



混合云 FlexPod

NetApp
November 04, 2025

This PDF was generated from <https://docs.netapp.com/zh-cn/flexpod/hybrid-cloud/fhc-cvcoe-solution-overview.html> on November 04, 2025. Always check docs.netapp.com for the latest.

目录

混合云	1
采用Cloud Volumes ONTAP for Epic的FlexPod 混合云	1
TR-4960: 《FlexPod 混合云与适用于Epic的Cloud Volumes ONTAP 》	1
解决方案组件	3
安装和配置	7
SAN 配置	11
解决方案验证	17
结论	24
从何处查找追加信息	25
适用于Google云平台的FlexPod 混合云与NetApp Cloud Volumes ONTAP 和Cisco Intersight	26
TR-4939: 《适用于Google云平台的FlexPod 混合云与NetApp Cloud Volumes ONTAP 和Cisco Intersight》	26
解决方案组件	28
安装和配置	32
解决方案验证	95
结论	102
采用NetApp Astra和适用于Red Hat OpenShift的Cisco Intersight的FlexPod 混合云	105
TR-4936: 采用NetApp Astra和适用于Red Hat OpenShift的Cisco Intersight的FlexPod 混合云	105
解决方案组件	107
安装和配置	115
解决方案验证	136
结论	157
适用于 FlexPod 的 NetApp Cloud Insights	159
TR-4868: 《适用于 FlexPod 的 NetApp Cloud Insights 》	159
用例	159
架构	160
设计注意事项	162
部署适用于 FlexPod 的 Cloud Insights	162
用例	174
视频和演示	182
追加信息	182
采用 FabricPool 的 FlexPod —将非活动数据分层到 Amazon AWS S3	183
TR-4801: 采用 FabricPool 的 FlexPod —将非活动数据分层到 Amazon AWS S3	183
FlexPod 概述和架构	183
FabricPool	185
FabricPool 要求	189
Configuration	193
性能注意事项	203
拥有成本	203

结论	203
从何处查找追加信息	203
适用于混合云的FlexPod 数据中心与Cisco CloudCenter和NetApp私有存储—设计	204

混合云

采用Cloud Volumes ONTAP for Epic的FlexPod 混合云

TR-4960：《FlexPod 混合云与适用于Epic的Cloud Volumes ONTAP》



与以下合作伙伴：

NetApp公司Kamini Singh

实现数字化转型的关键在于利用数据完成更多工作。医院需要生成大量数据、才能有效地运营组织并为患者提供服务。在治疗患者以及管理员工计划和医疗资源时、系统会收集和 处理相关信息。

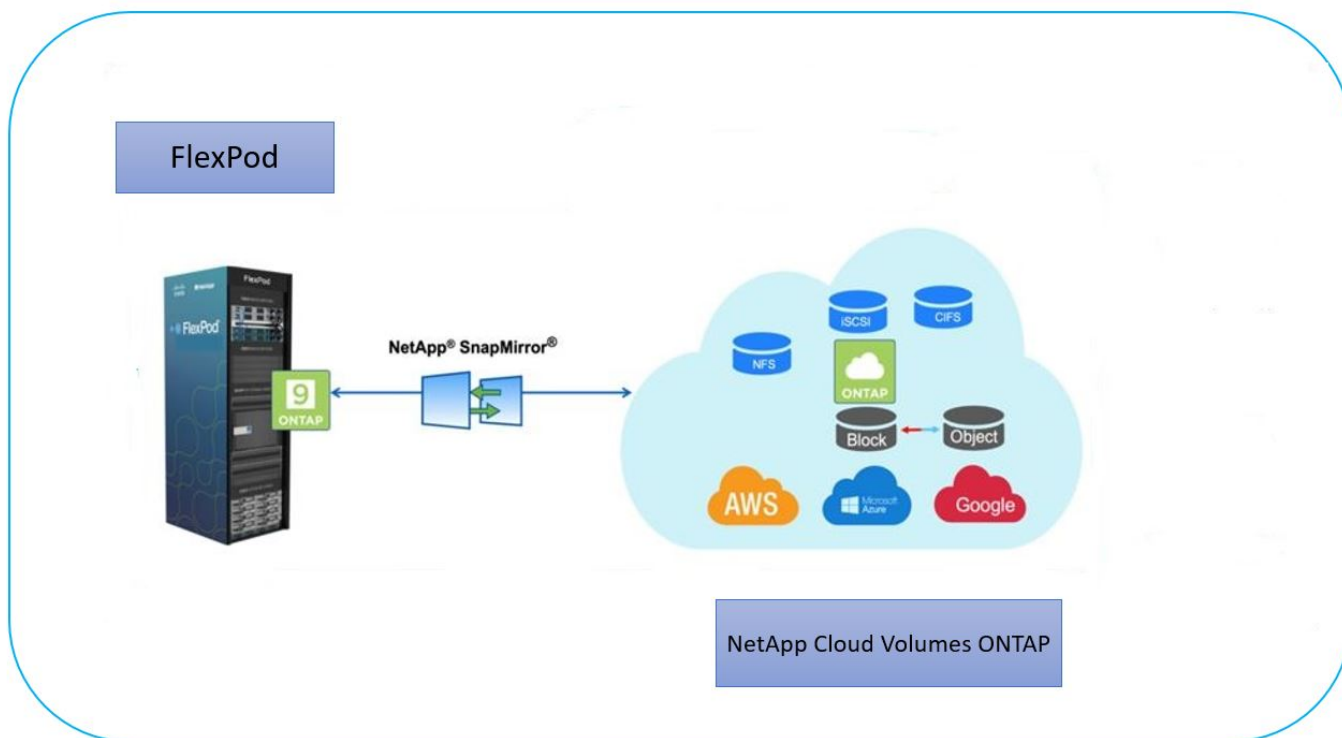
医疗保健数据的规模不断扩大、而且这些数据可以提供宝贵的洞察力、这使得医疗保健数据服务和数据保护变得既重要又具有挑战性。首先、医疗保健数据必须可用且受到保护、才能满足数据恢复、医疗业务连续性或合规性要求。

第二、必须随时提供医疗保健数据以供分析。这种分析通常采用基于人工智能(AI)和机器学习(ML)的方法来帮助医疗企业改进其解决方案并创造业务价值。

第三、随着医疗业务的增长、数据服务基础架构和数据保护方法必须适应医疗保健数据的增长。此外、由于需要将数据从创建数据的边缘移动到核心和云、以便使用数据分析或归档所需的资源、数据移动性变得越来越重要。

NetApp为包括医疗保健在内的企业级应用程序提供了一个数据管理解决方案、我们可以指导医院完成数字化转型之旅。NetApp Cloud Volumes ONTAP 提供了用于医疗保健数据管理的解决方案、可将数据从FlexPod 数据中心高效复制到AWS等公共云上部署的Cloud Volumes ONTAP。

通过利用经济高效且安全的公共云资源、Cloud Volumes ONTAP 通过高效的数据复制、内置存储效率和简单的灾难恢复测试增强了基于云的灾难恢复(Disaster Recovery、DR)。这些系统采用统一的控制和简单的拖放操作进行管理、可提供经济高效的保护、防止出现任何类型的错误、故障或灾难。Cloud Volumes ONTAP 提供了NetApp SnapMirror技术作为块级数据复制的解决方案、可通过增量更新使目标保持最新。



audience

本文档面向NetApp和合作伙伴解决方案工程师(SE)以及专业服务人员。NetApp假定读者具备以下背景知识：

- 深入了解SAN和NAS概念
- 熟悉NetApp ONTAP 存储系统的技术知识
- 熟悉ONTAP 软件的配置和管理技术

解决方案的优势

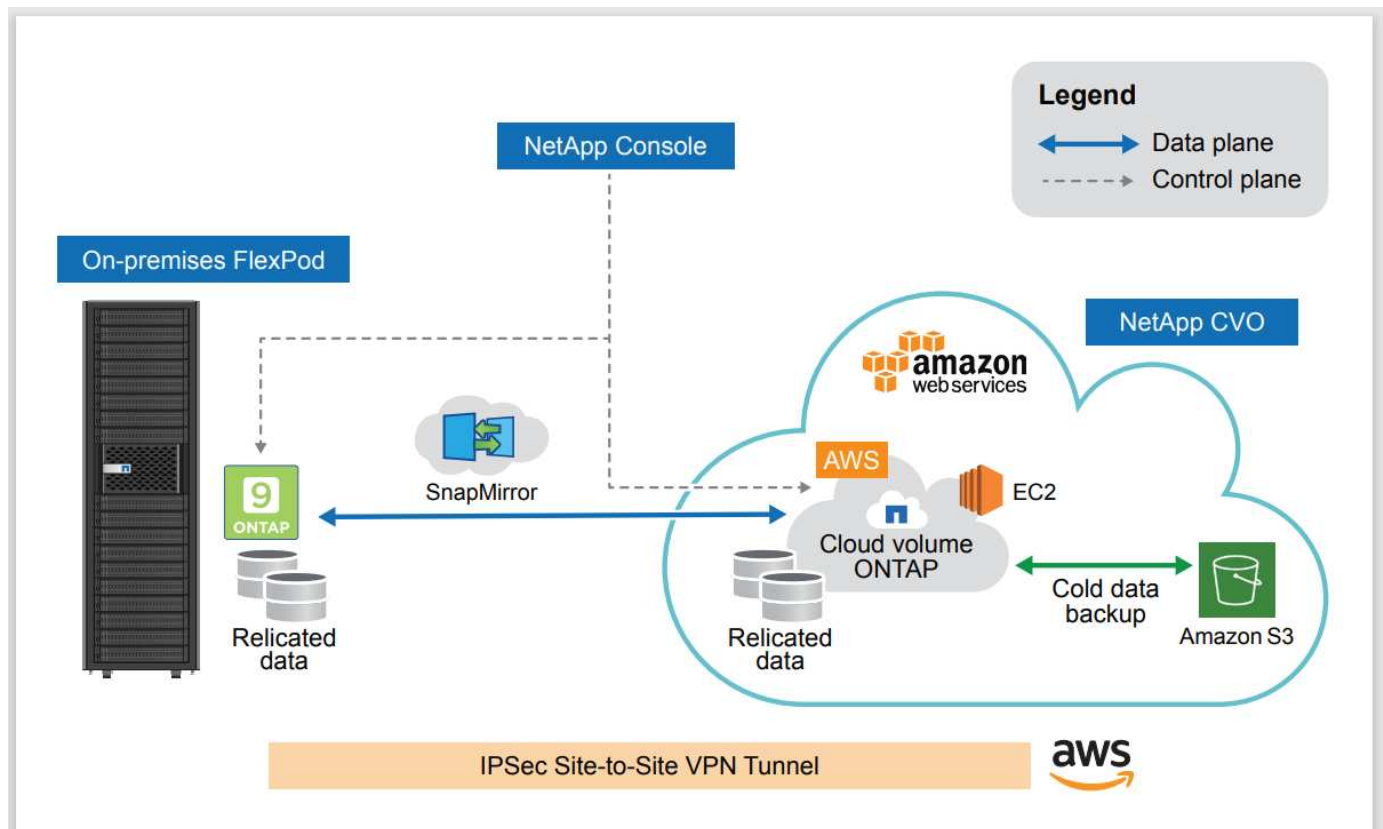
与NetApp Cloud Volumes ONTAP 集成的FlexPod 数据中心为医疗保健工作负载提供了以下优势：

- 自定义保护。Cloud Volumes ONTAP 提供从ONTAP 到云的块级数据复制、通过增量更新使目标保持最新。用户可以指定同步计划来确定何时传输源上的更改。这样可以为各种医疗保健数据提供自定义保护。
- *故障转移和故障恢复。*发生灾难时、存储管理员可以快速为云卷设置故障转移。恢复主站点后、在灾难恢复环境中创建的新数据将同步回源卷、以便重新建立二级数据复制。这样、医疗保健数据便可轻松恢复、而不会造成中断。
- *效率。*二级云副本的存储空间和成本通过数据压缩、精简配置和重复数据删除进行了优化。医疗保健数据以经过压缩和重复数据删除的形式在块级别传输、从而加快传输速度。数据也会自动分层到低成本对象存储、并且只有在访问时才会返回到高性能存储、例如在灾难恢复情形下。这样可以显著降低持续存储成本。
- 勒索软件防护 NetApp Console勒索软件防护功能可扫描本地和云环境中的数据源，检测安全漏洞，并提供其当前的安全状态和风险评分。然后它会提供可操作的建议，您可以进一步调查并遵循这些建议进行补救。这可以帮助您保护关键的医疗保健数据免受勒索软件攻击。

解决方案 拓扑

本节描述解决方案的逻辑拓扑结构。下图表示由FlexPod本地环境、运行在 Amazon Web Services (AWS) 上

的NetApp Cloud Volumes ONTAP (CVO) 和NetApp Console SaaS 平台组成的解决方案拓扑。



控制平面和数据平面会在端点之间清晰地指示。通过利用安全的站点到站点VPN连接、数据平面在FlexPod 的纯闪存FAS 上运行的ONTAP 实例与AWS中的NetApp CVO实例之间运行。将医疗保健工作负载数据从内部FlexPod 数据中心复制到NetApp Cloud Volumes ONTAP 时、会通过NetApp SnapMirror复制来处理。此外、此解决方案 还支持将NetApp CVO实例中的冷数据备份和分层到AWS S3。

"接下来：解决方案 组件。"

解决方案组件

"先前版本：解决方案 概述。"

FlexPod

FlexPod 是一组定义的硬件和软件、可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 包括NetApp ONTAP 存储、Cisco Nexus网络、Cisco MDS存储网络和Cisco统一计算系统(Cisco UCS)。

医疗保健组织正在寻找解决方案、以简化数字化转型并改善患者体验和结果。借助FlexPod、您可以获得一个安全、可扩展的平台、该平台可提高效率、并使员工能够更快地做出更明智的决策、从而为患者提供更好的护理。

FlexPod 是满足医疗保健工作负载需求的理想平台、因为它具有以下优势：

- 优化操作、更快地获得洞察力并获得更好的患者结果。
- 利用可扩展且可靠的基础架构简化映像应用程序。
- 借助经验证的方法快速高效地部署特定于医疗保健的应用程序、例如EHR。

EHR

电子健康记录(Electronic Health Records、EHRs)为大中型医疗团队、医院和综合医疗保健组织提供软件。客户还包括社区医院、学术机构、儿童组织、安全网络提供商和多医院系统。EHR集成软件涵盖临床、访问和收入功能、并扩展到家庭。

医疗保健提供商组织仍然面临着最大程度地发挥其在行业领先的EHRs上的巨大投资优势的压力。客户在为EHR解决方案和任务关键型应用程序设计数据中心时、通常会为其数据中心架构确定以下目标：

- EHR应用程序的高可用性
- 高性能
- 在数据中心轻松实施EHR
- 灵活性和可扩展性、支持通过新的EHR版本或应用程序实现增长
- 成本效益
- 易管理性，稳定性和易支持性
- 强大的数据保护，备份，恢复和业务连续性

FlexPod已获得 EHR 认证，并支持包含Cisco UCS、Intel Xeon 处理器、Red Hat Enterprise Linux (RHEL) 和 VMware ESXiCisco化的平台。该平台，加上 EHR 对运行ONTAP的NetApp存储的高舒适度评级，使您能够通过FlexPod在完全托管的私有云中运行您的医疗保健应用程序，该私有云还可以连接到任何公共云提供商。

NetApp Console

NetApp Console是一个企业级的、基于 SaaS 的管理平台，它使 IT 专家和云架构师能够使用NetApp云解决方案集中管理其混合多云基础架构。它提供了一个集中式系统，用于查看和管理您的本地和云存储，支持混合云、多云提供商和帐户。有关详细信息，请参阅 ["NetApp Console文档"](#)。

控制台代理

控制台代理实例使控制台能够管理公有云环境中的资源和进程。控制台提供的许多功能都需要控制台代理，它可以部署在云端或本地网络中。

控制台代理在以下位置受支持：

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- 内部部署

["了解有关控制台代理的更多信息"](#)。

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP 是一款软件定义的存储产品、可在云中运行ONTAP 数据管理软件、为文件和块工作负载提供高级数据管理。借助Cloud Volumes ONTAP 、您可以优化云存储成本并提高应用程序性能、同时增强数据保护、安全性和合规性。

主要优势包括：

- ***存储效率。** *利用内置的重复数据删除、数据压缩、精简配置和即时克隆功能最大限度地降低存储成本。
- ***高可用性。** *在云环境发生故障时提供企业级可靠性和持续运营。
- **数据保护。** Cloud Volumes ONTAP 使用行业领先的NetApp复制技术SnapMirror将内部数据复制到云、以便可以轻松地为多种使用情形提供二级副本。Cloud Volumes ONTAP 还与云备份相集成、提供备份和还原功能、以保护云数据并对其进行长期归档。
- ***数据分层。** *按需在高性能和低性能存储池之间切换、而无需使应用程序脱机。
- ***应用程序一致性。** *使用NetApp SnapCenter 技术提供NetApp Snapshot副本的一致性。
- **数据安全。** Cloud Volumes ONTAP 支持数据加密、并提供防病毒和勒索软件保护。
- ***隐私合规性控制。** *与Cloud Data sense集成有助于您了解数据环境并识别敏感数据。

更多详细信息，请参阅["Cloud Volumes ONTAP"](#)。

NetApp Active IQ Unified Manager

借助NetApp Active IQ Unified Manager、您可以通过一个经过重新设计的直观界面监控ONTAP 存储集群、从而利用社区智慧和AI分析提供智能。它可以全面洞察存储环境及其运行的虚拟机的运行状况、性能和主动性。当存储基础架构发生问题描述 时、Unified Manager可以通知您问题描述 的详细信息、以帮助识别根发生原因。通过虚拟机信息板、您可以查看虚拟机的性能统计信息、以便调查从vSphere主机向下经过网络并最终到达存储的整个I/O路径。

某些事件还提供了可用于更正问题描述 的补救措施。您可以为事件配置自定义警报、以便在发生时、通过电子邮件和SNMP陷阱通知您。通过Active IQ Unified Manager、您可以通过预测容量和使用趋势来规划用户的存储需求、以便在出现问题之前采取行动、防止做出长期可能导致其他问题的被动短期决策。

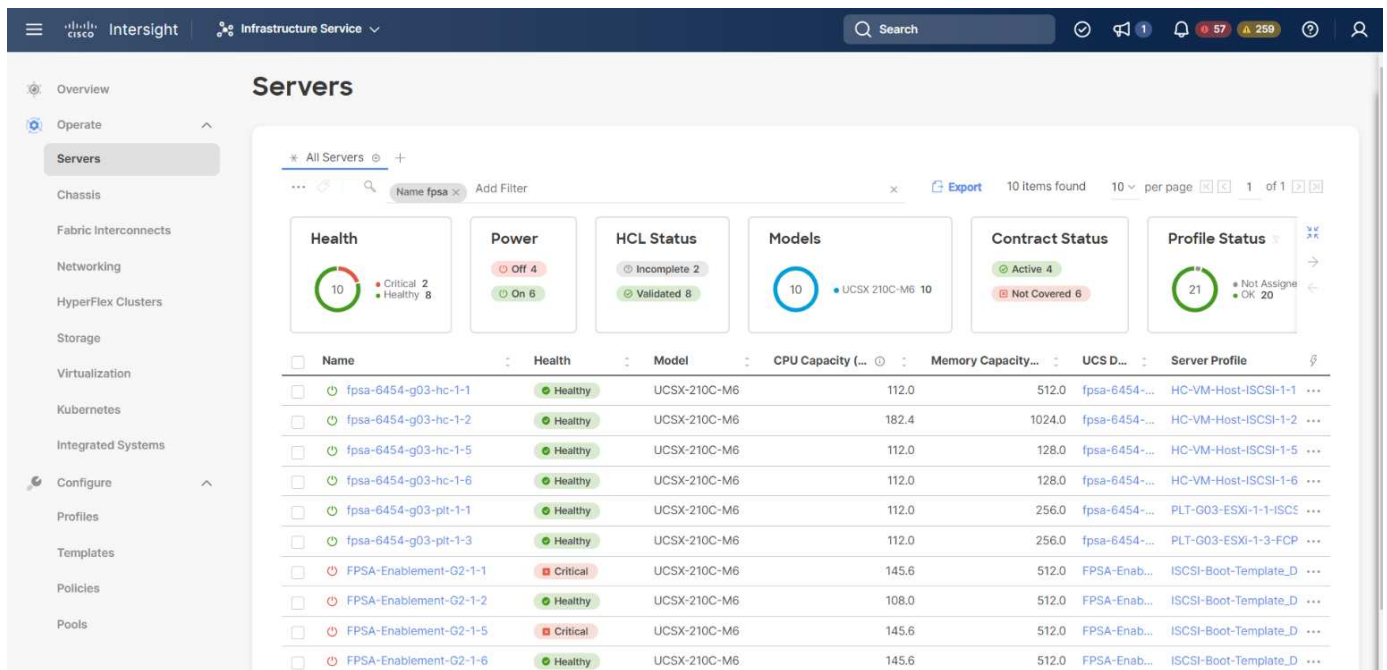
有关详细信息，请参阅 ["Active IQ Unified Manager"](#)。

Cisco Intersight

Cisco Intersight是一个SaaS平台、可为传统和云原生应用程序和基础架构提供智能自动化、可观察性和优化功能。该平台有助于推动IT团队的变革、并提供专为混合云设计的运营模式。Cisco Intersight具有以下优势：

- **更快的交付速度。** Intersight通过基于敏捷性的软件开发模式、以云或客户数据中心的服务形式提供、并经常进行更新和持续创新。这样、客户就可以专注于满足关键业务需求。
- **简化操作。** Intersight使用一个安全的SaaS交付工具、该工具具有通用清单、身份验证和API、可在整个堆栈和所有位置运行、从而简化操作、消除团队之间的孤岛。这样、您就可以管理内部、VM、K8s、无服务器、自动化、在内部和公共云中实现优化并控制成本。
- ***持续优化。** *您可以利用Cisco Intersight在每一层提供的智能以及Cisco TAC提供的智能来持续优化您的环境。这种智能将转换为建议的可自动化操作、以便您可以实时适应任何变化：从移动工作负载和监控物理服务器的运行状况到为您使用的公共云提供成本降低建议。

Cisco Intersight支持两种管理操作模式：UCSM受管模式(Umm)和Intersight受管模式(IMM)。在初始设置互联阵列期间、您可以为光纤连接的Cisco UCS系统选择本机UCSM受管模式(Umm)或视间受管模式(IMM)。在此解决方案 中、使用原生 IMM。下图显示了Cisco Intersight信息板。



VMware vSphere 7.0

VMware vSphere是一个虚拟化平台、可将大量基础架构(包括CPU、存储和网络)作为一个无缝、多功能且动态的操作环境进行全面管理。与管理单个计算机的传统操作系统不同、VMware vSphere可将整个数据中心的基础架构聚合在一起、从而创建一个具有资源的动力中心、这些资源可以快速动态地分配给任何需要的应用程序。

有关 VMware vSphere 及其组件的更多信息，请参阅["VMware vSphere"](#)。

VMware vCenter Server

VMware vCenter Server可通过一个控制台统一管理所有主机和VM、并对集群、主机和VM进行聚合性能监控。通过VMware vCenter Server、管理员可以深入了解计算集群、主机、虚拟机、存储、子操作系统、虚拟基础架构的其他关键组件。VMware vCenter可管理VMware vSphere环境中提供的丰富功能。

详细信息请参见["VMware vCenter"](#)。

硬件和软件版本

这种混合云解决方案可以扩展到任何运行受支持版本的软件、固件和硬件的FlexPod环境，具体定义见：["NetApp 互操作性表工具"](#)，["UCS硬件和软件兼容性"](#)，和["VMware 兼容性指南"](#)。

下表显示了内部FlexPod 硬件和软件版本。

组件	产品	version
计算	Cisco UCS X210c M6	5.0 (1b)
	Cisco UCS互联阵列6454	4.2 (2a)
网络	Cisco Nexus 9336C-x2 NX-OS	9.3 (9)
存储	NetApp AFF A400	ONTAP 9.11.1P2
	适用于 VMware vSphere 的 NetApp ONTAP 工具	9.11

组件	产品	version
	适用于 VMware VAAI 的 NetApp NFS 插件	2.0
	NetApp Active IQ Unified Manager	9.11P1
软件	VMware vSphere	7.0 (U3)
	VMware ESXi nenic 以太网驱动程序	1.0.35.0
	VMware vCenter设备	7.0.3
	Cisco Intersight Assist虚拟设备	1.0.9-342

下表显示了控制台和Cloud Volumes ONTAP版本。

供应商	产品	version
NetApp	控制台	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"下一步：安装和配置。"

安装和配置

"先前版本：解决方案 组件。"

NetApp Cloud Volumes ONTAP 部署

完成以下步骤以配置Cloud Volumes ONTAP 实例：

1. 准备公共云服务提供商环境。

您必须捕获解决方案 配置的公共云服务提供商的环境详细信息。例如、对于Amazon Web Services (AWS) 环境准备、您需要AWS访问密钥、AWS机密密钥以及区域、VPC、子网等其他网络详细信息。

2. 配置VPC端点网关。

要启用VPC与AWS S3服务之间的连接、需要使用VPC端点网关。此操作用于在CVO上启用备份、CVO是网关类型的端点。

3. 访问NetApp Console。

要访问控制台和其他云服务，您需要注册。"[NetApp Console](#)"。有关在控制台帐户中设置工作区和用户的信息，请参阅 "[NetApp Console设置和管理](#)"。您需要一个具有权限的帐户，才能直接从控制台在您的云提供商处部署控制台代理。要获取所需的权限，请参阅 "[NetApp Console的权限摘要](#)"。

4. 部署控制台代理。

在添加 Cloud Volume ONTAP系统之前，必须先部署控制台代理。如果您尝试在没有安装控制台代理的情况下创建第一个Cloud Volumes ONTAP系统，控制台会提示您。要从控制台在 AWS 中部署控制台代理，请参阅以下内容："[AWS 中的控制台代理安装选项](#)"。

5. 在AWS中启动Cloud Volumes ONTAP。

您可以在单系统配置中或在 AWS 中作为 HA 对启动 Cloud Volumes ONTAP 。 ["阅读分步说明"](#)。

有关这些步骤的详细信息、请参见 ["AWS中的Cloud Volumes ONTAP 快速入门指南"](#)。

在这个解决方案中，我们在 AWS 上部署了一个单节点Cloud Volumes ONTAP系统。

内部FlexPod 部署

要了解采用UCS X系列的FlexPod 、VMware和NetApp ONTAP 的设计详细信息、请参见 ["采用Cisco UCS X系列的FlexPod 数据中心"](#) 设计指南。本文档提供了在FlexPod 数据中心基础架构中整合Cisco Intersight-managed UCS X系列平台的设计指导。

有关部署内部FlexPod 实例的信息、请参见 ["本部署指南"](#)。

本文档提供了在FlexPod 数据中心基础架构中整合Cisco Intersight-managed UCS X系列平台的部署指导。本文档介绍了成功部署的配置和最佳实践。

FlexPod 既可以部署在UCS托管模式下、也可以部署在Cisco Intersight托管模式(IMM)下。如果要在UCS托管模式下部署FlexPod 、请参见此内容 ["设计指南"](#) 这是 ["部署指南"](#)。

使用Ansible可以通过基础架构作为代码自动部署FlexPod。下面是用于端到端FlexPod 部署的GitHub存储库的链接：

- 可以看到在UCS托管模式、NetApp ONTAP 和VMware vSphere下使用Cisco UCS的FlexPod 的可识别配置 ["此处"](#)。
- 可以看到在IMM、NetApp ONTAP 和VMware vSphere中使用Cisco UCS的FlexPod 的可识别配置 ["此处"](#)。

内部ONTAP 存储配置

本节介绍特定于此解决方案 的一些重要ONTAP 配置步骤。

1. 在运行iSCSI服务的情况下配置SVM。

```
1. vservers create -vservers Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security
-style unix
2. vservers add-protocols -vservers Healthcare_SVM -protocols iscsi
3. vservers iscsi create -vservers Healthcare_SVM
```

To verify:

```
A400-G0312::> vservers iscsi show -vservers Healthcare_SVM
Vserver: Healthcare_SVM
Target Name:
iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
Target Alias: Healthcare_SVM
Administrative Status: up
```

如果在集群配置期间未安装iSCSI许可证、请确保在创建iSCSI服务之前安装此许可证。

2. 创建FlexVol 卷。

```
1. volume create -vservers Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. 添加用于iSCSI访问的接口。

```
1. network interface create -vservers Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vservers Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vservers Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vservers Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
```

在此解决方案 中、我们创建了四个iSCSI逻辑接口(LIF)、每个节点上两个。

在部署了vCenter并向其添加了所有ESXi主机的情况下启动并运行FlexPod 实例后、我们需要部署一个Linux VM、该VM充当连接和访问NetApp ONTAP 存储的服务器。在此解决方案 中、我们已在vCenter中安装CentOS 8实例。

4. 创建LUN。

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1  
-size 200GB -ostype linux -space-reserve disabled
```

对于EHR操作数据库(ODB)、日志和应用程序工作负载、EHR建议将存储作为iSCSI LUN提供给服务器。如果您的AIX和RHEL操作系统版本支持、则NetApp还支持使用FCP和NVMe/FC、从而提高性能。FCP和NVMe/FC可以同时位于同一个网络结构中。

5. 创建igroup。

```
1. igroup create -vserver Healthcare_SVM -igroup ehr -protocol iscsi  
-ostype linux -initiator iqn.1994-05.com.redhat:8e91e9769336
```

igroup用于允许服务器访问LUN。对于Linux主机、可以在文件中找到服务器IQN
/etc/iscsi/initiatorname.iscsi。

6. 将 LUN 映射到 igroup 。

```
1. lun mapping create -vserver Healthcare_SVM -path  
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

将本地FlexPod存储添加到NetApp Console

使用控制台完成以下步骤，将FlexPod存储添加到系统中。

1. 从导航菜单中，选择“存储”>“系统”。
2. 在“系统”页面上，单击“添加系统”，然后选择“本地部署”。
3. 选择*内部部署ONTAP*。单击 * 下一步 *。
4. 在 "ONTAP 集群详细信息 " 页面上，输入管理员用户帐户的集群管理 IP 地址和密码。然后单击*添加*。
5. 在详细信息和凭据页面上、输入工作环境的名称和问题描述 、然后单击*执行*。

控制台发现ONTAP集群，并将其作为系统添加到“系统”页面。

有关详细信息、请参见页面 ["发现内部ONTAP 集群"](#)。

["下一步：SAN配置。"](#)

SAN 配置

"先前版本：安装和配置。"

本节介绍EHR为使软件与NetApp存储实现最佳集成而需要的主机端配置。在此部分中、我们将专门讨论Linux操作系统的主机集成。使用 "[NetApp 互操作性表工具（IMT）](#)" 验证所有版本的软件和固件。



以下配置步骤特定于此解决方案 中使用的CentOS 8主机。

NetApp主机实用程序套件

NetApp建议在连接到和访问NetApp存储系统的主机的操作系统上安装NetApp Host Utility Kit (Host Utilities)。支持本机Microsoft多路径I/O (MPIO)。操作系统必须支持多路径的非对称逻辑单元访问(ALUA)。安装Host Utilities 可为NetApp存储配置主机总线适配器(HBA)设置。

可以下载NetApp Host Utilities "[此处](#)"。在此解决方案 中、我们已在主机上安装Linux Host Utilities 7.1。

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

发现ONTAP 存储

确保iSCSI服务在应进行登录时正在运行。要为目标上的特定门户或目标上的所有门户设置登录模式、请使用iscsiadm 命令：

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

现在、您可以使用 sanlun 显示有关连接到主机的LUN的信息。确保以root身份登录到主机。

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
```

	device	host		lun	
vserver(cDOT/FlashRay)	lun-pathname	filename	adapter	protocol	size
product					

Healthcare_SVM	/dev/sdb	host33	iSCSI	200g	
cDOT					
	/vol/hc_iscsi_vol/iscsi_lun1				
Healthcare_SVM	/dev/sdc	host34	iSCSI	200g	
cDOT					
	/vol/hc_iscsi_vol/iscsi_lun1				

配置多路径

设备映射程序多路径(DM-Multipath)是Linux中的本机多路径实用程序。它可用于实现冗余并提高性能。它可以聚合或组合服务器和存储之间的多个I/O路径、从而在操作系统级别创建一个设备。

1. 在系统上设置DM-Multipath之前、请确保您的系统已更新并包含 device-mapper-multipath 软件包。

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. 配置文件为 /etc/multipath.conf 文件按如下所示更新配置文件。

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
    path_checker      readsector0
    no_path_retry     fail
}
devices {
    device {
        vendor        "NETAPP  "
        product        "LUN.*"
        no_path_retry  queue
        path_checker    tur
    }
}
```

3. 启用并启动多路径服务。

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start multipathd.service
```

4. 添加可加载的内核模块 dm-multipath 并重新启动多路径服务。最后、检查多路径状态。

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|+- policy='service-time 0' prio=50 status=active
|  `-- 33:0:0:0 sdb 8:16 active ready running
`+- policy='service-time 0' prio=10 status=enabled
  `-- 34:0:0:0 sdc 8:32 active ready running
```



有关这些步骤的详细信息、请参见 ["此处"](#)。

创建物理卷

使用 `pvccreate` 用于初始化块设备以用作物理卷的命令。初始化类似于格式化文件系统。

```
[root@hc-cloud-secure-1 ~]# pvccreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

创建卷组

要从一个或多个物理卷创建卷组、请使用 `vgcreate` 命令：此命令将按名称创建一个新卷组、并至少向其中添加一个物理卷。

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

。 `vgdisplay` 命令可用于以固定形式显示卷组属性(例如大小、块区、物理卷数量等)。

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
--- Volume group ---
VG Name                datavg
System ID
Format                 lvm2
Metadata Areas         1
Metadata Sequence No   1
VG Access               read/write
VG Status               resizable
MAX LV                 0
Cur LV                 0
Open LV                0
Max PV                 0
Cur PV                 1
Act PV                 1
VG Size                 <200.00 GiB
PE Size                 4.00 MiB
Total PE                51199
Alloc PE / Size         0 / 0
Free PE / Size          51199 / <200.00 GiB
VG UUID                 C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

创建逻辑卷

创建逻辑卷时、系统会使用卷组中的物理卷上的可用块区从卷组中划分逻辑卷。

```
[root@hc-cloud-secure-1 ~]# lvcreate -l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

此命令将创建一个名为的逻辑卷 `datalv` 这将使用卷组中的所有未分配空间 `datavg`。

创建文件系统

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv      isize=512    agcount=4, agsize=13106944
blks
        =                        sectsz=4096   attr=2, projid32bit=1
        =                        crc=1          finobt=1, sparse=1, rmapbt=0
        =                        reflink=1      bigtime=0 inobtcount=0
data      =                        bsize=4096   blocks=52427776, imaxpct=25
        =                        sunit=0        swidth=0 blks
naming    =version 2              bsize=4096   ascii-ci=0, ftype=1
log        =internal log          bsize=4096   blocks=25599, version=2
        =                        sectsz=4096   sunit=1 blks, lazy-count=1
realtime  =none                   extsz=4096   blocks=0, rtextents=0
```

创建要挂载的文件夹

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

挂载文件系统

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
devtmpfs	8072804	0	8072804	0%	/dev
tmpfs	8103272	0	8103272	0%	/dev/shm
tmpfs	8103272	9404	8093868	1%	/run
tmpfs	8103272	0	8103272	0%	/sys/fs/cgroup
/dev/mapper/cs-root	45496624	5642104	39854520	13%	/
/dev/sda2	1038336	258712	779624	25%	/boot
/dev/sda1	613184	7416	605768	2%	/boot/efi
tmpfs	1620652	12	1620640	1%	/run/user/42
tmpfs	1620652	0	1620652	0%	/run/user/0
/dev/mapper/datavg-datalv	209608708	1494520	208114188	1%	/file1

有关这些任务的详细信息、请参见页面 ["使用CLI命令管理LVM"](#)。

数据生成

`Dgen.pl`是一个用于 EHR I/O 模拟器 (GenerateIO) 的 perl 脚本数据生成器。LUN 内的数据由 EHR 生成。`Dgen.pl`脚本。该脚本旨在创建与 EHR 数据库中的数据类似的数据。

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .

```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/mapper/datavg-datalv	209608708	178167156	31441552	85%	/file1

运行时、Dgen.pl 默认情况下、脚本使用文件系统的85%来生成数据。

在内部ONTAP 和Cloud Volumes ONTAP 之间配置SnapMirror复制

NetApp SnapMirror 可通过 LAN 或 WAN 高速复制数据，从而在虚拟和传统环境中实现高数据可用性和快速数据复制。在将数据复制到 NetApp 存储系统并持续更新二级数据时，您的数据将保持最新，并在需要时保持可用。不需要外部复制服务器。

完成以下步骤以在内部ONTAP 系统和CVO之间配置SnapMirror复制。

1. 从导航菜单中，选择“存储”>“系统”。
2. 在“系统”中，选择包含源卷的系统，将其拖到要将卷复制到的系统，然后选择“复制”。

其余步骤将介绍如何在Cloud Volumes ONTAP 和内部ONTAP 集群之间创建同步关系。

3. *源和目标对等设置。*如果显示此页面、请为集群对等关系选择所有集群间LIF。
4. *源卷选择。*选择要复制的卷。
5. *目标磁盘类型和分层。*如果目标是Cloud Volumes ONTAP 系统、请选择目标磁盘类型、然后选择是否要启用数据分层。
6. *目标卷名称：*指定目标卷名称并选择目标聚合。如果目标是 ONTAP 集群，则还必须指定目标 Storage VM。
7. *最大传输速率。*指定可传输数据的最大速率(以MB/秒为单位)。
8. 复制策略。*选择一个默认策略或单击*其他策略、然后选择一个高级策略。如需帮助， ["了解复制策略"](#)。

9. *计划。*选择一次性副本或重复计划。有多个默认计划可用。如果您需要其他计划、则必须在上创建新计划 destination cluster 使用 System Manager。

10. 查看。*查看您选择的内容、然后单击*执行。

有关这些配置步骤的详细信息、请参见 ["此处"](#)。

控制台启动数据复制过程。在此阶段，您可以看到在本地ONTAP系统和Cloud Volumes ONTAP之间建立的 复制服务。

在Cloud Volumes ONTAP 集群中、您可以看到新创建的卷。

您还可以验证是否已在内部卷和云卷之间建立SnapMirror关系。

有关复制任务的详细信息、请参见*复制*选项卡。

["接下来：解决方案验证。"](#)

解决方案验证

["先前版本：SAN配置。"](#)

在本节中、我们将介绍一些解决方案 使用情形。

- SnapMirror的主要使用情形之一是数据备份。通过将数据复制到同一集群或远程目标、可以将SnapMirror用作主备份工具。
- 使用灾难恢复环境运行应用程序开发测试(开发/测试)。
- 灾难恢复。
- 数据分发和远程数据访问。

值得注意的是、此解决方案 中验证的相对较少的使用情形并不代表SnapMirror复制的整个功能。

应用程序开发和测试(开发/测试)

为了加快应用程序开发速度、您可以在灾难恢复站点快速克隆复制的数据并将其用于开发/测试应用程序。灾难恢复和开发/测试环境的主机代管可以显著提高备份或灾难恢复设施的利用率、并且按需开发/测试克隆可以根据需要提供尽可能多的数据副本、以便更快地投入生产。

NetApp FlexClone技术可用于快速创建SnapMirror目标FlexVol 卷的读写副本、以便您可以对二级副本进行读写访问、以确认所有生产数据是否可用。

要使用灾难恢复环境执行应用程序开发/测试、请完成以下步骤：

1. 创建生产数据的副本。为此、请为内部卷执行应用程序快照。应用程序快照创建包括三个步骤： Lock， Snap， 和 Unlock。
 - a. 暂停文件系统、以便暂停I/O并保持应用程序一致性。在步骤C中发出unquiesce命令之前、任何写入文件系统的应用程序都会保持等待状态步骤a、b和c通过透明的流程或工作流执行、不会影响应用程序SLA。


```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

此选项请求在进行新修改时冻结指定的文件系统。任何尝试写入冻结文件系统的进程都会被阻止、直到文件系统被解除冻结为止。

- b. 为内部卷创建快照。

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume  
hc_iscsi_vol -snapshot kamini
```

- c. 取消暂停文件系统以重新启动I/O

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

此选项用于取消冻结文件系统并允许操作继续。冻结阻止的任何文件系统修改均不会被阻止、并允许完成。

此外、还可以使用NetApp SnapCenter 执行应用程序一致的快照、NetApp在SnapCenter 中对上述工作流程进行了完整的编排。有关详细信息、请参见 ["此处"](#)。

2. 执行SnapMirror更新操作以使生产系统和灾难恢复系统保持同步。

```
singlecvoaws::> snapmirror update -destination-path  
svm_singlecvoaws:hc_iscsi_vol_copy -source-path  
Healthcare_SVM:hc_iscsi_vol  
  
Operation is queued: snapmirror update of destination  
"svm_singlecvoaws:hc_iscsi_vol_copy".
```

也可以通过NetApp ConsoleGUI 的“复制”选项卡执行SnapMirror更新。

3. 根据先前创建的应用程序快照创建FlexClone实例。

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW  
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy  
-junction-active true -foreground true -parent-snapshot kamini  
  
[Job 996] Job succeeded: Successful
```

对于上一项任务、也可以创建新的快照、但您必须按照上述相同步骤来确保应用程序一致性。

4. 激活FlexClone卷以在云中启动EHR实例。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
```

Vserver	Path	Igroup	LUN ID	Protocol
svm_singlecvoaws	/vol/kamini_clone/iscsi_lun1	ehr-igroup	0	iscsi

5. 在云中的EHR实例上执行以下命令以访问数据或文件系统。

a. 发现ONTAP 存储。检查多路径状态。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
```

Output:

controller(7mode/E-Series)/	device	host	lun
vserver(cDOT/FlashRay) lun-pathname filename	adapter	protocol	size
product			
svm_singlecvoaws	/dev/sda	host2	iSCSI 200g
cDOT	/vol/kamini_clone/iscsi_lun1		

```
sudo multipath -ll
```

Output:

```
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. 激活卷组。

```
sudo vgchange -ay datavg
```

Output:

```
1 logical volume(s) in volume group "datavg" now active
```

c. 挂载文件系统并显示文件系统信息的摘要。

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                                1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv 209608708 183987096 25621612   88%
/file1
```

这证明您可以使用灾难恢复环境进行应用程序开发/测试。通过在灾难恢复存储上执行应用程序开发/测试、您可以更多地利用资源、否则这些资源可能会在大部分时间处于闲置状态。

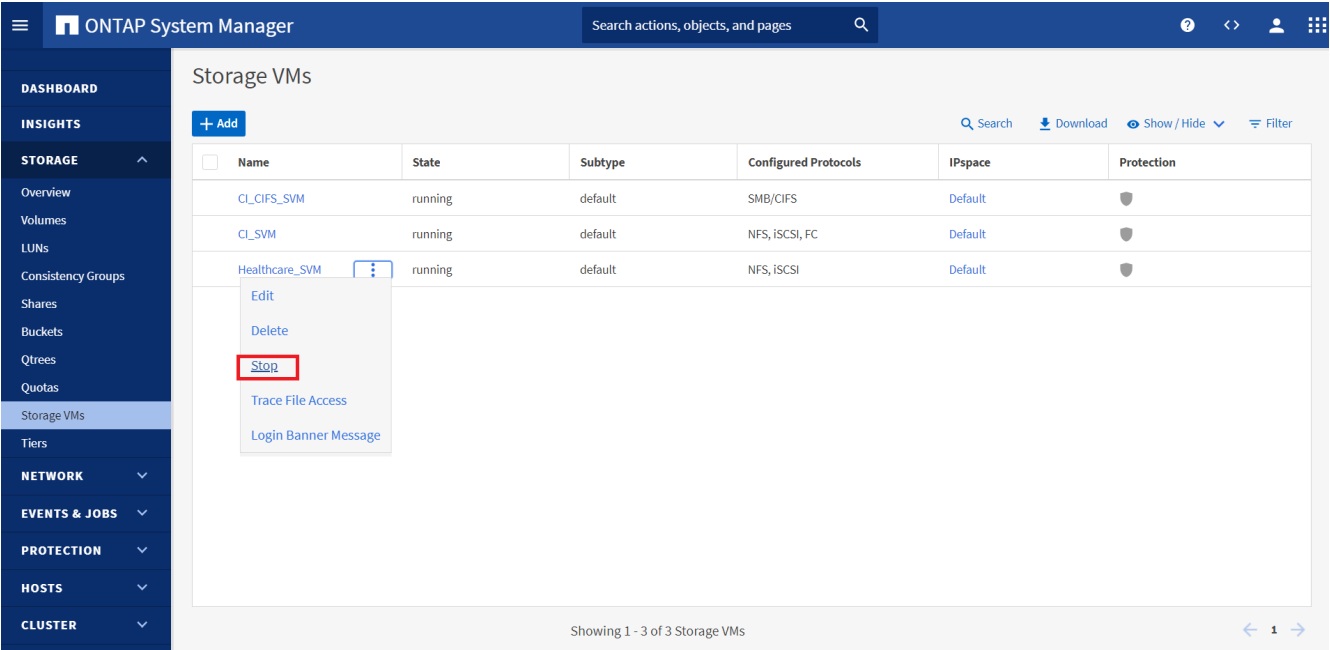
灾难恢复

SnapMirror技术也用作灾难恢复计划的一部分。如果将关键数据复制到其他物理位置、则发生严重灾难时、不必对业务关键型应用程序的数据长时间不可用进行发生原因 处理。客户端可以通过网络访问复制的数据、直到生产站点从损坏、意外删除、自然灾难等中恢复为止。

如果要故障恢复到主站点、SnapMirror可提供一种高效的方法来重新同步灾难恢复站点与主站点、只需反转SnapMirror关系、即可仅将更改过的数据或新数据从灾难恢复站点传输回主站点。主生产站点恢复正常应用程序操作后、SnapMirror将继续向灾难恢复站点传输数据、而无需再进行基线传输。

要验证成功的灾难恢复方案、请完成以下步骤：

- 1. 通过停止托管内部ONTAP 卷的SVM在源(生产)端模拟灾难 (hc_iscsi_vol) 。



确保已在FlexPod 实例中的内部ONTAP 和AWS中的Cloud Volumes ONTAP 之间设置SnapMirror复制、以

便您可以频繁创建应用程序快照。

SVM停止运行后，`hc\_iscsi\_vol`控制台中不显示音量。

2. 在CVO中激活灾难恢复。

- a. 中断本地ONTAP 和Cloud Volumes ONTAP 之间的SnapMirror复制关系、并提升CVO目标卷(hc_iscsi_vol_copy)到生产环境。

断开SnapMirror关系后、目标卷类型将从数据保护(DP)更改为读/写(RW)。

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume          type
-----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

- b. 激活Cloud Volumes ONTAP 中的目标卷以在云中的EC2实例上启动EHR实例。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver      Path                                Igroup    LUN ID
Protocol
-----
svm_singlecvoaws
          /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0      iscsi
```

- c. 要访问云中EHR实例上的数据和文件系统、请首先发现ONTAP 存储并验证多路径状态。

```

sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/          device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
-----
-----
svm_singleecvoaws                    /dev/sda  host2      iSCSI      200g
cDOT
                                /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running

```

d. 然后激活卷组。

```

sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active

```

e. 最后、挂载文件系统并显示文件系统信息。

```

sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096 25621612   88%
/file1

```

此输出显示、用户可以通过网络访问复制的数据、直到生产站点从灾难中恢复为止。

f. 反转SnapMirror关系。此操作将反转源卷和目标卷的角色。

执行此操作时、原始源卷中的内容将被目标卷的内容覆盖。当您要重新激活脱机的源卷时，这非常有用。

现在是CVO卷 (hc_iscsi_vol_copy)将成为源卷、内部卷也将成为源卷 (hc_iscsi_vol)将成为目标卷。

在上次数据复制和源卷禁用之间写入到原始源卷的任何数据都不会保留。

- a. 要验证对CVO卷的写入访问、请在云中的EHR实例上创建一个新文件。

```
cd /file1/  
sudo touch newfile
```

当生产站点关闭时、客户端仍可访问数据、并对Cloud Volumes ONTAP 卷执行写入操作、该卷现在是源卷。

如果要故障恢复到主站点、SnapMirror可提供一种高效的方法来重新同步灾难恢复站点与主站点、只需反转SnapMirror关系、即可仅将更改过的数据或新数据从灾难恢复站点传输回主站点。主生产站点恢复正常应用程序操作后、SnapMirror将继续向灾难恢复站点传输数据、而无需再进行基线传输。

本节说明了在生产站点发生灾难时成功解决灾难恢复方案的方法。现在、数据可以安全地由应用程序使用、这些应用程序现在可以在源站点完成还原期间为客户端提供服务。

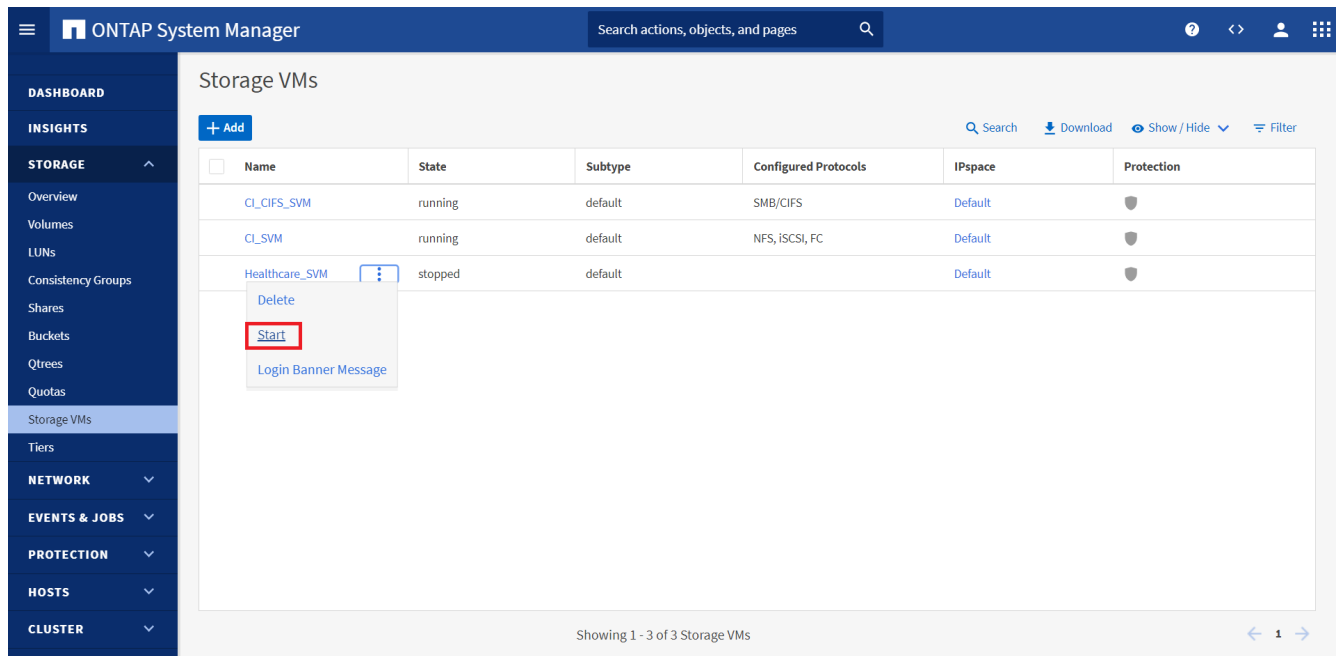
验证生产站点上的数据

恢复生产站点后、您必须确保还原原始配置、并且客户端能够从源站点访问数据。

在本节中、我们将讨论启动源站点、恢复内部ONTAP 和Cloud Volumes ONTAP 之间的SnapMirror关系、并最终对源端执行数据完整性检查

以下操作步骤 可用于验证生产站点上的数据：

1. 确保源站点现在已启动。为此、请启动托管内部ONTAP 卷的SVM (hc_iscsi_vol) 。



2. 中断Cloud Volumes ONTAP 和内部ONTAP 之间的SnapMirror复制关系、并提升内部卷 (hc_iscsi_vol)恢复生产。

断开SnapMirror关系后、内部卷类型将从数据保护(DP)更改为读/写(RW)。

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver          volume          type
-----
Healthcare_SVM hc_iscsi_vol RW
```

3. 反转SnapMirror关系。现在、是内部部署的ONTAP 卷 (hc_iscsi_vol)将成为源卷和之前的源卷、并成为Cloud Volumes ONTAP 卷 (hc_iscsi_vol_copy)将成为目标卷。

通过执行以下步骤、我们已成功还原原始配置。

4. 重新启动内部EHR实例。挂载文件系统并验证 newfile 在生产中断时、您在云中的EHR实例上创建的数据现在也存在。

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01 dir05 dir09 dir13 dir17 dir21 dir25 dir29 dir33 dir37 dir41 dir45 dir49 dir53 dir57 dir61 dir65 dir69 dir73 dir77 kamini
dir02 dir06 dir10 dir14 dir18 dir22 dir26 dir30 dir34 dir38 dir42 dir46 dir50 dir54 dir58 dir62 dir66 dir70 dir74 dir78 latest file
dir03 dir07 dir11 dir15 dir19 dir23 dir27 dir31 dir35 dir39 dir43 dir47 dir51 dir55 dir59 dir63 dir67 dir71 dir75 dir79 newfile
dir04 dir08 dir12 dir16 dir20 dir24 dir28 dir32 dir36 dir40 dir44 dir48 dir52 dir56 dir60 dir64 dir68 dir72 dir76 dir80
```

我们可以推断、从源到目标的数据复制已成功完成、并且数据完整性已保持不变。这样就完成了对生产站点上数据的验证。

"接下来：总结。"

结论

"先前版本：解决方案 验证。"

构建混合云是大多数医疗保健组织随时提供数据可用性的目标。在此解决方案 中、我们实施了采用Cloud Volumes ONTAP 的FlexPod 混合云解决方案、利用NetApp SnapMirror复制技术验证了一些用于备份和恢复医疗保健应用程序和工作负载的用例。

FlexPod 是Cisco和NetApp战略合作伙伴关系中经过严格测试和预先验证的融合基础架构、旨在提供可预测的低延迟系统性能和高可用性。这种方法可为EHR系统用户带来较高的舒适程度、并最终获得最佳响应时间。

借助NetApp、您可以像在内部数据中心运行NetApp存储功能一样、在云中运行EHR生产、灾难恢复、备份或分层。借助NetApp Cloud Volumes ONTAP 、NetApp可提供在云中有效运行EHR所需的企业级功能和性能。NetApp云选项可提供基于iSCSI的块和基于NFS或SMB的文件。

此解决方案 可满足医疗保健组织的需求、并使其能够朝着数字化转型迈进一步。它还可以帮助他们高效地管理应用程序和工作负载。

["下一步：从何处查找追加信息。"](#)

从何处查找追加信息

["上一篇：结论。"](#)

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- FlexPod 主页

["https://www.flexpod.com"](https://www.flexpod.com)

- 适用于FlexPod 的Cisco验证设计和部署指南

["https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"](https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html)

- NetApp Console

["https://console.netapp.com/"](https://console.netapp.com/)

- NetApp Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html)

- 在 AWS 中快速启动 Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html)

- SnapMirror 复制

["https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"](https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html)

- TR-3928：《NetApp Epic最佳实践》

<https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf>

- TR-4693：《适用于 Epic EHR 的 FlexPod 数据中心部署指南》

["https://www.netapp.com/media/10658-tr-4693.pdf"](https://www.netapp.com/media/10658-tr-4693.pdf)

- 适用于Epic的FlexPod

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.htm
l"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html)

- NetApp 互操作性表工具

["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)

- Cisco UCS 硬件和软件互操作性工具

["http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"](http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- VMware 兼容性指南

["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2023年3月	初始版本

适用于Google云平台的FlexPod 混合云与NetApp Cloud Volumes ONTAP 和Cisco Intersight

TR-4939：《适用于Google云平台的FlexPod 混合云与NetApp Cloud Volumes ONTAP 和Cisco Intersight》

NetApp公司Ruchika Lahoti

简介

利用灾难恢复(DR)保护数据是实现业务连续性的一个关键目标。灾难恢复允许组织将业务运营故障转移到二级位置、然后高效可靠地恢复并故障恢复到主站点。自然灾害、网络故障、软件漏洞和人为错误等多种问题都使制定灾难恢复策略成为IT的首要任务。

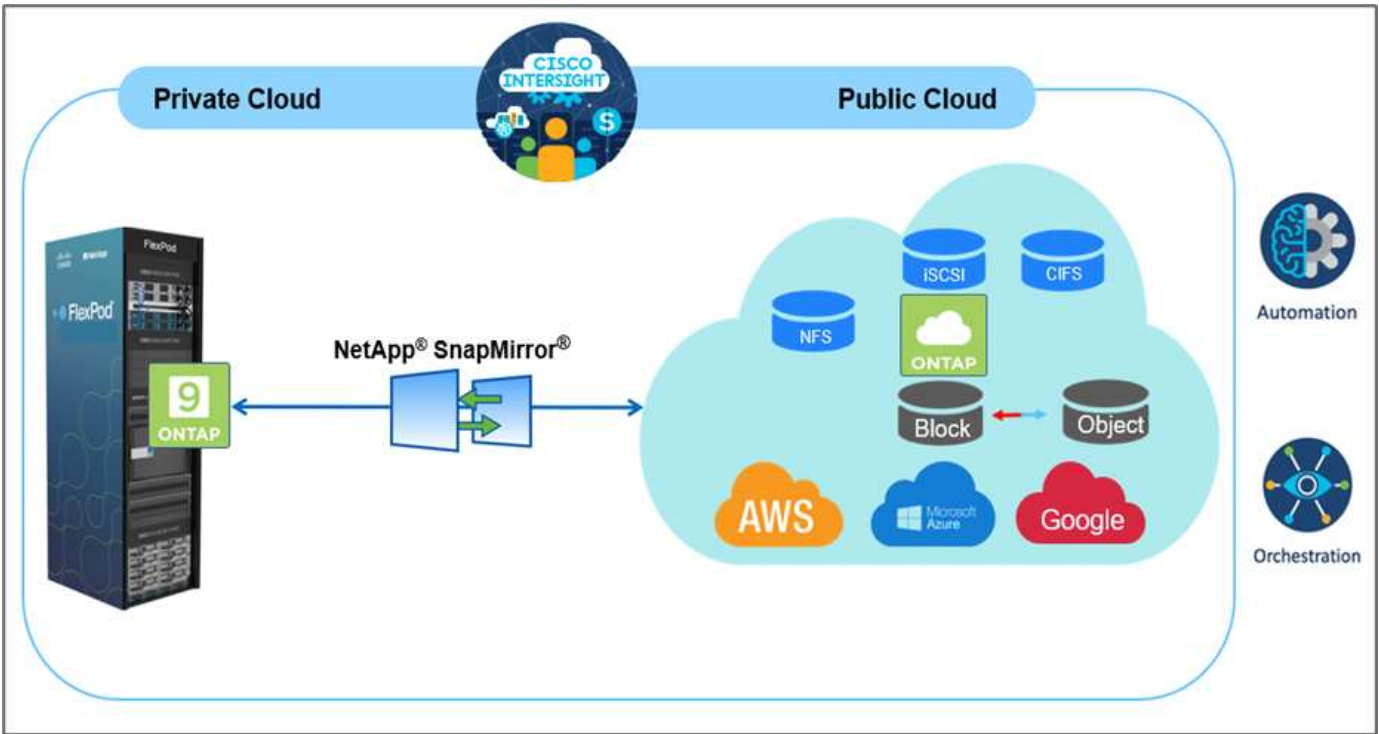
对于灾难恢复、主站点上运行的所有工作负载都必须在灾难恢复站点上复制。组织还必须拥有所有企业数据的最新副本、包括数据库、文件服务、NFS和iSCSI存储等。由于生产环境中的数据会不断更新、因此必须定期将更改传输到灾难恢复站点。

对于大多数组织来说、部署灾难恢复环境都是一项挑战、因为需要基础架构和站点独立性。所需的资源数量以及设置、测试和维护二级数据中心的成本可能非常高、通常会接近整个生产环境的成本。在保持数据持续同步并建立无缝故障转移和故障恢复的同时、尽可能减少数据占用空间并提供充分的保护、这是一项极具挑战性的任务。构建灾难恢复站点后、接下来的挑战是从生产环境复制数据并保持数据同步。

本技术报告将FlexPod 融合基础架构解决方案、基于Google Cloud的NetApp Cloud Volumes ONTAP 和Cisco Intersight汇集在一起、构成了一个用于灾难恢复的混合云数据中心。在本解决方案 中、我们将讨论如何使用Cisco Intersight Cloud Orchestrator设计和执行内部ONTAP 工作流。我们还将讨论部署NetApp Cloud

Volumes ONTAP 以及使用适用于HashiCorp Terraform的Cisco Intersight服务在FlexPod 和Cloud Volumes ONTAP 之间编排和自动化数据复制和灾难恢复。

下图提供了解决方案 概述。



此解决方案 具有多种优势、包括：

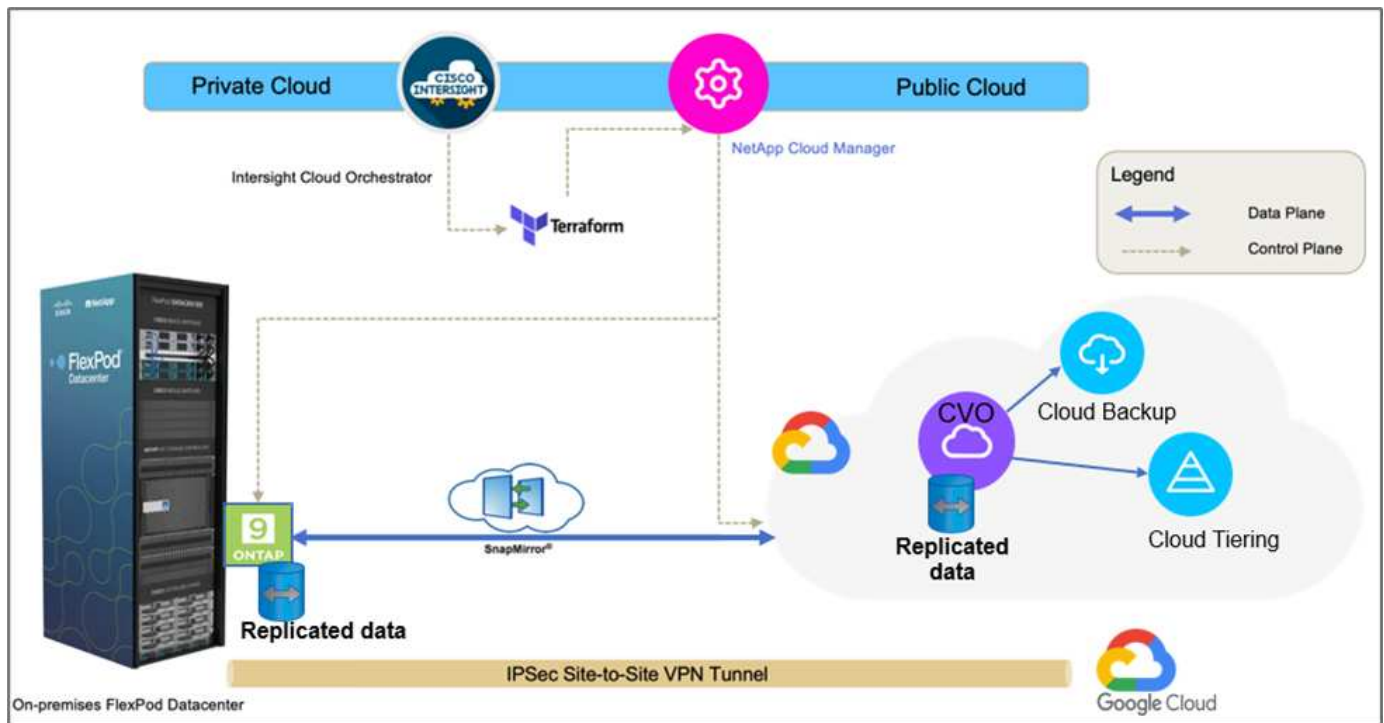
- 流程编排和自动化。 Cisco Intersight通过提供通过自动化交付的一致流程编排框架、简化了FlexPod 混合云基础架构的日常运营。
- 自定义保护。 Cloud Volumes ONTAP 提供从ONTAP 到云的块级数据复制、通过增量更新使目标保持最新。用户可以根据所传输源的更改、指定每5分钟或每小时的同步计划。
- *无缝故障转移和故障恢复。*发生灾难时、存储管理员可以快速故障转移到云卷。恢复主站点后、在灾难恢复环境中创建的新数据将同步回源卷、从而重新建立二级数据复制。
- *效率：*二级云副本的存储空间和成本通过数据压缩、精简配置和重复数据删除进行优化。数据以经过压缩和重复数据删除的形式在块级别传输、从而提高传输速度。数据也会自动分层到低成本对象存储、并且只有在访问时才会返回到高性能存储、例如在灾难恢复情形下。这样可以显著降低持续存储成本。
- *提高了IT工作效率。*使用Intersight作为一个安全的企业级基础架构和应用程序生命周期管理平台、可以简化解决方案 的配置管理以及手动任务的大规模自动化。

audience

本文档的受众包括但不限于：销售工程师、现场顾问、专业服务人员、IT经理、 合作伙伴工程师、站点可靠性工程师、云架构师、云工程师以及希望利用专为提高IT效率和实现IT创新而构建的基础架构的客户。

解决方案 拓扑

本节介绍解决方案 的逻辑拓扑。下图显示了内部FlexPod 环境、在Google Cloud上运行的NetApp Cloud Volumes ONTAP 、Cisco Intersight和NetApp Cloud Manager的解决方案 拓扑。



控制平面和数据平面会在端点之间清晰地指示。数据平面使用安全的站点到站点VPN连接将FlexPod 全闪存FAS上运行的ONTAP 实例连接到Google Cloud上的NetApp Cloud Volumes ONTAP 实例。

将工作负载数据从FlexPod 复制到NetApp Cloud Volumes ONTAP 由NetApp SnapMirror处理、整个过程使用Cisco Intersight Cloud Orchestrator在内部环境和云环境中进行协调。Cisco Intersight Cloud Orchestrator使用适用于NetApp Cloud Manager的Terraform资源提供商来执行与NetApp Cloud Volumes ONTAP 部署相关的操作并建立数据复制关系。



此解决方案 还支持将驻留在NetApp Cloud Volumes ONTAP 实例中的冷数据备份和分层到Google云存储。

"接下来：解决方案 组件。"

解决方案组件

"上一步：解决方案概述。"

FlexPod

FlexPod 是一组定义的硬件和软件、可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 包括NetApp ONTAP 存储、Cisco Nexus网络、Cisco MDS存储网络和Cisco统一计算系统(Cisco UCS)。该设计非常灵活、可以将网络、计算和存储安装到一个数据中心机架中、也可以根据客户的数据中心设计进行部署。端口密度允许网络组件容纳多种配置。

Cisco Intersight

Cisco Intersight是一个SaaS平台、可为传统和云原生应用程序和基础架构提供智能自动化、可观察性和优化功能。该平台有助于推动IT团队的变革、并提供专为混合云设计的运营模式。Cisco Intersight具有以下优势：

- *交付速度更快。*由于采用基于敏捷性的软件开发模式、可从云或客户数据中心以服务的形式交付、并经常进行更新和持续创新。这样、客户就可以专注于加快业务部门的交付速度。

- ***简化操作。***通过使用一个安全的SaaS交付工具以及通用清单、身份验证和API在整个堆栈和所有位置运行、简化操作、消除团队之间的孤岛。从内部管理物理服务器和虚拟机管理程序到虚拟机、K8s、无服务器、自动化、在内部和公有云之间实现优化和成本控制。
- ***持续优化。***利用Cisco Intersight在每一层提供的智能以及Cisco TAC持续优化您的环境。这种智能功能可转换为建议的可自动操作、因此您可以实时适应每个变化：从移动工作负载和监控物理服务器的运行状况到您使用的公有云的成本降低建议。

Cisco Intersight支持两种管理操作模式：UCSM受管模式(Umm)和Intersight受管模式(IMM)。在初始设置互联阵列期间、您可以为光纤连接的Cisco UCS系统选择原生 Umm或IMM。在此解决方案 中、使用原生 IMM。

Cisco Intersight许可

Cisco Intersight使用基于订阅的许可证、该许可证包含多个层。

Cisco Intersight许可证层如下：

- *** Cisco Intersight Essentials。***包括所有基本功能以及以下功能：
 - Cisco UCS Central
 - Cisco IMC Supervisor授权
 - 使用服务器配置文件进行基于策略的配置
 - 固件管理
 - 与硬件兼容性列表(Hardware Compatibility List、HCL)的兼容性评估
- *** Cisco Intersight Advantage。***包括Essentials层的特性和功能以及以下功能：
 - 在物理计算、网络、存储、VMware虚拟化和AWS公有云之间使用小工具、清单、容量、利用率功能以及跨域清单关联。
 - Cisco安全咨询服务、客户可以在此服务中收到有关受影响端点设备的重要安全警报和现场通知。
- *** Cisco Intersight Premier。***除了在高级版中提供的功能之外、Cisco Intersight Premier还提供以下功能：
 - 适用于Cisco和第三方计算、网络、存储、集成系统、虚拟化、容器和公共云平台
 - Cisco UCS Director的完整订阅授权、无需额外费用。

有关Intersight许可以及每个许可支持的功能的详细信息、请参见 ["此处"](#)。



在本解决方案 中、我们使用适用于HashiCorp Terraform的Intersight Cloud Orchestrator和Intersight服务。具有Intersight Premier许可证的用户可以使用这些功能、因此必须启用此许可层。

Terraform Cloud与ICO集成

您可以使用Cisco Intersight Cloud Orchestrator (ICO)创建和执行调用Terraform Cloud (TFC) API的工作流。调用Web API请求任务支持将Terraform Cloud作为目标、并且可以使用HTTP方法为其配置Terraform Cloud API。因此、工作流可以组合使用多个任务、这些任务使用通用API任务和其他操作调用多个Terraform Cloud API。要使用ICO功能、您需要获得Premier许可证。

Cisco Intersight Assist

Cisco Intersight Assist可帮助您将端点设备添加到Cisco Intersight。一个数据中心可能包含多个不直接与Cisco

Intersight连接的设备。Cisco Intersight支持但不直接连接到任何设备都需要连接机制。Cisco Intersight Assist可提供此连接机制、并帮助您将设备添加到Cisco Intersight中。

Cisco Intersight Virtual Appliance中提供了Cisco Intersight Assist、该设备以Open Virtual Appliance (OVA)文件格式包含的可部署虚拟机的形式进行分发。您可以在ESXi服务器上安装此设备。有关详细信息，请参见 "[《Cisco Intersight Virtual Appliance入门指南》](#)"。

将Intersight Assist申请到Intersight后、您可以使用通过Intersight Assist选项申请端点设备。有关详细信息，请参见 "[入门](#)"。

NetApp Cloud Volumes ONTAP

- 利用内置的重复数据删除、数据压缩、精简配置和克隆功能最大限度地降低存储成本。
- 在云环境发生故障时提供企业级可靠性和持续运营。
- Cloud Volumes ONTAP 使用行业领先的复制技术NetApp SnapMirror将内部数据复制到云中、因此可以轻松地为多种使用情形提供二级副本。
- Cloud Volumes ONTAP 还与Cloud Backup Service 集成、提供备份和还原功能、以保护和长期归档云数据。
- 按需在高性能和低性能存储池之间切换、而无需使应用程序脱机。
- 使用NetApp SnapCenter 提供Snapshot副本的一致性。
- Cloud Volumes ONTAP 支持数据加密，并提供防病毒和勒索软件保护。
- 与 Cloud Data sense 集成有助于您了解数据环境并识别敏感数据。

Cloud Central

Cloud Central提供了一个中央位置、用于访问和管理NetApp云数据服务。这些服务使您能够在云中运行关键应用程序、创建自动化灾难恢复站点、备份 SaaS 数据、并在多个云中有效地迁移和控制数据。有关详细信息，请参见 "[Cloud Central](#)"。

Cloud Manager

Cloud Manager是一款基于SaaS的企业级管理平台、IT专家和云架构师可以利用NetApp云解决方案集中管理其混合多云基础架构。它提供了一个集中式系统、用于查看和管理内部和云存储、以支持多个混合云提供商和客户。有关详细信息，请参见 "[Cloud Manager](#)"。

连接器

借助Connector、Cloud Manager可以管理公有 云环境中的资源和流程。要使用Cloud Manager提供的许多功能、需要使用Connector实例、并且可以部署在云或内部网络中。连接器在以下位置受支持：

- AWS
- Microsoft Azure
- Google Cloud
- 内部部署

NetApp Active IQ Unified Manager

借助NetApp Active IQ Unified Manager 、您可以通过一个经过重新设计的直观界面监控ONTAP 存储集群、该

界面可利用社区智慧和AI分析提供智能信息。它可以全面洞察存储环境及其运行的虚拟机的运行情况、性能和主动式情况。当存储基础架构发生问题描述 时、Unified Manager可以通知您问题描述 的详细信息、以帮助识别根发生原因。通过虚拟机信息板、您可以查看虚拟机的性能统计信息、以便调查从vSphere主机向下经过网络并最终到达存储的整个I/O路径。

某些事件还提供了更正问题描述 所需的补救措施。您可以为事件配置自定义警报、以便在发生时、通过电子邮件和SNMP陷阱通知您。Active IQ Unified Manager 可以预测容量和使用趋势、以便在出现问题之前主动采取行动、从而防止做出长期可能导致其他问题的被动短期决策、从而为用户的存储需求进行规划。

VMware vSphere

VMware vSphere是一个虚拟化平台、可将大量基础架构(包括CPU、存储和网络等资源)作为一个无缝、多功能且动态的操作环境进行全面管理。与管理单个计算机的传统操作系统不同、VMware vSphere可将整个数据中心的基础架构聚合在一起、从而创建一个具有资源的动力中心、这些资源可以快速动态地分配给任何需要的应用程序。

有关VMware vSphere的详细信息、请参见 ["此链接"](#)。

VMware vSphere vCenter

VMware vCenter Server可通过一个控制台统一管理所有主机和VM、并对集群、主机和VM进行聚合性能监控。通过VMware vCenter Server、管理员可以深入了解计算集群、主机、虚拟机、存储、子操作系统、 虚拟基础架构的其他关键组件。VMware vCenter可管理VMware vSphere环境中提供的丰富功能。

硬件和软件版本

此混合云解决方案 可以扩展到运行NetApp互操作性表工具和Cisco UCS硬件兼容性列表中定义的受支持软件、固件和硬件版本的任何FlexPod 环境。

在我们的内部环境中用作基线平台的FlexPod 解决方案 是根据所述准则和规格进行部署的 ["此处"](#)。

此环境中的网络基于ACI。有关详细信息，请参见 ["此处"](#)。

- 有关详细信息、请参见以下链接：
- ["NetApp 互操作性表工具"](#)
- ["VMware 兼容性指南"](#)
- ["Cisco UCS 硬件和软件互操作性工具"](#)

下表显示了FlexPod 硬件和软件版本。

组件	产品	version
计算	Cisco UCS X210C-M6	5.0 (1b)
	Cisco UCS互联阵列6454	4.2 (2a)
网络	Cisco Nexus 9332C (Spine)	14.2 (7秒)
	Cisco Nexus 9336C-x2 (叶)	14.2 (7秒)
	Cisco ACI	4.2 (7秒)
存储	NetApp AFF A220	9.11.1

组件	产品	version
	适用于 VMware vSphere 的 NetApp ONTAP 工具	9.10.
	适用于VMware VAAI的NetApp NFS 插件	2.0-15
	Active IQ Unified Manager	9.11
软件	vSphere ESXi	7.0 (U3)
	VMware vCenter设备	7.0.3
	Cisco Intersight Assist虚拟设备	1.0.11-306

Terraform配置在Terraform Cloud for Business帐户上执行。Terraform配置使用适用于NetApp Cloud Manager的Terraform提供程序。

下表列出了供应商、产品和版本。

组件	产品	version
HashiCorp	Terraform	1.2.7.

下表显示了Cloud Manager和Cloud Volumes ONTAP 的版本。

组件	产品	version
NetApp	Cloud Volumes ONTAP	9.11
	Cloud Manager	3.9.21

"接下来：安装和配置—部署FlexPod。"

安装和配置

部署FlexPod

"先前版本：解决方案 组件。"

要了解FlexPod 设计和部署详细信息、包括各种设计要素的配置以及相关最佳实践、请参见 ["经过Cisco验证的FlexPod 设计"](#)。

FlexPod 既可以部署在UCS托管模式下、也可以部署在Cisco Intersight托管模式下。如果您要在UCS托管模式下部署FlexPod 、可以找到最新的Cisco验证设计 ["此处"](#)。

Cisco Unified Compute System (Cisco UCS) X系列是一款全新的模块化计算系统、可通过云进行配置和管理。它旨在满足现代应用程序的需求、并通过适应性强、适应未来需求的模块化设计提高运营效率、灵活性和可扩展性。有关在FlexPod 基础架构中整合Cisco Intersight-托管UCS X系列平台的设计指南、请参见 ["此处"](#)。

可以找到部署了Cisco ACI的FlexPod ["此处"](#)。

"接下来：Cisco Intersight配置。"

Cisco Intersight配置

"先前版本：部署FlexPod。"

要配置Cisco Intersight和Intersight Assist、请参见Cisco为FlexPod 发现的经验验证的设计 "[此处](#)"。

"接下来：Terraform Cloud Integration with ICO前提条件。"

Terraform Cloud Integration with ICO前提条件

"先前版本：Cisco Intersight配置。"

操作步骤 1：连接Cisco Intersight和Terraform Cloud

1. 通过提供相关的Terraform Cloud帐户详细信息来声明或创建Terraform云目标。
2. 为私有云创建Terraform Cloud Agent目标、以便客户可以在数据中心安装代理并与Terraform Cloud进行通信。

有关详细信息、请参见 "[此链接](#)"。

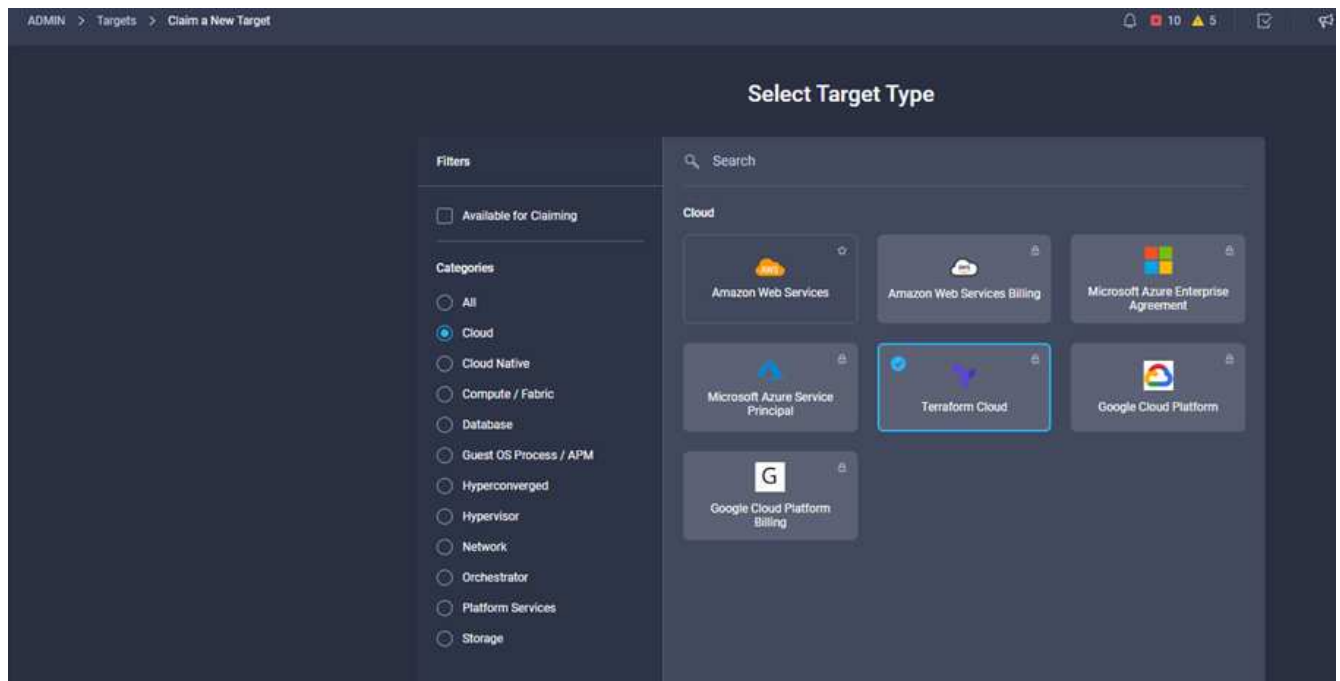
操作步骤 2：生成用户令牌

在为Terraform Cloud添加目标时、您必须从Terraform Cloud设置页面提供用户名和API令牌。

1. 登录到Terraform Cloud并转到*用户令牌*： "<https://app.terraform.io/app/settings/tokens>"。
2. 单击*创建新的API令牌*。
3. 分配一个要记住的名称并将令牌保存在安全位置。

操作步骤 3：声明Terraform云目标

1. 使用帐户管理员、设备管理员或设备技术人员权限登录到Intersight。
2. 导航到*管理>目标>申请新目标*。
3. 在*类别*中、单击*云*。
4. 单击* Terraform Cloud*并单击*开始*。



5. 输入目标的名称、Terraform Cloud的用户名、API令牌以及Terraform Cloud中的默认组织、如下图所示。
6. 在*默认受管主机*字段中、确保添加以下链接以及其他受管主机：
 - github.com
 - github-releases.githubusercontent.com

如果输入的所有内容均正确无误、您将在* Intersight Targets*部分中看到Terraform Cloud目标。

操作步骤 4：添加Terraform云代理

前提条件

- Terraform Cloud目标。
- 在部署Terraform Cloud Agent之前、向Intersight申请了Intersight协助。



每次协助只能申请五名代理。



创建与Terraform的连接后、必须启动Terraform代理才能执行Terraform代码。

1. 从Terraform Cloud目标的下拉列表中单击*声明Terraform Cloud Agent*。
2. 输入Terraform Cloud代理的详细信息。以下屏幕截图显示了Terraform代理的配置详细信息。

Terraform Cloud target

Name *
flexpod-solution-terraform-agent

Intersight Assist *
g13-intersight-appliance.fpmc.sa

Terraform Cloud Organization *
cisco-intersight-gc

Terraform Cloud Agent Pool Name *
flexpod-solution-agent-pool

Managed Hosts

Hostname / IP Address / Subnets *	
github.com	
github-releases.githubusercontent.com	



您可以更新任何Terraform Agent属性。如果目标处于*未连接*状态且从未处于*已连接*状态、则尚未为Terraform代理生成令牌。

在代理验证成功并生成代理令牌后、您无法重新配置组织和/或代理池。Terraform代理的成功部署状态为*已连接*。

启用并申请Terraform Cloud集成后、您可以在Cisco Intersight Assist中部署一个或多个Terraform Cloud代理。Terraform Cloud代理将建模为Terraform Cloud目标的子目标。申请代理目标时、您会看到一条消息、指示目标申请正在进行中。

几秒钟后、目标将移至*已连接*状态、Intersight平台会将HTTPS数据包从代理路由到Terraform Cloud网关。

您的Terraform代理应正确声明、并应在目标下显示为*已连接*。

"下一步：配置公有 云服务提供商。"

配置公有 云服务提供商

"先前版本：Terraform Cloud Integration with ICO前提条件。"

操作步骤 1：访问NetApp Cloud Manager

要访问NetApp Cloud Manager和其他云服务、您需要注册 "NetApp Cloud Central"。



要在Cloud Central帐户中设置工作空间 and 用户、请单击 ["此处"](#)。

操作步骤 2：部署连接器

要在Google Cloud中部署Connector、请参见此内容 ["链接"](#)。

["接下来：自动部署混合云NetApp存储。"](#)

自动部署混合云NetApp存储

["先前版本：配置公有 云服务提供商。"](#)

Google Cloud

您必须先启用API并创建一个服务帐户、以便为Cloud Manager提供部署和管理与Connector位于同一项目或不同项目中的Cloud Volumes ONTAP 系统的权限。

在Google Cloud项目中部署连接器之前、请确保此连接器未在内部或其他云提供商中运行。

在直接从 Cloud Manager 部署 Connector 之前，必须具有两组权限：

- 您需要使用有权从Cloud Manager启动Connector VM实例的Google帐户部署Connector。
- 部署Connector时、系统会提示您选择VM实例。Cloud Manager 可从服务帐户中获得代表您创建和管理 Cloud Volumes ONTAP 系统的权限。权限可通过向服务帐户附加自定义角色来提供。您需要设置两个YAML文件、这些文件包含用户和服务帐户所需的权限。了解如何使用 ["用于设置权限的YAML文件"](#) 此处。

请参见 ["此详细视频"](#) 所有必需的前提条件。

Cloud Volumes ONTAP 部署模式和架构

Cloud Volumes ONTAP 可作为单节点系统和高可用性(HA)节点对在Google Cloud中使用。根据要求、我们可以选择Cloud Volumes ONTAP 部署模式。不支持将单节点系统升级到 HA 对。如果要在单节点系统和HA对之间切换、则必须部署新系统并将现有系统中的数据复制到新系统。

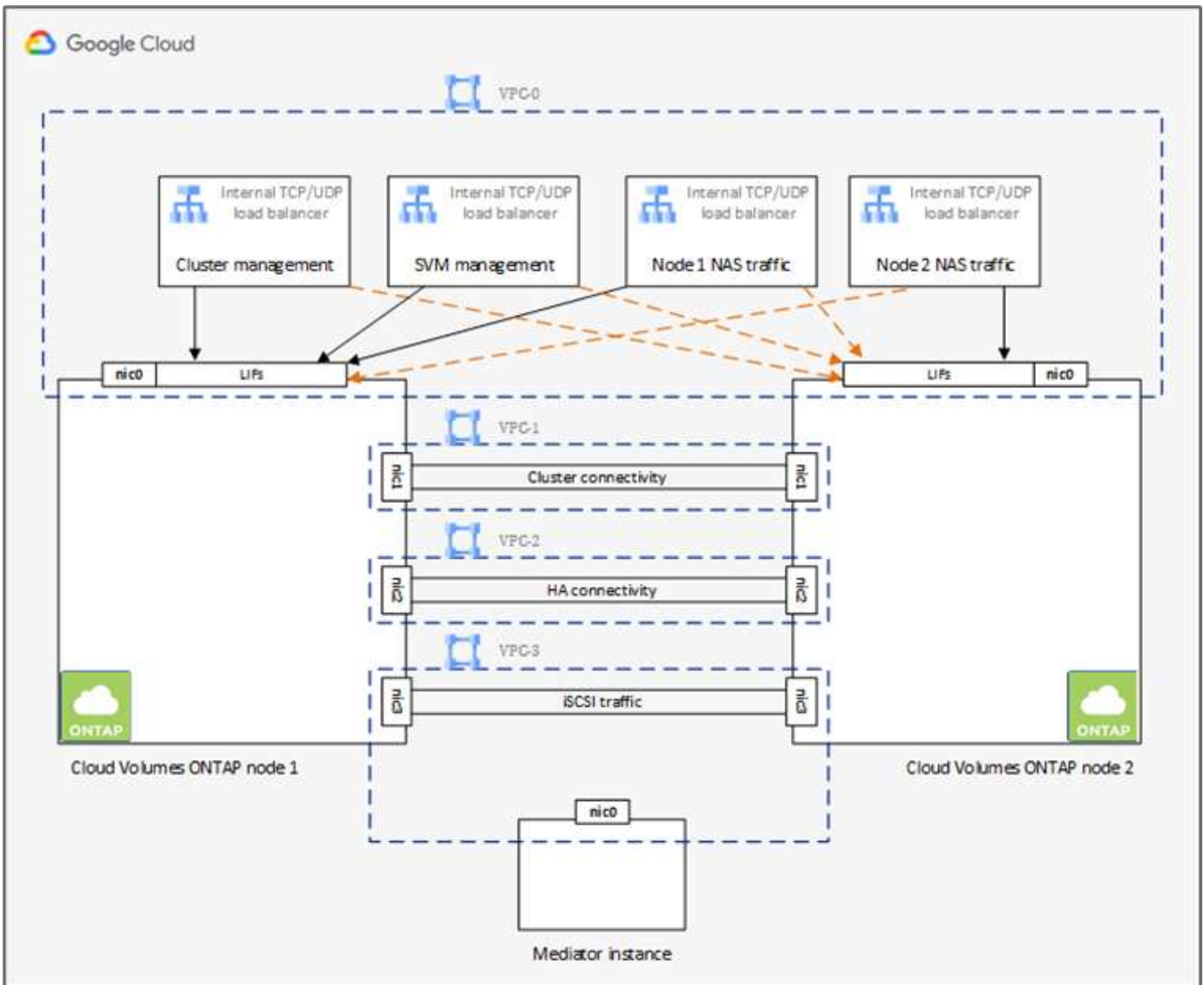
Google Cloud中的高可用性Cloud Volumes ONTAP

Google Cloud支持跨多个地理区域和一个区域内的多个区域部署资源。HA部署由两个ONTAP 节点组成、这两个节点使用Google Cloud中提供的功能强大的n1标准或n2标准计算机类型。数据会在两个Cloud Volumes ONTAP 节点之间同步复制、以便在发生故障时提供可用性。Cloud Volumes ONTAP 的高可用性部署要求每个VPC具有四个VPC和一个专用子网。四个vPC中的子网应配置非重叠的CIDR范围。

这四个VPC用于以下用途：

- VPC 0支持与数据和Cloud Volumes ONTAP 节点的入站通信。
- VPC 1可在Cloud Volumes ONTAP 节点之间提供集群连接。
- VPC 2支持在节点之间进行非易失性RAM (NVRAM)复制。
- VPC 3用于连接到HA调解器实例、以及用于节点重建的磁盘复制流量。

下图显示了Goggle Cloud中的高可用性Cloud Volumes ONTAP。



有关详细信息，请参见 ["此链接。"](#)。

有关Google Cloud中Cloud Volumes ONTAP 的网络连接要求、请参见 ["此链接。"](#)。

有关数据分层的详细信息、请参见 ["此链接。"](#)。

设置环境前提条件

可以使用Terraform配置自动创建Cloud Volumes ONTAP 集群、在内部卷和云卷之间配置SnapMirror、创建云卷等。这些Terraform配置托管在Terraform Cloud for Business帐户上。使用Intersight Cloud Orchestrator、您可以编排任务、例如在Terraform Cloud for Business帐户中创建工作空间、将所有必需的变量添加到工作空间、执行Terraform计划等。

对于这些自动化和业务流程任务、需要满足一些要求并提供一些数据、如以下各节所述。

GitHub 存储库

您需要一个GitHub帐户来托管Terraform代码。Intersight Orchestrator在Terraform Cloud for Business帐户中创建新的工作空间。此工作空间配置了版本控制工作流。为此、您需要将Terraform配置保留在GitHub存储库中、并在创建工作空间时将其作为输入提供。

"[此GitHub链接](#)" 使用各种资源提供Terraform配置。您可以通过派生此存储库并在GitHub帐户中创建副本。

在此存储库中、`provider.tf` 定义了所需的Terraform提供程序。使用适用于NetApp Cloud Manager的Terraform提供程序。

`variables.tf` 具有所有变量声明。这些变量的值将作为Intersight Cloud Orchestrator的工作流输入进行输入。这样可以方便地将值传递到工作空间并执行Terraform配置。

`resources.tf` 定义了向工作环境添加内部ONTAP、在Google Cloud上创建单节点Cloud Volumes ONTAP 集群、在内部和Cloud Volumes ONTAP 之间建立SnapMirror关系、在Cloud Volumes ONTAP 上创建云卷等所需的各种资源。

在此存储库中：

- `provider.tf` 将NetApp Cloud Manager定义为所需的Terraform提供程序。
- `variables.tf` 具有可变声明、这些声明可用作Intersight Cloud Orchestrator工作流的输入。这样可以方便地将值传递到工作空间并执行Terraform配置。
- `resources.tf` 定义各种资源、用于向工作环境添加内部ONTAP、在Google Cloud上创建单节点Cloud Volumes ONTAP 集群、在内部和Cloud Volumes ONTAP 之间建立SnapMirror关系、在Cloud Volumes ONTAP 上创建云卷等。

您可以添加一个额外的资源块来在Cloud Volumes ONTAP 上创建多个卷、也可以使用count或`for\_each` Terraform构造。

要将Terraform工作空间、模块和策略集连接到包含Terraform配置的git存储库、Terraform Cloud需要访问GitHub repo。

添加客户端、客户端的OAuth令牌ID将用作Intersight Cloud Orchestrator的工作流输入之一。

1. 登录到Terraform Cloud for Business帐户。导航到*设置>提供程序*。
2. 单击*添加VCS提供程序*。
3. 选择您的版本。
4. 按照*设置提供程序*下的步骤进行操作。
5. 您可以在* VCS Provider*中看到已添加的客户端。记下OAuth令牌ID。

刷新NetApp Cloud Manager API操作的令牌

除了 Web 浏览器界面之外，Cloud Manager 还具有一个 REST API，可使软件开发人员通过 SaaS 界面直接访问 Cloud Manager 功能。Cloud Manager 服务由多个不同的组件组成，这些组件共同构成一个可扩展的开发平台。通过刷新令牌、您可以生成要添加到每个API调用的授权标头中的访问令牌。

在不直接调用API的情况下、NetApp-cloudmanager提供程序会使用刷新令牌并将Terraform资源转换为相应的API调用。您需要从NetApp Cloud Manager API操作生成刷新令牌 "[NetApp Cloud Central](#)"。

要在Cloud Manager上创建资源、例如创建Cloud Volumes ONTAP 集群、配置SnapMirror等、您需要Cloud Manager Connector的客户端ID。

1. 登录到Cloud Manager： "<https://cloudmanager.netapp.com/>"。
2. 单击 * 连接器 *。

3. 单击 * 管理连接器 *。
4. 单击省略号并复制连接器ID。

开发Cisco Intersight Cloud Orchestrator工作流

在以下情况下、Cisco Intersight可提供Cisco Intersight Cloud Orchestrator:

- 您已安装Intersight Premier许可证。
- 您可以是帐户管理员、存储管理员、虚拟化管理员或服务器管理员、并且至少已为您分配一台服务器。

工作流设计器

工作流设计器可帮助您创建新工作流(以及任务和数据类型)并编辑现有工作流、以管理Cisco Intersight中的目标。

要启动工作流设计器、请转到*流程编排>工作流*。信息板会在*我的工作流*、*示例工作流*和*所有工作流*选项卡下显示以下详细信息:

- 验证状态
- 上次执行状态
- 按执行计数显示的前几个工作流
- 工作流类别排名靠前
- 系统定义的工作流数量
- 按目标划分的前几个工作流

您可以使用信息板创建、编辑、克隆或删除选项卡。要创建自己的自定义视图选项卡、请单击**并指定名称、然后选择需要显示在列、标记列和小工具中的参数。如果某个选项卡没有*锁定*图标、则可以重命名该选项卡。

信息板下是一个工作流表格列表、其中显示了以下信息:

- 显示名称
- Description
- 系统定义
- 默认版本
- 执行
- 上次执行状态
- 验证状态
- 上次更新时间
- 组织

"Actions"列可用于执行以下操作:

- *执行。*执行工作流。
- *历史记录。*显示工作流执行历史记录。

- *管理版本。*创建和管理工作流的版本。
- *删除。*删除工作流。
- *重试。*重试失败的工作流。

工作流

创建包含以下步骤的工作流：

- *定义工作流。*指定显示名称、问题描述 和其他重要属性。
- *定义工作流输入和工作流输出。*指定执行工作流必须使用哪些输入参数、以及成功执行时生成的输出
- *添加工作流任务。*在工作流设计器中添加工作流执行其功能所需的一个或多个工作流任务。
- *验证工作流。*验证工作流以确保在连接任务输入和输出时没有错误。

为内部**FlexPod** 存储创建工作流

要为内部FlexPod 存储配置工作流、请参见 "[此链接](#)。"

"[接下来：灾难恢复工作流](#)。"

灾难恢复工作流

"[先前版本：自动部署混合云NetApp存储](#)。"

步骤顺序如下：

1. 定义工作流。
 - 为工作流创建一个用户友好的简短名称、例如Disaster Recovery Workflow。
2. 定义工作流输入。我们为此工作流提供了以下信息：
 - 卷选项(卷名称、挂载路径)
 - 卷容量
 - 与新数据存储库关联的数据中心
 - 托管数据存储库的集群
 - 要在vCenter中创建的新数据存储库的名称
 - 新数据存储库的类型和版本
 - Terraform组织的名称
 - Terraform工作空间
 - Terraform工作空间的问题描述
 - 执行Terraform配置所需的变量(敏感和非敏感)
 - 启动计划的原因
3. 添加工作流任务。

与FlexPod 中的操作相关的任务包括：

- 在FlexPod 中创建卷。
- 向创建的卷添加存储导出策略。
- 将新创建的卷映射到VMware vCenter中的数据存储库。

与创建Cloud Volumes ONTAP 集群相关的任务：

- 添加Terraform工作空间
- 添加Terraform变量
- 添加Terraform敏感变量
- 启动新的Terraform计划
- 确认Terraform运行

4. 验证工作流。

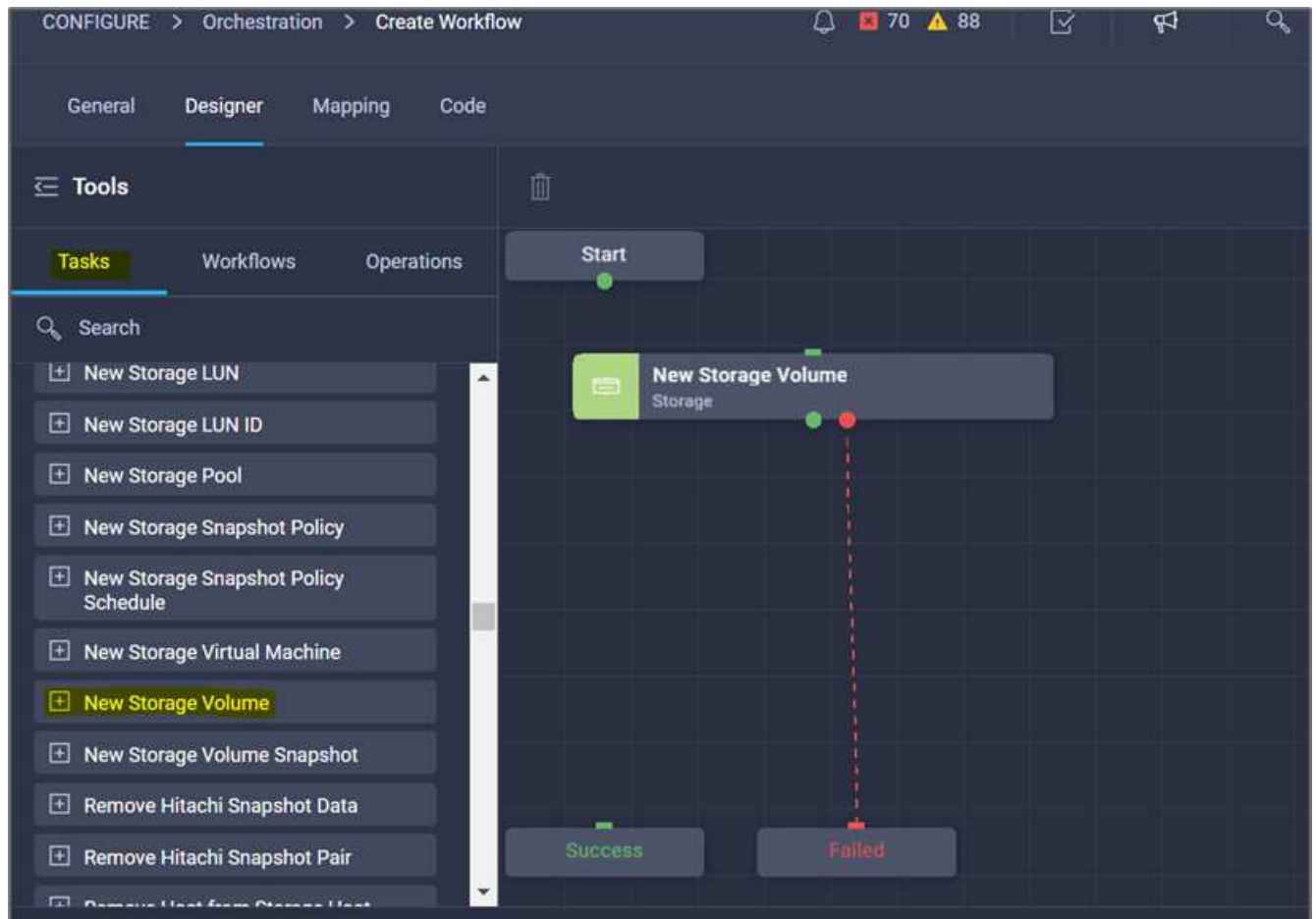
操作步骤 1：创建工作流

1. 单击左侧导航窗格中的*流程编排*、然后单击*创建工作流*。
2. 在*常规*选项卡中：
 - a. 提供显示名称(灾难恢复工作流)。
 - b. 选择组织、设置标记并提供问题描述。
3. 单击保存。

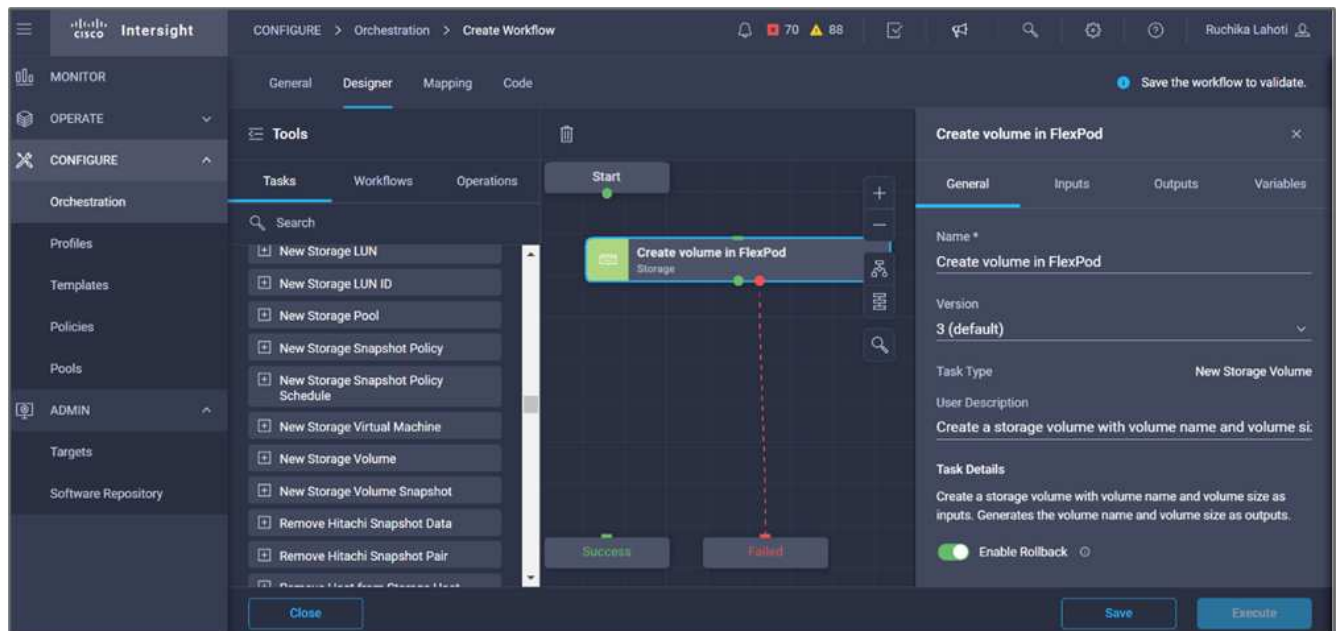
The screenshot shows the 'General' tab of a workflow configuration interface. The 'Display Name' is 'Disaster Recovery Workflow' and the 'Reference Name' is 'DisasterRecoveryWorkflow'. The 'Organization' is 'default' and the 'Version' is '2 (default)'. The 'Description' is 'Workflow which creates and configures SnapMirror between FlexPod Storage and Cloud Volumes ONTAP'. Under 'Workflow Execution', 'Failed/Terminated Actions' is checked, 'Enable Retry' is checked, 'Enable Auto Rollback' is unchecked, and 'Enable Debug Logs' is checked. At the bottom, there are tabs for 'Workflow Inputs', 'Workflow Variables', and 'Workflow Outputs', with 'Add Workflow Input' button below them.

操作步骤 2.在FlexPod 中创建新卷

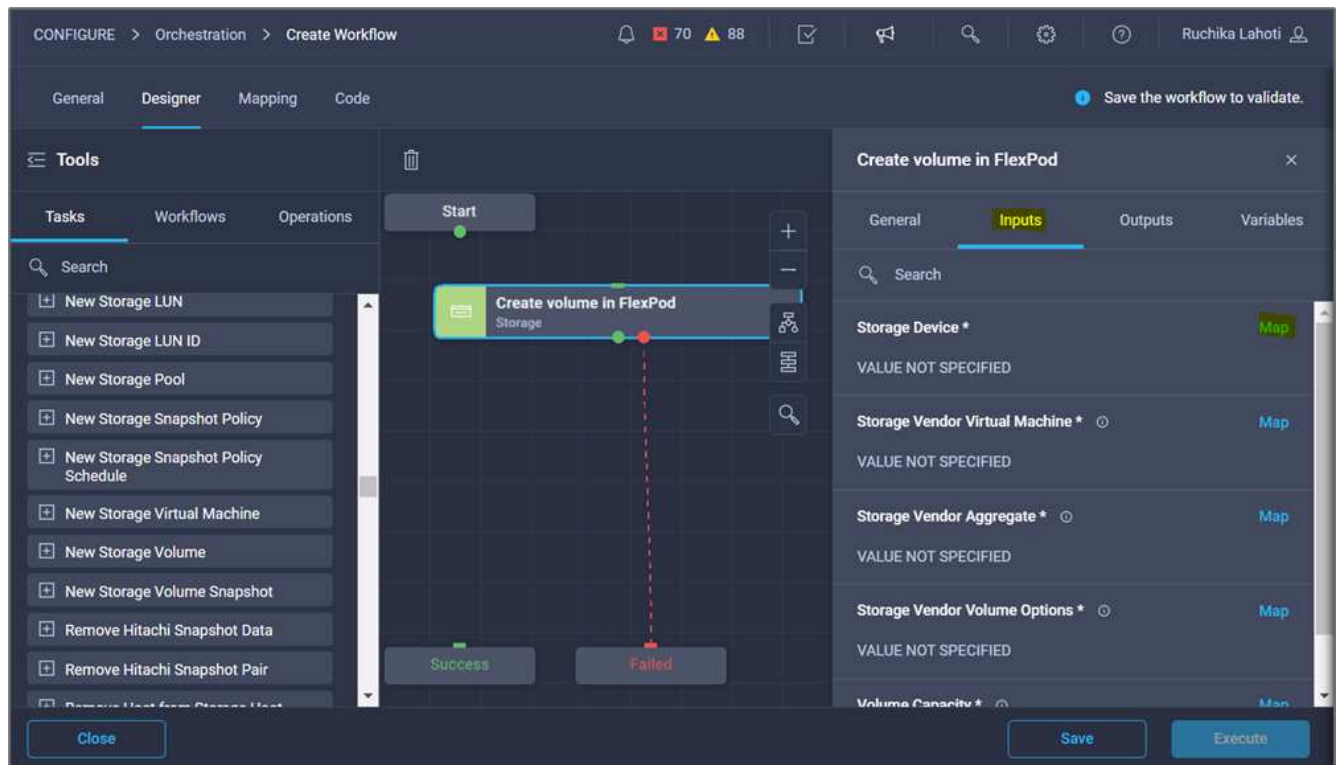
1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 将*存储>新存储卷*任务从*工具*部分拖放到*设计*区域中。
3. 单击*新建存储卷*。



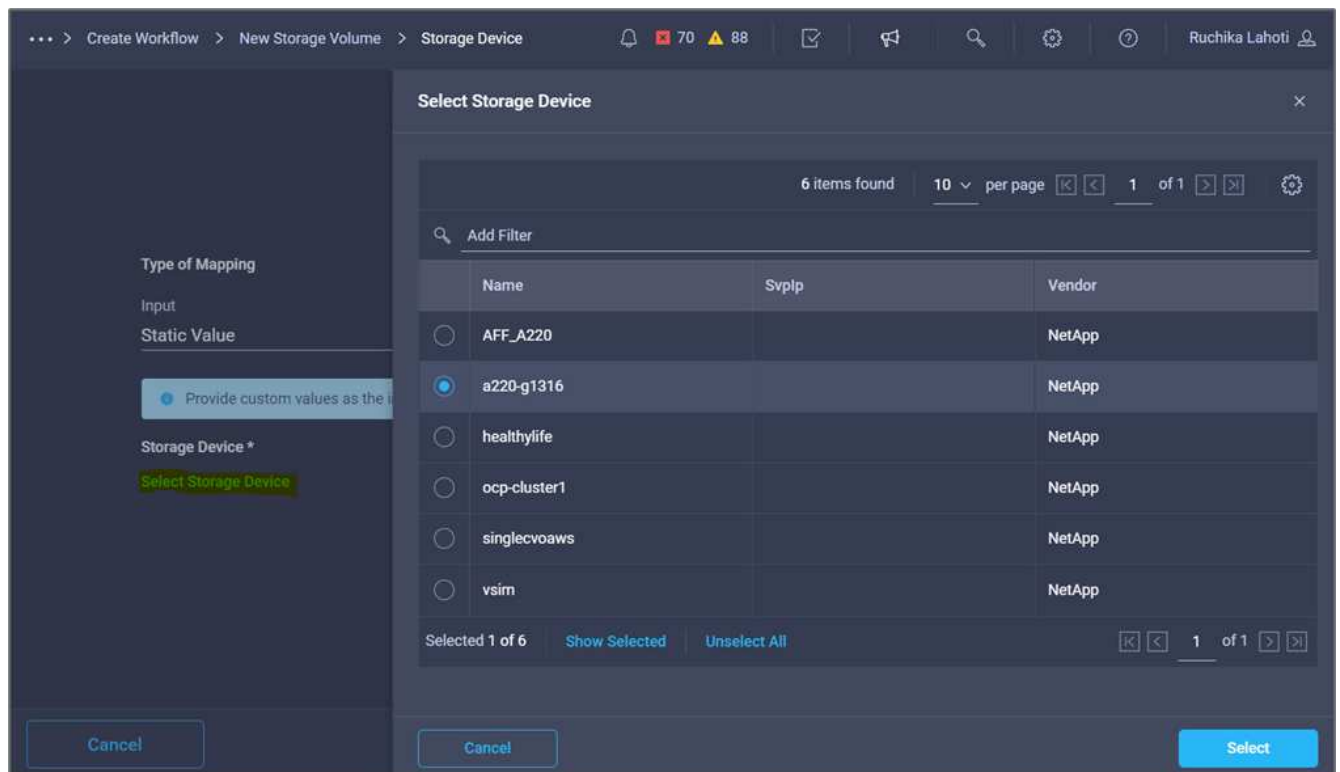
4. 在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是*在FlexPod 中创建卷*。



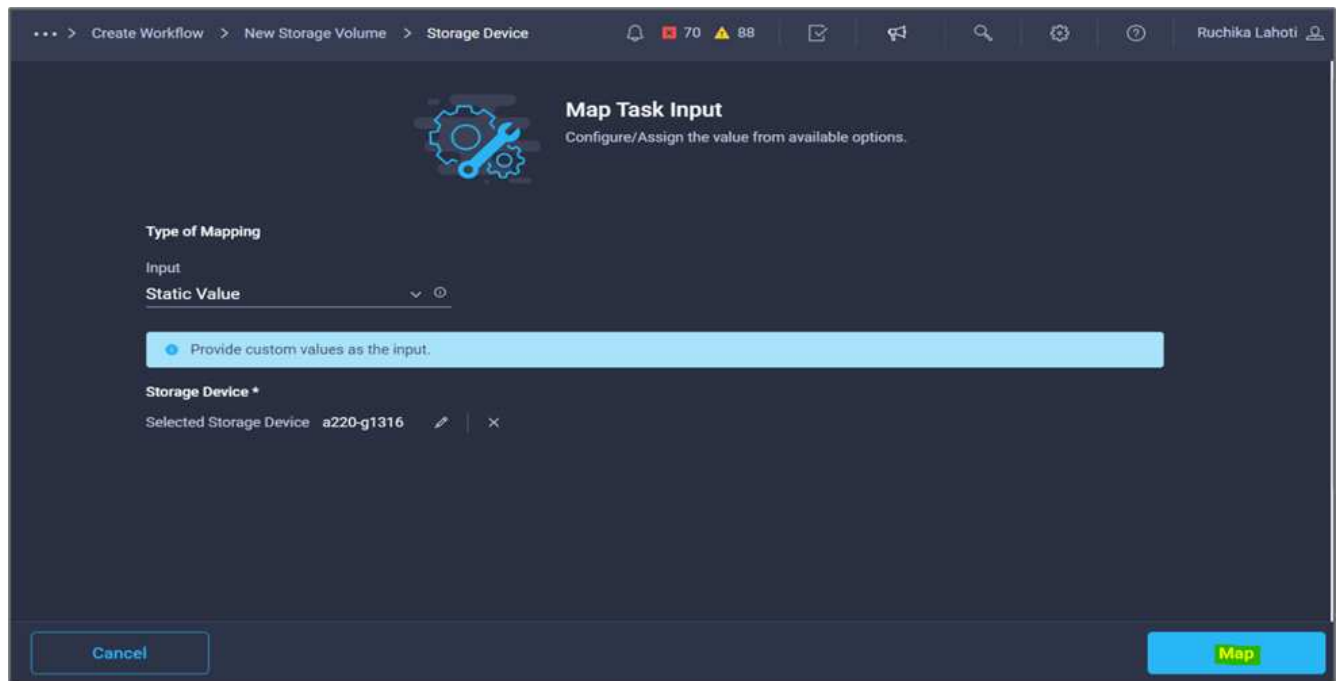
5. 在*任务属性*区域中、单击*输入*。
6. 单击*存储设备*字段中的*映射*。



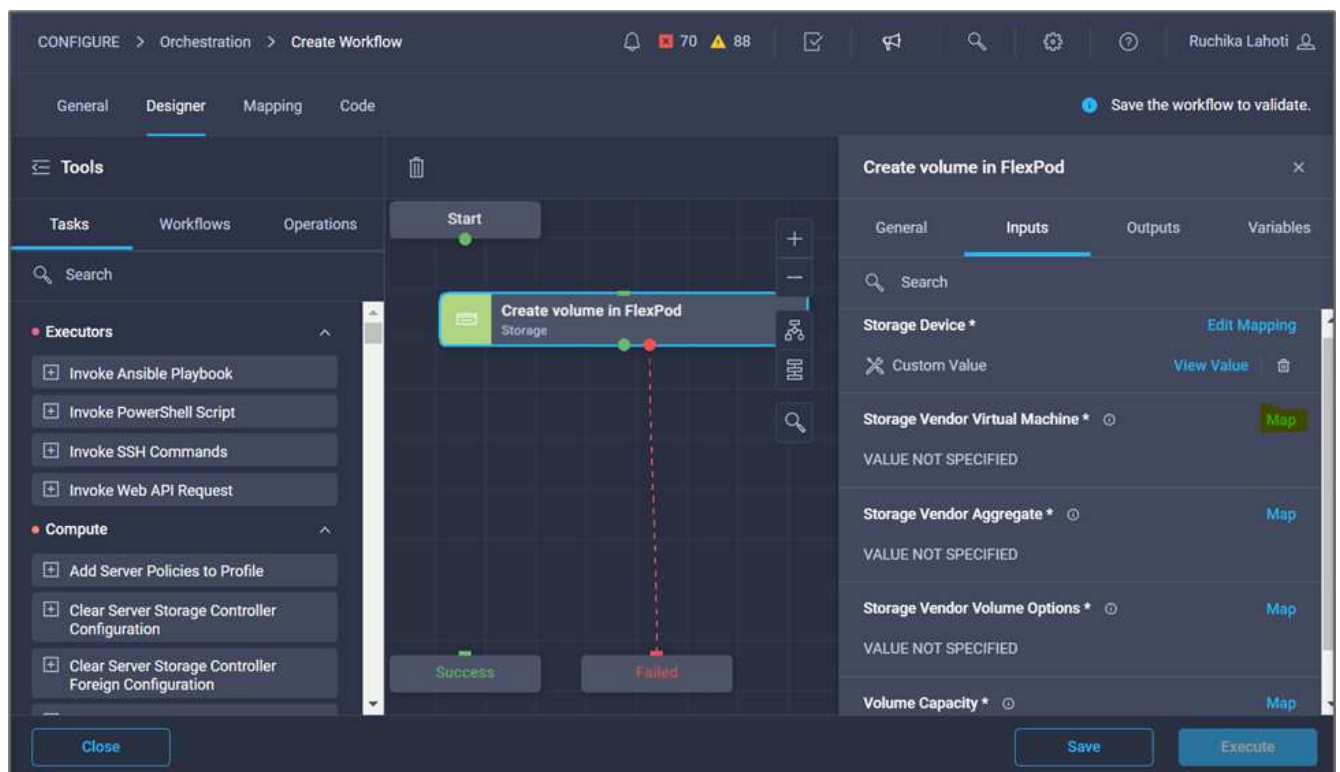
7. 选择*静态值*、然后单击*选择存储设备*。
8. 单击已添加的存储目标、然后单击*选择*。



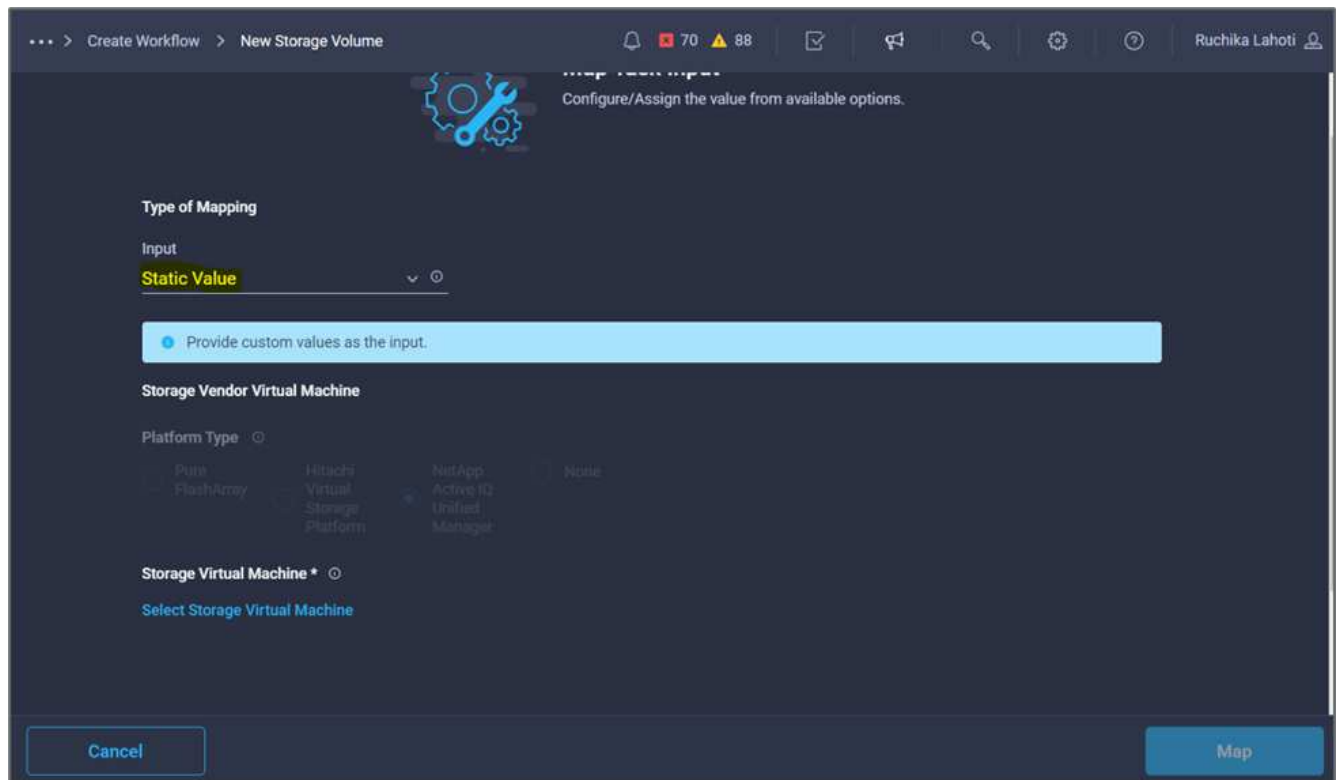
9. 单击*映射*。



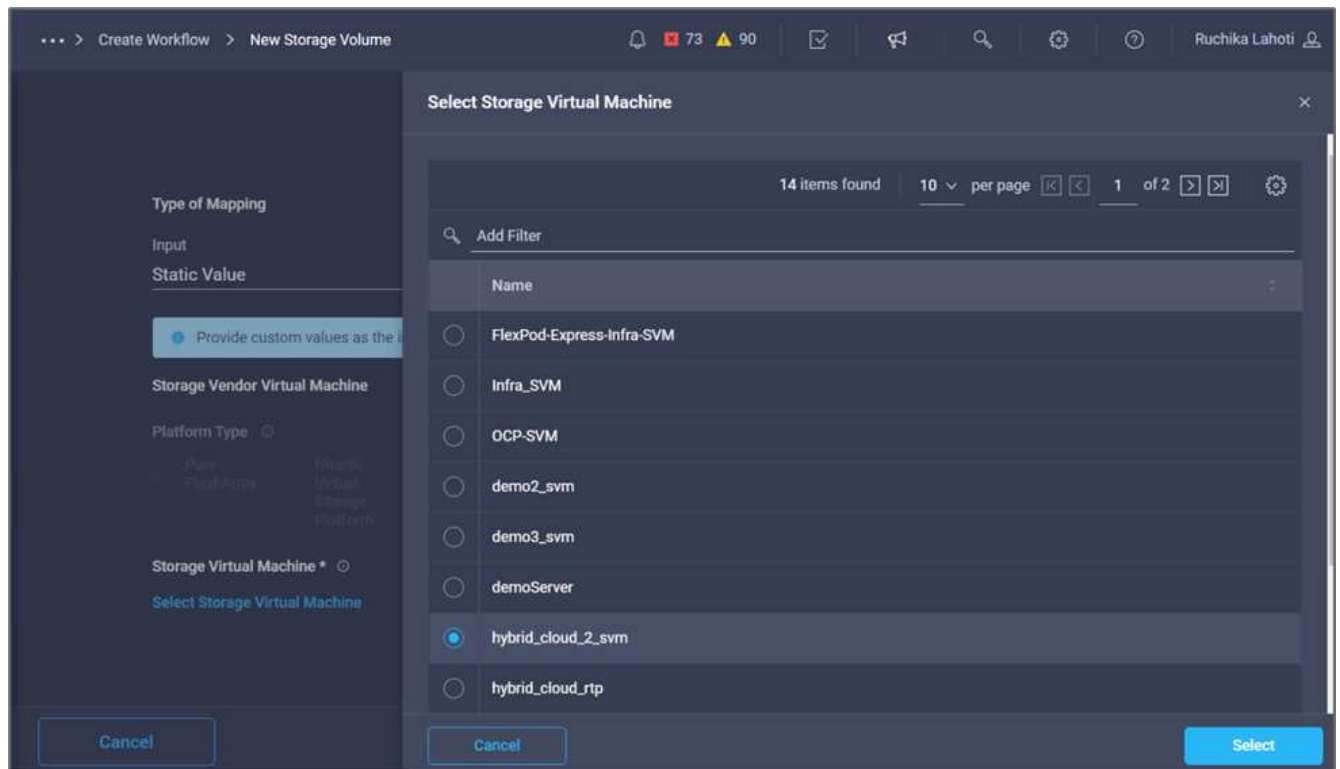
10. 单击*存储供应商虚拟机*字段中的*映射*。



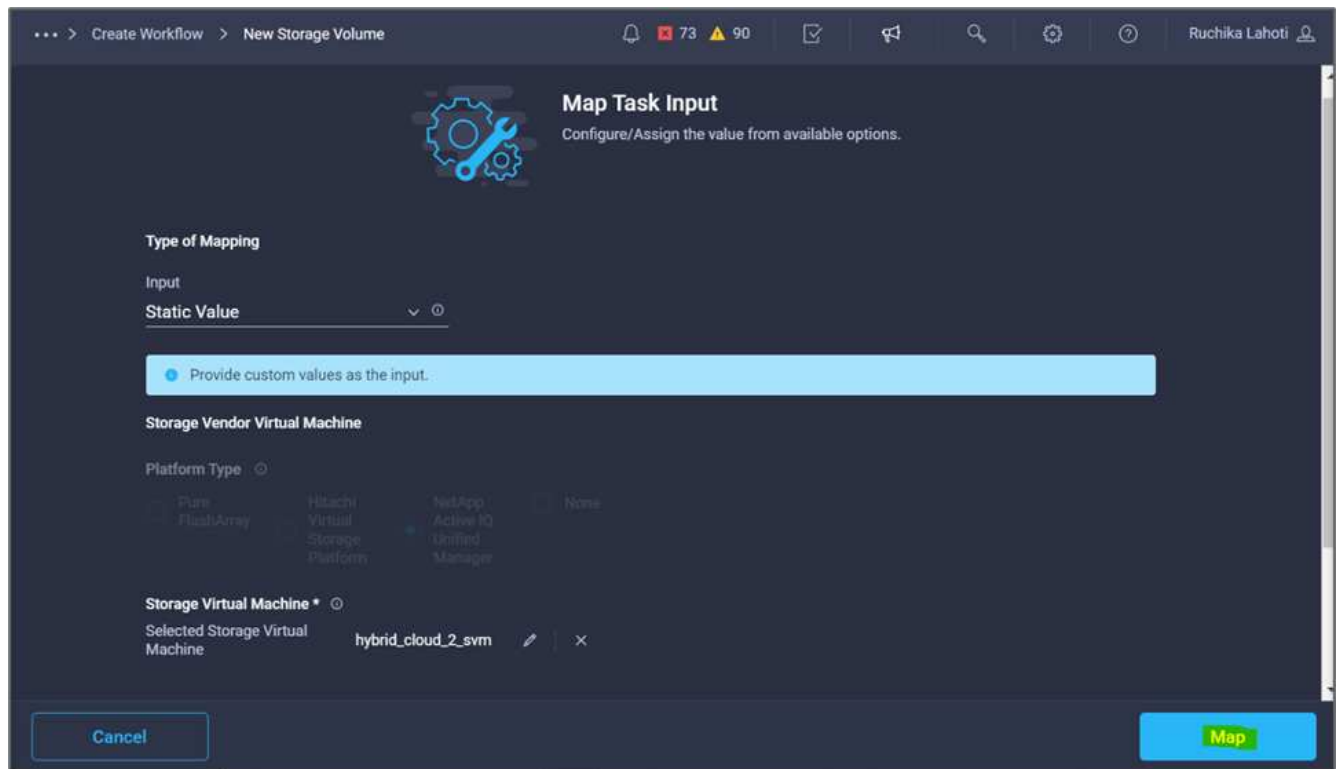
11. 选择*静态值*、然后单击*选择Storage Virtual Machine*。



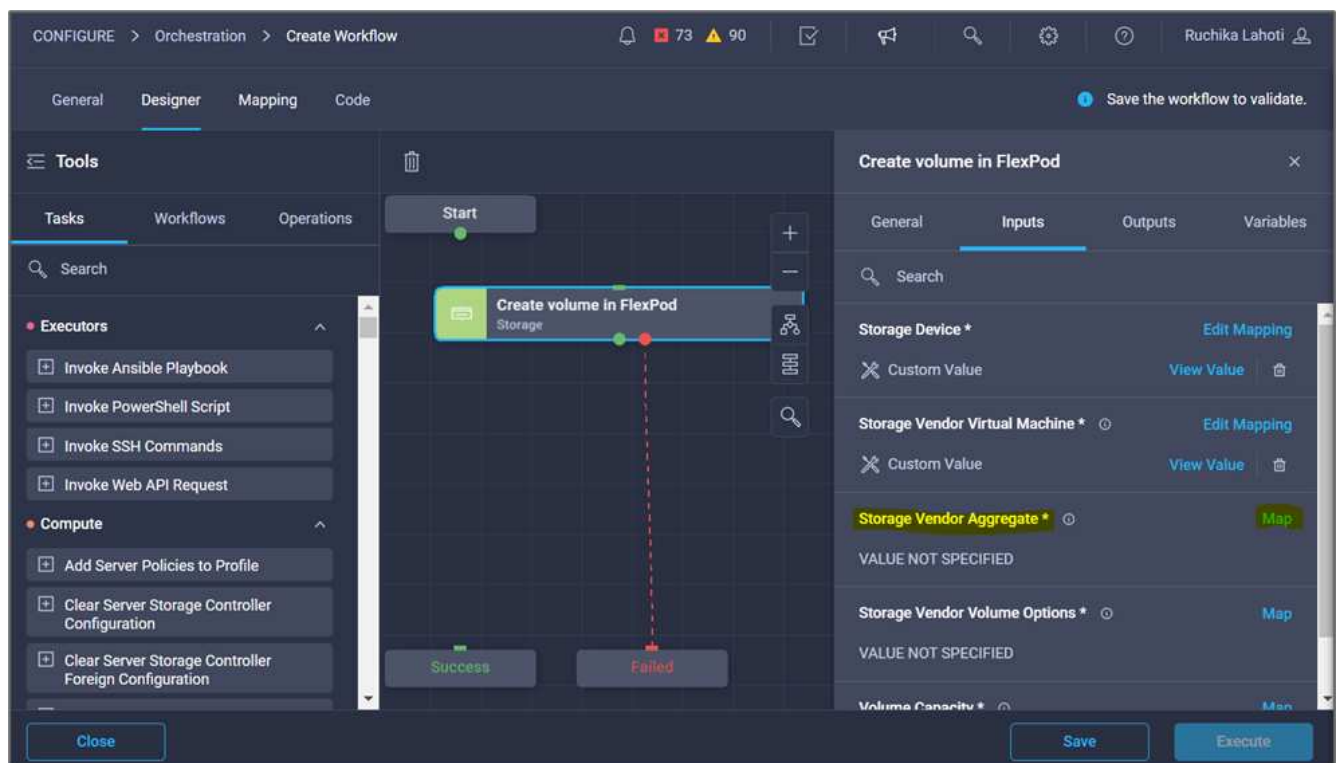
12. 选择需要创建卷的Storage Virtual Machine、然后单击*选择*。



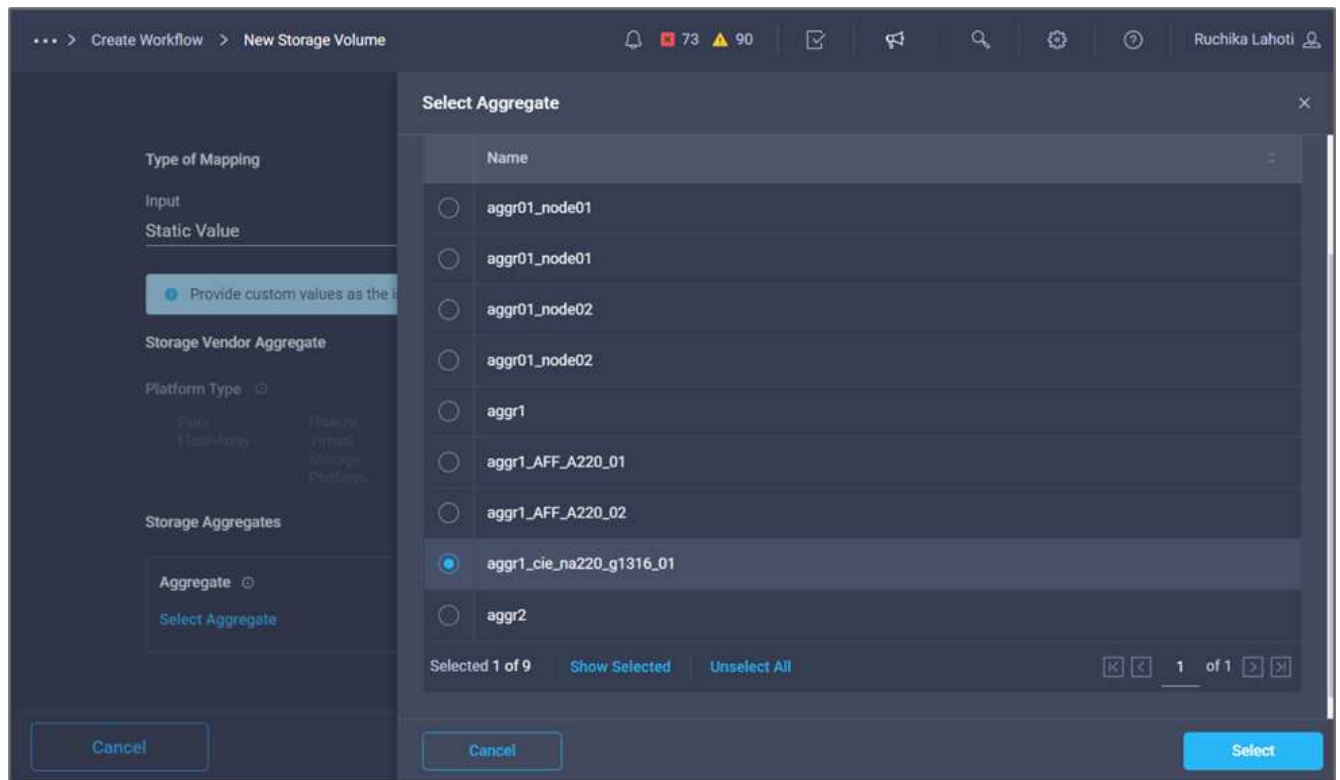
13. 单击*映射*。



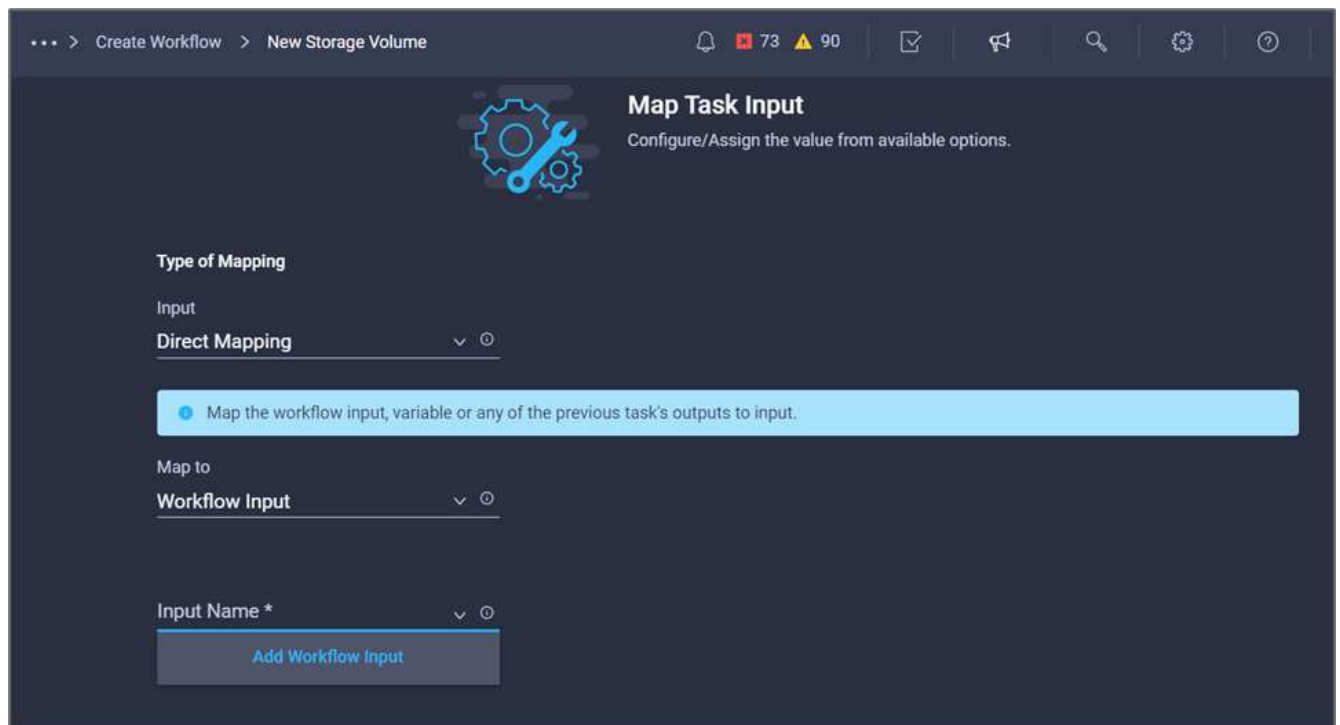
14. 单击*存储供应商聚合*字段中的*映射*。



15. 选择*静态值*、然后单击*选择存储聚合*。选择聚合并单击*选择*。



16. 单击*映射*。
17. 单击*存储供应商卷选项*字段中的*映射*。
18. 选择*直接映射*、然后单击*工作流输入*。



19. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)。

- b. 确保为*类型*选择了*存储供应商卷选项*。
- c. 单击*设置默认值并覆盖*。
- d. 单击*必需*。
- e. 将*平台类型*设置为* NetApp Active IQ Unified Manager *。
- f. 在*卷*下为创建的卷提供默认值。
- g. 单击*。nfs*。如果设置了NFS、则会创建NFS卷。如果此值设置为false、则会创建SAN卷。
- h. 提供挂载路径、然后单击*添加*。

Add Workflow Input

☒ Set Default Value ⓘ

☒ Allow User Override ⓘ

Default Values *

Storage Vendor Volume Options

Platform Type ⓘ

☐ Pure FlashArray ☐ Hitachi Virtual Storage Platform ☒ NetApp Active IQ Unified Manager ☐ None

Volume *

mssql_data_vol ⓘ

NFS Volume Option

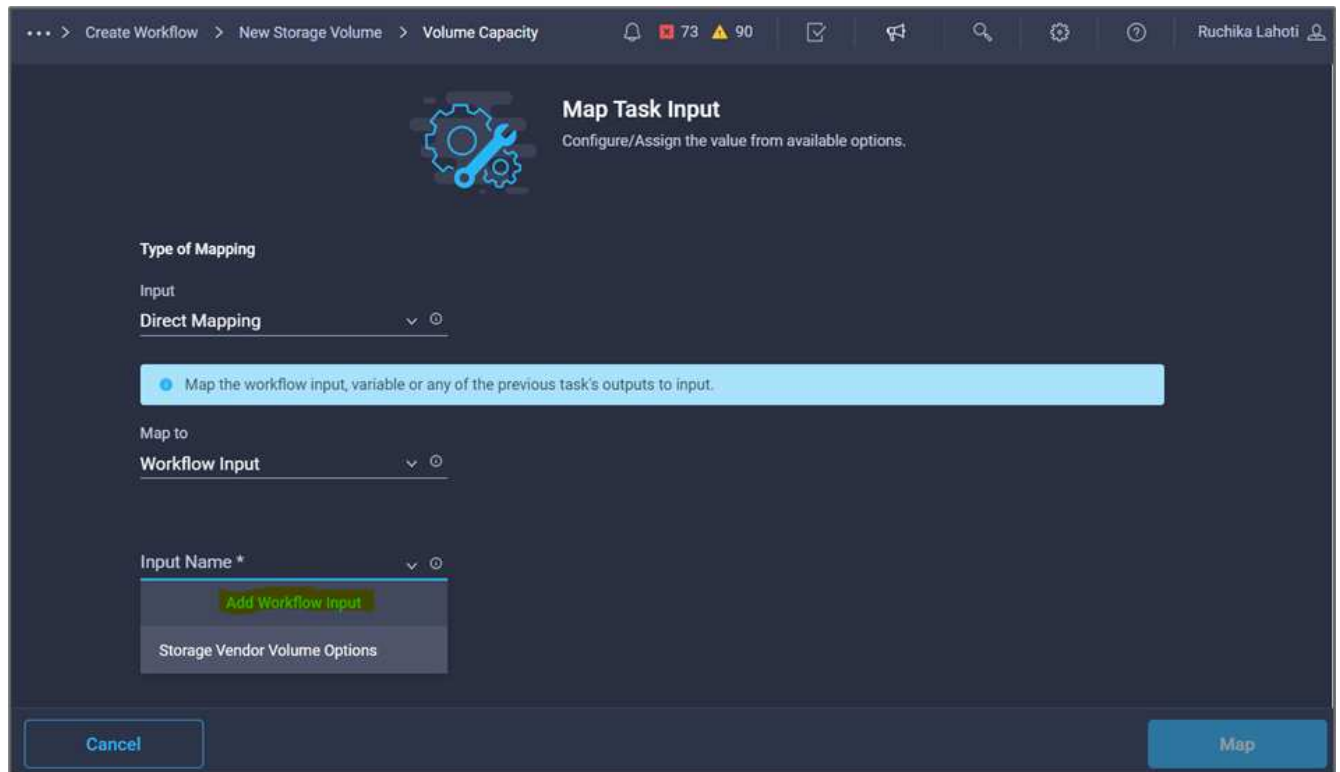
☒ NFS ⓘ

Mount Path

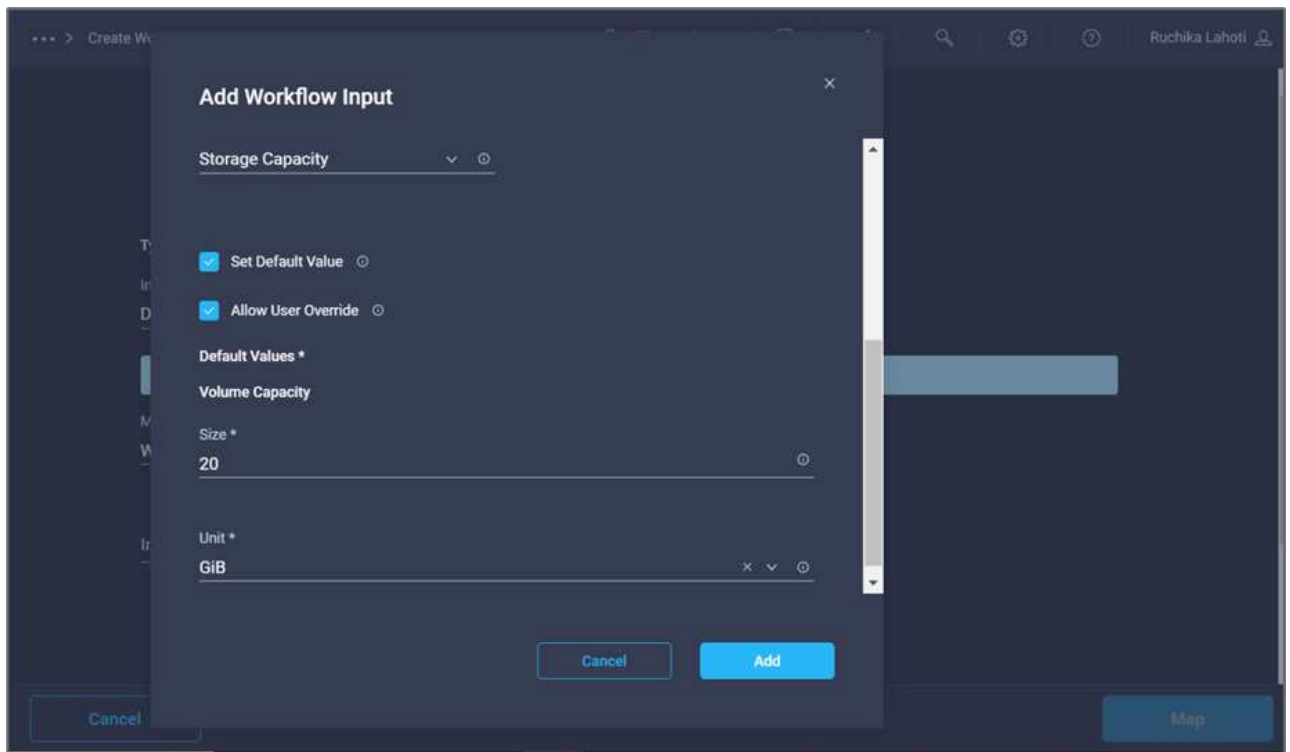
/mssql_data_vol ⓘ

Cancel Add

- 20. 单击*映射*。
- 21. 单击*卷容量*字段中的*映射*。
- 22. 选择*直接映射*、然后单击*工作流输入*。
- 23. 单击*输入名称*和*创建工作流输入*。

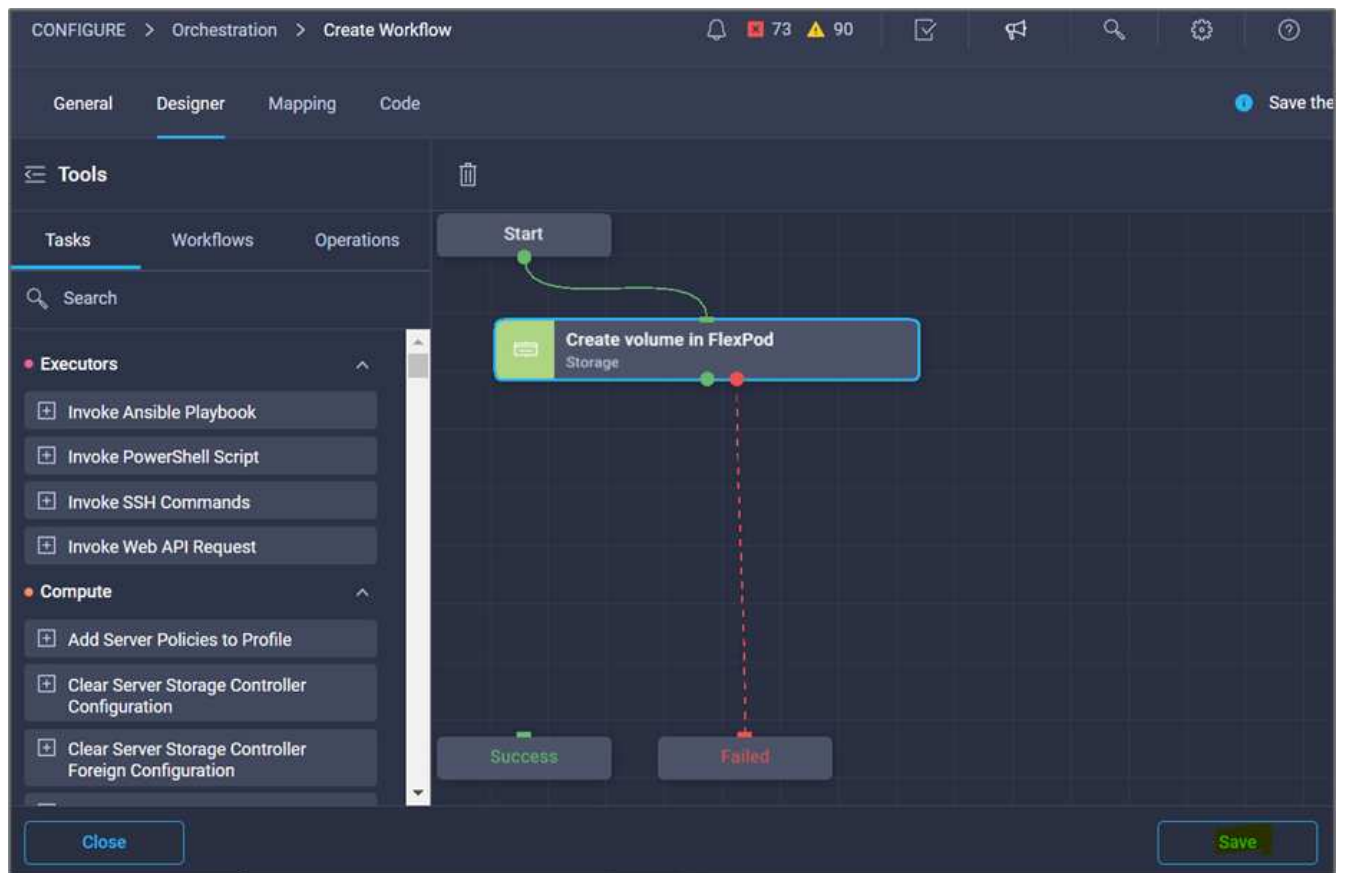


24. 在添加输入向导中：
- 提供显示名称和参考名称(可选)。
 - 单击*必需*。
 - 对于*类型*、选择*存储容量*。
 - 单击*设置默认值并覆盖*。
 - 为卷大小和单位提供默认值。
 - 单击 * 添加 *。



25. 单击*映射*。

26. 使用Connector在*启动*和*在FlexPod 中创建卷*任务之间创建连接、然后单击*保存*。

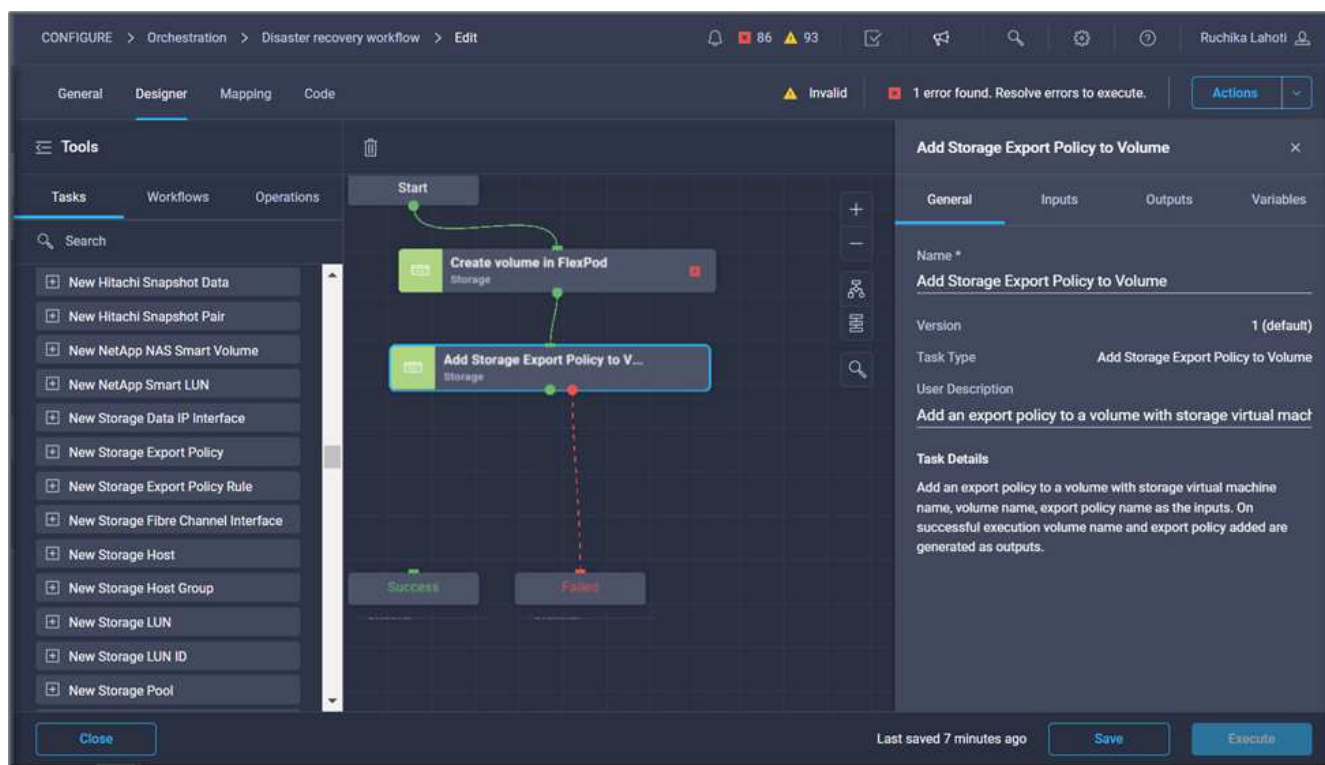




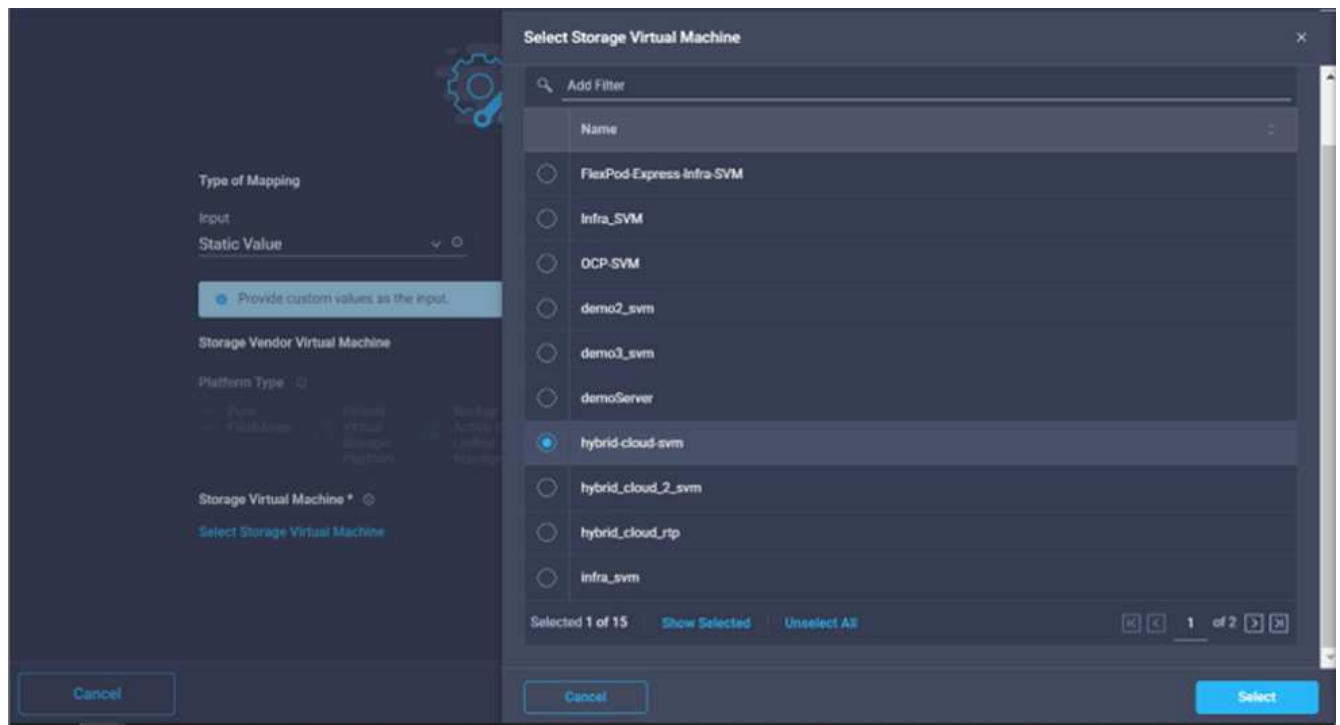
现在忽略此错误。显示此错误的原因是、*在FlexPod 中创建卷*和*成功*任务之间没有连接、而这是指定成功过渡所必需的。

操作步骤 3：添加存储导出策略

1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放*存储>将存储导出策略添加到卷*任务。
3. 单击*将存储导出策略添加到卷*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是添加存储导出策略。
4. 使用连接器在*在FlexPod 中创建卷*和*添加存储导出策略*任务之间建立连接。单击 * 保存 *。



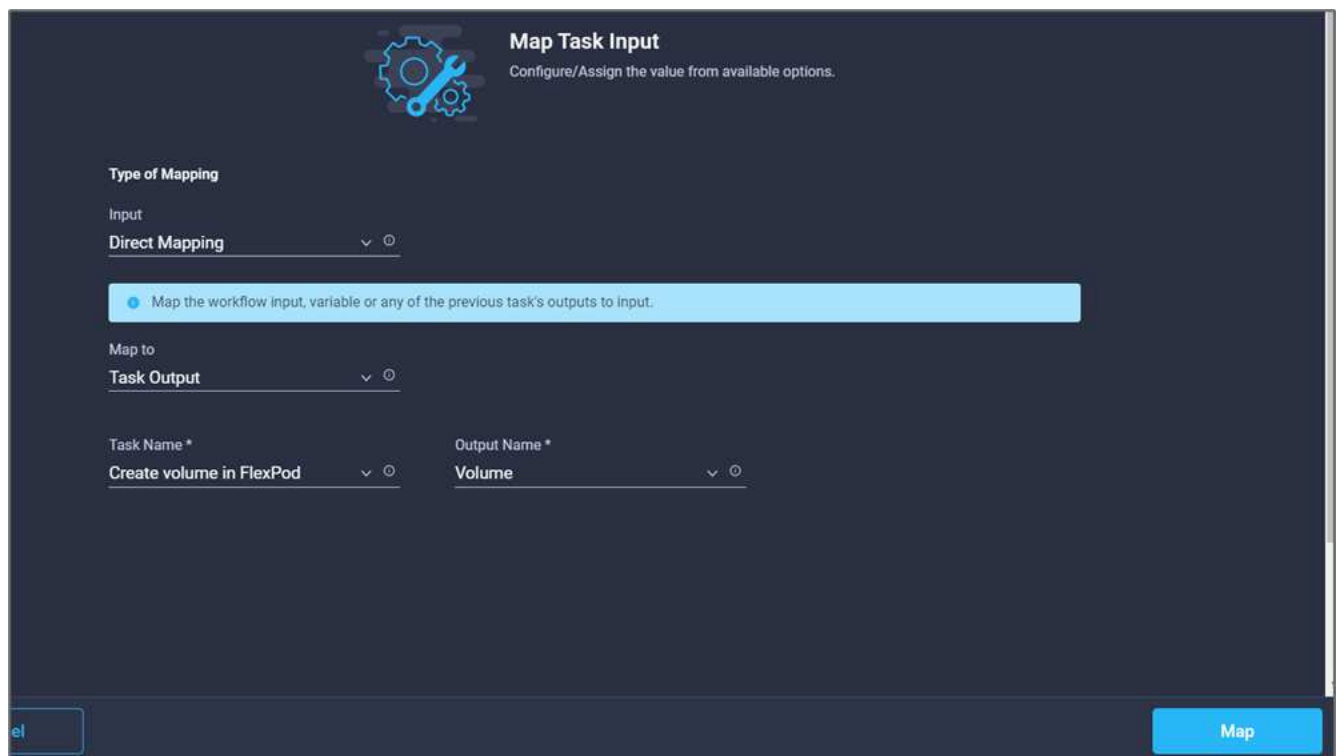
5. 在*任务属性*区域中、单击*输入*。
6. 单击*存储设备*字段中的*映射*。



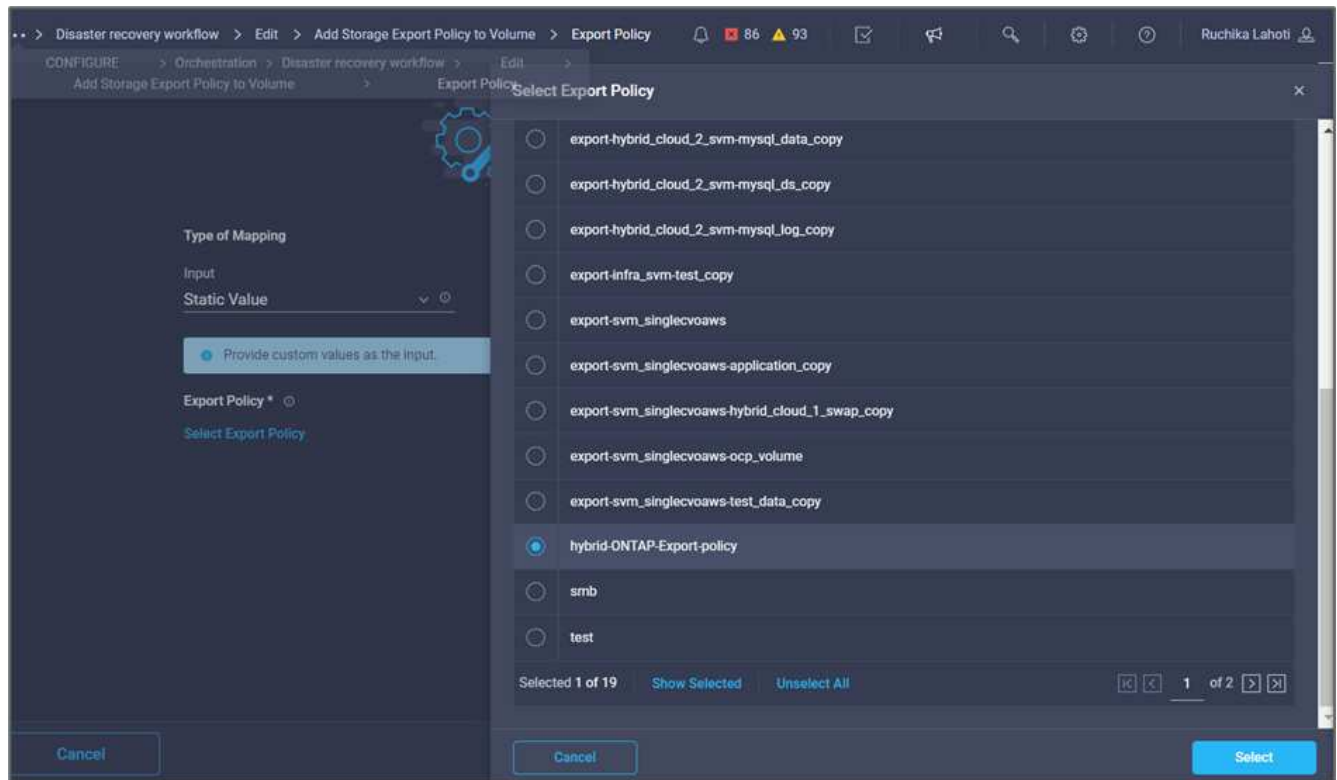
11. 单击*映射*。
12. 单击*卷*字段中的*映射*。
13. 单击*任务名称*、然后单击*在FlexPod 中创建卷*。单击*输出名称*、然后单击*卷*。



在Cisco Intersight Cloud Orchestrator中、您可以提供上一个任务的输出作为新任务的输入。在此示例中、*在FlexPod 中创建卷*任务提供了*卷*详细信息、作为*添加存储导出策略*任务的输入。



14. 单击*映射*。
15. 单击*导出策略*字段中的*映射*。
16. 选择*静态值*、然后单击*选择导出策略*。选择已创建的导出策略。



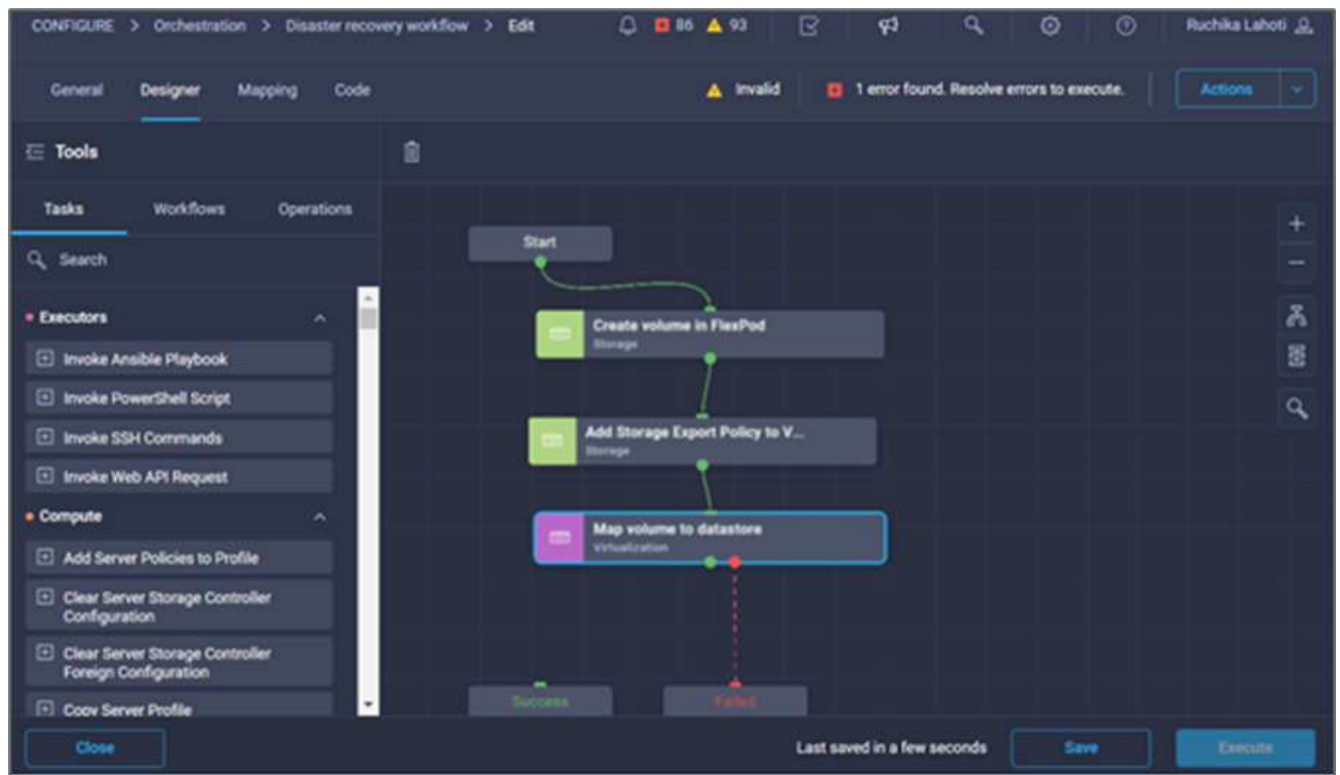
17. 单击*映射*、然后单击*保存*。



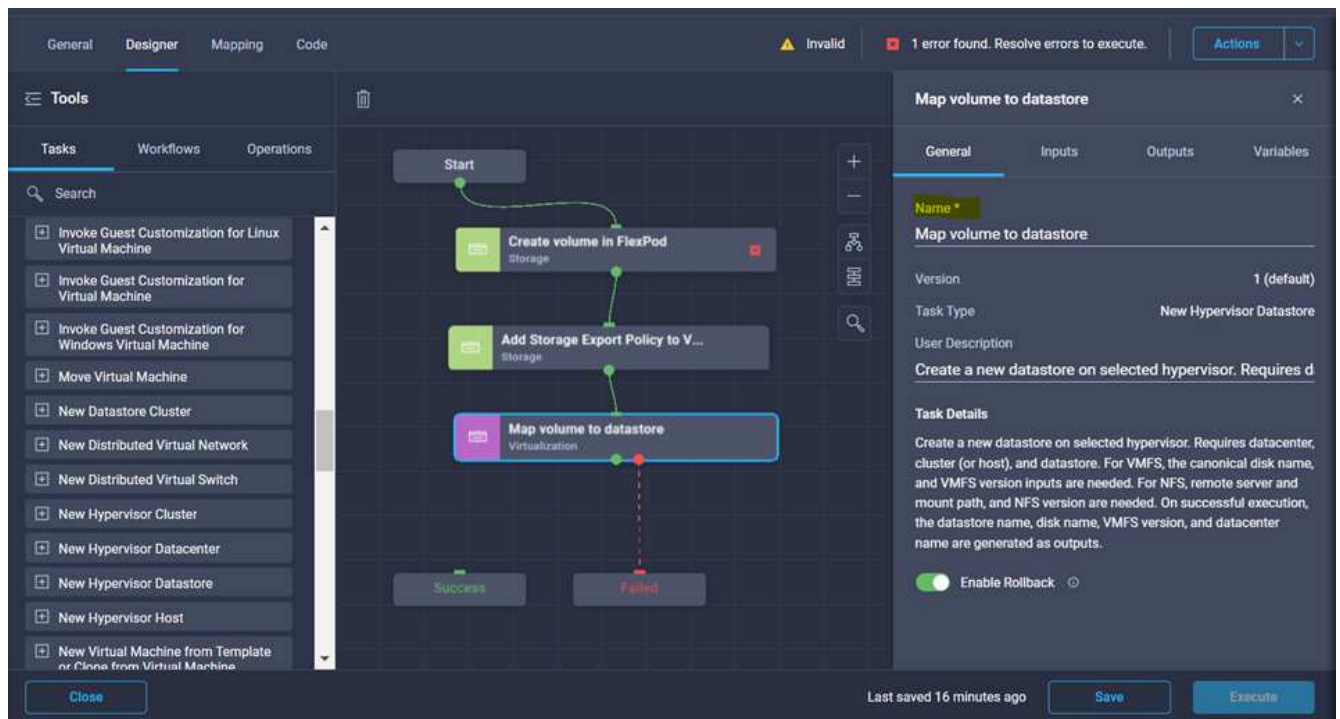
此时将向卷添加导出策略。接下来、创建一个新的数据存储库来映射已创建的卷。

操作步骤 4：将**FlexPod** 卷映射到数据存储库

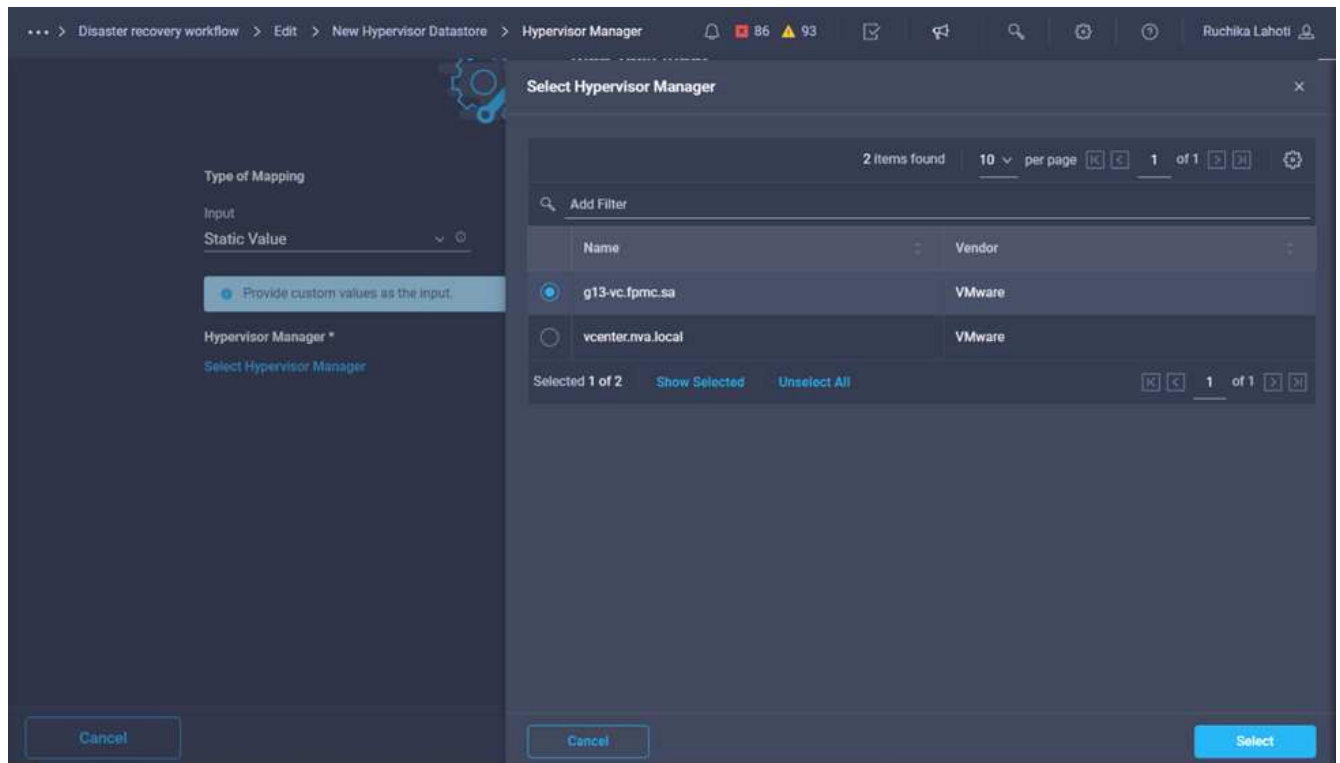
1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放*虚拟化>新虚拟机管理程序数据存储库*任务。
3. 使用Connector在*添加存储导出策略*和*新建虚拟机管理程序数据存储库*任务之间建立连接。单击 * 保存 *



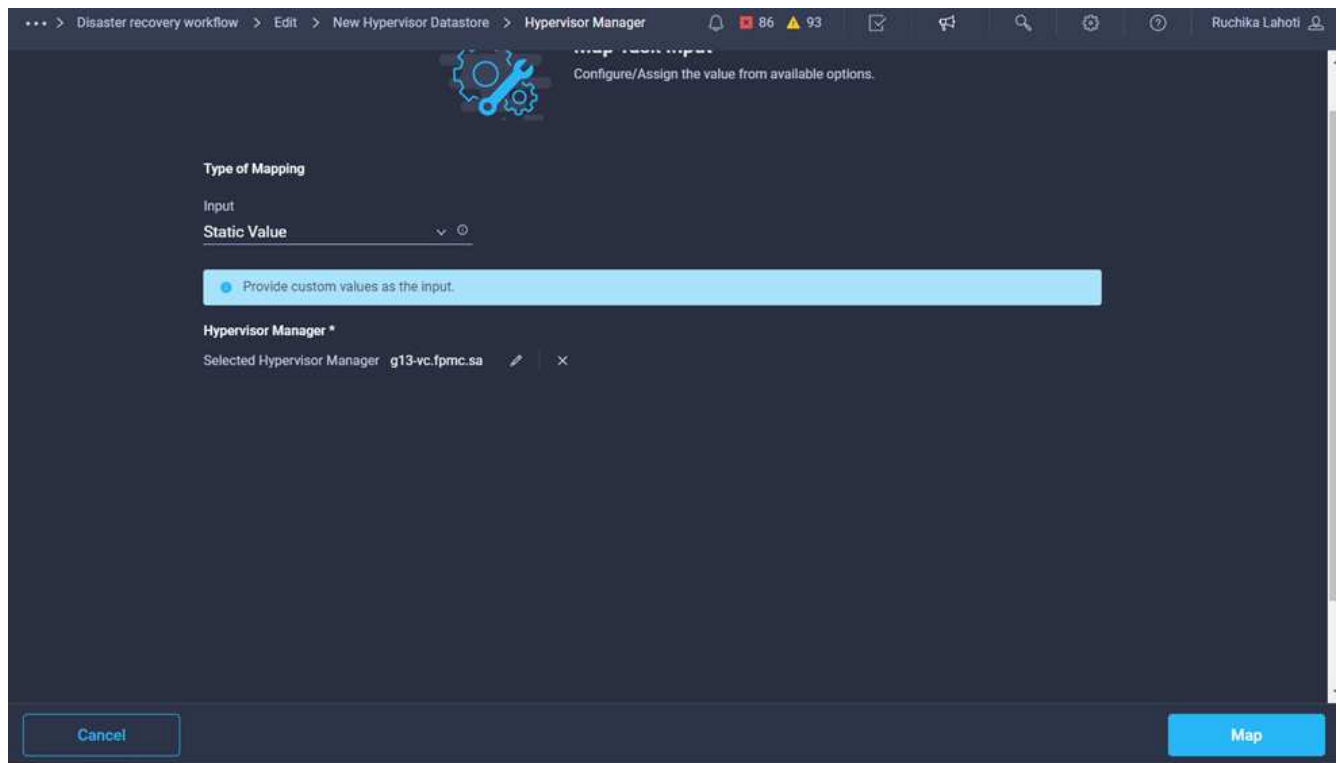
4. 单击*新建虚拟机管理程序数据存储库*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是*将卷映射到数据存储库*。



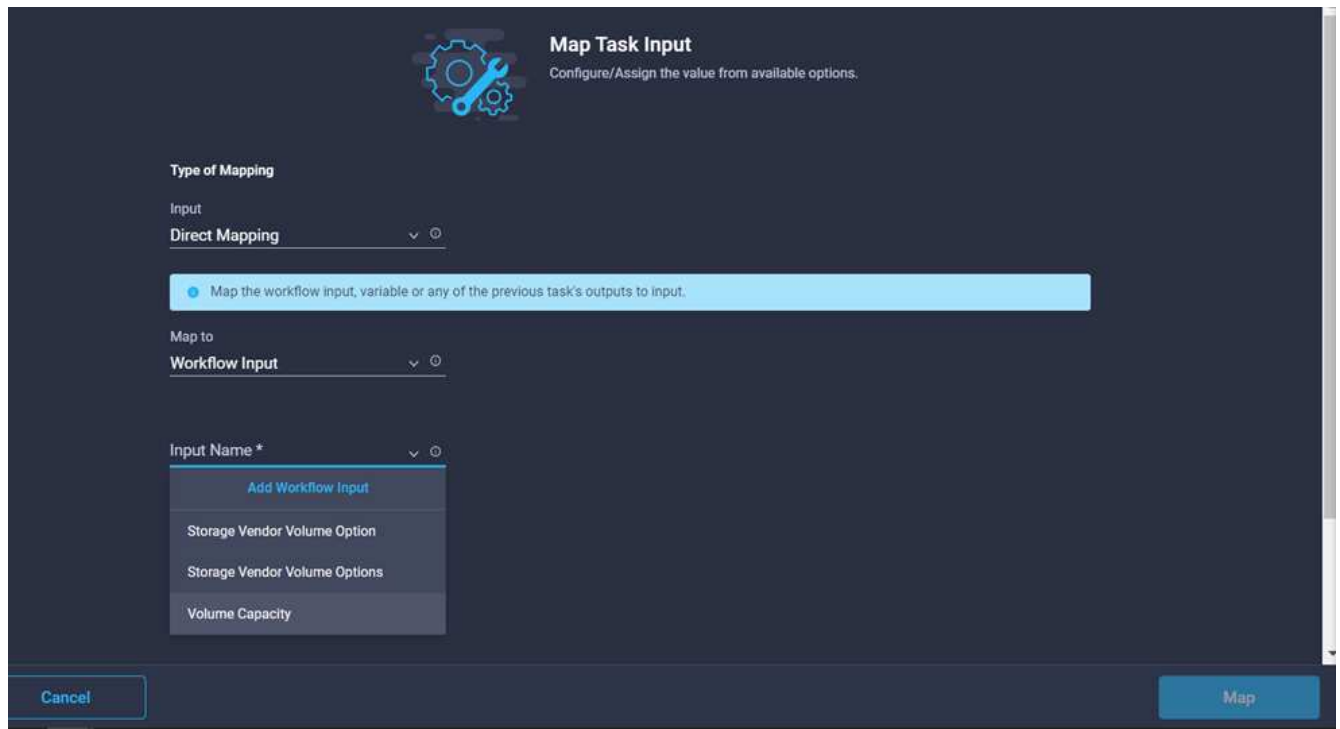
5. 在*任务属性*区域中、单击*输入*。
6. 单击*虚拟机管理程序管理器*字段中的*映射*。
7. 选择*静态值*、然后单击*选择虚拟机管理程序管理器*。单击VMware vCenter目标。



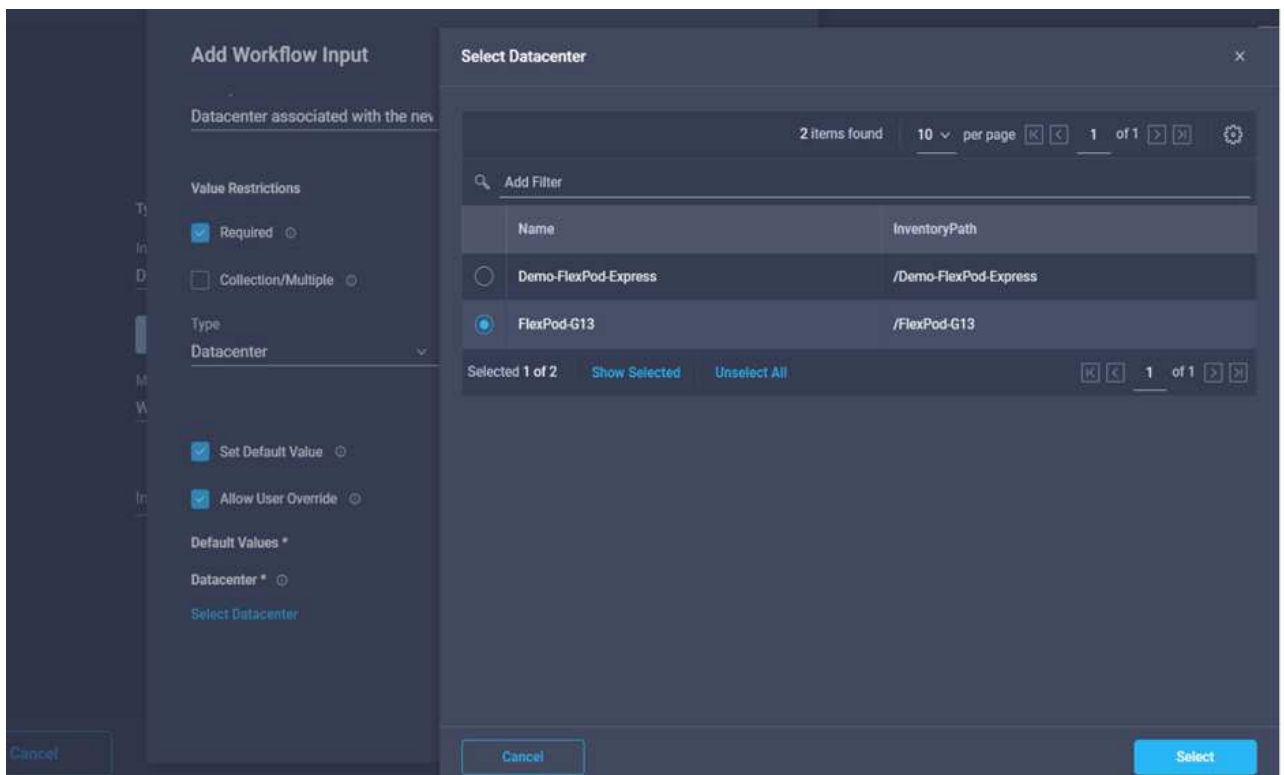
8. 单击*映射*。



9. 单击*数据中心*字段中的*映射*。这是与新数据存储库关联的数据中心。
10. 选择*直接映射*、然后单击* workflow 输入*。
11. 单击*输入名称*、然后单击*创建工作流输入*。

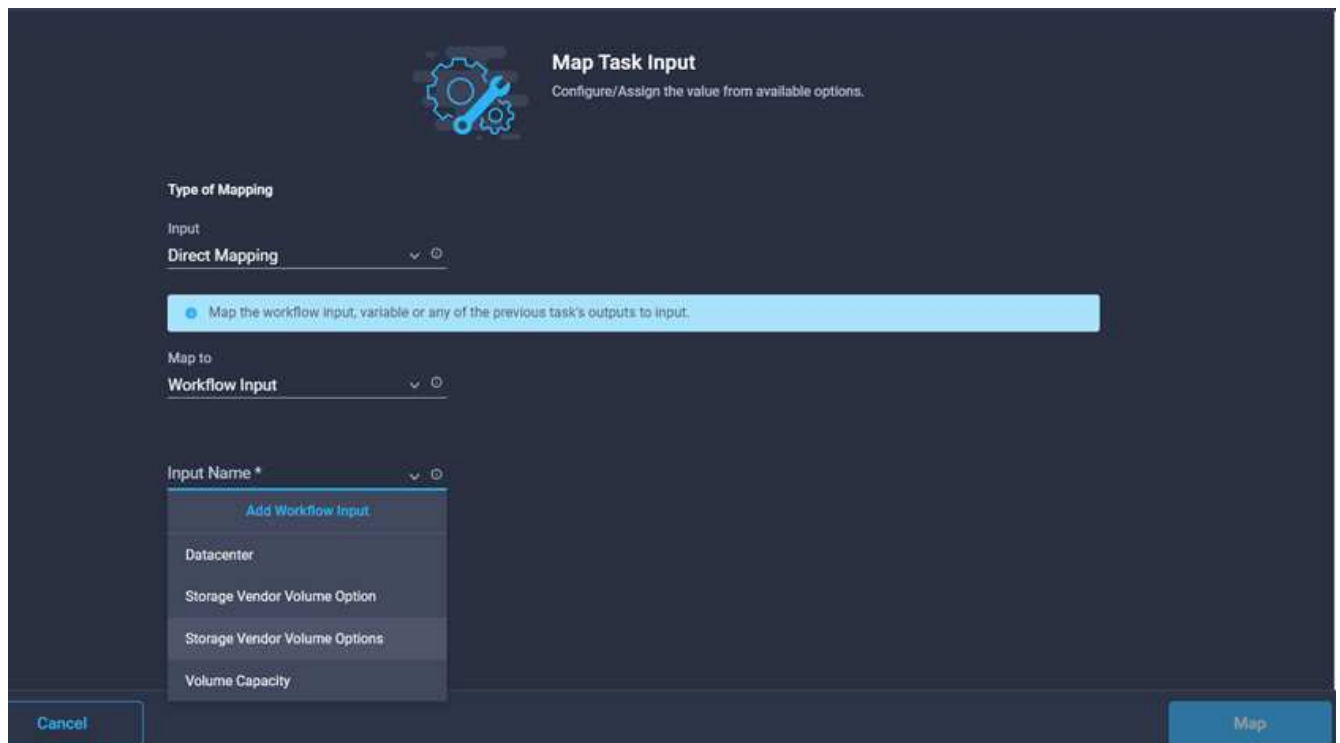


12. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)。
 - b. 选择*数据中心*作为类型。
 - c. 单击*设置默认值并覆盖*。
 - d. 单击*选择数据中心*。
 - e. 单击与新数据存储库关联的数据中心、然后单击*选择*。

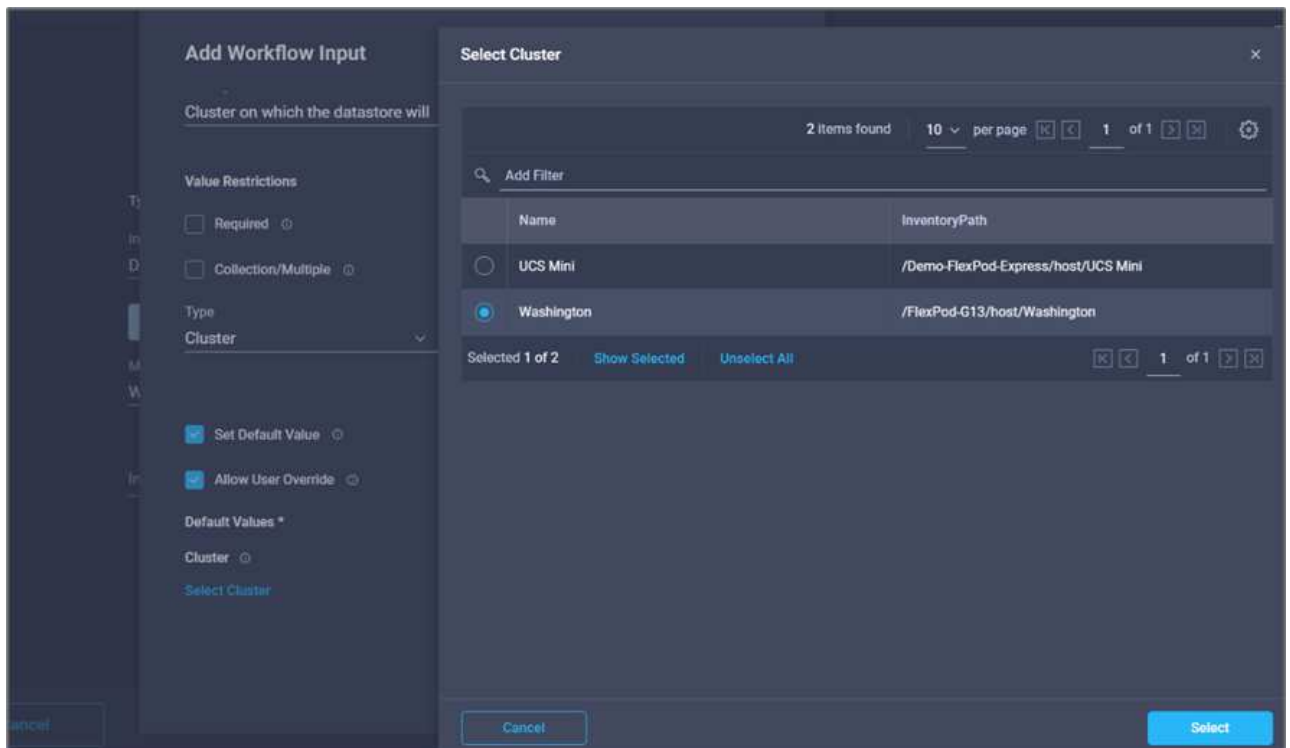


- 单击 * 添加 *。

13. 单击*映射*。
14. 单击*集群*字段中的*映射*。
15. 选择*直接映射*、然后单击*工作流输入*。



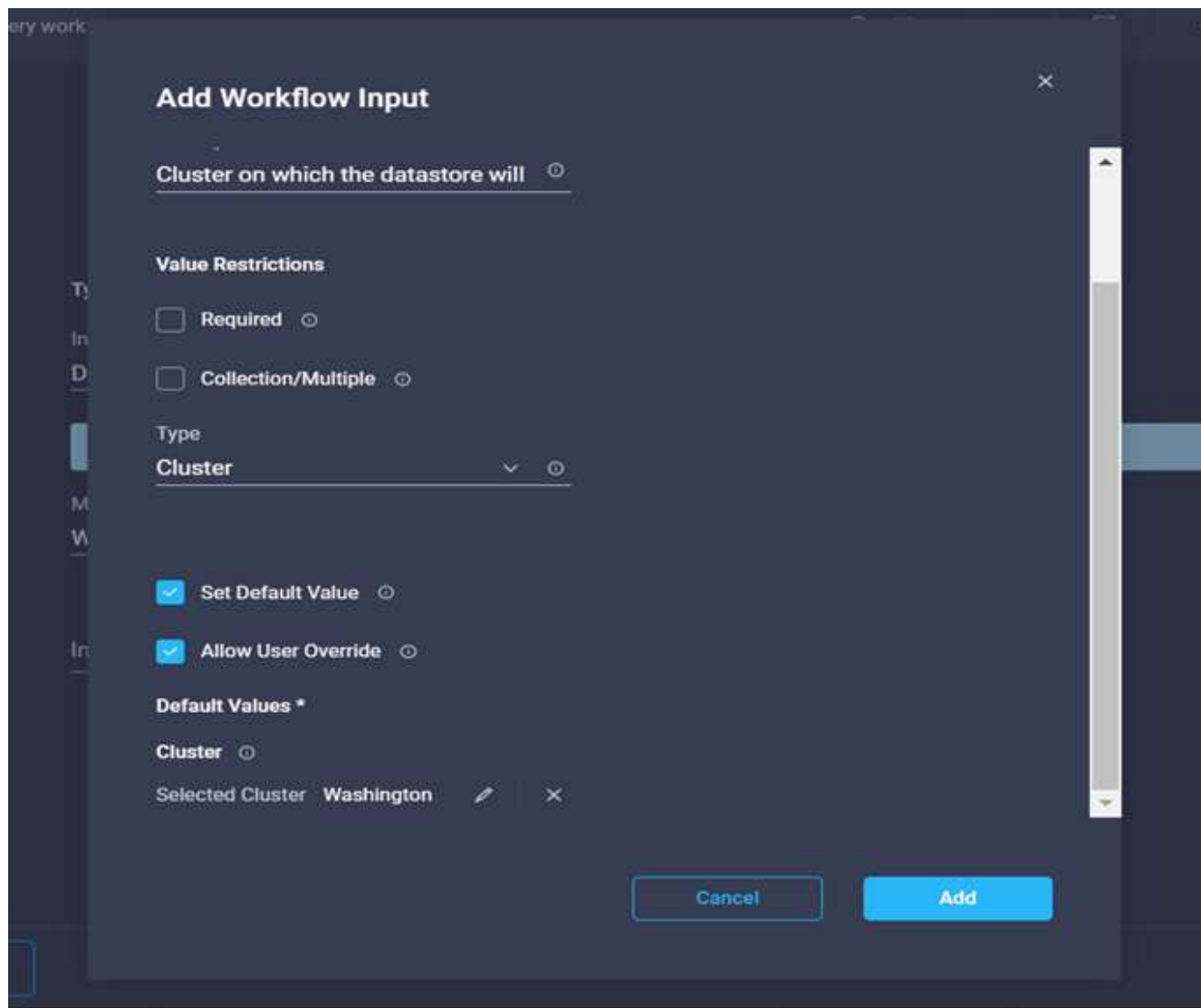
16. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)。
 - b. 单击*必需*。
 - c. 选择Cluster作为类型。
 - d. 单击*设置默认值并覆盖*。
 - e. 单击*选择集群*。
 - f. 单击与新数据存储库关联的集群。
 - g. 单击 * 选择 *。



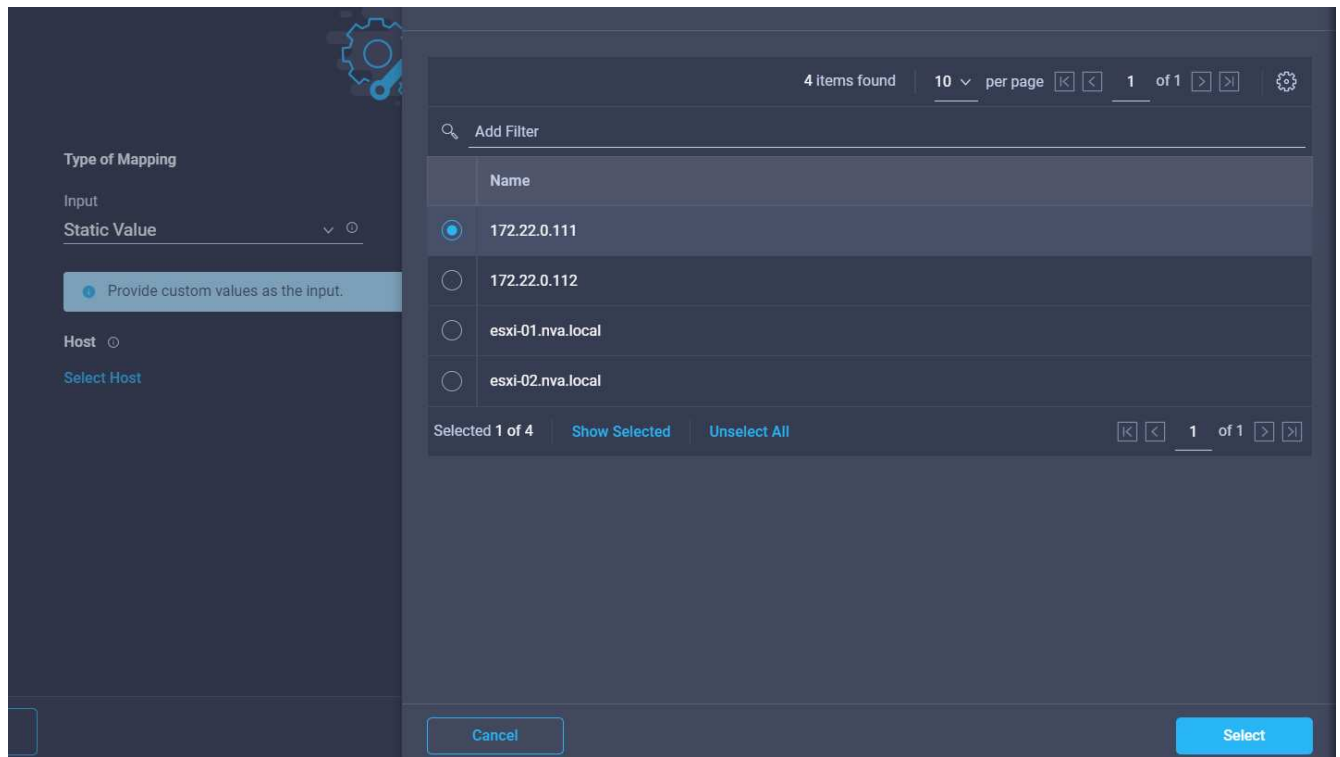
h. 单击 * 添加 *。

17. 单击*映射*。

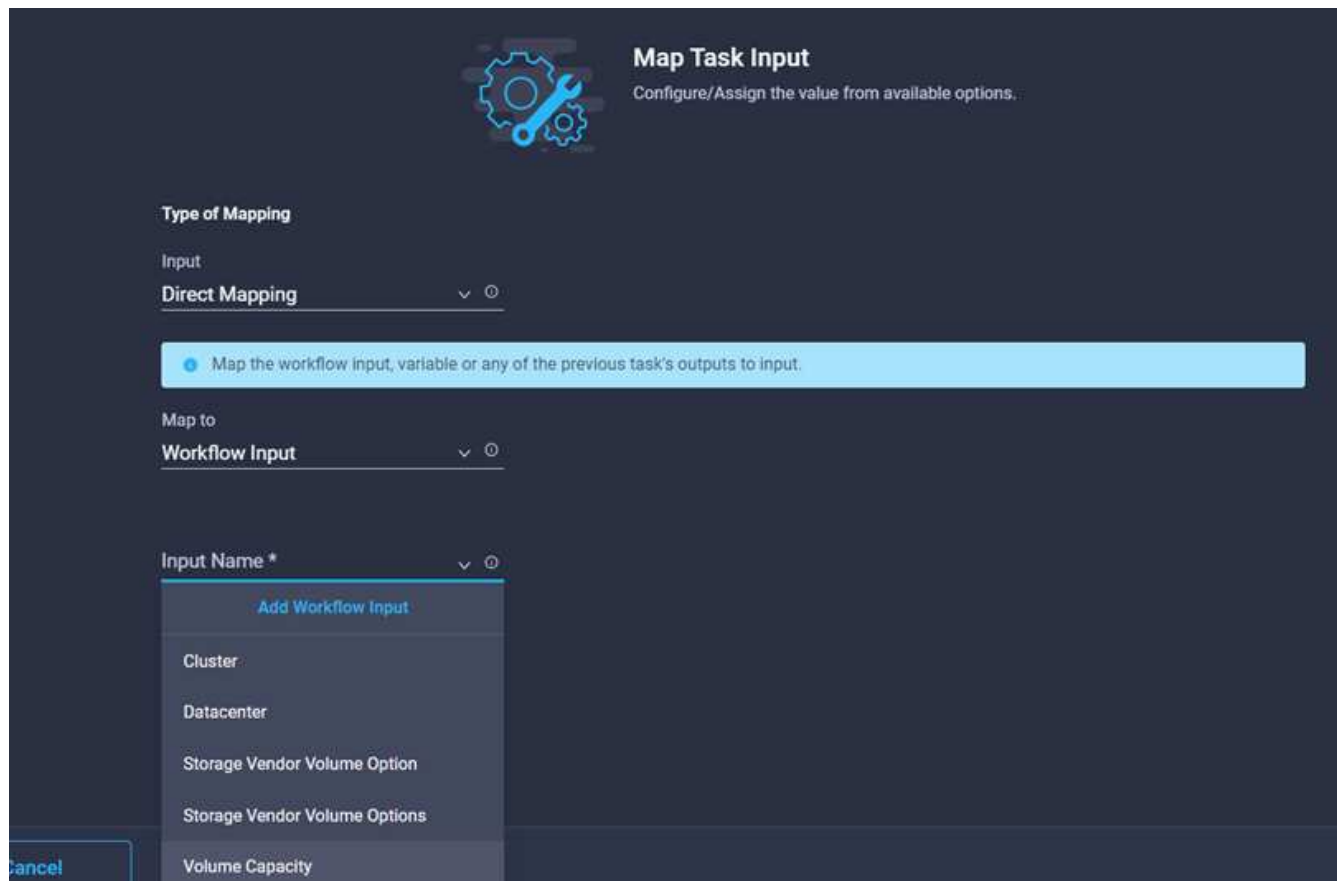
18. 单击*主机*字段中的*映射*。



19. 选择*静态值*、然后单击要托管数据存储库的主机。如果指定了集群、则会忽略主机。



20. 单击*选择并映射*。
21. 单击*数据存储库*字段中的*映射*。
22. 选择*直接映射*、然后单击*工作流输入*。
23. 单击*输入名称*和*创建工作流输入*。



The image shows a 'Map Task Input' configuration window. At the top, there is a gear icon and the title 'Map Task Input' with the subtitle 'Configure/Assign the value from available options.' Below this, the 'Type of Mapping' is set to 'Direct Mapping'. A light blue banner contains the instruction: 'Map the workflow input, variable or any of the previous task's outputs to input.' The 'Map to' dropdown is set to 'Workflow Input'. The 'Input Name *' dropdown is open, showing a list of options: 'Add Workflow Input' (highlighted in blue), 'Cluster', 'Datacenter', 'Storage Vendor Volume Option', 'Storage Vendor Volume Options', and 'Volume Capacity'. A 'Cancel' button is visible at the bottom left.

Map Task Input
Configure/Assign the value from available options.

Type of Mapping
Input
Direct Mapping

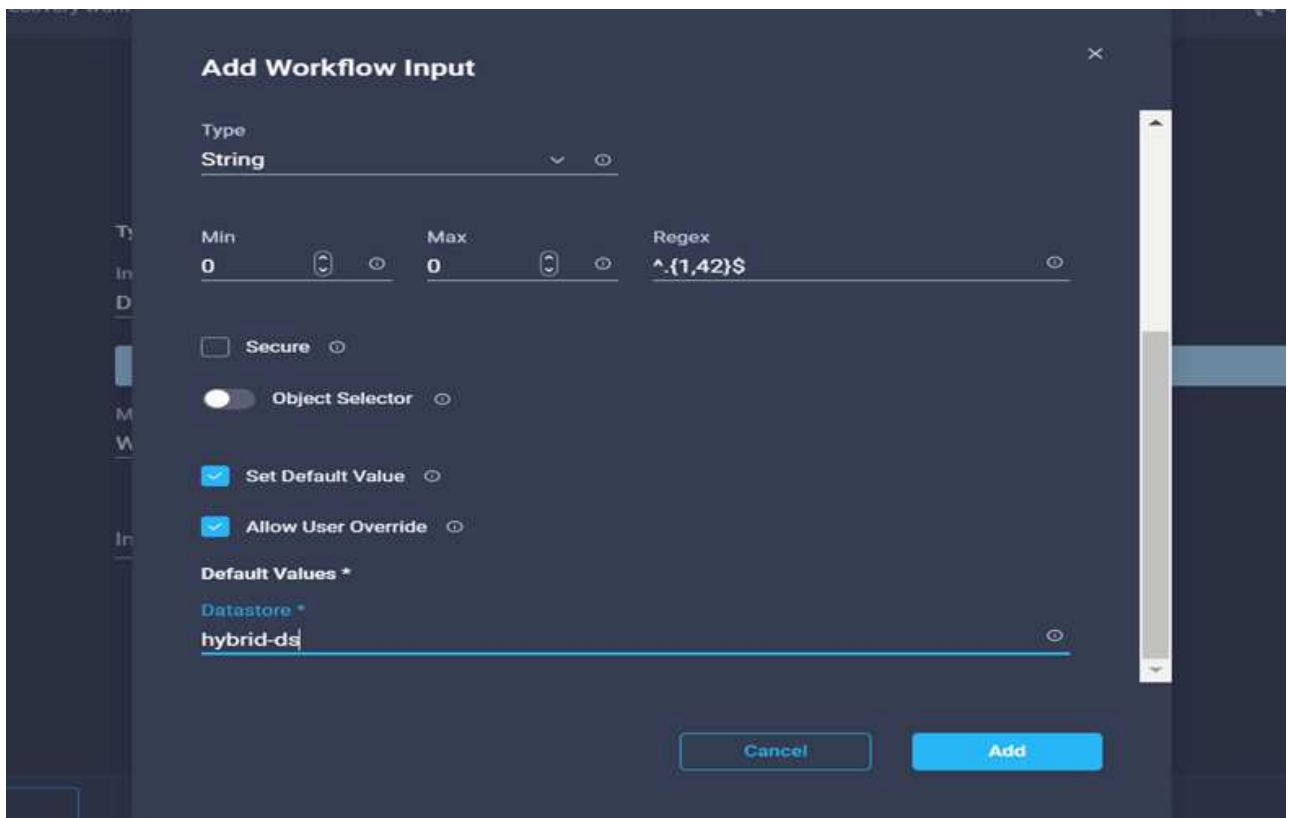
Map the workflow input, variable or any of the previous task's outputs to input.

Map to
Workflow Input

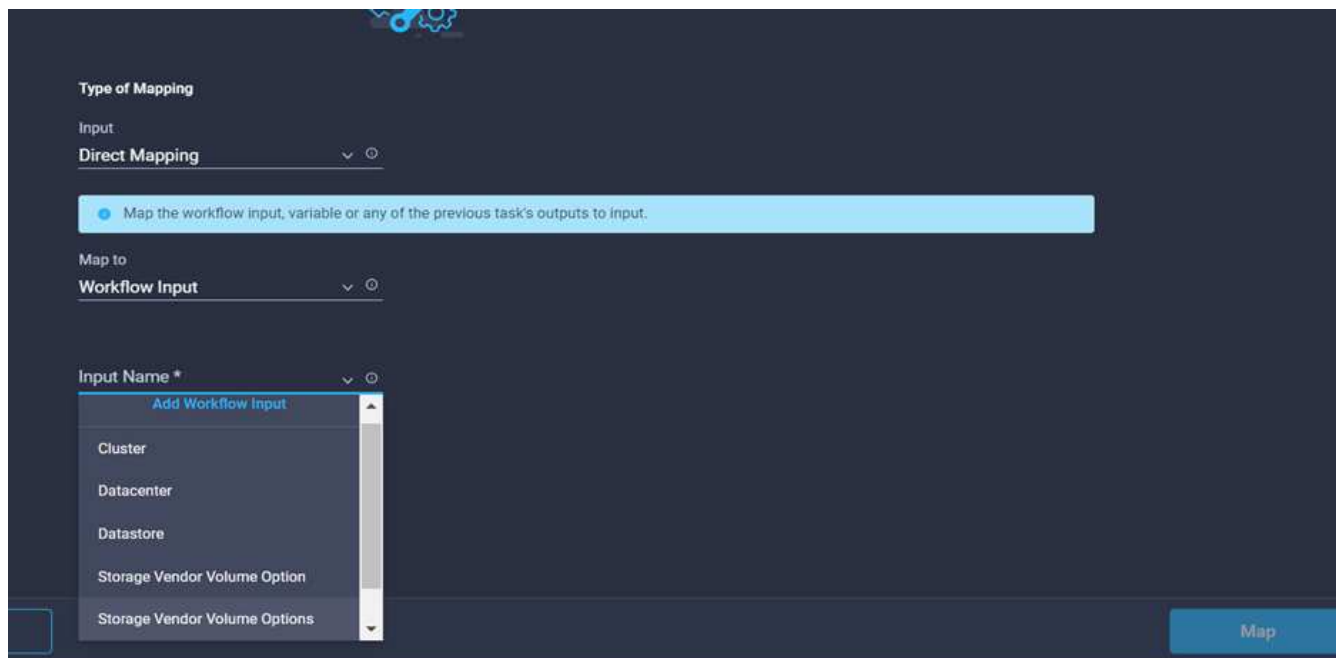
Input Name *
Add Workflow Input
Cluster
Datacenter
Storage Vendor Volume Option
Storage Vendor Volume Options
Volume Capacity

Cancel

24. 在添加输入向导中：
- 提供显示名称和参考名称(可选)。
 - 单击*必需*。
 - 单击*设置默认值并覆盖*。
 - 为数据存储库提供默认值、然后单击*添加*。



25. 单击*映射*。
26. 单击输入字段*数据存储库类型*中的*映射*。
27. 选择*直接映射*、然后单击*工作流输入*。
28. 单击*输入名称*和*创建工作流输入*。



29. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)、然后单击*必需*。

- b. 确保选择类型*数据存储库类型*、然后单击*设置默认值和覆盖*。

Add Workflow Input

Display Name *
Type of Datastore

Reference Name *
DatastoreVersion

Description
Type and version of the new dataset

Value Restrictions

☒ Required

☐ Collection/Multiple

Type
Types of Datastore

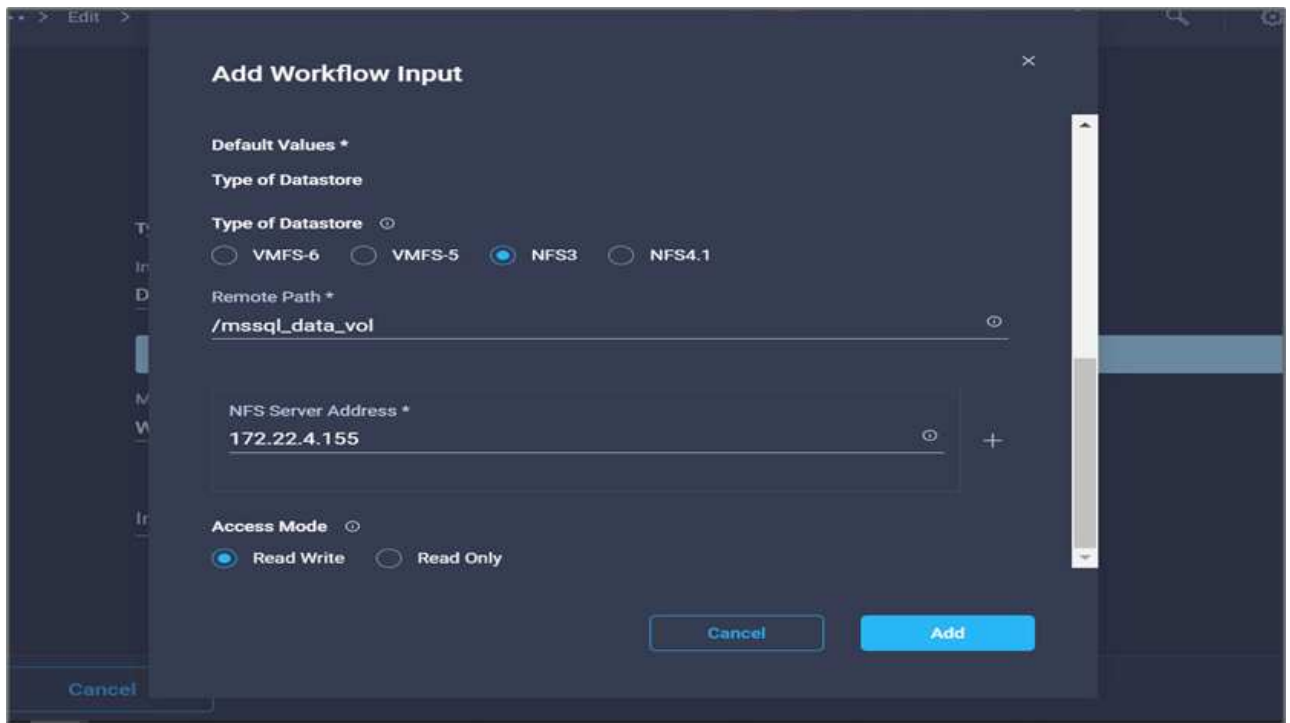
☒ Set Default Value

☒ Allow User Override

Default Values *
Type of Datastore

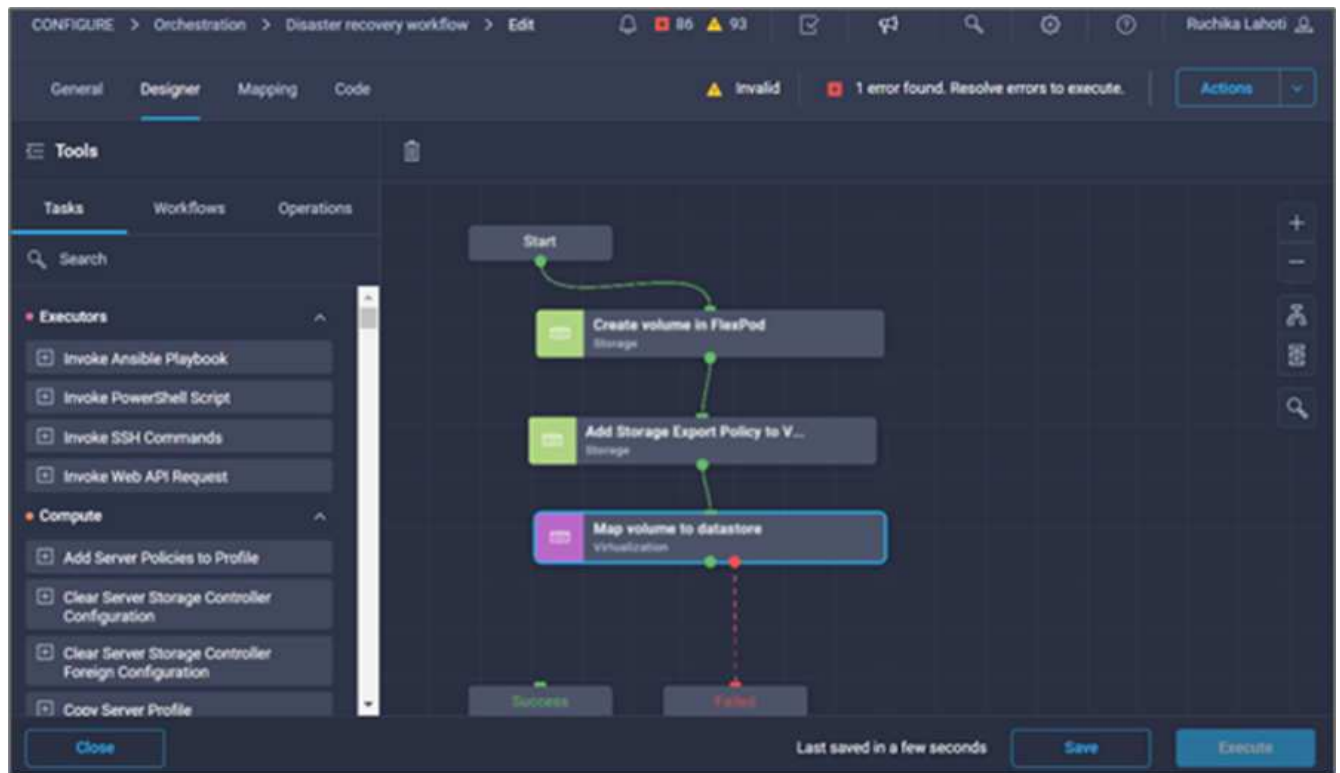
Cancel Add

- c. 提供远程路径。这是NFS挂载点的远程路径。
- d. 在NFS服务器地址中提供远程NFS服务器的主机名或IP地址。
- e. 单击*访问模式*。访问模式适用于NFS服务器。如果卷导出为只读、请单击只读。单击 * 添加 *。

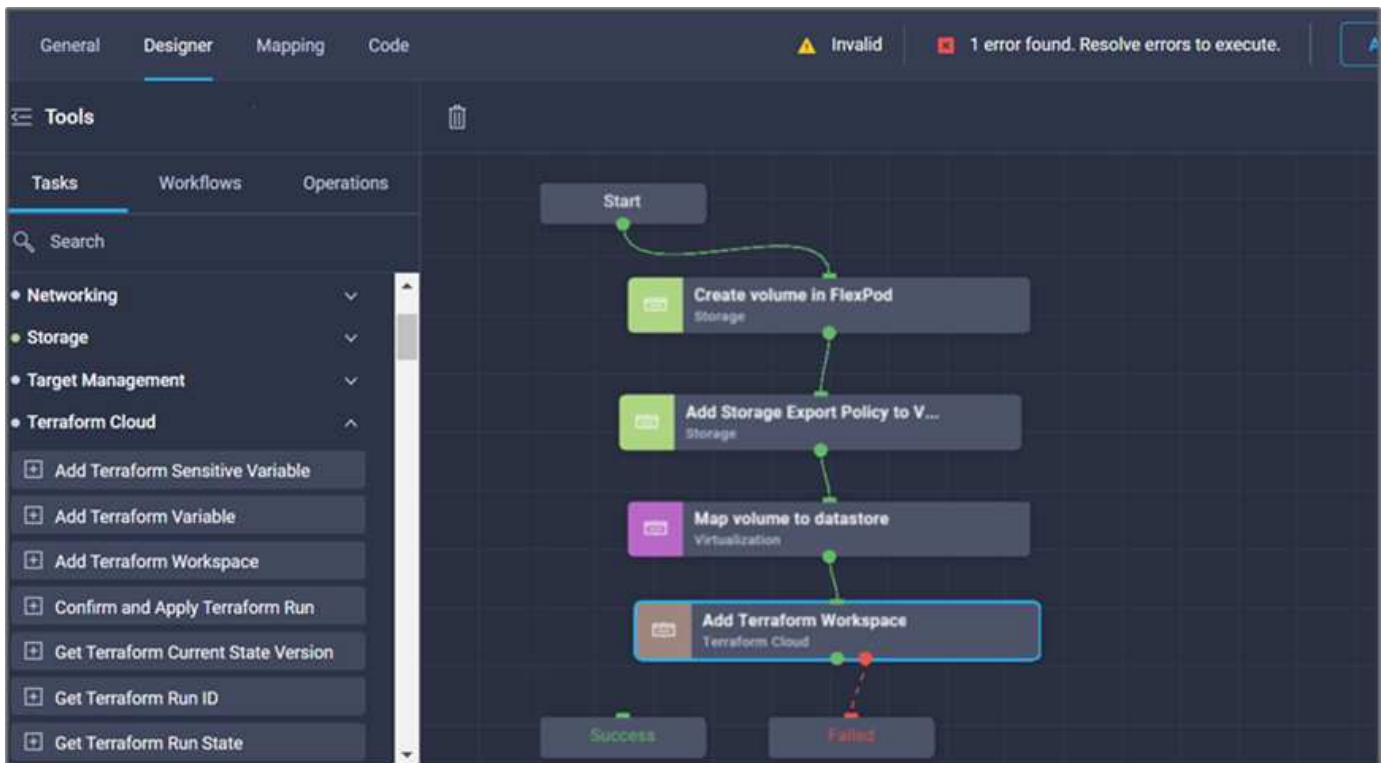


30. 单击*映射*。

31. 单击 * 保存 *。

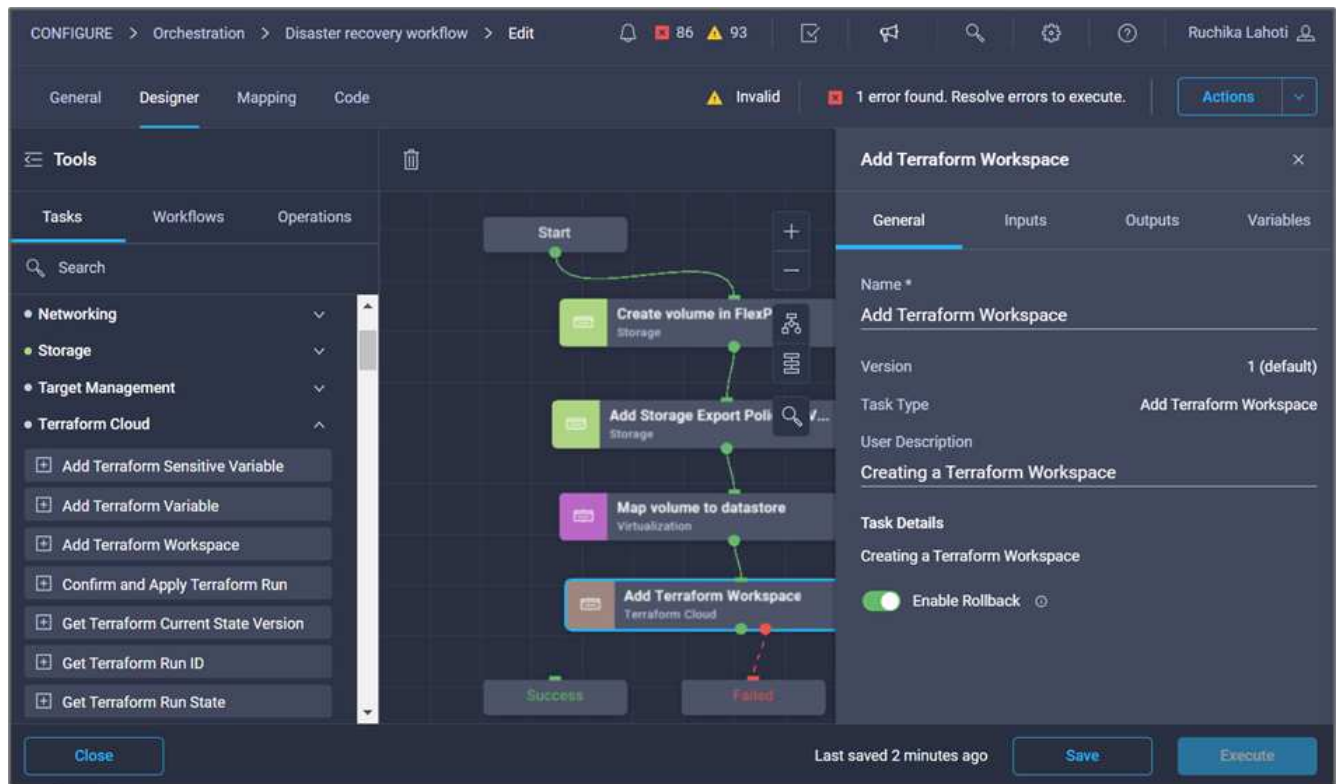


此操作将完成创建数据存储库的任务。在内部FlexPod 数据中心中执行的所有任务均已完成。

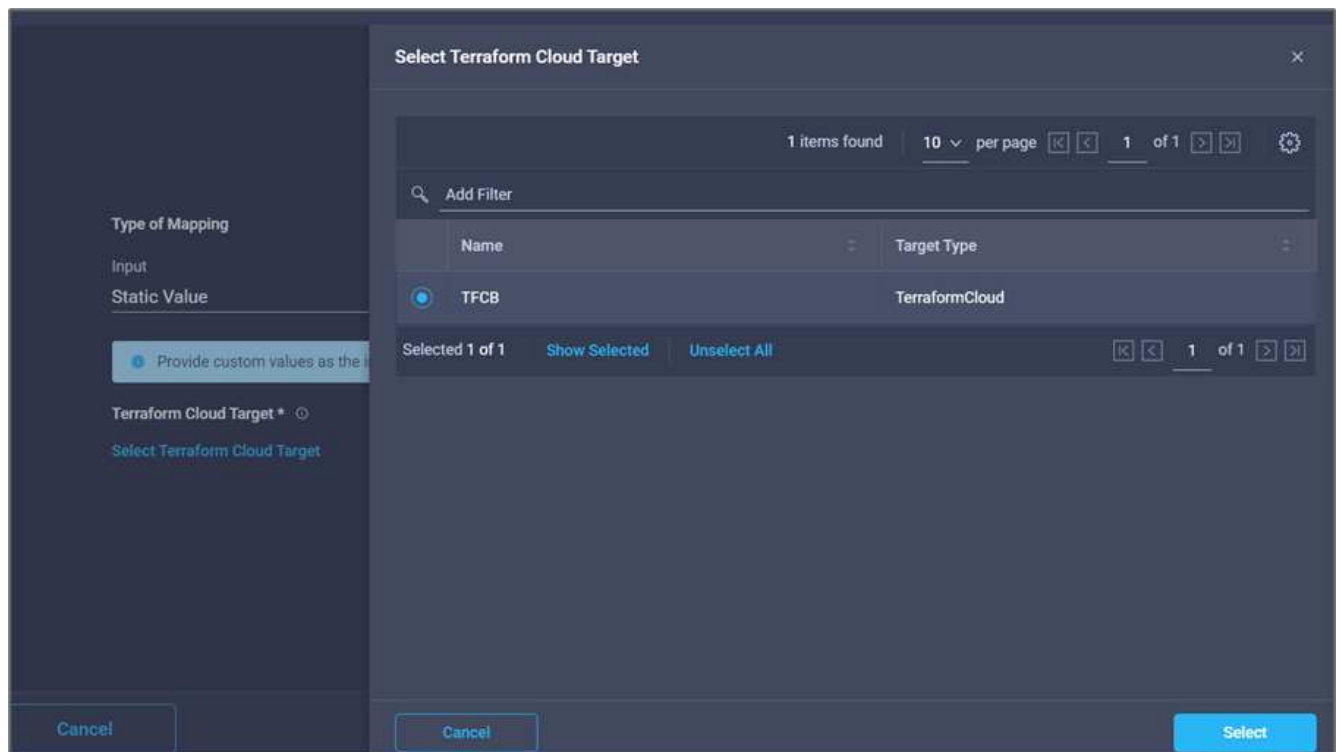


操作步骤 5：添加新的Terraform工作空间

1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从"设计"区域的"工具"部分拖放* Terraform Cloud >添加Terraform Workspace*任务。
3. 使用Connector将*映射卷连接到数据存储库*和*添加Terraform Workspace*任务、然后单击*保存*。
4. 单击*添加Terraform Workspace*。在任务属性区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。

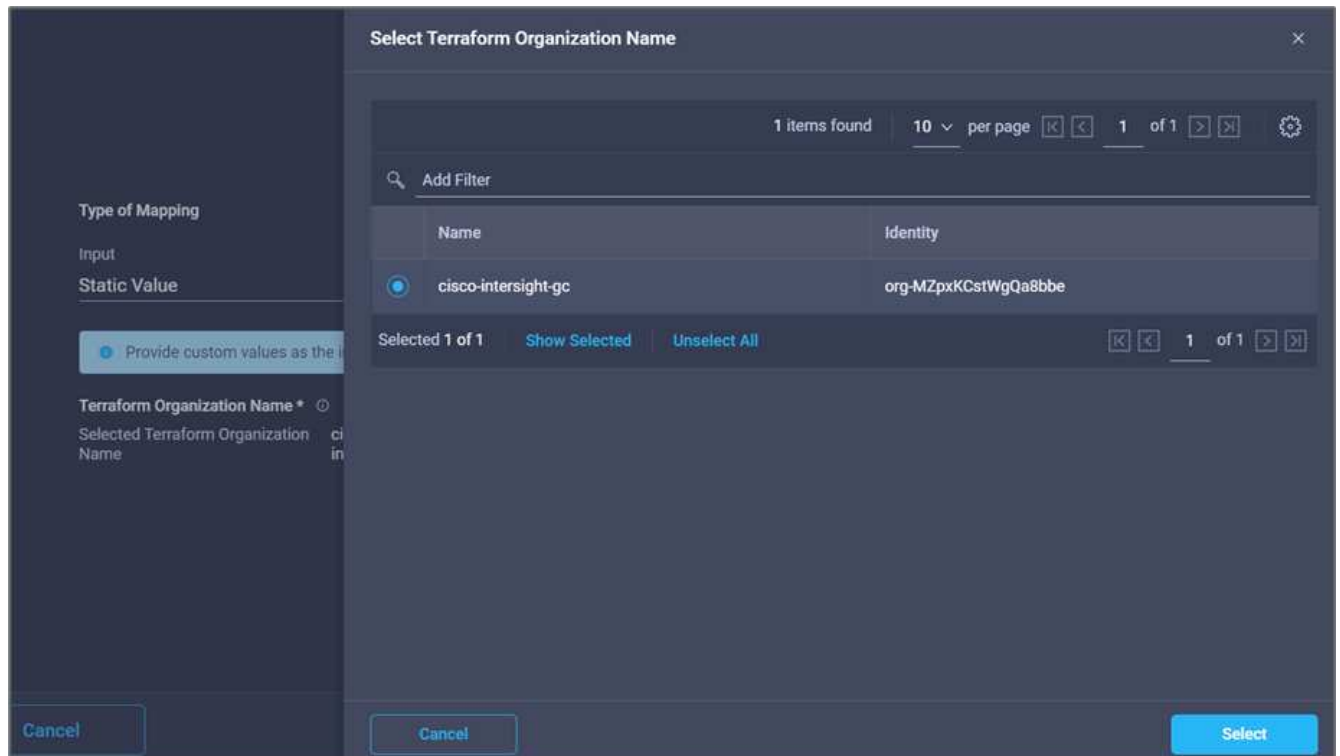


5. 在任务属性区域中、单击*输入*。
6. 单击输入字段* Terraform Cloud Target*中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择按照中所述添加的Terraform Cloud for Business帐户 "为HashiCorp Terraform配置Cisco Intersight Service"。

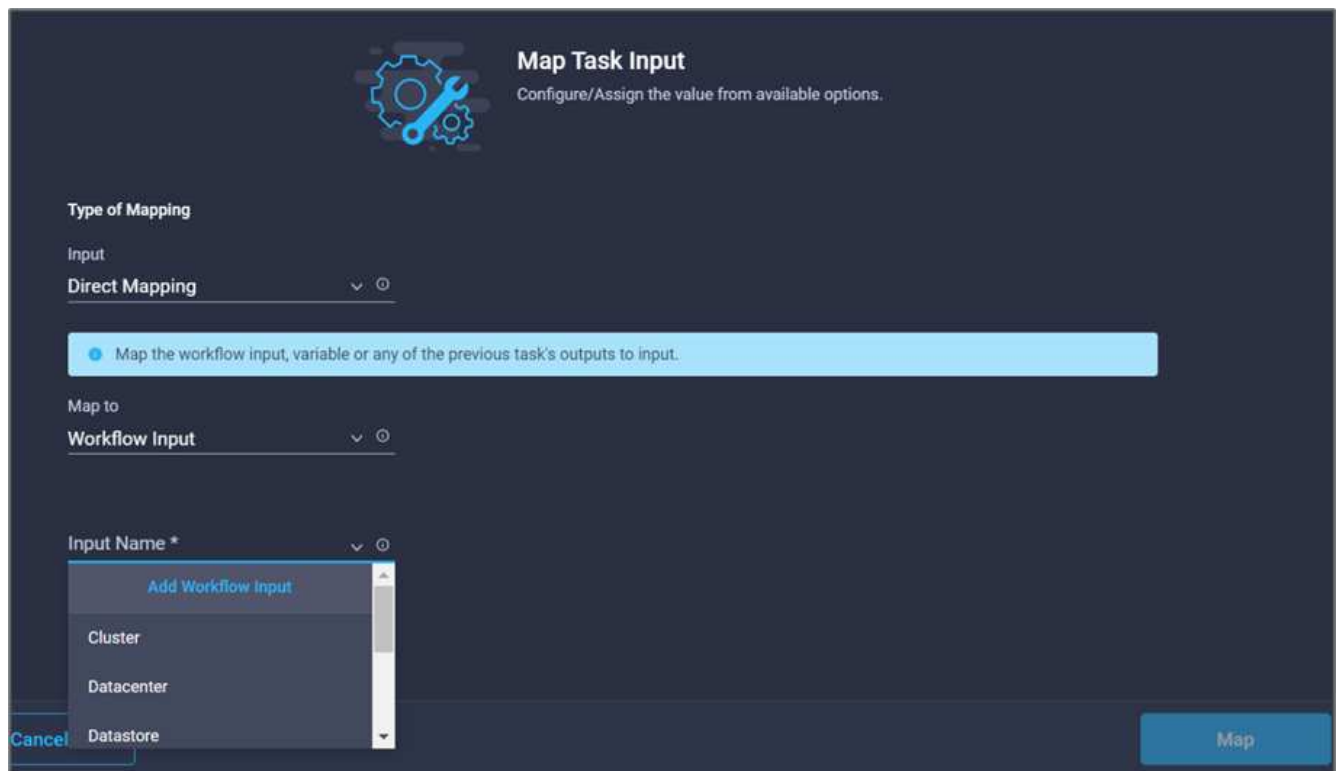


8. 单击*映射*。

9. 单击输入字段* Terraform Organization Name*中的*映射*。
10. 选择*静态值*、然后单击*选择Terraform Organization*。在Terraform Cloud for Business帐户中选择您所属的Terraform组织的名称。



11. 单击*映射*。
12. 单击* Terraform Workspace Name*字段中的*映射*。这是Terraform Cloud for Business帐户中的新工作空间。
13. 选择*直接映射*、然后单击* workflow 输入*。
14. 单击*输入名称*和*创建工作流输入*。



The image shows a 'Map Task Input' dialog box with a dark blue background. At the top left is a gear and wrench icon. The title 'Map Task Input' is at the top right, with the subtitle 'Configure/Assign the value from available options.' below it. The 'Type of Mapping' section has a dropdown menu set to 'Input', and the 'Direct Mapping' option is selected. A light blue instruction bar says 'Map the workflow input, variable or any of the previous task's outputs to input.' The 'Map to' section has a dropdown menu set to 'Workflow Input'. The 'Input Name *' section has a dropdown menu with options: 'Add Workflow Input' (highlighted in blue), 'Cluster', 'Datacenter', and 'Datastore'. At the bottom left is a 'Cancel' button, and at the bottom right is a 'Map' button.

Map Task Input
Configure/Assign the value from available options.

Type of Mapping
Input
Direct Mapping

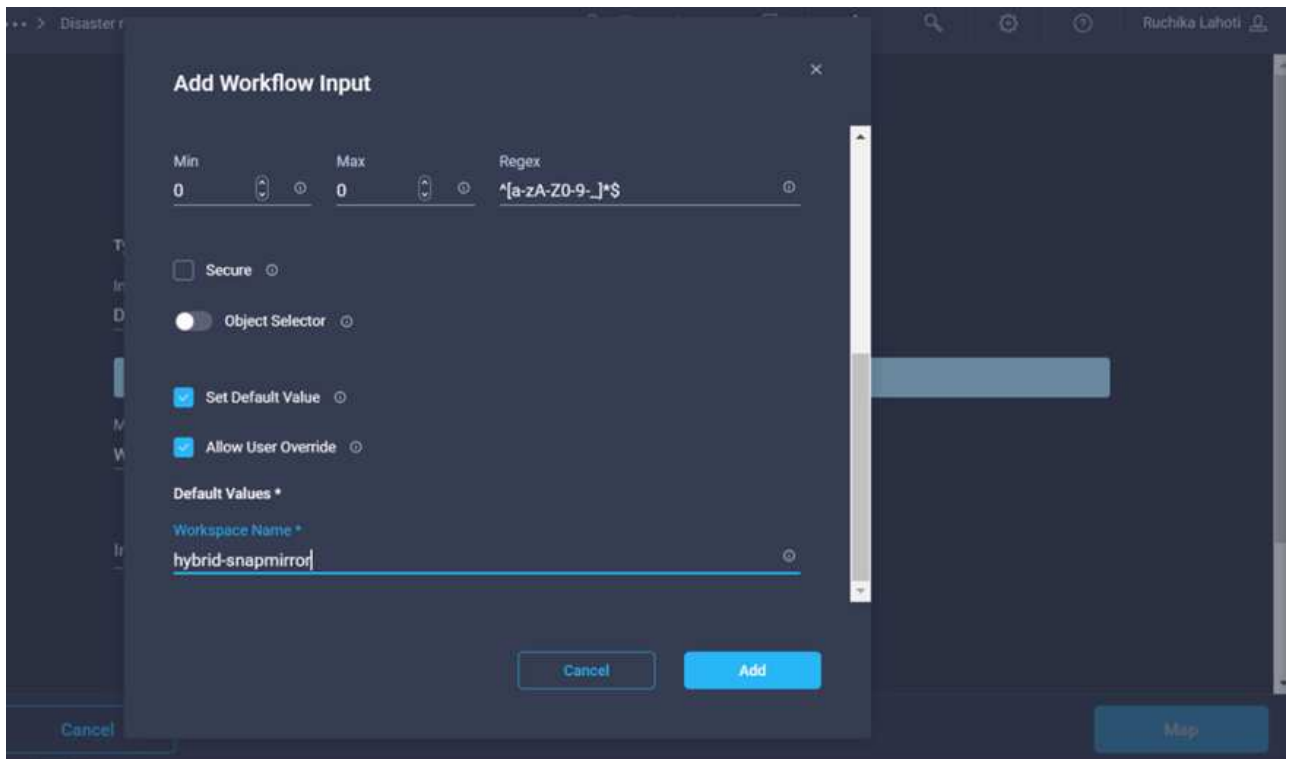
Map the workflow input, variable or any of the previous task's outputs to input.

Map to
Workflow Input

Input Name *
Add Workflow Input
Cluster
Datacenter
Datastore

Cancel Map

15. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)。
 - b. 单击*必需*。
 - c. 确保为*类型*选择*字符串*。
 - d. 单击*设置默认值并覆盖*。
 - e. 提供工作空间的默认名称。
 - f. 单击 * 添加 *。



16. 单击*映射*。
17. 单击*工作空间问题描述 字段中的*映射*。
18. 选择*直接映射*、然后单击*工作流输入*。
19. 单击*输入名称*和*创建工作流输入*。

Add Workflow Input

Workspace Description ⓘ WorkspaceDescription ⓘ

Description

Description of the Terraform Work: ⓘ

Value Restrictions

☐ Required ⓘ

☐ Collection/Multiple ⓘ

Type

String ▼ ⓘ

Min 0 ⓘ Max 0 ⓘ

Regex ⓘ

☐ Secure ⓘ

☐ Object Selector ⓘ

☒ Set Default Value ⓘ

☒ Allow User Override ⓘ

Cancel **Add**

20. 在添加输入向导中、完成以下步骤：
- 提供显示名称和参考名称(可选)。
 - 确保为*类型*选择*字符串*。
 - 单击*设置默认值并覆盖*。
 - 提供工作空间问题描述、然后单击*添加*。

Add Workflow Input

Value Restrictions

☐ Required ⓘ

☐ Collection/Multiple ⓘ

Type
String ▼ ⓘ

Min **0** ⓘ Max **0** ⓘ Regex ⓘ

☐ Secure ⓘ

☒ Object Selector ⓘ

☒ Set Default Value ⓘ

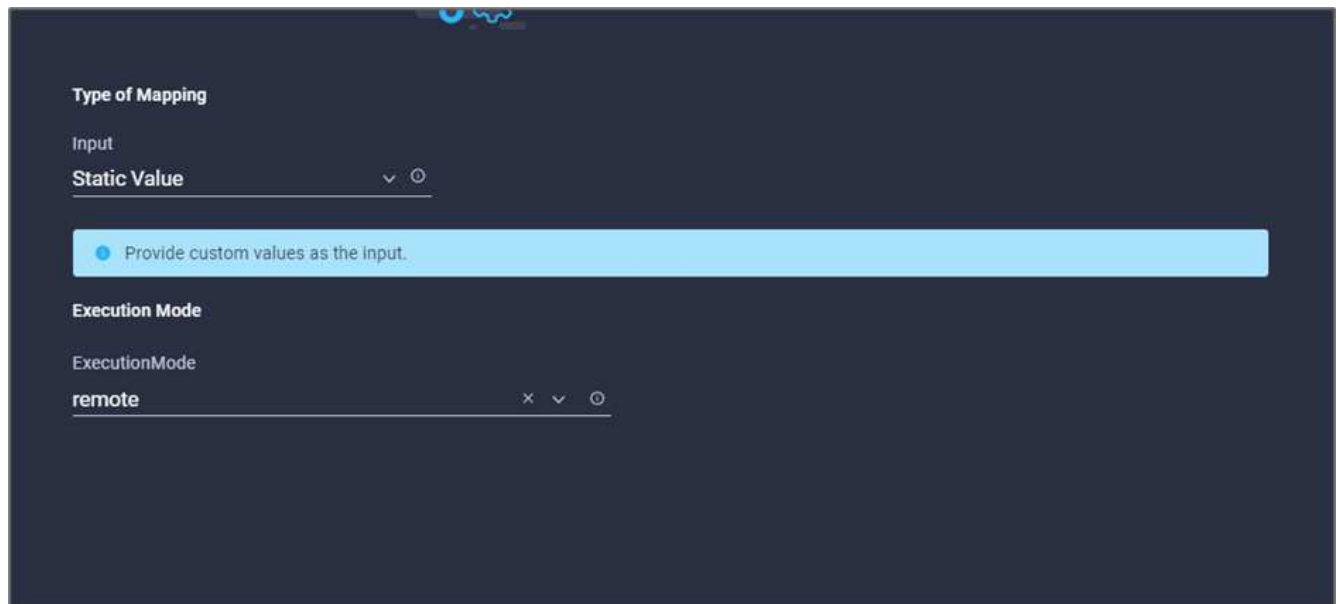
☒ Allow User Override ⓘ

Default Values *

Workspace Description
workspace to create CVO and configure SnapMirror ⓘ

Cancel Add

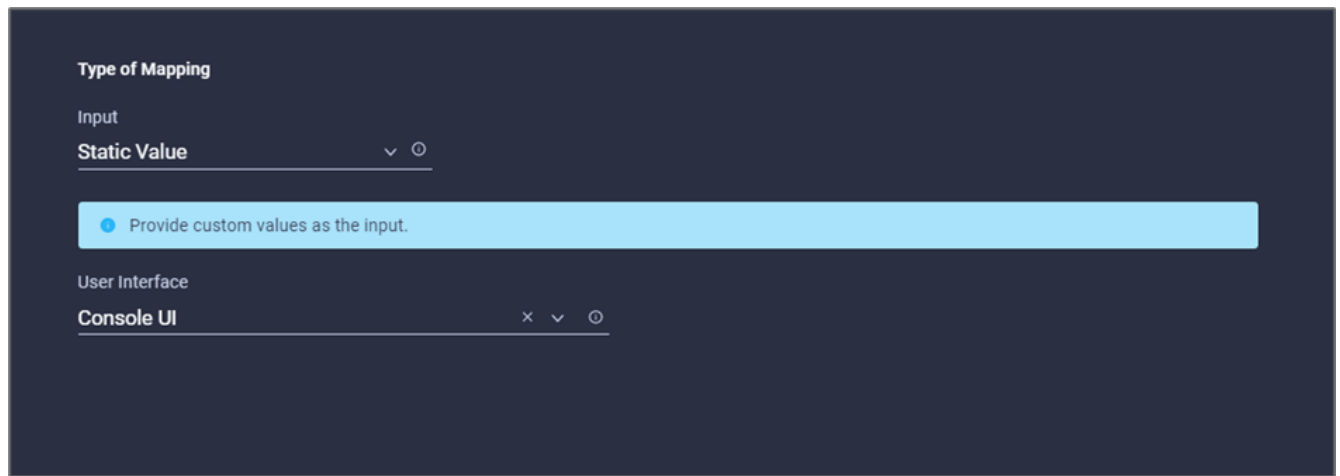
21. 单击*映射*。
22. 单击*执行模式*字段中的*映射*。
23. 选择*静态值*、单击*执行模式*、然后单击*远程*。



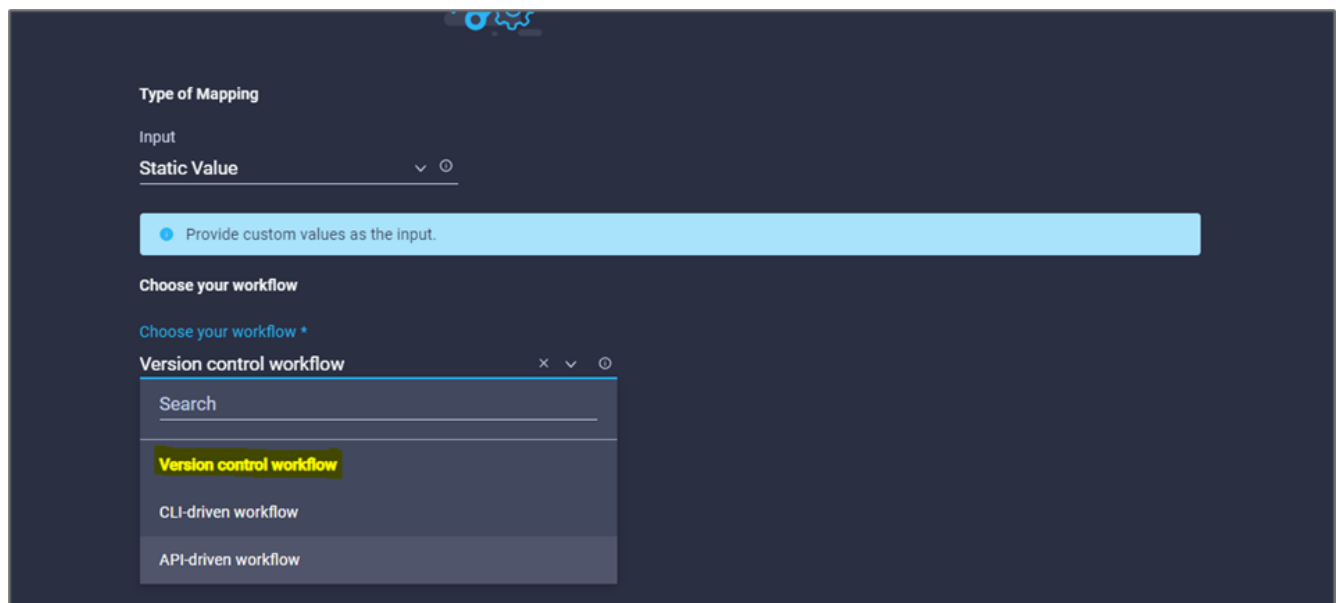
24. 单击*映射*。
25. 单击*应用方法*字段中的*映射*。
26. 选择*静态值*、然后单击*应用方法*。单击*手动应用*。



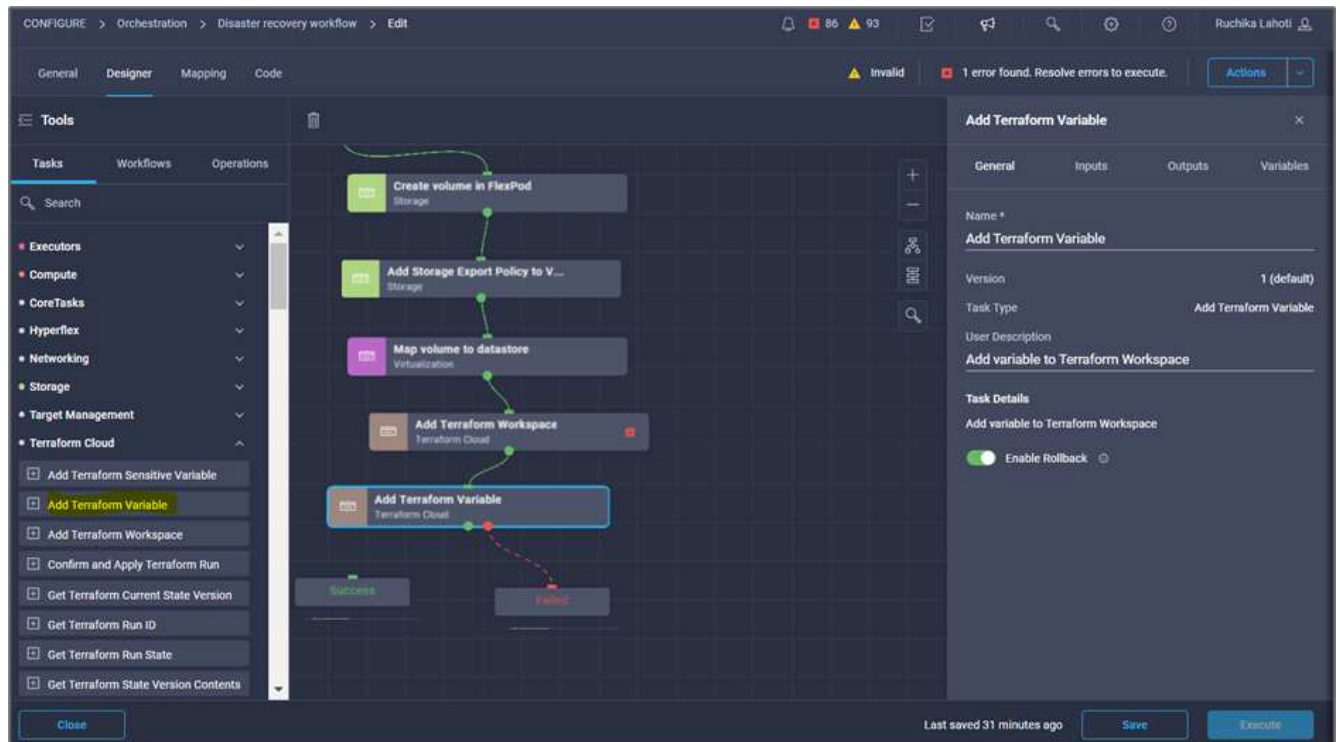
27. 单击*映射*。
28. 单击*用户界面*字段中的*映射*。
29. 选择*静态值*、然后单击*用户界面*。单击*控制台U*。



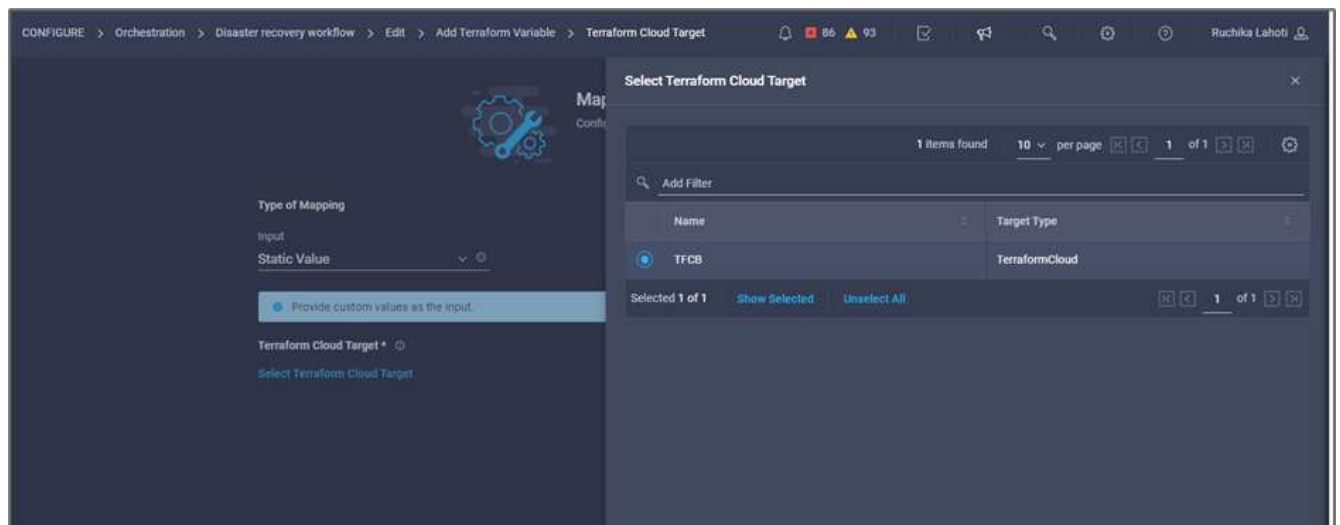
30. 单击*映射*。
31. 单击输入字段中的*映射*并选择您的工作流。
32. 选择*静态值*、然后单击*选择您的工作流*。单击*版本控制工作流*。



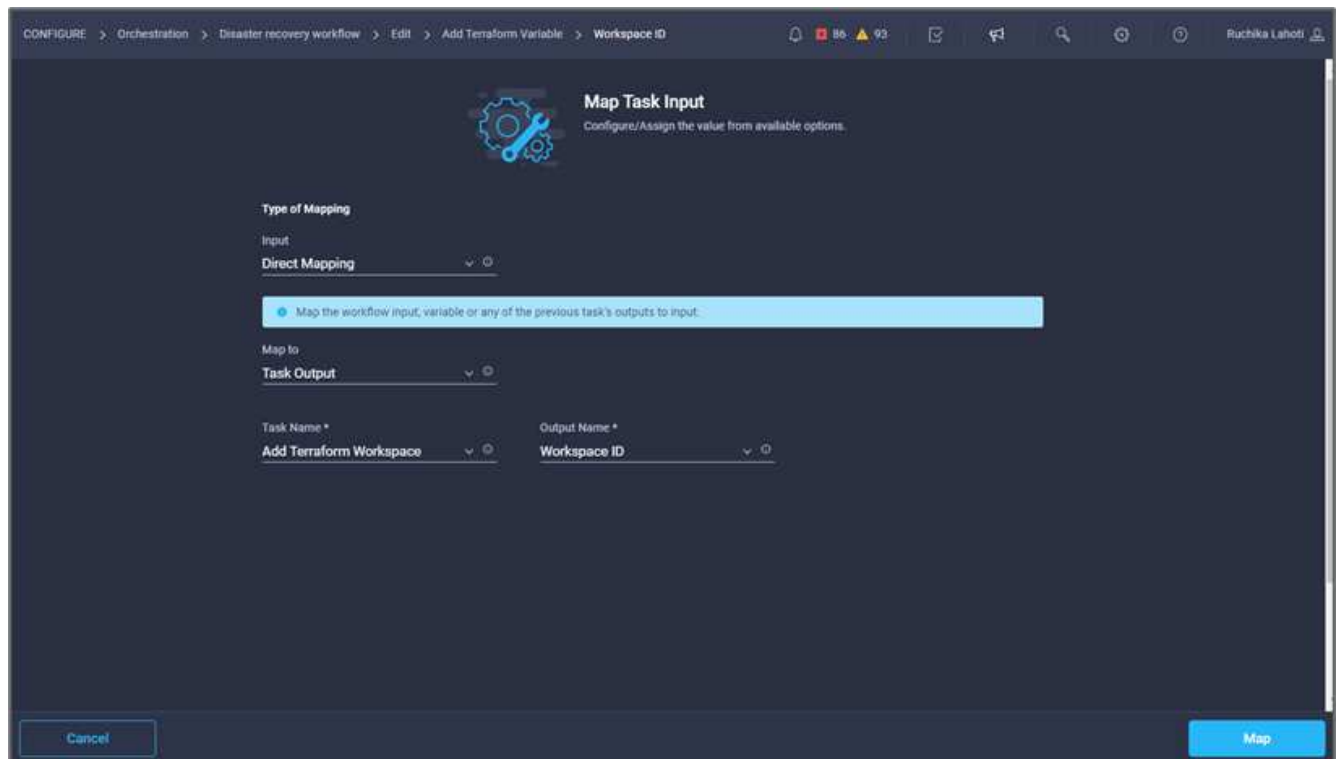
33. 提供以下GitHub存储库详细信息：
 - a. 在*存储库名称*中、输入一节中详细介绍的存储库名称 `""设置环境前提条件""`。
 - b. 按照一节中的详细说明提供OAuth令牌ID `""设置环境前提条件""`。
 - c. 选择*自动运行触发*选项。



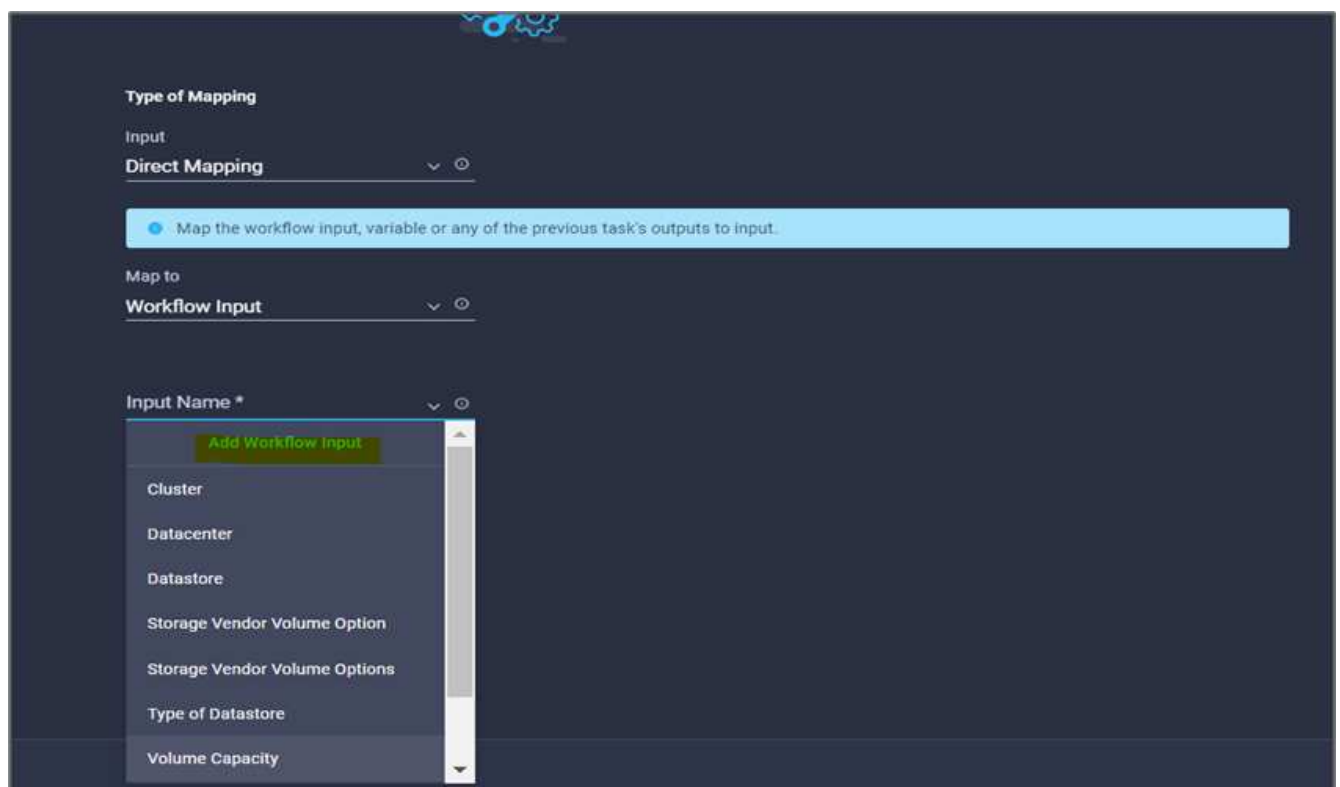
5. 在*工作流属性*区域中、单击*输入*。
6. 单击* Terraform Cloud Target*字段中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择按照中所述添加的Terraform Cloud for Business帐户 "为HashiCorp Terraform配置Cisco Intersight Service"。



8. 单击*映射*。
9. 单击* Terraform Organization Name 字段中的*映射*。
10. 选择*静态值*、然后单击*选择Terraform Organization*。在Terraform Cloud for Business帐户中选择您所属的Terraform组织的名称。



11. 单击*映射*。
12. 单击* Terraform Workspace Name*字段中的*映射*。
13. 选择*直接映射*、然后单击*任务输出*。
14. 单击*任务名称*、然后单击*添加Terraform Workspace*。



15. 单击*输出名称*、然后单击*工作空间名称*。
16. 单击*映射*。
17. 单击*添加变量选项*字段中的*映射*。
18. 选择*直接映射*、然后单击*工作流输入*。
19. 单击*输入名称*和*创建工作流输入*。

Add Workflow Input

Display Name *
Terraform Variable

Reference Name *
TerraformAddVariable

Description
Terraform Variable to be added

Value Restrictions

☒ Required

☐ Collection/Multiple

Type
String

Min
0

Max
0

Regex

☐ Secure

☐ Object Selector

Cancel **Add**

20. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)。
 - b. 确保为*类型*选择*字符串*。

- c. 单击*设置默认值并覆盖*。
- d. 单击*变量类型*、然后单击*非敏感变量*。

21. 在*添加Terraform变量*部分中、提供以下信息：

- 密钥name_of_on-prem-ontap
- *值。*请提供内部ONTAP 的名称。
- 内部ONTAP 的*问题描述。*名称。

22. 单击**以添加其他变量。

☒ Set Default Value ⓘ

☒ Allow User Override ⓘ

Default Values *

Terraform Variable

Key *

name_of_on-prem-ontap ⓘ

Value

Provide the name of On-premise ONTAP added in section Deploying ⓘ

Description

Name of the On-premise ONTAP ⓘ

☐ HCL ⓘ

+

Cancel Add

23. 添加所有Terraform变量、如下表所示。您还可以提供默认值。

Terraform变量名称	Description
name__of_on-prem-ontap	内部ONTAP (FlexPod)的名称
on-prem-ontap_cluster_IP	存储集群管理接口的IP地址
on-prem-ontap_user_name	存储集群的管理员用户名
分区	要创建工作环境的GCP区域
子网ID	要创建工作环境的GCP子网ID
vpc_id	要创建工作环境的VPC ID
capacity_package_name	要使用的许可证类型
source_volume	源卷的名称
source_storage_vm_name	源SVM的名称
destination_volume	Cloud Volumes ONTAP 上的卷名称
schedule_of_replication	默认值为1小时
name_of_volume_to_create_on_CVO	云卷的名称
工作空间ID	要创建工作环境的workspace ID
项目ID	要创建工作环境的project_id
name_of_CVO_cluster	Cloud Volumes ONTAP 工作环境的名称
gcp_service_account	Cloud Volumes ONTAP 工作环境的gcp_service_account

24. 单击*映射*、然后单击*保存*。

Add Terraform Variable

General

Inputs

Outputs

Variables

Search

Terraform Cloud Target *

Edit Mapping

Custom Value

View Value

Workspace ID *

Edit Mapping

Task Output

WorkspaceId | Add Terraform Work...

Terraform Variable

Edit Mapping

Workflow Input

Terraform Variables

Last saved an hour ago

Save

Execute

此时、将完成向工作空间添加所需Terraform变量的任务。接下来、将所需的敏感Terraform变量添加到工作空间中。您也可以将这两者合并到一个任务中。

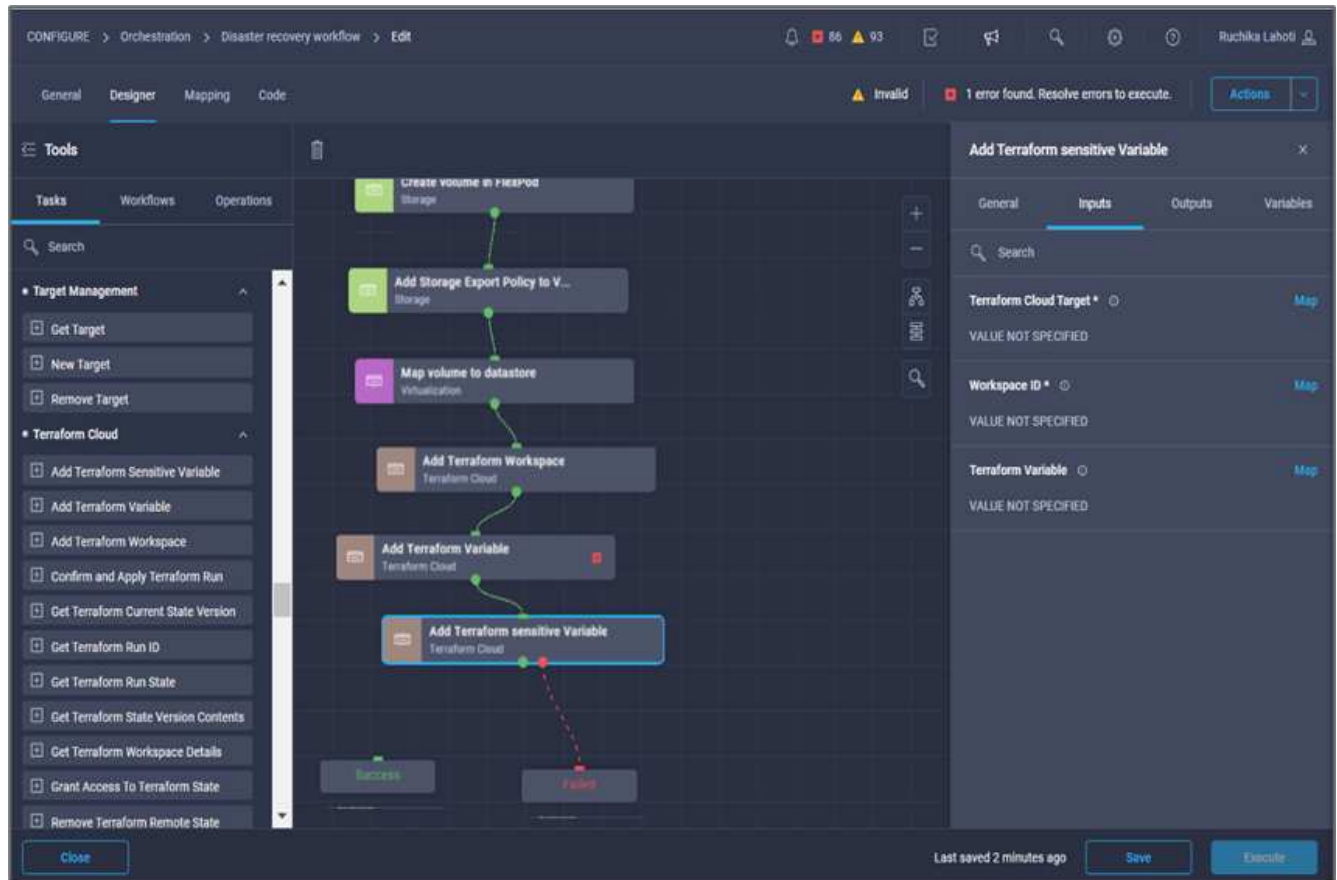
操作步骤 7：向工作空间添加敏感变量

1. 转到*设计器*选项卡、然后从*工具*部分中单击*工作流*。
2. 从*设计*区域的*工具*部分拖放* Terraform >添加Terraform变量*工作流。
3. 使用Connector连接两个*添加Terraform Workspace*任务。单击 * 保存 *。



此时将显示一条警告、指示这两个任务的名称相同。现在忽略此错误、因为您将在下一步中更改任务名称。

4. 单击*添加Terraform变量*。在*工作流属性*区域中、单击*常规*选项卡。将名称更改为*添加Terraform敏感变量*。



5. 在*工作流属性*区域中、单击*输入*。
6. 单击* Terraform Cloud Target*字段中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择在部分中添加的Terraform Cloud for Business帐户 "为HashiCorp Terraform配置Cisco Intersight Service"。 "
8. 单击*映射*。
9. 单击* Terraform Organization Name*字段中的*映射*。
10. 选择*静态值*、然后单击*选择Terraform Organization*。在Terraform Cloud for Business帐户中选择您所属的Terraform组织的名称。
11. 单击*映射*。
12. 单击* Terraform Workspace Name*字段中的*映射*。

13. 选择*直接映射*、然后单击*任务输出*。
14. 单击*任务名称*、然后单击*添加Terraform Workspace*。
15. 单击*输出名称*、然后单击输出*工作空间名称*。
16. 单击*映射*。
17. 单击*添加变量选项*字段中的*映射*。
18. 选择*直接映射*、然后单击*工作流输入*。
19. 单击*输入名称*和*创建工作流输入*。
20. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)。
 - b. 请务必为此类型选择* Terraform Add Variables Options*。
 - c. 单击*设置默认值*。
 - d. 单击*变量类型*、然后单击*敏感变量*。
 - e. 单击 * 添加 *。

Add Workflow Input

Display Name *
terraform sensitive variable ⓘ

Reference Name *
terraformensitivevariable ⓘ

Description
Add Variables ⓘ

Value Restrictions

☒ Required ⓘ

☐ Collection/Multiple ⓘ

Type
Terraform Add Variables Option ▾ ⓘ

☒ Set Default Value ⓘ

☐ Allow User Override ⓘ

Default Values *
terraform sensitive variable

Variable Type *
Sensitive Variables × ▾ ⓘ

Cancel Add

21. 在*添加Terraform变量*部分中、提供以下信息：

- 键。cloudmanager_refresh_token。
- *值。*输入NetApp Cloud Manager API操作的刷新令牌。
- *。问题描述。*刷新令牌。



有关为NetApp Cloud Manager API操作获取刷新令牌的详细信息、请参见一节 [“设置环境前提条件。”](#)

Add Workflow Input

☒ Set Default Value ⓘ

☐ Allow User Override ⓘ

Default Values *

terraform sensitive variable

Variable Type *

Sensitive Variables ⓘ

Add Sensitive Terraform Variables

Key *

cloudmanager_refresh_token ⓘ

Value ⓘ

ⓘ

Description ⓘ

cloudmanager refresh token ⓘ

☐ HCL ⓘ

+

Cancel

Add

22. 添加下表所示的所有Terraform敏感变量。您还可以提供默认值。

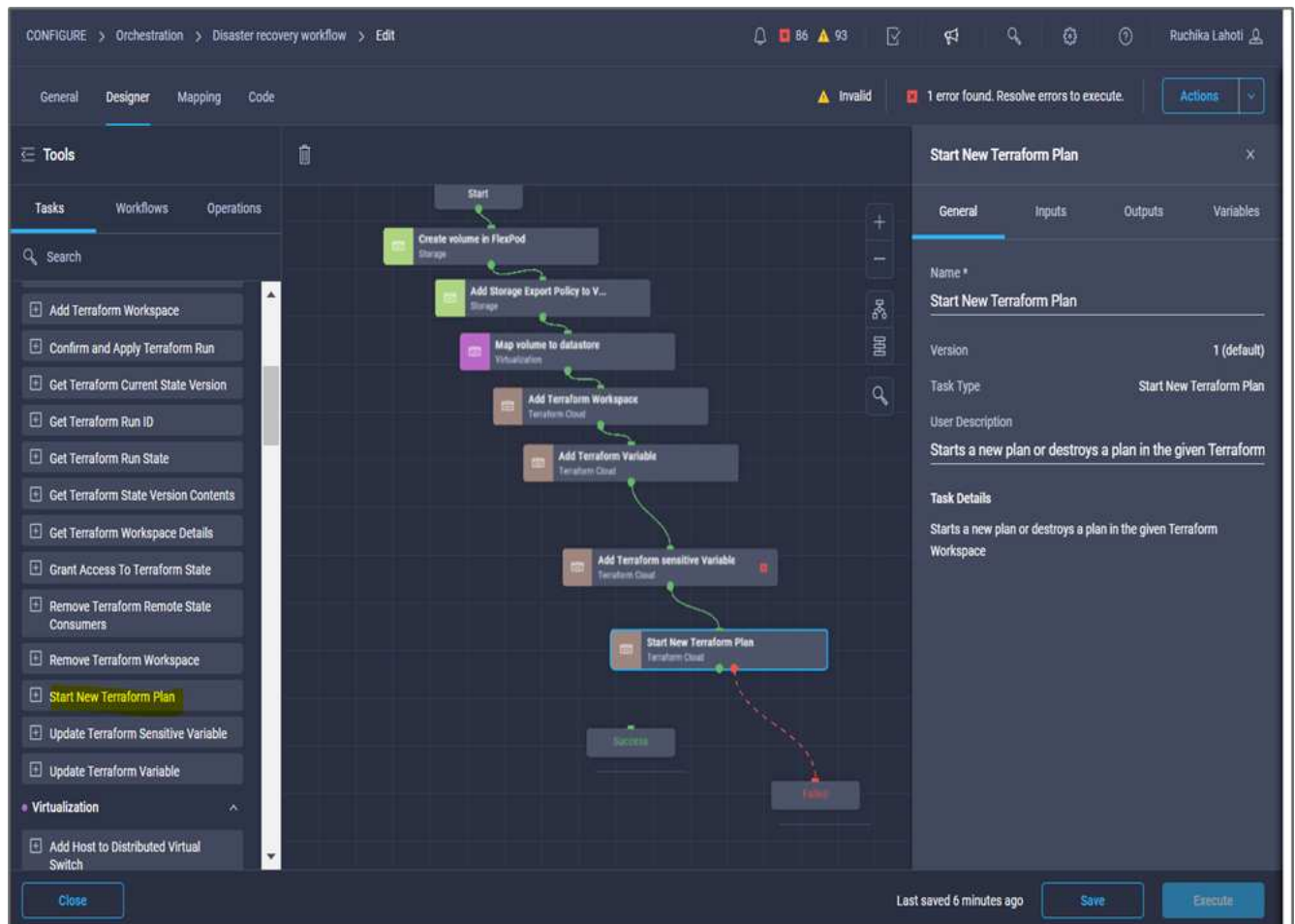
Terraform敏感变量名称	Description
cloudmanager_refresh_token	刷新令牌。请从以下位置获取：

Terraform敏感变量名称	Description
connector_id	Cloud Manager Connector的客户端ID。请从获取
CVO_admin_password	Cloud Volumes ONTAP 的管理员密码
on-prem-ontap_user_password	存储集群的管理员密码

- 单击*映射*。此操作将完成向工作空间添加所需的Terraform敏感变量的任务。接下来、在已配置的工作空间中启动新的Terraform计划。

操作步骤 8：启动新的Terraform计划

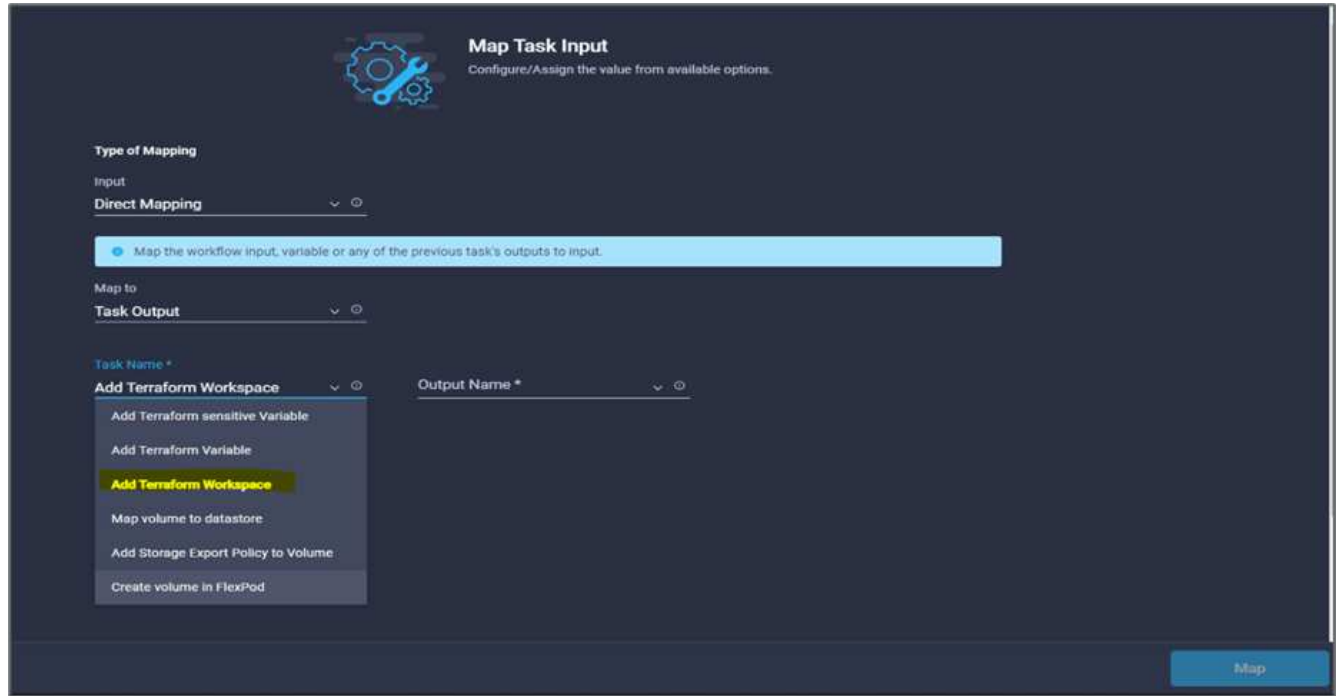
- 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
- 从*设计*区域的*工具*部分拖放* Terraform Cloud >启动新的Terraform Plan*任务。
- 使用Connector在任务*添加Terraform敏感变量*和*启动新的Terraform计划任务*之间建立连接。单击 * 保存 *。
- 单击*启动新的Terraform计划*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。



- 在*任务属性*区域中、单击*输入*。
- 单击* Terraform Cloud Target*字段中的*映射*。
- 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择在"为HashiCorp Terraform配置Cisco Intersight

Service "一节中添加的Terraform Cloud for Business帐户。

8. 单击*映射*。
9. 单击*工作空间ID*字段中的*映射*。
10. 选择*直接映射*、然后单击*任务输出*。
11. 单击*任务名称*、然后单击*添加Terraform Workspace*。



12. 单击*输出名称*、工作空间ID、然后单击*映射*。
13. 在*启动计划的原因*字段中单击*映射*。
14. 选择*直接映射*、然后单击*工作流输入*。
15. 单击*输入名称*、然后单击*创建工作流输入*。
16. 在添加输入向导中、完成以下步骤：
 - a. 提供显示名称和参考名称(可选)。
 - b. 确保为*类型*选择*字符串*。
 - c. 单击*设置默认值并覆盖*。
 - d. 输入*启动计划的原因*的默认值、然后单击*添加*。

Add Workflow Input

☒ Required ⓘ

☐ Collection/Multiple ⓘ

Type
String ▼ ⓘ

Min **0** ⓘ Max **0** ⓘ Regex ⓘ

☐ Secure ⓘ

☐ Object Selector ⓘ

☒ Set Default Value ⓘ

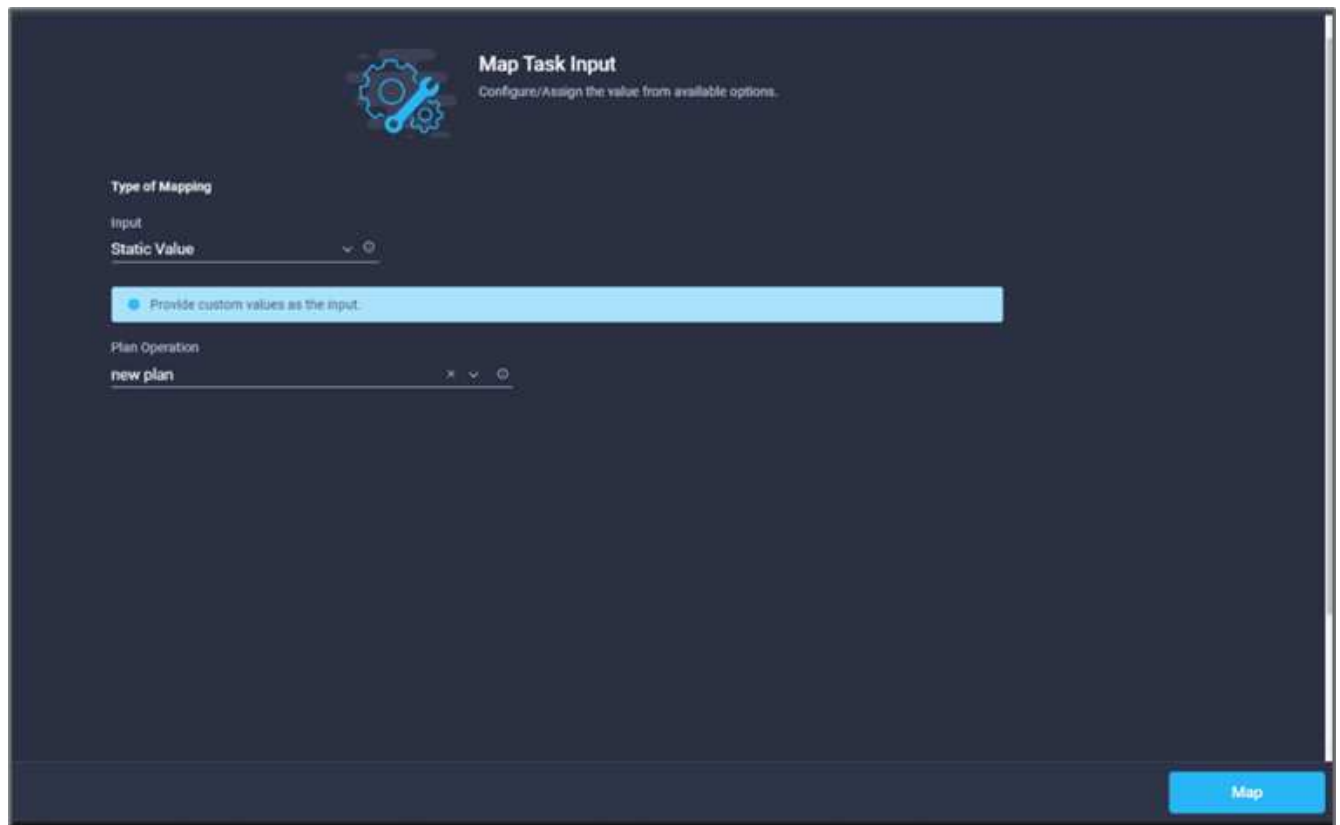
☒ Allow User Override ⓘ

Default Values *

Reason for starting plan *
terraform plan for replication between onprem volume and CVO ⓘ

Cancel Add

17. 单击*映射*。
18. 单击*计划操作*字段中的*映射*。
19. 选择*静态值*、然后单击*计划操作*。单击*新计划*。



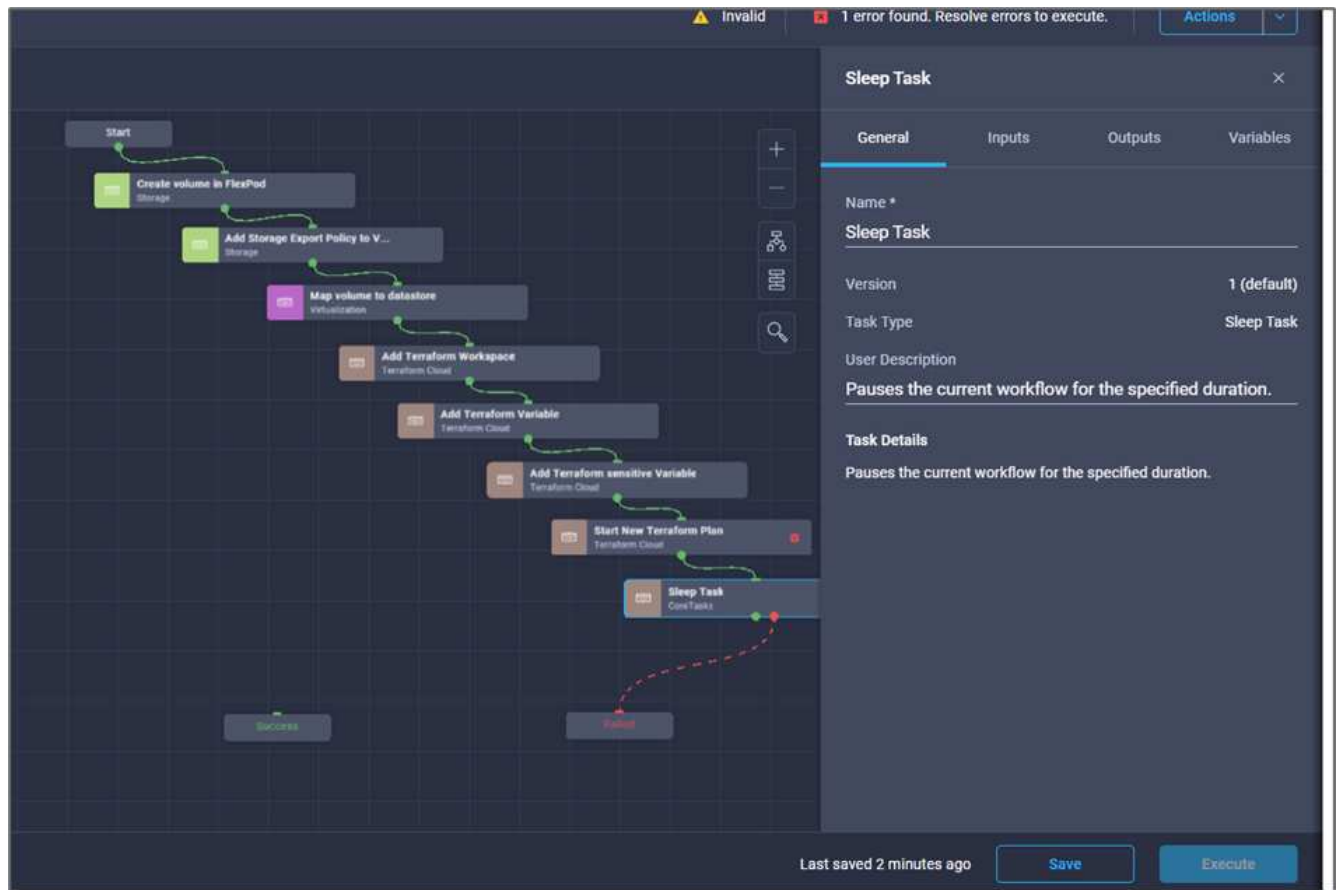
20. 单击*映射*。
21. 单击 * 保存 *。

此时、您将完成在Terraform Cloud for Business帐户中添加Terraform计划的任务。接下来、创建一个休眠任务几秒钟。

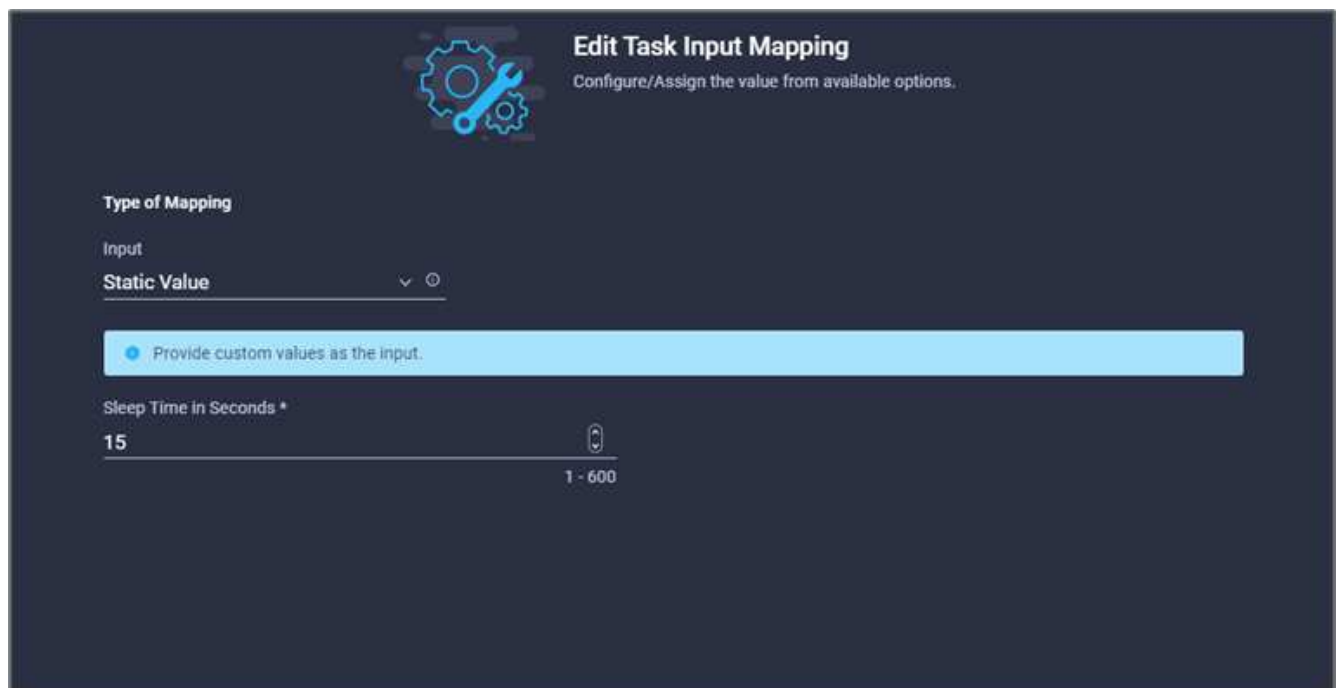
操作步骤 9：同步的休眠任务

Terraform Apply需要运行ID、而RunID是在Terraform Plan任务中生成的。在Terraform Plan和Terraform Apply操作之间等待几秒钟可避免时间问题。

1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放*核心任务>睡眠任务*。
3. 使用Connector连接任务*启动新的Terraform Plan*和*休眠任务*。单击 * 保存 *。



4. 单击*休眠任务*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是*同步*。
5. 在*任务属性*区域中、单击*输入*。
6. 单击*以秒为单位的睡眠时间*字段中的*映射*。
7. 选择*静态值*并输入*以15 表示*以秒为单位的睡眠时间。

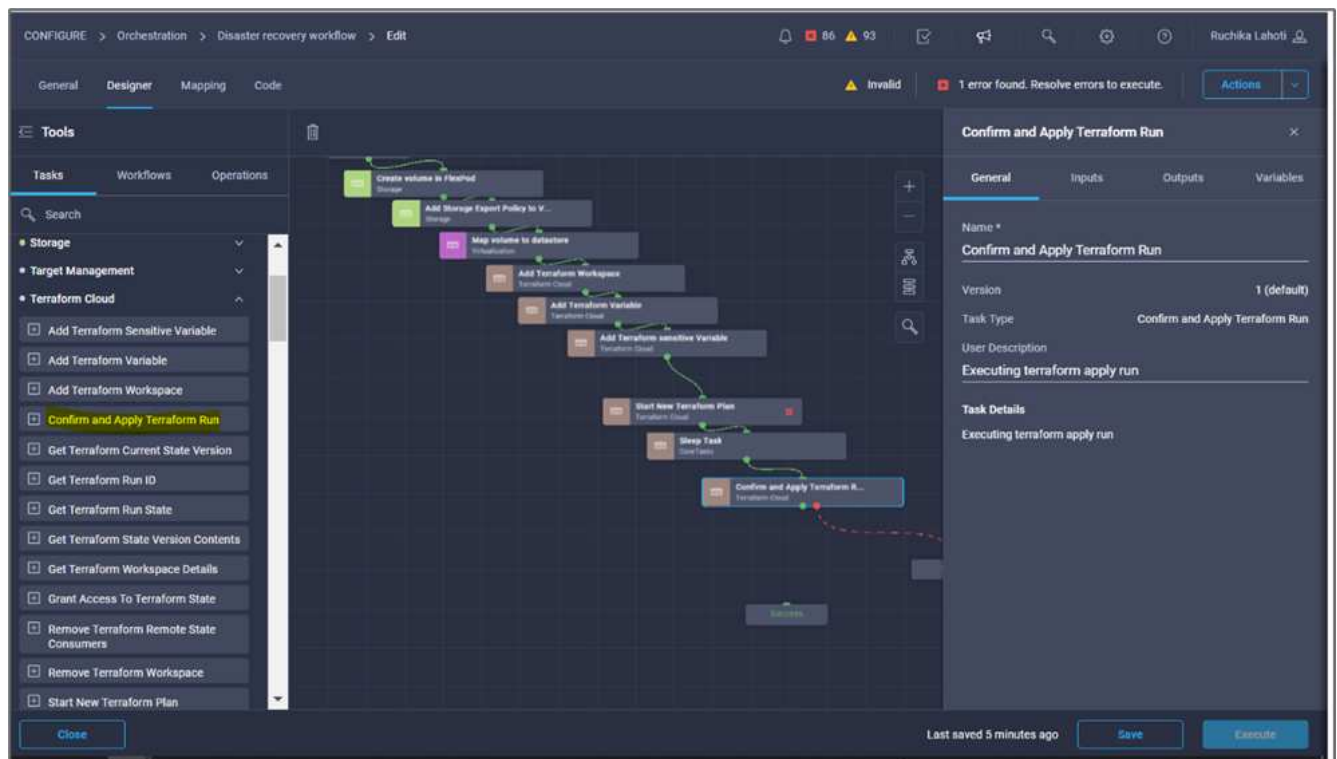


8. 单击*映射*。
9. 单击 * 保存 *。

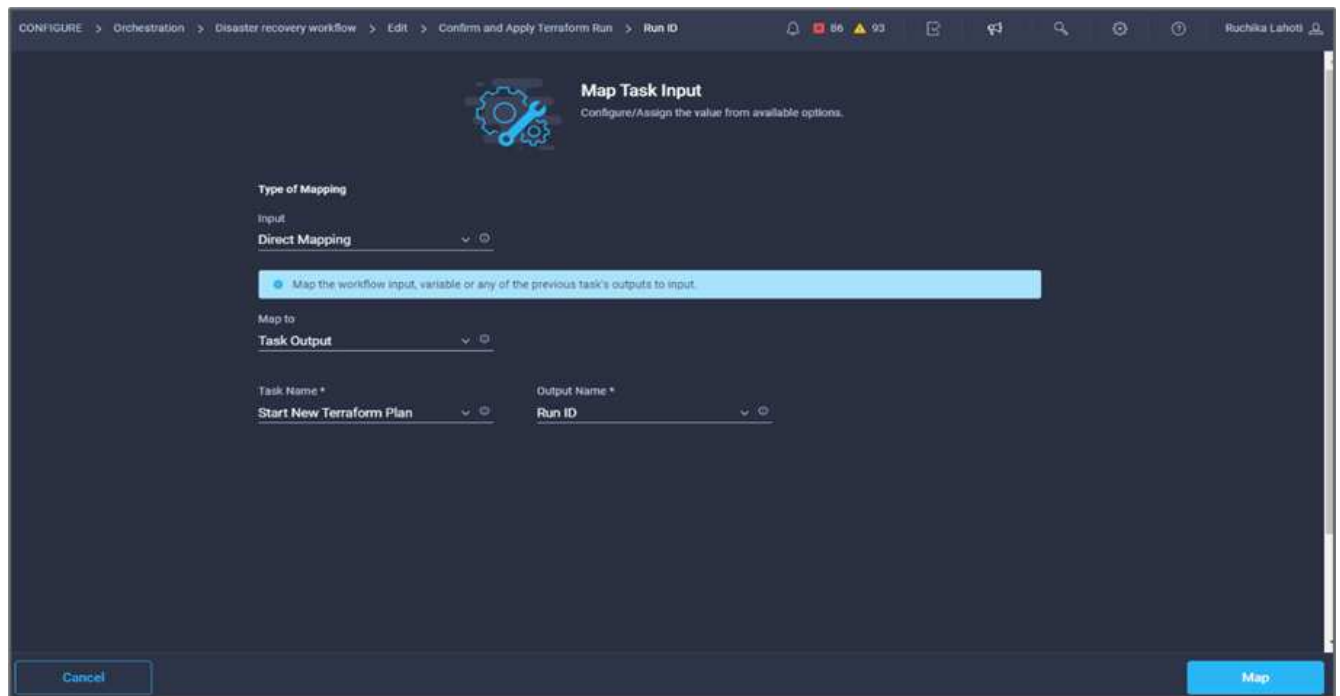
此操作将完成休眠任务。接下来、创建此工作流的最后一个任务、确认并应用Terraform Run。

操作步骤 10：确认并应用Terraform Run

1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放* Terraform Cloud >确认并应用Terraform Run*任务。
3. 使用连接器连接任务*同步*和*确认并应用Terraform Run*。单击 * 保存 *。
4. 单击*确认*和*应用Terraform Run*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。



5. 在*任务属性*区域中、单击*输入*。
6. 单击* Terraform Cloud Target*字段中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择添加在中的Terraform Cloud for Business帐户 "[为HashiCorp Terraform配置Cisco Intersight Service](#)"。 "
8. 单击*映射*。
9. 单击*运行ID*字段中的*映射*。
10. 选择*直接映射*、然后单击*任务输出*。
11. 单击*任务名称*、然后单击*开始新的Terraform计划*。
12. 单击*输出名称*、然后单击*运行ID*。



13. 单击*映射*。
14. 单击 * 保存 *。
15. 单击*自动对齐工作流*、以便对齐所有任务。单击 * 保存 *。



此时将完成确认并应用Terraform运行任务。使用Connector在*确认并应用Terraform Run*任务与*成功*和*失败*任务之间建立连接。

操作步骤 11：导入Cisco构建的工作流

通过Cisco Intersight Cloud Orchestrator、您可以将工作流从Cisco Intersight帐户导出到您的系统、然后将其导入到其他帐户。通过导出可导入到您帐户中的已构建工作流、创建了一个JSON文件。

中提供了工作流组件的JSON文件 "[GitHub 存储库](#)"。

"接下来：从控制器执行Terraform。"

从控制器执行Terraform

"上一步：灾难恢复工作流。"

我们可以使用控制器执行Terraform计划。如果您已经使用ICO工作流执行了Terraform计划、则可以跳过本节。

前提条件

解决方案 的设置首先从可访问Internet的管理工作站开始、然后再从可正常运行的Terraform安装开始。

有关安装Terraform的指南、请参见 ["此处"](#)。

克隆GitHub repo

此过程的第一步是将GitHub repoo克隆到管理工作站上的新空文件夹中。要克隆GitHub存储库、请完成以下步骤：

1. 在管理工作站上、为项目创建一个新文件夹。在此文件夹中创建一个名为`/root/snapmirror-CVO`的新文件夹、并将GitHub repo.
2. 在管理工作站上打开命令行或控制台界面、然后将目录更改为刚刚创建的新文件夹。
3. 使用以下命令克隆GitHub集合：

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. 将目录更改为名为`snapmirror-CVO`的新文件夹。

◦ Terraform执行*



- *初始化。*初始化(本地) Terraform环境。通常、每个会话仅执行一次。
- *计划。*将Terraform状态与云中的"正常运行"状态进行比较、然后构建并显示执行计划。这不会更改部署(只读)。
- *应用。*从计划阶段应用计划。这可能会更改部署(读取和写入)。
- *销毁。*受此特定Terraform环境管理的所有资源。

有关详细信息，请参见 ["此处"](#)。

"接下来：解决方案验证。"

解决方案验证

"先前：从控制器执行Terraform。"

在本节中、我们将通过一个示例数据复制工作流回顾解决方案、并采取一些衡量指标来验证从FlexPod 中运行的NetApp ONTAP 实例到Google Cloud上运行的NetApp Cloud Volumes ONTAP 的数据复制完整性。

我们在此解决方案 中使用了Cisco Intersight工作流编排程序、并将继续在我们的用例中使用此流程编排程序。

值得注意的是、此解决方案 中使用的一组有限的Cisco Intersight工作流并不代表Cisco Intersight所配备的一整套工作流。您可以根据特定要求创建自定义工作流、并通过Cisco Intersight触发这些工作流。

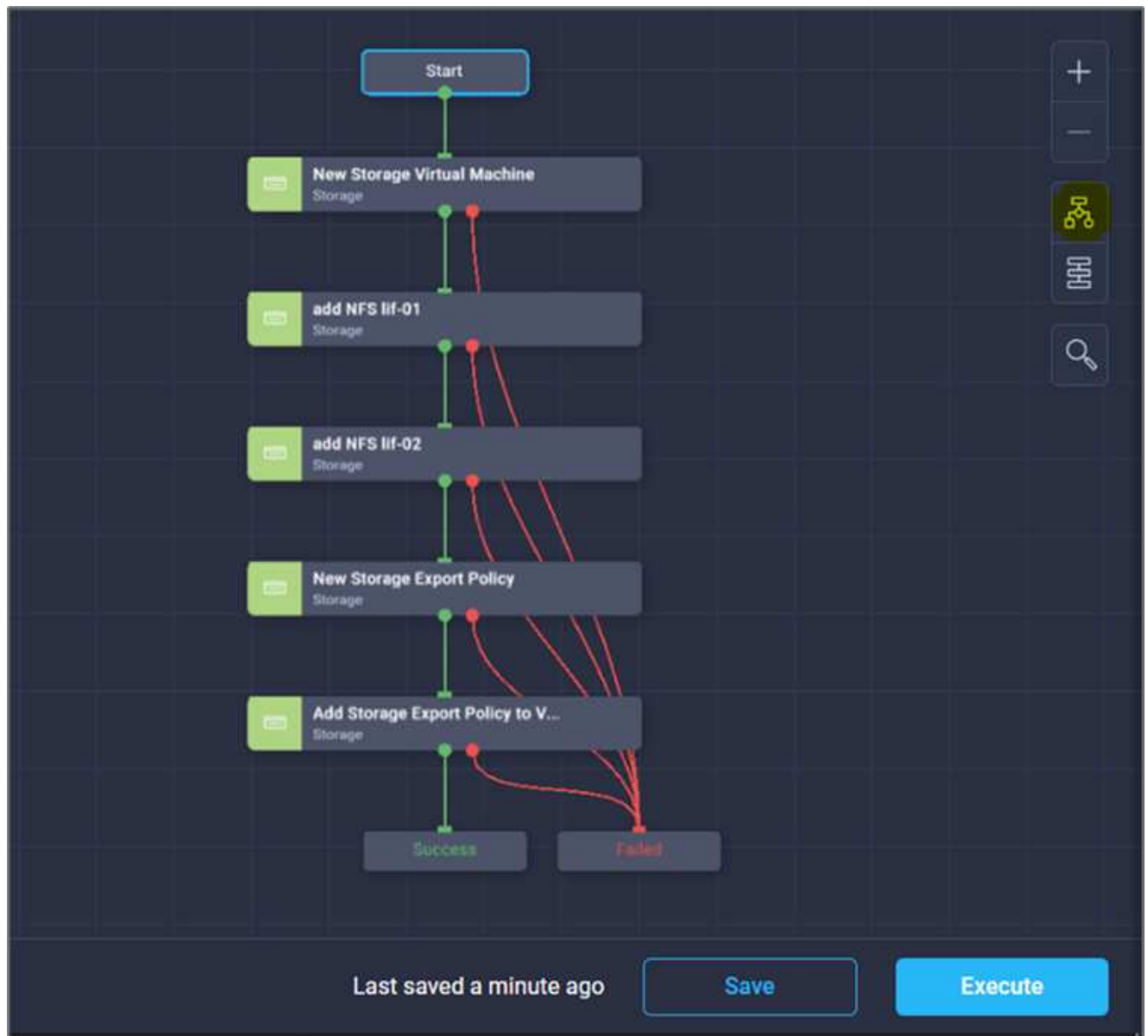
要验证成功的灾难恢复场景、请先使用SnapMirror将数据从ONTAP 中属于FlexPod 的卷移动到Cloud Volumes ONTAP。然后、您可以尝试从Google云计算实例访问数据、然后进行数据完整性检查。

以下高级步骤用于验证此解决方案 的成功标准：

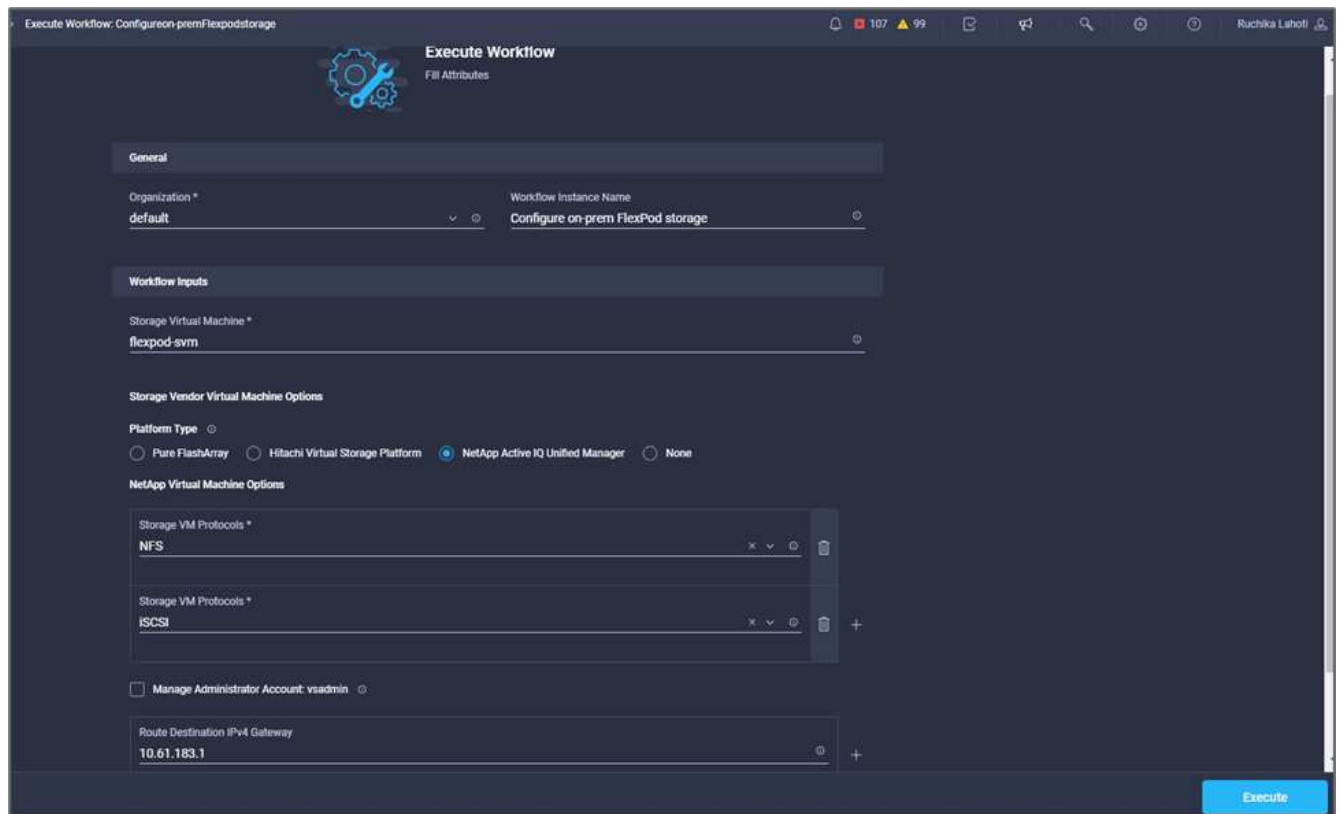
1. 对FlexPod 中ONTAP 卷中的示例数据集生成SHA256校验和。
2. 在FlexPod 中的ONTAP 和Cloud Volumes ONTAP 之间设置卷SnapMirror关系。
3. 将示例数据集从FlexPod 复制到Cloud Volumes ONTAP。
4. 中断SnapMirror关系并将Cloud Volumes ONTAP 中的卷提升为生产卷。
5. 将包含数据集的Cloud Volumes ONTAP 卷映射到Google Cloud中的计算实例。
6. 在Cloud Volumes ONTAP 中的示例数据集上生成SHA256校验和。
7. 比较源和目标上的校验和；可能是两端的校验和都匹配。

要执行内部工作流、请完成以下步骤：

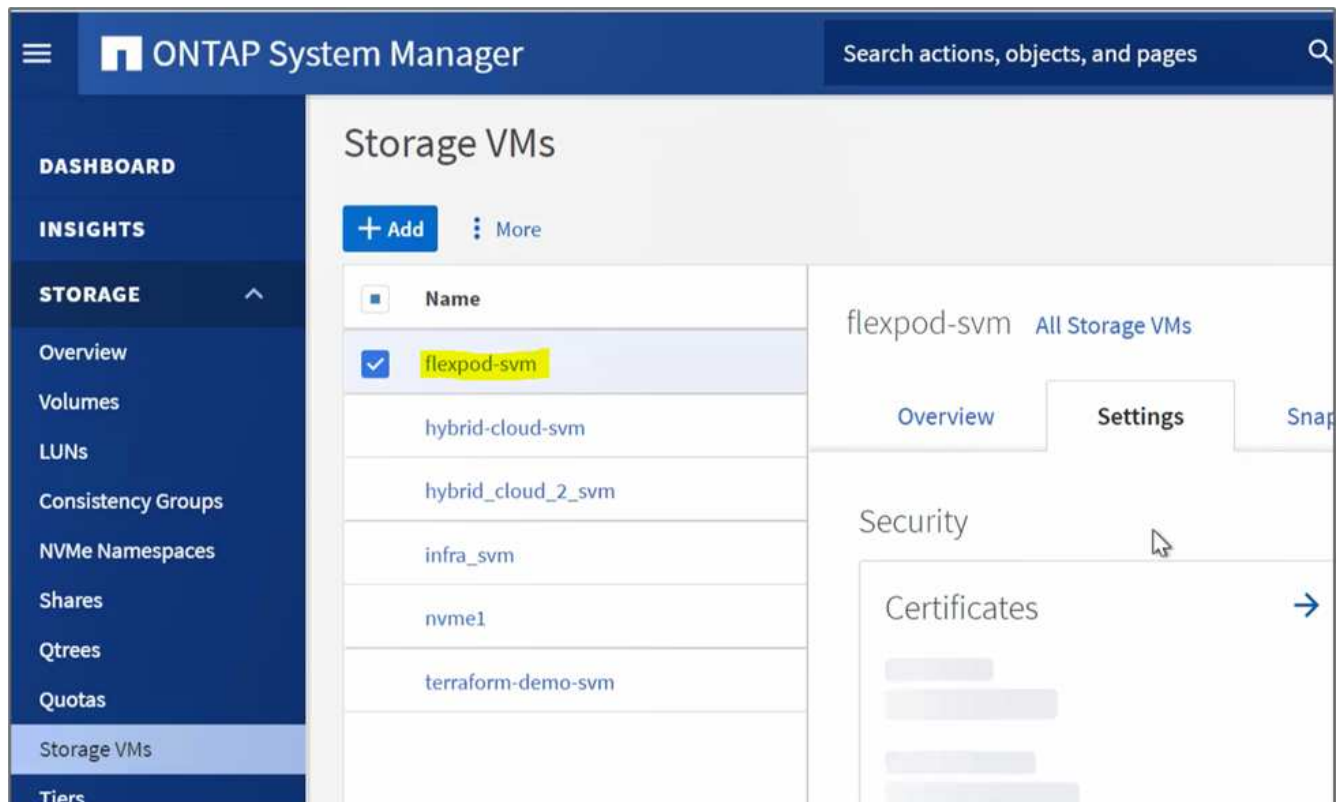
1. 在Intersight中为内部部署FlexPod 创建工作流。



2. 提供所需输入并执行工作流。



3. 在系统管理器中验证新创建的SVM。



4. 创建并执行另一个灾难恢复工作流、以便在内部FlexPod 中创建卷、并在FlexPod 和Cloud Volumes ONTAP 中的此卷之间建立SnapMirror关系。



5. 在ONTAP 系统管理器中验证新创建的卷。

ONTAP System Manager					Search actions, objects, and pages	
Volumes						
+ Add More						
	Name	Storage VM	Status	Capacity		
			(All)	>		
✓	application_copy	hybrid-cloud-svm	Online	3.12 MiB used 19 GiB available	20 GiB	
✓	audit_log_vol	hybrid-cloud-svm	Online	32.7 MiB used 200 GiB available	200 GiB	
✓	hybrid_cloud_svm_root	hybrid-cloud-svm	Online	1.68 MiB used 971 MiB available	1 GiB	
✓	test	hybrid-cloud-svm	Online	648 KiB used 972 MiB available	1 GiB	
✓	Test_Vol1	hybrid-cloud-svm	Online	10.6 MiB used 9.99 GiB available	10 GiB	

- 将同一个NFS卷挂载到内部虚拟机、然后复制样本数据集并执行校验和。

```

root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G   0% /dev
tmpfs           394M  1.1M  393M   1% /run
/dev/sda2       16G   11G   4.2G  72% /
tmpfs           2.0G   0    2.0G   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           2.0G   0    2.0G   0% /sys/fs/cgroup
/dev/loop1      55M   55M   0 100% /snap/core18/1705
/dev/loop2      69M   69M   0 100% /snap/lxd/14804
/dev/loop0      28M   28M   0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1 10G 512K 10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#

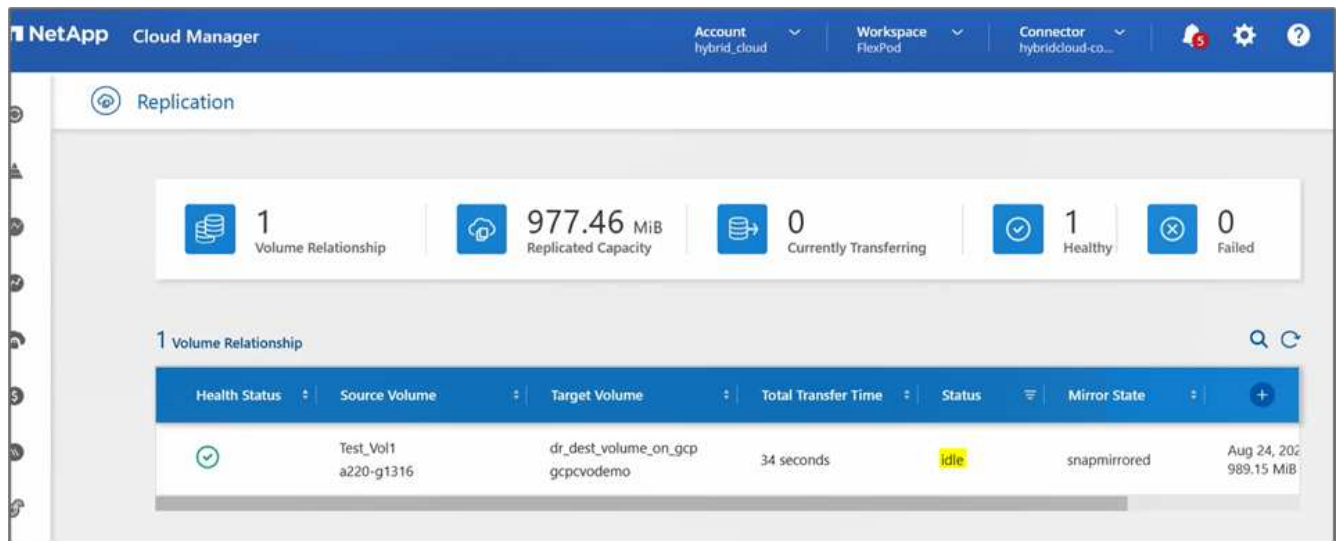
```

```

root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59 test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#

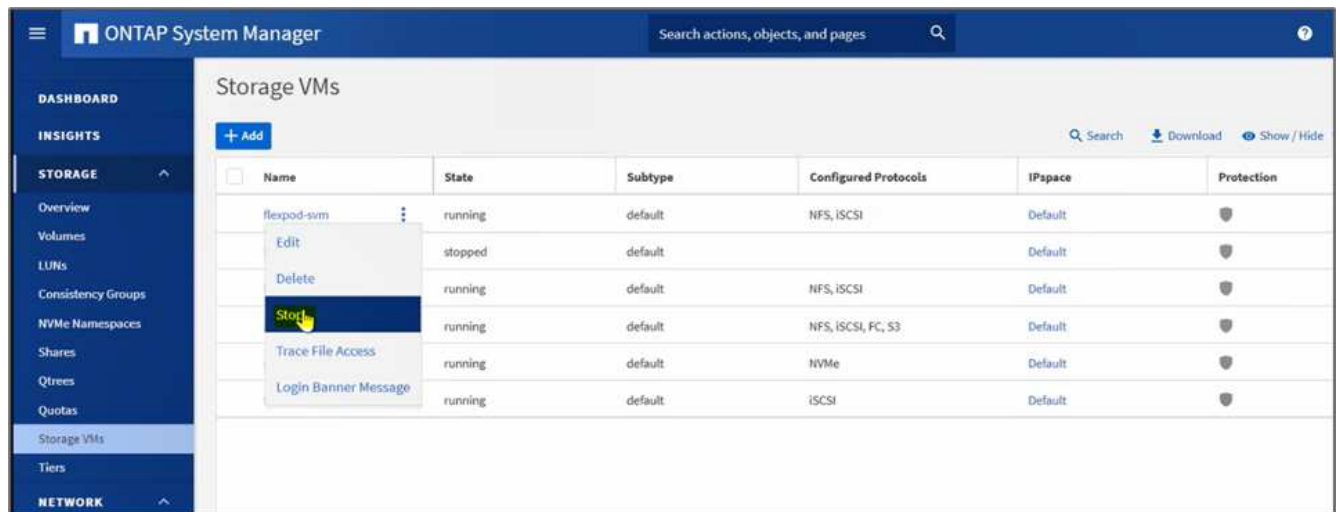
```

- 在Cloud Manager中检查复制状态。根据数据大小、数据传输可能需要几分钟的时间。完成后、您可以将SnapMirror状态显示为*闲置*。

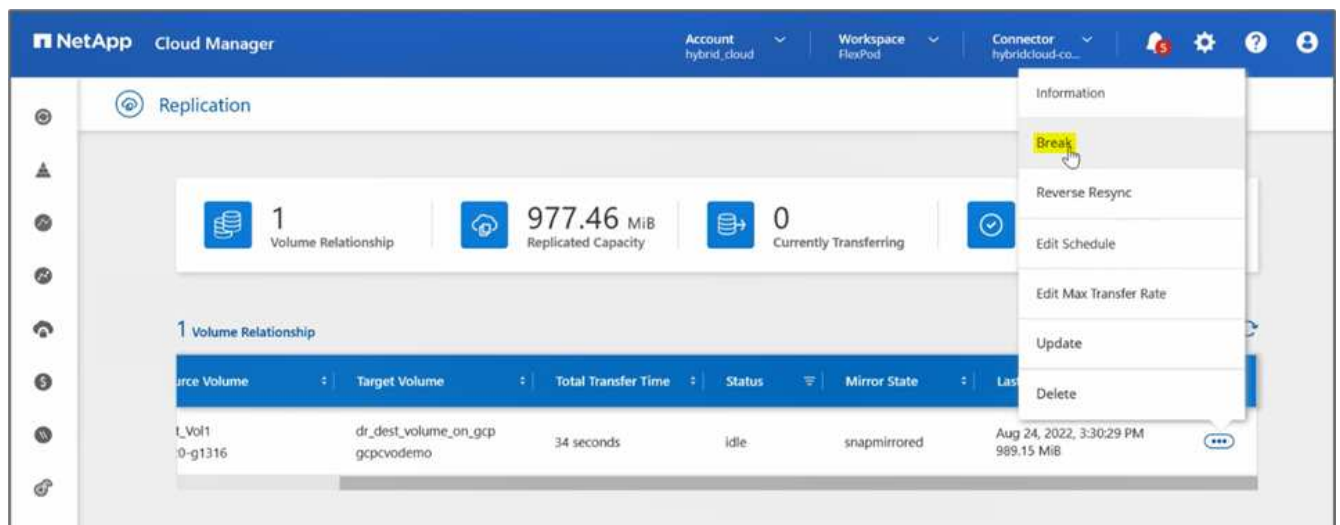


8. 数据传输完成后、通过停止托管`Test\_vol1`卷的SVM来模拟源端的灾难。

停止SVM后、在Cloud Manager中看不到`Test\_vol1`卷。



9. 中断复制关系并将Cloud Volumes ONTAP 目标卷提升为生产卷。



Mount Volume dr_dest_volume_on_gcp

Go to your Linux machine and enter this mount command

```
mount 172.30.116.153:/dr_dest_volume_on_gcp <dest...
```



12. 将卷挂载到计算实例、验证目标卷中是否存在数据、然后生成`sample\_data\_2GB`文件的SHA256校验和。

```
drwxr-xr-x 21 root    root          4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. 比较源(FlexPod)和目标(Cloud Volumes ONTAP)的校验和值。

14. 校验和与源和目标匹配。

您可以确认已成功完成从源到目标的数据复制、并保持数据完整性。现在、在源站点完成还原期间、应用程序可以安全地使用这些数据为客户端提供服务。

"接下来：总结。"

结论

"先前版本：解决方案 验证。"

在此解决方案 中、我们使用了NetApp云数据服务、Cloud Volumes ONTAP 和FlexPod 数据中心基础架构、使用由Cisco Intersight Cloud Orchestrator提供支持的公有 云构建灾难恢复解决方案。FlexPod 解决方案 不断发展、可帮助客户实现应用程序和业务交付流程的现代化。借助此解决方案、您可以使用公有 云作为瞬时或全时灾难恢复计划的首选位置来构建BCDr计划、同时保持较低的灾难恢复解决方案 成本。

内部FlexPod 和NetApp Cloud Volumes ONTAP 之间的数据复制由成熟的SnapMirror技术处理、但您也可以选择其他NetApp数据传输和同步工具、如Cloud Sync 、以满足您的数据移动性需求。基于TLS/AES的内置加密技术可确保传输中数据的安全性。

无论您是应用程序制定临时灾难恢复计划、还是为企业制定全职灾难恢复计划、此解决方案 中使用的产品组合都可以大规模满足这两项要求。在Cisco Intersight Workflow Orchestrator的支持下、可以通过预构建的工作流自动执行此操作、不仅无需重新构建流程、还可以加快BCDr计划的实施速度。

借助Cisco Intersight Cloud Orchestrator提供的自动化和流程编排功能、解决方案 可以轻松方便地管理FlexPod

内部部署和混合云中的数据复制。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

GitHub

- 使用的所有Terraform配置

["https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"](https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO)

- 用于导入工作流的JSON文件

["https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"](https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows)

Cisco Intersight

- Cisco Intersight帮助中心

["https://intersight.com/help/saas/home"](https://intersight.com/help/saas/home)

- Cisco Intersight Cloud Orchestrator文档：

["https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"](https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator)

- Cisco Intersight Service for HashiCorp Terraform文档

["https://intersight.com/help/saas/features/terraform_cloud/admin"](https://intersight.com/help/saas/features/terraform_cloud/admin)

- Cisco Intersight数据表

["https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html)

- Cisco Intersight Cloud Orchestrator数据表

["https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html)

- 适用于HashiCorp Terraform的Cisco Intersight Service数据表

["https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html)

FlexPod

- FlexPod 主页

["https://www.flexpod.com"](https://www.flexpod.com)

- 适用于 FlexPod 的 Cisco 验证设计和部署指南

"采用 UCS 托管模式的 FlexPod Datacenter 4.2 （ 1 ） ， VMware vSphere 7.0 U2 和 NetApp ONTAP 9.9 设计指南"

- 采用Cisco UCS X系列的FlexPod 数据中心

"https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

互操作性

- NetApp 互操作性表工具

"<http://support.netapp.com/matrix/>"

- Cisco UCS 硬件和软件互操作性工具

"<http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>"

- VMware 兼容性指南

"<http://www.vmware.com/resources/compatibility/search.php>"

NetApp Cloud Volumes ONTAP 参考文档

- NetApp Cloud Manager

"https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

<https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html>

- Cloud Volumes ONTAP TCO计算器

<https://cloud.netapp.com/google-cloud-calculator>

- Cloud Volumes ONTAP 规模估算工具

"<https://cloud.netapp.com/cvo-sizer>"

- 云评估工具

<https://cloud.netapp.com/assessments>

- NetApp混合云

<https://cloud.netapp.com/hybrid-cloud>

- Cloud Manager API 文档

"https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

对问题进行故障排除

["https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_\(CVO\)"](https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO))

Terraform

- Terraform Cloud

["https://www.terraform.io/cloud"](https://www.terraform.io/cloud)

- Terraform文档

["https://www.terraform.io/docs/"](https://www.terraform.io/docs/)

- NetApp Cloud Manager注册表

["https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/latest"](https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/latest)

GCP

- 适用于GCP的ONTAP 高可用性

["https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"](https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick)

- GCP的基础

<https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6>

采用NetApp Astra和适用于Red Hat OpenShift的Cisco Intersight的FlexPod 混合云

TR-4936: 采用NetApp Astra和适用于Red Hat OpenShift的Cisco Intersight的FlexPod 混合云

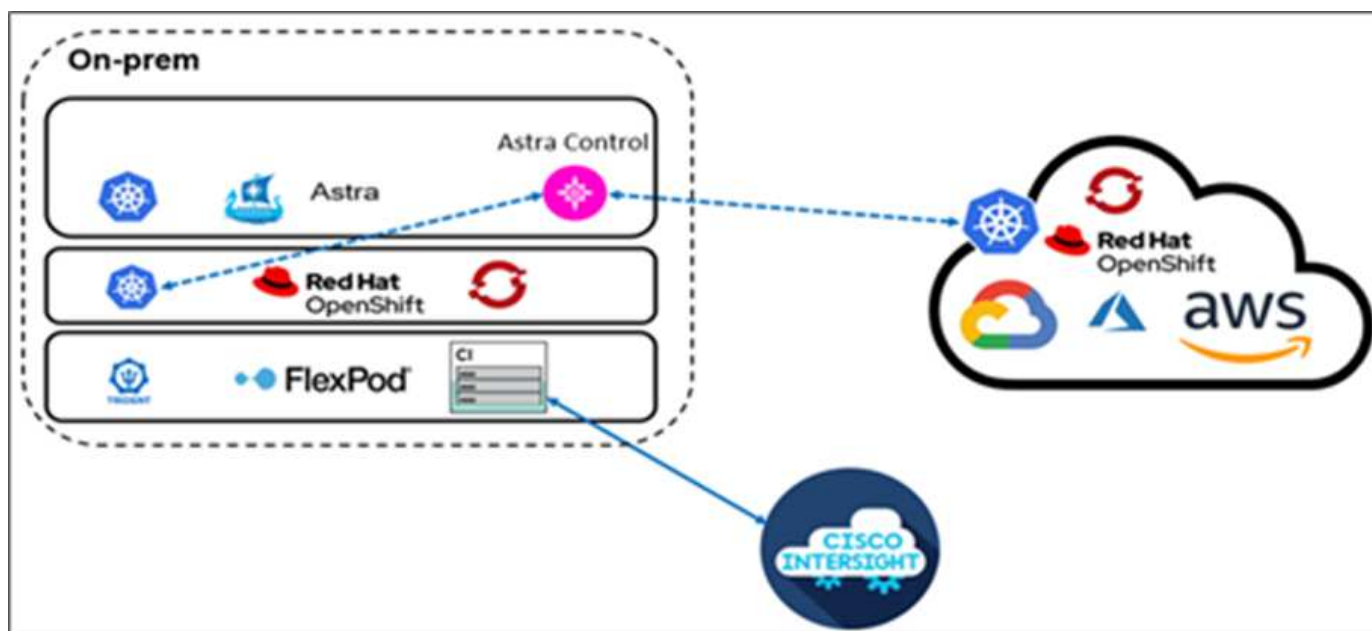
Abhinav Singh

简介

随着容器和Kubernetes成为开发、部署、运行、管理和扩展容器化应用程序的实际选择、企业越来越多地在这些应用程序上运行业务关键型应用程序。业务关键型应用程序在很大程度上依赖于状态。有状态应用程序具有关联的状态、数据和配置信息、并依靠先前的数据事务来执行其业务逻辑。在Kubernetes上运行的业务关键型应用程序仍然像传统应用程序一样具有可用性和业务连续性要求。服务中断可能会严重影响公司的收入、工作效率和声誉损失。因此、在集群、内部数据中心和混合云环境内部和之间快速轻松地保护、恢复和移动Kubernetes工作负载至关重要。企业已经认识到将业务转变为混合云模式的优势、将应用程序现代化到云原生外形规格的优势也在他们的市场中居高不下。

本技术报告将NetApp Astra控制中心与基于FlexPod 融合基础架构解决方案 的Red Hat OpenShift容器平台结合在一起、并扩展到Amazon Web Services (AWS)以构成混合云数据中心。以熟悉为基础 ["FlexPod 和Red Hat OpenShift"](#)本文档介绍了NetApp Astra控制中心、从安装、配置、应用程序保护工作流以及内部和云之间的应用程序迁移开始。同时、还讨论了在将NetApp Astra控制中心用于在Red Hat OpenShift上运行的容器化应用程序时、应用程序感知型数据管理功能(例如备份和恢复、业务连续性)的优势。

下图显示了解决方案 概述。



audience

本文档的目标受众包括首席技术官(CTO)、应用程序开发人员、Cloud解决方案 架构师、站点可靠性工程师(SRE)、开发运营工程师、ITOps以及专注于设计、托管和管理容器化应用程序的专业服务团队。

NetApp Astra Control—主要用例

NetApp Astra Control旨在为使用Cloud原生 微服务的客户简化应用程序保护：

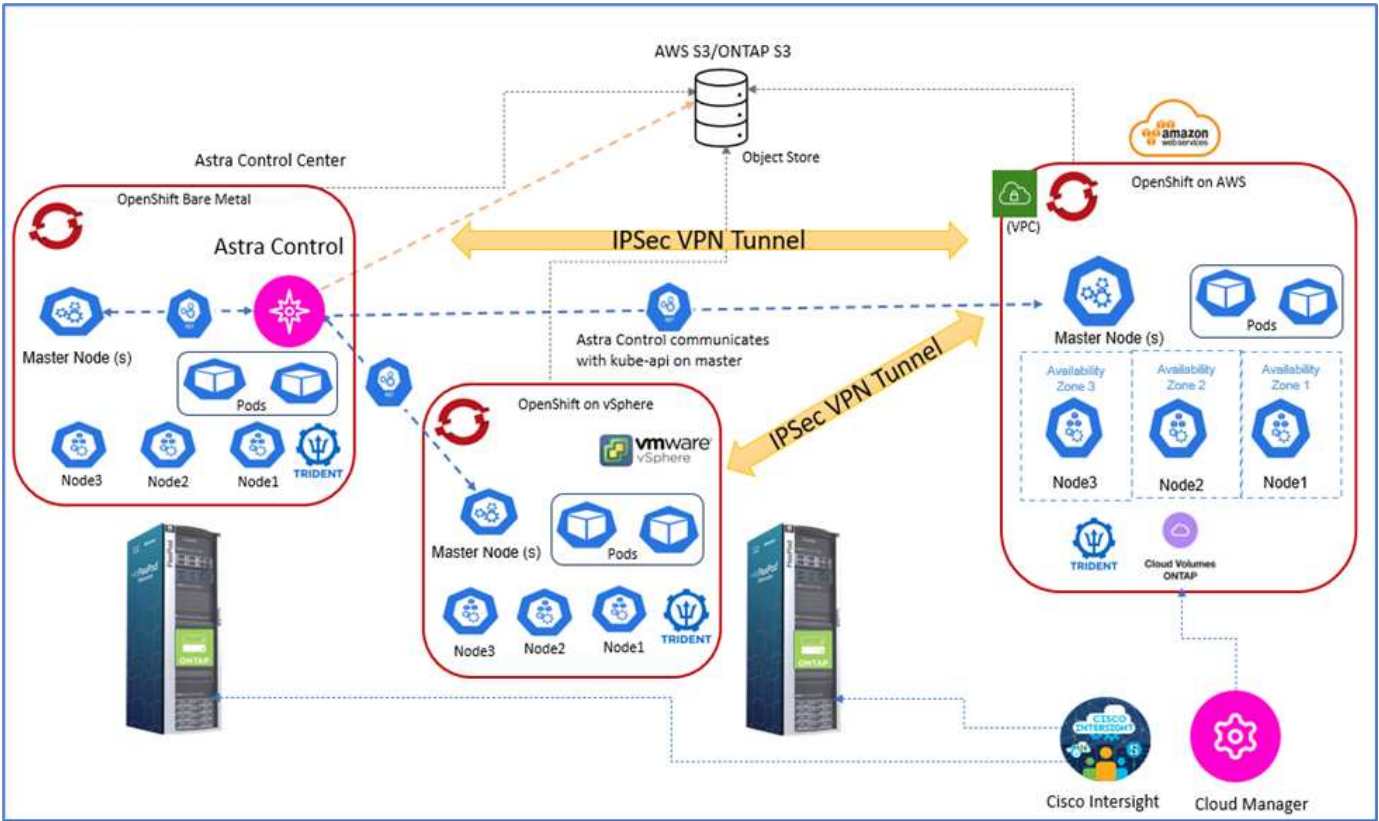
- *使用快照的时间点(PIT)应用程序表示。*借助Astra Control、您可以为容器化应用程序创建端到端快照、其中包括Kubernetes上运行的应用程序的配置详细信息以及相关的永久性存储。发生意外事件时、可以单击按钮将应用程序还原到已知正常状态。
- *完整副本应用程序备份。*借助Astra Control、您可以按预定义的计划执行完整的应用程序备份、该计划可用于自动将应用程序还原到同一K8s集群或另一个K8s集群。
- *应用程序可移植性和克隆迁移。*借助Astra Control、您可以将整个应用程序及其数据从一个Kubernetes集群克隆到另一个集群或同一个K8s集群中。无论集群位于何处、此功能还有助于在K8s集群之间移植或迁移应用程序(只需在克隆后删除源应用程序实例即可)。
- *自定义应用程序一致性。*借助Astra Control、您可以利用执行挂钩来控制应用程序暂停状态的定义。将'pre'和'post '执行挂钩置于快照和备份工作流中、在创建快照或备份之前、您的应用程序将以您自己的方式暂停。
- *自动执行应用程序级灾难恢复(DR)。*借助Astra Control、您可以为容器化应用程序配置业务连续性灾难恢复(Business Continuity Disaster Recovery、BCDR)计划。后端使用NetApp SnapMirror、并自动完成灾难恢复工作流的实施。

解决方案 拓扑

本节介绍解决方案 的逻辑拓扑。

下图显示了解决方案 拓扑结构、其中包括运行OpenShift容器平台集群的FlexPod 内部环境以及采用NetApp Cloud Volumes ONTAP 、Cisco Intersight和NetApp Cloud Manager SaaS平台的AWS上的自管理OpenShift容

器平台集群。



第一个OpenShift容器平台集群是在FlexPod 上安装的裸机集群、第二个OpenShift容器平台集群部署在FlexPod 上运行的VMware vSphere上、第三个OpenShift容器平台集群部署为 "专用集群" 作为一个自助管理基础架构、迁移到AWS上的现有虚拟私有云(VPC)中。

在此解决方案 中、FlexPod 通过站点到站点VPN连接到AWS、但是、客户也可以使用直接连接实施扩展到混合云。Cisco Intersight用于管理FlexPod 基础架构组件。

在此解决方案 中、Astra控制中心负责管理在FlexPod 和AWS上运行的OpenShift容器平台集群上托管的容器化应用程序。Astra控制中心安装在FlexPod 上运行的OpenShift裸机实例上。Astra Control与主节点上的Kube-API进行通信、并持续监控Kubernetes集群是否发生更改。添加到K8s集群中的任何新应用程序都会自动发现并提供管理。

容器化应用程序的PIT表示可以使用Astra控制中心捕获为快照。可以通过计划的保护策略或按需触发应用程序快照。对于Astra支持的应用程序、快照的崩溃状态是一致的。应用程序快照构成永久性卷中应用程序数据的快照、以及与该应用程序关联的各种Kubernetes资源的应用程序元数据。

可以使用使用预定义的备份计划或按需使用Astra Control创建应用程序的完整副本备份。对象存储用于存储应用程序数据的备份。NetApp ONTAP S3、NetApp StorageGRID 以及任何通用S3实施均可用作对象存储。

"接下来：解决方案 组件。"

解决方案组件

"上一步：解决方案概述。"

FlexPod

FlexPod 是一组定义的硬件和软件，可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 包括NetApp ONTAP 存储、Cisco Nexus网络、Cisco MDS存储网络、Cisco统一计算系统(Cisco UCS)。该设计非常灵活、可以将网络、计算和存储安装到一个数据中心机架中、也可以根据客户的数据中心设计进行部署。端口密度允许网络组件容纳多种配置。

Astra Control

Astra Control为公有 云和内部环境中托管的云原生应用程序提供应用程序感知型数据保护服务。Astra Control可在Kubernetes上运行的容器化应用程序提供数据保护、灾难恢复和迁移功能。

功能

Astra Control 为 Kubernetes 应用程序数据生命周期管理提供了关键功能：

- 自动管理永久性存储
- 创建应用程序一致的按需快照和备份
- 自动执行策略驱动的快照和备份操作
- 在混合云环境中将应用程序和关联数据从一个Kubernetes集群迁移到另一个集群
- 将应用程序克隆到同一个K8s集群或另一个K8s集群
- 直观显示应用程序保护状态
- 提供图形用户界面和完整的REST API列表、用于利用现有内部工具实施所有保护工作流。

Astra Control为容器化应用程序提供了一个单一的管理平台可视化视图、其中包括对在Kubernetes集群上创建的相关资源的深入了解。您可以使用一个门户查看所有云或所有数据中心中的所有集群、所有应用程序。您可以在所有环境(内部或公有 云)中使用Astra Control API来实施数据管理工作流。

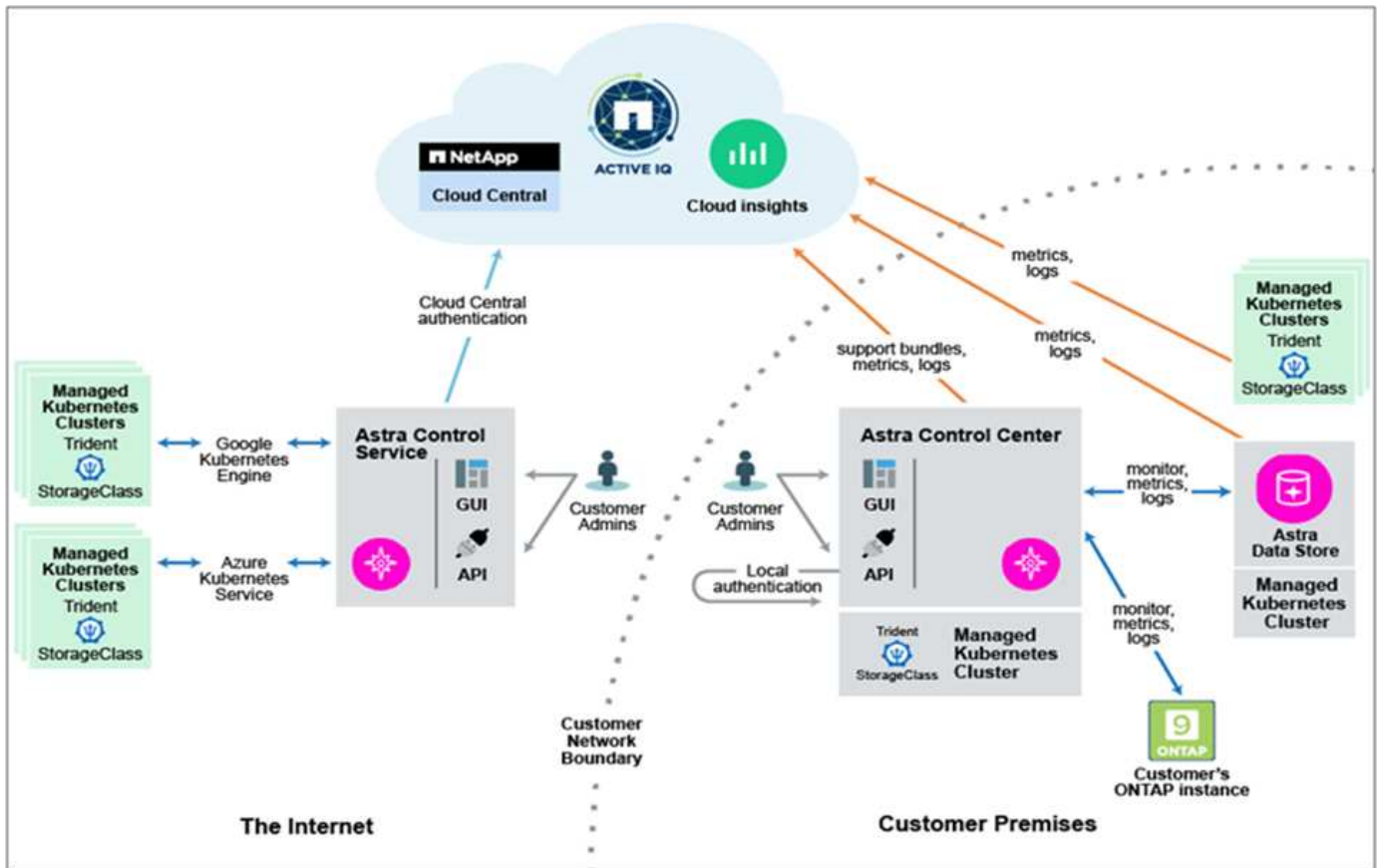
Astra Control消费模式

Astra Control有两种消费模式：

- * Astra Control Service。* NetApp托管的一项完全托管服务、可在Google Kubernetes Engine (GKEE) Azure Kubernetes Service (AKS)中为Kubernetes集群提供应用程序感知型数据管理。
- * Astra Control Center。*自管理软件、可为内部和混合云环境中运行的Kubernetes集群提供应用程序感知型数据管理。

本技术报告利用Astra控制中心管理Kubernetes上运行的云原生应用程序。

下图显示了Astra Control架构。



Astra Trident

Astra Trident是一款完全受支持的开源存储编排程序、适用于容器和Kubernetes分发版。它从一开始就经过精心设计、可帮助您使用行业标准界面(如)满足容器化应用程序的持久性需求 **"容器存储接口(CSI)"**。借助Astra Trident、微服务和容器化应用程序可以利用NetApp存储系统产品组合提供的企业级存储服务。

Astra Trident以 pod 的形式部署在 Kubernetes 集群上，为您的 Kubernetes 工作负载提供动态存储编排服务。它使您的容器化应用程序能够快速轻松地使用 NetApp 广泛的产品组合中的持久存储，其中包括NetApp ONTAP（NetApp AFF、NetApp FAS、NetApp ONTAP Select、Cloud 和Amazon FSx for NetApp ONTAP）、NetApp Element软件（NetApp SolidFire）以及Azure NetApp Files服务。在FlexPod环境中，Astra Trident用于动态配置和管理由托管在ONTAP存储平台（例如NetApp AFF和FAS系统以及Cloud Volumes ONTAP）上的NetApp FlexVol卷和 LUN 支持的容器的持久卷。Trident在Astra Control 提供的应用保护方案的实施中也发挥着关键作用。有关Astra Trident的更多信息，请参阅 ["Astra Trident文档"](#)。

存储后端

要使用Astra Trident、您需要受支持的存储后端。Trident后端定义了Trident与存储系统之间的关系。它会告诉Trident如何与该存储系统通信、以及Trident如何从该存储系统配置卷。Trident将自动从后端提供符合存储类定义的要求的存储池。

- ONTAP AFF 和 FAS 存储后端。作为存储软件和硬件平台、ONTAP 可提供核心存储服务、支持多个存储访问协议以及存储管理功能、例如NetApp Snapshot副本和镜像。
- Cloud Volumes ONTAP 存储后端
- ["Astra 数据存储"](#) 存储后端

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP 是一款软件定义的存储产品、可为文件和块工作负载提供高级数据管理。借助Cloud Volumes ONTAP、您可以优化云存储成本并提高应用程序性能、同时增强数据保护、安全性和合规性。

主要优势包括：

- 利用内置的重复数据删除，数据压缩，精简配置和克隆功能最大限度地降低存储成本。
- 在云环境发生故障时，确保企业级可靠性和持续运行。
- Cloud Volumes ONTAP 利用NetApp行业领先的复制技术SnapMirror将内部数据复制到云中、因此可以轻松地为多种使用情形提供二级副本。
- Cloud Volumes ONTAP 还与 Cloud Backup Service 集成，提供备份和还原功能，以保护云数据并对其进行长期归档。
- 按需在高性能和低性能存储池之间切换，而无需使应用程序脱机。
- 使用NetApp SnapCenter 确保Snapshot副本的一致性。
- Cloud Volumes ONTAP 支持数据加密，并提供防病毒和勒索软件保护。
- 与 Cloud Data sense 集成有助于您了解数据环境并识别敏感数据。

Cloud Central

Cloud Central提供了一个中央位置、用于访问和管理NetApp云数据服务。通过这些服务、您可以在云中运行关键应用程序、创建自动化灾难恢复站点、备份数据以及跨多个云有效迁移和控制数据。有关详细信息，请参见 ["Cloud Central。"](#)

Cloud Manager

Cloud Manager是一款基于SaaS的企业级管理平台、IT专家和云架构师可以利用NetApp的云解决方案集中管理其混合多云基础架构。它提供了一个集中式系统、用于查看和管理内部和云存储、支持混合、多个云提供商和客户。有关详细信息，请参见 ["Cloud Manager"](#)。

连接器

Connector是一个实例、可使Cloud Manager管理公有云环境中的资源和流程。要使用Cloud Manager提供的许多功能、需要使用Connector。连接器可以部署在云或内部网络中。

连接器在以下位置受支持：

- AWS
- Microsoft Azure
- Google Cloud
- 在您的内部环境中

要了解有关Connector的更多信息、请参见 ["此链接。"](#)

NetApp Cloud Insights

Cloud Insights 是一款NetApp云基础架构监控工具、可用于监控由Astra控制中心管理的Kubernetes集群的性能

和利用率。Cloud Insights 将存储使用量与工作负载相关联。在 Astra 控制中心中启用 Cloud Insights 连接后，遥测信息将显示在 Astra 控制中心 UI 页面中。

NetApp Active IQ Unified Manager

借助NetApp Active IQ Unified Manager、您可以通过一个经过重新设计的直观界面监控ONTAP 存储集群、该界面可通过社区智慧和AI分析提供智能。它可以全面洞察存储环境及其运行的虚拟机(VM)的运行状况、性能和主动式能力。当存储基础架构发生问题描述 时、Unified Manager可以通知您问题描述 的详细信息、以帮助确定根发生原因。通过VM信息板、您可以查看VM的性能统计信息、以便调查从VMware vSphere主机到网络最后再到存储的整个I/O路径。某些事件还提供了可用于更正问题描述 的补救措施。您可以为事件配置自定义警报、以便在发生问题时、通过电子邮件和SNMP陷阱通知您。Active IQ Unified Manager 可以预测容量和使用趋势、以便在出现问题之前主动采取行动、从而防止做出长期可能导致其他问题的被动短期决策、从而为用户的存储需求进行规划。

Cisco Intersight

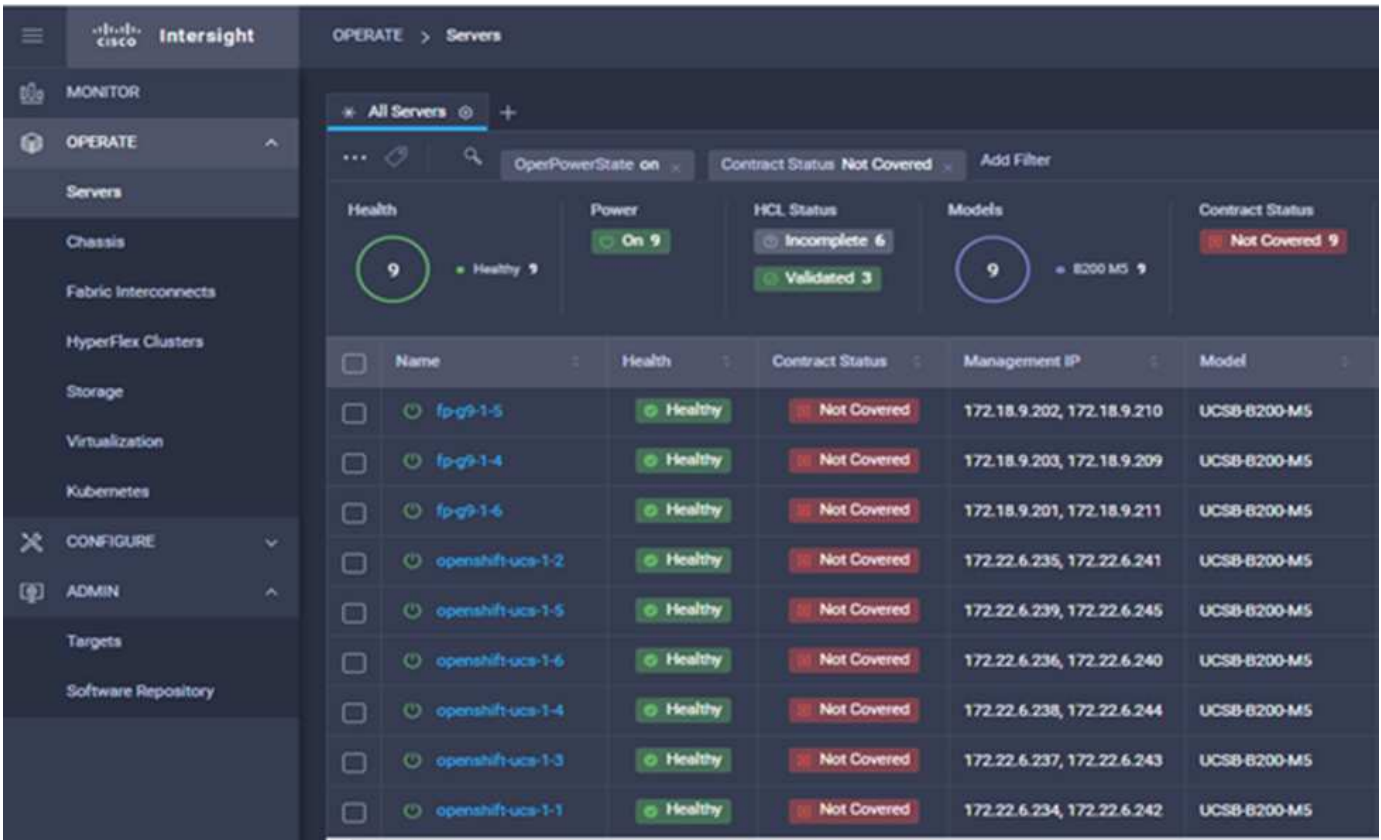
Cisco Intersight是一个SaaS平台、可为传统和云原生应用程序和基础架构提供智能自动化、可观察性和优化功能。该平台可帮助IT团队推动变革、并提供专为混合云设计的运营模式。

Cisco Intersight具有以下优势：

- *交付速度更快。*由于采用基于敏捷性的软件开发模式、可从云或客户数据中心以服务的形式交付、并经常进行更新和持续创新。这样、客户就可以专注于加快业务部门的交付速度。
- *简化操作。*通过使用一个安全的SaaS交付工具以及通用清单、身份验证和API在整个堆栈和所有位置之间运行、简化操作、消除团队之间的孤岛。从内部管理物理服务器和虚拟机管理程序到虚拟机、K8s、无服务器、自动化、在内部和公有 云之间实现优化和成本控制。
- *持续优化。*利用Cisco Intersight在每一层提供的智能以及Cisco TAC持续优化您的环境。这种智能功能可转换为建议的可自动操作、因此您可以实时适应每个变化：从移动工作负载和监控物理服务器的运行状况到自动调整K8s集群大小、再到您所使用的公有 云的成本降低建议。

Cisco Intersight支持两种管理操作模式：UCSM受管模式(Umm)和Intersight受管模式(IMM)。在首次设置互联阵列期间、您可以为光纤连接的Cisco UCS系统选择原生 Umm或IMM。在此解决方案 中、使用原生 Umm。

下图显示了Cisco Intersight信息板。

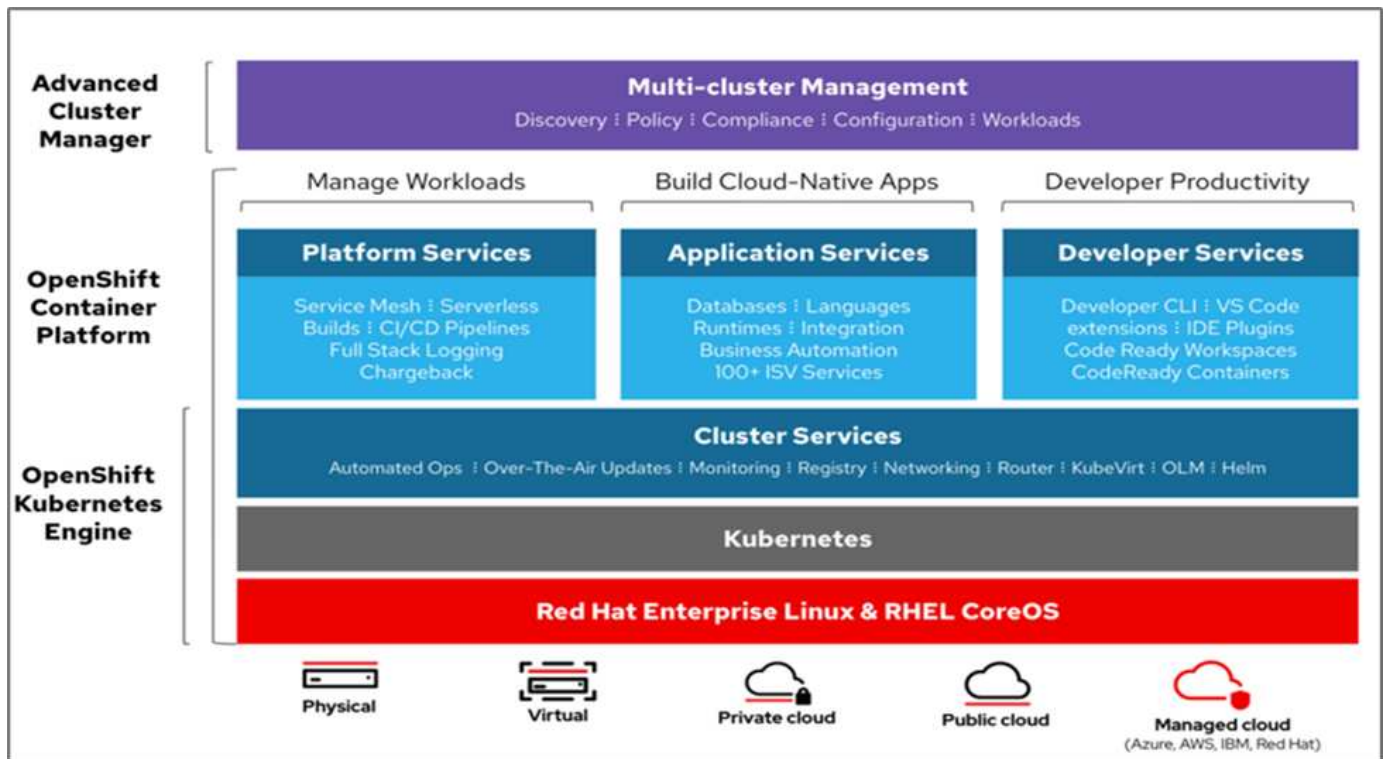


Red Hat OpenShift 容器平台

Red Hat OpenShift容器平台是一个容器应用程序平台、它将CRI-O和Kubernetes汇集在一起、并提供一个API和Web界面来管理这些服务。CRI-O是Kubernetes容器运行时接口(CRI)的实施、可使用与Open Container Initiative (OCI)兼容的运行。它是使用Docker作为Kubernetes运行时的轻型替代方案。

OpenShift容器平台允许客户创建和管理容器。容器是独立的进程、在其自身环境中运行、独立于操作系统和底层基础架构。OpenShift容器平台有助于开发、部署和管理基于容器的应用程序。它提供了一个自助服务平台、可按需创建、修改和部署应用程序、从而加快开发和发布生命周期。OpenShift容器平台具有一个基于微服务的架构、该架构包含可协同工作的小型分离单元。它在Kubernetes集群上运行、其中包含有关对象的数据存储在etcd中、etcd是一个可靠的集群模式密钥值存储。

下图概述了Red Hat OpenShift容器平台。



Kubernetes基础架构

在OpenShift容器平台中、Kubernetes跨一组CRI-O运行时主机管理容器化应用程序、并提供部署、维护和应用程序扩展机制。CRI-O服务软件包、实例化和运行容器化应用程序。

Kubernetes集群由一个或多个主节点和一组工作节点组成。此解决方案 设计包括硬件和软件堆栈中的高可用性(HA)功能。Kubernetes集群设计为在HA模式下运行、其中包含三个主节点和至少两个辅助节点、以帮助确保集群不会出现单点故障。

Red Hat核心操作系统

OpenShift容器平台使用Red Hat Enterprise Linux CoreOS (RHCOS)、这是一种面向容器的操作系统、它结合了CoreOS和Red Hat Atomic Host操作系统的一些最佳特性和功能。RHCOS专门为从OpenShift容器平台运行容器化应用程序而设计、可与新工具配合使用、以实现快速安装、基于操作员的管理和简化的升级。

RHCOS包括以下功能：

- IGNITION、OpenShift容器平台将其用作首次启动系统配置、用于首次启动和配置计算机。
- CRI-O是一种Kubernetes原生 容器运行时实施、它与操作系统紧密集成、可提供高效且优化的Kubernetes体验。CRI-O可提供运行、停止和重新启动容器的功能。它完全取代了OpenShift容器平台3中使用的Docker容器引擎。
- Kubernetes的主节点代理Kubelet负责启动和监控容器。

VMware vSphere 7.0

VMware vSphere是一个虚拟化平台、可将大量基础架构(包括CPU、存储和网络等资源)作为一个无缝、多功能且动态的操作环境进行全面管理。与管理单个计算机的传统操作系统不同、VMware vSphere可将整个数据中心的基础架构聚合在一起、从而创建一个具有资源的动力中心、这些资源可以快速动态地分配给任何需要的应用程序。

有关详细信息，请参见 ["VMware vSphere"](#)。

VMware vSphere vCenter

VMware vCenter Server可通过一个控制台统一管理所有主机和VM、并对集群、主机和VM进行聚合性能监控。通过VMware vCenter Server、管理员可以深入了解计算集群、主机、虚拟机、存储、子操作系统、虚拟基础架构的其他关键组件。VMware vCenter可管理VMware vSphere环境中提供的丰富功能。

硬件和软件版本

可以将此解决方案 扩展到运行中定义的受支持软件、固件和硬件版本的任何FlexPod 环境 ["NetApp 互操作性表工具"](#) 和 ["Cisco UCS硬件兼容性列表。"](#) OpenShift集群以裸机方式安装在FlexPod 和VMware vSphere上。

要管理多个OpenShift (K8s)集群、只需要一个Astra控制中心实例、而每个OpenShift集群上都安装了Trident CSI。Astra控制中心可以安装在其中任何一个OpenShift集群上。在此解决方案 中、Astra控制中心安装在OpenShift裸机集群上。

下表列出了OpenShift的FlexPod 硬件和软件版本。

组件	产品	version
计算	Cisco UCS互联阵列6454	4.1 (3c)
	Cisco UCS B200 M5服务器	4.1 (3c)
网络	Cisco Nexus 9336C-x2 NX-OS	9.3 (8)
存储	NetApp AFF A700	9.11.1
	NetApp Astra 控制中心	22.04.0
	NetApp Astra Trident CSI插件	22.04.0
	NetApp Active IQ Unified Manager	9.11
软件	VMware ESXi nenic 以太网驱动程序	1.0.35.0
	vSphere ESXi	7.0 (U2)
	VMware vCenter设备	7.0 U2b
	Cisco Intersight Assist虚拟设备	1.0.9-342
	OpenShift容器平台	4.9.
	OpenShift容器平台主节点	RHCOS 4.9
	OpenShift容器平台工作节点	RHCOS 4.9

下表列出了AWS上OpenShift的软件版本。

组件	产品	version
计算	主实例类型：m5.xlarge	不适用
	员工实例类型：m5.large	不适用
网络	虚拟私有云传输网关	不适用

组件	产品	version
存储	NetApp Cloud Volumes ONTAP	9.11.1
	NetApp Astra Trident CSI插件	22.04.0
软件	OpenShift容器平台	4.9.
	OpenShift容器平台主节点	RHCOS 4.9
	OpenShift容器平台工作节点	RHCOS 4.9

"接下来：适用于OpenShift容器平台4的FlexPod 裸机安装。"

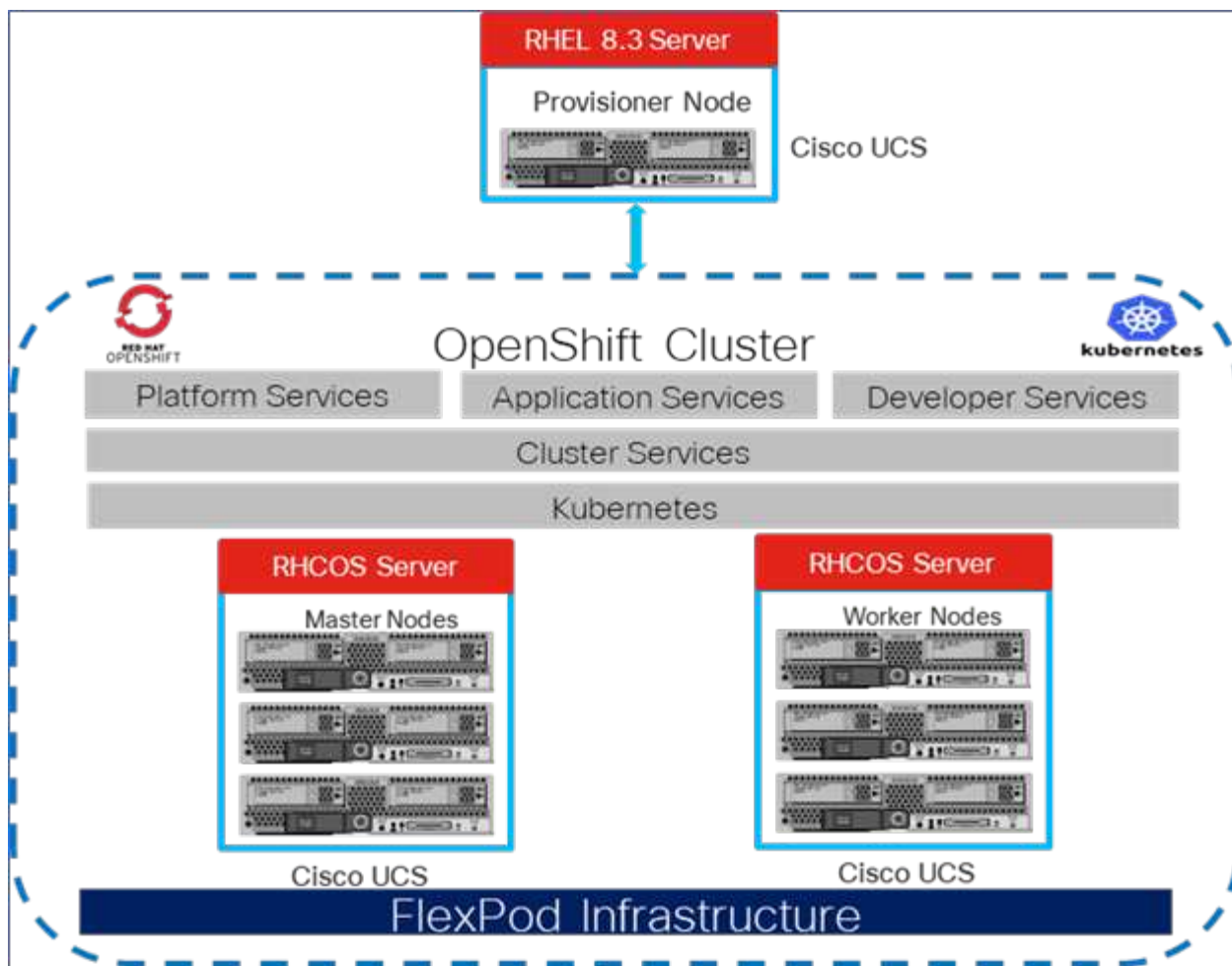
安装和配置

适用于**OpenShift**容器平台**4**的**FlexPod** 裸机安装

"先前版本：解决方案 组件。"

要了解适用于OpenShift容器平台4的FlexPod 裸机设计、部署详细信息以及NetApp Astra Trident安装和配置、请参见 "[采用OpenShift的FlexPod Cisco经验验证的设计和部署指南\(CVD\)](#)"。此CVD涵盖使用Ansible的FlexPod 和OpenShift容器平台部署。CVD还提供了有关准备工作节点、Astra Trident安装、存储后端和存储类配置的详细信息、这些配置是部署和配置Astra控制中心的几个前提条件。

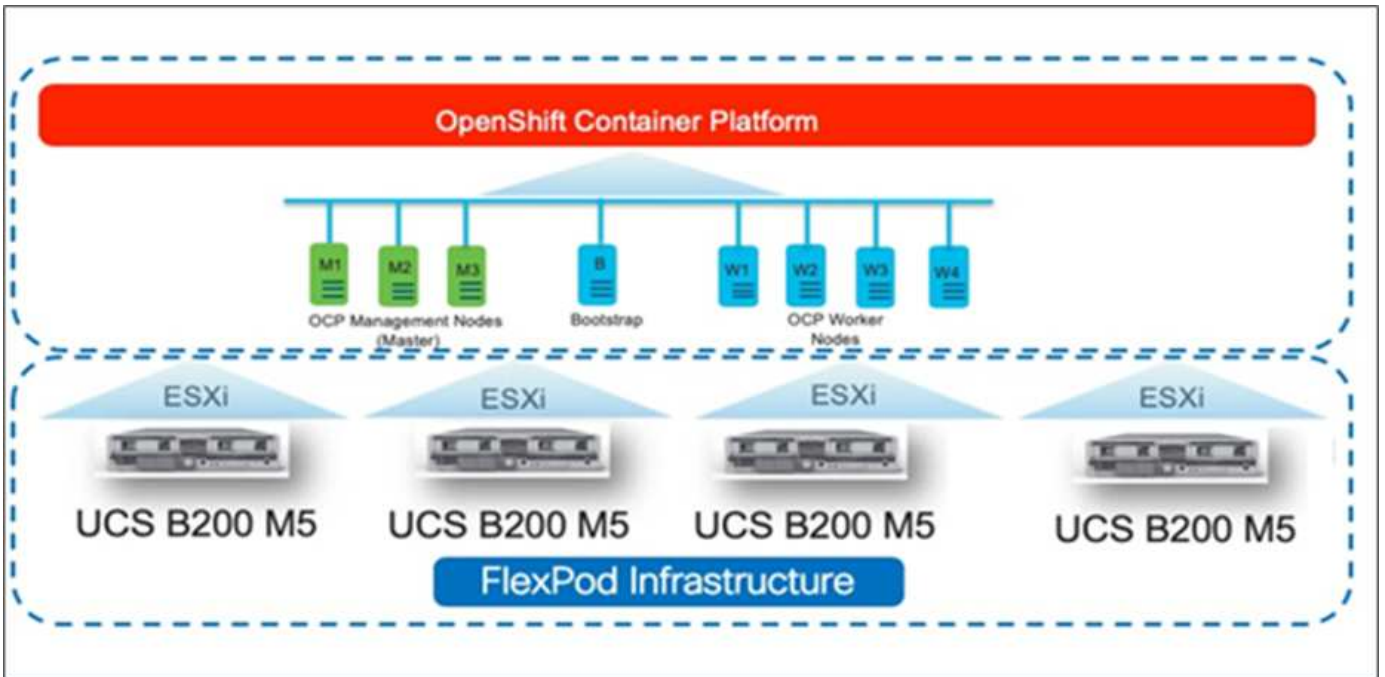
下图显示了FlexPod 上的OpenShift容器平台4裸机。



VMware安装上的适用于OpenShift容器平台4的FlexPod

有关在运行VMware vSphere的FlexPod 上部署Red Hat OpenShift容器平台4的详细信息、请参见 ["适用于OpenShift容器平台的FlexPod 数据中心4."](#)。

下图显示了vSphere上适用于OpenShift容器平台4的FlexPod。



"接下来：在AWS上运行Red Hat OpenShift。"

AWS上的Red Hat OpenShift

"先前版本：适用于OpenShift容器平台4的FlexPod 裸机安装。"

AWS上会部署一个单独的自管理OpenShift容器平台4集群作为灾难恢复站点。主节点和工作节点跨越三个可用性区域、以实现高可用性。

Instances (6) Info								
Search Clear filters								
☐	Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name	
☐	ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	-	
☐	ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	-	
☐	ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	-	
☐	ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	-	
☐	ocpaws-v58kn-worker-us-east-1b-7nmhc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	-	
☐	ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	-	

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
ip-172-30-164-128.ec2.internal	Ready	worker	29m	v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal	Ready	master	36m	v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal	Ready	master	33m	v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal	Ready	worker	30m	v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal	Ready	master	36m	v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal	Ready	worker	28m	v1.22.8+f34b40c

OpenShift部署为 "专用集群" 添加到AWS上的现有VPC中。专用OpenShift容器平台集群不会公开外部端点、只能从内部网络访问、并且在Internet上不可见。使用NetApp Cloud Manager部署单节点NetApp Cloud Volumes ONTAP 、它为Astra Trident提供存储后端。

有关在AWS上安装OpenShift的详细信息、请参见 "OpenShift文档"。

"下一步： NetApp Cloud Volumes ONTAP。 "

NetApp Cloud Volumes ONTAP

"先前版本： AWS上的Red Hat OpenShift。 "

NetApp Cloud Volumes ONTAP 实例部署在AWS上、并用作Astra Trident的后端存储。在添加Cloud Volumes ONTAP 工作环境之前、必须先部署连接器。如果您尝试在没有连接器的情况下创建首个Cloud Volumes ONTAP 工作环境、Cloud Manager将提示您。要在AWS中部署Connector、请参见 "创建连接器"。

要在AWS上部署Cloud Volumes ONTAP 、请参见 "AWS快速入门"。

部署Cloud Volumes ONTAP 后、您可以在OpenShift容器平台集群上安装Astra Trident并配置存储后端和Snapshot类。

"接下来： 在OpenShift容器平台上安装Astra Control Center。 "

在OpenShift容器平台上安装Astra Control Center

"先前版本： NetApp Cloud Volumes ONTAP。 "

您可以将Astra控制中心安装在FlexPod 上运行的OpenShift集群上、也可以安装在具有Cloud Volumes ONTAP 存储后端的AWS上。在此解决方案 中、Astra控制中心部署在OpenShift裸机集群上。

可以使用所述的标准过程安装Astra控制中心 "此处" 或从Red Hat OpenShift OperatorHub获取。Astra控制操作员是Red Hat认证的操作员。在此解决方案 中、使用Red Hat OperatorHub安装Astra控制中心。

环境要求

- Astra控制中心支持多个Kubernetes分发版；对于Red Hat OpenShift、支持的版本包括Red Hat OpenShift容器平台4.8或4.9。
- 除了环境和最终用户的应用程序资源要求之外、Astra控制中心还需要以下资源：

组件	要求
存储后端容量	至少500 GB可用
工作节点	至少3个辅助节点、每个节点具有4个CPU核心和12 GB RAM
完全限定域名(FQDN)地址	Astra 控制中心的 FQDN 地址
Astra Trident	已安装并配置 Astra Trident 21.04 或更高版本

组件	要求
入口控制器或负载均衡器	配置入口控制器以使用URL或负载均衡器公开Astra控制中心、以提供IP地址、并将其解析为FQDN

- 您必须具有可将Astra Control Center构建映像推送到的现有私有映像注册表。您需要提供用于上传映像的映像注册表的URL。



执行某些工作流时会提取某些映像、并在必要时创建和销毁容器。

- Astra 控制中心要求创建一个存储类并将其设置为默认存储类。Astra 控制中心支持由 Astra Trident 提供的以下 ONTAP 驱动程序：
 - ontap-NAS
 - ontap-nas-flexgroup
 - ontap-san
 - ontap-san-economy.



我们假设已部署的OpenShift集群安装了Astra Trident并配置了ONTAP 后端、同时还定义了默认存储类。

- 对于OpenShift环境中的应用程序克隆、Astra Control Center需要允许OpenShift挂载卷并更改文件所有权。要修改ONTAP 导出策略以允许执行这些操作、请运行以下命令：

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```



要将第二个OpenShift操作环境添加为托管计算资源、请确保已启用Astra Trident卷快照功能。要使用Astra Trident启用和测试卷快照、请参见官方信息 "[Astra Trident说明](#)"。

- 答 "[VolumeSnapClass](#)" 应在管理应用程序的所有Kubernetes集群上进行配置。这也可能包括安装了Astra控制中心的K8s集群。Astra控制中心可以管理运行该控制中心的K8s集群上的应用程序。

应用程序管理要求

- *许可。*要使用Astra控制中心管理应用程序、您需要获得Astra控制中心许可证。
- *命名空间。*命名空间是可由Astra控制中心作为应用程序进行管理的最大实体。您可以选择根据现有命名空间中的应用程序标签和自定义标签筛选出组件、并将部分资源作为应用程序进行管理。
- *存储类。*如果您安装的应用程序明确设置了StorageClass、并且需要克隆该应用程序、则克隆操作的目标集群必须具有最初指定的StorageClass。将显式设置了StorageClass的应用程序克隆到不具有相同StorageClass的集群失败。
- * Kubernetes Resources。*使用非Astra Control捕获的Kubernetes资源的应用程序可能无法提供完整的应用程序数据管理功能。Astra Control可以捕获以下Kubernetes资源：

Kubernetes资源		
ClusterRole	ClusterRoleBinding.	配置映射
自定义资源定义	自定义资源	cronjob
DemonSet	HorizontalPodAutoscaler	传入
DeploymentConfig	MutatingWebhook	PersistentVolumeClaim
POD	PodDisruptionBuget	播客模板
网络策略	ReplicaSet	Role
RoleBinding.	路由	机密
验证 Webhook		

使用 OpenShift OperatorHub 安装 Astra 控制中心

以下操作步骤 将使用Red Hat OperatorHub安装Astra控制中心。在此解决方案 中、Astra控制中心安装在运行于FlexPod 上的裸机OpenShift集群上。

1. 从下载 Astra 控制中心捆绑包 (Astra-control-center-[version].tar.gz) ["NetApp 支持站点"](#)。
2. 从下载Astra控制中心证书和密钥的.zip文件 ["NetApp 支持站点"](#)。
3. 验证捆绑包的签名。

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. 提取Astra映像。

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. 更改为 Astra 目录。

```
cd astra-control-center-[version]
```

6. 将映像添加到本地注册表。

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. 使用相应的脚本加载映像、标记映像并将其推送到本地注册表。

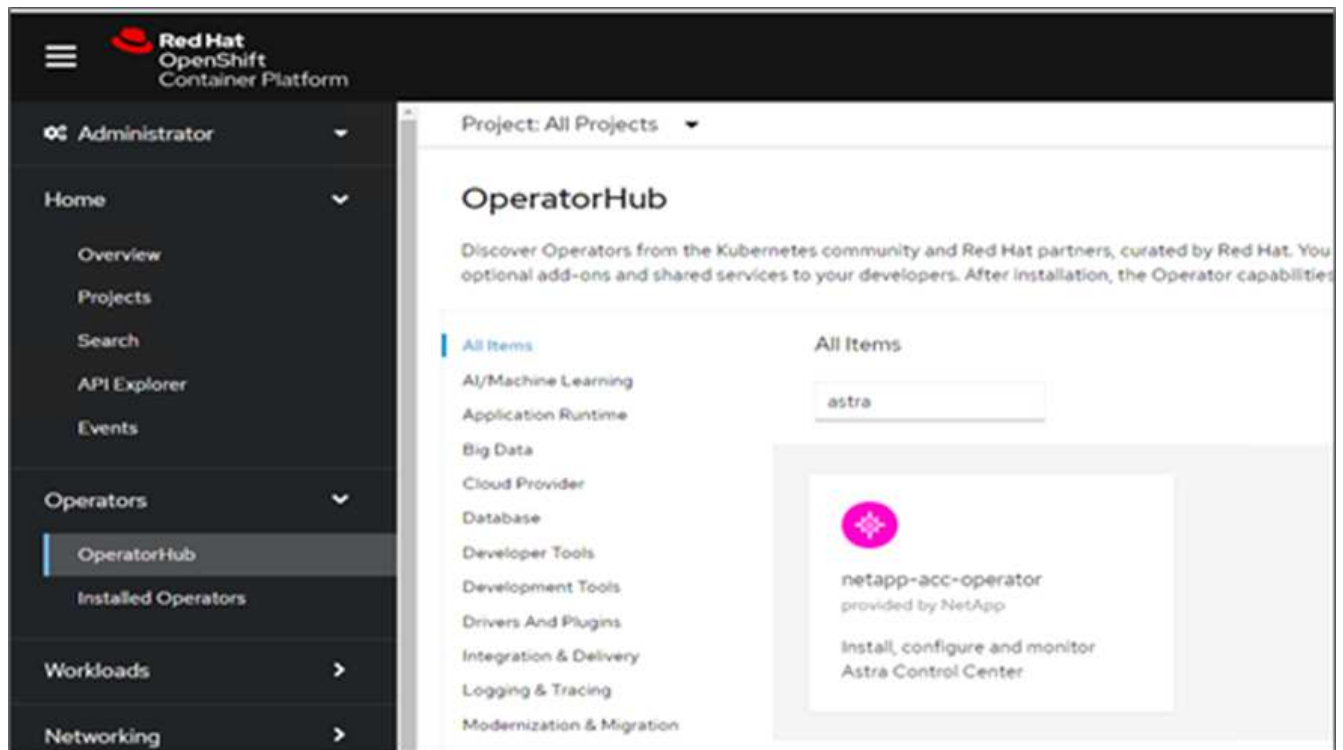
对于 Docker :

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
    # Load to local cache. And store the name of the loaded image trimming
    the 'Loaded images: '
    astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //' )
    astraImage=$(echo ${astraImage} | sed 's!localhost/!!!')
    # Tag with local image repo.
    docker tag ${astraImage} ${REGISTRY}/${astraImage}
    # Push to the local repo.
    docker push ${REGISTRY}/${astraImage}
done
```

对于 Podman :

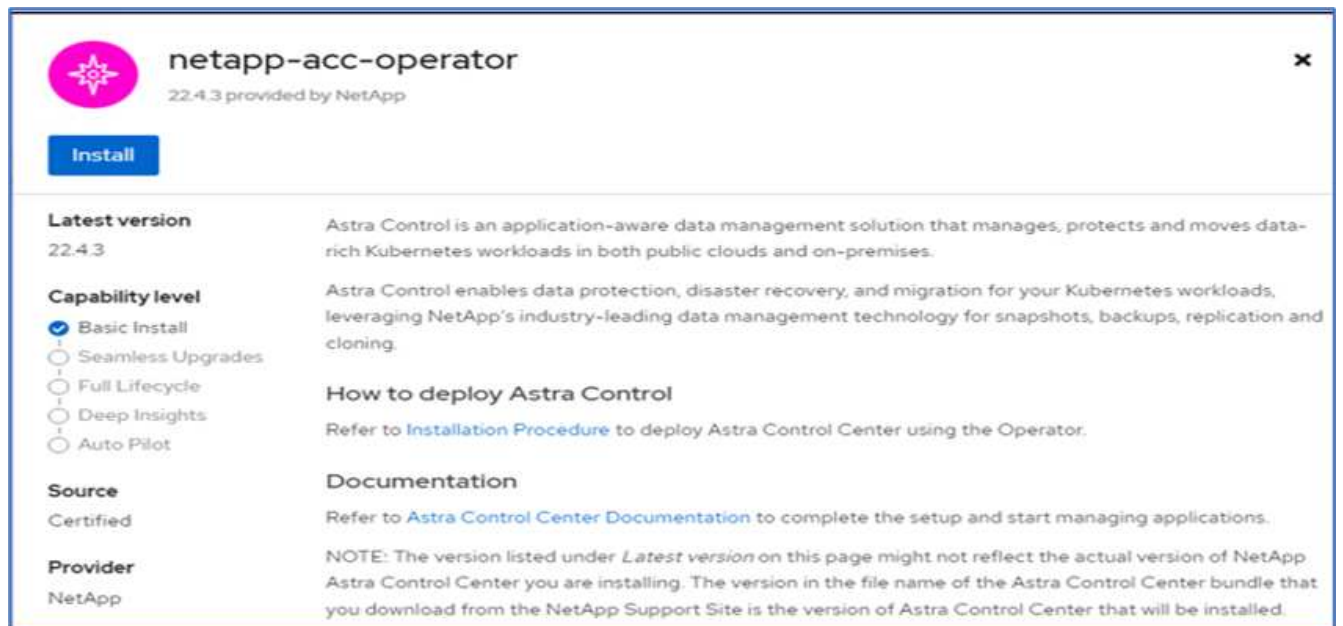
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
    # Load to local cache. And store the name of the loaded image trimming
    the 'Loaded images: '
    astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //' )
    astraImage=$(echo ${astraImage} | sed 's!localhost/!!!')
    # Tag with local image repo.
    podman tag ${astraImage} ${REGISTRY}/${astraImage}
    # Push to the local repo.
    podman push ${REGISTRY}/${astraImage}
done
```

8. 登录到裸机OpenShift集群Web控制台。从侧面菜单中、选择Operators > OperatorHub。输入`Astra`以列出`NetApp-Acc-operator`。



`NetApp-Acc-operator`是一个经过认证的Red Hat OpenShift操作员、并列在OperatorHub目录下。

9. 选择`NetApp-Acc-operator`、然后单击安装。



10. 选择相应的选项、然后单击安装。

OperatorHub > Operator Installation

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel * ⓘ

☐ alpha

☒ stable

Installation mode *

☒ All namespaces on the cluster (default)
Operator will be available in all Namespaces.

☐ A specific namespace on the cluster
This mode is not supported by this Operator

Installed Namespace *

PR netapp-acc-operator (Operator recommended)

Namespace creation
Namespace **netapp-acc-operator** does not exist and will be created.

Update approval * ⓘ

☐ Automatic

☒ Manual

Manual approval applies to all operators in a namespace
Installing an operator with manual approval causes all operators installed in namespace **netapp-acc-operator** to function as manual approval strategy. To allow automatic approval, all operators installed in the namespace must use automatic approval strategy.

netapp-acc-operator
provided by NetApp

Provided APIs

ACC Astra Control Center
AstraControlCenter is the Schema for the astracontrolcenters API.

Install **Cancel**

11. 批准安装并等待操作员安装。

netapp-acc-operator
22.4.3 provided by NetApp

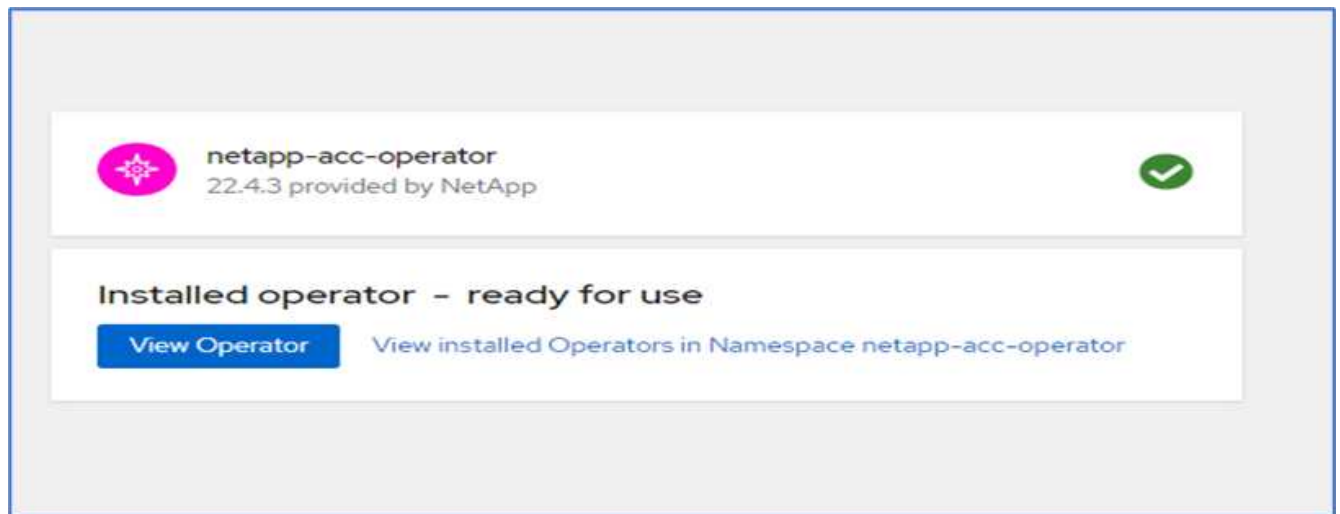
Manual approval required

Review the **manual install plan** for operators **acc-operator.v22.4.3**. Once approved, the following resources will be created in order to satisfy the requirements for the components specified in the plan. Click the resource name to view the resource in detail.

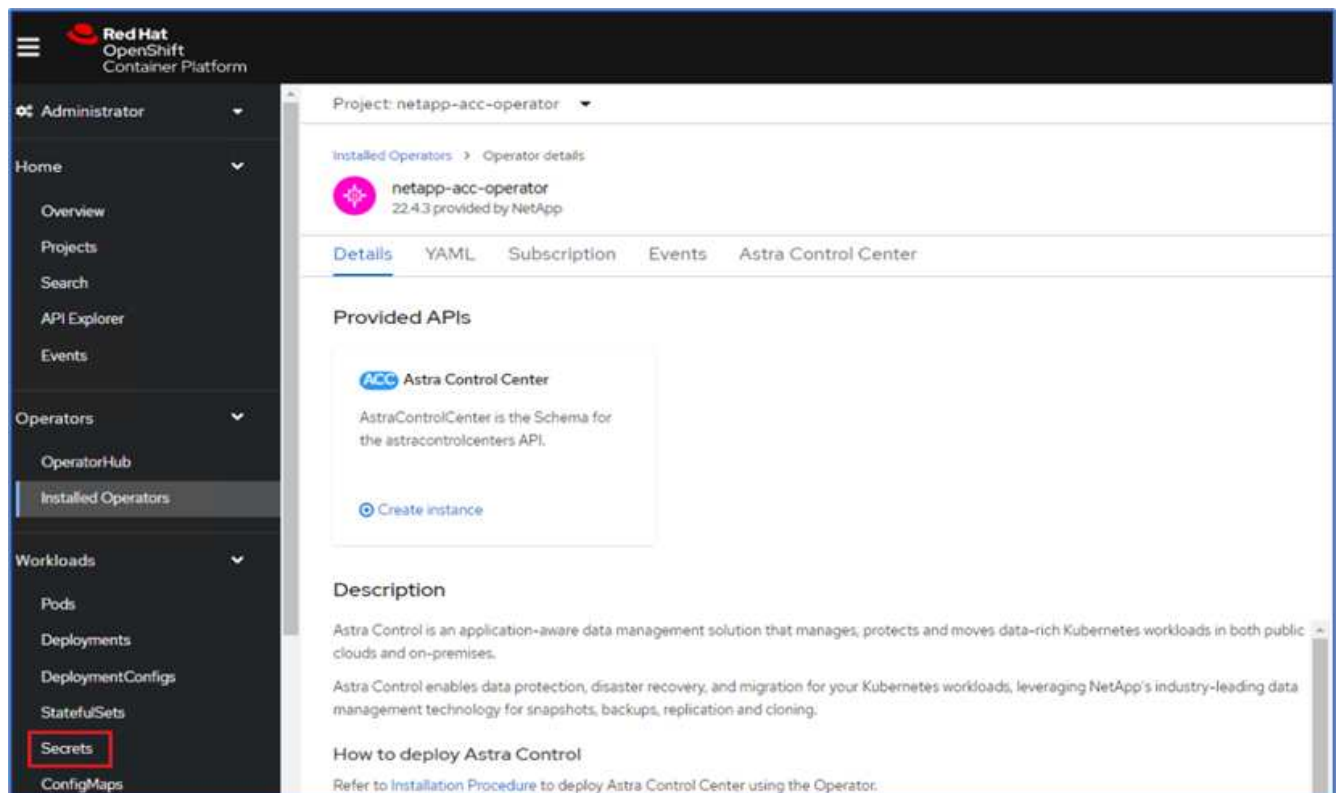
Approve **Deny**

[View installed Operators in Namespace netapp-acc-operator](#)

12. 在此阶段、操作员已成功安装并准备就绪、可以使用。单击View Operator开始安装Astra Control Center。



13. 在安装Astra控制中心之前、请创建Pull密钥、以便从先前推送的Docker注册表下载Astra映像。



14. 要从Docker私有repo中提取Astra控制中心映像、请在`NetApp-Acc-operator`命名空间中创建一个密钥。此机密名称将在Astra控制中心YAML清单中稍后提供。

Project: netapp-acc-operator ▼

Create image pull secret

Image pull secrets let you authenticate against a private image registry.

Secret name *

Unique name of the new secret.

Authentication type

Registry server address *

For example quay.io or docker.io

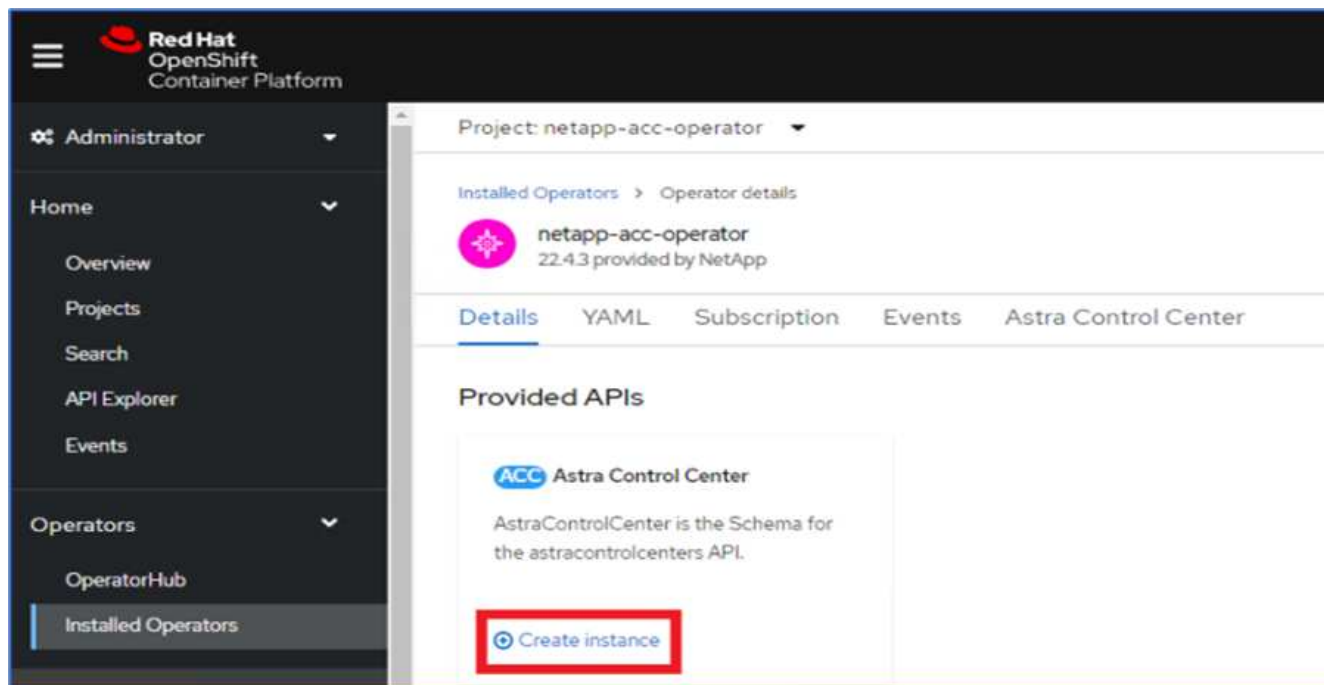
Username *

Password *

Email

[+ Add credentials](#)

15. 从侧面菜单中、选择Operators > Installed Operators、然后单击提供的API部分下的Create Instance。



16. 填写创建AstraControlCenter表单。提供名称、Astra地址和Astra版本。

The screenshot shows the 'Create AstraControlCenter' form. The form is titled 'Create AstraControlCenter' and includes a note: 'Create by completing the form. Default values may be provided by the Operator authors.' The form is configured via 'Form view' (selected) or 'YAML view'. A note states: 'Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.' The form fields are:

- Name ***: acc
- Labels**: app=frontend
- Auto Support ***: AutoSupport indicates willingness to participate in NetApp's proactive support application, NetApp Active IQ. An internet connection is required (port 442) and all support data is anonymized. The default election is true and indicates no support data will be sent to NetApp. An empty or blank election is the same as a default election. Air gapped installations should enter false.
- Astra Address ***: acc.ocp.flexpod.netapp.com
AstraAddress defines how Astra will be found in the data center. This IP address and/or DNS A record must be created prior to provisioning Astra Control Center. Example - "astra.example.com" The A record and its IP address must be allocated prior to provisioning Astra Control Center.
- Astra Version ***: 22.04.0
Version of AstraControlCenter to deploy. You are provided a Helm repository with a corresponding version. Example - 1.5.2, 1.4.2-patch



在Astra Address下、提供Astra控制中心的FQDN地址。此地址用于访问Astra控制中心Web控制台。FQDN还应解析为可访问的IP网络、并应在DNS中进行配置。

17. 输入帐户名称、电子邮件地址、管理员姓氏、并保留默认卷回收策略。如果使用的是负载均衡器、请将"传入类型"设置为`AccTraefik`。否则、请为`In防护.Controller`选择Generic。在映像注册表下、输入容器映像注册表路径和密钥。

Project: netapp-acc-operator

Account Name *
ocp
Astra Control Center account name

Email *
abhinav3@netapp.com
EmailAddress will be notified by Astra as events warrant.

Last Name
Singh
The last name of the SRE supporting Astra.

Volume Reclaim Policy
Retain
Reclaim policy to be set for persistent volumes

Ingress Type
AccTraefik
IngressType The type of ingress to that ACC should be configured for

Astra Kube Config Secret

AstraKubeConfigSecret if present and secret exists operator will attempt to add KubeConfig to Managed Clusters.

Image Registry
The container image registry that is hosting the Astra application images, ACC Operator and ACC Helm Repository.

Name
[redacted]
The name of the image registry. For example "example.registry/astra". Do not prefix with protocol.

Secret
astra-registry-cred
The name of the Kubernetes secret that will authenticate with the image registry.



在此解决方案 中、使用了金属负载均衡器。因此、入口类型为AccTraefik。这会将Astra控制中心traefik网关公开为loadbalancer类型的Kubernetes服务。

18. 输入管理员的名字、配置资源扩展并提供存储类。单击创建。

Image Registry
The container image registry that is hosting the Astra application images, ACC Operator and ACC Helm Repository.

First Name
Abhinav
The first name of the SRE supporting Astra.

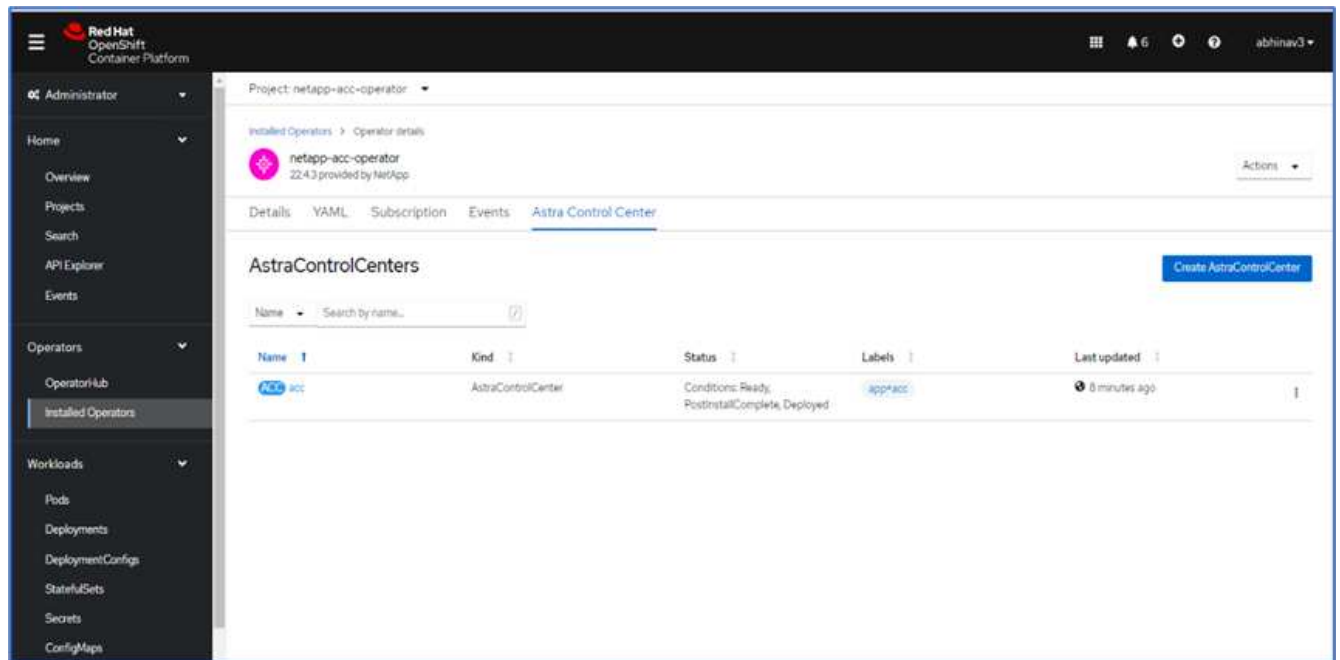
Astra Resources Scaler
Default
Scaling options for AstraControlCenter Resource limits.

Storage Class
ocp-nas-sc-gold
The storage class to be used for PVCs. If not set, default storage class will be used.

Crds
Options for how ACC should handle CRDs.Options for how ACC should handle CRDs.Options for how ACC should handle CRDs.Options for how ACC should handle CRDs.

Create **Cancel**

Astra控制中心实例的状态应从"Deploying (部署)"更改为"Ready (就绪)"。



19. 确认所有系统组件均已成功安装、并且所有Pod均已运行。

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                     READY   STATUS    RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v          1/1     Running   0           10m
acc-operator-controller-manager-5c656c44c6-tqnmn  2/2     Running   0           13m
activity-589c6d59f4-x2sfs               1/1     Running   0           6m4s
api-token-authentication-4q5lj           1/1     Running   0           5m26s
api-token-authentication-pzptd           1/1     Running   0           5m27s
api-token-authentication-tbtg6           1/1     Running   0           5m27s
asup-669df8d49-qps54                    1/1     Running   0           5m26s
authentication-5867c5f56f-dnpp2          1/1     Running   0           3m54s
bucketservice-85495bc475-5zcc5           1/1     Running   0           5m55s
cert-manager-67f486bbc6-txhh6            1/1     Running   0           9m5s
cert-manager-cainjector-75959db744-4l5p5  1/1     Running   0           9m6s
cert-manager-webhook-765556b869-g6wdf    1/1     Running   0           9m6s
```

9m6s			
cloud-extension-5d595f85f-txrfl	1/1	Running	0
5m27s			
cloud-insights-service-674649567b-5s4wd	1/1	Running	0
5m49s			
composite-compute-6b58d48c69-46vhc	1/1	Running	0
6m11s			
composite-volume-6d447fd959-chnrt	1/1	Running	0
5m27s			
credentials-66668f8ddd-8qc5b	1/1	Running	0
7m20s			
entitlement-fd6fc5c58-wxnmh	1/1	Running	0
6m20s			
features-756bbb7c7c-rgcrm	1/1	Running	0
5m26s			
fluent-bit-ds-278pg	1/1	Running	0
3m35s			
fluent-bit-ds-5pqc6	1/1	Running	0
3m35s			
fluent-bit-ds-8l7cq	1/1	Running	0
3m35s			
fluent-bit-ds-9qbft	1/1	Running	0
3m35s			
fluent-bit-ds-nj475	1/1	Running	0
3m35s			
fluent-bit-ds-x9pd8	1/1	Running	0
3m35s			
graphql-server-698d6f4bf-kftwc	1/1	Running	0
3m20s			
identity-5d4f4c87c9-wjz6c	1/1	Running	0
6m27s			
influxdb2-0	1/1	Running	0
9m33s			
krakend-657d44bf54-8cb56	1/1	Running	0
3m21s			
license-594bbdc-rghdg	1/1	Running	0
6m28s			
login-ui-6c65fbabd4-jg8wz	1/1	Running	0
3m17s			
loki-0	1/1	Running	0
9m30s			
metrics-facade-75575f69d7-hnlk6	1/1	Running	0
6m10s			
monitoring-operator-65dff79cfb-z78vk	2/2	Running	0
3m47s			
nats-0	1/1	Running	0

10m			
nats-1	1/1	Running	0
9m43s			
nats-2	1/1	Running	0
9m23s			
nautilus-7bb469f857-4hlc6	1/1	Running	0
6m3s			
nautilus-7bb469f857-vz94m	1/1	Running	0
4m42s			
openapi-8586db4bcd-gwwvf	1/1	Running	0
5m41s			
packages-6bdb949cfb-nrq8l	1/1	Running	0
6m35s			
polaris-consul-consul-server-0	1/1	Running	0
9m22s			
polaris-consul-consul-server-1	1/1	Running	0
9m22s			
polaris-consul-consul-server-2	1/1	Running	0
9m22s			
polaris-mongodb-0	2/2	Running	0
9m22s			
polaris-mongodb-1	2/2	Running	0
8m58s			
polaris-mongodb-2	2/2	Running	0
8m34s			
polaris-ui-5df7687dbd-trcnf	1/1	Running	0
3m18s			
polaris-vault-0	1/1	Running	0
9m18s			
polaris-vault-1	1/1	Running	0
9m18s			
polaris-vault-2	1/1	Running	0
9m18s			
public-metrics-7b96476f64-j88bw	1/1	Running	0
5m48s			
storage-backend-metrics-5fd6d7cd9c-vc4j	1/1	Running	0
5m59s			
storage-provider-bb85ff965-m7qrq	1/1	Running	0
5m25s			
telegraf-ds-4zqgz	1/1	Running	0
3m36s			
telegraf-ds-cp9x4	1/1	Running	0
3m36s			
telegraf-ds-h4n59	1/1	Running	0
3m36s			
telegraf-ds-jnp2q	1/1	Running	0

3m36s			
telegraf-ds-pdz5j	1/1	Running	0
3m36s			
telegraf-ds-znqtp	1/1	Running	0
3m36s			
telegraf-rs-rt64j	1/1	Running	0
3m36s			
telemetry-service-7dd9c74bfc-sfkzt	1/1	Running	0
6m19s			
tenancy-d878b7fb6-wf8x9	1/1	Running	0
6m37s			
traefik-6548496576-5v2g6	1/1	Running	0
98s			
traefik-6548496576-g82pq	1/1	Running	0
3m8s			
traefik-6548496576-psn49	1/1	Running	0
38s			
traefik-6548496576-qrkfd	1/1	Running	0
2m53s			
traefik-6548496576-srs6r	1/1	Running	0
98s			
trident-svc-679856c67-78kbt	1/1	Running	0
5m27s			
vault-controller-747d664964-xmn6c	1/1	Running	0
7m37s			

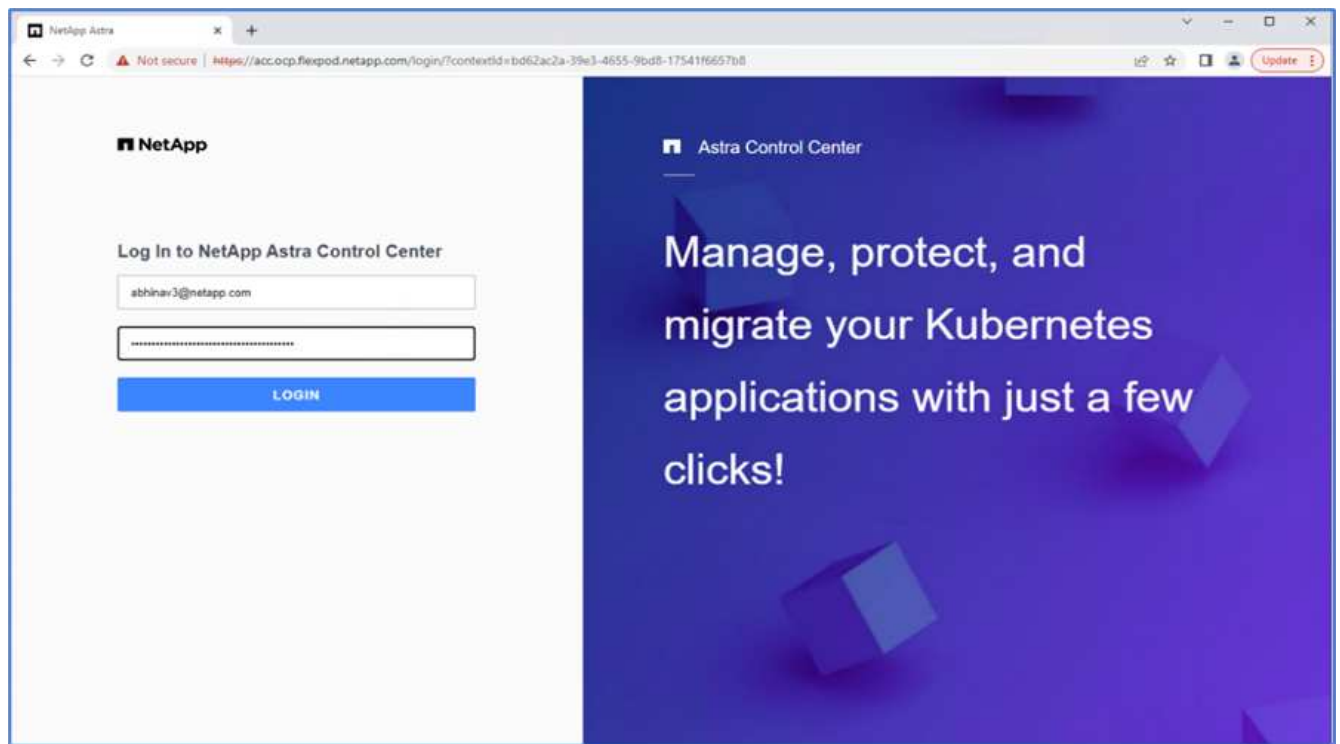


每个POD的状态应为"runned"。部署系统Pod可能需要几分钟的时间。

20. 所有Pod运行时、运行以下命令以检索一次性密码。在输出的YAML版本中、检查`status.deploymentState`字段中的已部署值、然后复制`status.uuid`值。密码为`Acc-`、后跟UUID值。(Acc-UUID)。

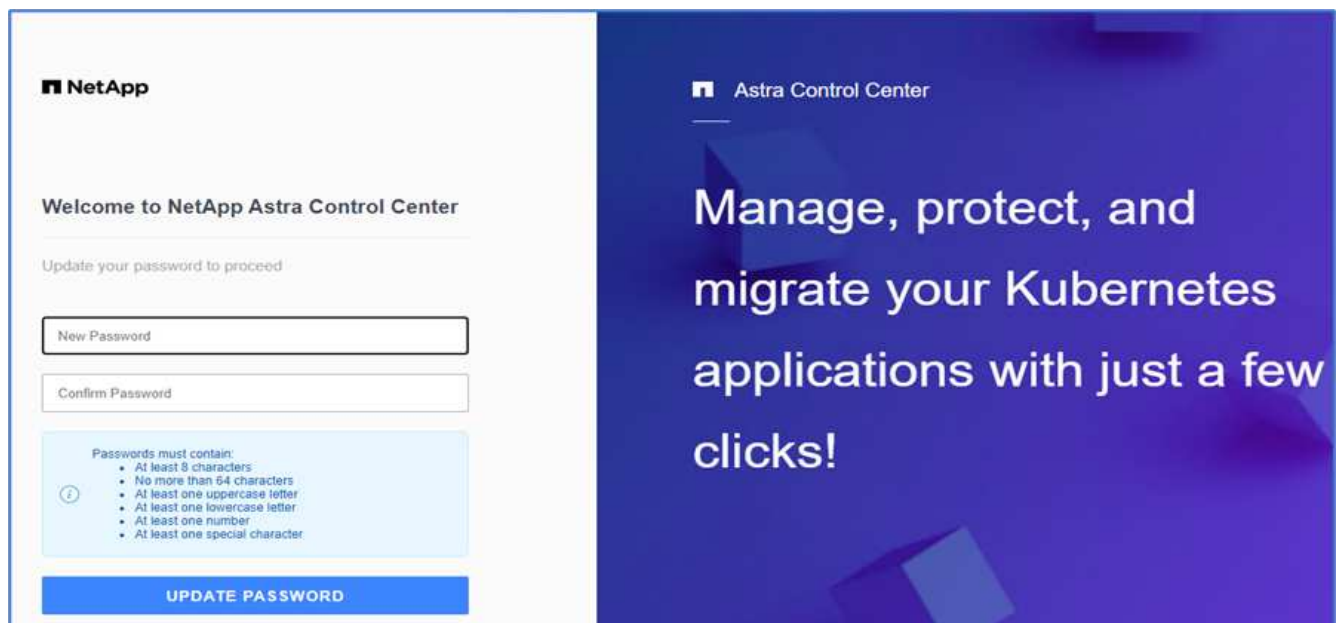
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. 在浏览器中、使用您提供的FQDN导航到URL。
22. 使用默认用户名(即安装期间提供的电子邮件地址)和一次性密码Acc-UUID登录。



如果您输入的密码三次不正确、则管理员帐户将锁定15分钟。

23. 更改密码并继续。

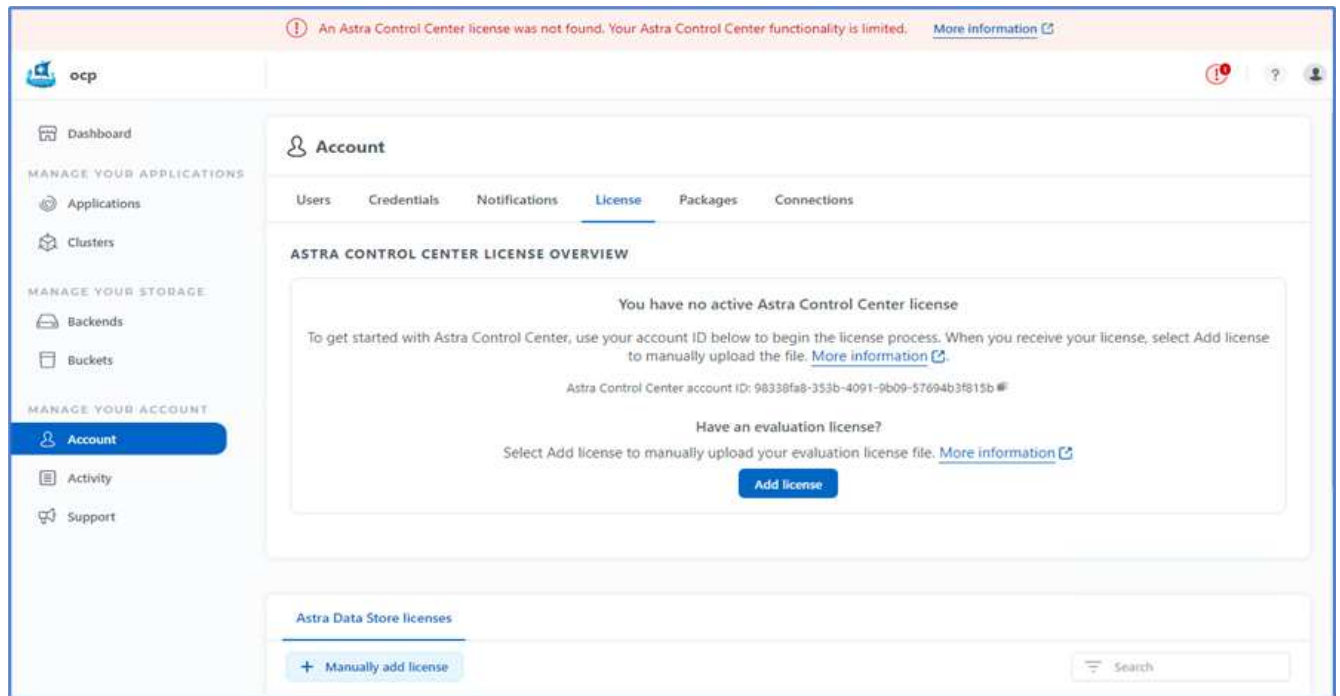


有关Astra控制中心安装的详细信息、请参见 "[Astra控制中心安装概述](#)" 页面。

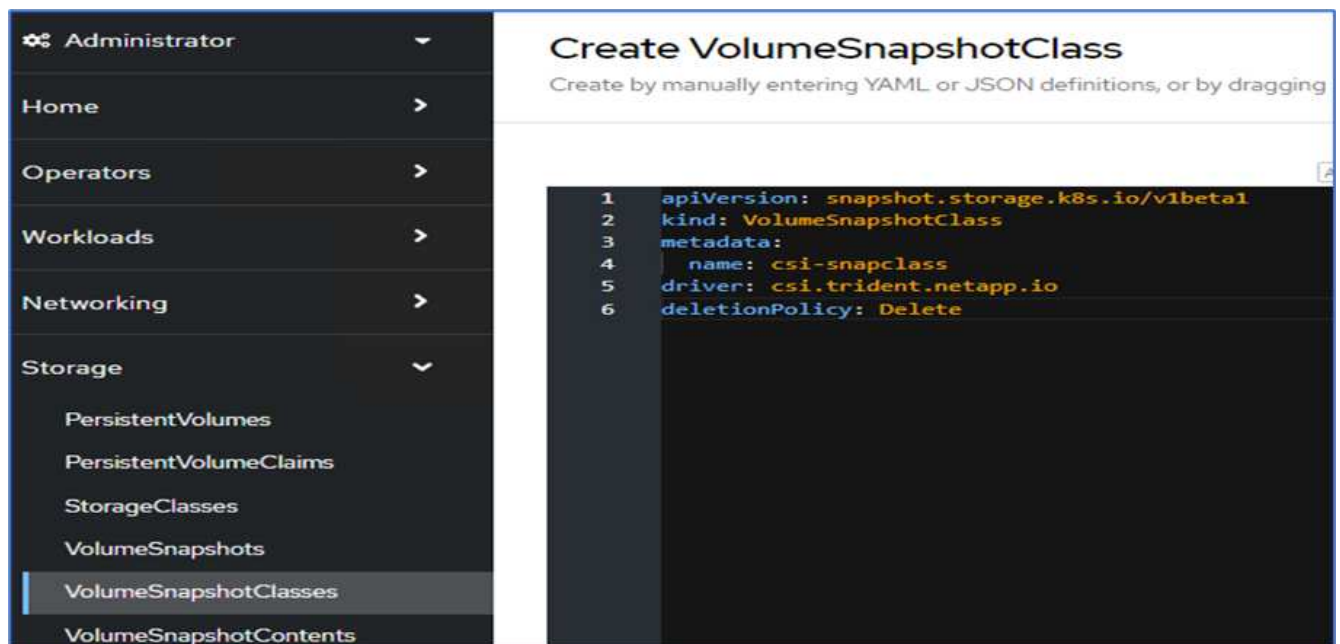
设置 **Astra** 控制中心

安装Astra控制中心后、登录到用户界面、上传许可证、添加集群、管理存储以及添加存储分段。

1. 在主页上的Account下、转到License选项卡并选择Add License以上传Astra许可证。



- 在添加OpenShift集群之前、请从OpenShift Web控制台创建Astra Trident卷快照类。卷快照类配置了`csi.trident.netapp.io`驱动程序。



- 要添加Kubernetes集群、请转到主页上的Clusters、然后单击Add Kubernetes Cluster。然后上传集群的`kubeconfig`文件并提供凭据名称。单击下一步。

Add Kubernetes cluster

STEP 1/3: CREDENTIALS

CREDENTIALS

Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.

Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.

Upload file

Paste from clipboard

Kubeconfig YAML file
kubeconfig-noingress

Credential name
onprem-ocp-bm

Cancel

Next →

- 系统会自动发现现有存储类。选择默认存储类、单击下一步、然后单击添加集群。

Add cluster

STEP 2/3: STORAGE

STORAGE

Existing storage classes are discovered and verified as eligible for use with Astra Control. You can use your existing default, or choose to set a new default at this time.

Applications with persistent volumes on eligible storage classes are validated for use with Astra Control.

Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligible
☒	ocp-nas-sc-gold	csi.trident.netapp.io	Delete	Immediate	

← Back

Next →

- 只需几分钟即可添加集群。要添加其他OpenShift容器平台集群、请重复步骤1–4。



要将其他OpenShift操作环境添加为托管计算资源、请确保使用Astra Trident "VolumeSnapshotClass对象" 已定义。

- 要管理存储、请转至后端、单击"Actions against the backend that you would like to manage"下的三个点。单击Manage。

Name	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
c190-cluster	Discovered	Not available yet	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
healthylife	Discovered	Not available yet	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
singlecvoaws	Discovered	Not available yet	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮

7. 提供ONTAP 凭据、然后单击下一步。查看相关信息、然后单击受管。后端应类似于以下示例。

Name	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
c190-cluster	Available	0.4/10.64 TiB: 3.8%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
healthylife	Available	5.16/106.42 TiB: 4.8%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
singlecvoaws	Available	0.07/0.62 TiB: 11.9%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮

8. 要将存储分段添加到Astra Control、请选择Bucket并单击Add。

Name	Description	State	Type
+ Add			

9. 选择存储分段类型并提供存储分段名称、S3服务器名称或IP地址和S3凭据。单击更新。



在此解决方案 中、AWS S3和ONTAP S3存储分段均已使用。您也可以使用StorageGRID。

存储分段状态应为运行状况良好。

Name	Description	State	Type	Actions
acc-aws-bucket		Healthy	Generic S3	
astra-bucket	On Prem S3 Bucket	Healthy	NetApp ONTAP S3	

作为向Astra控制中心注册Kubernetes集群以实现应用程序感知型数据管理的一部分、Astra Control会自动创建角色绑定和NetApp监控命名空间、以便从应用程序Pod和工作节点收集指标和日志。将一个受支持的基于ONTAP的存储类设置为默认值。

你先请 "将集群添加到 Astra Control 管理中"、您可以在集群上安装应用程序(在Astra Control之外)、然后转到Astra Control中的应用程序页面来管理这些应用程序及其资源。有关使用Astra管理应用程序的详细信息、请参见 "应用程序管理要求"。

"接下来：解决方案 验证概述。"

解决方案验证

概述

"先前版本：在OpenShift容器平台上安装Astra Control Center。"

在本节中、我们将回顾解决方案 以及一些使用情形：

- 将有状态应用程序从远程备份还原到云中运行的另一个OpenShift集群。
- 将有状态应用程序还原到OpenShift集群中的同一命名空间。
- 通过从一个FlexPod 系统(OpenShift容器平台裸机)克隆到另一个FlexPod 系统(VMware上的OpenShift容器平台)来实现应用程序移动性。

值得注意的是、此解决方案 仅验证了少数使用情形。此验证并不代表Astra控制中心的全部功能。

"接下来：使用远程备份恢复应用程序。"

通过远程备份恢复应用程序

"上一步：解决方案 验证概述。"

借助Astra、您可以进行完整的应用程序一致的备份、用于将应用程序及其数据还原到在内部数据中心或公有云中运行的不同Kubernetes集群。

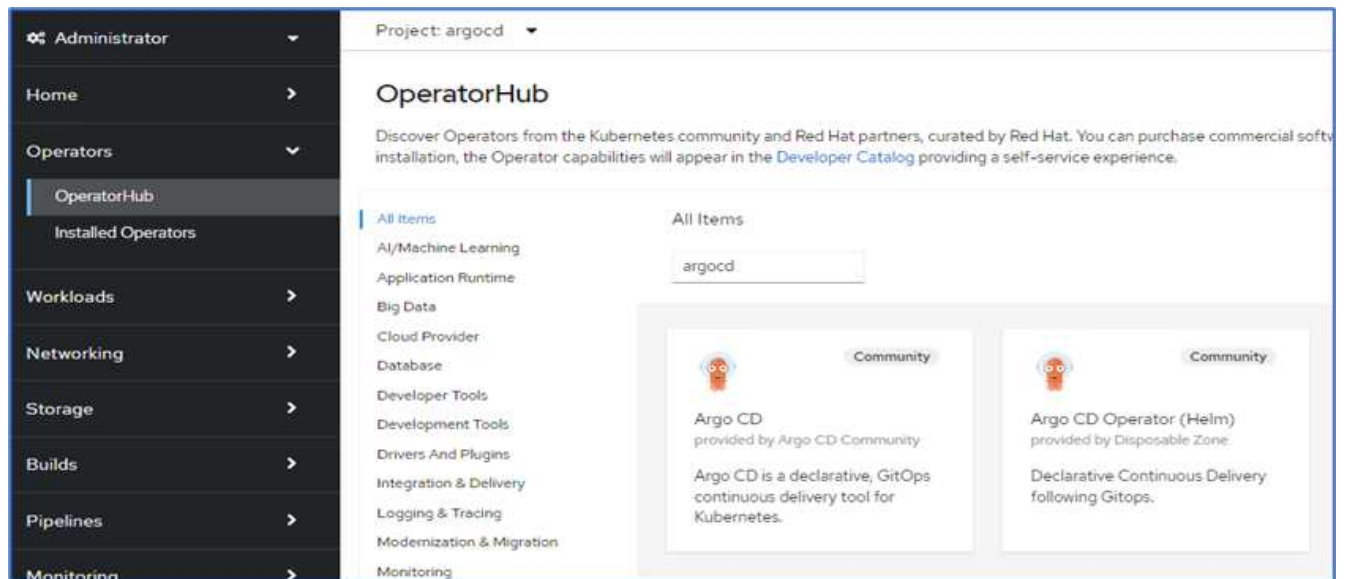
要验证应用程序恢复是否成功、请模拟FlexPod 系统上运行的应用程序的内部故障、并使用远程备份将应用程序还原到云中运行的K8s集群。

此示例应用程序是一个使用MySQL作为数据库的价目表应用程序。为了实现部署自动化、我们使用了 "Argo CD" 工具。Argo CD是一款适用于Kubernetes的声明性GitOps持续交付工具。

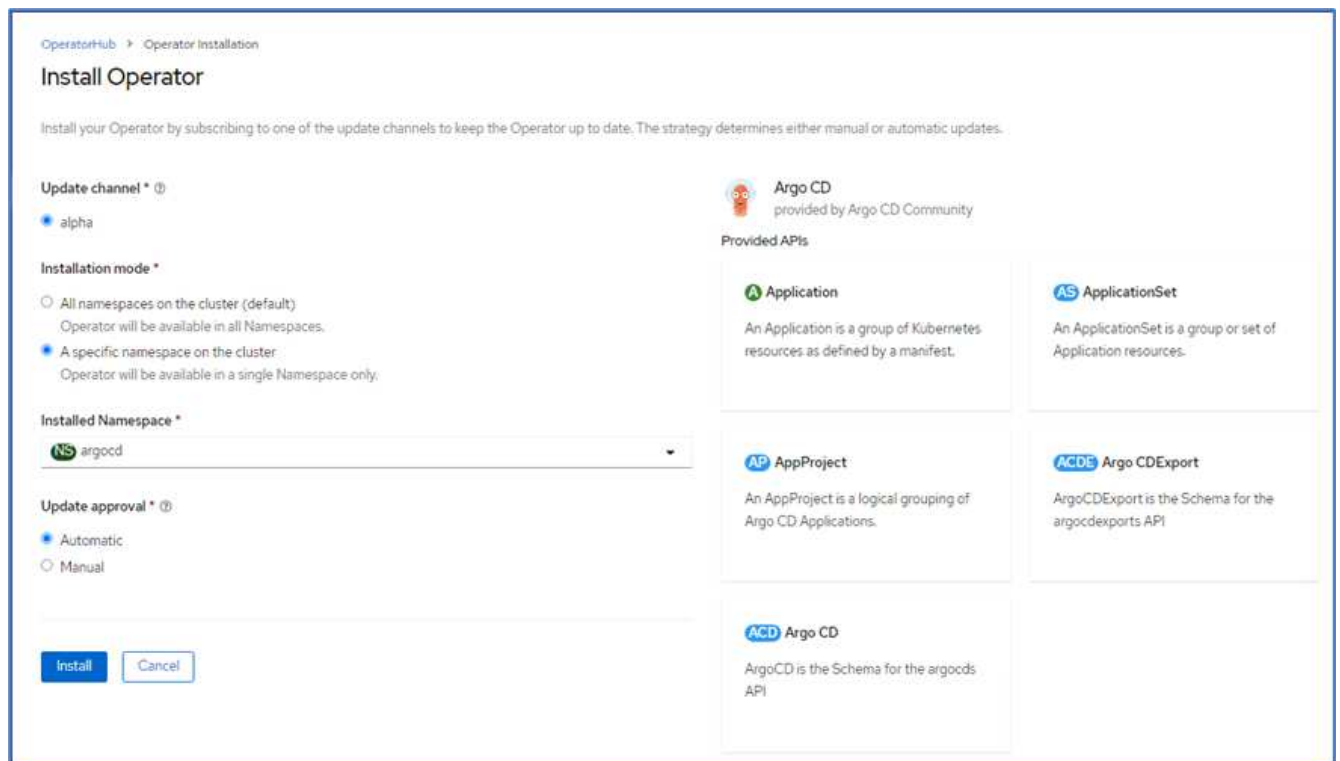
1. 登录到内部OpenShift集群并创建一个名为`argocd`的新项目。



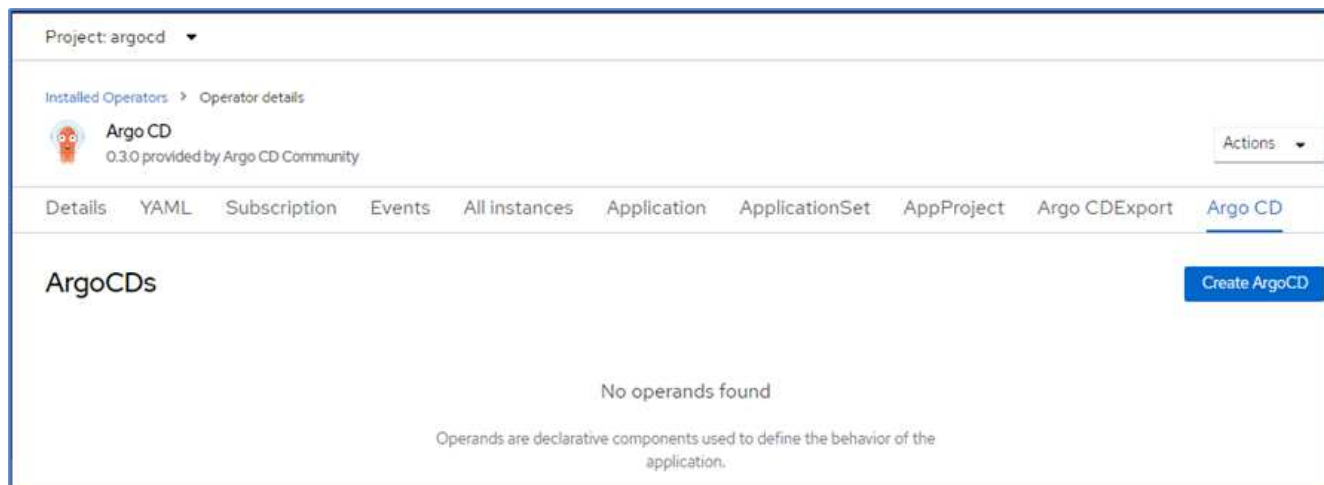
2. 在OperatorHub中、搜索`argocd`并选择Argo CD operator。



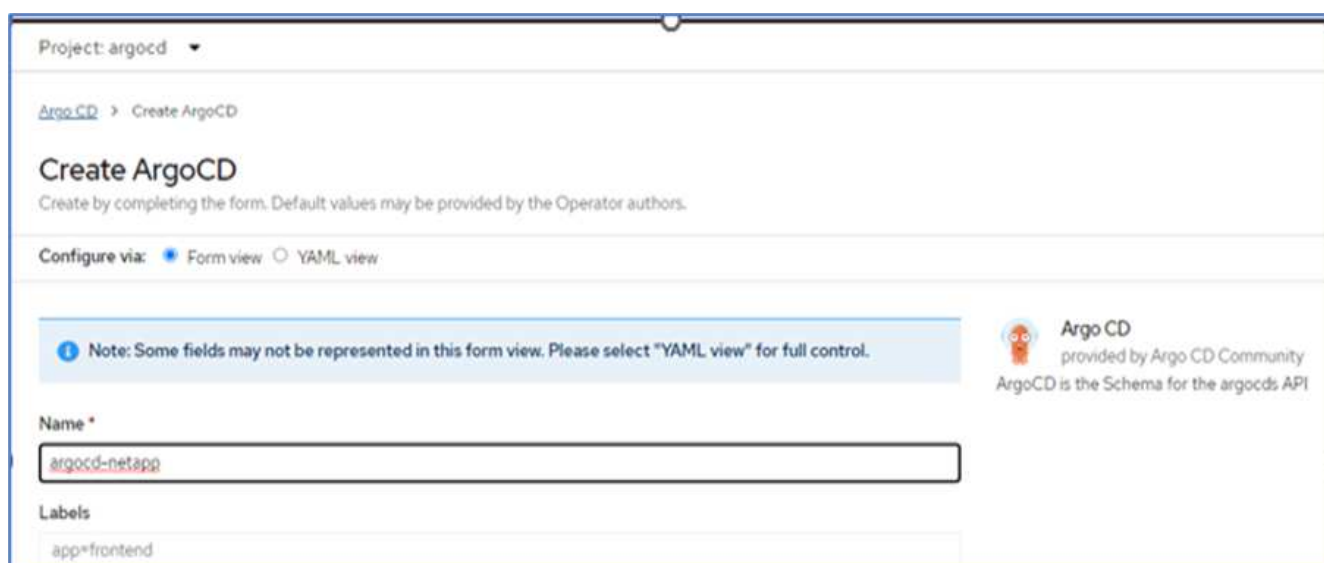
3. 在`argocd`命名空间中安装操作符。



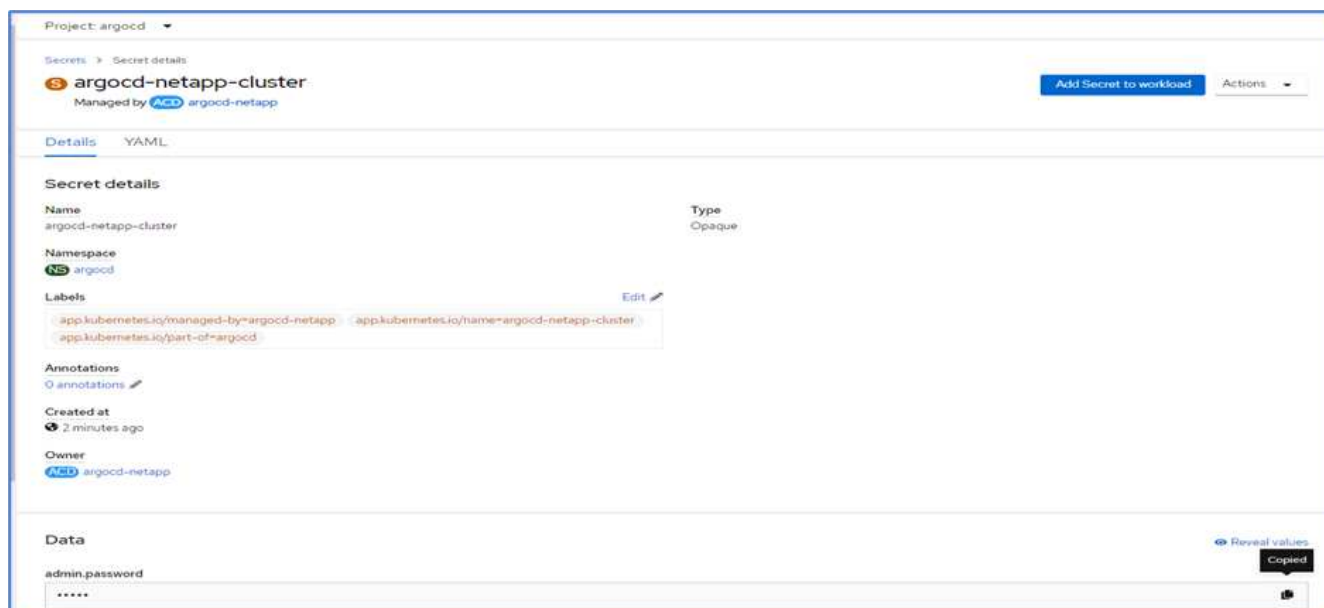
4. 转到运算符并单击创建ArgoCD。



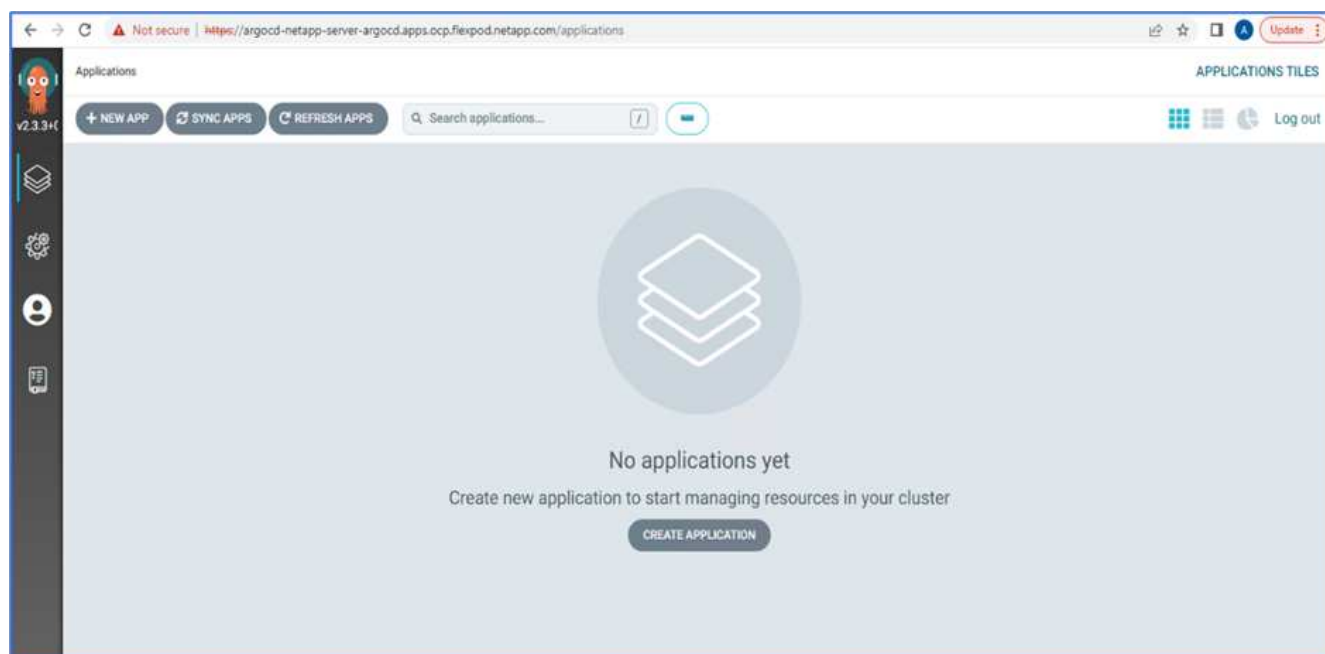
5. 要在`argocd`项目中部署Argo CD实例、请提供一个名称、然后单击创建。



6. 要登录到Argo CD、默认用户为admin、密码位于名为`argocd-netapp-cluster`的机密文件中。



7. 从侧面菜单中、选择路由>位置、然后单击`argocd` routes的URL。输入用户名和密码。



8. 通过CLI将内部OpenShift集群添加到Argo CD。

```

####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER          SERVER
*          default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
          default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added

```

9. 在ArgoCD UI中、单击新应用程序并输入有关应用程序名称和代码存储库的详细信息。

CREATE

CANCEL

EDIT AS YAML

GENERAL

Application Name

pricelist

Project

default

SYNC POLICY

Manual

SYNC OPTIONS

☐ SKIP SCHEMA VALIDATION

☒ AUTO-CREATE NAMESPACE

☐ PRUNE LAST

☐ APPLY OUT OF SYNC ONLY

☐ RESPECT IGNORE DIFFERENCES

PRUNE PROPAGATION POLICY: foreground

☐ REPLACE ⚠️

☐ RETRY

SOURCE

Repository URL

https://github.com/netapp-abhinav/demo/

GIT ▼

Revision

main

Branches ▼

Path

pricelists/

10. 输入要随命名空间一起部署应用程序的OpenShift集群。

DESTINATION

Cluster URL

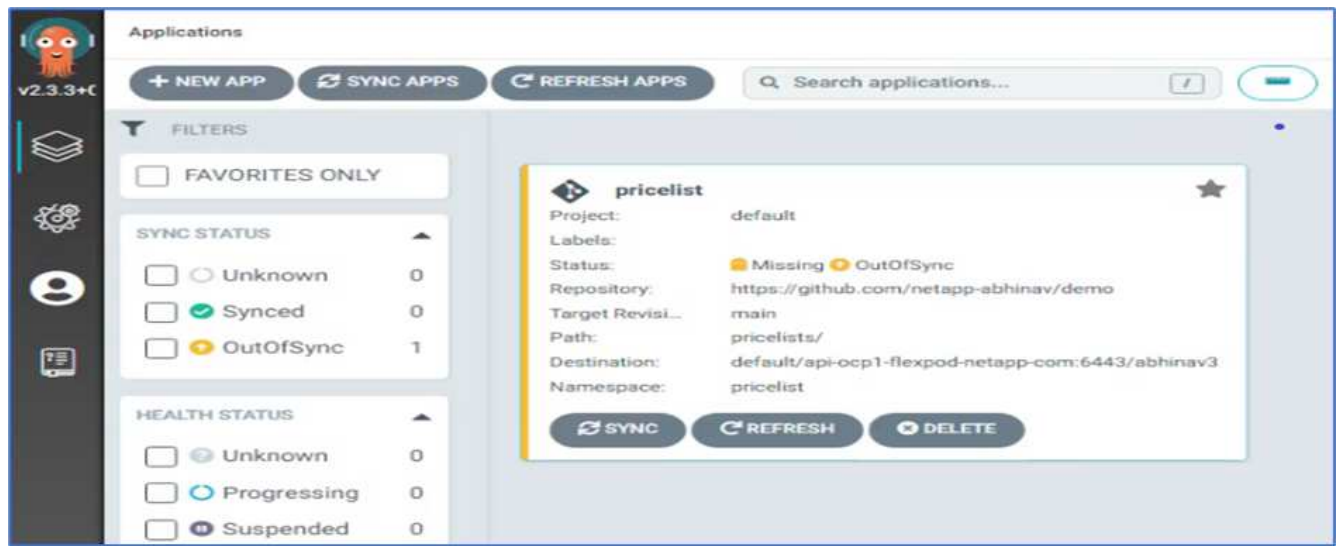
https://api.ocp1.flexpod.netapp.com:6443

URL ▼

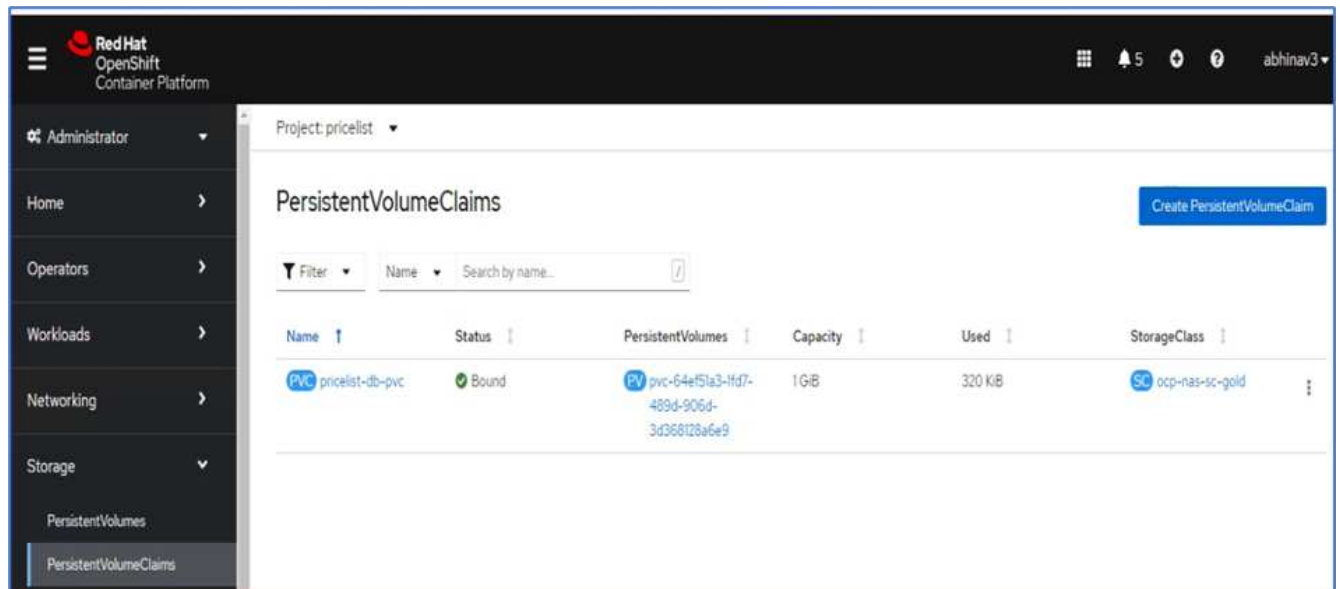
Namespace

pricelist

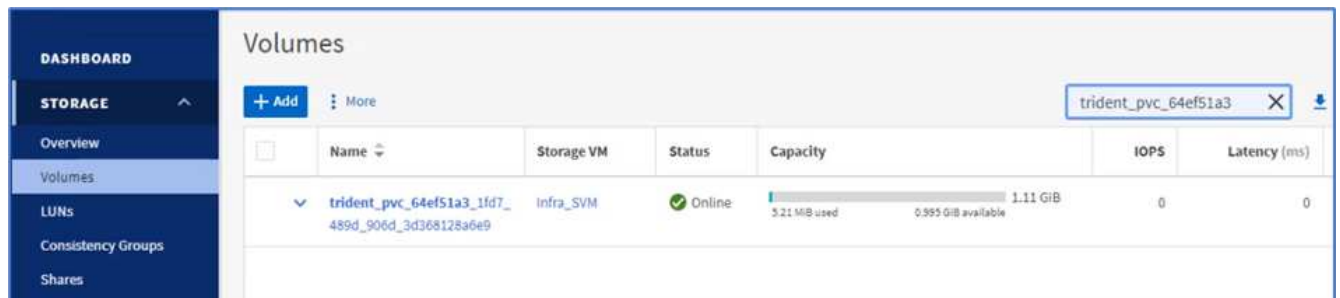
11. 要在内部OpenShift集群上部署此应用、请单击同步。



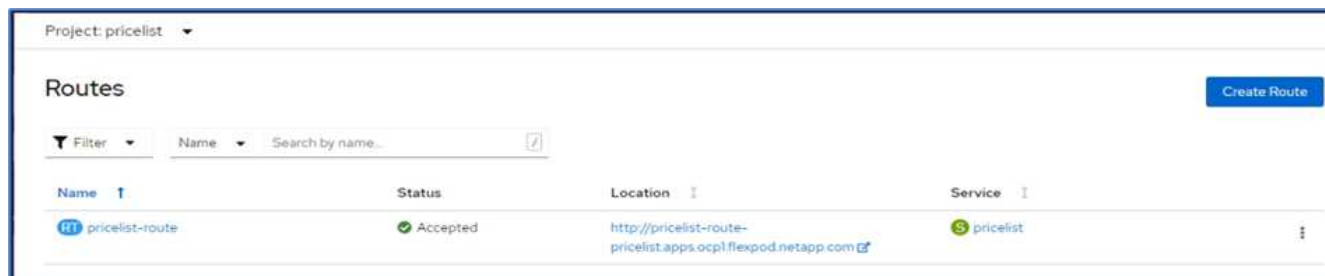
12. 在OpenShift容器平台控制台中、转至项目价目表、然后在存储下验证PVC的名称和大小。



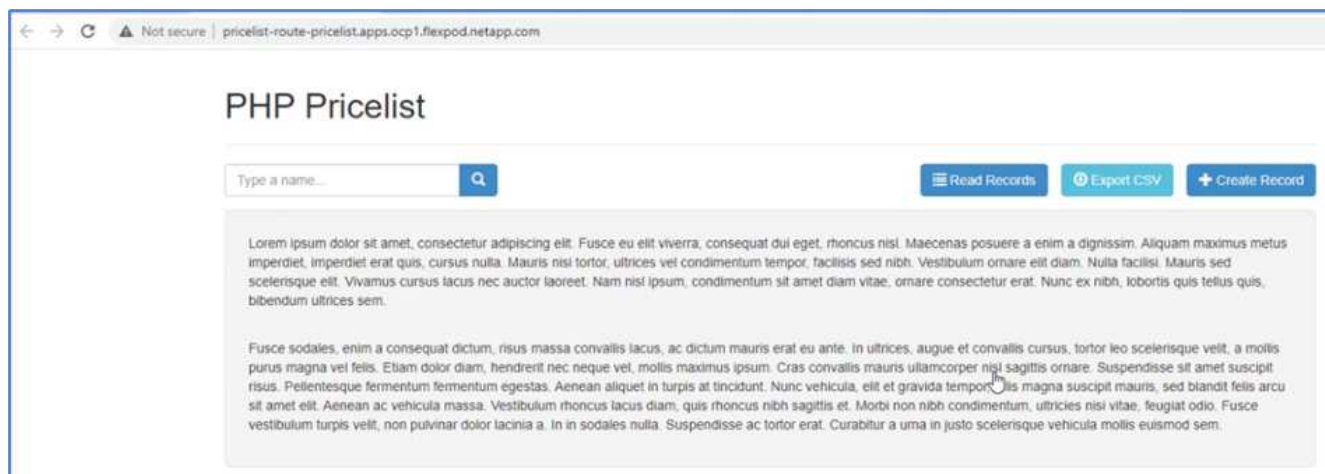
13. 登录到System Manager并验证PVC。



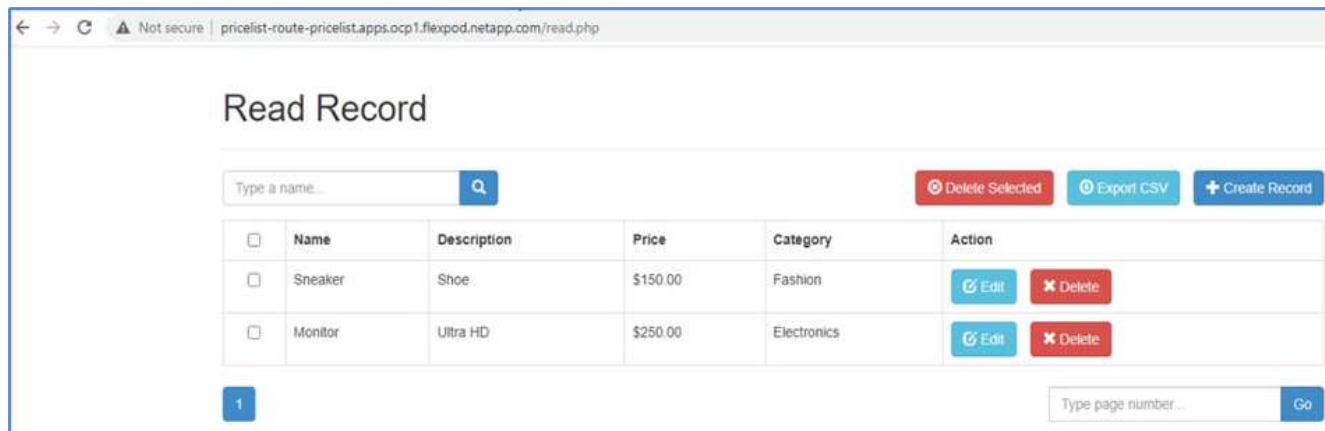
14. Pod运行后、从侧面菜单中选择Networking > routes、然后单击Location下的URL。



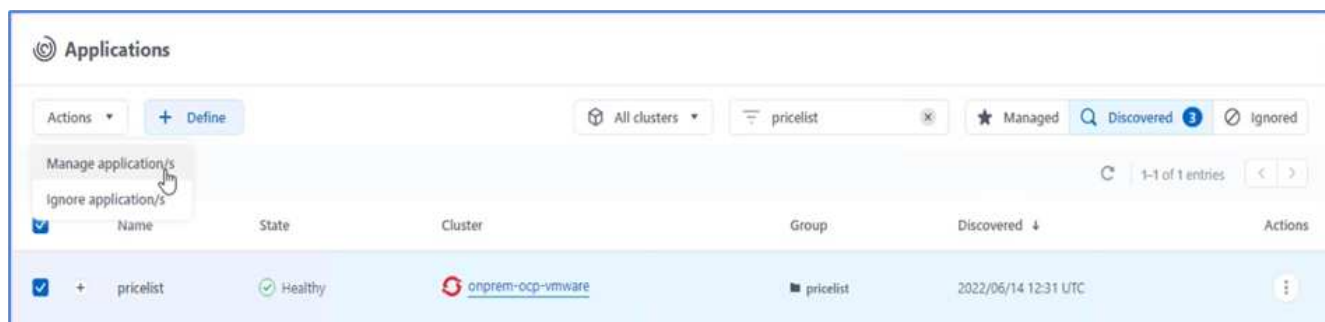
15. 此时将显示Pricelist应用程序主页。



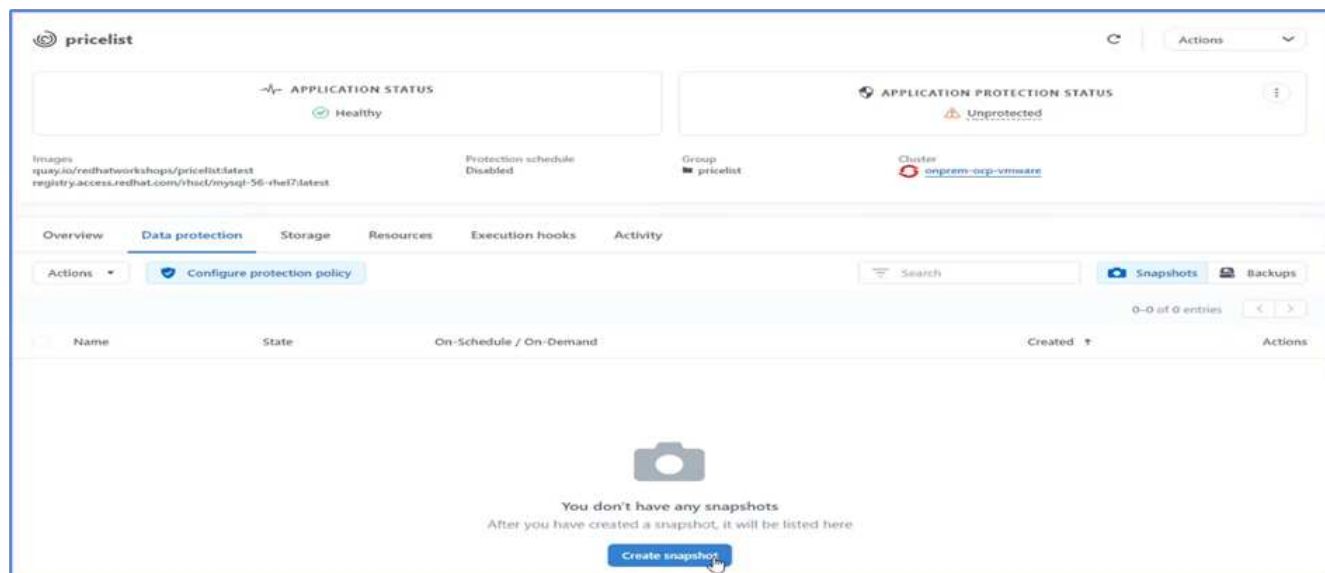
16. 在网页上创建一些记录。



17. 此应用程序会在Astra控制中心中发现。要管理此应用程序、请转到"应用程序">"已发现"、选择"价目表"应用程序、然后单击"操作"下的"管理应用程序"。

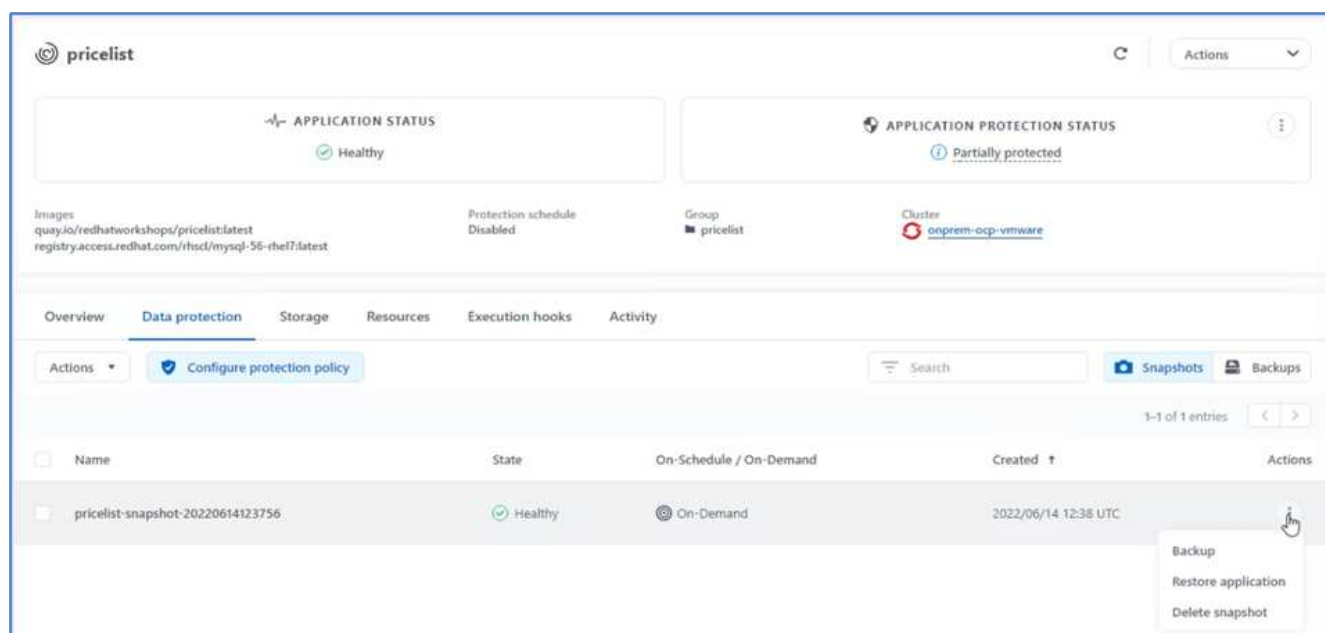


18. 单击Pricelist应用程序、然后选择Data Protection。此时、不应存在快照或备份。单击Create Snapshot以创建按需快照。



NetApp Astra控制中心既支持按需快照、也支持计划快照和备份。

19. 创建快照并使其运行状况良好后、使用该快照创建远程备份。此备份存储在S3存储分段中。



20. 选择AWS S3存储分段并启动备份操作。

Back up namespace application

STEP 1/2: DETAILS

✕

BACKUP DETAILS

Snapshot (optional)
pricelist-snapshot-20220614123756

Name
pricelist-backup-20220614123837

BACKUP DESTINATION

Bucket
acc-aws-bucket - AWS S3 bucket for ACC Available Default

OVERVIEW

Application backups
Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

- Namespace application pricelist
- Namespace pricelist
- Cluster onprem-ocp-vmware

Cancel

Next

21. 备份操作应在AWS S3存储分段中创建一个包含多个对象的文件夹。

Amazon S3 > Buckets > acc-aws-bucket > 04330ccb-f13e-4eef-8f52-755f56aa3a3f/

Copy S3 URI

Objects

Properties

Objects (5)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

↻

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

☐	Name	Type	Last modified	Size	Storage class
☐	config	-	June 14, 2022, 05:39:19 (UTC-07:00)	155.0 B	Standard
☐	data/	Folder	-	-	-
☐	index/	Folder	-	-	-
☐	keys/	Folder	-	-	-
☐	snapshots/	Folder	-	-	-

22. 远程备份完成后、通过停止托管PV后备卷的Storage Virtual Machine (SVM)来模拟内部灾难。

ONTAP System Manager

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Volumes

LUNs

Consistency Groups

Storage VMs

+ Add

Infra

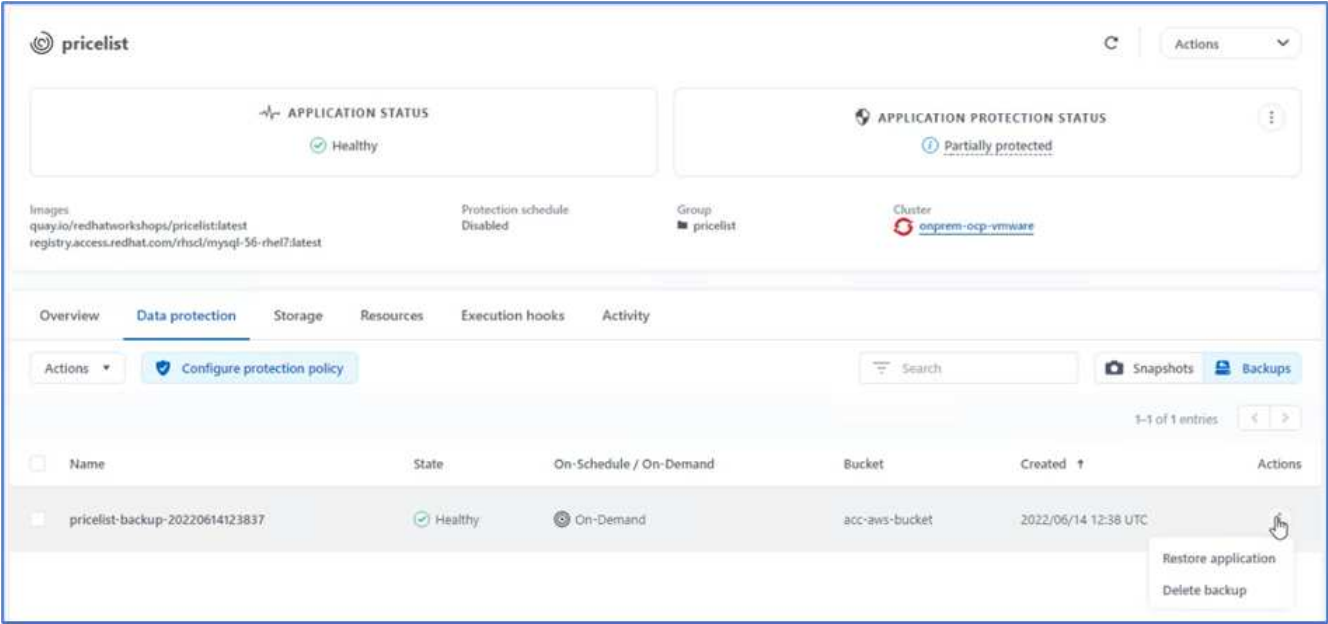
☐	Name	State	Subtype	Configured Protocols	IPspace
☐	Infra_SVM	stopped	default		Default

23. 刷新网页以确认中断。此网页不可用。

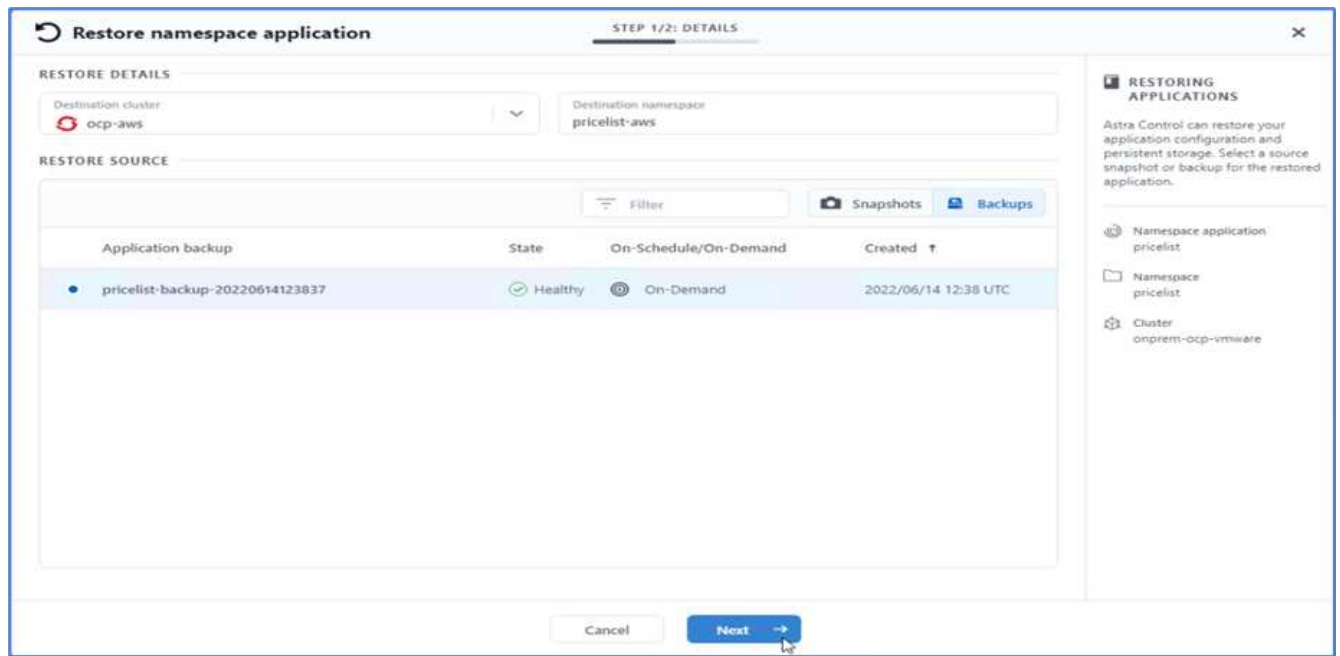


正如预期、网站已关闭、因此、让我们使用Astra快速从远程备份恢复应用程序、并将其恢复到AWS中运行的OpenShift集群。

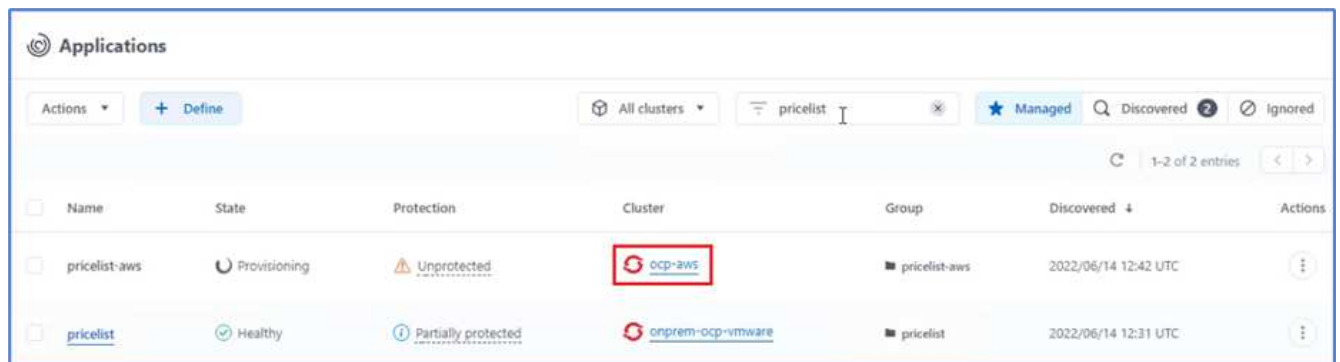
24. 在Astra Control Center中、单击Pricelist应用程序、然后选择Data Protection > Backups。选择备份、然后单击操作下的还原应用程序。



25. 选择`OCP-AWS`作为目标集群、并为命名空间提供一个名称。单击按需备份、下一步、然后单击还原。



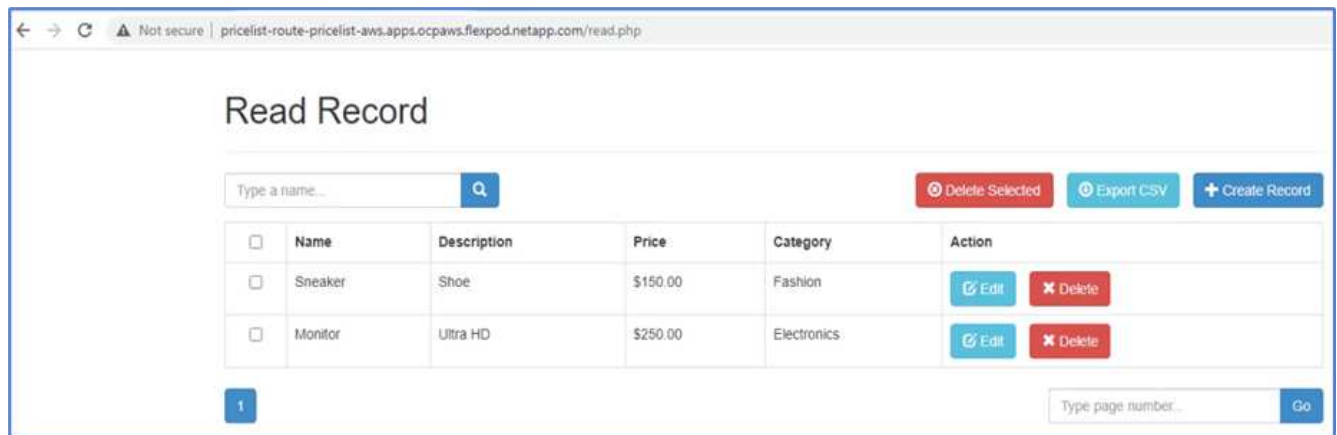
26. 在AWS中运行的OpenShift集群上会显示一个名为`pricelist-app`的新应用程序。



27. 在OpenShift Web控制台中验证相同的。



28. 运行`pricelist-AWS`项目下的所有Pod后、转到routes并单击URL以启动网页。



此过程将验证价格表应用程序是否已成功还原、以及在Astra控制中心的帮助下、在AWS上无缝运行的OpenShift集群上是否保持了数据完整性。

利用**Snapshot**副本和**DevTest**应用程序移动性保护数据

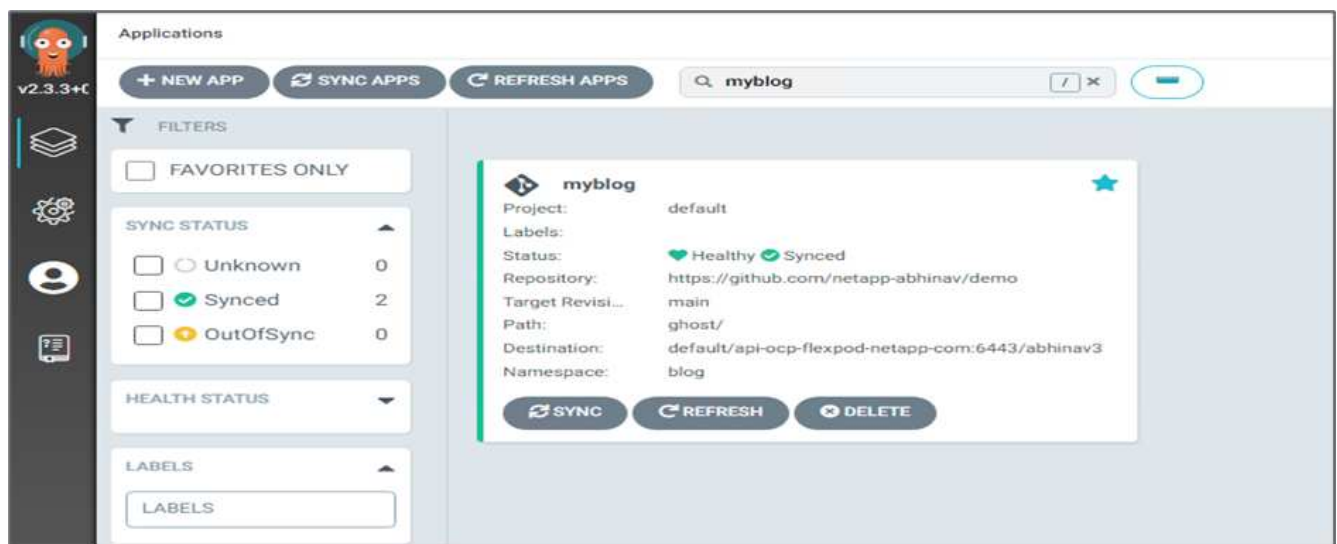
此用例由两部分组成、如下各节所述。

第1部分

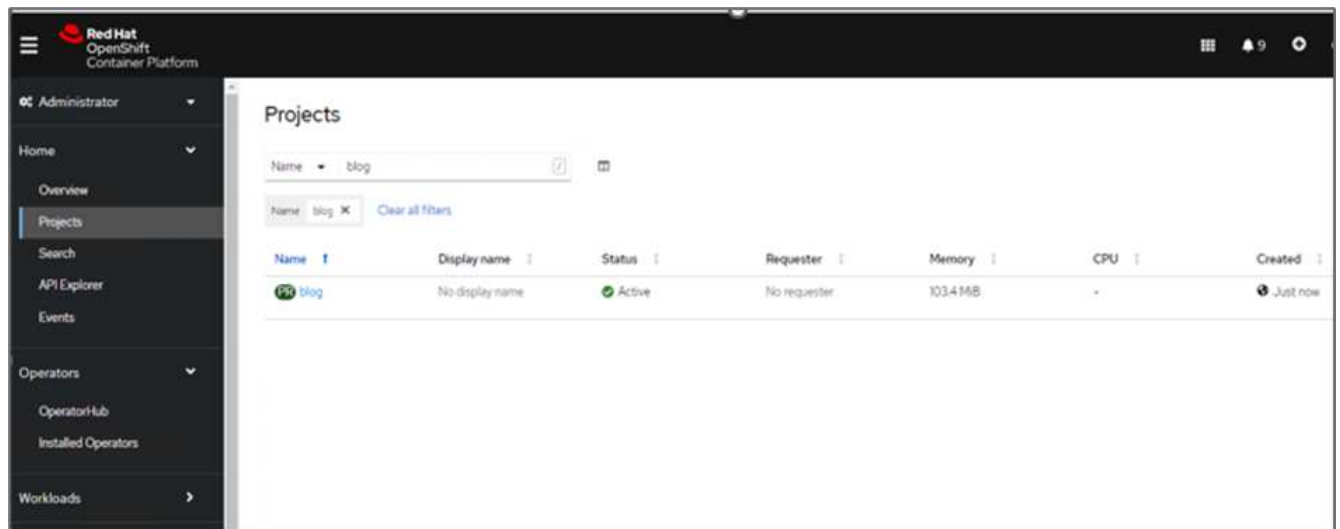
借助Astra控制中心、您可以创建应用程序感知型快照以实现本地数据保护。如果意外删除或损坏数据、您可以使用先前记录的快照将应用程序和关联数据还原到已知正常状态。

在这种情况下、开发和测试(DevTest)团队部署了一个示例有状态应用程序(博客站点)、该应用程序是一个Ghost博客应用程序、并添加了一些内容、然后将该应用程序升级到最新版本。Ghost应用程序对数据库使用SQLite。在升级应用程序之前、可以使用Astra控制中心创建一个快照(按需)来进行数据保护。详细步骤如下：

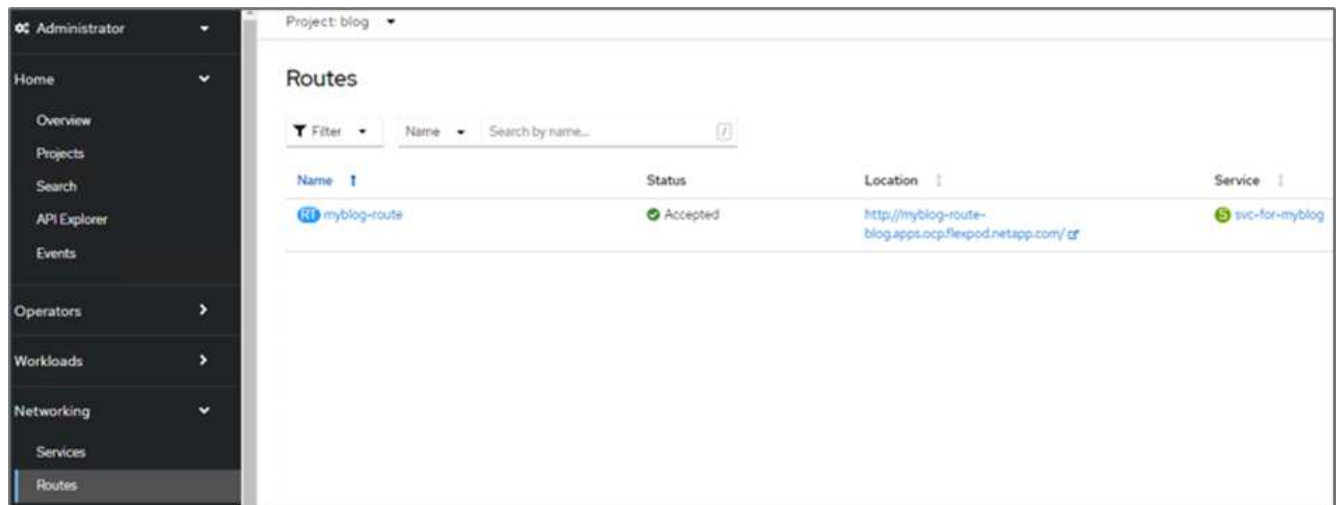
1. 部署示例博客应用程序并从ArgoCD进行同步。



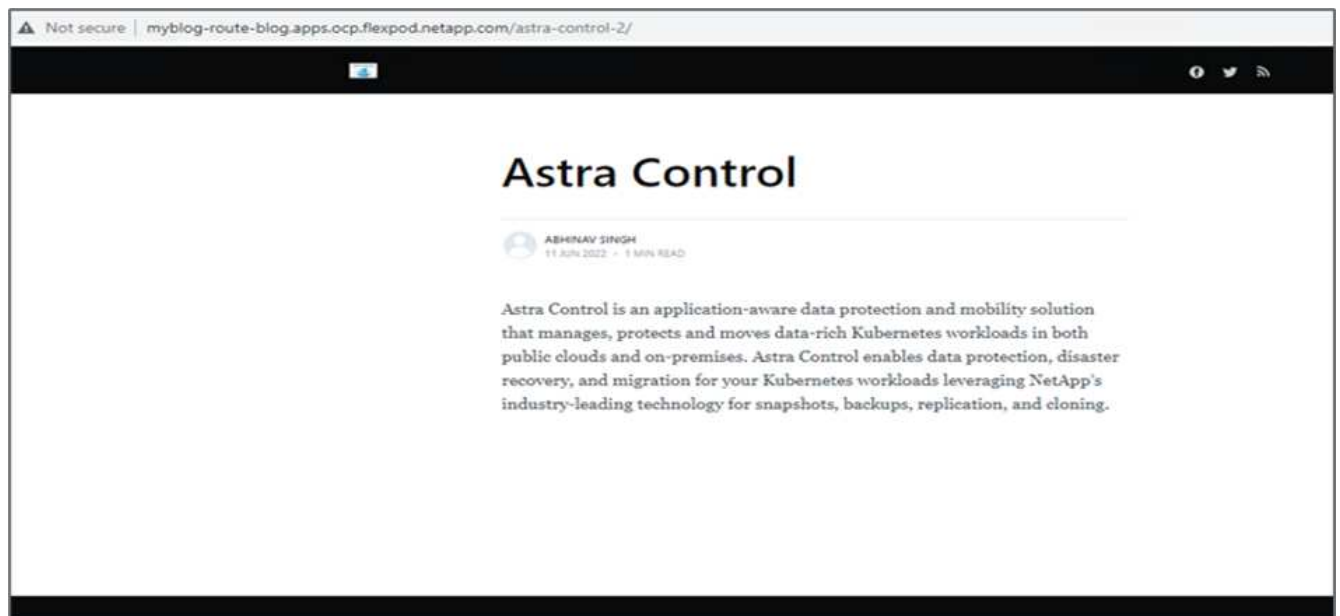
2. 登录到第一个OpenShift集群、转到Project、然后在搜索栏中输入Billog。



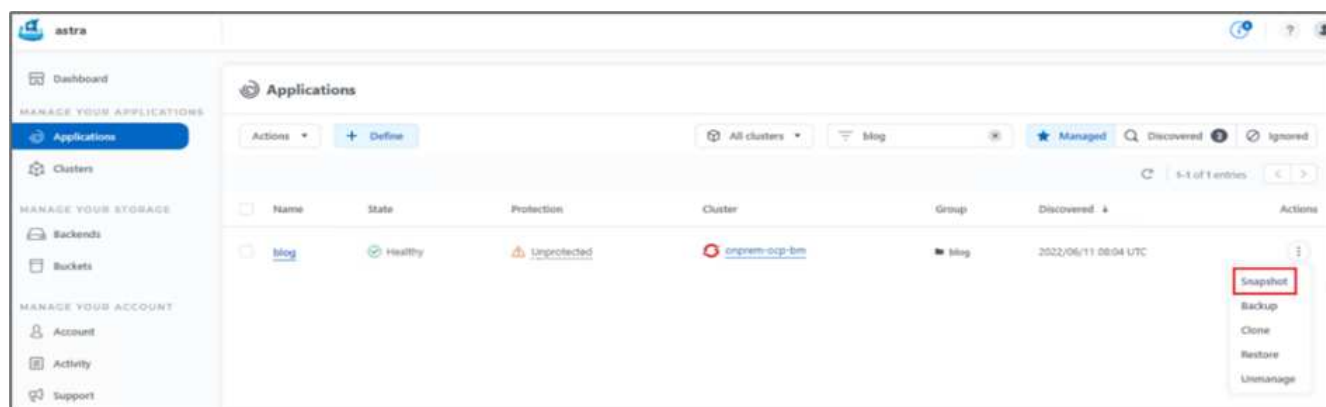
3. 从侧面菜单中、选择网络>路由、然后单击URL。



4. 此时将显示博客主页。向博客站点添加一些内容并发布。

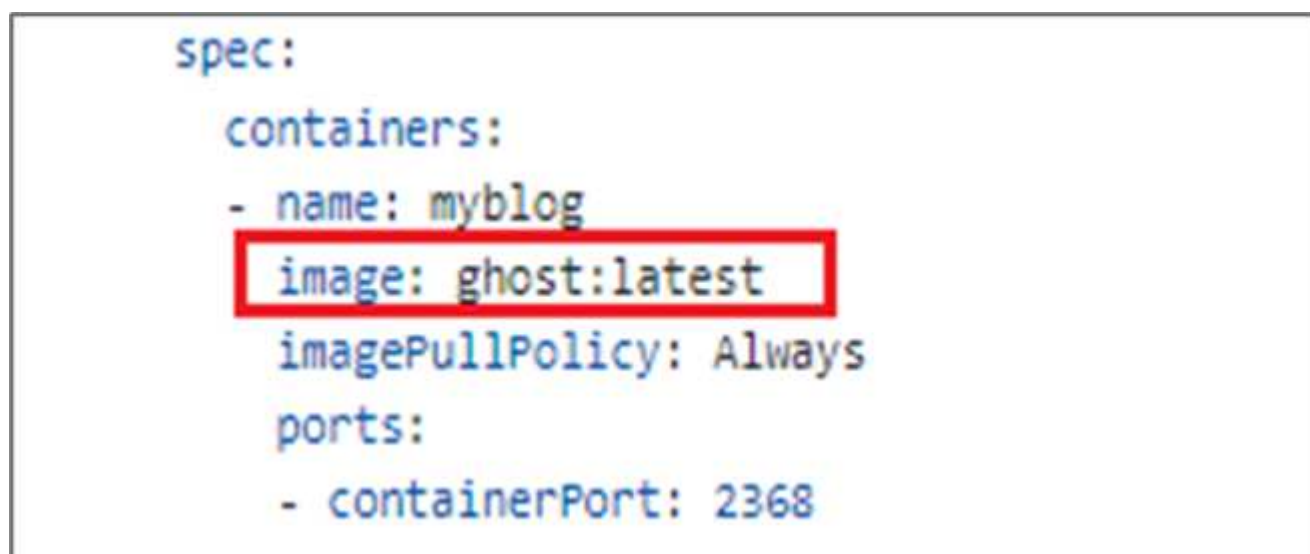


5. 转到Astra控制中心。首先从"已发现"选项卡管理应用程序、然后创建Snapshot副本。



您还可以通过按定义的计划创建快照、备份或同时创建这两者来保护应用程序。有关详细信息，请参见 ["通过快照和备份保护应用程序"](#)。

6. 成功创建按需快照后、将应用程序升级到最新版本。当前映像版本为`Ghost: 3.6-alpine`、目标版本为`Ghost: Latest`。要升级此应用程序、请直接更改Git存储库并将其同步到Argo CD。



7. 您可以看到、由于博客站点关闭以及整个应用程序损坏、不支持直接升级到最新版本。

Project: blog ▾

Pods ▸ Pod details

myblog-5f899f7b76-zv7rq CrashLoopBackOff

Details Metrics YAML Environment **Logs** Events Terminal

Log stream ended. myblog ▾ Current log ▾

```
34 lines
[2022-06-11 12:54:05] +[36mINFO+[39m Creating database backup
[2022-06-11 12:54:05] +[36mINFO+[39m Database backup written to: /var/lib/ghost/content/data/astra.ghost.2022-06-11-12-54-05.json
[2022-06-11 12:54:05] +[36mINFO+[39m Running migrations.
[2022-06-11 12:54:06] +[36mINFO+[39m Rolling back: Unable to run migrations.
[2022-06-11 12:54:06] +[36mINFO+[39m Rollback was successful.
[2022-06-11 12:54:06] +[31mERROR+[39m Unable to run migrations
+[[31m
+[[31mUnable to run migrations+[[39m

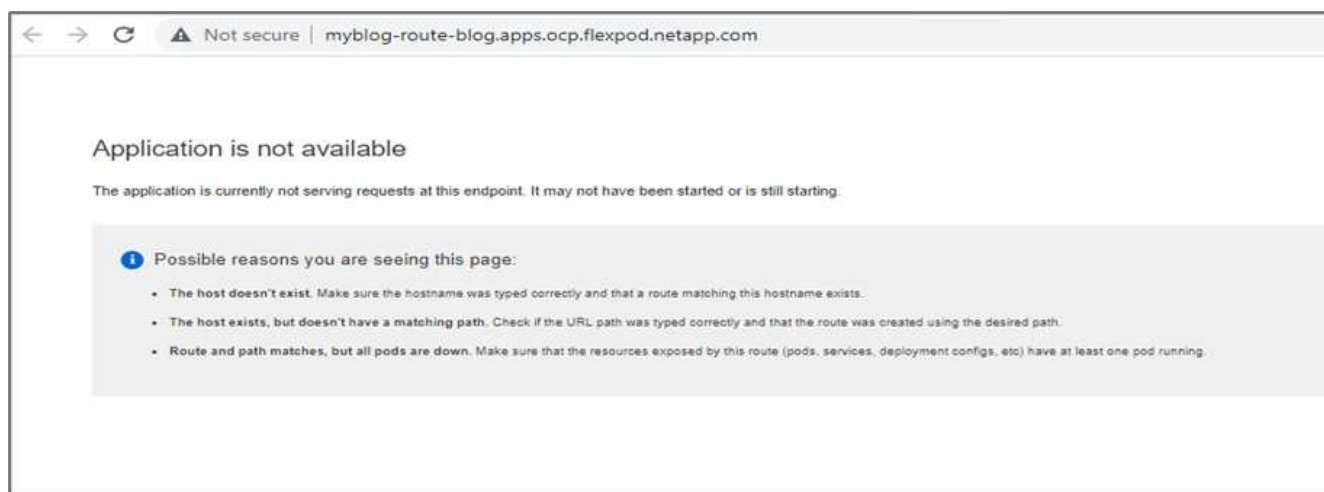
+[[37mYou must be on the latest v3.x to update across major versions - https://ghost.org/docs/update/" +[[39m
+[[33mRun 'ghost update v3' to get the latest v3.x version, then run 'ghost update' to get to the latest." +[[39m

+[[1m+[[37mError ID: +[[39m+[[22m
+[[90m93b99ce0-e985-11ec-9301-7d29b2c73999+[[39m

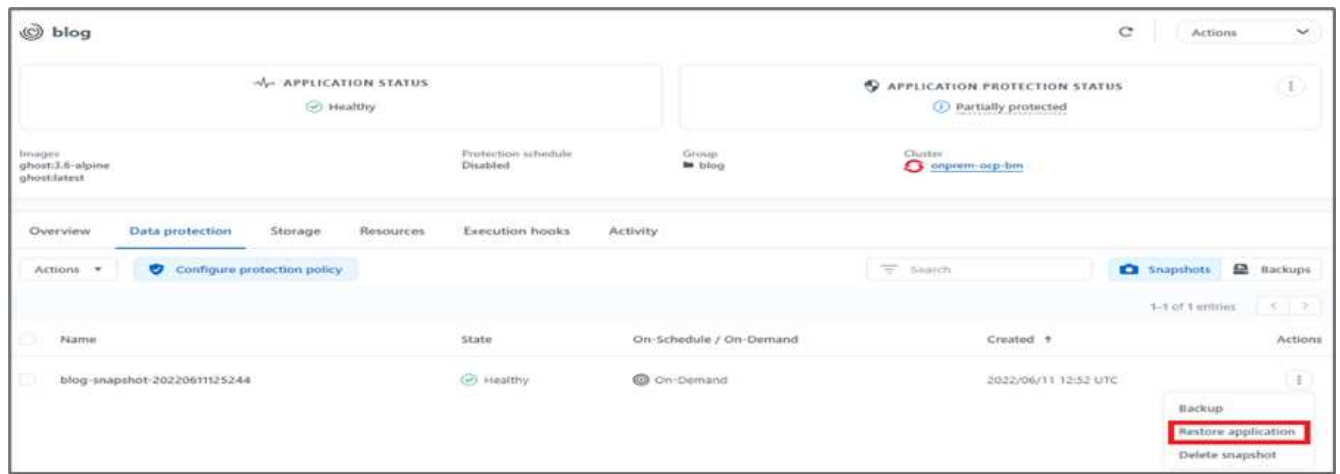
+[[90m-----+[[39m

+[[90mInternalServerError: Unable to run migrations
at /var/lib/ghost/versions/5.2.2/node_modules/knex-migrator/lib/index.js:1032:19
at up (/var/lib/ghost/versions/5.2.2/core/server/data/migrations/utils/migrations.js:118:19)
at Object.up (/var/lib/ghost/versions/5.2.2/core/server/data/migrations/utils/migrations.js:54:19)
at /var/lib/ghost/versions/5.2.2/node_modules/knex-migrator/lib/index.js:982:33
at /var/lib/ghost/versions/5.2.2/node_modules/knex/lib/execution/transaction.js:221:22+[[39m
+[[39m
[2022-06-11 12:54:06] +[[35mWARN+[[39m Ghost is shutting down
[2022-06-11 12:54:06] +[[35mWARN+[[39m Ghost has shut down
[2022-06-11 12:54:06] +[[35mWARN+[[39m Your site is now offline
[2022-06-11 12:54:06] +[[35mWARN+[[39m Ghost was running for a few seconds
```

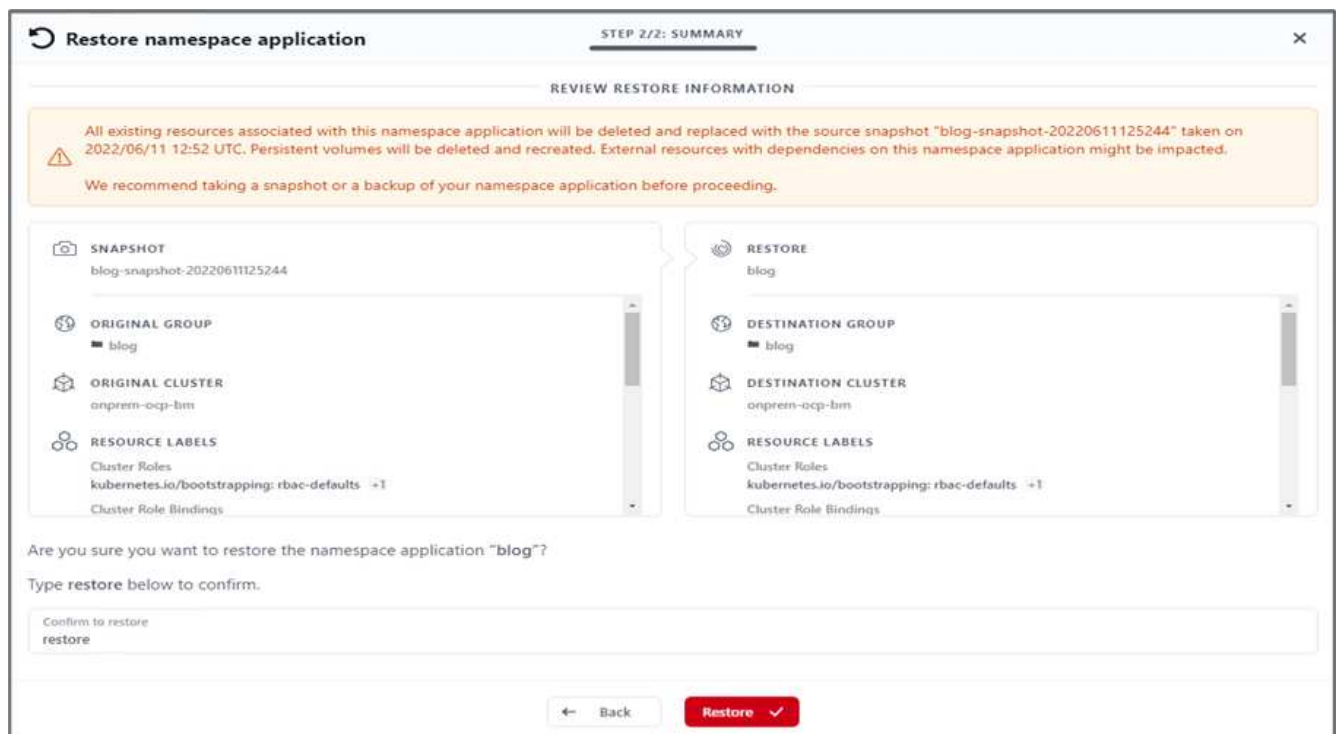
8. 要确认博客站点不可用、请刷新URL。



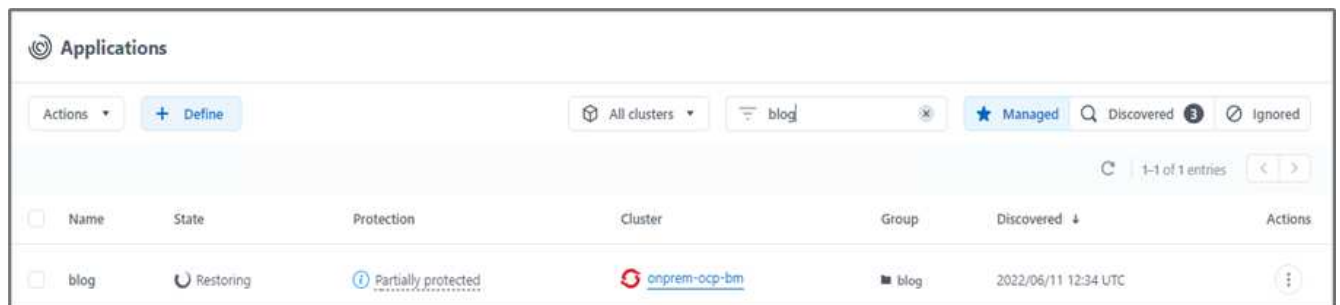
9. 从快照还原应用程序。



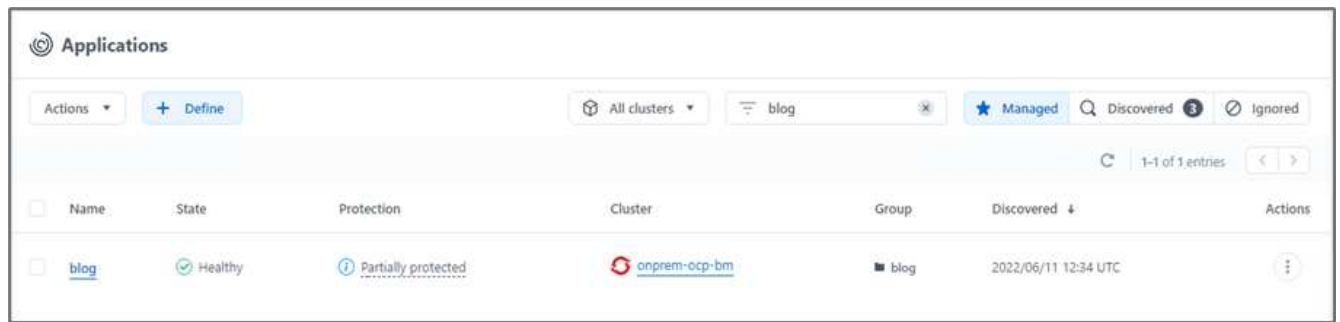
10. 此应用程序将在同一个OpenShift集群上还原。



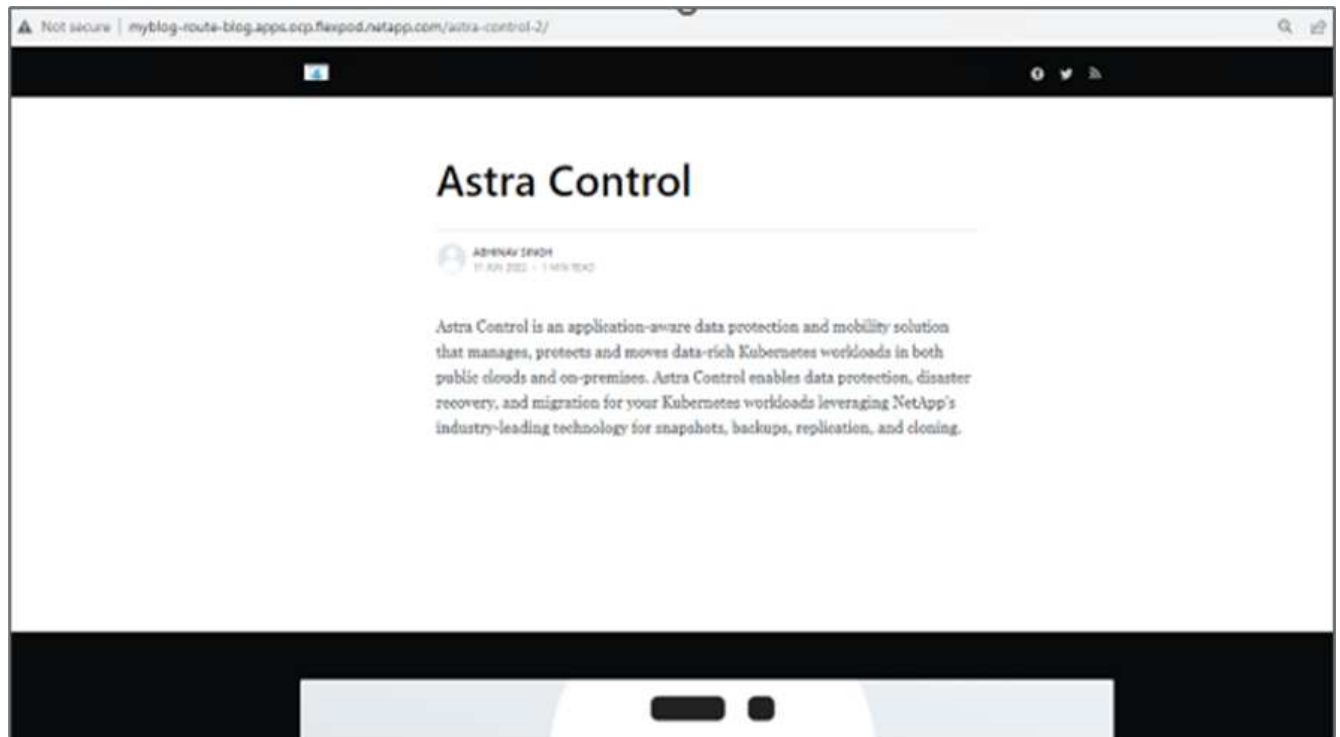
11. 应用程序还原过程将立即启动。



12. 只需几分钟、即可从可用快照成功还原应用程序。



13. 要查看此网页是否可用、请刷新此URL。



在Astra控制中心的帮助下、DevTest团队可以使用快照成功恢复博客站点应用程序及其关联数据。

第2部分

借助Astra控制中心、您可以将整个应用程序及其数据从一个Kubernetes集群移动到另一个集群、无论这些集群位于何处(内部或云中)。

1. DevTest团队最初会先将应用程序升级到受支持的版本(ghost-4.6. alpine)、然后再升级到最终版本(ghost-latest)以使其可投入生产。然后、他们会将克隆的应用程序升级到在其他FlexPod 系统上运行的生产OpenShift集群。
2. 此时、该应用程序将升级到最新版本、并可克隆到生产集群。

Project: blog ▾

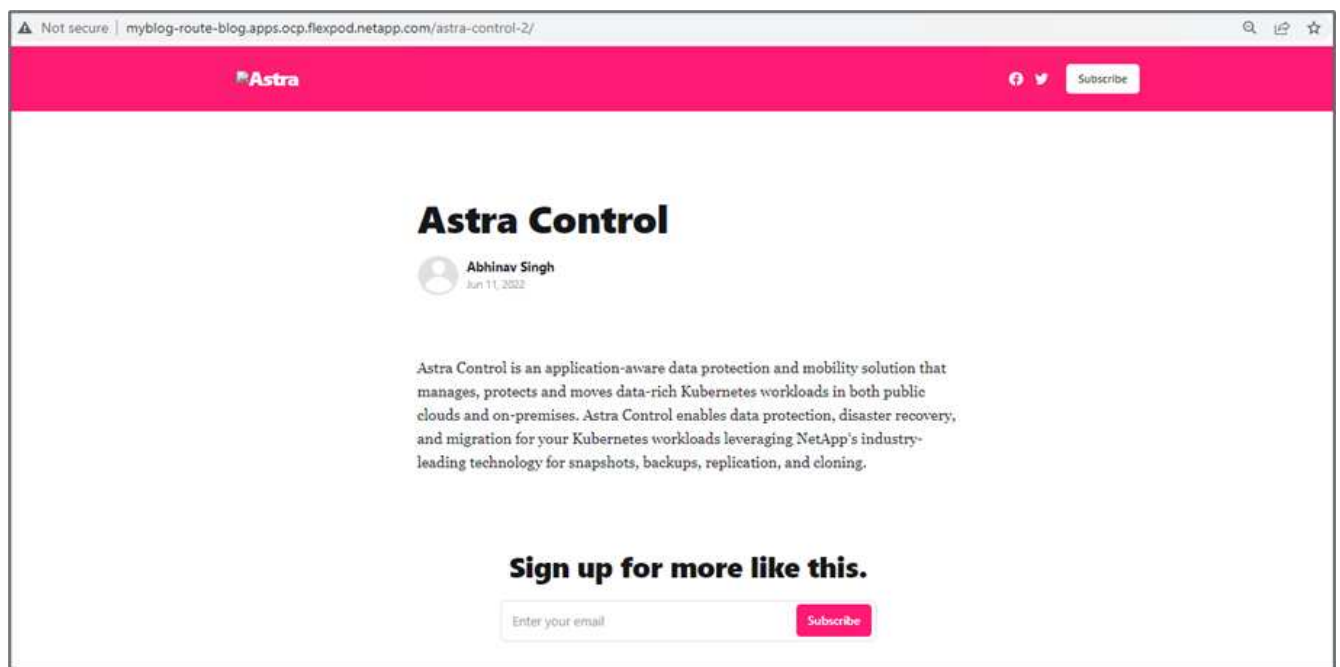
Pods > Pod details

myblog-55ffd9f658-tkbfq Running

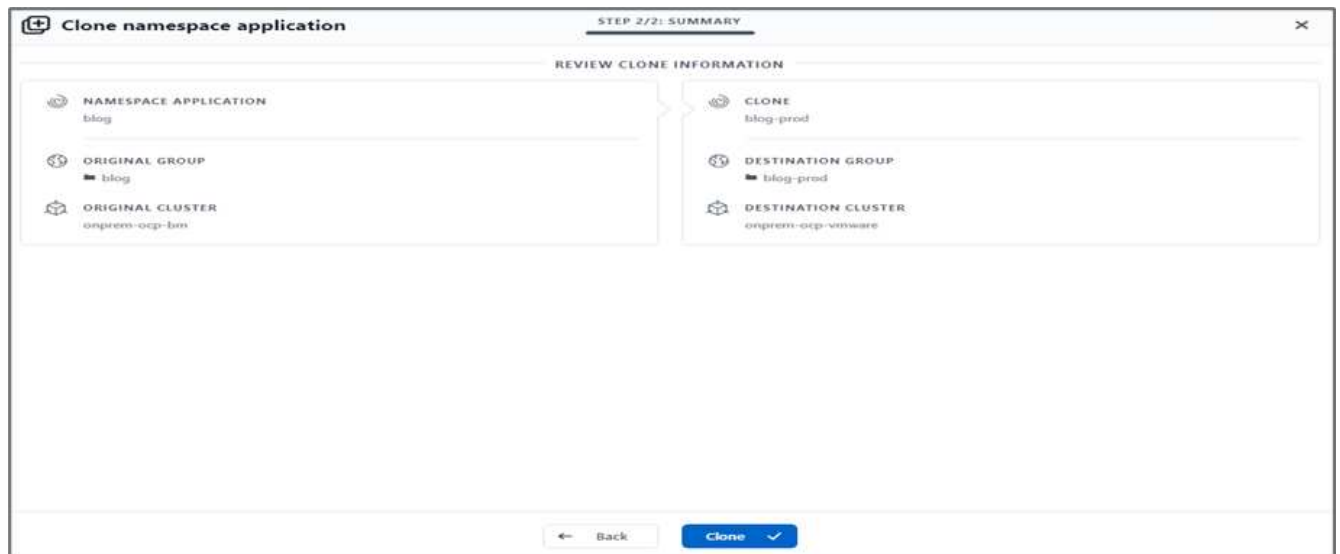
Details Metrics YAML Environment Logs Events Terminal

```
180 ports:
181   - containerPort: 2368
182     protocol: TCP
183   imagePullPolicy: Always
184   volumeMounts:
185     - name: content
186       mountPath: /var/lib/ghost/content
187     - name: kube-api-access-t2sdz
188       readOnly: true
189       mountPath: /var/run/secrets/kubernetes.io/serviceaccount
190     terminationMessagePolicy: File
191     image: 'ghost:latest'
192   serviceAccount: default
193   volumes:
194     - name: content
195       persistentVolumeClaim:
196         claimName: blog-content
```

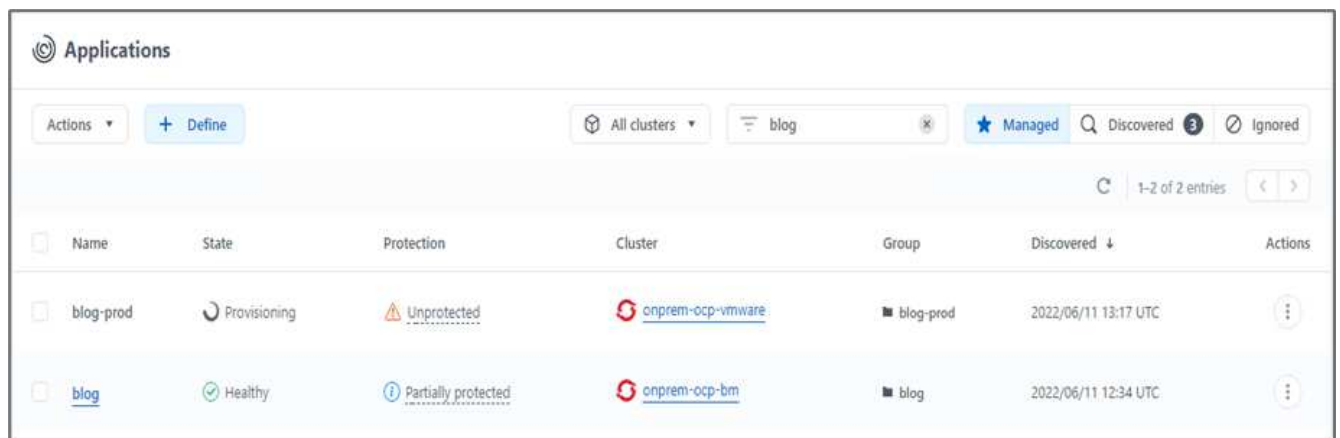
3. 要验证新主题、请刷新博客站点。



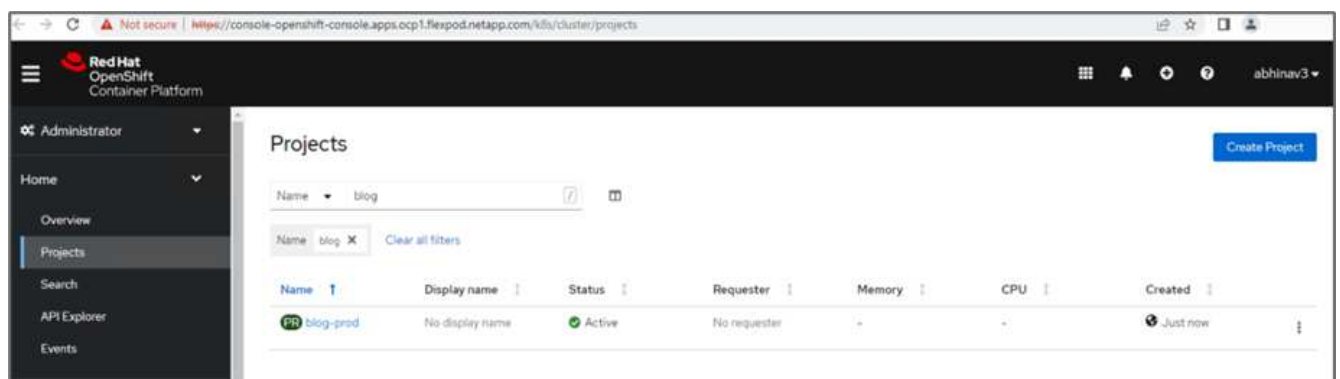
4. 从Astra控制中心、将应用程序克隆到在VMware vSphere上运行的另一个生产OpenShift集群。



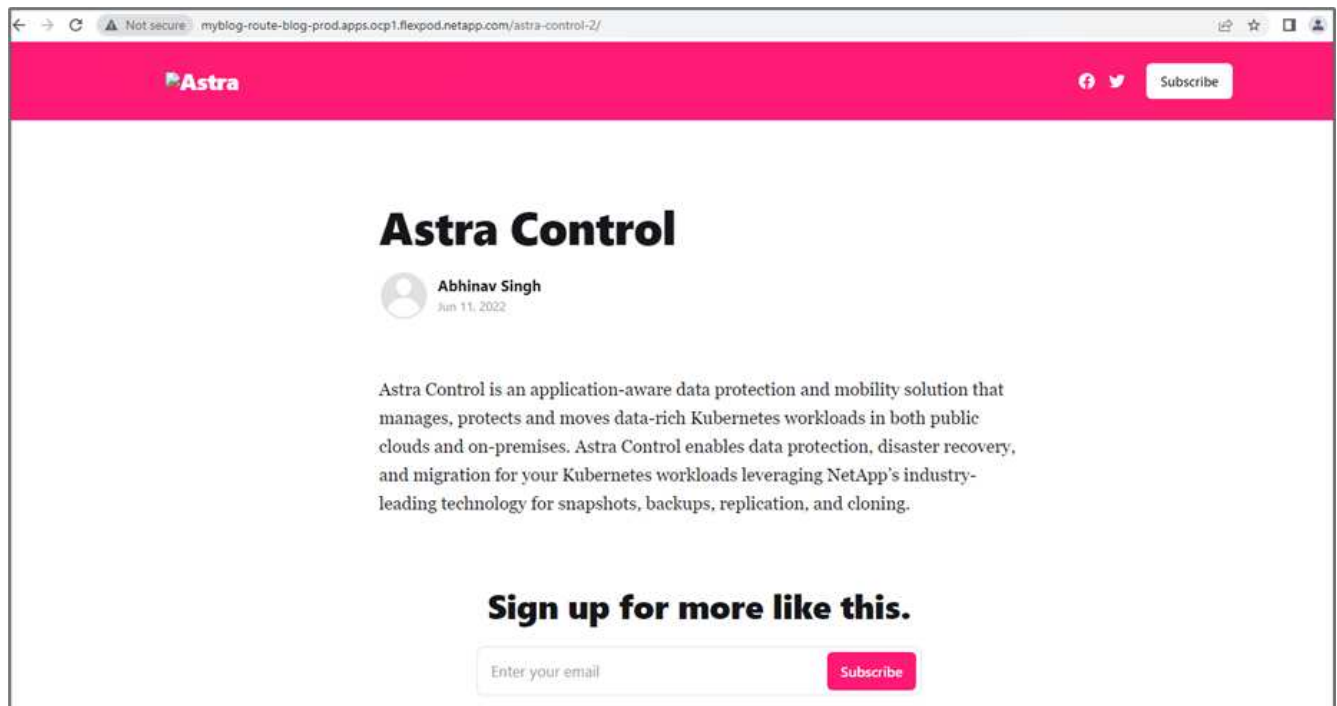
现在、生产OpenShift集群中会配置一个新的应用程序克隆。



5. 登录到生产OpenShift集群并搜索项目博客。



6. 从侧面菜单中、选择Networking > routes、然后单击Location下的URL。此时将显示与此内容相同的主页。



Astra控制中心解决方案 验证到此结束。现在、无论Kubernetes集群位于何处、您都可以将整个应用程序及其数据从一个Kubernetes集群克隆到另一个Kubernetes集群。

"接下来：总结。"

结论

"先前：使用远程备份恢复应用程序。"

在此解决方案 中、我们使用NetApp Astra产品组合为在FlexPod 和AWS上运行的容器化应用程序实施了保护计划。NetApp Astra控制中心和Astra Trident以及Cloud Volumes ONTAP、Red Hat OpenShift和FlexPod 基础架构构成了此解决方案 的核心组件。

我们展示了通过捕获快照保护应用程序的能力、并执行完整备份来在云和内部环境中运行的不同K8s集群之间还原应用程序。

此外、我们还演示了如何跨K8s集群克隆应用程序、从而使客户能够将其应用程序迁移到所需位置的所选K8s集群。

FlexPod 不断发展、客户可以利用它来实现应用程序和业务交付流程的现代化。借助此解决方案、FlexPod 客户可以放心地为云原生应用程序构建BCDr计划、并将公有 云作为一个位置来实施瞬时或全时灾难恢复计划、同时保持较低的解决方案 成本。

使用Astra Control、您可以将整个应用程序及其数据从一个Kubernetes集群移动到另一个集群、无论这些集群位于何处。它还可以帮助您加快云原生应用程序的部署、操作和保护速度。

故障排除

有关故障排除指导、请参见 ["联机文档"](#)。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- FlexPod 主页

["https://www.flexpod.com"](https://www.flexpod.com)

- 适用于FlexPod 的Cisco验证设计和部署指南

["https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"](https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html)

- 使用Ansible为VMware部署基础架构代码FlexPod

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment)

- 使用Ansible将基础架构作为Red Hat OpenShift裸机的代码进行FlexPod 部署

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html)

- Cisco UCS 硬件和软件互操作性工具

["http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"](http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- Cisco Intersight数据表

["https://intersight.com/help/saas/home"](https://intersight.com/help/saas/home)

- NetApp Astra文档

["https://docs.netapp.com/us-en/astra-control-center/index.html"](https://docs.netapp.com/us-en/astra-control-center/index.html)

- NetApp Astra 控制中心

["https://docs.netapp.com/us-en/astra-control-center/index.html"](https://docs.netapp.com/us-en/astra-control-center/index.html)

- NetApp Astra Trident

["https://docs.netapp.com/us-en/trident/index.html"](https://docs.netapp.com/us-en/trident/index.html)

- NetApp Cloud Manager

["https://docs.netapp.com/us-en/occm/concept_overview.html"](https://docs.netapp.com/us-en/occm/concept_overview.html)

- NetApp Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"](https://docs.netapp.com/us-en/occm/task_getting_started_aws.html)

- Red Hat OpenShift

["https://www.openshift.com/"](https://www.openshift.com/)

- NetApp 互操作性表工具

["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2022年7月	针对ACC22.04.0的版本。

适用于 FlexPod 的 NetApp Cloud Insights

TR-4868：《适用于 FlexPod 的 NetApp Cloud Insights》

NetApp 公司 Alan Cowles



与以下合作伙伴：

本技术报告详细介绍的解决方案是 NetApp Cloud Insights 服务的配置，用于监控运行 NetApp ONTAP 的 NetApp AFF A800 存储系统，该存储系统是作为 FlexPod Datacenter 解决方案的一部分部署的。

客户价值

此处详细介绍的解决方案为有意在混合云环境中全面监控解决方案的客户提供了价值，其中 ONTAP 作为主存储系统进行部署。其中包括使用 NetApp AFF 和 FAS 存储系统的 FlexPod 环境。

用例

此解决方案适用场景的使用情形如下：

- 希望监控作为 FlexPod 解决方案一部分部署的 ONTAP 存储系统中的各种资源和利用率的组织。
- 希望对使用 AFF 或 FAS 系统的 FlexPod 解决方案中发生的问题进行故障排除并缩短解决时间的组织。
- 对成本优化预测感兴趣的组织，包括自定义信息板，用于提供有关资源浪费的详细信息，以及在包括 ONTAP 在内的 FlexPod 环境中可以节省哪些成本。

目标受众

解决方案的目标受众包括以下组：

- IT 主管以及关注成本优化和业务连续性的人员。
- 对数据中心或混合云设计和管理感兴趣的解决方案架构师。
- 负责故障排除和意外事件解决的技术支持工程师。

您可以对 Cloud Insights 进行配置，以提供多种有用的数据类型，这些数据可用于协助进行规划，故障排除，维护以及确保业务连续性。使用 Cloud Insights 监控 FlexPod Datacenter 解决方案，并在易于理解的自定义信息板中显示聚合的数据；不仅可以预测部署中的资源何时需要扩展以满足需求，还可以确定导致系统出现问题的特定应用程序或存储卷。这有助于确保所监控的基础架构可预测并根据预期运行，从而使组织能够按定义的 SLA 交付并根据需要扩展基础架构，从而避免浪费和额外成本。

架构

在本节中，我们将回顾 FlexPod 数据中心融合基础架构的架构，包括由 Cloud Insights 监控的 NetApp AFF A800 系统。

解决方案技术

FlexPod Datacenter 解决方案由以下最低组件组成，可提供高度可用，易于扩展，经验证且受支持的融合基础架构环境。

- 两个 NetApp ONTAP 存储节点（一个 HA 对）
- 两个 Cisco Nexus 数据中心网络交换机
- 两个 Cisco MDS 光纤交换机（FC 部署可选）
- 两个 Cisco UCS 互联阵列
- 一个带有两个 Cisco UCS B 系列刀片式服务器的 Cisco UCS 刀片式服务器机箱

或

- 两个 Cisco UCS C 系列机架式服务器

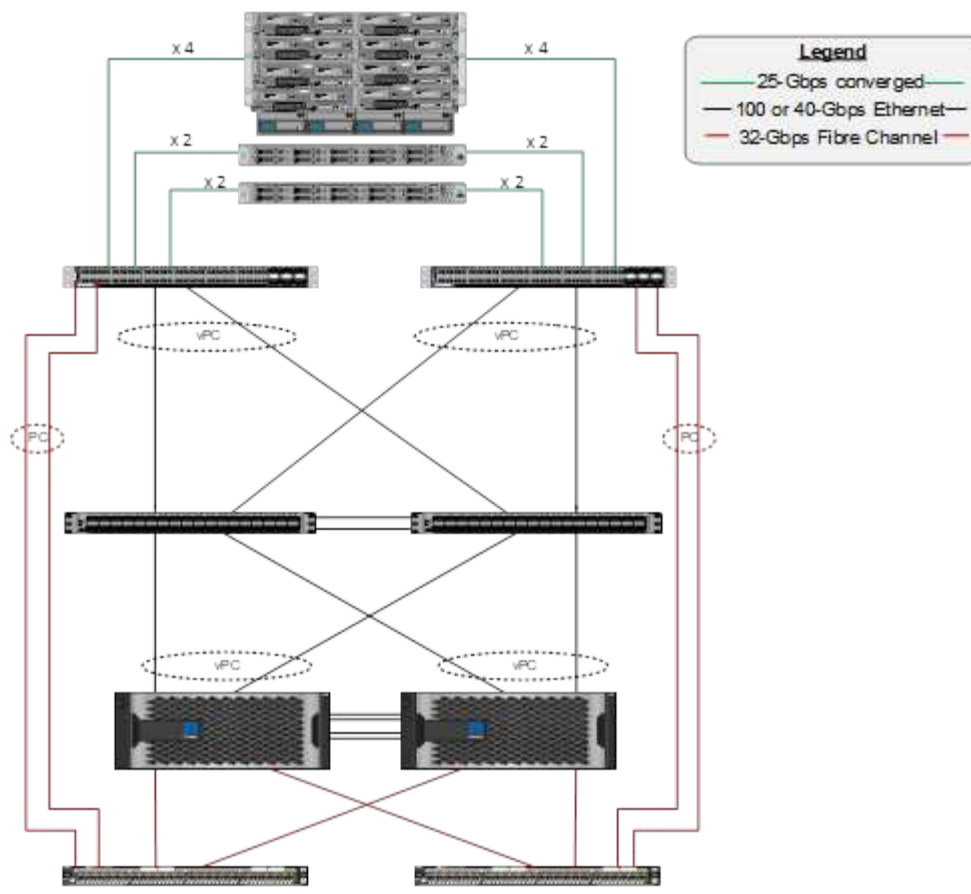
要使 Cloud Insights 收集数据，组织必须将采集单元部署为其 FlexPod 数据中心环境中的虚拟机或物理机，或者部署在可与从中收集数据的组件联系的位置。您可以在运行多个受支持的 Windows 或 Linux 操作系统的系统上安装采集单元软件。下表列出了此软件的解决方案组件。

操作系统	version
Microsoft Windows	10
Microsoft Windows Server	2012 ， 2012 R2 ， 2016 ， 2019
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

架构图

下图显示了解决方案架构。

Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects, UCS 2408 Fabric Extenders, UCS B-Series Blade Servers with UCS VIC 1440, and UCS C-Series Rack Servers with UCS VIC 1457



硬件要求

下表列出了实施解决方案所需的硬件组件。在任何特定解决方案实施中使用的硬件组件可能会因客户要求而异。

硬件	数量
Cisco Nexus 9336C-x2	2.
Cisco UCS 6454 互联阵列	2.
Cisco UCS 5108 刀片式服务器机箱	1.
Cisco UCS 2408 阵列扩展器	2.
Cisco UCS B200 M5 刀片式服务器	2.
NetApp AFF A800	2.

软件要求

下表列出了实施解决方案所需的软件组件。在任何特定解决方案实施中使用的软件组件可能会因客户要求而异。

软件	version
Cisco Nexus 固件	9.3 (5)
Cisco UCS 版本	4.1 (2a)
NetApp ONTAP 版本	9.7

软件	version
NetApp Cloud Insights 版本	2020 年 9 月，基本版
Red Hat Enterprise Linux	7.6
VMware vSphere	6.7U3.

用例详细信息

此解决方案适用场景的使用情形如下：

- 使用提供给 NetApp Active IQ 数字顾问的数据分析环境，以评估存储系统风险并提供存储优化建议。
- 通过实时检查系统统计信息对部署在 FlexPod Datacenter 解决方案中的 ONTAP 存储系统中的问题进行故障排除。
- 生成自定义信息板，以便轻松监控在 FlexPod 数据中心融合基础架构中部署的 ONTAP 存储系统的特定关注点。

设计注意事项

FlexPod Datacenter 解决方案是由 Cisco 和 NetApp 设计的一种融合基础架构，可为运行企业工作负载提供动态，高可用性和可扩展的数据中心环境。解决方案中的计算和网络资源由 Cisco UCS 和 Nexus 产品提供，存储资源由 ONTAP 存储系统提供。当更新的硬件型号或软件和固件版本可用时，解决方案设计会定期进行增强。这些详细信息以及解决方案设计和部署的最佳实践均包含在 Cisco Validated Design （CVD）或 NetApp Verified Architecture （NVA）文档中，并定期发布。

我们提供了详细介绍 FlexPod Datacenter 解决方案设计的最新 CVD 文档 ["此处"](#)。

部署适用于 FlexPod 的 Cloud Insights

要部署解决方案，您必须完成以下任务：

1. 注册 Cloud Insights 服务
2. 创建要配置为采集单元的 VMware 虚拟机（VM）
3. 安装 Red Hat Enterprise Linux （RHEL）主机
4. 在 Cloud Insights 门户中创建采集单元实例并安装软件
5. 将受监控的存储系统从 FlexPod 数据中心添加到 Cloud Insights。

注册 NetApp Cloud Insights 服务

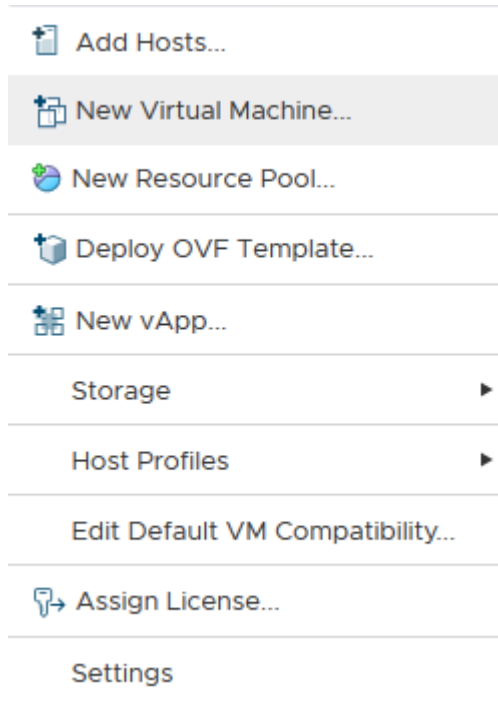
要注册 NetApp Cloud Insights 服务，请完成以下步骤：

1. 转至 ["https://cloud.netapp.com/cloud-insights"](https://cloud.netapp.com/cloud-insights)
2. 单击屏幕中央的按钮开始 14 天免费试用，或者单击右上角的链接注册或使用现有 NetApp Cloud Central 帐户登录。

创建要配置为采集单元的 **VMware** 虚拟机

要创建 VMware VM 以配置为采集单元，请完成以下步骤：

1. 启动 Web 浏览器并登录到 VMware vSphere，然后选择要托管 VM 的集群。
2. 右键单击该集群，然后从菜单中选择创建虚拟机。



3. 在新建虚拟机向导中，单击下一步。
4. 指定虚拟机的名称并选择要将其安装到的数据中心，然后单击下一步。
5. 在以下页面上，选择要将虚拟机安装到的集群，节点或资源组，然后单击下一步。
6. 选择托管 VM 的共享数据存储库，然后单击下一步。
7. 确认虚拟机的兼容模式已设置为 ESXi 6.7 或更高版本，然后单击下一步。
8. 选择子操作系统系列 Linux，子操作系统版本：Red Hat Enterprise Linux 7（64 位）。

Select a guest OS

Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: 

Guest OS Version: 

Compatibility: ESXi 6.7 and later (VM version 14)

CANCEL

BACK

NEXT

9. 下一页用于自定义虚拟机上的硬件资源。Cloud Insights 采集单元需要以下资源。选择资源后，单击下一步：
- a. 两个 CPU
 - b. 8 GB RAM
 - c. 100 GB 硬盘空间
 - d. 一种可通过端口 443 上的 SSL 连接访问 FlexPod 数据中心和 Cloud Insights 服务器中资源的网络。
 - e. 要从中启动的选定 Linux 分发版（Red Hat Enterprise Linux）的 ISO 映像。

Customize hardware

Configure the virtual machine hardware

Virtual Hardware VM Options

ADD NEW DEVICE

> CPU *	2		
> Memory *	8		GB
> New Hard disk *	100		GB
> New SCSI controller *	VMware Paravirtual		
> New Network *	VM_Network	☒	Connect...
> New CD/DVD Drive *	Datastore ISO File	☒	Connect...
> Video card *	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		

Compatibility: ESXi 6.7 and later (VM version 14)

CANCEL BACK NEXT

10. 要创建虚拟机，请在准备完成页面上查看设置，然后单击完成。

安装 Red Hat Enterprise Linux

要安装 Red Hat Enterprise Linux ， 请完成以下步骤：

- 1. 启动虚拟机，单击窗口以启动虚拟控制台，然后选择安装 Red Hat Enterprise Linux 7.6 选项。

Red Hat Enterprise Linux 7.6

Install Red Hat Enterprise Linux 7.6

Test this media & install Red Hat Enterprise Linux 7.6

Troubleshooting

>

Press Tab for full configuration options on menu items.

2. 选择首选语言，然后单击 Continue 。

下一页是安装摘要。大多数选项都应接受默认设置。

3. 您必须通过执行以下选项来自定义存储布局：

- a. 要自定义服务器的分区，请单击安装目标。
- b. 确认已选择具有黑色复选标记的 100 GiB VMware 虚拟磁盘，然后选择 I will Configure Partitioning 单选按钮。

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

100 GiB



VMware Virtual disk
sda / 100 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks



Add a disk...

Disks left unselected here will not be touched.

Other Storage Options

Partitioning

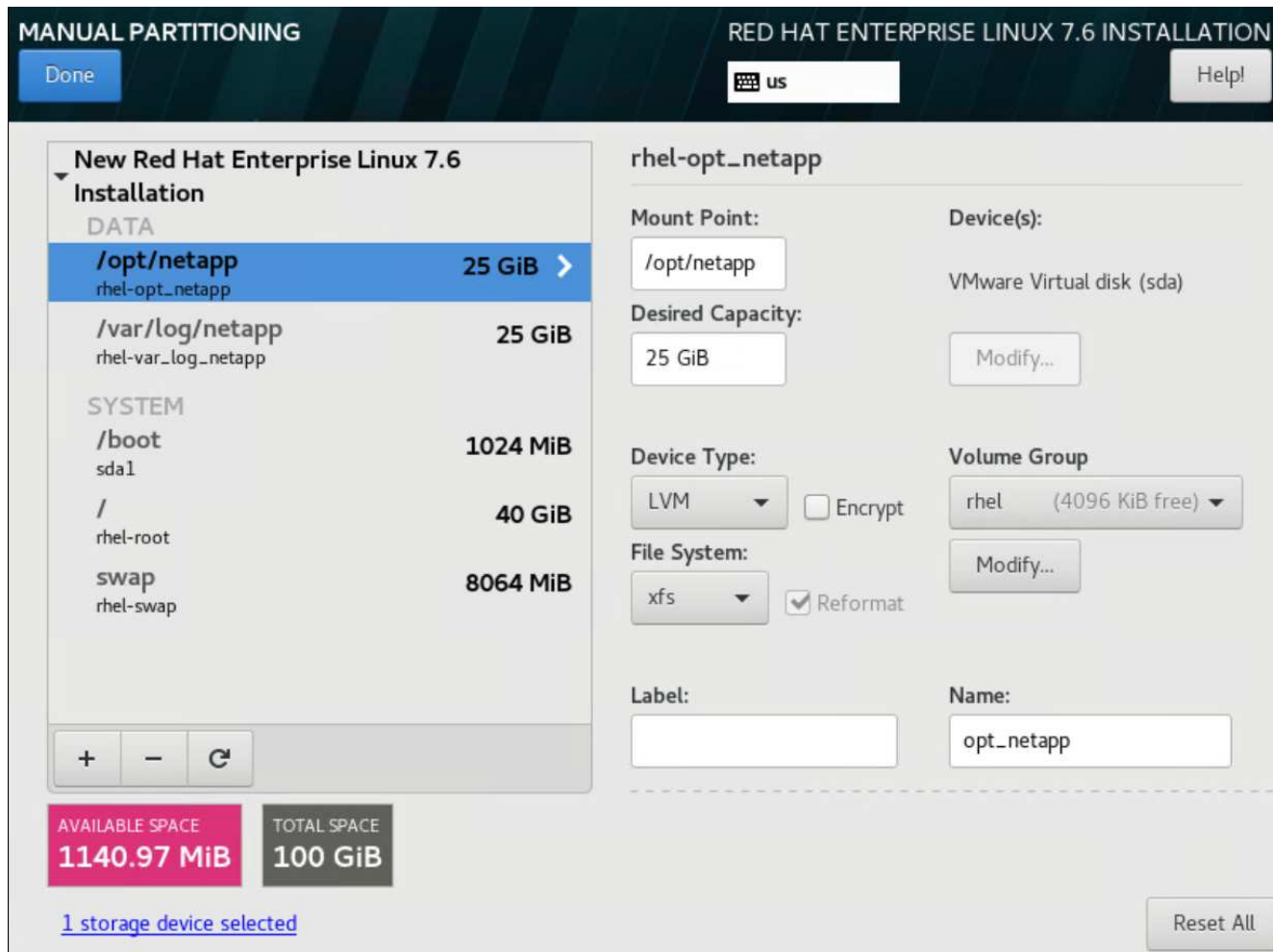
- ☐ Automatically configure partitioning. ☒ I will configure partitioning.
☐ I would like to make additional space available.

[Full disk summary and boot loader...](#)

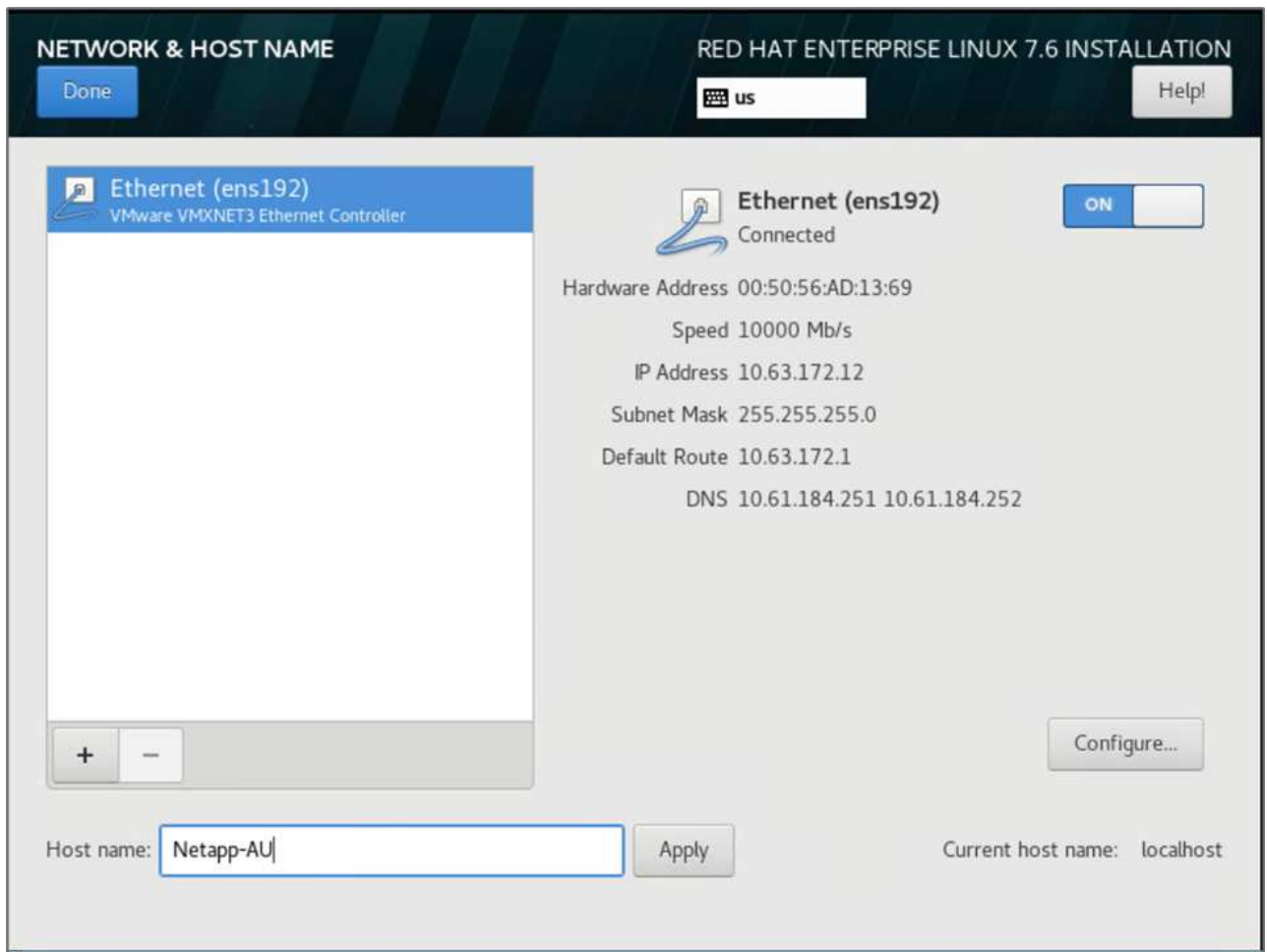
1 disk selected; 100 GiB capacity; 100 GiB free [Refresh...](#)

c. 单击 Done 。

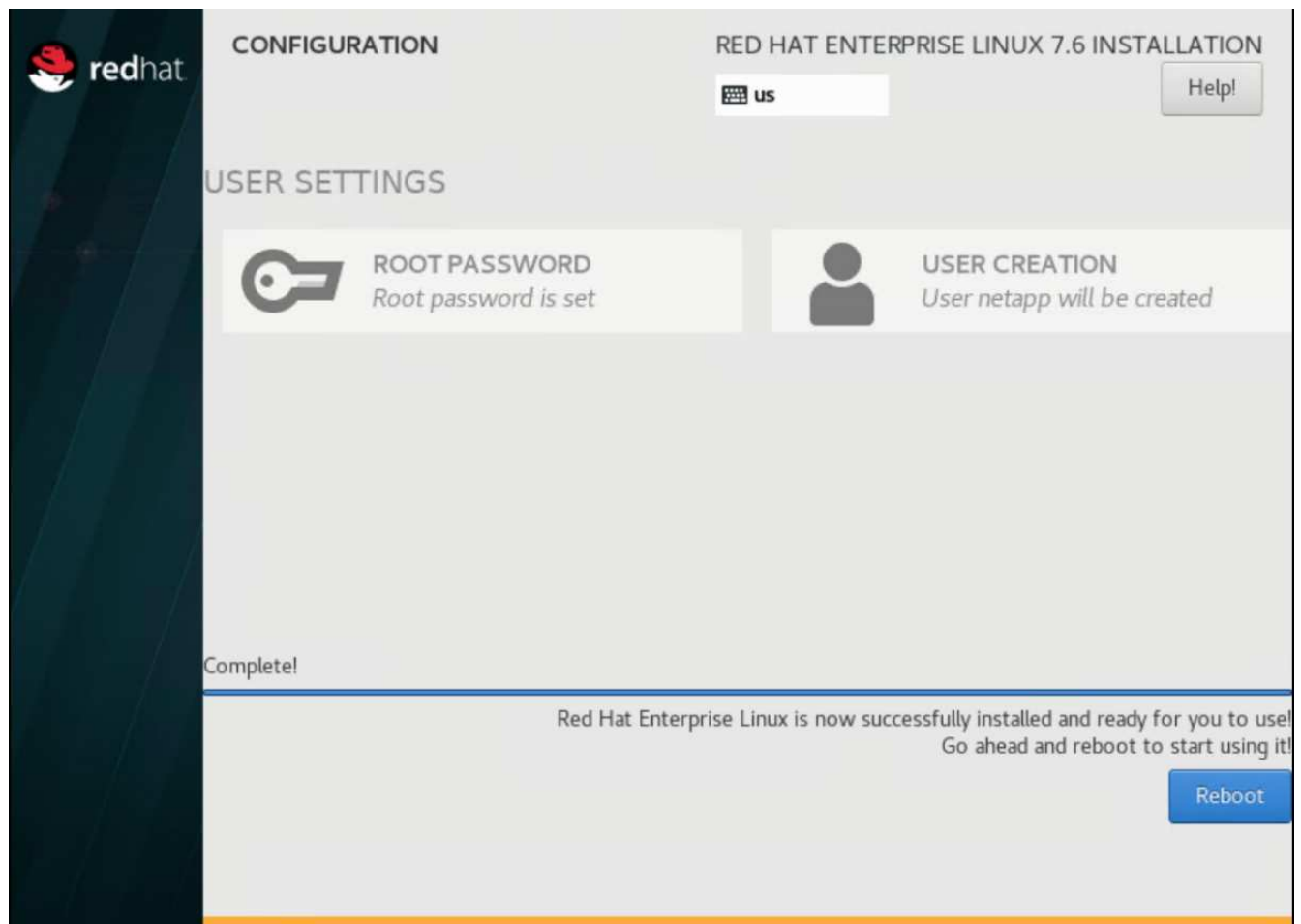
此时将显示一个新菜单，用于自定义分区表。每个为 `/opt/NetApp` 和 `/var/log/NetApp` 专用 25 GB。您可以自动将其余存储分配给系统。



- a. 要返回到安装摘要，请单击完成。
4. 单击网络 and 主机名。
 - a. 输入服务器的主机名。
 - b. 单击滑块按钮打开网络适配器。如果在网络上配置了动态主机配置协议（DHCP），您将收到一个 IP 地址。如果不是，请单击配置，然后手动分配地址。



- c. 。单击 Done 以返回到 Installation Summary 。
5. 在安装摘要页面上，单击开始安装。
6. 在安装进度页面上，您可以设置 root 密码或创建本地用户帐户。安装完成后，单击重新启动以重新启动服务器。



7. 系统重新启动后，登录到服务器并将其注册到 Red Hat 订阅管理器。

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

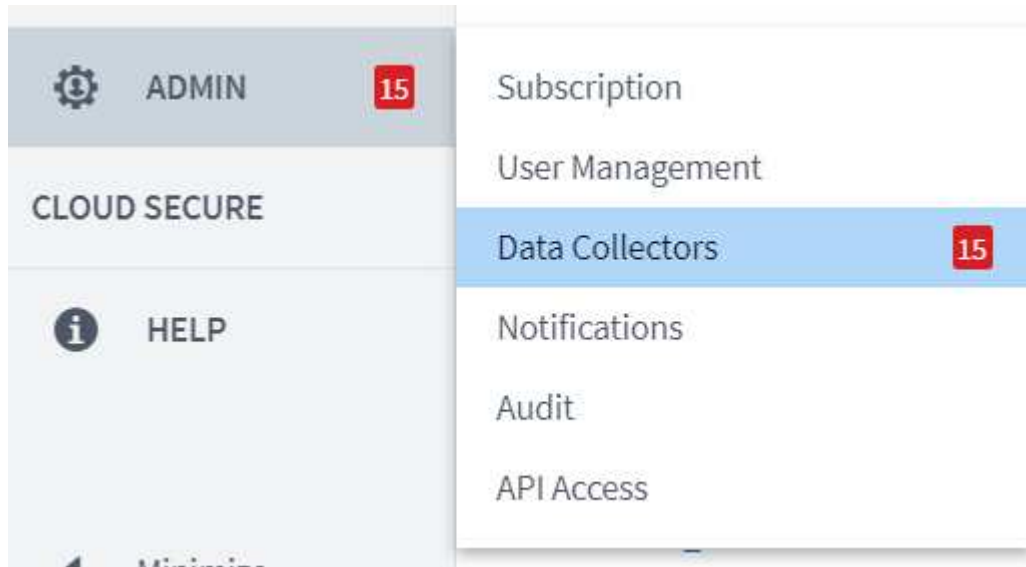
8. 附加 Red Hat Enterprise Linux 的可用订阅。

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

在 **Cloud Insights** 门户中创建采集单元实例并安装软件

要在 Cloud Insights 门户中创建采集单元实例并安装软件，请完成以下步骤：

1. 从 Cloud Insights 的主页中，将鼠标悬停在主菜单左侧的 "Admin" 条目上，然后从菜单中选择 "Data Collectors" 。



2. 在数据收集器页面的顶部中间，单击采集单元的连接。



3. 要创建新的采集单元，请单击右侧的按钮。



4. 选择要用于托管采集单元的操作系统，然后按照以下步骤从网页复制安装脚本。

在此示例中，它是一个 Linux 服务器，提供一个代码片段和一个令牌，用于粘贴到主机的命令行界面中。此网页将等待采集单元连接。

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

Linux

Linux Versions Supported Production Best Practices

Need Help?

This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

[illegible]

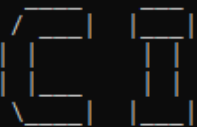
3 Please ensure you have copied and pasted the snippet into the bash shell.

[illegible]

172

```


Welcome to CloudInsights (R) ..
Acquisition Unit



NetApp (R)
Installation: /opt/netapp/cloudinsights
Logs:        /opt/netapp/cloudinsights/logs -> /var/log/netapp/cloudinsights

To control the CloudInsights service:
  sudo cloudinsights-service.sh --help
To uninstall:
  sudo cloudinsights-uninstall.sh --help

1/8 Acquisition Unit Starting
2/8 Connecting to Cloud Insights
3/8 Sending Certificate-Signing Request..
4/8 Logging in to Cloud Insights
5/8 Updating Security Settings..
6/8 Downloading Data Collection Modules
7/8 Registering to Cloud Insights
8/8 Acquisition Unit Ready

Acquisition Unit has been installed successfully.
[root@Netapp-AU ~]#
```

将受监控的存储系统从 **FlexPod** 数据中心添加到 **Cloud Insights**

要从 FlexPod 部署添加 ONTAP 存储系统，请完成以下步骤：

1. 返回到 Cloud Insights 门户上的 Acquisition Units 页面，找到列出的新注册的单元。要显示单元的摘要，请单击该单元。

NetApp PCS Sa... / Admin / Acquisition Units / NetApp-AU					Restart
Summary					
Name NetApp-AU	IP 10.1.156.115	Status OK	Last Reported 9 minutes ago	Note	

2. 要启动向导以添加存储系统，请在摘要页面上单击用于创建数据收集器的按钮。第一页显示可从中收集数据的所有系统。使用搜索栏搜索 ONTAP 。

Choose a Data Collector to Monitor


 Cloud Volumes ONTAP


 Data ONTAP 7-Mode


 ONTAP Data Management
 Software


 ONTAP Select

3. 选择 ONTAP 数据管理软件。

此时将显示一个页面，用于为部署命名并选择要使用的采集单元。您可以提供 ONTAP 系统的连接信息和凭据，并对连接进行测试以确认。







Select a Data Collector
Configure Data Collector


 ONTAP Data Management Software

Configure Collector

Add credentials and required settings
[Need Help?](#)



Configuration: Successfully pinged 192.168.156.50.

Configuration: Successfully executed test command on device.

Name ⓘ

Acquisition Unit

NetApp-AU

NetApp Management IP Address

User Name

Password

Complete Setup

Test Connection

 Advanced Configuration

4. 单击 Complete Setup。

此门户将返回到 "数据收集器" 页面，而数据收集器将开始首次轮询，以便从 FlexPod 数据中心的 ONTAP 存储系统收集数据。

FlexPod Datacenter	All stand-by	NetApp ONTAP Data Management Software	NetApp-AU	192.168.156.50	 Polling...
--------------------	--------------	---------------------------------------	-----------	----------------	--

用例

通过设置并配置 Cloud Insights 来监控您的 FlexPod Datacenter 解决方案，我们可以在信

息板上探索一些可执行的任务，以评估和监控您的环境。在本节中，我们重点介绍了 Cloud Insights 的五个主要用例：

- Active IQ 集成
- 探索实时信息板
- 创建自定义信息板
- 高级故障排除
- 存储优化

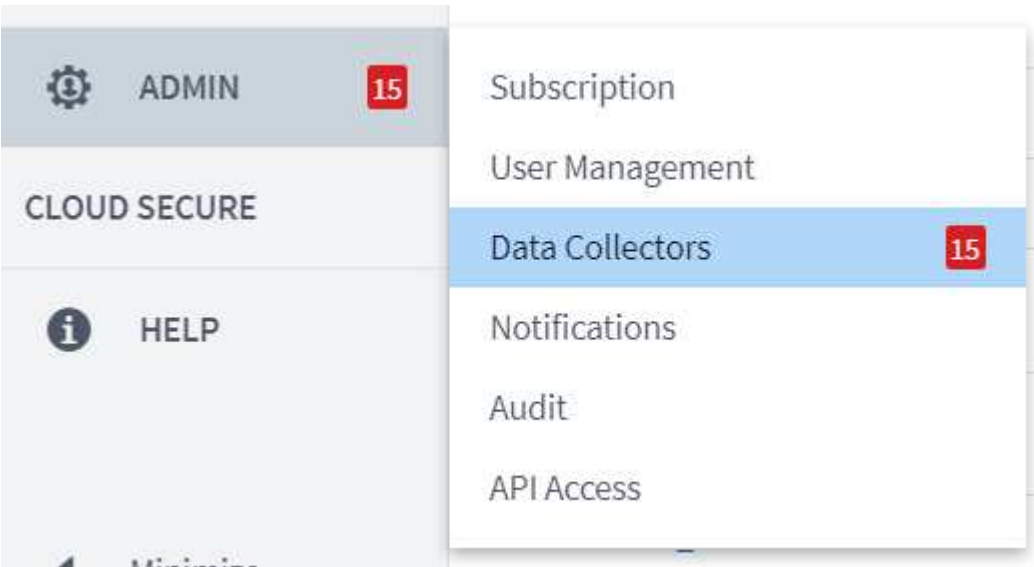
Active IQ 集成

Cloud Insights 已完全集成到 Active IQ 存储监控平台中。作为 FlexPod Datacenter 解决方案的一部分部署的 ONTAP 系统会自动配置为通过每个系统内置的 AutoSupport 功能将信息发送回 NetApp。这些报告会按计划生成，或者在系统中检测到故障时动态生成。通过 AutoSupport 传输的数据会进行聚合，并显示在 Cloud Insights 的 Active IQ 菜单下易于访问的信息板中。

通过 Cloud Insights 信息板访问 Active IQ 信息

要通过 Cloud Insights 信息板访问 Active IQ 信息，请完成以下步骤：

1. 单击左侧管理菜单下的 Data Collector 选项。



2. 筛选环境中的特定 Data Collector。在此示例中，我们按术语 FlexPod 进行筛选。

NetApp PCS Sa... / Admin / Data Collectors

Data Collectors 15

Acquisition Units 8

Data Collectors (1)

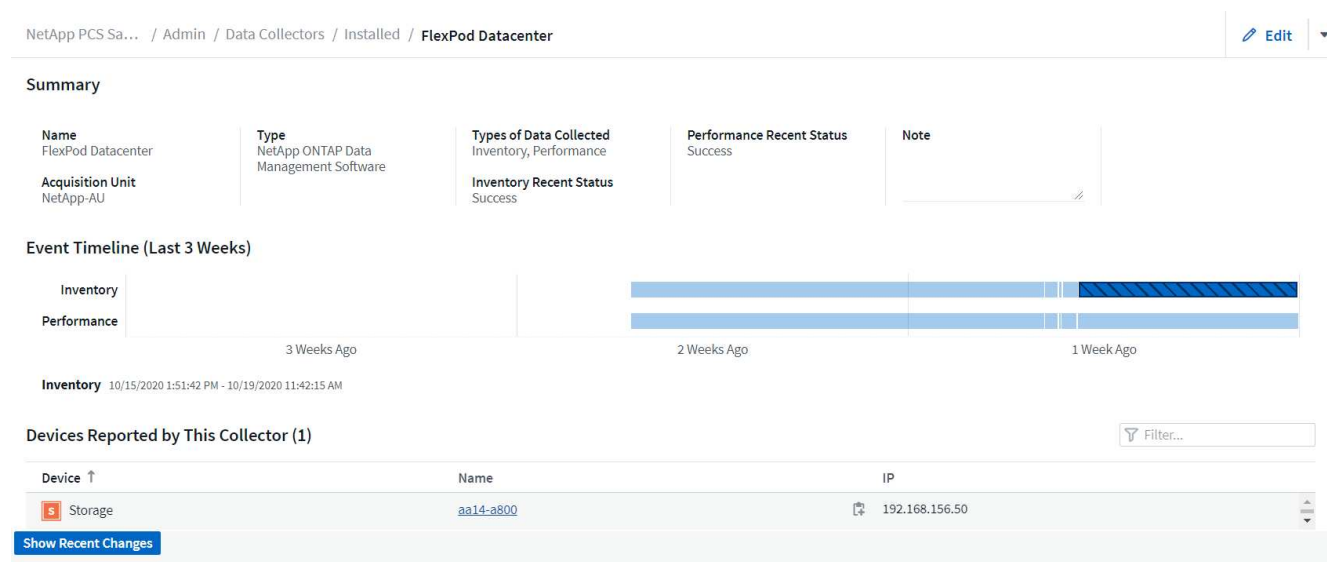
+ Data Collector

Bulk Actions ▾

FlexPod

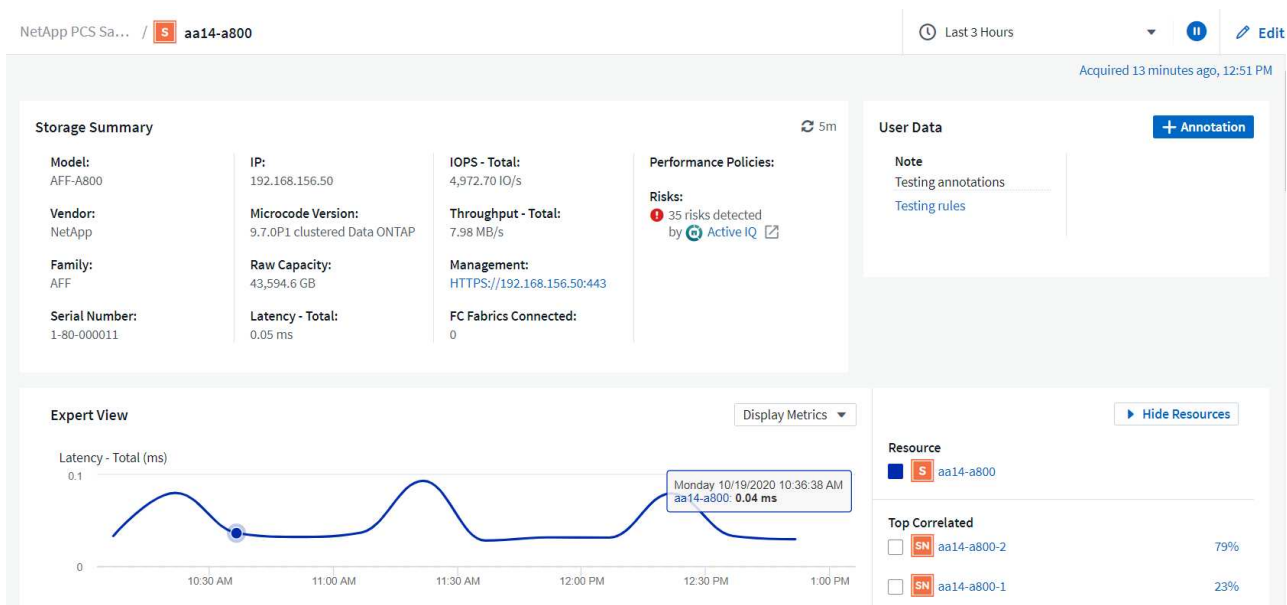
☐	Name	Status	Type	Acquisition Unit	IP	Impact ↓	Last Acquired
	FlexPod Datacenter	All successful	NetApp ONTAP Data Management Software	NetApp-AU	192.168.156.50		10 minutes ago ⋮

3. 单击 Data Collector 以获取该收集器所监控的环境和设备的摘要。



在底部附近的设备列表下，单击要监控的 ONTAP 存储系统的名称。此时将显示一个信息板，其中包含有关系统的信息，包括以下详细信息：

- 型号
- 系列
- ONTAP 版本
- 原始容量
- 平均 IOPS
- 平均延迟
- 平均吞吐量



此外，在此页面上的性能策略部分下，您可以找到指向 NetApp Active IQ 的链接。

 5m

Performance Policies:

Risks:

 35 risks detected by  Active IQ 

4. 要打开一个新的浏览器选项卡并转到风险缓解页面，其中显示了哪些节点受到影响，风险有多严重以及需要采取哪些适当措施来更正已确定的问题，请单击 Active IQ 链接。




Active IQ Digital Advisor
Discovery Dashboard
Asset Insights


 Set a default view

Home > Cisco Systems Inc. > CISCO SYSTEMS - RTP - BUILDING 9 > aa14-a800

The Risk Acknowledgment feature has been migrated to Active IQ Digital Advisor. [Click here](#) to view and acknowledge risks.

Health
Security Vulnerability
Proactive Remediation
Best Practices
Performance
System Health
Storage Virtual Machine Health
Health Trending

☒ High
☒ Medium
☒ Low

Ack	Node	Serial No	Impact Level	Public	Category	Risk	Details	Corrective Action
	aa14-a800-2	941834000459	High	No	ONTAP	A network interface (LIF) using a port on a X1116A, X1146A or X91146A NIC might not fail over to an alternate port.	A previously operational port on a X1116A, X1146A or X91146A NIC that encounters a fatal error with no preceding "link down" event will still report the link status as "up", instead of reporting link status as "down". Potential Impact: Any network interface (LIF) using the port does not fail over to an alternate port in the event of failure.	Bug ID: 1322372
	aa14-a800-2	941834000459	High	Yes	FAS Hardware	On AFF A800 systems an erroneous 'Critical High' sensor reading can result in a system shutdown.	This AFF-A800 system is running BMC firmware 10.3 which is susceptible to bug 1279964. Potential Impact: System disruption caused by an erroneous 'Critical High' sensor reading.	Bug ID: 1279964
	aa14-a800-2	941834000459	High	Yes	ONTAP	AFF systems running an unfixed version of ONTAP with data compaction enabled and host services over FCP, iSCSI or NVMe can experience a disruption in service due to BUG 1273955.	This system is running ONTAP 9.7P1 and is utilizing FCP, iSCSI or NVMe protocols and has compaction enabled and therefore is exposed to BUG 1273955. Potential Impact: The system may experience performance degradation and possible panic.	Bug ID: 1273955
	aa14-a800-2	941834000459	High	Yes	ONTAP	ONTAP 9.7 running on an All-Flash FAS (AFF) system having SAN workload might cause a controller disruption.	ONTAP 9.7 running on an All-Flash FAS (AFF) system having SAN workload with inline compression combined with cross-volume inline deduplication might cause a storage controller disruption. Potential Impact: The system may experience a disruption.	KB ID: SU426
	aa14-a800-1	941834000183	High	No	ONTAP	A network interface (LIF) using a port on a X1116A, X1146A or X91146A NIC might not fail over to an alternate port.	A previously operational port on a X1116A, X1146A or X91146A NIC that encounters a fatal error with no preceding "link down" event will still report the link status as "up", instead of reporting link status as "down".	Bug ID: 1322372

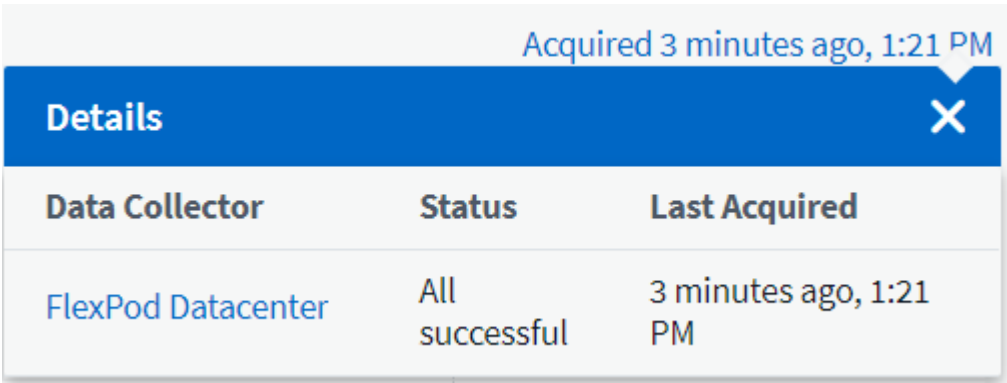
1 - 17 of 17 results

浏览实时信息板

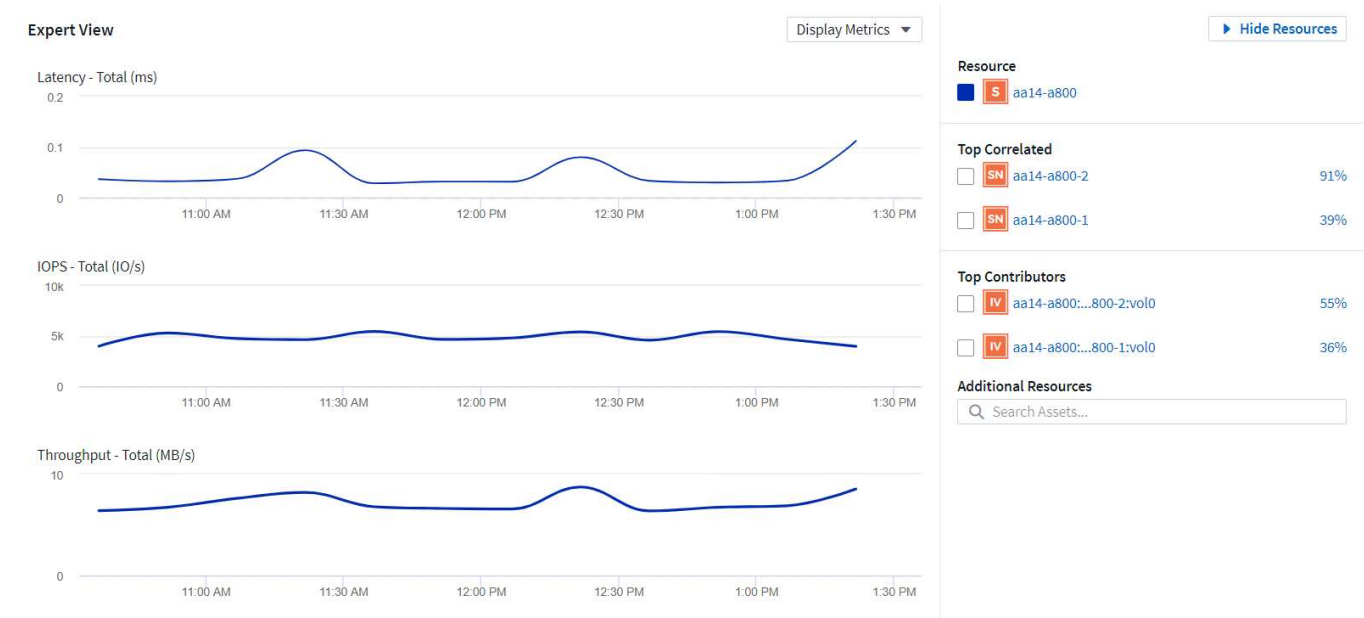
Cloud Insights 可以显示从 FlexPod Datacenter 解决方案中部署的 ONTAP 存储系统轮询的信息的实时信息板。Cloud Insights 采集单元定期收集数据，并使用收集的信息填充默认存储系统信息板。

通过 Cloud Insights 信息板访问实时图形

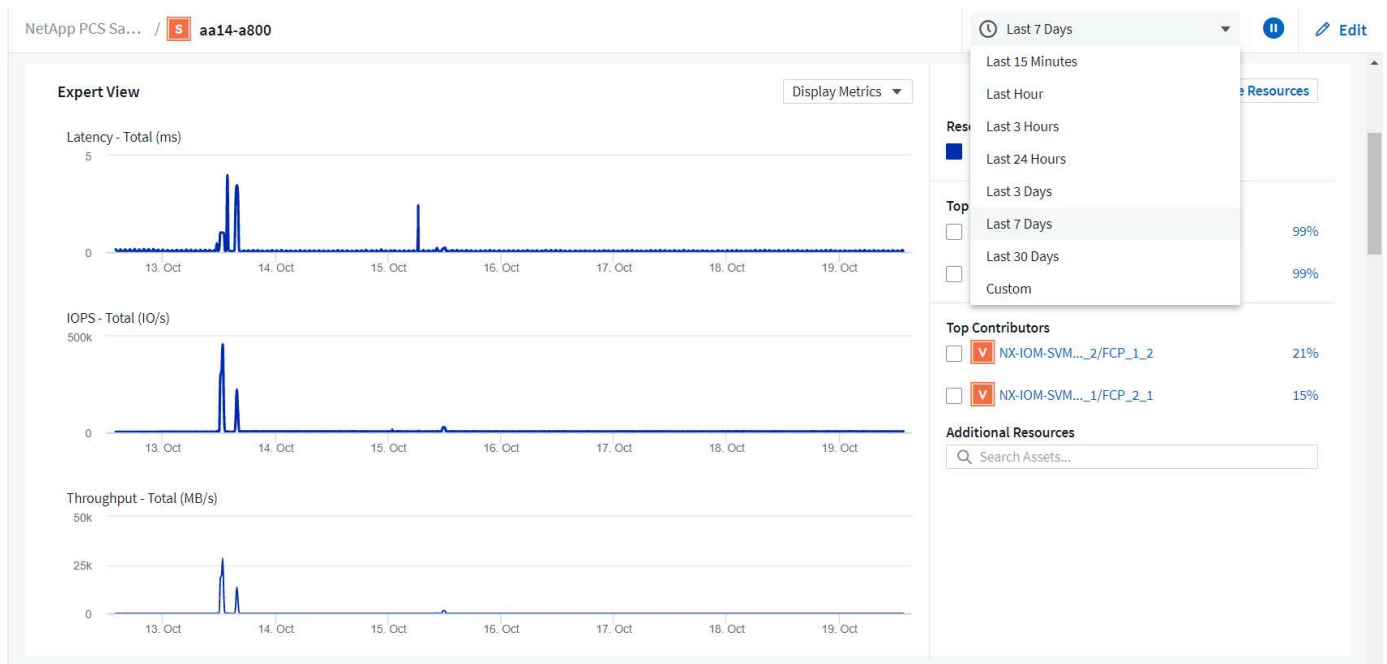
在存储系统信息板中，您可以看到 Data Collector 上次更新信息的时间。下图显示了这方面的一个示例。



默认情况下，存储系统信息板会在 "Expert View" 部分中显示多个交互式图形，这些图形显示所轮询的存储系统或每个节点的系统范围指标，包括：延迟，IOPS 和吞吐量。下图显示了这些默认图形的示例。



默认情况下，图形显示过去三小时的信息，但您可以将其设置为多个不同的值或存储系统信息板右上角下拉列表中的自定义值。如下图所示。



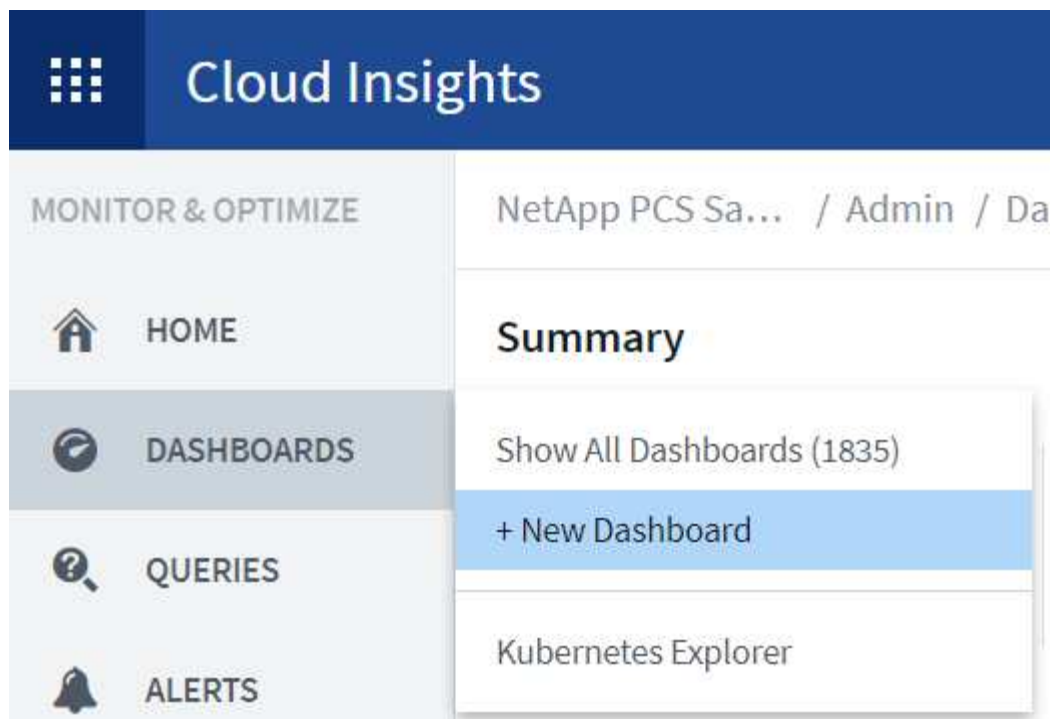
创建自定义信息板

除了使用显示系统范围信息的默认信息板之外，您还可以使用 Cloud Insights 创建完全自定义的信息板，以便集中精力关注 FlexPod Datacenter 解决方案中特定存储卷的资源使用情况。因此，在融合基础架构中部署的应用程序需要依靠这些卷才能有效运行。这样做可以帮助您更好地了解特定应用程序及其在数据中心环境中使用的资源。

创建自定义信息板以评估存储资源

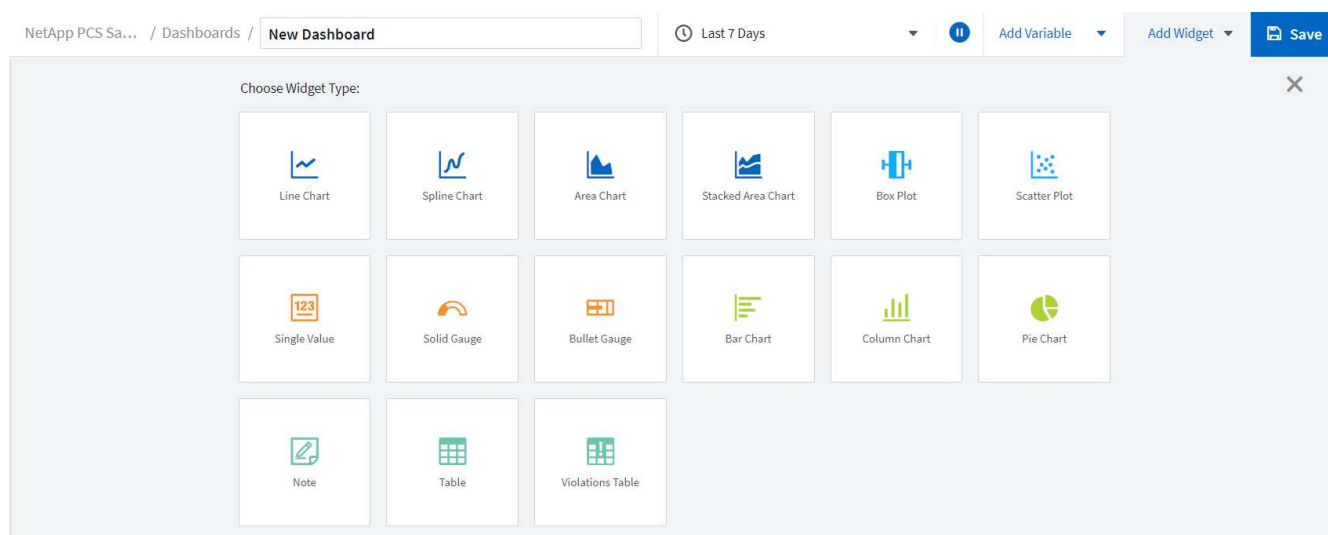
要创建自定义信息板以评估存储资源，请完成以下步骤：

1. 要创建自定义信息板，请将鼠标悬停在 Cloud Insights 主菜单上的 Dashboards 上，然后单击下拉列表中的 + New Dashboard 。



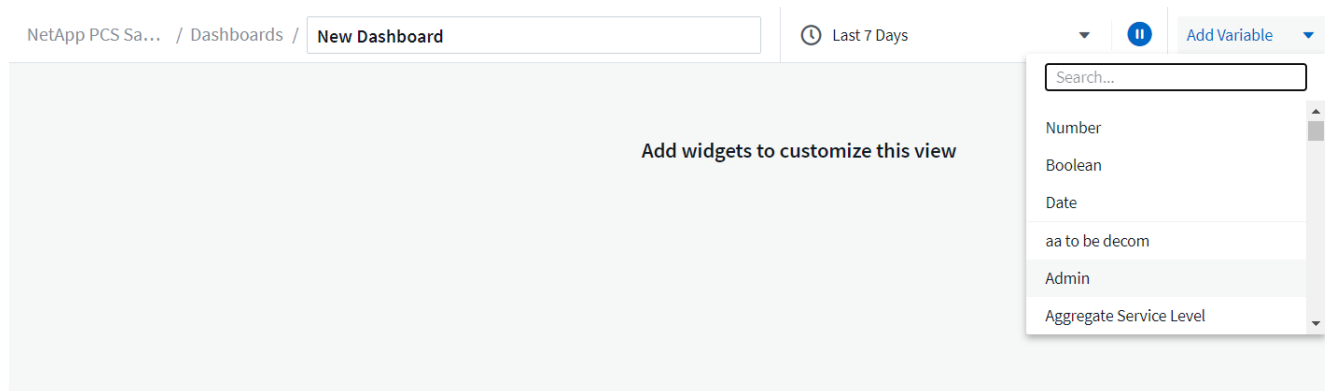
此时将打开 "New Dashboard" 窗口。

2. 为信息板命名，然后选择用于显示数据的小工具类型。您可以从多种图形类型中选择，甚至可以从注释或表类型中选择以显示收集的数据。

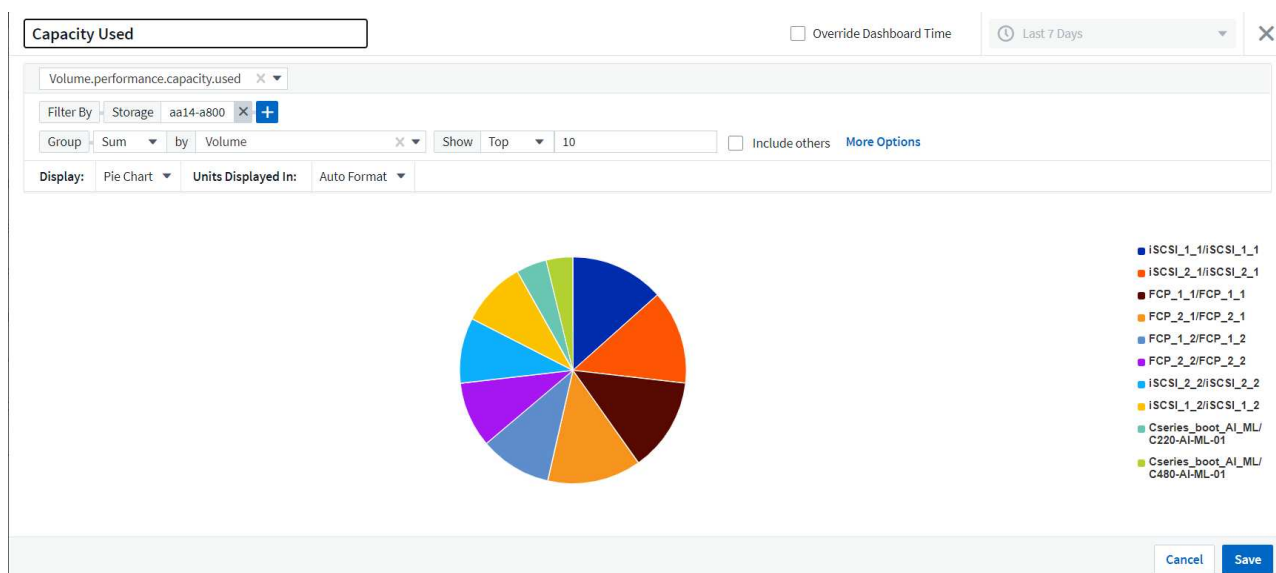


3. 从添加变量菜单中选择自定义变量。

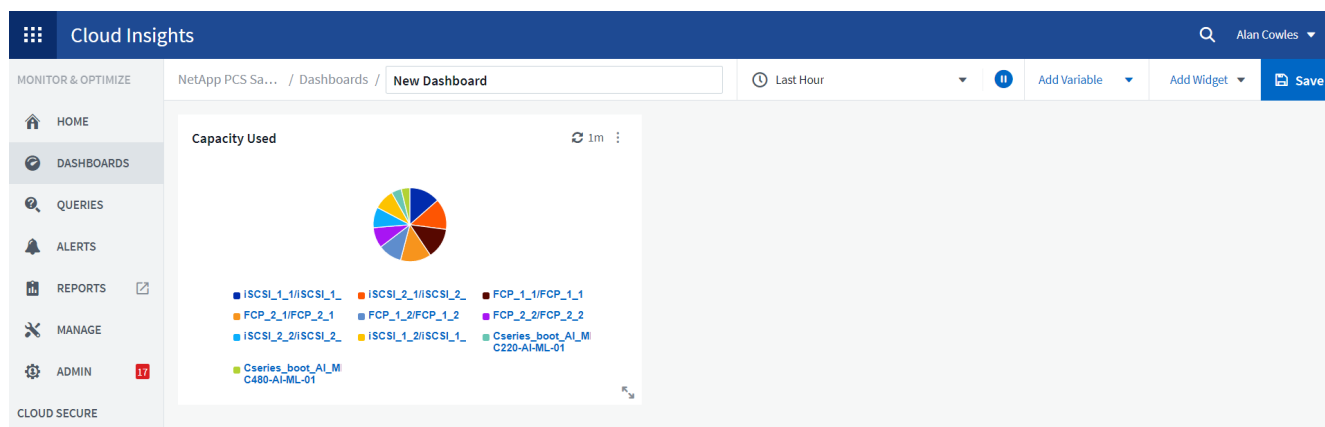
这样，所提供的数据就可以集中显示更具体或更专业的因素。



4. 要创建自定义信息板，请选择要使用的小工具类型，例如饼图以按卷显示存储利用率：
 - a. 从添加小工具下拉列表中选择饼图小工具。
 - b. 使用描述性标识符为小工具命名，例如 `Capacity used`。
 - c. 选择要显示的对象。例如，您可以按关键字卷搜索并选择 `volume.performance.capacity.used`。
 - d. 要按存储系统进行筛选，请使用筛选器并在 FlexPod Datacenter 解决方案中键入存储系统的名称。
 - e. 自定义要显示的信息。默认情况下，此选项将显示 ONTAP 数据卷并列出排名前 10 位的卷。
 - f. 要保存自定义信息板，请单击 **Save**。



保存自定义小工具后，浏览器将返回到 "新建信息板" 页面，在此页面中显示新创建的小工具，并允许执行交互操作，例如修改数据轮询期。



高级故障排除

Cloud Insights 支持将高级故障排除方法应用于 FlexPod 数据中心融合基础架构中的任何存储环境。使用上述每个功能的组件：Active IQ 集成，具有实时统计信息的默认信息板以及自定义信息板，可以尽早检测到可能出现的问题并快速解决。使用 Active IQ 中的风险列表，客户可以找到报告的可能导致问题描述的配置错误，或者发现已报告的错误以及可对其进行补救的代码修补版本。通过观察 Cloud Insights 主页上的实时信息板，可以帮助您发现系统性能模式，这种模式可能是问题呈上升趋势的早期指标，并有助于迅速解决问题。最后，客户可以创建自定义信息板，从而可以专注于其基础架构中最重要资产，并直接监控这些资产，以确保满足其业务连续性目标。

存储优化

除了故障排除之外，还可以使用 Cloud Insights 收集的数据来优化部署在 FlexPod 数据中心融合基础架构解决方案中的 ONTAP 存储系统。如果某个卷的延迟较高，可能是因为多个具有高性能需求的 VM 共享同一个数据存储库，则此信息将显示在 Cloud Insights 信息板上。利用这些信息，存储管理员可以选择将一个或多个 VM 迁移到其他卷，在聚合层之间或 ONTAP 存储系统中的节点之间迁移存储卷，从而实现性能优化的环境。从 Active IQ 与 Cloud Insights 集成中收集的信息可以突出显示导致性能低于预期的配置问题，并提供建议的更正操作，如果实施，可以修复任何问题，并确保存储系统经过优化。

视频和演示

您可以观看有关使用 NetApp Cloud Insights 评估内部环境中资源的视频演示 ["此处"](#)。

您可以观看使用 NetApp Cloud Insights 监控基础架构并为基础架构设置警报阈值的视频演示 ["此处"](#)。

您可以观看使用 NetApp Cloud Insights 评估环境中各个应用程序的视频演示 ["此处"](#)。

追加信息

要了解有关本文档中所述信息的更多信息，请查看以下网站：

- Cisco 产品文档

["https://www.cisco.com/c/en/us/support/index.html"](https://www.cisco.com/c/en/us/support/index.html)

- FlexPod 数据中心

["https://www.flexpod.com"](https://www.flexpod.com)

- NetApp Cloud Insights

["https://cloud.netapp.com/cloud-insights"](https://cloud.netapp.com/cloud-insights)

- NetApp 产品文档

["https://docs.netapp.com"](https://docs.netapp.com)

采用 FabricPool 的 FlexPod —将非活动数据分层到 Amazon AWS S3

TR-4801：采用 FabricPool 的 FlexPod —将非活动数据分层到 Amazon AWS S3

NetApp 公司 Scott kovacs

闪存存储价格持续下降，因此可供以前不考虑使用闪存存储的工作负载和应用程序使用。但是，最高效地利用存储投资对于 IT 经理来说仍然至关重要。IT 部门仍然需要在极少或根本不增加预算的情况下提供性能更高的服务。为了帮助满足这些需求，NetApp FabricPool 允许您利用云的经济效益，将不常用的数据从昂贵的内部闪存存储迁移到公有云中更经济高效的存储层。将不常访问的数据迁移到云中可释放 AFF 或 FAS 系统上的宝贵闪存存储空间，从而将更多业务关键型工作负载容量提供给高性能闪存层。

本技术报告介绍了 NetApp 和 Cisco 在 FlexPod 融合基础架构架构环境下 ONTAP 的 FabricPool 数据分层功能。您应熟悉 FlexPod 数据中心融合基础架构架构和 ONTAP 存储软件，以便从本技术报告中讨论的概念中充分受益。在熟悉 FlexPod 和 ONTAP 的基础上，我们将讨论 FabricPool，它的工作原理以及如何使用它来更高效地利用内部闪存存储。本报告中的大部分内容在中进行了更详细的介绍 ["TR-4598：FabricPool 最佳实践"](#) 和其他 ONTAP 产品文档。此内容针对 FlexPod 基础架构进行了精简，并不能完全涵盖 FabricPool 的所有使用情形。ONTAP 9.6 提供了所有已研究的功能和概念。

中提供了有关 FlexPod 的追加信息 ["TR-4036 FlexPod 数据中心技术规格"](#)。

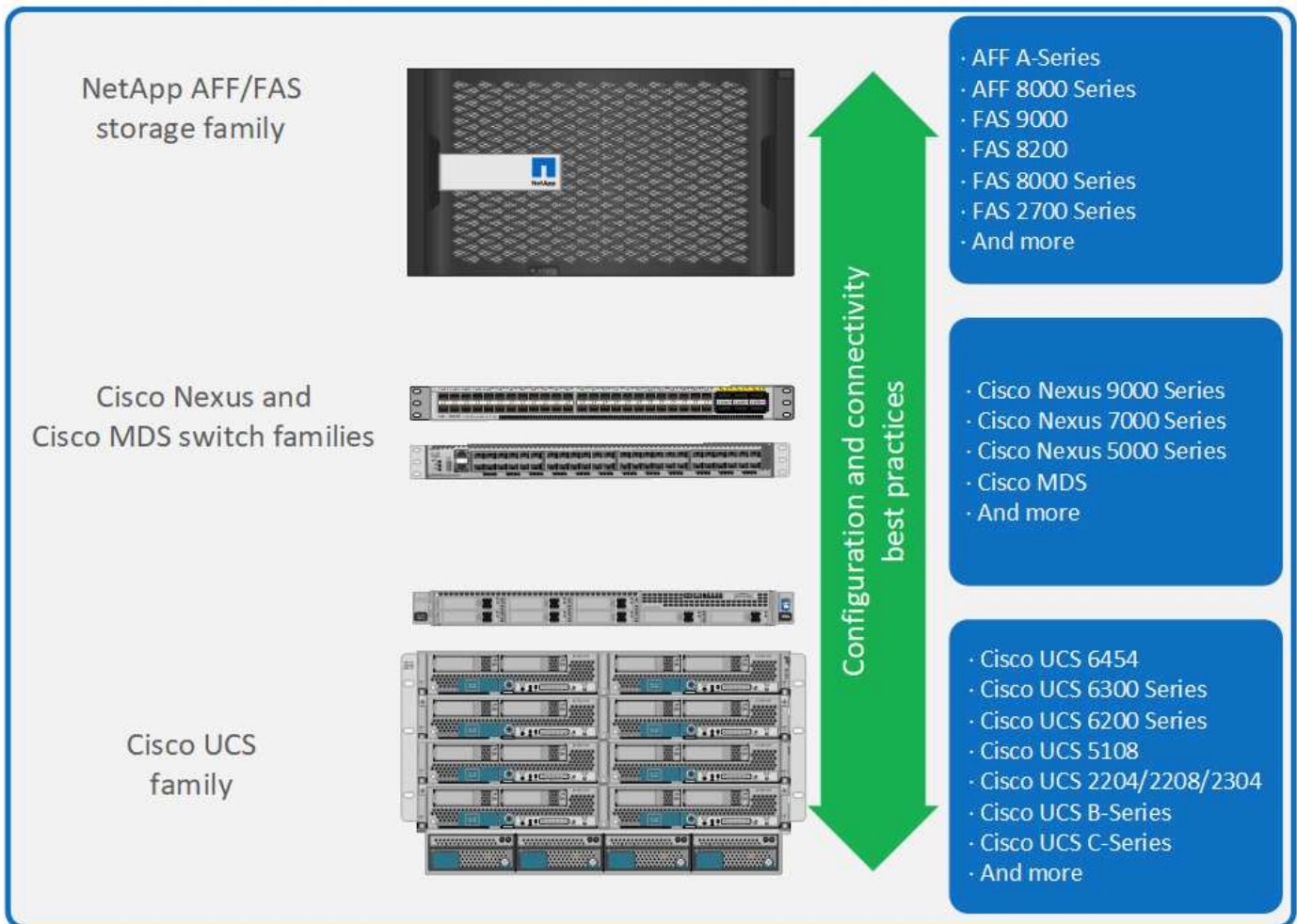
FlexPod 概述和架构

FlexPod 概述

FlexPod 是一组定义的硬件和软件，可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 在一个软件包中包含 NetApp AFF 存储，Cisco Nexus 网络，Cisco MDS 存储网络，Cisco 统一计算系统（Cisco UCS）和 VMware vSphere 软件。该设计非常灵活，可以将网络，计算和存储安装到一个数据中心机架中，也可以根据客户的数据中心设计进行部署。端口密度允许网络组件容纳多种配置。

FlexPod 架构的一个优势是能够自定义或灵活调整环境以满足客户的需求。FlexPod 单元可以根据需求和需求的变化轻松进行扩展。一个单元既可以纵向扩展（向 FlexPod 单元添加资源），也可以横向扩展（添加更多 FlexPod 单元）。FlexPod 参考架构重点介绍了光纤通道和基于 IP 的存储解决方案的故障恢复能力，成本效益以及部署简便性。存储系统能够在一个接口上提供多个协议，这为客户提供了一个选择并保护了他们的投资，因为它确实是一种 "一次线" 架构。下图显示了 FlexPod 的许多硬件组件。

FlexPod Datacenter solution

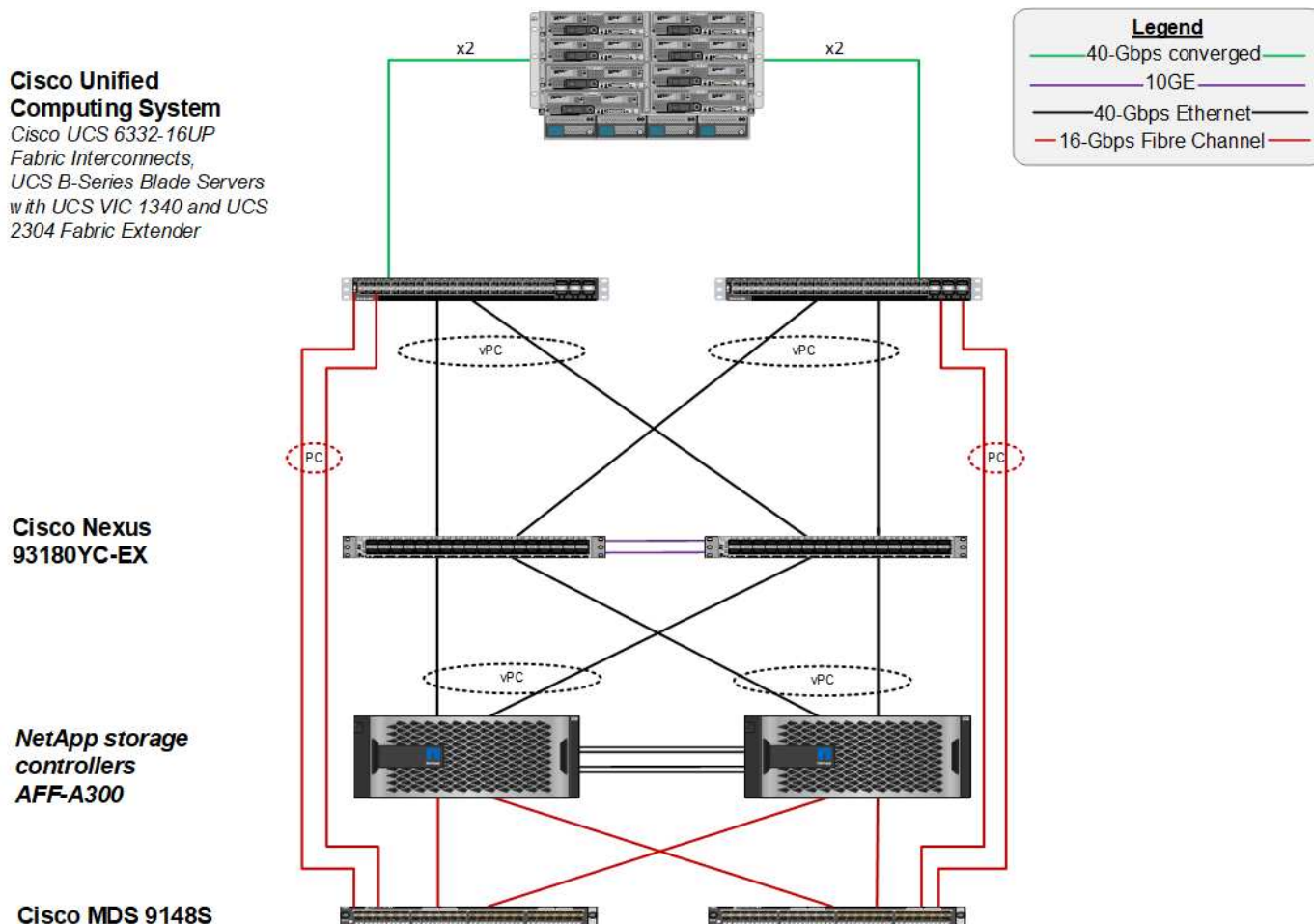


FlexPod 架构

下图显示了 VMware vSphere 和 FlexPod 解决方案的组件以及 Cisco UCS 6454 互联阵列所需的网络连接。此设计包含以下组件：

- Cisco UCS 5108 刀片式服务器机箱与 Cisco UCS 互联阵列之间的端口通道 40 Gb 以太网连接
- Cisco UCS 互联阵列与 Cisco Nexus 9000 之间的 40 Gb 以太网连接
- Cisco Nexus 9000 和 NetApp AFF A300 存储阵列之间的 40 Gb 以太网连接

随着 Cisco UCS 互联阵列和 NetApp AFF A300 之间的 Cisco MDS 交换机的推出，这些基础架构选项得以扩展。此配置可使 FC 启动的主机对共享存储进行 16 Gb FC 块级访问。此参考架构强化了一次线连接策略，因为在向该架构添加额外存储时，不需要从主机重新布线到 Cisco UCS 互联阵列。



FabricPool

FabricPool 概述

FabricPool 是 ONTAP 中的一种混合存储解决方案，它使用全闪存（SSD）聚合作为性能层，并将公有云服务中的对象存储作为云层。根据数据是否经常访问，此配置可以基于策略移动数据。ONTAP 平台上的 AFF 和纯 SSD 聚合在 FabricPool 中均支持 FAS。数据处理在块级别执行，全闪存性能层中经常访问的数据块标记为热块，不常访问的数据块标记为冷块。

使用 FabricPool 有助于降低存储成本，而不会影响性能，效率，安全性或保护。FabricPool 对企业级应用程序是透明的，它可以降低存储 TCO，而无需重新构建应用程序基础架构，从而充分利用云效率。

FlexPod 可以从 FabricPool 的存储分层功能中受益，从而更高效地利用 ONTAP 闪存存储。非活动虚拟机（VM），不常用的 VM 模板以及 NetApp SnapCenter for vSphere 中的 VM 备份可能会占用数据存储库卷中的宝贵空间。将冷数据移至云层可为 FlexPod 基础架构上托管的高性能任务关键型应用程序释放空间和资源。



光纤通道和 iSCSI 协议通常需要较长的时间才能发生超时（60 到 120 秒），但它们不会像 NAS 协议那样重试建立连接。如果 SAN 协议超时，则必须重新启动应用程序。即使是短暂的中断，也可能对使用 SAN 协议的生产应用程序造成灾难性的后果，因为无法保证与公有云的连接。为了避免这种问题描述，NetApp 建议在对 SAN 协议访问的数据进行分层时使用私有云。

在 ONTAP 9.6 中，FabricPool 与所有主要公有云提供商相集成：阿里云对象存储服务，Amazon AWS S3，Google 云存储，IBM 云对象存储和 Microsoft Azure Blob 存储。本报告重点介绍了 Amazon AWS S3 存储作为云对象层的选择。

复合聚合

通过将 ONTAP 闪存聚合与云对象存储（例如 AWS S3 存储分段）关联来创建 FabricPool 实例，以创建复合聚合。在复合聚合中创建卷时，它们可以利用 FabricPool 的分层功能。将数据写入卷时，ONTAP 会为每个数据块分配一个温度。首次写入块时，会为其分配温度为 "热"。随着时间的推移，如果不访问数据，则会经历一个冷却过程，直到最终将其分配为冷状态为止。然后，这些不常访问的数据块将从性能 SSD 聚合分层到云对象存储。

ONTAP 中的卷分层策略会修改块从指定为冷存储到移动到云对象存储这段时间。通过修改 ONTAP 设置，控制块变冷所需的天数，可以进一步细化。数据分层的候选对象包括传统卷快照，适用于 vSphere 的 SnapCenter VM 备份和其他基于 NetApp Snapshot 的备份，以及 vSphere 数据存储库中任何不常用的块，例如 VM 模板和不常访问的 VM 数据。

非活动数据报告

ONTAP 中提供了非活动数据报告（IDR）功能，用于帮助评估可从聚合分层的冷数据量。默认情况下，ONTAP 9.6 会启用 IDR，并使用默认的 31 天散热策略来确定卷中的哪些数据处于非活动状态。



分层的冷数据量取决于卷上设置的分层策略。此数量可能与 IDR 使用默认 31 天冷却期检测到的冷数据量不同。

对象创建和数据移动

FabricPool 可在 NetApp WAFL 块级别运行，并可运行散热块，将这些块串联到存储对象中，然后将这些对象迁移到云层。每个 FabricPool 对象均为 4 MB，由 1,024 个 4 KB 块组成。根据领先云提供商的性能建议，对象大小固定为 4 MB，不能更改。如果读取冷块并使其变热，则只会提取 4 MB 对象中请求的块并将其移回性能层。整个对象和整个文件都不会迁移回。仅迁移必要的块。



如果 ONTAP 检测到顺序读取的机会，则会在读取数据块之前从云层请求数据块以提高性能。

默认情况下，只有在性能聚合利用率超过 50% 时，才会将数据移至云层。可以将此阈值设置为较低的百分比，以便将性能闪存层上的少量数据存储移至云。如果分层策略是仅在聚合接近容量时移动冷数据，则这可能很有用。

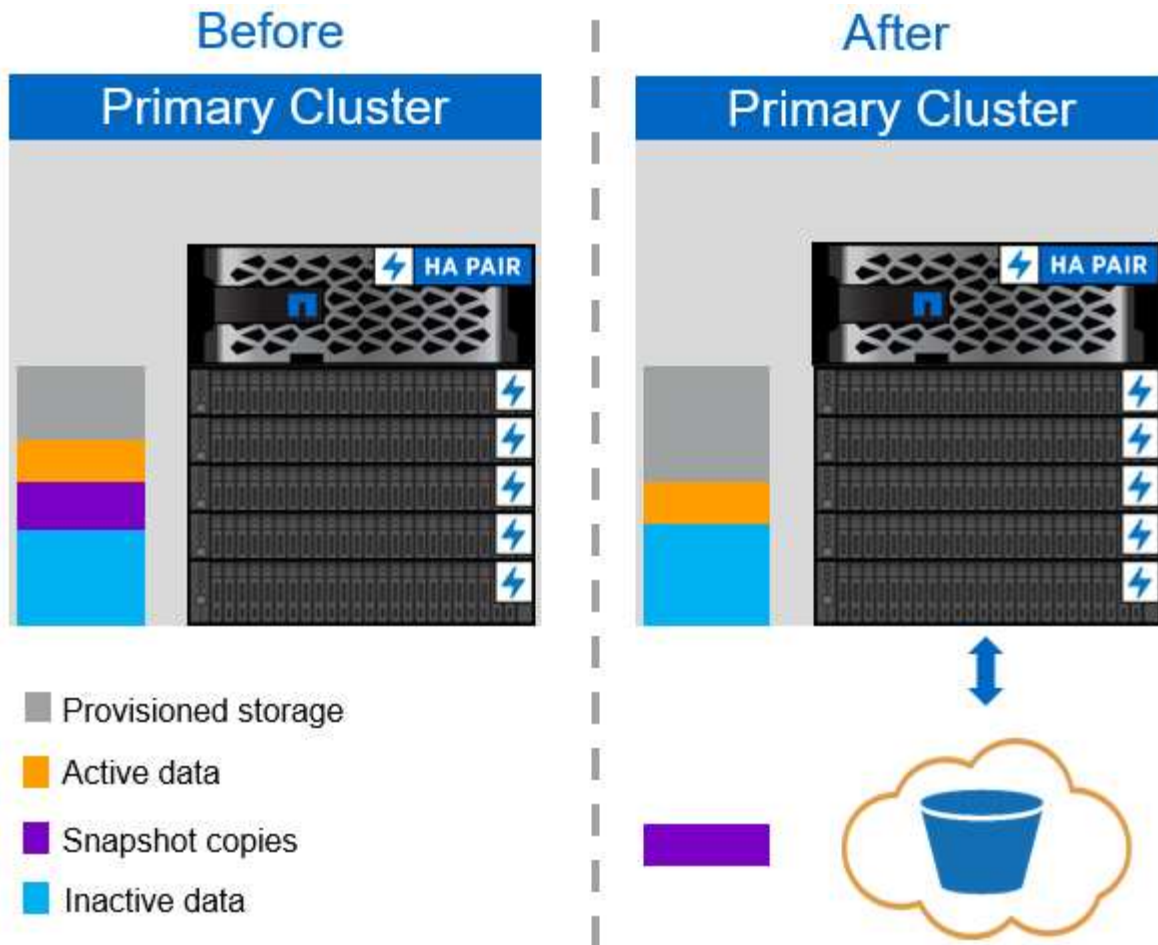
如果性能层利用率超过 70% 的容量，则冷数据将直接从云层读取，而不会回写到性能层。通过防止对使用率较高的聚合执行冷数据回写，FabricPool 可保留聚合以用于活动数据。

回收性能层空间

如前文所述，FabricPool 的主要使用情形是帮助最高效地使用高性能内部闪存存储。FlexPod 虚拟基础架构的卷快照和 VM 备份形式的冷数据可能会占用大量昂贵的闪存存储。通过实施以下两种分层策略之一，可以释放有价值的性能层存储：仅快照或自动。

仅 Snapshot 分层策略

下图所示的仅 Snapshot 分层策略将占用空间但未与活动文件系统共享块的 VM 的冷卷快照数据和 SnapCenter for vSphere 备份移动到云对象存储中。仅 Snapshot 分层策略会将冷数据块移至云层。如果需要还原，则云中的冷块会变热并移回内部的性能闪存层。



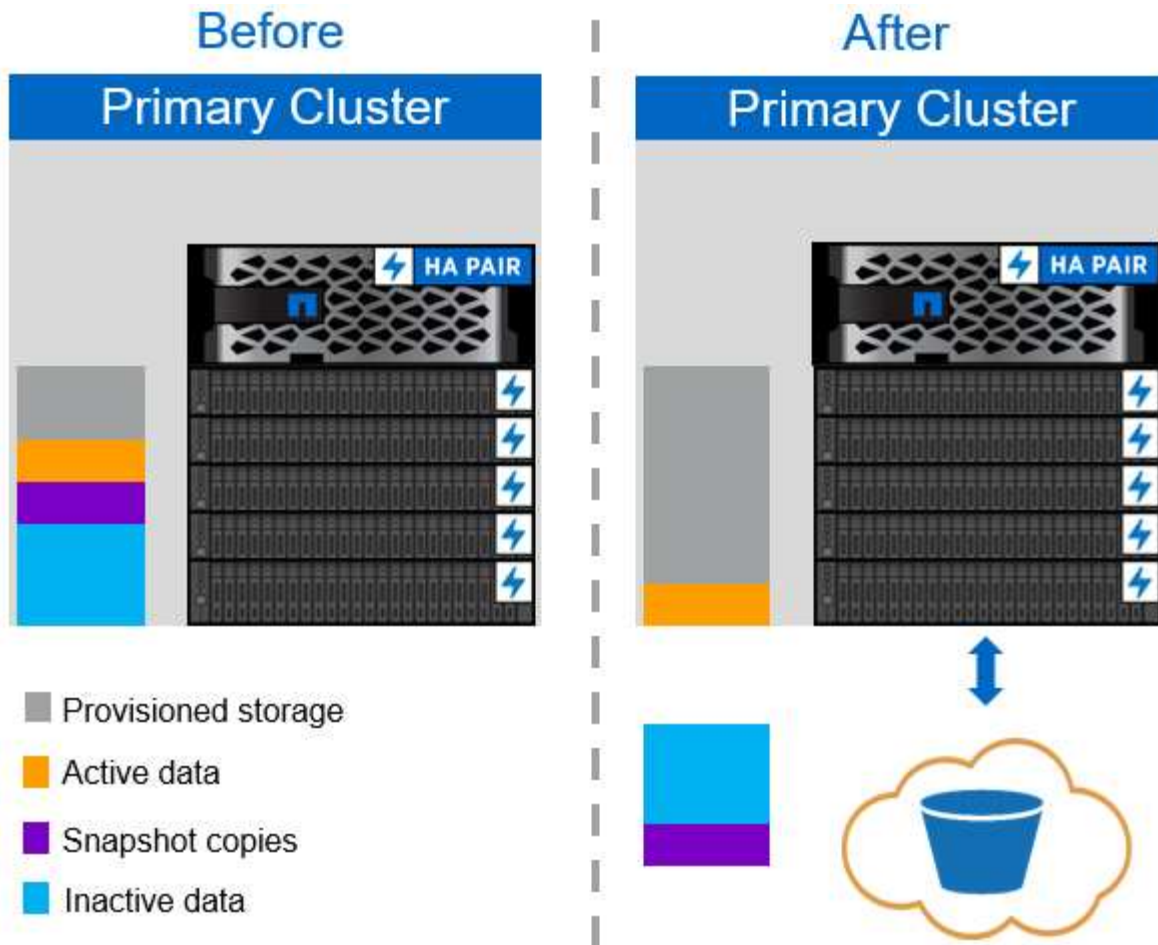
自动分层策略

下图所示的 FabricPool 自动分层策略不仅会将冷快照数据块移至云，还会移动活动文件系统中的任何冷块。这可能包括 VM 模板以及数据存储库卷中未使用的任何 VM 数据。移动哪些冷块由卷的 `tiering-minimum-cooling-days` 设置控制。如果应用程序随机读取云层中的冷块，则这些块会变热并恢复到性能层。但是，如果冷块通过防病毒扫描程序等顺序进程读取，则这些块将保持冷状态并保留在云对象存储中；它们不会移回性能层。

使用自动分层策略时，不常访问的热块将以云连接的速度从云层中回滚。如果应用程序对延迟敏感，则可能会影响虚拟机性能，在对数据存储库使用自动分层策略之前，应考虑这一点。NetApp 建议将集群间 LIF 放置在速度为 10GbE 的端口上，以获得足够的性能。



在将对象存储附加到 FabricPool 聚合之前，应使用对象存储配置器测试该对象存储的延迟和吞吐量。



所有分层策略

与 "自动" 和 "仅 Snapshot" 策略不同，所有分层策略会将整个数据卷立即移动到云层。此策略最适合二级数据保护或归档卷，对于这些卷，数据必须出于历史或法规目的进行保留，但很少被访问。不建议对 VMware 数据存储库卷使用 all 策略，因为写入数据存储库的任何数据都会立即移至云层。后续读取操作将从云执行，可能会给驻留在数据存储库卷中的 VM 和应用程序带来性能问题。

安全性

安全性是云和 FabricPool 关注的核心问题。性能层支持 ONTAP 的所有原生安全功能，在将数据传输到云层时，数据移动也会受到保护。FabricPool 使用 "AES-256-GCM" 在性能层上使用加密算法，并将此加密端到云层进行维护。移动到云对象存储的数据块通过传输层安全（Transport Layer Security，TLS）v1.2 进行保护，以保持存储层之间的数据机密性和完整性。



支持通过未加密连接与云对象存储进行通信，但 NetApp 不建议这样做。

数据加密

数据加密对于保护知识产权，贸易信息和个人身份客户信息至关重要。FabricPool 完全支持 NetApp 卷加密（NetApp Volume Encryption，NVE）和 NetApp 存储加密（NetApp Storage Encryption，NSE），以维护现有数据保护策略。将性能层上的所有加密数据移动到云层时，这些数据仍保持加密状态。客户端加密密钥归 ONTAP 所有，服务器端对象存储加密密钥归相应的云对象存储所有。未使用 NVE 加密的任何数据都将使用 AES-256-GCM 算法进行加密。不支持其他 AES-256 密码。



使用 NSE 或 NVE 是可选的，使用 FabricPool 不需要。

FabricPool 要求

FabricPool 要求使用 ONTAP 9.2 或更高版本，并在本节列出的任何平台上使用 SSD 聚合。其他 FabricPool 要求取决于所附加的云层。对于容量固定且相对较小的入门级 AFF 平台，例如 NetApp AFF C190，FabricPool 可以非常高效地将非活动数据移至云层。

平台

以下平台支持 FabricPool：

- NetApp AFF
 - A800
 - A700S，A700
 - A320，A300
 - A220，A200
 - C190
 - AFF8080，AFF8060 和 AFF8040
- NetApp FAS
 - FAS9000
 - FAS8200
 - FAS8080，FAS8060 和 FAS8040
 - FAS2750，FAS2720
 - FAS2650，FAS2620



只有 FAS 平台上的 SSD 聚合才能使用 FabricPool。

- 云层
 - 阿里云对象存储服务（标准，不常访问）
 - Amazon S3（Standard，Standard-IA，One Zone-IA，智能分层）
 - Amazon Commercial Cloud Services（C2S）
 - Google Cloud Storage（多区域，区域，近线，冷线）
 - IBM Cloud Object Storage（标准，存储，冷存储，Flex）
 - Microsoft Azure Blob Storage（热存储和冷存储）

集群间 LIFs

使用 FabricPool 的集群高可用性（HA）对需要两个集群间逻辑接口（LIF）才能与云层进行通信。NetApp 建议在其他 HA 对上创建集群间 LIF，以便将云层无缝附加到这些节点上的聚合。

ONTAP 用于连接到 AWS S3 对象存储的 LIF 必须位于 10 Gbps 端口上。

如果在具有不同路由的节点上使用多个克隆用户 LIF，NetApp 建议将其放置在不同的 IP 空间中。在配置期间，FabricPool 可以从多个 IP 空间中进行选择，但无法选择 IP 空间中的特定集群间 LIF。



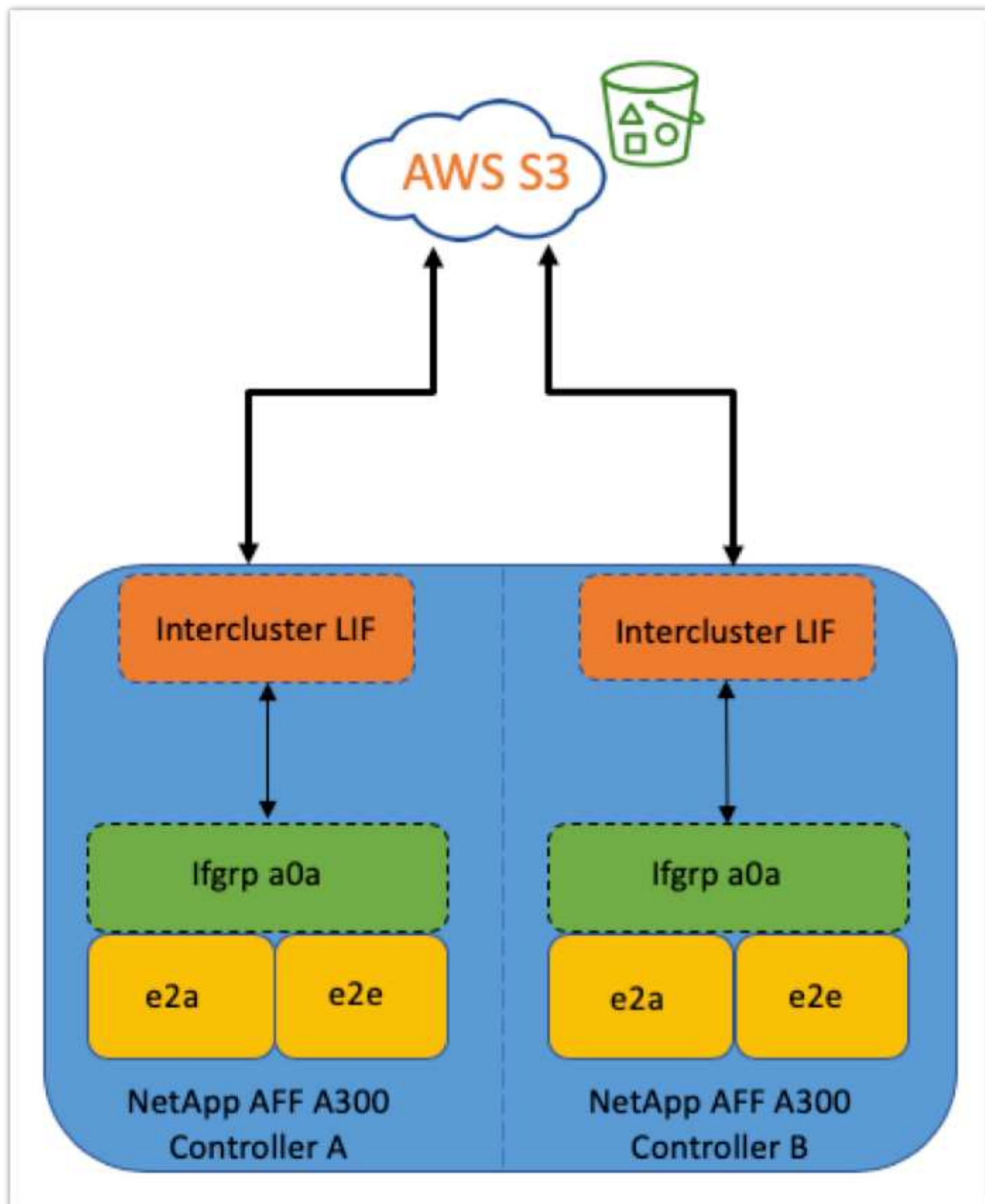
禁用或删除集群间 LIF 会中断与云层的通信。

连接

FabricPool 读取延迟是与云层连接的函数。使用 10 Gbps 端口的集群间 LIF（如下图所示）可提供充足的性能。NetApp 建议验证特定网络环境的延迟和吞吐量，以确定其对 FabricPool 性能的影响。



在低性能环境中使用 FabricPool 时，必须继续满足客户端应用程序的最低性能要求，并相应地调整恢复时间目标。



对象存储配置程序

对象存储配置程序（如下图所示）可通过 ONTAP 命令行界面访问，它可在将对象存储连接到 FabricPool 聚合之前测试这些对象存储的延迟和吞吐量性能。



必须先将云层添加到 ONTAP 中，然后才能将其与对象存储配置程序结合使用。

使用以下命令从 ONTAP 中的高级权限模式启动对象存储配置程序：

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

要查看结果，请运行以下命令：

```
storage aggregate object-store profiler show
```

云层提供的性能与性能层上的性能不同（通常为 GB/ 秒）。虽然 FabricPool 聚合可以轻松提供类似于 SATA 的性能，但对于不需要类似 SATA 的性能的分层解决方案，它们还可以承受高达 10 秒的延迟和低吞吐量。

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24
```

Op	Size	Total	Failed	Latency (ms)			Throughput
				min	max	avg	
PUT	4MB	1084	0	336	5951	2817	69.55MB
GET	4KB	158636	0	27	1132	41	32.22MB
GET	8KB	0	0	0	0	0	0B
GET	32KB	0	0	0	0	0	0B
GET	256KB	0	0	0	0	0	0B

```
5 entries were displayed.
```

Volumes

存储精简配置是 FlexPod 虚拟基础架构管理员的标准做法。NetApp Virtual Storage Console（VSC）无需任何空间保证（精简配置）即可为 VMware 数据存储库配置存储卷，并根据 NetApp 最佳实践使用优化的存储效率设置。如果使用 VSC 创建 VMware 数据存储库，则无需执行其他操作，因为不应为该数据存储库卷分配空间保证。



FabricPool 无法将云层附加到包含使用 " 无 " 以外的空间保证的卷的聚合（例如 " 卷 "）。

```
volume modify -space-guarantee none
```

设置 space-guarantee none 参数可为卷提供精简配置。此保证类型的卷所占用的空间量会随着数据的添加而增加，而不是由初始卷大小决定。这种方法对于 FabricPool 至关重要，因为卷必须支持热数据并恢复到性能层的云层数据。

许可

在为 AFF 和 FAS 混合闪存系统附加第三方对象存储提供程序（例如 Amazon S3）作为云层时，FabricPool 需要基于容量的许可证。

FabricPool 许可证以永久或按期限（1 年或 3 年）形式提供。

当存储在云层上的数据量（已用容量）达到许可容量时，分层到云层将停止。除非增加许可证容量，否则无法对其他数据进行分层，包括使用所有分层策略将 SnapMirror 副本分层到卷。虽然分层停止，但仍可从云层访问数据。在增加许可容量之前，其他冷数据仍会保留在 SSD 上。

购买任何新的 ONTAP 9.5 或更高版本的集群时都会附带一个 10 TB 容量的基于期限的免费 FabricPool 许可证，但可能会产生额外的支持成本。可以以 1 TB 为增量购买 FabricPool 许可证（包括现有许可证的额外容量）。

只能从不包含 FabricPool 聚合的集群中删除 FabricPool 许可证。



FabricPool 许可证在集群范围内有效。购买许可证时、您应具有UUID (cluster identify show)。有关其他许可信息，请参见 ["NetApp 知识库"](#)。

Configuration

软件版本

下表显示了经过验证的硬件和软件版本。

层	Device	图像	注释
存储	NetApp AFF A300	ONTAP 9.6P2	
计算	采用 Cisco UCS VIC 1340 的 Cisco UCS B200 M5 刀片式服务器	4.0 版（4b）	
网络	Cisco Nexus 6332-16UP 互联阵列	4.0 版（4b）	
	NX-OS 独立模式下的 Cisco Nexus 93180YC-EX 交换机	版本 7.0（3） i7（6）	
存储网络	Cisco MDS 9148S	8.3（2）版	
虚拟机管理程序		VMware vSphere ESXi 6.7U2	ESXi 6.7.013006603
		VMware vCenter Server	vCenter Server 6.7.0.30000 内部版本 13639309
云提供商		Amazon AWS S3	具有默认选项的标准 S3 存储分段

中概述了 FabricPool 的基本要求 ["FabricPool 要求"](#)。满足所有基本要求后，完成以下步骤以配置 FabricPool：

- 1. 安装 FabricPool 许可证。

2. 创建 AWS S3 对象存储分段。
3. 将云层添加到 ONTAP 。
4. 将云层附加到聚合。
5. 设置卷分层策略。

"下一步：安装 FabricPool 许可证。"

安装 FabricPool 许可证

获取 NetApp 许可证文件后，您可以使用 OnCommand System Manager 进行安装。要安装许可证文件，请完成以下步骤：

1. 单击配置。
2. 单击集群。
3. 单击许可证。
4. 单击添加。
5. 单击选择文件以浏览并选择文件。
6. 单击添加。

The screenshot shows the OnCommand System Manager interface. The left sidebar has a menu with 'Configuration' and 'Licenses' highlighted with red boxes. The main panel displays the 'Licenses' section with a table of installed licenses. A dialog box titled 'Add License Packages' is open, showing a text area for license keys and a 'License Files' section with a 'Choose Files' button.

Package	Entitlement Risk	Description
(DEPRECATED)-Cluster Base License	-NA-	Installed on a cluster
Trusted Platform Module License	-NA-	No License Available
FabricPool License	-NA-	Installed on a cluster
NFS License	Medium risk	Medium risk
CIFS License		
ISCSI License		
FCP License		
SnapRestore License		
SnapMirror License		
FlexClone License		
SnapVault License		
SnapLock License		

Add License Packages

Enter comma separated license keys

License Files

Browse to select a file... Choose Files

License files are required for features that use capacity based licenses. [Know more](#)

Add Cancel

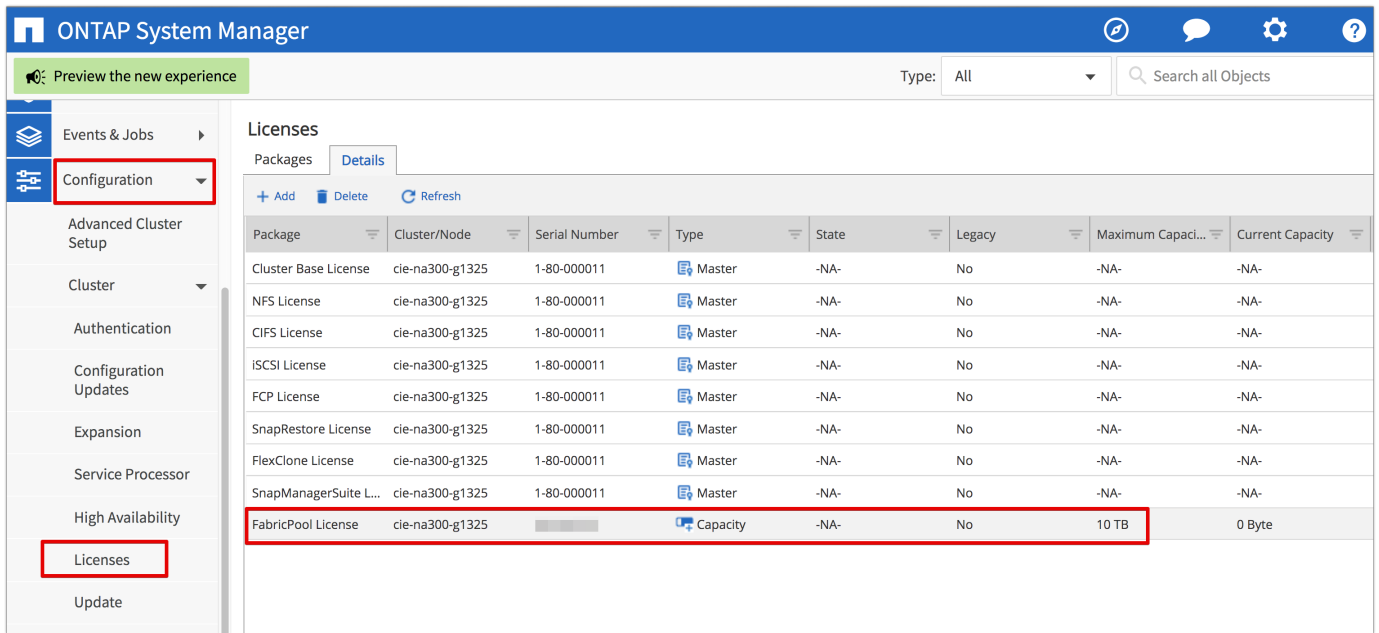
许可证容量

您可以使用 ONTAP 命令行界面或 OnCommand 系统管理器查看许可证容量。要查看许可的容量，请在 ONTAP 命令行界面中运行以下命令：

```
system license show-status
```

在 OnCommand 系统管理器中，完成以下步骤：

- 1. 单击配置。
- 2. 单击许可证。
- 3. 单击详细信息选项卡。



最大容量和当前容量列在 FabricPool 许可证行中。

"接下来：创建 AWS S3 存储分段。"

创建 AWS S3 存储分段

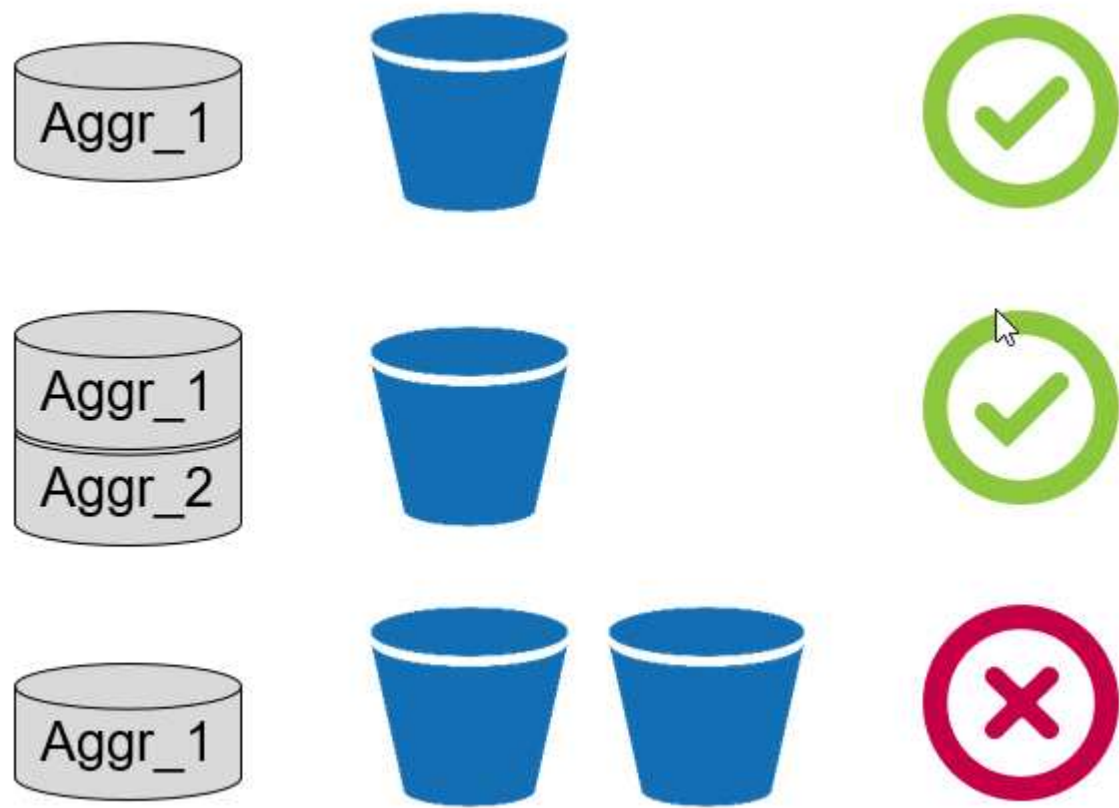
存储分段是用于保存数据的对象存储容器。您必须先提供存储数据的存储分段的名称和位置，然后才能将其作为云层添加到聚合中。

无法使用 OnCommand System Manager ， OnCommand Unified Manager 或 ONTAP 创建存储分段。

FabricPool 支持为每个聚合连接一个存储分段，如下图所示。一个存储分段可以附加到一个聚合，一个存储分段可以附加到多个聚合。但是，不能将单个聚合附加到多个分段。虽然一个存储分段可以附加到一个集群中的多个聚合，但 NetApp 不建议将一个存储分段附加到多个集群中的聚合。

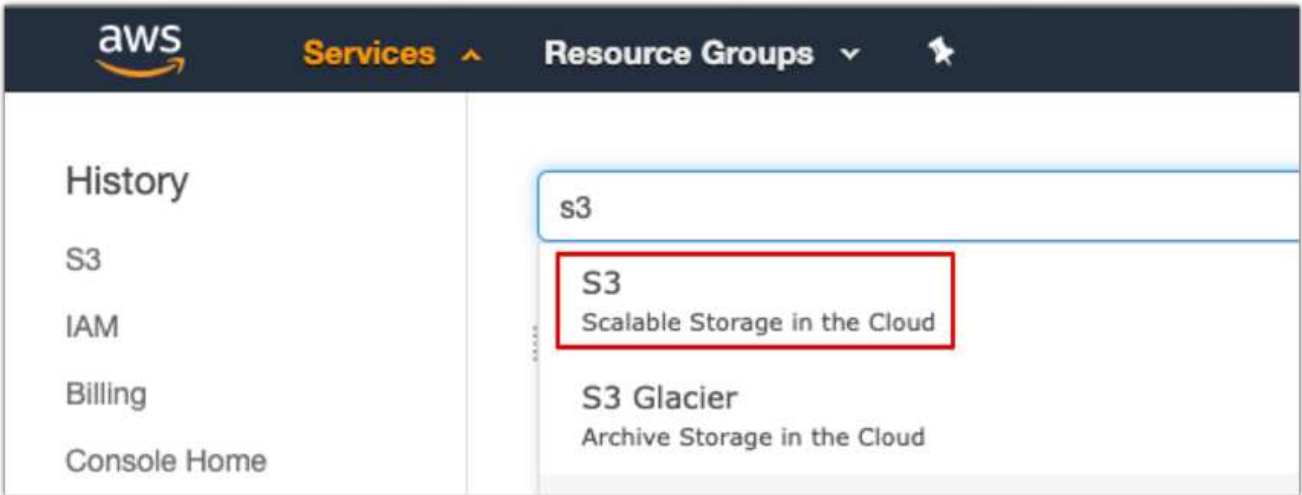
在规划存储架构时，请考虑分段到聚合关系可能会对性能产生何种影响。许多对象存储提供程序都会在存储分段

或容器级别设置支持的最大 IOPS 数。需要最高性能的环境应使用多个分段，以减少对象存储 IOPS 限制可能影响多个 FabricPool 聚合的性能的可能性。将单个存储分段或容器附加到集群中的所有 FabricPool 聚合对于重视易管理性而不是云层性能的环境来说，可能会更加有利。



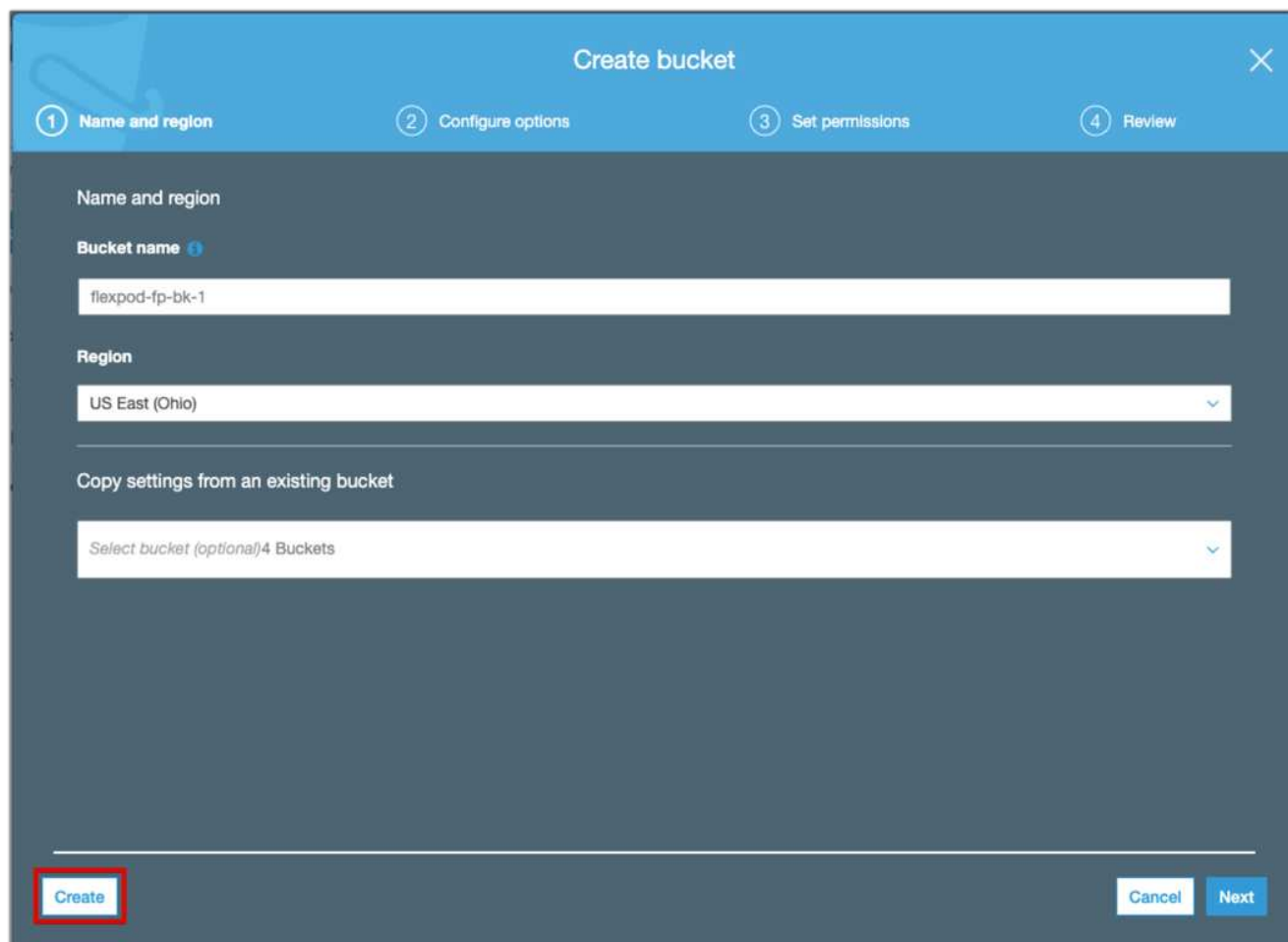
创建 S3 存储区。

1. 在 AWS 管理控制台中的主页页面中，在搜索栏中输入 s3 。
2. 在云中选择 S3 可扩展存储。



3. 在 S3 主页上，选择创建存储分段。

4. 输入符合 DNS 要求的名称，然后选择要创建存储分段的区域。



5. 单击创建以创建对象存储分段。

"接下来：将云层添加到 ONTAP"

将云层添加到 **ONTAP**

在将对象存储附加到聚合之前，必须将其添加到 ONTAP 并由其标识。可以使用 OnCommand 系统管理器或 ONTAP 命令行界面完成此任务。

FabricPool 支持将 Amazon S3，IBM 对象云存储和 Microsoft Azure Blob 存储对象存储作为云层。

您需要以下信息：

- 服务器名称（FQDN）；例如，`s3.amazonaws.com`
- 访问密钥 ID
- 机密密钥
- 容器名称（存储分段名称）

要使用 OnCommand System Manager 添加云层，请完成以下步骤：

- 1. 启动 OnCommand 系统管理器。
- 2. 单击存储。
- 3. 单击聚合和磁盘。
- 4. 单击 Cloud Tiers 。
- 5. 选择对象存储提供程序。
- 6. 根据需要填写对象存储提供程序的文本字段。

在容器名称字段中，输入对象存储的分段或容器名称。

- 7. 单击保存并附加聚合。

Add Cloud Tier

Cloud tiers/ object stores are used to store infrequently-accessed data. [Learn more](#)

Cloud Tier Provider

Amazon S3

Type

Amazon S3

Name

aws_infra_fp_bk_1

Server Name (FQDN)

s3.amazonaws.com

Access Key ID

Secret Key

Container Name

flexpod-fp-bkt-1

Encryption

Enabled

ONTAP 命令行界面

要使用 ONTAP 命令行界面添加云层，请输入以下命令：

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipSPACE default
```

"下一步：将云层附加到 ONTAP 聚合。"

将云层附加到 **ONTAP** 聚合

在将对象存储添加到 ONTAP 并由其标识后，必须将其附加到聚合才能创建 FabricPool。可以使用 OnCommand 系统管理器或 ONTAP 命令行界面完成此任务。

可以将多种类型的对象存储连接到一个集群，但每个聚合只能附加一种类型的对象存储。例如，一个聚合可以使用 Google Cloud，另一个聚合可以使用 Amazon S3，但一个聚合无法同时附加到这两个聚合。

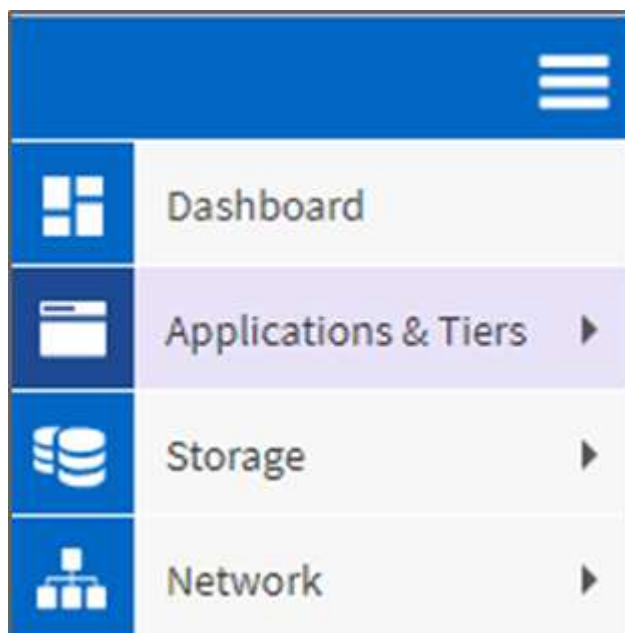


将云层附加到聚合是一项永久性操作。无法从已附加到的聚合中取消附加云层。

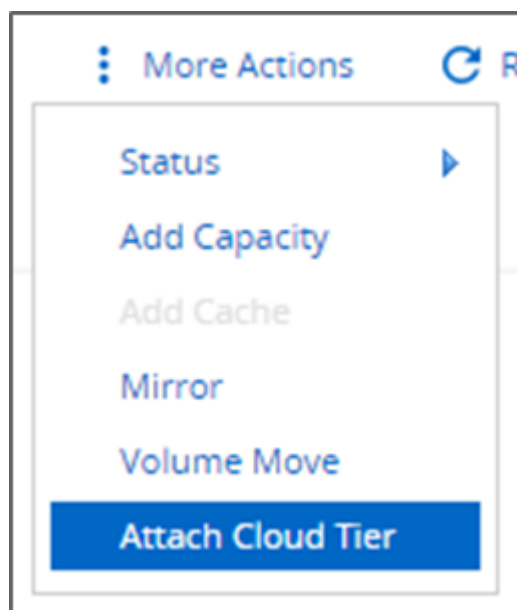
OnCommand 系统管理器

要使用 OnCommand System Manager 将云层附加到聚合，请完成以下步骤：

1. 启动 OnCommand 系统管理器。
2. 单击应用程序和层。



3. 单击存储层。
4. 单击某个聚合。
5. 单击操作并选择附加云层。



6. 选择云层。
7. 查看并更新聚合上卷的分层策略（可选）。默认情况下，卷分层策略设置为仅 Snapshot。
8. 单击保存。

ONTAP 命令行界面

要使用 ONTAP 命令行界面将云层附加到聚合，请运行以下命令：

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

示例

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"下一步：设置卷分层策略。"

设置卷分层策略

默认情况下，卷使用无卷分层策略。创建卷后，可以使用 OnCommand 系统管理器或 ONTAP 命令行界面更改卷分层策略。

在与 FlexPod 结合使用时，FabricPool 提供了三种卷分层策略：自动，仅 Snapshot 和无。

- * 自动 *

- 卷中的所有冷块都会移至云层。假设聚合的利用率超过 50%，则非活动块大约需要 31 天才能变冷。使用 `tiering-minimum-cooling-days` 设置，自动冷却期可在 2 天到 63 天之间进行调整。
- 如果随机读取卷中分层策略设置为 "自动" 的冷块，则这些冷块会变热并写入性能层。
- 如果卷中分层策略设置为自动的冷块按顺序读取，则这些冷块将保持冷状态并保留在云层上。它们不会写入性能层。

- * 仅 Snapshot *

- 卷中未与活动文件系统共享的冷 Snapshot 块将移至云层。假设聚合的利用率超过 50%，则非活动快照块变冷大约需要 2 天时间。使用 `tiering-minimum-cooling-days` 设置，仅 Snapshot 散热期可从 2 天调整为 63 天。
- 读取卷中分层策略设置为仅 Snapshot 的冷块时，这些冷块会变热并写入性能层。

- * 无（默认） *

- 设置为使用无作为分层策略的卷不会将冷数据分层到云层。
- 将分层策略设置为无会阻止新的分层。
- 先前已移至云层的卷数据将保留在云层中，直到变热为止，并会自动移回性能层。

OnCommand 系统管理器

要使用 OnCommand 系统管理器更改卷的分层策略，请完成以下步骤：

1. 启动 OnCommand 系统管理器。
2. 选择一个卷。
3. 单击更多操作并选择更改分层策略。
4. 选择要应用于卷的分层策略。
5. 单击保存。

CHANGE VOLUME TIERING POLICY

Select the tiering policy that you want to apply for the selected volume.

Volume Name	Tiering Policy
affa3..._fp_1	auto

Tiering Policy

- snapshot-only
- none
- auto
- all

Save Cancel

ONTAP 命令行界面

要使用 ONTAP 命令行界面更改卷的分层策略，请运行以下命令：

```
volume modify -vserver <svm_name> -volume <volume_name>  
-tiering-policy <auto|snapshot-only|all|none>
```

"下一步：设置卷分层最小冷却天数。"

设置卷分层最小冷却天数

`tiering-minimum-cooling-days` 设置可确定在使用自动或仅 Snapshot 策略的卷中的非活动数据被视为冷数据并符合分层条件之前必须经过多少天。

自动

自动分层策略的默认 分层最小冷却天数 设置为 31 天。

由于读取会使块温度保持较高，因此增加此值可能会减少符合分层条件的数据量，并增加性能层上保留的数据量。

如果要将此值从默认 31 天减少，请注意，数据在标记为冷之前不应再处于活动状态。例如，如果多天工作负载要在第 7 天执行大量写入，则应将卷的 `tiering-minimum-cooling-days` 设置设置为不低于 8 天。



对象存储与文件或块存储不是事务存储。如果对卷中作为对象存储的文件进行更改，而这些文件的最小散热天数过长，则可能会创建新对象，碎片化现有对象，并增加存储效率低下的问题。

仅 Snapshot

仅 Snapshot 分层策略的默认 `tiering-minimum-cooling-days` 设置为 2 天。至少 2 天可以为后台进程提供更多时间，以实现最高的存储效率，并防止日常数据保护进程不得不从云层读取数据。

ONTAP 命令行界面

要使用 ONTAP 命令行界面更改卷的 `tiering-minimum-cooling-days` 设置，请运行以下命令：

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum  
-cooling-days <2-63>
```

需要高级权限级别。



在自动和仅 Snapshot 之间更改分层策略（反之亦然）会重置性能层上块的非活动时间。例如，如果将分层策略设置为仅 Snapshot，则使用自动卷分层策略且性能层上的数据处于非活动状态 20 天的卷将性能层数据非活动重置为 0 天。

性能注意事项

调整性能层的大小

在考虑规模估算时，请记住，性能层应能够执行以下任务：

- 支持热数据
- 支持冷数据，直到分层扫描将数据移至云层
- 支持热数据并写入到性能层的云层数据
- 支持与附加云层关联的 WAFL 元数据

对于大多数环境，FabricPool 聚合上的性能容量比为 1：10 非常保守，同时可显著节省存储空间。例如，如果要 200 TB 分层到云层，则性能层聚合至少应为 20 TB。



如果性能层容量大于 70%，则从云层写入到性能层将被禁用。如果发生这种情况，则直接从云层读取块。

调整云层大小

在考虑规模估算时，充当云层的对象存储应能够执行以下任务：

- 支持读取现有冷数据
- 支持写入新冷数据
- 支持对象删除和碎片整理

拥有成本

。“FabricPool 经济计算器”可通过独立 IT 分析机构 Evaluator Group 获得，帮助预测内部和云之间在冷数据存储方面的成本节省。该计算器提供了一个简单的界面，用于确定在性能层上存储不常访问的数据的成本，而不是在数据生命周期的剩余时间将其发送到云层。根据 5 年的计算结果，我们会利用源容量，数据增长，快照容量和冷数据百分比这四个关键因素来确定该时间段内的存储成本。

结论

云之旅因组织，业务单位甚至组织内的业务单位而异。有些选择采用速度较快，而另一些则采用较为保守的方法。无论企业规模大小如何，采用云的速度如何，FabricPool 都能融入云战略，进一步展示了 FlexPod 基础架构的效率和可扩展性优势。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- FabricPool 最佳实践

["www.netapp.com/us/media/tr-4598.pdf"](http://www.netapp.com/us/media/tr-4598.pdf)

- NetApp 产品文档

["https://docs.netapp.com"](https://docs.netapp.com)

- TR-4036 : 《 FlexPod 数据中心技术规格》

["https://www.netapp.com/us/media/tr-4036.pdf"](https://www.netapp.com/us/media/tr-4036.pdf)

适用于混合云的**FlexPod** 数据中心与**Cisco CloudCenter**和**NetApp**私有存储—设计

NetApp公司Cisco David Arnette Haseeb Niazi

Cisco Validated Design (CVD)提供经过设计、测试和记录的系统 and 解决方案、以促进和改进客户部署。这些设计将广泛的技术和产品融入到了一系列解决方案中、这些解决方案是为满足客户的业务需求而开发的、并为客户从设计到部署提供指导。

["适用于混合云的FlexPod 数据中心与Cisco CloudCenter和NetApp私有存储—设计"](#)

版权信息

版权所有 © 2025 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。