具有自管理组件的混合云

NetApp public and hybrid cloud solutions

NetApp
February 26, 2026

目录

具有自管理组件的混合云

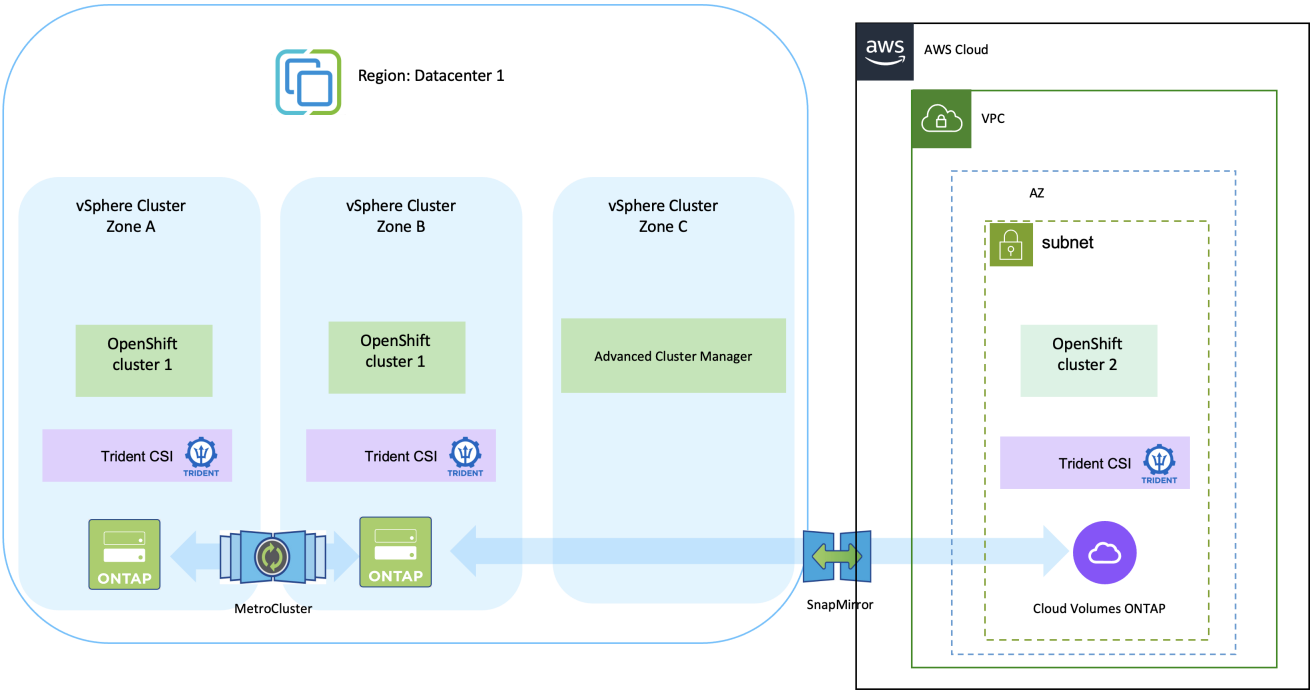
NetApp解决方案与混合云中的 Red Hat OpenShift 容器平台工作负载

当客户准备将部分选定的工作负载或所有工作负载从数据中心迁移到云端时，他们可能正处于现代化转型的某个阶段。他们可能出于各种原因选择在云中使用自管理的 OpenShift 容器和自管理的NetApp存储。他们应该在云中规划和部署 Red Hat OpenShift 容器平台 (OCP)，以便成功构建一个可用于生产的环境，以便从数据中心迁移容器工作负载。他们的 OCP 集群可以在其数据中心部署在 VMware 或 Bare Metal 上，也可以在云环境中部署在 AWS、Azure 或 Google Cloud 上。

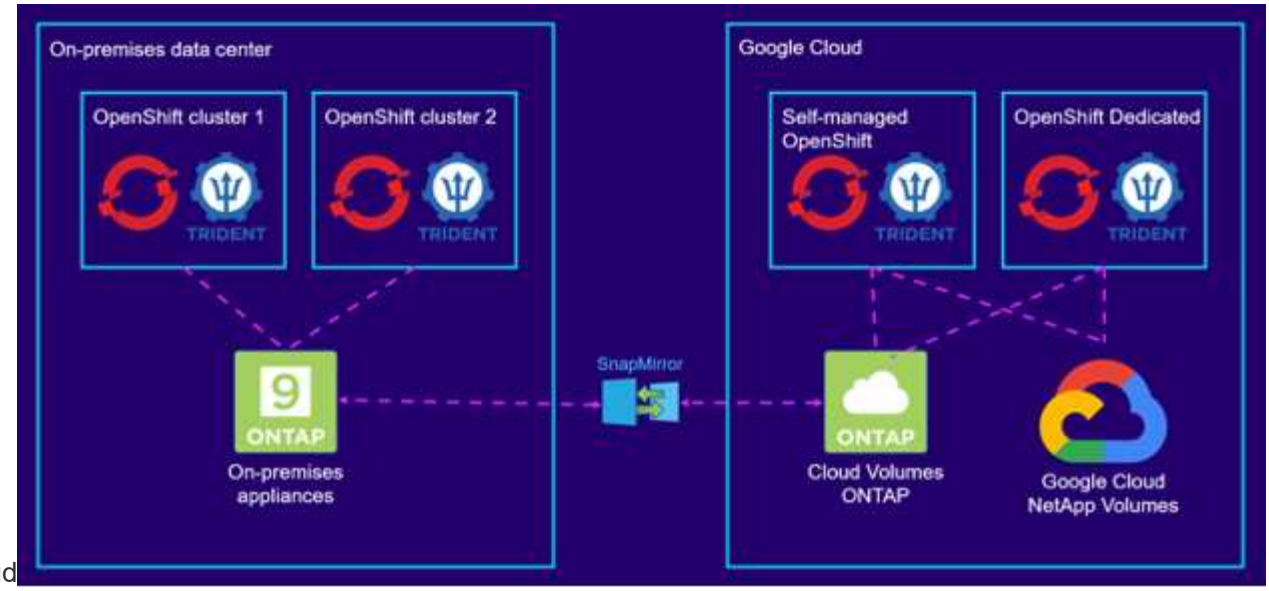
NetApp Cloud Volumes ONTAP存储为 AWS、Azure 和 Google Cloud 中的容器部署提供数据保护、可靠性和灵活性。 Trident作为动态存储供应器，为客户的有状态应用程序使用持久性Cloud Volumes ONTAP存储。 Trident Protect 可用于有状态应用程序的数据管理需求，例如数据保护、迁移和业务连续性。

使用Trident Protect 为混合云中的 OpenShift Container 工作负载提供数据保护和迁移解决方案

本地和
AWS

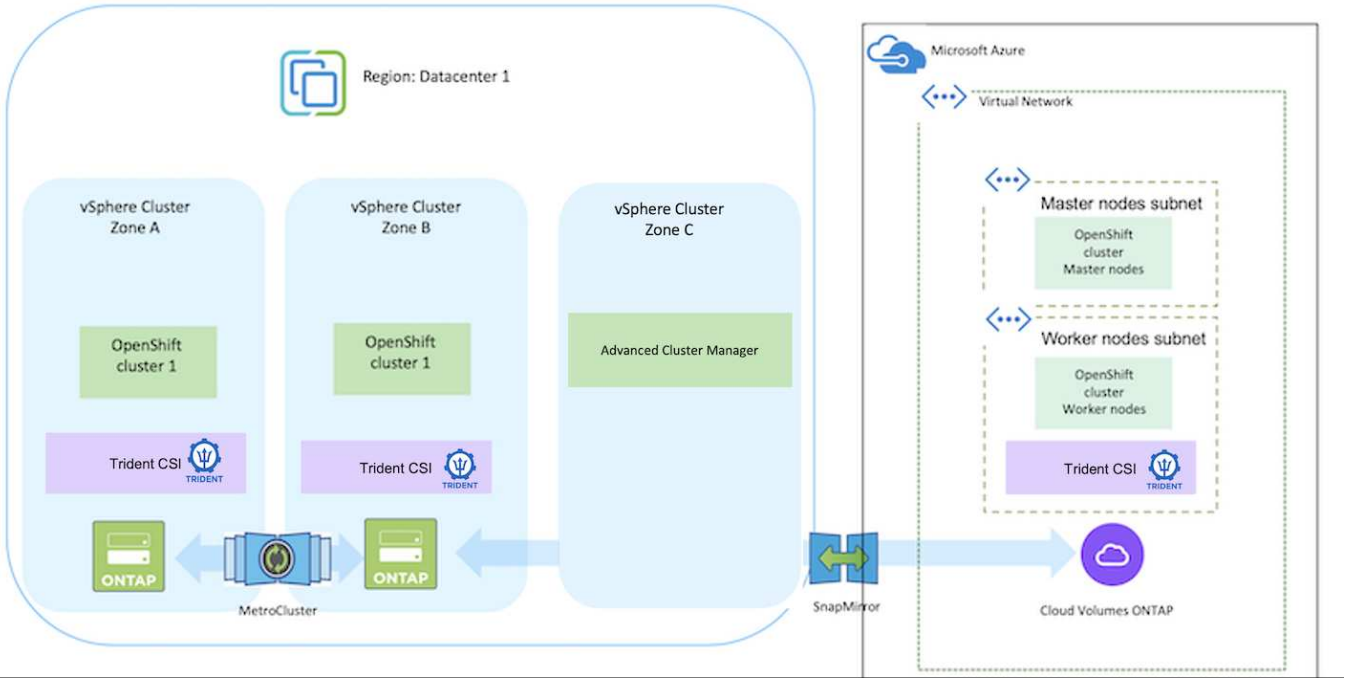


本地和 Google



Cloud

本地和 Azure
云

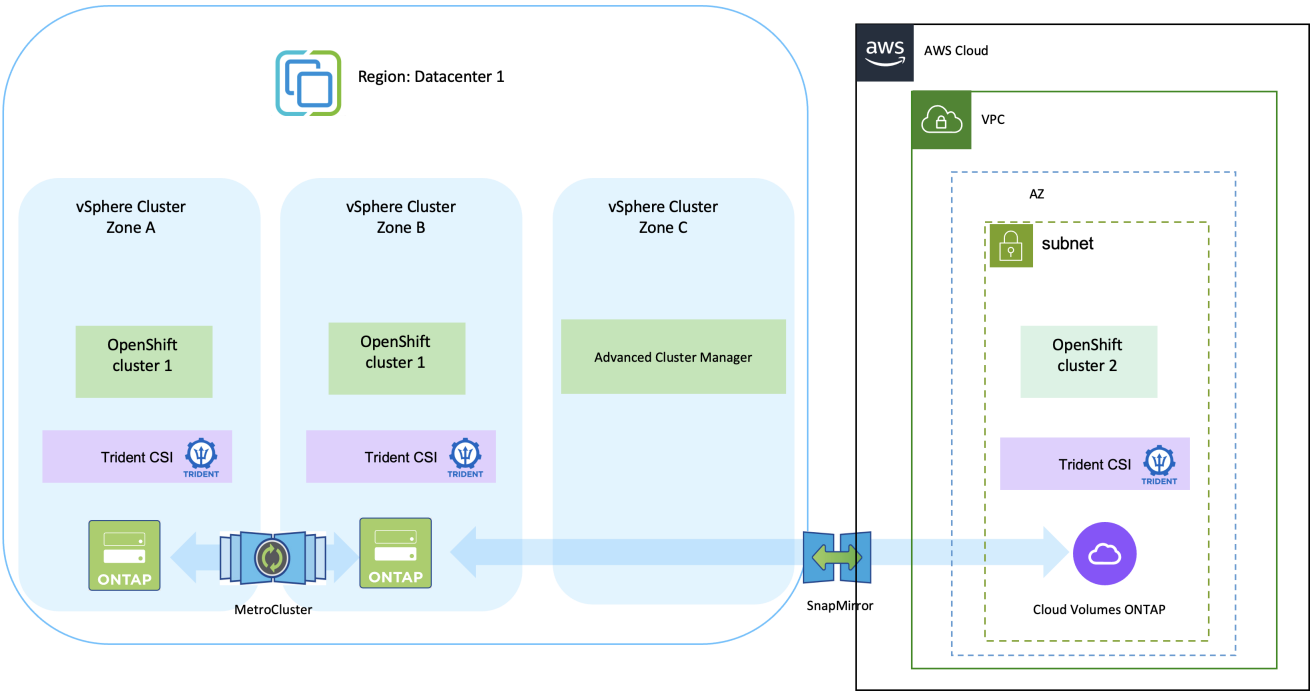


在 AWS 上部署和配置 Red Hat OpenShift Container 平台

本节介绍了如何在 AWS 中设置和管理 OpenShift 集群并在其上部署有状态应用程序的高级工作流程。它展示了如何使用NetApp Cloud Volumes ONTAP存储在Trident的帮助下提供持久卷。提供了有关使用Trident Protect 为有状态应用程序执行数据保护和迁移活动的详细信息。

有几种方法可以在 AWS 上部署 Red Hat OpenShift Container 平台集群。此设置的高级描述提供了所使用的特定方法的文档链接。您可以参考"资源部分"。

下图描述了部署在 AWS 上并使用 VPN 连接到数据中心的集群。



设置过程可分为以下步骤：

从高级集群管理在 **AWS** 上安装 **OCP** 集群。

- 创建具有站点到站点 VPN 连接（使用 pfSense）的 VPC 以连接到本地网络。
- 内部网络具有互联网连接。
- 在 3 个不同的 AZ 中创建 3 个私有子网。
- 为 VPC 创建 Route 53 私有托管区域和 DNS 解析器。

从高级集群管理 (ACM) 向导在 AWS 上创建 OpenShift 集群。参考说明"此处"。

您还可以从 OpenShift 混合云控制台在 AWS 中创建集群。参考"此处"以获取说明。

使用 ACM 创建集群时，您可以在表单视图中填写详细信息后通过编辑 yaml 文件来自定义安装。集群创建完成后，可以通过ssh登录到集群的节点进行故障排除或额外的手动配置。使用您在安装过程中提供的 ssh 密钥和用户名 core 登录。

使用**BlueXP**在 **AWS** 中部署**Cloud Volumes ONTAP** 。

- 在本地 VMware 环境中安装连接器。参考说明"此处"。
- 使用连接器在 AWS 中部署 CVO 实例。参考说明"此处"。

该连接器也可以安装在云环境中。参考"此处"了解更多信息。

在 **OCP** 集群中安装**Trident**

- 使用 Helm 部署Trident Operator。参考说明"此处"
- 创建后端和存储类。参考说明"此处"。

使用**Trident**的 **CSI** 拓扑功能实现多区域架构

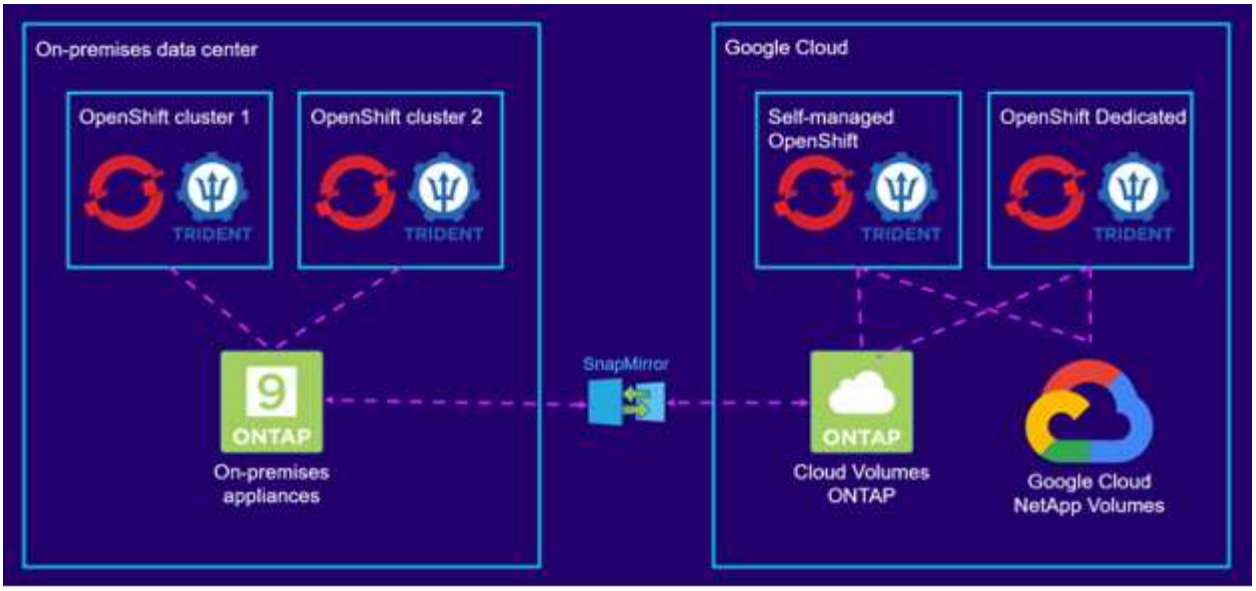
如今，云提供商使 Kubernetes/OpenShift 集群管理员能够生成基于区域的集群节点。节点可以位于一个区域内的不同可用区，也可以跨多个区域。为了方便在多区域架构中为工作负载配置卷， Trident使用了 CSI 拓扑。使用 CSI 拓扑功能，可以根据区域和可用区域将对卷的访问限制到节点子集。参考"此处"了解更多详细信息。

Kubernetes 支持两种卷绑定模式： - 当 ***VolumeBindingMode*** 设置为 ***Immediate***（默认）时，Trident会在没有任何拓扑感知的情况下创建卷。持久卷的创建不依赖于请求 pod 的调度要求。 - 当 ***VolumeBindingMode*** 设置为 ***WaitForFirstConsumer*** 时，PVC 的持久卷的创建和绑定将被延迟，直到使用该 PVC 的 pod 被调度和创建。这样，就可以创建卷来满足拓扑要求所强制执行的调度约束。 Trident存储后端可以设计为根据可用区域（拓扑感知后端）选择性地配置卷。对于使用此类后端的 StorageClasses，只有在受支持的区域/区域中调度的应用程序请求时才会创建卷。 （拓扑感知 StorageClass）参考"此处"了解更多详细信息。

在 Google Cloud 上部署和配置 Red Hat OpenShift 容器平台

本节介绍了如何在 GCP 中设置和管理 OpenShift 集群以及在其上部署有状态应用程序的高级工作流程。它展示了如何使用Google Cloud NetApp Volumes和NetApp Cloud Volumes ONTAP存储在Trident的帮助下提供持久卷。

下图显示了在 GCP 上部署并使用 VPN 连接到数据中心的集群。



在 GCP 中部署 Red Hat OpenShift Container 平台集群有多种方法。此设置的高级描述提供了所使用的特定方法的文档链接。您可以参考"资源部分"。

设置过程可分为以下步骤：

从 **CLI** 在 **GCP** 上安装 **OCP** 集群

- 确保您已满足所有规定的先决条件"此处"。
- 为了实现本地和 GCP 之间的 VPN 连接，我们创建并配置了一个 pfSense VM。有关说明，请参阅 "此处"。
  - 只有在 Google Cloud Platform 中创建 VPN 网关后，才能配置 pfSense 中的远程网关地址。
  - 只有在 OpenShift 集群安装程序运行并创建集群的基础架构组件后，才能配置第 2 阶段的远程网络 IP 地址。
  - 只有在安装程序创建集群的基础架构组件后，才能配置 Google Cloud 中的 VPN。
- 现在在 GCP 上安装 OpenShift 集群。
  - 获取安装程序和pull secret，按照文档提供的步骤部署集群 "此处"。
  - 安装在 Google Cloud Platform 中创建一个 VPC 网络。它还在 Cloud DNS 中创建一个私有区域并添加 A 记录。
    - 使用VPC网络的CIDR块地址配置pfSense并建立VPN连接。确保防火墙设置正确。
    - 使用 Google Cloud DNS 的 A 记录中的 IP 地址在本地环境的 DNS 中添加 A 记录。
  - 集群安装完成，会提供一个kubeconfig文件以及登录集群控制台的用户名和密码。

部署**Google Cloud NetApp Volumes**

- 可以按照概述将Google Cloud NetApp Volumes添加到您的项目中"此处"。

使用**BlueXP**在 **GCP** 中部署**Cloud Volumes ONTAP**

- 在 Google Cloud 中安装连接器。参考说明 "此处"。
- 使用连接器在 Google Cloud 中部署 CVO 实例。请参阅此处的说明。 https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

在 **GCP** 中的 **OCP** 集群中安装**Trident**

- 部署Trident 的方法有很多，如下所示 "此处"。
- 对于这个项目， Trident是通过按照说明手动部署Trident Operator 来安装的 "此处"。
- 创建后端和存储类。参考说明"此处"。

使用**Trident**的 **CSI** 拓扑功能实现多区域架构

如今，云提供商使 Kubernetes/OpenShift 集群管理员能够生成基于区域的集群节点。节点可以位于一个区域内的不同可用区，也可以跨多个区域。为了方便在多区域架构中为工作负载配置卷， Trident使用了 CSI 拓扑。使用 CSI 拓扑功能，可以根据区域和可用区域将对卷的访问限制到节点子集。参考"此处"了解更多详细信息。

> Kubernetes 支持两种卷绑定模式： - 当 ***VolumeBindingMode*** 设置为 ***Immediate***（默认）时，Trident会在没有任何拓扑感知的情况下创建卷。持久卷的创建不依赖于请求 pod 的调度要求。 - 当 ***VolumeBindingMode*** 设置为 ***WaitForFirstConsumer*** 时，PVC 的持久卷的创建和绑定将被延迟，直到使用该 PVC 的 pod 被调度和创建。这样，就可以创建卷来满足拓扑要求所强制执行的调度约束。 Trident存储后端可以设计为根据可用区域（拓扑感知后端）选择性地配置卷。对于使用此类后端的 StorageClasses，只有在受支持的区域/区域中调度的应用程序请求时才会创建卷。 （拓扑感知 StorageClass）参考"此处"了解更多详细信息。

演示视频

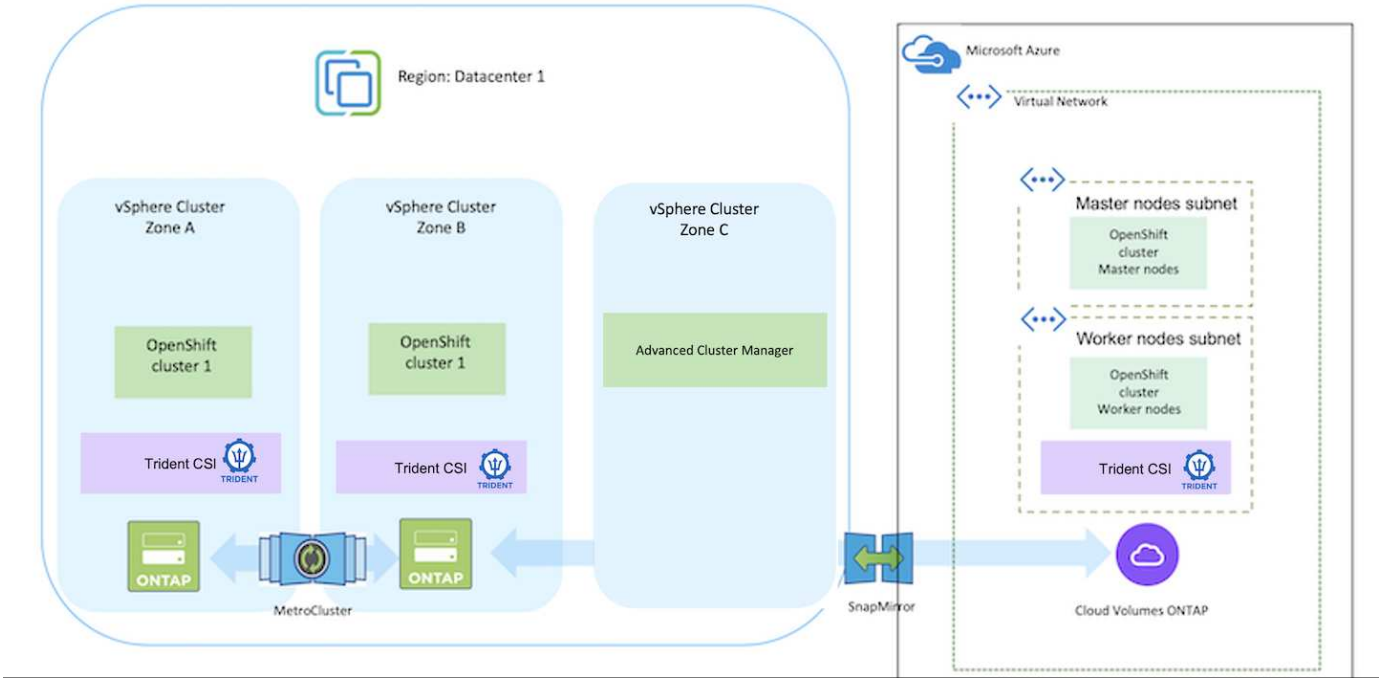
在 Google Cloud Platform 上安装 OpenShift 集群

将 OpenShift 集群导入Trident Protect

在 Azure 上部署和配置 Red Hat OpenShift 容器平台

本节介绍了如何在 Azure 中设置和管理 OpenShift 群集以及在其上部署有状态应用程序的高级工作流程。它展示了如何使用NetApp Cloud Volumes ONTAP存储在Trident的帮助下提供持久卷。提供了有关使用Trident Protect 为有状态应用程序执行数据保护和迁移活动的详细信息。

下图显示了在 Azure 上部署并使用 VPN 连接到数据中心的集群。



有几种方法可以在 Azure 中部署 Red Hat OpenShift Container 平台集群。此设置的高级描述提供了所使用的特定方法的文档链接。您可以参考"资源部分"。

设置过程可分为以下步骤：

从 **CLI** 在 **Azure** 上安装 **OCP** 群集。

- 确保您已满足所有规定的先决条件"此处"。
- 创建 VPN、子网和网络安全组以及私有 DNS 区域。创建 VPN 网关和站点到站点 VPN 连接。
- 为了实现本地和 Azure 之间的 VPN 连接，我们创建并配置了一个 pfSense VM。有关说明，请参阅"此处"。
- 获取安装程序和pull secret，按照文档提供的步骤部署集群"此处"。
- 集群安装完成，会提供一个kubeconfig文件以及登录集群控制台的用户名和密码。

下面给出了一个示例 install-config.yaml 文件。

```
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 中安装连接器。参考说明 "此处"。
- 使用连接器在 Azure 中部署 CVO 实例。请参阅说明链接： https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [此处。]

使用**Trident**的 **CSI** 拓扑功能实现多区域架构

如今，云提供商使 Kubernetes/OpenShift 集群管理员能够生成基于区域的集群节点。节点可以位于一个区域内的不同可用区，也可以跨多个区域。为了方便在多区域架构中为工作负载配置卷， Trident使用了 CSI 拓扑。使用 CSI 拓扑功能，可以根据区域和可用区域将对卷的访问限制到节点子集。参考"此处"了解更多详细信息。

Kubernetes 支持两种卷绑定模式： - 当 ***VolumeBindingMode*** 设置为 ***Immediate***（默认）时，Trident会在没有任何拓扑感知的情况下创建卷。持久卷的创建不依赖于请求 pod 的调度要求。 - 当 ***VolumeBindingMode*** 设置为 ***WaitForFirstConsumer*** 时，PVC 的持久卷的创建和绑定将被延迟，直到使用该 PVC 的 pod 被调度和创建。这样，就可以创建卷来满足拓扑要求所强制执行的调度约束。 Trident存储后端可以设计为根据可用区域（拓扑感知后端）选择性地配置卷。对于使用此类后端的 StorageClasses，只有在受支持的区域/区域中调度的应用程序请求时才会创建卷。 （拓扑感知 StorageClass）参考"此处"了解更多详细信息。

使用Trident Protect 进行数据保护

此页面显示了使用Trident Protect (ACC) 在 VMware vSphere 或云中运行的基于 Red Hat OpenShift Container 的应用程序的数据保护选项。

当用户使用 Red Hat OpenShift 对其应用程序进行现代化改造时，应该制定数据保护策略来保护它们免受意外删除或任何其他人为错误的影响。通常，出于监管或合规目的，还需要制定保护策略来保护其数据免受灾难。

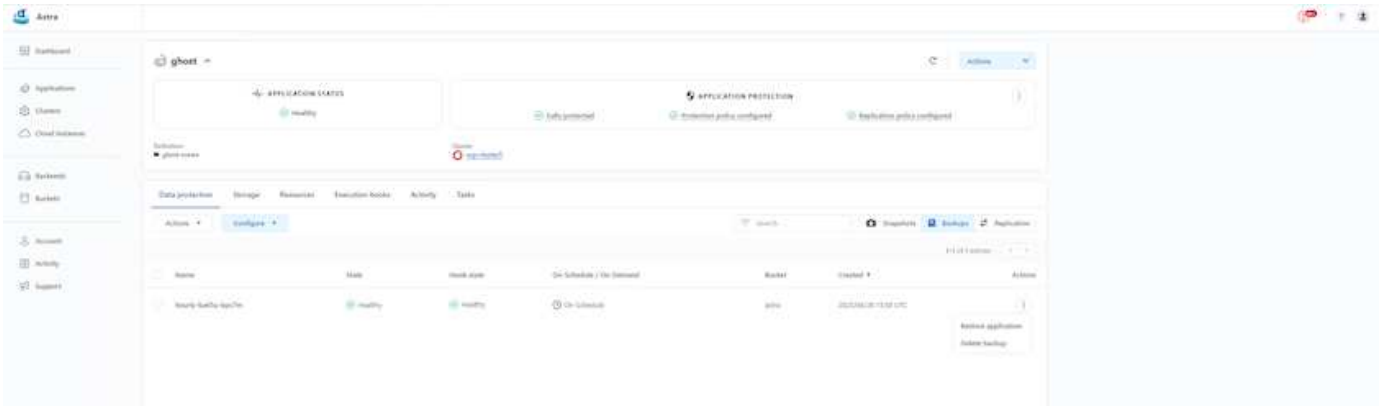
数据保护的要求多种多样，从恢复到某个时间点的副本到无需任何人工干预即可自动故障转移到不同的故障域。许多客户选择ONTAP作为其 Kubernetes 应用程序的首选存储平台，因为它具有丰富的功能，例如多租户、多协议、高性能和容量产品、多站点位置的复制和缓存、安全性和灵活性。

客户可以将云环境设置为其数据中心的扩展，以便他们可以利用云的优势，并为将来转移其工作负载做好准备。对于这样的客户，将他们的OpenShift应用程序和数据备份到云环境成为不可避免的选择。然后，他们可以将应用程序和相关数据恢复到云端或数据中心的 OpenShift 集群。

使用 **ACC** 备份和恢复

应用程序所有者可以审查和更新 ACC 发现的应用程序。 Trident Protect 可以使用 CSI 获取 Snapshot 副本，并使用时间点 Snapshot 副本执行备份。备份目标可以是云环境中的对象存储。可以为计划备份和要保留的备份版本数量配置保护策略。最小 RPO 为一小时。

使用 **ACC** 从备份还原应用程序



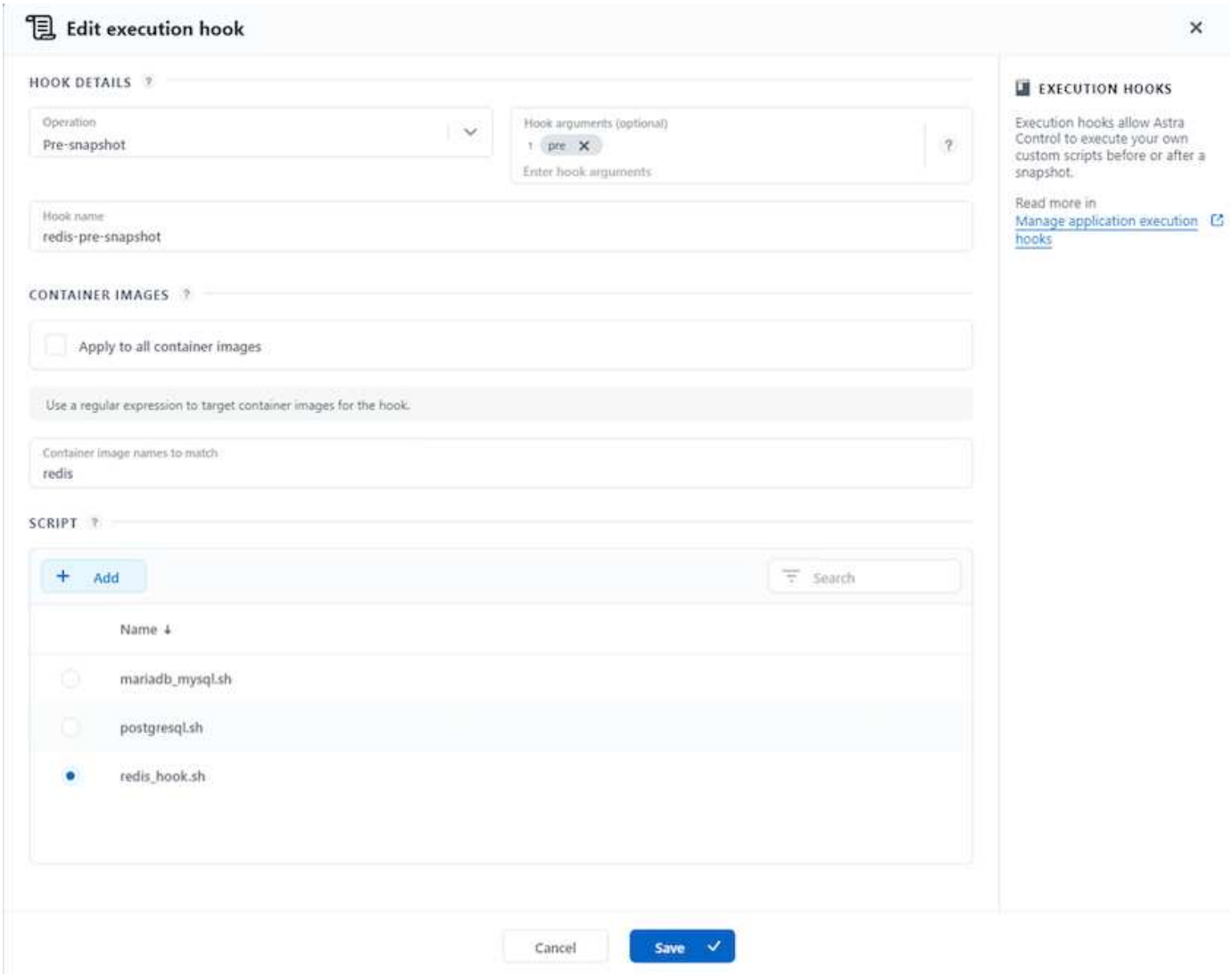
应用程序特定的执行钩子

即使存储阵列级数据保护功能可用，通常仍需要采取额外的步骤来确保备份和恢复应用程序的一致性。特定于应用程序的附加步骤可以是： - 在创建 Snapshot 副本之前或之后。 - 在创建备份之前或之后。 - 从 Snapshot 副本或备份恢复后。

Trident Protect 可以执行这些特定于应用程序的步骤，这些步骤被编码为称为执行钩子的自定义脚本。

NetApp 的"开源项目 Verda"为流行的云原生应用程序提供执行挂钩，使保护应用程序变得简单、强大且易于协调。如果您拥有存储库中没有的应用程序的足够信息，请随意为该项目做出贡献。

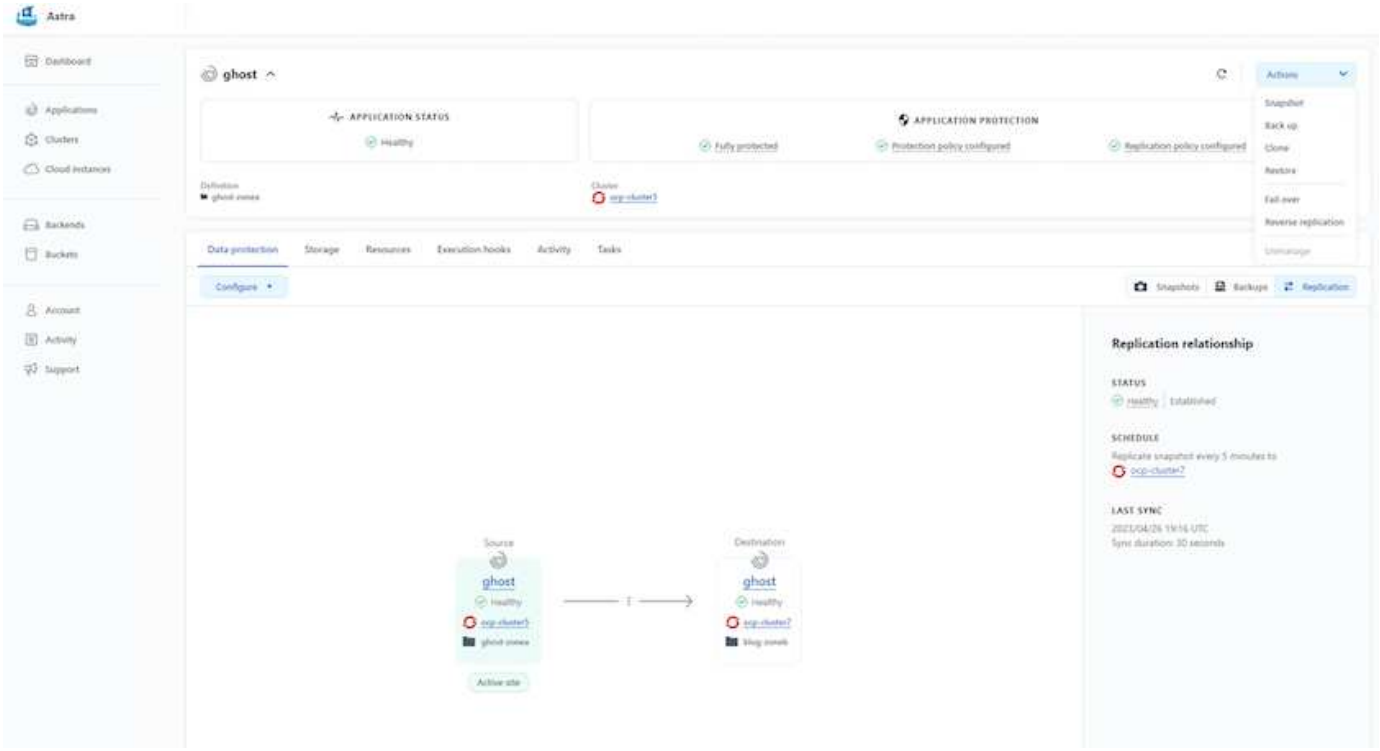
Redis 应用程序预快照的示例执行挂钩。



使用 ACC 进行复制

对于区域保护或低 RPO 和 RTO 解决方案，可以将应用程序复制到在不同站点（最好是在另一个区域）运行的另一个 Kubernetes 实例。 Trident Protect 利用ONTAP异步SnapMirror ，RPO 低至 5 分钟。参考"此处"有关SnapMirror设置说明。

带有 ACC 的SnapMirror



san-economy 和 nas-economy 存储驱动程序不支持复制功能。参考"此处"了解更多详细信息。

演示视频：

"Trident Protect 灾难恢复演示视频"

使用Trident Protect 进行数据保护

有关Trident Protect 数据保护功能的详细信息"此处"

使用 ACC 进行灾难恢复（使用复制进行故障转移和故障恢复）

使用Astra Control 进行应用程序故障转移和故障恢复

使用Trident Protect 进行数据迁移

此页面显示了带有Trident Protect (ACC) 的 Red Hat OpenShift 集群上的容器工作负载的数据迁移选项。具体来说，客户可以使用Trident Protect 将部分选定的工作负载或所有工作负载从其本地数据中心迁移到云端，将其应用程序克隆到云端以进行测试，或将其从数据中心迁移到云端

数据迁移

要将应用程序从一个环境迁移到另一个环境，可以使用 ACC 的以下功能之一：

- 复制
- 备份和恢复

- 克隆

请参阅"数据保护部分"用于复制和备份和恢复选项。

参考"此处"有关克隆的更多详细信息。

Astra复制功能仅支持Trident容器存储接口 (CSI)。但是，nas-economy 和 san-economy 驱动程序不支持复制。

使用 **ACC** 执行数据复制