



采用Red Hat OpenShift的NetApp混合云

NetApp Solutions

NetApp
March 12, 2024

目录

采用Red Hat OpenShift容器工作负载的NetApp混合云	1
适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案	1
适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案	12
适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案	22
适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案	38

采用Red Hat OpenShift容器工作负载的NetApp混合云

适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案

概述

NetApp发现、越来越多的客户正在利用围绕Kubernetes构建的容器和流程编排平台来打造现代化的传统企业级应用程序以及构建新应用程序。Red Hat OpenShift容器平台就是我们看到许多客户采用的一个示例。

随着越来越多的客户开始在企业中采用容器、NetApp已做好充分准备、可以满足有状态应用程序的持久存储需求以及数据保护、数据安全和数据迁移等传统数据管理需求。但是、可以使用不同的策略、工具和方法来满足这些需求。

**NetApp ONTAP 基于下面列出的存储选项，可为容器和部署提供安全性、数据保护、可靠性和灵活性。

- 内部环境中的自行管理存储：
 - NetApp光纤连接存储(FAS)、NetApp全闪存FAS阵列(AFF)、NetApp全SAN阵列(ASA)和ONTAP Select
- 内部部署中由提供商管理的存储：
 - NetApp Keystone 提供存储即服务(STaaS)
- 云中的自行管理存储：
 - NetApp Cloud Volumes ONTAP (CVO)可在超大容量云中提供自行管理的存储
- 云中由提供商管理的存储：
 - Cloud Volumes Service for Google Cloud (CVS)、Azure NetApp Files (ANF)、Amazon FSx for NetApp ONTAP 可在超云中提供完全托管的存储

ONTAP feature highlights

Storage Administration	Performance & Scalability
<ul style="list-style-type: none"> • Multi-tenancy • FlexVol & FlexGroup • LUN • Quotas 	<ul style="list-style-type: none"> • ONTAP CLI & API • System Manager & BlueXP <ul style="list-style-type: none"> • FlexCache • FlexClone <ul style="list-style-type: none"> • iSCSI, session trunking, multipathing • Scale-out clusters
Availability & Resilience	Access Protocols
<ul style="list-style-type: none"> • Multi-AZ HA deployment (MetroCluster) • SnapShot & SnapRestore • SnapMirror 	<ul style="list-style-type: none"> • NFS –v3, v4, v4.1, v4.2 • SMB – v2, v3 <ul style="list-style-type: none"> • iSCSI • Multi-protocol access
Storage Efficiency	Security & Compliance
<ul style="list-style-type: none"> • Deduplication & Compression • Compaction 	<ul style="list-style-type: none"> • Thin provisioning • Data Tiering (Fabric Pool) <ul style="list-style-type: none"> • Fpolicy & Vscan • Active Directory integration <ul style="list-style-type: none"> • LDAP & Kerberos • Certificate based authentication

NetApp BlueXP使您能够从一个控制平台/接口管理所有存储和数据资产。

您可以使用BlueXP创建和管理云存储(例如Cloud Volumes ONTAP 和Azure NetApp Files)、移动、保护和分析数据以及控制许多内部和边缘存储设备。

NetApp Astra Trident是一款符合CSI的存储编排程序，支持快速、轻松地使用由上述各种NetApp存储选项提供支持的永久性存储。它是由NetApp维护和支持的开源软件。



Astra Trident CSI feature highlights

CSI specific	Security
<ul style="list-style-type: none"> • CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies • CSI topology • Volume expansion 	<ul style="list-style-type: none"> • Dynamic-export policy management • iSCSI initiator-groups dynamic management • iSCSI bidirectional CHAP
Control	Installation methods
<ul style="list-style-type: none"> • Storage and performance consumption • Monitoring 	<ul style="list-style-type: none"> • Volume Import • Cross Namespace Volume Access • Binary • Helm chart • Operator • GitOps
Choose your access mode	Choose your protocol
<ul style="list-style-type: none"> • RWO (ReadWriteOnce, i.e 1↔1) • RWX (ReadWriteMany, i.e 1↔n) • ROX (ReadOnlyMany) 	<ul style="list-style-type: none"> • NFS • SMB • iSCSI

业务关键型容器工作负载所需的不仅仅是永久性卷。他们的数据管理要求也需要保护和迁移应用程序Kubernetes对象。



除了用户数据之外、应用程序数据还包括Kubernetes对象：以下是一些示例： - Kubernetes对象、例如Pod规格、PVC、部署、服务-自定义配置对象、例如配置映射和密钥-持久数据、例如Snapshot副本、备份、克隆-自定义资源、例如CRS和CRD

NetApp Astra Control作为完全托管和自我管理软件提供，可提供流程编排，实现强大的应用程序数据管理。请参见 "[Astra 文档](#)" 有关Astra系列产品的更多详细信息。

本参考文档使用NetApp Astra Control Center验证了在Red Hat OpenShift容器平台上部署的基于容器的应用程序的迁移和保护。此外、解决方案还提供了有关部署和使用Red Hat高级集群管理(ACM)来管理容器平台的详细信息。本文档还重点介绍了使用Astra Trident CSI配置程序将NetApp存储与Red Hat OpenShift容器平台集成的详细信息。Astra Control Center部署在集线器集群上、用于管理容器应用程序及其永久性存储生命周期。最后、它还提供了一个解决方案、用于在AWS (ROSA)中使用Amazon FSx for NetApp ONTAP (FSxN)作为永久性存储的受管Red Hat OpenShift集群上对容器工作负载进行复制、故障转移和故障恢复。

适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案的价值主张

大多数客户并不只是在没有任何现有基础架构的情况下开始构建基于Kubennet的环境。他们可能是一家传统的IT公司、在虚拟机(例如、在大型VMware环境中)上运行大多数企业级应用程序。然后、他们开始构建基于容器的小型环境、以满足现代应用程序开发团队的需求。这些计划通常从小规模入手、随着团队学习这些新技术和技能、并开始认识到采用这些新技术和技能的诸多优势、这些计划开始变得越来越普及。对客户来说、好消息是NetApp可以满足这两种环境的需求。这套采用Red Hat OpenShift的混合多云解决方案将赋予NetApp客户采用现代云技术和服务的能力、而无需全面革新整个基础架构和组织。无论客户应用程序和数据托管在内部环境、云中、虚拟机上还是容器上、NetApp都可以提供一致的数据管理、保护、安全性和可移动性。借助这些新解决方案、NetApp数十年来在内部数据中心环境中提供的相同价值将在整个企业数据范围内实现、而无需投入大量资金来重新利用、获得新技能或组建新团队。无论客户处于云之旅的哪个阶段、NetApp都能很好地帮助他们解决这些业务挑战。

采用Red Hat OpenShift的NetApp混合多云：

- 为客户提供经验证的设计和实践、展示在将Red Hat OpenShift与基于NetApp的存储解决方案结合使用时、客户管理、保护、保护和迁移其数据和应用程序的最佳方式。
- 为在VMware环境、裸机基础架构或这两者的组合中使用NetApp存储运行Red Hat OpenShift的客户提供最佳实践。
- 演示内部环境和云环境以及同时使用这两者的混合环境的策略和选项。

适用于Red Hat OpenShift容器工作负载的受支持NetApp混合云解决方案

解决方案 使用OpenShift容器平台(OCP)、OpenShift高级集群管理器(ACM)、NetApp ONTAP、NetApp BlueXP和NetApp Astra控制中心(ACC)测试和验证迁移和集中数据保护。

对于此解决方案、NetApp会对以下情形进行测试和验证。根据以下特征、解决方案可分为多种情形：

- 内部部署
- 云

- 自行管理的OpenShift集群和自行管理的NetApp存储
- 提供商管理的OpenShift集群和提供商管理的NetApp存储

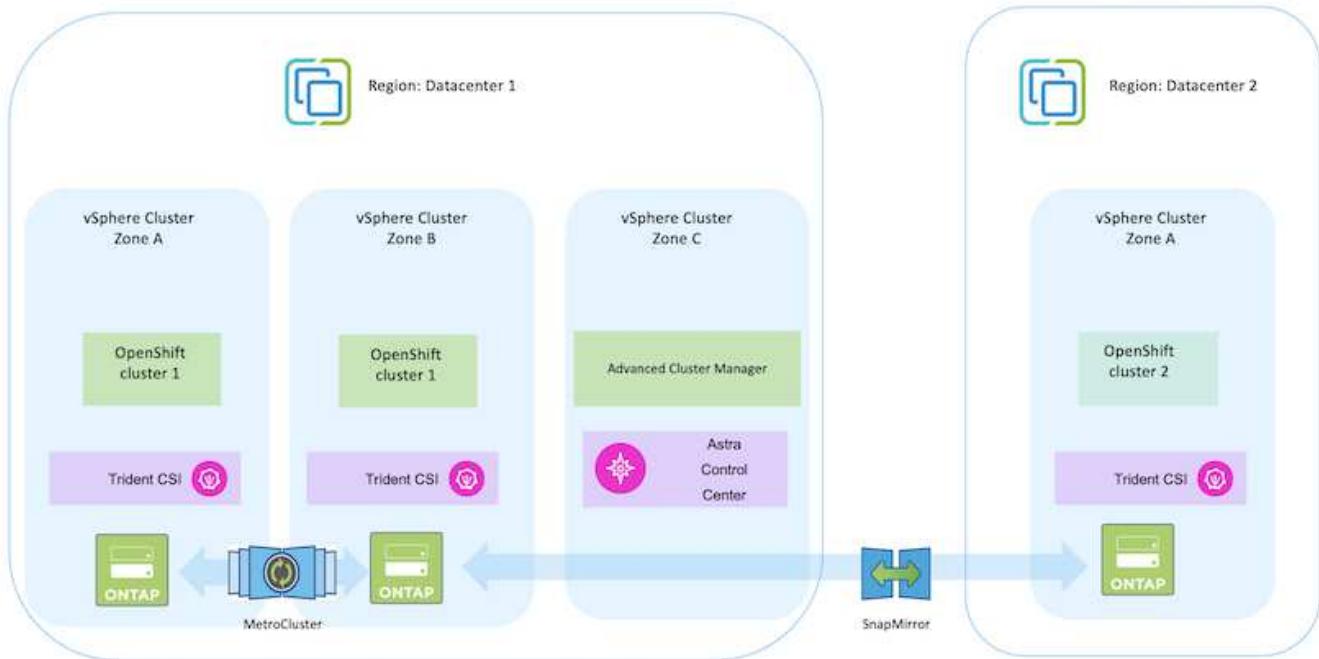
我们将在未来构建更多的解决方案和用例。

方案1：使用ACC在内部环境中保护和迁移数据

内部：自行管理的**OpenShift**集群和自行管理的**NetApp**存储

- 使用ACC创建Snapshot副本、备份和恢复以保护数据。
- 使用ACC对容器应用程序执行SnapMirror复制。

场景 1

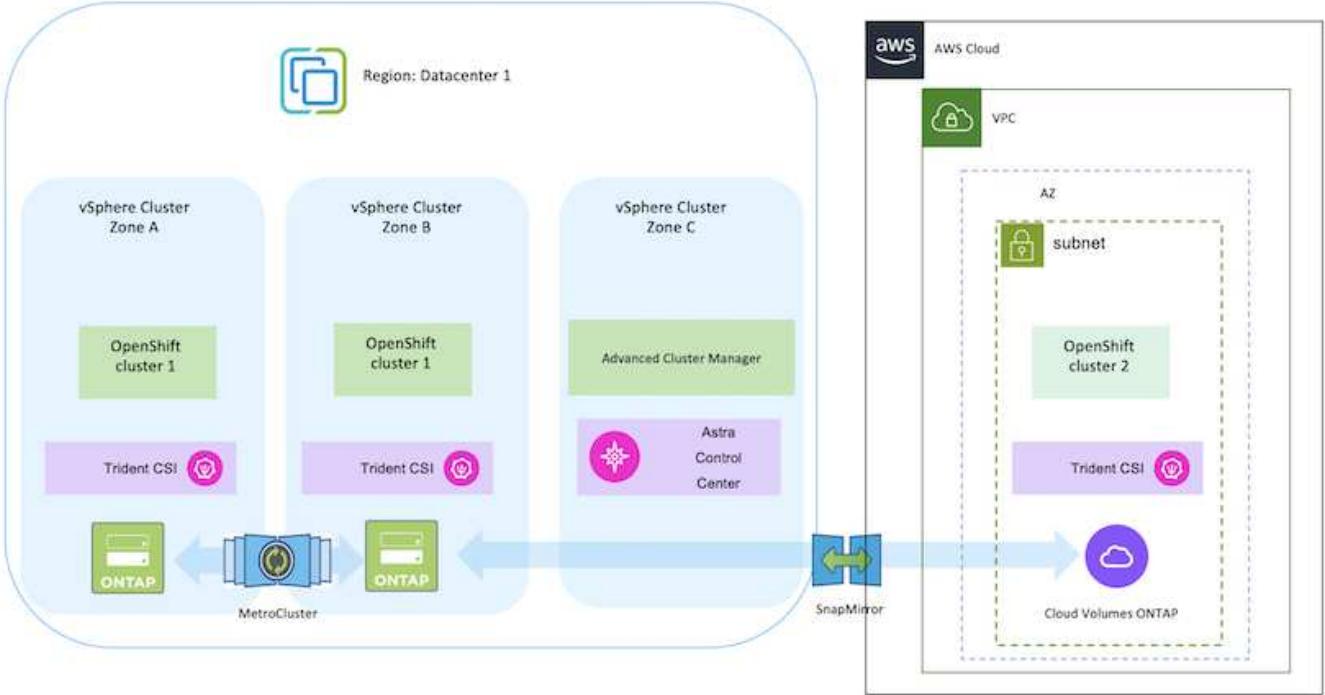


方案2：使用ACC保护数据并将其从内部环境迁移到AWS环境

内部：自行管理的**OpenShift**集群和自行管理的**NetApp**存储 AWS云：自行管理的**OpenShift**集群和自行管理的**存储****

- 使用ACC执行备份和恢复以保护数据。
- 使用ACC对容器应用程序执行SnapMirror复制。

场景 2

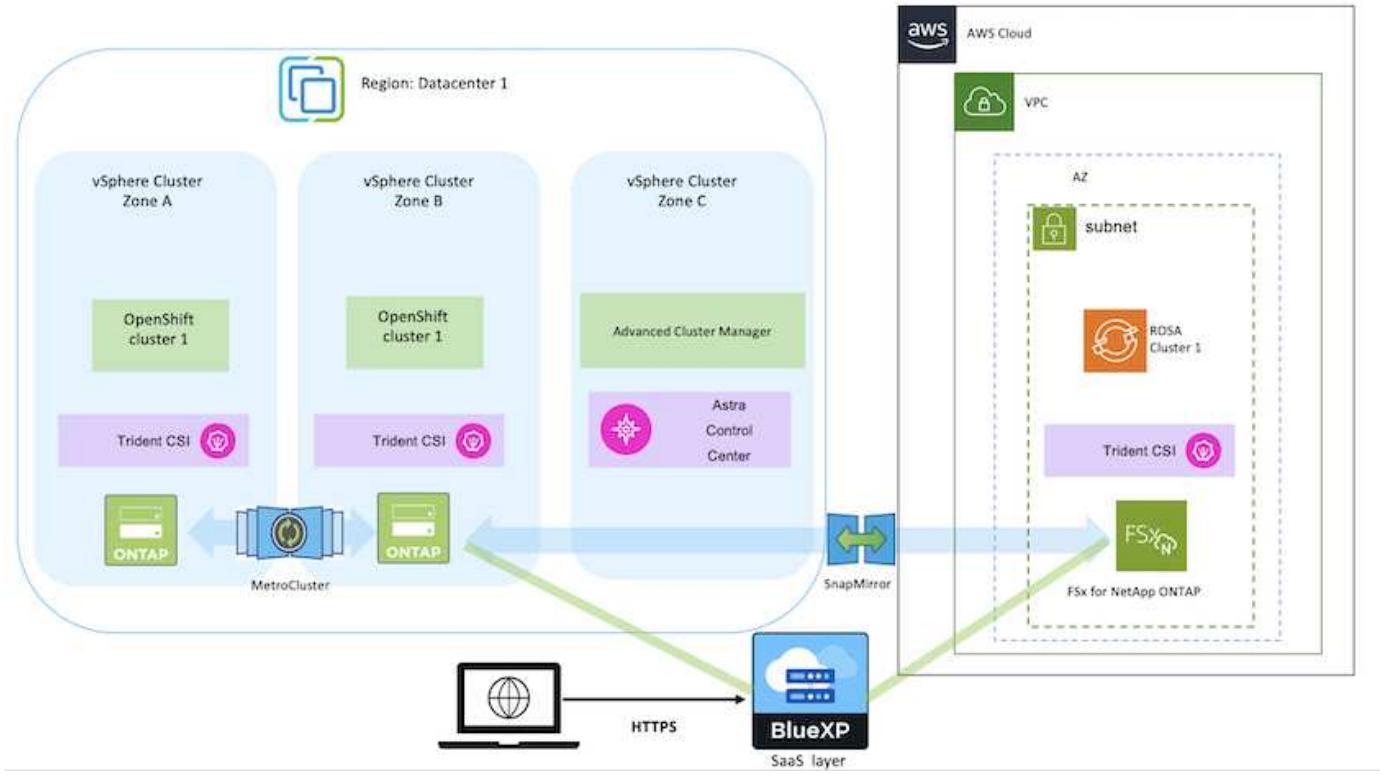


方案3：数据保护以及从内部环境迁移到AWS环境

内部：自行管理的**OpenShift**集群和自行管理的存储 **AWS云**：提供商管理的**OpenShift**集群(**ROSA**)和提供商管理的存储(**FSxN**)

- 使用BlueXP执行永久性卷复制(**FSxN**)。
- 使用OpenShift GitOps重新创建应用程序元数据。

方案3.

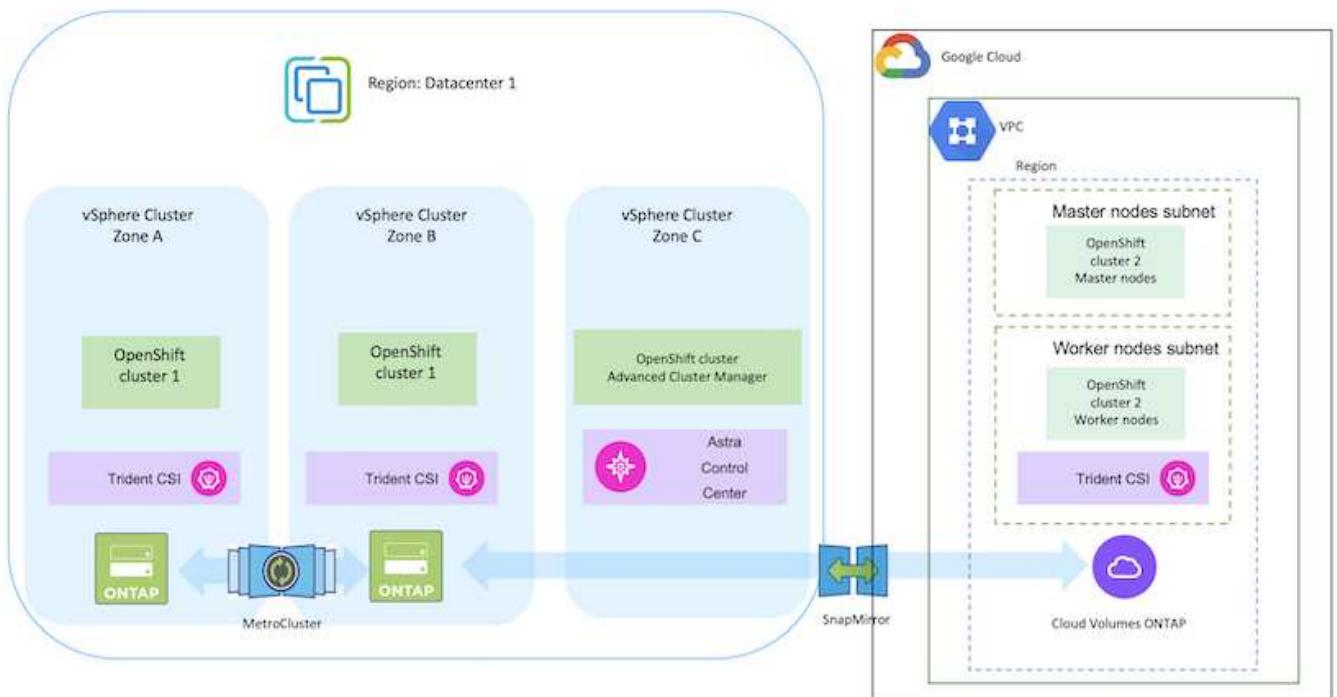


方案4：使用ACC保护数据并将数据从内部环境迁移到GCP环境

内部：自行管理的OpenShift集群和自行管理的存储

Google Cloud：自行管理的OpenShift集群和自行管理的存储

- 使用ACC执行备份和恢复以保护数据。
- 使用ACC对容器应用程序执行SnapMirror复制。



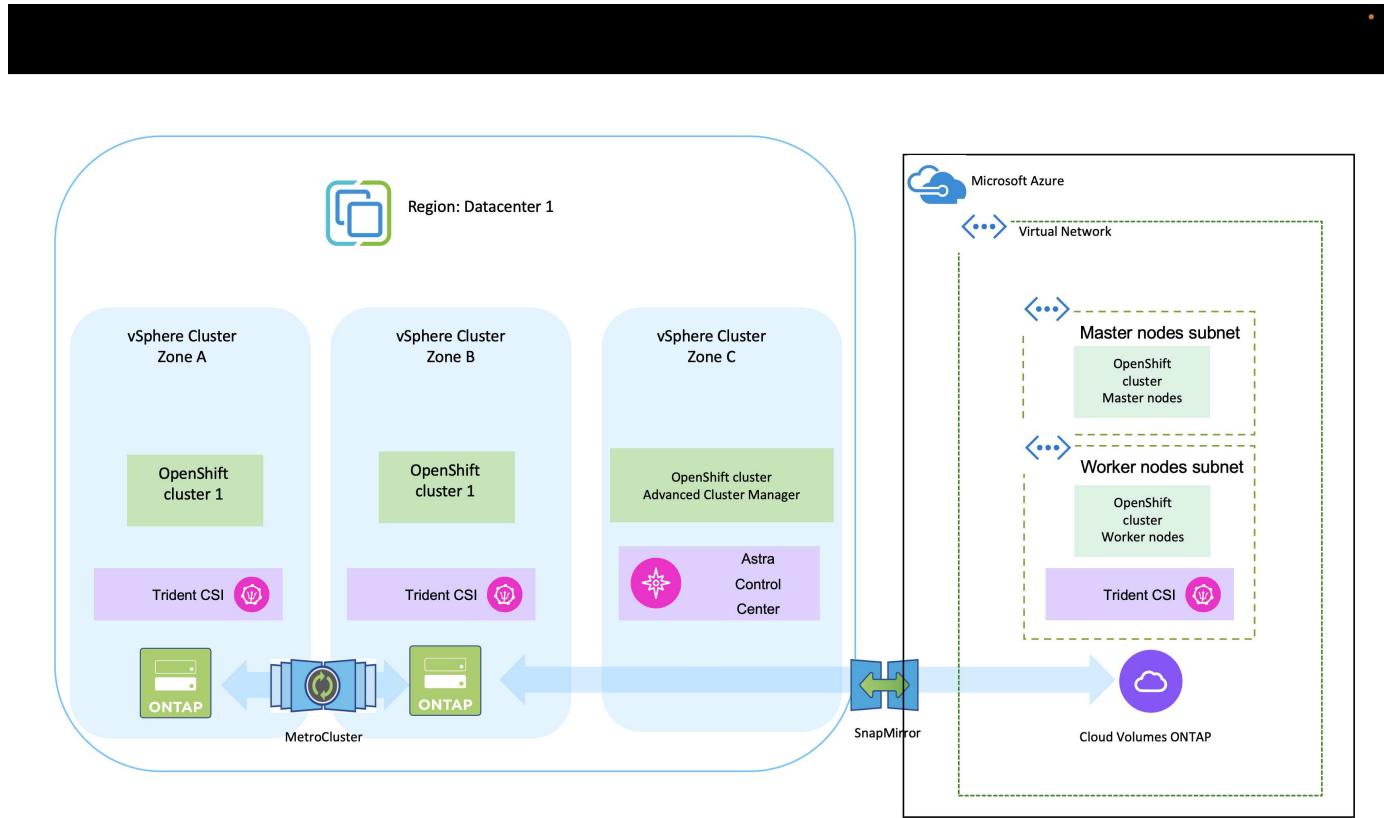
有关在MetroCluster 配置中使用ONTAP 时的注意事项、请参见 "[此处](#)"。

方案5：使用ACC保护数据并将其从内部环境迁移到Azure环境

内部：自行管理的**OpenShift**集群和自行管理的存储

Azure云：自行管理的**OpenShift**集群和自行管理的存储

- 使用ACC执行备份和恢复以保护数据。
- 使用ACC对容器应用程序执行SnapMirror复制。



有关在MetroCluster 配置中使用ONTAP 时的注意事项、请参见 "[此处](#)"。

解决方案 验证中使用的各种组件的版本

解决方案 使用OpenShift容器平台、OpenShift高级集群管理器、NetApp ONTAP 和NetApp Asta控制中心测试和验证迁移和集中式数据保护。

解决方案的方案1、2和3已使用下表所示的版本进行了验证：

* 组件 *	* 版本 *
VMware	vSphere Client 8.0.0.10200 VMware ESXi、8.0.0、20842819
集线器集群	OpenShift 4.11.34
源集群和目标集群	OpenShift 4.12.9、在内部和AWS中

NetApp Astra三端	TRIdent服务器和客户端23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
*NetApp ONTAP *	ONTAP 9.12.1
*AWS FSx for NetApp ONTAP *	单可用性(AZ)

已使用下表所示的版本对解决方案的方案4进行了验证：

* 组件 *	* 版本 *
VMware	vSphere Client 8.0.2.00000版 VMware ESXi 8.0.2、22380479
集线器集群	OpenShift 4.13.13.
源集群和目标集群	OpenShift 4.13.12. 内部部署和Google Cloud中
NetApp Astra三端	TRIdent服务器和客户端23.07.0
NetApp Astra Control Center	符合23.07.0-25标准
*NetApp ONTAP *	ONTAP 9.12.1
* Cloud Volumes ONTAP *	单可用性(AZ)、单节点、9.14.0

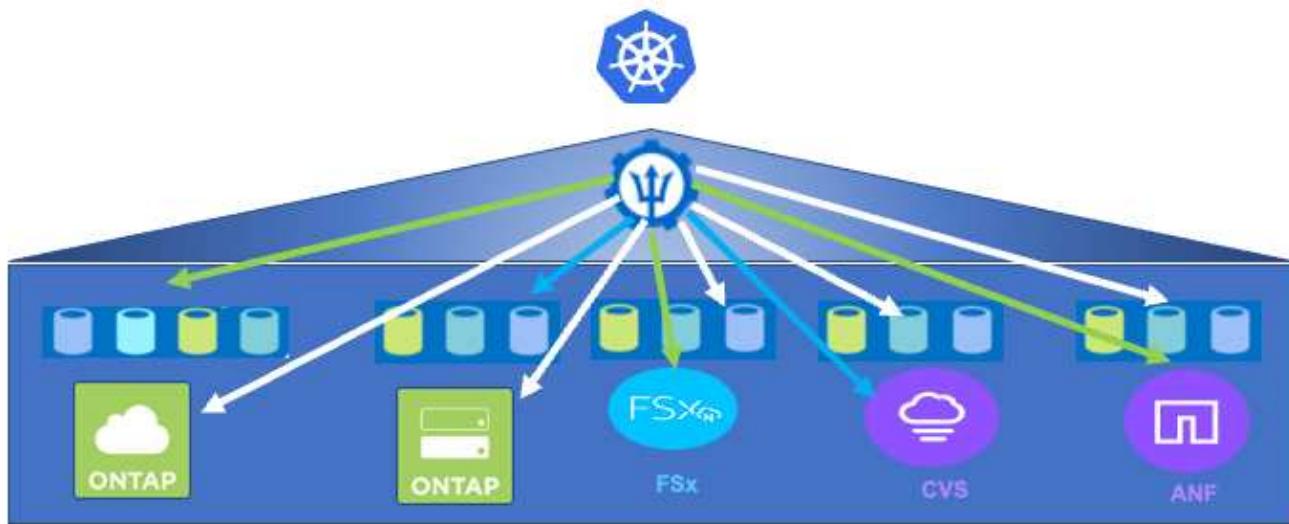
已使用下表所示的版本对解决方案的方案5进行了验证：

* 组件 *	* 版本 *
VMware	vSphere Client 8.0.2.00000版 VMware ESXi 8.0.2、22380479
源集群和目标集群	OpenShift 4.13.25 在内部和Azure中
NetApp Astra三端	通过三项技术实现的服务器和客户端以及Astra Control配置程序23.10.0
NetApp Astra Control Center	行政协调会23.10.
*NetApp ONTAP *	ONTAP 9.12.1
* Cloud Volumes ONTAP *	单可用性(AZ)、单节点、9.14.0

支持NetApp存储与Red Hat Open Shift容器的集成

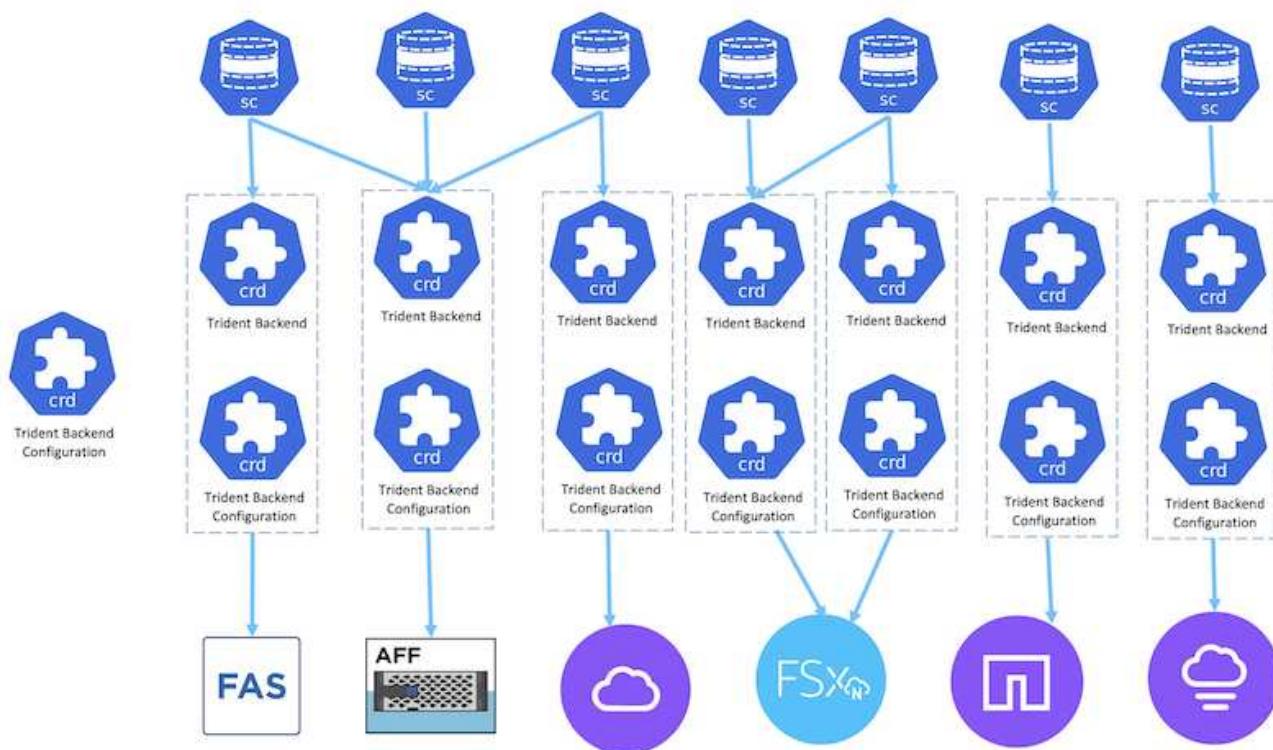
无论Red Hat Open Shift容器是在VMware上运行还是在超大型机中运行、NetApp A作用力三端均可用作其支持的各种后端NetApp存储的CSI配置程序。

下图展示了可使用NetApp Astra Dent与OpenShift集群集成的各种后端NetApp存储。

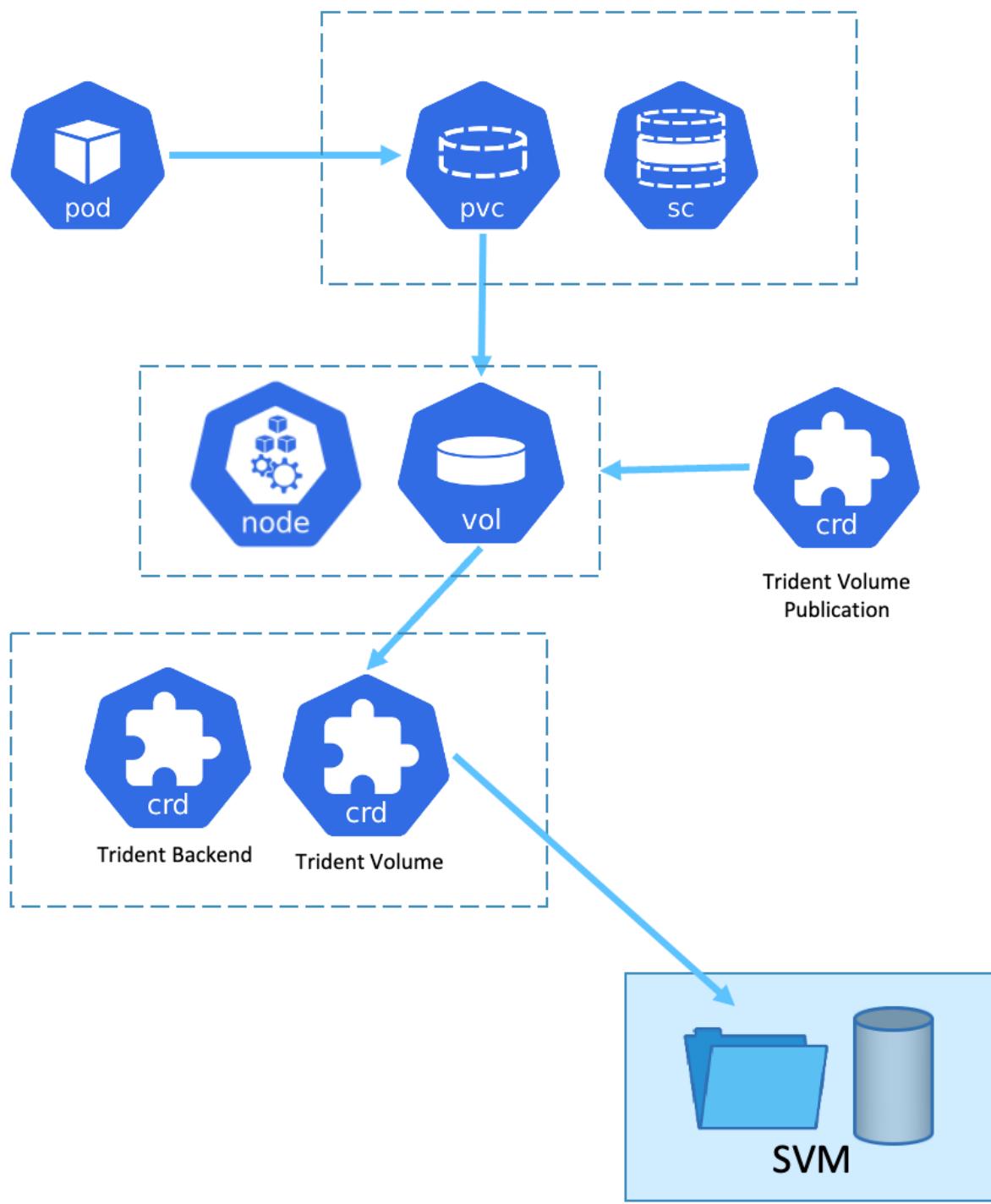


ONTAP Storage Virtual Machine (SVM)可提供安全多租户。一个OpenShift集群可以连接到一个或多个SVM、甚至可以连接到多个ONTAP 集群。存储类会根据参数或标签筛选后端存储。存储管理员可定义使用三级联后端配置连接到存储系统所需的参数。成功建立连接后、它将创建三项技术后端并填充存储类可以筛选的信息。

存储器和后端之间的关系如下所示。



应用程序所有者使用存储类请求永久性卷。存储类用于筛选后端存储。POD与后端存储之间的关系如下所示。



容器存储接口(CSI)选项

在vSphere环境中、客户可以选择VMware CSI驱动程序和/或Astra三端CSI与ONTAP集成。使用VMware CSI时、永久性卷会用作本地SCSI磁盘、而使用三端技术时、则会使用网络。由于VMware CSI不支持使用ONTAP的rwx访问模式、因此如果需要rwx模式、应用程序需要使用TRIDENT CSI。对于基于FC的部署、首选使用VMware CSI、而SnapMirror业务连续性(SMBC)可提供区域级高可用性。

VMware CSI支持

- 基于核心块的数据存储库(FC、 FCoE、 iSCSI、 NVMeoF)
- 基于核心文件的数据存储库(NFS v3、 v4)
- vVol数据存储库(块和文件)

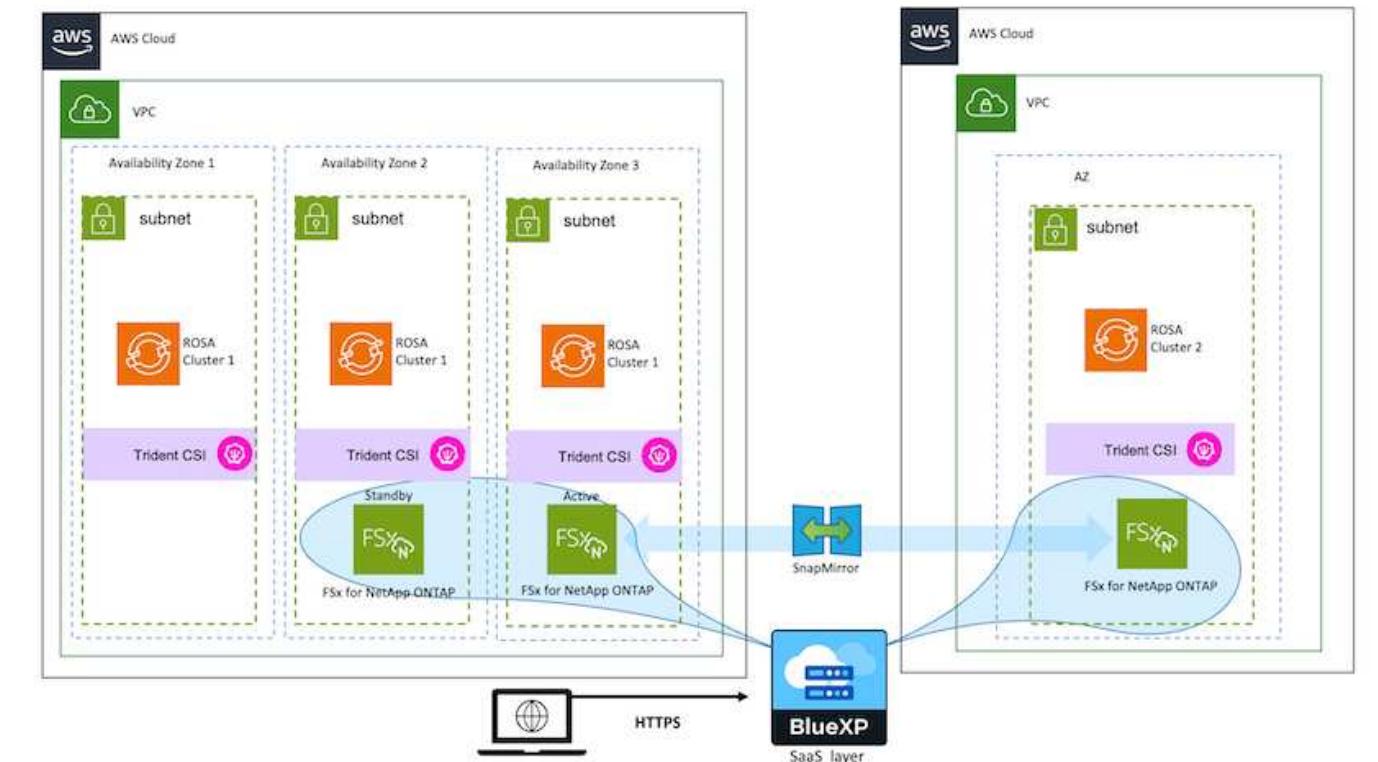
通过以下驱动程序、可以支持ONTAP

- ONTAP SAN (专用卷)
- ONTAP SAN经济模式(共享卷)
- ONTAP NAS (专用卷)
- ONTAP—NAS—经济型(共享卷)
- ONTAP—NAS—Flexgroup (专用大规模卷)

对于VMware CSI和Asta三端CSI、ONTAP 均支持对NFS使用nconnect、会话中继、Kerberos等、对块协议使用多路径、chap身份验证等。

在AWS中、FSx for NetApp ONTAP (FSxN)可以部署在单个可用性区域(AZ)或多个可用性区域(AZ)中。对于需要高可用性的生产工作负载、与单个AZ相比、多可用性可提供分区级容错、并具有更好的NVMe读取缓存。有关详细信息、请查看 "[AWS性能准则](#)"。

为了节省灾难恢复站点的成本、可以使用一个AZ FSx ONTAP。



有关FSx ONTAP 支持的SVM数量、请参见 "[管理FSx ONTAP Storage Virtual Machine](#)"

适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案

概述

NetApp发现、越来越多的客户正在利用围绕Kubernetes构建的容器和流程编排平台来打造现代化的传统企业级应用程序以及构建新应用程序。Red Hat OpenShift容器平台就是我们看到许多客户采用的一个示例。

随着越来越多的客户开始在企业中采用容器、NetApp已做好充分准备、可以满足有状态应用程序的持久存储需求以及数据保护、数据安全和数据迁移等传统数据管理需求。但是、可以使用不同的策略、工具和方法来满足这些需求。

**NetApp ONTAP 基于下面列出的存储选项，可为容器和部署提供安全性、数据保护、可靠性和灵活性。

- 内部环境中的自行管理存储：
 - NetApp光纤连接存储(FAS)、NetApp全闪存FAS阵列(AFF)、NetApp全SAN阵列(ASA)和ONTAP Select
- 内部部署中由提供商管理的存储：
 - NetApp Keystone 提供存储即服务(STaaS)
- 云中的自行管理存储：
 - NetApp Cloud Volumes ONTAP (CVO)可在超大容量云中提供自行管理的存储
- 云中由提供商管理的存储：
 - Cloud Volumes Service for Google Cloud (CVS)、Azure NetApp Files (ANF)、Amazon FSx for NetApp ONTAP 可在超云中提供完全托管的存储



ONTAP feature highlights

Storage Administration	Performance & Scalability
<ul style="list-style-type: none">• Multi-tenancy• FlexVol & FlexGroup• LUN• Quotas	<ul style="list-style-type: none">• ONTAP CLI & API• System Manager & BlueXP
Availability & Resilience	Access Protocols
<ul style="list-style-type: none">• Multi-AZ HA deployment (MetroCluster)• SnapShot & SnapRestore• SnapMirror	<ul style="list-style-type: none">• SnapMirror Business Continuity• SnapMirror Cloud
Storage Efficiency	Security & Compliance
<ul style="list-style-type: none">• Deduplication & Compression• Compaction	<ul style="list-style-type: none">• Thin provisioning• Data Tiering (Fabric Pool)
	<ul style="list-style-type: none">• iSCSI• Multi-protocol access
	<ul style="list-style-type: none">• Fpolicy & Vscan• Active Directory integration
	<ul style="list-style-type: none">• LDAP & Kerberos• Certificate based authentication

NetApp BlueXP使您能够从一个控制平台/接口管理所有存储和数据资产。

您可以使用BlueXP创建和管理云存储(例如Cloud Volumes ONTAP 和Azure NetApp Files)、移动、保护和分析数据以及控制许多内部和边缘存储设备。

NetApp Astra Trident是一款符合CSI的存储编排程序，支持快速、轻松地使用由上述各种NetApp存储选项提供支持的永久性存储。它是由NetApp维护和支持的开源软件。



Astra Trident CSI feature highlights

CSI specific <ul style="list-style-type: none">CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copiesCSI topologyVolume expansion	Security <ul style="list-style-type: none">Dynamic-export policy managementiSCSI initiator-groups dynamic managementiSCSI bidirectional CHAP
Control <ul style="list-style-type: none">Storage and performance consumptionMonitoring <ul style="list-style-type: none">Volume ImportCross Namespace Volume Access	Installation methods <ul style="list-style-type: none">BinaryHelm chartOperatorGitOps
Choose your access mode <ul style="list-style-type: none">RWO (ReadWriteOnce, i.e 1↔1)RWOP (ReadWriteOnce POD)RWX (ReadWriteMany, i.e 1↔n)ROX (ReadOnlyMany)	Choose your protocol <ul style="list-style-type: none">NFSSMBiSCSI

业务关键型容器工作负载所需的不仅仅是永久性卷。他们的数据管理要求也需要保护和迁移应用程序Kubernetes对象。



除了用户数据之外、应用程序数据还包括Kubernetes对象：以下是一些示例： - Kubernetes对象、例如Pod规格、PVC、部署、服务-自定义配置对象、例如配置映射和密钥-持久数据、例如Snapshot副本、备份、克隆-自定义资源、例如CRS和CRD

NetApp Astra Control作为完全托管和自我管理软件提供，可提供流程编排，实现强大的应用程序数据管理。请参见 "[Astra 文档](#)" 有关Astra系列产品的更多详细信息。

本参考文档使用NetApp Astra Control Center验证了在RedHat OpenShift容器平台上部署的基于容器的应用程序的迁移和保护。此外、解决方案还提供了有关部署和使用Red Hat高级集群管理(ACM)来管理容器平台的详细信息。本文档还重点介绍了使用Astra Trident CSI配置程序将NetApp存储与Red Hat OpenShift容器平台集成的详细信息。Astra Control Center部署在集线器集群上、用于管理容器应用程序及其永久性存储生命周期。最后、它还提供了一个解决方案、用于在AWS (ROSA)中使用Amazon FSx for NetApp ONTAP (FSxN)作为永久性存储的受管Red Hat OpenShift集群上对容器工作负载进行复制、故障转移和故障恢复。

NetApp解决方案 在VMware上运行Red Hat OpenShift容器平台工作负载

如果客户需要在私有数据中心的基础架构上运行现代化容器化应用程序、他们可以做到这一点。他们应规划和部署Red Hat OpenShift容器平台(OCP)、以便为部署容器工作负载打造一个成功的生产就绪环境。其OCP集群可以部署在VMware或裸机上。

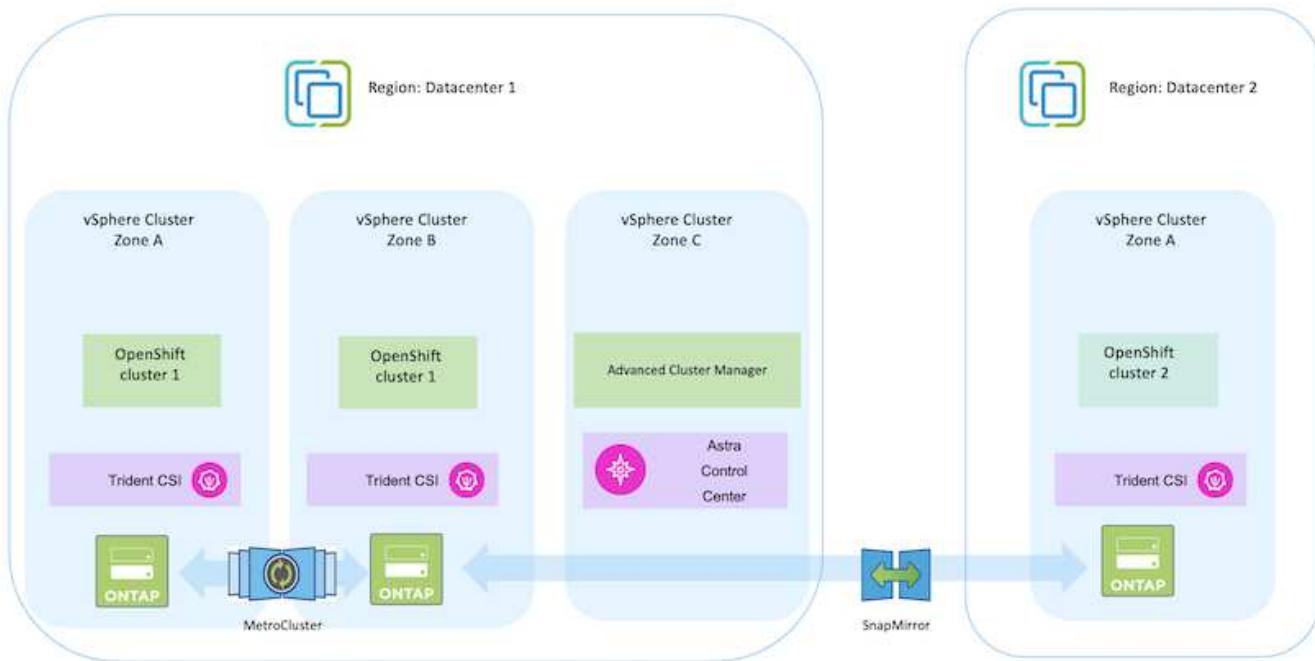
NetApp ONTAP 存储可为容器部署提供数据保护、可靠性和灵活性。Asta三端存储作为动态存储配置程序、用

于为客户的有状态应用程序使用永久性ONTAP 存储。Astra Control Center可用于编排有状态应用程序的许多数据管理要求、例如数据保护、迁移和业务连续性。

在VMware vSphere中、NetApp ONTAP 工具提供了一个vCenter插件、可用于配置数据存储库。应用标记并将其与OpenShift结合使用、以存储节点配置和数据。基于NVMe的存储可降低延迟并提高性能。

此解决方案 提供了有关使用Astra控制中心保护数据和迁移容器工作负载的详细信息。对于此解决方案、容器工作负载部署在内部环境中vSphere上的Red Hat OpenShift集群上。注意：未来、我们将为裸机上OpenShift集群上的容器工作负载提供解决方案。

使用Astra控制中心为OpenShift容器工作负载提供数据保护和迁移解决方案



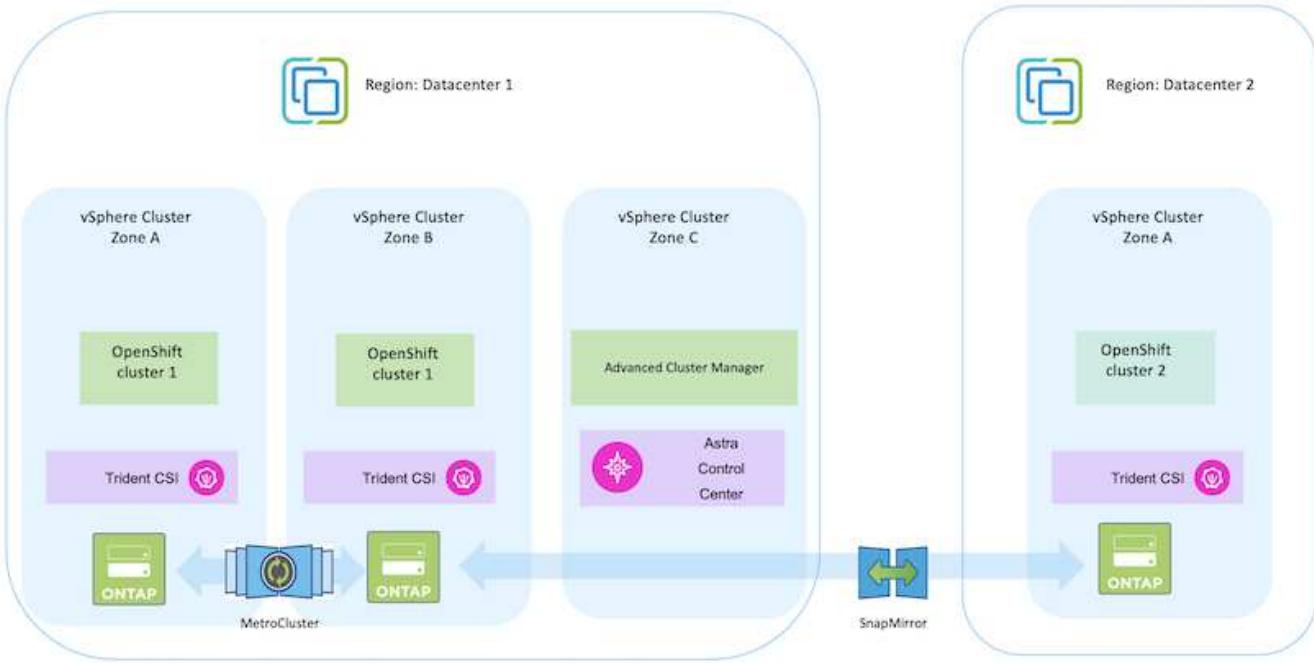
在VMware上部署和配置Red Hat OpenShift容器平台

本节将简要介绍如何设置和管理OpenShift集群以及管理其中有状态应用程序的工作流。其中展示了如何在Asta三端存储的帮助下使用NetApp ONTAP 存储阵列来提供永久性卷。本节详细介绍了如何使用Astra Control Center为有状态应用程序执行数据保护和迁移活动。



部署Red Hat OpenShift容器平台集群的方法有多种。此高级设置问题描述 提供了所用特定方法的文档链接。您可以在中提供的相关链接中参考其他方法 "[资源部分](#)"。

下图展示了在数据中心内VMware上部署的集群。



设置过程可细分为以下步骤：

部署和配置CentOS VM

- 它部署在VMware vSphere环境中。
- 此VM用于部署某些组件、例如NetApp Asta三端磁盘和适用于解决方案 的NetApp Asta控制中心。
- 在安装期间、会在此虚拟机上配置一个root用户。

在VMware vSphere上部署和配置OpenShift容器平台集群(集线器集群)

请参见的说明 "辅助部署" 部署OCP集群的方法。

💡 请记住以下内容：-创建ssh公共密钥和专用密钥以提供给安装程序。如果需要、这些密钥将用于登录到主节点和工作节点。-从辅助安装程序下载安装程序。此程序用于启动您在VMware vSphere环境中为主节点和工作节点创建的VM。-虚拟机应满足最低CPU、内存和硬盘要求。(请参阅上的vm create命令 "[这](#)" 提供此信息的主节点和工作节点的页面)—应在所有VM上启用diskUUID。-至少为主节点创建3个节点、为工作节点创建3个节点。-安装程序发现它们后、打开VMware vSphere集成切换按钮。

在集线器集群上安装高级集群管理

可使用集线器集群上的高级集群管理操作员进行安装。请参阅说明 "[此处](#)"。

在集线器集群上安装内部**Red Hat Quay**注册表。

- 要推送Asta映像、需要使用内部注册表。在集线器集群中使用Operator安装Quay内部注册表。
- 请参阅说明 "[此处](#)"。

安装两个额外的**OCP**集群(源和目标)

- 可以使用集线器集群上的ACM部署其他集群。
- 请参阅说明 "[此处](#)"。

配置**NetApp ONTAP**存储

- 在VMware环境中安装可连接到OCP VM的ONTAP 集群。
- 创建SVM。
- 配置NAS数据If以访问SVM中的存储。

在**OCP**集群上安装**NetApp Trident**

- 在集线器、源和目标集群这三个集群上安装NetApp三项功能
- 请参阅说明 "[此处](#)"。
- 为ONTAP—NAS创建存储后端。
- 为ONTAP NAS创建存储类。
- 请参阅说明 "[此处](#)"。

安装**NetApp Asta Control Center**

- NetApp Asta Control Center可使用集线器集群上的Asta Operator进行安装。
- 请参阅说明 "[此处](#)"。

请记住：*从支持站点下载NetApp Asta Control Center映像。 *将图像推送到内部注册表。 *请参阅此处的说明。

在源集群上部署应用程序

使用OpenShift GitOps部署应用程序。(例如Postgres, Ghost)

将源集群和目标集群添加到Astra控制中心。

将集群添加到Astra Control管理后、您可以在集群上安装应用程序(Astra Control之外)、然后转到Astra Control中的“应用程序”页面定义应用程序及其资源。请参见 [“开始管理Astra Control Center的应用程序部分”](#)。

下一步是使用Astra Control Center进行数据保护、并将数据从源集群迁移到目标集群。

使用Astra保护数据

此页面显示了使用Astra Control Center (ACC)在VMware vSphere上运行的基于Red Hat OpenShift容器的应用程序的数据保护选项。

随着用户利用Red Hat OpenShift对其应用程序进行现代化改造、应制定数据保护策略、以防止意外删除或任何其他人为错误。出于监管或合规目的、通常还需要制定保护策略来保护数据免受灾难的影响。

数据保护的要求各不相同、从还原到时间点副本、到自动故障转移到其他故障域、无需任何人为干预。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、高性能和高容量产品、适用于多站点位置的复制和缓存、以及安全性和灵活性。

ONTAP 中的数据保护可通过临时或策略控制的方式实现-快照-备份和恢复

Snapshot副本和备份均可保护以下类型的数据：-表示应用程序状态的应用程序元数据-与应用程序关联的任何永久性数据卷-属于应用程序的任何资源项目

使用ACC创建Snapshot

可以使用Snapshot和ACC捕获数据的时间点副本。保护策略用于定义要保留的Snapshot副本数。可用的最小计划选项为每小时。与计划内Snapshot副本相比、可以随时创建按需手动Snapshot副本、创建时间间隔也更短。Snapshot副本存储在与应用程序相同的已配置卷上。

使用ACC配置Snapshot

The screenshot shows the ACC interface with the 'ghost' application selected. The main area displays the 'APPLICATION STATUS' and 'APPLICATION PROTECTION' sections. Under 'APPLICATION PROTECTION', there is a table listing four replication schedules:

Name	Status	Last state	On Schedule / On-Demand	Created
replication-schedule-weekly-living	healthy	healthy	On Schedule	2023/06/20 14:54 (UTC)
ghost-snapshot-20230620T1100Z	healthy	healthy	On Schedule	2023/06/20 11:00 (UTC)
ghost-snapshot-20230620T1100Z	healthy	healthy	On Schedule	2023/06/20 11:00 (UTC)
ghost-snapshot-20230620T1100Z	healthy	healthy	On Demand	2023/06/20 14:54 (UTC)

使用ACC进行备份和恢复

备份基于Snapshot。ACC可以使用CSI创建Snapshot副本、并使用时间点Snapshot副本执行备份。备份存储在外部对象存储中(任何兼容S3、包括位于不同位置的ONTAP S3)。可以为计划的备份和要保留的备份版本数配置

保护策略。最小RPO为1小时。

使用**ACC**从备份还原应用程序

ACC从存储备份的S3存储分段还原应用程序。

The screenshot shows the Astra Control dashboard with the 'ghost' application selected. The top navigation bar includes 'Dashboard', 'Applications', 'Clusters', 'Cloud instances', 'Metrics', 'Metrics', 'Metrics', and 'Imports'. The main area displays the 'ghost' application's status as 'healthy' and its protection settings. It shows 'Auto-protected' and 'Retention policy configured' with a '3 days' duration. Below this, there are tabs for 'Data protection', 'Storage', 'Resource', 'Execution hooks', 'Activity', and 'Tasks'. Under 'Data protection', a table lists a single entry: 'ghost' with a status of 'healthy', a 'Last backup' timestamp of '2023-06-20T15:00 UTC', and a note indicating it is a 'Redis application' with 'Online backup' enabled.

特定于应用程序的执行挂钩

此外、还可以将执行挂钩配置为与托管应用程序的数据保护操作结合运行。尽管提供了存储阵列级别的数据保护功能、但通常还需要执行额外的步骤才能使备份和还原保持应用程序一致。应用程序专用的其他步骤可能包括：
-创建Snapshot副本之前或之后。-创建备份之前或之后。-从Snapshot副本或备份还原之后。

Astra Control可以执行这些应用程序专用步骤、这些步骤编码为称为执行挂钩的自定义脚本。

"[NetApp Verda GitHub项目](#)" 为常见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、强大且易于编排。如果您有足够的信息来支持存储库中没有的应用程序、请随时为该项目做出贡献。

为**Redis**应用程序创建**Snapshot**前创建副本的示例执行挂钩。

HOOK DETAILS

Operation: Pre-snapshot

Hook arguments (optional): pre

Hook name: redis-pre-snapshot

CONTAINER IMAGES

Container image names to match: redis

SCRIPT

- + Add
- Name: mariadb_mysql.sh
- Name: postgresql.sh
- Name: redis_hook.sh (selected)

Cancel Save ✓

使用ACC复制

为了实现区域保护或实现低RPO和RTO解决方案，可以将应用程序复制到在其他站点(最好是在其他区域)运行的另一个Kubornetes实例。ACC利用ONTAP async SnapMirror并将RPO低至5分钟。复制操作是通过复制到ONTAP来完成的、然后进行故障转移会在目标集群中创建Kubernetes资源。

i 请注意、复制与备份和还原不同、在备份和还原中、备份将转到S3并从S3执行还原。请访问以下链接：[https://docs.netapp.com/us-en/astra-control-center/concepts/data-protection.html#replication-to-a-remote-cluster\[here\]](https://docs.netapp.com/us-en/astra-control-center/concepts/data-protection.html#replication-to-a-remote-cluster[here])、了解有关这两种类型的数据保护之间差异的更多详细信息。

请参见 "[此处](#)" 有关SnapMirror设置说明、请参见。

采用ACC的SnapMirror



SAN经济型和NAS经济型存储驱动程序不支持复制功能。请参见 "[此处](#)" 了解更多详细信息。

演示视频：

["使用Astra Control Center进行灾难恢复的演示视频"](#)

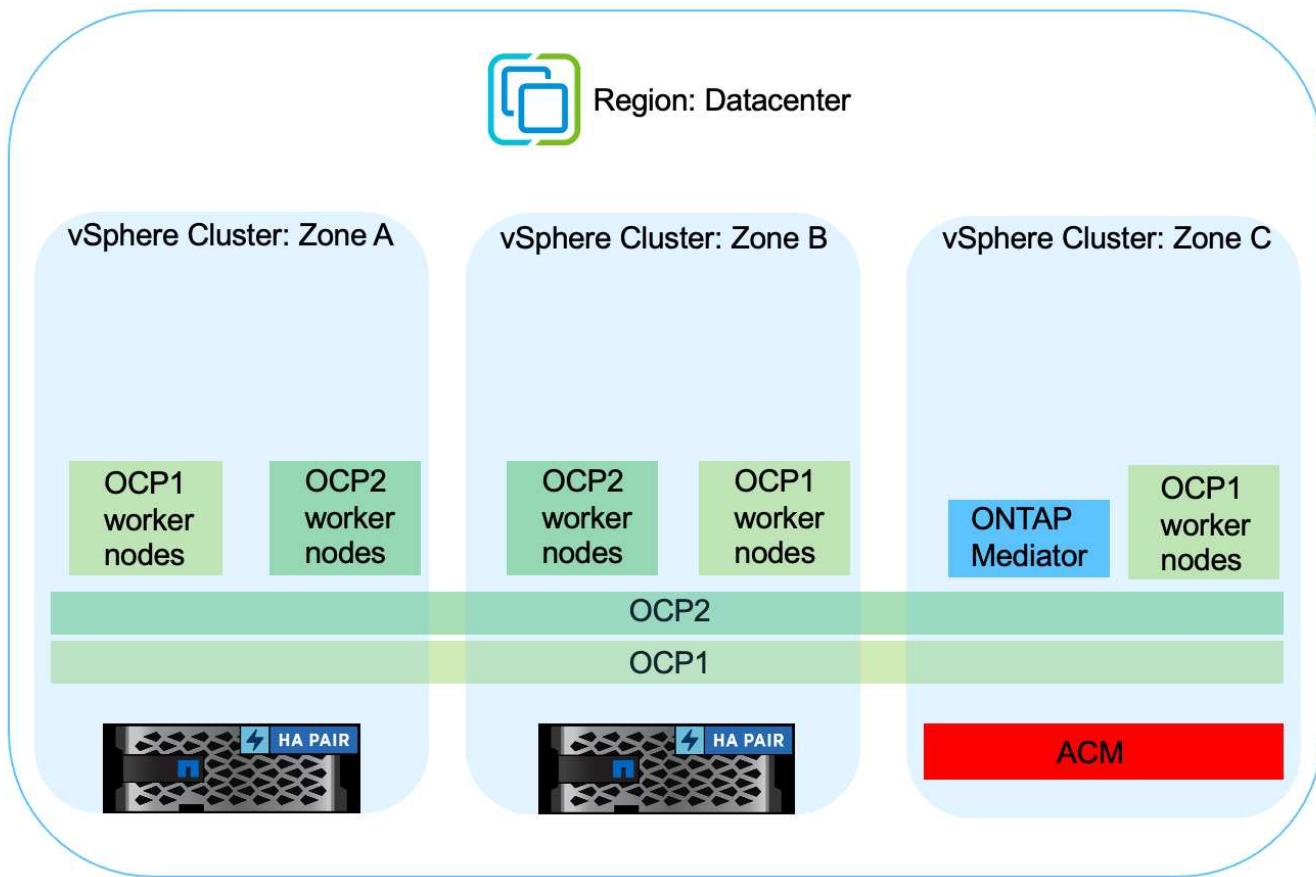
[使用Astra Control Center保护数据](#)

借助**MetroCluster** 实现业务连续性

我们大多数适用于ONTAP 的硬件平台都具有高可用性功能、可防止设备发生故障、从而避免执行灾难恢复。但是、为了防止火灾或任何其他灾难、并在零RPO和低RTO的情况下继续开展业务、通常会使用MetroCluster 解决方案。

当前拥有ONTAP 系统的客户可以通过在距离限制范围内添加受支持的ONTAP 系统来扩展到MetroCluster 、从而提供区域级灾难恢复。Astra三端存储接口(CSI、容器存储接口)支持NetApp ONTAP 、包括MetroCluster 配置以及Cloud Volumes ONTAP 、Azure NetApp Files 、AWS FSx for NetApp ONTAP 等其他选项 Astra三端存储为ONTAP 提供了五个存储驱动程序选项、所有这些选项均支持MetroCluster 配置。请参见 "[此处](#)" 有关Astra三端存储驱动程序支持的ONTAP 存储驱动程序的更多详细信息。

MetroCluster 解决方案 需要第2层网络扩展或功能才能从两个容错域访问相同的网络地址。 MetroCluster 配置到位后、解决方案 对应用程序所有者是透明的、因为MetroCluster SVM中的所有卷都受到保护、并可获得SyncMirror 的优势(零RPO)。



对于三元数据后端配置(TBC)、在使用MetroCluster 配置时、请勿指定dataLIF和SVM。为管理LIF指定SVM管理IP并使用vsadmin角色凭据。

有关Astra Control Center数据保护功能的详细信息、请参见 "[此处](#)"

使用Astra Control Center迁移数据

此页面显示了使用Astra Control Center (ACC)的Red Hat OpenShift集群上容器工作负载的数据迁移选项。

通常需要在不同环境之间移动Kubernetes应用程序。要迁移应用程序及其永久性数据、可以使用NetApp ACC。

在不同的Kubernetes环境之间迁移数据

ACC支持各种Kubernetes类型、包括Google Anthos、Red Hat OpenShift、Tanzu Kubernetes Grid、Grancher Kubernetes Engine、Upstream Kubernetes、等等 有关更多详细信息、请参见 "[此处](#)"。

要将应用程序从一个集群迁移到另一个集群、您可以使用ACC的以下功能之一：

- 复制
- 备份和恢复
- 克隆

请参见 "[数据保护部分](#)" 用于复制、备份和恢复选项。

请参见 "[此处](#)" 有关克隆的更多详细信息。



只有通过三元容器存储接口(CSI)才能使用Astra复制功能。但是、NAS经济型和SAN经济型驱动程序不支持复制。

使用ACC执行数据复制

适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案

概述

NetApp发现、越来越多的客户正在利用围绕Kubernetes构建的容器和流程编排平台来打造现代化的传统企业级应用程序以及构建新应用程序。Red Hat OpenShift容器平台就是我们看到许多客户采用的一个示例。

随着越来越多的客户开始在企业中采用容器、NetApp已做好充分准备、可以满足有状态应用程序的持久存储需求以及数据保护、数据安全和数据迁移等传统数据管理需求。但是、可以使用不同的策略、工具和方法来满足这些需求。

**NetApp ONTAP 基于下面列出的存储选项，可为容器和部署提供安全性、数据保护、可靠性和灵活性。

- 内部环境中的自行管理存储：
 - NetApp光纤连接存储(FAS)、NetApp全闪存FAS阵列(AFF)、NetApp全SAN阵列(ASA)和ONTAP Select
- 内部部署中由提供商管理的存储：
 - NetApp Keystone 提供存储即服务(STaaS)
- 云中的自行管理存储：

- NetApp Cloud Volumes ONTAP (CVO)可在超大容量云中提供自行管理的存储
- 云中由提供商管理的存储：
 - Cloud Volumes Service for Google Cloud (CVS)、 Azure NetApp Files (ANF)、 Amazon FSx for NetApp ONTAP 可在超云中提供完全托管的存储



ONTAP feature highlights

Storage Administration	Performance & Scalability
<ul style="list-style-type: none"> • Multi-tenancy • FlexVol & FlexGroup • LUN • Quotas 	<ul style="list-style-type: none"> • ONTAP CLI & API • System Manager & BlueXP
Availability & Resilience	Access Protocols
<ul style="list-style-type: none"> • Multi-AZ HA deployment (MetroCluster) • SnapShot & SnapRestore • SnapMirror 	<ul style="list-style-type: none"> • SnapMirror Business Continuity • SnapMirror Cloud
Storage Efficiency	Security & Compliance
<ul style="list-style-type: none"> • Deduplication & Compression • Compaction 	<ul style="list-style-type: none"> • Thin provisioning • Data Tiering (Fabric Pool)
	<ul style="list-style-type: none"> • iSCSI • Multi-protocol access
	<ul style="list-style-type: none"> • Fpolicy & Vscan • Active Directory integration
	<ul style="list-style-type: none"> • LDAP & Kerberos • Certificate based authentication

NetApp BlueXP使您能够从一个控制平台/接口管理所有存储和数据资产。

您可以使用BlueXP创建和管理云存储(例如Cloud Volumes ONTAP 和Azure NetApp Files)、移动、保护和分析数据以及控制许多内部和边缘存储设备。

NetApp Asta Trident是一款符合CSI的存储编排程序，支持快速、轻松地使用由上述各种NetApp存储选项提供支持的永久性存储。它是由NetApp维护和支持的开源软件。

Astra Trident CSI feature highlights



CSI specific <ul style="list-style-type: none">CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copiesCSI topologyVolume expansion	Security <ul style="list-style-type: none">Dynamic-export policy managementiSCSI initiator-groups dynamic managementiSCSI bidirectional CHAP
Control <ul style="list-style-type: none">Storage and performance consumptionMonitoringVolume ImportCross Namespace Volume Access	Installation methods <ul style="list-style-type: none">BinaryHelm chartOperatorGitOps
Choose your access mode <ul style="list-style-type: none">RWO (ReadWriteOnce, i.e 1↔1)RWX (ReadWriteMany, i.e 1↔n)ROX (ReadOnlyMany)RWOP (ReadWriteOnce POD)	Choose your protocol <ul style="list-style-type: none">NFSSMBiSCSI

业务关键型容器工作负载所需的不仅仅是永久性卷。他们的数据管理要求也需要保护和迁移应用程序Kubernetes对象。



除了用户数据之外、应用程序数据还包括Kubernetes对象：以下是一些示例： - Kubernetes对象、例如Pod规格、PVC、部署、服务-自定义配置对象、例如配置映射和密钥-持久数据、例如Snapshot副本、备份、克隆-自定义资源、例如CRS和CRD

NetApp Astra Control作为完全托管和自我管理软件提供，可提供流程编排，实现强大的应用程序数据管理。请参见 "[Astra 文档](#)" 有关Astra系列产品的更多详细信息。

本参考文档使用NetApp Astra Control Center验证了在Red Hat OpenShift容器平台上部署的基于容器的应用程序的迁移和保护。此外、解决方案还提供了有关部署和使用Red Hat高级集群管理(ACM)来管理容器平台的详细信息。本文档还重点介绍了使用Astra Trident CSI配置程序将NetApp存储与Red Hat OpenShift容器平台集成的详细信息。Astra Control Center部署在集线器集群上、用于管理容器应用程序及其永久性存储生命周期。最后、它还提供了一个解决方案、用于在AWS (ROSA)中使用Amazon FSx for NetApp ONTAP (FSxN)作为永久性存储的受管Red Hat OpenShift集群上对容器工作负载进行复制、故障转移和故障恢复。

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

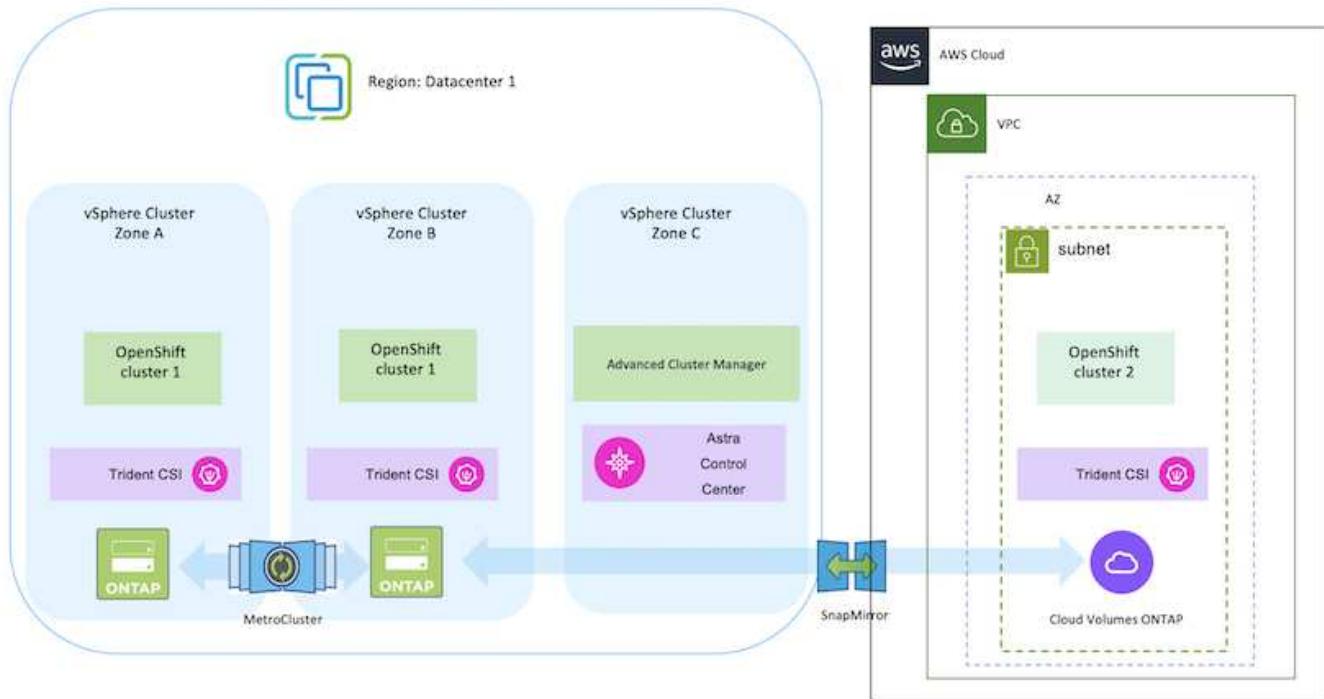
当客户准备将部分选定工作负载或所有工作负载从其数据中心迁移到云时、他们可能正处于现代化之旅的一个阶段。出于各种原因、他们可能会选择在云中使用自行管理的OpenShift容器和自行管理的NetApp存储。他们应在云中规划和部署Red Hat OpenShift容器平台(OCP)、以便打造一个成功的生产就绪环境、从而从数据中心迁移容器工作负载。他们的OCP集群可以部署在数据中心的VMware或裸机上、也可以部署在云环境中的AWS、Azure或Google Cloud上。

NetApp Cloud Volumes ONTAP 存储可为AWS、Azure和Google Cloud中的容器部署提供数据保护、可靠性和灵活性。Astra三端存储作为动态存储配置程序、用于为客户的有状态应用程序使用永久性Cloud Volumes ONTAP 存储。Astra Control Center可用于编排有状态应用程序的许多数据管理要求、例如数据保护、迁移和业

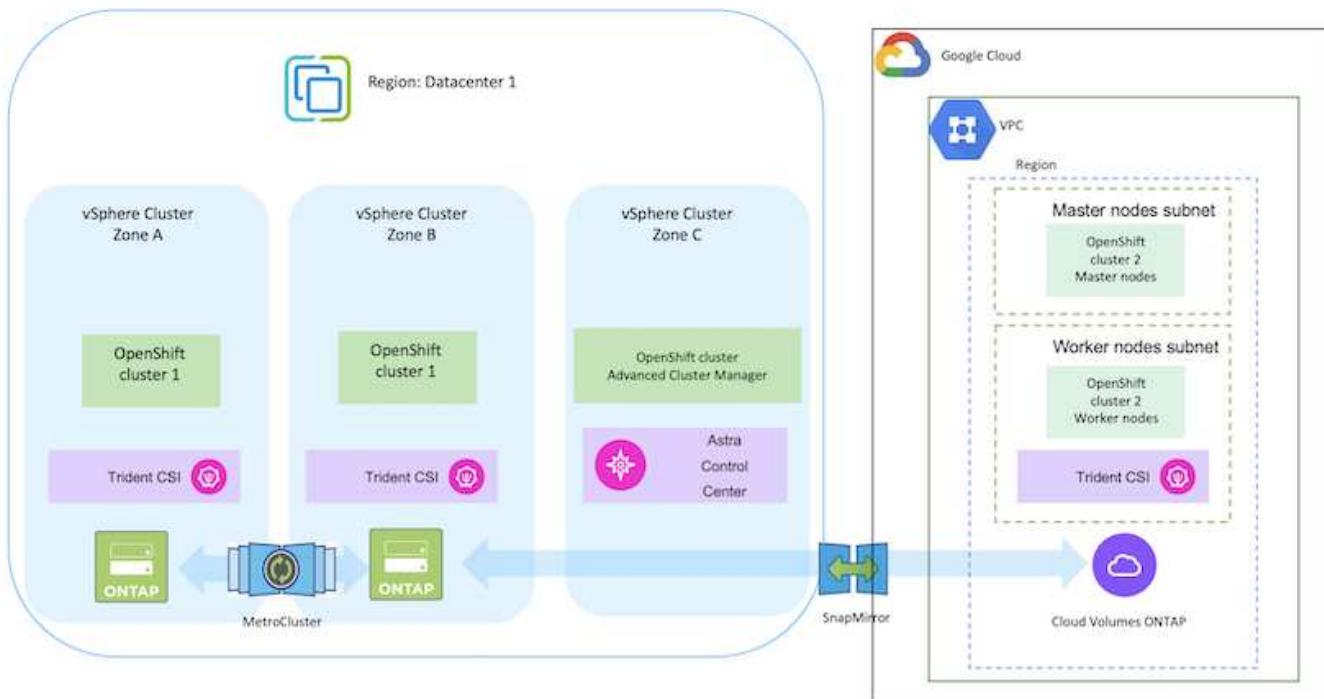
务连续性。

使用**Astra**控制中心在混合云中为**OpenShift**容器工作负载提供数据保护和迁移解决方案

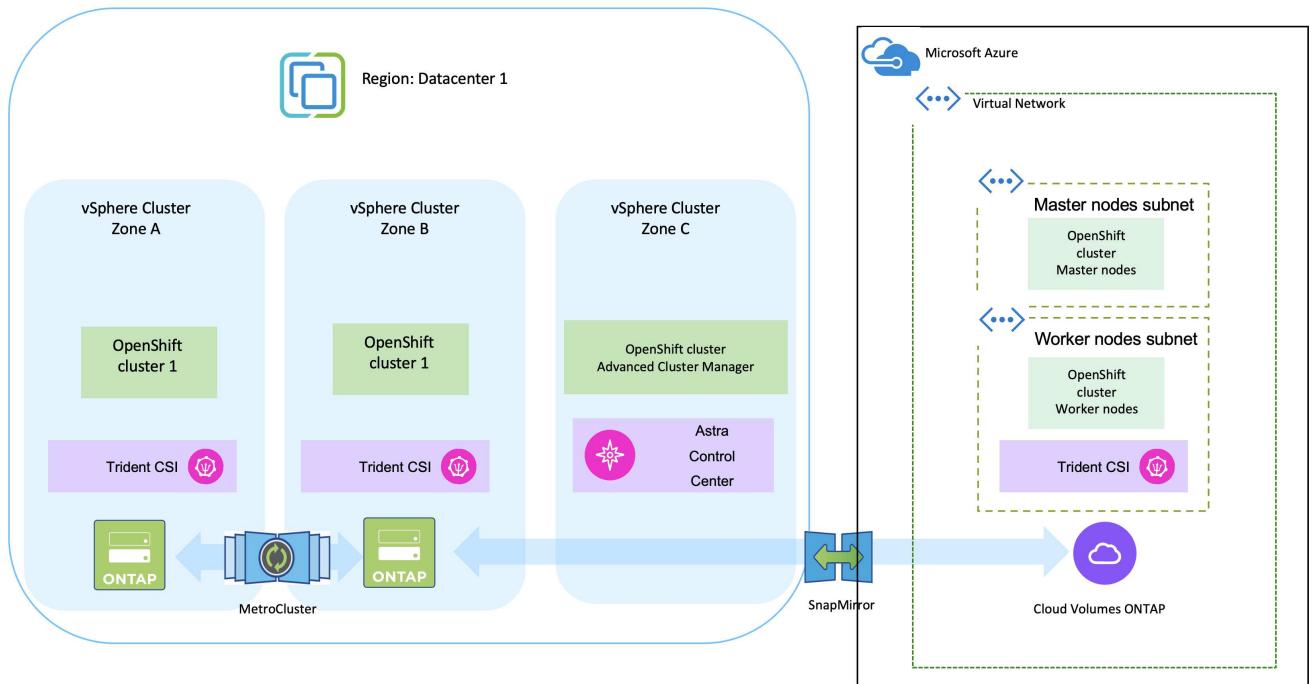
内部部署和AWS



内部部署和Google Cloud



内部部署和Azure Cloud



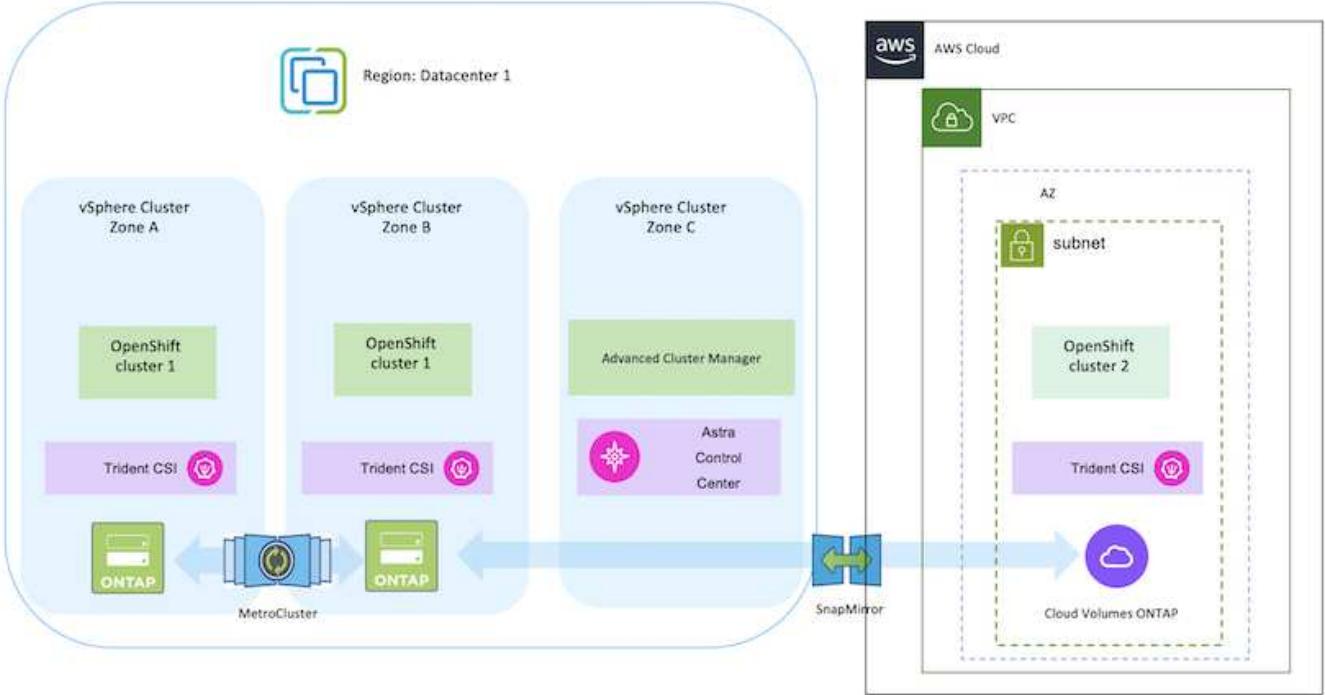
在AWS上部署和配置Red Hat OpenShift容器平台

本节简要介绍了如何在AWS中设置和管理OpenShift集群以及在这些集群上部署有状态应用程序的工作流。其中展示了如何利用NetApp Cloud Volumes ONTAP存储在Asta三端存储的帮助下提供永久性卷。本节详细介绍了如何使用Astra Control Center为有状态应用程序执行数据保护和迁移活动。



可以通过多种方法在AWS上部署Red Hat OpenShift容器平台集群。此高级设置问题描述 提供了所用特定方法的文档链接。您可以在中提供的相关链接中参考其他方法 "[资源部分](#)"。

下图展示了在AWS上部署并使用VPN连接到数据中心的集群。



设置过程可细分为以下步骤：

通过高级集群管理在**AWS**上安装**OCP**集群。

- 创建具有站点到站点VPN连接的VPC (使用pfSense)以连接到内部网络。
- 内部网络具有Internet连接。
- 在3个不同的AZs中创建3个专用子网。
- 为VPC创建Route 53专用托管区域和DNS解析程序。

使用高级集群管理(ACM)向导在AWS上创建OpenShift集群。请参阅说明 "[此处](#)"。

- i** 您也可以从OpenShift混合云控制台在AWS中创建集群。请参见 "[此处](#)" 有关说明，请参见。
- i** 使用ACM创建集群时、您可以在表单视图中填写详细信息后编辑YAML文件、从而自定义安装。创建集群后、您可以通过ssh登录到集群节点、以便进行故障排除或其他手动配置。使用您在安装期间提供的ssh密钥和username core进行登录。

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

- 在内部VMware环境中安装连接器。请参阅说明 "[此处](#)"。
- 使用连接器在AWS中部署CVO实例。请参阅说明 "[此处](#)"。

- i** 该连接器也可以安装在云环境中。请参见 "[此处](#)" 适用于追加信息。

在OCP集群中安装Asta Trident

- 使用Helm部署三级联操作员。请参阅说明 "[此处](#)"
- 创建后端和存储类。请参阅说明 "[此处](#)"。

将AWS上的OCP集群添加到Astra Control Center。

将AWS中的OCP集群添加到Astra Control Center。

对多区域架构使用三元数据的CSI拓扑功能

如今、云提供商支持Kubernetes/OpenShift集群管理员生成基于分区的集群节点。节点可以位于一个区域内的不同可用性区域中，也可以位于不同区域之间。为了便于在多区域架构中为工作负载配置卷，Astra Trident 使用了CSI拓扑。使用CSI拓扑功能，可以根据区域和可用性区域将对卷的访问限制为一小部分节点。请参见 "[此处](#)" 了解更多详细信息。

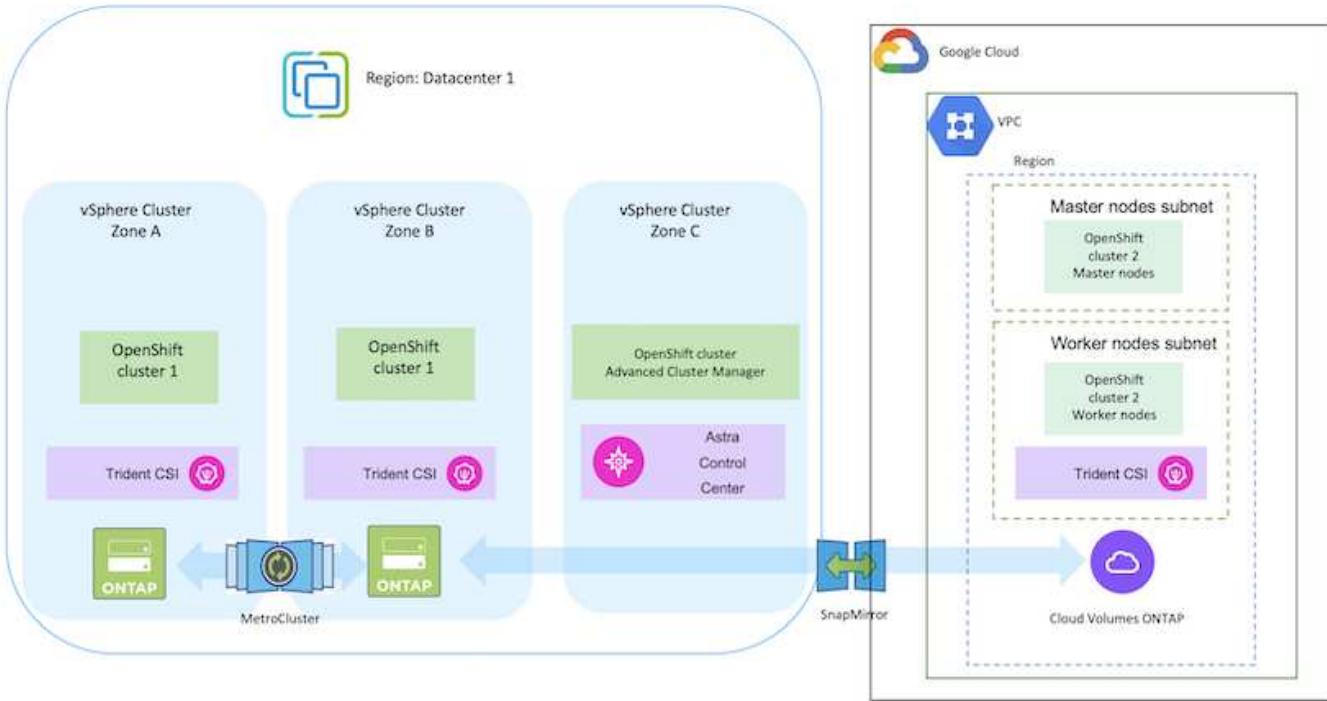
 Kubernetes支持两种卷绑定模式：-将 **VolumeBindingMode** 设置为 **_Immediate**(默认)时、Astra Trident会在没有任何拓扑感知功能的情况下创建卷。创建永久性卷时，不会依赖于请求的 Pod 的计划要求。-当 **VolumeBindingMode** 设置为 **_WaitForFirstConsumer**时，为PVC创建和绑定永久性卷的操作会延迟，直到计划和创建使用PVC的Pod为止。这样，卷就会根据拓扑要求强制实施的计划限制来创建。Astra三叉设计存储后端可以根据可用性区域选择性地配置卷(拓扑感知型后端)。对于使用此后端的 StorageClasses，只有在受支持区域 / 区域中计划的应用程序请求时，才会创建卷。(拓扑感知型存储类)请参见 "[此处](#)" 了解更多详细信息。

在GCP上部署和配置Red Hat OpenShift容器平台

在GCP上部署和配置Red Hat OpenShift容器平台

本节简要介绍了如何在GCP中设置和管理OpenShift集群以及在这些集群上部署有状态应用程序的工作流。其中展示了如何利用NetApp Cloud Volumes ONTAP 存储在Astra三端存储的帮助下提供永久性卷。本节详细介绍了如何使用Astra Control Center为有状态应用程序执行数据保护和迁移活动。

下图显示了部署在GCP上并使用VPN连接到数据中心的集群。



可以通过多种方法在GCP中部署Red Hat OpenShift容器平台集群。此高级设置问题描述 提供了所用特定方法的文档链接。您可以在中提供的相关链接中参考其他方法 "[资源部分](#)"。

设置过程可细分为以下步骤：

使用命令行界面在**GCP**上安装**OCP**集群。

- 确保您已满足上述所有前提条件 "[此处](#)"。
- 对于内部和GCP之间的VPN连接、我们会创建并配置一个pfSense VM。有关说明，请参见 "[此处](#)"。
 - 只有在Google Cloud Platform中创建VPN网关后、才能在pfSense中配置远程网关地址。
 - 只有在OpenShift集群安装程序运行并为集群创建基础架构组件之后、才能配置阶段2的远程网络IP地址。
 - 只有在安装程序为集群创建基础架构组件后、才能在Google Cloud中配置VPN。
- 现在、在GCP上安装OpenShift集群。
 - 获取安装程序和拉取密钥、然后按照文档中提供的步骤部署集群 "[此处](#)"。
 - 此安装将在Google Cloud Platform中创建VPC网络。它还会在云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地址在内部环境的DNS中添加A记录。
 - 集群安装完成、并将提供一个kubeconfigfile文件以及用户名和密码以登录到集群的控制台。

使用BlueXP在GCP中部署Cloud Volumes ONTAP。

- 在Google Cloud中安装连接器。请参阅说明 "[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的OCP集群中安装Asta Trident

- 有多种方法可用于部署Asta三端到子、如图所示 "[此处](#)"。
- 对于此项目、Asta Dent是按照说明手动部署Asta Dent Operator来安装的 "[此处](#)"。
- 创建后端和存储类。请参阅说明 "[此处](#)"。

将GCP上的OCP集群添加到Astra Control Center。

- 创建一个具有集群角色的单独KubeConfig文件、该角色包含由Astra Control管理集群所需的最低权限。可以找到相关说明 "[此处](#)"。
- 按照说明将集群添加到Astra Control Center "[此处](#)"

对多区域架构使用三元数据的CSI拓扑功能

如今、云提供商支持Kubernetes/OpenShift集群管理员生成基于分区的集群节点。节点可以位于一个区域内的不同可用性区域中，也可以位于不同区域之间。为了便于在多区域架构中为工作负载配置卷，Astra Trident 使用了 CSI 拓扑。使用 CSI 拓扑功能，可以根据区域和可用性区域将对卷的访问限制为一小部分节点。请参见 "[此处](#)" 了解更多详细信息。

Kubernetes支持两种卷绑定模式：-将*VolumeBindingMode* 设置为 *_Immediate*(默认)时、Astra Trident会在没有任何拓扑感知功能的情况下创建卷。创建永久性卷时，不会依赖于请求的 Pod 的计划要求。-当*VolumeBindingMode* 设置为 *_WaitForFirstConsumer*时，为PVC创建和绑定永久性卷的操作会延迟，直到计划和创建使用PVC的Pod为止。这样，卷就会根据拓扑要求强制实施的计划限制来创建。Astra三叉设计存储后端可以根据可用性区域选择性地配置卷(拓扑感知型后端)。对于使用此后端的 StorageClasses，只有在受支持区域 / 区域中计划的应用程序请求时，才会创建卷。(拓扑感知型存储类)请参见 "[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Astra Control Center

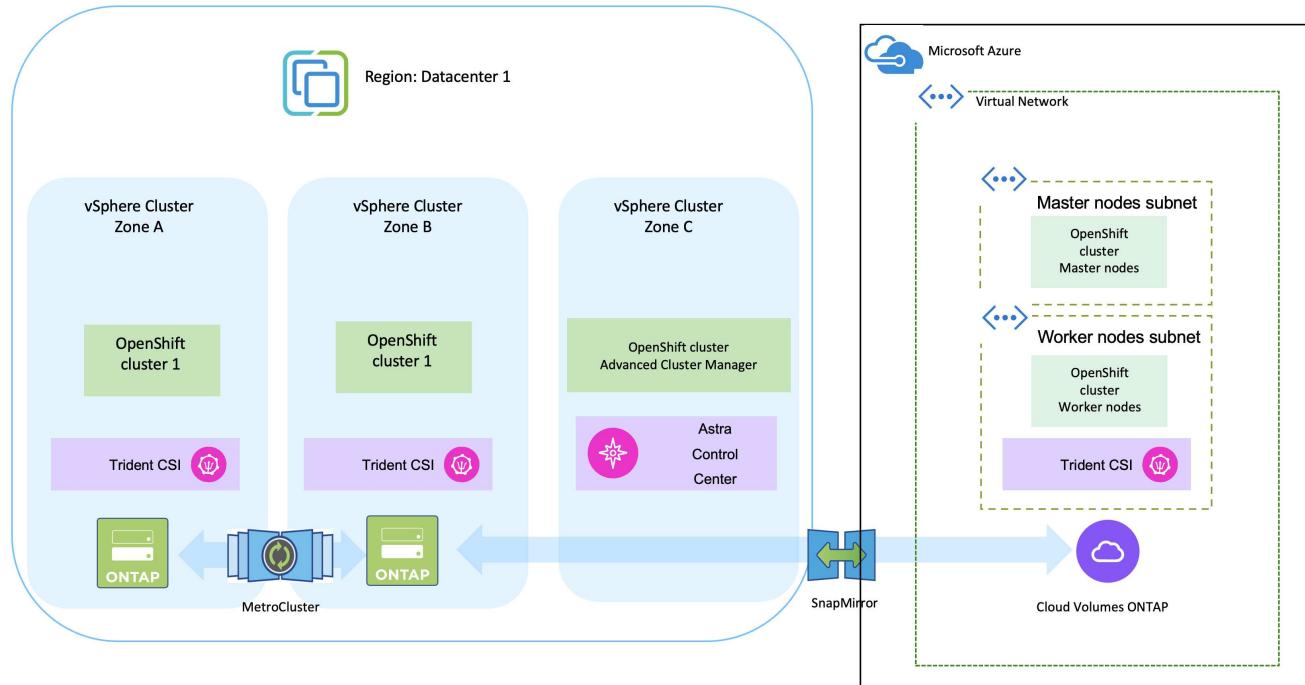
在Azure上部署和配置Red Hat OpenShift容器平台

在Azure上部署和配置Red Hat OpenShift容器平台

本节简要介绍了如何在Azure中设置和管理OpenShift集群并在其上部署有状态应用程序的工作流。它展示了如何借助Asta三端磁盘/Asta控件配置程序使用NetApp Cloud Volumes

ONTAP存储来提供永久性卷。本节详细介绍了如何使用Astra Control Center为有状态应用程序执行数据保护和迁移活动。

下图显示了部署在Azure上并使用VPN连接到数据中心的集群。



可以通过多种方法在Azure中部署Red Hat OpenShift容器平台集群。此高级设置问题描述 提供了所用特定方法的文档链接。您可以在中提供的相关链接中参考其他方法 "[资源部分](#)"。

设置过程可细分为以下步骤：

使用命令行界面在Azure上安装OCP集群。

- 确保您已满足上述所有前提条件 "[此处](#)"。
- 创建VPN、子网和网络安全组以及专用DNS区域。创建VPN网关和站点间VPN连接。
- 对于内部环境与Azure之间的VPN连接、我们会创建并配置一个pfSense VM。有关说明，请参见 "[此处](#)"。
- 获取安装程序和拉取密钥、然后按照文档中提供的步骤部署集群 "[此处](#)"。
- 集群安装完成、并将提供一个kubeconfigfile文件以及用户名和密码以登录到集群的控制台。

下面提供了一个示例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中的中安装连接器。请参阅说明 "[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](#)]。

在Azure的OCP集群中安装A作用 力控制配置程序

- 对于此项目、所有集群(即、部署了Astra Control Center的集群、Azure中的集群)上都安装了Astra Control置管程序(ACP)。了解有关Astra Control配置程序的更多信息 "[此处](#)"。
- 创建后端和存储类。请参阅说明 "[此处](#)"。

将Azure上的OCP集群添加到Astra控制中心。

- 创建一个具有集群角色的单独KubeConfig文件、该角色包含由Astra Control管理集群所需的最低权限。可以找到相关说明["此处"](#)。
- 按照说明将集群添加到Astra Control Center
["此处"](#)

对多区域架构使用三元数据的CSI拓扑功能

如今、云提供商支持Kubernetes/OpenShift集群管理员生成基于分区的集群节点。节点可以位于一个区域内的不同可用性区域中，也可以位于不同区域之间。为了便于在多区域架构中为工作负载配置卷，Astra Trident 使用了 CSI 拓扑。使用 CSI 拓扑功能，可以根据区域和可用性区域将对卷的访问限制为一小部分节点。请参见["此处"](#) 了解更多详细信息。

Kubernetes支持两种卷绑定模式：-将 **VolumeBindingMode** 设置为 **_Immediate**(默认)时、Astra Trident会在没有任何拓扑感知功能的情况下创建卷。创建永久性卷时，不会依赖于请求的 Pod 的计划要求。-当 **VolumeBindingMode** 设置为 **_WaitForFirstConsumer**时，为PVC创建和绑定永久性卷的操作会延迟，直到计划和创建使用PVC的Pod为止。这样，卷就会根据拓扑要求强制实施的计划限制来创建。Astra三叉设计存储后端可以根据可用性区域选择性地配置卷(拓扑感知型后端)。对于使用此后端的 StorageClasses，只有在受支持区域 / 区域中计划的应用程序请求时，才会创建卷。(拓扑感知型存储类)请参见["此处"](#) 了解更多详细信息。

演示视频

[使用Astra Control对应用程序进行故障转移和故障恢复](#)

使用Astra Control Center保护数据

此页面显示了在VMware vSphere上运行的基于Red Hat OpenShift容器的应用程序的数据保护选项、或者使用Astra Control Center (ACC)在云中运行的应用程序。

随着用户利用Red Hat OpenShift对其应用程序进行现代化改造、应制定数据保护策略、以防止意外删除或任何其他人为错误。出于监管或合规目的、通常还需要制定保护策略来保护数据免受灾难的影响。

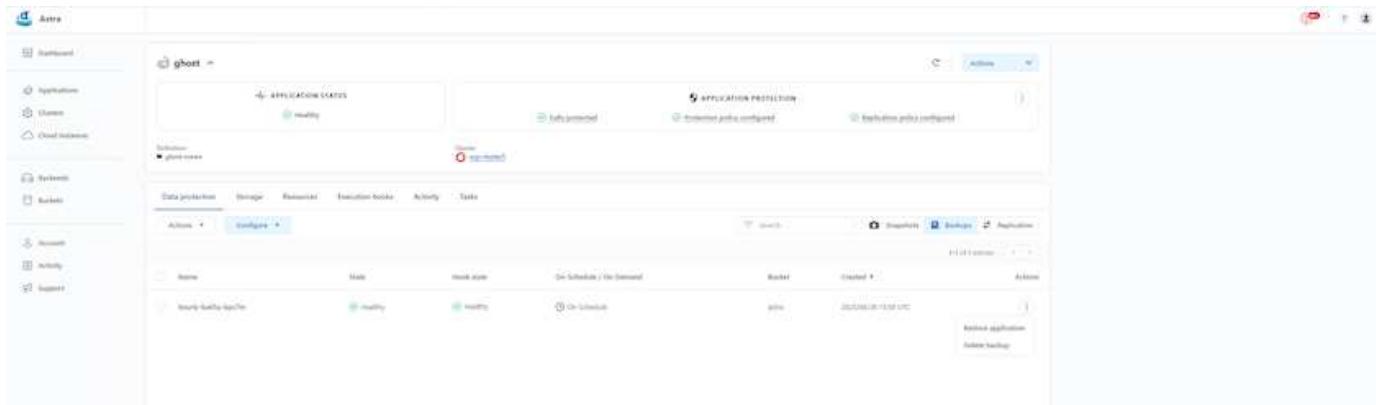
数据保护的要求各不相同、从还原到时间点副本、到自动故障转移到其他故障域、无需任何人为干预。许多客户选择ONTAP 作为其Kubernetes应用程序的首选存储平台、因为它具有丰富的功能、例如多租户、多协议、高性能和高容量产品、适用于多站点位置的复制和缓存、以及安全性和灵活性。

客户可以将云环境设置为其数据中心扩展、以便充分利用云的优势、并做好在未来移动工作负载的准备。对于这类客户而言、将其OpenShift应用程序及其数据备份到云环境是不可避免的选择。然后、他们可以将应用程序和关联数据还原到云中的OpenShift集群或数据中心。

使用ACC进行备份和恢复

应用程序所有者可以查看和更新ACC发现的应用程序。ACC可以使用CSI创建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。可以为计划的备份和要保留的备份版本数配置保护策略。最小RPO为1小时。

使用ACC从备份还原应用程序



特定于应用程序的执行挂钩

尽管可以使用存储阵列级别的数据保护功能、但通常需要执行额外的步骤才能使备份和还原应用程序保持一致。应用程序专用的其他步骤可能包括：-创建Snapshot副本之前或之后。-创建备份之前或之后。-从Snapshot副本或备份还原之后。Astra Control可以执行这些应用程序专用步骤、这些步骤编码为称为执行挂钩的自定义脚本。

NetApp的 "[开源项目Verda](#)" 为常见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、强大且易于编排。如果您有足够的信息来支持存储库中没有的应用程序、请随时为该项目做出贡献。

为Redis应用程序创建Snapshot前创建副本的示例执行挂钩。

HOOK DETAILS

Operation: Pre-snapshot

Hook arguments (optional): pre

Enter hook arguments:

Hook name: redis-pre-snapshot

CONTAINER IMAGES

Apply to all container images

Container image names to match: redis

SCRIPT

+ Add

Name
mariadb_mysql.sh
postgresql.sh
redis_hook.sh

Cancel Save ✓

EXECUTION HOOKS

Execution hooks allow Astra Control to execute your own custom scripts before or after a snapshot.

Read more in [Manage application execution hooks](#)

使用ACC复制

为了实现区域保护或实现低RPO和RTO解决方案，可以将应用程序复制到在其他站点(最好是在其他区域)运行的另一个Kubernetes实例。ACC利用ONTAP async SnapMirror并将RPO低至5分钟。请参见 "[此处](#)" 有关SnapMirror设置说明、请参见。

采用ACC的SnapMirror

The screenshot shows the Astra Control Center (ACC) interface. On the left, there's a sidebar with navigation links: Dashboard, Applications, Clusters, Cloud Instances, Backends, Buckets, Account, Activity, and Support. The main area is titled 'ghost' and displays the 'APPLICATION STATUS' and 'APPLICATION PROTECTION' sections. Under 'APPLICATION STATUS', it shows 'Healthy' for both 'Destination' (ghost-infra) and 'Cluster' (ocp-cluster). Under 'APPLICATION PROTECTION', it shows 'Fully protected' and 'Protection policy configured'. Below these sections, there are tabs for 'Data protection', 'Storage', 'Resources', 'Execution hooks', 'Activity', and 'Tasks'. A 'Configure' button is also present. On the right side, there's a 'Actions' dropdown with options like Snapshot, Back up, Clone, Restore, Fail-over, Reverse replication, and Unmanage. At the bottom, there are buttons for Snapshots, Backups, and Replication. The 'Replication relationship' section on the right shows a diagram with two nodes: 'Source' (ghost) and 'Destination' (ghost). An arrow points from Source to Destination, labeled 'Active site'. The 'STATUS' section indicates 'Established' with a green 'Healthy' icon. The 'SCHEDULE' section shows a scheduled replication task: 'Replicate snapshot every 5 minutes to ocp-cluster?'. The 'LAST SYNC' section shows the last sync occurred on '2023/04/26 19:16 UTC' with a duration of '30 seconds'.



SAN经济型和NAS经济型存储驱动程序不支持复制功能。请参见 "[此处](#)" 了解更多详细信息。

演示视频：

["使用Asta Control Center进行灾难恢复的演示视频"](#)

[使用Astra Control Center保护数据](#)

有关Astra Control Center数据保护功能的详细信息、请参见 "[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Asta Control对应用程序进行故障转移和故障恢复](#)

使用Astra Control Center迁移数据

此页面显示了使用Astra Control Center (ACC)的Red Hat OpenShift集群上容器工作负载的数据迁移选项。具体而言、客户可以使用ACC将部分选定工作负载或所有工作负载从内部数据中心迁移到云、将应用程序克隆到云中进行测试、或者从数据中心迁移到云

数据迁移

要将应用程序从一个环境迁移到另一个环境、您可以使用ACC的以下功能之一：

- 复制
- 备份和恢复
- 克隆

请参见 "数据保护部分" 用于复制、备份和恢复选项。请参见 "此处" 有关克隆的更多详细信息。



只有通过三元容器存储接口(CSI)才能使用Astra复制功能。但是、NAS经济型和SAN经济型驱动程序不支持复制。

使用ACC执行数据复制

The screenshot shows the Astra application protection interface. On the left, there's a sidebar with options like Dashboard, Applications, Clusters, Cloud Instances, Backends, Buckets, Account, Activity, and Support. The main area is titled 'ghost' and shows 'APPLICATION STATUS' with a 'Healthy' status. Below it, 'Data protection' is selected in the navigation bar, which includes tabs for Storage, Resources, Execution hooks, Activity, and Tasks. A 'Configure' button is also present. To the right, there's a 'Actions' dropdown with options like Snapshot, Back up, Clone, Restore, Fail-over, Reverse replication, and Unmanage. A 'Replication relationship' section is displayed, showing a 'Source' cluster (ghost) replicating to a 'Destination' cluster (ghost). The status is 'Established'. It shows a scheduled replication every 5 minutes to 'ghost-cluster?'. The last sync was at 2023/04/26 19:16 UTC with a duration of 30 seconds. There are also buttons for Snapshot, Backup, and Replication.

适用于Red Hat OpenShift容器工作负载的NetApp混合云解决方案

概述

NetApp发现、越来越多的客户正在利用围绕Kubernetes构建的容器和流程编排平台来打造现代化的传统企业级应用程序以及构建新应用程序。Red Hat OpenShift容器平台就是我们看到许多客户采用的一个示例。

随着越来越多的客户开始在企业中采用容器、NetApp已做好充分准备、可以满足有状态应用程序的持久存储需求以及数据保护、数据安全和数据迁移等传统数据管理需求。但是、可以使用不同的策略、工具和方法来满足这些需求。

**NetApp ONTAP 基于下面列出的存储选项，可为容器和部署提供安全性、数据保护、可靠性和灵活性。

- 内部环境中的自行管理存储：
 - NetApp光纤连接存储(FAS)、NetApp全闪存FAS阵列(AFF)、NetApp全SAN阵列(ASA)和ONTAP Select
- 内部部署中由提供商管理的存储：
 - NetApp Keystone 提供存储即服务(STaaS)
- 云中的自行管理存储：

- NetApp Cloud Volumes ONTAP (CVO)可在超大容量云中提供自行管理的存储
- 云中由提供商管理的存储：
 - Cloud Volumes Service for Google Cloud (CVS)、 Azure NetApp Files (ANF)、 Amazon FSx for NetApp ONTAP 可在超云中提供完全托管的存储



ONTAP feature highlights

Storage Administration	Performance & Scalability
<ul style="list-style-type: none"> • Multi-tenancy • FlexVol & FlexGroup • LUN • Quotas 	<ul style="list-style-type: none"> • ONTAP CLI & API • System Manager & BlueXP
Availability & Resilience	Access Protocols
<ul style="list-style-type: none"> • Multi-AZ HA deployment (MetroCluster) • SnapShot & SnapRestore • SnapMirror 	<ul style="list-style-type: none"> • SnapMirror Business Continuity • SnapMirror Cloud
Storage Efficiency	Security & Compliance
<ul style="list-style-type: none"> • Deduplication & Compression • Compaction 	<ul style="list-style-type: none"> • Thin provisioning • Data Tiering (Fabric Pool)
	<ul style="list-style-type: none"> • iSCSI • Multi-protocol access
	<ul style="list-style-type: none"> • Fpolicy & Vscan • Active Directory integration
	<ul style="list-style-type: none"> • LDAP & Kerberos • Certificate based authentication

NetApp BlueXP使您能够从一个控制平台/接口管理所有存储和数据资产。

您可以使用BlueXP创建和管理云存储(例如Cloud Volumes ONTAP 和Azure NetApp Files)、移动、保护和分析数据以及控制许多内部和边缘存储设备。

NetApp Asta Trident是一款符合CSI的存储编排程序，支持快速、轻松地使用由上述各种NetApp存储选项提供支持的永久性存储。它是由NetApp维护和支持的开源软件。

Astra Trident CSI feature highlights



CSI specific <ul style="list-style-type: none">CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copiesCSI topologyVolume expansion	Security <ul style="list-style-type: none">Dynamic-export policy managementiSCSI initiator-groups dynamic managementiSCSI bidirectional CHAP
Control <ul style="list-style-type: none">Storage and performance consumptionMonitoringVolume ImportCross Namespace Volume Access	Installation methods <ul style="list-style-type: none">BinaryHelm chartOperatorGitOps
Choose your access mode <ul style="list-style-type: none">RWO (ReadWriteOnce, i.e 1↔1)RWX (ReadWriteMany, i.e 1↔n)ROX (ReadOnlyMany)RWOP (ReadWriteOnce POD)	Choose your protocol <ul style="list-style-type: none">NFSSMBiSCSI

业务关键型容器工作负载所需的不仅仅是永久性卷。他们的数据管理要求也需要保护和迁移应用程序Kubernetes对象。



除了用户数据之外、应用程序数据还包括Kubernetes对象：以下是一些示例： - Kubernetes对象、例如Pod规格、PVC、部署、服务-自定义配置对象、例如配置映射和密钥-持久数据、例如Snapshot副本、备份、克隆-自定义资源、例如CRS和CRD

NetApp Astra Control作为完全托管和自我管理软件提供，可提供流程编排，实现强大的应用程序数据管理。请参见 "[Astra 文档](#)" 有关Astra系列产品的更多详细信息。

本参考文档使用NetApp Astra Control Center验证了在Red Hat OpenShift容器平台上部署的基于容器的应用程序的迁移和保护。此外、解决方案还提供了有关部署和使用Red Hat高级集群管理(ACM)来管理容器平台的详细信息。本文档还重点介绍了使用Astra Trident CSI配置程序将NetApp存储与Red Hat OpenShift容器平台集成的详细信息。Astra Control Center部署在集线器集群上、用于管理容器应用程序及其永久性存储生命周期。最后、它还提供了一个解决方案、用于在AWS (ROSA)中使用Amazon FSx for NetApp ONTAP (FSxN)作为永久性存储的受管Red Hat OpenShift集群上对容器工作负载进行复制、故障转移和故障恢复。

NetApp解决方案 在AWS上运行托管Red Hat OpenShift容器平台工作负载

NetApp解决方案 在AWS上运行托管Red Hat OpenShift容器平台工作负载

客户可能"生于云"、也可能正处于现代化之旅的某一时刻、准备将部分选定工作负载或所有工作负载从数据中心迁移到云。他们可以选择在云中使用提供商管理的OpenShift容器和提供商管理的NetApp存储来运行工作负载。他们应该在云中规划和部署托管Red Hat OpenShift容器集群(ROSA)、以便为其容器工作负载提供一个成功的生产就绪环境。在AWS云中、他们还可以部署FSx for NetApp ONTAP 来满足存储需求。

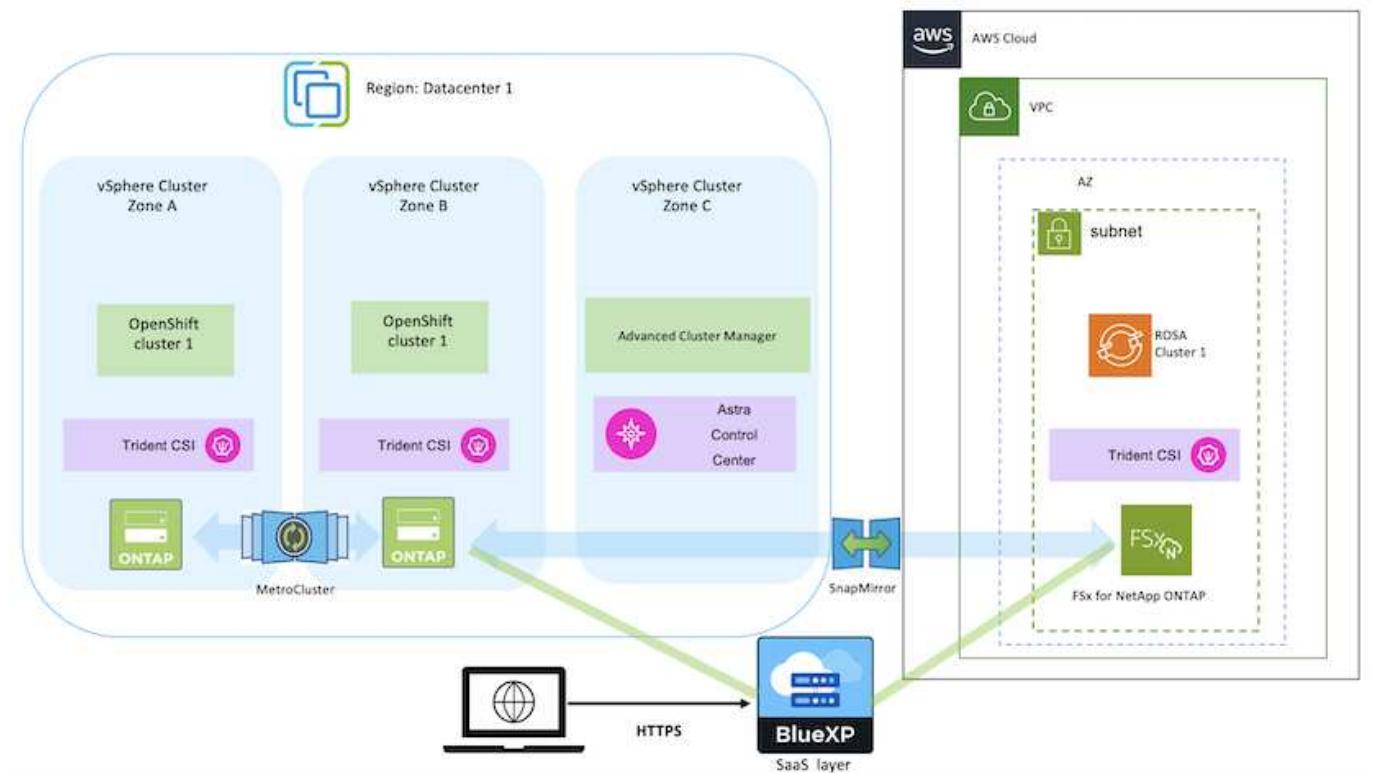
FSx for NetApp ONTAP 可为AWS中的容器部署提供数据保护、可靠性和灵活性。Astra三端存储作为动态存储配置程序、用于为客户的有状态应用程序使用永久性FSxN存储。

由于可以在HA模式下部署ROSA、并且控制平台节点分布在多个可用性区域中、因此FSx ONTAP 还可以配置Multi-AZ选项、以提供高可用性并防止出现AZ故障。



从文件系统的首选可用性区域(AZ)访问Amazon FSx文件系统时、无需支付数据传输费用。有关定价的详细信息、请参见 "[此处](#)"。

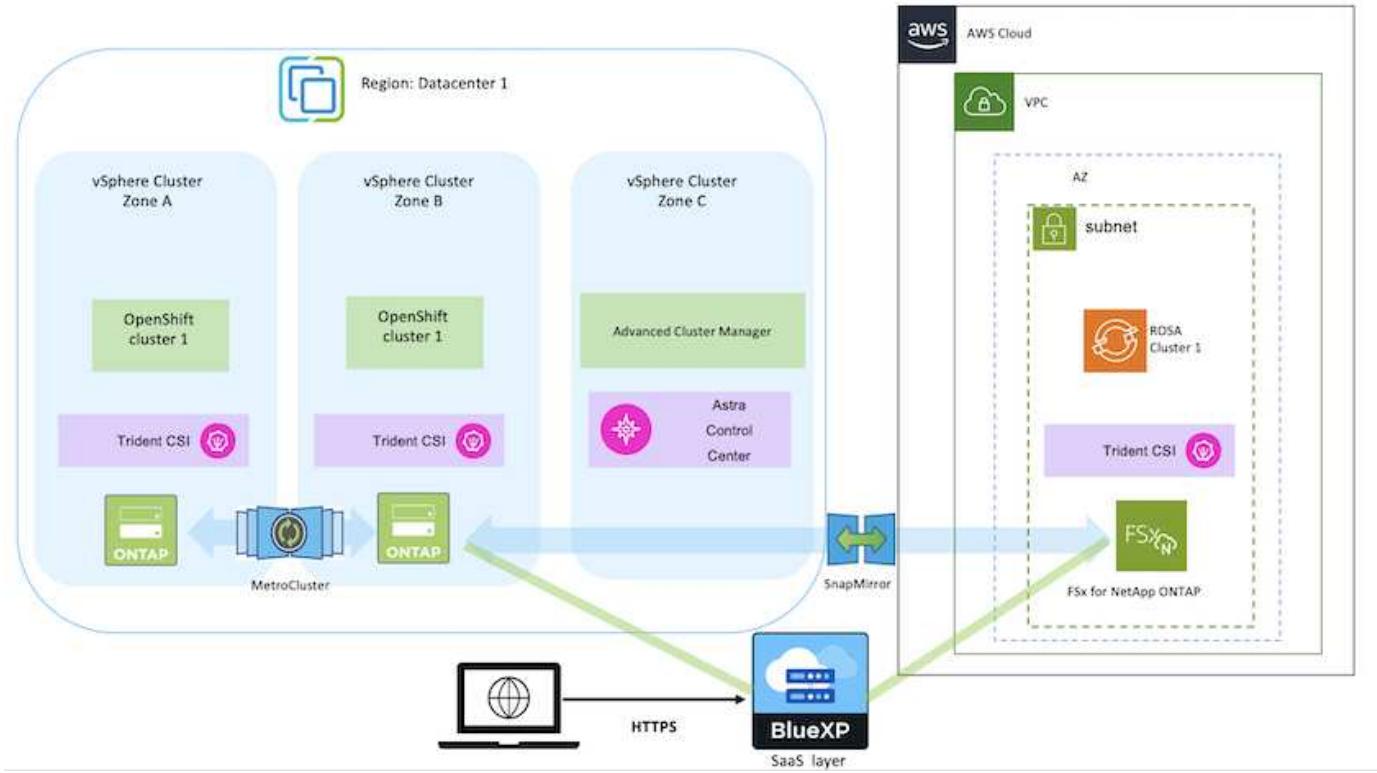
适用于OpenShift容器工作负载的数据保护和迁移解决方案



在AWS上部署和配置托管Red Hat OpenShift容器平台

本节简要介绍了在AWS (ROSA)上设置托管Red Hat OpenShift集群的工作流。其中显示了Asta三端存储使用托管FSx for NetApp ONTAP (FSxN)作为存储后端来提供永久性卷。其中详细介绍了如何使用BlueXP在AWS上部署FSxN。此外、还提供了有关使用BlueXP和OpenShift GitOps (Argo CD)为ROSA集群上有状态应用程序执行数据保护和迁移活动的详细信息。

下图展示了在AWS上部署并使用FSxN作为后端存储的ROSA集群。



i 此解决方案已通过在AWS中的两个VPC中使用两个ROSA集群进行验证。每个ROSA集群都使用Asta Trdent与FSxN集成。可以通过多种方法在AWS中部署ROSA集群和FSxN。此高级设置问题描述提供了所用特定方法的文档链接。您可以在中提供的相关链接中参考其他方法 "[资源部分](#)"。

设置过程可细分为以下步骤：

安装ROSA集群

- 创建两个VPC并在VPC之间设置VPC对等连接。
- 请参见 "[此处](#)" 有关安装ROSA集群的说明。

安装FSxN

- 从BlueXP在vPC上安装FSxN。请参见 "[此处](#)" 以便创建BlueXP帐户并开始使用。请参见 "[此处](#)" 用于安装FSxN。请参见 "[此处](#)" 用于在AWS中创建连接器以管理FSxN。
- 使用AWS部署FSxN。请参见 "[此处](#)" 适用于使用AWS控制台进行部署。

在ROSA集群上安装TRIDent (使用Helm图表)

- 使用Helm图表在ROSA集群上安装三端存储。Helm图表的URL: <https://netapp.github.io/trident-helm-chart>

将FSxN与适用于ROSA集群的Asta Trident集成



当所有受管集群使用ApplicationSet注册到ArgoCD时、可以使用OpenShift GitOps将Asta Trident CSI部署到这些集群。

```
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TRIDleNT创建后端和存储类(适用于FsxN)

- 请参见 "[此处](#)" 有关创建后端和存储类的详细信息、请参见。
- 从OpenShift控制台使用默认的三端CSI为FsxN创建存储类。请参见以下屏幕截图：

The screenshot shows the Red Hat OpenShift Service on AWS interface. The left sidebar has a navigation menu with items like Home, Operators, Workloads, Networking, Storage (selected), PersistentVolumes, PersistentVolumeClaims, StorageClasses (selected), and VolumeSnapshots. The main content area is titled "StorageClasses" and contains a table with the following data:

Name	Provisioner	Reclaim policy
SC fsxn-nas - Default	csi.trident.netapp.io	Delete
SC gp2	kubernetes.io/aws-ebs	Delete
SC gp2-csi	ebs.csi.aws.com	Delete
SC gp3	ebs.csi.aws.com	Delete
SC gp3-csi	ebs.csi.aws.com	Delete

A "Create StorageClass" button is located in the top right corner of the table header.

使用OpenShift GitOps部署应用程序(Argo CD)

- 在集群上安装OpenShift GitOps Operator。请参阅说明 "[此处](#)"。
- 为集群设置新的Argo CD实例。请参阅说明 "[此处](#)"。

打开Argo CD的控制台并部署应用程序。例如、您可以使用带有Helm Chart的Argo CD部署Jenkins应用程序。创建应用程序时、系统会提供以下详细信息：Project: default cluster: <https://kubernetes.default.svc> 命名空间：Jenkins Helm图表的URL：<https://charts.bitnami.com/bitnami>

Helm参数：globL.storageClass：fsxn-nas

数据保护

此页面显示了使用Astra Control Service在AWS上托管Red Hat OpenShift (ROSA)集群的数据保护选项。Astra Control Service (ACS)提供了一个易于使用的图形用户界面、您可以使用该界面添加集群、定义在其中运行的应用程序以及执行应用程序感知型数据管理活动。此外、还可以使用支持工作流自动化的API访问ACS功能。

NetApp Astra控制(ACS或ACC)由Astra三端驱动。Astra三端集成了多种类型的Kubernetes集群、例如Red Hat OpenShift、EKS、AKS、SUSE缓存器、Anthos等。具有各种NetApp ONTAP存储风格、例如FAS/AFFF、ONTAP Select、CVO、Google Cloud Volumes Service、Azure NetApp Files和Amazon FSx for NetApp ONTAP。

本节详细介绍了使用ACS的以下数据保护选项：

- 显示备份和还原在一个区域运行的ROSA应用程序并还原到另一个区域的视频。

- 显示ROSA应用程序的Snapshot和Restore的视频。
- 安装ROSA集群的分步详细信息、Amazon FSx for NetApp ONTAP、使用NetApp Astra三端集成到存储后端、在ROSA集群上安装PostgreSQL应用程序、使用ACS创建应用程序快照并从中还原应用程序。
- 一篇博客、详细介绍了如何使用ACS在使用FSx for ONTAP的ROSA集群上为mysql应用程序创建快照并从快照中还原。

备份/从备份中还原

以下视频显示了在一个区域运行的ROSA应用程序的备份以及还原到另一个区域的过程。

[FSx NetApp ONTAP for Red Hat OpenShift Service on AWS](#)

快照/从快照还原

以下视频显示了如何创建ROSA应用程序的快照以及之后如何从快照中还原。

[使用Amazon FSx for NetApp ONTAP存储在AWS上的Red Hat OpenShift Service \(ROSA\)集群上为应用程序创建快照/还原](#)

博客

- ["使用Astra Control Service对带有Amazon FSx存储的ROSA集群上的应用程序进行数据管理"](#)

创建快照并从中还原的分步详细信息

前提条件设置

- ["AWS 帐户"](#)
- ["Red Hat OpenShift帐户"](#)
- 使用的IAM用户 ["适当的权限"](#) 创建和访问ROSA集群
- ["AWS命令行界面"](#)
- ["罗莎命令行界面"](#)
- ["OpenShift命令行界面"\(OC\)](#)
- 具有子网以及相应网关和路由的VPC
- ["已安装罗莎群集" VPC](#)
- ["适用于 NetApp ONTAP 的 Amazon FSX" 在同一个VPC中创建](#)
- 从访问ROSA集群 ["OpenShift混合云控制台"](#)

后续步骤

1. 创建管理员用户并登录到集群。
2. 为集群创建一个kubeconfig文件。
3. 在集群上安装Astra Trdent。
4. 使用三端CSI配置程序创建后端、存储类和快照类配置。

5. 在集群上部署PostgreSQL应用程序。
6. 创建数据库并添加记录。
7. 将集群添加到ACS中。
8. 在ACS中定义应用程序。
9. 使用ACS创建快照。
10. 删除PostgreSQL应用程序中的数据库。
11. 使用ACS从快照还原。
12. 验证您的应用程序是否已从快照中还原。

1. 创建管理员用户并登录到群集

使用以下命令创建管理员用户以访问ROSA集群：(只有在安装时未创建管理员用户时、才需要创建管理员用户)

```
rosa create admin --cluster=<cluster-name>
```

此命令将提供如下输出。使用登录到集群 `oc login` 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
```



您也可以使用令牌登录到集群。如果您在创建集群时已创建管理员用户，则可以使用管理员用户凭据从Red Hat OpenShift Hybrid Cloud控制台登录到集群。然后、通过单击右上角显示已登录用户名的、您可以获取 `oc login` 命令(令牌登录)。

2. 为群集创建kubeconfig*文件

按照步骤进行操作 "[此处](#)" 为ROSA集群创建kubeconfig.稍后在将集群添加到ACS中时、将使用此kubeconfig.文件。

3. 在群集上安装Asta Trident

在ROSA集群上安装Asta Trident (最新版本)。要执行此操作、您可以按照给定的任一过程进行操作 "[此处](#)"。要从集群控制台使用Helm安装Trident、请先创建一个名为Trident的项目。

Red Hat
OpenShift Service on AWS

cluster-admin ▾

Projects Create Project

Filter Name trident

Name trident Clear all filters

Name	Display name	Status	Requester	Created
PR trident	trident	Active	rosaadmin	Feb 12, 2024, 9:54 PM

然后、在"开发工具"视图中、创建Helm图表存储库。对于URL字段、请使用 '<https://netapp.github.io/trident-helm-chart>'。然后为三端操作员创建舵版本。

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>

Project: trident ▾

Developer Catalog > Helm Charts

Helm Charts

Browse for charts that help manage complex installations and upgrades. Cluster administrators can customize the catalog. Alternatively, developers can try to configure their own custom Helm Chart repository.

All items

CI/CD

Languages

Other

Chart Repositories

Astra Trident (1)

OpenShift Helm Charts (87)

Source

Community (33)

Partner (42)

Red Hat (12)

All items

 Filter by keyword...

A-Z ▾



Helm Charts

Trident Operator

A Helm chart for deploying NetApp's Trident CSI storage provisioner using the Trident...

返回控制台上的"Administrator view"(管理员视图)、然后在三级工程中选择Pod、以验证所有三级工程模块是否正在运行。

Name	Status	Ready	Restarts	Owner	Mem
trident-controller-69cff44ddf-4dqnj	Running	6/6	0	RS trident-controller-69cff44ddf	-
trident-node-linux-4b6fm	Running	2/2	0	OS trident-node-linux	-
trident-node-linux-4sckw	Running	2/2	0	OS trident-node-linux	-
trident-node-linux-7i42w	Running	2/2	0	OS trident-node-linux	-
trident-node-linux-dbhp4	Running	2/2	0	OS trident-node-linux	-
trident-node-linux-gj5km	Running	2/2	0	OS trident-node-linux	-
trident-node-linux-r79c8	Running	2/2	0	OS trident-node-linux	-
trident-node-linux-tzwdp	Running	2/2	0	OS trident-node-linux	-
trident-node-linux-vdvxt	Running	2/2	0	OS trident-node-linux	-
trident-operator-7f7fd45c68-6crcb	Running	1/1	0	RS trident-operator-7f7fd45c68	-

4. 使用三端CSI配置程序创建后端、存储类和快照类配置

使用下面显示的YAML文件创建三元后端对象、存储类对象和卷快照对象。请务必为您创建的Amazon FSx for NetApp ONTAP文件系统提供凭据、并在后端的YAML配置中提供管理LIF和文件系统的Vserver名称。要获取这些详细信息、请转到适用于Amazon FSx的AWS控制台并选择文件系统、然后导航到管理选项卡。此外、单击更新以设置的密码 fsxadmin 用户。



您可以使用命令行创建对象、也可以从混合云控制台使用YAML文件创建对象。

FSx > File systems > fs-049f9a23aac951429

fsx-for-rosa (fs-049f9a23aac951429)

▼ Summary

File system ID fs-049f9a23aac951429	SSD storage capacity 1024 GiB	Update	Availability Zones us-west-2b
Lifecycle state Available	Throughput capacity 128 MB/s	Update	Creation time 2024-02-12T20:15:23-05:00
File system type ONTAP	Provisioned IOPS 3072	Update	
Deployment type Single-AZ	Number of HA pairs 1	Update	

Network & security | Monitoring & performance | **Administration** | Storage virtual machines | Volumes | Backups | Updates | Tags

ONTAP administration

Management endpoint - DNS name management.fs-049f9a23aac951429.fsx.us-west-2.amazonaws.com	Management endpoint - IP address 10.49.9.135	ONTAP administrator username fsxadmin
Inter-cluster endpoint - DNS name intercluster.fs-049f9a23aac951429.fsx.us-west-2.amazonaws.com	Inter-cluster endpoint - IP address 10.49.9.49 10.49.9.251	ONTAP administrator password Update

Trident后端配置

```

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

```

存储类

```

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

```

快照类

```

apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete

```

发出下面所示的命令、验证是否已创建后端、存储类和trdent-snapshotclass对象。

```

[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]$ ■

```

此时、您需要进行的一项重要修改是将ONTAP NAS设置为默认存储类、而不是GP3、以便您稍后部署的PostgreSQL应用程序可以使用默认存储类。在集群的OpenShift控制台中、在"Storage"下选择"StorageClasses"。将当前默认类的标注编辑为false、并将ONTAP NAS存储类的标注storageclass.Kubernetes.io/is-default-class设置为true。

The screenshot shows the Red Hat OpenShift StorageClasses configuration interface. On the left, a sidebar lists existing StorageClasses: SC gp2, SC gp2-csi, SC gp3 - Default, SC gp3-csi, and SC ontap-nas. The main area displays a table of StorageClasses with columns for Name, Provisioner, and Reclaim policy. A modal dialog titled "Edit annotations" is open over the table, allowing the addition of annotations. One annotation is currently listed: storageclass.kubernetes.io/is-default=true with a value of false. There are "Cancel" and "Save" buttons at the bottom of the modal.

Name	Provisioner	Reclaim policy
SC gp2	kubernetes.io/aws-ebs	Delete
SC gp2-csi	ebs.csi.aws.com	Delete
SC gp3 - Default	ebs.csi.aws.com	Delete
SC gp3-csi	ebs.csi.aws.com	Delete
SC ontap-nas	csi.trident.netapp.io	Delete

This screenshot shows the main list view of StorageClasses. It includes a search bar at the top and a table below with columns for Name, Provisioner, and Reclaim policy. The same five StorageClasses listed in the first screenshot are present here, each with a "Delete" option and a more options menu (three dots). A "Create StorageClass" button is located in the top right corner of the list view.

Name	Provisioner	Reclaim policy
SC gp2	kubernetes.io/aws-ebs	Delete
SC gp2-csi	ebs.csi.aws.com	Delete
SC gp3	ebs.csi.aws.com	Delete
SC gp3-csi	ebs.csi.aws.com	Delete
SC ontap-nas - Default	csi.trident.netapp.io	Delete

5. 在群集上部署PostgreSQL应用程序

您可以从命令行部署此应用程序，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="PGPASSWORD=$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]$
```

如果您看不到应用程序Pod正在运行，则可能是由于安全上下文约束而导致错误。

```
[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
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: [jint64<1001]: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, provider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provider "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or serviceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceaccount, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, provider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, provider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

编辑以修复此错误 `runAsUser` 和 `fsGroup` 中的字段 `statefulset.apps/postgresql` 具有的输出中的 `_id` 的对象 `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应用程序应正在运行，并使用Amazon FSx支持的永久性卷作为NetApp ONTAP存储。

```
[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. 创建数据库并添加记录

```
[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 set securityContext.allowPrivilegeEscalation=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 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. 将集群添加到ACs中

登录到ACS。选择cluster、然后单击Add。选择其他并上传或粘贴kubeconfig.

Add cluster STEP 1/3: DETAILS

PROVIDER

Microsoft Azure Google Cloud Platform aws Amazon Web Services Other

KUBECONFIG

Please ensure that the kubeconfig used for this cluster has a long-lived token associated with it.

Provide Astra Control access to your Kubernetes clusters by entering a kubeconfig credential. Follow these [instructions](#) on how to create a dedicated admin-role kubeconfig.

Upload file Paste or type

```
XJuZXRLcy5pb9zZXJ2aWN1YWNjb3VudC9zZXJ2aWN1LWFjY291bnQubmFtZSI6ImFzdHJhY29udHJvbC1zZXJ2aWN1LWFjY291bnQiLCJrdWJlcm5ldGVzLmlvL3N1cn2pY2VhY2NvdW50L3N1cn2pY2UtYWNjb3VudC51aWQiOiI4NzFhOTI4MC0wMTEyLTRmYzAtOWFkNS0zZDI5NzA2N2NiNTcILCJzdWIiOjzeXN0ZW06c2VydmljZWfjY291bnQ6ZGVmYXVsdDphc3RyYWNvbnRyb2wtc2VydmljZS1hY2NvdW50In0.M7-IRxcaKOe7S-LkW-8ZDYOShQ5U1laSbJ-0Si5r0EBvfcQ3tSf40VC72nM4BqYbN8cm0y0V8IpF30G7tYA9XAIdwX98xAXJ00T2UOG2xbylWfOqLCFDk3_uS9uqU63t8LLmeenCBiOm9PaD3XWHFZZcTXXpdKqtzWfmBLxYhuN1CzBMY7S55MVnB2WD_eikptN02alvaWmIZjrUQL0_g8Uj2Exe9vVh1KPfb0Cx4TvHncbathvL6mZ1N7Om
```

Cancel **Next →**

单击“Next”并选择ONTAP—NAS作为ACS的默认存储类。单击“Next”(下一步)，查看详细信息，然后单击“Add”(添加)群集。

Add cluster STEP 2/3: STORAGE

STORAGE

Assign a new default storage class

The following storage classes are available on the cluster.

Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligibility
<input type="radio"/>	gp2	kubernetes.io/aws-ebs	Delete	WaitForFirstConsumer	✗ Ineligible
<input type="radio"/>	gp2-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	✓ Eligible
<input type="radio"/>	gp3	ebs.csi.aws.com	Delete	WaitForFirstConsumer	✓ Eligible
<input type="radio"/>	gp3-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	✓ Eligible
<input checked="" type="radio"/>	ontap-nas Default	csi.trident.netapp.io	Delete	Immediate	✓ Eligible

← Back **Next →**

8.在ACs中定义应用程序

在ACS中定义PostgreSQL应用程序。在登录页面中，选择“Applications”、**Define**并填写相应的详细信息。单击“下一步”几次，查看详细信息，然后单击“定义”。应用程序将添加到ACS。

Storage

Assign a new default storage class

The following storage classes are available on the cluster.

Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligibility
<input type="radio"/>	gp2	kubernetes.io/aws-ebs	Delete	WaitForFirstConsumer	Not Eligible
<input type="radio"/>	gp2-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	Eligible
<input type="radio"/>	gp3	ebs.csi.aws.com	Delete	WaitForFirstConsumer	Eligible
<input type="radio"/>	gp3-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	Eligible
<input checked="" type="radio"/>	ontap-nas Default	csi.trident.netapp.io	Delete	Immediate	Eligible

← Back Next →

9. 使用ACs创建快照

可通过多种方法在ACS中创建快照。您可以从显示应用程序详细信息的页面中选择应用程序并创建快照。您可以单击创建快照来创建按需快照或配置保护策略。

只需单击“创建快照”、提供名称、查看详细信息并单击“快照”、即可创建按需快照。操作完成后、快照状态将更改为“运行状况良好”。

Dashboard

Applications

Clusters

Cloud instances

Buckets

Account

Activity

Support

NetApp

Data protection Storage Resources Execution hooks Activity Tasks Snapshots

Actions Configure protection policy Search Create snapshot

0-0 of 0 entries

<input type="checkbox"/>	Name	State	On-Schedule / On-Demand	Created ↑	Actions
 You don't have any snapshots After you have created a snapshot, it will be listed here					

The screenshot shows the PostgreSQL UI interface. On the left sidebar, there are links for Dashboard, Applications, Clusters, Cloud instances, Buckets, Account, Activity, and Support. The main area displays 'APPLICATION STATUS' with a green 'Available' icon and 'APPLICATION PROTECTION' with a 'Partially protected' status and a 'No scheduled protection policy' warning. Below this, a 'Definition' section shows 'postgresql'. A 'Cluster' section shows 'api-rosa-cluster1-nn5w-p1...' with a red warning icon. The 'Data protection' tab is selected in the top navigation bar, showing a table with one entry: 'postgresql-snapshot-20240213154610' which is healthy, on-demand, and was created on 2024/02/13 15:48 UTC.

10.删除PostgreSQL应用程序中的数据库

重新登录到PostgreSQL、列出可用数据库、删除先前创建的数据库并重新列出、以确保数据库已被删除。

```
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 |           |           | =c/postgres
postgres | postgres | UTF8     | libc          | en_US.UTF-8 | en_US.UTF-8 |           |           |
template0 | postgres | UTF8     | libc          | en_US.UTF-8 | en_US.UTF-8 |           |           |
+
template1 | postgres | UTF8     | libc          | en_US.UTF-8 | en_US.UTF-8 |           |           |
+
(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 |           |           | =c/postgres
template0 | postgres | UTF8     | libc          | en_US.UTF-8 | en_US.UTF-8 |           |           |
+
template1 | postgres | UTF8     | libc          | en_US.UTF-8 | en_US.UTF-8 |           |           |
+
(3 rows)
```

11.使用ACs从快照恢复

要从快照还原应用程序、请转到ACS UI登录页面、选择应用程序、然后选择还原。您需要选择要从中还原的快照或备份。(通常、您会根据所配置的策略创建多个)。在接下来的几个屏幕中做出适当的选择，然后单

击*Restore*。从快照还原后、应用程序状态将从还原变为可用。

The screenshot shows the NetApp Application Protection interface for the 'postgresql' application. The left sidebar includes links for Dashboard, Applications, Clusters, Cloud instances, Buckets, Account, Activity, and Support. The main area displays the 'APPLICATION STATUS' as 'Available' and 'APPLICATION PROTECTION' status as 'Partially protected'. A cluster named 'api-rosa-cluster1-nn5w-p1-op...' is listed. The 'Data protection' tab is selected, showing a table with one entry: 'postgresql-snapshot-20240213164912' (Healthy, On-Demand, Created: 2024/02/13 16:50 UTC). The 'Actions' menu on the right offers options like Snapshot, Back up, Clone, Restore, and Unmanage.

The screenshot shows the 'RESTORE TYPE' section, which allows restoring to new namespaces or original namespaces. The 'Restore to original namespaces' option is selected. Below it, the 'RESTORE SOURCE' section shows a table of available snapshots. One snapshot, 'postgresql-snapshot-20240213164912' (Healthy, On-Demand, Created: 2024/02/13 16:50 UTC), is selected. At the bottom, there are 'Cancel' and 'Next' buttons.

The screenshot shows the Astra Control web interface for managing PostgreSQL clusters. On the left sidebar, there are links for Dashboard, Applications, Clusters, Cloud instances, Buckets, Account, Activity, and Support. The main area is titled 'postgresql' and displays the 'APPLICATION STATUS' as 'Available' and 'APPLICATION PROTECTION' as 'Partially protected'. Below this, it shows a 'Definition' of 'postgresql' and a 'Cluster' named 'api-rosa-cluster1-nn5w-p1-op...'. The 'Data protection' tab is selected, featuring a 'Configure protection policy' button. A table lists a single snapshot: 'postgresql-snapshot-20240213164912' which is 'Healthy' and 'On-Demand', created on '2024/02/13 16:50 UTC'.

12.验证您的应用程序是否已从快照中恢复

登录到PostgreSQL客户端、您现在应该可以看到表以及以前的表中的记录。就是这样。只需单击一个按钮、您的应用程序便已恢复到先前的状态。这就是我们使用Astra Control为客户提供实现的简单体验。

```
[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.allowPrivilegeEscalation=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 securityContext.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 | +         | +         | =c/postgres
  postgres | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | +         | +         | postgres=CTc/postgres
template0 | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | +         | +         | =c/postgres
template1 | postgres | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | +         | +         | 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)
```

Activate Windows

数据迁移

此页面显示了使用FSx for NetApp ONTAP 作为永久性存储的托管Red Hat OpenShift集群上容器工作负载的数据迁移选项。

数据迁移

AWS上的Red Hat OpenShift服务以及适用于NetApp ONTAP 的FSx (FSxN)是AWS服务产品组合的一部分。FSxN可用于单AZ或多AZ选项。Multi-Az选项可防止数据受到可用性区域故障的影响。FSxN可以与Astra Trident集成、为ROSA集群上的应用程序提供永久性存储。

使用Helm将FSxN与TRident集成图表

Rosa集群与Amazon FSx for ONTAP集成

容器应用程序的迁移涉及：

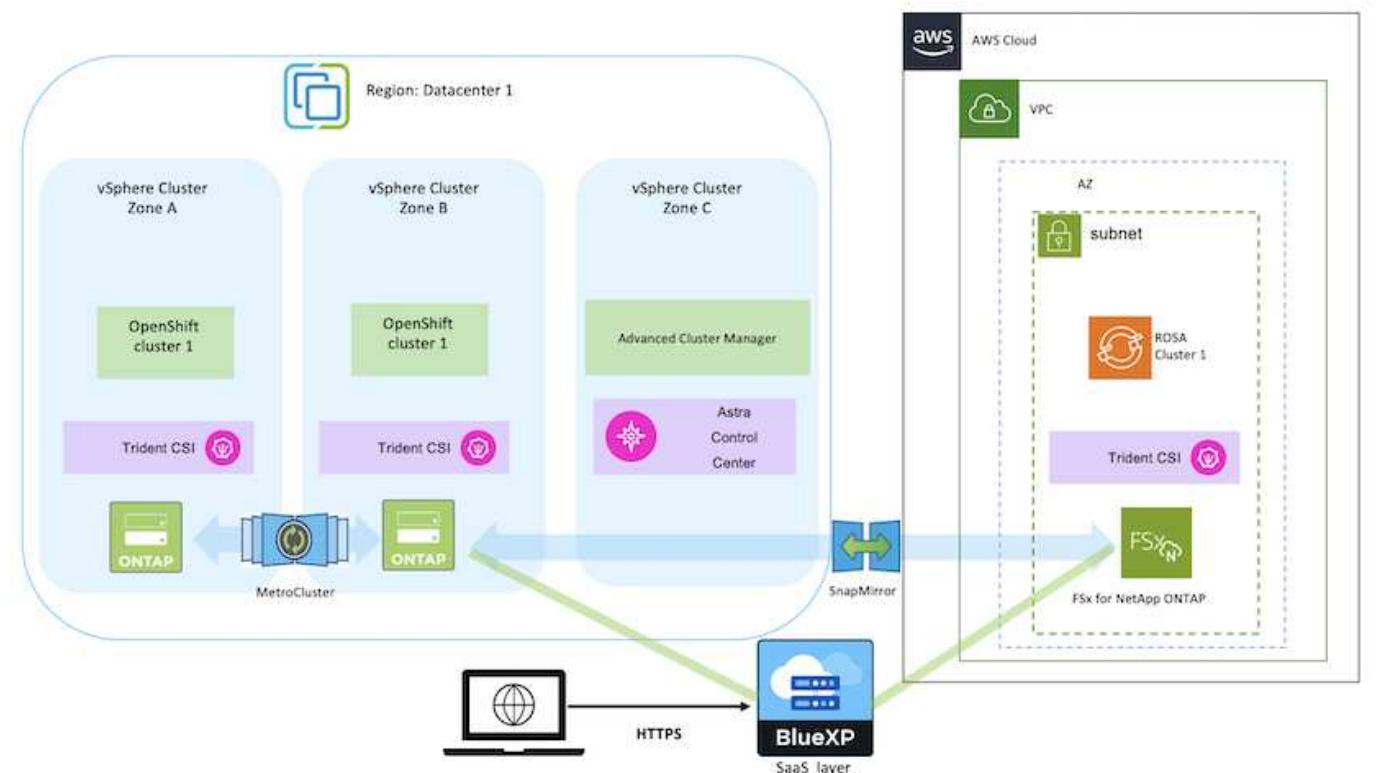
- 永久性卷：可使用BlueXP来实现。另一种选择是使用Astra Control Center处理从内部环境到云环境的容器应用程序迁移。自动化也可以用于相同目的。
- 应用程序元数据：可以使用OpenShift GitOps (Argo CD)来实现。

使用FSxN对ROSA集群上的应用程序进行故障转移和故障恢复、以实现永久性存储

以下视频演示了使用BlueXP和Argo CD的应用程序故障转移和故障恢复场景。

对ROSA集群上的应用程序进行故障转移和故障恢复

适用于OpenShift容器工作负载的数据保护和迁移解决方案



版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。