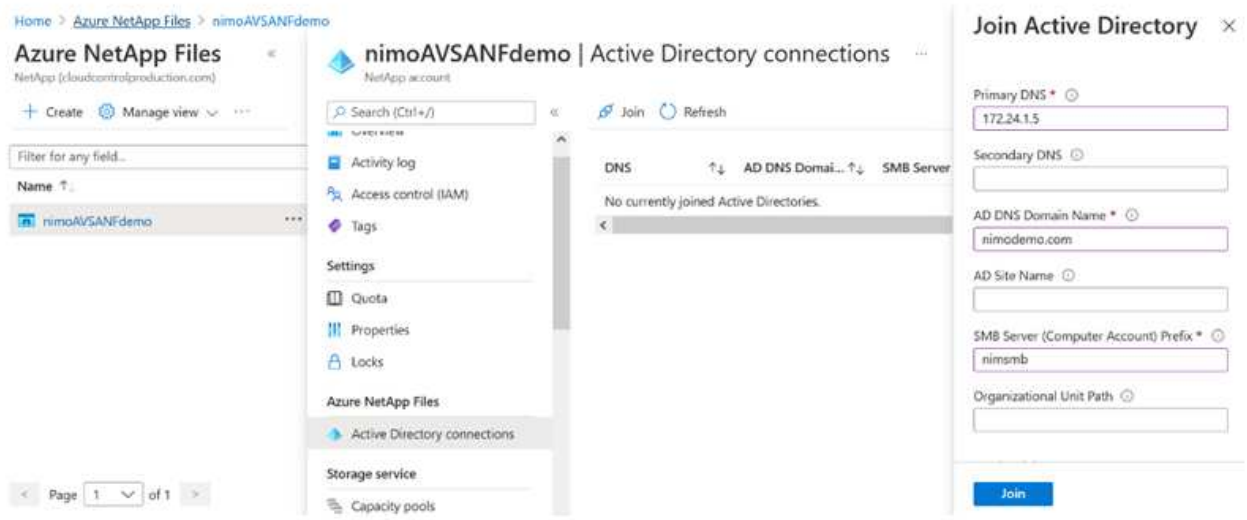
   如需詳細資訊、請參閱 "設定容量資源池"。



3. 設定委派的子網路Azure NetApp Files 以供使用、並在建立磁碟區時指定此子網路。如需建立委派子網路的詳細步驟、請參閱 "將子網路委派Azure NetApp Files 給"。

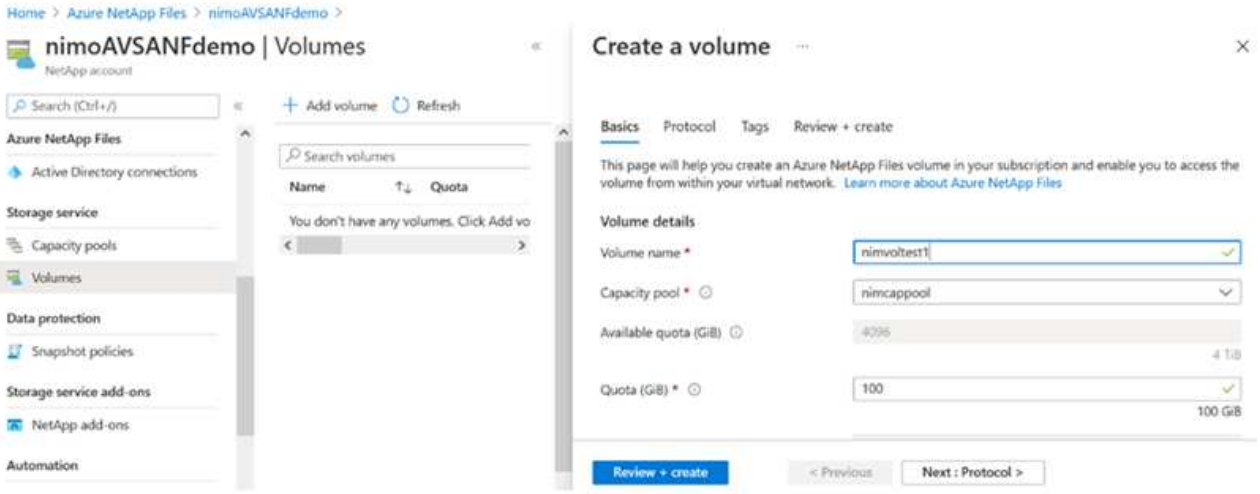


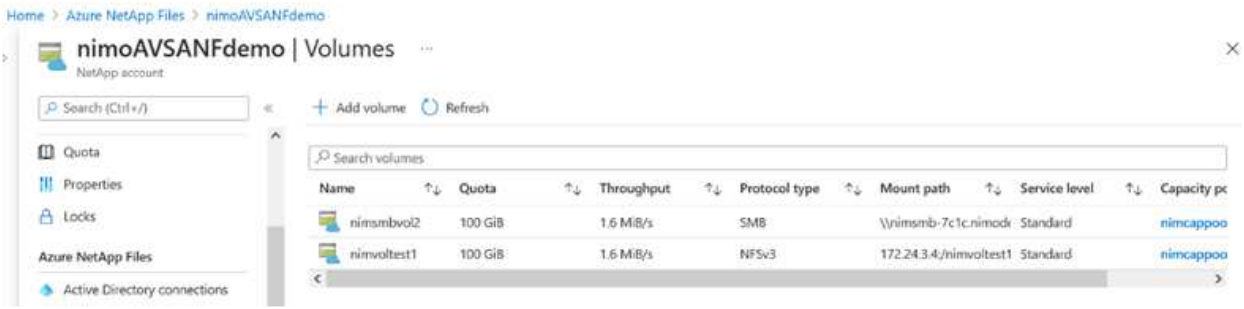
4. 使用容量集區刀鋒下的Volume刀鋒來新增SMB Volume。在建立SMB磁碟區之前、請先確認已設定Active Directory連接器。



5. 按一下「Review + Create（檢閱+建立）」以建立SMB Volume。

   如果應用程式是SQL Server、則啟用SMB持續可用度。

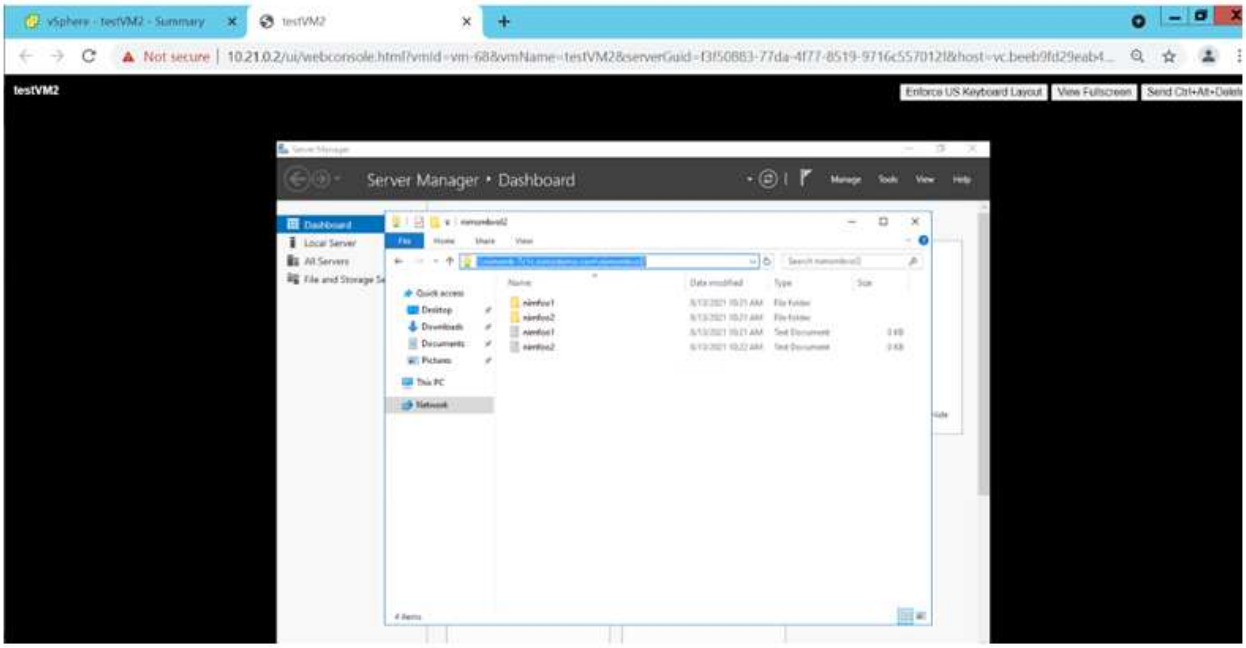


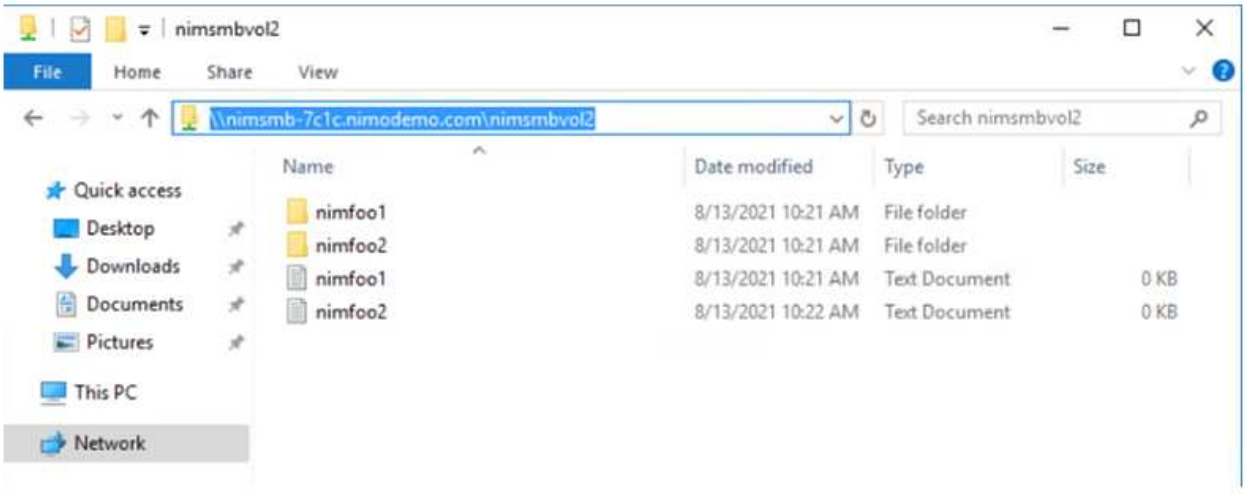


如需深入瞭Azure NetApp Files 解根據大小或配額而提供的效能、請參閱 "效能考量Azure NetApp Files"。

6. 連線到位後、即可掛載磁碟區並用於應用程式資料。

若要完成此作業、請從Azure入口網站按一下Volumes刀鋒、然後選取要掛載的磁碟區、並存取掛載指示。複製路徑、然後使用「對應網路磁碟機」選項、將磁碟區掛載到執行Azure VMware Solution SDDC的VM上。





7. 若要在Azure VMware Solution SDDC上執行的Linux VM上掛載NFS Volume、請使用相同的程序。使用Volume重新塑造或動態服務層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:~$
```

如需詳細資訊、請參閱 "動態變更磁碟區的服務層級"。

驗證（CVO）Cloud Volumes ONTAP

NetApp以NetApp的整套儲存軟體為基礎、是領先業界的雲端資料管理解決方案、原生可在Amazon Web Services（AWS）、Microsoft Azure和Google Cloud Platform（GCP）上使用。Cloud Volumes ONTAP ONTAP

這是ONTAP 由軟體定義的版本、會消耗雲端原生儲存設備、讓您在雲端和內部環境中擁有相同的儲存軟體、減少重新訓練IT人員以全新方法管理資料的需求。

CVO讓客戶能夠無縫地將資料從邊緣移至資料中心、移至雲端和移回、將混合式雲端整合在一起、所有這些都是透過單一窗格管理主控台NetApp Cloud Manager進行管理。

根據設計、CVO提供極致效能和進階資料管理功能、即使是雲端最嚴苛的應用程式、也能輕鬆滿足需求

以客體連線儲存設備形式提供的資訊（**CVO**）**Cloud Volumes ONTAP**

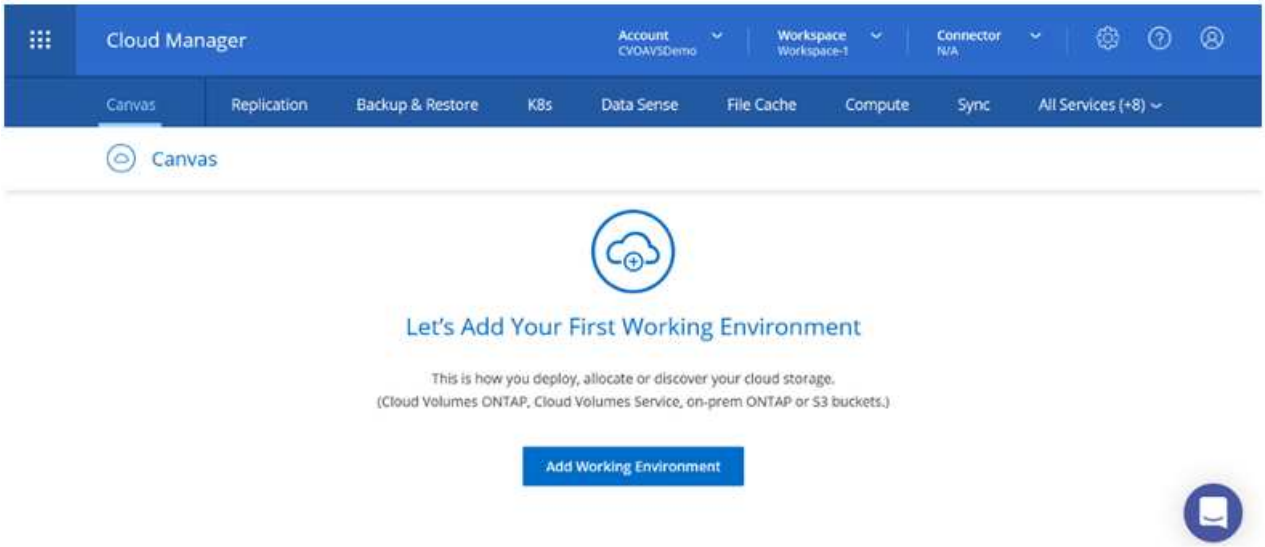
在Cloud Volumes ONTAP Azure中部署全新的功能

您可以從Azure VMware解決方案SDDC環境中建立的VM掛載支援資源和LUN。Cloud Volumes ONTAP由於Cloud Volumes ONTAP 支援iSCSI、SMB及NFS傳輸協定、所以也可在Linux用戶端和Windows用戶端上掛載這些磁碟區。只需幾個簡單步驟、即可設定各個資料區。Cloud Volumes ONTAP

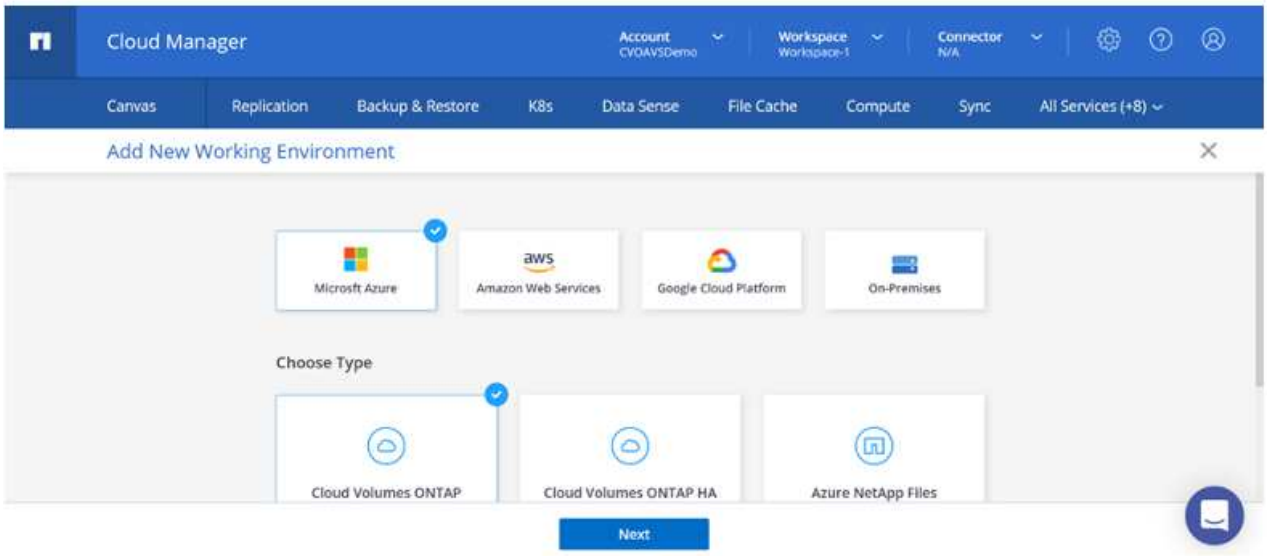
若要將磁碟區從內部部署環境複寫至雲端以進行災難恢復或移轉、請使用站台對站台VPN或ExpressRoute、建立與Azure的網路連線。將內部部署的資料複寫到Cloud Volumes ONTAP 內部部署的不適用範圍。若要在內部部署Cloud Volumes ONTAP 和不間斷系統之間複寫資料、請參閱 "設定系統之間的資料複寫"。

使用 "Szizer Cloud Volumes ONTAP" 以準確調整Cloud Volumes ONTAP 實體執行個體的大小。同時監控內部部署的效能、以做Cloud Volumes ONTAP 為VMware內部資料的輸入。

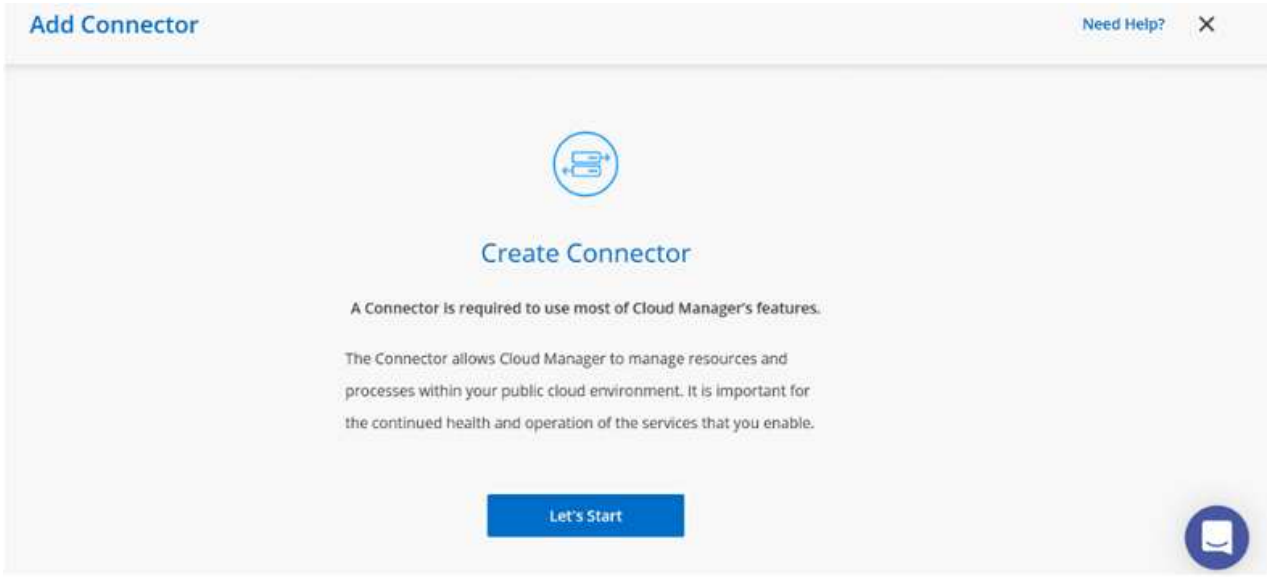
1. 登入NetApp Cloud Central：「Fabric View（架構檢視）」畫面隨即顯示。找到Cloud Volumes ONTAP 「解決方案」索引標籤、然後選取「前往Cloud Manager」。登入之後、便會顯示「畫版」畫面。



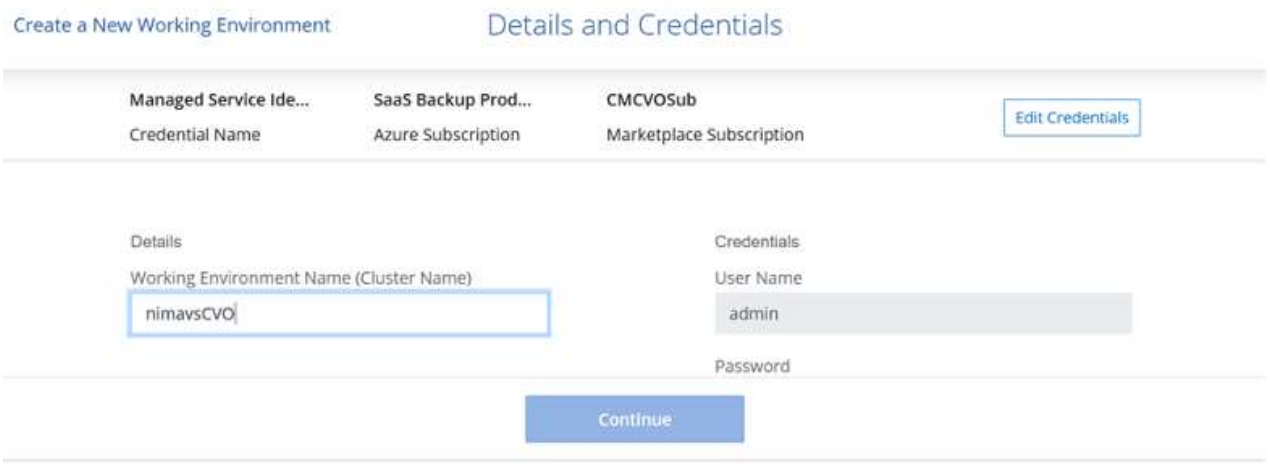
2. 在Cloud Manager首頁上、按一下「Add a Working Environment（新增工作環境）」、然後選取「Microsoft Azure」做為雲端和系統組態類型。



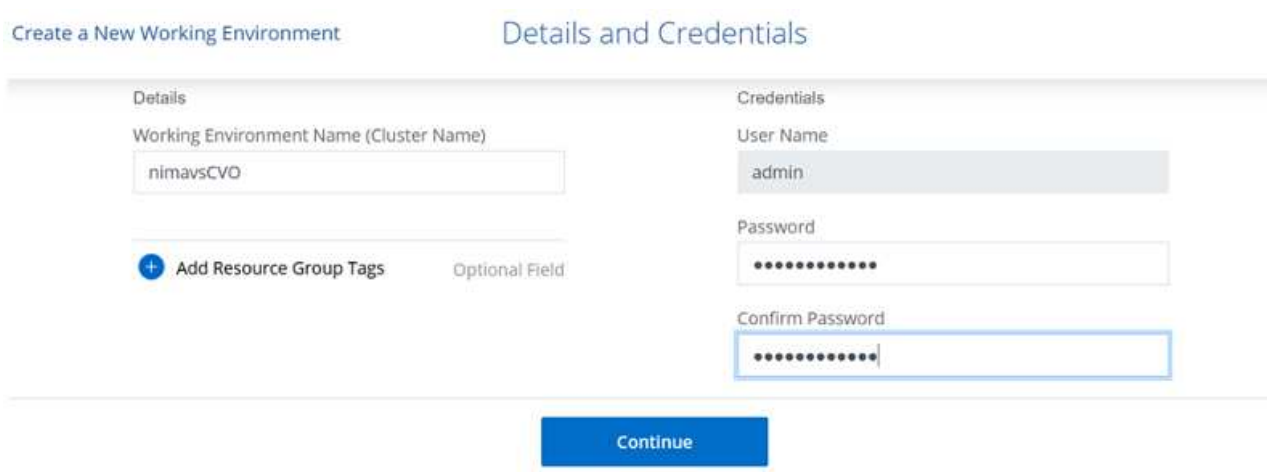
3. 建立第一個Cloud Volumes ONTAP 運作環境時、Cloud Manager會提示您部署Connector。



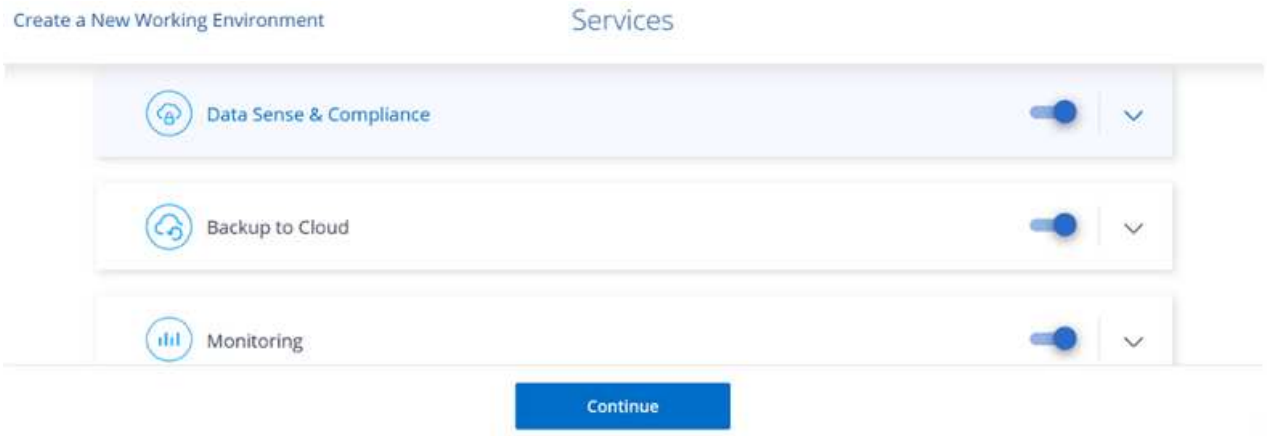
4. 建立連接器之後、請更新詳細資料和認證欄位。



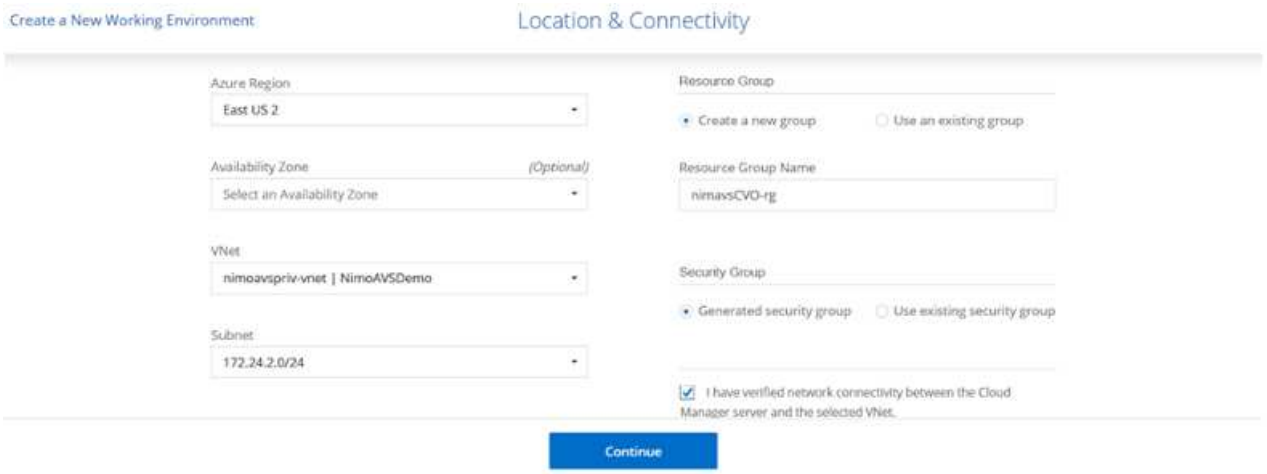
5. 提供要建立的環境詳細資料、包括環境名稱和管理員認證資料。將Azure環境的資源群組標記新增為選用參數。完成後、按一下「Continue（繼續）」。



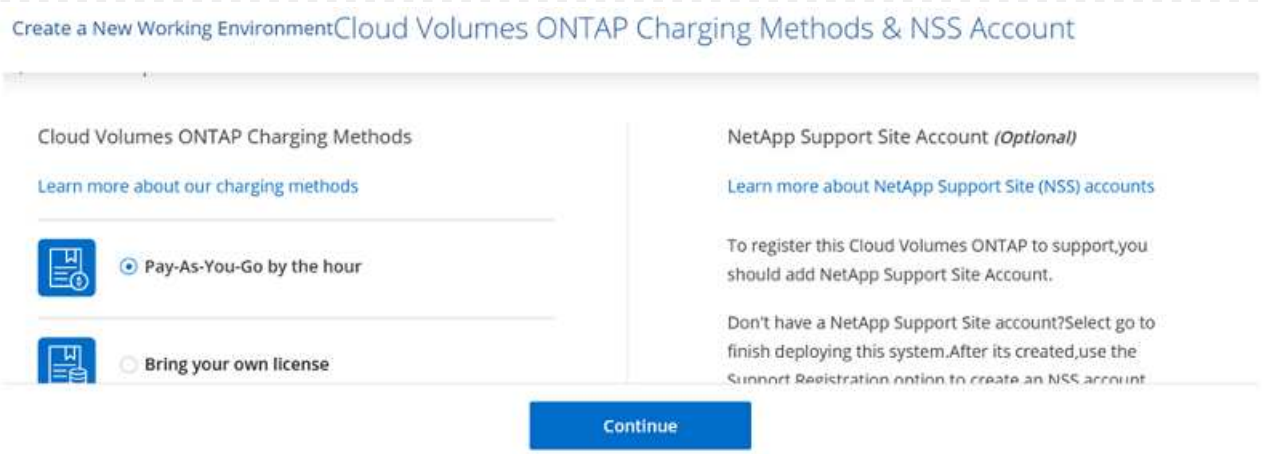
6. 選取 Cloud Volumes ONTAP 部署的附加服務、包括 BlueXP 分類、 BlueXP 備份與還原、以及 Cloud Insights 。選取服務、然後按一下「Continue（繼續）」。



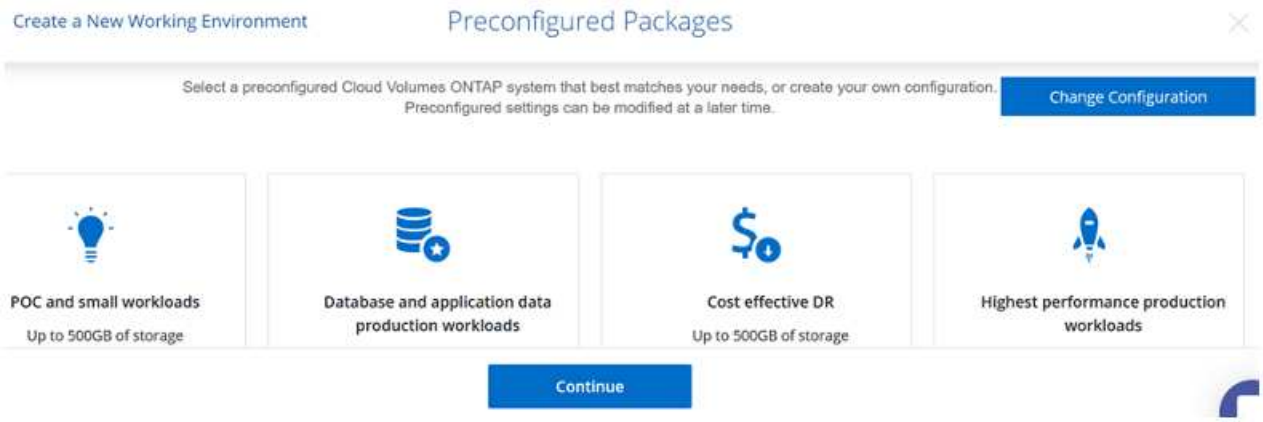
7. 設定Azure位置和連線能力。選取要使用的Azure區域、資源群組、vnet和子網路。



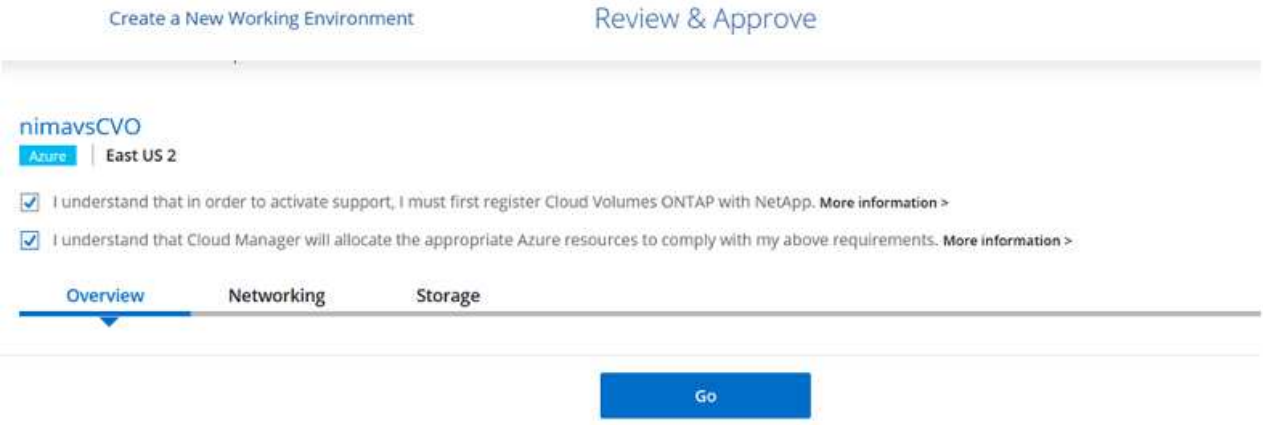
8. 選取使用許可選項：「隨用隨付」或「BYOL」以使用現有的授權。在此範例中、會使用隨用隨付選項。



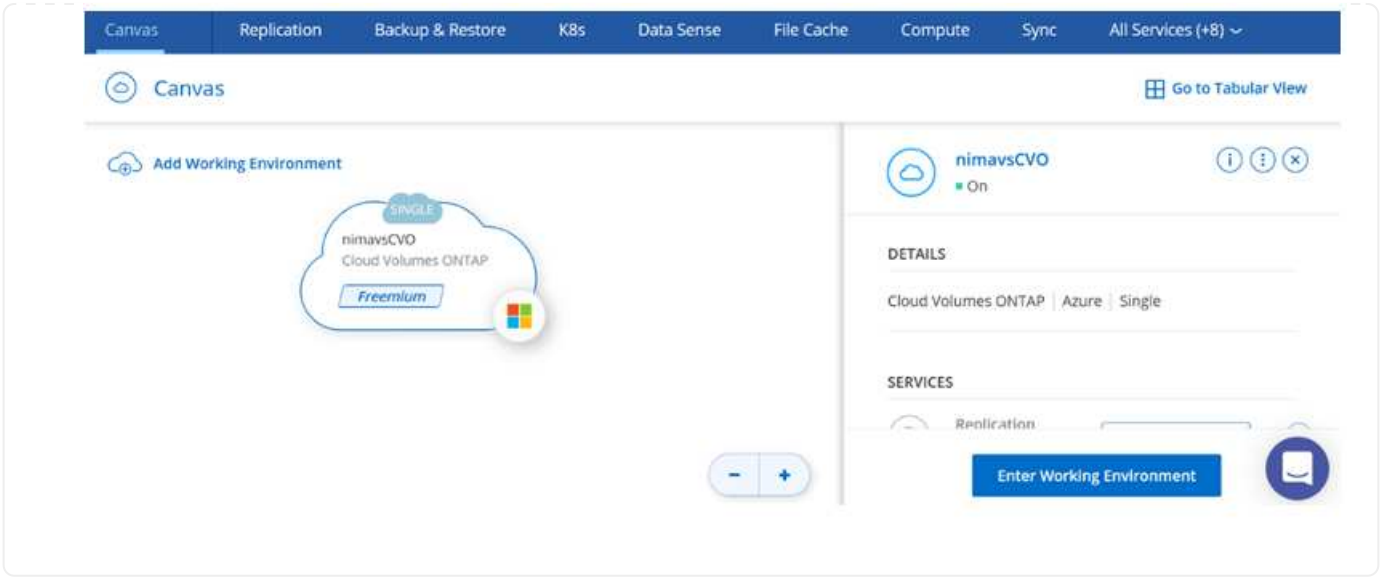
9. 針對各種工作負載類型、可在多個預先設定的套件之間進行選擇。



10. 接受兩項有關啟動Azure資源支援與配置的協議。若要建立Cloud Volumes ONTAP 此解決方案、請按一下「Go（執行）」。

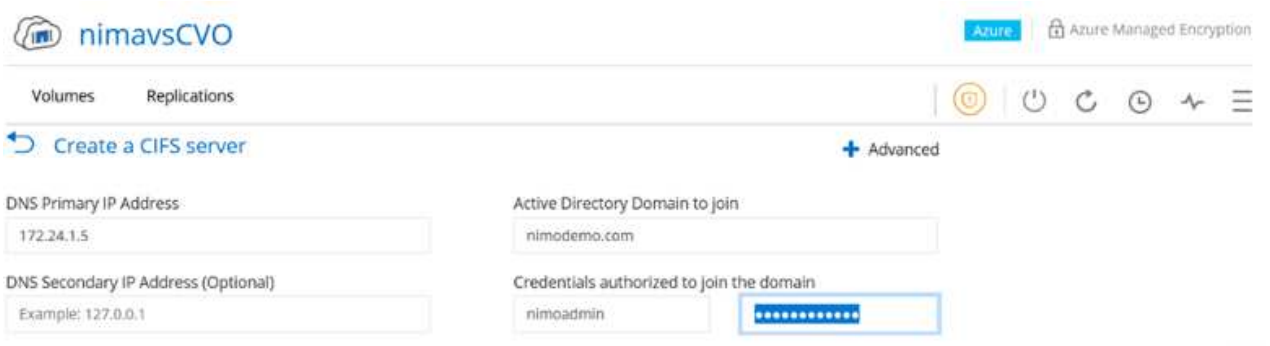


11. 完成供應後、此功能會列在「畫版」頁面上的工作環境中。Cloud Volumes ONTAP

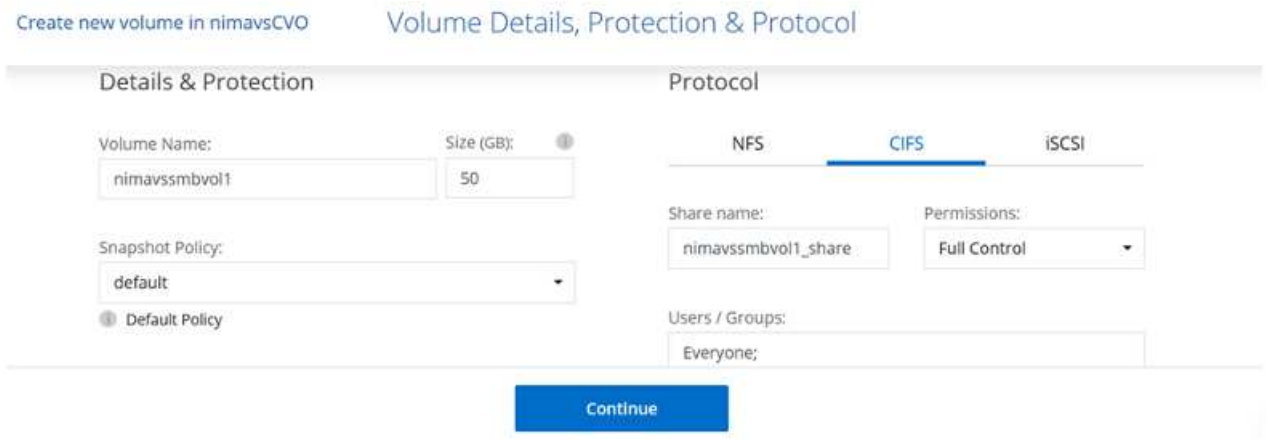

Canvas
Replication
Backup & Restore
K8s
Data Sense
File Cache
Compute
Sync
All Services (+8)
Canvas
Go to Tabular View
Add Working Environment
SINGLE
nimavsCVO
Cloud Volumes ONTAP
Freemium
nimavsCVO
On
DETAILS
Cloud Volumes ONTAP | Azure | Single
SERVICES
Replication
Enter Working Environment

SMB Volume的其他組態

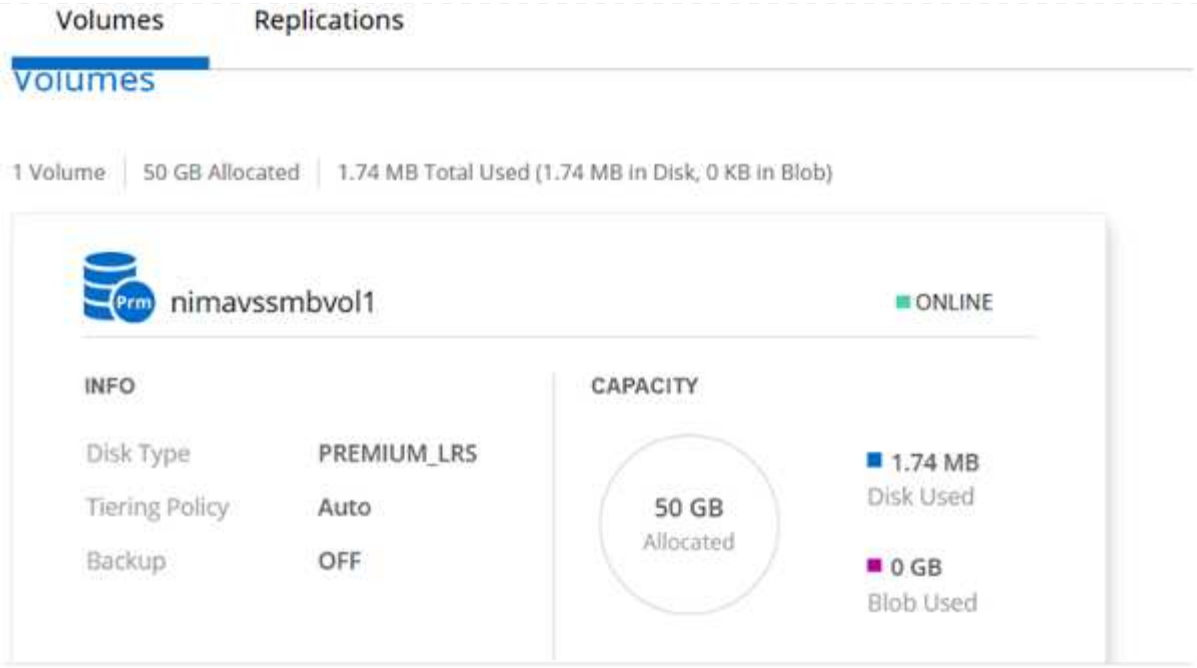
1. 工作環境準備好之後、請確定CIFS伺服器已設定適當的DNS和Active Directory組態參數。您必須先執行此步驟、才能建立SMB Volume。



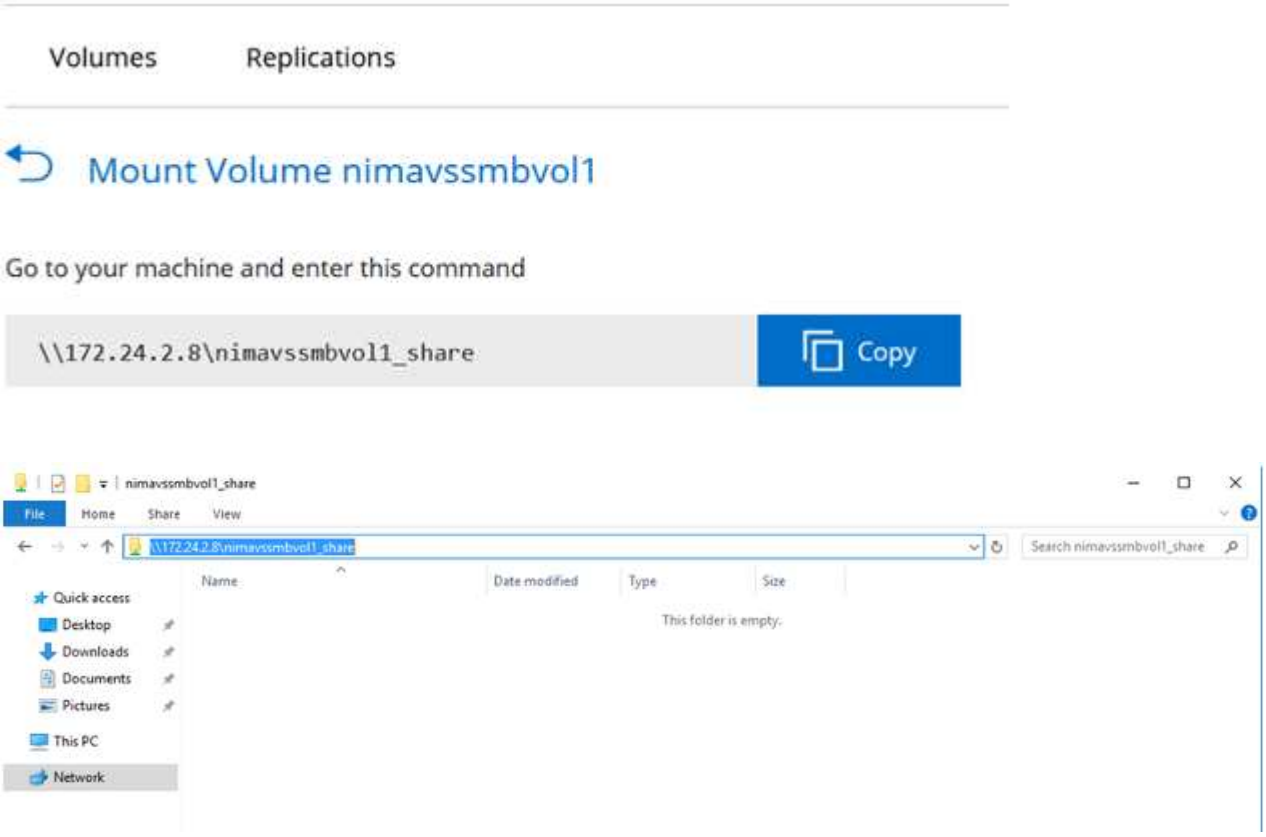
2. 建立SMB Volume是一項簡單的程序。選取CVO執行個體以建立磁碟區、然後按一下Create Volume（建立磁碟區）選項。選擇適當的大小、然後由Cloud Manager選擇內含的Aggregate、或使用進階分配機制將其放置在特定的Aggregate上。在此示範中、SMB被選取為傳輸協定。



3. 在配置磁碟區之後、該磁碟區會出現在「Volumes（磁碟區）」窗格下方。由於CIFS共用區已配置完成、因此請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。如果從內部部署環境複寫磁碟區、則不需要執行此步驟、因為檔案和資料夾權限都會保留為SnapMirror複寫的一部分。

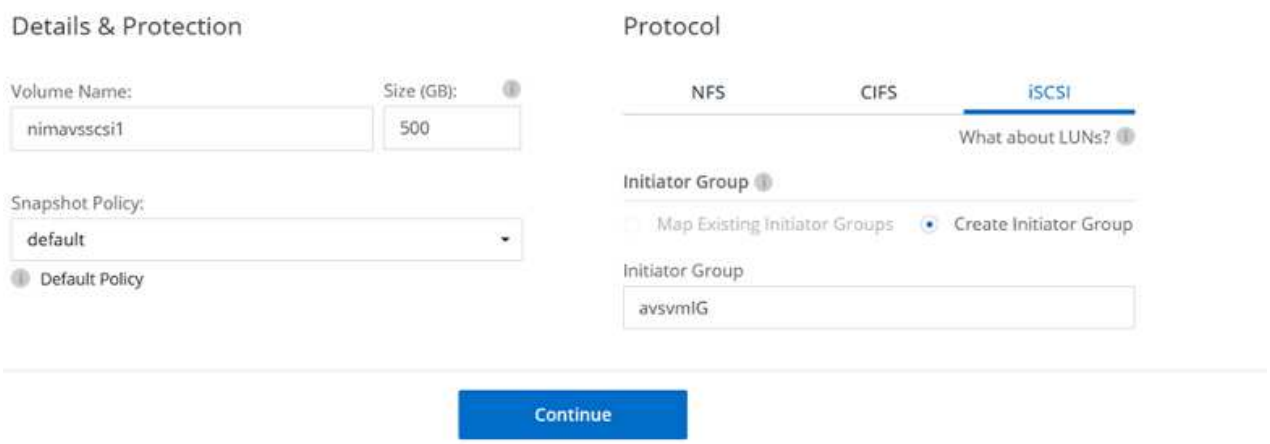


4. 建立磁碟區之後、請使用mount命令、從Azure VMware Solution SDDC主機上執行的VM連線至共用區。
5. 複製下列路徑、然後使用「對應網路磁碟機」選項將磁碟區掛載到執行Azure VMware Solution SDDC的VM上。



若要將LUN連線至主機、請完成下列步驟：

1. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 「功能不全」環境以建立及管理Volume。
2. 按一下「Add Volume（新增Volume）」>「New Volume（新Volume）」、然後選取「iSCSI（iSCSI）」、按一下「繼續」。



3. 配置磁碟區之後、選取磁碟區、然後按一下「Target IQN」。若要複製iSCSI合格名稱（IQN）、請按一下複製。設定從主機到 LUN 的 iSCSI 連線。

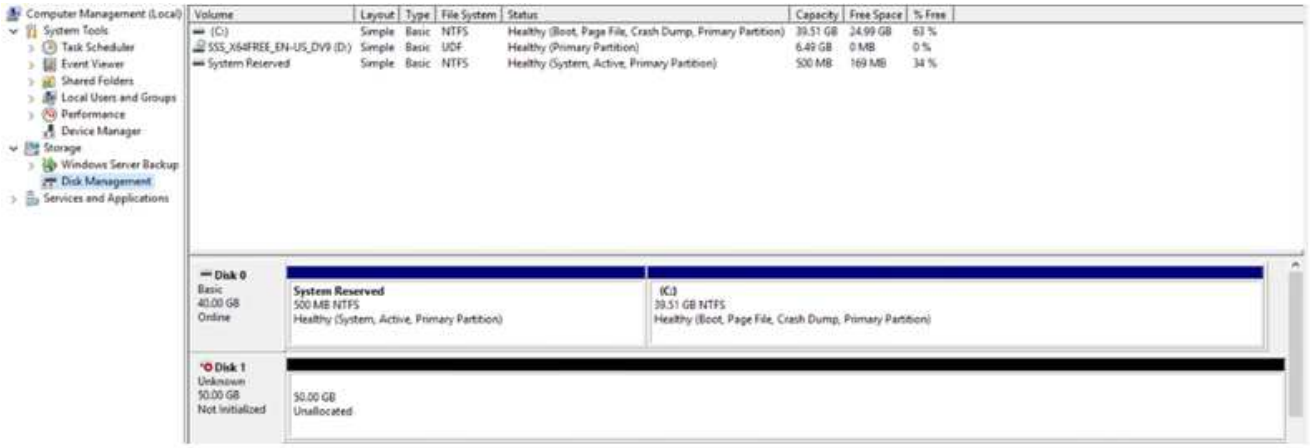
   若要針對駐留在Azure VMware Solution SDDC上的主機達成相同目標：

   a. 將RDP移至Azure VMware Solution SDDC上裝載的VM。
   b. 開啟「iSCSI啟動器內容」對話方塊：「伺服器管理員」>「儀表板」>「工具」>「iSCSI啟動器」。
   c. 在「Discovery（探索）」索引標籤中、按一下「Discover Portal（探索入口網站）」或「Add Portal（新增入口網站）」、然後輸入iSCSI目標連接埠的IP位
   d. 從「目標」索引標籤中選取探索到的目標、然後按一下「登入」或「連線」。
   e. 選取「啟用多重路徑」、然後選取「電腦啟動時自動還原此連線」或「將此連線新增至最愛目標清單」。按一下進階。

      附註： Windows主機必須與叢集中的每個節點建立iSCSI連線。原生DSM會選取最佳路徑。

儲存虛擬機器（SVM）上的LUN會在Windows主機上顯示為磁碟。主機不會自動探索任何新增的磁碟。完成下列步驟、觸發手動重新掃描以探索磁碟：

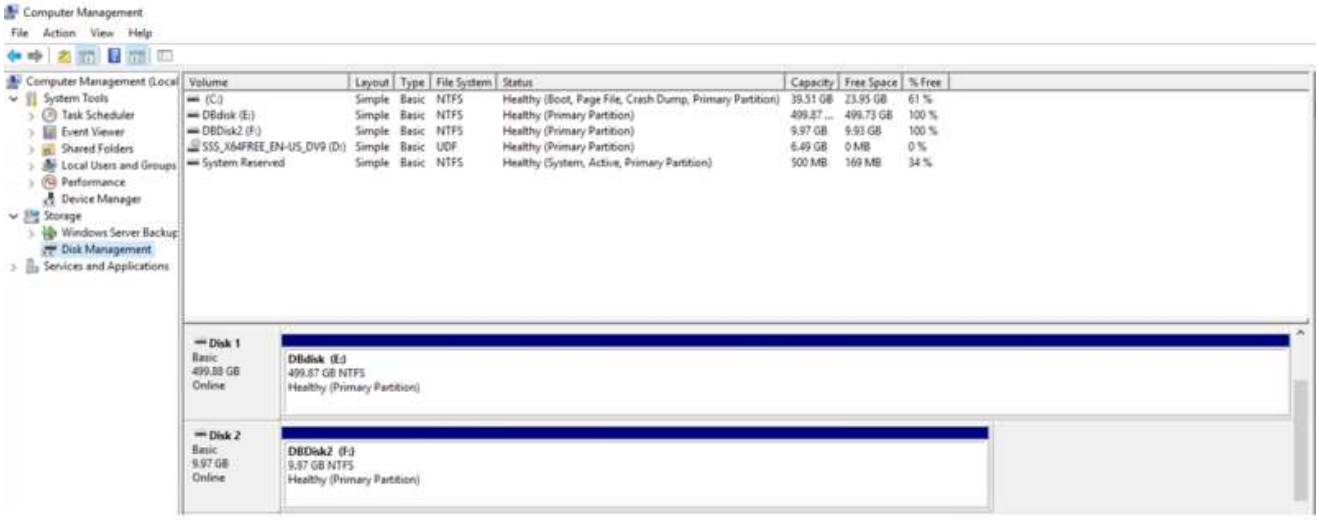
1. 開啟Windows電腦管理公用程式：「開始」>「系統管理工具」>「電腦管理」。
2. 展開導覽樹狀結構中的「Storage（儲存）」節點。
3. 按一下「磁碟管理」。
4. 按一下「行動」>「重新掃描磁碟」。

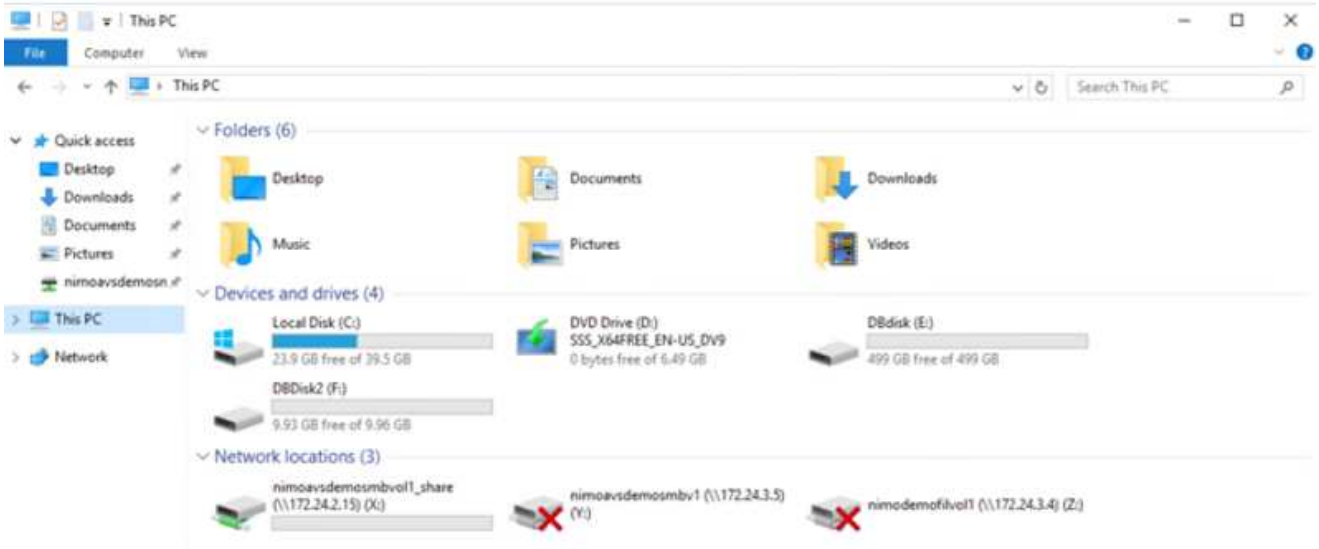


當Windows主機首次存取新LUN時、它沒有分割區或檔案系統。初始化LUN；並可選擇完成下列步驟、以檔案系統格式化LUN：

1. 啟動Windows磁碟管理。

2. 以滑鼠右鍵按一下LUN、然後選取所需的磁碟或磁碟分割類型。
3. 依照精靈中的指示進行。在此範例中、磁碟機E：已掛載



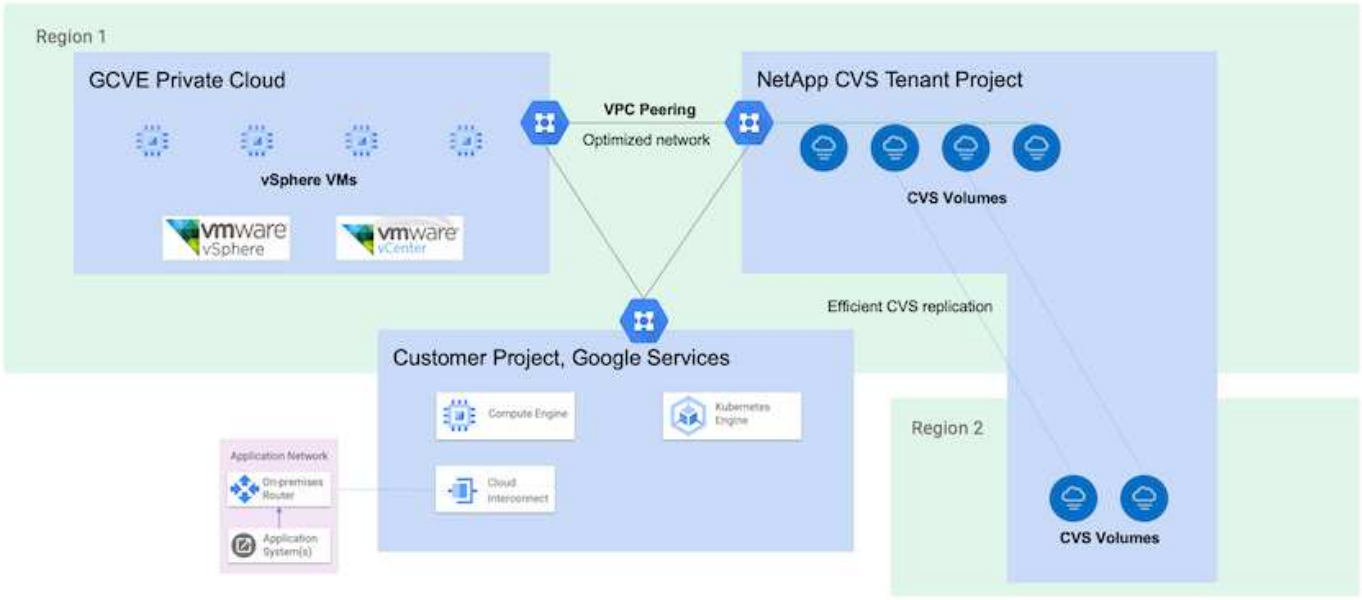


Google Cloud VMware Engine 補充 **NFS** 資料存放區、含 **NetApp** 雲端 **Volume Service**

總覽

作者：NetApp Suresh ThopPay

需要在 Google Cloud VMware Engine （ GCVE ）環境中增加儲存容量的客戶、可以使用 NetApp Cloud Volume Service 來裝載作為補充 NFS 資料存放區。
在 NetApp Cloud Volume Service 上儲存資料可讓客戶在不同地區之間複寫資料、以防止萬用磁碟機發生災難。



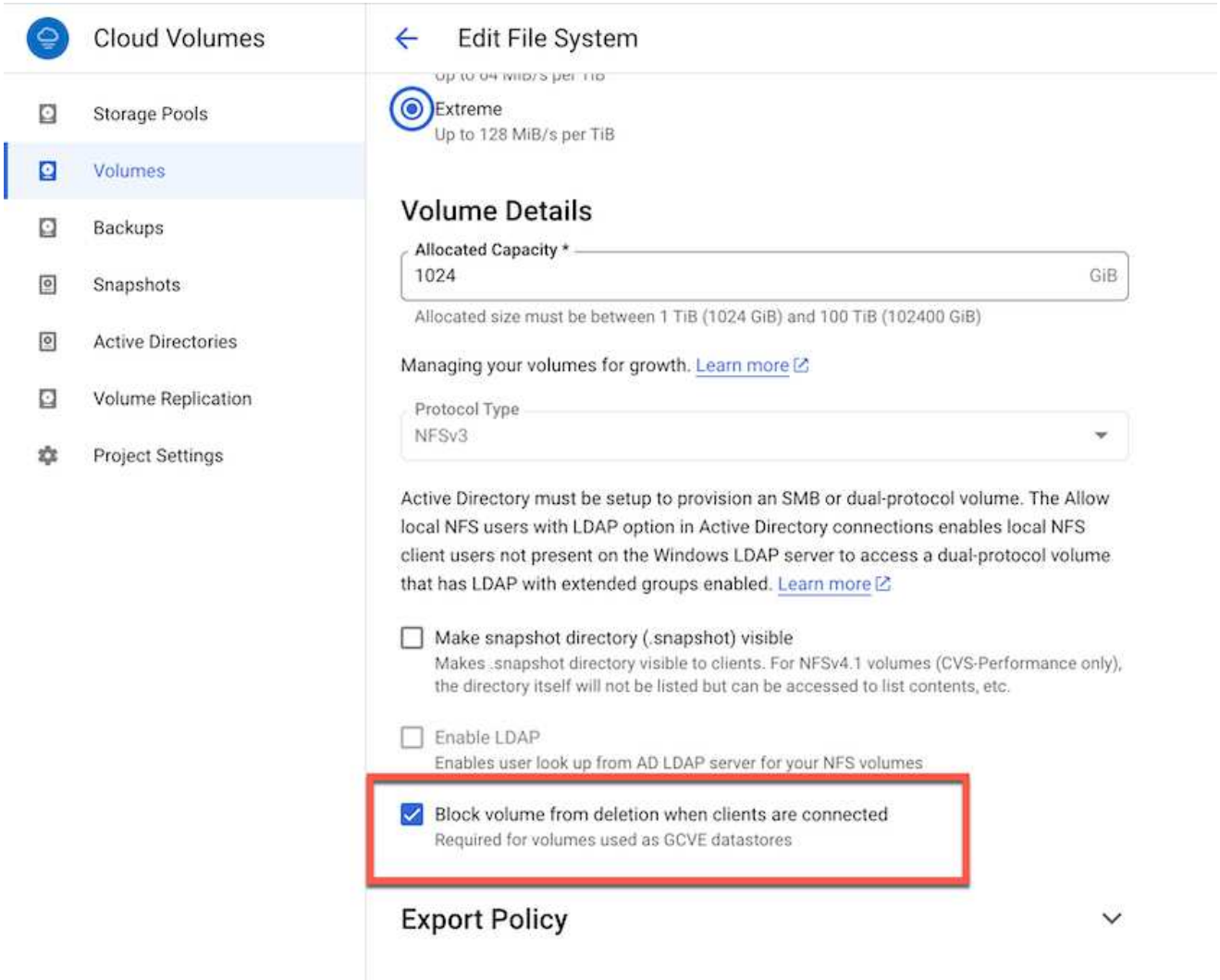
在 **GCVE** 上從 **NetApp CVS** 掛載 **NFS** 資料存放區的部署步驟

配置 **CVS** 效能 **Volume**

NetApp Cloud Volume Service Volume 可以透過進行資源配置
"使用 Google Cloud Console"
"使用 NetApp BlueXP 入口網站或 API"

將 **CVS Volume** 標記為不可刪除的

為了避免在 VM 執行時意外刪除 Volume 、請確保將該 Volume 標示為不可刪除、如下面的螢幕快照所示。



如需詳細資訊、請參閱 "正在建立 NFS Volume" 文件。

確保 **NetApp CVS** 租戶 **VPC** 存在 **GCVE** 上的私有連線。

若要掛載 NFS 資料存放區、 GCVE 與 NetApp CVS 專案之間應該存在私有連線。
如需詳細資訊、請參閱 "如何設定私有服務存取"

掛載 **NFS** 資料存放區

如需如何在 GCVE 上掛載 NFS 資料存放區的指示、請參閱 "如何使用 NetApp CVS 建立 NFS 資料存放區"

由於 vSphere 主機是由 Google 管理、因此您無法安裝 NFS vSphere API for Array Integration （ VAAI ） vSphere 安裝套件（ VIB ）。
如果您需要虛擬磁碟區（ vVol ）支援、請通知我們。
如果您想要使用巨型框架、請參閱 "GCP 上支援的最大 MTU 大小"

利用 **NetApp** 雲端 **Volume Service** 節省成本

若要深入瞭解 NetApp Cloud Volume Service 可為您的 GCVE 儲存需求節省的潛在成本、請查看 "NetApp ROI 計算機"

參考連結

- "Google 部落格：如何使用 NetApp CVS 做為 Google Cloud VMware Engine 的資料存放區"
- "NetApp 部落格：將儲存豐富應用程式移轉至 Google Cloud 的更佳方式"

適用於**GCP**的**NetApp**儲存選項

GCP支援客戶連線的NetApp儲存設備Cloud Volumes ONTAP 搭配使用NetApp功能（CVO）或Cloud Volumes Service 使用支援功能（CVS）。

驗證（**CVO**）**Cloud Volumes ONTAP**

NetApp以NetApp的整套儲存軟體為基礎、是領先業界的雲端資料管理解決方案、原生可在Amazon Web Services（AWS）、Microsoft Azure和Google Cloud Platform（GCP）上使用。Cloud Volumes ONTAP ONTAP

這是ONTAP 由軟體定義的版本、會消耗雲端原生儲存設備、讓您在雲端和內部環境中擁有相同的儲存軟體、減少重新訓練IT人員以全新方法管理資料的需求。

CVO讓客戶能夠無縫地將資料從邊緣移至資料中心、移至雲端和移回、將混合式雲端整合在一起、所有這些都是透過單一窗格管理主控台NetApp Cloud Manager進行管理。

根據設計、CVO提供極致效能和進階資料管理功能、即使是雲端最嚴苛的應用程式、也能輕鬆滿足需求

以客體連線儲存設備形式提供的資訊（**CVO**）**Cloud Volumes ONTAP**

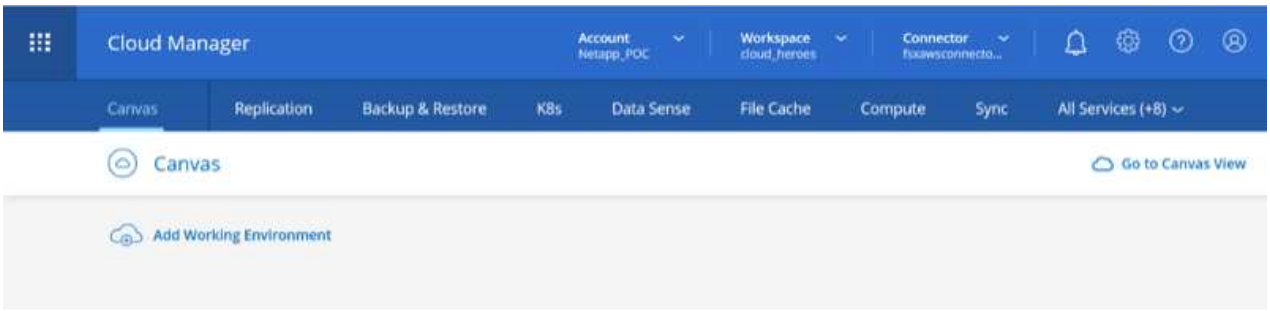
在Cloud Volumes ONTAP Google Cloud部署功能（自行部署）

可從GCVM私有雲端環境中建立的VM掛載支援資源和LUN。Cloud Volumes ONTAP這些磁碟區也可掛載於Linux用戶端、Windows用戶端和LUN、在透過iSCSI掛載時、可在Linux或Windows用戶端上作為區塊裝置存取、因為Cloud Volumes ONTAP 此功能支援iSCSI、SMB及NFS傳輸協定。只需幾個簡單步驟、即可設定各個資料區。Cloud Volumes ONTAP

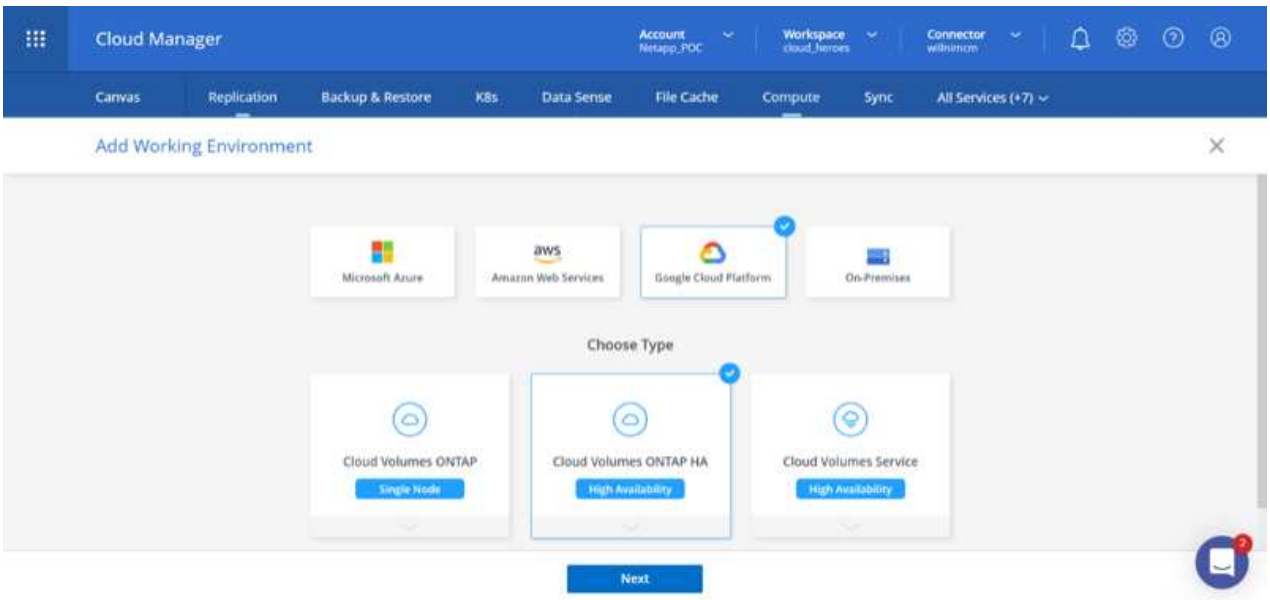
若要將磁碟區從內部部署環境複寫至雲端、以進行災難恢復或移轉、請使用站台對站台VPN或雲端互連、建立與Google Cloud的網路連線。將內部部署的資料複寫到Cloud Volumes ONTAP 內部部署的不適用範圍。若要在內部部署Cloud Volumes ONTAP 和不間斷系統之間複寫資料、請參閱 xref:./ehc/"設定系統之間的資料複寫"。

使用 "Szizer Cloud Volumes ONTAP" 以準確調整Cloud Volumes ONTAP 實體執行個體的大小。同時監控內部部署的效能、以做Cloud Volumes ONTAP 為VMware內部資料的輸入。

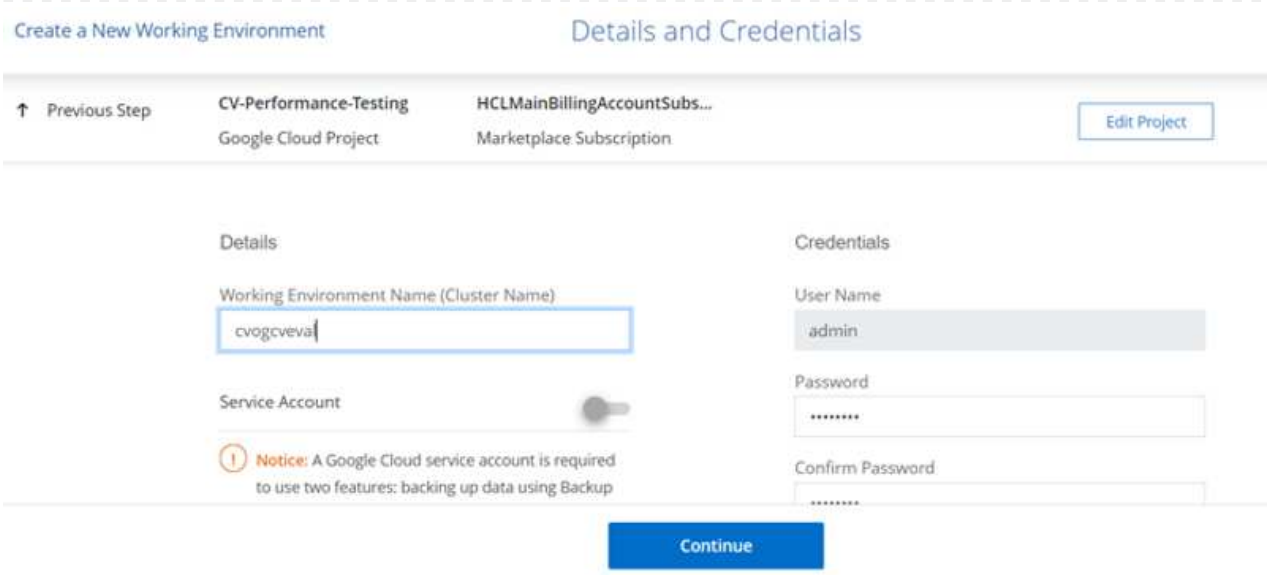
1. 登入NetApp Cloud Central：「Fabric View（架構檢視）」畫面隨即顯示。找到Cloud Volumes ONTAP 「解決方案」索引標籤、然後選取「前往Cloud Manager」。登入之後、便會顯示「畫版」畫面。



2. 在Cloud Manager的「CanvasTM」索引標籤上、按一下「Add a Working Environment（新增工作環境）」、然後選取「Google Cloud Platform（Google Cloud Platform）」做為雲端和系統組態類型。然後按「Next（下一步）」。

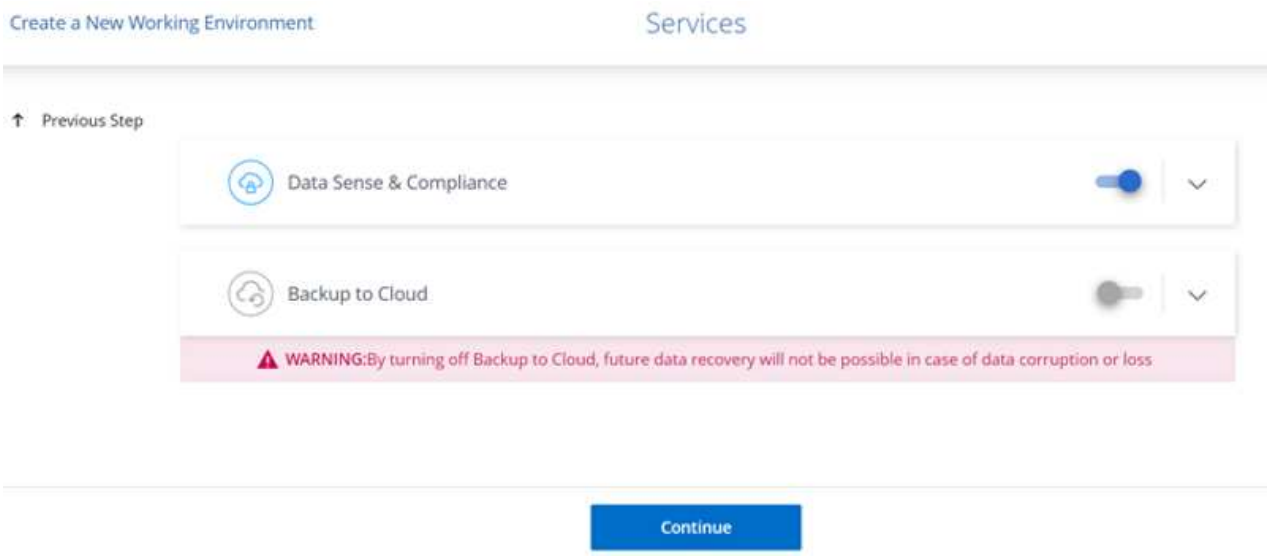


3. 提供要建立的環境詳細資料、包括環境名稱和管理員認證資料。完成後、按一下「Continue（繼續）」。

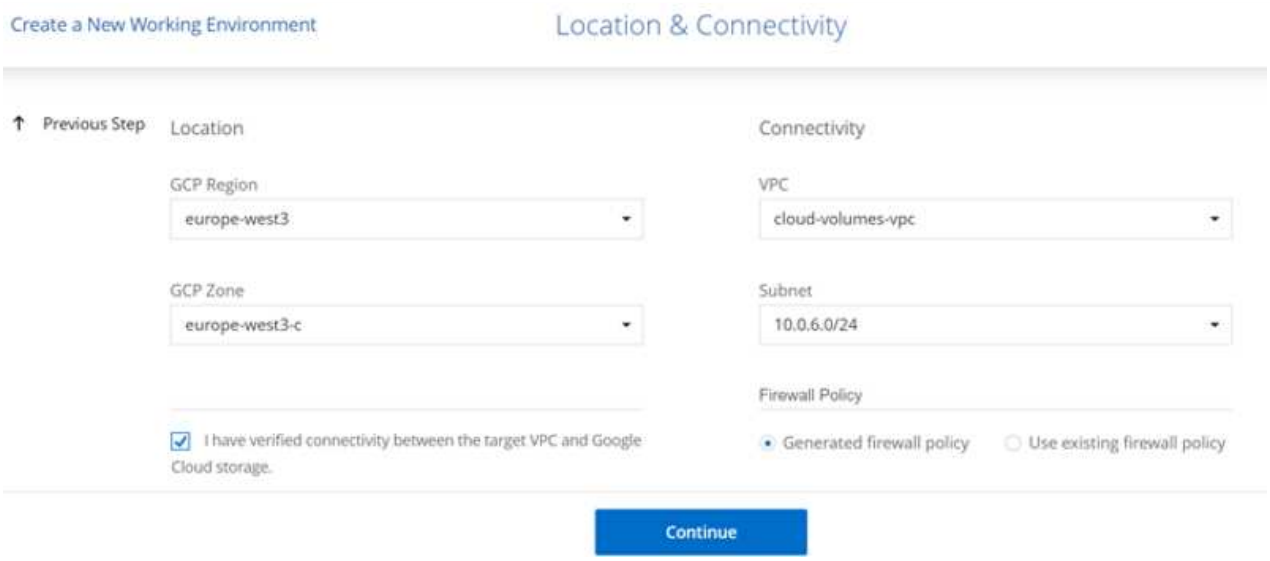


4. 選取或取消選取Cloud Volumes ONTAP 適用於不支援的部署附加服務、包括Data Sense & Compliance或Backup to Cloud。然後按一下「Continue（繼續）」。

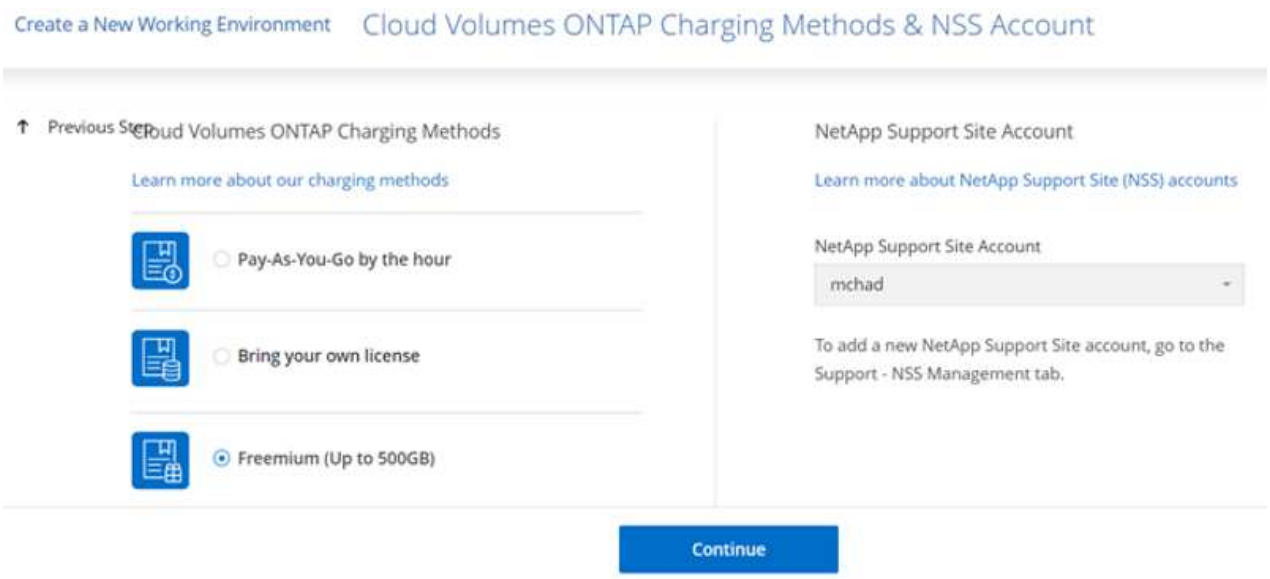
   提示：停用附加服務時、會顯示驗證快顯訊息。在CVO部署之後、可新增/移除附加服務、如果不需要、請考慮取消選取附加服務、以避免成本。



5. 選取位置、選擇防火牆原則、然後選取核取方塊以確認網路連線至Google Cloud儲存設備。

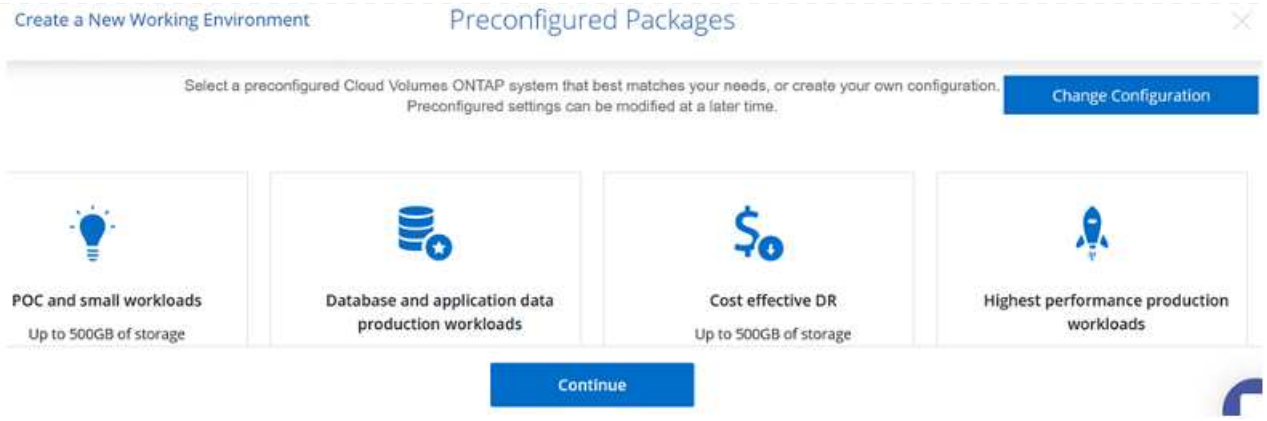


6. 選取使用許可選項：「隨用隨付」或「BYOL」以使用現有的授權。在此範例中、會使用Freemium選項。然後按一下「Continue（繼續）」。

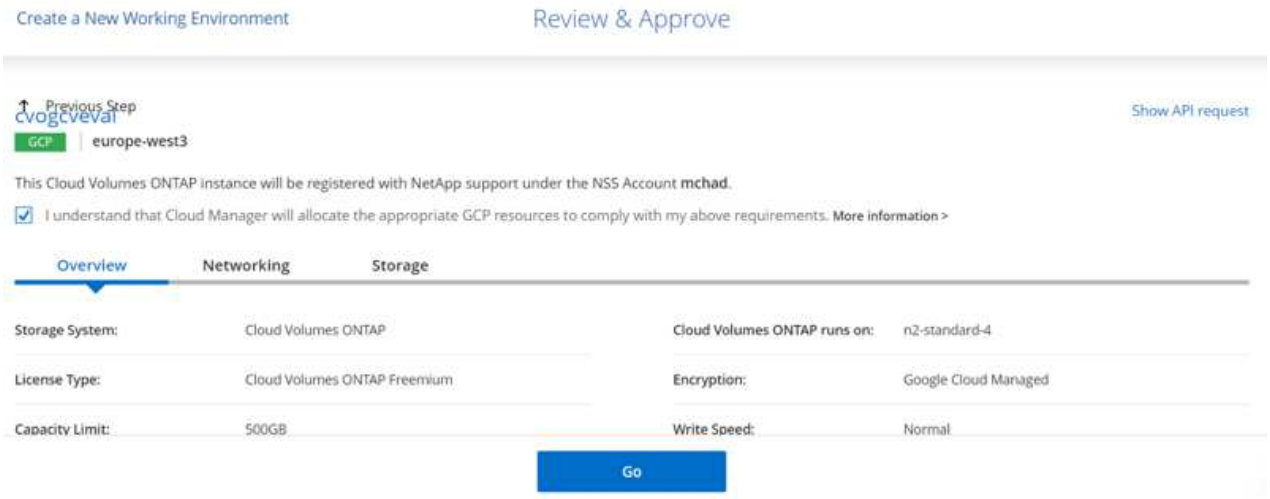


7. 根據將部署在AWS SDDC上VMware雲端上的VM上的工作負載類型、選擇幾個預先設定的套件。

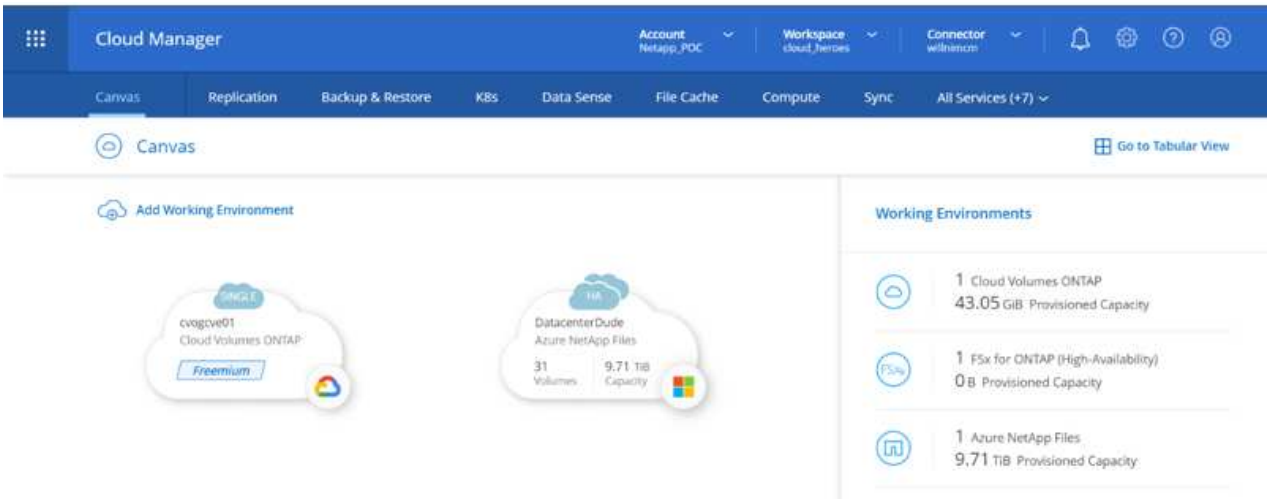
   提示：按ONTAP 一下「Change Configuration（變更組態）」、將滑鼠移到方塊上以取得詳細資料、或自訂CVO元件和版本。



8. 在「Review & Approve（檢閱與核准）」頁面上、檢閱並確認所做的選擇。若要建立Cloud Volumes ONTAP 此實例、請按一下「Go（執行）」。



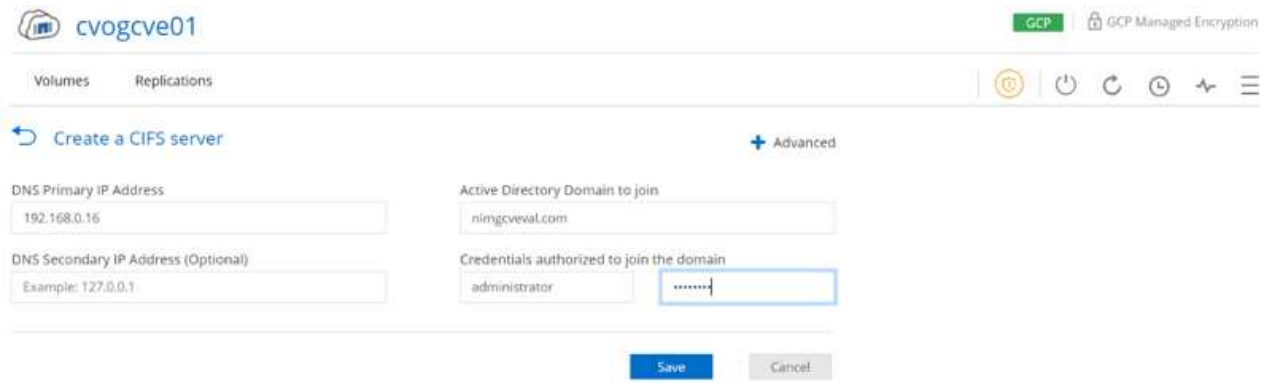
9. 完成供應後、此功能會列在「畫版」頁面上的工作環境中。Cloud Volumes ONTAP



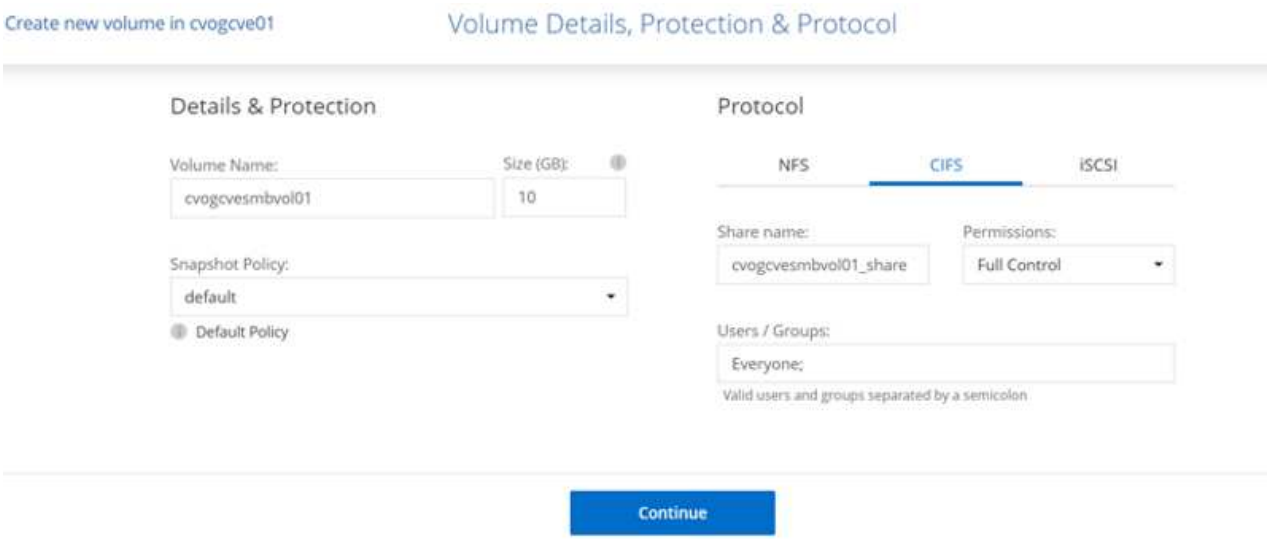
SMB Volume的其他組態

1. 工作環境準備好之後、請確定CIFS伺服器已設定適當的DNS和Active Directory組態參數。您必須先執行此步驟、才能建立SMB Volume。

   提示：按一下「Menu（功能表）」圖示（o）、選取「Advanced（進階）」以顯示更多選項、然後選取「CIFS setup（CIFS設定）」。



2. 建立SMB Volume是一項簡單的程序。在畫版中、按兩下Cloud Volumes ONTAP 執行作業的環境以建立及管理磁碟區、然後按一下「Create Volume（建立磁碟區）」選項。選擇適當的大小、然後由Cloud Manager選擇內含的Aggregate、或使用進階分配機制將其放置在特定的Aggregate上。在此示範中、CIFS/SMB被選取為傳輸協定。

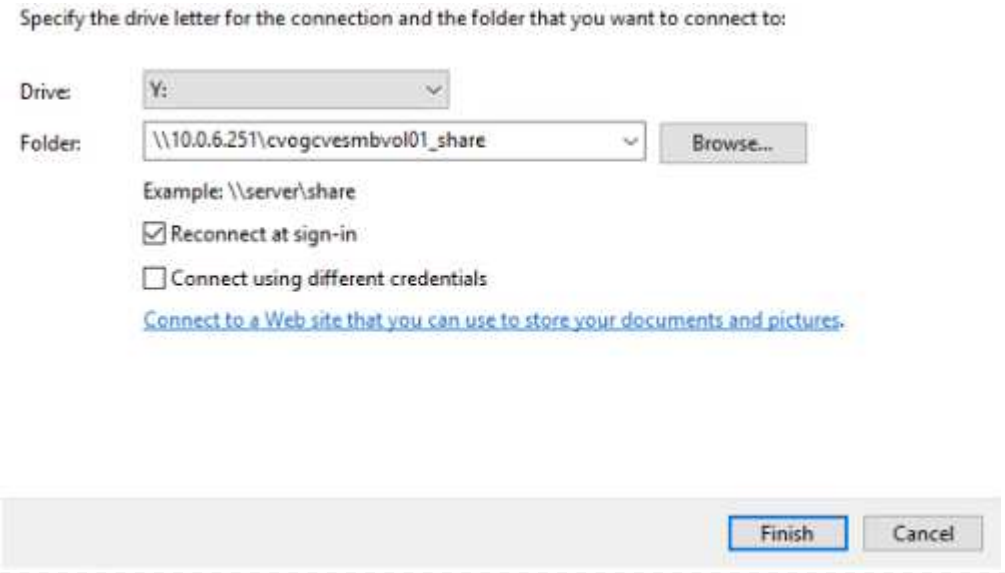


3. 在配置磁碟區之後、該磁碟區會出現在「Volumes（磁碟區）」窗格下方。由於CIFS共用區已配置完成、因此請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。如果從內部部署環境複寫磁碟區、則不需要執行此步驟、因為檔案和資料夾權限都會保留為SnapMirror複寫的一部分。

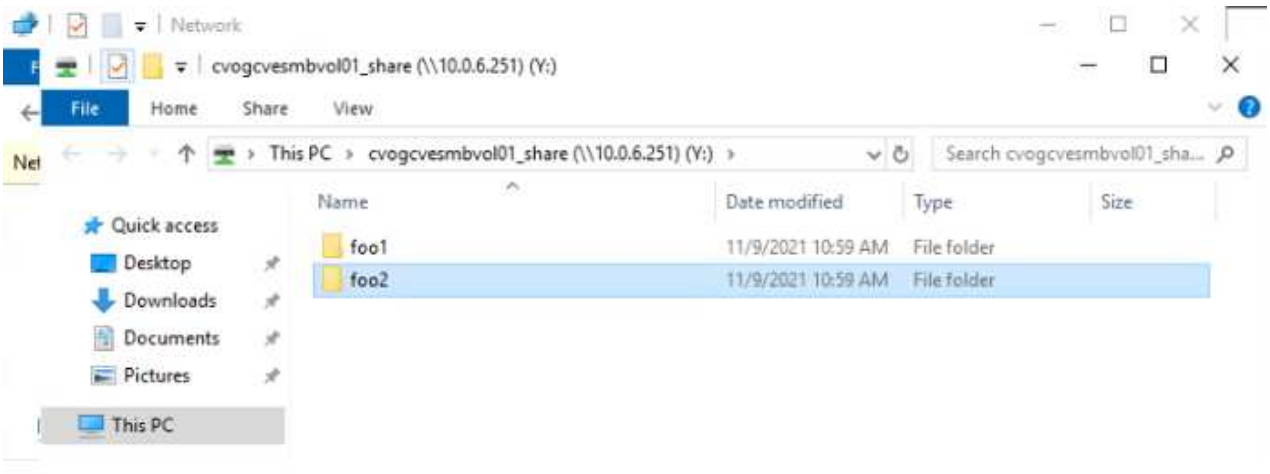
   提示：按一下Volume功能表（o）以顯示其選項。

4. 建立磁碟區之後、請使用mount命令顯示磁碟區連線指示、然後從Google Cloud VMware Engine上的VM連線至共用區。

5. 複製下列路徑、然後使用「對應網路磁碟機」選項、在Google Cloud VMware Engine上執行的VM上掛載磁碟區。



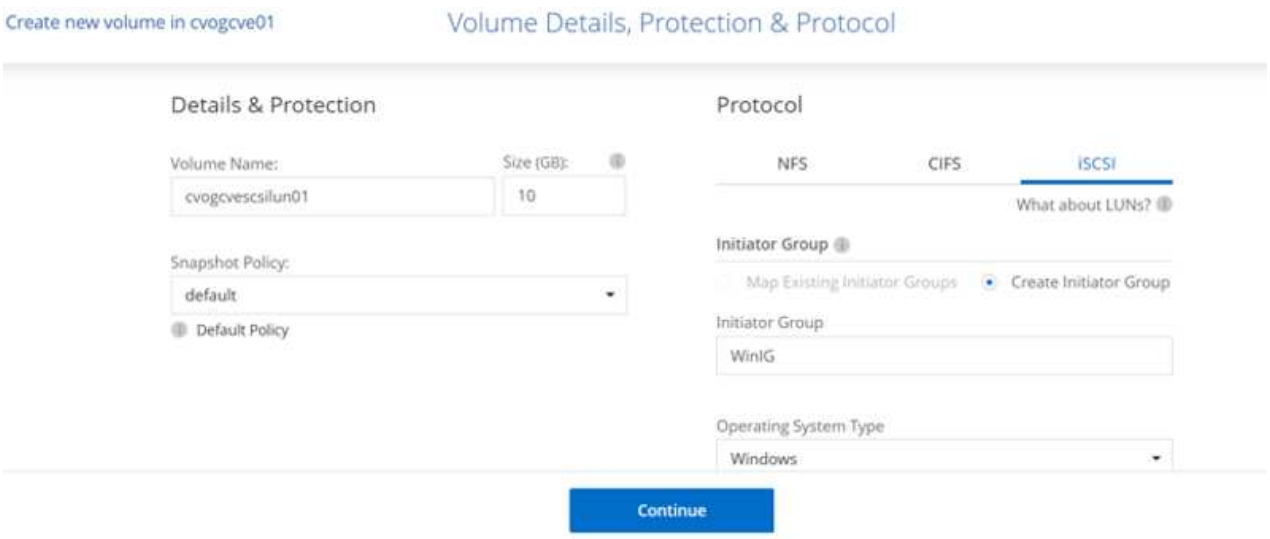
一旦完成對應、就能輕鬆存取、並據此設定NTFS權限。

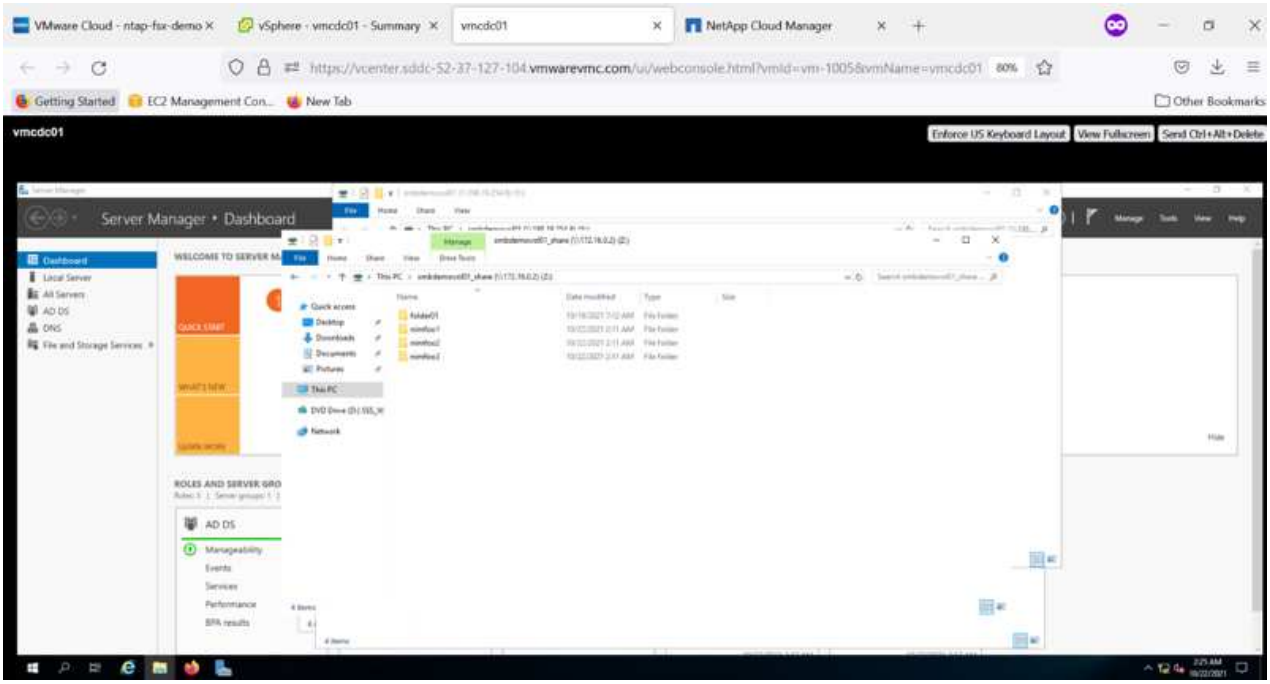


將Cloud Volumes ONTAP 支援的LUN連接到主機

若要將Cloud Volumes ONTAP LUN連接至主機、請完成下列步驟：

1. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 「功能不全」環境以建立及管理Volume。
2. 按一下「Add Volume（新增Volume）」>「New Volume（新Volume）」、然後選取「iSCSI（iSCSI）」、按一下「繼續」。





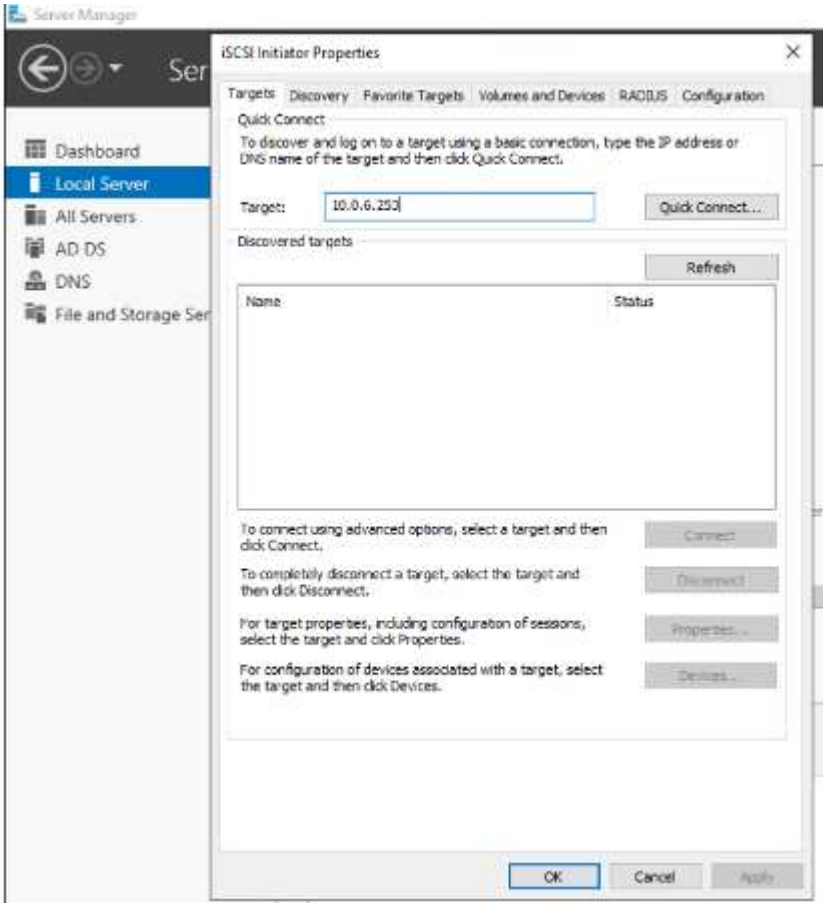
3. 配置磁碟區後、選取Volume（Volume）功能表（o）、然後按一下Target IQN。若要複製iSCSI合格名稱（IQN）、請按一下複製。設定從主機到 LUN 的 iSCSI 連線。

若要針對位於Google Cloud VMware Engine上的主機達成相同的目標：

1. 從RDP移至Google Cloud VMware Engine上裝載的VM。
2. 開啟「iSCSI啟動器內容」對話方塊：「伺服器管理員」>「儀表板」>「工具」>「iSCSI啟動器」。

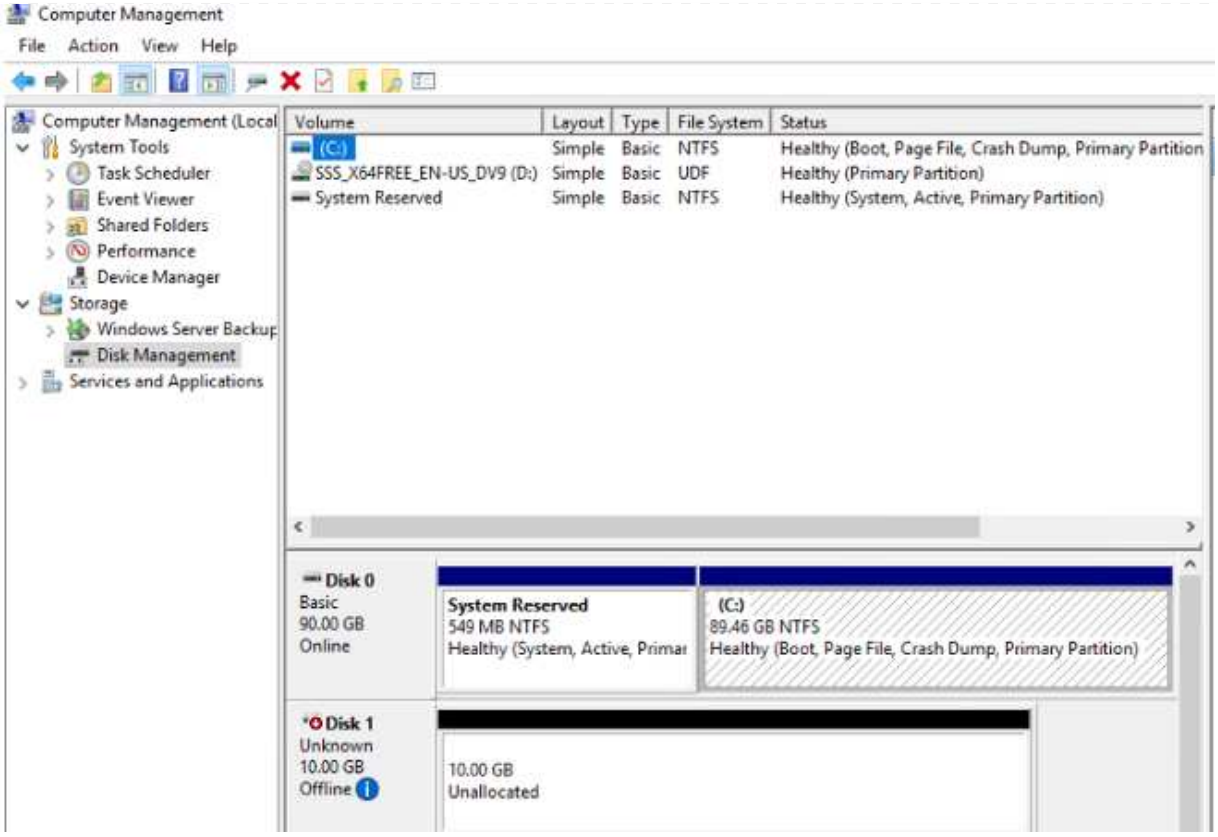
3. 在「Discovery（探索）」索引標籤中、按一下「Discover Portal（探索入口網站）」或「Add Portal（新增入口網站）」、然後輸入iSCSI目標連接埠的IP位
4. 從「目標」索引標籤中選取探索到的目標、然後按一下「登入」或「連線」。
5. 選取「啟用多重路徑」、然後選取「電腦啟動時自動還原此連線」或「將此連線新增至最愛目標清單」。按一下進階。

Windows主機必須與叢集中的每個節點建立iSCSI連線。原生DSM會選取最佳路徑。



儲存虛擬機器（SVM）上的LUN會在Windows主機上顯示為磁碟。主機不會自動探索任何新增的磁碟。完成下列步驟、觸發手動重新掃描以探索磁碟：

a. 開啟Windows電腦管理公用程式：「開始」>「系統管理工具」>「電腦管理」。
b. 展開導覽樹狀結構中的「Storage（儲存）」節點。
c. 按一下「磁碟管理」。
d. 按一下「行動」>「重新掃描磁碟」。

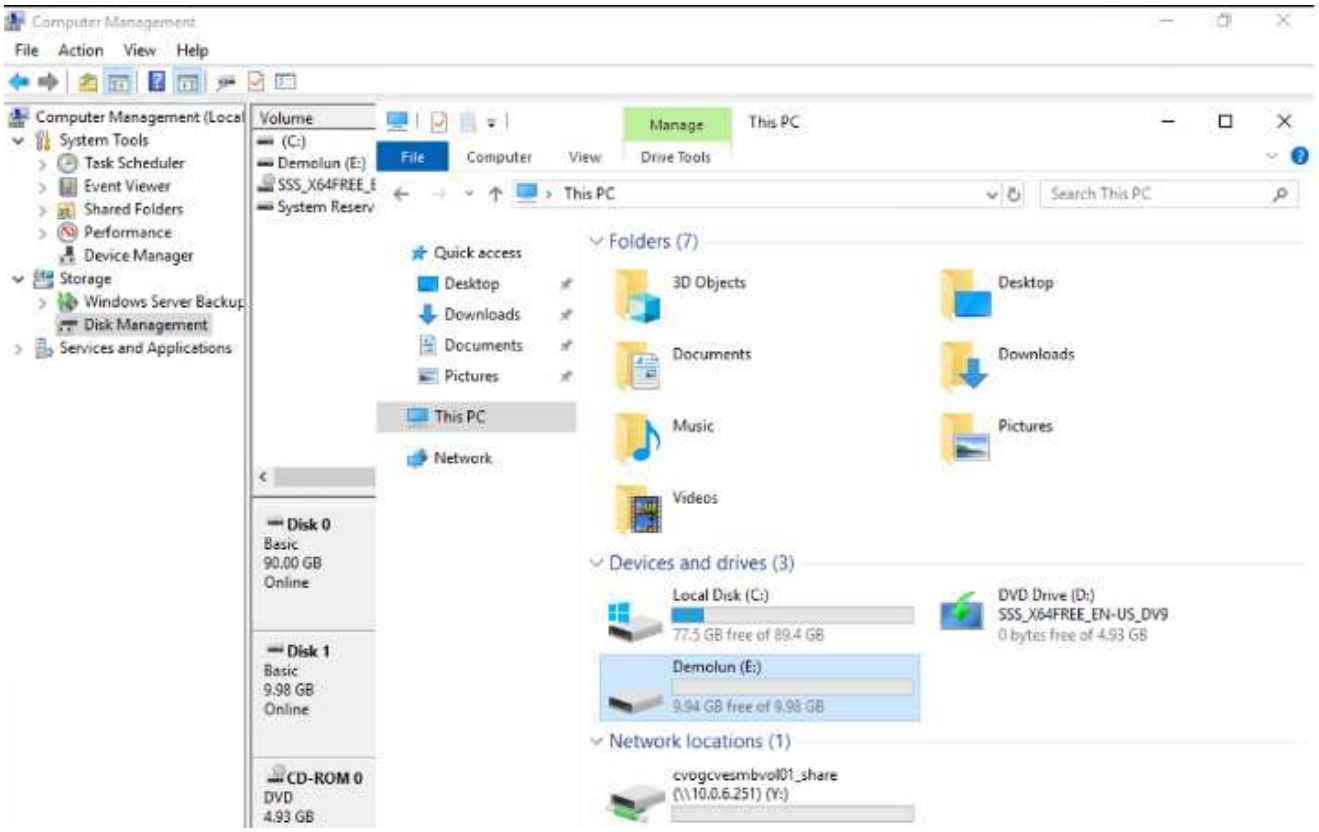


當Windows主機首次存取新LUN時、它沒有分割區或檔案系統。初始化LUN；並可選擇完成下列步驟、以檔案系統格式化LUN：

a. 啟動Windows磁碟管理。

b. 以滑鼠右鍵按一下LUN、然後選取所需的磁碟或磁碟分割類型。

c. 依照精靈中的指示進行。在此範例中、磁碟機F：已掛載。



在Linux用戶端上、確定iSCSI精靈正在執行。配置LUN後、請參閱此處的詳細指南、瞭解如何使用Ubuntu進行iSCSI組態設定。若要驗證、請從Shell執行lsblk cmd。

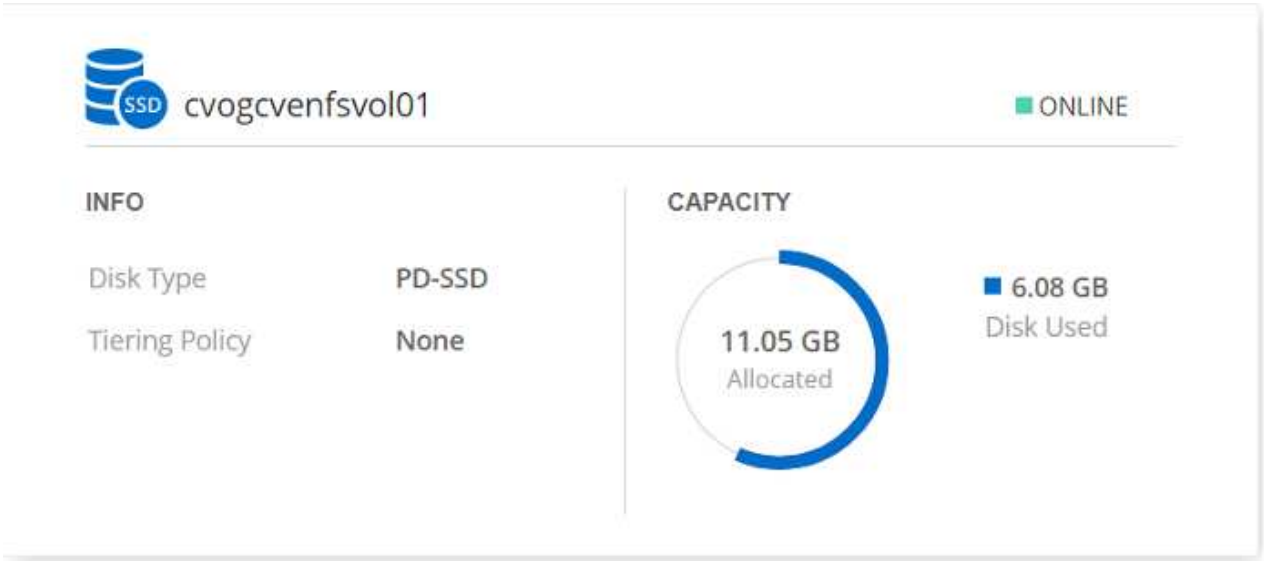
```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    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
niyaz@nimubu01:~$ 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Cloud Volumes ONTAP Linux用戶端上掛載不只是NFS磁碟區

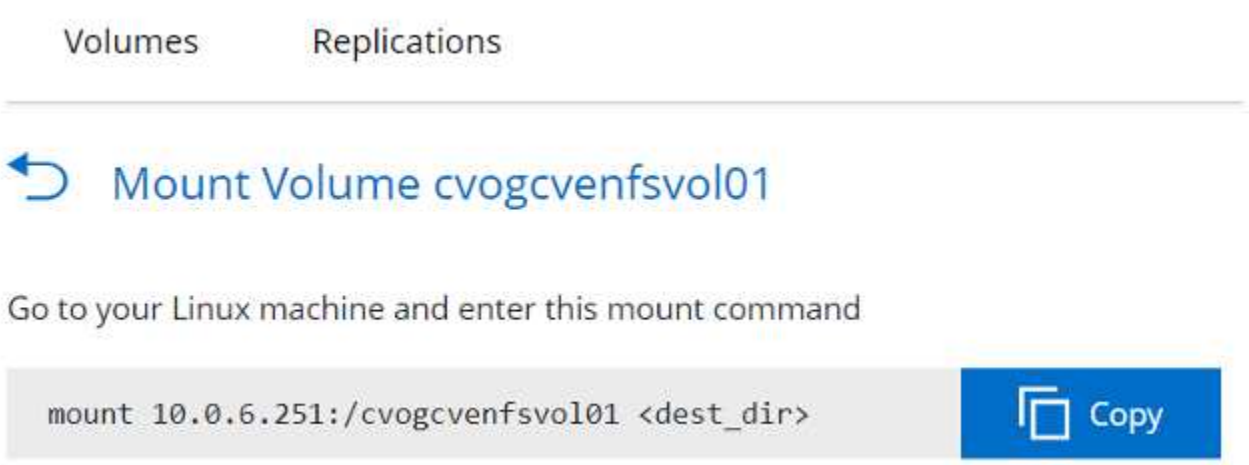
若要從Cloud Volumes ONTAP Google Cloud VMware Engine內的VM掛載支援（DIY）檔案系統、請依照下列步驟進行：

請依照下列步驟配置Volume

1. 按一下「Volumes（磁碟區）」索引標籤中的「Create New Volume
2. 在「Create New Volume」（建立新磁碟區）頁面上、選取一個磁碟區類型：



3. 在「Volumes（磁碟區）」索引標籤中、將滑鼠游標放在磁碟區上、選取功能表圖示（o）、然後按一下「Mount Command（掛載命令）」。



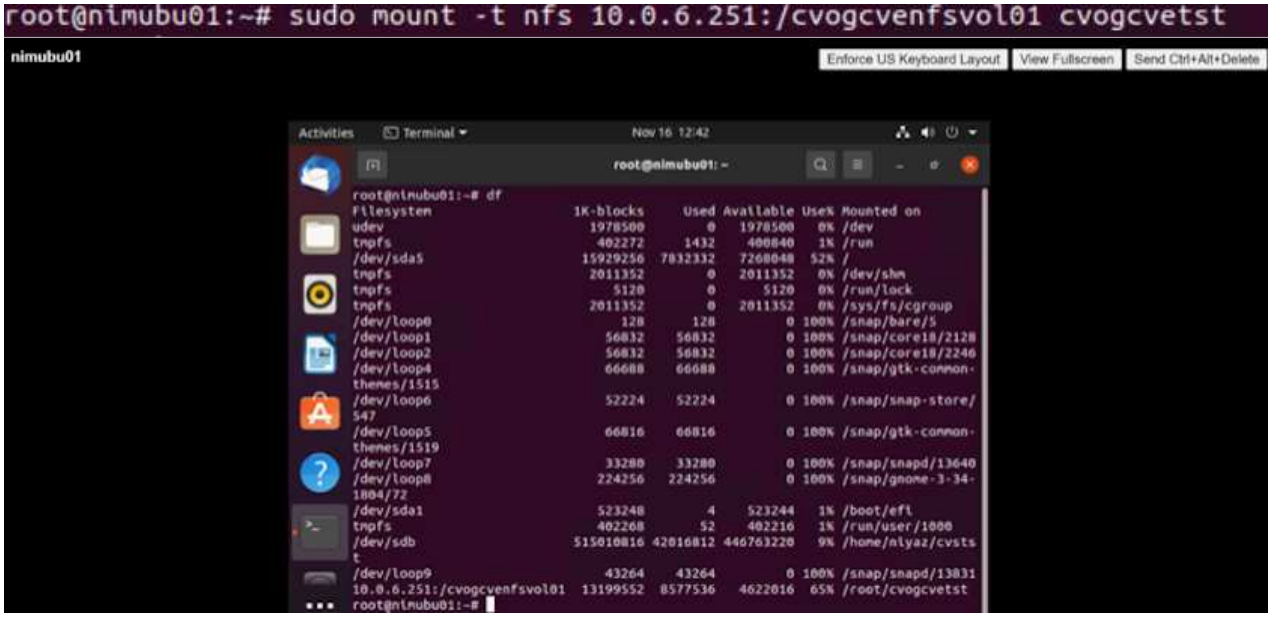
4. 按一下複製。
5. 連線至指定的Linux執行個體。
6. 使用安全Shell（SSH）開啟執行個體上的終端機、然後以適當的認證登入。
7. 使用下列命令建立磁碟區掛載點的目錄。

```
$ sudo mkdir /cvogcvetst
```

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

8. 將Cloud Volumes ONTAP 流通NFS磁碟區掛載到上一步建立的目錄。

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



CVS（CVS）Cloud Volumes Service

Cloud Volumes Services（CVS）是一套完整的資料服務產品組合、可提供進階雲端解決方案。Cloud Volumes Services支援主要雲端供應商的多種檔案存取傳輸協定（NFS和SMB支援）。

其他優點與功能包括：使用Snapshot保護資料與還原；在內部部署或雲端上複寫、同步及移轉資料目的地的特殊功能；以及在專屬Flash儲存系統層級上提供一致的高效能。

以客體連線儲存設備的形式提供資訊（CVS）Cloud Volumes Service

使用Cloud Volumes Service VMware Engine設定功能

可從VMware Engine環境中建立的VM掛載支援資源。Cloud Volumes Service由於Cloud Volumes Service支援SMB和NFS傳輸協定、因此也可以在Linux用戶端上掛載磁碟區並對應至Windows用戶端。只需簡單的步驟即可設定各個資料區。Cloud Volumes Service

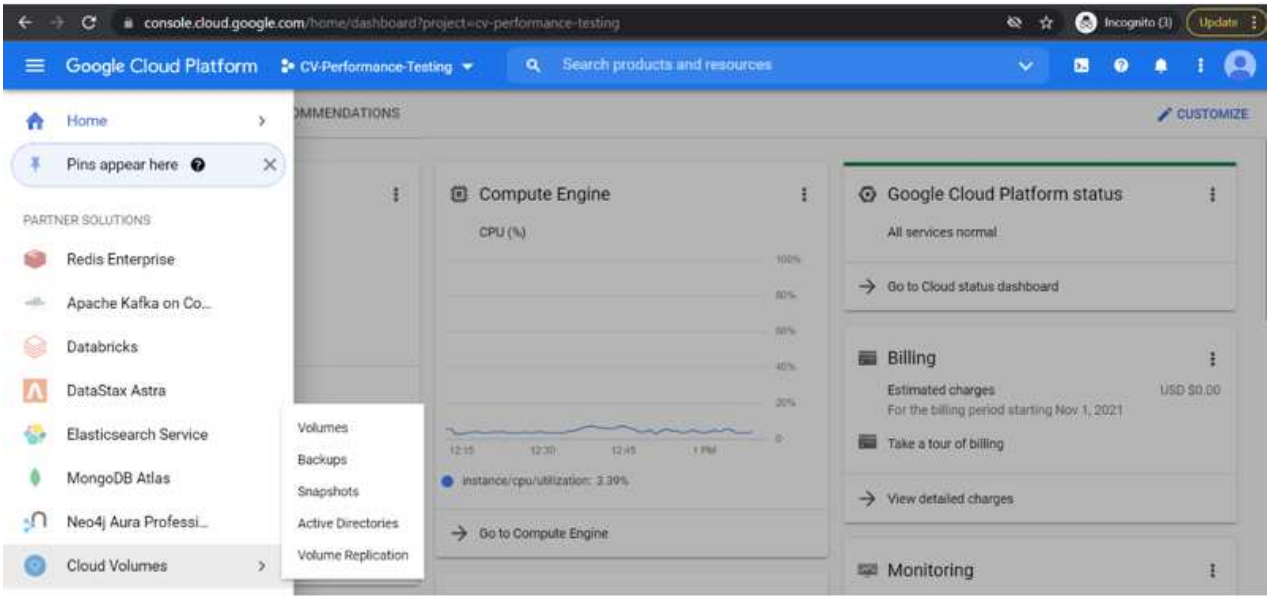
Cloud Volume Service和Google Cloud VMware Engine私有雲必須位於相同的地區。

若要Cloud Volumes Service 從Google Cloud Marketplace購買、啟用及設定NetApp for Google Cloud的NetApp解決方案、請依照下列詳細說明操作 "指南"。

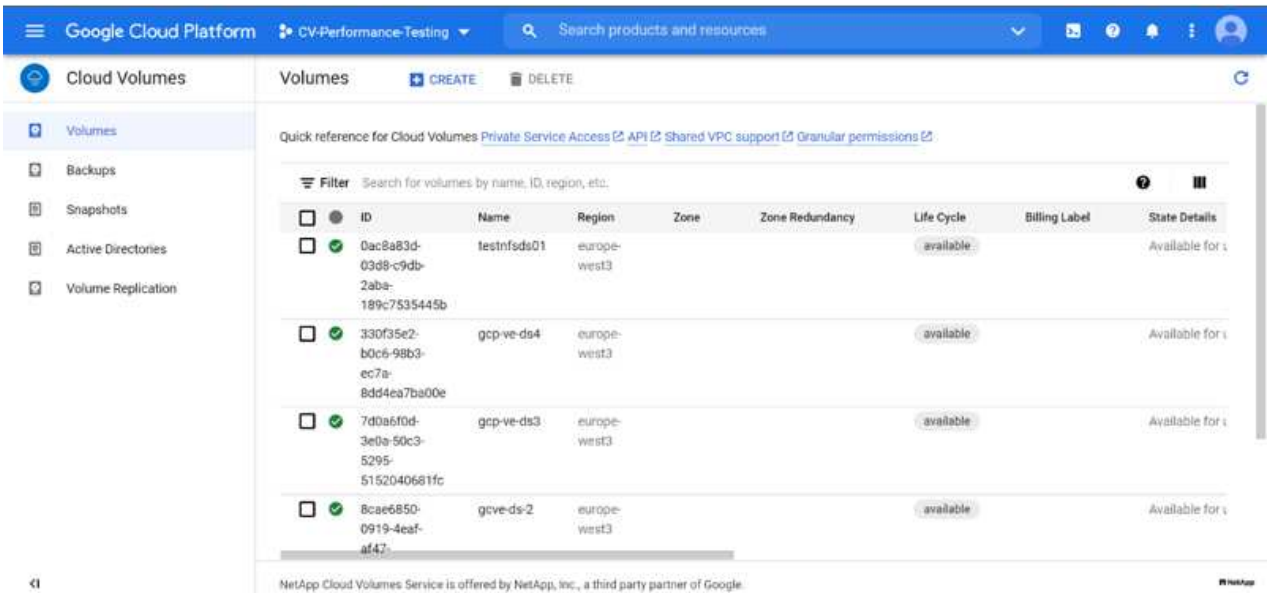
建立CVS NFS磁碟區至GCVG私有雲

若要建立及掛載NFS磁碟區、請完成下列步驟：

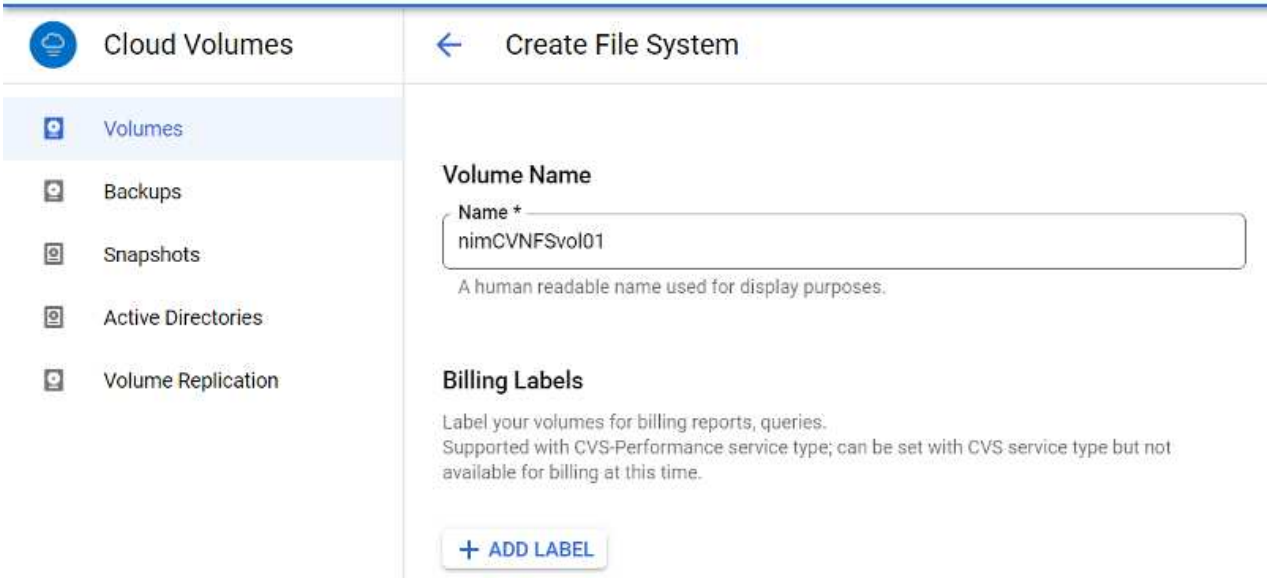
1. 從Google雲端主控台的合作夥伴解決方案存取Cloud Volumes。



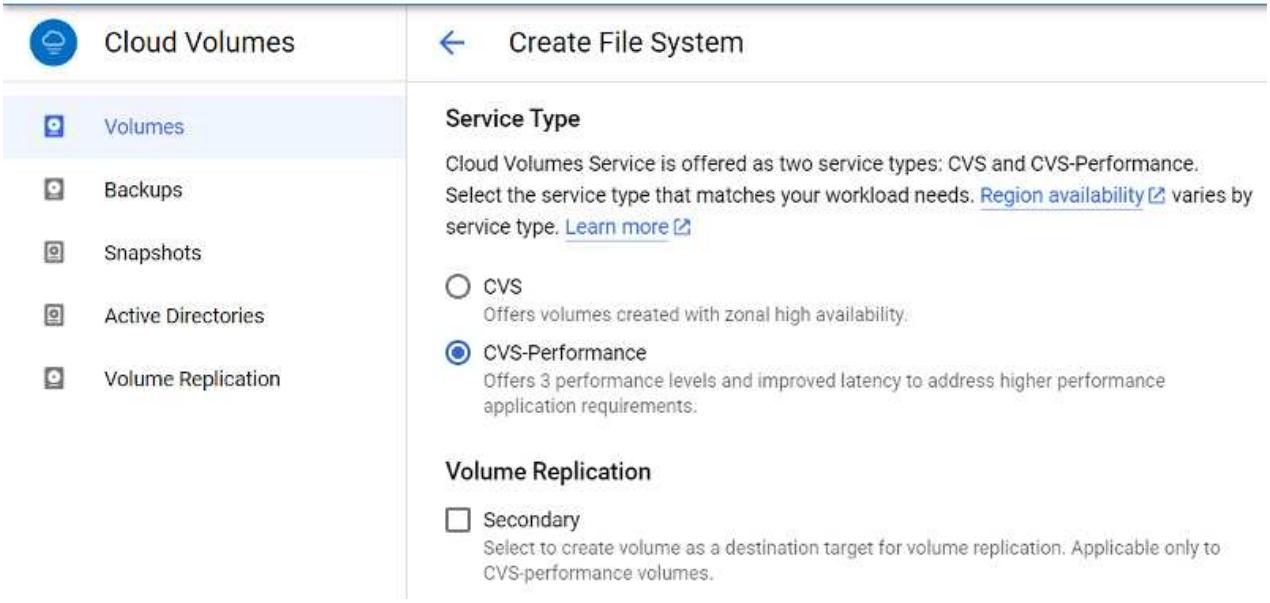
2. 在Cloud Volumes主控台中、前往Volumes（磁碟區）頁面、然後按一下Create（建立）。



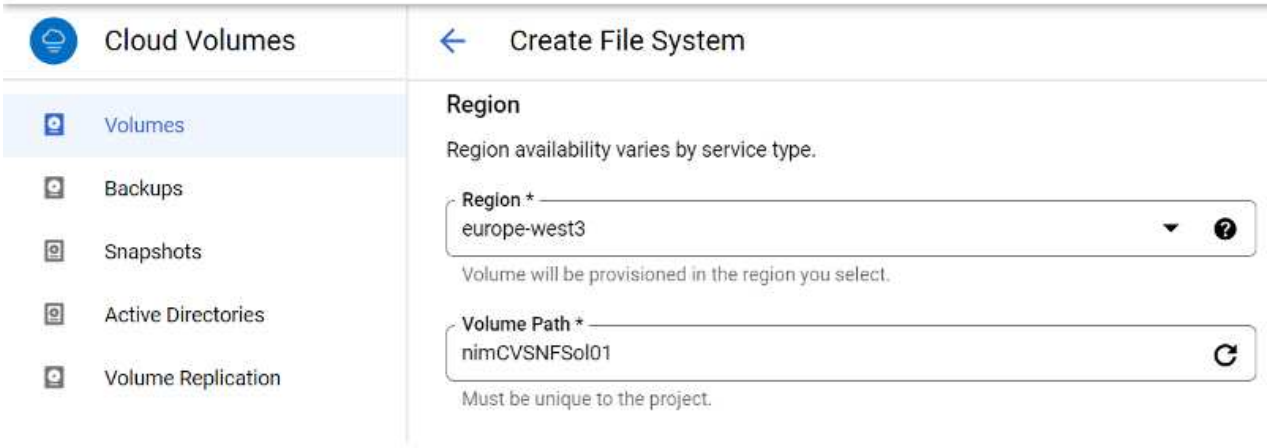
3. 在「Create File System」（建立檔案系統）頁面上、指定計費機制所需的磁碟區名稱和計費標籤。



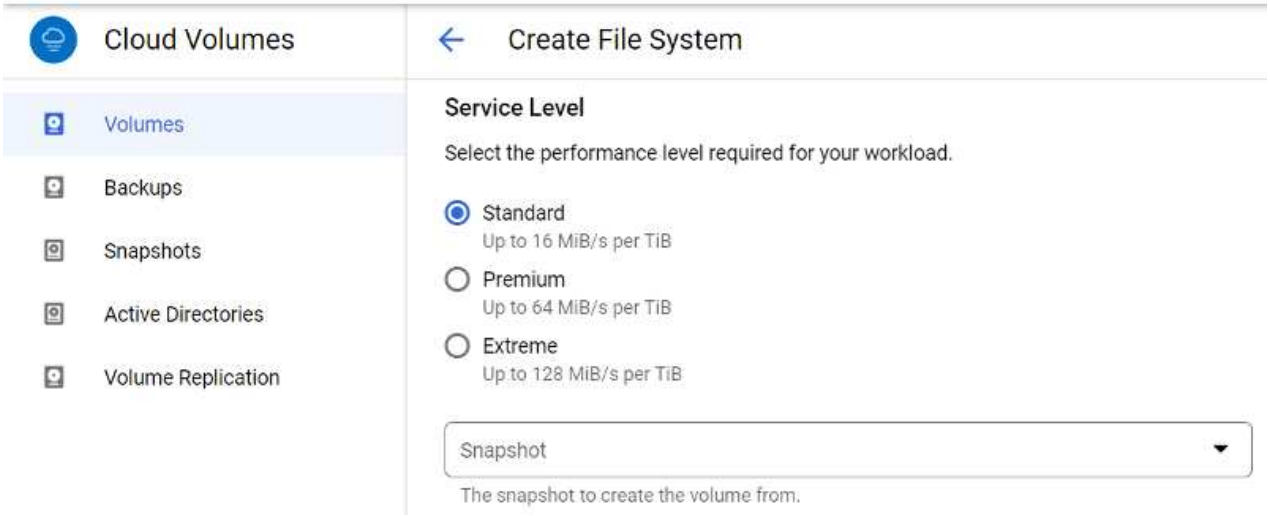
4. 選取適當的服務。若為GCVE/、請根據應用程式工作負載需求、選擇CVs-Performance和所需的服務層級、以改善延遲並提高效能。



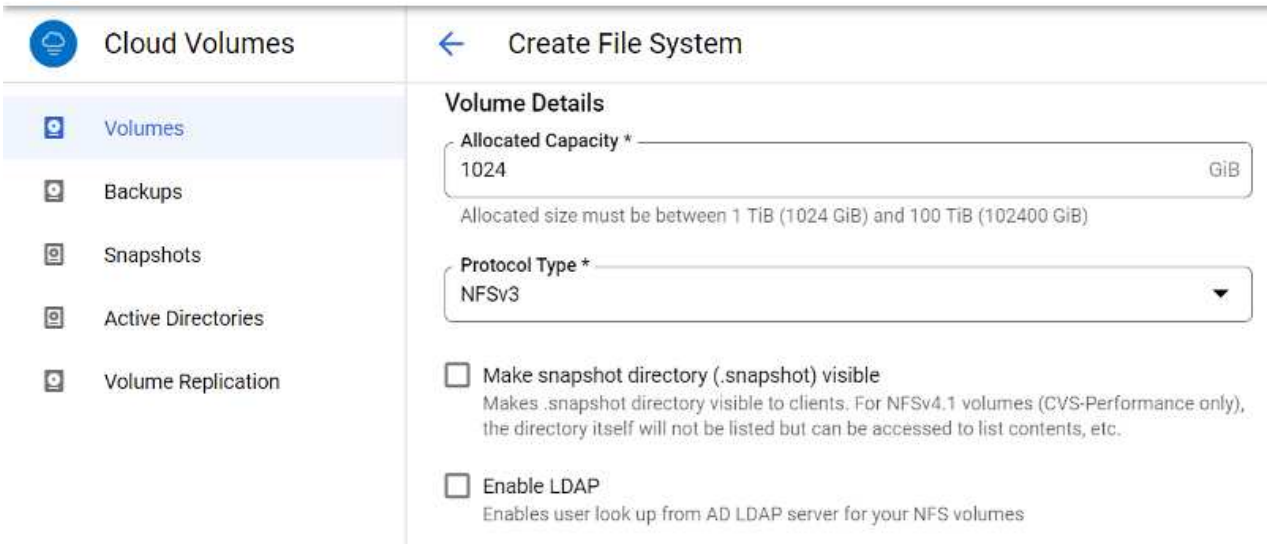
5. 為Volume和Volume路徑指定Google Cloud區域（該專案中所有雲端磁碟區的Volume路徑必須是唯一的）



6. 選取磁碟區的效能等級。

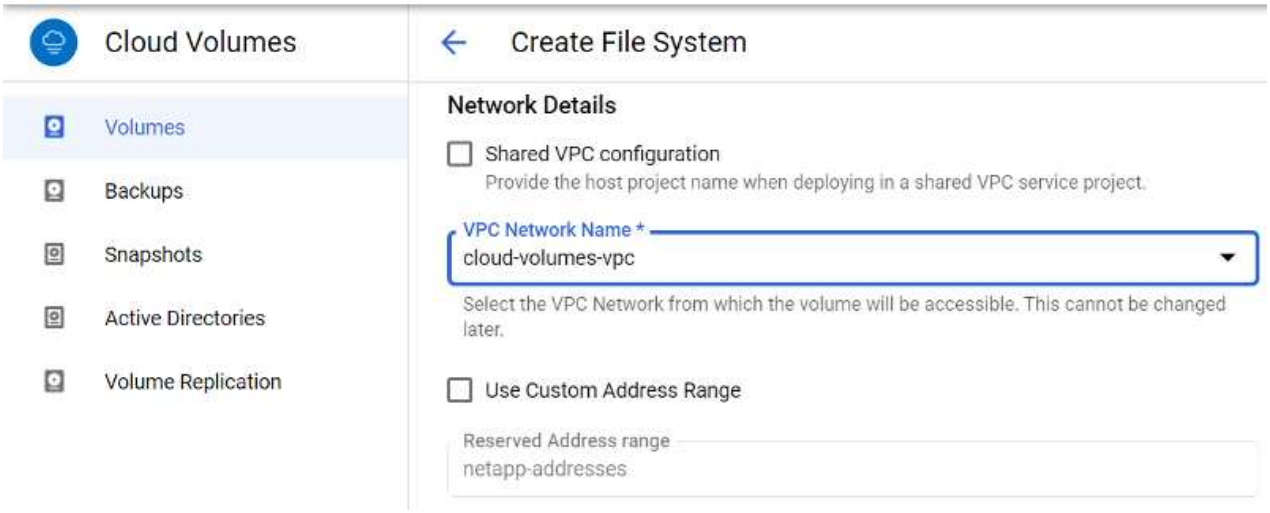


7. 指定磁碟區的大小和傳輸協定類型。在此測試中、使用NFSv3。



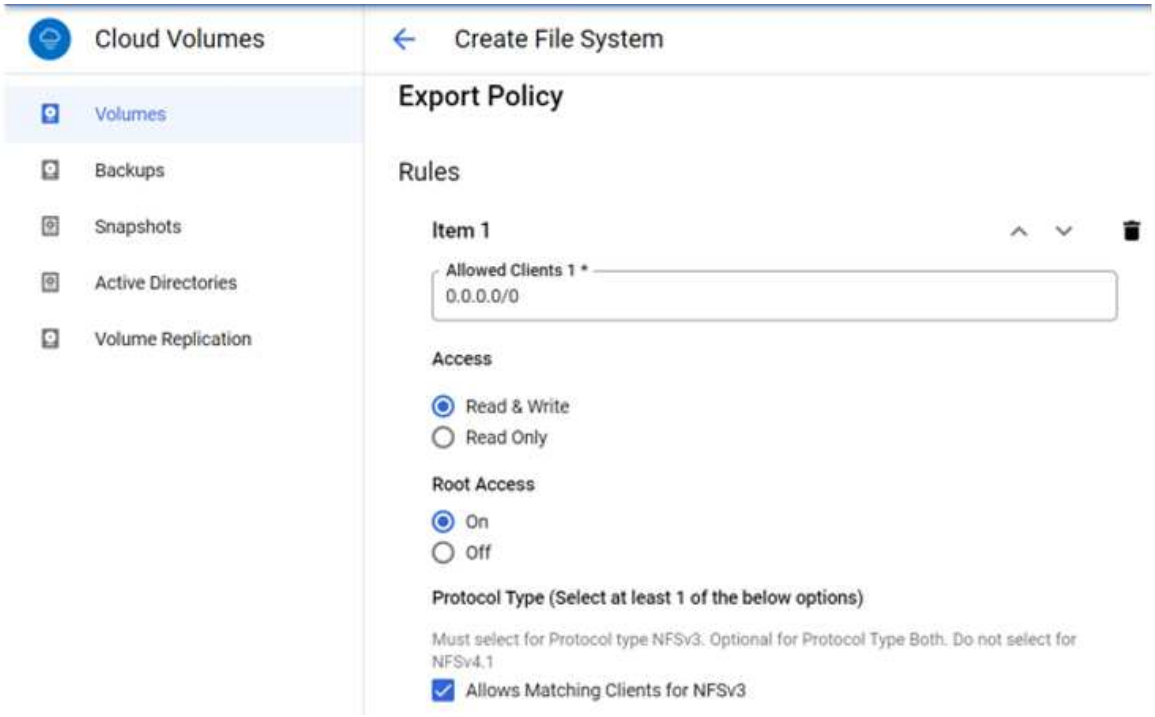
8. 在此步驟中、選取可存取磁碟區的VPC網路。確保VPC對等作業已就緒。

提示：如果VPC對等處理尚未完成、則會顯示快顯按鈕、引導您完成對等處理命令。開啟Cloud Shell工作階段、執行適當的命令、讓您的VPC與Cloud Volumes Service 效能提升者對等。如果您決定事先準備VPC對等、請參閱這些指示。



9. 新增適當的規則來管理匯出原則規則、然後選取對應NFS版本的核取方塊。

   附註：除非新增匯出原則、否則無法存取NFS磁碟區。



10. 按一下「儲存」以建立磁碟區。

將**NFS**匯出安裝到**VMware Engine**上執行的**VM**

在準備掛載NFS磁碟區之前、請確定私有連線的對等狀態列示為「Active」（作用中）。狀態為「作用中」時、請使用mount命令。

若要掛載NFS Volume、請執行下列步驟：

1. 在Cloud Console中、前往Cloud Volumes（雲端磁碟區）> Volumes（磁碟區）。
2. 前往「Volumes（磁碟區）」頁面
3. 按一下您要掛載NFS匯出的NFS磁碟區。
4. 向右捲動、按一下「Show More（顯示更多）」下方的「Mount Instructions（掛載指示）」

若要從VMware VM的客體作業系統內執行掛載程序、請依照下列步驟進行：

1. 在虛擬機器上使用SSH用戶端和SSH。
2. 在執行個體上安裝NFS用戶端。
   a. 在Red Hat Enterprise Linux或SUSE Linux執行個體上：

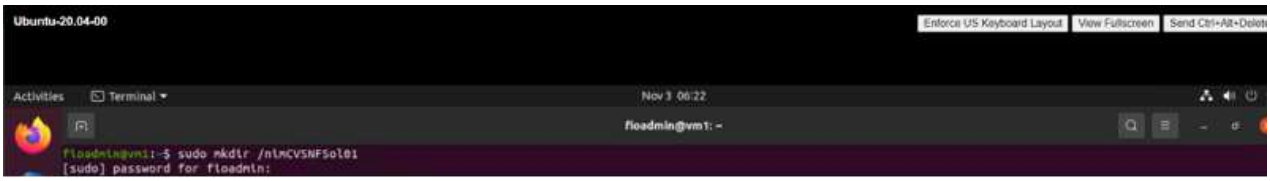
```
 sudo yum install -y nfs-utils
```

.. 在Ubuntu或Debian執行個體上：

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

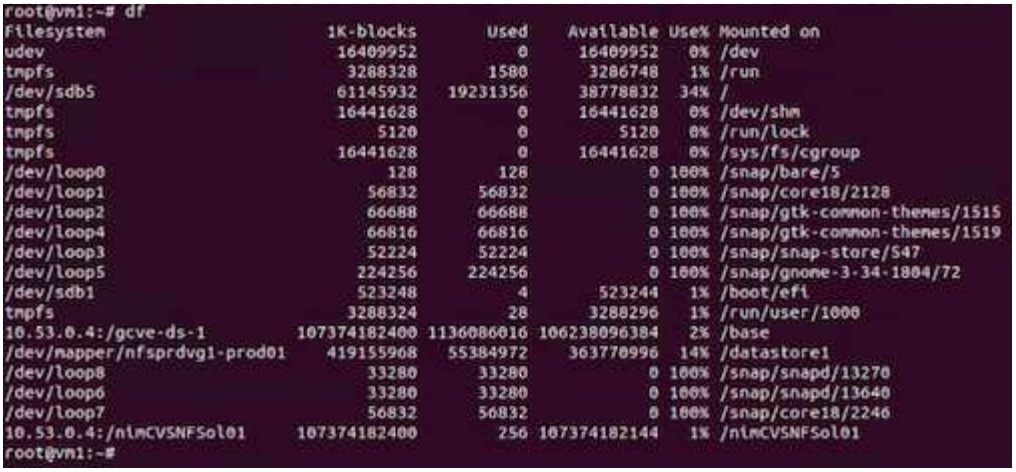
3. 在執行個體上建立新目錄、例如「/NimCVSNFSol01」：

```
sudo mkdir /nimCVSNFSol01
```



4. 使用適當的命令掛載磁碟區。實驗室命令範例如下：

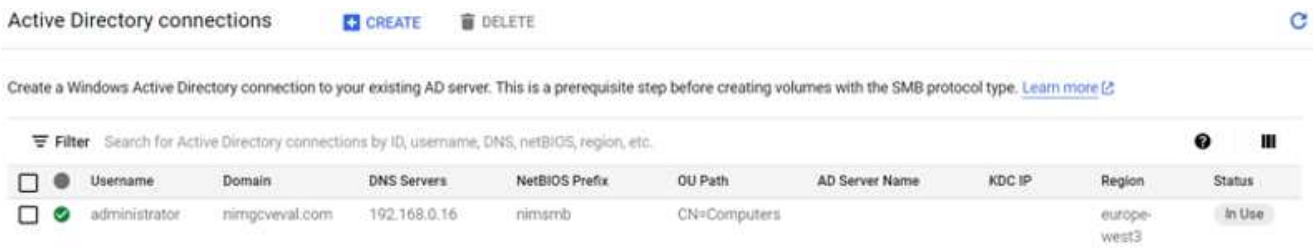
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     38778832  34% /
tmpfs                           16441628           0     16441628   0% /dev/shm
tmpfs                               5120           0         5120   0% /run/lock
tmpfs                           16441628           0     16441628   0% /sys/fs/cgroup
/dev/loop0                            128         128            0 100% /snap/bare/5
/dev/loop1                          56832       56832            0 100% /snap/core18/2128
/dev/loop2                          66688       66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                          66816       66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                          52224       52224            0 100% /snap/snap-store/547
/dev/loop5                         224256      224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                          523248           4       523244   1% /boot/efi
tmpfs                             3288324          28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1          107374182400  1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01    419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nlmCVSNFSol01      107374182400         256 107374182144   1% /nlmCVSNFSol01
root@vm1:~#
```

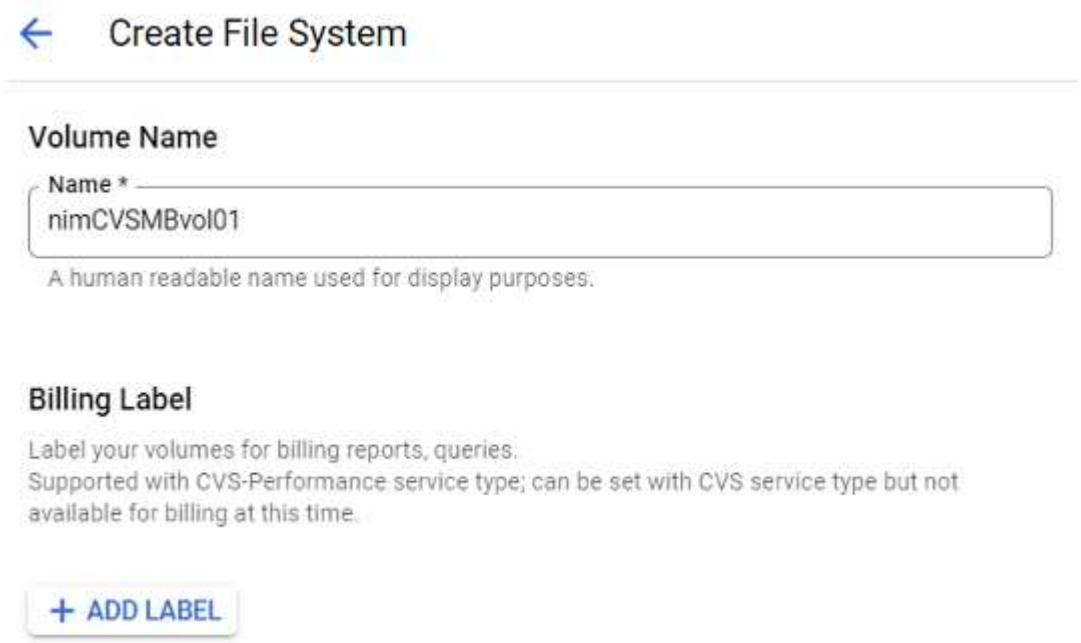
建立SMB共用並掛載到VMware Engine上執行的VM

對於SMB磁碟區、請確定在建立SMB磁碟區之前已設定Active Directory連線。

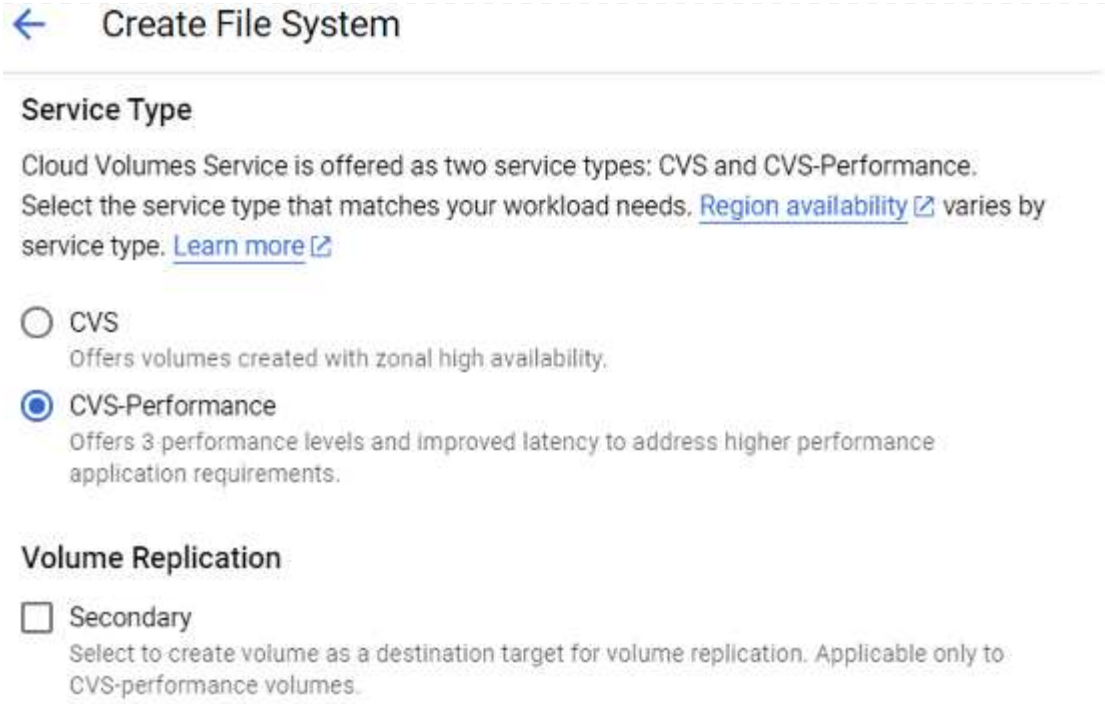


一旦AD連線就位、請以所需的服務層級建立磁碟區。除了選取適當的傳輸協定之外、步驟就像建立NFS Volume一樣。

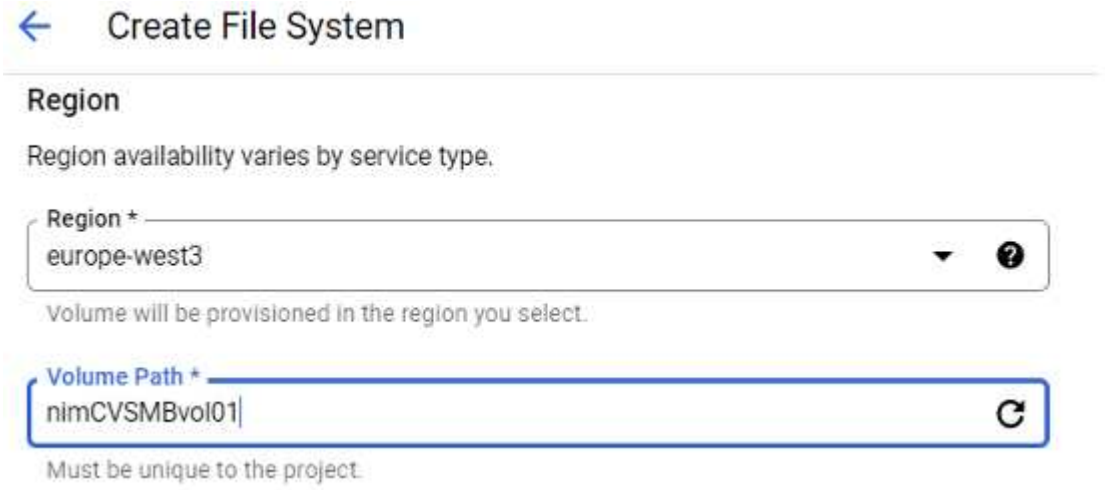
1. 在Cloud Volumes主控台中、前往Volumes（磁碟區）頁面、然後按一下Create（建立）。
2. 在「Create File System」（建立檔案系統）頁面上、指定計費機制所需的磁碟區名稱和計費標籤。



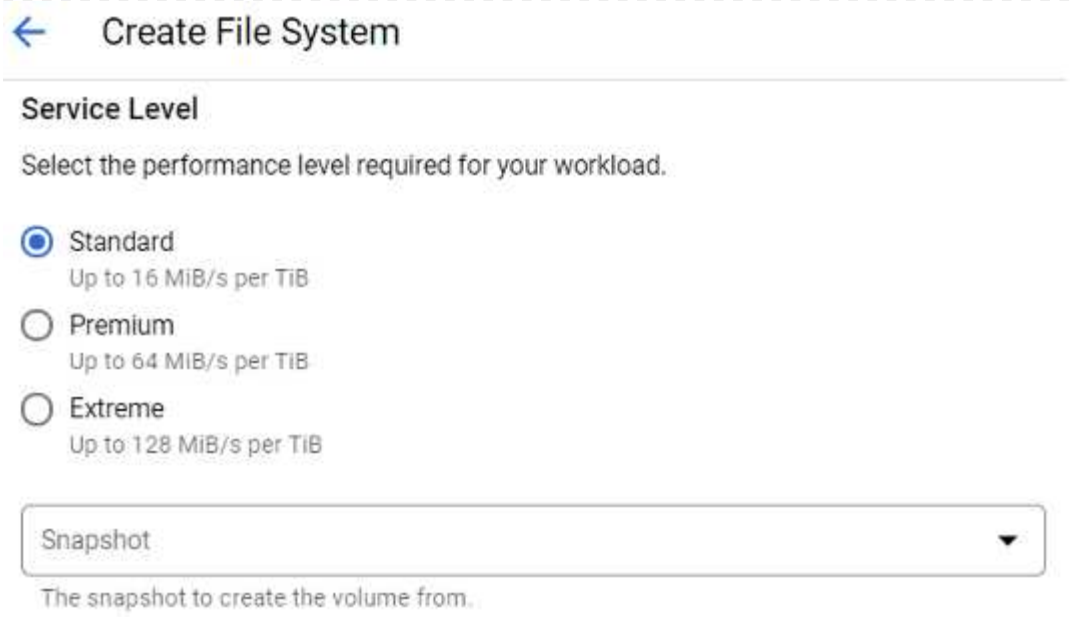
3. 選取適當的服務。若為GCVE/、請根據工作負載需求選擇CVs-Performance和所需的服務層級、以改善延遲並提高效能。



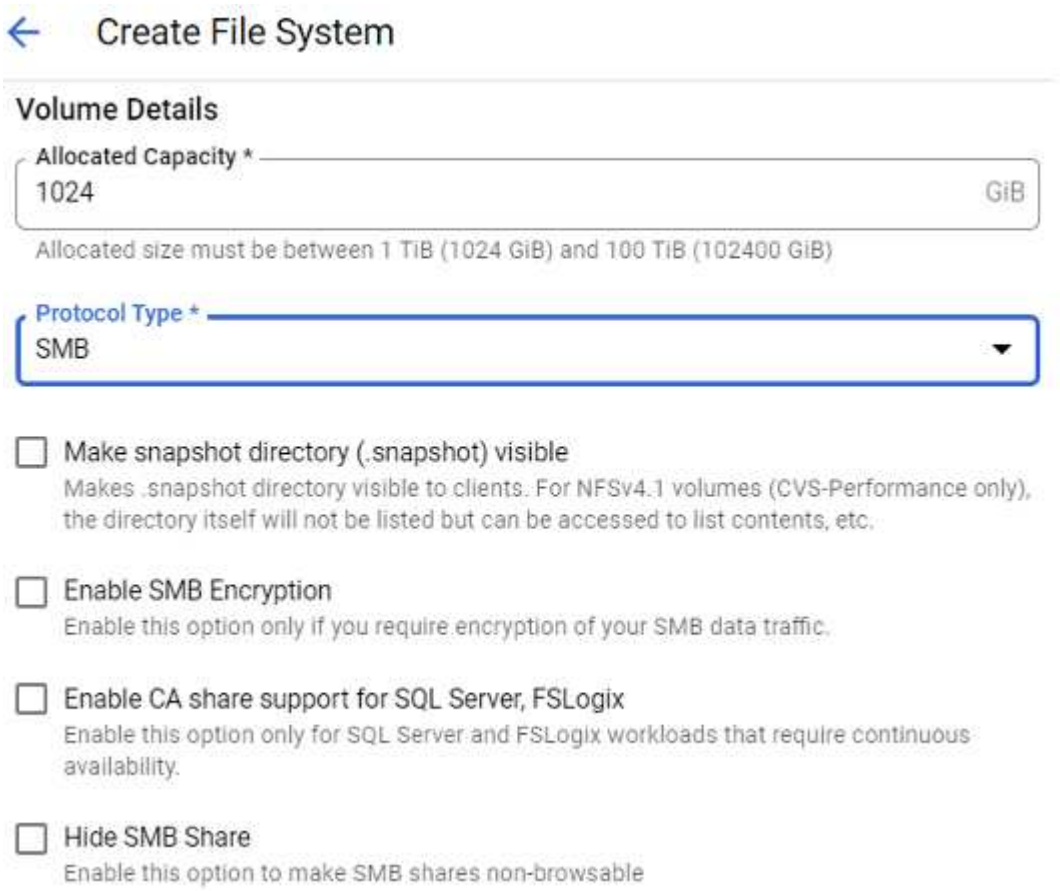
4. 為Volume和Volume路徑指定Google Cloud區域（該專案中所有雲端磁碟區的Volume路徑必須是唯一的）



5. 選取磁碟區的效能等級。

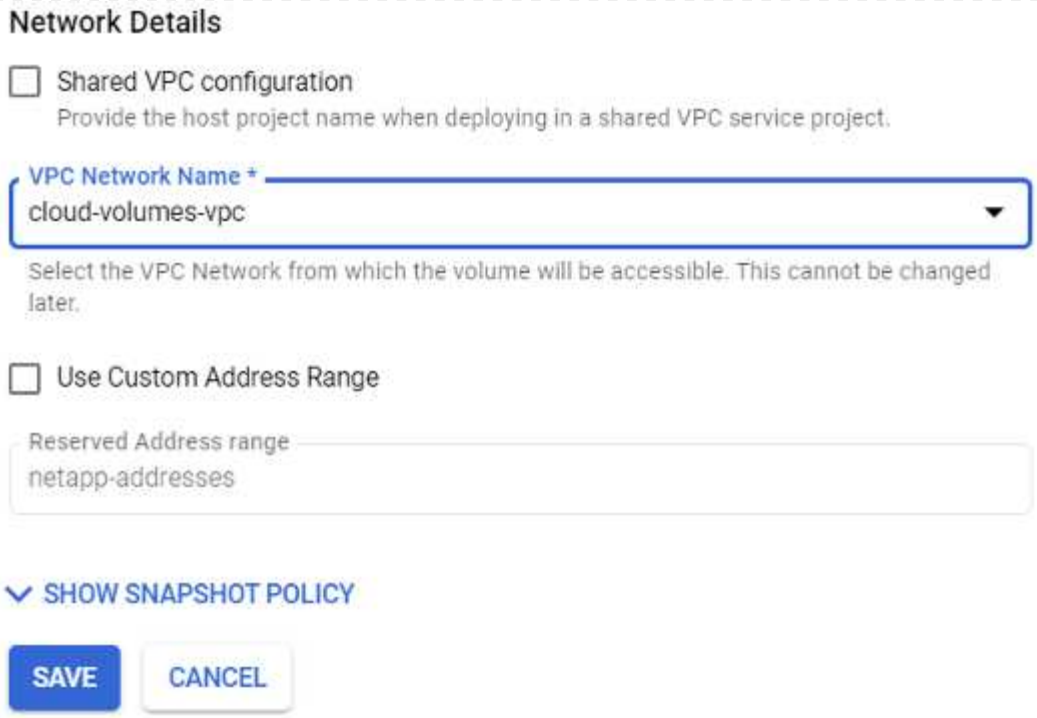


6. 指定磁碟區的大小和傳輸協定類型。在此測試中、使用SMB。



7. 在此步驟中、選取可存取磁碟區的VPC網路。確保VPC對等作業已就緒。

   提示：如果VPC對等處理尚未完成、則會顯示快顯按鈕、引導您完成對等處理命令。開啟Cloud Shell工作階段、執行適當的命令、讓您的VPC與Cloud Volumes Service 效能提升者對等。如果您決定事先準備VPC對等、請參閱這些資訊 "說明"。



8. 按一下「儲存」以建立磁碟區。

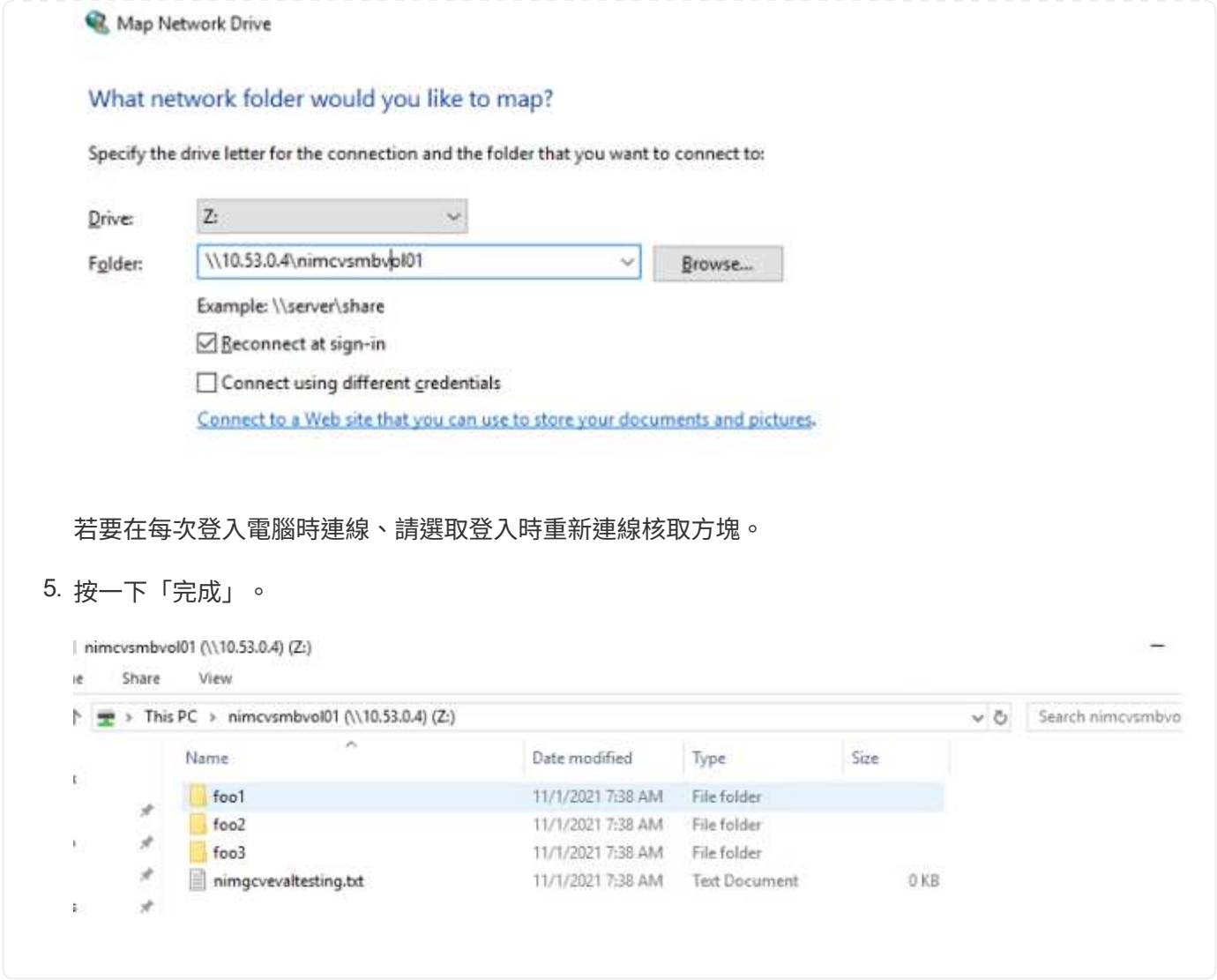
若要掛載SMB Volume、請執行下列步驟：

1. 在Cloud Console中、前往Cloud Volumes（雲端磁碟區）> Volumes（磁碟區）。
2. 前往「Volumes（磁碟區）」頁面
3. 按一下您要對應SMB共用區的SMB Volume。
4. 向右捲動、按一下「Show More（顯示更多）」下方的「Mount Instructions（掛載指示）」

若要從VMware VM的Windows來賓作業系統中執行掛載程序、請依照下列步驟進行：

1. 按一下「開始」按鈕、然後按一下「電腦」。
2. 按一下「對應網路磁碟機」。
3. 在「磁碟機」清單中、按一下任何可用的磁碟機代號。
4. 在資料夾方塊中、輸入：

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



若要在每次登入電腦時連線、請選取登入時重新連線核取方塊。

5. 按一下「完成」。

AWS、**Azure**和**GCP**上的補充**NFS**資料存放區可用度

深入瞭解全球區域對AWS、Azure和Google Cloud Platform（GCP）上的補充NFS資料存放區的支援。

AWS區域可用度

AWS / VMC上的補充NFS資料存放區可用度由Amazon定義。首先、您需要判斷VMC和FSxN是否在指定的區域中可用。接下來、您需要判斷該區域是否支援FSxN補充NFS資料存放區。

- 檢查VMC的可用度 "請按這裡"。
- Amazon定價指南提供FSxN（FSx ONTAP ）的可用位置資訊。您可以找到這些資訊 "請按這裡"。
- VMC的FSxN補充NFS資料存放區即將推出。

在資訊仍在發佈期間、下表將目前對VMC、FSxN和FSxN的支援識別為補充NFS資料存放區。

美洲

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
美國東部（北維吉尼亞州）	是的	是的	是的
美國東部（俄亥俄州）	是的	是的	是的
美國西部（北加州）	是的	否	否
美國西部（俄勒岡州）	是的	是的	是的
GovCloud（美國西部）	是的	是的	是的
加拿大（中部）	是的	是的	是的
南美洲（聖保羅）	是的	是的	是的

最後更新日期：2022年6月2日。

EMEA

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
歐洲（愛爾蘭）	是的	是的	是的
歐洲（倫敦）	是的	是的	是的
歐洲（法蘭克福）	是的	是的	是的
歐洲（巴黎）	是的	是的	是的
歐洲（米蘭）	是的	是的	是的
歐洲（斯德哥爾摩）	是的	是的	是的

最後更新日期：2022年6月2日。

亞太地區

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
亞太地區（悉尼）	是的	是的	是的
亞太地區（東京）	是的	是的	是的
亞太地區（大阪）	是的	否	否
亞太地區（新加坡）	是的	是的	是的
亞太地區（首爾）	是的	是的	是的
亞太地區（Mumbai）	是的	是的	是的
亞太地區（雅加達）	否	否	否
亞太地區（香港）	是的	是的	是的

最後更新日期：2022年9月28日。

Azure區域可用度

Azure / AVS上補充NFS資料存放區的可用度由Microsoft定義。首先、您需要判斷AVS和ANF是否在特定地區提供。接下來、您需要判斷該區域是否支援ANF補充NFS資料存放區。

- 查看AVS和ANF的可用度 "請按這裡"。
- 檢查ANF補充NFS資料存放區的可用度 "請按這裡"。

GCP區域可用度

GCP區域上市時間將於GCP上市時公佈。

摘要與結論：為何選擇**NetApp**混合式多雲端搭配**VMware**

NetApp Cloud Volumes搭配適用於大型超大規模擴充系統的VMware解決方案、可為想要運用混合雲的組織提供極大潛力。本節其餘部分提供使用案例、說明整合NetApp Cloud Volumes可實現真正的混合式多雲功能。

使用案例**1**：最佳化儲存設備

使用RVtoolsouting執行規模調整練習時、總是能清楚看出、馬力（vcpU/vMem）的規模與儲存設備平行。許多時候、組織發現自己的儲存空間需要磁碟機的大小、遠超馬力所需的大小。

透過整合NetApp Cloud Volumes、組織可以透過簡單的移轉方法實現vSphere型雲端解決方案、無需重新建立平台、無需變更IP、也無需變更架構。此外、此最佳化可讓您擴充儲存設備佔用空間、同時將vSphere中所需的主機數量維持在最低、但不會變更可用的儲存階層架構、安全性或檔案。這可讓您最佳化部署、並將整體TCO降低35%至45%。這項整合也可讓您在數秒內將儲存設備從溫儲存設備擴充至正式作業層級的效能。

使用案例**2**：雲端移轉

企業組織正面臨從內部部署資料中心移轉應用程式至公有雲的壓力、原因有多種：即將到期的租賃期限；從資本支出（資本支出）移轉至營運支出（營運支出）支出的財務指示；或只是由上而下的任務、將一切移至雲端。

當速度至關重要時、只有簡化的移轉方法才可行、因為為了適應雲端的特定IaaS平台而重新建立平台和重構應用程式的速度緩慢且昂貴、通常需要數月的時間。將NetApp Cloud Volumes與具頻寬效率的SnapMirror複寫結合、以利連接客體的儲存設備（包括結合應用程式一致的Snapshot複本和HCX的RDM）、實現雲端特定移轉（例如 Azure移轉）、或是用於複寫VM的協力廠商產品）、這項移轉作業比仰賴耗時的I/O篩選機制更容易。

使用案例**3**：資料中心擴充

當資料中心因為季節性需求尖峰或是組織內部的穩定成長而達到容量限制時、移轉至雲端代管的VMware以及NetApp Cloud Volumes是一項簡單的解決方案。運用NetApp Cloud Volumes、可在可用度區域之間提供高可用度、並提供動態擴充功能、輕鬆建立、複寫及擴充儲存設備。運用NetApp Cloud Volumes可克服延伸叢集的需求、將主機叢集容量降至最低。

使用案例**4**：災難恢復至雲端

在傳統的方法中、如果發生災難、複寫到雲端的VM將需要在還原之前、先轉換至雲端本身的Hypervisor平台、而非在危機期間處理的工作。

透過使用NetApp Cloud Volumes進行與來賓連線的儲存設備、並使用SnapCenter 內部部署的VMware和SnapMirror複寫、以及公有雲虛擬化解決方案、可以設計出更好的災難恢復方法、讓VM複本能夠在完全一致的VMware SDDC基礎架構上還原、並搭配雲端特定的恢復工具（例如 Azure Site Recovery）或同等的協力廠商工具、例如Veeam。這種方法也能讓您快速執行災難恢復訓練、並從勒索軟體中恢復。如此一來、您也可以隨需新增主機、以擴充至完整正式作業環境進行測試或災難期間。

使用案例**5**：應用程式現代化

應用程式放入公有雲之後、組織就會想要利用數百種強大的雲端服務來進行現代化和擴充。使用NetApp Cloud Volumes之後、現代化是一項簡單的程序、因為應用程式資料並未鎖定在vSAN中、因此可在多種使用案例（包括Kubernetes）中進行資料移動。

結論

無論您的目標是全雲端或混合雲、NetApp Cloud Volumes都能提供絕佳的選項來部署及管理應用程式工作負載、以及檔案服務和區塊傳輸協定、同時讓應用程式層的資料需求順暢無礙、進而降低TCO。

無論使用案例為何、請選擇您最喜愛的雲端/超大規模伺服器搭配NetApp Cloud Volumes、以快速實現雲端效益、一致的基礎架構、以及跨內部部署和多個雲端的作業、工作負載的雙向可攜性、以及企業級容量和效能。

這是用來連接儲存設備的熟悉程序。請記住、這只是以新名稱變更資料的位置、工具和程序都維持不變、而NetApp Cloud Volumes則有助於最佳化整體部署。

VMware混合雲使用案例

NetApp混合式多雲端與**VMware**的使用案例

在規劃混合雲或雲端優先部署時、對IT組織而言重要的使用案例總覽。

熱門使用案例

使用案例包括：

- 災難恢復、
- 在資料中心維護期間代管工作負載*快速爆發、除了本機資料中心的資源配置之外、還需要額外的資源、
- VMware站台擴充、
- 快速移轉至雲端、
- 開發/測試、及
- 運用雲端輔助技術來現代化應用程式。

在本文件中、我們將使用VMware使用案例來詳細說明雲端工作負載參考資料。這些使用案例包括：

- 保護（包括災難恢復和備份/還原）
- 移轉
- 延伸

IT發展歷程中

大多數組織都在轉型與現代化的過程中。在這個流程中、公司正嘗試使用現有的VMware投資、同時善用雲端效益、並探索各種方法、使移轉程序盡可能順暢無礙。這種方法會讓他們的現代化工作變得非常簡單、因為資料已經在雲端中。

此案例最簡單的答案是每個超大規模擴充系統中的VMware產品。如同NetApp®Cloud Volumes、VMware提供一種將內部部署VMware環境移轉或延伸至任何雲端的方法、讓您保留現有的內部部署資產、技能和工具、同時在雲端原生執行工作負載。如此可降低風險、因為不會發生服務中斷或需要變更IP、讓IT團隊能夠使用現有的技能和工具、以內部部署的方式操作。如此一來、雲端移轉速度就會加快、並能更順暢地移轉至混合式多雲端架構。

瞭解補充**NFS**儲存選項的重要性

雖然VMware在任何雲端上都能為每位客戶提供獨特的混合式功能、但有限的補充NFS儲存選項限制了它對於儲存繁重工作負載的組織的效用。由於儲存設備直接與主機相連、因此擴充儲存設備的唯一方法是新增更多主機、而且儲存密集型工作負載的成本會增加35%至40%以上。這些工作負載只需要額外的儲存容量、而非額外的馬力。但這表示需要支付額外的主機費用。

讓我們來思考以下案例：

客戶只需要五部主機來處理CPU和記憶體、但需要大量的儲存需求、而且需要12部主機來滿足儲存需求。這項需求最終會在只需要增加儲存容量的情況下、購買額外的馬力、進而大幅提高財務規模。

當您規劃雲端採用和移轉時、務必評估最佳方法、並採取最簡單的方法來減少總投資。任何應用程式移轉最常見且最簡單的方法、就是在沒有虛擬機器（VM）或資料轉換的情況下、重新裝載（也稱為移轉）。使用NetApp Cloud Volumes搭配VMware軟體定義資料中心（SDDC）、同時輔助vSAN、可提供輕鬆的移轉選項。

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

深入瞭解NetApp為AWS帶來的解決方案。

VMware將雲端工作負載定義為三種類別之一：

- 保護（包括災難恢復和備份/還原）
- 移轉
- 延伸

請瀏覽下列各節提供的解決方案。

保護

- "使用AWS上的VMC進行災難恢復（與來賓連線）"
- "Veeam 備份擴大機；使用適用於 ONTAP 的 FSX 在 VMC 中還原"
- "利用FSX進行ONTAP 災難恢復（DRO）以支援VMware及VMC"
- "使用 Veeam Replication 和 FSX for ONTAP 在 AWS 上進行災難恢復至 VMware Cloud"

移轉

- "使用VMware HCX將工作負載移轉至FSxN資料存放區"

延伸

即將推出！！

適用於**Azure VMware**解決方案（**AVS**）

深入瞭解NetApp為Azure提供的解決方案。

VMware將雲端工作負載定義為三種類別之一：

- 保護（包括災難恢復和備份/還原）
- 移轉
- 延伸

請瀏覽下列各節提供的解決方案。

保護

- "使用ANF和Jetstream（補充NFS資料存放區）進行災難恢復"
- "使用ANF和CVO（與來賓連線的儲存設備）進行災難恢復"
- "災難恢復（ DRO ）與 ANF 和 AVS"
- "使用 Veeam Replication 和 Azure NetApp Files 資料存放區、將災難恢復至 Azure VMware 解決方案"

移轉

- "使用VMware HCX將工作負載移轉至Azure NetApp Files VMware資料存放區"

延伸

即將推出！！

NetApp Solutions for Google Cloud VMware Engine （ GCVE ）

深入瞭解NetApp為GCP帶來的解決方案。

VMware將雲端工作負載定義為三種類別之一：

- 保護（包括災難恢復和備份/還原）
- 移轉
- 延伸

請瀏覽下列各節提供的解決方案。

保護

- "應用程式災難恢復：SnapCenter 利用功能不全Cloud Volumes ONTAP 、功能不全和Veeam複寫"
- "利用 NetApp SnapCenter 和 Veeam 複寫功能、將應用程式一致的災難恢復功能複製到 GCVE 上的 NetApp CVS"

移轉

- "使用VMware HCX將工作負載移轉至NetApp Cloud Volume Service NFS資料存放區"
- "使用 Veeam 複寫至 NetApp Cloud Volume Service NFS 資料存放區"

延伸

即將推出！！

適用於**AWS VMC**的**NetApp**功能

深入瞭解NetApp為AWS VMware Cloud（VMC）帶來的功能：從NetApp做為來賓連線儲存設備或補充NFS資料存放區、移轉工作流程、延伸/突增至雲端、備份/還原及災難恢復。

從下列選項中選取、跳至所需內容的區段：

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

在**AWS**中設定**VMC**

如同內部部署、規劃雲端型虛擬化環境對於成功建立虛擬機器和移轉的正式作業就緒環境來說、是非常重要的。

本節說明如何在AWS SDDC上設定及管理VMware Cloud、並搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的將Cloud Volumes ONTAP 功能連接到AWS VMC的方法。

設定程序可分為下列步驟：

- 部署及設定適用於AWS的VMware Cloud
- 將VMware Cloud連接至FSX ONTAP VMware

檢視詳細資訊 "VMC的組態步驟"。

適用於**VMC**的**NetApp**儲存選項

NetApp儲存設備可在AWS VMC中以多種方式使用、例如猜測連接的或補充的NFS資料存放區。

請造訪 "支援的NetApp儲存選項" 以取得更多資訊。

AWS支援下列組態的NetApp儲存設備：

- FSX ONTAP 支援以客為本的連線儲存設備
- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- FSX ONTAP 不只是NFS的補充資料存放區

檢視詳細資訊 "VMC的來賓連線儲存選項"。檢視詳細資訊 "VMC的補充NFS資料存放區選項"。

解決方案使用案例

有了NetApp和VMware雲端解決方案、許多使用案例都很容易部署在AWS VMC中。每個VMware定義的雲端領域都定義了使用案例：

- 保護（包括災難恢復和備份/還原）
- 延伸
- 移轉

"瀏覽NetApp的AWS VMC解決方案"

保護 **AWS / VMC** 上的工作負載

TR-4931：在**Amazon Web Services**和**Guest Connect**上使用**VMware Cloud**進行災難恢復

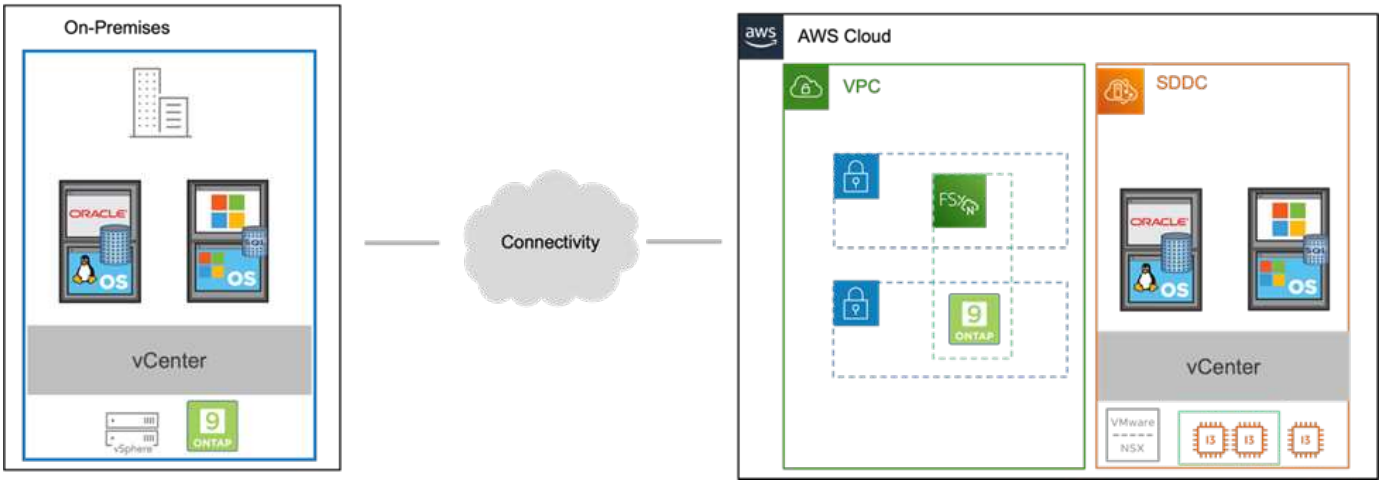
作者：Chris Reno、Josh Powell和Suresh Thopp付款- NetApp解決方案工程

總覽

備受肯定的災難恢復（DR）環境與計畫、對於組織而言至關重要、因為如此一來、組織就能確保在重大停機事件中迅速還原業務關鍵應用程式。本解決方案著重於示範DR使用案例、重點在於內部部署的VMware與NetApp技術、以及使用AWS上的VMware Cloud。

NetApp與VMware的整合歷史悠久、已有數萬家客戶選擇NetApp做為其虛擬化環境的儲存合作夥伴、證明這一點。這項整合會繼續與雲端的來賓連線選項整合、以及最近與NFS資料存放區的整合。本解決方案著重於通常稱為來賓連線儲存設備的使用案例。

在客體連線儲存設備中、客體VMDK會部署在VMware資源配置的資料存放區上、而應用程式資料則儲存在iSCSI或NFS上、並直接對應至VM。Oracle和MS SQL應用程式用於示範DR案例、如下圖所示。



假設、先決條件和元件總覽

在部署此解決方案之前、請先檢閱元件的總覽、部署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。

"災難恢復解決方案要求、預先要求和規劃"

使用**SnapCenter NetApp**執行災難恢復

在本解決方案中SnapCenter 、支援針對SQL Server和Oracle應用程式資料提供應用程式一致的快照。此組態搭配SnapMirror技術、可在內部部署AFF 的Sfx6 ONTAP 和FSX支援叢集之間提供高速資料複寫功能。此外、Veeam備份與複寫也為我們的虛擬機器提供備份與還原功能。

在本節中、我們將說明SnapCenter 如何設定用於備份與還原的SnapMirror、SnapMirror和Veeam。

下列各節涵蓋在次要站台完成容錯移轉所需的組態和步驟：

設定**SnapMirror**關係和保留排程

為了長期歸檔和保留、可在主要儲存系統（主儲存系統>鏡射）和次要儲存系統（主儲存系統>保存庫）內更新SnapMirror關係。SnapCenter若要這麼做、您必須使用SnapMirror建立並初始化目的地Volume與來源Volume之間的資料複寫關係。

來源ONTAP 和目的地的不全系統必須位於使用Amazon VPC對等網路、傳輸閘道、AWS Direct Connect或AWS VPN進行對等處理的網路中。

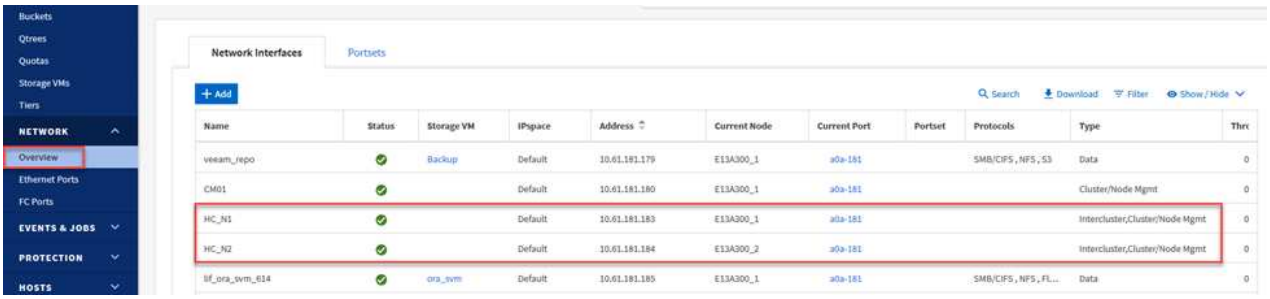
在內部部署ONTAP 的SnapMirror系統與FSXSing之間建立SnapMirror關係時、必須執行下列步驟ONTAP ：

請參閱 "FSX- ONTAP for Sfor Sfor Sfor - ONTAP 《用戶指南》" 如需建立SnapMirror與FSX關係的詳細資訊、

記錄來源與目的地叢集間邏輯介面

對於ONTAP 內部部署的來源版的來源版系統、您可以從System Manager或CLI擷取叢集間的LIF資訊。

1. 在「支援系統管理程式」中ONTAP 、瀏覽至「網路總覽」頁面、並擷取「類型：叢集間」的IP位址、這些位址已設定為與安裝FSx的AWS VPC通訊。



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.
```

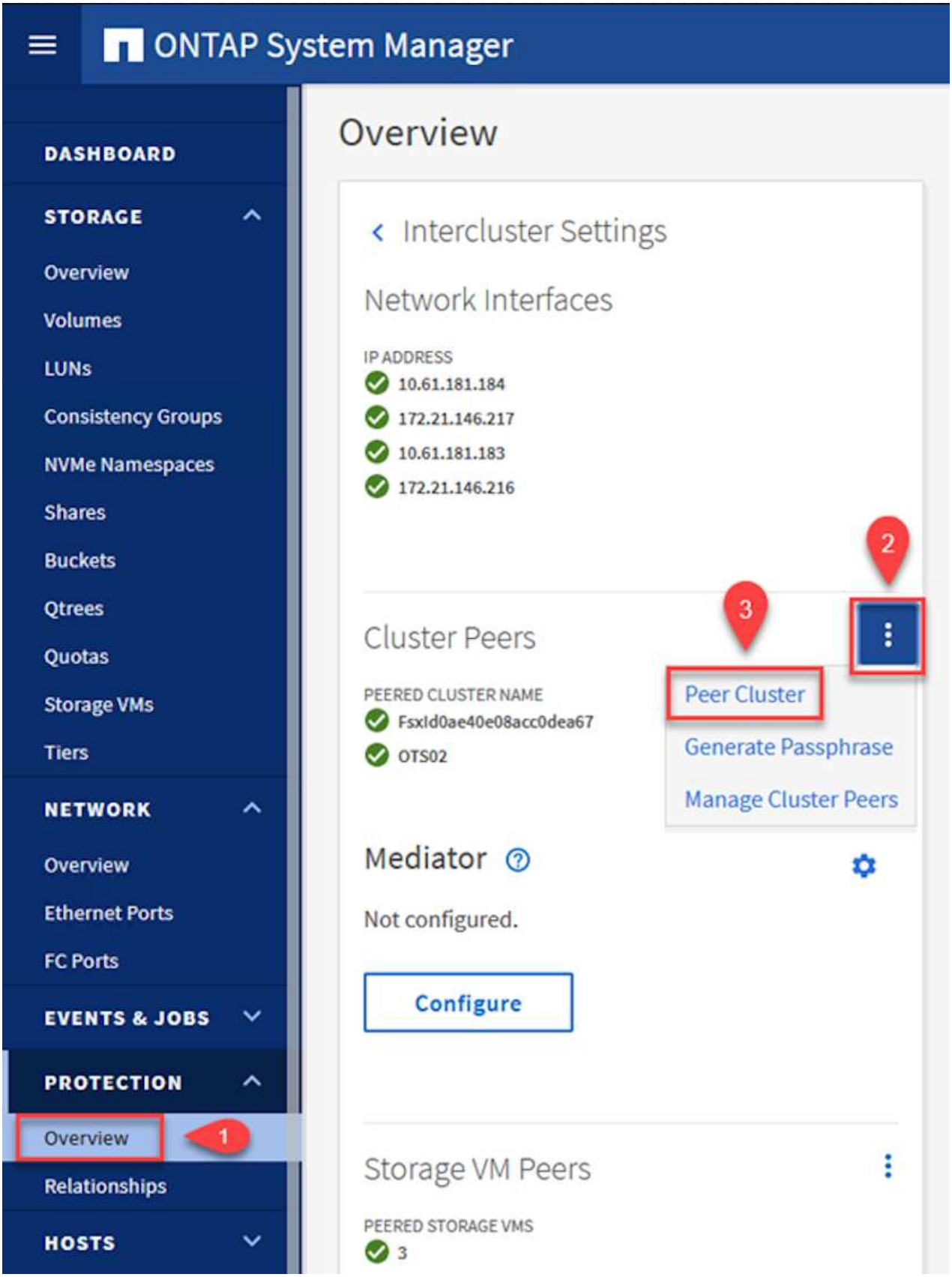
在**ONTAP Sfx6**和**FSX**之間建立叢集對等關係

若要在ONTAP 各個叢集之間建立叢集對等關係、必須ONTAP 在其他對等叢集中確認在起始的叢集上輸入的獨特通關密碼。

1. 使用「叢集對等點create」命令、在目的地FSX叢集上設定對等。出現提示時、請輸入稍後在來源叢集上使用的唯一密碼、以完成建立程序。

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

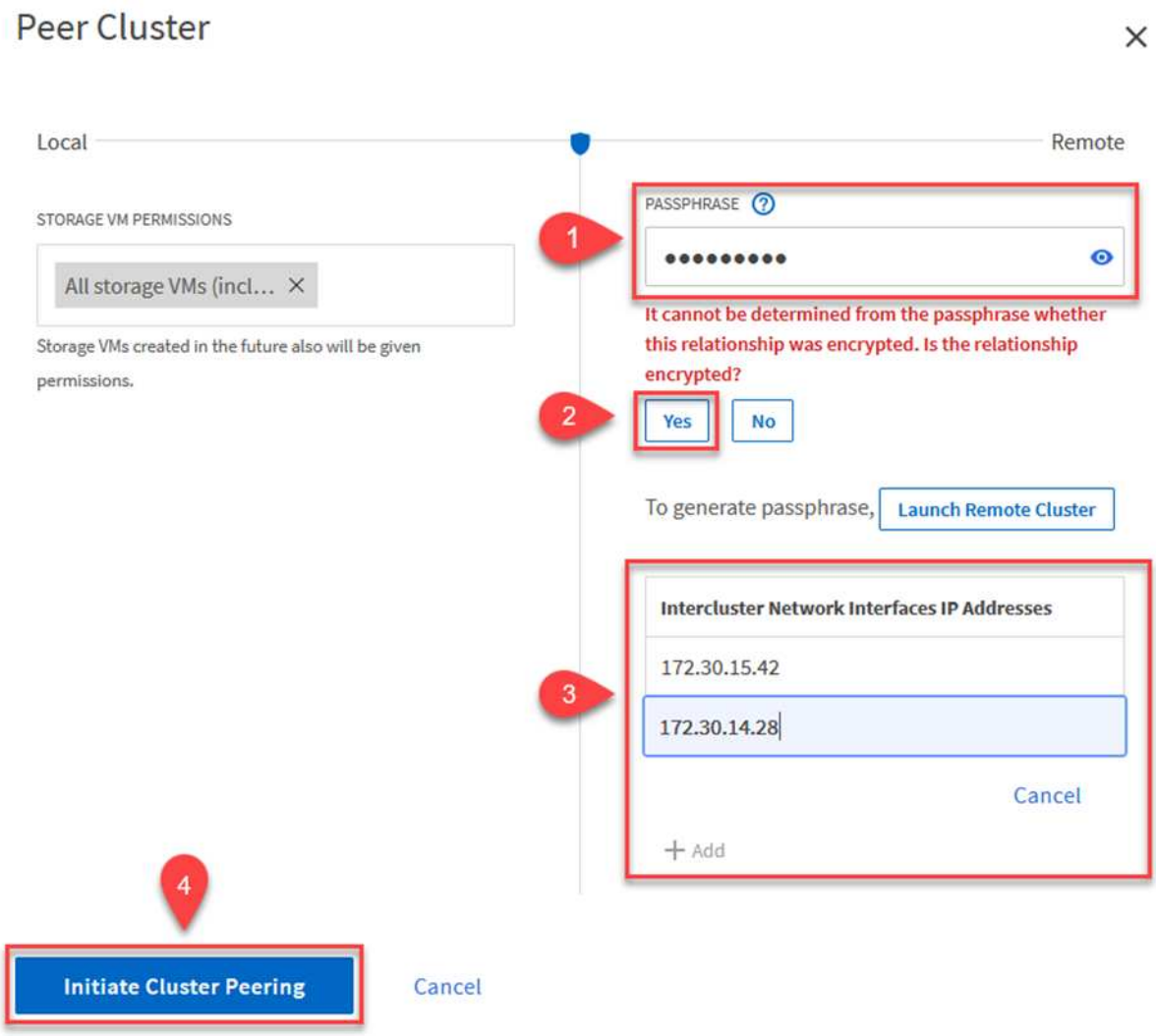
2. 在來源叢集上、您可以使用ONTAP SysSystem Manager或CLI建立叢集對等關係。從「系統管理程式」中、瀏覽至「保護」>「總覽」、然後選取「對等叢集」ONTAP 。



3. 在對等叢集對話方塊中、填寫必要資訊：
   a. 輸入用於在目的地FSX叢集上建立對等叢集關係的通關密碼。
   b. 選取「是」以建立加密關係。

c. 輸入目的地FSX叢集的叢集間LIF IP位址。

d. 按一下「初始化叢集對等」以完成程序。



4. 使用下列命令驗證來自FSX叢集的叢集對等關係狀態：

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

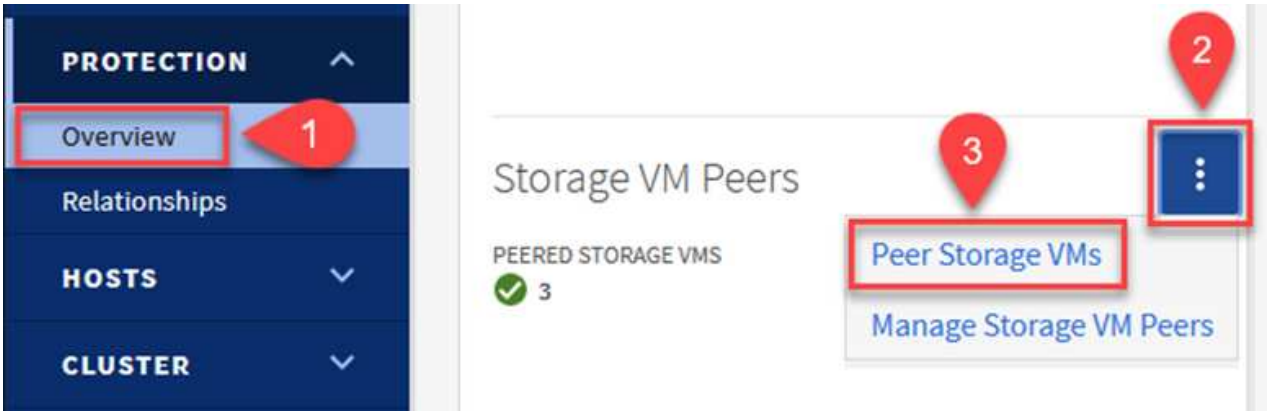
```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

下一步是在包含SnapMirror關係的磁碟區的目的地與來源儲存虛擬機器之間建立SVM關係。

1. 從來源FSX叢集、從CLI使用下列命令建立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 的物件叢集、接受與ONTAP SysSystem Manager或CLI的對等關係。
3. 從「支援系統管理程式」移至「保護」>「總覽」、然後在「儲存VM對等端點」下選取「對等儲存VM」ONTAP 。



4. 在對等儲存VM對話方塊中、填寫必填欄位：
   - 來源儲存VM
   - 目的地叢集
   - 目的地儲存VM

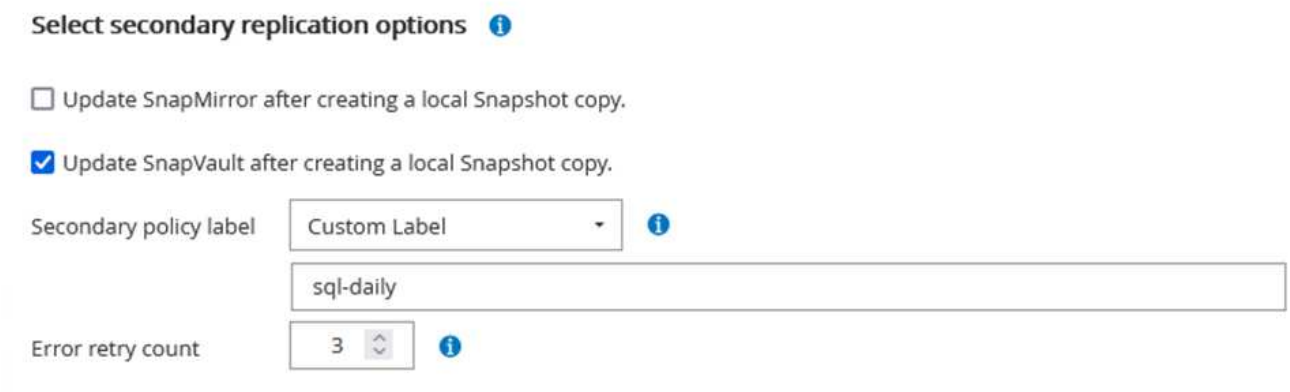
5. 按一下對等儲存VM以完成SVM對等處理程序。

可管理主要儲存系統上以快照複本形式存在的備份保留排程。SnapCenter這是SnapCenter 在建立一套以功能為基礎的原則時所建立的。不管理保留在二線儲存系統上的備份保留原則。SnapCenter這些原則是透過在次要FSX叢集上建立的SnapMirror原則來個別管理、並與與來源Volume處於SnapMirror關係中的目的地磁碟區相關聯。

建立SnapCenter Eshot原則時、您可以選擇指定次要原則標籤、並將其新增至SnapCenter 擷取此備份時所產生之每個Snapshot的SnapMirror標籤。

在二線儲存設備上、這些標籤會符合與目的地Volume相關的原則規則、以強制保留快照。

以下範例顯示SnapMirror標籤、其存在於所有快照上、這些快照是作為每日備份SQL Server資料庫和記錄磁碟區的原則之一。



如需建立SnapCenter SQL Server資料庫的各項功能性原則的詳細資訊、請參閱 "本文檔SnapCenter"。

您必須先建立SnapMirror原則、其中規定要保留的快照複本數量。

1. 在FSX叢集上建立SnapMirror原則。

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

2. 使用SnapMirror標籤將規則新增至原則、這些標籤符合SnapCenter 在《保護原則》中指定的次要原則標籤。

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

下列指令碼提供可新增至原則的規則範例：

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

針對每個SnapMirror標籤和要保留的快照數量（保留期間）建立其他規則。

建立目的地**Volume**

若要在FSXTM上建立目的地Volume、使其成為來源Volume中快照複本的接收者、請在FSxTM上執行下列命令ONTAP ：

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

在來源與目的地磁碟區之間建立**SnapMirror**關係

若要在來源與目的地Volume之間建立SnapMirror關係、請在FSX ONTAP Sf2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。此程序會啟動從來源磁碟區產生的新快照、並將其複製到目的地磁碟區。

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

在**SnapCenter** 內部部署及設定**Windows**靜態伺服器。

在**SnapCenter** 內部部署**Windows**功能伺服器

此解決方案使用NetApp SnapCenter 解決方案來執行SQL Server和Oracle資料庫的應用程式一致備份。搭配使用Veeam備份與複寫來備份虛擬機器VMDK、可為內部部署與雲端型資料中心提供全方位的災難恢復解決方案。

NetApp支援網站提供支援軟體、可安裝在位於網域或工作群組的Microsoft Windows系統上。SnapCenter 如需詳細的規劃指南和安裝指示、請參閱 "NetApp文件中心"。

您可SnapCenter 從取得此軟體 "此連結"。

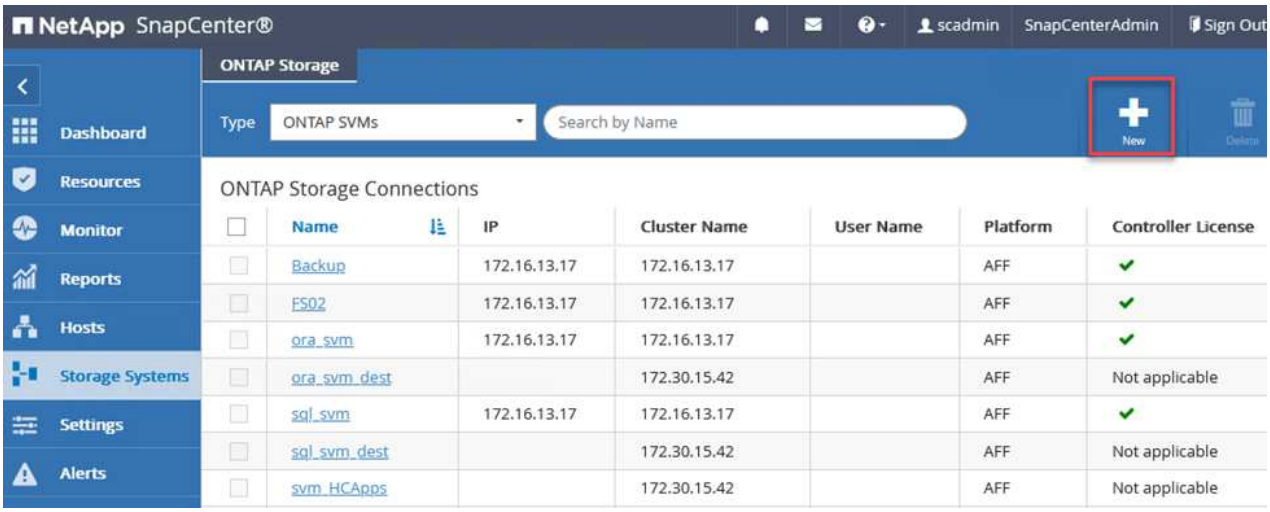
安裝完畢後、您可以SnapCenter 使用_\https://Virtual_Cluster_IP_or_FQDN:8146_從網頁瀏覽器存取此功能。

登入主控台之後、您必須設定SnapCenter 支援備份SQL Server和Oracle資料庫的功能。

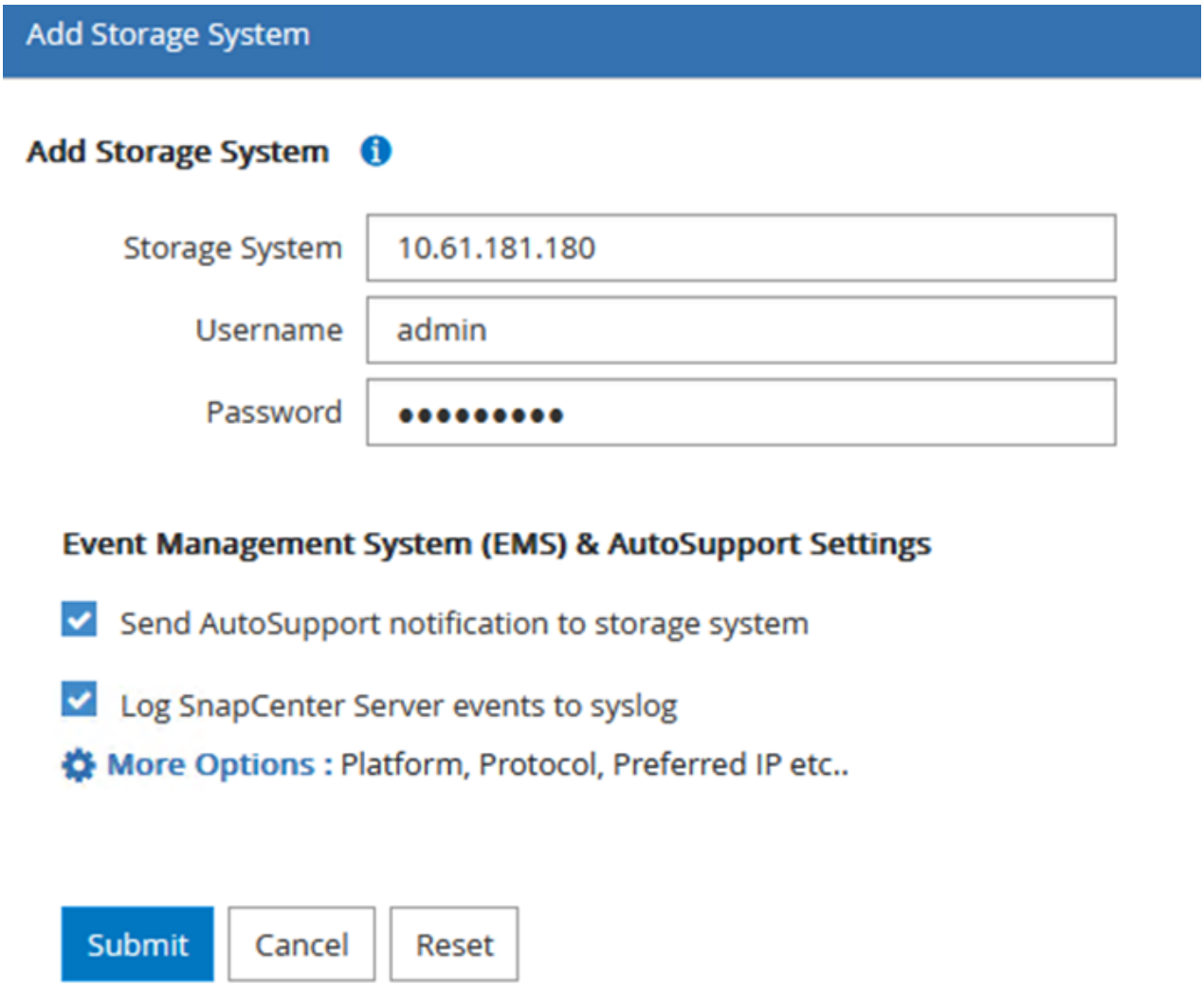
將儲存控制器新增**SnapCenter** 至

若要將儲存控制器新增SnapCenter 至效益區、請完成下列步驟：

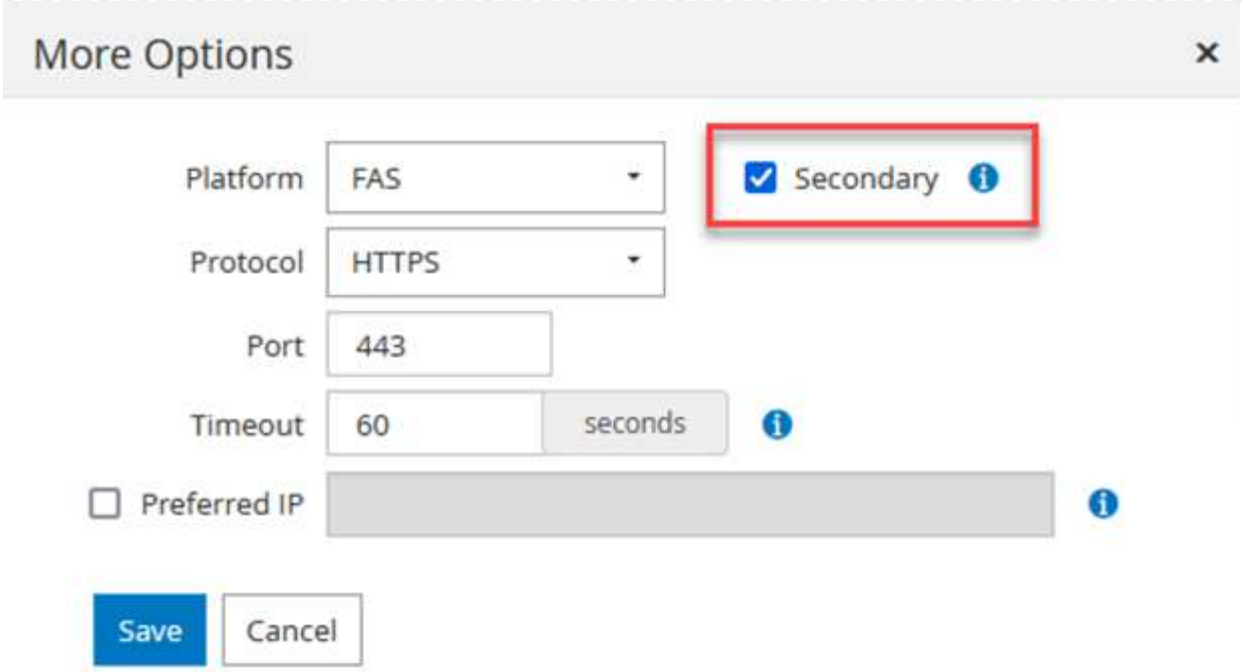
1. 從左功能表中選取「Storage Systems（儲存系統）」、然後按一下「New（新增）」開始將儲存控制器新增SnapCenter 至VMware。



2. 在「Add Storage System（新增儲存系統）」對話方塊中、新增本機內部部署ONTAP 的元件叢集的管理IP位址、以及使用者名稱和密碼。然後按一下「提交」開始探索儲存系統。



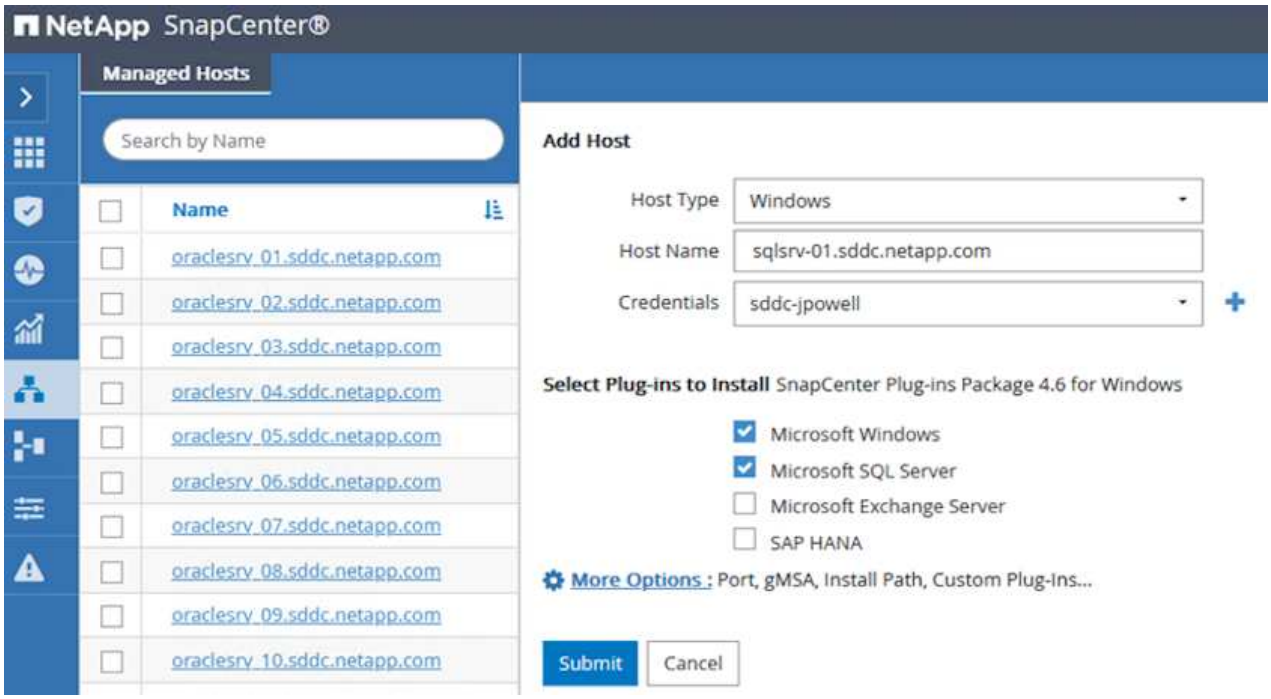
3. 重複此程序、將FSX ONTAP 更新SnapCenter 為支援。在這種情況下、請選取「Add Storage System」（新增儲存系統）視窗底部的「More Options」（更多選項）、然後按一下「Secondary」（次要）核取方塊、將FSX系統指定為使用SnapMirror複本或我們的主要備份快照更新的次要儲存系統。



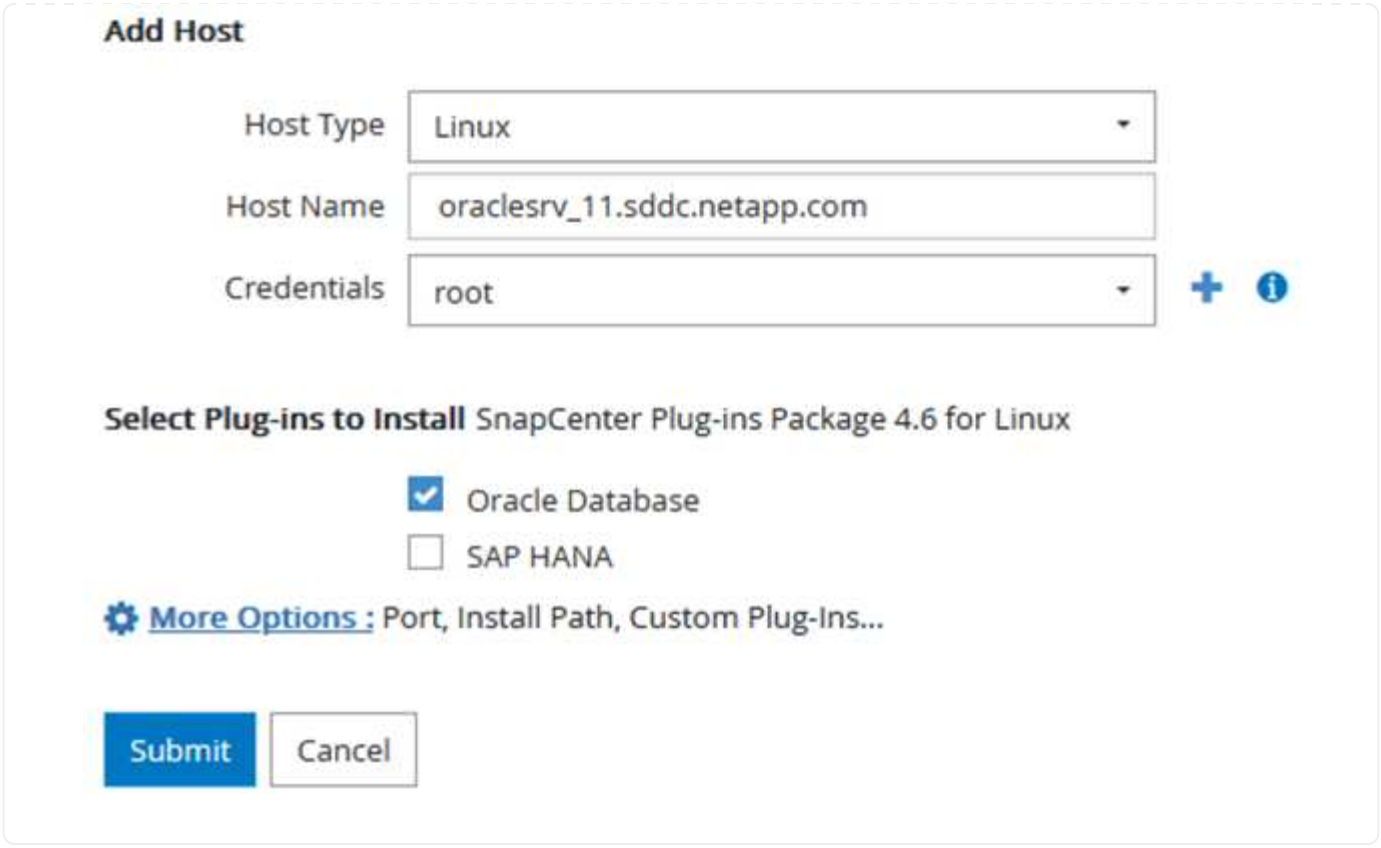
如需將儲存系統新增SnapCenter 至效益管理系統的相關資訊、請參閱文件、網址為 "此連結"。

下一步是將主機應用程式伺服器新增SnapCenter 至SQL Server和Oracle的程序類似。

1. 從左功能表中選取「hosts」、然後按一下「Add（新增）」、開始將儲存控制器新增SnapCenter 至VMware。
2. 在Add hosts（新增主機）視窗中、新增Host Type（主機類型）、Hostname（主機名稱）和主機系統認證。選取外掛程式類型。若為SQL Server、請選取Microsoft Windows和Microsoft SQL Server外掛程式。



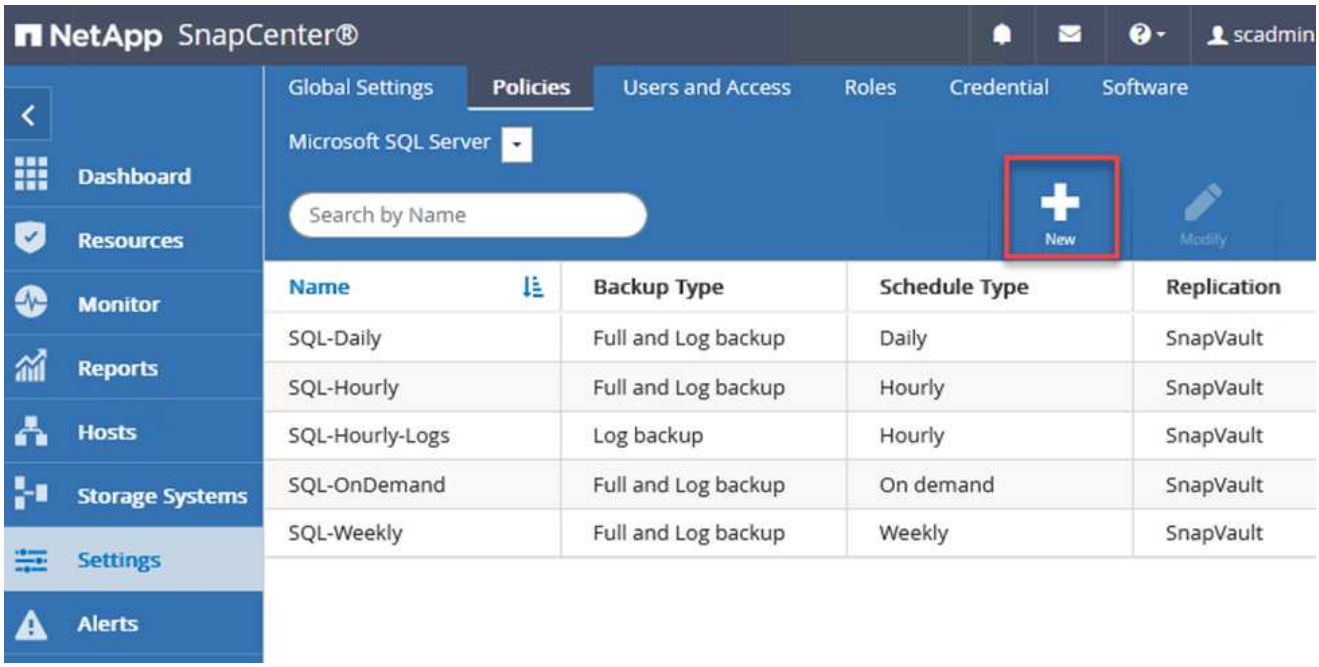
3. 對於Oracle、請在「新增主機」對話方塊中填寫必填欄位、然後選取Oracle資料庫外掛程式的核取方塊。然後按一下「提交」開始探索程序、並將主機新增SnapCenter 至VMware。


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

建立**SnapCenter** 不規則

原則會針對備份工作建立要遵循的特定規則。其中包括但不限於備份排程、複寫類型、SnapCenter 以及如何處理備份和刪節交易記錄。

您可以在SnapCenter 「功能性」（英語）的「設定」（Settings）區段中存取原則。

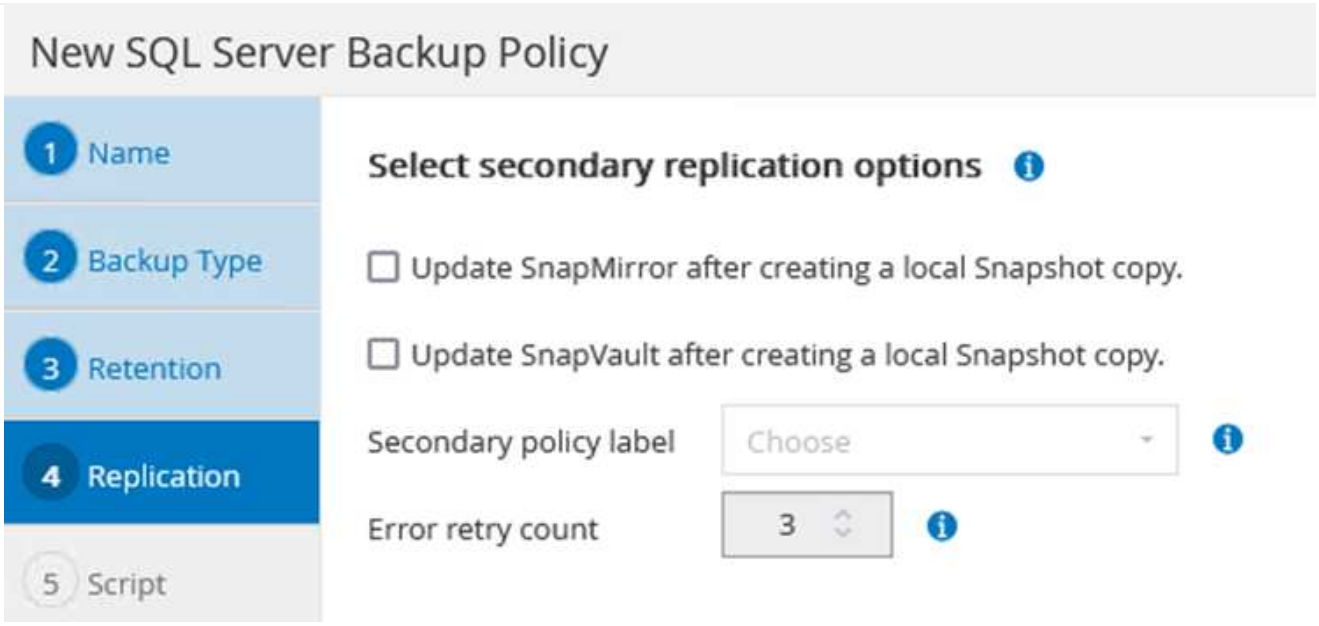


如需建立SQL Server備份原則的完整資訊、請參閱 "本文檔SnapCenter"。

如需建立Oracle備份原則的完整資訊、請參閱 "本文檔SnapCenter"。

- 附註： *
- 當您逐步完成原則建立精靈時、請特別注意「複寫」區段。在本節中、您將說明您要在備份程序中取得的次要SnapMirror複本類型。
- 「建立本機Snapshot複本後再更新SnapMirror」設定是指當位於同一個叢集上的兩個儲存虛擬機器之間存在SnapMirror關係時、更新SnapMirror關係。
- 「建立SnapVault 本機快照複本後更新功能」設定可用來更新兩個獨立叢集之間、內部部署ONTAP的SnapMirror系統與Cloud Volumes ONTAP BIOS或FSxN之間存在的SnapMirror關係。

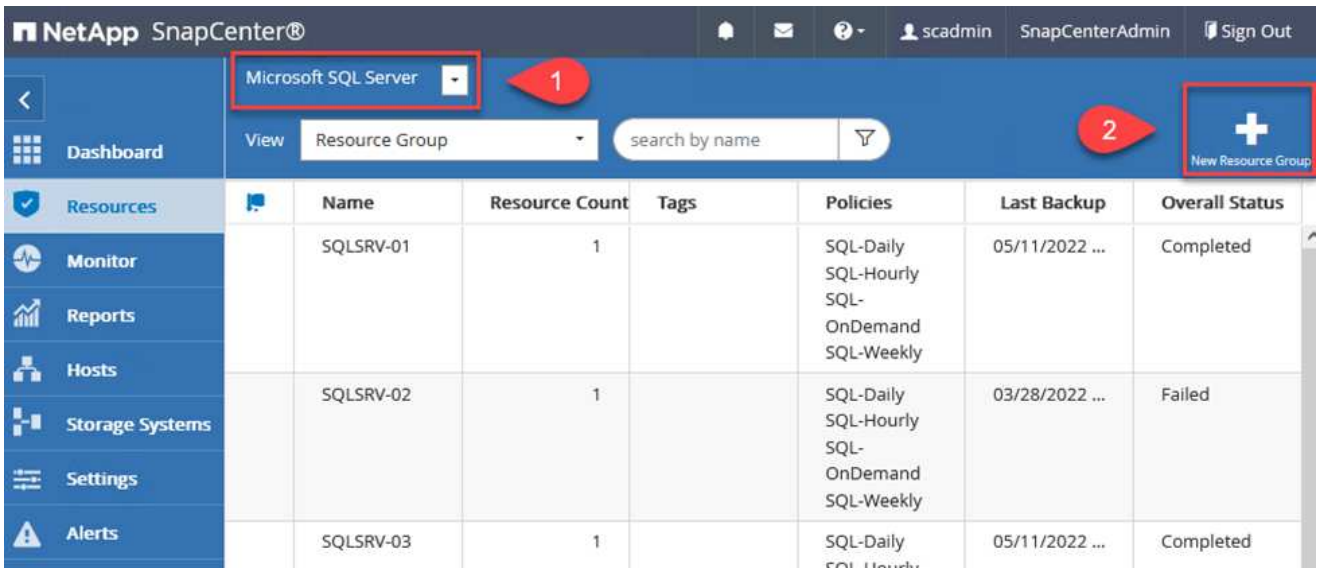
下圖顯示上述選項、以及它們在備份原則精靈中的外觀。



建立**SnapCenter** 資源群組

資源群組可讓您選取要納入備份的資料庫資源、以及這些資源所遵循的原則。

1. 前往左側功能表的「資源」區段。
2. 在視窗頂端、選取要使用的資源類型（在此情況下是Microsoft SQL Server）、然後按一下「New Resource Group（新資源群組）」。



本《支援》文件涵蓋SnapCenter 建立SQL Server和Oracle資料庫資源群組的逐步詳細資料。

如需備份SQL資源、請遵循 "此連結"。

如需備份Oracle資源、請遵循 "此連結"。

部署及設定**Veeam**備份伺服器

解決方案中使用Veeam備份與複寫軟體來備份應用程式虛擬機器、並使用Veeam橫向擴充備份儲存庫（SOBR）將備份複本歸檔至Amazon S3儲存庫。在本解決方案中、Veeam部署於Windows伺服器上。如需部署Veeam的具體指引、請參閱 "Veeam說明中心技術文件"。

設定**Veeam**橫向擴充備份儲存庫

在您部署並授權軟體之後、您可以建立橫向擴充備份儲存庫（SOBR）作為備份工作的目標儲存設備。您也應該將S3儲存區納入異地備份VM資料、以便進行災難恢復。

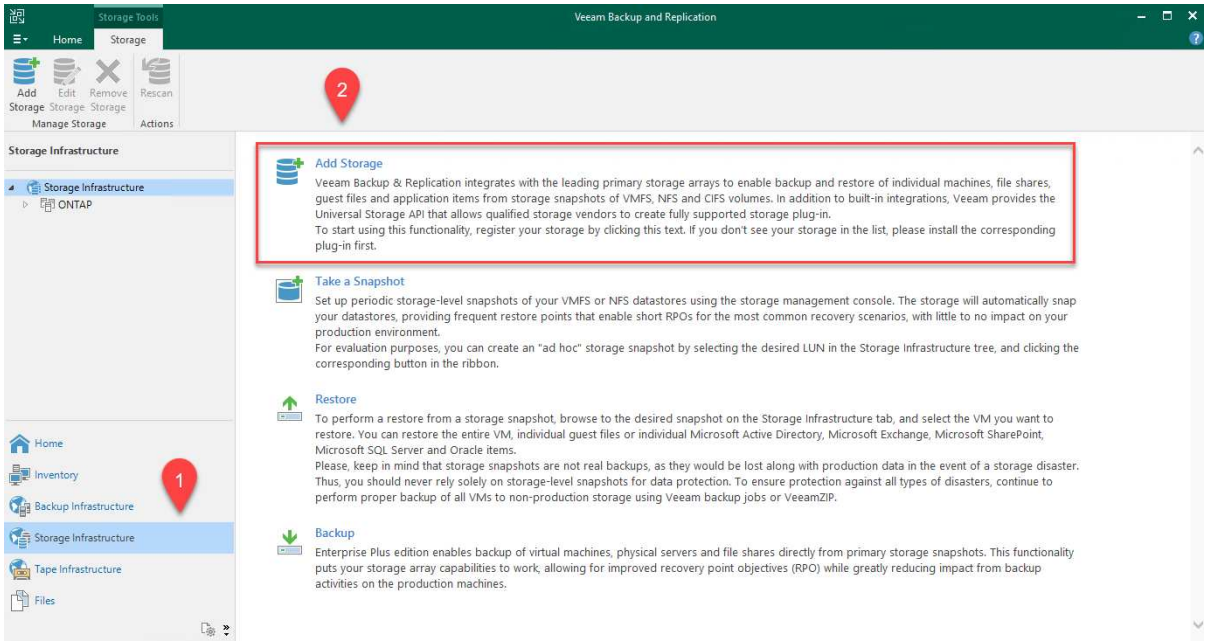
請先參閱下列必要條件、再開始使用。

1. 在內部部署ONTAP 的支援系統上建立SMB檔案共用區、做為備份的目標儲存設備。
2. 建立Amazon S3儲存庫以納入SOBR。這是用於異地備份的儲存庫。

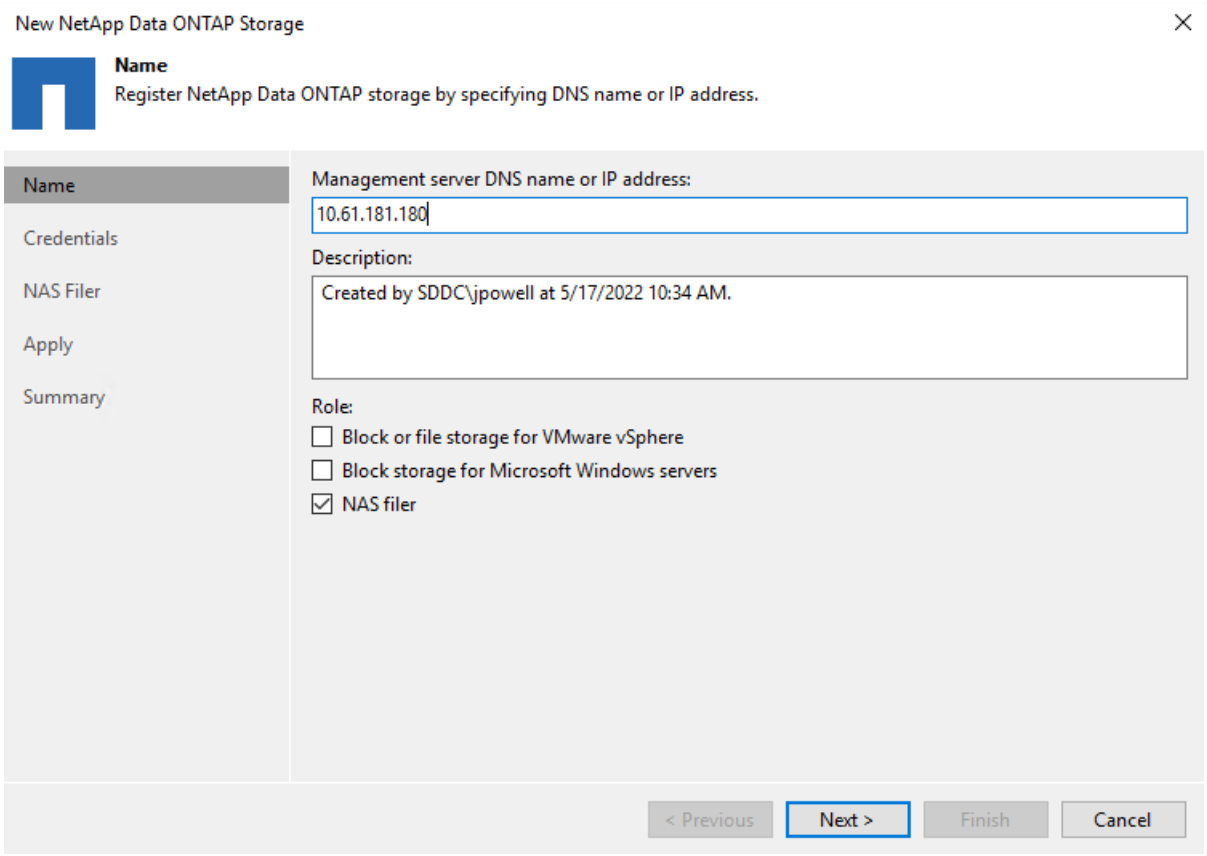
新增**ONTAP** 功能至**Veeam**

首先、在ONTAP Veeam中新增功能不支援的儲存叢集和相關的SMB/NFS檔案系統作為儲存基礎架構。

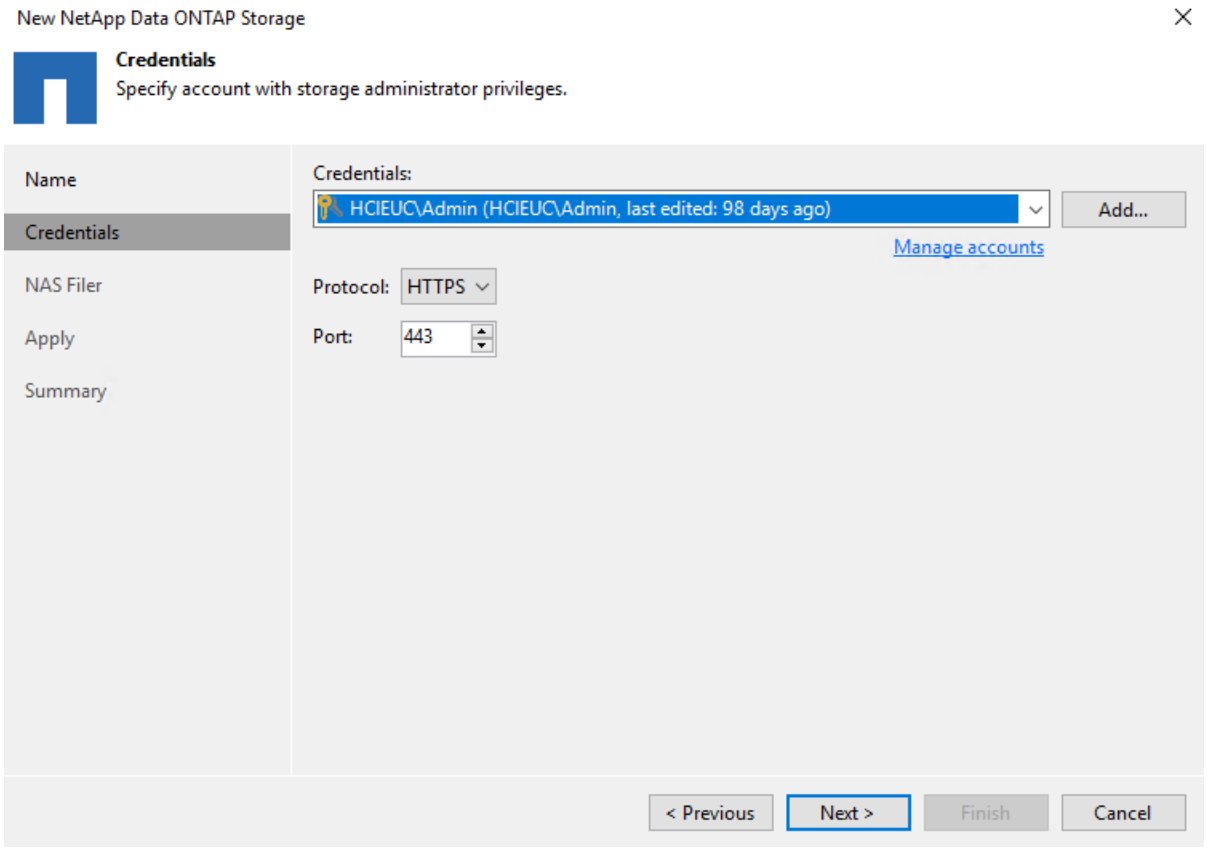
1. 開啟Veeam主控台並登入。瀏覽至Storage Infrastructure、然後選取Add Storage。



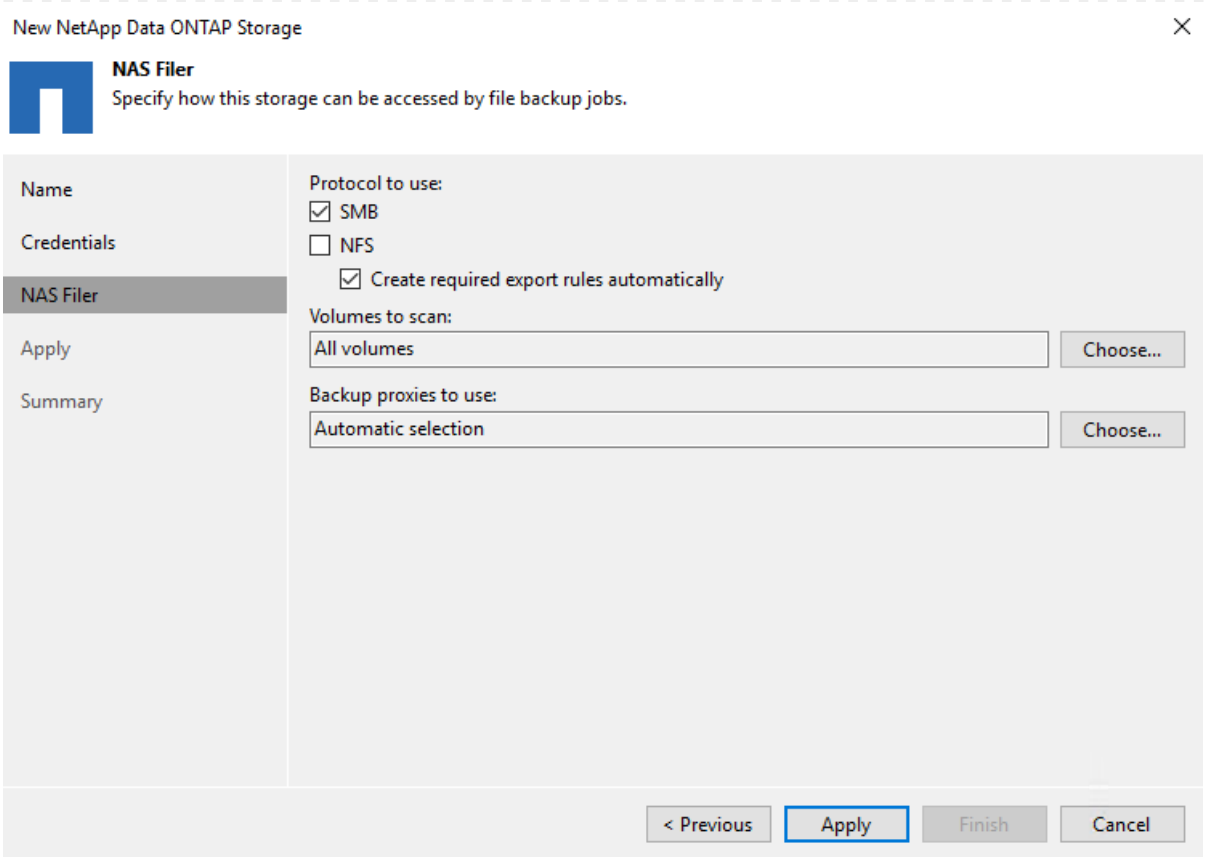
2. 在「Add Storage（新增儲存設備）」精靈中、選取NetApp作為儲存設備廠商、然後選取Data ONTAP 「NetApp」。
3. 輸入管理IP位址、然後勾選NAS Filer方塊。按一下「下一步」



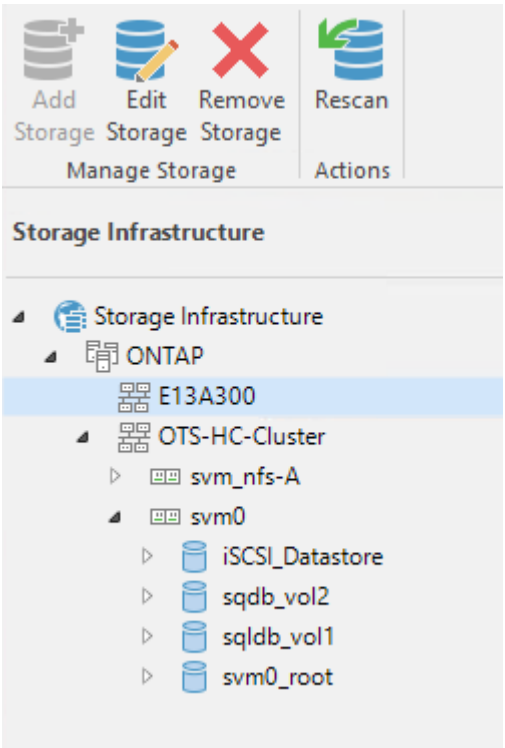
4. 新增您的認證資料以存取ONTAP 整個叢集。



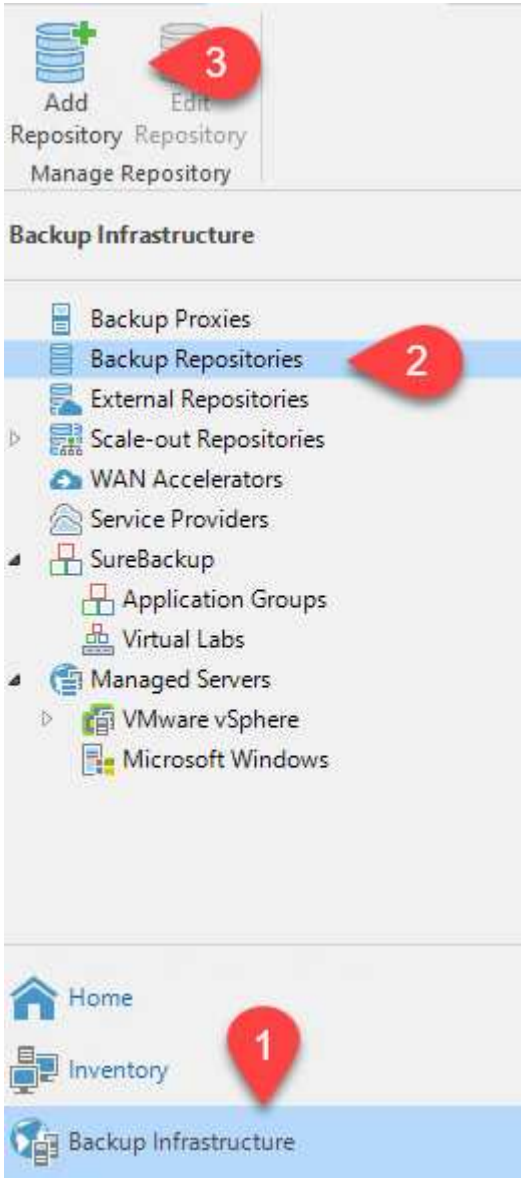
5. 在NAS FilerTM頁面上、選擇所需的掃描傳輸協定、然後選取Next（下一步）。



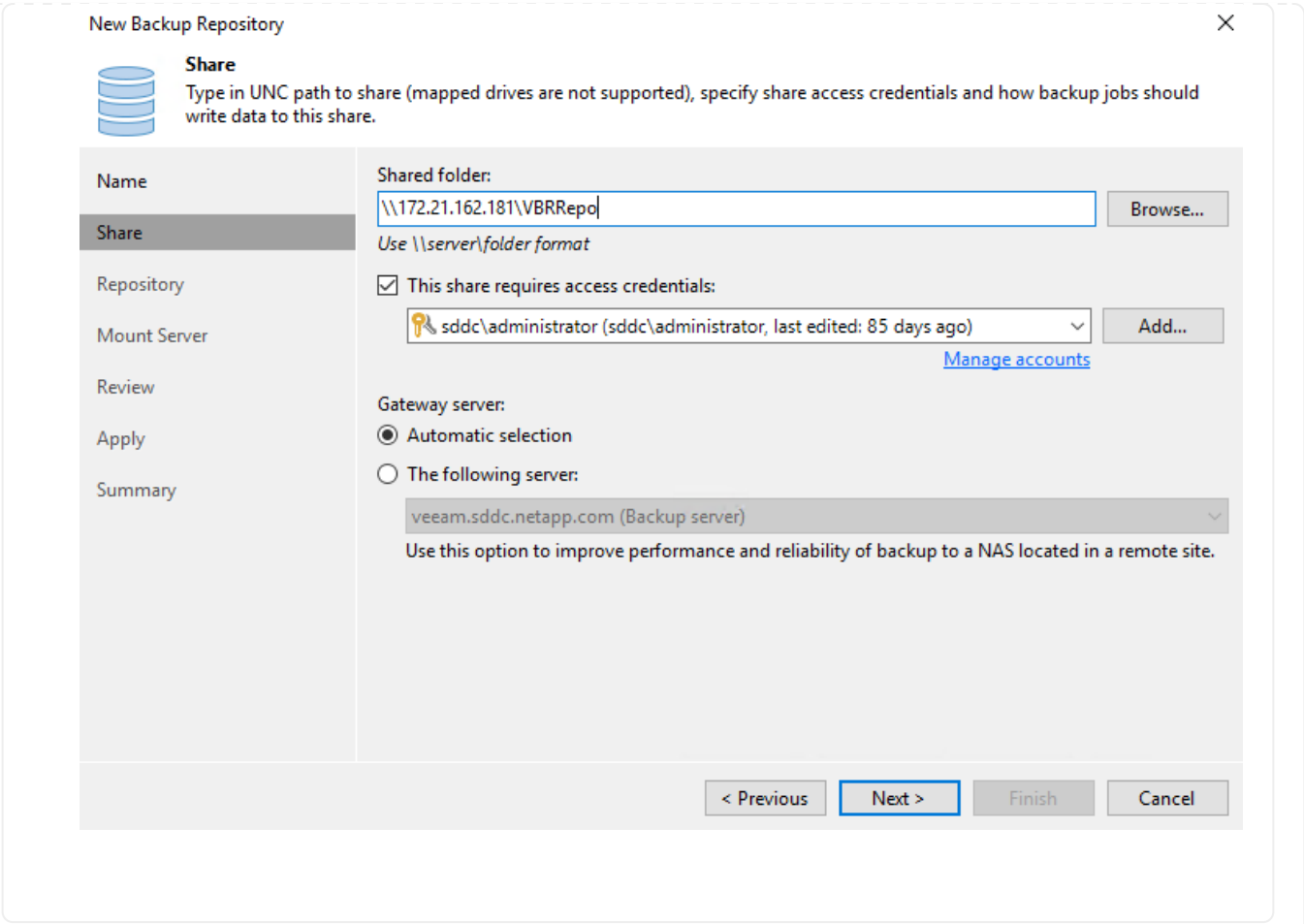
6. 完成精靈的「Apply（套用）」和「Summary（摘要）」頁面、然後按一下「Finish（完成）」開始儲存探索程序。掃描完成後、ONTAP 即可將支援此功能的叢集與NAS檔案管理器一起新增為可用資源。



7. 使用新發現的NAS共用區建立備份儲存庫。從備份基礎架構選取備份儲存庫、然後按一下新增儲存庫功能表項目。



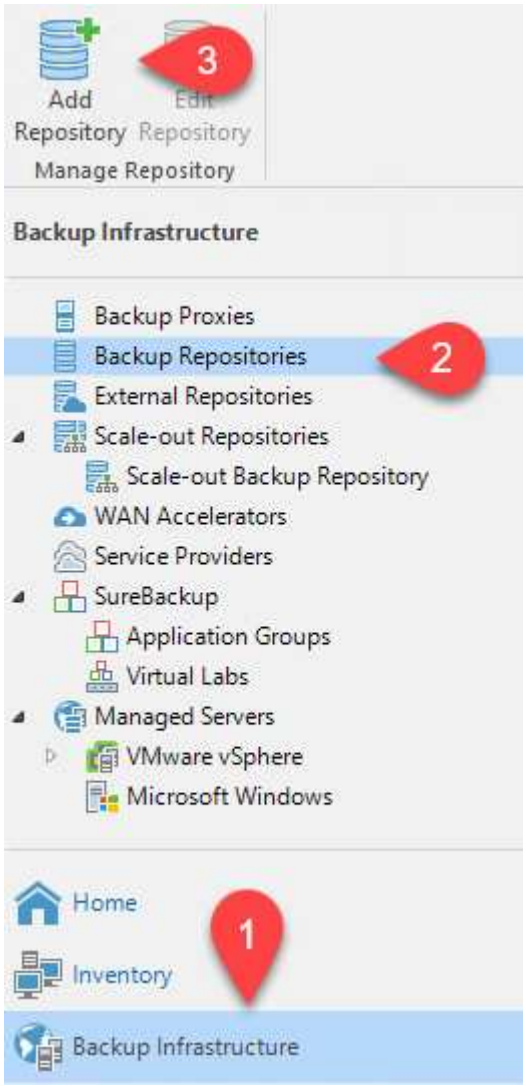
8. 請依照「新備份儲存庫精靈」中的所有步驟來建立儲存庫。如需建立Veeam備份儲存庫的詳細資訊、請參閱 "Veeam文件"。


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

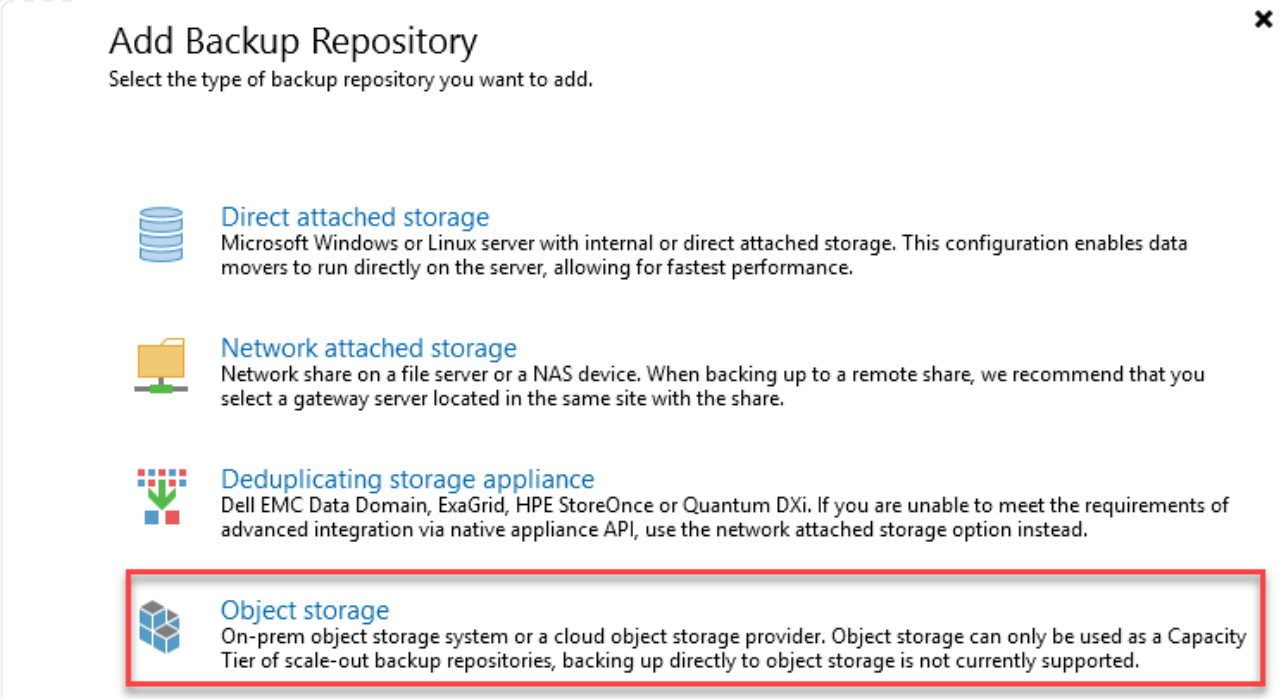
將**Amazon S3**儲存庫新增為備份儲存庫

下一步是將Amazon S3儲存設備新增為備份儲存庫。

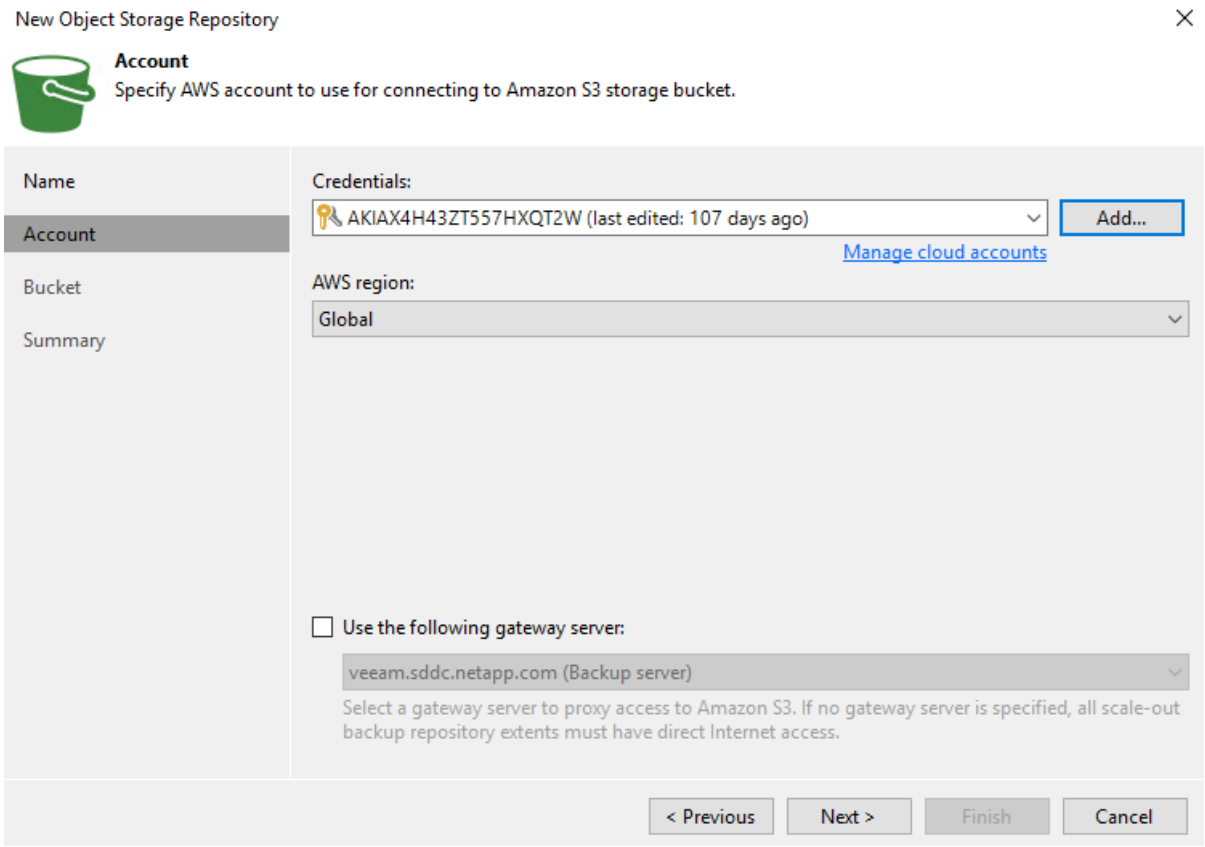
1. 瀏覽至「備份基礎架構」>「備份儲存庫」。按一下新增儲存庫。



2. 在「新增備份儲存庫」精靈中、選取「物件儲存設備」、然後選取「Amazon S3」。這會啟動「新增物件儲存庫」精靈。



3. 提供物件儲存庫的名稱、然後按「Next（下一步）」。
4. 在下一節中、提供您的認證資料。您需要AWS存取金鑰和秘密金鑰。

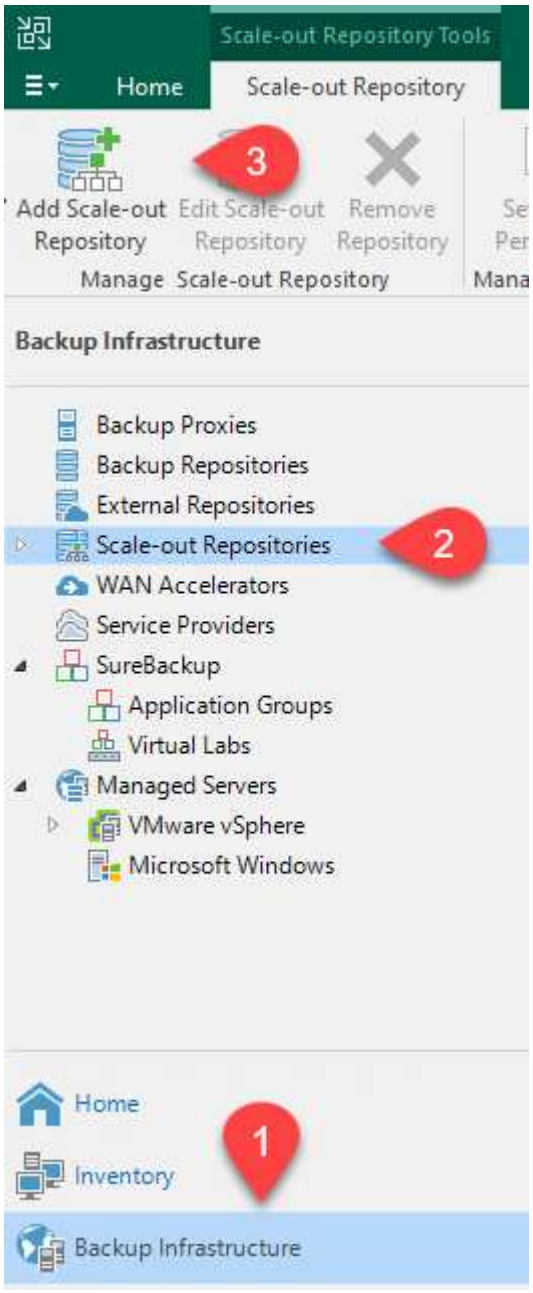


5. Amazon組態載入後、請選擇您的資料中心、儲存庫和資料夾、然後按一下「Apply（套用）」。最後、按一下「完成」以關閉精靈。

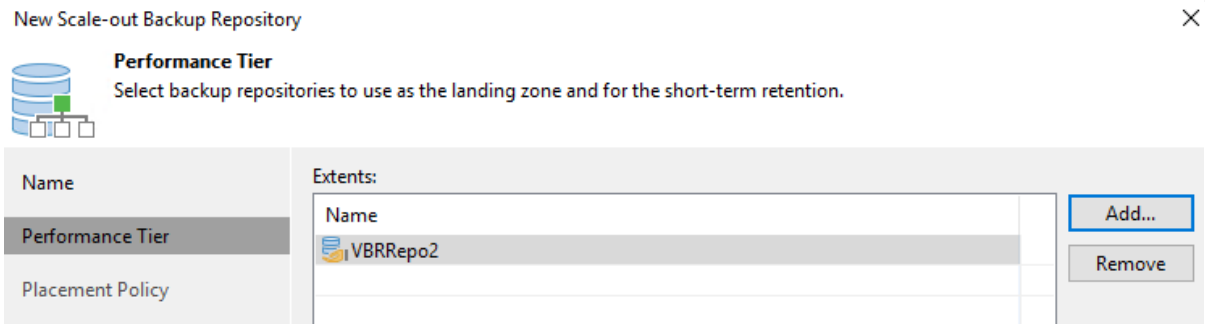
建立橫向擴充備份儲存庫

現在我們已將儲存儲存庫新增至Veeam、我們可以建立SOBR、將備份複本自動分層至異地Amazon S3物件儲存設備、以進行災難恢復。

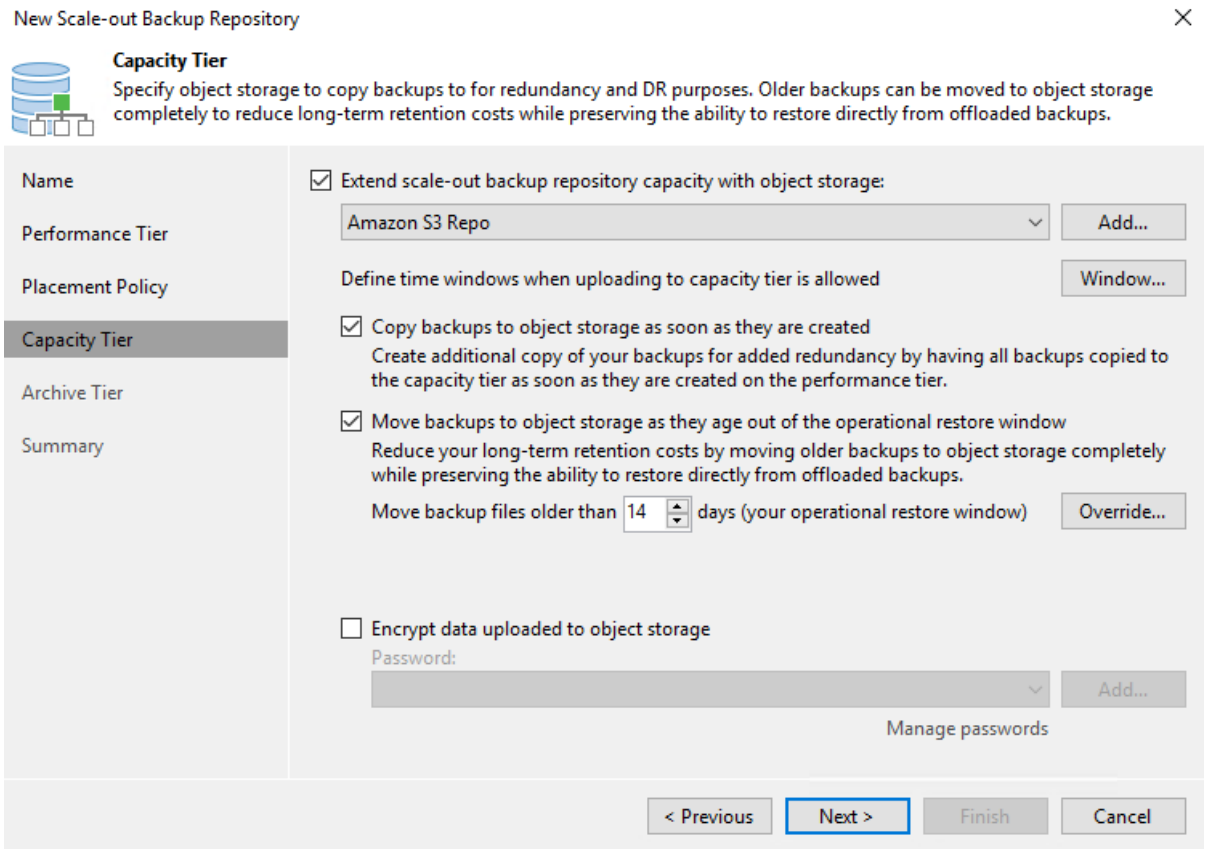
1. 從備份基礎架構選取橫向擴充儲存庫、然後按一下新增橫向擴充儲存庫功能表項目。



2. 在「新增橫向擴充備份儲存庫」中、提供SOBR名稱、然後按「下一步」。
3. 對於效能層、請選擇包含SMB共用的備份儲存庫、該SMB共用位於本機ONTAP 的資訊區叢集上。



4. 針對「放置原則」、請根據您的需求選擇「資料位置」或「效能」。選取「下一步」。
5. 在容量層方面、我們將SOBR延伸至Amazon S3物件儲存設備。為了進行災難恢復、請在建立備份後立即選取「複製備份到物件儲存設備」、以確保我們的次要備份能夠及時交付。



6. 最後、選取「Apply（套用）」和「Finish（完成）」以完成建立SOBR。

建立橫向擴充備份儲存庫工作

設定Veeam的最後步驟、是使用新建立的SOBR作為備份目的地來建立備份工作。建立備份工作是任何儲存系統管理員的常用程序、我們不在此詳述詳細步驟。如需在Veeam中建立備份工作的完整資訊、請參閱 "Veeam說明中心技術文件"。

BlueXP 備份與還原工具與組態

若要將應用程式VM和資料庫Volume容錯移轉至執行於AWS的VMware Cloud Volume服務、您必須同時安裝SnapCenter 並設定執行中的VMware Server和Veeam備份與複寫伺服器執行個體。容錯移轉完成後、您也必須設定這些工具、以便恢復正常的備份作業、直到規劃並執行內部部署資料中心的容錯回復為止。

部署次要**Windows SnapCenter** 功能伺服器

支援VMware Cloud SDDC部署的VMware伺服器、或安裝在VPC中的EC2執行個體上、並可透過網路連線至VMware Cloud環境。SnapCenter

NetApp支援網站提供支援軟體、可安裝在位於網域或工作群組的Microsoft Windows系統上。SnapCenter 如需詳細的規劃指南和安裝指示、請參閱 "NetApp文件中心"。

您可以在找到SnapCenter 該軟件 "此連結"。

設定次要**Windows SnapCenter** 靜態伺服器

若要還原鏡射至FSXS庫ONTAP 的應用程式資料、您必須先執行內部部署SnapCenter 的整套還原資料庫。完成此程序後、將重新建立與VM的通訊、並使用FSX還原ONTAP 做為主要儲存設備來恢復應用程式備份。

若要達成此目標、您必須在SnapCenter the努力伺服器上完成下列項目：

1. 將電腦名稱設定為與原始內部部署SnapCenter 的內部部署伺服器相同。
2. 設定網路功能、以便與VMware Cloud和FSX ONTAP 支援例項進行通訊。
3. 完成還原SnapCenter 整套程序以還原整個資料庫。
4. 確認SnapCenter 支援功能為災難恢復模式、以確保FSX現在是備份的主要儲存設備。
5. 確認已與還原的虛擬機器重新建立通訊。

部署次要**Veeam**備份與擴大機；複寫伺服器

您可以將Veeam備份與複寫伺服器安裝在AWS或EC2執行個體上VMware Cloud的Windows伺服器上。如需詳細的實作指南、請參閱 "Veeam說明中心技術文件"。

設定次要**Veeam**備份與擴大機；複寫伺服器

若要還原已備份至Amazon S3儲存設備的虛擬機器、您必須在Windows伺服器上安裝Veeam伺服器、並將其設定為與VMware Cloud、FNSX ONTAP 及包含原始備份儲存庫的S3儲存庫進行通訊。此外、還必須在FSX ONTAP 更新上設定新的備份儲存庫、以便在VM還原後進行新的備份。

若要執行此程序、必須完成下列項目：

1. 設定網路功能、以便與VMware Cloud、FSX ONTAP 功能區及內含原始備份儲存庫的S3儲存區進行通訊。
2. 將FSXSf2 ONTAP 上的SMB共用區設定為新的備份儲存庫。
3. 將原本作為橫向擴充備份儲存庫一部分的S3儲存庫掛載到內部部署。
4. 還原VM之後、請建立新的備份工作來保護SQL和Oracle VM。

如需使用Veeam還原VM的詳細資訊、請參閱一節 "使用Veeam完整還原還原應用程式VM"。

適用於災難恢復的資料庫備份**SnapCenter**

支援基礎MySQL資料庫及組態資料的備份與還原、以便在發生災難時恢復該伺服器。SnapCenter SnapCenter就我們的解決方案而言、我們在SnapCenter VPC內的AWS EC2執行個體上恢復了該資料庫和組態。如需此步驟的詳細資訊、請參閱 "此連結"。

支援需求**SnapCenter**

下列先決條件是SnapCenter 進行資訊備份所需的條件：

- 在內部部署ONTAP 的支援系統上建立一個Volume和SMB共用區、以找出備份的資料庫和組態檔案。
- 內部部署ONTAP 的SnapMirror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SnapCenter 的還原資料庫和組態檔案的快照。
- 安裝在雲端帳戶的Windows Server、可安裝在EC2執行個體或VMware Cloud SDDC的VM上。
- 安裝在Windows EC2執行個體或VMware Cloud VM上的SnapCenter

支援備份與還原程序摘要**SnapCenter**

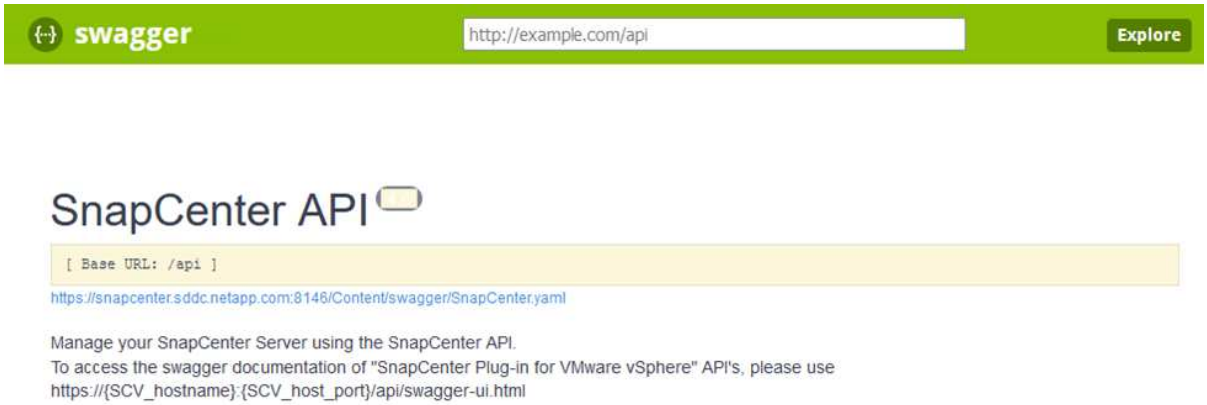
- 在內部部署ONTAP 的內部系統上建立一個磁碟區、以裝載備份資料庫和組態檔案。
- 在內部部署與FSx/CVO之間建立SnapMirror關係。
- 掛載SMB共用區。
- 擷取Swagger授權權杖以執行API工作。
- 啟動資料庫還原程序。
- 使用xcopy公用程式將資料庫和組態檔案本機目錄複製到SMB共用區。
- 在FSX上、建立ONTAP 一個Clone of the Sf2 Volume（透過內部部署的SnapMirror複製）。
- 將SMB共用區從FSX掛載至EC2/VMware Cloud。
- 將還原目錄從SMB共用複製到本機目錄。
- 從Swagger執行SQL Server還原程序。

支援執行REST API命令的Web用戶端介面。SnapCenter如需透過Swagger存取REST API的相關資訊、請參閱SnapCenter 上的《》文件 "此連結"。

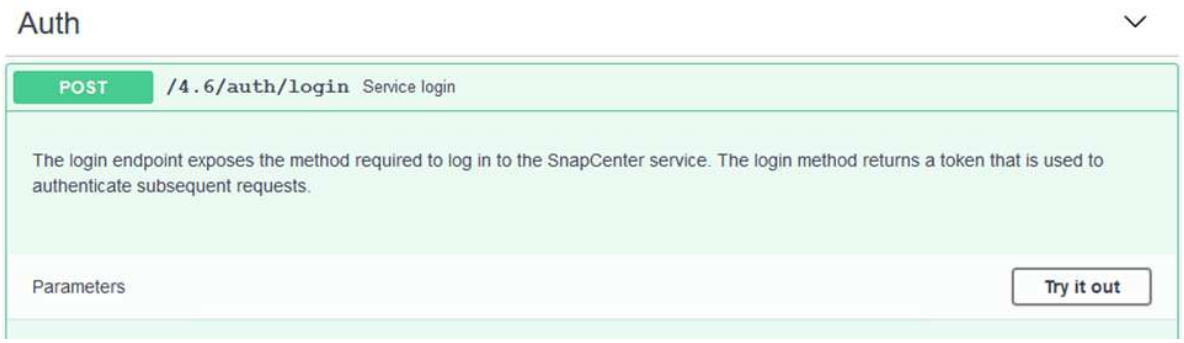
登入**Swagger**並取得授權權杖

瀏覽至Swagger頁面後、您必須擷取授權權杖、才能啟動資料庫還原程序。

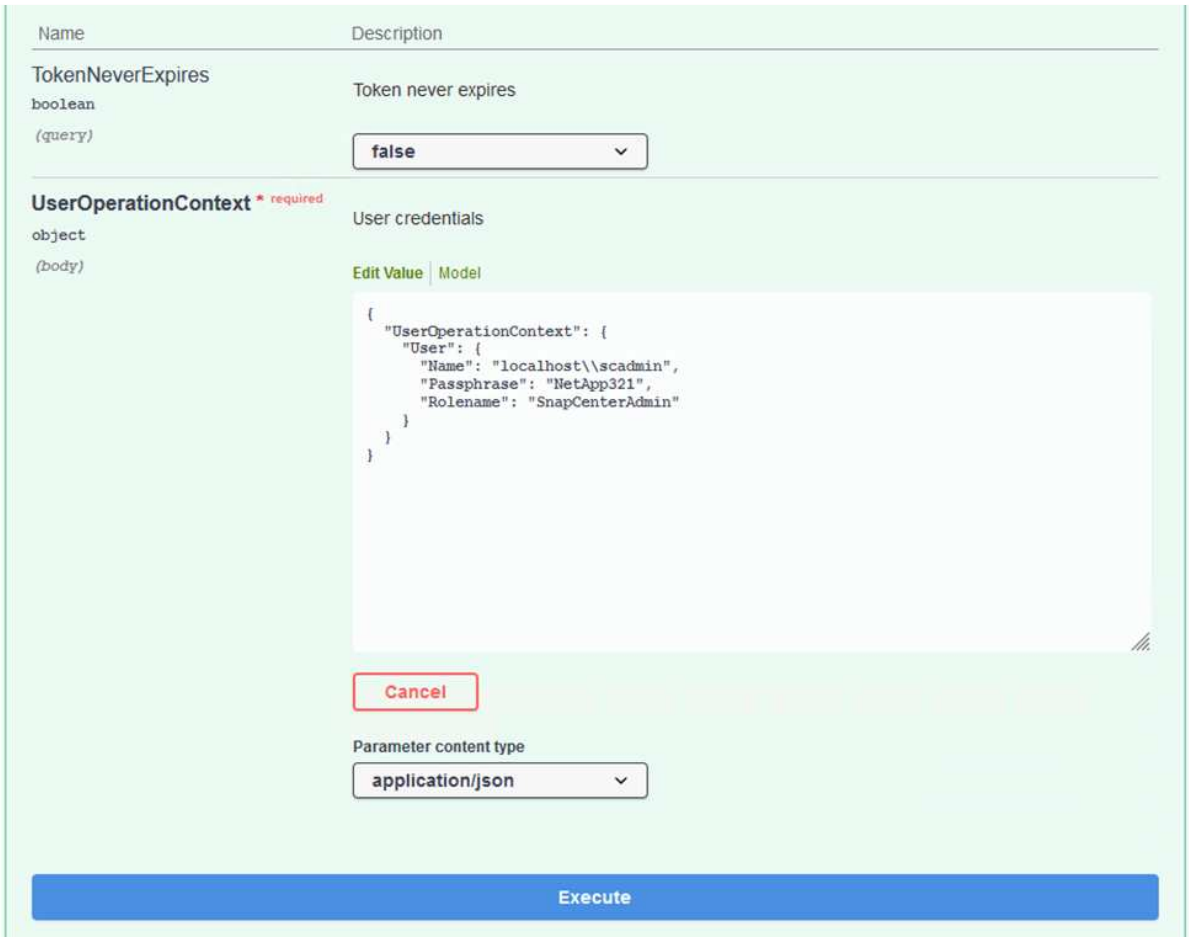
1. 請至SnapCenter https://<SnapCenter伺服器IP：8146/swagger/_存取《Seswagger API》網頁。



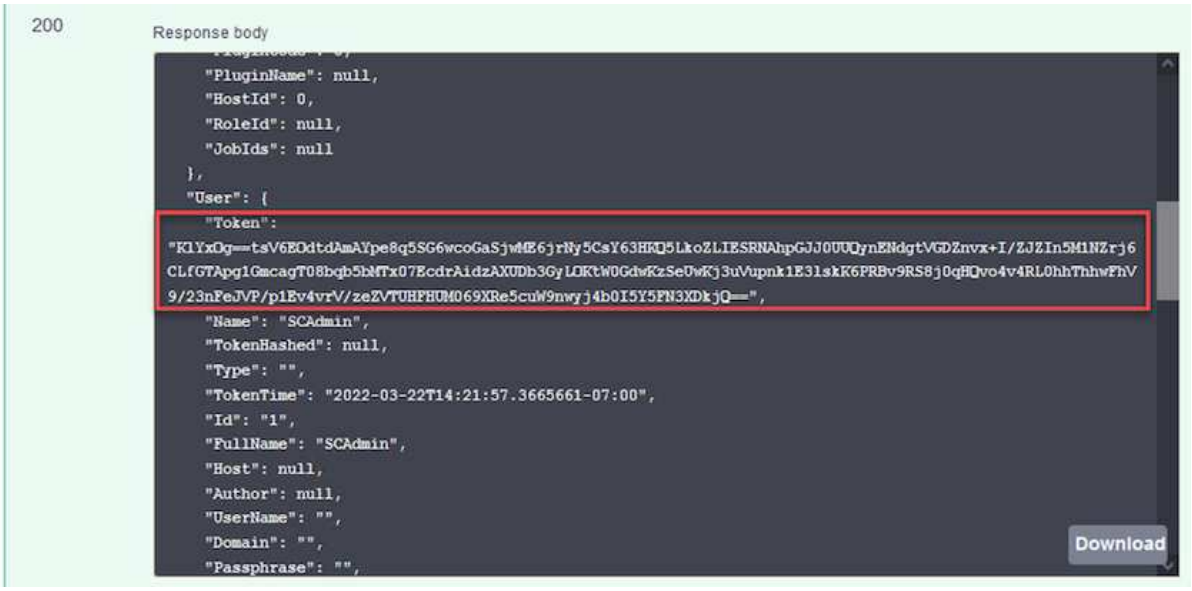
2. 展開「驗證」區段、然後按一下「試用」。



3. 在UserOperationConttext區域中、填入SnapCenter 「資訊」認證和角色、然後按一下「執行」。



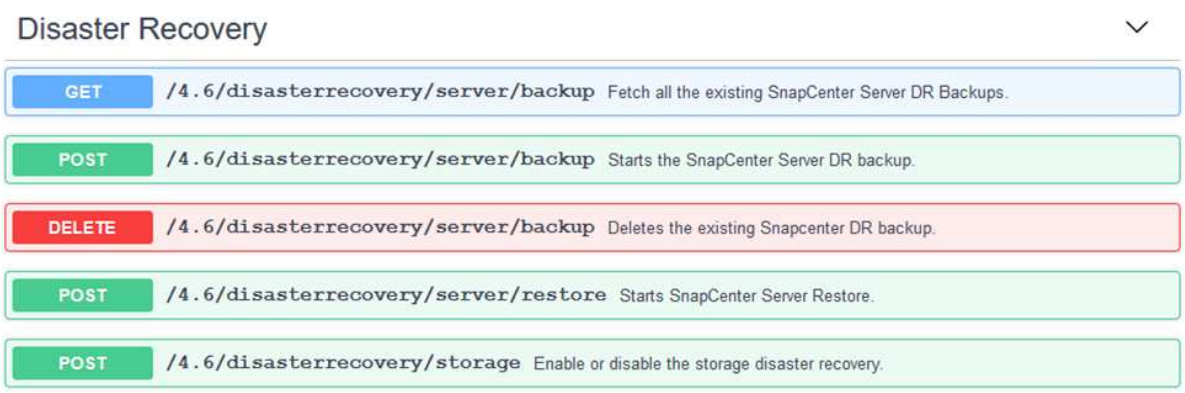
4. 在下方的「回應」本文中、您可以看到權杖。執行備份程序時、請複製權杖文字以進行驗證。



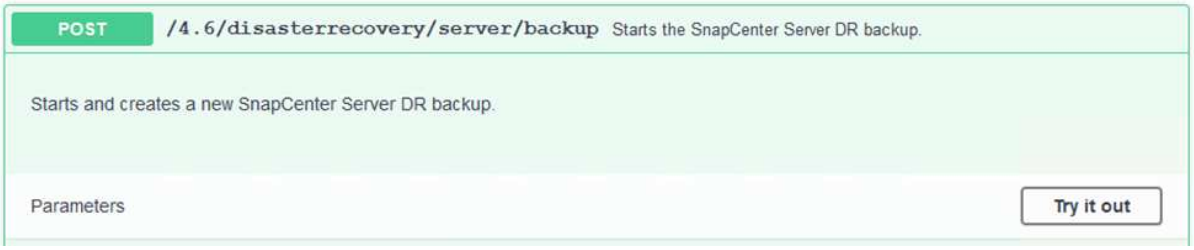
執行**SnapCenter** 資料庫的還原備份

接下來前往Swagger頁面上的Disaster Recovery區域、開始SnapCenter 執行VMware還原程序。

1. 按一下「Disaster Recovery（災難恢復）」區域即可展開。

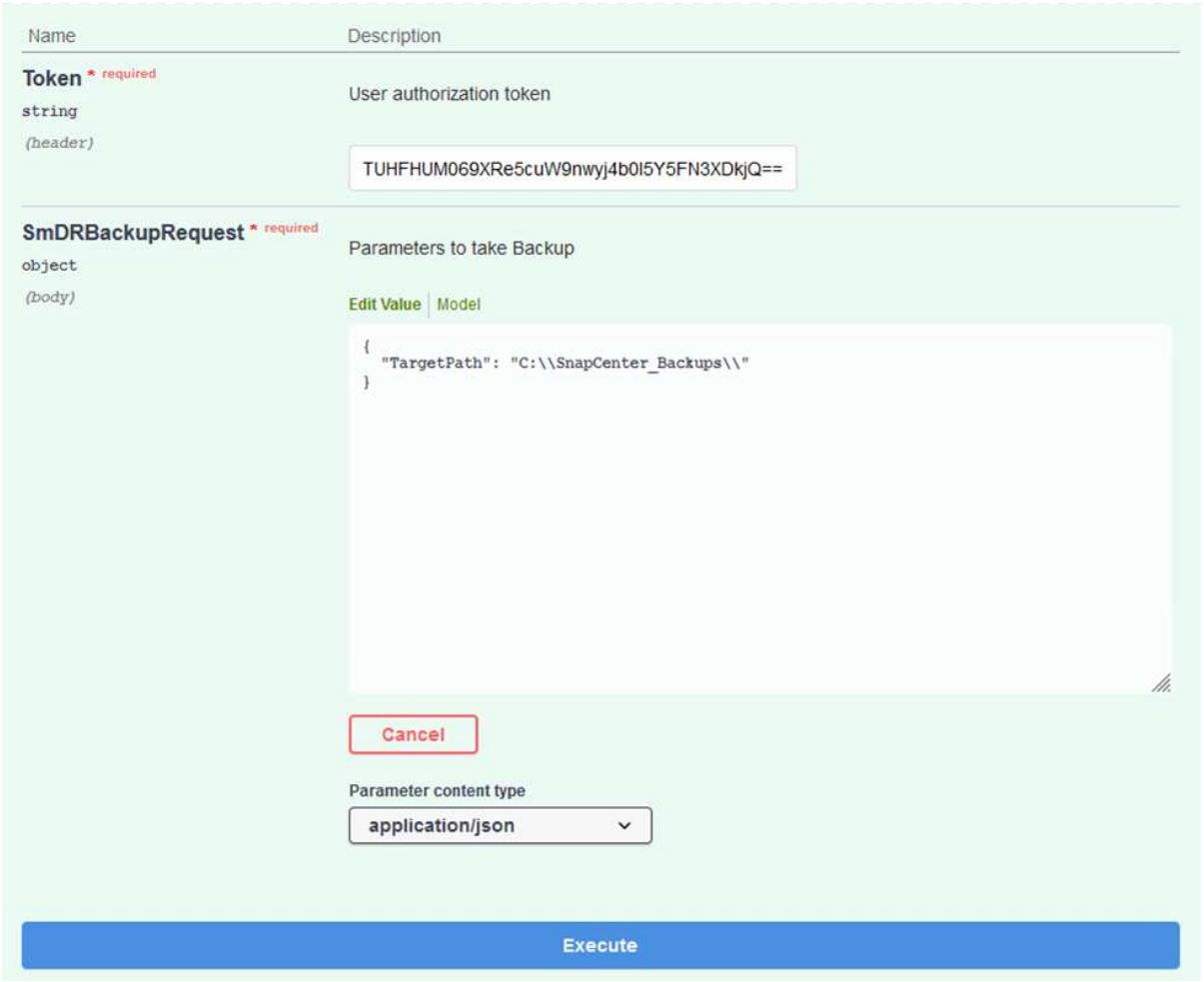


2. 展開「/4.6/dissterrecovery /server/Backup」區段、然後按一下「Try it out（試用）」。



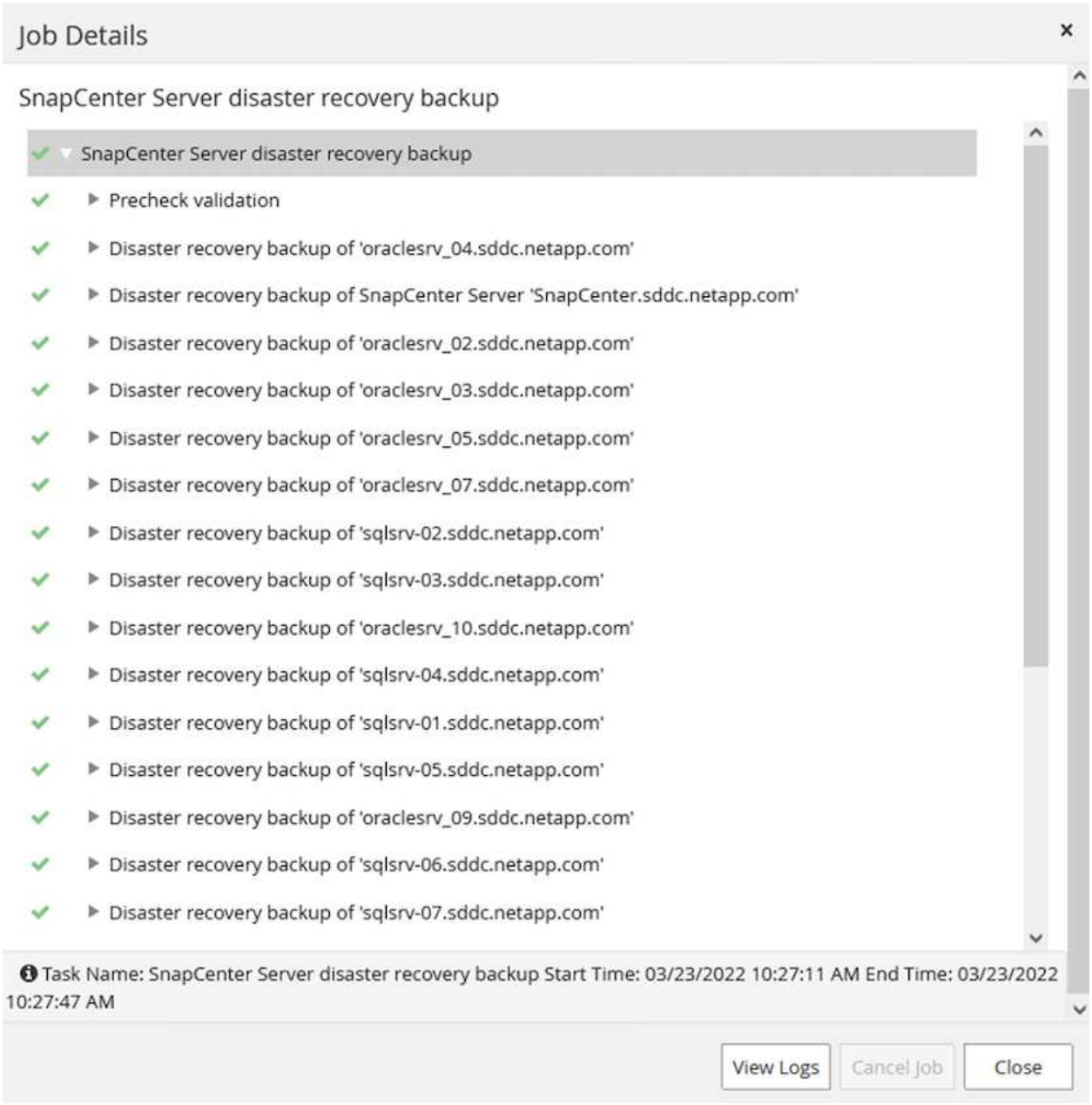
3. 在「SmDRBackup Request」區段中、新增正確的本機目標路徑、然後選取「執行」以開始SnapCenter 備份整個過程中的資料庫和組態。

備份程序不允許直接備份到NFS或CIFS檔案共用區。


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

從**SnapCenter** 無法監控備份工作

登入SnapCenter 功能以在開始資料庫還原程序時檢閱記錄檔。在「Monitor（監控）」區段下、您可以檢視SnapCenter 有關支援伺服器災難恢復備份的詳細資料。



使用**XCOPY**公用程式將資料庫備份檔案複製到**SMB**共用區

接下來、您必須將備份從SnapCenter 位於支援服務器上的本機磁碟機移至CIFS共用區、以便SnapMirror將資料複製到位於AWS FSX執行個體上的次要位置。使用xcopy搭配保留檔案權限的特定選項。

以系統管理員身分開啟命令提示字元。在命令提示字元中輸入下列命令：

```
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
```

容錯移轉

災難發生在主站台

如果發生在一線內部部署資料中心的災難、我們的案例包括使用AWS上的VMware Cloud、將容錯移轉到位於Amazon Web Services基礎架構上的二線站台。我們假設虛擬機器和內部部署ONTAP 的VMware叢集已無法再存取。此外SnapCenter 、無法再存取VMware和Veeam虛擬機器、而且必須在我們的次要站台上重建。

本節說明將基礎架構容錯移轉至雲端、並涵蓋下列主題：

- 還原資料庫。SnapCenter建立新SnapCenter 的支援伺服器之後、請還原MySQL資料庫和組態檔案、並將資料庫切換為災難恢復模式、以便次要FSX儲存設備成為主要儲存設備。
- 使用Veeam備份與複寫還原應用程式虛擬機器。連接內含VM備份的S3儲存設備、匯入備份、然後將其還原至AWS上的VMware Cloud。
- 使用SnapCenter 支援功能還原SQL Server應用程式資料。
- 使用SnapCenter 支援功能還原Oracle應用程式資料。

資料庫還原程序**SnapCenter**

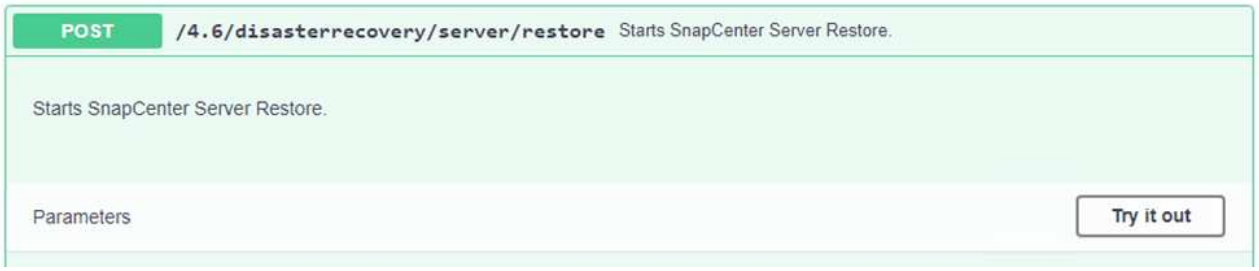
支援災難恢復案例、可備份及還原MySQL資料庫和組態檔案。SnapCenter這可讓管理員在SnapCenter 內部部署資料中心維持對該資料庫的定期備份、並於稍後將該資料庫還原至次要SnapCenter 的還原資料庫。

若要存取SnapCenter 遠端SnapCenter 還原伺服器上的還原備份檔案、請完成下列步驟：

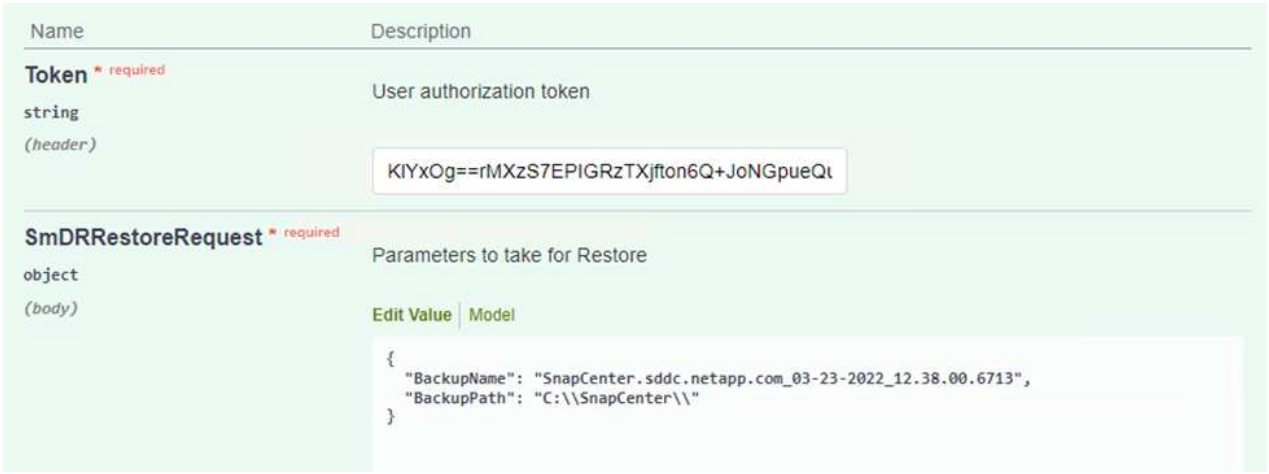
1. 中斷來自FSX叢集的SnapMirror關係、這會使磁碟區變成讀取/寫入。
2. 建立CIFS伺服器（如有必要）、並建立CIFS共用區、指向複製Volume的交會路徑。
3. 使用xcopy將備份檔案複製到二線SnapCenter 版的本機目錄。
4. 安裝SnapCenter vsv4.6。
5. 請確保SnapCenter 該伺服器的FQDN與原始伺服器相同。若要成功還原資料庫、就必須執行此動作。

若要開始還原程序、請完成下列步驟：

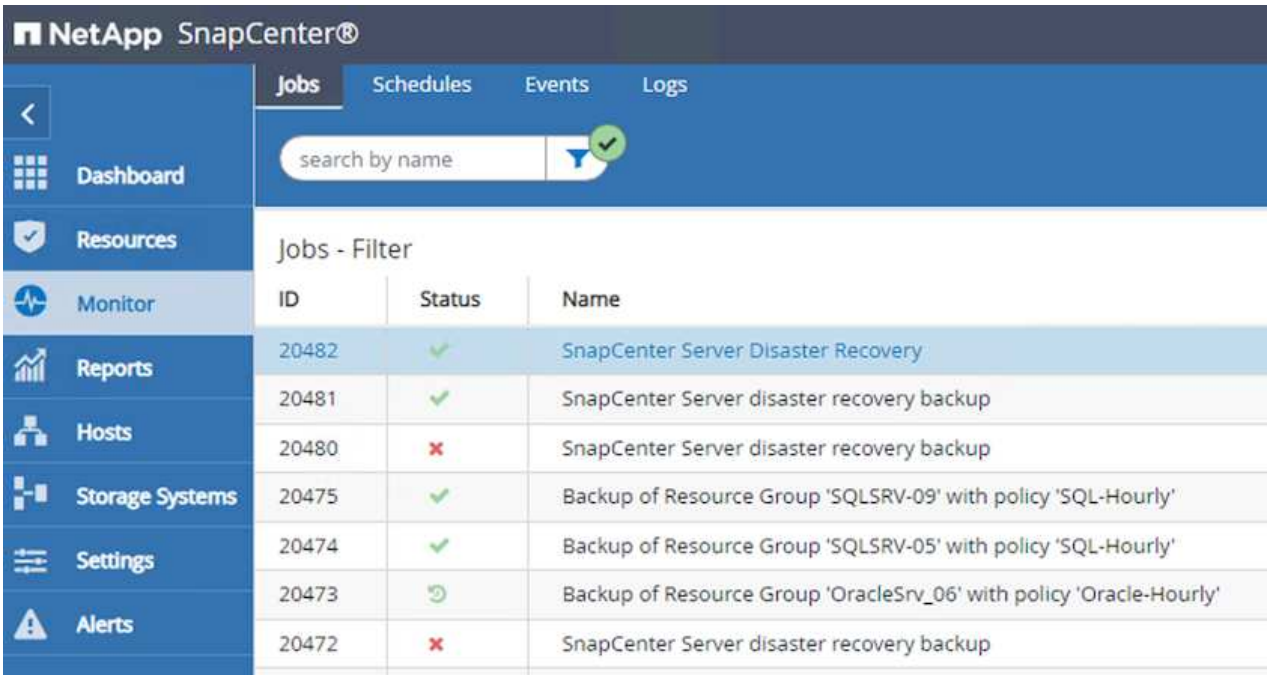
1. 瀏覽至次要SnapCenter 版伺服器的Swagger API網頁、並依照先前的指示取得授權權杖。
2. 瀏覽至Swagger頁面的Disaster Recovery（災難恢復）區段、選取「/4.6/disasterrecovery / server/recovery」（/4.6/disasterrecovery /伺服器/還原）、然後按一下「Try it out（試用）」。

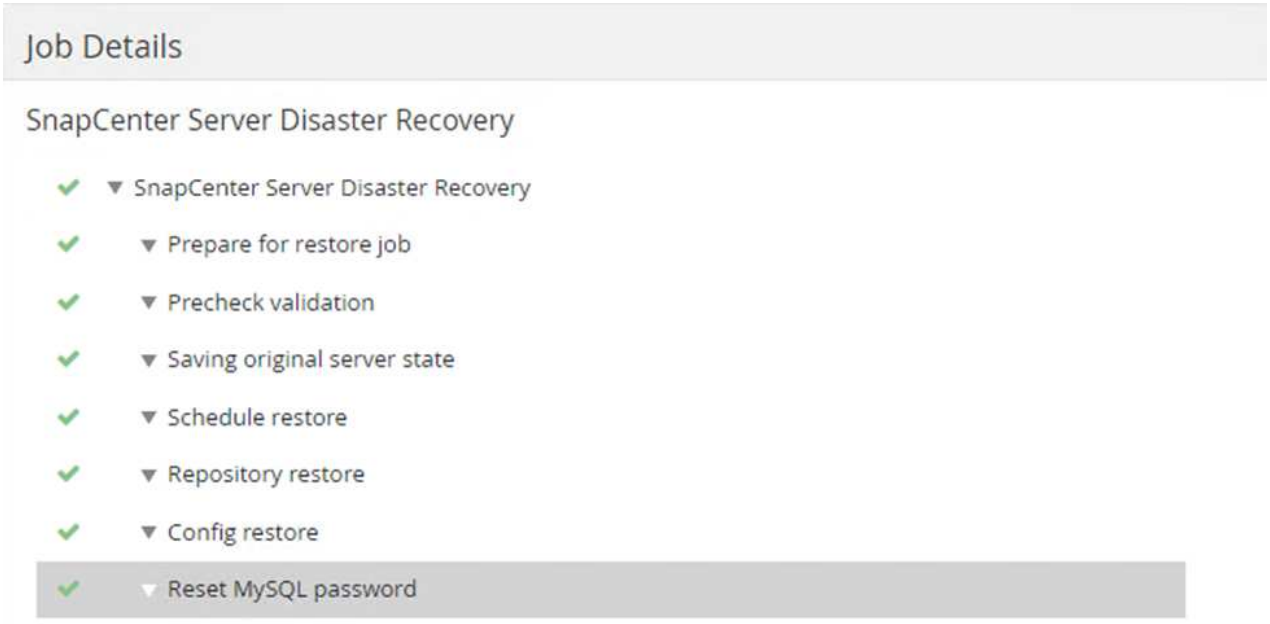


3. 貼上您的授權權杖、然後在「SmDRResterRequest」區段中、貼上備份名稱和次要SnapCenter 伺服器上的本機目錄。



4. 選取「執行」按鈕以開始還原程序。
5. 從功能區塊瀏覽至「監控」區段、以檢視還原工作的進度。SnapCenter





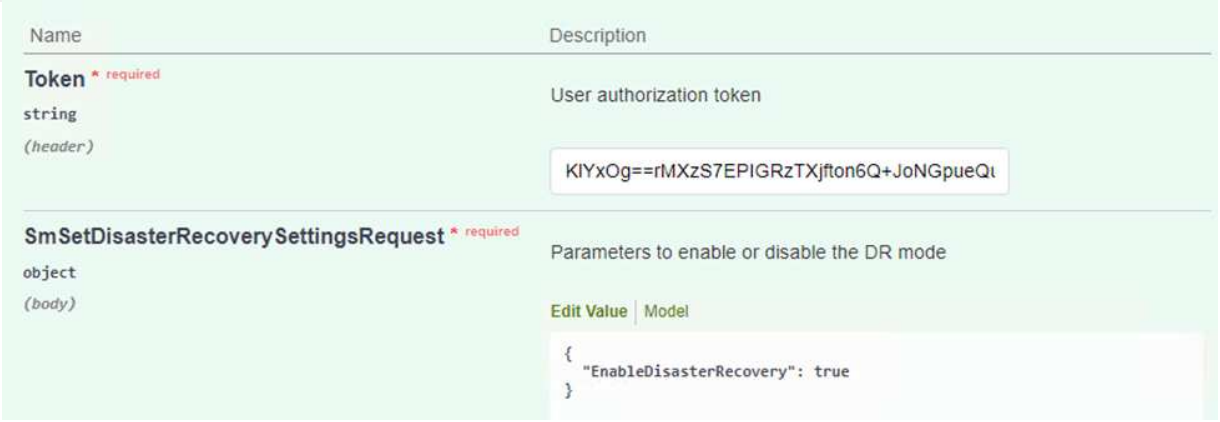
6. 若要從二線儲存設備啟用SQL Server還原、您必須將SnapCenter 此還原資料庫切換為「災難恢復」模式。這是以個別作業的形式執行、並在Swagger API網頁上啟動。

   a. 瀏覽至「Disaster Recovery（災難恢復）」區段、然後按一下「/4.6/dissterrecovery / storage（/4.6/disstersterrecovery

   b. 貼入使用者授權權杖。

   c. 在SmSetDissterRecoverySettingsRequest區段中、將「EnablDisasterRecover」變更為「true」。

   d. 按一下「執行」以啟用SQL Server的災難恢復模式。



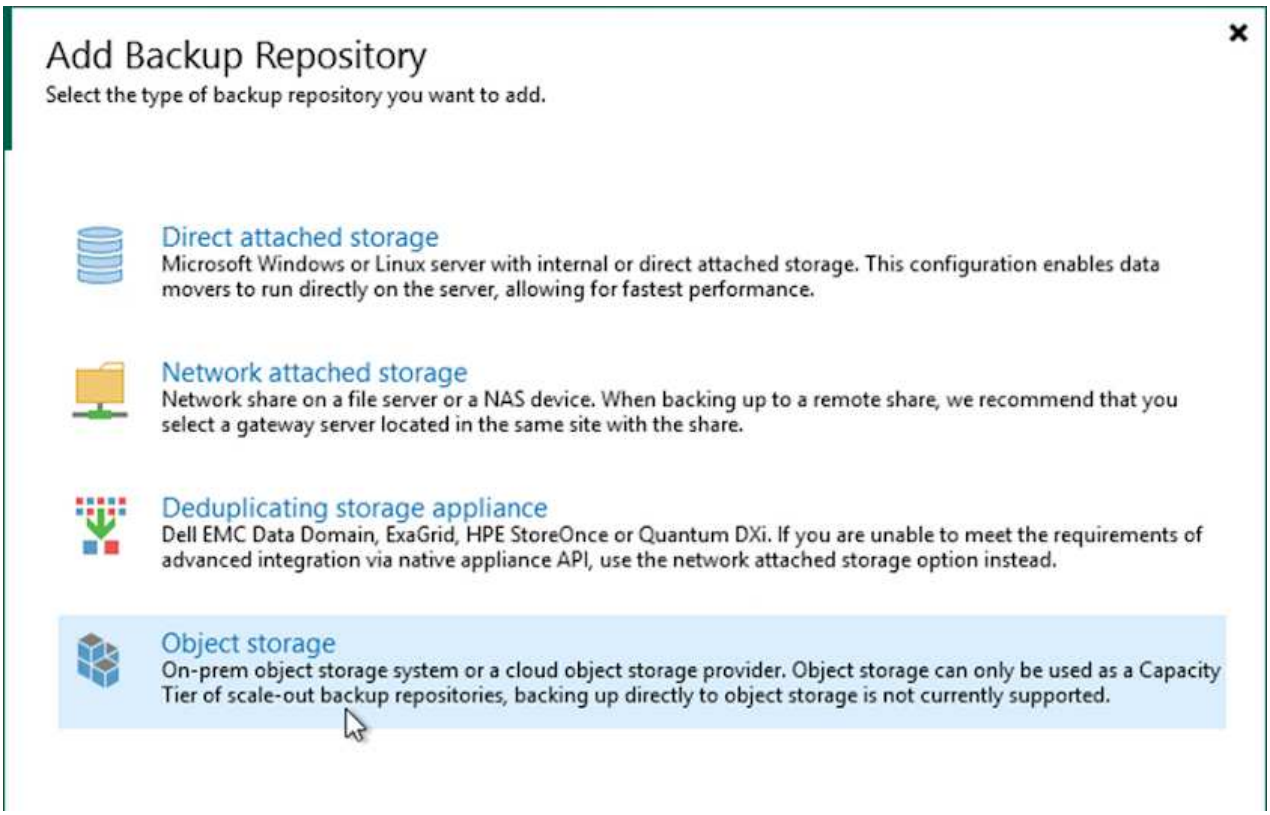
請參閱其他程序的相關意見。

使用**Veeam**完整還原還原應用程式**VM**

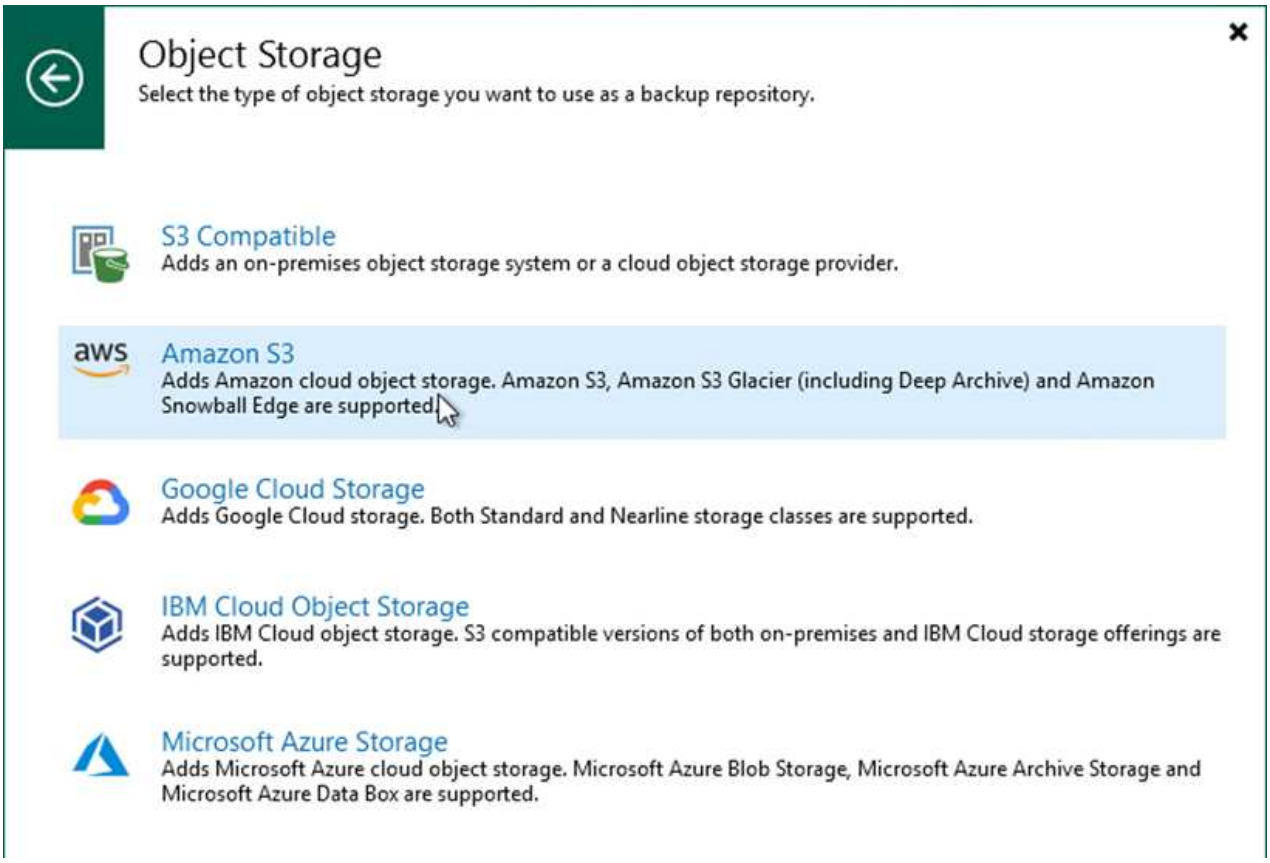
從次要Veeam伺服器、從S3儲存設備匯入備份、並將SQL Server和Oracle VM還原至VMware Cloud叢集。

若要從內部部署橫向擴充備份儲存庫中的S3物件匯入備份、請完成下列步驟：

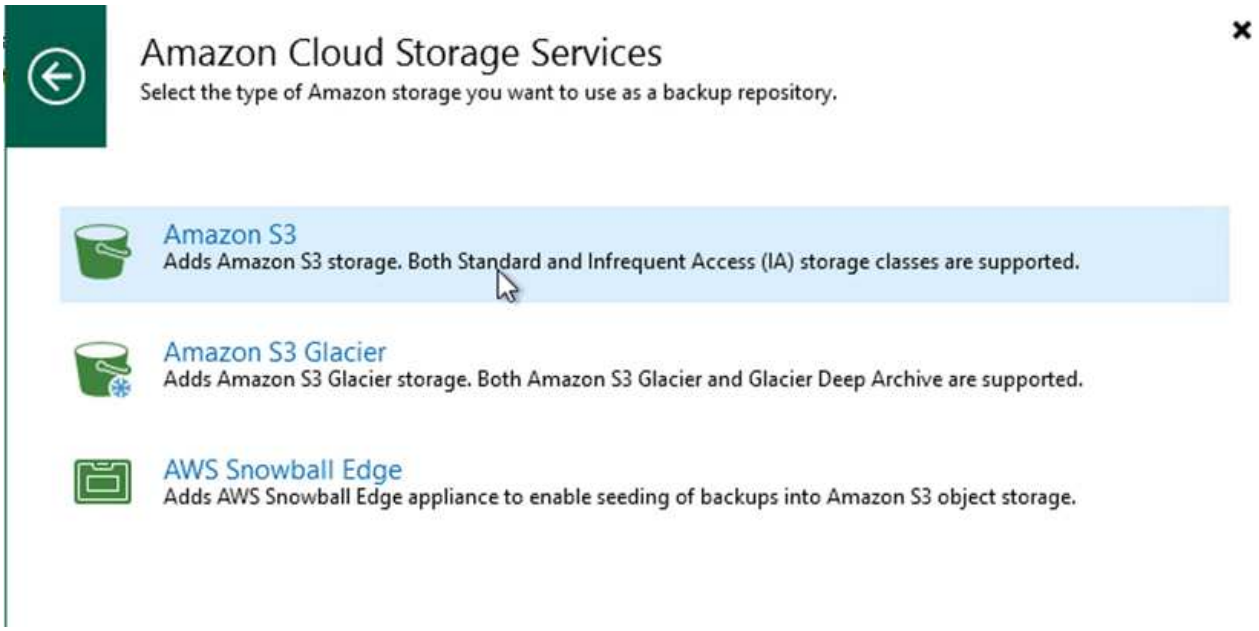
1. 移至「備份儲存庫」、然後按一下上方功能表中的「新增儲存庫」、以啟動「新增備份儲存庫」精靈。在精靈的第一頁、選取「物件儲存」作為備份儲存庫類型。



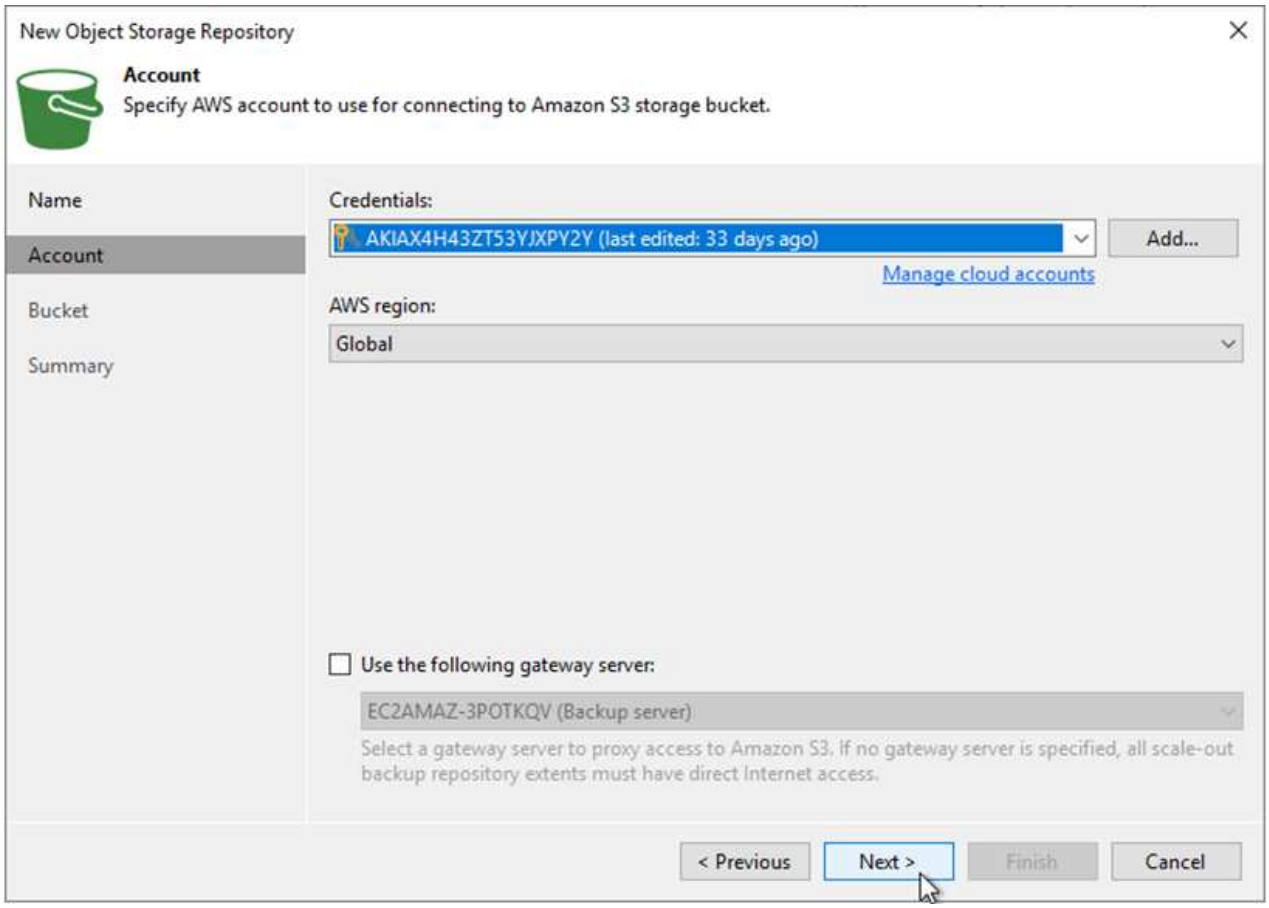
2. 選取「Amazon S3」作為「物件儲存類型」。



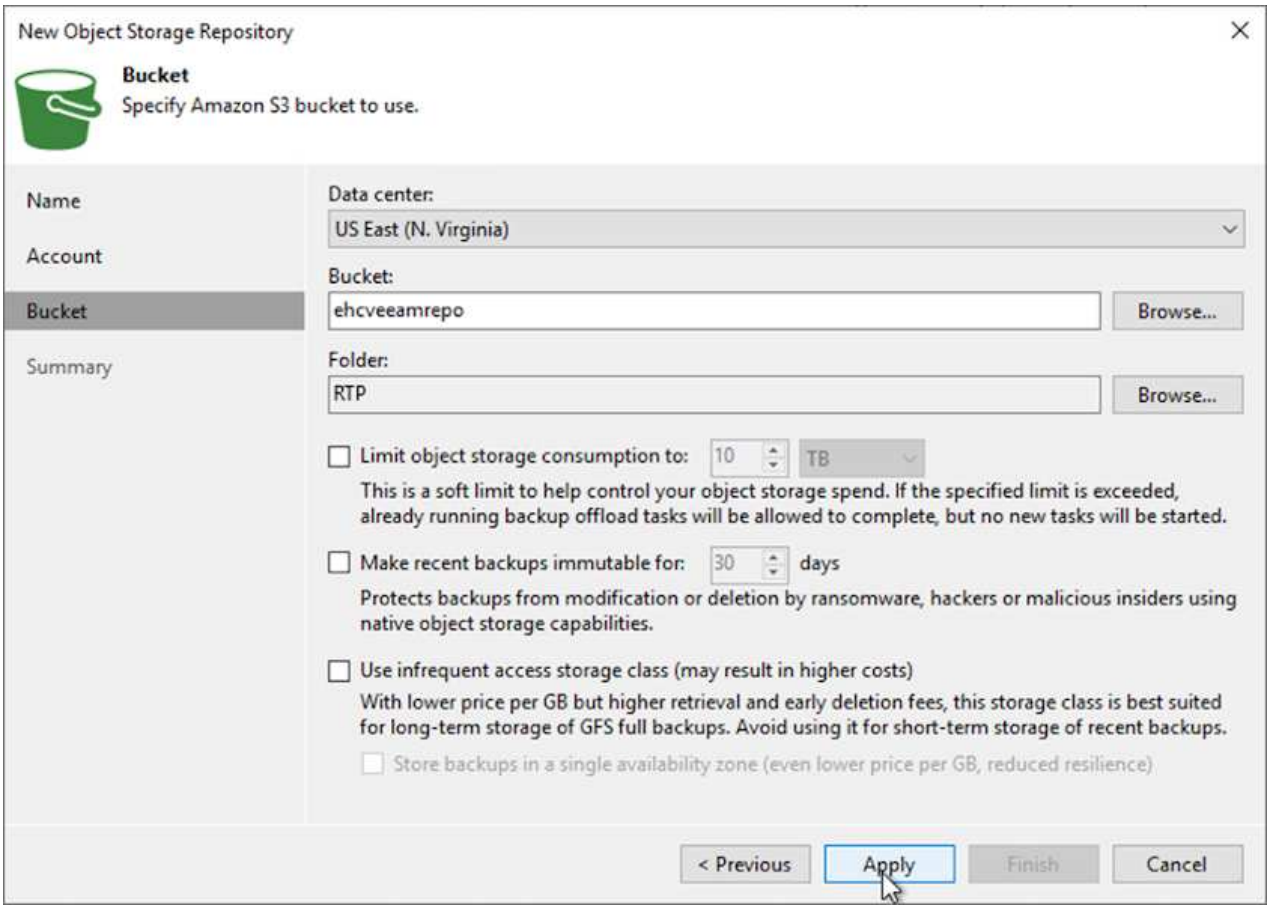
3. 從Amazon Cloud Storage Services清單中、選取Amazon S3。



4. 從下拉式清單中選取預先輸入的認證資料、或新增認證資料以存取雲端儲存資源。按一下「下一步」繼續。



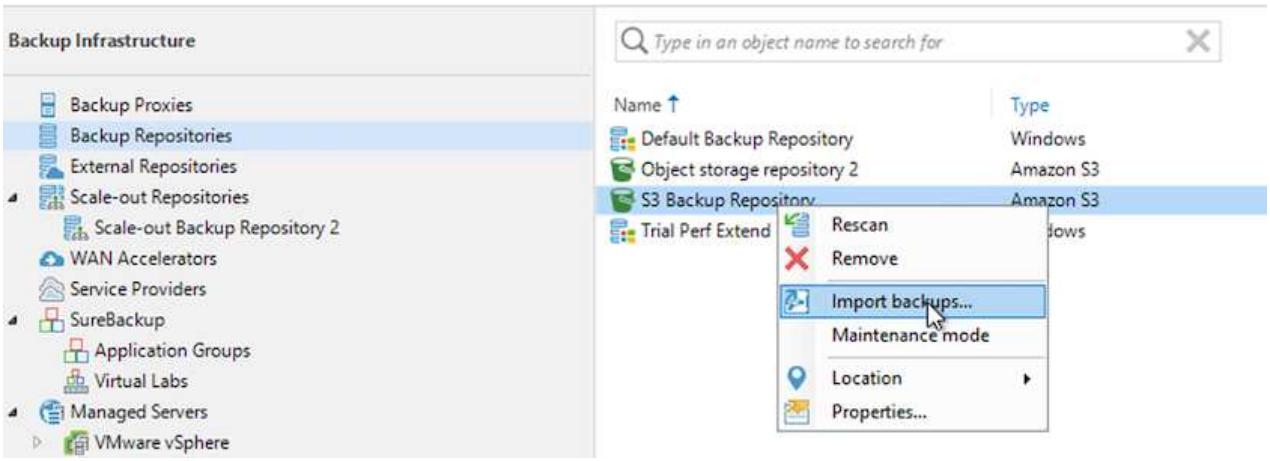
5. 在「時段」頁面上、輸入資料中心、時段、資料夾及任何所需選項。按一下套用。



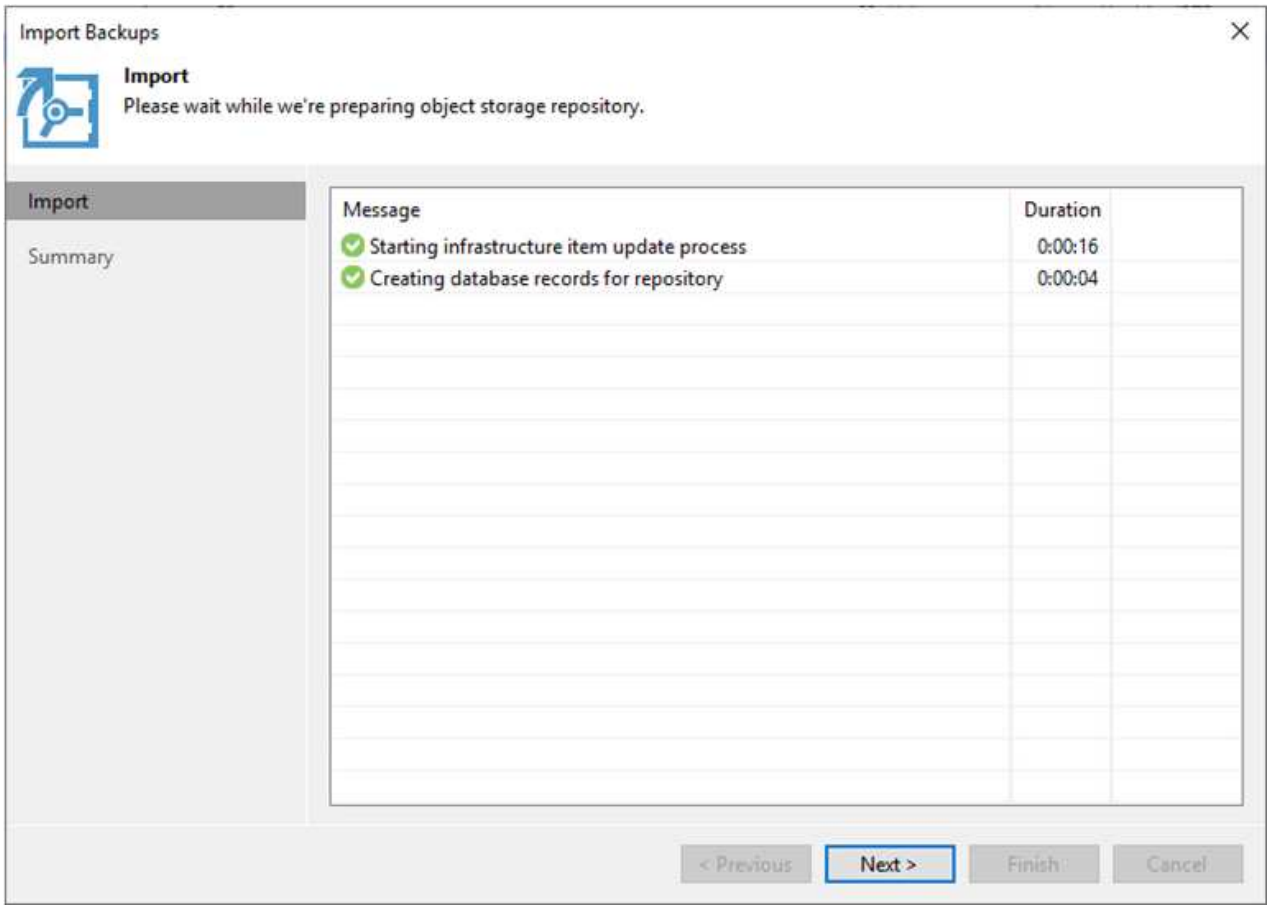
6. 最後、選取「完成」以完成程序並新增儲存庫。

若要從上一節新增的S3儲存庫匯入備份、請完成下列步驟。

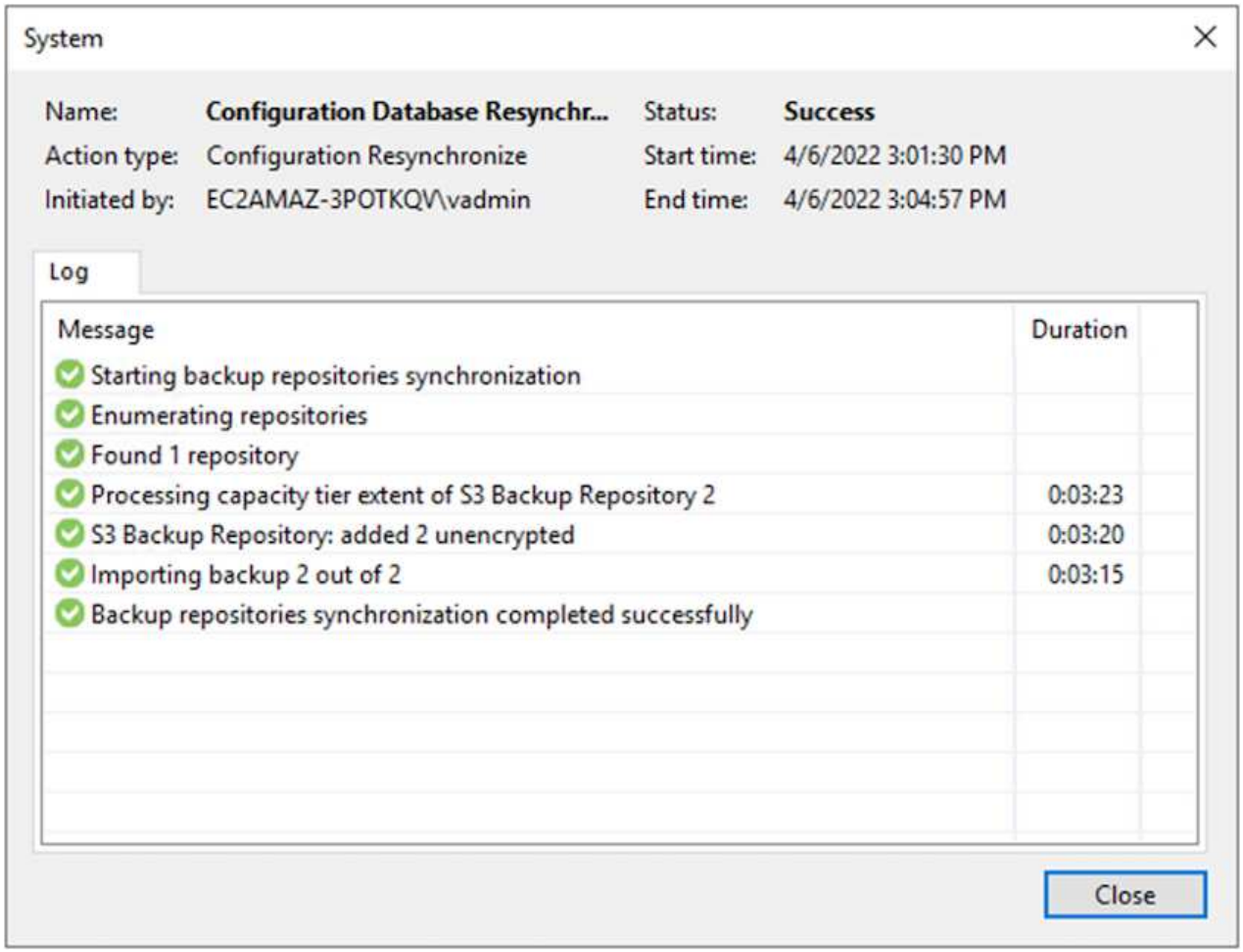
1. 從S3備份儲存庫選取匯入備份、以啟動匯入備份精靈。



2. 建立匯入的資料庫記錄之後、請在摘要畫面中選取「Next（下一步）」、然後選取「Finish（完成）」、開始匯入程序。



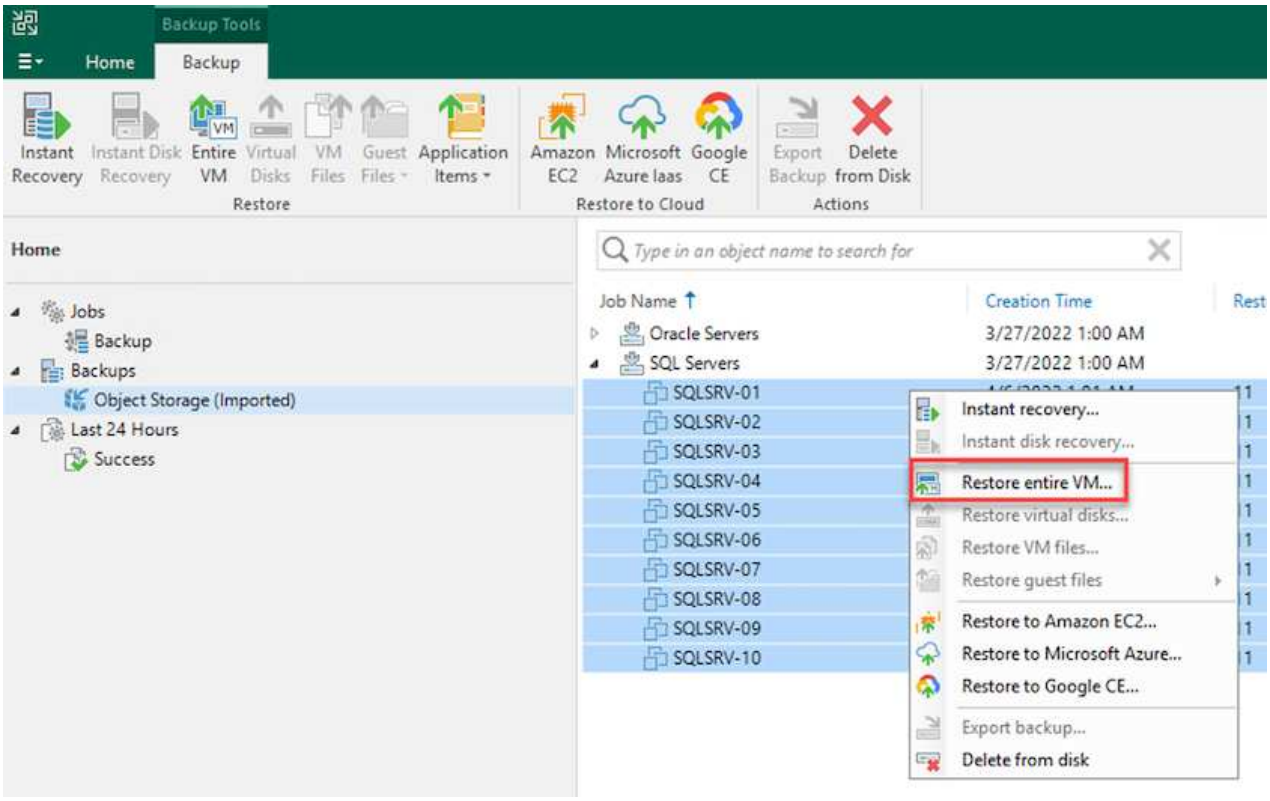
3. 匯入完成後、您可以將VM還原至VMware Cloud叢集。


System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

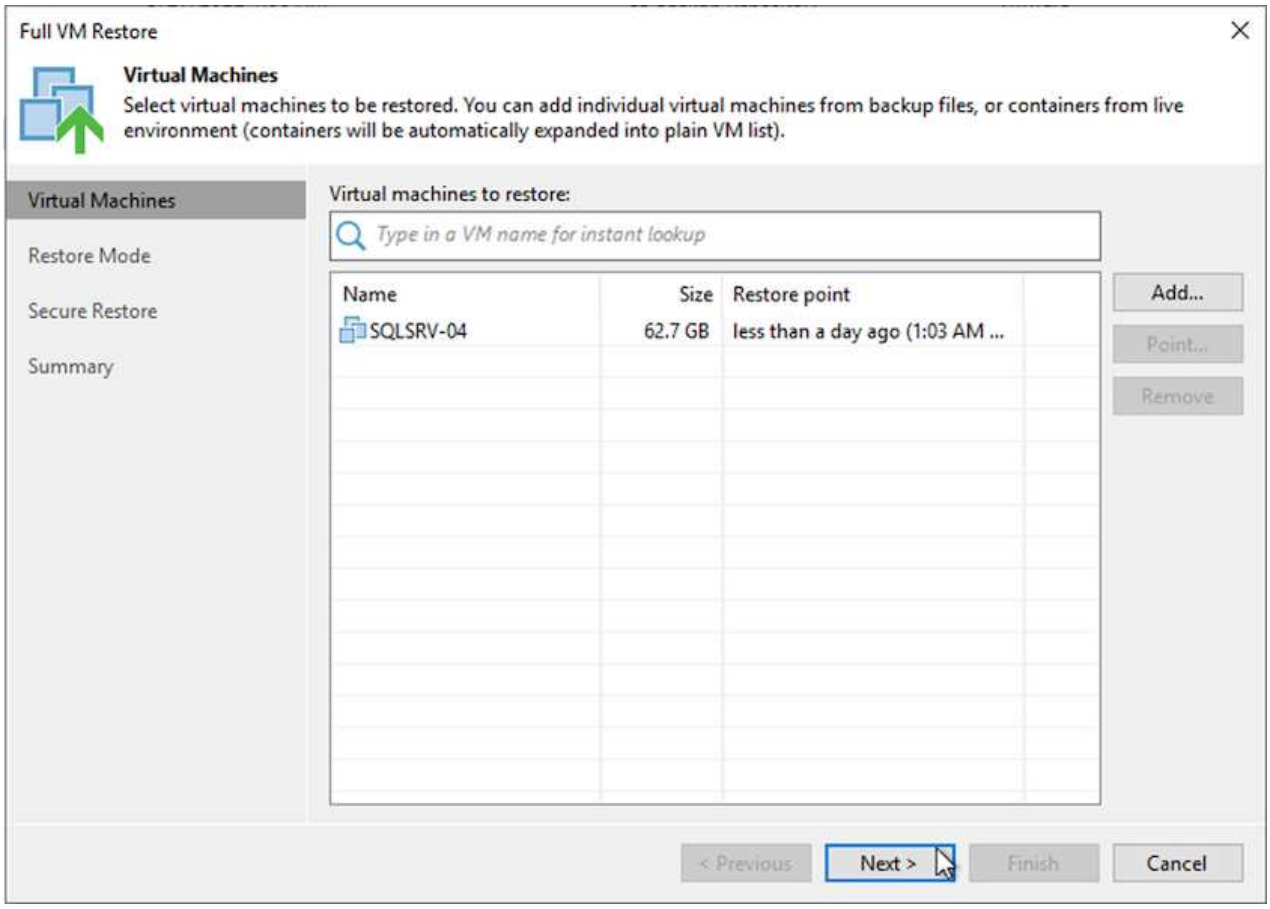
使用**Veeam**完整還原將應用程式**VM**還原至**VMware Cloud**

若要將SQL和Oracle虛擬機器還原至AWS工作負載網域/叢集上的VMware Cloud、請完成下列步驟。

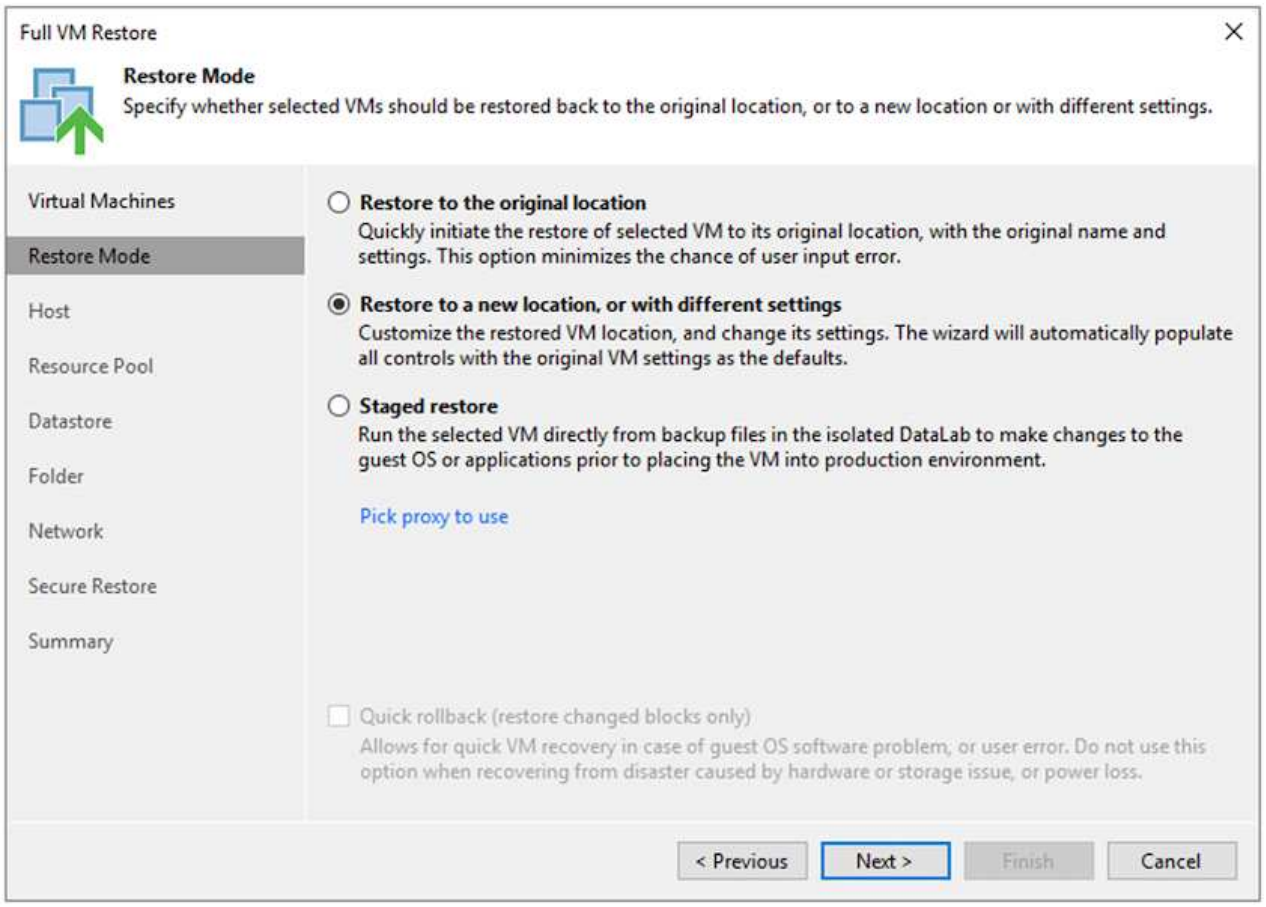
1. 在Veeam首頁中、選取包含匯入備份的物件儲存設備、選取要還原的VM、然後按一下滑鼠右鍵並選取「還原整個VM」。



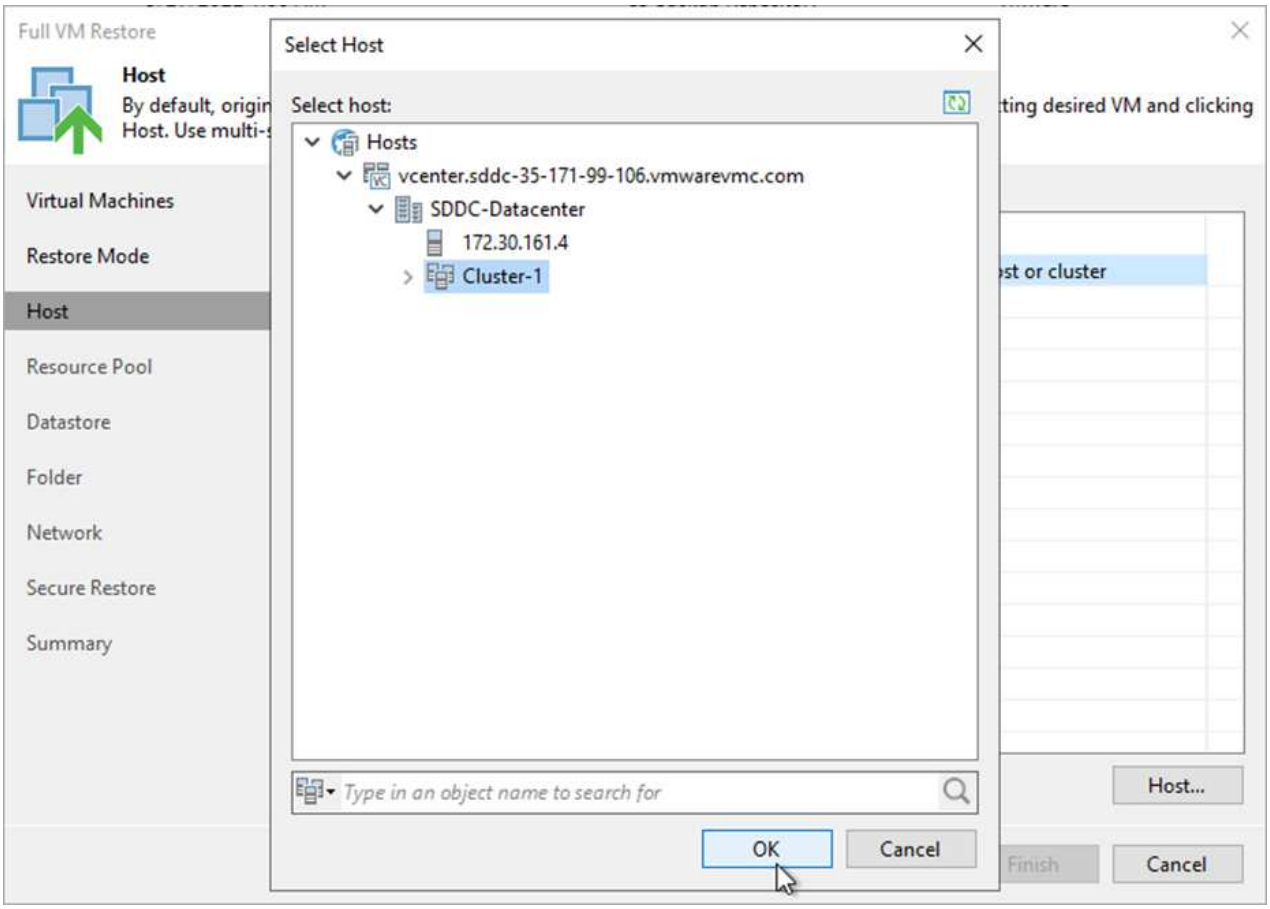
2. 在完整VM還原精靈的第一頁、視需要修改要備份的VM、然後選取「Next（下一步）」。



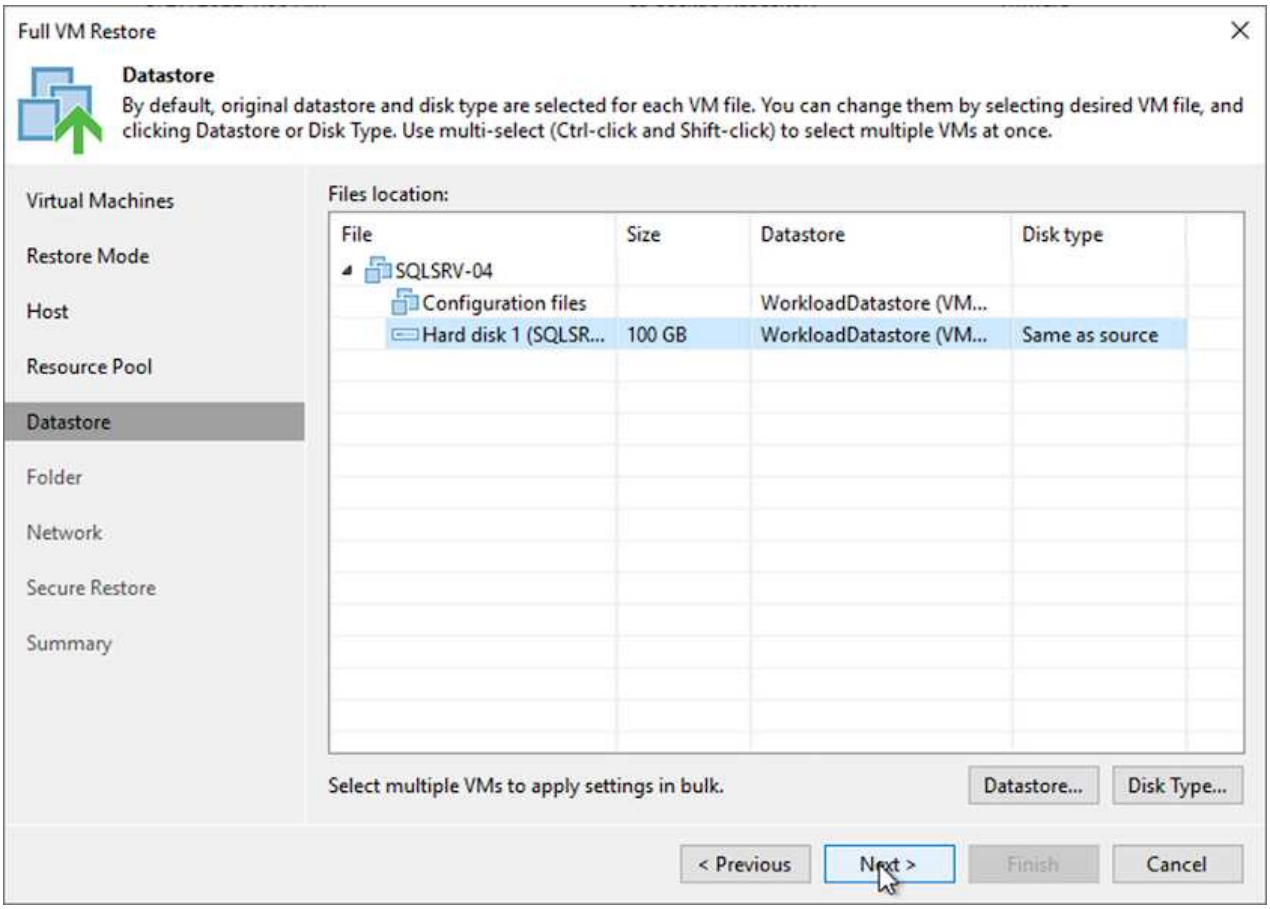
3. 在「還原模式」頁面上、選取「還原至新位置」或「使用不同的設定」。



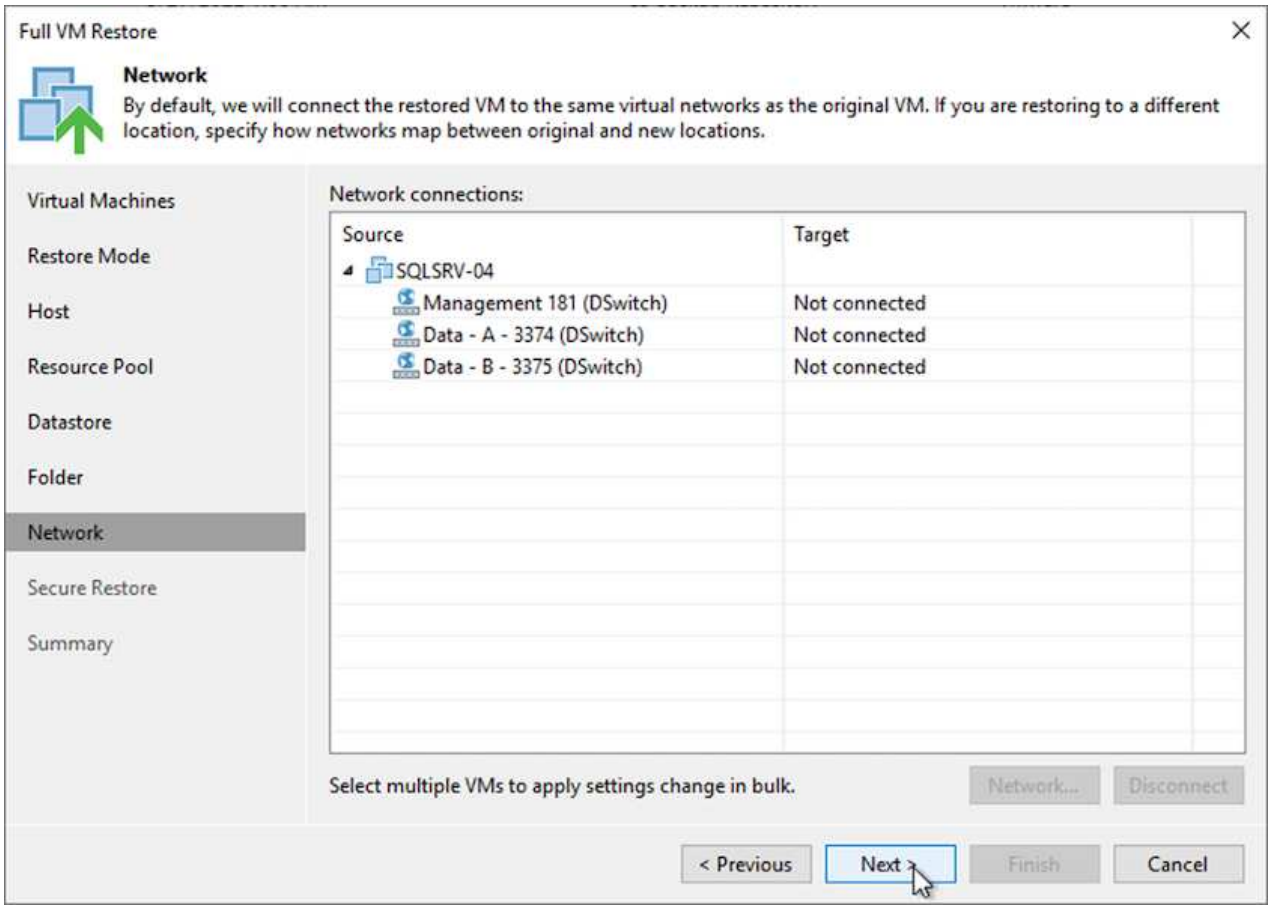
4. 在主機頁面上、選取要還原VM的目標ESXi主機或叢集。

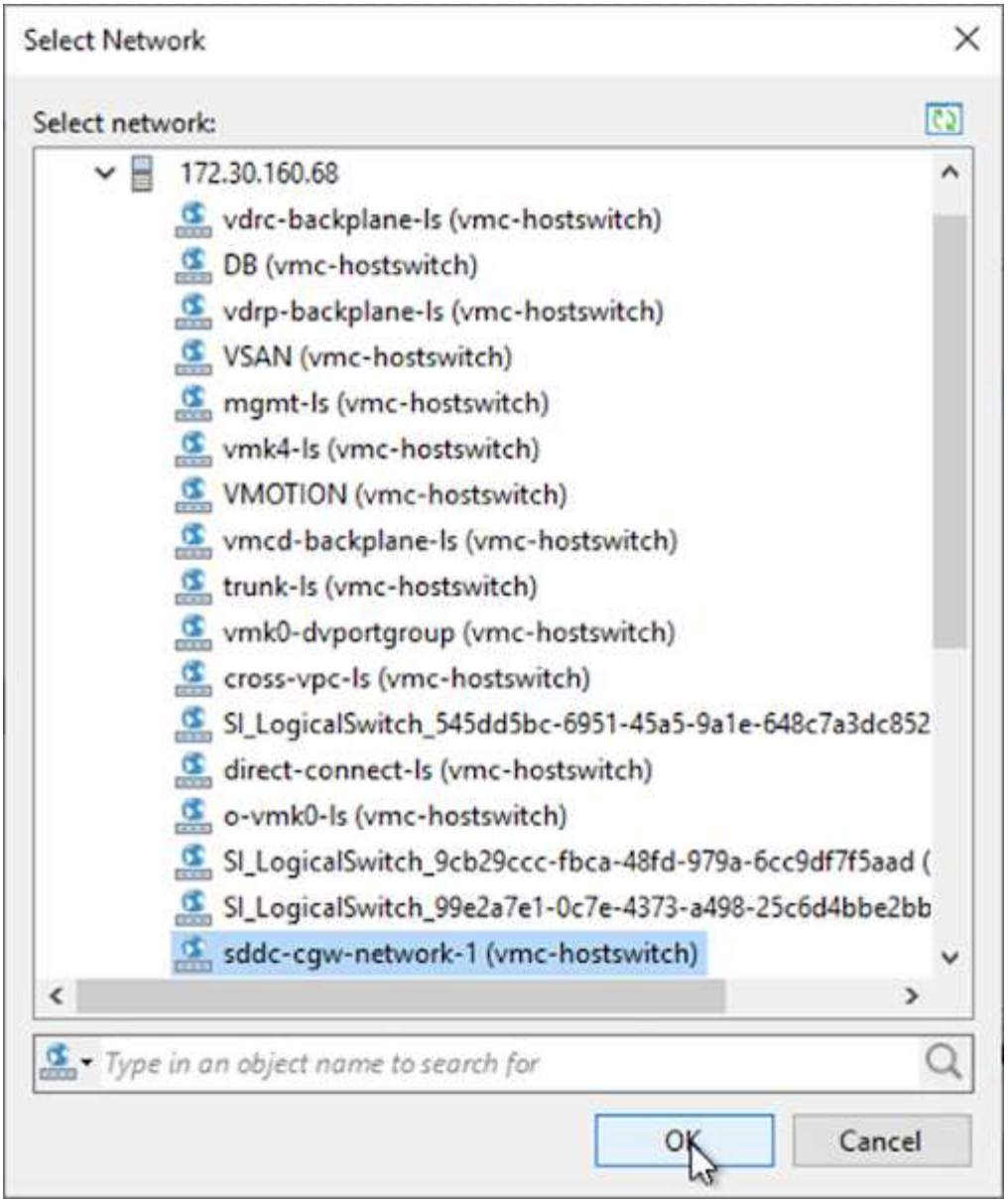


5. 在「資料存放區」頁面上、選取組態檔和硬碟的目標資料存放區位置。



6. 在「網路」頁面上、將VM上的原始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. 選取是否掃描還原的VM以尋找惡意軟體、檢閱摘要頁面、然後按一下「Finish（完成）」以開始還原。

還原**SQL Server**應用程式資料

下列程序提供如何在發生導致內部部署站台無法運作的災難時、在AWS的VMware Cloud Services中還原SQL Server的指示。

為了繼續執行恢復步驟、假設您已完成下列先決條件：

1. Windows Server VM已使用Veeam完整還原還原至VMware Cloud SDDC。
2. 我們SnapCenter 已建立次要的伺服器、SnapCenter 並已使用一節中所述的步驟完成還原資料庫和組態設定 "支援備份與還原程序摘要。SnapCenter"

VM：SQL Server VM的還原後組態

在VM還原完成後、您必須設定網路和其他項目、以便重新探索SnapCenter 位於支援中心內的主機VM。

1. 指派新的IP位址給管理、iSCSI或NFS。
2. 將主機加入Windows網域。
3. 將主機名稱新增至DNS或SnapCenter 到伺服器上的主機檔案。

如果SnapCenter 使用與目前網域不同的網域認證來部署這個程式、您就必須變更SQL Server VM上適用於Windows Service外掛程式的登入帳戶。變更登入帳戶後、請重新啟動SnapCenter 適用於Windows的WESTSMCore、外掛程式和適用於SQL Server服務的外掛程式。

若要自動重新探索SnapCenter 還原的虛擬機器、FQDN必須與原先新增至SnapCenter 內部部署的虛擬機器相同。

設定FSX儲存設備以進行SQL Server還原

若要完成SQL Server VM的災難恢復還原程序、您必須中斷現有的SnapMirror與FSX叢集之間的關係、並授予對該磁碟區的存取權。若要這麼做、請完成下列步驟。

1. 若要中斷SQL Server資料庫和記錄磁碟區的現有SnapMirror關係、請從FSXCLI執行下列命令：

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

2. 建立包含SQL Server Windows VM iSCSI IQN的啟動器群組、以授予LUN存取權：

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

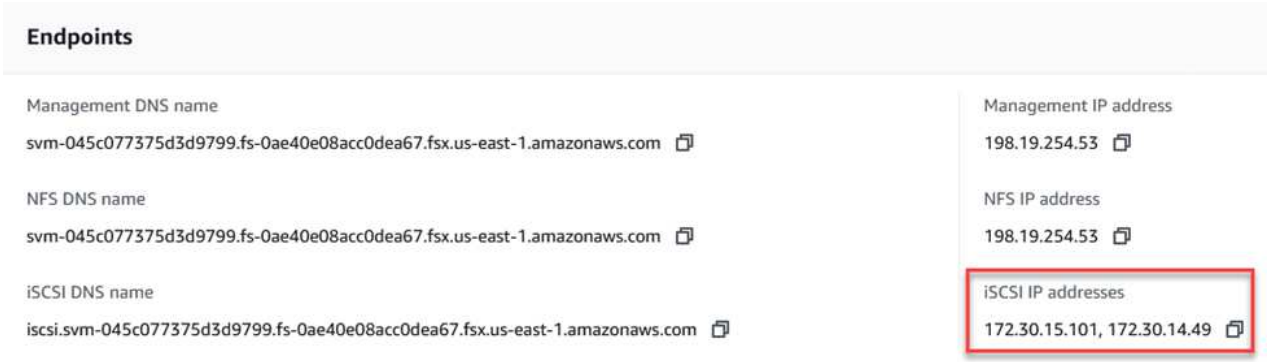
3. 最後、將LUN對應至您剛建立的啟動器群組：

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

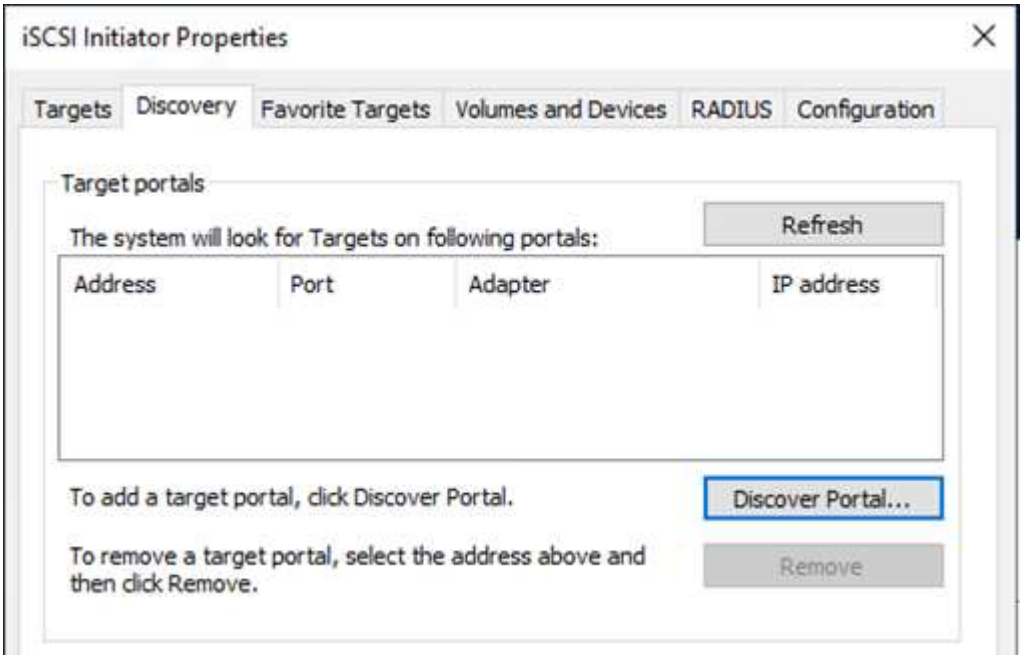
4. 若要尋找路徑名稱、請執行「LUN show」命令。

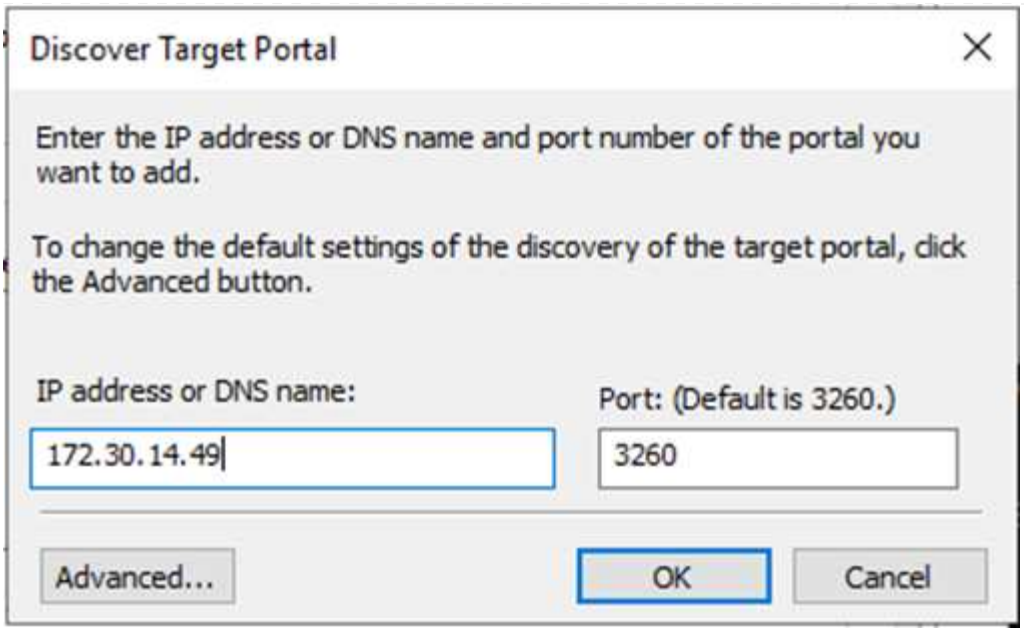
設定**Windows VM**以進行**iSCSI**存取、並探索檔案系統

1. 在SQL Server VM中、設定iSCSI網路介面卡、以便在已建立連線至FSX執行個體上iSCSI目標介面的VMware連接埠群組上進行通訊。
2. 開啟iSCSI啟動器內容公用程式、並清除「Discovery」（探索）、「Favorite Target」（最愛目標）和「Target」（目標）索引標籤上的舊連線設定。
3. 找到用於存取FSX執行個體/叢集上iSCSI邏輯介面的IP位址。這可在AWS主控台的Amazon FSX > ONTAP VMware Storage Virtual Machines下找到。

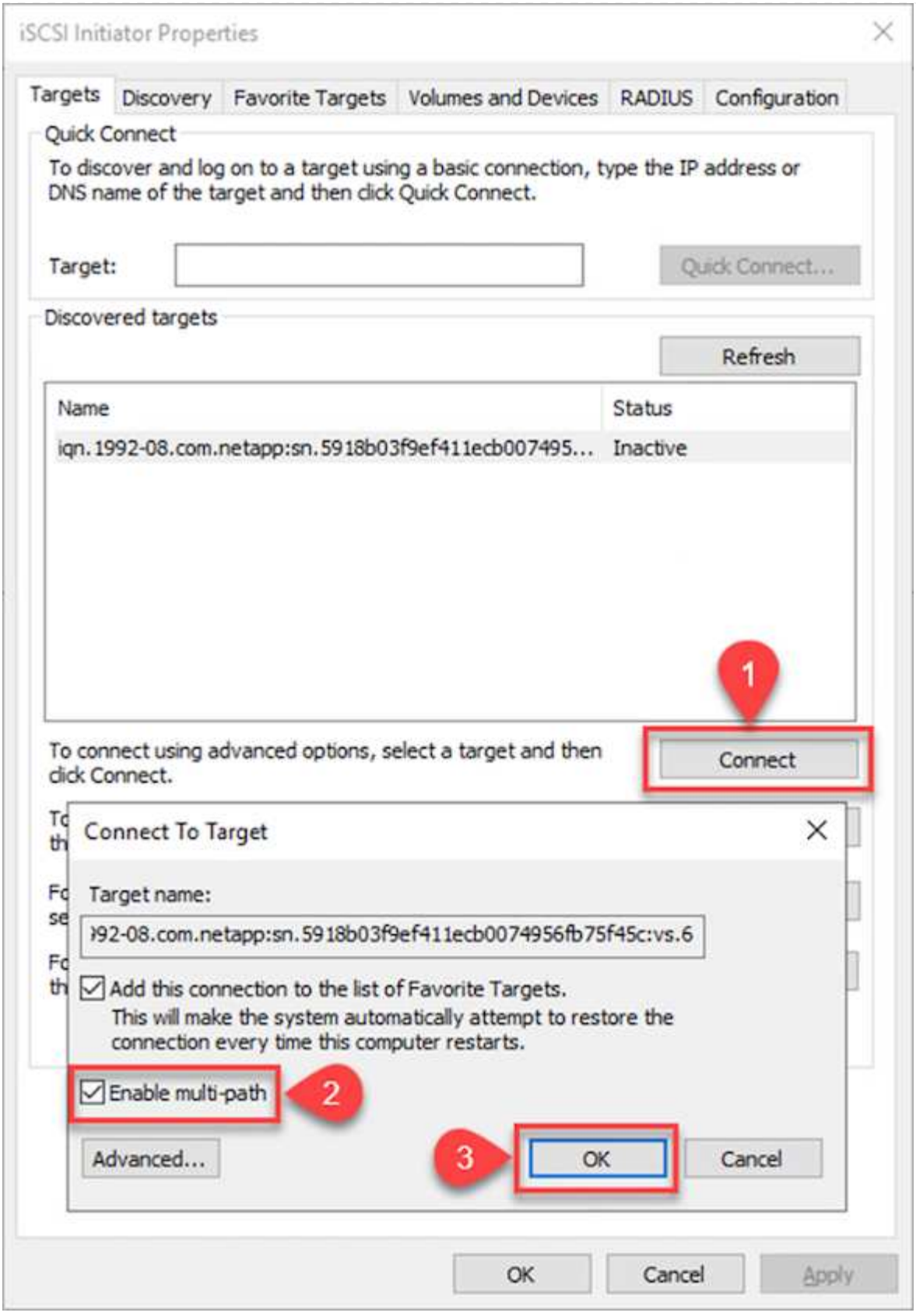


4. 在「Discovery（探索）」索引標籤中、按一下「Discover Portal（探索入口網站）」、然後輸入FSX iSCSI目標的IP位址。

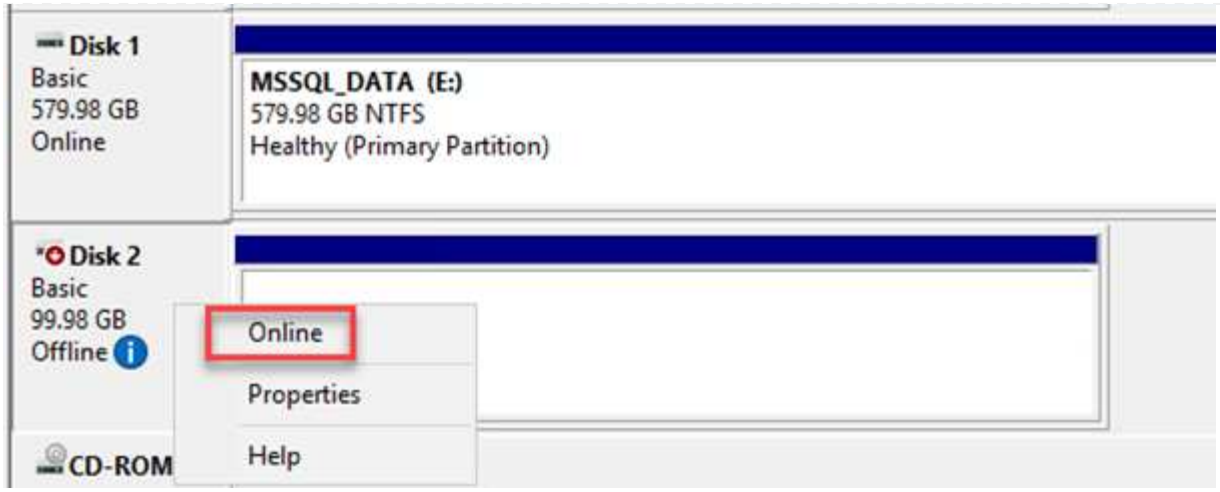




5. 在「Target」（目標）索引標籤上、按一下「Connect」（連線）、選取「Enable Multi-Path（啟用多重路徑）」（若適用於您的組態）、然後按一下「OK（確定）」連線至

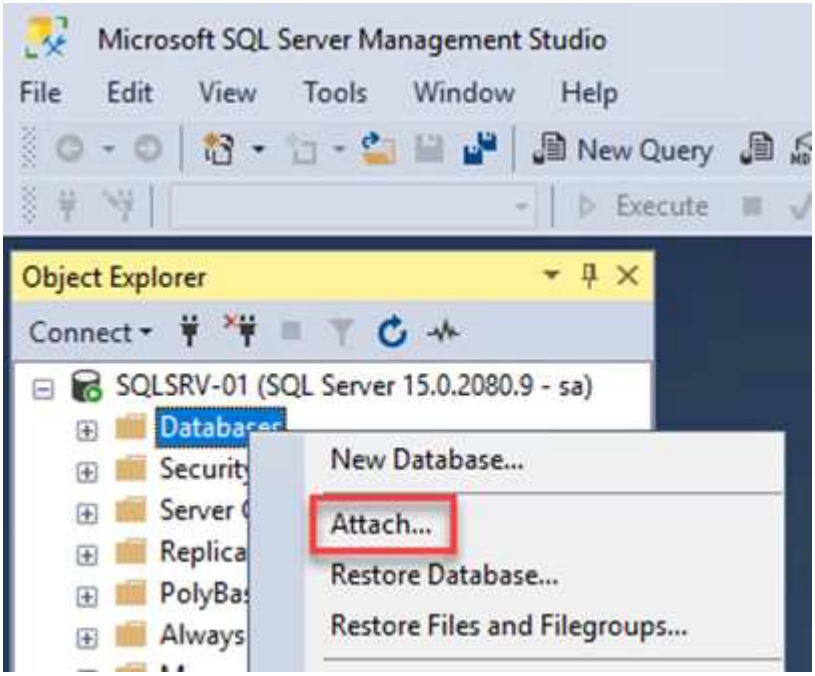


6. 開啟「電腦管理」公用程式、使磁碟上線。請確認它們保留的磁碟機代號與先前所保留的相同。

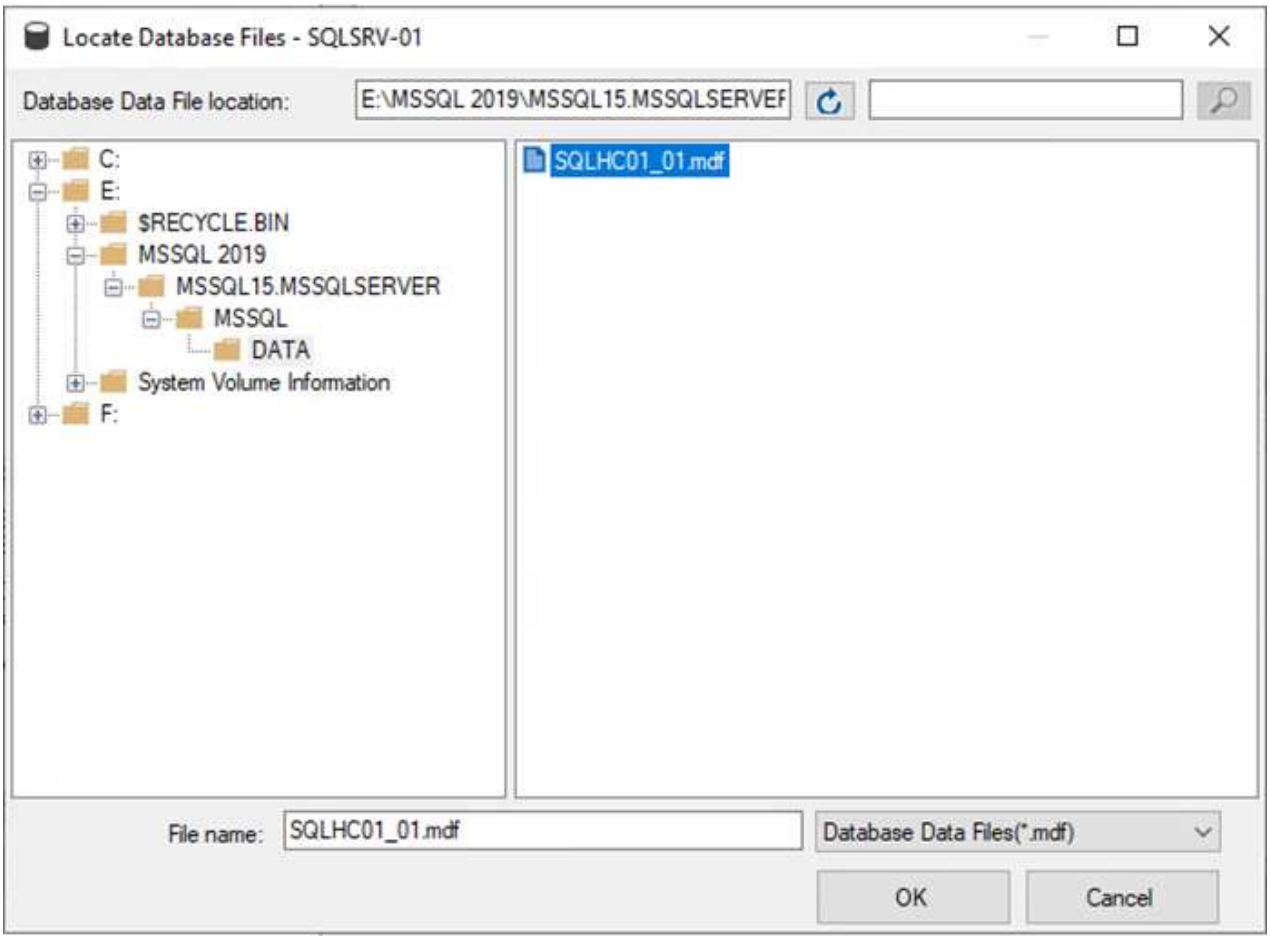

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

附加**SQL Server**資料庫

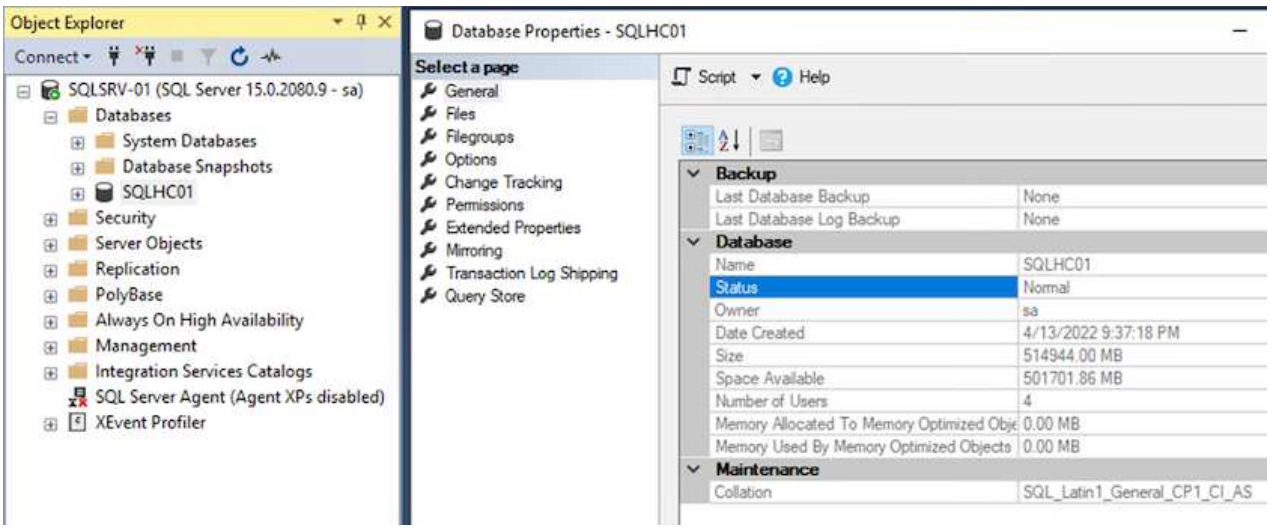
1. 從SQL Server VM開啟Microsoft SQL Server Management Studio、然後選取附加以開始連線至資料庫的程序。



2. 按一下「Add（新增）」、然後瀏覽至包含SQL Server主要資料庫檔案的資料夾、選取該檔案、然後按一下「OK（確定）」。



3. 如果交易記錄位於不同的磁碟機上、請選擇包含交易記錄的資料夾。
4. 完成後、按一下「確定」以附加資料庫。

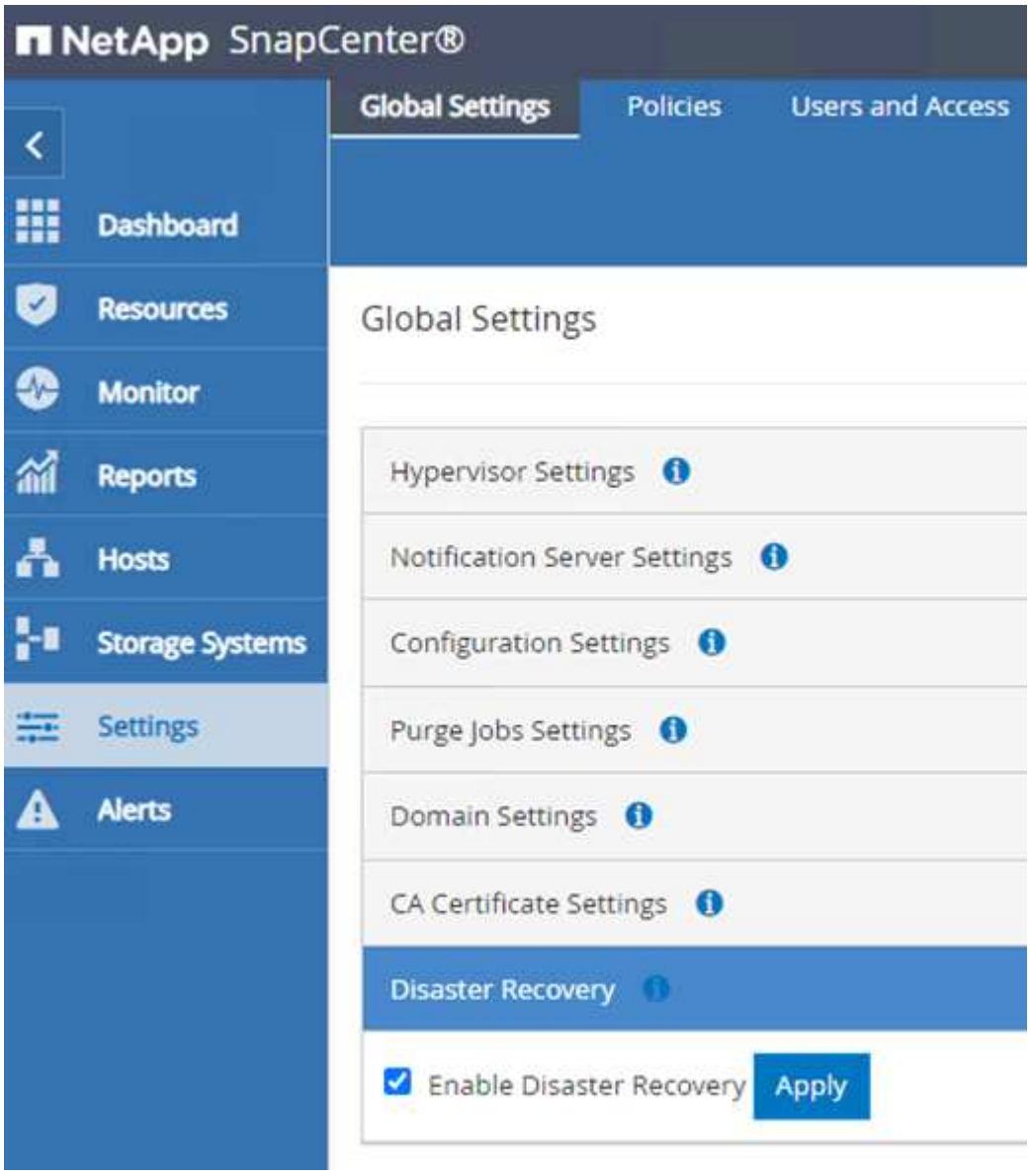


確認**SnapCenter** 與**SQL Server**外掛程式的通訊

利用還原為先前狀態的功能、它會自動重新探索SQL Server主機。SnapCenter若要使其正常運作、請記住下列先決條件：

- 必須將此項目置於災難恢復模式。SnapCenter這可透過Swagger API或災難恢復下的「全域設定」來完成。
- SQL Server的FQDN必須與內部部署資料中心執行的執行個體相同。
- 原始SnapMirror關係必須中斷。
- 包含資料庫的LUN必須掛載到SQL Server執行個體和附加的資料庫。

若要確認SnapCenter 此功能為災難恢復模式、請從SnapCenter Websweb用戶端瀏覽至「設定」。前往「Global Settings（全域設定）」索引標籤、然後按一下「Disaster Recovery（災難恢復）請確定已啟用「啟用災難恢復」核取方塊。



還原**Oracle**應用程式資料

下列程序提供如何在發生導致內部部署站台無法運作的災難時、在AWS的VMware Cloud Services中恢復Oracle應用程式資料的指示。

完成下列先決條件、以繼續執行恢復步驟：

1. Oracle Linux伺服器VM已使用Veeam完整還原還原至VMware Cloud SDDC。
2. 已SnapCenter 建立次要的功能、SnapCenter 並已使用本節所述的步驟還原了資料庫和組態檔案 "支援備份與還原程序摘要。SnapCenter"

設定FSXfor Oracle還原–中斷SnapMirror關係

若要讓Oracle伺服器能夠存取位於FSxN執行個體上的次要儲存磁碟區、您必須先中斷現有的SnapMirror關係。

1. 登入FSX CLI之後、請執行下列命令、檢視依正確名稱篩選的磁碟區。

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

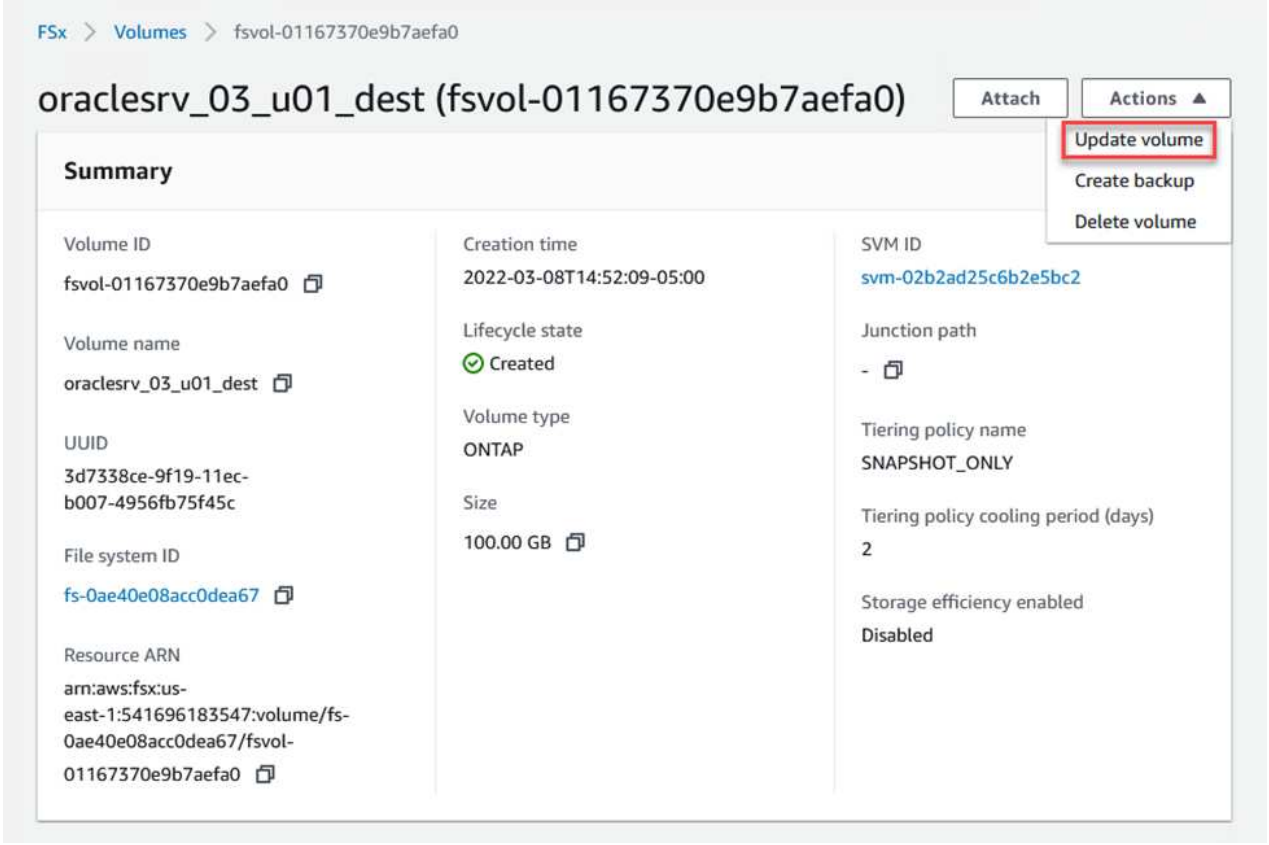
```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

2. 執行下列命令以中斷現有的SnapMirror關係。

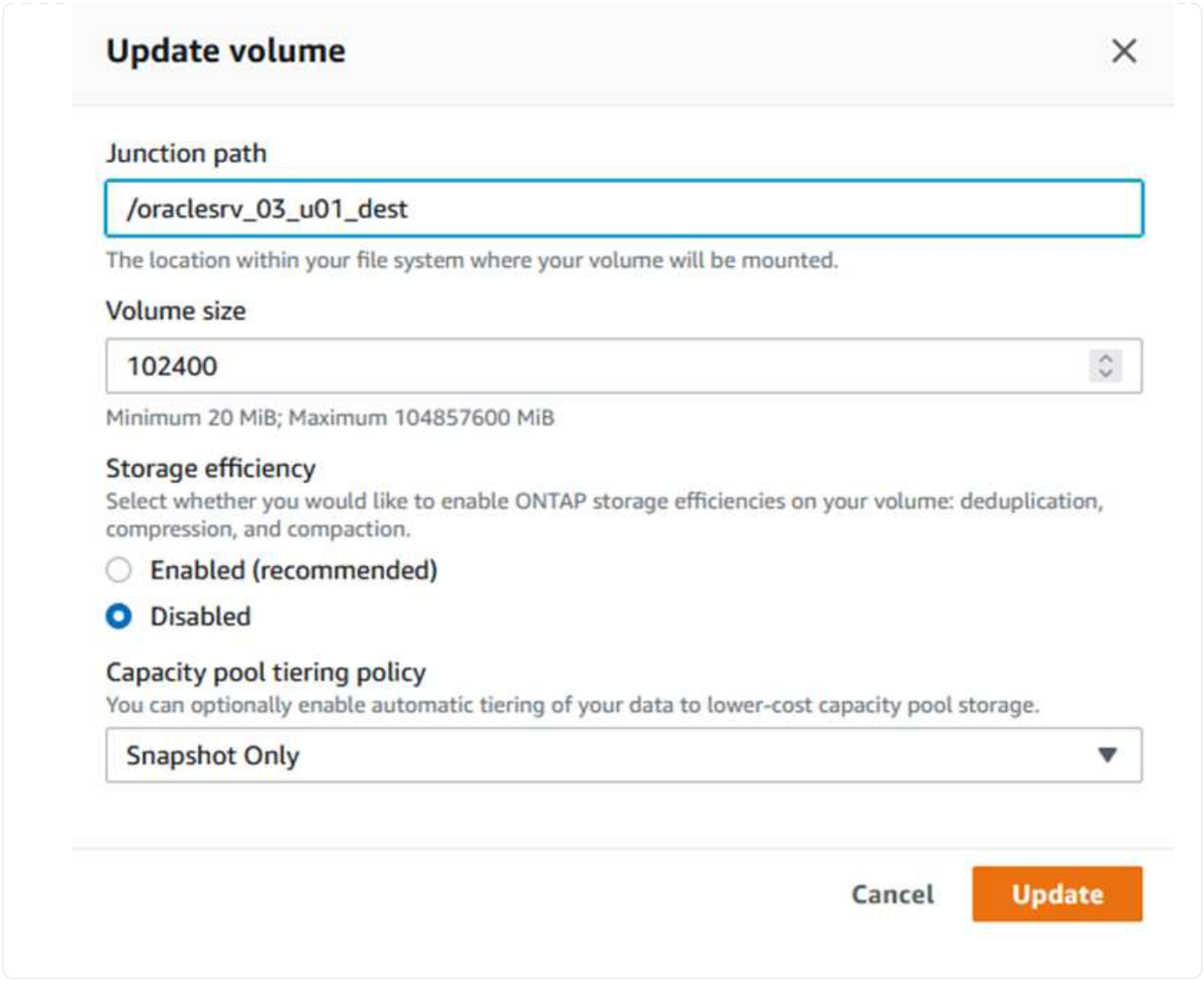
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. 更新Amazon FSX Web用戶端中的交會路徑：



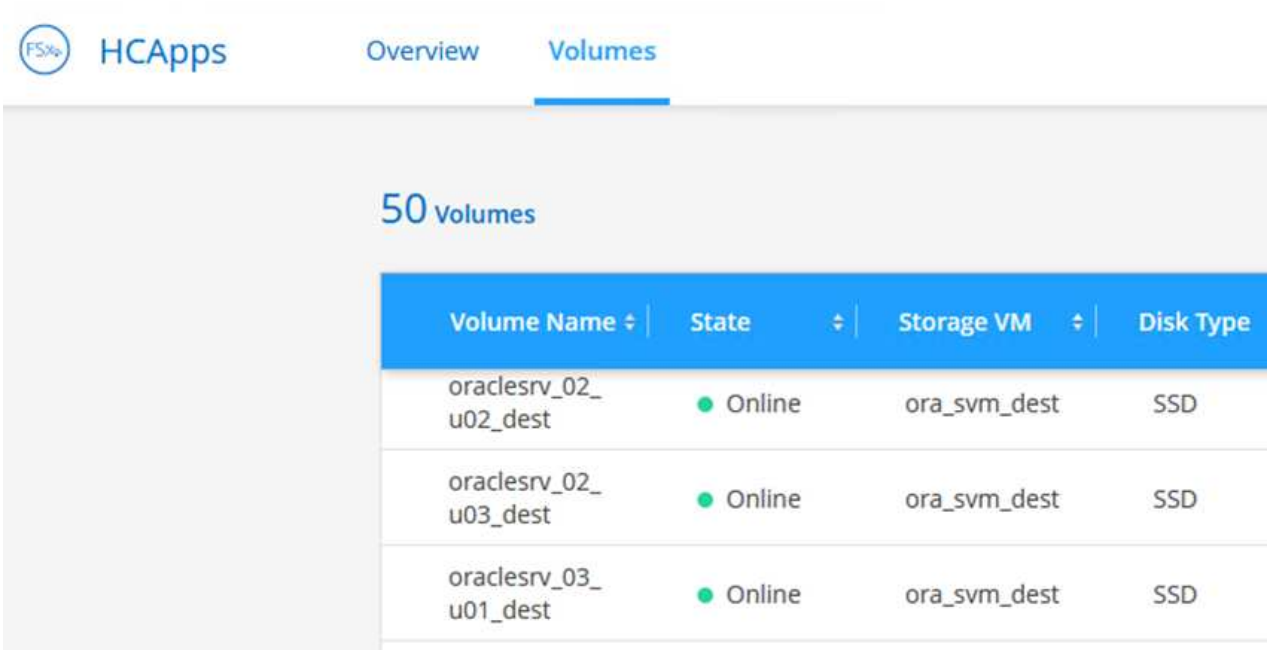
4. 新增交會路徑名稱、然後按一下「Update（更新）」。從Oracle伺服器掛載NFS Volume時、請指定此交會路徑。


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

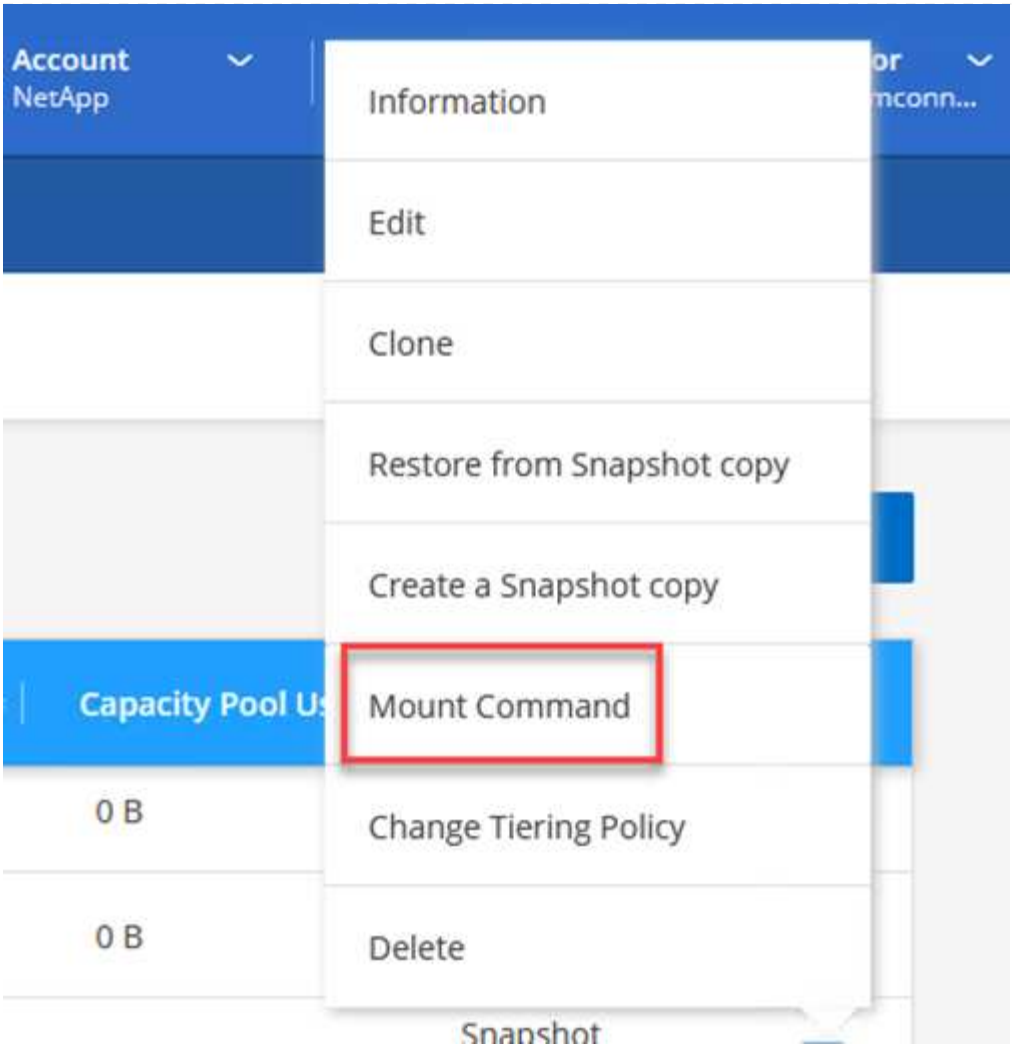
在**Oracle**伺服器上掛載**NFS**磁碟區

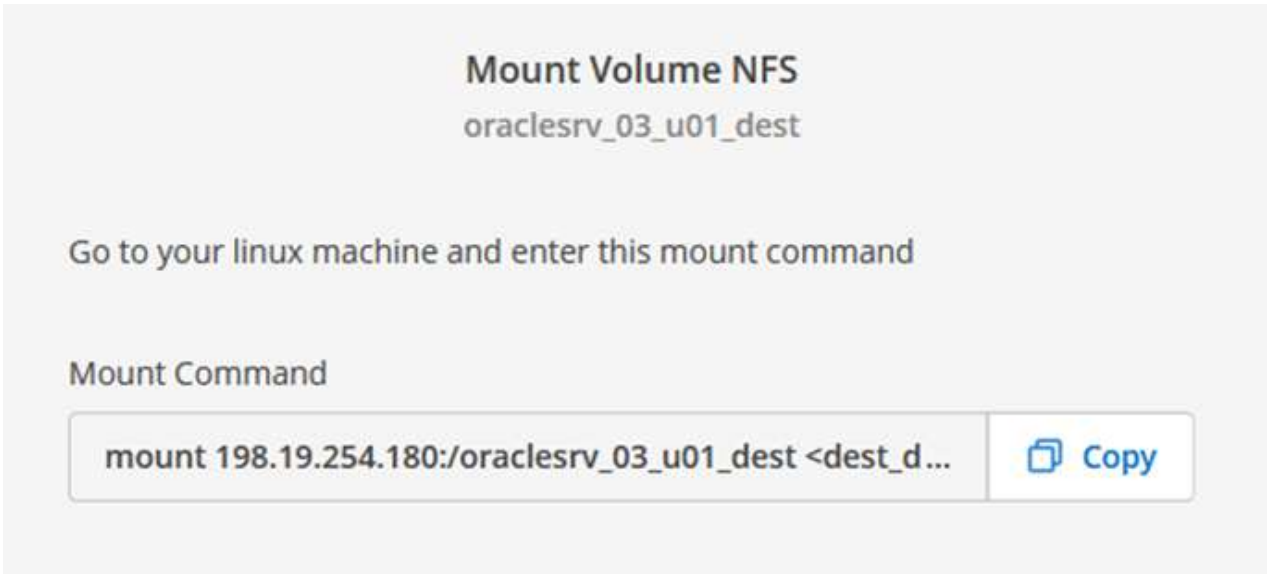
在Cloud Manager中、您可以使用正確的NFS LIF IP位址來取得掛載命令、以掛載包含Oracle資料庫檔案和記錄檔的NFS磁碟區。

1. 在Cloud Manager中、存取FSX叢集的Volume清單。



2. 從動作功能表中、選取Mount Command（掛載命令）以檢視及複製要在Oracle Linux伺服器上使用的掛載命令。





3. 將NFS檔案系統掛載至Oracle Linux Server。用於掛載NFS共用的目錄已存在於Oracle Linux主機上。
4. 在Oracle Linux伺服器上、使用mount命令掛載NFS磁碟區。

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

針對與Oracle資料庫相關的每個Volume重複此步驟。

若要讓NFS掛載在重新開機時持續執行、請編輯「/etc/stabs」檔案以包含掛載命令。

5. 重新啟動Oracle伺服器。Oracle資料庫應正常啟動、並可供使用。

容錯回復

成功完成本解決方案所述的容錯移轉程序後、SnapCenter 即可恢復在AWS中執行的備份功能、而FSXfor ONTAP 效益現已被指定為主要儲存設備、且不存在與原始內部部署資料中心的SnapMirror關係。在內部部署恢復正常功能之後、您可以使用與本文件所述相同的程序、將資料鏡射回內部部署ONTAP 的更新儲存系統。

如本文件所述、您可以設定SnapCenter 將應用程式資料Volume從FSXfor ONTAP the Sfor the Sf8鏡射至ONTAP 內部部署的靜態儲存系統。同樣地、您也可以設定Veeam使用橫向擴充備份儲存庫、將備份複本複製到Amazon S3、以便駐留在內部部署資料中心的Veeam備份伺服器能夠存取這些備份。

容錯回復不在本文件的範圍之內、但容錯回復與此處概述的詳細程序幾乎沒有什麼不同。

結論

本文件所述的使用案例著重於已獲證實的災難恢復技術、強調NetApp與VMware之間的整合。NetApp ONTAP 支援的資料鏡射技術已獲證實、可讓組織設計跨越內部部署和ONTAP 與頂尖雲端供應商共同使用的不實技術的災難恢復解決方案。

FSX for ONTAP Sfor AWS是這樣的解決方案之一、可與SnapCenter 支援將SyncMirror 應用程式資料複製到雲端的功能不間斷地整合到功能上。Veeam備份與複寫是另一項廣為人知的技術、可與NetApp ONTAP 的VMware還原儲存系統完美整合、並提供容錯移轉至vSphere原生儲存設備的功能。

本解決方案提供使用來自ONTAP 代管SQL Server和Oracle應用程式資料之VMware系統的來賓連線儲存設備的災難恢復解決方案。利用SnapMirror提供易於管理的解決方案、可在支援應用程式的各個系統上保護應用程式磁碟區、並將其複製到位於雲端的FSX或CVO。SnapCenter ONTAP支援DR的解決方案可將所有應用程式資料容錯移轉至AWS上的VMware Cloud。SnapCenter

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- 解決方案文件連結

  "NetApp混合式多雲端搭配VMware解決方案"

  "NetApp解決方案"

在 **VMware Cloud** 中使用 **Amazon FSX for ONTAP** 進行 **Veeam** 備份與還原

作者： Josh Powell - NetApp 解決方案工程部

總覽

Veeam 備份與複寫是有效且可靠的解決方案、可在 VMware Cloud 中保護資料。此解決方案展示了正確的設定和組態、可讓您使用 Veeam 備份和複寫來備份和還原位於 VMware Cloud 中適用於 ONTAP NFS 資料存放區的 FSX 上的應用程式 VM 。

VMware Cloud （在 AWS 中）支援使用 NFS 資料存放區做為補充儲存設備、而 FSX for NetApp ONTAP 則是安全的解決方案、適合需要儲存大量資料給雲端應用程式的客戶、可在 SDDC 叢集中的 ESXi 主機數量之外進行擴充。這項整合式 AWS 儲存服務提供高效率的儲存設備、具備所有傳統的 NetApp ONTAP 功能。

使用案例

本解決方案可解決下列使用案例：

- 使用適用於 NetApp ONTAP 的 FSX 作為備份儲存庫、備份及還原 VMC 中託管的 Windows 和 Linux 虛擬機器。
- 使用適用於 NetApp ONTAP 的 FSX 作為備份儲存庫、備份及還原 Microsoft SQL Server 應用程式資料。
- 使用適用於 NetApp ONTAP 的 FSX 作為備份儲存庫、備份及還原 Oracle 應用程式資料。

使用 **Amazon FSX for ONTAP** 的 **NFS** 資料存放區

此解決方案中的所有虛擬機器都位於適用於 ONTAP 補充 NFS 資料存放區的 FSX 上。將 FSX for ONTAP 作為補充 NFS 資料存放區有幾項優點。例如、它可讓您：

- 在雲端中建立可擴充且高可用度的檔案系統、無需複雜的設定與管理。
- 與現有的 VMware 環境整合、讓您使用熟悉的工具和程序來管理雲端資源。
- 從 ONTAP 提供的進階資料管理功能（例如快照和複寫）中獲益、以保護您的資料並確保其可用性。

解決方案部署總覽

此清單提供設定 Veeam 備份與複寫、使用適用於 ONTAP 的 FSX 作為備份儲存庫執行備份與還原工作、以及執行 SQL Server 、 Oracle VM 和資料庫還原所需的高階步驟：

1. 為 ONTAP 檔案系統建立 FSX 、作為 Veeam 備份與複寫的 iSCSI 備份儲存庫。
2. 部署 Veeam Proxy 以分散備份工作負載、並裝載位於 ONTAP 適用的 FSX 上的 iSCSI 備份儲存庫。
3. 設定 Veeam 備份工作來備份 SQL Server 、 Oracle 、 Linux 和 Windows 虛擬機器。
4. 還原 SQL Server 虛擬機器和個別資料庫。
5. 還原 Oracle 虛擬機器和個別資料庫。

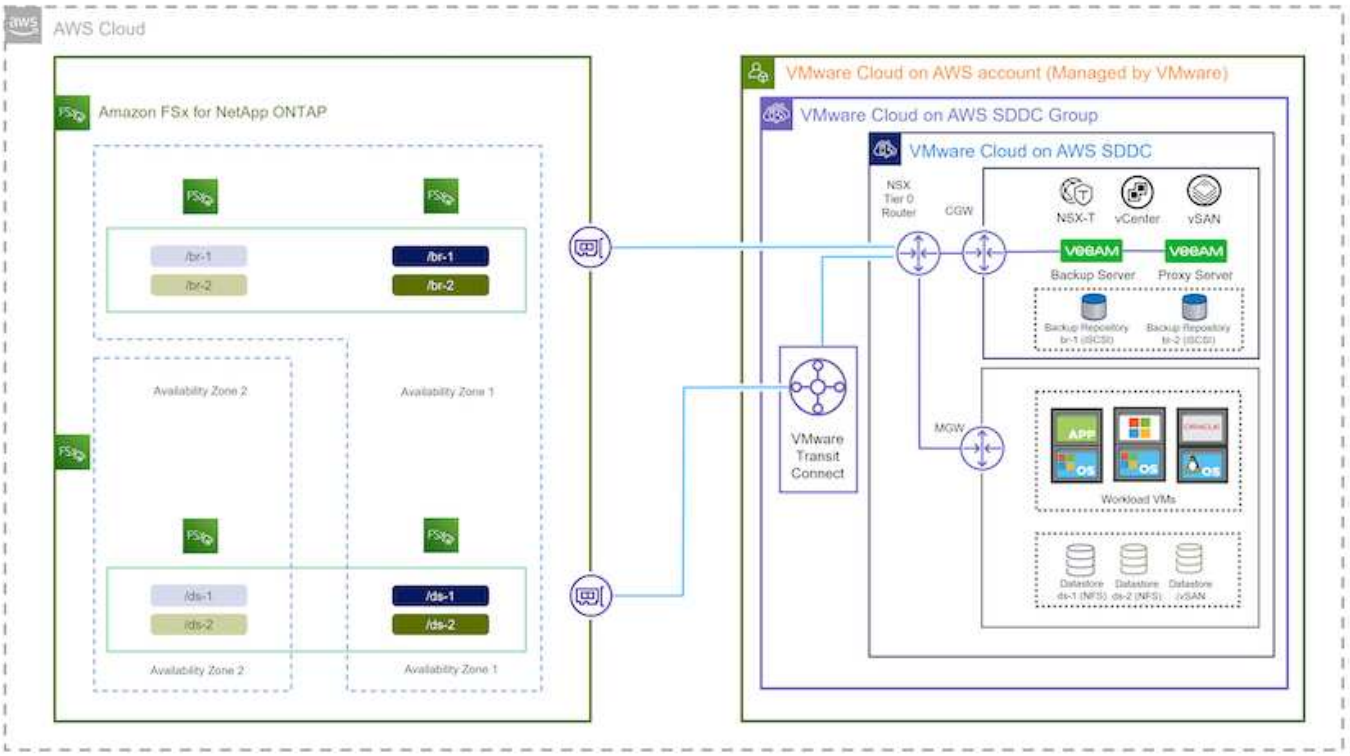
先決條件

此解決方案的目的是展示在 VMware Cloud 中執行、位於由 FSX for NetApp ONTAP 託管的 NFS 資料存放區上的虛擬機器的資料保護功能。本解決方案假設已設定下列元件、可供使用：

1. ONTAP 檔案系統的 FSX 、其中有一或多個 NFS 資料存放區連線至 VMware Cloud 。
2. 安裝了 Veeam 備份與複寫軟體的 Microsoft Windows Server VM 。
    - Veeam 備份與複寫伺服器已使用其 IP 位址或完整網域名稱來探索 vCenter 伺服器。
3. 在解決方案部署期間與 Veeam Backup Proxy 元件一起安裝的 Microsoft Windows Server VM 。
4. 內含 VMDK 的 Microsoft SQL Server VM 、以及位於 ONTAP NFS 資料存放區的 FSX 上的應用程式資料。對於此解決方案、我們在兩個獨立的 VMDK 上有兩個 SQL 資料庫。
    - 附註：最佳實務做法是將資料庫和交易記錄檔放在不同的磁碟機上、如此可改善效能和可靠性。部分原因是交易記錄會依序寫入、而資料庫檔案則是隨機寫入。
5. Oracle 資料庫 VM 搭配 VMDK 、以及位於 ONTAP NFS 資料存放區的 FSX 上的應用程式資料。
6. Linux 和 Windows 檔案伺服器 VM 、其中 VMDK 位於 ONTAP NFS 資料存放區的 FSX 上。
7. Veeam 需要特定的 TCP 連接埠、才能在備份環境中的伺服器和元件之間進行通訊。在 Veeam 備份基礎架構元件上、系統會自動建立必要的防火牆規則。如需網路連接埠需求的完整清單、請參閱的「連接埠」一節 "Veeam Backup and Replication User Guide for VMware vSphere"。

高層架構

本解決方案的測試/驗證是在實驗室中執行、可能與最終部署環境相符或不相符。如需詳細資訊、請參閱下列各節。



硬體/軟體元件

此解決方案的目的是展示在 VMware Cloud 中執行、位於由 FSX for NetApp ONTAP 託管的 NFS 資料存放區上的虛擬機器的資料保護功能。本解決方案假設下列元件已設定好可供使用：

- Microsoft Windows VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上
- Linux （ CentOS ） VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上
- Microsoft SQL Server VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上
  - 兩個資料庫分別託管在不同的 VMDK 上
- Oracle VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上

解決方案部署

在本解決方案中、我們提供詳細說明、說明如何使用 Veeam 備份與複寫軟體來部署及驗證解決方案、以在 AWS 上的 VMware Cloud SDDC 中執行 SQL Server 、 Oracle 、 Windows 和 Linux 檔案伺服器虛擬機器的備份與還原。此解決方案中的虛擬機器位於由 FSX for ONTAP 主控的補充 NFS 資料存放區。此外、 ONTAP 檔案系統的另一個 FSX 可用來裝載 iSCSI 磁碟區、以用於 Veeam 備份儲存庫。

我們將介紹用於 ONTAP 檔案系統建立的 FSX 、用於備份儲存庫的裝載 iSCSI 磁碟區、建立及執行備份工作、以及執行 VM 和資料庫還原。

如需適用於 NetApp ONTAP 的 FSX 詳細資訊、請參閱 "適用於 ONTAP 的 FSX 使用者指南"。

如需 Veeam 備份與複寫的詳細資訊、請參閱 "Veeam說明中心技術文件" 網站。

如需在 AWS 上使用 Veeam Backup and Replication 搭配 VMware Cloud 時的考量與限制、請參閱 "VMware Cloud on AWS 和 VMware Cloud on Dell EMC Support 。考量與限制"。

部署 **Veeam Proxy** 伺服器

Veeam Proxy 伺服器是 Veeam 備份與複寫軟體的元件、在來源與備份或複寫目標之間扮演中介角色。Proxy 伺服器可在本機處理資料、協助最佳化及加速備份工作期間的資料傳輸、並可使用不同的傳輸模式、使用 VMware vStorage API 來存取資料保護、或透過直接儲存存取來存取資料。

選擇 Veeam Proxy 伺服器設計時、請務必考慮所需的並行工作數、以及傳輸模式或儲存存取類型。

如需設定 Proxy 伺服器數量及其系統需求的大小、請參閱 "Veeam VMware vSphere 最佳實務指南"。

Veeam Data Mover 是 Veeam Proxy 伺服器的元件、使用傳輸模式作為從來源取得 VM 資料並將其傳輸至目標的方法。傳輸模式是在備份工作組態期間指定的。您可以使用直接儲存存取、從 NFS 資料存放區增加效率備份。

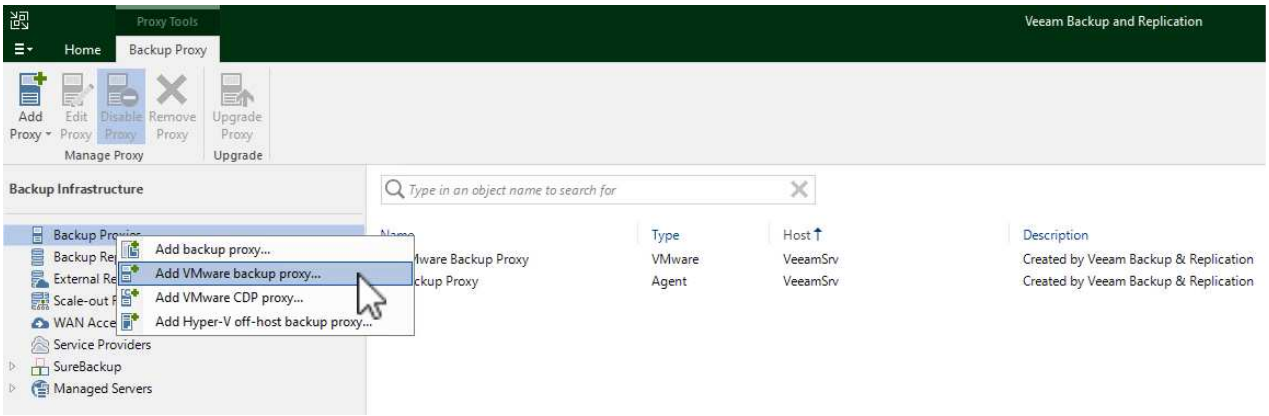
如需傳輸模式的詳細資訊、請參閱 "Veeam Backup and Replication User Guide for VMware vSphere"。

在接下來的步驟中、我們將在 VMware Cloud SDDC 中的 Windows VM 上部署 Veeam Proxy Server 。

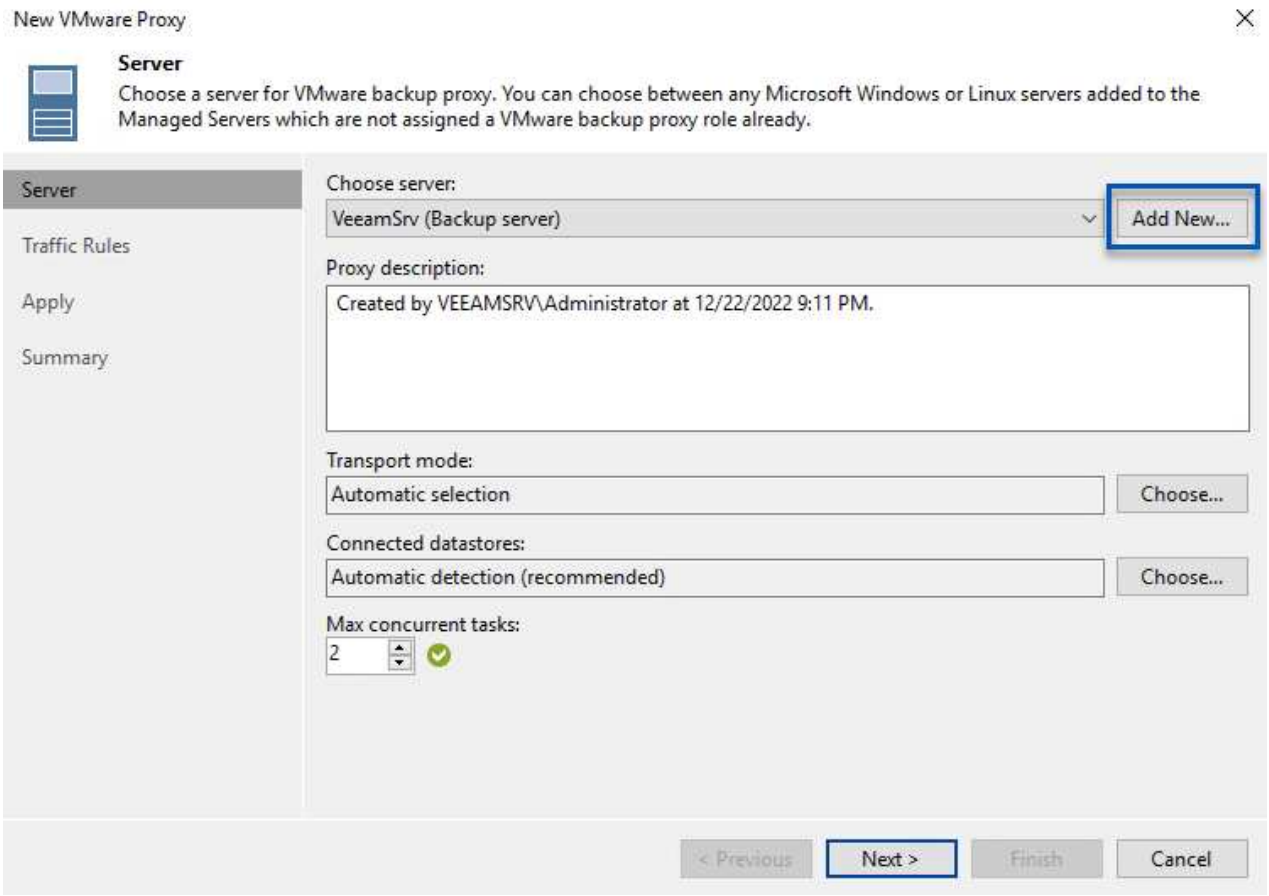
部署 **Veeam Proxy** 以分散備份工作負載

在此步驟中、 Veeam Proxy 會部署至現有的 Windows VM 。如此可在主要 Veeam Backup Server 和 Veeam Proxy 之間分配備份工作。

1. 在 Veeam Backup and Replication 伺服器上、開啟管理主控台、然後在左下角的功能表中選取 * Backup Infrastructure* 。
2. 在 * 備份代理 * 上按一下滑鼠右鍵、然後按一下 * 新增 VMware 備份代理伺服器 … * 以開啟精靈。

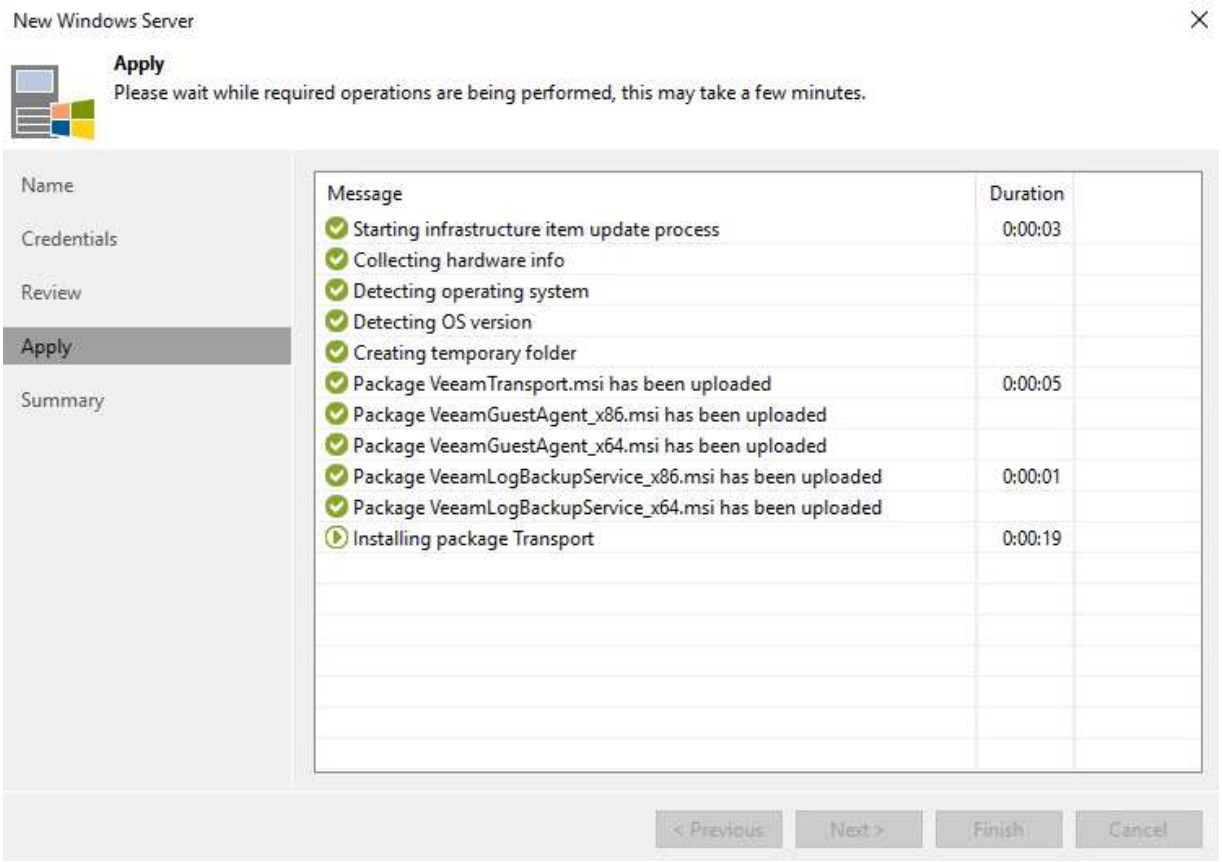


3. 在 * 新增 VMware Proxy* 精靈中、按一下 * 新增 … * 按鈕以新增 Proxy 伺服器。

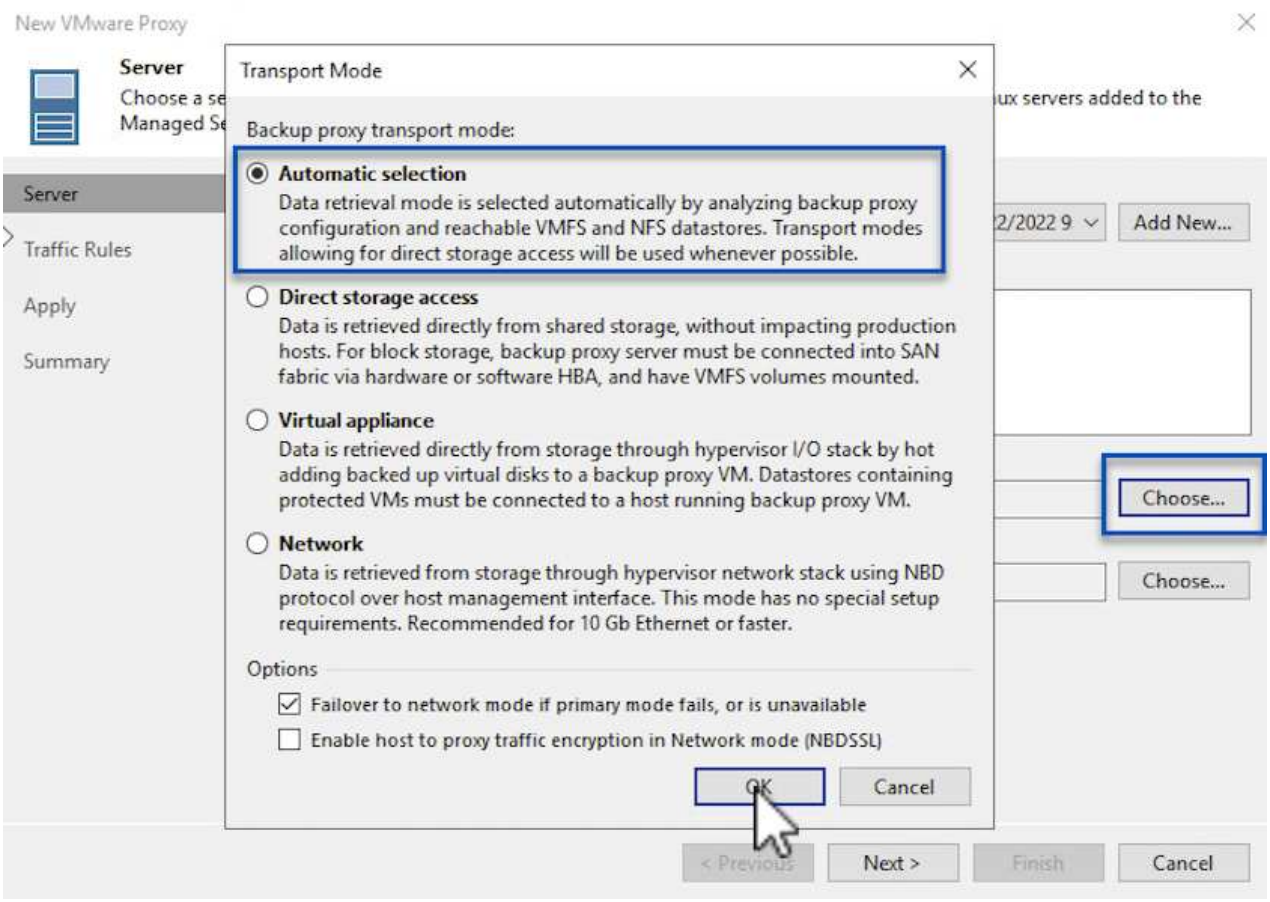


4. 選取以新增 Microsoft Windows 、然後依照提示新增伺服器：
   - 填寫 DNS 名稱或 IP 位址

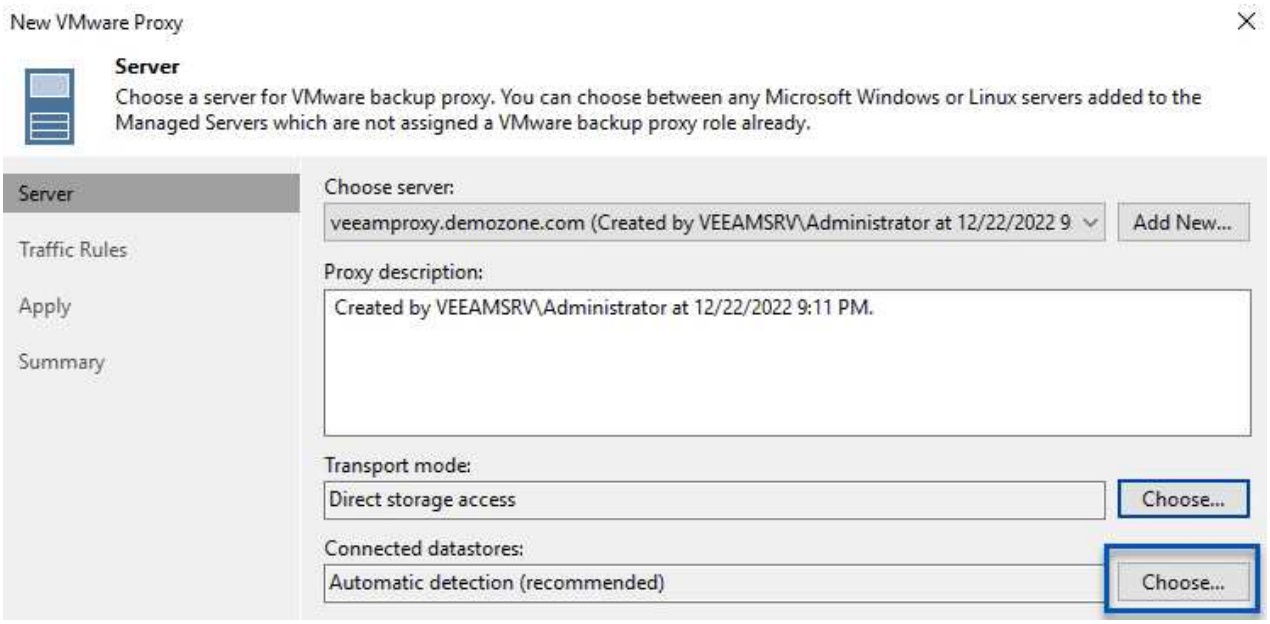
- 選取要用於新系統上認證的帳戶、或新增認證
- 檢閱要安裝的元件、然後按一下 * 套用 * 開始部署

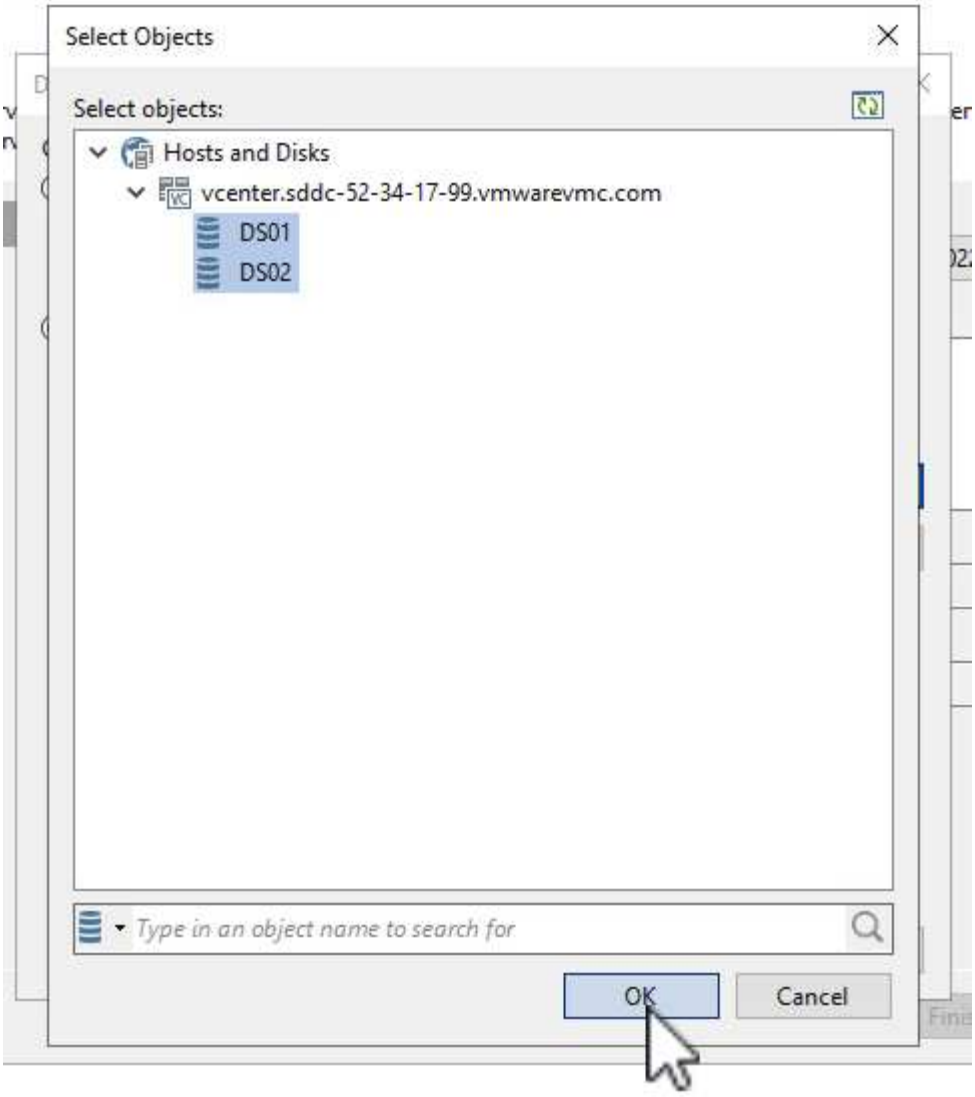


5. 回到 * 新增 VMware Proxy* 精靈、選擇傳輸模式。在我們的案例中、我們選擇 * 自動選擇 * 。

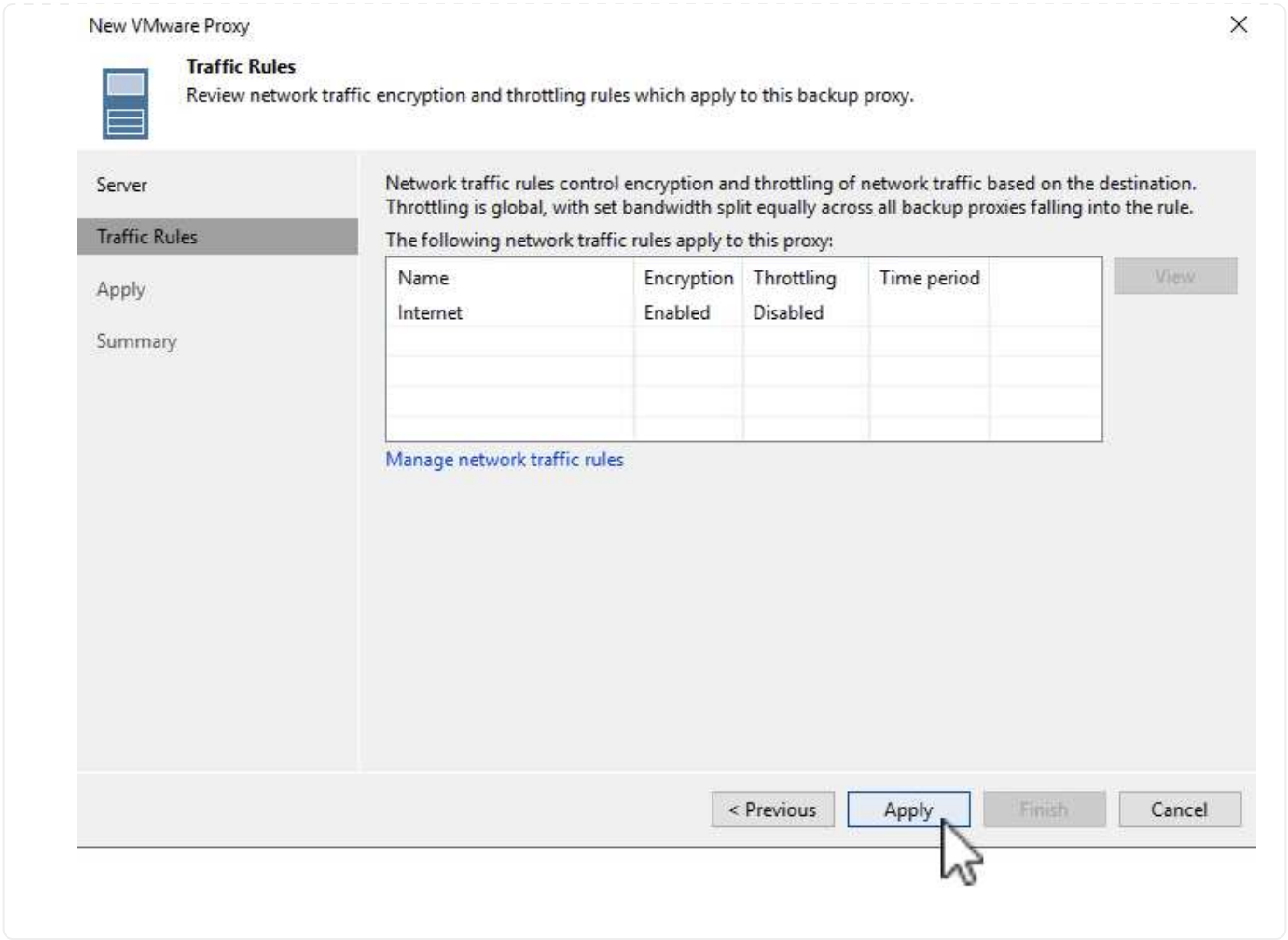


6. 選取您要 VMware Proxy 直接存取的連線資料存放區。





7. 設定並套用任何特定的網路流量規則、例如所需的加密或節流。完成後、按一下 * 套用 * 按鈕以完成部署。



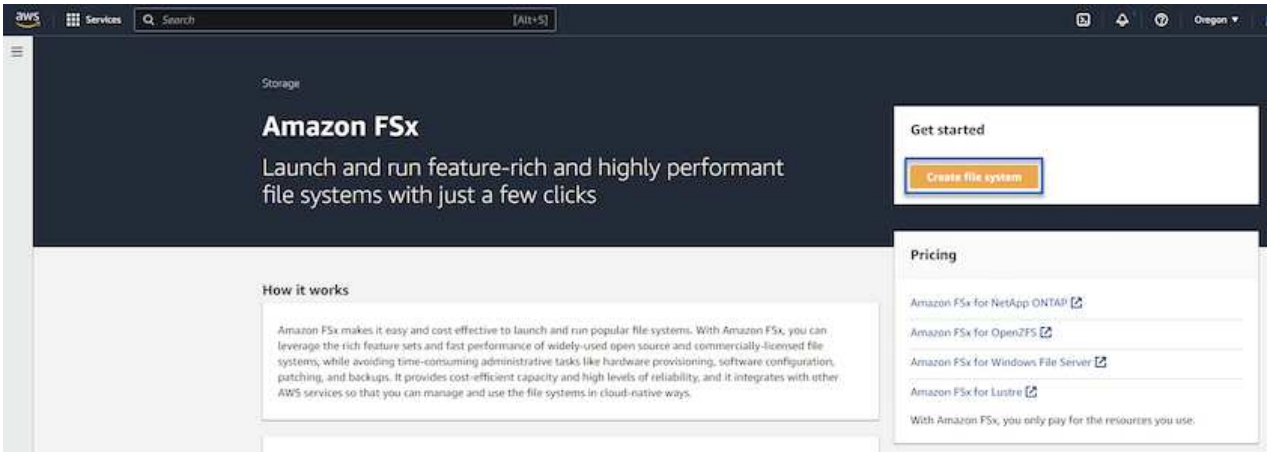
設定儲存與備份儲存庫

主要 Veeam 備份伺服器和 Veeam Proxy 伺服器可以直接連線儲存設備的形式存取備份儲存庫。在本節中、我們將介紹如何為 ONTAP 檔案系統建立 FSX 、將 iSCSI LUN 掛載至 Veeam 伺服器、以及建立備份儲存庫。

為 **ONTAP** 檔案系統建立 **FSX**

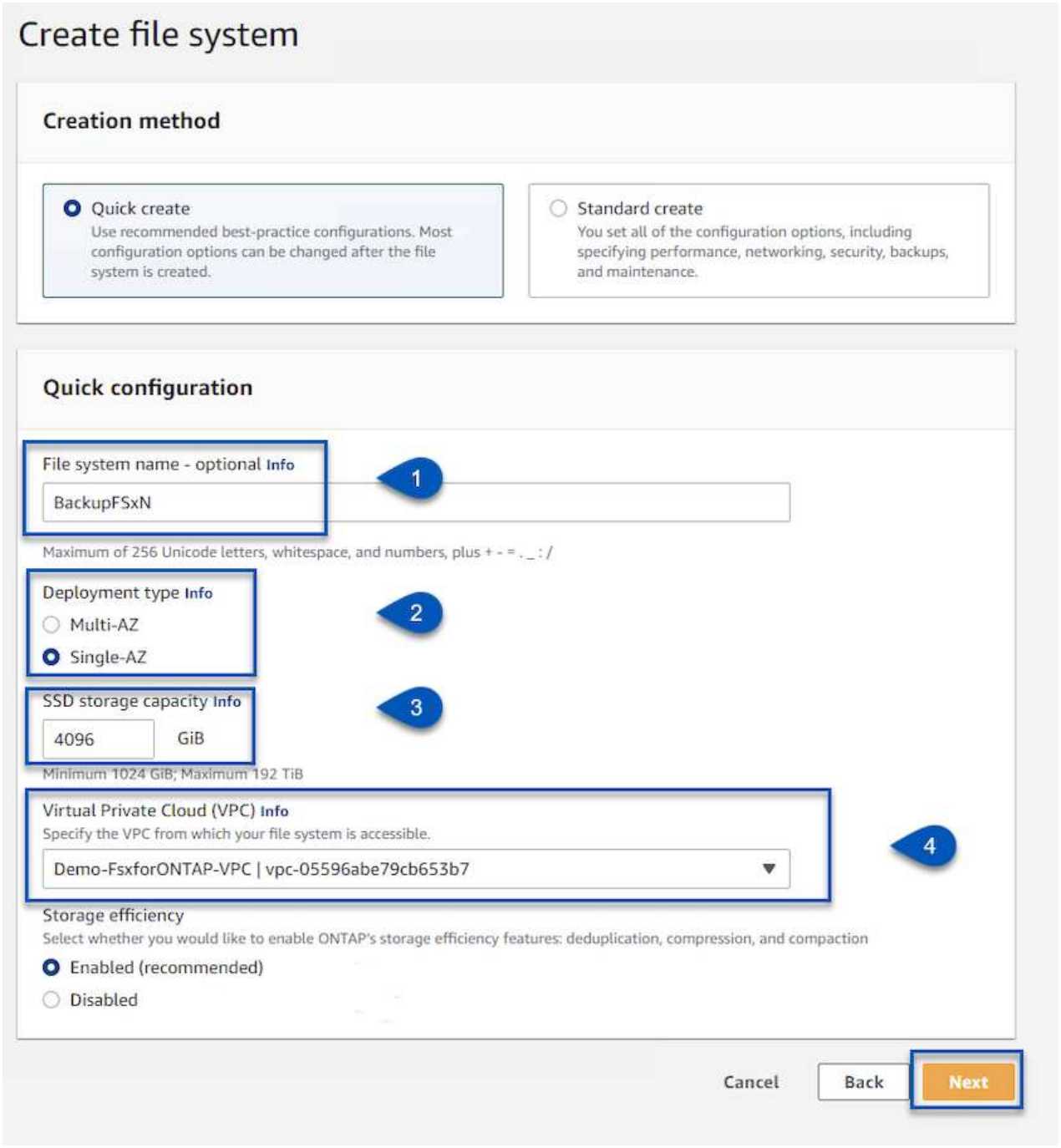
為 ONTAP 檔案系統建立一個 FSX 、用於裝載 Veeam 備份儲存庫的 iSCSI 磁碟區。

1. 在 AWS 主控台、前往 FSX 、然後 * 建立檔案系統 *



2. 選擇 * Amazon FSX for NetApp ONTAP * 、然後選擇 * Next* 繼續。

3. 填寫檔案系統名稱、部署類型、 SSD 儲存容量、以及 ONTAP 叢集的 FSX 所在的 VPC 。這必須是設定為與 VMware Cloud 中的虛擬機器網路通訊的 VPC 。按一下 * 下一步 * 。



4. 檢閱部署步驟、然後按一下 * 建立檔案系統 * 、開始建立檔案系統的程序。

設定及掛載 iSCSI LUN

在適用於 ONTAP 的 FSX 上建立和設定 iSCSI LUN 、並掛載至 Veeam 備份和 Proxy 伺服器。這些 LUN 稍後將用於建立 Veeam 備份儲存庫。

在適用於 ONTAP 的 FSX 上建立 iSCSI LUN 是一個多步驟程序。建立磁碟區的第一步可以在 Amazon FSX 主控台或 NetApp ONTAP CLI 中完成。

如需使用適用於 ONTAP 的 FSX 的詳細資訊、請參閱 "適用於 ONTAP 的 FSX 使用者指南"。

1. 從 NetApp ONTAP CLI 使用下列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. 建立包含 Veeam 備份和 Proxy 伺服器 iSCSI IQN 的啟動器群組、以授予對 LUN 的存取權：

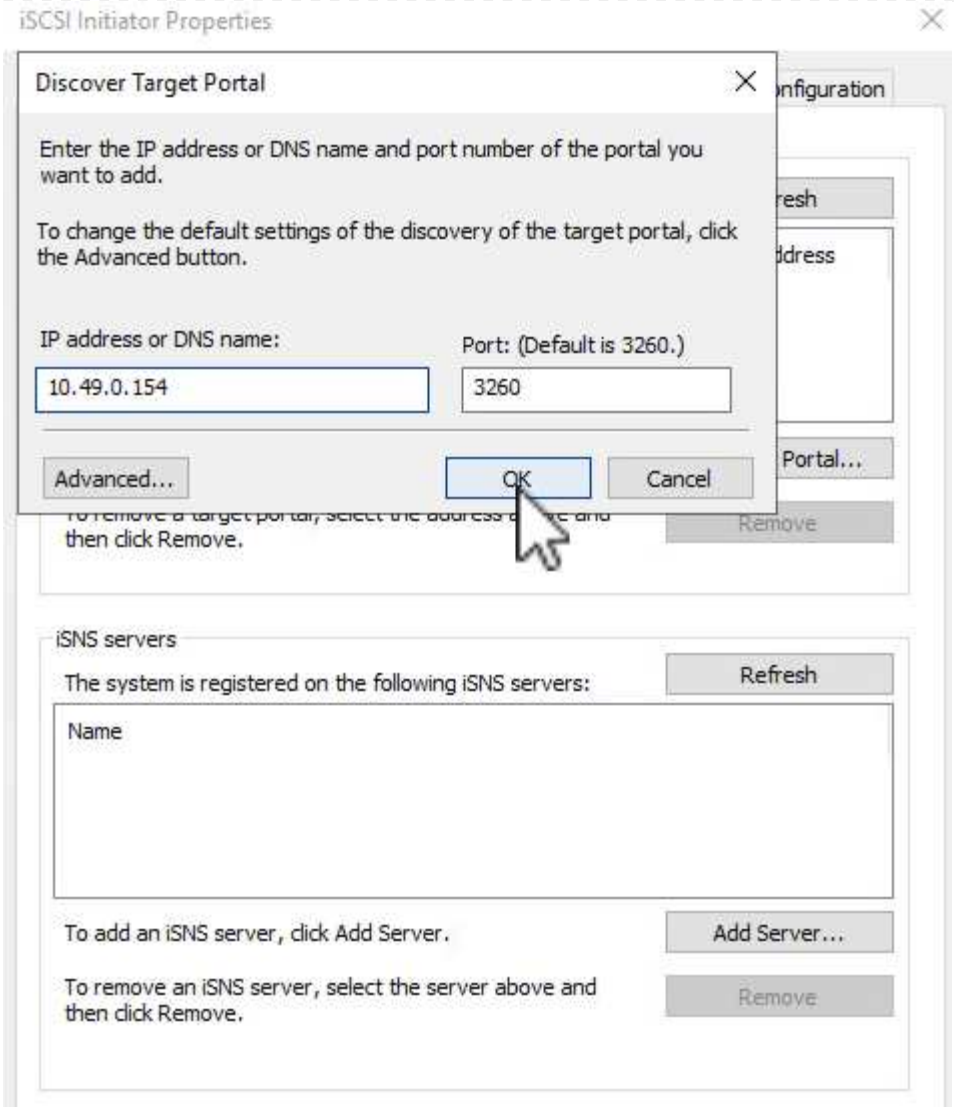
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

若要完成上述步驟、您必須先從 Windows 伺服器上的 iSCSI 啟動器內容擷取 IQN 。

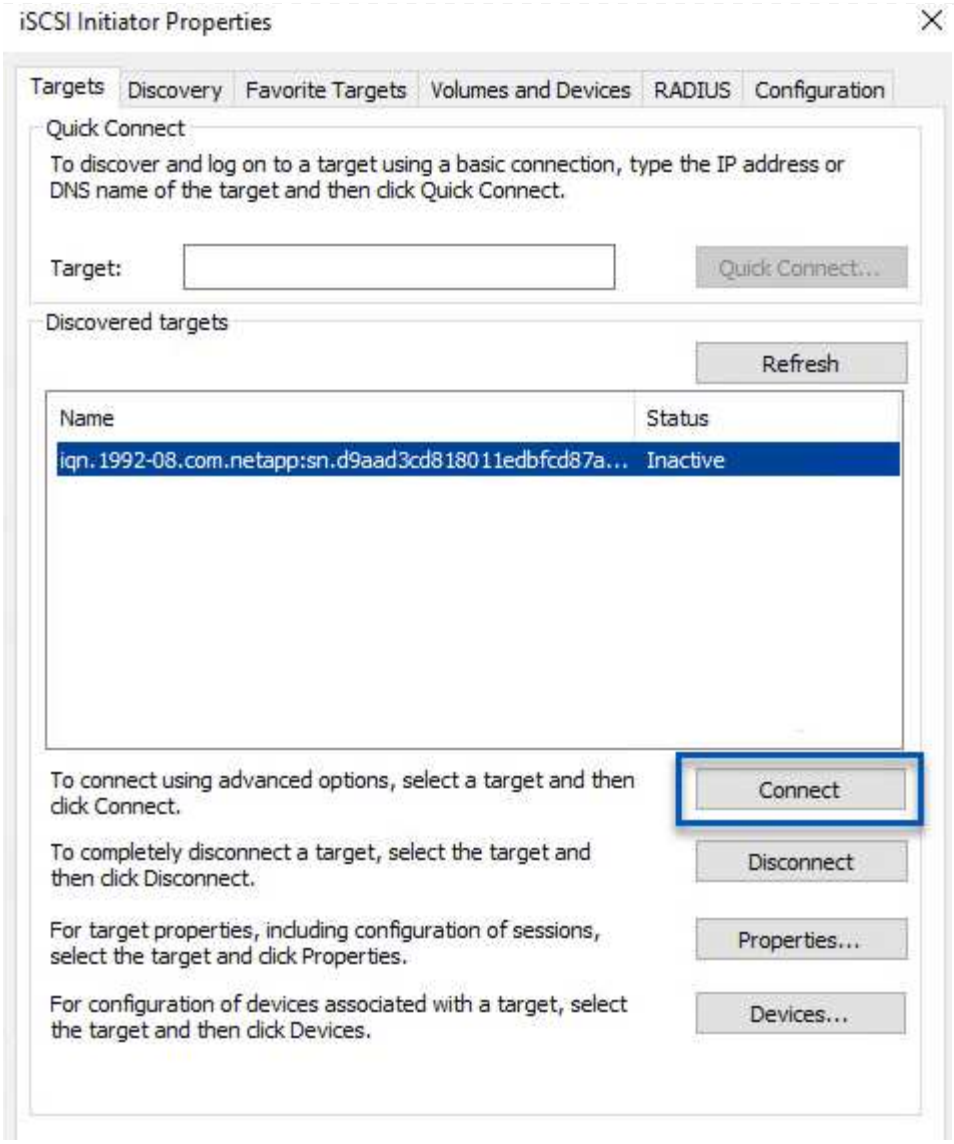
4. 最後、將LUN對應至您剛建立的啟動器群組：

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

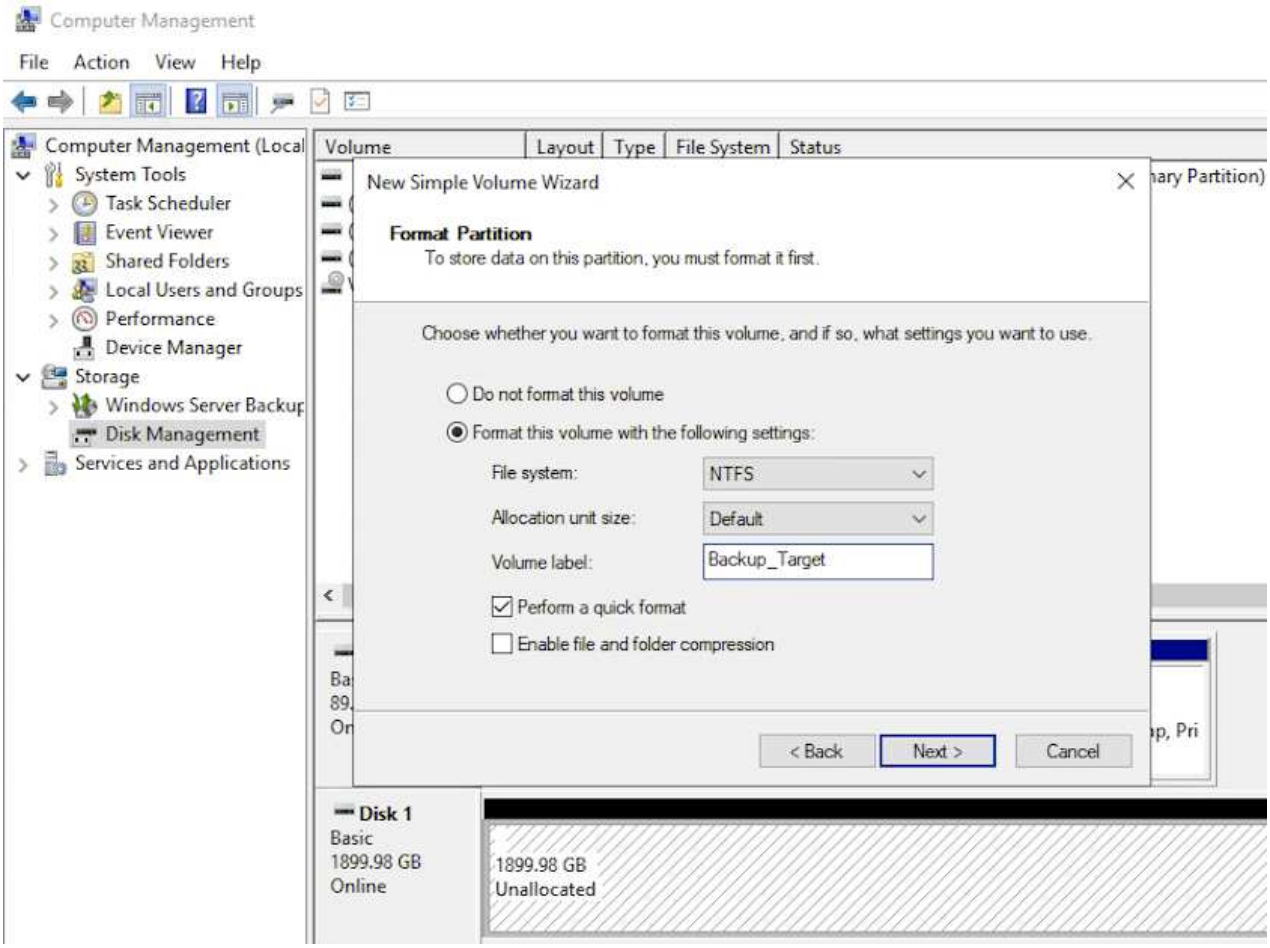
5. 若要掛載 iSCSI LUN 、請登入 Veeam 備份與複寫伺服器、然後開啟 iSCSI 啟動器內容。移至 * Discover （探索） * 標籤、然後輸入 iSCSI 目標 IP 位址。



6. 在 * 目標 * 索引標籤上、反白非作用中的 LUN 、然後按一下 * 連線 * 。勾選 * 啟用多重路徑 * 方塊、然後按一下 * 確定 * 以連線至 LUN 。



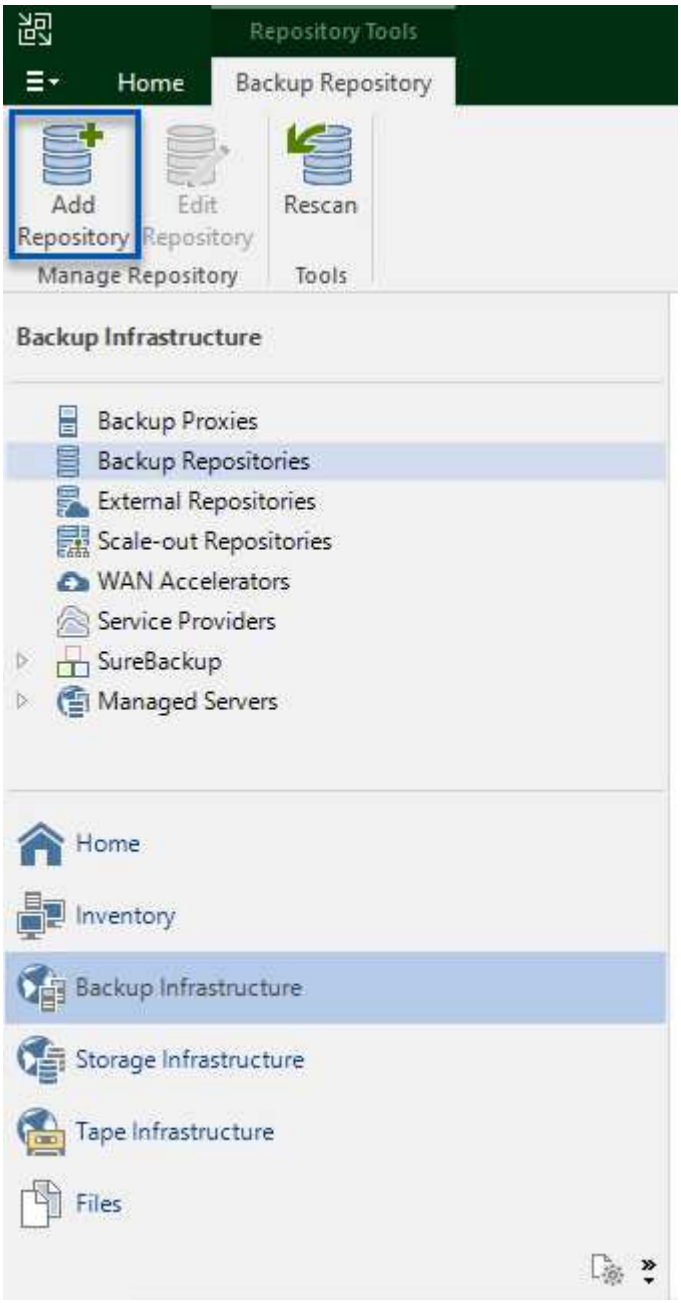
7. 在磁碟管理公用程式中、初始化新的 LUN 、並建立具有所需名稱和磁碟機代號的磁碟區。勾選 * 啟用多重路徑 * 方塊、然後按一下 * 確定 * 以連線至 LUN 。



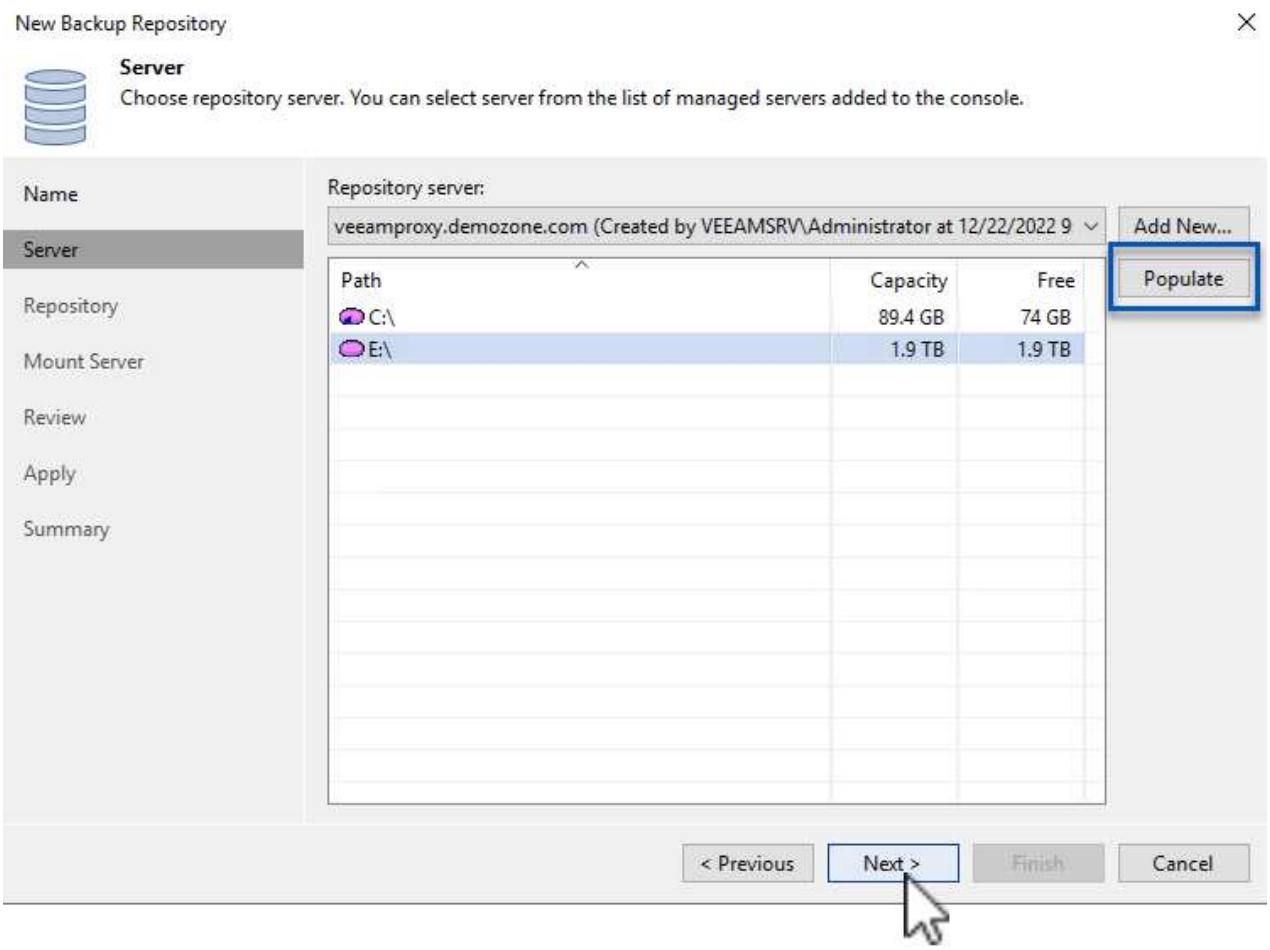
8. 重複這些步驟、在 Veeam Proxy 伺服器上掛載 iSCSI 磁碟區。

在 Veeam Backup and Replication 主控台中、為 Veeam Backup 和 Veeam Proxy 伺服器建立備份儲存庫。這些儲存庫將作為虛擬機器備份的備份目標。

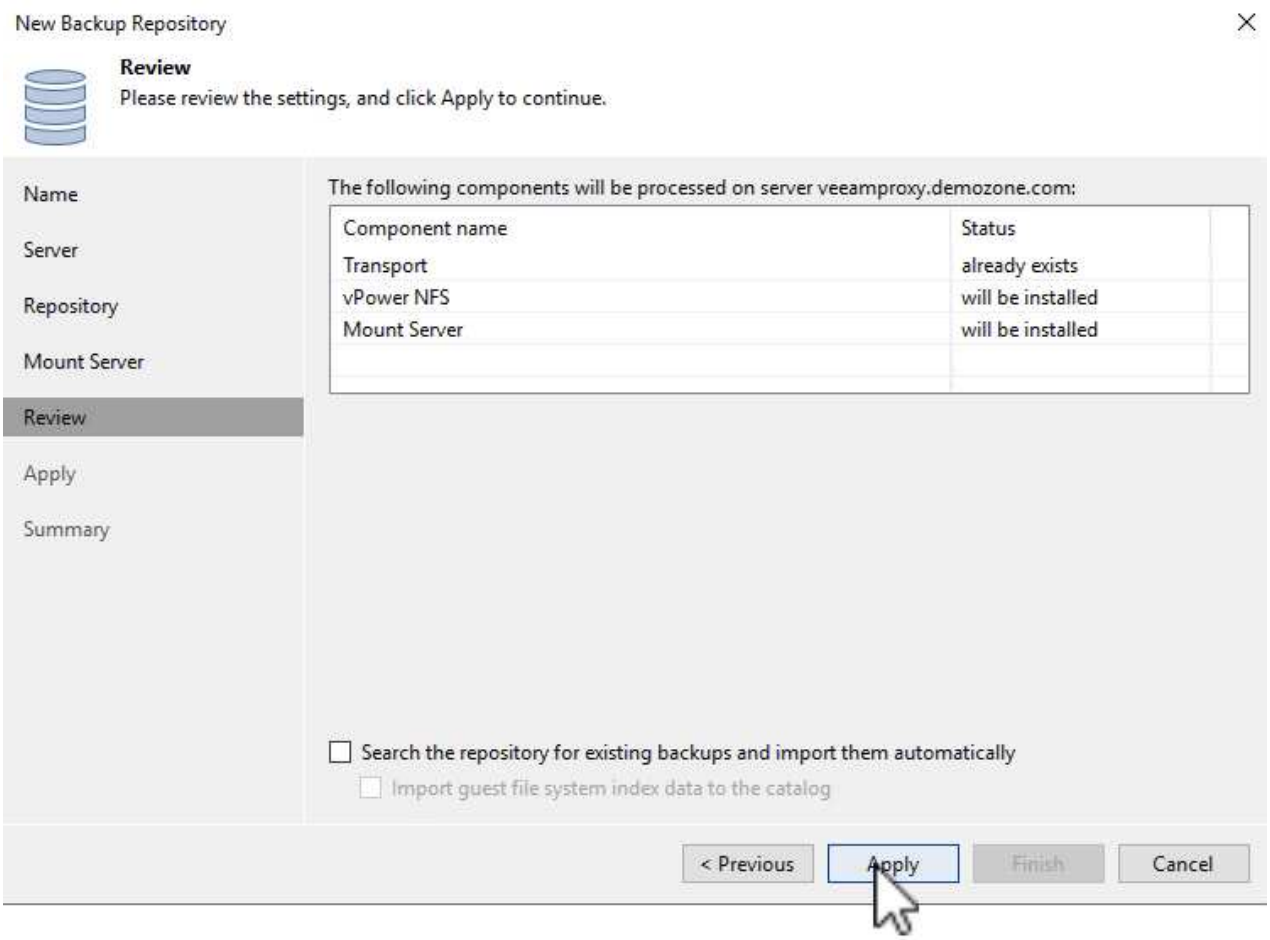
1. 在 Veeam Backup and Replication 主控台中、按一下左下角的 * Backup Infrastructure* 、然後選取 * 新增儲存庫 *



2. 在「新增備份儲存庫」精靈中、輸入儲存庫的名稱、然後從下拉式清單中選取伺服器、然後按一下「 * 填入 * 」按鈕以選擇要使用的 NTFS 磁碟區。



3. 在下一頁中、選擇在執行進階還原時、用來將備份掛載到的掛載伺服器。依預設、這是連接儲存庫儲存設備的相同伺服器。
4. 檢閱您的選擇、然後按一下 * 套用 * 以開始建立備份儲存庫。



5. 對任何其他 Proxy 伺服器重複這些步驟。

設定 **Veeam** 備份工作

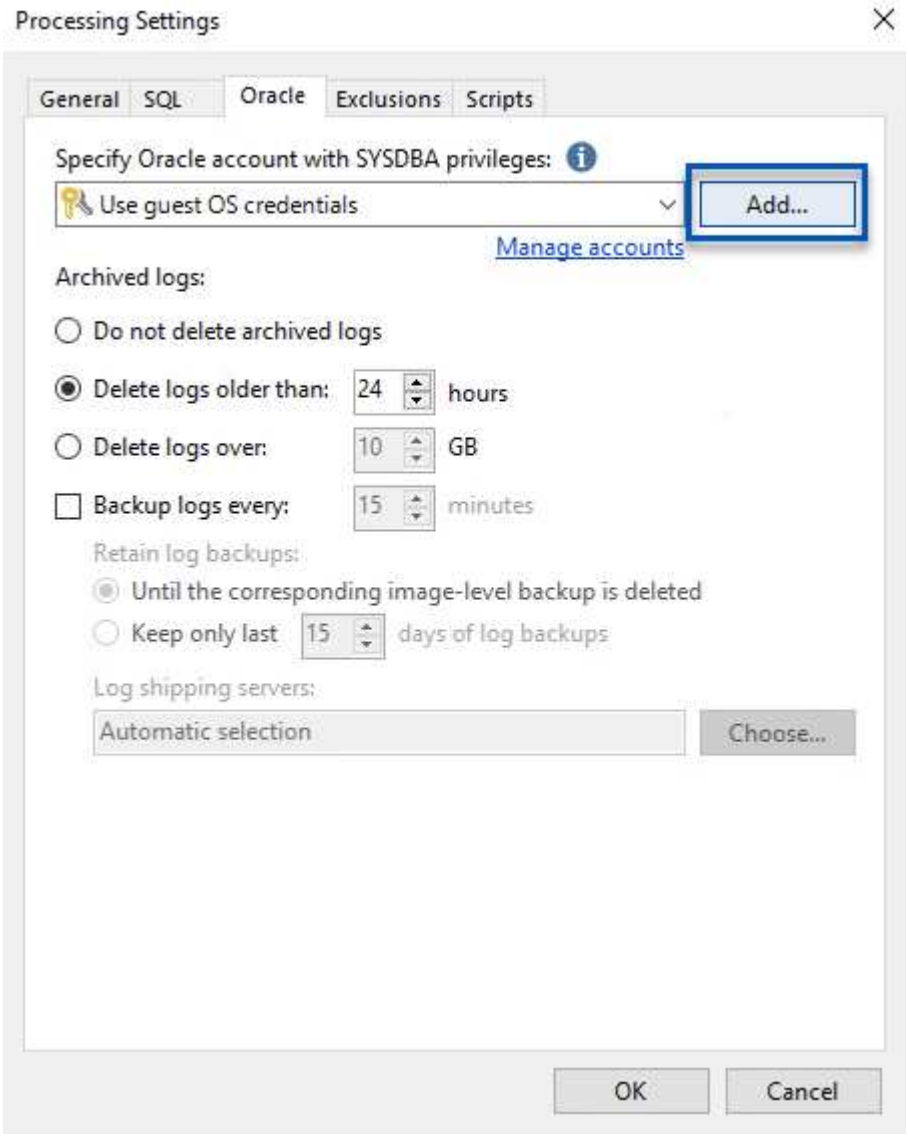
應使用上一節的備份儲存庫來建立備份工作。建立備份工作是任何儲存系統管理員的正常作業、我們並未涵蓋此處的所有步驟。如需在Veeam中建立備份工作的完整資訊、請參閱 "Veeam說明中心技術文件"。

在本解決方案中、會針對下列項目分別建立備份工作：

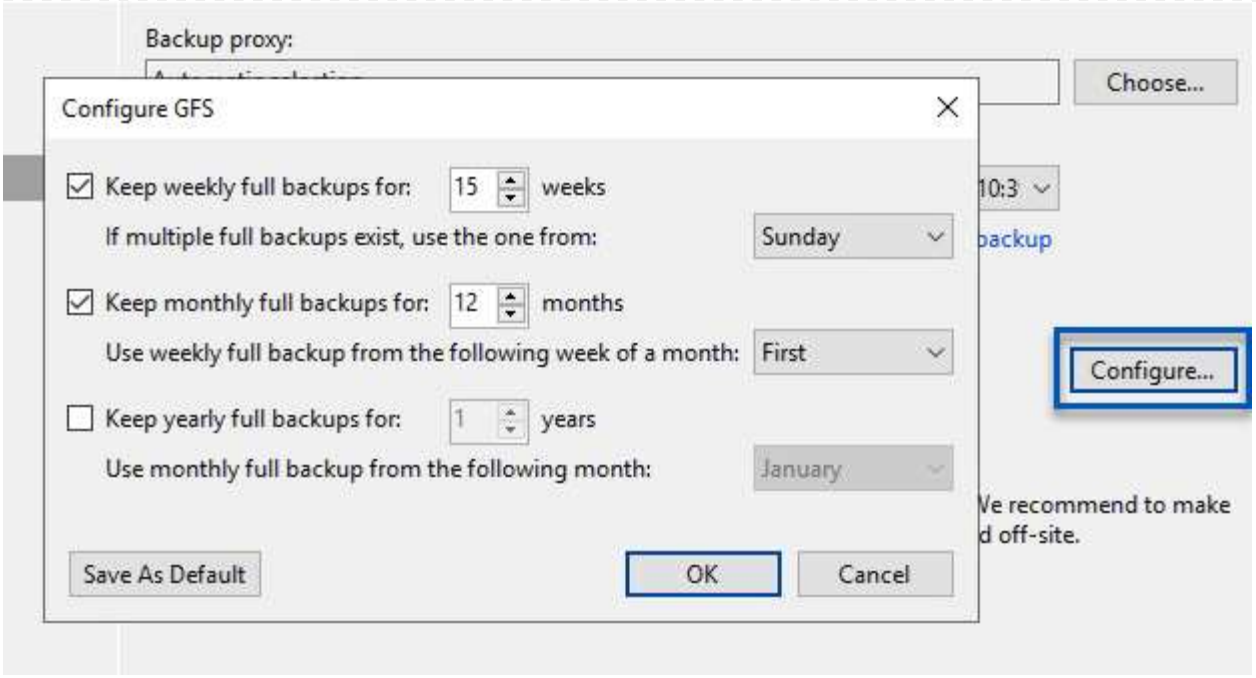
- Microsoft Windows SQL Server
- Oracle 資料庫伺服器
- Windows 檔案伺服器
- Linux 檔案伺服器

設定 **Veeam** 備份工作時的一般考量

1. 啟用應用程式感知處理、以建立一致的備份並執行交易記錄處理。
2. 啟用應用程式感知處理後、請將具有管理員權限的正確認證新增至應用程式、因為這可能與來賓作業系統認證不同。



3. 若要管理備份的保留原則、請勾選 * 保留某些完整備份以供歸檔之用 * 、然後按一下 * 組態 … * 按鈕以設定原則。



使用 **Veeam** 完整還原還原應用程式 **VM**

使用 Veeam 執行完整還原是執行應用程式還原的第一步。我們驗證了 VM 的完整還原功能已開啟、而且所有服務都正常執行。

還原伺服器是任何儲存系統管理員的常用項目之一、我們並未涵蓋此處的所有步驟。如需在 Veeam 中執行完整還原的完整資訊、請參閱 "Veeam說明中心技術文件"。

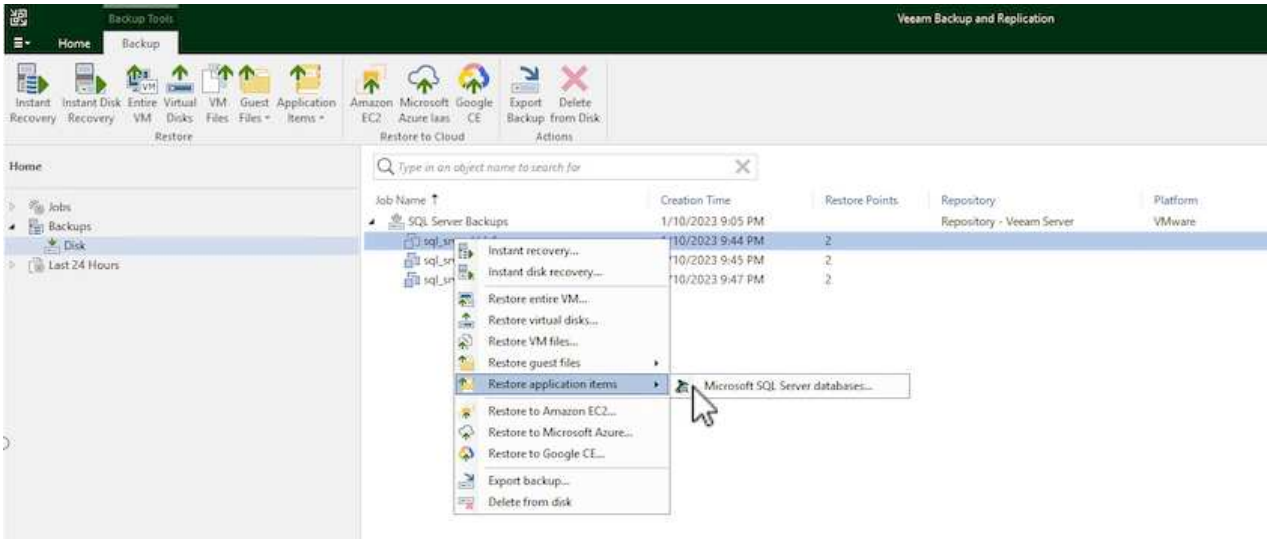
還原 **SQL Server** 資料庫

Veeam 備份與複寫提供數種還原 SQL Server 資料庫的選項。在此驗證中、我們使用 Veeam Explorer for SQL Server 搭配 Instant Recovery 來執行 SQL Server 資料庫的還原。SQL Server Instant Recovery 是一項功能、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。這項快速恢復程序可將停機時間降至最低、並確保業務持續運作。其運作方式如下：

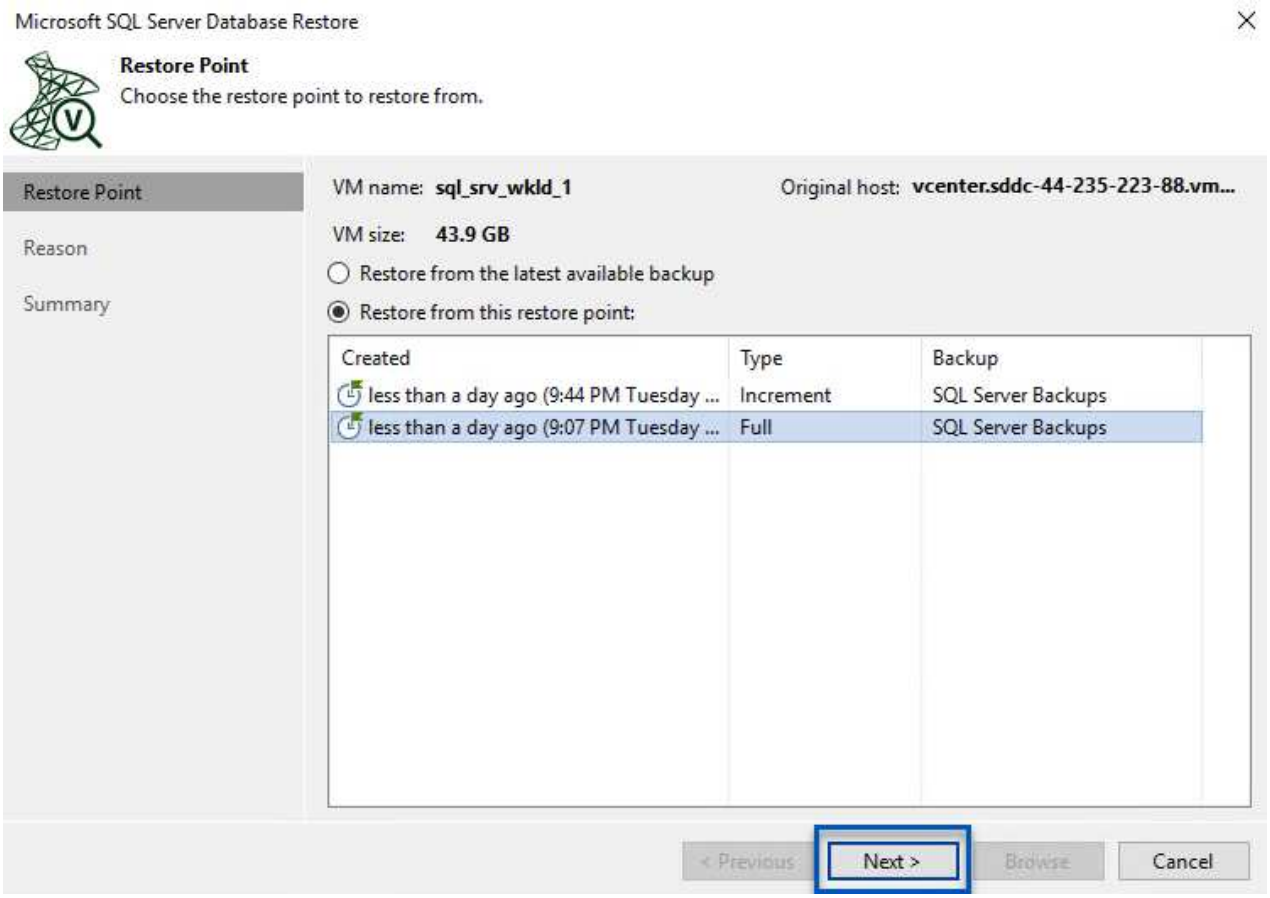
- Veeam Explorer * 裝載包含要還原的 SQL Server 資料庫的備份 * 。
- 軟體 * 直接從掛載的檔案發佈資料庫 * 、使其可在目標 SQL Server 執行個體上作為暫存資料庫存取。
- 在使用暫存資料庫時、 Veeam Explorer * 會將使用者查詢 * 重新導向至此資料庫、確保使用者可以繼續存取及使用資料。
- 在背景中、 Veeam * 會執行完整的資料庫還原 * 、將資料從暫存資料庫傳輸到原始資料庫位置。
- 完整資料庫還原完成後、 Veeam Explorer * 會將使用者查詢切換回原始 * 資料庫、並移除暫存資料庫。

使用 **Veeam Explorer Instant Recovery** 還原 **SQL Server** 資料庫

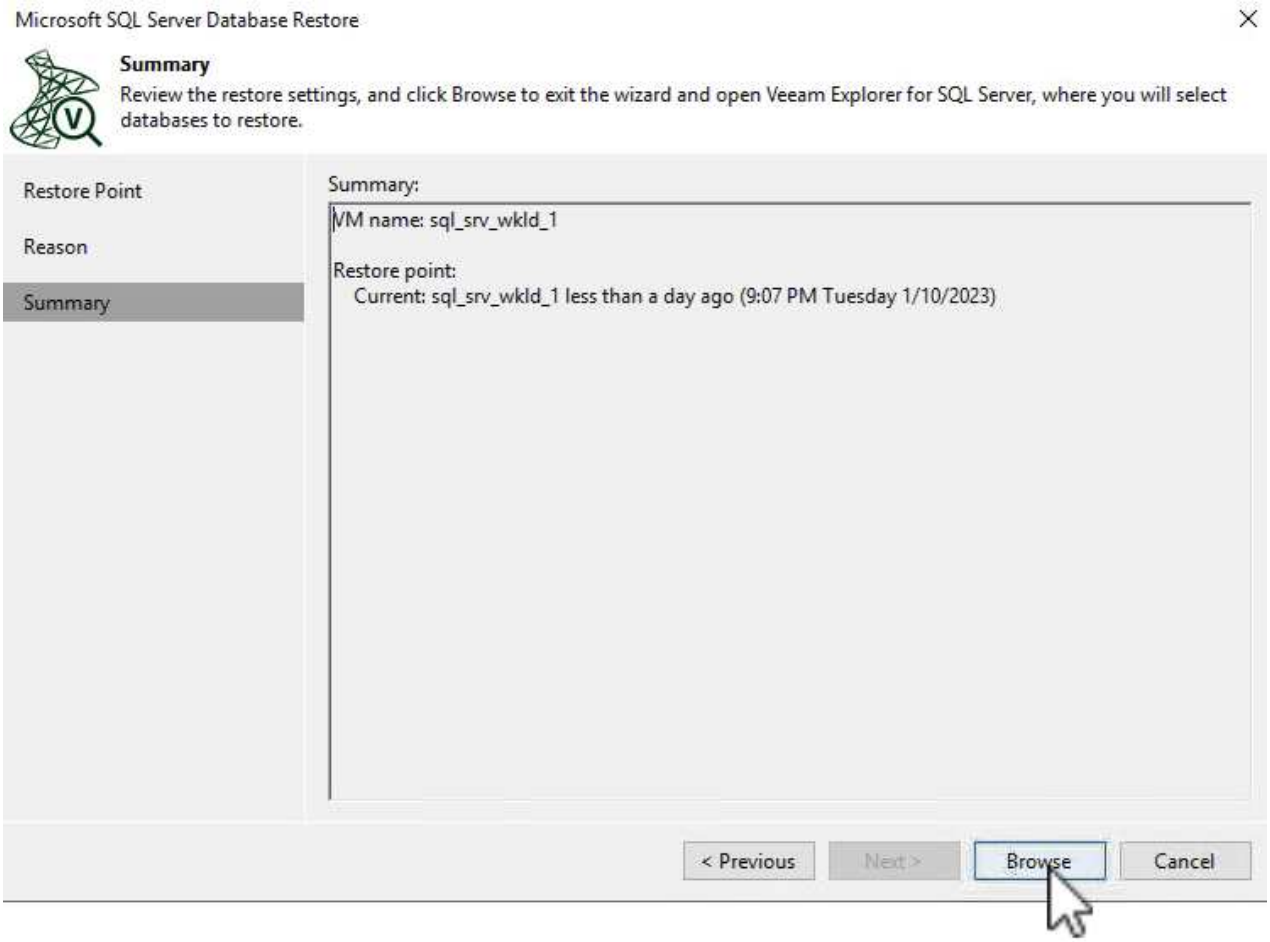
1. 在 Veeam 備份與複寫主控台中、瀏覽至 SQL Server 備份清單、在伺服器上按一下滑鼠右鍵、然後選取 * 還原應用程式項目 * 、再選取 * Microsoft SQL Server 資料庫 … * 。



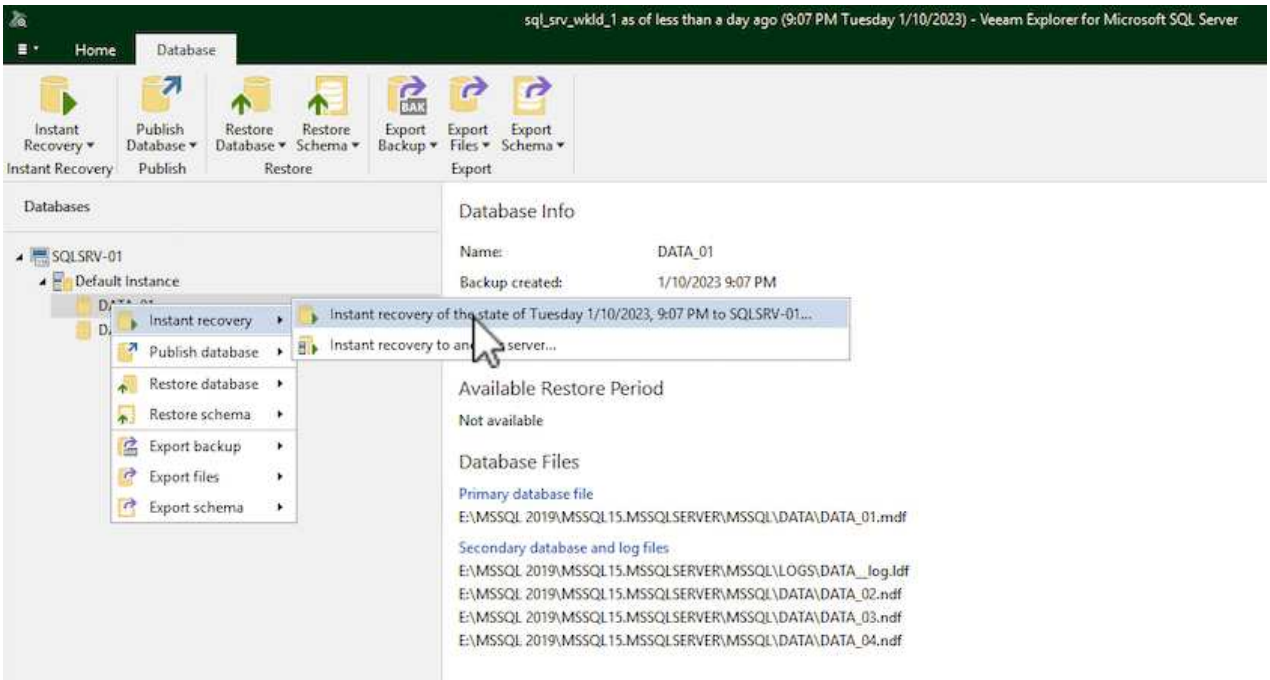
2. 在 Microsoft SQL Server 資料庫還原精靈中、從清單中選取還原點、然後按一下 * 下一步 * 。



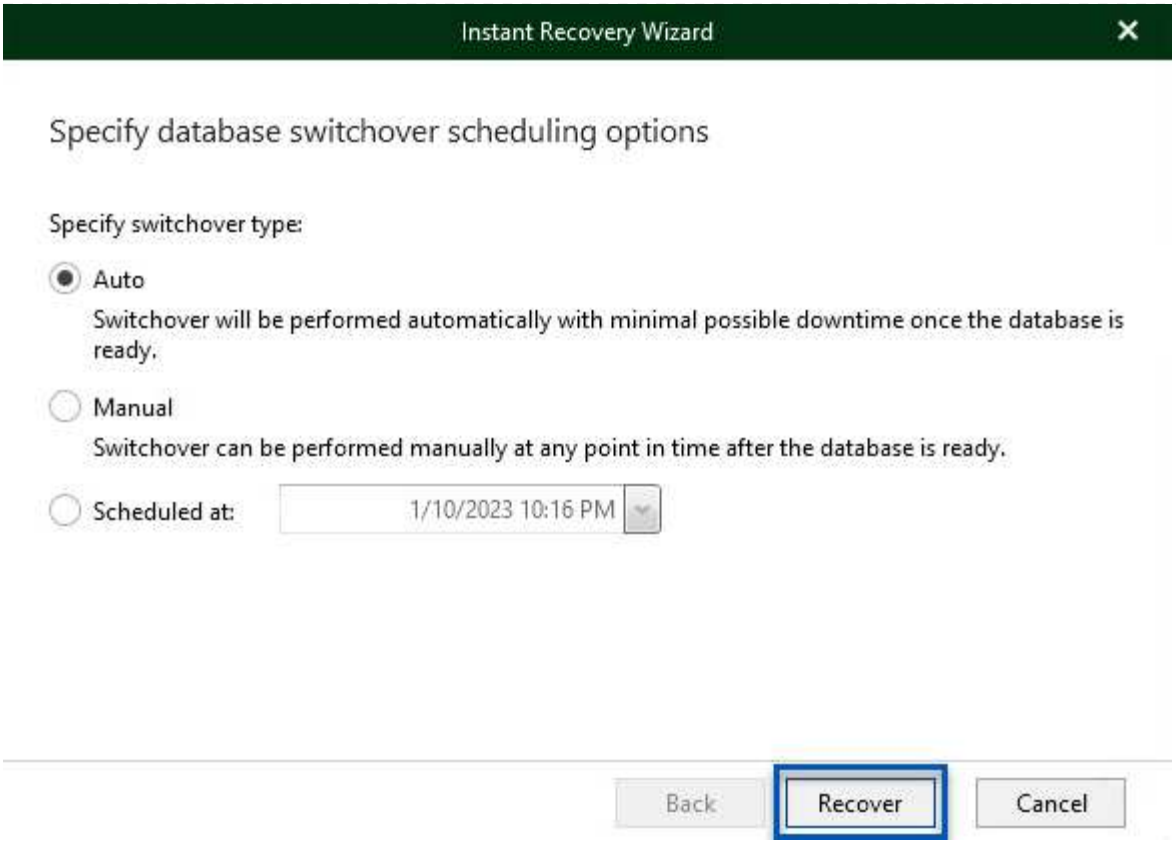
3. 如有需要、請輸入 * 還原原因 * 、然後按一下「摘要」頁面上的 * 瀏覽 * 按鈕、啟動適用於 Microsoft SQL Server 的 Veeam Explorer 。



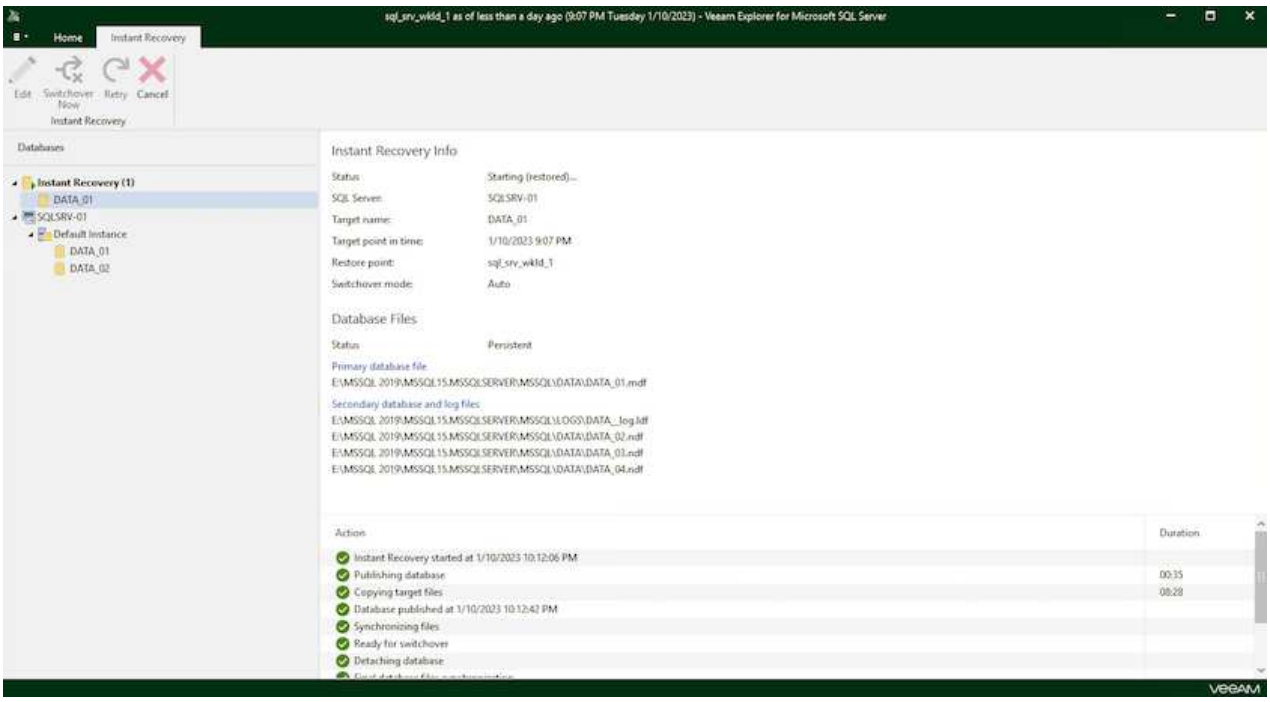
4. 在 Veeam Explorer 中展開資料庫執行個體清單、按一下滑鼠右鍵並選取 * 立即還原 * 、然後選取要還原的特定還原點。



5. 在即時恢復嚮導中指定轉換類型。這可以在最短停機時間內自動進行、手動或在指定時間進行。然後按一下 * 恢復 * 按鈕開始還原程序。



6. 可從 Veeam Explorer 監控還原程序。



如需使用 Veeam Explorer 執行 SQL Server 還原作業的詳細資訊、請參閱中的 Microsoft SQL Server 一節 "Veeam Explorers 使用者指南"。

使用 **Veeam Explorer** 還原 **Oracle** 資料庫

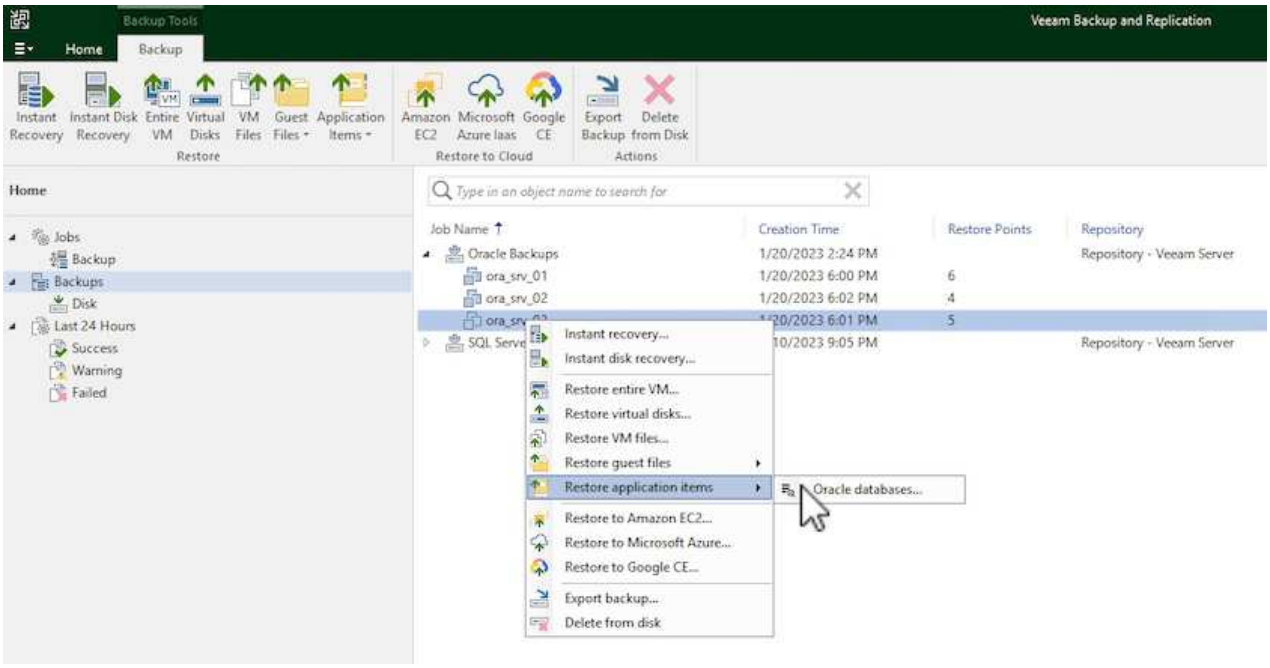
Veeam Explorer for Oracle 資料庫提供使用 Instant Recovery 執行標準 Oracle 資料庫還原或不中斷還原的功能。它也支援發佈資料庫、可快速存取、還原 Data Guard 資料庫、以及從 RMAN 備份還原。

如需使用 Veeam Explorer 執行 Oracle 資料庫還原作業的詳細資訊、請參閱中的 Oracle 一節 "Veeam Explorers 使用者指南"。

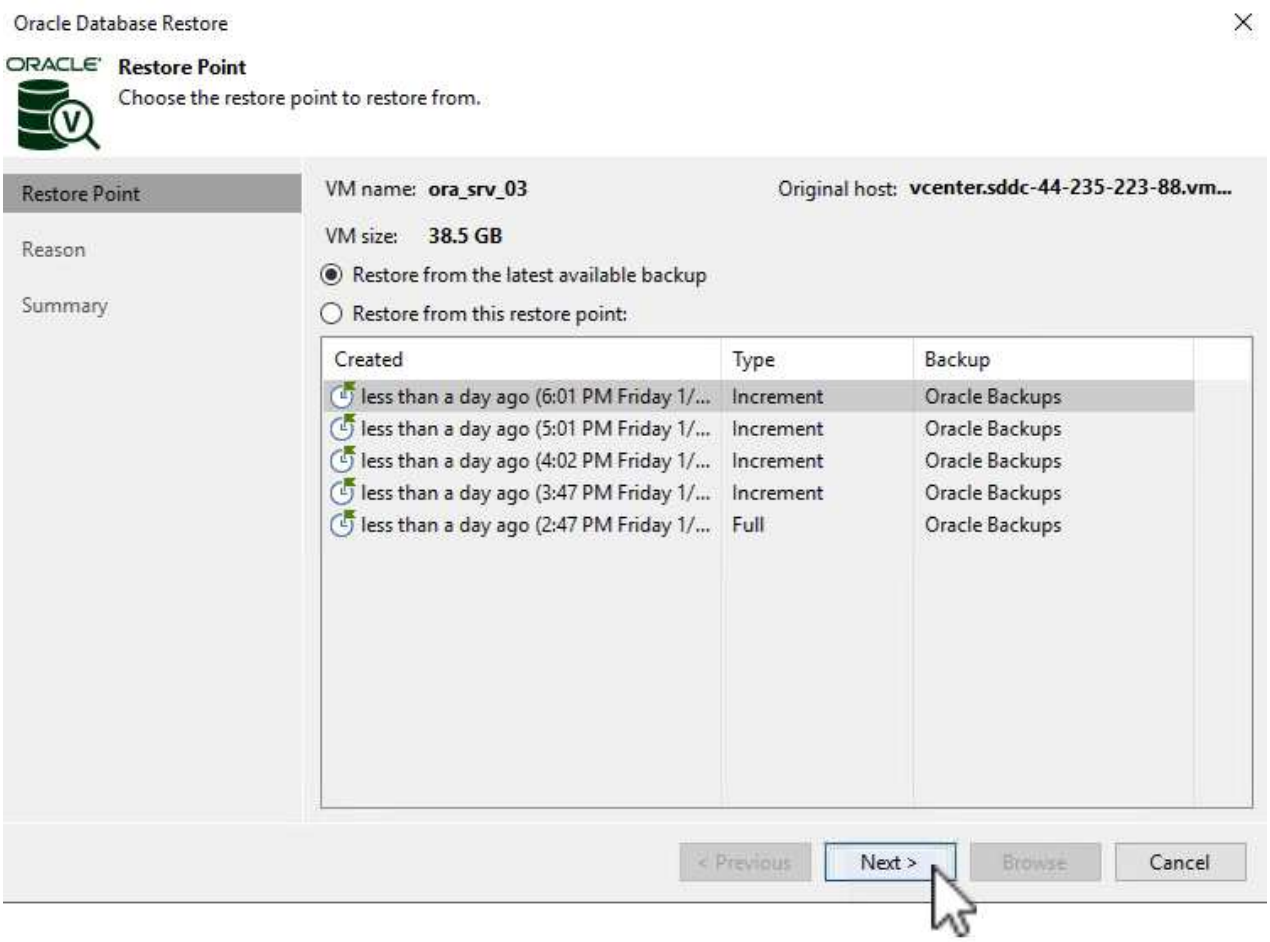
使用 **Veeam Explorer** 還原 **Oracle** 資料庫

在本節中、使用 Veeam Explorer 將 Oracle 資料庫還原至不同的伺服器。

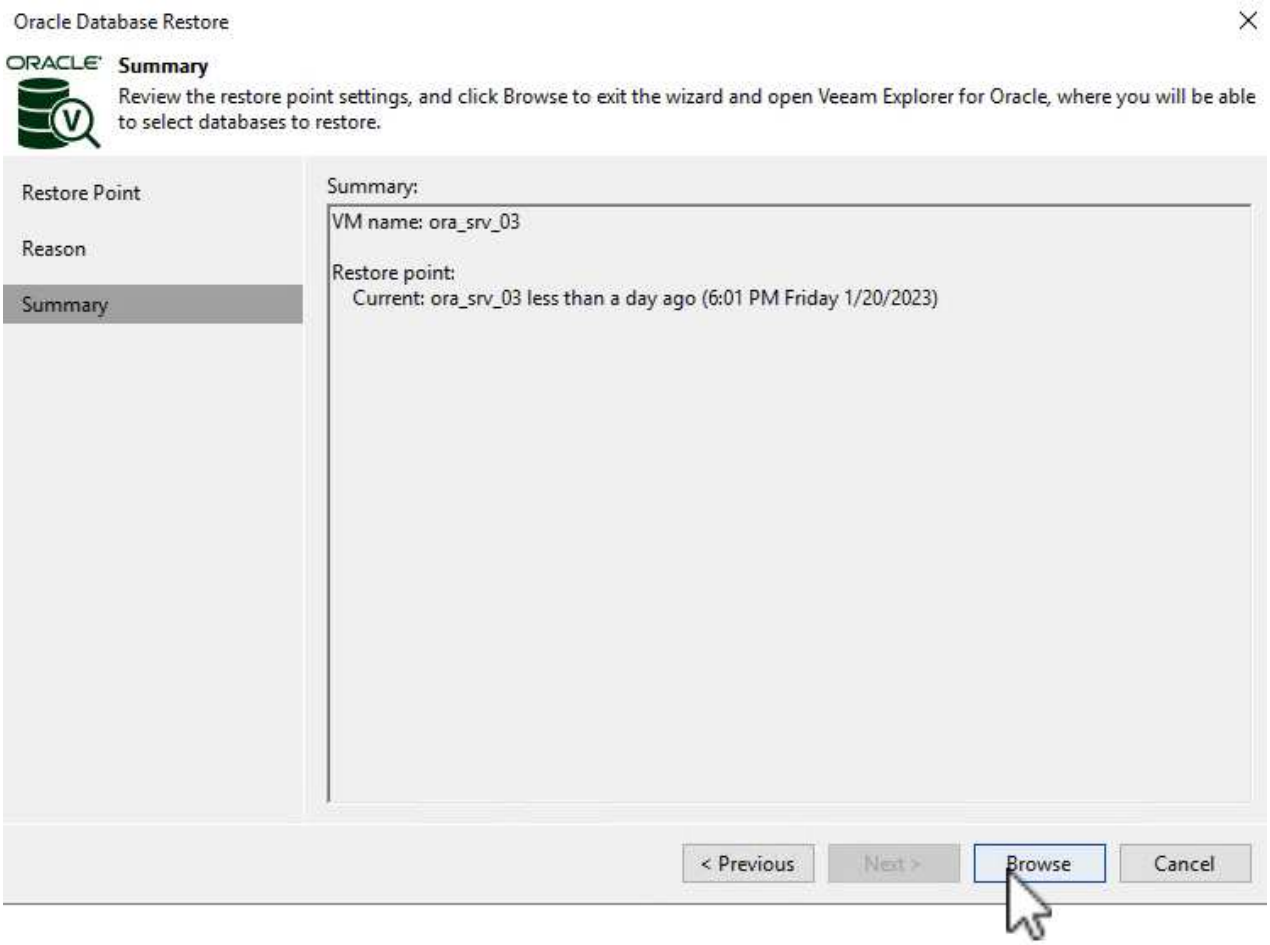
1. 在 Veeam 備份與複寫主控台中、瀏覽至 Oracle 備份清單、在伺服器上按一下滑鼠右鍵、然後選取 * 還原應用程式項目 * 、再選取 * Oracle 資料庫 … * 。



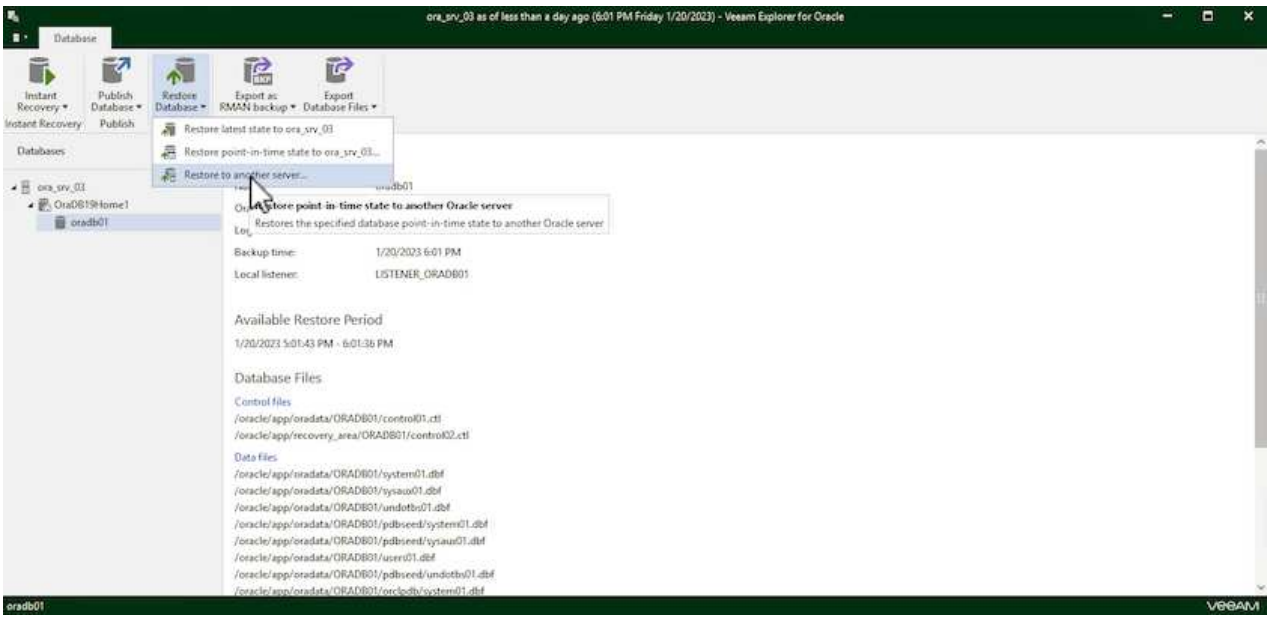
2. 在 Oracle 資料庫還原精靈中、從清單中選取還原點、然後按一下 * 下一步 * 。



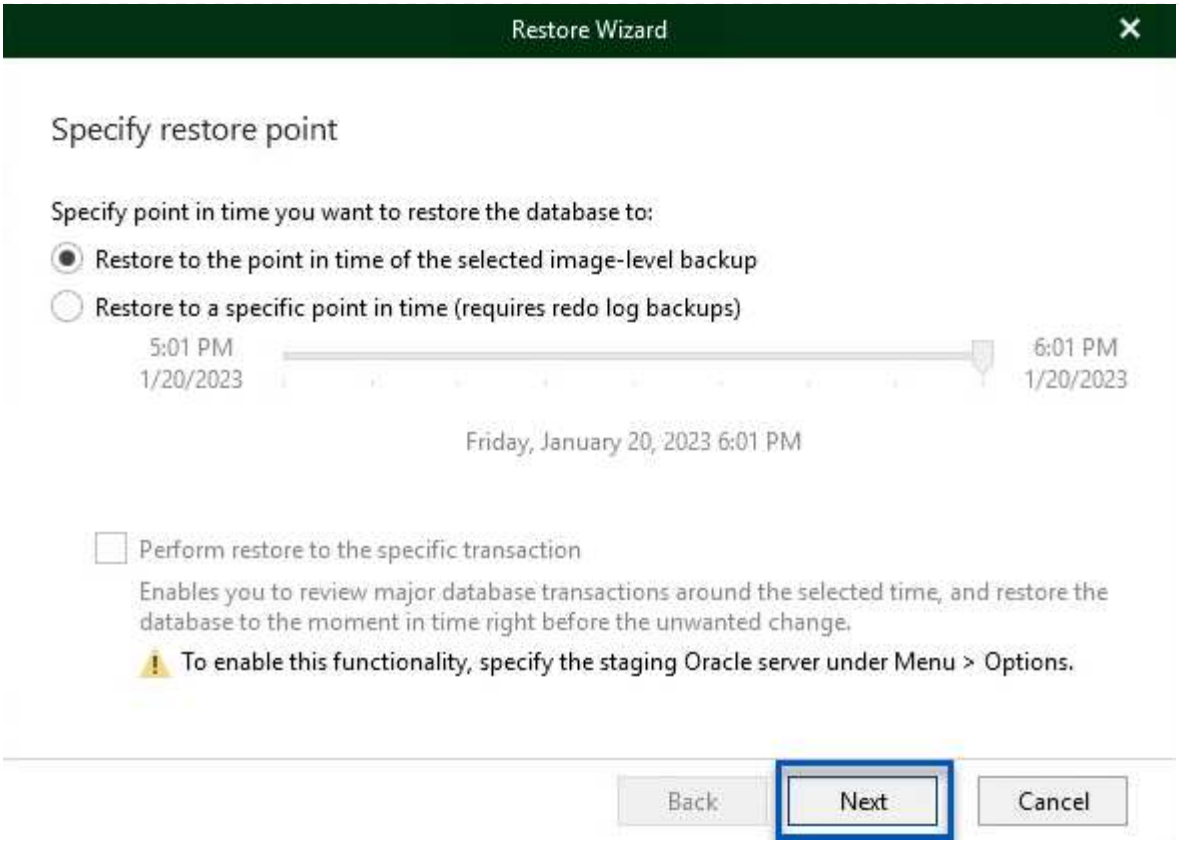
3. 如有需要、請輸入 * 還原原因 * 、然後在「摘要」頁面上按一下 * 瀏覽 * 按鈕、啟動 Veeam Explorer for Oracle 。



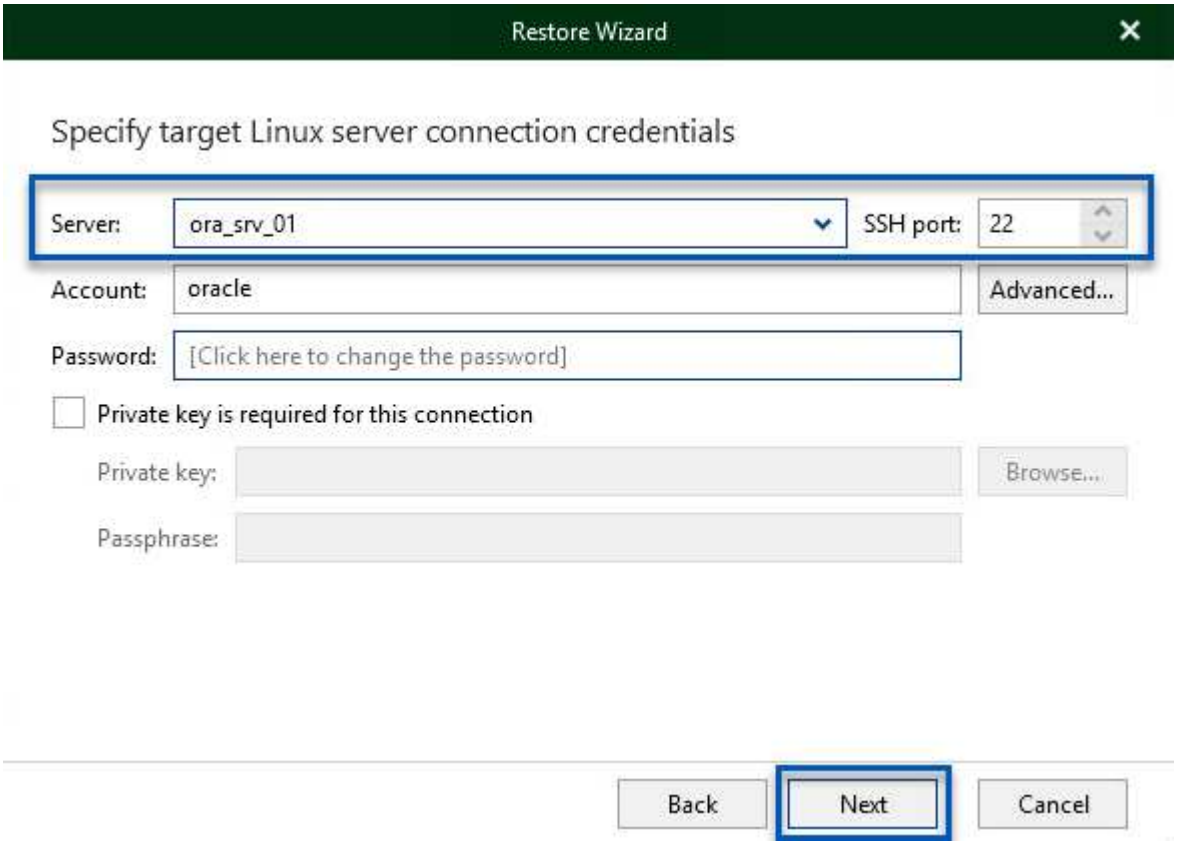
4. 在 Veeam Explorer 中展開資料庫執行個體清單、按一下要還原的資料庫、然後從頂端的 * 還原資料庫 * 下拉式功能表中選取 * 還原至其他伺服器 ...* 。



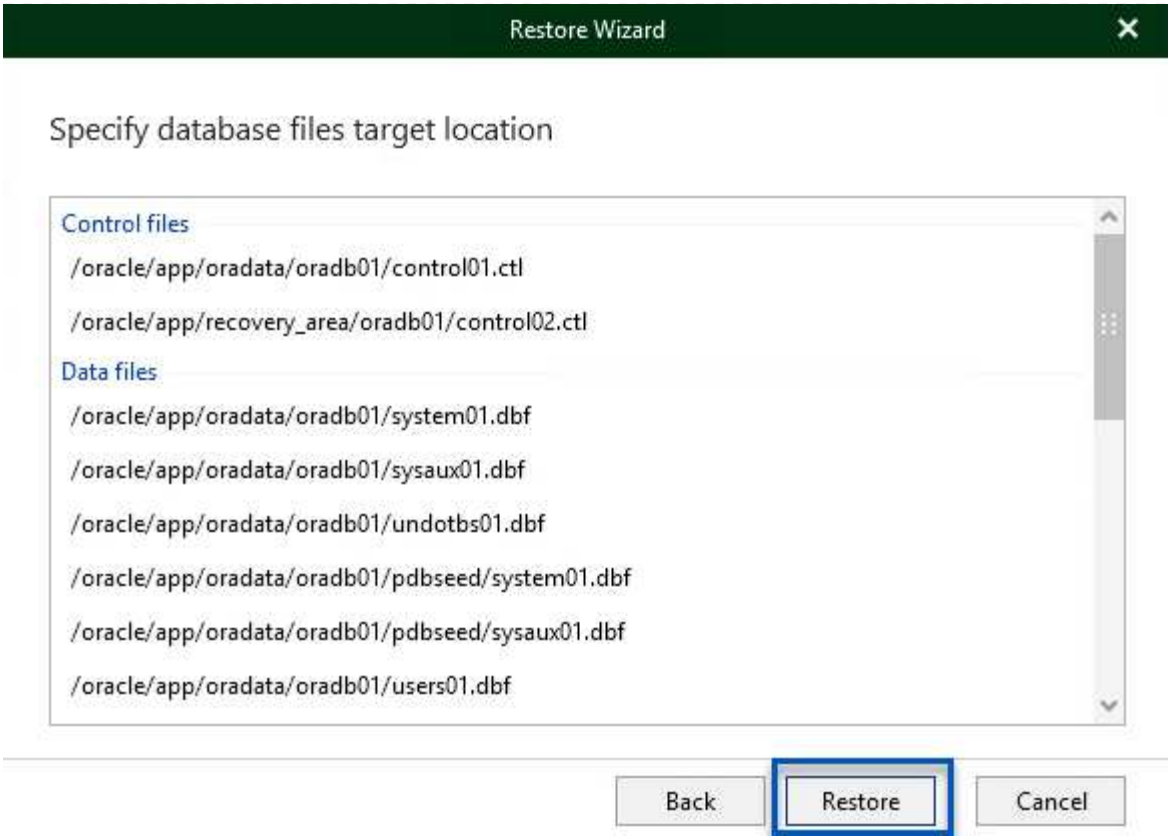
5. 在還原精靈中指定還原點、然後按一下 * 下一步 * 。



6. 指定要還原資料庫的目標伺服器和帳戶認證、然後按一下 * 下一步 * 。



7. 最後、指定資料庫檔案的目標位置、然後按一下 * 還原 * 按鈕開始還原程序。

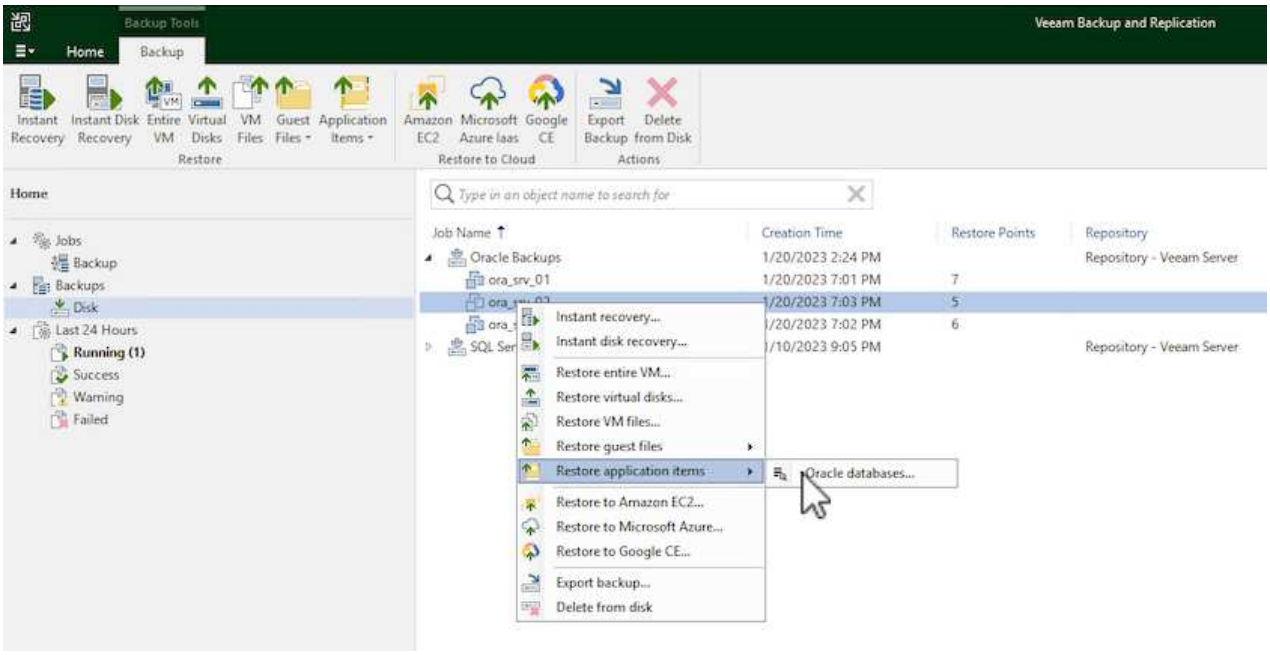


8. 資料庫恢復完成後、請檢查伺服器上的 Oracle 資料庫是否正確啟動。

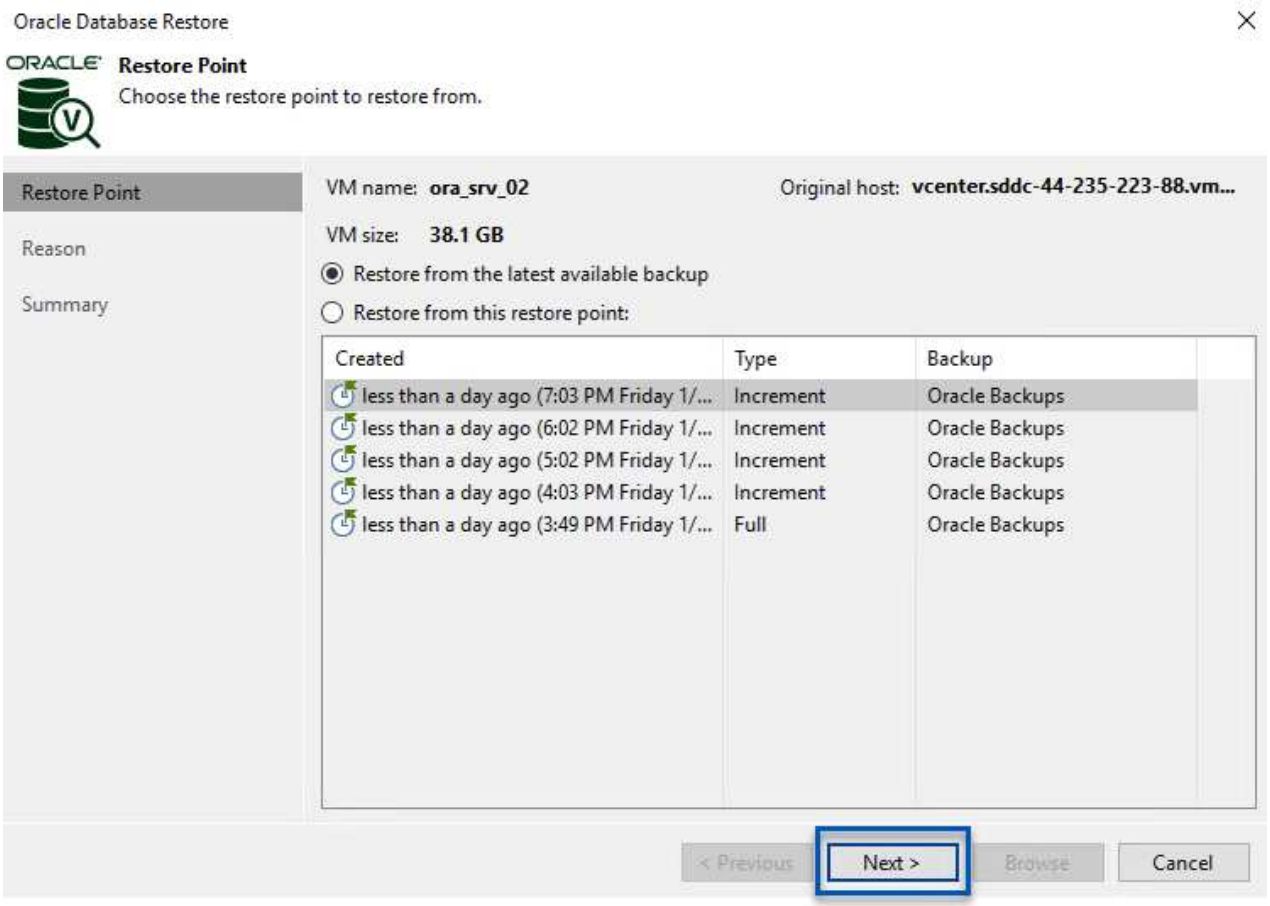
將 **Oracle** 資料庫發佈至替代伺服器

在本節中、資料庫會發佈到替代伺服器、以便在不啟動完整還原的情況下快速存取。

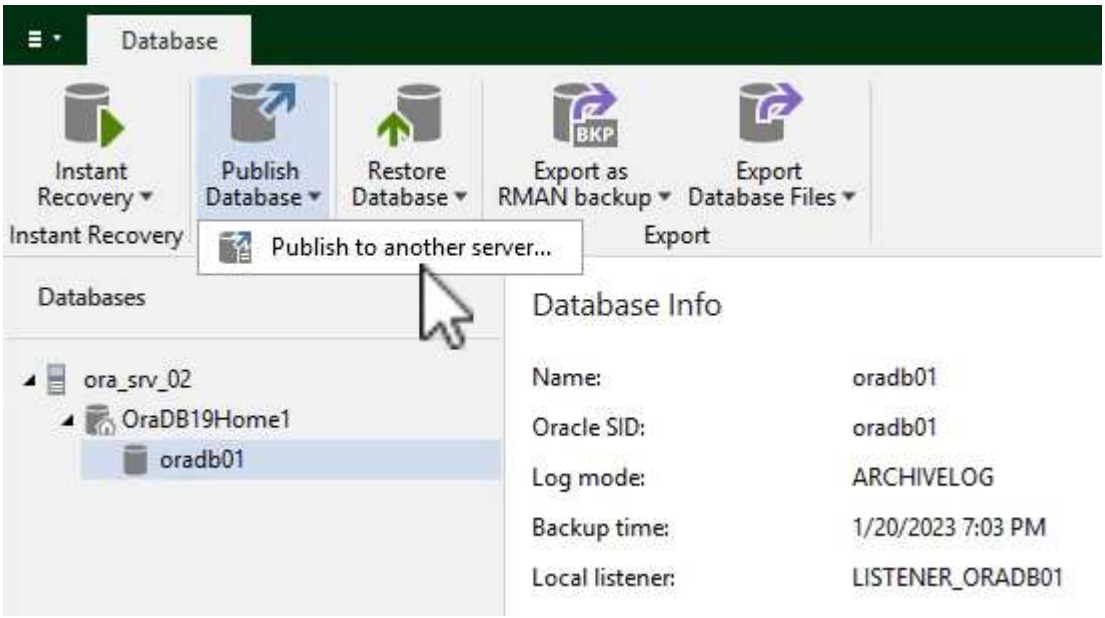
1. 在 Veeam 備份與複寫主控台中、瀏覽至 Oracle 備份清單、在伺服器上按一下滑鼠右鍵、然後選取 * 還原應用程式項目 * 、再選取 * Oracle 資料庫 … * 。



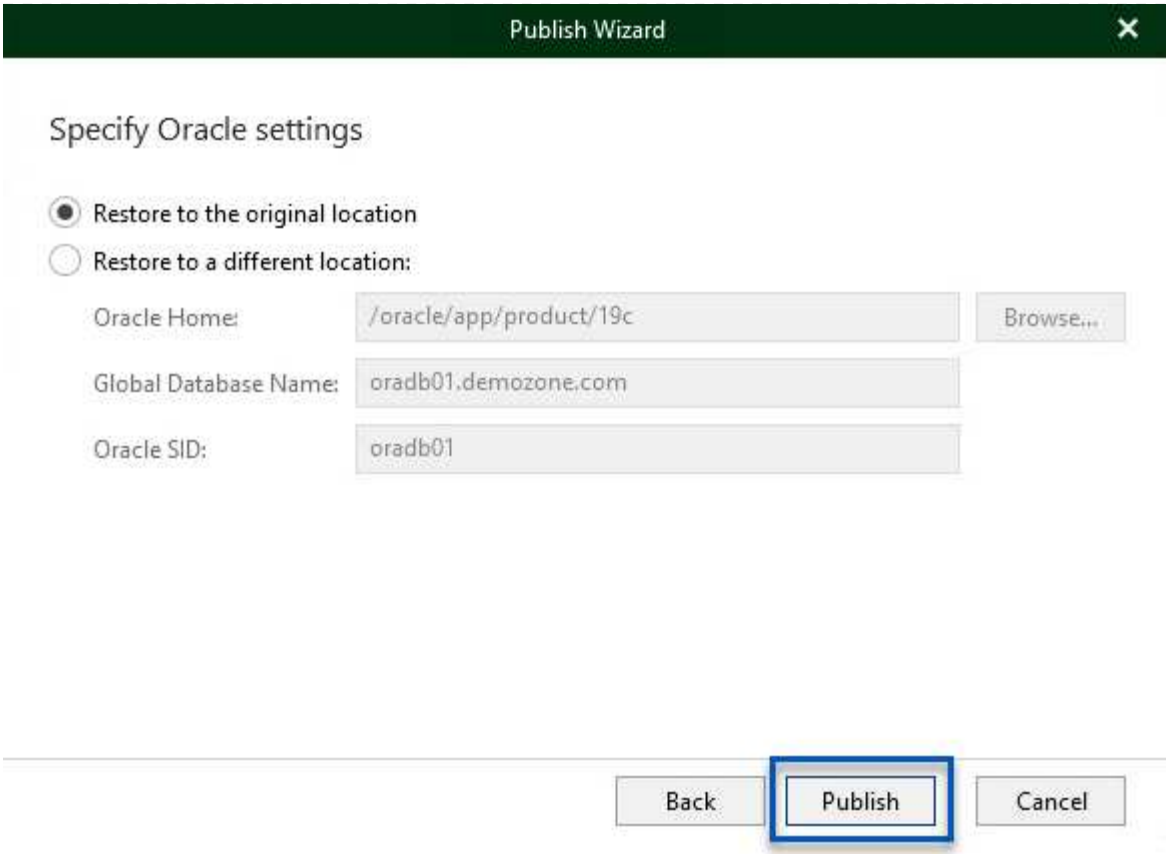
2. 在 Oracle 資料庫還原精靈中、從清單中選取還原點、然後按一下 * 下一步 * 。



3. 如有需要、請輸入 * 還原原因 * 、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 中展開資料庫執行個體清單、按一下要還原的資料庫、然後從頂端的 * 發佈資料庫 * 下拉式功能表中選取 * 發佈至其他伺服器 ...* 。



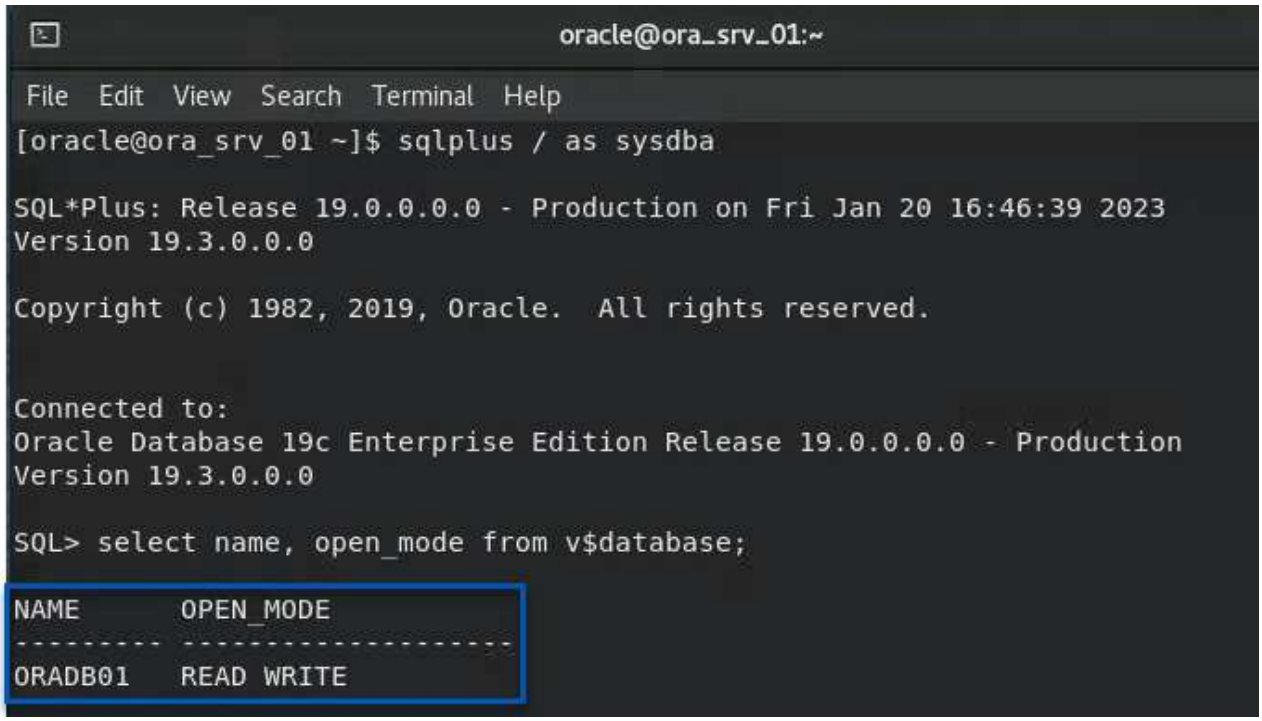
5. 在發佈精靈中、指定要發佈資料庫的還原點、然後按一下 * 下一步 * 。
6. 最後、指定目標 Linux 檔案系統位置、然後按一下 * Publish * 開始還原程序。



7. 當發佈完成後、請登入目標伺服器並執行下列命令、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 是執行業務關鍵應用程式及儲存敏感資料的強大平台。對於仰賴 VMware Cloud 的企業而言、安全的資料保護解決方案是不可或缺的、可確保業務持續運作、並協助防範網路威脅和資料遺失。選擇可靠且健全的資料保護解決方案、企業就能確信關鍵資料安全無虞、不受任何影響。

本文件中的使用案例著重於備受肯定的資料保護技術、強調 NetApp 、 VMware 和 Veeam 之間的整合。FSX for ONTAP 在 AWS 中支援做為 VMware Cloud 的補充 NFS 資料存放區、並用於所有虛擬機器和應用程式資料。Veeam 備份與複寫是一套全方位的資料保護解決方案、旨在協助企業改善、自動化及簡化備份與還原程序。Veeam 與 ONTAP 的 FSX 上託管的 iSCSI 備份目標磁碟區搭配使用、可為位於 VMware Cloud 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。

其他資訊

若要深入瞭解本解決方案所提供的技術、請參閱下列其他資訊。

- "適用於 ONTAP 的 FSX 使用者指南"
- "Veeam說明中心技術文件"
- "VMware Cloud on AWS 支援。考量與限制"

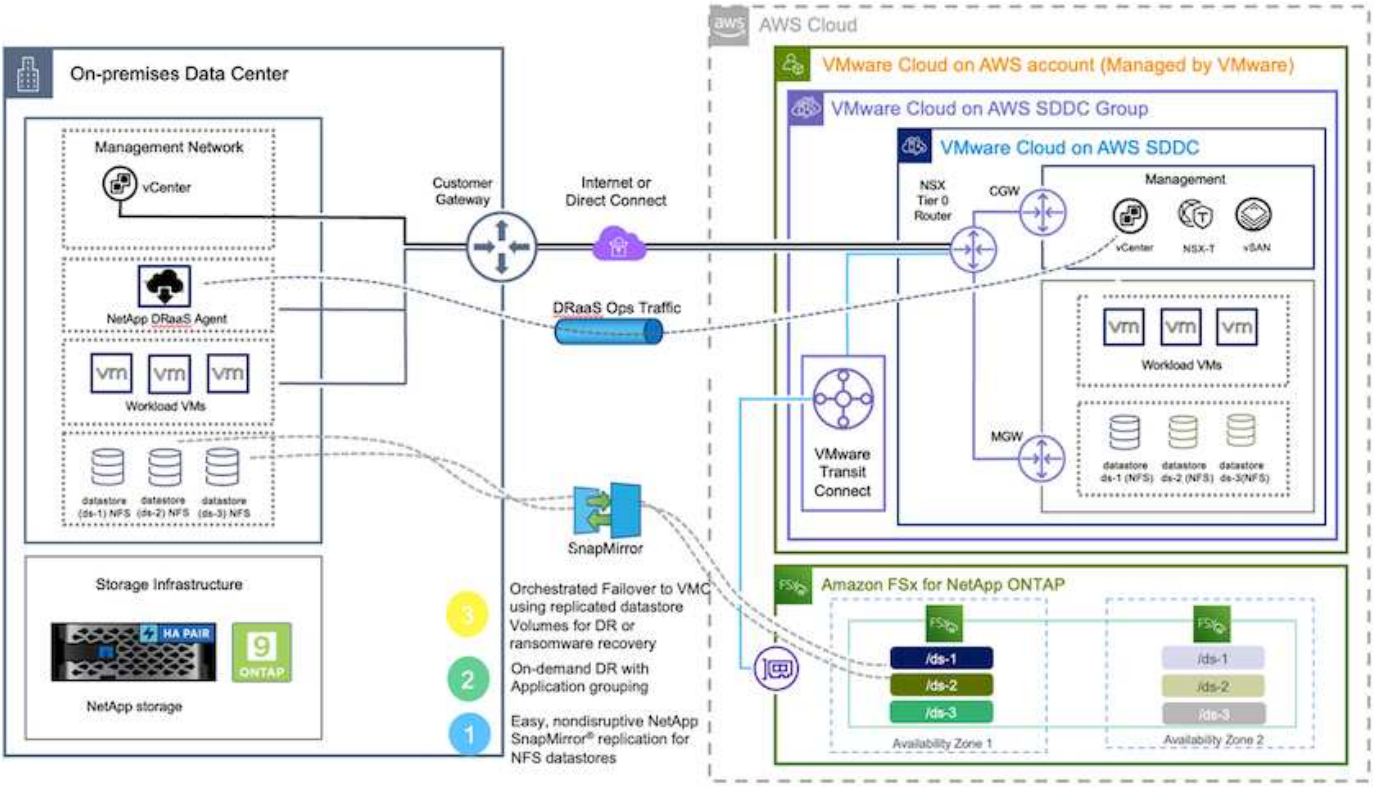
TR-4955：使用**FSX**進行災難恢復**ONTAP** 、以利實現**VMware vCenter**與**VMC**（**AWS VMware Cloud**）

NetApp公司Niyazz Mohamed

總覽

災難恢復至雲端是一種彈性且具成本效益的方法、可保護工作負載免受站台停機和資料毀損事件（例如勒索軟體）的影響。有了NetApp SnapMirror技術、內部部署的VMware工作負載可以複寫到FSX、ONTAP 以便在AWS中執行。

災難恢復協調程式（DRO；含UI的指令碼解決方案）可用來無縫恢復從內部部署複寫到FSX以ONTAP 供支援的工作負載。DRO透過VM登錄到VMC、將SnapMirror層級的還原作業自動化、並直接在NSS-T上進行網路對應所有VMC環境均隨附此功能。



快速入門

在**AWS**上部署及設定**VMware Cloud**

"AWS上的VMware Cloud" 為AWS生態系統中的VMware工作負載提供雲端原生體驗。每個VMware軟體定義資料中心（SDDC）都會在Amazon Virtual Private Cloud（VPC）上執行、並提供完整的VMware堆疊（包括vCenter Server）、NSX-T軟體定義網路、vSAN軟體定義儲存設備、以及一或多個ESXi主機、為工作負載提供運算與儲存資源。若要在AWS上設定VMC環境、請執行下列步驟 "連結"。也可將一個指示燈式叢集用於DR用途。

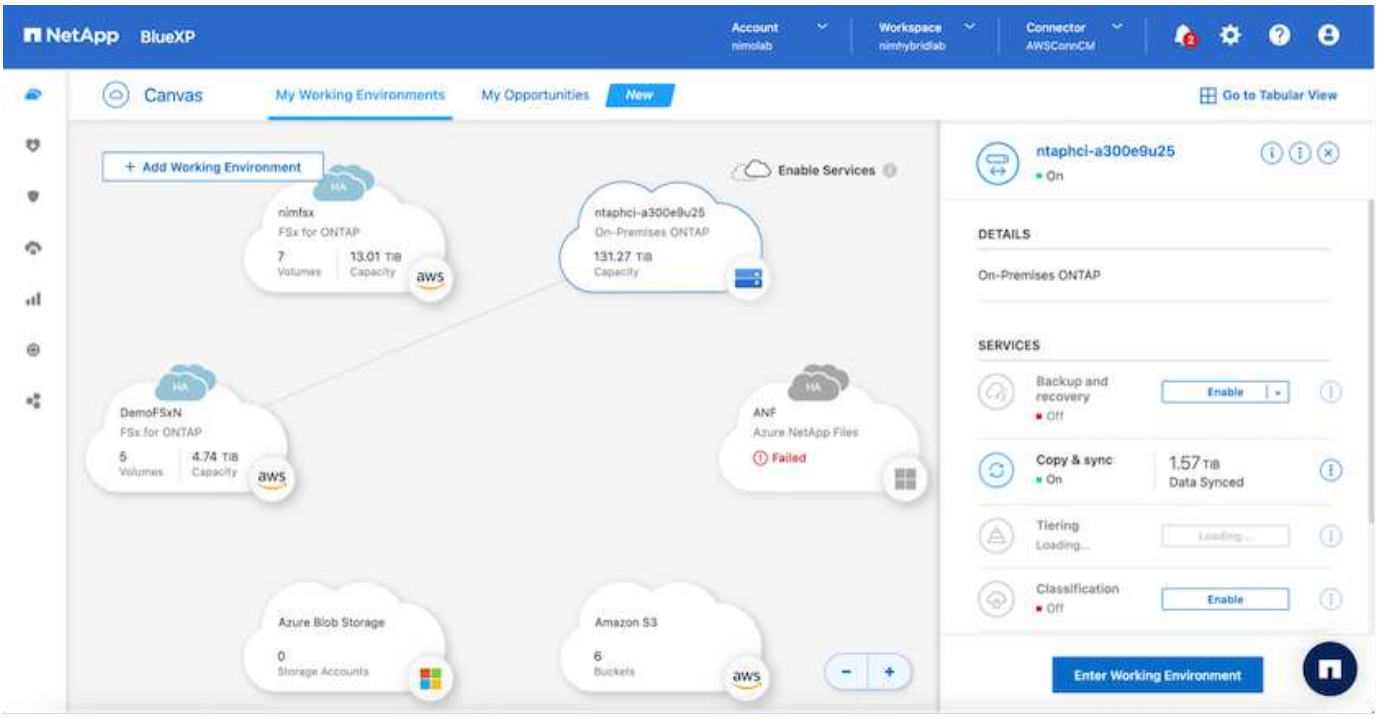
在初始版本中、DRO支援現有的指示燈叢集。隨需建立SDDC將於即將推出的版本中提供。

配置和設定**FSXfor ONTAP Sf**

Amazon FSX for NetApp ONTAP Sfing是一項全託管服務、以熱門的NetApp ONTAP Sfor NetApp文件系統為基礎、提供高度可靠、可擴充、高效能且功能豐富的檔案儲存設備。請依照下列步驟操作 "連結" 配置和設定FSXfor ONTAP Sf。

部署**SnapMirror**並將其設定為**FSXfor ONTAP Sfor Sfor**

下一步是使用NetApp BlueXP、探索AWS ONTAP 執行個體上已配置的FSX、並以ONTAP 適當的頻率將所需的資料存放區磁碟區從內部部署環境複寫到FSX以供使用、並保留NetApp Snapshot複本：



請遵循此連結中的步驟來設定BlueXP。您也可以使用NetApp ONTAP 的CLI來排程此連結的複寫作業。

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、以確保符合先決條件。然後安裝套件。

先決條件

- 請確定已連線至來源和目的地vCenter及儲存系統。
- 如果您使用DNS名稱、則應該已有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執行個體搭配使用。

作業系統需求

- Ubuntu 20.04（LTS）、至少2 GB和4個vCPU
- 下列套件必須安裝在指定的代理VM上：
  - Docker
  - Docker編寫
  - Jq

變更權限 `docker.sock`： `sudo chmod 666 /var/run/docker.sock`。

- `deploy.sh` 指令碼會執行所有必要的先決條件。

安裝套件

1. 在指定的虛擬機器上下載安裝套件：

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

代理程式可安裝在內部部署或AWS VPC內。

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

```
tar xvf DRO-prereq.tar
```

3. 瀏覽至目錄並執行部署指令碼、如下所示：

```
sudo sh deploy.sh
```

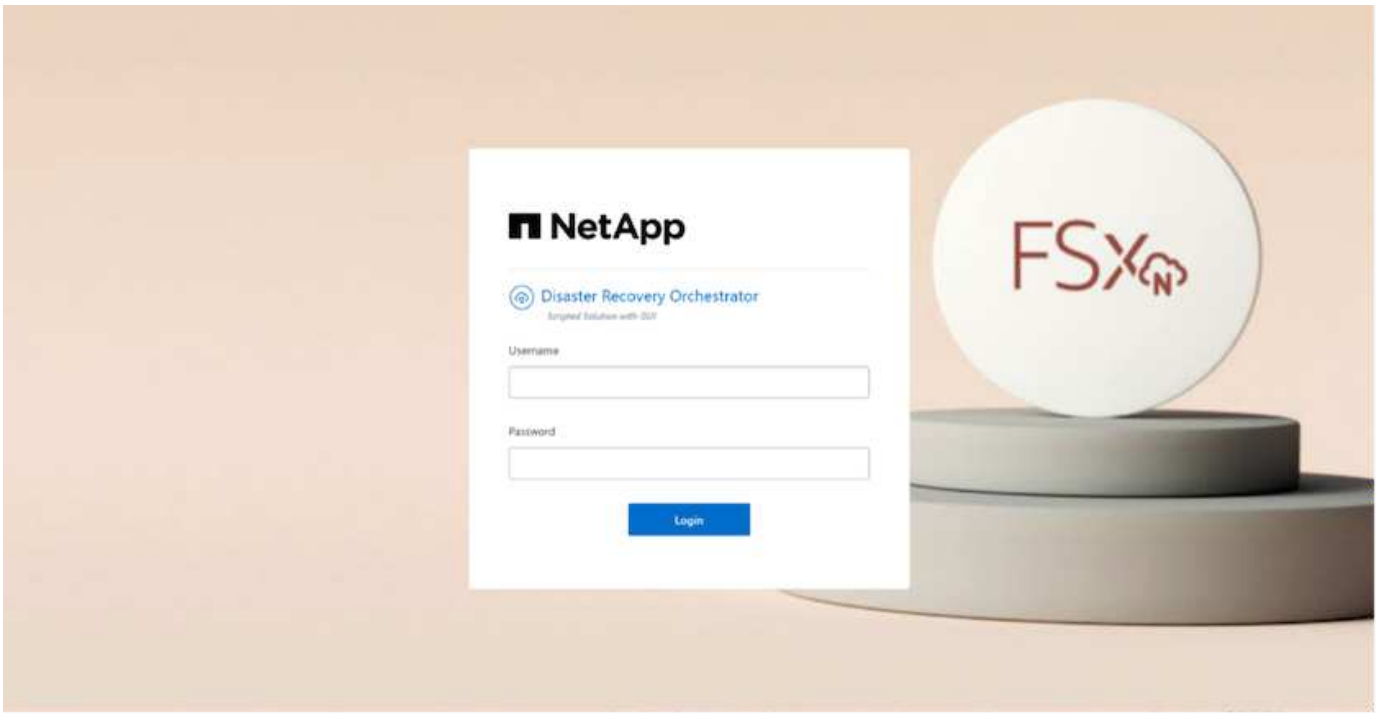
4. 使用下列項目存取UI：

```
https://<host-ip-address>
```

使用下列預設認證：

```
Username: admin
Password: admin
```

您可以使用「變更密碼」選項來變更密碼。



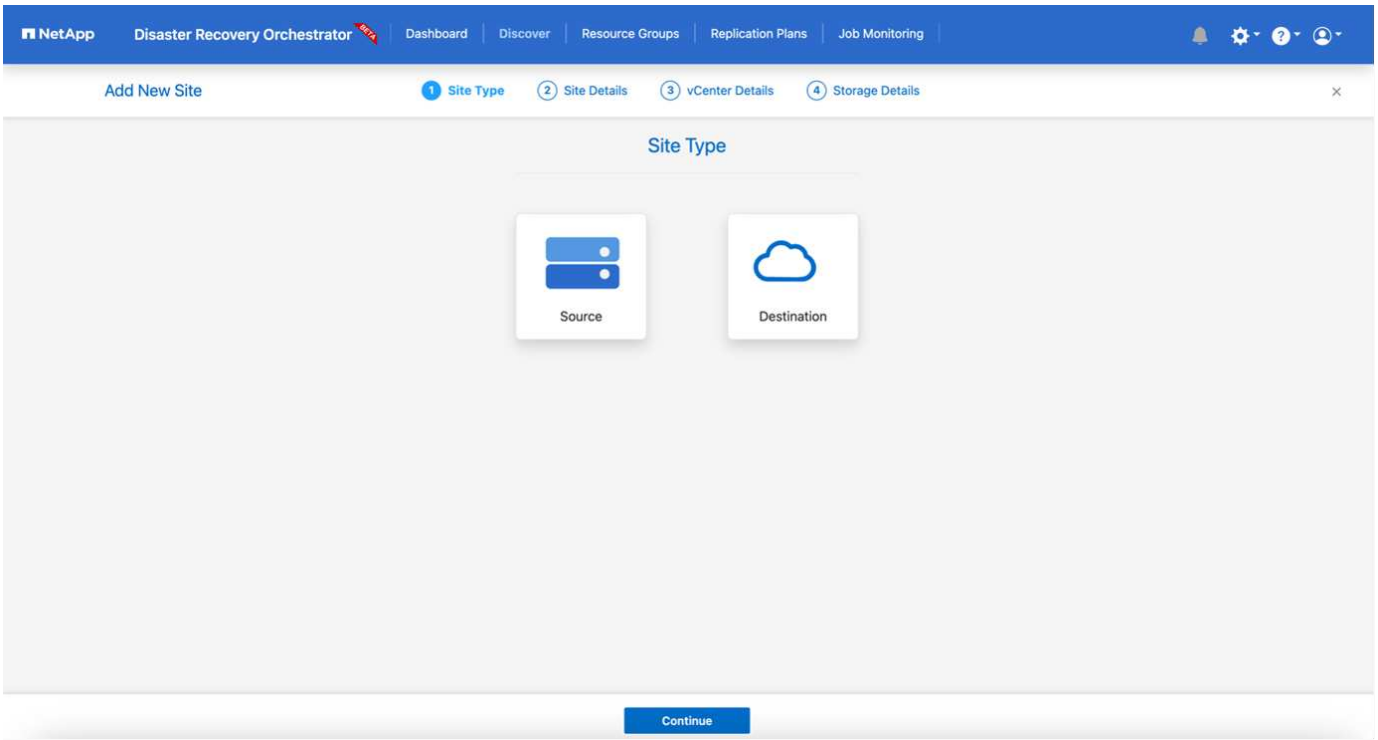
DRO組態

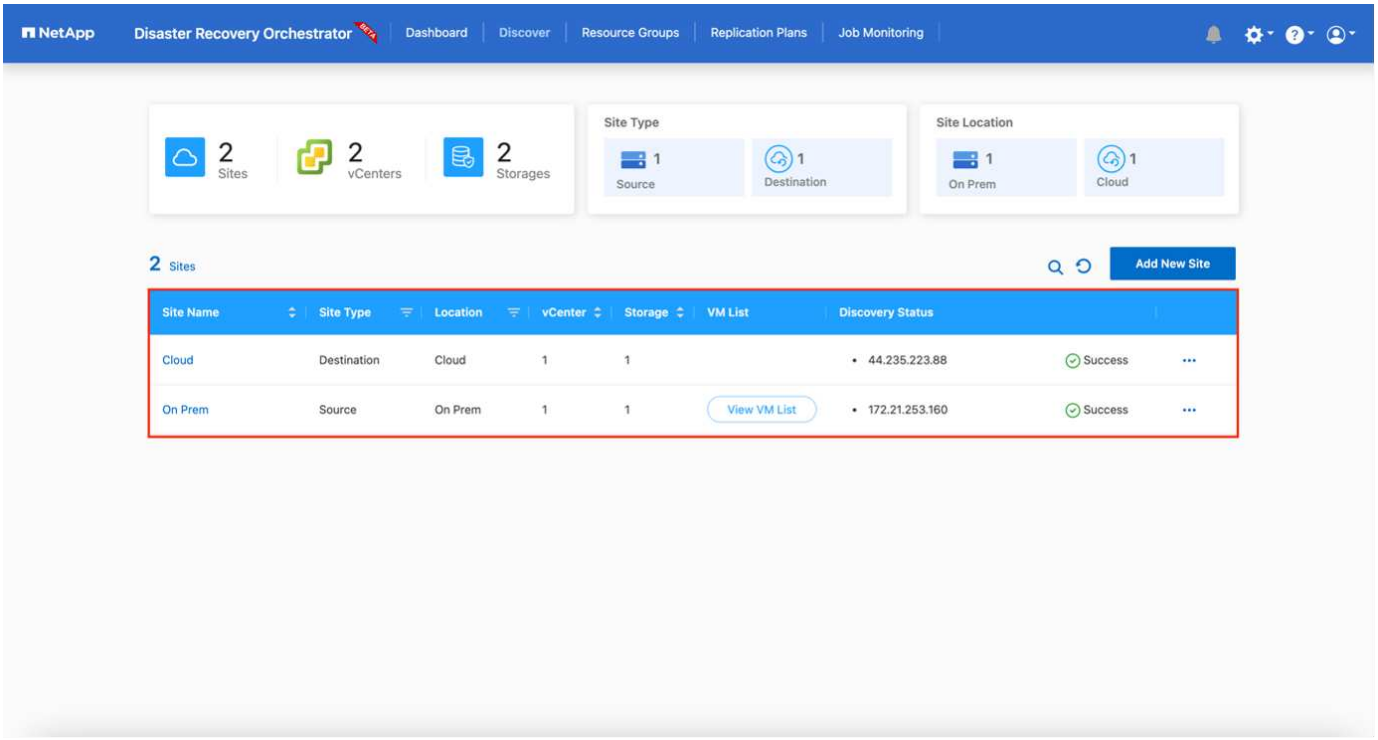
FSXfor ONTAP VMware和VMC設定正確之後、您可以開始設定DRO、使用FSXfor ONTAP Sfor VMware上的唯讀SnapMirror複本、將內部部署工作負載自動還原至VMC。

NetApp建議將DRO代理程式部署在AWS中、也部署到ONTAP 部署FSX for Sf2的相同VPC（也可連接對等端點）、因此DRO代理程式可以透過網路與內部部署元件、以及使用FSXfor ONTAP VMware和VMC資源進行通訊。

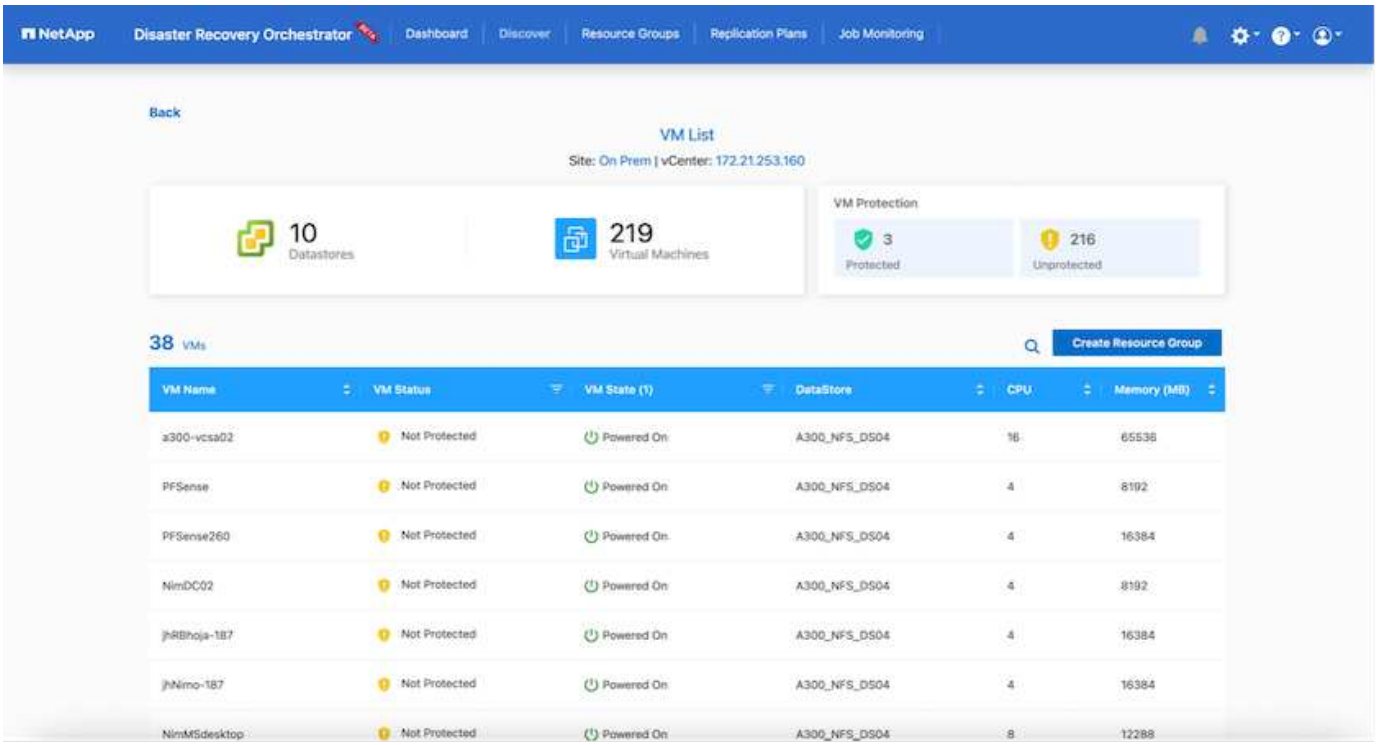
第一步是探索內部部署和雲端資源（vCenter和儲存設備）、並將其新增至DRO。在支援的瀏覽器中開啟DRO、然後使用預設的使用者名稱和密碼（admin/admin）和新增站台。您也可以使用「探索」選項來新增站台。新增下列平台：

- 內部部署
  - 內部部署vCenter
  - 儲存系統ONTAP
- 雲端
  - VMC vCenter
  - FSX ONTAP





新增後、DRO會執行自動探索、並顯示從來源儲存設備到FSX ONTAP for Sf0具有對應SnapMirror複本的VM。DRO會自動偵測VM所使用的網路和連接埠群組、並填入這些群組。



下一步是將所需的虛擬機器分成功能群組、做為資源群組。

資源群組

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

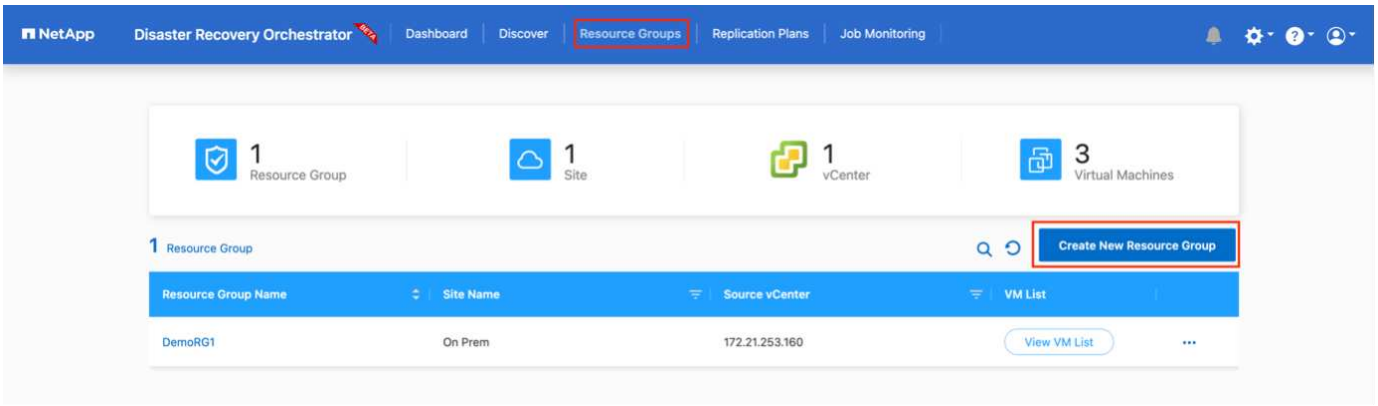
若要開始建立資源群組、請完成下列步驟：

1. 存取*資源群組*、然後按一下*建立新的資源群組*。
2. 在「新資源群組」下、從下拉式清單中選取來源網站、然後按一下「建立」。
3. 提供*資源群組詳細資料*、然後按一下*繼續*。
4. 使用搜尋選項選取適當的VM。
5. 選取所選VM的開機順序和開機延遲（秒）。選取每個VM並設定其優先順序、以設定開機順序。三個是所有VM的預設值。

   選項如下：

   1–第一台開機的虛擬機器3–預設5–最後一台開機的虛擬機器

6. 按一下「建立資源群組」。

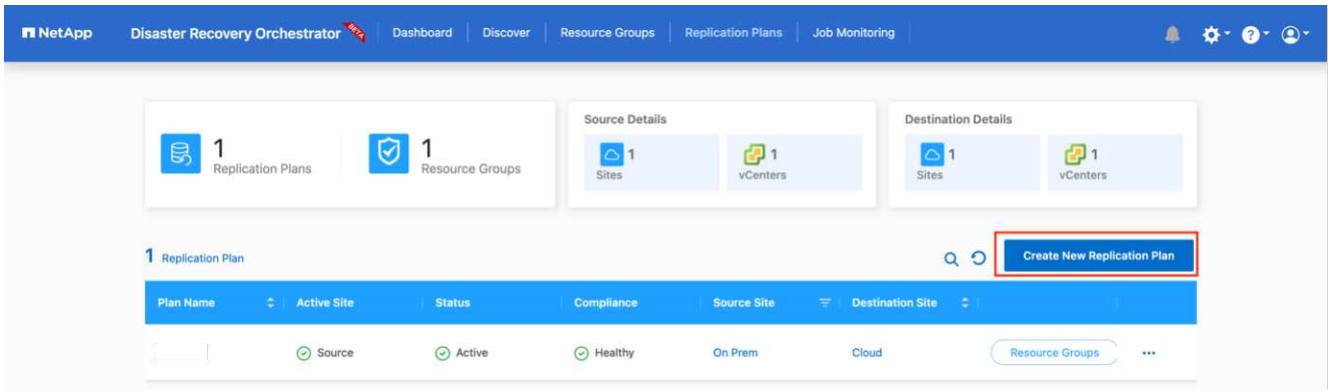


複寫計畫

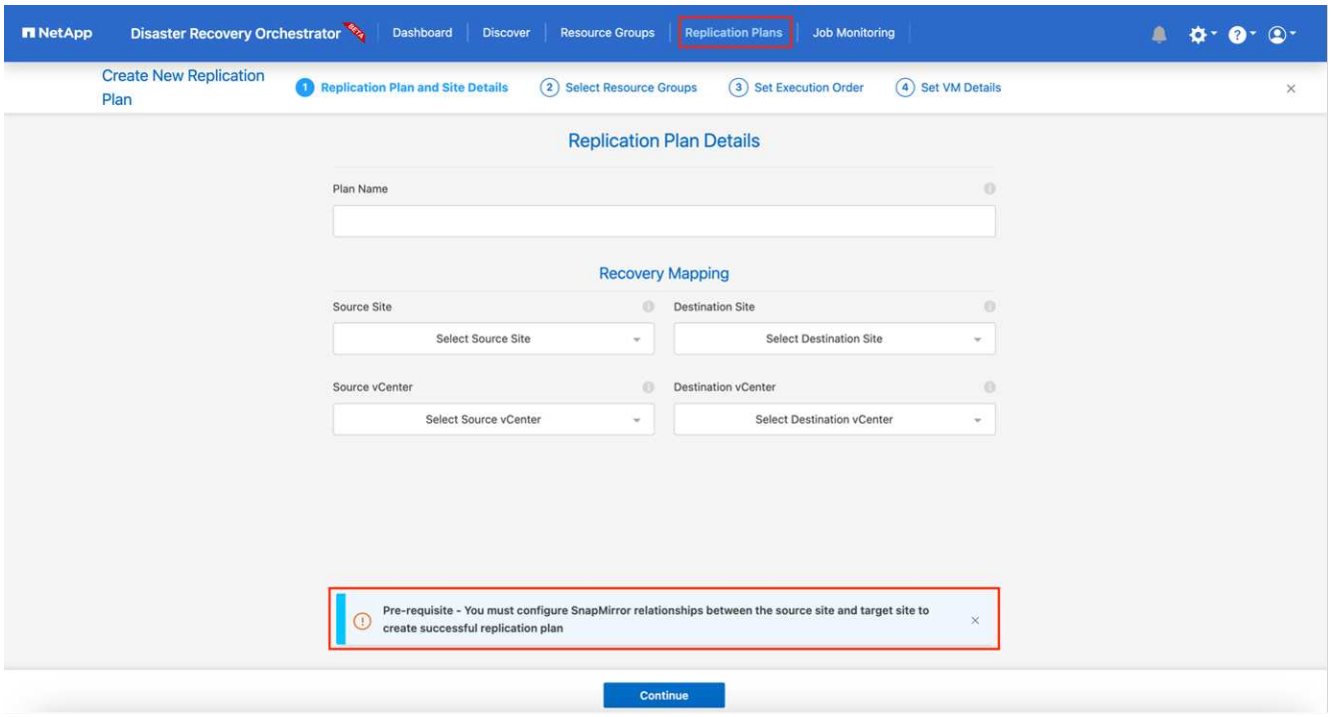
在發生災難時、您需要一套恢復應用程式的計畫。從下拉式清單中選取來源和目的地vCenter平台、然後選取要納入此計畫的資源群組、以及應用程式應如何還原和開啟的分組（例如、網域控制器、層級1、層級2等）。這類計畫有時也稱為藍圖。若要定義恢復計畫、請瀏覽至*複寫計畫*索引標籤、然後按一下*新增複寫計畫*。

若要開始建立複寫計畫、請完成下列步驟：

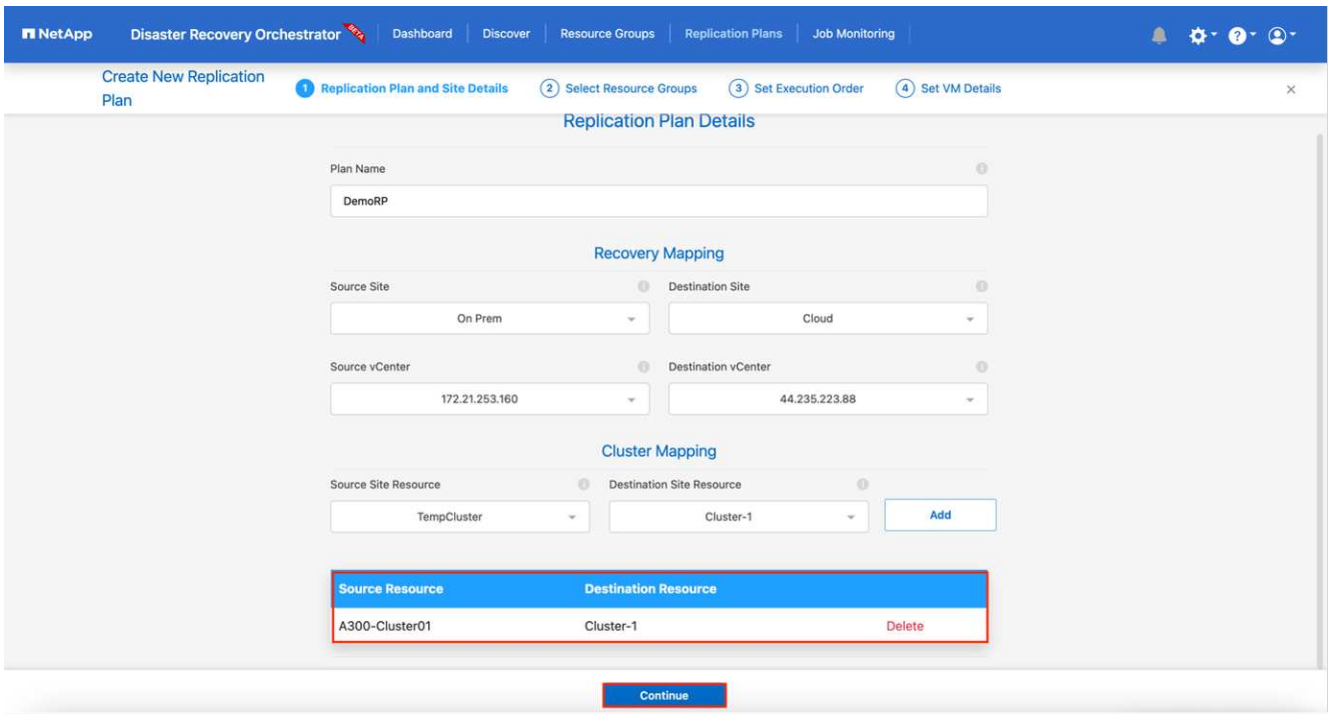
1. 存取*複寫計畫*、然後按一下*建立新的複寫計畫*。



2. 在「新的複寫計畫」下、提供計畫名稱、並選取來源站台、相關聯的vCenter、目的地站台及相關的vCenter來新增還原對應。

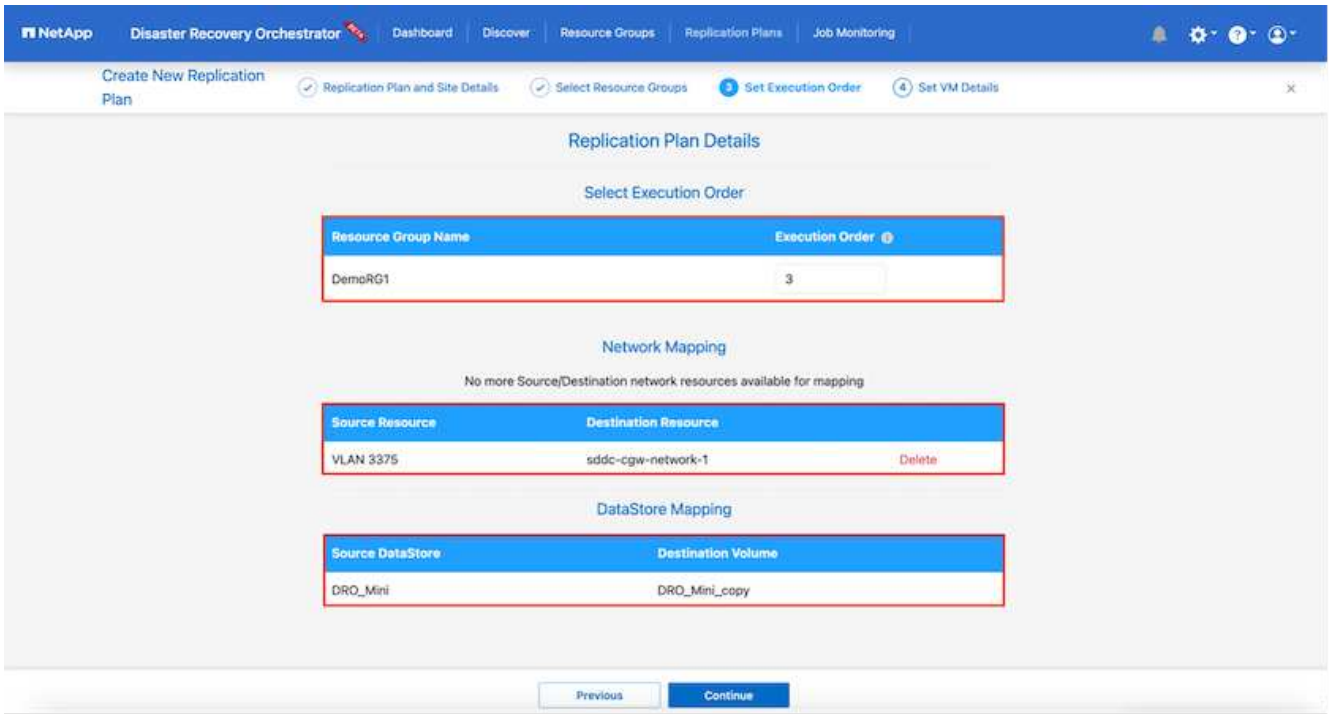


3. 完成恢復對應後、選取叢集對應。

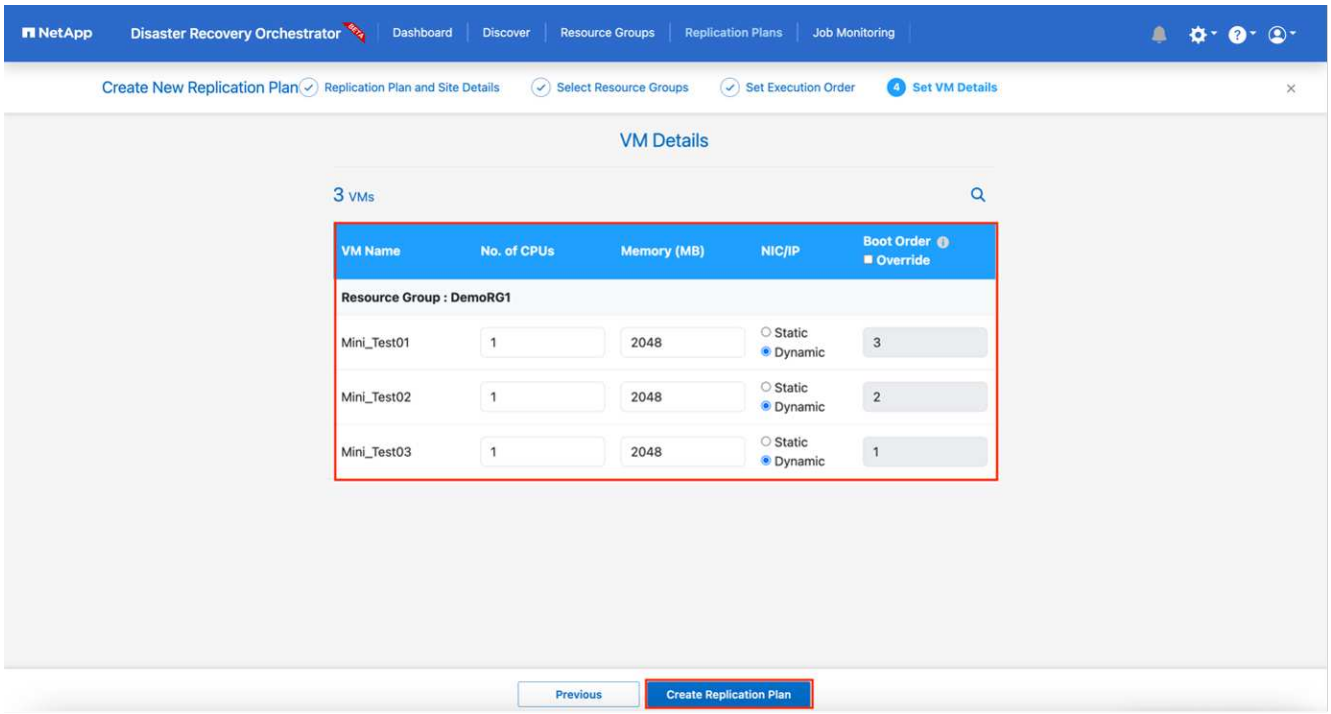


4. 選擇*資源群組詳細資料*、然後按一下*繼續*。
5. 設定資源群組的執行順序。此選項可讓您在存在多個資源群組時、選取作業順序。
6. 完成後、選取網路對應至適當的區段。區段應已在VMC中進行資源配置、因此請選取適當的區段來對應VM。
7. 根據VM的選擇、會自動選取資料存放區對應。

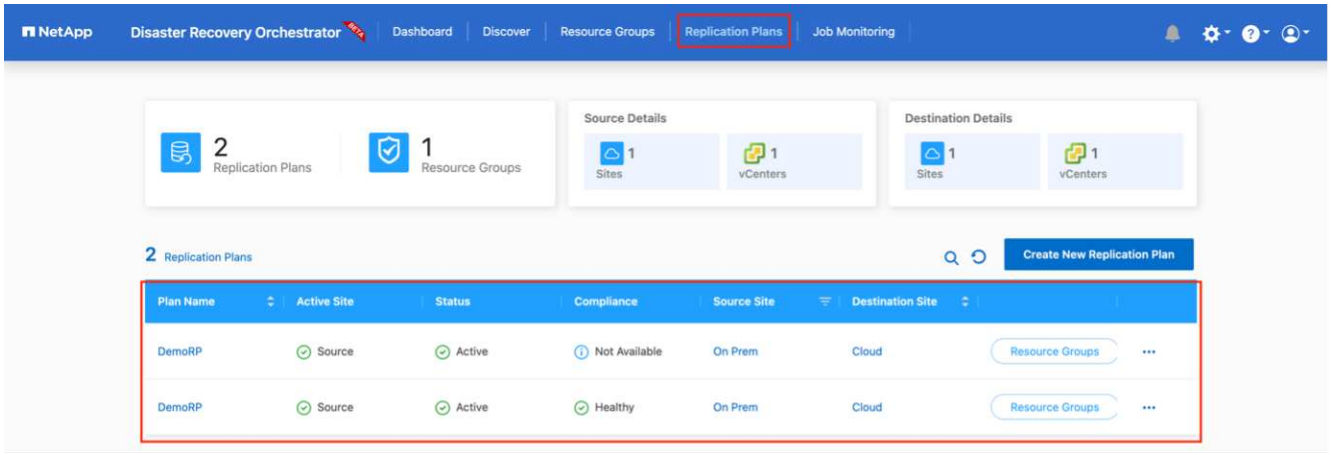
SnapMirror位於磁碟區層級。因此、所有VM都會複寫到複寫目的地。請務必選取屬於資料存放區一部分的所有VM。如果未選取、則只會處理屬於複寫計畫一部分的VM。



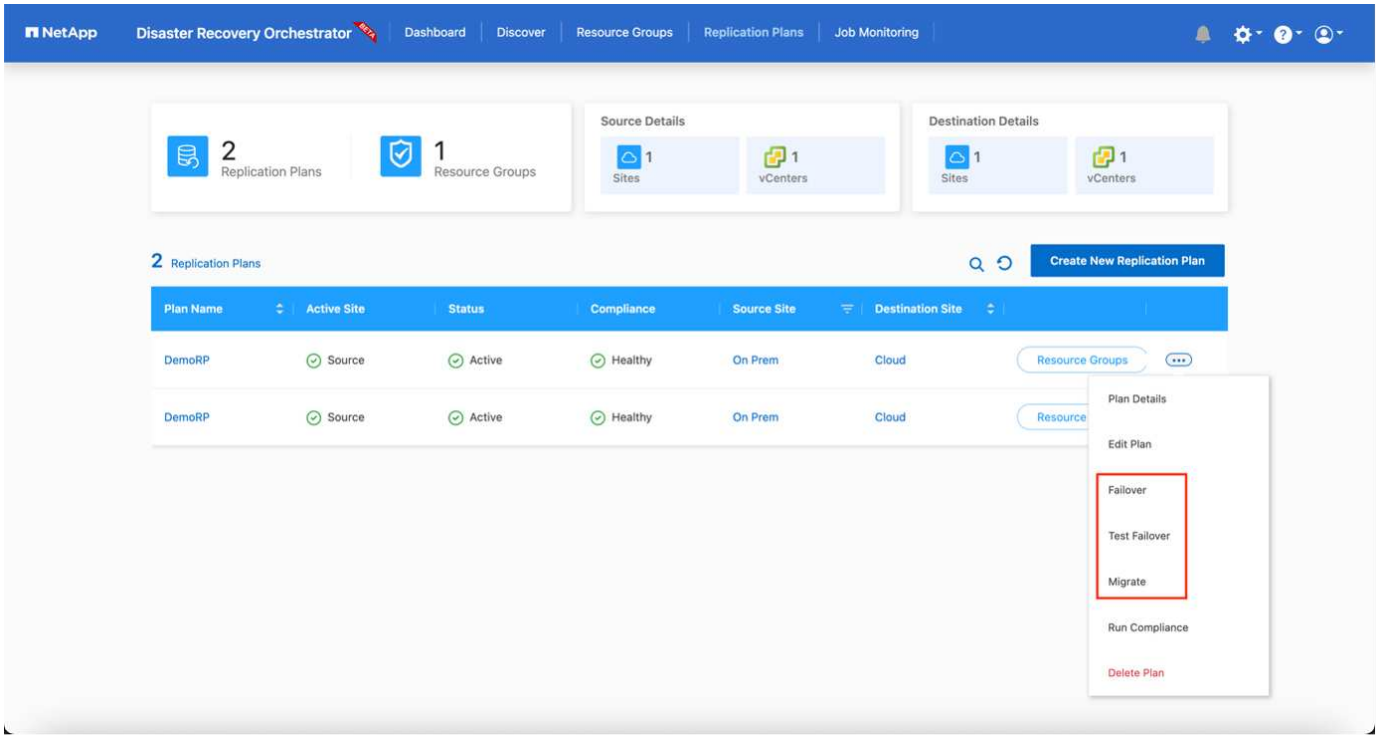
8. 在VM詳細資料下、您可以選擇調整VM的CPU和RAM參數大小、這對於將大型環境還原至較小的目標叢集或執行DR測試而不需配置一對一的實體VMware基礎架構而言、非常有幫助。此外、您也可以針對資源群組中所有選取的VM、修改開機順序和開機延遲（秒）。如果在資源群組開機順序選擇期間所選取的項目有任何變更、則還有其他選項可修改開機順序。依預設、系統會使用在資源群組選取期間選取的開機順序；不過、在此階段可以執行任何修改。

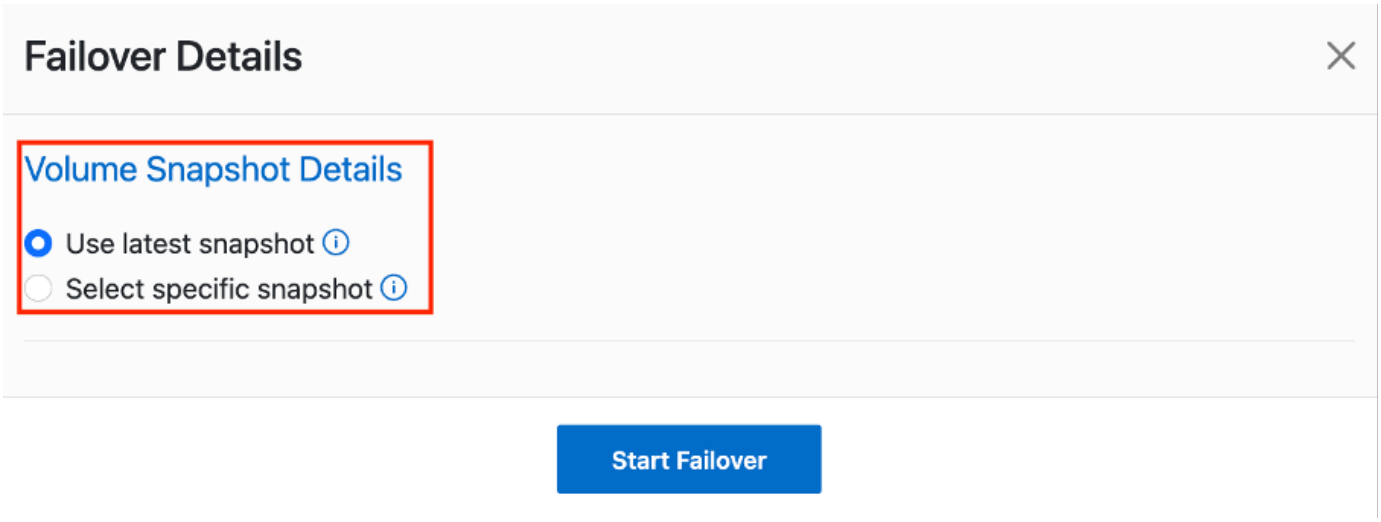


9. 按一下「建立複寫計畫」。

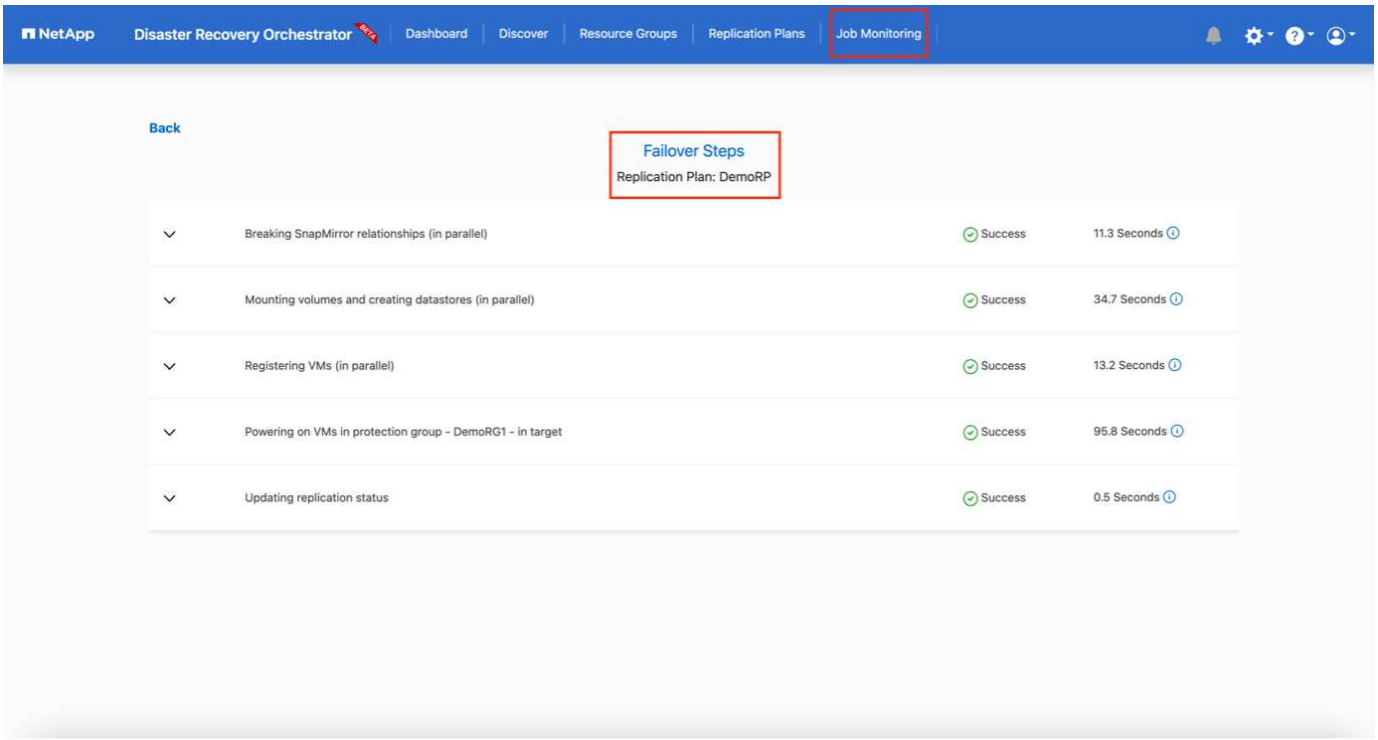


建立複寫計畫之後、即可根據需求來執行容錯移轉選項、測試容錯移轉選項或移轉選項。在容錯移轉和測試容錯移轉選項期間、會使用最新的SnapMirror Snapshot複本、或從時間點Snapshot複本（根據SnapMirror的保留原則）選取特定的Snapshot複本。如果您面臨勒索軟體之類的毀損事件、最近的複本已遭入侵或加密、則時間點選項可能非常實用。DRO會顯示所有可用的時間點。若要以複寫計畫中指定的組態觸發容錯移轉或測試容錯移轉、您可以按一下*容錯移轉*或*測試容錯移轉*。

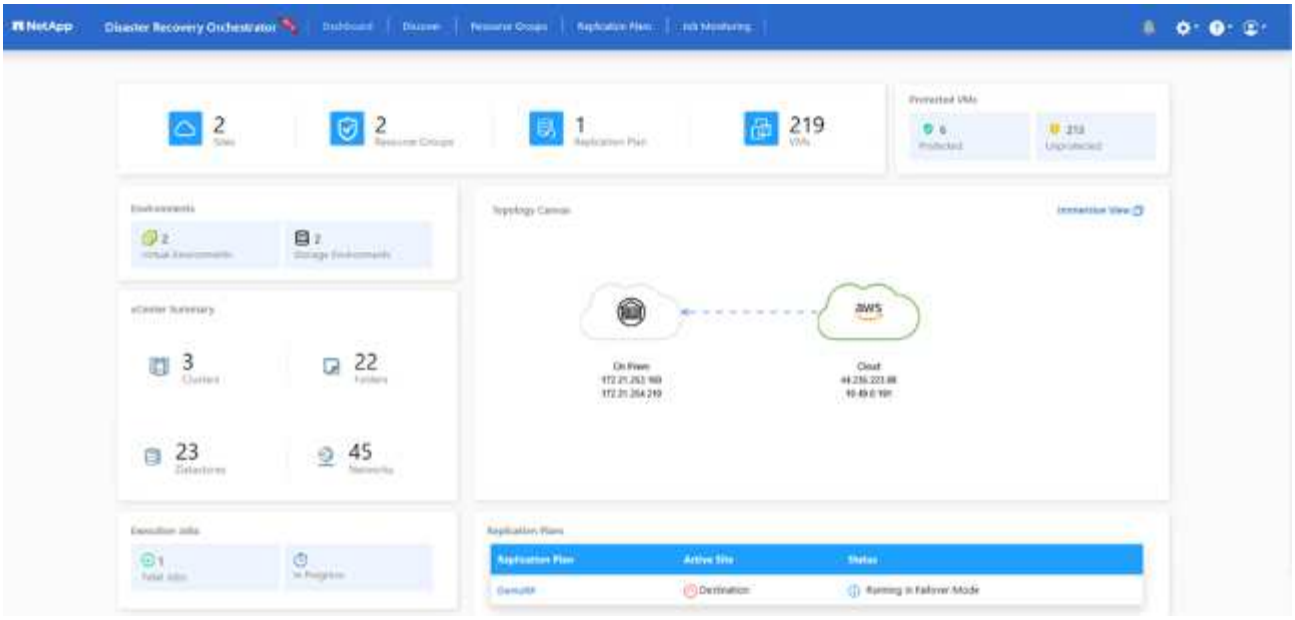




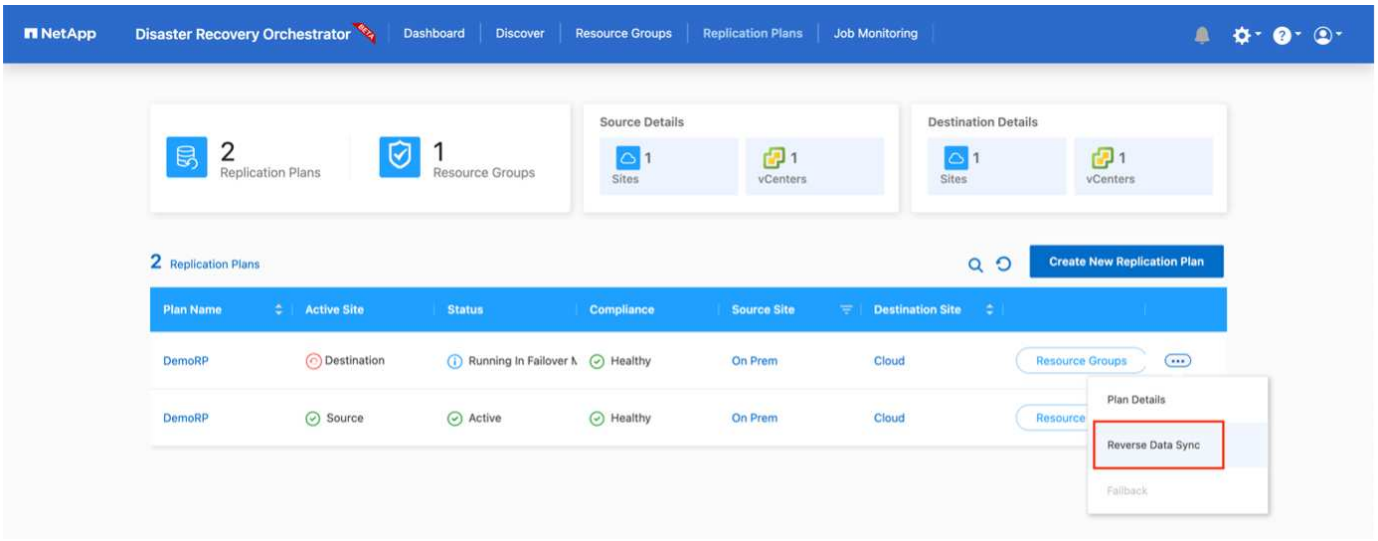
複寫計畫可在工作功能表中監控：

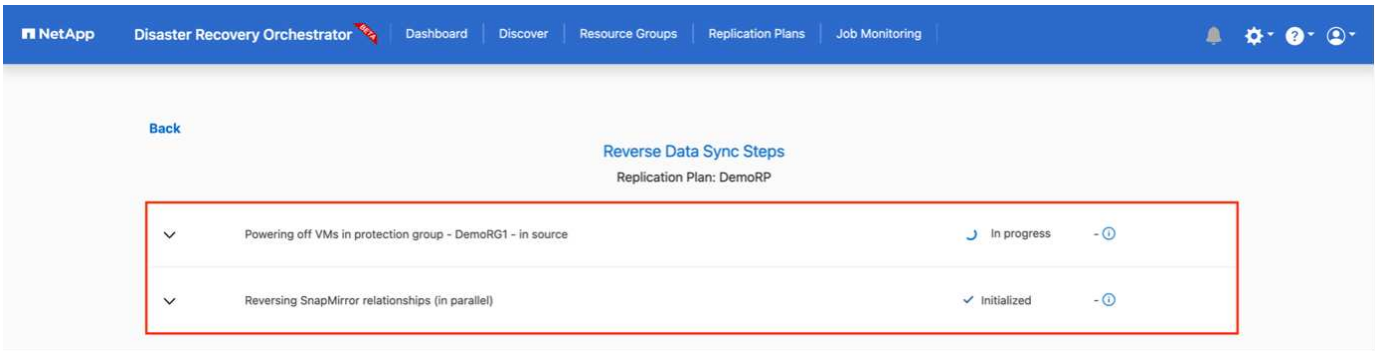


在觸發容錯移轉之後、可在VMC vCenter（VM、網路、資料存放區）中看到還原的項目。根據預設、虛擬機器會還原至工作負載資料夾。

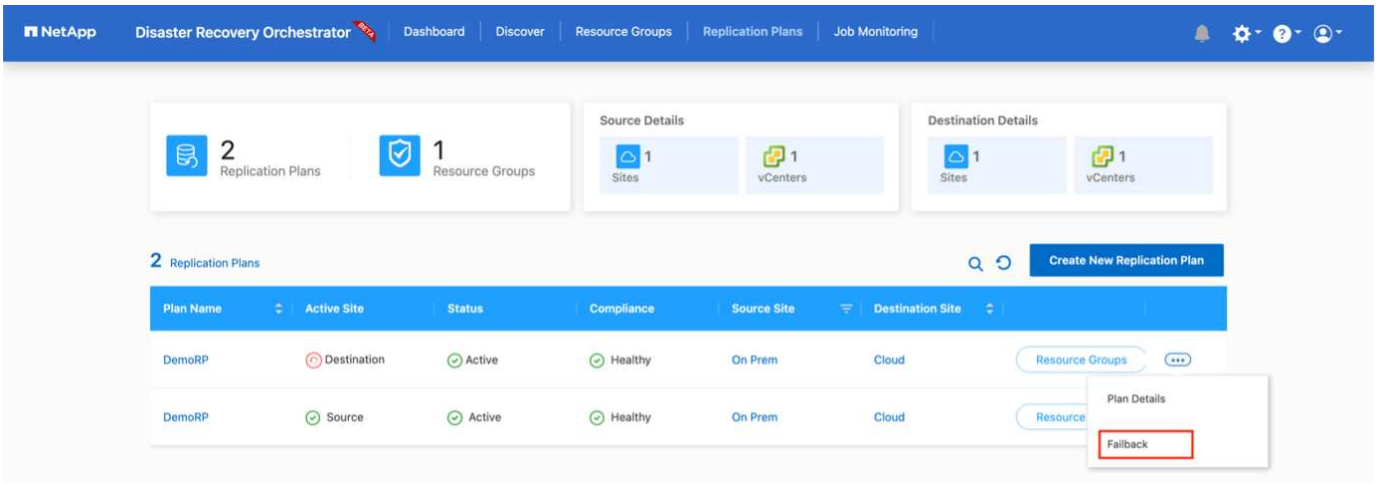


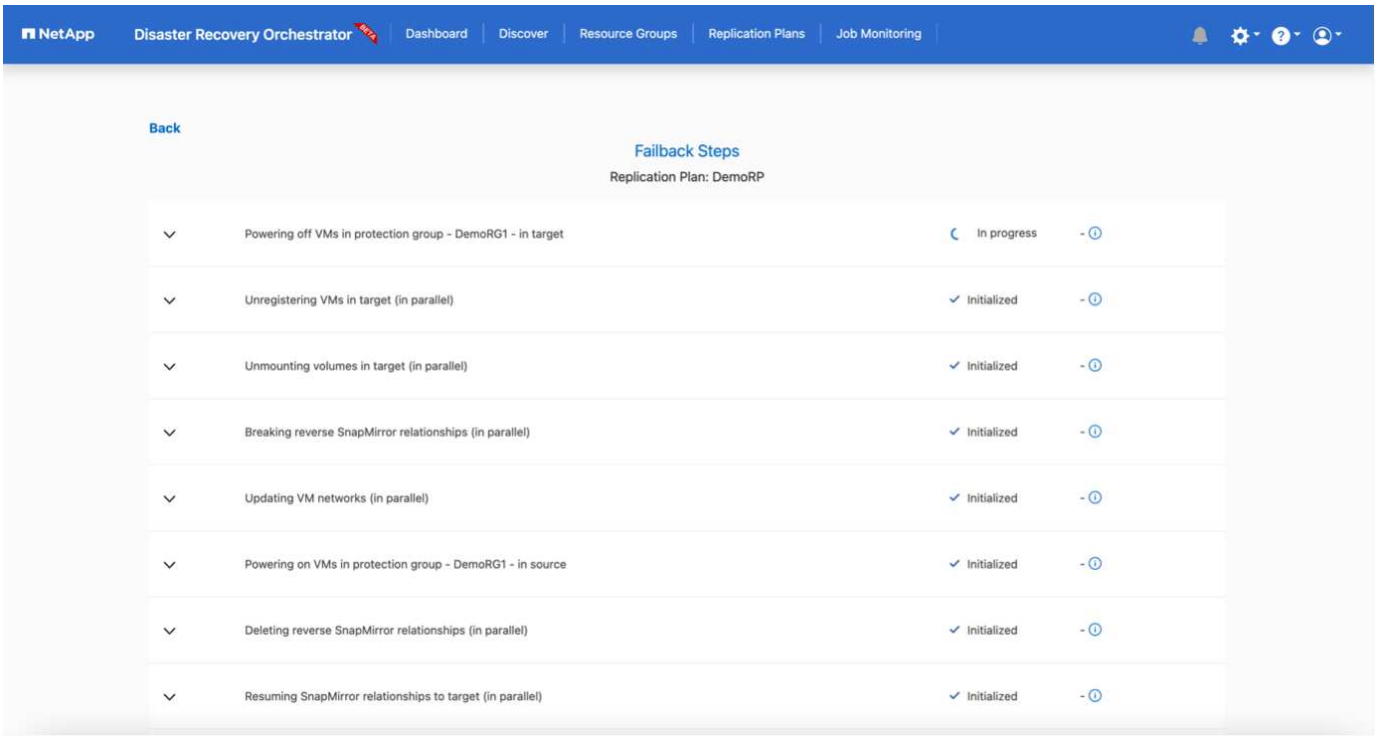
容錯回復可在複寫計畫層級觸發。對於測試容錯移轉、可利用「切換」選項來復原變更、並移除FlexClone關係。與容錯移轉相關的容錯回復是兩個步驟的程序。選取複寫計畫、然後選取*反轉資料同步*。



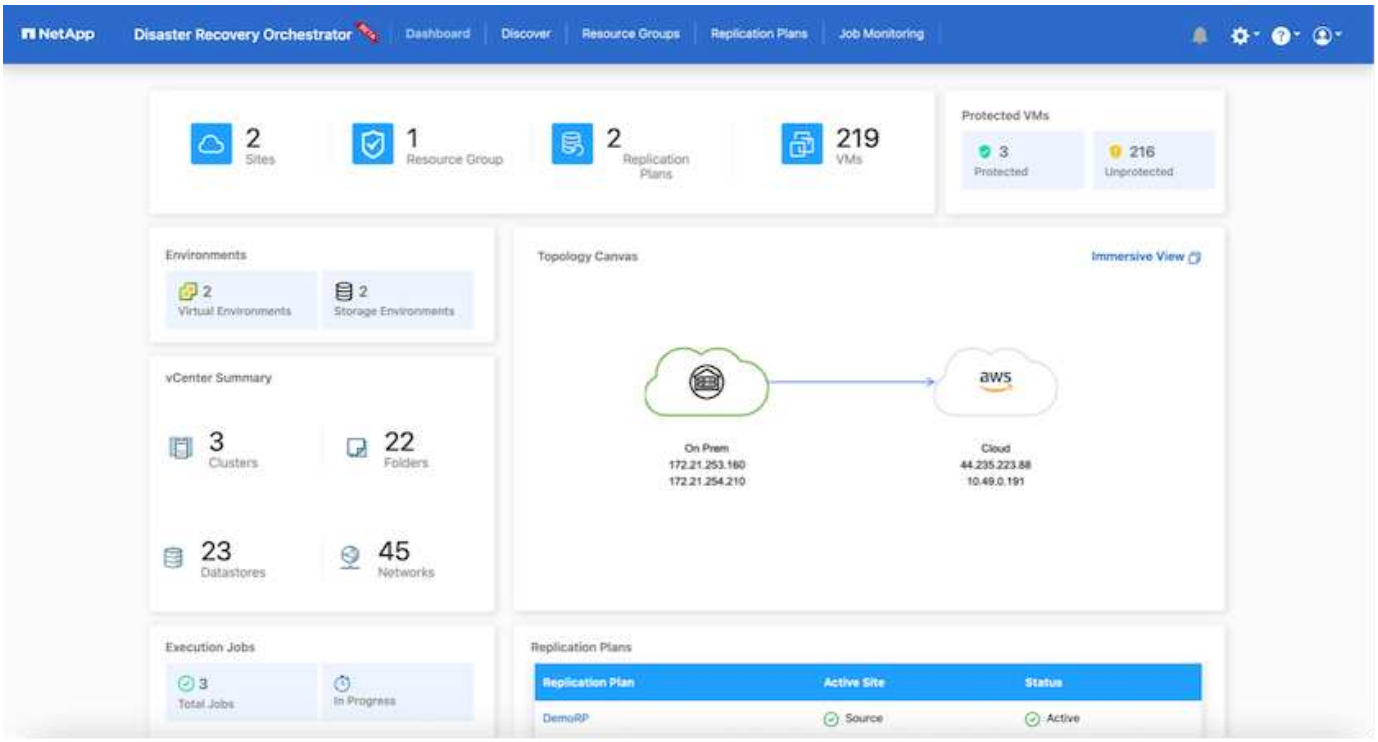


完成後、您可以觸發容錯回復、將其移回原始正式作業站台。





從NetApp BlueXP中、我們可以看到適當磁碟區（對應至VMC的磁碟區為讀寫磁碟區）的複寫健全狀況已經中斷。在測試容錯移轉期間、DRO不會對應目的地或複本磁碟區。相反地、它會製作所需SnapMirror（或Snapshot）執行個體的FlexClone複本、並公開FlexClone執行個體、而FlexClone執行個體不會耗用額外的實體容量來ONTAP 進行FSXfor Sf2。此程序可確保磁碟區未被修改、即使在DR測試或分類工作流程期間、複本工作仍可繼續執行。此外、此程序可確保在發生錯誤或恢復毀損的資料時、能夠清除還原作業、而不會造成複本遭到破壞的風險。



勒索軟體恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體而言、IT組織很難鎖定安全回報點所在的位置、一旦確定了安全回報點、就能保護恢復的工作負載、避免遭受例如睡眠中的惡意軟體或易受影響的應用程式等重複發生的攻擊。

DRO可讓您從任何可用時間點恢復系統、藉此解決這些疑慮。您也可以將工作負載還原至功能性且隔離的網路、以便應用程式在不受北南流量影響的位置彼此運作和通訊。這可讓您的安全團隊安全進行鑑識、並確保沒有隱藏或睡眠中的惡意軟體。

效益

- 使用高效且彈性的SnapMirror複寫。
- 利用Snapshot複本保留功能、將資料恢復到任何可用的時間點。
- 從儲存、運算、網路及應用程式驗證步驟中、將所有必要步驟完全自動化、以恢復數百至數千部VM。
- 使用不變更複寫磁碟區的方法、使用ONTAP FlexClone技術來恢復工作負載。
  - 避免磁碟區或Snapshot複本的資料毀損風險。
  - 避免災難恢復測試工作流程期間的複寫中斷。
  - 災難恢復資料與雲端運算資源可能用於災難恢復以外的工作流程、例如DevTest、安全性測試、修補或升級測試、以及補救測試。
- CPU與RAM最佳化、可將還原作業移至較小的運算叢集、協助降低雲端成本。

使用 **Veeam Replication** 和 **FSX for ONTAP** 在 **AWS** 上進行災難恢復至 **VMware Cloud**

作者： Niyaz Mohamed - NetApp 解決方案工程

總覽

Amazon FSx for NetApp ONTAP 與 AWS 上的 VMware Cloud 整合、是以 NetApp ONTAP 檔案系統為基礎的 AWS 託管外部 NFS 資料存放區、可附加至 SDDC 中的叢集。它為客戶提供靈活、高效能的虛擬化儲存基礎架構、可在運算資源之外進行擴充。

對於那些希望使用 VMware Cloud on AWS SDDC 做為災難恢復目標的客戶、 ONTAP 資料存放區的 FSX 可用於使用任何驗證的協力廠商解決方案、提供 VM 複寫功能、從內部部署複寫資料。透過新增適用於 ONTAP 資料存放區的 FSX 、相較於在 AWS SDDC 上建置 VMware 雲端、它將可實現成本最佳化的部署、並提供大量的 ESXi 主機以容納儲存設備。

此方法也可協助客戶在 VMC 中使用試驗性光叢集、以及將 ONTAP 資料存放區的 FSX 來裝載 VM 複本。同樣的程序也可透過正常容錯移轉複寫計畫、以作為移轉選項延伸至 VMware Cloud on AWS 。

問題陳述

本文件說明如何使用適用於 ONTAP 資料存放區和 Veeam 備份與複寫的 FSX 、以使用 VM 複寫功能、為內部部署的 VMware VM 設定災難恢復至 VMware Cloud on AWS 。

Veeam 備份與複寫功能可在現場及遠端複寫災難恢復（ DR ）。複寫虛擬機器時、 Veeam 備份與複寫會在 AWS SDDC 叢集上的目標 VMware Cloud 上、以原生 VMware vSphere 格式建立 VM 的精確複本、並使複本與原始 VM 保持同步。

複寫可提供最佳的恢復時間目標（ RTO ）值、因為虛擬機器的複本處於就緒啟動狀態。 這種複寫機制可確保工作負載在發生災難事件時、可在 AWS SDDC 上的 VMware Cloud 上快速啟動。Veeam 備份與複寫軟體也能最佳化流量傳輸、以便透過 WAN 進行複寫、並降低連線速度。此外、它也會篩選出重複的資料區塊、零資料區塊、交換檔案和排除的 VM 來賓作業系統檔案、並壓縮複本流量。

為了避免複寫工作佔用整個網路頻寬、可以制定 WAN 加速器和網路節流規則。Veeam Backup & Replication 中的複寫程序是由工作所驅動、這表示複寫是透過設定複寫工作來執行。發生災難事件時、可觸發容錯移轉、藉由容錯移轉至複本來恢復 VM 。

執行容錯移轉時、複寫的 VM 會接管原始 VM 的角色。容錯移轉可以執行至複本的最新狀態、或是任何已知的還原點。如此一來、就能視需要進行勒索軟體恢復或隔離測試。在 Veeam 備份與複寫中、容錯移轉與容錯回復是暫時的中繼步驟、應進一步完成。Veeam 備份與複寫提供多種選項來處理不同的災難恢復案例。

[使用 Veeam Replication 和適用於 VMC 的 FSX ONTAP 的災難恢復案例圖表]

解決方案部署

高階步驟

1. Veeam 備份與複寫軟體是在內部環境中執行、並具備適當的網路連線能力。
2. 在 AWS 上設定 VMware Cloud 、請參閱 VMware Cloud Tech Zone 文章 "VMware Cloud on AWS 與 Amazon FSX for NetApp ONTAP 部署指南整合" 若要部署、請在 AWS SDDC 上設定 VMware Cloud 、將 ONTAP 的 FSx 設定為 NFS 資料存放區。（以最小組態設定的試行環境可用於 DR 用途。發生事件時、 VM 會容錯移轉至此叢集、並可新增其他節點）。
3. 設定複寫工作、以使用 Veeam 備份與複寫建立 VM 複本。
4. 建立容錯移轉計畫並執行容錯移轉。
5. 災難事件完成且主站台正常運作後、切換回正式作業的 VM 。

Veeam VM 複寫至 **VMC** 和 **ONTAP** 資料存放區的 **FSX** 的先決條件

1. 確保 Veeam 備份與複寫備份虛擬機器已連線至來源 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簡短名稱、並連線至來源和目標 vCenter 。
3. ONTAP 資料存放區的目標 FSX 必須有足夠的可用空間來儲存複寫 VM 的 VMDK

如需其他資訊、請參閱涵蓋的「考量與限制」 "請按這裡"。

部署詳細資料

步驟 **1** ：複寫 **VM**

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

若要複寫 VM 、請依照下列步驟進行：

1. 開啟 Veeam 備份與複寫主控台。
2. 在首頁檢視中、選取複寫工作 > 虛擬機器 > VMware vSphere 。
3. 指定工作名稱並選取適當的進階控制核取方塊。按一下「下一步」
   - 如果內部部署和 AWS 之間的連線頻寬有限、請選取複本植入核取方塊。
   - 如果 AWS SDDC 上 VMware Cloud 上的區段與內部部署站台網路不相符、請選取「網路重新對應（適用於具有不同網路的 AWS VMC 站台）」核取方塊。
   - 如果內部生產站台的 IP 定址方案與 AWS VMC 站台的配置不同、請選取複本重新 IP （適用於具有不同 IP 定址方案的 DR 站台）核取方塊。

     [Dr Veeam FSX 影像 2.] | *dr-veeam-fsx-image2.png*
4. 在 * 虛擬機器 * 步驟中、選取需要複寫至 FSX 的 VM 、以將 ONTAP 資料存放區附加至 AWS SDDC 上的 VMware Cloud 。虛擬機器可放置在 vSAN 上、以填滿可用的 vSAN 資料存放區容量。在試驗性光叢集中、 3 節點叢集的可用容量將會受到限制。其餘資料可複寫至 ONTAP 資料存放區的 FSX 。按一下 * 新增 * 、然後在 * 新增物件 * 視窗中選取必要的 VM 或 VM 容器、然後按一下 * 新增 * 。單擊 * 下一步 * 。

   [Dr Veeam FSX 影像 3.] | *dr-veeam-fsx-image3.png*
5. 之後、將目的地選取為 AWS SDDC 叢集 / 主機上的 VMware Cloud 、以及 VM 複本適用的資源集區、 VM 資料夾和 ONTAP 資料存放區的 FSX 。然後按一下 * 下一步 * 。

   [Dr Veeam FSX Image4] | *dr-veeam-fsx-image4.png*
6. 在下一個步驟中、視需要在來源和目的地虛擬網路之間建立對應。

   [Dr Veeam FSX 影像 5.] | *dr-veeam-fsx-image5.png*
7. 在 * 工作設定 * 步驟中、指定將儲存 VM 複本中繼資料、保留原則等的備份儲存庫。
8. 在 **Data Transfer** 步驟中更新 **Source** 和 **Target** 代理服務器，並保留 **Automatic** 選擇（默認）並保持 **Direct** 選項，然後單擊 **Next** （下一步）。
9. 在 * 來賓處理 * 步驟中、視需要選取 * 啟用應用程式感知處理 * 選項。單擊 * 下一步 * 。

   [Dr Veeam FSX 影像 6.] | *dr-veeam-fsx-image6.png*
10. 選擇複寫排程以定期執行複寫工作。
11. 在精靈的 * 摘要 * 步驟中、檢閱複寫工作的詳細資料。若要在精靈關閉後立即啟動工作、請選取 * 按一下「完成」時執行工作 * 核取方塊、否則請取消選取核取方塊。然後按一下 * 完成 * 以關閉精靈。

    [Dr Veeam FSX 影像 7.] | *dr-veeam-fsx-image7.png*

複寫工作啟動後、會在目的地 VMC SDDC 叢集 / 主機上填入具有指定尾碼的虛擬機器。

[Dr Veeam FSX 影像 8.] | *dr-veeam-fsx-image8.png*

如需 Veeam 複寫的其他資訊、請參閱 "複寫的運作方式"。

步驟 **2** ：建立容錯移轉計畫

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

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

只有在初始複寫完成且 VM 複本處於就緒狀態時、才能新增容錯移轉計畫。

執行容錯移轉計畫時可同時啟動的虛擬機器數量上限為 10 個。

在容錯移轉過程中、來源 VM 將不會關閉。

若要建立 * 容錯移轉計畫 * 、請執行下列步驟：

1. 在主畫面上、選取 * 容錯移轉計畫 > VMware vSphere * 。
2. 接下來、請提供計畫的名稱和說明。可視需要新增容錯移轉前後指令碼。例如、在啟動複寫的虛擬機器之前、請先執行指令碼來關閉虛擬機器。

   [Dr Veeam FSX 影像 9.] | *dr-veeam-fsx-image9.png*

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

   [Dr Veeam FSX 影像 10.] | *dr-veeam-fsx-image10.png*

如需建立複寫工作的其他資訊、請參閱 "建立複寫工作"。

步驟 **3** ：執行容錯移轉計畫

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

確保已建立網路區段、以避免災難恢復訓練期間發生 IP 衝突。

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

[Dr Veeam FSX 影像 11.] | *dr-veeam-fsx-image11.png*

[Dr Veeam FSX 影像 12.] | *dr-veeam-fsx-image12.png*

VM 複本的狀態會從「準備就緒」變更為「容錯移轉」、而 VM 會在 AWS SDDC 叢集 / 主機上的目的地 VMware Cloud 上啟動。

[Dr Veeam FSX 版本 13.] | *dr-veeam-fsx-image13.png*

容錯移轉完成後、 VM 的狀態會變更為「容錯移轉」。

[Dr Veeam FSX 影像 14.] | *dr-veeam-fsx-image14.png*

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

如需容錯移轉計畫的詳細資訊、請參閱 "容錯移轉計畫"。

步驟 **4** ：容錯回復至正式作業網站

當容錯移轉計畫執行時、它會被視為中間步驟、需要根據需求完成。選項包括：

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

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

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

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

[Dr Veeam FSX 影像 15.] | *dr-veeam-fsx-image15.png*

[Dr Veeam FSX 影像 16.] | *dr-veeam-fsx-image16.png*

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

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

[Dr Veeam FSX 影像 17.] | *dr-veeam-fsx-image17.png*

[Dr Veeam FSX 影像 18.] | *dr-veeam-fsx-image18.png*

在容錯回復至正式作業後、虛擬機器都會還原回原始正式作業站台。

[Dr Veeam FSX 影像 19.] | *dr-veeam-fsx-image19.png*

結論

ONTAP 資料存放區功能的 FSX 可讓 Veeam 或任何經過驗證的協力廠商工具、使用 Pilot Light 叢集提供低成本的 DR 解決方案、而無需在叢集中直立放置大量主機、只需容納 VM 複本即可。這是一套強大的解決方案、可處理量身打造的自訂災難恢復計畫、並可重複使用內部現有的備份產品以滿足災難恢復需求、進而透過內部部署的災難恢復資料中心、實現雲端型災難恢復。當發生災難時、只要按一下按鈕、即可依照計畫進行容錯移轉或容錯移轉、並決定啟動 DR 站台。

若要深入瞭解此程序、歡迎觀看詳細的逐步解說影片。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

在 **AWS / VMC** 上移轉工作負載

TR 4942：**ONTAP** 使用**VMware HCX**將工作負載移轉至**FSx**支援資料存放區

作者：NetApp解決方案工程

總覽：使用**VMware HCX**、**FSx ONTAP** 補充資料存放區和**VMware Cloud**移轉虛擬機器

Amazon Web Services（AWS）上的VMware Cloud（VMC）的常見使用案例、其補充NFS資料存放區位於Amazon FSX for NetApp ONTAP 的NetApp功能區上、就是移轉VMware工作負載。VMware HCX是首選選選項、提供多種移轉方法、可將內部部署虛擬機器（VM）及其資料（在任何VMware支援的資料存放區上執行）移至VMC資料存放區、其中包括FSXfor ONTAP VMware上的補充NFS資料存放區。

VMware HCX主要是一個行動平台、其設計旨在簡化跨雲端的工作負載移轉、工作負載重新平衡及營運不中斷。它是AWS上VMware Cloud的一部分、提供許多移轉工作負載的方法、可用於災難恢復（DR）作業。

本文件提供部署及設定VMware HCX的逐步指引、包括內部部署及雲端資料中心端的所有主要元件、可實現各種VM移轉機制。

如需詳細資訊、請參閱 "HCX部署簡介" 和 "在AWS SDDC目的地環境上安裝檢查清單B - HCX搭配VMware Cloud"。

高階步驟

此清單提供安裝及設定VMware HCX的高階步驟：

1. 透過VMware Cloud Services Console啟動VMC軟體定義資料中心（SDDC）的HCX。
2. 在內部部署的vCenter Server中下載並部署HCX Connector OVA安裝程式。
3. 使用授權金鑰啟動HCX。
4. 將內部部署的VMware HCX Connector與VMC HCX Cloud Manager配對。
5. 設定網路設定檔、運算設定檔和服務網格。
6. （選用）執行「Network Extension（網路延伸）」以延伸網路並避免重新IP。
7. 驗證應用裝置狀態、並確保可以進行移轉。
8. 移轉VM工作負載。

先決條件

開始之前、請先確定符合下列先決條件。如需詳細資訊、請參閱 "準備安裝HCX"。在具備連線能力等先決條件之後、從VMC的VMware HCX主控台產生授權金鑰、即可設定及啟動HCX。啟用HCX之後、就會部署vCenter外掛程式、並可透過vCenter主控台進行管理來存取。

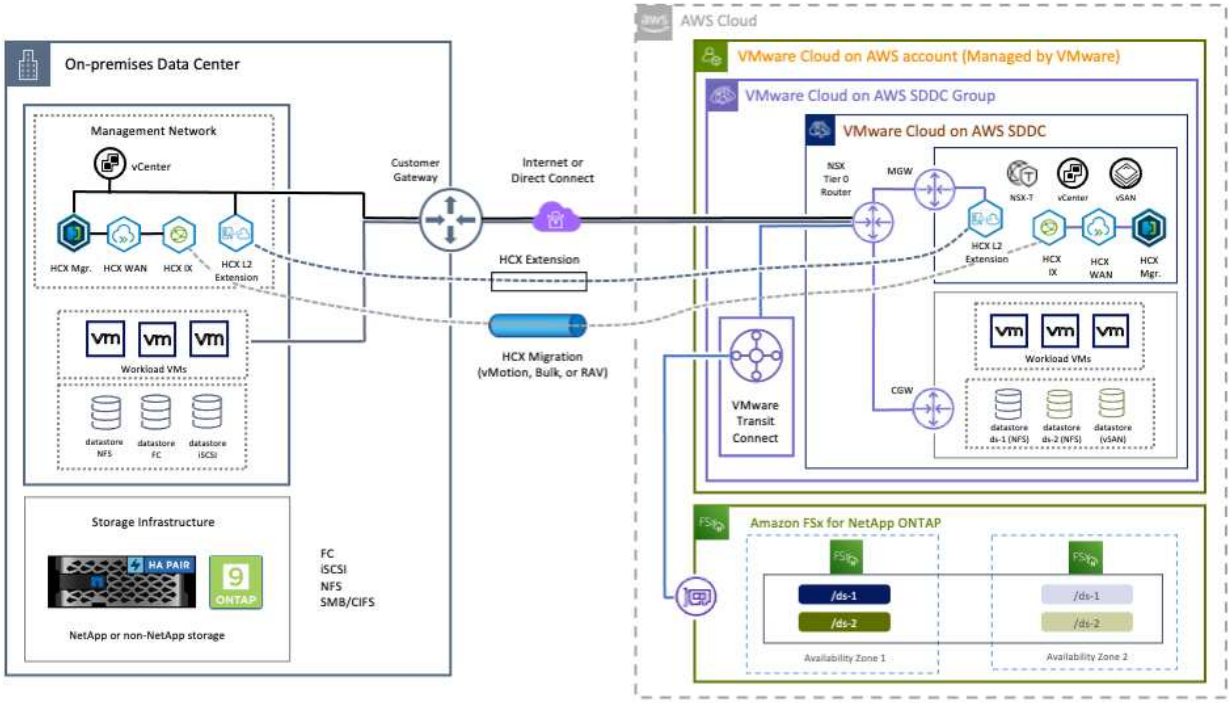
在繼續執行HCX啟動與部署之前、必須先完成下列安裝步驟：

1. 請使用現有的VMC SDDC、或在這之後建立新的SDDC "NetApp連結" 或是這種情況 "VMware連結"。
2. 從內部部署vCenter環境到VMC SDDC的網路路徑、必須使用vMotion來支援VM移轉。
3. 請確定所需的 "防火牆規則和連接埠" 允許內部部署vCenter Server與SDDC vCenter之間的VMotion流量。
4. FSx for ONTAP SforiNFS Volume應安裝為VMC SDDC的補充資料存放區。 若要將NFS資料存放區附加至適當的叢集、請遵循本文所述的步驟 "NetApp連結" 或是這種情況 "VMware連結"。

高層架構

為了進行測試、此驗證所使用的內部部署實驗室環境是透過站台對站台VPN連線至AWS VPC、因此可透過外部傳輸閘道、在內部部署連線至AWS和VMware Cloud SDDC。HCx移轉與網路延伸流量會透過網際網路在內部部署與VMware雲端目的地SDDC之間傳輸。此架構可修改為使用Direct Connect私有虛擬介面。

下圖說明高層架構。



解決方案部署

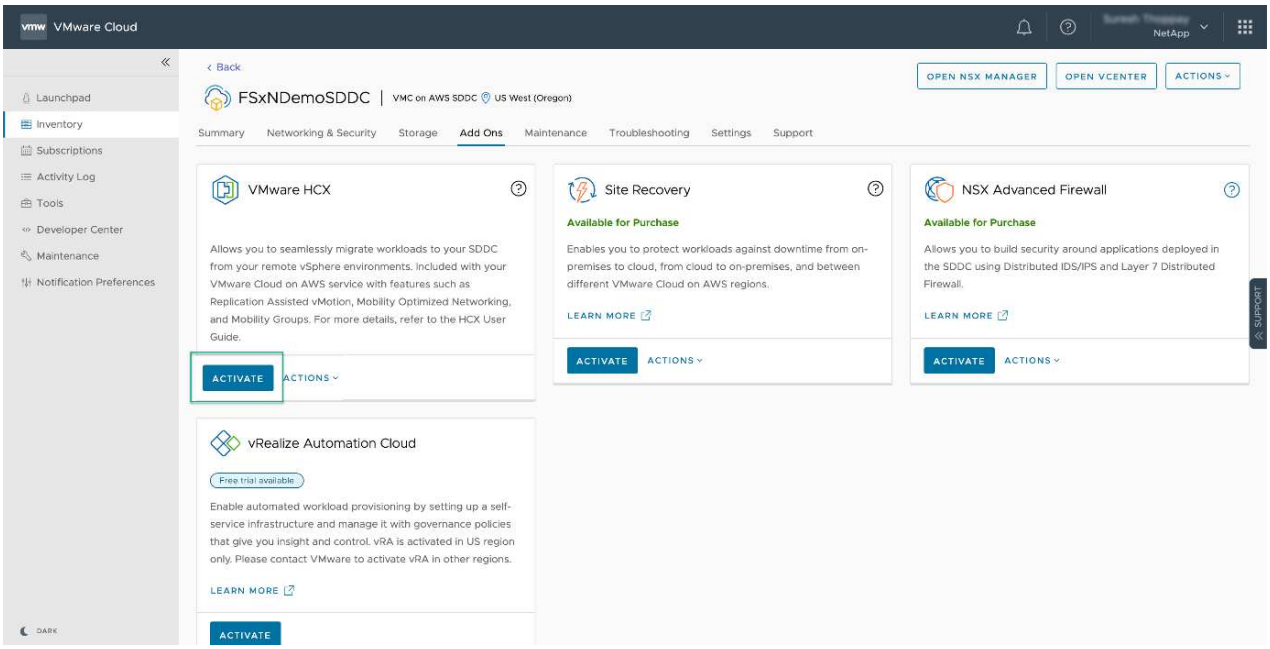
請依照一系列步驟完成本解決方案的部署：

步驟**1**：使用附加元件選項透過**VMC SDDC**啟動**HCX**

若要執行安裝、請完成下列步驟：

1. 登入VMC主控台： "vmc.vmware.com" 並存取庫存。
2. 若要選取適當的SDDC並存取附加元件、請按一下「View Details on SDDC（在SDDC上檢視詳細資料）」、然後選取「Add Ons（新增附加元件）」索引標籤。
3. 按一下「啟用VMware HCX」。

   完成此步驟最多需要25分鐘。

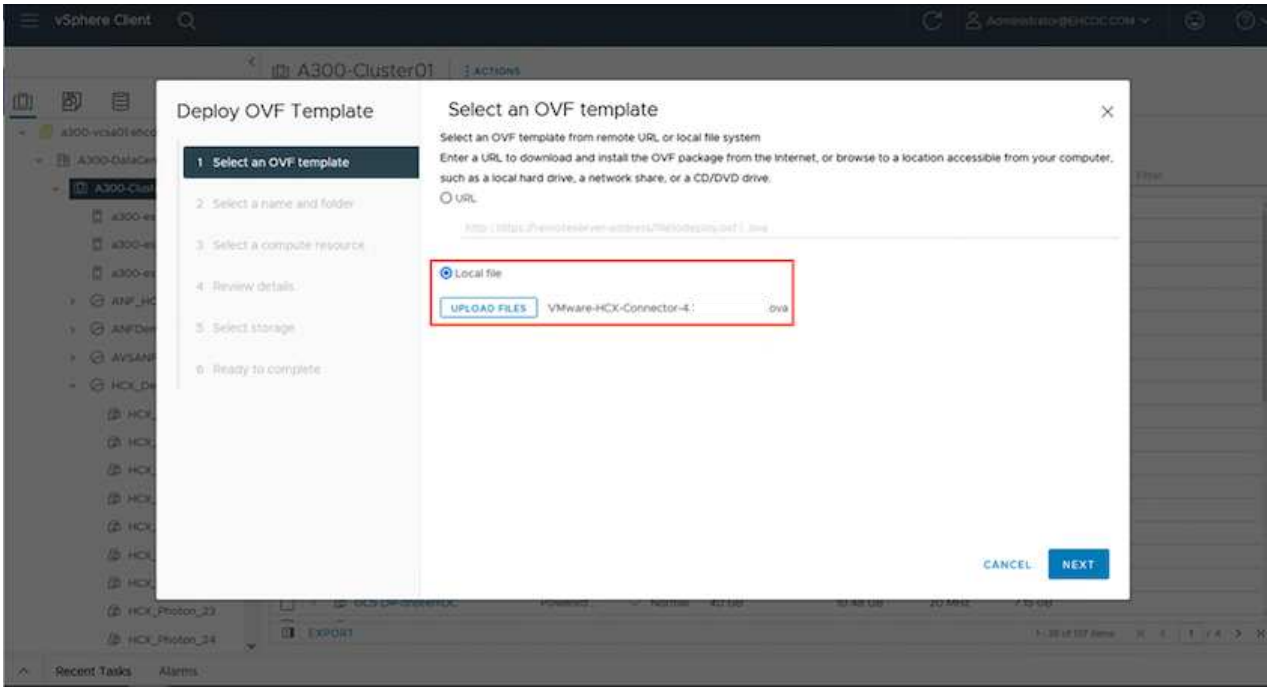


4. 部署完成後、確認vCenter Console中有可用的HCX Manager及其相關外掛程式、以驗證部署。
5. 建立適當的管理閘道防火牆、以開啟存取HCX Cloud Manager所需的連接埠。HCX Cloud Manager現在已可開始執行HCX作業。

步驟**2**：在內部部署**vCenter Server**中部署安裝程式**OVA**

若要讓內部部署連接器與VMC中的HCX Manager通訊、請確定內部部署環境中已開啟適當的防火牆連接埠。

1. 從VMC主控台瀏覽至HCX儀表板、移至「Administration」（管理）、然後選取「Systems Update」（系統更新）索引標籤。按一下「Request a Download Link for the HCX Connector OVA image（申請HCX Connector OVA映像的下載連結
2. 下載HCX Connector之後、在內部部署的vCenter Server中部署OVA。以滑鼠右鍵按一下vSphere叢集、然後選取部署OVF範本選項。

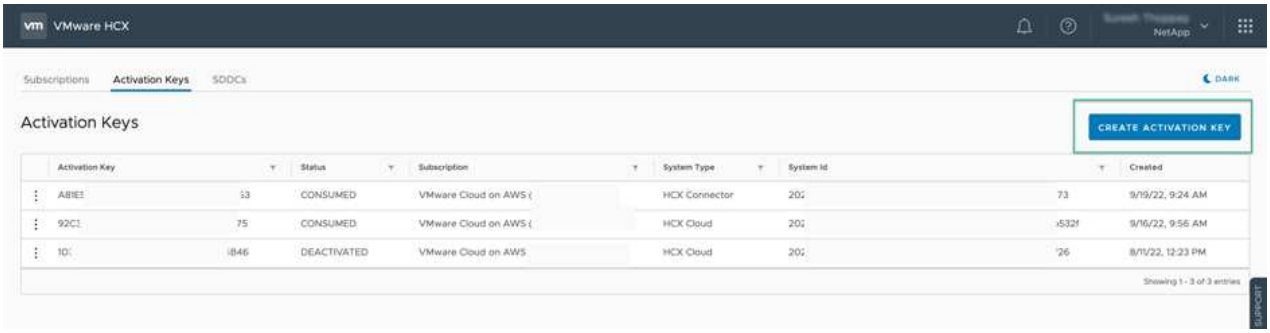


3. 在「部署OVF範本」精靈中輸入必要資訊、按一下「下一步」、然後按一下「完成」以部署VMware HCX Connector OVA。
4. 手動開啟虛擬應用裝置電源。如需逐步指示、請前往 "VMware HCX使用者指南"。

步驟3：使用授權金鑰啟動HCX Connector

在內部部署VMware HCX Connector OVA並啟動應用裝置之後、請完成下列步驟以啟動HCX Connector。從VMC的VMware HCX主控台產生授權金鑰、並在VMware HCX Connector安裝期間輸入授權。

1. 從VMware Cloud Console移至「Inventory（資源清冊）」、選取SDDC、然後按一下「View Details（檢視詳細資料）」。在「Add Ons（新增選項）」索引標籤的VMware HCX動態磚中、按一下「Open HCX（開啟HCX）」。
2. 在「啟用金鑰」索引標籤中、按一下「建立啟動金鑰」。選取「System Type（系統類型）」作為HCX Connector、然後按一下「Confirm（確認）」以產生金鑰。複製啟動金鑰。



部署在內部部署的每個HCX Connector都需要個別的金鑰。

3. 登入內部部署的VMware HCX Connector、網址為 "https://hcxconnectorIP:9443" 使用系統管理員認證。

使用在OVA部署期間定義的密碼。

4. 在「授權」區段中、輸入從步驟2複製的啟動金鑰、然後按一下「啟動」。

內部部署的HCX Connector必須能存取網際網路、才能成功完成啟動。

5. 在「資料中心位置」下、提供在內部部署環境中安裝VMware HCX Manager所需的位置。按一下「繼續」。
6. 在「System Name（系統名稱）」下、更新名稱、然後按「Continue（繼續）」。
7. 選取「Yes（是）」、然後繼續。
8. 在「Connect your vCenter（連線vCenter）」下、提供vCenter Server的IP位址或完整網域名稱（FQDN）和認證、然後按一下「Continue（繼續）」。

使用FQDN以避免稍後發生通訊問題。

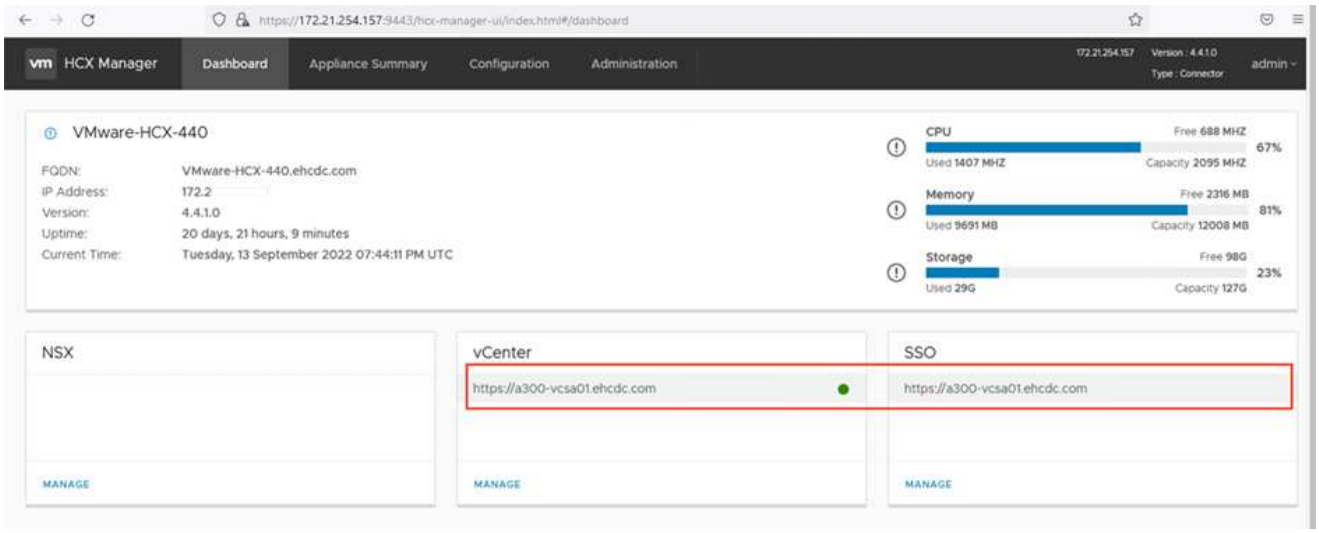
9. 在「Configure SSO/PSC（設定SSO/PSC）」下、提供Platform Services Controller的FQDN或IP位址、然後按一下「Continue（繼續）」。

輸入vCenter Server的IP位址或FQDN。

10. 確認輸入的資訊正確無誤、然後按一下「重新啟動」。

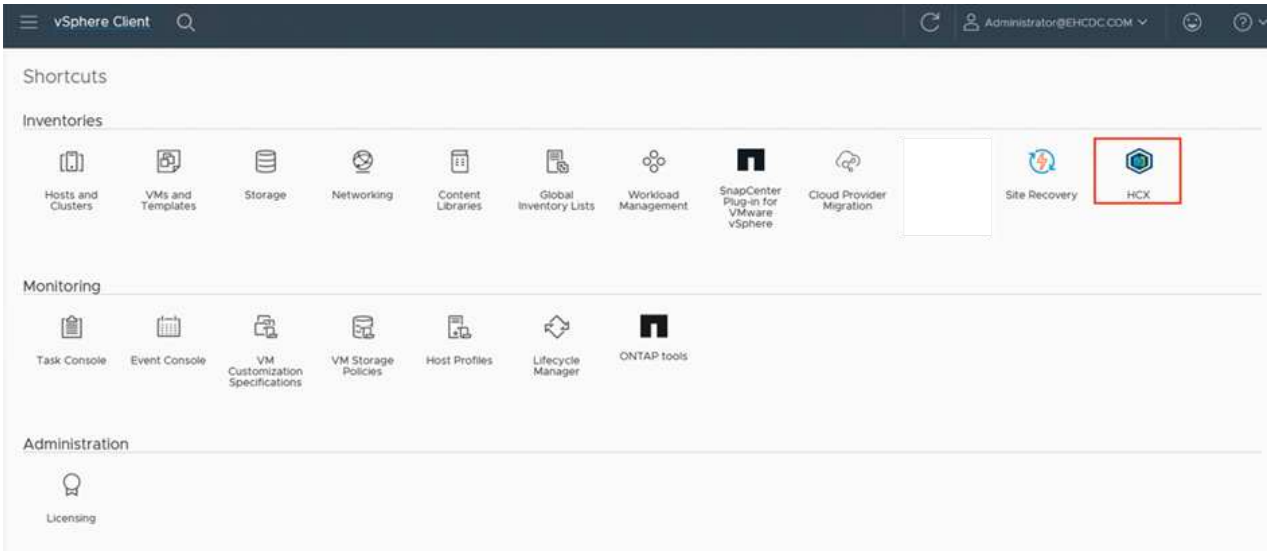
11. 完成後、vCenter Server會顯示為綠色。vCenter Server和SSO都必須具有正確的組態參數、此參數應與上一頁相同。

此程序大約需要10–20分鐘、而外掛程式則要新增至vCenter Server。

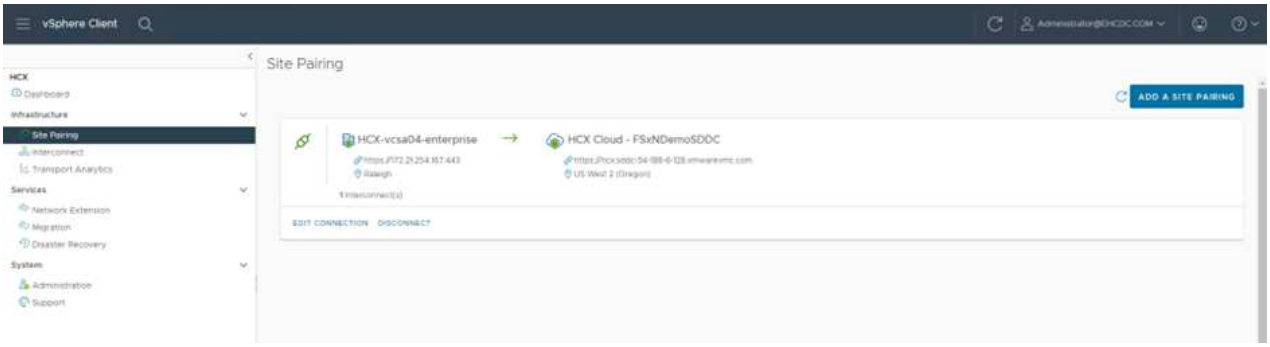


步驟4：將內部部署的VMware HCX Connector與VMC HCX Cloud Manager配對

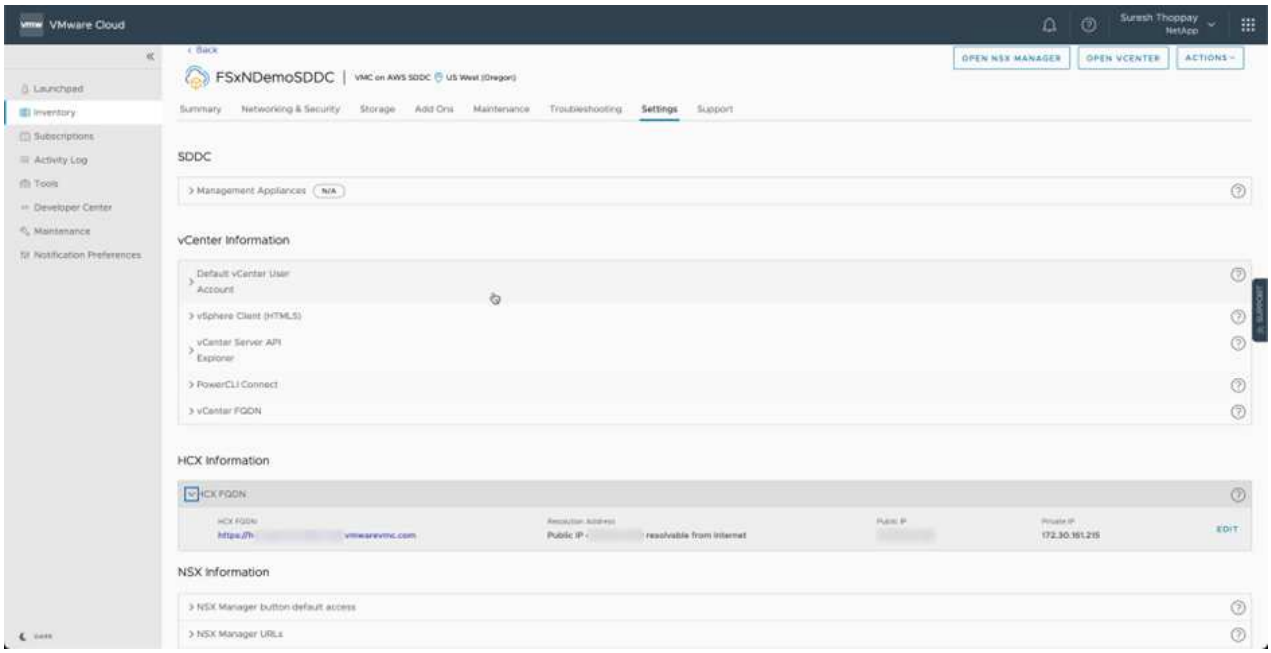
1. 若要在內部部署vCenter Server和VMC SDDC之間建立站台配對、請登入內部部署vCenter Server、然後存取HCX vSphere Web Client外掛程式。

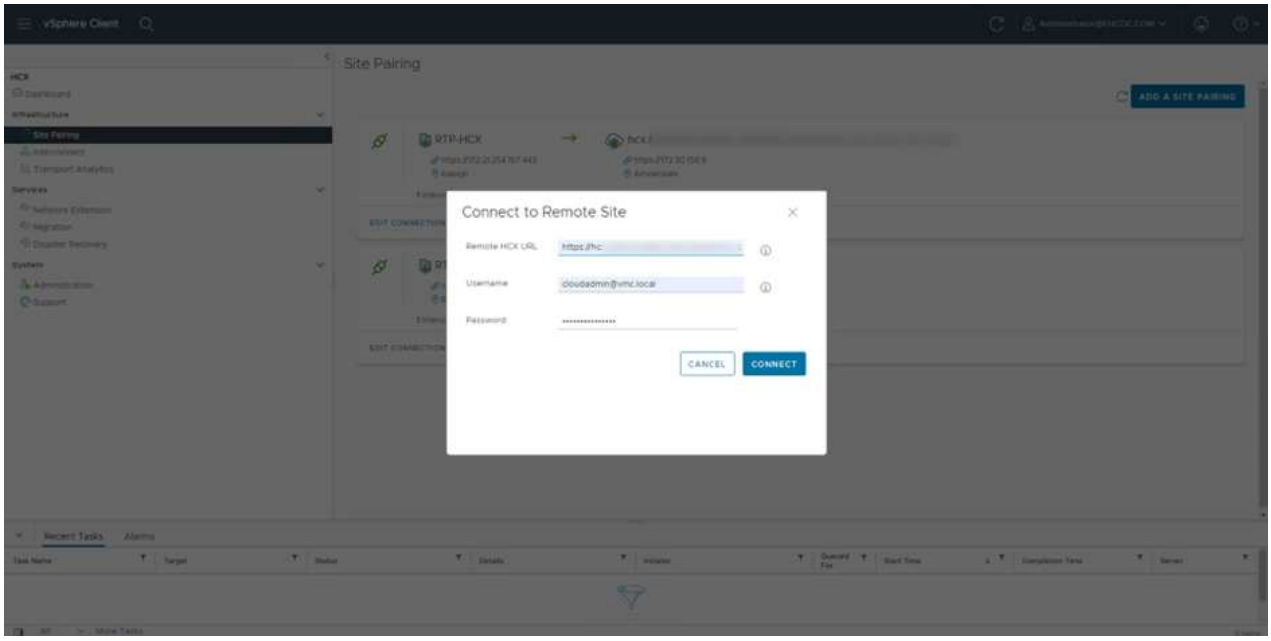


2. 按一下「基礎架構」下的「新增站台配對」。若要驗證遠端站台、請輸入VMC HCX Cloud Manager URL或IP位址、以及CloudAdmin角色的認證資料。



HCx資訊可從SDDC設定頁面擷取。





3. 若要啟動站台配對、請按一下「Connect（連線）」。

   VMware HCX Connector必須能夠透過連接埠443與HCX Cloud Manager IP通訊。

4. 建立配對之後、即可在HCX儀表板上取得新設定的站台配對。

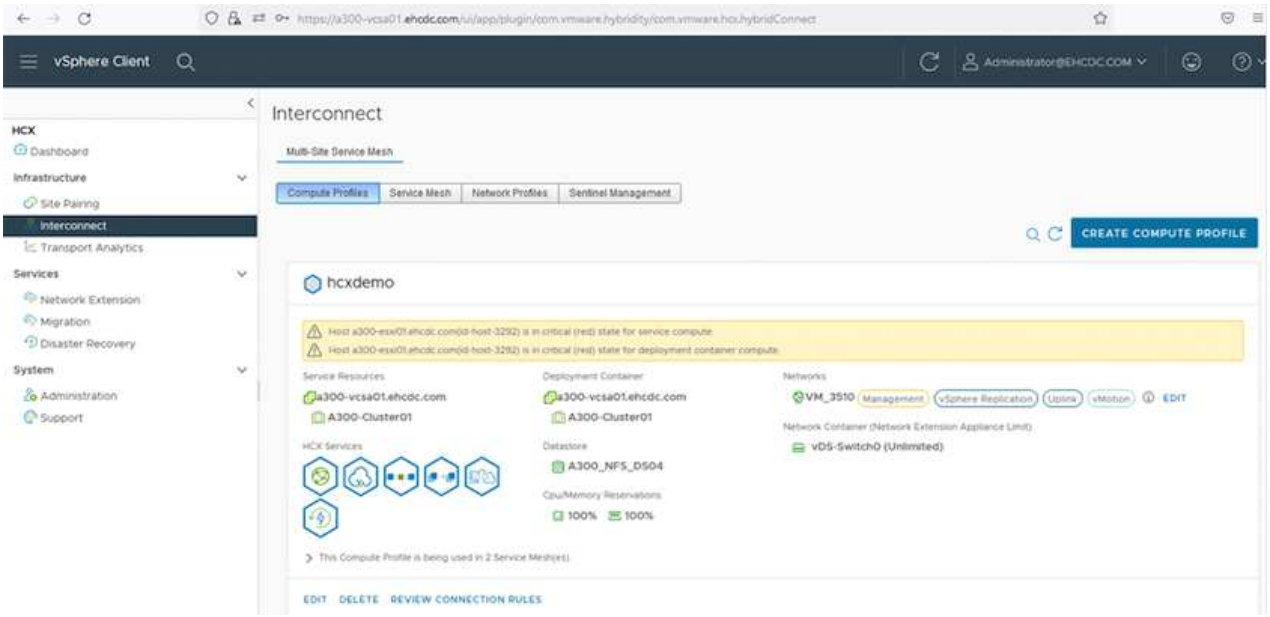
步驟**5**：設定網路設定檔、運算設定檔和服務網格

VMware HCX互連（HCX-IX）應用裝置可透過網際網路提供安全通道功能、並可透過私有連線至目標站台、以啟用複寫和VMotion型功能。互連提供加密、流量工程和SD-WAN。若要建立HCI IX-IX互連設備、請完成下列步驟：

1. 在「基礎架構」下、選取「互連」>「多站台服務網狀架構」>「運算設定檔」>「建立運算設定檔」。

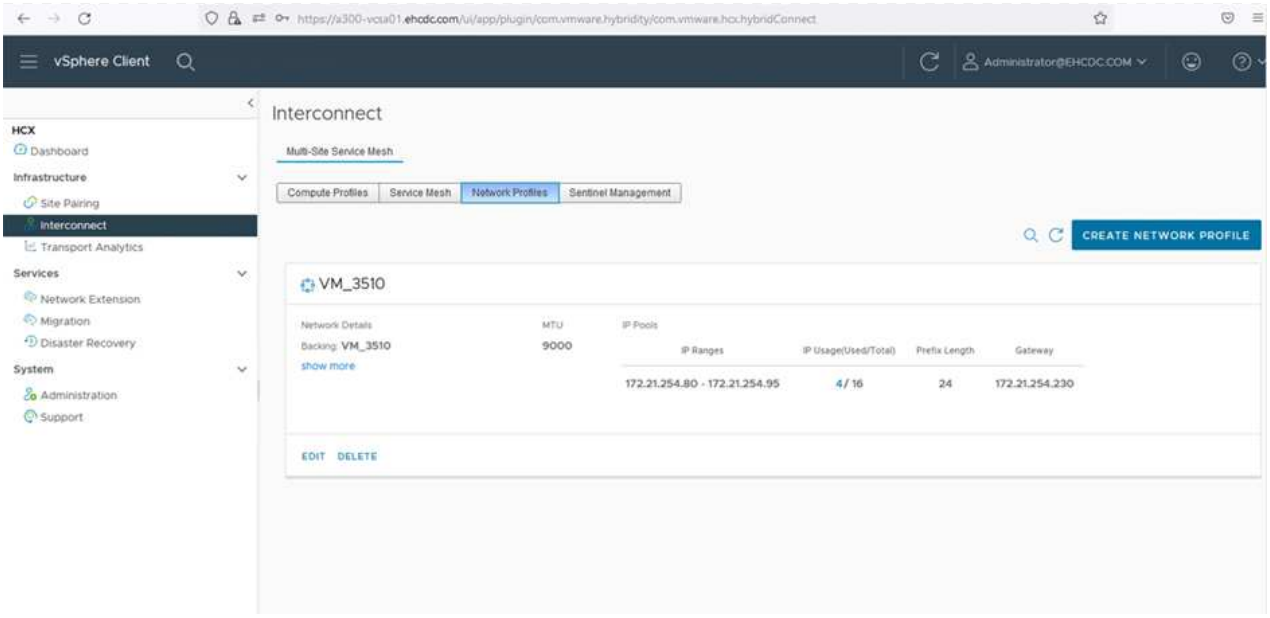
   運算設定檔包含部署互連虛擬應用裝置所需的運算、儲存和網路部署參數。他們也會指定HCX服務可以存取VMware資料中心的哪個部分。

   如需詳細指示、請參閱 "建立運算設定檔"。



2. 建立運算設定檔之後、選取「Multi-Site Service Mesh」（多站台服務網格）>「Network Profiles」（網路設定檔）>「Create Network Profile」（建立網路設定檔）、即可建立網路設定檔。
3. 網路設定檔會定義一系列IP位址和網路、以供HCX用於其虛擬應用裝置。

   這需要兩個以上的IP位址。這些IP位址將從管理網路指派給虛擬應用裝置。

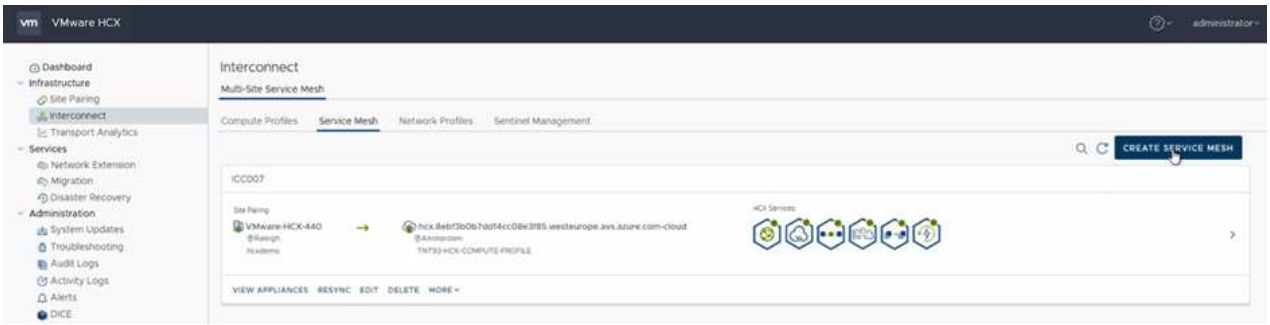


如需詳細指示、請參閱 "建立網路設定檔"。

如果您透過網際網路連線至SD-WAN、則必須在「網路與安全性」區段下保留公用IP。

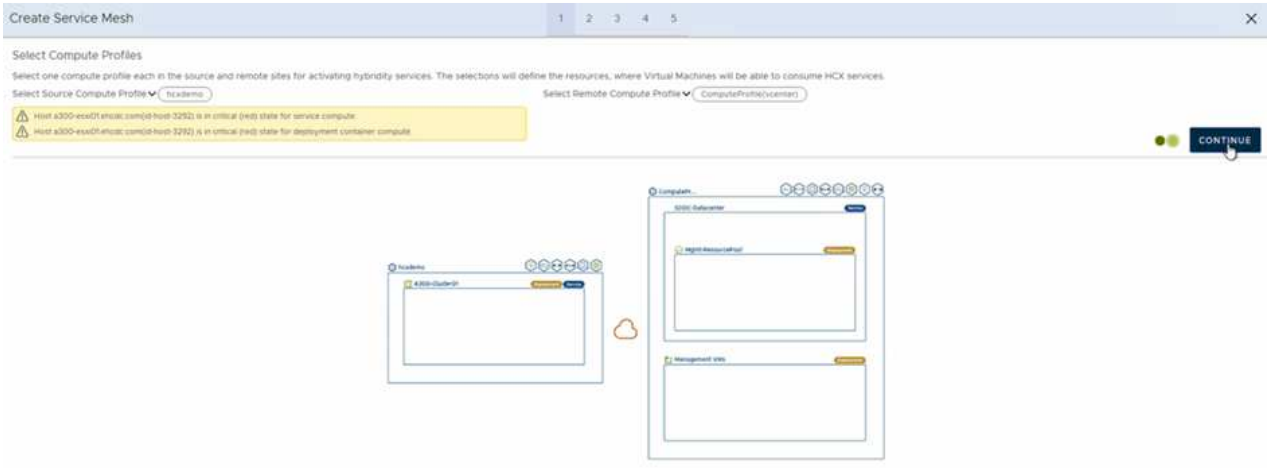
4. 若要建立服務網格、請選取Interconnect選項中的Service Mesh（服務網格）索引標籤、然後選取內部部署和VMC SDDC站台。

   服務網格會建立本機和遠端運算和網路設定檔配對。

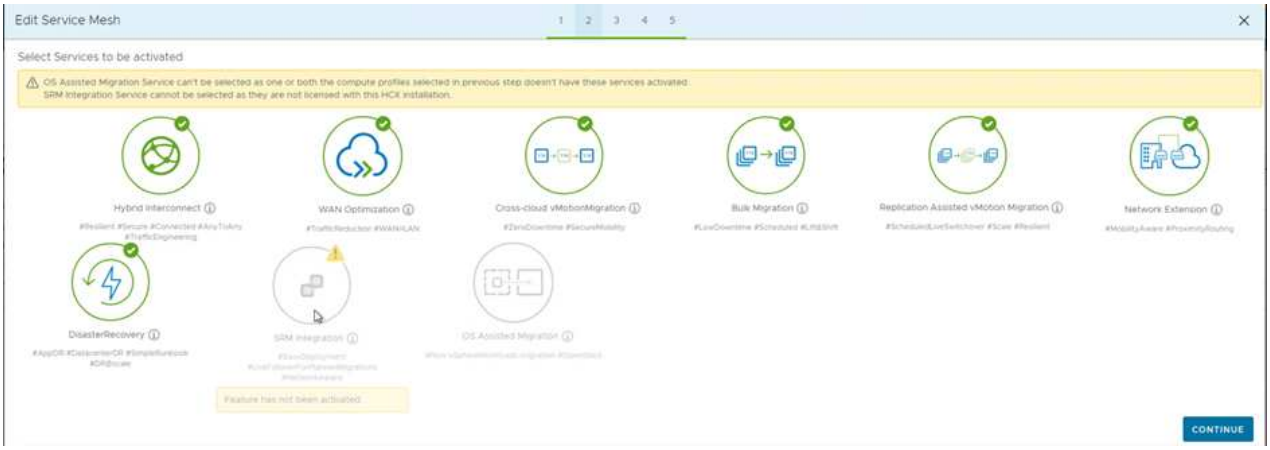


此程序的一部分涉及部署HCX應用裝置、這些裝置將會自動設定在來源和目標站台上、以建立安全的傳輸架構。

5. 選取來源和遠端運算設定檔、然後按一下「Continue（繼續）」。

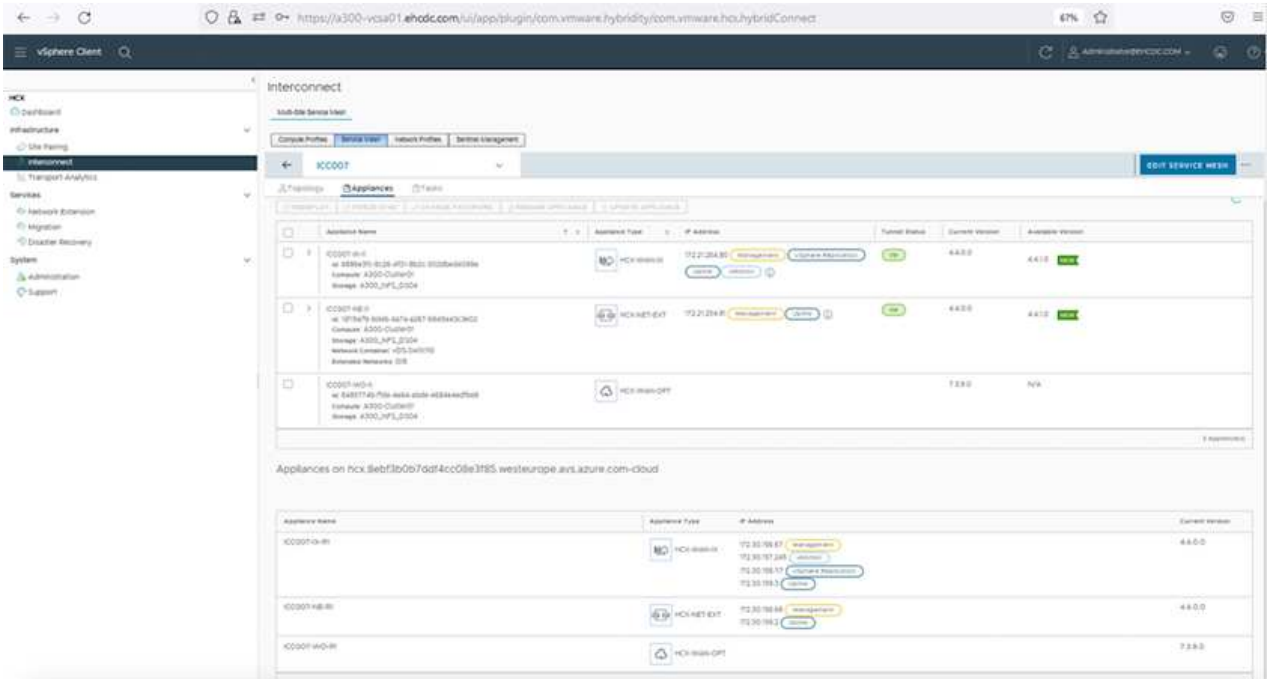


6. 選取要啟動的服務、然後按一下「Continue（繼續）」。



複寫輔助VMotion移轉、SRM整合及OS輔助移轉需要HCX Enterprise授權。

7. 建立服務網格的名稱、然後按一下「完成」開始建立程序。完成部署約需30分鐘。設定好服務網格後、就會建立移轉工作負載VM所需的虛擬基礎架構和網路。


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

步驟**6**：移轉工作負載

HCx可在兩個或多個不同的環境（例如內部部署環境和VMC SDDC）之間提供雙向移轉服務。應用程式工作負載可使用各種移轉技術、例如HCX大量移轉、HCX vMotion、HCX冷移轉、HCX複寫輔助vMotion（可搭配HCX Enterprise版本使用）、以及HCX OS輔助移轉（可搭配HCX Enterprise版本使用）、移轉至或移轉至HCX啟動的站台。

若要深入瞭解可用的HCX移轉技術、請參閱 "VMware HCX移轉類型"

HCX-IX應用裝置使用行動代理程式服務來執行VMotion、Cold和Replication輔助VMotion（RAV）移轉。

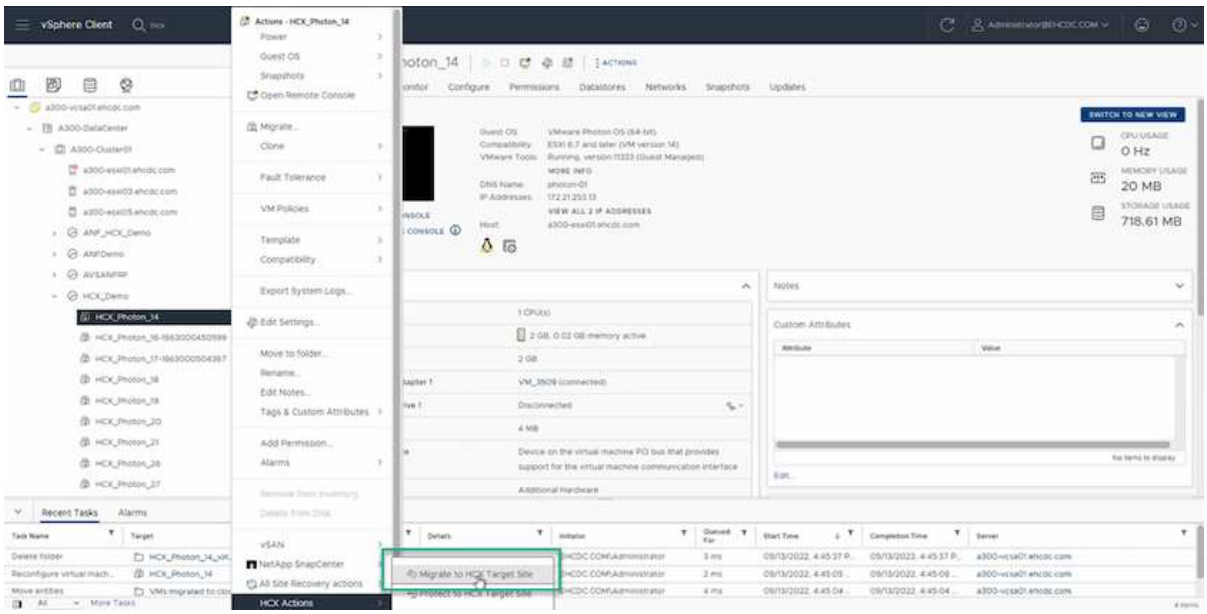
HCX-IX應用裝置會將行動代理程式服務新增為vCenter Server中的主機物件。此物件上顯示的處理器、記憶體、儲存設備和網路資源、並不代表裝載IX應用裝置的實體Hypervisor實際使用量。

VMware HCX vMotion

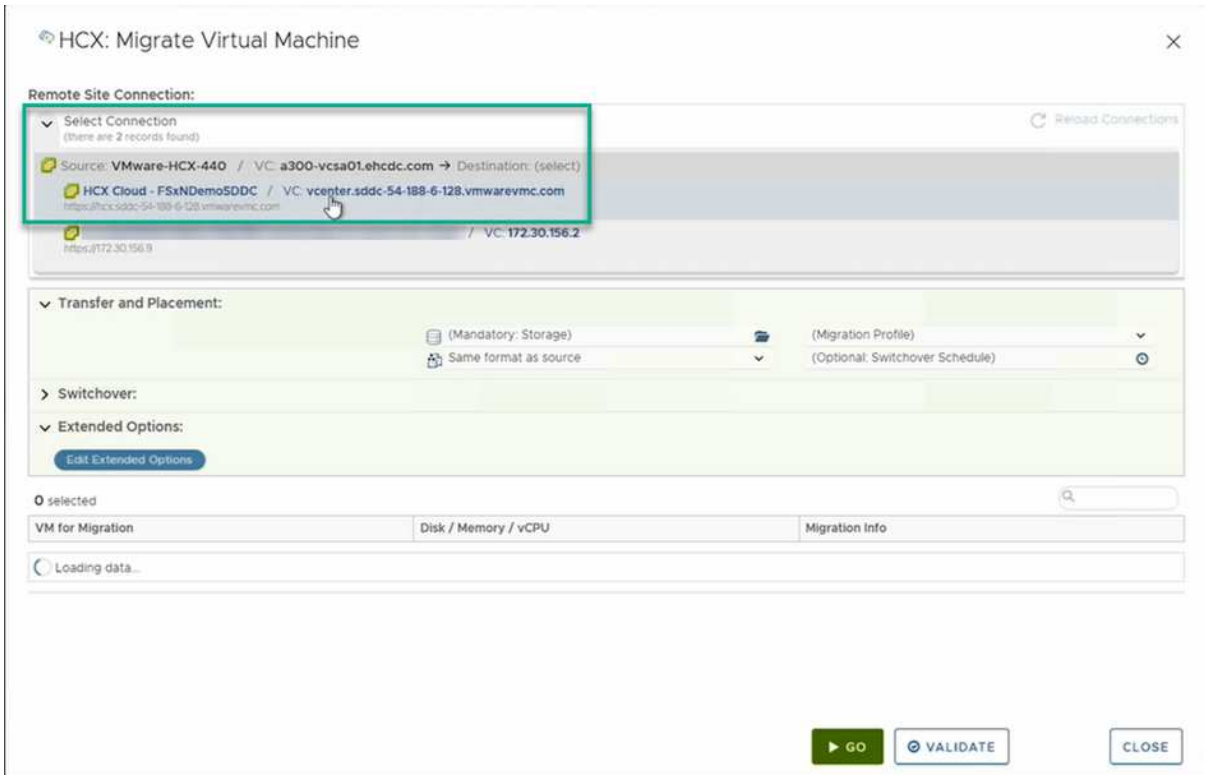
本節說明HCX VMotion機制。此移轉技術使用VMware VMotion傳輸協定將VM移轉至VMC SDDC。VMotion移轉選項可用於一次移轉單一VM的VM狀態。此移轉方法不會中斷服務。

網路擴充功能應已就緒（適用於連接VM的連接埠群組）、以便在不需要變更IP位址的情況下移轉VM。

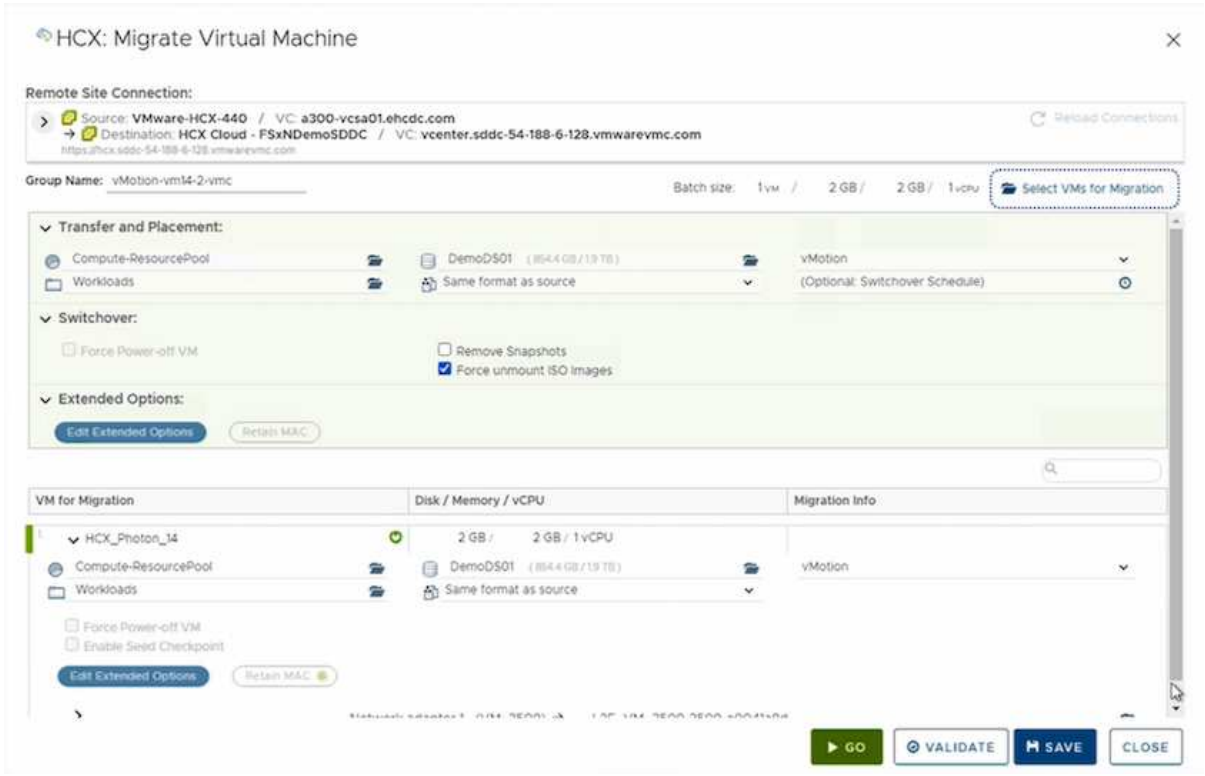
1. 從內部部署vSphere用戶端移至「Inventory」、在要移轉的VM上按一下滑鼠右鍵、然後選取「HCX Actions」（HCX動作）>「移轉至HCX目標站台」。



2. 在移轉虛擬機器精靈中、選取遠端站台連線（目標VMC SDDC）。



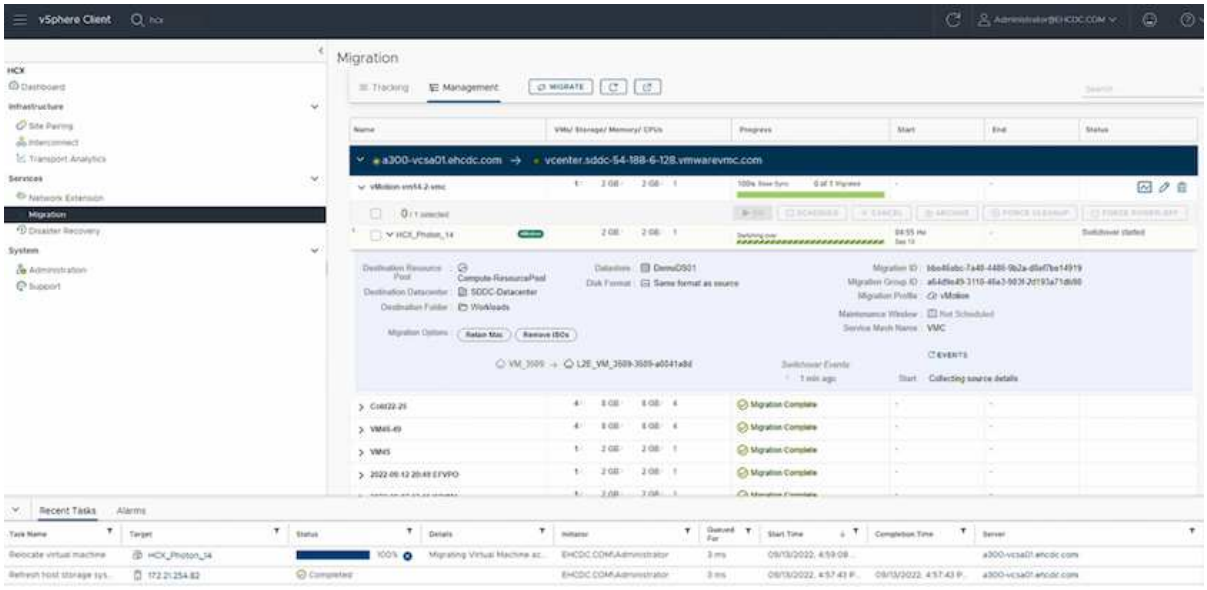
3. 新增群組名稱、並在「Transfer and Placement（傳輸和放置）」下更新必填欄位（叢集、儲存設備和目的地網路）、然後按一下「Validate（驗證）」。



4. 驗證檢查完成後、按一下「Go（執行）」以啟動移轉。

VMotion傳輸會擷取VM作用中記憶體、其執行狀態、IP位址及其MAC位址。如需有關HCX VMotion需求與限制的詳細資訊、請參閱 "瞭解VMware HCX VMotion和冷移轉"。

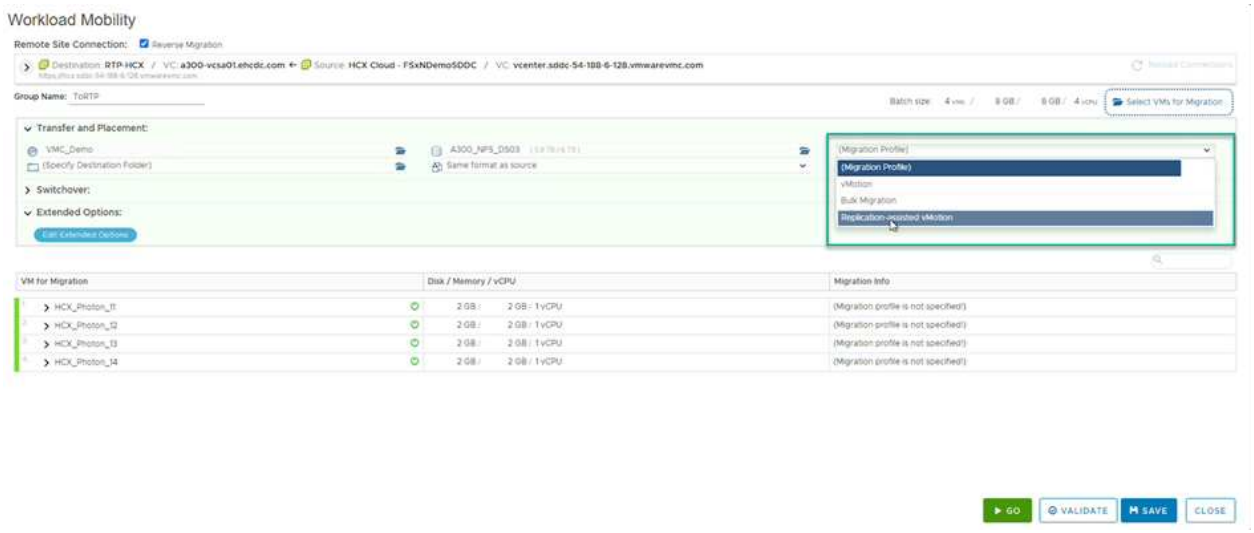
5. 您可以從HCX >移轉儀表板監控VMotion的進度和完成。



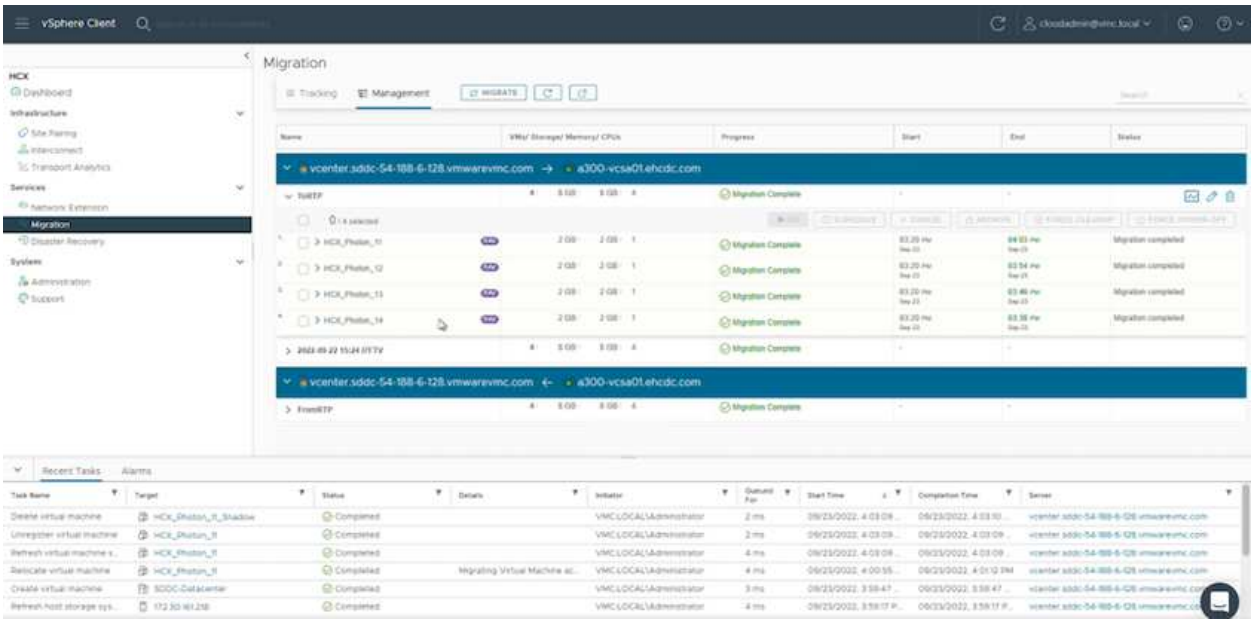
VMware複寫輔助vMotion

您可能從VMware文件中看到、VMware HCX Replication輔助VMotion（RAV）結合了大量移轉與VMotion的優點。大量移轉使用vSphere Replication平行移轉多個VM、而VM會在切換期間重新開機。HCx vMotion可在不中斷的情況下進行移轉、但會在複寫群組中一次連續執行一部VM。Rav會平行複寫VM、並保持同步、直到切換期間為止。在切換過程中、它一次移轉一個VM、而不會停機。

下列快照顯示移轉設定檔為「複寫輔助vMotion」。



與少數VM的vMotion相比、複寫的持續時間可能會更長。使用RAV時、只能同步差異並納入記憶體內容。以下是移轉狀態的快照、顯示移轉的開始時間與每個VM的結束時間如何相同。



如需HCX移轉選項的其他資訊、以及如何使用HCX將工作負載從內部部署移轉至AWS上的VMware Cloud、請參閱 "VMware HCX使用者指南"。

VMware HCX VMotion需要100Mbps或更高的處理量能力。

目標VMC FSX for ONTAP VMware資料存放區必須有足夠的空間來容納移轉作業。

結論

無論您是針對全雲端或混合雲、或是內部部署中任何類型/廠商儲存設備上的資料、Amazon FSx for NetApp ONTAP 支援HCX都能提供絕佳的選項來部署和移轉工作負載、同時將資料需求無縫接軌至應用程式層、進而降低TCO。無論使用案例為何、請選擇VMC搭配使用FSXfor ONTAP VMware資料存放區、以快速實現雲端效益、一致的基礎架構、以及跨內部部署和多個雲端的作業、工作負載的雙向可攜性、以及企業級容量和效能。使用VMware vSphere複寫、VMware vMotion或甚至是NFC-複本來連接儲存設備及移轉VM的程序與程序、都是相當熟悉的程序。

重點摘要

本文件的重點包括：

- 現在您可以將Amazon FSx ONTAP 支援資料存放區與VMC SDDC搭配使用。
- 您可以輕鬆地將資料從任何內部部署資料中心移轉至使用FSXfor ONTAP VMware資料存放區執行的VMC
- 您可以輕鬆擴充和縮減FSX- ONTAP 支援資料存放區、以滿足移轉活動期間的容量和效能需求。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請參閱下列網站連結：

- VMware Cloud文件

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSX for NetApp ONTAP 的支援文件

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX使用者指南

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

區域可用度–**VMC**的補充**NFS**資料存放區

AWS / VMC上的補充NFS資料存放區可用度由Amazon定義。首先、您需要判斷VMC和FSxN是否在指定的區域中可用。接下來、您需要判斷該區域是否支援FSxN補充NFS資料存放區。

- 檢查VMC的可用度 "請按這裡"。
- Amazon定價指南提供FSxN（FSx ONTAP ）的可用位置資訊。您可以找到這些資訊 "請按這裡"。
- VMC的FSxN補充NFS資料存放區即將推出。

在資訊仍在發佈期間、下表將目前對VMC、FSxN和FSxN的支援識別為補充NFS資料存放區。

美洲

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
美國東部（北維吉尼亞州）	是的	是的	是的
美國東部（俄亥俄州）	是的	是的	是的
美國西部（北加州）	是的	否	否
美國西部（俄勒岡州）	是的	是的	是的
GovCloud（美國西部）	是的	是的	是的
加拿大（中部）	是的	是的	是的
南美洲（聖保羅）	是的	是的	是的

最後更新日期：2022年6月2日。

EMEA

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
歐洲（愛爾蘭）	是的	是的	是的
歐洲（倫敦）	是的	是的	是的
歐洲（法蘭克福）	是的	是的	是的
歐洲（巴黎）	是的	是的	是的
歐洲（米蘭）	是的	是的	是的
歐洲（斯德哥爾摩）	是的	是的	是的

最後更新日期：2022年6月2日。

亞太地區

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
亞太地區（悉尼）	是的	是的	是的
亞太地區（東京）	是的	是的	是的
亞太地區（大阪）	是的	否	否
亞太地區（新加坡）	是的	是的	是的
亞太地區（首爾）	是的	是的	是的
亞太地區（Mumbai）	是的	是的	是的
亞太地區（雅加達）	否	否	否
亞太地區（香港）	是的	是的	是的

最後更新日期：2022年9月28日。

適用於**Azure AVS**的**NetApp**功能

深入瞭解NetApp為Azure VMware解決方案（AVS）帶來的功能：從NetApp做為來賓連線儲存設備或補充NFS資料存放區、到移轉工作流程、延伸/突增至雲端、備份/還原及災難恢復、皆可從中獲益。

從下列選項中選取、跳至所需內容的區段：

- "在Azure中設定AVS"
- "適用於AVS的NetApp儲存選項"
- "NetApp / VMware雲端解決方案"

在**Azure**中設定**AVS**

如同內部部署、規劃雲端型虛擬化環境對於成功建立虛擬機器和移轉的正式作業就緒環境來說、是非常重要的。

本節說明如何設定及管理Azure VMware解決方案、以及如何搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的連線Cloud Volumes ONTAP 至Azure VMware解決方案的方法。

設定程序可分為下列步驟：

- 註冊資源供應商並建立私有雲
- 連線至新的或現有的ExpressRoute虛擬網路閘道
- 驗證網路連線能力並存取私有雲端

檢視詳細資訊 "AVS的組態步驟"。

適用於**AVS**的**NetApp**儲存選項

NetApp儲存設備可在Azure AVS中以多種方式使用、無論是作為猜測連接的或作為補充NFS資料存放區。

請造訪 "支援的NetApp儲存選項" 以取得更多資訊。

Azure以下列組態支援NetApp儲存設備：

- 以客體連線儲存設備的形式提供Azure NetApp Files
- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- 作爲NFS補充資料存放區的能力（ANF Azure NetApp Files ）

檢視詳細資訊 "AVS的來賓連線儲存選項"。檢視詳細資訊 "AVS的補充NFS資料存放區選項"。

解決方案使用案例

有了NetApp和VMware雲端解決方案、在Azure AVS中部署的許多使用案例都很簡單。系統會針對VMware定義的每個雲端領域定義SE案例：

- 保護（包括災難恢復和備份/還原）
- 延伸
- 移轉

"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**進行災難恢復

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

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

本文件提供對Jetstream災難恢復作業原則及其主要元件的瞭解。

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

規劃及啟動大量VM的保護（例如、超過100個）時、請使用位於Jetstream DR Automation Toolkit的容量規劃工具（CPt）。提供要保護的VM清單、以及其RTO和恢復群組偏好設定、然後執行CPt。

執行下列功能：

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

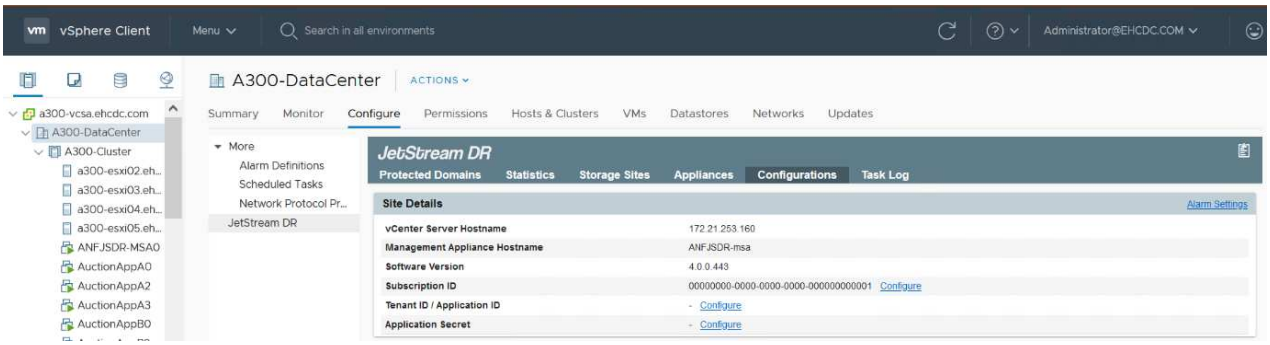
指定的網域數量和內容取決於各種VM特性、例如平均IOPS、總容量、優先順序（定義容錯移轉順序）、RTO及其他特性。

在內部部署資料中心安裝**Jetstream DR**

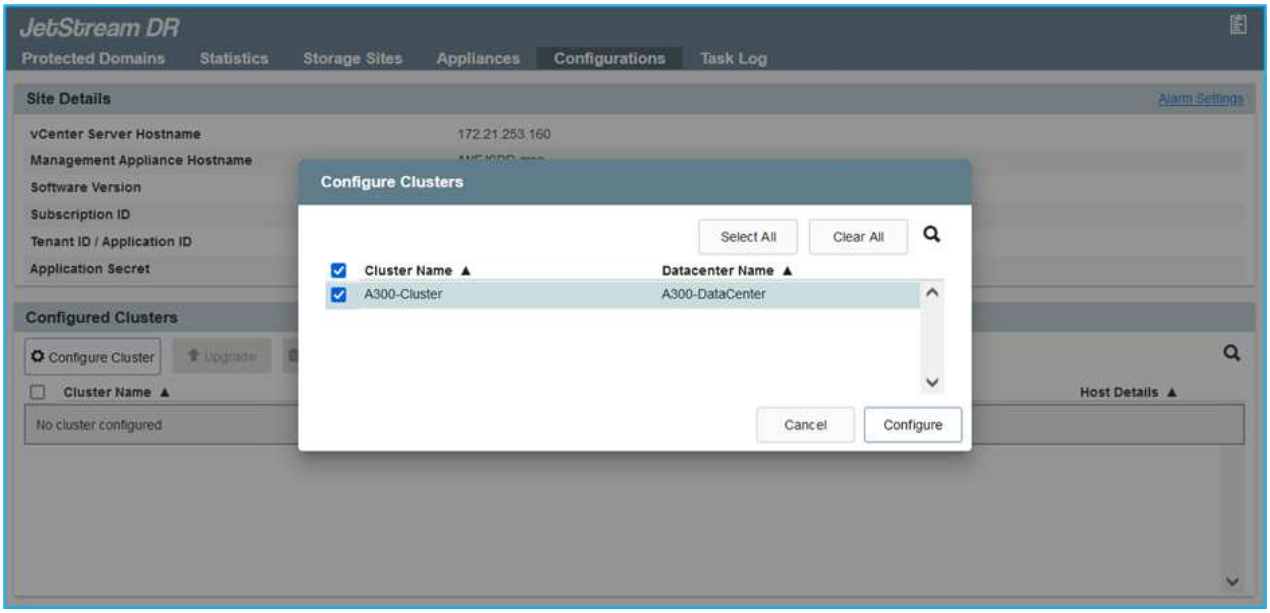
Jetstream DR軟體包含三個主要元件：「Jetstream DR管理伺服器虛擬應用裝置（MSA）」、「DR虛擬應用裝置（DRVA）」和「主機元件（I/O篩選套件）」。MSA用於在運算叢集上安裝及設定主機元件、然後管理Jetstream DR軟體。下列清單提供安裝程序的詳細說明：

如何為內部部署安裝**Jetstream DR**

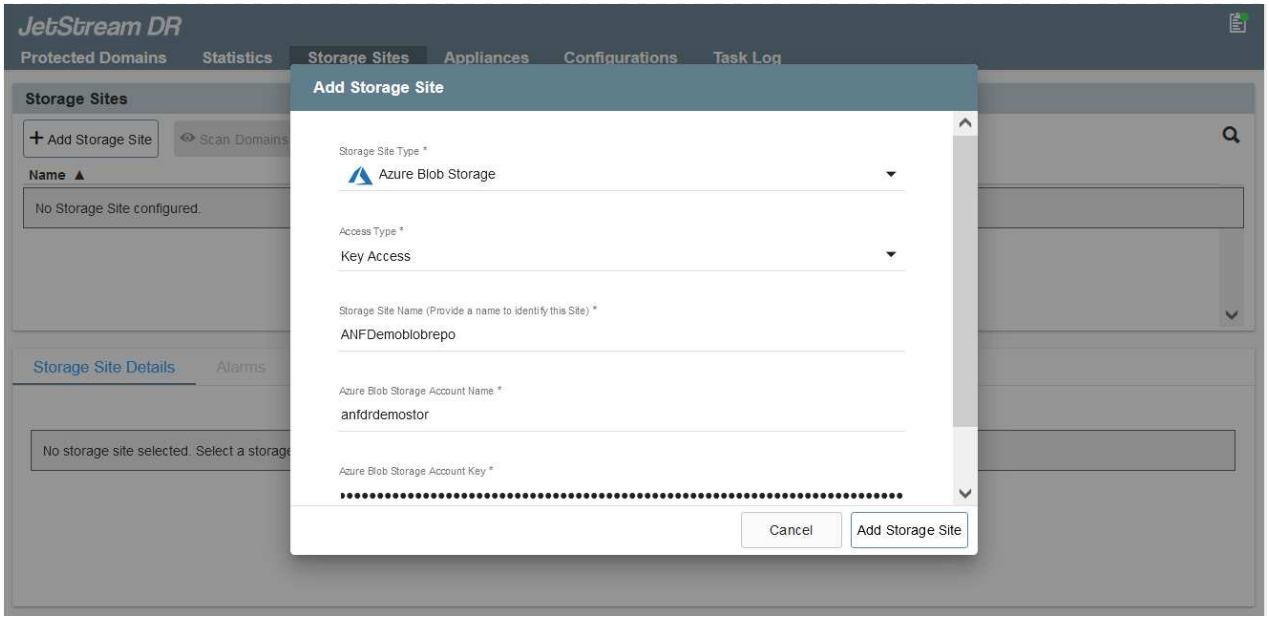
1. 檢查先決條件。
2. 執行容量規劃工具以取得資源和組態建議（可選、但建議用於概念驗證試用）。
3. 將Jetstream DR MSA部署至指定叢集內的vSphere主機。
4. 在瀏覽器中使用其DNS名稱啟動MSA。
5. 向MSA登錄vCenter伺服器。若要執行安裝、請完成下列詳細步驟：
6. 部署了Jetstream DR MSA並註冊vCenter Server之後、請使用vSphere Web Client存取Jetstream DR外掛程式。您可以瀏覽至「資料中心」>「設定」>「Jetstream DR」來完成此作業。



7. 在Jetstream DR介面中、選取適當的叢集。



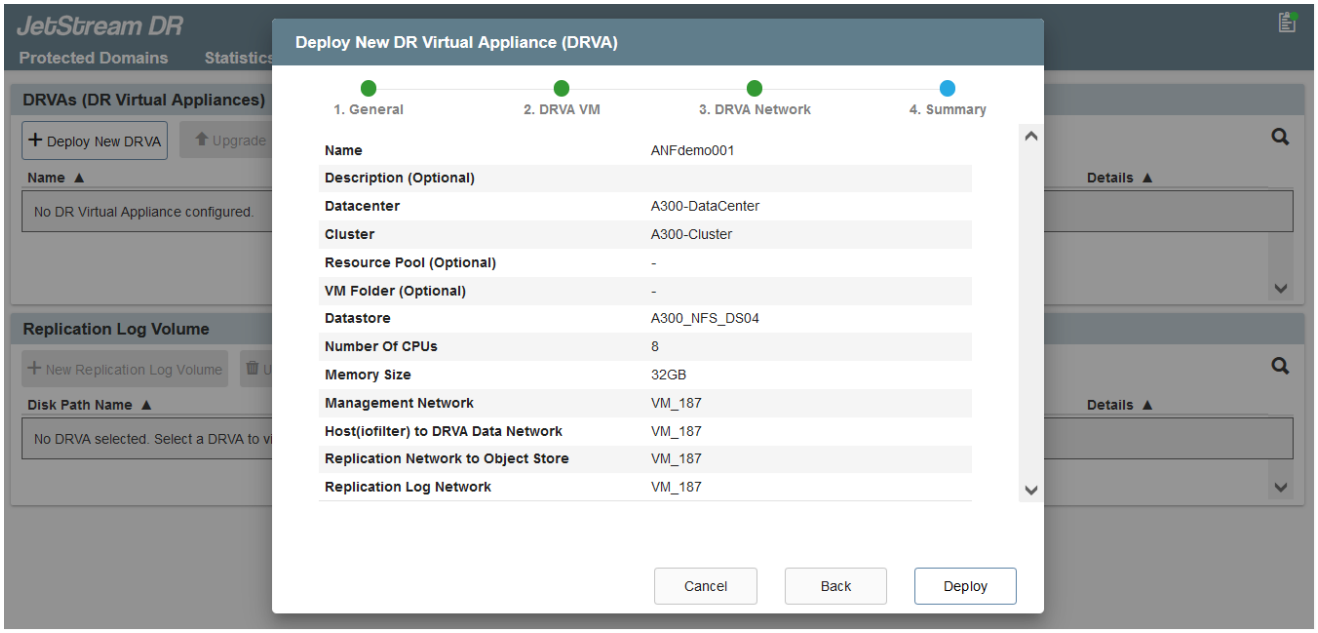
8. 使用I/O篩選套件設定叢集。



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

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

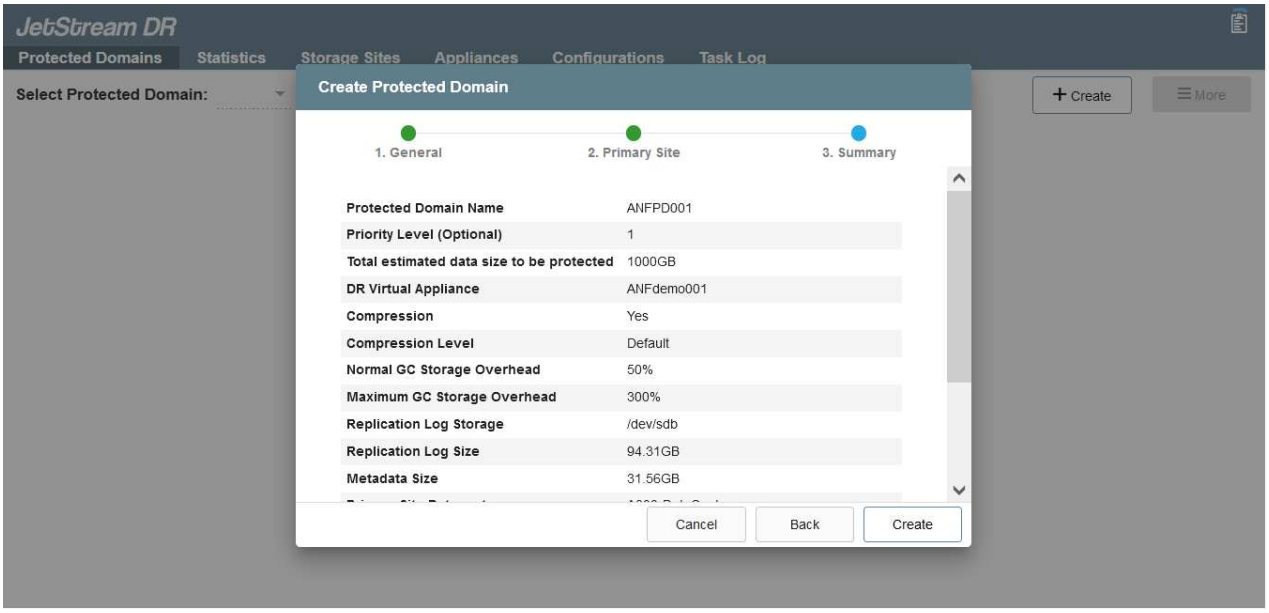
Jetstream DRVA是一種虛擬應用裝置、有助於在資料複寫程序中發揮關鍵功能。受保護的叢集必須至少包含一個DRVA、而且每個主機通常會設定一個DRVA。每個DRVA都能管理多個受保護的網域。



在此範例中、我們為80部虛擬機器建立了四部DRVA。

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

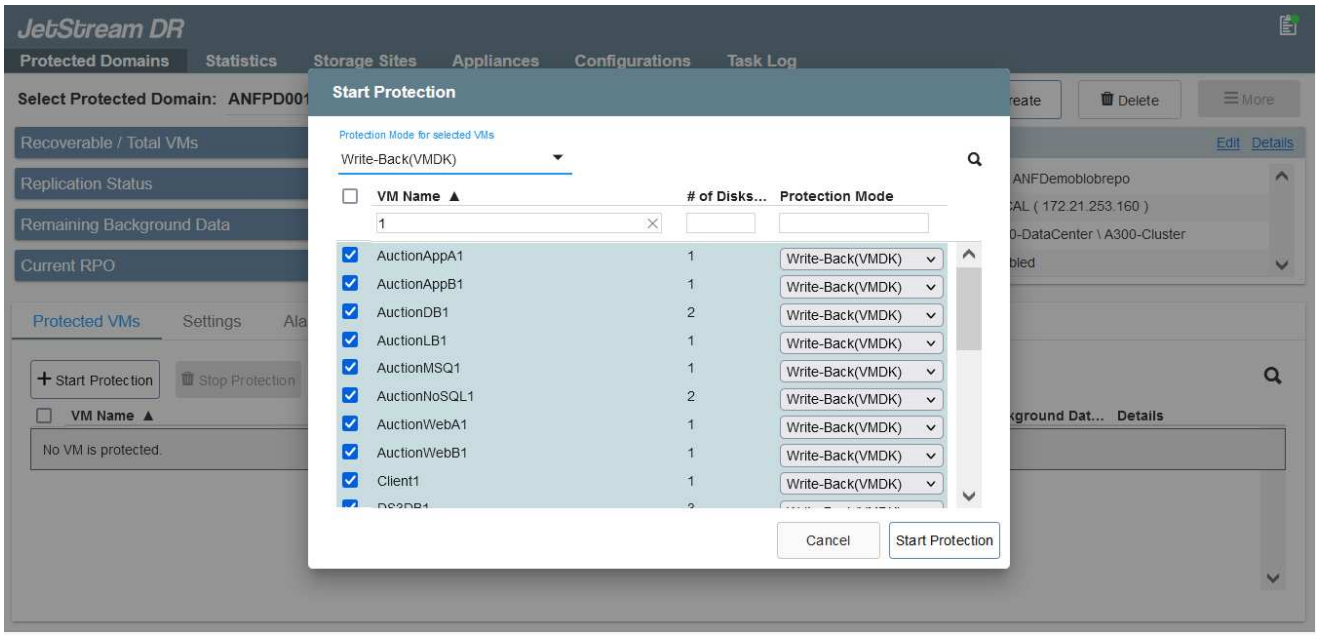
並指派容錯移轉/容錯回復作業的優先順序。



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

確認受保護網域中的所有VM都使用相同的保護模式。

回寫（VMDK）模式可提供更高的效能。



驗證複寫記錄磁碟區是否放置在高效能儲存設備上。

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

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

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

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

應在AVS叢集上設定網路組態（包括區段建立）、以符合內部部署需求。

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

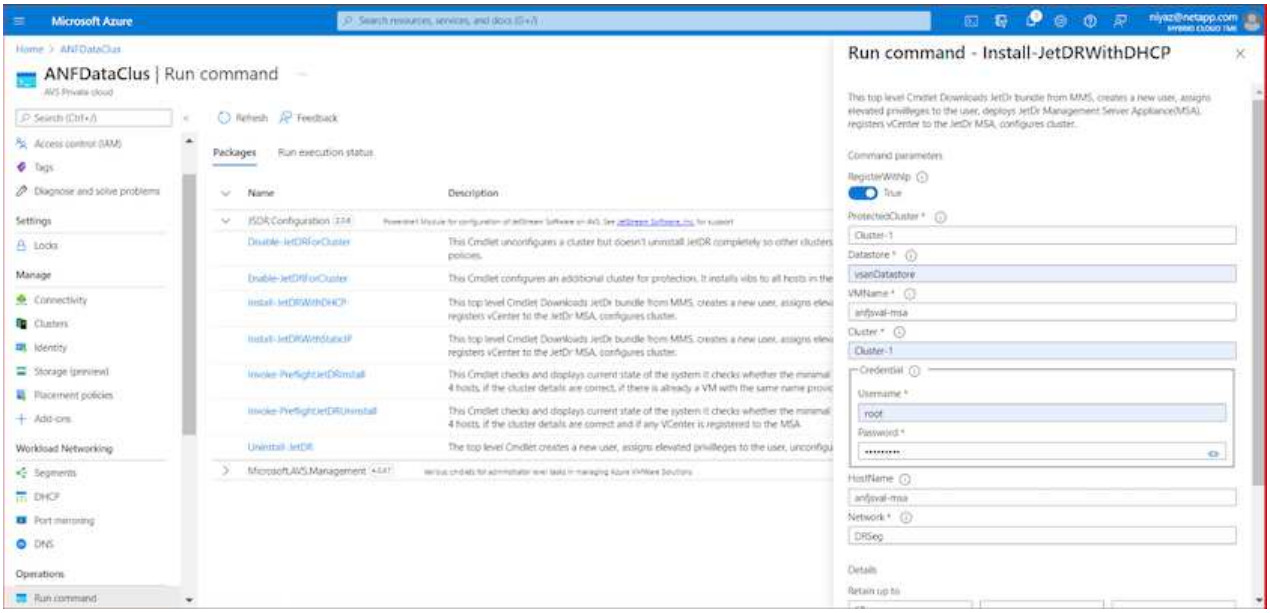
如何在私有雲中安裝**AVS**的**Jetstream DR**

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

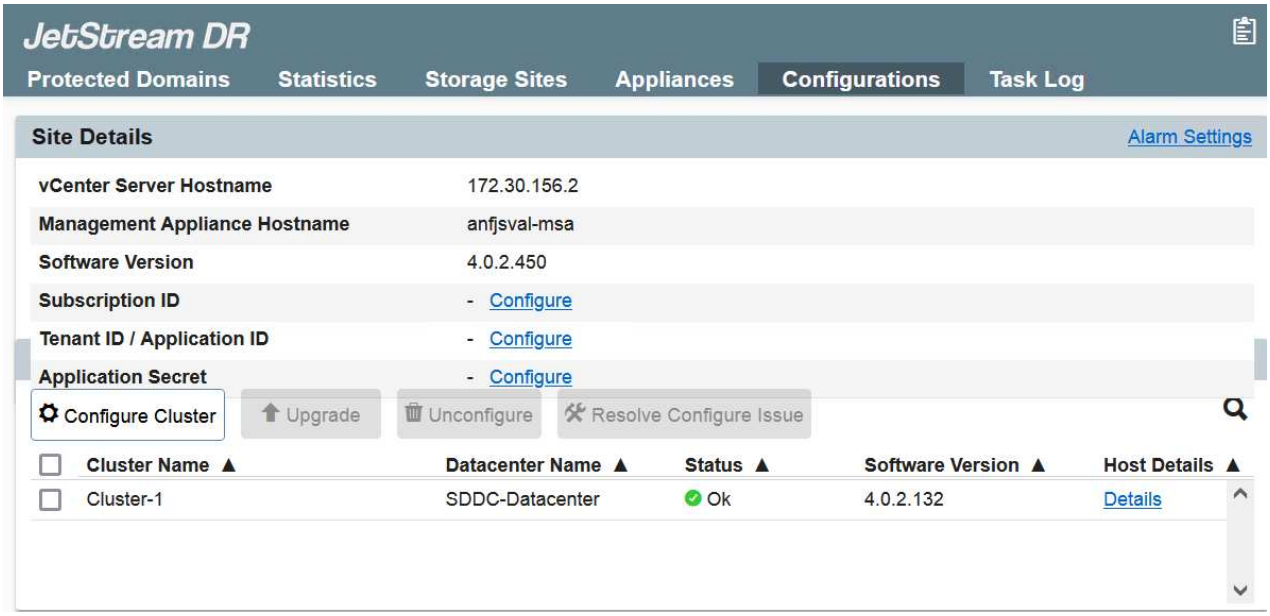
1. 從Azure入口網站移至Azure VMware解決方案、選取私有雲、然後選取執行命令>套件> JSDR.Configuration。

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

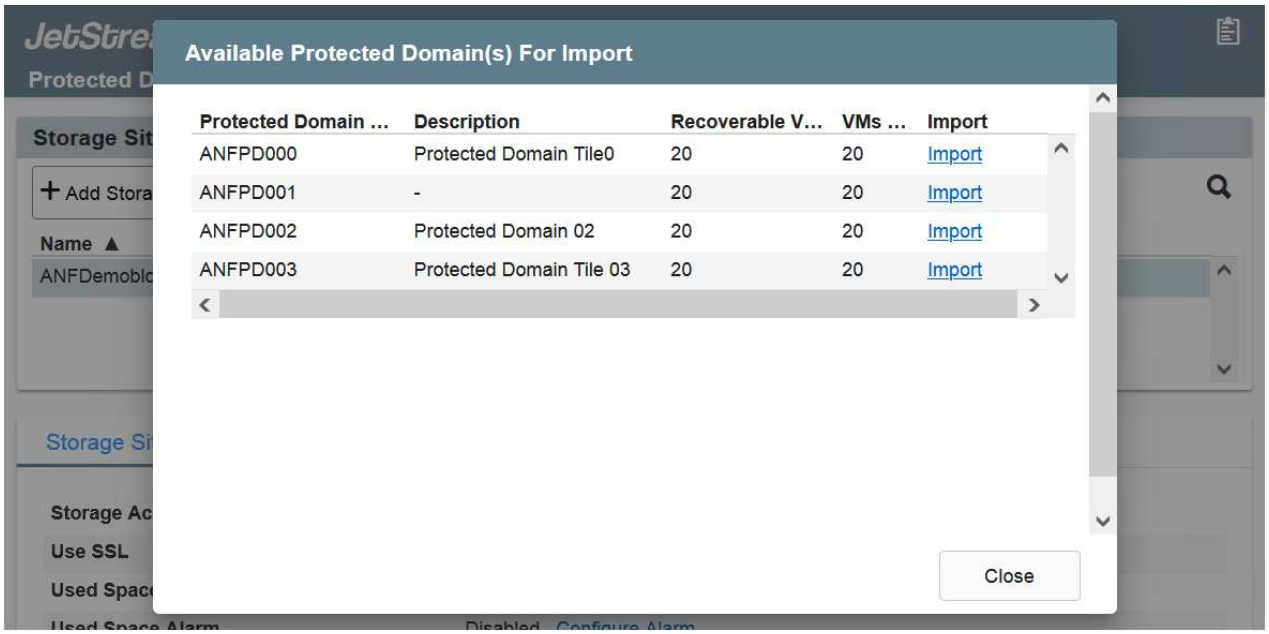
下列螢幕快照顯示使用DHCP型IP位址進行安裝。



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



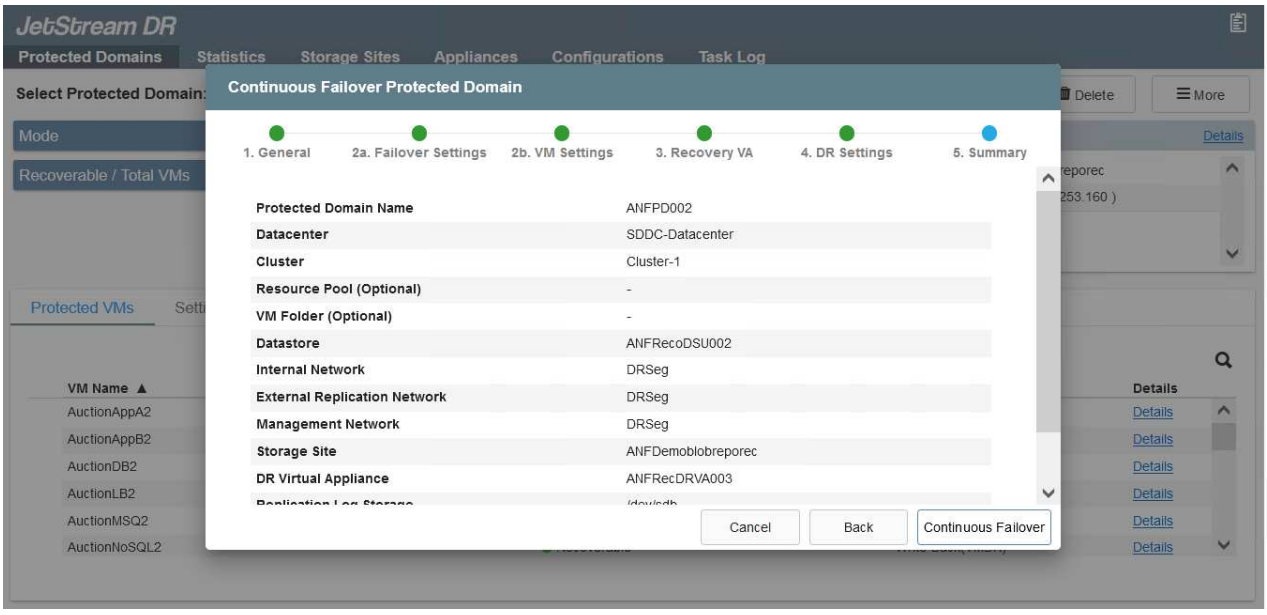
3. 從Jetstream DR介面新增Azure Blob Storage帳戶、以保護內部部署叢集做為儲存站台、然後執行「掃描網域」選項。



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

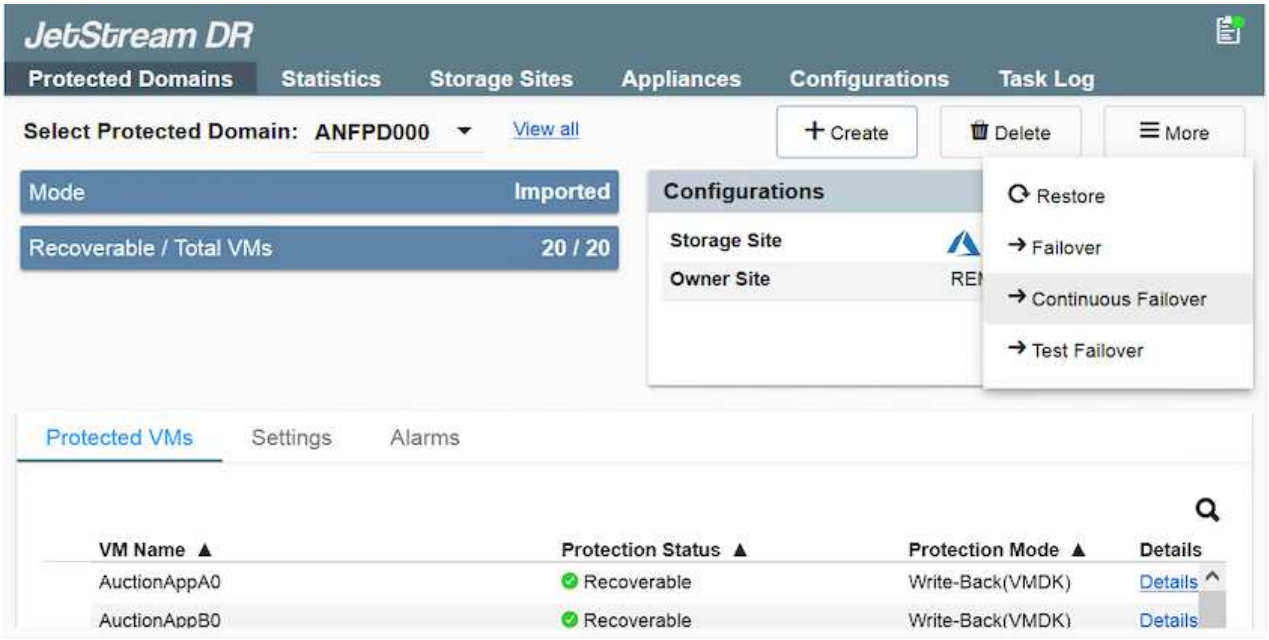
> 您也可以使用已建立的CPT計畫來自動化這些步驟。

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



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

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



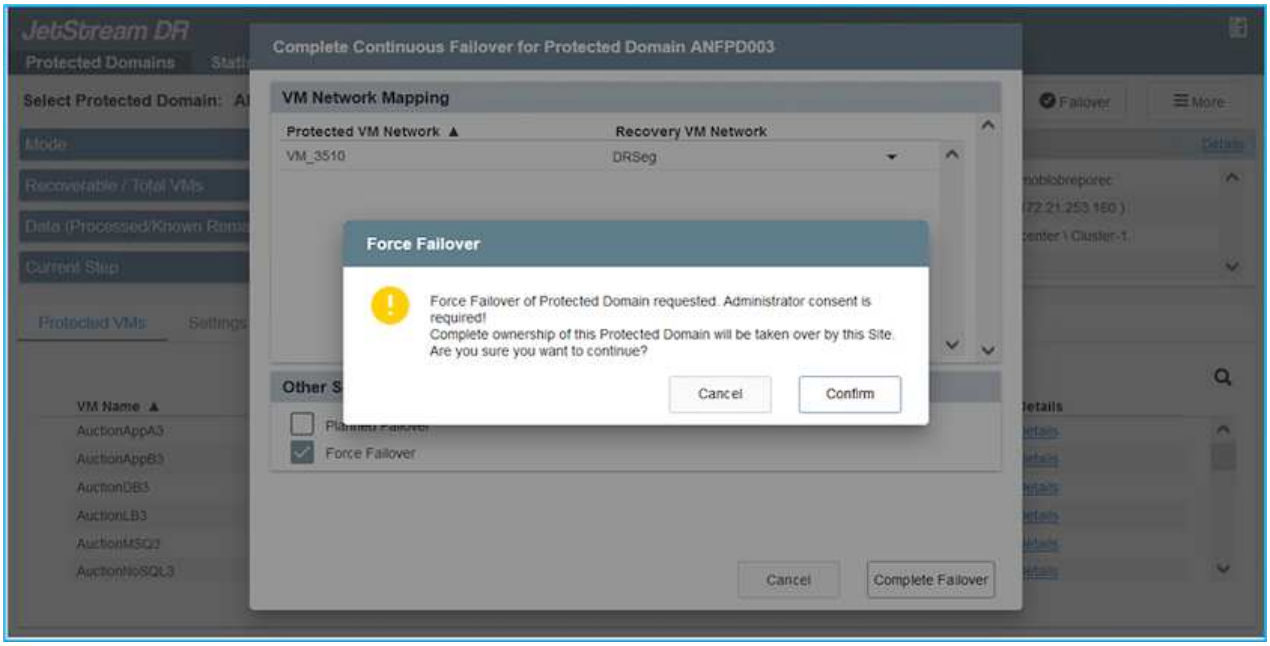
執行容錯移轉/容錯回復

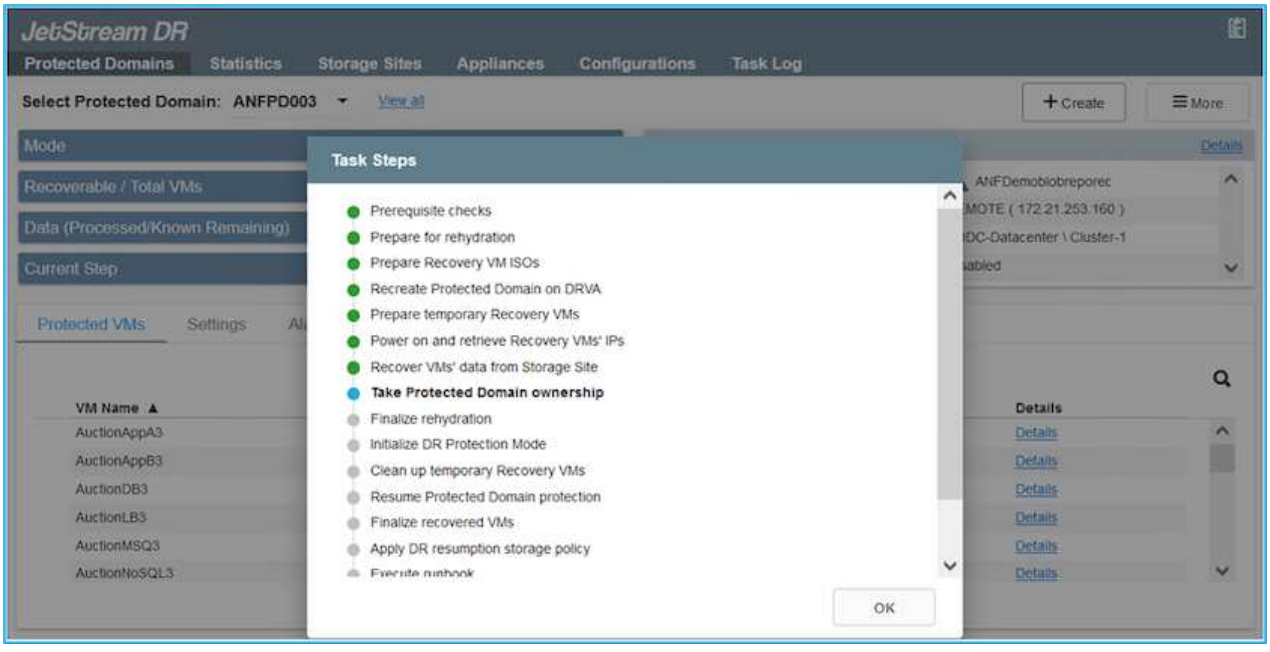
如何執行容錯移轉/容錯回復

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

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

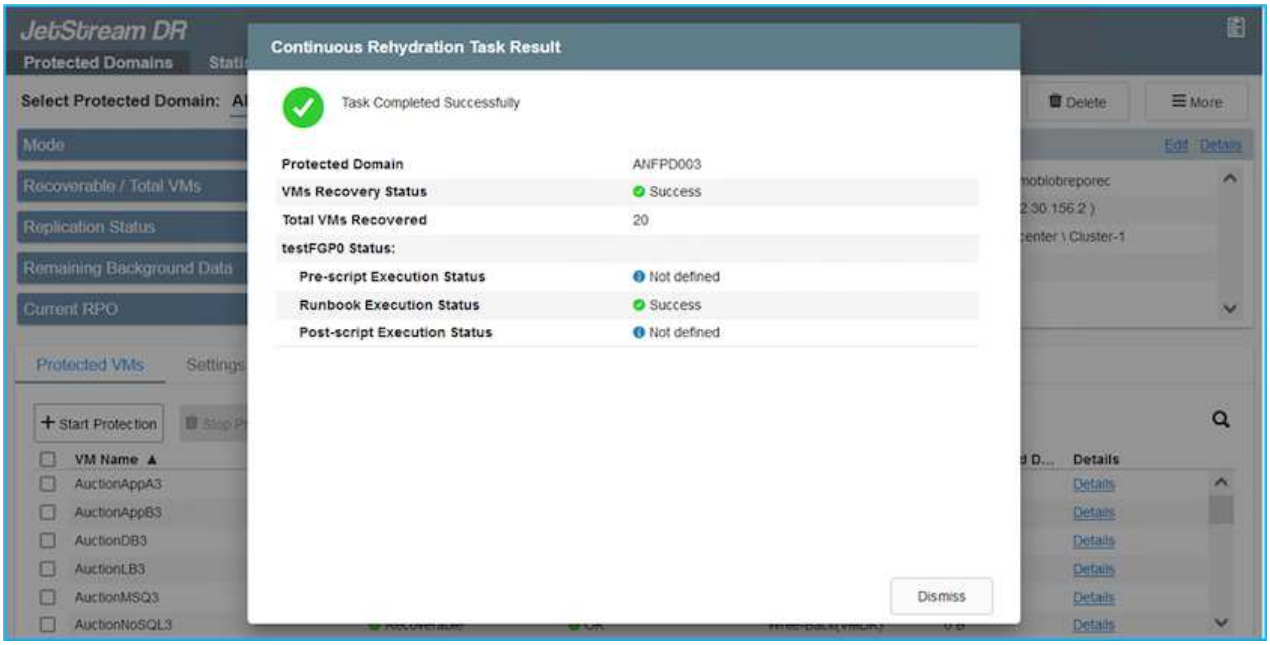
   在AVS中啟動受保護的VM後、容錯移轉（持續或標準還原）會自動恢復保護、而在Azure Blob Storage中、則會繼續將資料複寫到適當/原始的容器中。





   工作列會顯示容錯移轉活動的進度。

2. 當工作完成時、存取恢復的VM並維持正常營運。

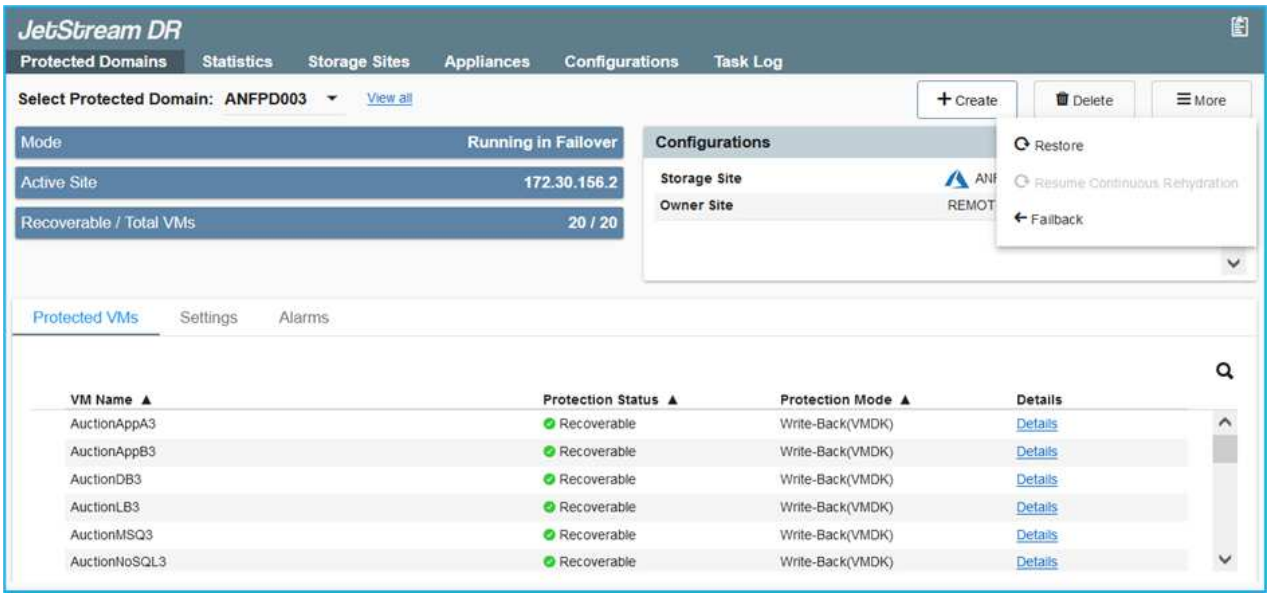


在主站台啟動並再次執行之後、即可執行容錯回復。恢復VM保護、並檢查資料一致性。

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

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

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



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

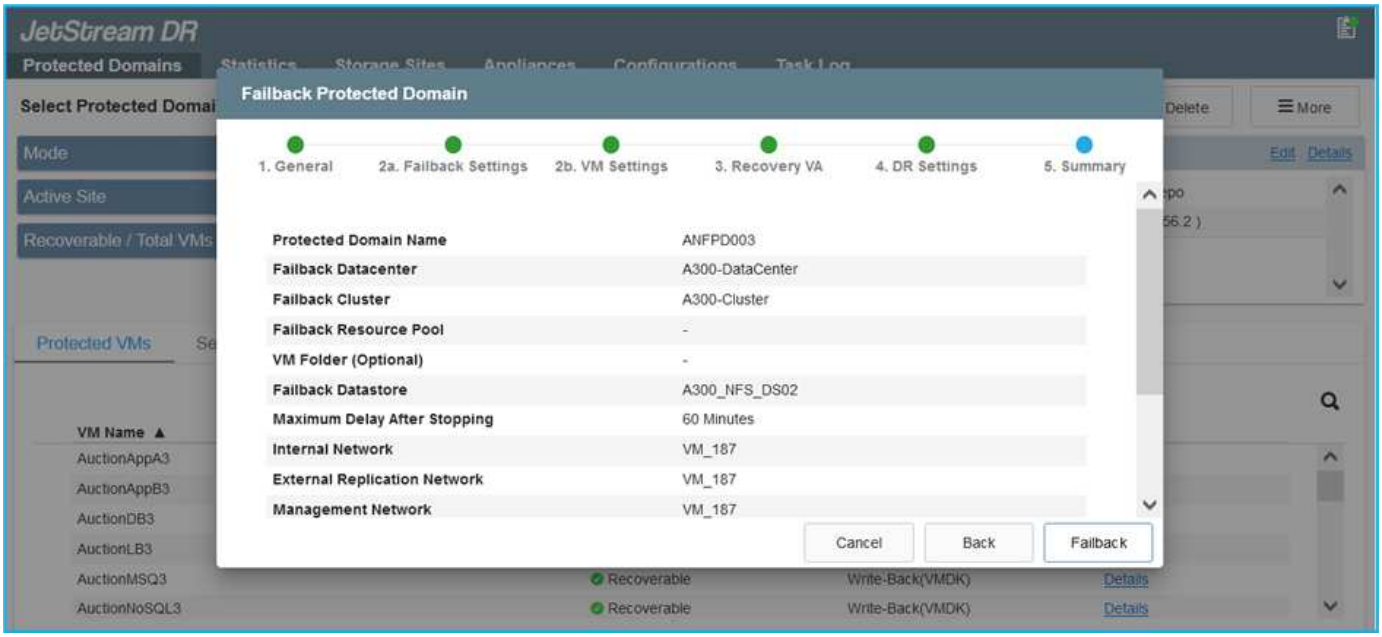
指定在恢復站台暫停VM並在受保護站台重新啟動之後的最大延遲。這次包括在停止容錯移轉虛擬機器之後完成複寫、清理恢復站台的時間、以及在受保護站台重新建立虛擬機器的時間。NetApp建議的值為10分鐘。

完成容錯回復程序、然後確認恢復VM保護和資料一致性。

Ransomware恢復

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

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



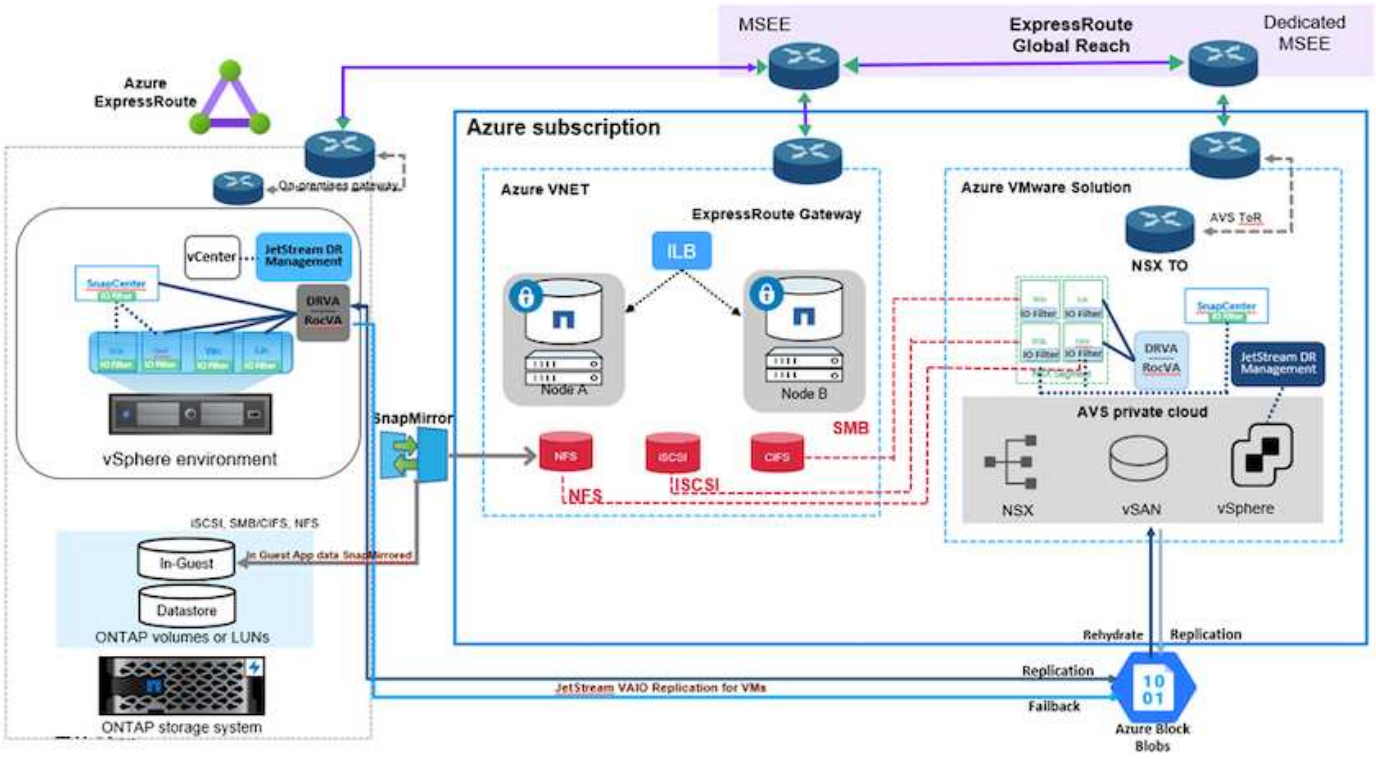
使用**CVO**和**AVS**（與來賓連線的儲存設備）進行災難恢復

總覽

作者：Ravi BCB和Niyazz Mohamed, NetApp

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

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



假設

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

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

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

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

部署災難恢復解決方案

解決方案部署總覽

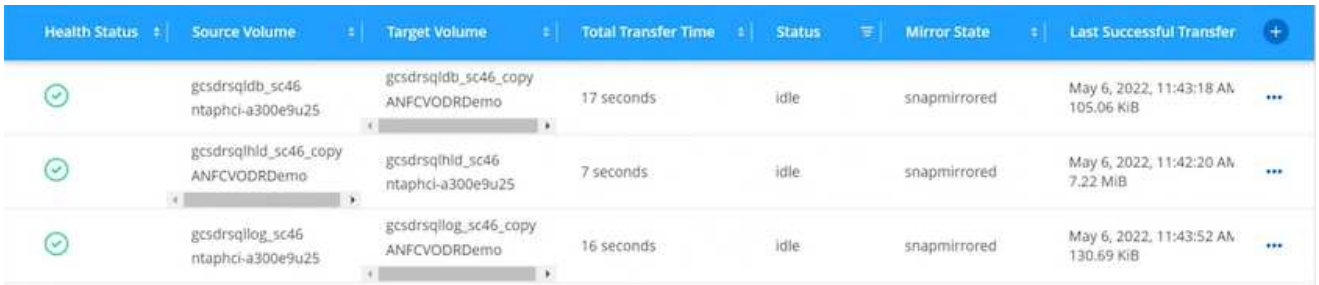
1. 確保應用程式資料是以SnapCenter 不必要的RPO要求使用支援功能進行備份。
2. 在Cloud Volumes ONTAP 適當的訂購和虛擬網路中使用Cloud Manager、以正確的執行個體大小進行配置。
   a. 為相關的應用程式磁碟區設定SnapMirror。
   b. 更新SnapCenter 中的備份原則、以便在排程工作之後觸發SnapMirror更新。
3. 在內部部署資料中心安裝Jetstream DR軟體、並開始保護虛擬機器。
4. 在Azure VMware解決方案私有雲中安裝Jetstream DR軟體。

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

部署詳細資料

在**Azure**上設定**CVO**、並將磁碟區複寫至**CVO**

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



設定**AVS**主機和**CVO**資料存取

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

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

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

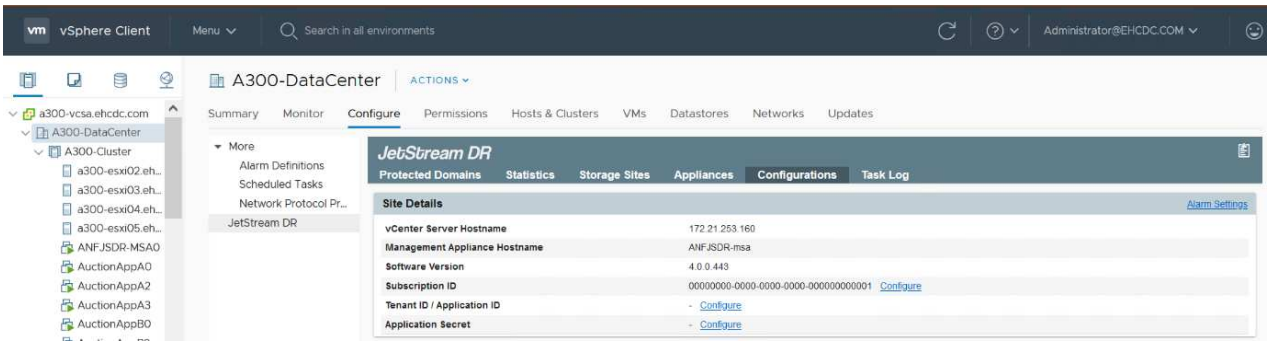
若要設定AVS SDDC（無論是隨需或是以指示燈模式）、請參閱 "在Azure上部署及設定虛擬化環境"。先決條件是確認位於AVS主機上的客體VM能夠在Cloud Volumes ONTAP 建立連線之後、從支援中心使用資料。

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

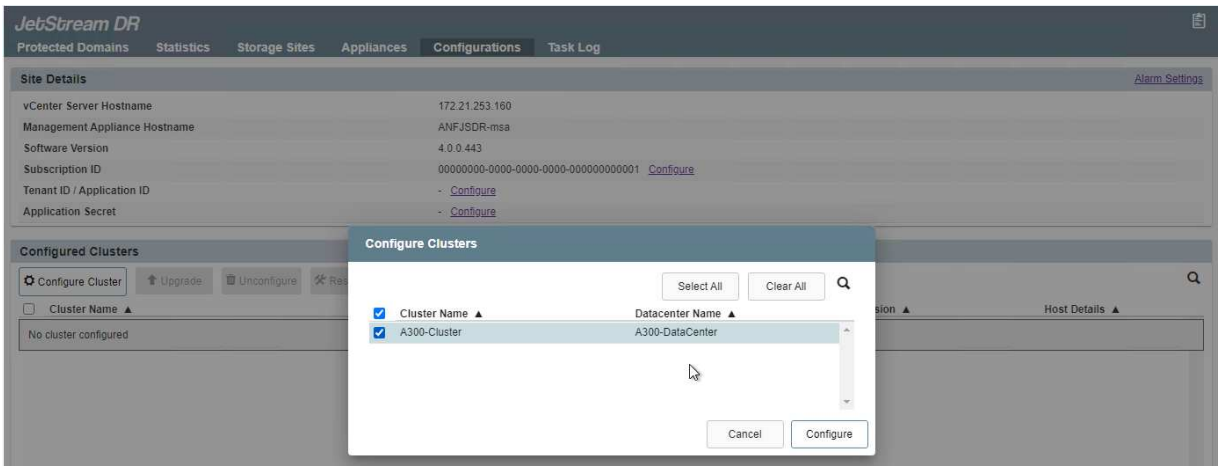
在內部部署資料中心安裝**Jetstream DR**

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

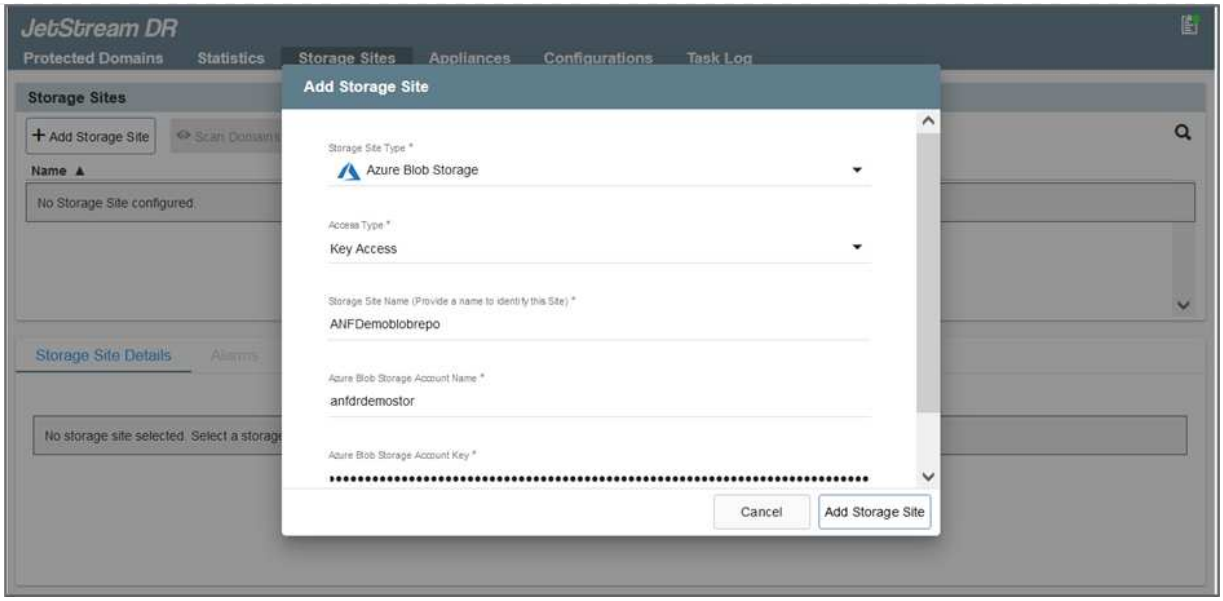
1. 檢查先決條件。
2. 執行容量規劃工具以取得資源和組態建議。
3. 將Jetstream DR MSA部署至指定叢集中的每個vSphere主機。
4. 在瀏覽器中使用其DNS名稱啟動MSA。
5. 向MSA登錄vCenter伺服器。
6. 部署了Jetstream DR MSA並註冊vCenter Server之後、請使用vSphere Web Client瀏覽至Jetstream DR外掛程式。您可以瀏覽至「資料中心」>「設定」>「Jetstream DR」來完成此作業。



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

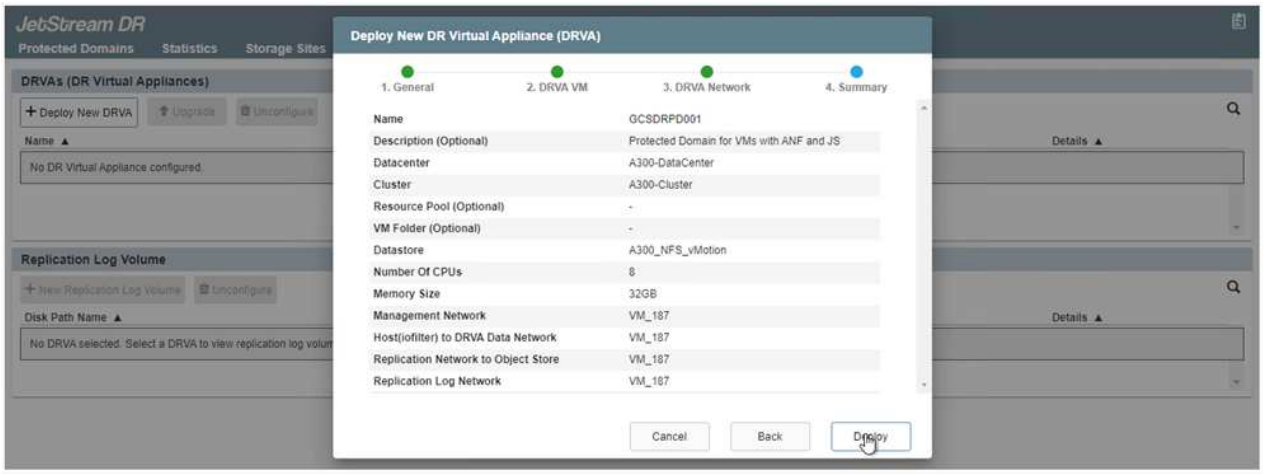


   b. 新增位於恢復站台的Azure Blob儲存設備。

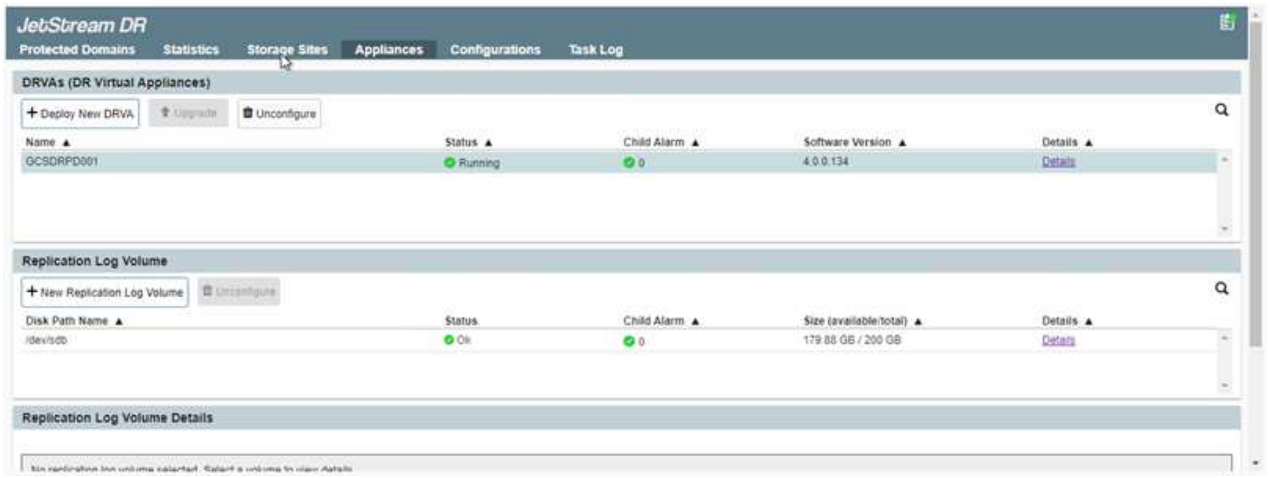


8. 從「應用裝置」索引標籤部署所需數量的DR虛擬應用裝置（DRVA）。

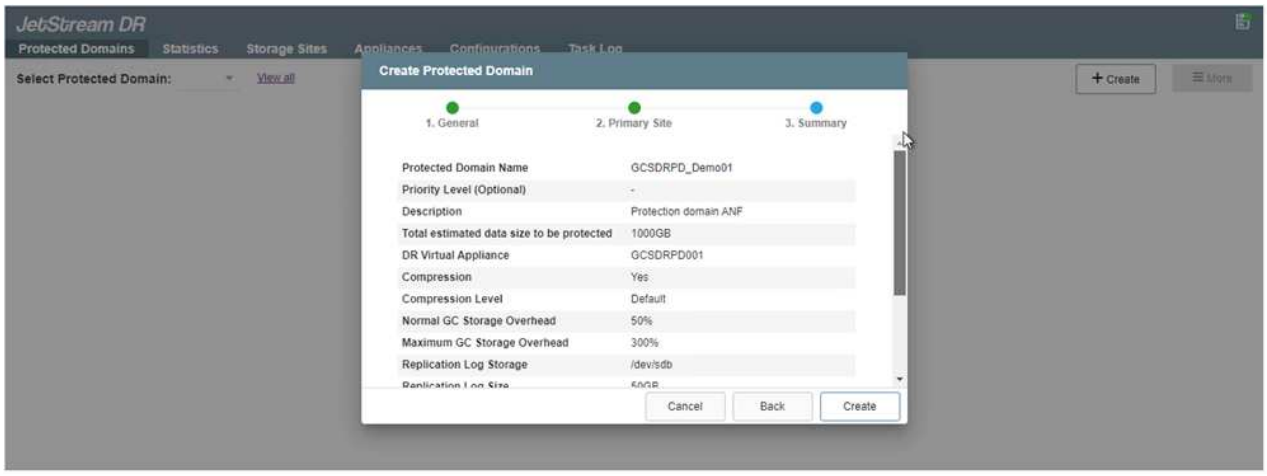
   使用容量規劃工具來預估所需的DRVA數量。

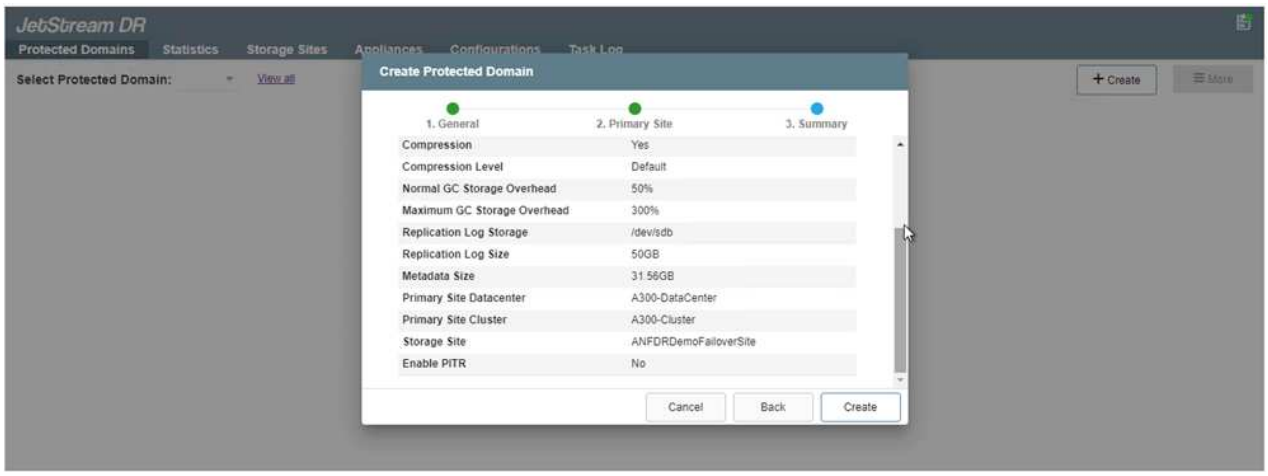


9. 使用可用的資料存放區或獨立的共享iSCSI儲存池中的VMDK、為每個DRVA建立複寫記錄磁碟區。



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

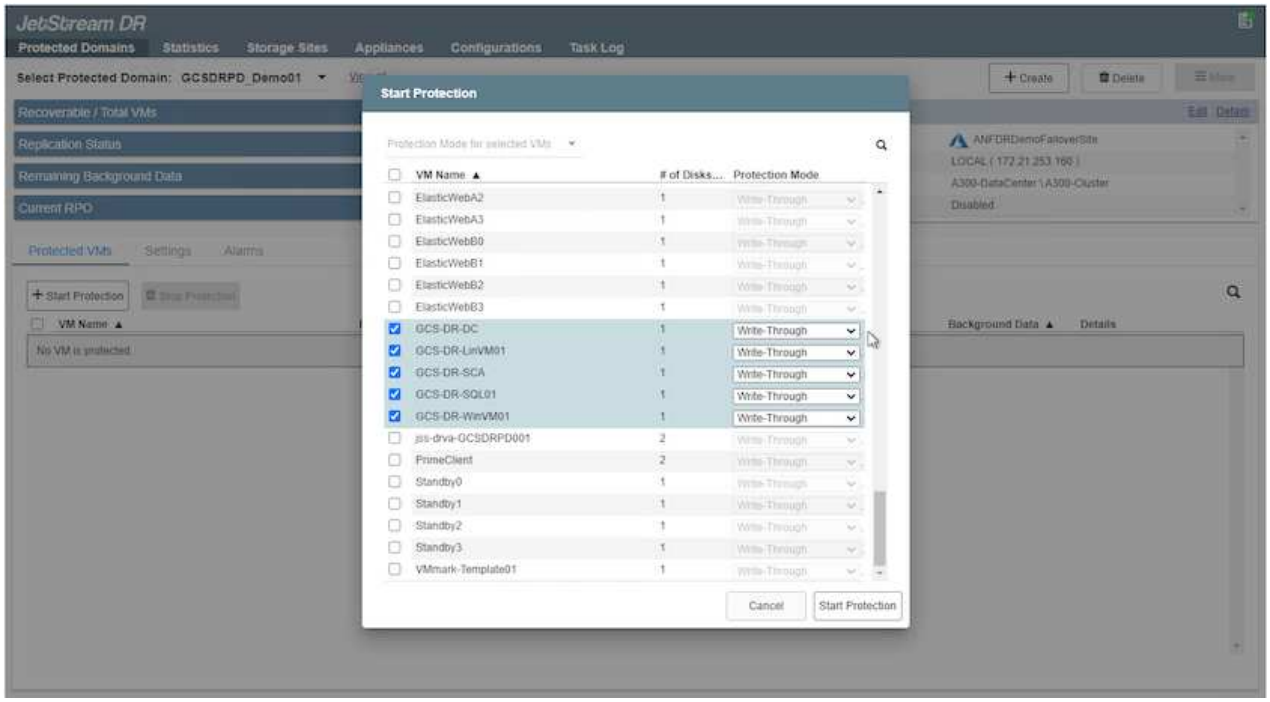




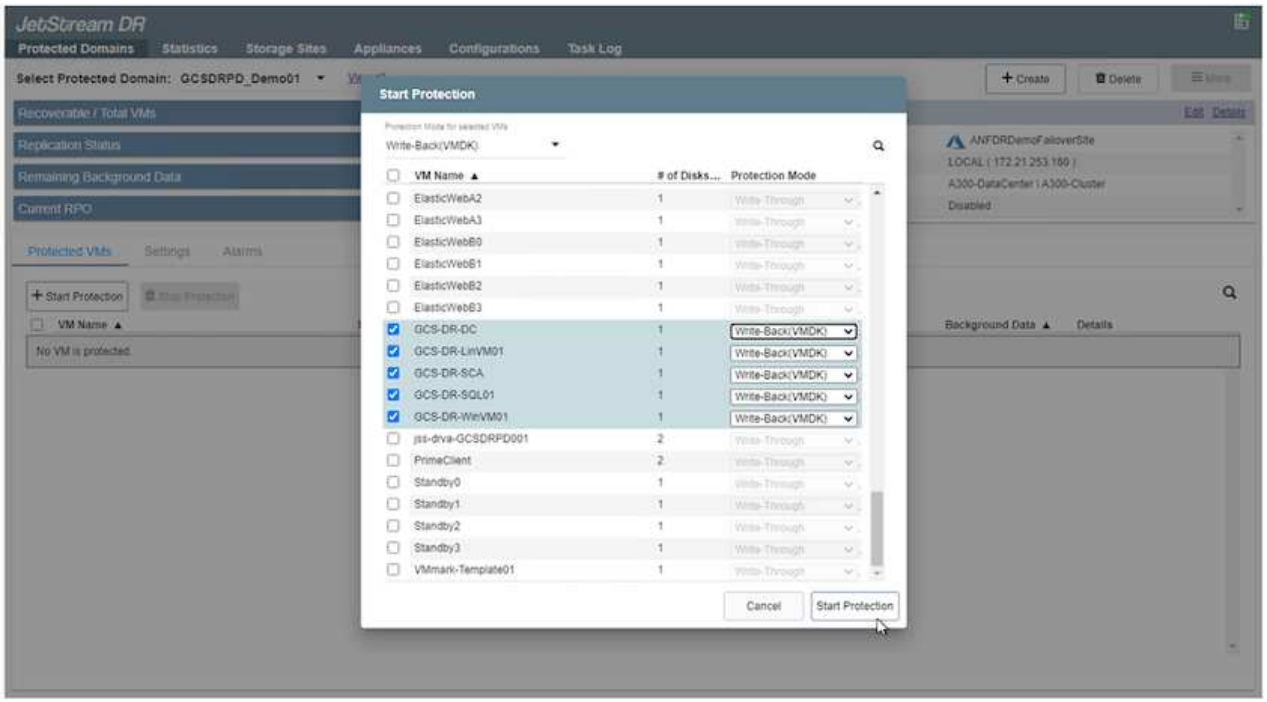
11. 選取要保護的VM、並根據相依性將VM分組為應用程式群組。應用程式定義可讓您將一組VM分組為邏輯群組、其中包含開機順序、開機延遲、以及可在恢復時執行的選用應用程式驗證。

請確定保護網域中的所有VM都使用相同的保護模式。

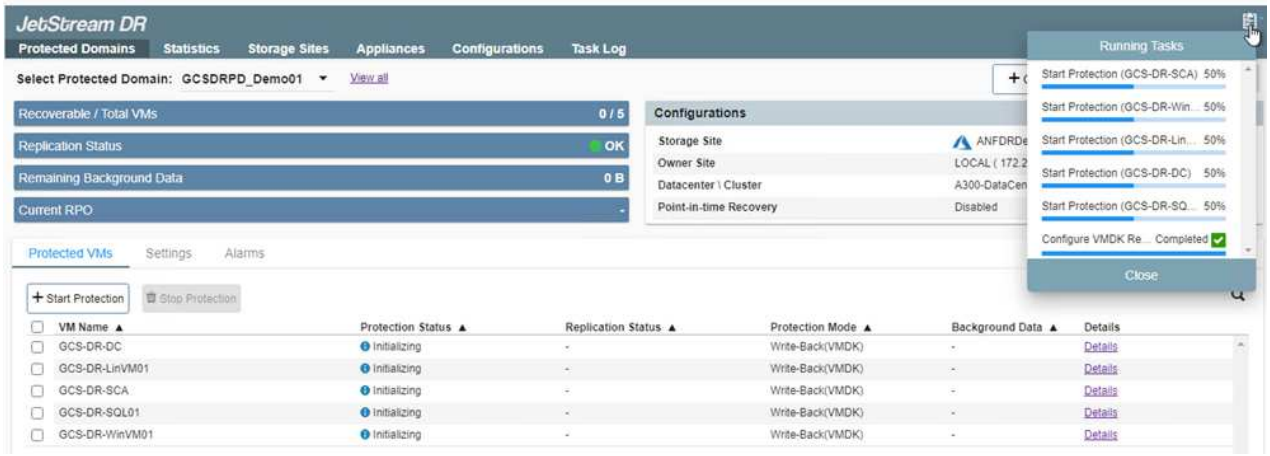
回寫（VMDK）模式可提供更高的效能。



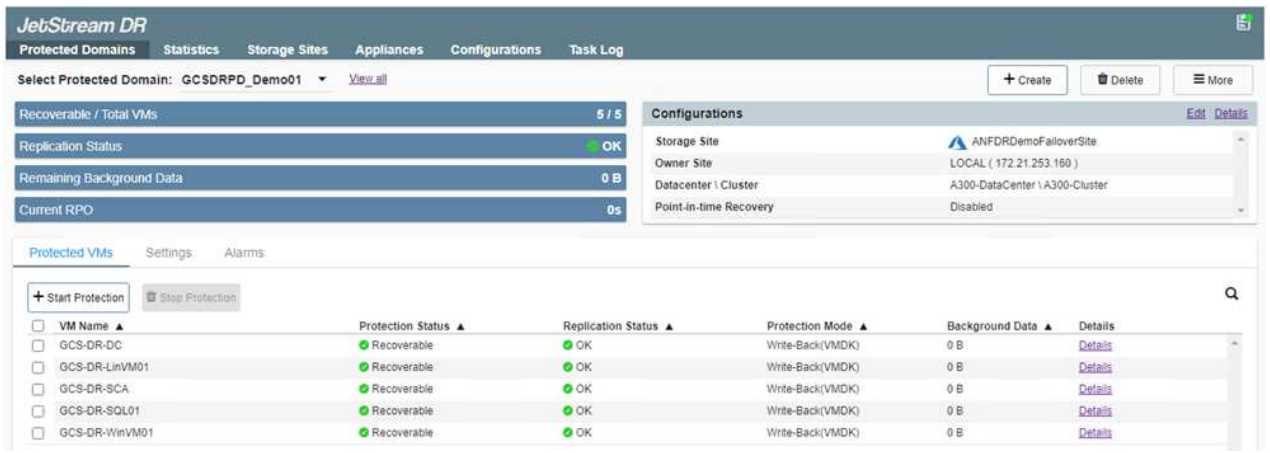
12. 請確定複寫記錄磁碟區放置在高效能儲存設備上。



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



14. 複寫完成後、VM保護狀態會標示為可恢復。

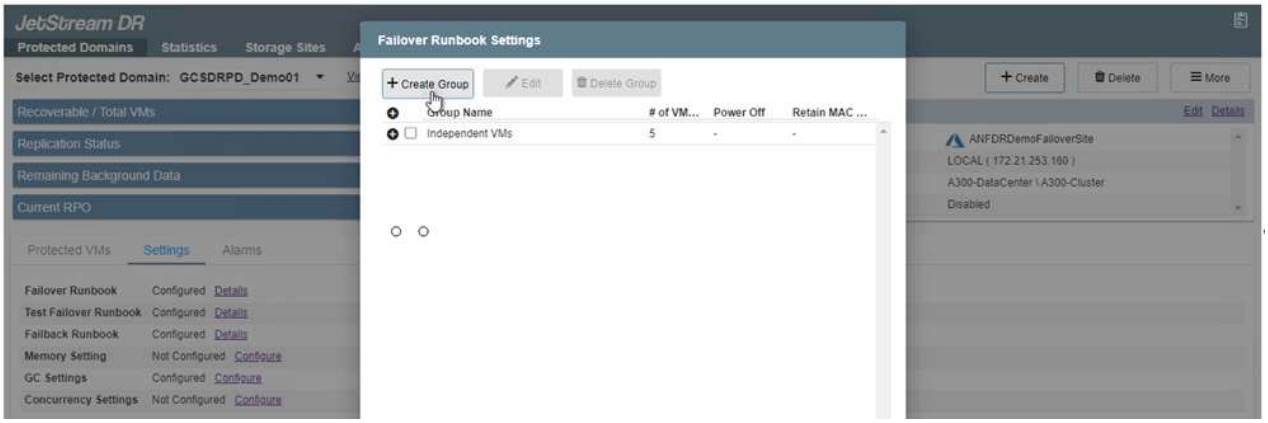


容錯移轉Runbook可設定為群組VM（稱為恢復群組）、設定開機順序、以及修改CPU / 記憶體設定和IP組態。

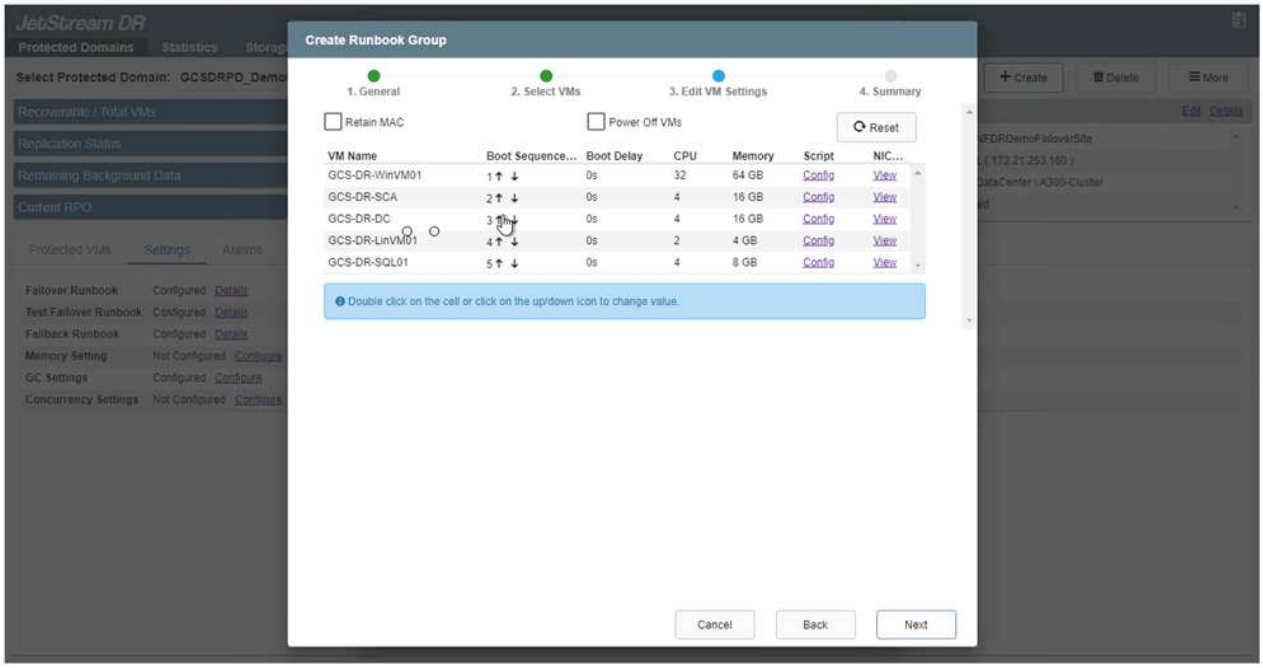
15. 按一下「設定」、然後按一下Runbook「設定」連結以設定Runbook群組。

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

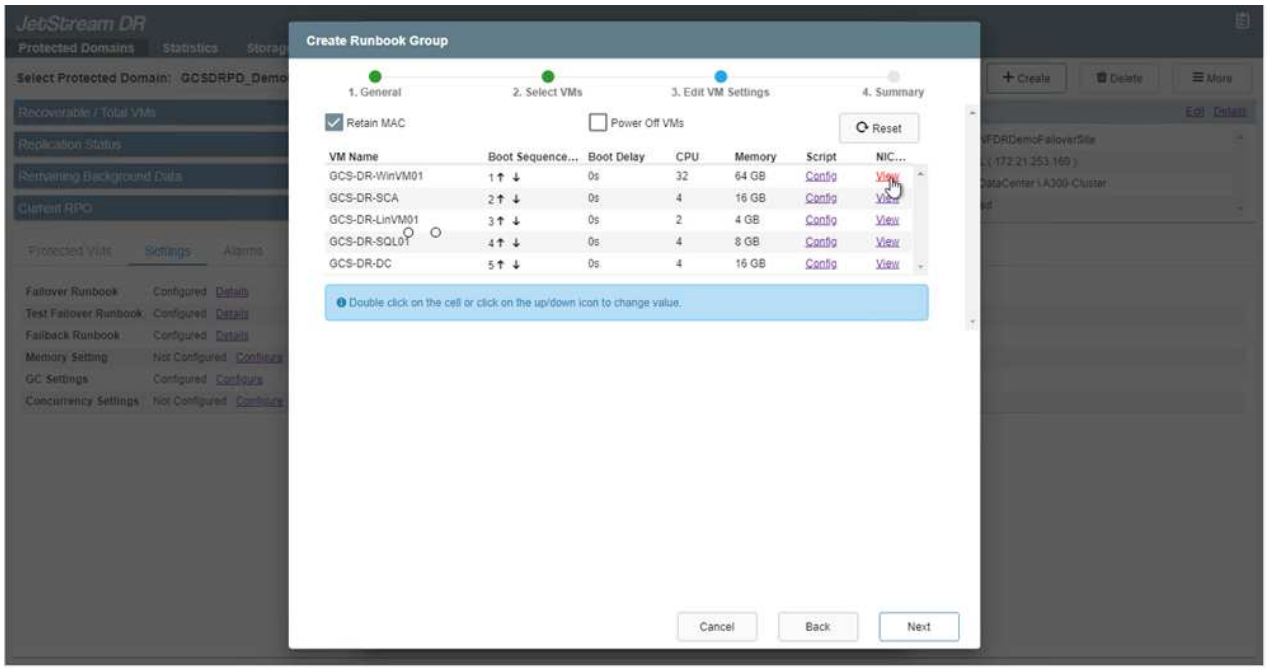
如有需要、請在畫面下方套用自訂的預先指令碼和後置指令碼、以便在執行手冊群組作業之前和之後自動執行。確定Runbook指令碼位於管理伺服器上。



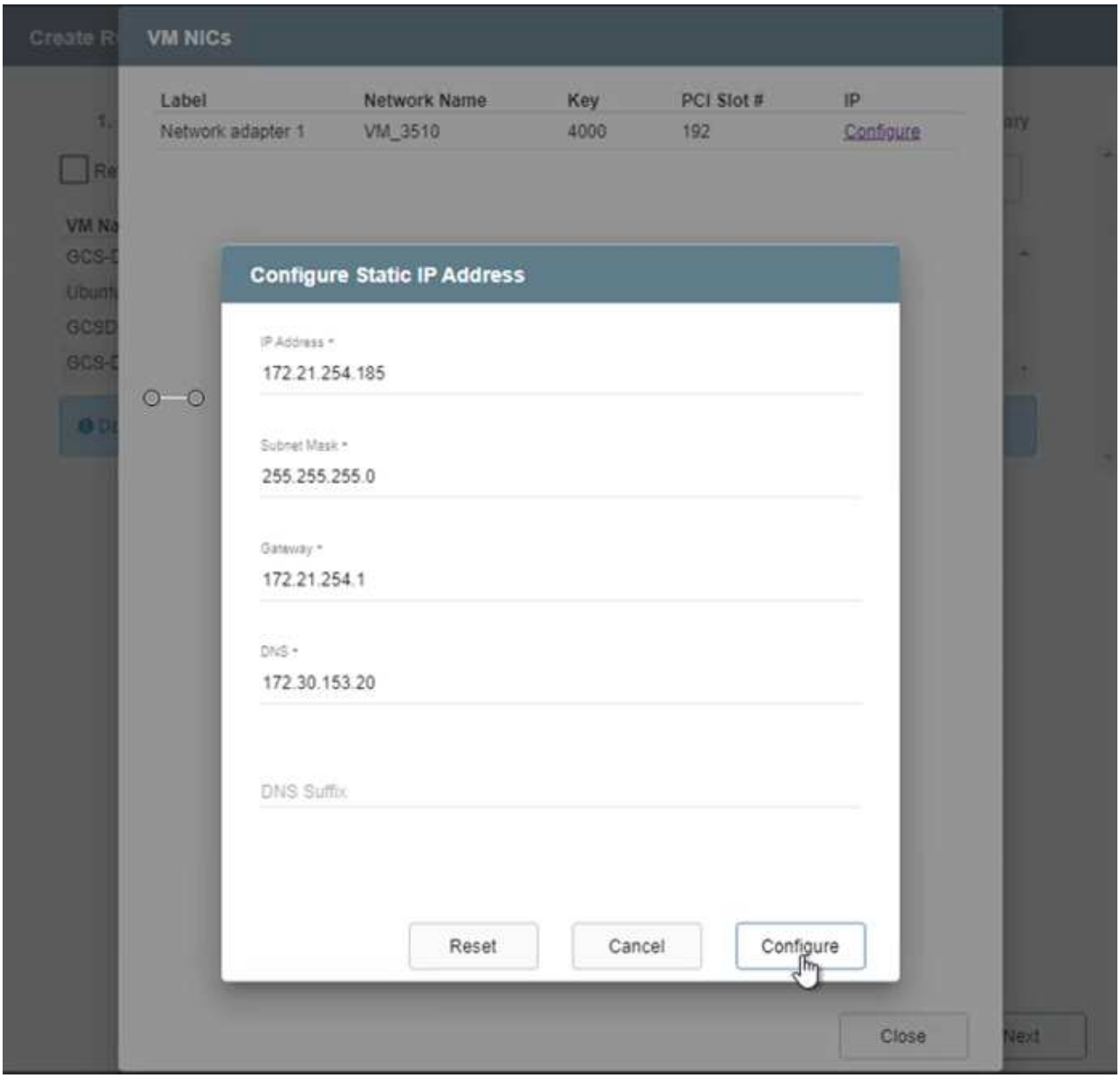
17. 視需要編輯VM設定。指定用於恢復VM的參數、包括開機順序、開機延遲（以秒為單位）、CPU數量、以及要分配的記憶體容量。按一下向上或向下箭頭、變更VM的開機順序。也提供了用於保留MAC的選項。

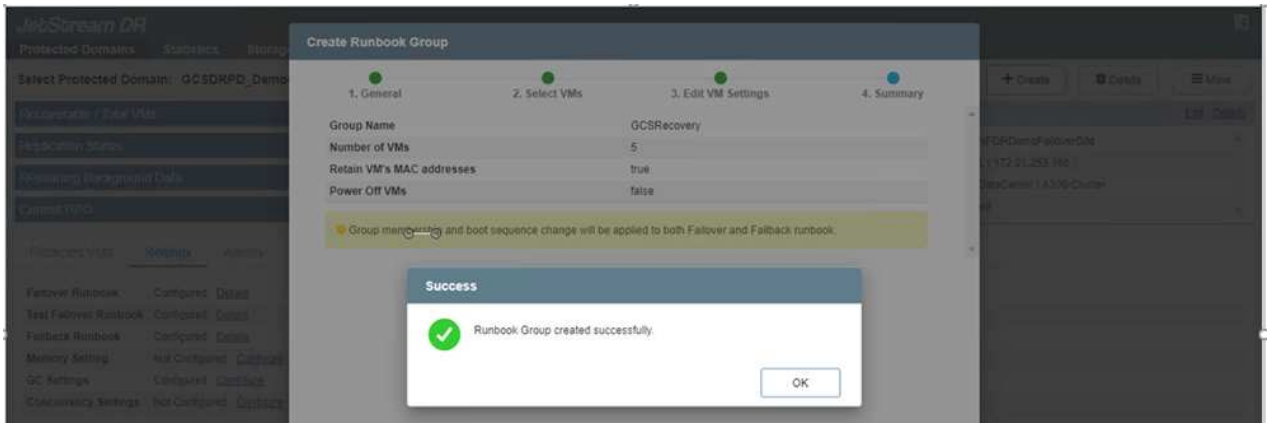


18. 靜態IP位址可針對群組中的個別VM手動設定。按一下VM的NIC View連結、手動設定其IP位址設定。



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





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

在私有雲中安裝**AVS**的**Jetstream DR**

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

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

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

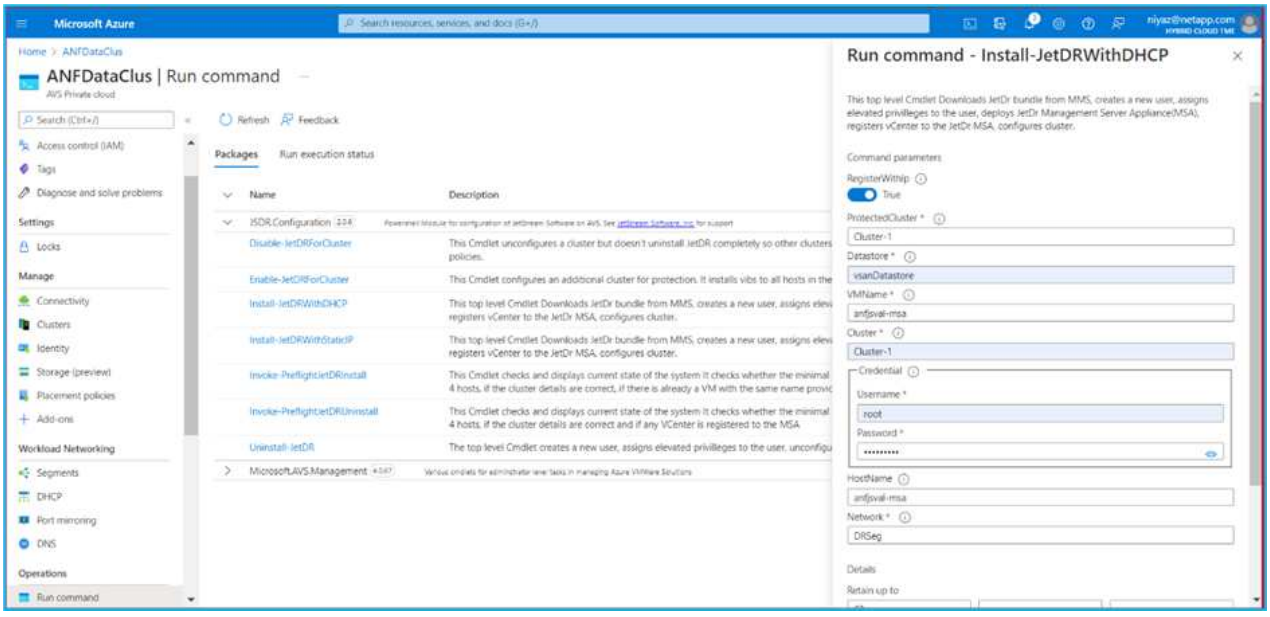
應在AVS叢集上設定網路組態（包括區段建立）、以符合內部部署需求。

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

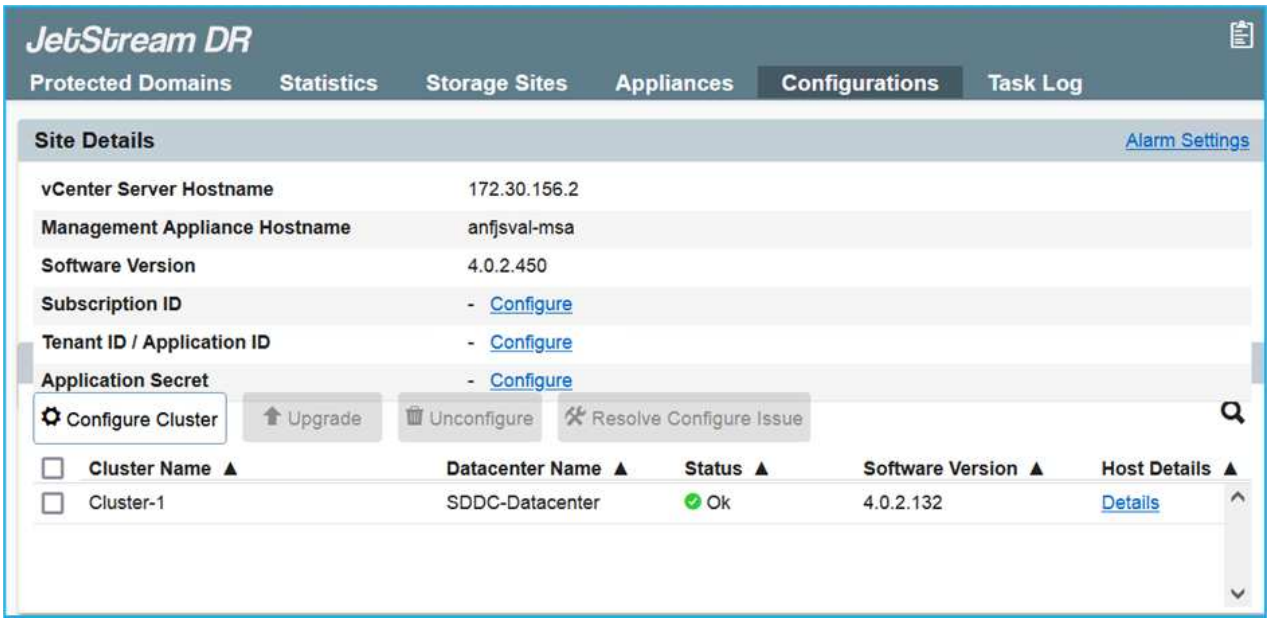
1. 若要在Azure VMware解決方案私有雲上安裝適用於AVS的Jetstream DR、請使用Run命令。從Azure入口網站移至Azure VMware解決方案、選取私有雲、然後選取執行命令>套件> JSDR.Configuration。

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

   下列螢幕快照顯示使用DHCP型IP位址進行安裝。

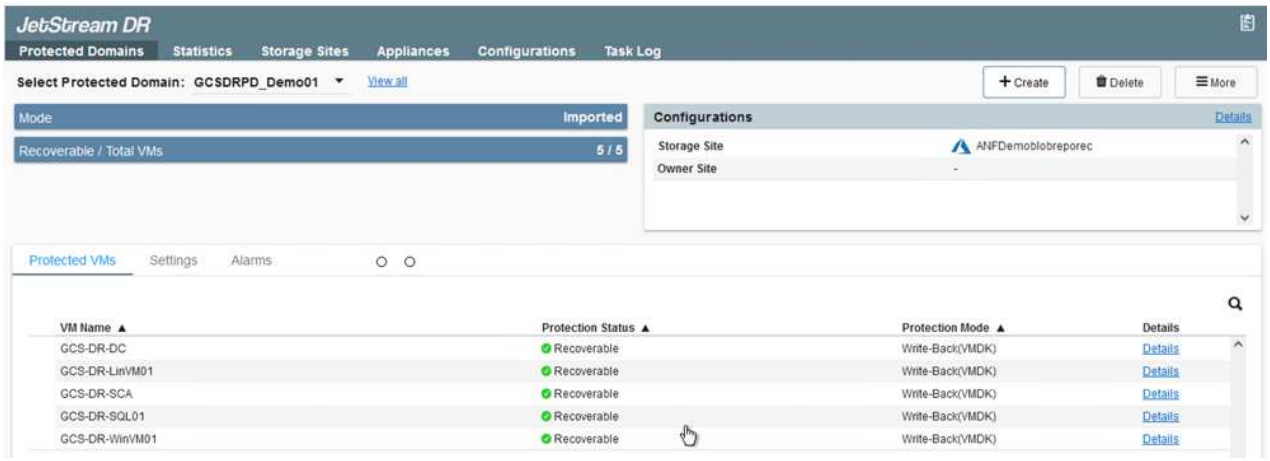


2. 在安裝AVS的Jetstream DR完成後、請重新整理瀏覽器。若要存取Jetstream DR UI、請前往SDDC資料中心>組態> Jetstream DR。



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

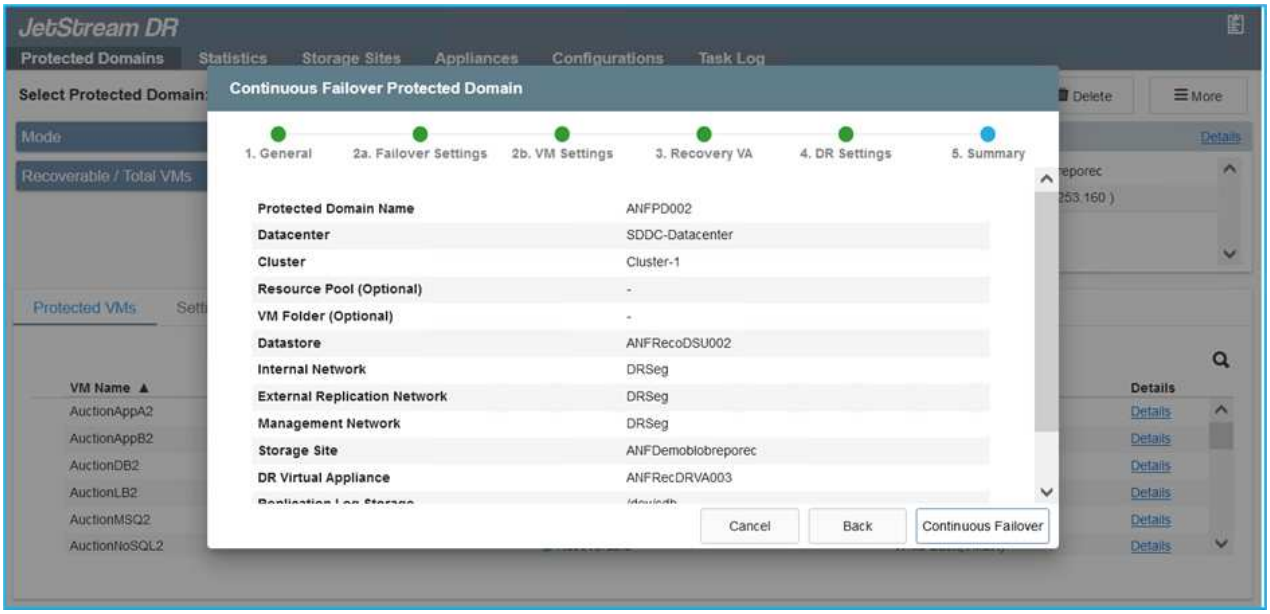
4. 網域已匯入以供還原。移至「受保護的網域」索引標籤、確認已選取所需的網域、或從「選取受保護的網域」功能表中選擇所需的網域。隨即顯示受保護網域中可恢復的VM清單。



5. 匯入受保護的網域之後、請部署DRVA設備。

您也可以使用由CPt建立的計畫來自動化這些步驟。

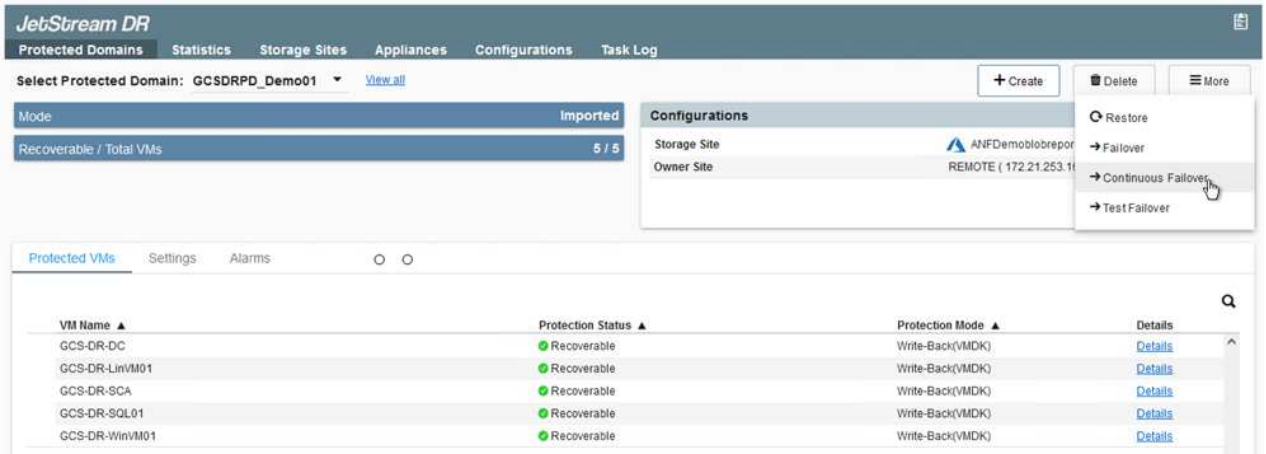
6. 使用可用的vSAN或ANF資料存放區建立複寫記錄磁碟區。
7. 匯入受保護的網域、並將恢復VA設定為使用ANF資料存放區來放置VM。



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

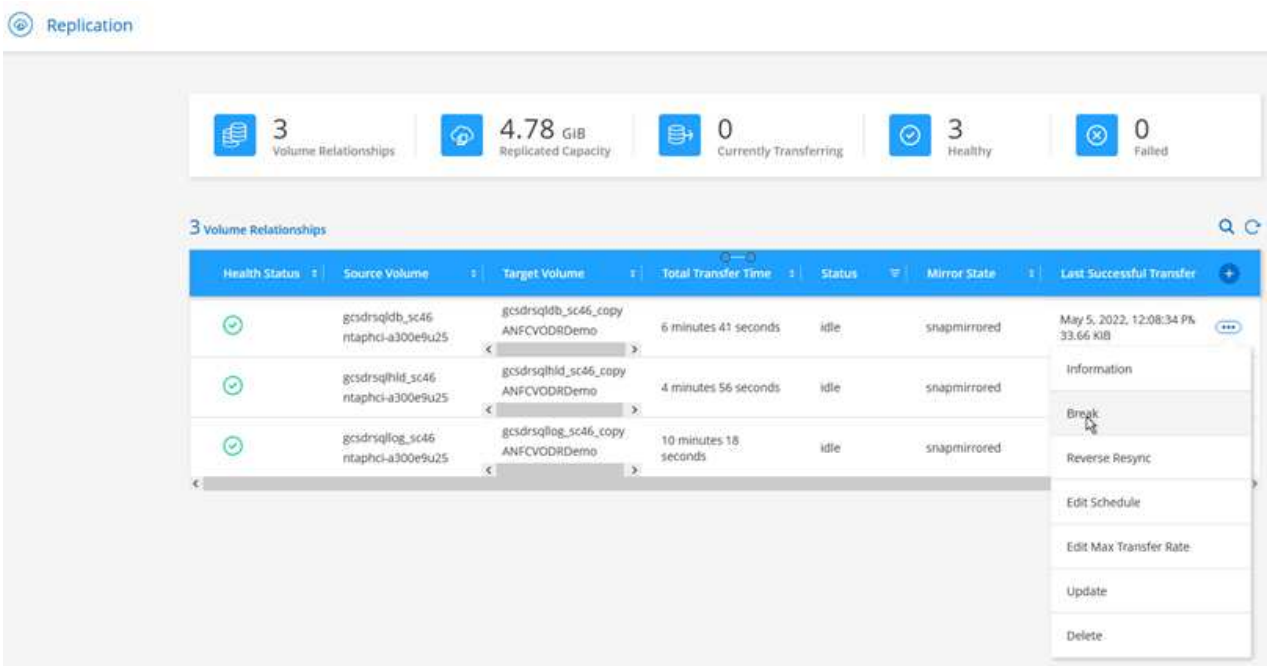
8. 選取適當的容錯移轉選項（持續容錯移轉或容錯移轉）。在此範例中、會選取持續還原（持續容錯移轉）。

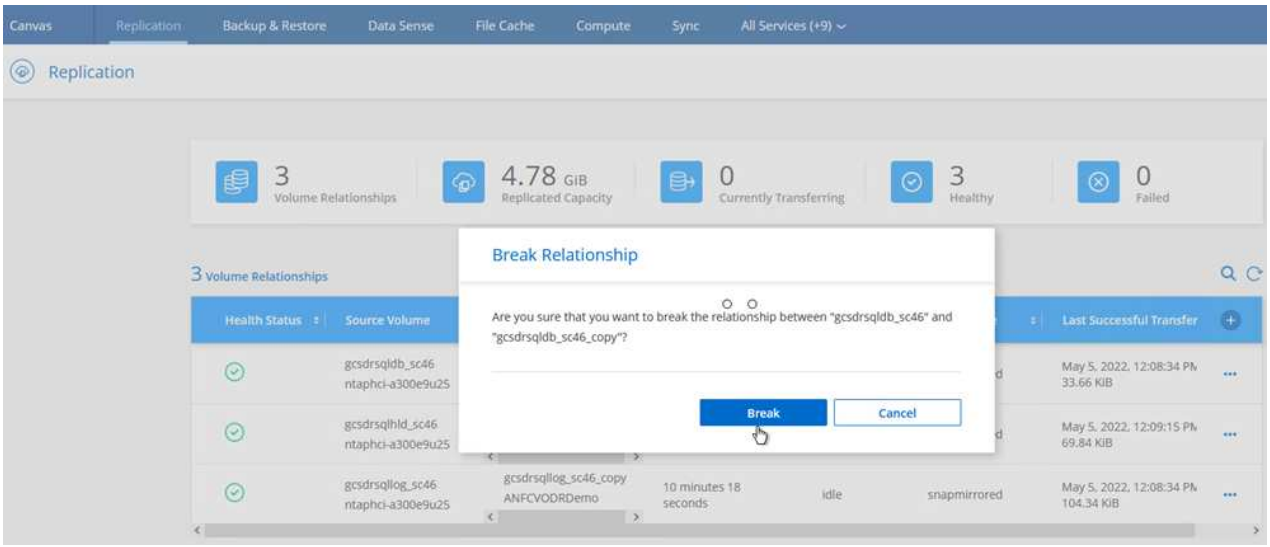
雖然執行組態時、「持續容錯移轉」和「容錯移轉」模式各有不同、但兩種容錯移轉模式的設定步驟相同。容錯移轉步驟會一起設定及執行、以回應災難事件。您可以隨時設定持續容錯移轉、然後在正常系統作業期間、允許在背景執行。發生災難事件之後、持續容錯移轉作業便會完成、以便立即將受保護VM的擁有權轉移到恢復站台（RTO接近零）。



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

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

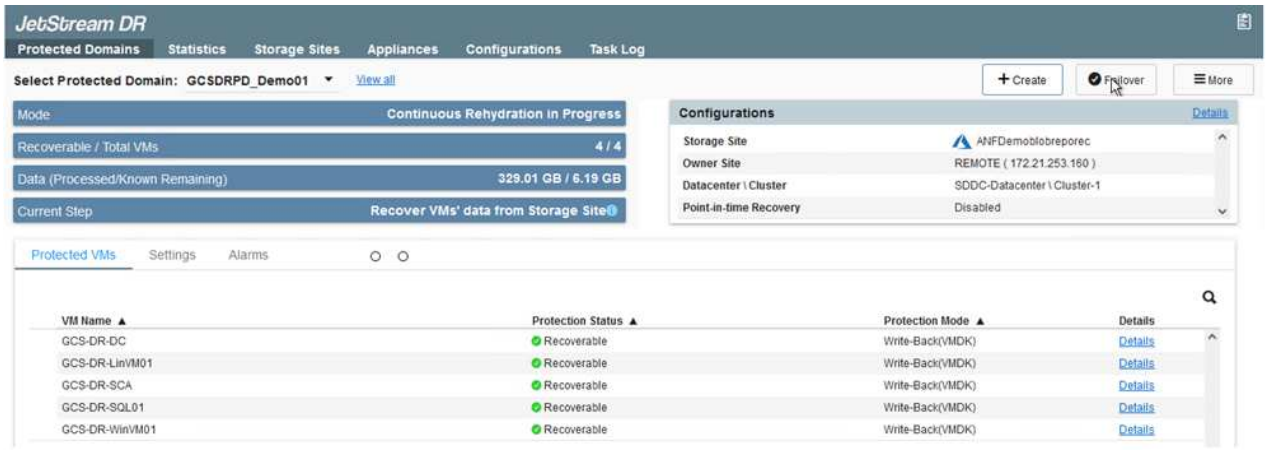


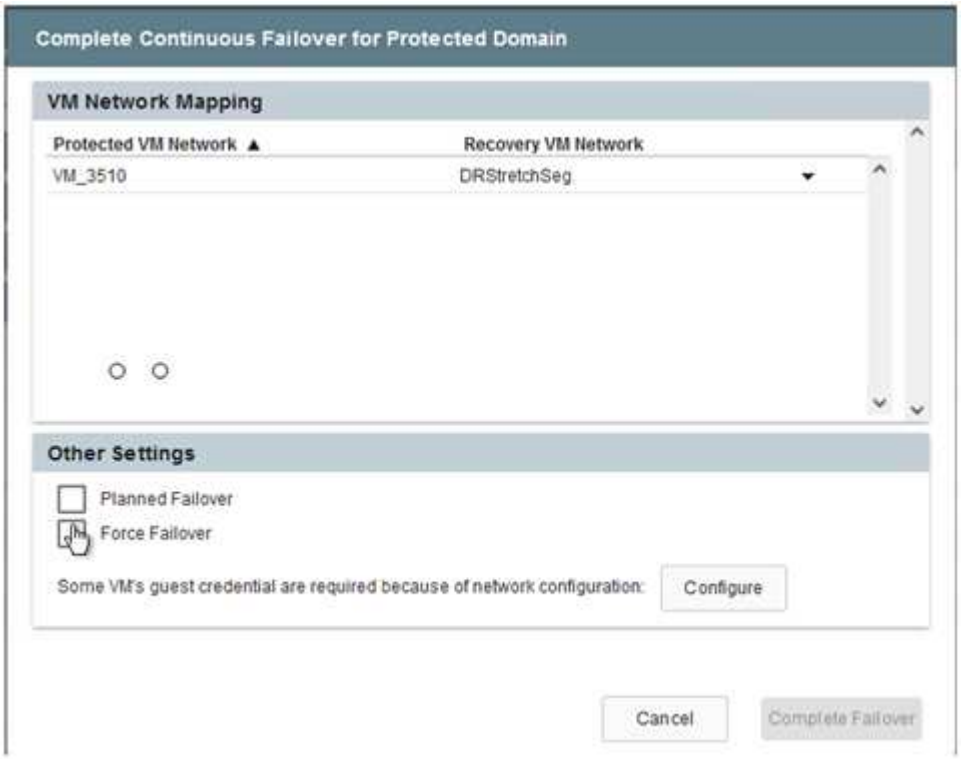


此步驟可輕鬆自動化、以利恢復程序。

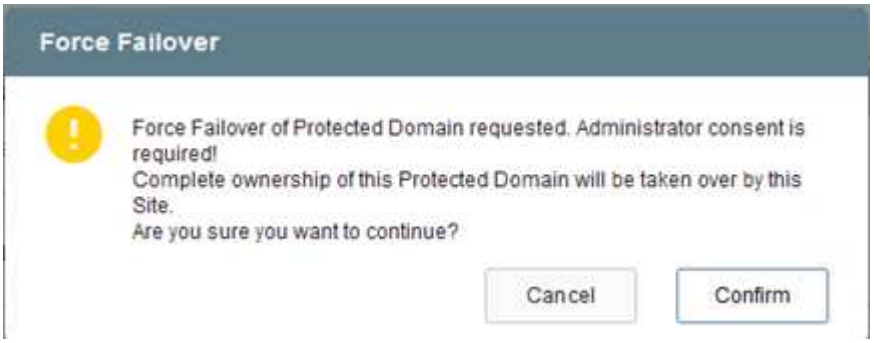
2. 存取AVS SDDC（目的地端）上的Jetstream UI、然後觸發容錯移轉選項以完成容錯移轉。工作列會顯示容錯移轉活動的進度。

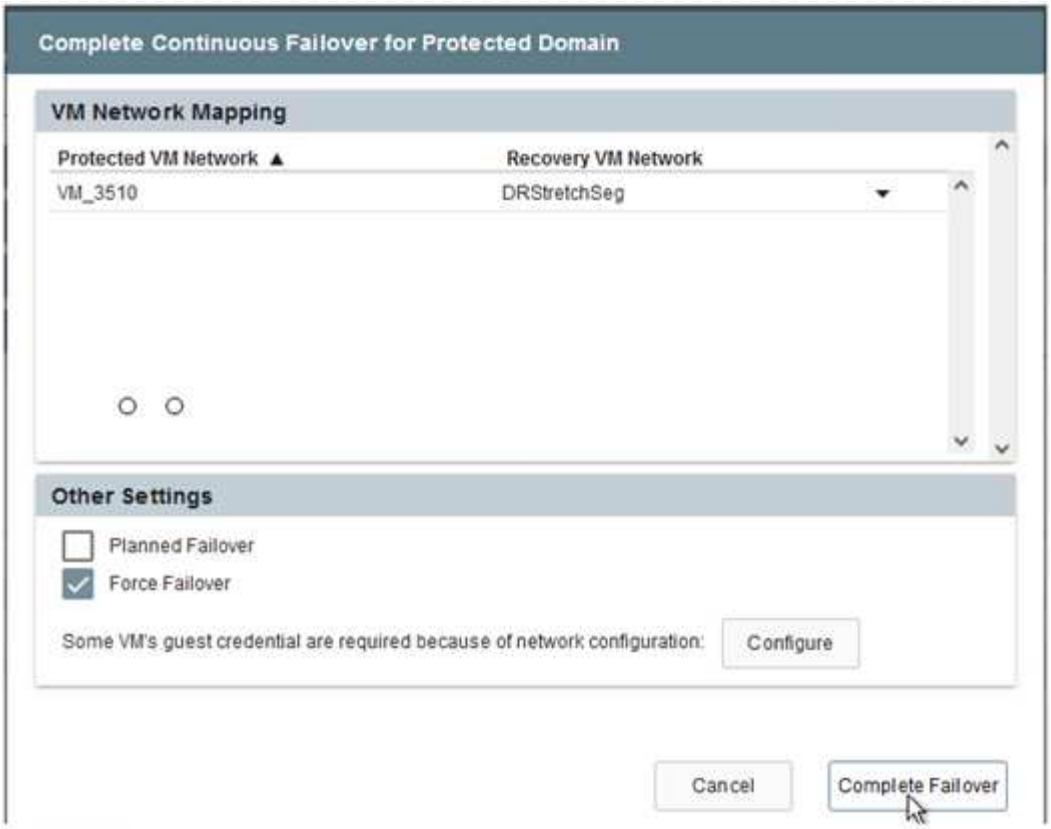
   在完成容錯移轉時所出現的對話視窗中、容錯移轉工作可以指定為已規劃或假設為強制進行。





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





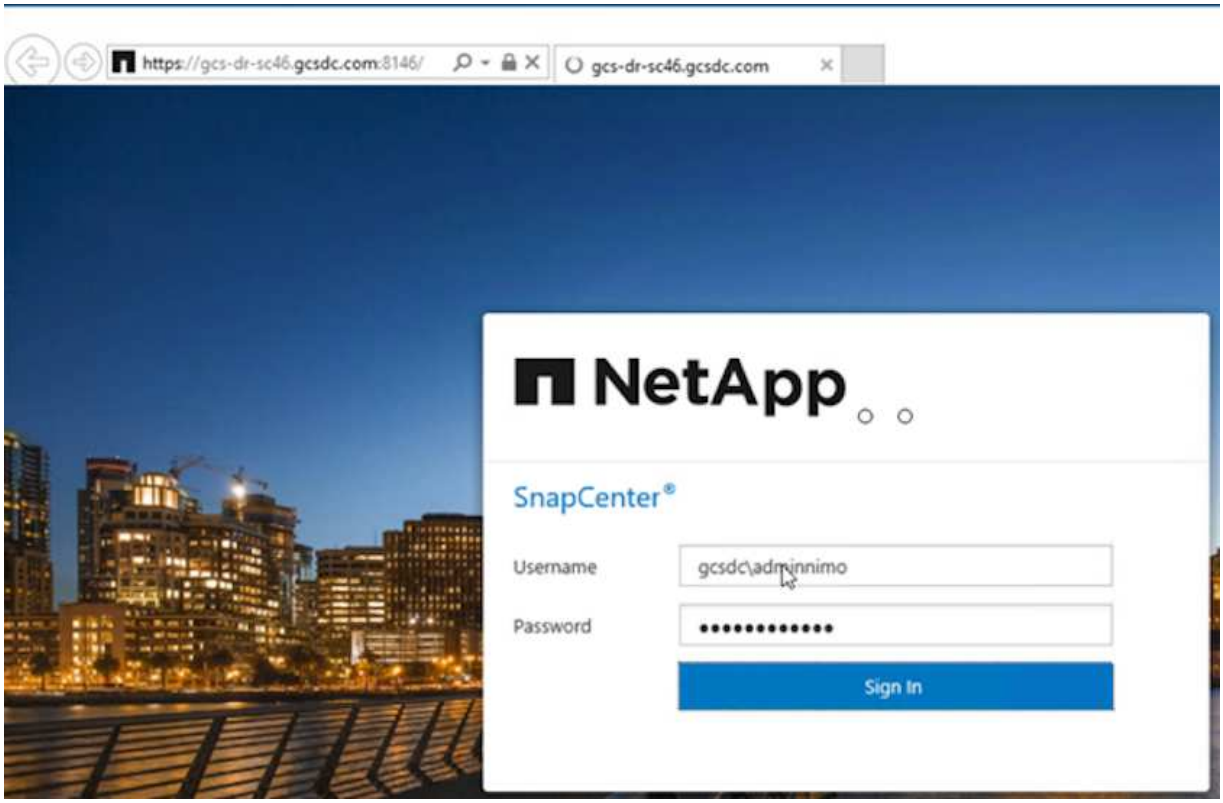
3. 持續容錯移轉完成後、會出現一則訊息、確認工作已完成。當工作完成時、請存取恢復的VM來設定iSCSI或NFS工作階段。

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

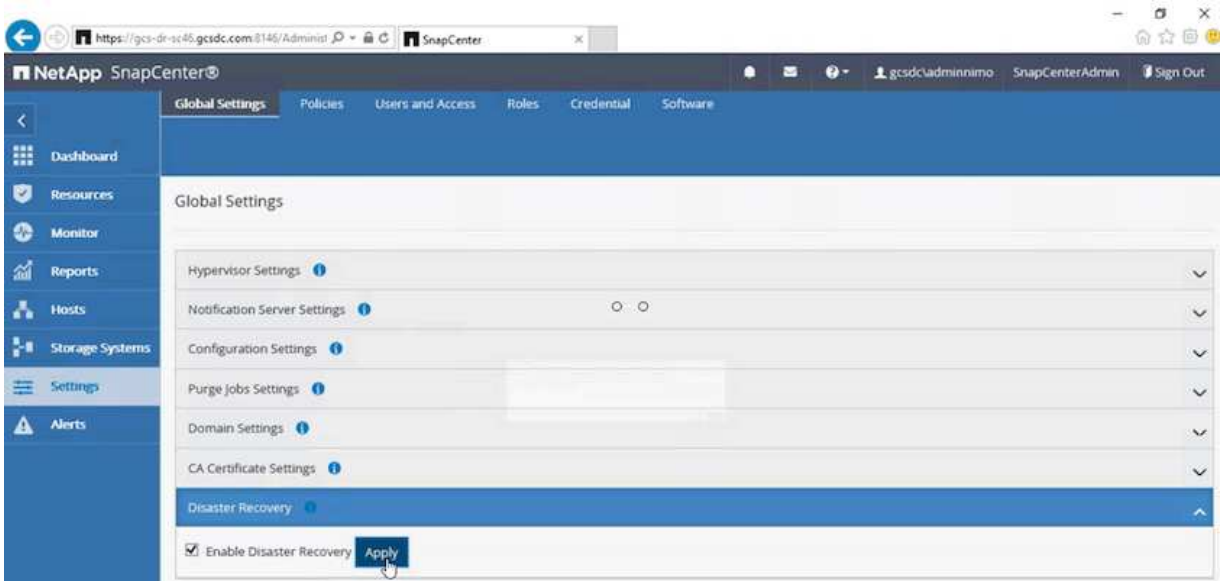
為了驗證容錯移轉組態和基礎架構、可以在測試模式（測試容錯移轉選項）下操作、觀察虛擬機器及其資料從物件存放區恢復到測試還原環境的過程。在測試模式下執行容錯移轉程序時、其運作方式類似於實際的容錯移轉程序。

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

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



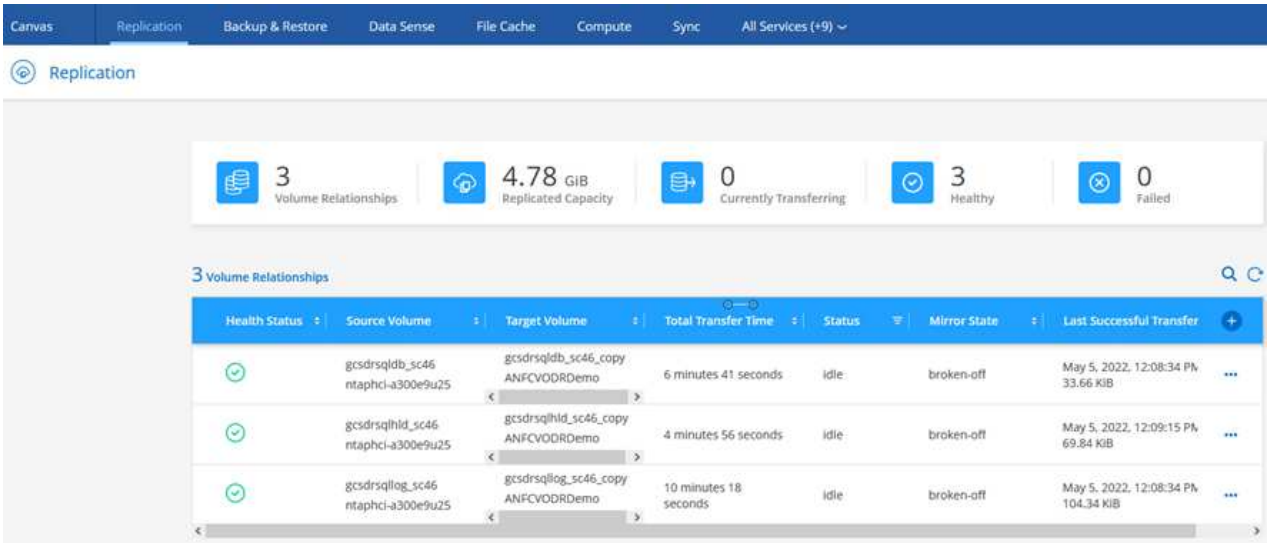
   b. 在「設定」頁面中、瀏覽至「設定」>「全域設定」>「災難恢復」。
   c. 選取「啟用災難恢復」。
   d. 按一下套用。



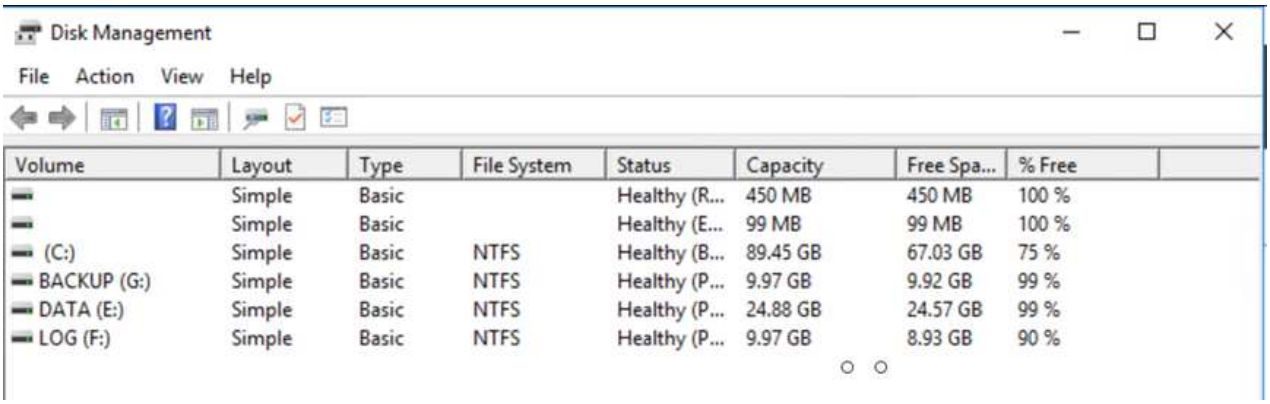
   e. 按一下「監控」>「工作」、確認DR工作是否已啟用。

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

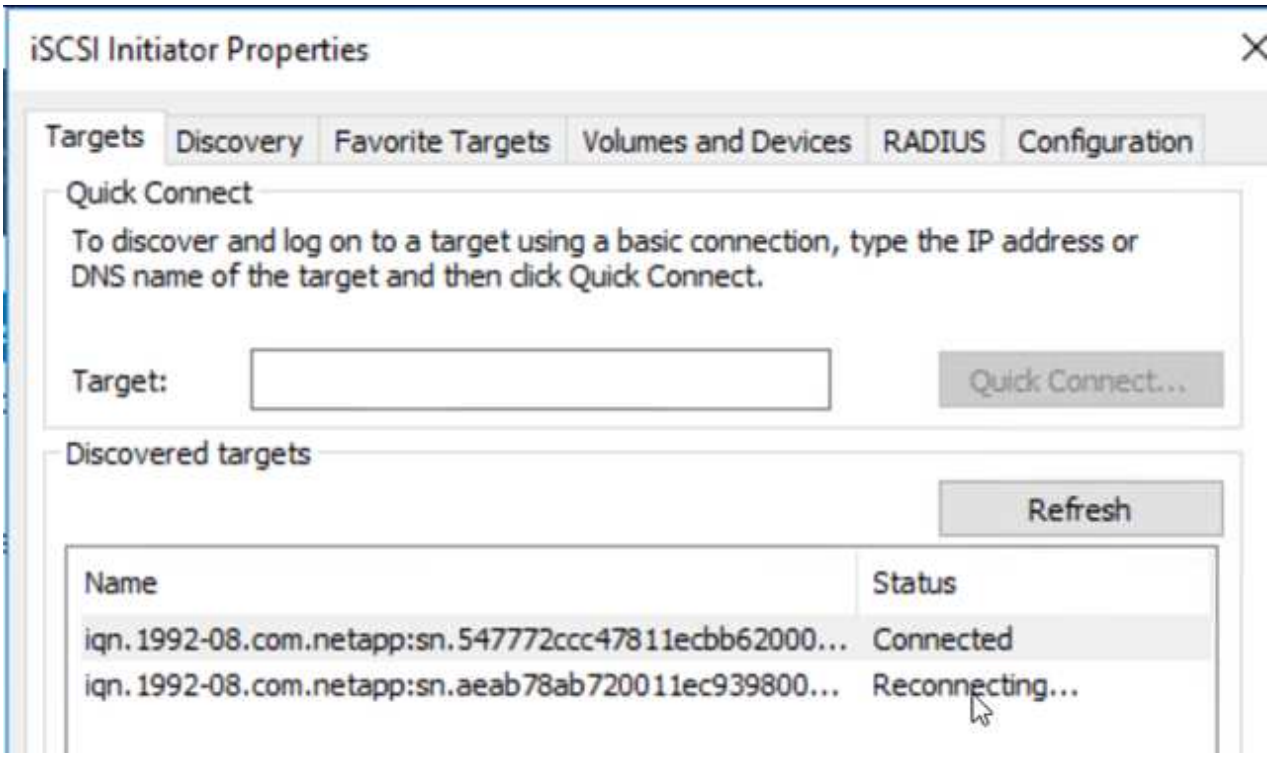
6. 確定SnapMirror關係已中斷。



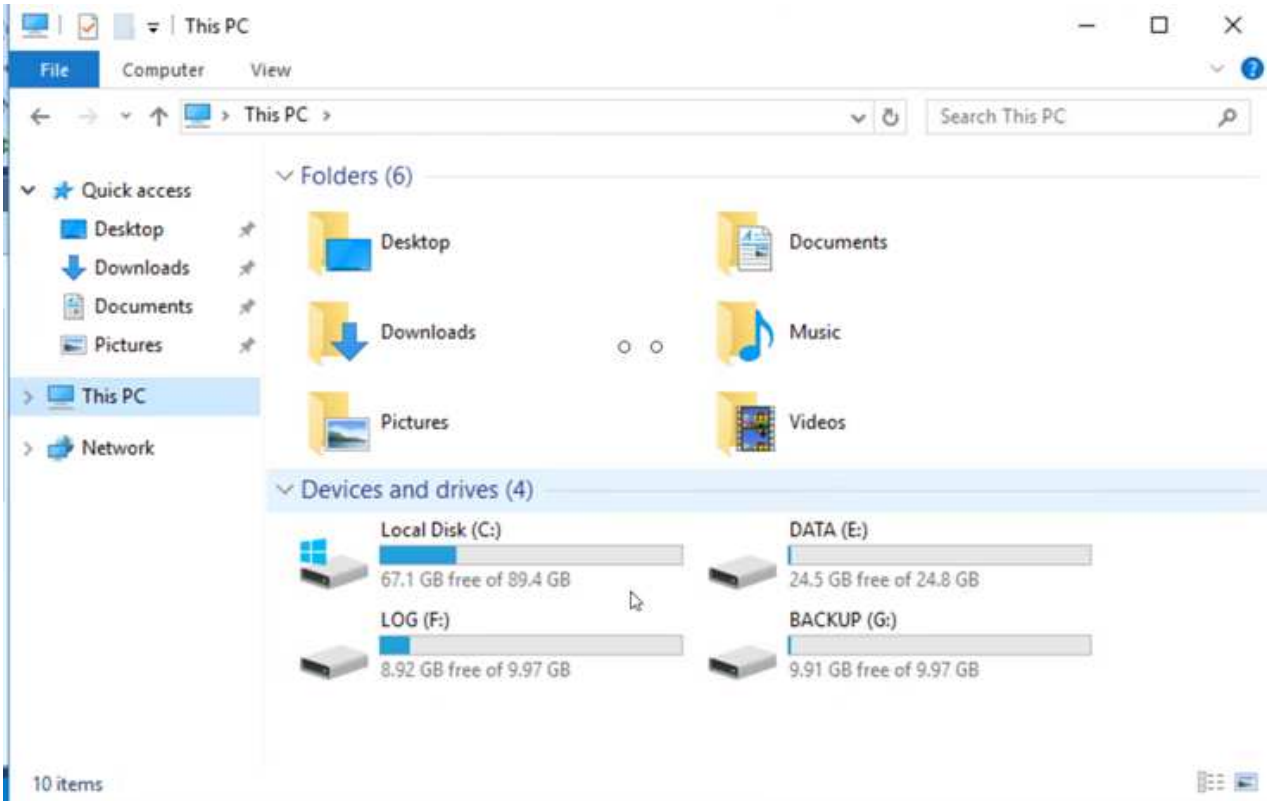
7. 使用Cloud Volumes ONTAP 相同的磁碟機代號、將LUN從支援系統連接到已恢復的SQL客體VM。



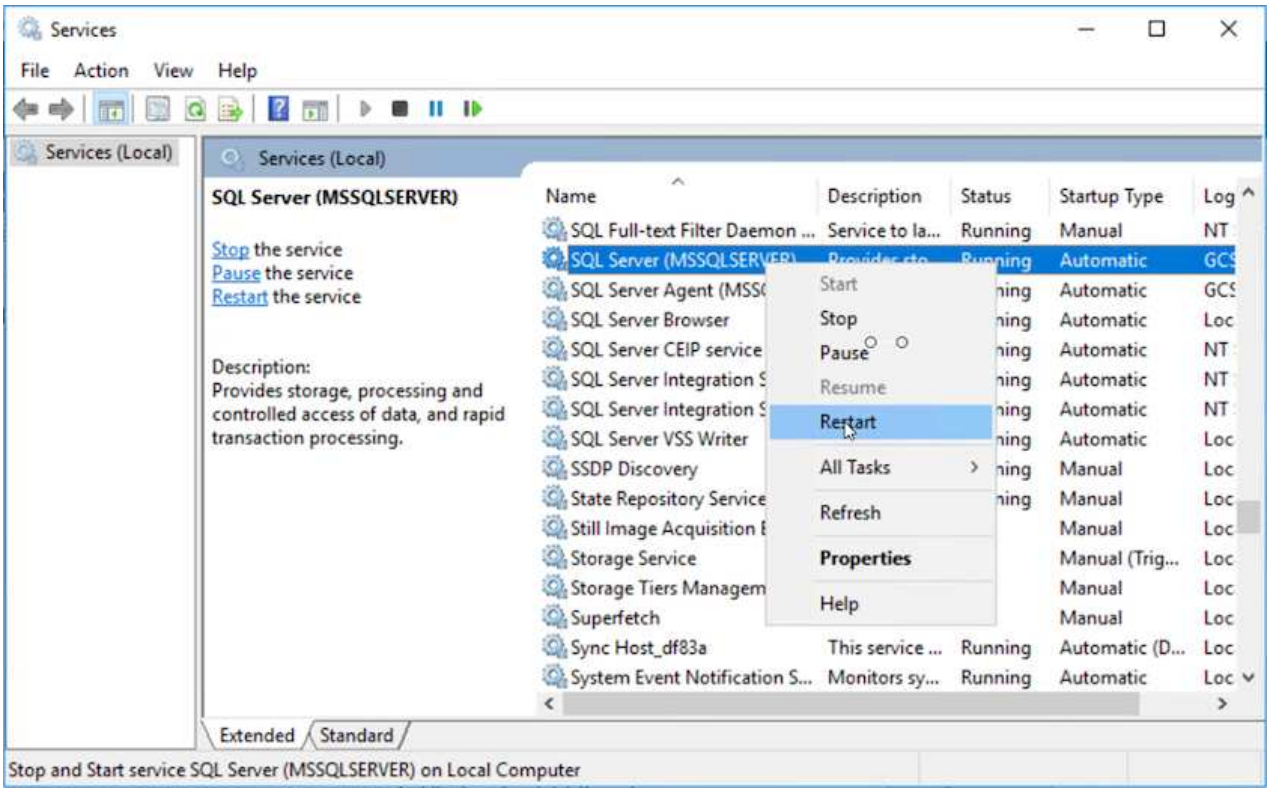
8. 開啟iSCSI啟動器、清除先前中斷連線的工作階段、並新增新目標及複寫Cloud Volumes ONTAP 的支援區的多重路徑。



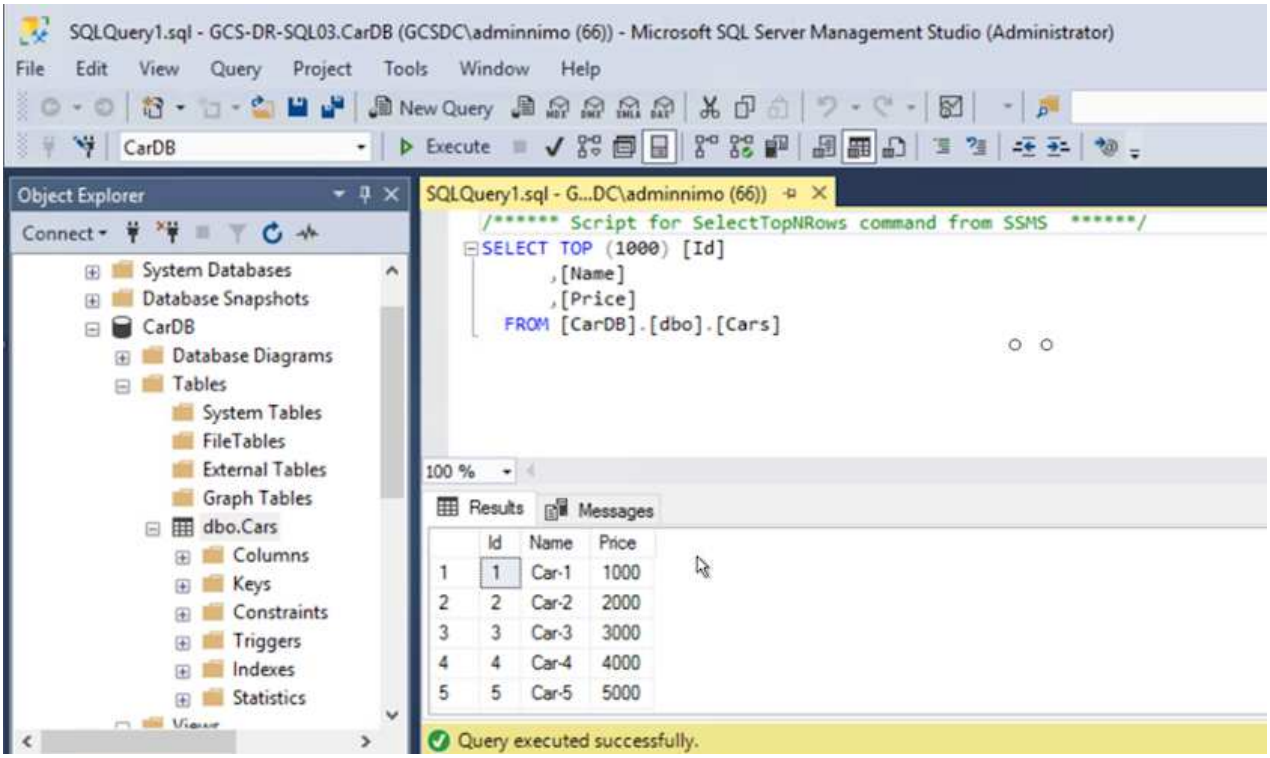
9. 請確定所有磁碟均使用與DR之前相同的磁碟機代號進行連線。



10. 重新啟動MSSQL伺服器服務。



11. 請確定SQL資源重新連線。



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

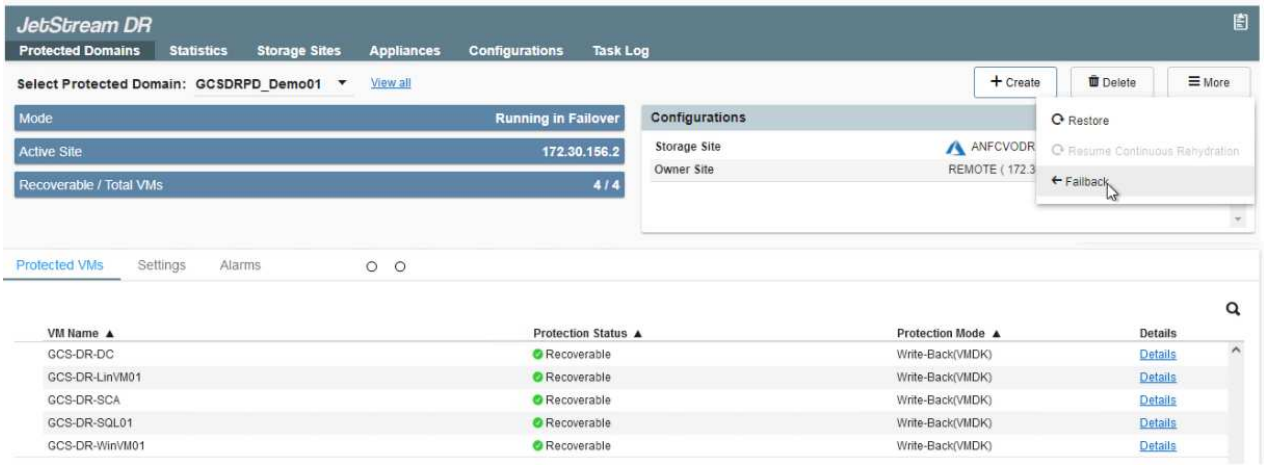
此時、您可以執行作業並正常營運。

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

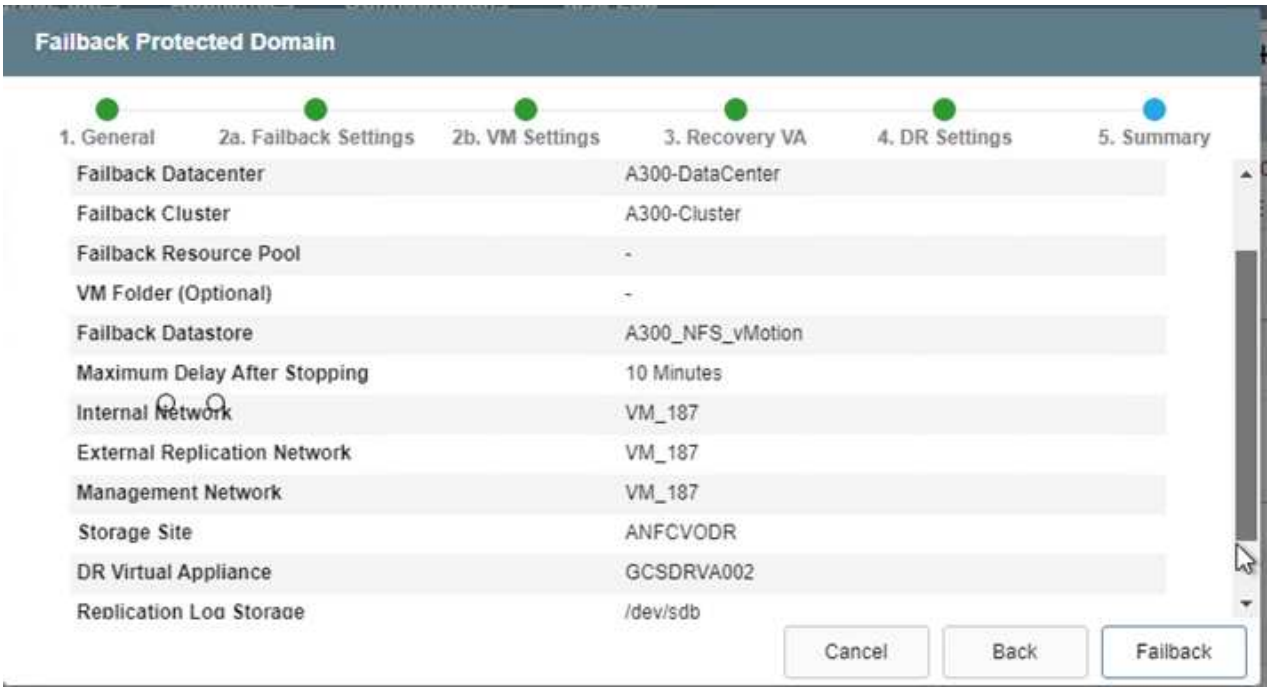
當主要站台重新啟動並執行之後、您就可以執行容錯回復。系統會由Jetstream恢復VM保護、且SnapMirror關係必須回復。

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

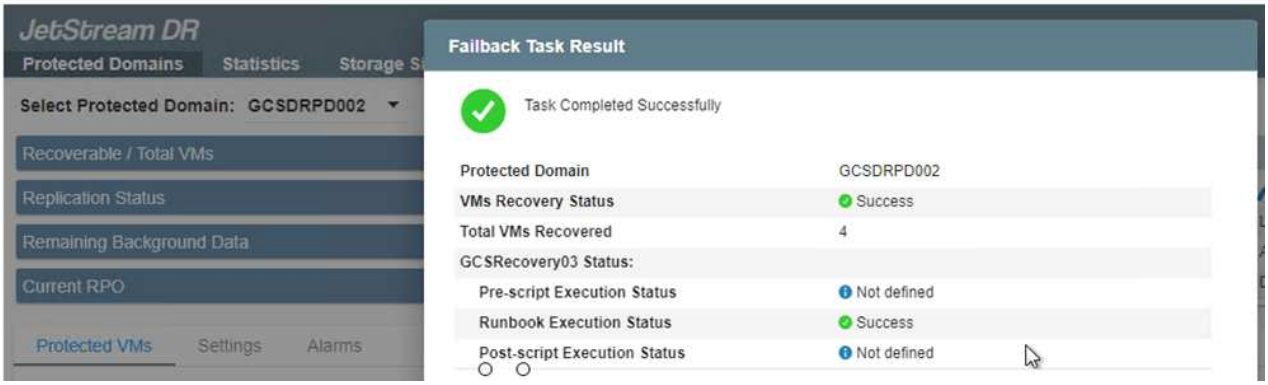
此外、也可使用由程式管理產生的容錯回復計畫、將VM及其資料從物件存放區傳回原始的VMware環境。



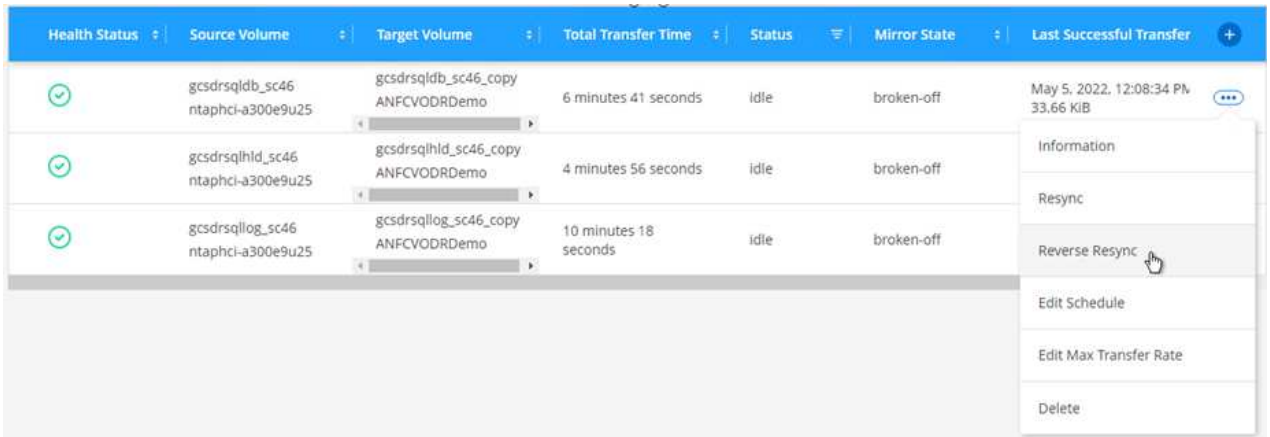
在恢復站台中暫停VM並在受保護站台重新啟動VM之後、請指定最大延遲。完成此程序所需的時間包括：停止容錯移轉VM後完成複寫、清理恢復站台所需的時間、以及在受保護站台重新建立VM所需的時間。NetApp建議使用10分鐘。

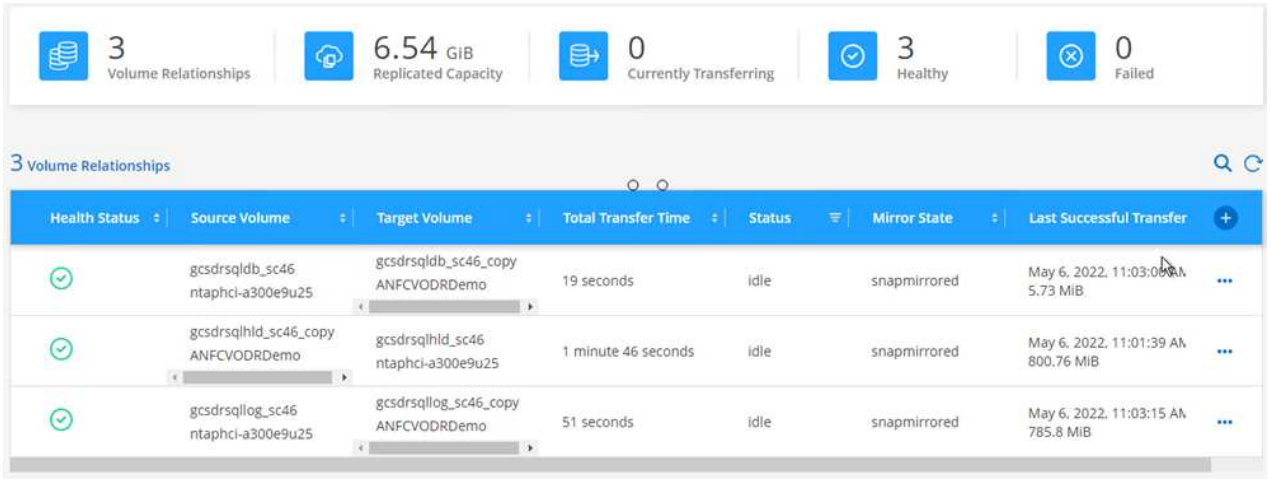


3. 完成容錯回復程序、然後確認恢復VM保護和資料一致性。

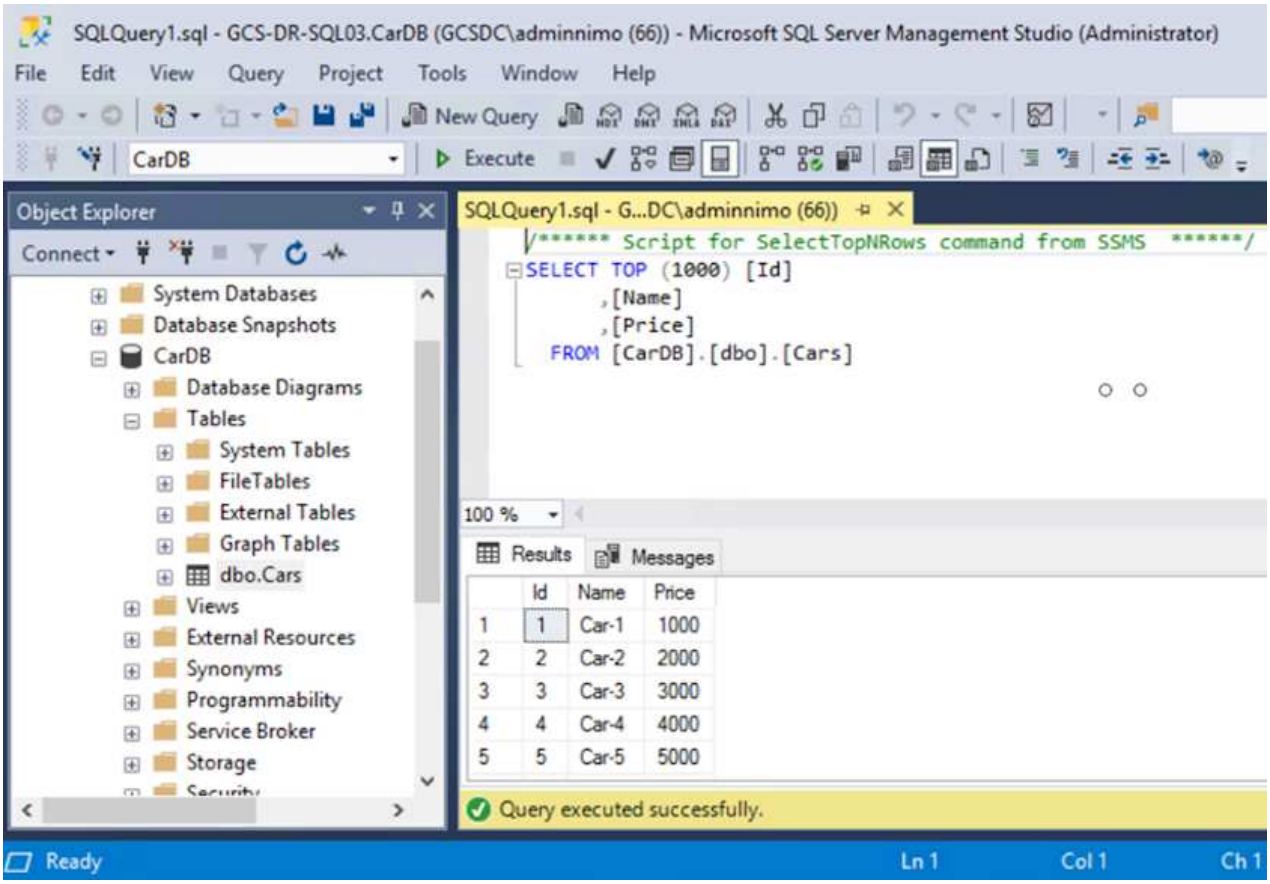


4. 恢復虛擬機器後、請中斷次要儲存設備與主機的連線、並連線至主要儲存設備。





5. 重新啟動MSSQL伺服器服務。
6. 驗證SQL資源是否重新連線。



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

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

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

用程式。

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

本解決方案的優點

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

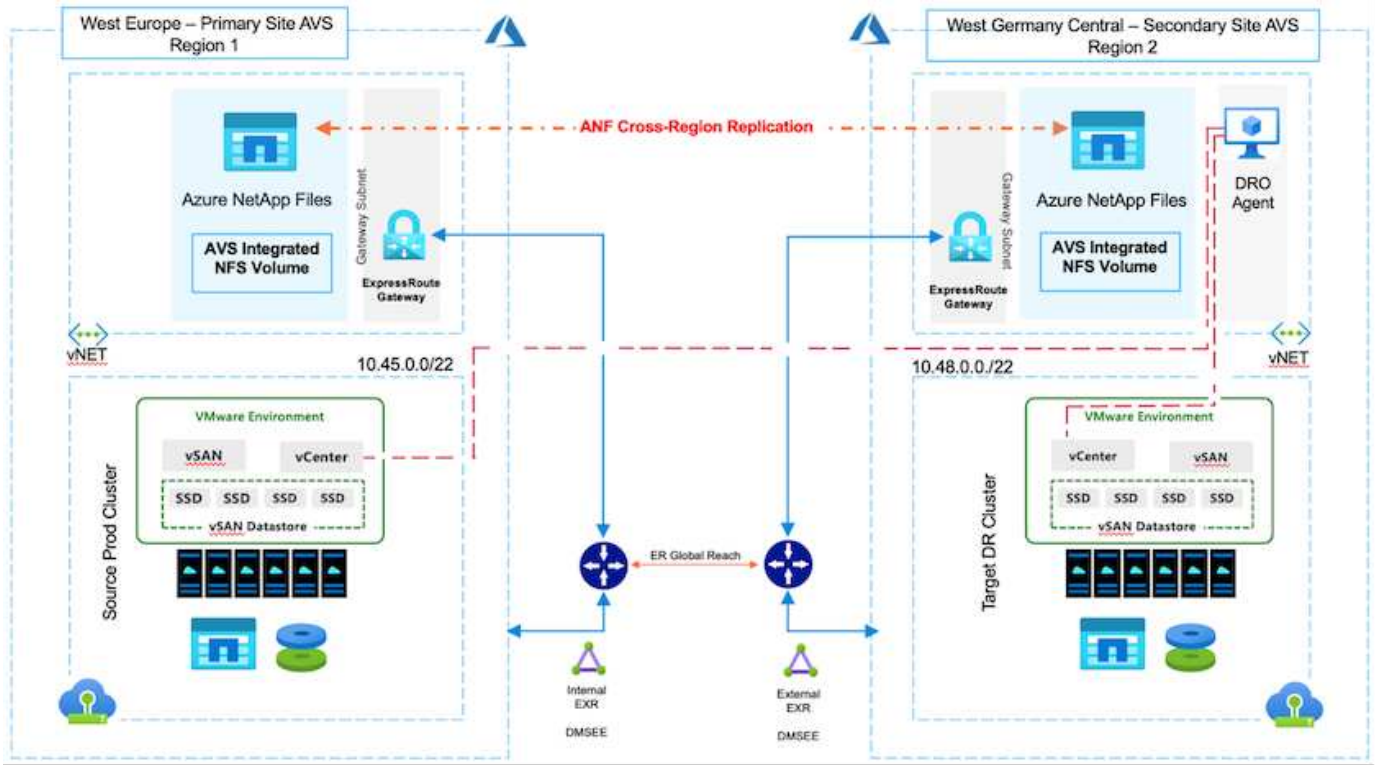
TR-4755 ：使用 **Azure NetApp Files** （ **anf** ）和 **Azure VMware** 解決方案（ **AVS** ）進行災難恢復

作者： NetApp 解決方案工程公司 Niyaz Mohamed

總覽

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

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



先決條件和一般建議

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

不支援串聯和扇入及扇出拓撲。

快速入門

部署 **Azure VMware** 解決方案

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

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

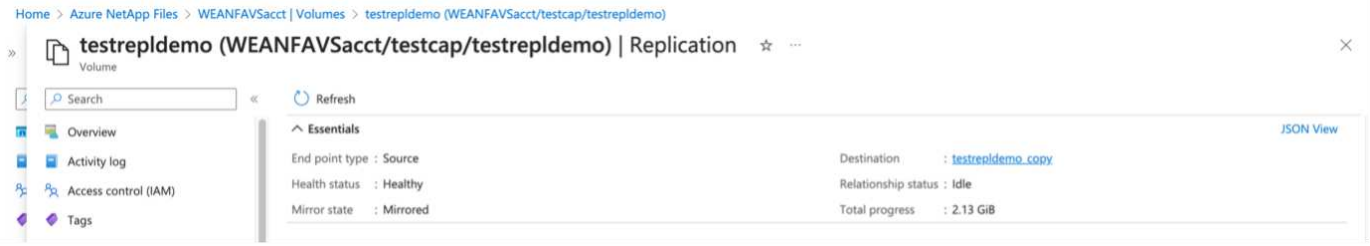
在初始版本中、 DRO 支援現有的 AVS SDDC 叢集。隨需建立SDDC將於即將推出的版本中提供。

配置和配置 **Azure NetApp Files**

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

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

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



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

跨區域複寫關係是先決條件、必須事先建立。

DRO安裝

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

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

。 `deploy.sh` 指令碼會執行所有必要的先決條件。

步驟如下：

1. 在指定的虛擬機器上下載安裝套件：

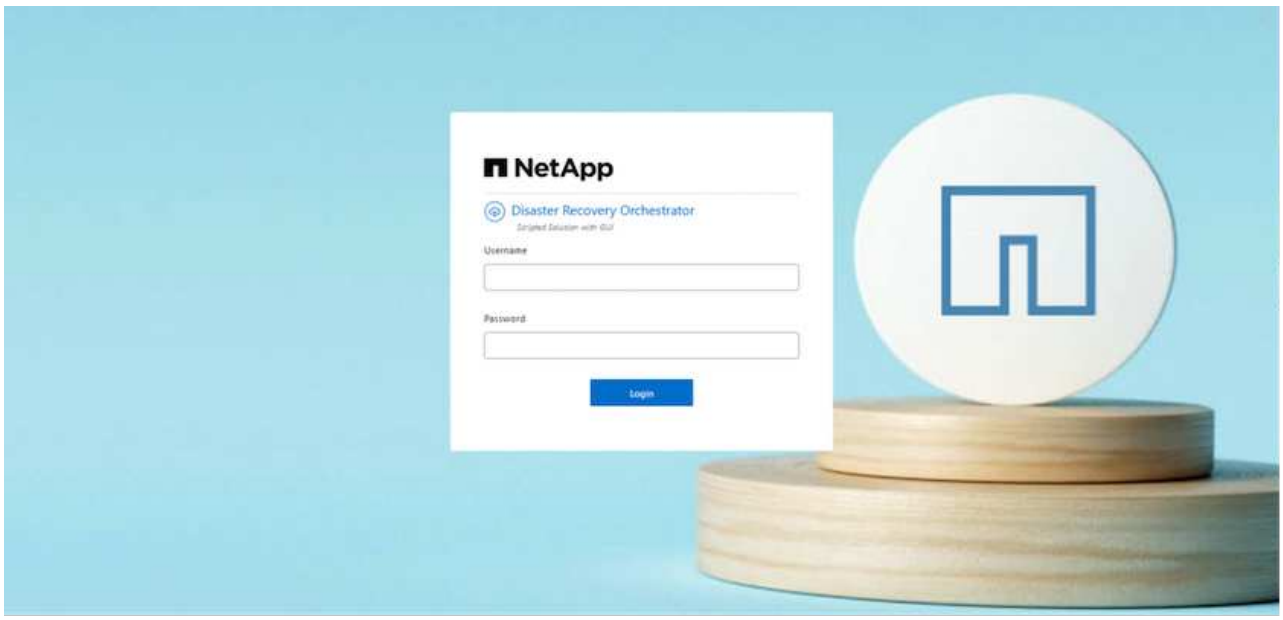
```
git clone https://github.com/NetApp/DRO-Azure.git
```

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

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

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

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



DRO組態

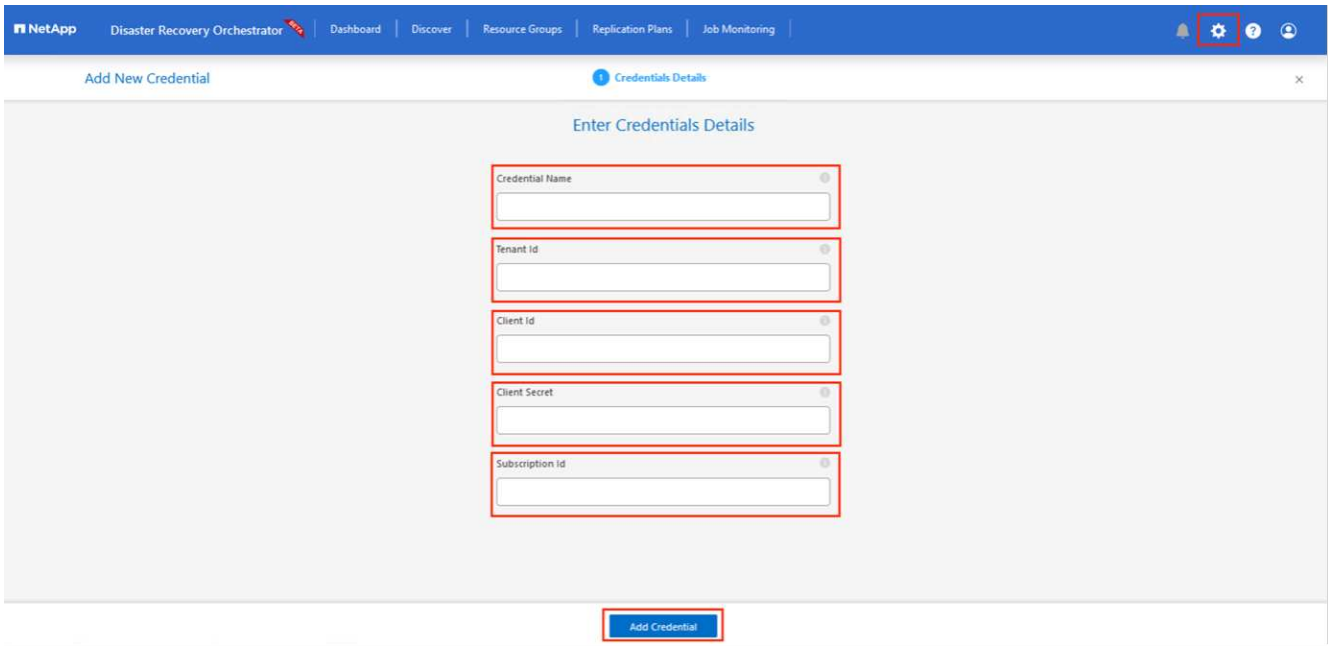
正確設定 Azure NetApp Files 和 AVS 之後、您可以開始設定 DRO 、將工作負載從主要 AVS 站台自動恢復到次要 AVS 站台。NetApp 建議在次要 AVS 站台部署 DRO 代理程式、並設定 ExpressRoute 閘道連線、以便 DRO 代理程式能透過網路與適當的 AVS 和 Azure NetApp Files 元件進行通訊。

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

若要執行此作業、請完成下列步驟：

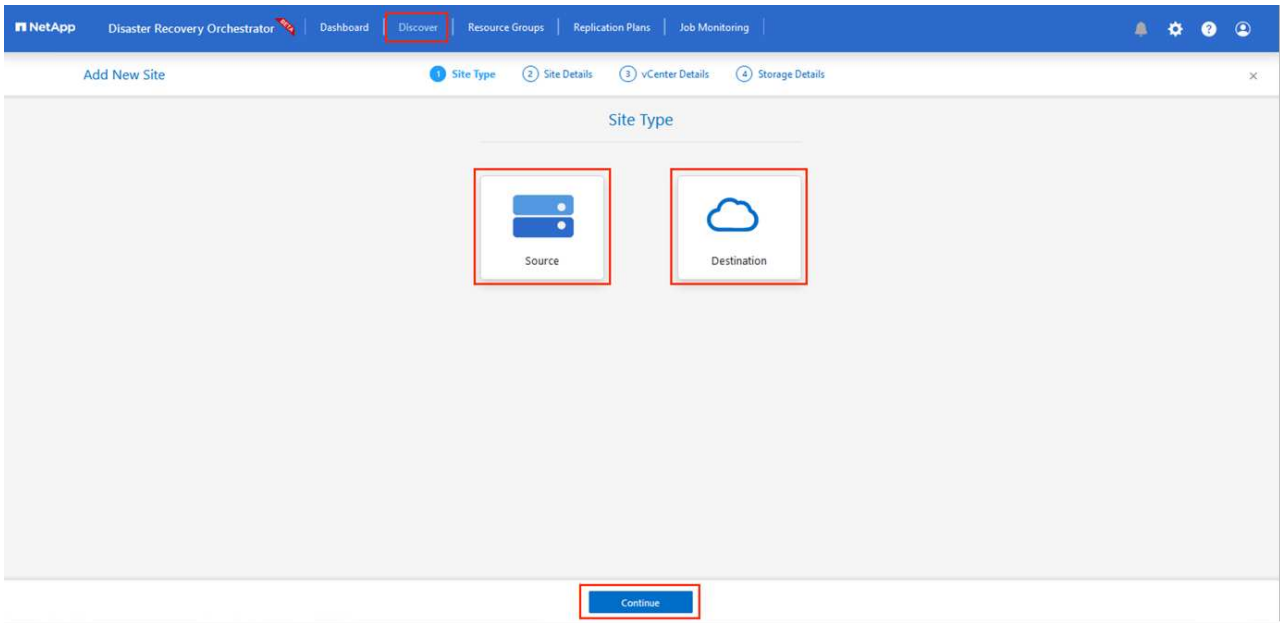
1. 在支援的瀏覽器中開啟 DRO 、並使用預設的使用者名稱和密碼 /admin/admin）。您可以使用變更密碼選項、在第一次登入後重設密碼。
2. 在 DRO 主控台的右上角、按一下 * 設定 * 圖示、然後選取 * 認證 * 。
3. 按一下新增認證、然後依照精靈中的步驟進行。
4. 若要定義認證、請輸入有關授與必要權限的 Azure Active Directory 服務主體的資訊：
   - 認證名稱
   - 租戶 ID
   - 用戶端ID
   - 用戶端機密
   - 訂閱 ID

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



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

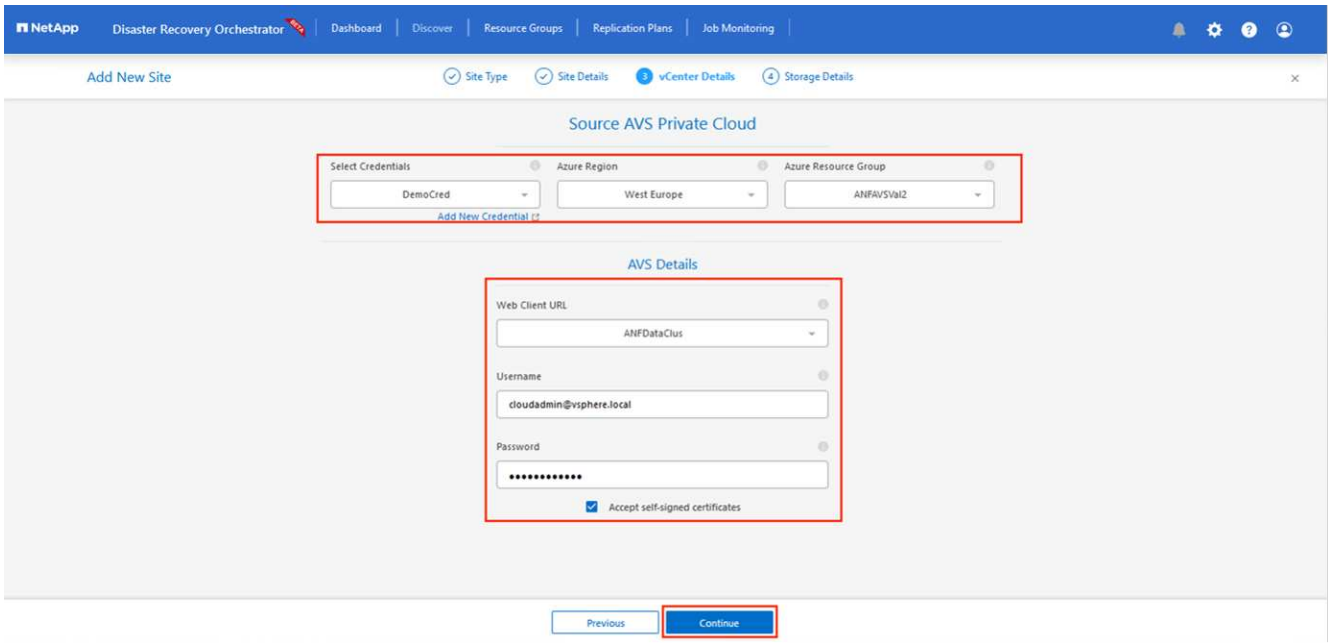
6. 移至 * 探索 * 標籤。
7. 按一下 * 新增站台 * 。
8. 新增下列主要 AVS 站台（在主控台中指定為 * 來源 * ）。
   - SDDC vCenter
   - Azure NetApp Files 儲存帳戶
9. 新增下列次要 AVS 站台（在主控台中指定為 * 目的地 * ）。
   - SDDC vCenter
   - Azure NetApp Files 儲存帳戶



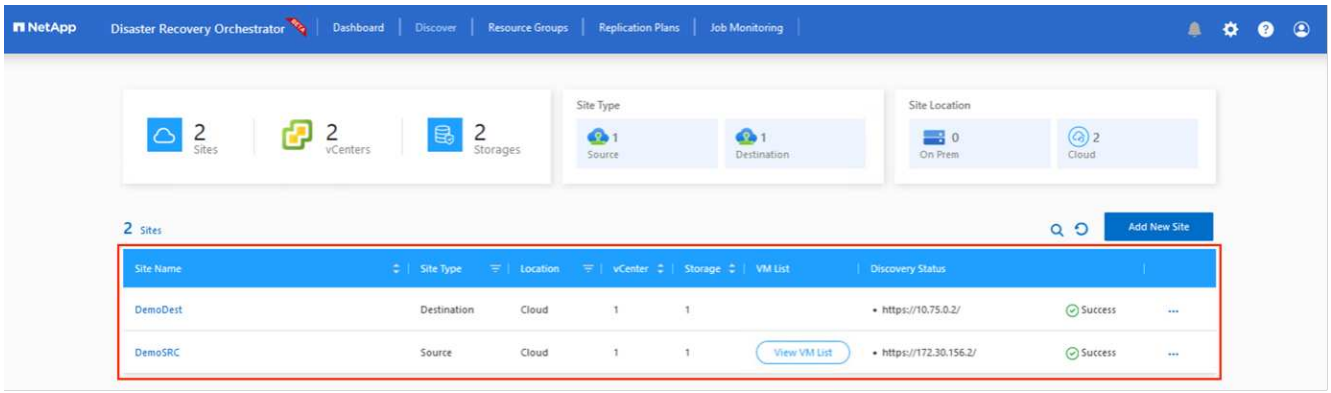
10. 按一下 * 來源 * 、 * 輸入易記的網站名稱、然後選取連接器、即可新增網站詳細資料。然後按一下 * 繼續 * 。

> 為了進行示範、本文件涵蓋新增來源網站。

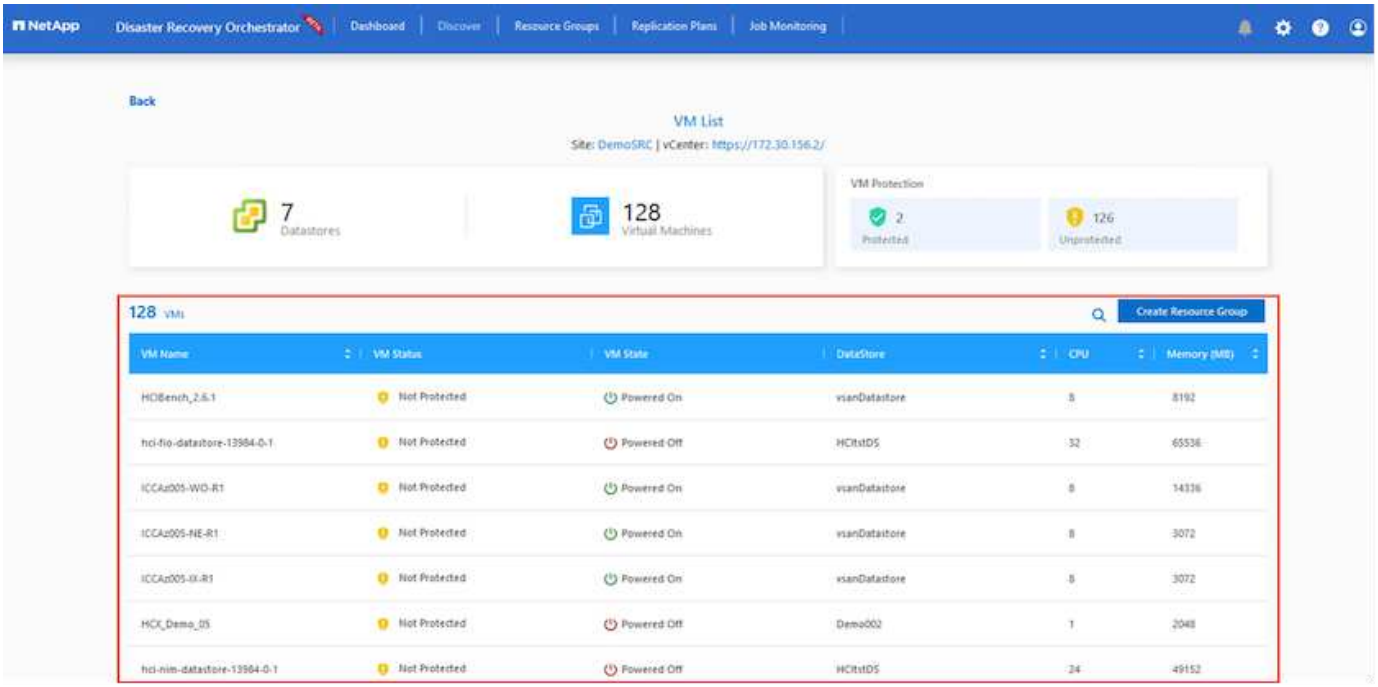
11. 更新 vCenter 詳細資料。若要這麼做、請從主 AVS SDDC 的下拉式清單中選取認證、 Azure 區域和資源群組。
12. DRO 會列出區域內所有可用的 SDDC 。從下拉式清單中選取指定的私有雲 URL 。
13. 輸入 `cloudadmin@vsphere.local` 使用者認證。您可以從 Azure Portal 存取此功能。請遵循本文件中所述的步驟 "連結"。完成後、按一下 * 繼續 * 。



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



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



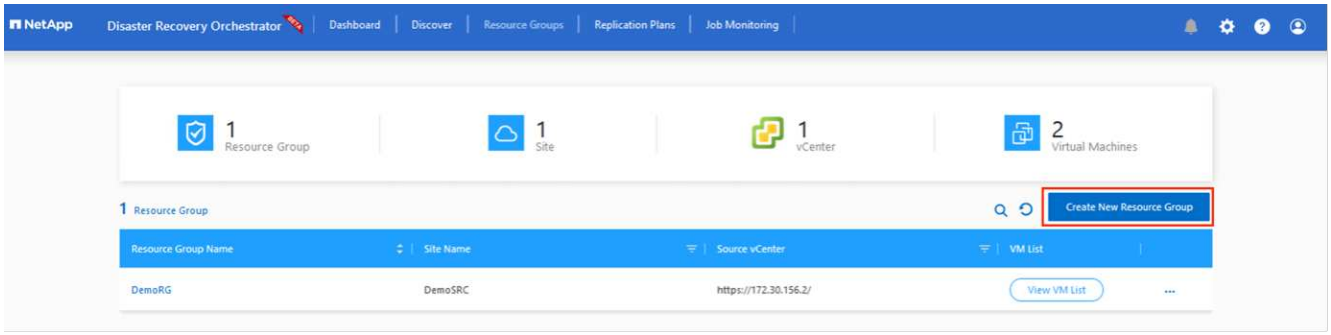
下一步是將所需的虛擬機器分組為其功能群組、做為資源群組。

資源群組

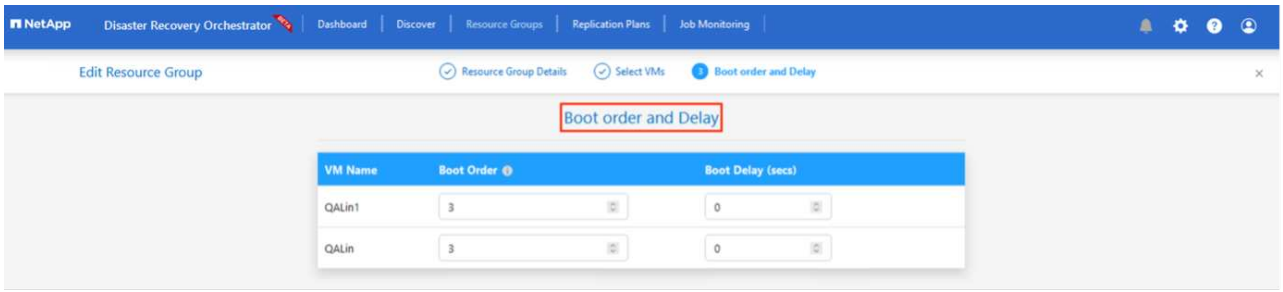
新增平台之後、將您要恢復的虛擬機器分組到資源群組中。DRO資源群組可讓您將一組相依的虛擬機器分組至邏輯群組、其中包含開機順序、開機延遲、以及可在恢復時執行的選用應用程式驗證。

若要開始建立資源群組、請按一下 * 建立新資源群組 * 功能表項目。

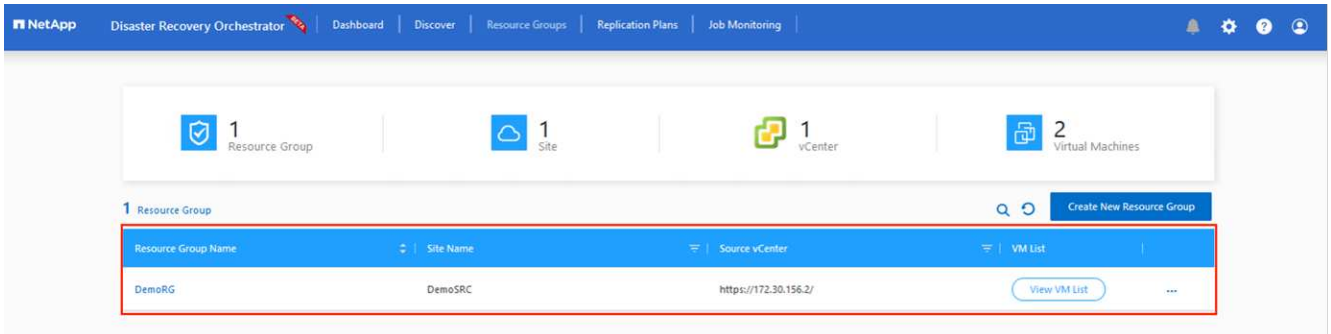
1. 存取 * 資源群組 * 、然後按一下 * 建立新資源群組 * 。



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



6. 按一下「建立資源群組」。

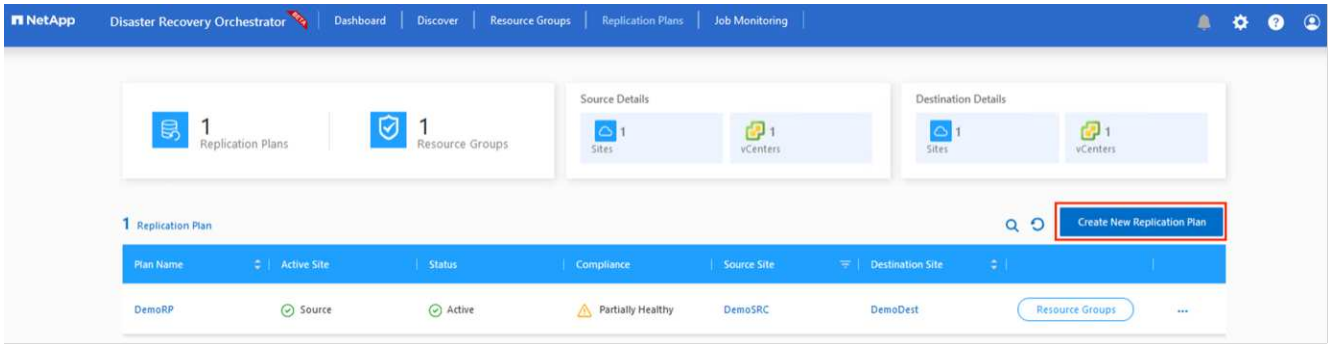


複寫計畫

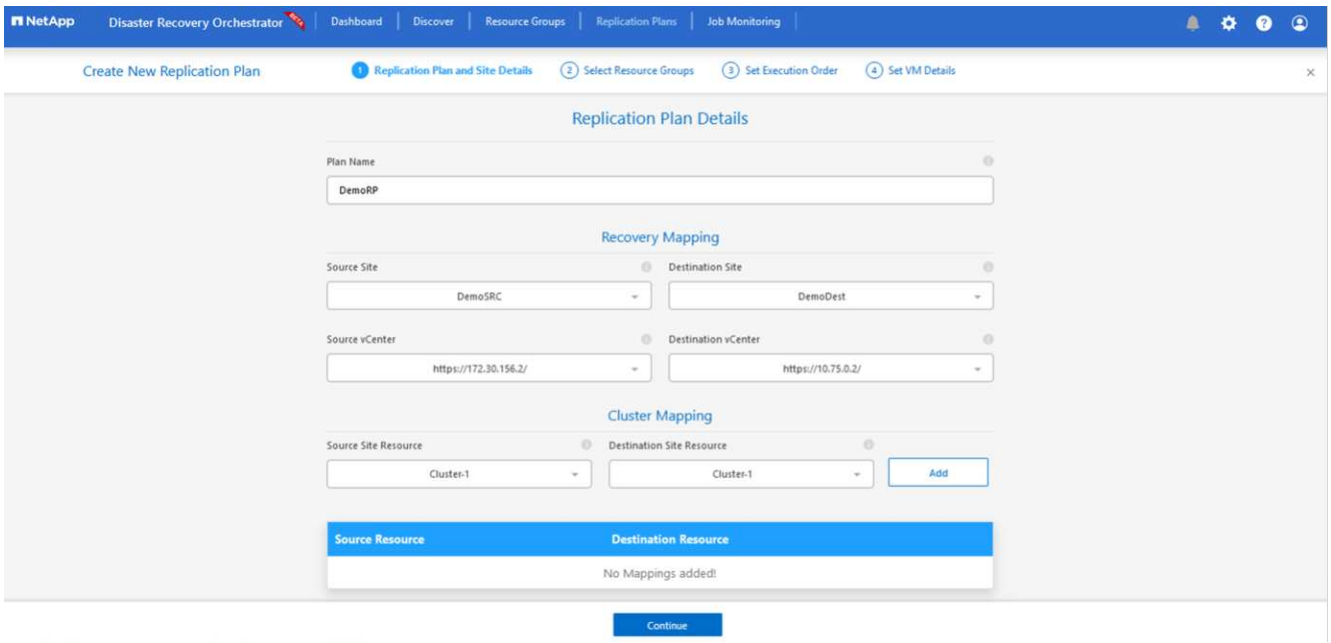
您必須制定計畫、以便在發生災難時恢復應用程式。從下拉式清單中選取來源和目的地 vCenter 平台、選擇要納入此計畫的資源群組、並包含應用程式還原和開機方式的分組（例如、網域控制站、層級 1 、層級 2 等）。計畫通常也稱為藍圖。若要定義恢復計畫、請瀏覽至複寫計畫索引標籤、然後按一下 * 新增複寫計畫 * 。

若要開始建立複寫計畫、請完成下列步驟：

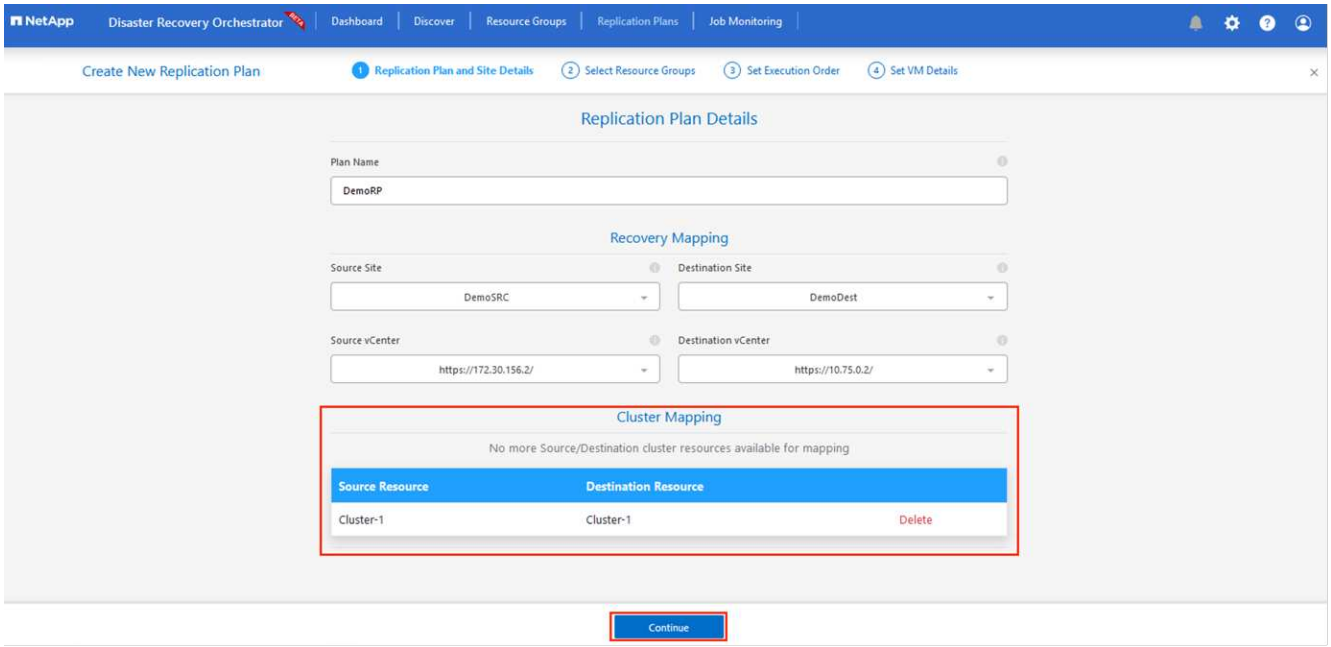
1. 瀏覽至 * 複寫計畫 * 、然後按一下 * 建立新複寫計畫 * 。



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

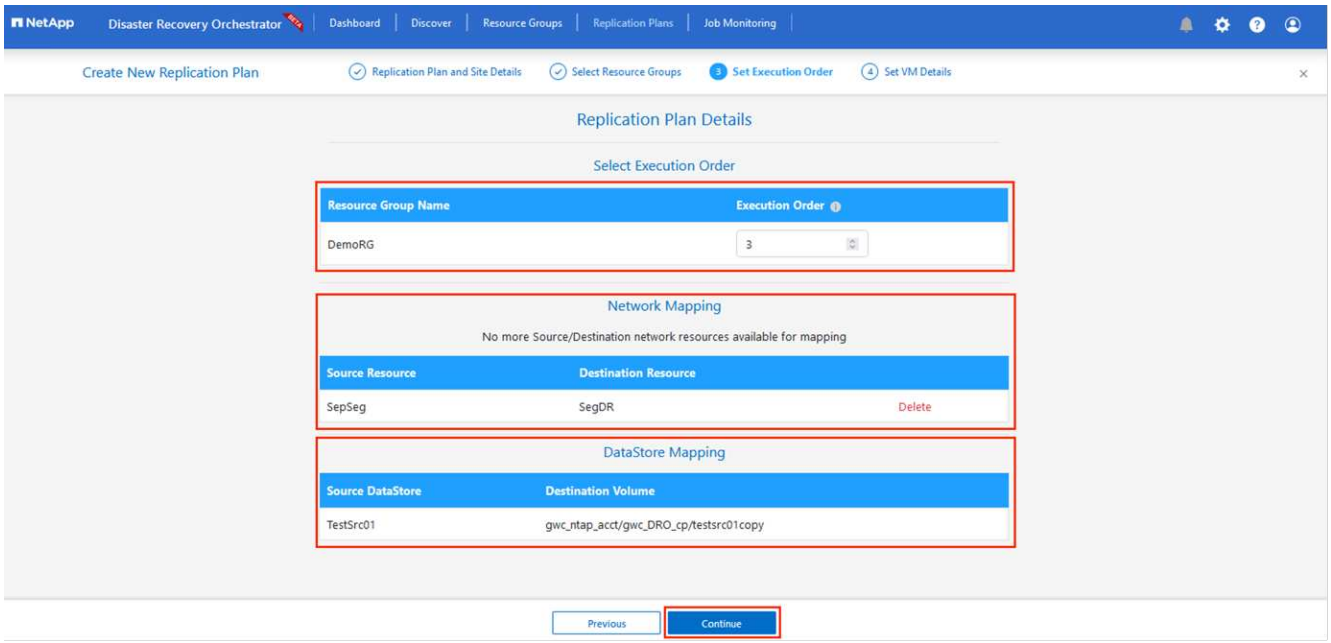


3. 恢復對應完成後、選取 * 叢集對應 * 。



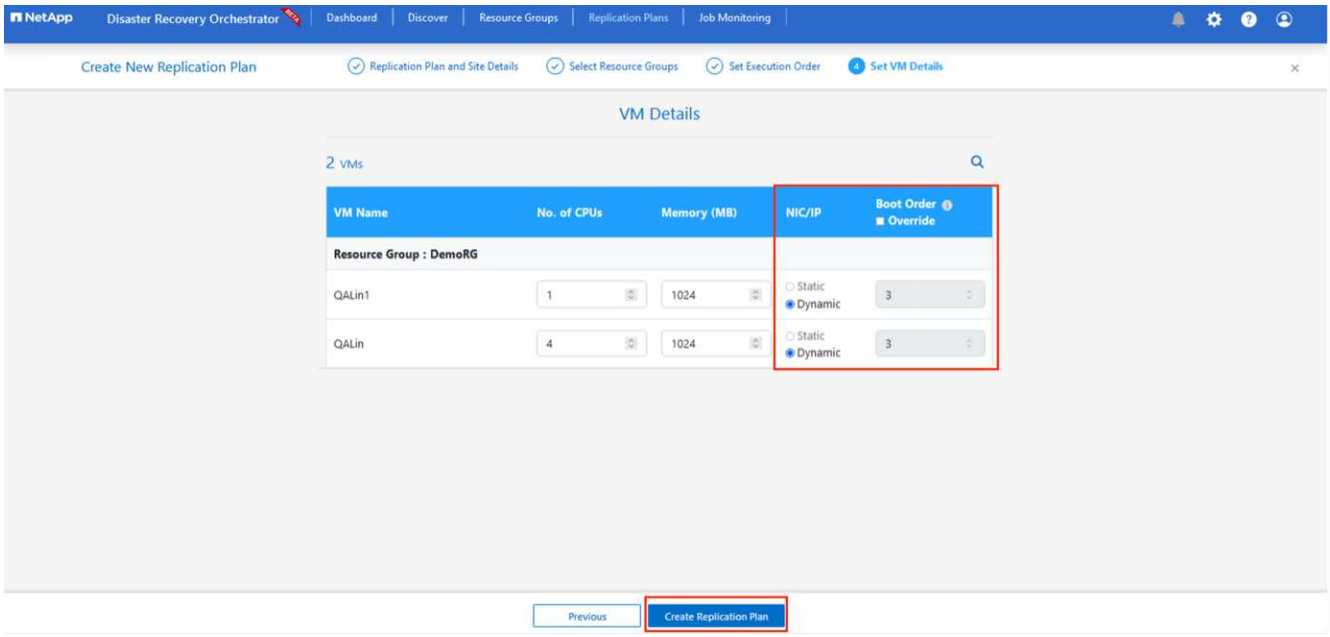
4. 選擇*資源群組詳細資料*、然後按一下*繼續*。
5. 設定資源群組的執行順序。此選項可讓您在存在多個資源群組時、選取作業順序。
6. 完成後、請將網路對應設定為適當的區段。這些區段應已在次要 AVS 叢集上進行佈建、若要將 VM 對應至這些區段、請選取適當的區段。
7. 資料存放區對應會根據虛擬機器的選擇自動選取。

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

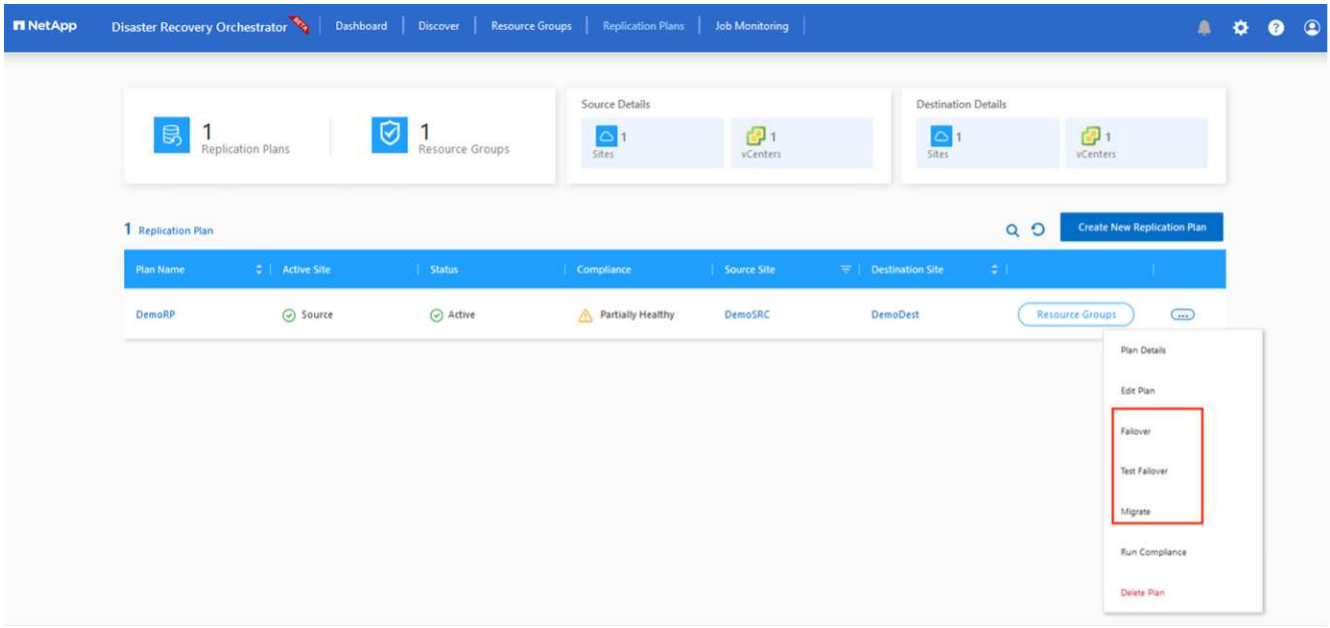


8. 在 VM 詳細資料下、您可以選擇性地調整 VM CPU 和 RAM 參數的大小。當您將大型環境恢復到較小的目標叢集、或是在執行災難恢復測試時、而不需要佈建一對一實體 VMware 基礎架構、這項功能將會非常有幫

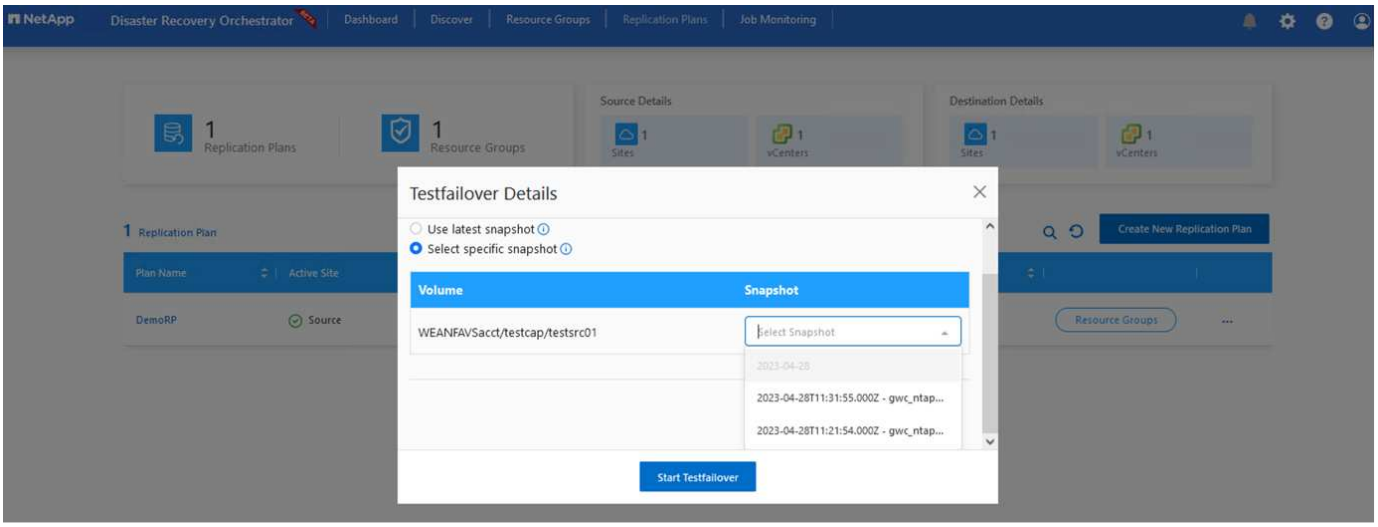
助。此外、也可修改資源群組中所有選定虛擬機器的開機順序和開機延遲（秒）。如果您在資源群組開機順序選擇期間所選取的項目需要任何變更、則還有其他選項可修改開機順序。根據預設、會使用在資源群組選擇期間所選的開機順序、但在此階段可以執行任何修改。



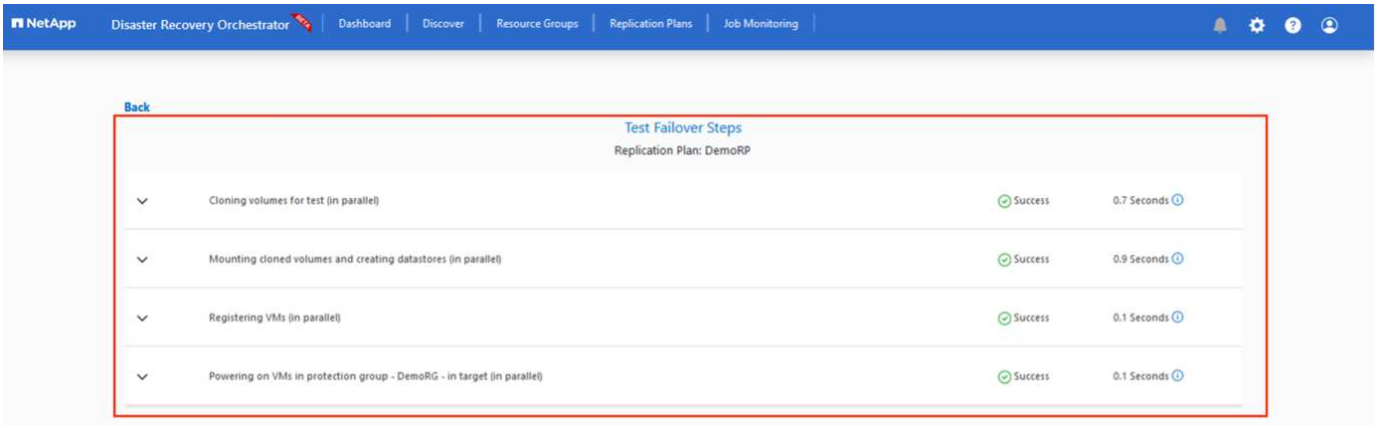
9. 按一下 * 建立複寫計畫 * 。建立複寫計畫之後、您可以根據需求來執行容錯移轉、測試容錯移轉或移轉選項。



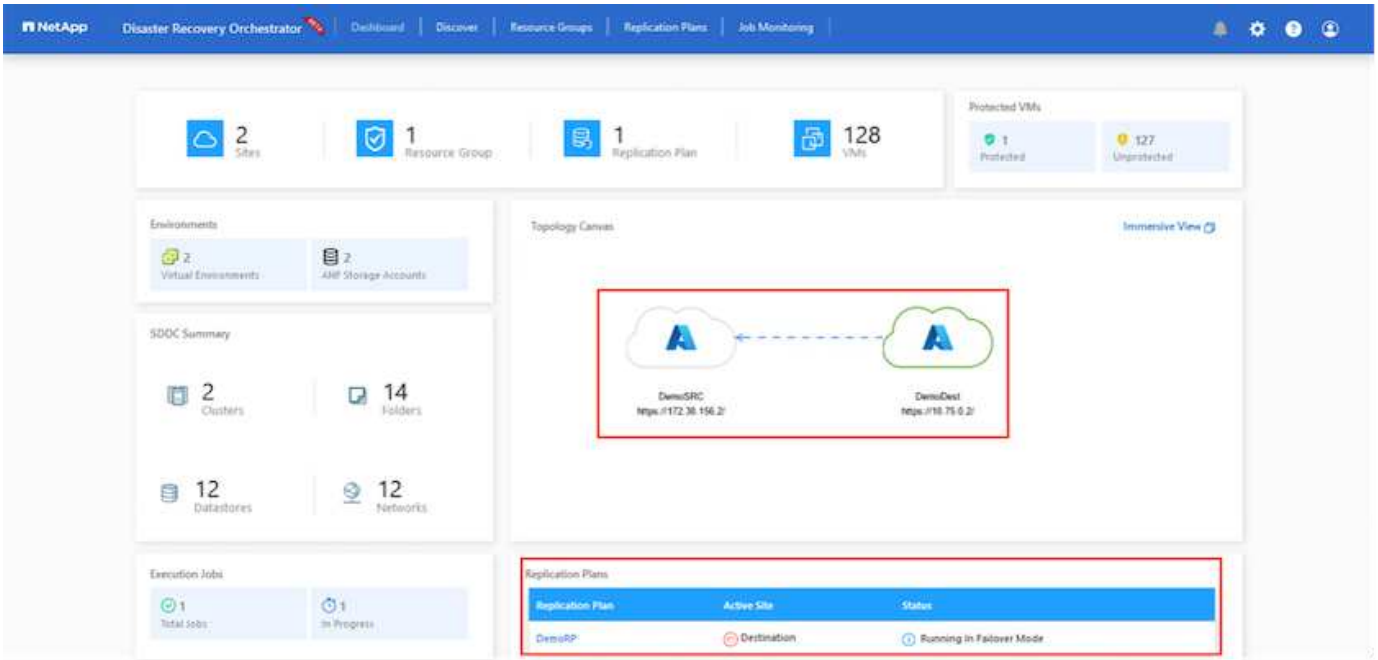
在容錯移轉和測試容錯移轉選項期間、會使用最新的快照、或是從時間點快照中選取特定的快照。如果您面臨勒索軟體等毀損事件、而最近的複本已經遭到入侵或加密、則時間點選項可能非常有用。DRO 會顯示所有可用的時間點。



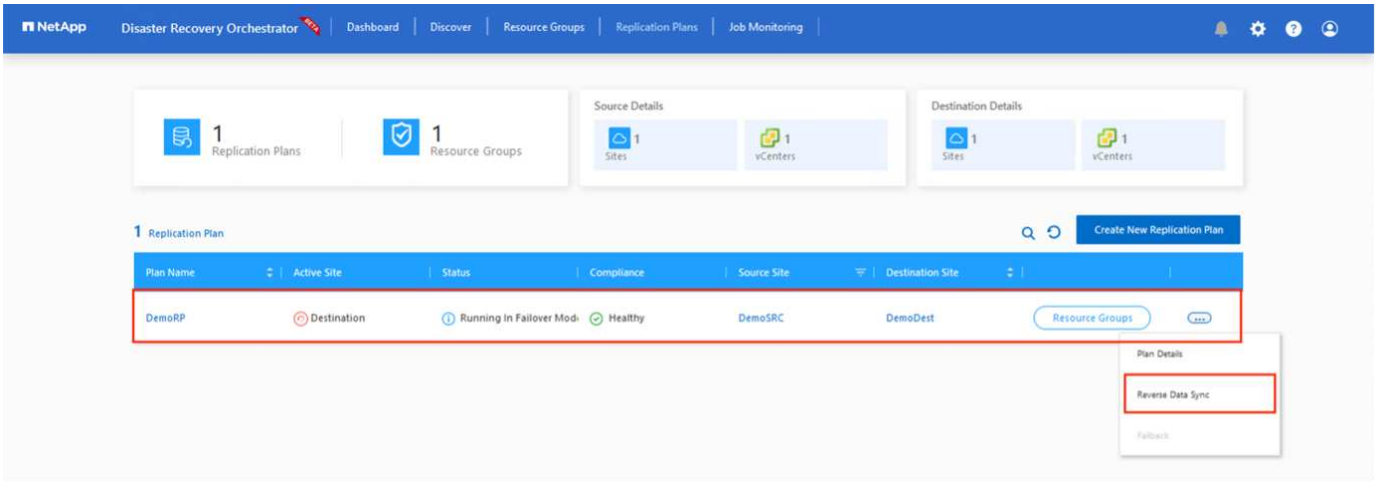
若要使用複寫計畫中指定的組態觸發容錯移轉或測試容錯移轉，您可以按一下 * 容錯移轉 * 或 * 測試容錯移轉 * 。您可以在工作功能表中監控複寫計畫。



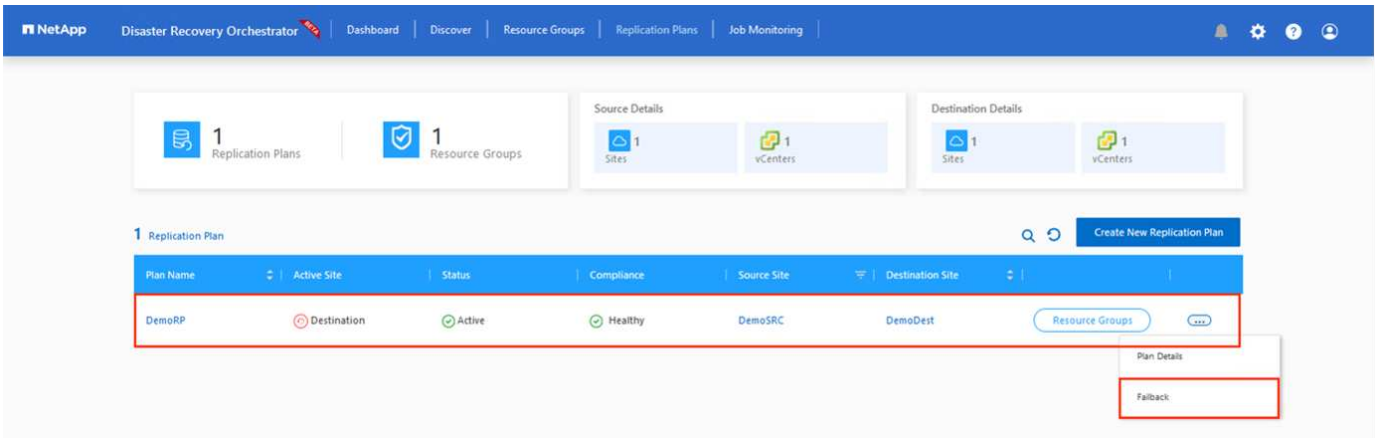
觸發容錯移轉後、可在次要站台 AVS SDDC vCenter （ VM 、網路和資料存放區）中看到復原的項目。依預設、 VM 會還原至 Workload 資料夾。

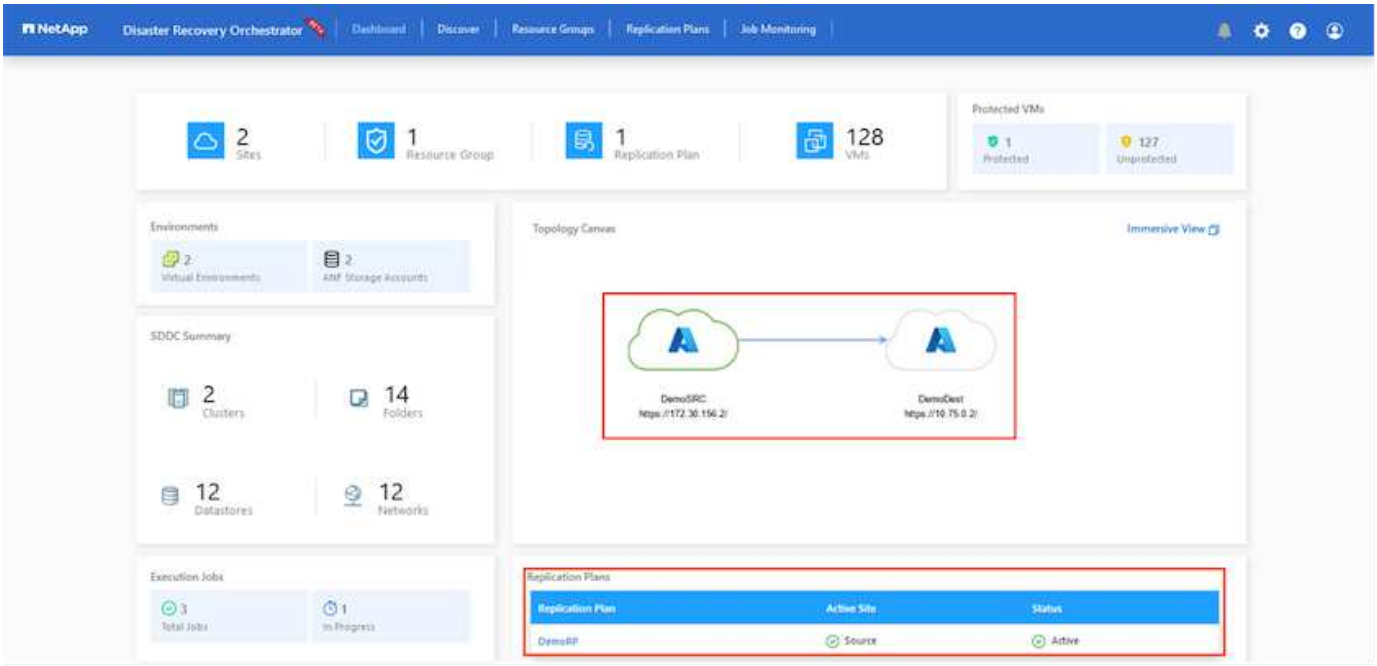


可在複寫計畫層級觸發容錯回復。在測試容錯移轉時、可使用「切紙」選項來回復變更並移除新建立的磁碟區。與容錯移轉相關的容錯回復是兩個步驟的程序。選取複寫計畫、然後選取 * 反轉資料同步 * 。



完成此步驟後、觸發容錯回復、以移回主要 AVS 站台。





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

勒索軟體恢復

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

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

結論

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

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

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- 為 Azure NetApp Files 建立 Volume 複寫

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

- Azure NetApp Files 磁碟區的跨區域複寫

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

- "Azure VMware解決方案"

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

- 在Azure上部署及設定虛擬化環境

  "在 Azure 上設定 AVS"

- 部署及設定 Azure VMware 解決方案

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

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

作者： Niyaz Mohamed - NetApp 解決方案工程

總覽

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

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

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

本文檔的用途

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

Veeam 備份與複寫是適用於虛擬環境的備份與複寫應用程式。複寫虛擬機器時、 Veeam 備份與複寫會從 AVS 複寫、軟體會在目標 AVS SDDC 叢集上以原生 VMware vSphere 格式建立 VM 的精確複本。 Veeam 備份與複

寫會將複本與原始 VM 保持同步。複寫可提供最佳的恢復時間目標（ RTO ）、因為災難恢復站台上有已掛載的 VM 複本處於就緒啟動狀態。

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

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

[]

解決方案部署

高階步驟

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

   以最小組態設定的試驗環境可用於災難恢復。發生事件時、 VM 會容錯移轉至此叢集、並可新增其他節點）。
3. 設定複寫工作、以使用 Veeam 備份與複寫建立 VM 複本。
4. 建立容錯移轉計畫並執行容錯移轉。
5. 災難事件完成且主站台正常運作後、切換回正式作業的 VM 。

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

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

如需其他資訊、請參閱涵蓋的「考量與限制」 "請按這裡"。

部署詳細資料

步驟 **1** ：複寫 **VM**

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

若要複寫 VM 、請依照下列步驟進行：

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

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

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

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

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

   []
10. 選擇複寫排程以定期執行複寫工作。

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

[]

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

[]

如需 Veeam 複寫的其他資訊、請參閱 "複寫的運作方式"

步驟 **2** ：建立容錯移轉計畫

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

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

只有在初始複寫完成且 VM 複本處於就緒狀態時、才能新增容錯移轉計畫。

執行容錯移轉計畫時可同時啟動的虛擬機器數量上限為 10 個

在容錯移轉過程中、來源 VM 將不會關閉

若要建立 * 容錯移轉計畫 * 、請執行下列步驟：

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

   []

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

   []

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

   []

如需建立複寫工作的其他資訊、請參閱 "建立複寫工作"。

步驟 3 ：執行容錯移轉計畫

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

請確定已建立網路區段、以避免容錯移轉期間發生 IP 衝突。

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

[]

[]

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

[]

容錯移轉完成後、 VM 的狀態會變更為「容錯移轉」。

[]

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

如需容錯移轉計畫的詳細資訊、請參閱 "容錯移轉計畫"。

步驟 **4** ：容錯回復至正式作業網站

當容錯移轉計畫執行時、它會被視為中間步驟、需要根據需求完成。選項包括：

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

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

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

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

[]

[]

[]

[]

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

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

[]

在容錯回復至正式作業後、虛擬機器都會還原回原始正式作業站台。

[]

結論

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

若要深入瞭解此程序、歡迎觀看詳細的逐步解說影片。

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

在 **Azure / AVS** 上移轉工作負載

TR-4940：**Azure NetApp Files** 使用**VMware HCX -**快速入門指南、將工作負載移轉至**VMware Infrastructure**資料存放區

作者：NetApp解決方案工程

總覽：使用**VMware HCX**、**Azure NetApp Files** 不含資料存放區和**Azure VMware**解決方案來移轉虛擬機器

Azure VMware解決方案與Azure NetApp Files VMware資料存放區最常見的使用案例之一、就是移轉VMware工作負載。VMware HCX是首選的選項、提供各種移轉機制、可將內部部署的虛擬機器（VM）及其資料移至Azure NetApp Files 各個資料存放區。

VMware HCX主要是一個移轉平台、其設計旨在簡化應用程式移轉、工作負載重新平衡、甚至是雲端之間的營運不中斷。它是Azure VMware解決方案私有雲的一部分、提供許多移轉工作負載的方法、可用於災難恢復（DR）作業。

本文件提供有關配置Azure NetApp Files VMware資料存放區的逐步指引、接下來是下載、部署及設定VMware HCX、包括內部部署及Azure VMware解決方案端的所有主要元件、包括互連、網路擴充及WAN最佳化、以啟用各種VM移轉機制。

VMware HCX可與任何資料存放區類型搭配使用、因為移轉作業是在VM層級進行。因此、本文件適用於目前打算以Azure NetApp Files Azure VMware解決方案部署VMware解決方案以實現具成本效益的VMware雲端部署的NetApp客戶和非NetApp客戶。

高階步驟

此清單提供在Azure雲端端安裝及設定HCX Cloud Manager、以及在內部部署安裝HCX Connector所需的高階步驟：

1. 透過Azure入口網站安裝HCX。
2. 在內部部署的VMware vCenter Server中下載並部署HCX Connector Open Virtualization Appliance（OVA）安裝程式。
3. 使用授權金鑰啟動HCX。
4. 將內部部署的VMware HCX Connector與Azure VMware解決方案HCX Cloud Manager配對。
5. 設定網路設定檔、運算設定檔和服務網格。
6. （選用）執行網路擴充、以避免在移轉期間重新取得IP。
7. 驗證應用裝置狀態、並確保可以進行移轉。
8. 移轉VM工作負載。

先決條件

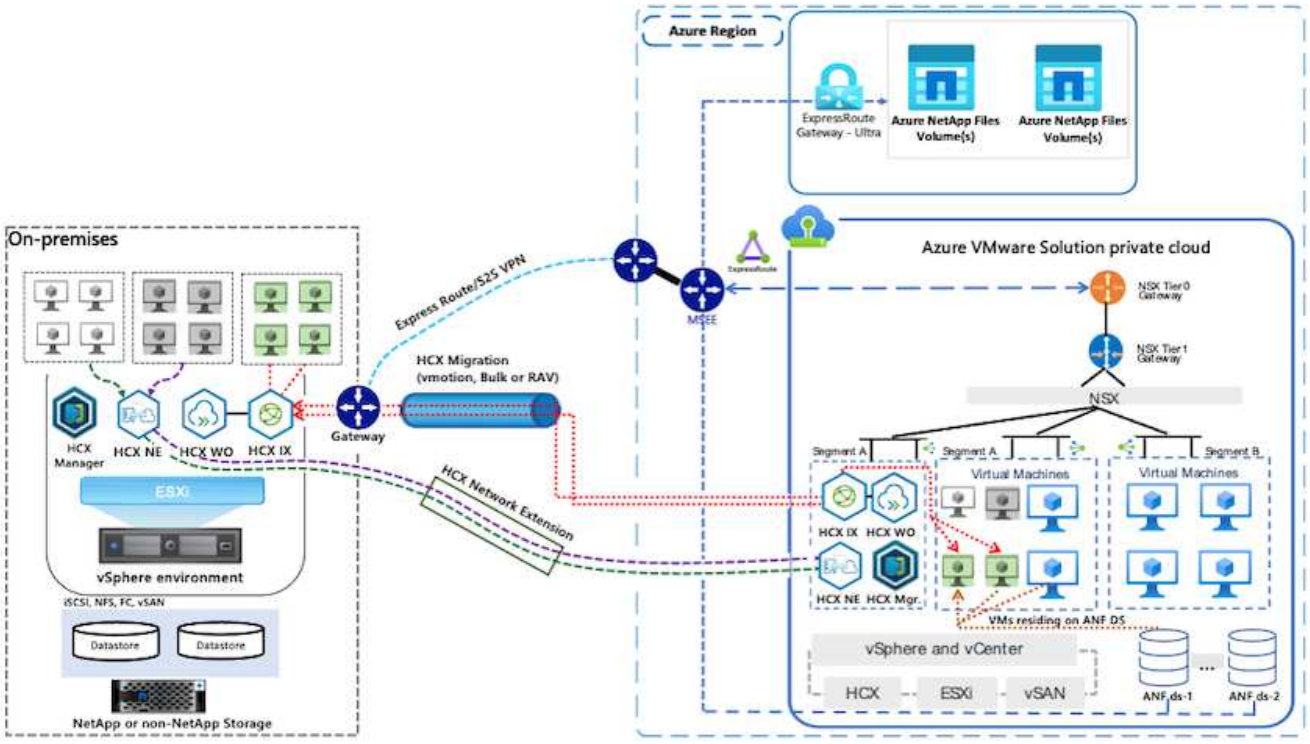
開始之前、請先確定符合下列先決條件。如需詳細資訊、請參閱 "連結"。在具備連線能力等先決條件之後、請從Azure VMware解決方案入口網站產生授權金鑰、以設定並啟動HCX。下載OVA安裝程式之後、請繼續執行下列安裝程序。

> HCx進階為預設選項、VMware HCX Enterprise版本也可透過支援票證取得、而且不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）、或使用此功能建立私有雲端 "NetApp連結" 或是這種情況 "Microsoft連結"。
- 若要從內部部署的VMware vSphere資料中心移轉VM及相關資料、需要從資料中心連線至SDDC環境。移轉工作負載之前、 "設定站台對站台VPN或Express路由全域連線連線" 在內部部署環境與各自私有雲端之間。
- 從內部部署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移轉VM。
- 請確定所需的 "防火牆規則和連接埠" 允許內部部署vCenter Server與SDDC vCenter之間的VMotion流量。在私有雲端上、預設會設定VMotion網路上的路由傳送。
- 應在Azure VMware解決方案中以資料存放區的形式掛載不適用的NFS Volume。Azure NetApp Files請依照本節詳細說明的步驟進行 "連結" 將Azure NetApp Files 不完整的資料存放區附加至Azure VMware解決方案主機。

高層架構

為了進行測試、此驗證所使用的內部部署實驗室環境是透過站台對站台VPN連線、因此可內部部署連線至Azure VMware解決方案。



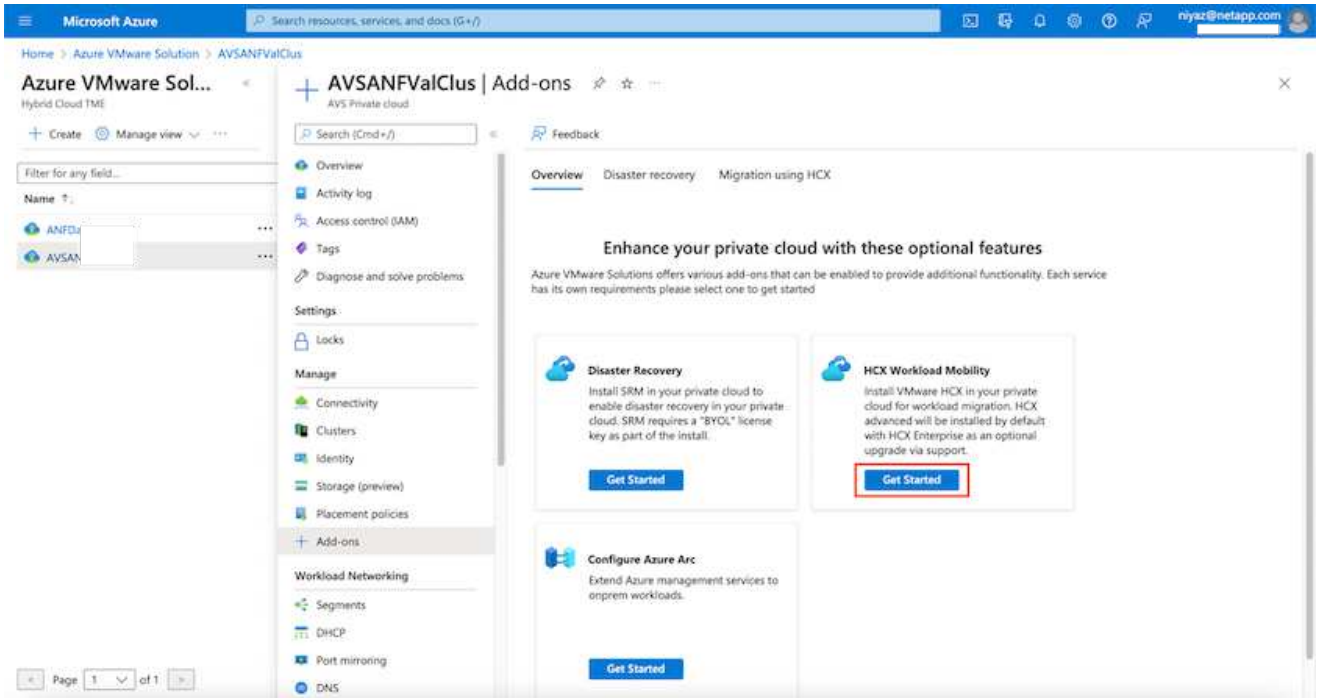
解決方案部署

請依照一系列步驟完成本解決方案的部署：

步驟1：使用附加元件選項透過Azure Portal安裝HCX

若要執行安裝、請完成下列步驟：

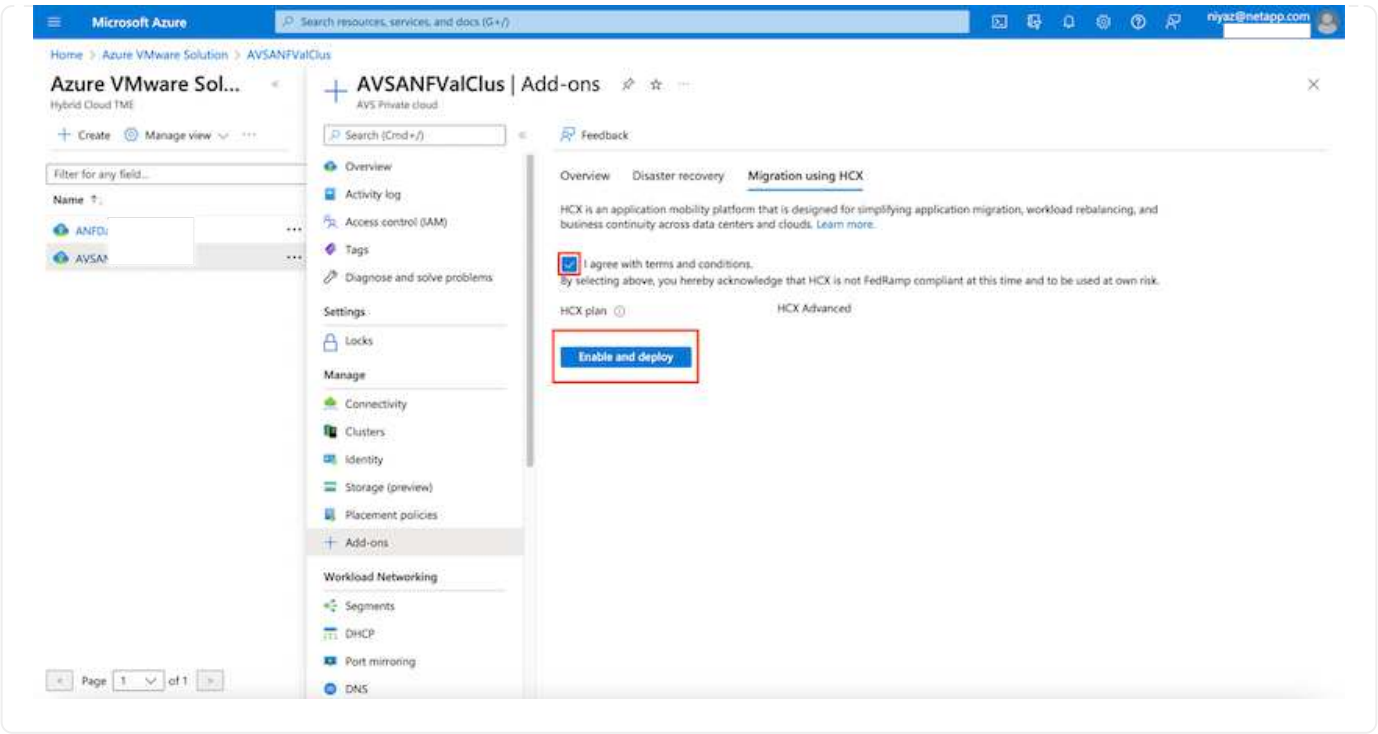
1. 登入Azure Portal並存取Azure VMware Solution私有雲。
2. 選取適當的私有雲並存取附加元件。您可以瀏覽至*管理>附加元件*來完成此作業。
3. 在「HCX工作負載行動性」區段中、按一下「入門」。



1. 選取「我同意條款與條件」選項、然後按一下「啟用與部署」。

預設部署為HCX Advanced。開啟支援要求以啟用Enterprise Edition。

部署約需25至30分鐘。


Microsoft Azure
Search resources, services, and docs (G+/)
niyaz@netapp.com
Home > Azure VMware Solution > AVSANFValClus
Azure VMware Sol...
Hybrid Cloud TME
Create
Manage view
Filter for any field...
Name
ANFDu
AVSAN
Page 1 of 1
AVSANFValClus | Add-ons
AVS Private cloud
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Clusters
Identity
Storage (preview)
Placement policies
Add-ons
Workload Networking
Segments
DHCP
Port mirroring
DNS
Feedback
Overview
Disaster recovery
Migration using HCX
HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. Learn more.
I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.
HCX plan
HCX Advanced
Enable and deploy

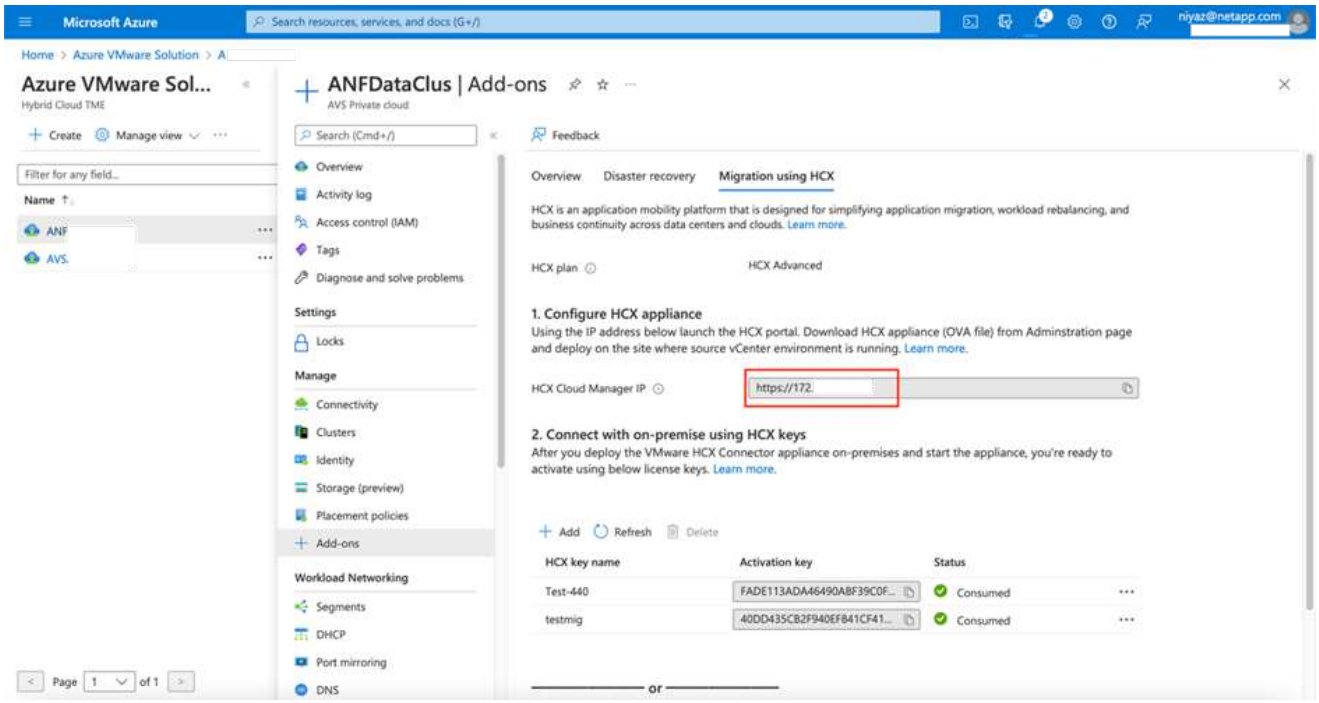
步驟2：在內部部署vCenter Server中部署安裝程式OVA

若要讓內部部署連接器連線至Azure VMware解決方案中的HCX Manager、請確定內部部署環境中已開啟適當的防火牆連接埠。

若要在內部部署vCenter Server中下載並安裝HCX Connector、請完成下列步驟：

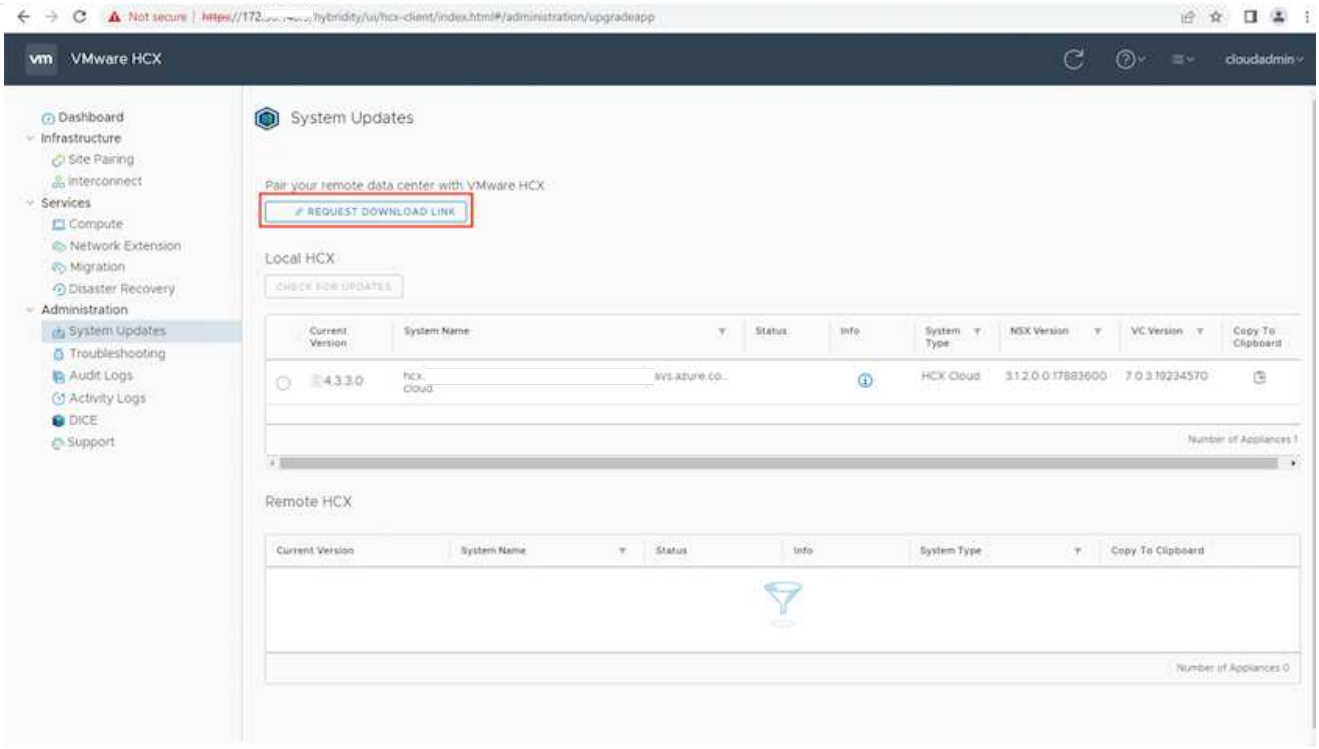
1. 從Azure入口網站、前往Azure VMware解決方案、選取私有雲、然後選取*管理>附加元件>使用HCX移轉*、然後複製HCX Cloud Manager入口網站、即可下載OVA檔案。

使用預設的CloudAdmin使用者認證資料來存取HCX入口網站。

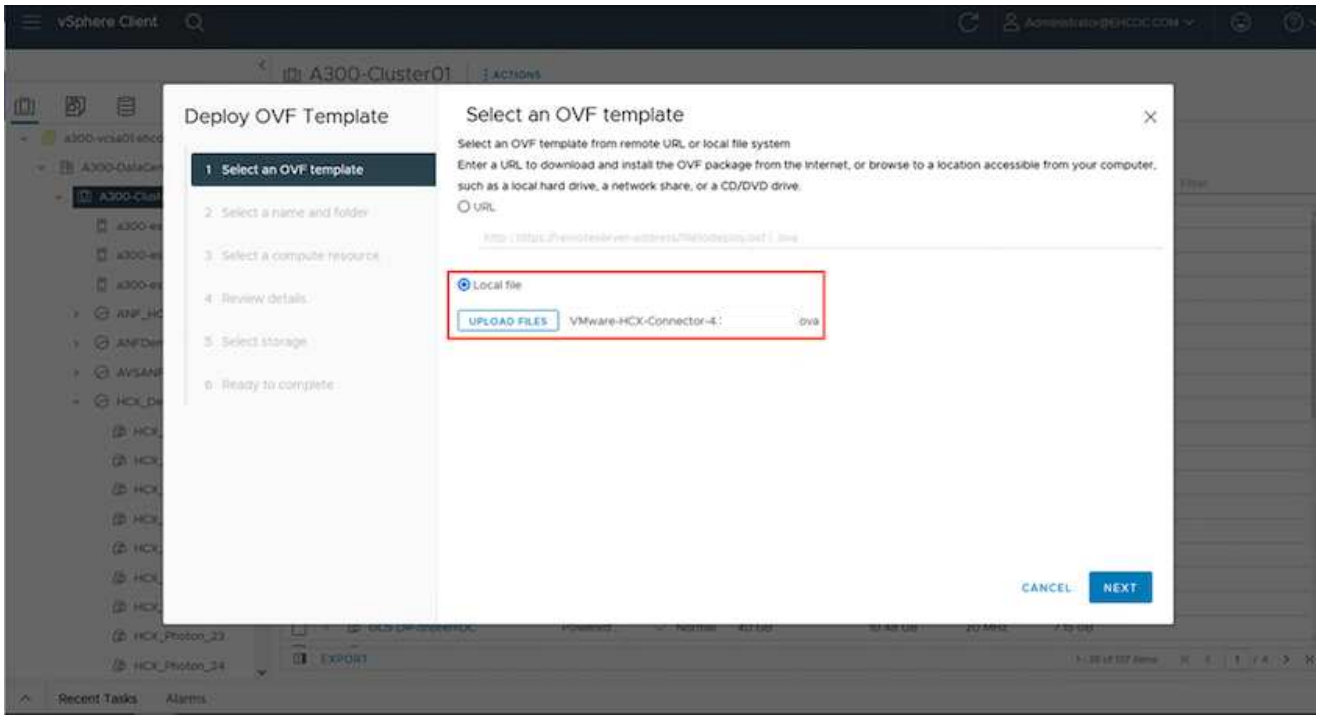


1. 使用jumphost、以mailto：cloudadmin@vple.1[cloudadmin@vplore.erl]存取HCX入口網站之後、請瀏覽至*管理>系統更新*、然後按一下*要求下載連結*。

下載或複製OVA連結、然後貼到瀏覽器中、開始下載VMware HCX Connector OVA檔案、以便部署在內部部署vCenter Server上。



1. 下載OVA之後、請使用*部署OVF範本*選項、將其部署至內部部署的VMware vSphere環境。



1. 輸入OVA部署的所有必要資訊、按一下*「下一步」、然後按一下「*完成」以部署VMware HCX連接器OVA。

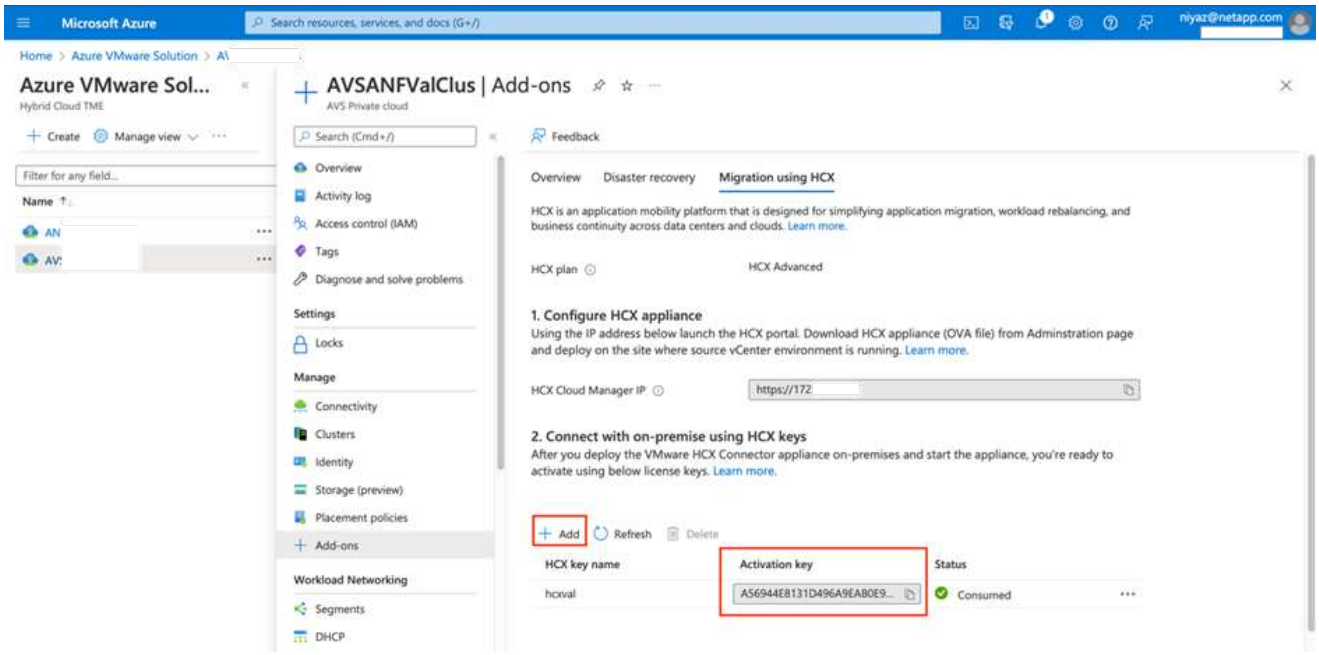
手動啟動虛擬應用裝置。

如需逐步指示、請參閱 "VMware HCX使用者指南"。

步驟3：使用授權金鑰啟動**HCX Connector**

在內部部署VMware HCX Connector OVA並啟動應用裝置之後、請完成下列步驟以啟動HCX Connector。從Azure VMware解決方案入口網站產生授權金鑰、並在VMware HCX Manager中啟動。

1. 從Azure入口網站、前往Azure VMware解決方案、選取私有雲、然後選取*管理>附加元件>使用HCX*移轉。
2. 在「使用**HCX**金鑰與內部部署連線」下、按一下「新增」、然後複製啟動金鑰。



每個部署的內部部署HCX Connector都需要個別的金鑰。

1. 登入內部部署的VMware HCX Manager、網址為 "https://hcxmanagerIP:9443" 使用系統管理員認證。

使用在OVA部署期間定義的密碼。

1. 在授權中、輸入從步驟3複製的金鑰、然後按一下「啟動」。

內部部署的HCX Connector應可存取網際網路。

1. 在*資料中心位置*下、提供最接近內部部署VMware HCX Manager的安裝位置。按一下 * 繼續 * 。
2. 在*系統名稱*下、更新名稱、然後按一下*繼續*。
3. 按一下*是、繼續*。
4. 在「連線您的**VCenter**」下、提供vCenter Server的完整網域名稱（FQDN）或IP位址、以及適當的認證資料、然後按一下「繼續」。

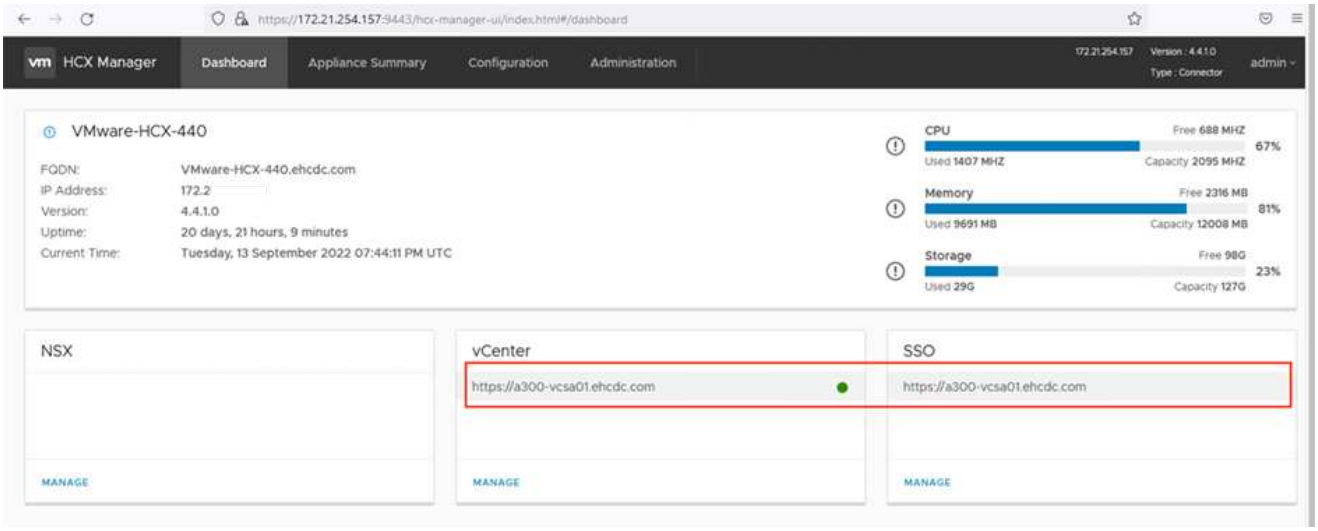
使用FQDN以避免稍後發生連線問題。

1. 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。

1. 驗證輸入的資訊是否正確、然後按一下*重新啟動*。
2. 服務重新啟動後、vCenter Server會在顯示的頁面上顯示為綠色。vCenter Server和SSO都必須具有適當的組態參數、此參數應與上一頁相同。

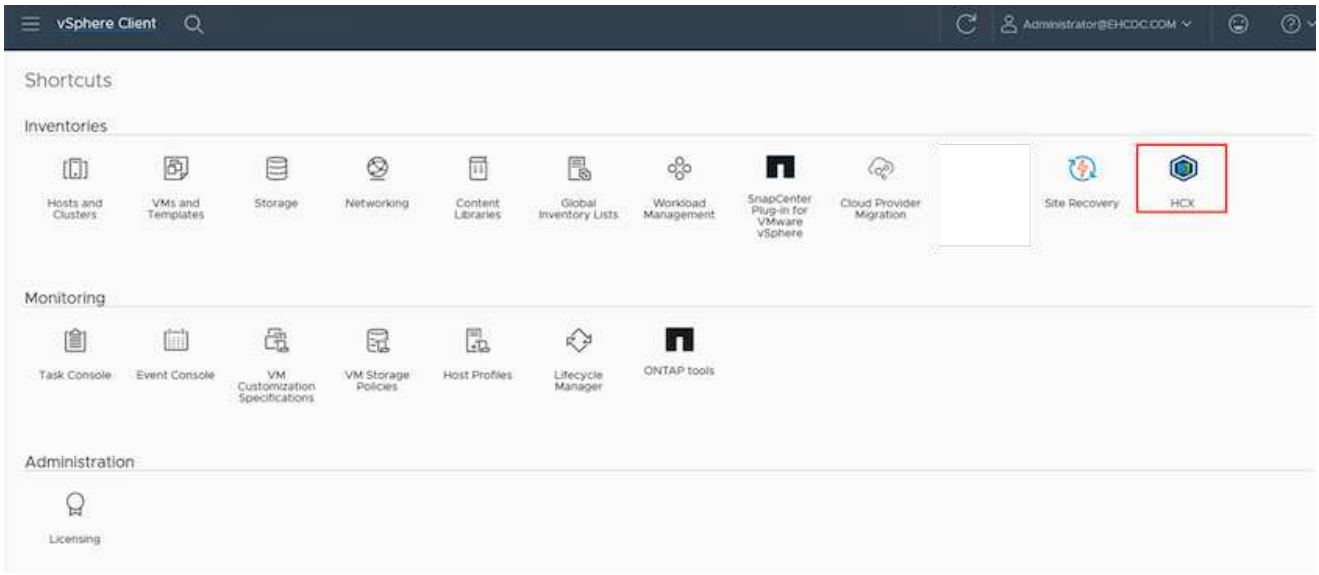
此程序大約需要10到20分鐘、而外掛程式則要新增至vCenter Server。



步驟4：將內部部署的VMware HCX Connector與Azure VMware解決方案HCX Cloud Manager配對

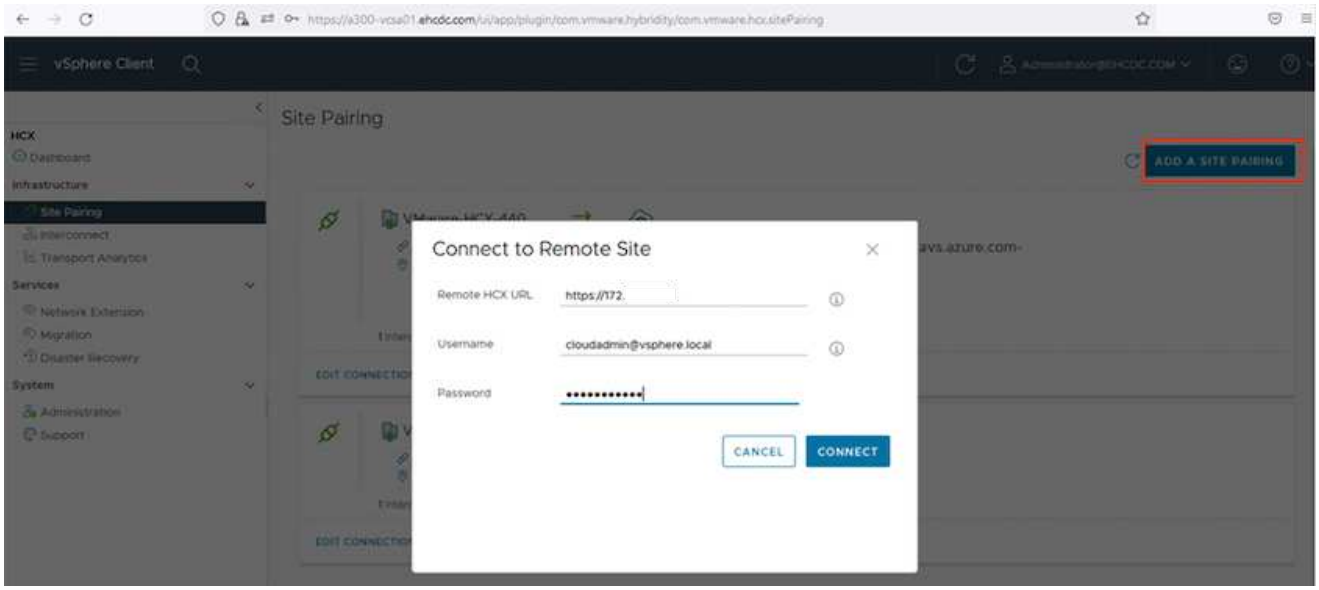
在內部部署和Azure VMware解決方案中安裝HCX Connector之後、請新增配對、以設定內部部署的VMware HCX Connector for Azure VMware Solution私有雲。若要設定站台配對、請完成下列步驟：

1. 若要在內部部署的vCenter環境與Azure VMware Solution SDDC之間建立站台配對、請登入內部部署的vCenter Server、然後存取新的HCX vSphere Web Client外掛程式。



1. 按一下「基礎架構」下的「新增站台配對」。

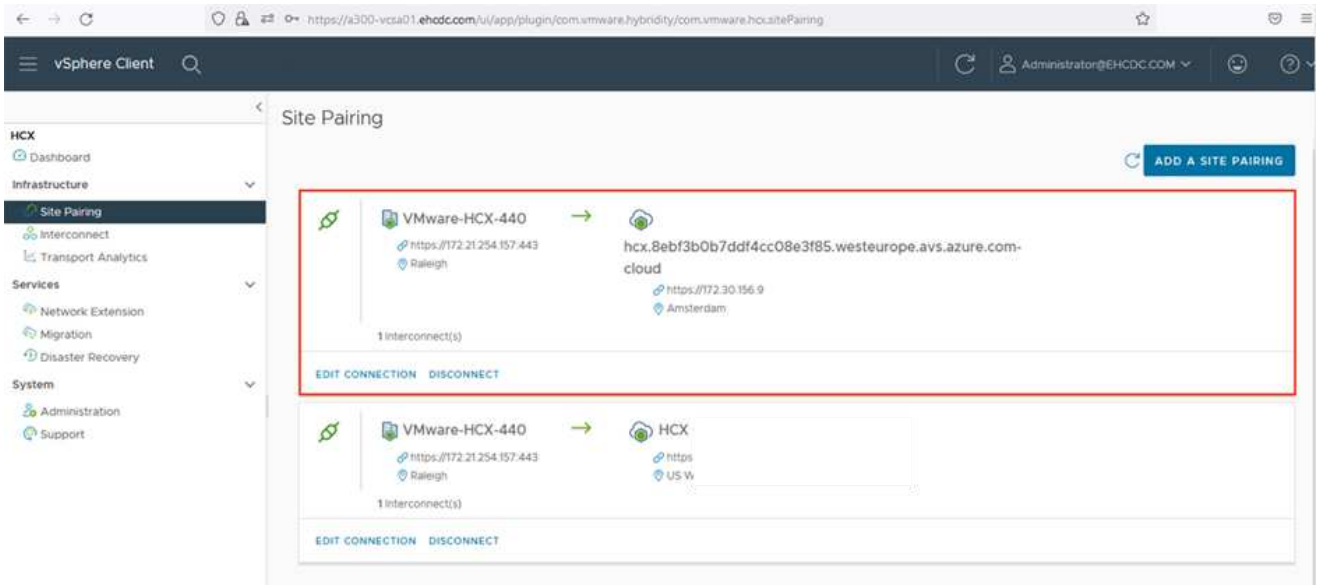
輸入Azure VMware Solution HCX Cloud Manager URL或IP位址、以及CloudAdmin角色存取私有雲端的認證資料。



1. 按一下「連線」。

VMware HCX Connector必須能夠透過連接埠443路由傳送至HCX Cloud Manager IP。

1. 建立配對之後、即可在HCX儀表板上取得新設定的站台配對。

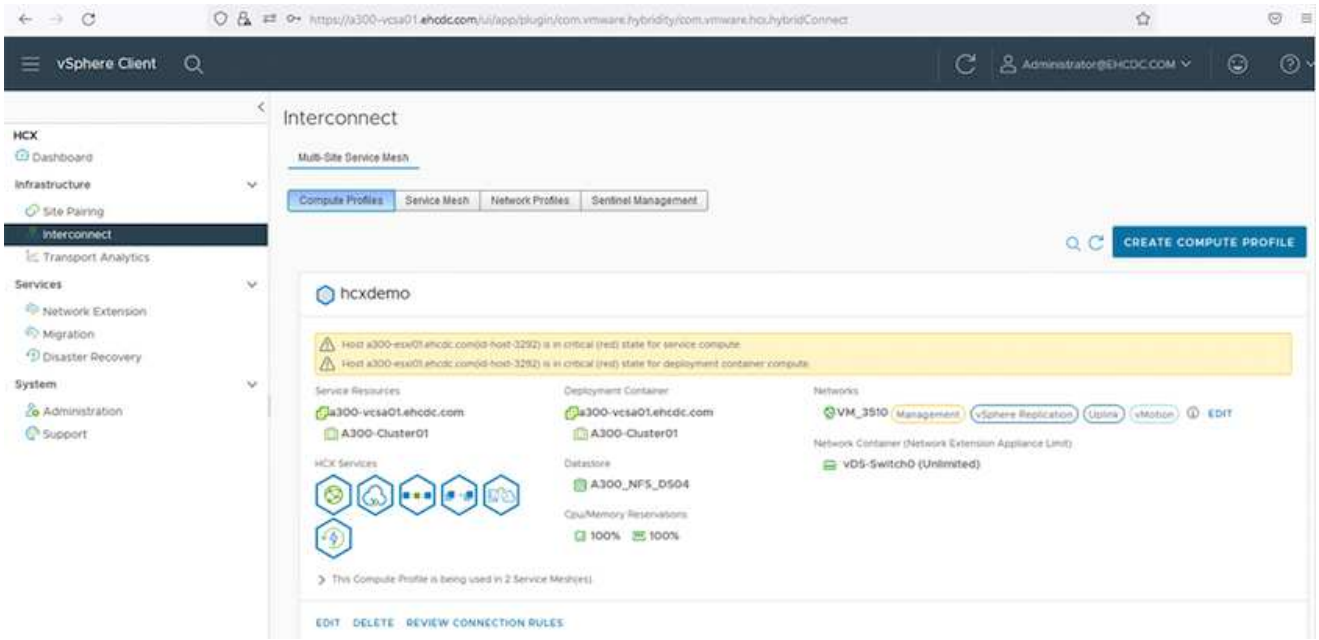


步驟**5**：設定網路設定檔、運算設定檔和服務網格

VMware HCX互連服務應用裝置可透過網際網路提供複寫及vMotion型移轉功能、並可透過私有連線連至目標站台。互連可提供加密、流量工程及VM行動性。若要建立互連服務應用裝置、請完成下列步驟：

1. 在「基礎架構」下、選取「互連>多站台服務網狀架構>運算設定檔」>「建立運算設定檔」。

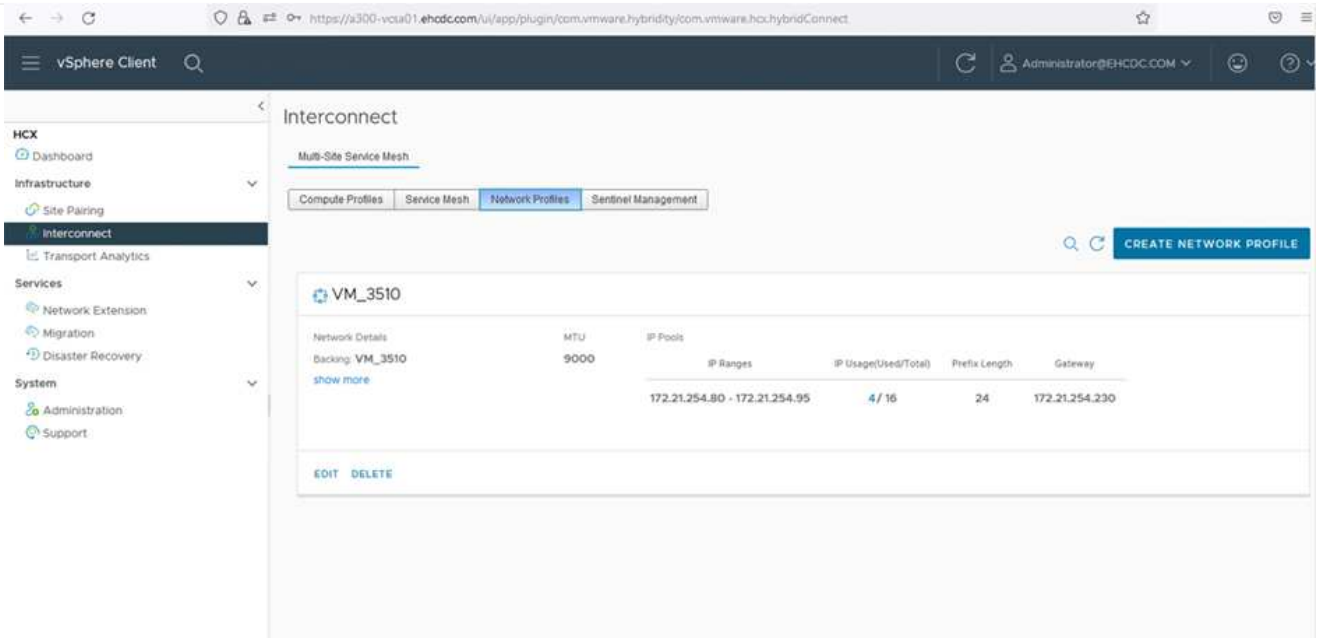
運算設定檔定義部署參數、包括部署的應用裝置、以及HCX服務可存取的VMware資料中心部分。



1. 建立運算設定檔之後、選取*多站台服務網格>網路設定檔>建立網路設定檔*、即可建立網路設定檔。

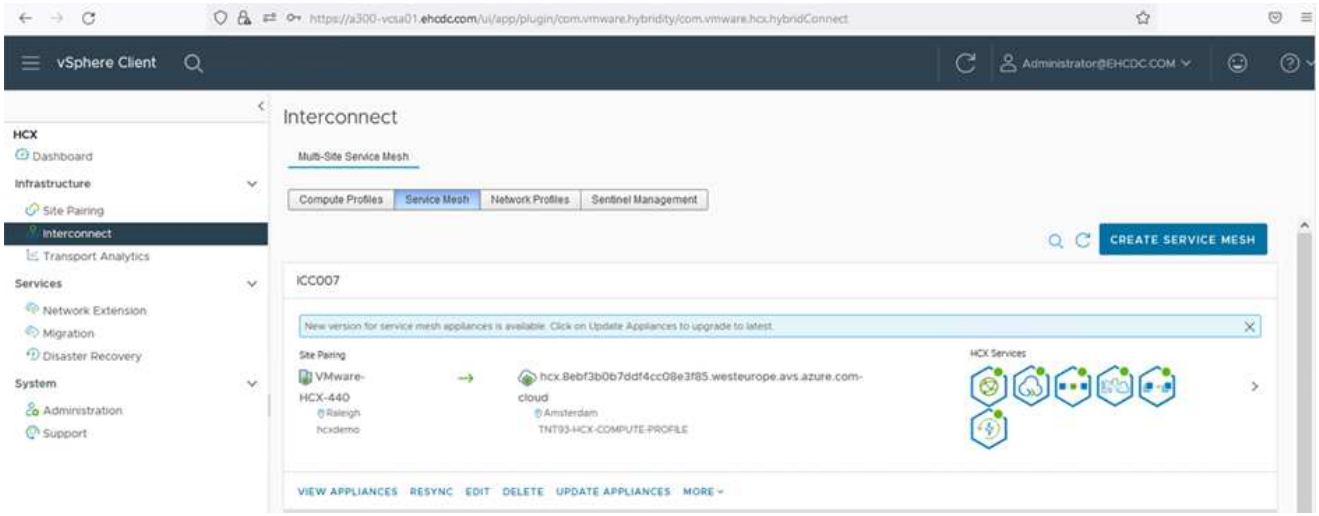
網路設定檔會定義一系列的IP位址和網路、以供HCX用於其虛擬應用裝置。

此步驟需要兩個以上的IP位址。這些IP位址會從管理網路指派給互連設備。

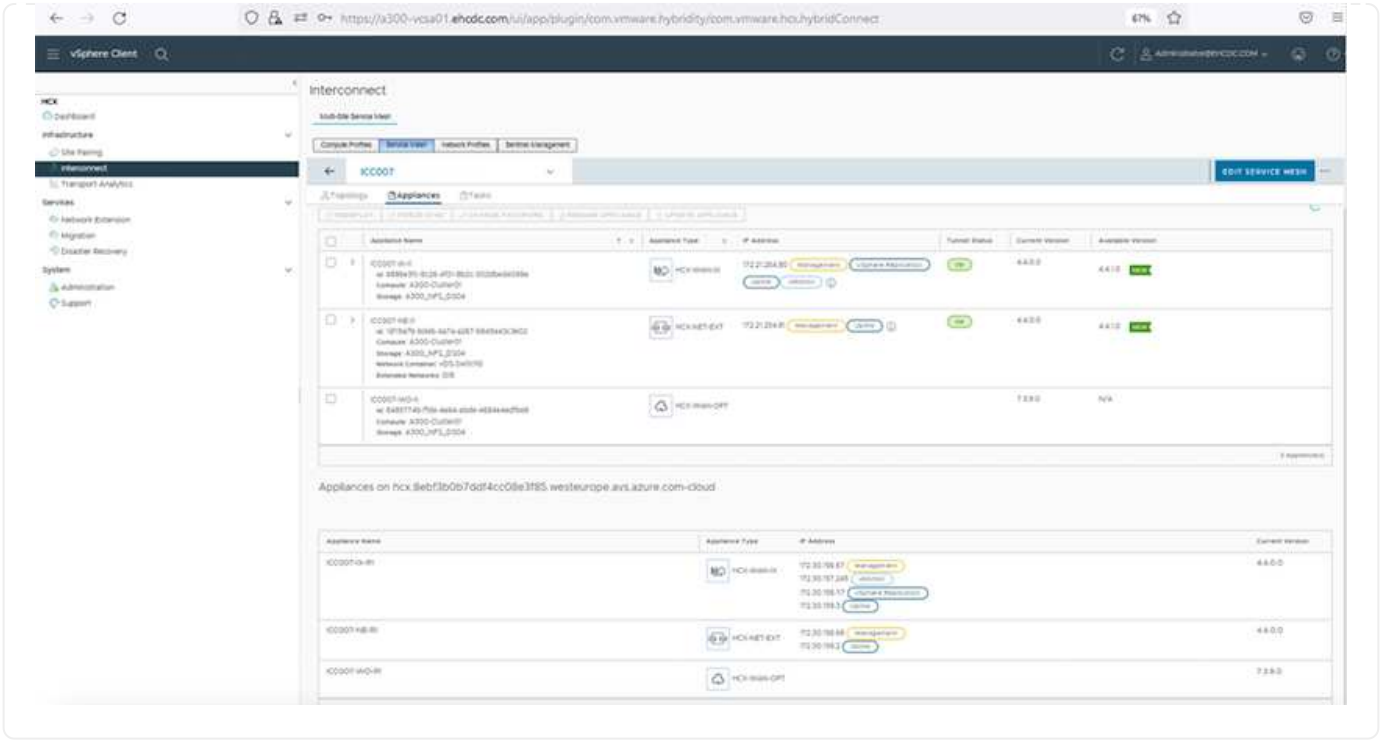


1. 目前、運算和網路設定檔已成功建立。
2. 選取「互連」選項中的「服務網格」索引標籤、然後選取內部部署和Azure SDDC站台、即可建立服務網格。
3. Service Mesh會指定本機和遠端運算和網路設定檔配對。

在此程序中、會在來源和目標站台上部署並自動設定HCX應用裝置、以建立安全的傳輸架構。



1. 這是組態的最後一步。完成部署需要將近30分鐘的時間。設定好服務網格後、環境就能準備好、成功建立IPsec通道來移轉工作負載VM。


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

步驟**6**：移轉工作負載

使用各種VMware HCX移轉技術、可在內部部署與Azure SDDC之間雙向移轉工作負載。VM可以使用多種移轉技術（例如HCX大量移轉、HCX vMotion、HCX冷移轉、HCX複寫輔助vMotion（適用於HCX Enterprise Edition）、以及HCX OS輔助移轉）（適用於HCX Enterprise Edition）、在VMware HCX啟動的實體之間移動。

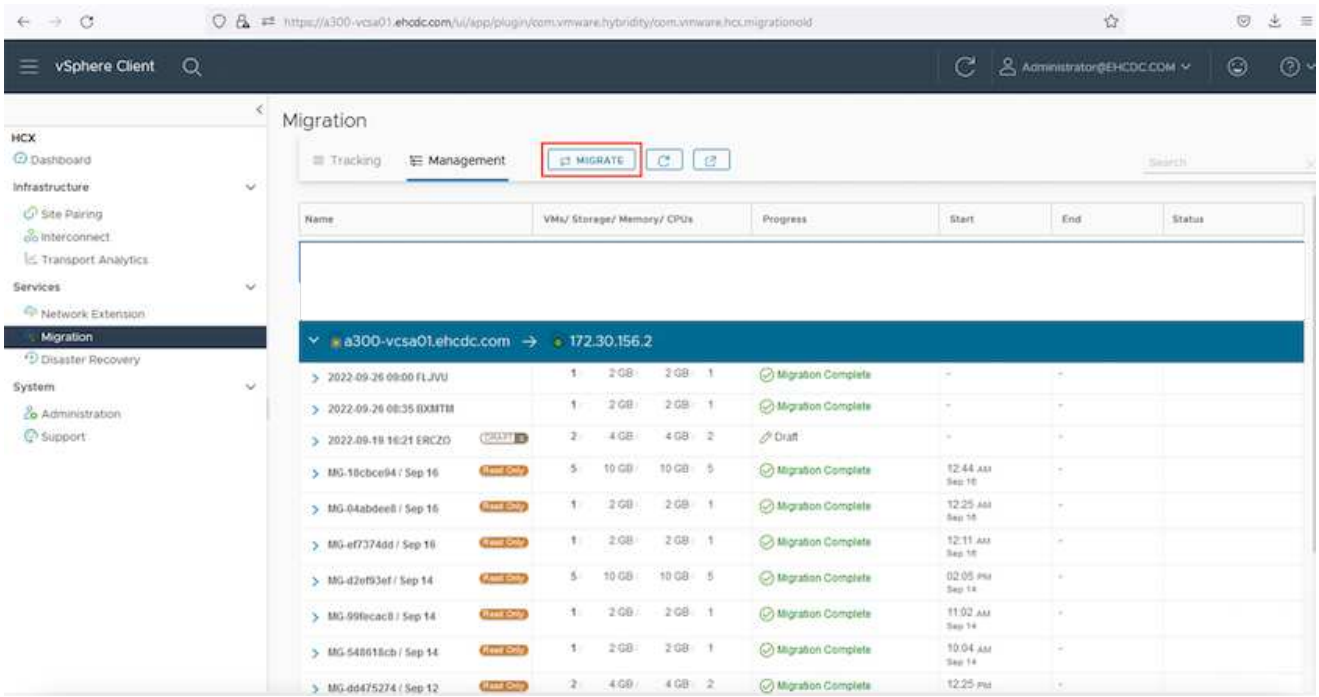
若要深入瞭解各種HCX移轉機制、請參閱 "VMware HCX移轉類型"。

大量移轉

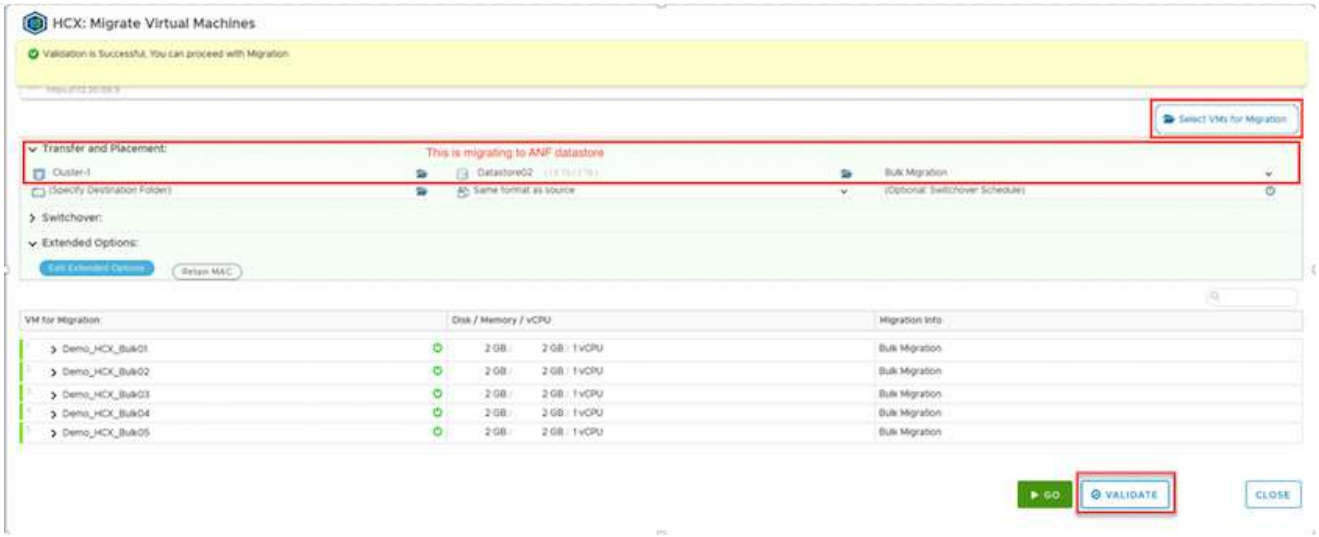
本節詳細說明大量移轉機制。在大量移轉期間、HCX的大量移轉功能會使用vSphere Replication移轉磁碟檔案、同時在目的地vSphere HCX執行個體上重新建立VM。

若要啟動大量VM移轉、請完成下列步驟：

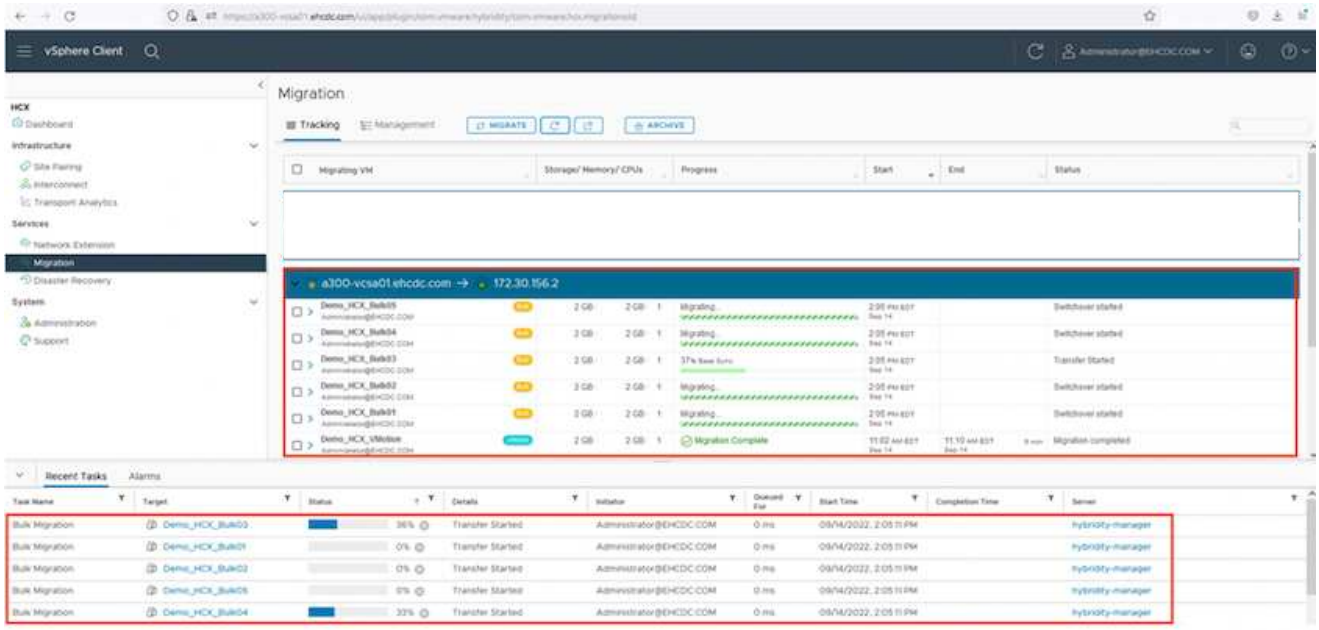
1. 存取*服務>移轉*下的*移轉*索引標籤。



1. 在*遠端站台連線*下、選取遠端站台連線、然後選取來源和目的地。在此範例中、目的地是Azure VMware解決方案SDDC HCX端點。
2. 按一下*選取要移轉的VM 。這會提供所有內部部署**VM**的清單。根據**MATCH**：**Value**運算式選取**VM**、然後按一下 Add*。
3. 在*傳輸與放置*區段中、更新必要欄位（叢集、儲存、目的地*和*網路）、包括移轉設定檔、然後按一下*驗證*。

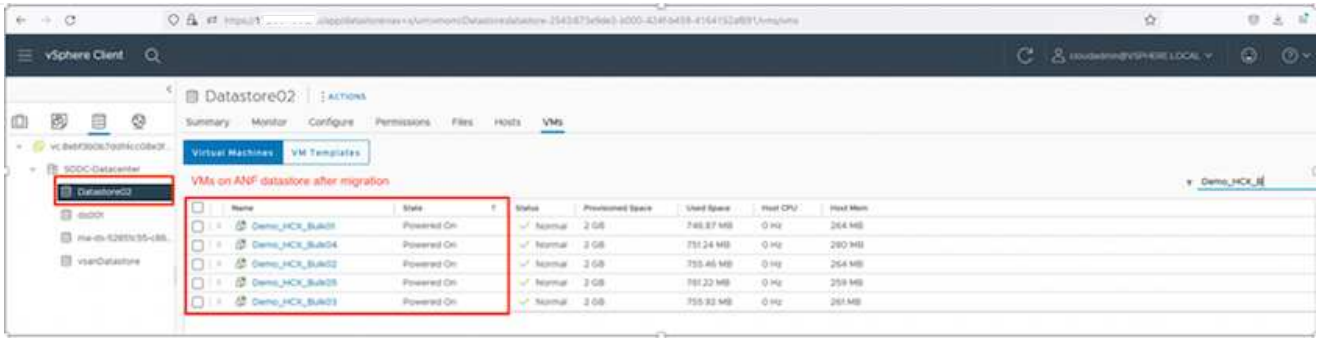


1. 驗證檢查完成後、按一下「執行」以啟動移轉。



在此移轉期間、Azure NetApp Files 會在目標vCenter內的指定支援資料存放區上建立一個預留位置磁碟、以便將來源VM磁碟的資料複寫到預留位置磁碟。觸發HGR以與目標進行完整同步、並在基準完成後、根據恢復點目標（RPO）週期執行遞增同步。完成完整/遞增同步後、除非設定特定排程、否則系統會自動觸發切換。

1. 移轉完成後、請存取目的地SDDC vCenter以驗證相同項目。

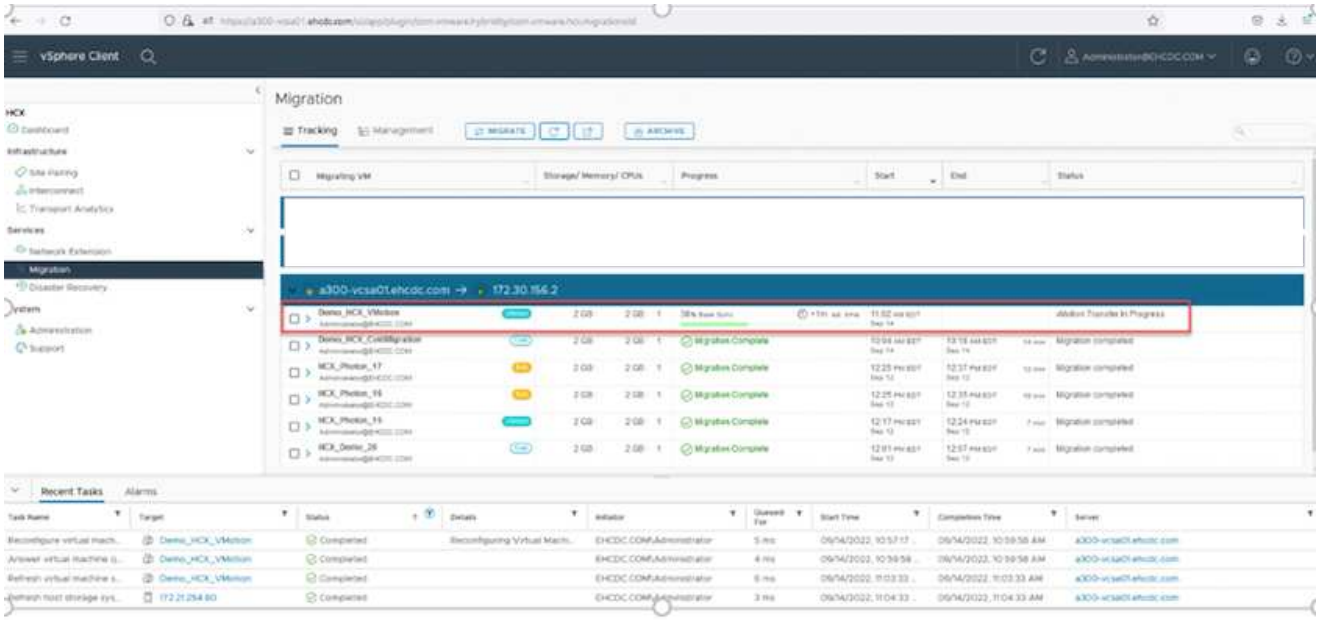


如需各種移轉選項的其他詳細資訊、以及如何使用HCX將工作負載從內部部署移轉至Azure VMware解決方案、請參閱 "VMware HCX使用者指南"。

若要深入瞭解此程序、歡迎觀看下列影片：

使用 HCX 移轉工作負載

以下是HCX vMotion選項的快照。



若要深入瞭解此程序、歡迎觀看下列影片：

HCx VMotion

請確定有足夠的頻寬可供處理移轉作業。

目標ANF資料存放區應有足夠空間來處理移轉作業。

結論

無論您的目標是全雲端或混合雲、或是內部部署中任何類型/廠商儲存設備上的資料、Azure NetApp Files 無論是部署或移轉應用程式工作負載、都能提供絕佳的選項、同時將資料需求無縫移轉至應用程式層、進而降

低TCO。無論使用案例為何、請選擇Azure VMware解決方案搭配Azure NetApp Files VMware解決方案、以快速實現雲端效益、一致的基礎架構、以及跨內部部署和多個雲端的作業、工作負載的雙向可攜性、以及企業級容量和效能。使用VMware vSphere複寫、VMware VMotion、甚至是網路檔案複本（NFC）來連接儲存設備及移轉VM的程序與程序、都是相當熟悉的程序。

重點摘要

本文件的重點包括：

- 您現在可以在Azure NetApp Files Azure VMware解決方案SDDC上使用效能不實的資料存放區。
- 您可以輕鬆地將資料從內部部署移轉至Azure NetApp Files 不受資料保護的資料存放區。
- 您可以輕鬆擴充及縮減Azure NetApp Files 整個VMware資料存放區、以滿足移轉活動期間的容量和效能需求。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請參閱下列網站連結：

- Azure VMware解決方案文件

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

- 本文檔 Azure NetApp Files

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

- VMware HCX使用者指南

"https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

區域可用度：**Anf**的補充**NFS**資料存放區

Azure / AVS上補充NFS資料存放區的可用度由Microsoft定義。首先、您需要判斷AVS和ANF是否在特定地區提供。接下來、您需要判斷該區域是否支援ANF補充NFS資料存放區。

- 查看AVS和ANF的可用度 "請按這裡"。
- 檢查ANF補充NFS資料存放區的可用度 "請按這裡"。

適用於**Google Cloud Platform GCVE**的**NetApp**功能

深入瞭解 NetApp 提供給 Google Cloud Platform （ GCP ） Google Cloud VMware Engine （ GCVE ）的功能：從 NetApp 作為來賓連線儲存設備、或是輔助 NFS 資料存放區、移轉工作流程、擴充 / 突增至雲端、備份 / 還原及災難恢復。

從下列選項中選取、跳至所需內容的區段：

- "在GCP中設定GCVE"

- "適用於GCVE的NetApp儲存選項"
- "NetApp / VMware雲端解決方案"

在**GCP**中設定**GCVE**

如同內部部署、規劃雲端型虛擬化環境對於成功建立虛擬機器和移轉的正式作業就緒環境來說、是非常重要的。

本節說明如何設定及管理GCVE,並搭配可用的選項來連接NetApp儲存設備。

客體內儲存設備是唯一支援的方法、可將Cloud Volumes ONTAP 「效益」和「雲端Volume服務」連線至GCVE.

設定程序可分為下列步驟：

- 部署及設定GCVE
- 啟用對GCVE的私有存取

檢視詳細資訊 "GCVE.的組態步驟"。

適用於**GCVE**的**NetApp**儲存選項

NetApp儲存設備可在GCP GCVG內以多種方式使用、無論是作為猜測連接或作為補充NFS資料存放區。

請造訪 "支援的NetApp儲存選項" 以取得更多資訊。

Google Cloud支援下列組態的NetApp儲存設備：

- 以客體連線儲存設備形式提供的資訊（CVO）Cloud Volumes ONTAP
- 以客體連線儲存設備的形式提供資訊（CVS）Cloud Volumes Service
- 作爲NFS補充資料存放區的CVS Cloud Volumes Service

檢視詳細資訊 "GCVE的來賓連線儲存選項"。

深入瞭解 "NetApp Cloud Volumes Service 支援Google Cloud VMware Engine的資料儲存區（NetApp部落格）" 或 "如何使用NetApp CVS做為Google Cloud VMware Engine的資料存放區（Google部落格）"

解決方案使用案例

有了NetApp和VMware雲端解決方案、在Azure AVS中部署的許多使用案例都很簡單。系統會針對VMware定義的每個雲端領域定義SE案例：

- 保護（包括災難恢復和備份/還原）
- 延伸
- 移轉

"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** 複寫、實現應用程式一致的災難恢復

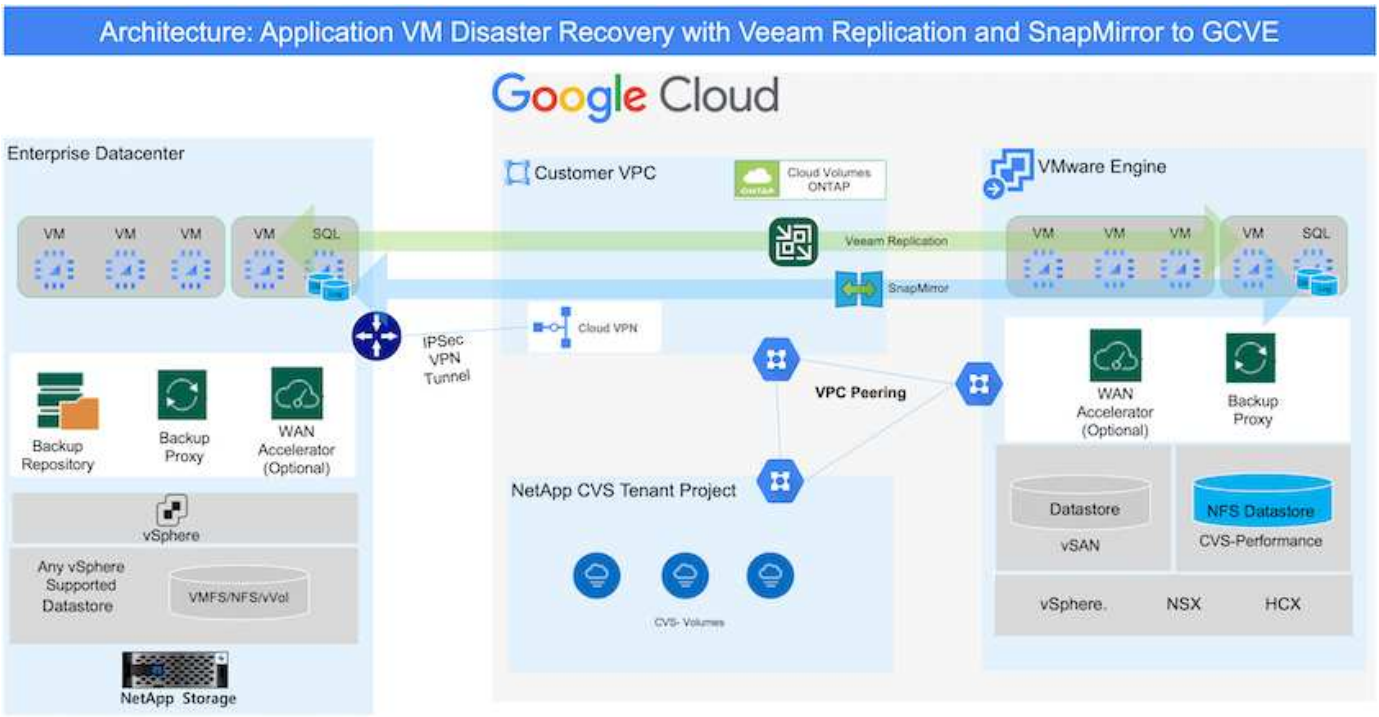
作者：NetApp Suresh ThopPay

總覽

許多客戶都在尋找一套有效的災難恢復解決方案、以供其在 VMware vSphere 上代管的應用程式 VM 使用。其中許多使用現有的備份解決方案來在災難恢復期間執行恢復。
該解決方案多次增加 RTO 、但未能達到他們的期望。為了降低 RPO 和 RTO 、只要有適當權限的網路連線能力和環境、就能在內部部署到 GCVE 之間使用 Veeam VM 複寫。
注意： Veeam VM Replication 無法保護 VM 來賓連接的儲存裝置、例如 iSCSI 或 NFS 裝載在來賓 VM 內。需要分別保護這些資料。

為了針對 SQL VM 進行應用程式一致的複寫、並降低 RTO 、我們使用 SnapCenter 來協調 SQL 資料庫和記錄磁碟區的 SnapMirror 作業。

本文件提供逐步方法、以設定及執行使用NetApp SnapMirror、Veeam及Google Cloud VMware Engine（GCVE）的災難恢復。



假設

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

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

若要在內部部署環境與Google Cloud網路之間建立連線、請使用專屬互連或Cloud VPN等連線選項。應根據內部部署的VLAN設計來建立區段。

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

部署災難恢復解決方案

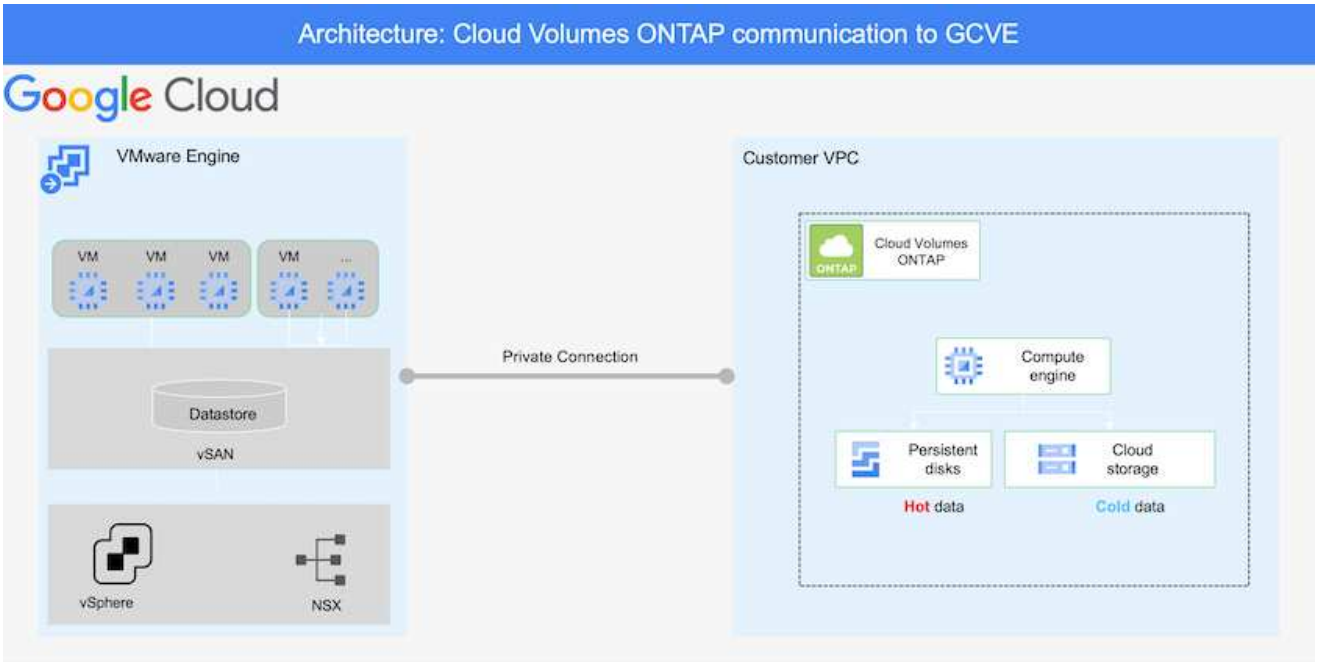
解決方案部署總覽

1. 確保應用程式資料是以SnapCenter 不必要的RPO要求使用支援功能進行備份。
2. 在適當的訂閱和虛擬網路中、使用 BlueXP 以正確的執行個體大小來佈建 Cloud Volumes ONTAP 。
   a. 為相關的應用程式磁碟區設定SnapMirror。
   b. 更新SnapCenter 中的備份原則、以便在排程工作之後觸發SnapMirror更新。
3. 安裝Veeam軟體、並開始將虛擬機器複寫至Google Cloud VMware Engine執行個體。
4. 在災難事件期間、使用 BlueXP 中斷 SnapMirror 關係、並使用 Veeam 觸發虛擬機器的容錯移轉。
   a. 重新連接應用程式VM的iSCSI LUN和NFS掛載。
   b. 將應用程式上線。
5. 在主站台恢復後、透過反向重新同步SnapMirror來叫用容錯回復至受保護站台。

部署詳細資料

在Google Cloud上設定CVO、並將磁碟區複寫至CVO

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



如需設定 SnapCenter 和複寫資料的逐步說明範例、請參閱 "利用SnapCenter 功能進行複寫設定"

使用 SnapCenter 審查 SQL VM 保護

設定GCVO主機和CVO資料存取

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

NetApp Cloud Volume Service for NFS Datastore 和 Cloud Volumes ONTAP for SQL 資料庫和記錄可部署至任何 VPC 、 GCVE 應與該 VPC 建立私有連線、以掛載 NFS 資料存放區、並讓 VM 連線至 iSCSI LUN 。

若要設定GCVE/ SDDC、請參閱 "在Google Cloud Platform（GCP）上部署及設定虛擬化環境"。先決條件是確認駐留在GCVM主機上的來賓VM能夠在Cloud Volumes ONTAP 建立連線之後、從支援中心取用資料。

正確設定好VMware和GCVETM之後Cloud Volumes ONTAP 、請開始設定Veeam、使用Veeam複寫功能、並利用SnapMirror將應用程式Volume複本複製到Cloud Volumes ONTAP VMware、將內部部署工作負載的恢復作業自動化至GCVETM（使用應用程式VMDK的VM和使用客體內建儲存設備的VM）。

安裝**Veeam**元件

根據部署案例、需要部署的Veeam備份伺服器、備份儲存庫和備份Proxy。在此使用案例中、不需要為Veeam部署物件存放區、也不需要橫向擴充儲存庫。
"如需安裝程序、請參閱Veeam文件"
如需其他資訊、請參閱 "使用 Veeam Replication 移轉"

使用**Veeam**設定**VM**複寫

內部部署的vCenter和GCVE- vCenter都需要向Veeam註冊。 "設定vSphere VM複寫工作" 在精靈的「來賓處理」步驟中、選取「停用應用程式處理」、因為我們將使用SnapCenter 支援應用程式的功能來進行應用程式感知備份與還原。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

容錯移轉**Microsoft SQL Server VM**

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

本解決方案的優點

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

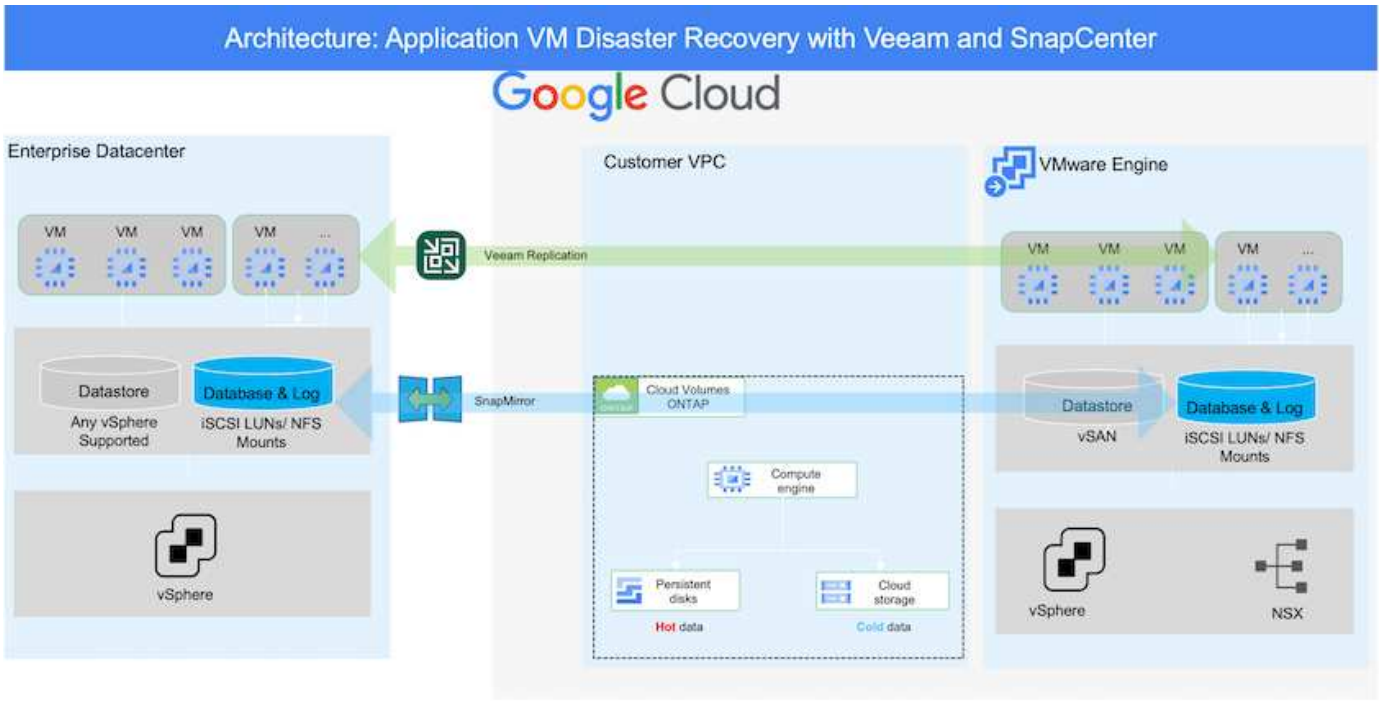
應用程式災難恢復：**SnapCenter** 利用功能不全**Cloud Volumes ONTAP** 、功能不全和**Veeam**複寫

作者：NetApp Suresh ThopPay

總覽

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

本文件提供逐步方法、以設定及執行使用NetApp SnapMirror、Veeam及Google Cloud VMware Engine（GCVE）的災難恢復。



假設

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

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

若要在內部部署環境與Google Cloud網路之間建立連線、請使用專屬互連或Cloud VPN等連線選項。應根據內部部署的VLAN設計來建立區段。

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

部署災難恢復解決方案

解決方案部署總覽

1. 確保應用程式資料是以SnapCenter 不必要的RPO要求使用支援功能進行備份。
2. 在Cloud Volumes ONTAP 適當的訂購和虛擬網路中使用Cloud Manager、以正確的執行個體大小進行配置。
   a. 為相關的應用程式磁碟區設定SnapMirror。
   b. 更新SnapCenter 中的備份原則、以便在排程工作之後觸發SnapMirror更新。
3. 安裝Veeam軟體、並開始將虛擬機器複寫至Google Cloud VMware Engine執行個體。
4. 在災難事件期間、請使用Cloud Manager中斷SnapMirror關係、並觸發Veeam虛擬機器的容錯移轉。

a. 重新連接應用程式VM的iSCSI LUN和NFS掛載。

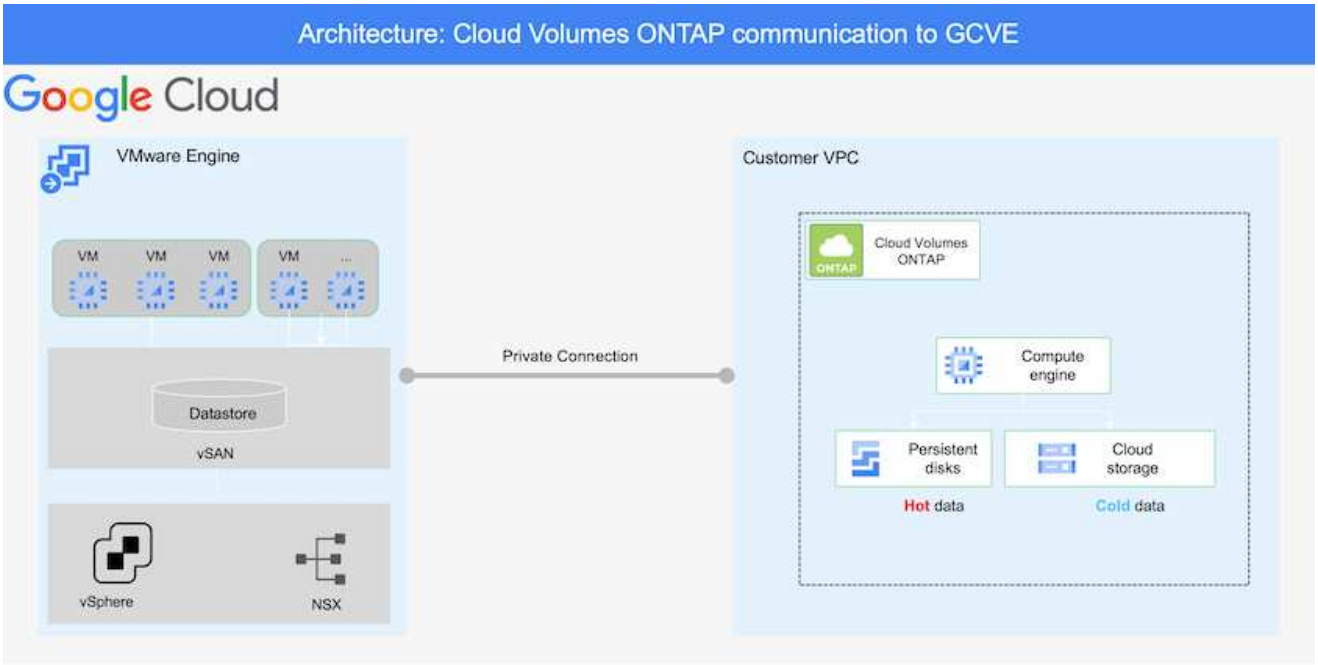
b. 將應用程式上線。

5. 在主站台恢復後、透過反向重新同步SnapMirror來叫用容錯回復至受保護站台。

部署詳細資料

在**Google Cloud**上設定**CVO**、並將磁碟區複寫至**CVO**

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



如需設定 SnapCenter 和複寫資料的逐步說明範例、請參閱 "利用SnapCenter 功能進行複寫設定"

利用SnapCenter 功能進行複寫設定

設定**GCVO**主機和**CVO**資料存取

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

可將支援範例部署至任何VPC、而GCVR應具有與該VPC的私有連線、以便讓VM連線至iSCSI LUN 。Cloud Volumes ONTAP

若要設定GCVE/ SDDC、請參閱 "在Google Cloud Platform（GCP）上部署及設定虛擬化環境"。先決條件是確認駐留在GCVM主機上的來賓VM能夠在Cloud Volumes ONTAP 建立連線之後、從支援中心取用資料。

正確設定好VMware和GCVETM之後Cloud Volumes ONTAP 、請開始設定Veeam、使用Veeam複寫功能、並利用SnapMirror將應用程式Volume複本複製到Cloud Volumes ONTAP VMware、將內部部署工作負載的恢復作業自動化至GCVETM（使用應用程式VMDK的VM和使用客體內建儲存設備的VM）。

安裝**Veeam**元件

根據部署案例、需要部署的Veeam備份伺服器、備份儲存庫和備份Proxy。在此使用案例中、不需要為Veeam部署物件存放區、也不需要橫向擴充儲存庫。https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["如需安裝程序、請參閱Veeam文件"]

使用**Veeam**設定**VM**複寫

內部部署的vCenter和GCVE- vCenter都需要向Veeam註冊。 "設定vSphere VM複寫工作" 在精靈的「來賓處理」步驟中、選取「停用應用程式處理」、因為我們將使用SnapCenter 支援應用程式的功能來進行應用程式感知備份與還原。

設定vSphere VM複寫工作

容錯移轉**Microsoft SQL Server VM**

容錯移轉Microsoft SQL Server VM

本解決方案的優點

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

試。

- Veeam Replication允許變更DR站台上的VM IP位址。

在 GCP / GCVE 上移轉工作負載

使用**VMware HCX -**快速入門指南、將工作負載移轉至**Google Cloud VMware Engine**上的**NetApp Cloud Volume Service**資料存放區

作者：NetApp解決方案工程

總覽：使用**VMware HCX**、**NetApp Cloud Volume Service**資料存放區和**Google Cloud VMware Engine**（**GCVE**）移轉虛擬機器

Google Cloud VMware Engine和Cloud Volume Service資料存放區最常見的使用案例之一、就是移轉VMware工作負載。VMware HCX是首選選選項、提供各種移轉機制、可將內部部署虛擬機器（VM）及其資料移轉至Cloud Volume Service NFS資料存放區。

VMware HCX主要是一個移轉平台、其設計旨在簡化應用程式移轉、工作負載重新平衡、甚至是雲端之間的營運不中斷。它包含在Google Cloud VMware Engine私有雲中、提供許多移轉工作負載的方法、可用於災難恢復（DR）作業。

本文件逐步引導您進行Cloud Volume Service資料存放區的資源配置、接著下載、部署及設定VMware HCX、包括內部部署及Google Cloud VMware Engine端的所有主要元件、包括互連、網路擴充及WAN最佳化、以啟用各種VM移轉機制。

> VMware HCX可與任何資料存放區類型搭配使用、因為移轉作業是在VM層級進行。因此、本文件適用於目前打算使用Google Cloud VMware Engine部署Cloud Volume Service的NetApp客戶和非NetApp客戶、以實現具成本效益的VMware雲端部署。

高階步驟

此清單提供從內部部署HCX Connector配對與移轉VM至Google Cloud VMware Engine端HCX Cloud Manager所需的高階步驟：

1. 透過Google VMware Engine入口網站準備HCX。
2. 在內部部署的VMware vCenter Server中下載並部署HCX Connector Open Virtualization Appliance（OVA）安裝程式。
3. 使用授權金鑰啟動HCX。
4. 將內部部署的VMware HCX Connector與Google Cloud VMware Engine HCX Cloud Manager配對。
5. 設定網路設定檔、運算設定檔和服務網格。
6. （選用）執行網路擴充、以避免在移轉期間重新取得IP。
7. 驗證應用裝置狀態、並確保可以進行移轉。
8. 移轉VM工作負載。

先決條件

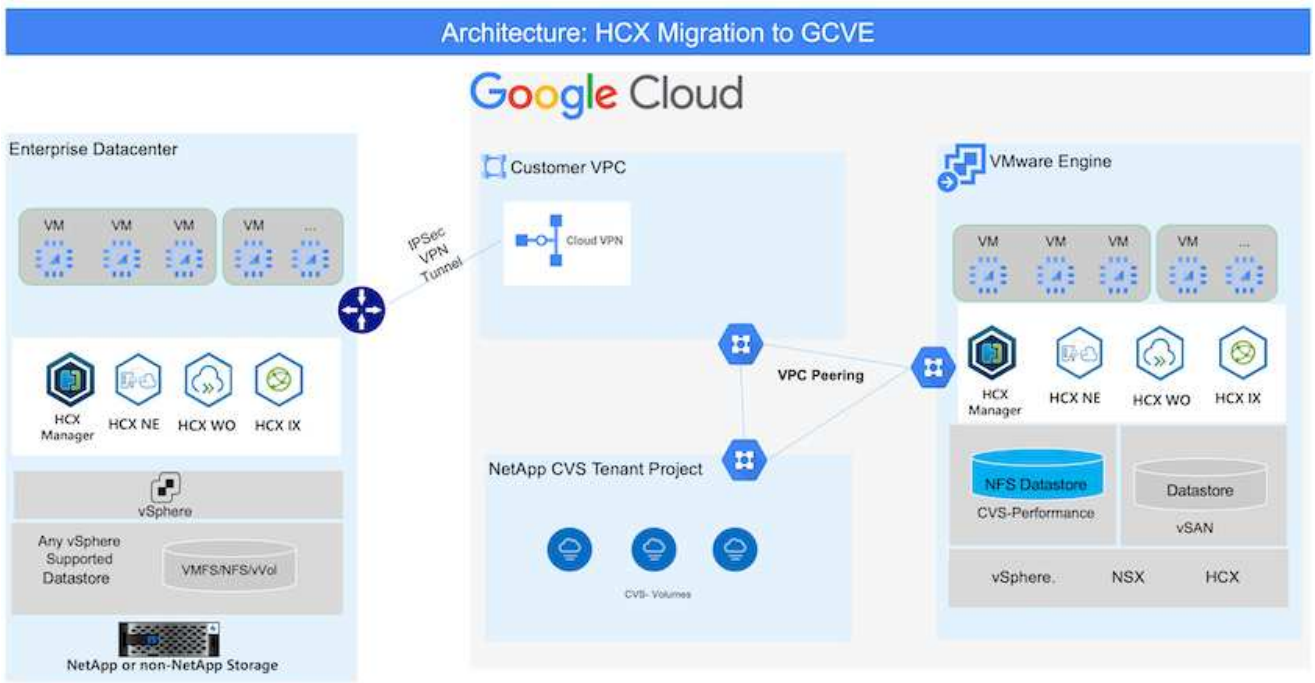
開始之前、請先確定符合下列先決條件。如需詳細資訊、請參閱 "連結"。在具備連線能力等先決條件之後、請從Google Cloud VMware Engine入口網站下載HCX授權金鑰。下載OVA安裝程式之後、請繼續執行下列安裝程序。

> HCx進階為預設選項、VMware HCX Enterprise版本也可透過支援票證取得、而且不需額外付費即可獲得支援。請參閱 "此連結"

- 使用現有的Google Cloud VMware Engine軟體定義資料中心（SDDC）、或使用此功能建立私有雲端 "NetApp連結" 或是這種情況 "Google連結"。
- 若要從內部部署的VMware vSphere資料中心移轉VM及相關資料、需要從資料中心連線至SDDC環境。移轉工作負載之前、 "設定Cloud VPN或Cloud Interconnect連線" 在內部部署環境與各自私有雲端之間。
- 從內部部署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移轉VM。
- 請確定所需的 "防火牆規則和連接埠" 允許內部部署vCenter Server與SDDC vCenter之間的VMotion流量。
- Cloud Volume Service NFS磁碟區應以資料存放區的形式掛載於Google Cloud VMware Engine。請依照本節詳細說明的步驟進行 "連結" 將Cloud Volume Service資料存放區附加至Google Cloud VMware Engines主機。

高層架構

為了進行測試、此驗證所使用的內部部署實驗室環境是透過Cloud VPN連線、可在內部部署連線至Google Cloud VPC。



如需HCX的詳細圖表、請參閱 "VMware連結"

解決方案部署

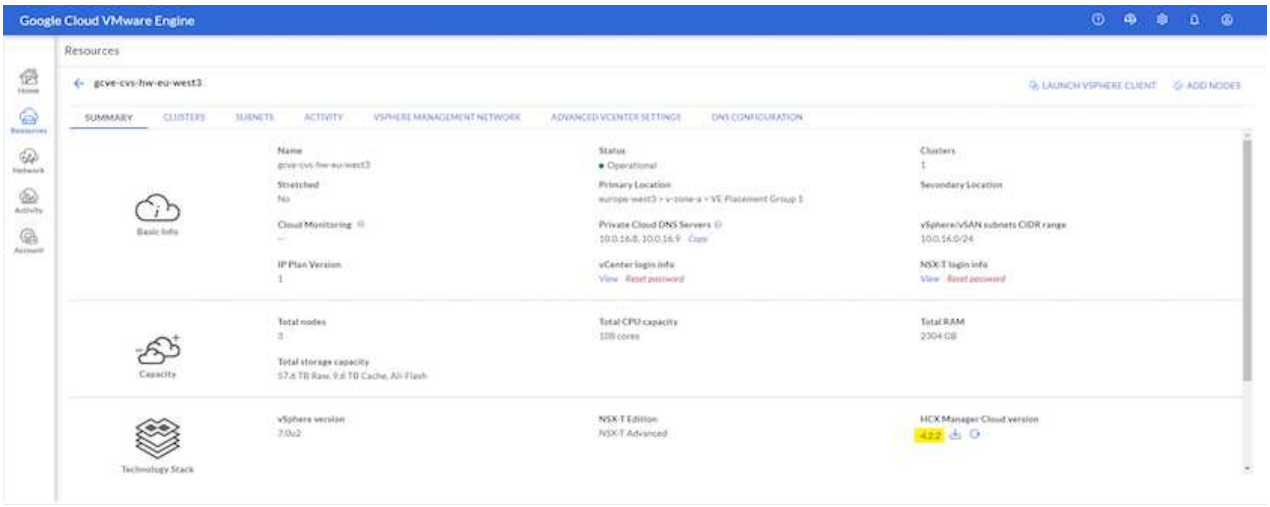
請依照一系列步驟完成本解決方案的部署：

步驟1：透過Google VMware Engine Portal準備HCX

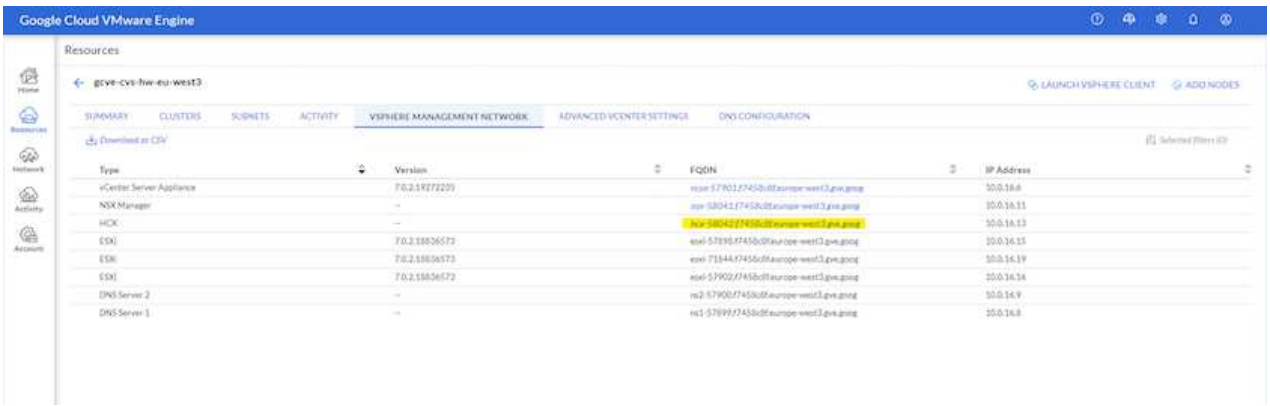
HCx Cloud Manager元件會在您使用VMware Engine配置私有雲時自動安裝。若要準備站台配對、請完成下列步驟：

1. 登入Google VMware Engine入口網站、然後登入HCX Cloud Manager。

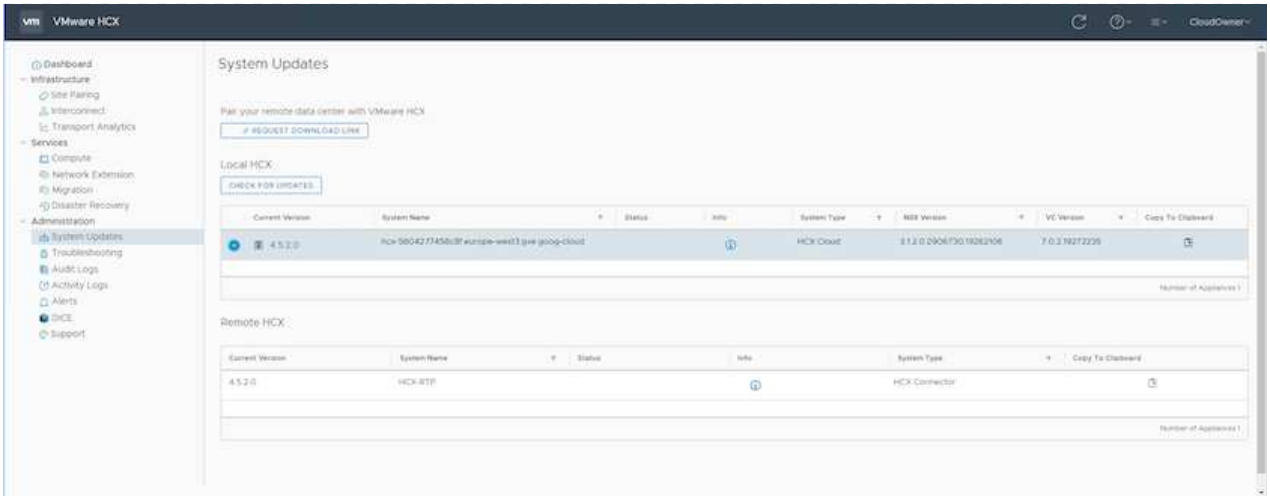
   您可以按一下HCX版本連結、登入HCX主控台



   或按一下vSphere管理網路索引標籤下的HCX FQDN。



2. 在HCX Cloud Manager中、前往*管理>系統更新*。
3. 按一下*「Request download*（申請下載連結*）」、然後下載OVA檔案。



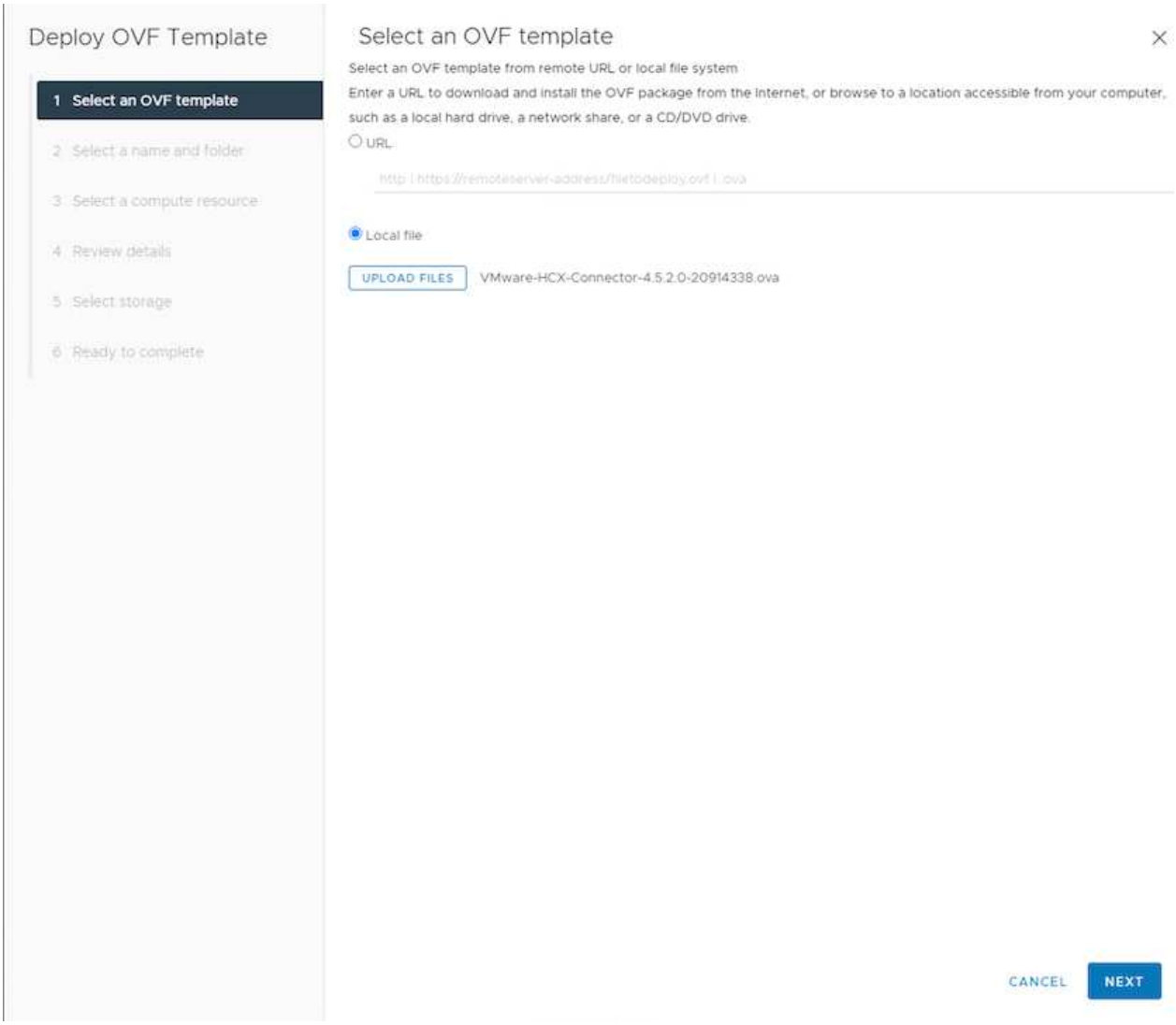
4. 將HCX Cloud Manager更新為HCX Cloud Manager UI提供的最新版本。

步驟**2**：在內部部署**vCenter Server**中部署安裝程式**OVA**

若要讓內部部署連接器連線至Google Cloud VMware Engine中的HCX Manager、請確定內部部署環境中已開啟適當的防火牆連接埠。

若要在內部部署vCenter Server中下載並安裝HCX Connector、請完成下列步驟：

1. 如前一步驟所述、請從Google Cloud VMware Engine上的HCX主控台下載ova。
2. 下載OVA之後、請使用*部署OVF範本*選項、將其部署至內部部署的VMware vSphere環境。



3. 輸入OVA部署的所有必要資訊、按一下*「下一步」、然後按一下「*完成」以部署VMware HCX連接器OVA。

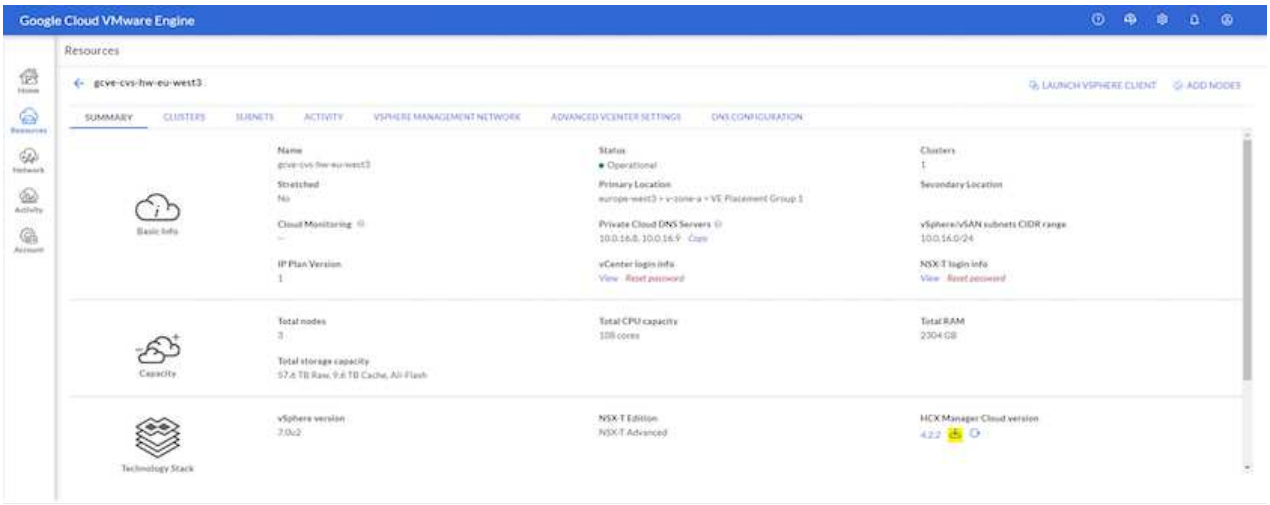
手動啟動虛擬應用裝置。

如需逐步指示、請參閱 "VMware HCX使用者指南"。

步驟3：使用授權金鑰啟動**HCX Connector**

在內部部署VMware HCX Connector OVA並啟動應用裝置之後、請完成下列步驟以啟動HCX Connector。從Google Cloud VMware Engine入口網站產生授權金鑰、然後在VMware HCX Manager中啟動。

1. 在VMware Engine入口網站中、按一下「Resources（資源）」、選取私有雲、然後*按一下「HCX Manager Cloud Version *（HCX Manager Cloud Version *）」下的「Download（下載）」圖示。



開啟下載的檔案、然後複製授權金鑰字串。

2. 登入內部部署的VMware HCX Manager、網址為 "https://hcxmanagerIP:9443" 使用系統管理員認證。

   使用在OVA部署期間定義的hcxmanagerIP和密碼。

3. 在授權中、輸入從步驟3複製的金鑰、然後按一下「啟動」。

   內部部署的HCX Connector應可存取網際網路。

4. 在*資料中心位置*下、提供最接近內部部署VMware HCX Manager的安裝位置。按一下 * 繼續 * 。
5. 在*系統名稱*下、更新名稱、然後按一下*繼續*。
6. 按一下*是、繼續*。
7. 在「連線您的**VCenter**」下、提供vCenter Server的完整網域名稱（FQDN）或IP位址、以及適當的認證資料、然後按一下「繼續」。

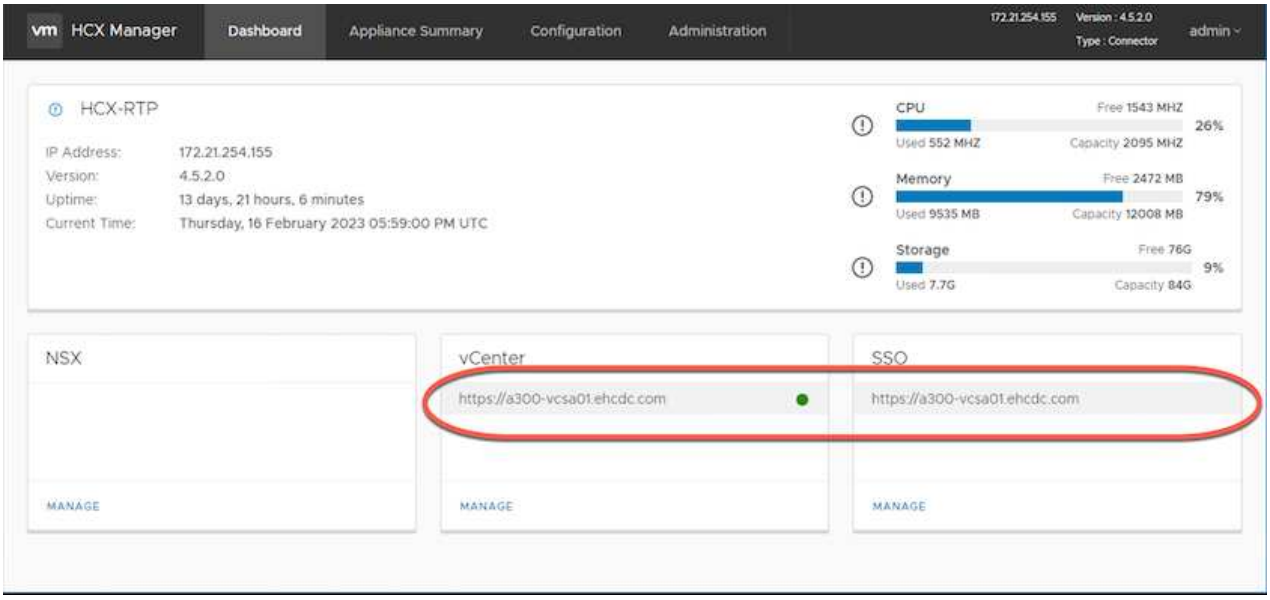
   使用FQDN以避免稍後發生連線問題。

8. 在「組態**SSO/PSC** *」下、提供平台服務控制器（**PSC**）**FQDN**或**IP**位址、然後按一下「*繼續」。

   若為內嵌PSC、請輸入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會在顯示的頁面上顯示為綠色。vCenter Server和SSO都必須具有適當的組態參數、此參數應與上一頁相同。

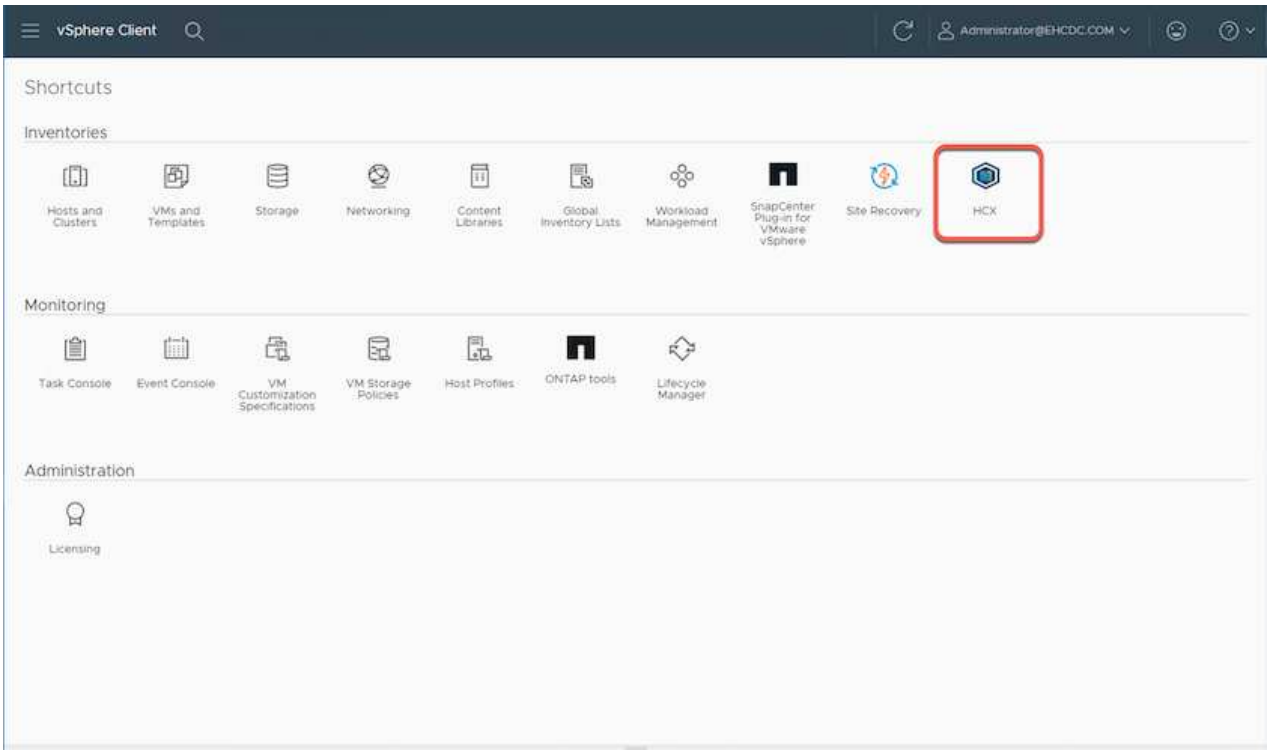
此程序大約需要10到20分鐘、而外掛程式則要新增至vCenter Server。



步驟4：將內部部署的VMware HCX Connector與Google Cloud VMware Engine HCX Cloud Manager配對

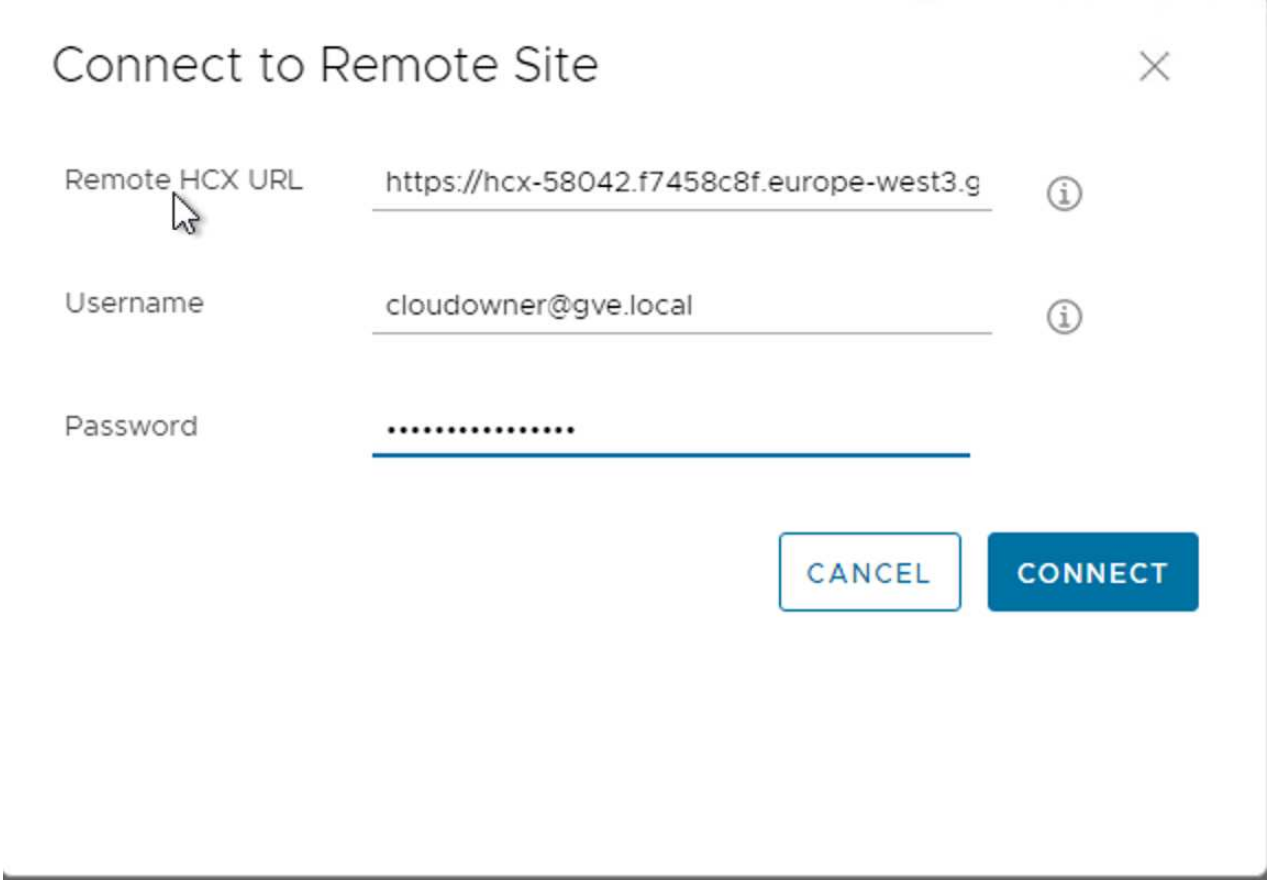
在內部部署vCenter上部署和設定HCX Connector之後、請新增配對以建立與Cloud Manager的連線。若要設定站台配對、請完成下列步驟：

1. 若要在內部部署vCenter環境與Google Cloud VMware Engine SDDC之間建立站台配對、請登入內部部署vCenter Server、然後存取新的HCX vSphere Web Client外掛程式。



2. 按一下「基礎架構」下的「新增站台配對」。

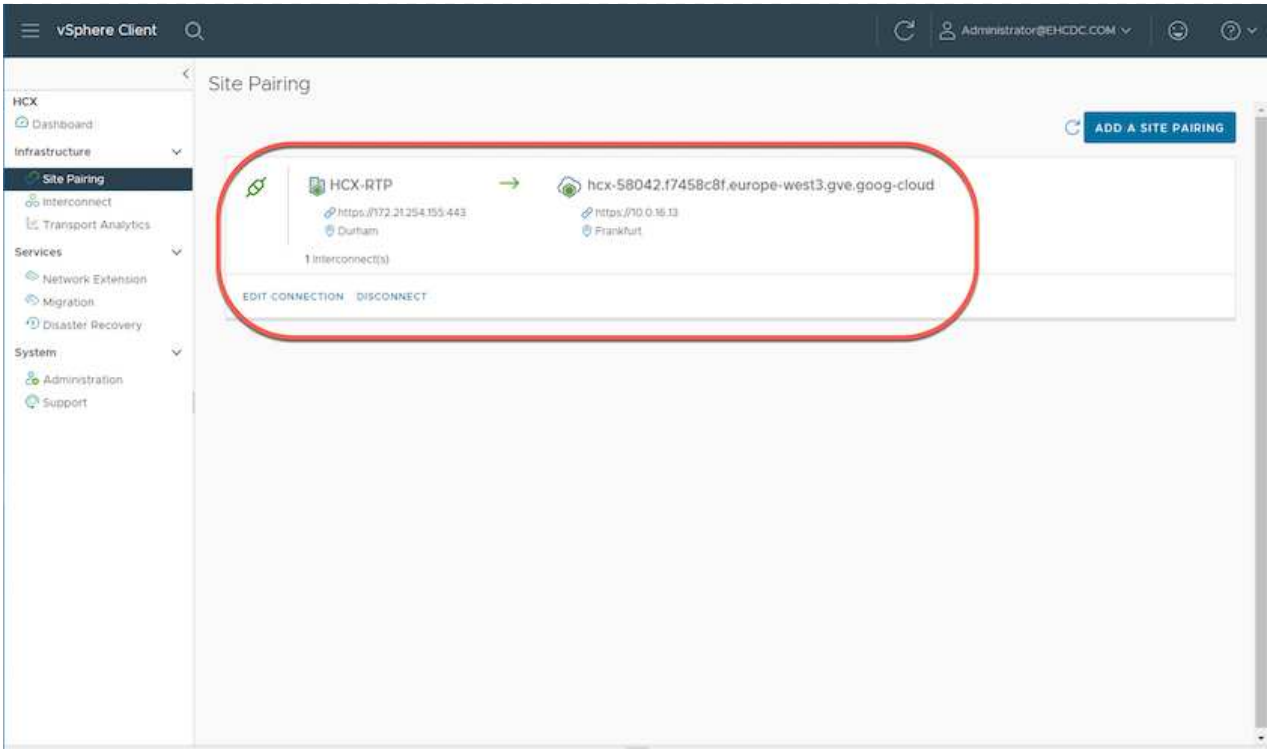
輸入Google Cloud VMware Engine HCX Cloud Manager URL或IP位址、以及具有雲端擁有者角色存取私有雲權限的使用者認證資料。



3. 按一下「連線」。

   VMware HCX Connector必須能夠透過連接埠443路由傳送至HCX Cloud Manager IP。

4. 建立配對之後、即可在HCX儀表板上取得新設定的站台配對。

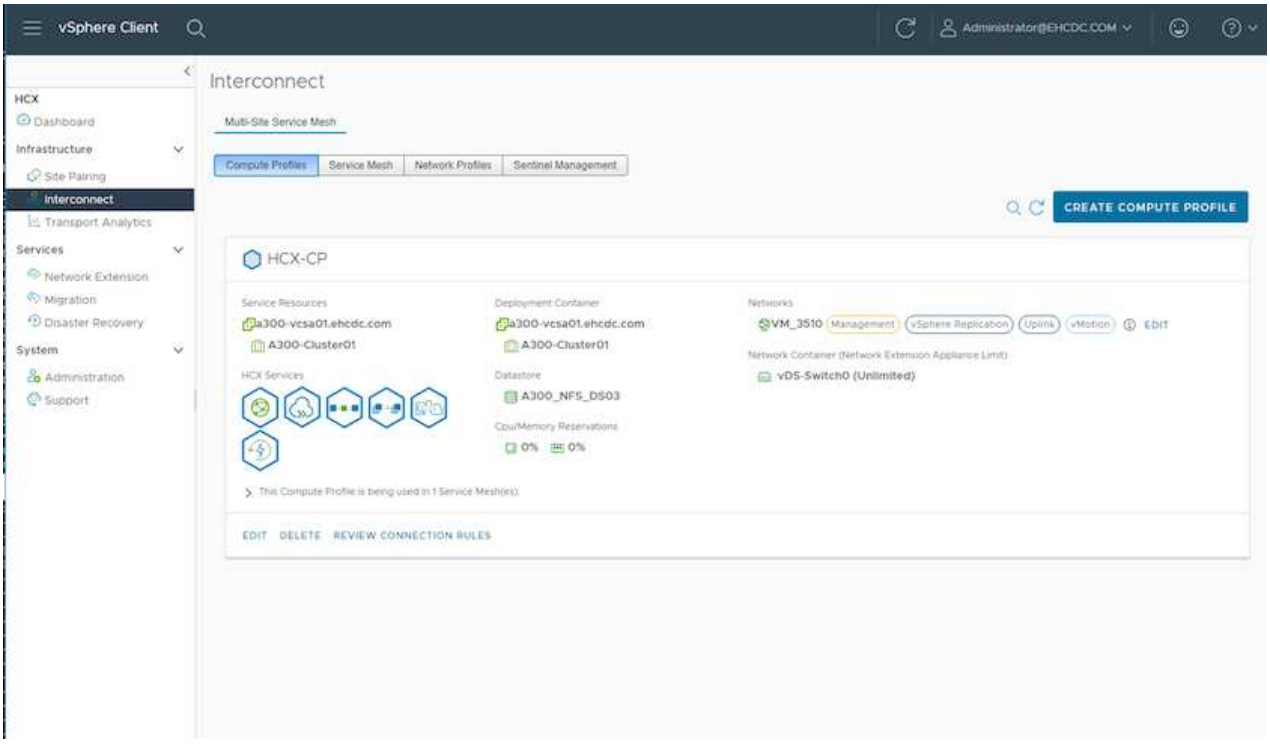

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

步驟**5**：設定網路設定檔、運算設定檔和服務網格

VMware HCX互連服務應用裝置可透過網際網路提供複寫及vMotion型移轉功能、並可透過私有連線連至目標站台。互連可提供加密、流量工程及VM行動性。若要建立互連服務應用裝置、請完成下列步驟：

1. 在「基礎架構」下、選取「互連>多站台服務網狀架構>運算設定檔」>「建立運算設定檔」。

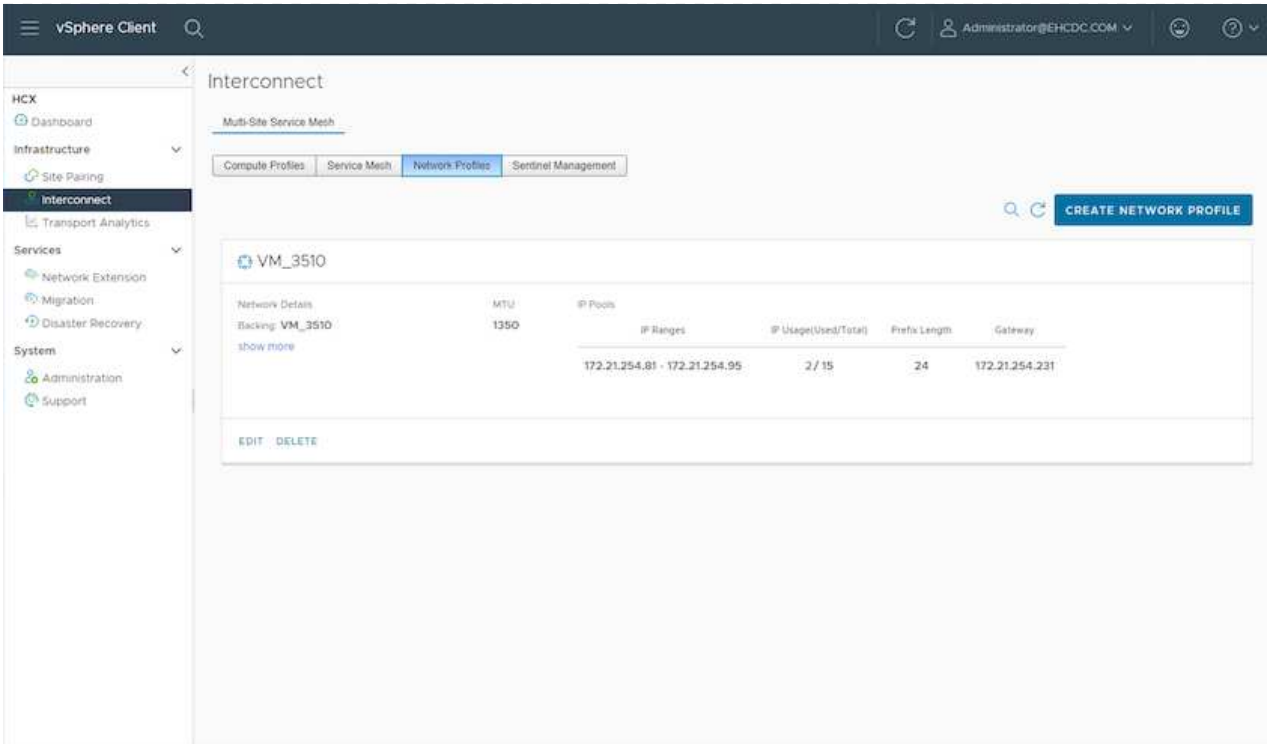
   運算設定檔定義部署參數、包括部署的應用裝置、以及HCX服務可存取的VMware資料中心部分。



2. 建立運算設定檔之後、選取*多站台服務網格>網路設定檔>建立網路設定檔*、即可建立網路設定檔。

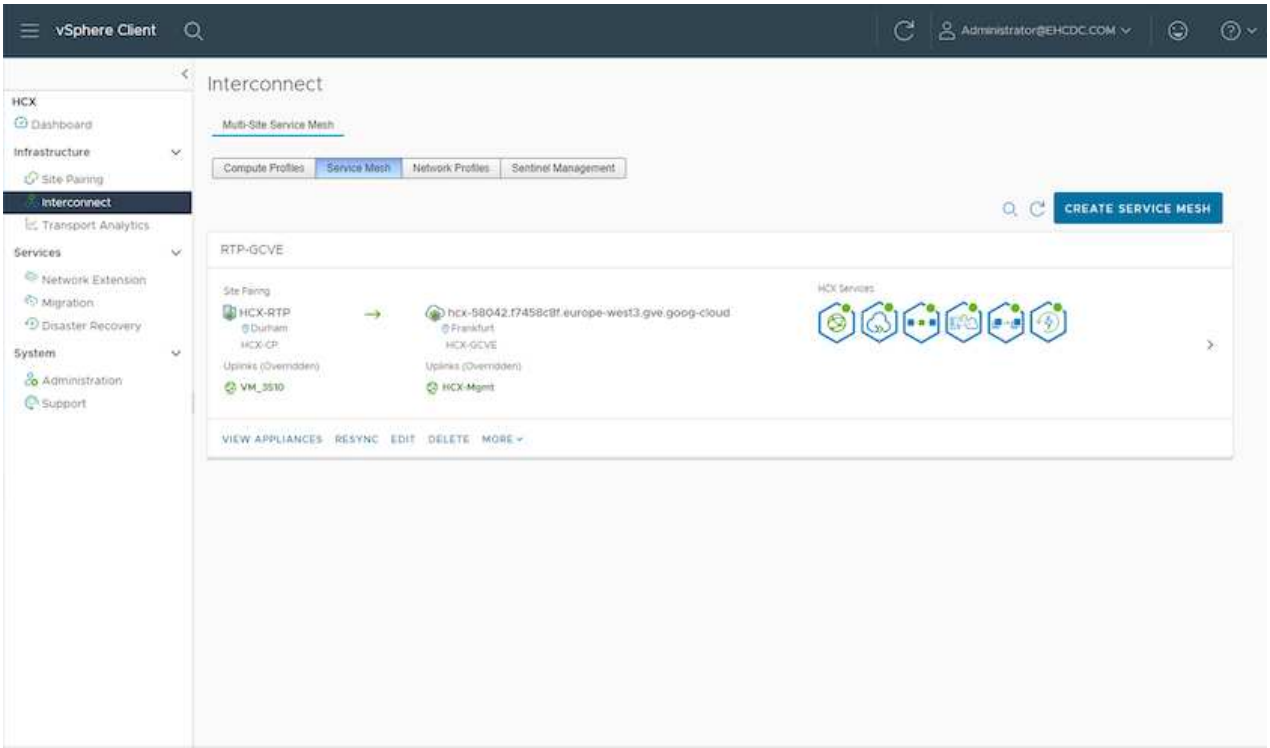
   網路設定檔會定義一系列的IP位址和網路、以供HCX用於其虛擬應用裝置。

   此步驟需要兩個以上的IP位址。這些IP位址會從管理網路指派給互連設備。

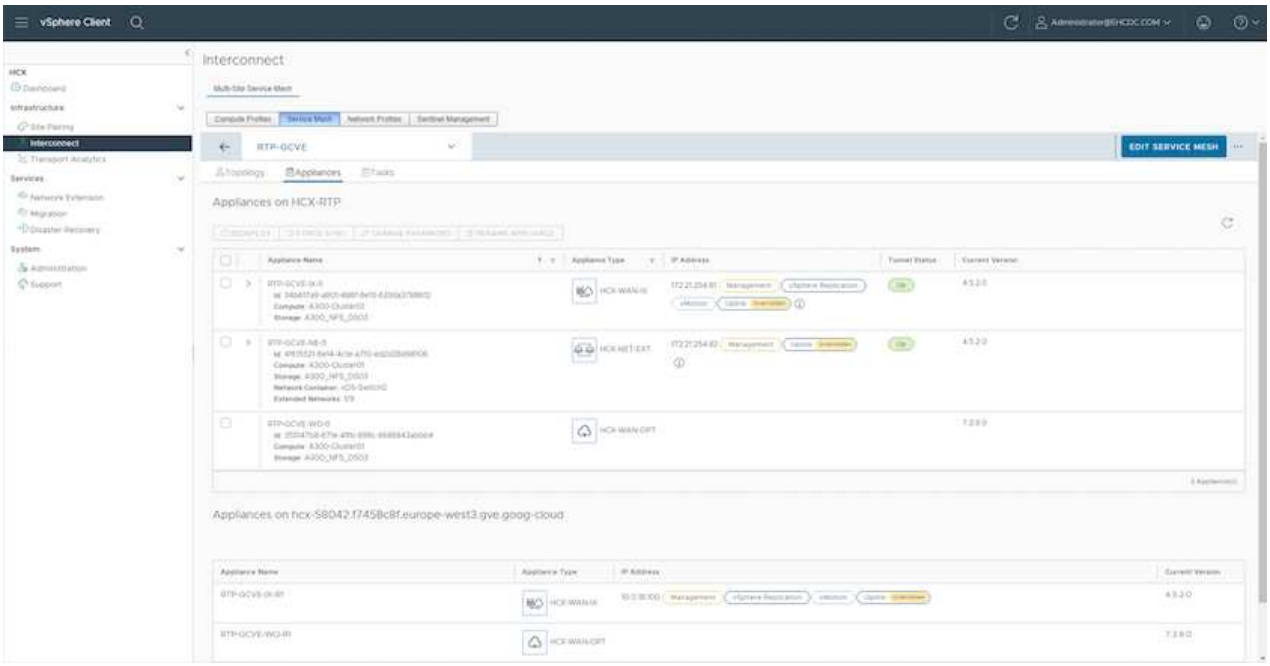


3. 目前、運算和網路設定檔已成功建立。
4. 選取「互連」選項中的「服務網格」索引標籤、然後選取內部部署和GCVC SDDC站台、即可建立服務網格。
5. Service Mesh會指定本機和遠端運算和網路設定檔配對。

在此程序中、會在來源和目標站台上部署並自動設定HCX應用裝置、以建立安全的傳輸架構。



6. 這是組態的最後一步。完成部署需要將近30分鐘的時間。設定好服務網格後、環境就能準備好、成功建立IPsec通道來移轉工作負載VM。



步驟**6**：移轉工作負載

使用各種VMware HCX移轉技術、可在內部部署與GCVC SDDC之間雙向移轉工作負載。VM可以使用多種移轉技術（例如HCX大量移轉、HCX vMotion、HCX冷移轉、HCX複寫輔助vMotion（適用於HCX Enterprise Edition）、以及HCX OS輔助移轉）（適用於HCX Enterprise Edition）、在VMware HCX啟動的實體之間移動。

若要深入瞭解各種HCX移轉機制、請參閱 "VMware HCX移轉類型"。

HCX-IX應用裝置使用行動代理程式服務來執行VMotion、Cold和Replication輔助VMotion（RAV）移轉。

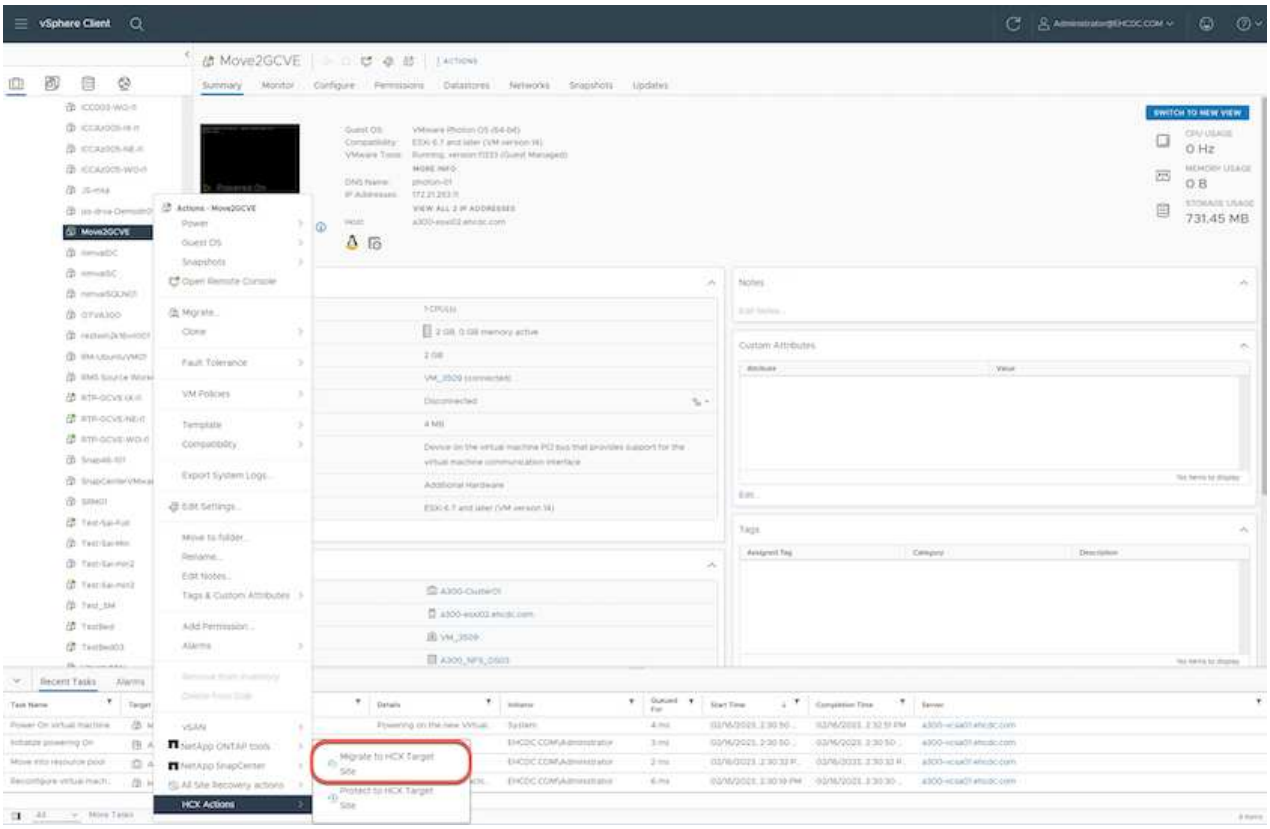
HCX-IX應用裝置會將行動代理程式服務新增為vCenter Server中的主機物件。此物件上顯示的處理器、記憶體、儲存設備和網路資源、並不代表裝載IX應用裝置的實體Hypervisor實際使用量。

- HCX VMotion*

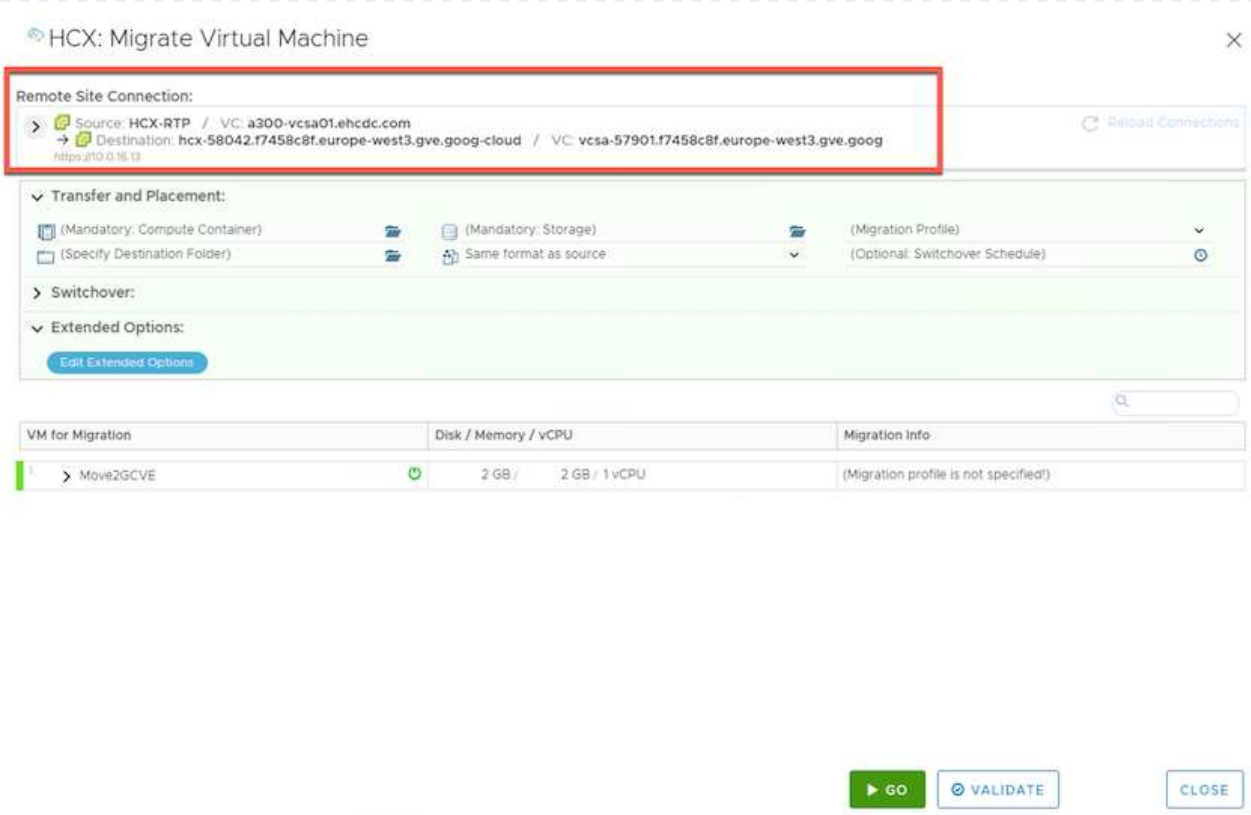
本節說明HCX VMotion機制。此移轉技術使用VMware VMotion傳輸協定將VM移轉至GCVM。VMotion移轉選項可用於一次移轉單一VM的VM狀態。此移轉方法不會中斷服務。

網路擴充功能應已就緒（適用於連接VM的連接埠群組）、以便在不需要變更IP位址的情況下移轉VM。

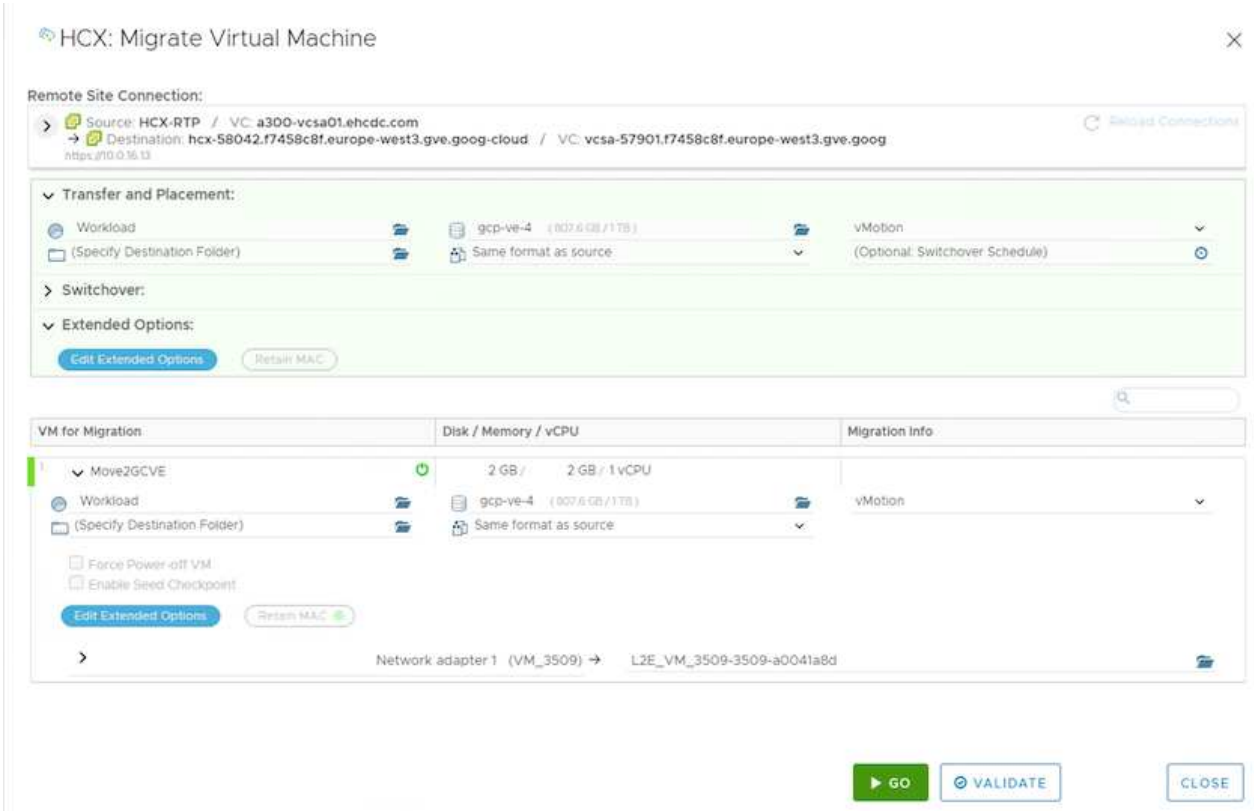
1. 從內部部署vSphere用戶端移至「Inventory」、在要移轉的VM上按一下滑鼠右鍵、然後選取「HCX Actions」（HCX動作）>「移轉至HCX目標站台」。



2. 在「移轉虛擬機器」精靈中、選取「遠端站台連線」（目標GCVE）。



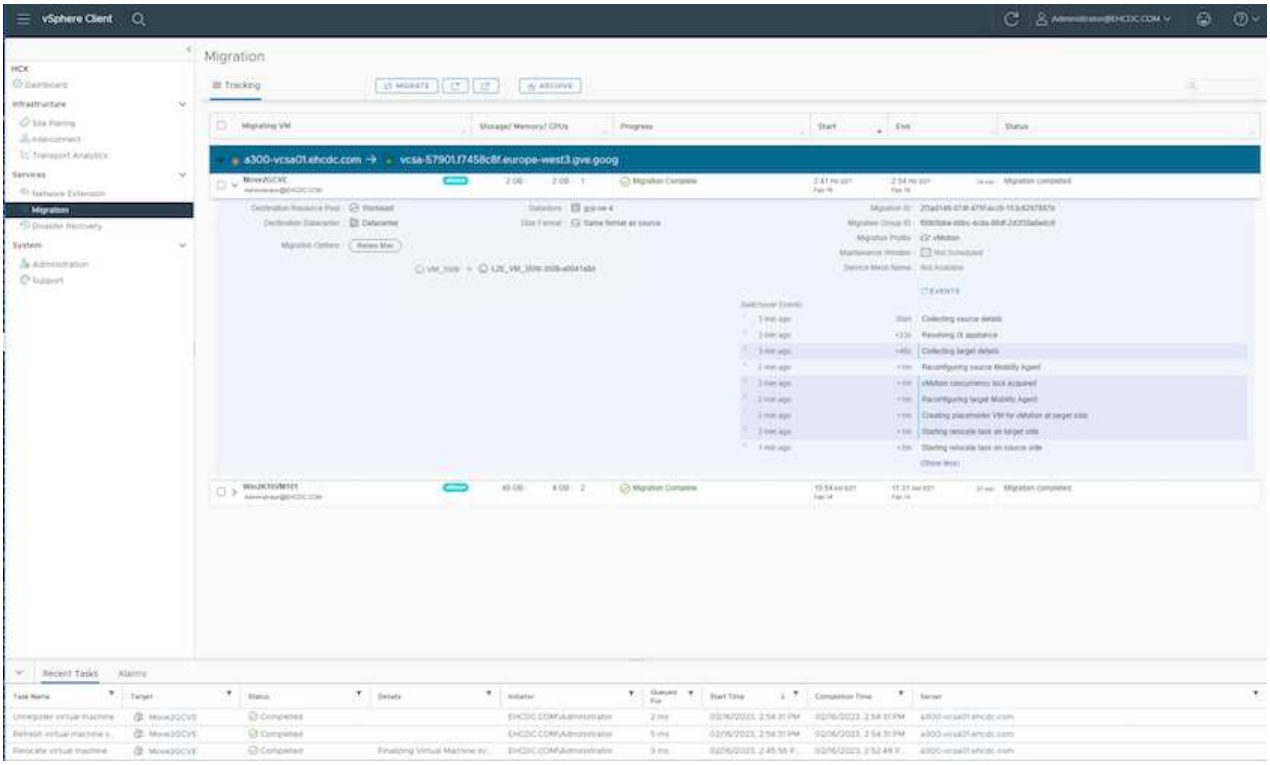
3. 更新必填欄位（叢集、儲存設備和目的地網路）、按一下「Validate（驗證）」。



4. 驗證檢查完成後、按一下「Go（執行）」以啟動移轉。

VMotion傳輸會擷取VM作用中記憶體、其執行狀態、IP位址及其MAC位址。如需有關HCX VMotion需求與限制的詳細資訊、請參閱 "瞭解VMware HCX VMotion和冷移轉"。

5. 您可以從HCX >移轉儀表板監控VMotion的進度和完成。



目標CVS NFS資料存放區應有足夠空間來處理移轉作業。

結論

無論您的目標是全雲端或混合雲、或是位於內部部署的任何類型/廠商儲存設備上的資料、Cloud Volume Service和HCX都能提供絕佳的選項、讓應用程式層能夠順暢地部署和移轉應用程式工作負載、同時降低TCO、進而將資料需求無縫移轉至應用程式層。無論使用案例為何、您都可以選擇Google Cloud VMware Engine搭配Cloud Volume Service來快速實現雲端效益、一致的基礎架構、以及跨內部部署和多個雲端的作業、工作負載的雙向可攜性、以及企業級容量和效能。使用VMware vSphere複寫、VMware VMotion、甚至是網路檔案複本（NFC）來連接儲存設備及移轉VM的程序與程序、都是相當熟悉的程序。

重點摘要

本文件的重點包括：

- 您現在可以在Google Cloud VMware Engine SDDC上使用Cloud Volume Service做為資料存放區。
- 您可以輕鬆地將資料從內部部署移轉至Cloud Volume Service資料存放區。
- 您可以輕鬆擴充及縮減Cloud Volume Service資料存放區、以滿足移轉活動期間的容量和效能需求。

Google和**VMware**提供的影片供參考

來自**Google**

- "部署HCX Connector搭配GCVE"
- "設定HCX ServiceMesh搭配GCV"
- "使用HCX將VM移轉至GCV"

來自**VMware**

- "HCx Connector部署（用於GCVF）"
- "GCVF的HCx ServiceMesh組態"
- "HCx工作負載移轉至GCV"

何處可找到其他資訊

若要深入瞭解本文所述資訊、請參閱下列網站連結：

- Google Cloud VMware Engine文件

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service文件

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- VMware HCX使用者指南

  "https://docs.vmware.com/en/VMware-HCX/index.html"

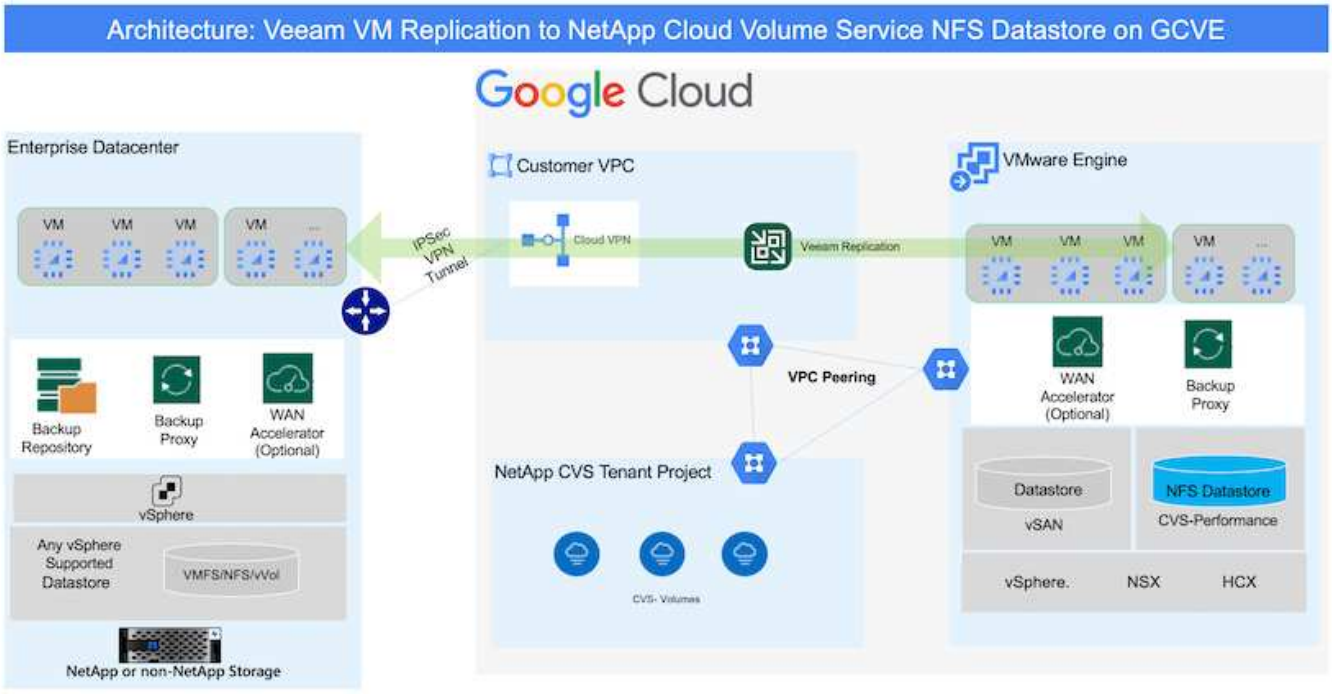
VM 移轉至 **Google Cloud** 上的 **NetApp** 雲端 **Volume Service NFS** 資料存放區使用 **Veeam** 複寫功能的 **VMware** 引擎

總覽

作者：NetApp Suresh ThopPay

在 VMware vSphere 上執行的 VM 工作負載可透過 Veeam Replication 功能移轉至 Google Cloud VMware Engine （ GCVE ）。

本文件提供逐步設定及執行 VM 移轉的方法、使用 NetApp Cloud Volume Service 、 Veeam 及 Google Cloud VMware Engine （ GCVE ）。



假設

本文件假設您已備有 Google Cloud VPN 或 Cloud Interconnect 或其他網路選項、可從現有的 vSphere 伺服器建立網路連線至 Google Cloud VMware Engine 。

> 將內部部署資料中心連線至Google Cloud的選項有多種、讓我們無法在此文件中概述特定的工作流程。
> 請參閱 "Google Cloud文件" 以取得適當的內部部署與 Google 連線方法。

部署移轉解決方案

解決方案部署總覽

1. 請確定 NetApp Cloud Volume Service 的 NFS 資料存放區已裝載於 GCVE vCenter 。
2. 確保 Veeam Backup Recovery 已部署在現有的 VMware vSphere 環境中
3. 建立複寫工作、開始將虛擬機器複寫至 Google Cloud VMware Engine 執行個體。
4. 執行 Veeam 複寫工作的容錯移轉。
5. 在 Veeam 上執行永久性容錯移轉。

部署詳細資料

請確定 **NetApp Cloud Volume Service** 的 **NFS** 資料存放區已裝載於 **GCVE vCenter**

登入 GCVE vCenter 、確保 NFS 資料存放區有足夠的可用空間。
如果沒有、請參閱 "將 NetApp CVS 掛載為 GCVE 上的 NFS 資料存放區"

確保 **Veeam Backup Recovery** 已部署在現有的 **VMware vSphere** 環境中

請參閱 "Veeam Replication Components" 安裝必要元件的文件。

建立複寫工作、開始將虛擬機器複寫至 **Google Cloud VMware Engine** 執行個體。

內部部署的vCenter和GCVE- vCenter都需要向Veeam註冊。 "設定vSphere VM複寫工作"
以下是說明方法的影片
"設定複寫工作"。

> 複本 VM 的 IP 可能與來源 VM 不同、也可以連線至不同的連接埠群組。如需詳細資訊、請參閱上述影片。

執行 **Veeam** 複寫工作的容錯移轉

若要移轉 VM 、請執行 "執行容錯移轉"

在 **Veeam** 上執行永久性容錯移轉。

若要將 GCVE 視為新的來源環境、請執行 "永久性容錯移轉"

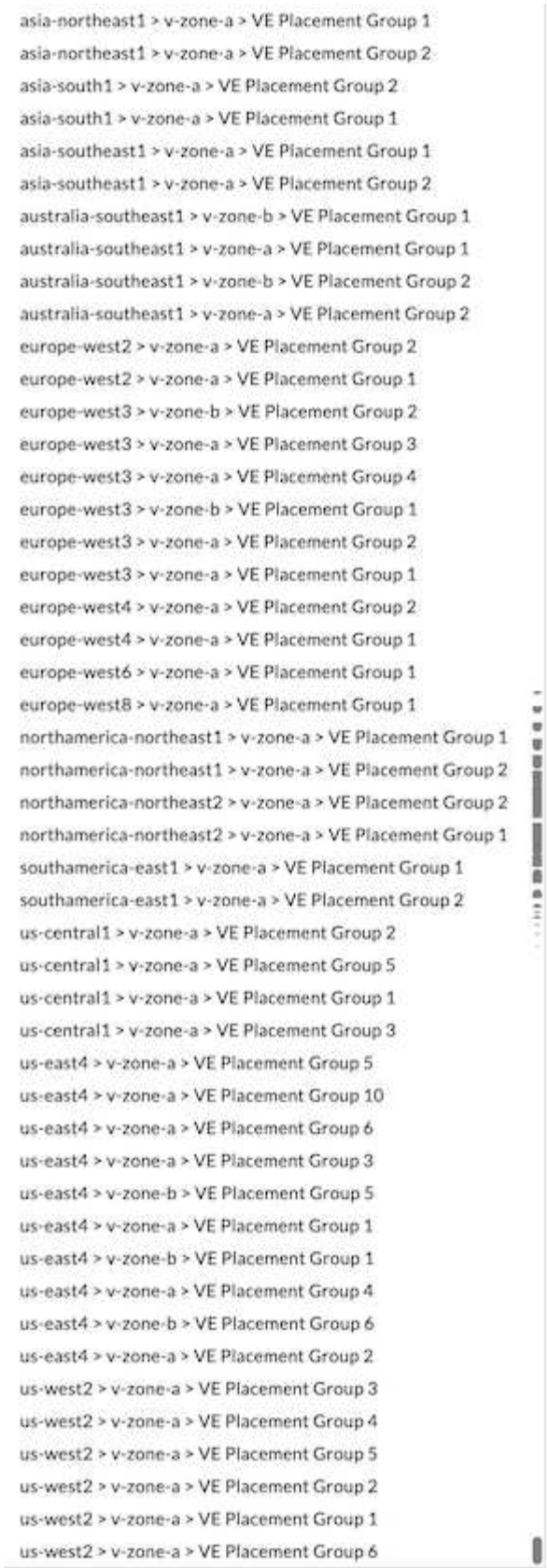
本解決方案的優點

- 現有的 Veeam 備份基礎架構可用於移轉。
- Veeam Replication 允許變更目標站台上的 VM IP 位址。
- 能夠重新對應 Veeam 以外複寫的現有資料（例如 BlueXP 複寫的資料）
- 能夠在目標站台上指定不同的網路連接埠群組。
- 可指定 VM 的開機順序。
- 利用 VMware 變更區塊追蹤功能、將透過 WAN 傳送的資料量降到最低。
- 能夠執行複寫的前置和後置指令碼。
- 能夠執行快照的前後指令碼。

區域可用度–**Google Cloud Platform**（**GCP**）的補充**NFS**資料存放區

NetApp Cloud Volume Service 支援 GCVE 的 NFS 補充資料存放區。

> GCVE NFS 資料存放區只能使用 CVS-Performance 磁碟區。
> 如需可用位置的資訊、請參閱 "全球區域地圖"



Google Cloud VMware Engine 可在下列位置取得

為了將延遲降至最低、您想要掛載磁碟區的 NetApp CVS Volume 和 GCVE 應該位於相同的可用性區域。

與 Google 和 NetApp 解決方案架構師合作、以實現可用度和 TCO 最佳化。

安全性總覽- Cloud Volumes Service Google Cloud中的NetApp解決方案（CVS）

TR-4918：安全性總覽- Google Cloud Volumes Service Cloud中的NetApp功能

Oliver Krause、Justin Parisi、NetApp

文件範圍

安全性、尤其是在基礎架構不受儲存管理員控制的雲端環境中、對於信任您的資料、以提供由雲端供應商提供的服務而言、是非常重要的。本文檔概述NetApp提供的安全產品 "支援Google Cloud Cloud Volumes Service"。

目標對象

本文件的目標對象包括但不限於下列角色：

- 雲端供應商
- 儲存管理員
- 儲存架構設計師
- 現場資源
- 企業決策者

如果您對本技術報告內容有任何疑問、請參閱一節 "「聯絡我們」。"

縮寫	定義
CVS軟體	支援服務類型CVS Cloud Volumes Service
CVS效能	Cloud Volume Service、服務類型CVs-Performance
PSA	

Google Cloud的功能介紹如何保護資料安全Cloud Volumes Service

在Google Cloud中使用支援多種方式、以原生方式保護資料安全。Cloud Volumes Service

安全的架構與租戶模式

透過分割不同端點的服務管理（控制面板）和資料存取（資料面板）、提供Google Cloud中的安全架構、使兩者都不會影響其他端點（請參閱一節）Cloud Volumes Service "「架構」Cloud Volumes Service"）。它使用Google的 "私有服務存取"（PSA）架構以提供服務。此架構可區分由NetApp提供及營運的服務供應商、以及客戶專案中的虛擬私有雲端（VPC）服務消費者、這些客戶是想要存取Cloud Volumes Service VMware檔案共享的客戶。

在此架構中、租戶（請參閱一節 "「租賃模式」"）定義為Google Cloud專案、除非使用者明確連線、否則這些專案彼此之間完全隔離。租戶可利用Cloud Volumes Service 這個功能、將資料磁碟區、外部名稱服務及解決方案的其他重要部分、與其他租戶完全隔離在一起。由於此平台是透過VPC對等連接、因此隔離也適用於此平台。Cloud Volumes Service您Cloud Volumes Service 可以使用共享VPC、在多個專案之間共用一個支援區塊（請參閱一節） "「共享VPC」"）。您可以將存取控制套用至SMB共用和NFS匯出、以限制可以檢視或修改資料集的人員或內容。

針對控制面板提供強大的身分識別管理功能

在執行不完整組態的控制面板Cloud Volumes Service 中、使用管理身分識別管理 "身分識別存取管理（IAM）"。IAM是一項標準服務、可讓您控制Google Cloud專案執行個體的驗證（登入）和授權（權限）。所有組態都是透過Cloud Volumes Service 使用TLS 1.2加密的安全HTTPS傳輸來執行、而驗證則是使用JWT權杖來執行、以提高安全性。Google Console UI Cloud Volumes Service for the取消功能、可將使用者輸入內容轉譯為Cloud Volumes Service 使用者對功能不整的API呼叫。

安全強化：限制攻擊面

有效安全性的一部分是限制服務中可用的攻擊面數量。攻擊面可能包括各種內容、包括閒置資料、飛行傳輸、登入及資料集本身。

託管服務可移除設計中固有的部分攻擊面。基礎架構管理、如一節所述 "「服務營運、」" 由專屬團隊處理、並自動化以減少人員實際接觸組態的次數、有助於減少刻意和非蓄意的錯誤數量。網路已被隔離、因此只有必要的服務才能彼此存取。加密會被納入資料儲存設備、只有資料層需要Cloud Volumes Service 得到資訊管理員的安全注意。藉由將大部分的管理隱藏在API介面之後、可藉由限制攻擊面來實現安全性。

零信任模式

過去、IT安全理念一直是信任、但卻是驗證、而且只是仰賴外部機制（例如防火牆和入侵偵測系統）來減輕威脅。然而、攻擊與入侵事件演變成透過網路釣魚、社交工程、內部威脅及其他驗證方法、規避環境中的驗證、進而進入網路並造成嚴重破壞。

零信任已成為安全性的新方法、目前的宗旨是「在驗證一切的同時、不信任任何事物」。 因此、預設不允許任何存取。這項強制原則有多種執行方式、包括標準防火牆和入侵偵測系統（IDS）、也有下列方法：

- 強式驗證方法（例如AES加密的Kerberos或JWT權杖）
- 單一強身分識別來源（例如Windows Active Directory、輕量型目錄存取傳輸協定（LDAP）和Google IAM）
- 網路區隔和安全的多租戶共享（預設只允許租戶存取）
- 以最低權限存取原則進行精細的存取控制
- 專屬且值得信賴的小型專屬系統管理員清單、提供數位稽核與書面記錄

在Google Cloud上執行的解決方案採用零信任模式、實作「無信任、驗證一切」的立場。Cloud Volumes Service

加密

加密閒置資料（請參閱一節 "「閒置時的資料加密」"）搭配NetApp Volume Encryption（NVE）和線上使用XTS-AES-256密碼 "「SMB加密」" 或NFS Kerberos 5p支援。瞭解跨區域複寫傳輸受到TLS 1.2加密保護、讓您高枕無憂（請參閱一節） "「跨區域複寫」"）。此外、Google網路也提供加密通訊（請參閱一節 "「傳輸中的資料加密」"）提供額外的保護層、防範攻擊。如需傳輸加密的詳細資訊、請參閱一節 "「Google Cloud Network」"。

資料保護與備份

安全性不只是預防攻擊而已。這也與我們如何在攻擊發生時或發生時從攻擊中恢復有關。此策略包括資料保護與備份。提供在停電時複製到其他地區的方法（請參閱一節Cloud Volumes Service "「跨區域複寫」"）或資料集受到勒索軟體攻擊的影響。也Cloud Volumes Service 可以使用、將資料非同步備份到非執行個體的位置 "支援Cloud Volumes Service"。透過定期備份、降低安全事件的時間、節省成本、並使系統管理員感到焦慮。

利用領先業界的**Snapshot**複本、快速緩解勒索軟體

除了資料保護與備份、Cloud Volumes Service 支援不可變的Snapshot複本（請參閱一節）"「可永久保存的Snapshot複本」"）允許從勒索軟體攻擊中恢復的磁碟區（請參閱一節"「服務營運」"）在發現問題的幾秒鐘內、並將中斷時間降至最低。恢復時間與影響取決於Snapshot排程、但您可以建立Snapshot複本、在勒索軟體攻擊中提供最少一小時的差異。Snapshot複本對效能和容量使用率的影響微乎其微、是保護資料集的低風險高報酬方法。

安全考量與攻擊面

瞭解如何保護資料安全的第一步、就是找出風險和潛在的攻擊面。

其中包括（但不限於）下列項目：

- 系統管理與登入
- 閒置資料
- 資料傳輸中
- 網路和防火牆
- 勒索軟體、惡意軟體和病毒

瞭解攻擊面可協助您更妥善地保護環境安全。在Google Cloud中、不需進行任何管理互動、即可將許多主題納入考量、並在預設情況下實作安全功能。Cloud Volumes Service

確保安全登入

保護關鍵基礎架構元件的安全時、必須確保只有獲核准的使用者才能登入及管理您的環境。如果不良的使用者違反您的管理認證、他們就能擁有城堡的金鑰、而且可以執行任何他們想要的動作：變更組態、刪除磁碟區和備份、建立後端或停用Snapshot排程。

支援Google Cloud的解決方案可透過模糊化的儲存即服務（StaaS）、防止未經授權的系統管理登入。Cloud Volumes Service由雲端供應商完全維護、無法從外部登入。Cloud Volumes Service所有的設定和組態作業都是完全自動化的、因此除非情況非常罕見、否則人員管理員永遠不需要與系統互動。

如果需要登入、Cloud Volumes Service Google Cloud中的功能驗證可確保登入安全、只要維護一份可供登入系統之受信任系統管理員的簡短清單即可。這項網關保存功能有助於減少可能的不良使用者存取權。此外、Google Cloud網路也將系統隱藏在網路安全層的背後、只向外界公開所需的內容。如需Google Cloud Cloud Volumes Service 的資訊、請參閱「架構」一節"「架構」Cloud Volumes Service 。"

叢集管理與升級

有潛在安全風險的兩個領域包括叢集管理（如果不良的使用者具有管理存取權限、會發生什麼事）和升級（如果軟體映像遭到破壞、會發生什麼事）。

儲存管理保護

儲存設備即服務可移除對雲端資料中心外部終端使用者的存取權限、進而移除管理員曝險的額外風險。而唯一的組態是由客戶進行資料存取。每個租戶都會管理自己的磁碟區、而且沒有租戶能夠觸及其他Cloud Volumes Service 的實體執行個體。此服務是由自動化管理、其中只有一小份受信任的系統管理員清單、可透過本節所述的程序存取系統"「服務營運。」"

CVS效能服務類型提供跨區域複寫選項、可在區域故障時、為不同區域提供資料保護。在這些情況Cloud

Volumes Service 下、可將無法存取的功能故障轉移至未受影響的區域、以維持資料存取。

服務升級

更新有助於保護易受影響的系統。每項更新都提供安全性增強功能和錯誤修正、可將攻擊面減至最低。軟體更新是從集中式儲存庫下載、並在允許更新之前驗證、以驗證是否使用正式映像、以及升級是否受到不良行為的影響。

有了NetApp、雲端供應商團隊就能處理更新、提供具備組態與升級能力的專家、並將程序自動化且經過完整測試、藉此消除系統管理員團隊面臨的風險風險。Cloud Volumes Service升級不會中斷營運、Cloud Volumes Service 而為了獲得最佳整體效果、我們會維護最新的更新。

如需執行這些服務升級之系統管理員團隊的相關資訊、請參閱一節 "「服務營運。」"

保護閒置資料的安全

當磁碟遭竊、退回或重新使用時、靜止資料加密對於保護敏感資料非常重要。使用軟體式加密、可保護靜態資料Cloud Volumes Service 。

- Google產生的金鑰用於CVs-SW。
- 如需CVS效能、每個Volume金鑰會儲存在Cloud Volumes Service 內建於支援核心的金鑰管理程式中、此管理程式使用NetApp ONTAP 還原資料模組來產生AES-256加密金鑰。CryptoModis會列在CMVP FIPS 140-2驗證模組清單中。請參閱 "FIPS 140-2認證編號4144"。

自2021年11月起、客戶管理的加密（CMEK）功能預覽已推出CVS效能。此功能可讓您使用Google金鑰管理服務（KMS）中所裝載的個別專案、每個區域的主要金鑰、來加密每個Volume金鑰。KMS可讓您附加外部金鑰管理程式。

如需如何設定KMS以獲得CVS效能的詳細資訊、 "請參閱Cloud Volumes Service 《》文件"。

如需架構的詳細資訊、請參閱一節 "「架構」Cloud Volumes Service 。"

保護資料傳輸安全

除了確保閒置資料的安全、Cloud Volumes Service 您也必須能夠在資料在執行個體與用戶端或複寫目標之間傳輸時、保護資料安全。利用加密方法（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點對端點加密的NFS Kerberos 5p）、為透過NAS傳輸的傳輸中資料提供加密功能。Cloud Volumes Service

利用AES-GCM加密方法、複寫Cloud Volumes Service 不中斷的實體磁碟區使用TLS 1.2。

預設會停用最不安全的傳輸協定、例如：Telnet、NDMP等。不過、DNS並非Cloud Volumes Service 由支援DNS的功能加密（不支援DNS安全）、因此應盡可能使用外部網路加密來加密。請參閱一節 "「傳輸中的資料加密」" 以取得更多關於保護資料傳輸安全的資訊。

如需NAS傳輸協定加密的相關資訊、請參閱一節 "「NAS傳輸協定」。"

NAS權限的使用者和群組

保護雲端資料的一部分是適當的使用者和群組驗證、其中存取資料的使用者會在環境中驗證為真實使用者、而群組則包含有效的使用者。這些使用者和群組提供初始共用和匯出存取、以及儲存系統中檔案和資料夾的權限驗證。

針對SMB共用和Windows型權限、使用標準的Active Directory型Windows使用者和群組驗證。Cloud Volumes

Service此服務也能運用UNIX身分識別供應商、例如LDAP for UNIX使用者和群組進行NFS匯出、NFSv4 ID驗證、Kerberos驗證及NFSv4 ACL。

目前僅支援Active Directory LDAP Cloud Volumes Service 搭配「以供LDAP使用」功能。

偵測、防範及防範勒索軟體、惡意軟體及病毒

勒索軟體、惡意軟體和病毒是系統管理員持續面臨的威脅、企業組織最需要注意的是偵測、防範和防範這些威脅。關鍵資料集上的單一勒索軟體事件可能會花費數百萬美元、因此您可以採取最大程度的行動來降低風險。

雖然目前不包含原生偵測或預防措施、例如防毒保護或Cloud Volumes Service "自動勒索軟體偵測"、您可以透過啟用定期Snapshot排程、快速從勒索軟體事件中恢復。Snapshot複本是不可變更的、而且是檔案系統中變更區塊的唯讀指標、幾乎是即時性的、對效能的影響最小、而且只有在資料變更或刪除時才會佔用空間。您可以設定Snapshot複本的排程、以符合所需的可接受恢復點目標（RPO）/恢復時間目標（RTO）、而且每個Volume最多可保留1、024個Snapshot複本。

Snapshot支援不需額外付費（除了Snapshot複本所保留的變更區塊/資料的資料儲存費用）Cloud Volumes Service 、而且在發生勒索軟體攻擊時、也可在攻擊發生之前、用於回溯至Snapshot複本。快照還原只需幾秒鐘即可完成、之後您就能恢復正常的資料服務。如需詳細資訊、請參閱 "NetApp勒索軟體解決方案"。

若要防止勒索軟體影響您的業務、需要採用多層方法、其中包括下列一項或多項：

- 端點保護
- 透過網路防火牆防範外部威脅
- 偵測資料異常
- 關鍵資料集的多重備份（現場與異地）
- 定期還原備份測試
- 不可變的唯讀NetApp Snapshot複本
- 關鍵基礎架構的多因素驗證
- 系統登入的安全性稽核

這份清單遠非詳盡無遺、但在處理勒索軟體攻擊的可能性時、這是一個很好的藍圖。在Google Cloud中提供多種方法來保護勒索軟體事件、並減少其影響。Cloud Volumes Service

不可變的**Snapshot**複本

由於資料刪除或整個磁碟區遭到勒索軟體攻擊、因此本機可提供可自訂排程的不可變唯讀Snapshot複本、以便在資料刪除或整個磁碟區遭到勒索軟體攻擊時、快速進行時間點還原。Cloud Volumes Service快照還原至先前的良好Snapshot複本、可根據Snapshot排程和RTO/RPO的保留期間、迅速將資料遺失減至最低。Snapshot技術的效能影響微乎其微。

由於VMware的Snapshot複本Cloud Volumes Service 是唯讀的、因此除非勒索軟體擴散到未注意到的資料集、而且Snapshot複本已被勒索軟體感染、否則這些複本將不會受到勒索軟體的感染。因此、您也必須考慮根據資料異常狀況來偵測勒索軟體。目前無法原生提供偵測功能、但您可以使用外部監控軟體。Cloud Volumes Service

備份與還原

支援標準NAS用戶端備份功能（例如透過NFS或SMB進行備份）Cloud Volumes Service 。

- CVS效能提供跨區域磁碟區複寫至其他CVS效能磁碟區的功能。如需詳細資訊、請參閱 "Volume複製" 請參閱Cloud Volumes Service 《》文件。
- CVS軟體提供服務原生Volume備份/還原功能。如需詳細資訊、請參閱 "雲端備份" 請參閱Cloud Volumes Service 《》文件。

Volume複寫提供確切的來源磁碟區複本、可在發生災難時（包括勒索軟體事件）進行快速容錯移轉。

跨區域複寫

CVS效能可讓您在Google雲端區域之間安全地複寫磁碟區、以便在NetApp控制的後端服務網路上使用TLS1.2 AES 256 GCM加密、並使用特定介面在Google網路上執行複寫、以保護資料及歸檔使用案例。主要（來源）Volume包含作用中正式作業資料、並複寫至次要（目的地）Volume、以提供主要資料集的確切複本。

初始複寫會傳輸所有區塊、但更新只會傳輸主磁碟區中變更的區塊。例如、如果將位於主要磁碟區上的1TB資料庫複寫到次要磁碟區、則初始複寫時會傳輸1TB的空間。如果該資料庫在初始化與下一個更新之間有幾百列（假設、幾MB）的變更、則只有變更列的區塊會複寫到次要（幾MB）。這有助於確保傳輸時間保持低、並降低複寫費用。

檔案和資料夾的所有權限都會複寫到次要磁碟區、但共用存取權限（例如匯出原則和規則、SMB共用和共用ACL）必須分開處理。在站台容錯移轉的情況下、目的地站台應利用相同的名稱服務和Active Directory網域連線、以一致的方式處理使用者和群組的身分識別和權限。當發生災難時、您可以使用次要Volume做為容錯移轉目標、方法是打破複寫關係、將次要Volume轉換為讀寫。

Volume複本為唯讀、可在異地提供不可改變的資料複本、以便在病毒感染資料或勒索軟體加密主要資料集的情況下、快速恢復資料。唯讀資料不會加密、但如果主要磁碟區受到影響並發生複寫、則受感染的區塊也會複寫。您可以使用較舊且不受影響的Snapshot複本進行還原、但SLA可能超出承諾的RTO/RPO範圍、視偵測到攻擊的速度而定。

此外、您也可以利用Google Cloud的跨區域複寫（CRR）管理功能、防止惡意的管理動作、例如磁碟區刪除、Snapshot刪除或Snapshot排程變更。這是透過建立自訂角色來完成、這些角色可分隔磁碟區管理員、這些管理員可以刪除來源磁碟區、但不能中斷鏡射、因此無法從CRR管理員刪除目的地磁碟區、因為他們無法執行任何Volume作業。請參閱 "安全考量" 關於每個系統管理員群組所允許的權限、請參閱Cloud Volumes Service 《參考資料》文件。

支援**Cloud Volumes Service**

雖然此功能可提供高資料持久性、但外部事件可能導致資料遺失。Cloud Volumes Service如果發生病毒或勒索軟體等安全事件、備份與還原對於及時恢復資料存取而言、將會變得非常重要。系統管理員可能不小心刪除Cloud Volumes Service 了一個聲音區。或者、使用者只是想保留資料的備份版本好幾個月、而在磁碟區內保留額外的Snapshot複本空間、就成為成本上的挑戰。雖然Snapshot複本應該是保留過去幾週備份版本以還原遺失資料的首選方法、但它們位於磁碟區內部、如果磁碟區消失、就會遺失。

基於上述所有理由、NetApp Cloud Volumes Service 支援透過提供備份服務 "支援Cloud Volumes Service"。

利用Google Cloud Storage（GCS）、即可在該磁碟區上產生一份複本。Cloud Volumes Service它只會備份儲存在磁碟區內的實際資料、而非可用空間。它的運作方式永遠是遞增的、也就是說、它只會在繼續備份變更的資料時、一次傳輸磁碟區內容、一次又一次從該處傳輸。相較於採用多個完整備份的傳統備份概念、它可節省大量備份儲存設備、進而降低成本。由於備份空間的每月價格比磁碟區低、因此是延長備份版本時間的理想選擇。

使用者可以使用Cloud Volumes Service 支援還原功能、將任何備份版本還原至相同區域內的相同或不同磁碟區。如果刪除來源磁碟區、則會保留備份資料、並需要獨立管理（例如刪除）。

支援的支援功能已內建於支援的選項中。Cloud Volumes Service Cloud Volumes Service使用者可依Cloud Volumes Service 每個Volume啟動「支援功能」備份、以決定要保護的磁碟區。請參閱 "支援的文件Cloud Volumes Service" 如需備份的相關資訊、請參閱 "支援的最大備份版本數"、排程和 "定價"。

專案的所有備份資料都儲存在GCS儲存區內、此儲存區由服務管理、使用者看不到。每個專案都使用不同的儲存庫。目前、這些庫位與Cloud Volumes Service 《非洲地理區（Sin the Same volume）」位於同一個區域、但我們正在討論更多選項。如需最新狀態、請參閱文件。

從資料庫傳輸Cloud Volumes Service 到GCS時、會使用內部服務的Google網路、搭配HTTPS和TLS1.2。資料會以Google管理的金鑰進行閒置加密。

若要管理Cloud Volumes Service 此功能（建立、刪除及還原備份）、使用者必須擁有 "角色/netappcloudVolumes.admin" 角色：

架構

總覽

信任雲端解決方案的一部分是瞭解架構及其安全性。本節說明Cloud Volumes Service Google中的各個環節、以協助您減輕資料安全的潛在疑慮、並指出可能需要採取額外組態步驟才能獲得最安全部署的領域。

整體的架構Cloud Volumes Service 可以分為兩個主要元件：控制面板和資料面板。

控制面

在這個過程中、由NetApp原生自動化軟體的管理員負責管理後端基礎架構。Cloud Volumes Service Cloud Volumes Service此架構對終端使用者完全透明、包括網路、儲存硬體、軟體更新等、有助於為Cloud Volumes Service 諸如更新的雲端解決方案提供價值。

資料平面

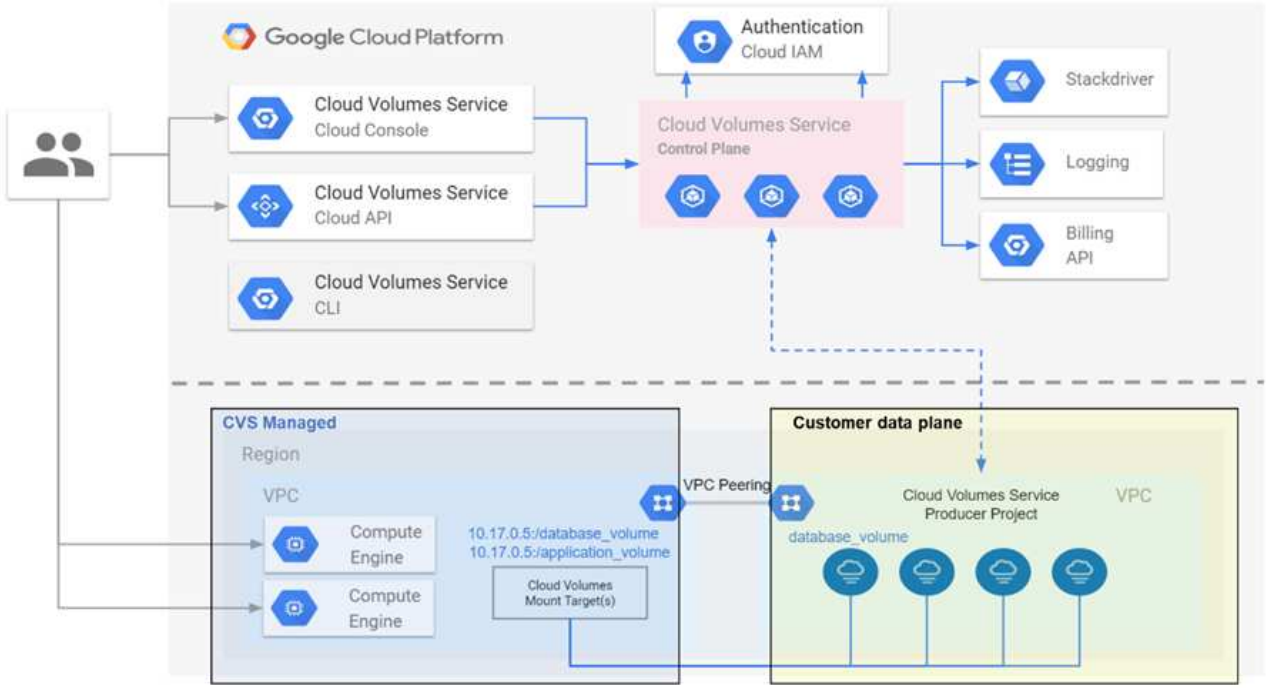
在資料架構Cloud Volumes Service 中、資料層面包括實際的資料量和Cloud Volumes Service 整體的支援（例如存取控制、Kerberos驗證等）。資料平面完全由Cloud Volumes Service 最終使用者和使用者控制。

每個平面的安全與管理方式各有不同。以下各節涵蓋這些差異、從Cloud Volumes Service 架構概述開始。

架構**Cloud Volumes Service**

以類似其他Google Cloud原生服務的方式、例如CloudSQL、Google Cloud VMware Engine（GCVE）和Filestore Cloud Volumes Service 、即用功能 "Google PSA" 以提供服務。在PSAA中、服務是建置於服務製造商專案內、此專案使用的 "VPC網路對等關係" 連線至服務使用者。服務製造商由NetApp提供及營運、服務消費者是客戶專案中的VPC、負責託管想要存取Cloud Volumes Service VMware檔案共享的客戶。

下圖、請參閱 "架構區段" 在本文件中Cloud Volumes Service 、顯示了高階檢視。



虛線上方的部分顯示服務的控制面、控制磁碟區生命週期。虛線下方的部分顯示資料平面。左藍色方塊描繪使用者VPC（服務消費者）、右藍色方塊則是NetApp提供的服務製造商。兩者都透過VPC對等連接。

租賃模式

在本例中、個別專案被視為獨特的租戶。Cloud Volumes Service這表示每個專案都會執行對磁碟區、Snapshot複本等的操作。換句話說、所有磁碟區都屬於在其中建立的專案、而且根據預設、只有該專案能管理及存取其中的資料。這被視為服務的控制面板檢視。

共享**VPC**

在資料平面檢視中Cloud Volumes Service 、無法連接至共享的VPC。您可以在託管專案或連接至共享VPC的其中一個服務專案中建立磁碟區。連接至該共享VPC的所有專案（主機或服務）都能到達網路層（TCP/IP）的磁碟區。由於在共享VPC上具有網路連線能力的所有用戶端都可能透過NAS傳輸協定存取資料、因此必須使用個別Volume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連接Cloud Volumes Service 到五部VPC。在控制面板上、專案可讓您管理所有建立的磁碟區、無論這些磁碟區連接到哪個VPC。在資料層面上、VPC彼此隔離、而且每個磁碟區只能連接至一個VPC。

個別磁碟區的存取是由特定傳輸協定（NFS/SMB）存取控制機制所控制。

換句話說、在網路層上、所有連線至共享VPC的專案都能看到該磁碟區、而在管理端、控制面板只能讓擁有者專案查看該磁碟區。

VPC服務控制

VPC服務控管機制建立了Google Cloud服務周邊的存取控制、這些服務已連接至網際網路、可在全球各地存取。這些服務可透過使用者身分識別提供存取控制、但無法限制來自哪些網路位置要求。VPC服務控制功能引進限制存取已定義網路的功能、藉此彌補這項落差。

此資料平面並未連線至外部網際網路、而是連線至具有明確定義網路邊界（周邊）的私有VPC。Cloud Volumes Service在該網路中、每個磁碟區都使用特定於傳輸協定的存取控制。任何外部網路連線都是由Google Cloud專案管理員明確建立。然而、控制面板並未提供與資料面板相同的保護、任何人只要擁有有效的認證資料（"JWT權杖"）。

簡而言之Cloud Volumes Service 、不需要支援VPC服務控制、也不明確使用VPC服務控制、即可透過資料中心提供網路存取控制功能。

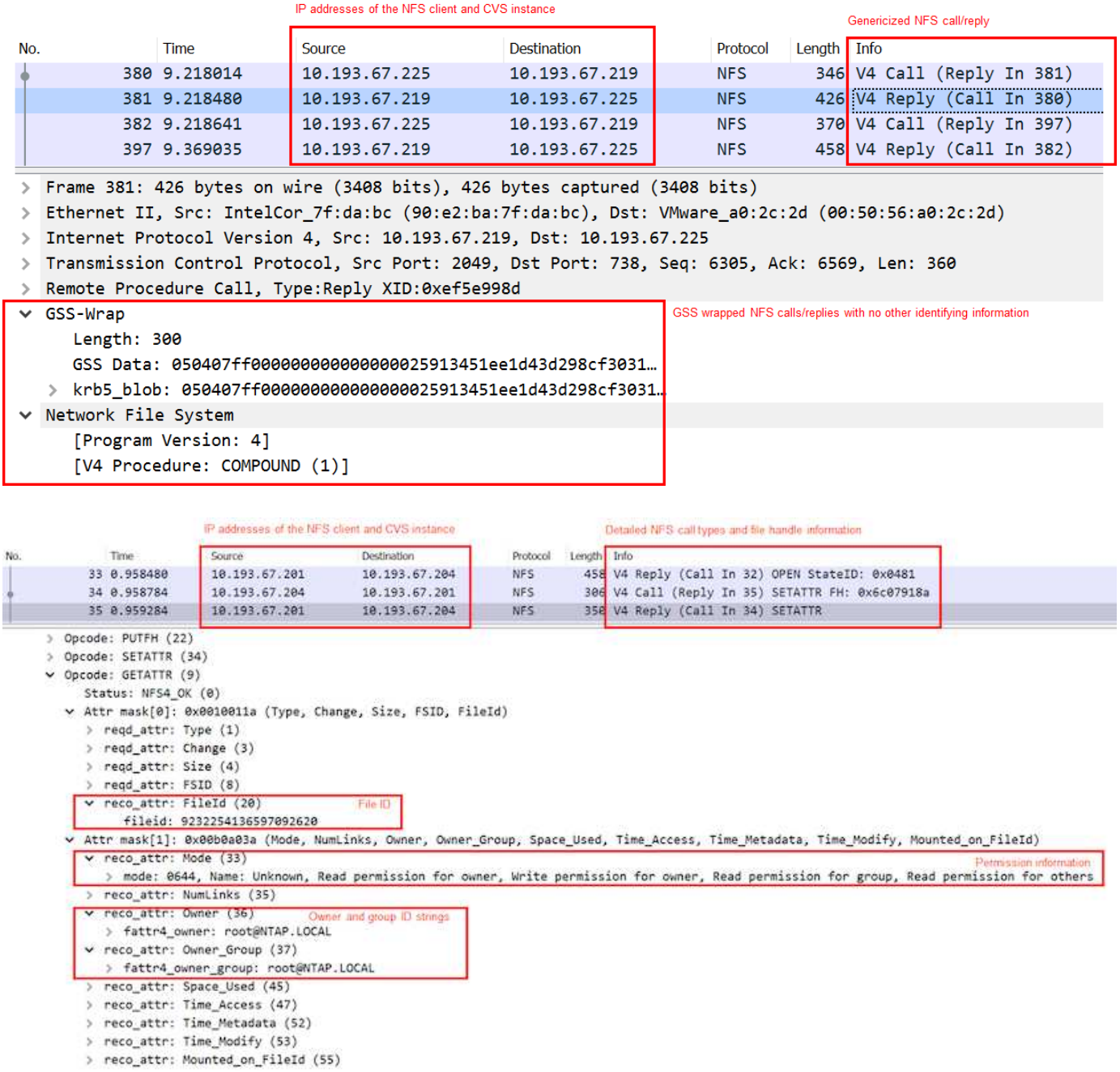
封包偵測/追蹤考量

封包擷取可用於疑難排解網路問題或其他問題（例如NAS權限、LDAP連線等）、但也可惡意用來取得網路IP位址、MAC位址、使用者和群組名稱、以及端點使用的安全層級等資訊。由於Google Cloud網路、VPC和防火牆規則的設定方式、如果沒有使用者登入認證或、就很難取得不必要的網路封包存取權 "JWT權杖" 雲端執行個體。封包擷取只能在端點（例如虛擬機器（VM））上進行、而且只能在VPC內部的端點上進行、除非使用共享VPC和（或）外部網路通道/ IP轉送來明確允許外部流量進入端點。無法從用戶端外部窺探流量。

使用共享VPC時、會使用NFS Kerberos和/或進行傳輸中加密 "SMB加密" 可以遮罩從追蹤中收集到的大部分資訊。不過、有些流量仍會以純文字形式傳送、例如 "DNS" 和 "LDAP查詢"。下圖顯示從Cloud Volumes Service來源於指令集的純文字LDAP查詢擷取的封包、以及可能公開的識別資訊。目前支援透過SSL加密或LDAP的Cloud Volumes Service LDAP查詢不支援。CVS效能支援LDAP簽署（若Active Directory要求）。CVS軟體不支援LDAP簽署。

unixUserPassword是由LDAP查詢、不會以純文字傳送、而是以Salted雜湊傳送。根據預設、Windows LDAP不會填入unixUserPassword欄位。只有當您需要利用Windows LDAP透過LDAP互動登入用戶端時、才需要此欄位。不支援互動式LDAP登入執行個體。Cloud Volumes Service

下圖顯示NFS Kerberos對話擷取的封包擷取、位於透過AUTH_SYS擷取NFS的旁邊。請注意、追蹤中的可用資訊在兩者之間有何差異、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。



VM網路介面

攻擊者可能會嘗試將新的網路介面卡（NIC）新增至中的VM "混雜模式"（連接埠鏡射）或在現有NIC上啟用雜亂模式、以利窺探所有流量。在Google Cloud中、新增NIC需要完全關閉虛擬機器、才能建立警示、因此攻擊者無法察覺。

此外、NIC完全無法設定為雜亂模式、而且會在Google Cloud中觸發警示。

控制面板架構

所有的功能都是透過API來執行。Cloud Volumes Service整合至GCP雲端主控台的BIOS管理也會使用此功能的Cloud Volumes Service Cloud Volumes Service

身分識別與存取管理

身分識別與存取管理 ("IAM"）是一項標準服務、可讓您控制Google Cloud專案執行個體的驗證（登入）和授權（權限）。Google IAM提供完整的權限授權與移除稽核追蹤。目前Cloud Volumes Service 無法提供控制面板稽核。

授權/權限總覽

IAM提供Cloud Volumes Service 內建的精細權限來執行功能。您可以找到 "請在此填寫詳細權限清單"。

IAM也提供兩種預先定義的角色：「netappcloudVolumes.admin」和「netappcloudVolumes.viewer」。這些角色可指派給特定使用者或服務帳戶。

指派適當的角色和權限、讓IAM使用者能夠管理Cloud Volumes Service 功能。

使用精細權限的範例包括：

- 建立只有「Get / List / cred/ update」權限的自訂角色、讓使用者無法刪除磁碟區。
- 使用僅具有「napshot.*」權限的自訂角色、建立用於建置應用程式一致Snapshot整合的服務帳戶。
- 建立自訂角色、將「volumereplication*」委派給特定使用者。

服務帳戶

透過Cloud Volumes Service 指令碼或進行功能不均的API呼叫 "Terraform"、您必須建立角色為「角色/netappcloudVolumes.admin」的服務帳戶。您可以使用此服務帳戶、以Cloud Volumes Service 兩種不同的方式產生驗證申請表API要求所需的JWT權杖：

- 產生Json金鑰、並使用Google API從其衍生JWT權杖。這是最簡單的方法、但需要手動管理機密（Json金鑰）。
- 使用 "服務帳戶模擬" 使用角色/iam.serviceAccountTokenCreator`。程式碼（指令碼、Terraform等）會與一起執行 "應用程式預設認證" 並模擬服務帳戶以取得其權限。這種方法反映了Google的最佳安全實務做法。

請參閱 "建立您的服務帳戶和私密金鑰" 如需詳細資訊、請參閱Google雲端文件。

部分**API Cloud Volumes Service**

利用HTTPS（TLSv1.2）作為基礎網路傳輸、藉此使用REST型API。Cloud Volumes Service您可以找到最新的API定義 "請按這裡" 以及如何使用API的相關資訊、請參閱 "Google雲端文件中的Cloud Volumes API"。

API端點由NetApp使用標準HTTPS（TLSv1.2）功能來操作及保護。

JWT權杖

API驗證是以JWT承載權杖執行 ("RFC-7519"）。必須使用Google Cloud IAM驗證來取得有效的JWT權杖。這必須透過提供服務帳戶Json金鑰、從IAM擷取權杖來完成。

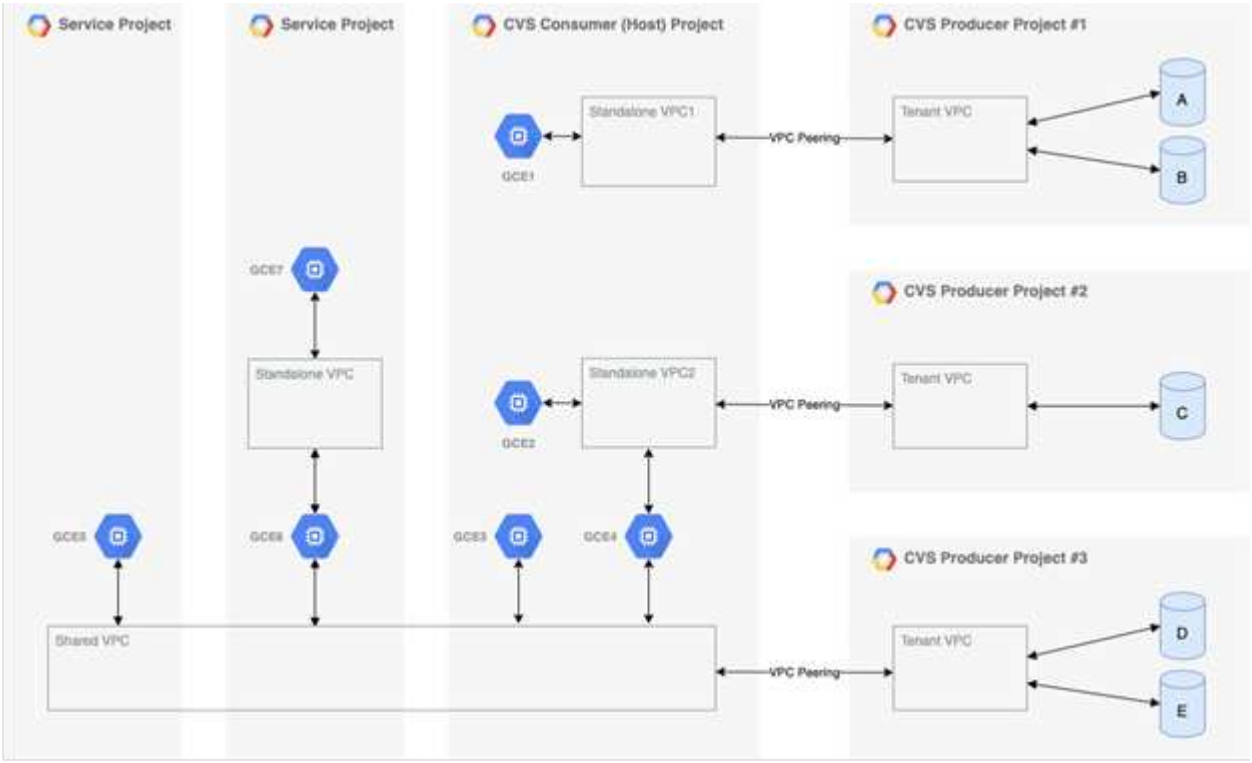
稽核記錄

目前沒有使用者可存取的控制面板稽核記錄可供使用。

適用於Google Cloud的解決方案運用Google Cloud Cloud Volumes Service "私有服務存取" 架構。在此架構中、使用者可以連線Cloud Volumes Service 到這個功能。此架構使用服務網路和VPC對等架構、如同其他Google Cloud服務、確保租戶之間完全隔離。

如需Cloud Volumes Service Google Cloud的架構總覽、請參閱 "架構Cloud Volumes Service"。

使用者VPC（獨立式或共享）會在Cloud Volumes Service 託管的代管租戶專案中連接至VPC、以裝載這些磁碟區。



上圖顯示一個專案（中間是CVS消費者專案）、其中三個VPC網路連接Cloud Volumes Service 到多個運算引擎VM（GCE1-7）共用磁碟區：

- VPC1允許GCE1存取磁碟區A和B
- VPC2可讓GCE2和GCE4存取Volume C
- 第三個VPC網路是共享的VPC、與兩個服務專案共用。它可讓GCE3、GCE4、GCE5和GCE6存取Volume D和E共享VPC網路僅支援CVS效能服務類型的磁碟區。

GCE7無法存取任何Volume。

資料可在傳輸中（使用Kerberos和/或SMB加密）加密、Cloud Volumes Service 也可在支援中加密。

傳輸中的資料加密

傳輸中的資料可在NAS傳輸協定層加密、Google Cloud網路本身也會加密、如下列各節所述。

Google Cloud網路

Google Cloud會加密網路層級的流量、如所述 "傳輸中加密" 在Google文件中。如「Cloud Volumes Services Architecture」一節所述、Cloud Volumes Service NetApp控制的PSAPa生產商專案將提供此功能。

在CVs-SW的情況下、生產商租戶會執行Google VM來提供服務。Google Cloud Volumes Service 會自動加密使用者VM和不支援的VM之間的流量。

雖然CVS效能的資料路徑在網路層上並未完全加密、但NetApp與Google仍使用這種組合 "IEEE 802.1AE加密（MAC安全）"、 "封裝" （資料加密）和實體受限的網路、以保護Cloud Volumes Service 資料在整個過程中在整個過程中在靜止CVS效能服務類型和Google Cloud之間傳輸。

NAS傳輸協定

NFS和SMB NAS傳輸協定可在傳輸協定層提供選用的傳輸加密。

SMB加密

"SMB加密" 提供SMB資料的端點對端點加密、並保護資料免於在不受信任的網路上遭人竊取。您可以啟用用戶端/伺服器資料連線（僅適用於支援SMB3.x的用戶端）和伺服器/網域控制器驗證的加密。

啟用SMB加密時、不支援加密的用戶端將無法存取共用區。

支援RC4-HMAC、AES-122-CTS-HMA-SHA1和AES-256-CTS-HMA-SHA1安全密碼、以進行SMB加密。Cloud Volumes ServiceSMB會交涉至伺服器支援的最高加密類型。

NFSv4.1 Kerberos

對於NFSv4.1、CVS效能提供如所述的Kerberos驗證 "RFC7530"。您可以針對每個磁碟區啟用Kerberos。

Kerberos目前最強大的加密類型是AES-256-CTS-HMA-SHA1。NetApp Cloud Volumes Service 支援AES-256-CTS-HMA-SHA1、AES-123-CTS-HMA-SHA1、DES3和DES for NFS。它也支援CIFS/SMB流量的ARCFOUR-HMAC（RC4）、但不支援NFS。

Kerberos為NFS裝載提供三種不同的安全性層級、可讓您選擇Kerberos安全性的強度。

根據RedHat "通用掛載選項" 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.
```

一般而言、Kerberos安全性層級越高、效能就越差、因為用戶端和伺服器花費時間來加密和解密所傳送的每個封包的NFS作業。許多用戶端和NFS伺服器都支援AES-NI卸載至CPU、以獲得更好的整體體驗、但Kerberos 5p（完整端對端加密）的效能影響遠高於Kerberos 5（使用者驗證）的影響。

下表顯示每個層級在安全性和效能方面的差異。

安全性層級	安全性	效能
NFSv3—系統	• 最不安全；純文字、含數字使用者ID /群組ID • 能夠檢視UID、GID、用戶端IP位址、匯出路徑、檔案名稱、封包擷取的權限	• 最適合大多數情況
NFSv4.x—系統	• 比NFSv3（用戶端ID、名稱字串/網域字串比對）更安全、但仍是純文字 • 能夠檢視UID、GID、用戶端IP位址、名稱字串、網域ID、 在封包擷取中匯出路徑、檔案名稱、權限	• 適合連續工作負載（例如VM、資料庫、大型檔案） • 高檔案數/高中繼資料的不良（差30-50%）
NFS—KRB5	• 每個NFS封包中的認證Kerberos加密：在GSS包裝程式的RPC呼叫中、將使用者/群組的UID/GID封包起來 • 要求存取掛載的使用者需要有效的Kerberos票證（透過使用者名稱/密碼或手動金鑰索引標籤交換）；票證會在指定的時間段後過期、使用者必須重新驗證才能存取 • 不加密NFS作業或掛載/連接埠對應器/ NLM等輔助通訊協定（可參閱匯出路徑、IP位址、檔案處理、權限、檔案名稱、 封包擷取的時間/時間）	• 在大多數情況下最佳的Kerberos；比AUTH_SYS更糟

安全性層級	安全性	效能
NFS：krb5i	• 每個NFS封包中的認證Kerberos加密：在GSS包裝程式的RPC呼叫中、將使用者/群組的UID/GID封包起來 • 要求存取掛載的使用者需要有效的Kerberos票證（透過使用者名稱/密碼或手動金鑰索引標籤交換）；票證會在指定的時間段後過期、使用者必須重新驗證才能存取 • 不加密NFS作業或掛載/連接埠對應器/ NLM等輔助通訊協定（可參閱匯出路徑、IP位址、檔案處理、權限、檔案名稱、 封包擷取的時間/時間） • 每個封包都會新增Kerberos GSS Checksum、以確保不會攔截封包。如果校驗和相符、則允許對話。	• 優於krb5p、因為NFS有效負載未加密；只有與krb5相比、新增的額外負荷才是完整性Checksum。krb5i的效能不會比krb5差很多、但會有一些降低。
NFS–krb5p	• 每個NFS封包中的認證Kerberos加密：在GSS包裝程式的RPC呼叫中、將使用者/群組的UID/GID封包起來 • 要求存取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Keytab交換）；票證會在指定的時間段後過期、而且使用者必須重新驗證才能存取 • 所有NFS封包有效負載都會使用GSS包裝進行加密（無法在封包擷取中看到檔案處理代碼、權限、檔案名稱、atime/mtime）。 • 包括完整性檢查。 • NFS作業類型可見（Fsinfo, access, GetAttr等）。 • 輔助通訊協定（掛載、連接埠對應、NLM等）未加密-（請參閱匯出路徑、IP位址）	• 安全性層級效能最差；krb5p必須加密/解密更多資料。 • 使用NFSv4.x的效能優於krb5p、適用於高檔案數工作負載。

在VMware中、已設定的Active Directory伺服器會做為Kerberos伺服器和LDAP伺服器（從RFC2307相容架構查詢使用者身分）Cloud Volumes Service 。不支援其他Kerberos或LDAP伺服器。NetApp強烈建議您使用LDAP進行Cloud Volumes Service 身分識別管理。如需有關NFS Kerberos如何顯示在封包擷取中的資訊、請參閱一節"「封包偵測/追蹤考量。」"

閒置資料加密

所有的流通量Cloud Volumes Service 均使用AES-256加密進行閒置加密、這表示寫入媒體的所有使用者資料都會加密、而且只能使用每個磁碟區的金鑰來解密。

- 在CVS軟體中、會使用Google產生的金鑰。
- 如需CVS效能、每個Volume金鑰會儲存在Cloud Volumes Service 內建於此功能的關鍵管理程式中。

自2021年11月起、客戶管理的加密金鑰（CMEK）功能已可供預覽。這可讓您使用裝載於的每個專案個別區域主金鑰來加密每個Volume金鑰 "Google金鑰管理服務（KMS）。" KMS可讓您附加外部金鑰管理程式。

如需設定KMS以獲得CVS效能的相關資訊、請參閱 "設定客戶管理的加密金鑰"。

防火牆

可公開多個TCP連接埠以服務NFS和SMB共用：Cloud Volumes Service

- "NFS存取所需的連接埠"
- "SMB存取所需的連接埠"

此外、SMB、含LDAP的NFS（包括Kerberos）及雙傳輸協定組態、都需要存取Windows Active Directory網域。Active Directory連線必須是 "已設定" 以每個區域為基礎。Active Directory網域控制器（DC）是使用來識別 "DNS型DC探索" 使用指定的DNS伺服器。系統會使用任何傳回的DC。指定Active Directory站台可限制合格的DC清單。

使用分配給的CIDR範圍內的IP位址、即可將其移出Cloud Volumes Service `gcloud compute address` 命令的同時 "登入Cloud Volumes Service 時"。您可以使用此CIDR做為來源位址、為Active Directory網域控制器設定傳入防火牆。

Active Directory網域控制器必須具備 "請依照Cloud Volumes Service 此處所述、將連接埠公開給這些開發署"。

NAS傳輸協定

NAS傳輸協定總覽

NAS傳輸協定包括NFS（v3和v4.1）和SMB/CIFS（2.x和3.x）。這些通訊協定是CVS如何允許跨多個NAS用戶端共用存取資料。此外Cloud Volumes Service 、支援同時存取NFS和SMB/CIFS用戶端（雙傳輸協定）、同時遵守NAS共用中檔案和資料夾的所有身分識別和權限設定。為了維持最高的資料傳輸安全性、Cloud Volumes Service 支援使用SMB加密和NFS Kerberos 5p的傳輸協定加密。

雙傳輸協定僅適用於CVs-Performance。

NAS傳輸協定的基本概念

NAS傳輸協定是讓網路上的多個用戶端存取儲存系統上相同資料的方法、例如Cloud Volumes Service GPC上的NFS和SMB是定義的NAS傳輸協定、可在Cloud Volumes Service 客戶端/伺服器上運作、其中的伺服器是由支援服務器使用。用戶端會傳送存取、

讀取和寫入要求給伺服器、伺服器負責協調檔案的鎖定機制、儲存權限、以及處理身分識別和驗證要求。

例如、如果NAS用戶端想要在資料夾中建立新檔案、則會遵循下列一般程序。

1. 用戶端會要求伺服器提供目錄的相關資訊（權限、擁有者、群組、檔案ID、可用空間、 等）；如果要求的用戶端和使用者對父資料夾擁有必要的權限、伺服器就會回應該資訊。
2. 如果目錄上的權限允許存取、則用戶端會詢問伺服器所建立的檔案名稱是否已存在於檔案系統中。如果檔案名稱已在使用中、建立就會失敗。如果檔案名稱不存在、伺服器會讓用戶端知道它可以繼續。
3. 用戶端會呼叫伺服器、以使用目錄處理和檔案名稱來建立檔案、並設定存取和修改時間。伺服器會對檔案發出唯一的檔案ID、以確保沒有以相同的檔案ID建立其他檔案。
4. 用戶端會在寫入作業之前傳送呼叫來檢查檔案屬性。如果權限允許、用戶端就會寫入新檔案。如果傳輸協定/應用程式使用鎖定、用戶端會要求伺服器提供鎖定、以防止其他用戶端在鎖定時存取檔案、以避免資料毀損。

NFS

NFS是一種分散式檔案系統傳輸協定、是在Request for Comments（RFC）中定義的開放式IETF標準、可讓任何人實作該傳輸協定。

透過匯出可供用戶端或一組用戶端存取的路徑、將位於此功能的Volume Cloud Volumes Service 共享給NFS用戶端。掛載這些匯出的權限是由匯出原則和規則所定義、Cloud Volumes Service 這些原則和規則可由資訊管理員設定。

NetApp NFS實作被視為傳輸協定的黃金標準、可用於無數的企業NAS環境。以下各節涵蓋Cloud Volumes Service 支援的NFS和特定安全功能、以及如何實作這些功能。

預設的本機**UNIX**使用者和群組

包含多個預設UNIX使用者和群組、可提供各種基本功能。Cloud Volumes Service這些使用者和群組目前無法修改或刪除。目前無法將新的本機使用者和群組新增Cloud Volumes Service 至無法更新的功能。外部LDAP名稱服務必須提供預設使用者和群組以外的UNIX使用者和群組。

下表顯示預設使用者和群組及其對應的數字ID。NetApp建議不要在LDAP或重新使用這些數字ID的本機用戶端上建立新的使用者或群組。

預設使用者：數字**ID**	預設群組：數字**ID**
• 根目錄：0 • pcuser:65534 • 無人：65535	• 根目錄：0 • 精靈：1. • pcuser:65534 • 無人：65535

使用NFSv4.1時、root使用者在NFS用戶端上執行列出命令的目錄時、可能會顯示為nobnobody。這是因為用戶端的ID網域對應組態。請參閱「」一節 NFSv4.1和nobody使用者/群組 以取得此問題的詳細資訊及解決方法。

root使用者

在Linux中、root帳戶可以存取Linux型檔案系統中的所有命令、檔案和資料夾。由於此帳戶的強大功能、安全性最佳實務做法通常會要求root使用者停用或限制某種方式。在NFS匯出中、root使用者對檔案和資料夾的控制能力、可Cloud Volumes Service 透過匯出原則和規則、以及稱為root squash的概念、在整個過程中加以控制。

root使用者之間的衝突可確保存取NFS掛載的root使用者被擠到匿名的數字使用者65534（請參閱「」一節）[匿名使用者]」）、目前僅適用於使用CVS效能的情況、方法是在建立匯出原則規則期間選取「Off」（關閉）進行root存取。如果root使用者被擠到匿名使用者、就無法再執行chown或 "setuid/setgid命令（sticky位元）" 在NFS掛載的檔案或資料夾上、root使用者建立的檔案或資料夾會將anon UID顯示為擁有者/群組。此外、NFSv4 ACL無法由root使用者修改。不過、root使用者仍可存取不具有明確權限的chmod和刪除檔案。如果您想限制root使用者的檔案和資料夾權限存取、請考慮使用具有NTFS ACL的磁碟區、建立名為「root」的Windows使用者、並將所需權限套用至檔案或資料夾。

匿名使用者

匿名（anon）使用者ID會指定對應至用戶端要求的UNIX使用者ID或使用者名稱、而該用戶端要求沒有有效的NFS認證。使用root使用者時、這可能包括root使用者。Anon的Cloud Volumes Service 使用者是65534。

此UID通常與Linux環境中的使用者名稱「nobnob」或「nfsnobn」相關聯。也使用65534作為本機UNIX使用者的pcuser'（請參閱「Cloud Volumes Service預設的本機UNIX使用者和群組」）、這也是Windows到UNIX名稱對應的預設後援使用者、但LDAP中找不到有效的相符UNIX使用者。

由於Linux使用者名稱與Cloud Volumes Service 適用於UID 65534的使用者名稱不同、因此使用NFSv4.1時對應至65534的使用者名稱字串可能不相符。因此、您可能會在某些檔案和資料夾上看到「無人」的使用者身分。請參閱「」一節NFSv4.1和nobody使用者/群組」以取得此問題的相關資訊及解決方法。

存取控制/匯出

NFS裝載的初始匯出/共用存取是透過匯出原則中包含的主機型匯出原則規則來控制。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共用區、以及允許存取主機的層級。匯出原則規則組態選項取決於Cloud Volumes Service 哪些方面。

對於CVS軟體、下列選項可用於匯出原則組態：

- *用戶端相符*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。*選取「讀取/寫入」或「唯讀」來控制對EXPE/CVs-Performance的存取層級、提供下列選項：
- *用戶端相符*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。*選取「讀取/寫入」或「唯讀」以控制匯出的存取層級。
- *根存取權（開啟/關閉）。*設定根分區（請參閱「[root使用者]」的詳細資料）。
- *傳輸協定類型。*這會將NFS掛載的存取限制為特定的傳輸協定版本。為Volume指定NFSv3和NFSv4.1時、請將兩者留白或同時勾選兩個方塊。
- * Kerberos安全性層級（選取「啟用Kerberos」時）。*提供krb5、krb5i及/或krb5p選項、以進行唯讀或讀寫存取。

變更擁有權（**chown**）和變更群組（**chgrp**）

NFS on Cloud Volumes Service 支援僅允許root使用者在檔案和資料夾上執行chown / chgrp。其他使用者也會看到「不允許操作」錯誤、即使是他們自己擁有的檔案也一樣。如果您使用root quash（如一節中所述）[root使

用者]」）時、root會被擠到非root使用者、且不允許存取chown和chgrp。目前在不允許非root使用者使用chown和chgrp的因應措施Cloud Volumes Service 。如果需要變更擁有權、請考慮使用雙傳輸協定磁碟區、並將安全樣式設定為NTFS、以便從Windows端控制權限。

權限管理

支援兩種模式位元（例如rwx的644、777等）和NFSv4.1 ACL、以控制使用UNIX安全型態之磁碟區在NFS用戶端上的權限。Cloud Volumes Service標準權限管理用於這些項目（例如、chmod、chown或nfs4_setfacl）、並可與任何支援這些項目的Linux用戶端搭配使用。

此外、當使用設為NTFS的雙傳輸協定磁碟區時、NFS用戶端可以利用Cloud Volumes Service 指向Windows使用者的名稱對應功能來解析NTFS權限。這需要LDAP連線Cloud Volumes Service 至才能提供數字ID對使用者名稱的轉譯、因為Cloud Volumes Service 需要有效的UNIX使用者名稱才能正確對應至Windows使用者名稱。

為**NFSv3**提供精細的**ACL**

模式位元權限僅涵蓋語義中的擁有者、群組及其他所有人、這表示基本NFSv3沒有精細的使用者存取控制。由於不支援POSIX ACL、也不支援擴充屬性（例如chatr）、因此使用NFSv3時、只有在下列情況下才能使用精細的ACL：Cloud Volumes Service

- NTFS安全型磁碟區（需要CIFS伺服器）、具有有效的UNIX至Windows使用者對應。
- 使用管理用戶端掛載NFSv4.1套用NFSv4.1 ACL以套用ACL。

這兩種方法都需要LDAP連線才能進行UNIX身分識別管理、並填入有效的UNIX使用者和群組資訊（請參閱一節"「LDAP」"）和僅適用於CVS效能執行個體。若要將NTFS安全型磁碟區搭配NFS使用、您必須使用雙傳輸協定（SMB和NFSv3）或雙傳輸協定（SMB和NFSv4.1）、即使沒有建立SMB連線。若要在NFSv3掛載中使用NFSv4.1 ACL、您必須選取「兩者（NFSv3/NFSv4.1）」作為傳輸協定類型。

一般UNIX模式位元在權限方面的精細度與NTFS或NFSv4.x ACL所提供的精細度不同。下表比較NFSv3模式位元與NFSv4.1 ACL之間的權限精細度。如需NFSv4.1 ACL的相關資訊、請參閱 "nfs4_ACL - NFSv4存取控制清單"。

NFSv3模式位元	NFSv4.1 ACL
• 設定執行時的使用者ID • 設定執行時的群組ID • 儲存交換的文字（未在POSIX中定義） • 擁有者的讀取權限 • 擁有者的寫入權限 • 對檔案擁有者執行權限；或在目錄中查詢（搜尋）擁有者權限 • 群組的讀取權限 • 群組的寫入權限 • 對檔案上的群組執行權限；或查詢（搜尋）目錄中的群組權限 • 其他人的讀取權限 • 其他人的寫入權限 • 對檔案上的其他人執行權限；或查詢（搜尋）目錄中的其他人權限	存取控制項目（ACE）類型（允許/拒絕/稽核）*繼承旗標*目錄繼承*檔案繼承*不傳播繼承*僅繼承 權限*讀取資料（檔案）/ list-directory（目錄）寫入資料（檔案）/建立檔案（目錄）*附加資料（檔案）/ **create**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*寫入屬性*讀取命名屬性*寫入命名屬性*寫入命名屬性 ACL

最後、根據RPC封包限制、NFS群組成員資格（NFSv3和NFSv4.x）的AUTH_SYS預設上限為16。NFS Kerberos最多可提供32個群組、NFSv4 ACL則可透過精細的使用者和群組ACL（每個ACE最多可容納1024個項目）來移除限制。

此外Cloud Volumes Service 、支援範圍更廣泛、最多可將支援的群組數量擴充至32個。這需要LDAP連線至包含有效UNIX使用者和群組身分識別的LDAP伺服器。如需設定此項目的詳細資訊、請參閱 "建立及管理NFS磁碟區" 在Google文件中。

NFSv3使用者與群組ID

NFSv3使用者和群組ID會以數字ID而非名稱的形式出現在線路上。使用NFSv3時、由於UNIX安全型磁碟區只使用模式位元、因此無法針對這些數字ID進行使用者名稱解析。Cloud Volumes Service當NFSv4.1 ACL存在時、即使使用NFSv3、仍需要數字ID查詢和/或名稱字串查詢、才能正確解析ACL。使用NTFS安全型磁碟區時Cloud Volumes Service 、必須先將數字ID解析為有效的UNIX使用者、然後對應至有效的Windows使用者以協商存取權限。

NFSv3使用者與群組ID的安全性限制

使用NFSv3時、用戶端和伺服器永遠不需要確認使用者使用數字ID進行讀取或寫入、這只是隱含信任而已。如此一來、只要偽造任何數字ID、檔案系統就會遭受潛在的資料外洩。為了避免這類安全漏洞、Cloud Volumes Service 我們提供一些選項供大家選擇。

- 實作Kerberos for NFS會強制使用者使用使用者名稱和密碼或Keytab檔案進行驗證、以取得Kerberos票證、以便存取掛載。Kerberos適用於CVS效能執行個體、僅適用於NFSv4.1。
- 限制匯出原則規則中的主機清單、會限制NFSv3用戶端存取Cloud Volumes Service 該卷的權限。
- 使用雙傳輸協定磁碟區並將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使用者名稱、以便正確驗證以存取裝載。這需要啟用LDAP並設定UNIX使用者和群組身分識別。

- 浪費root使用者的力量可限制root使用者對NFS掛載所造成的損害、但並不會完全消除風險。如需詳細資訊、請參閱「」一節[root使用者]。」

最後、NFS安全性僅限於您所使用的傳輸協定版本。NFSv3的整體效能比NFSv4.1高、但提供的安全性層級卻不相同。

NFSv4.1

NFSv4.1提供比NFSv3更高的安全性與可靠性、原因如下：

- 透過租賃型機制進行整合式鎖定
- 狀態工作階段
- 單一連接埠上的所有NFS功能（2049）
- 僅TCP
- ID網域對應
- Kerberos整合（NFSv3可以使用Kerberos、但僅適用於NFS、而非用於NLM等輔助傳輸協定）

NFSv4.1相依性

由於NFSv4.1還有額外的安全功能、因此不需要使用NFSv3（類似於SMB需要相依性（例如Active Directory）的方式）、也會涉及一些外部相依性。

NFSv4.1 ACL

支援NFSv4.x ACL、相較於一般的POSIX式權限、可提供明顯的優勢、例如：Cloud Volumes Service

- 精細控制使用者對檔案和目錄的存取
- 更好的NFS安全性
- 改善與CIFS/SMB的互通性
- 使用AUTH_SYS安全性移除每位使用者16個群組的NFS限制
- ACL不需要群組ID（GID）解析、因此能有效移除GID限制NFSv4.1 ACL、而非Cloud Volumes Service 從無法更新的NFS用戶端控制。若要使用NFSv4.1 ACL、請確定用戶端的軟體版本支援這些ACL、並已安裝適當的NFS公用程式。

NFSv4.1 ACL與**SMB**用戶端之間的相容性

NFSv4 ACL與Windows檔案層級ACL（NTFS ACL）不同、但具有類似的功能。不過、在多重傳輸協定NAS環境中、如果有NFSv4.1 ACL、而且您使用的是雙傳輸協定存取（NFS和SMB位於同一個資料集）、則使用SMB2.0及更新版本的用戶端將無法從Windows安全性索引標籤檢視或管理ACL。

NFSv4.1 ACL的運作方式

下列術語為參考定義：

- *存取控制清單（ACL）。*權限項目清單。
- *存取控制項目（ACE）。*清單中的權限項目。

當用戶端在設定作業期間、在檔案上設定NFSv4.1 ACL時、Cloud Volumes Service 會將物件上的ACL設定為由任何現有的ACL取代。如果檔案上沒有ACL、則檔案的模式權限會從Owner@、group @和任何人@計算。如果檔案上有任何現有的SUID/SGID/便利貼位元、則不會受到影響。

當用戶端在GetAttr作業期間取得檔案的NFSv4.1 ACL時、Cloud Volumes Service 會讀取與物件相關聯的NFSv4.1 ACL、建構ACE清單、並將清單傳回用戶端。如果檔案具有NT ACL或模式位元、則會從模式位元建構ACL並傳回用戶端。

如果ACL中存在拒絕的ACE、則會拒絕存取；如果存在允許的ACE、則會授予存取權。不過、如果ACL中沒有任何ACE、也會拒絕存取。

安全性描述元由安全性ACL（SACL）和判別ACL（DACL）組成。當NFSv4.1與CIFS/SMB互操作時、DACL會以一對一的方式對應NFSv4和CIFS。DACL由允許和拒絕的ACE組成。

如果在已設定NFSv4.1 ACL的檔案或資料夾上執行基本的「chmod」、則會保留現有的使用者和群組ACL、但會修改預設的「擁有者」、「群組@」、「每個人@」ACL。

使用NFSv4.1 ACL的用戶端可以設定及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、該物件會繼承ACL中已標記適當的所有ACE "繼承旗標"。

如果檔案或目錄具有NFSv4.1 ACL、則無論使用哪種傳輸協定來存取檔案或目錄、該ACL都能用來控制存取。

只要將ACE標記為正確的繼承旗標、檔案和目錄就會從父目錄的NFSv4 ACL繼承ACE（可能需要適當的修改）。

當檔案或目錄是因NFSv4要求而建立時、產生的檔案或目錄上的ACL取決於檔案建立要求是否包含ACL或僅包含標準UNIX檔案存取權限。ACL也取決於父目錄是否具有ACL。

- 如果要求包含ACL、則會使用該ACL。
- 如果要求僅包含標準UNIX檔案存取權限、且父目錄沒有ACL、則會使用用戶端檔案模式來設定標準UNIX檔案存取權限。
- 如果要求僅包含標準UNIX檔案存取權限、且父目錄具有不可繼承的ACL、則會針對新物件設定以傳遞至要求的模式位元為基礎的預設ACL。
- 如果要求僅包含標準UNIX檔案存取權限、但父目錄具有ACL、則只要將ACE標記為適當的繼承旗標、父目錄ACL中的ACE就會由新檔案或目錄繼承。

ACE權限

NFSv4.1 ACL權限使用一系列大小寫字母值（例如「raptncy」）來控制存取。如需這些字母值的詳細資訊、請參閱 "使用方法：使用NFSv4 ACL"。

具有**umask**和**ACL**繼承的**NFSv4.1 ACL**行為

"NFSv4 ACL可提供ACL繼承功能"。ACL繼承意味著在使用NFSv4.1 ACL集的物件下建立的檔案或資料夾、可以根據的組態來繼承ACL "ACL繼承旗標"。

"umask" 用於控制在目錄中建立檔案和資料夾的權限等級、而無需系統管理員互動。根據預設Cloud Volumes Service 、支援使用者使用支援功能來覆寫繼承的ACL、這是預期的行為 "RFC 5661"。

ACL格式化

NFSv4.1 ACL具有特定格式化。下列範例是檔案上的ACE設定：

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上述範例遵循下列ACL格式準則：

```
type:flags:principal:permissions
```

一種「A」表示「允許」。 在此情況下不會設定繼承旗標、因為主體不是群組、不包含繼承。此外、由於ACE不是稽核項目、因此不需要設定稽核旗標。如需NFSv4.1 ACL的詳細資訊、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）、則ACL可能無法如預期般運作、或ACL變更可能無法套用及拋出錯誤。

範例錯誤包括：

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

明確拒絕

NFSv4.1權限可包含擁有者、群組及所有人的明確拒絕屬性。這是因為NFSv4.1 ACL是預設拒絕ACL、這表示如果某個ACL未由ACE明確授予、就會拒絕該ACL。明確拒絕屬性會覆寫任何明確或不明確的存取ACE。

拒絕ACE的屬性標籤設定為「D」。

在以下範例中、允許群組@擁有所有讀取和執行權限、但拒絕所有寫入權限。

```
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
```

應盡可能避免使用拒絕的ACE、因為它們可能會造成混淆和複雜；允許不明確定義的ACL被隱含拒絕。當設定拒絕ACE時、使用者預期會被授予存取權限時、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：

- 擁有者擁有完整權利。
- 群組具有唯讀。
- 其他人則為唯讀。

不過、即使權限調整為等同的775個權限、仍會因為每個人都設定明確的拒絕權限而拒絕存取。

NFSv4.1 ID網域對應相依性

NFSv4.1利用ID網域對應邏輯做為安全層、協助驗證嘗試存取NFSv4.1掛載的使用者確實是他們宣稱的對象。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名稱字串、並傳送至Cloud Volumes Service該實例。如果該使用者名稱/群組名稱和ID字串組合不相符、則使用者和（或）群組會被擠到用戶端上「/etc/idmapd.conf」檔案中指定的預設nober使用者。

此ID字串是適當遵循權限的必要條件、尤其是使用NFSv4.1 ACL和/或Kerberos時。因此、需要使用名稱服務伺服器相依性（例如LDAP伺服器）來確保用戶端之間的一致性、Cloud Volumes Service 以及使用者和群組名稱身分識別解析是否正確。

使用靜態預設ID網域名稱值「defaultv4iddomain.com」Cloud Volumes Service 。NFS用戶端的ID網域名稱設定預設為DNS網域名稱、但您可以在「/etc/idmapd.conf」中手動調整ID網域名稱。

如果在Cloud Volumes Service 支援功能中啟用LDAP、Cloud Volumes Service 則當NFS ID網域在DNS中變更為搜尋網域所設定的項目時、不需要修改用戶端、除非他們使用不同的DNS網域搜尋名稱。

當能夠解析本機檔案或LDAP中的使用者名稱或群組名稱時、會使用網域字串、而非相符的網域ID則會對nobnobody進行儲存。Cloud Volumes Service如果Cloud Volumes Service 無法在本機檔案或LDAP中找到使用者名稱或群組名稱、則會使用數字ID值、NFS用戶端會正確解析名稱（這與NFSv3行為類似）。

在不變更用戶端的NFSv4.1 ID網域以符合Cloud Volumes Service 使用的功能的情況下、您會看到下列行為：

- UNIX使用者和群組的本機項目Cloud Volumes Service （例如root、如本機UNIX使用者和群組所定義）會被浪費在nobnobody值。
- 如果Cloud Volumes Service DNS網域不同於NFS用戶端和Cloud Volumes Service 更新、則UNIX使用者和在LDAP中有項目的群組（如果將Sfuse設定為使用LDAP）會被浪費給任何人。
- 沒有本機項目或LDAP項目的UNIX使用者和群組會使用數字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、則只會顯示數字ID。

以下顯示上述案例的結果：

```
# 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
```

當用戶端和伺服器ID網域相符時、相同的檔案清單看起來就像這樣：

```
# 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
```

如需此問題及其解決方法的詳細資訊、請參閱「」一節NFSv4.1和nobody使用者/群組。」

Kerberos相依性

如果您打算使用Kerberos搭配NFS、Cloud Volumes Service 則必須搭配下列功能搭配使用才能使用：

- 適用於Kerberos Distribution Center服務（Kdc）的Active Directory網域
- Active Directory網域中的使用者和群組屬性會填入UNIX資訊以供LDAP功能使用（Cloud Volumes Service 在列舉NFS Kerberos時、需要使用者的SPN-UNIX使用者對應才能正常運作）。
- LDAP已在Cloud Volumes Service 實例上啟用
- DNS服務的Active Directory網域

NFSv4.1和**nobody**使用者/群組

NFSv4.1組態最常見的問題之一、就是檔案或資料夾列在使用「ls」的清單中、顯示為「user:group」的「nobnon:nobnobnone」組合。

例如：

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

數字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、檔案可能會顯示正確的擁有者、但不會顯示「nobody」為群組。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

誰是無人？

NFSv4.1中的「nobn」使用者與「nfsnobnobn」使用者不同。您可以執行「id」命令來檢視NFS用戶端如何查

看每位使用者：

```
# 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時、「noban」使用者是由「idmapd.conf」檔案定義的預設使用者、可定義為任何您要使用的使用者。

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

為什麼會發生這種情況？

由於透過名稱字串對應來確保安全性是NFSv4.1作業的重要宗旨、因此名稱字串不適當時的預設行為是將該使用者分成通常無法存取使用者和群組所擁有之檔案和資料夾的使用者。

當您在檔案清單中看到使用者和（或）群組的「nobnoby」時、這通常表示NFSv4.1中的某些項目設定錯誤。區分大小寫的功能可在此處發揮。

例如、如果user1@CVSDEM.LOSLL（uid、1234、gid、1234）正在存取匯出、Cloud Volumes Service 則必須找到user1@CVSDEM.LOSLL（uid、gid、1234）。如果Cloud Volumes Service 使用者在支援資料的範本中是USER1@CVSDEMO.在許多情況下、您可以在用戶端的訊息檔案中看到下列內容：

```
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'
```

用戶端和伺服器必須都同意使用者確實是他們聲稱的對象、因此您必須檢查下列項目、以確保用戶端看到的使用者擁有Cloud Volumes Service 與此使用者相同的資訊。

- * NFSv4.x ID網域。*用戶端：「idmapd.conf」檔案；Cloud Volumes Service 使用「defaultv4iddomain.com」、無法手動變更。如果將LDAP搭配NFSv4.1使用、Cloud Volumes Service 則將ID網域變更為DNS搜尋網域所使用的網域、與AD網域相同。
- *使用者名稱和數字ID。*這會決定用戶端尋找使用者名稱的位置、並運用名稱服務交換器組態：用戶端：「nsswitch.conf」和（或）本機密碼和群組檔案；Cloud Volumes Service 不允許對此進行修改、但會在啟用時自動將LDAP新增至組態。
- *群組名稱和數字ID。*這會決定用戶端尋找群組名稱的位置、並運用名稱服務交換器組態（用戶端：「nsswitch.conf」和/或本機密碼和群組檔案）；Cloud Volumes Service 不允許對此進行修改、但會在啟用時自動將LDAP新增至組態。

在幾乎所有的情況Cloud Volumes Service 下、如果您在用戶端的使用者和群組清單中看到「nobnoby」、問題在於使用者或群組名稱網域ID轉譯功能會在更新到NFS用戶端之間進行。若要避免這種情況發生、請使用LDAP

來解決用戶端和Cloud Volumes Service 客戶端之間的使用者和群組資訊。

在用戶端上檢視**NFSv4.1**的名稱**ID**字串

如果您使用NFSv4.1、NFS作業期間會發生名稱字串對應、如前所述。

除了使用「/var/log/Messages」來找出NFSv4 ID的問題、您也可以使用 "nfsidmap -l" NFS用戶端上的命令、可檢視哪些使用者名稱已正確對應至NFSv4網域。

例如、此命令會在用戶端找到使用者之後輸出、Cloud Volumes Service 並由用戶端存取NFSv4.x掛載：

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

如果未正確對應至NFSv4.1 ID網域的使用者（在此案例中為「NetApp-user」）嘗試存取相同的掛載、並接觸檔案、就會依照預期指派「nobnan:nobnobnobn」。

```
# 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
```

nfidmap -l輸出顯示螢幕上的使用者為「pcuser"、但不是「NetApp-user"；這是我們的匯出原則規則（「65534」）中的匿名使用者。

```
# 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開發的網路檔案共用傳輸協定、可透過乙太網路為多個SMB用戶端提供集中式使用者/群組驗證、權限、鎖定及檔案共用。檔案和資料夾會以共用的方式呈現給用戶端、您可以設定各種共用內容、並透過共用層級權限來提供存取控制。SMB可以呈現給任何支援該傳輸協定的用戶端、包括Windows、Apple和Linux用戶端。

支援SMB 2.1和3.x版的傳輸協定。Cloud Volumes Service

存取控制/**SMB**共用區

- 當Windows使用者名稱要求存取Cloud Volumes Service 到此卷時、Cloud Volumes Service 功能區會使用Cloud Volumes Service 由管理員設定的方法尋找UNIX使用者名稱。
- 如果已設定外部UNIX身分識別供應商（LDAP）、且Windows / UNIX使用者名稱相同、則Windows使用者名稱會將1：1對應至UNIX使用者名稱、而不需要任何額外的組態。啟用LDAP時、會使用Active Directory來裝載使用者和群組物件的UNIX屬性。
- 如果Windows名稱和UNIX名稱不一致、則必須將LDAP設定為允許Cloud Volumes Service 使用LDAP名稱對應組態（請參閱一節）"「使用LDAP進行非對稱名稱對應」"）。
- 如果未使用LDAP、則Windows SMB使用者會對應至Cloud Volumes Service 預設的本地UNIX使用者、名稱為「pcuser" in fuse」。這表示在Windows中、對應到「pcuser'」的使用者所寫入的檔案、會在多重傳輸協定NAS環境中、將UNIX擁有權顯示為「pcuser'」。這裏的「pcuser」實際上是Linux環境中的「nobnobody」使用者（UID 65534）。

在僅使用SMB的部署中、「pcuser'」對應仍會發生、但這並不重要、因為Windows使用者和群組擁有權已正確顯示、而且不允許NFS存取SMB專屬磁碟區。此外、純SMB磁碟區在建立之後、不支援轉換成NFS或雙傳輸協定磁碟區。

Windows利用Kerberos與Active Directory網域控制器進行使用者名稱驗證、這需要與Cloud Volumes Service AD DC交換使用者名稱/密碼、此區段是由實例外部的。當SMB用戶端使用「\伺服器名稱」的UNC路徑時、就會使用Kerberos驗證、下列情況為真：

- 伺服器名稱存在DNS A/Aaaa項目
- 伺服器名稱具有SMB / CIFS存取的有效SPN

建立一個支援功能的SMB Volume時、會依區段中的定義建立機器帳戶名稱Cloud Volumes Service "「Cloud Volumes Service 如何在Active Directory中顯示此功能。」" 該機器帳戶名稱也會成為SMB共用存取路徑、因為Cloud Volumes Service 它利用動態DNS（DDNS）在DNS中建立必要的A/AAAA和PTr項目、以及在機器帳戶主體上建立必要的SPN-s項目。

若要建立PTr項目、Cloud Volumes Service DNS伺服器上必須存在適用於此實例IP位址的反向對應區域。

例如Cloud Volumes Service 、此Sesvvolume使用下列的UNC共用路徑：「\cs-east- 433d.cvsdemo.local'」。

在Active Directory中、這些是Cloud Volumes Service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轉送/反轉查詢結果：

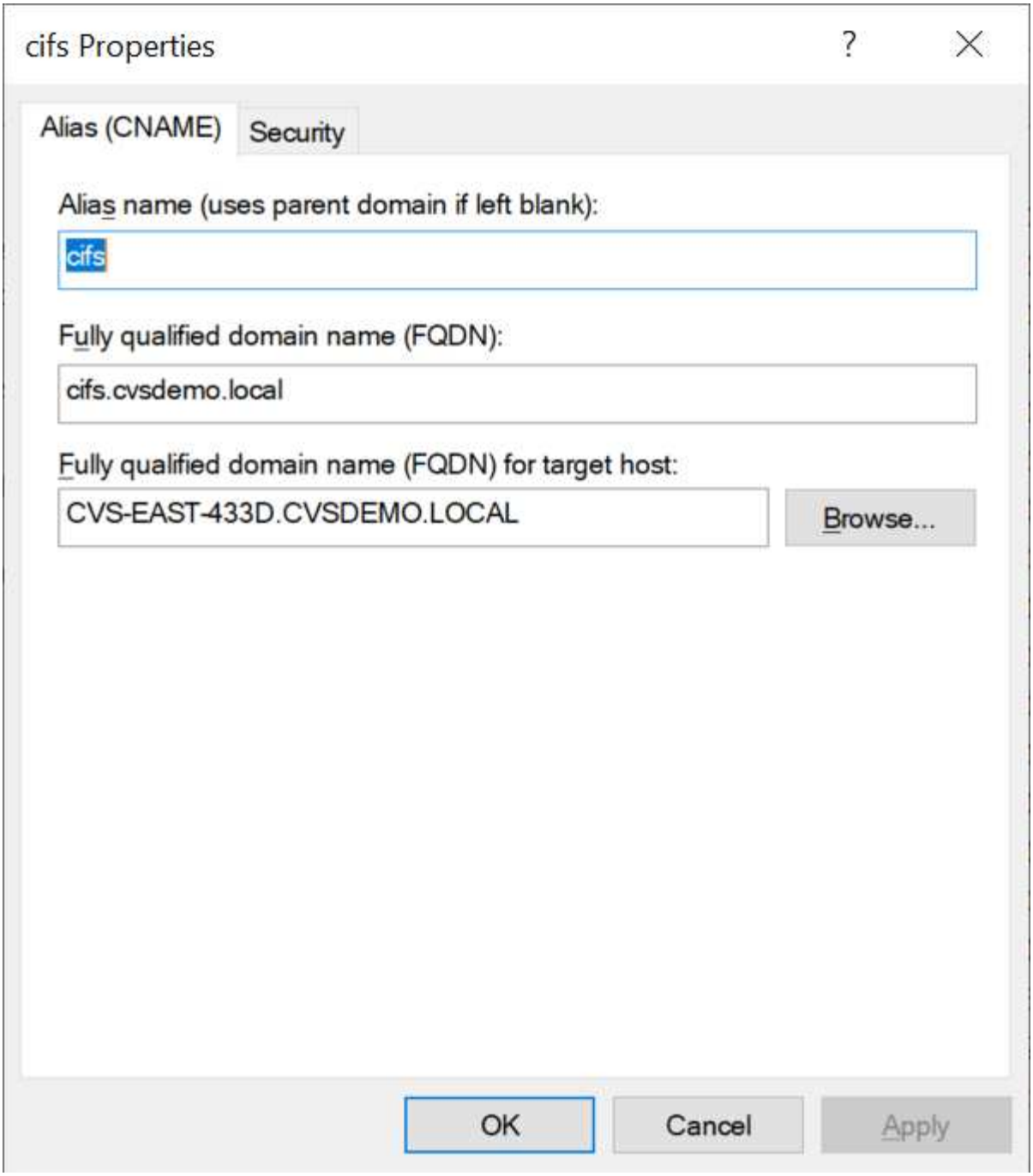
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

或者、啟用Cloud Volumes Service /要求SMB加密以利執行更多存取控制、以利執行支援。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、終端使用者可能會擔心安全問題、因為他們知道Cloud Volumes Service 使用中的機器帳戶名稱以供使用。在其他情況下、您可能只想提供更簡單的存取路徑給終端使用者。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、可以利用DNS中稱為「CNAME-」記錄的名稱。例如、如果您想要使用名稱「\CIFS」來存取共享區、而不是「\CVS東- 433d.cvsdemo.local」、但仍想要使用Kerberos驗證、DNS中的一種命名為「CNAME」、指向現有的A/AAAA記錄、以及新增至現有機器帳戶的其他SPN-s、則可提供Kerberos存取。



這是在新增CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-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、我們可以使用與CNAMA相關的SPN來查看工作階段設定要求。

```
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驗證的語言

支援下列項目Cloud Volumes Service "方言" SMB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驗證層級。啟用AES和SMB加密後、安全層級會進一步提升。

支援LM和NTLM驗證的向下相容性。Cloud Volumes Service當Kerberos設定錯誤時（例如建立SMB別名時）、共用存取會回復到較弱的驗證方法（例如：NTLMv2）。由於這些機制較不安全、因此在某些Active Directory環境中會停用這些機制。如果停用較弱的驗證方法、但未正確設定Kerberos、則共用存取會失敗、因為沒有有效的驗證方法可以還原。

如需在Active Directory中設定/檢視支援的驗證層級的相關資訊、請參閱 "網路安全性：LAN Manager驗證層級"。

權限模式

NTFS/檔案權限

NTFS權限是指套用至檔案系統中符合NTFS邏輯的檔案和資料夾。您可以在「基本」或「進階」中套用NTFS權限、並可設定為「允許」或「允許」以進行存取控制。

基本權限包括：

- 完全控制
- 修改
- 讀取與執行
- 讀取
- 寫入

當您設定使用者或群組的權限（稱為ACE）時、該使用者或群組會駐留在ACL中。NTFS權限使用與UNIX模式位元相同的讀取/寫入/執行基礎、但也可延伸至更精細且延伸的存取控制（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模式位元提供的精細度與NTFS權限不同（例如、能夠設定ACL中個別使用者和群組物件的權限、或是設定延伸屬性）。不過NFSv4.1 ACL確實提供與NTFS ACL相同的功能。

NTFS權限比共用權限更為特定、可搭配共用權限使用。使用NTFS權限結構時、會套用最嚴格的限制。因此、在定義存取權限時、明確拒絕使用者或群組甚至會覆寫「完全控制」。

NTFS權限由Windows SMB用戶端控制。

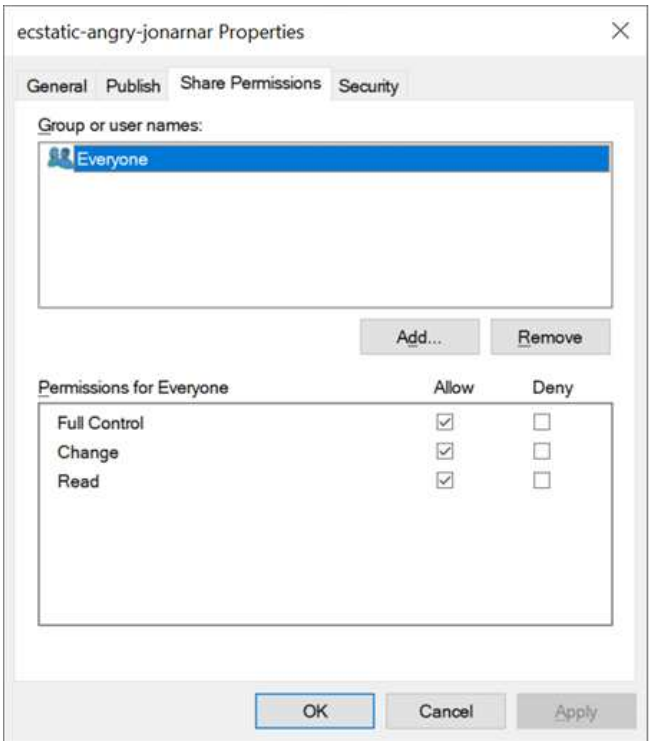
共用權限

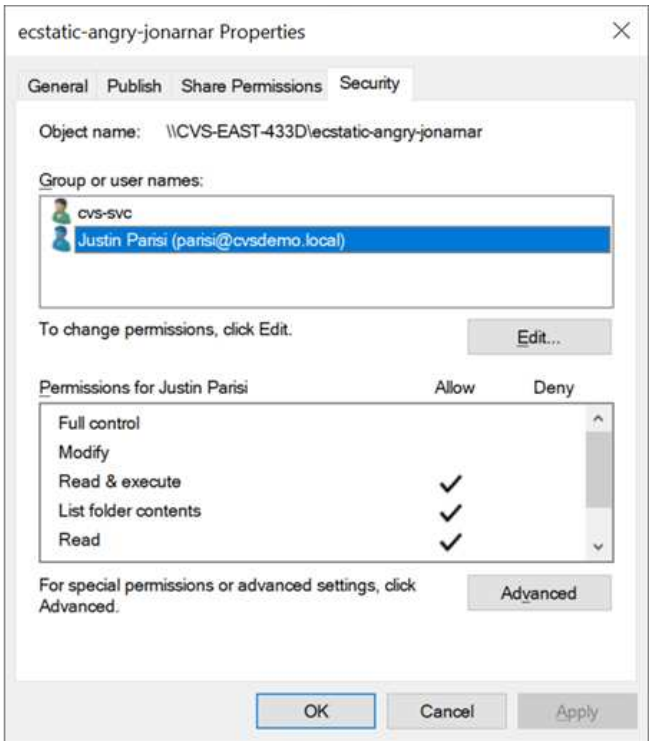
共用權限比NTFS權限更為一般（唯讀/變更/完全控制）、並控制SMB共用的初始項目、類似於NFS匯出原則規則的運作方式。

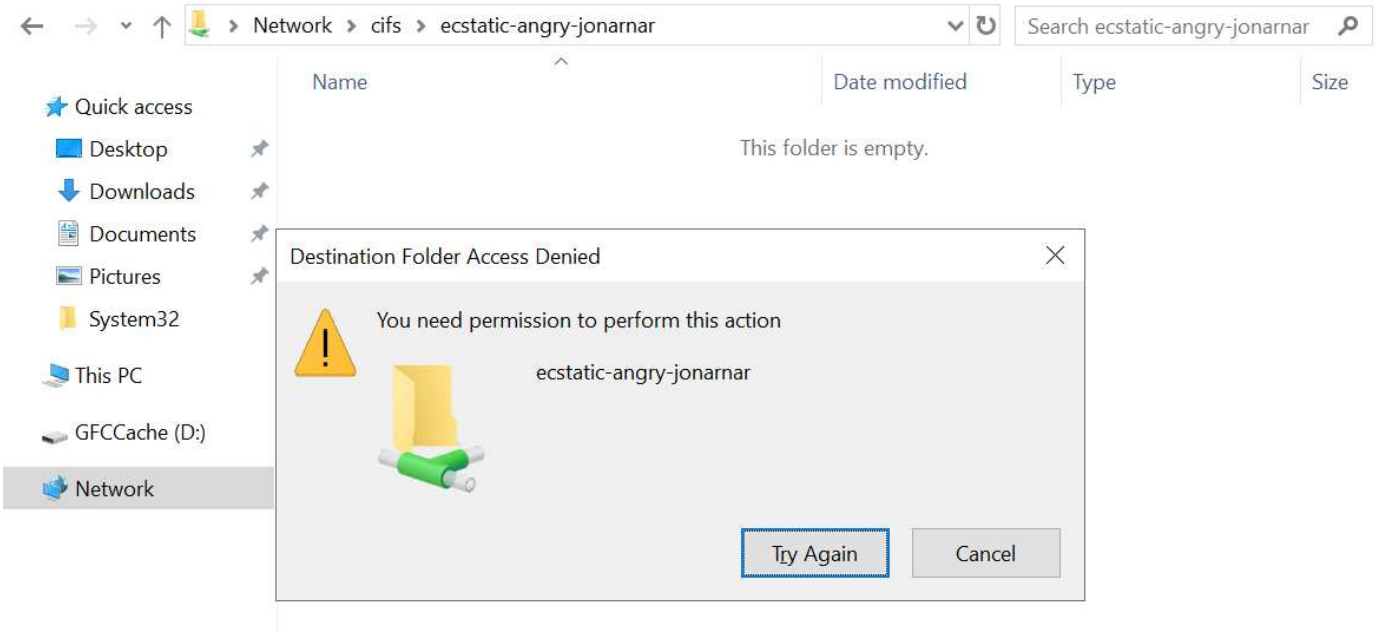
雖然NFS匯出原則規則可透過主機型資訊（例如IP位址或主機名稱）來控制存取、但SMB共用權限可以使用共用ACL中的使用者和群組ACE來控制存取。您可以從Windows用戶端或Cloud Volumes Service 從功能區管理UI設定共用ACL。

根據預設、共用ACL和初始Volume ACL包括「完全控制的每個人」。檔案ACL應該變更、但共用權限會被共用區中物件的檔案權限所取代。

例如、如果使用者只能讀取Cloud Volumes Service 對此實體磁碟區檔案ACL的存取權、則即使共用ACL設定為「擁有完全控制權的所有人」、仍無法存取建立檔案和資料夾、如下圖所示。







若要獲得最佳的安全性結果、請執行下列步驟：

- 從共用和檔案ACL中移除「所有人」、改為設定使用者或群組的共用存取權。
- 使用群組進行存取控制、而非個別使用者、以利管理、並更快移除/新增使用者、透過群組管理來共用ACL。
- 允許對共用權限上的ACE進行較少限制、較為一般的共用存取、並鎖定具有檔案權限的使用者和群組存取、以達到更精細的存取控制。
- 避免一般使用明確拒絕ACL、因為它們會覆寫允許ACL。限制使用者或群組的明確拒絕ACL、以防止他們快速存取檔案系統。
- 請務必注意 "ACL繼承" 修改權限時的設定；在目錄或磁碟區的最上層設定具有高檔案計數的繼承旗標、表示該目錄或磁碟區下方的每個檔案都已新增繼承權限、 這可能會在調整每個檔案時產生不必要的行為、例如非

預期的存取/拒絕、以及冗長的權限修改。

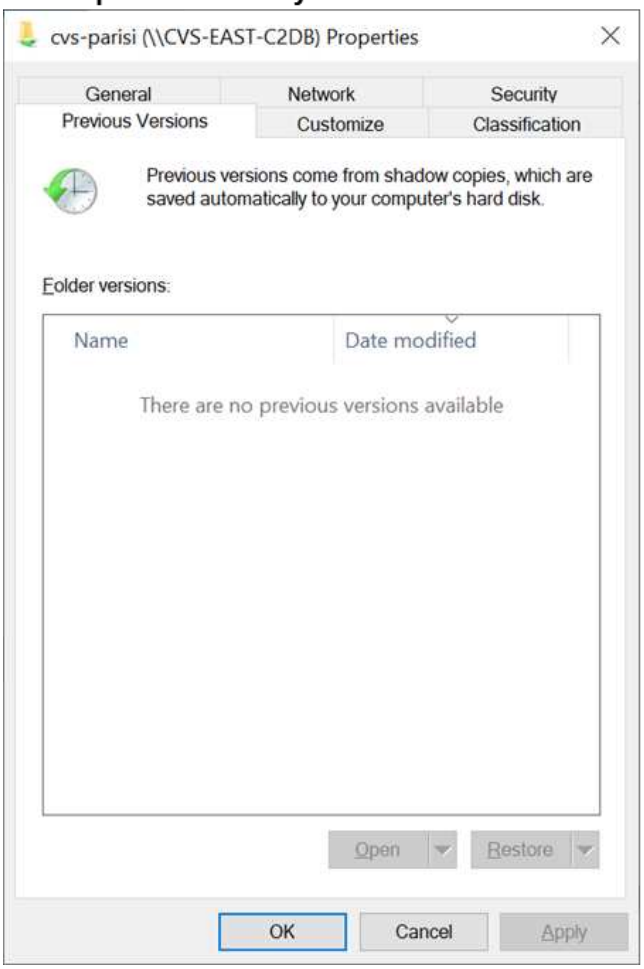
SMB共享安全功能

當您第一次在Cloud Volumes Service 支援SMB存取的情況下建立Volume時、系統會提供一系列的選項來保護該Volume。

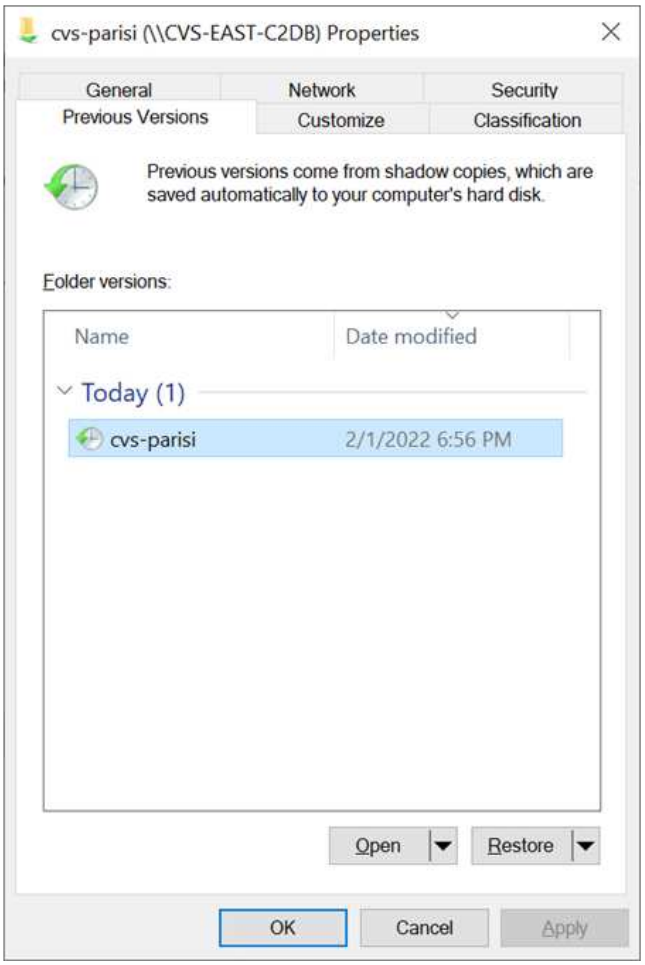
這些選項中的部分取決於Cloud Volumes Service 「樣層」（「效能」或「軟體」）、選項包括：

- *使Snapshot目錄可見（同時適用於CVs-Performance和CVs-SW）。*此選項控制SMB用戶端是否可以存取SMB共用區（「\伺服器\共用~snapshot」和/或「舊版」索引標籤）中的Snapshot目錄。未核取預設設定、這表示磁碟區預設為隱藏及不允許存取「~snapshot」目錄、而且磁碟區的「舊版」索引標籤不會顯示Snapshot複本。

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



基於安全理由、效能理由（將這些資料夾隱藏在AV掃描之外）或偏好、可能需要從終端使用者處隱藏Snapshot複本。由於「支援快照」是唯讀的、因此即使這些快照可見、終端使用者仍無法刪除或修改Snapshot目錄中的檔案。Cloud Volumes Service應用Snapshot複本時、檔案或資料夾的檔案權限。如果檔案或資料夾的權限在Snapshot複本之間變更、則變更也會套用至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檔案或資料夾。雖然無法刪除或修改Snapshot目錄中的檔案、但仍可將檔案或資料夾從Snapshot目錄中複製出來。

- 啟用**SMB**加密（同時適用於**CVs-Performance**和**CVs-SW**）。 SMB加密預設為停用（未核取）。核取此方塊可啟用SMB加密、這表示SMB用戶端與伺服器之間的流量會在傳輸中加密、並以議定的最高支援加密層級進行加密。支援高達AES-256的SMB加密。Cloud Volumes Service啟用SMB加密確實會造成效能損失、而

您的SMB用戶端可能會或可能不會察覺到這種情況、範圍大致介於10-20%之間。NetApp強烈建議測試、以瞭解效能損失是否可接受。

- *隱藏SMB共用區（同時適用於CVS效能和CVS軟體）。*設定此選項會隱藏SMB共用路徑、使其無法正常瀏覽。這表示不知道共用路徑的用戶端在存取預設的UNC路徑（例如：「\CVS SMB」）時、無法看到共用區。核取此核取方塊時、只有明確知道SMB共用路徑或由群組原則物件定義共用路徑的用戶端才能存取該路徑（透過混淆來確保安全）。
- *啟用存取型列舉（ABE）（僅限CVs-SW）。*這類似於隱藏SMB共用區、但共用區或檔案只會隱藏在沒有存取物件權限的使用者或群組中。例如、如果不允許Windows使用者「Joe」透過權限至少讀取存取權、則Windows使用者「Joe」根本看不到SMB共用區或檔案。此功能預設為停用、您可以選取核取方塊來啟用此功能。如需ABE的詳細資訊、請參閱NetApp知識庫文章 "存取型列舉（ABE）如何運作？"
- 啟用持續可用的（**CA**）共用支援（僅限**CVS**效能）。 "持續可用的SMB共用" 透過在Cloud Volumes Service整個節點之間複寫鎖定狀態、將容錯移轉事件期間的應用程式中斷降至最低。這不是一項安全功能、但確實能提供更好的整體恢復能力。目前、此功能僅支援SQL Server和FSLogix應用程式。

預設隱藏共用

當SMB伺服器是以Cloud Volumes Service 支援功能建立時、就會出現這種情況 "隱藏的管理共用" （使用$命名慣例）、這是在資料Volume SMB共用區之外建立的。其中包括C$（命名空間存取）和IPC$（共用具名管道、用於程式之間的通訊、例如用於Microsoft管理主控台（MMC）存取的遠端程序呼叫（RPC））。

IPC$共用區不含共用ACL、無法修改、嚴格用於RPC呼叫和 "Windows預設不允許匿名存取這些共用"。

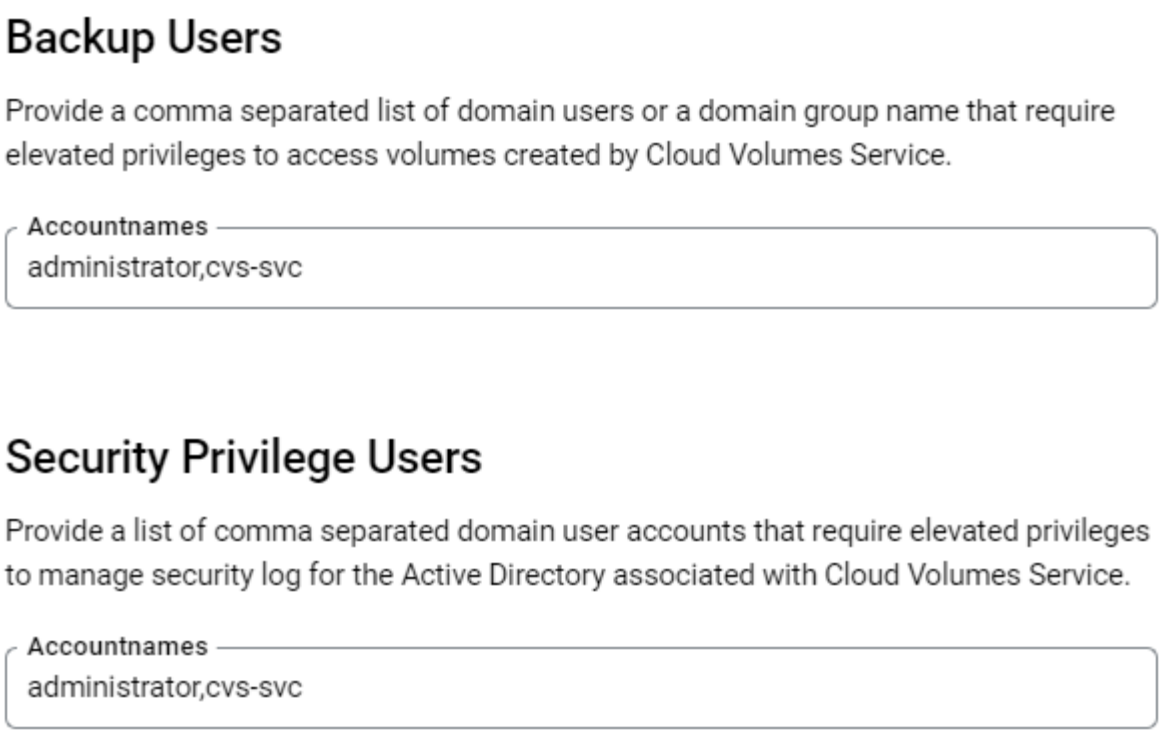
依預設、C$共用可讓BUILTIN/系統管理員存取、但Cloud Volumes Service 由於能夠存取C$共用區、因此無法檢視Cloud Volumes Service 所有安裝於此的磁碟區、因此無法存取共享ACL。因此、嘗試瀏覽至「\SERVER\C$」失敗。

具有本機/**BUILTIN**/系統管理員/備份權限的帳戶

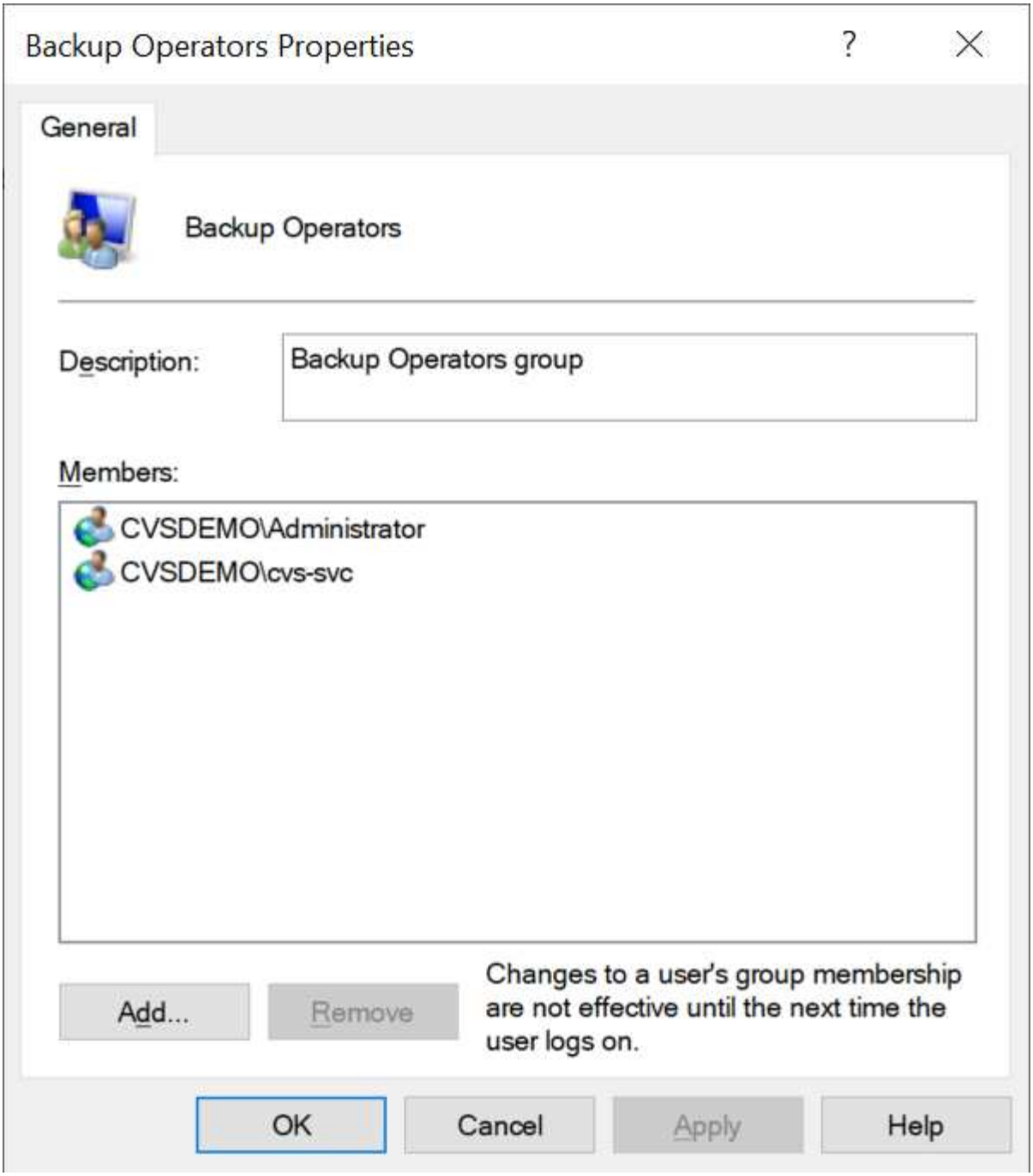
由於本機群組（例如BUILTIN\Administrator）會套用存取權限給選取的網域使用者和群組、因此、支援SMB伺服器的功能與一般Windows SMB伺服器類似。Cloud Volumes Service

當您指定要新增至備份使用者的使用者時、該使用者會新增至Cloud Volumes Service 使用該Active Directory連線的執行個體中BUILTIN\Backup Operators群組、然後取得 "SeBackup權限和Se恢復 權限"。

當您將使用者新增至「安全性權限使用者」時、系統會將SeSecurityPrivilege賦予使用者、這在某些應用程式使用案例（例如）中很有用 "SMB共用上的SQL Server"。



您可以Cloud Volumes Service 透過具有適當權限的MMC檢視本地的群組成員資格。下圖顯示使用Cloud Volumes Service 者已透過使用此功能新增的使用者。

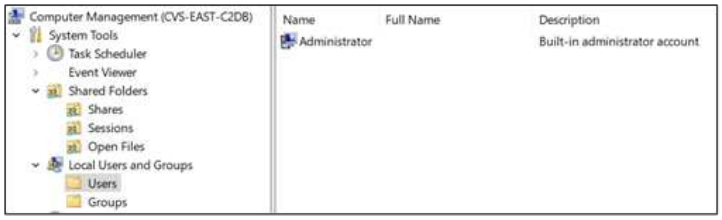


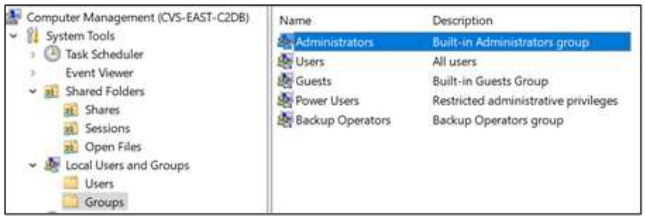
下表顯示預設BUILTIN群組清單、以及預設新增的使用者/群組。

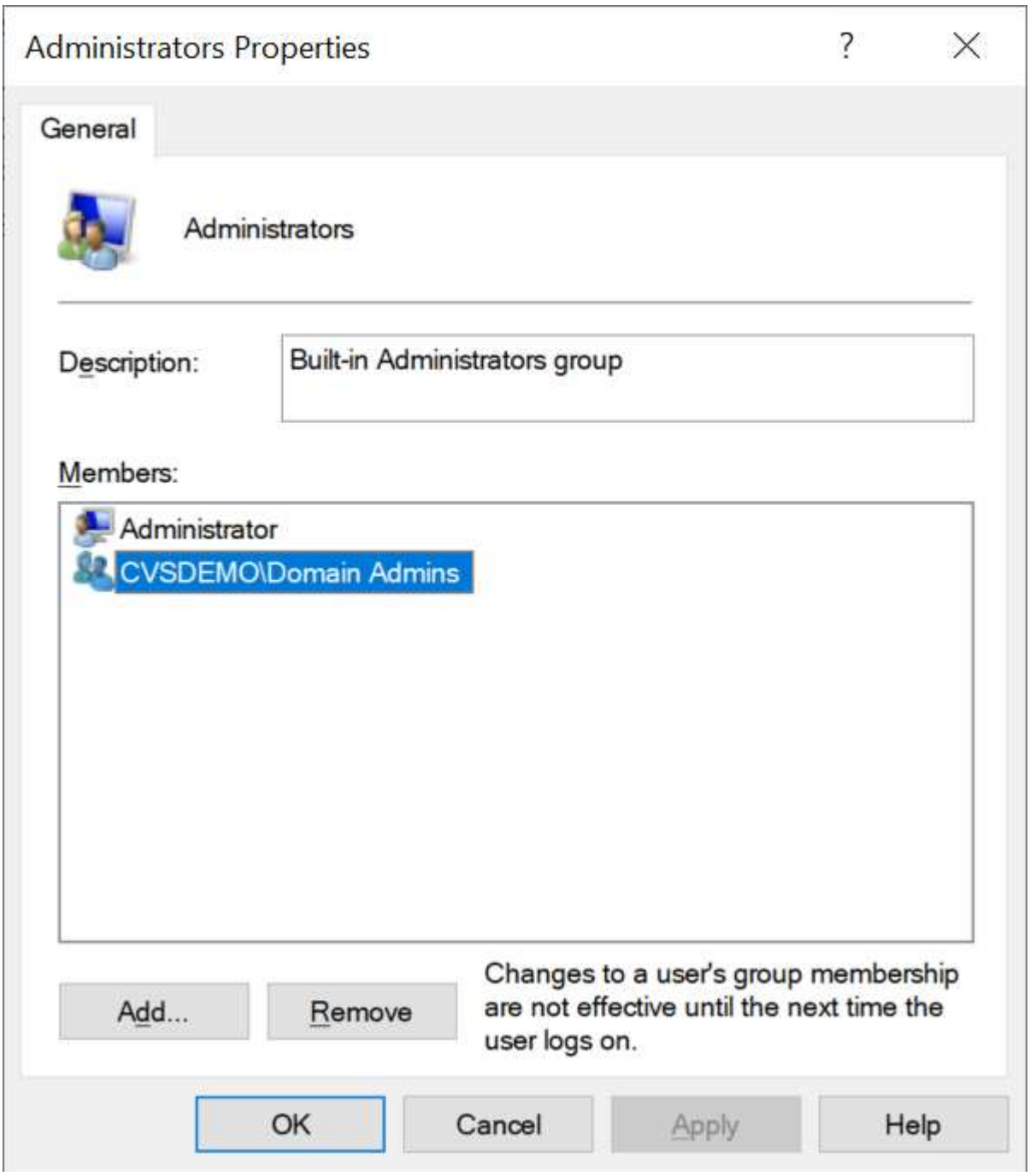
本機/**BUILTIN.**群組	預設成員
內建\系統管理員*	網域\網域管理員
內建\備份操作員*	無
內建\訪客	網域\網域來賓
內建\超級使用者	無
內建\網域使用者	網域\網域使用者

*群組成員資格是由Cloud Volumes Service 不實Active Directory連線組態所控制。

您可以在MMC視窗中檢視本機使用者和群組（及群組成員）、但無法從這個主控台新增或刪除物件或變更群組成員資格。根據預設、Cloud Volumes Service 只有Domain Admins群組和Administrator會新增至功能區的BUILTIN\Administrator群組。目前您無法修改此項目。







MMC/電腦管理存取

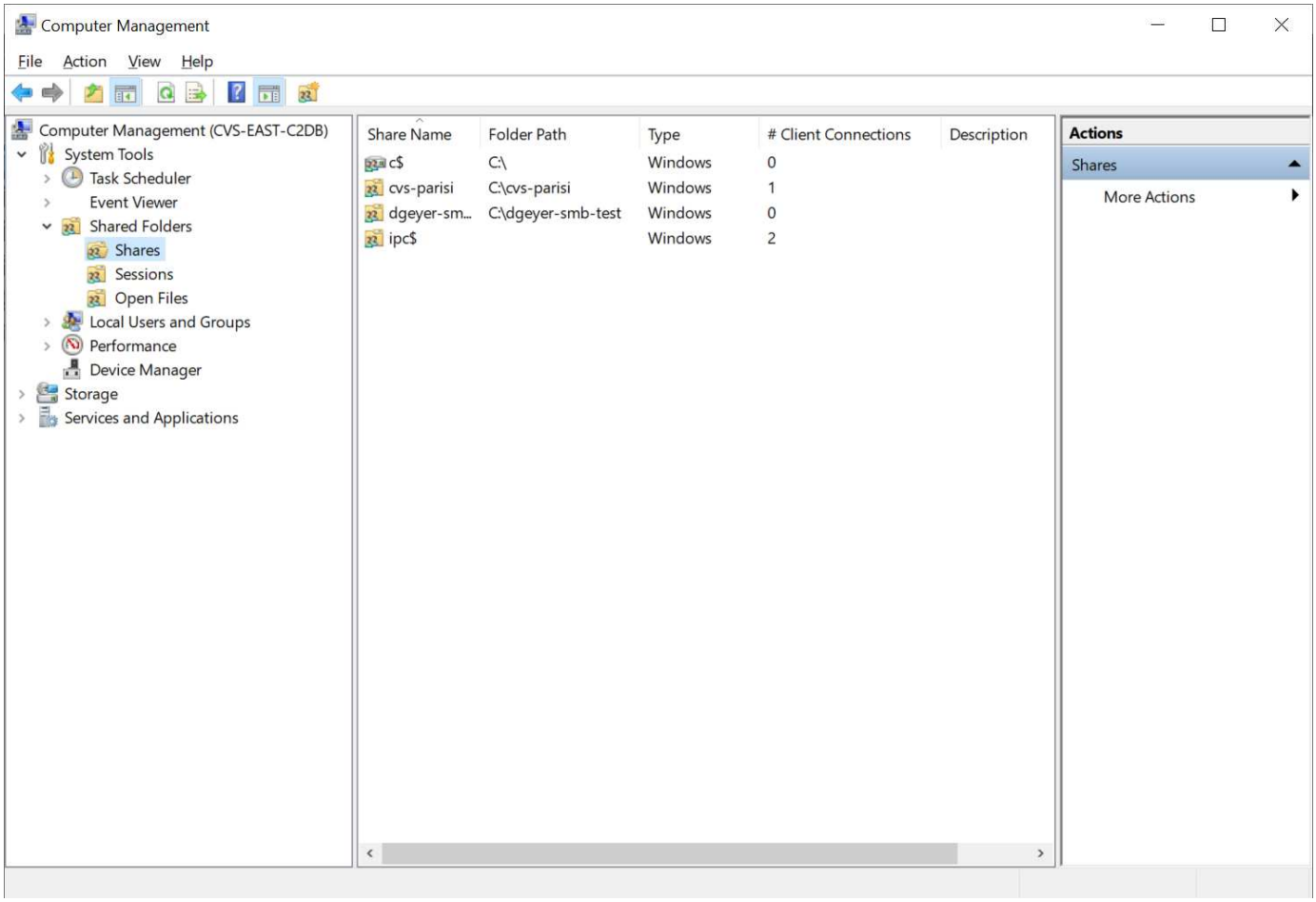
SMB存取Cloud Volumes Service 功能可連線至電腦管理MMC、讓您檢視共用區、管理共用ACL、以及檢視/管理SMB工作階段和開啟檔案。

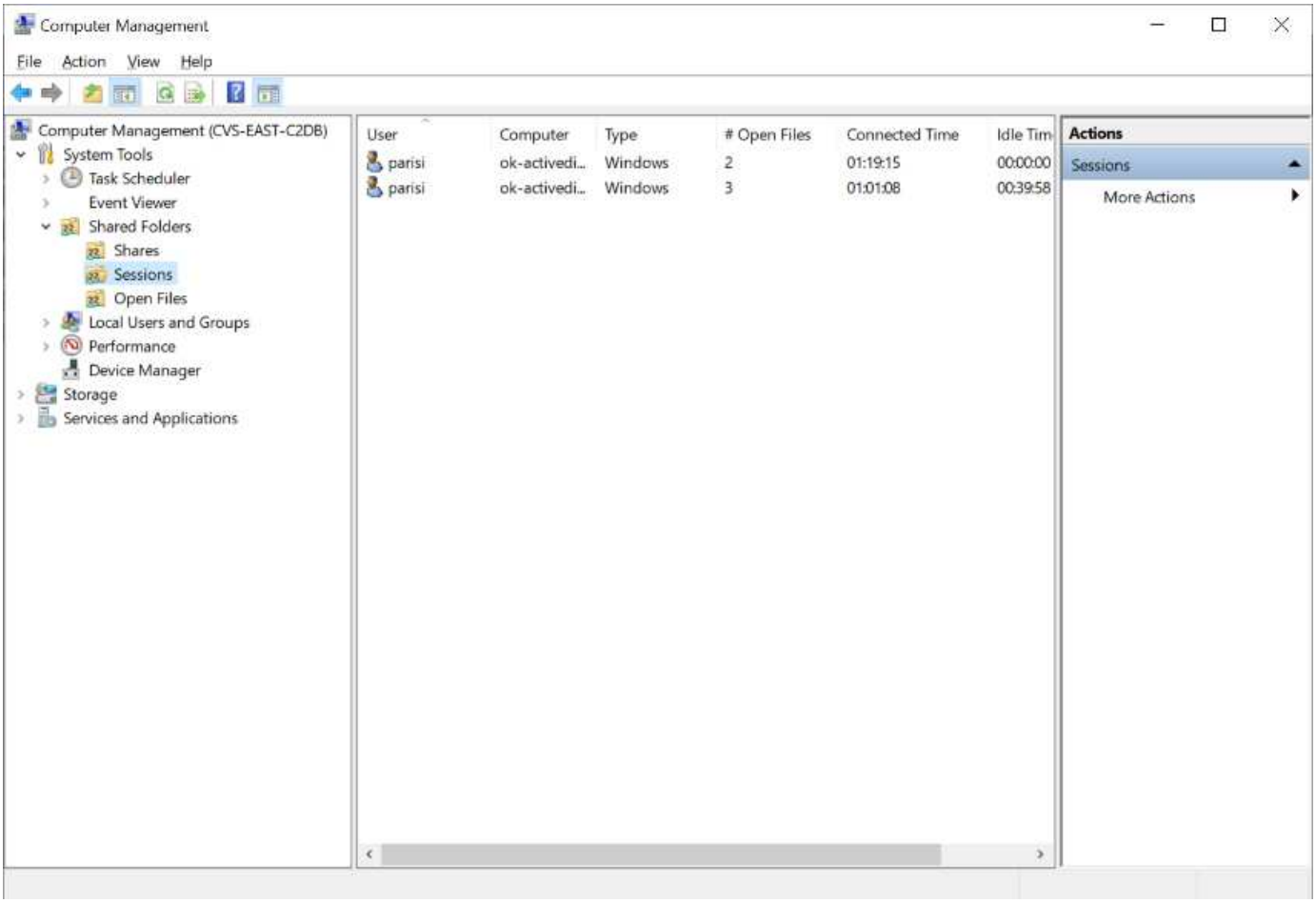
若要使用MMC來檢視Cloud Volumes Service SMB共用區和Sessions、目前登入的使用者必須是網域管理員。其他使用者可以從MMC檢視或管理SMB伺服器、並在嘗試檢視Cloud Volumes Service 有關Sisb執行個體的共用或工作階段時、收到「您沒有權限」對話方塊。

若要連線至SMB伺服器、請開啟「電腦管理」、在「電腦管理」上按一下滑鼠右鍵、然後選取「連線至其他電腦」。這會開啟「Select Computer（選取電腦）」對話方塊、您可以在其中輸入SMB伺服器名稱（可在Cloud Volumes Service 《支援資料》資料冊中找到）。

當您檢視具有適當權限的SMB共用時、Cloud Volumes Service 您會看到共享Active Directory連線的所有可用共享區。若要控制這種行為、請在Cloud Volumes Service 現象區執行個體上設定隱藏SMB共用選項。

請記住、每個地區只允許一個Active Directory連線。





下表顯示MMC支援/不支援的功能清單。

支援的功能	不支援的功能
• 檢視共享區 • 檢視作用中的SMB工作階段 • 檢視開啟的檔案 • 檢視本機使用者和群組 • 檢視本機群組成員資格 • 列舉系統中的工作階段、檔案和樹狀結構連線清單 • 關閉系統中開啟的檔案 • 關閉開啟的工作階段 • 建立/管理共用	• 建立新的本機使用者/群組 • 管理/檢視現有的本機使用者/群組 • 檢視事件或效能記錄 • 管理儲存設備 • 管理服務與應用程式

SMB伺服器安全性資訊

本產品的SMB伺服器Cloud Volumes Service 使用一系列選項來定義SMB連線的安全性原則、包括Kerberos時鐘偏移、票證存留期、加密等。

下表列出這些選項、其功能、預設組態、以及是否可以使用Cloud Volumes Service 更新。部分選項不適用

於Cloud Volumes Service 此功能。

安全選項	它的作用	預設值	可以改變嗎？
Kerberos時鐘最大偏差（分鐘）	最大Cloud Volumes Service 程度地縮短了在各個領域控制器之間的時間偏差。如果時間偏移超過5分鐘、Kerberos驗證就會失敗。這會設為Active Directory預設值。	5.	否
Kerberos票證壽命（小時）	Kerberos票證在要求續約之前保持有效的最長時間。如果在10小時之前沒有續約、您必須取得新的通知單。系統會自動執行這些續約作業。Cloud Volumes Service10小時為Active Directory預設值。	10.	否
Kerberos票證續約上限（天）	在需要新授權要求之前、可以續約Kerberos票證的最大天數。自動更新SMB連線的問題單。Cloud Volumes ServiceActive Directory預設值為七天。	7.	否
Kerberos Kdc連線逾時（秒）	Kdc連線逾時前的秒數。	3.	否
需要簽署傳入的SMB流量	設定為需要SMB流量的簽署。如果設為true、則不支援簽署的用戶端會失敗連線。	錯	
本機使用者帳戶需要密碼複雜度	用於本機SMB使用者的密碼。由於不支援建立本機使用者、因此此選項不適用於支援。Cloud Volumes Service Cloud Volumes Service	是的	否
Active Directory LDAP連線使用start_tls	用於啟用Active Directory LDAP的啟動TLS連線。目前不支援啟用此功能。Cloud Volumes Service	錯	否
為啟用Kerberos的AES-128和AES-256加密	這會控制AES加密是否用於Active Directory連線、並在建立/修改Active Directory連線時、使用「啟用Active Directory驗證的AES加密」選項加以控制。	錯	是的

安全選項	它的作用	預設值	可以改變嗎？
LM相容層級	Active Directory連線所支援的驗證語言層級。請參閱「」一節SMB驗證的語言」以取得更多資訊。	vLMvb-krb	否
傳入CIFS流量需要SMB加密	所有共用都需要SMB加密。這不是Cloud Volumes Service 由靜止使用；而是根據每個磁碟區設定加密（請參閱「」一節）SMB共享安全功能」）。	錯	否
用戶端工作階段安全性	設定LDAP通訊的簽署和/或密封。目前未在Cloud Volumes Service 不必要的情況下設定、但未來版本可能需要此功能來解決此問題。因Windows修補程式而導致的LDAP驗證問題補救措施將在一節中說明"「LDAP通道繫結。」"。	無	否
SMB2可啟用DC連線	使用SMB2進行DC連線。預設為啟用。	系統預設值	否
LDAP轉介追蹤	使用多個LDAP伺服器時、如果第一個伺服器中找不到項目、參照追蹤功能可讓用戶端參照清單中的其他LDAP伺服器。目前不支援此功能Cloud Volumes Service 。	錯	否
使用LDAPS進行安全的Active Directory連線	啟用LDAP over SSL。目前不受Cloud Volumes Service 支援。	錯	否
DC連線需要加密	需要加密才能成功建立DC連線。在功能不完整的情況下、預設為停用Cloud Volumes Service 。	錯	否

雙傳輸協定/多傳輸協定

支援將相同的資料集共享給SMB和NFS用戶端、同時維持適當的存取權限Cloud Volumes Service ("雙傳輸協定")。這是透過協調不同傳輸協定之間的身分識別對應、以及使用集中式後端LDAP伺服器、將UNIX身分識別提供Cloud Volumes Service 給支援中心來完成。您可以使用Windows Active Directory為Windows和UNIX使用者提供方便使用的功能。

存取控制

- *共享存取控制。*決定哪些用戶端和（或）使用者和群組可以存取NAS共用區。對於NFS、匯出原則和規則會控制用戶端對匯出的存取。NFS匯出是從Cloud Volumes Service 整個過程中管理。SMB使用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。您只能使用從SMB用戶端設定共用層級ACL "MMC/電腦管理" 擁有Cloud Volumes Service 管理員權限的帳戶（請參閱一節） "「擁有本機/BUILTIN/系統管理員/備份權限的帳戶。」"）。

- *檔案存取控制。*控制檔案或資料夾層級的權限、且永遠從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用戶端運用NTFS權限。

將資料提供給NFS和SMB的磁碟區存取控制權取決於使用中的傳輸協定。如需雙協定權限的相關資訊、請參閱「」一節[權限模式]。」

使用者對應

當用戶端存取Volume時Cloud Volumes Service 、嘗試將傳入的使用者對應至相反方向的有效使用者。這是確定跨傳輸協定適當存取的必要條件、並確保要求存取的使用者確實是他們聲稱的對象。

例如、如果名為「Joe」的Windows使用者嘗試透過SMB存取具有UNIX權限的Volume、Cloud Volumes Service則會執行搜尋、尋找名為「Joe」的對應UNIX使用者。如果存在、則以Windows使用者「Joe」的身分寫入SMB共用區的檔案會顯示為來自NFS用戶端的UNIX使用者「Joe」。

或者、如果名為「Joe」的UNIX使用者嘗試以Cloud Volumes Service Windows權限存取某個Windows Volume、則UNIX使用者必須能夠對應至有效的Windows使用者。否則、將拒絕存取磁碟區。

目前、只有Active Directory支援使用LDAP進行外部UNIX身分識別管理。如需設定此服務存取權的詳細資訊、請參閱 "建立AD連線"。

權限模式

使用雙傳輸協定設定時Cloud Volumes Service 、利用磁碟區的安全樣式來判斷ACL的類型。這些安全型態是根據所指定的NAS傳輸協定來設定、或是在建立Cloud Volumes Service 完實體磁碟區時選擇使用雙傳輸協定。

- 如果您只使用NFS、Cloud Volumes Service 則Sfelles Volume會使用UNIX權限。
- 如果您只使用SMB、Cloud Volumes Service 則支援使用NTFS權限的功能。

如果要建立雙傳輸協定磁碟區、您可以在建立磁碟區時選擇ACL樣式。這項決定應以所需的權限管理為基礎。如果使用者管理來自Windows / SMB用戶端的權限、請選取NTFS。如果您的使用者偏好使用NFS用戶端和chmod/chown、請使用UNIX安全性樣式。

建立**Active Directory**連線的考量事項

支援將您的實例連接至外部Active Directory伺服器、以便同時為SMB和UNIX使用者進行身分識別管理。Cloud Volumes Service Cloud Volumes Service建立Active Directory連線是Cloud Volumes Service 在支援功能方面使用SMB的必要條件。

此設定提供多種選項、需要考量安全性。外部Active Directory伺服器可以是內部部署執行個體或原生雲端。如果您使用的是內部部署的Active Directory伺服器，請勿將網域暴露給外部網路（例如使用DMZ或外部IP位址）。而是使用安全的私有通道或VPN、單向樹系信任或內部部署網路專用的網路連線 "私有 Google 存取"。如需詳細資訊、請參閱Google Cloud文件 "在Google Cloud中使用Active Directory的最佳實務做法"。

CVS軟體要求Active Directory伺服器位於同一個地區。如果嘗試在CVs-SW中連線至其他地區、嘗試就會失敗。使用CVs-SW時、請務必建立包含Active Directory DC的Active Directory網站、然後在Cloud Volumes Service 其中指定站台、以避免跨區域DC連線嘗試。

Active Directory認證

啟用SMB或LDAP for NFS時Cloud Volumes Service 、支援使用者可與Active Directory控制器互動、以建立機器帳戶物件來進行驗證。這與Windows SMB用戶端加入網域的方式並不不同、而且需要對Active Directory中的組織單位（OU）擁有相同的存取權限。

在許多情況下、安全性群組不允許在Cloud Volumes Service 外部伺服器上使用Windows系統管理員帳戶、例如在某些情況下、Windows系統管理員使用者會完全停用、這是安全性最佳實務做法。

建立SMB機器帳戶所需的權限

若要新增Cloud Volumes Service 物件至Active Directory、則該帳戶具有網域的管理權限或擁有 "委派權限以建立及修改機器帳戶物件" 需要指定的OU。您可以透過Active Directory中的委派控制精靈來執行此作業、方法是建立自訂工作、讓使用者以提供下列存取權限來存取電腦物件的建立/刪除：

- 讀取/寫入
- 建立/刪除所有子物件
- 讀取/寫入所有內容
- 變更/重設密碼

這樣做會自動將已定義使用者的安全ACL新增至Active Directory中的OU、並將Active Directory環境的存取權限減至最低。在委派使用者之後、此視窗中的使用者名稱和密碼可提供為Active Directory認證。

> ⓘ 傳遞至Active Directory網域的使用者名稱和密碼會在機器帳戶物件查詢和建立期間、運用Kerberos加密技術來提高安全性。

Active Directory連線詳細資料

。 "Active Directory連線詳細資料" 提供欄位給系統管理員、以提供機器帳戶放置的特定Active Directory架構資訊、例如：

- * Active Directory連線類型。*用於指定區域中的Active Directory連線是用於Cloud Volumes Service 供應各種類型的SView或CVS效能服務的磁碟區。如果現有連線的設定不正確、使用或編輯時可能無法正常運作。
- 網域。 Active Directory網域名稱。
- *站台。*將Active Directory伺服器限制為特定站台、以確保安全性和效能 "考量"。當多個Active Directory伺服器橫跨多個區域時、這是必要的、因為Cloud Volumes Service 目前不支援將Active Directory驗證要求允許在Cloud Volumes Service 不同於此執行個體的區域內執行Active Directory伺服器。（例如、Active Directory網域控制器所在的區域僅支援CVs-Performance、但您想要在CVs-SW執行個體中使用SMB共用區）。
- * DNS伺服器。* DNS伺服器、用於名稱查詢。
- * NetBios名稱（選用）。*如果需要、則為伺服器的NetBios名稱。這是使用Active Directory連線建立新機器帳戶時所使用的功能。例如、如果將NetBios名稱設為CVs-East、則機器帳戶名稱將為CVs-East-{12334}。請參閱一節 "如何在Active Directory中顯示此功能Cloud Volumes Service" 以取得更多資訊。
- *組織單位（OU）。*建立電腦帳戶的特定OU。如果您要將機器帳戶的控制權委派給使用者至特定OU、這很有用。
- * AES Encryption。*您也可以勾選或取消勾選「啟用AD驗證的AES加密」核取方塊。啟用AES加密以進行Active Directory驗證、可在Cloud Volumes Service 使用者和群組查詢期間、提供額外的安全性、以利執行功能以進行通訊。啟用此選項之前、請先洽詢您的網域管理員、確認Active Directory網域控制器支援AES

驗證。

根據預設、大部分的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Cloud Volumes Service 已設定「更新Active Directory」連線以啟用AES。否則會發生驗證失敗。啟用AES加密並不會停用較弱的密碼、而是將AES密碼的支援新增至Cloud Volumes Service 該SMB機器帳戶。

Kerberos領域詳細資料

此選項不適用於SMB伺服器。而是在設定NFS Kerberos for Cloud Volumes Service the Sing系統時使用。填入這些詳細資料時、NFS Kerberos領域會設定（類似於Linux上的krb5..conf檔案）、並在Cloud Volumes Service 建立實體磁碟區時指定NFS Kerberos時使用、因為Active Directory連線會做為NFS Kerberos發佈中心（kdc ）。

非Windows KDC目前不支援Cloud Volumes Service 搭配使用。

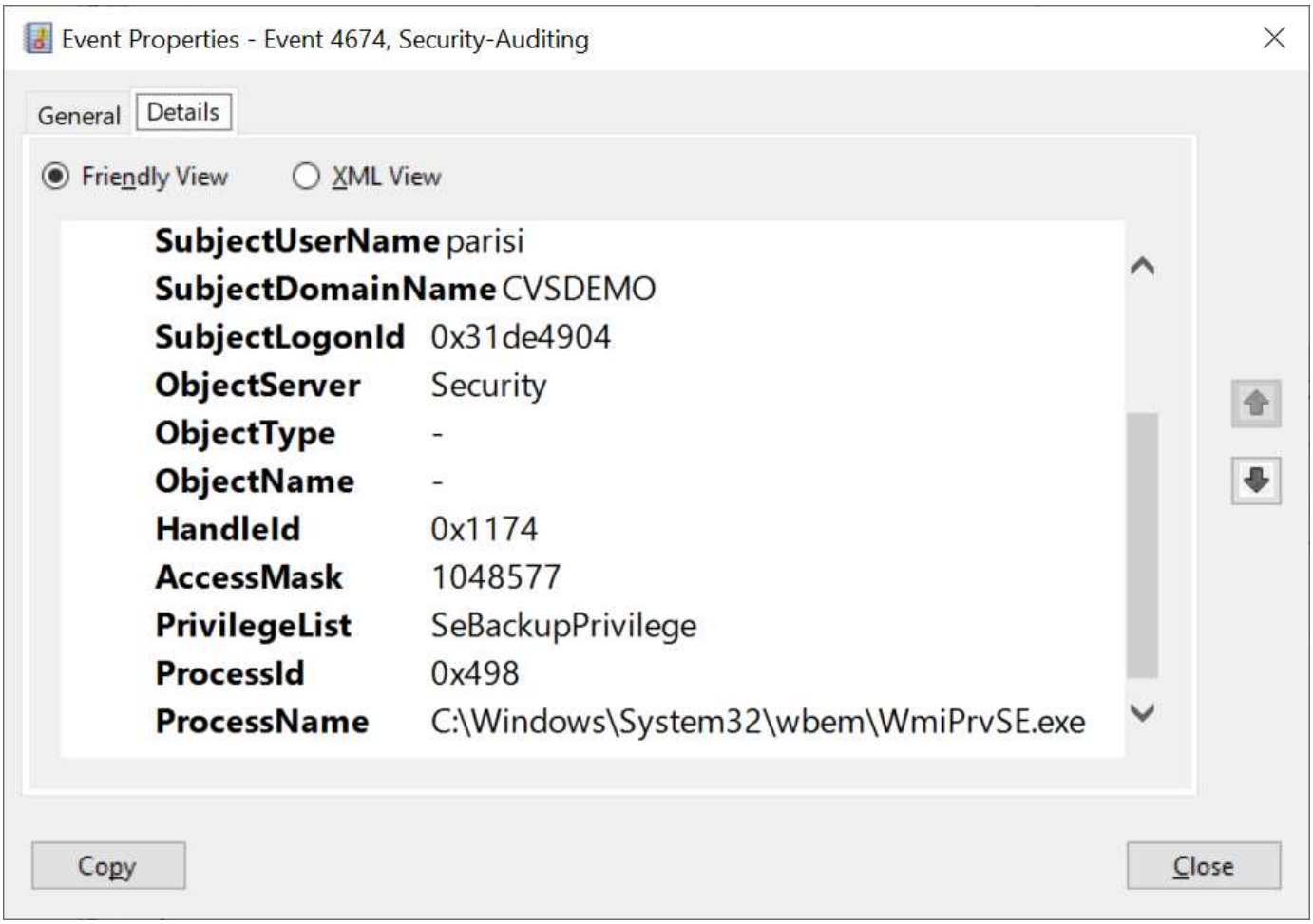
區域

區域可讓您指定Active Directory連線所在的位置。此區域必須與Cloud Volumes Service 《非洲地理區：

- *本機NFS使用者搭配LDAP.*本節中、也有允許本機NFS使用者搭配LDAP的選項。如果您想要將UNIX使用者群組成員資格支援延伸到NFS（延伸群組）的16群組限制之外、則必須取消選取此選項。不過、使用延伸群組時、需要設定用於UNIX身分識別的LDAP伺服器。如果您沒有LDAP伺服器、請取消選取此選項。如果您有LDAP伺服器、而且想要使用本機UNIX使用者（例如root）、請選取此選項。

備份使用者

此選項可讓您指定對Cloud Volumes Service 該Windows Volume具有備份權限的Windows使用者。某些應用程式必須具備備份權限（SeBackup權限）、才能在NAS磁碟區中正確備份及還原資料。此使用者擁有大量的磁碟區資料存取權限、因此您應該考慮 "啟用該使用者存取的稽核"。啟用後、稽核事件會顯示在「事件檢視器」>「Windows記錄」>「安全性」中。



安全性權限使用者

此選項可讓您指定Windows使用者、這些使用者具有Cloud Volumes Service 對此功能進行安全性修改的權限。某些應用程式需要安全性權限（SeSecurityPrivilege）（"例如SQL Server"）在安裝期間正確設定權限。管理安全性記錄時需要此權限。雖然此權限不如SeBackup權限強大、但NetApp建議您使用 "稽核使用者存取權限" 如果需要、請使用此權限層級。

如需詳細資訊、請參閱 "指派給新登入的特殊權限"。

如何在**Active Directory**中顯示此功能**Cloud Volumes Service**

在Active Directory中顯示為一般機器帳戶物件。Cloud Volumes Service命名慣例如下。

- CIFS/SMB和NFS Kerberos會建立個別的機器帳戶物件。
- 啟用LDAP的NFS會在Active Directory中建立機器帳戶、以進行Kerberos LDAP繫結。
- 具有LDAP的雙傳輸協定磁碟區會共用CIFS/SMB機器帳戶、以供LDAP和SMB使用。
- CIFS/SMB機器帳戶的機器帳戶命名慣例為：名稱-1234（隨機四位數ID、加上連字號、加上<10個字元名稱）。您可以使用Active Directory連線上的[NetBios名稱]設定來定義名稱（請參閱「」一節）Active Directory連線詳細資料」）。
- NFS Kerberos使用NFS-name-1234作為 命名慣例（最多15個字元）。如果使用超過15個字元、則名稱為nfs -截短名稱-1234.
- 僅NFS的CVS效能執行個體若啟用LDAP、則會建立SMB機器帳戶、以與CIFS/SMB執行個體相同的命名慣

例來繫結至LDAP伺服器。

- 建立SMB機器帳戶時、預設的隱藏管理共用區（請參閱一節"「預設隱藏共用」"）也會建立（c$、admin$、ipc$）、但這些共用區並未指派ACL、因此無法存取。
- 依預設、機器帳戶物件會放置在CN=電腦中、但您可以在必要時指定不同的OU。請參閱「」一節建立SMB機器帳戶所需的權限」、以瞭解新增/移除Cloud Volumes Service 機器帳戶物件所需的存取權限。

當將SMB機器帳戶新增至Active Directory時Cloud Volumes Service 、會填入下列欄位：

- （使用指定的SMB伺服器名稱）
- dnsHostName（含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AES加密、則允許使用DES_CBC_MD5、RC4 _HMAC_MD5、AES128 _CTs_HMAC_SHA1_96、AES256_CTs_HMAC_SHA1_96進行Kerberos票證交換）
- 名稱（使用SMB伺服器名稱）
- SamAccountName（含SMBserver$）
- servicePrincipalName（含主機/smbserver.domain.com和主機/smbserver SPN for Kerberos）

如果您要停用機器帳戶上較弱的Kerberos加密類型（加密類型）、可以將機器帳戶上的MSDS-SupportedEncryptionTypes值變更為下表中的其中一個值、以僅允許AES。

msDS-SupportedEncryptionTypes值	已啟用**EncType**
2.	ds_CBC_MD5
4.	RC4_HMAC
8.	僅限AES122_CTs_HMAC_SHA1_96
16	僅限AES256_CTs_HMAC_SHA1_96
24	AES122_CTs_HMAC_SHA1_96 與AES256_CTs_HMAC_SHA1_96
30	DES_CBC_MD5、RC4_HMAC、AES122_CTs_HMAC_SHA1_96和AES256_CTs_HMAC_SHA1_96

若要啟用SMB機器帳戶的AES加密、請在建立Active Directory連線時按一下「啟用AD驗證的AES加密」。

若要啟用NFS Kerberos的AES加密、"請參閱Cloud Volumes Service 《》文件"。

其他**NAS**基礎架構服務相依性（**Kdc**、**LDAP**和**DNS**）

使用Cloud Volumes Service 適用於NAS共享的功能時、可能需要外部相依性才能正常運作。在特定情況下、這些相依關係仍在發揮。下表顯示各種組態選項、以及必要的相依性（如果有）。

組態	所需相依性
僅限NFSv3	無
僅NFSv3 Kerberos	Windows Active Directory：* kdc * DNS * LDAP

組態	所需相依性
僅限NFSv4.1	用戶端ID對應組態（/etc/idmap.conf）
僅NFSv4.1 Kerberos	• 用戶端ID對應組態（/etc/idmap.conf） • Windows Active Directory：Kdc DNS LDAP
僅限SMB	Active Directory：* kdc * dns
多重傳輸協定NAS（NFS和SMB）	• 用戶端ID對應組態（僅限NFSv4.1；/etc/idmap.conf） • Windows Active Directory：Kdc DNS LDAP

機器帳戶物件的**Kerberos Keytab**旋轉/密碼重設

利用SMB機器帳戶Cloud Volumes Service 、此資訊可排定SMB機器帳戶的定期密碼重設。這些密碼會使用Kerberos加密進行重設、並在晚上11點到凌晨1點之間的隨機時間、於每四個星期日的排程中運作。這些密碼重設會變更Kerberos金鑰版本、旋轉Cloud Volumes Service 儲存在支援系統上的金鑰索引標籤、並協助維護執行Cloud Volumes Service 於支援更新版本的SMB伺服器的安全性。機器帳戶密碼是隨機配置的、系統管理員不知道。

對於NFS Kerberos機器帳戶、密碼重設只會在建立新的金鑰索引標籤並與Kdc交換時進行。目前Cloud Volumes Service 無法在不執行此動作的情況下進行。

用於**LDAP**和**Kerberos**的網路連接埠

使用LDAP和Kerberos時、您應該判斷這些服務所使用的網路連接埠。您可以在中找到Cloud Volumes Service一份完整的清單、其中列出了供列舉使用的連接埠 "安全考量的相關文件Cloud Volumes Service"。

LDAP

充當LDAP用戶端、並使用標準LDAP搜尋查詢來查詢UNIX身分識別的使用者和群組。Cloud Volumes Service如果您想要使用Cloud Volumes Service 超出由供應之標準預設使用者的使用者和群組、則必須使用LDAP。如果您打算搭配使用者主體使用NFS Kerberos（例如user1@domain.com）、也必須使用LDAP。目前僅支援使用Microsoft Active Directory的LDAP。

若要將Active Directory當作UNIX LDAP伺服器使用、您必須在要用於UNIX身分識別的使用者和群組上填入必要的UNIX屬性。使用預設的LDAP架構範本來查詢屬性Cloud Volumes Service "RFC-2307-bis"。因此、下表顯示使用者和群組所需的最低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 "管理雙傳輸協定存取。"

屬性	它的作用
UID*	指定UNIX使用者名稱
uidNumber*	指定UNIX使用者的數字ID
gidNumber*	指定UNIX使用者的主要群組數字ID
objectClass *	指定要使用的物件類型；Cloud Volumes Service 物件類別清單中必須包含「使用者」（預設會包含在大部分的Active Directory部署中）。

屬性	它的作用
名稱	帳戶的一般資訊（真實姓名、電話號碼等、也稱為gecos）
unixUserPassword	無需設定、不適用於NAS驗證的UNIX身分識別查詢。設定此選項會將設定的unixUserPassword值設為純文字。
unixHomeDirectory	當使用者從Linux用戶端驗證LDAP時、定義UNIX主目錄的路徑。如果您要使用LDAP來執行UNIX主目錄功能、請設定此選項。
LoginShell	當使用者根據LDAP驗證時、定義Linux用戶端的Basash/profile Shell路徑。

*表示屬性是使用Cloud Volumes Service 功能不正確的必要條件。其餘屬性僅供用戶端使用。

屬性	它的作用
CN*	指定UNIX群組名稱。使用Active Directory for LDAP時、會在第一次建立物件時設定此選項、但稍後可加以變更。此名稱不得與其他物件相同。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不允許兩個具有相同CN屬性的物件。若要解決此問題、請將Windows使用者重新命名為唯一名稱（例如user-UNIX）；Cloud Volumes Service LDAP in Wesc使用UNIX使用者名稱的uid屬性。
gidNumber*	指定UNIX群組的數字ID。
objectClass *	指定要使用的物件類型；Cloud Volumes Service 使用物件類別清單時、需要將群組包含在物件類別清單中（此屬性預設會包含在大部分的Active Directory部署中）。
memberUid	指定哪些UNIX使用者是UNIX群組的成員。在Active Directory LDAP Cloud Volumes Service 的不實情況下、此欄位是不必要的。「支援組成員資格」功能使用「成員」欄位Cloud Volumes Service 。
成員*	群組成員資格/次要UNIX群組所需。此欄位是透過新增Windows使用者至Windows群組來填入。但是，如果Windows群組未填入UNIX屬性，則不會包含在UNIX使用者的群組成員資格清單中。任何需要在NFS中使用的群組、都必須填入此表格中所列的必要UNIX群組屬性。

*表示屬性是使用Cloud Volumes Service 功能不正確的必要條件。其餘屬性僅供用戶端使用。

LDAP連結資訊

若要查詢LDAP中的使用者、Cloud Volumes Service 必須將（登入）連結至LDAP服務。此登入具有唯讀權限、可用於查詢LDAP UNIX屬性以進行目錄查詢。目前只能使用SMB機器帳戶來進行LDAP連結。

您只能針對「CVS效能」執行個體啟用LDAP、並將其用於NFSv3、NFSv4.1或雙傳輸協定磁碟區。Active Directory連線必須與Cloud Volumes Service 支援LDAP的Volume在相同的地區建立、才能成功部署。

啟用LDAP時、會在特定情況下發生下列情況。

- 如果Cloud Volumes Service 僅將NFSv3或NFSv4.1用於該項目、則會在Active Directory網域控制器中建立新的機器帳戶、Cloud Volumes Service 而在其中的LDAP用戶端則會使用機器帳戶認證來繫結至Active Directory。不會為NFS磁碟區和預設的隱藏管理共用建立SMB共用區（請參閱一節）"「預設隱藏共用」"）刪除共享ACL。
- 如果Cloud Volumes Service 將雙傳輸協定磁碟區用於執行此項目、則Cloud Volumes Service 只會使用專為SMB存取所建立的單一機器帳戶、將位於的LDAP用戶端連結至Active Directory。不會建立其他機器帳戶。
- 如果專屬SMB磁碟區是分開建立（在啟用LDAP的NFS磁碟區之前或之後）、則LDAP繫結的機器帳戶會與SMB機器帳戶共用。
- 如果也啟用NFS Kerberos、則會建立兩個機器帳戶：一個用於SMB共用和（或）LDAP繫結、另一個用於NFS Kerberos驗證。

LDAP查詢

雖然LDAP繫結已加密、但LDAP查詢會使用通用LDAP連接埠389、以純文字形式透過線路傳送。這個廣為人知的連接埠目前無法在Cloud Volumes Service 更新過程中進行變更。因此、在網路中存取封包偵測功能的人可以看到使用者和群組名稱、數字ID和群組成員資格。

不過、Google Cloud VM無法窺探其他VM的單點傳播流量。只有主動參與LDAP流量（亦即能夠連結）的VM、才能看到來自LDAP伺服器的流量。如需Cloud Volumes Service 更多有關資料包偵測功能的資訊、請參閱一節"「封包偵測/追蹤考量。」"

LDAP用戶端組態預設值

在Cloud Volumes Service 某個實例中啟用LDAP時、預設會以特定組態詳細資料建立LDAP用戶端組態。在某些情況下、選項可能不適用於Cloud Volumes Service 不支援的功能（不支援）、也可能無法設定。

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
LDAP伺服器清單	設定用於查詢的LDAP伺服器名稱或IP位址。這並不適用於Cloud Volumes Service 不適用。而是使用Active Directory網域來定義LDAP伺服器。	未設定	否
Active Directory網域	設定Active Directory網域用於LDAP查詢。利用DNS中的SRVs LDAP記錄、在網域中尋找LDAP伺服器。Cloud Volumes Service	設定為Active Directory連線中指定的Active Directory網域。	否
慣用的Active Directory伺服器	設定要用於LDAP的慣用Active Directory伺服器。不受Cloud Volumes Service 支援。而是使用Active Directory站台來控制LDAP伺服器選擇。	未設定。	否

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
使用SMB伺服器認證進行連結	使用SMB機器帳戶連結至LDAP。目前Cloud Volumes Service 、唯一受支援的LDAP綁定方法就是支援的功能。	是的	否
架構範本	用於LDAP查詢的架構範本。	MS-AD-BIS	否
LDAP伺服器連接埠	用於LDAP查詢的連接埠號碼。目前僅使用標準LDAP連接埠389。Cloud Volumes Service目前不支援LDAPS/Port 636。	389	否
是否已啟用LDAPS	控制LDAP over Secure Socket Layer（SSL）是否用於查詢和連結。目前不受Cloud Volumes Service支援。	錯	否
查詢逾時（秒）	查詢逾時。如果查詢的時間超過指定值、查詢就會失敗。	3.	否
最小綁定驗證層級	支援的最低連結層級。由於使用機器帳戶進行LDAP連結、且Active Directory預設不支援匿名連結、因此此選項不適用於安全性。Cloud Volumes Service	匿名	否
連結DN	使用簡單繫結時用於繫結的使用者/辨別名稱（DN）。使用機器帳戶進行LDAP連結、目前不支援簡單的連結驗證。Cloud Volumes Service	未設定	否
基礎DN	用於LDAP搜尋的基礎DN。	Windows網域用於Active Directory連線、採用DN格式（亦即DC=DOWN, DC=local）。	否
基礎搜尋範圍	基礎DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。僅支援子樹狀結構搜尋。Cloud Volumes Service	子樹狀結構	否

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
使用者DN	定義使用者開始搜尋LDAP查詢的DN。目前不支援Cloud Volumes Service使用此功能、因此所有使用者搜尋都從基礎DN開始。	未設定	否
使用者搜尋範圍	使用者DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援設定使用者搜尋範圍。Cloud Volumes Service	子樹狀結構	否
群組DN	定義群組開始搜尋LDAP查詢的DN。目前不支援Cloud Volumes Service使用此功能、因此所有群組搜尋都會從基礎DN開始。	未設定	否
群組搜尋範圍	群組DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援設定群組搜尋範圍。Cloud Volumes Service	子樹狀結構	否
網路群組DN	定義netgroup開始搜尋LDAP查詢的DN。目前不支援Cloud Volumes Service 使用此功能、因此所有網路群組搜尋都會從基礎DN開始。	未設定	否
網路群組搜尋範圍	netgroup DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援設定netgroup搜尋範圍。Cloud Volumes Service	子樹狀結構	否
透過LDAP使用start_tls	利用Start TLS透過連接埠389進行憑證型LDAP連線。目前不受Cloud Volumes Service 支援。	錯	否
啟用各主機的網路群組查詢	可依主機名稱進行網路群組查詢、而非展開網路群組以列出所有成員。目前不受Cloud Volumes Service 支援。	錯	否

LDAP用戶端選項	它的作用	預設值	可以改變嗎？
網路群組的主機DN	定義netgroup by host開始搜尋LDAP查詢的DN。不支援Cloud Volumes Service 以主機為單位的netgroup。	未設定	否
Netgroup依主機搜尋範圍	netgroup by主機DN搜尋的搜尋範圍。值可以包括base、onel海拔 或子樹狀結構。不支援Cloud Volumes Service 以主機為單位的netgroup。	子樹狀結構	否
用戶端工作階段安全性	定義LDAP使用的工作階段安全性層級（簽署、認證或無）。如果Active Directory要求、則CVS效能可支援LDAP簽署。CVS軟體不支援LDAP簽署。目前不支援這兩種服務類型的密封。	無	否
LDAP參照追蹤	使用多個LDAP伺服器時、如果第一個伺服器中找不到項目、參照追蹤功能可讓用戶端參照清單中的其他LDAP伺服器。目前不支援此功能Cloud Volumes Service 。	錯	否
群組成員資格篩選器	提供自訂LDAP搜尋篩選器、以便在從LDAP伺服器查詢群組成員資格時使用。目前不支援Cloud Volumes Service 使用此功能。	未設定	否

使用**LDAP**進行非對稱名稱對應

根據預設、不需特殊組態、即可雙向對應具有相同使用者名稱的Windows使用者和UNIX使用者。Cloud Volumes Service只要Cloud Volumes Service 找到有效的UNIX使用者（使用LDAP）、就會產生1：1名稱對應。例如、如果使用Windows使用者「johnsmith」、Cloud Volumes Service 那麼如果在LDAP中找到名為「johnsmith」的UNIX使用者、則名稱對應會為該使用者成功、所有由「johnsmith」建立的檔案/資料夾都會顯示正確的使用者擁有權、 而影響「johnsmith」的所有ACL、無論使用的是哪種NAS傳輸協定、都是受到尊重的。這稱為對稱名稱對應。

非對稱名稱對應是指Windows使用者和UNIX使用者身分不相符的情況。舉例Cloud Volumes Service 來說、如果Windows使用者「johnsmith」的UNIX身分為「jsmith」、那麼就需要一種方式來瞭解這種差異。由於目前不支援建立靜態名稱對應規則、因此LDAP必須用於查詢Windows和UNIX身分識別的使用者身分、以確保檔案和資料夾擁有適當的所有權、以及預期的權限。Cloud Volumes Service

根據預設Cloud Volumes Service 、在名稱對應資料庫的n-switches中加入「LDAP」、以便使用LDAP提供非對稱名稱的名稱對應功能、您只需修改部分使用者/群組屬性、以反映Cloud Volumes Service 出本產品的外觀。

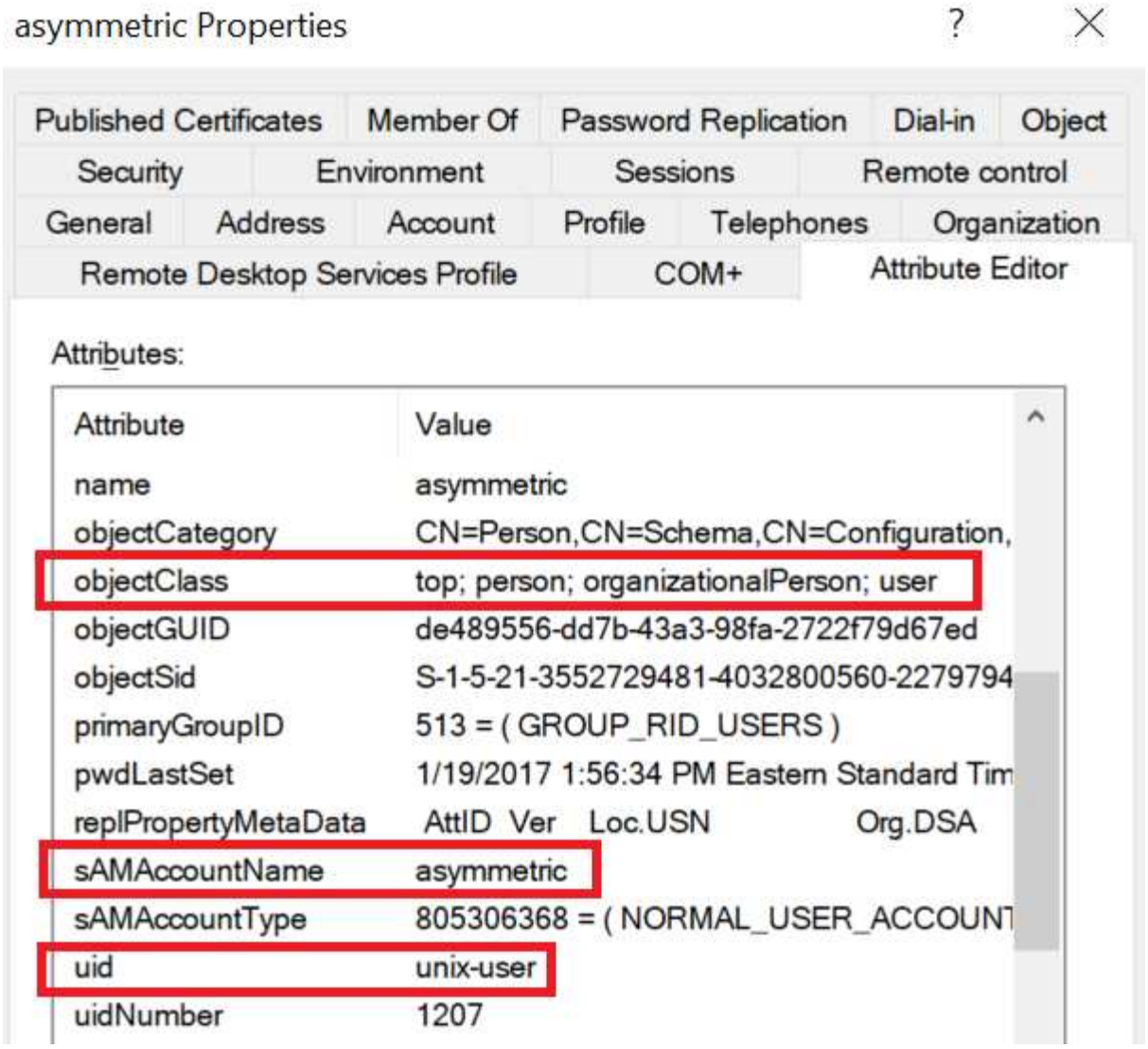
下表顯示在LDAP中必須填入哪些屬性才能使用非對稱名稱對應功能。在大多數情況下、Active Directory已設定為執行此作業。

屬性**Cloud Volumes Service**	它的作用	供名稱對應之用的值**Cloud Volumes Service**
Windows到UNIX的objectClass	指定要使用的物件類型。（也就是使用者、群組、posixAccount等）	必須包含使用者（如有需要、可包含多個其他值）。
Windows至UNIX屬性	定義建立時的Windows使用者名稱。可將此功能用於Windows到UNIX的查詢。Cloud Volumes Service	此處無需變更；sAMAccountName與Windows登入名稱相同。
UID	定義UNIX使用者名稱。	所需的UNIX使用者名稱。

由於目前無法在LDAP查詢中使用網域前置碼、因此多個網域LDAP環境無法在LDAP namemap查詢中正常運作。Cloud Volumes Service

以下範例顯示Windows名稱為「不對稱」、UNIX名稱為「UNIX使用者」的使用者、以及從SMB和NFS寫入檔案時所遵循的行為。

下圖顯示LDAP屬性從Windows伺服器的外觀。



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
```

從NFS將檔案寫入為「UNIX使用者」時、NFS用戶端會產生下列結果：

```
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、您可以看到檔案擁有者已設定為適當的Windows使用者：

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

相反地、Windows使用者從SMB用戶端建立的「非對稱」檔案、會顯示適當的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通道繫結

由於Windows Active Directory網域控制器存在弱點、 "Microsoft安全性摘要報告ADV190023" 變更DC允許LDAP繫結的方式。

對功能的影響Cloud Volumes Service 與對任何LDAP用戶端的影響相同。目前不支援通道連結。Cloud Volumes Service由於根據預設、透過協商來支援LDAP簽署、因此LDAP通道繫結不應成為問題。Cloud Volumes Service如果您在啟用通道繫結的情況下、無法連結至LDAP、請遵循ADV190023的修正步驟、讓LDAP從Cloud Volumes Service 支援區連結成功。

DNS

Active Directory和Kerberos都依賴DNS來解析主機名稱與IP / IP之間的主機名稱。DNS需要開啟連接埠53。不修改DNS記錄、也不支援使用Cloud Volumes Service "動態DNS" 在網路介面上。

您可以設定Active Directory DNS、限制哪些伺服器可以更新DNS記錄。如需詳細資訊、請參閱 "安全的Windows DNS"。

請注意、Google專案中的資源預設為使用Google Cloud DNS、而Google Cloud DNS並未與Active Directory DNS連線。使用Cloud DNS的用戶端無法解析Cloud Volumes Service 由解決所傳回的UNC路徑。加入Active Directory網域的Windows用戶端已設定為使用Active Directory DNS、並可解析此類的UNC路徑。

若要將用戶端加入Active Directory、您必須將其DNS組態設定為使用Active Directory DNS。您也可以設定Cloud DNS、將要求轉送至Active Directory DNS。請參閱 "為什麼我的用戶端無法解析SMB NetBios名稱？" 以取得更多資訊。

目前不支援DNSSEC、DNS查詢則以純文字執行。Cloud Volumes Service

檔案存取稽核

目前不支援Cloud Volumes Service 使用此功能。

防毒保護

您必須在Cloud Volumes Service 用戶端執行「從位向至NAS共享區的」功能中的防毒掃描。目前沒有原生的防毒整合Cloud Volumes Service 功能可搭配使用。

服務營運

這個支援團隊負責管理Google Cloud的後端服務、並運用多種策略來保護平台安全、防止不必要的存取。Cloud Volumes Service

每位客戶都有自己專屬的子網路、預設會有與其他客戶隔離的存取權限、Cloud Volumes Service 而在這個子網路中、每個租戶都會獲得自己的命名空間和VLAN、以實現整體資料隔離。驗證使用者之後、服務交付引擎（SDE）只能讀取該租戶專屬的組態資料。

實體安全性

在適當的預先核准下、只有現場工程師和NetApp認可的現場支援工程師（FSE）才能存取機箱和機架進行實體工作。不允許進行儲存與網路管理。只有這些現場資源能夠執行硬體維護工作。

對於現場工程師、會提出一份工作說明書（SOW）的票證、其中包括機架ID和裝置位置（RU）、以及所有其他詳細資料均包含在票證中。對於NetApp FSE、必須向Colo出示網站參訪票證、票證中必須包含訪客的詳細資料、日期和時間、以供稽核之用。FSE的SOW會在內部傳達給NetApp。

營運團隊

支援此功能的營運團隊Cloud Volumes Service 由Production Engineering和Site可靠性工程師（SRE）組成、負責雲端Volume Services、以及NetApp現場支援工程師和硬體合作夥伴。所有營運團隊成員均已獲得Google Cloud認證、並會針對每張提出的問題單、維護詳細的工作記錄。此外、也有嚴格的變更控管與核准程序、確保每項決策都經過適當的審查。

SRE團隊負責管理控制面板、以及如何將資料從UI要求路由傳送至Cloud Volumes Service 支援的後端硬體和軟體。SRE團隊也會管理系統資源、例如磁碟區和inode上限。SRES不得與客戶資料互動或存取。SRES也能與退貨材料授權（RMA）協調、例如新磁碟或後端硬體的記憶體更換要求。

客戶責任

客戶負責管理組織的Active Directory和使用者角色管理、以及磁碟區和資料作業。Cloud Volumes Service客戶可以擁有管理角色、並可使用NetApp和Google Cloud提供的兩個預先定義角色（管理員和檢視者）、將權限委派給同一個Google Cloud專案中的其他終端使用者。

系統管理員可以對等客戶專案中的任何VPC、Cloud Volumes Service 使客戶認爲適當。客戶有責任管理其Google Cloud市場訂閱的存取權、以及管理可存取資料層面的VPC。

惡意**SRE**保護

可能會產生的一項疑慮是Cloud Volumes Service 、當發生惡意SRE或SRE認證遭入侵時、如何保護不受攻擊？

只有少數SRE人員能夠存取正式作業環境。系統管理權限進一步限制給少數經驗豐富的系統管理員。我們的安全資訊與事件管理（SIEM）威脅情報平台會記錄所有在整個流程環境中由任何人執行的行動Cloud Volumes Service 、並偵測到任何基礎異常或可疑活動。因此、在Cloud Volumes Service 對該後端造成太多損害之前、可以追蹤並減輕惡意行為。

Volume生命週期

僅管理服務中的物件、而非磁碟區內的資料。Cloud Volumes Service只有存取磁碟區的用戶端才能管理資料、ACL、檔案擁有者等。這些磁碟區中的資料會在閒置時加密、而且只能由Cloud Volumes Service 執行個體的租戶存取。

支援的Volume生命週期Cloud Volumes Service 是「cree-update-delete」。Volume會保留Volume的Snapshot複本、直到磁碟區被刪除為止、而且只有通過驗證Cloud Volumes Service 的NetApp管理員才能刪除Cloud Volumes Service 整個實體中的Volume。當系統管理員要求刪除磁碟區時、需要輸入磁碟區名稱的其他步驟來驗證刪除作業。刪除磁碟區後、磁碟區便會消失、無法恢復。

如果終止了某個方面的合約、NetApp會在特定時間段後將磁碟區標示為刪除。Cloud Volumes Service在該期間到期之前、您可以應客戶的要求來恢復磁碟區。

認證

Cloud Volumes Services for Google Cloud目前已通過ISO/IEC 27001：2013和ISO/IEC 27018：2019標準的認證。該服務最近也收到SOC2類型I證明報告。如需NetApp對資料安全性與隱私權承諾的相關資訊、請參閱 "法規遵循：資料安全與資料隱私"。

GDPR

我們對隱私權和遵守GDPR的承諾、已在我們的多個公司中提供 "客戶合約"、例如我們的 "客戶資料處理附錄"、其中包括 "標準合約條款" 由歐盟委員會提供。我們也會在隱私權政策中做出這些承諾、並以公司行為準則中所列的核心價值為後盾。

其他資訊和聯絡資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- Google Cloud文件Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google私有服務存取

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp產品文件

  "https://www.netapp.com/support-and-training/documentation/"

- 密碼編譯驗證模組方案—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 NFS Kerberos in Sf2

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

聯絡我們

請告訴我們如何改善這份技術報告。

請聯絡我們：mailto：doccomments@netapp.com doccomments@netapp.com。在主題行中加入技術報告4918。

BlueXP 備份與還原

適用於 **VM** 的 **BlueXP** 備份與還原

適用於 **VMware** 的 **3-2-1 Data Protection** 、搭配 **SnapCenter** 外掛程式、以及適用於 **VM** 的 **BlueXP** 備份與還原

作者： Josh Powell - NetApp 解決方案工程部

總覽

3-2-1 備份策略是業界公認的資料保護方法、提供全方位的方法來保護寶貴資料。 這項策略是可靠的、即使發生意外的災難、仍會有可用的資料複本。

此策略包含三項基本規則：

1. 請至少保留三份資料複本。如此可確保即使有一個複本遺失或毀損、您仍至少還有兩個剩餘的複本要重新放回。
2. 將兩個備份複本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範裝置特定或媒體特定的故障。如果某個裝置受損或某種類型的媒體故障、另一個備份複本則不受影響。
3. 最後、請確定至少有一個備份複本位於異地。異地儲存設備可作為故障防護、避免發生局部災難、例如火災或洪水、使現場複本無法使用。

本解決方案文件涵蓋 3-2-1 備份解決方案、使用適用於 VMware vSphere （ SCV ）的 SnapCenter 外掛程式來建立內部部署虛擬機器的主要和次要備份、以及虛擬機器的 BlueXP 備份和還原、以便將我們的資料複本備份到雲端儲存設備或 StorageGRID 。

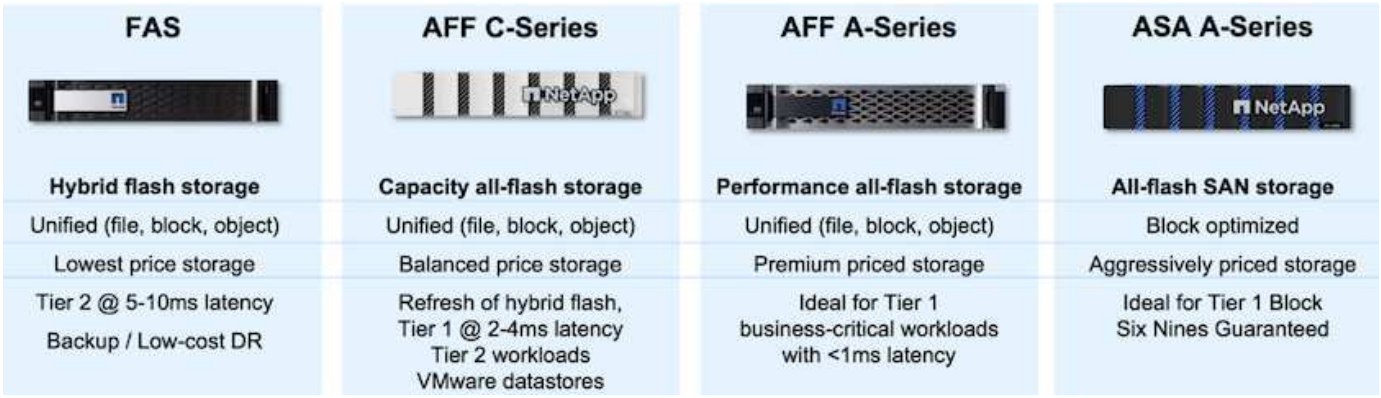
使用案例

本解決方案可解決下列使用案例：

- 使用適用於 VMware vSphere 的 SnapCenter 外掛程式、備份及還原內部部署虛擬機器和資料存放區。
- 備份及還原位於 ONTAP 叢集上的內部部署虛擬機器和資料存放區、並使用 BlueXP 備份與還原功能備份至虛擬機器的物件儲存區。

NetApp ONTAP 資料儲存

ONTAP 是 NetApp 領先業界的儲存解決方案、無論您是透過 SAN 或 NAS 傳輸協定存取、都能提供統一化的儲存設備。3-2-1 備份策略可確保內部部署的資料受到多種媒體類型的保護、而 NetApp 提供的平台範圍從高速快閃到低成本媒體。



如需 NetApp 所有硬體平台的詳細資訊、請參閱 "NetApp 資料儲存"。

VMware vSphere的插件SnapCenter

SnapCenter Plugin for VMware vSphere 是一項資料保護產品、與 VMware vSphere 緊密整合、可輕鬆管理虛擬機器的備份與還原。作爲該解決方案的一部分， SnapMirror 提供了一種快速可靠的方法，用於在輔助 ONTAP 存儲羣集上創建虛擬機數據的第二個不可變備份副本。有了這種架構、就能從主要或次要備份位置輕鬆啟動虛擬機器還原作業。

選擇控制閥是使用 OVA 檔案部署為 Linux 虛擬應用裝置。外掛程式現在使用遠端外掛程式架構。遠端外掛程式會在 vCenter 伺服器外部執行、並裝載於選擇控制閥虛擬應用裝置上。

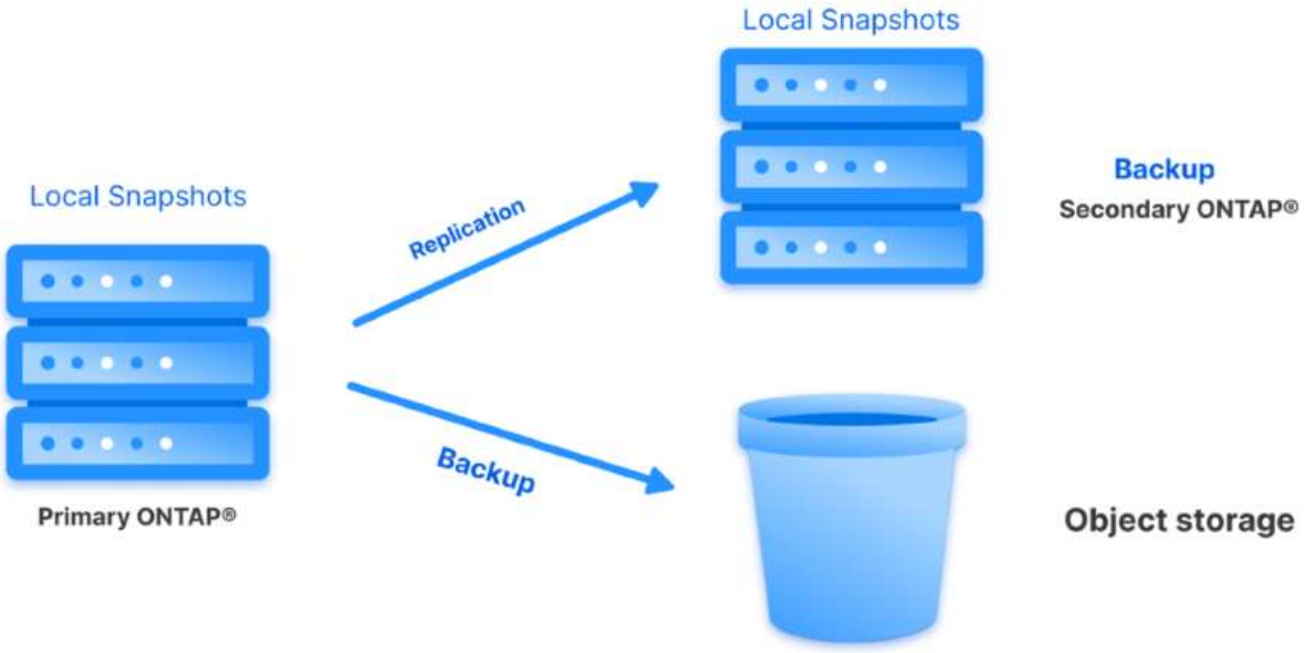
如需選擇控制閥的詳細資訊、請參閱 "VMware vSphere文件的VMware外掛程式SnapCenter"。

適用於虛擬機器的 **BlueXP** 備份與還原

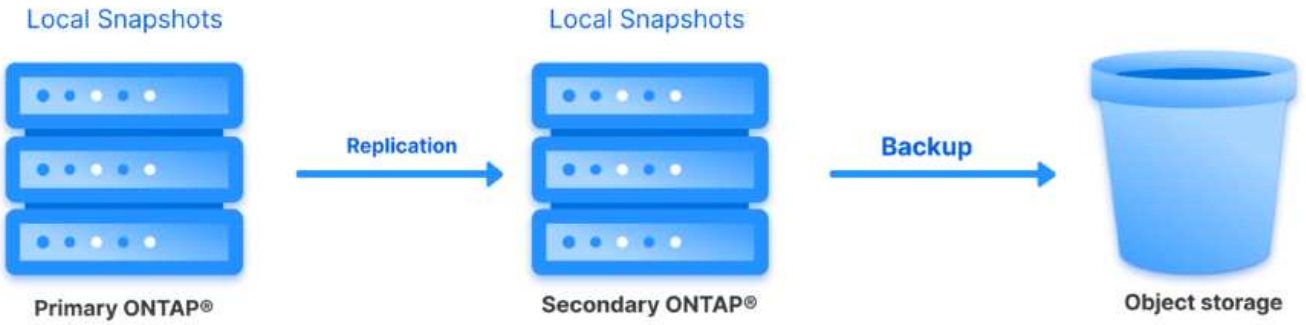
BlueXP 備份與還原是一種雲端型的資料管理工具、可提供單一控制面板、在內部部署和雲端環境中執行各種備份與還原作業。NetApp BlueXP 備份與還原套件的一部分是整合 SnapCenter Plugin for VMware vSphere （內部部署）的功能、可將資料複本延伸至雲端中的物件儲存設備。這會建立第三份資料的異地複本、該複本來自主要或次要儲存備份。BlueXP 備份與還原可讓您輕鬆設定儲存原則、從這兩個內部部署位置中的任一位置傳輸資料複本。

在 BlueXP 備份與還原中選擇主要與次要備份作為來源、將會實作下列兩種拓撲之一：

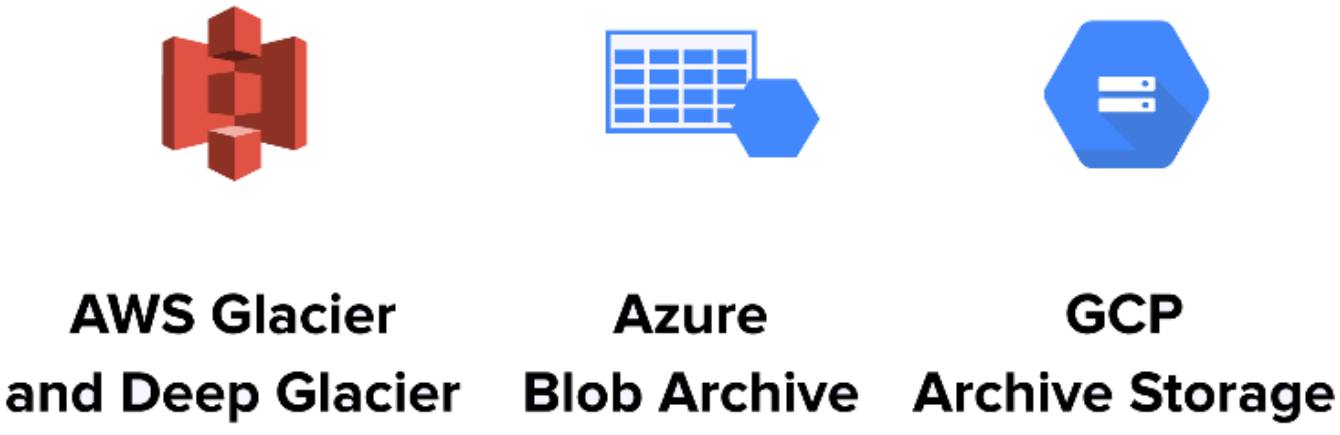
- 扇出拓撲 * –當 SnapCenter Plug-in for VMware vSphere 啟動備份時、會立即擷取本機快照。然後選擇控制閥啓動 SnapMirror 操作，將最近的快照複製到輔助 ONTAP 羣集。在 BlueXP 備份與還原中、原則會指定主要 ONTAP 叢集做為資料快照複本的來源、以便將資料傳輸至雲端供應商所選的物件儲存設備。



- 層疊拓撲 * –使用選擇控制閥建立主要和次要資料複本、與上述的扇出拓撲相同。不過、這次在 BlueXP 備份與還原中建立原則、指定備份至物件儲存設備將來自次要 ONTAP 叢集。



BlueXP 備份與還原可建立內部部署 ONTAP 快照的備份複本、以供保存至 AWS Glacier 、 Azure Blob 及 GCP Archive 儲存設備。



此外、您也可以使用 NetApp StorageGRID 做為物件儲存備份目標。如需 StorageGRID 的詳細資訊、請參閱 "StorageGRID 登陸頁面"。

解決方案部署總覽

此清單提供設定此解決方案、並從選擇控制閥和 BlueXP 備份與恢復執行備份與還原作業所需的高階步驟：

1. 設定用於主要和次要資料複本的 ONTAP 叢集之間的 SnapMirror 關係。
2. 為 VMware vSphere 設定 SnapCenter 外掛程式。
   a. 新增儲存系統
   b. 建立備份原則
   c. 建立資源群組
   d. 執行備份第一個備份工作
3. 設定虛擬機器的 BlueXP 備份與還原
   a. 新增工作環境
   b. 探索選擇控制閥和 vCenter 應用裝置
   c. 建立備份原則
   d. 啟動備份
4. 使用選擇控制閥從主要和次要儲存設備還原虛擬機器。
5. 使用 BlueXP 備份與還原、從物件儲存設備還原虛擬機器。

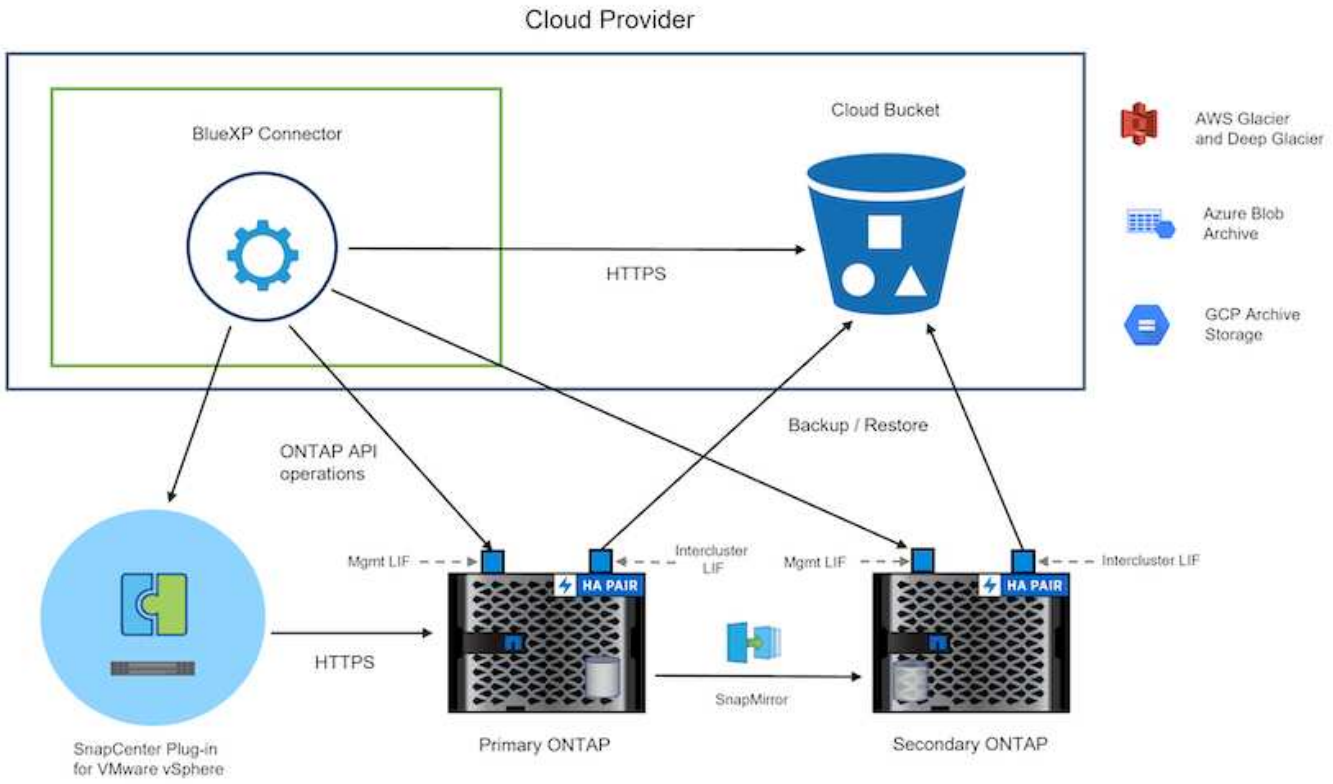
先決條件

此解決方案的目的是展示在 VMware vSphere 中執行、位於 NetApp ONTAP 託管的 NFS 資料存放區上的虛擬機器的資料保護功能。本解決方案假設已設定下列元件、可供使用：

1. ONTAP 儲存叢集、具有連接至 VMware vSphere 的 NFS 或 VMFS 資料存放區。NFS 和 VMFS 資料存放區均受支援。此解決方案使用 NFS 資料存放區。
2. 針對用於 NFS 資料存放區的磁碟區建立 SnapMirror 關係的次要 ONTAP 儲存叢集。
3. 安裝適用於雲端供應商的 BlueXP Connector 、用於物件儲存備份。
4. 要備份的虛擬機器位於主要 ONTAP 儲存叢集上的 NFS 資料存放區上。
5. BlueXP 連接器與內部部署 ONTAP 儲存叢集管理介面之間的網路連線。
6. BlueXP 連接器與內部部署的選擇控制閥設備 VM 之間、以及 BlueXP 連線器與 vCenter 之間的網路連線。
7. 內部部署 ONTAP 叢集間的生命體與物件儲存服務之間的網路連線。
8. 在主要和次要 ONTAP 儲存叢集上設定用於管理 SVM 的 DNS 。如需詳細資訊、請參閱 "設定DNS進行主機名稱解析"。

高層架構

本解決方案的測試/驗證是在實驗室中執行、可能與最終部署環境相符或不相符。



解決方案部署

在本解決方案中、我們提供詳細說明、說明如何部署和驗證採用 SnapCenter Plug-in for VMware vSphere 的解決方案、以及 BlueXP 備份和還原、以在位於內部部署資料中心的 VMware vSphere 叢集內執行 Windows 和 Linux 虛擬機器的備份和還原。此設定中的虛擬機器儲存在 ONTAP A300 儲存叢集所主控的 NFS 資料存放區上。此外、獨立的 ONTAP A300 儲存叢集可作為使用 SnapMirror 複寫之磁碟區的次要目的地。此外、在 Amazon Web Services 和 Azure Blob 上託管的物件儲存設備也被部署為第三份資料複本的目標。

我們將繼續為由選擇控制閥管理的備份次要複本建立 SnapMirror 關係、並在選擇控制閥和 BlueXP 備份和恢復中設定備份工作。

如需 SnapCenter Plug-in for VMware vSphere 的詳細資訊、請參閱 "VMware vSphere文件的VMware外掛程式SnapCenter"。

如需 BlueXP 備份與還原的詳細資訊、請參閱 "BlueXP 備份與還原文件"。

在 **ONTAP** 叢集之間建立 **SnapMirror** 關係

適用於 VMware vSphere 的 SnapCenter 外掛程式使用 ONTAP SnapMirror 技術來管理次要 SnapMirror 和 / 或 SnapVault 複本傳輸至次要 ONTAP 叢集的作業。

選擇控制閥備份原則可選擇使用 SnapMirror 或 SnapVault 關係。主要的差異在於、使用 SnapMirror 選項時、原則中為備份所設定的保留排程、在主要和次要位置會相同。SnapVault 是專為歸檔而設計、使用此選項時、可針對次要 ONTAP 儲存叢集上的快照複本、建立個別的 SnapMirror 保留排程。

可以在 BlueXP 中設定 SnapMirror 關係、其中許多步驟都是自動化的、或者可以使用系統管理員和 ONTAP CLI 來完成。以下將討論所有這些方法。

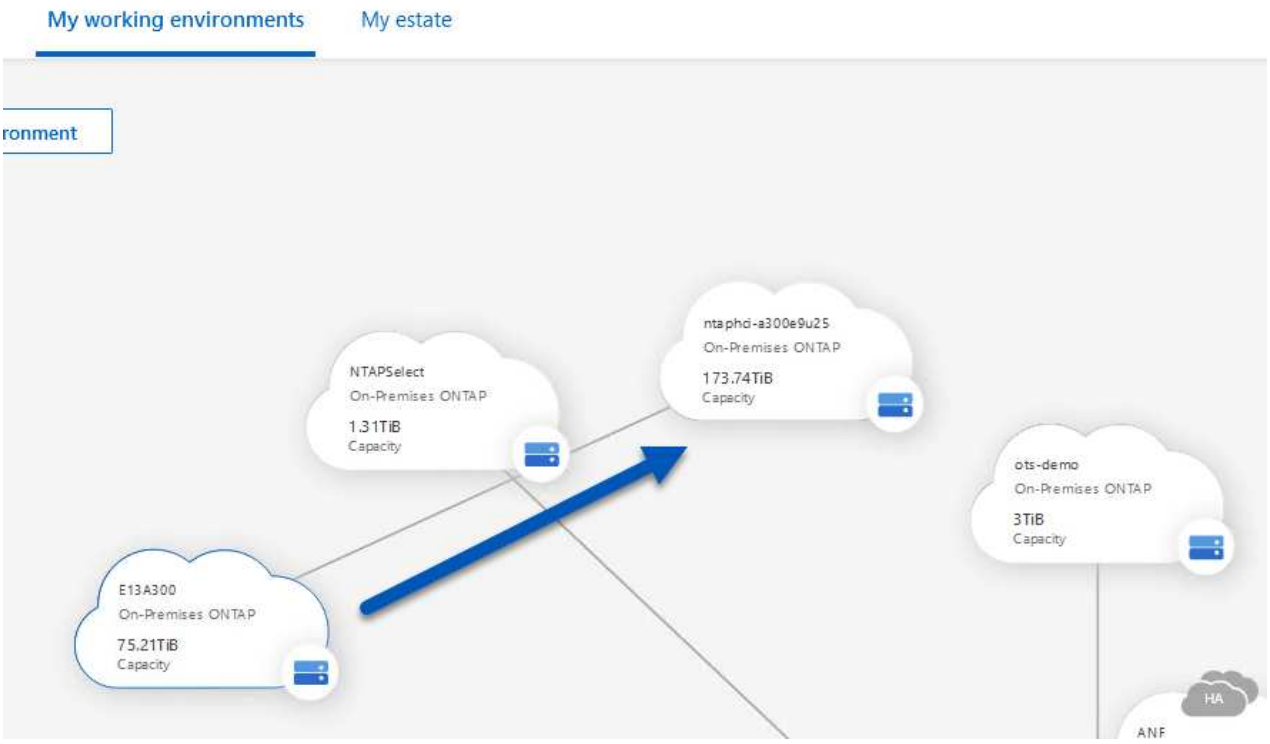
與 **BlueXP** 建立 **SnapMirror** 關係

必須從 BlueXP 網路主控台完成下列步驟：

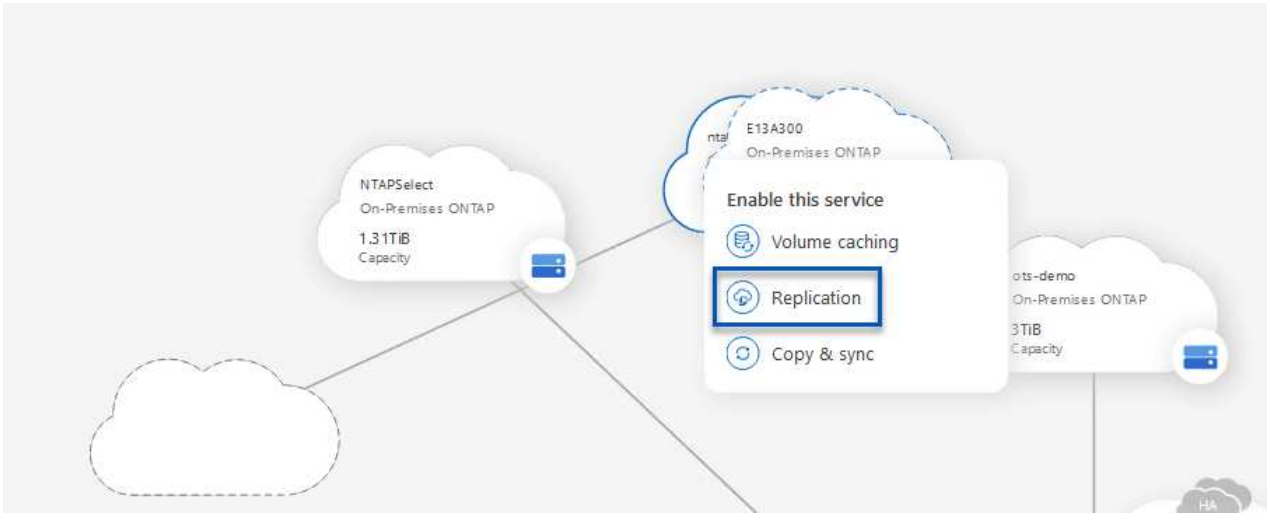
主要和次要 **ONTAP** 儲存系統的複寫設定

請先登入 BlueXP 網路主控台、然後瀏覽至 Canvas 。

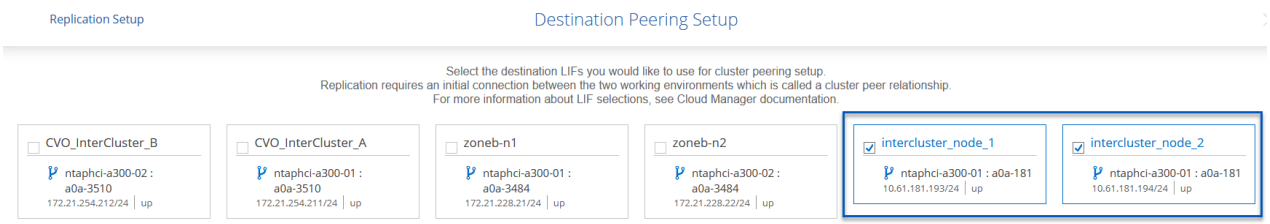
1. 將來源（主要） ONTAP 儲存系統拖放到目的地（次要） ONTAP 儲存系統上。



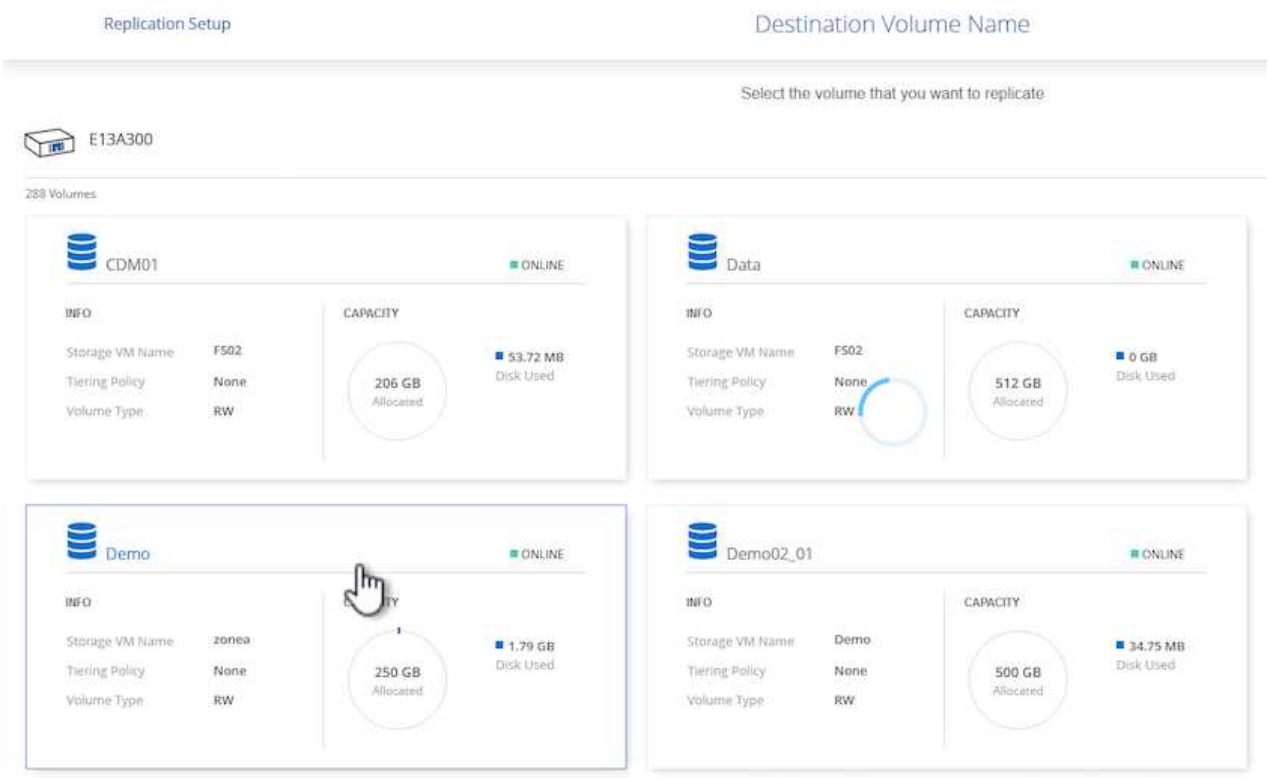
2. 從出現的功能表中選取 * Replication * 。



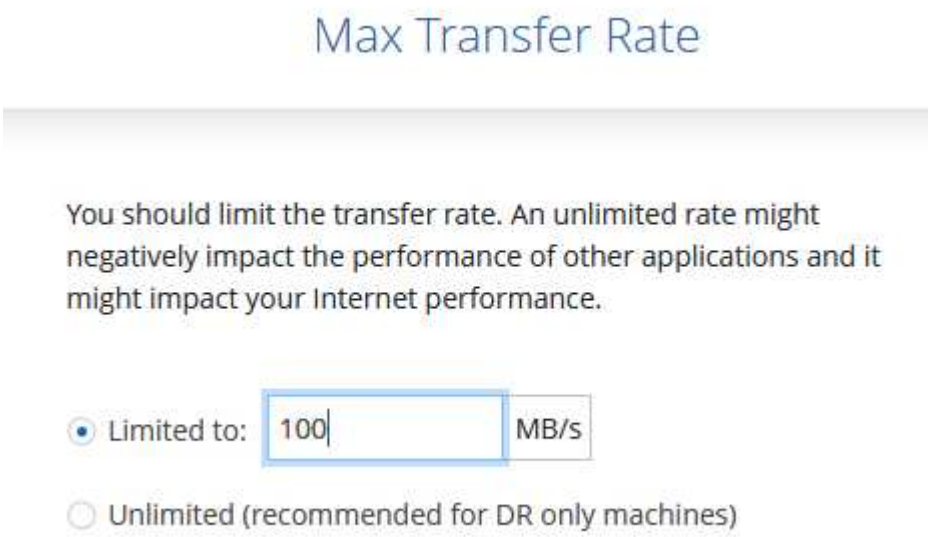
3. 在「 *Destination 對等項設定 * 」頁面上、選取儲存系統之間連線所要使用的目的地叢集間生命。



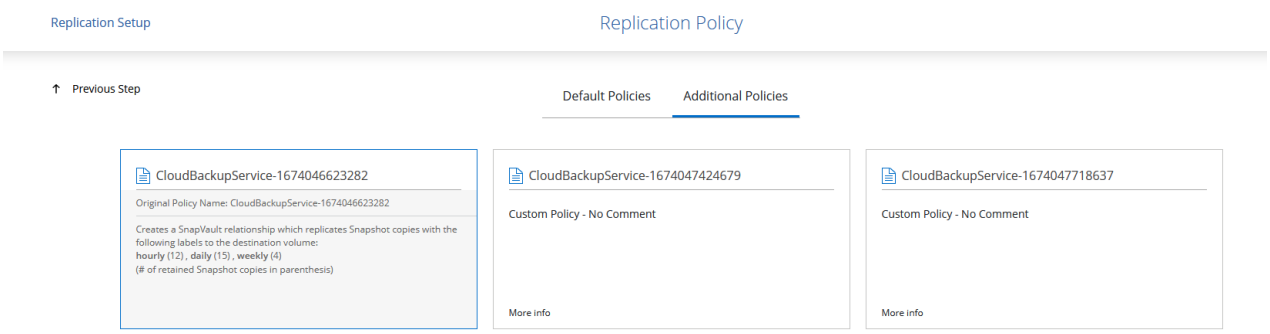
4. 在 * 目的地 Volume Name* 頁面上、先選取來源 Volume 、然後填寫目的地 Volume 名稱、再選取目的地 SVM 和 Aggregate 。按一下 * 下一步 * 繼續。



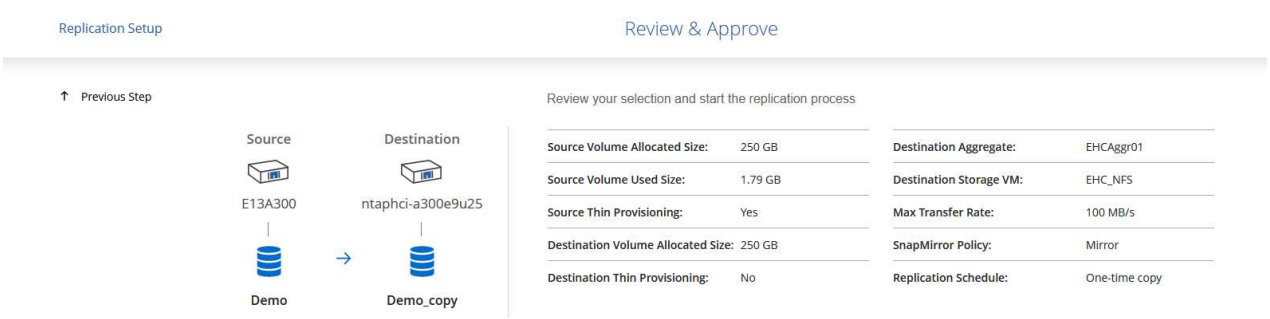
5. 選擇複寫的最大傳輸速率。



6. 選擇決定次要備份保留排程的原則。此原則可事先建立（請參閱以下 * 建立快照保留原則 * 步驟的手動程序）、也可視需要在事後變更。



7. 最後、請檢閱所有資訊、然後按一下「 **Go** 」按鈕以開始複寫設定程序。



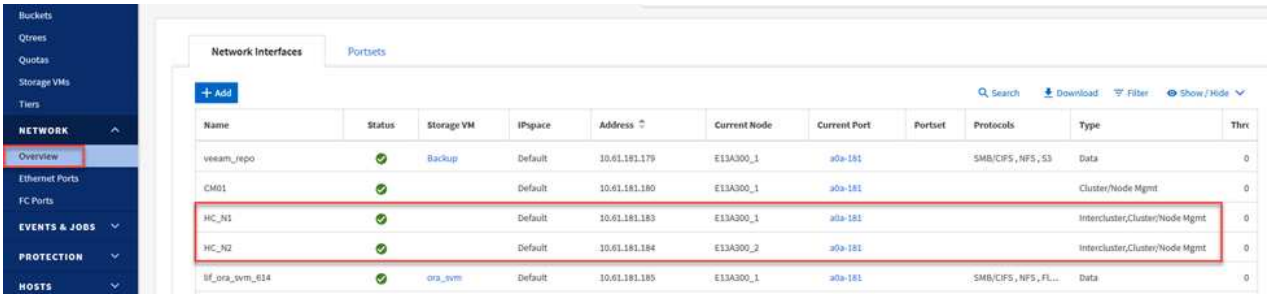
與 **System Manager** 和 **ONTAP CLI** 建立 **SnapMirror** 關係

所有建立 SnapMirror 關係所需的步驟都可以使用系統管理器或 ONTAP CLI 來完成。下節提供這兩種方法的詳細資訊：

記錄來源與目的地叢集間邏輯介面

對於來源和目的地 ONTAP 叢集、您可以從系統管理員或 CLI 擷取叢集間 LIF 資訊。

1. 在「支援系統管理程式」中ONTAP 、瀏覽至「網路總覽」頁面、並擷取「類型：叢集間」的IP位址、這些位址已設定為與安裝FSx的AWS VPC通訊。



2. 若要使用 CLI 擷取叢集間 IP 位址、請執行下列命令：

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

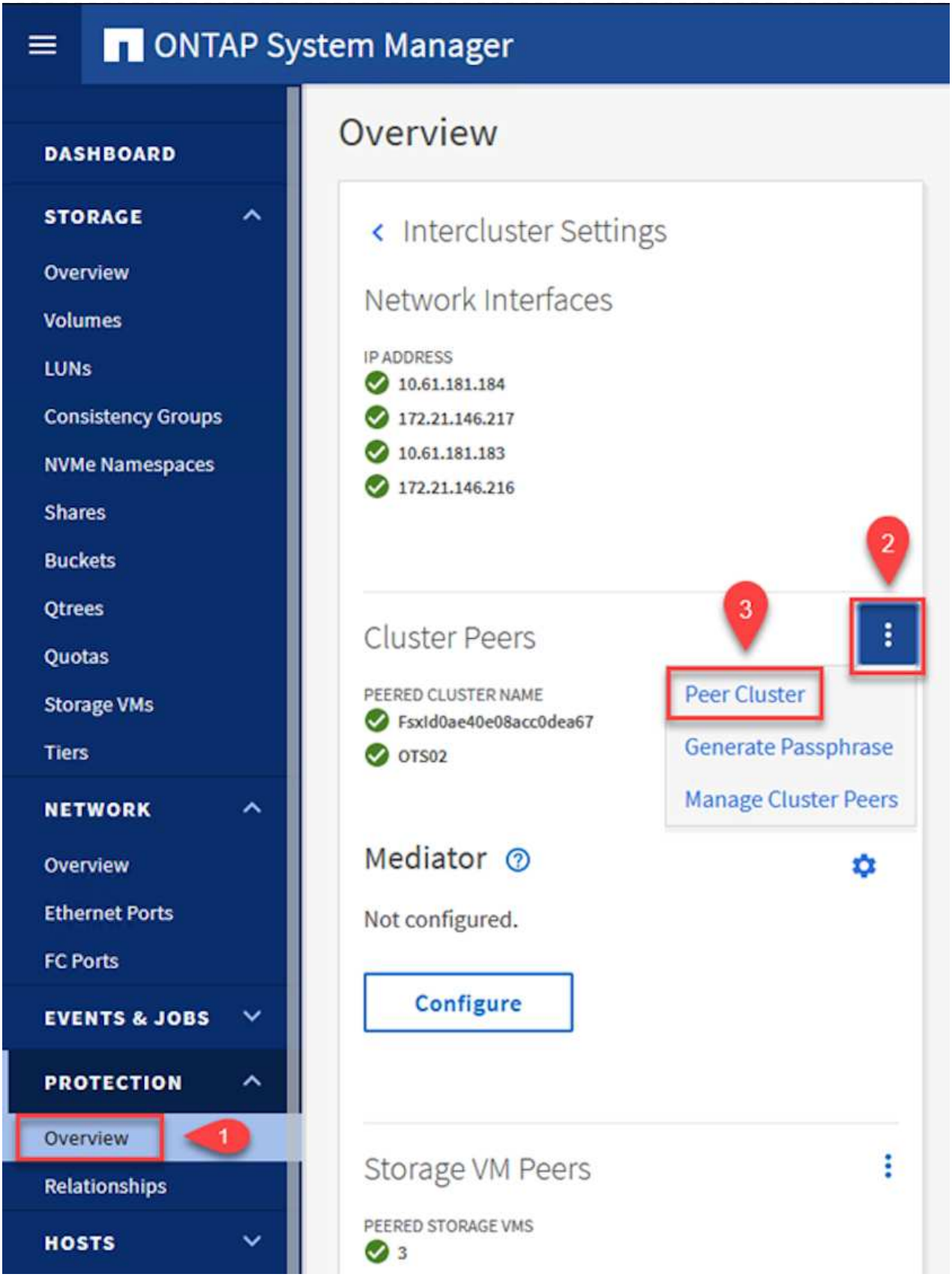
在 **ONTAP** 叢集之間建立叢集對等關係

若要在ONTAP 各個叢集之間建立叢集對等關係、必須ONTAP 在其他對等叢集中確認在起始的叢集上輸入的獨特通關密碼。

1. 使用在目的地 ONTAP 叢集上設定對等關係 `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、以完成建立程序。

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

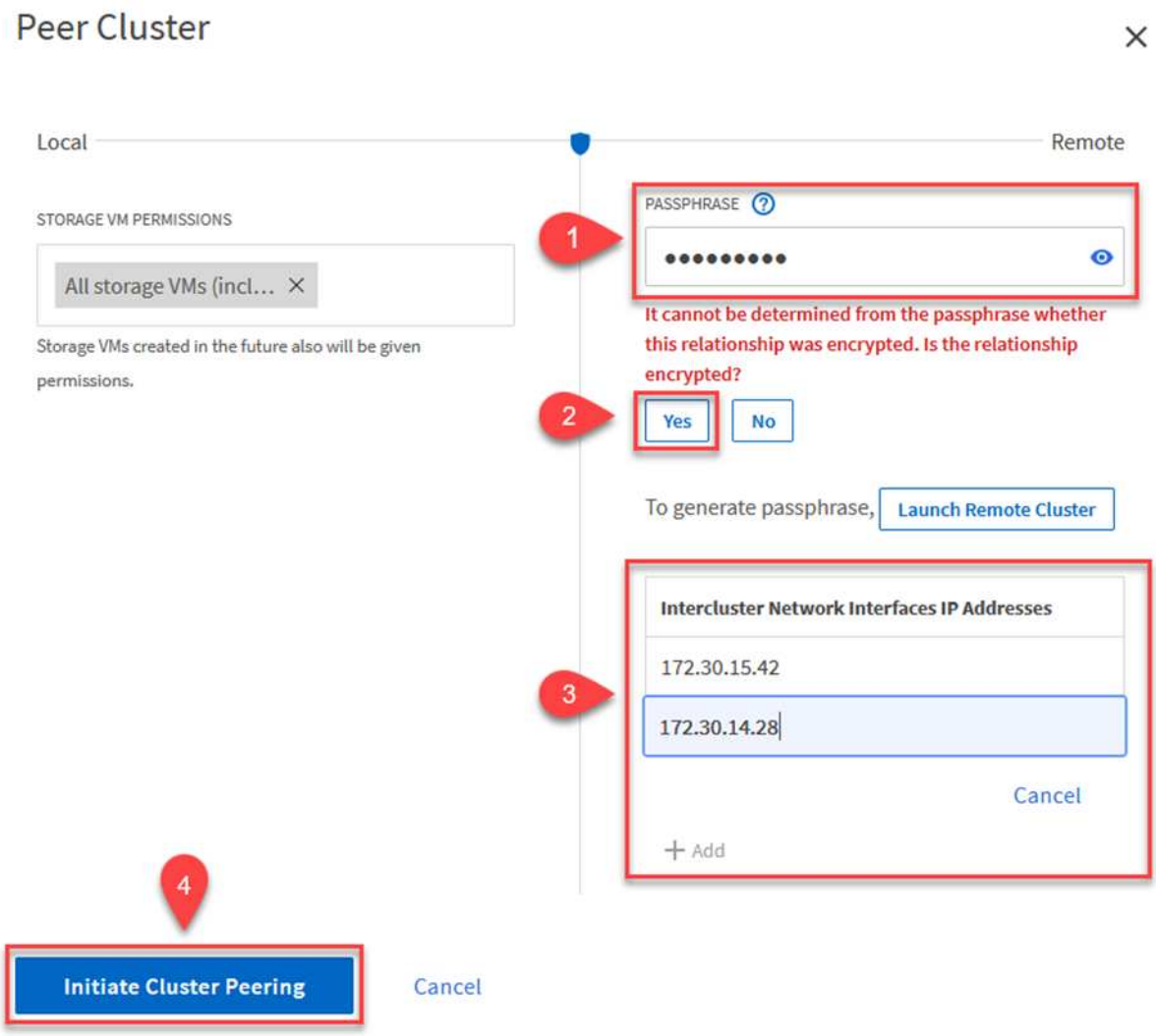
2. 在來源叢集上、您可以使用ONTAP SysSystem Manager或CLI建立叢集對等關係。從「系統管理程式」中、瀏覽至「保護」>「總覽」、然後選取「對等叢集」ONTAP 。



3. 在對等叢集對話方塊中、填寫必要資訊：
   a. 輸入用於在目的地 ONTAP 叢集上建立對等叢集關係的複雜密碼。
   b. 選取「是」以建立加密關係。

c. 輸入目的地 ONTAP 叢集的叢集間 LIF IP 位址。

d. 按一下「初始化叢集對等」以完成程序。



4. 使用下列命令、從目的地 ONTAP 叢集驗證叢集對等關係的狀態：

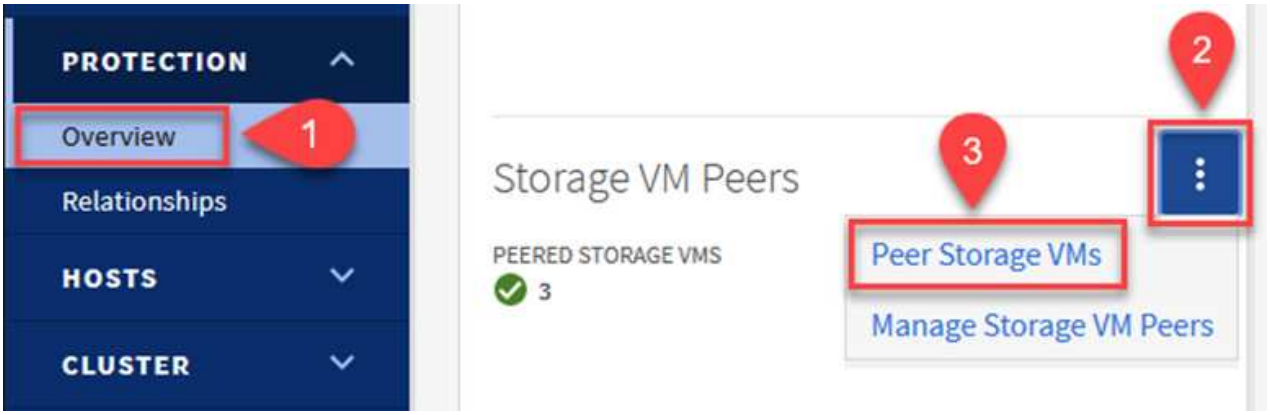
```
ONTAP-Dest::> cluster peer show
```

下一步是在包含SnapMirror關係的磁碟區的目的地與來源儲存虛擬機器之間建立SVM關係。

1. 從目的地 ONTAP 叢集、使用 CLI 中的下列命令建立 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 的物件叢集、接受與ONTAP SysSystem Manager或CLI的對等關係。
3. 從「支援系統管理程式」移至「保護」>「總覽」、然後在「儲存VM對等端點」下選取「對等儲存VM」ONTAP 。



4. 在對等儲存VM對話方塊中、填寫必填欄位：
   - 來源儲存VM
   - 目的地叢集
   - 目的地儲存VM

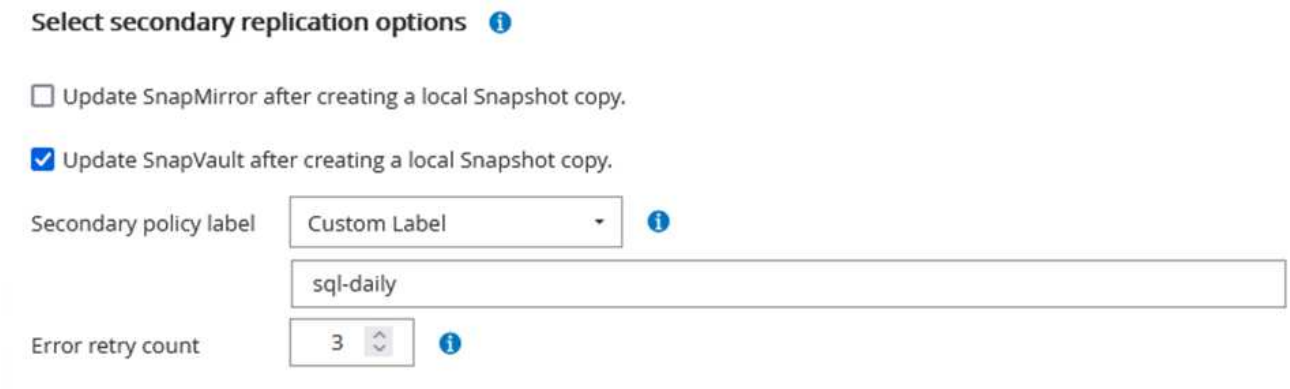
5. 按一下對等儲存VM以完成SVM對等處理程序。

可管理主要儲存系統上以快照複本形式存在的備份保留排程。SnapCenter這是SnapCenter 在建立一套以功能為基礎的原則時所建立的。不管理保留在二線儲存系統上的備份保留原則。SnapCenter這些原則是透過在次要FSX叢集上建立的SnapMirror原則來個別管理、並與與來源Volume處於SnapMirror關係中的目的地磁碟區相關聯。

建立SnapCenter Eshot原則時、您可以選擇指定次要原則標籤、並將其新增至SnapCenter 擷取此備份時所產生之每個Snapshot的SnapMirror標籤。

在二線儲存設備上、這些標籤會符合與目的地Volume相關的原則規則、以強制保留快照。

以下範例顯示SnapMirror標籤、其存在於所有快照上、這些快照是作為每日備份SQL Server資料庫和記錄磁碟區的原則之一。



如需建立SnapCenter SQL Server資料庫的各項功能性原則的詳細資訊、請參閱 "本文檔SnapCenter"。

您必須先建立SnapMirror原則、其中規定要保留的快照複本數量。

1. 在FSX叢集上建立SnapMirror原則。

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

2. 使用SnapMirror標籤將規則新增至原則、這些標籤符合SnapCenter 在《保護原則》中指定的次要原則標籤。

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

下列指令碼提供可新增至原則的規則範例：

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

針對每個SnapMirror標籤和要保留的快照數量（保留期間）建立其他規則。

建立目的地**Volume**

若要在 ONTAP 上建立目的地磁碟區、以接收來源磁碟區的快照複本、請在目的地 ONTAP 叢集上執行下列命令：

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

在來源與目的地磁碟區之間建立**SnapMirror**關係

若要在來源和目的地磁碟區之間建立 SnapMirror 關係、請在目的地 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。此程序會啟動從來源磁碟區產生的新快照、並將其複製到目的地磁碟區。

若要建立 Volume 、請在目的地 ONTAP 叢集上執行下列命令：

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

設定 **VMware vSphere** 的 **SnapCenter** 外掛程式

安裝後、即可從 vCenter Server Appliance Management 介面存取 SnapCenter Plug-in for VMware vSphere 。選擇控制閥將管理安裝在 ESXi 主機上且包含 Windows 和 Linux VM 的 NFS 資料存放區備份。

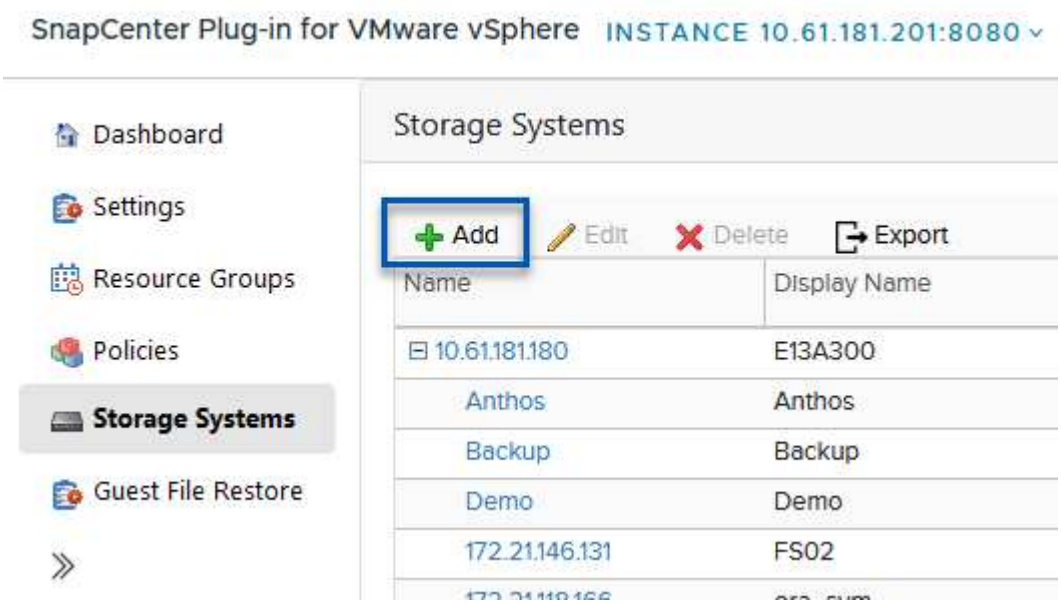
檢閱 "資料保護工作流程" 選擇控制閥文件的章節、以取得設定備份所需步驟的詳細資訊。

若要設定虛擬機器和資料存放區的備份、必須從外掛程式介面完成下列步驟。

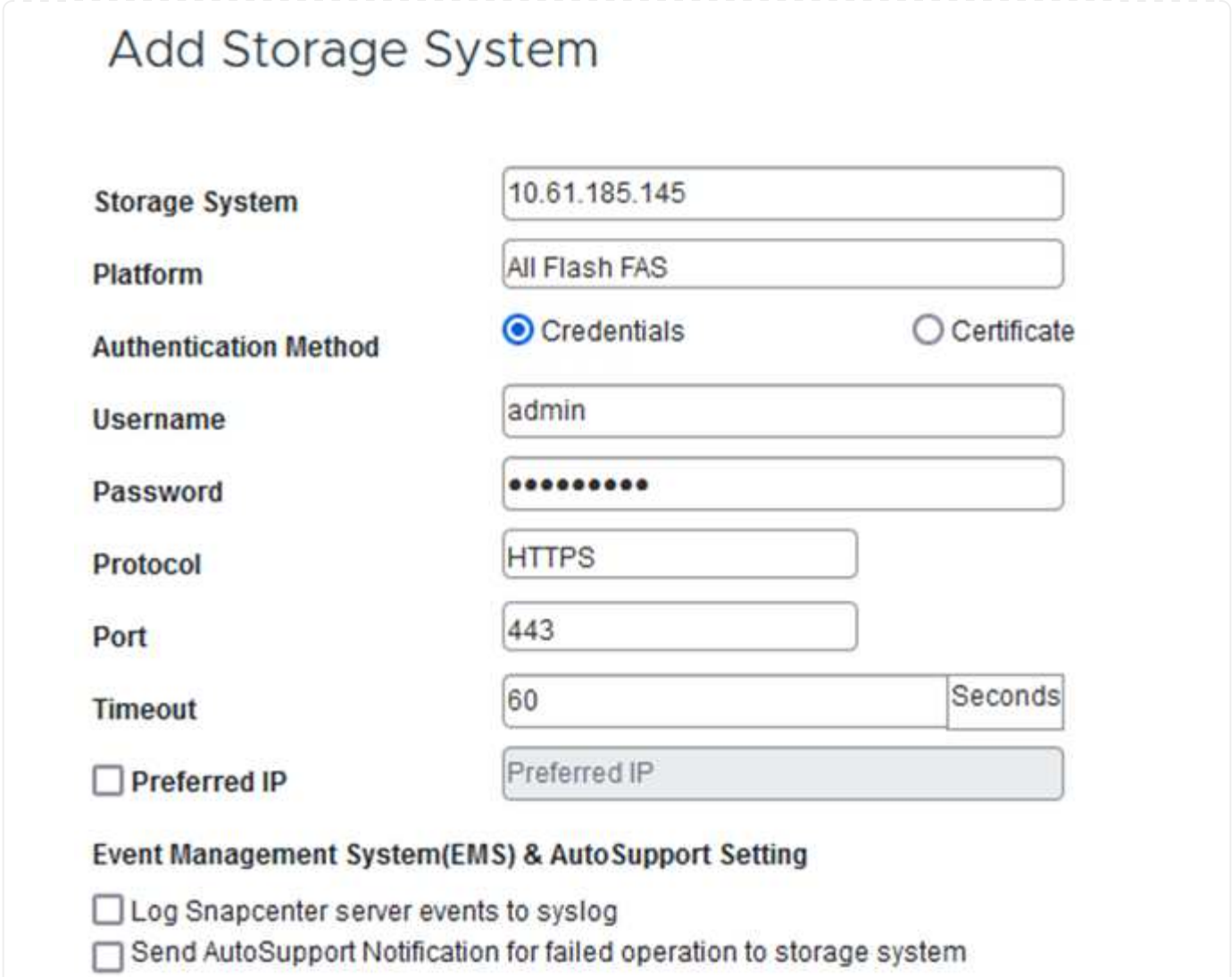
Discovery ONTAP 儲存系統

探索用於主要和次要備份的 ONTAP 儲存叢集。

1. 在 SnapCenter Plug-in for VMware vSphere 中、瀏覽左側功能表中的 * 儲存系統 * 、然後按一下 * 新增 * 按鈕。



2. 填寫主要 ONTAP 儲存系統的認證資料與平台類型、然後按一下 * 新增 * 。



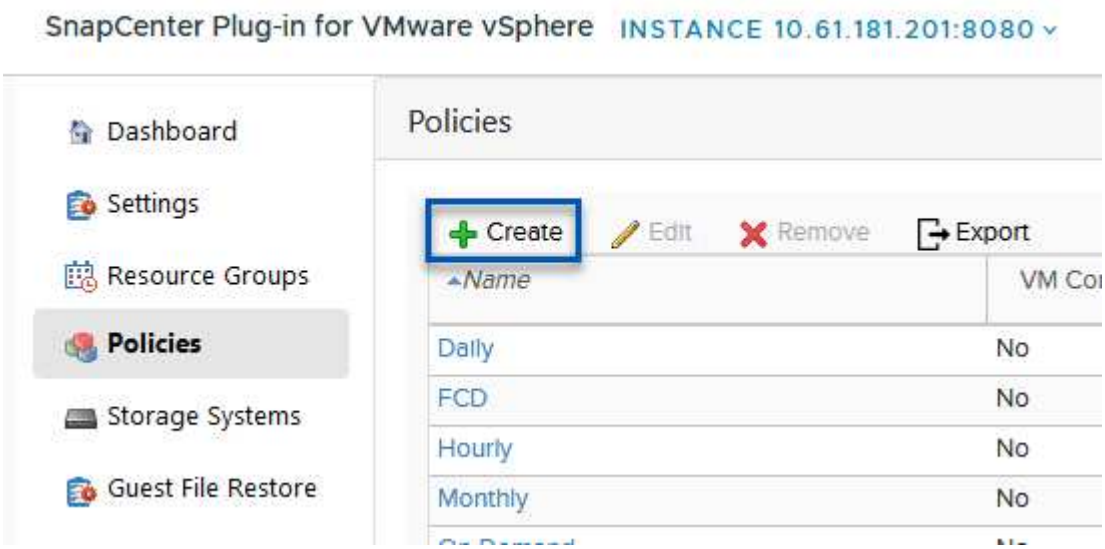
3. 對次 ONTAP 儲存系統重複此程序。

原則指定由選擇控制閥管理之備份的保留期間、頻率和複寫選項。

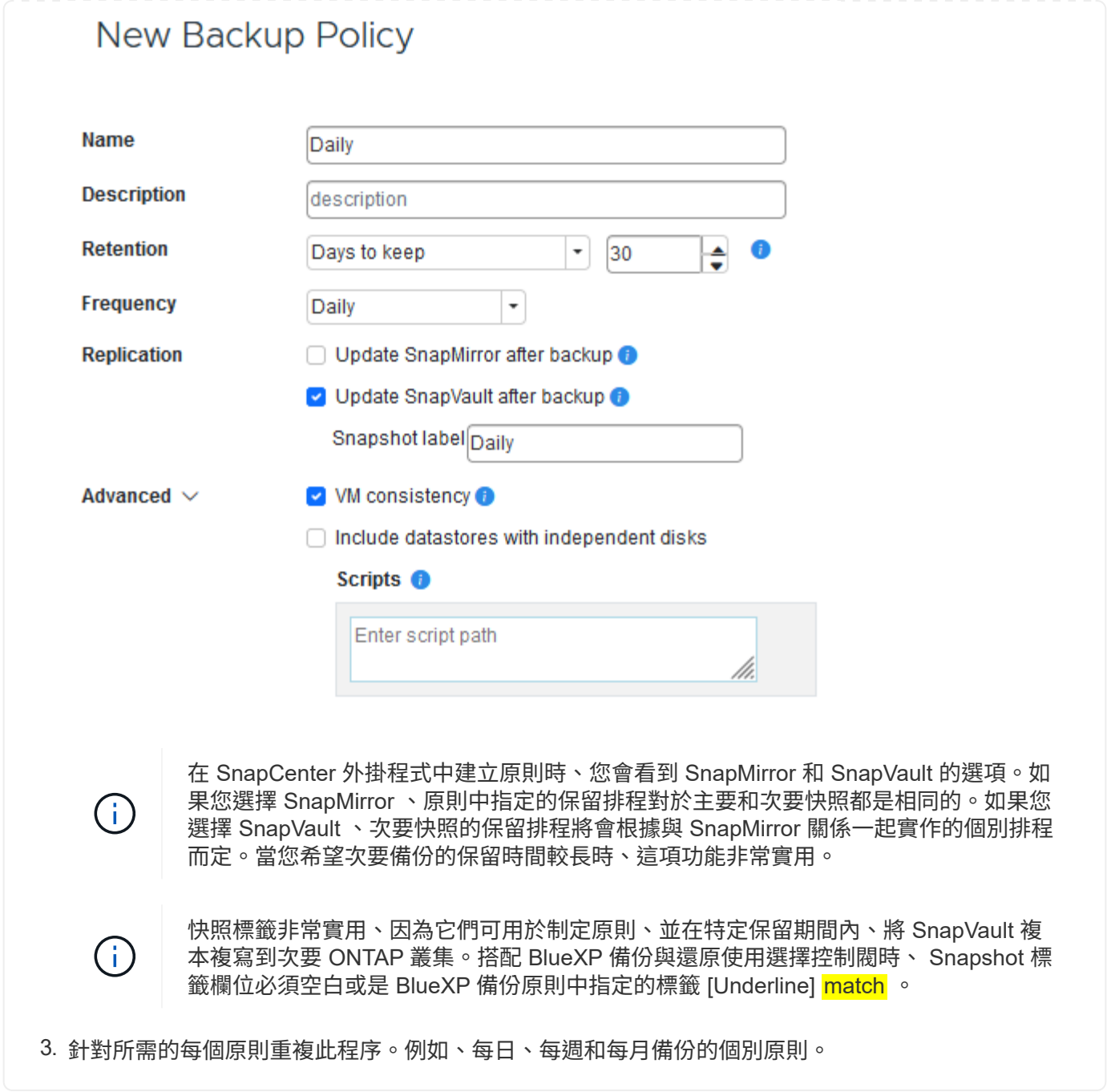
檢閱 "為VM和資料存放區建立備份原則" 如需詳細資訊、請參閱文件的一節。

若要建立備份原則、請完成下列步驟：

1. 在 SnapCenter Plug-in for VMware vSphere 中、瀏覽左側功能表中的 * 原則 * 、然後按一下 * 建立 * 按鈕。



2. 指定原則、保留期間、頻率和複寫選項、以及快照標籤的名稱。



在 SnapCenter 外掛程式中建立原則時、您會看到 SnapMirror 和 SnapVault 的選項。如果您選擇 SnapMirror 、原則中指定的保留排程對於主要和次要快照都是相同的。如果您選擇 SnapVault 、次要快照的保留排程將會根據與 SnapMirror 關係一起實作的個別排程而定。當您希望次要備份的保留時間較長時、這項功能非常實用。

快照標籤非常實用、因為它們可用於制定原則、並在特定保留期間內、將 SnapVault 複本複寫到次要 ONTAP 叢集。搭配 BlueXP 備份與還原使用選擇控制閥時、 Snapshot 標籤欄位必須空白或是 BlueXP 備份原則中指定的標籤 [Underline] match 。

3. 針對所需的每個原則重複此程序。例如、每日、每週和每月備份的個別原則。

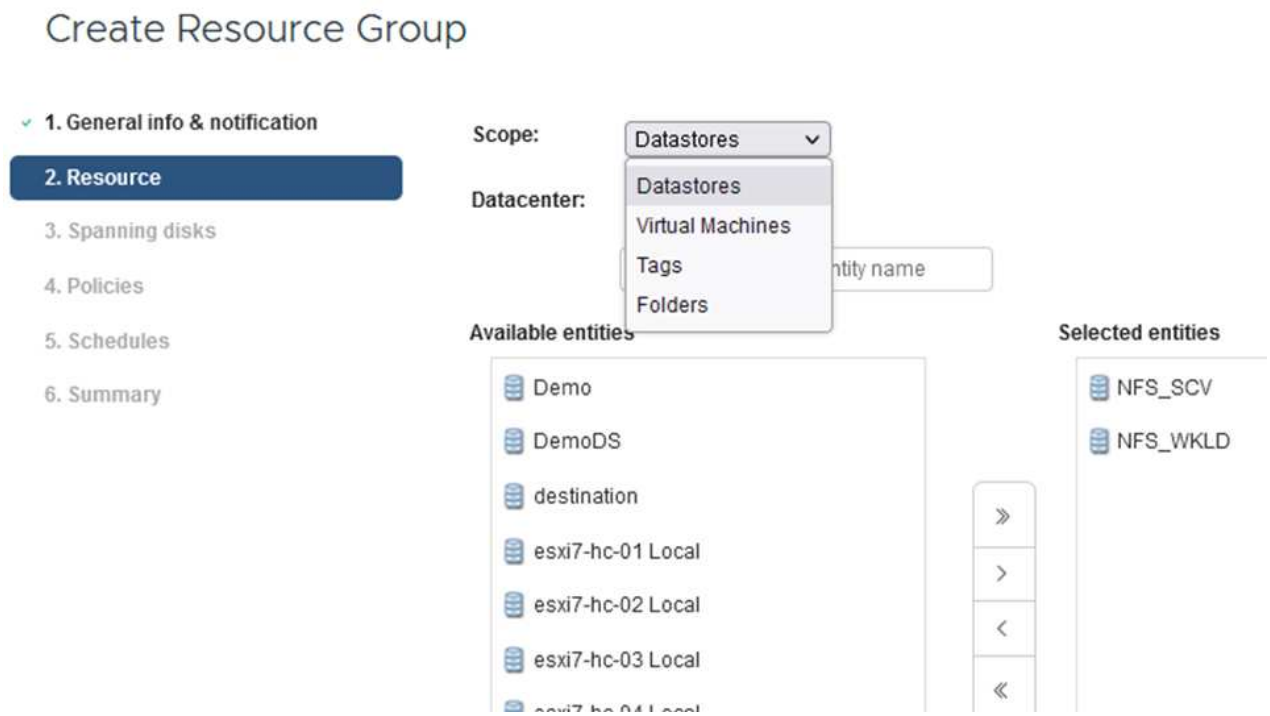
資源群組包含要納入備份工作的資料存放區和虛擬機器、以及相關的原則和備份排程。

檢閱 "建立資源群組" 如需詳細資訊、請參閱文件的一節。

若要建立資源群組、請完成下列步驟。

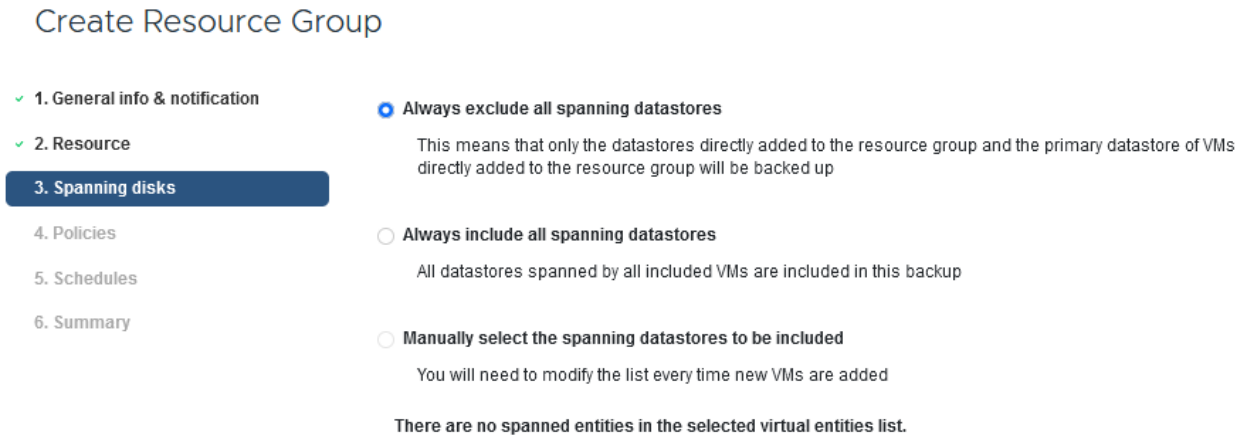
1. 在 SnapCenter Plug-in for VMware vSphere 中、瀏覽左側功能表中的 * 資源群組 * 、然後按一下 * 建立 * 按鈕。

2. 在「建立資源群組」精靈中、輸入群組的名稱和說明、以及接收通知所需的資訊。按一下 * 下一步 *
3. 在下一頁選取要包含在備份工作中的資料存放區和虛擬機器、然後按一下 * 下一步 * 。



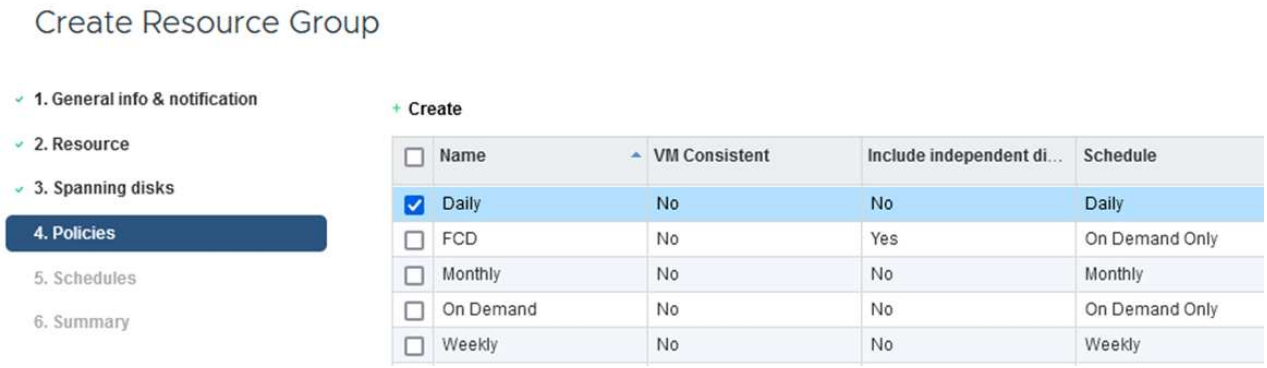
您可以選擇特定 VM 或整個資料存放區。無論您選擇哪種類型、都會備份整個磁碟區（和資料存放區）、因為備份是建立基礎磁碟區快照的結果。在大多數情況下、選擇整個資料存放區最簡單。不過、如果您希望在還原時限制可用 VM 的清單、則只能選擇一個子集進行備份。

4. 選擇多個資料存放區上的 VMDK 虛擬機器跨距資料存放區選項、然後按一下 * 下一步 * 。



BlueXP 備份與還原目前不支援使用跨多個資料存放區的 VMDK 來備份 VM 。

5. 在下一頁中、選取將與資源群組相關聯的原則、然後按一下 * 下一步 * 。



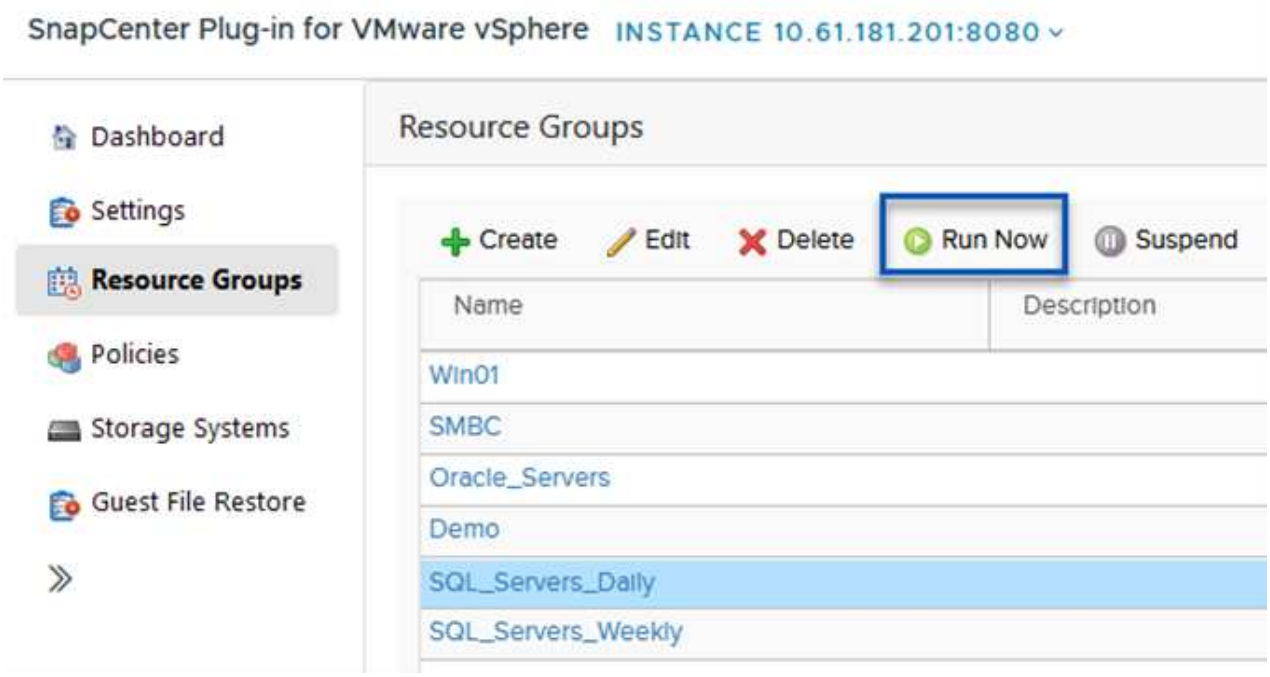
使用 BlueXP 備份和恢復將選擇控制閥管理的快照備份到物件儲存時、每個資源群組只能與單一原則相關聯。

6. 選取一個排程、以決定備份的執行時間。按一下 * 下一步 * 。

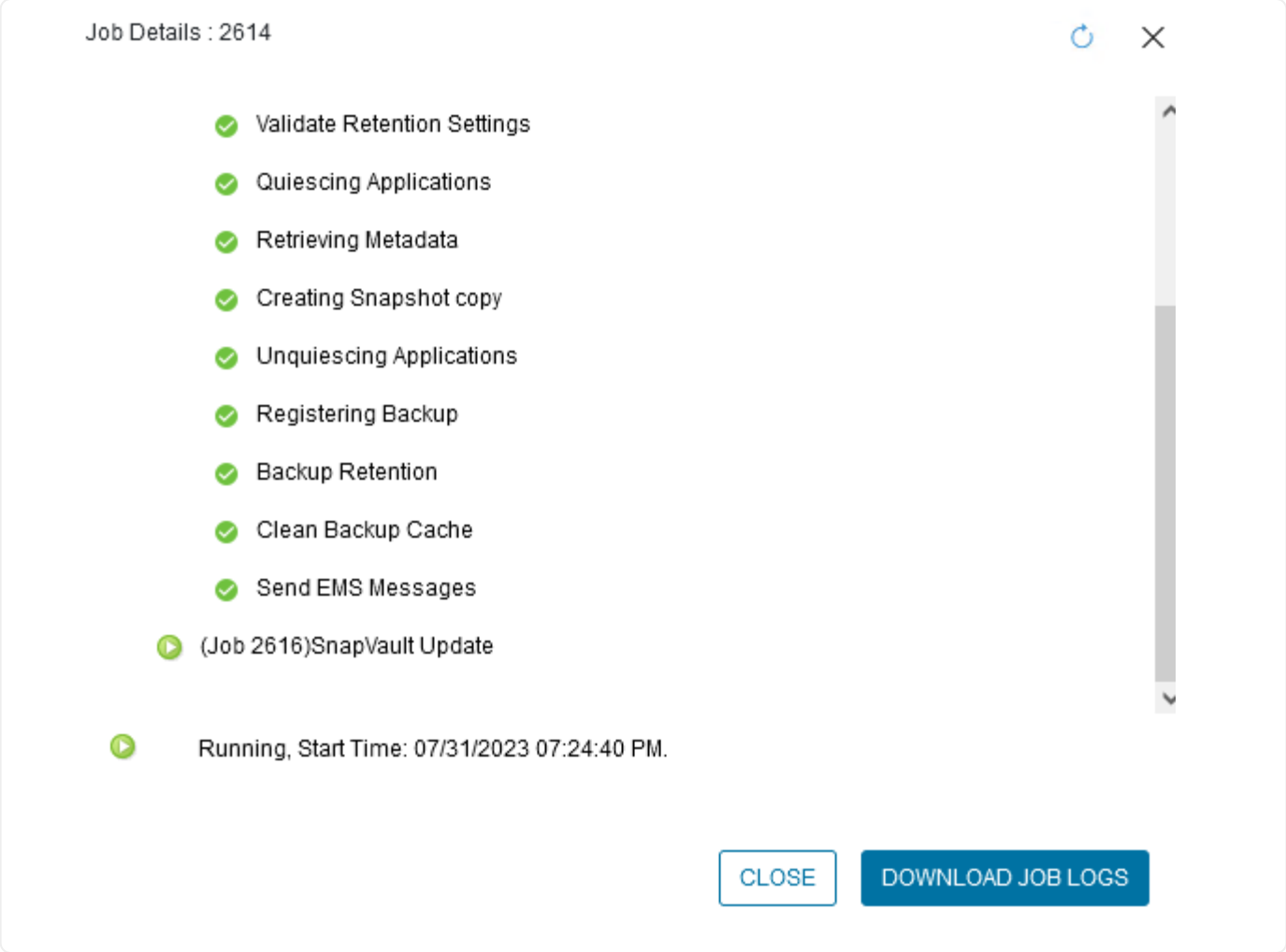
7. 最後、請檢閱摘要頁面、然後按 * 完成 * 完成資源群組的建立。

在此最後一個步驟中、請執行備份工作並監控其進度。至少必須在選擇控制閥中成功完成一個備份工作、才能從 BlueXP 備份與恢復中找到資源。

1. 在 SnapCenter Plug-in for VMware vSphere 中、瀏覽左側功能表中的 * 資源群組 * 。
2. 若要啟動備份工作、請選取所需的資源群組、然後按一下 * 立即執行 * 按鈕。



3. 若要監控備份工作、請瀏覽左側功能表上的 * 儀表板 * 。在 * 最近的工作活動 * 下、按一下工作 ID 號碼以監控工作進度。



在 **BlueXP** 備份與還原中設定備份至物件儲存設備

為了讓 BlueXP 有效管理資料基礎架構、必須先安裝 Connector 。Connector 會執行探索資源和管理資料作業所涉及的動作。

如需 BlueXP Connector 的詳細資訊、請參閱 "深入瞭解連接器" 在 BlueXP 文件中。

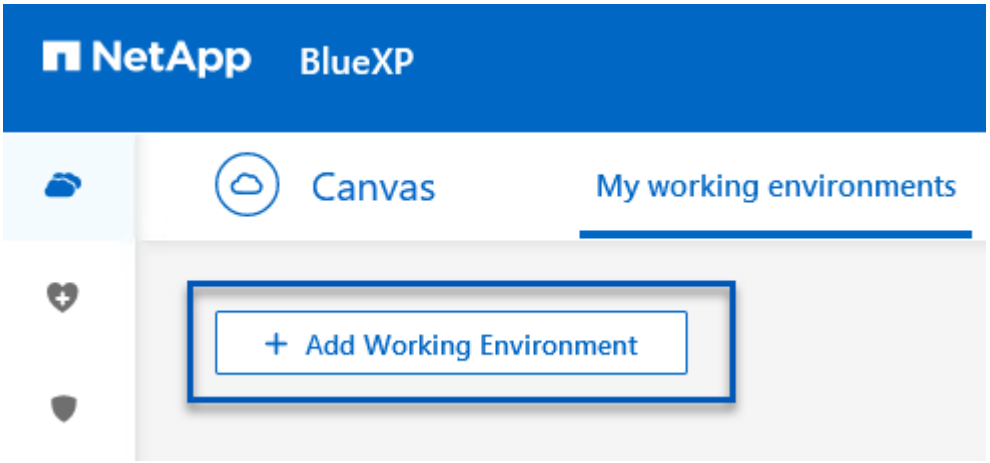
安裝用於雲端供應商的連接器後、即可從 Canvas 檢視物件儲存設備的圖形呈現。

若要設定 BlueXP 備份與恢復、以備份由內部部署選擇控制閥管理的資料、請完成下列步驟：

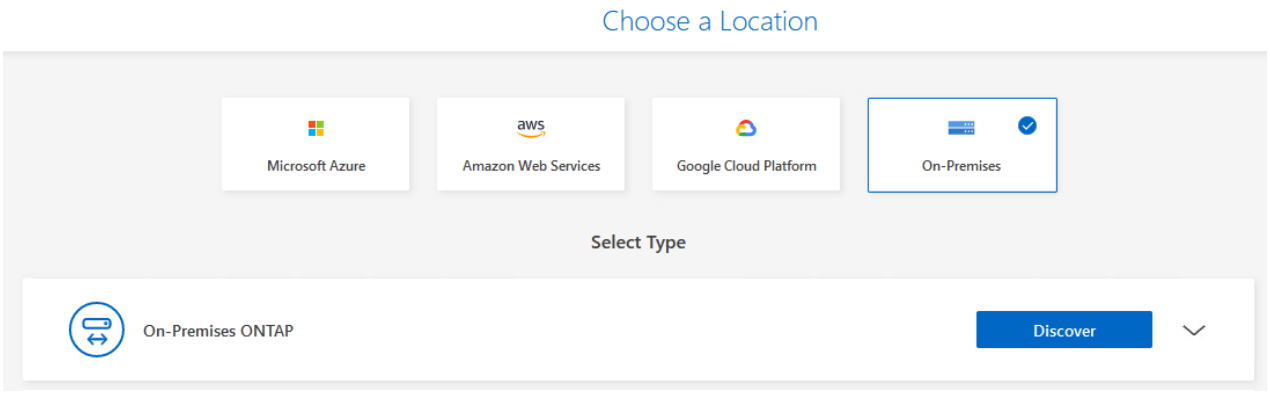
將工作環境新增至 **Canvas**

第一步是將內部部署 ONTAP 儲存系統新增至 BlueXP

1. 從 Canvas 選取 * 新增工作環境 * 開始。



2. 從選擇的位置選擇 * 內部部署 * 、然後按一下 * 探索 * 按鈕。



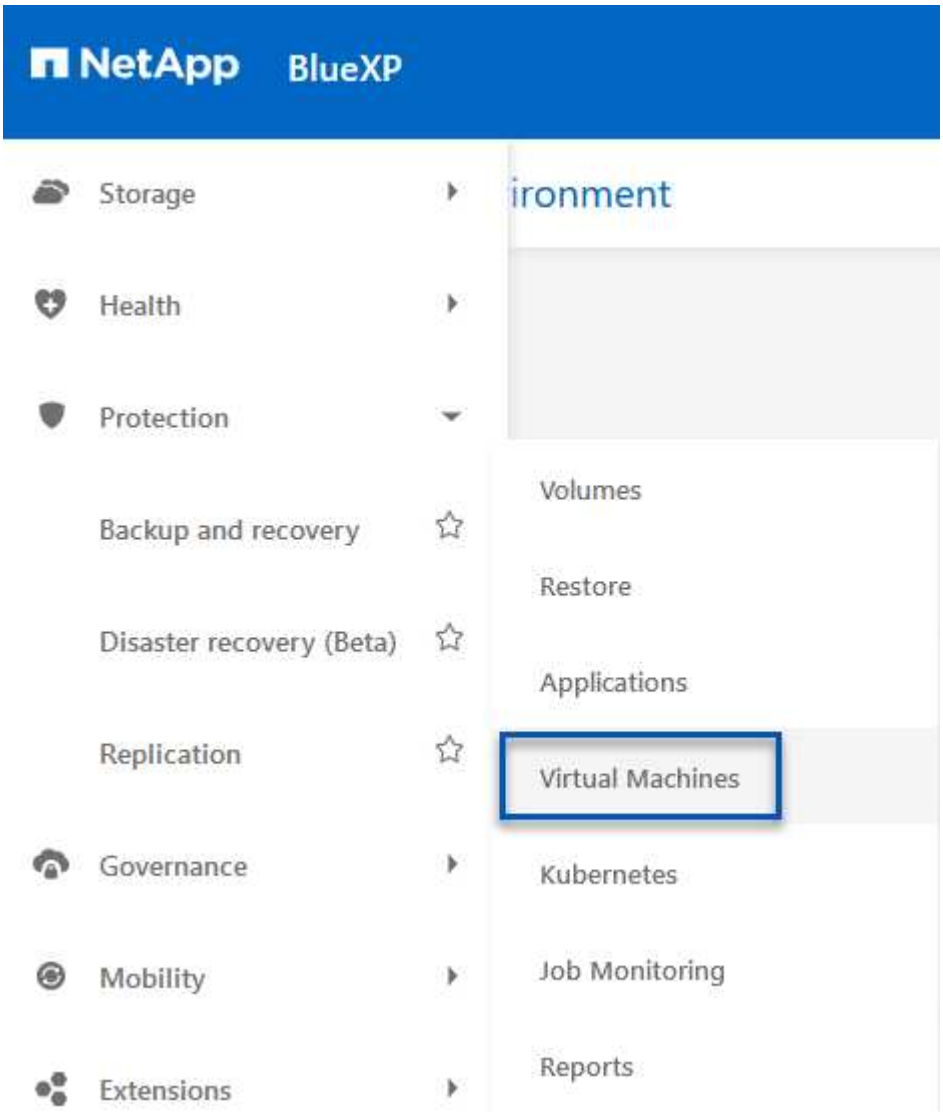
3. 填寫 ONTAP 儲存系統的認證資料、然後按一下「 * 探索 * 」按鈕以新增工作環境。


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

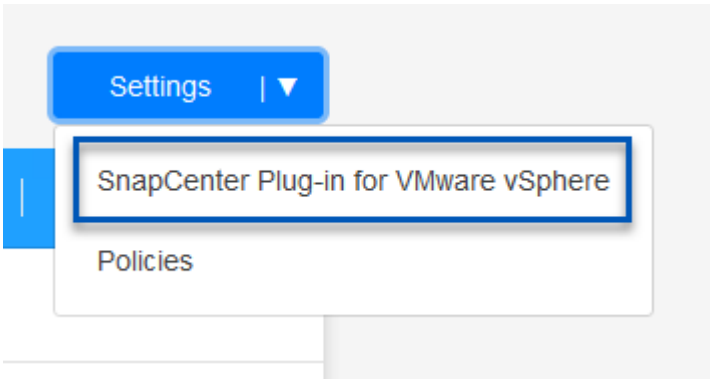
探索內部部署的選擇控制閥應用裝置和 **vCenter**

若要探索內部部署資料存放區和虛擬機器資源、請新增選擇控制閥資料代理程式的資訊、以及 vCenter 管理應用裝置的認證。

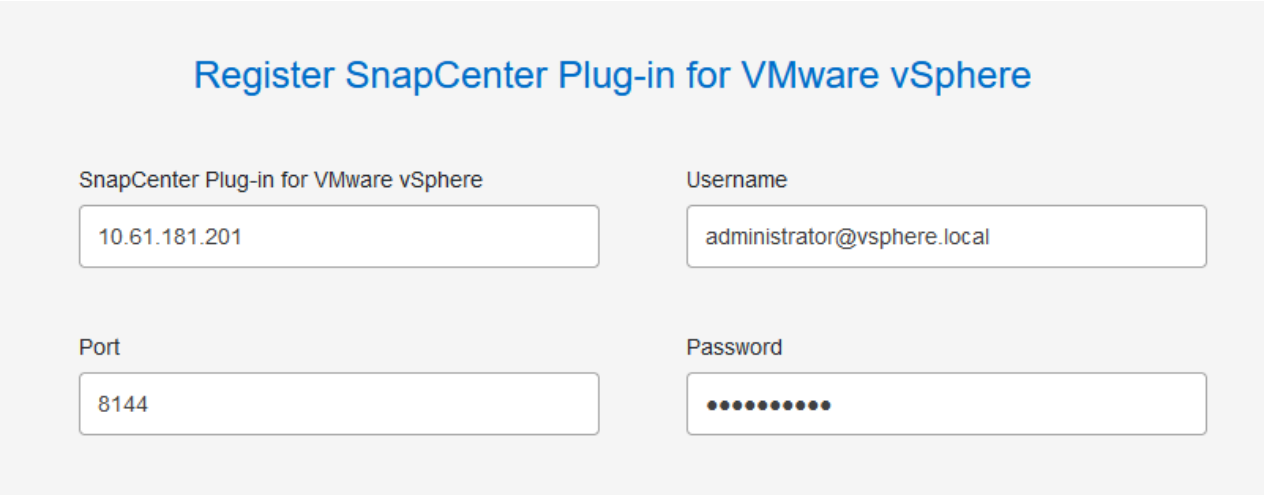
1. 從 BlueXP 左側功能表選擇 * 保護 > 備份與還原 > 虛擬機器 *



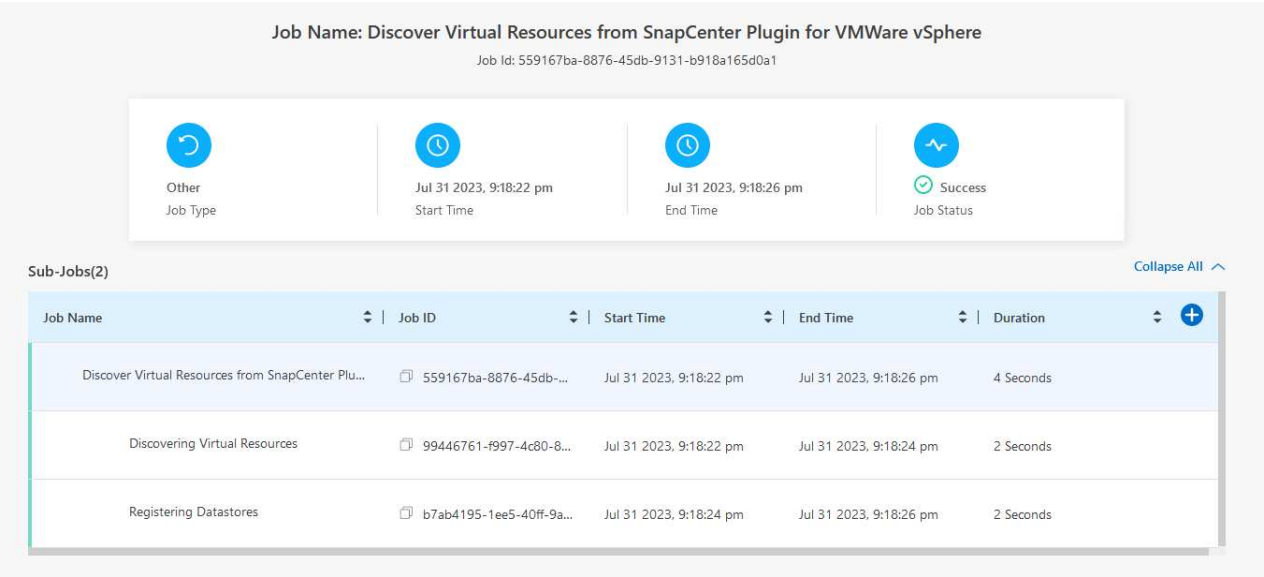
2. 從虛擬機器主畫面存取 * 設定 * 下拉式功能表、然後選取 * 適用於 VMware vSphere 的 SnapCenter 外掛程式 * 。



3. 按一下 * 註冊 * 按鈕、然後輸入 SnapCenter 外掛應用裝置的 IP 位址和連接埠編號、以及 vCenter 管理應用裝置的使用者名稱和密碼。按一下 * 註冊 * 按鈕開始探索程序。



4. 工作進度可從「工作監控」標籤進行監控。



5. 完成探索後、您將能夠檢視所有探索到的選擇控制閥設備中的資料存放區和虛擬機器。

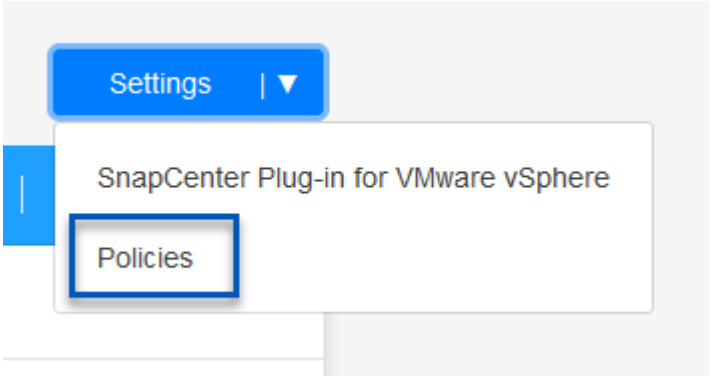
   影像：： bxp-SCV 混合式 -23.png[檢視可用資源]

建立 **BlueXP** 備份原則

在 BlueXP 虛擬機器的備份與還原中、建立原則以指定保留期間、備份來源和歸檔原則。

如需建立原則的詳細資訊、請參閱 "建立備份資料存放區的原則"。

1. 從 BlueXP 虛擬機器備份與還原主頁、存取 * 設定 * 下拉式功能表、然後選取 * 原則 * 。



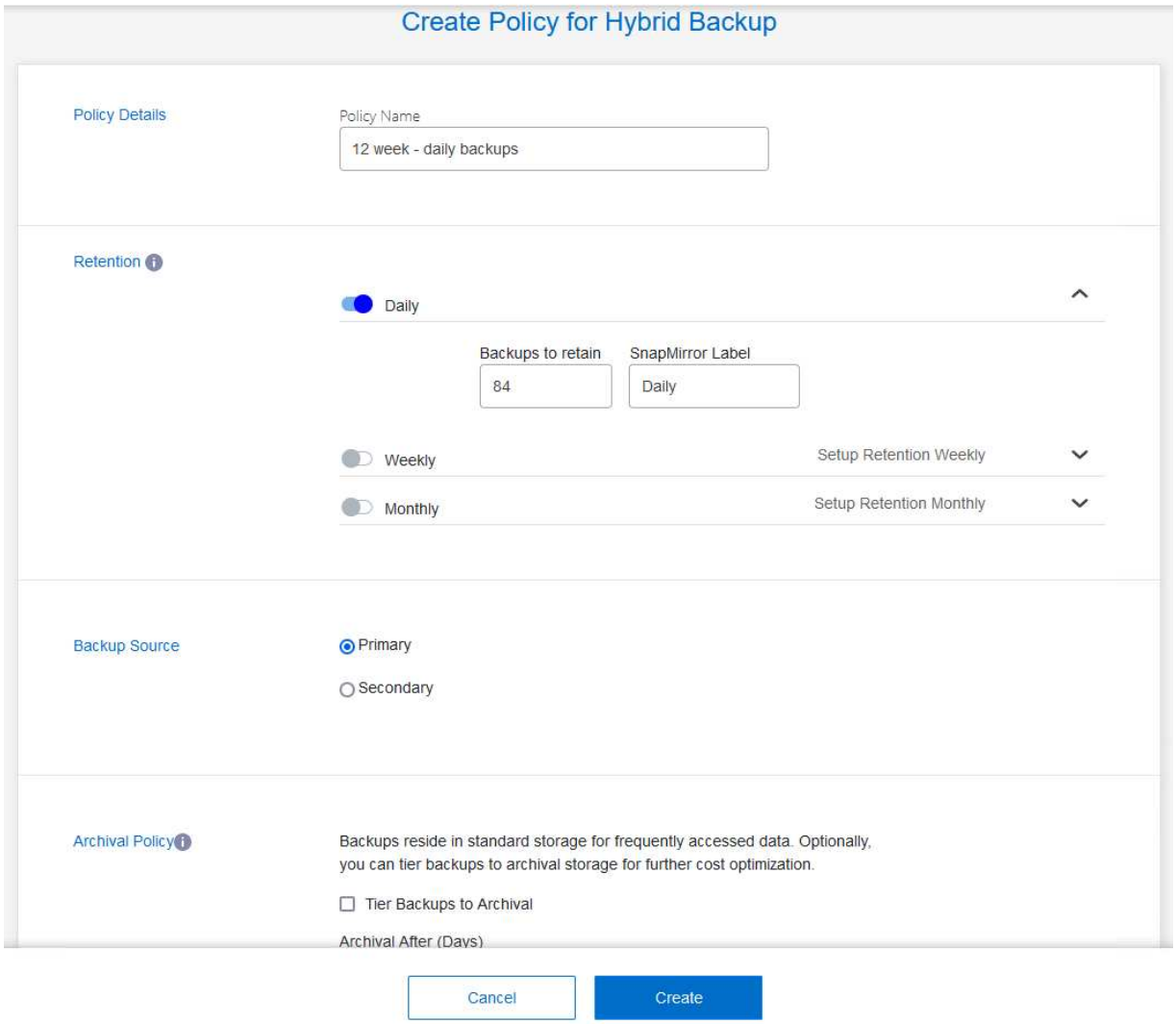
2. 按一下 * 建立原則 * 以存取 * 建立混合式備份原則 * 視窗。

   a. 新增原則名稱

   b. 選取所需的保留期間

   c. 選擇備份來源為主要或次要內部部署 ONTAP 儲存系統

   d. 您也可以選擇指定備份層級到歸檔儲存設備的時間期限、以節省額外成本。



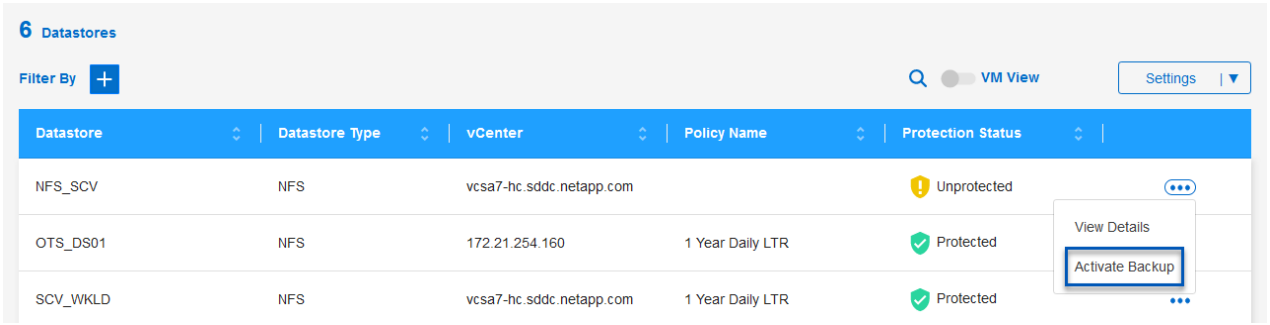
此處輸入的 SnapMirror 標籤用於識別要套用原則的備份。標籤名稱必須與對應的內部部署選擇控制閥政策中的標籤名稱相符。

3. 按一下 * 建立 * 以完成原則建立。

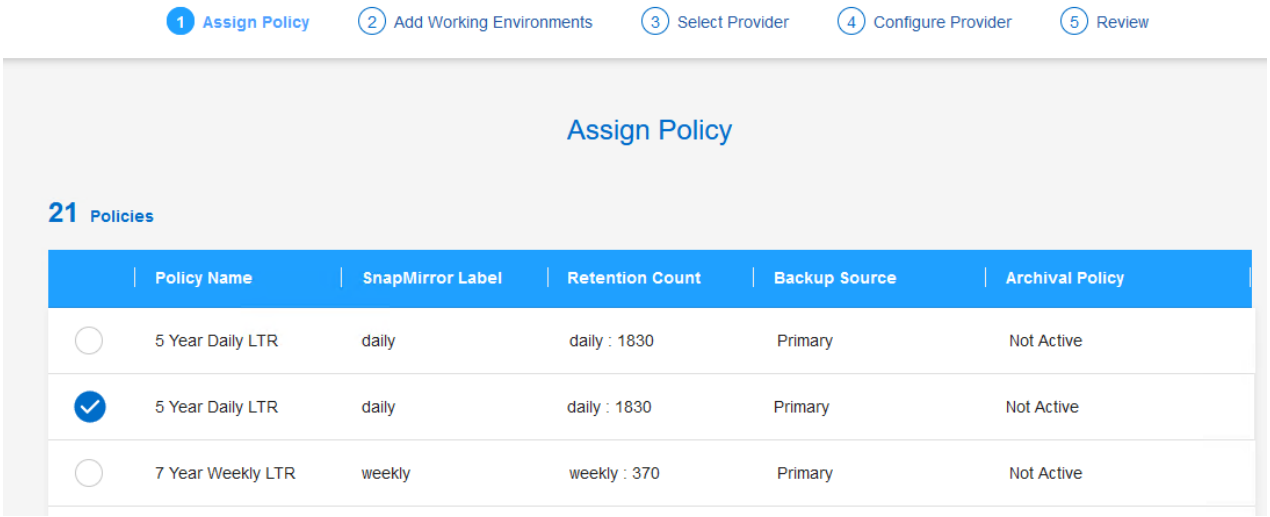
最後一步是啟動個別資料存放區和虛擬機器的資料保護。下列步驟概述如何啟動備份至 AWS 。

如需詳細資訊、請參閱 "將資料存放區備份至Amazon Web Services"。

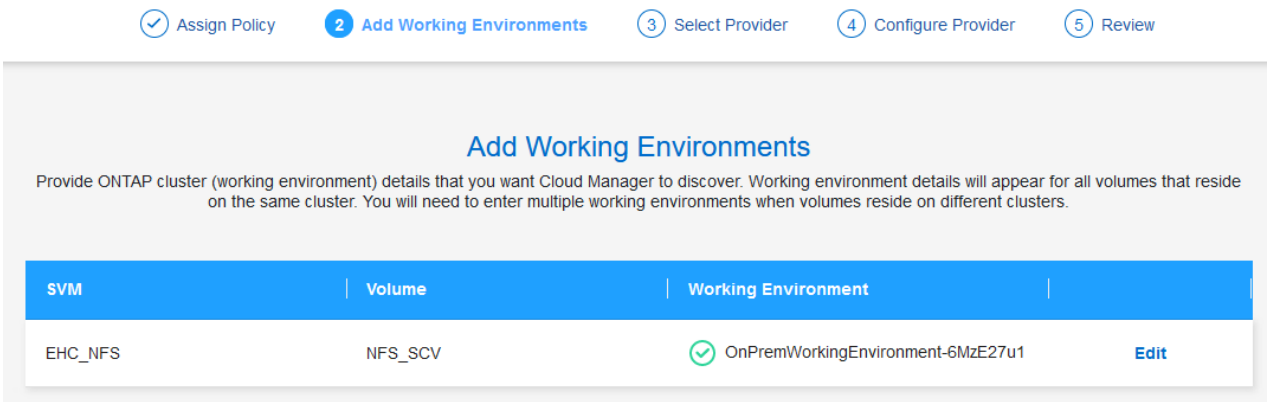
1. 從 BlueXP 虛擬機器備份與還原主頁、存取要備份的資料存放區的設定下拉式清單、然後選取 * 啟動備份 * 。



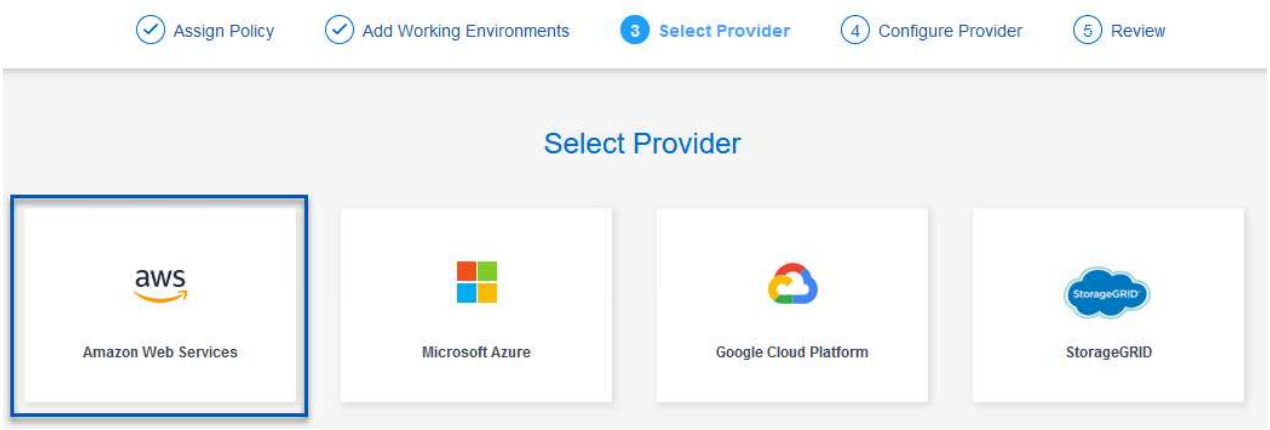
2. 指派用於資料保護作業的原則、然後按一下 * 下一步 * 。



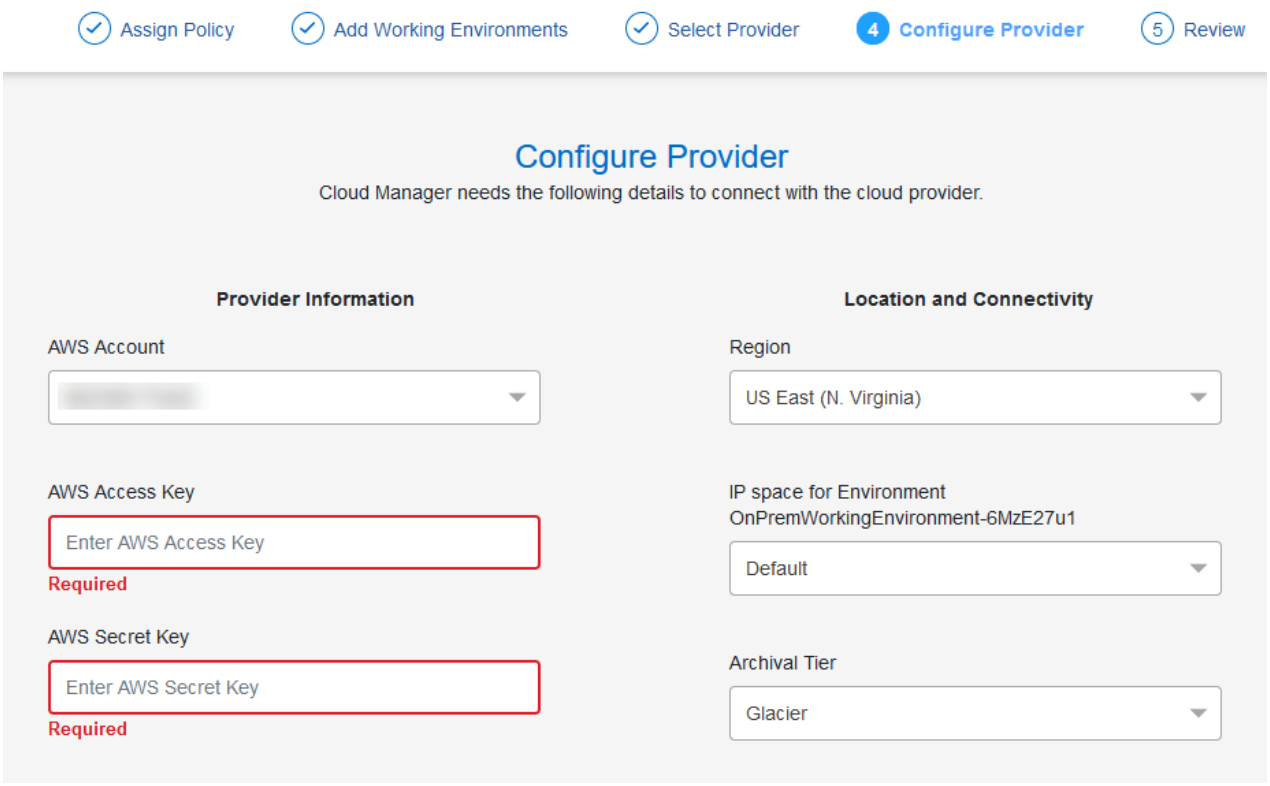
3. 在「 * 新增工作環境 * 」頁面上、如果先前發現工作環境、則應顯示具有核取記號的資料存放區和工作環境。如果先前尚未發現工作環境、您可以在此處新增。按一下 * 下一步 * 繼續。



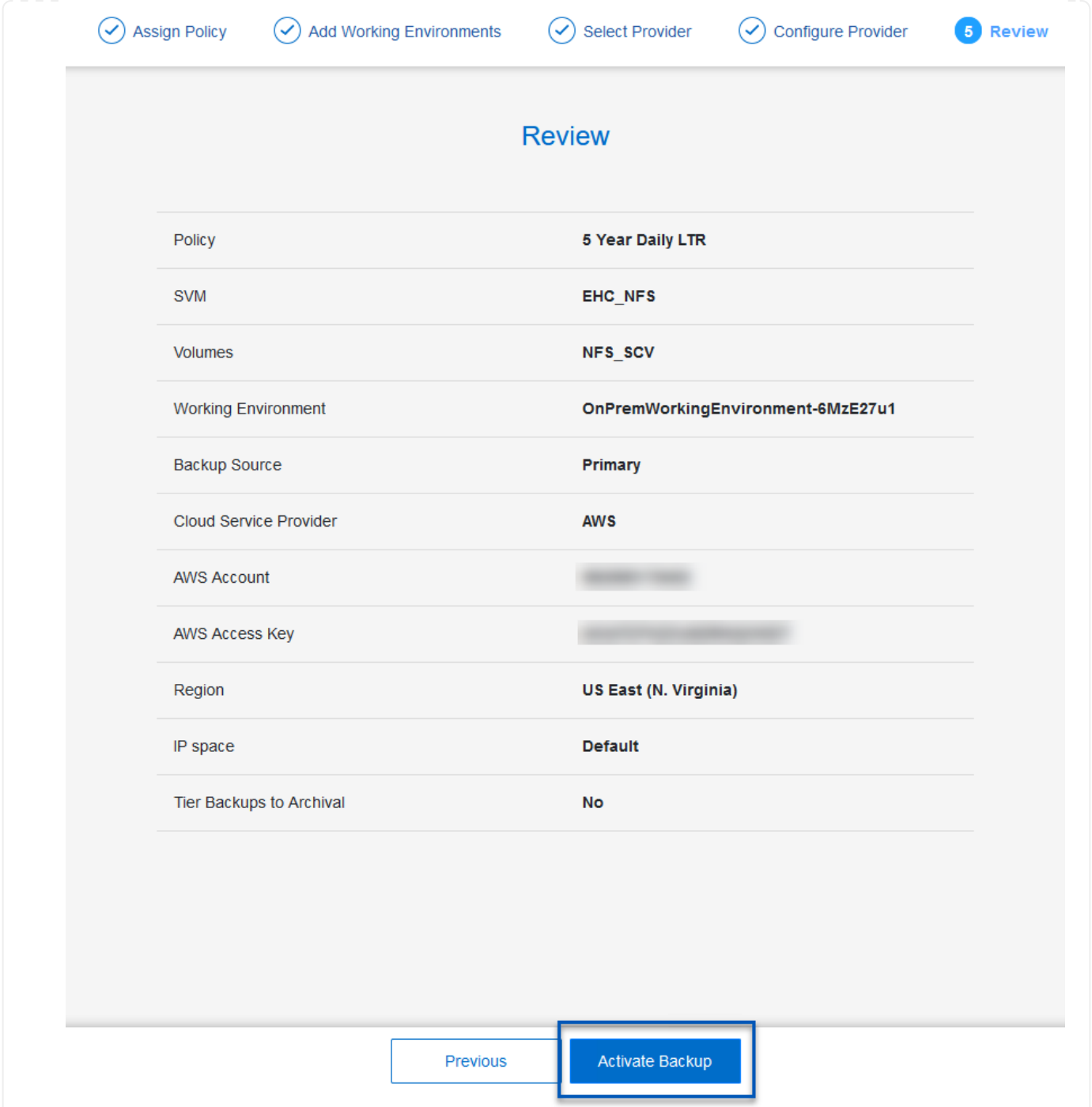
4. 在「 * 選擇供應商 * 」頁面上、按一下 AWS 、然後按一下「 * 下一步 * 」按鈕繼續。



5. 填寫 AWS 的供應商特定認證資訊、包括使用的 AWS 存取金鑰和秘密金鑰、區域和歸檔層。此外、請為內部部署 ONTAP 儲存系統選取 ONTAP IP 空間。按一下 * 下一步 * 。



6. 最後、請檢閱備份工作詳細資料、然後按一下 * 啟動備份 * 按鈕、以啟動資料存放區的資料保護。



此時資料傳輸可能不會立即開始。BlueXP 每小時會掃描任何未處理的快照、然後將其傳輸至物件儲存設備。

在資料遺失的情況下還原虛擬機器

確保資料安全只是全方位資料保護的一個層面。同樣重要的是、在資料遺失或勒索軟體攻擊時、能夠從任何位置迅速還原資料。這項功能對於維持無縫業務營運和達成恢復點目標至關重要。

NetApp 提供高度適應的 3-2-1 策略、可針對主要、次要及物件儲存位置的保留排程提供自訂控制。這項策略提供彈性、可針對特定需求量身打造資料保護方法。

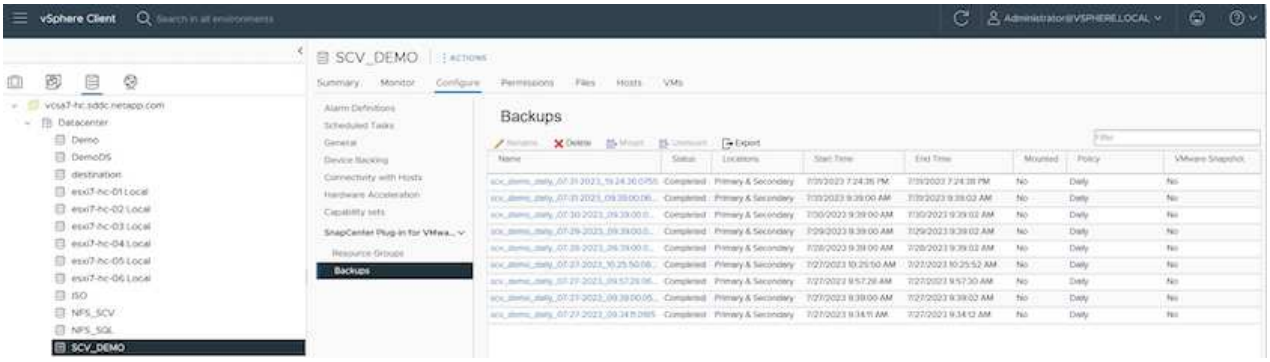
本節概述 SnapCenter Plug-in for VMware vSphere 的資料還原程序、以及適用於虛擬機器的 BlueXP 備份與還原程序。

從適用於 **VMware vSphere** 的 **SnapCenter** 外掛程式還原虛擬機器

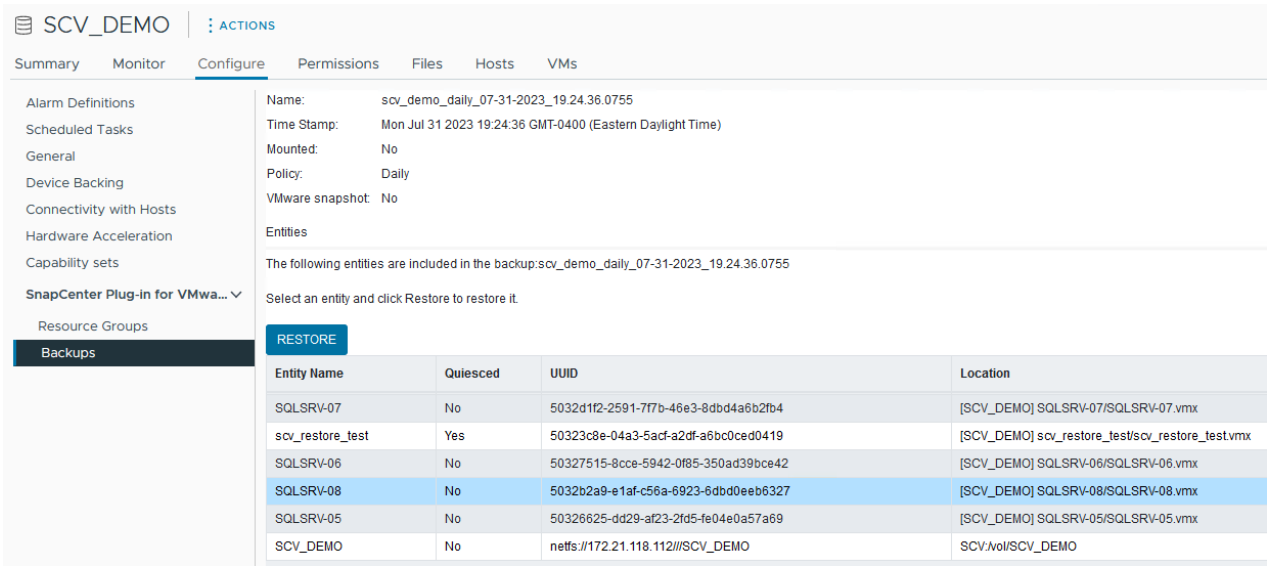
針對此解決方案、虛擬機器已還原至原始位置和其他位置。本解決方案並未涵蓋選擇控制閥資料恢復功能的所有層面。如需所有選擇控制閥必須提供的詳細資訊、請參閱 "從備份還原VM" 請參閱產品文件。

請完成下列步驟、從主要或次要儲存設備還原虛擬機器。

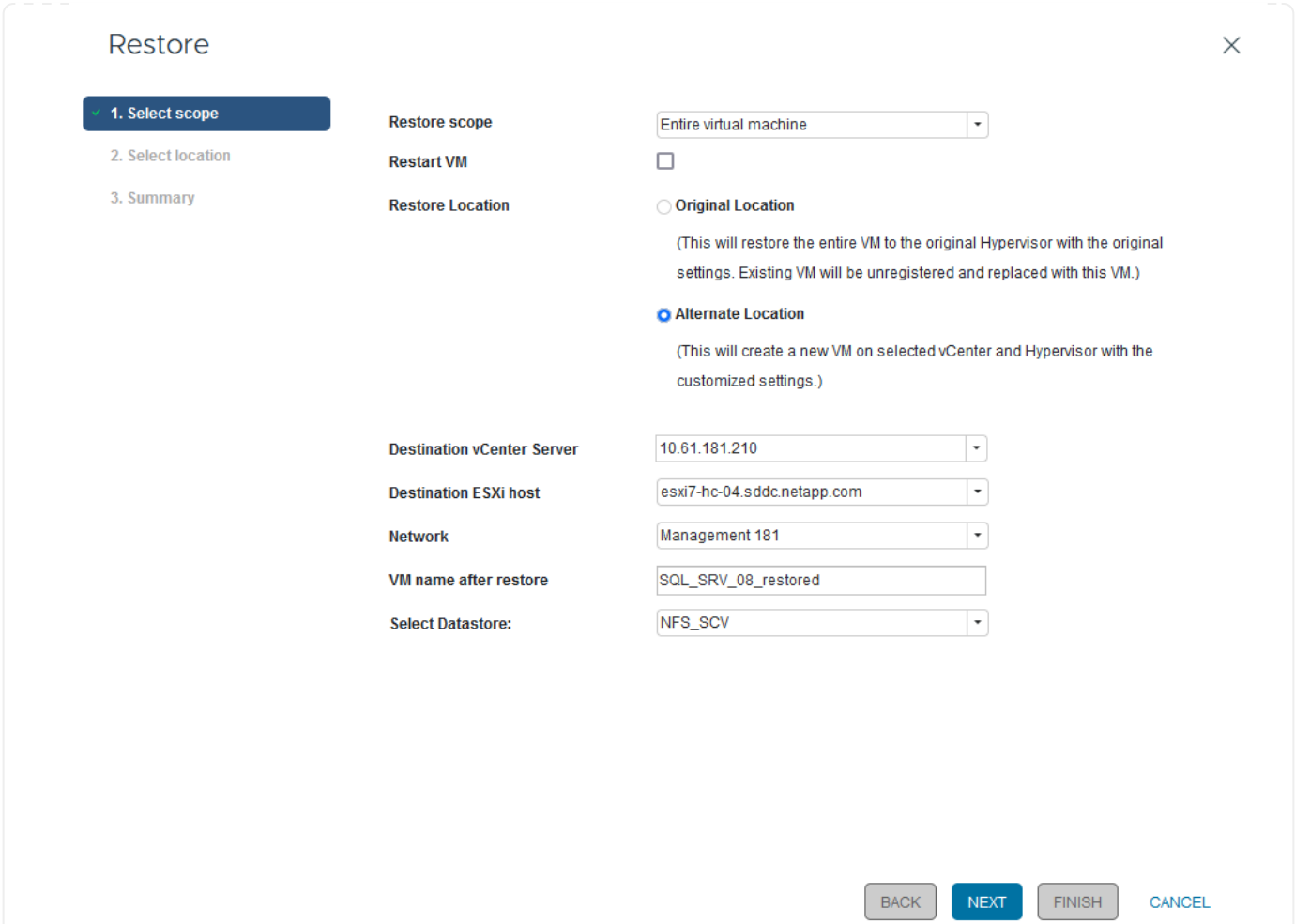
1. 從 vCenter 用戶端瀏覽至 * 清查 > Storage* 、然後按一下包含您要還原之虛擬機器的資料存放區。
2. 從 * 組態 * 標籤按一下 * 備份 * 以存取可用備份清單。



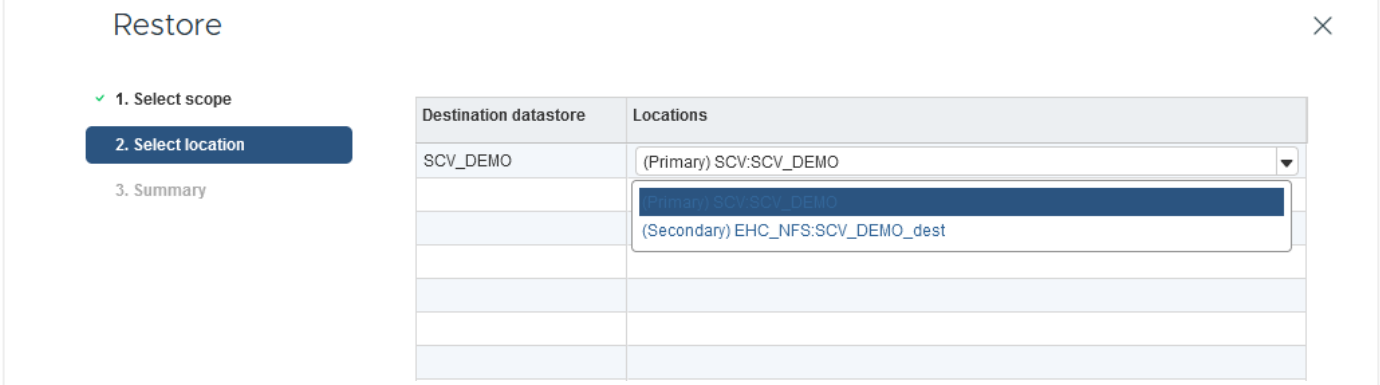
3. 按一下備份以存取虛擬機器清單、然後選取要還原的虛擬機器。按一下 * 還原 * 。



4. 從還原精靈中、選取以還原整個虛擬機器或特定 VMDK 。選取以安裝至原始位置或替代位置、在還原後提供 VM 名稱、以及目的地資料存放區。單擊 * 下一步 * 。



5. 選擇從主要或次要儲存位置進行備份。



6. 最後、檢閱備份工作摘要、然後按一下「完成」以開始還原程序。

從 **BlueXP** 備份還原虛擬機器、並針對虛擬機器進行還原

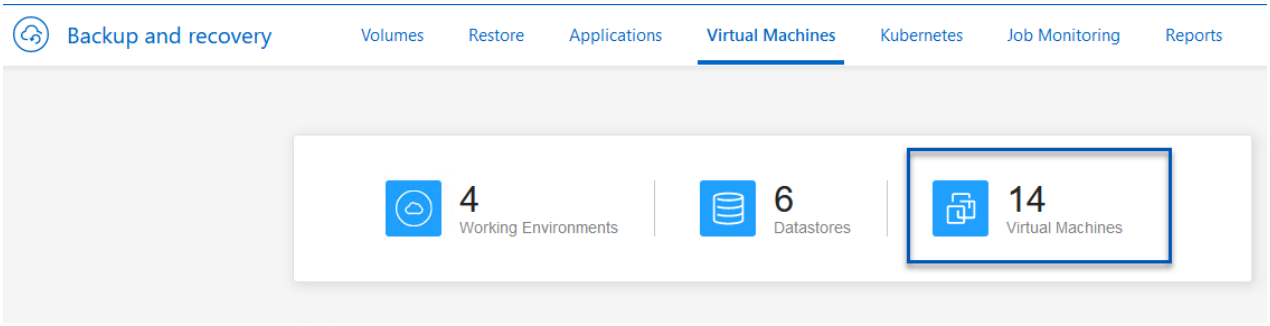
BlueXP 虛擬機器的備份與還原功能可將虛擬機器還原至其原始位置。還原功能可透過 BlueXP 網路主控台存取。

如需詳細資訊、請參閱 "從雲端還原虛擬機器資料"。

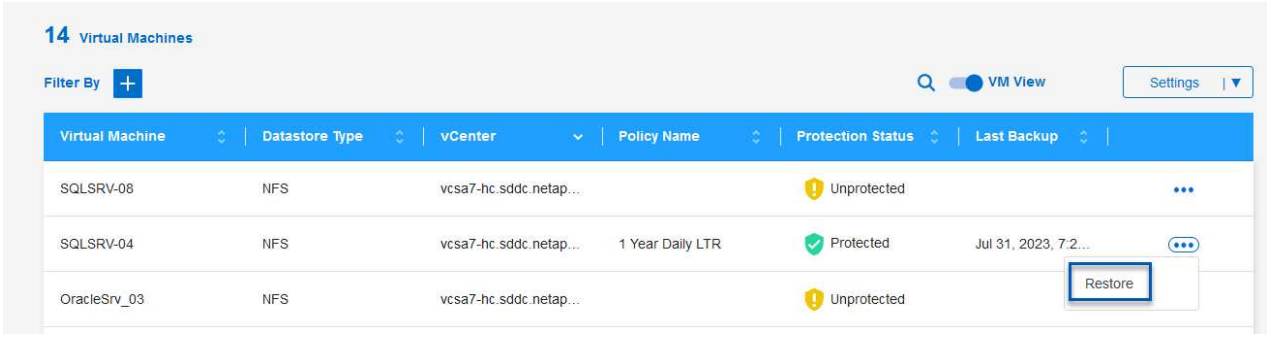
從 **BlueXP** 備份與還原還原虛擬機器

若要從 BlueXP 備份與還原還原虛擬機器、請完成下列步驟。

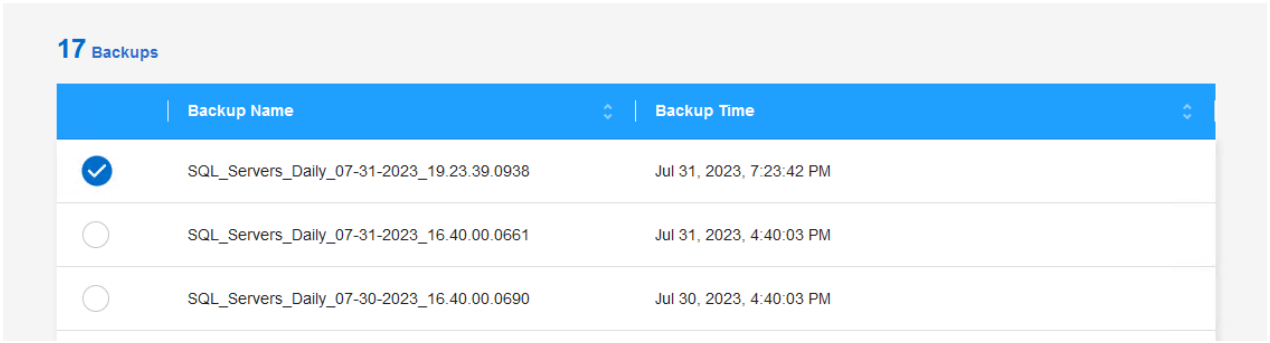
1. 瀏覽至 * 保護 > 備份與還原 > 虛擬機器 * 、然後按一下虛擬機器以檢視可供還原的虛擬機器清單。



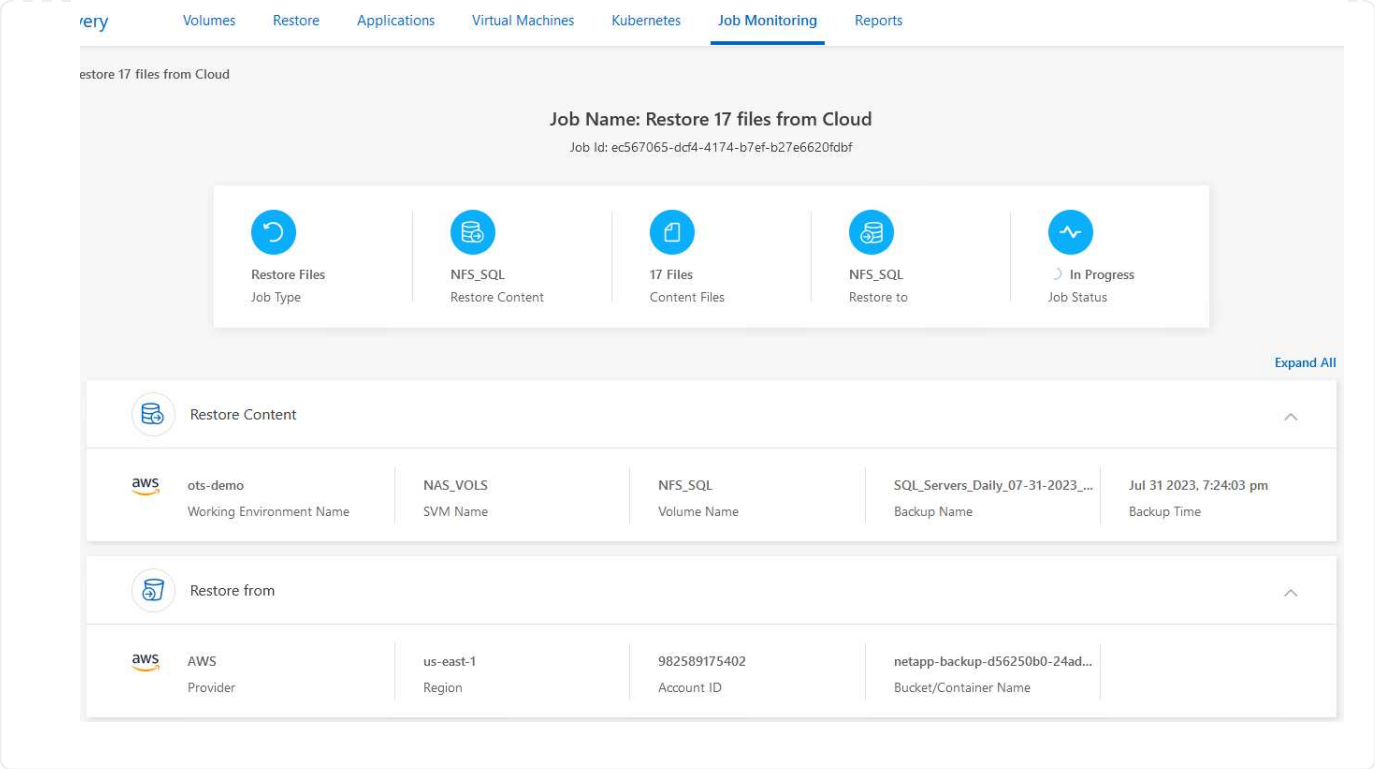
2. 存取要還原的虛擬機器的設定下拉式功能表、然後選取



3. 選取要還原的備份、然後按一下 * 下一步 * 。



4. 檢閱備份工作摘要、然後按一下 * 還原 * 以開始還原程序。
5. 從 * 工作監控 * 標籤監控還原工作的進度。



結論

搭配 SnapCenter Plug-in for VMware vSphere 和 BlueXP 虛擬機器備份與還原實作的 3-2-1 備份策略、可為資料保護提供強大、可靠且具成本效益的解決方案。這項策略不僅確保資料備援和可存取性、還能靈活地從任何位置、以及從內部部署的 ONTAP 儲存系統和雲端型物件儲存設備還原資料。

本文件中的使用案例著重於備受肯定的資料保護技術、強調 NetApp 、 VMware 與領先業界的雲端供應商之間的整合。適用於 VMware vSphere 的 SnapCenter 外掛程式可與 VMware vSphere 無縫整合、有效集中管理資料保護作業。這項整合可簡化虛擬機器的備份與還原程序、在 VMware 生態系統中輕鬆進行排程、監控及靈活的還原作業。BlueXP 虛擬機器的備份與還原功能提供安全無線備份的虛擬機器資料至雲端型物件儲存設備、可在 3-2-1 中提供一（ 1 ）個備份。直覺式介面和邏輯工作流程為重要資料的長期歸檔提供了安全的平台。

其他資訊

若要深入瞭解本解決方案所提供的技術、請參閱下列其他資訊。

- "VMware vSphere文件的VMware外掛程式SnapCenter"
- "BlueXP文件"

VMware Sovereign Cloud

適用於 **Sovereign Cloud** 的 **VMware** 資源

NetApp 與 VMware Sovereign Cloud

VMware Sovereign Cloud 概觀

對於處理及維護高度敏感資料的許多實體（例如國家和州政府）、以及受到高度管制的產

業（例如金融和醫療）、主權概念正逐漸成為雲端運算的必要元件。各國政府也希望擴大數位經濟能力、減少對跨國企業雲端服務的依賴。

VMware Sovereign Cloud 方案

VMware 將主權雲端定義為：

- 保護和釋放私營和公營部門組織的重要資料（例如國家資料、公司資料和個人資料）的價值
- 為數位經濟提供國家能力
- 使用稽核的安全控制來保護資料安全
- 確保遵守資料隱私權法律
- 提供資料駐留和資料主權、並完全控制司法管轄區、藉此改善資料控管

與值得信賴的 VMware Sovereign 雲端服務供應商合作

為了確保成功、企業組織必須與他們信任的合作夥伴合作、並能託管真實且自主的主權雲端平台。VMware Cloud 供應商在 VMware Sovereign Cloud 方案中獲得肯定、致力於根據現代化的軟體定義架構來設計和營運雲端解決方案、這些架構體現了 VMware Sovereign Cloud 架構中概述的關鍵原則和最佳實務。

- * 資料主權與司法管轄控制 * –所有資料均為居民、並受收集資料所在國家 / 地區的專屬控制與權限所規範。營運在司法管轄區內進行全面管理
- * 資料存取與完整性 * ：雲端基礎架構具有恢復能力、並可在管轄區內至少兩個資料中心位置使用、並提供安全且私有的連線選項。
- * 資料安全與法規遵循 * ：資訊安全管理系統控管已通過業界認可的全球（或區域）標準認證、並定期稽核。
- * 資料獨立與行動力 * ：支援現代化的應用程式架構、以防止廠商的雲端束縛、並實現應用程式可攜性與獨立性

如需 VMware 的詳細資訊、請造訪：

- "VMware Sovereign Cloud 概述"
- "什麼是 VMware Sovereign Cloud ？"
- "介紹全新的 VMware Sovereign Cloud 方案"
- "VMware Sovereign Cloud 技術白皮書"

Netpp 搭配 VMware Sovereign Cloud ：使用案例

NetApp 整合多項 NetApp 技術、支援 VMware Sovereign Cloud 概念。

請使用下列連結、深入瞭解 NetApp 技術與 VMware Sovereign Cloud 的整合：

- "NetApp StorageGRID 做為物件存放區延伸"

NetApp StorageGRID 做為物件存放區延伸

NetApp 與 VMware 合作、將 NetApp StorageGRID 整合至 VMware Cloud Director 、以支援 VMware Sovereign Cloud 。此 VMware Cloud Director 外掛程式可讓服務供應商將 StorageGRID 當作物件儲存產品（

無論使用案例為何）、並可透過服務供應商用來管理其產品目錄其他部分的相同 VMware 多租戶解決方案（ VMware Cloud Director ）來進行 StorageGRID 管理。

提供 VMware Sovereign 雲端的合作夥伴可以選擇 NetApp StorageGRID 來協助他們以非結構化資料來管理和維護雲端環境。其原生支援業界標準 API （例如 Amazon S3 API ）的通用相容性、有助於確保不同雲端環境之間的互通性順暢、而自動化生命週期管理等獨特創新技術則有助於確保更具成本效益的保護、儲存及長期維護客戶的非結構化資料。

NetApp 的 Sovereign Cloud 與 Cloud Director 供應商客戶的整合：

- 確保敏感資料（包括中繼資料）仍受到主權控制、同時防止外國主管機關存取可能違反資料隱私權法律的資料。
- 提高安全性與法規遵循能力、保護應用程式與資料不受瞬息萬變的攻擊模式影響、同時維持與值得信賴的本機持續相容。基礎架構、內建架構及當地專家。
- 符合未來需求的基礎架構、可快速因應瞬息萬變的資料隱私法規、安全威脅及地緣政治。
- 透過安全的資料共享與分析、在不違反隱私權法律的情況下推動創新、進而充分發揮資料價值。資料完整性受到保護、以確保獲得準確的洞見。

如需 StorageGRID 整合的詳細資訊、請參閱下列項目：

- "NetApp 公告"

NetApp 混合式多雲端搭配 Red Hat OpenShift Container 工作負載

適用於 Red Hat OpenShift Container 工作負載的 NetApp 混合式多雲端解決方案

總覽

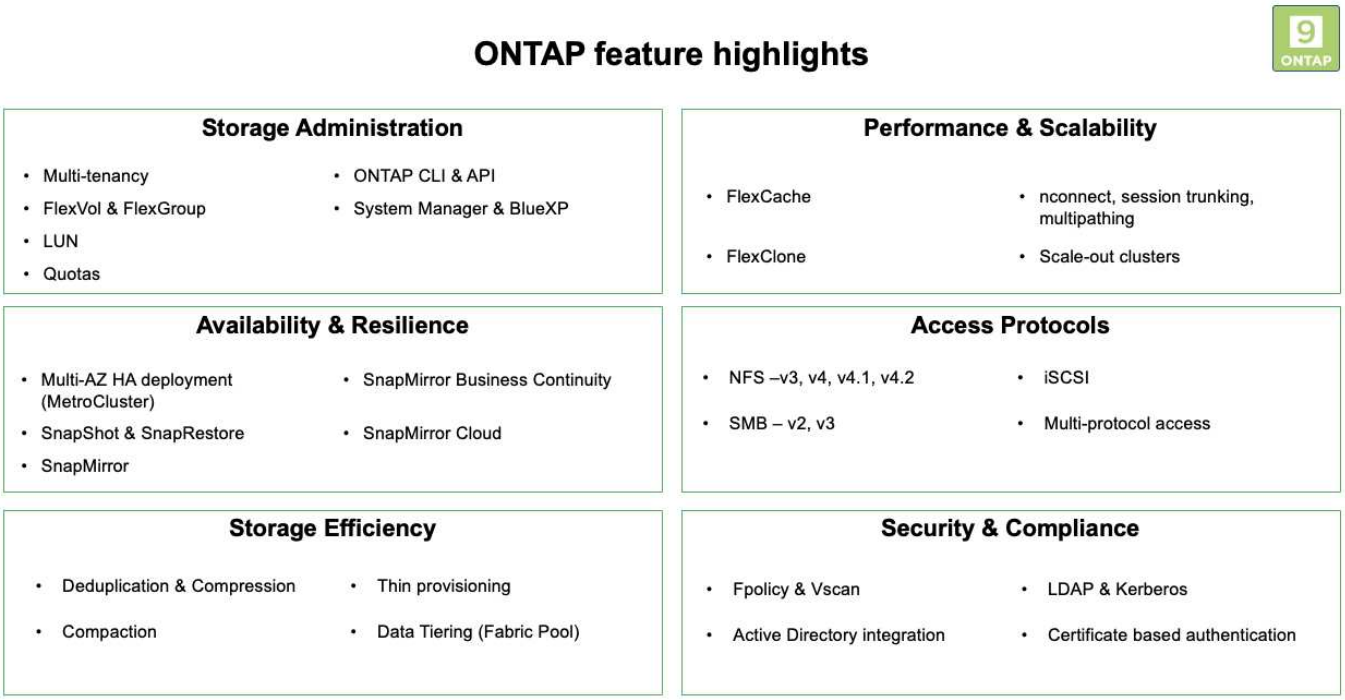
NetApp 發現客戶使用 Kubernetes 建置的容器和協調作業平台、將舊有企業應用程式現代化、並建置新的應用程式。Red Hat OpenShift Container Platform 是我們許多客戶採用的範例之一。

隨著越來越多客戶開始在企業內採用容器、 NetApp 的定位非常完美、可協助滿足其有狀態應用程式的持續儲存需求、以及資料保護、資料安全性和資料移轉等傳統資料管理需求。不過、這些需求是使用不同的策略、工具和方法來滿足的。

以 NetApp ONTAP * 為基礎的儲存選項如下所列、可為容器和 Kubernetes 部署提供安全性、資料保護、可靠性和靈活度。

- 內部部署的自我管理儲存設備：
  - NetApp Fabric 附加儲存設備（ FAS ）、 NetApp All Flash FAS Array （ AFF ）、 NetApp All SAN Array （ ASA ）和 ONTAP Select
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（ STaaS ）
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （ CVO ）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：

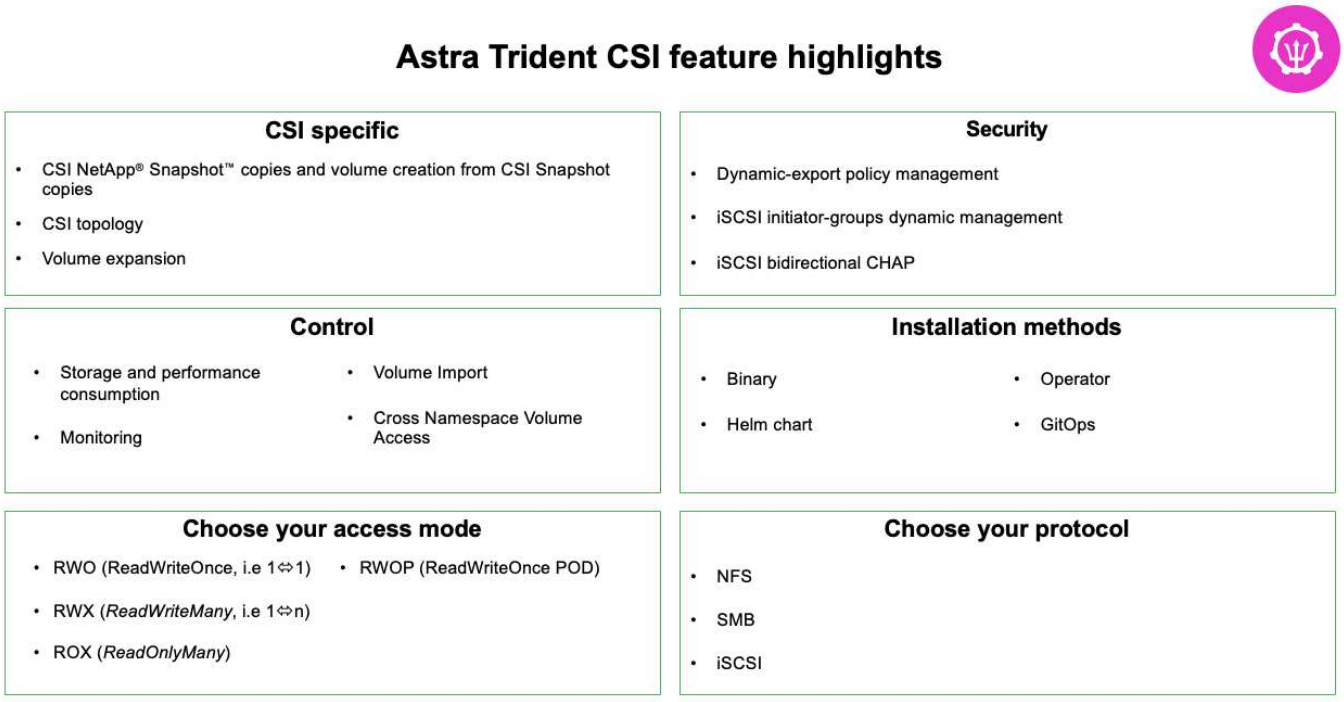
- Cloud Volumes Service for Google Cloud （ CVS ）、 Azure NetApp Files （ anf ）、 Amazon FSX for NetApp ONTAP 可在超大型擴充器中提供完全託管的儲存設備



- NetApp BlueXP** 可讓您從單一控制平面 / 介面管理所有儲存設備和資料資產。

您可以使用 BlueXP 來建立和管理雲端儲存設備（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 Astra Trident * 是符合 CSI 標準的 Storage Orchestrator 、可快速輕鬆地使用由上述各種 NetApp 儲存選項作為後盾的持續儲存設備。這是由 NetApp 維護和支援的開放原始碼軟體。



業務關鍵容器工作負載不只需要持續的磁碟區、他們的資料管理需求也需要保護及移轉應用程式 Kubernetes 物件。

> 應用程式資料除了包含使用者資料外、還包括 Kubernetes 物件：以下是一些範例： - Kubernetes 物件、例如 Pod 規格、 PVC 、部署、服務 - 自訂組態物件、例如組態對應和機密 - 持續性資料、例如 Snapshot 複本、備份、複本 - 自訂資源、例如 CRS 和 CRD

- NetApp Astra Control** 可作為完全託管和自我管理的軟體使用、可協調功能以提供健全的應用程式資料管理。請參閱 "Astra文件" 如需 Astra 系列產品的詳細資訊、請參閱。

本參考文件提供移轉與保護容器型應用程式的驗證、這些應用程式部署在 RedHat OpenShift Container 平台上、並使用 NetApp Astra Control Center 。此外、此解決方案還提供部署和使用 Red Hat Advanced Cluster Management （ACM）來管理容器平台的高階詳細資料。本文件也重點介紹使用 Astra Trident CSI 資源配置程式、將 NetApp 儲存設備與 Red Hat OpenShift 容器平台整合的詳細資料。Astra Control Center 部署在集線器叢集上、用於管理容器應用程式及其持續儲存生命週期。最後、它為 AWS （ROSA）中受管理 Red Hat OpenShift 叢集上的容器工作負載提供複寫和容錯移轉及容錯移轉解決方案、使用 Amazon FSx for NetApp ONTAP （FSxN）作為持續儲存設備。

適用於 **Red Hat OpenShift Container** 工作負載的 **NetApp** 混合式多雲端解決方案的價值主張

大多數客戶不只是在沒有任何現有基礎架構的情況下、就開始建置 Kubernetes 型環境。或許他們是一家傳統的 IT 商店、在虛擬機器上執行大部分的企業應用程式（例如大型 VMware 環境）。然後他們開始建置小型的容器型環境、以滿足其現代化應用程式開發團隊的需求。這些計畫通常從小規模開始、隨著團隊學習這些新技術和技能、開始變得更普及、並開始認識採用這些技術和技能的許多好處。客戶的好消息是 NetApp 可以滿足這兩種環境的需求。這套適用於混合式多雲端與 Red Hat OpenShift 的解決方案、可讓 NetApp 客戶採用現代化的雲端技術與服務、而無需徹底檢修整個基礎架構與組織。無論客戶的應用程式和資料是在內部部署、雲端、在虛擬機器上執行、或是在容器上執行、 NetApp 都能提供一致的資料管理、保護、安全性和可攜性。有了這些新解決方案、 NetApp 在內部部署資料中心環境中所提供的價值數十年來、將可在整個企業資料領域中提供、而無需投入大量資金來重新調整、取得新技能或建立新團隊。無論客戶的雲端旅程處於何種階段、NetApp 都能協助客戶解決這些業務挑戰。

NetApp 混合式多雲端搭配 Red Hat Openshift ：

- 為客戶提供經過驗證的設計和實務做法、以示範客戶在使用 Red Hat OpenShift 搭配 NetApp 型儲存解決方案時、如何管理、保護、保護及移轉資料和應用程式的最佳方法。
- 針對在 VMware 環境、裸機基礎架構或兩者的組合中、搭配 NetApp 儲存設備執行 Red Hat OpenShift 的客戶、提供最佳實務做法。
- 針對內部部署和雲端環境、以及兩者都使用的混合式環境、示範策略和選項。

適用於 **Red Hat OpenShift Container** 工作負載的 **NetApp** 混合式多雲端支援解決方案

本解決方案使用 OpenShift Container 平台（OCP）、 OpenShift Advanced Cluster Manager （ACM）、 NetApp ONTAP 、 NetApp BlueXP 和 NetApp Astra Control Center （ACC）來測試及驗證移轉與集中式資料保護。

對於此解決方案、 NetApp 會測試並驗證下列情境。根據下列特性、將解決方案分成多種情境：

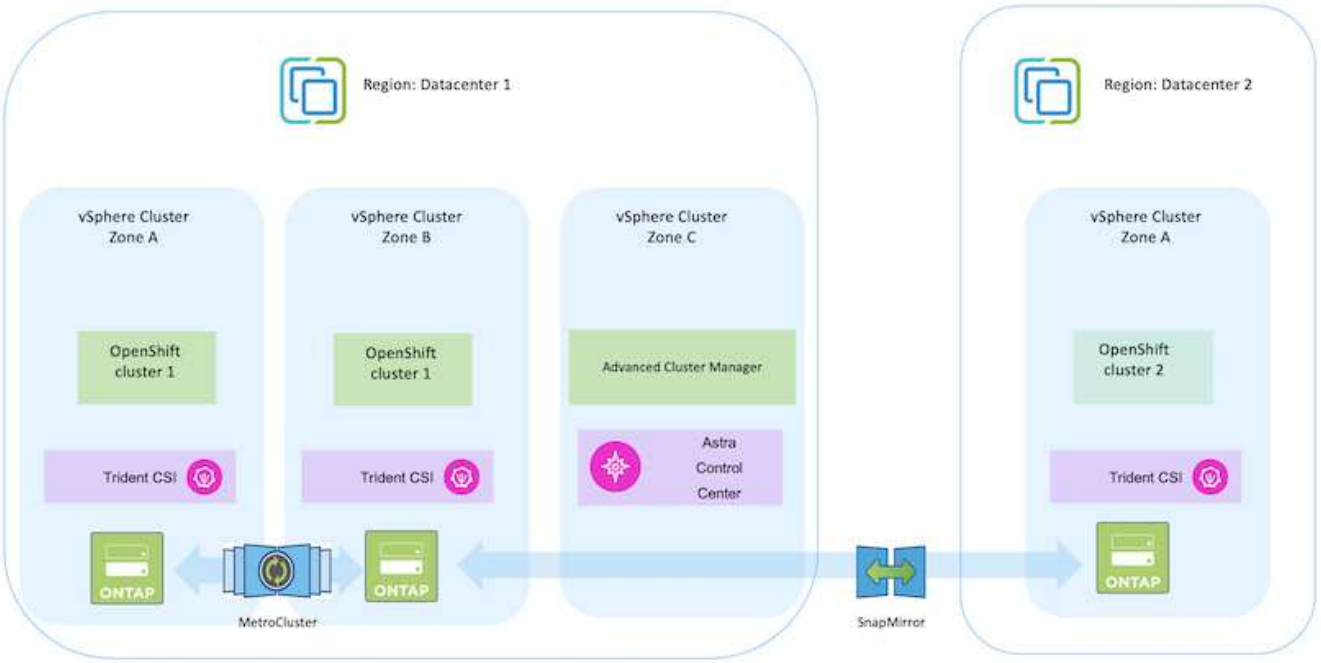
- 內部部署
- 雲端
  - 自我管理的 OpenShift 叢集和自我管理的 NetApp 儲存設備
  - 由供應商管理的 OpenShift 叢集和由供應商管理的 NetApp 儲存設備

我們將在未來建立更多解決方案和使用案例。 **

案例 **1** ：使用主動定速控制系統在內部環境中保護資料及移轉

- 內部部署：自我管理的 OpenShift 叢集與自我管理的 NetApp 儲存設備 **
  - 使用 Acc 建立 Snapshot 複本、備份與還原、以保護資料。
  - 使用 Acc 執行容器應用程式的 SnapMirror 複寫。

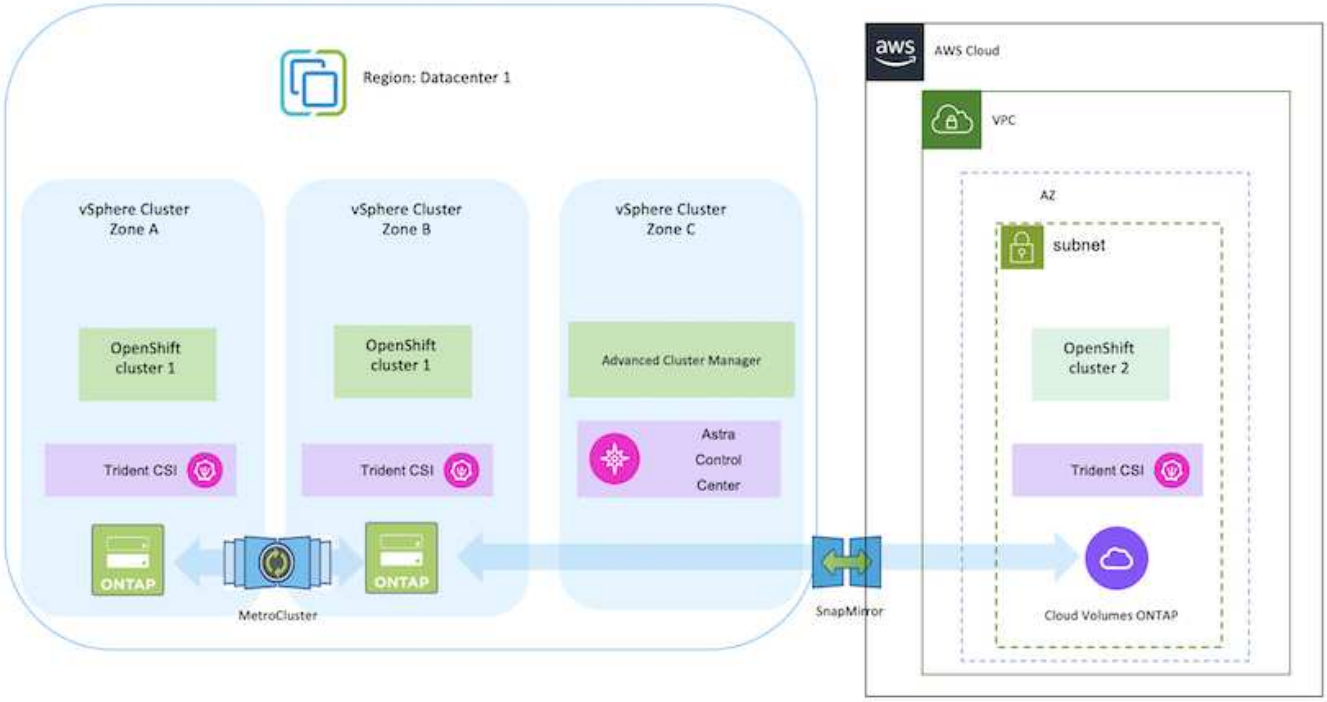
案例**1**



案例 **2** ：使用主動定速控制系統、從內部環境到 **AWS** 環境的資料保護與移轉

- 內部部署：自我管理的 OpenShift 叢集與自我管理的儲存設備 **AWS Cloud** ：自我管理的 **OpenShift** 叢集與自我管理的儲存設備
  - 使用主動定速控制系統執行備份與還原、以保護資料。
  - 使用 Acc 執行容器應用程式的 SnapMirror 複寫。

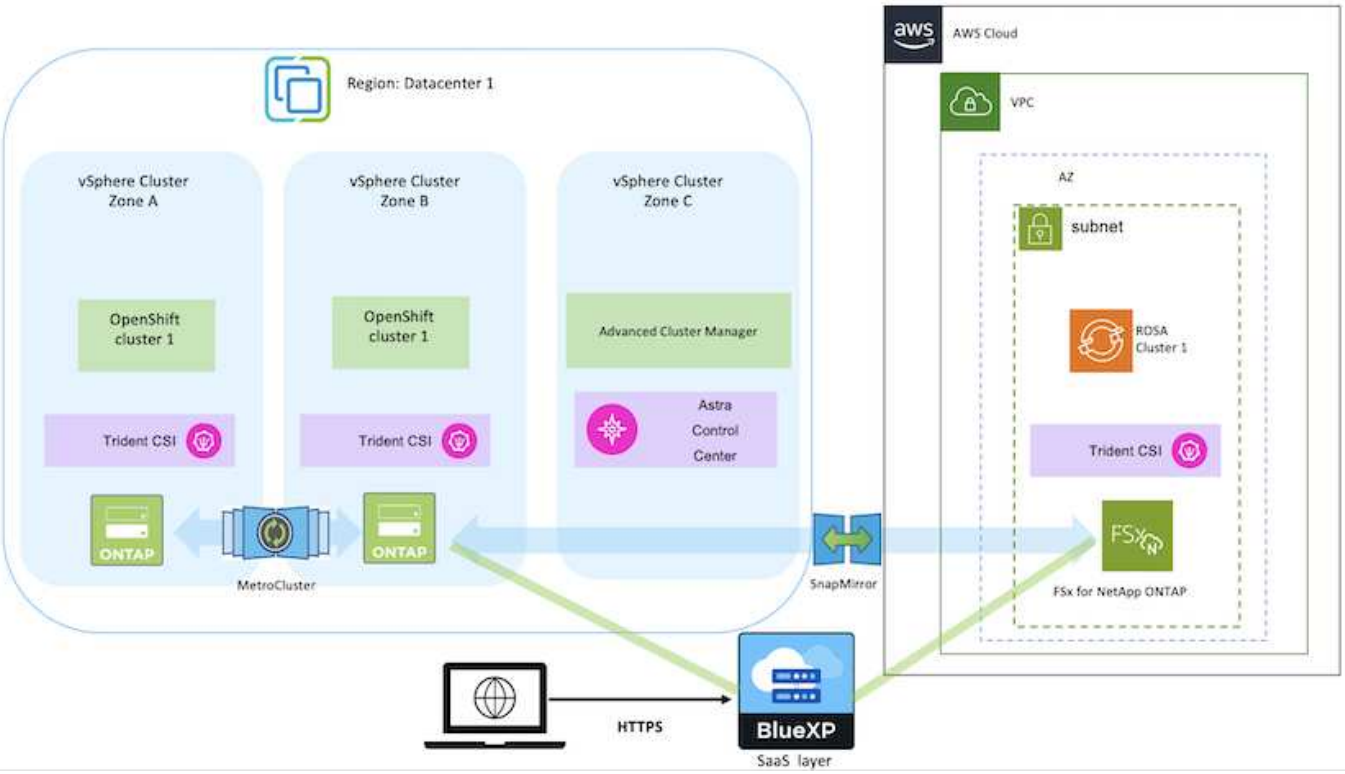
案例**2**



案例 **3** ：資料保護、從內部環境移轉至 **AWS** 環境

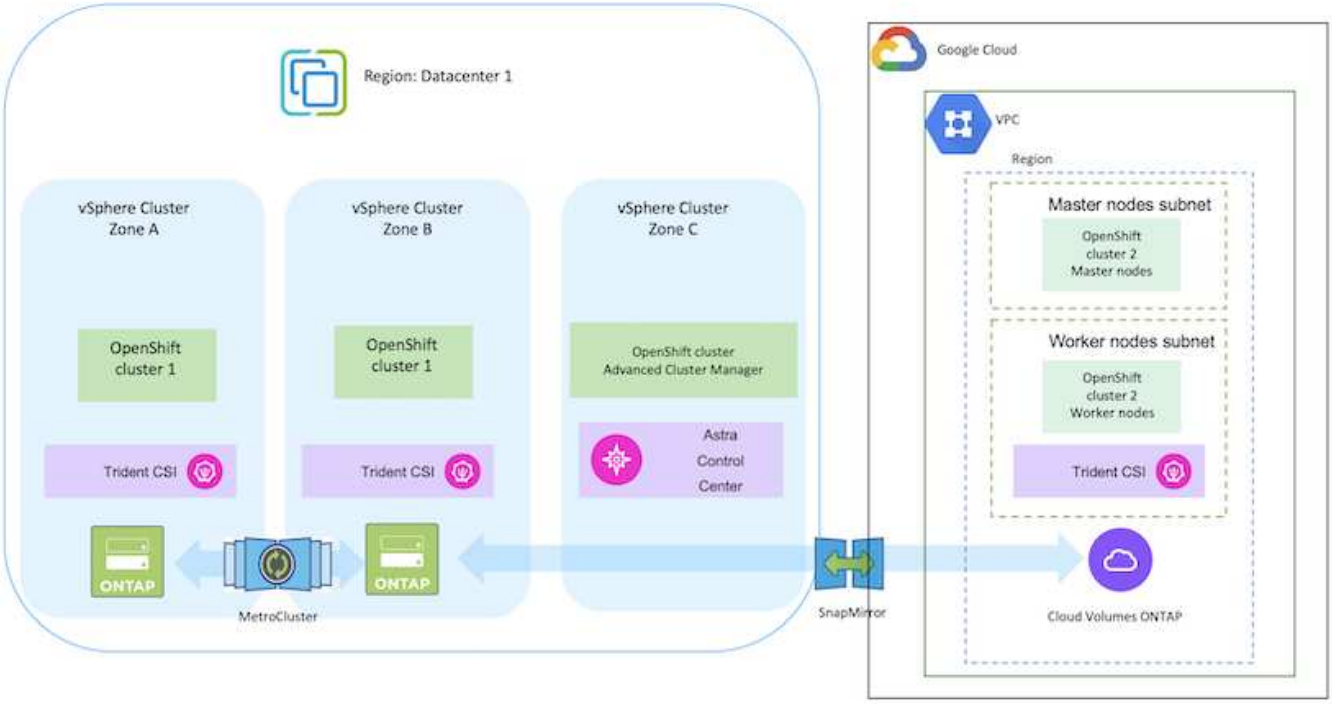
- 內部部署：自我管理的 OpenShift 叢集與自我管理的儲存設備 **AWS Cloud** ：由供應商管理的 **OpenShift** 叢集（ **ROSA** ）和由供應商管理的儲存設備（ **FSxN** ）
  - 使用 BlueXP 執行持續磁碟區（ FSxN ）的複寫。
  - 使用 OpenShift GitOps 重新建立應用程式中繼資料。

案例 **3**



案例 **4** ：使用主動定速控制系統、從內部環境到 **GCP** 環境的資料保護與移轉

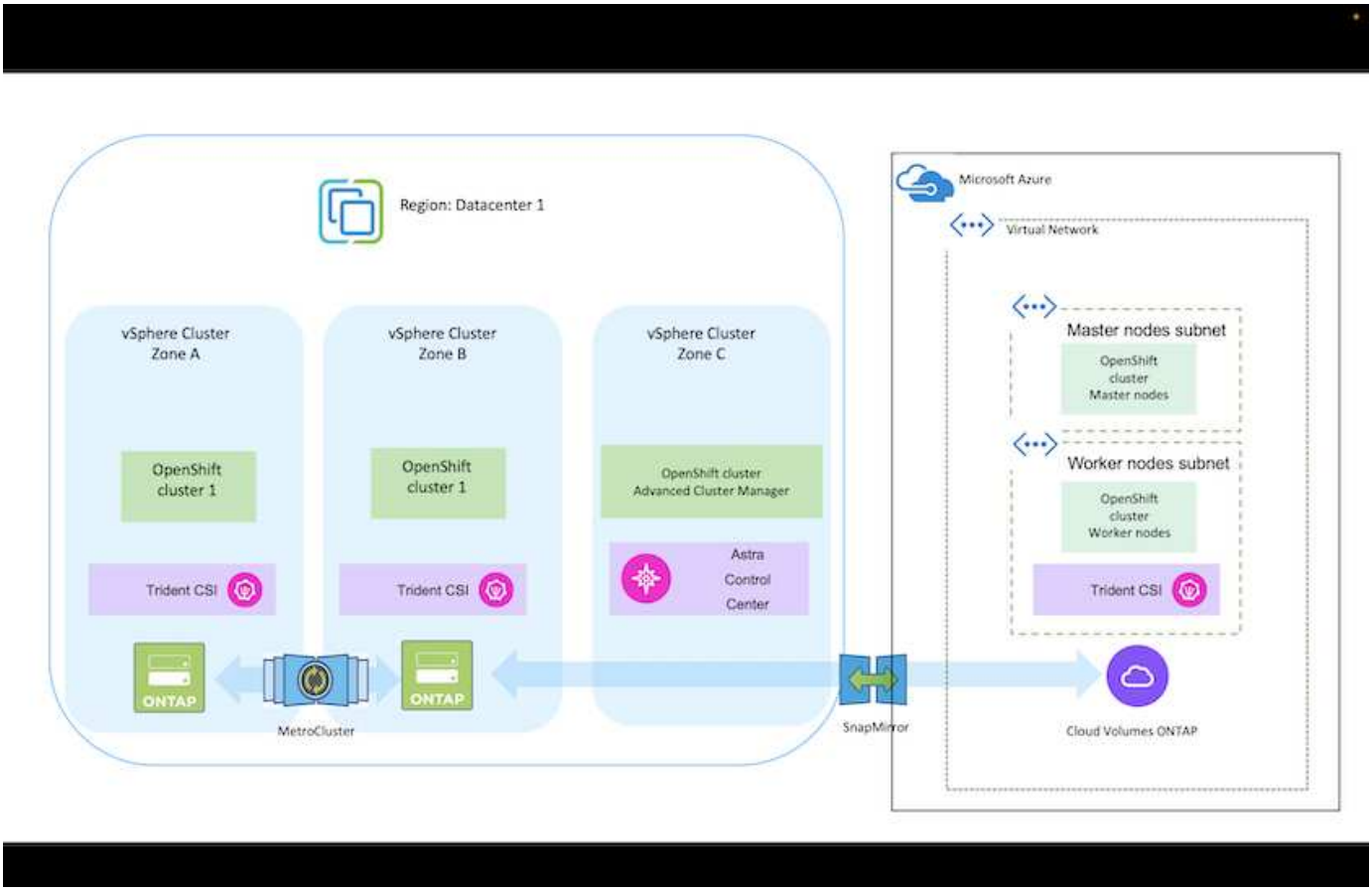
- 內部部署：自我管理的 OpenShift 叢集與自我管理的儲存設備 **
- Google Cloud ：自我管理的 OpenShift 叢集與自我管理的儲存設備 **
  - 使用主動定速控制系統執行備份與還原、以保護資料。
  - 使用 Acc 執行容器應用程式的 SnapMirror 複寫。



如需在 MetroCluster 組態中使用 ONTAP 的考量、請參閱 "請按這裡"。

案例 **5** ：使用主動定速控制系統、從內部環境到 **Azure** 環境的資料保護與移轉

- 內部部署：自我管理的 OpenShift 叢集與自我管理的儲存設備 **
- Azure Cloud ：自我管理的 OpenShift 叢集與自我管理儲存設備 **
  - 使用主動定速控制系統執行備份與還原、以保護資料。
  - 使用 Acc 執行容器應用程式的 SnapMirror 複寫。



如需在 MetroCluster 組態中使用 ONTAP 的考量、請參閱 "請按這裡"。

解決方案驗證中使用的各種元件版本

此解決方案使用 OpenShift Container 平台、 OpenShift 進階叢集管理程式、 NetApp ONTAP 和 NetApp Astra 控制中心來測試及驗證移轉與集中式資料保護。

解決方案的案例 1 、 2 和 3 已使用下表所示的版本進行驗證：

元件	版本
* VMware *	vSphere Client 8.0.0.10200 版 VMware ESXi 、 8.0.0 、 20842819
* 集線器叢集 *	OpenShift 4.11.34
* 來源與目的地叢集 *	OpenShift 4.12.9 內部部署和 AWS
* NetApp Astra Trident *	Trident Server 和 Client 23.04.0
* NetApp Astra 控制中心 *	Acc 22.11.0-82
* NetApp ONTAP *	零點9.12.1. ONTAP
* AWS FSX for NetApp ONTAP *	單— AZ

解決方案的案例 4 已使用下表所示的版本進行驗證：

元件	版本
* VMware *	vSphere Client 8.0.2.00000 版 VMware ESXi 、 8.0.2 、 22380479
* 集線器叢集 *	OpenShift 4.13.13.
* 來源與目的地叢集 *	OpenShift 4.13.12. 內部部署和 Google Cloud
* NetApp Astra Trident *	Trident Server 和 Client 23.07.0
* NetApp Astra 控制中心 *	ACC 23.07.0-25
* NetApp ONTAP *	零點9.12.1. ONTAP
* Cloud Volumes ONTAP *	單一 AZ 、單一節點、 9.14.0

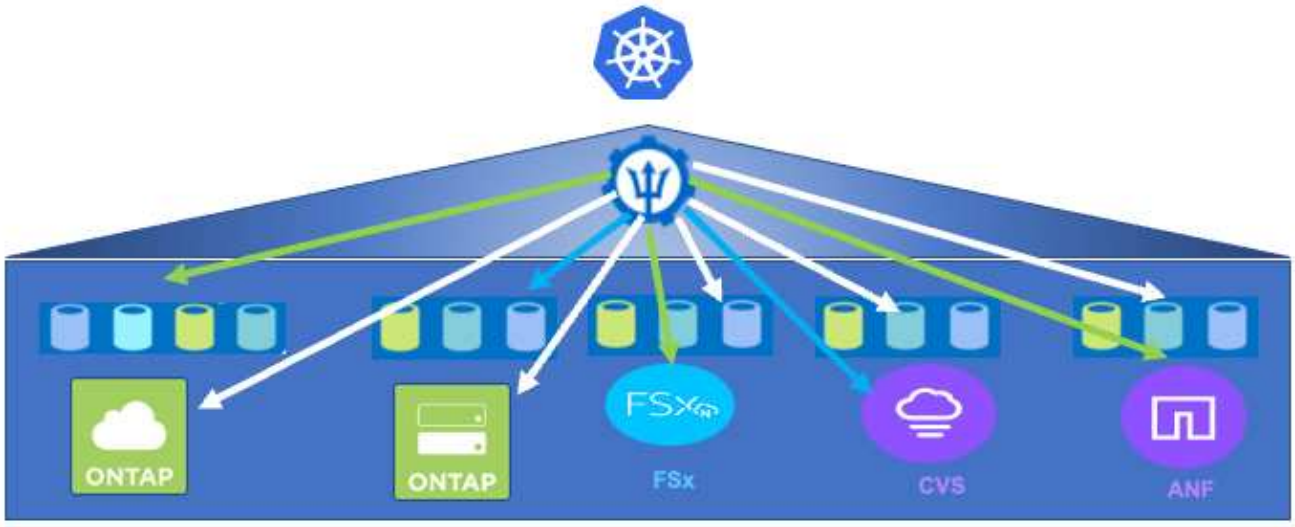
解決方案的案例 5 已使用下表所示的版本進行驗證：

元件	版本
* VMware *	vSphere Client 8.0.2.00000 版 VMware ESXi 、 8.0.2 、 22380479
* 來源與目的地叢集 *	OpenShift 4.13.25 內部部署和 Azure 中
* NetApp Astra Trident *	Trident 伺服器與用戶端及 Astra 控制備置程式 23.10.0
* NetApp Astra 控制中心 *	Acc 23.10
* NetApp ONTAP *	零點9.12.1. ONTAP
* Cloud Volumes ONTAP *	單一 AZ 、單一節點、 9.14.0

支援與 **Red Hat Open Shift Container** 的 **NetApp** 儲存整合

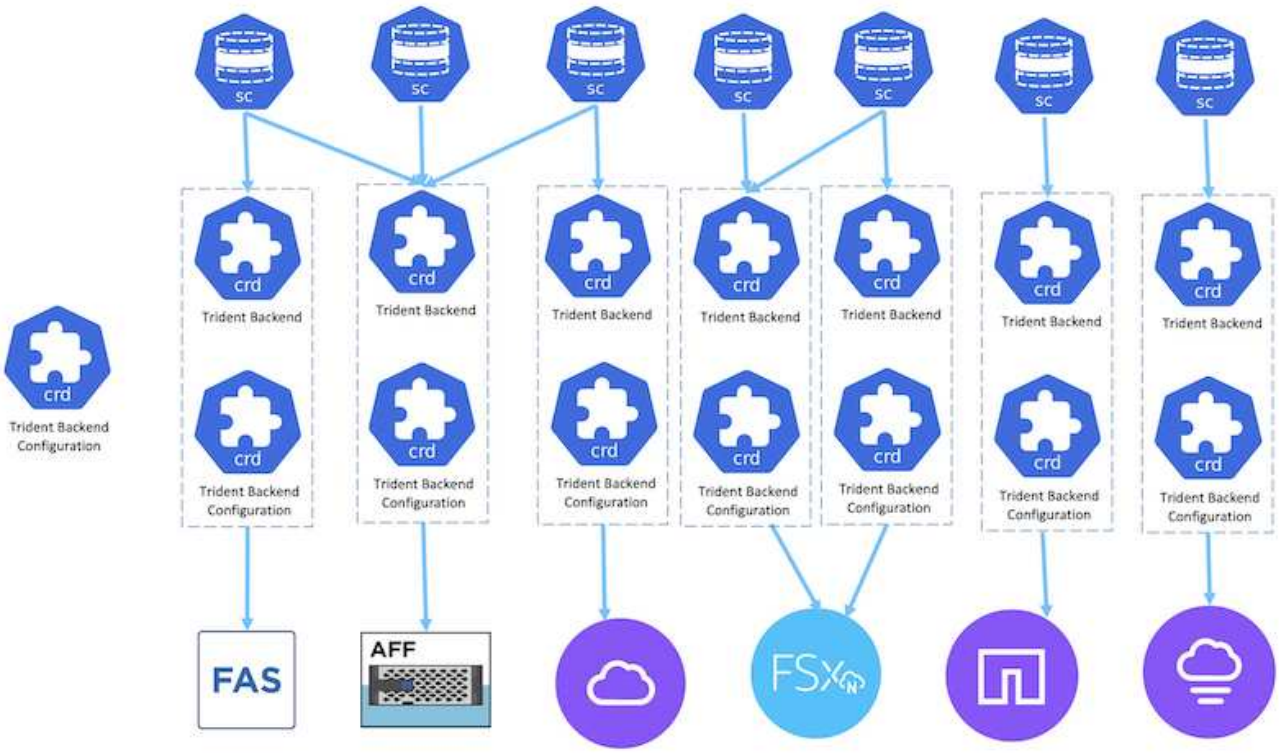
無論 Red Hat Open Shift 容器是在 VMware 上執行、或是在超大規模環境中執行、NetApp Astra Trident 都可作為其支援的各種類型後端 NetApp 儲存設備的 CSI 資源配置程式。

下圖說明各種後端 NetApp 儲存設備、可與使用 NetApp Astra Trident 的 OpenShift 叢集整合。

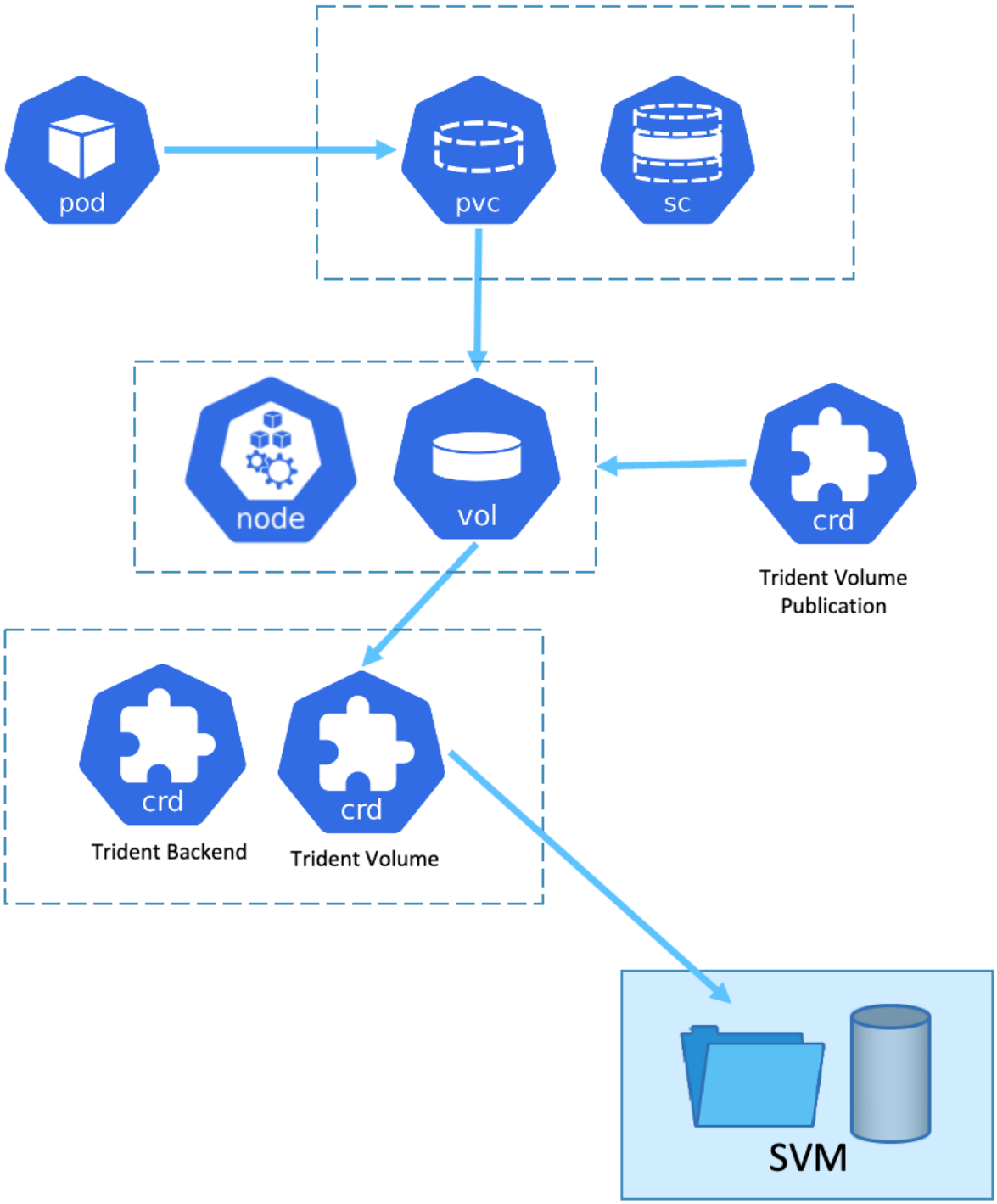


ONTAP 儲存虛擬機器（ SVM ）提供安全的多租戶共享。單一 OpenShift 叢集可連線至單一 SVM 或多個 SVM 、甚至連至多個 ONTAP 叢集。儲存類別會根據參數或標籤來篩選後端儲存設備。儲存管理員會使用 Trident 後端組態來定義連接至儲存系統的參數。成功建立連線時、它會建立 Trident 後端、並填入儲存類別可篩選的資訊。

以下顯示 storagecasser 與後端之間的關係。



應用程式擁有者使用儲存類別要求持續磁碟區。儲存類別會篩選後端儲存設備。Pod 與後端儲存設備之間的關係如下所示。



Container Storage Interface （ CSI ）選項

在 vSphere 環境中、客戶可以選擇 VMware CSI 驅動程式和 / 或 Astra Trident CSI 來與 ONTAP 整合。使用 VMware CSI 時、持續磁碟區會作為本機 SCSI 磁碟使用、而使用 Trident 時、則會與網路一起使用。由於 VMware CSI 不支援搭配 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 。在 FC 型部署中、 VMware CSI 是首選、 SnapMirror Business Continuity （ SMBC ）可提供區域層級的高可用度。

VMware CSI 支援

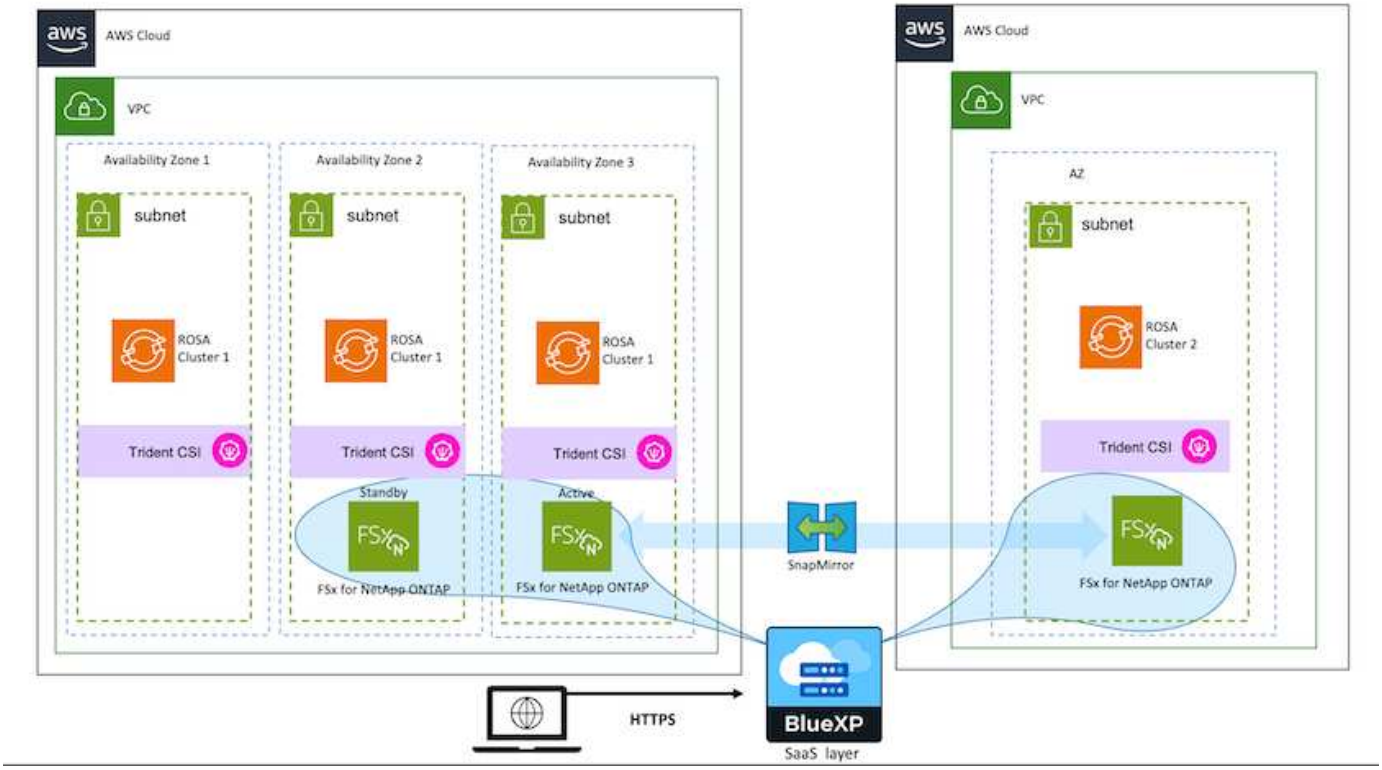
- 核心區塊型資料存放區（ FC 、 FCoE 、 iSCSI 、 NVMeoF ）
- 核心檔案型資料存放區（ NFS v3 、 v4 ）
- VVOL 資料存放區（區塊和檔案）

Trident 提供下列驅動程式來支援 ONTAP

- ONTAP-SAN （專用磁碟區）
- ONTAP SAN 經濟型（共享 Volume ）
- ONTAP-NAS （專用磁碟區）
- ONTAP NAS 經濟型（共享 Volume ）
- ONTAP-NAS-Flexgroup （專用大型 Volume ）

對於 VMware CSI 和 Astra Trident CSI 、 ONTAP 支援 nconnect 、工作階段主幹、 Kerberos 等、適用於 NFS 和多重路徑、 chap 驗證等區塊傳輸協定。

在 AWS 中、適用於 NetApp ONTAP （ FSxN ）的 FSx 可部署在單一可用性區域（ AZ ）或多個 AZ 中。對於需要高可用度的正式作業工作負載、多個 AZ 可提供區域層級的容錯能力、而且與單一 AZ 相比、 NVMe 讀取快取能力更佳。如需詳細資訊、請參閱 "AWS 效能準則"。
為了節省災難恢復站台的成本、可以使用單一 AZ FSX ONTAP 。



如需 FSX ONTAP 支援的 SVM 數量、請參閱 "管理 FSX ONTAP 儲存虛擬機器"

適用於 **Red Hat OpenShift Container** 工作負載的 **NetApp** 混合式多雲端解決方案

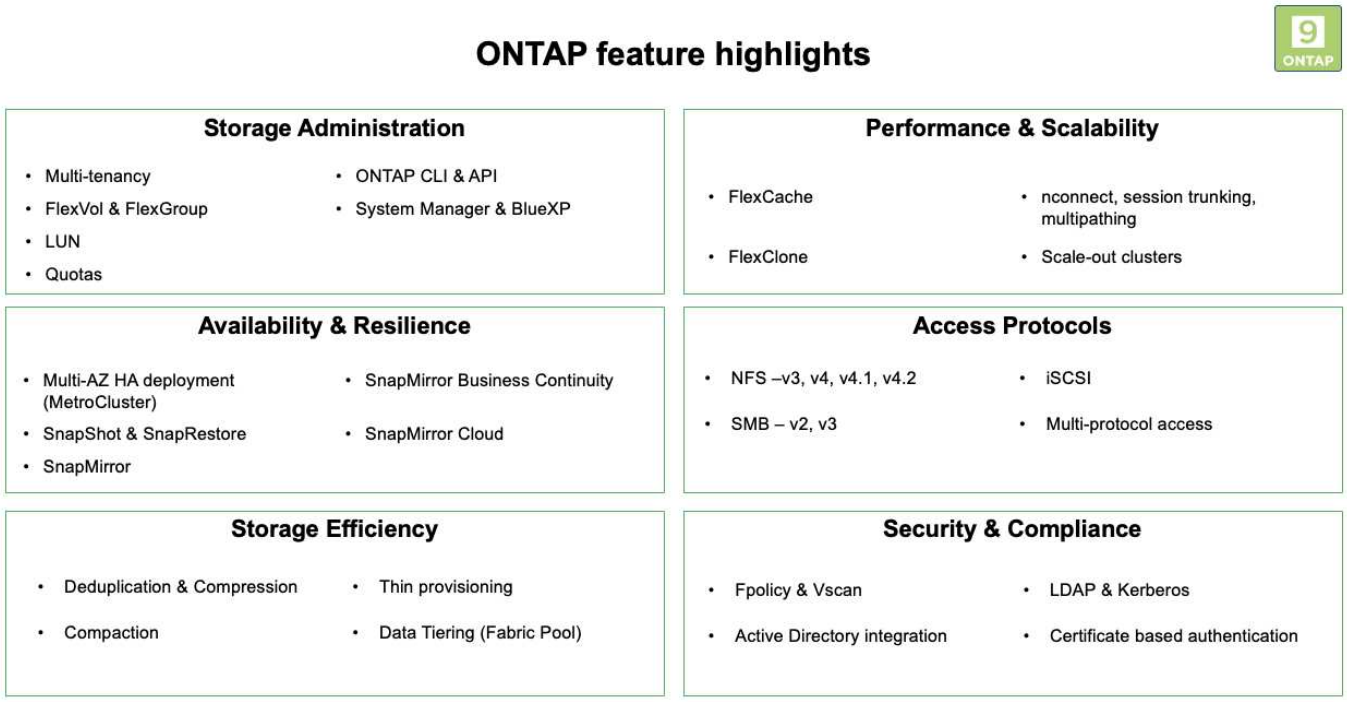
總覽

NetApp 發現客戶使用 Kubernetes 建置的容器和協調作業平台、將舊有企業應用程式現代化、並建置新的應用程式。Red Hat OpenShift Container Platform 是我們許多客戶採用的範例之一。

隨著越來越多客戶開始在企業內採用容器、 NetApp 的定位非常完美、可協助滿足其有狀態應用程式的持續儲存需求、以及資料保護、資料安全性和資料移轉等傳統資料管理需求。不過、這些需求是使用不同的策略、工具和方法來滿足的。

以 NetApp ONTAP * 為基礎的儲存選項如下所列、可為容器和 Kubernetes 部署提供安全性、資料保護、可靠性和靈活度。

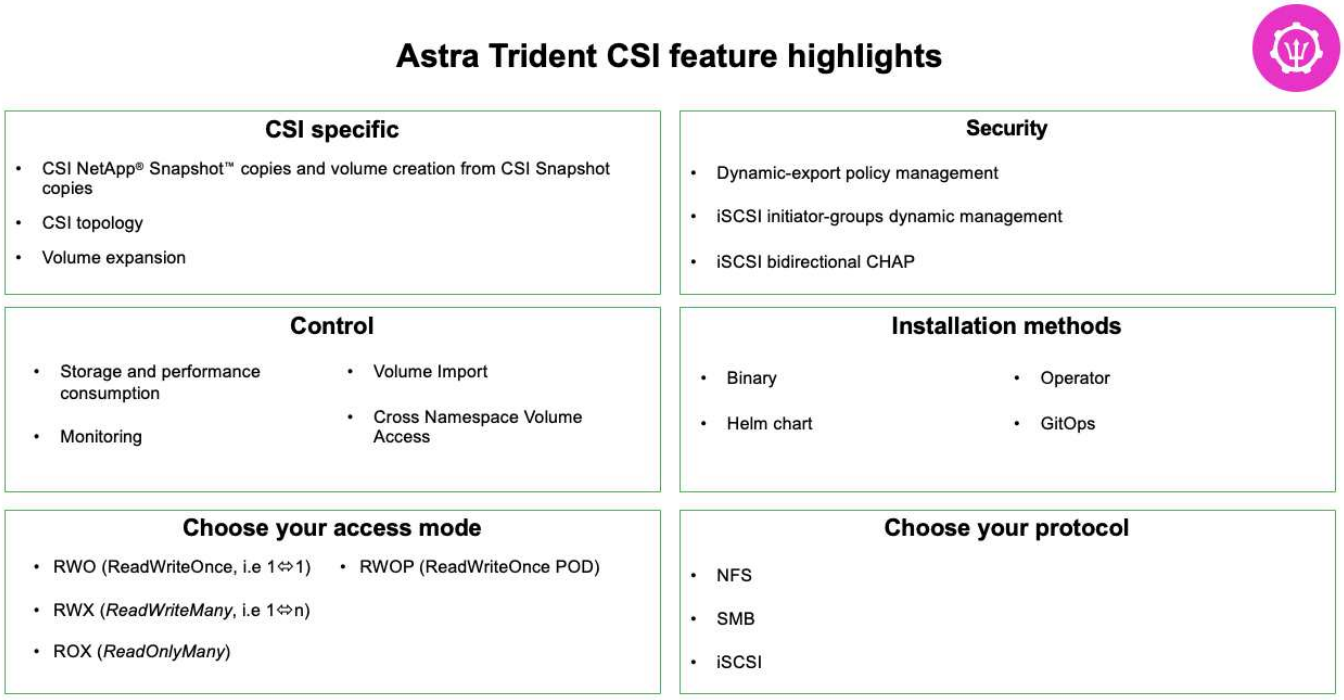
- 內部部署的自我管理儲存設備：
  - NetApp Fabric 附加儲存設備（ FAS ）、 NetApp All Flash FAS Array （ AFF ）、 NetApp All SAN Array （ ASA ）和 ONTAP Select
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（ STaaS ）
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （ CVO ）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：
  - Cloud Volumes Service for Google Cloud （ CVS ）、 Azure NetApp Files （ anf ）、 Amazon FSX for NetApp ONTAP 可在超大型擴充器中提供完全託管的儲存設備



- NetApp BlueXP** 可讓您從單一控制平面 / 介面管理所有儲存設備和資料資產。

您可以使用 BlueXP 來建立和管理雲端儲存設備（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 Astra Trident * 是符合 CSI 標準的 Storage Orchestrator 、可快速輕鬆地使用由上述各種 NetApp 儲存選項作為後盾的持續儲存設備。這是由 NetApp 維護和支援的開放原始碼軟體。



業務關鍵容器工作負載不只需要持續的磁碟區、他們的資料管理需求也需要保護及移轉應用程式 Kubernetes 物件。

應用程式資料除了包含使用者資料外、還包括 Kubernetes 物件：以下是一些範例： - Kubernetes 物件、例如 Pod 規格、 PVC 、部署、服務 - 自訂組態物件、例如組態對應和機密 - 持續性資料、例如 Snapshot 複本、備份、複本 - 自訂資源、例如 CRS 和 CRD

- NetApp Astra Control** 可作為完全託管和自我管理的軟體使用、可協調功能以提供健全的應用程式資料管理。請參閱 "Astra文件" 如需 Astra 系列產品的詳細資訊、請參閱。

本參考文件提供移轉與保護容器型應用程式的驗證、這些應用程式部署在 RedHat OpenShift Container 平台上、並使用 NetApp Astra Control Center 。此外、此解決方案還提供部署和使用 Red Hat Advanced Cluster Management （ ACM ）來管理容器平台的高階詳細資料。本文件也重點介紹使用 Astra Trident CSI 資源配置程式、將 NetApp 儲存設備與 Red Hat OpenShift 容器平台整合的詳細資料。Astra Control Center 部署在集線器叢集上、用於管理容器應用程式及其持續儲存生命週期。最後、它為 AWS （ ROSA ）中受管理 Red Hat OpenShift 叢集上的容器工作負載提供複寫和容錯移轉及容錯移轉解決方案、使用 Amazon FSx for NetApp ONTAP （ FSxN ）作為持續儲存設備。

NetApp 解決方案搭配 **VMware** 上的 **Red Hat OpenShift Container** 平台工作負載

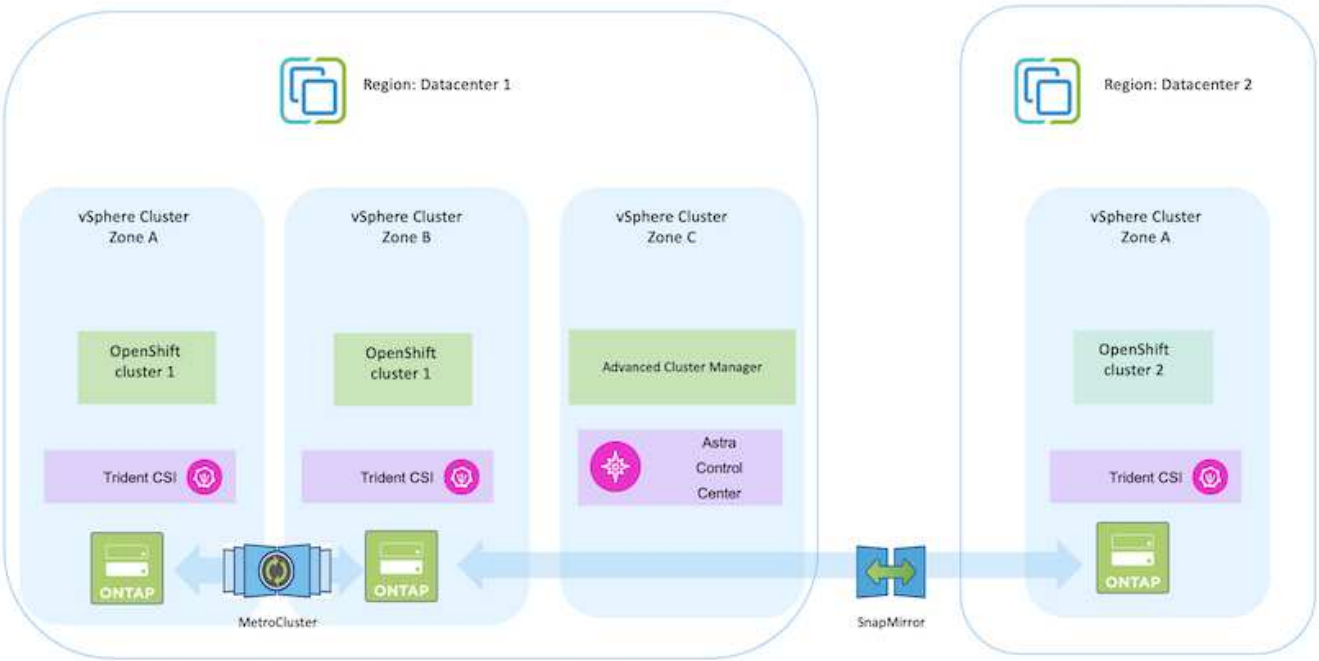
如果客戶需要在其私有資料中心的基礎架構上執行現代化的容器化應用程式、他們可以這麼做。他們應該規劃並部署 Red Hat OpenShift Container 平台（ OCP ）、以打造成功部署容器工作負載的正式作業環境。他們的 OCP 叢集可以部署在 VMware 或裸機上。

NetApp ONTAP 儲存設備可為容器部署提供資料保護、可靠性和靈活度。Astra Trident 是動態儲存資源配置程式、可為客戶的有狀態應用程式使用持續的 ONTAP 儲存設備。Astra Control Center 可用來協調有狀態應用程式的許多資料管理需求、例如資料保護、移轉和業務持續運作。

有了 VMware vSphere 、 NetApp ONTAP 工具就能提供 vCenter 外掛程式、可用於佈建資料存放區。套用標籤並搭配 OpenShift 使用、以儲存節點組態和資料。NVMe 型儲存設備提供較低的延遲和高效能。

此解決方案提供使用 Astra Control Center 的資料保護和容器工作負載移轉的詳細資料。對於此解決方案、容器工作負載會部署在內部部署環境中 vSphere 上的 Red Hat OpenShift 叢集上。附註：未來我們將為裸機上 OpenShift 叢集上的容器工作負載提供解決方案。

使用 **Astra Control Center** 為 **OpenShift Container** 工作負載提供資料保護與移轉解決方案

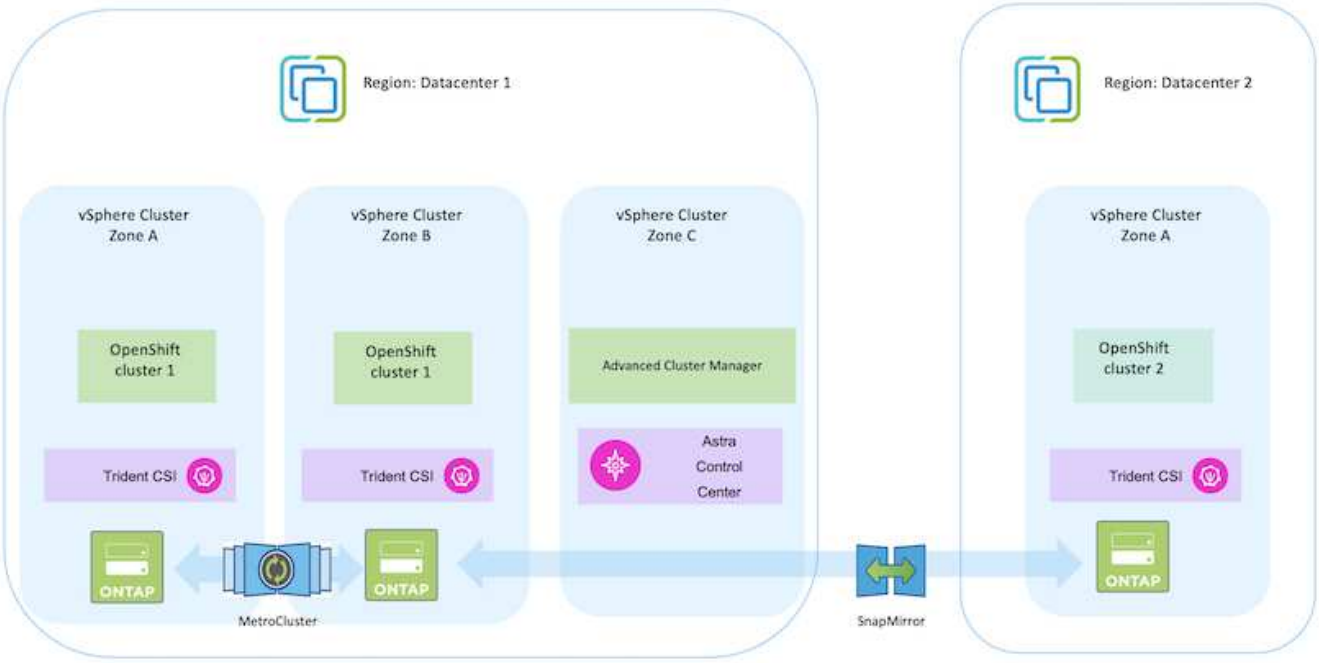


在 **VMware** 上部署和設定 **Red Hat OpenShift Container** 平台

本節說明如何設定和管理 OpenShift 叢集、以及如何管理其上的有狀態應用程式的高階工作流程。它顯示在 Astra Trident 協助下使用 NetApp ONTAP 儲存陣列來提供持續的磁碟區。詳細說明如何使用 Astra Control Center 來執行有狀態應用程式的資料保護和移轉活動。

部署 Red Hat OpenShift Container 平台叢集有多種方法。此設定的高階說明提供所使用特定方法的文件連結。您可以參閱中提供的相關連結中的其他方法 "資源區段"。

下圖說明在資料中心部署在 VMware 上的叢集。



設定程序可分為下列步驟：

部署及設定 **CentOS VM**

- 它部署在 VMware vSphere 環境中。
- 此 VM 用於部署某些元件、例如 NetApp Astra Trident 和 NetApp Astra Control Center 、以供解決方案使用。
- 在安裝期間、已在此 VM 上設定 root 使用者。

在 **VMware vSphere** （ **Hub** 叢集）上部署及設定 **OpenShift Container Platform** 叢集

請參閱的說明 "輔助部署" 部署 OCP 叢集的方法。

請記住下列事項： - 建立 ssh 公開金鑰和私密金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。此程式用於開機您在 VMware vSphere 環境中為主節點和工作節點所建立的 VM 。虛擬機器應具備最低的 CPU 、記憶體和硬碟需求。（請參閱上的 VM create 命令 "這" 主節點和提供此資訊的工作節點頁面）：應在所有 VM 上啟用磁碟 UUID 。- 至少為主節點建立 3 個節點、為工作者建立 3 個節點。- 安裝程式發現這些項目後、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 叢集上的進階叢集管理操作員來安裝。請參閱說明 "請按這裡"。

在 **Hub** 叢集上安裝內部 **Red Hat Quay** 登錄。

- 必須有內部登錄才能推送 Astra 映像。使用 Hub 叢集中的「操作員」來安裝 Quay 內部登錄。
- 請參閱說明 "請按這裡"

安裝兩個額外的 **OCP** 叢集（來源和目的地）

- 您可以使用 Hub 叢集上的 ACM 來部署其他叢集。
- 請參閱說明 "請按這裡"。

設定 **NetApp ONTAP** 儲存設備

- 在 VMware 環境中安裝可連線至 OCP VM 的 ONTAP 叢集。
- 建立 SVM 。
- 設定 NAS 資料 LIF 以存取 SVM 中的儲存設備。

在 **OCP** 叢集上安裝 **NetApp Trident**

- 在所有三個叢集上安裝 NetApp Trident ：集線器、來源和目的地叢集
- 請參閱說明 "請按這裡"。
- 爲 ONTAP 一 NAS 創建一個存儲後端。
- 為 ONTAP-NAS 建立儲存類別。
- 請參閱指示 "請按這裡"。

安裝 **NetApp Astra Control Center**

- NetApp Astra Control Center 是使用 Hub 叢集上的 Astra 運算子來安裝。
- 請參閱說明 "請按這裡"。

值得記住的重點： * 從支援網站下載 NetApp Astra Control Center 映像。* 將映像推送至內部登錄。* 請參閱此處的說明。

在來源叢集上部署應用程式

使用 OpenShift GitOps 部署應用程式。（例如Postgres 、 Ghost ）

將來源叢集和目的地叢集新增至 **Astra Control Center** 。

> 將叢集新增至 Astra Control 管理之後、您可以在叢集上安裝應用程式（ Astra Control 之外）、然後前往 Astra Control 中的「應用程式」頁面來定義應用程式及其資源。請參閱 "開始管理 Astra Control Center 的應用程式區段"。

下一步是使用 Astra Control Center 從來源叢集到目的地叢集進行資料保護和資料移轉。

使用 **Astra** 保護資料

本頁顯示在 VMware vSphere 上使用 Astra Control Center （ ACC ）執行的 Red Hat OpenShift Container 應用程式資料保護選項。

當使用者使用 Red Hat OpenShift 將應用程式現代化的過程中、應制定資料保護策略、以保護他們不受意外刪除或任何其他人為錯誤的影響。為了保護資料不受萬用者的影響、通常也需要採取保護策略來達到法規或法規遵循的目的。

資料保護的需求各不相同、從還原到時間點複本、到自動容錯移轉到不同的故障網域、而無需人為介入。許多客戶選擇 ONTAP 做為其 Kubernetes 應用程式的首選儲存平台、因為其豐富的功能包括多租戶、多重傳輸協定、高效能與容量、多站台位置的複寫與快取、安全性與靈活度。

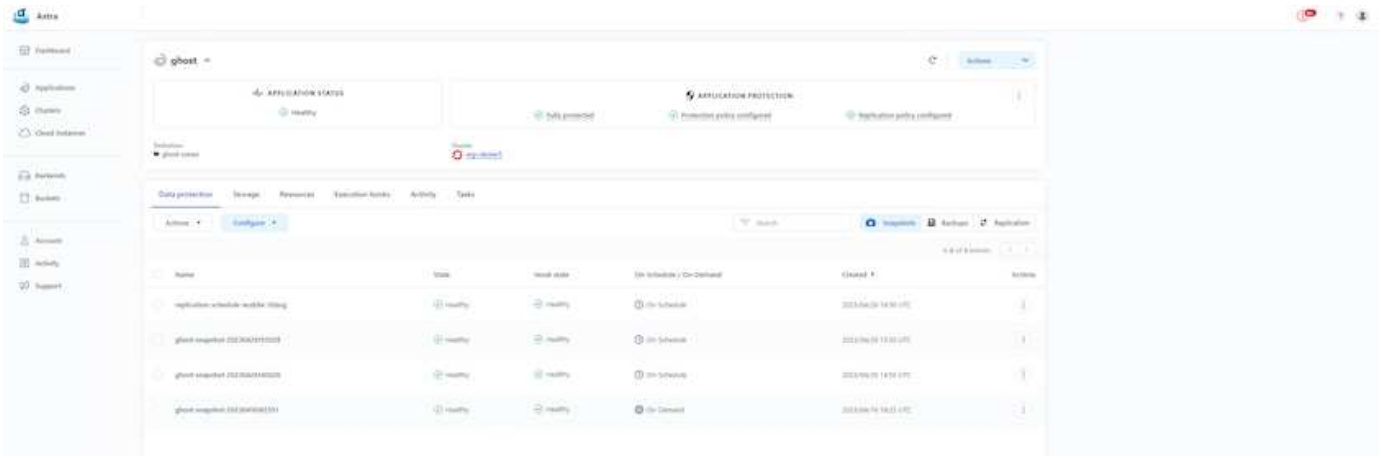
ONTAP 中的資料保護可以使用臨機操作或原則控制的方式來達成 - 快照 - 備份與還原

Snapshot 複本和備份都能保護下列資料類型： - 代表應用程式狀態的應用程式中繼資料 - 任何與應用程式相關的持續資料磁碟區 - 屬於應用程式的任何資源成品

使用 **Acc** 快照

使用 Snapshot with Acc 可擷取資料的時間點複本。保護原則定義要保留的 Snapshot 複本數量。最低排程選項為每小時一次。您可以隨時以比排程 Snapshot 複本更短的時間間隔來進行手動隨選 Snapshot 複本。Snapshot 複本會儲存在與應用程式相同的已佈建磁碟區上。

使用 **Acc** 設定 **Snapshot**



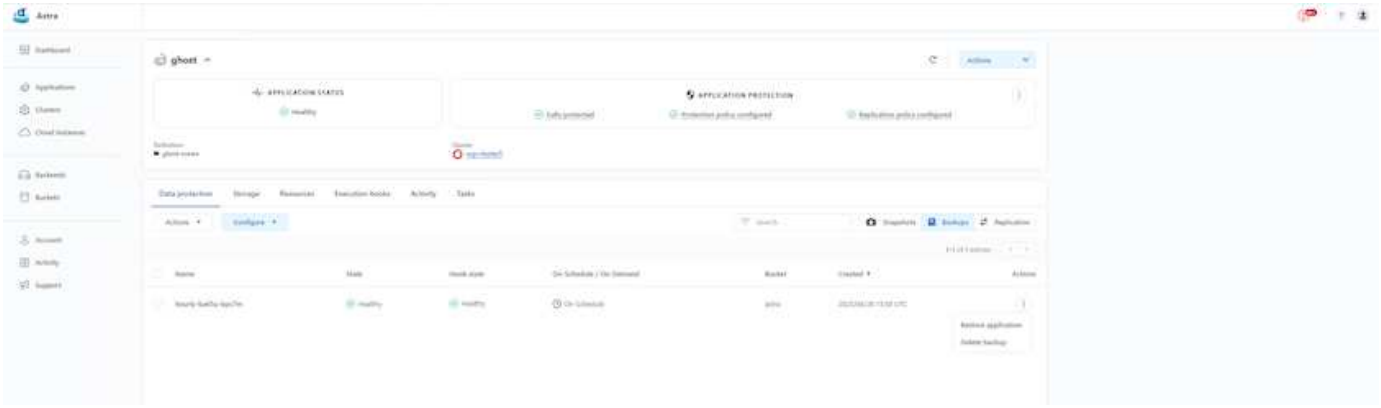
使用 **Acc** 進行備份與還原

備份是以 Snapshot 為基礎。主動定速控制系統可以使用 CSI 來製作 Snapshot 複本、並使用時間點 Snapshot 複本來執行備份。備份會儲存在外部物件存放區（任何相容的 S3 、包括位於不同位置的 ONTAP S3 ）。您可

以針對排程備份和要保留的備份版本數量、設定保護原則。最小 RPO 為一小時。

使用 **Acc** 從備份還原應用程式

主動定速控制系統會從儲存備份的 S3 儲存區還原應用程式。



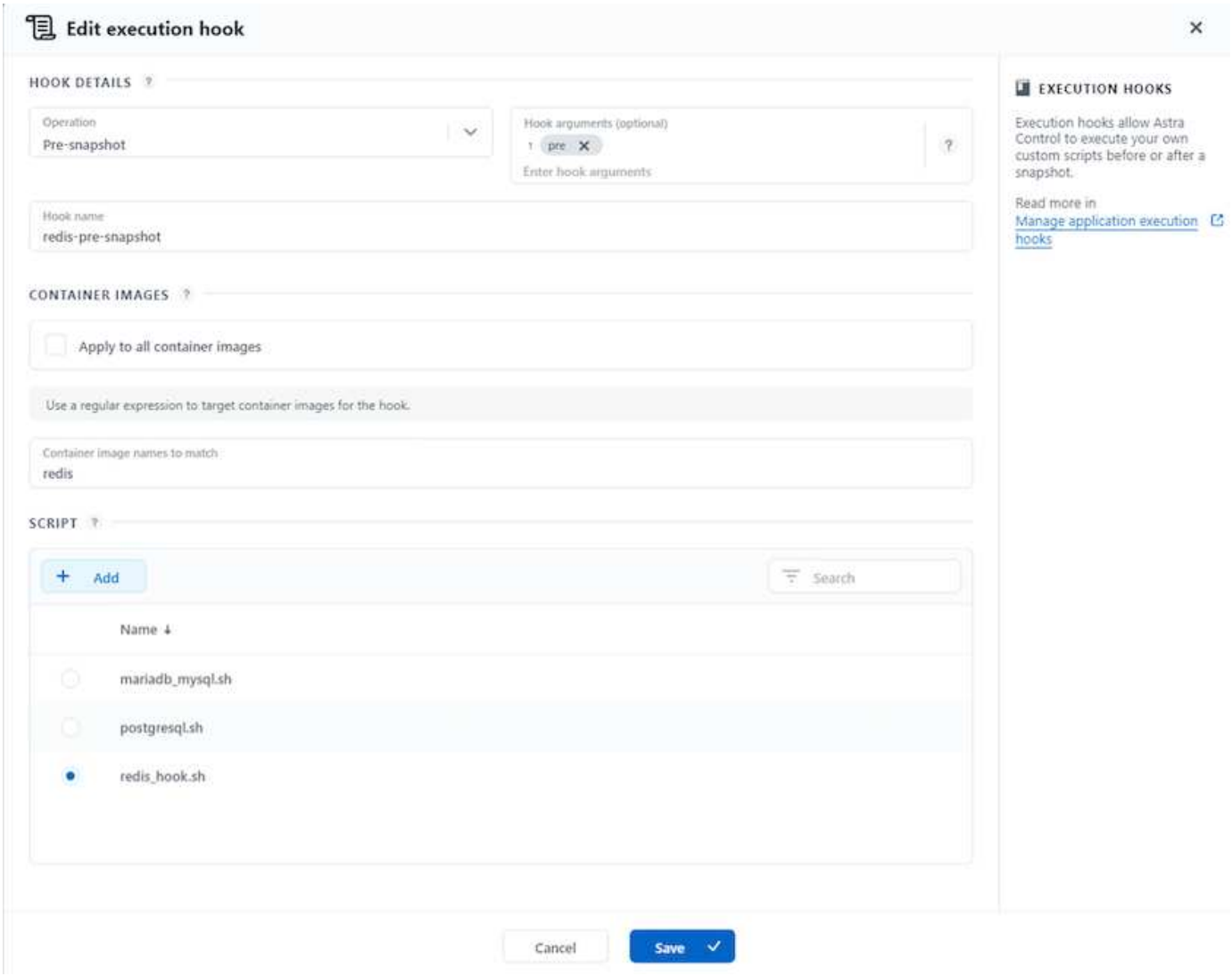
應用程式特定的執行攔截器

此外、執行攔截器可設定為與託管應用程式的資料保護作業一起執行。雖然儲存陣列層級的資料保護功能可供使用、但通常需要額外的步驟才能使備份與還原作業一致。應用程式專屬的其他步驟可能是：建立 Snapshot 複本之前或之後。- 建立備份之前或之後。從 Snapshot 複本或備份還原之後。

Astra Control 可以執行這些應用程式專屬步驟、這些步驟編碼為稱為執行攔截程式的自訂指令碼。

"NetApp Verda GitHub專案" 提供常用雲端原生應用程式的執行掛鉤、讓保護應用程式變得簡單、強大且易於協調。如果您有足夠的資訊可用於儲存庫中未包含的應用程式、請隨時為該專案做出貢獻。

Redis 應用程式快照前的執行掛鉤範例。



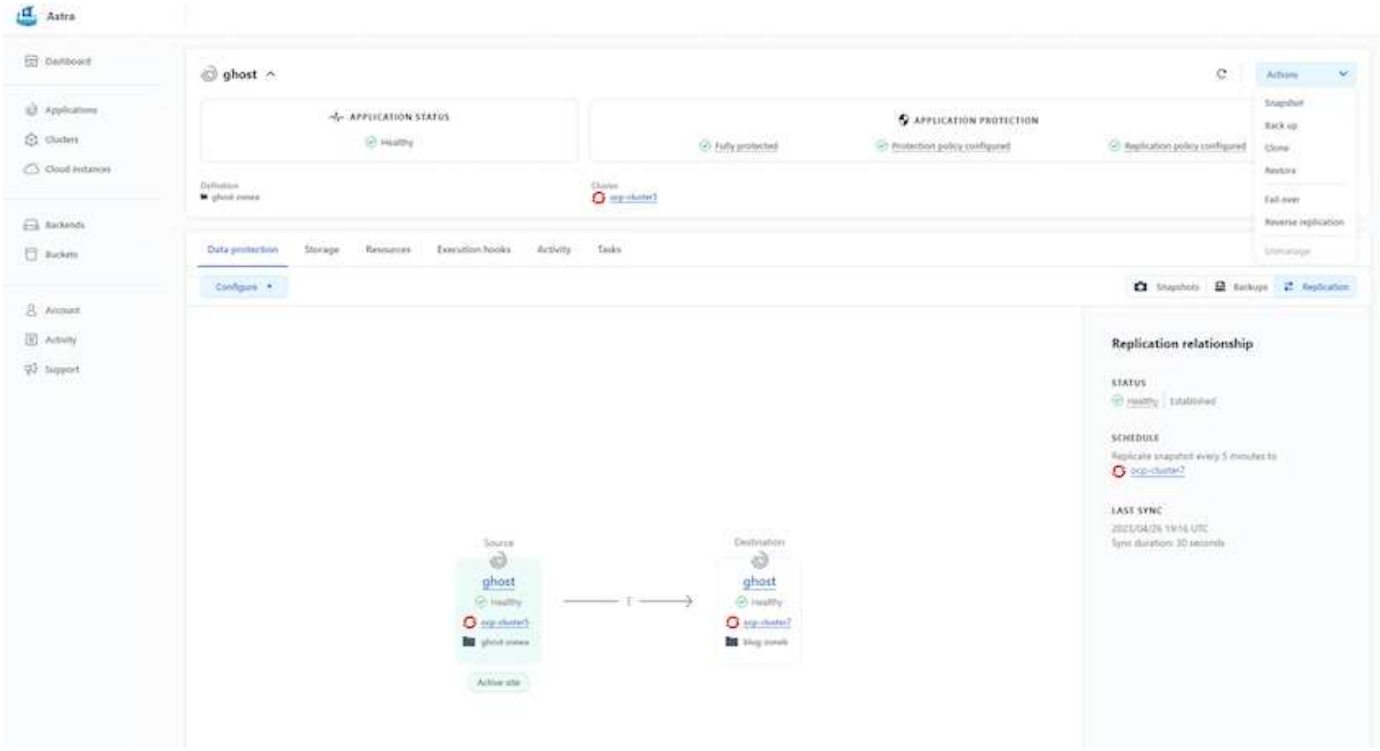
使用 **Acc** 進行複寫

為了提供區域保護、或是採用低 RPO 和 RTO 解決方案、應用程式可以複寫到另一個在不同站台上執行的 Kubernetes 執行個體、最好是在其他區域。主動定速控制系統採用 ONTAP 非同步 SnapMirror 、 RPO 最短可達 5 分鐘。複寫是透過複寫到 ONTAP 、然後容錯移轉會在目的地叢集中建立 Kubernetes 資源。

請注意、複寫與備份移至 S3 並從 S3 執行還原的備份與還原不同。請參閱連結： here 以取得兩種資料保護類型之間差異的其他詳細資料。

請參閱 "請按這裡" SnapMirror 安裝說明。

SnapMirror 搭配 **Acc**



SAN 經濟型和 NAS 經濟型儲存驅動程式不支援複寫功能。請參閱 "請按這裡" 以取得更多詳細資料。

示範影片：

"Astra Control Center 的災難恢復示範影片"

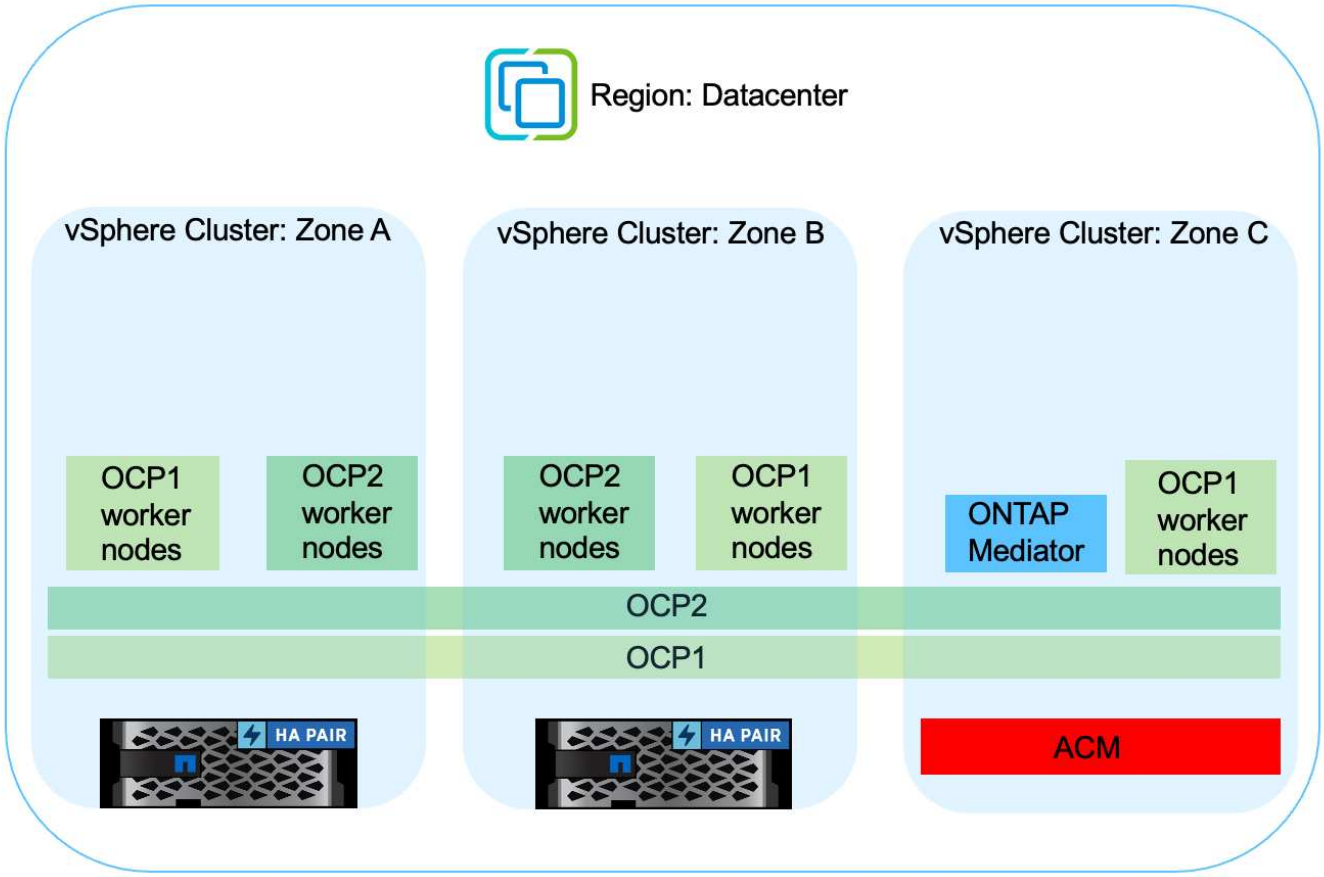
Astra Control Center 提供資料保護功能

使用 **MetroCluster** 實現營運不中斷

我們的 ONTAP 硬體平台大多具備高可用度功能、可防止裝置故障、避免執行災難恢復。但為了防範火災或任何其他災難、並以零 RPO 和低 RTO 持續經營業務、通常會使用 MetroCluster 解決方案。

目前擁有 ONTAP 系統的客戶可在提供區域層級災難恢復的距離限制內新增支援的 ONTAP 系統、以延伸至 MetroCluster 。Astra Trident 、 CSI （ Container 儲存介面）支援 NetApp ONTAP 、包括 MetroCluster 組態、以及其他選項、例如 Cloud Volumes ONTAP 、 Azure NetApp Files 、 AWS FSX for NetApp ONTAP 等 Astra Trident 提供五種 ONTAP 儲存驅動程式選項、所有選項都支援 MetroCluster 組態。請參閱 "請按這裡" 如需 Astra Trident 支援的 ONTAP 儲存驅動程式的詳細資訊、請參閱。

MetroCluster 解決方案需要第 2 層網路擴充功能、或從兩個故障網域存取相同的網路位址。一旦 MetroCluster 組態就緒、應用程式擁有者就能清楚瞭解解決方案、因為 MetroCluster SVM 中的所有磁碟區都受到保護、並享有 SyncMirror （零 RPO ）的優勢。



對於 Trident 後端組態（ TBC ）、使用 MetroCluster 組態時、請勿指定 dataLIF 和 SVM 。指定用於管理 LIF 的 SVM 管理 IP 、並使用 vsadmin 角色認證。

我們提供 Astra Control Center 資料保護功能的詳細資訊 "請按這裡"

使用 **Astra Control Center** 進行資料移轉

此頁面顯示 Red Hat OpenShift 叢集搭配 Astra Control Center （ACC）的容器工作負載資料移轉選項。

Kubernetes 應用程式通常需要從一個環境移至另一個環境。若要移轉應用程式及其持續資料、可以使用 NetApp ACC 。

不同 **Kubernetes** 環境之間的資料移轉

ACC 支援各種 Kubernetes 口味、包括 Google Anthos 、 Red Hat OpenShift 、 Tanzu Kubernetes Grid 、 Rancher Kubernetes Engine 、上游 Kubernetes 、 等 如需其他詳細資料、請參閱 "請按這裡"。

若要將應用程式從一個叢集移轉至另一個叢集、您可以使用下列 Acc 功能之一：

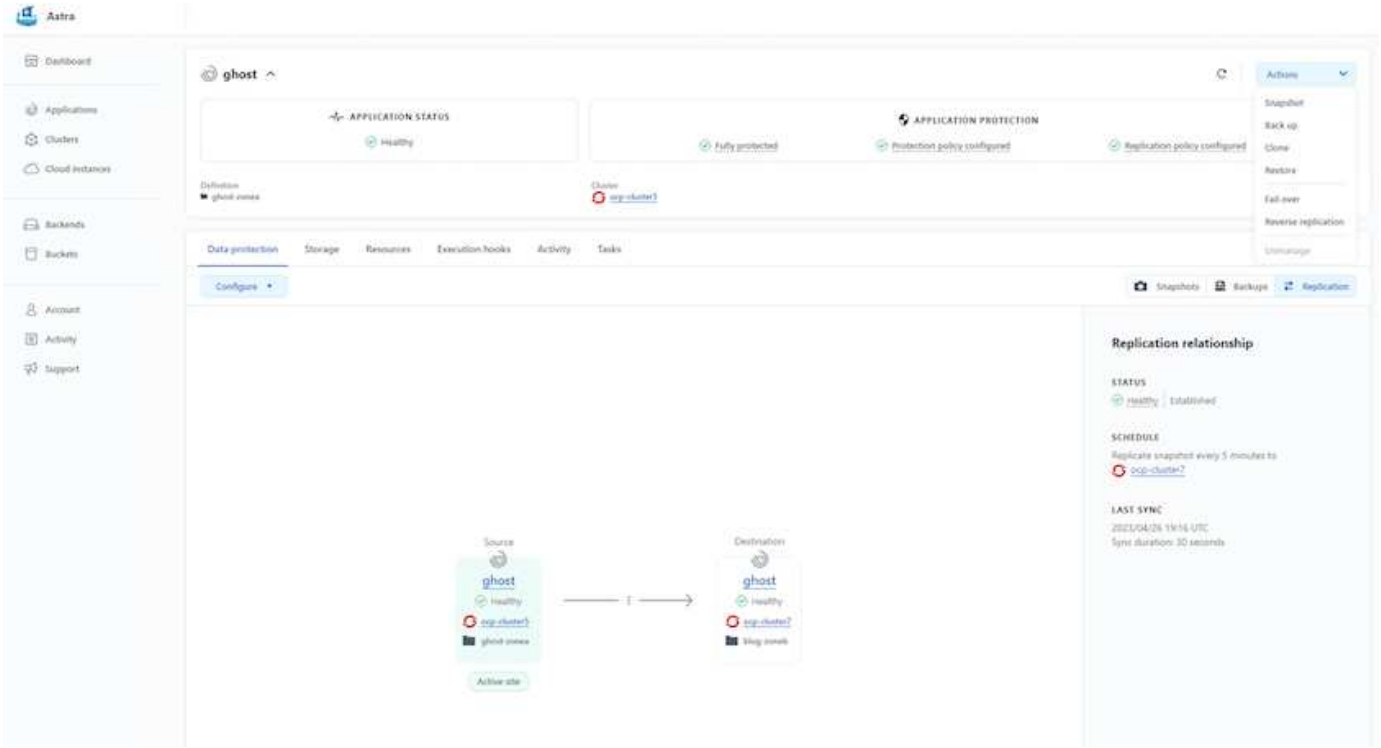
- 複寫
- 備份與還原
- 複製

請參閱 "資料保護區段" 適用於 複寫與備份與還原 選項。

請參閱 "請按這裡" 如需關於 複製的其他詳細資料 。

Astra Replication 功能僅支援 Trident Container Storage Interface （ CSI ）。不過、 NAS 經濟型和 SAN 經濟型驅動程式不支援複寫。

使用 **Acc** 執行資料複寫



適用於 **Red Hat OpenShift Container** 工作負載的 **NetApp** 混合式多雲端解決方案

總覽

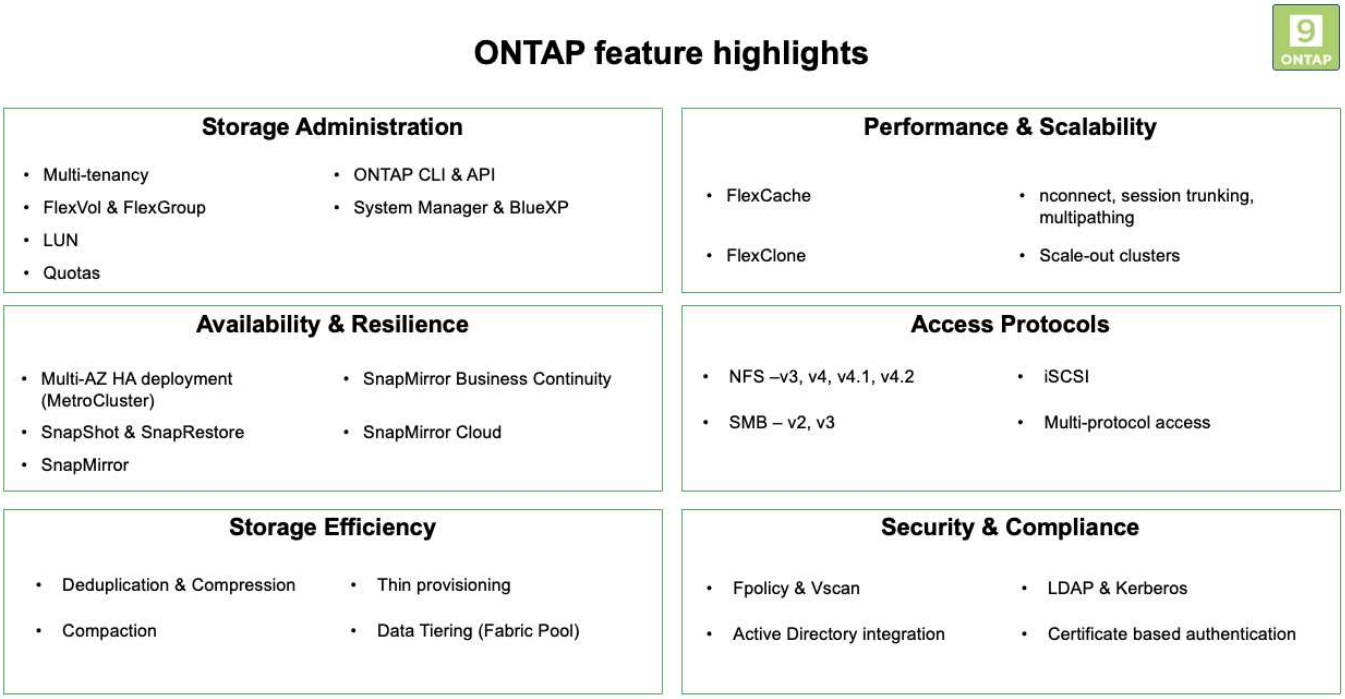
NetApp 發現客戶使用 Kubernetes 建置的容器和協調作業平台、將舊有企業應用程式現代化、並建置新的應用程式。Red Hat OpenShift Container Platform 是我們許多客戶採用的範例之一。

隨著越來越多客戶開始在企業內採用容器、 NetApp 的定位非常完美、可協助滿足其有狀態應用程式的持續儲存需求、以及資料保護、資料安全性和資料移轉等傳統資料管理需求。不過、這些需求是使用不同的策略、工具和方法來滿足的。

以 NetApp ONTAP * 為基礎的儲存選項如下所列、可為容器和 Kubernetes 部署提供安全性、資料保護、可靠性和靈活度。

- 內部部署的自我管理儲存設備：
  - NetApp Fabric 附加儲存設備（ FAS ）、 NetApp All Flash FAS Array （ AFF ）、 NetApp All SAN Array （ ASA ）和 ONTAP Select
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（ STaaS ）

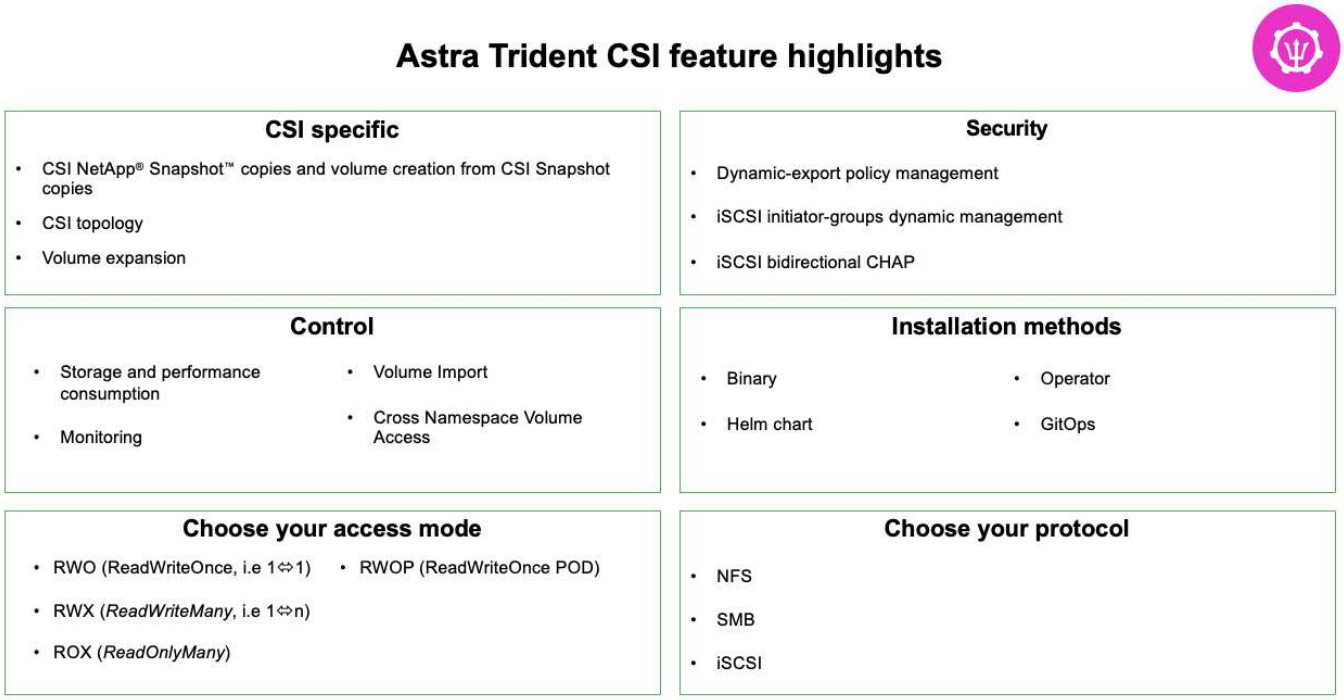
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （ CVO ）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：
  - Cloud Volumes Service for Google Cloud （ CVS ）、 Azure NetApp Files （ anf ）、 Amazon FSX for NetApp ONTAP 可在超大型擴充器中提供完全託管的儲存設備



- NetApp BlueXP** 可讓您從單一控制平面 / 介面管理所有儲存設備和資料資產。

您可以使用 BlueXP 來建立和管理雲端儲存設備（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 Astra Trident * 是符合 CSI 標準的 Storage Orchestrator 、可快速輕鬆地使用由上述各種 NetApp 儲存選項作為後盾的持續儲存設備。這是由 NetApp 維護和支援的開放原始碼軟體。



業務關鍵容器工作負載不只需要持續的磁碟區、他們的資料管理需求也需要保護及移轉應用程式 Kubernetes 物件。

> 應用程式資料除了包含使用者資料外、還包括 Kubernetes 物件：以下是一些範例： - Kubernetes 物件、例如 Pod 規格、 PVC 、部署、服務 - 自訂組態物件、例如組態對應和機密 - 持續性資料、例如 Snapshot 複本、備份、複本 - 自訂資源、例如 CRS 和 CRD

- NetApp Astra Control** 可作為完全託管和自我管理的軟體使用、可協調功能以提供健全的應用程式資料管理。請參閱 "Astra文件" 如需 Astra 系列產品的詳細資訊、請參閱。

本參考文件提供移轉與保護容器型應用程式的驗證、這些應用程式部署在 RedHat OpenShift Container 平台上、並使用 NetApp Astra Control Center 。此外、此解決方案還提供部署和使用 Red Hat Advanced Cluster Management （ACM）來管理容器平台的高階詳細資料。本文件也重點介紹使用 Astra Trident CSI 資源配置程式、將 NetApp 儲存設備與 Red Hat OpenShift 容器平台整合的詳細資料。Astra Control Center 部署在集線器叢集上、用於管理容器應用程式及其持續儲存生命週期。最後、它為 AWS （ROSA）中受管理 Red Hat OpenShift 叢集上的容器工作負載提供複寫和容錯移轉及容錯移轉解決方案、使用 Amazon FSx for NetApp ONTAP （FSxN）作為持續儲存設備。

採用混合雲的 **Red Hat OpenShift Container** 平台工作負載的 **NetApp** 解決方案

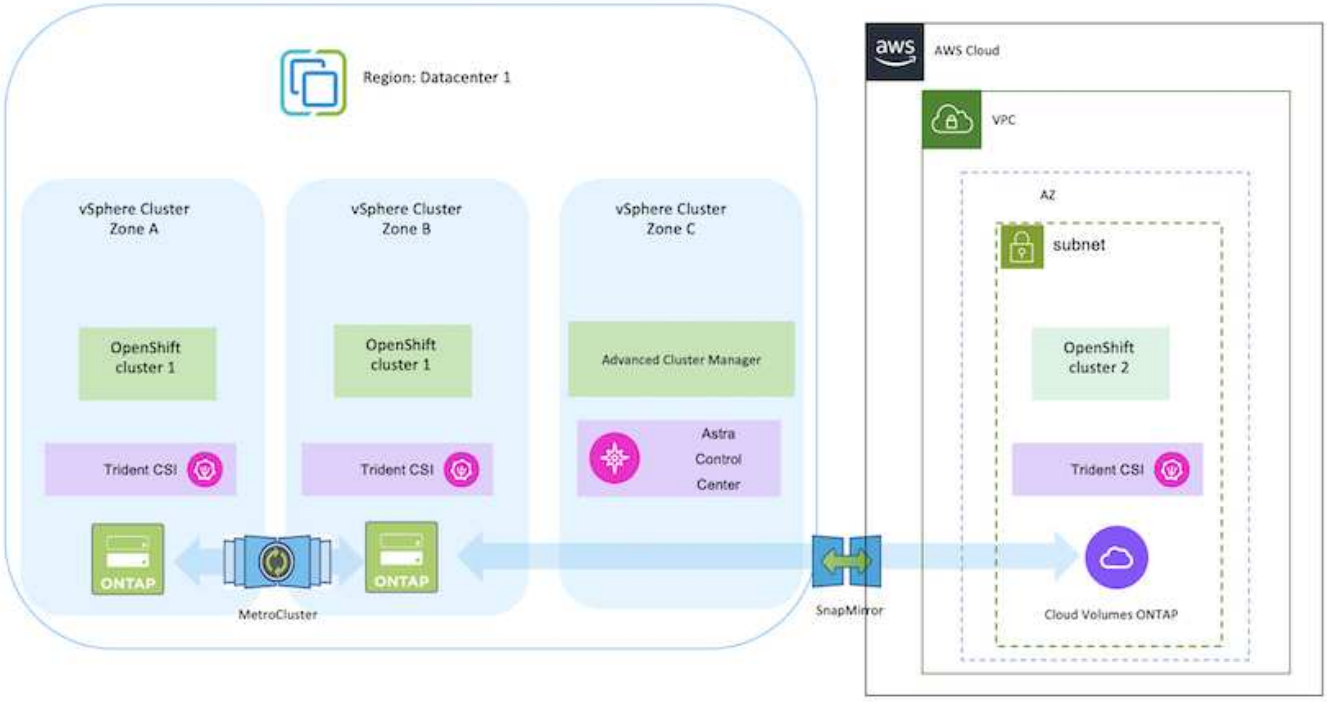
當客戶準備好將某些特定工作負載或所有工作負載從資料中心移至雲端時、他們可能正處於現代化過程的某個階段。他們可能會基於各種原因、選擇在雲端使用自我管理的 OpenShift 容器和自我管理的 NetApp 儲存設備。他們應該規劃並部署雲端中的 Red Hat OpenShift Container 平台（OCP）、以打造成功的正式作業環境、從資料中心移轉其容器工作負載。他們的 OCP 叢集可以部署在 VMware 或裸機上的資料中心、以及雲端環境中的 AWS 、 Azure 或 Google Cloud 上。

NetApp Cloud Volumes ONTAP 儲存設備可為 AWS 、 Azure 和 Google Cloud 中的容器部署提供資料保護、可靠性和靈活度。Astra Trident 是動態儲存資源配置程式、可為客戶的有狀態應用程式使用持續的 Cloud Volumes ONTAP 儲存設備。Astra Control Center 可用來協調有狀態應用程式的許多資料管理需求、例如資料保護、移轉

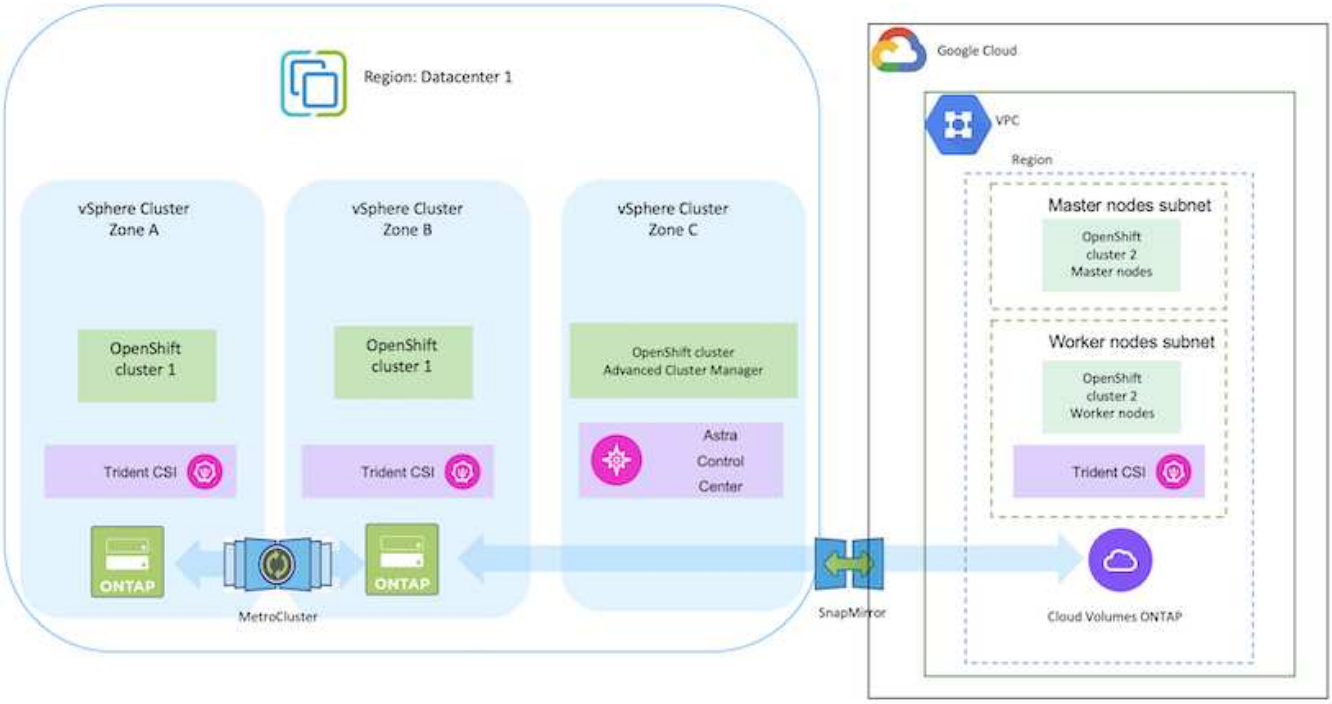
和業務持續運作。

使用 **Astra Control Center** 在混合雲中為 **OpenShift Container** 工作負載提供資料保護與移轉解決方案

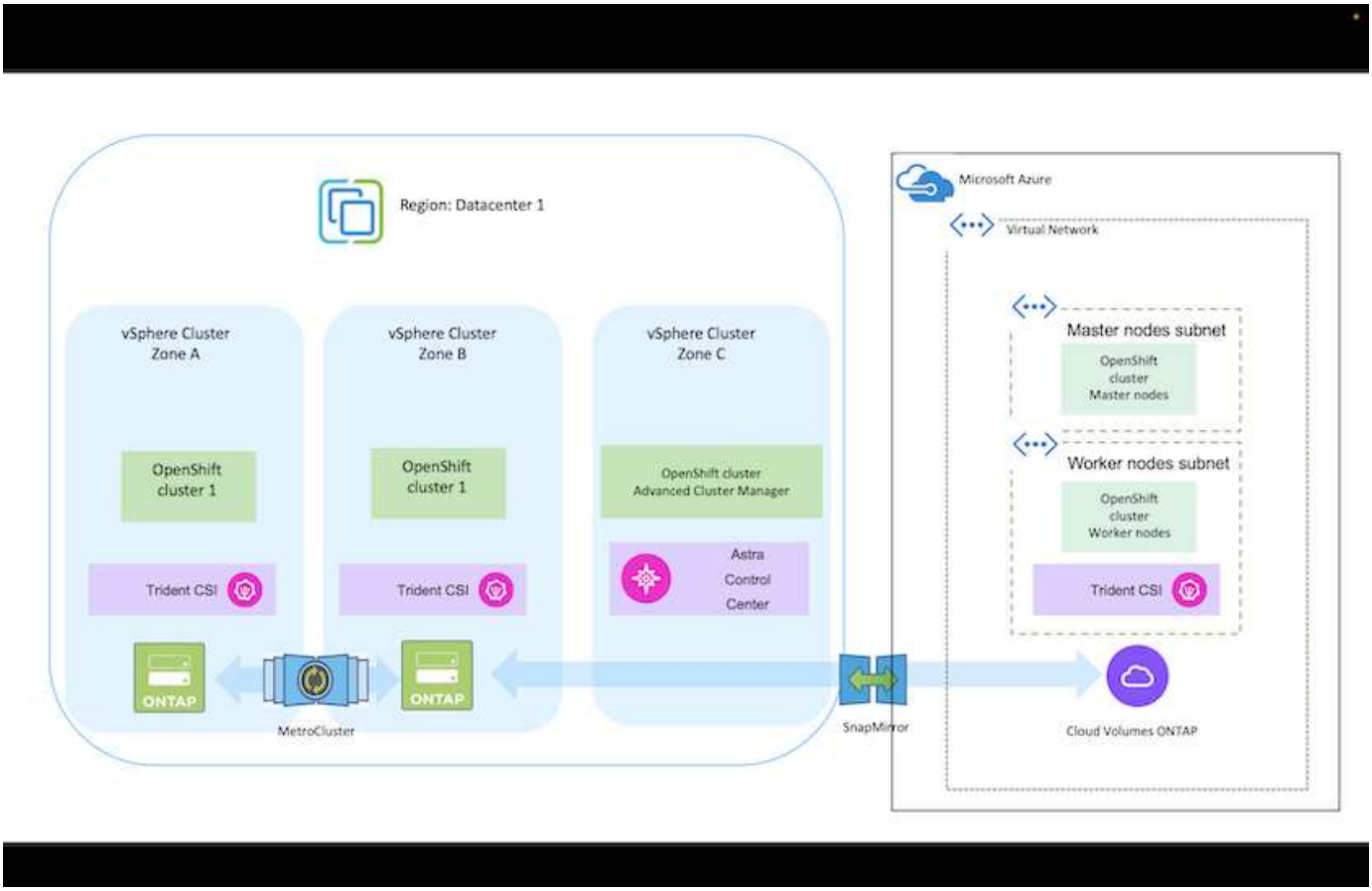
內部部署和 AWS



內部部署和 Google Cloud



內部部署與 Azure Cloud

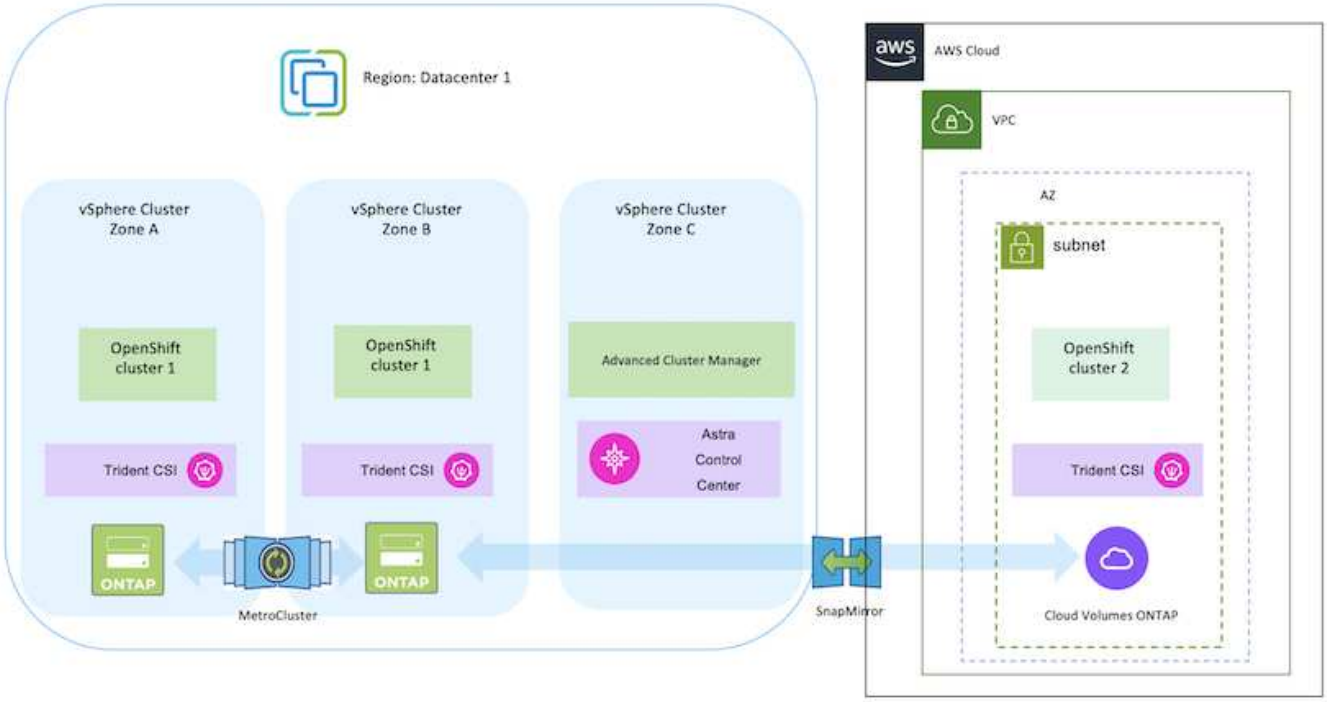


在 **AWS** 上部署和設定 **Red Hat OpenShift Container** 平台

本節說明如何在 AWS 中設定和管理 OpenShift 叢集、以及在叢集上部署有狀態應用程式的高階工作流程。它顯示在 Astra Trident 協助下使用 NetApp Cloud Volumes ONTAP 儲存設備來提供持續的磁碟區。詳細說明如何使用 Astra Control Center 來執行有狀態應用程式的資料保護和移轉活動。

在 AWS 上部署 Red Hat OpenShift Container 平台叢集有多種方法。此設定的高階說明提供所使用特定方法的文件連結。您可以參閱中提供的相關連結中的其他方法 "資源區段"。

下圖說明在 AWS 上部署並使用 VPN 連線至資料中心的叢集。



設定程序可分為下列步驟：

從進階叢集管理在 **AWS** 上安裝 **OCP** 叢集。

- 使用站台對站台 VPN 連線（使用 pfSense ）建立 VPC 以連線至內部部署網路。
- 內部網路具備網際網路連線能力。
- 在 3 個不同的 AZs 中建立 3 個子網路。
- 為 VPC 建立路由 53 私有代管區域和 DNS 解析程式。

從進階叢集管理（ACM ）精靈在 AWS 上建立 OpenShift 叢集。請參閱指示 "請按這裡"。

您也可以從 OpenShift 混合雲主控台在 AWS 中建立叢集。請參閱 "請按這裡" 以取得相關指示。

使用 ACM 建立叢集時、您可以在表單檢視中填入詳細資料後、編輯 yaml 檔案、以自訂安裝。建立叢集之後、您可以 ssh 登入叢集的節點進行疑難排解或其他手動設定。請使用您在安裝期間提供的 ssh 金鑰和使用者名稱核心來登入。

使用 **BlueXP** 在 **AWS** 中部署 **Cloud Volumes ONTAP** 。

- 在內部部署的 VMware 環境中安裝連接器。請參閱指示 "請按這裡"。
- 使用連接器在 AWS 中部署 CVO 執行個體。請參閱指示 "請按這裡"。

連接器也可以安裝在雲端環境中。請參閱 "請按這裡" 以取得更多資訊。

在 **OCP** 叢集中安裝 **Astra Trident**

- 使用 Helm 部署 Trident 操作員。請參閱指示 "請按這裡"
- 建立後端和儲存類別。請參閱指示 "請按這裡"。

將 **AWS** 上的 **OCP** 叢集新增至 **Astra Control Center** 。

將 AWS 中的 OCP 叢集新增至 Astra Control Center 。

在多區域架構中使用 **Trident** 的 **CSI** 拓撲功能

如今、雲端供應商讓 Kubernetes/OpenShift 叢集管理員能夠為以區域為基礎的叢集建立節點。節點可位於某個區域內的不同可用度區域、或位於不同區域之間。為了協助在多區域架構中配置工作負載的磁碟區、Astra Trident使用了csi拓撲。使用「csi拓撲」功能、可根據區域和可用性區域、限制對磁碟區的存取、只能存取一部分節點。請參閱 "請按這裡" 以取得更多詳細資料。

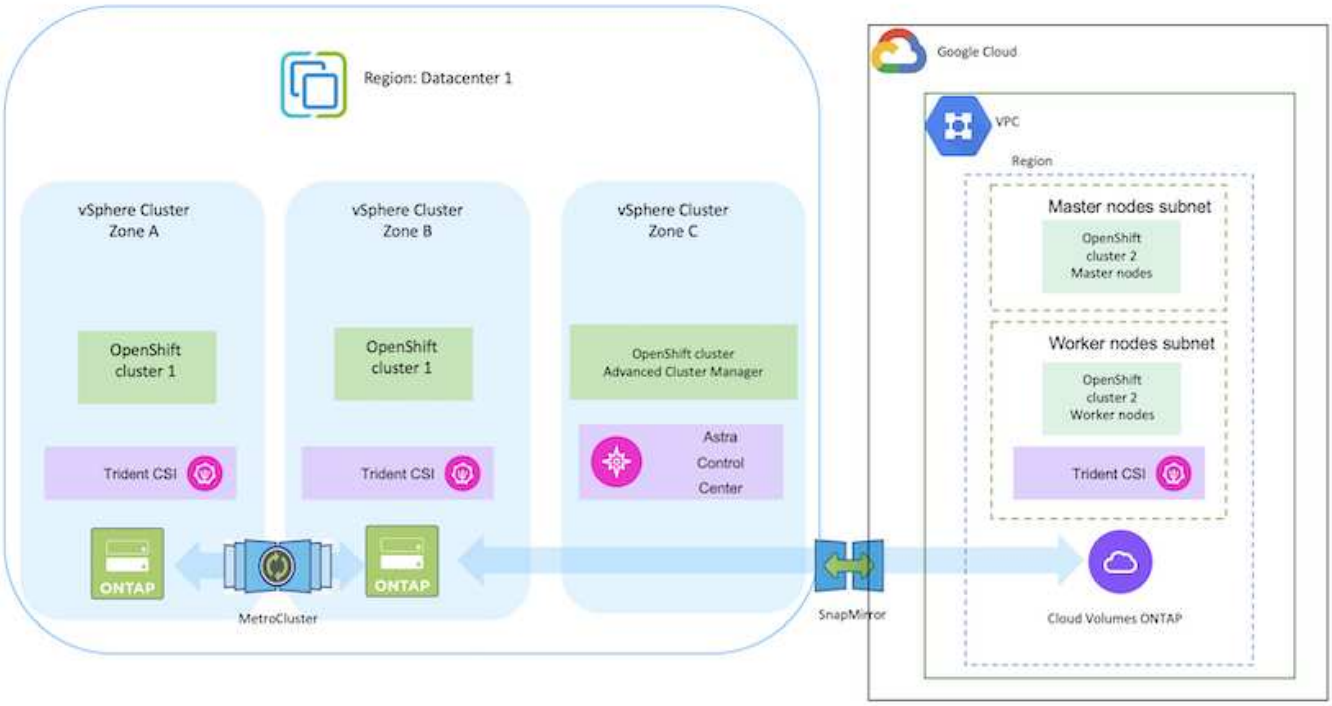
Kubernetes 支援兩種磁碟區繫結模式： - 當 ***Volume BindingMode*** 設為 ***Immediate*** （預設）時、 Astra Trident 會在沒有任何拓撲感知的情況下建立磁碟區。建立永續性磁碟區時、不會對要求的Pod排程需求有任何相依性。- 當 ***Volume BindingMode*** 設定為 **_WaitForFirstConsumer**（客戶） 時、永久 Volume 的建立與繫結將延遲、直到排程並建立使用 PVC 的 Pod 為止。如此一來、就能建立磁碟區、以符合拓撲需求所強制執行的排程限制。Astra Trident 儲存後端可根據可用性區域（可識別拓撲的後端）、選擇性地配置磁碟區。對於使用此類後端的StorageClass、只有在受支援地區/區域中排程的應用程式要求時、才會建立Volume。（可識別拓撲的StorageClass ）請參閱 "請按這裡" 以取得更多詳細資料。

在 **GCP** 上部署和設定 **Red Hat OpenShift Container** 平台

在 **GCP** 上部署和設定 **Red Hat OpenShift Container** 平台

本節說明如何在 GCP 中設定及管理 OpenShift 叢集、以及在其中部署有狀態應用程式的高階工作流程。它顯示在 Astra Trident 協助下使用 NetApp Cloud Volumes ONTAP 儲存設備來提供持續的磁碟區。詳細說明如何使用 Astra Control Center 來執行有狀態應用程式的資料保護和移轉活動。

下圖顯示了在 GCP 上部署並使用 VPN 連線至資料中心的叢集。



在 GCP 中部署 Red Hat OpenShift Container 平台叢集有多種方法。此設定的高階說明提供所使用特定方法的文件連結。您可以參閱中提供的相關連結中的其他方法 "資源區段"。

設定程序可分為下列步驟：

從 **CLI** 在 **GCP** 上安裝 **OCP** 叢集。

- 請確定您已符合上述所有先決條件 "請按這裡"。
- 針對內部部署與 GCP 之間的 VPN 連線、我們建立並設定了 pfSense VM 。如需相關指示、請參閱 "請按這裡"。
  - 只有在 Google Cloud Platform 中建立 VPN 閘道之後、才能在 pfSense 中設定遠端閘道位址。
  - 只有在 OpenShift 叢集安裝程式執行並建立叢集的基礎架構元件之後、才能設定階段 2 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之後、才能在 Google Cloud 中設定 VPN 。
- 現在在 GCP 上安裝 OpenShift 叢集。
  - 請取得安裝程式和抽取密碼、並依照文件中所提供的步驟部署叢集 "請按這裡"。
  - 安裝作業會在 Google Cloud Platform 中建立 VPC 網路。它也會在 Cloud DNS 中建立私有區域、並新增記錄。
    - 使用 VPC 網路的 CIDR 區塊位址來設定 pfSense 並建立 VPN 連線。確保防火牆設定正確。
    - 使用 Google Cloud DNS A 記錄中的 IP 位址、在內部部署環境的 DNS 中新增記錄。
  - 叢集安裝完成、並將提供一個 kubeconfig 檔案、使用者名稱和密碼、以登入叢集的主控台。

使用 **BlueXP** 在 **GCP** 中部署 **Cloud Volumes ONTAP** 。

- 在 Google Cloud 中安裝 Connector 。請參閱指示 "請按這裡"。
- 使用 Connector 在 Google Cloud 中部署 CVO 執行個體。請參閱此處的指示。 https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

在 **GCP** 的 **OCP** 叢集中安裝 **Astra Trident**

- 如圖所示、部署 Astra Trident 有許多方法 "請按這裡"。
- 針對此專案、 Astra Trident 是依照指示手動部署 Astra Trident 操作員來安裝 "請按這裡"。
- 建立後端和儲存類別。請參閱指示 "請按這裡"。

將 **GCP** 上的 **OCP** 叢集新增至 **Astra Control Center** 。

- 使用叢集角色建立獨立的 KubeConfig 檔案、其中包含 Astra Control 管理叢集所需的最低權限。您可以找到相關指示 "請按這裡"。
- 依照指示將叢集新增至 Astra Control Center "請按這裡"

在多區域架構中使用 **Trident** 的 **CSI** 拓撲功能

如今、雲端供應商讓 Kubernetes/OpenShift 叢集管理員能夠為以區域為基礎的叢集建立節點。節點可位於某個區域內的不同可用度區域、或位於不同區域之間。為了協助在多區域架構中配置工作負載的磁碟區、Astra Trident使用了csi拓撲。使用「csi拓撲」功能、可根據區域和可用性區域、限制對磁碟區的存取、只能存取一部分節點。請參閱 "請按這裡" 以取得更多詳細資料。

Kubernetes 支援兩種磁碟區繫結模式： - 當 ***Volume BindingMode*** 設為 ***Immediate*** （預設）時、 Astra Trident 會在沒有任何拓撲感知的情況下建立磁碟區。建立永續性磁碟區時、不會對要求的Pod排程需求有任何相依性。- 當 ***Volume BindingMode*** 設定為 **_WaitForFirstConsumer**（客戶） 時、永久 Volume 的建立與繫結將延遲、直到排程並建立使用 PVC 的 Pod 為止。如此一來、就能建立磁碟區、以符合拓撲需求所強制執行的排程限制。Astra Trident 儲存後端可根據可用性區域（可識別拓撲的後端）、選擇性地配置磁碟區。對於使用此類後端的StorageClass、只有在受支援地區/區域中排程的應用程式要求時、才會建立Volume。（可識別拓撲的StorageClass ）請參閱 "請按這裡" 以取得更多詳細資料。

[底線]#* 示範影片 * #

在 Google Cloud Platform 上安裝 OpenShift 叢集

將 OpenShift 叢集匯入 Astra Control Center

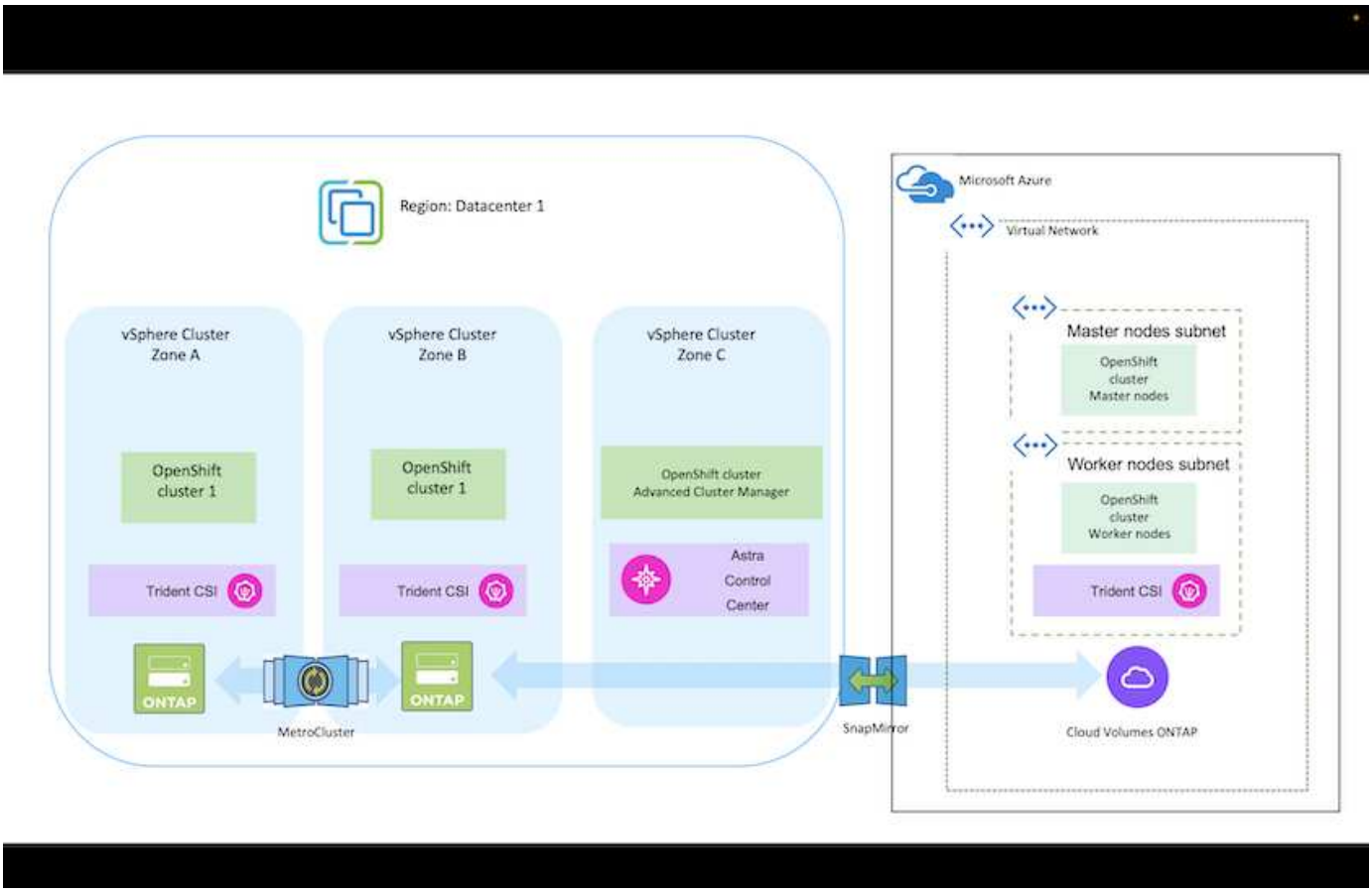
在 **Azure** 上部署及設定 **Red Hat OpenShift Container** 平台

在 **Azure** 上部署及設定 **Red Hat OpenShift Container** 平台

本節說明如何在 Azure 中設定及管理 OpenShift 叢集、以及如何在其中部署有狀態應用程

式的高階工作流程。它顯示在 Astra Trident / Astra 控制資源配置程式的協助下、 NetApp Cloud Volumes ONTAP 儲存設備的使用情形、以提供持續的磁碟區。詳細說明如何使用 Astra Control Center 來執行有狀態應用程式的資料保護和移轉活動。

下圖顯示部署在 Azure 上且使用 VPN 連線至資料中心的叢集。



在 Azure 中部署 Red Hat OpenShift Container 平台叢集有多種方法。此設定的高階說明提供所使用特定方法的文件連結。您可以參閱中提供的相關連結中的其他方法 "資源區段"。

設定程序可分為下列步驟：

從 **CLI** 在 **Azure** 上安裝 **OCP** 叢集。

- 請確定您已符合上述所有先決條件 "請按這裡"。
- 建立 VPN 、子網路和網路安全性群組、以及私有 DNS 區域。建立 VPN 閘道和站台對站台 VPN 連線。
- 針對內部部署與 Azure 之間的 VPN 連線、我們建立並設定了 pfSense VM 。如需相關指示、請參閱 "請按這裡"。
- 請取得安裝程式和抽取密碼、並依照文件中所提供的步驟部署叢集 "請按這裡"。
- 叢集安裝完成、並將提供一個 kubeconfig 檔案、使用者名稱和密碼、以登入叢集的主控台。

下面提供了一個範例 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 **BlueXP** 在 **Azure** 中部署 **Cloud Volumes ONTAP** 。

- 在 Azure 中安裝接頭。請參閱指示 "請按這裡"。
- 使用 Connector 在 Azure 中部署 CVO 執行個體。請參閱指示連結： https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [此處。]

在 **Azure** 的 **OCP** 叢集中安裝 **Astra Control Provisioner**

- 在此專案中、 Astra Control Provisioner （ ACP ）安裝在所有叢集（內部叢集、部署 Astra Control Center 的內部叢集、以及 Azure 中的叢集）上。深入瞭解 Astra Control 資源配置程式 "請按這裡"。
- 建立後端和儲存類別。請參閱指示 "請按這裡"。

將 **Azure** 上的 **OCP** 叢集新增至 **Astra Control Center** 。

- 使用叢集角色建立獨立的 KubeConfig 檔案、其中包含 Astra Control 管理叢集所需的最低權限。您可以找到相關指示 "請按這裡"。
- 依照指示將叢集新增至 Astra Control Center "請按這裡"

在多區域架構中使用 **Trident** 的 **CSI** 拓撲功能

如今、雲端供應商讓 Kubernetes/OpenShift 叢集管理員能夠為以區域為基礎的叢集建立節點。節點可位於某個區域內的不同可用度區域、或位於不同區域之間。為了協助在多區域架構中配置工作負載的磁碟區、Astra Trident使用了csi拓撲。使用「csi拓撲」功能、可根據區域和可用性區域、限制對磁碟區的存取、只能存取一部分節點。請參閱 "請按這裡" 以取得更多詳細資料。

Kubernetes 支援兩種磁碟區繫結模式： - 當 ***Volume BindingMode*** 設為 ***Immediate*** （預設）時、 Astra Trident 會在沒有任何拓撲感知的情況下建立磁碟區。建立永續性磁碟區時、不會對要求的Pod排程需求有任何相依性。- 當 ***Volume BindingMode*** 設定為 **_WaitForFirstConsumer**（客戶） 時、永久 Volume 的建立與繫結將延遲、直到排程並建立使用 PVC 的 Pod 為止。如此一來、就能建立磁碟區、以符合拓撲需求所強制執行的排程限制。Astra Trident 儲存後端可根據可用性區域（可識別拓撲的後端）、選擇性地配置磁碟區。對於使用此類後端的StorageClass、只有在受支援地區/區域中排程的應用程式要求時、才會建立Volume。（可識別拓撲的StorageClass ）請參閱 "請按這裡" 以取得更多詳細資料。

[底線]#* 示範影片 * #

使用 Astra Control 進行應用程式的容錯移轉和容錯回復

使用 **Astra Control Center** 保護資料

此頁面顯示在 VMware vSphere 上或在雲端上使用 Astra Control Center （ ACC ）執行的 Red Hat OpenShift Container 應用程式的資料保護選項。

當使用者使用 Red Hat OpenShift 將應用程式現代化的過程中、應制定資料保護策略、以保護他們不受意外刪除或任何其他人為錯誤的影響。為了保護資料不受萬用者的影響、通常也需要採取保護策略來達到法規或法規遵循的目的。

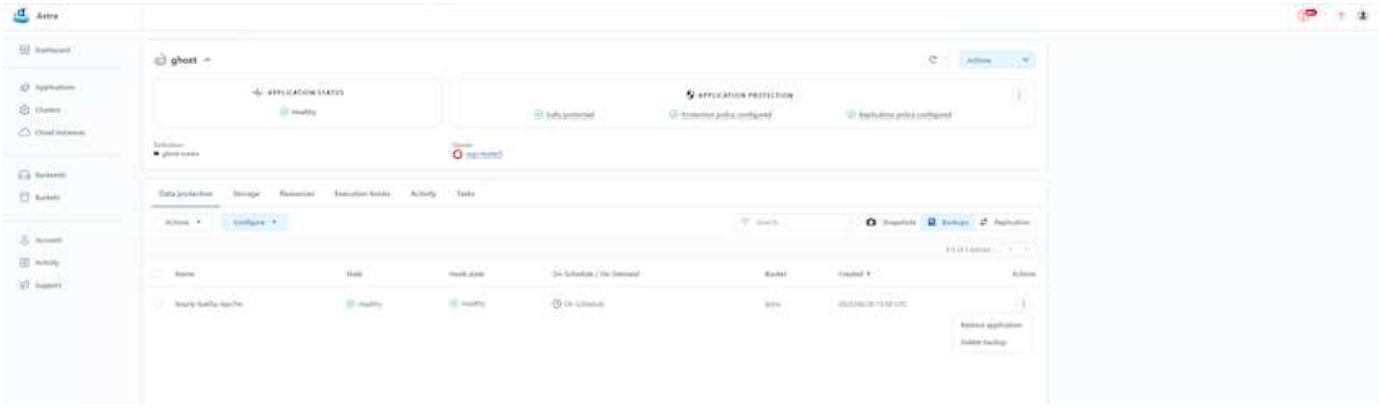
資料保護的需求各不相同、從還原到時間點複本、到自動容錯移轉到不同的故障網域、而無需人為介入。許多客戶選擇 ONTAP 做為其 Kubernetes 應用程式的首選儲存平台、因為其豐富的功能包括多租戶、多重傳輸協定、高效能與容量、多站台位置的複寫與快取、安全性與靈活度。

客戶可能會將雲端環境設定為資料中心擴充、以便充分運用雲端的優勢、並在未來的某個時間、妥善移動工作負載。對於這類客戶而言、將 OpenShift 應用程式及其資料備份到雲端環境是不可避免的選擇。然後、他們可以將應用程式及相關資料還原至雲端或資料中心的 OpenShift 叢集。

使用 **Acc** 進行備份與還原

應用程式擁有者可以檢閱及更新 Acc 探索到的應用程式。主動定速控制系統可以使用 CSI 來製作 Snapshot 複本、並使用時間點 Snapshot 複本來執行備份。備份目的地可以是雲端環境中的物件存放區。您可以針對排程備份和要保留的備份版本數量、設定保護原則。最小 RPO 為一小時。

使用 **Acc** 從備份還原應用程式

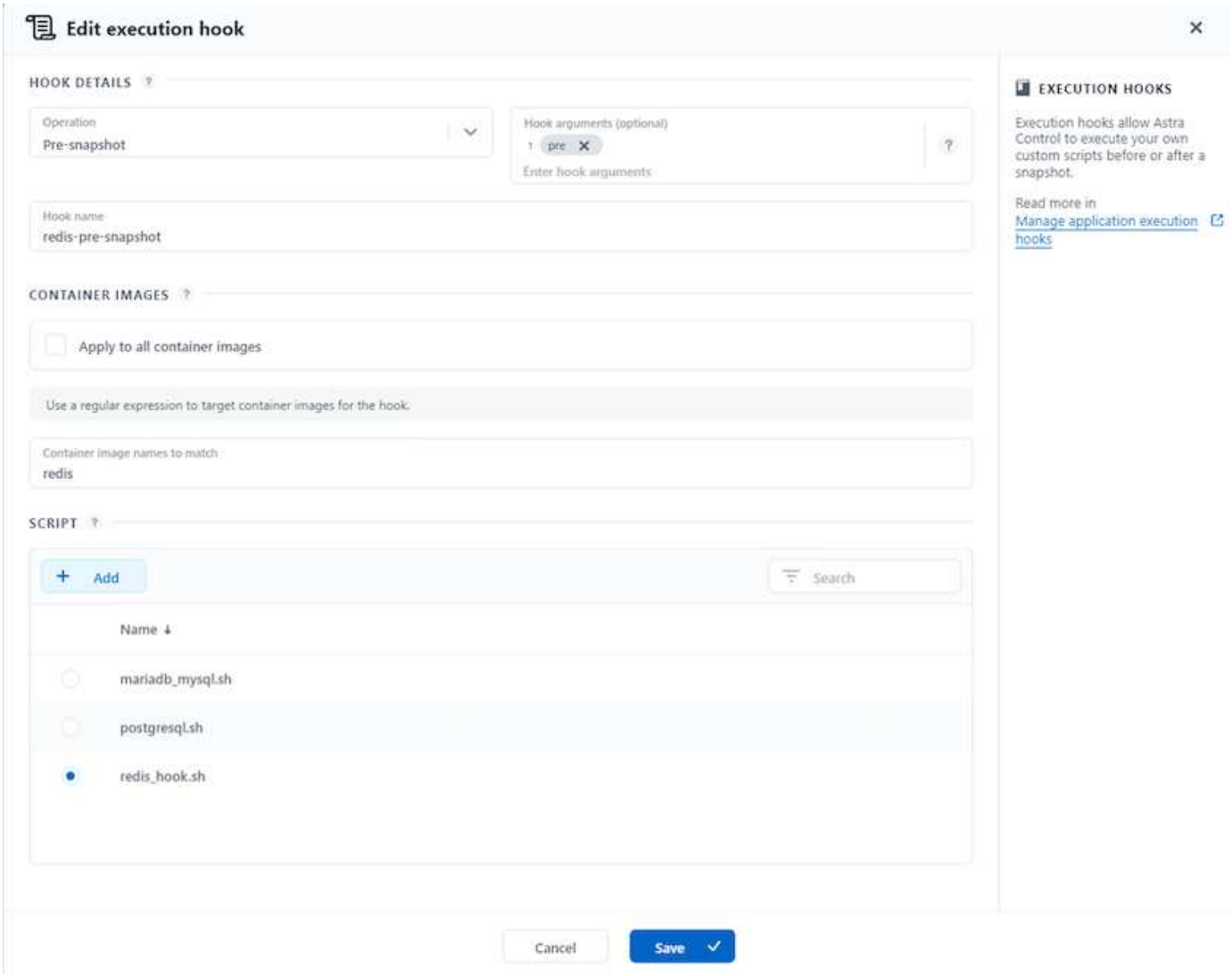


應用程式特定的執行攔截器

雖然儲存陣列層級的資料保護功能可供使用、但通常需要額外的步驟才能使備份和還原應用程式一致。應用程式專屬的其他步驟可能是：建立 Snapshot 複本之前或之後。- 建立備份之前或之後。從 Snapshot 複本或備份還原之後。Astra Control 可以執行這些應用程式專屬步驟、這些步驟編碼為稱為執行攔截程式的自訂指令碼。

NetApp 的 "開放原始碼專案 Verda" 提供常用雲端原生應用程式的執行掛鉤、讓保護應用程式變得簡單、強大且易於協調。如果您有足夠的資訊可用於儲存庫中未包含的應用程式、請隨時為該專案做出貢獻。

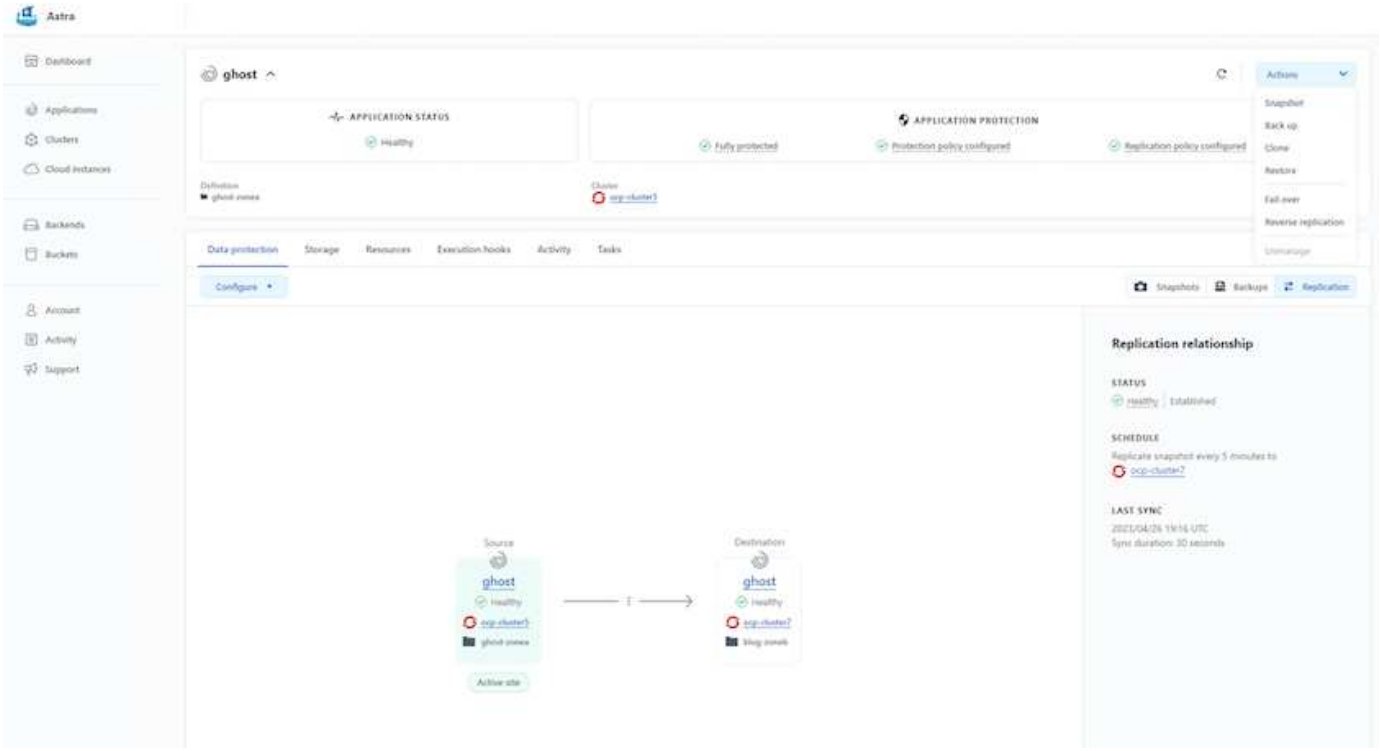
Redis 應用程式快照前的執行掛鉤範例。



使用 **Acc** 進行複寫

為了提供區域保護、或是採用低 RPO 和 RTO 解決方案、應用程式可以複寫到另一個在不同站台上執行的 Kubernetes 執行個體、最好是在其他區域。主動定速控制系統採用 ONTAP 非同步 SnapMirror 、 RPO 最短可達 5 分鐘。請參閱 "請按這裡" SnapMirror 安裝說明。

SnapMirror 搭配 Acc



SAN 經濟型和 NAS 經濟型儲存驅動程式不支援複寫功能。請參閱 "請按這裡" 以取得更多詳細資料。

示範影片：

"Astra Control Center 的災難恢復示範影片"

Astra Control Center 提供資料保護功能

我們提供 Astra Control Center 資料保護功能的詳細資訊 "請按這裡"

災難恢復（使用複寫進行容錯移轉和容錯回復）

使用 Astra Control 進行應用程式的容錯移轉和容錯回復

使用 **Astra Control Center** 進行資料移轉

此頁面顯示 Red Hat OpenShift 叢集搭配 Astra Control Center （ ACC ）的容器工作負載資料移轉選項。特別是、客戶可以使用 ACC 將部分選定的工作負載或所有工作負載從內部部署資料中心移至雲端、將應用程式複製到雲端、以供測試之用、或是從資料中心移至雲端

資料移轉

若要將應用程式從一個環境移轉至另一個環境、您可以使用下列 Acc 功能之一：

- 複寫
- 備份與還原

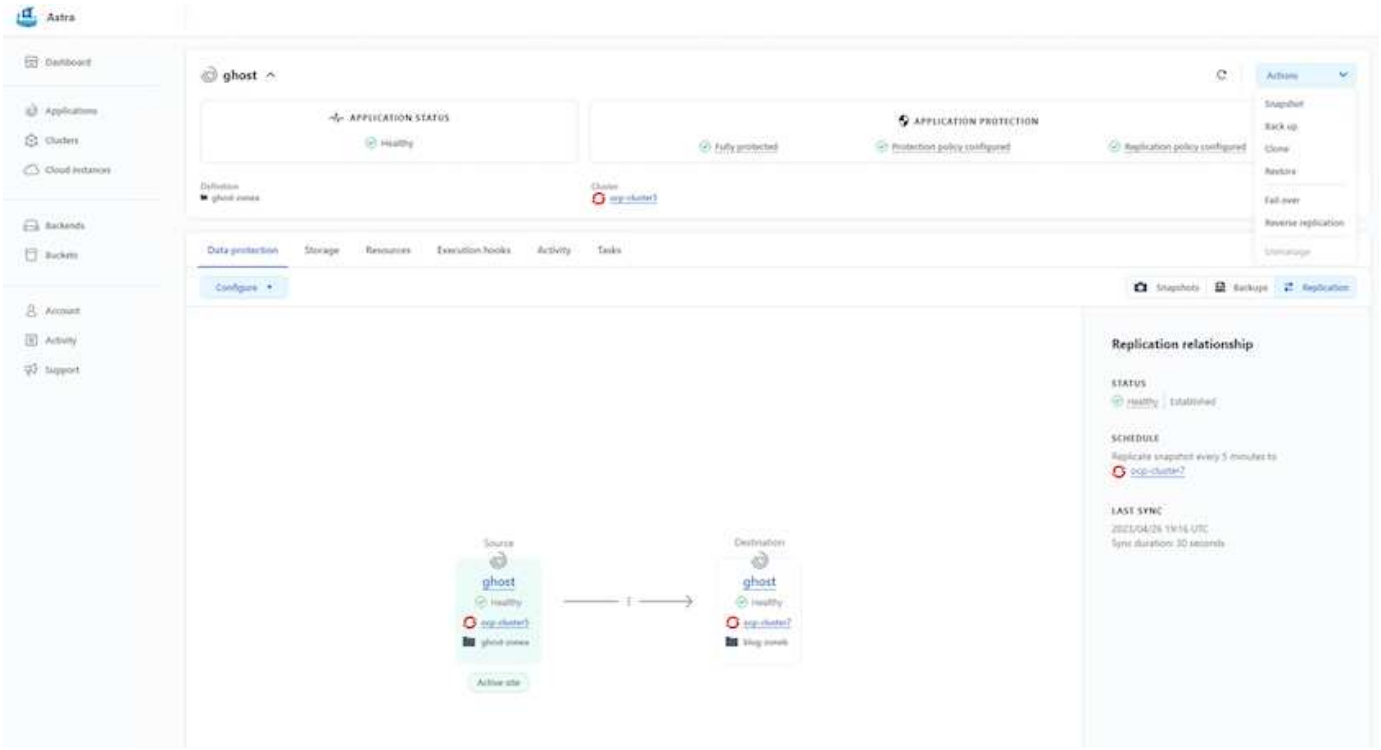
- 複製

請參閱 "資料保護區段" 適用於 複寫與備份與還原 選項。

請參閱 "請按這裡" 如需關於 複製的其他詳細資料 。

> Astra Replication 功能僅支援 Trident Container Storage Interface （CSI）。不過、 NAS 經濟型和 SAN 經濟型驅動程式不支援複寫。

使用 **Acc** 執行資料複寫



適用於 **Red Hat OpenShift Container** 工作負載的 **NetApp** 混合式多雲端解決方案

總覽

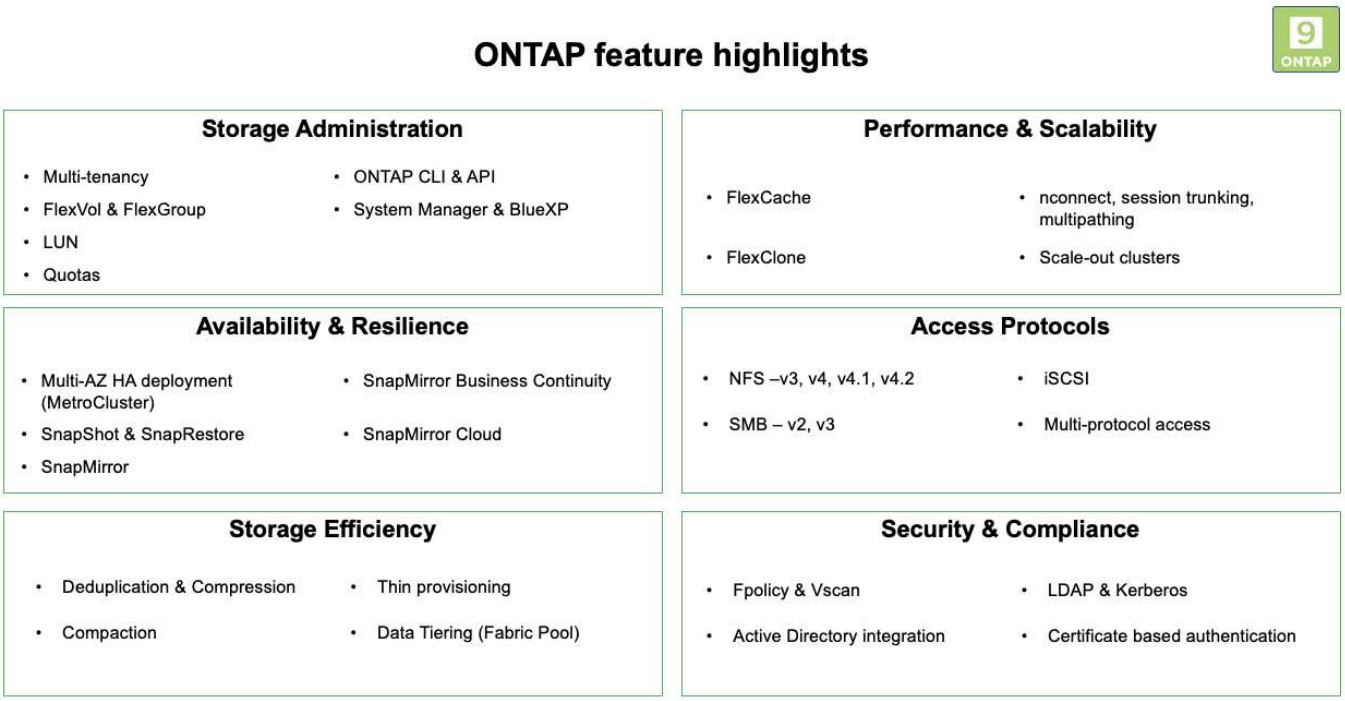
NetApp 發現客戶使用 Kubernetes 建置的容器和協調作業平台、將舊有企業應用程式現代化、並建置新的應用程式。Red Hat OpenShift Container Platform 是我們許多客戶採用的範例之一。

隨著越來越多客戶開始在企業內採用容器、 NetApp 的定位非常完美、可協助滿足其有狀態應用程式的持續儲存需求、以及資料保護、資料安全性和資料移轉等傳統資料管理需求。不過、這些需求是使用不同的策略、工具和方法來滿足的。

以 NetApp ONTAP * 為基礎的儲存選項如下所列、可為容器和 Kubernetes 部署提供安全性、資料保護、可靠性和靈活度。

- 內部部署的自我管理儲存設備：
  - NetApp Fabric 附加儲存設備（FAS）、 NetApp All Flash FAS Array （AFF）、 NetApp All SAN Array （ASA）和 ONTAP Select

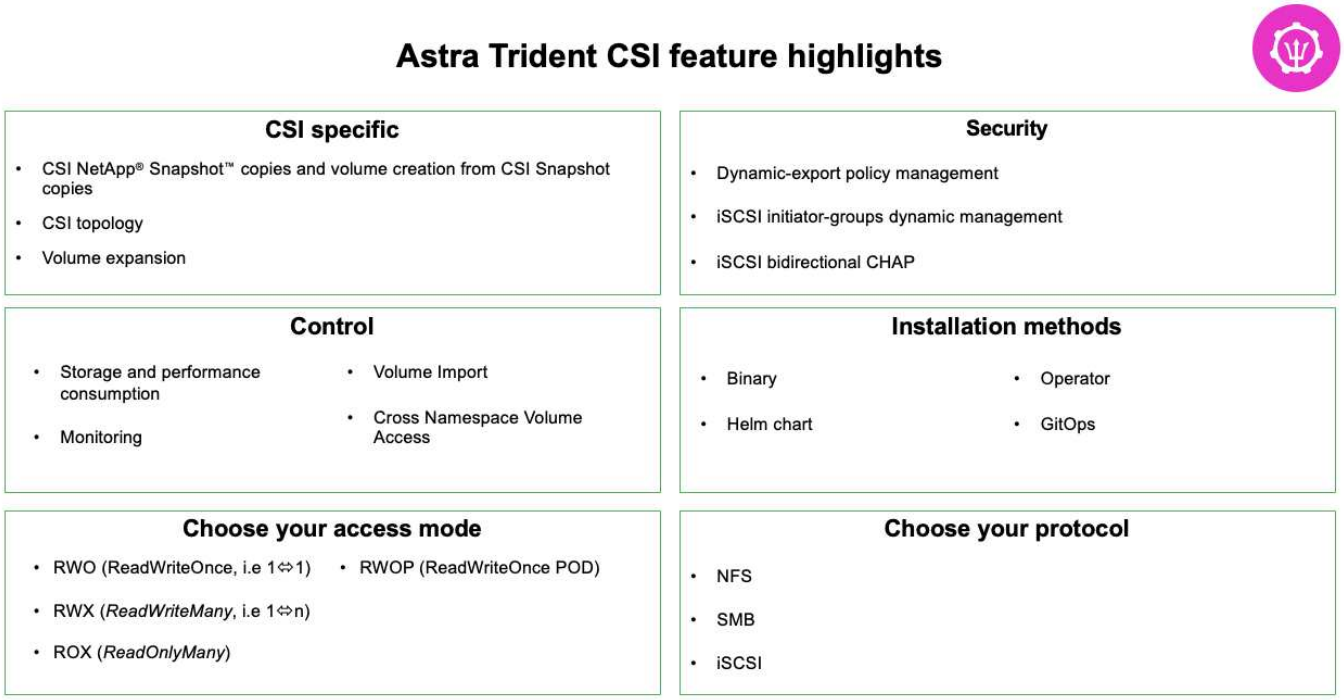
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（ STaaS ）
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （ CVO ）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：
  - Cloud Volumes Service for Google Cloud （ CVS ）、 Azure NetApp Files （ anf ）、 Amazon FSX for NetApp ONTAP 可在超大型擴充器中提供完全託管的儲存設備



- NetApp BlueXP** 可讓您從單一控制平面 / 介面管理所有儲存設備和資料資產。

您可以使用 BlueXP 來建立和管理雲端儲存設備（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 Astra Trident * 是符合 CSI 標準的 Storage Orchestrator 、可快速輕鬆地使用由上述各種 NetApp 儲存選項作為後盾的持續儲存設備。這是由 NetApp 維護和支援的開放原始碼軟體。



業務關鍵容器工作負載不只需要持續的磁碟區、他們的資料管理需求也需要保護及移轉應用程式 Kubernetes 物件。

應用程式資料除了包含使用者資料外、還包括 Kubernetes 物件：以下是一些範例： - Kubernetes 物件、例如 Pod 規格、 PVC 、部署、服務 - 自訂組態物件、例如組態對應和機密 - 持續性資料、例如 Snapshot 複本、備份、複本 - 自訂資源、例如 CRS 和 CRD

- NetApp Astra Control** 可作為完全託管和自我管理的軟體使用、可協調功能以提供健全的應用程式資料管理。請參閱 "Astra文件" 如需 Astra 系列產品的詳細資訊、請參閱。

本參考文件提供移轉與保護容器型應用程式的驗證、這些應用程式部署在 RedHat OpenShift Container 平台上、並使用 NetApp Astra Control Center 。此外、此解決方案還提供部署和使用 Red Hat Advanced Cluster Management （ACM）來管理容器平台的高階詳細資料。本文件也重點介紹使用 Astra Trident CSI 資源配置程式、將 NetApp 儲存設備與 Red Hat OpenShift 容器平台整合的詳細資料。Astra Control Center 部署在集線器叢集上、用於管理容器應用程式及其持續儲存生命週期。最後、它為 AWS （ROSA）中受管理 Red Hat OpenShift 叢集上的容器工作負載提供複寫和容錯移轉及容錯移轉解決方案、使用 Amazon FSx for NetApp ONTAP （FSxN）作為持續儲存設備。

在 **AWS** 上使用託管 **Red Hat OpenShift Container** 平台工作負載的 **NetApp** 解決方案

在 **AWS** 上使用託管 **Red Hat OpenShift Container** 平台工作負載的 **NetApp** 解決方案

客戶可能是「天生於雲端」、或是準備好將某些特定工作負載或所有工作負載從資料中心移至雲端時、處於現代化過程的某個階段。他們可以選擇在雲端使用由供應商管理的 OpenShift 容器和由供應商管理的 NetApp 儲存設備來執行工作負載。他們應該規劃並部署雲端中的託管 Red Hat OpenShift Container 叢集（ROSA）、以便為其容器工作負載打造成功的正式作業環境。當他們位於 AWS 雲端時、也可以針對 NetApp ONTAP 部署 FSX 以滿足儲存需求。

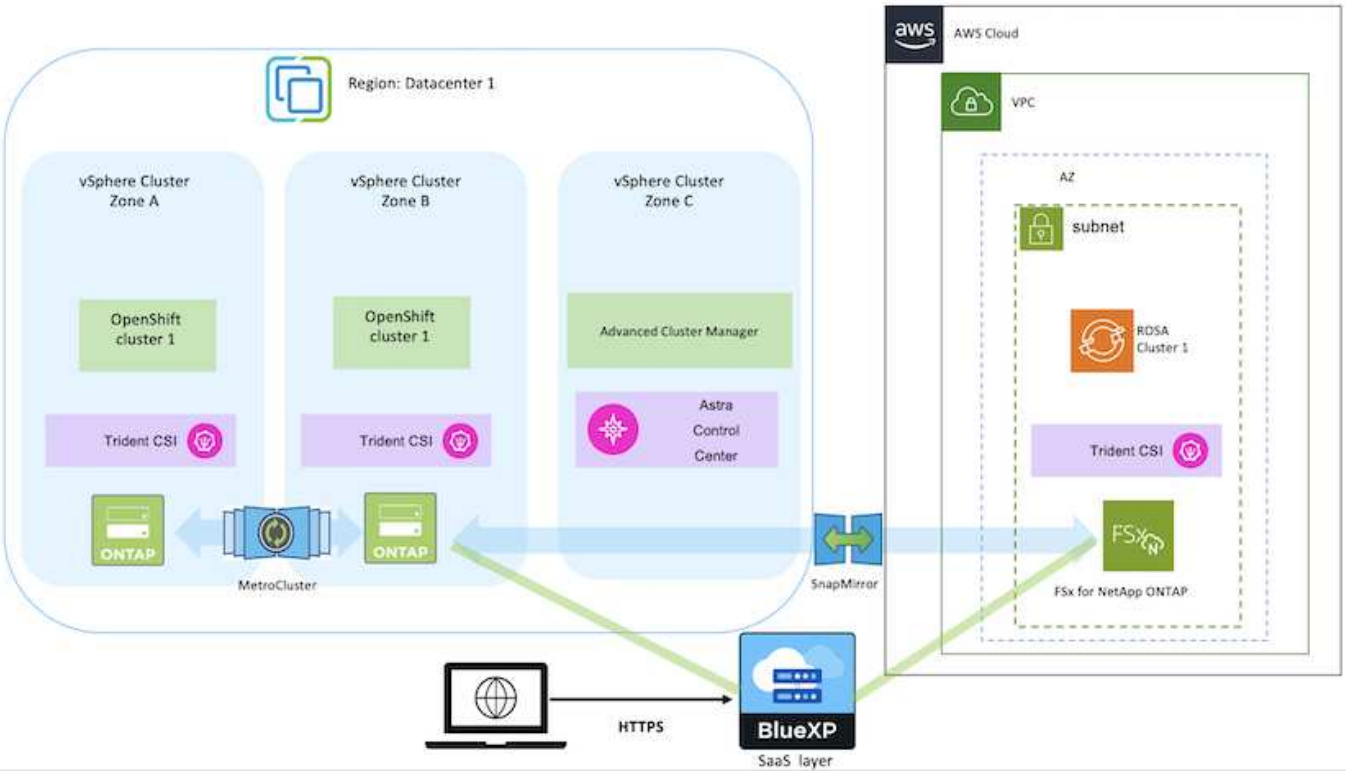
適用於 NetApp ONTAP 的 FSX 可為 AWS 中的容器部署提供資料保護、可靠性和靈活度。Astra Trident 是動態

儲存資源配置程式、可為客戶的有狀態應用程式使用持續的 FSxN 儲存設備。

由於 ROSA 可在 HA 模式中部署、控制平面節點分散於多個可用性區域、因此也可透過 Multi-AZ 選項來配置 FSX ONTAP 、以提供高可用度並防範 AZ 故障。

> 從檔案系統的慣用可用性區域（ AZ ）存取 Amazon FSX 檔案系統時、不會收取資料傳輸費用。如需定價的詳細資訊、請參閱 "請按這裡"。

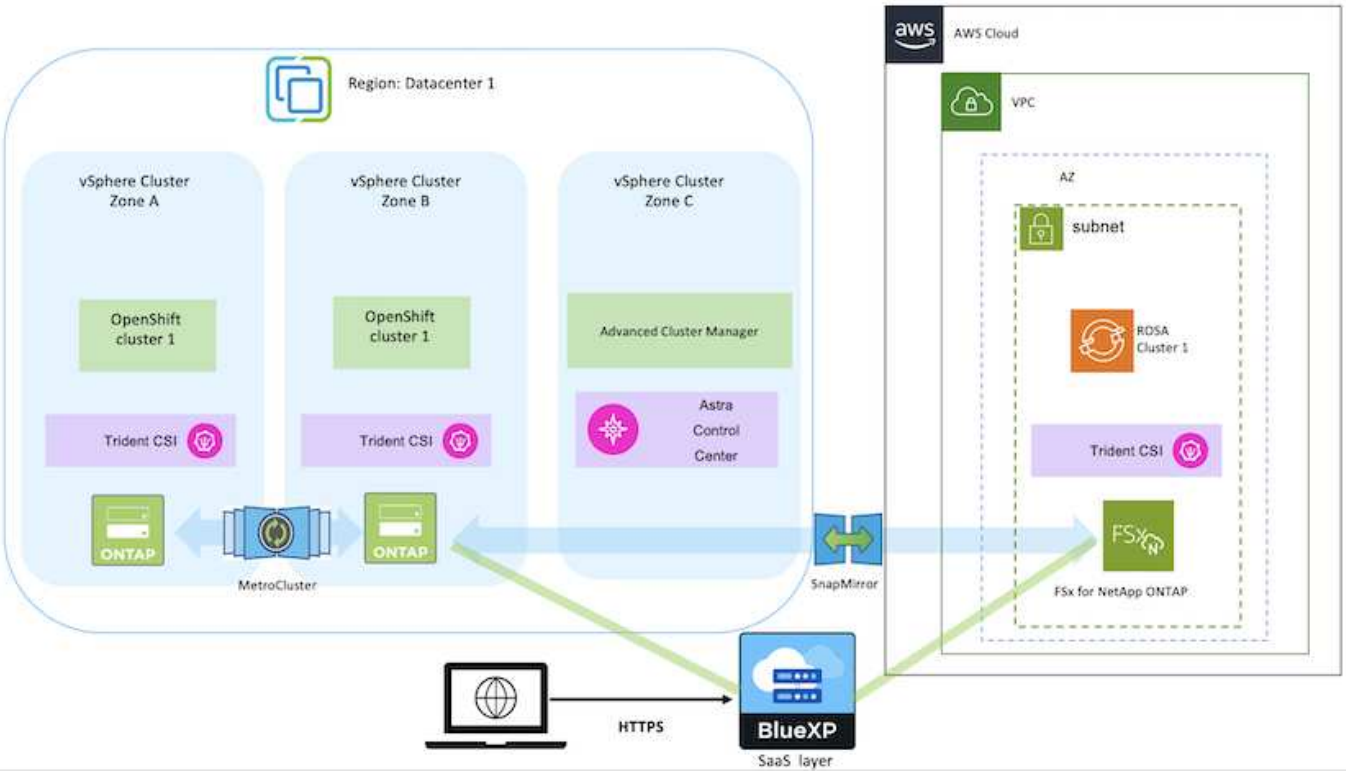
適用於 **OpenShift Container** 工作負載的資料保護與移轉解決方案



在 **AWS** 上部署及設定 **Managed Red Hat OpenShift Container** 平台

本節說明在 AWS （ ROSA ）上設定託管 Red Hat OpenShift 叢集的高階工作流程。它顯示 Astra Trident 使用託管 FSx for NetApp ONTAP （ FSxN ）作為儲存後端、以提供持續的磁碟區。詳細說明如何使用 BlueXP 在 AWS 上部署 FSxN 。此外、我們也提供有關使用 BlueXP 和 OpenShift GitOps （ Argo CD ）在 ROSA 叢集上為有狀態的應用程式執行資料保護和移轉活動的詳細資訊。

下圖說明在 AWS 上部署的 ROSA 叢集、並使用 FSxN 作為後端儲存設備。



此解決方案已在 AWS 的兩個 VPC 中使用兩個 ROSA 叢集進行驗證。每個 ROSA 叢集都使用 Astra Trident 與 FSxN 整合。在 AWS 中部署 ROSA 叢集和 FSxN 有幾種方法。此設定的高階說明提供所使用特定方法的文件連結。您可以參閱中提供的相關連結中的其他方法 "資源區段"。

設定程序可分為下列步驟：

安裝 **ROSA** 叢集

- 建立兩台 VPC 、並設定 VPC 之間的 VPC 對等連線。
- 請參閱 "請按這裡" 以取得安裝 ROSA 叢集的指示。

安裝 **FSxN**

- 在 BlueXP 的 VPC 上安裝 FSxN 。請參閱 "請按這裡" 用於建立 BlueXP 帳戶和開始使用。請參閱 "請按這裡" 用於安裝 FSxN 。請參閱 "請按這裡" 在 AWS 中建立連接器以管理 FSxN 。
- 使用 AWS 部署 FSxN 。請參閱 "請按這裡" 使用 AWS 主控台進行部署。

在 **ROSA** 叢集上安裝 **Trident** （使用 **Helm** 圖表）

- 使用 Helm 圖表在 ROSA 叢集上安裝 Trident 。Helm 圖表的 URL ： https://netapp.github.io/trident-helm-chart

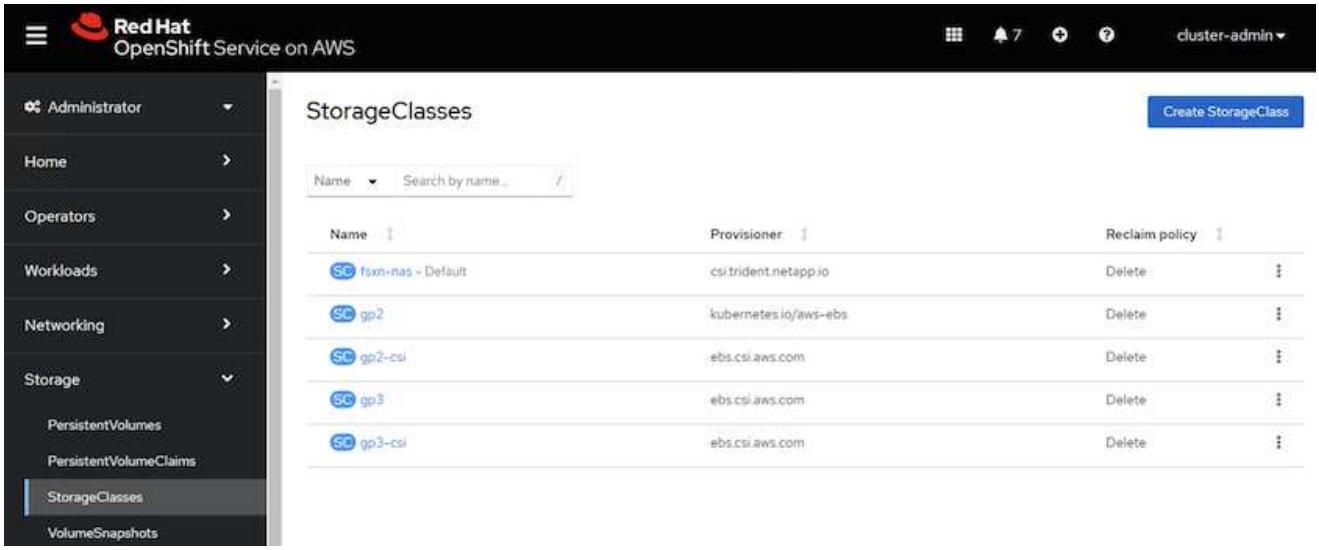
將 FSxN 與 Astra Trident 整合至 ROSA 叢集

OpenShift GitOps 可用於在所有託管叢集使用 ApplicationSet 登錄 ArgoCD 時、將 Astra Trident CSI 部署至這些叢集。

```yaml
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 **FSxN** ）

- 請參閱 "請按這裡" 如需建立後端和儲存類別的詳細資訊、
- 從 OpenShift Console 將為 FsxN 建立的儲存類別設為 Trident CSI 作為預設值。請參閱以下螢幕擷取畫面：



使用 **OpenShift GitOps** （ **Argo CD** ）部署應用程式

- 在叢集上安裝 OpenShift GitOps 運算子。請參閱指示 "請按這裡"。
- 為叢集設定新的 Argo CD 執行個體。請參閱指示 "請按這裡"。

開啟 Argo CD 的主控台、然後部署應用程式。例如、您可以使用 Argo CD 搭配 Helm 圖表來部署 Jenkins 應用程式。建立應用程式時、會提供下列詳細資料：專案：預設叢集： https://kubernetes.default.svc命名空間： Jenkins The URL for the Helm Chart: https://charts.bitnami.com/bitnami

船舵參數： global.storageClass ： fsxn-NAS

資料保護

本頁顯示使用 Astra Control Service 在 AWS （ ROSA ）叢集上管理 Red Hat OpenShift 的資料保護選項。Astra Control Service （ ACS ）提供簡單易用的圖形化使用者介面、可讓您新增叢集、定義在叢集上執行的應用程式、以及執行應用程式感知的資料管理活動。您也可以使用 API 來存取 ACS 功能、以自動化工作流程。

驅動 Astra 控制（ ACS 或 ACC ）是 NetApp Astra Trident 。Astra Trident 整合了多種 Kubernetes 叢集類型、例如 Red Hat OpenShift 、 EKS 、 aks 、 SUSE Rancher 、 Anthos 等。 提供各種 NetApp ONTAP 儲存設備、例如 FAS / AFF 、 ONTAP Select 、 CVO 、 Google Cloud Volumes Service 、 Azure NetApp Files 和 Amazon FSX for NetApp ONTAP 。

本節詳細說明使用 ACS 的下列資料保護選項：

- 顯示在某個區域執行之 ROSA 應用程式的備份與還原、並還原至另一個區域的影片。

- 顯示 ROSA 應用程式快照與還原的影片。
- 安裝 ROSA 叢集 Amazon FSX for NetApp ONTAP 的逐步詳細資料、使用 NetApp Astra Trident 與儲存後端整合、在 ROSA 叢集上安裝 PostgreSQL 應用程式、使用 ACS 建立應用程式快照、並從其中還原應用程式。
- 一個部落格、顯示在使用 ACS 的 ONTAP 適用的 FSX 之 ROSA 叢集上、從 mysql 應用程式的快照建立及還原的逐步詳細資料。

從備份備份 / 還原

下列影片顯示在某個區域執行的 ROSA 應用程式備份、並還原至另一個區域。

AWS 上適用於 Red Hat OpenShift 服務的 FSX NetApp ONTAP

快照 / 從快照還原

下列影片顯示在拍攝 ROSA 應用程式的快照、並在之後從快照還原。

使用 Amazon FSX 進行 NetApp ONTAP 儲存的 AWS （ ROSA ）叢集上 Red Hat OpenShift 服務上的應用程式快照 / 還原

部落格

- "使用 Astra Control Service 來管理內含 Amazon FSX 儲存設備的 ROSA 叢集上的應用程式資料"

建立快照並從快照還原的逐步詳細資料

必要設定

- "AWS帳戶"
- "Red Hat OpenShift 帳戶"
- IAM 使用者 "適當的權限" 建立及存取 ROSA 叢集
- "AWS CLI"
- "ROSA CLI"
- "OpenShift CLI"（ OC ）
- 具備子網路和適當閘道和路由的 VPC
- "已安裝 ROSA 叢集" 進入 VPC
- "Amazon FSX for NetApp ONTAP 產品" 在同一個 VPC 中建立
- 從存取 ROSA 叢集 "OpenShift 混合雲主控台"

後續步驟

1. 建立管理員使用者並登入叢集。
2. 為叢集建立一個 kubeconfig 檔案。
3. 在叢集上安裝 Astra Trident 。
4. 使用 Trident CSI 資源管理程式建立後端、儲存類別和快照類別組態。

5. 在叢集上部署 PostgreSQL 應用程式。
6. 建立資料庫並新增記錄。
7. 將叢集新增至 ACS 。
8. 在 ACS 中定義應用程式。
9. 使用 ACS 建立快照。
10. 刪除 PostgreSQL 應用程式中的資料庫。
11. 使用 ACS 從快照還原。
12. 確認您的應用程式已從快照中還原。

1.建立管理員使用者並登入叢集

使用下列命令建立管理員使用者、即可存取 ROSA 叢集：（只有在安裝時未建立管理員使用者時、才需要建立管理員使用者）

```
rosa create admin --cluster=<cluster-name>
```

此命令會提供如下所示的輸出。使用登入叢集 `oc login` 輸出中提供的命令。

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

您也可以使用權杖登入叢集。如果您在建立叢集時已建立管理員使用者、則可以使用管理員使用者認證、從 Red Hat OpenShift 混合雲主控台登入叢集。然後按一下右上角顯示登入使用者名稱的、即可取得 `oc login` 命令列的命令（權杖登入）。

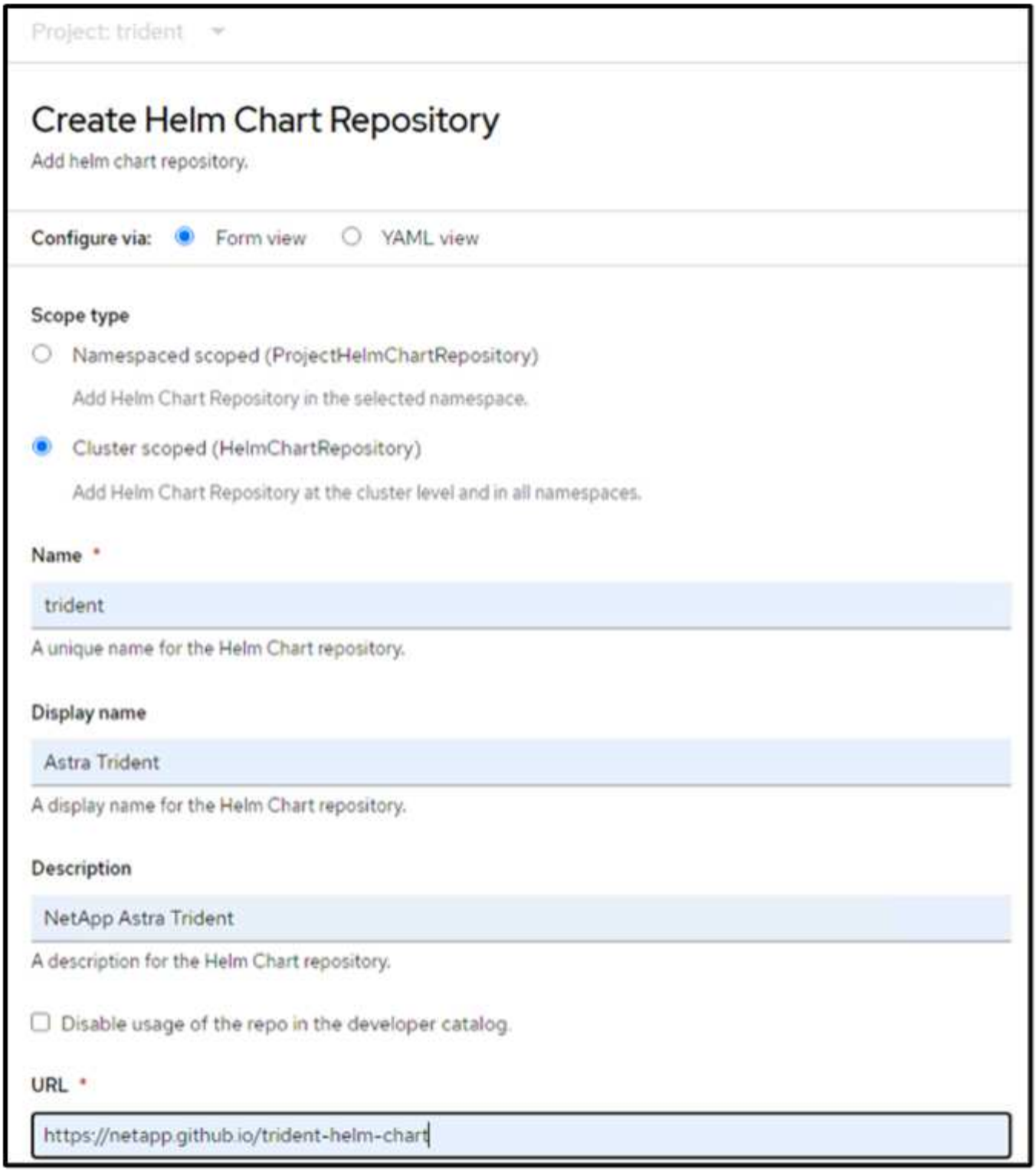
2.為叢集建立一個 **kubeconfig** 檔案

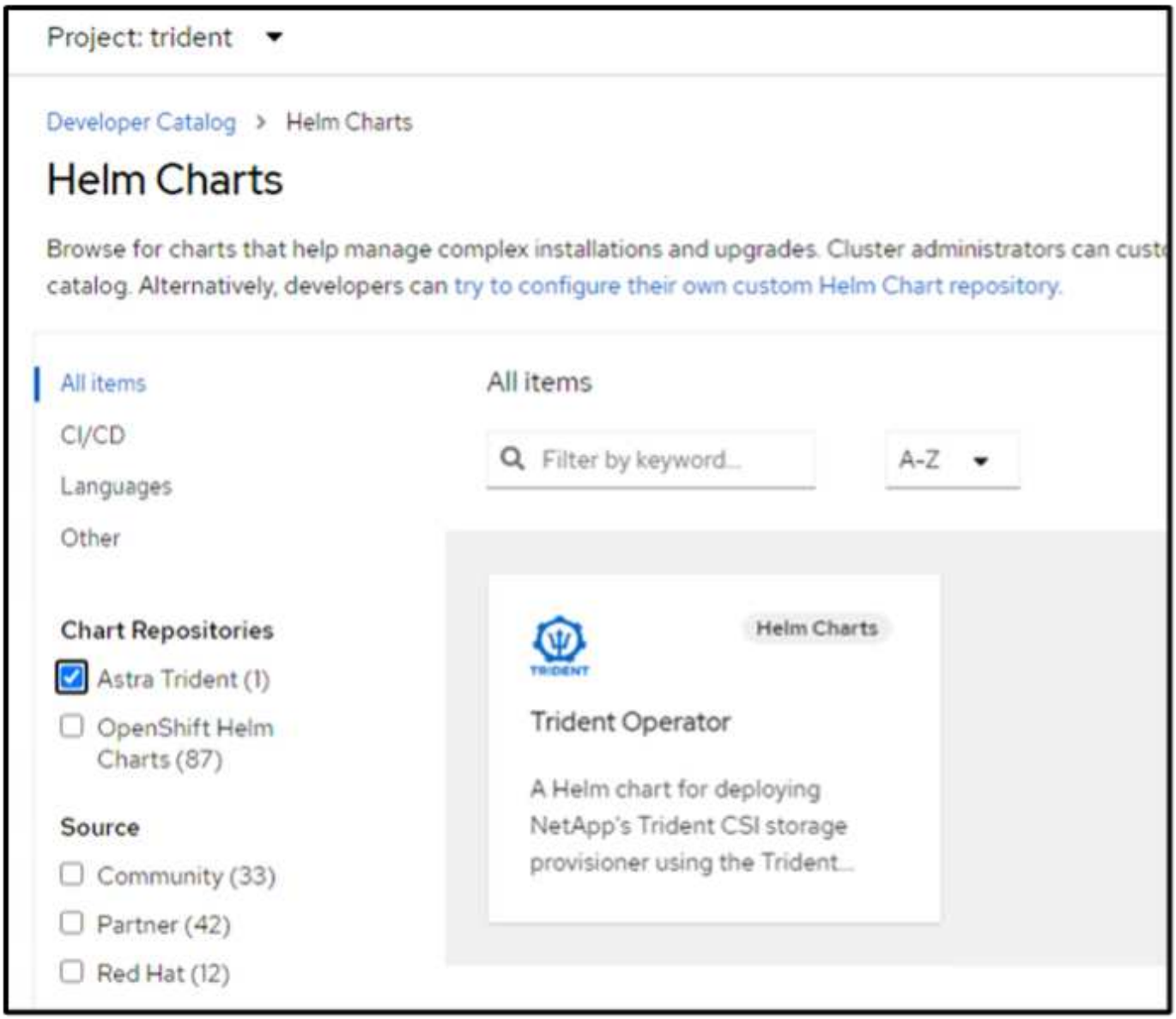
請依照程序進行 "請按這裡" 為 ROSA 叢集建立 KRBeconfig 檔案。將叢集新增至 ACS 後、將會使用此 kubeconfig 檔案。

3.在叢集上安裝 **Astra Trident**

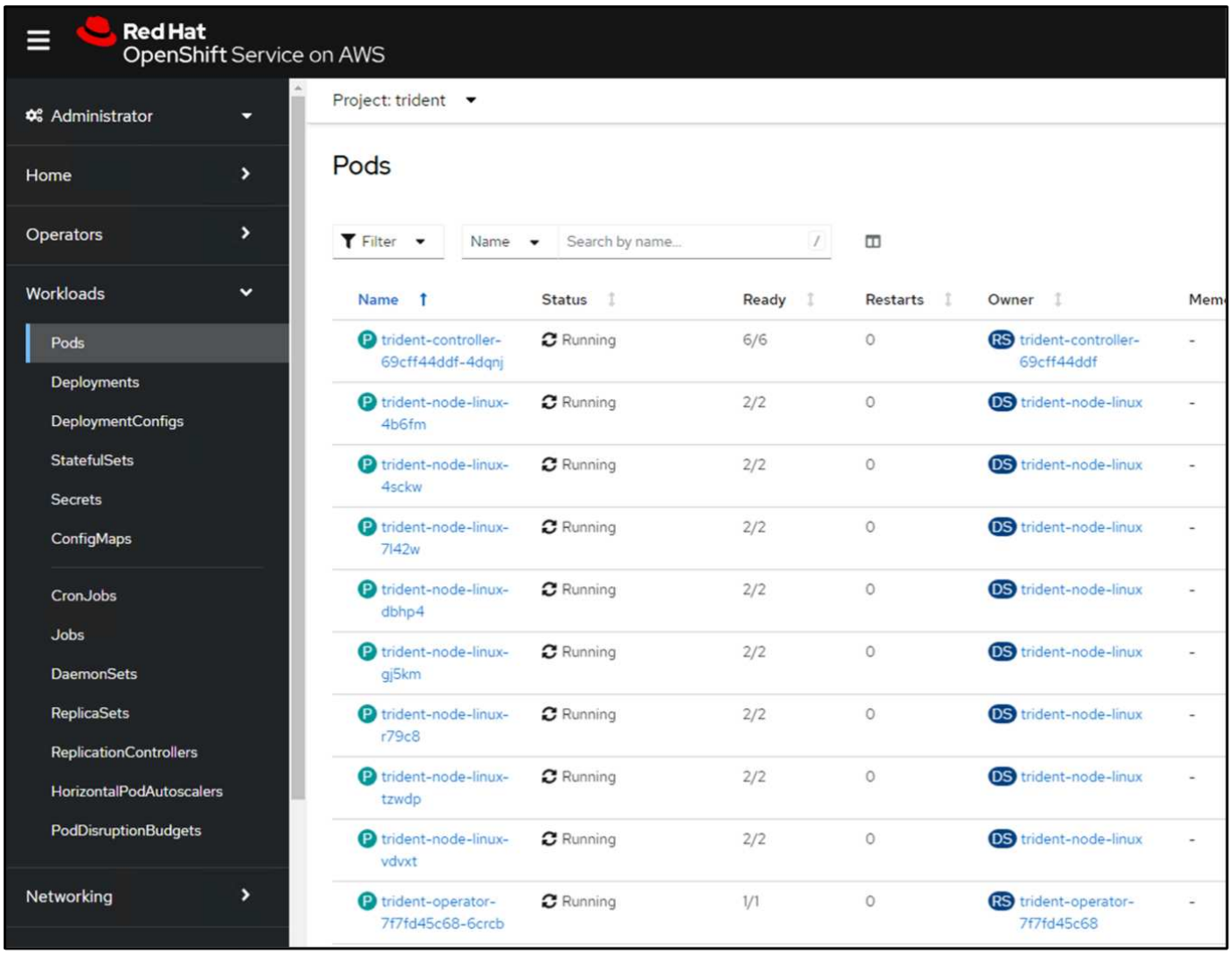
在 ROSA 叢集上安裝 Astra Trident （最新版本）。若要這麼做、您可以遵循所提供的任何一個程序 "請按這裡"。若要從叢集主控台使用 helm 來安裝 Trident 、請先建立名為 Trident 的專案。

然後從「開發人員」檢視中建立 Helm 圖表儲存庫。供 URL 欄位使用 `'https://netapp.github.io/trident-helm-chart'`。然後為 Trident 運算子建立 helm 版本。


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



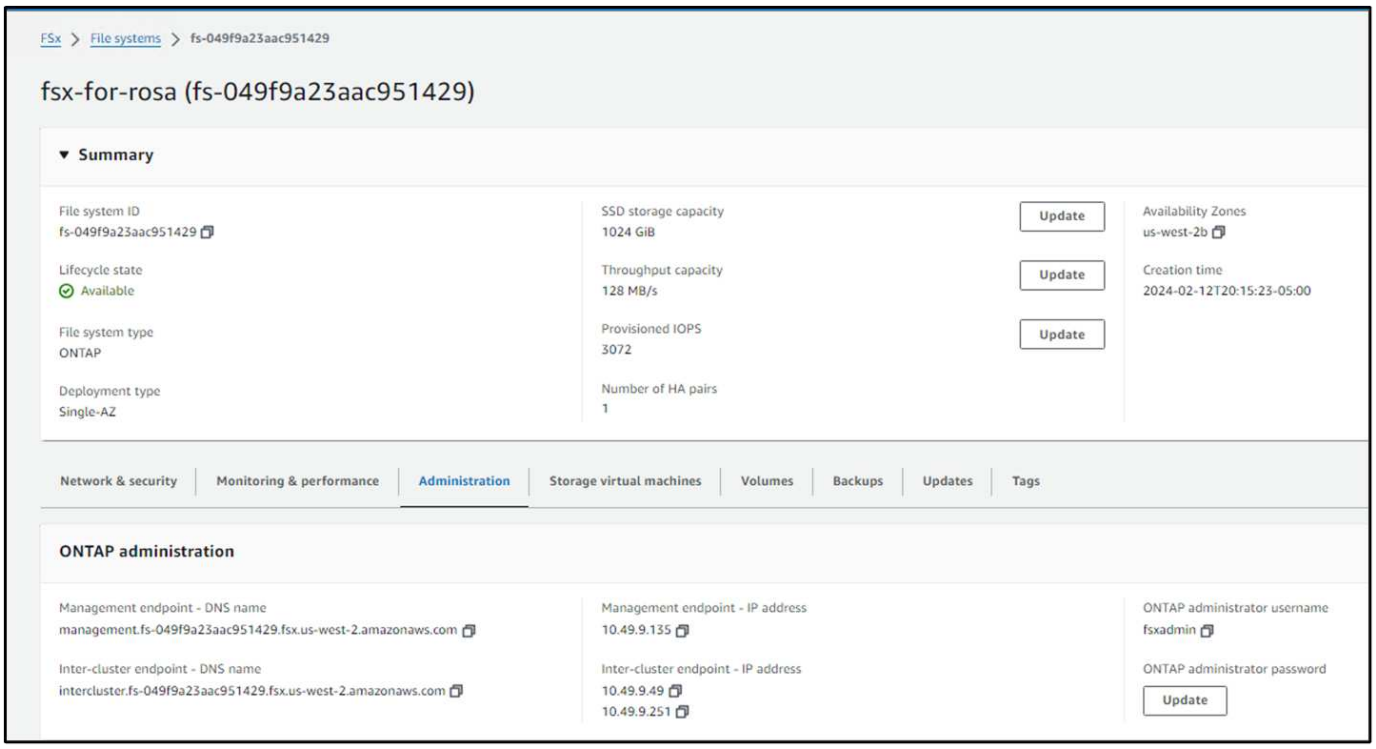
返回主控台的「管理員」檢視、然後在 Trident 專案中選取「群組」、以確認所有 Trident 群組都在執行中。



4.使用 **Trident CSI** 資源管理程式 建立後端、儲存類別和快照類別組態

請使用下方顯示的 yaml 檔案來建立 Trident 後端物件、儲存類別物件和 Volumesnapshot 物件。請務必在後端組態 yaml 中、為您所建立的 NetApp ONTAP 檔案系統提供 Amazon FSX 的認證、以及檔案系統的管理 LIF 和 Vserver 名稱。若要取得這些詳細資料、請前往 Amazon FSX 的 AWS 主控台並選取檔案系統、然後瀏覽至管理索引標籤。此外、按一下更新以設定的密碼 `fsxadmin` 使用者：

您可以使用命令列來建立物件、或使用混合雲主控台的 yaml 檔案來建立物件。



- Trident 後端組態 **

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

- 儲存等級 **

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

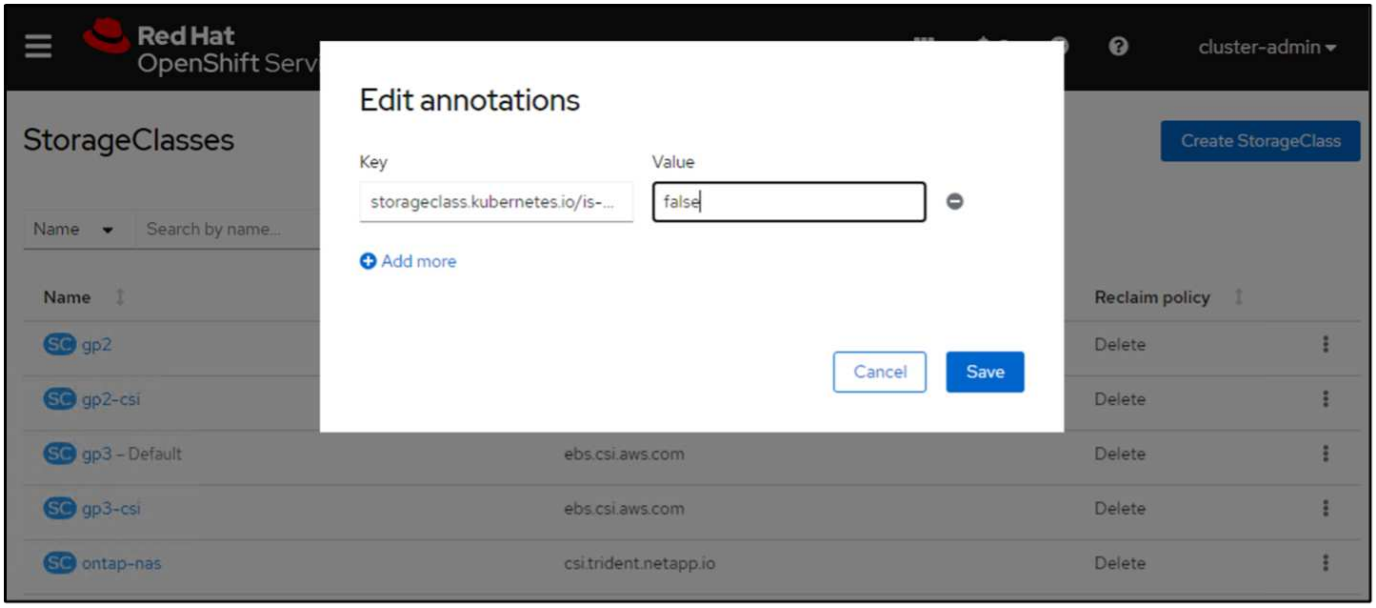
- 快照類別 **

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

發出下列命令、確認已建立後端、儲存類別和 Trident -snapshotClass 物件。

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

此時、您需要進行的重要修改是將 ONTAP NAS 設定為預設儲存類別、而非 GP3 、以便您稍後部署的 PostgreSQL 應用程式可以使用預設儲存類別。在叢集的 Openshift 主控台中、選取 Storage （儲存設備）下的 StorageClasses （儲存設備類別）。將目前預設類別的註釋編輯為假、並將 ONTAP NAS 儲存類別的標註 storagecasse.Kubernetes.IO/is 預設類別設定為 true 。



5.在叢集上部署 **PostgreSQL** 應用程式

您可以從命令列部署應用程式、如下所示：

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

如果您沒有看到應用程式 Pod 正在執行、則可能會因為安全內容限制而導致錯誤。

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/postgresql      ClusterIP   172.30.245.50   <none>        5432/TCP   12m
service/postgresql-hl   ClusterIP   None            <none>        5432/TCP   12m

NAME                          READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer   persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate       statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate           statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

編輯以修正錯誤 `runAsUser` 和 `fsGroup` 中的欄位 `statefuleset.apps/postgresql` 的輸出中有 uid 的物件 `oc get project` 命令、如下所示。

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

PostgreSQL 應用程式應執行、並使用 Amazon FSX 支援的持續磁碟區來儲存 NetApp ONTAP 。

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

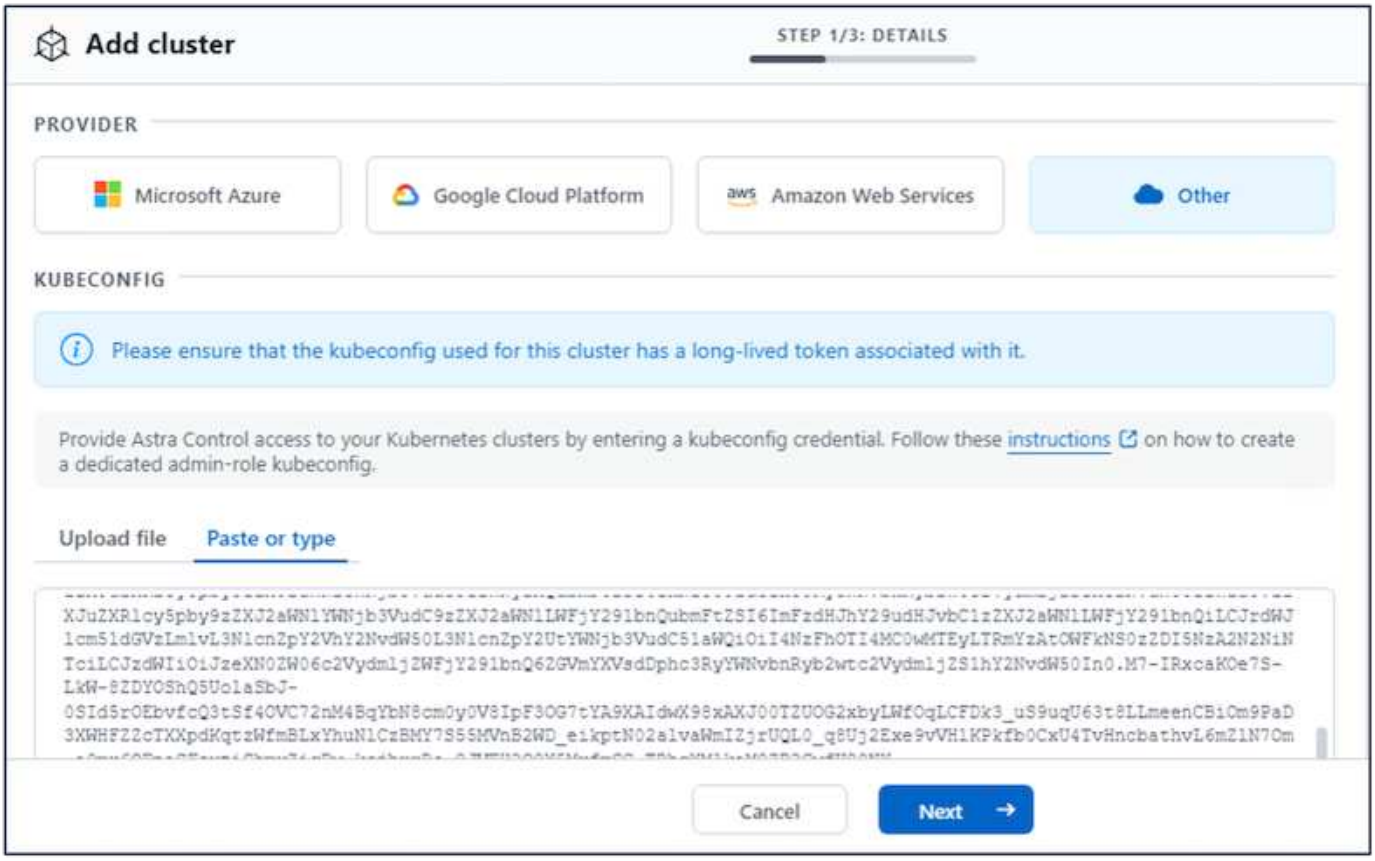
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6.建立資料庫並新增記錄

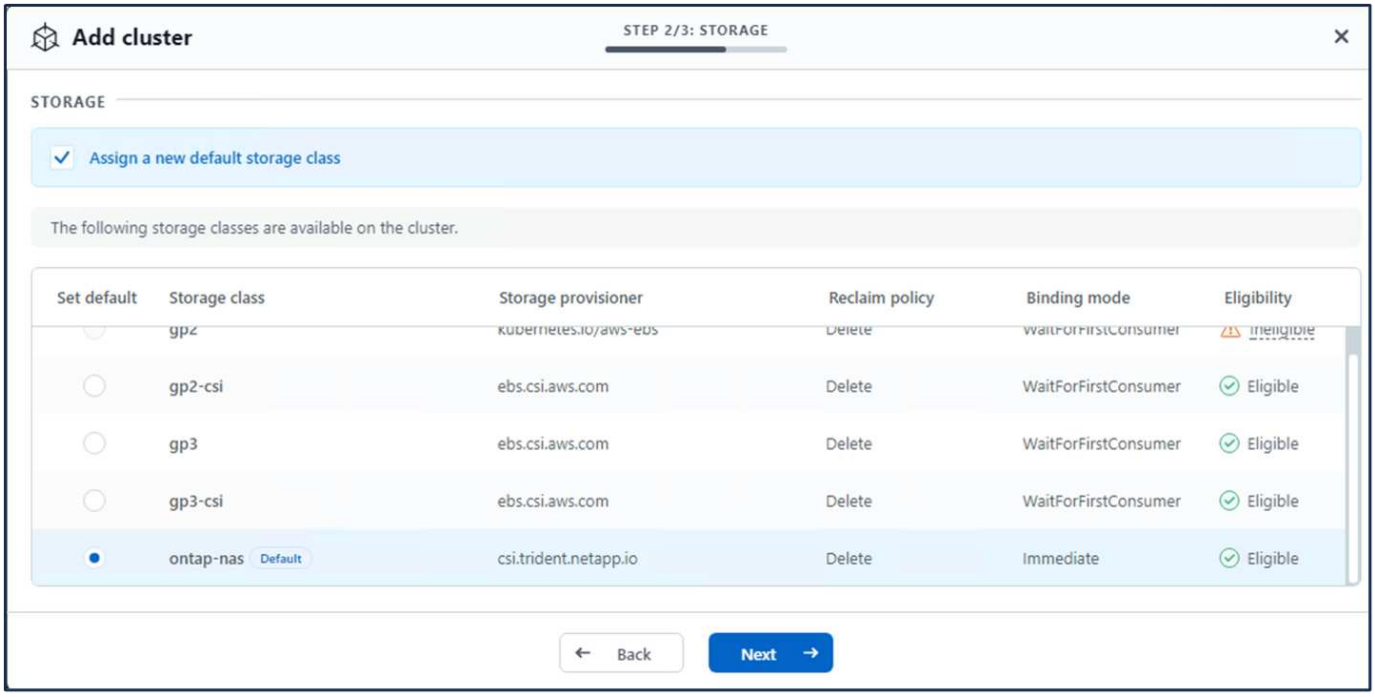
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7.將叢集新增至 **ACS**

登入 ACS 。選取叢集、然後按一下新增。選取「其他」、然後上傳或貼上 Kupleconfig 檔案。

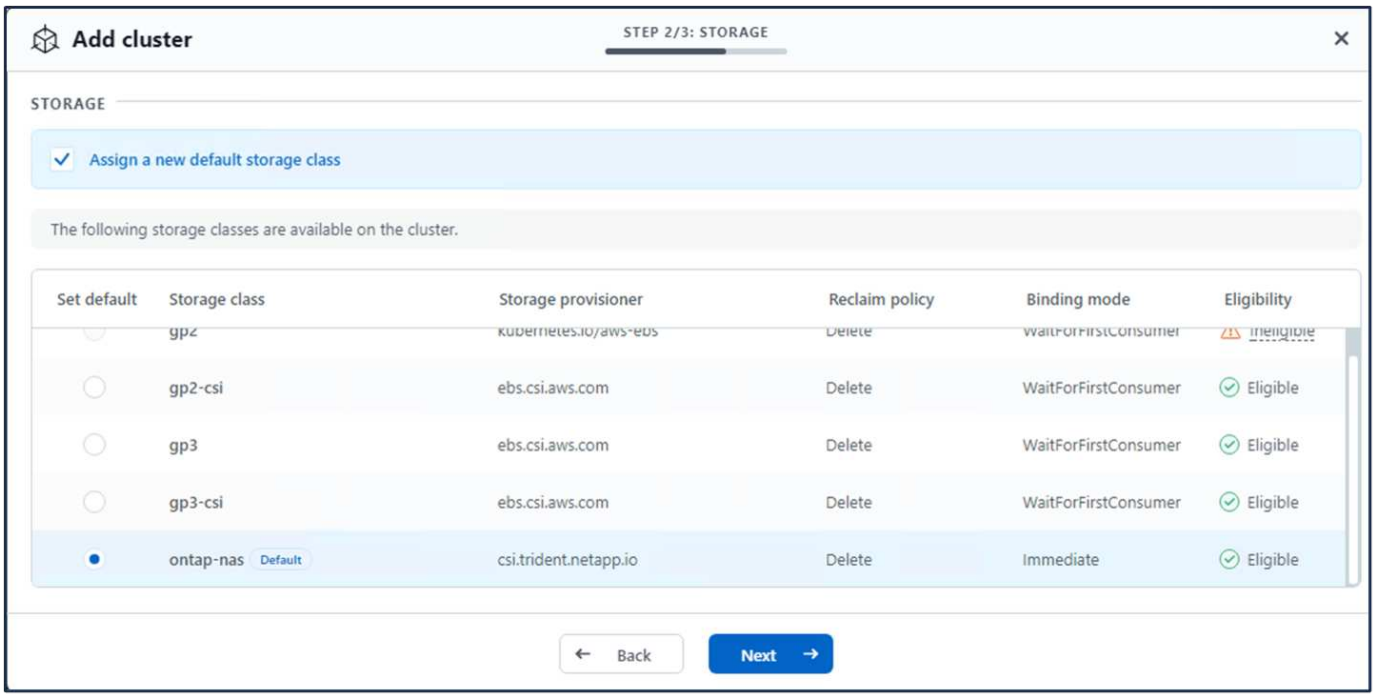


按一下 * 下一步 * 、然後選取 ONTAP NAS 作為 ACS 的預設儲存類別。按一下 * 下一步 * 、檢閱詳細資料和 * 新增 * 叢集。



8.在 **ACS** 中定義應用程式

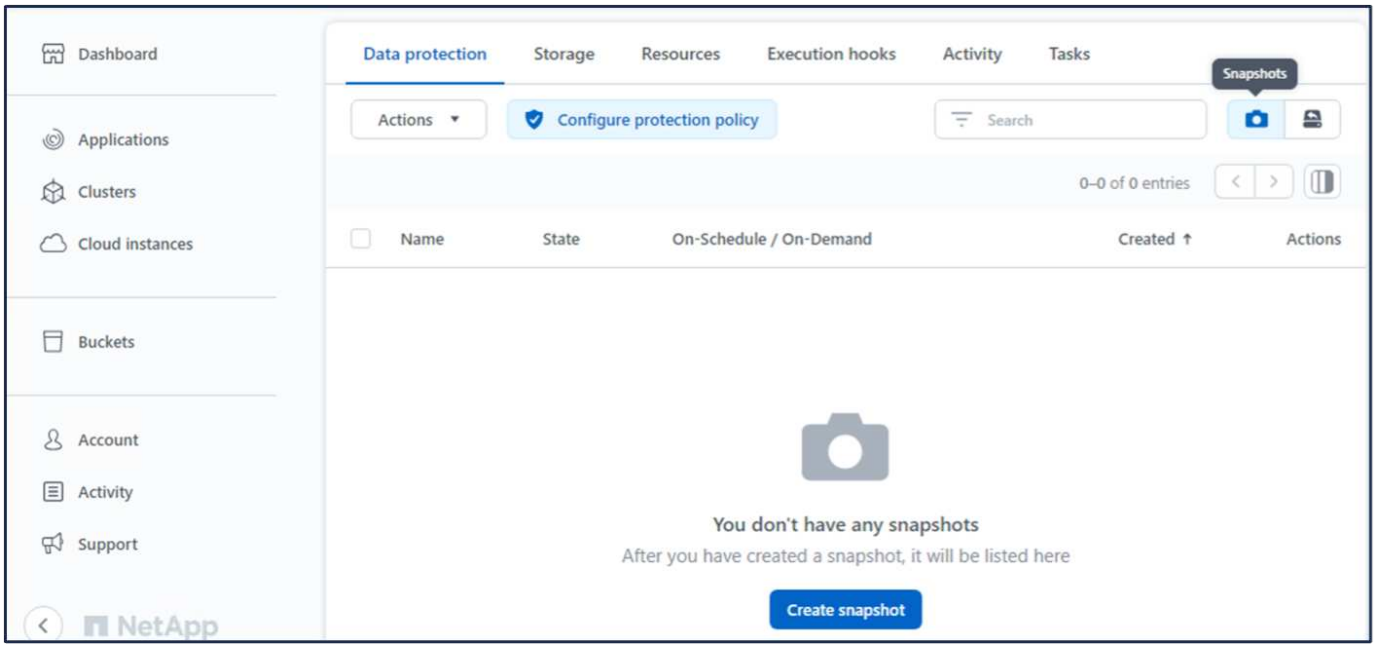
在 ACS 中定義 PostgreSQL 應用程式。從登陸頁面、選取 * 應用程式 * 、 * 定義 * 、然後填寫適當的詳細資料。按幾次 * 下一步 * 、檢閱詳細資料、然後按一下 * 定義 * 。應用程式隨即新增至 ACS 。

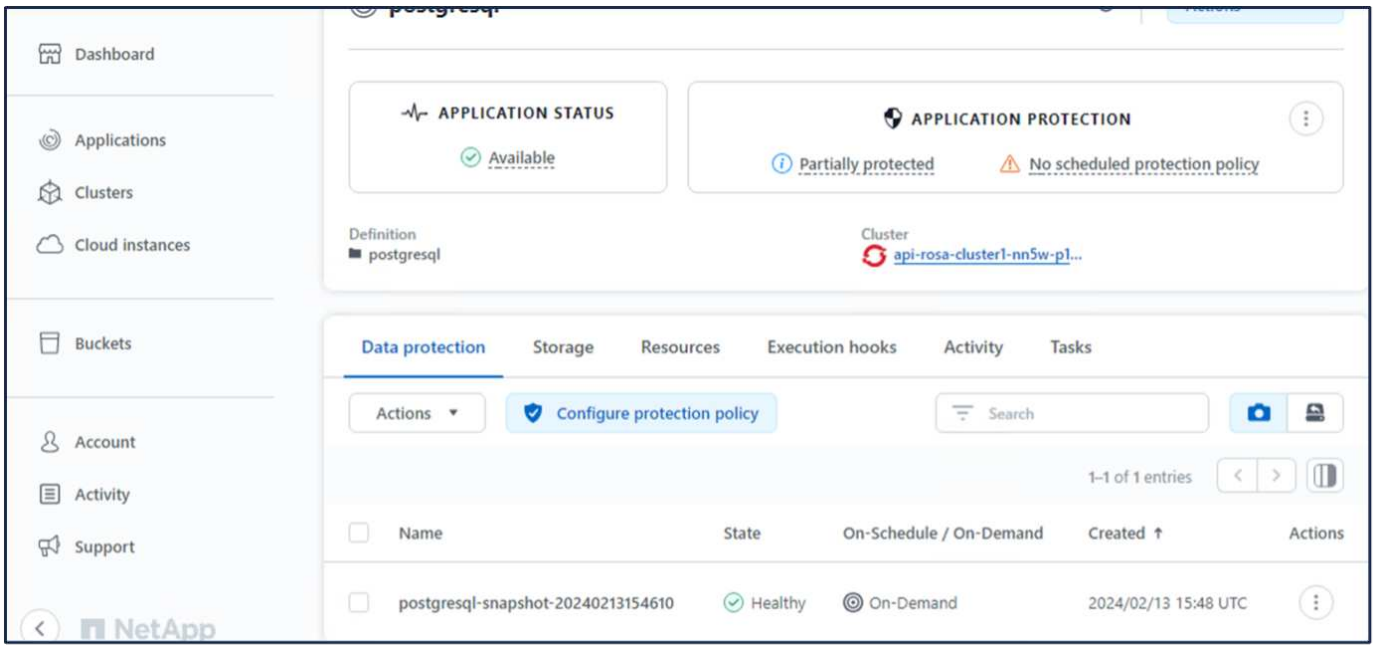


9.使用 **ACS** 建立快照

在 ACS 中建立快照的方法有許多種。您可以選取應用程式、並從顯示應用程式詳細資料的頁面建立快照。您可以按一下「建立快照」來建立隨選快照、或是設定保護原則。

只要按一下 * 建立 SnapShot * 、提供名稱、檢閱詳細資料、然後按一下 * Snapshot * 、即可建立隨選快照。作業完成後、快照狀態會變更為「健全」。





10.刪除 **PostgreSQL** 應用程式中的資料庫

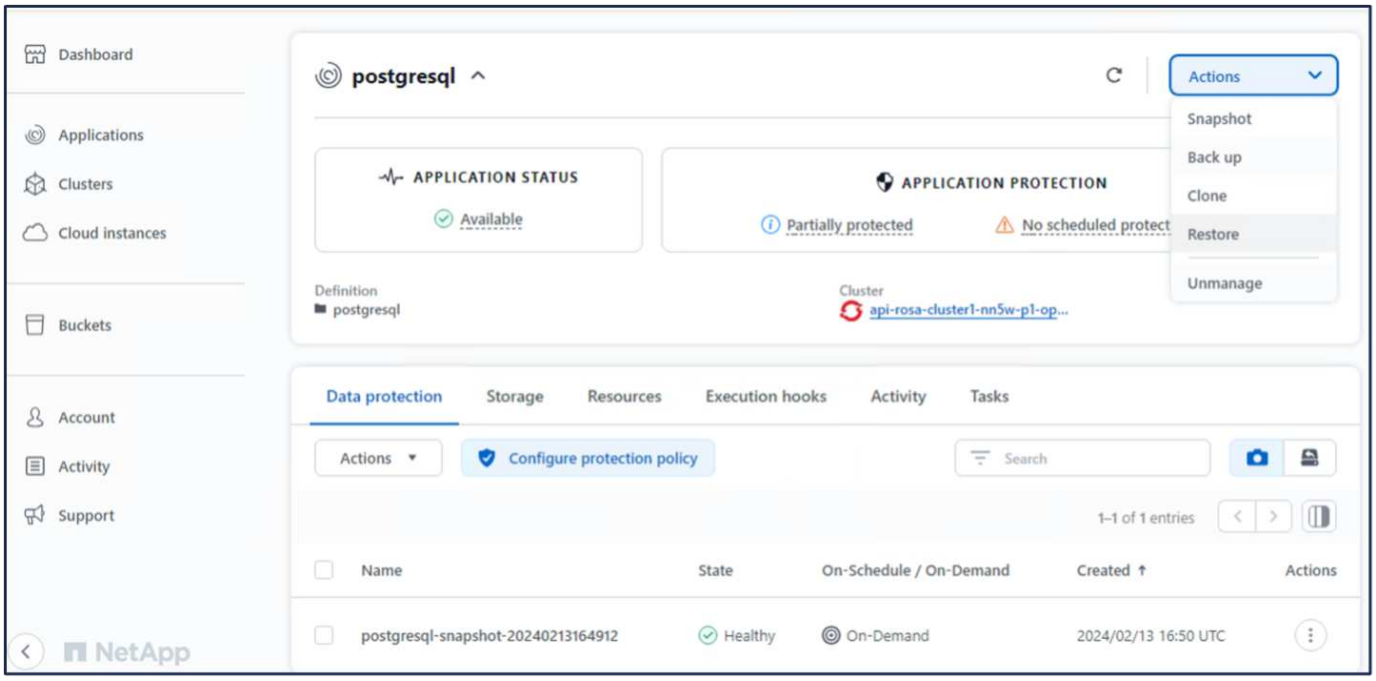
重新登入 PostgreSQL 、列出可用的資料庫、刪除您先前建立的資料庫、然後再次列出、以確保資料庫已刪除。

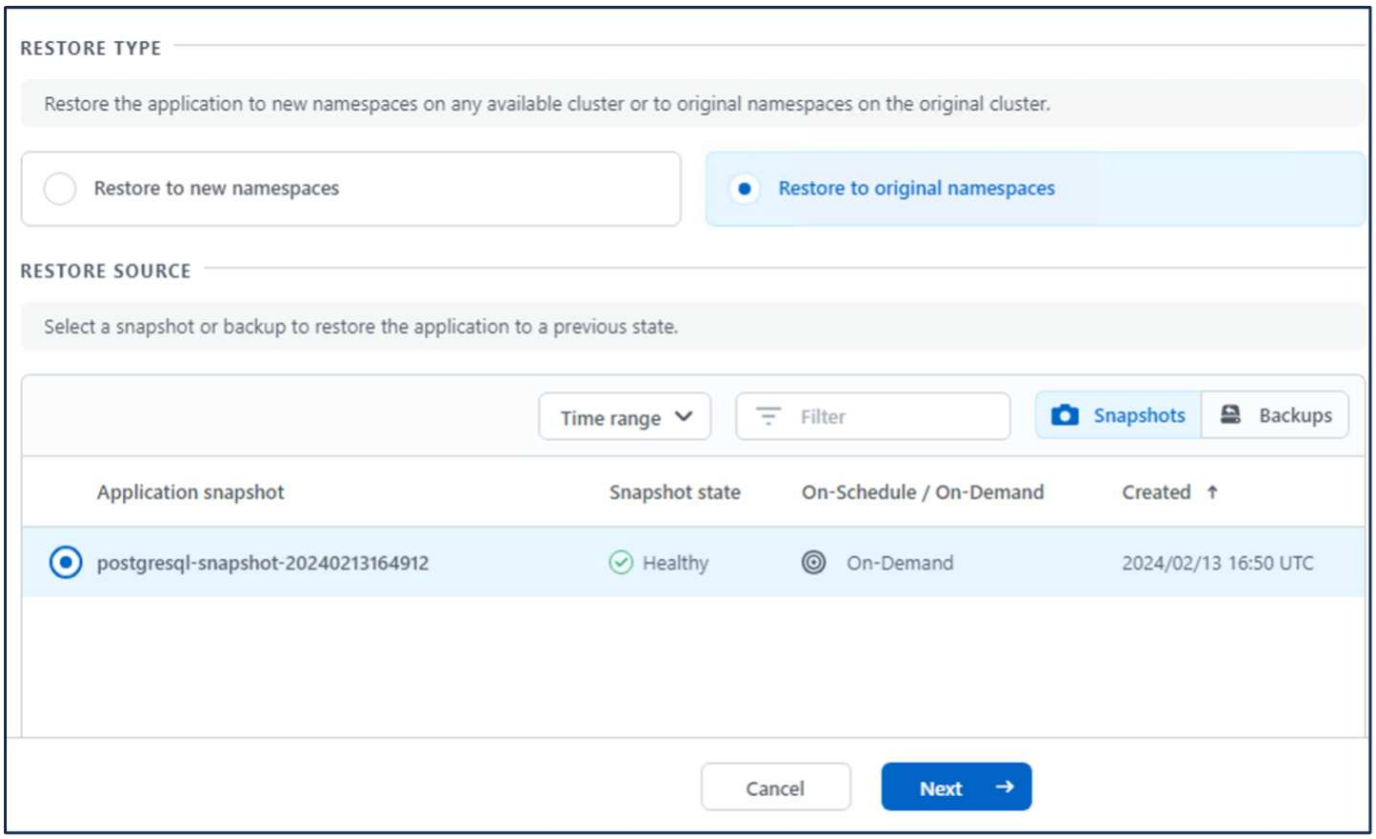
```
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
-
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
-
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

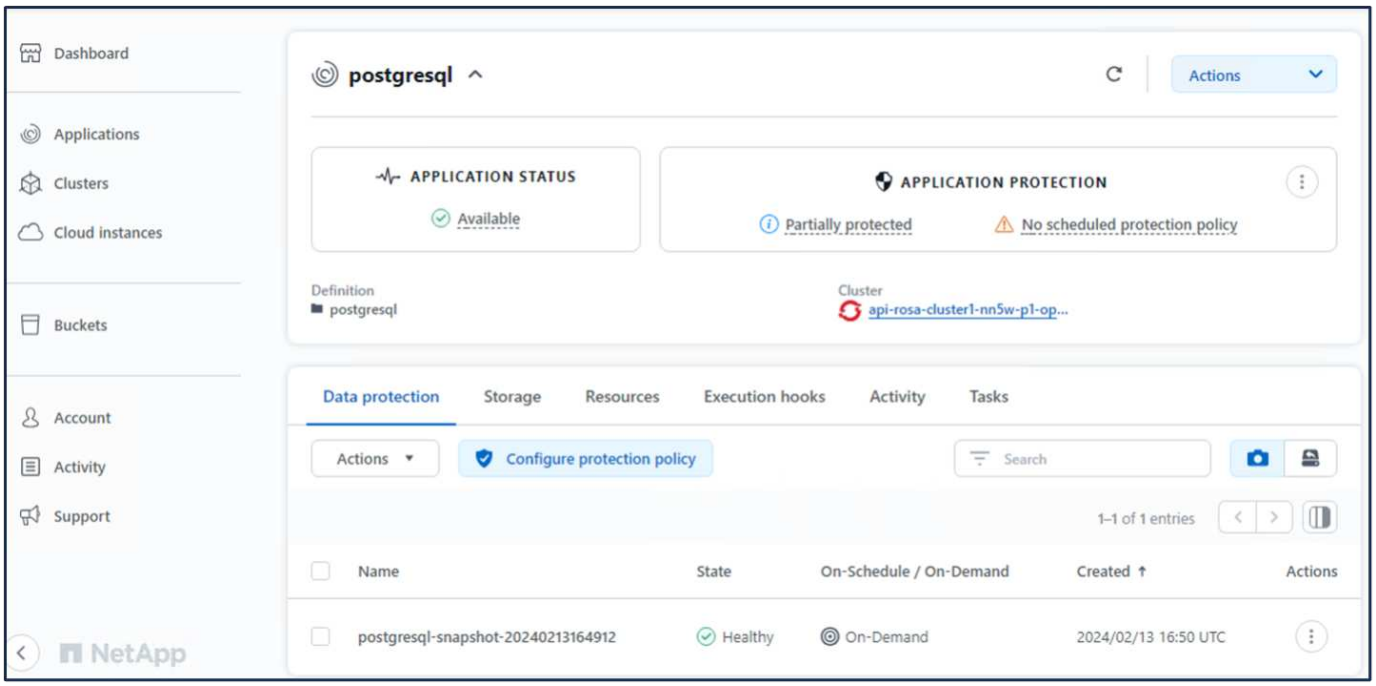
11.使用 **ACS** 從快照還原

若要從快照還原應用程式、請前往 ACS UI 登陸頁面、選取應用程式、然後選取還原。您需要選擇要還原的快照或備份。（通常、您會根據已設定的原則建立多個）。在接下來的幾個畫面中做出適當的選擇、然後按一下 * 還

原 * 。應用程式狀態會在從快照還原後、從還原移至可用狀態。







12.確認您的應用程式已從 **SnapShot** 中還原

登入 PostgreSQL 用戶端、您現在應該會在先前的表格中看到表格和記錄。 就是這樣。只要按一下按鈕、您的應用程式就會還原至先前的狀態。這就是我們利用 Astra Control 為客戶打造的簡單方式。

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```


資料移轉

本頁顯示使用適用於 NetApp ONTAP 的 FSX 進行持續儲存的託管 Red Hat OpenShift 叢集上的容器工作負載資料移轉選項。

AWS 上的 Red Hat OpenShift 服務以及適用於 NetApp ONTAP 的 FSx （ FSxN ）是 AWS 服務產品組合的一部分。FSxN 適用於單一 AZ 或多 AZ 選項。Multi-Az 選項可提供資料保護、避免可用性區域故障。FSxN 可與 Astra Trident 整合、為 ROSA 叢集上的應用程式提供持續儲存。

使用 **Helm** 圖表將 **FSxN** 與 **Trident** 整合

ROSA 叢集整合 Amazon FSX for ONTAP

容器應用程式的移轉包括：

- 持續磁碟區：這可以使用 BlueXP 來完成。另一個選項是使用 Astra Control Center 來處理從內部部署移轉至雲端環境的容器應用程式。自動化可用於相同用途。
- 應用程式中繼資料：這可以使用 OpenShift GitOps （ Argo CD ）來完成。

使用 **FSxN** 進行持續儲存、在 **ROSA** 叢集上容錯移轉及容錯回復應用程式

以下影片示範使用 BlueXP 和 Argo CD 的應用程式容錯移轉和容錯回復案例。

ROSA 叢集上應用程式的容錯移轉和容錯回復

適用於 **OpenShift Container** 工作負載的資料保護與移轉解決方案