含自我管理元件的混合雲（內部部署/AWS/GCP/Azure）

NetApp Solutions

NetApp
April 12, 2024

目錄

適用於 Red Hat OpenShift Container 工作負載的 NetApp 混合式多雲端解決方案

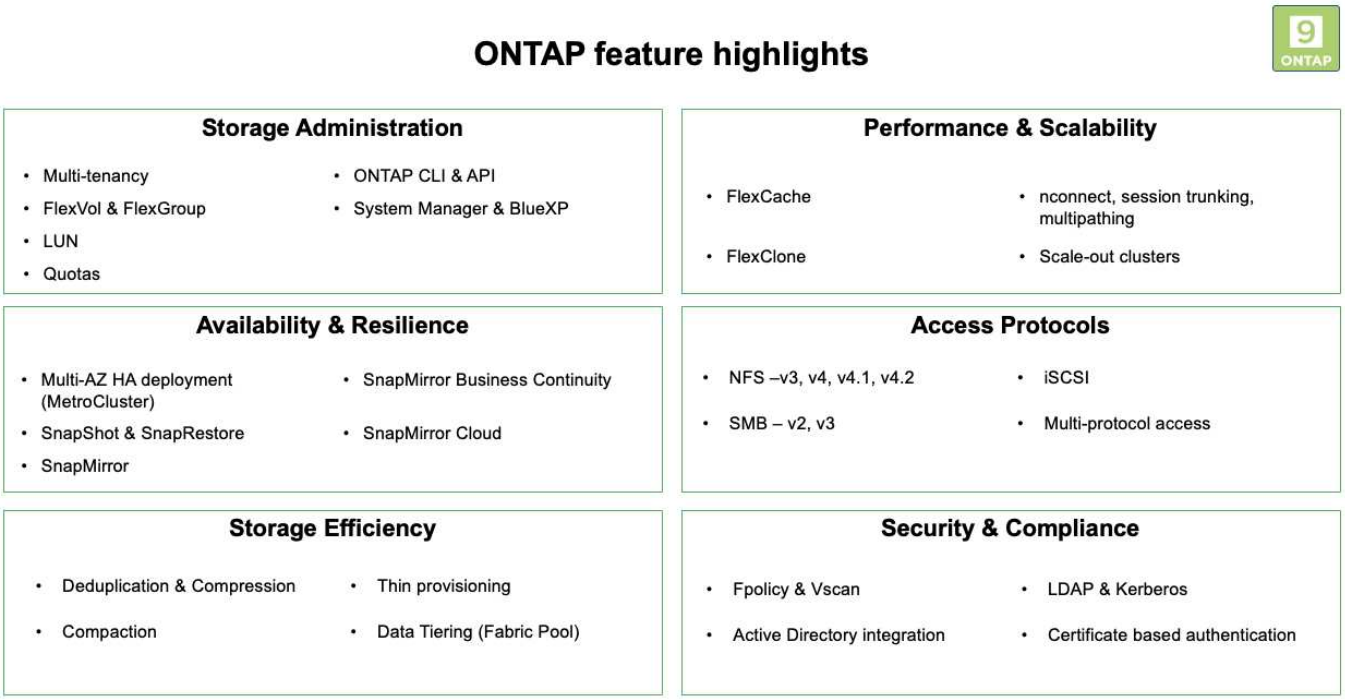
總覽

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。

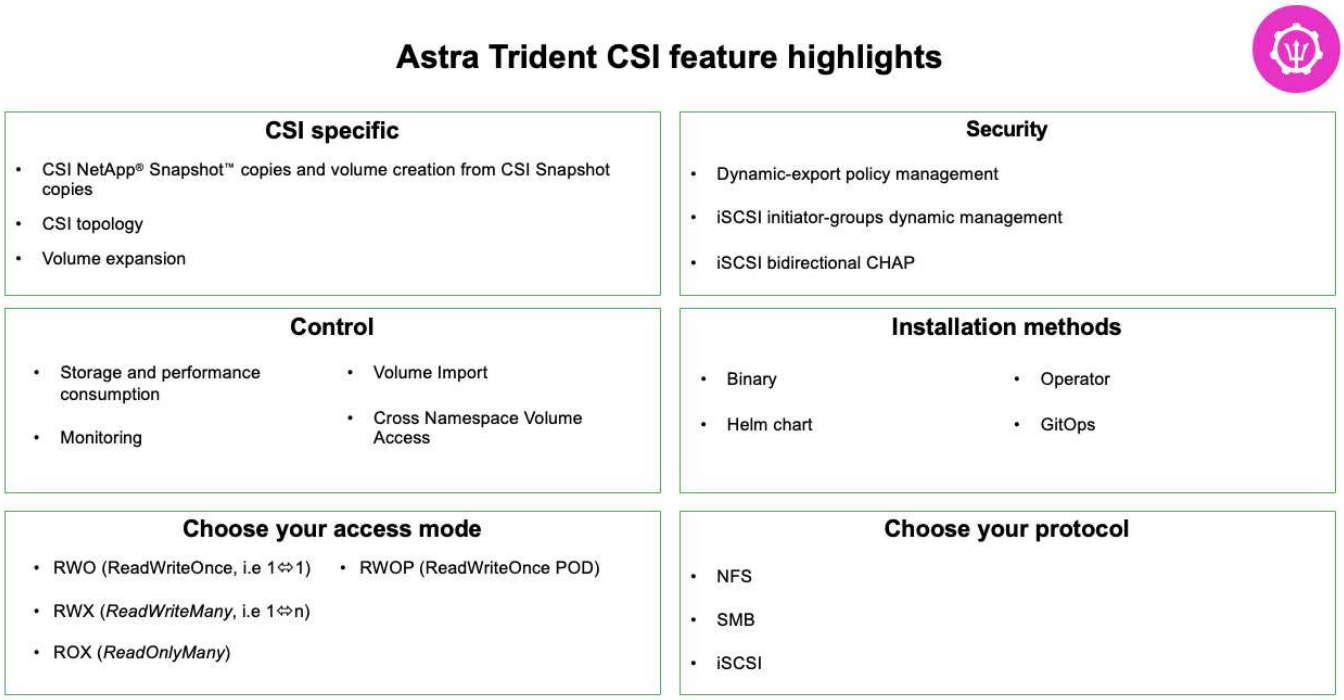
- 內部部署的自我管理儲存設備：
  - NetApp Fabric 附加儲存設備（FAS）、 NetApp All Flash FAS Array （AFF）、 NetApp All SAN Array （ASA）和 ONTAP Select
- 內部部署的供應商託管儲存設備：
  - NetApp Keystone 提供儲存即服務（STaaS）
- 雲端中的自我管理儲存設備：
  - NetApp Cloud Volumes ONTAP （CVO）可在超大型磁碟機中提供自我管理的儲存設備
- 雲端中由供應商管理的儲存設備：
  - Cloud Volumes Service for Google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

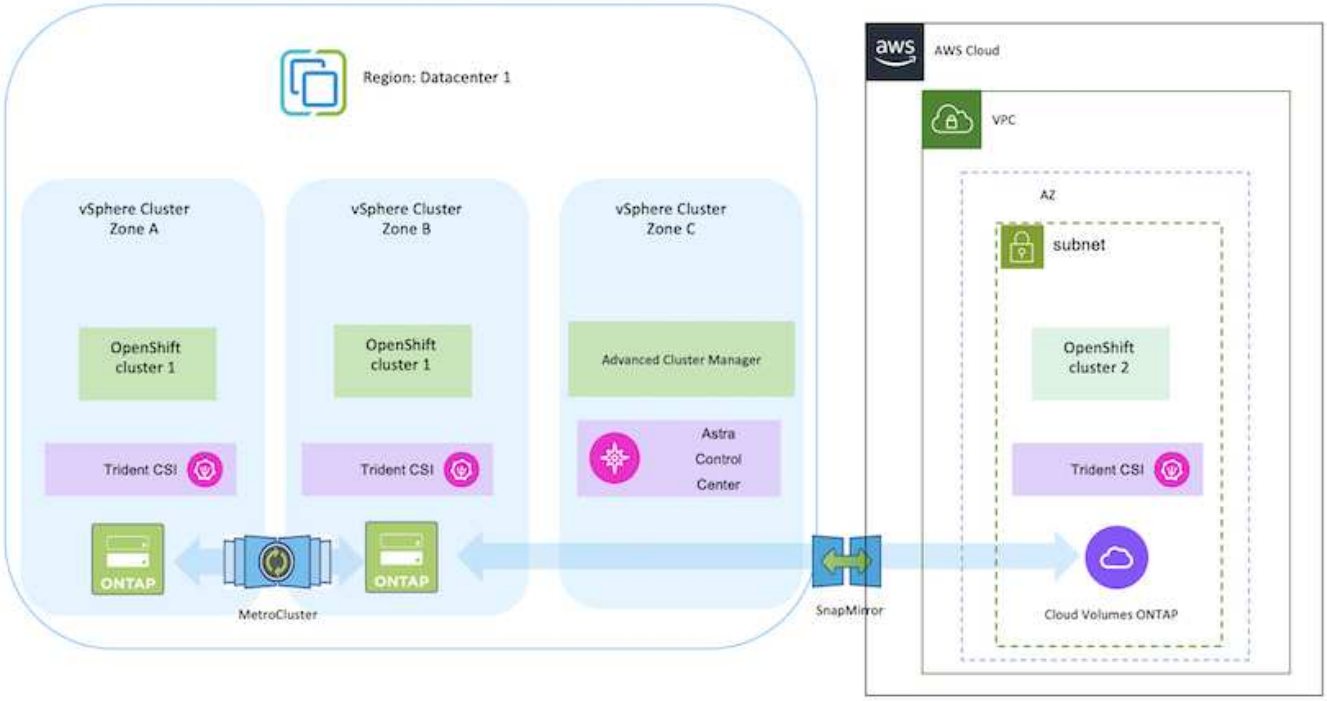
採用混合雲的 **Red Hat OpenShift Container** 平台工作負載的 **NetApp** 解決方案

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。

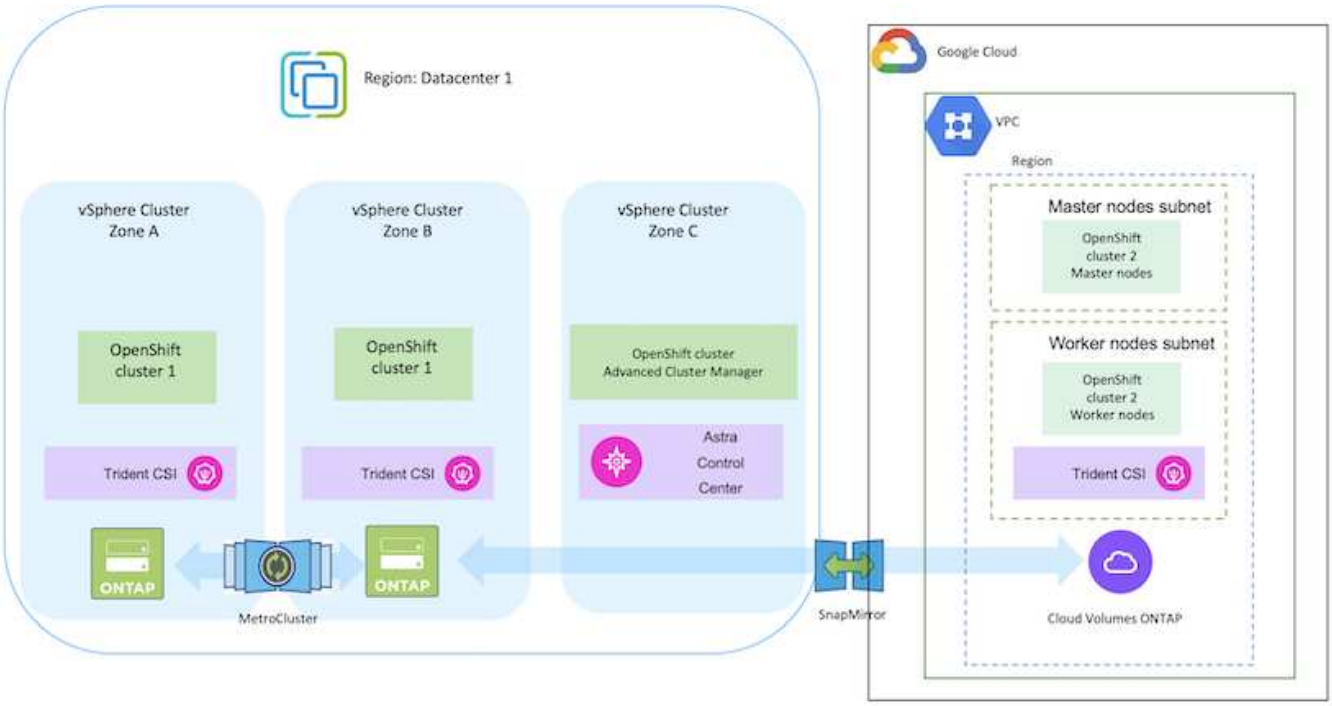
NetApp Cloud Volumes ONTAP 儲存設備可為 AWS 、 Azure 和 Google Cloud 中的容器部署提供資料保護、可靠性和靈活度。Astra Trident 是動態儲存資源配置程式、可為客戶的有狀態應用程式使用持續的 Cloud Volumes ONTAP 儲存設備。Astra Control Center 可用來協調有狀態應用程式的許多資料管理需求、例如資料保護、移轉和業務持續運作。

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

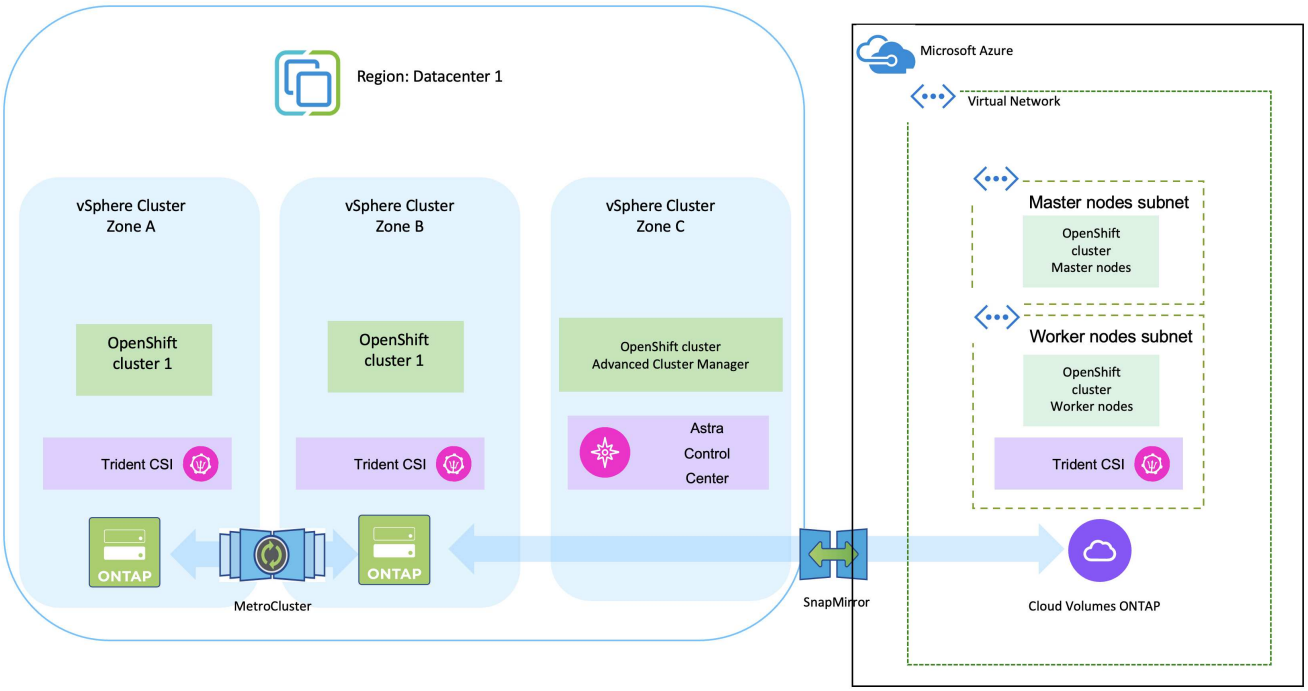


內部部署和 Google Cloud



內部部署與 Azure Cloud

[redacted]



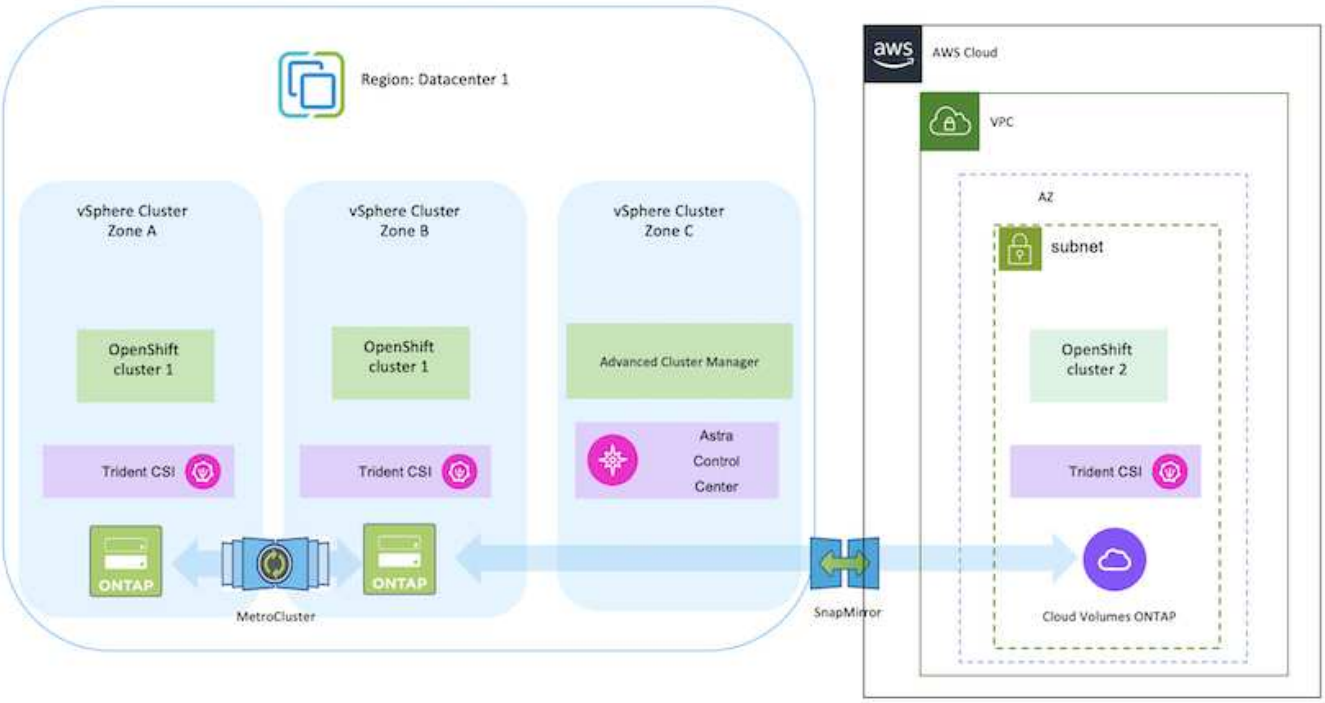
[redacted]

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。

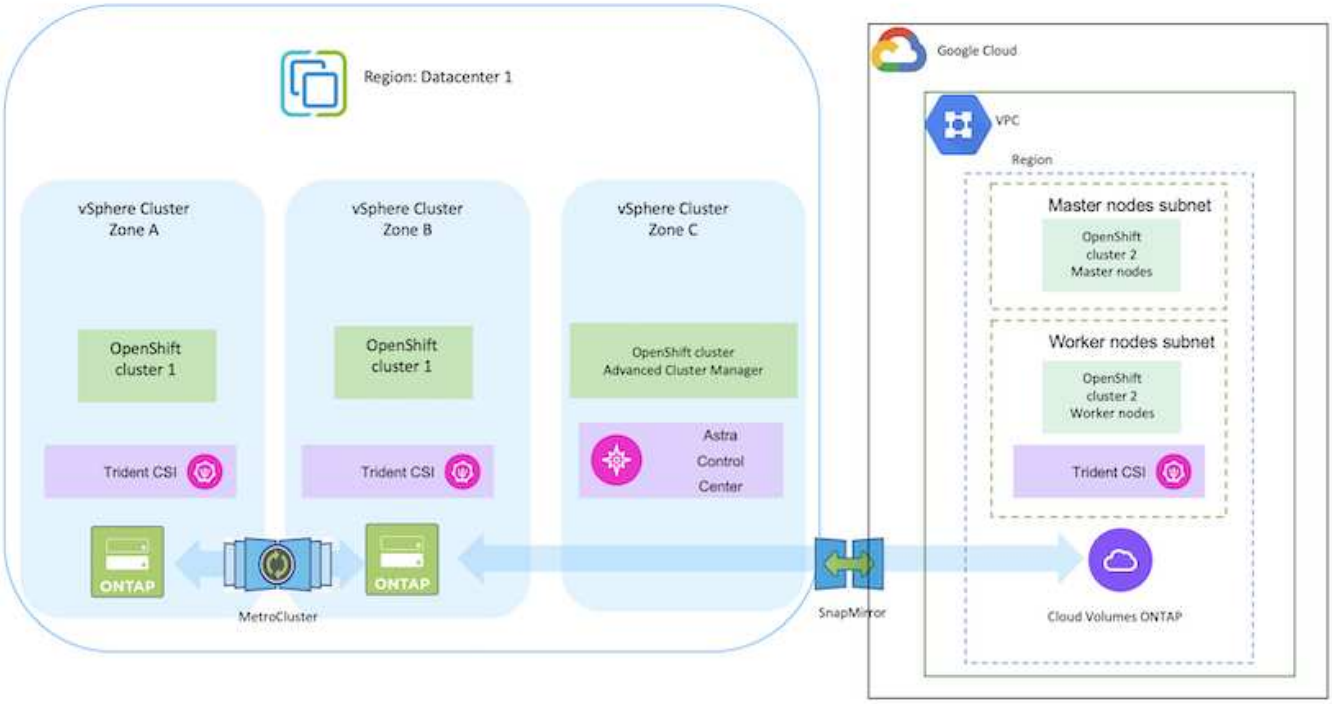
Kubernetes 支援兩種磁碟區繫結模式： - 當 ***Volume BindingMode*** 設為 ***Immediate*** （預設）時、 Astra Trident 會在沒有任何拓撲感知的情況下建立磁碟區。建立永續性磁碟區時、不會對要求的Pod排程需求有任何相依性。- 當 ***Volume BindingMode*** 設定為 **_WaitForFirstConsumer**（客戶） 時、永久 Volume 的建立與繫結將延遲、直到排程並建立使用 PVC 的 Pod 為止。如此一來、就能建立磁碟區、以符合拓撲需求所強制執行的排程限制。Astra Trident 儲存後端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

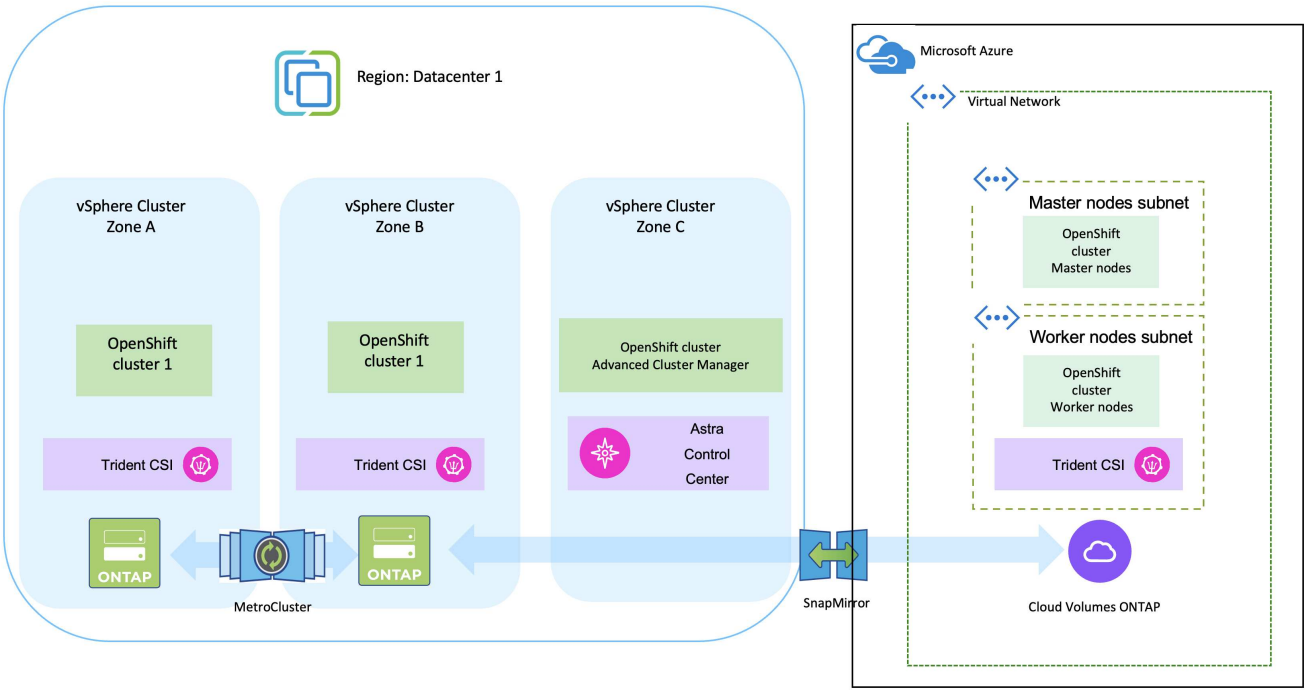
將 OpenShift 叢集匯入 Astra Control Center

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。

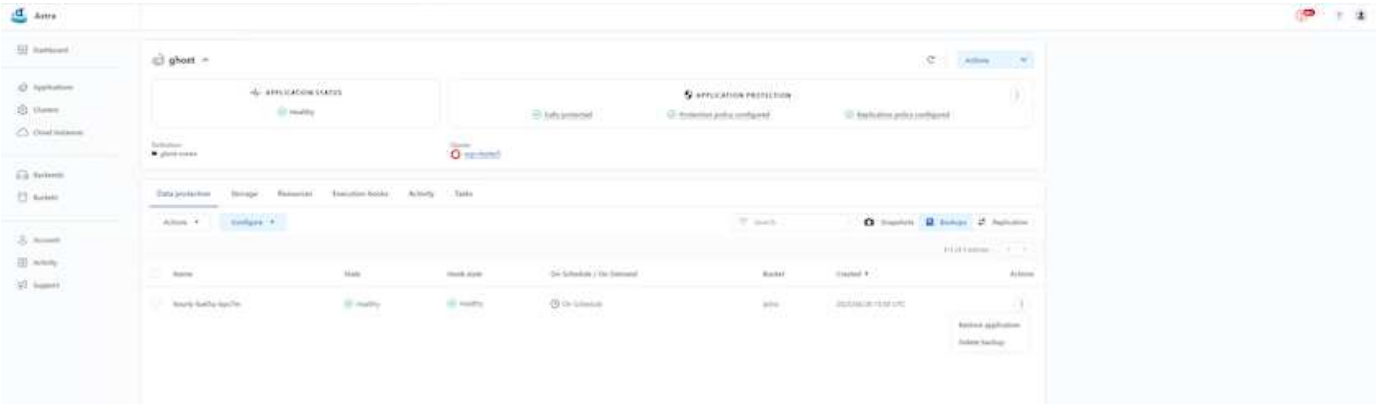
資料保護的需求各不相同、從還原到時間點複本、到自動容錯移轉到不同的故障網域、而無需人為介入。許多客戶選擇 ONTAP 做為其 Kubernetes 應用程式的首選儲存平台、因為其豐富的功能包括多租戶、多重傳輸協定、高效能與容量、多站台位置的複寫與快取、安全性與靈活度。

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

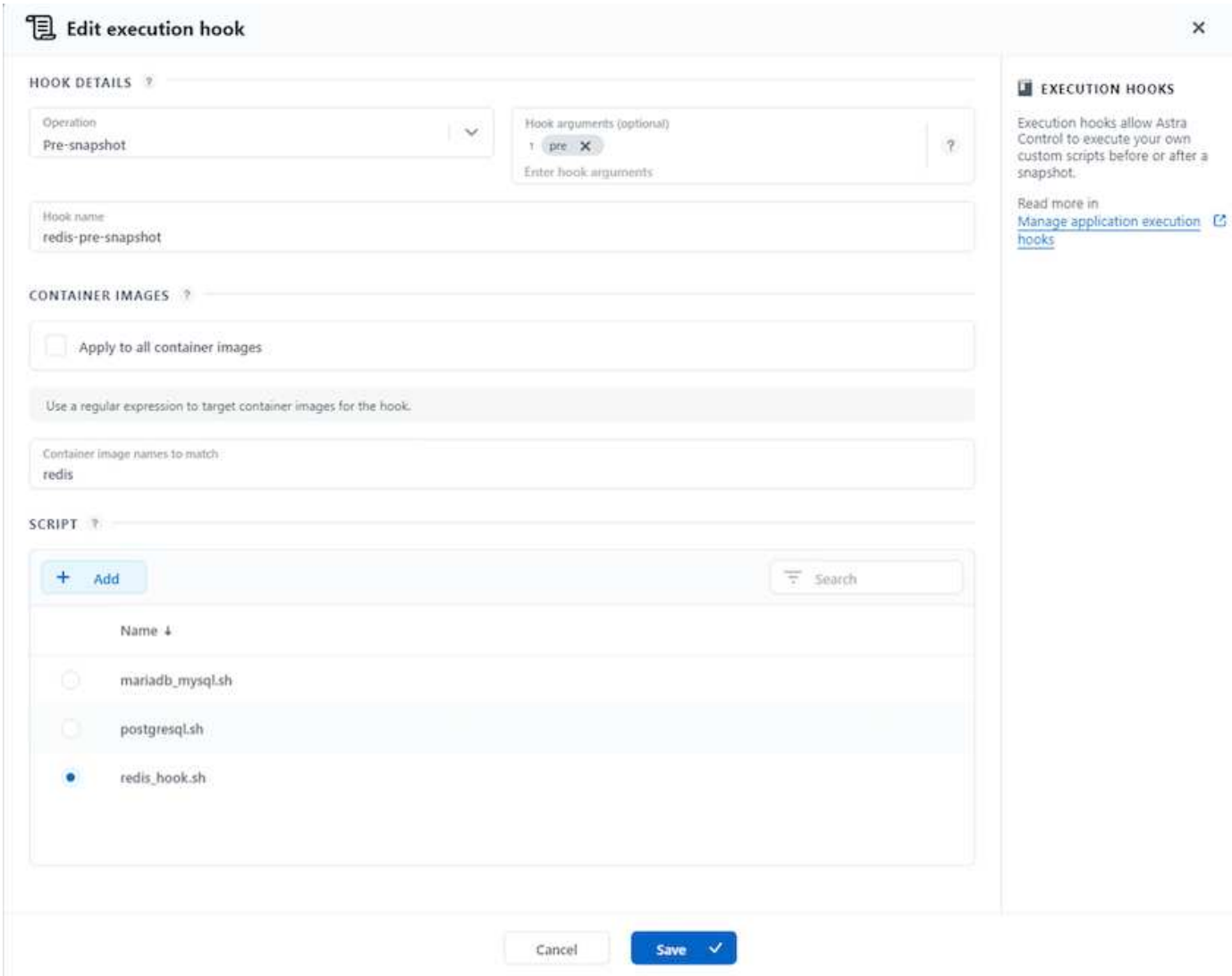


應用程式特定的執行攔截器

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。

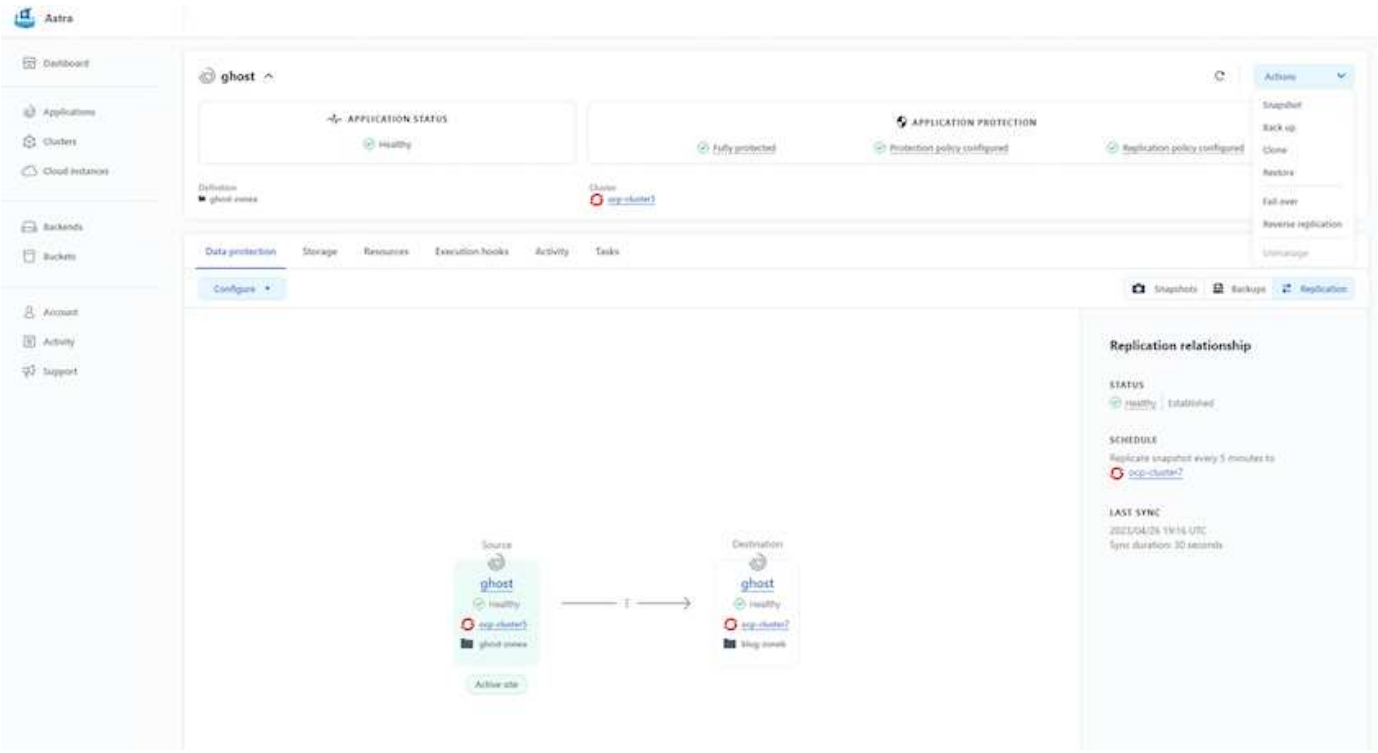
Redis 應用程式快照前的執行掛鉤範例。



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