NetApp 混合式多雲端搭配 Red Hat OpenShift

NetApp Solutions

NetApp
April 12, 2024

目錄

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

ONTAP feature highlights

Storage Administration

- Multi-tenancy
- FlexVol & FlexGroup
- LUN
- Quotas
- ONTAP CLI & API
- System Manager & BlueXP

Performance & Scalability

- FlexCache
- FlexClone
- nconnect, session trunking, multipathing
- Scale-out clusters

Availability & Resilience

- Multi-AZ HA deployment (MetroCluster)
- SnapShot & SnapRestore
- SnapMirror
- SnapMirror Business Continuity
- SnapMirror Cloud

Access Protocols

- NFS –v3, v4, v4.1, v4.2
- SMB – v2, v3
- iSCSI
- Multi-protocol access

Storage Efficiency

- Deduplication & Compression
- Compaction
- Thin provisioning
- Data Tiering (Fabric Pool)

Security & Compliance

- Fpolicy & Vscan
- Active Directory integration
- LDAP & Kerberos
- Certificate based authentication

- 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。

Astra Trident CSI feature highlights

CSI specific

- CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies
- CSI topology
- Volume expansion

Security

- Dynamic-export policy management
- iSCSI initiator-groups dynamic management
- iSCSI bidirectional CHAP

Control

- Storage and performance consumption
- Monitoring
- Volume Import
- Cross Namespace Volume Access

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

- RWO (ReadWriteOnce, i.e 1⇔1)
- RWX (*ReadWriteMany*, i.e 1⇔n)
- ROX (*ReadOnlyMany*)
- RWOP (ReadWriteOnce POD)

Choose your protocol

- NFS
- SMB
- iSCSI

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：

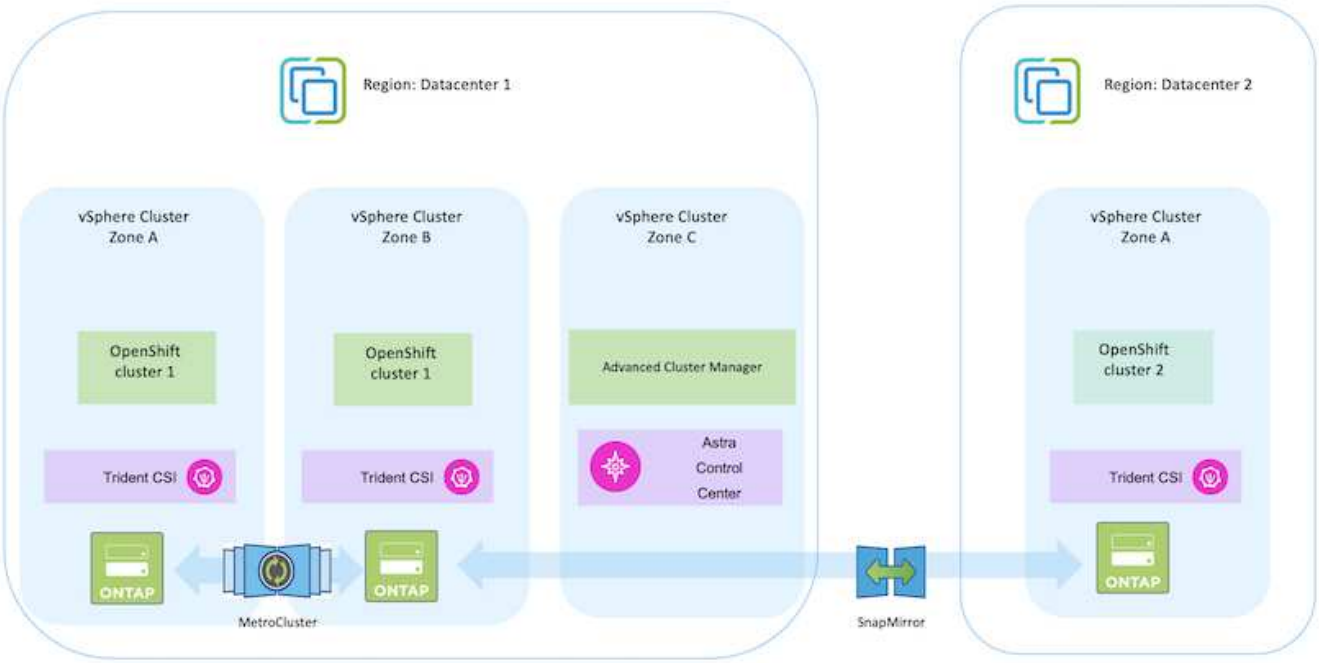
- 內部部署
- 雲端
  - 自我管理的 OpenShift 叢集和自我管理的 NetApp 儲存設備
  - 由供應商管理的 OpenShift 叢集和由供應商管理的 NetApp 儲存設備

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。

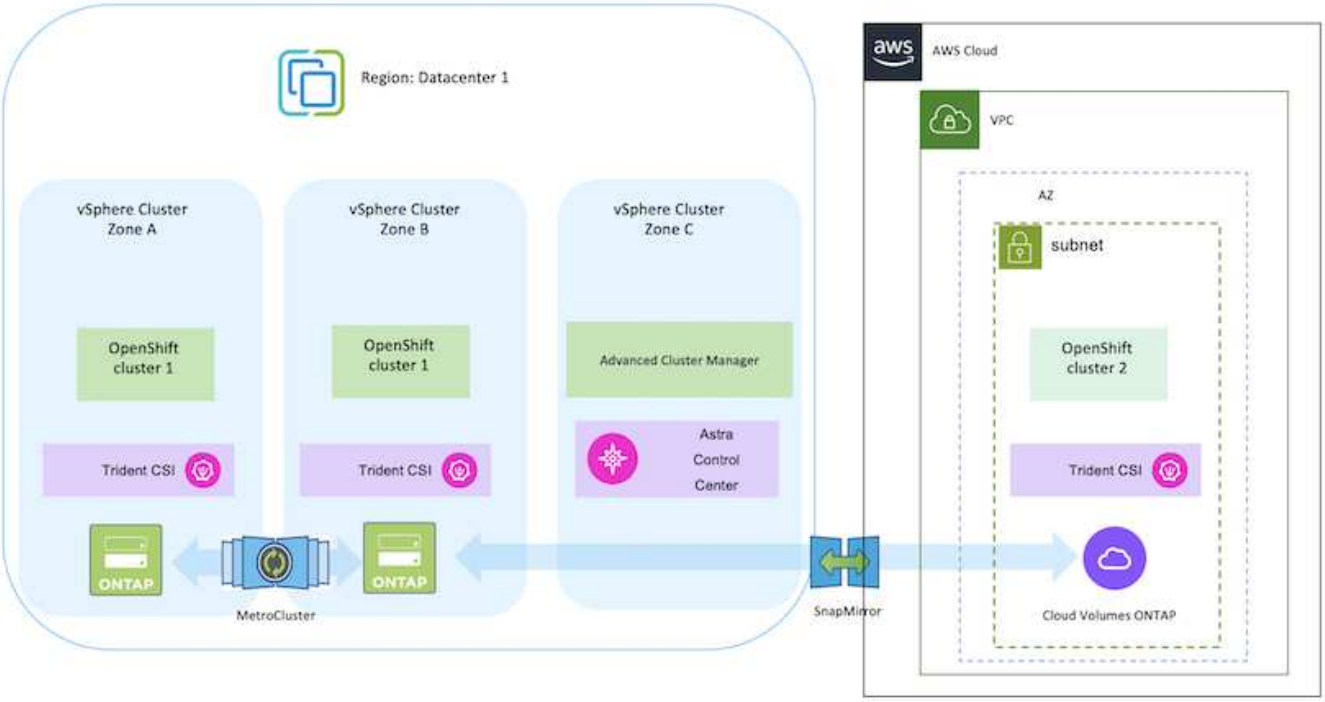
案例**1**



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。

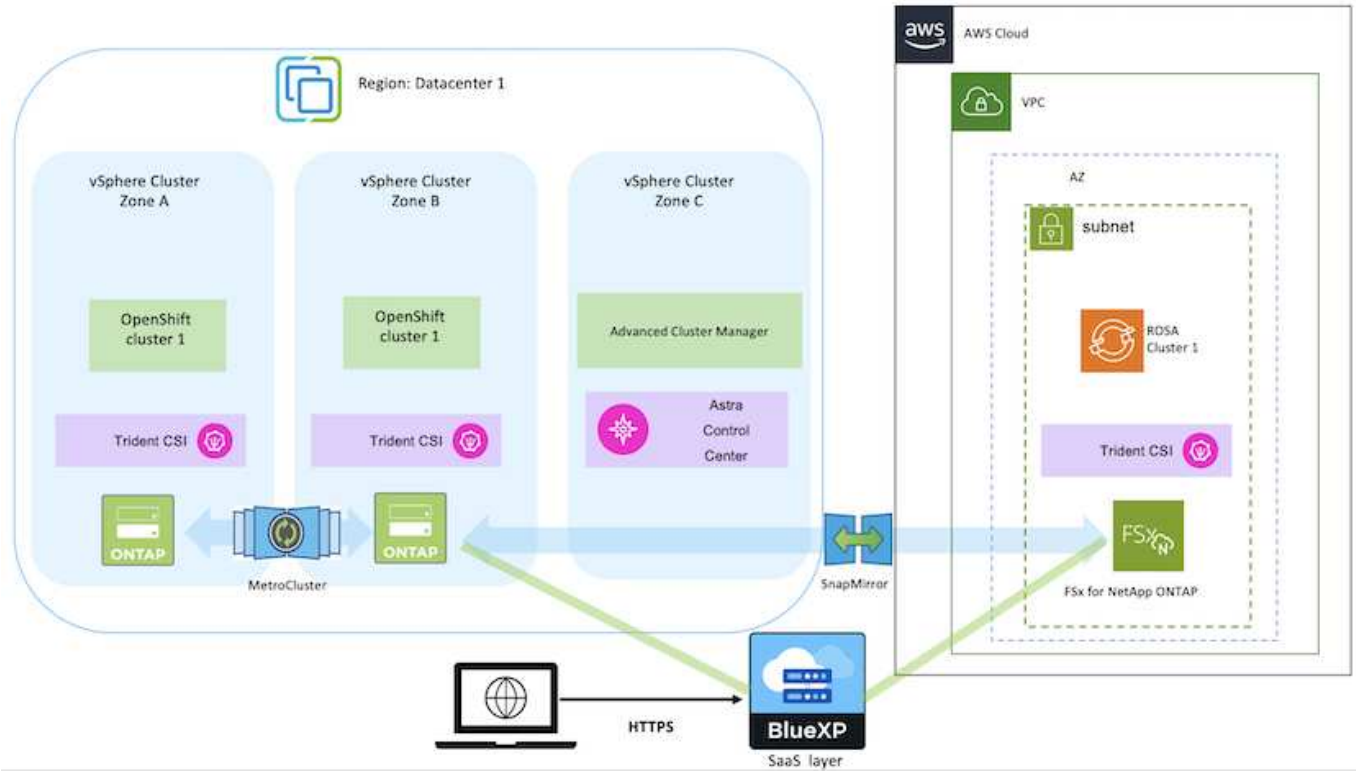
案例**2**



案例 **3** ：資料保護、從內部環境移轉至 **AWS** 環境

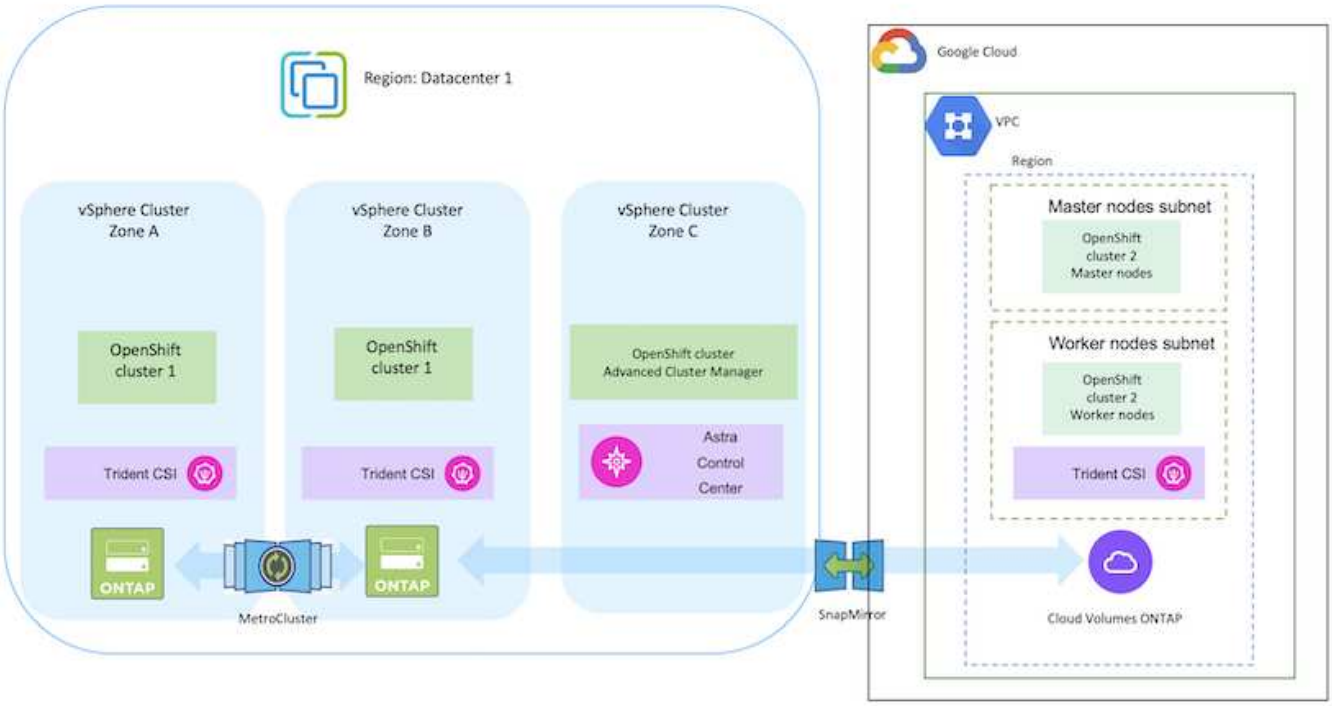
- 內部部署：自我管理的 OpenShift 叢集與自我管理的儲存設備 **AWS Cloud** ：由供應商管理的 **OpenShift** 叢集（**ROSA**）和由供應商管理的儲存設備（**FSxN**）
  - 使用 BlueXP 執行持續磁碟區（FSxN）的複寫。
  - 使用 OpenShift GitOps 重新建立應用程式中繼資料。

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

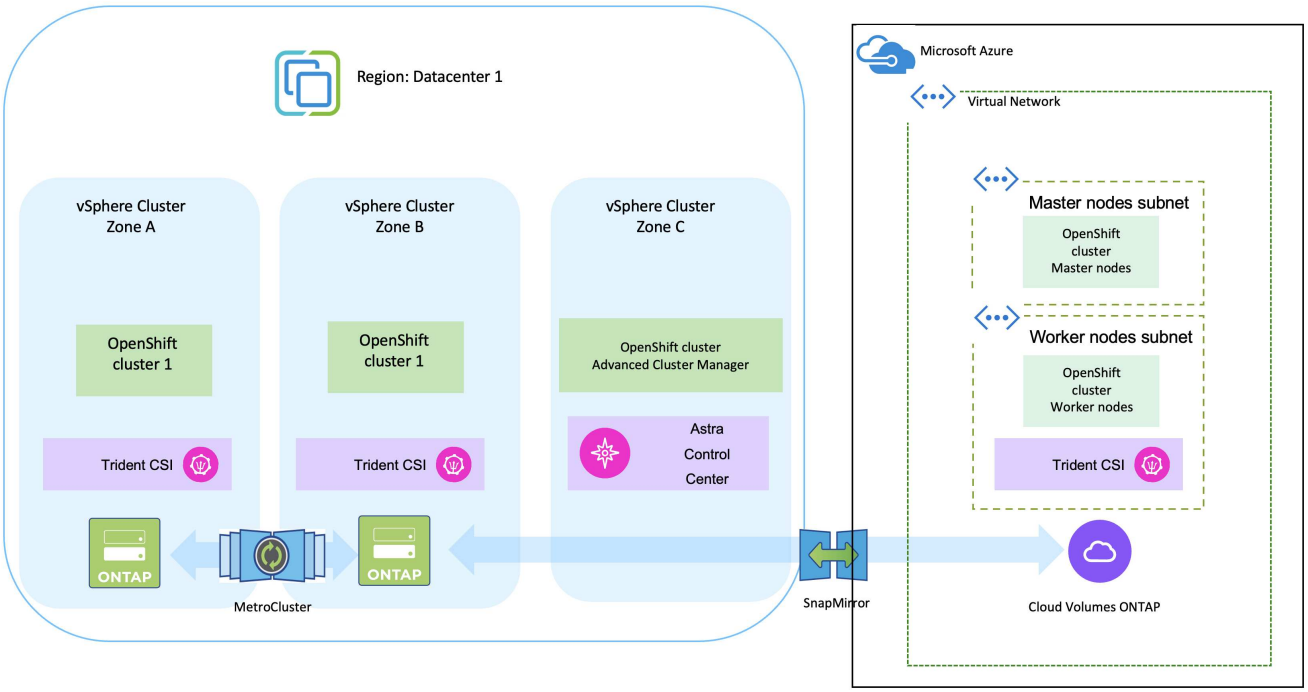
- 內部部署：自我管理的 OpenShift 叢集與自我管理的儲存設備 **
- Google Cloud ：自我管理的 OpenShift 叢集與自我管理的儲存設備 **
  - 使用主動定速控制系統執行備份與還原、以保護資料。
  - 使用 Acc 執行容器應用程式的 SnapMirror 複寫。



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 *	單一 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

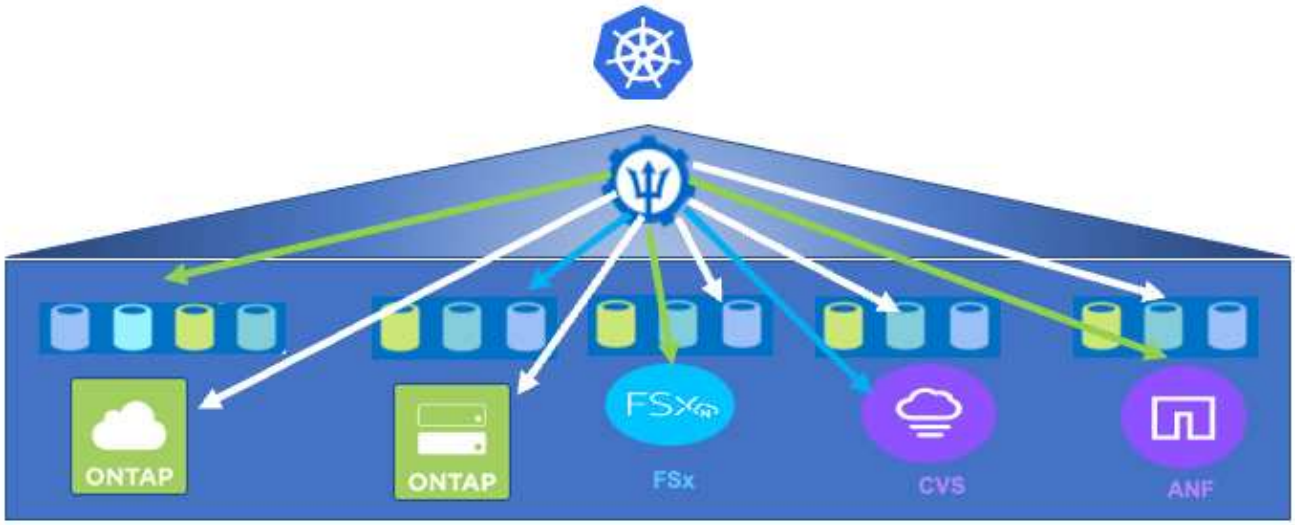
解決方案的案例 5 已使用下表所示的版本進行驗證：

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

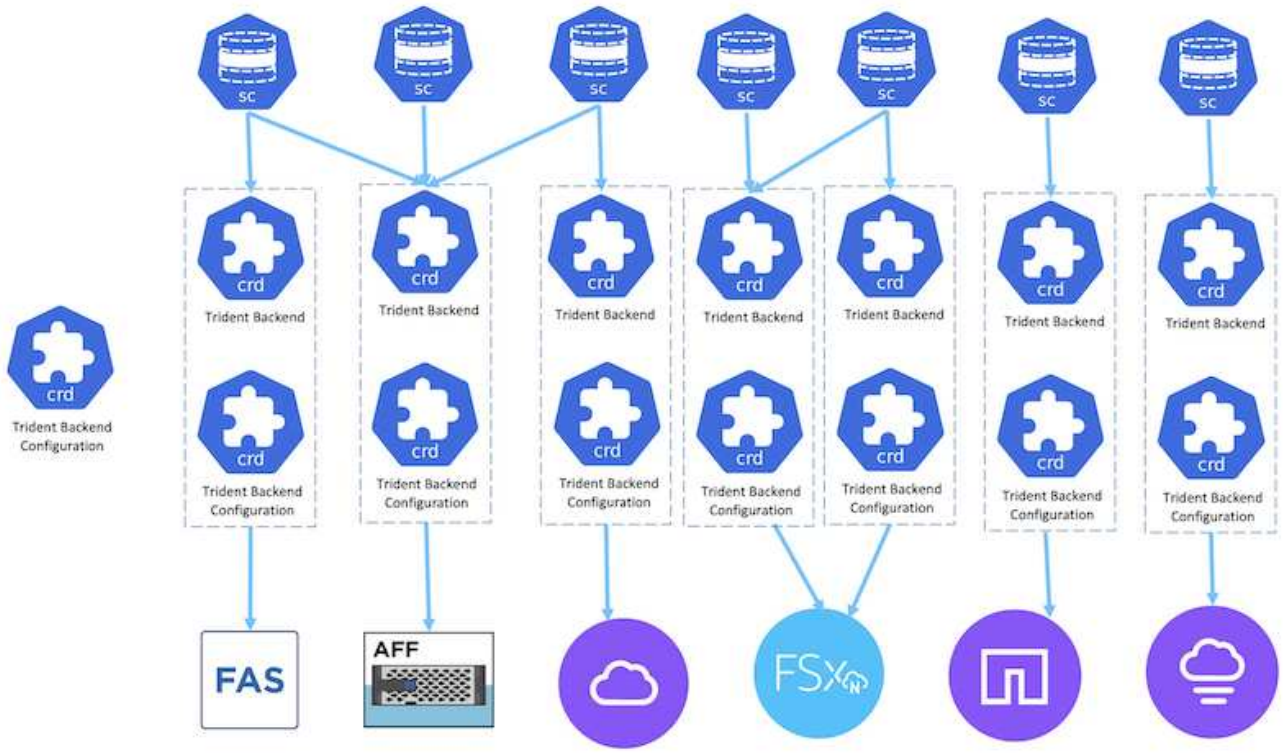
無論 Red Hat Open Shift 容器是在 VMware 上執行、或是在超大規模環境中執行、NetApp Astra Trident 都可作為其支援的各種類型後端 NetApp 儲存設備的 CSI 資源配置程式。

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。

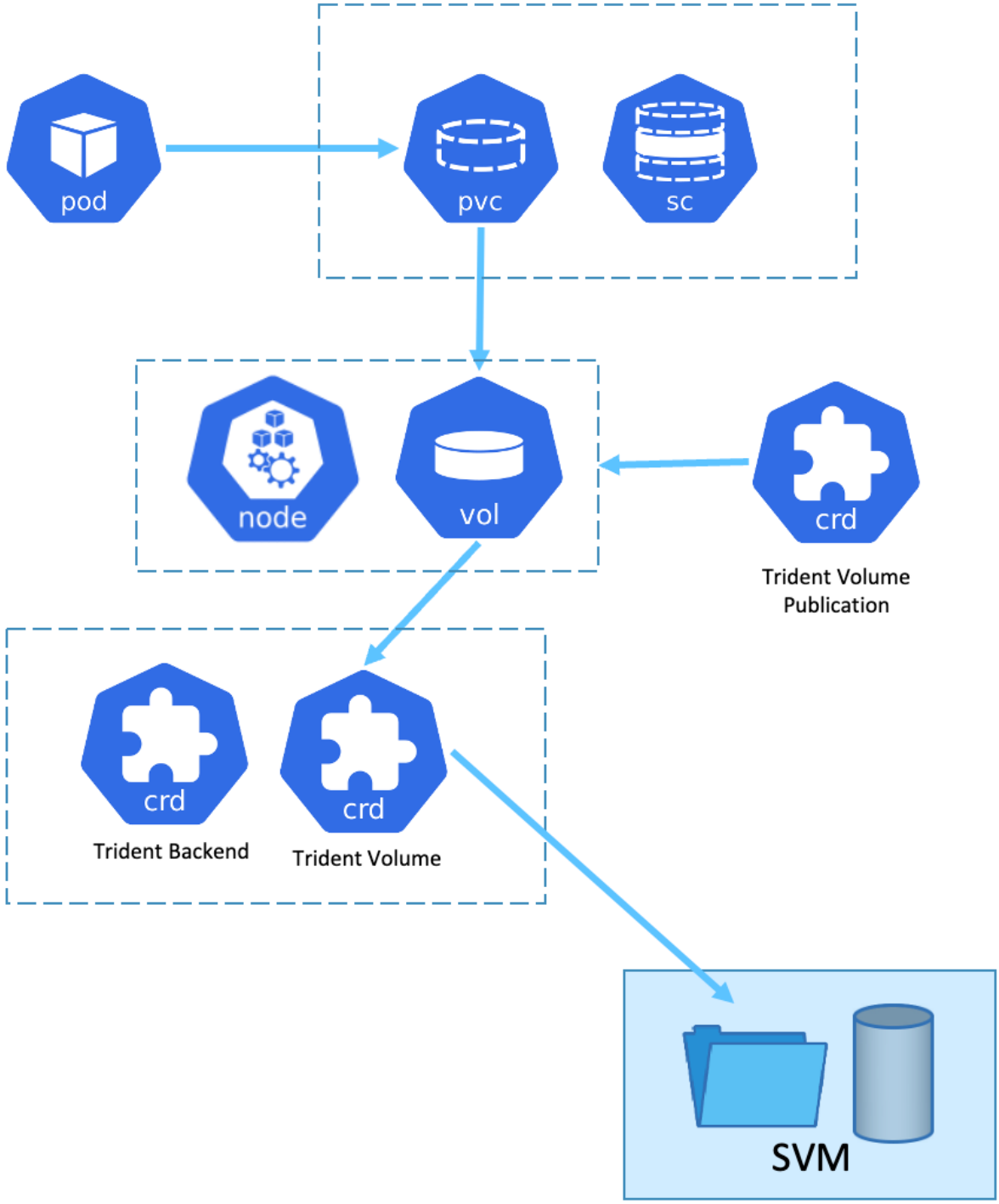


ONTAP 儲存虛擬機器（SVM）提供安全的多租戶共享。單一 OpenShift 叢集可連線至單一 SVM 或多個 SVM、甚至連至多個 ONTAP 叢集。儲存類別會根據參數或標籤來篩選後端儲存設備。儲存管理員會使用 Trident 後端組態來定義連接至儲存系統的參數。成功建立連線時、它會建立 Trident 後端、並填入儲存類別可篩選的資訊。

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

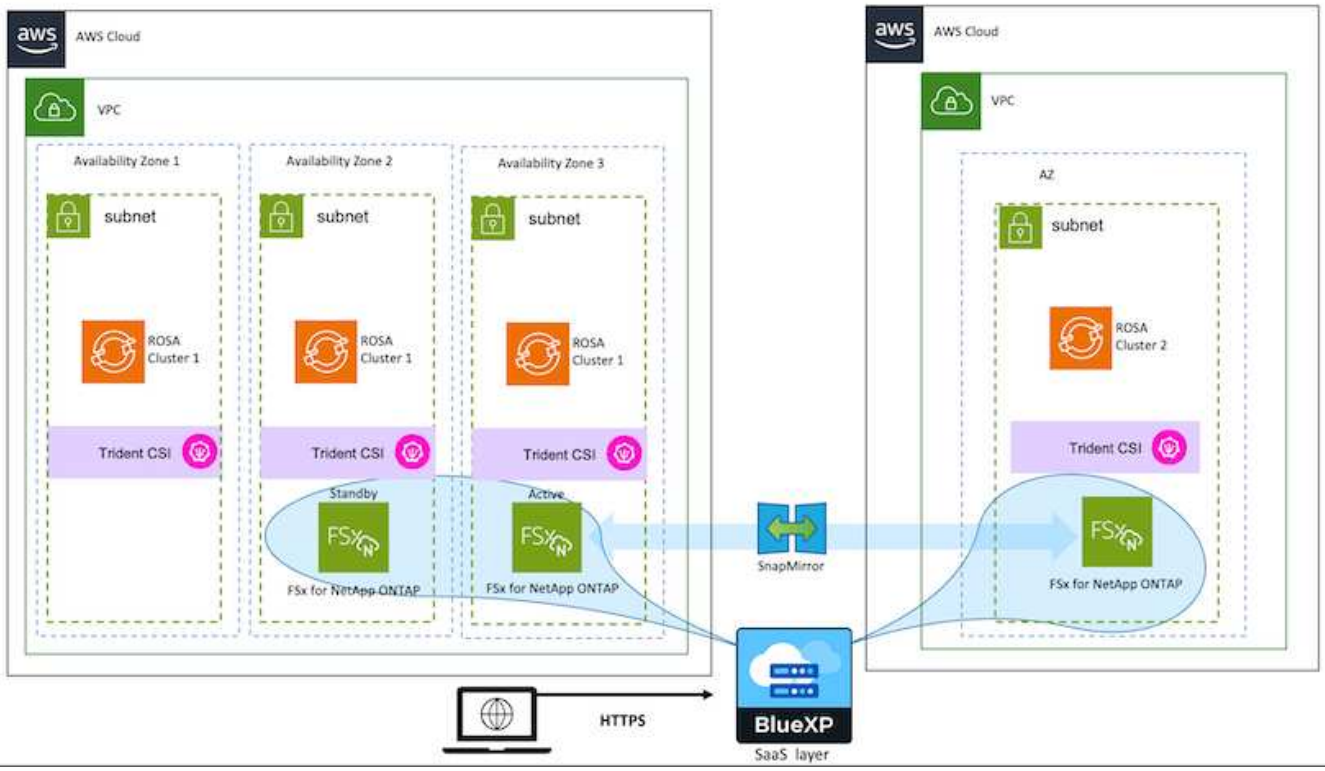
- 核心區塊型資料存放區（FC 、 FCoE 、 iSCSI 、 NVMeoF ）
- 核心檔案型資料存放區（NFS v3 、 v4 ）
- VVOL 資料存放區（區塊和檔案）

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

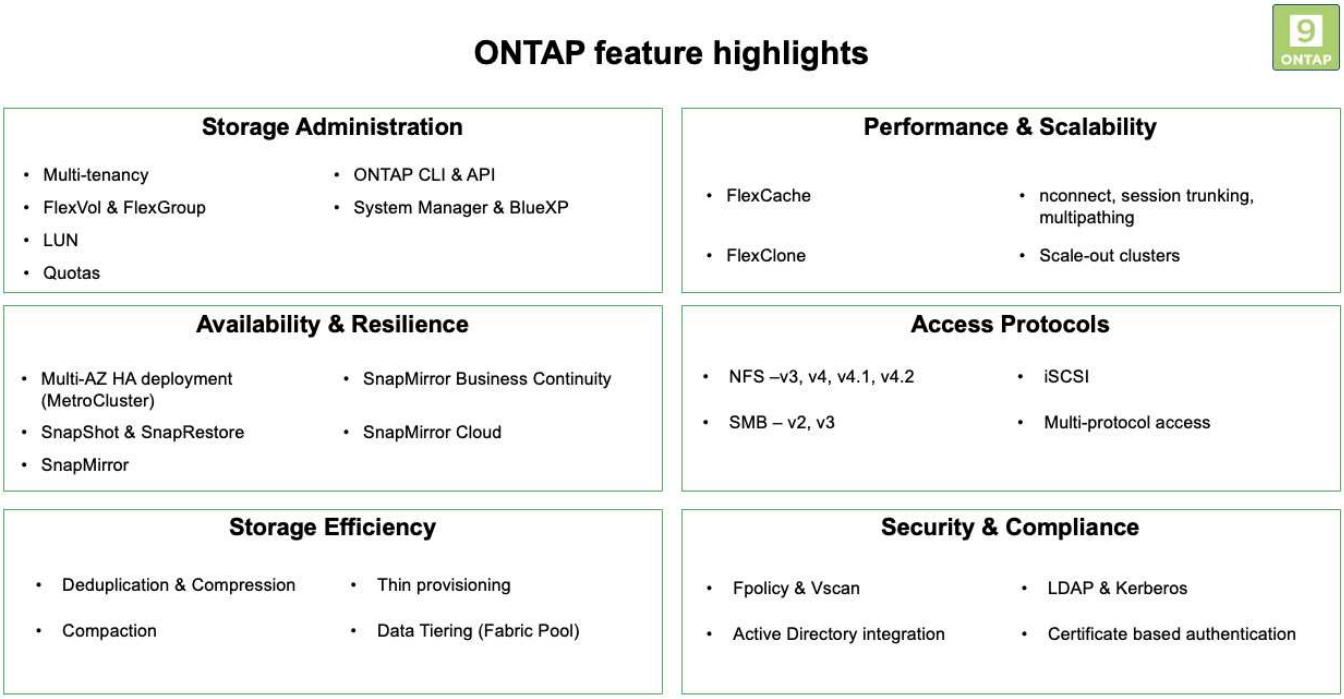
總覽

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。

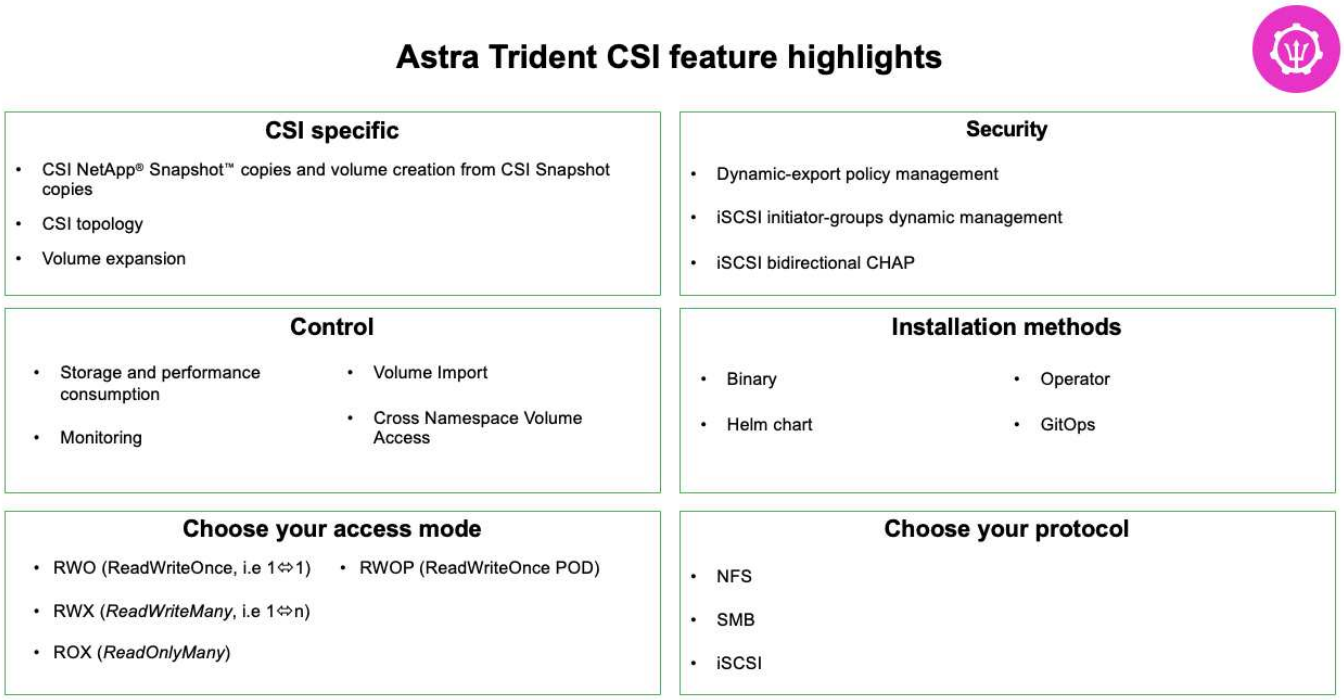
- 內部部署的自我管理儲存設備：
  - NetApp Fabric 附加儲存設備（FAS）、 NetApp All Flash FAS Array （AFF）、 NetApp All SAN Array （ASA）和 ONTAP Select
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（STaaS）
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （CVO）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：
  - Cloud Volumes Service for Google 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

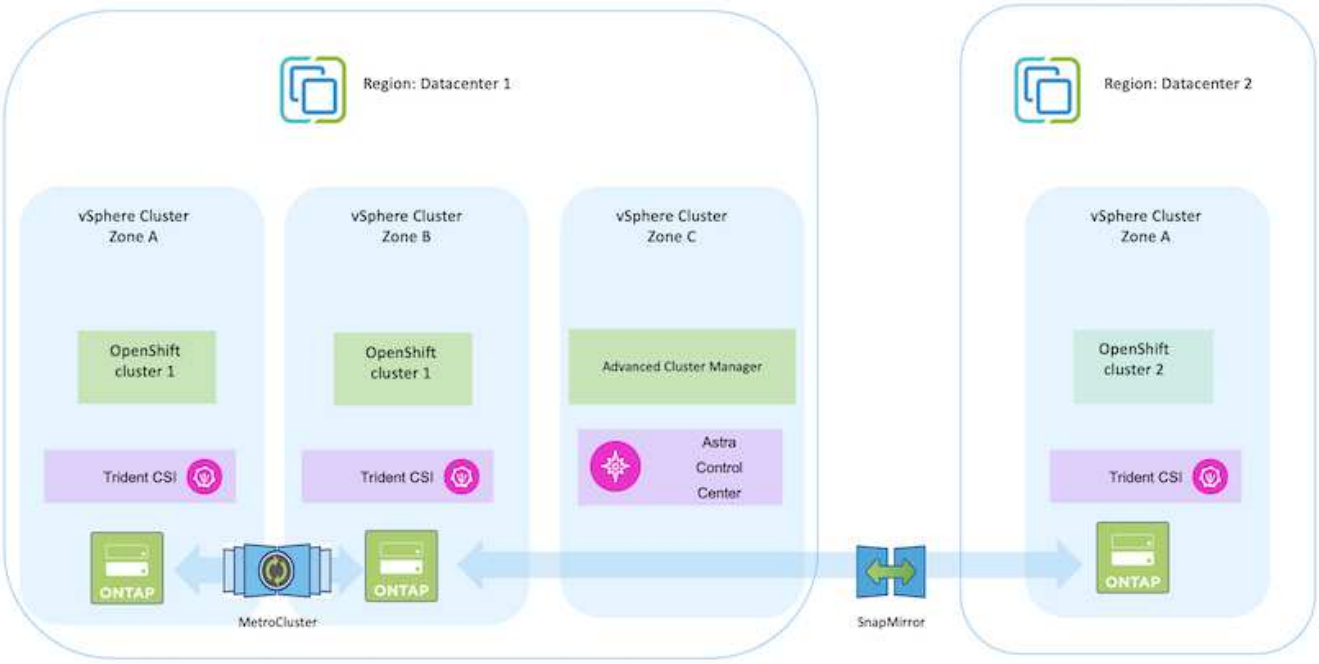
署容器工作負載的正式作業環境。他們的 OCP 叢集可以部署在 VMware 或裸機上。

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

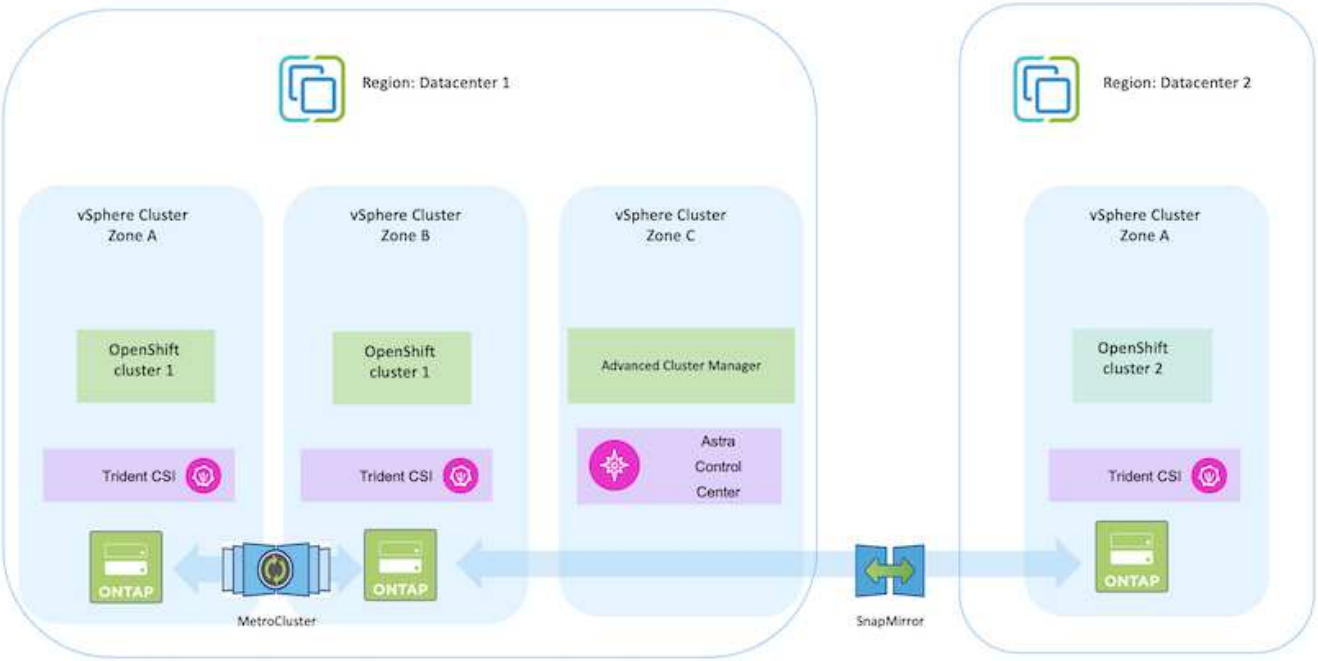


在 **VMware** 上部署和設定 **Red Hat OpenShift Container** 平台

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 — 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。

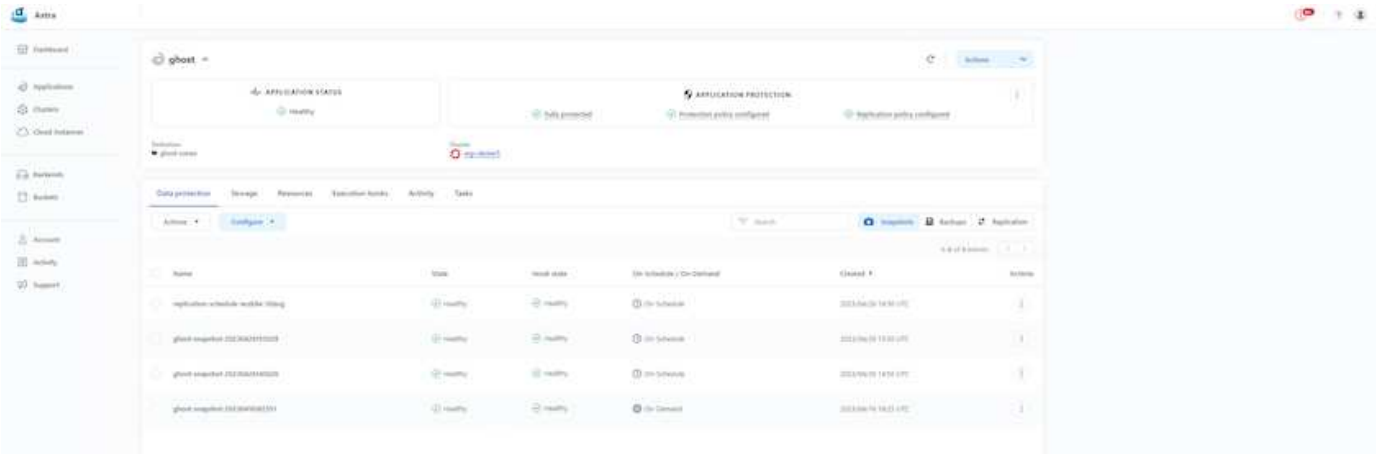
ONTAP 中的資料保護可以使用臨機操作或原則控制的方式來達成 - 快照 - 備份與還原

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**



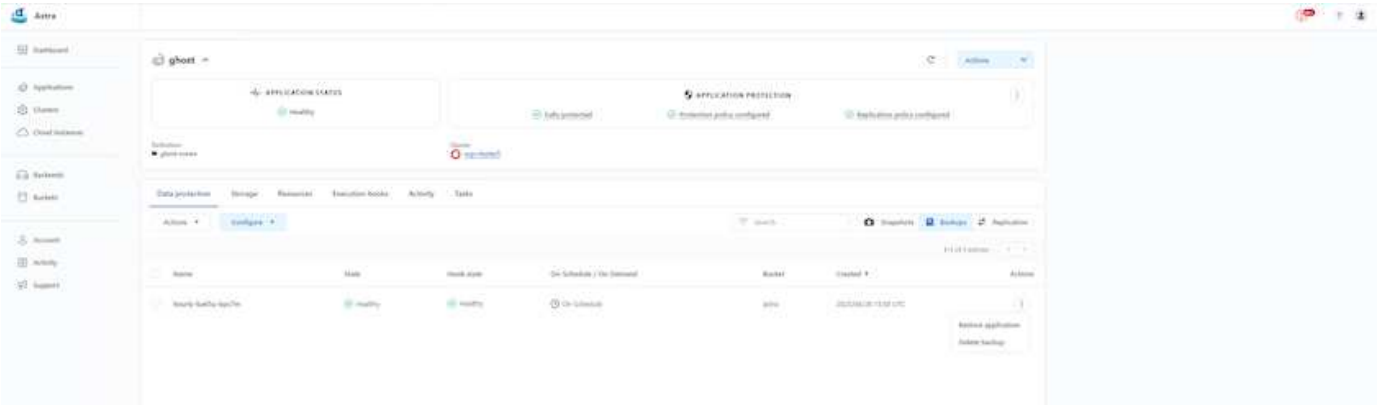
使用 **Acc** 進行備份與還原

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。



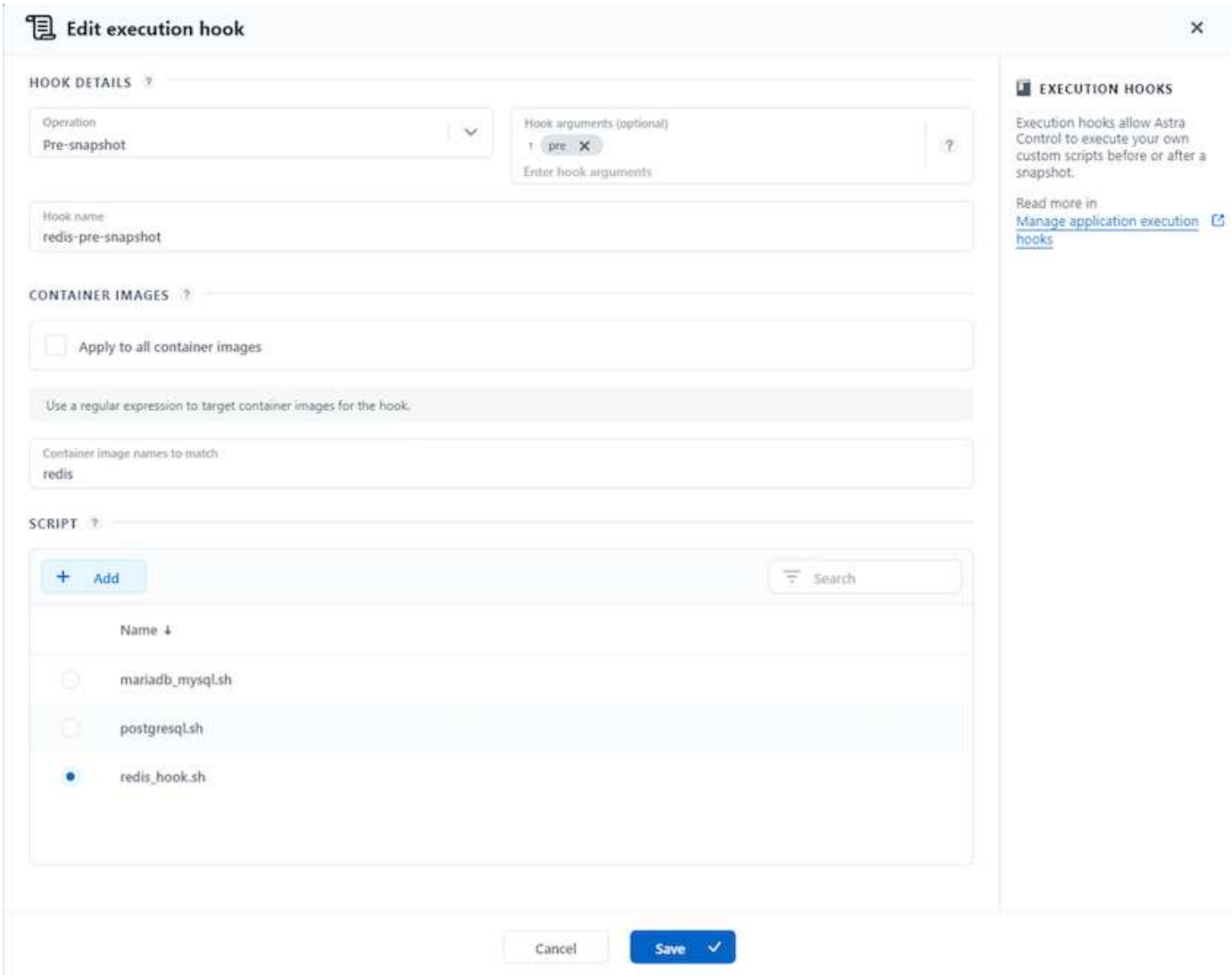
應用程式特定的執行攔截器

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。



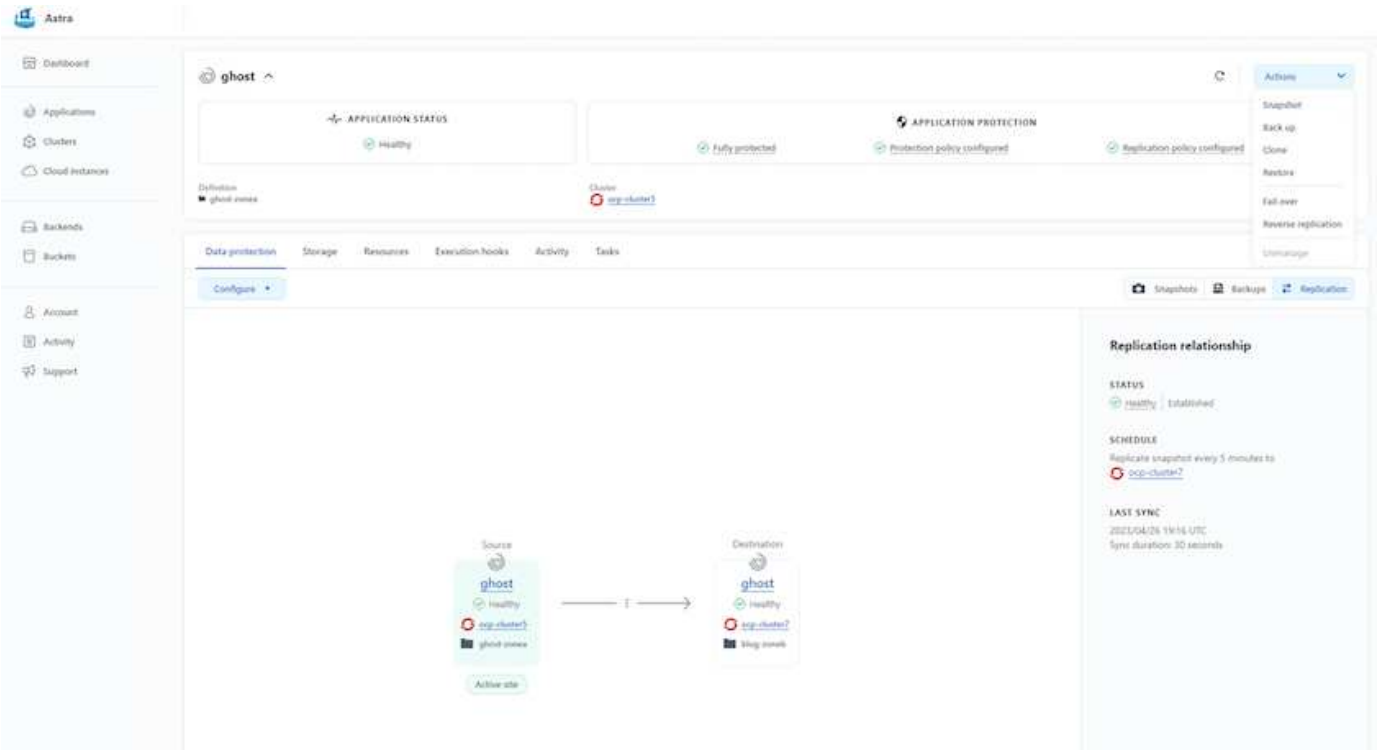
使用 **Acc** 進行複寫

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"

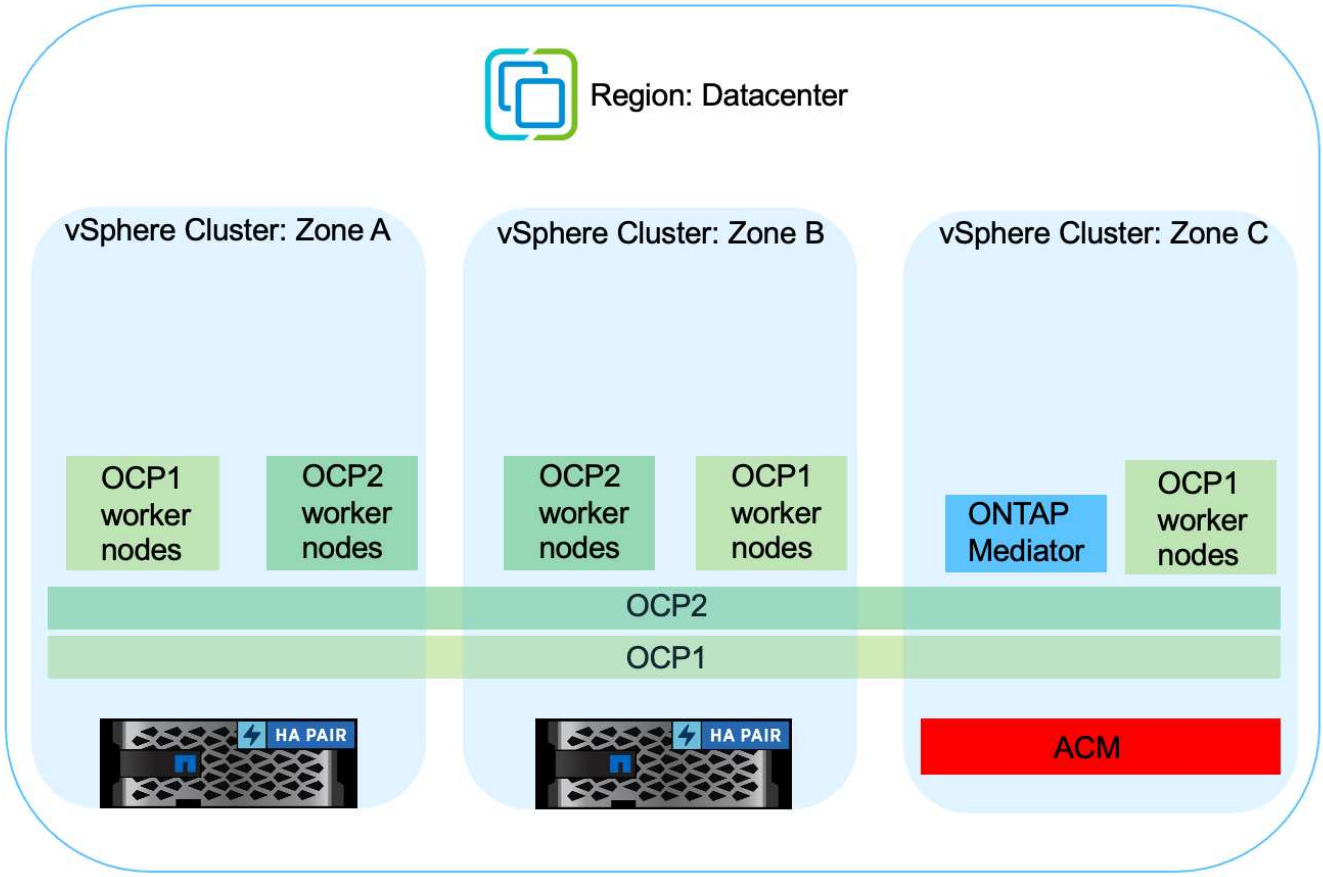
Astra Control Center 提供資料保護功能

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：

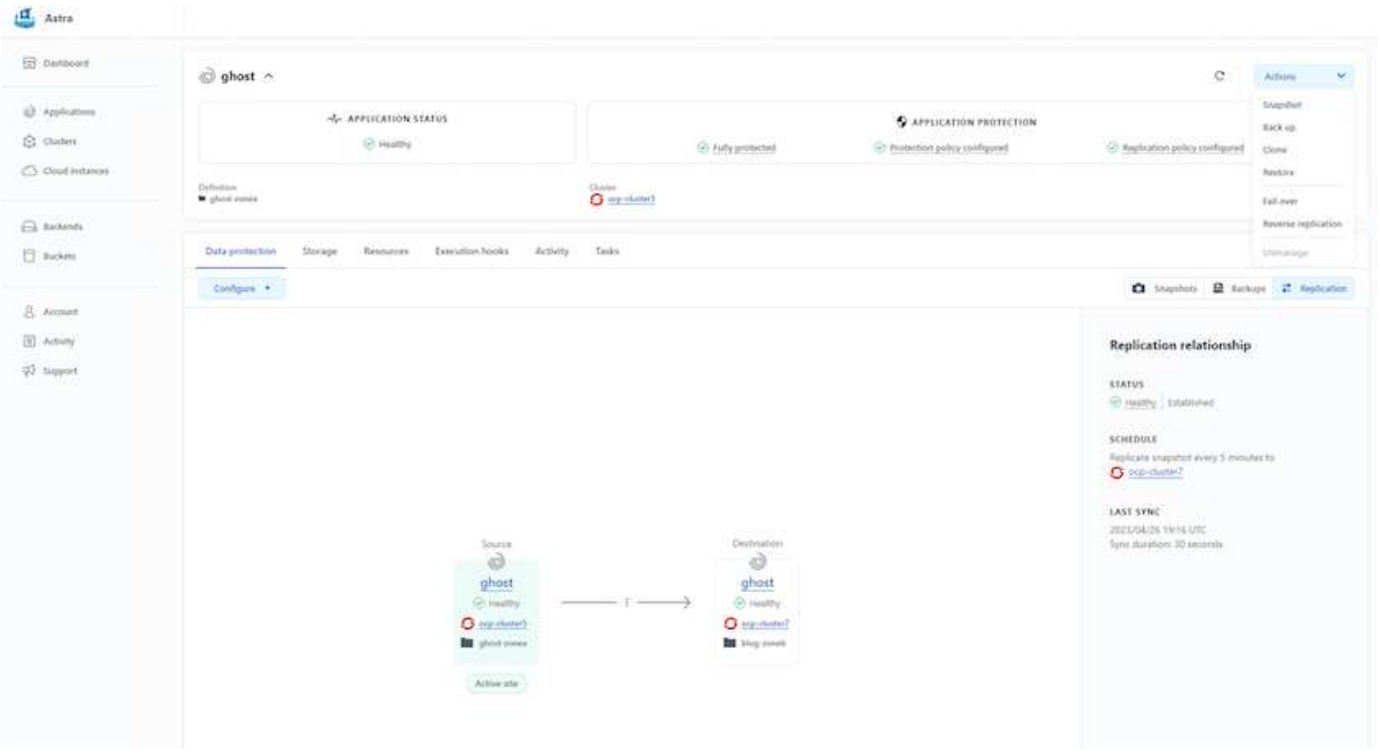
- 複寫
- 備份與還原
- 複製

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

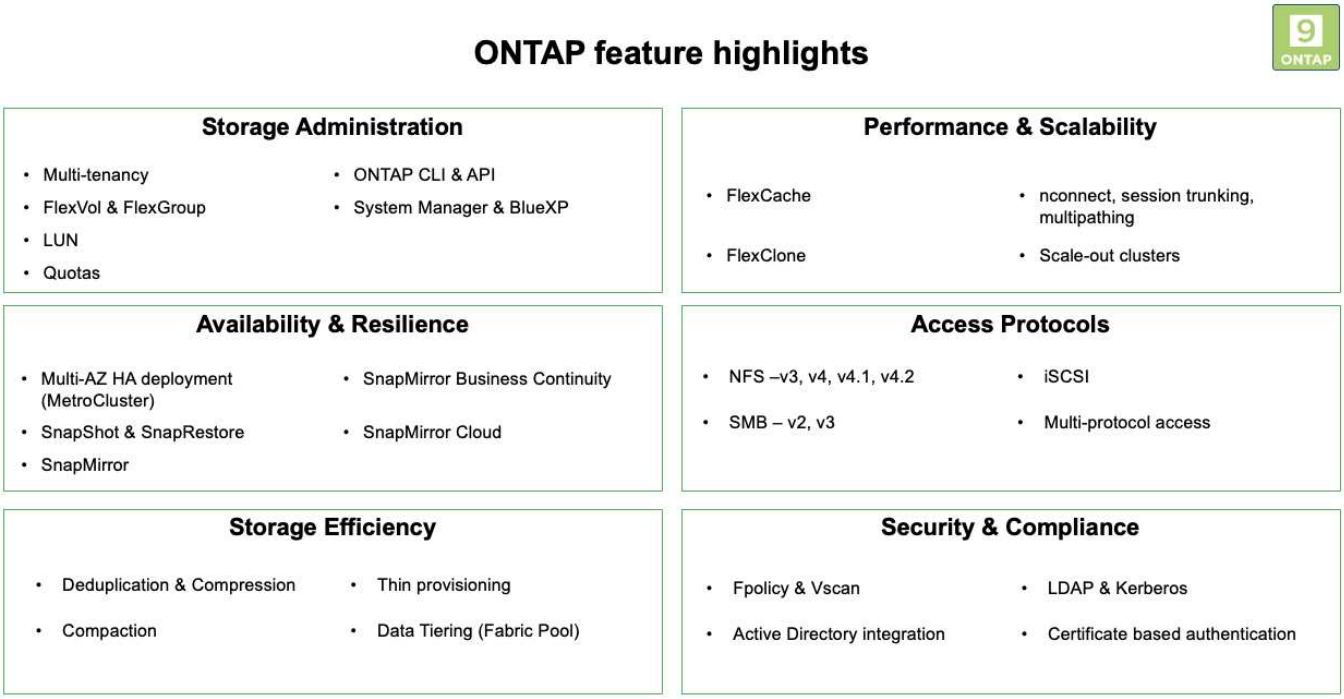
NetApp 發現客戶使用 Kubernetes 建置的容器和協調作業平台、將舊有企業應用程式現代化、並建置新的應用程式。Red Hat OpenShift Container Platform 是我們許多客戶採用的範例之一。

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

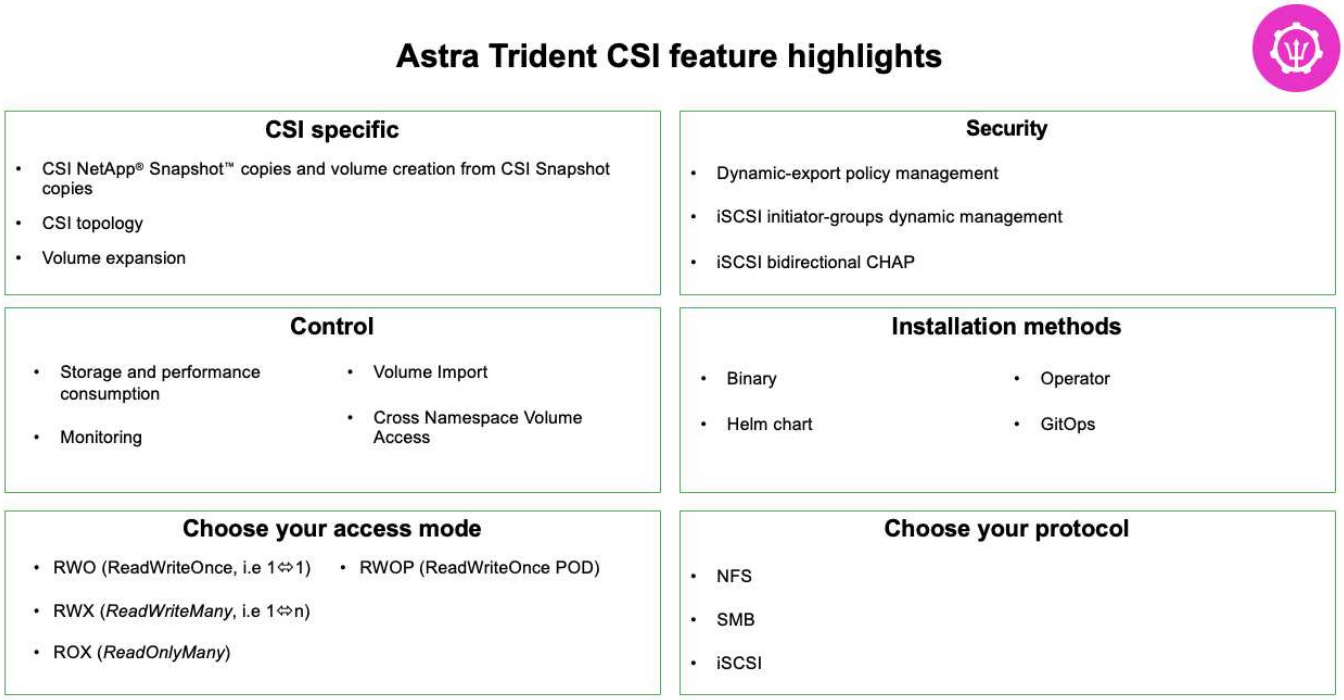
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（STaaS）
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （CVO）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：
  - Cloud Volumes Service for Google Cloud （CVS）、Azure NetApp Files （anf）、Amazon FSX for NetApp ONTAP 可在超大型擴充器中提供完全託管的儲存設備



- 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

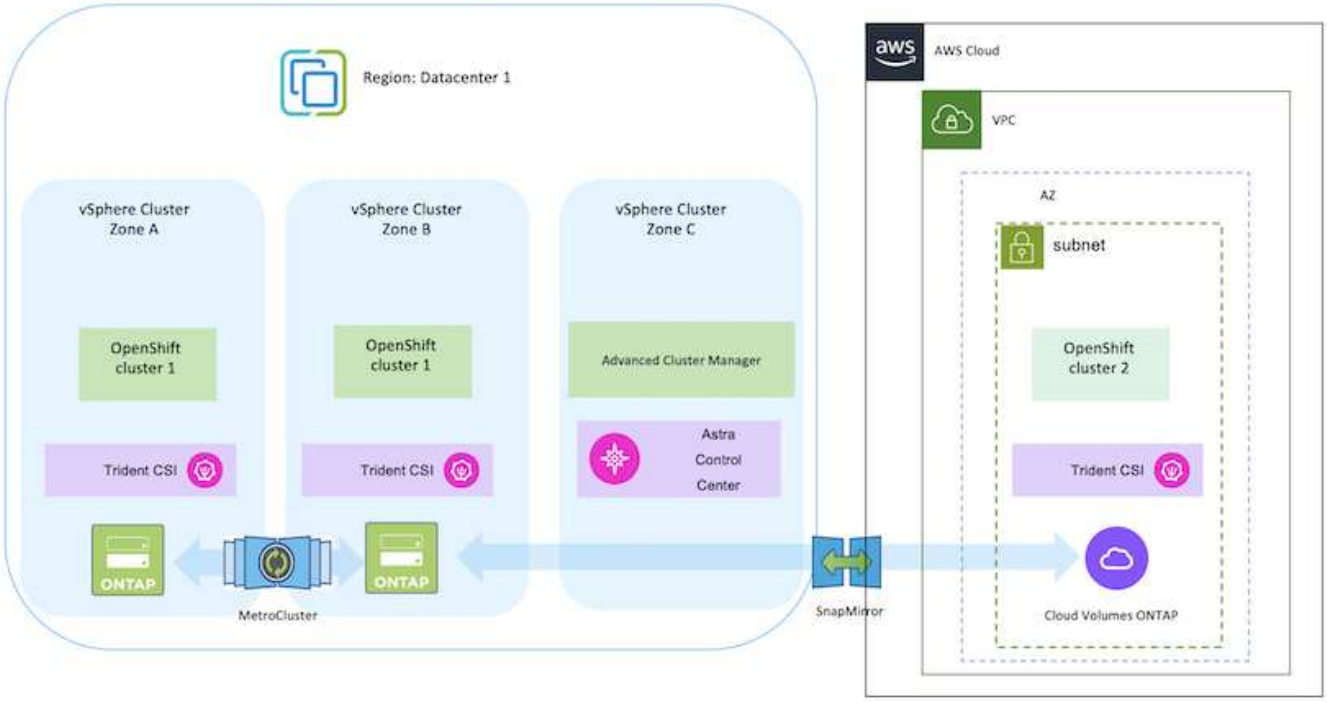
當客戶準備好將某些特定工作負載或所有工作負載從資料中心移至雲端時、他們可能正處於現代化過程的某個階段。他們可能會基於各種原因、選擇在雲端使用自我管理的 OpenShift 容器和自我管理的 NetApp 儲存設備。他們應該規劃並部署雲端中的 Red Hat OpenShift Container 平台（OCP）、以打造成功的正式作業環境、從資料中心移轉其容器工作負載。他們的 OCP 叢集可以部署在 VMware 或裸機上的資料中心、以及雲端環境中的 AWS 、 Azure 或 Google Cloud 上。

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

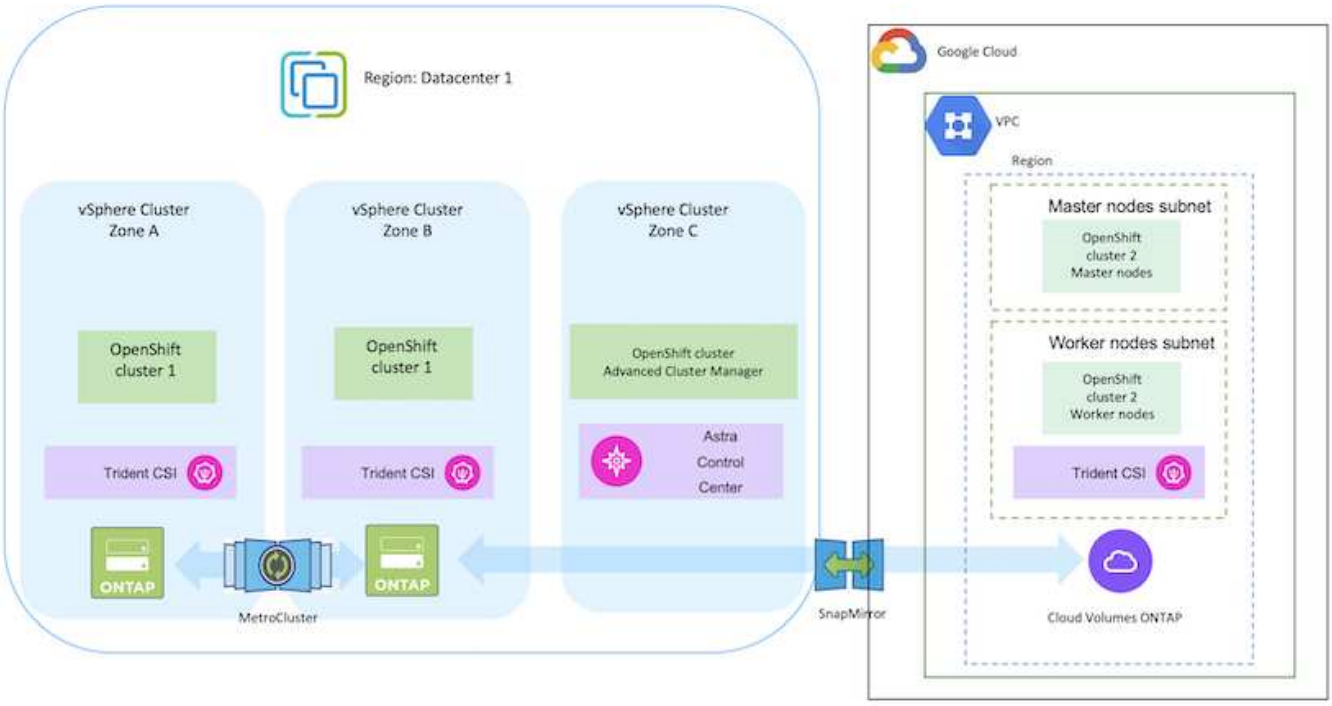
和業務持續運作。

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

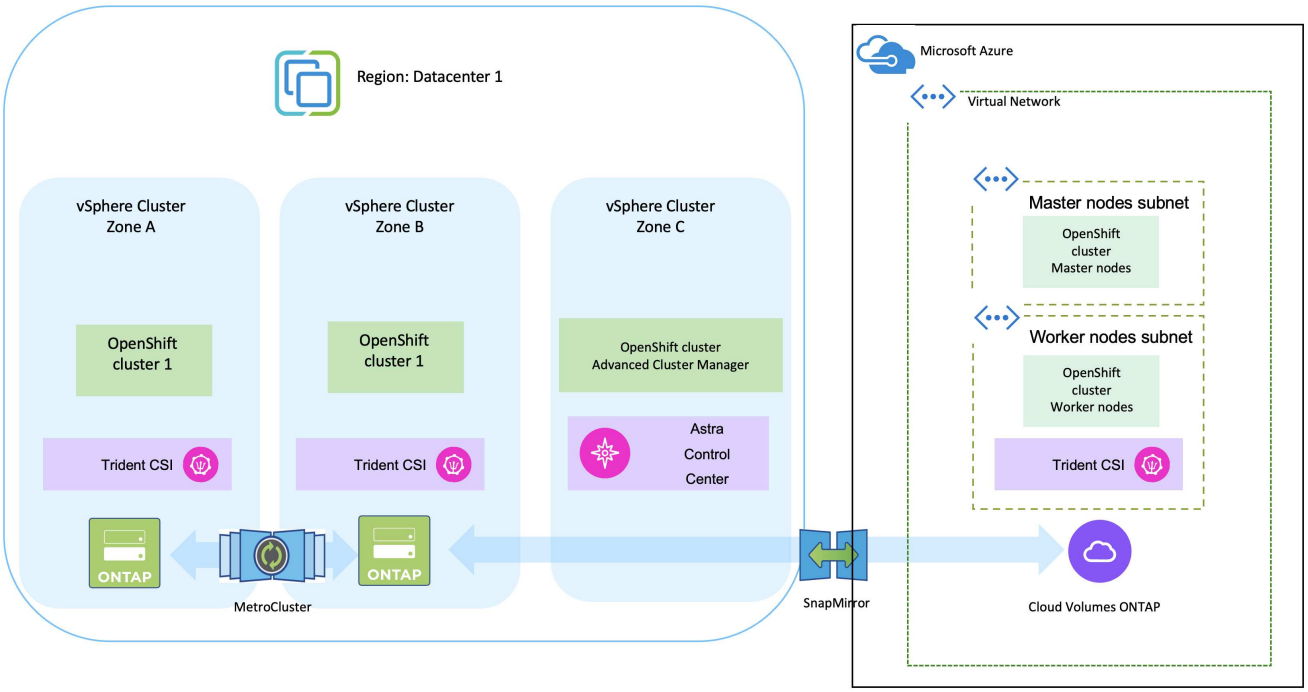
內部部署和 AWS



內部部署和 Google Cloud



內部部署與 Azure Cloud

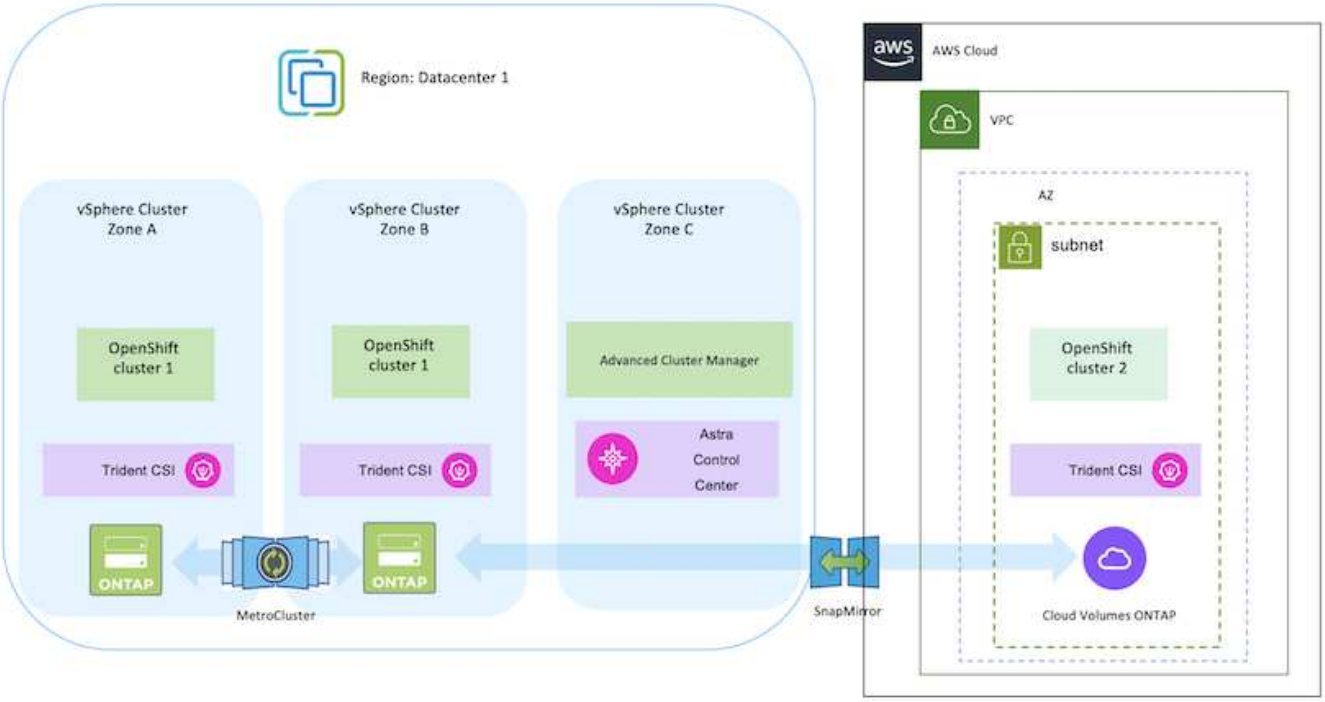


在 **AWS** 上部署和設定 **Red Hat OpenShift Container** 平台

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。

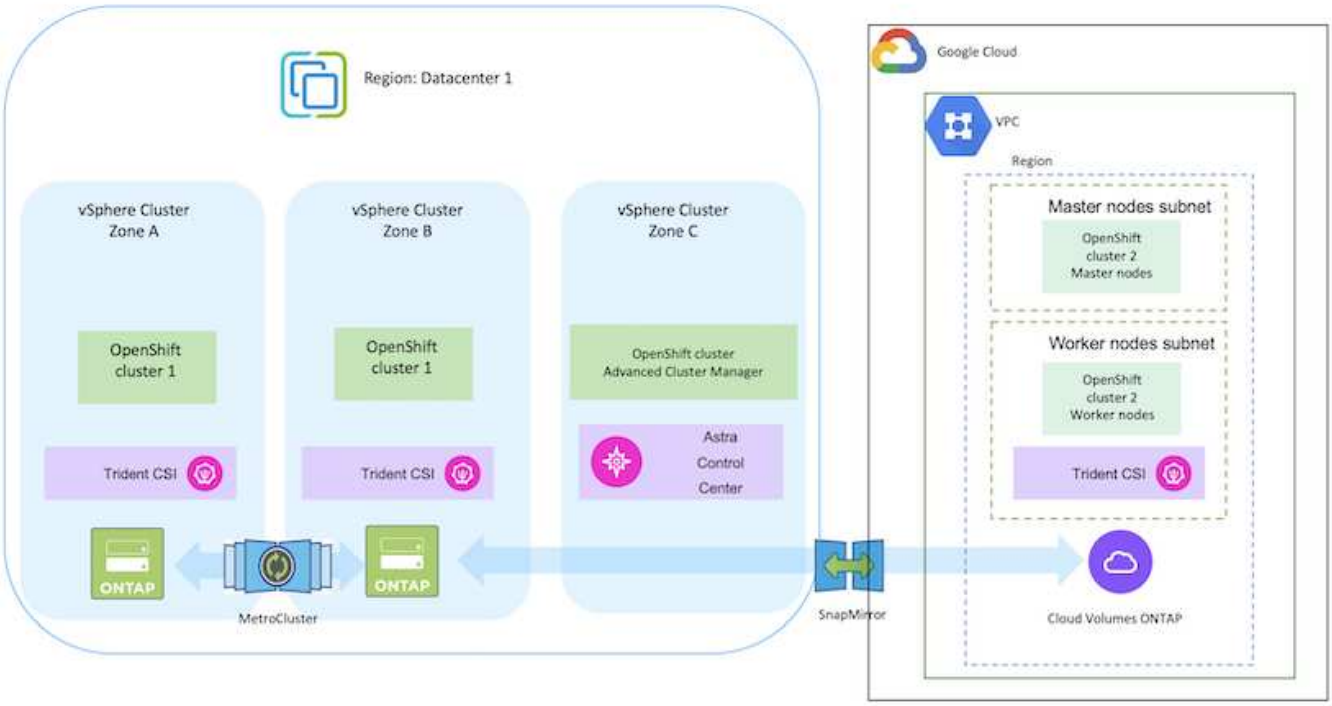
> Kubernetes 支援兩種磁碟區繫結模式： - 當 ***Volume BindingMode*** 設為 ***Immediate*** （預設）時、 Astra Trident 會在沒有任何拓撲感知的情況下建立磁碟區。建立永續性磁碟區時、不會對要求的Pod排程需求有任何相依性。- 當 ***Volume BindingMode*** 設定為 **_WaitForFirstConsumer**（客戶） 時、永久 Volume 的建立與繫結將延遲、直到排程並建立使用 PVC 的 Pod 為止。如此一來、就能建立磁碟區、以符合拓撲需求所強制執行的排程限制。Astra Trident 儲存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

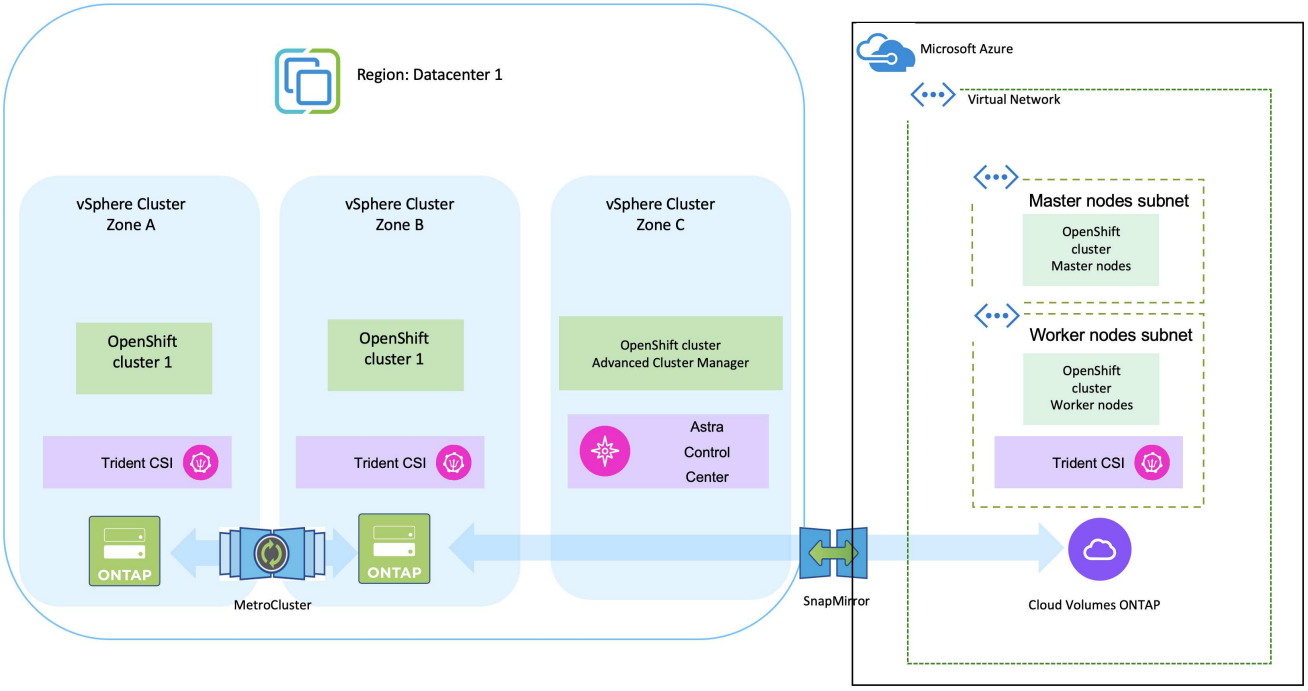
在 **Azure** 上部署及設定 **Red Hat OpenShift Container** 平台

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。

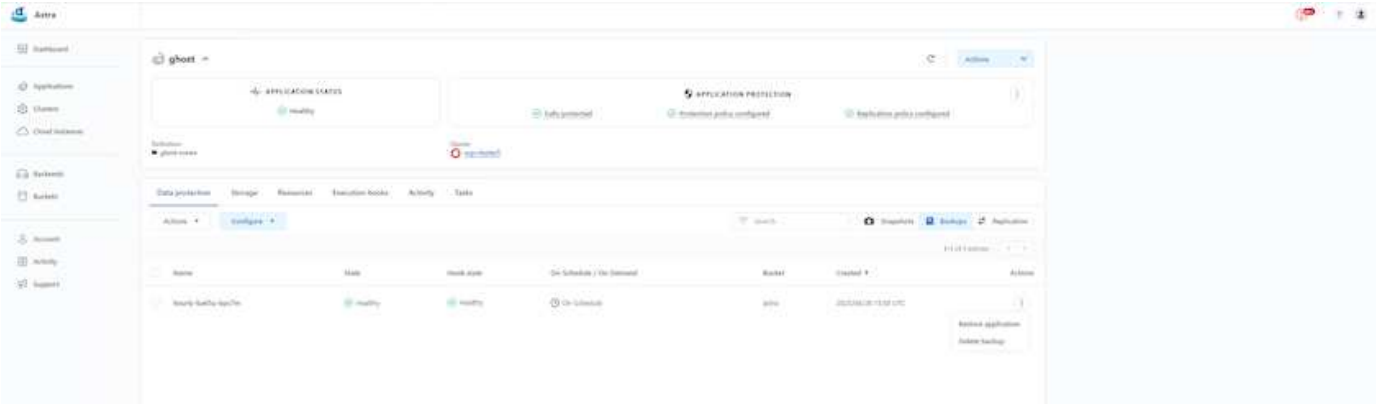
資料保護的需求各不相同、從還原到時間點複本、到自動容錯移轉到不同的故障網域、而無需人為介入。許多客戶選擇 ONTAP 做為其 Kubernetes 應用程式的首選儲存平台、因為其豐富的功能包括多租戶、多重傳輸協定、高效能與容量、多站台位置的複寫與快取、安全性與靈活度。

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

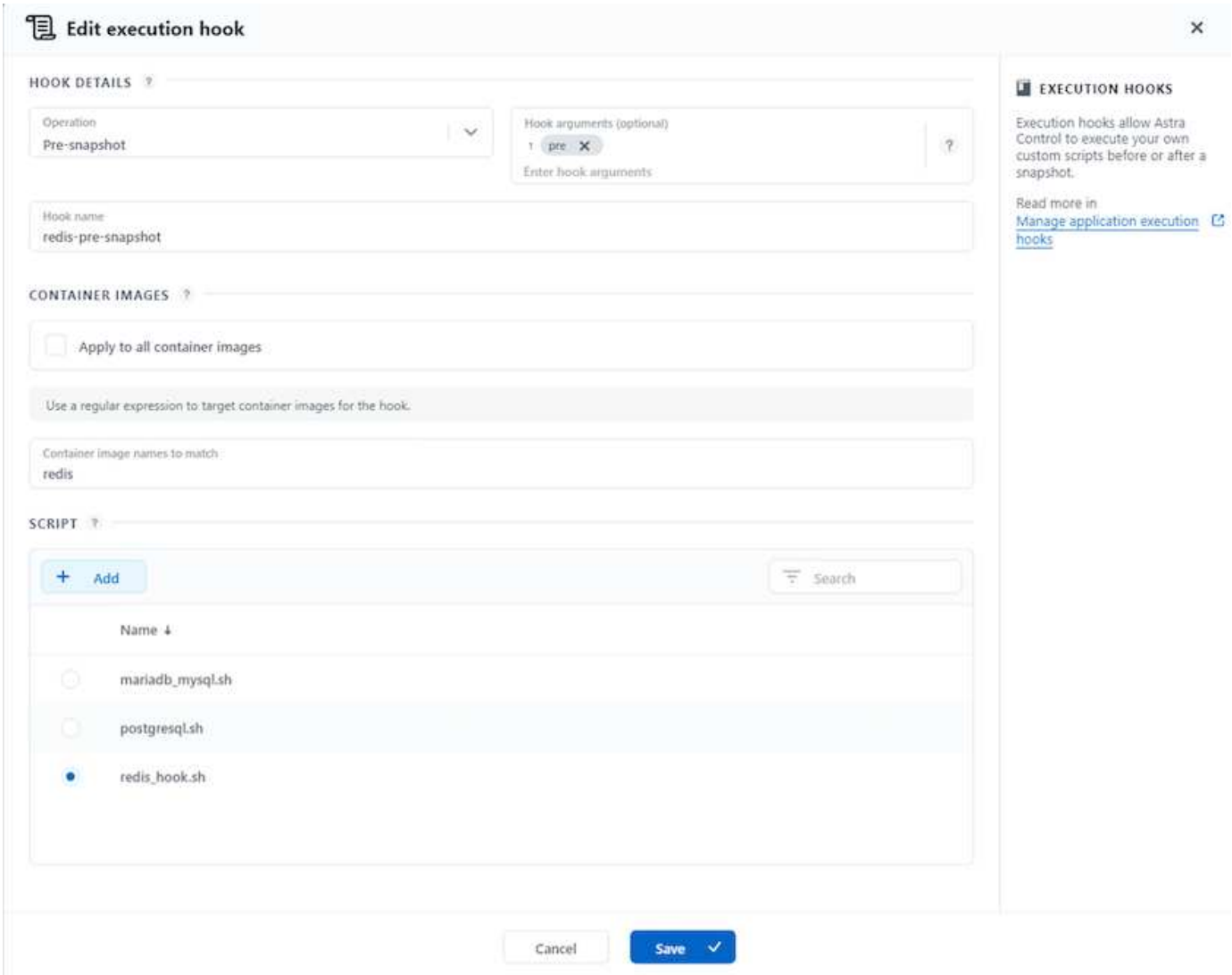


應用程式特定的執行攔截器

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。

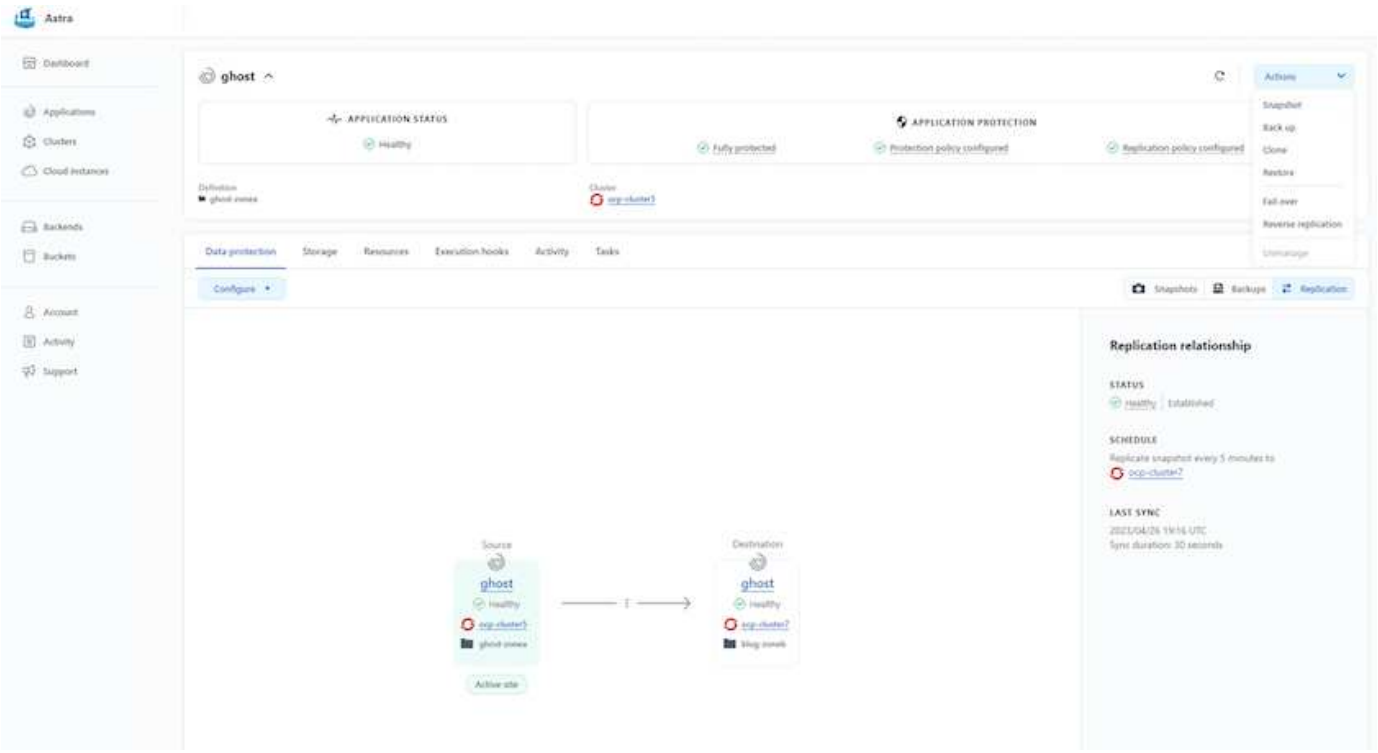
Redis 應用程式快照前的執行掛鉤範例。



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：

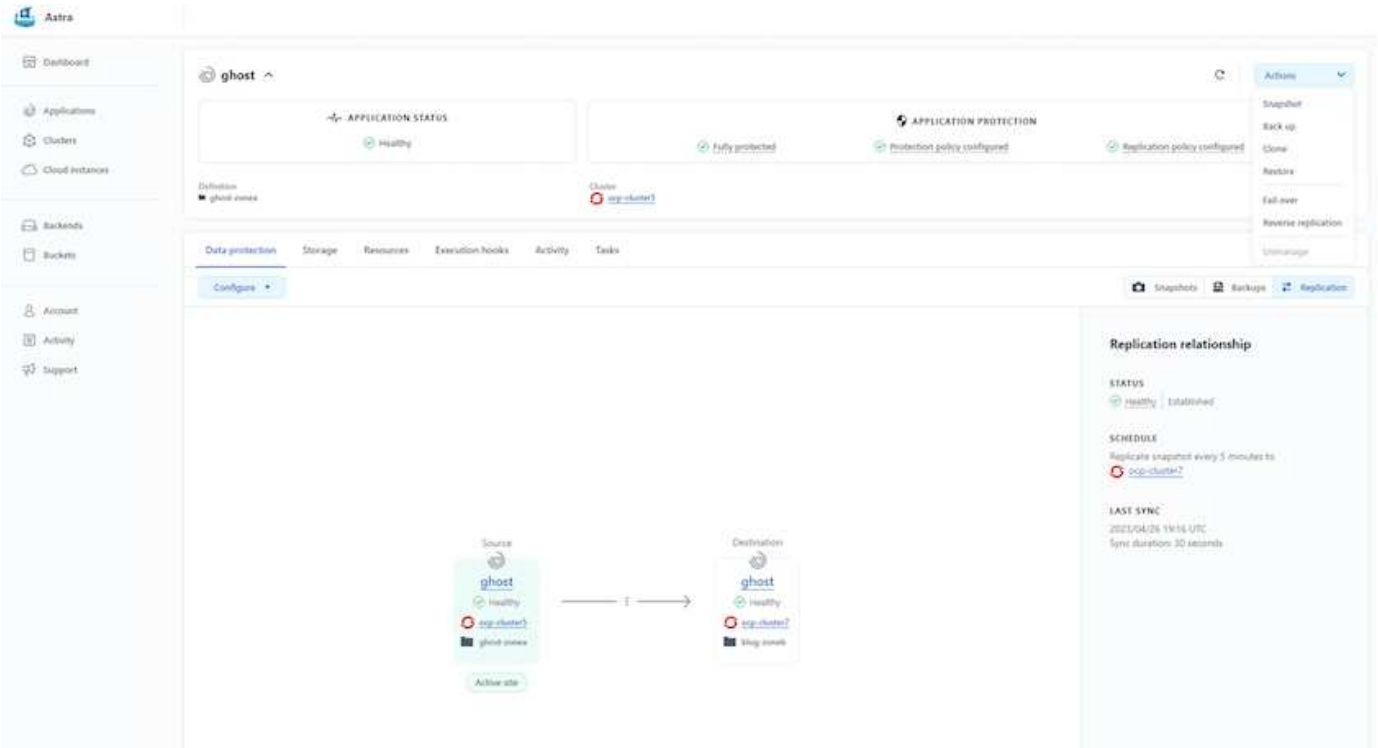
- 複寫
- 備份與還原

- 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

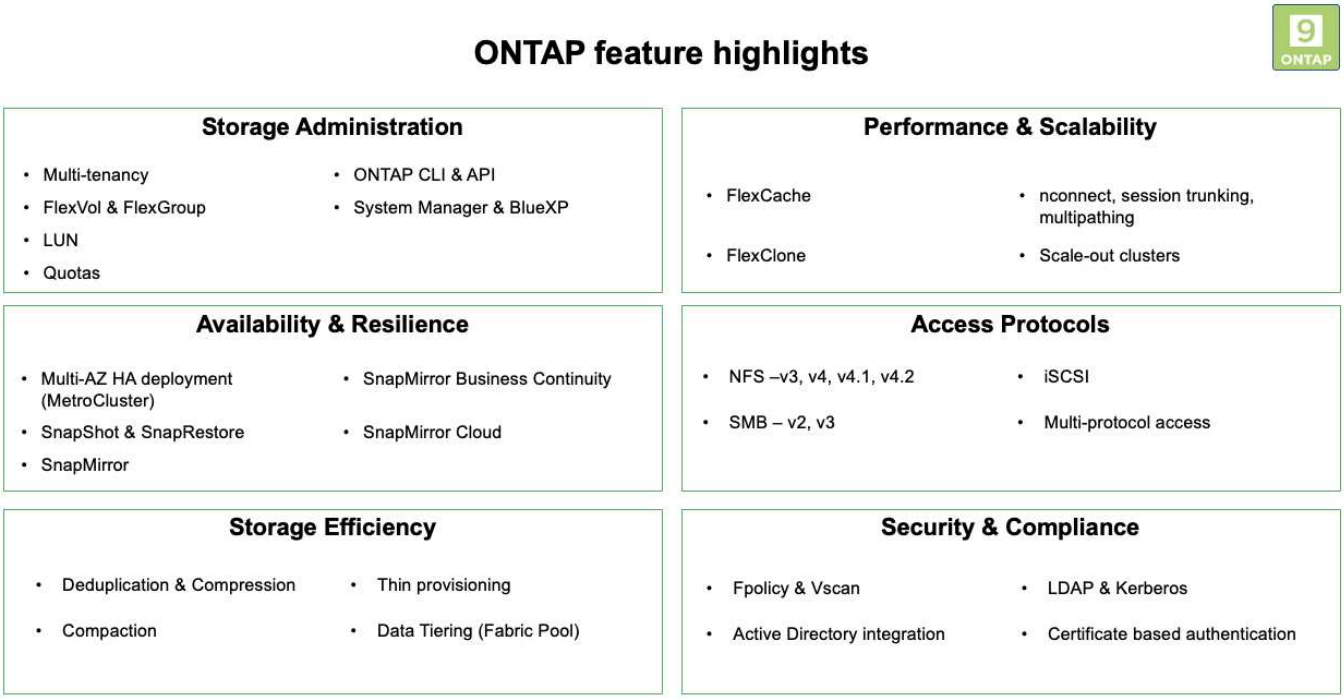
NetApp 發現客戶使用 Kubernetes 建置的容器和協調作業平台、將舊有企業應用程式現代化、並建置新的應用程式。Red Hat OpenShift Container Platform 是我們許多客戶採用的範例之一。

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

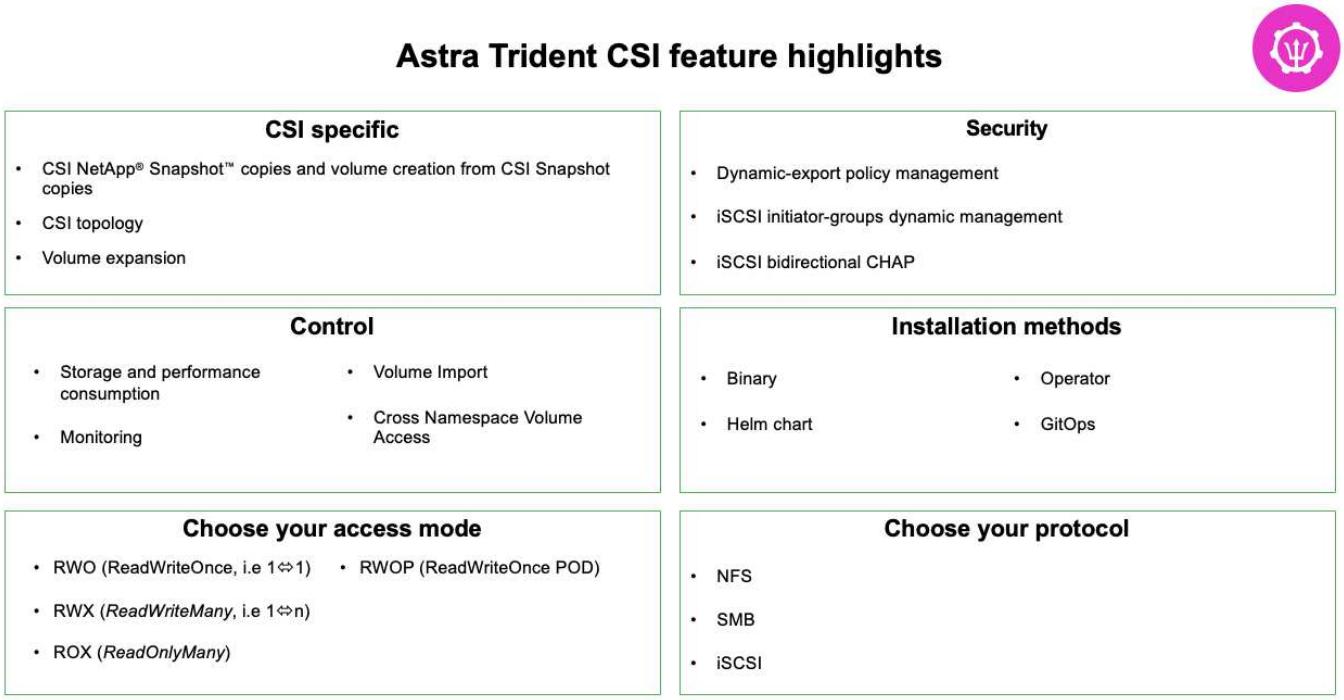
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（STaaS）
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （CVO）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：
  - Cloud Volumes Service for Google Cloud （CVS）、Azure NetApp Files （anf）、Amazon FSX for NetApp ONTAP 可在超大型擴充器中提供完全託管的儲存設備



- 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

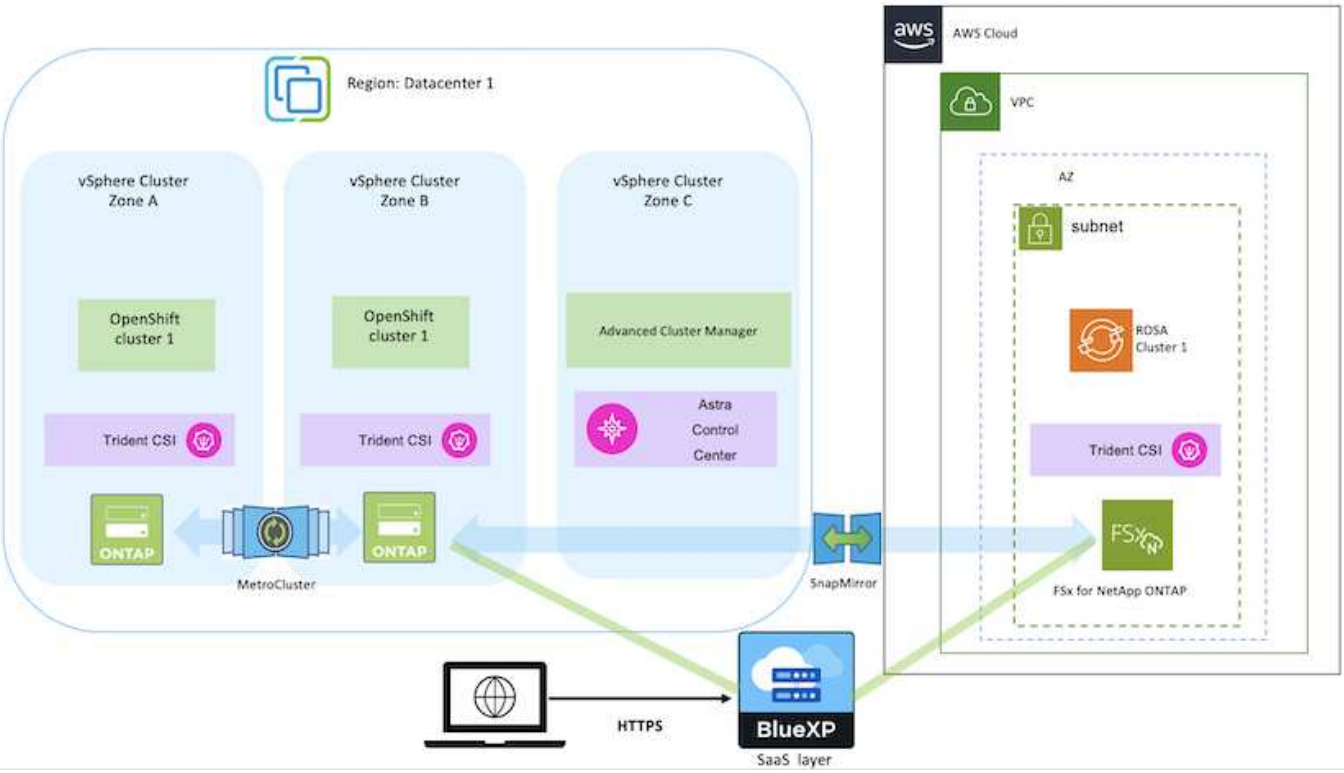
客戶可能是「天生於雲端」、或是準備好將某些特定工作負載或所有工作負載從資料中心移至雲端時、處於現代化過程的某個階段。他們可以選擇在雲端使用由供應商管理的 OpenShift 容器和由供應商管理的 NetApp 儲存設備來執行工作負載。他們應該規劃並部署雲端中的託管 Red Hat OpenShift Container 叢集（ROSA）、以便為其容器工作負載打造成功的正式作業環境。當他們位於 AWS 雲端時、也可以針對 NetApp ONTAP 部署 FSX 以滿足儲存需求。

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"。

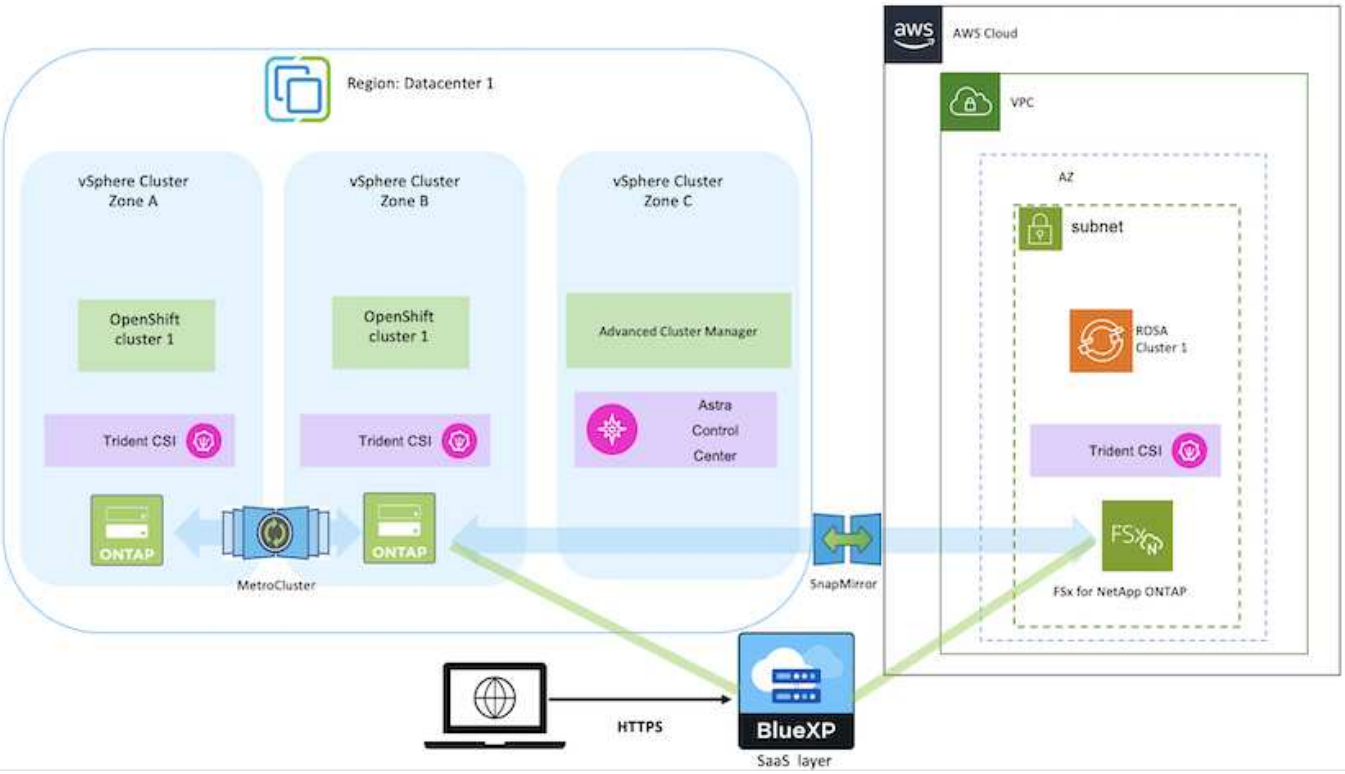
適用於 **OpenShift Container** 工作負載的資料保護與移轉解決方案



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

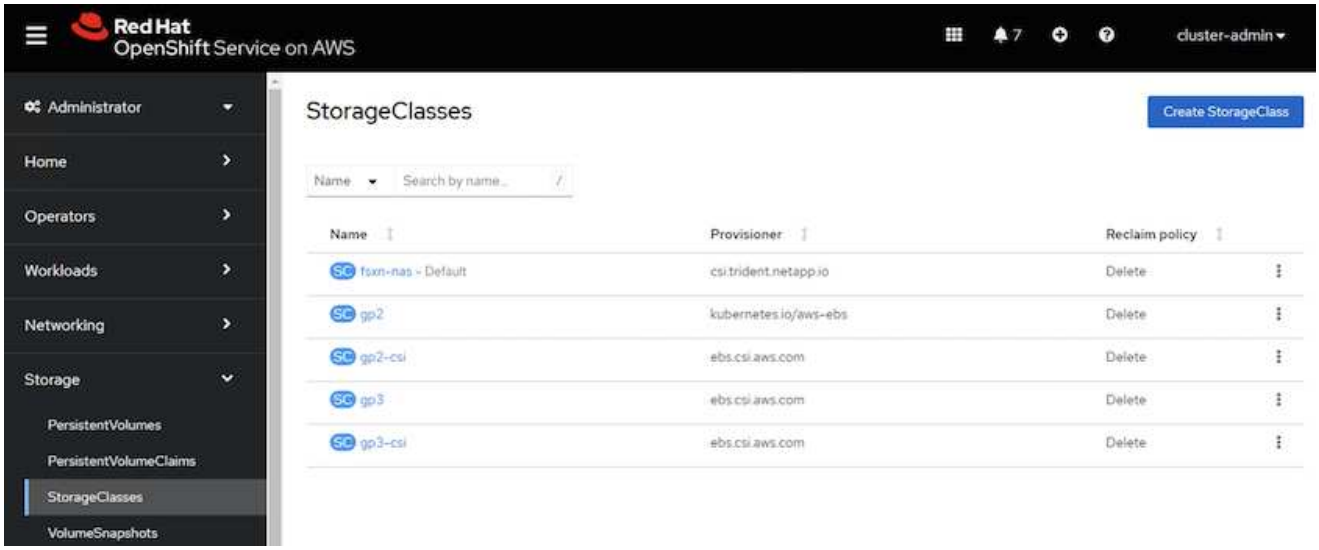
將 FSxN 與 Astra Trident 整合至 ROSA 叢集

> 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
```

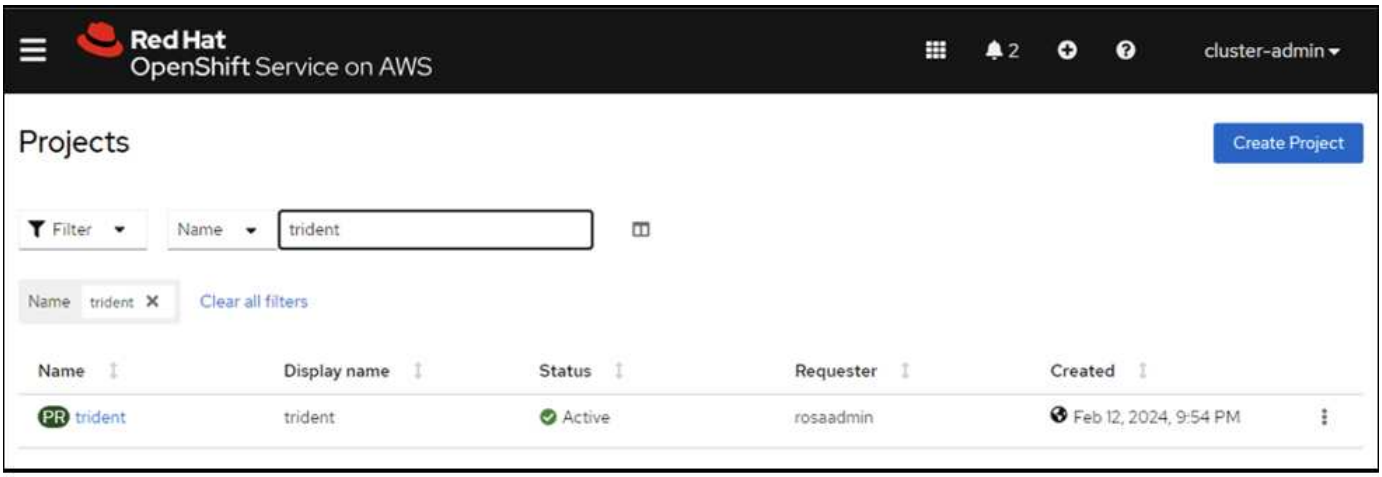
> 您也可以使用權杖登入叢集。如果您在建立叢集時已建立管理員使用者、則可以使用管理員使用者認證、從 Red Hat OpenShift 混合雲主控台登入叢集。然後按一下右上角顯示登入使用者名稱的、即可取得 `oc login` 命令列的命令（權杖登入）。

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

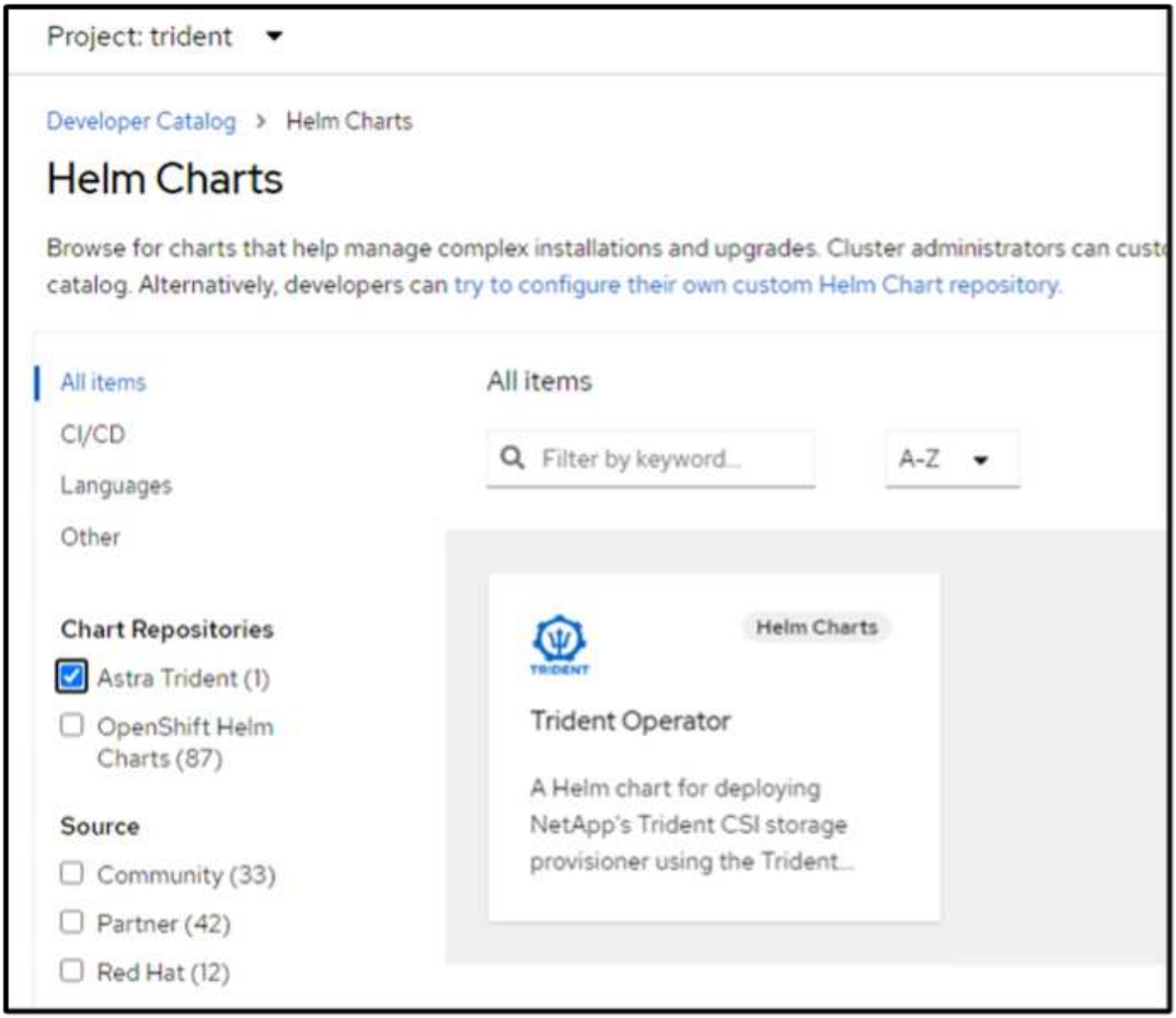
NetApp Astra Trident

A description for the Helm Chart repository.

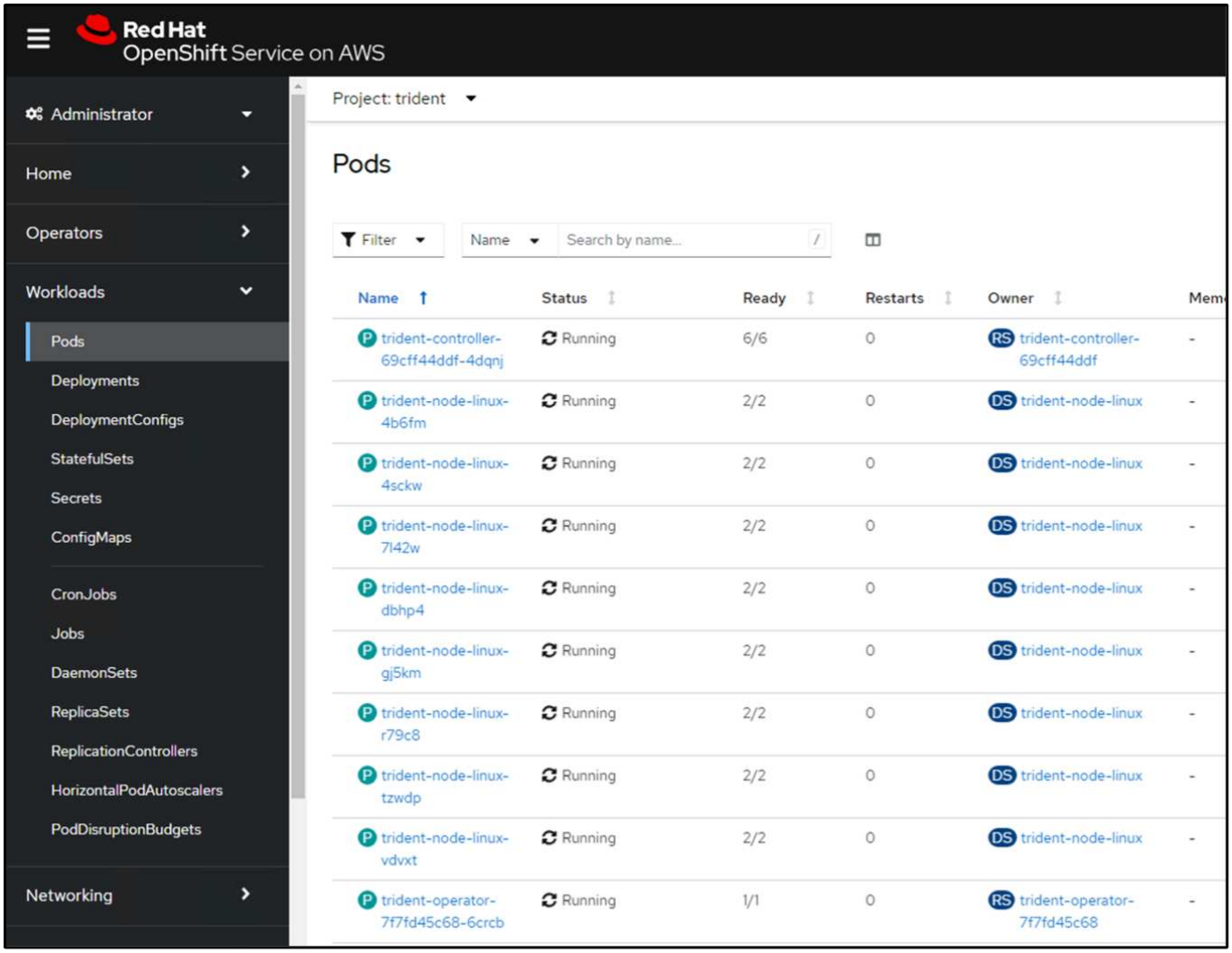
[ ] Disable usage of the repo in the developer catalog.

URL *

https://netapp.github.io/trident-helm-chart



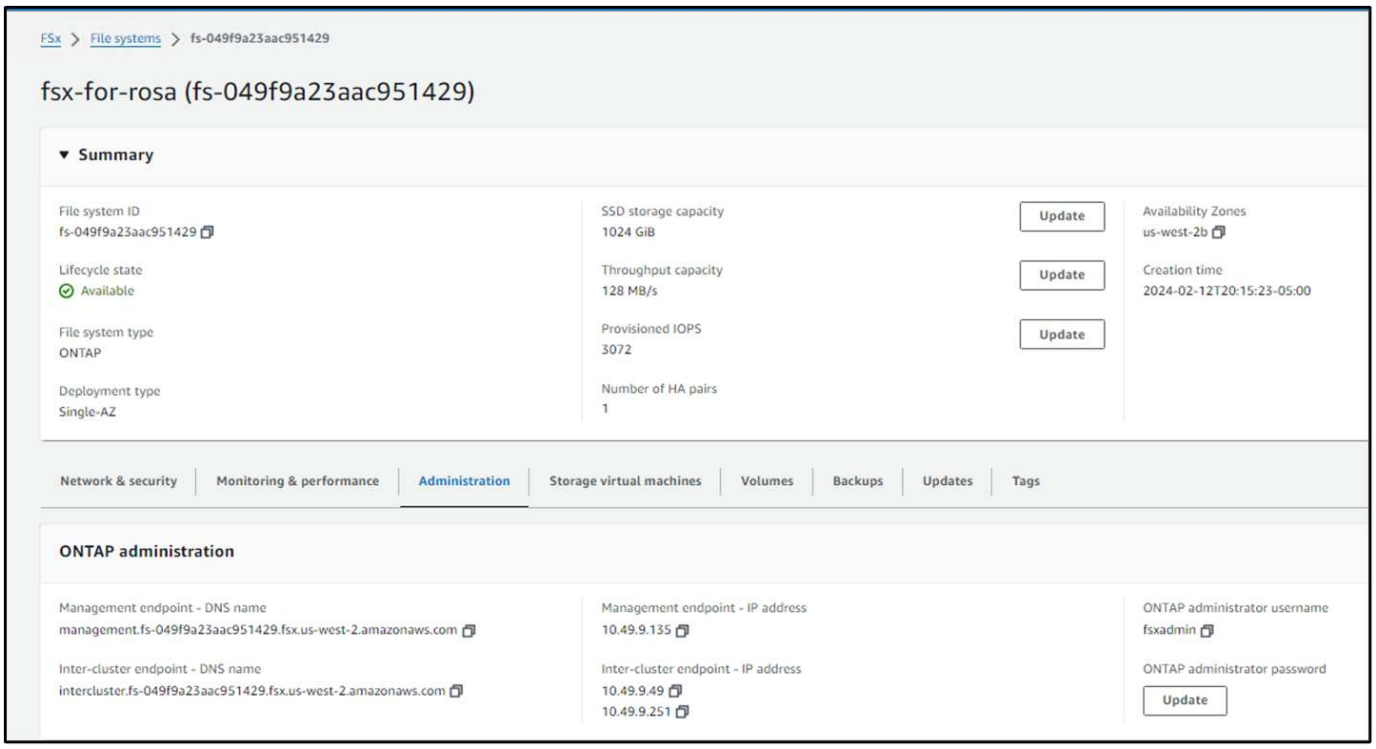
返回主控台的「管理員」檢視、然後在 Trident 專案中選取「群組」、以確認所有 Trident 群組都在執行中。



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 **

```yaml
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
```

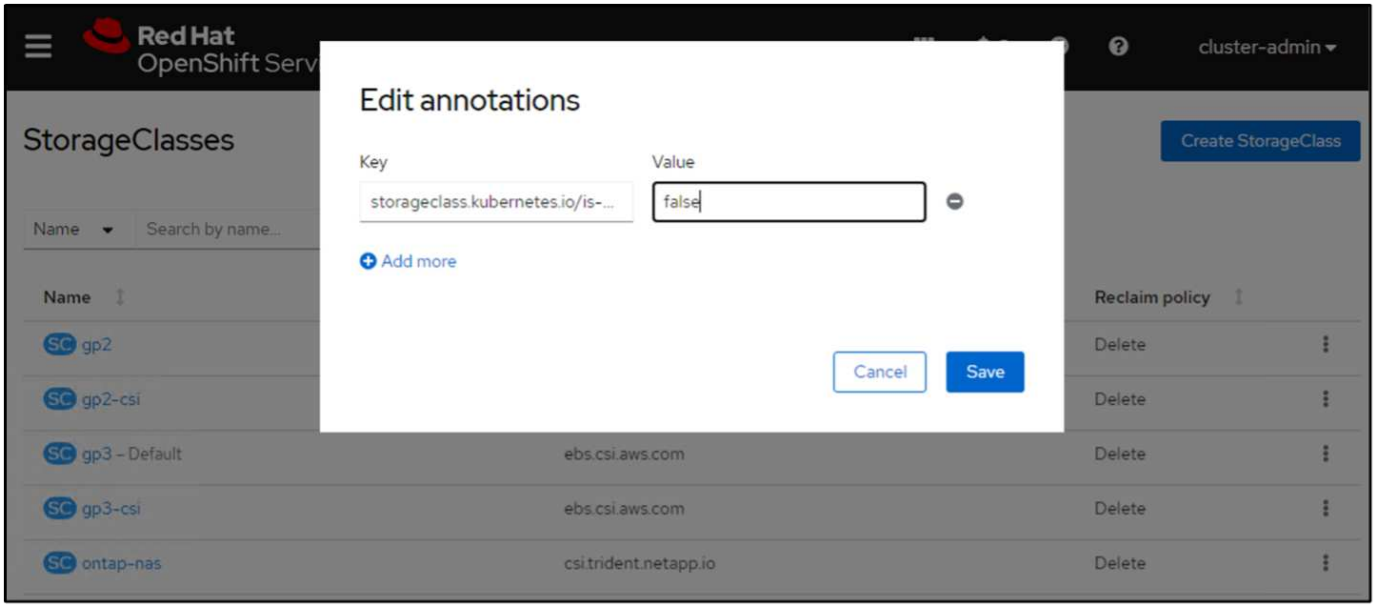
- 快照類別 **

```yaml
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]$
```

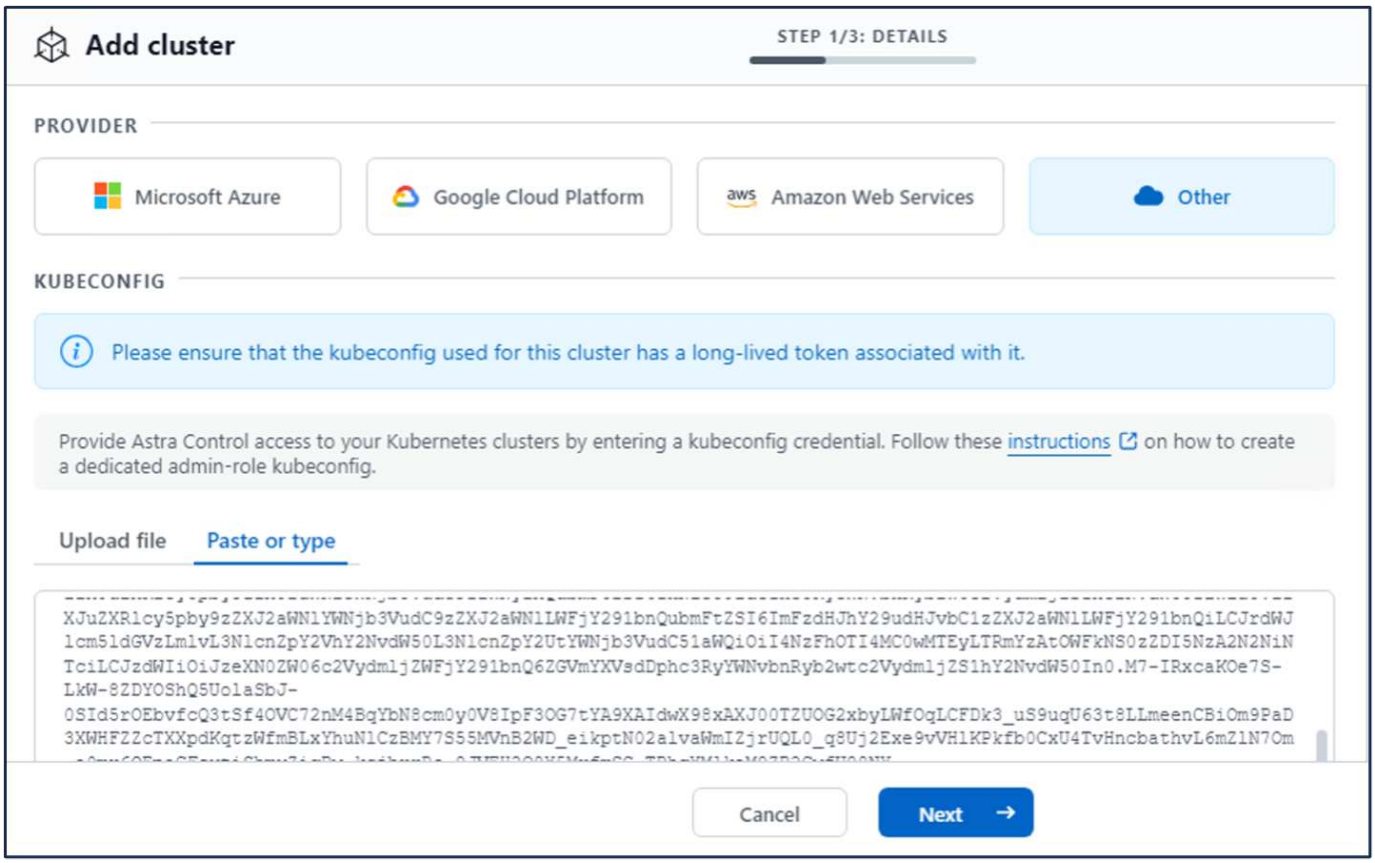
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6.建立資料庫並新增記錄

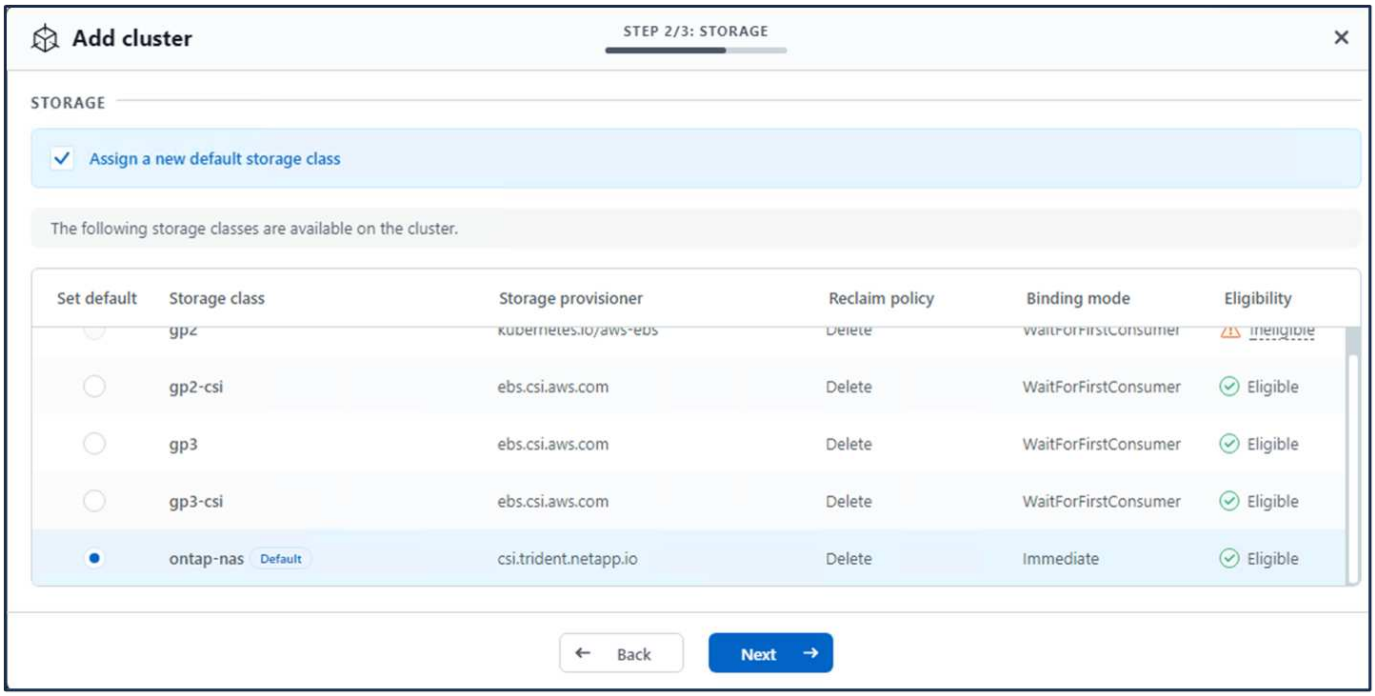
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --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。

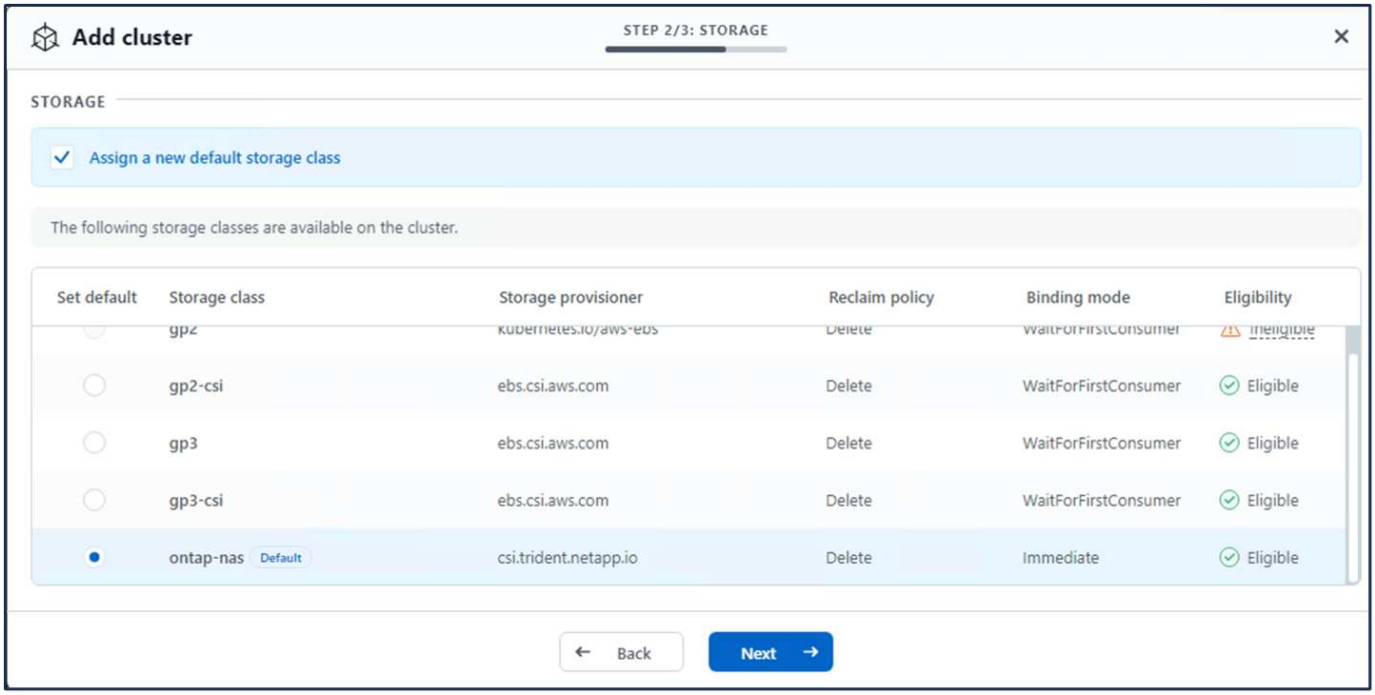


按一下 * 下一步 * 、然後選取 ONTAP NAS 作為 ACS 的預設儲存類別。按一下 * 下一步 * 、檢閱詳細資料和 * 新增 * 叢集。



8.在 **ACS** 中定義應用程式

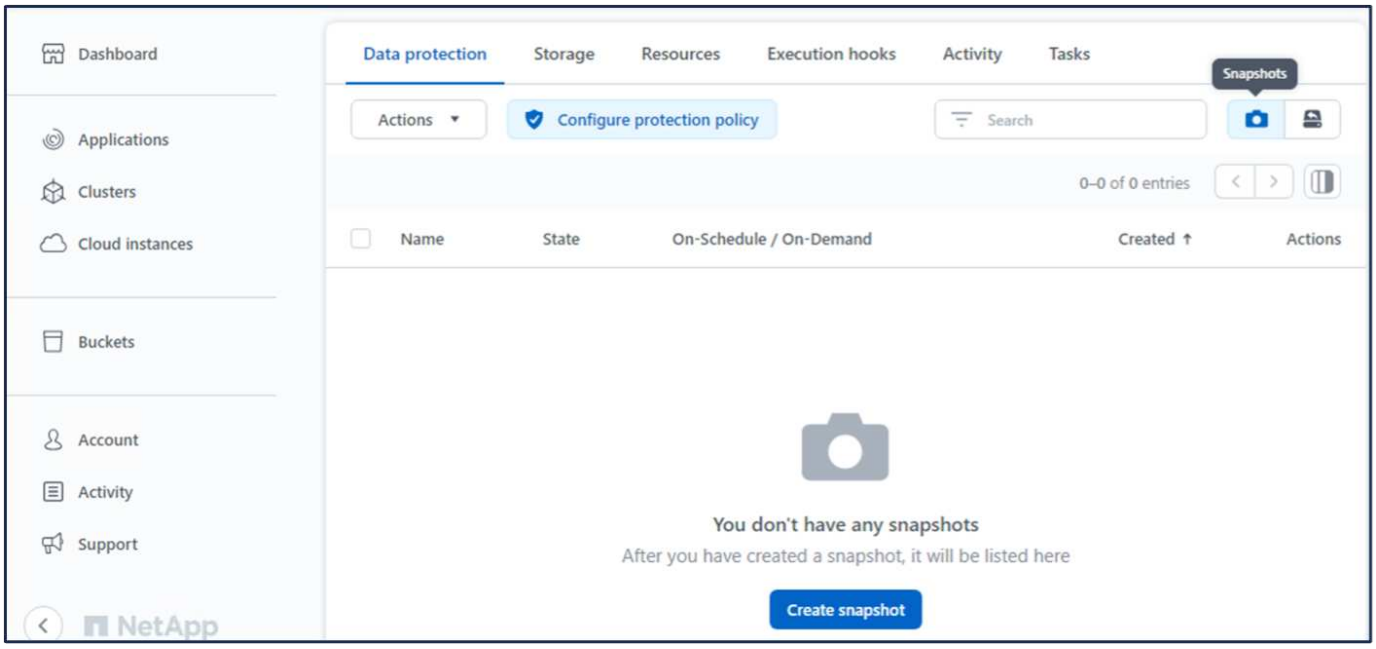
在 ACS 中定義 PostgreSQL 應用程式。從登陸頁面、選取 * 應用程式 * 、 * 定義 * 、然後填寫適當的詳細資料。按幾次 * 下一步 * 、檢閱詳細資料、然後按一下 * 定義 * 。應用程式隨即新增至 ACS 。

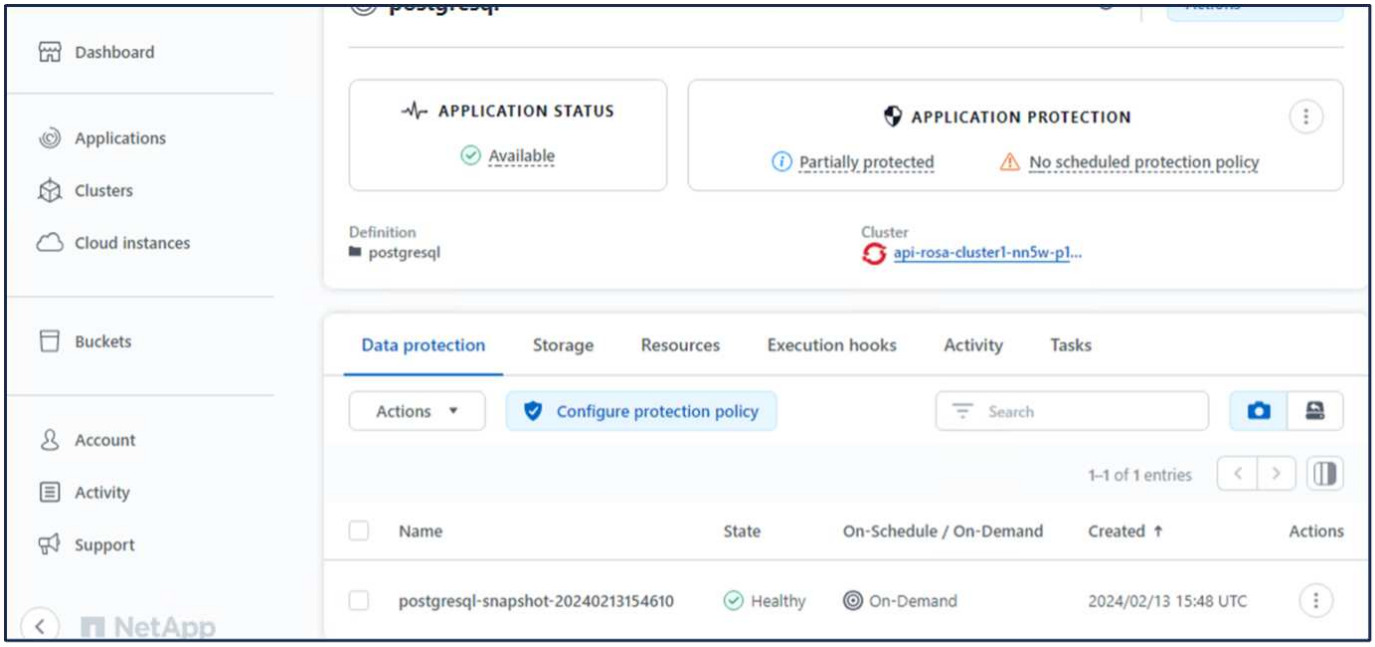


9.使用 **ACS** 建立快照

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

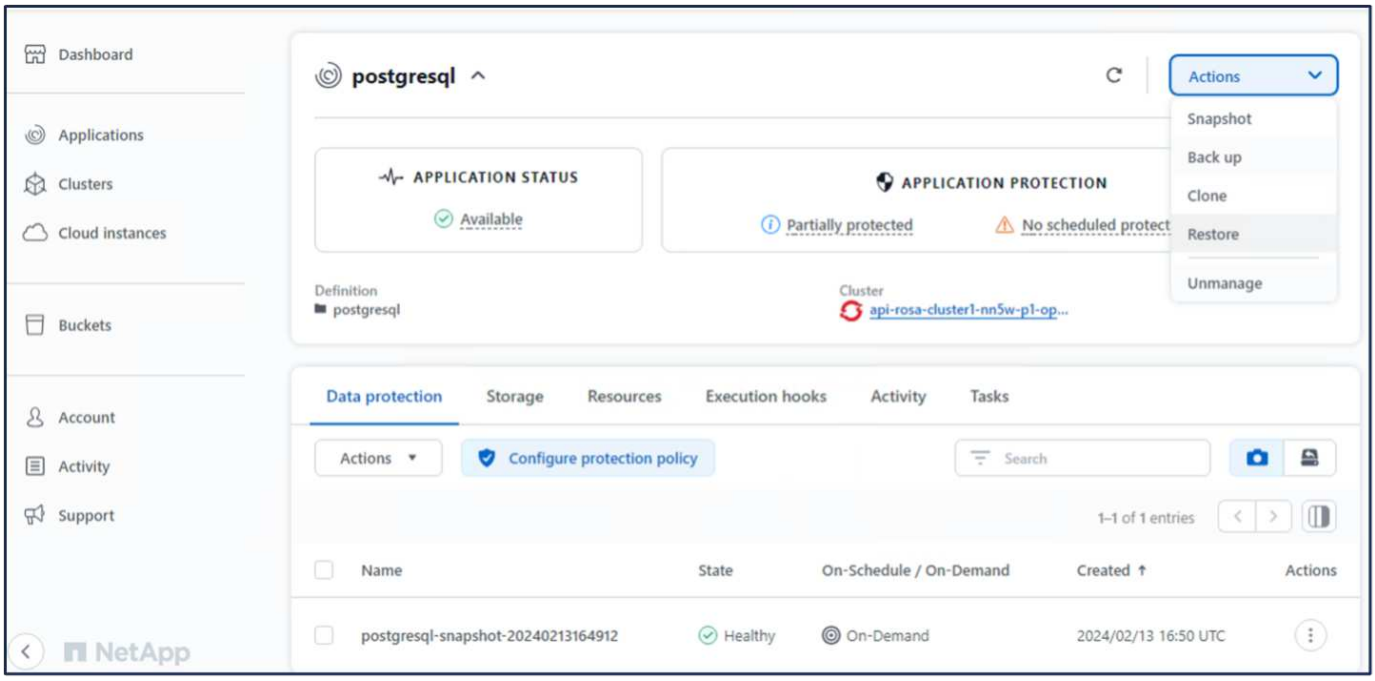
重新登入 PostgreSQL 、列出可用的資料庫、刪除您先前建立的資料庫、然後再次列出、以確保資料庫已刪除。

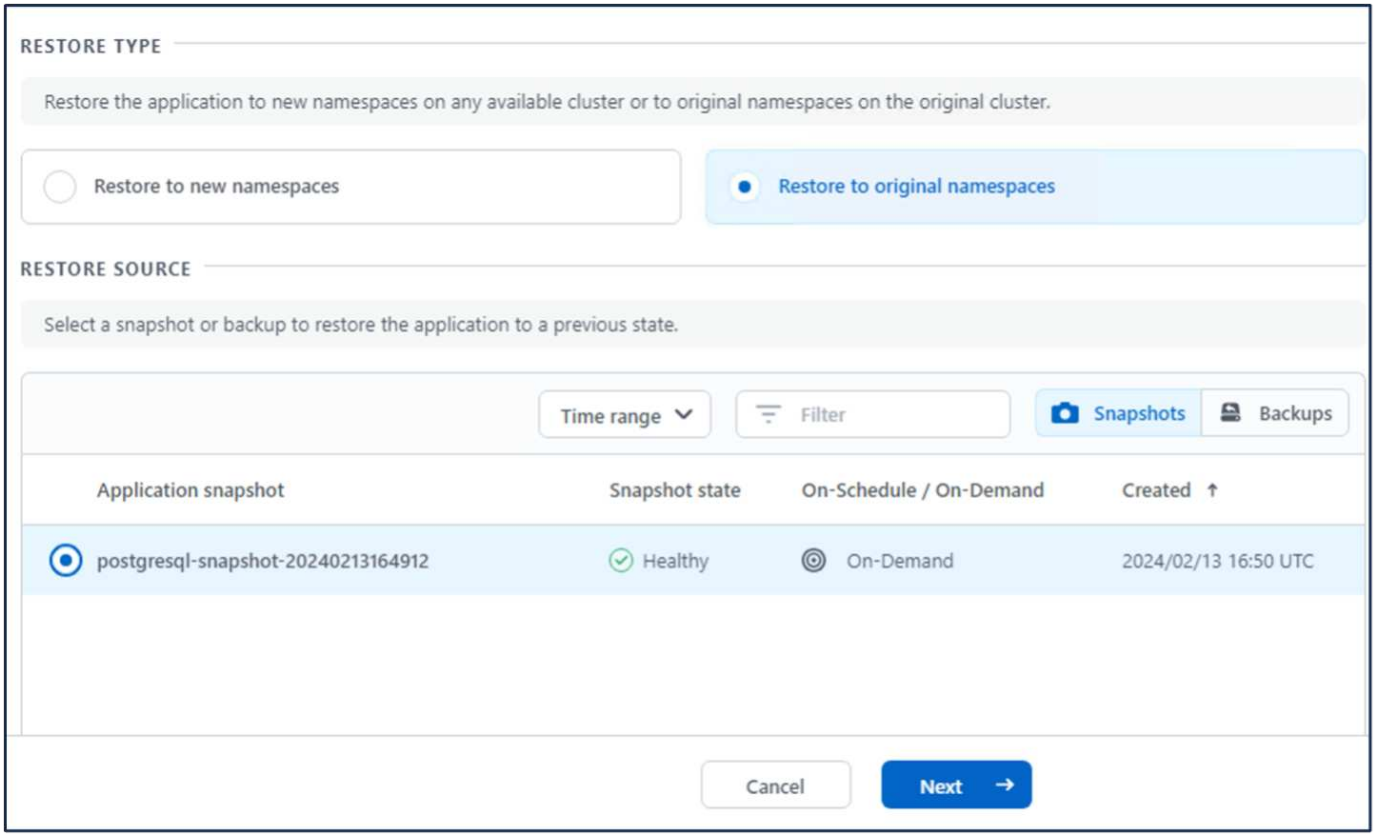
```
postgres=# \l
                                                    List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+---------------
 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)
```

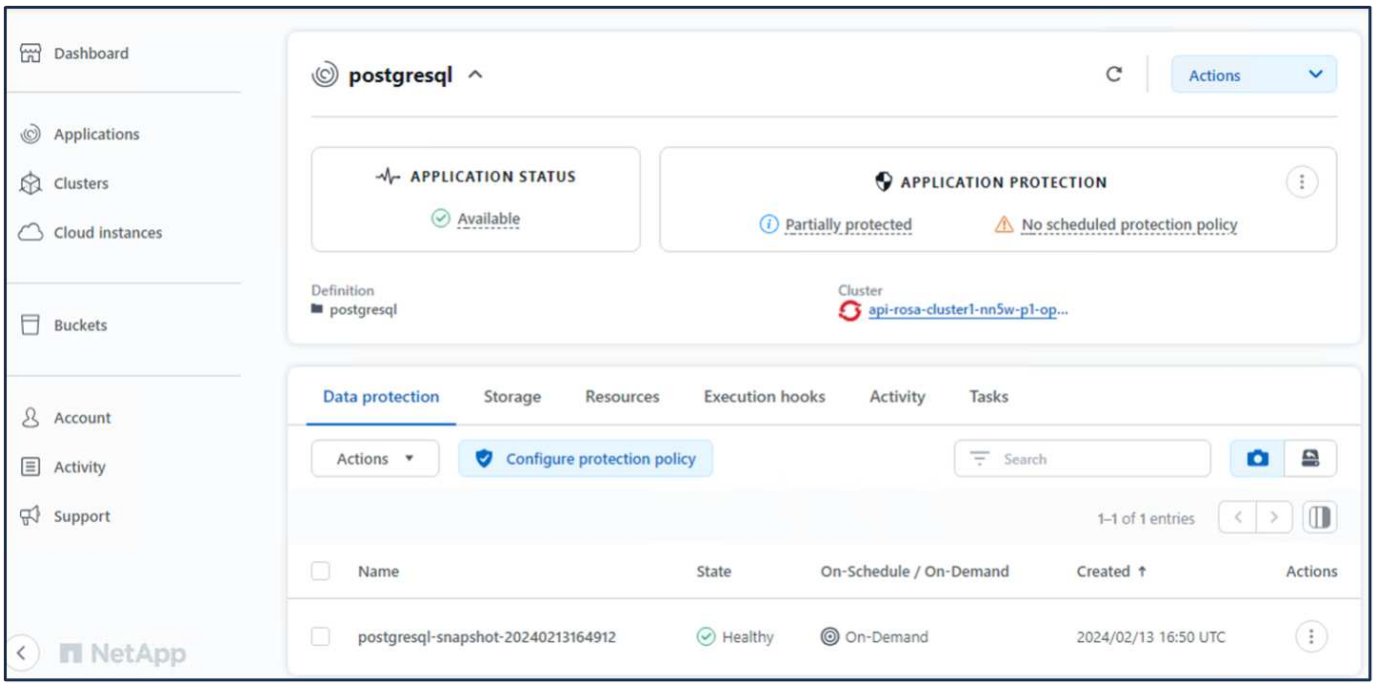
11.使用 **ACS** 從快照還原

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。

資料移轉

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