NetApp公共云和混合云解决方案

NetApp public and hybrid cloud solutions

NetApp

November 11, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

目录

NetApp公共云和混合云解决方案 1
NetApp公有云和混合云解决方案的新功能 2
NetApp混合多云与 VMware 解决方案 3
VMware 的公有云 3
NetApp与 VMware 的混合多云概述 3
面向超大规模企业 VMware 的NetApp解决方案 6
NetApp混合多云与 VMware 支持的配置 9
超大规模配置中的 VMware 9
公共云中的NetApp存储 33
总结与结论： NetApp为何选择 VMware 作为混合多云平台 128
VMware 混合云用例 129
NetApp与 VMware 混合多云的用例 129
面向超大规模企业 VMware 的NetApp解决方案 130
适用于 Amazon VMware 托管云 (VMC) 的NetApp解决方案 131
适用于 Azure VMware 解决方案 (AVS) 的NetApp解决方案 131
适用于 Google Cloud VMware Engine (GCVE) 的NetApp解决方案 132
适用于 AWS/VMC 的NetApp 132
NetApp的 AWS VMC 功能 132
保护 AWS/VMC 上的工作负载 133
在 AWS/VMC 上迁移工作负载 243
适用于 AWS/EVS 的NetApp 256
将 FSx ONTAP挂载为 EVS 的外部数据存储 256
保护 EVS 的 FSx ONTAP 数据存储 280
NetApp适用于 Azure/AVS 313
NetApp的 Azure AVS 功能 313
保护 Azure/AVS 上的工作负载 315
在 Azure/AVS 上迁移工作负载 379
NetApp适用于 GCP/GCVE 392
NetApp针对 Google Cloud Platform GCVE 的功能 392
保护 GCP/GCVE 上的工作负载 393
迁移 GCP/GCVE 上的工作负载 424
使用Google Cloud NetApp Volumes保护 Google Cloud 中的数据 441
NetApp Disaster Recovery 499
针对 VMware 的 3-2-1 数据保护：使用 SnapCenter 插件和 NetApp Backup and Recovery 保护 VMware 工作负载 499
NetApp Disaster Recovery 532
NetApp混合多云与 Red Hat OpenShift 容器工作负载 572
开始使用 572
适用于 Red Hat OpenShift 容器工作负载的NetApp混合多云解决方案 572

NetApp混合多云解决方案针对 Red Hat OpenShift 容器工作负载的价值主张 574
NetApp混合多云支持 Red Hat OpenShift 容器工作负载的解决方案 574
解决方案验证中使用的各种组件的版本 578
支持NetApp Storage 与 Red Hat OpenShift Containers 的集成 579
其他文档 583
Openshift 适用于本地 583
NetApp解决方案与 VMware 上的 Red Hat OpenShift Container 平台工作负载 583
在 VMware 上部署和配置 Red Hat OpenShift Container 平台 584
使用Trident Protect 进行数据保护 586
具有自管理组件的混合云 587
NetApp解决方案与混合云中的 Red Hat OpenShift 容器平台工作负载 587
在 AWS 上部署和配置 Red Hat OpenShift Container 平台 589
在 Google Cloud 上部署和配置 Red Hat OpenShift 容器平台 591
在 Azure 上部署和配置 Red Hat OpenShift 容器平台 593
使用Trident Protect 进行数据保护 595
具有提供商管理组件的混合云 595
具有托管 Red Hat OpenShift 容器平台工作负载的NetApp解决方案 595
在 AWS 上部署和配置托管 Red Hat OpenShift 容器平台 596
使用Google Cloud NetApp Volumes在 Google Cloud 上部署和配置 OpenShift Dedicated 598
数据保护 600
适用于 Red Hat OpenShift 工作负载的其他NetApp混合多云解决方案 600
使用Trident Protect 保护数据 601
使用 Trident Protect 为 OpenShift Container Platform 中的 Container Apps 提供数据保护 601
使用 Trident Protect 保护 Red Hat OpenShift Virtualization 中的虚拟机 612
使用第三方工具保护容器应用 633
使用 OpenShift API for Data Protection (OADP) 为 OpenShift Container Platform 中的容器应用提供数据保护 633
OpenShift API for Data Protection (OADP) Operator 的安装 634
在 OpenShift Container Platform 中为应用程序创建按需备份 643
将应用程序从一个集群迁移到另一个集群 645
从备份恢复应用程序 650
使用 Velero 删除备份和恢复 656
观看有关NetApp混合多云解决方案的视频和演示 658
观看有关使用NetApp的 Amazon Web Services 混合多云解决方案的视频 658
来宾连接存储 658
TCO 和补充数据存储 658
迁移工作流程 (HCX) 658
观看有关使用NetApp的 Azure VMware 云的混合多云解决方案的视频 658
补充数据存储 658
灾难恢复 658
迁移工作流程 (HCX) 658

观看有关NetApp的 Red Hat OpenShift 混合多云解决方案的视频 659
快照和恢复 659
存储集成 659
故障转移和故障恢复 659
解决方案自动化 659
阅读NetApp专家的云解决方案博客 660
VMware 与 AWS 和Amazon FSx for ONTAP 的集成 660
Azure VMware 解决方案 660
Google Cloud VMware 引擎 660
数据保护和管理 660
NetApp适用于 OpenShift 容器工作负载 660
VMware 主权云 660
法律声明 661
版权 661
商标 661
专利 661
隐私政策 661

NetApp公共云和混合云解决方案

NetApp公有云和混合云解决方案的新功能

了解公共和混合云解决方案的新功能。

[[18-august-2025]]
== 2025年8月18日

NetApp解决方案网站现在是"NetApp解决方案系列"，其中包括以下网站：

- "NetApp人工智能解决方案"
- "NetApp容器解决方案"
- "NetApp数据管理解决方案"
- "NetApp数据库解决方案"
- NetApp公共云和混合云解决方案
- "适用于 SAP 的NetApp解决方案"
- "NetApp虚拟化解决方案"

NetApp混合多云与 VMware 解决方案

VMware 的公有云

NetApp与 VMware 的混合多云概述

大多数 IT 组织都遵循混合云优先方法。这些组织正处于转型阶段，客户正在评估其当前的 IT 环境，然后根据评估和发现练习将其工作负载迁移到云端。

客户迁移到云的因素可能包括弹性和爆发、数据中心退出、数据中心整合、生命周期终止场景、合并、收购等。迁移的原因可能因每个组织及其各自的业务优先级而异。当迁移到混合云时，选择正确的云存储对于释放云部署和弹性的威力非常重要。

公共云中的 VMware Cloud 选项

本节介绍每个云提供商如何在各自的公共云产品中支持 VMware 软件定义数据中心 (SDDC) 和/或 VMware Cloud Foundation (VCF) 堆栈。

Azure VMware 解决方案

Azure VMware 解决方案是一种混合云服务，允许在 Microsoft Azure 公共云中完全运行 VMware SDDC。Azure VMware 解决方案是完全由 Microsoft 管理和支持的第一方解决方案，并由 VMware 利用 Azure 基础架构进行了验证。这意味着，当部署 Azure VMware 解决方案时，客户可以获得 VMware 的 ESXi 用于计算虚拟化、vSAN 用于超融合存储以及 NSX 用于网络和安全，同时利用 Microsoft Azure 的全球影响力、一流的数据中心设施以及靠近丰富的原生 Azure 服务和解决方案生态系统的优势。

AWS 上的 VMware Cloud

VMware Cloud on AWS 将 VMware 的企业级 SDDC 软件引入 AWS 云，并优化了对原生 AWS 服务的访问。VMware Cloud on AWS 由 VMware Cloud Foundation 提供支持，集成了 VMware 的计算、存储和网络虚拟化产品（VMware vSphere、VMware vSAN 和 VMware NSX）以及 VMware vCenter Server 管理，并针对专用、弹性、裸机 AWS 基础架构上运行进行了优化。

Google Cloud VMware 引擎

Google Cloud VMware Engine 是一款基础架构即服务 (IaaS) 产品，它基于 Google Cloud 高性能可扩展基础架构和 VMware Cloud Foundation 堆栈（VMware vSphere、vCenter、vSAN 和 NSX-T）构建。此服务可快速迁移至云端，将现有 VMware 工作负载从本地环境无缝迁移或扩展到 Google Cloud Platform，无需承担重构应用程序或重新调整运维的成本、精力或风险。这是一项由 Google 销售和支持的服务，并与 VMware 密切合作。

SDDC 私有云和NetApp Cloud Volumes 主机托管以最小的网络延迟提供最佳性能。

你可知道？

无论使用哪种云，部署 VMware SDDC 时，初始集群都包含以下产品：

- VMware ESXi 主机用于计算虚拟化，并使用 vCenter Server Appliance 进行管理
- VMware vSAN 超融合存储，整合了每个 ESXi 主机的物理存储资产

- VMware NSX 用于虚拟网络和安全，并使用 NSX Manager 集群进行管理

存储配置

对于计划托管存储密集型工作负载并在任何云托管 VMware 解决方案上进行扩展的客户，默认的超融合基础架构要求扩展应同时在计算和存储资源上进行。

通过与NetApp Cloud Volumes（例如Azure NetApp Files、 Amazon FSx ONTAP、 Cloud Volumes ONTAP （适用于所有三大超大规模服务器）以及适用于 Google Cloud 的Google Cloud NetApp Volumes ）集成，客户现在可以选择单独扩展其存储，并且仅根据需要向 SDDC 集群添加计算节点。

注：

- VMware 不建议不平衡的集群配置，因此扩展存储意味着添加更多主机，这意味着更多的 TCO。
- 仅可以有一个 vSAN 环境。因此，所有存储流量都将直接与生产工作负载竞争。
- 没有提供多个性能层来满足应用程序要求、性能和成本的选项。
- 建立在集群主机之上的 vSAN 的存储容量很容易达到极限。使用NetApp Cloud Volumes 扩展存储以托管活动数据集或将较冷的数据分层到持久存储。

Azure NetApp Files、 Amazon FSx ONTAP、 Cloud Volumes ONTAP （三大超大规模服务器均可使用）以及适用于 Google Cloud 的Google Cloud NetApp Volumes可与来宾虚拟机结合使用。这种混合存储架构由保存客户操作系统和应用程序二进制数据的 vSAN 数据存储组成。应用程序数据通过基于来宾的 iSCSI 启动器或 NFS/SMB 挂载附加到虚拟机，这些挂载分别与Amazon FSx ONTAP、Cloud Volume ONTAP、 Azure NetApp Files和 Google Cloud 的Google Cloud NetApp Volumes直接通信。这种配置使您可以轻松克服存储容量方面的挑战，就像使用 vSAN 一样，可用的空闲空间取决于所使用的松弛空间和存储策略。

让我们考虑一下 VMware Cloud on AWS 上的三节点 SDDC 集群：

- 三节点 SDDC 的总原始容量 = 31.1TB（每个节点大约 10TB）。
- 添加其他主机之前需要维护的松弛空间 = 25% = (.25 x 31.1TB) = 7.7TB。
- 扣除剩余空间后的可用原始容量 = 23.4TB
- 可用的有效空闲空间取决于所应用的存储策略。

  例如：

  - RAID 0 = 有效可用空间 = 23.4TB（可用原始容量/1）
  - RAID 1 = 有效可用空间 = 11.7TB（可用原始容量/2）
  - RAID 5 = 有效可用空间 = 17.5TB（可用原始容量/1.33）

因此，使用NetApp Cloud Volumes 作为客户机连接存储将有助于扩展存储和优化 TCO，同时满足性能和数据保护要求。

在撰写本文档时，客舱内存储是唯一可用的选项。

需要记住的要点

- 在混合存储模型中，将第 1 层或高优先级工作负载放置在 vSAN 数据存储上，以满足任何特定的延迟要求，因为它们是主机本身的一部分并且在附近。对于任何可以接受事务延迟的工作负载虚拟机，请使用客户机内

机制。

- 使用 NetApp SnapMirror 技术将工作负载数据从本地 ONTAP 系统复制到 Cloud Volumes ONTAP 或 Amazon FSx ONTAP，以使用块级机制轻松迁移。这不适用于 Azure NetApp Files 和 Google Cloud NetApp Volumes。要将数据迁移到 Azure NetApp Files 或 Google Cloud NetApp Volumes，请使用 NetApp XCP、NetApp Copy and Sync、rysnc 或 robocopy，具体取决于使用的文件协议。
- 测试表明，从相应的 SDDC 访问存储时会有 2-4ms 的额外延迟。在映射存储时，将此额外的延迟考虑进应用程序要求中。
- 为了在测试故障转移和实际故障转移期间挂载来宾连接的存储，请确保重新配置 iSCSI 启动器、为 SMB 共享更新 DNS、并在 fstab 中更新 NFS 挂载点。
- 确保虚拟机内部的 Microsoft 多路径 I/O (MPIO)、防火墙和磁盘超时注册表设置配置正确。

这仅适用于来宾连接的存储。

NetApp云存储的优势

NetApp云存储具有以下优势：

- 通过独立于计算扩展存储来提高计算到存储的密度。
- 允许您减少主机数量，从而降低总体 TCO。
- 计算节点故障不会影响存储性能。
- Azure NetApp Files的卷重塑和动态服务级别功能允许您通过调整稳定状态工作负载的大小来优化成本，从而防止过度配置。
- Cloud Volumes ONTAP的存储效率、云分层和实例类型修改功能允许以最佳方式添加和扩展存储。
- 防止过度配置存储资源，仅在需要时添加。
- 高效的 Snapshot 副本和克隆允许您快速创建副本而不会对性能产生任何影响。
- 通过使用 Snapshot 副本的快速恢复来帮助应对勒索软件攻击。
- 提供高效的基于增量块传输的区域灾难恢复和跨区域的集成备份块级别，提供更好的 RPO 和 RTO。

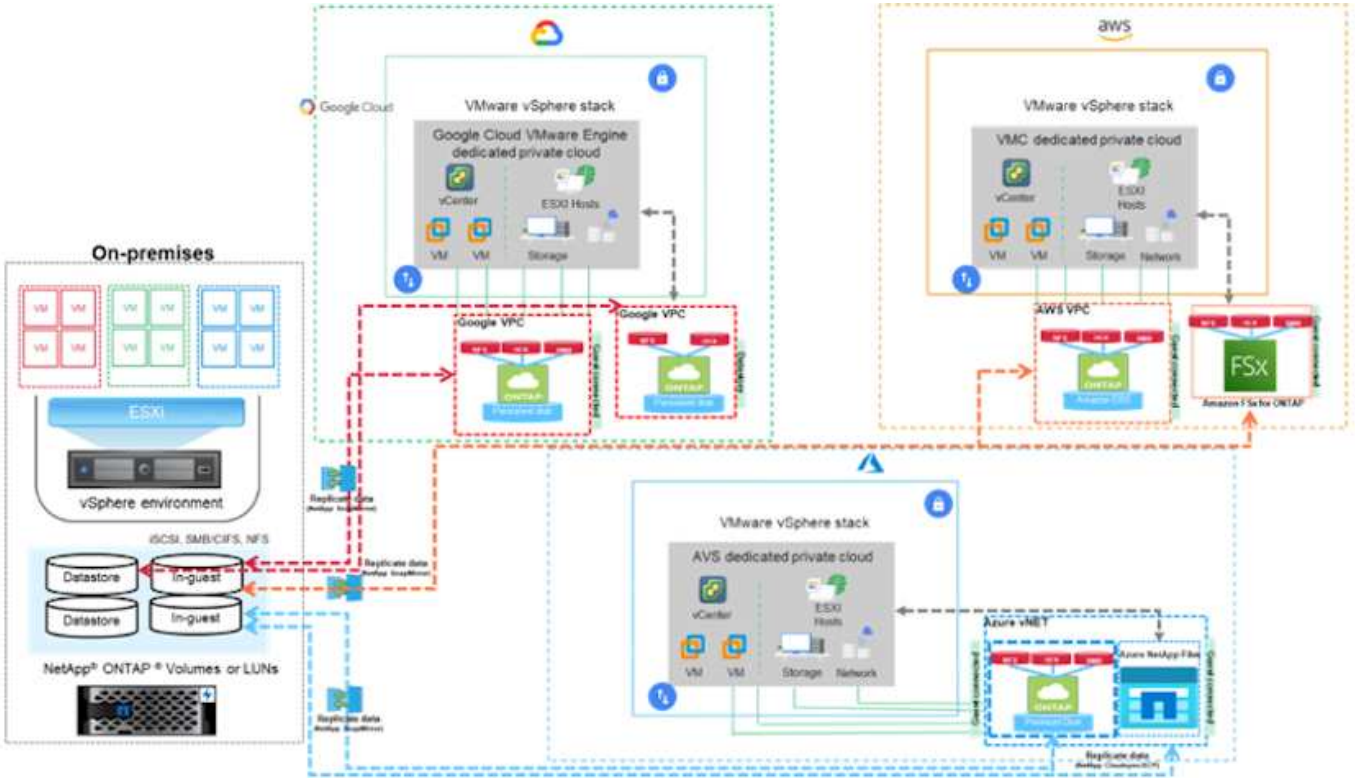
假设

- 启用SnapMirror技术或其他相关数据迁移机制。有许多连接选项，从本地到任何超大规模云。使用适当的路径并与相关的网络团队合作。
- 在撰写本文档时，客舱内存储是唯一可用的选项。

与NetApp解决方案架构师和相应的超大规模云架构师合作，规划和确定存储以及所需的主机数量。 NetApp建议在使用Cloud Volumes ONTAP大小调整器之前先确定存储性能要求，以确定存储实例类型或具有正确吞吐量的适当服务级别。

详细架构

从高层次的角度来看，该架构（如下图所示）涵盖了如何使用NetApp Cloud Volumes ONTAP、 Google Cloud NetApp Volumes for Google Cloud 和Azure NetApp Files作为额外的客户机存储选项，实现跨多个云提供商的混合多云连接和应用程序可移植性。



面向超大规模企业 **VMware** 的**NetApp**解决方案

详细了解NetApp为三大 (3) 个主要超大规模企业带来的功能 - 从NetApp作为来宾连接存储设备或补充 NFS 数据存储到迁移工作流、扩展/爆发到云、备份/恢复和灾难恢复。

选择您的云，让NetApp完成剩下的工作！



要查看特定超大规模器的功能，请单击该超大规模器的相应选项卡。

通过选择以下选项跳转到所需内容的部分：

- "超大规模配置中的 VMware"
- "NetApp存储选项"
- "NetApp /VMware 云解决方案"

超大规模配置中的 **VMware**

与本地一样，规划基于云的虚拟化环境对于成功创建虚拟机和迁移的生产就绪环境至关重要。

AWS/VMC

本节介绍如何设置和管理 VMware Cloud on AWS SDDC，并将其与可用于连接NetApp存储的选项结合使用。

客户机内存储是将Cloud Volumes ONTAP连接到 AWS VMC 的唯一支持方法。

设置过程可分为以下步骤：

- 部署和配置 VMware Cloud for AWS
- 将 VMware Cloud 连接到 FSx ONTAP

查看详细信息"VMC 的配置步骤"。

Azure/AVS

本部分介绍如何设置和管理 Azure VMware 解决方案，并将其与用于连接NetApp存储的可用选项结合使用。

来宾内存储是将Cloud Volumes ONTAP连接到 Azure VMware 解决方案的唯一支持方法。

设置过程可分为以下步骤：

- 注册资源提供者并创建私有云
- 连接到新的或现有的 ExpressRoute 虚拟网络网关
- 验证网络连接并访问私有云

查看详细信息"AVS配置步骤"。

良好操作规范/良好行为规范

本节介绍如何设置和管理 GCVE，以及如何将其与可用于连接NetApp存储的选项结合使用。

客户机内存储是将Cloud Volumes ONTAP和Google Cloud NetApp Volumes连接到 GCVE 的唯一支持方法。

设置过程可分为以下步骤：

- 部署和配置 GCVE
- 启用对 GCVE 的私人访问

查看详细信息"GCVE 的配置步骤"。

NetApp存储选项

NetApp存储可以在 3 个主要超大规模服务器中以多种方式使用 - 既可以作为客户机连接，也可以作为补充 NFS 数据存储。

请访问"支持的NetApp存储选项"了解更多信息。

AWS/VMC

AWS 支持以下配置的NetApp存储：

- FSx ONTAP作为来宾连接存储
- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- FSx ONTAP作为补充 NFS 数据存储

查看详细信息"VMC 的客户机连接存储选项"。查看详细信息"VMC 的补充 NFS 数据存储选项"。

Azure/AVS

Azure 支持以下配置的NetApp存储：

- Azure NetApp Files(ANF) 作为来宾连接存储
- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- Azure NetApp Files(ANF) 作为补充 NFS 数据存储

查看详细信息"AVS 的来宾连接存储选项"。查看详细信息"AVS 的补充 NFS 数据存储选项"。

良好操作规范/良好行为规范

Google Cloud 支持以下配置的NetApp存储：

- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- Google Cloud NetApp Volumes （NetApp Volumes）作为来宾连接存储
- Google Cloud NetApp Volumes （NetApp Volumes）作为补充 NFS 数据存储

查看详细信息"GCVE 的来宾连接存储选项"。查看详细信息"GCVE 的补充 NFS 数据存储选项"。

阅读更多"Google Cloud NetApp Volumes数据存储区支持 Google Cloud VMware Engine（NetApp博客）"或者"如何将Google Cloud NetApp Volumes用作 Google Cloud VMware Engine 的数据存储区（Google 博客）"

NetApp /VMware 云解决方案

借助NetApp和 VMware 云解决方案，许多用例都可以轻松地部署在您选择的超大规模中。 VMware 将主要的云工作负载用例定义为：

- 保护（包括灾难恢复和备份/还原）

- 迁移
- 延长

AWS/VMC

"浏览适用于 AWS/VMC 的NetApp解决方案"

Azure/AVS

"浏览适用于 Azure/AVS 的NetApp解决方案"

良好操作规范/良好行为规范

"浏览适用于 Google Cloud Platform (GCP)/GCVE 的NetApp解决方案"

NetApp混合多云与 VMware 支持的配置

了解主要超大规模企业对NetApp存储支持的组合。

	访客已连接	补充 **NFS** 数据存储
AWS	CVO FSx ONTAP"详细信息"	FSx ONTAP"详细信息"
蔚蓝	CVO ANF"详细信息"	心钠素"详细信息"
GCP	CVO NetApp卷"详细信息"	NetApp卷"详细信息"

超大规模配置中的 VMware

在云提供商中配置虚拟化环境

这里介绍了如何在每个受支持的超大规模器中配置虚拟化环境的详细信息。

AWS/VMC

本节介绍如何设置和管理 VMware Cloud on AWS SDDC，并将其与可用于连接NetApp存储的选项结合使用。

客户机内存储是将Cloud Volumes ONTAP连接到 AWS VMC 的唯一支持方法。

设置过程可分为以下步骤：

- 部署和配置 VMware Cloud for AWS
- 将 VMware Cloud 连接到 FSx ONTAP

查看详细信息"VMC 的配置步骤"。

Azure/AVS

本部分介绍如何设置和管理 Azure VMware 解决方案，并将其与用于连接NetApp存储的可用选项结合使用。

来宾内存储是将Cloud Volumes ONTAP连接到 Azure VMware 解决方案的唯一支持方法。

设置过程可分为以下步骤：

- 注册资源提供者并创建私有云
- 连接到新的或现有的 ExpressRoute 虚拟网络网关
- 验证网络连接并访问私有云

查看详细信息"AVS配置步骤"。

良好操作规范/良好行为规范

本节介绍如何设置和管理 GCVE，以及如何将其与可用于连接NetApp存储的选项结合使用。

客户机内存储是将Cloud Volumes ONTAP和Google Cloud NetApp Volumes连接到 GCVE 的唯一支持方法。

设置过程可分为以下步骤：

- 部署和配置 GCVE
- 启用对 GCVE 的私人访问

查看详细信息"GCVE 的配置步骤"。

在 **AWS** 上部署和配置虚拟化环境

与本地部署一样，规划 AWS 上的 VMware Cloud 对于成功创建虚拟机和迁移的生产就绪环境至关重要。

本节介绍如何设置和管理 VMware Cloud on AWS SDDC，并将其与可用于连接NetApp存储的选项结合使用。

目前，客户机内存储是将Cloud Volumes ONTAP (CVO) 连接到 AWS VMC 的唯一支持方法。

设置过程可分为以下步骤：

▼ 部署和配置 **VMware Cloud for AWS**

"AWS 上的 VMware Cloud"为 AWS 生态系统中基于 VMware 的工作负载提供云原生体验。每个 VMware 软件定义数据中心 (SDDC) 都在 Amazon 虚拟私有云 (VPC) 中运行，并提供完整的 VMware 堆栈（包括 vCenter Server）、NSX-T 软件定义网络、vSAN 软件定义存储以及一个或多个为您的工作负载提供计算和存储资源的 ESXi 主机。

本节介绍如何设置和管理 VMware Cloud on AWS，以及如何将其与具有客户机内存储的 AWS 上的Amazon FSx ONTAP和/或Cloud Volumes ONTAP结合使用。

目前，客户机内存储是将Cloud Volumes ONTAP (CVO) 连接到 AWS VMC 的唯一支持方法。

设置过程可分为三个部分：

▼ 注册 **AWS** 账户

注册"亚马逊网络服务账户"。

您需要一个 AWS 账户才能开始使用（假设尚未创建）。无论是新的还是现有的，您都需要帐户的管理权限才能执行此过程中的许多步骤。看看这个"链接"有关 AWS 凭证的更多信息。

▼ 注册 **My VMware** 帐户

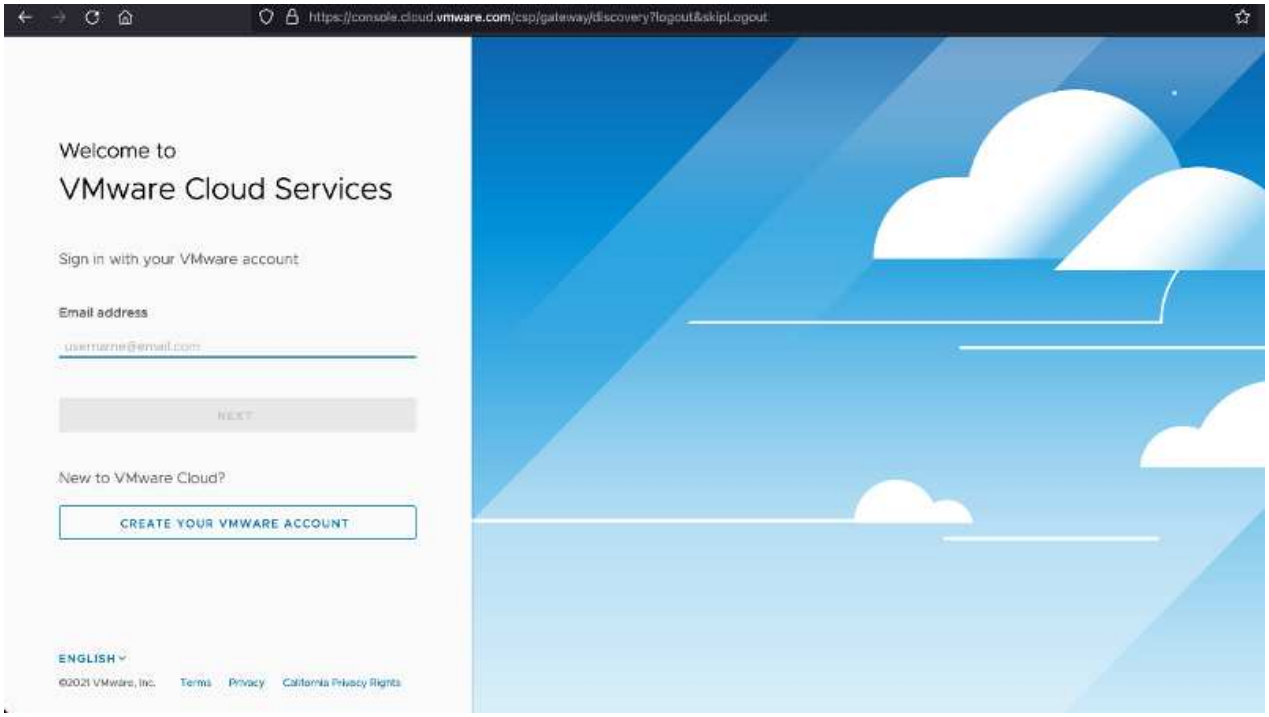
注册"我的 VMware"帐户。

要访问 VMware 的云产品组合（包括 AWS 上的 VMware Cloud），您需要一个 VMware 客户帐户或 My VMware 帐户。如果您尚未创建 VMware 帐户，请创建一个"此处"。

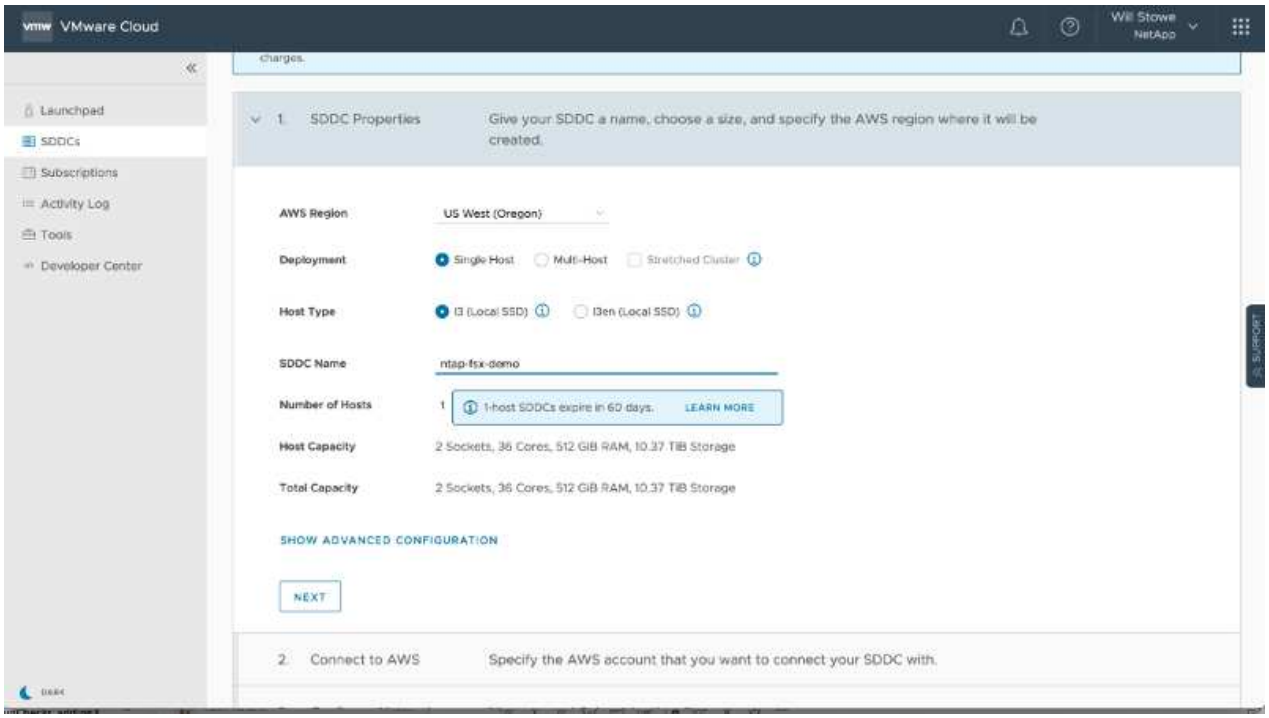
▼ 在 **VMware Cloud** 中调配 **SDDC**

配置 VMware 帐户并执行适当的大小调整后，部署软件定义数据中心是使用 VMware Cloud on AWS 服务的下一步。要创建 SDDC，请选择一个 AWS 区域来托管它，为 SDDC 命名，并指定您希望 SDDC 包含多少个 ESXi 主机。如果您还没有 AWS 帐户，您仍然可以创建包含单个 ESXi 主机的入门配置 SDDC。

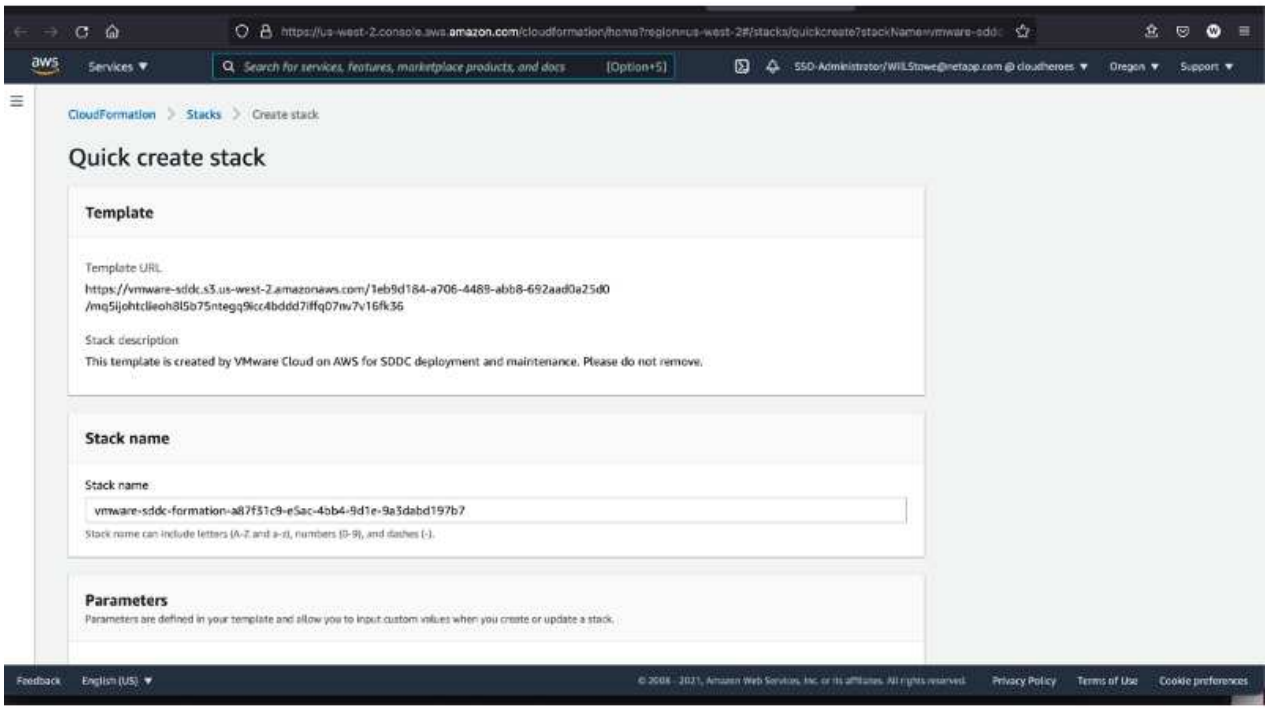
1. 使用现有或新创建的 VMware 凭据登录 VMware Cloud Console。

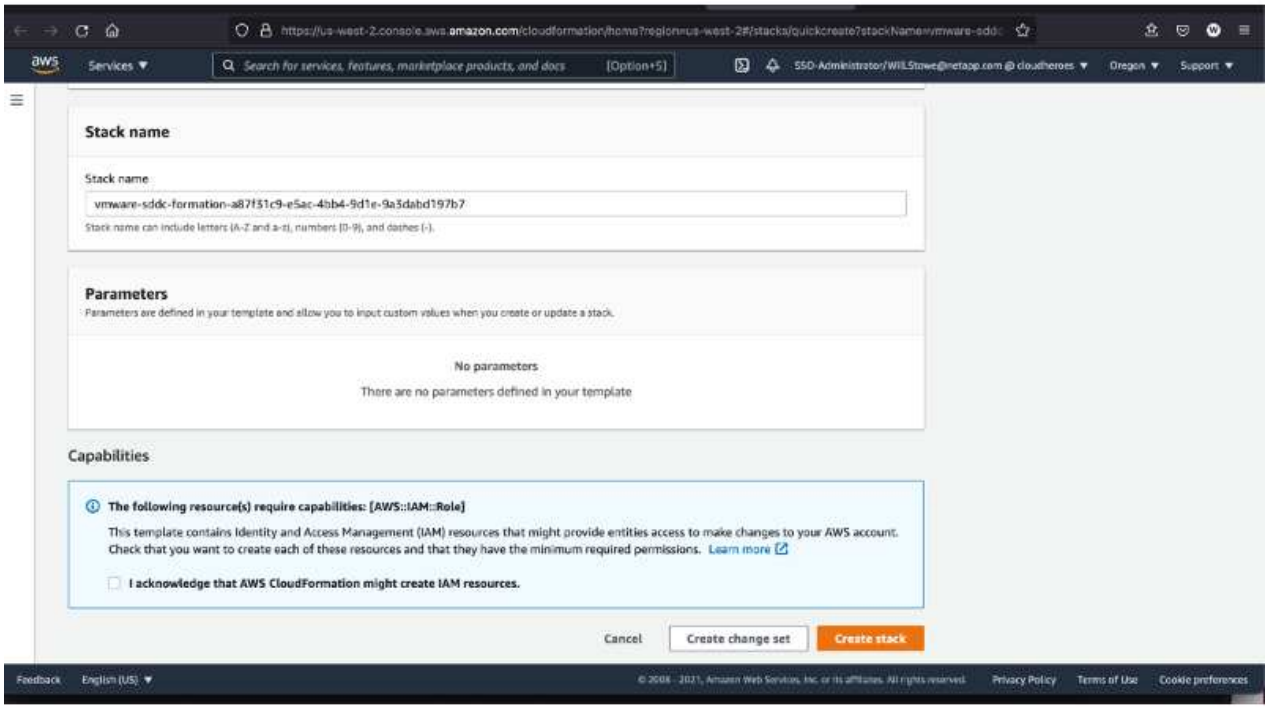


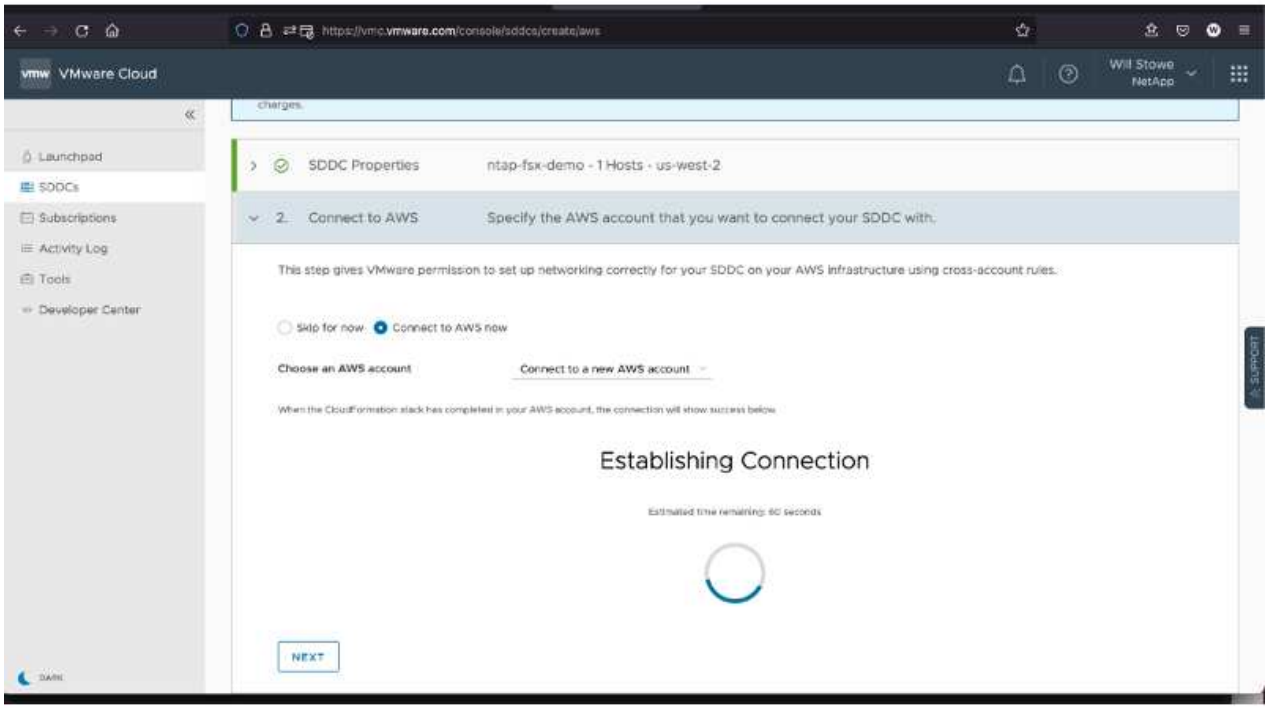
2. 配置 AWS 区域、部署、主机类型以及 SDDC 名称：

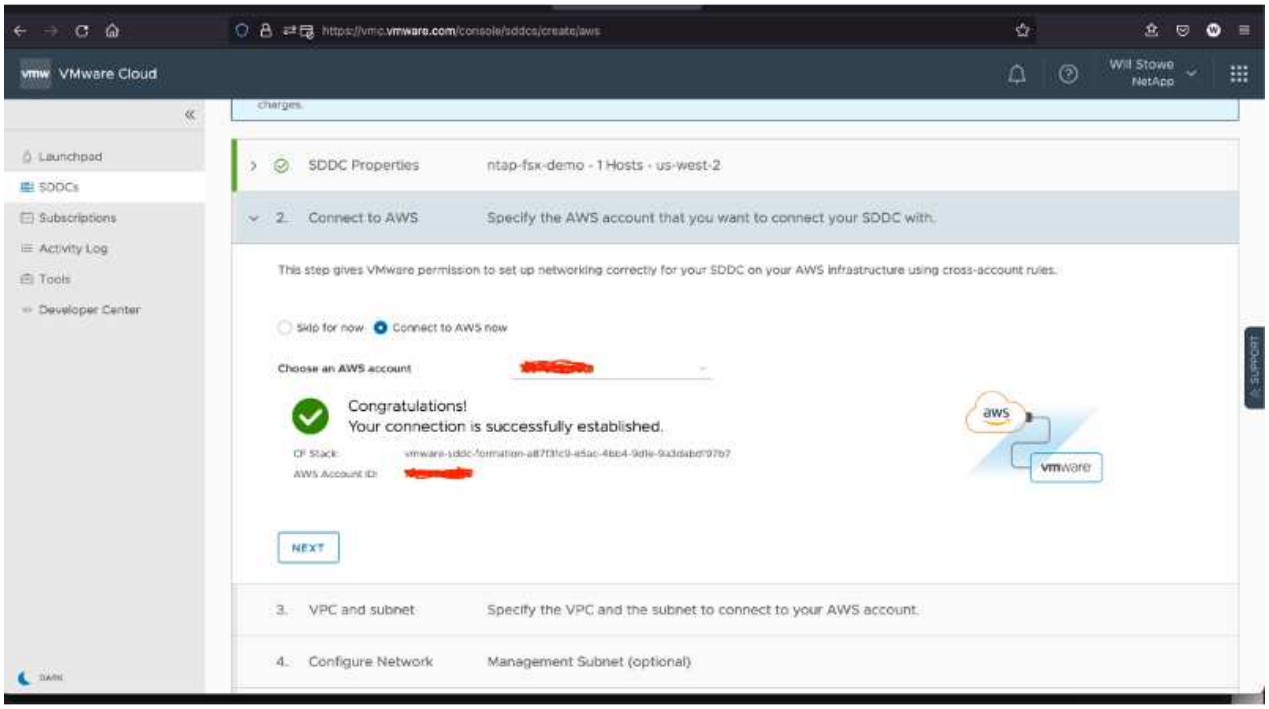


3. 连接到所需的 AWS 账户并执行 AWS Cloud Formation 堆栈。



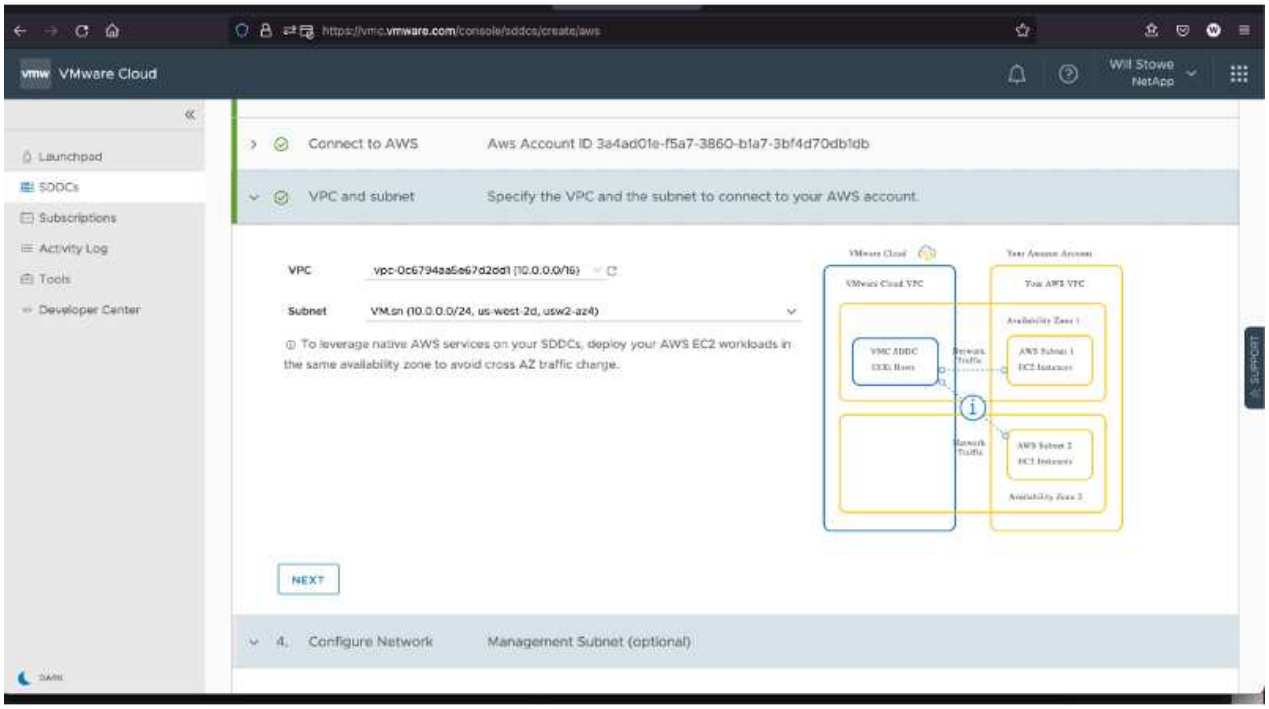

Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack


VMware Cloud
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
SDDC Properties
ntap-fsx-demo - 1 Hosts - us-west-2
2. Connect to AWS
Specify the AWS account that you want to connect your SDDC with.
This step gives VMware permission to set up networking correctly for your SDDC on your AWS infrastructure using cross-account rules.
Skip for now
Connect to AWS now
Choose an AWS account
Connect to a new AWS account
Establishing Connection
NEXT

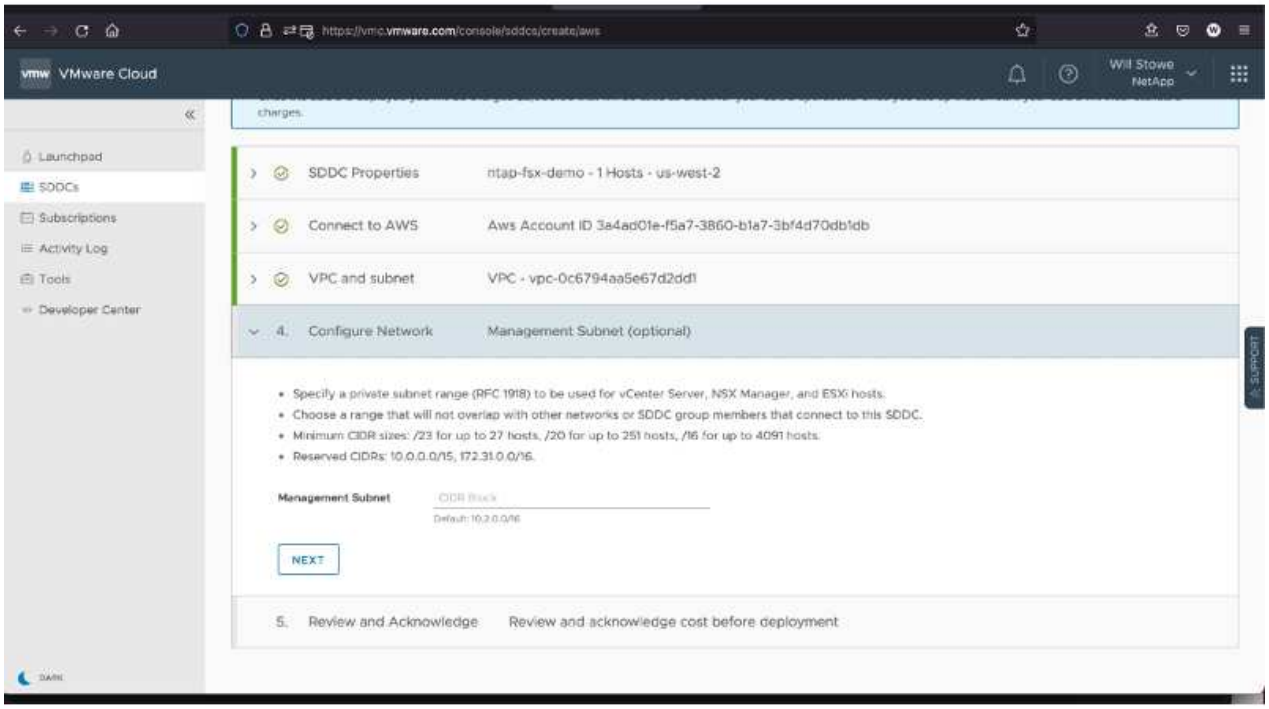


本次验证采用单主机配置。

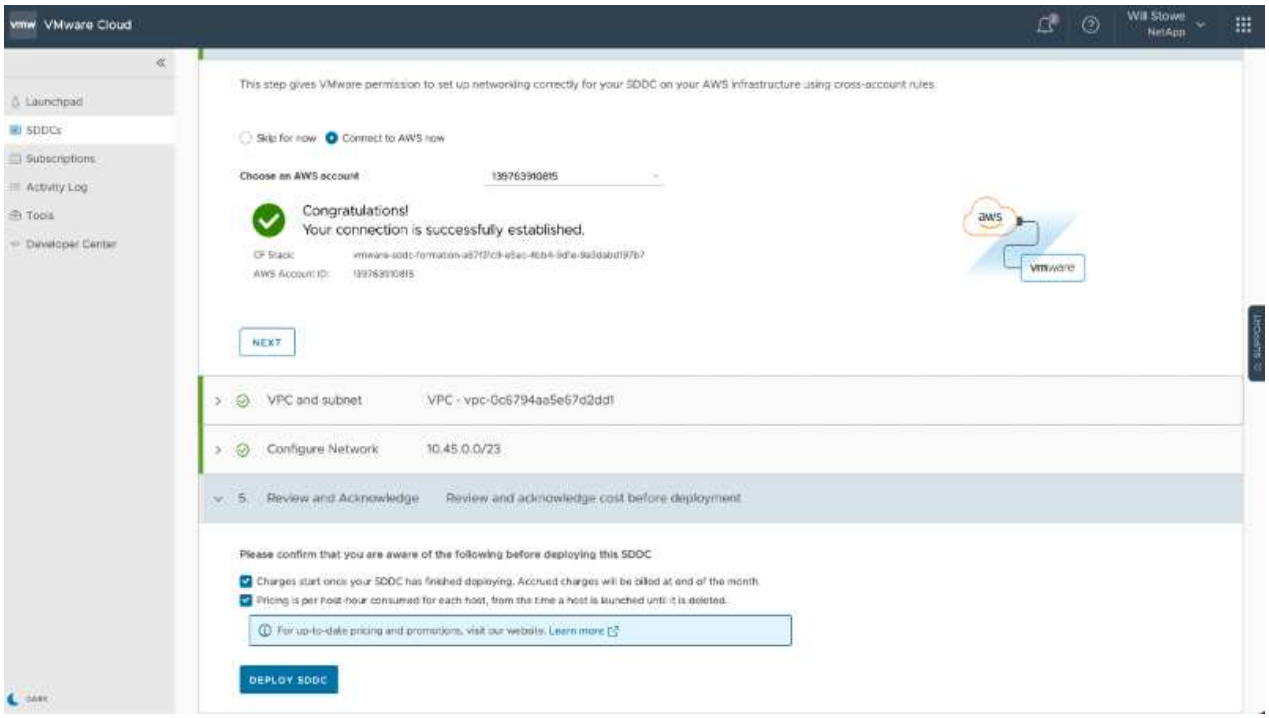
4. 选择所需的 AWS VPC 来连接 VMC 环境。



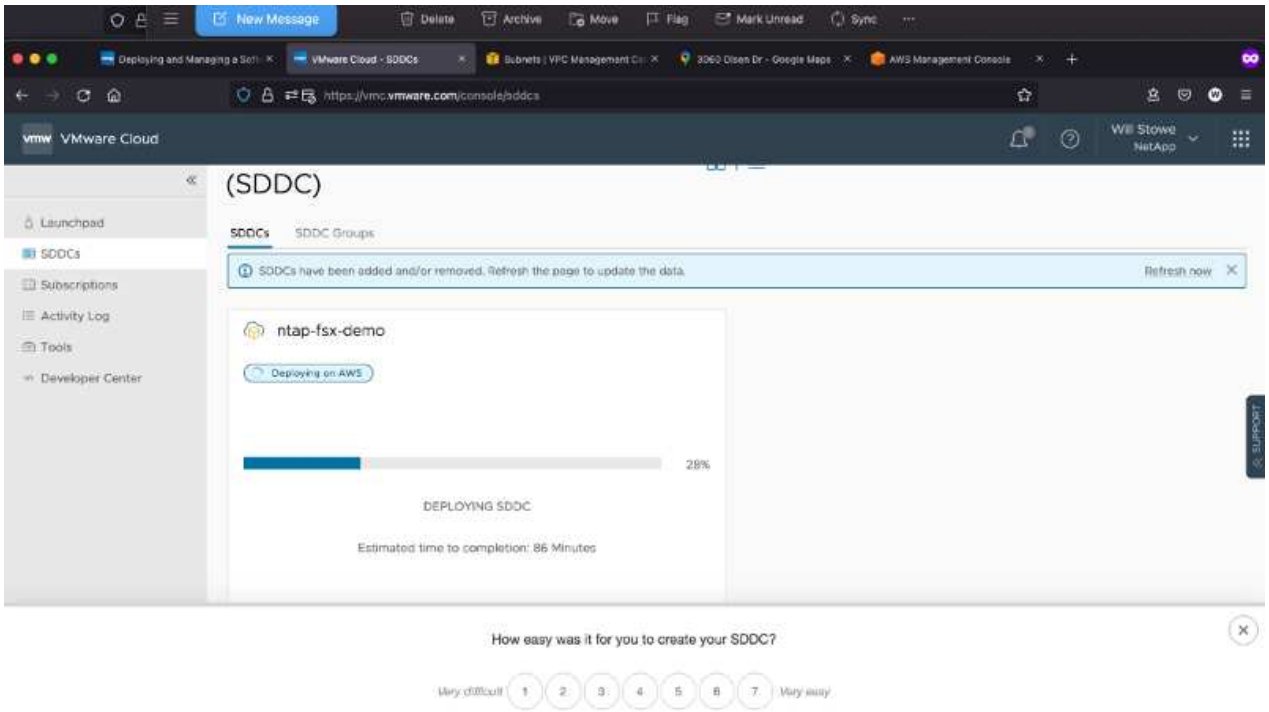
5. 配置 VMC 管理子网；此子网包含 VMC 管理的服务，如 vCenter、NSX 等。不要选择与任何其他需要连接到 SDDC 环境的网络重叠的地址空间。最后，请遵循下面注明的 CIDR 大小的建议。



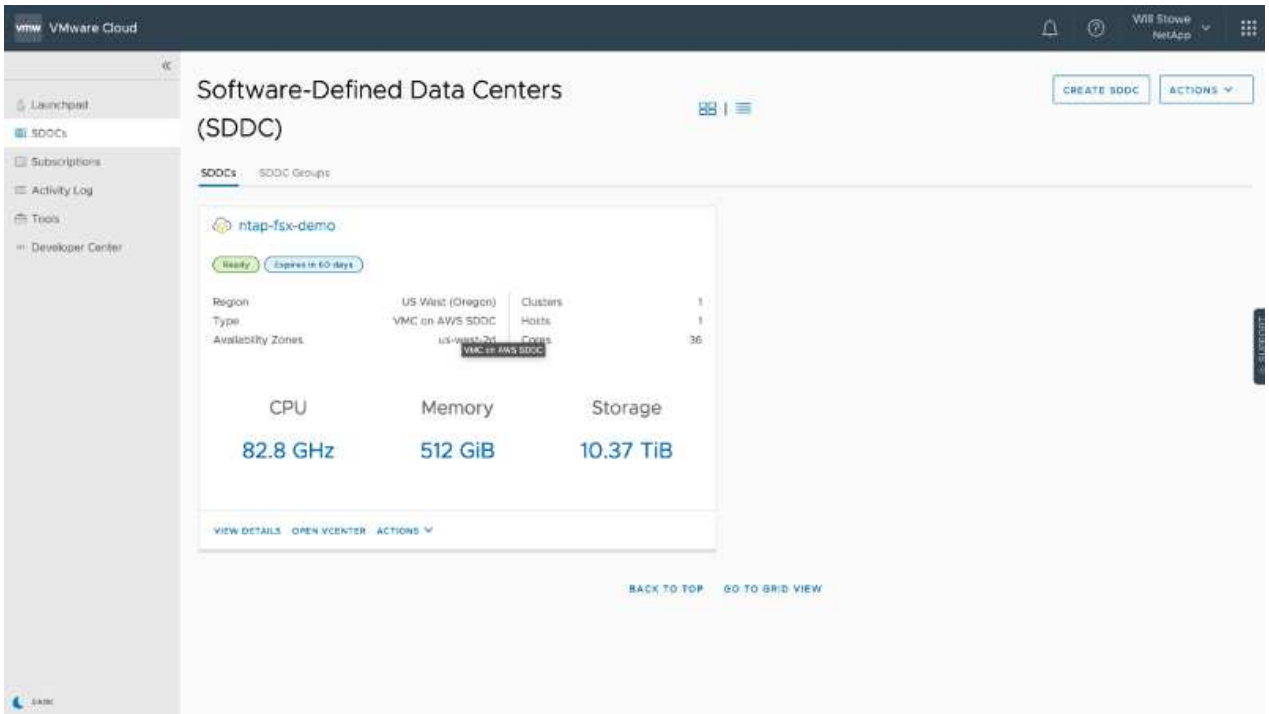
6. 查看并确认 SDDC 配置，然后单击部署 SDDC。



部署过程通常需要大约两个小时才能完成。



7. 完成后，SDDC 即可使用。

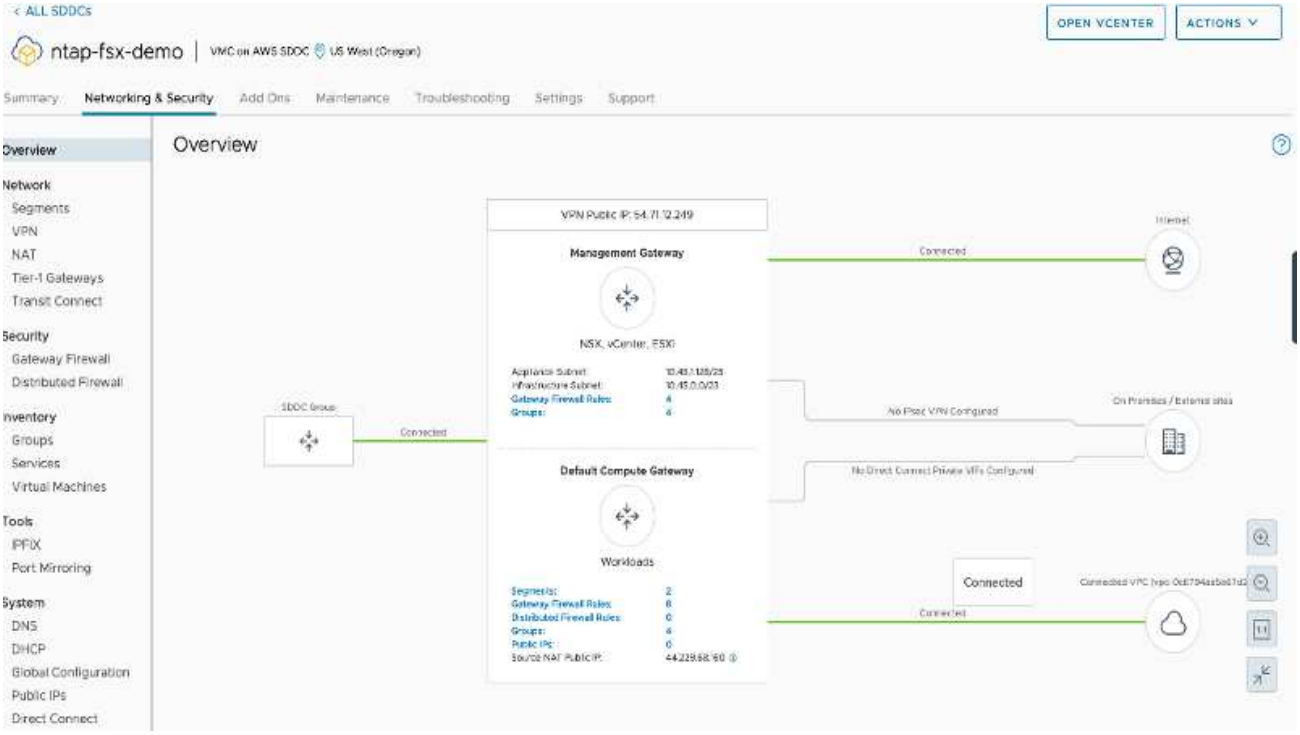


有关 SDDC 部署的分步指南，请参阅"从 VMC 控制台部署 SDDC"。

▼ 将 **VMware Cloud** 连接到 **FSx ONTAP**

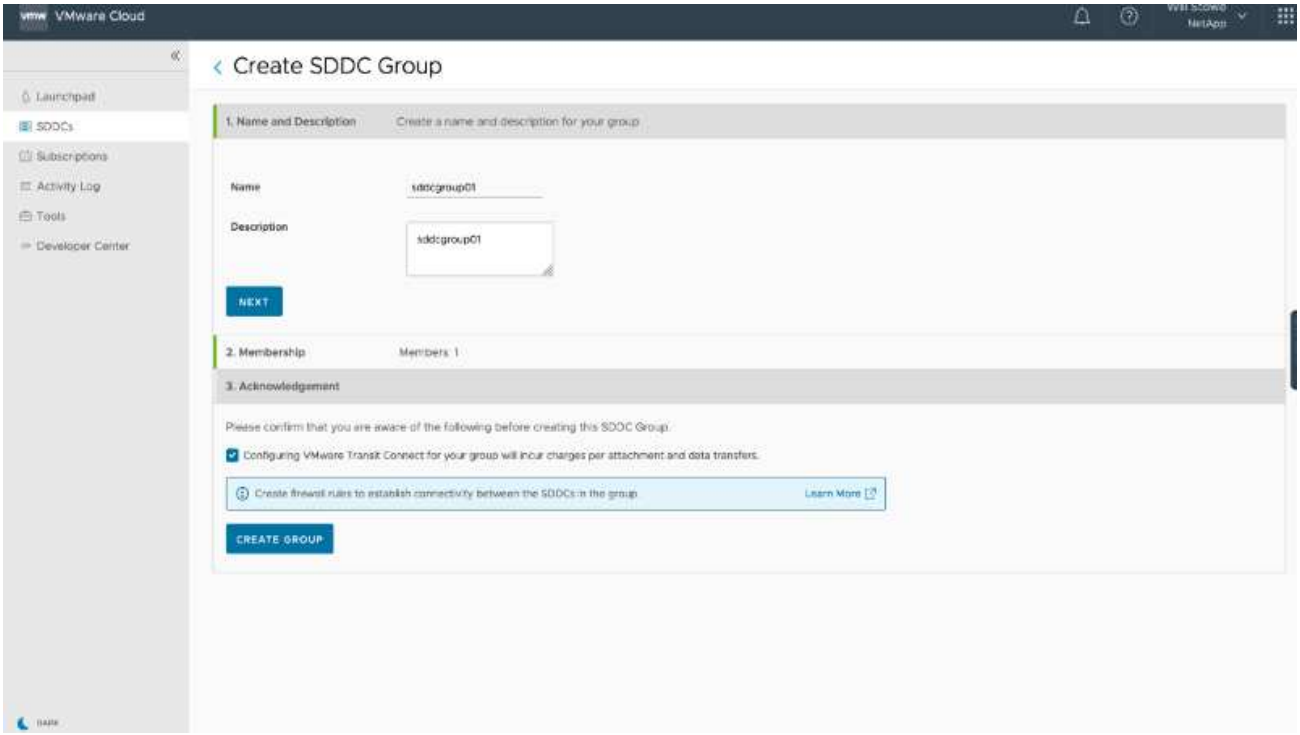
要将 VMware Cloud 连接到 FSx ONTAP，请完成以下步骤：

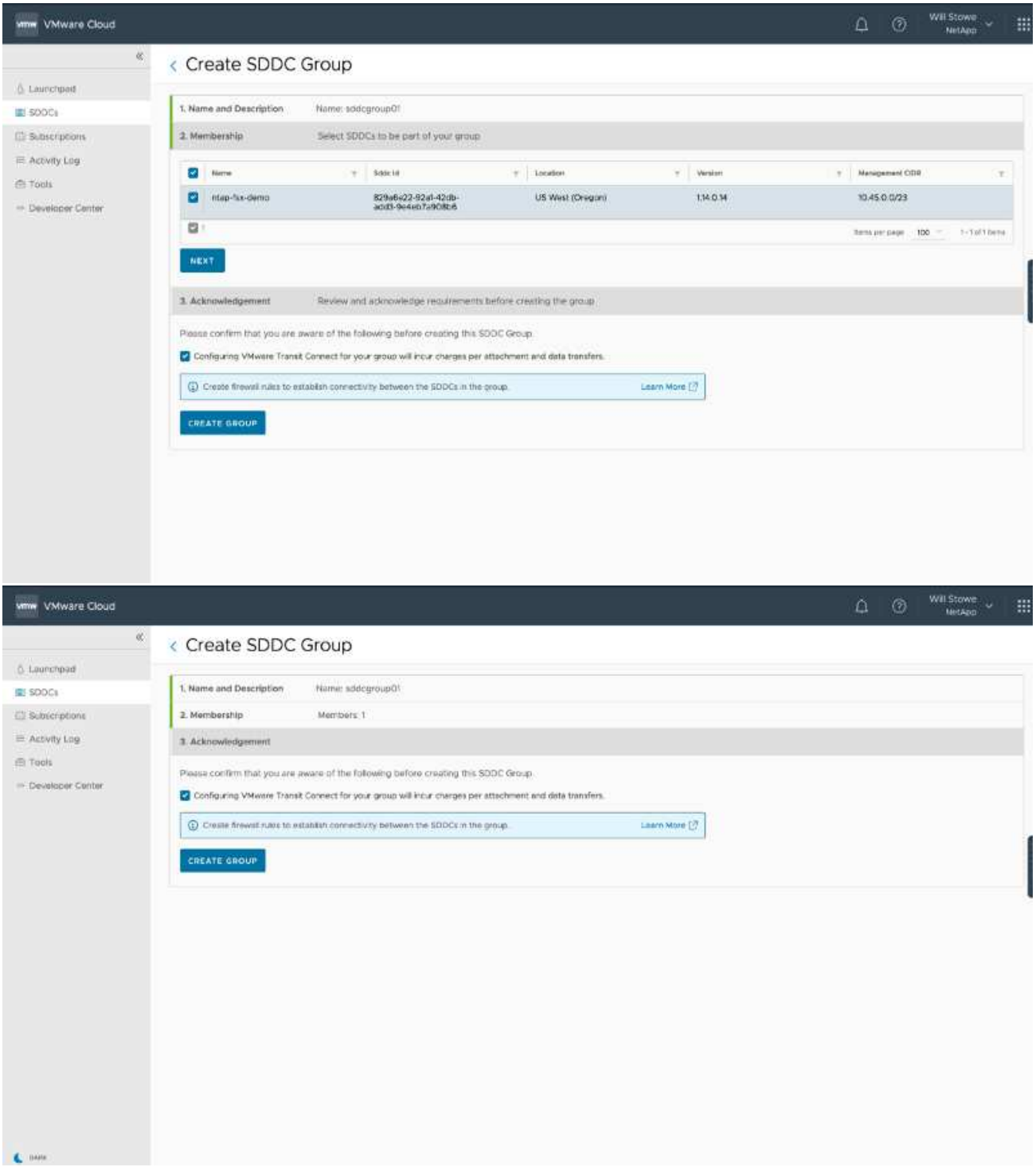
1. VMware Cloud 部署完成并连接到 AWS VPC 后，您必须将Amazon FSx ONTAP部署到新的 VPC 中，而不是原始连接的 VPC（参见下面的屏幕截图）。如果 FSx（NFS 和 SMB 浮动 IP）部署在连接的 VPC 中，则无法访问。请记住，像Cloud Volumes ONTAP这样的 ISCSI 端点在连接的 VPC 中可以正常工作。



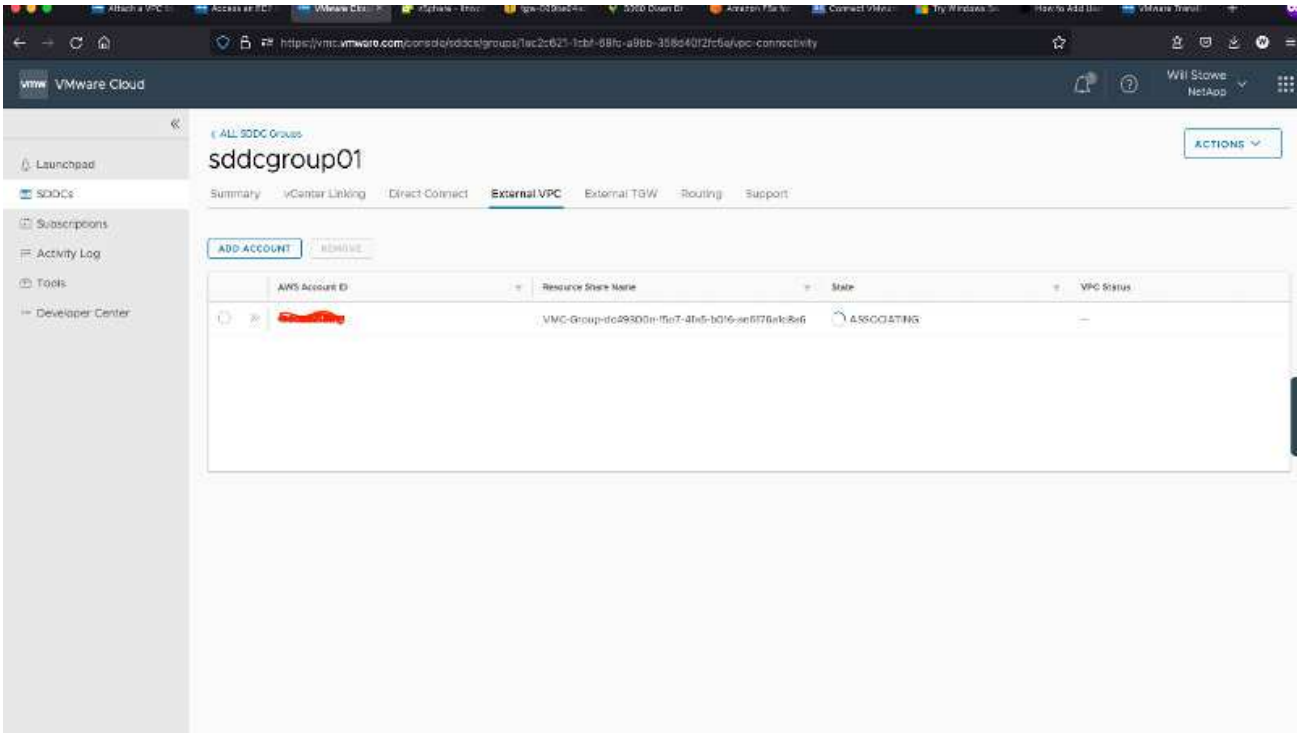
2. 在同一区域部署额外的 VPC，然后将Amazon FSx ONTAP部署到新的 VPC 中。

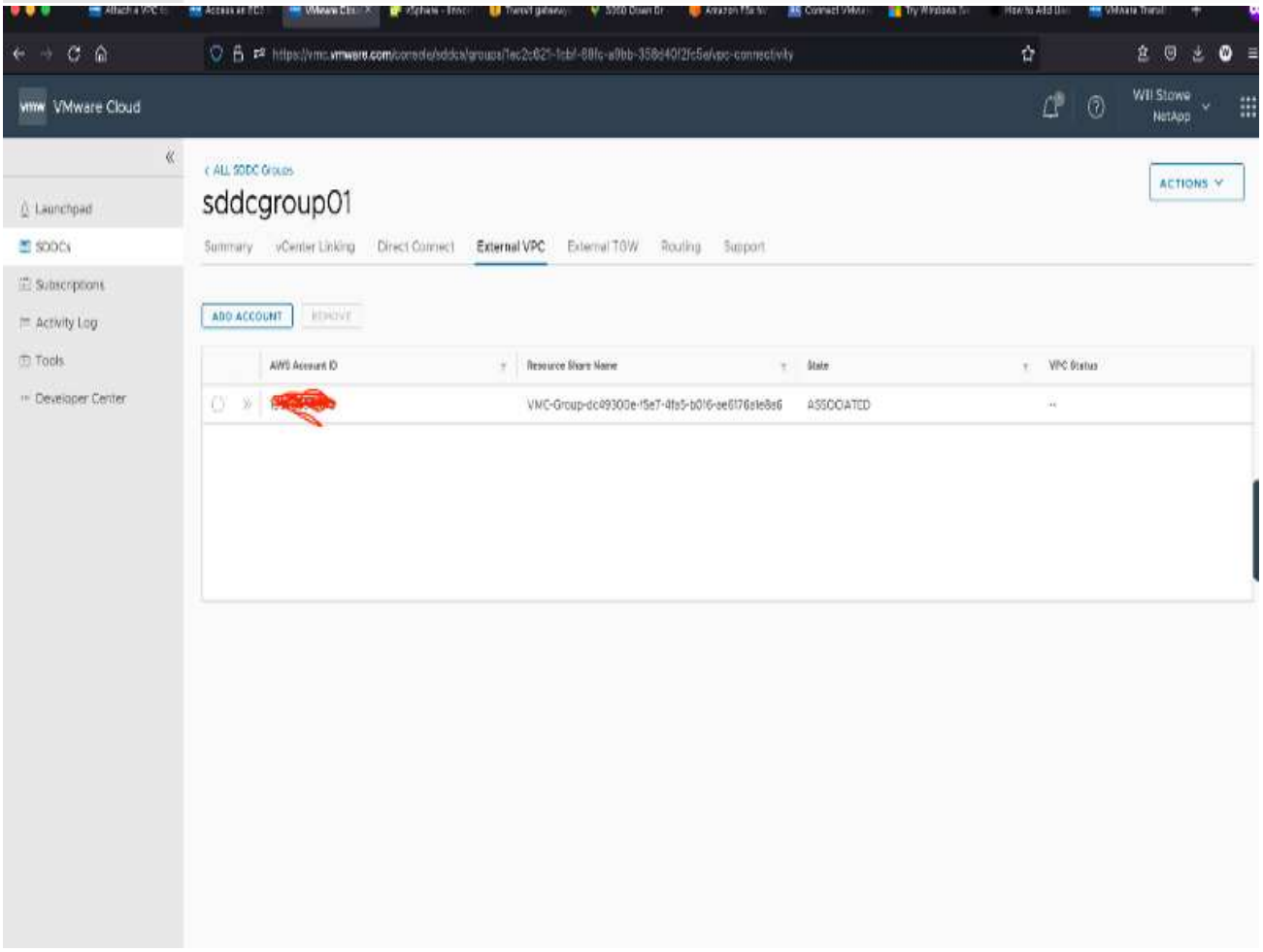
VMware Cloud 控制台中的 SDDC 组配置启用了连接到部署 FSx 的新 VPC 所需的网络配置选项。在步骤 3 中，验证是否选中“为您的组配置 VMware Transit Connect 将产生每个附件和数据传输的费用”，然后选择“创建组”。该过程可能需要几分钟才能完成。



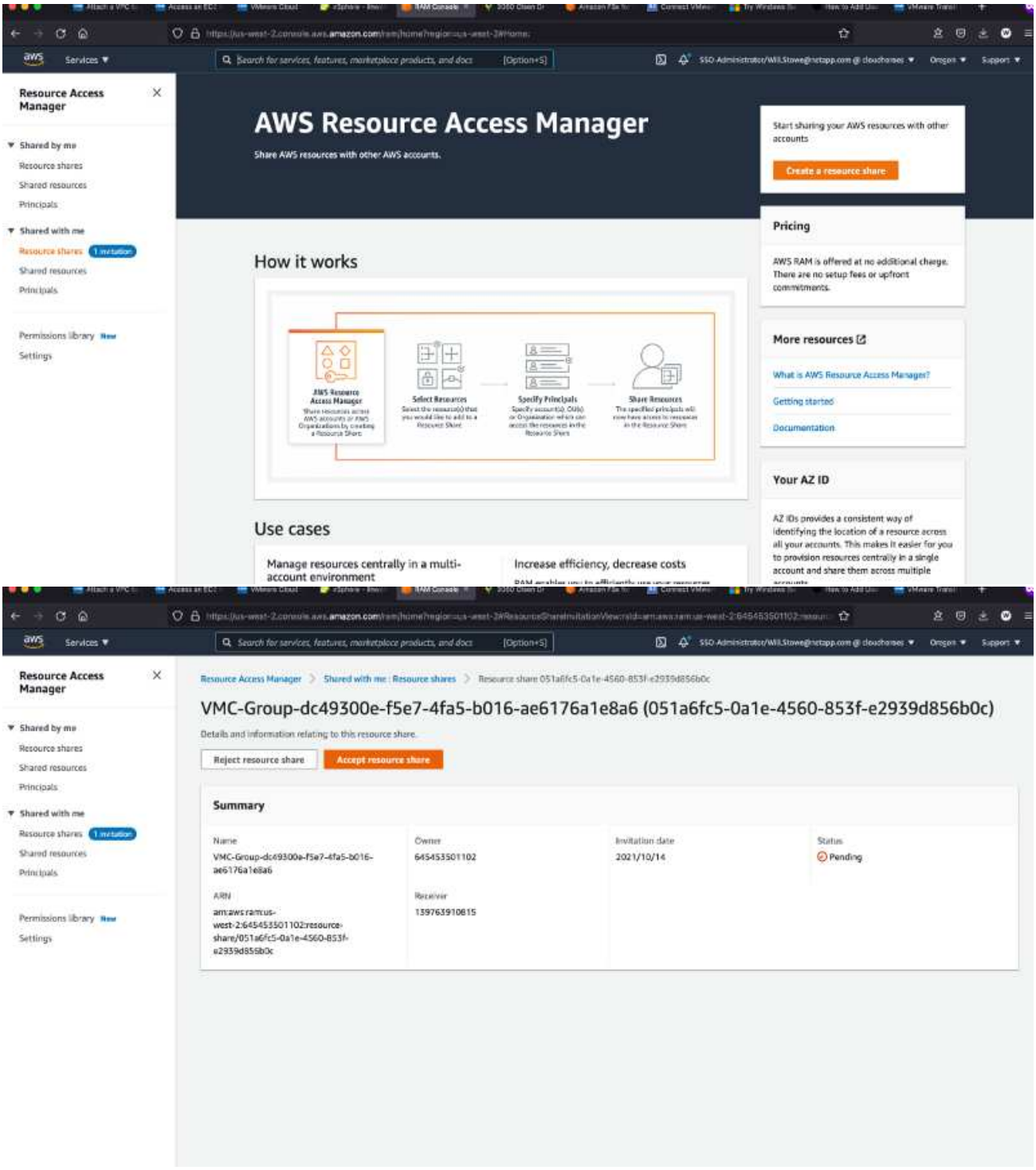


3. 将新创建的 VPC 附加到刚创建的 SDDC 组。选择外部 VPC 选项卡并按照"连接外部 VPC 的说明"到群里。此过程可能需要 10 到 15 分钟才能完成。



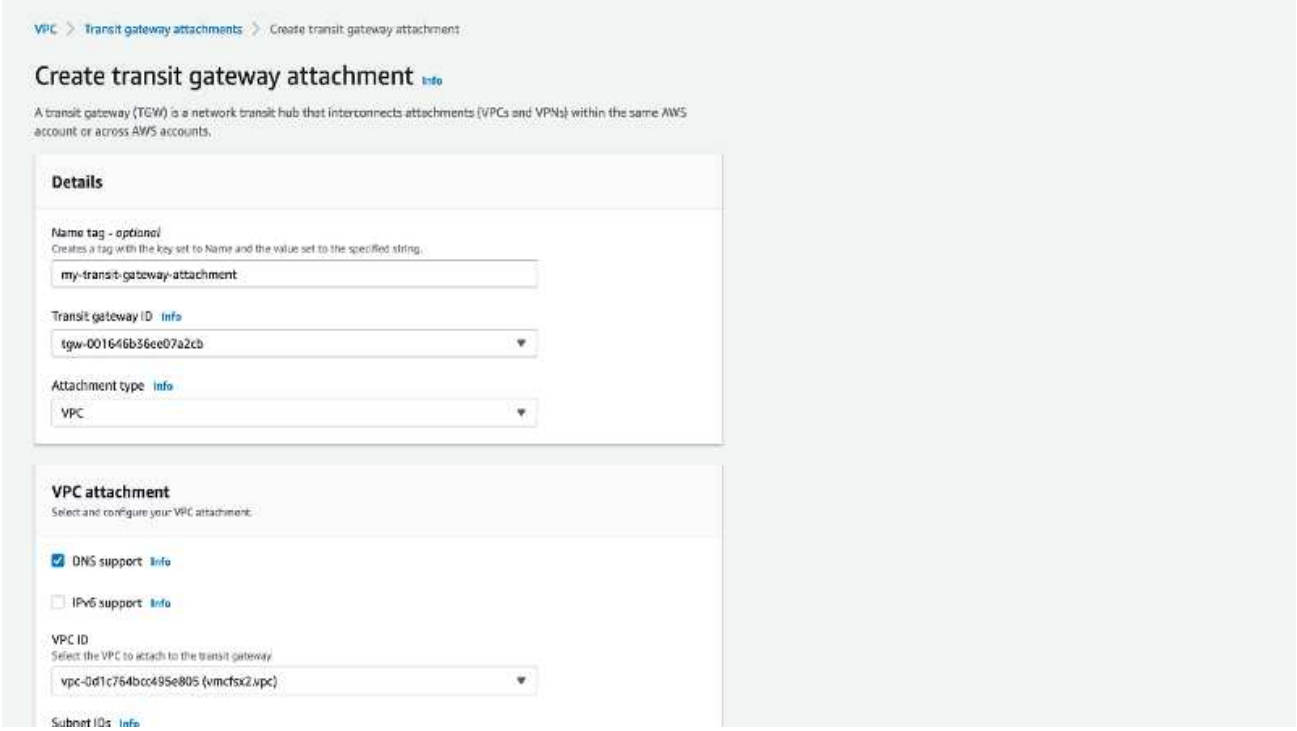


4. 作为外部 VPC 流程的一部分，您将通过 AWS 控制台通过资源访问管理器提示新的共享资源。共享资源是"AWS Transit Gateway"由 VMware Transit Connect 管理。

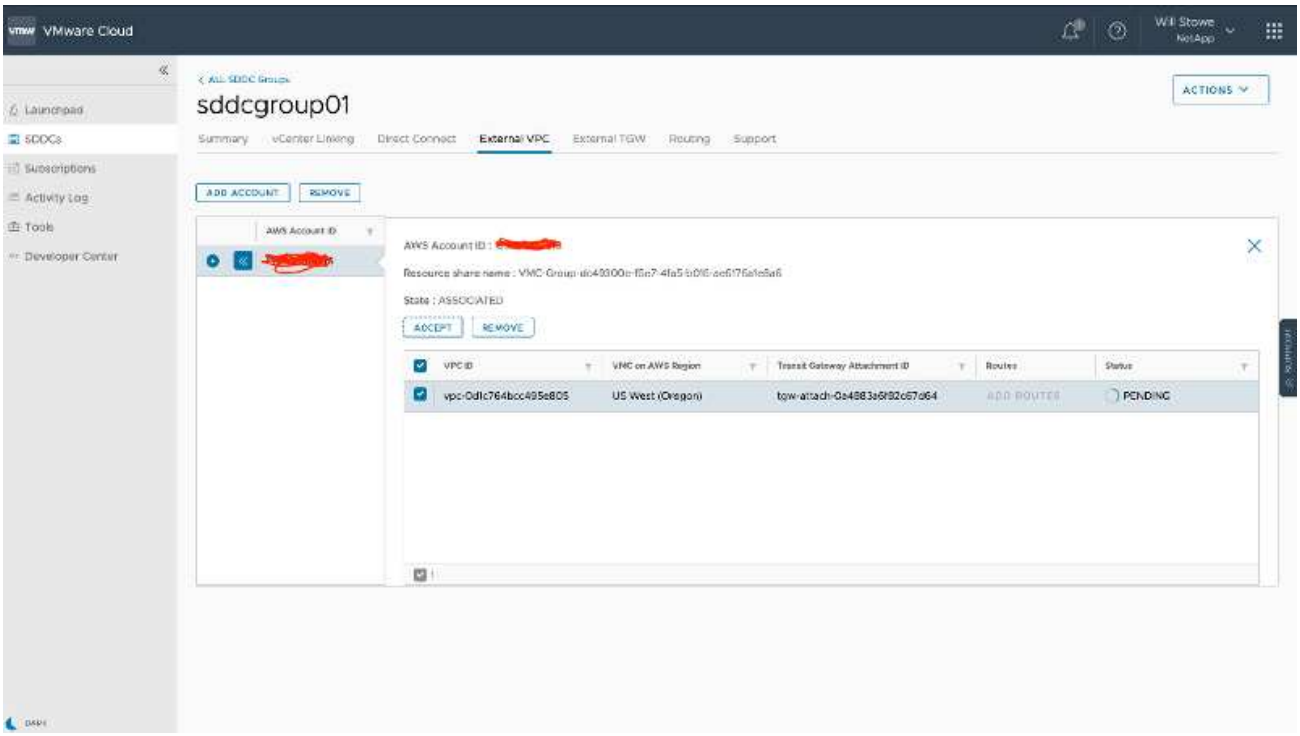

Resource Access Manager
Shared by me
Resource shares
Shared resources
Principals
Shared with me
Resource shares 1 invitation
Shared resources
Principals
Permissions library New
Settings
AWS Resource Access Manager
Share AWS resources with other AWS accounts.
Start sharing your AWS resources with other accounts
Create a resource share
How it works
Pricing
AWS RAM is offered at no additional charge. There are no setup fees or upfront commitments.
More resources
What is AWS Resource Access Manager?
Getting started
Documentation
Your AZ ID
AZ IDs provides a consistent way of identifying the location of a resource across all your accounts. This makes it easier for you to provision resources centrally in a single account and share them across multiple
Use cases
Manage resources centrally in a multi-account environment
Increase efficiency, decrease costs

Resource Access Manager
Shared by me
Resource shares
Shared resources
Principals
Shared with me
Resource shares 1 invitation
Shared resources
Principals
Permissions library New
Settings
Resource Access Manager > Shared with me : Resource shares > Resource share 051a6fc5-0a1e-4560-853f-e2939d856b0c
VMC-Group-dc49300e-f5e7-4fa5-b016-ae6176a1e8a6 (051a6fc5-0a1e-4560-853f-e2939d856b0c)
Details and information relating to this resource share.
Reject resource share
Accept resource share
Summary
Name
VMC-Group-dc49300e-f5e7-4fa5-b016-ae6176a1e8a6
Owner
645453501102
Invitation date
2021/10/14
Status
Pending
ARN
arn:aws:ram:us-west-2:645453501102:resource-share/051a6fc5-0a1e-4560-853f-e2939d856b0c
Receiver
139763910815

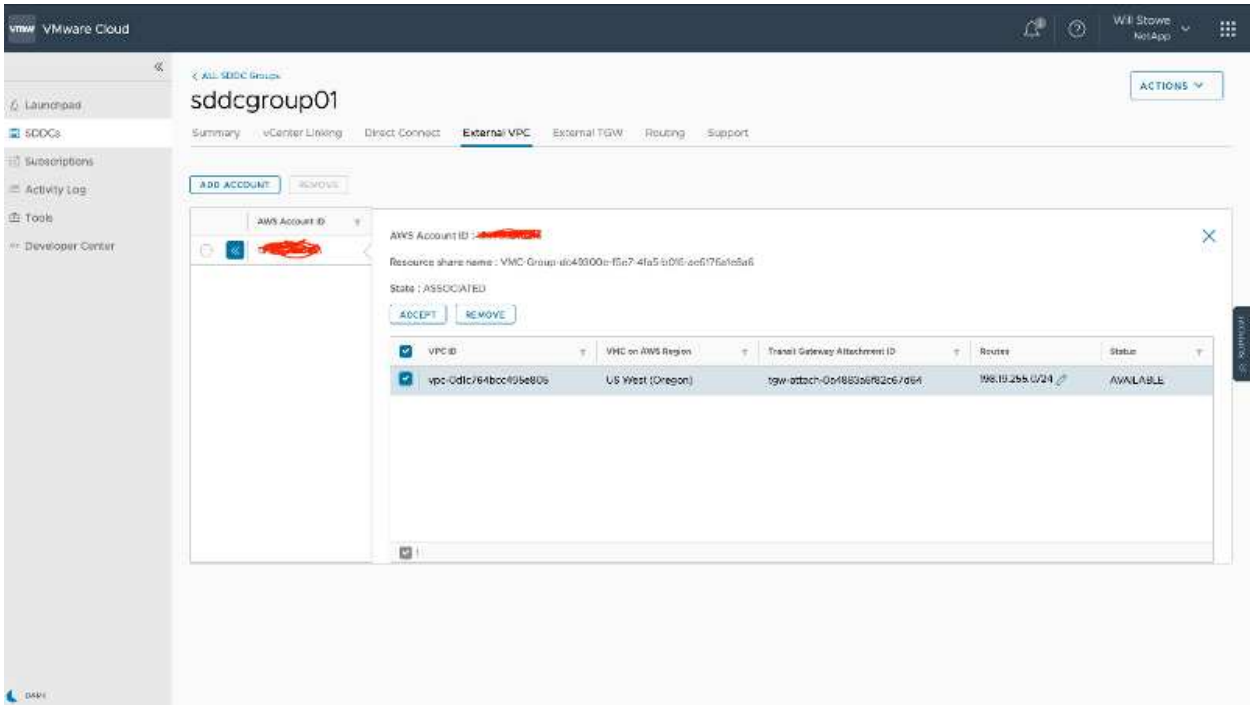
5. 创建传输网关附件。



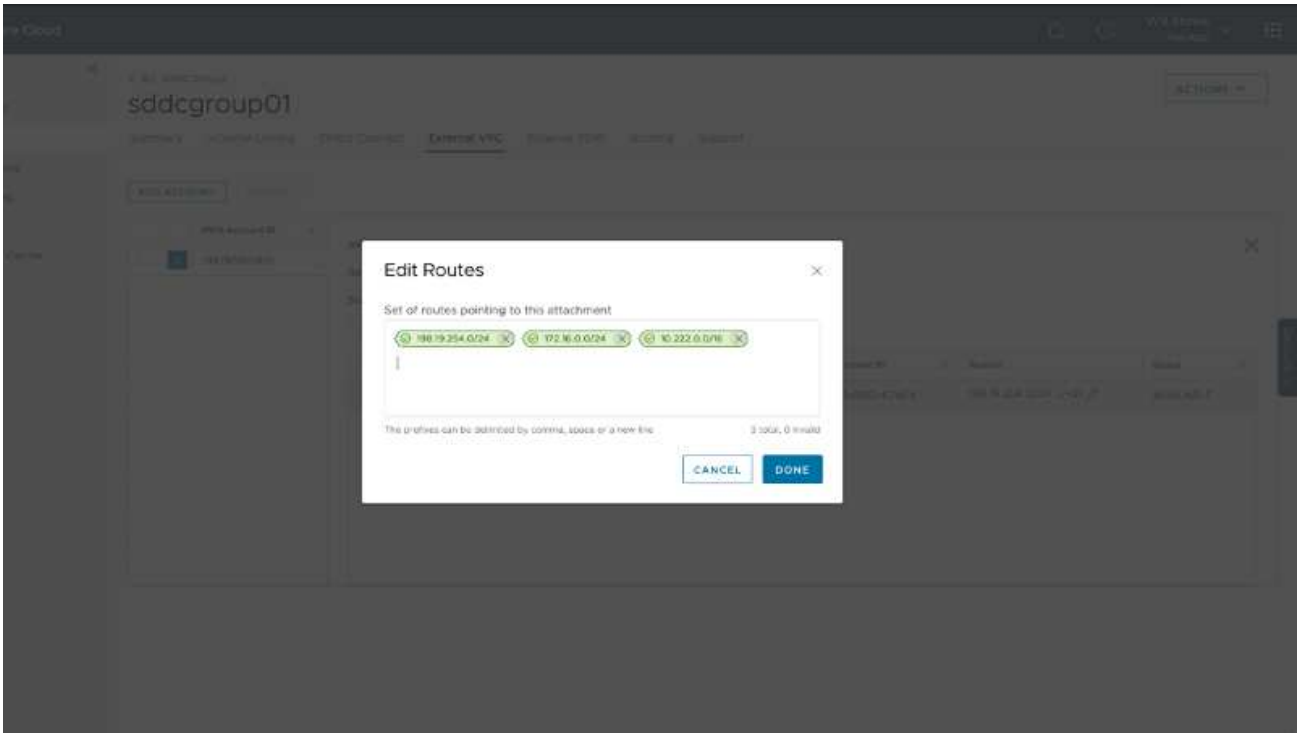
6. 返回 VMC 控制台，接受 VPC 附件。此过程大约需要 10 分钟才能完成。



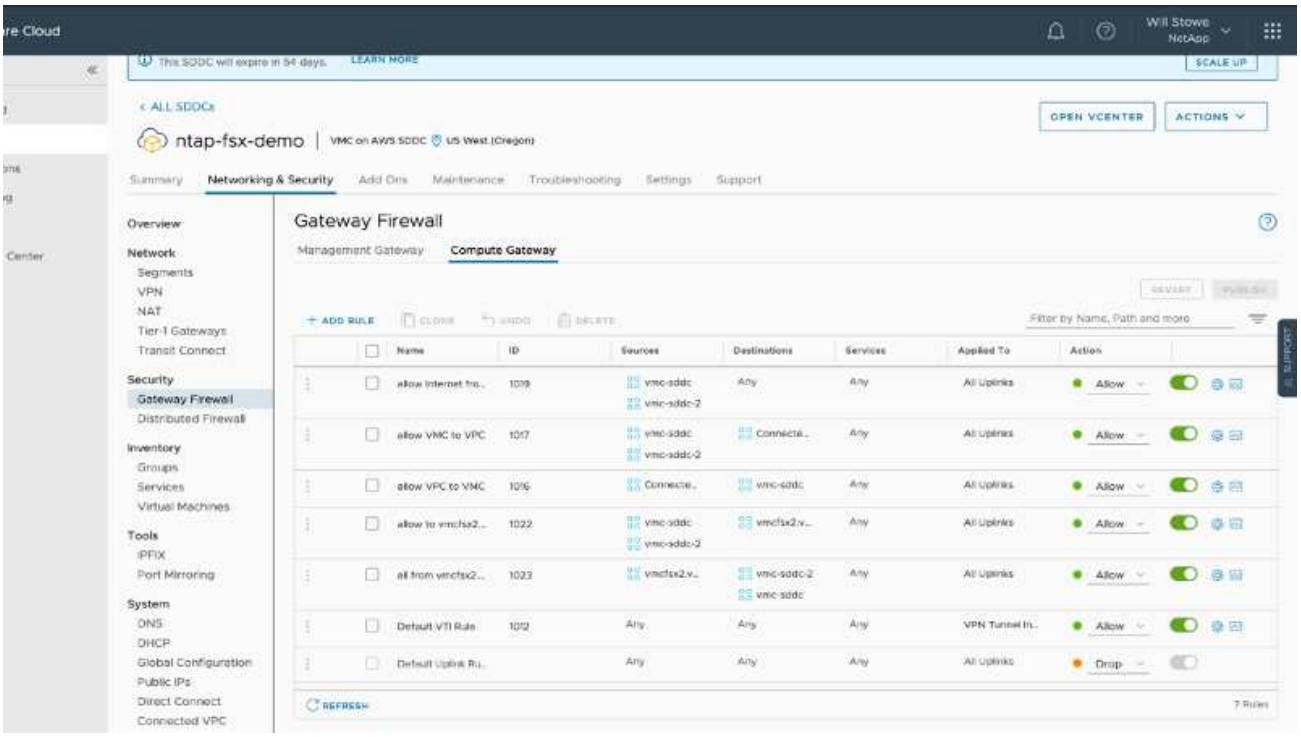
7. 在“外部 VPC”选项卡中，单击“路由”列中的编辑图标，并添加以下所需路由：
   - Amazon FSx ONTAP浮动 IP 范围的路由"浮动IP"。
   - Cloud Volumes ONTAP的浮动 IP 范围的路由（如果适用）。
   - 新创建的外部 VPC 地址空间的路由。



8. 最后，允许双向流量"防火墙规则"用于访问 FSx/CVO。遵循这些"详细步骤"用于 SDDC 工作负载连接的计算网关防火墙规则。



9. 为管理和计算网关配置防火墙组后，可以按如下方式访问 vCenter：



下一步是验证是否根据您的要求配置了Amazon FSx ONTAP或Cloud Volumes ONTAP ，以及是否配置了卷以从 vSAN 卸载存储组件以优化部署。

在 **Azure** 上部署和配置虚拟化环境

与本地一样，规划 Azure VMware 解决方案对于成功创建 VM 和迁移的生产就绪环境至关重要。

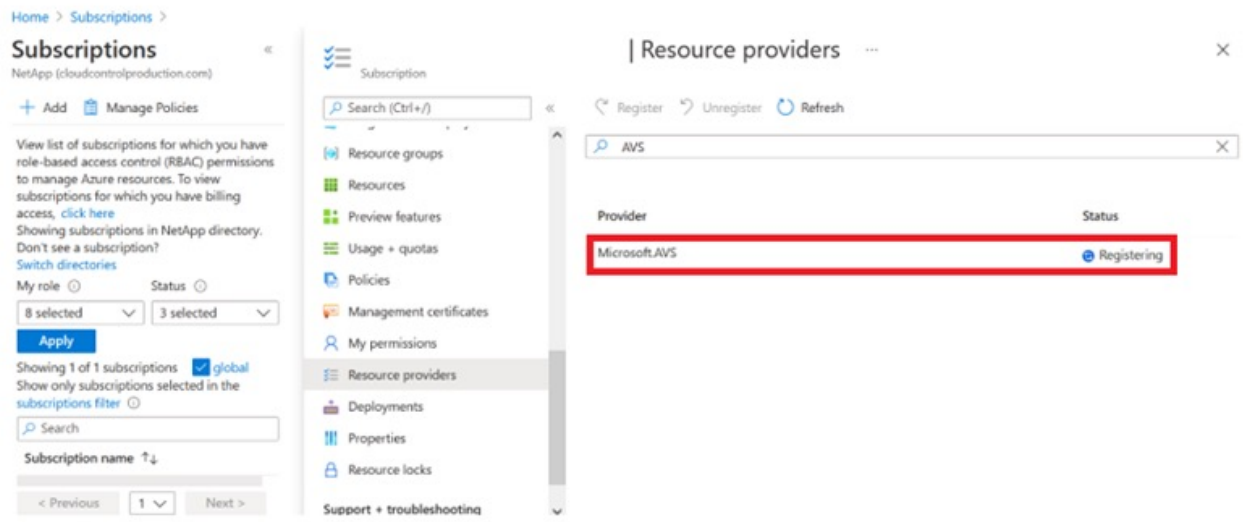
本部分介绍如何设置和管理 Azure VMware 解决方案，并将其与用于连接NetApp存储的可用选项结合使用。

设置过程可分为以下步骤：

▼ 注册资源提供者并创建私有云

要使用 Azure VMware 解决方案，请首先在已识别的订阅中注册资源提供程序：

1. Sign inAzure 门户。
2. 在 Azure 门户菜单上，选择“所有服务”。
3. 在“所有服务”对话框中，输入订阅，然后选择“订阅”。
4. 要查看，请从订阅列表中选择订阅。
5. 选择资源提供商并在搜索中输入 Microsoft.AVS。
6. 如果资源提供者尚未注册，请选择注册。

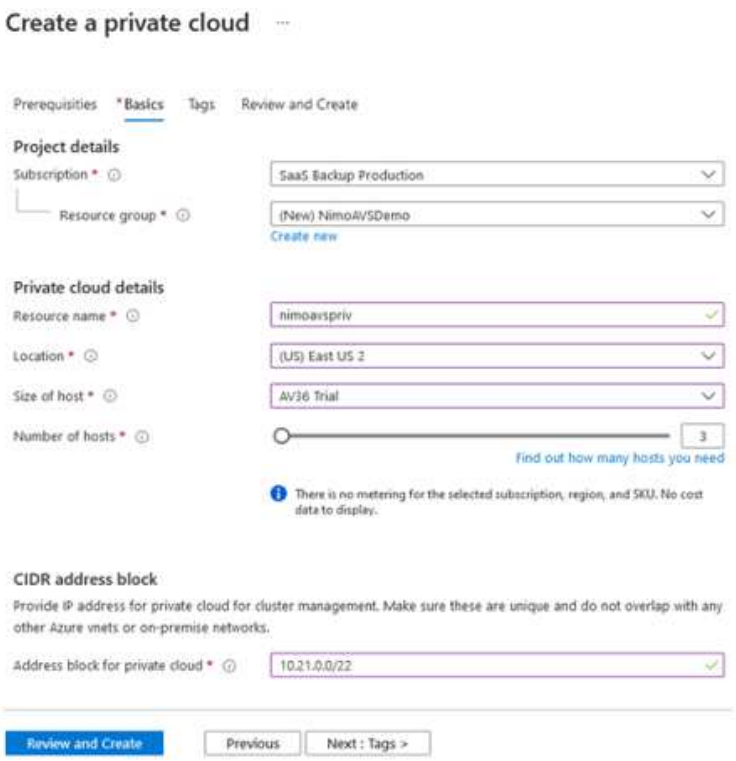




7. 注册资源提供程序后，使用 Azure 门户创建 Azure VMware 解决方案私有云。
8. Sign inAzure 门户。
9. 选择创建新资源。
10. 在“搜索市场”文本框中，输入“Azure VMware 解决方案”并从结果中选择它。
11. 在 Azure VMware 解决方案页上，选择“创建”。
12. 在“基本信息”选项卡中，输入字段中的值并选择“审阅 + 创建”。

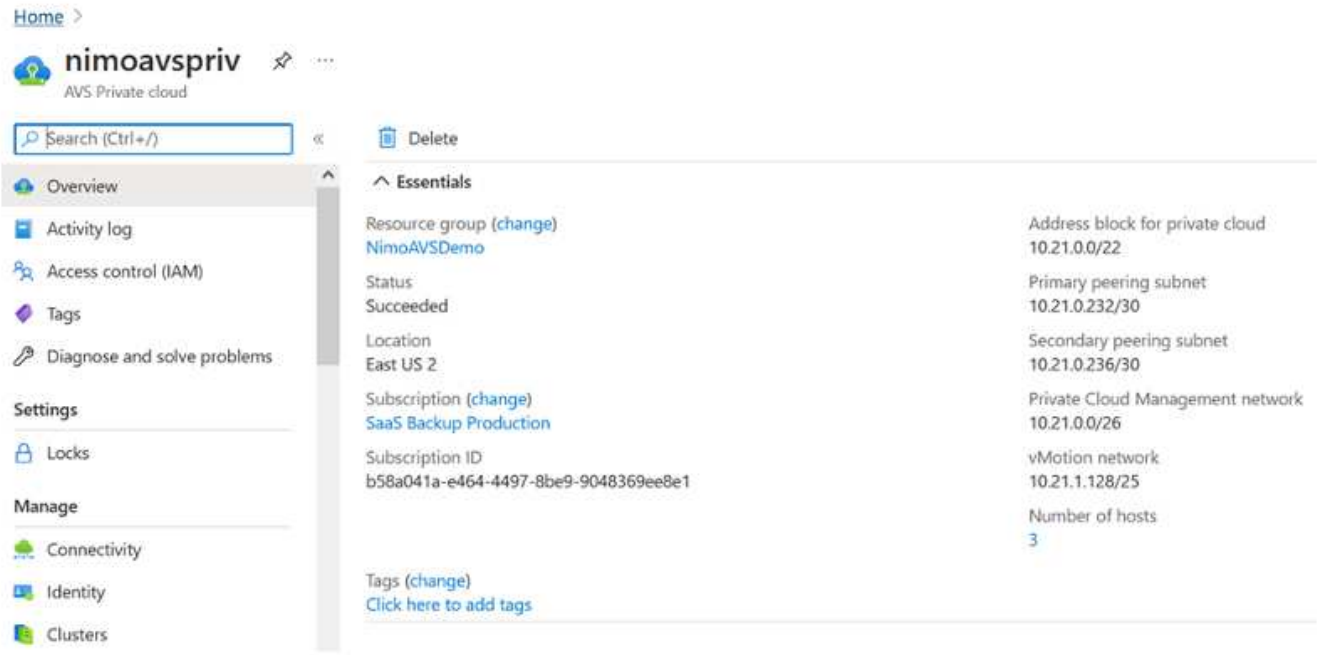
注：

- 为了快速启动，请在规划阶段收集所需的信息。
- 选择现有资源组或为私有云创建新的资源组。资源组是部署和管理 Azure 资源的逻辑容器。
- 确保 CIDR 地址是唯一的，并且不与其他 Azure 虚拟网络或本地网络重叠。 CIDR 代表私有云管理网络，用于集群管理服务，例如 vCenter Server 和 NSX-T Manager。 NetApp建议使用 /22 地址空间。在此示例中，使用 10.21.0.0/22。



配置过程大约需要 4 至 5 个小时。该过程完成后，通过从 Azure 门户访问私有云来验证部署是否成功。部署完成后将显示“成功”状态。

Azure VMware 解决方案私有云需要 Azure 虚拟网络。由于 Azure VMware 解决方案不支持本地 vCenter，因此需要执行额外的步骤才能与现有的本地环境集成。还需要设置 ExpressRoute 线路和虚拟网络网关。在等待群集预配完成时，创建一个新的虚拟网络或使用现有的虚拟网络连接到 Azure VMware 解决方案。



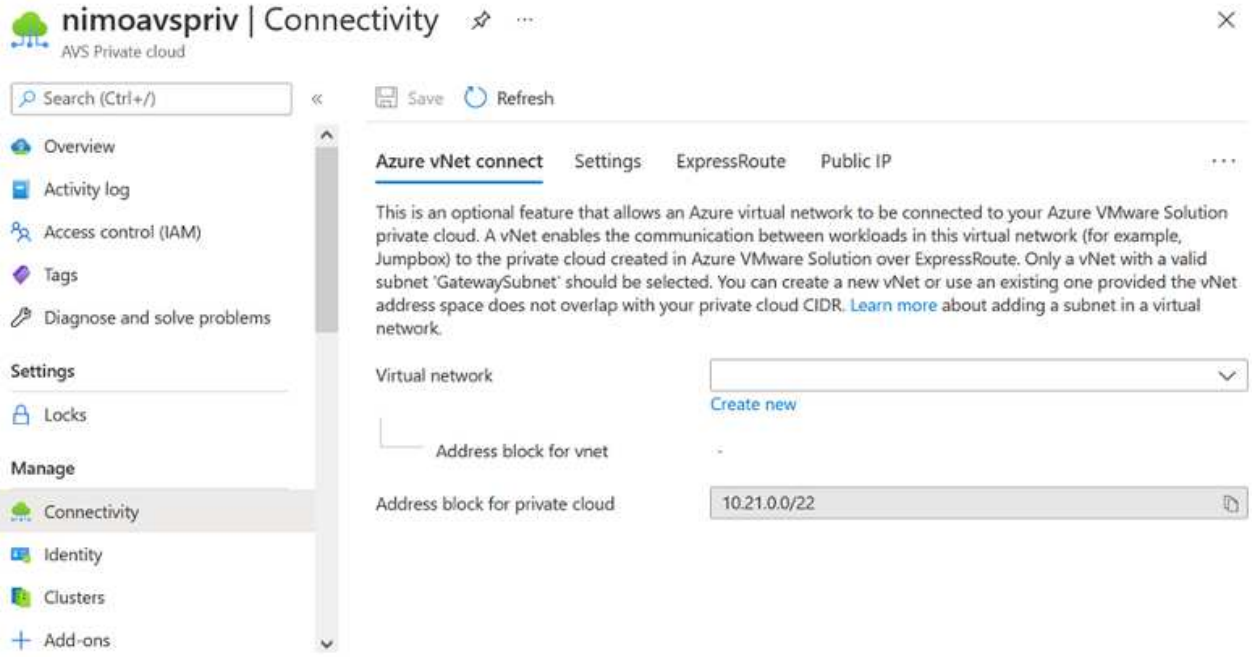
▼ 连接到新的或现有的 **ExpressRoute** 虚拟网络网关

要创建新的 Azure 虚拟网络 (VNet)，请选择 Azure VNet Connect 选项卡。或者，您也可以使用创建虚拟网络向导从 Azure 门户手动创建一个：

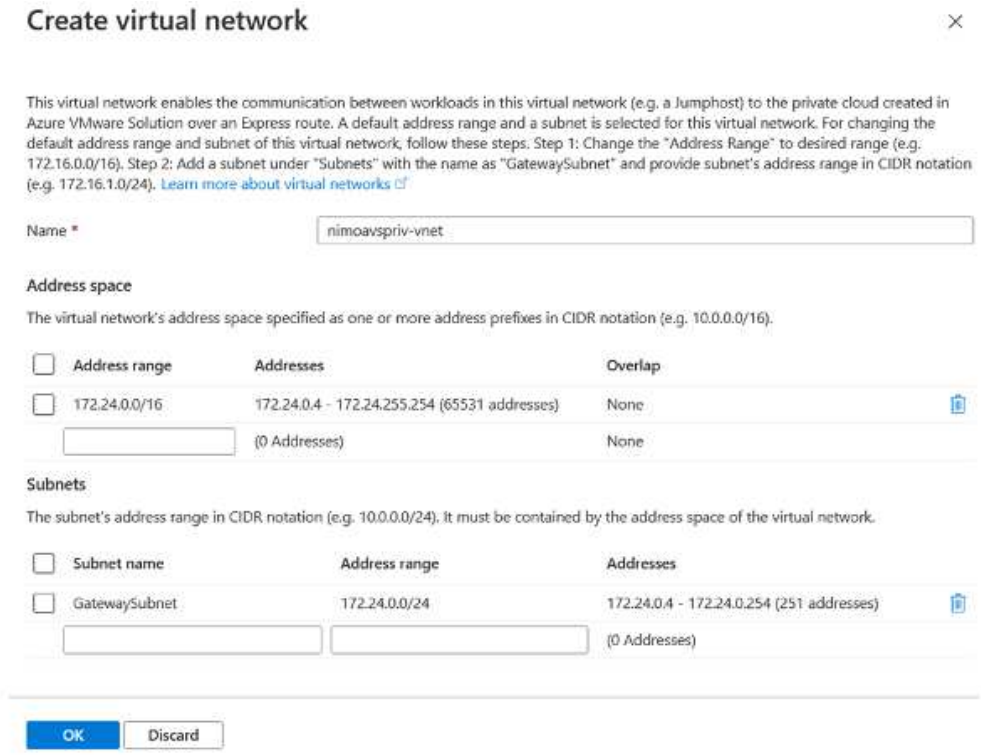
1. 转到 Azure VMware 解决方案私有云并访问“管理”选项下的“连接”。
2. 选择 Azure VNet Connect。
3. 要创建新的 VNet，请选择“新建”选项。

   此功能允许 VNet 连接到 Azure VMware 解决方案私有云。 VNet 通过 ExpressRoute 自动为 Azure VMware 解决方案中创建的私有云创建所需的组件（例如，跳转框、共享服务（如Azure NetApp Files和 Cloud Volume ONTAP）），从而实现此虚拟网络中的工作负载之间的通信。

   *注意：*VNet 地址空间不应与私有云 CIDR 重叠。



4. 提供或更新新 VNet 的信息并选择“确定”。

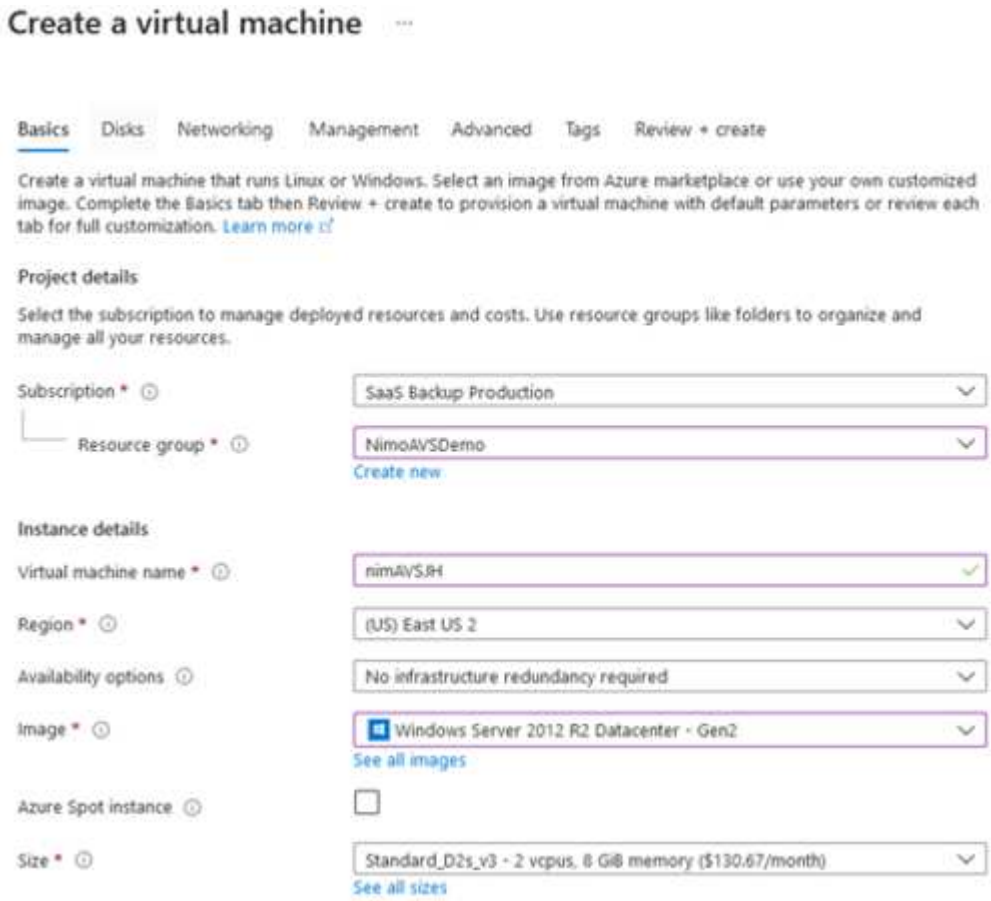


在指定的订阅和资源组中创建具有提供的地址范围和网关子网的 VNet。

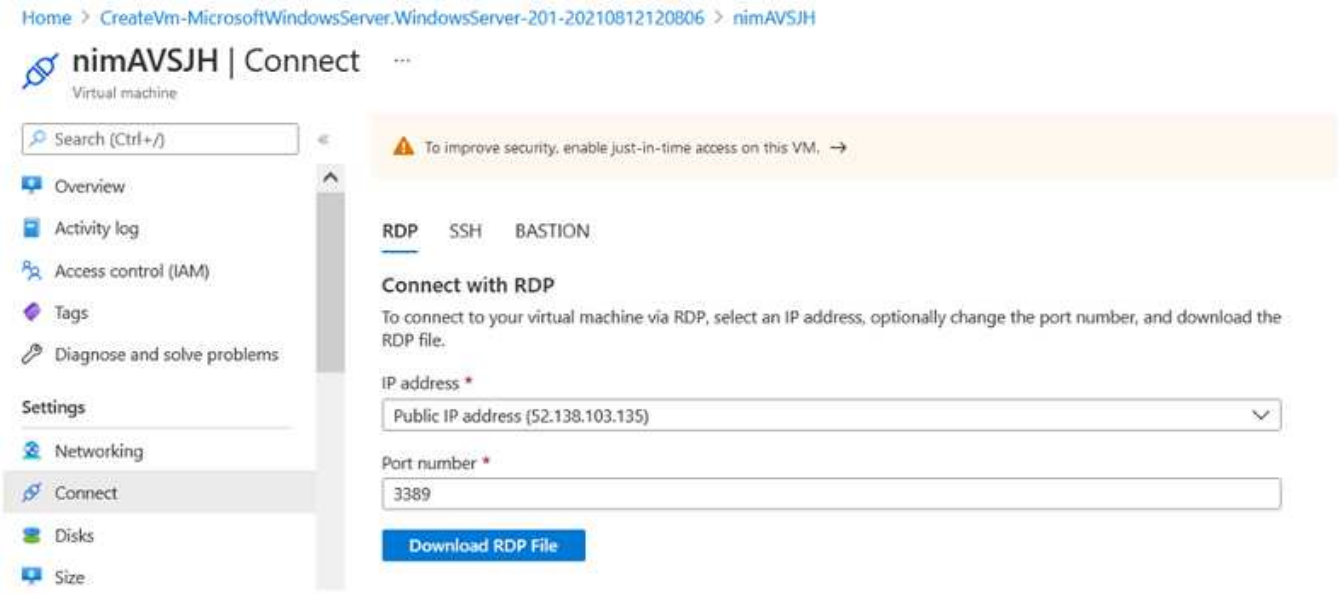
如果手动创建 VNet，请使用适当的 SKU 和 ExpressRoute 作为网关类型创建虚拟网络网关。部署完成后，使用授权密钥将 ExpressRoute 连接连接到包含 Azure VMware 解决方案私有云的虚拟网络网关。有关更多信息，请参阅"在 Azure 中为 VMware 私有云配置网络" 。

▼ 验证网络连接以及对 **Azure VMware** 解决方案私有云的访问

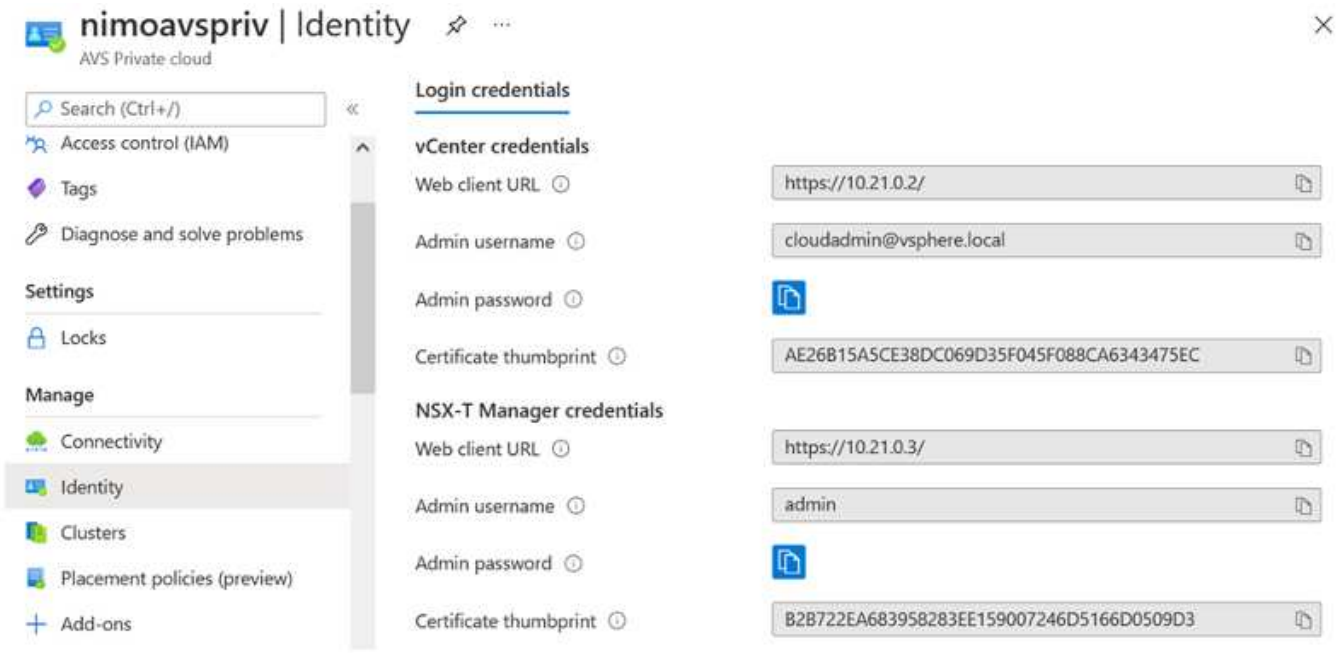
Azure VMware 解决方案不允许您使用本地 VMware vCenter 管理私有云。相反，需要跳转主机才能连接到 Azure VMware 解决方案 vCenter 实例。在指定的资源组中创建跳转主机并登录到 Azure VMware 解决方案 vCenter。此跳转主机应是为连接而创建的同一虚拟网络上的 Windows VM，并且应提供对 vCenter 和 NSX Manager 的访问权限。



配置虚拟机后，使用“连接”选项访问 RDP。



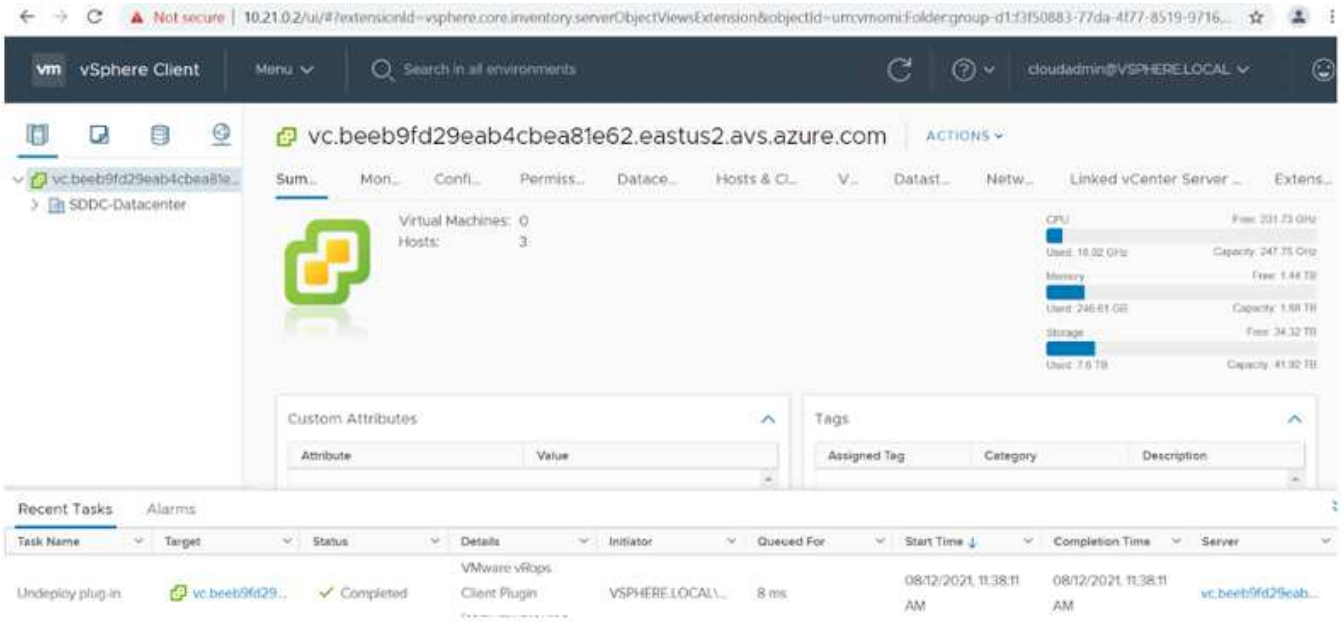
使用云管理员用户从这个新创建的跳转主机虚拟机Sign in到 vCenter。要访问凭据，请转到 Azure 门户并导航到“身份”（在私有云中的“管理”选项下）。可以从这里复制私有云 vCenter 和 NSX-T 管理器的 URL 和用户凭据。



在 Windows 虚拟机中，打开浏览器并导航到 vCenter Web 客户端 URL("`https://10.21.0.2/`") 并使用管理员用户名为 **cloudadmin@vsphere.local** 并粘贴复制的密码。同样，也可以使用 Web 客户端 URL 访问 NSX-T 管理器("`https://10.21.0.3/`") 并使用管理员用户名和粘贴复制的密码来创建新的段或修改现有的层网关。

对于每个配置的 SDDC，Web 客户端 URL 都是不同的。





Azure VMware 解决方案 SDDC 现已部署并配置。利用 ExpressRoute Global Reach 将本地环境连接到 Azure VMware 解决方案私有云。有关更多信息，请参阅"将本地环境与 Azure VMware 解决方案对等" 。

在 **Google Cloud Platform (GCP)** 上部署和配置虚拟化环境

与本地一样，规划 Google Cloud VMware Engine (GCVE) 对于成功创建虚拟机和迁移的生产就绪环境至关重要。

本节介绍如何设置和管理 GCVE，以及如何将其与可用于连接NetApp存储的选项结合使用。

设置过程可分为以下步骤：

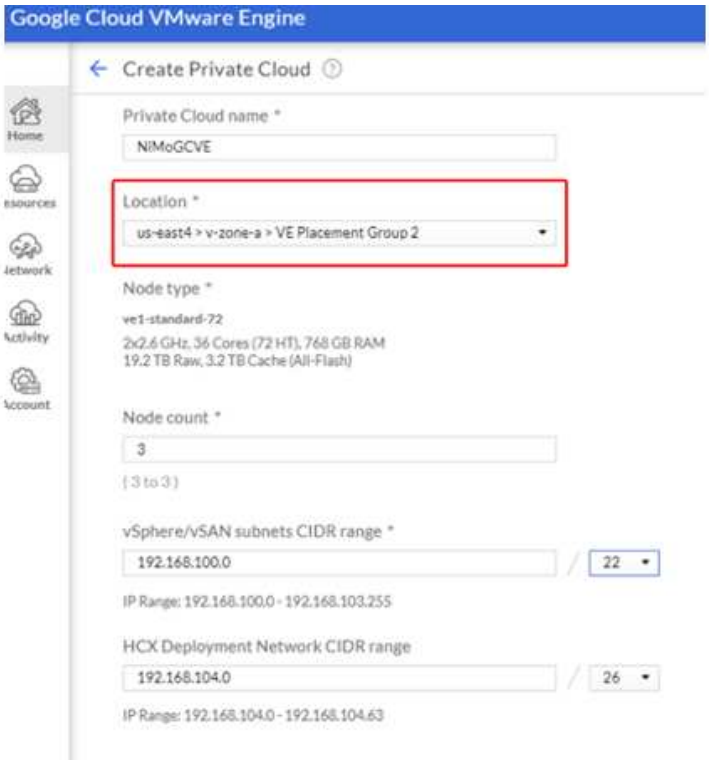
▼ 部署和配置 **GCVE**

要在 GCP 上配置 GCVE 环境，请登录 GCP 控制台并访问 VMware Engine 门户。

点击“新建私有云”按钮，输入GCVE私有云所需的配置。在“位置”上，确保将私有云部署在部署NetApp Volumes/CVO 的同一区域/区域中，以确保最佳性能和最低延迟。

先决条件：

- 设置 VMware Engine 服务管理员 IAM 角色
- "启用 VMWare Engine API 访问和节点配额"
- 确保 CIDR 范围不与任何本地或云子网重叠。 CIDR 范围必须为 /27 或更高。



注意：私有云创建可能需要 30 分钟到 2 小时。

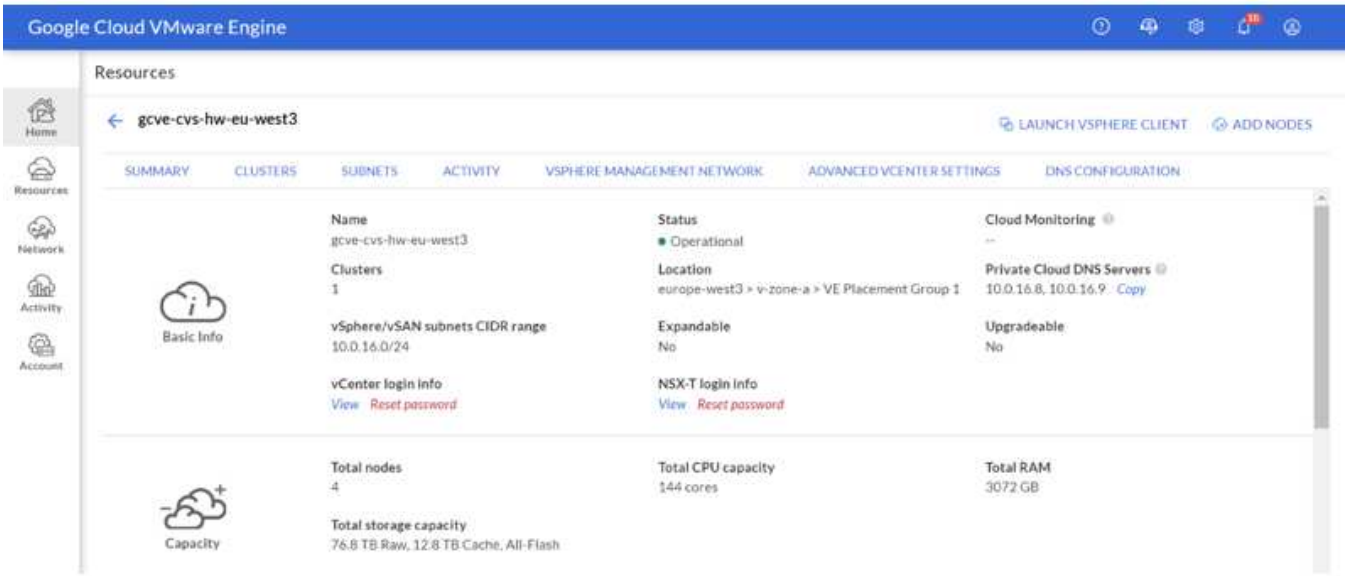
▼ 启用对 **GCVE** 的私人访问

一旦私有云配置完毕，配置对私有云的私有访问，实现高吞吐量和低延迟的数据路径连接。

这将确保运行 Cloud Volumes ONTAP 实例的 VPC 网络能够与 GCVE 私有云进行通信。为此，请按照"GCP 文档"。对于 Cloud Volume Service，通过在租户主机项目之间执行一次性对等，在 VMware Engine 和 Google Cloud NetApp Volumes 之间建立连接。如需了解详细步骤，请按照此"链接"。

Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

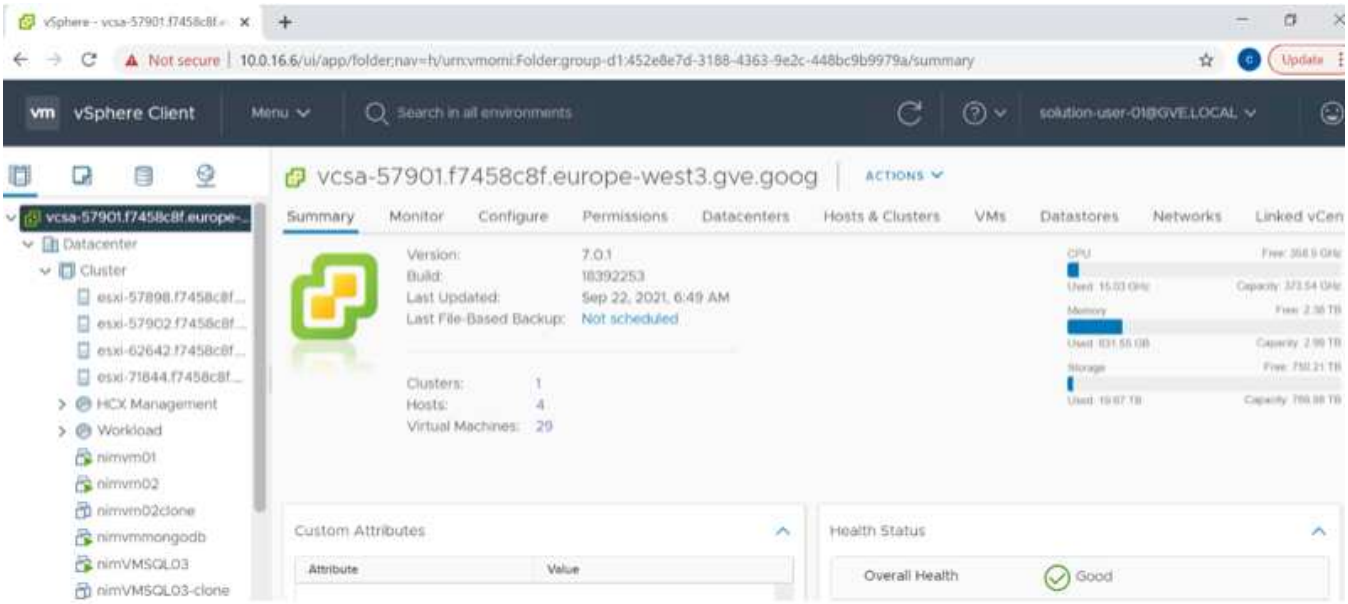
使用 CloudOwner@gve.local 用户Sign invcenter。要访问凭据，请转到 VMware Engine 门户，转到资源，然后选择适当的私有云。在“基本信息”部分中，单击 vCenter 登录信息（vCenter Server、HCX 管理器）或 NSX-T 登录信息（NSX 管理器）的“查看”链接。



在 Windows 虚拟机中，打开浏览器并导航到 vCenter Web 客户端 URL("`https://10.0.16.6/`") 并使用管理员用户名作为 CloudOwner@gve.local 并粘贴复制的密码。同样，也可以使用 Web 客户端 URL 访问 NSX-T 管理器("`https://10.0.16.11/`") 并使用管理员用户名和粘贴复制的密码来创建新的段或修改现有的层网关。

要从本地网络连接到 VMware Engine 私有云，请利用云 VPN 或 Cloud Interconnect 进行适当的连接，并确保所需的端口已打开。有关详细步骤，请按照"链接"。





▼ 将**Google Cloud NetApp Volumes**补充数据存储区部署到 **GCVE**

参考"使用NetApp卷将补充 NFS 数据存储部署到 GCVE 的过程"

公共云中的**NetApp**存储

面向公共云提供商的**NetApp**存储选项

探索NetApp在三大超大规模数据中心中作为存储的选项。

AWS/VMC

AWS 支持以下配置的NetApp存储：

- FSx ONTAP作为来宾连接存储
- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- FSx ONTAP作为补充 NFS 数据存储

查看详细信息"VMC 的客户机连接存储选项"。查看详细信息"VMC 的补充 NFS 数据存储选项"。

Azure/AVS

Azure 支持以下配置的NetApp存储：

- Azure NetApp Files(ANF) 作为来宾连接存储
- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- Azure NetApp Files(ANF) 作为补充 NFS 数据存储

查看详细信息"AVS 的来宾连接存储选项"。查看详细信息"AVS 的补充 NFS 数据存储选项"。

良好操作规范/良好行为规范

Google Cloud 支持以下配置的NetApp存储：

- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- Google Cloud NetApp Volumes （NetApp Volumes）作为来宾连接存储
- Google Cloud NetApp Volumes （NetApp Volumes）作为补充 NFS 数据存储

查看详细信息"GCVE 的来宾连接存储选项"。查看详细信息"GCVE 的补充 NFS 数据存储选项"。

阅读更多"Google Cloud NetApp Volumes数据存储区支持 Google Cloud VMware Engine（NetApp博客）"或者"如何将Google Cloud NetApp Volumes用作 Google Cloud VMware Engine 的数据存储区（Google 博客）"

Amazon Web Services：使用**NetApp**存储的选项

NetApp存储可以作为来宾连接存储或补充存储附加到 Amazon Web Services。

Amazon FSx for NetApp ONTAP (FSx ONTAP) 作为补充 **NFS** 数据存储

Amazon FSx ONTAP提供了部署和管理应用程序工作负载以及文件服务的绝佳选项，同时通过使数据需求无缝连接到应用程序层来降低 TCO。无论使用情况如何，选择 VMware Cloud on AWS 以及Amazon FSx ONTAP都可以快速实现云优势、一致的基础架构和从本地到 AWS 的操作、工作负载的双向可移植性以及企业级容量和性能。它与连接存储所用的过程和程序相同。

欲了解更多信息，请访问：

- "FSx ONTAP作为补充 NFS 数据存储：概述"
- "Amazon FSx for ONTAP作为补充数据存储"

Amazon FSx for NetApp ONTAP作为来宾连接存储

Amazon FSx ONTAP是一项完全托管的服务，它基于 NetApp 流行的ONTAP文件系统构建，提供高度可靠、可扩展、高性能且功能丰富的文件存储。 FSx ONTAP将NetApp文件系统的熟悉功能、性能、功能和 API 操作与完全托管的 AWS 服务的灵活性、可扩展性和简单性相结合。

FSx ONTAP提供功能丰富、快速且灵活的共享文件存储，可从在 AWS 或本地运行的 Linux、Windows 和 macOS 计算实例广泛访问。 FSx ONTAP提供具有亚毫秒级延迟的高性能固态硬盘 (SSD) 存储。借助 FSx ONTAP，您可以为您的工作负载实现 SSD 级别的性能，同时只需为一小部分数据支付 SSD 存储费用。

使用 FSx ONTAP管理数据更容易，因为您只需单击按钮即可快照、克隆和复制文件。此外，FSx ONTAP会自动将您的数据分层到成本较低的弹性存储中，从而减少您配置或管理容量的需要。

FSx ONTAP还提供高可用性和持久性存储，具有完全托管的备份和跨区域灾难恢复支持。为了更轻松地保护和保护您的数据，FSx ONTAP支持流行的数据安全和防病毒应用程序。

欲了解更多信息，请访问"FSx ONTAP作为来宾连接存储"

Cloud Volumes ONTAP (CVO) 作为来宾连接存储

Cloud Volumes ONTAP（或称 CVO）是基于 NetApp 的ONTAP存储软件构建的业界领先的云数据管理解决方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的软件定义版本，使用云原生存储，允许您在云端和本地使用相同的存储软件，从而无需重新培训

IT 人员采用全新方法来管理数据。

CVO 使客户能够无缝地将数据从边缘移动到数据中心、云端并返回，从而将您的混合云整合在一起 - 所有这些都通过单一窗格管理控制台NetApp Cloud Manager 进行管理。

通过设计，CVO 可提供极高的性能和先进的数据管理功能，以满足您在云中最苛刻的应用程序的需求。

欲了解更多信息，请访问"CVO 作为客户连接存储"。

TR-4938：使用 **VMware Cloud on AWS** 将**Amazon FSx ONTAP**挂载为 **NFS** 数据存储

本文档概述了如何使用 VMware Cloud on AWS 将Amazon FSx ONTAP作为 NFS 数据存储挂载。

简介

每个成功的组织都走在转型和现代化的道路上。作为此过程的一部分，公司通常利用其现有的 VMware 投资来利用云优势并探索如何尽可能无缝地迁移、爆发、扩展和为流程提供灾难恢复。迁移到云的客户必须评估弹性和爆发、数据中心退出、数据中心整合、生命周期终止场景、合并、收购等用例。

尽管 VMware Cloud on AWS 是大多数客户的首选，因为它为客户提供了独特的混合功能，但有限的本机存储选项限制了它对于存储工作负载繁重的组织的实用性。由于存储直接与主机绑定，因此扩展存储的唯一方法是添加更多主机，这可能会使存储密集型工作负载的成本增加 35-40% 或更多。这些工作负载需要额外的存储和隔离性能，而不是额外的马力，但这意味着需要支付额外的主机费用。这就是 "最近的整合"FSx ONTAP对于使用 VMware Cloud on AWS 的存储和性能密集型工作负载非常有用。

让我们考虑以下场景：客户需要八台主机来提供马力（vCPU/vMem），但他们对存储也有很大的需求。根据他们的评估，他们需要 16 台主机来满足存储需求。这会增加总体 TCO，因为他们必须购买所有额外的马力，而他们真正需要的只是更多的存储空间。这适用于任何用例，包括迁移、灾难恢复、爆发、开发/测试等等。

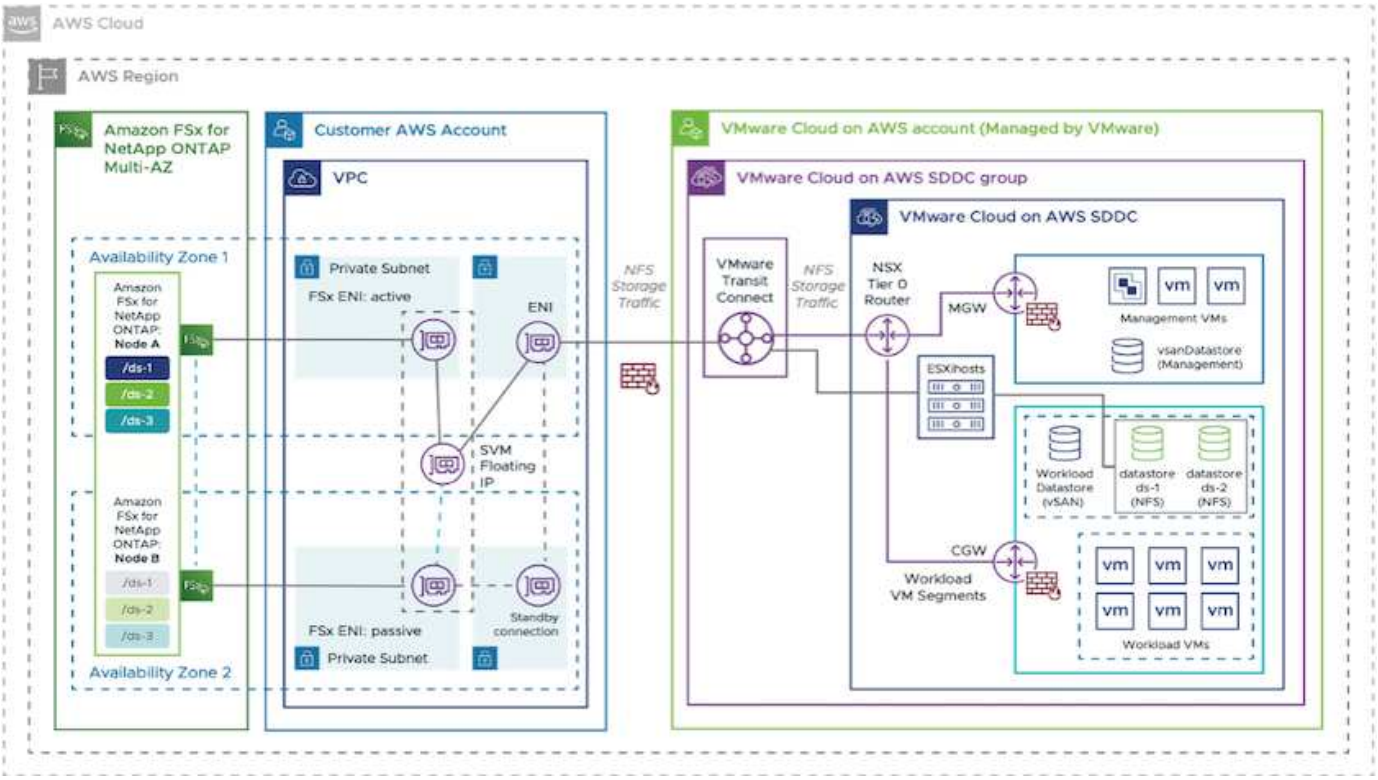
本文档将引导您完成将 FSx ONTAP配置并连接为 VMware Cloud on AWS 的 NFS 数据存储所需的步骤。

VMware 也提供此解决方案。请访问"VMware Cloud on AWS 文档"了解更多信息。

连接选项

VMware Cloud on AWS 支持 FSx ONTAP的多可用区和单可用区部署。

本节介绍高级连接架构以及实施解决方案所需的步骤，以扩展 SDDC 集群中的存储，而无需添加其他主机。



高级部署步骤如下：

1. 在新的指定 VPC 中创建Amazon FSx ONTAP 。
2. 创建 SDDC 组。
3. 创建 VMware Transit Connect 和 TGW 附件。
4. 配置路由（AWS VPC 和 SDDC）和安全组。
5. 将 NFS 卷作为数据存储附加到 SDDC 集群。

在将 FSx ONTAP配置并连接为 NFS 数据存储之前，您必须首先设置 VMware on Cloud SDDC 环境或将现有 SDDC 升级到 v1.20 或更高版本。有关更多信息，请参阅"VMware Cloud on AWS 入门" 。

FSx ONTAP目前不支持延伸集群。

结束语

本文档介绍了使用 AWS 上的 VMware 云配置Amazon FSx ONTAP所需的步骤。 Amazon FSx ONTAP提供了部署和管理应用程序工作负载以及文件服务的绝佳选项，同时通过使数据需求无缝连接到应用程序层来降低 TCO。无论使用情况如何，选择 VMware Cloud on AWS 以及Amazon FSx ONTAP都可以快速实现云优势、一致的基础架构和从本地到 AWS 的操作、工作负载的双向可移植性以及企业级容量和性能。它与连接存储所用的过程和程序相同。请记住，只是数据的位置随着新名称而发生了变化；工具和流程都保持不变， Amazon FSx ONTAP有助于优化整体部署。

要了解有关此过程的更多信息，请随意观看详细的演示视频。

Amazon FSx ONTAP VMware 云

VMware Cloud 准备就绪并连接到 AWS VPC 后，您必须将Amazon FSx ONTAP部署到新指定的 VPC 中，而不是原来连接的或现有的默认 VPC 中。

首先，在 SDDC 所在的同一区域和可用区中部署一个额外的 VPC，然后将Amazon FSx ONTAP部署到新的 VPC 中。 "VMware Cloud 中的 SDDC 组的配置"控制台启用连接到将部署 FSx ONTAP 的新指定的 VPC 所需的网络配置选项。

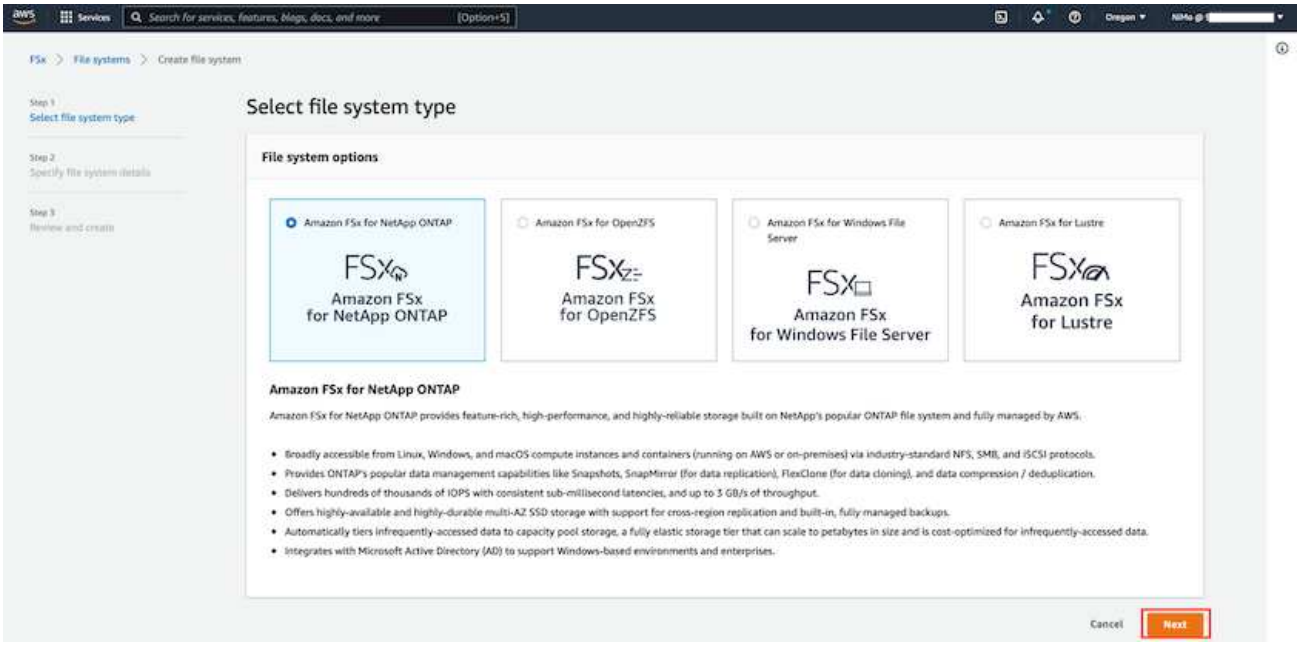
在与 VMware Cloud on AWS SDDC 相同的可用区域中部署 FSx ONTAP 。

您无法在已连接的 VPC 中部署 FSx ONTAP 。相反，您必须将其部署在新的指定 VPC 中，然后通过 SDDC 组将 VPC 连接到 VMware Managed Transit Gateway (vTGW)。

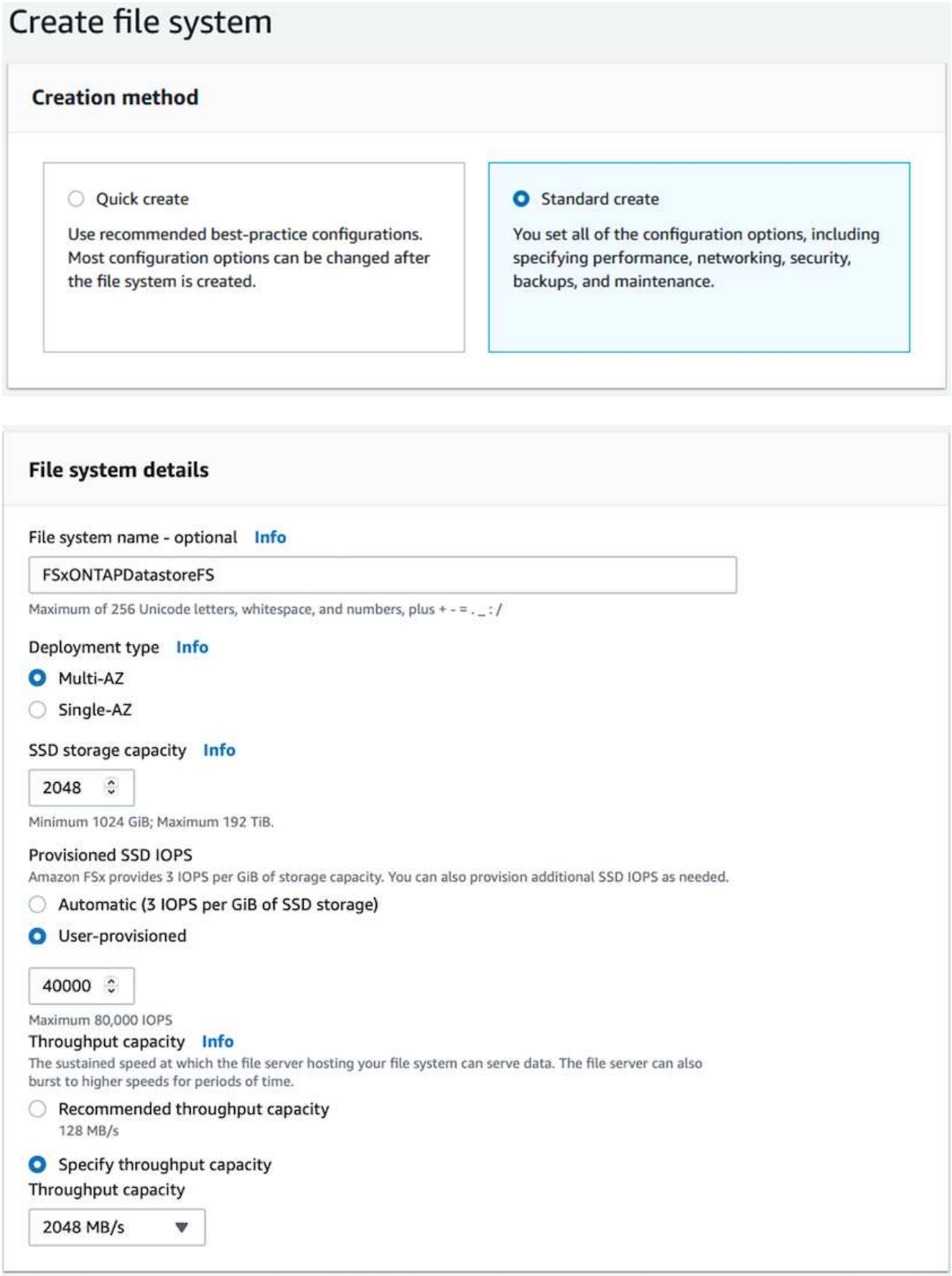
▼ 步骤 **1**：在新的指定 **VPC** 中创建**Amazon FSx ONTAP**

要创建和挂载Amazon FSx ONTAP文件系统，请完成以下步骤：

1. 打开Amazon FSx控制台 `https://console.aws.amazon.com/fsx/`并选择*创建文件系统*来启动*文件系统创建*向导。
2. 在选择文件系统类型页面上，选择 * Amazon FSx ONTAP*，然后单击 下一步。出现“创建文件系统”页面。



3. 对于创建方法，选择*标准创建*。



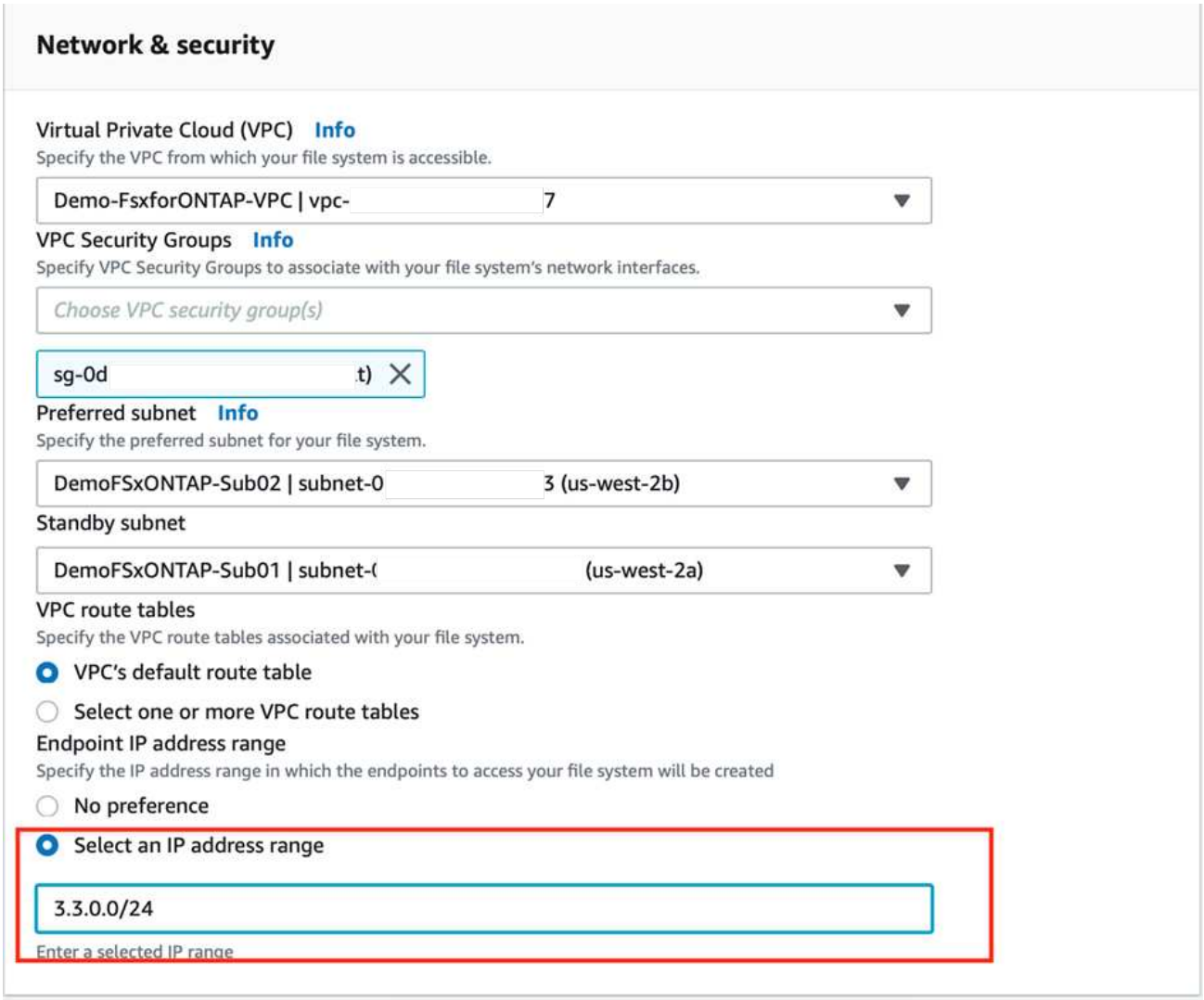
不同客户的数据存储大小差异很大。虽然每个 NFS 数据存储区建议的虚拟机数量是主观的，但许多因素决定了可放置在每个数据存储区上的虚拟机的最佳数量。虽然大多数管理员

只考虑容量，但发送到 VMDK 的并发 I/O 量是影响整体性能的最重要因素之一。使用本地的性能统计数据来相应地调整数据存储卷的大小。

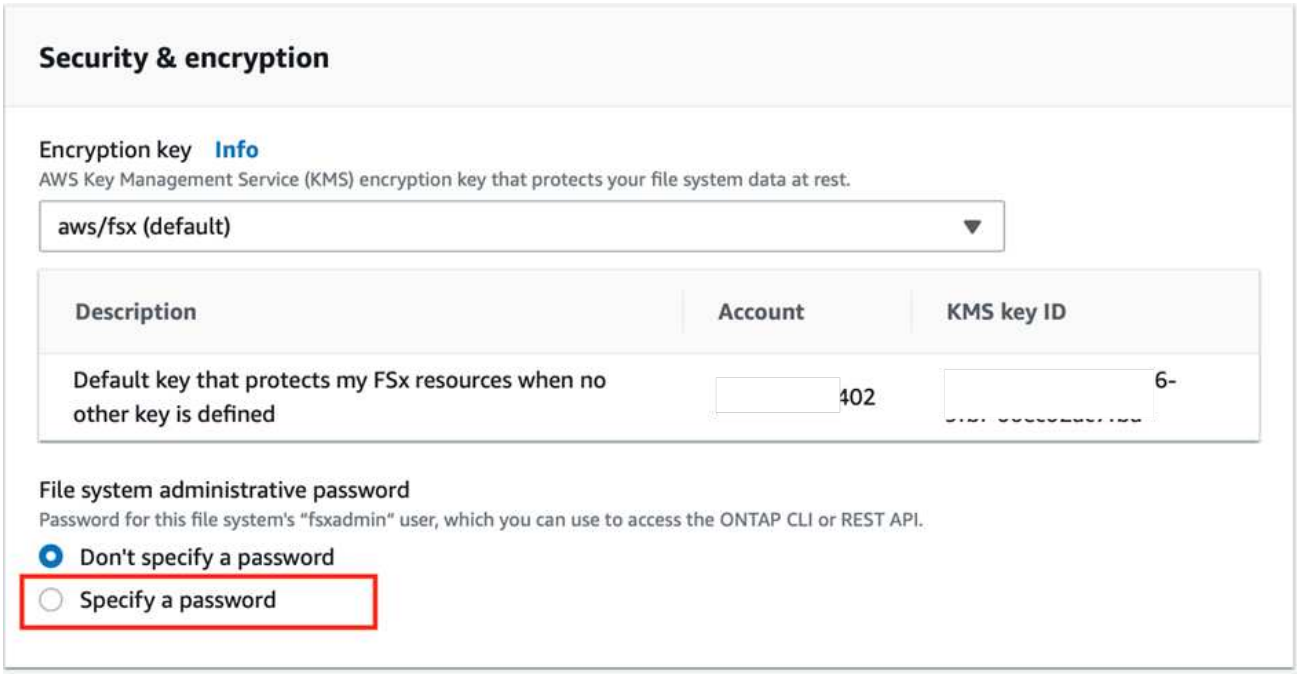
4. 在虚拟私有云 (VPC) 的 网络 部分中，选择适当的 VPC 和首选子网以及路由表。在这种情况下，从下拉菜单中选择 Demo-FSxforONTAP-VPC。

确保这是一个新的指定 VPC，而不是连接的 VPC。

默认情况下，FSx ONTAP使用 198.19.0.0/16 作为文件系统的默认端点 IP 地址范围。确保端点 IP 地址范围与 AWS SDDC 上的 VMC、关联的 VPC 子网和本地基础设施不冲突。如果您不确定，请使用没有冲突的不重叠范围。

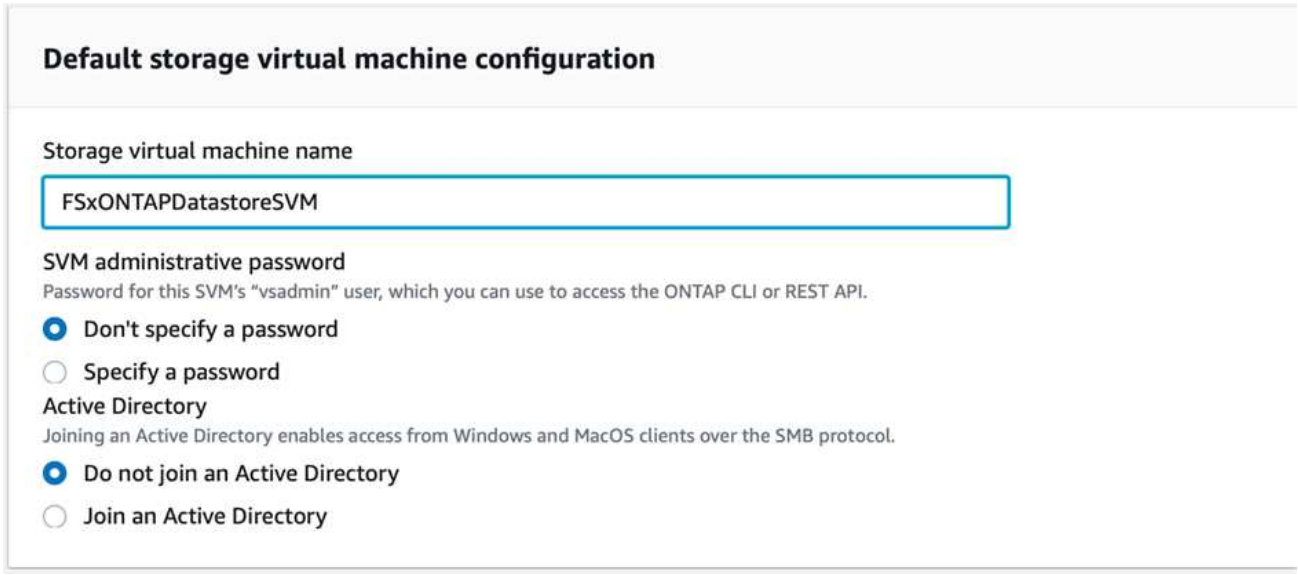


5. 在加密密钥的“安全和加密”部分中，选择保护文件系统静态数据的 AWS Key Management Service (AWS KMS) 加密密钥。对于*文件系统管理密码*，请输入 fsxadmin 用户的安全密码。



6. 在“默认存储虚拟机配置”部分中，指定 SVM 的名称。

从 GA 开始，支持四个 NFS 数据存储。



7. 在“默认卷配置”部分中，指定数据存储所需的卷名称和大小，然后单击“下一步”。这应该是一个 NFSv3 卷。对于*存储效率*，选择*已启用*以打开ONTAP存储效率功能（压缩、重复数据删除和压缩）。创建完成后，使用shell使用*_volumemodify_*修改卷参数，如下所示：

设置	配置
容量保证（空间保证方式）	无（精简配置）– 默认设置
fractional_reserve（部分储备）	0% – 默认设置
snap_reserve（快照空间百分比）	0%

设置	配置
自动调整大小（自动调整大小模式）	grow_shrink
存储效率	已启用 – 默认设置
自动删除	卷/oldest_first
卷分层策略	仅限快照 – 默认设置
尝试先行	自动增长
Snapshot 策略	无

使用以下 SSH 命令创建和修改卷：

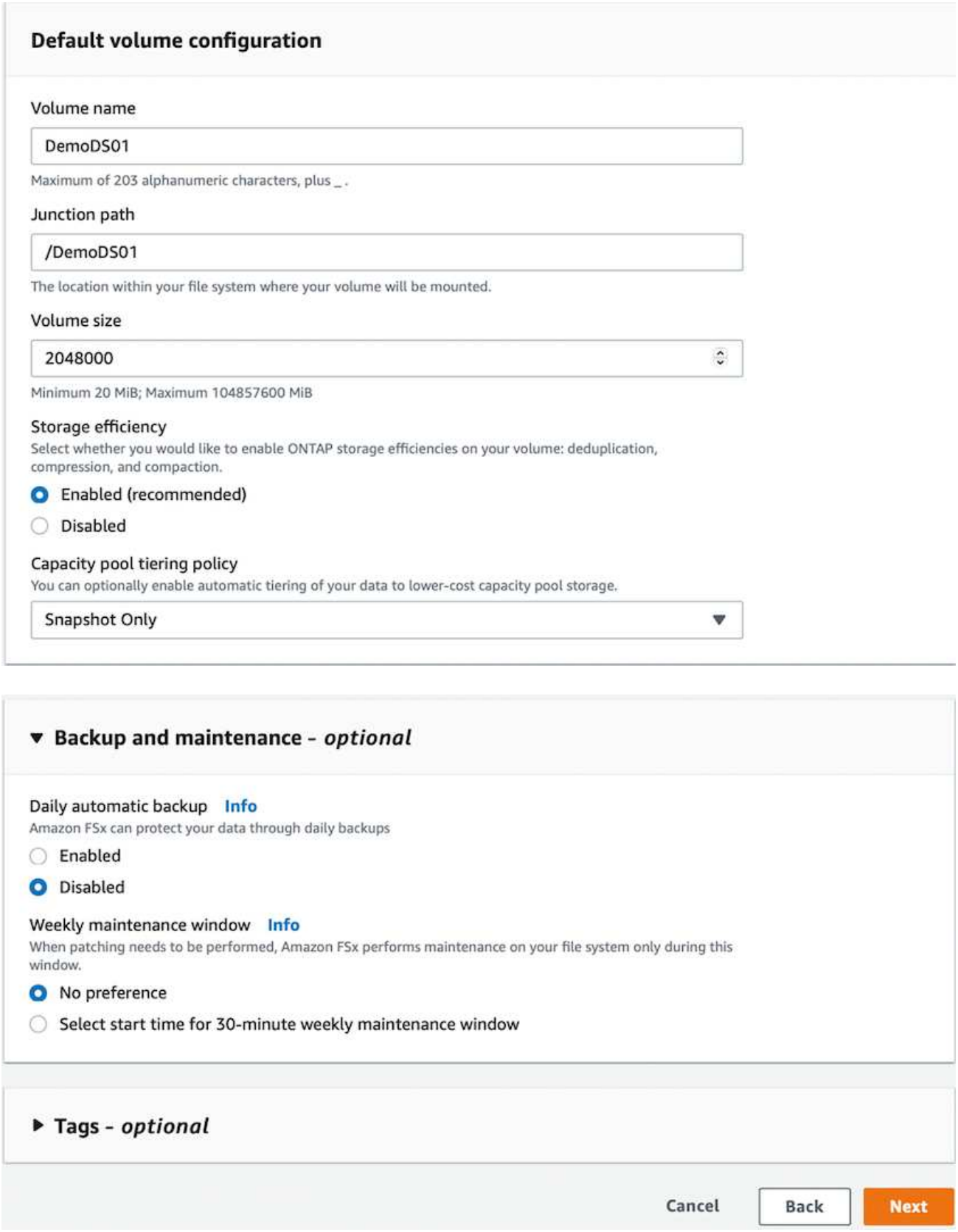
从 **shell** 创建新数据存储卷的命令：

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy snapshot-
only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy
none -junction-path /DemoDS002
```

*注意：*通过 shell 创建的卷将需要几分钟才能显示在 AWS 控制台中。

修改默认未设置的音量参数的命令：

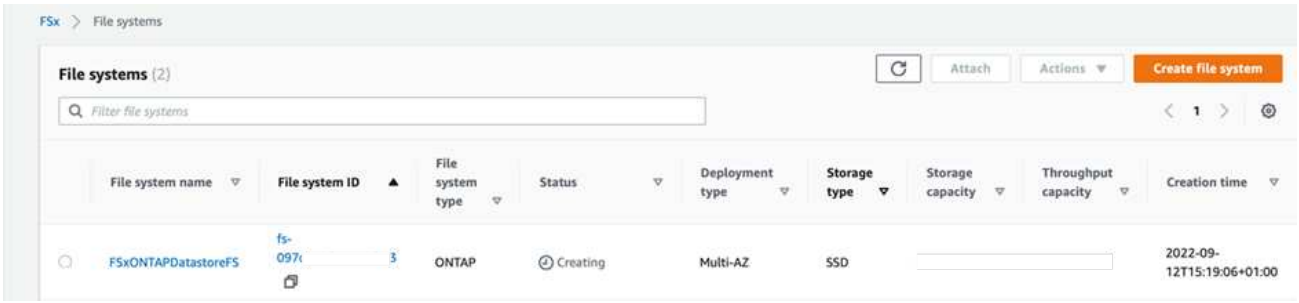
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```

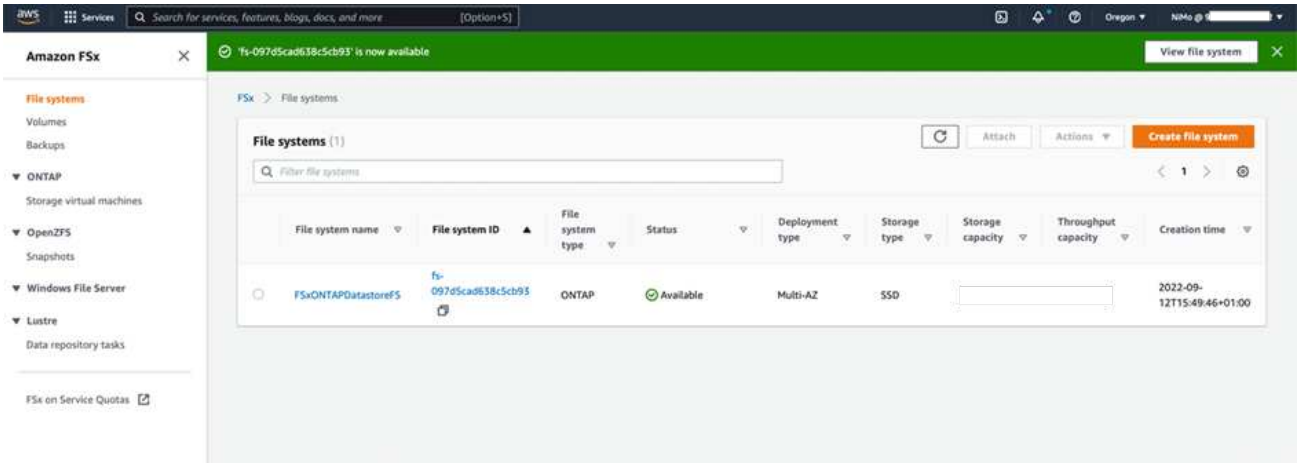


在初始迁移场景中，默认快照策略可能会导致数据存储容量已满的问题。为了克服这个问题，修改快照策略以满足需要。

8. 查看“创建文件系统”页面上显示的文件系统配置。

9. 单击“创建文件系统”。





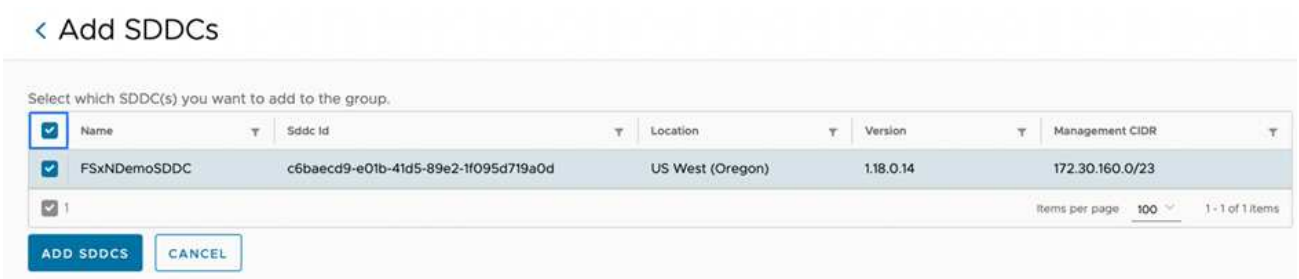
根据容量和性能要求重复上述步骤，创建更多存储虚拟机或文件系统以及数据存储卷。

要了解Amazon FSx ONTAP性能，请参阅 "Amazon FSx ONTAP性能"。

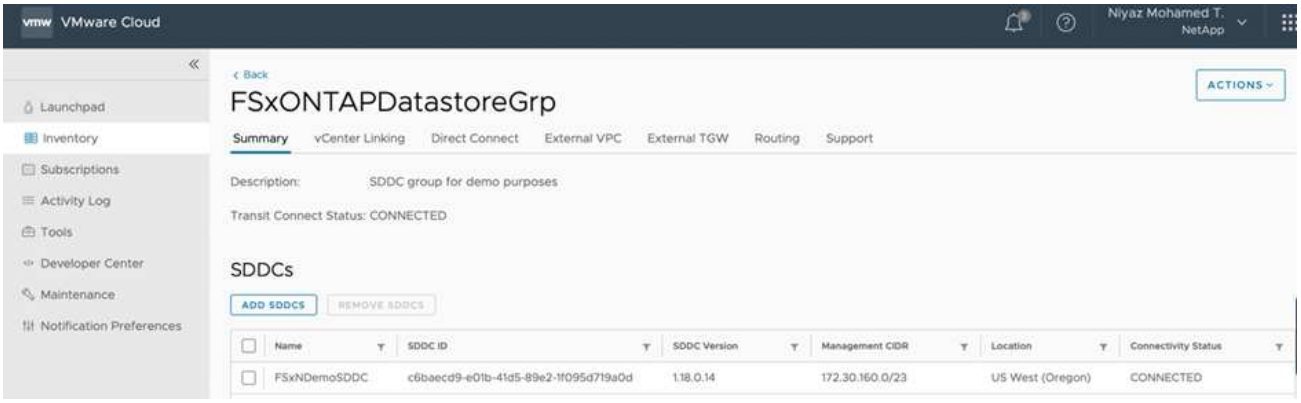
▼ 步骤 2：创建 **SDDC** 组

创建文件系统和 SVM 后，使用 VMware Console 创建 SDDC 组并配置 VMware Transit Connect。为此，请完成以下步骤，并记住必须在 VMware Cloud Console 和 AWS Console 之间导航。

1. 登录 VMC 控制台 `https://vmc.vmware.com`。
2. 在“库存”页面上，单击“**SDDC** 组”。
3. 在 **SDDC Groups** 选项卡上，单击 **ACTIONS** 并选择 **Create SDDC Group**。为了演示目的，SDDC 组被称为 `FSxONTAPDatastoreGrp`。
4. 在成员资格网格上，选择要作为组成员包含的 SDDC。

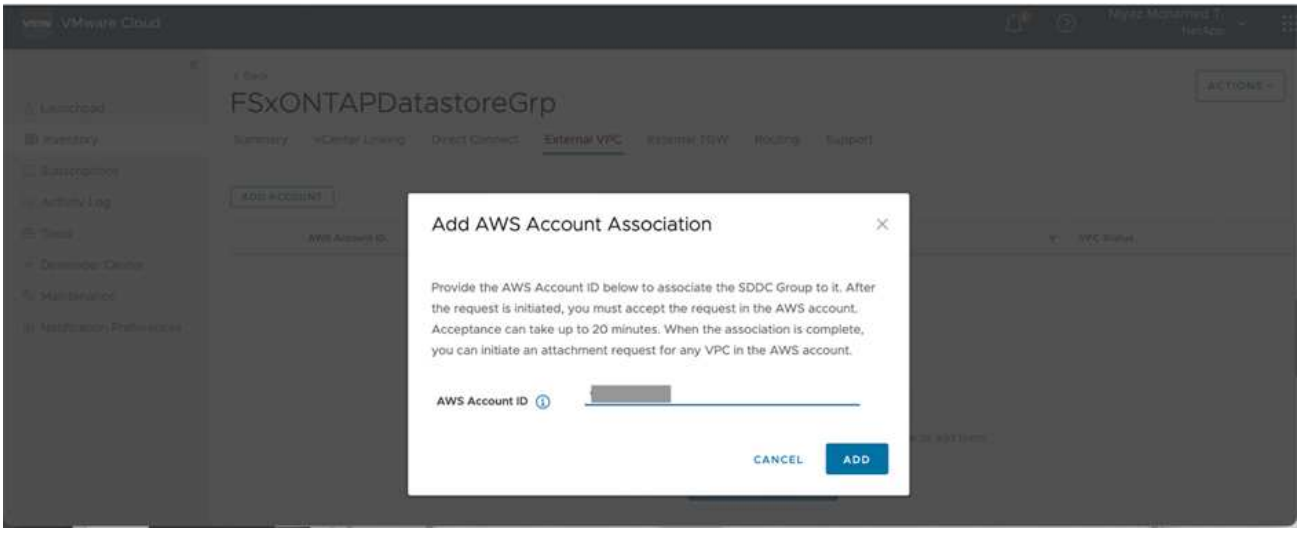


5. 验证是否选中“为您的组配置 VMware Transit Connect 将产生每个附件和数据传输的费用”，然后选择*创建组*。该过程可能需要几分钟才能完成。

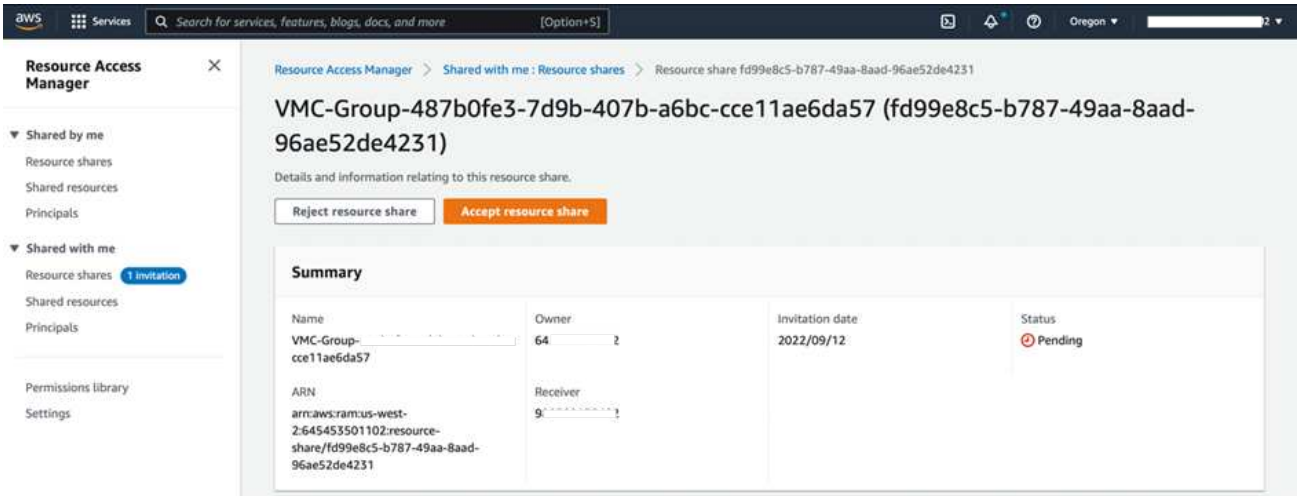


▼ 步骤 **3**：配置 **VMware Transit** 连接

1. 将新创建的指定 VPC 附加到 SDDC 组。选择“外部 VPC”选项卡并按照 "将外部 VPC 附加到组的说明"。此过程可能需要 10-15 分钟才能完成。

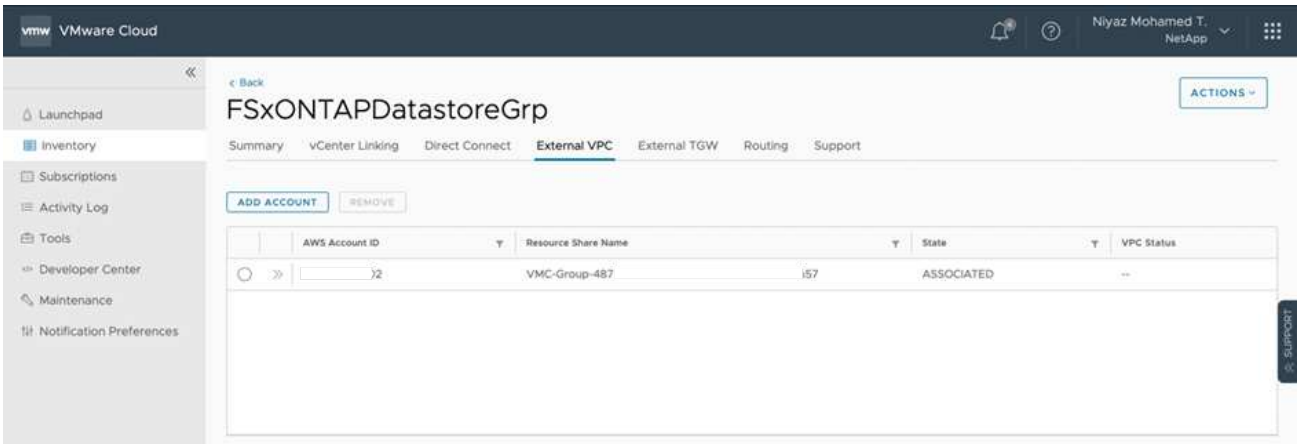


2. 单击“添加帐户”。
   a. 提供用于配置 FSx ONTAP文件系统的 AWS 账户。
   b. 单击“添加”。
3. 返回 AWS 控制台，登录同一个 AWS 账户并导航到 资源访问管理器 服务页面。有一个按钮供您接受资源共享。



作为外部 VPC 流程的一部分，您将通过 AWS 控制台通过资源访问管理器提示新的共享资源。共享资源是由 VMware Transit Connect 管理的 AWS Transit Gateway。

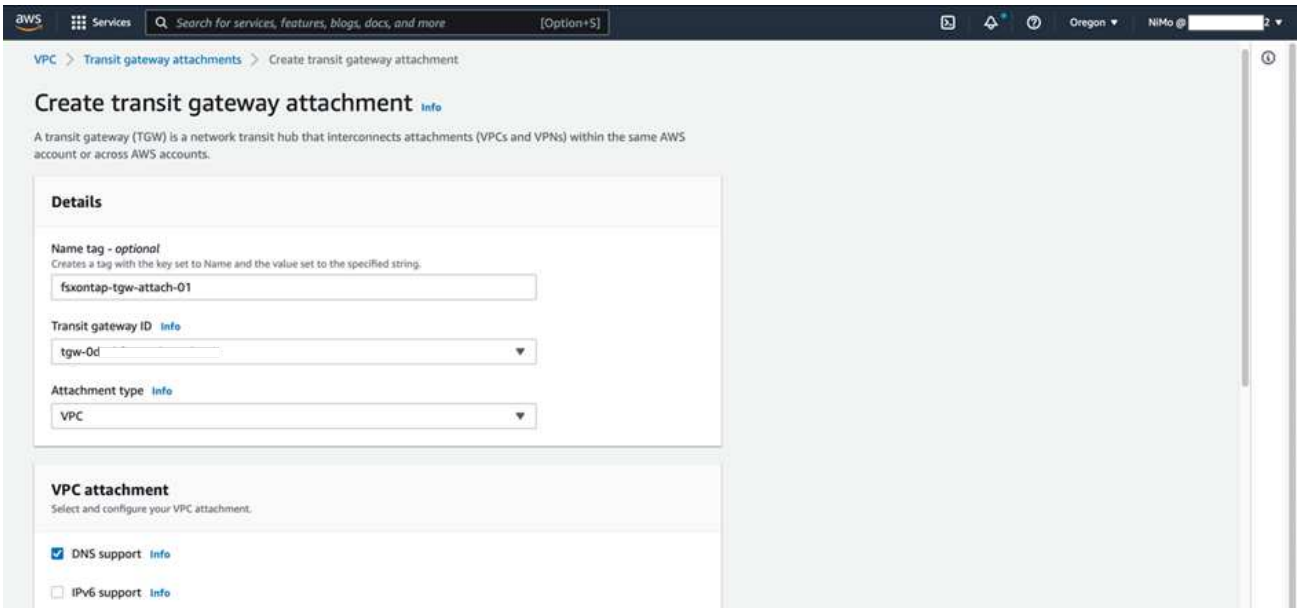
4. 点击*接受资源共享*。



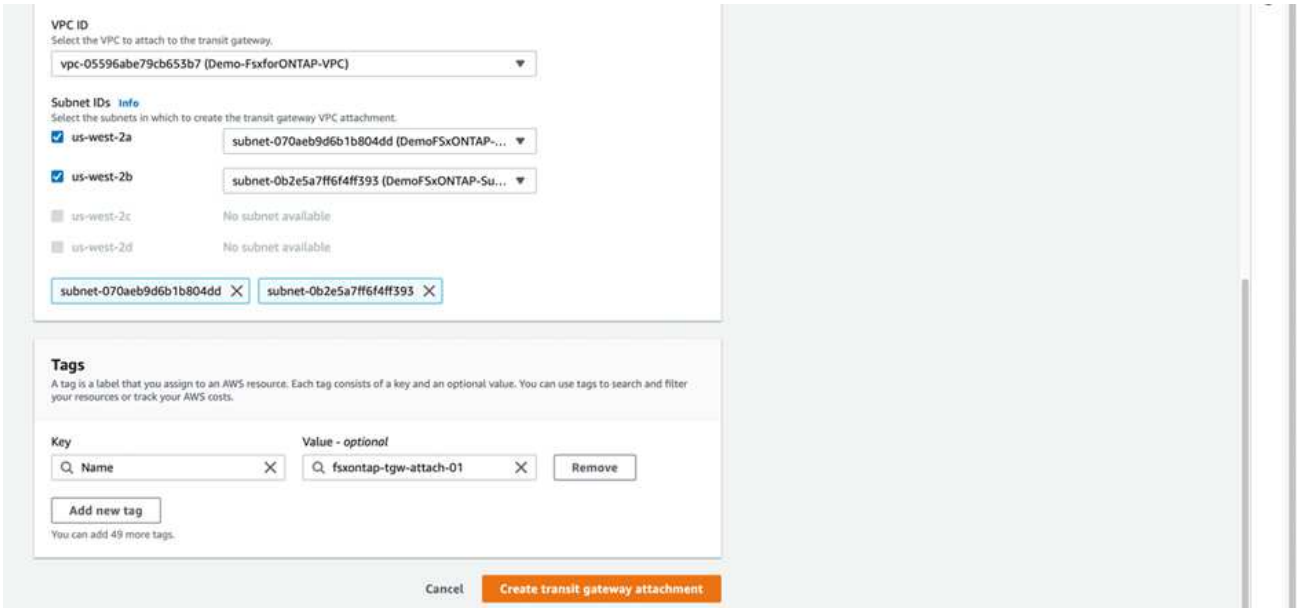
5. 回到 VMC 控制台，您现在看到外部 VPC 处于关联状态。这可能需要几分钟才能出现。

▼ 步骤 **4**：创建中转网关连接

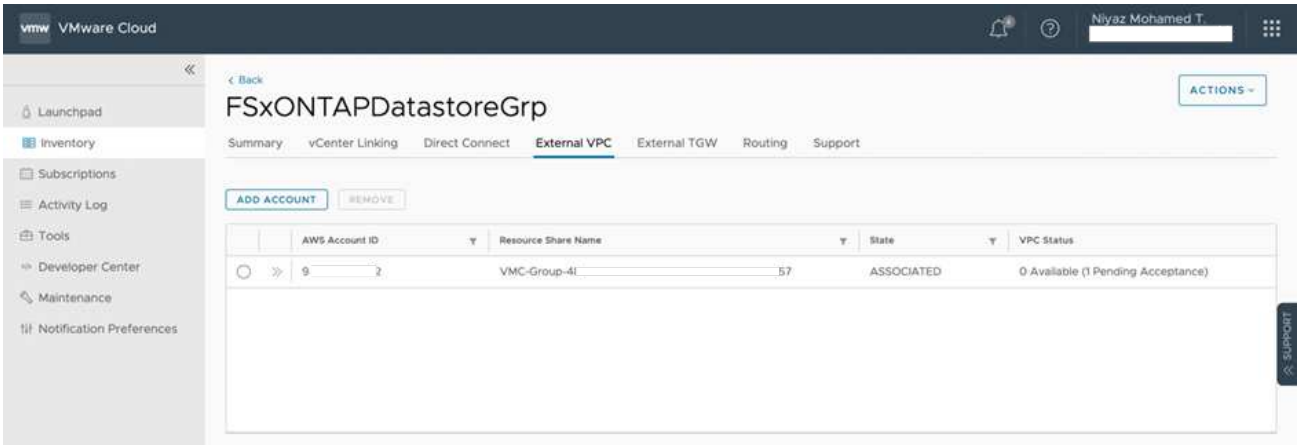
1. 在 AWS 控制台中，转到 VPC 服务页面并导航到用于配置 FSx 文件系统的 VPC。在这里，您可以通过单击右侧导航窗格上的“Transit Gateway Attachment”（中转网关附件）来创建中转网关附件。
2. 在 **VPC** 附件 下，确保选中 DNS 支持并选择部署了 FSx ONTAP的 VPC。

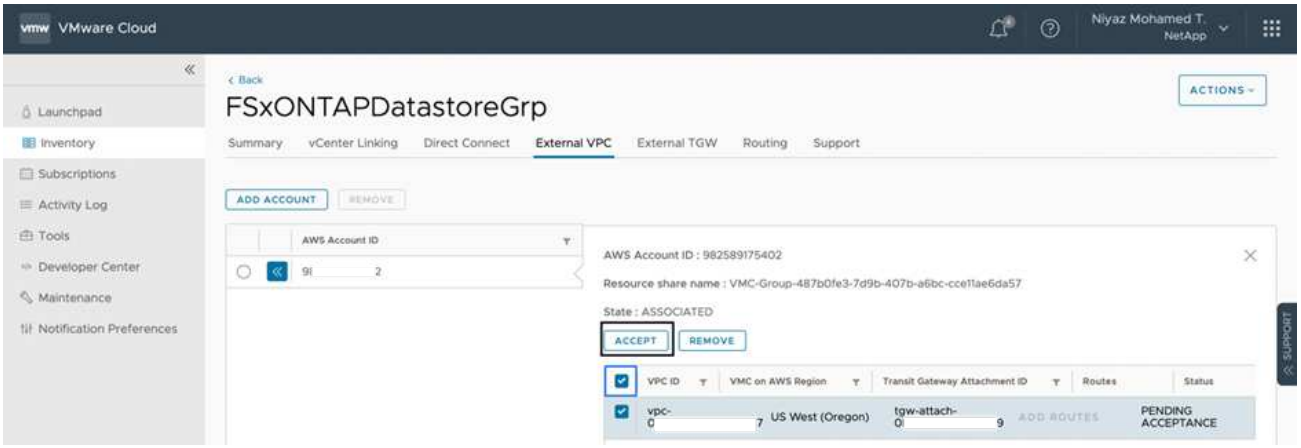


3. 单击“创建”*“中转网关附件”*。



4. 返回 VMware Cloud Console，导航回 SDDC 组 > 外部 VPC 选项卡。选择用于 FSx 的 AWS 账户 ID，单击 VPC，然后单击 接受。

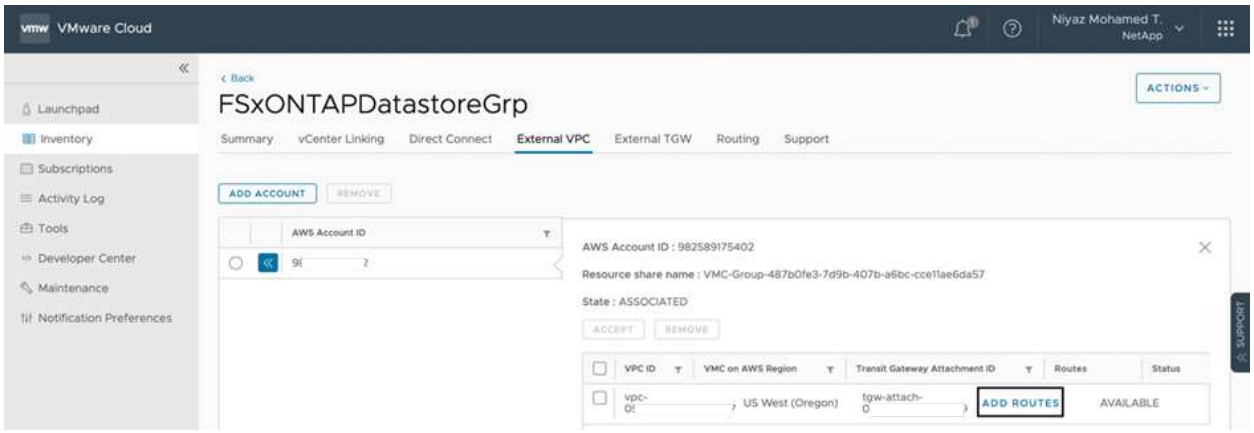


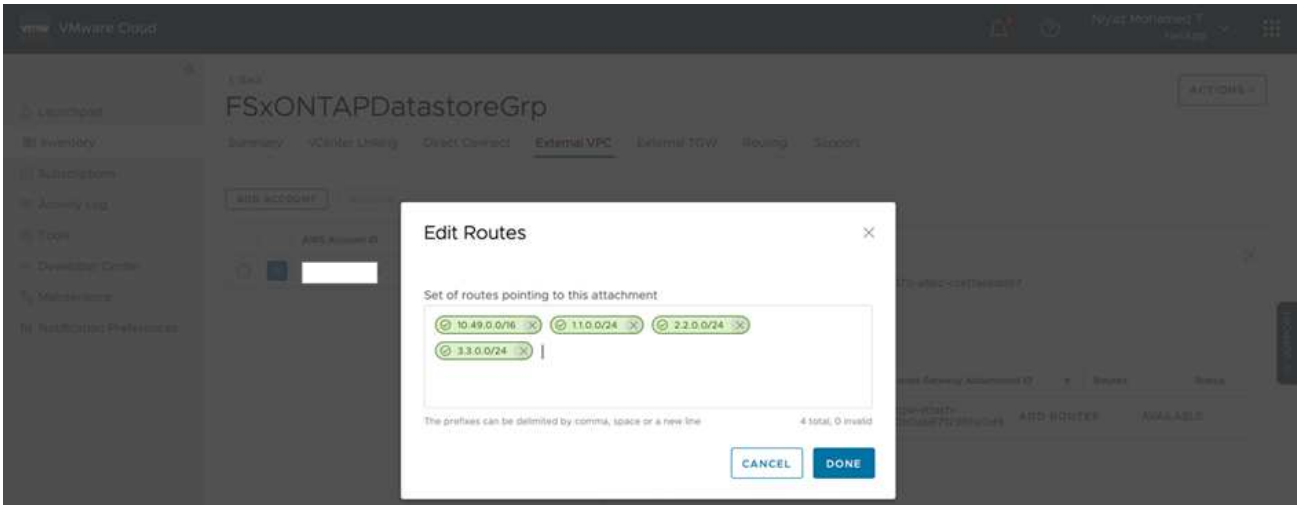


此选项可能需要几分钟才会出现。

5. 然后在 外部 **VPC** 选项卡中的 路由 列中，单击 添加路由 选项并添加所需的路由：

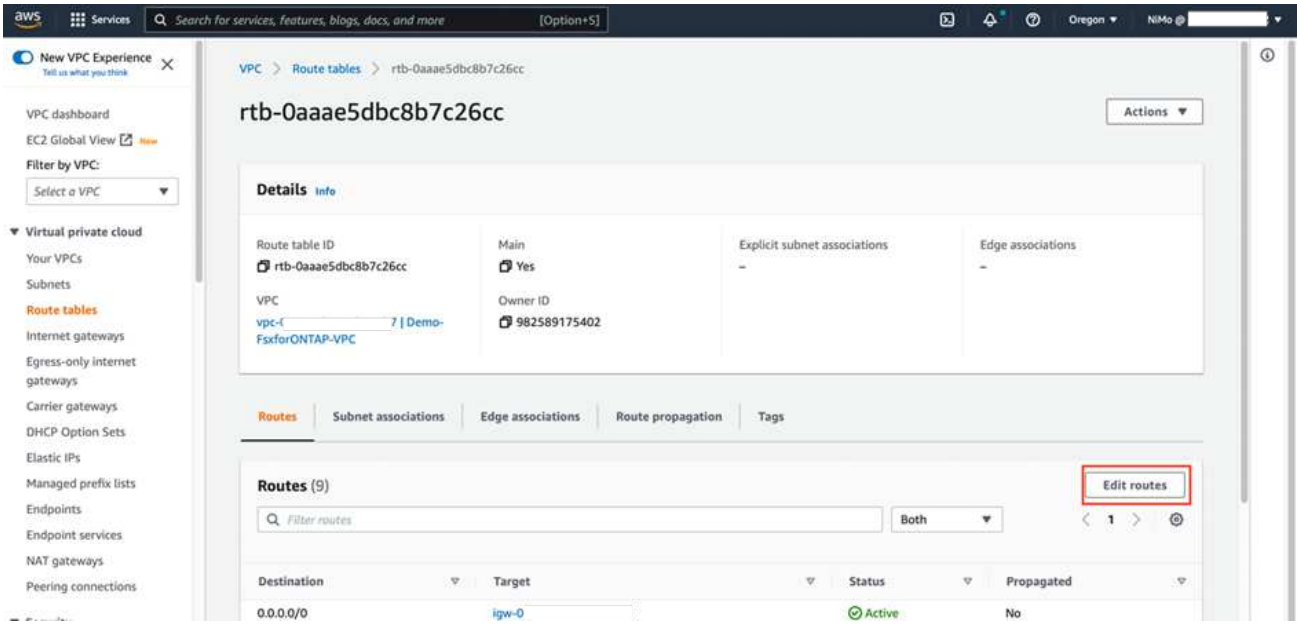
   - Amazon FSx ONTAP浮动 IP 的浮动 IP 范围的路由。
   - 新创建的外部 VPC 地址空间的路由。



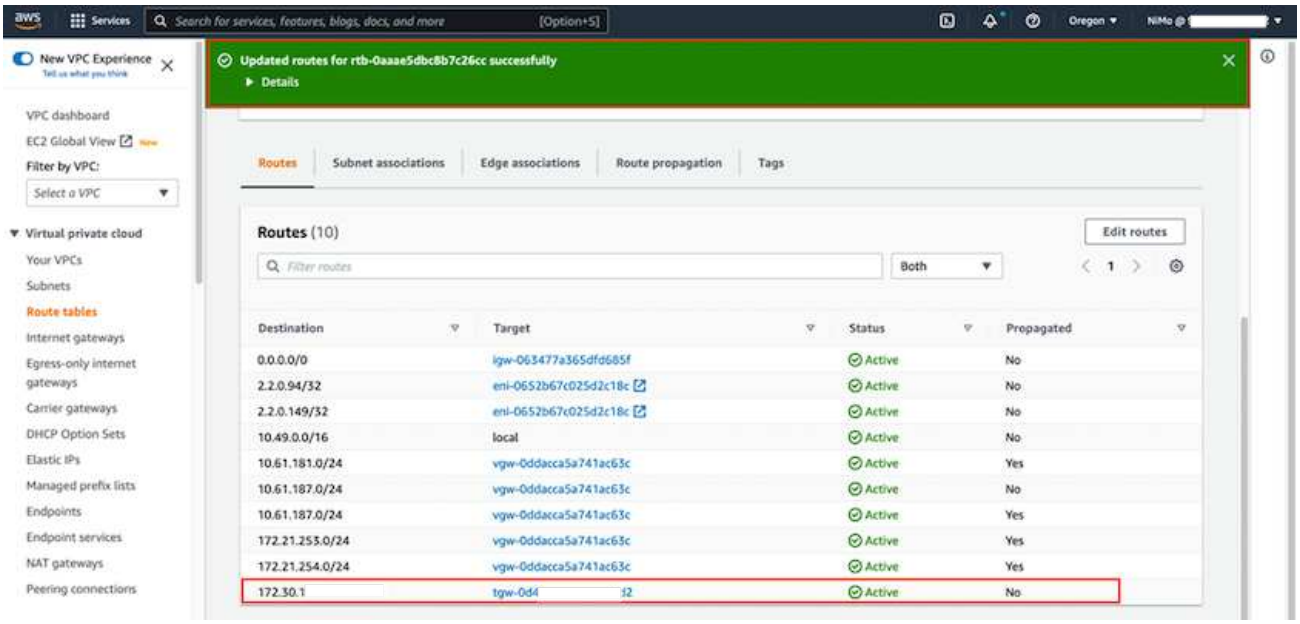


▼ 步骤 **5**：配置路由（**AWS VPC** 和 **SDDC**）和安全组

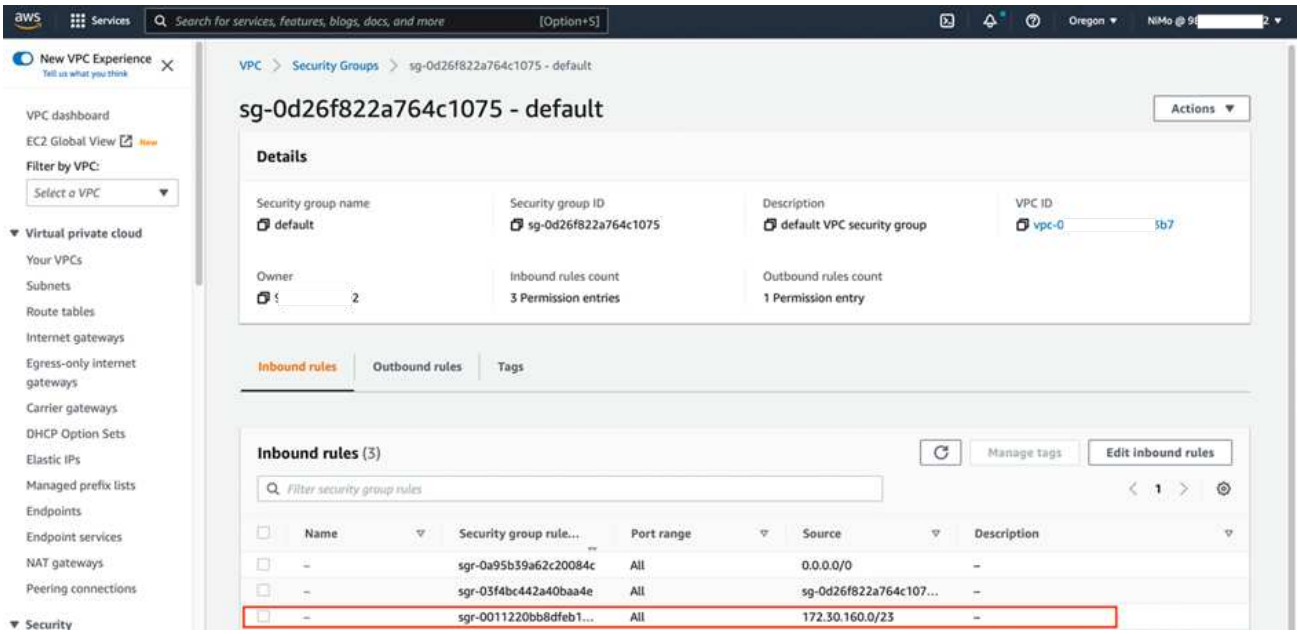
1. 在 AWS 控制台中，通过在 VPC 服务页面中找到 VPC 并选择 VPC 的 主 路由表来创建返回 SDDC 的路由。
2. 浏览到下方面板中的路线表，然后单击“编辑路线”。



3. 在*编辑路由*面板中，单击*添加路由*，然后通过选择*Transit Gateway*和关联的 TGW ID 输入 SDDC 基础架构的 CIDR。单击“保存更改”。



4. 下一步是验证关联 VPC 中的安全组是否使用 SDDC 组 CIDR 的正确入站规则进行更新。
5. 使用 SDDC 基础架构的 CIDR 块更新入站规则。



验证 VPC（FSx ONTAP所在的位置）路由表是否已更新，以避免出现连接问题。

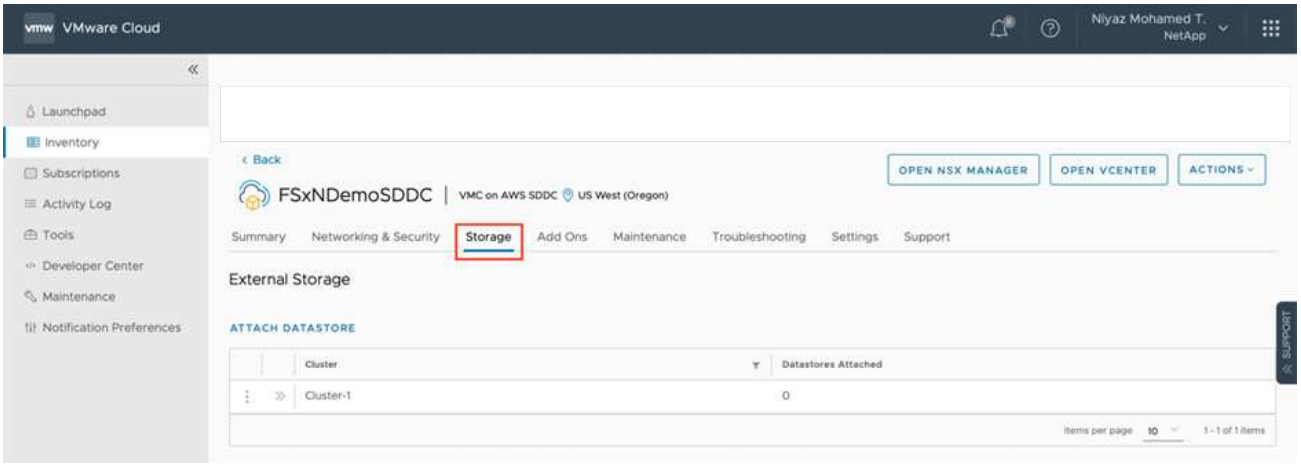
更新安全组以接受 NFS 流量。

这是准备与适当的 SDDC 连接的最后一步。配置文件系统、添加路由并更新安全组后，就可以挂载数据存储了。

▼ 步骤 **6**：将 **NFS** 卷作为数据存储附加到 **SDDC** 集群

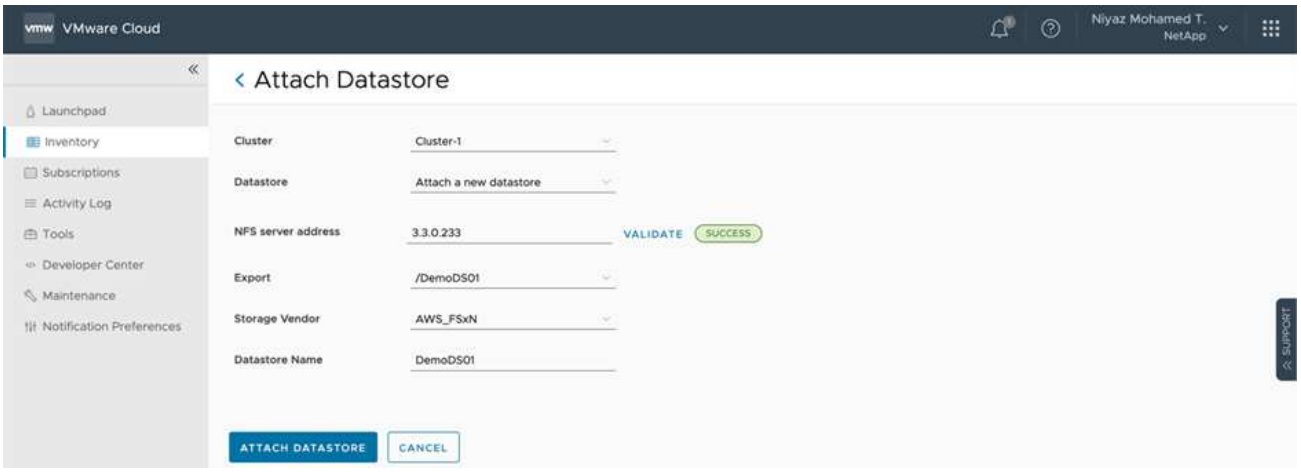
在配置文件系统并建立连接后，访问 VMware Cloud Console 来挂载 NFS 数据存储。

1. 在 VMC 控制台中，打开 SDDC 的 存储 选项卡。

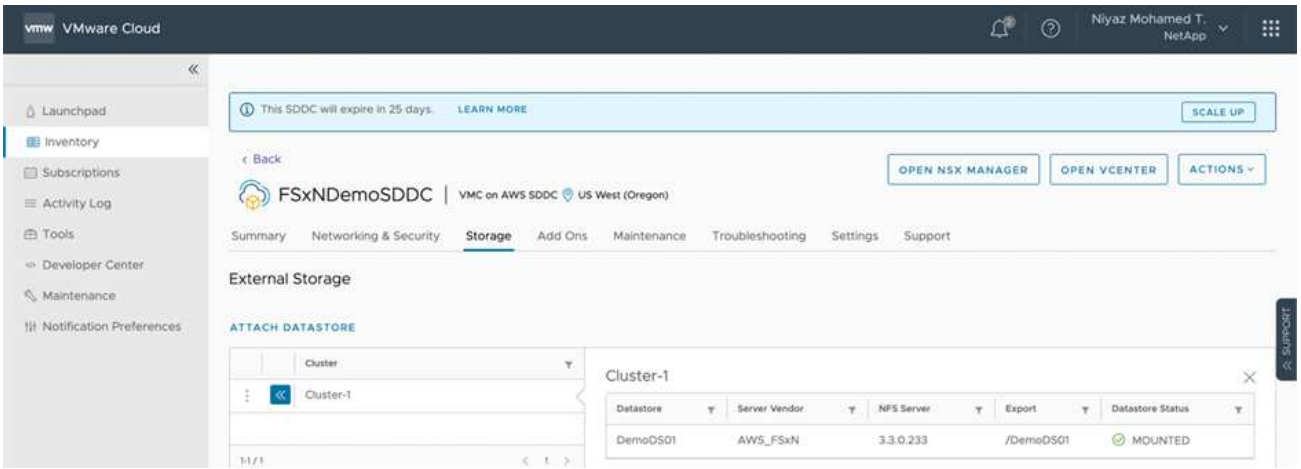


2. 单击“附加数据存储”并填写所需的值。

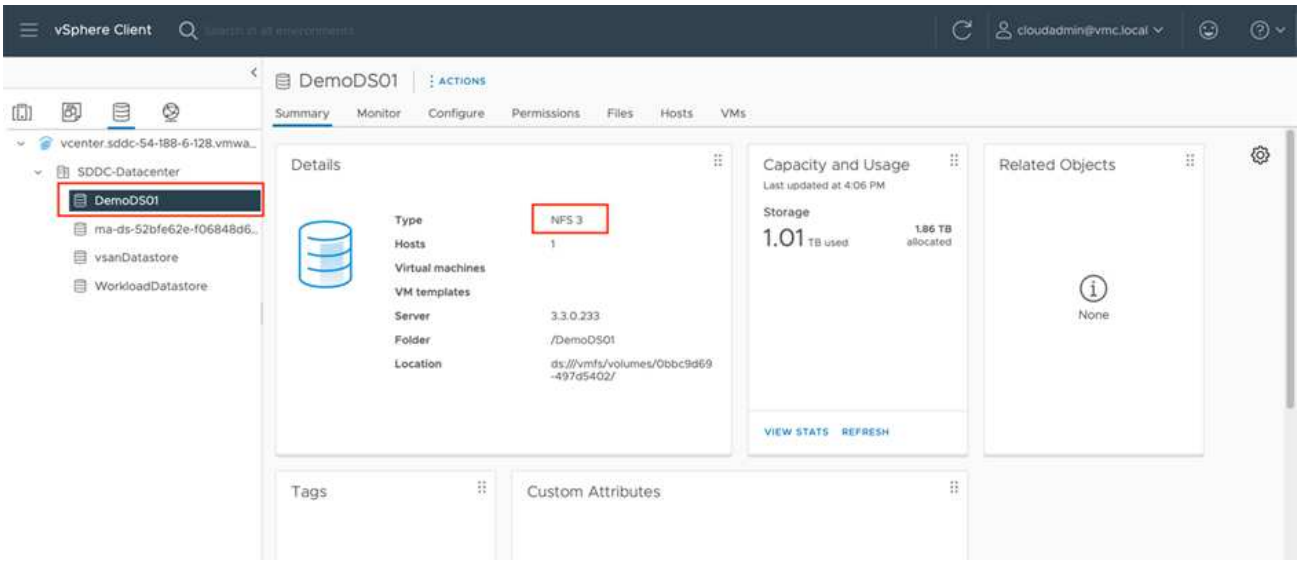
NFS 服务器地址是 NFS IP 地址，可以在 AWS 控制台中的 FSx > 存储虚拟机选项卡 > 端点下找到。



3. 单击“**ATTACH DATASTORE**”将数据存储附加到集群。



4. 通过访问 vCenter 来验证 NFS 数据存储，如下所示：



适用于 **AWS** 的**NetApp**来宾连接存储选项

AWS 支持使用本机 FSx 服务 (FSx ONTAP) 或Cloud Volumes ONTAP (CVO) 连接来宾的NetApp存储。

FSx ONTAP

Amazon FSx ONTAP是一项完全托管的服务，它基于 NetApp 流行的ONTAP文件系统构建，提供高度可靠、可扩展、高性能且功能丰富的文件存储。 FSx ONTAP将NetApp文件系统的熟悉功能、性能、功能和 API 操作与完全托管的 AWS 服务的灵活性、可扩展性和简单性相结合。

FSx ONTAP提供功能丰富、快速且灵活的共享文件存储，可从在 AWS 或本地运行的 Linux、Windows 和 macOS 计算实例广泛访问。 FSx ONTAP提供具有亚毫秒级延迟的高性能固态硬盘 (SSD) 存储。借助 FSx ONTAP，您可以为您的工作负载实现 SSD 级别的性能，同时只需为一小部分数据支付 SSD 存储费用。

使用 FSx ONTAP管理数据更容易，因为您只需单击按钮即可快照、克隆和复制文件。此外，FSx ONTAP会自动将您的数据分层到成本较低的弹性存储中，从而减少您配置或管理容量的需要。

FSx ONTAP还提供高可用性和持久性存储，具有完全托管的备份和跨区域灾难恢复支持。为了更轻松地保护和保护您的数据，FSx ONTAP支持流行的数据安全和防病毒应用程序。

FSx ONTAP作为来宾连接存储

▼ 使用 **VMware Cloud on AWS** 配置**Amazon FSx ONTAP**

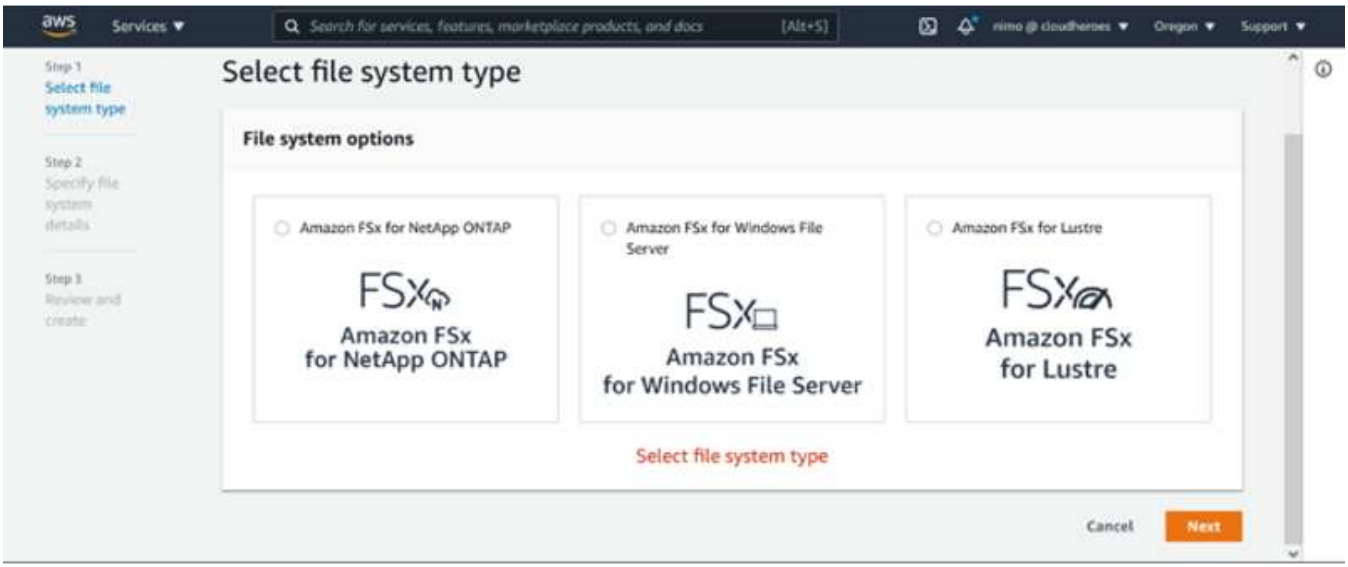
可以从在 AWS 的 VMware Cloud 上的 VMware SDDC 环境中创建的虚拟机挂载Amazon FSx ONTAP文件共享和 LUN。这些卷还可以安装在 Linux 客户端上，并使用 NFS 或 SMB 协议映射到 Windows 客户端上，并且当通过 iSCSI 安装时，可以在 Linux 或 Windows 客户端上将 LUNS 作为块设备进行访问。可以按照以下步骤快速设置适用于NetApp ONTAP文件系统的Amazon FSx 。

> Amazon FSx ONTAP和 VMware Cloud on AWS 必须位于同一可用区，才能获得更好的性能并避免可用区之间的数据传输费用。

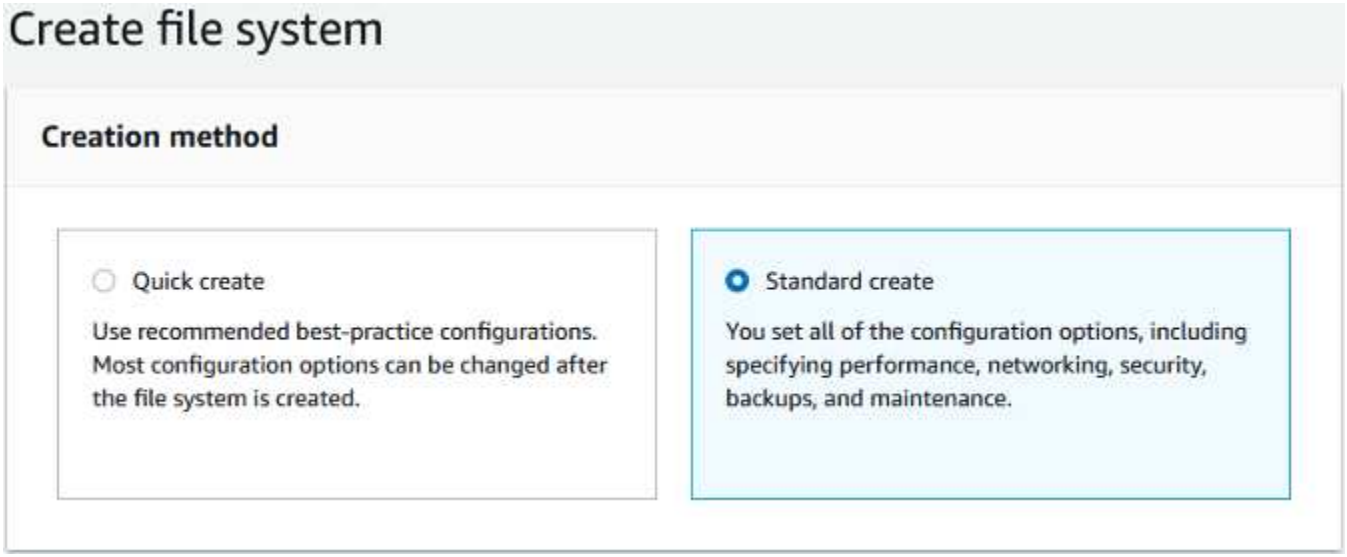
▼ 创建并挂载**Amazon FSx ONTAP**卷

要创建和挂载Amazon FSx ONTAP文件系统，请完成以下步骤：

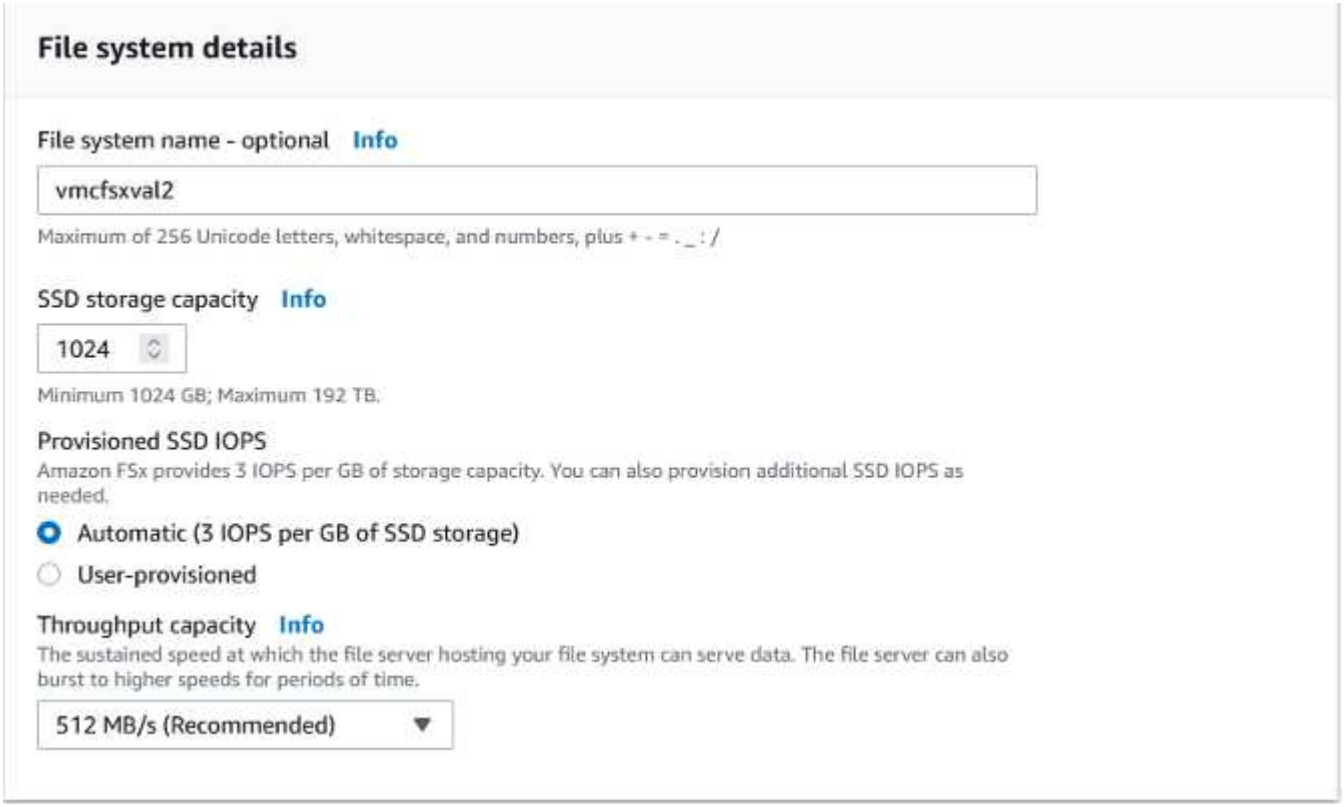
1. 打开"Amazon FSx控制台"并选择创建文件系统以启动文件系统创建向导。
2. 在选择文件系统类型页面上，选择Amazon FSx ONTAP，然后选择下一步。出现“创建文件系统”页面。



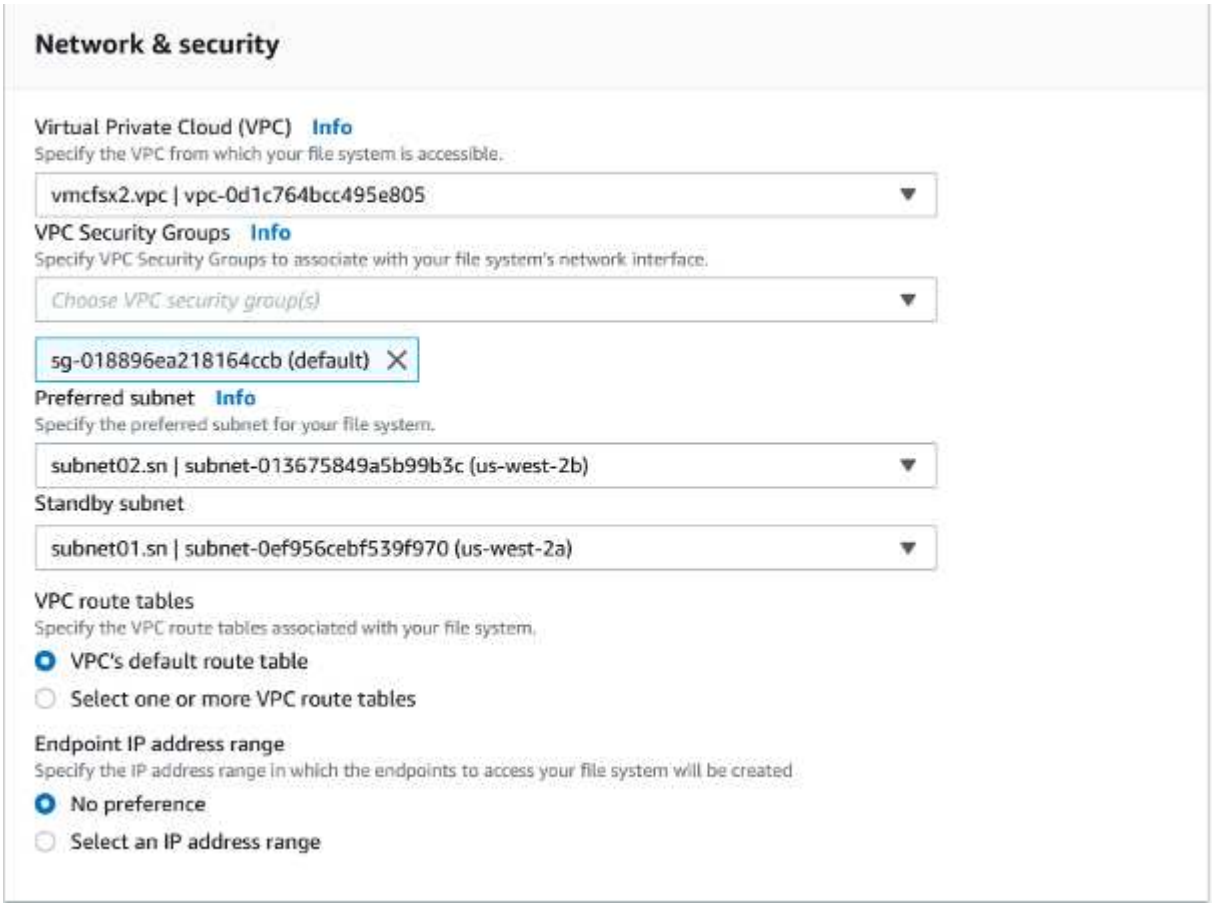
1. 在网络部分中，对于虚拟私有云 (VPC)，选择适当的 VPC 和首选子网以及路由表。在这种情况下，从下拉菜单中选择了 vmcfsx2.vpc。



1. 对于创建方法，请选择标准创建。您也可以选择“快速创建”，但本文档使用“标准创建”选项。

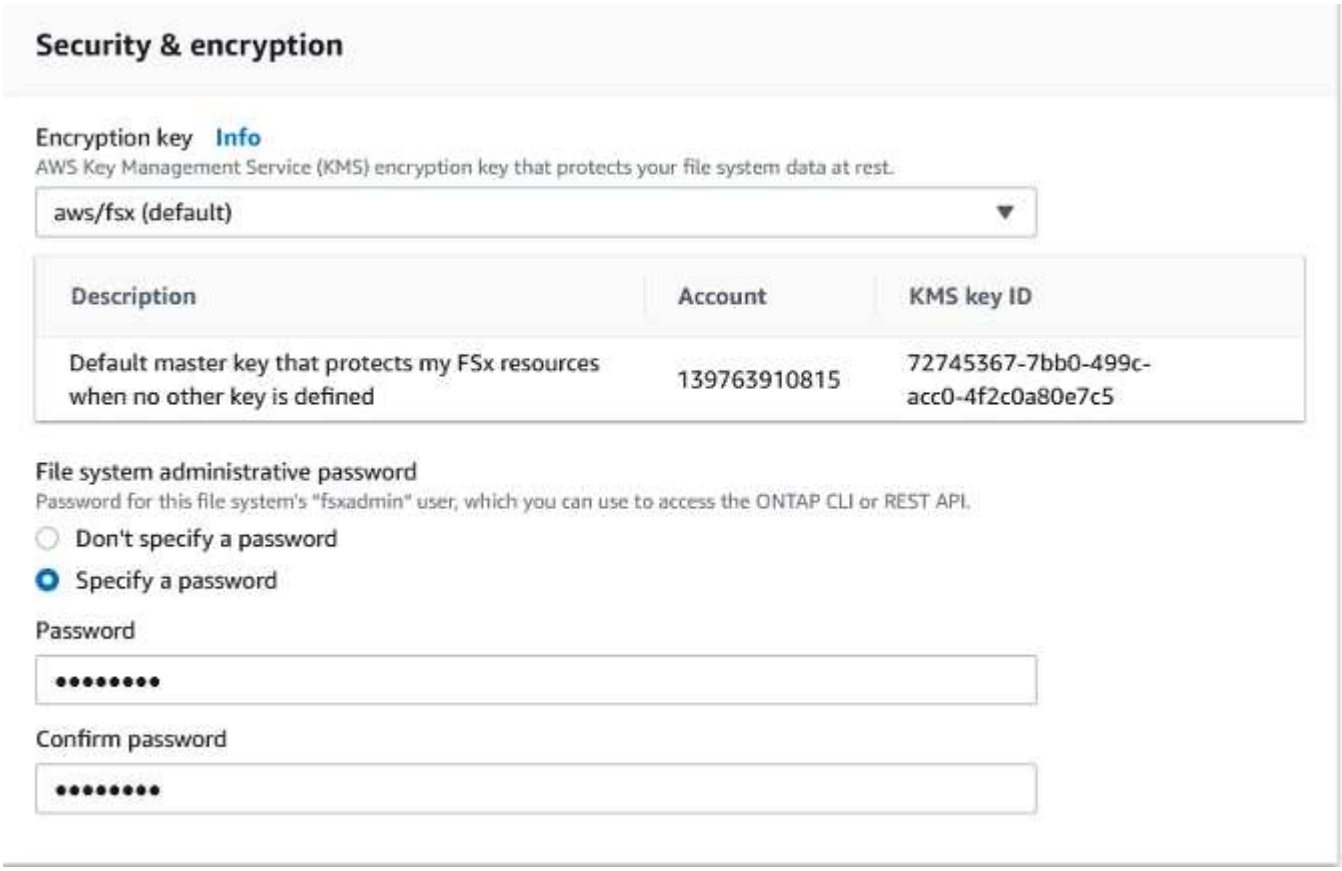


1. 在网络部分中，对于虚拟私有云 (VPC)，选择适当的 VPC 和首选子网以及路由表。在这种情况下，从下拉菜单中选择了 vmcfsx2.vpc。

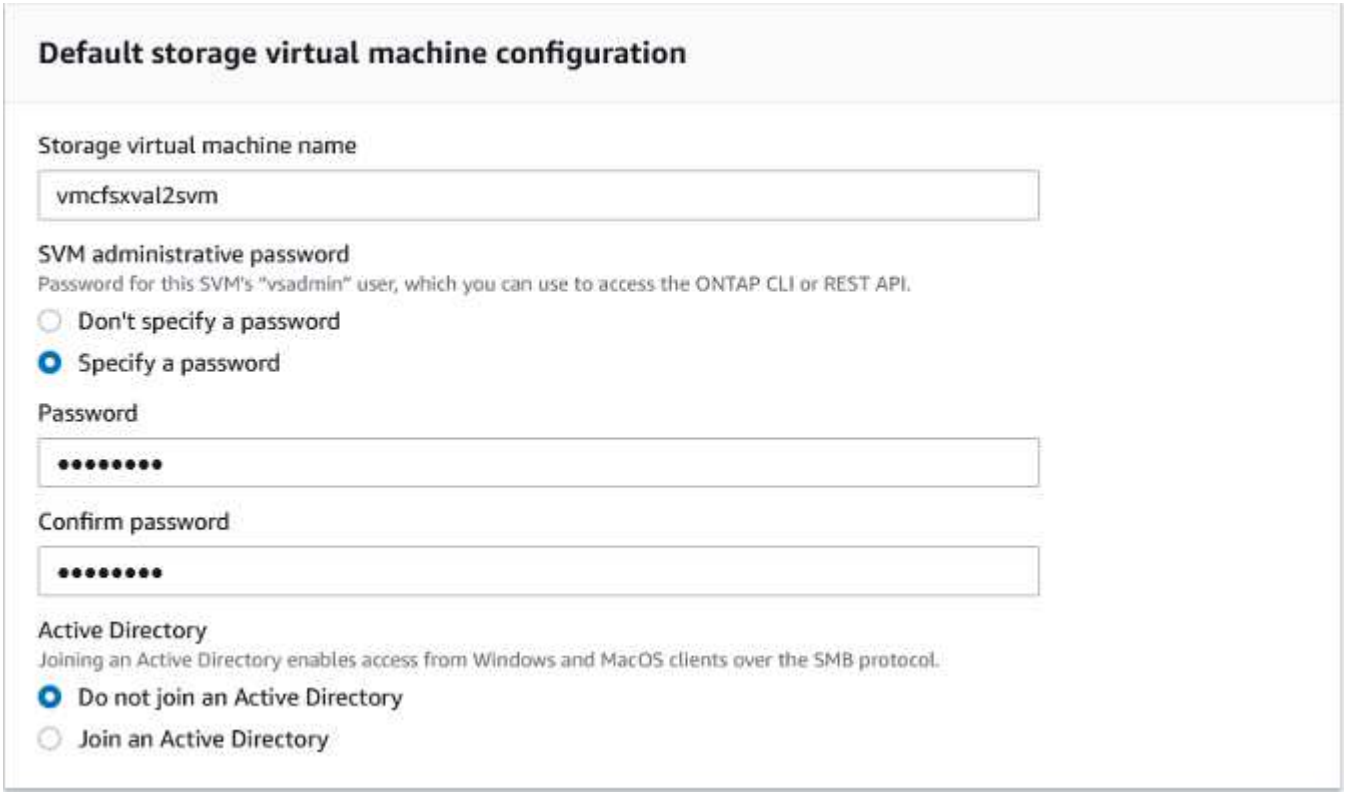


在网络部分中，对于虚拟私有云 (VPC)，选择适当的 VPC 和首选子网以及路由表。在这种情况下，从下拉菜单中选择了 vmcfsx2.vpc。

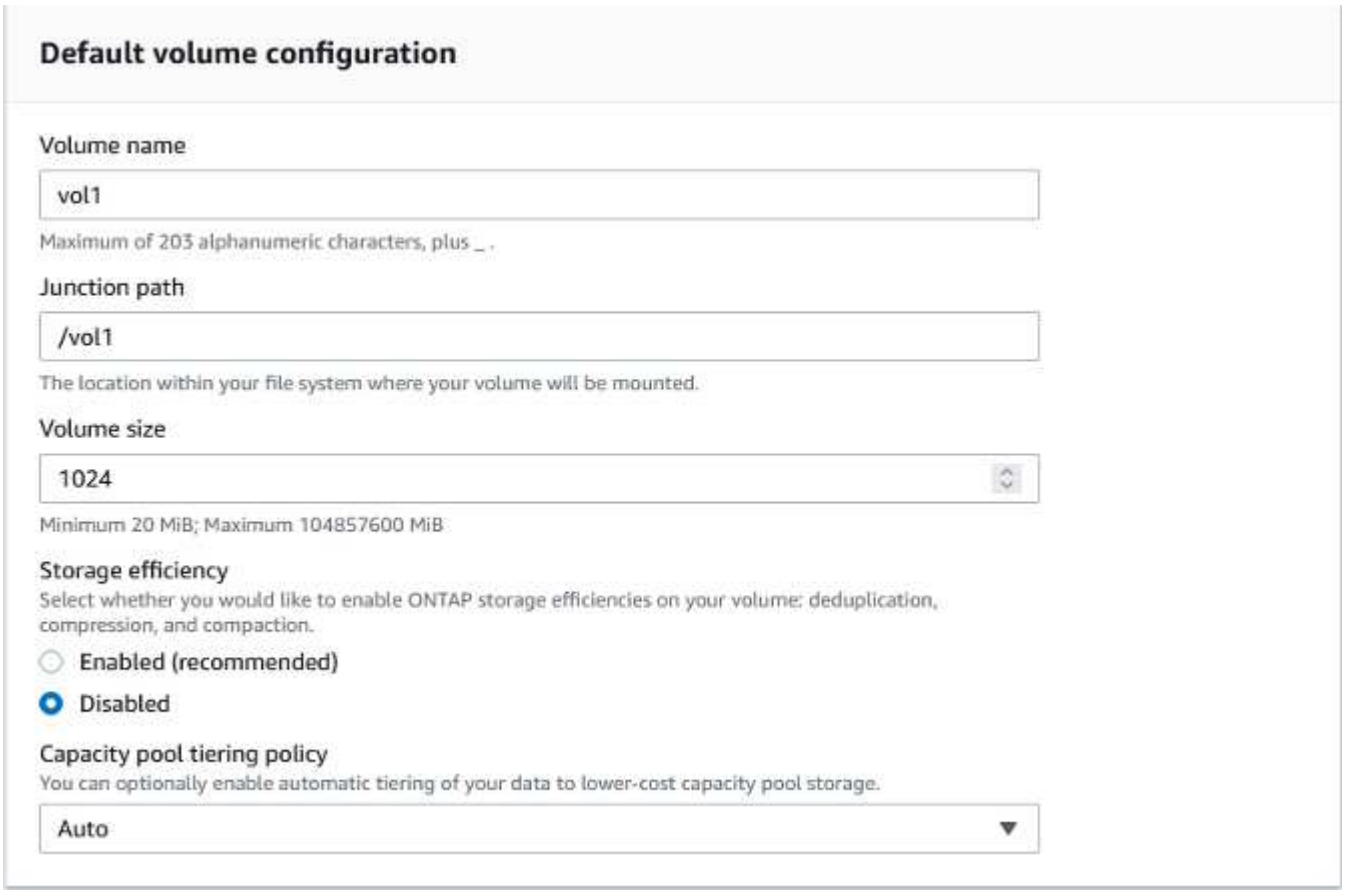
1. 在安全和加密部分中，对于加密密钥，选择保护文件系统静态数据的 AWS Key Management Service (AWS KMS) 加密密钥。对于文件系统管理密码，请输入 fsxadmin 用户的安全密码。



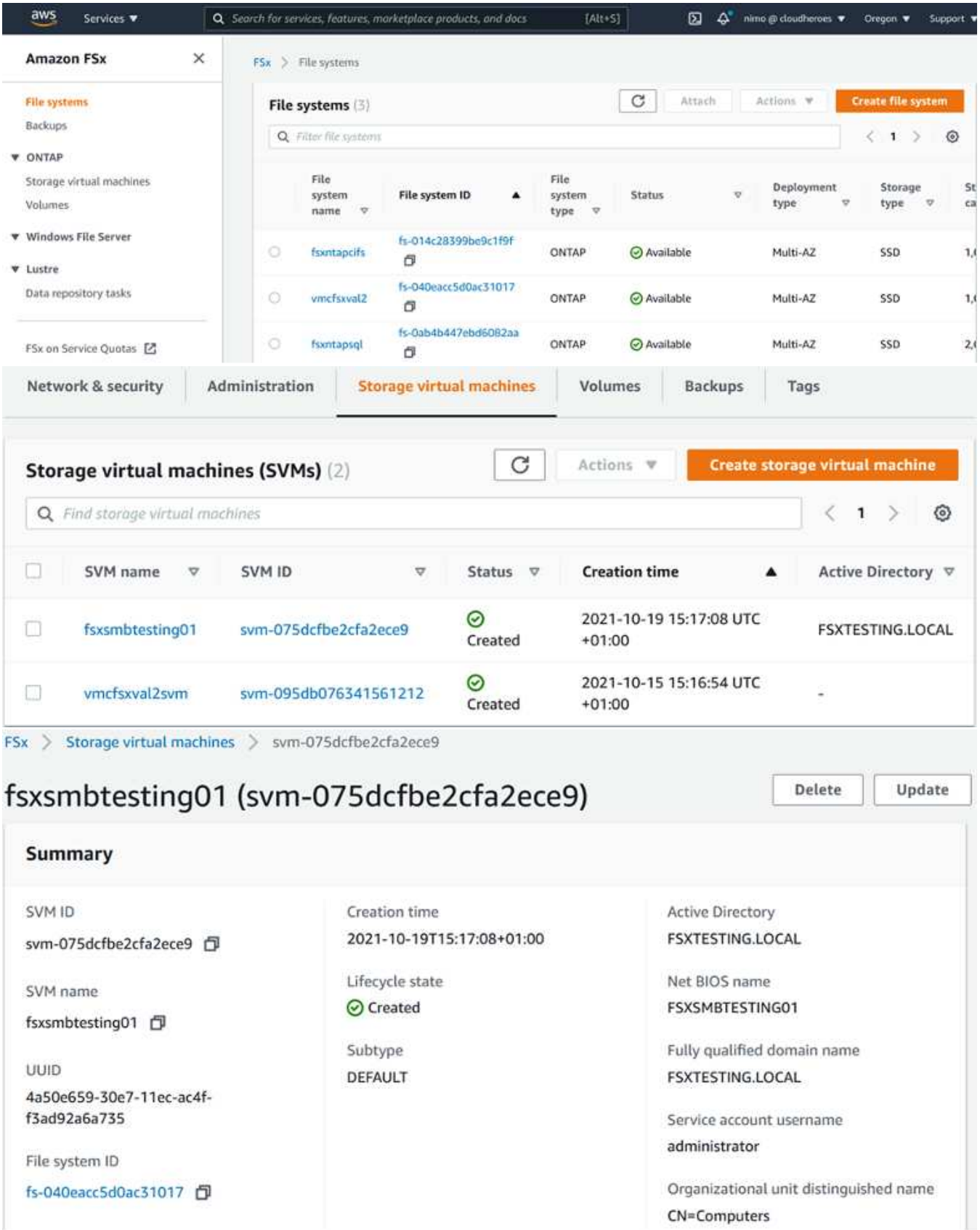
1. 在虚拟机中指定与 vsadmin 一起使用的密码，以便使用 REST API 或 CLI 管理ONTAP 。如果未指定密码，则可以使用 fsxadmin 用户来管理 SVM。在 Active Directory 部分中，确保将 Active Directory 加入到 SVM 以配置 SMB 共享。在默认存储虚拟机配置部分，为此验证中的存储提供一个名称，SMB 共享是使用自管理 Active Directory 域进行配置的。



1. 在默认卷配置部分中，指定卷名称和大小。这是一个 NFS 卷。对于存储效率，选择“启用”以打开ONTAP存储效率功能（压缩、重复数据删除和压缩）或选择“禁用”以关闭它们。



1. 查看“创建文件系统”页面上显示的文件系统配置。
2. 单击“创建文件系统”。



有关详细信息，请参阅"Amazon FSx ONTAP入门"。

按照上述方法创建文件系统后，创建具有所需大小和协议的卷。

1. 打开"Amazon FSx控制台"。
2. 在左侧导航窗格中，选择文件系统，然后选择要为其创建卷的ONTAP文件系统。
3. 选择卷选项卡。
4. 选择创建卷选项卡。
5. 出现“创建卷”对话框。

出于演示目的，本节创建了一个 NFS 卷，可以轻松将其安装在 AWS 上的 VMware 云上运行的虚拟机上。nfsdemovol01 的创建方式如下所示：



▼ 在 **Linux** 客户端上挂载 **FSx ONTAP**卷

要挂载上一步中创建的 FSx ONTAP卷。从 AWS SDDC 上的 VMC 中的 Linux VM，请完成以下步骤：

1. 连接到指定的Linux实例。
2. 使用安全外壳 (SSH) 在实例上打开终端并使用适当的凭据登录。
3. 使用以下命令为卷的挂载点创建一个目录：

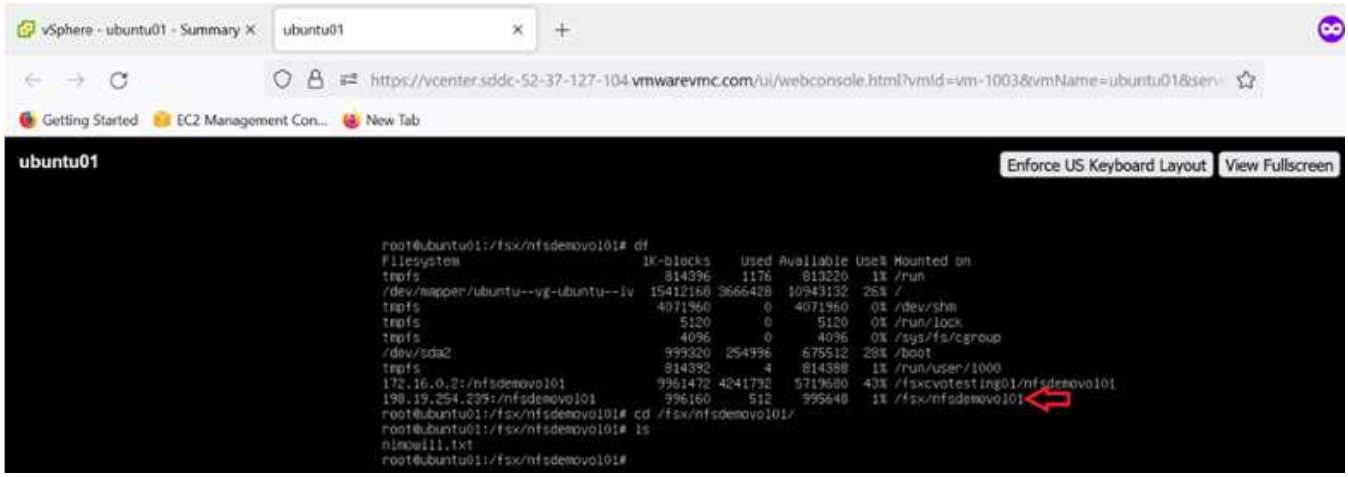
```
$ sudo mkdir /fsx/nfsdemovol01
```

. 将Amazon FSx ONTAP NFS 卷挂载到上一步创建的目录。

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. 执行后，运行 df 命令来验证挂载。



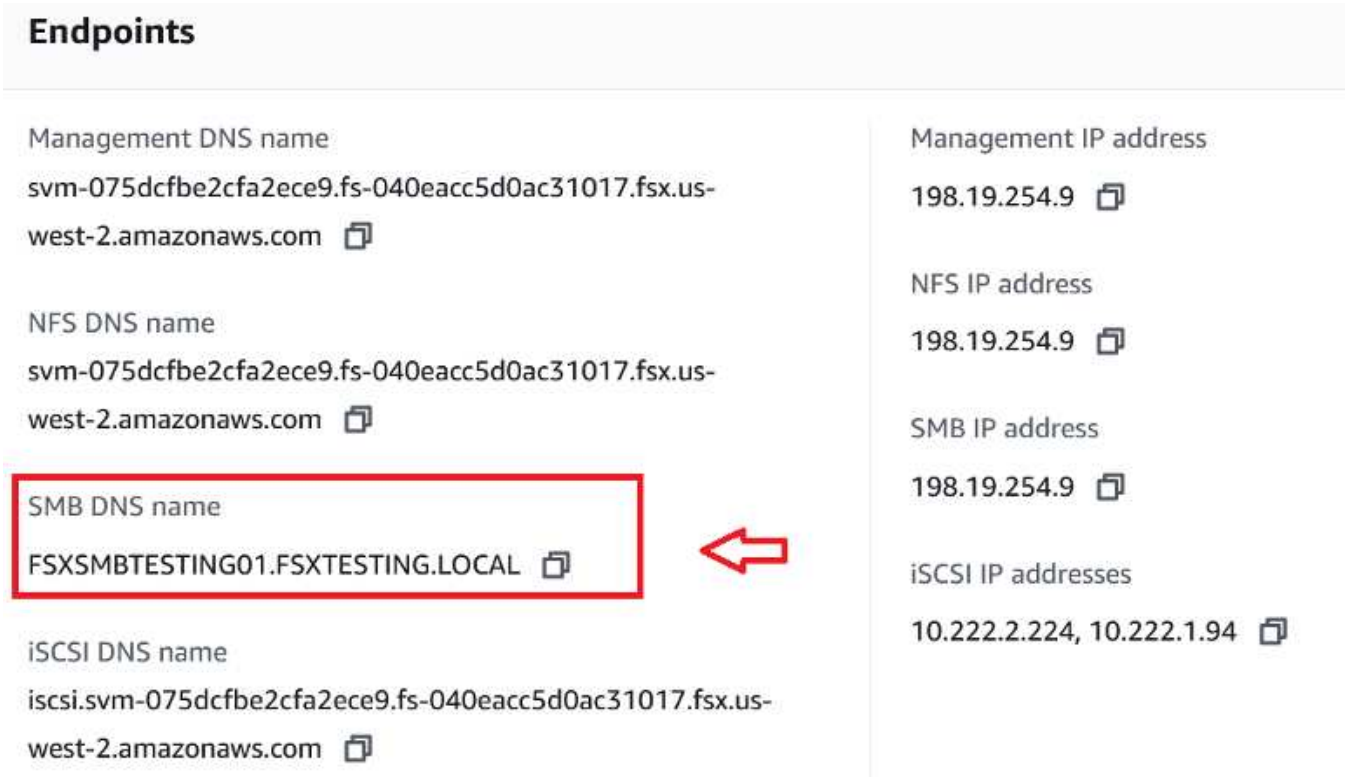
在 Linux 客户端上挂载 FSx ONTAP卷

▼ 将 **FSx ONTAP**卷附加到 **Microsoft Windows** 客户端

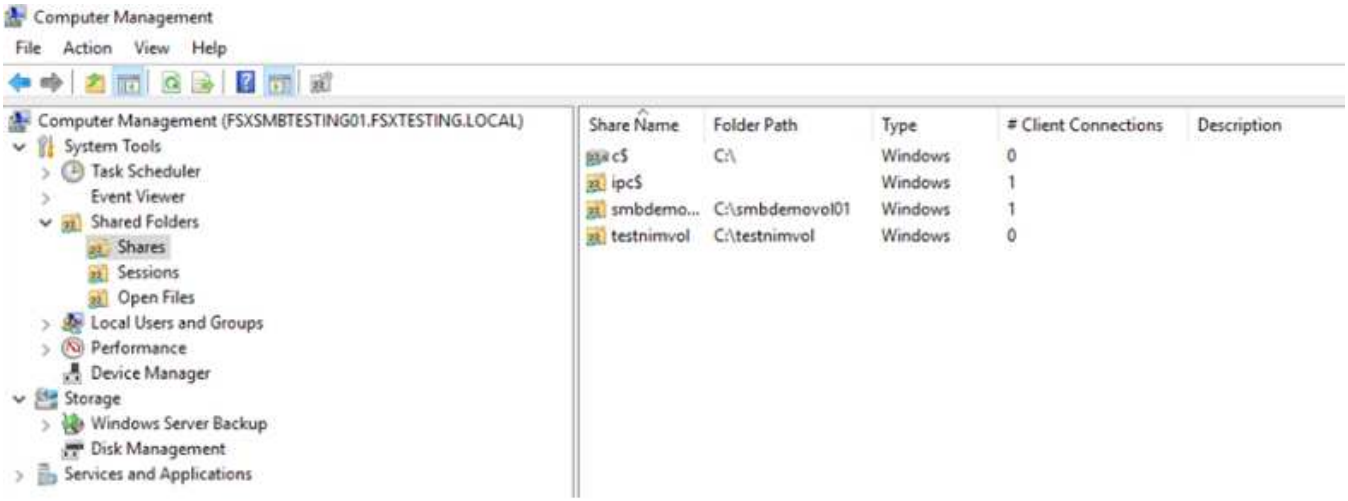
要管理和映射Amazon FSx文件系统上的文件共享，必须使用共享文件夹 GUI。

1. 打开开始菜单并使用以管理员身份运行 fsmgmt.msc。执行此操作将打开共享文件夹 GUI 工具。
2. 单击操作 > 所有任务并选择连接到另一台计算机。
3. 对于另一台计算机，输入存储虚拟机 (SVM) 的 DNS 名称。例如，本例中使用 FSXSMBTESTING01.FSXTESTING.LOCAL。

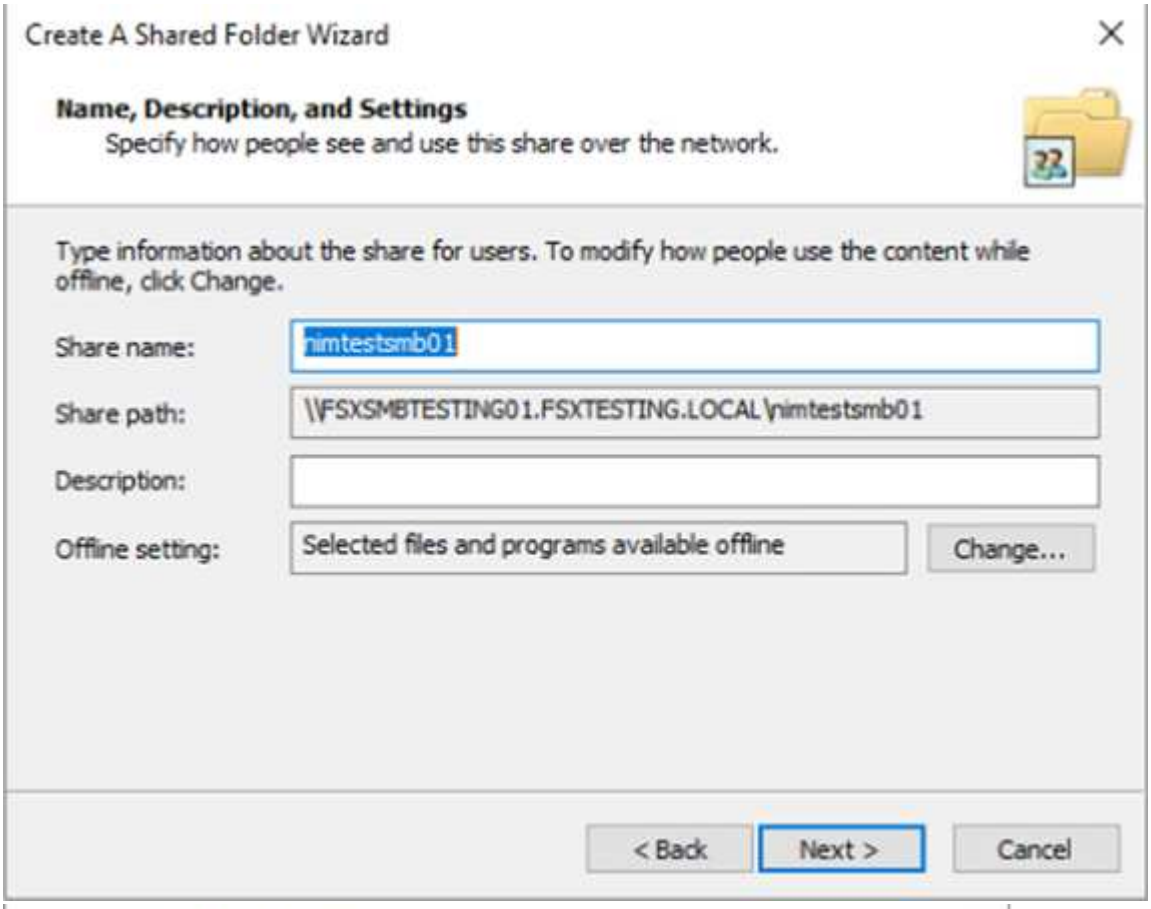
在Amazon FSx控制台上找到 SVM 的 DNS 名称，选择存储虚拟机，选择 SVM，然后向下滚动到终端节点以找到 SMB DNS 名称。单击“OK”。 Amazon FSx文件系统出现在共享文件夹列表中。



1. 在共享文件夹工具中，选择左侧窗格中的共享以查看Amazon FSx文件系统的活动共享。



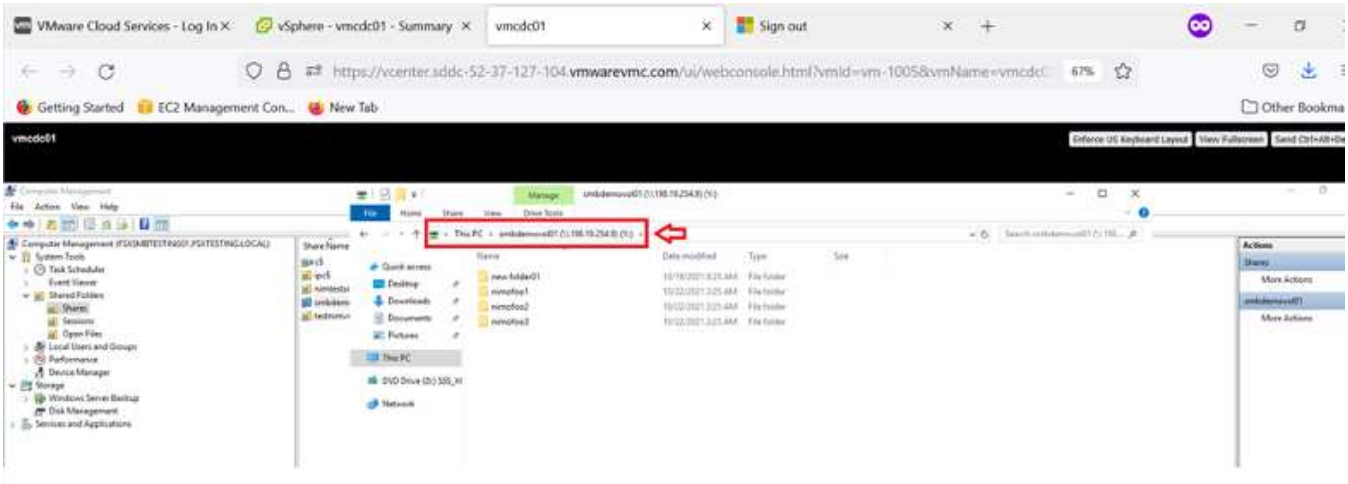
1. 现在选择一个新的共享并完成创建共享文件夹向导。





要了解有关在Amazon FSx文件系统上创建和管理 SMB 共享的更多信息，请参阅"创建 SMB 共享"。

1. 连接建立后，即可连接 SMB 共享并用于应用程序数据。为此，复制共享路径并使用映射网络驱动器选项将卷挂载到 AWS SDDC 上 VMware Cloud 上运行的虚拟机上。



▼ 使用 **iSCSI** 将 **FSx ONTAP LUN** 连接到主机

使用 iSCSI 将 FSx ONTAP LUN 连接到主机

FSx 的 iSCSI 流量通过上一节提供的路由遍历 VMware Transit Connect/AWS Transit Gateway。要在Amazon FSx ONTAP中配置 LUN，请按照以下文档操作"此处"。

在 Linux 客户端上，确保 iSCSI 守护程序正在运行。配置 LUN 后，请参阅有关使用 Ubuntu 配置 iSCSI 的详细指南（作为示例）"此处" 。

本文描述了如何将 iSCSI LUN 连接到 Windows 主机：

▼ 在 **FSx ONTAP**中配置 **LUN**：

1. 使用 FSx for ONTAP文件系统的管理端口访问NetApp ONTAP CLI。
2. 按照大小调整输出的指示创建具有所需大小的 LUN。

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

在此示例中，我们创建了一个大小为 5g（5368709120）的 LUN。

1. 创建必要的 igroup 来控制哪些主机可以访问特定的 LUN。

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators

--------- ------------ -------- --------
------------------------------------
```

```
vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

显示了两个条目。

1. 使用以下命令将 LUN 映射到 igroup：

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------- ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

显示了两个条目。

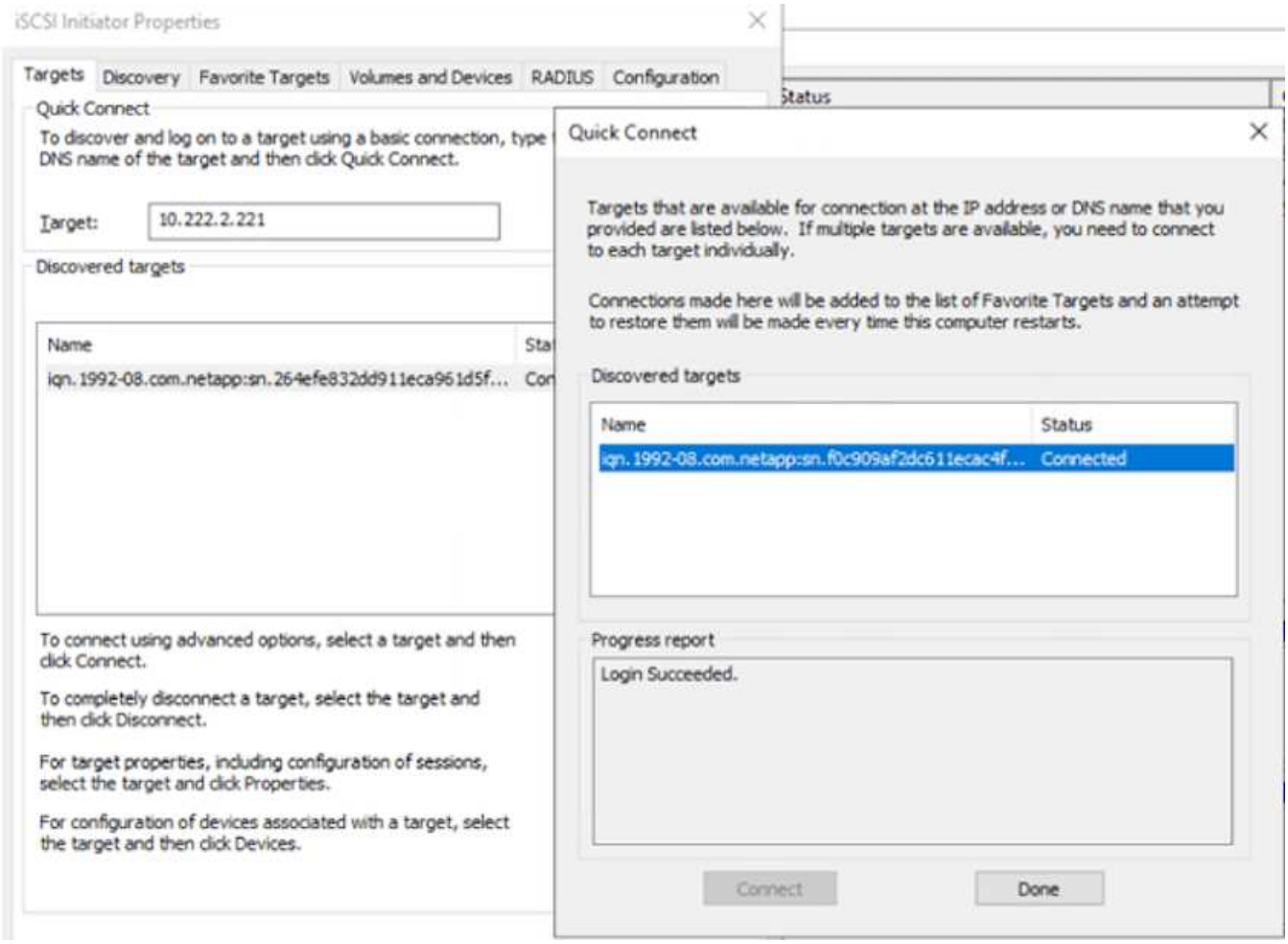
1. 将新配置的 LUN 连接到 Windows VM：

要将新的 LUN 连接到位于 VMware cloud on AWS SDDC 上的 Windows 主机，请完成以下步骤：

1. 通过 RDP 连接到 VMware Cloud on AWS SDDC 上托管的 Windows VM。
2. 导航到服务器管理器 > 仪表板 > 工具 > iSCSI 启动器以打开 iSCSI 启动器属性对话框。
3. 在“发现”选项卡中，单击“发现门户”或“添加门户”，然后输入 iSCSI 目标端口的 IP 地址。

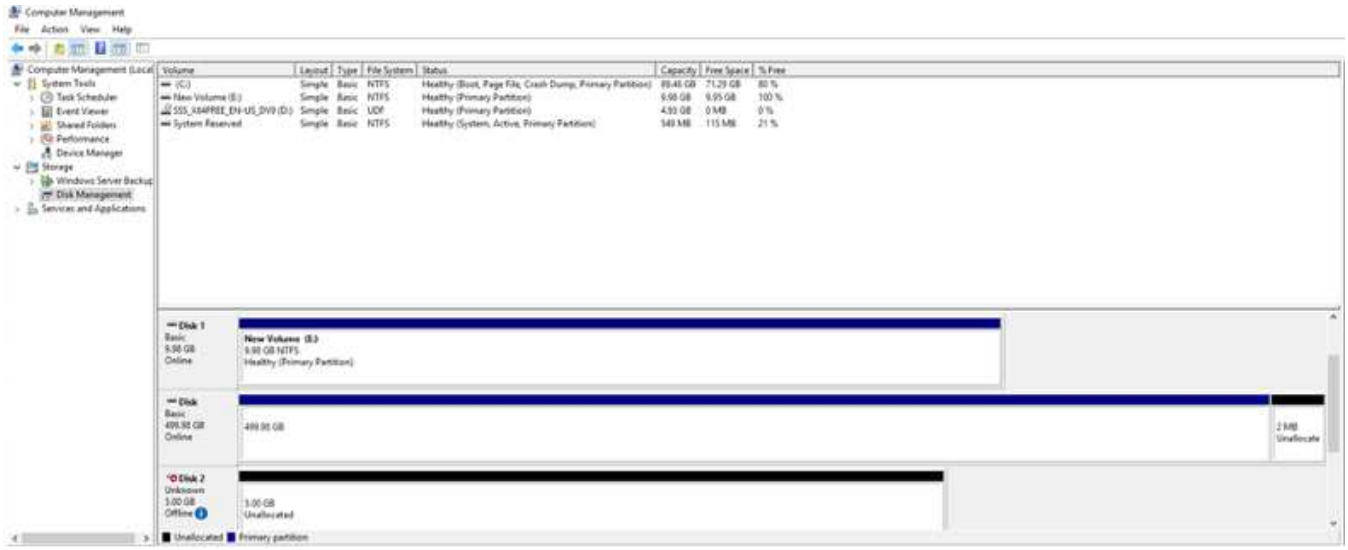
4. 从“目标”选项卡中，选择发现的目标，然后单击“登录”或“连接”。
5. 选择启用多路径，然后选择“计算机启动时自动恢复此连接”或“将此连接添加到收藏目标列表”。单击“高级”。

Windows 主机必须与群集中的每个节点建立 iSCSI 连接。本机 DSM 选择最佳路径以供使用。



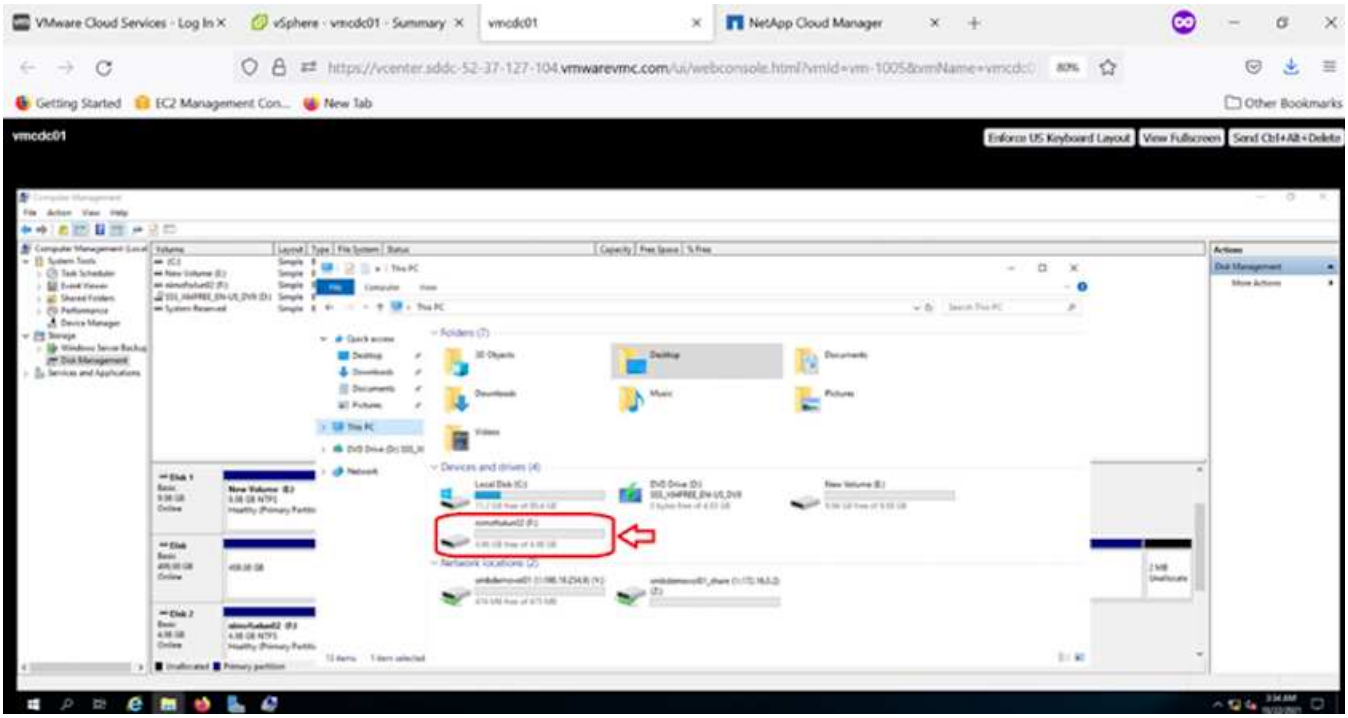
存储虚拟机 (SVM) 上的 LUN 对于 Windows 主机来说显示为磁盘。主机不会自动发现任何新添加的磁盘。通过完成以下步骤触发手动重新扫描以发现磁盘：

1. 打开 Windows 计算机管理实用程序：开始 > 管理工具 > 计算机管理。
2. 在导航树中展开存储节点。
3. 单击“磁盘管理”。
4. 单击操作 > 重新扫描磁盘。



当 Windows 主机首次访问新的 LUN 时，它没有分区或文件系统。通过完成以下步骤初始化 LUN，并（可选）使用文件系统格式化 LUN：

1. 启动 Windows 磁盘管理。
2. 右键单击 LUN，然后选择所需的磁盘或分区类型。
3. 按照向导中的说明进行操作。在此示例中，已安装驱动器 F:。



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP（或称 CVO）是基于 NetApp 的ONTAP存储软件构建的业界领先的云数据管理解决方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的软件定义版本，使用云原生存储，允许您在云端和本地使用相同的存储软件，从而无需重新培训 IT 人员采用全新方法来管理数据。

CVO 使客户能够无缝地将数据从边缘移动到数据中心、云端并返回，从而将您的混合云整合在一起 - 所有这些都通过单一窗格管理控制台NetApp Cloud Manager 进行管理。

CVO 的设计旨在提供极致的性能和先进的数据管理功能，以满足您在云端最苛刻的应用程序

Cloud Volumes ONTAP (CVO) 作为来宾连接存储

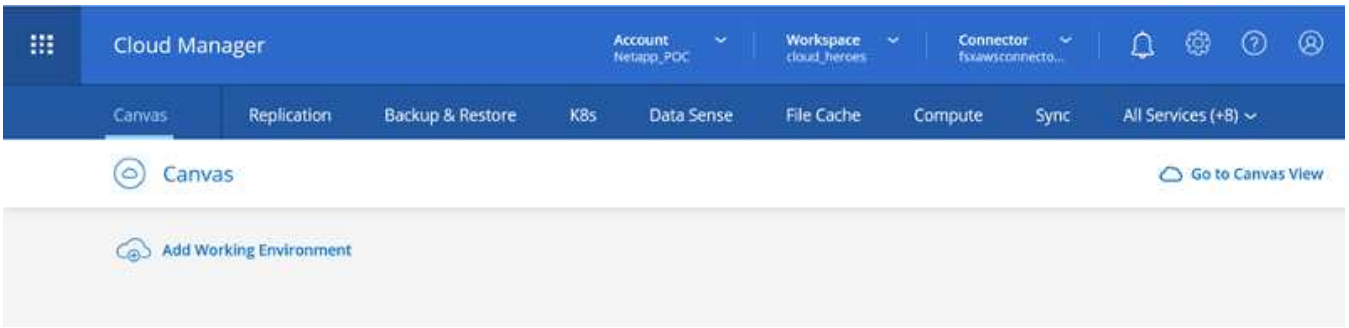
▼ 在 AWS 中部署新的Cloud Volumes ONTAP实例（自行部署）

可以从在 VMware Cloud on AWS SDDC 环境中创建的虚拟机挂载Cloud Volumes ONTAP共享和 LUN。这些卷还可以安装在本机 AWS VM Linux Windows 客户端上，并且当通过 iSCSI 安装时，可以在 Linux 或 Windows 客户端上将 LUNS 作为块设备访问，因为Cloud Volumes ONTAP支持 iSCSI、SMB 和 NFS 协议。只需几个简单的步骤即可设置Cloud Volumes ONTAP卷。

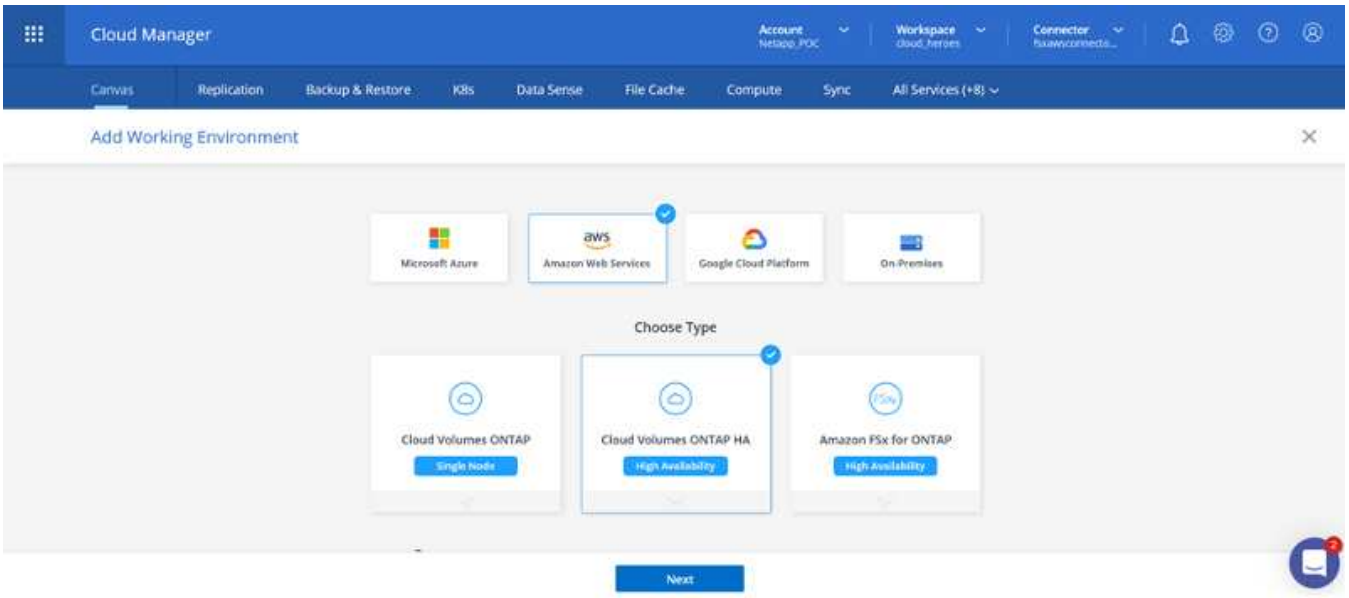
要将卷从本地环境复制到云以实现灾难恢复或迁移，请使用站点到站点 VPN 或 DirectConnect 建立与 AWS 的网络连接。将数据从本地复制到Cloud Volumes ONTAP超出了本文档的范围。要在本地和Cloud Volumes ONTAP系统之间复制数据，请参阅"设置系统之间的数据复制"。

使用"Cloud Volumes ONTAP大小调整器"可准确调整 Cloud Volumes ONTAP 实例的大小。此外，监控本地性能以用作 Cloud Volumes ONTAP sizer 中的输入。

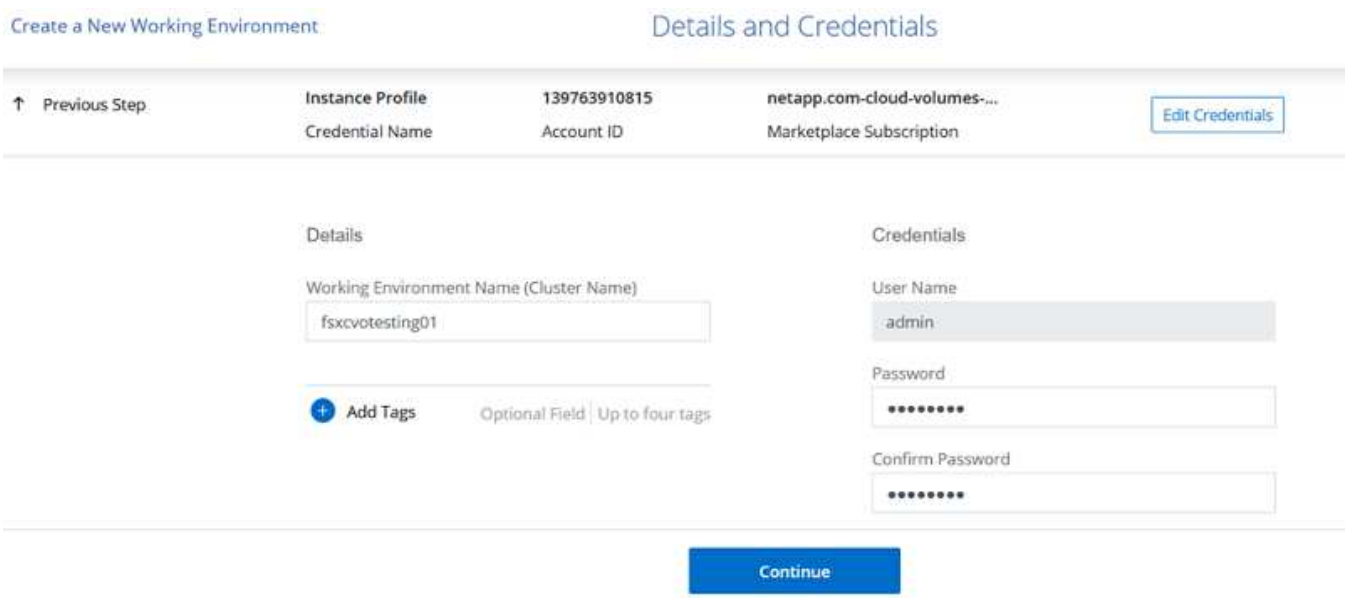
1. 登录NetApp Cloud Central；显示 Fabric View 屏幕。找到Cloud Volumes ONTAP选项卡并选择转到云管理器。登录后，将显示 Canvas 屏幕。



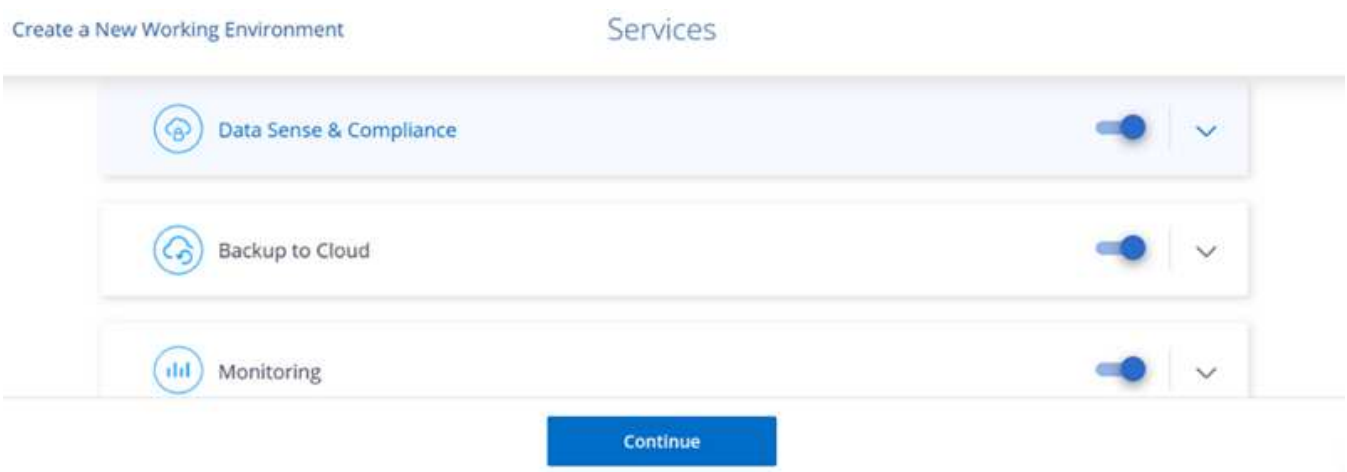
1. 在云管理器主页上，单击添加工作环境，然后选择 AWS 作为云和系统配置类型。



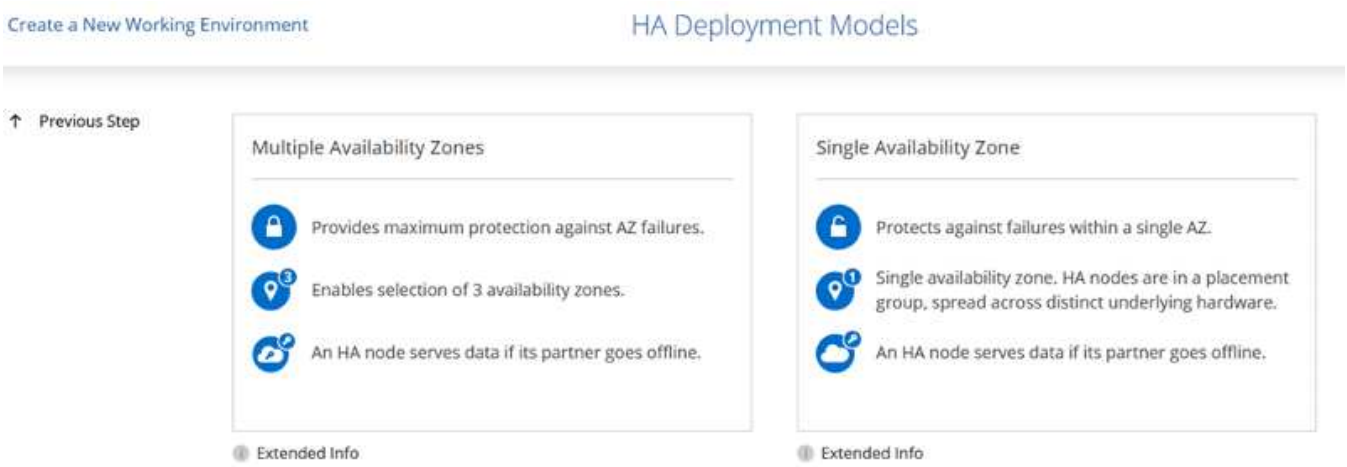
1. 提供要创建的环境的详细信息，包括环境名称和管理员凭据。单击“Continue”。



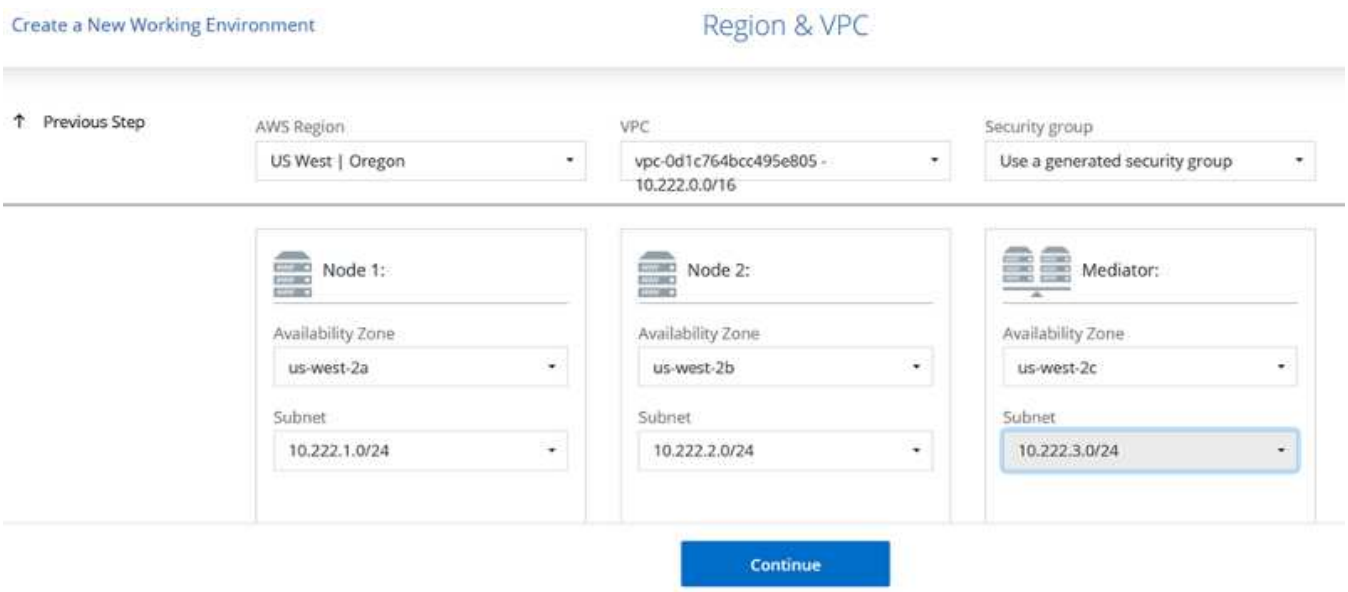
1. 选择 Cloud Volumes ONTAP 部署的附加服务，包括 NetApp Data Classification、NetApp Backup and Recovery 以及 Data Infrastructure Insights。单击继续。



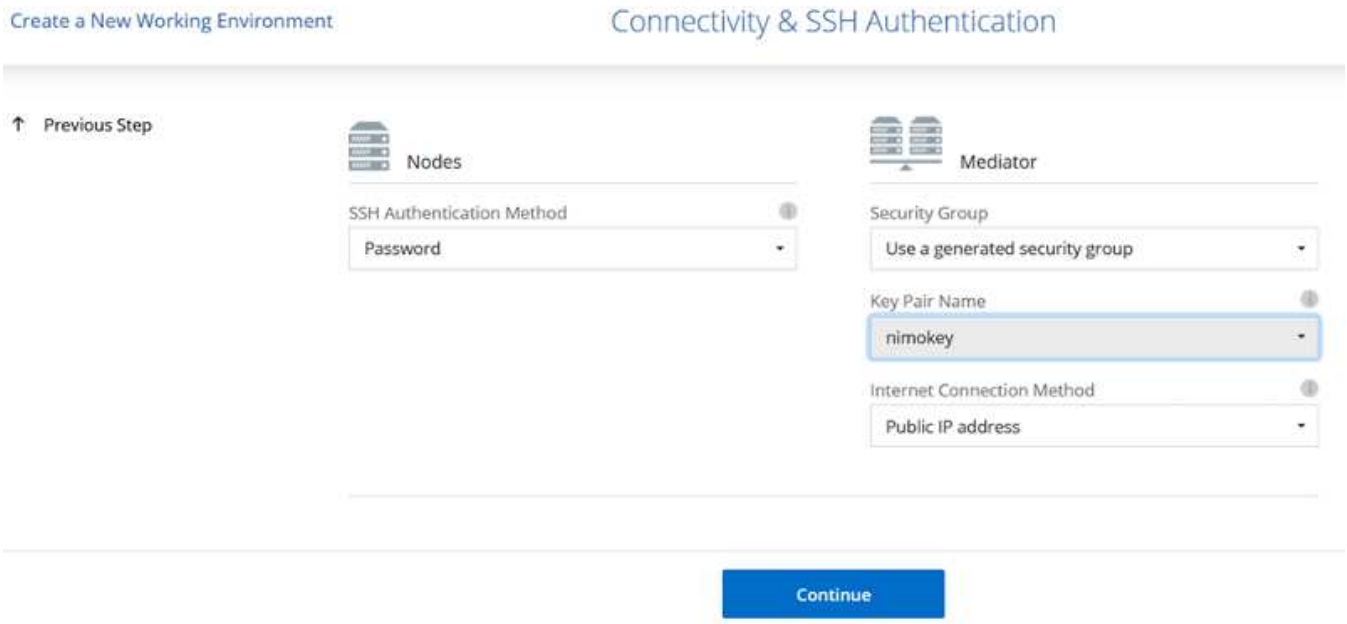
1. 在 HA 部署模型页面上，选择多可用区配置。



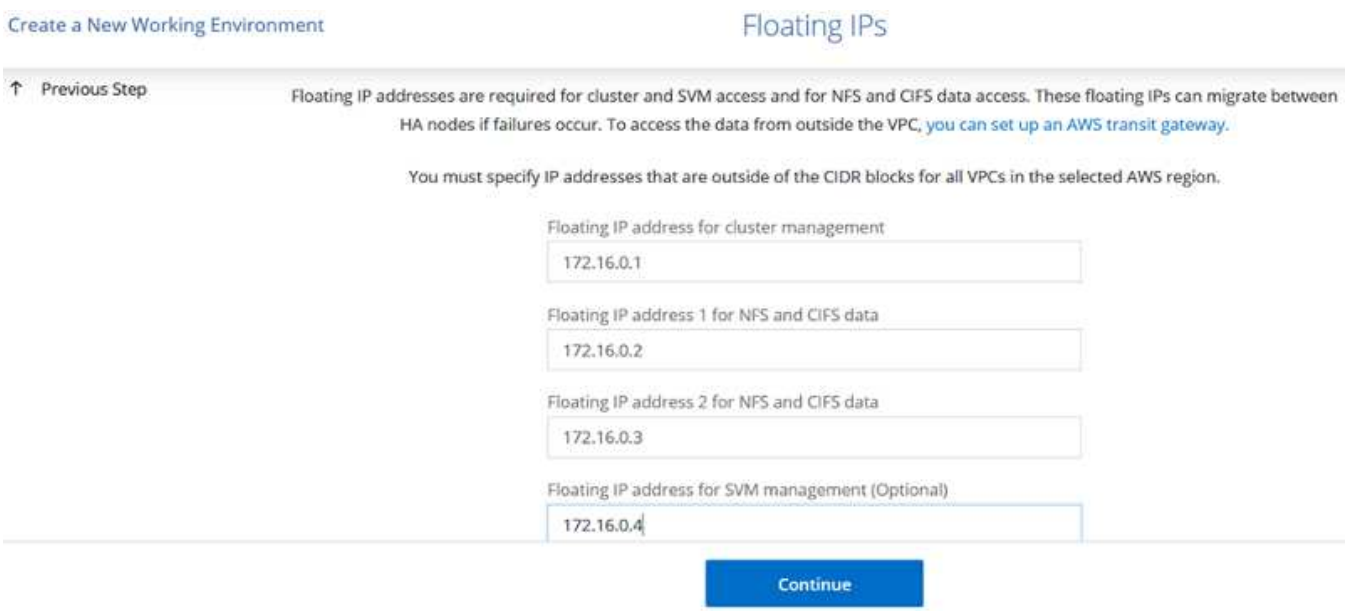
1. 在“区域和 VPC”页面，输入网络信息，然后单击“继续”。



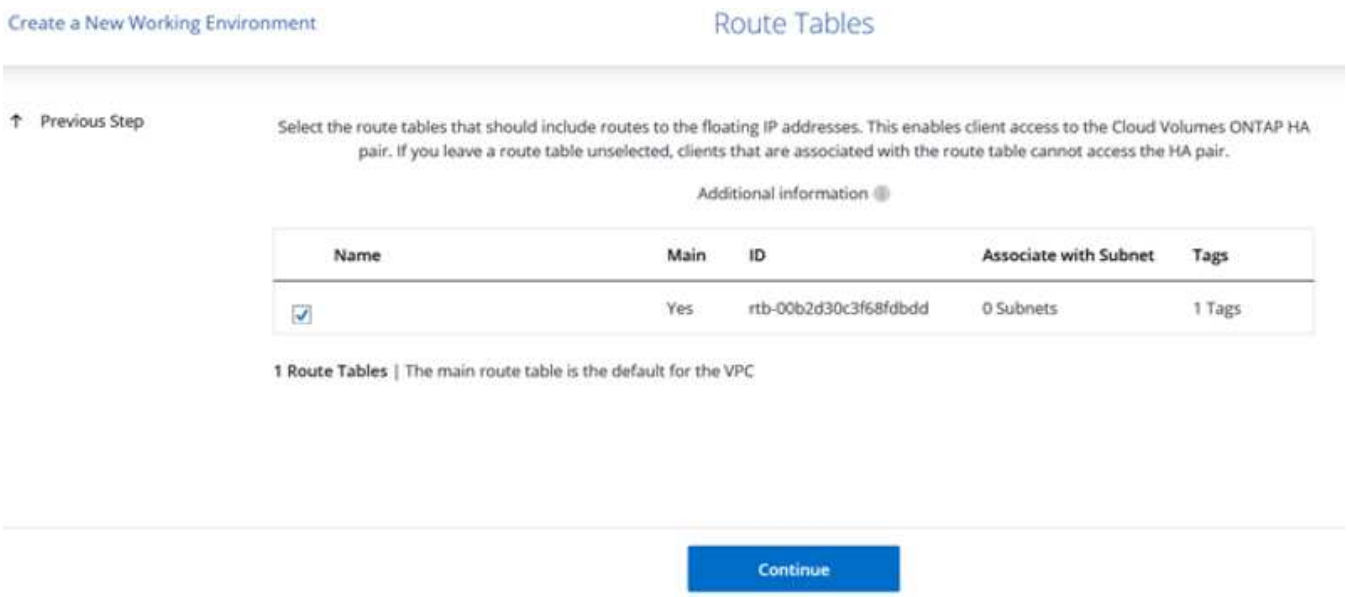
1. 在“连接和 SSH 身份验证”页面上，选择 HA 对和中介的连接方法。



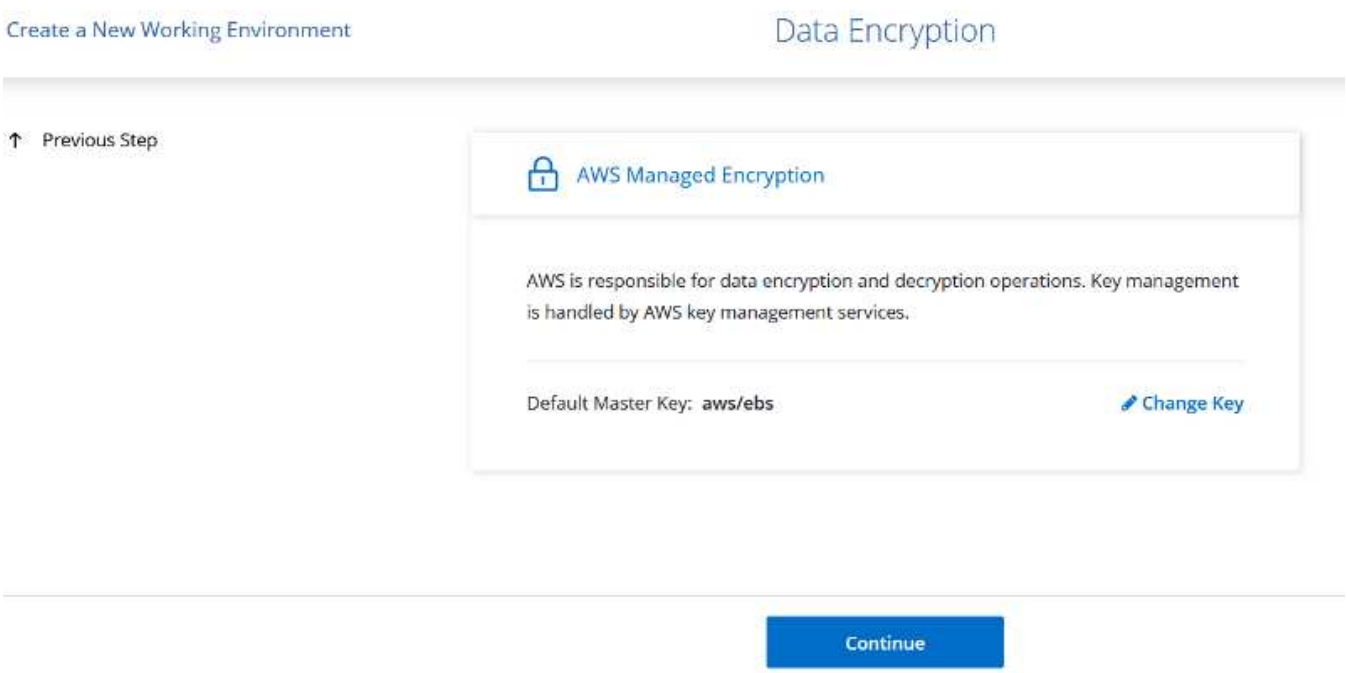
1. 指定浮动 IP 地址，然后单击继续。



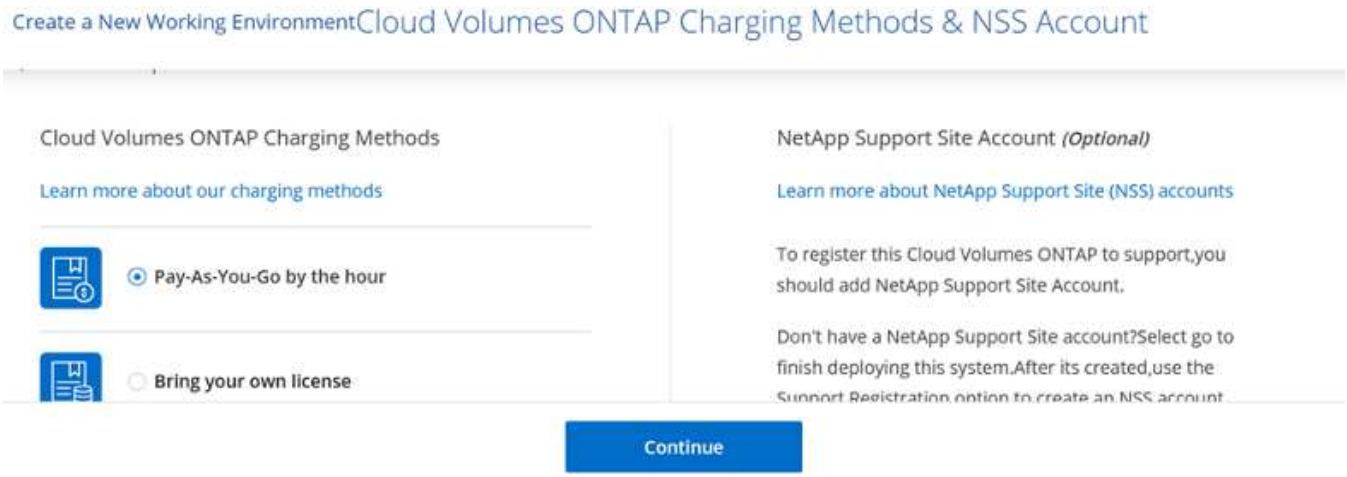
1. 选择适当的路由表以包含到浮动 IP 地址的路由，然后单击继续。



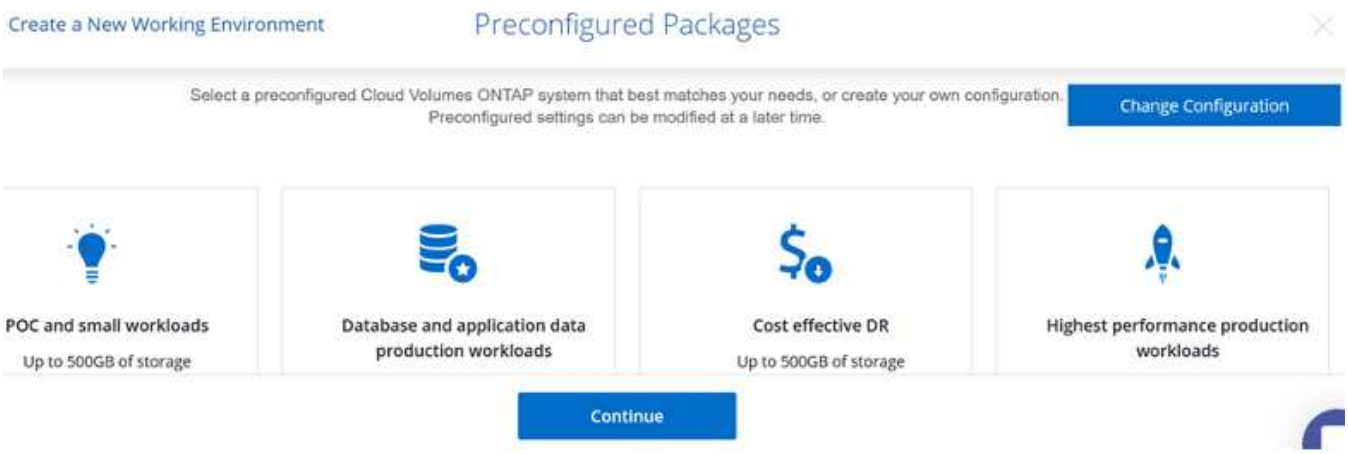
1. 在数据加密页面上，选择 AWS 托管加密。



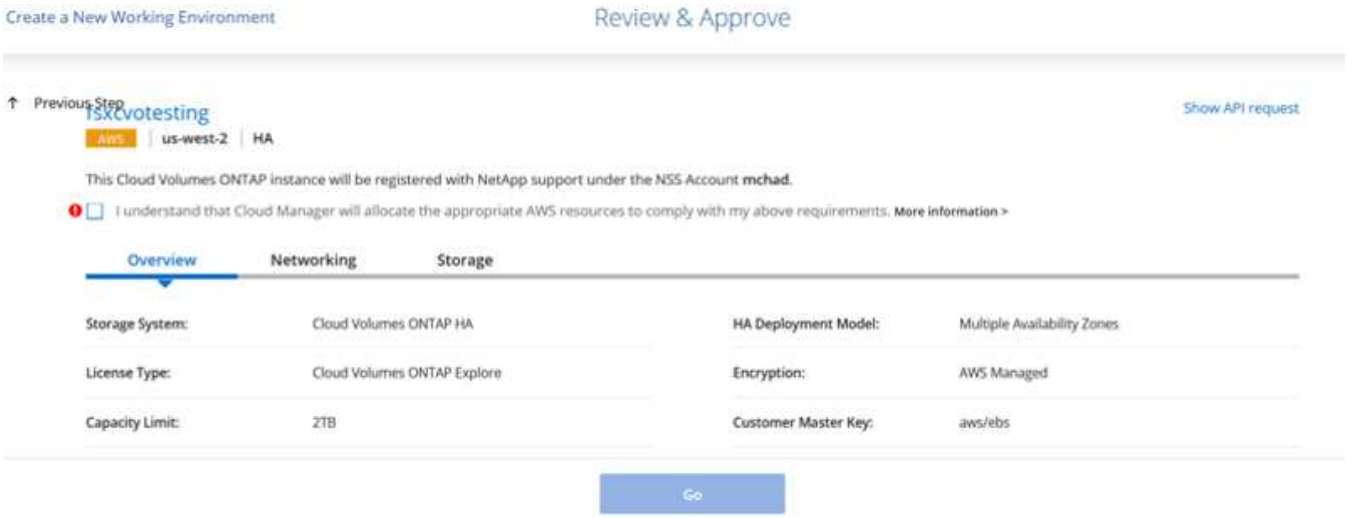
1. 选择许可证选项：按使用量付费或使用现有许可证的 BYOL。在此示例中，使用了按使用量付费选项。



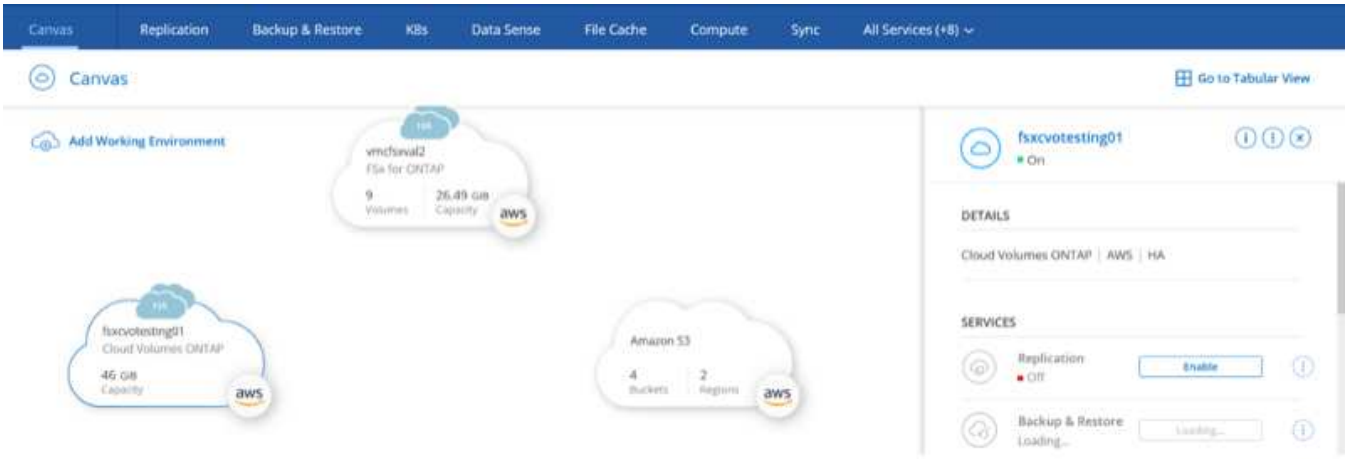
1. 根据要在 AWS SDDC 上的 VMware 云上运行的虚拟机上部署的工作负载类型，在几个可用的预配置包中进行选择。



1. 在“审核并批准”页面上，审核并确认选择。要创建Cloud Volumes ONTAP实例，请单击“开始”。

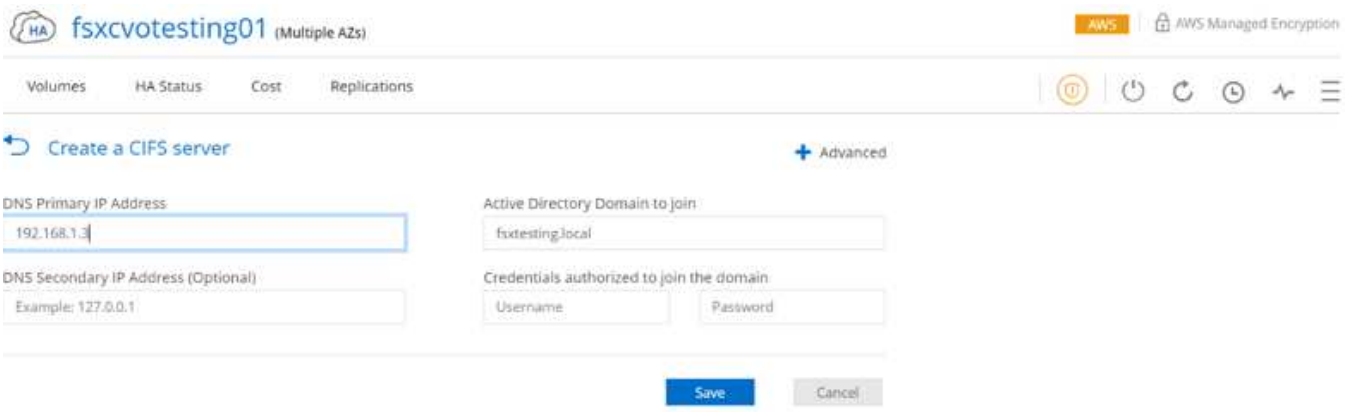


1. 配置Cloud Volumes ONTAP后，它会列在 Canvas 页面上的工作环境中。

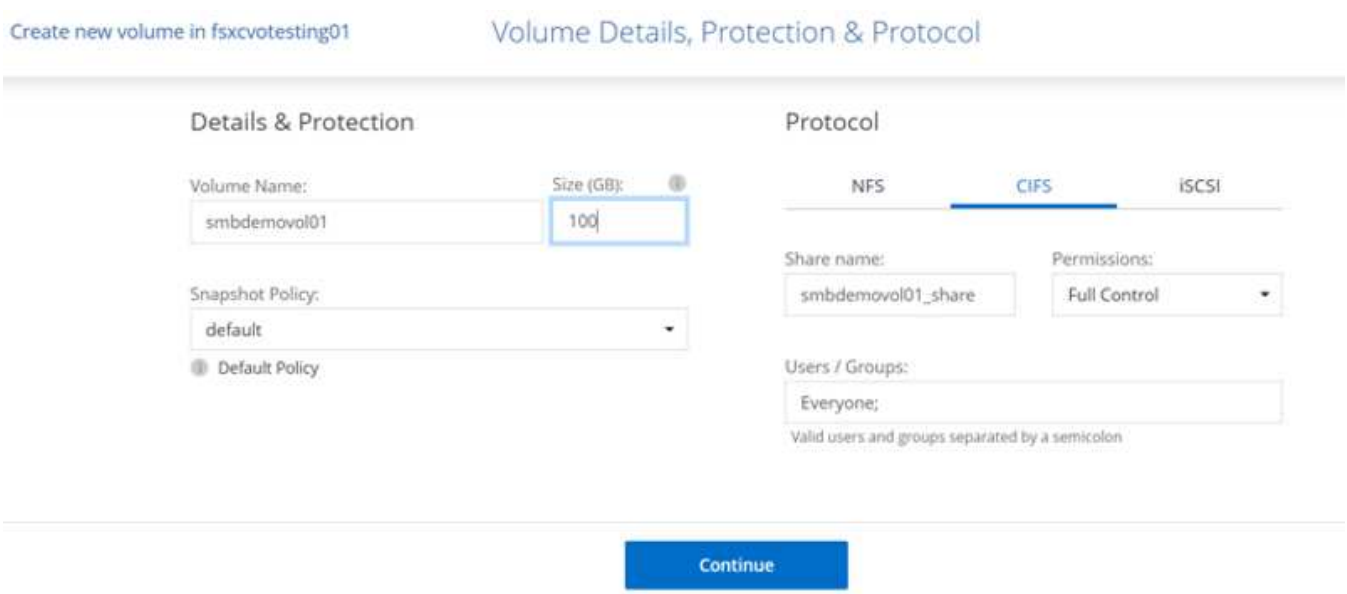


▼ **SMB** 卷的附加配置

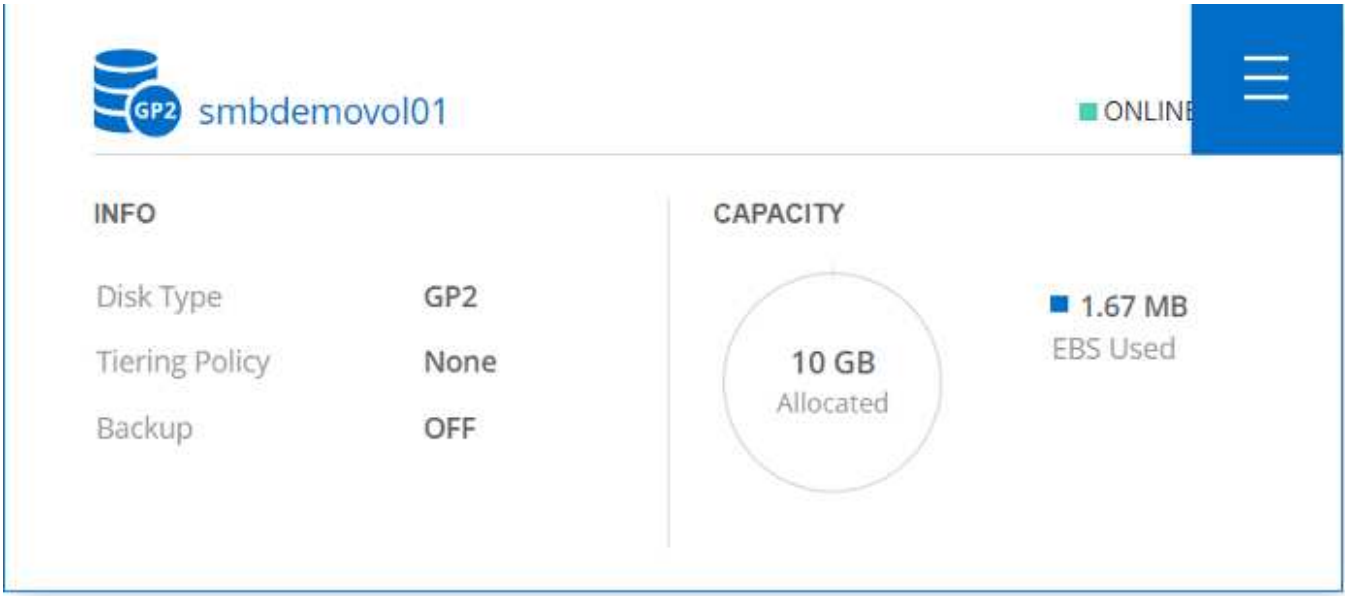
1. 工作环境准备好后，请确保 CIFS 服务器配置了适当的 DNS 和 Active Directory 配置参数。在创建 SMB 卷之前，需要执行此步骤。



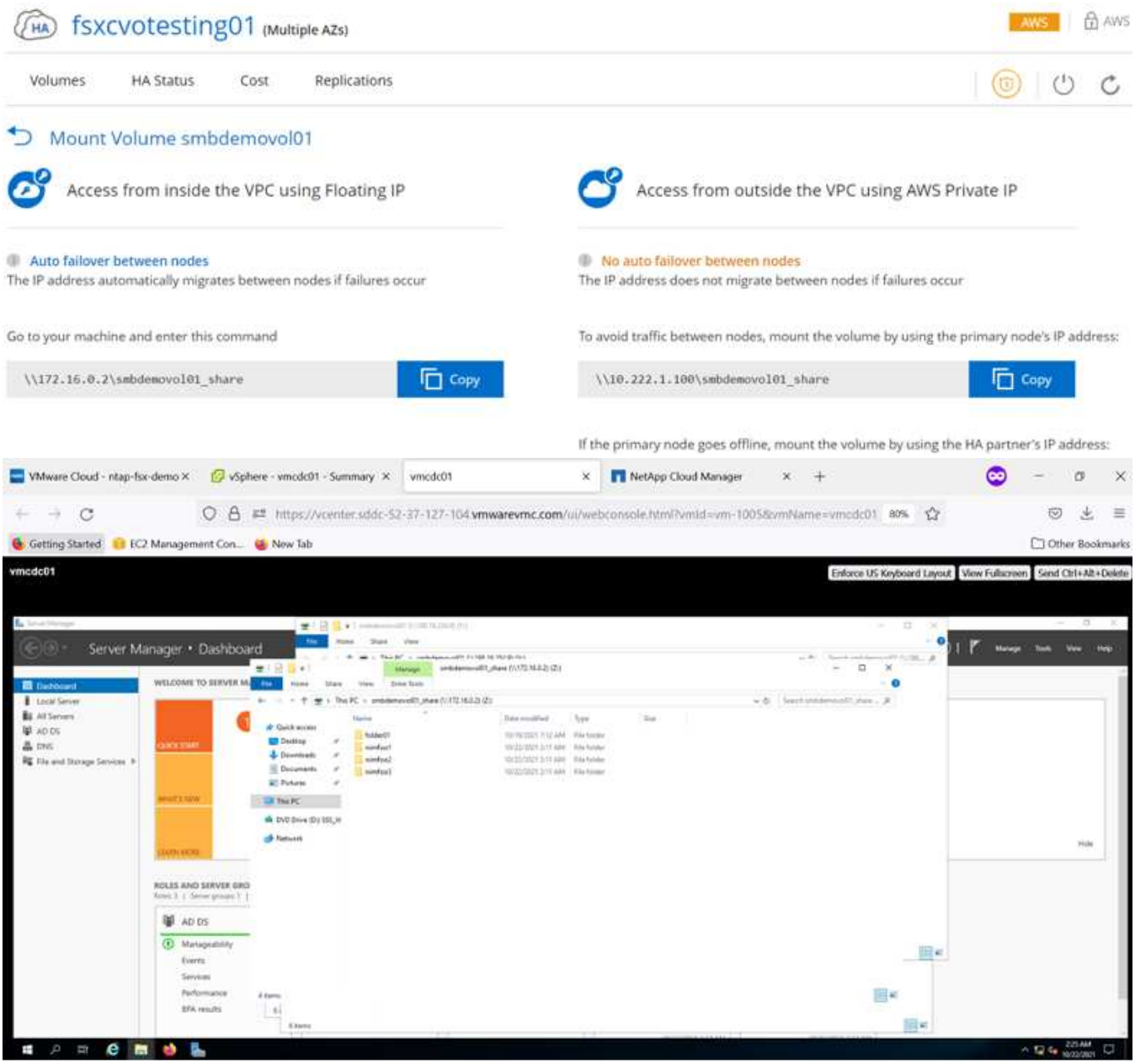
1. 选择要创建卷的 CVO 实例，然后单击“创建卷”选项。选择适当的大小，云管理器选择包含的聚合或使用高级分配机制放置在特定的聚合上。对于此演示，选择 SMB 作为协议。



1. 卷配置完成后，可在“卷”窗格下使用。由于已配置 CIFS 共享，因此您应该授予用户或组对文件和文件夹的权限，并验证这些用户是否可以访问共享并创建文件。



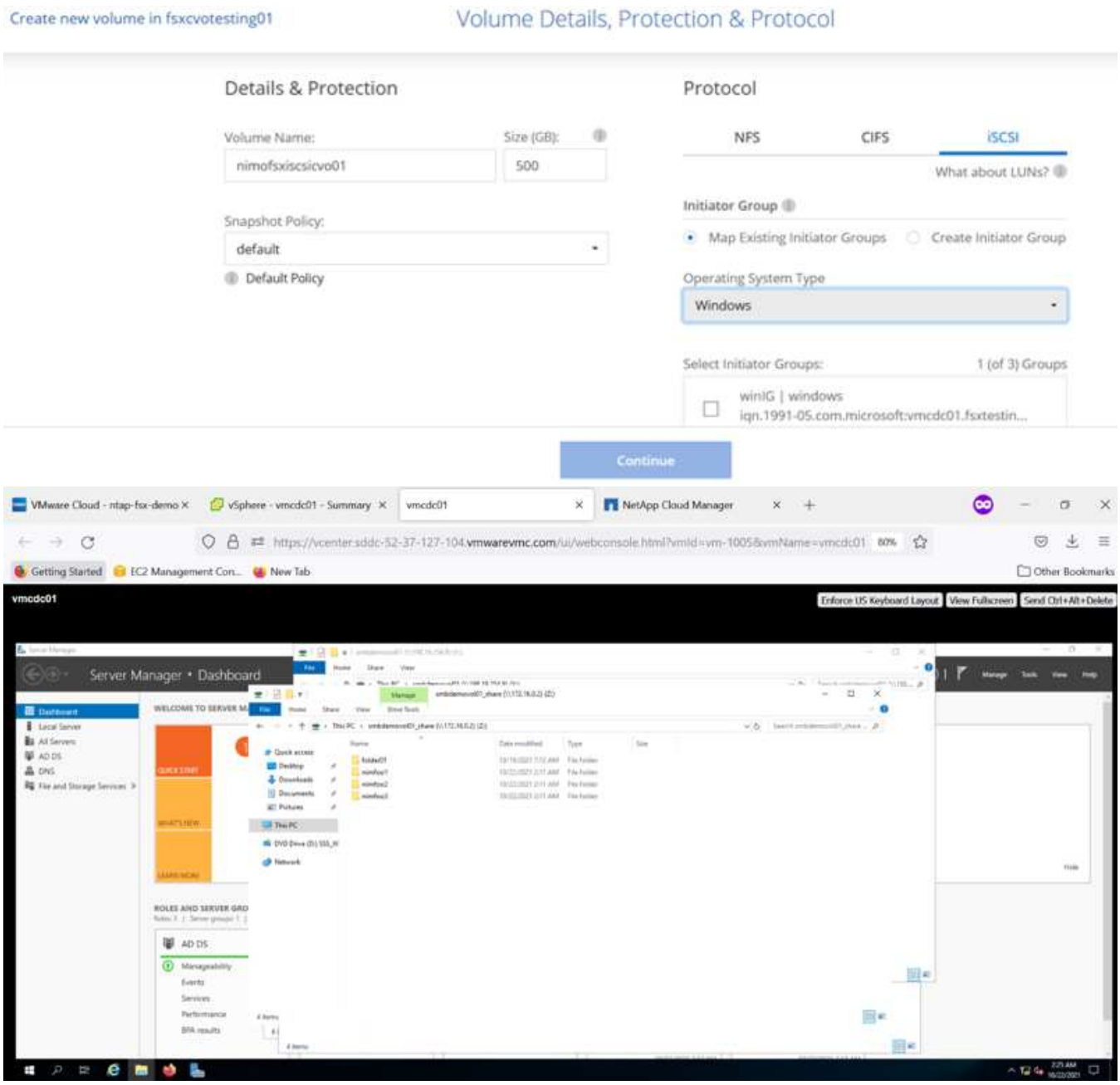
1. 创建卷后，使用 mount 命令从 AWS SDDC 主机中 VMware Cloud 上运行的虚拟机连接到共享。
2. 复制以下路径并使用映射网络驱动器选项将卷挂载到 AWS SDDC 中 VMware Cloud 上运行的虚拟机上。



▼ 将 **LUN** 连接到主机

要将Cloud Volumes ONTAP LUN 连接到主机，请完成以下步骤：

1. 在 Cloud Manager Canvas 页面上，双击Cloud Volumes ONTAP工作环境以创建和管理卷。
2. 单击添加卷 > 新卷，选择 iSCSI，然后单击创建启动器组。单击“Continue”。



1. 配置卷后，选择该卷，然后单击目标 IQN。要复制 iSCSI 限定名称 (IQN)，请单击复制。建立从主机到 LUN 的 iSCSI 连接。

要对位于 VMware Cloud on AWS SDDC 上的主机完成相同操作，请完成以下步骤：

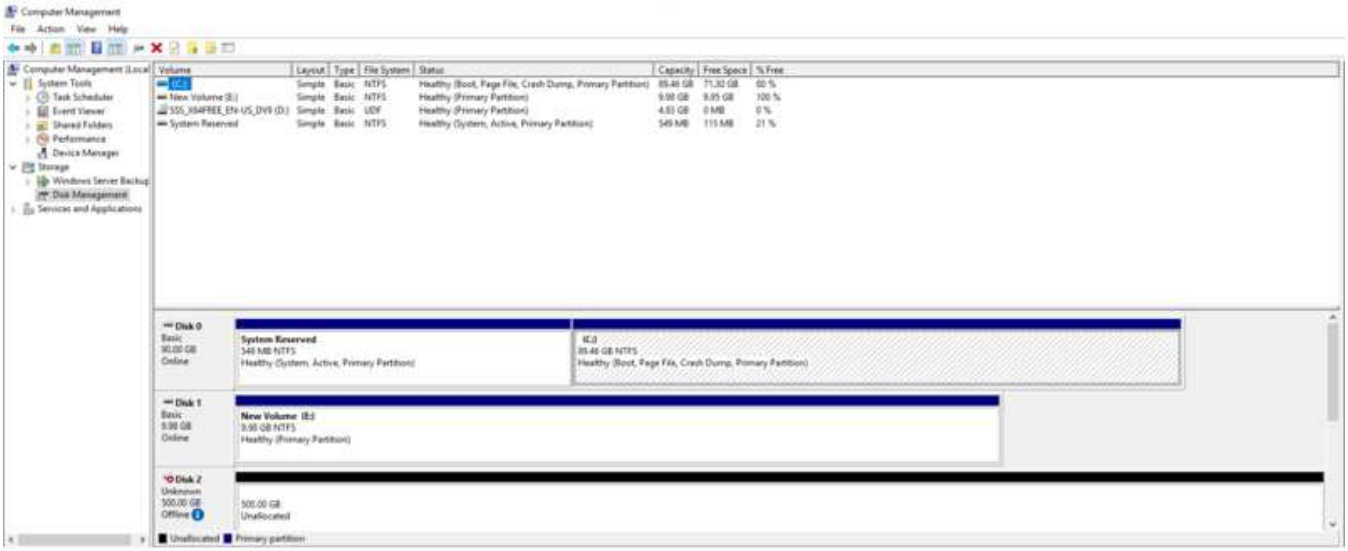
1. 通过 RDP 连接到 AWS 上的 VMware 云上托管的 VM。
2. 打开 iSCSI 发起程序属性对话框：服务器管理器 > 仪表板 > 工具 > iSCSI 发起程序。
3. 在“发现”选项卡中，单击“发现门户”或“添加门户”，然后输入 iSCSI 目标端口的 IP 地址。
4. 从“目标”选项卡中，选择发现的目标，然后单击“登录”或“连接”。
5. 选择启用多路径，然后选择计算机启动时自动恢复此连接或将此连接添加到收藏目标列表。单击“高级”。

Windows 主机必须与群集中的每个节点建立 iSCSI 连接。本机 DSM 选择最佳路径以供使用。



SVM 中的 LUN 对 Windows 主机来说显示为磁盘。主机不会自动发现任何新添加的磁盘。通过完成以下步骤触发手动重新扫描以发现磁盘：

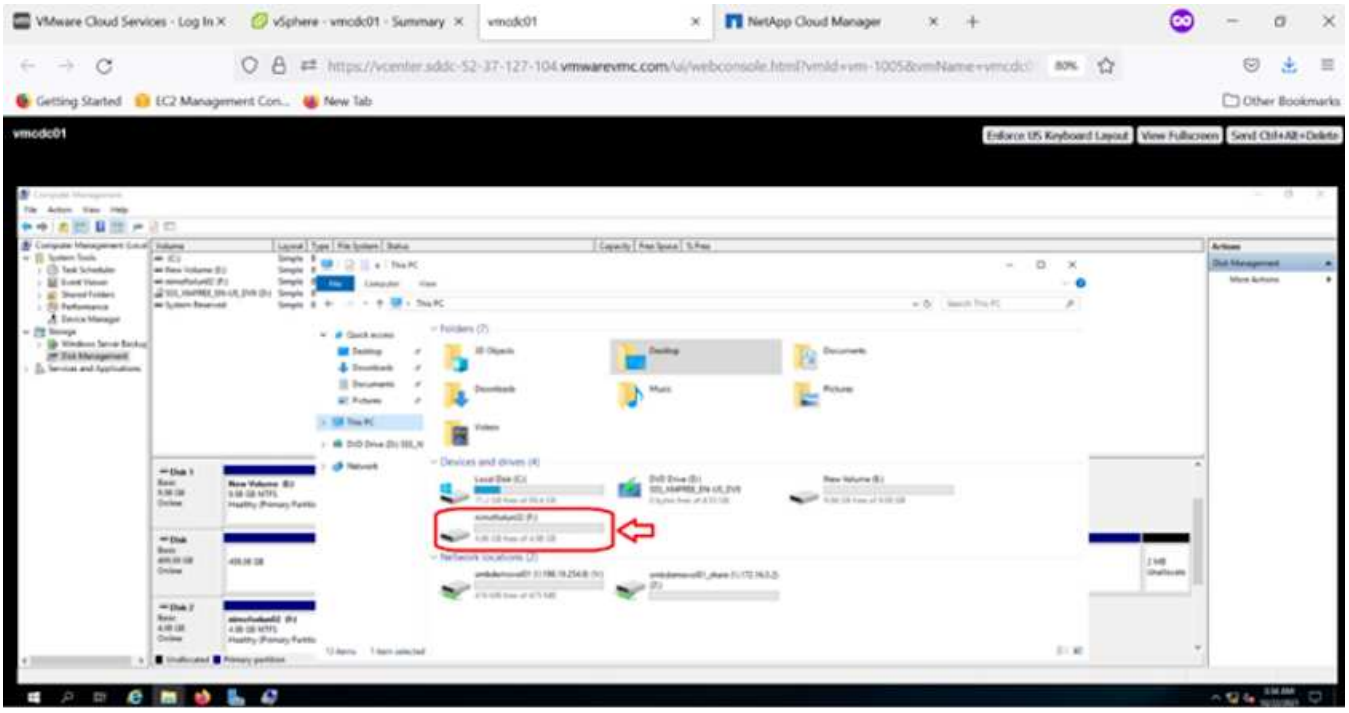
1. 打开 Windows 计算机管理实用程序：开始 > 管理工具 > 计算机管理。
2. 在导航树中展开存储节点。
3. 单击“磁盘管理”。
4. 单击操作 > 重新扫描磁盘。



当 Windows 主机首次访问新的 LUN 时，它没有分区或文件系统。初始化 LUN；并且（可选）通过完成以下步骤使用文件系统格式化 LUN：

1. 启动 Windows 磁盘管理。

2. 右键单击 LUN，然后选择所需的磁盘或分区类型。
3. 按照向导中的说明进行操作。在此示例中，已安装驱动器 F:。



在 Linux 客户端上，确保 iSCSI 守护程序正在运行。配置 LUN 后，请参阅有关 Linux 发行版的 iSCSI 配置的详细指南。例如，Ubuntu iSCSI 配置可以找到"此处"。要验证，请从 shell 运行 lsblk cmd。

▼ 在 **Linux** 客户端上挂载**Cloud Volumes ONTAP NFS** 卷

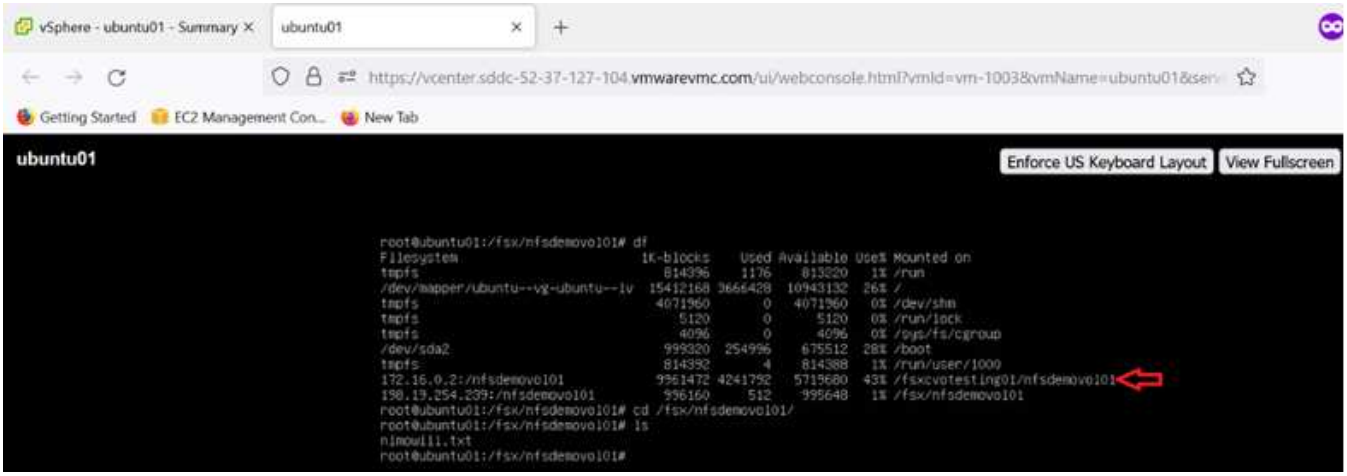
要从 AWS SDDC 上的 VMC 内的虚拟机挂载Cloud Volumes ONTAP (DIY) 文件系统，请完成以下步骤：

1. 连接到指定的Linux实例。
2. 使用安全外壳 (SSH) 在实例上打开终端并使用适当的凭据登录。
3. 使用以下命令为卷的挂载点创建一个目录。

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. 将Amazon FSx ONTAP NFS 卷挂载到上一步创建的目录。
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```

```
root@ubuntu01:/fsx# mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdemovol01_
```



Azure 虚拟化服务：使用**NetApp**存储的选项

NetApp存储可以作为来宾连接存储或补充存储附加到 Azure VMware 服务。

Azure NetApp Files(ANF) 作为补充 **NFS** 数据存储

ESXi 版本 3 在本地部署中引入了 NFS 数据存储支持，这极大地扩展了 vSphere 的存储功能。

在 NFS 上运行 vSphere 是内部虚拟化部署广泛采用的选项，因为它提供了强大的性能和稳定性。如果您在本地数据中心拥有大量网络附加存储 (NAS)，则应考虑使用 Azure NetApp File 数据存储在 Azure 中部署 Azure VMware 解决方案 SDDC，以克服容量和性能挑战。

Azure NetApp Files基于业界领先、高可用性的NetApp ONTAP数据管理软件构建。 Microsoft Azure 服务分为三类：基础、主流和专业。 Azure NetApp Files属于专业类别，并由已在许多地区部署的硬件提供支持。借助内置的高可用性 (HA)， Azure NetApp Files可以保护您的数据免受大多数中断的影响，并为您提供业界领先的 99.99%^ 正常运行时间的 SLA。

有关 ANF 作为补充 NFS 数据存储的更多信息，请访问：

- "ANF 作为补充 NFS 数据存储：概述"
- "Azure 中的补充 NFS 数据存储选项"

Azure NetApp Files(ANF) 作为来宾连接存储

Azure NetApp Files为 Azure 带来企业级数据管理和存储，以便您可以轻松管理工作负载和应用程序。将您的工作负载迁移到云端并运行它们，而不会牺牲性能。

Azure NetApp Files消除了障碍，因此您可以将所有基于文件的应用程序迁移到云端。这是第一次，您不必重新构建您的应用程序，并且您可以轻松获得应用程序的持久存储。

由于该服务是通过 Microsoft Azure 门户提供的，因此用户可以作为 Microsoft 企业协议的一部分体验完全托管的服务。由 Microsoft 管理的世界一流的支持让您完全放心。此单一解决方案使您能够快速轻松地添加多协议工作负载。您可以构建和部署基于 Windows 和 Linux 文件的应用程序，甚至对于传统环境也是如此。

欲了解更多信息，请访问"ANF 作为来宾连接存储"。

Cloud Volumes ONTAP (CVO) 作为来宾连接存储

Cloud Volumes ONTAP (CVO) 是基于 NetApp ONTAP存储软件构建的业界领先的云数据管理解决方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的软件定义版本，使用云原生存储，允许您在云端和本地使用相同的存储软件，从而无需重新培训 IT 人员采用全新方法来管理数据。

CVO 使客户能够无缝地将数据从边缘移动到数据中心、云端并返回，从而将您的混合云整合在一起 - 所有这些都通过单一窗格管理控制台NetApp Cloud Manager 进行管理。

CVO 的设计旨在提供极致的性能和先进的数据管理功能，以满足您在云端最苛刻的应用程序

欲了解更多信息，请访问"CVO 作为客户连接存储"。

ANF 数据存储解决方案概述

每个成功的组织都走在转型和现代化的道路上。作为此过程的一部分，公司通常会使用其现有的 VMware 投资，同时利用云优势并探索如何使迁移、爆发、扩展和灾难恢复过程尽可能无缝。迁移到云端的客户必须评估弹性和爆发、数据中心退出、数据中心整合、生命周期终止场景、合并、收购等问题。每个组织所采用的方法可能因其各自的业务优先级而异。在选择基于云的操作时，选择具有适当性能和最小阻碍的低成本模型是一个关键目标。除了选择正确的平台之外，存储和工作流程编排对于释放云部署和弹性的力量也尤为重要。

使用案例

尽管 Azure VMware 解决方案为客户提供了独特的混合功能，但有限的本机存储选项限制了其对于存储工作负载繁重的组织的实用性。由于存储直接与主机绑定，因此扩展存储的唯一方法是添加更多主机，这可能会使存储密集型工作负载的成本增加 35-40% 或更多。这些工作负载需要额外的存储空间，而不是额外的马力，但这意味着需要支付额外的主机费用。

让我们考虑以下场景；客户需要六台主机来提供马力（vCPU/vMem），但他们对存储也有很大的需求。根据他们的评估，他们需要 12 台主机来满足存储需求。这会增加总体 TCO，因为他们必须购买所有额外的马力，而他们真正需要的只是更多的存储空间。这适用于任何用例，包括迁移、灾难恢复、爆发、开发/测试等等。

Azure VMware 解决方案的另一个常见用例是灾难恢复 (DR)。大多数组织都没有万无一失的 DR 策略，或者他们可能很难证明仅为了 DR 而运行幽灵数据中心是合理的。管理员可能会使用试点集群或按需集群来探索零占用空间 DR 选项。然后他们可以扩展存储而无需添加额外的主机，这可能是一个有吸引力的选择。

总而言之，用例可以按两种方式分类：

- 使用 ANF 数据存储扩展存储容量
- 使用 ANF 数据存储作为灾难恢复目标，以便在软件定义数据中心 (SDDC) 之间的本地或 Azure 区域内实现成本优化的恢复工作流。本指南深入介绍了如何使用Azure NetApp Files为数据存储提供优化存储（当前处于公共预览阶段）以及 Azure VMware 解决方案中一流的数据保护和 DR 功能，使您能够从 vSAN 存储中卸载存储容量。

有关使用 ANF 数据存储的更多信息，请联系您所在地区的NetApp或 Microsoft 解决方案架构师。

Azure VMware 解决方案

Azure VMware 解决方案 (AVS) 是一种混合云服务，可在 Microsoft Azure 公共云中提供功能齐全的 VMware SDDC。 AVS 是使用 Azure 基础架构、完全由 Microsoft 管理和支持并经过 VMware 验证的第一方解决方案。因此，客户可以获得用于计算虚拟化的 VMware ESXi、用于超融合存储的 vSAN 以及用于网络和安全的 NSX，同时利用 Microsoft Azure 的全球影响力、一流的数据中心设施以及与丰富的原生 Azure 服务和解决方案生态系统的接近性。 Azure VMware 解决方案 SDDC 和Azure NetApp Files的组合以最小的网络延迟提供了最佳性能。

无论使用哪种云，部署 VMware SDDC 时，初始集群都包含以下组件：

- VMware ESXi 主机用于计算虚拟化，并使用 vCenter 服务器设备进行管理。
- VMware vSAN 超融合存储，整合了每个 ESXi 主机的物理存储资产。
- VMware NSX 用于虚拟网络和安全，并使用 NSX Manager 集群进行管理。

结束语

无论您的目标是全云还是混合云，Azure NetApp文件都提供了出色的选项来部署和管理应用程序工作负载以及文件服务，同时通过使数据需求无缝连接到应用程序层来降低 TCO。无论用例如何，选择 Azure VMware 解决方案以及Azure NetApp Files都可以快速实现云优势、跨本地和多个云的一致基础架构和操作、工作负载的双向可移植性以及企业级容量和性能。它与用于连接存储的熟悉的过程和程序相同。请记住，只是数据的位置随着新名称而发生了变化；工具和流程都保持不变， Azure NetApp Files有助于优化整体部署。

总结

该文件的要点包括：

- 您现在可以将Azure NetApp Files用作 AVS SDDC 上的数据存储。
- 提高应用程序响应时间并提供更高的可用性，以便在需要的时间和地点提供访问工作负载数据。
- 通过简单、即时的调整大小功能简化 vSAN 存储的整体复杂性。
- 使用动态重塑功能保证关键任务工作负载的性能。
- 如果 Azure VMware 解决方案云是目标，Azure NetApp Files是优化部署的正确存储解决方案。

在哪里可以找到更多信息

要了解有关本文档中描述的信息的更多信息，请参阅以下网站链接：

- Azure VMware 解决方案文档

  "https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files文档

  "https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- 将Azure NetApp Files数据存储附加到 Azure VMware 解决方案主机（预览版）

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-

hosts?tabs=azure-portal/

在 **Azure** 中创建补充 **NFS** 数据存储

ESXi 版本 3 在本地部署中引入了 NFS 数据存储支持，这极大地扩展了 vSphere 的存储功能。

在 NFS 上运行 vSphere 是内部虚拟化部署广泛采用的选项，因为它提供了强大的性能和稳定性。如果您在本地数据中心拥有大量网络附加存储 (NAS)，则应考虑使用 Azure NetApp File 数据存储在 Azure 中部署 Azure VMware 解决方案 SDDC，以克服容量和性能挑战。

Azure NetApp Files基于业界领先、高可用性的NetApp ONTAP数据管理软件构建。 Microsoft Azure 服务分为三类：基础、主流和专业。 Azure NetApp Files属于专业类别，并由已在许多地区部署的硬件提供支持。凭借内置的高可用性 (HA)， Azure NetApp Files可保护您的数据免受大多数中断的影响，并为您提供行业领先的 SLA "99.99%"正常运行时间。

在引入Azure NetApp Files数据存储功能之前，计划托管性能和存储密集型工作负载的客户的横向扩展操作需要扩展计算和存储。

请记住以下问题：

- 不建议在 SDDC 集群中使用不平衡的集群配置。因此，扩展存储意味着添加更多主机，这意味着更多的 TCO。
- 仅可实现一个 vSAN 环境。因此，所有存储流量都直接与生产工作负载竞争。
- 没有提供多个性能层来满足应用程序要求、性能和成本的选项。
- 在集群主机之上构建的 vSAN 很容易达到存储容量的极限。通过将 Azure 原生平台即服务 (PaaS) 产品（如Azure NetApp Files）集成为数据存储，客户可以选择单独扩展其存储，并且仅根据需要向 SDDC 集群添加计算节点。这种能力克服了上述挑战。

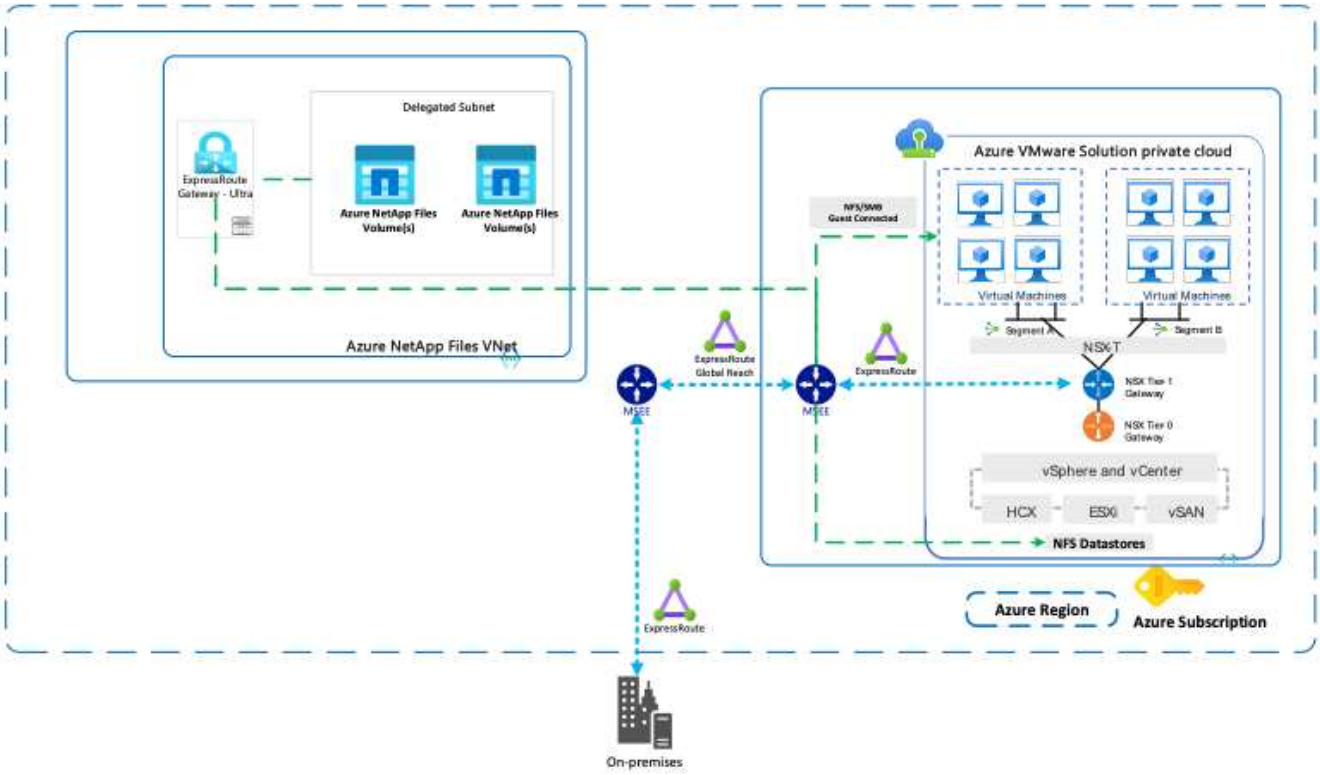
Azure NetApp Files还允许您部署多个数据存储，通过将虚拟机放置在适当的数据存储中并分配所需的服务级别以满足工作负载性能要求，这有助于模拟本地部署模型。凭借其独特的多协议支持功能，客户存储成为 SQL 和 Oracle 等数据库工作负载的附加选项，同时还可使用补充 NFS 数据存储功能来容纳剩余的 VMDK。除此之外，本机快照功能使您能够执行快速备份和粒度恢复。



联系 Azure 和NetApp解决方案架构师来规划和调整存储大小并确定所需的主机数量。 NetApp建议在最终确定测试、POC 和生产部署的数据存储布局之前确定存储性能要求。

详细架构

从高层次的角度来看，该架构描述了如何实现跨本地环境和 Azure 的混合云连接和应用程序可移植性。它还描述了如何使用Azure NetApp Files作为补充 NFS 数据存储以及作为 Azure VMware 解决方案上托管的客户虚拟机的客户机存储选项。



浆纱

迁移或灾难恢复中最重要的方面是确定目标环境的正确规模。了解需要多少个节点才能完成从本地到 Azure VMware 解决方案的直接迁移练习非常重要。

对于大小调整，请使用 RVTools（首选）或其他工具（如 Live Optics 或 Azure Migrate）使用来自本地环境的历史数据。 RVTools 是捕获 vCPU、vMem、vDisk 和所有所需信息（包括已开启或关闭的虚拟机）以表征目标环境的理想工具。

要运行 RVtools，请完成以下步骤：

1. 下载并安装 RVTools。
2. 运行 RVTools，输入连接到本地 vCenter Server 所需的信息，然后按“登录”。
3. 将库存导出到 Excel 电子表格。
4. 编辑电子表格并从 vInfo 选项卡中删除任何不理想的虚拟机。此方法提供了有关存储要求的清晰输出，可用于根据所需数量的主机正确调整 Azure VMware SDDC 群集的大小。

> 与来宾内存储一起使用的来宾虚拟机必须单独计算；但是， Azure NetApp Files可以轻松覆盖额外的存储容量，从而保持较低的整体 TCO。

部署和配置 **Azure VMware** 解决方案

与本地一样，规划 Azure VMware 解决方案对于成功创建虚拟机和迁移的生产就绪环境至关重要。

本节介绍如何设置和管理 AVS，以便将其与Azure NetApp Files结合使用，作为具有来宾内存储的数据存储。

设置过程可分为三个部分：

- 注册资源提供者并创建私有云。
- 连接到新的或现有的 ExpressRoute 虚拟网络网关。
- 验证网络连接并访问私有云。参考这个"链接"有关 Azure VMware 解决方案 SDDC 预配过程的分步演练。

使用 **Azure VMware** 解决方案配置**Azure NetApp Files**

Azure NetApp Files之间的新集成使您能够通过 Azure VMware 解决方案资源提供程序 API/CLI 使用Azure NetApp Files卷创建 NFS 数据存储，并将数据存储安装在私有云中您选择的集群上。除了容纳 VM 和应用程序 VMDK 之外，Azure NetApp文件卷还可以从在 Azure VMware 解决方案 SDDC 环境中创建的 VM 中装载。由于Azure NetApp Files支持服务器消息块 (SMB) 和网络文件系统 (NFS) 协议，因此卷可以安装在 Linux 客户端上并映射到 Windows 客户端上。

> 为了获得最佳性能，请将Azure NetApp Files部署在与私有云相同的可用区域中。与 Express 路由快速路径共置可提供最佳性能，同时最大程度地减少网络延迟。

要将 Azure NetApp文件卷附加为 Azure VMware 解决方案私有云的 VMware 数据存储，请确保满足以下先决条件。

▼ 前提条件

1. 使用 az login 并验证订阅是否已注册到 Microsoft.AVS 命名空间中的 CloudSanExperience 功能。

```
az login –tenant xcvxcvxc- vxcv- xcvx- cvxc- vxcvxcvxcv
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

1. 如果未注册，则注册。

```
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

> 注册大约需要 15 分钟才能完成。

1. 要检查注册状态，请运行以下命令。

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
--query properties.state
```

1. 如果注册停留在中间状态超过 15 分钟，则取消注册，然后重新注册该标志。

```
az feature unregister --name "CloudSanExperience" --namespace
"Microsoft.AVS"
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

1. 验证订阅是否已注册到 Microsoft.AVS 命名空间中的 AnfDatastoreExperience 功能。

```
az feature show --name "AnfDatastoreExperience" --namespace
"Microsoft.AVS" --query properties.state
```

1. 验证 vmware 扩展是否已安装。

```
az extension show --name vmware
```

1. 如果扩展已安装，请验证版本是否为 3.0.0。如果安装了旧版本，请更新扩展。

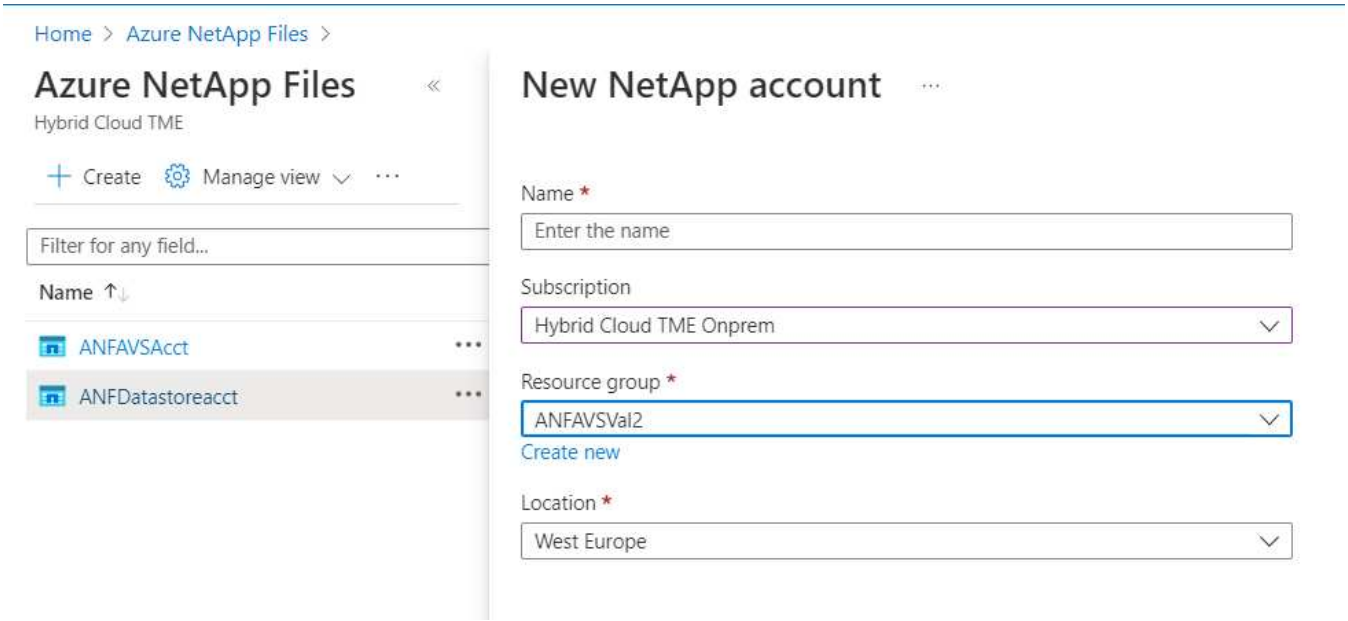
```
az extension update --name vmware
```

1. 如果尚未安装该扩展，请安装它。

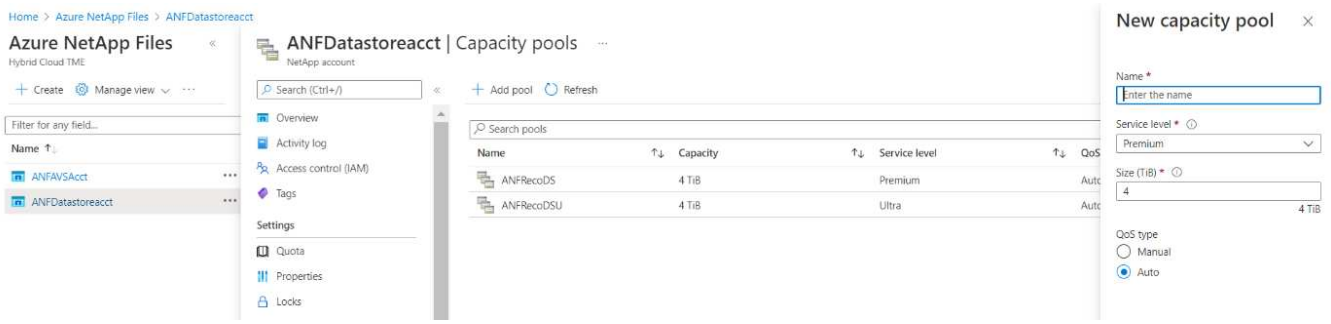
```
az extension add --name vmware
```

▼ 创建并装载**Azure NetApp Files**卷

1. 登录 Azure 门户并访问Azure NetApp Files。验证对Azure NetApp FilesAzure NetApp Files的访问权限，并使用 `az provider register `--namespace Microsoft.NetApp –wait`命令。注册后，创建一个NetApp帐户。参考这个 "链接"了解详细步骤。



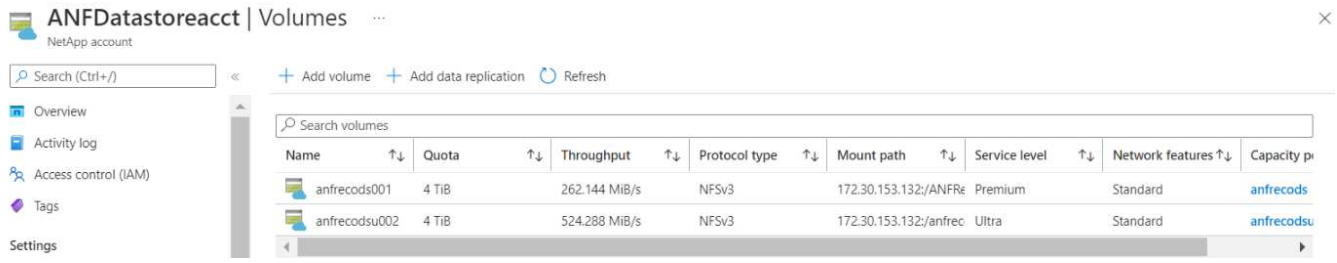
1. 创建NetApp帐户后，设置具有所需服务级别和大小的容量池。有关详细信息，请参阅此 "链接"。



需要记住的要点

- Azure NetApp Files上的数据存储支持 NFSv3。
- 在补充默认 vSAN 存储的同时，根据需要对容量受限的工作负载使用高级或标准层，对性能受限的工作负载使用超级层。

1. 为Azure NetApp Files配置委托子网，并在创建卷时指定此子网。有关创建委托子网的详细步骤，请参阅此 "链接"。
2. 使用容量池边栏选项卡下的卷边栏选项卡为数据存储添加 NFS 卷。



若要了解Azure NetApp Files卷按大小或配额的性能，请参阅"Azure NetApp Files的性能注意事项"。

▼ 将 **Azure NetApp**文件数据存储添加到私有云

可以使用 Azure 门户将Azure NetApp Files卷附加到您的私有云。关注此"来自微软的链接"使用 Azure 门户逐步挂载 Azure NetApp文件数据存储。

要将 Azure NetApp文件数据存储添加到私有云，请完成以下步骤：

1. 注册所需的功能后，通过运行适当的命令将 NFS 数据存储附加到 Azure VMware 解决方案私有云群集。
2. 使用 Azure VMware 解决方案私有云群集中的现有 ANF 卷创建数据存储。

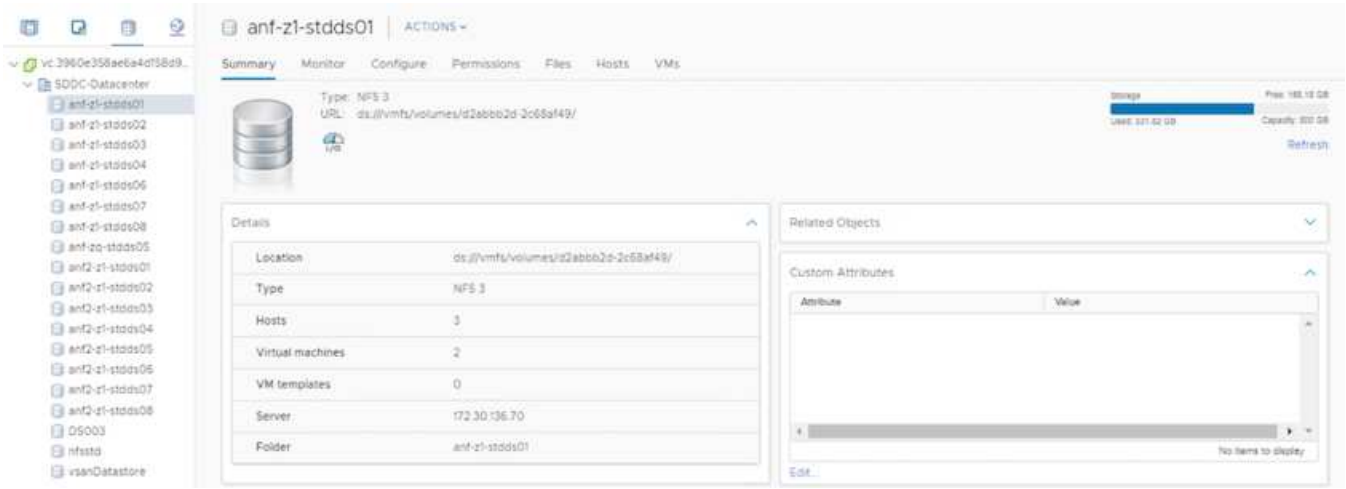
```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
```

```
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}

. List all the datastores in a private cloud cluster.
```

C:\Users\niyaz>az vmware 数据存储列表 --resource-group anfavsval2 --cluster Cluster-1 --private-cloud ANFDataClus [{ “diskPoolVolume”：null，“id”：“/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDS001”， “name”：“ANFRecoDS001”， “netAppVolume”：{ “id”：“/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001”， “resourceGroup”：“anfavsval2”}，“provisioningState”：“成功”， “resourceGroup”：“anfavsval2”， “type”：“Microsoft.AVS/privateClouds/clusters/datastores”}，{ “diskPoolVolume”：null， “id”：“/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002”， “name”：“ANFRecoDSU002”， “netAppVolume”：{ “id”：“/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002”， “resourceGroup”：“NetApp”}，“provisioningState”：“成功”， “resourceGroup”：“anfavsval2”， “type”：“Microsoft.AVS/privateClouds/clusters/datastores”}]

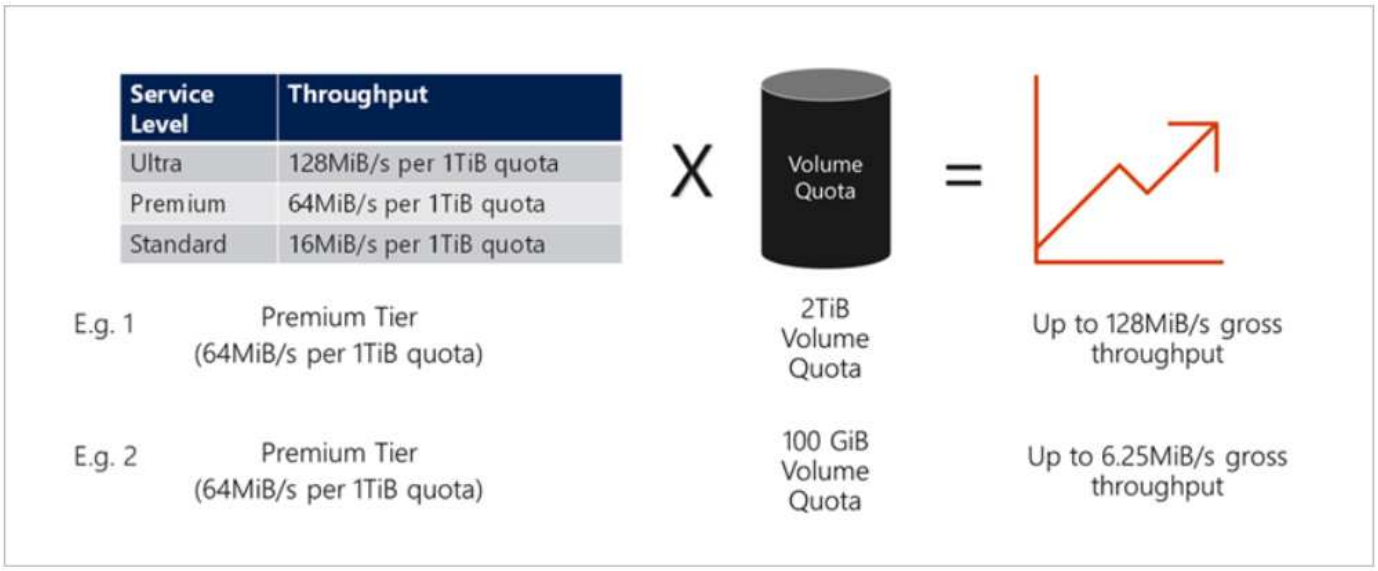
1. 在建立必要的连接后，卷将作为数据存储安装。



尺寸和性能优化

Azure NetApp Files支持三种服务级别：标准级（每 TB 16MBps）、高级级（每 TB 64MBps）和超级级（每 TB 128MBps）。配置正确的卷大小对于数据库工作负载的最佳性能非常重要。使用Azure NetApp Files，卷性能和吞吐量限制根据以下因素确定：

- 卷所属容量池的服务级别
- 分配给卷的配额
- 容量池的服务质量 (QoS) 类型（自动或手动）



有关更多信息，请参阅 "Azure NetApp Files的服务级别" 。

参考这个"来自微软的链接"以获得可在规模调整练习期间使用的详细性能基准。

需要记住的要点

- 使用高级或标准层作为数据存储卷，以获得最佳容量和性能。如果需要性能，则可以使用超级层。
- 对于来宾挂载要求，请使用 Premium 或 Ultra 层；对于来宾虚拟机的文件共享要求，请使用 Standard 或 Premium 层卷。

性能考虑

重要的是要理解，使用 NFS 版本 3 时，ESXi 主机和单个存储目标之间的连接只有一个活动管道。这意味着尽管可能存在可用于故障转移的备用连接，但单个数据存储和底层存储的带宽仅限于单个连接所能提供的带宽。

为了利用Azure NetApp Files卷的更多可用带宽，ESXi 主机必须与存储目标建立多个连接。为了解决此问题，您可以配置多个数据存储区，每个数据存储区使用 ESXi 主机和存储之间的单独连接。

为了获得更高的带宽，最佳做法是使用多个 ANF 卷创建多个数据存储区，创建 VMDK，并在 VMDK 之间对逻辑卷进行条带化。

参考这个"来自微软的链接"以获得可在规模调整练习期间使用的详细性能基准。

需要记住的要点

- Azure VMware 解决方案默认允许八个 NFS 数据存储。这可以通过支持请求来增加。
- 利用 ER 快速路径和 Ultra SKU 实现更高的带宽和更低的延迟。更多信息
- 借助 Azure NetApp文件中的“基本”网络功能，来自 Azure VMware 解决方案的连接受 ExpressRoute 线路和 ExpressRoute 网关的带宽约束。
- 对于具有“标准”网络功能的Azure NetApp Files卷，支持 ExpressRoute FastPath。启用后，FastPath 会将网络流量直接发送到Azure NetApp Files卷，绕过网关，提供更高的带宽和更低的延迟。

增加数据存储的大小

卷重塑和动态服务级别变化对于 SDDC 来说是完全透明的。在Azure NetApp Files中，这些功能可提供持续的性能、容量和成本优化。通过从 Azure 门户调整卷大小或使用 CLI 来增加 NFS 数据存储的大小。完成后，访问 vCenter，转到数据存储选项卡，右键单击相应的数据存储，然后选择刷新容量信息。这种方法可用于增加数据存储容量，并以动态方式提高数据存储的性能，且无需停机。这个过程对于应用程序来说也是完全透明的。

需要记住的要点

- 卷重塑和动态服务级别功能允许您通过调整稳定状态工作负载的大小来优化成本，从而避免过度配置。
- 未启用 VAAI

工作负载

▼ 迁移

最常见的用例之一是迁移。使用 VMware HCX 或 vMotion 移动本地虚拟机。或者，您可以使用 Rivermeadow 将虚拟机迁移到Azure NetApp Files数据存储。

▼ 数据保护

备份虚拟机并快速恢复它们是 ANF 数据存储的一大优势。使用 Snapshot 副本快速复制您的 VM 或数据存储而不影响性能，然后将它们发送到 Azure 存储以实现长期数据保护，或使用跨区域复制将其发送到辅助区域以实现灾难恢复。这种方法仅存储改变的信息，从而最大限度地减少了存储空间和网络带宽。

使用Azure NetApp FilesSnapshot 副本进行常规保护，并使用应用程序工具保护驻留在来宾虚拟机上的事务数据（例如 SQL Server 或 Oracle）。这些 Snapshot 副本与 VMware（一致性）快照不同，适合长期保护。

使用 ANF 数据存储，“恢复到新卷”选项可用于克隆整个数据存储卷，并且恢复的卷可以作为另一个数据存储安装到 AVS SDDC 内的主机。安装数据存储后，可以注册、重新配置和定制其中的虚拟机，就像单独克隆的虚拟机一样。

▼ 适用于虚拟机的 **NetApp Backup and Recovery**

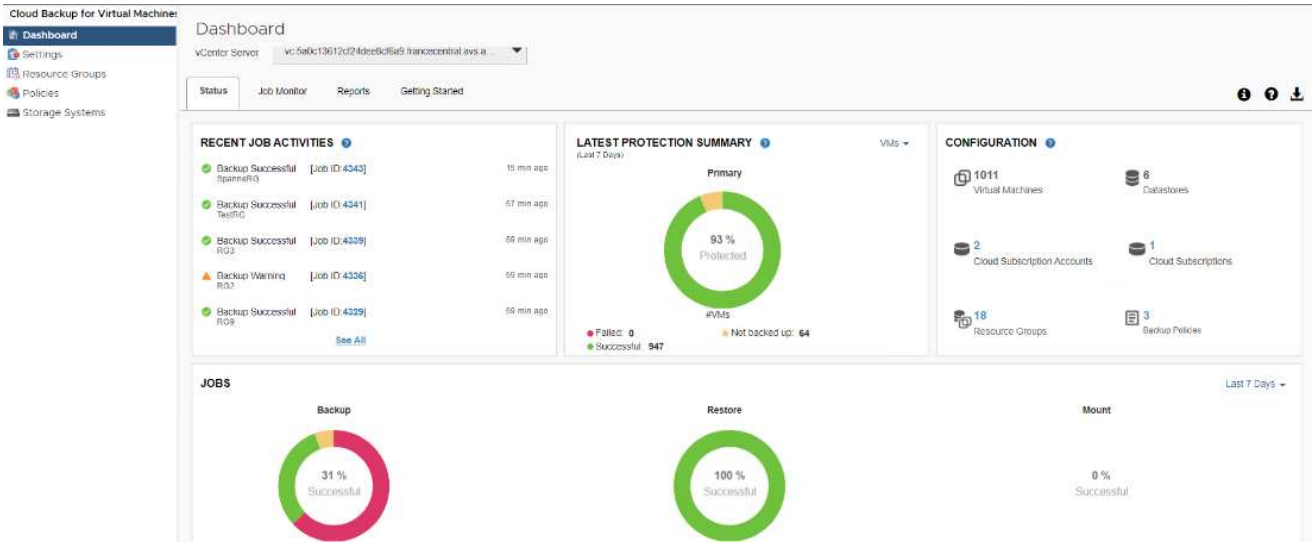
NetApp Backup and Recovery for Virtual Machines 在 vCenter 上提供 vSphere Web 客户端 GUI，可通过备份策略保护 Azure VMware Solution 虚拟机和 Azure NetApp Files 数据存储。这些策略可定义计划、保留期及其他功能。NetApp Backup and Recovery for Virtual Machines 功能可通过使用 Run 命令进行部署。

可以通过完成以下步骤来安装设置和保护策略：

1. 使用“运行”命令在 Azure VMware Solution 私有云中安装针对虚拟机的 NetApp Backup and Recovery。

2. 添加云订阅凭据（客户端和密钥值），然后添加包含您想要保护的资源的云订阅帐户（NetApp帐户和相关资源组）。
3. 创建一个或多个备份策略来管理资源组备份的保留、频率和其他设置。
4. 创建一个容器来添加一个或多个需要使用备份策略保护的资源。
5. 如果发生故障，将整个 VM 或特定的单个 VMDK 恢复到同一位置。

借助Azure NetApp Files Snapshot 技术，备份和恢复速度非常快。



▼ 使用**Azure NetApp Files**、**JetStream DR** 和 **Azure VMware** 解决方案进行灾难恢复

灾难恢复到云端是一种具有弹性且经济高效的方法，可以保护工作负载免受站点中断和数据损坏事件（例如勒索软件）的影响。使用 VMware VAIO 框架，可以将本地 VMware 工作负载复制到 Azure Blob 存储并进行恢复，从而实现最少或几乎无数据丢失以及接近零的 RTO。 JetStream DR 可用于无缝恢复从本地复制到 AVS 以及特别是Azure NetApp Files 的工作负载。它通过使用灾难恢复站点的最少资源和经济高效的云存储实现经济高效的灾难恢复。 JetStream DR 通过 Azure Blob Storage 自动恢复到 ANF 数据存储。 JetStream DR 根据网络映射将独立的虚拟机或相关虚拟机组恢复到恢复站点基础设施中，并提供时间点恢复以进行勒索软件保护。

"采用 ANF、JetStream 和 AVS 的 DR 解决方案" 。

适用于 **Azure** 的**NetApp**来宾连接存储选项

Azure 支持通过本机Azure NetApp Files(ANF) 服务或Cloud Volumes ONTAP (CVO) 连接来宾的NetApp存储。

Azure NetApp Files(ANF)

Azure netApp Files 为 Azure 带来企业级数据管理和存储，以便您可以轻松管理工作负载和应用程序。将您的工作负载迁移到云端并运行它们，而不会牺牲性能。

Azure netApp Files 消除了障碍，因此您可以将所有基于文件的应用程序迁移到云端。这是第一次，您不必重新构建您的应用程序，并且您可以轻松获得应用程序的持久存储。

由于该服务是通过 Microsoft Azure 门户提供的，因此用户可以作为 Microsoft 企业协议的一部分体验完全托管的服务。由 Microsoft 管理的世界一流的支持让您完全放心。此单一解决方案使您能够快速轻松地添加多协议工

作负载。您可以构建和部署基于 Windows 和 Linux 文件的应用程序，甚至对于传统环境也是如此。

Azure NetApp Files(ANF) 作为来宾连接存储

▼ 使用 **Azure VMware** 解决方案 **(AVS)** 配置**Azure NetApp Files**

可以从 Azure VMware 解决方案 SDDC 环境中创建的 VM 装载Azure NetApp Files共享。由于Azure NetApp Files支持 SMB 和 NFS 协议，因此卷也可以安装在 Linux 客户端上并映射到 Windows 客户端上。只需五个简单的步骤即可设置Azure NetApp Files卷。

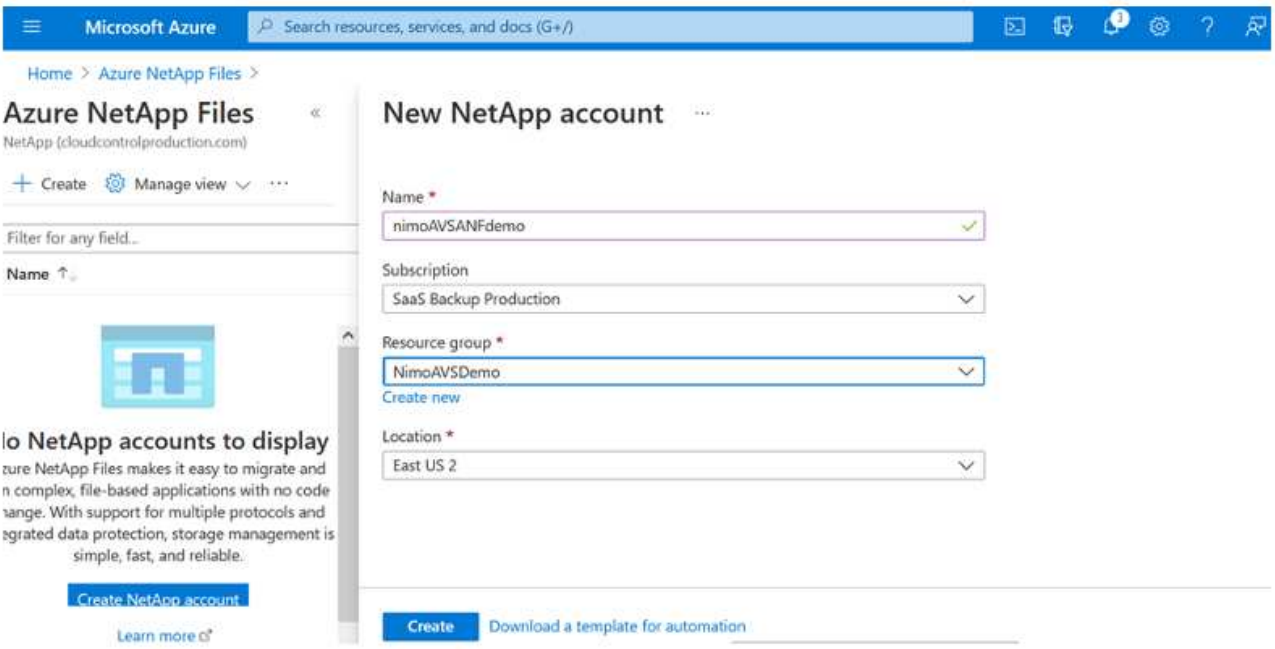
Azure NetApp Files和 Azure VMware 解决方案必须位于同一 Azure 区域。

▼ 创建并装载**Azure NetApp Files**卷

要创建和装载Azure NetApp Files卷，请完成以下步骤：

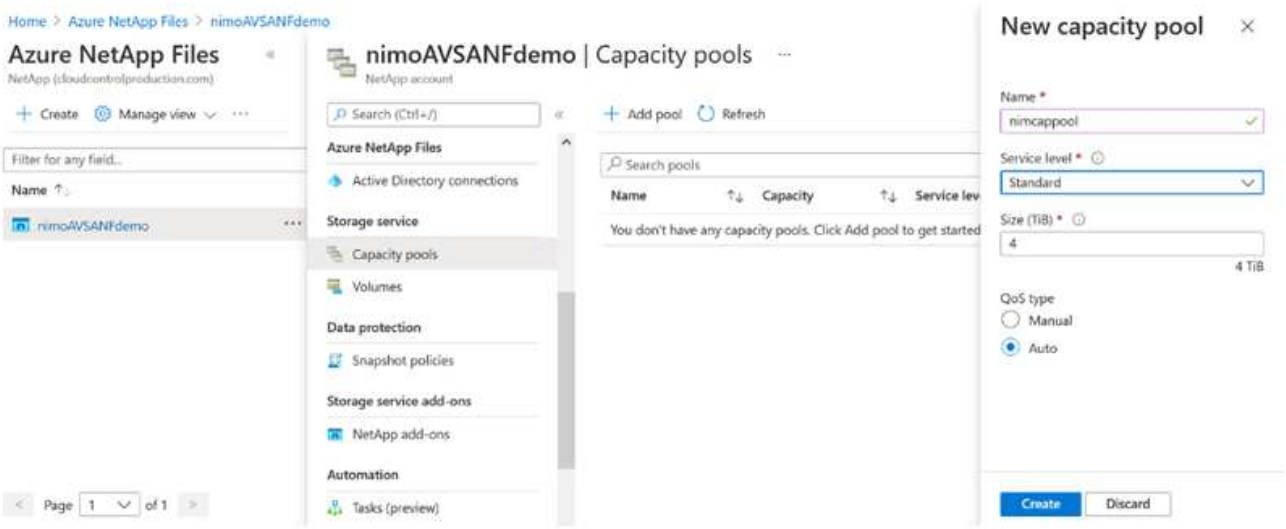
1. 登录 Azure 门户并访问Azure NetApp Files。验证对Azure NetApp Files服务的访问，并使用NetApp provider register --namespace Microsoft.NetApp –wait 命令注册Azure NetApp Files资源提供程序。注册完成后，创建一个NetApp帐户。

   详细步骤请参见"Azure NetApp Files共享"。本页将指导您完成逐步的过程。

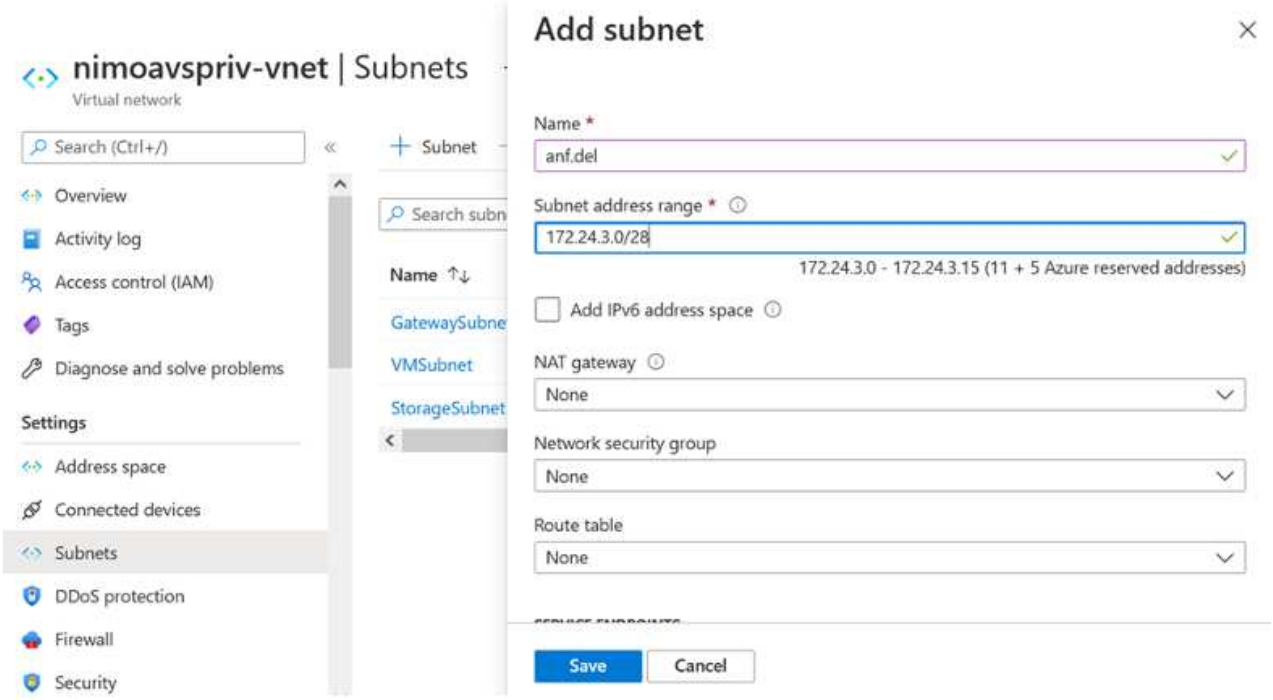


2. 创建NetApp帐户后，设置具有所需服务级别和大小的容量池。

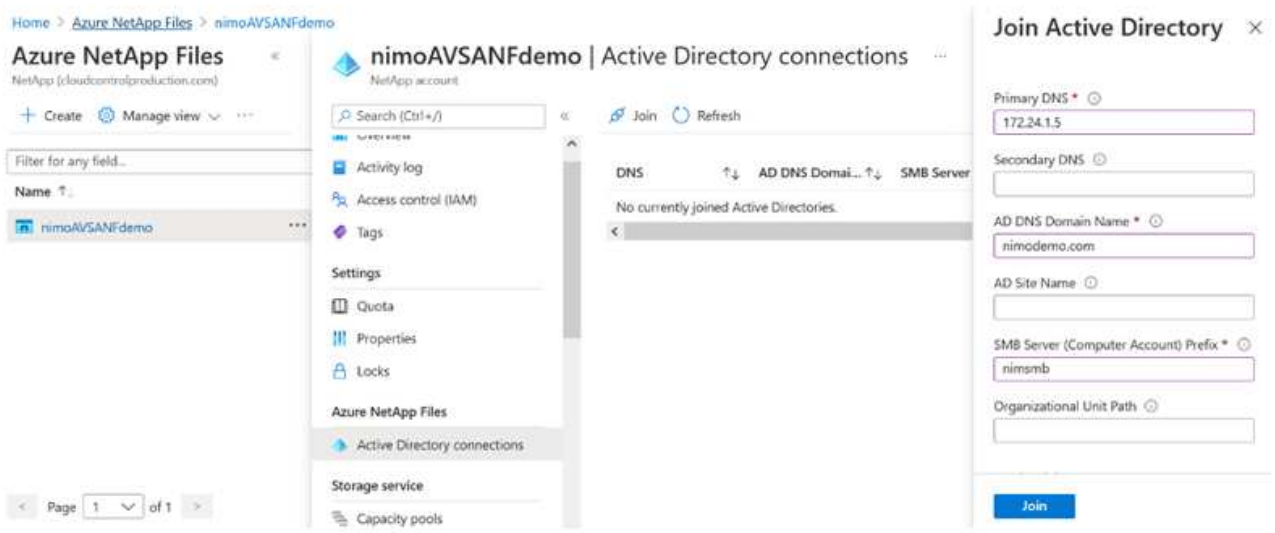
   有关更多信息，请参阅"设置容量池Set up a capacity pool" 。



3. 为Azure NetApp Files配置委托子网，并在创建卷时指定此子网。有关创建委托子网的详细步骤，请参阅"将子网委托给Azure NetApp Files"。

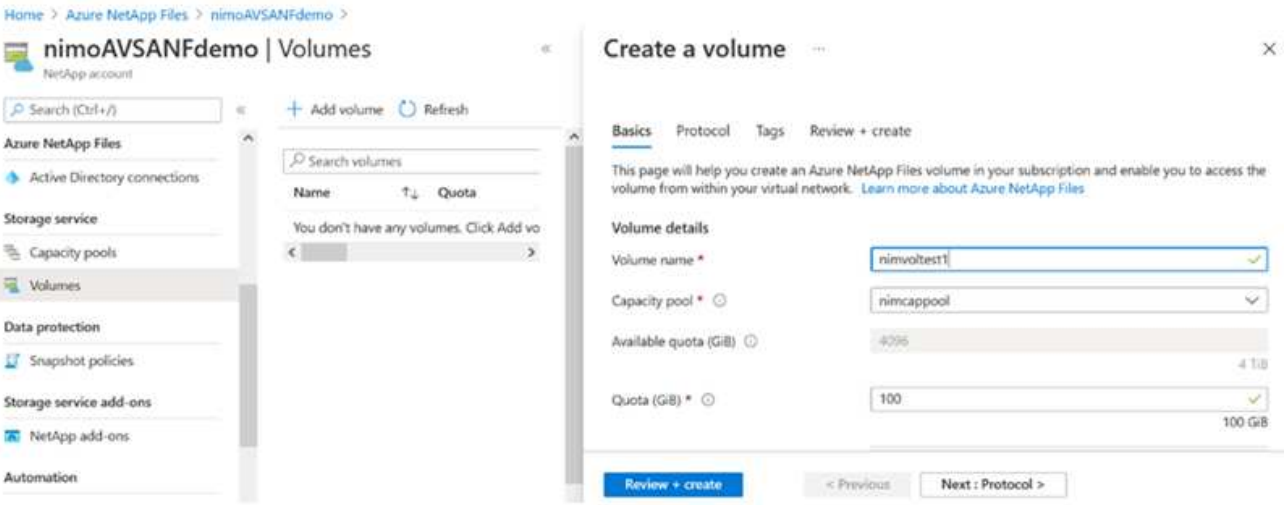


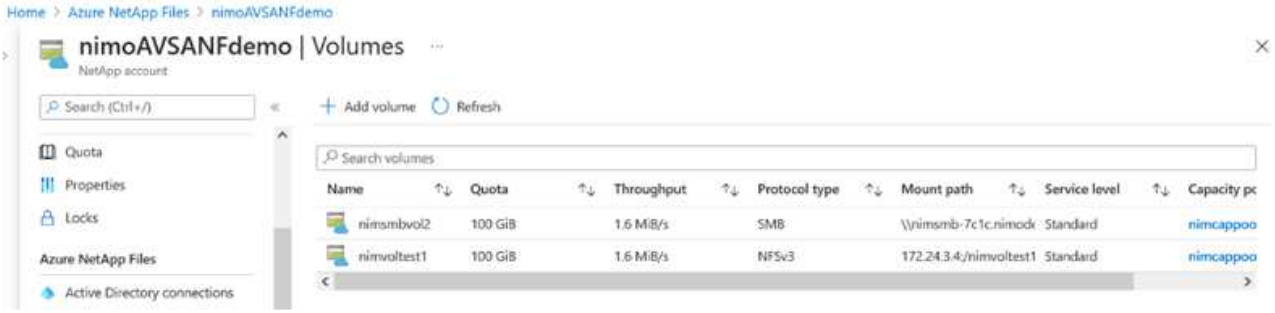
4. 使用“容量池”边栏选项卡下的“卷”边栏选项卡添加 SMB 卷。确保在创建 SMB 卷之前配置了 Active Directory 连接器。



5. 单击“查看 + 创建”以创建 SMB 卷。

   如果应用程序是 SQL Server，则启用 SMB 持续可用性。

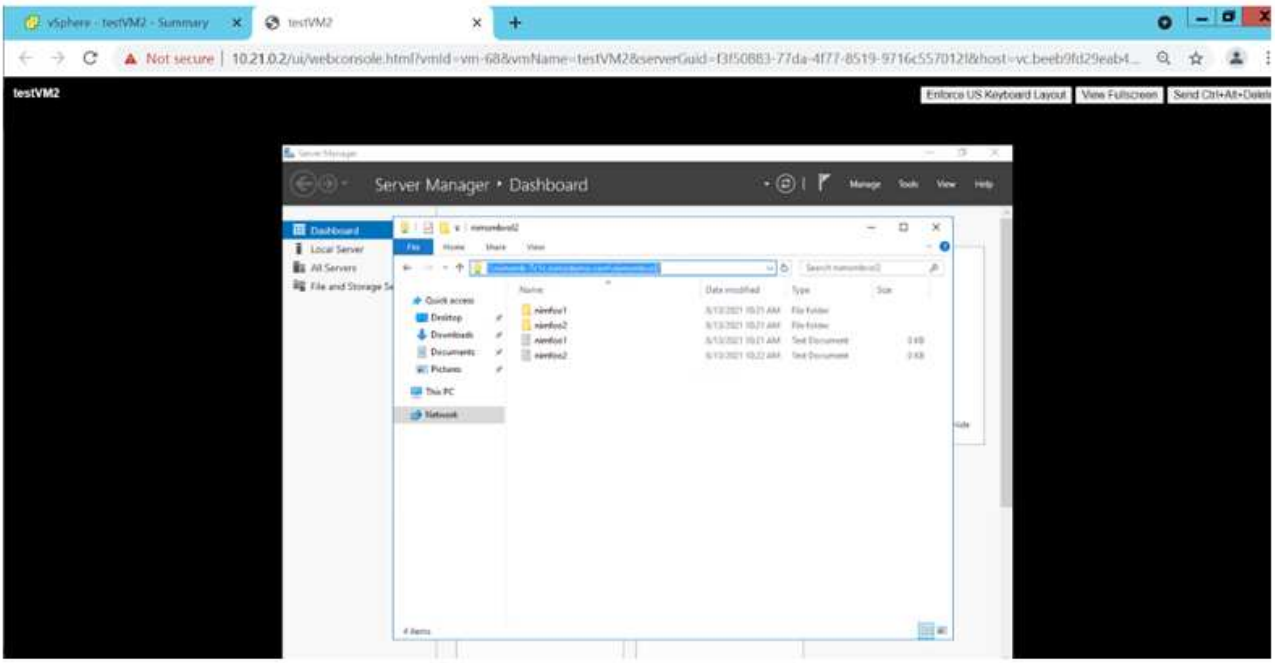


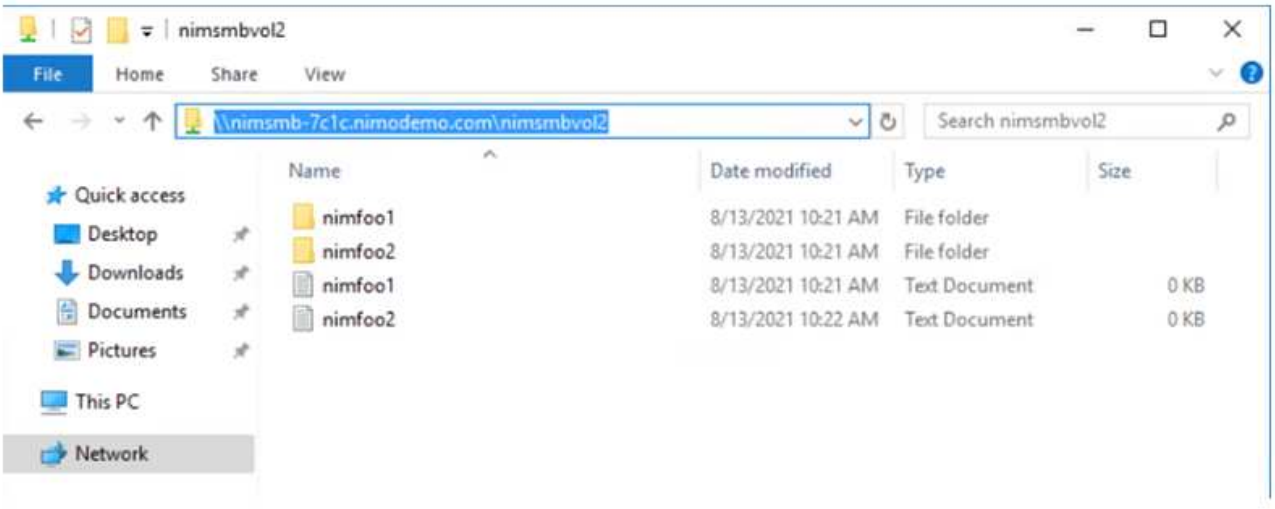


若要详细了解Azure NetApp Files卷按大小或配额的性能，请参阅"Azure NetApp Files的性能注意事项"。

6. 连接建立后，即可挂载该卷并将其用于应用程序数据。

   为此，请在 Azure 门户中单击“卷”边栏选项卡，然后选择要挂载的卷并访问挂载说明。复制路径并使用映射网络驱动器选项将卷装载到在 Azure VMware 解决方案 SDDC 上运行的 VM 上。





7. 要在 Azure VMware 解决方案 SDDC 上运行的 Linux VM 上装载 NFS 卷，请使用相同的过程。使用卷重塑或动态服务级别功能来满足工作负载需求。

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                   1K-blocks     Used Available Use% Mounted on
udev                           8168112        0   8168112   0% /dev
tmpfs                          1639548     1488   1638060   1% /run
/dev/sda5                     50824704  7902752  40310496  17% /
tmpfs                          8197728        0   8197728   0% /dev/shm
tmpfs                             5120        0      5120   0% /run/lock
tmpfs                          8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                       56832    56832         0 100% /snap/core18/2128
/dev/loop2                       66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                      224256   224256         0 100% /snap/gnome-3-34-188
4/72
/dev/loop3                       52224    52224         0 100% /snap/snap-store/547
/dev/loop4                       33152    33152         0 100% /snap/snapd/12704
/dev/sda1                       523248        4    523244   1% /boot/efi
tmpfs                          1639544       52   1639492   1% /run/user/1000
/dev/sr0                         54738    54738         0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

有关更多信息，请参阅"动态更改卷的服务级别" 。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP（或称 CVO）是基于 NetApp 的ONTAP存储软件构建的业界领先的云数据管理解决方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的软件定义版本，使用云原生存储，允许您在云端和本地使用相同的存储软件，从而无需重新培训 IT 人员采用全新方法来管理数据。

CVO 使客户能够无缝地将数据从边缘移动到数据中心、云端并返回，从而将您的混合云整合在一起 - 所有这些

都通过单一窗格管理控制台NetApp Cloud Manager 进行管理。

CVO 的设计旨在提供极致的性能和先进的数据管理功能，以满足您在云端最苛刻的应用程序

Cloud Volumes ONTAP (CVO) 作为来宾连接存储

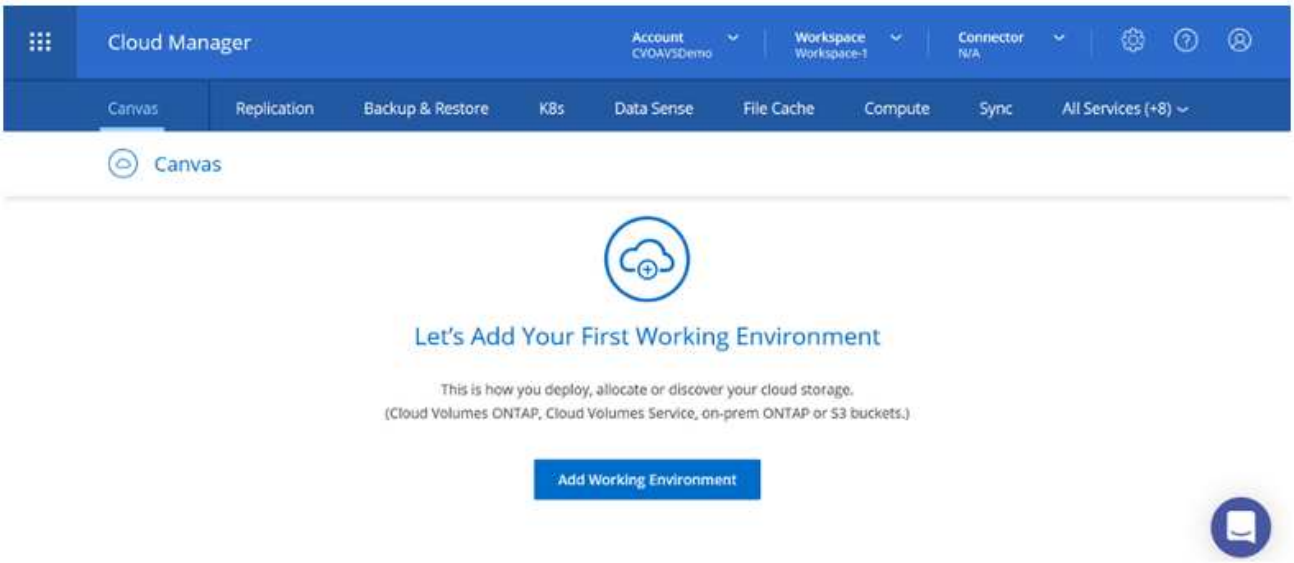
▼ 在 **Azure** 中部署新的**Cloud Volumes ONTAP**

可以从在 Azure VMware 解决方案 SDDC 环境中创建的 VM 挂载Cloud Volumes ONTAP共享和 LUN。由于Cloud Volumes ONTAP支持 iSCSI、SMB 和 NFS 协议，因此卷也可以安装在 Linux 客户端和 Windows 客户端上。只需几个简单的步骤即可设置Cloud Volumes ONTAP卷。

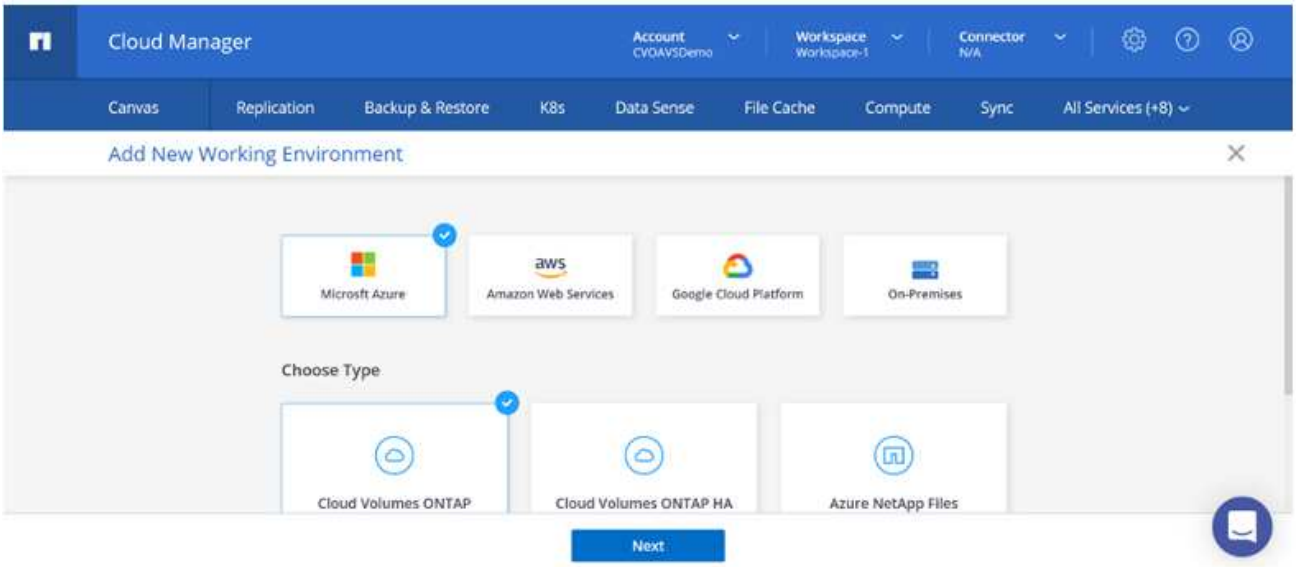
要将卷从本地环境复制到云中以用于灾难恢复或迁移目的，请使用站点到站点 VPN 或 ExpressRoute 建立与 Azure 的网络连接。将数据从本地复制到Cloud Volumes ONTAP超出了本文档的范围。要在本地和Cloud Volumes ONTAP系统之间复制数据，请参阅"设置系统之间的数据复制"。

使用 "Cloud Volumes ONTAP大小调整器" 准确调整 Cloud Volumes ONTAP 实例的大小。此外，还应监控本地性能，以用作 Cloud Volumes ONTAP sizer 中的输入。

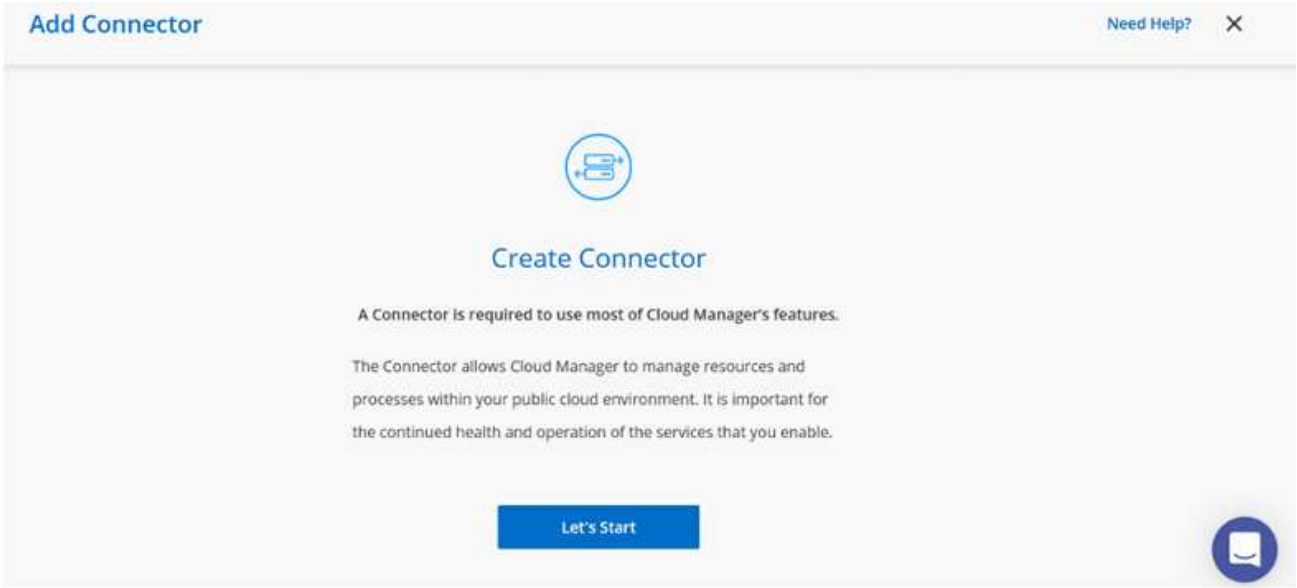
1. 登录NetApp Cloud Central — 显示 Fabric View 屏幕。找到Cloud Volumes ONTAP选项卡并选择转到云管理器。登录后，将显示 Canvas 屏幕。



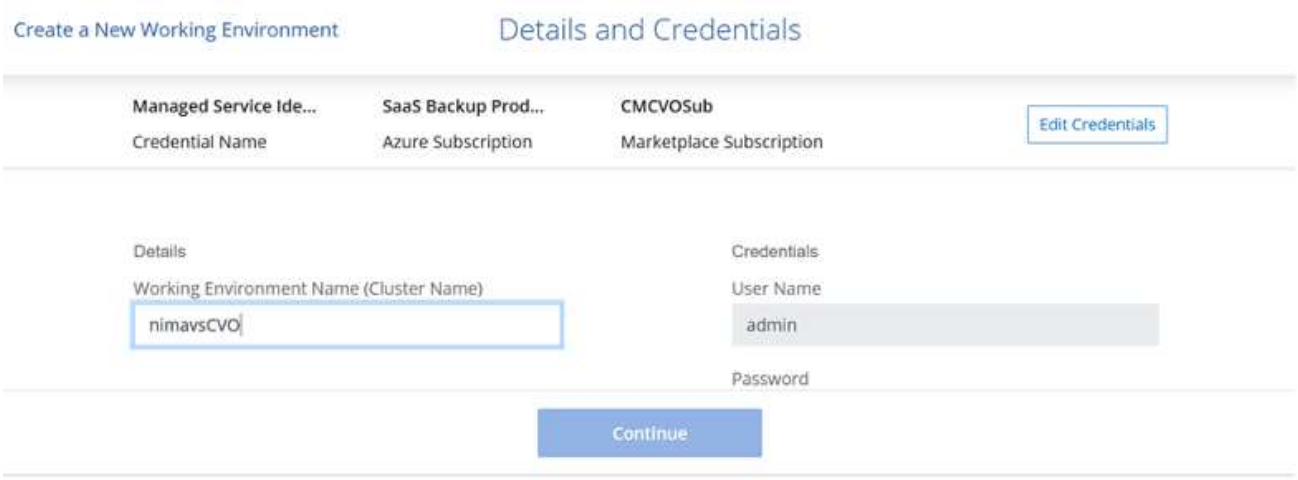
2. 在云管理器主页上，单击添加工作环境，然后选择 Microsoft Azure 作为云和系统配置类型。



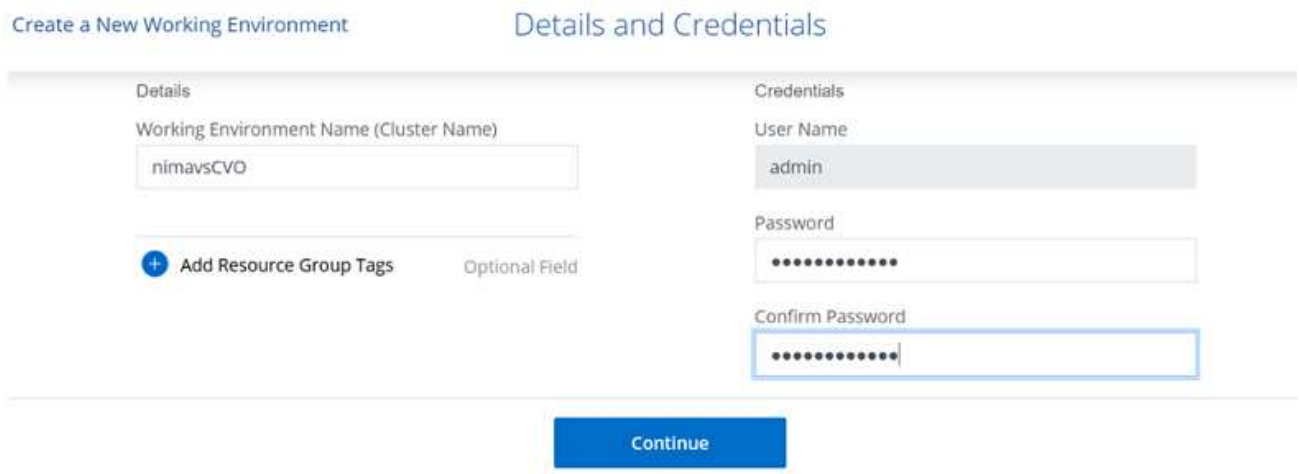
3. 创建第一个Cloud Volumes ONTAP工作环境时，Cloud Manager 会提示您部署连接器。



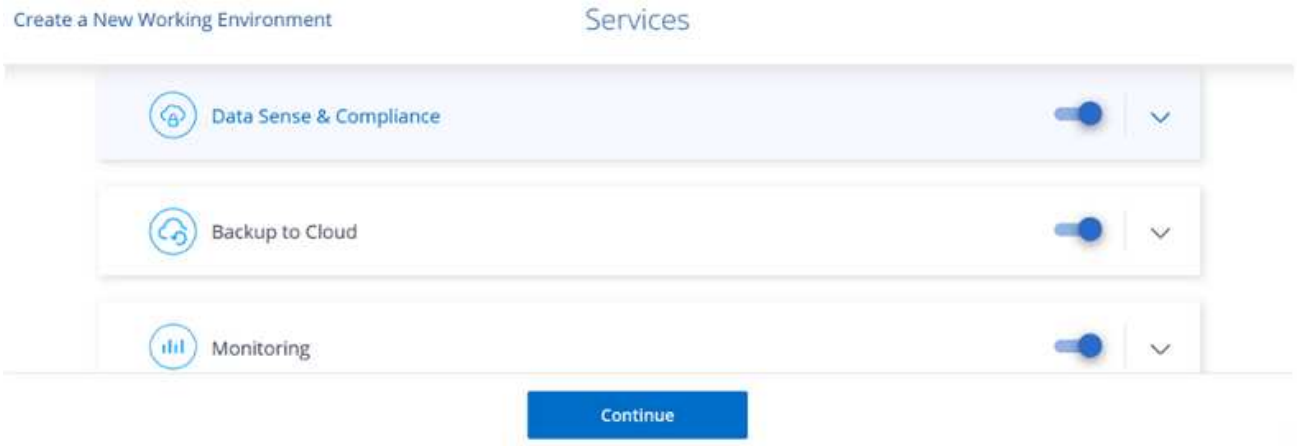
4. 创建连接器后，更新详细信息和凭据字段。



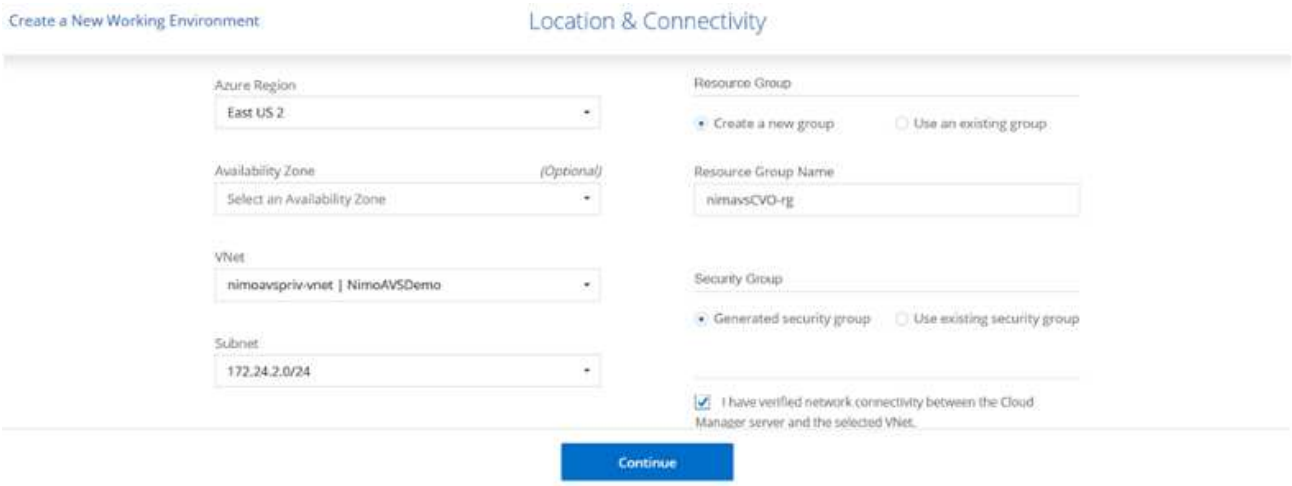
5. 提供要创建的环境的详细信息，包括环境名称和管理员凭据。添加 Azure 环境的资源组标签作为可选参数。完成后，单击“继续”。



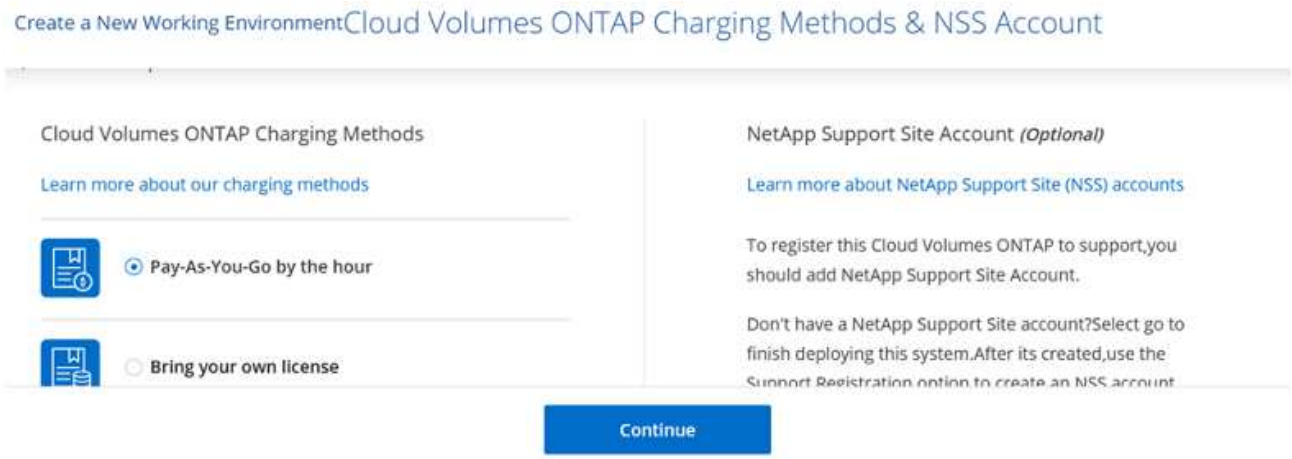
6. 选择 Cloud Volumes ONTAP 部署的附加服务，包括 NetApp Data Classification、NetApp Backup and Recovery 以及 Data Infrastructure Insights。选择服务，然后单击“继续”。



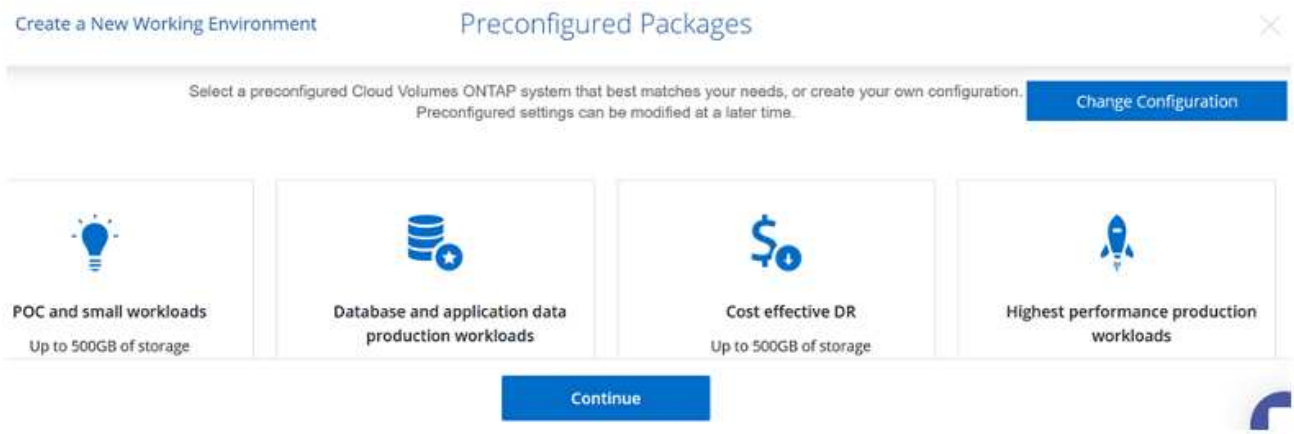
7. 配置 Azure 位置和连接。选择要使用的 Azure 区域、资源组、VNet 和子网。



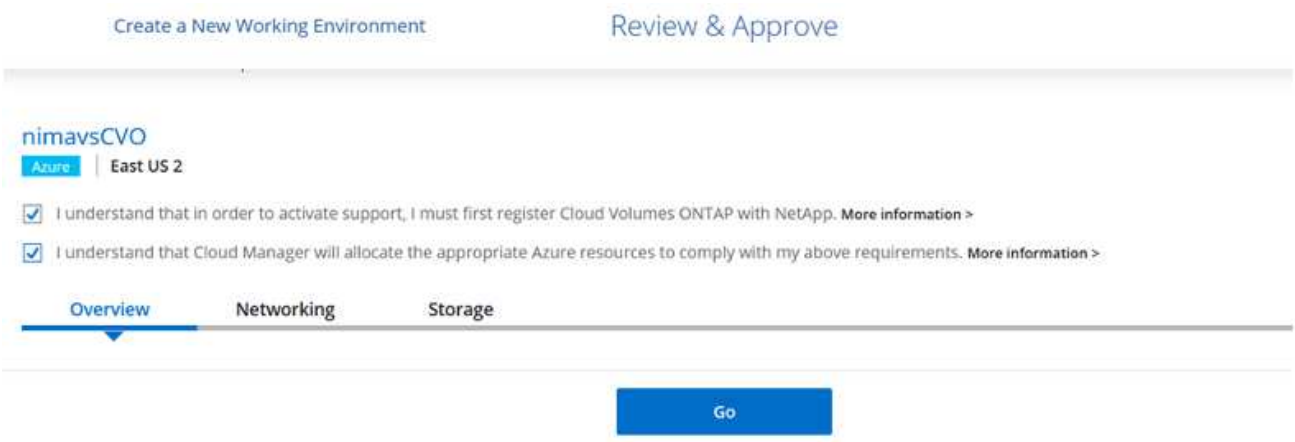
8. 选择许可证选项：按使用量付费或使用现有许可证的 BYOL。在此示例中，使用了按使用量付费选项。



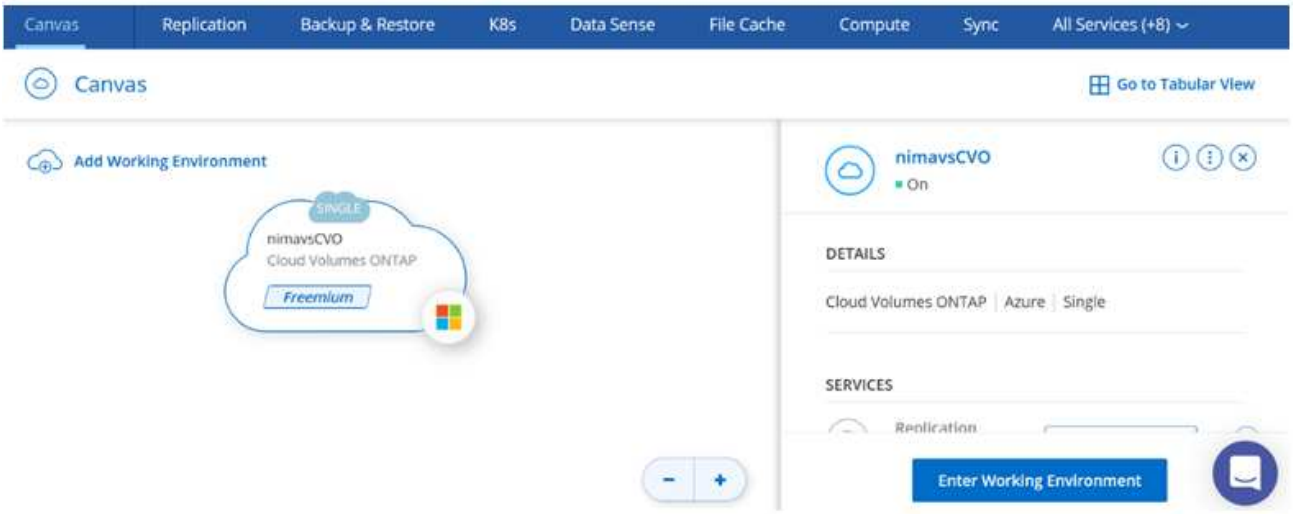
9. 在适用于各种类型工作负载的几个预配置包中进行选择。



10. 接受有关激活支持和分配 Azure 资源的两个协议。要创建Cloud Volumes ONTAP实例，请单击“Go”。

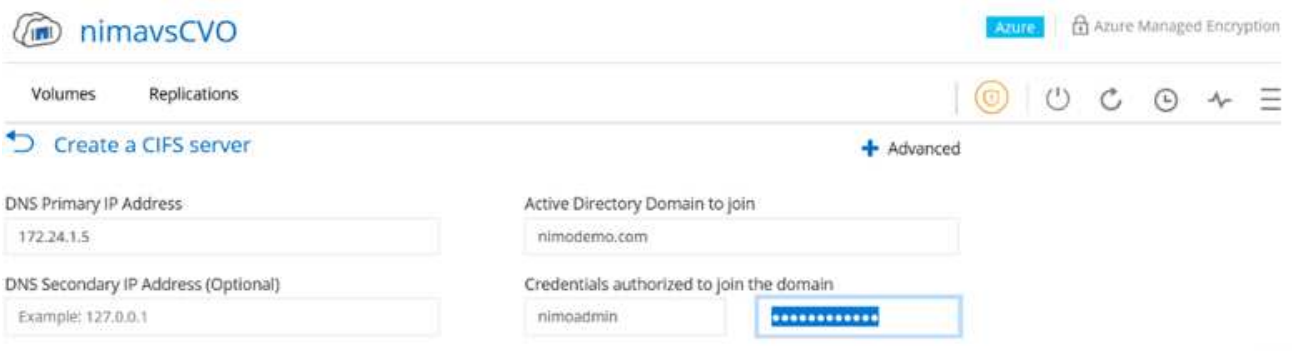


11. 配置Cloud Volumes ONTAP后，它会列在 Canvas 页面上的工作环境中。

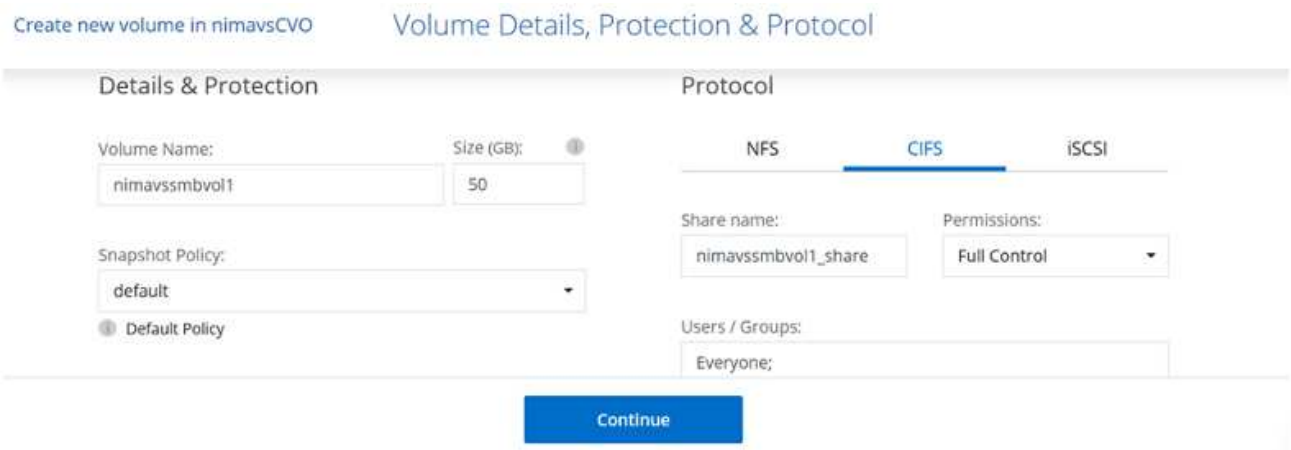


▼ **SMB** 卷的附加配置

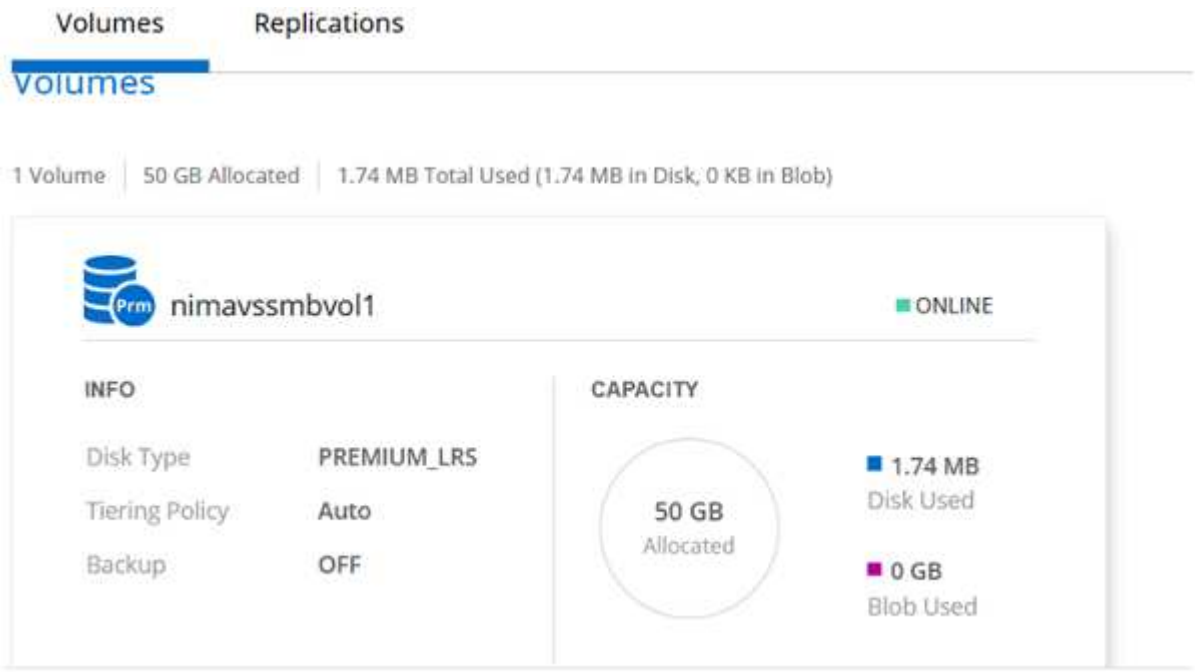
1. 工作环境准备好后，请确保 CIFS 服务器配置了适当的 DNS 和 Active Directory 配置参数。在创建 SMB 卷之前，需要执行此步骤。



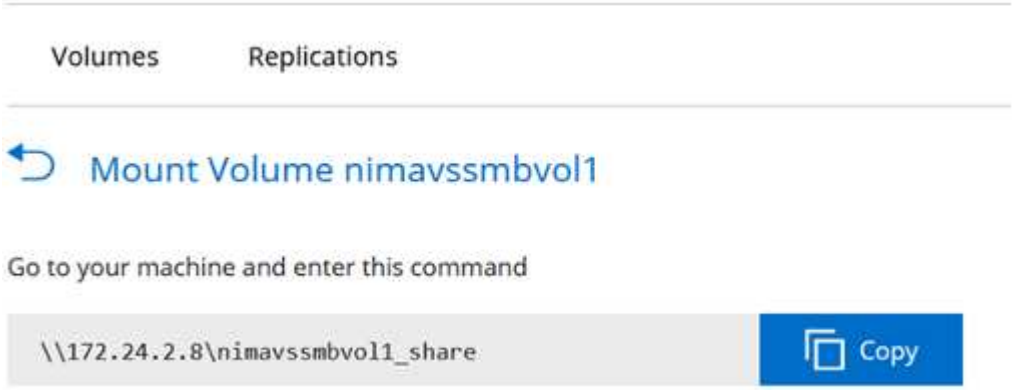
2. 创建 SMB 卷是一个简单的过程。选择要创建卷的 CVO 实例，然后单击“创建卷”选项。选择适当的大小，云管理器选择包含的聚合或使用高级分配机制放置在特定的聚合上。对于此演示，选择 SMB 作为协议。

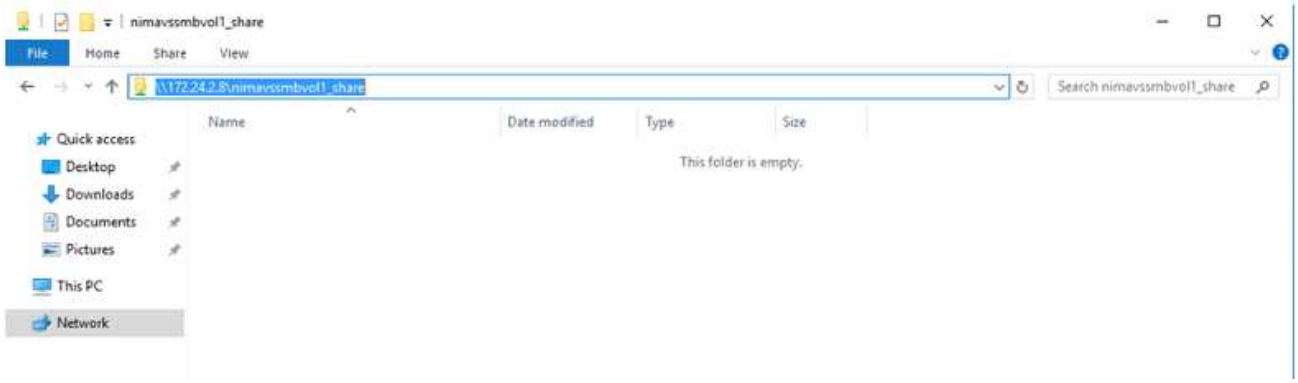


3. 卷配置完成后，它将在“卷”窗格下可用。由于已配置 CIFS 共享，请授予您的用户或组对文件和文件夹的权限，并验证这些用户是否可以访问共享并创建文件。如果从本地环境复制卷，则不需要此步骤，因为文件和文件夹权限都将作为SnapMirror复制的一部分保留。



4. 创建卷后，使用 mount 命令从 Azure VMware 解决方案 SDDC 主机上运行的 VM 连接到共享。
5. 复制以下路径并使用映射网络驱动器选项将卷装载到在 Azure VMware 解决方案 SDDC 上运行的 VM 上。

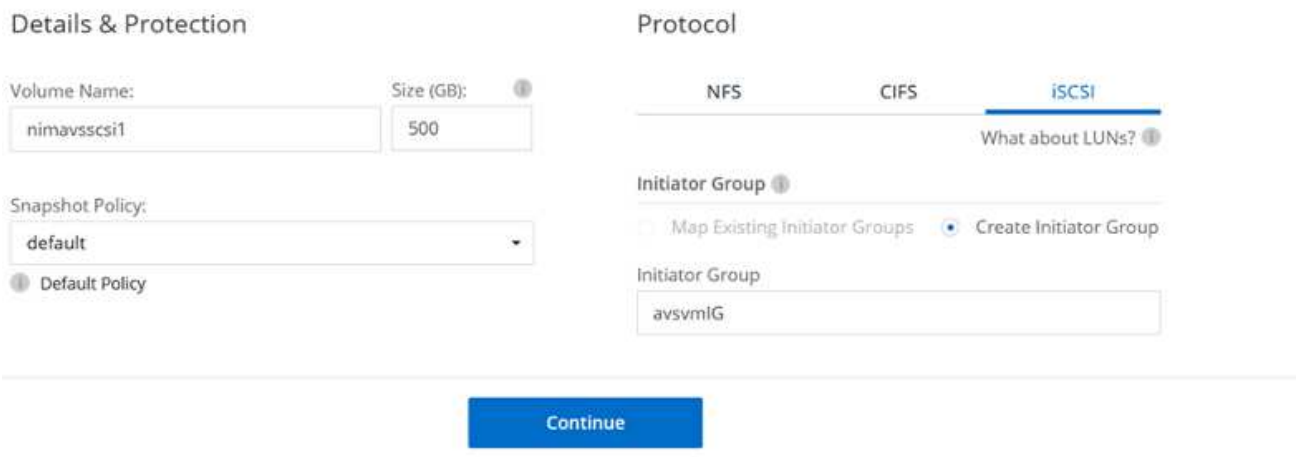




▼ 将 **LUN** 连接到主机

要将 LUN 连接到主机，请完成以下步骤：

1. 在“画布”页面上，双击Cloud Volumes ONTAP工作环境以创建和管理卷。
2. 单击添加卷 > 新卷并选择 iSCSI，然后单击创建启动器组。单击“Continue”。



3. 配置卷后，选择该卷，然后单击目标 IQN。要复制 iSCSI 限定名称 (IQN)，请单击复制。建立从主机到 LUN 的 iSCSI 连接。

   要对驻留在 Azure VMware 解决方案 SDDC 上的主机完成相同操作，请执行以下操作：

   a. 通过 RDP 连接到 Azure VMware 解决方案 SDDC 上托管的 VM。

b. 打开 iSCSI 发起程序属性对话框：服务器管理器 > 仪表板 > 工具 > iSCSI 发起程序。

c. 在“发现”选项卡中，单击“发现门户”或“添加门户”，然后输入 iSCSI 目标端口的 IP 地址。

d. 从“目标”选项卡中，选择发现的目标，然后单击“登录”或“连接”。

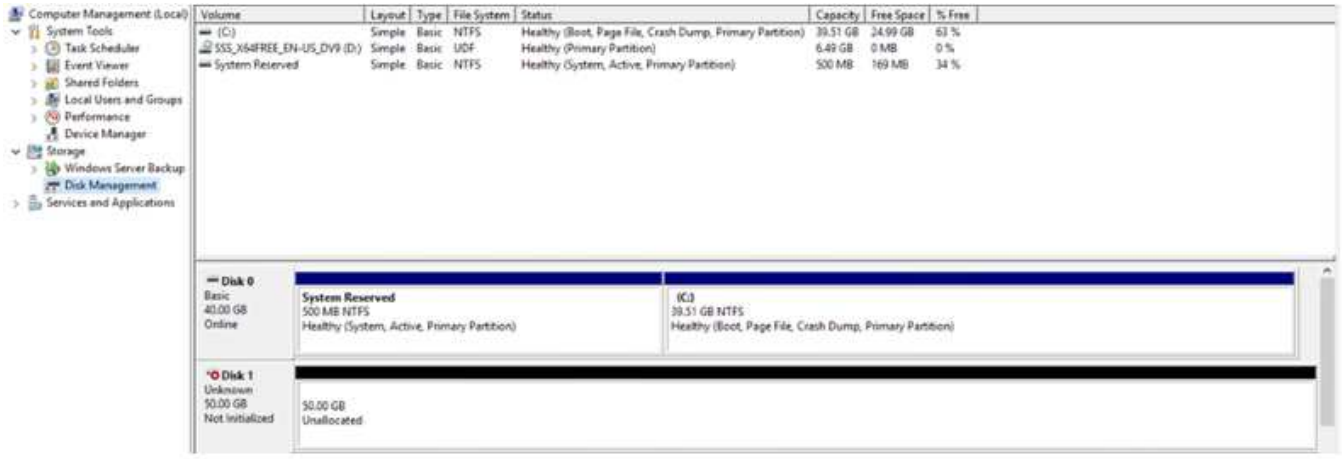
e. 选择启用多路径，然后选择计算机启动时自动恢复此连接或将此连接添加到收藏目标列表。单击“高级”。

*注意：*Windows 主机必须与集群中的每个节点建立 iSCSI 连接。本机 DSM 选择要使用的最佳路径。



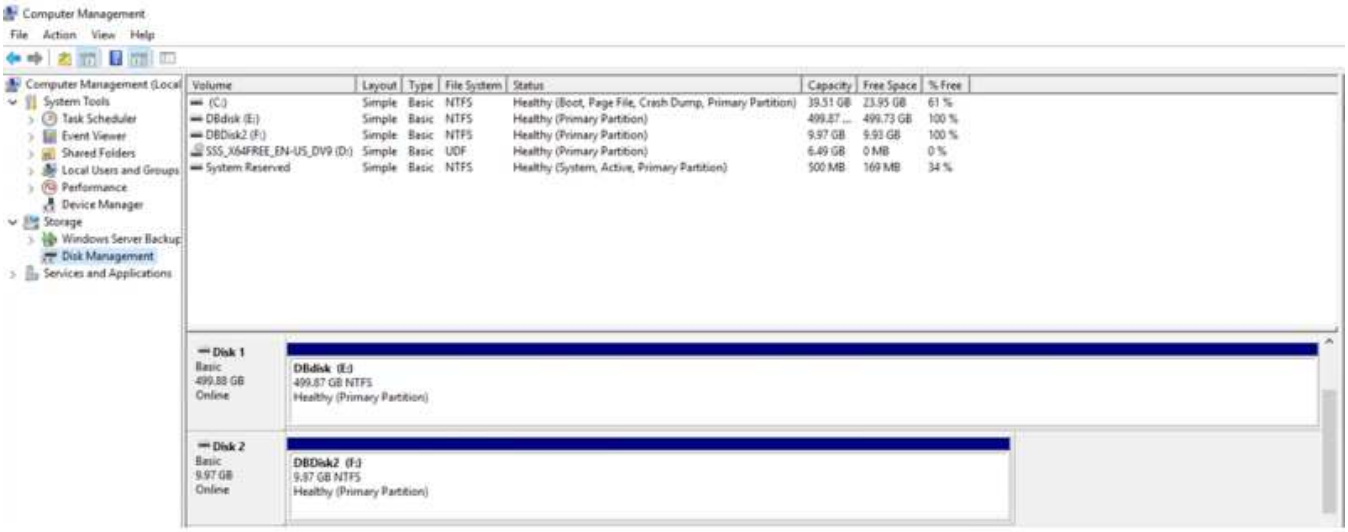
存储虚拟机 (SVM) 上的 LUN 对于 Windows 主机来说显示为磁盘。主机不会自动发现任何新添加的磁盘。通过完成以下步骤触发手动重新扫描以发现磁盘：

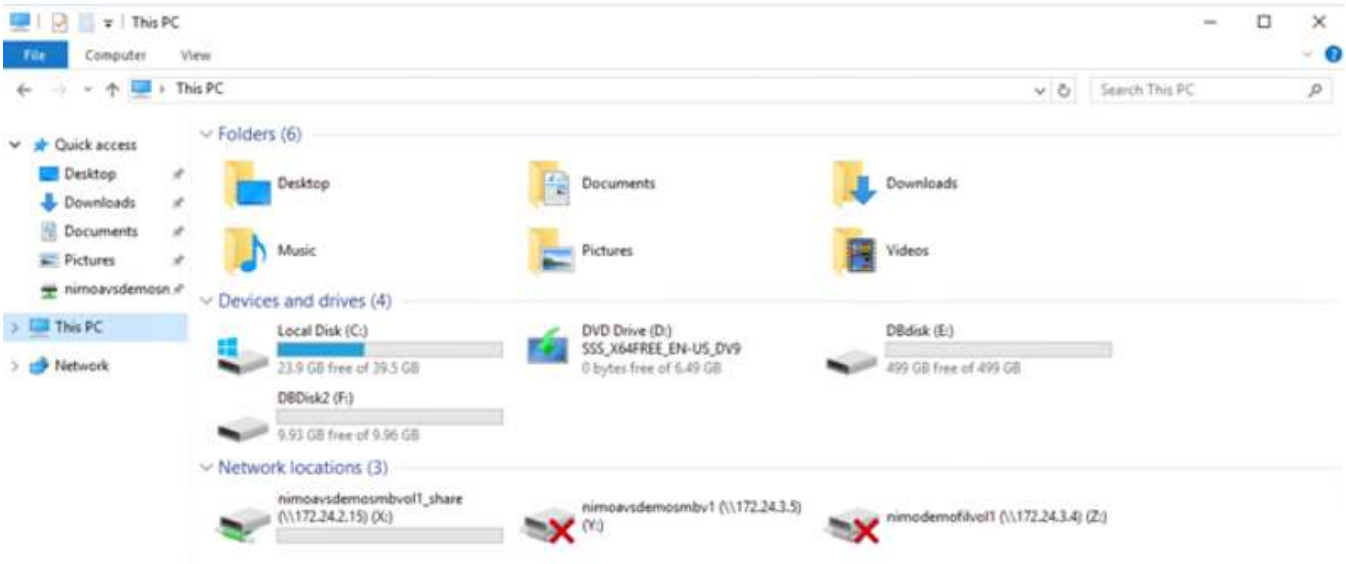
1. 打开 Windows 计算机管理实用程序：开始 > 管理工具 > 计算机管理。
2. 在导航树中展开存储节点。
3. 单击“磁盘管理”。
4. 单击操作 > 重新扫描磁盘。



当 Windows 主机首次访问新的 LUN 时，它没有分区或文件系统。初始化 LUN；并且（可选）通过完成以下步骤使用文件系统格式化 LUN：

1. 启动 Windows 磁盘管理。
2. 右键单击 LUN，然后选择所需的磁盘或分区类型。
3. 按照向导中的说明进行操作。在此示例中，已安装驱动器 E:





Google Cloud VMware Engine：使用**NetApp**存储的选项

NetApp存储可以作为来宾连接存储或补充存储附加到 Google Cloud Virtualization Engine。

Google Cloud NetApp Volumes （NetApp Volumes）作为补充 NFS 数据存储区

需要在 Google Cloud VMware Engine (GCVE) 环境中增加存储容量的客户可以利用Google Cloud NetApp Volumes作为补充 NFS 数据存储进行挂载。将数据存储在Google Cloud NetApp Volumes上允许客户在区域之间进行复制以防止灾难。

欲了解更多信息，请访问"Google Cloud NetApp Volumes （NetApp Volumes）作为补充 NFS 数据存储区"

NetApp CVO 作为客户连接存储

Cloud Volumes ONTAP（或称 CVO）是基于 NetApp 的ONTAP存储软件构建的业界领先的云数据管理解决方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的软件定义版本，使用云原生存储，允许您在云端和本地使用相同的存储软件，从而无需重新培训 IT 人员采用全新方法来管理数据。

CVO 使客户能够无缝地将数据从边缘移动到数据中心、云端并返回，从而将您的混合云整合在一起 - 所有这些都通过单一窗格管理控制台NetApp Cloud Manager 进行管理。

通过设计，CVO 可提供极高的性能和先进的数据管理功能，以满足您在云中最苛刻的应用程序的需求。

欲了解更多信息，请访问"NetApp CVO 作为客户连接存储"

Google Cloud NetApp Volumes （NetApp Volumes）作为来宾连接存储

可以从在 VMware Engine 环境中创建的虚拟机挂载Google Cloud NetApp Volumes共享。由于Google Cloud NetApp Volumes支持 SMB 和 NFS 协议，因此这些卷也可以安装在 Linux 客户端上并映射到 Windows 客户端上。可以通过简单的步骤来设置Google Cloud NetApp Volumes卷。

Google Cloud NetApp Volumes和 Google Cloud VMware Engine 私有云必须位于同一区域。

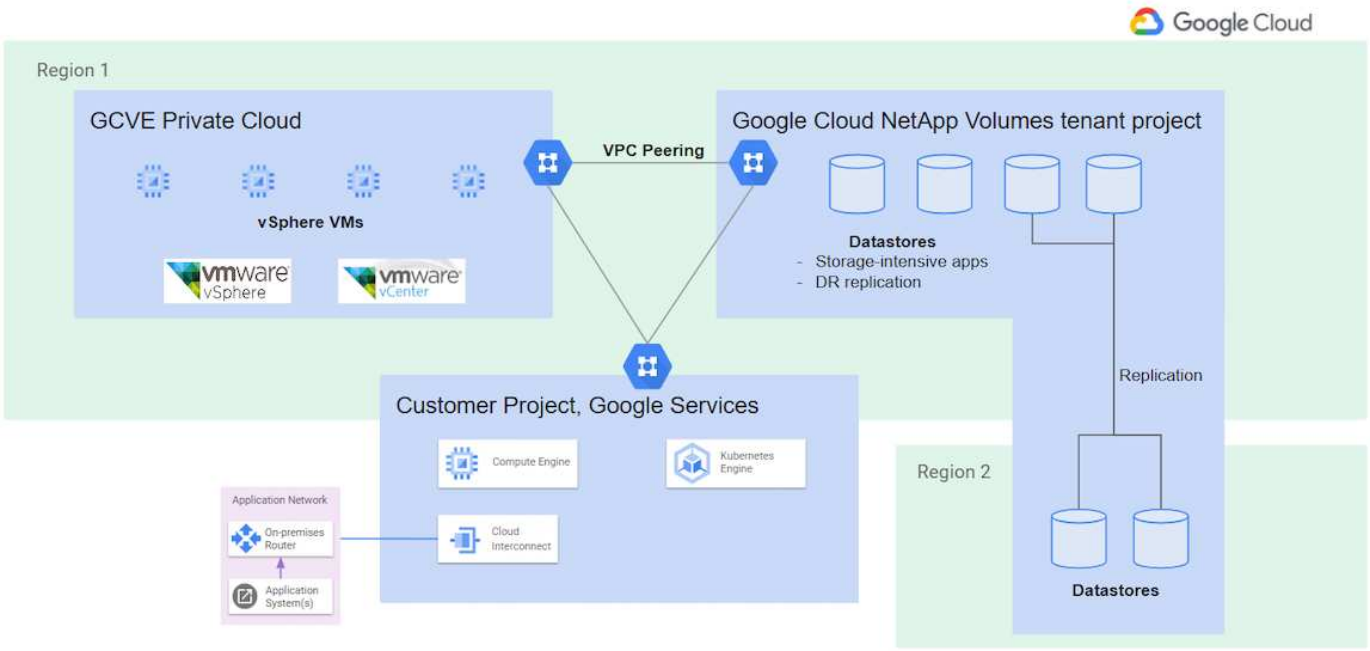
欲了解更多信息，请访问"Google Cloud NetApp Volumes （NetApp Volumes）作为来宾连接存储"

Google Cloud VMware Engine 补充 **NFS** 数据存储与**Google Cloud NetApp Volumes**

客户可以使用 NFS 补充数据存储和Google Cloud NetApp Volumes扩展 Google Cloud VMware Engine 上的存储容量。

概述

需要在 Google Cloud VMware Engine (GCVE) 环境上增加存储容量的客户可以利用 Netapp Cloud Volume Service 作为补充 NFS 数据存储进行安装。将数据存储在Google Cloud NetApp Volumes上允许客户在区域之间进行复制以防止灾难。



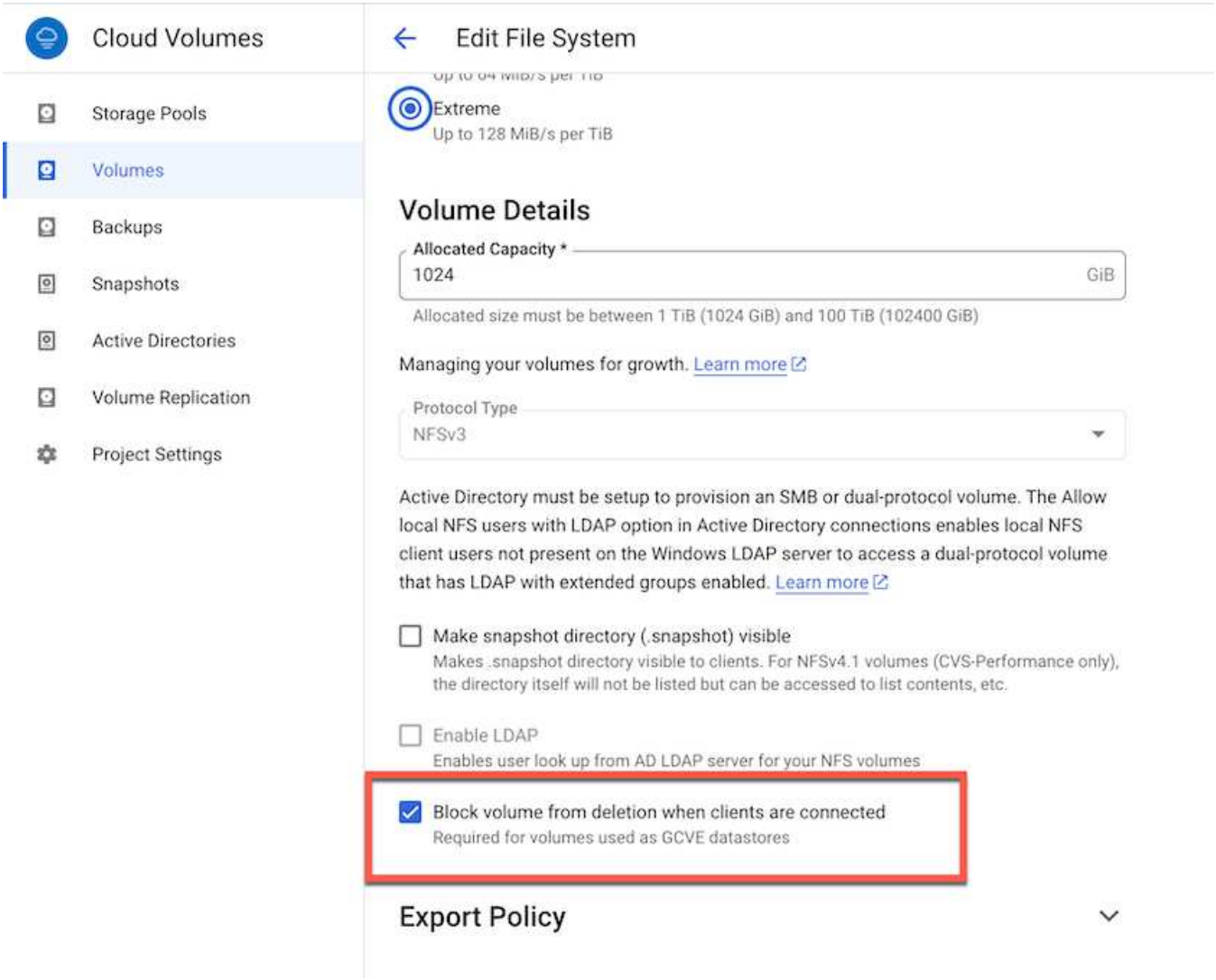
在 **GCVE** 上从**Google Cloud NetApp Volumes (NetApp Volumes)** 挂载 **NFS** 数据存储区的部署步骤

▼ 配置**NetApp**卷 - 性能卷

Google Cloud NetApp Volumes 卷可以通过以下方式配置："使用 Google Cloud Console" "使用 Google Cloud CLI 或 API"

▼ 将**NetApp Volumes** 卷标记为不可删除

为避免在 VM 运行时意外删除卷，请确保将卷标记为不可删除，如下面的屏幕截图所示。



如需了解更多信息，请参阅 "创建 NFS 卷" 文档。

▼ 确保**NetApp Volumes Tenant VPC** 的 **GCVE** 上存在专用连接。

要挂载 NFS 数据存储区，GCVE 和NetApp Volumes 项目之间应该存在私有连接。欲了解更多信息，请参阅"如何设置私人服务访问"

▼ 挂载 **NFS** 数据存储

有关如何在 GCVE 上挂载 NFS 数据存储的说明，请参阅"如何使用NetApp卷创建 NFS 数据存储"

由于 vSphere 主机由 Google 管理，因此您无权安装 NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB)。如果您需要虚拟卷 (vVol) 支持，请告知我们。如果您想使用巨型帧，请参阅"GCP 上支持的最大 MTU 大小"

使用**Google Cloud NetApp Volumes**节省成本

要详细了解使用 Google Cloud NetApp Volumes 可为您在 GCVE 上的存储需求节省的金额，请查看 "NetApp投资回报率计算器"

参考链接

- "Google 博客 - 如何使用NetApp Volumes 作为 Google Cloud VMware Engine 的数据存储区"

- "NetApp博客 - 将存储丰富的应用程序迁移到 Google Cloud 的更好方法"

适用于 **GCP** 的**NetApp**存储选项

GCP 支持通过Cloud Volumes ONTAP (CVO) 或Google Cloud NetApp Volumes (NetApp Volumes) 连接来宾的NetApp存储。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP（或称 CVO）是基于 NetApp 的ONTAP存储软件构建的业界领先的云数据管理解决方案，可在 Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud Platform (GCP) 上原生使用。

它是ONTAP的软件定义版本，使用云原生存储，允许您在云端和本地使用相同的存储软件，从而无需重新培训 IT 人员采用全新方法来管理数据。

CVO 使客户能够无缝地将数据从边缘移动到数据中心、云端并返回，从而将您的混合云整合在一起 - 所有这些都通过单一窗格管理控制台NetApp Cloud Manager 进行管理。

CVO 的设计旨在提供极致的性能和先进的数据管理功能，以满足您在云端最苛刻的应用程序

Cloud Volumes ONTAP (CVO) 作为来宾连接存储

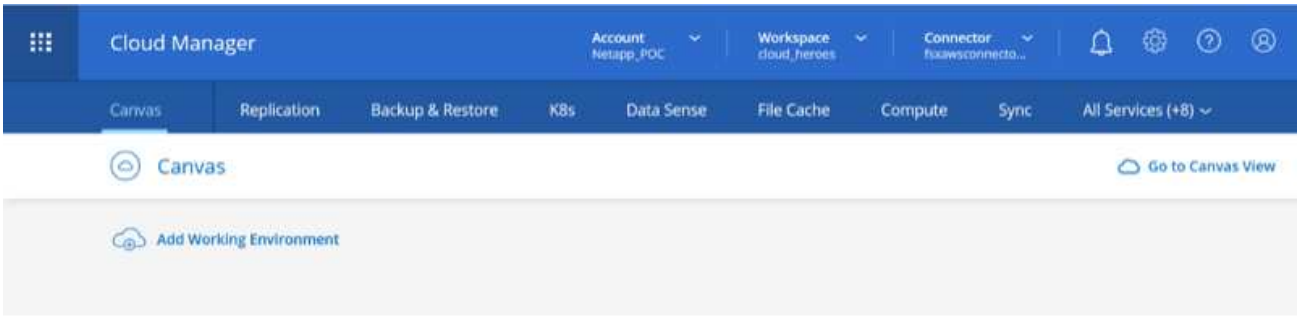
▼ 在 **Google Cloud** 中部署**Cloud Volumes ONTAP** （自行部署）

可以从在 GCVE 私有云环境中创建的虚拟机挂载Cloud Volumes ONTAP共享和 LUN。这些卷还可以安装在 Linux 客户端和 Windows 客户端上，并且当通过 iSCSI 安装时，可以在 Linux 或 Windows 客户端上将 LUNS 作为块设备进行访问，因为Cloud Volumes ONTAP支持 iSCSI、SMB 和 NFS 协议。只需几个简单的步骤即可设置Cloud Volumes ONTAP卷。

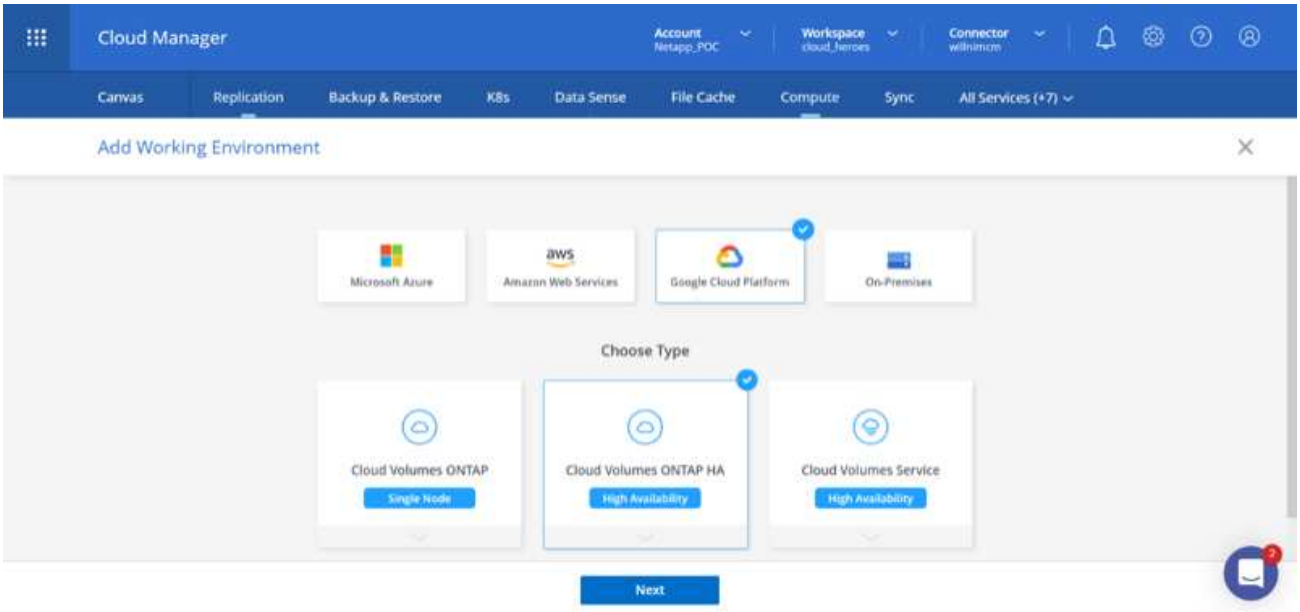
要将卷从本地环境复制到云端以用于灾难恢复或迁移，请使用站点到站点 VPN 或 Cloud Interconnect 建立与 Google Cloud 的网络连接。将数据从本地复制到Cloud Volumes ONTAP超出了本文档的范围。要在本地和Cloud Volumes ONTAP系统之间复制数据，请参阅"设置系统之间的数据复制"。

使用 "Cloud Volumes ONTAP大小调整器" 准确调整 Cloud Volumes ONTAP 实例的大小。此外，还应监控本地性能，以用作 Cloud Volumes ONTAP sizer 中的输入。

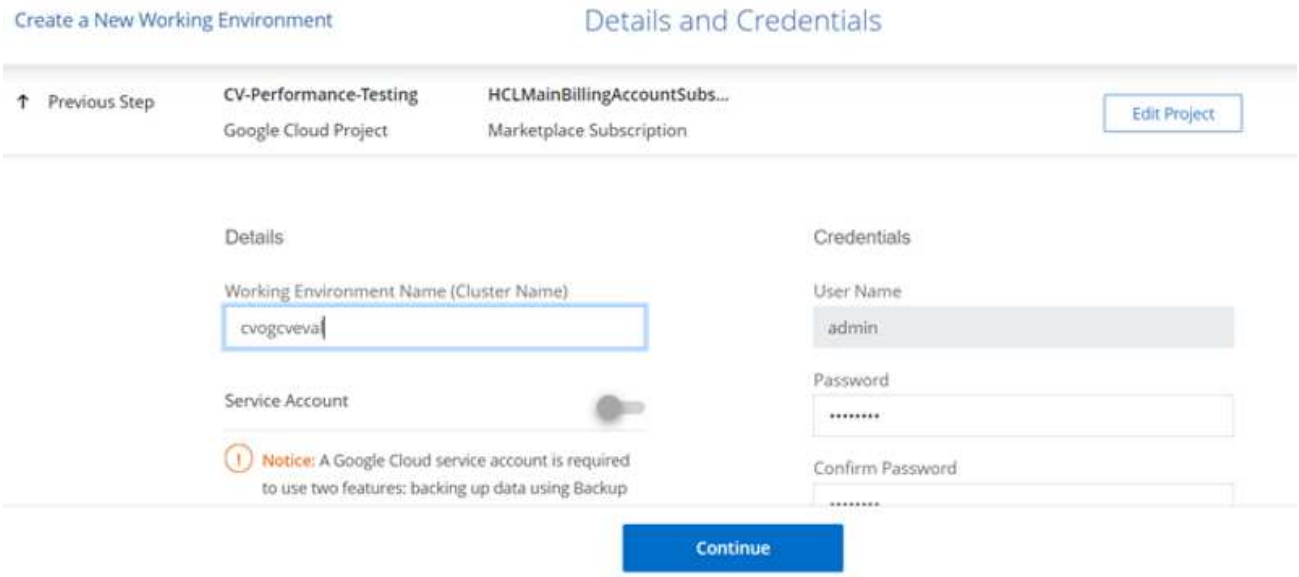
1. 登录NetApp Cloud Central — 显示 Fabric View 屏幕。找到Cloud Volumes ONTAP选项卡并选择转到云管理器。登录后，将显示 Canvas 屏幕。



2. 在 Cloud Manager Canvas 选项卡上，单击添加工作环境，然后选择 Google Cloud Platform 作为云和系统配置类型。然后单击“下一步”。

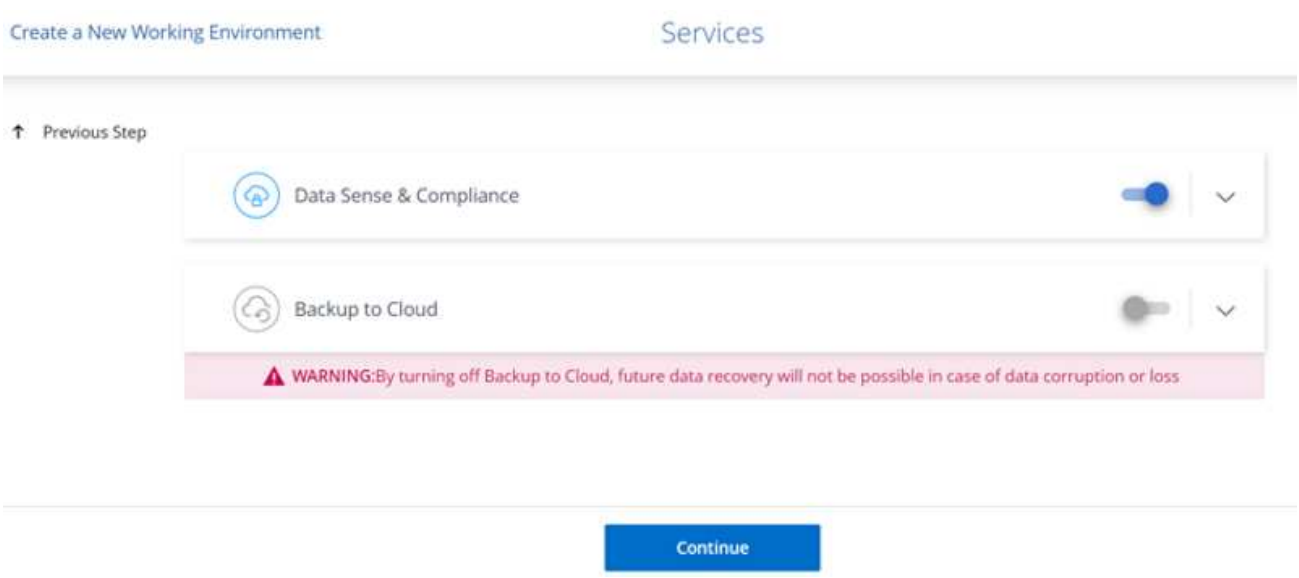


3. 提供要创建的环境的详细信息，包括环境名称和管理员凭据。完成后，单击“继续”。

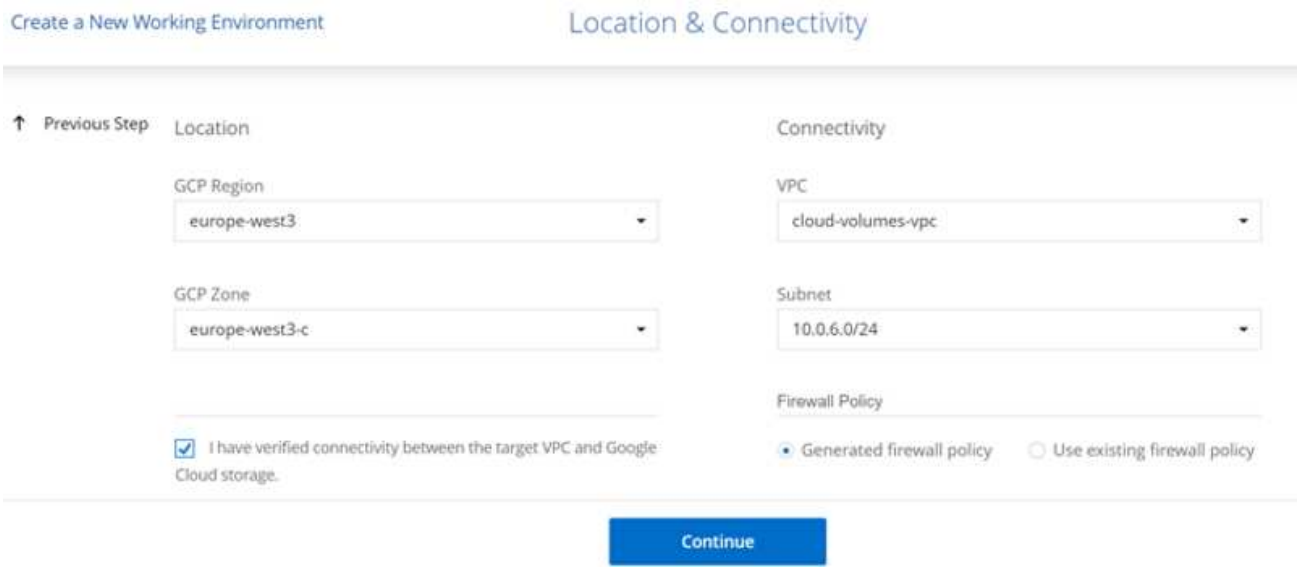


4. 选择或取消选择Cloud Volumes ONTAP部署的附加服务，包括数据感知与合规性或备份到云。然后，单击“继续”。

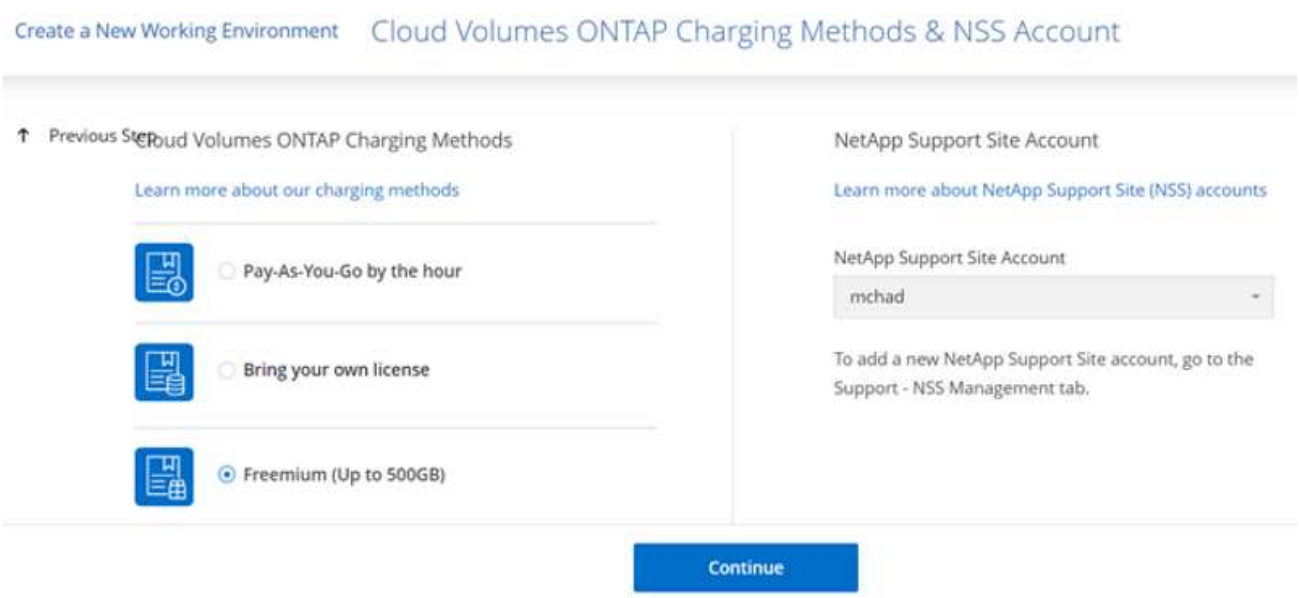
   提示：停用附加服务时将显示验证弹出消息。 CVO 部署后可以添加/删除附加服务，如果从一开始就不需要，请考虑取消选择它们以避免成本。



5. 选择一个位置，选择防火墙策略，然后选中复选框以确认与 Google Cloud 存储的网络连接。

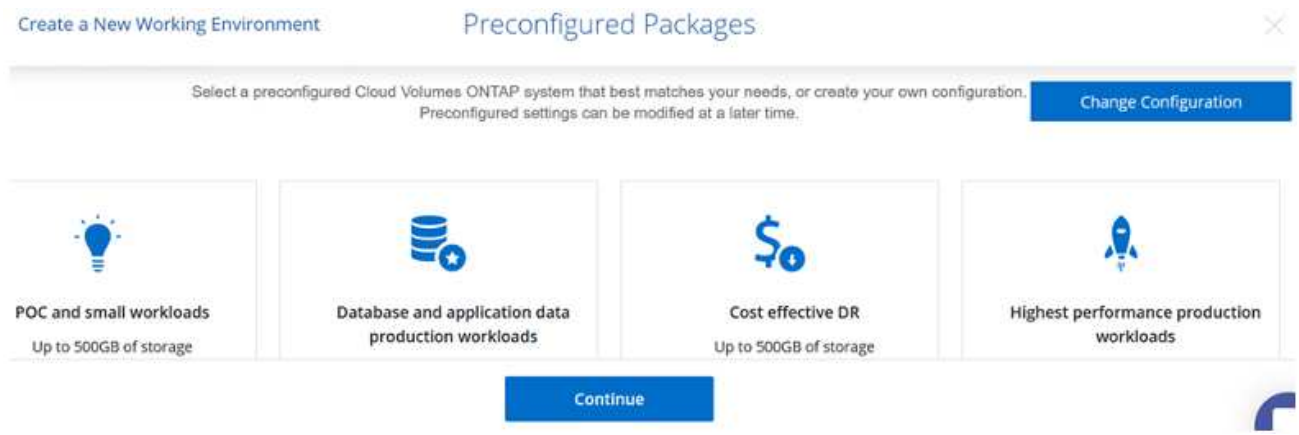


6. 选择许可证选项：按使用量付费或使用现有许可证的 BYOL。在此示例中，使用了免费增值选项。然后，点击继续。

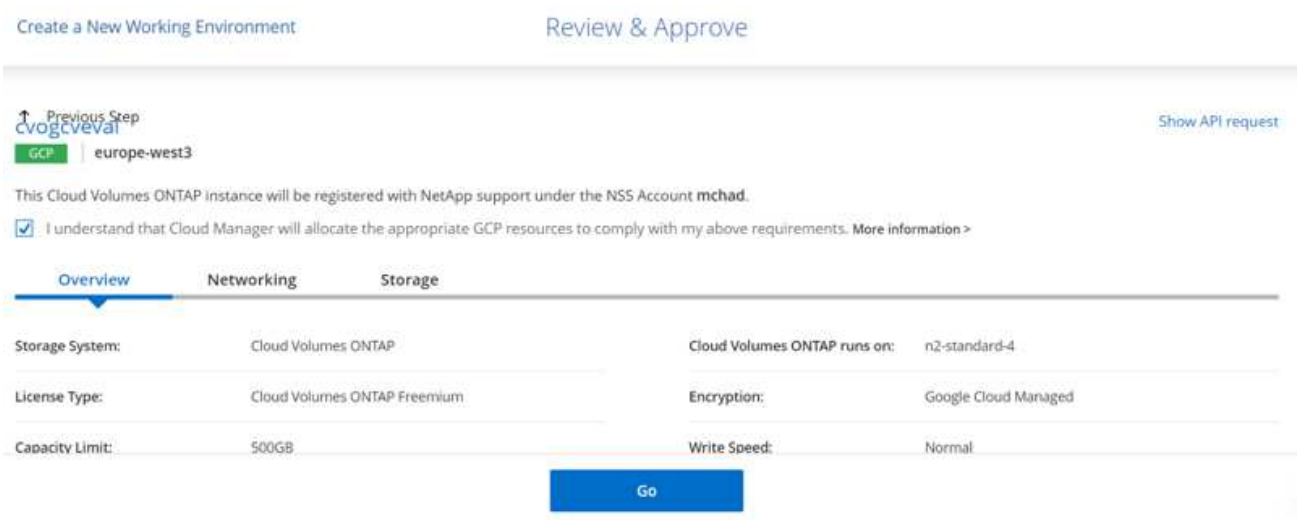


7. 根据将在 AWS SDDC 上的 VMware 云上运行的虚拟机上部署的工作负载类型，在几个可用的预配置包中进行选择。

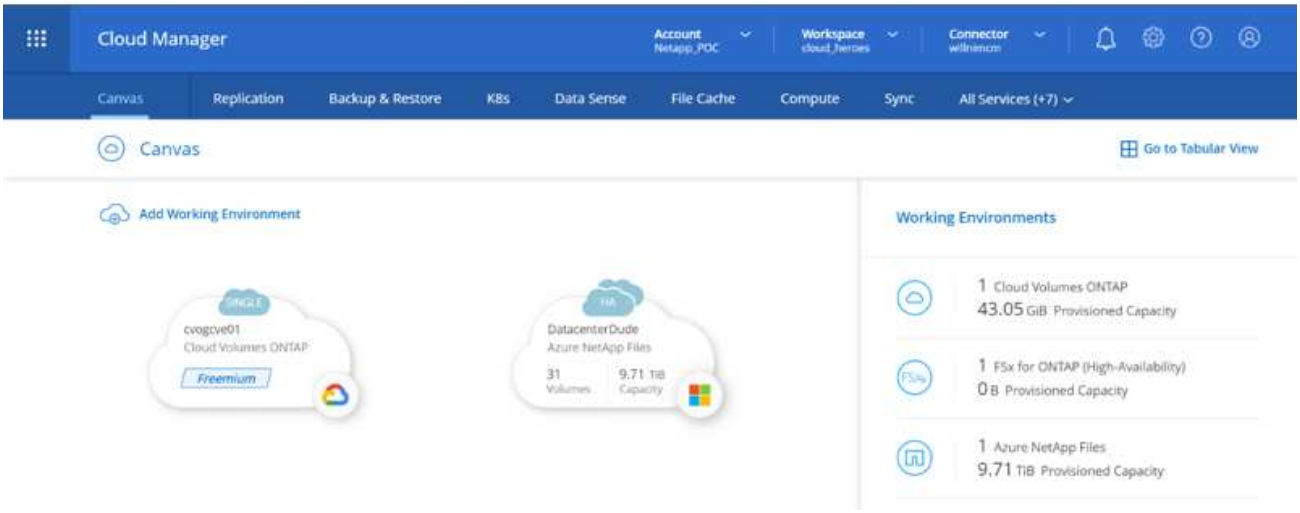
   提示：将鼠标悬停在图块上以查看详细信息，或单击“更改配置”自定义 CVO 组件和ONTAP版本。



8. 在“审核并批准”页面上，审核并确认选择。要创建Cloud Volumes ONTAP实例，请单击“开始”。



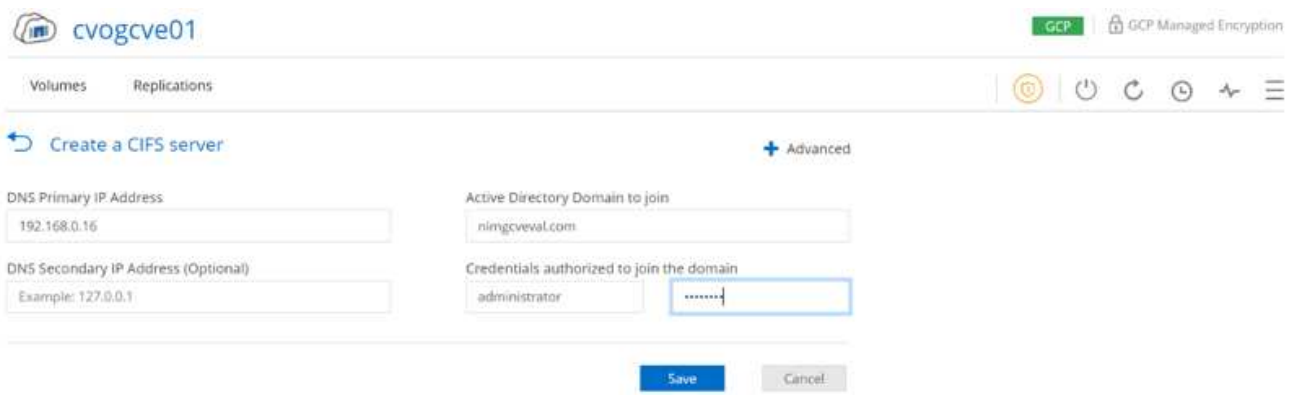
9. 配置Cloud Volumes ONTAP后，它会列在 Canvas 页面上的工作环境中。



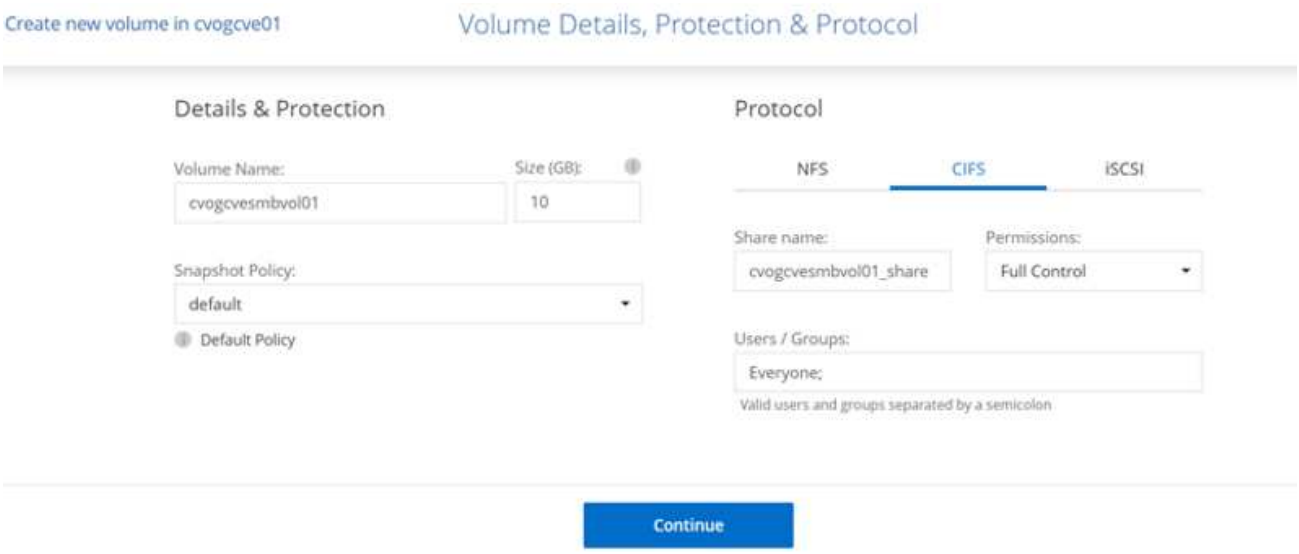
▼ **SMB** 卷的附加配置

1. 工作环境准备好后，请确保 CIFS 服务器配置了适当的 DNS 和 Active Directory 配置参数。在创建 SMB 卷之前，需要执行此步骤。

   提示：单击菜单图标 (º)，选择高级以显示更多选项并选择 CIFS 设置。



2. 创建 SMB 卷是一个简单的过程。在 Canvas 中，双击Cloud Volumes ONTAP工作环境来创建和管理卷，然后单击创建卷选项。选择适当的大小，云管理器选择包含的聚合或使用高级分配机制放置在特定的聚合上。对于此演示，选择 CIFS/SMB 作为协议。



3. 卷配置完成后，它将在“卷”窗格下可用。由于已配置 CIFS 共享，请授予您的用户或组对文件和文件夹的权限，并验证这些用户是否可以访问共享并创建文件。如果从本地环境复制卷，则不需要此步骤，因为文件和文件夹权限都将作为SnapMirror复制的一部分保留。

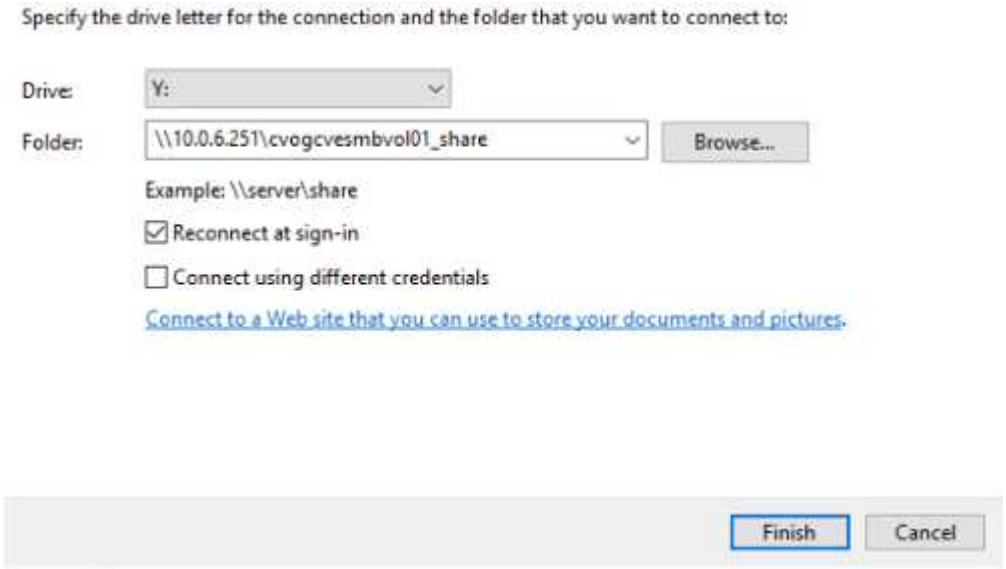
   提示：单击音量菜单 (⁰) 以显示其选项。



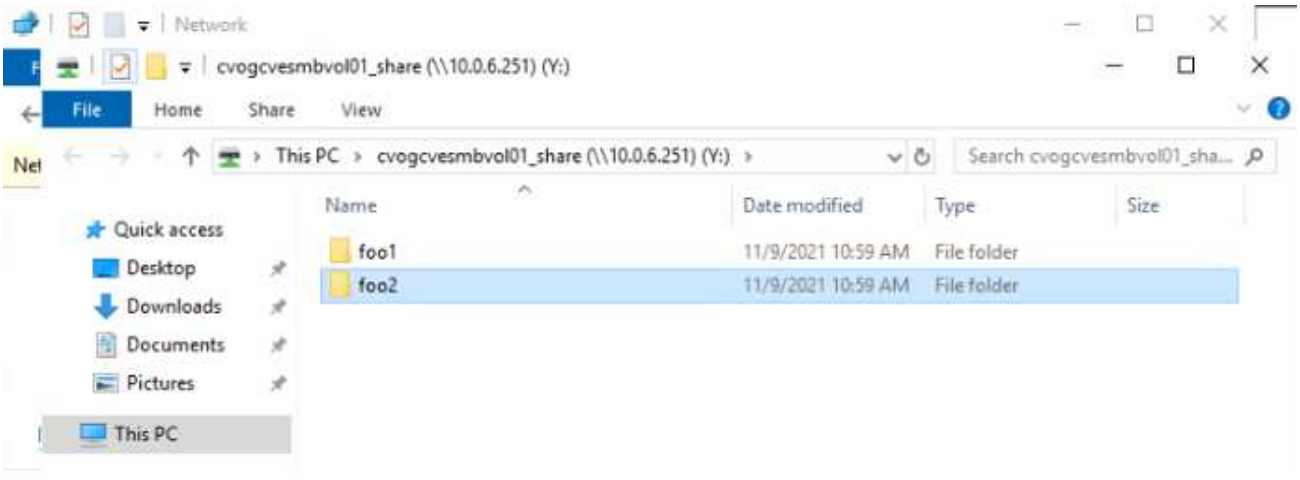
4. 创建卷后，使用 mount 命令显示卷连接说明，然后从 Google Cloud VMware Engine 上的虚拟机连接到共享。



5. 复制以下路径并使用映射网络驱动器选项将卷挂载到在 Google Cloud VMware Engine 上运行的虚拟机上。



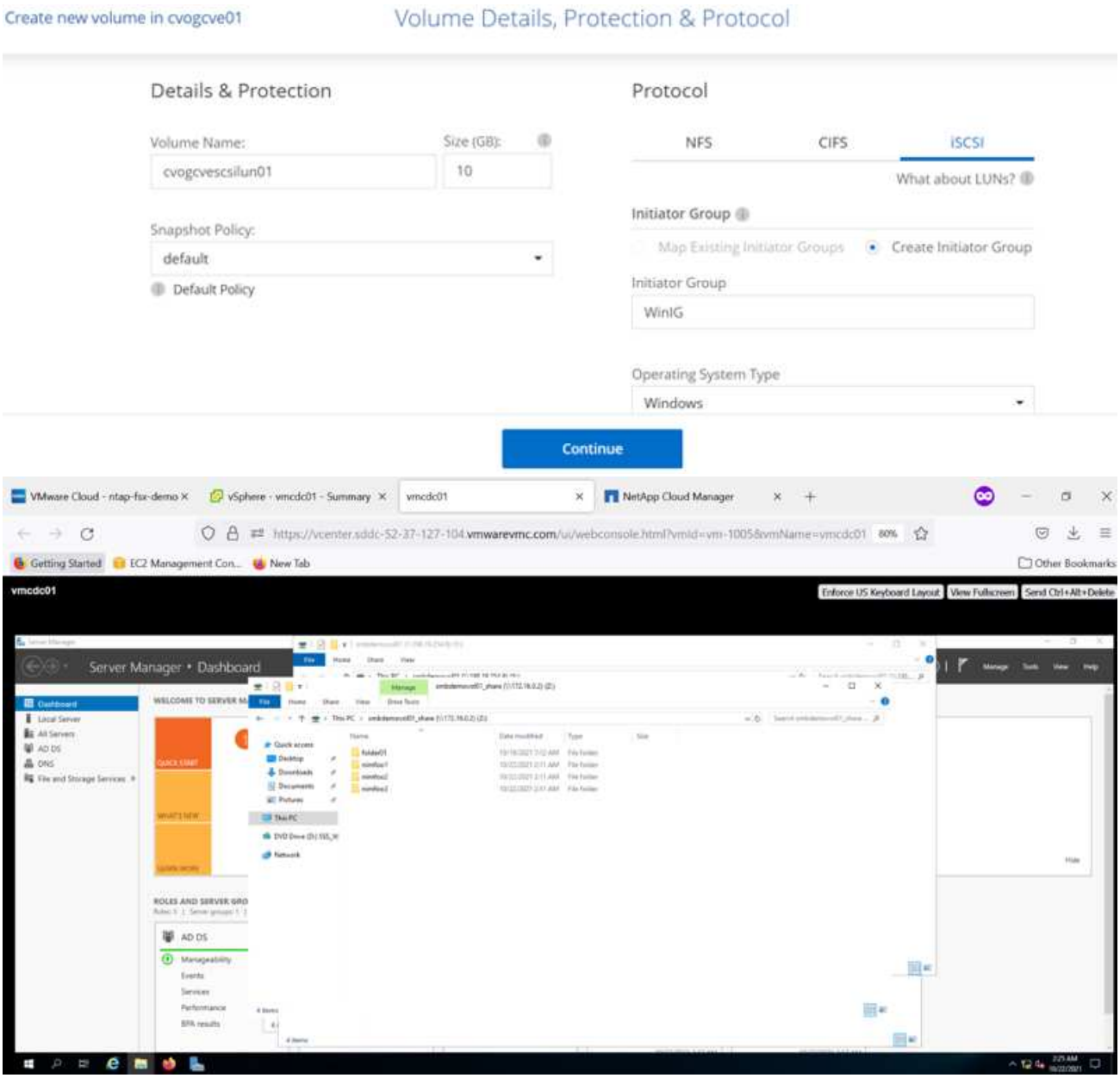
一旦映射，就可以轻松访问，并且可以相应地设置 NTFS 权限。



▼ **Cloud Volumes ONTAP**上的 **LUN** 连接到主机

要将云卷ONTAP LUN 连接到主机，请完成以下步骤：

1. 在“画布”页面上，双击Cloud Volumes ONTAP工作环境以创建和管理卷。
2. 单击添加卷 > 新卷并选择 iSCSI，然后单击创建启动器组。单击“Continue”。



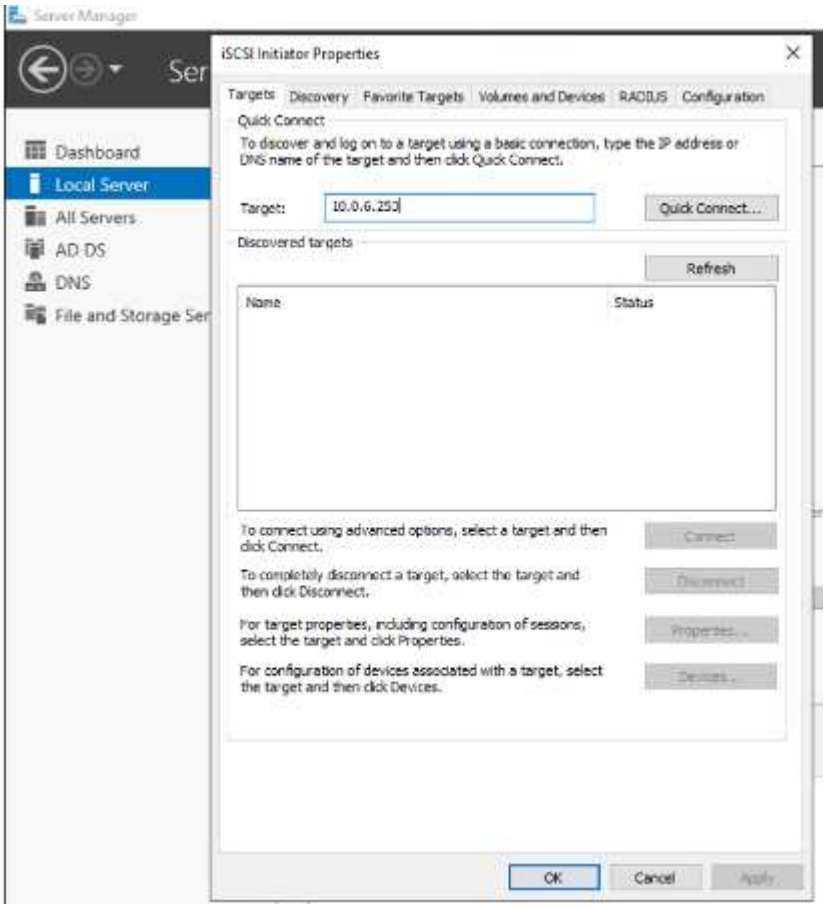
3. 配置卷后，选择卷菜单 (º)，然后单击目标 iQN。要复制 iSCSI 限定名称 (iQN)，请单击复制。建立从主机到 LUN 的 iSCSI 连接。

要对驻留在 Google Cloud VMware Engine 上的主机完成相同操作：

1. 通过 RDP 连接到托管在 Google Cloud VMware Engine 上的虚拟机。
2. 打开 iSCSI 发起程序属性对话框：服务器管理器 > 仪表板 > 工具 > iSCSI 发起程序。
3. 在“发现”选项卡中，单击“发现门户”或“添加门户”，然后输入 iSCSI 目标端口的 IP 地址。
4. 从“目标”选项卡中，选择发现的目标，然后单击“登录”或“连接”。

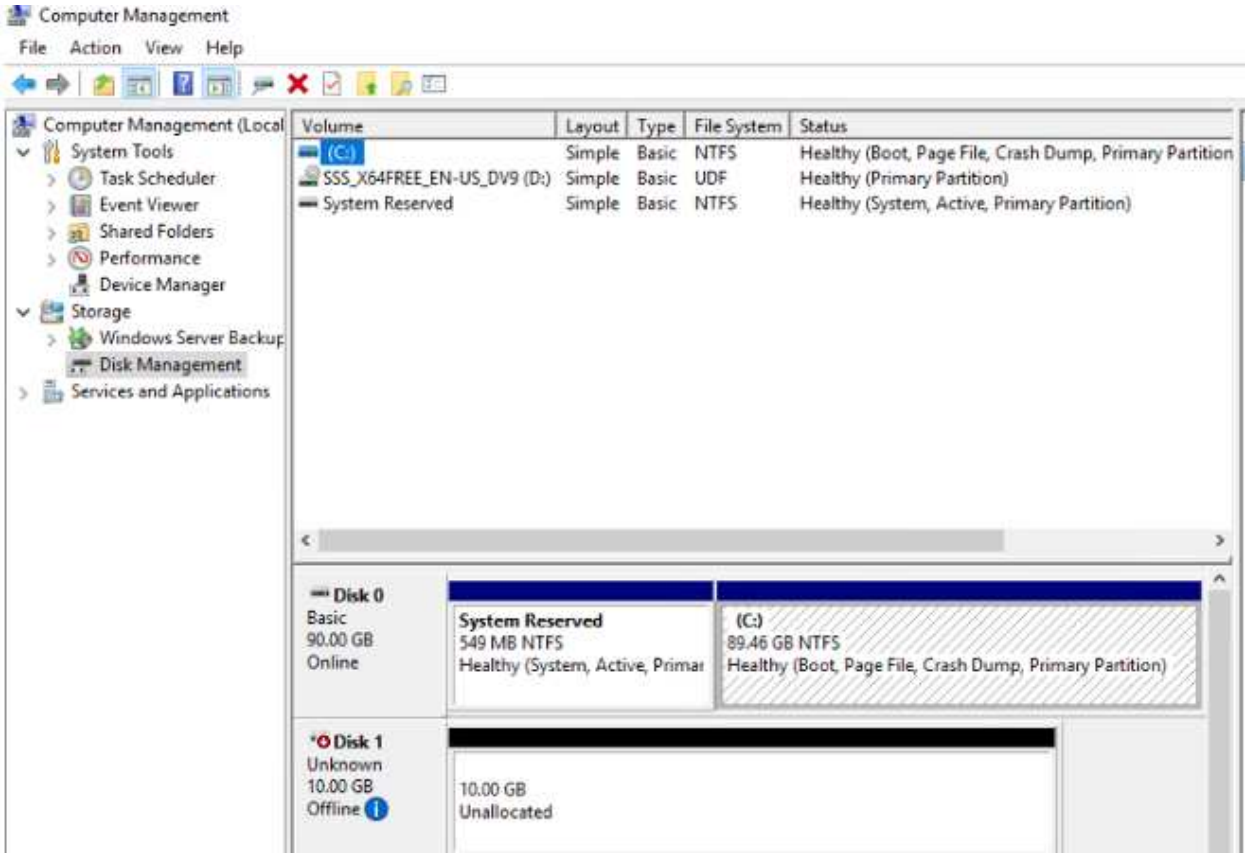
5. 选择启用多路径，然后选择计算机启动时自动恢复此连接或将此连接添加到收藏目标列表。单击“高级”。

> Windows 主机必须与群集中的每个节点建立 iSCSI 连接。本机 DSM 选择最佳路径以供使用。



存储虚拟机 (SVM) 上的 LUN 对于 Windows 主机来说显示为磁盘。主机不会自动发现任何新添加的磁盘。通过完成以下步骤触发手动重新扫描以发现磁盘：

a. 打开 Windows 计算机管理实用程序：开始 > 管理工具 > 计算机管理。
b. 在导航树中展开存储节点。
c. 单击“磁盘管理”。
d. 单击操作 > 重新扫描磁盘。

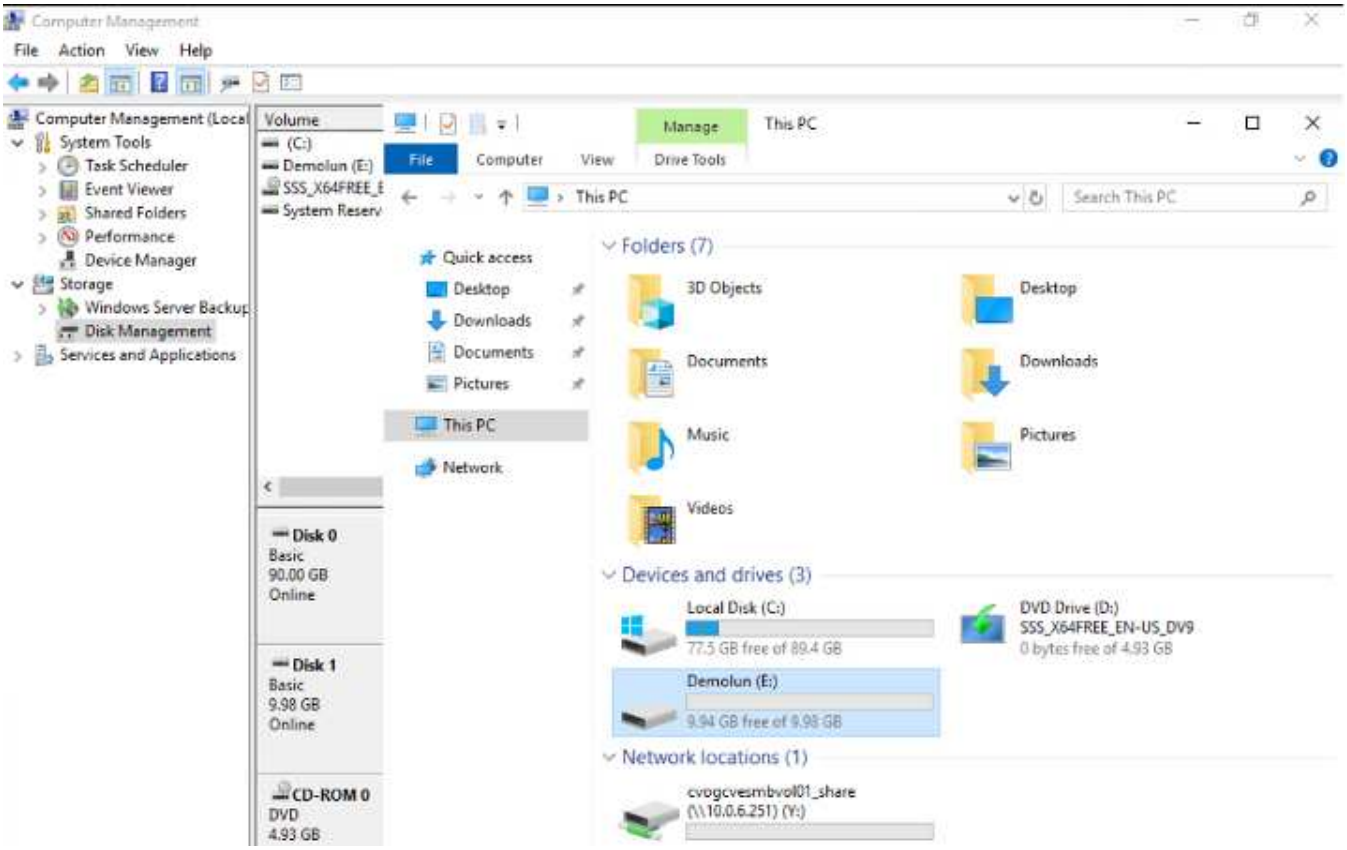


当 Windows 主机首次访问新的 LUN 时，它没有分区或文件系统。初始化 LUN；并且（可选）通过完成以下步骤使用文件系统格式化 LUN：

a. 启动 Windows 磁盘管理。

b. 右键单击 LUN，然后选择所需的磁盘或分区类型。

c. 按照向导中的说明进行操作。在此示例中，已安装驱动器 F:。



在 Linux 客户端上，确保 iSCSI 守护程序正在运行。配置 LUN 后，请参阅此处以 Ubuntu 为例的 iSCSI 配置详细指南。要验证，请从 shell 运行 lsblk cmd。

```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

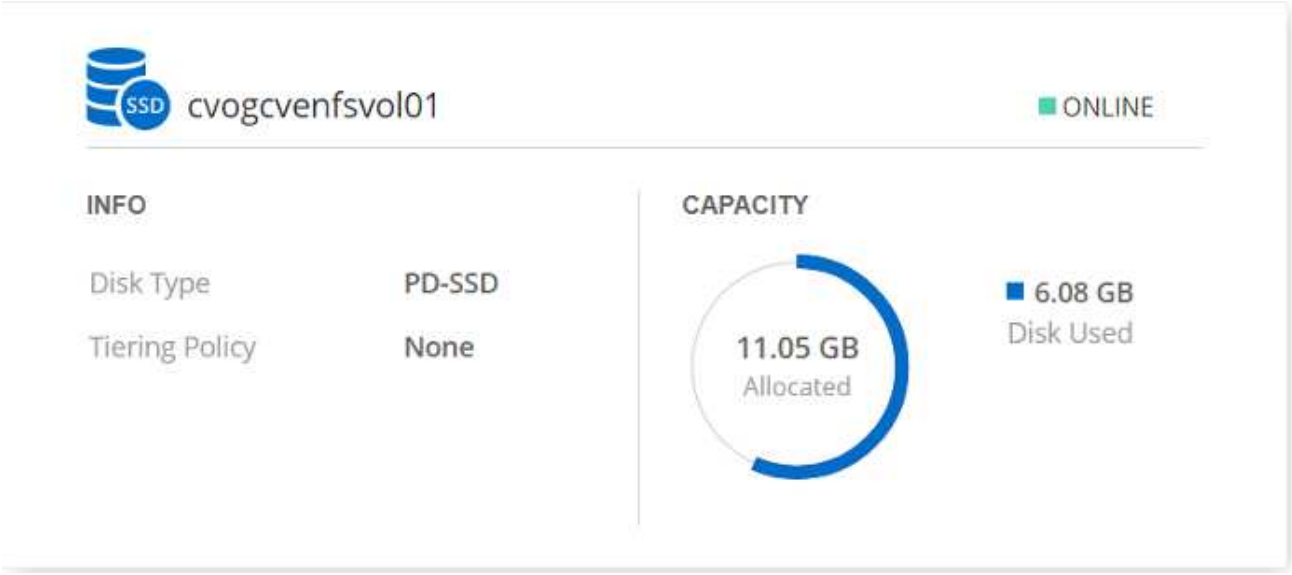
```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M     0 100% /snap/snap-store/547
/dev/loop0       56M   56M     0 100% /snap/core18/2128
/dev/loop4       33M   33M     0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M   1% /boot/efi
tmpfs           394M   64K  394M   1% /run/user/1000
/dev/loop5       33M   33M     0 100% /snap/snapd/13640
/dev/loop6       56M   56M     0 100% /snap/core18/2246
/dev/loop7      128K  128K     0 100% /snap/bare/5
/dev/loop8       66M   66M     0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M   1% /mnt
```

▼ 在 **Linux** 客户端上挂载**Cloud Volumes ONTAP NFS** 卷

要从 Google Cloud VMware Engine 中的虚拟机挂载Cloud Volumes ONTAP (DIY) 文件系统，请按照以下步骤操作：

按照以下步骤配置卷

1. 在卷选项卡中，单击创建新卷。
2. 在“创建新卷”页面上，选择卷类型：



3. 在“卷”选项卡中，将鼠标光标放在卷上，选择菜单图标 (º)，然后单击“挂载命令”。



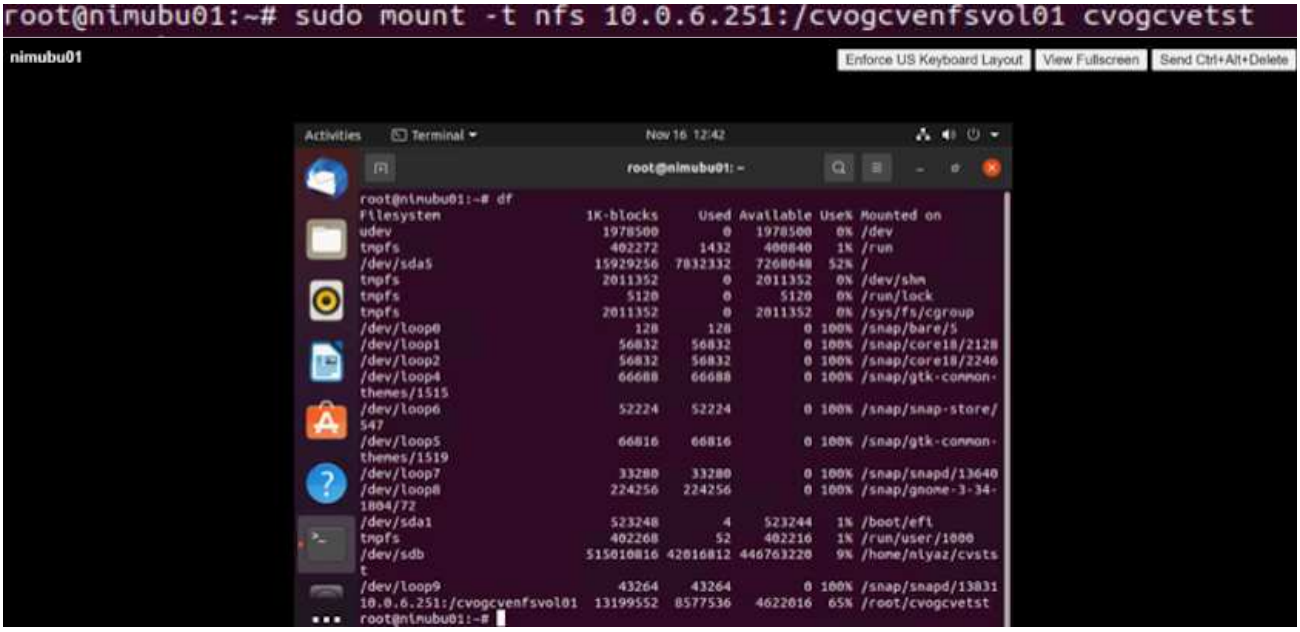
4. 单击“复制”。
5. 连接到指定的Linux实例。
6. 使用安全外壳 (SSH) 在实例上打开终端并使用适当的凭据登录。
7. 使用以下命令为卷的挂载点创建一个目录。

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. 将Cloud Volumes ONTAP NFS 卷挂载到上一步创建的目录。

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



Google Cloud NetApp Volumes(NetApp卷)

Google Cloud NetApp Volumes （NetApp Volumes）是一套完整的数据服务组合，可提供先进的云解决方案。NetApp Volumes 支持主要云提供商的多种文件访问协议（NFS 和 SMB 支持）。

其他优势和功能包括：使用快照进行数据保护和恢复；在本地或云端复制、同步和迁移数据目的地的特殊功能；以及在专用闪存系统级别保持一致的高性能。

Google Cloud NetApp Volumes （NetApp Volumes）作为来宾连接存储

▼ 使用 **VMware Engine** 配置**NetApp**卷

可以从在 VMware Engine 环境中创建的虚拟机挂载Google Cloud NetApp Volumes共享。由于Google Cloud NetApp Volumes支持 SMB 和 NFS 协议，因此这些卷也可以安装在 Linux 客户端上并映射到 Windows 客户端上。可以通过简单的步骤来设置Google Cloud NetApp Volumes卷。

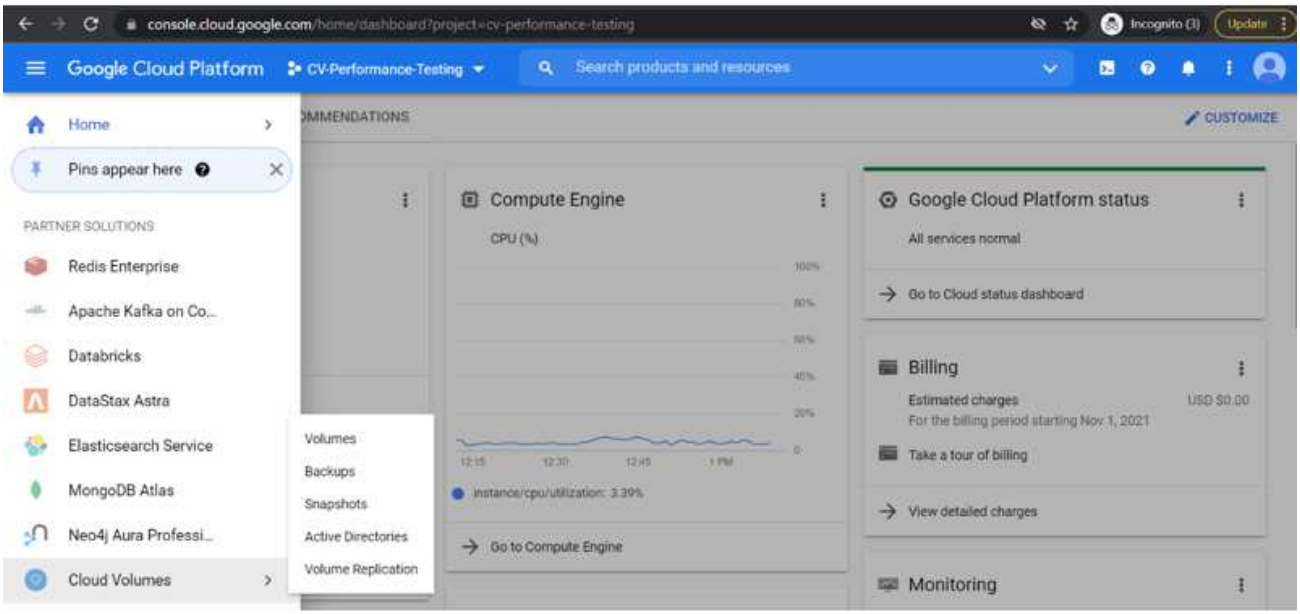
Google Cloud NetApp Volumes和 Google Cloud VMware Engine 私有云必须位于同一区域。

要从 Google Cloud Marketplace 购买、启用和配置适用于 Google Cloud 的 Google Google Cloud NetApp Volumes ，请按照以下详细说明操作"指导"。

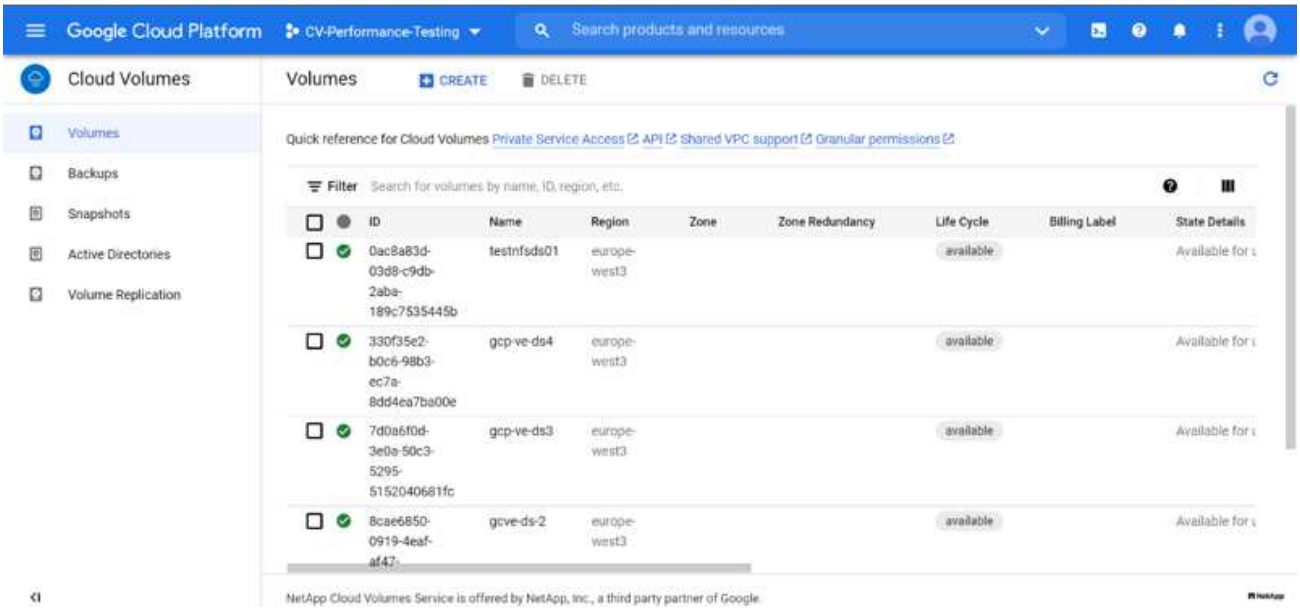
▼ 创建**NetApp Volumes NFS** 卷到 **GCVE** 私有云

要创建和挂载 NFS 卷，请完成以下步骤：

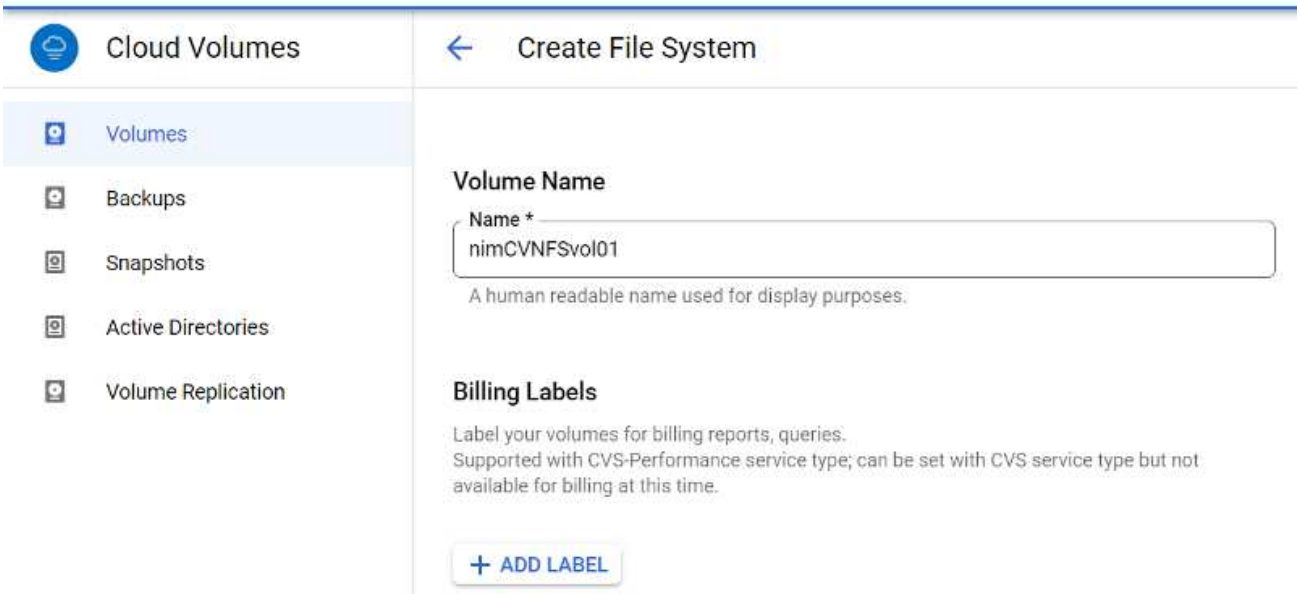
1. 从 Google 云控制台中的合作伙伴解决方案访问 Cloud Volumes。



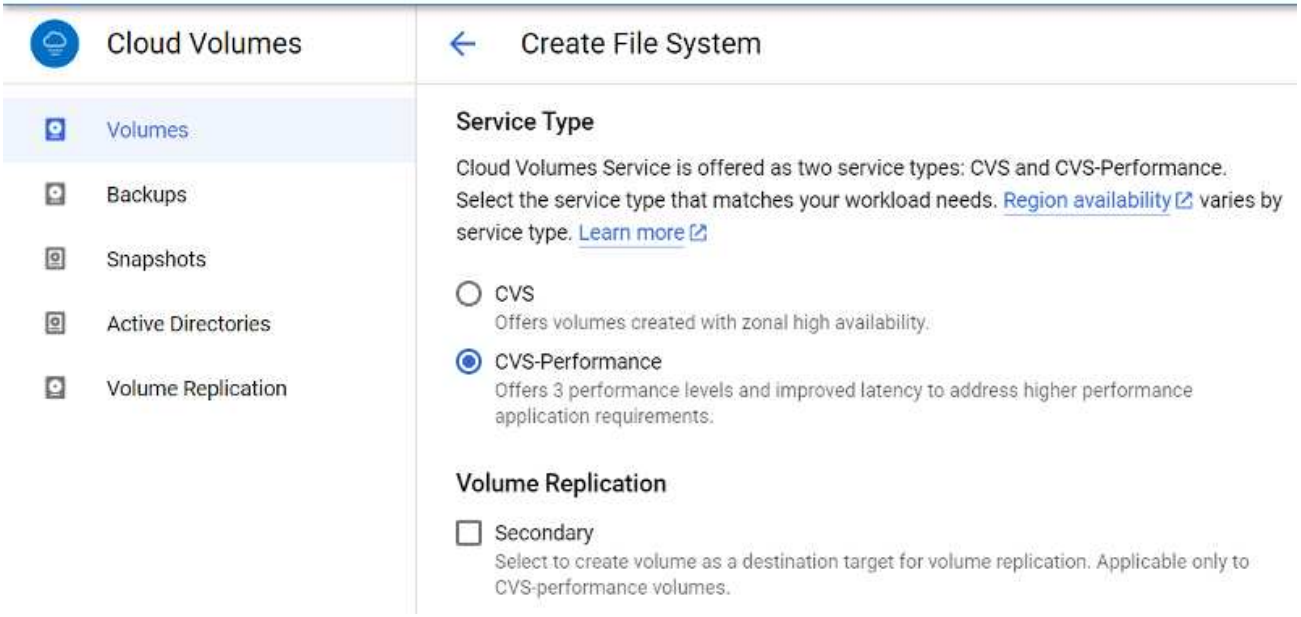
2. 在 Cloud Volumes 控制台中，转到卷页面并单击创建。



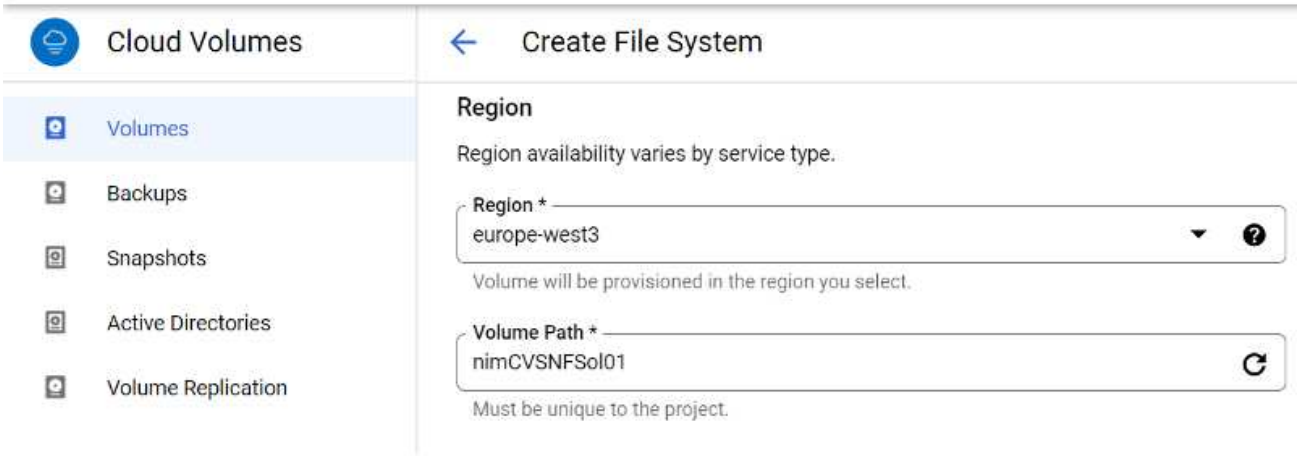
3. 在创建文件系统页面上，根据退款机制的需要指定卷名称和计费标签。



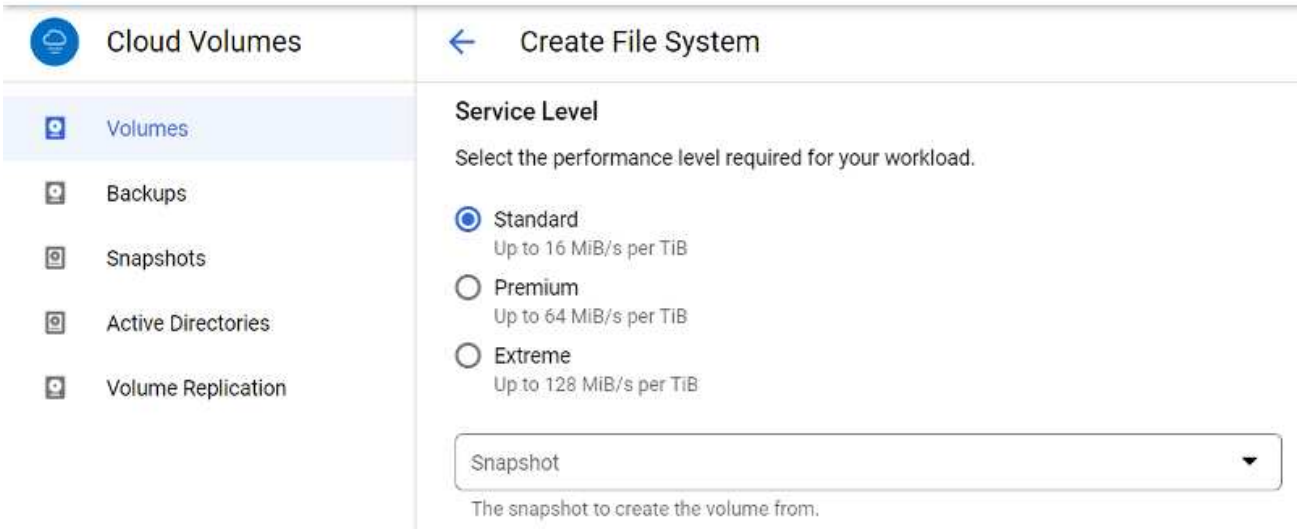
4. 选择适当的服务。对于 GCVE，根据应用程序工作负载要求选择NetApp Volumes-Performance 和所需的服务级别，以改善延迟并提高性能。



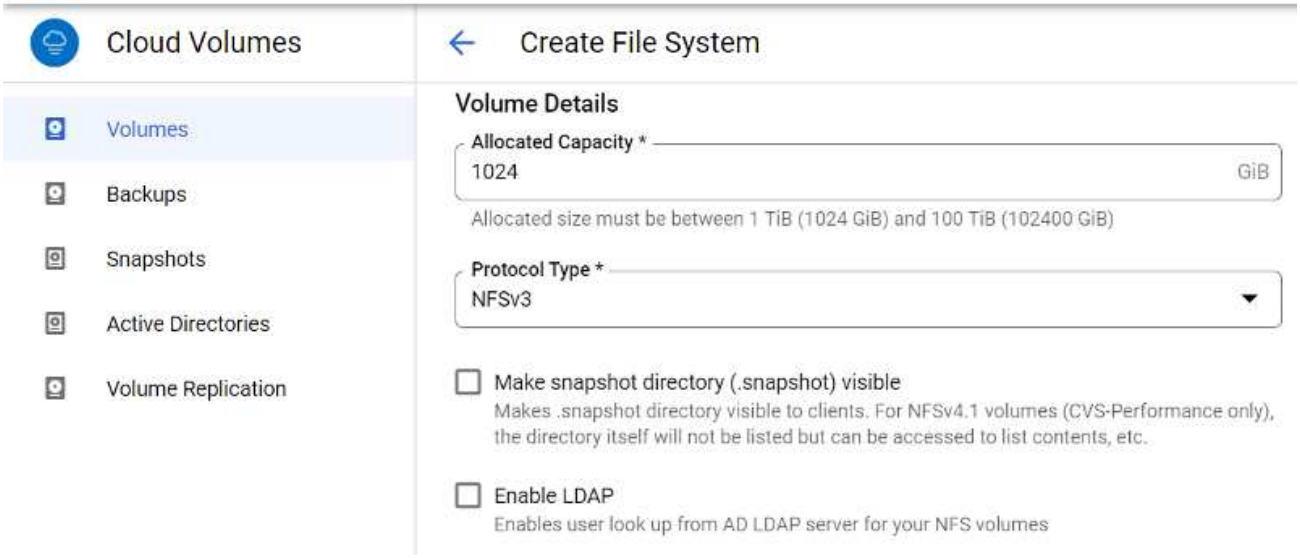
5. 指定卷和卷路径的 Google Cloud 区域（卷路径在项目的所有云卷中必须是唯一的）



6. 选择卷的性能级别。

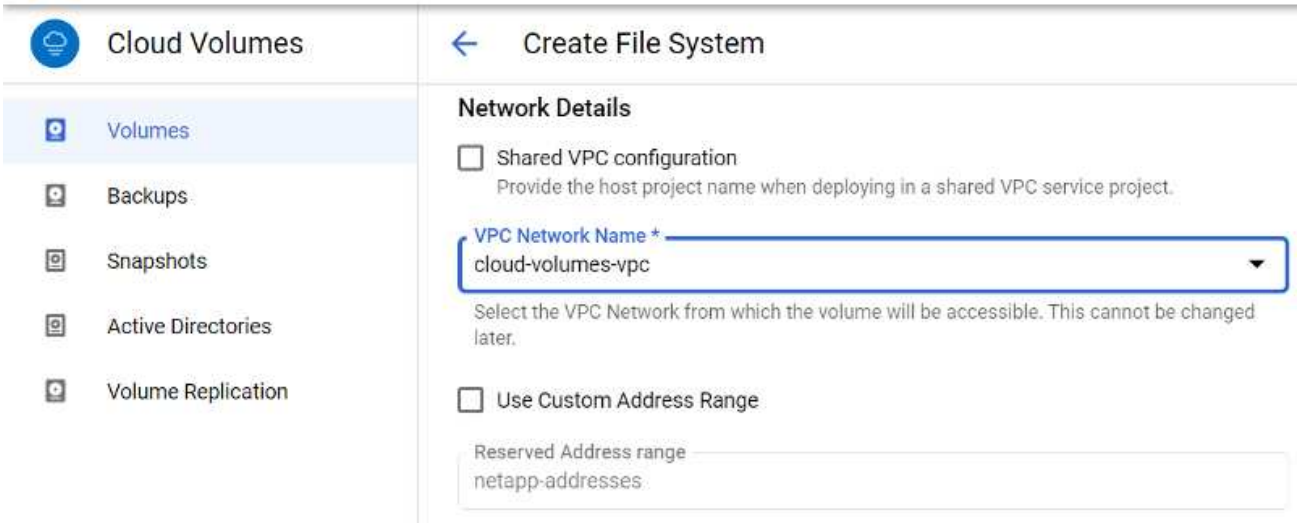


7. 指定卷的大小和协议类型。本次测试采用的是NFSv3。



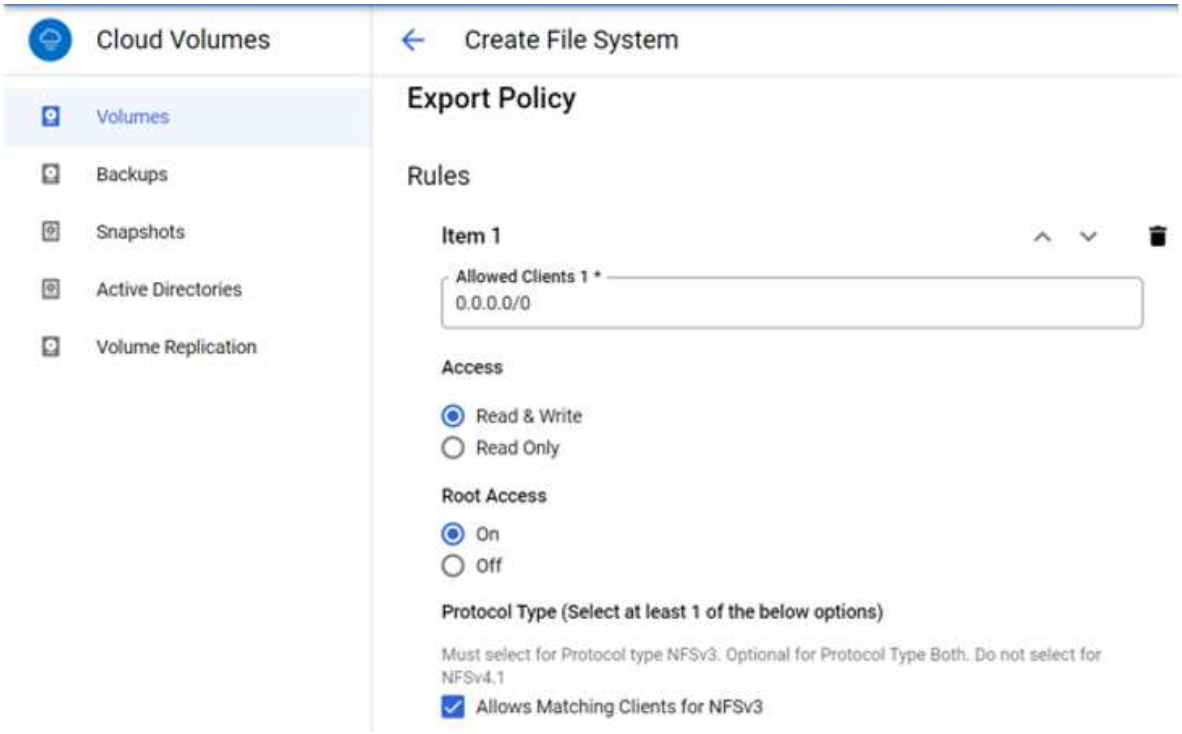
8. 在此步骤中，选择可访问卷的 VPC 网络。确保 VPC 对等连接已到位。

   提示：如果尚未完成 VPC 对等连接，则会显示一个弹出按钮来指导您完成对等连接命令。打开 Cloud Shell 会话并执行适当的命令以将您的 VPC 与Google Cloud NetApp Volumes生产者对等连接。如果您决定提前准备 VPC 对等连接，请参阅这些说明。



9. 通过添加适当的规则来管理导出策略规则并选中相应 NFS 版本的复选框。

   注意：除非添加导出策略，否则无法访问 NFS 卷。



10. 单击“保存”以创建卷。



▼ 将 **NFS** 导出挂载到在 **VMware Engine** 上运行的虚拟机

在准备挂载 NFS 卷之前，请确保私有连接的对等状态列为“活动”。一旦状态为“活动”，请使用 mount 命令。

要挂载 NFS 卷，请执行以下操作：

1. 在 Cloud Console 中，转到 Cloud Volumes > Volumes。
2. 转到卷页面
3. 单击要挂载 NFS 导出的 NFS 卷。
4. 滚动到右侧，在“显示更多”下单击“安装说明”。

要从 VMware VM 的客户操作系统中执行安装过程，请按照以下步骤操作：

1. 使用 SSH 客户端和 SSH 连接到虚拟机。
2. 在实例上安装 nfs 客户端。
   a. 在 Red Hat Enterprise Linux 或 SuSE Linux 实例上：

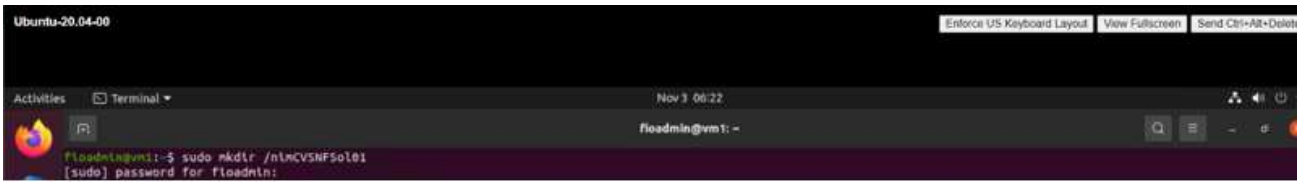
```
sudo yum install -y nfs-utils
```

.. 在 Ubuntu 或 Debian 实例上：

```
sudo apt-get install nfs-common
```

3. 在实例上创建一个新目录，例如“/nimCVSNFSol01”：

```
sudo mkdir /nimCVSNFSol01
```



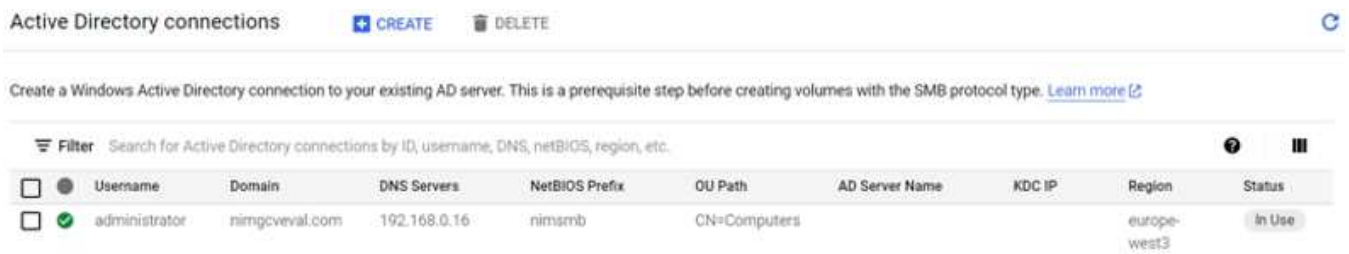
4. 使用适当的命令挂载卷。实验室的示例命令如下：

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```

```
root@vm1:~# sudo mkdir nimCVSNFSol01
root@vm1:~# sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp 10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
root@vm1:~# df
Filesystem                     1K-blocks       Used    Available Use% Mounted on
udev                            16409952          0     16409952   0% /dev
tmpfs                            3288328       1580      3286748   1% /run
/dev/sdb5                       61145932   19231356     38778832  34% /
tmpfs                           16441628          0     16441628   0% /dev/shm
tmpfs                               5120          0         5120   0% /run/lock
tmpfs                           16441628          0     16441628   0% /sys/fs/cgroup
/dev/loop0                        128        128            0 100% /snap/bare/5
/dev/loop1                      56832      56832            0 100% /snap/core18/2128
/dev/loop2                      66688      66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                      66816      66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                      52224      52224            0 100% /snap/snap-store/547
/dev/loop5                     224256     224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                      523248          4       523244   1% /boot/efi
tmpfs                          3288324         28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1       107374182400 1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01   419155968   55384972    363770996  14% /datastore1
/dev/loop8                      33280      33280            0 100% /snap/snapd/13270
/dev/loop6                      33280      33280            0 100% /snap/snapd/13640
/dev/loop7                      56832      56832            0 100% /snap/core18/2246
10.53.0.4:/nimCVSNFSol01   107374182400        256 107374182144   1% /nimCVSNFSol01
root@vm1:~#
```

▼ 创建 **SMB** 共享并将其挂载到在 **VMware Engine** 上运行的虚拟机

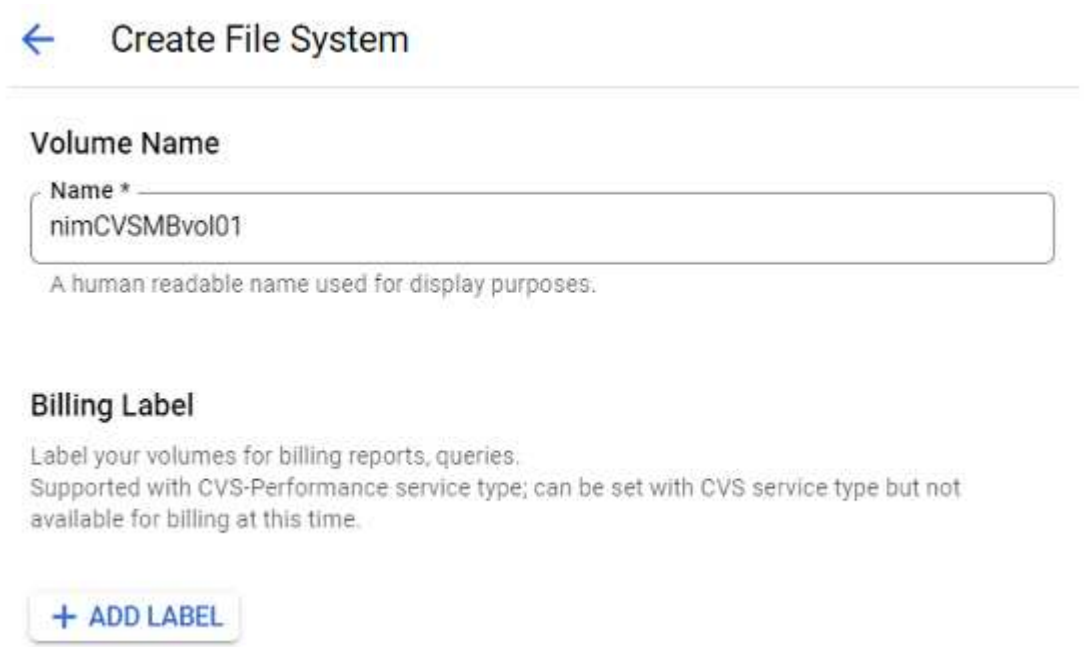
对于 SMB 卷，请确保在创建 SMB 卷之前配置了 Active Directory 连接。



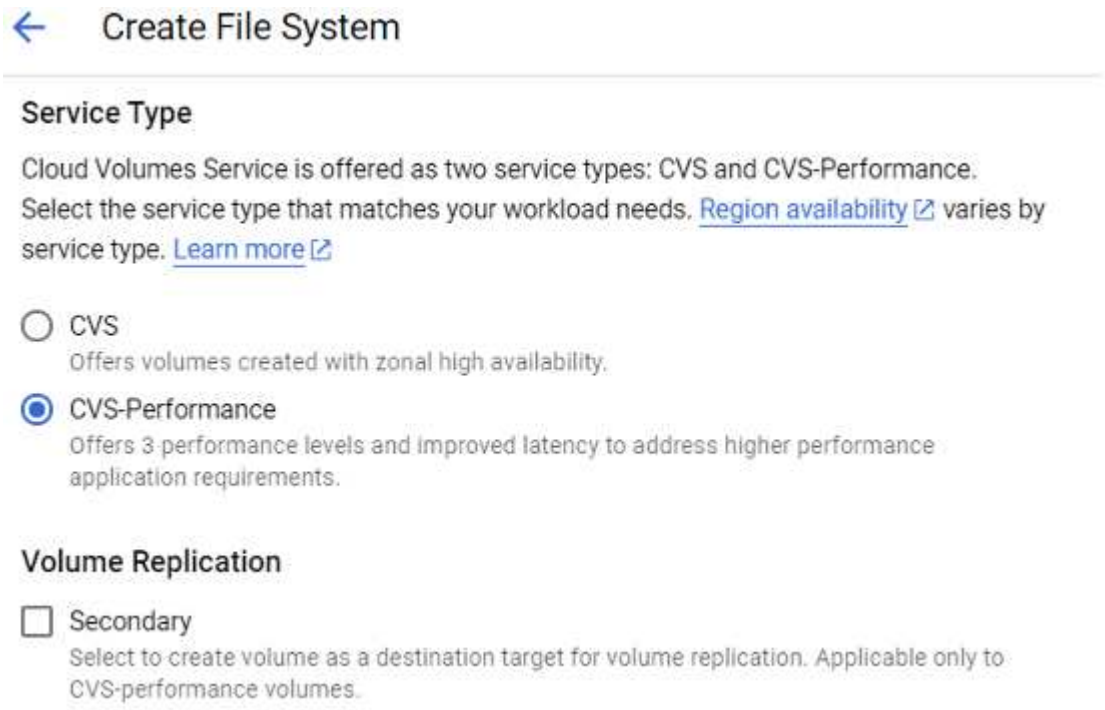
一旦 AD 连接到位，即可创建具有所需服务级别的卷。除了选择适当的协议外，步骤与创建 NFS 卷类似。

1. 在 Cloud Volumes 控制台中，转到卷页面并单击创建。

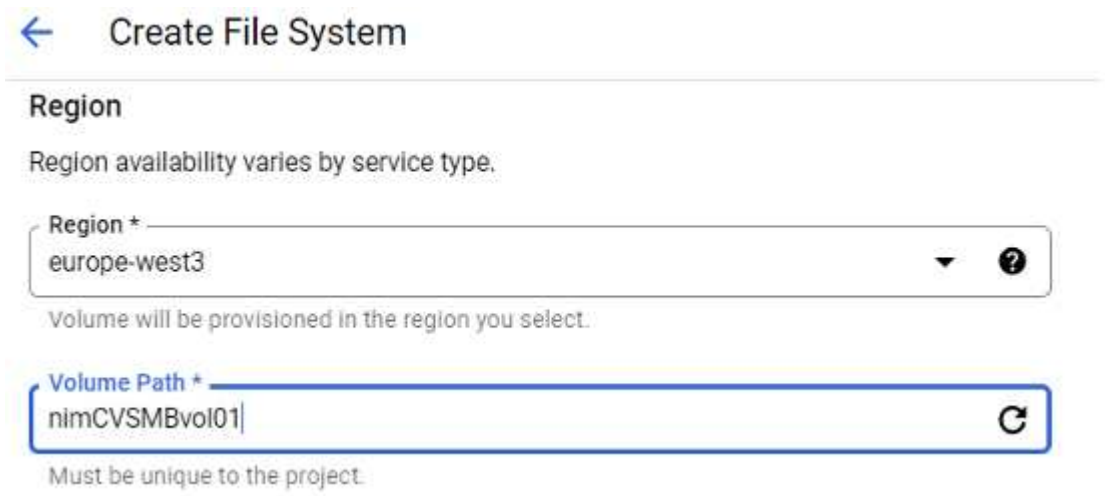
2. 在创建文件系统页面上，根据退款机制的需要指定卷名称和计费标签。



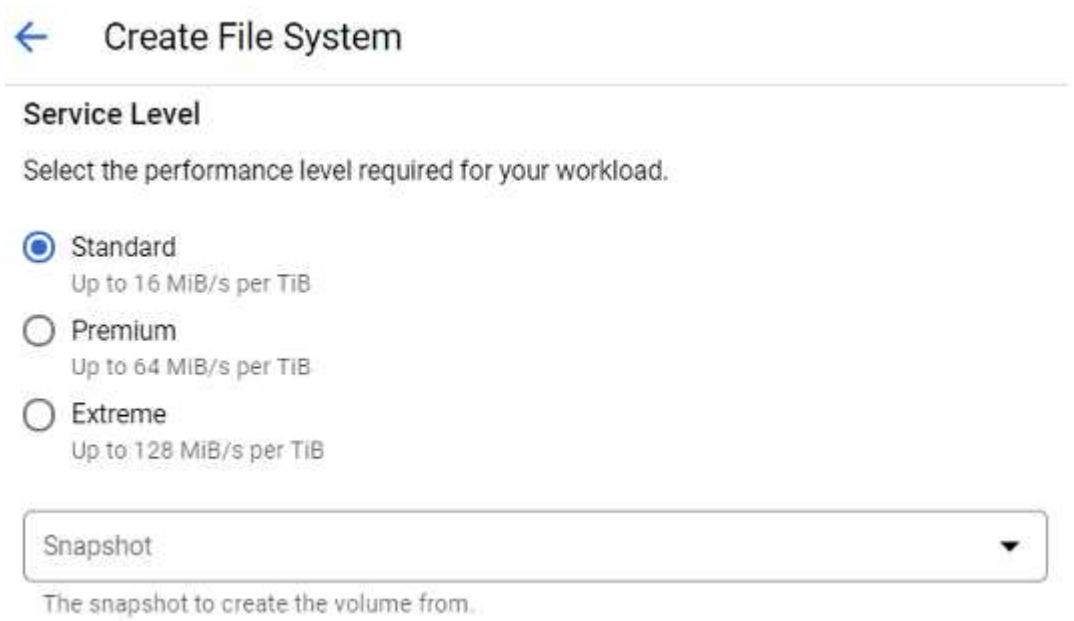
3. 选择适当的服务。对于 GCVE，根据工作负载要求选择NetApp Volumes-Performance 和所需的服务级别，以改善延迟并提高性能。



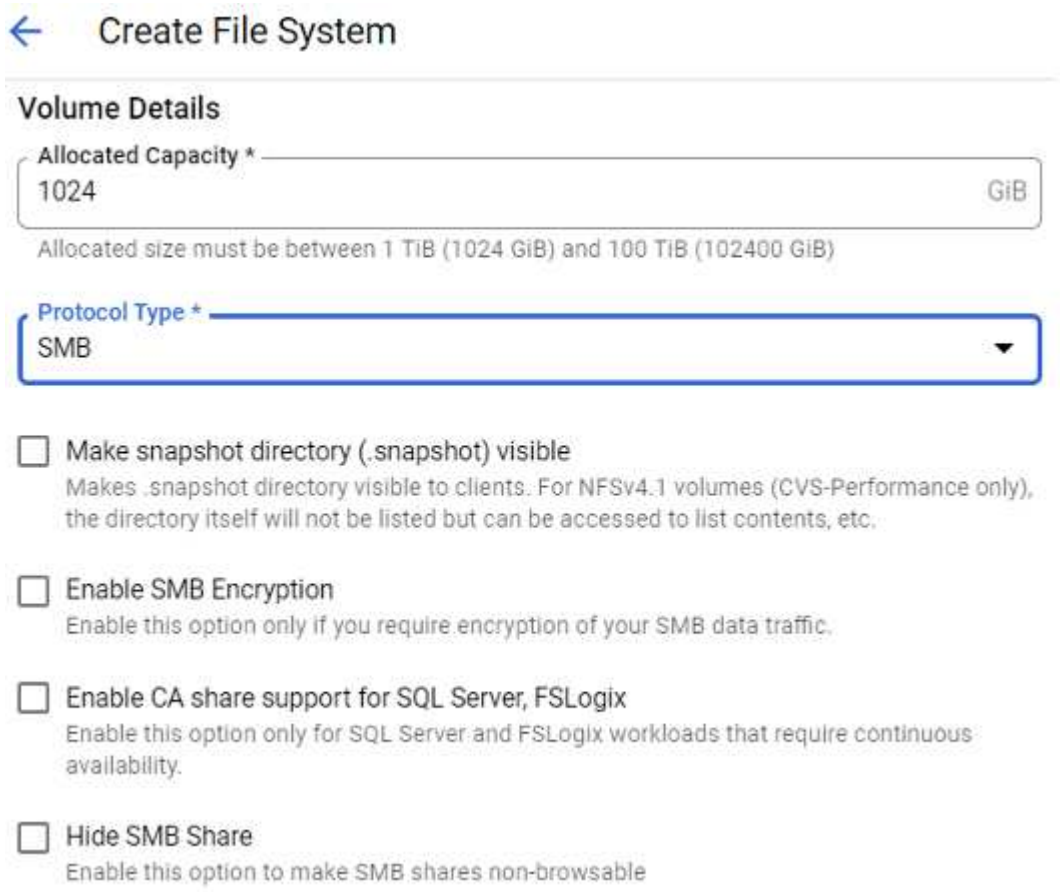
4. 指定卷和卷路径的 Google Cloud 区域（卷路径在项目的所有云卷中必须是唯一的）



5. 选择卷的性能级别。

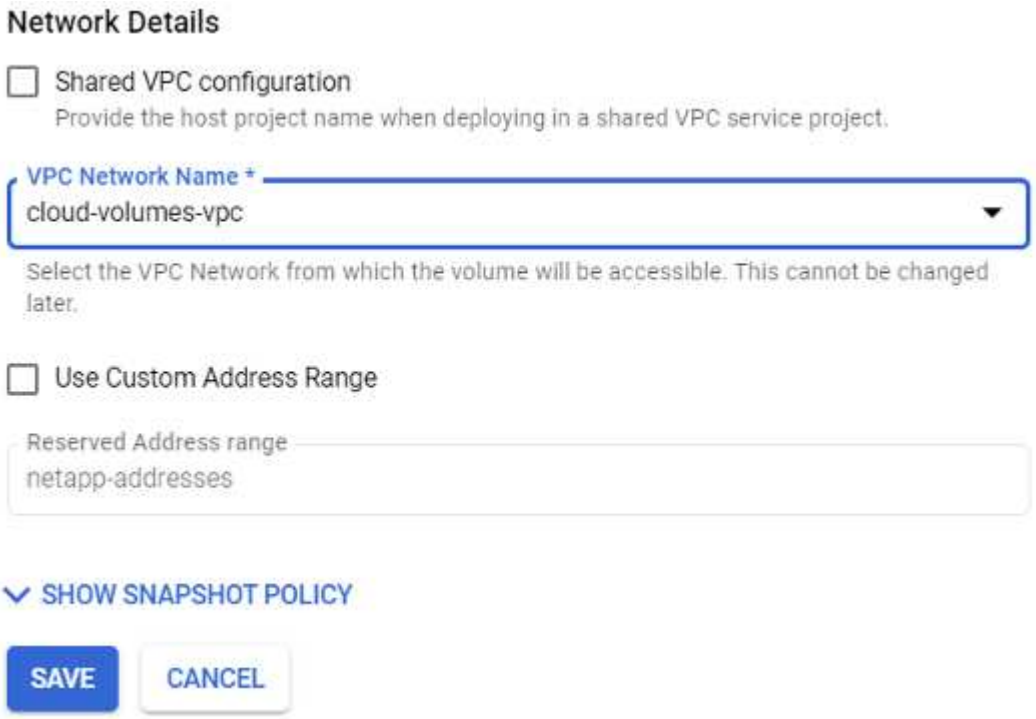


6. 指定卷的大小和协议类型。本次测试中使用了 SMB。



7. 在此步骤中，选择可访问卷的 VPC 网络。确保 VPC 对等连接已到位。

   提示：如果尚未完成 VPC 对等互连，将显示一个弹出按钮，引导您完成对等互连命令。打开 Cloud Shell 会话并执行相应的命令，将您的 VPC 与 Google Cloud NetApp Volumes 生产者进行对等互连。如果您决定事先准备好 VPC 对等互连，请参阅这些 "指示"。



8. 单击“保存”以创建卷。



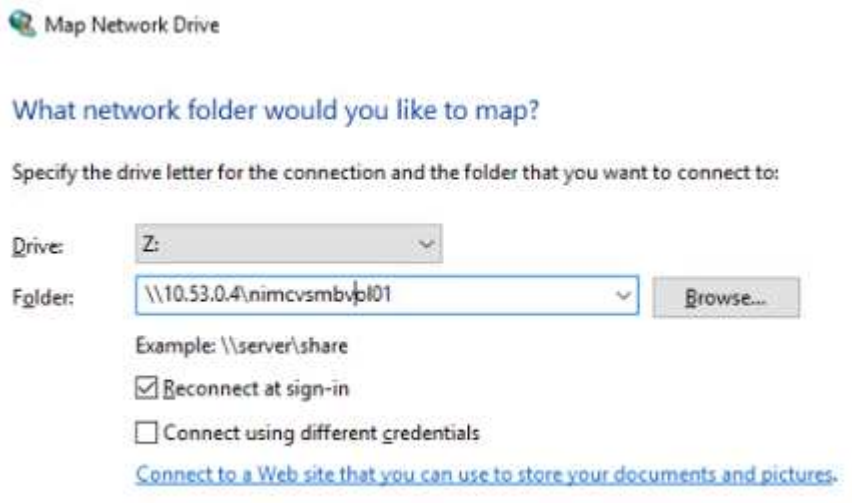
要安装 SMB 卷，请执行以下操作：

1. 在 Cloud Console 中，转到 Cloud Volumes > Volumes。
2. 转到卷页面
3. 单击要映射 SMB 共享的 SMB 卷。
4. 滚动到右侧，在“显示更多”下单击“安装说明”。

要从 VMware VM 的 Windows 客户操作系统中执行安装过程，请按照以下步骤操作：

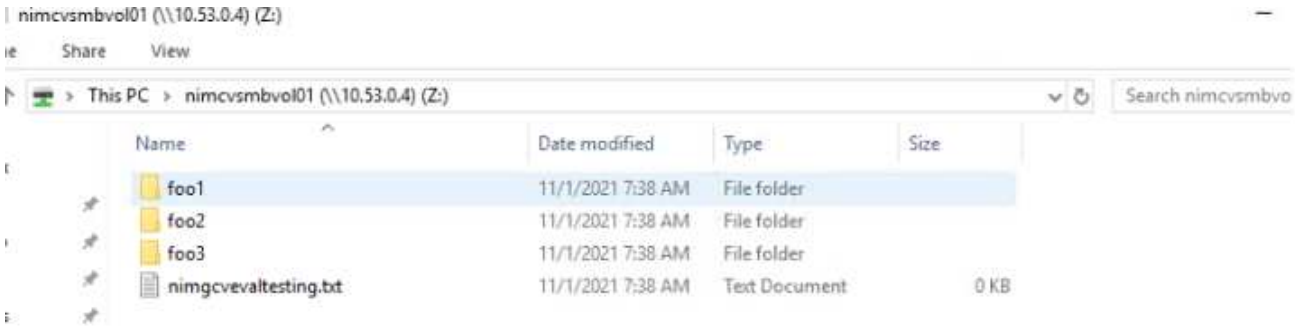
1. 单击“开始”按钮，然后单击“计算机”。
2. 单击“映射网络驱动器”。
3. 在驱动器列表中，单击任何可用的驱动器号。
4. 在文件夹框中，键入：

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



若要在每次登录计算机时进行连接，请选中“登录时重新连接”复选框。

5. 单击“完成”。



总结与结论： **NetApp**为何选择 **VMware** 作为混合多云平台

NetApp Cloud Volumes 与针对主要超大规模企业的 VMware 解决方案为希望利用混合云的组织提供了巨大的潜力。本节的其余部分提供了用例，表明集成NetApp Cloud Volumes可以实现真正的混合多云功能。

用例 **#1**：优化存储

当使用 RVtools 输出执行大小调整练习时，马力（vCPU/vMem）比例与存储平行是显而易见的。很多时候，组织会发现他们所处的境地是，所需的存储空间使集群的规模远远超出了马力所需的范围。

通过集成NetApp Cloud Volumes，组织可以通过简单的迁移方法实现基于 vSphere 的云解决方案，无需重新平台化、无需 IP 更改、无需架构更改。此外，通过此优化，您可以扩展存储空间，同时将主机数量保持在 vSphere 所需的最少量，但不会改变存储层次结构、安全性或可用的文件。这使您可以优化部署并将总体 TCO 降低 35–45%。通过这种集成，您还可以在几秒钟内将存储从热存储扩展到生产级性能。

用例**2**：云迁移

由于多种原因，组织面临着将应用程序从本地数据中心迁移到公共云的压力：租约即将到期；财务指令要求从资本支出 (capex) 转向运营支出 (opex)；或者仅仅是自上而下的命令要求将所有内容迁移到云端。

当速度至关重要时，只有简化的迁移方法是可行的，因为重新平台化和重构应用程序以适应云的特定 IaaS 平台既缓慢又昂贵，通常需要数月时间。通过将NetApp Cloud Volumes 与用于客户机连接存储的带宽高效的SnapMirror复制（包括与应用程序一致的 Snapshot 副本和 HCX 结合的 RDM、特定于云的迁移（例如 Azure Migrate）或用于复制虚拟机的第三方产品）相结合，这种转变比依赖耗时的 I/O 过滤机制更容易。

用例**3**：数据中心扩展

当数据中心由于季节性需求高峰或仅仅是稳定的有机增长而达到容量限制时，迁移到云托管的 VMware 以及NetApp Cloud Volumes 是一个简单的解决方案。利用NetApp Cloud Volumes，可以通过提供跨可用区域的高可用性和动态扩展功能，非常轻松地创建、复制和扩展存储。利用NetApp Cloud Volumes 有助于克服对延伸集群的需求，从而最大限度地减少主机集群容量。

用例 **#4**：灾难恢复至云端

在传统方法中，如果发生灾难，复制到云中的虚拟机需要转换到云自己的虚拟机管理程序平台才能恢复 - 这不是危机期间要处理的任务。

通过使用NetApp Cloud Volumes 进行来宾连接存储，使用来自本地的SnapCenter和SnapMirror复制以及公共云虚拟化解决方案，可以设计出一种更好的灾难恢复方法，允许在完全一致的 VMware SDDC 基础架构上恢复虚拟机副本以及特定于云的恢复工具（例如 Azure Site Recovery）或等效的第三方工具（如 Veeam）。这种方法

还使您能够快速执行灾难恢复演习和勒索软件恢复。通过按需添加主机，您还可以扩展到全面生产以进行测试或在灾难期间进行扩展。

用例 **#5**：应用程序现代化

应用程序进入公共云后，组织将希望利用数百种强大的云服务来实现其现代化和扩展。通过使用NetApp Cloud Volumes，现代化是一个简单的过程，因为应用程序数据不会被锁定在 vSAN 中，并且允许在包括 Kubernetes 在内的广泛用例中实现数据移动。

结束语

无论您的目标是全云还是混合云， NetApp Cloud Volumes 都提供了出色的选项来部署和管理应用程序工作负载以及文件服务和块协议，同时通过使数据需求无缝连接到应用程序层来降低 TCO。

无论使用情况如何，选择您最喜欢的云/超大规模器以及NetApp Cloud Volumes，以快速实现云优势、一致的基础架构和跨本地和多个云的操作、工作负载的双向可移植性以及企业级容量和性能。

它与用于连接存储的熟悉的过程和程序相同。请记住，新名称只是改变了数据的位置；工具和流程都保持不变，NetApp Cloud Volumes 有助于优化整体部署。

VMware 混合云用例

NetApp与 VMware 混合多云的用例

概述在规划混合云或云优先部署时对 IT 组织重要的用例。

热门用例

用例包括：

- 灾难恢复，
- 在数据中心维护期间托管工作负载，* 快速爆发，需要超出本地数据中心配置的额外资源，
- VMware 站点扩展，
- 快速迁移到云端，
- 开发/测试，以及
- 利用云补充技术实现应用程序的现代化。

在本文档中，将使用 VMware 用例详细说明云工作负载参考。这些用例是：

- 保护（包括灾难恢复和备份/还原）
- 迁移
- 延长

IT 之旅

大多数组织都处于转型和现代化的征程中。作为此过程的一部分，公司正在尝试利用其现有的 VMware 投资，同时利用云优势并探索使迁移过程尽可能无缝的方法。由于数据已经在云端，这种方法将使他们的现代化工作变

得非常容易。

对于这种情况最简单的答案是每个超大规模企业都提供 VMware 产品。与NetApp Cloud Volumes 一样，VMware 提供了一种将本地 VMware 环境移动或扩展到任何云的方法，使您能够保留现有的本地资产、技能和工具，同时在云中本地运行工作负载。这降低了风险，因为不会出现服务中断或需要更改 IP，并使 IT 团队能够使用现有技能和工具以在本地的方式进行操作。这可以加速云迁移并更顺利地过渡到混合多云架构。

了解补充 **NFS** 存储选项的重要性

虽然任何云中的 VMware 都为每个客户提供了独特的混合功能，但有限的补充 NFS 存储选项限制了其对于存储工作负载繁重的组织的实用性。由于存储直接与主机绑定，因此扩展存储的唯一方法是添加更多主机 - 而这会使存储密集型工作负载的成本增加 35-40% 或更多。这些工作负载只需要额外的存储空间，而不是额外的马力。但这意味着需要支付额外的主机费用。

让我们考虑一下这种情况：

一个客户只需要五台主机来提供 CPU 和内存，但是有大量的存储需求，需要 12 台主机来满足存储需求。当他们只需要增加存储空间时，这个要求最终会真正打破财务平衡，因为他们必须购买额外的马力。

当您规划云采用和迁移时，评估最佳方法并采取最简单的途径来减少总投资始终非常重要。对于任何应用程序迁移来说，最常见和最简单的方法是重新托管（也称为提升和转移），其中不需要虚拟机（VM）或数据转换。将NetApp Cloud Volumes 与 VMware 软件定义数据中心 (SDDC) 结合使用，在补充 vSAN 的同时，提供了简单的提升和转移选项。

面向超大规模企业 **VMware** 的**NetApp**解决方案

详细了解NetApp为每个超大规模企业中的 VMware 环境提供的解决方案 - 从迁移工作流、扩展/爆发到云、备份/恢复到灾难恢复。

适用于 **VMware** 环境的**NetApp**解决方案

无论您采用混合云模型还是“云优先”模型， NetApp都提供各种解决方案来满足在云或混合云模型中管理工作负载的最常见用例。

NetApp还为每个超大规模服务器中的存储提供解决方案，这些存储可作为客户机内（客户机连接）存储或补充 NFS 数据存储。所有解决方案均按照 VMware 的云工作负载分类进行分类。这些分类包括：

- 保护（包括灾难恢复和备份/还原）
- 迁移
- 延长

有关每个超大规模企业可用解决方案的更多详细信息，请访问：

- "AWS/VMC 解决方案"
- "Azure/AVS 解决方案"
- "GCP/GCVE 解决方案"

适用于 **Amazon VMware** 托管云 **(VMC)** 的**NetApp**解决方案

详细了解NetApp为 AWS 带来的解决方案。

VMware 将云工作负载分为以下三类：

- 保护（包括灾难恢复和备份/还原）
- 迁移
- 延长

浏览以下部分中可用的解决方案。

保护

- "使用 AWS 上的 VMC 进行灾难恢复（来宾连接）"
- "使用 FSx ONTAP在 VMC 中备份和恢复 Veeam"
- "使用 FSx ONTAP和 VMC 实现灾难恢复 (DRO)"
- "使用 Veeam Replication 和 FSx ONTAP实现 VMware Cloud on AWS 灾难恢复"

迁移

- "使用 VMware HCX 将工作负载迁移到 FSx ONTAP数据存储区"

延长

即将推出！！

适用于 **Azure VMware** 解决方案 **(AVS)** 的**NetApp**解决方案

详细了解NetApp为 Azure 带来的解决方案。

VMware 将云工作负载分为以下三类：

- 保护（包括灾难恢复和备份/还原）
- 迁移
- 延长

浏览以下部分中可用的解决方案。

保护

- "使用 ANF 和 JetStream 进行灾难恢复（补充 NFS 数据存储）"
- "使用 ANF 和 CVO（来宾连接存储）进行灾难恢复"
- "使用 ANF 和 AVS 的灾难恢复 (DRO)"
- "使用 Veeam Replication 和Azure NetApp Files数据存储区对 Azure VMware 解决方案进行灾难恢复"

迁移

- "使用 VMware HCX 将工作负载迁移到Azure NetApp Files数据存储"

延长

即将推出！！

适用于 **Google Cloud VMware Engine (GCVE)** 的**NetApp**解决方案

详细了解NetApp为 GCP 带来的解决方案。

VMware 将云工作负载分为以下三类：

- 保护（包括灾难恢复和备份/还原）
- 迁移
- 延长

浏览以下部分中可用的解决方案。

保护

- "使用SnapCenter、 Cloud Volumes ONTAP和 Veeam Replication 实现应用程序灾难恢复"
- "使用NetApp SnapCenter和 Veeam Replication 实现应用程序一致性灾难恢复，以在 GCVE 上复制NetApp卷"

迁移

- "使用 VMware HCX 将工作负载迁移到Google Cloud NetApp Volumes NFS 数据存储区"
- "使用 Veeam 到Google Cloud NetApp Volumes NFS 数据存储区的虚拟机复制"

延长

即将推出！！

适用于 **AWS/VMC** 的**NetApp**

NetApp的 **AWS VMC** 功能

详细了解NetApp为 AWS VMware Cloud (VMC) 带来的功能 - 从NetApp作为来宾连接存储设备或补充 NFS 数据存储到迁移工作流、扩展/爆发到云、备份/恢复和灾难恢复。

通过选择以下选项跳转到所需内容的部分：

- "在 AWS 中配置 VMC"
- "适用于 VMC 的NetApp存储选项"
- "NetApp /VMware 云解决方案"

在 **AWS** 中配置 **VMC**

与本地一样，规划基于云的虚拟化环境对于成功创建虚拟机和迁移的生产就绪环境至关重要。

本节介绍如何设置和管理 VMware Cloud on AWS SDDC，并将其与可用于连接NetApp存储的选项结合使用。

客户机内存储是将Cloud Volumes ONTAP连接到 AWS VMC 的唯一支持方法。

设置过程可分为以下步骤：

- 部署和配置 VMware Cloud for AWS
- 将 VMware Cloud 连接到 FSx ONTAP

查看详细信息"VMC 的配置步骤"。

适用于 **VMC** 的**NetApp**存储选项

NetApp存储在 AWS VMC 中可以以多种方式使用 - 既可以作为猜测连接，也可以作为补充 NFS 数据存储。

请访问"支持的NetApp存储选项"了解更多信息。

AWS 支持以下配置的NetApp存储：

- FSx ONTAP作为来宾连接存储
- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- FSx ONTAP作为补充 NFS 数据存储

查看详细信息"VMC 的客户机连接存储选项"。查看详细信息"VMC 的补充 NFS 数据存储选项"。

解决方案用例

借助NetApp和 VMware 云解决方案，许多用例都可以轻松地部署在您的 AWS VMC 中。针对 VMware 定义的每个云区域都定义了用例：

- 保护（包括灾难恢复和备份/还原）
- 延长
- 迁移

"浏览适用于 AWS VMC 的NetApp解决方案"

保护 **AWS/VMC** 上的工作负载

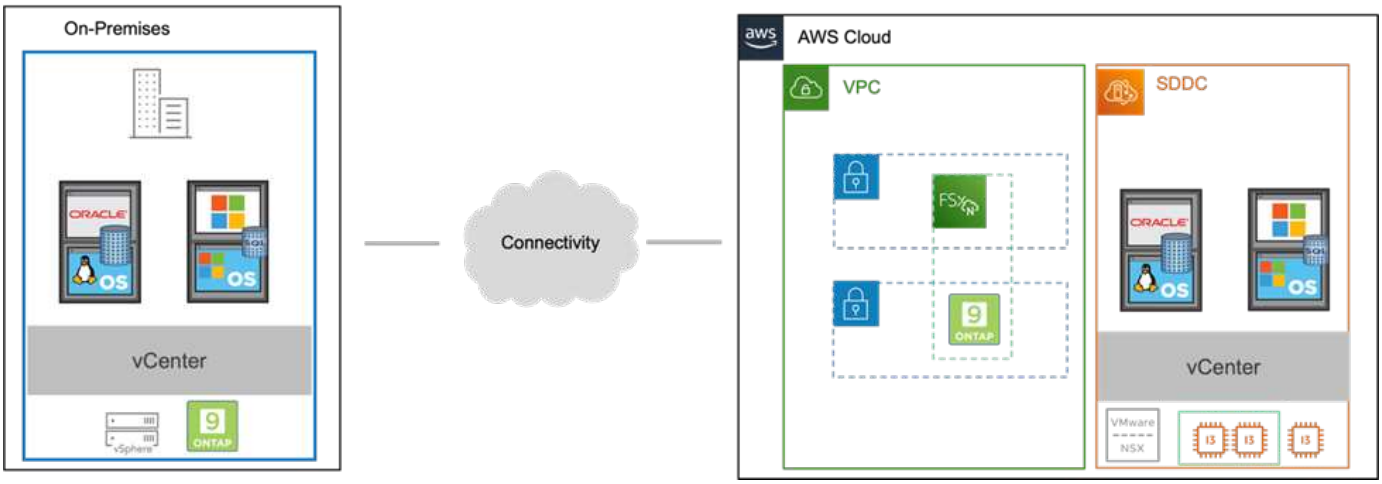
TR-4931：使用 **VMware Cloud on Amazon Web Services** 和 **Guest Connect** 进行灾难恢复

经过验证的灾难恢复 (DR) 环境和计划对于组织至关重要，以确保在发生重大中断时能够快速恢复关键业务应用程序。该解决方案专注于演示 DR 用例，重点关注 VMware 和NetApp技术，包括本地和 AWS 上的 VMware Cloud。

概述

NetApp与 VMware 的整合历史悠久，数以万计的客户选择NetApp作为其虚拟化环境的存储合作伙伴，就证明了这一点。这种集成延续了云中的客户连接选项以及最近与 NFS 数据存储的集成。该解决方案专注于通常称为客户连接存储的用例。

在来宾连接存储中，来宾 VMDK 部署在 VMware 配置的数据存储上，应用程序数据存放在 iSCSI 或 NFS 上并直接映射到 VM。 Oracle 和 MS SQL 应用程序用于演示 DR 场景，如下图所示。



假设、先决条件和组件概述

在部署此解决方案之前，请查看组件概述、部署此解决方案所需的先决条件以及记录此解决方案时所做的假设。

"DR 解决方案要求、先决条件和规划"

使用**SnapCenter**执行灾难恢复

在此解决方案中， SnapCenter为 SQL Server 和 Oracle 应用程序数据提供应用程序一致的快照。此配置与SnapMirror技术相结合，可在我们的内部AFF和 FSx ONTAP集群之间提供高速数据复制。此外，Veeam Backup & Replication 为我们的虚拟机提供备份和恢复功能。

在本节中，我们介绍SnapCenter、 SnapMirror和 Veeam 的备份和恢复配置。

以下部分介绍在辅助站点完成故障转移所需的配置和步骤：

配置**SnapMirror**关系和保留计划

SnapCenter可以更新主存储系统 (主 > 镜像) 和二级存储系统 (主 > 保险库) 内的SnapMirror关系，以实现长期存档和保留。为此，您必须使用SnapMirror在目标卷和源卷之间建立并初始化数据复制关系。

源 ONTAP 系统和目标ONTAP系统必须位于使用 Amazon VPC 对等连接、传输网关、AWS Direct Connect 或 AWS VPN 进行对等连接的网络中。

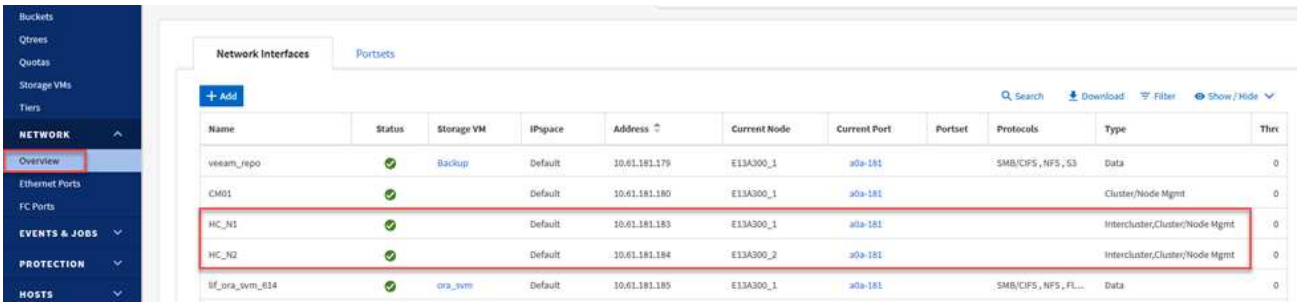
在本地ONTAP系统和 FSx ONTAP之间设置SnapMirror关系需要执行以下步骤：

请参阅 "FSx ONTAP – ONTAP用户指南"有关使用 FSx 创建SnapMirror关系的更多信息。

▼ 记录源和目标集群间逻辑接口

对于位于本地的源ONTAP系统，您可以从系统管理器或 CLI 检索集群间 LIF 信息。

1. 在ONTAP系统管理器中，导航到网络概览页面并检索配置为与安装了 FSx 的 AWS VPC 通信的类型：集群间的 IP 地址。



2. 要检索 FSx 的集群间 IP 地址，请登录 CLI 并运行以下命令：

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

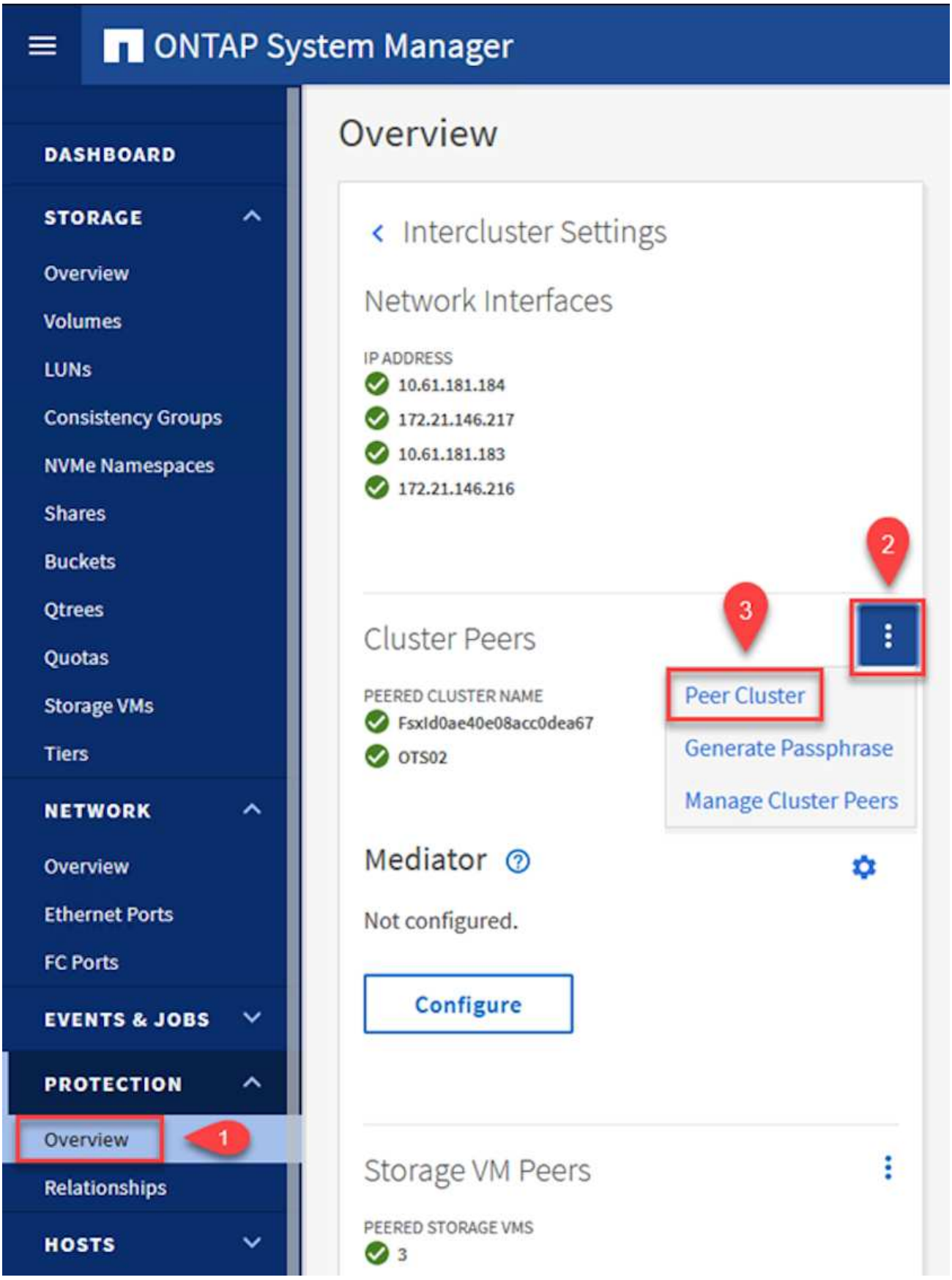
▼ 在**ONTAP**和 **FSx** 之间建立集群对等连接

要在ONTAP集群之间建立集群对等连接，必须在另一个对等集群中确认在启动ONTAP集群中输入的唯一密码。

1. 使用以下方式在目标 FSx 集群上设置对等连接 `cluster peer create`命令。出现提示时，请输入稍后在源集群上使用的唯一密码来完成创建过程。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. 在源集群中，您可以使用ONTAP系统管理器或 CLI 建立集群对等关系。从ONTAP系统管理器中，导航到“保护”>“概览”，然后选择“对等集群”。

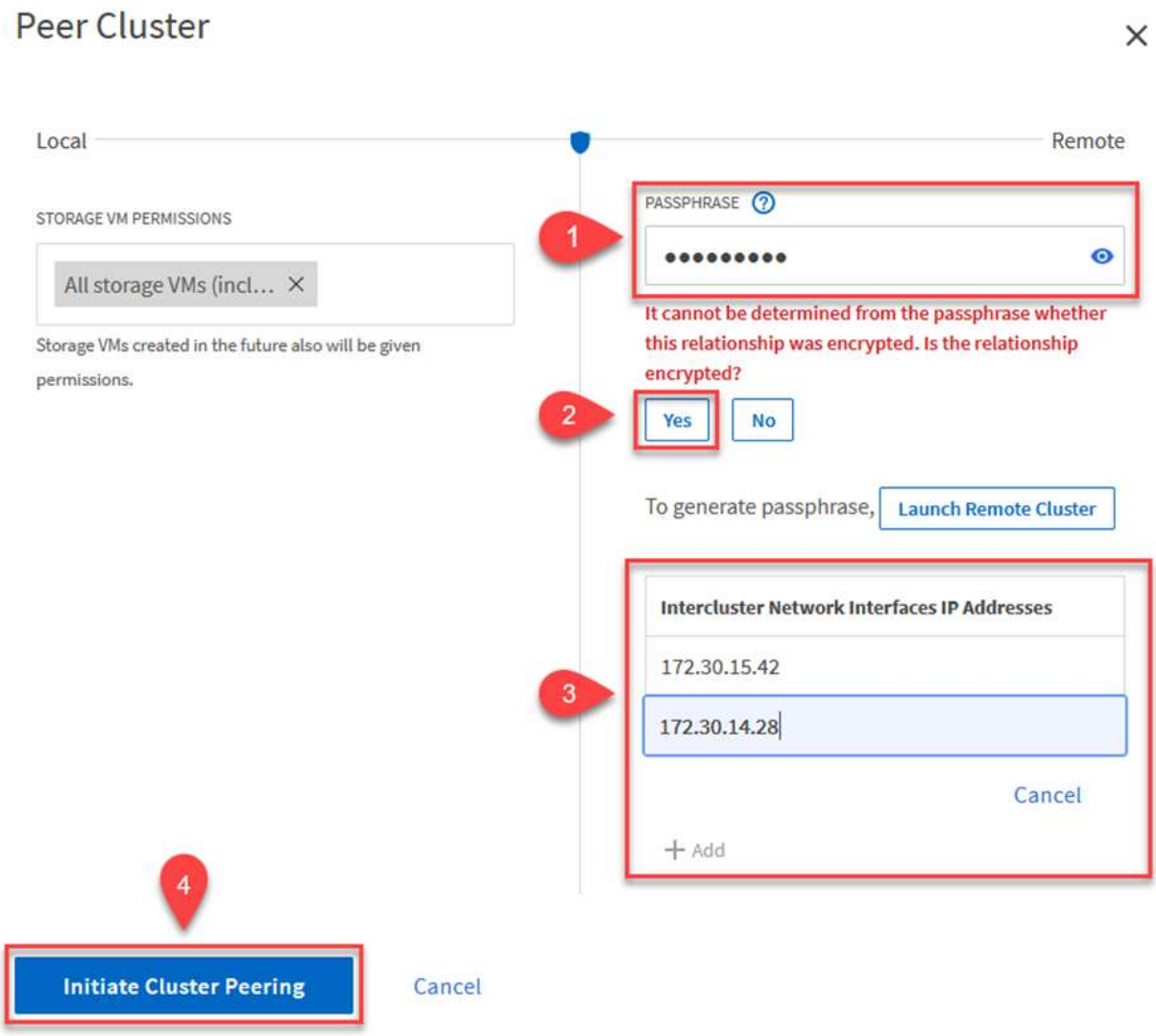


3. 在对等集群对话框中，填写所需信息：
   a. 输入用于在目标 FSx 集群上建立对等集群关系的密码。

b. 选择 `Yes`建立加密关系。

c. 输入目标 FSx 集群的集群间 LIF IP 地址。

d. 单击“启动集群对等”以完成该过程。



4. 使用以下命令从 FSx 集群验证集群对等关系的状态：

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

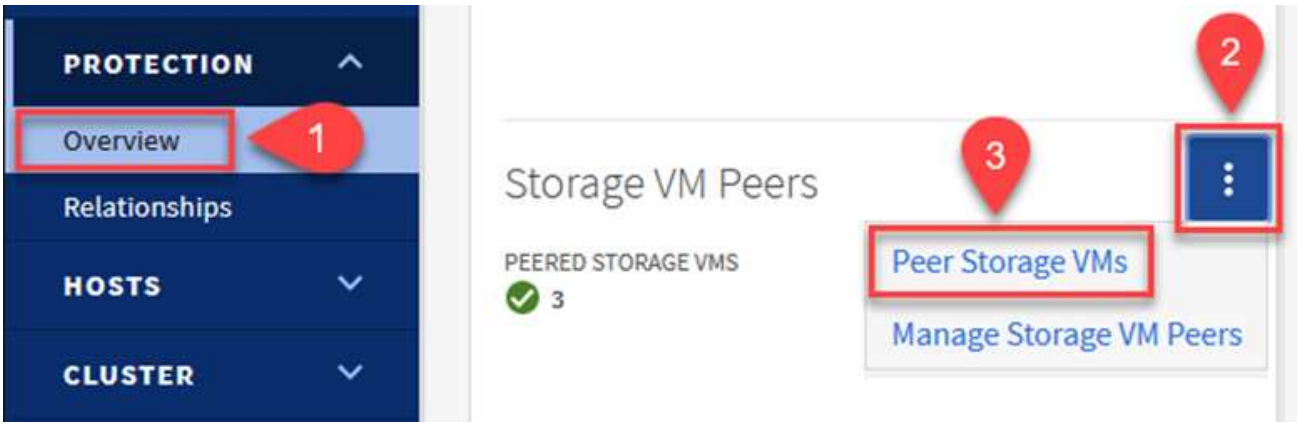
▼ 建立 **SVM** 对等关系

下一步是在包含将处于SnapMirror关系中的卷的目标存储虚拟机和源存储虚拟机之间建立 SVM 关系。

1. 从源 FSx 集群，使用 CLI 中的以下命令创建 SVM 对等关系：

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup
-peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 从源ONTAP集群，使用ONTAP系统管理器或 CLI 接受对等关系。
3. 从ONTAP系统管理器中，转到“保护”>“概览”，然后选择“存储虚拟机对等体”下的“对等存储虚拟机”。



4. 在对等存储虚拟机的对话框中，填写必填字段：
   - 源存储虚拟机
   - 目标集群
   - 目标存储虚拟机



5. 单击“对等存储虚拟机”以完成 SVM 对等连接过程。

▼ 创建快照保留策略

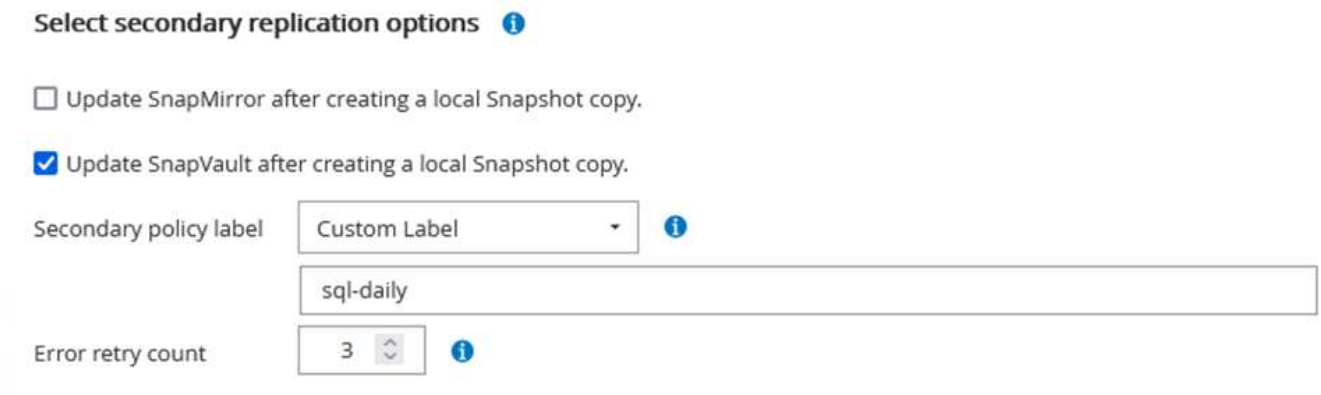
SnapCenter管理主存储系统上作为快照副本存在的备份的保留计划。这是在SnapCenter中创建策略时建立的。 SnapCenter不管理保留在二级存储系统上的备份的保留策略。这些策略通过在辅助 FSx 集群上创建

的SnapMirror策略单独进行管理，并与与源卷具有SnapMirror关系的目标卷相关联。

创建SnapCenter策略时，您可以选择指定一个辅助策略标签，该标签将添加到执行SnapCenter备份时生成的每个快照的SnapMirror标签中。

在二级存储上，这些标签与目标卷相关的策略规则相匹配，以强制保留快照。

以下示例显示了一个SnapMirror标签，该标签存在于作为用于 SQL Server 数据库和日志卷的每日备份的策略的一部分生成的所有快照上。



有关为 SQL Server 数据库创建SnapCenter策略的更多信息，请参阅 "SnapCenter文档"。

您必须首先创建一个SnapMirror策略，其中包含规定要保留的快照副本数量的规则。

1. 在 FSx 集群上创建SnapMirror策略。

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. 向具有与SnapCenter策略中指定的二级策略标签匹配的SnapMirror标签的策略添加规则。

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

以下脚本提供了可以添加到策略的规则示例：

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

为每个SnapMirror标签和要保留的快照数量（保留期）创建附加规则。

▼ 创建目标卷

要在 FSx 上创建将作为源卷快照副本接收者的目标卷，请在 FSx ONTAP上运行以下命令：

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

▼ 在源卷和目标卷之间创建**SnapMirror**关系

要在源卷和目标卷之间创建SnapMirror关系，请在 FSx ONTAP上运行以下命令：

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

▼ 初始化**SnapMirror**关系

初始化 SnapMirror 关系。此过程启动从源卷生成的新快照并将其复制到目标卷。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

在本地部署和配置 **Windows SnapCenter**服务器。

▼ 在本地部署 **Windows SnapCenter**服务器

该解决方案使用NetApp SnapCenter对 SQL Server 和 Oracle 数据库进行应用程序一致性备份。与 Veeam Backup & Replication 结合使用来备份虚拟机 VMDK，这为本地和基于云的数据中心提供了全面的灾难恢复解决方案。

SnapCenter software可从NetApp支持站点获取，并可安装在域或工作组中的 Microsoft Windows 系统上。详细的规划指南和安装说明可以在 "NetApp文档中心"。

SnapCenter software可从以下网址获取 "此链接"。

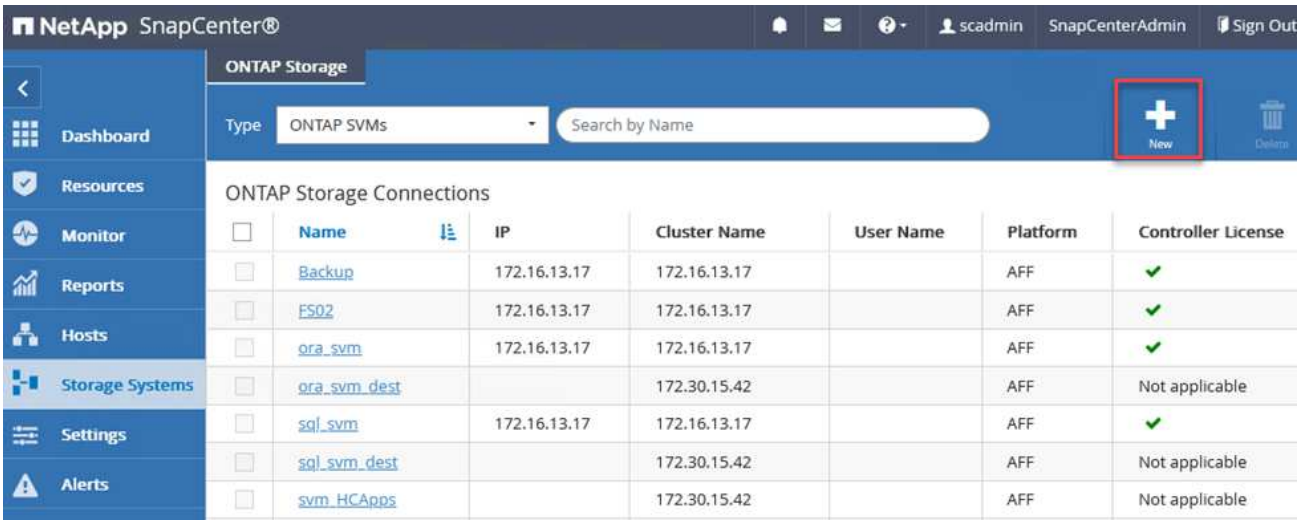
安装完成后，您可以使用 *https://Virtual_Cluster_IP_or_FQDN:8146* 从 Web 浏览器访问SnapCenter控制台。

登录控制台后，您必须配置SnapCenter以备份 SQL Server 和 Oracle 数据库。

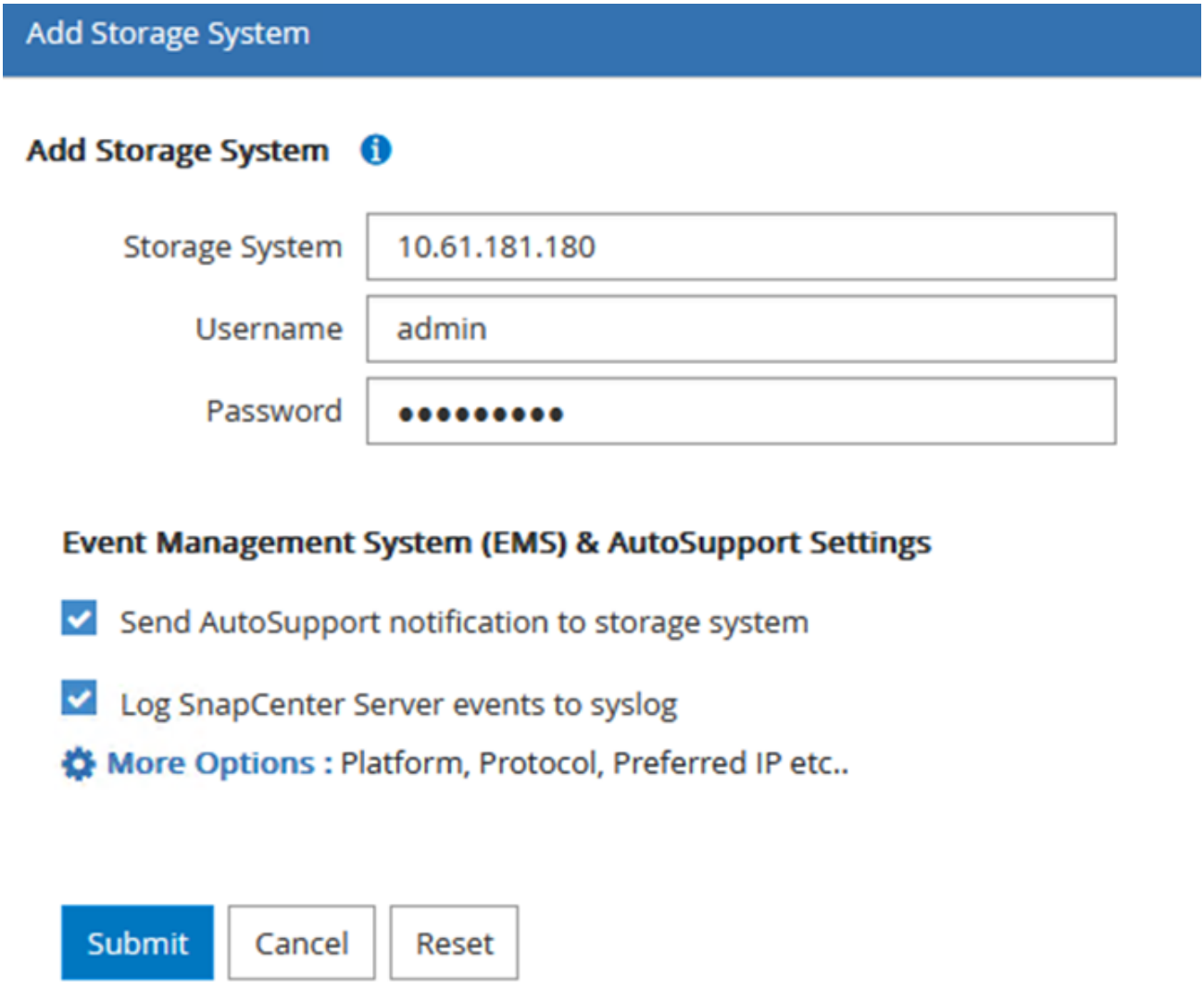
▼ 向**SnapCenter**添加存储控制器

要将存储控制器添加到SnapCenter，请完成以下步骤：

1. 从左侧菜单中，选择“存储系统”，然后单击“新建”开始将存储控制器添加到SnapCenter的过程。

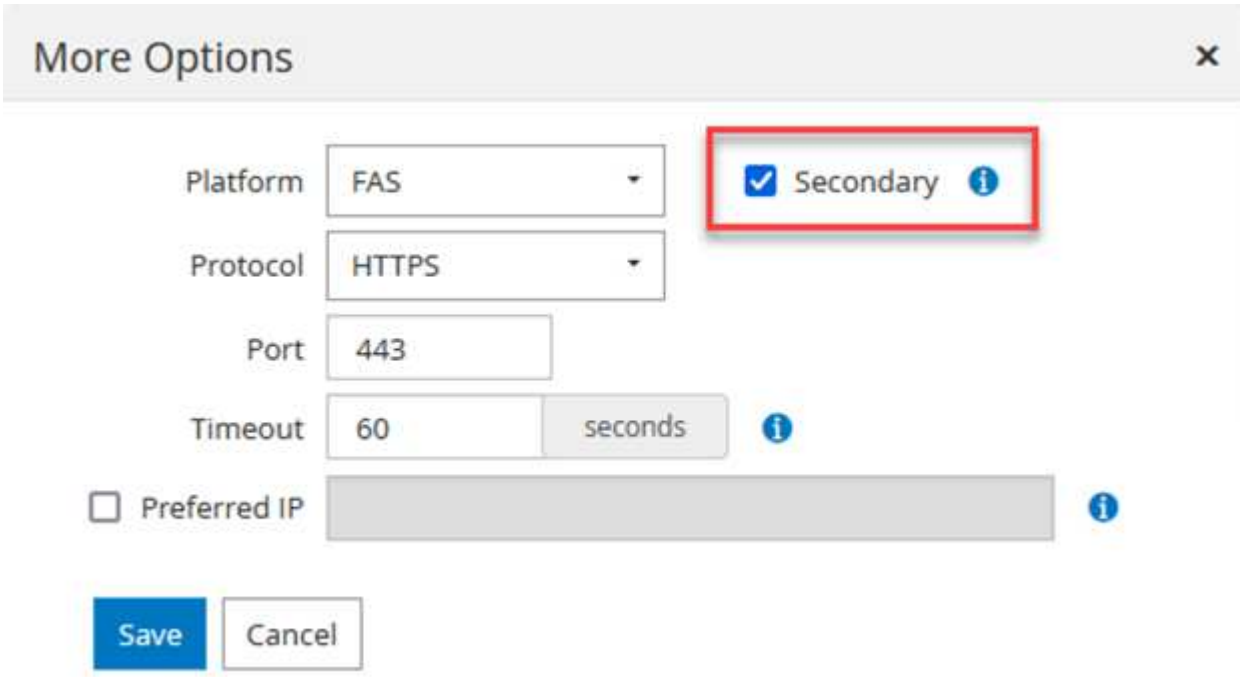


2. 在添加存储系统对话框中，添加本地ONTAP集群的管理 IP 地址以及用户名和密码。然后单击“提交”开始发现存储系统。



3. 重复此过程将 FSx ONTAP系统添加到SnapCenter。在这种情况下，选择“添加存储系统”窗口底部的“更多选项”，然后单击“辅助”复选框，将 FSx 系统指定为使用SnapMirror副本或我们的主备份快照更新的辅助

存储系统。

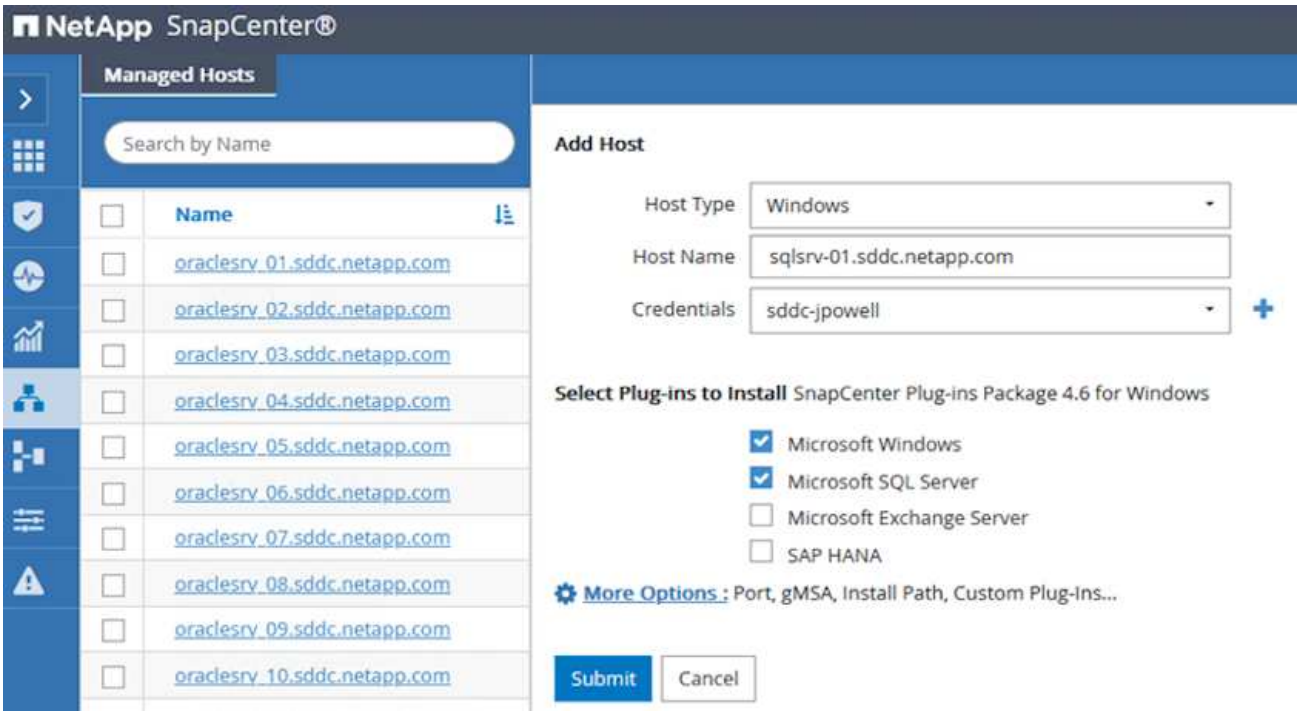


有关向SnapCenter添加存储系统的更多信息，请参阅以下文档： "此链接" 。

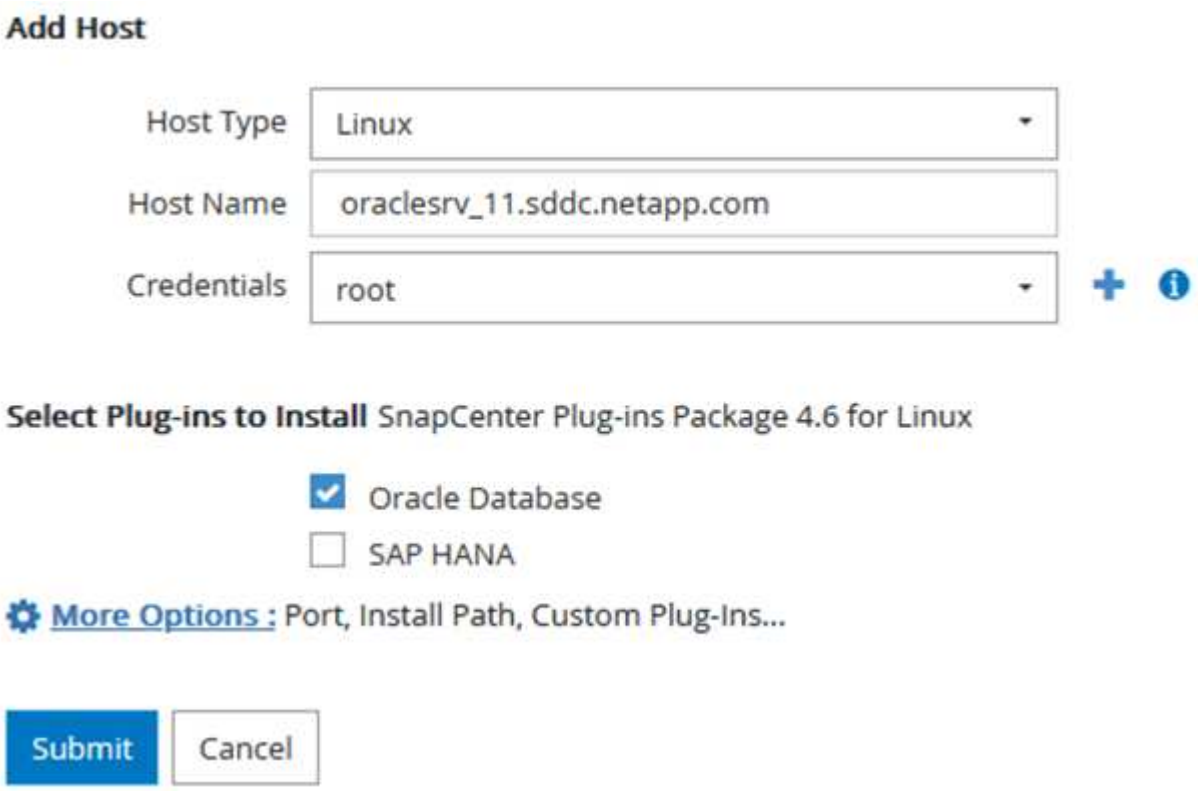
▼ 将主机添加到**SnapCenter**

下一步是将主机应用程序服务器添加到SnapCenter。 SQL Server 和 Oracle 的过程类似。

1. 从左侧菜单中，选择“主机”，然后单击“添加”以开始向SnapCenter添加存储控制器的过程。
2. 在添加主机窗口中，添加主机类型、主机名和主机系统凭据。选择插件类型。对于 SQL Server，选择 Microsoft Windows 和 Microsoft SQL Server 插件。



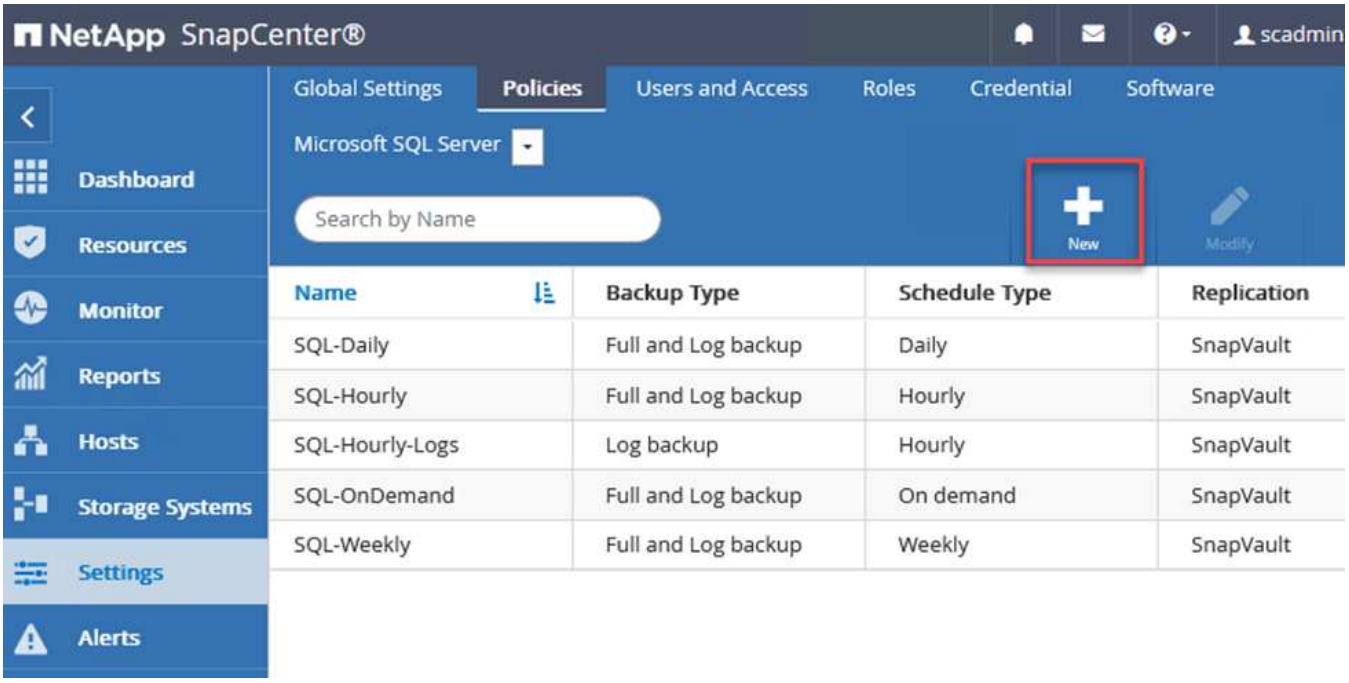
3. 对于 Oracle，请在“添加主机”对话框中填写必填字段，并选中 Oracle 数据库插件的复选框。然后单击“提交”以开始发现过程并将主机添加到SnapCenter。



▼ 创建**SnapCenter**策略

策略制定了备份工作需要遵循的具体规则。它们包括但不限于备份计划、复制类型以及SnapCenter如何处理备份和截断事务日志。

您可以在SnapCenter Web 客户端的“设置”部分访问策略。



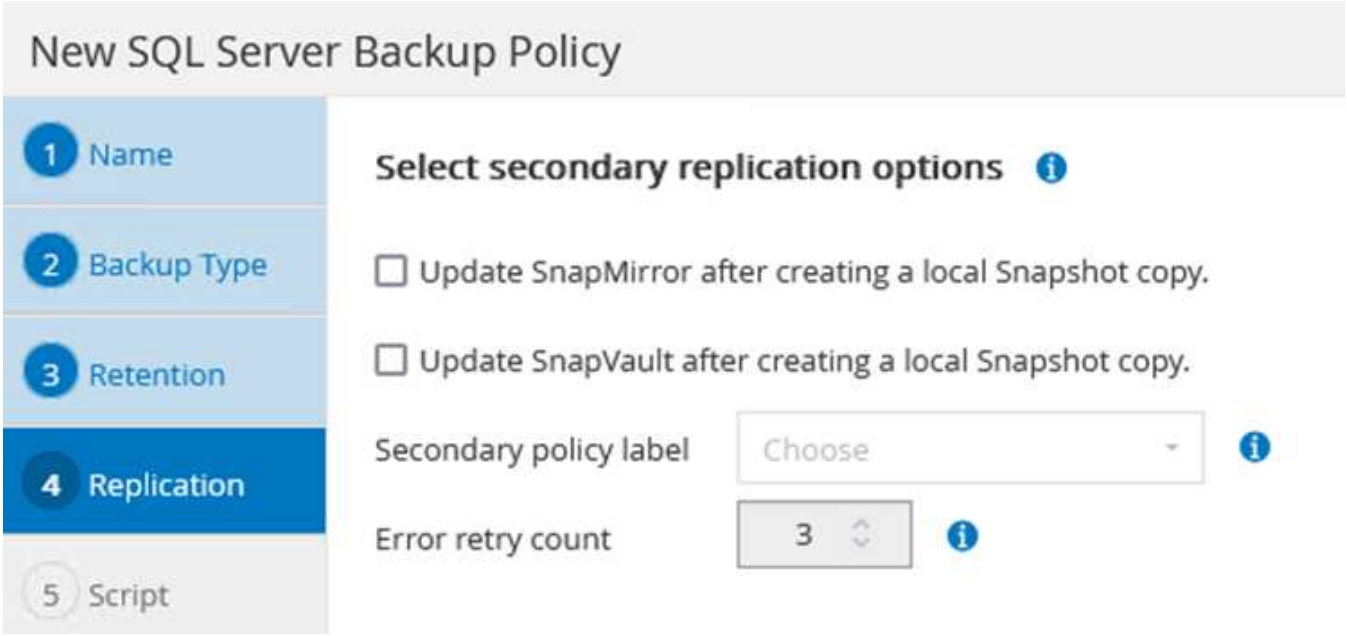
有关创建 SQL Server 备份策略的完整信息，请参阅 "SnapCenter文档"。

有关创建 Oracle 备份策略的完整信息，请参阅 "SnapCenter文档"。

笔记：

- 在您完成策略创建向导的过程中，请特别注意复制部分。在本节中，您将规定在备份过程中要获取的辅助SnapMirror副本的类型。
- “创建本地 Snapshot 副本后更新SnapMirror ”设置是指当位于同一集群上的两个存储虚拟机之间存在SnapMirror关系时更新该关系。
- “创建本地 SnapShot 副本后更新SnapVault ”设置用于更新两个独立集群之间以及本地ONTAP系统与Cloud Volumes ONTAP或 FSx ONTAP之间存在的SnapMirror关系。

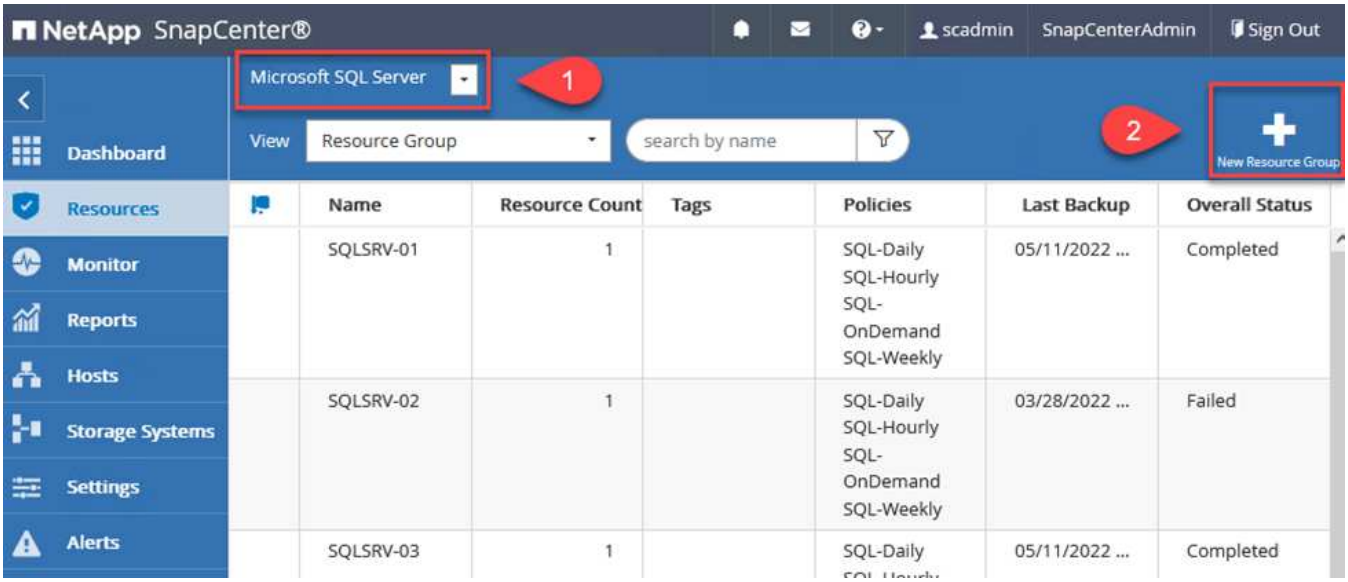
下图显示了上述选项以及它们在备份策略向导中的外观。



▼ 创建**SnapCenter**资源组

资源组允许您选择要包含在备份中的数据库资源以及这些资源遵循的策略。

1. 转到左侧菜单中的资源部分。
2. 在窗口顶部，选择要使用的资源类型（在本例中为 Microsoft SQL Server），然后单击新建资源组。



SnapCenter文档涵盖了为 SQL Server 和 Oracle 数据库创建资源组的分步详细信息。

要备份 SQL 资源，请按照 "此链接"。

要备份 Oracle 资源，请按照 "此链接"。

部署和配置 **Veeam** 备份服务器

该解决方案使用 Veeam Backup & Replication 软件来备份我们的应用程序虚拟机，并使用 Veeam 横向扩展备份存储库 (SOBR) 将备份副本存档到 Amazon S3 存储桶。在本解决方案中，Veeam 部署在 Windows 服务器上。有关部署 Veeam 的具体指导，请参阅 "Veeam 帮助中心 技术文档"。

▼ 配置 **Veeam** 横向扩展备份存储库

部署并获得软件许可后，您可以创建横向扩展备份存储库 (SOBR) 作为备份作业的目标存储。您还应该包含一个 S3 存储桶作为异地 VM 数据的备份，以实现灾难恢复。

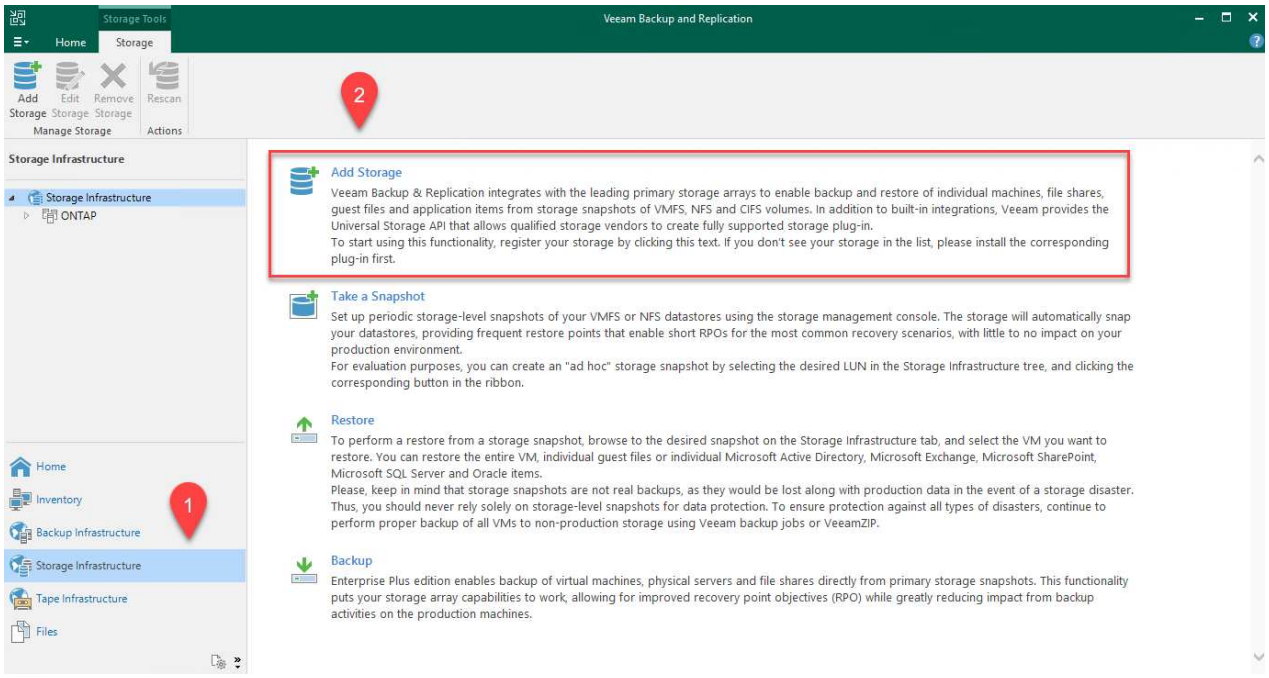
开始之前请参阅以下先决条件。

1. 在本地ONTAP系统上创建 SMB 文件共享作为备份的目标存储。
2. 创建一个 Amazon S3 存储桶以包含在 SOBR 中。这是异地备份的存储库。

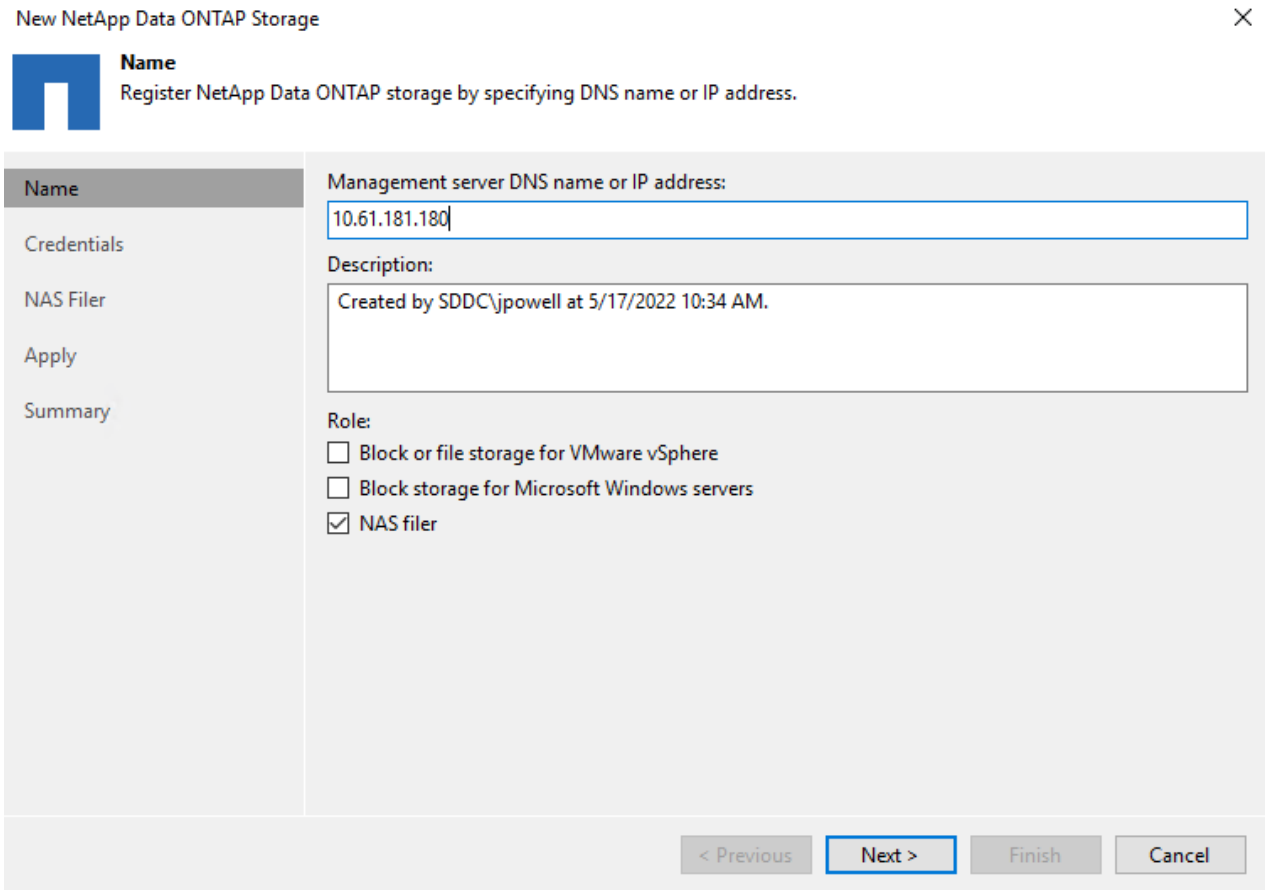
▼ 将**ONTAP**存储添加到 **Veeam**

首先，在 Veeam 中添加ONTAP存储集群和相关的 SMB/NFS 文件系统作为存储基础架构。

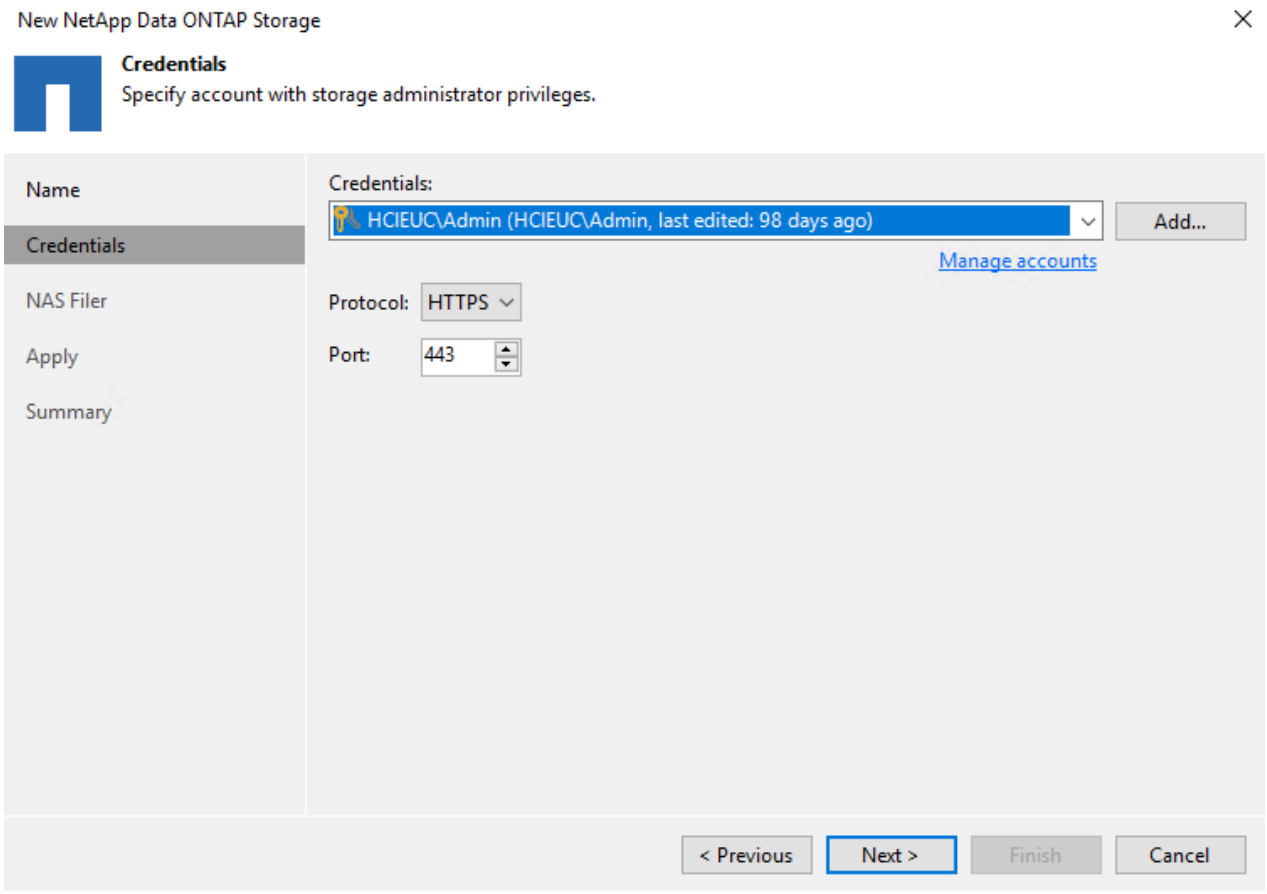
1. 打开 Veeam 控制台并登录。导航到存储基础设施，然后选择添加存储。



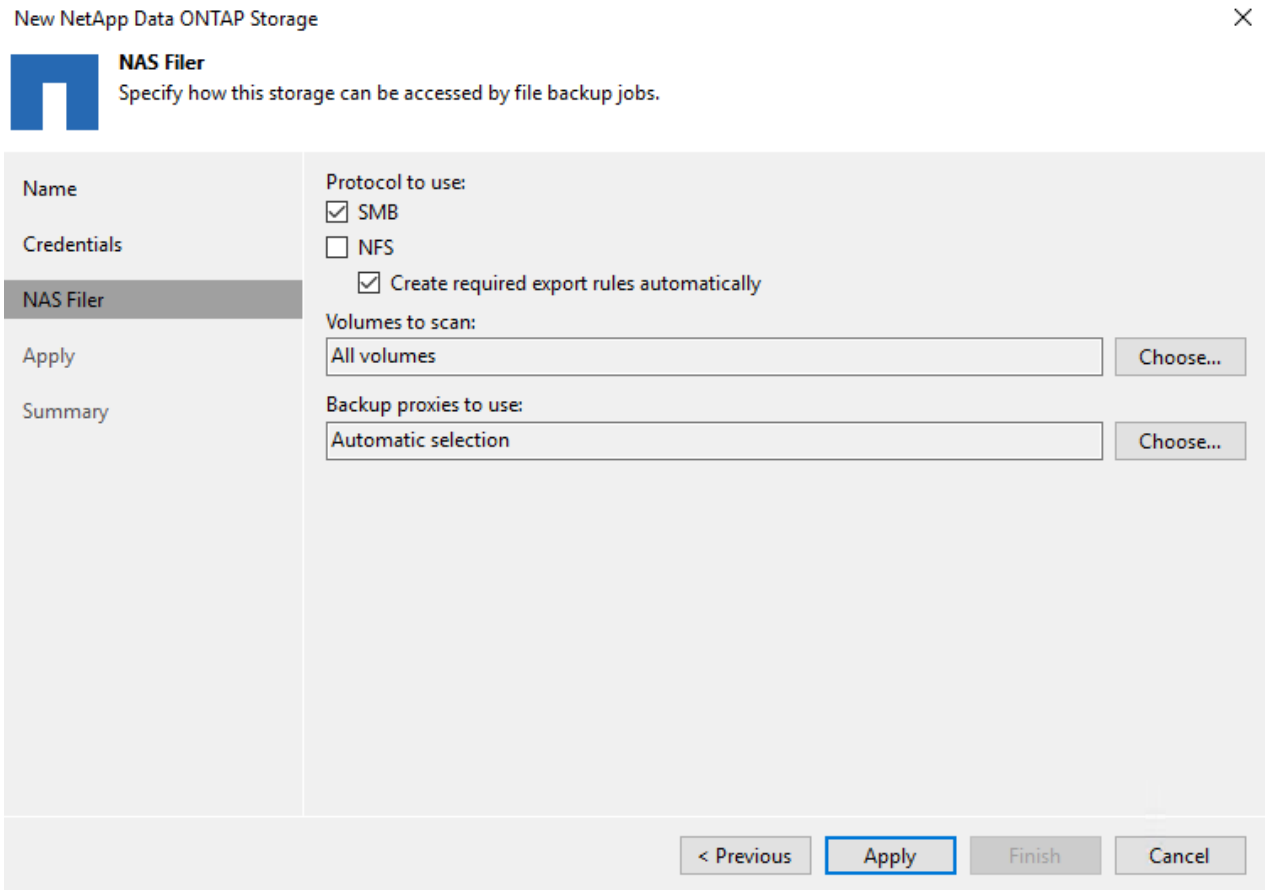
2. 在添加存储向导中，选择NetApp作为存储供应商，然后选择Data ONTAP。
3. 输入管理 IP 地址并选中 NAS Filer 框。单击“下一步”。



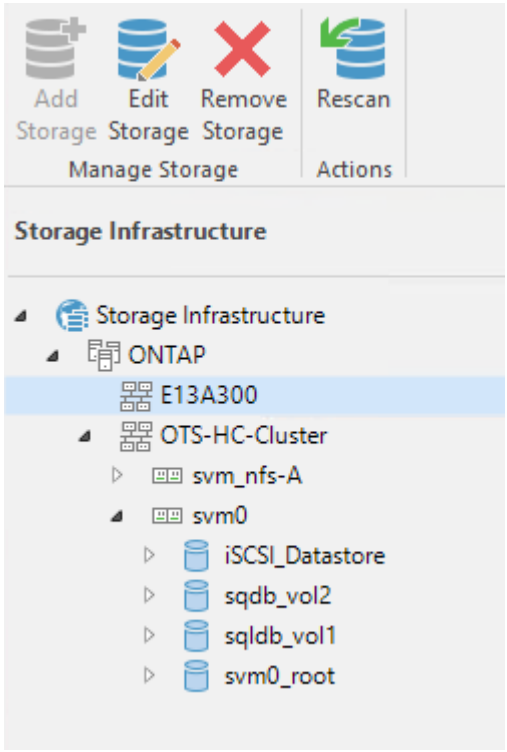
4. 添加您的凭据以访问ONTAP集群。



5. 在 NAS Filer 页面上，选择要扫描的协议，然后选择下一步。

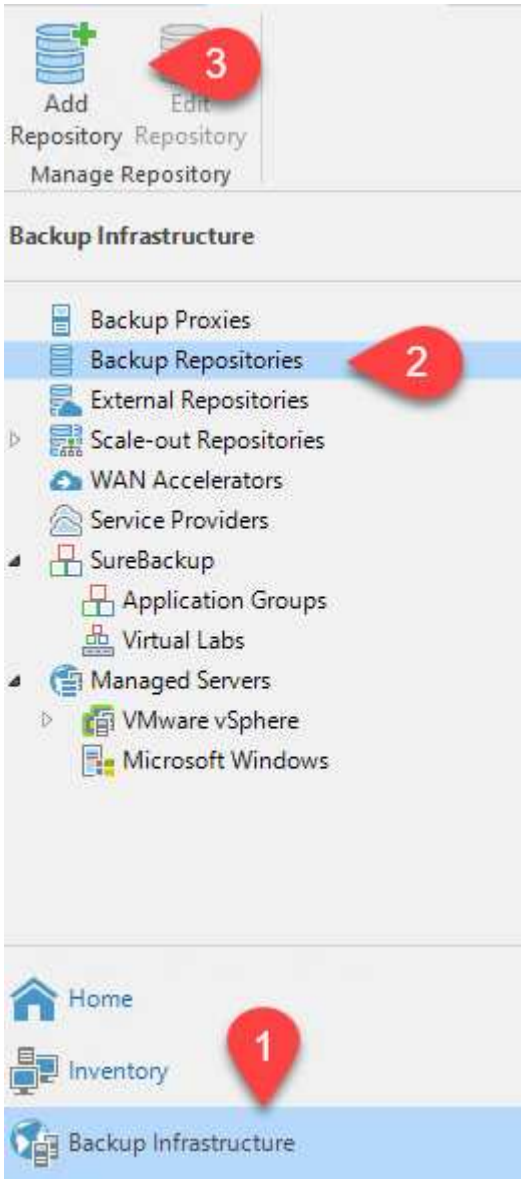


6. 完成向导的“应用”和“摘要”页面，然后单击“完成”以开始存储发现过程。扫描完成后， ONTAP集群将与 NAS 文件服务器一起添加为可用资源。

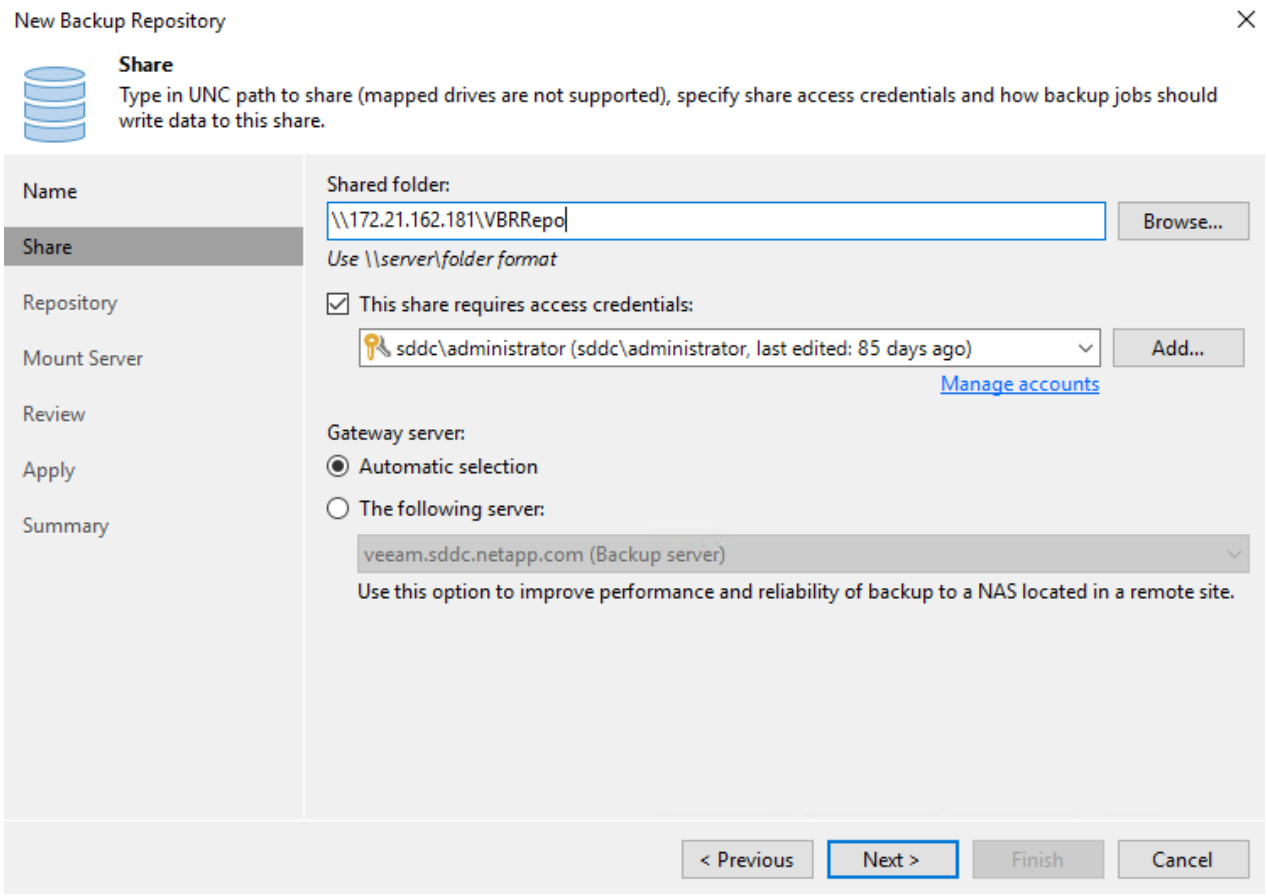


7. 使用新发现的 NAS 共享创建备份存储库。从备份基础架构中，选择备份存储库并单击添加存储库菜单

项。



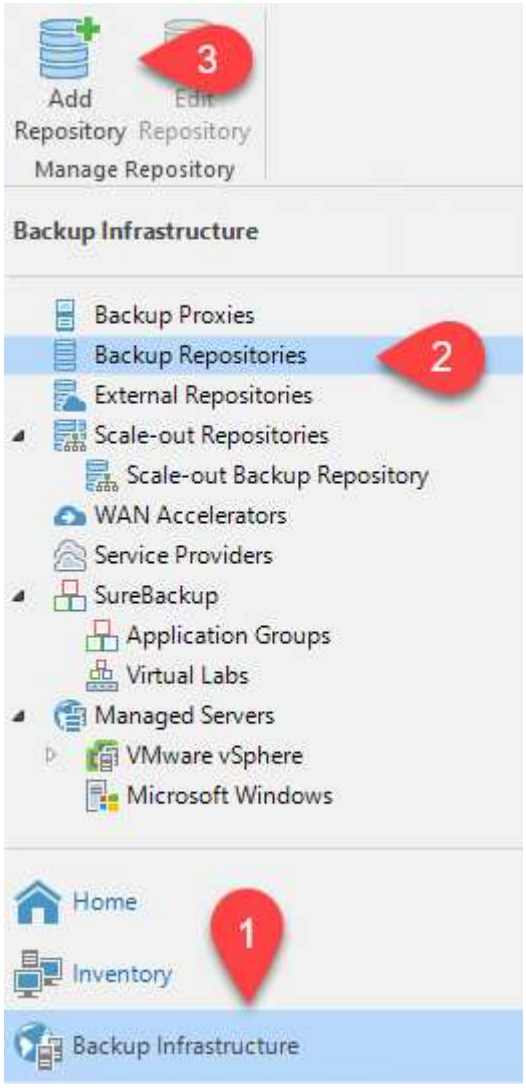
8. 按照新建备份存储库向导中的所有步骤来创建存储库。有关创建 Veeam Backup 存储库的详细信息，请参阅 "Veeam 文档"。



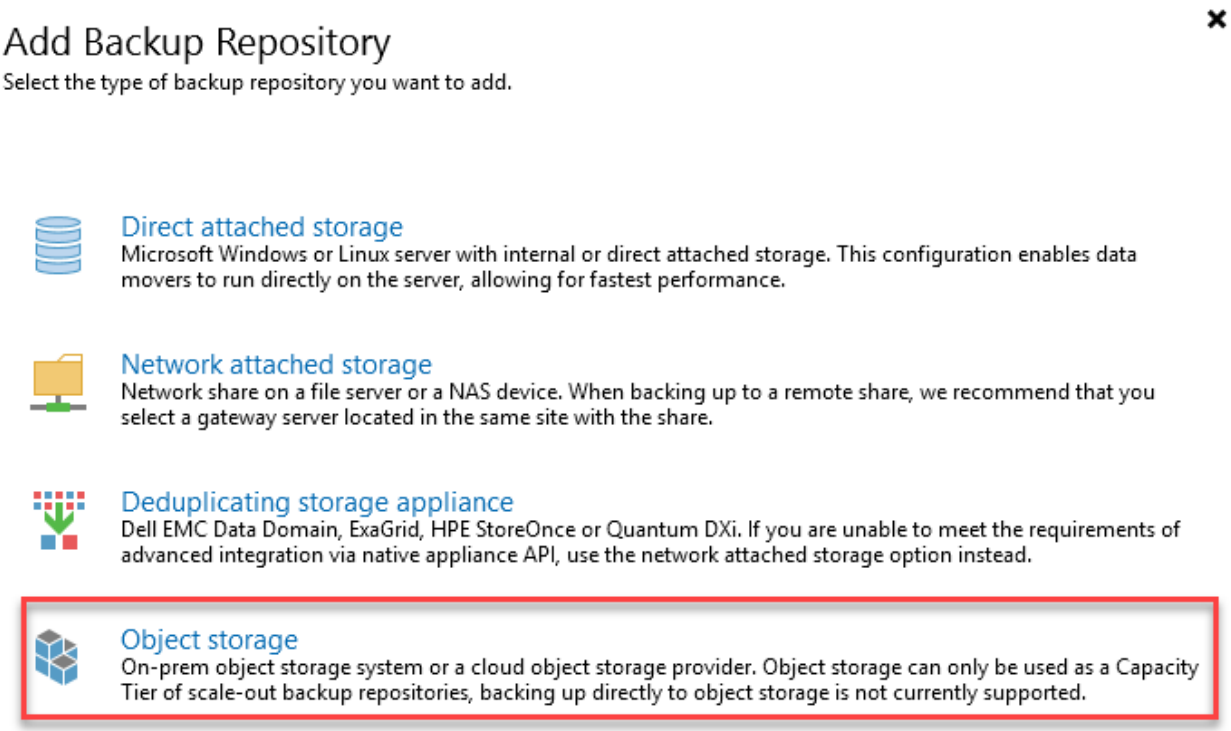
▼ 添加 **Amazon S3** 存储桶作为备份存储库

下一步是添加 Amazon S3 存储作为备份存储库。

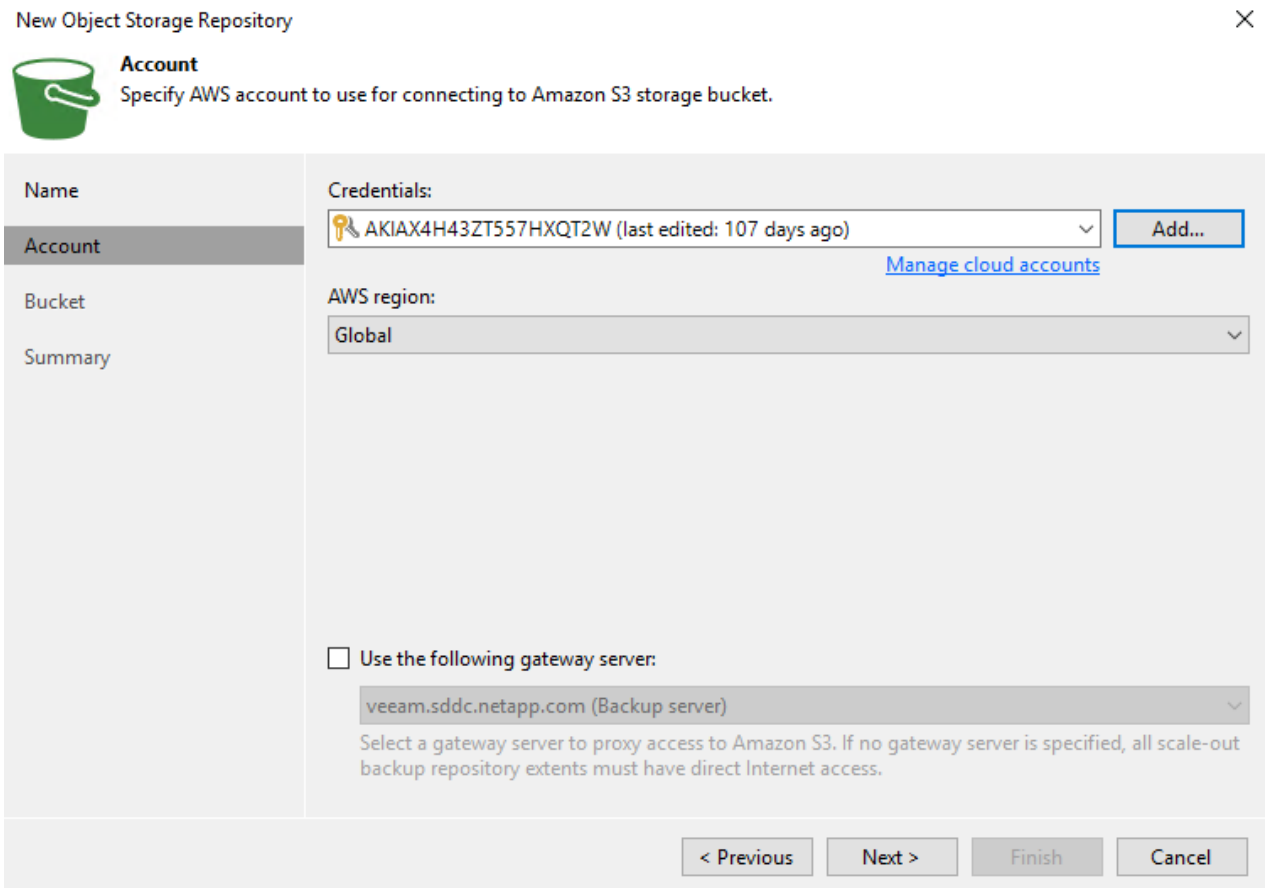
1. 导航到备份基础设施 > 备份存储库。单击添加存储库。



2. 在添加备份存储库向导中，选择对象存储，然后选择 Amazon S3。这将启动新对象存储库向导。



3. 为您的对象存储库提供一个名称，然后单击下一步。
4. 在下一部分中，提供您的凭据。您需要一个 AWS 访问密钥和密钥。



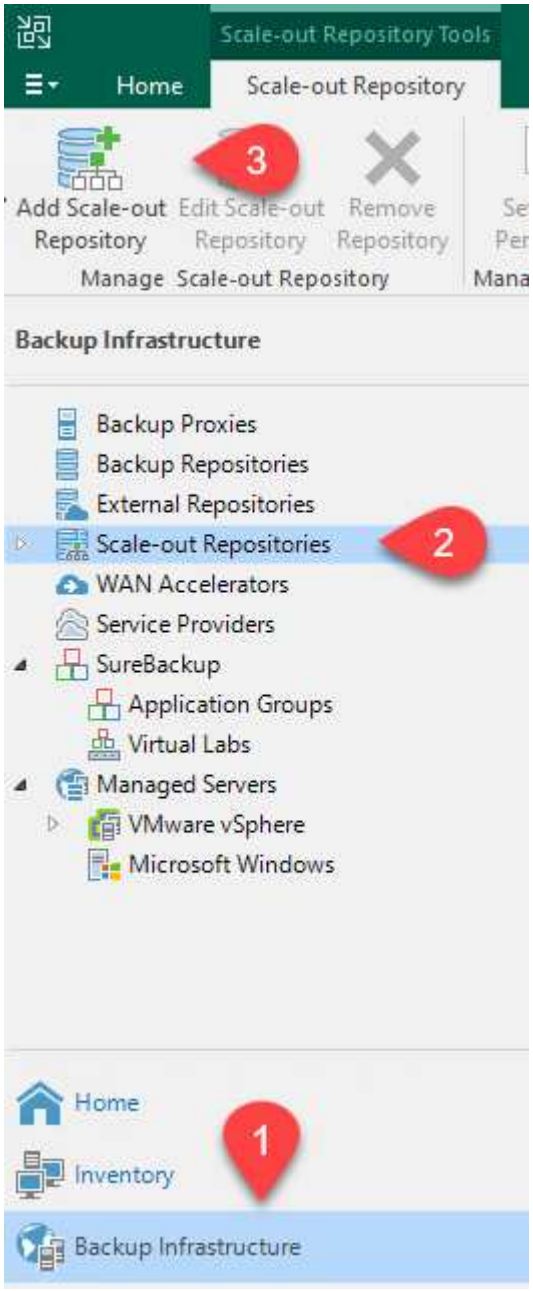
5. 加载 Amazon 配置后，选择您的数据中心、存储桶和文件夹，然后单击“应用”。最后，单击“完成”关闭

向导。

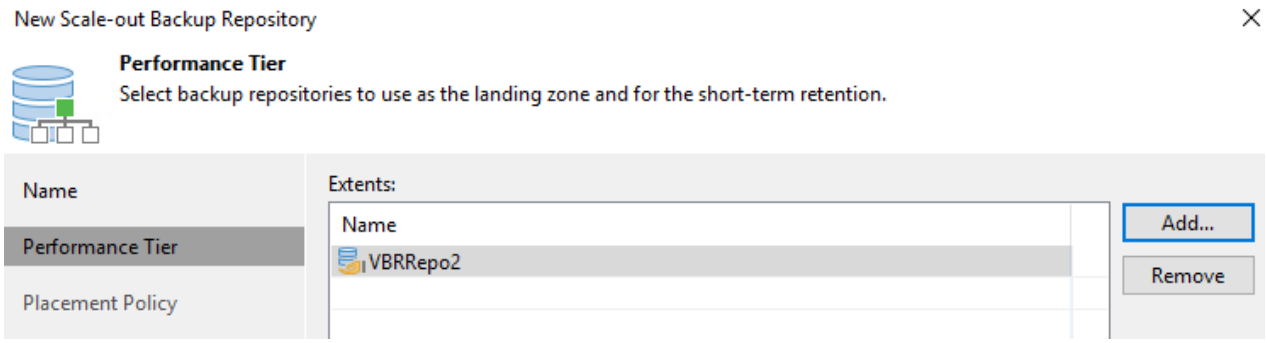
▼ 创建横向扩展备份存储库

现在我们已经将存储库添加到 Veeam，我们可以创建 SOBR 来自动将备份副本分层到我们的异地 Amazon S3 对象存储中，以实现灾难恢复。

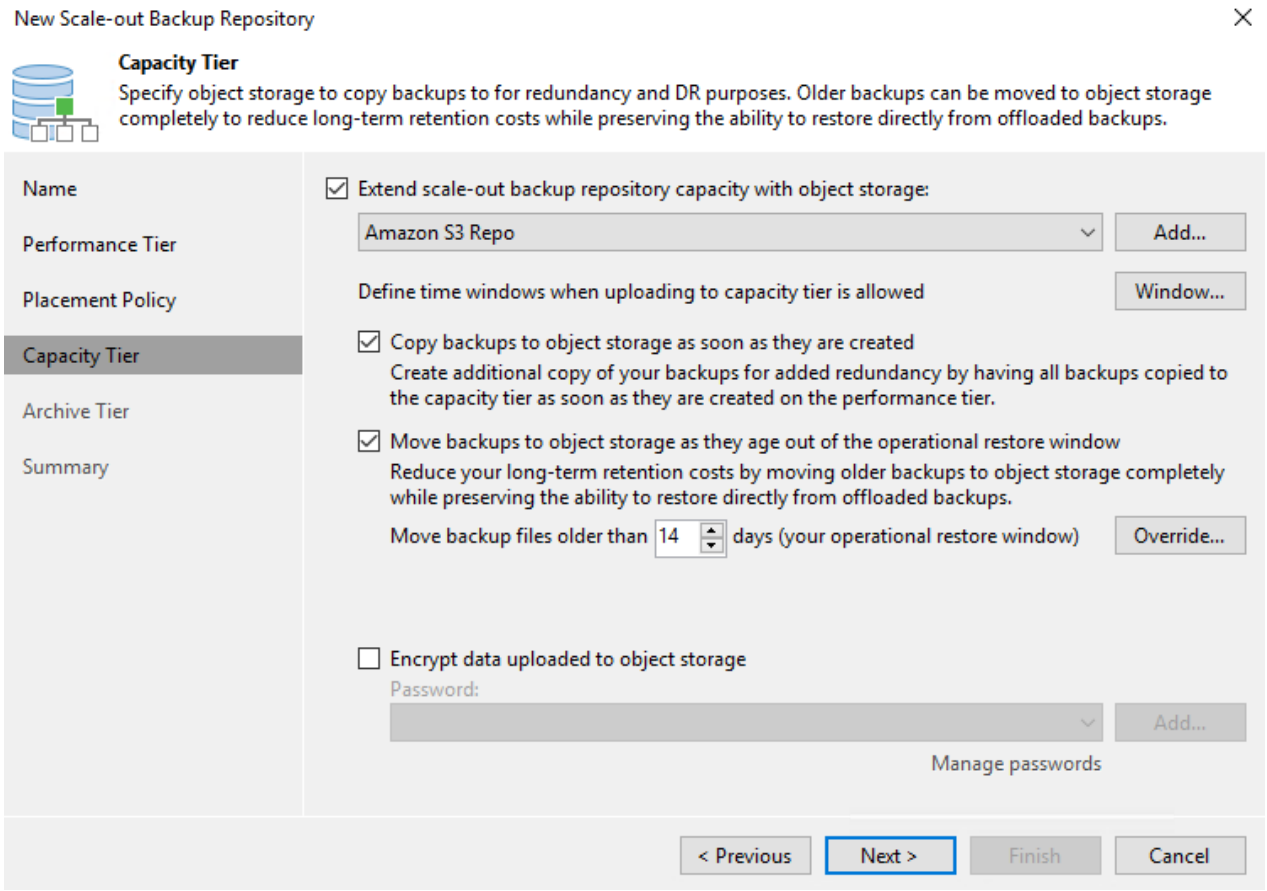
1. 从备份基础架构中，选择扩展存储库，然后单击添加扩展存储库菜单项。



2. 在新的横向扩展备份存储库中为 SOBR 提供一个名称，然后单击下一步。
3. 对于性能层，选择包含位于本地ONTAP集群上的 SMB 共享的备份存储库。



4. 对于放置策略，请根据您的要求选择数据局部性或性能。选择下一步。
5. 对于容量层，我们使用 Amazon S3 对象存储扩展 SOBR。为了实现灾难恢复，请选择“在创建备份后立即将其复制到对象存储”，以确保及时交付我们的二次备份。



6. 最后，选择“应用”和“完成”以完成 SOBR 的创建。

▼ 创建横向扩展备份存储库作业

配置 Veeam 的最后一步是使用新创建的 SOBR 作为备份目标来创建备份作业。创建备份作业是任何存储管理员的正常工作的一部分，我们在此不介绍详细步骤。有关在 Veeam 中创建备份作业的更多完整信息，请参阅 "Veeam 帮助中心技术文档"。

NetApp Backup and Recovery 工具及配置

要将应用程序虚拟机和数据库卷故障转移到在 AWS 中运行的 VMware Cloud Volume 服务，您必须安装并配置SnapCenter Server 和 Veeam Backup and Replication Server 的运行实例。故障转移完成后，您还必须配置

这些工具以恢复正常的备份操作，直到计划并执行故障恢复到本地数据中心。

▼ 部署辅助 **Windows SnapCenter**服务器

SnapCenter Server 部署在 VMware Cloud SDDC 中，或安装在与 VMware Cloud 环境具有网络连接的 VPC 中的 EC2 实例上。

SnapCenter software可从NetApp支持站点获取，并可安装在域或工作组中的 Microsoft Windows 系统上。详细的规划指南和安装说明可以在 "NetApp文档中心"。

您可以在以下位置找到SnapCenter software "此链接"。

▼ 配置辅助 **Windows SnapCenter**服务器

要执行镜像到 FSx ONTAP 的应用程序数据还原，您必须首先执行本地SnapCenter数据库的完整还原。此过程完成后，将重新建立与虚拟机的通信，并且现在可以使用 FSx ONTAP作为主存储恢复应用程序备份。

为此，您必须在SnapCenter服务器上完成以下项目：

1. 将计算机名称配置为与原始本地SnapCenter服务器相同。
2. 配置网络以与 VMware Cloud 和 FSx ONTAP实例通信。
3. 完成恢复SnapCenter数据库的过程。
4. 确认SnapCenter处于灾难恢复模式，以确保 FSx 现在是备份的主要存储。
5. 确认已与恢复的虚拟机重新建立通信。

▼ 部署辅助 **Veeam Backup & Replication** 服务器

您可以在 AWS 上的 VMware Cloud 中的 Windows 服务器或 EC2 实例上安装 Veeam Backup & Replication 服务器。有关详细的实施指南，请参阅 "Veeam 帮助中心技术文档"。

▼ 配置辅助 **Veeam Backup & Replication** 服务器

要对已备份到 Amazon S3 存储的虚拟机进行还原，必须在 Windows 服务器上安装 Veeam Server，并将其配置为与 VMware Cloud、FSx ONTAP和包含原始备份存储库的 S3 存储桶通信。它还必须在 FSx ONTAP上配置一个新的备份存储库，以便在虚拟机恢复后进行新的备份。

要执行此过程，必须完成以下项目：

1. 配置网络以与 VMware Cloud、FSx ONTAP和包含原始备份存储库的 S3 存储桶进行通信。
2. 将 FSx ONTAP上的 SMB 共享配置为新的备份存储库。
3. 安装用作本地扩展备份存储库一部分的原始 S3 存储桶。
4. 恢复虚拟机后，建立新的备份作业来保护 SQL 和 Oracle 虚拟机。

有关使用 Veeam 恢复虚拟机的更多信息，请参阅"使用 Veeam Full Restore 恢复应用程序虚拟机"。

SnapCenter数据库备份用于灾难恢复

SnapCenter允许备份和恢复其底层 MySQL 数据库和配置数据，以便在发生灾难时恢复SnapCenter服务器。对于我们的解决方案，我们恢复了位于我们的 VPC 中的 AWS EC2 实例上的SnapCenter数据库和配置。有关SnapCenter灾难恢复的更多信息，请参阅 "此链接"。

▼ **SnapCenter**备份前提条件

SnapCenter备份需要满足以下先决条件：

- 在本地ONTAP系统上创建的卷和 SMB 共享，用于定位备份数据库和配置文件。
- 本地ONTAP系统与 AWS 账户中的 FSx 或 CVO 之间的SnapMirror关系。此关系用于传输包含备份的SnapCenter数据库和配置文件的快照。
- 安装在云帐户中的 Windows Server，可以在 EC2 实例上，也可以在 VMware Cloud SDDC 中的 VM 上。
- SnapCenter安装在 VMware Cloud 中的 Windows EC2 实例或 VM 上。

▼ **SnapCenter**备份和还原过程摘要

- 在本地ONTAP系统上创建一个卷，用于托管备份数据库和配置文件。
- 在本地和 FSx/CVO 之间建立SnapMirror关系。
- 挂载 SMB 共享。
- 检索用于执行 API 任务的 Swagger 授权令牌。
- 启动数据库恢复过程。
- 使用 xcopy 实用程序将 db 和配置文件本地目录复制到 SMB 共享。
- 在 FSx 上，创建ONTAP卷的克隆（通过SnapMirror从本地复制）。
- 将 SMB 共享从 FSx 挂载到 EC2/VMware Cloud。
- 将恢复目录从 SMB 共享复制到本地目录。
- 从 Swagger 运行 SQL Server 还原过程。

▼ 备份**SnapCenter**数据库和配置

SnapCenter提供了一个用于执行 REST API 命令的 Web 客户端界面。有关通过 Swagger 访问 REST API 的信息，请参阅SnapCenter文档 "此链接"。

▼ 登录**Swagger**并获取授权令牌

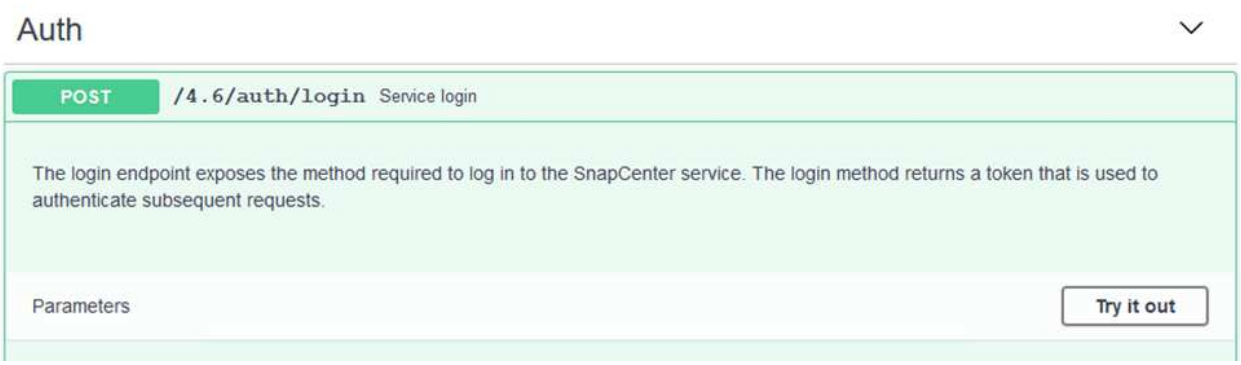
导航到 Swagger 页面后，您必须检索授权令牌才能启动数据库恢复过程。

1. 访问SnapCenter Swagger API 网页，地址为 *https://< SnapCenter*服务器 *IP>:8146/swagger/*。

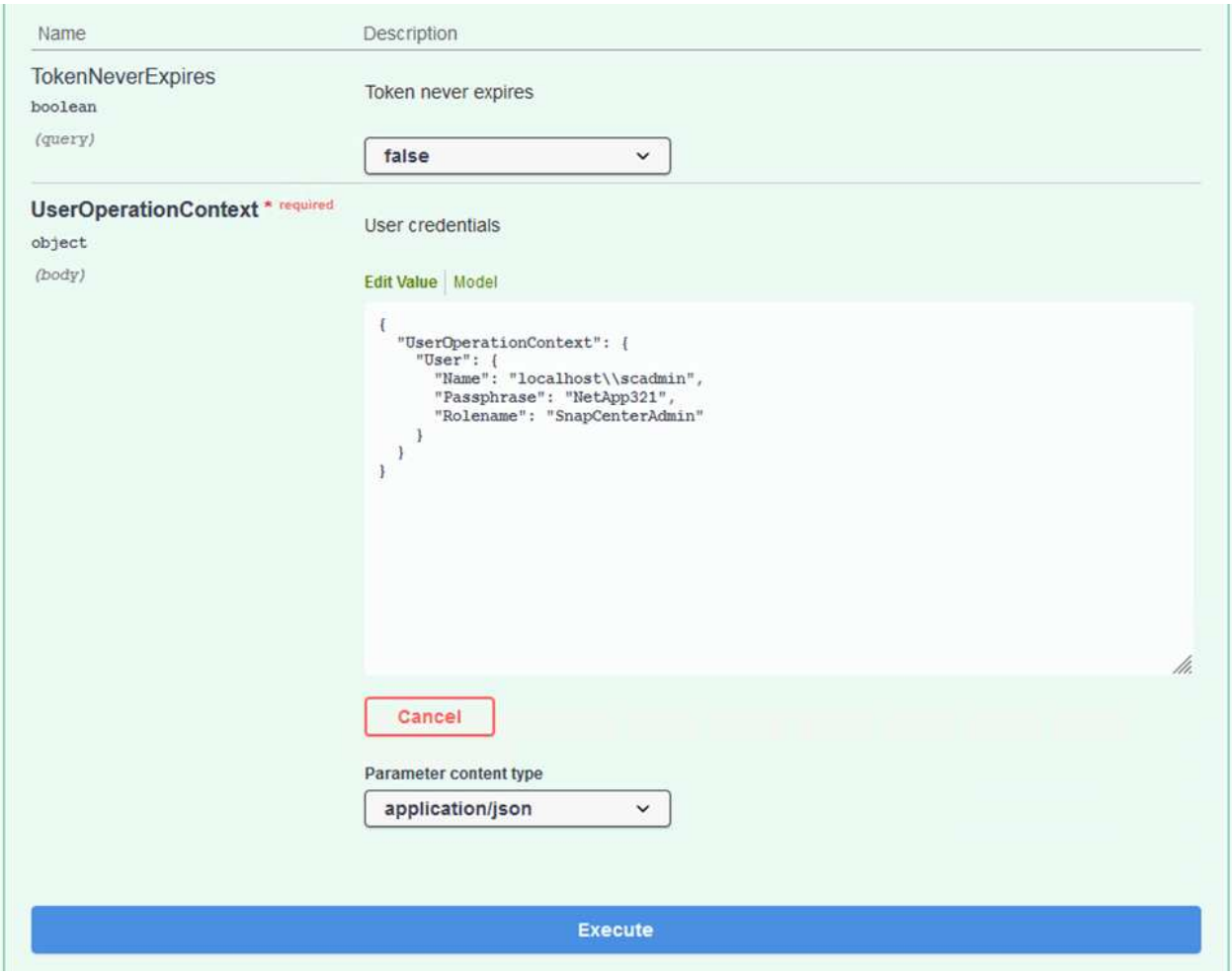




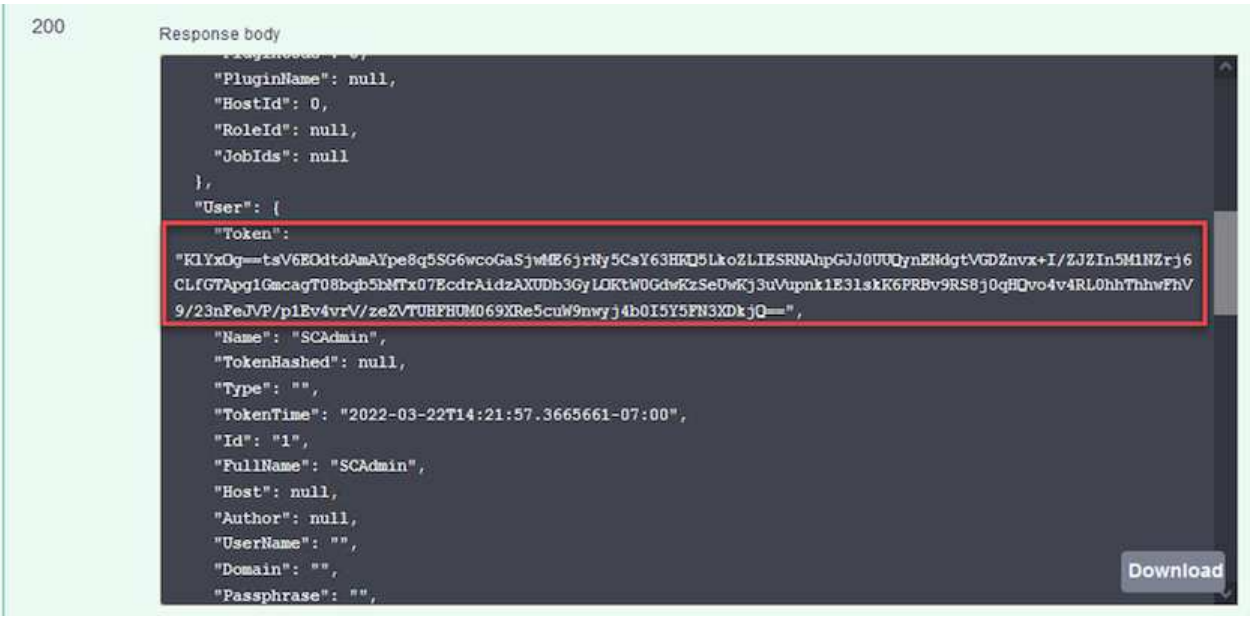
2. 展开“Auth”部分并单击“Try it Out”。



3. 在 UserOperationContext 区域，填写SnapCenter凭据和角色，然后单击“执行”。



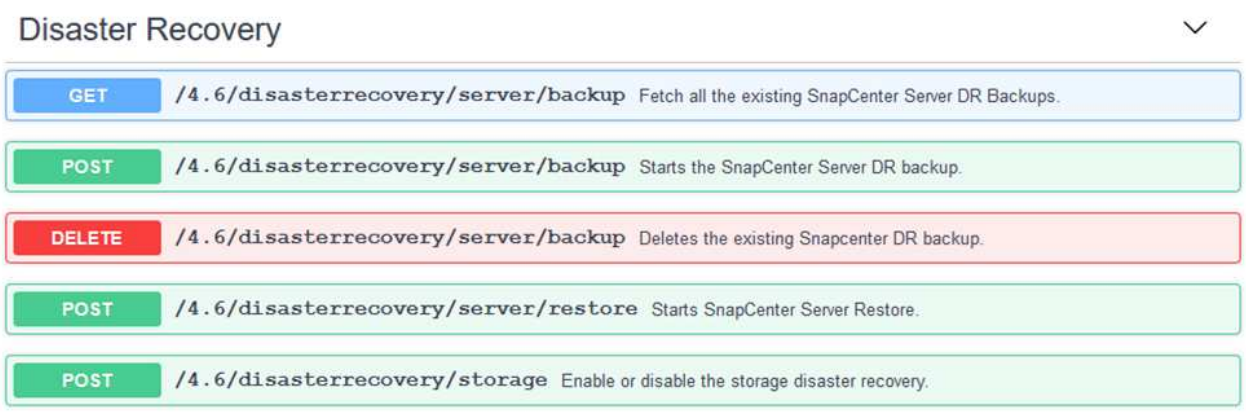
4. 在下面的响应主体中，您可以看到令牌。执行备份过程时复制令牌文本以进行身份验证。



▼ 执行**SnapCenter**数据库备份

接下来转到 Swagger 页面上的灾难恢复区域以开始SnapCenter备份过程。

1. 单击“灾难恢复”区域以展开它。

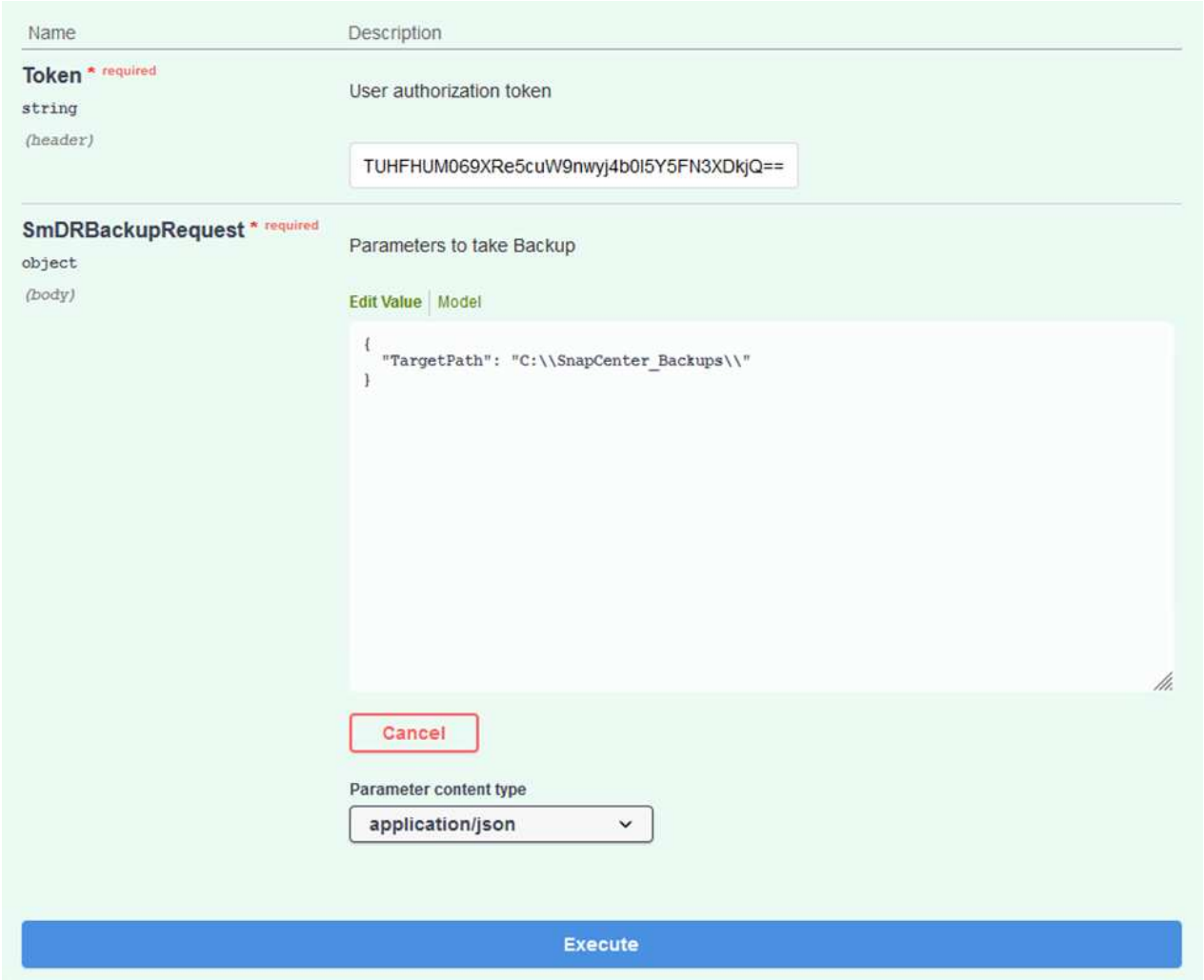


2. 展开 `/4.6/disasterrecovery/server/backup`部分并单击“试用”。



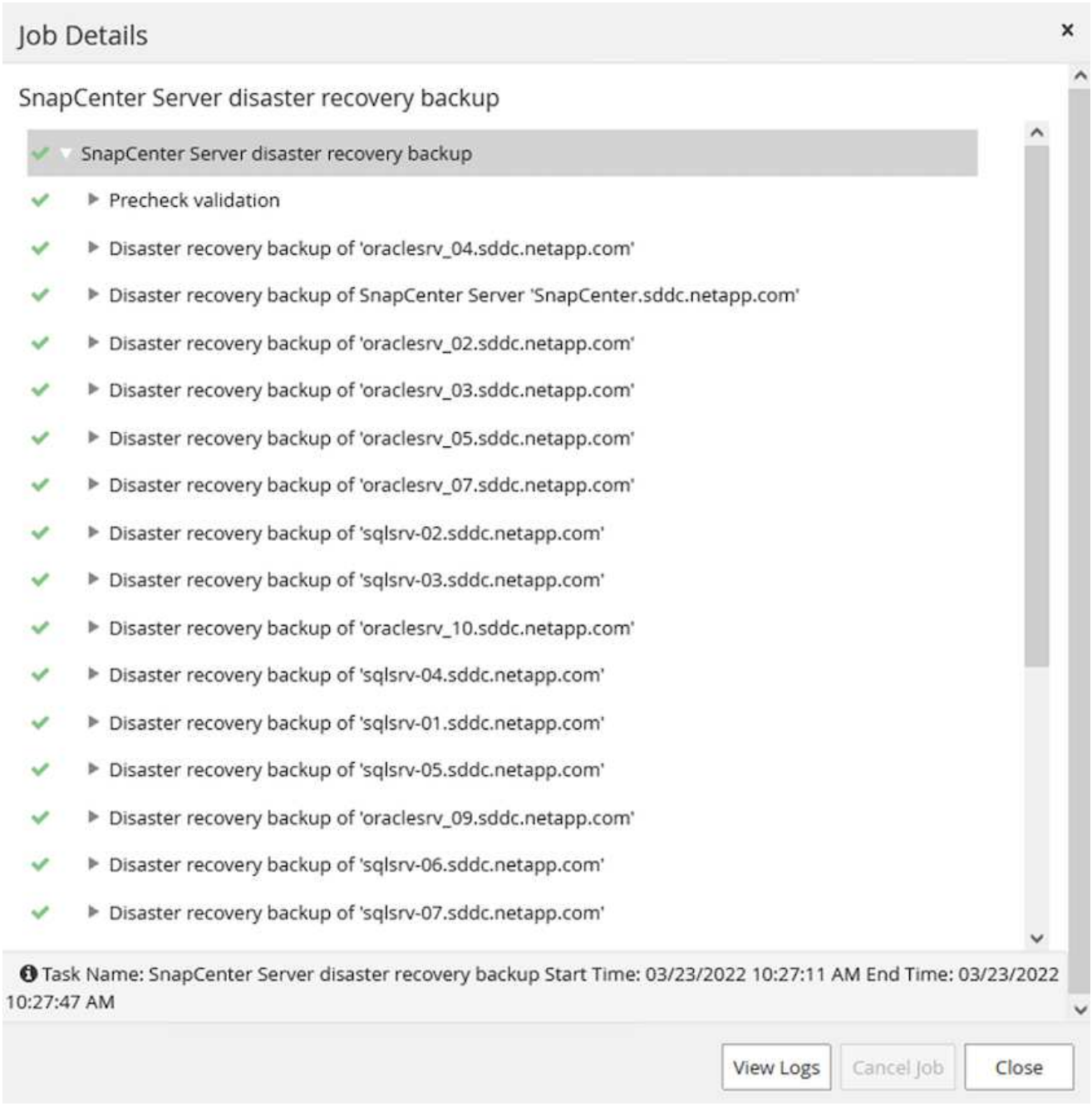
3. 在 SmDRBackupRequest 部分中，添加正确的本地目标路径并选择执行以启动SnapCenter数据库和配置的备份。

备份过程不允许直接备份到 NFS 或 CIFS 文件共享。



▼ 从**SnapCenter**监控备份作业

在启动数据库还原过程时登录SnapCenter查看日志文件。在“监视”部分下，您可以查看SnapCenter服务器灾难恢复备份的详细信息。



▼ 使用 **XCOPY** 实用程序将数据库备份文件复制到 **SMB** 共享

接下来，您必须将备份从SnapCenter服务器上的本地驱动器移动到 CIFS 共享，该共享用于将数据通过SnapMirror复制到位于 AWS 中 FSx 实例上的辅助位置。使用带有特定选项的 xcopy 来保留文件的权限。

以管理员身份打开命令提示符。在命令提示符下，输入以下命令：

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X /E
/H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O /X
/E /H /K
```

▼ 主站点发生灾难

对于发生在主本地数据中心的灾难，我们的场景包括使用 VMware Cloud on AWS 将故障转移到位于 Amazon Web Services 基础架构上的辅助站点。我们假设虚拟机和我们的内部ONTAP集群不再可访问。此外， SnapCenter和 Veeam 虚拟机都不再可访问，必须在我们的辅助站点上重建。

本节讨论将我们的基础设施故障转移到云端，并涵盖以下主题：

- SnapCenter数据库还原。建立新的SnapCenter服务器后，恢复 MySQL 数据库和配置文件，并将数据库切换到灾难恢复模式，以允许辅助 FSx 存储成为主存储设备。
- 使用 Veeam Backup & Replication 恢复应用程序虚拟机。连接包含 VM 备份的 S3 存储，导入备份，然后将其还原到 VMware Cloud on AWS。
- 使用SnapCenter还原 SQL Server 应用程序数据。
- 使用SnapCenter恢复 Oracle 应用程序数据。

▼ **SnapCenter**数据库还原过程

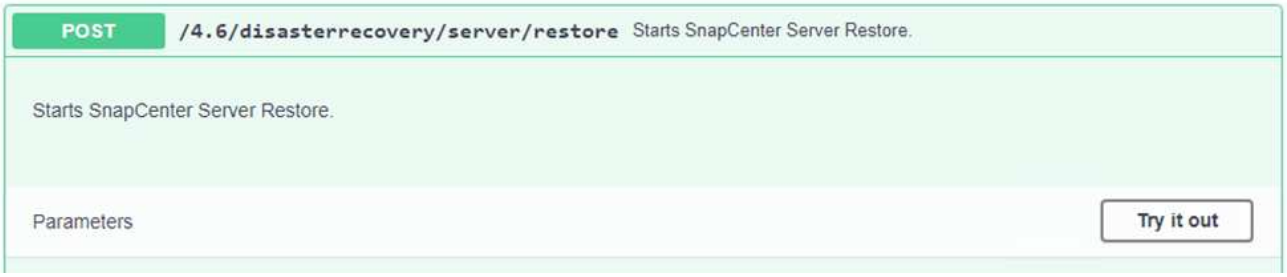
SnapCenter通过允许备份和恢复其 MySQL 数据库和配置文件来支持灾难恢复场景。这允许管理员在本地数据中心维护SnapCenter数据库的定期备份，然后将该数据库还原到辅助SnapCenter数据库。

要访问远程SnapCenter服务器上的SnapCenter备份文件，请完成以下步骤：

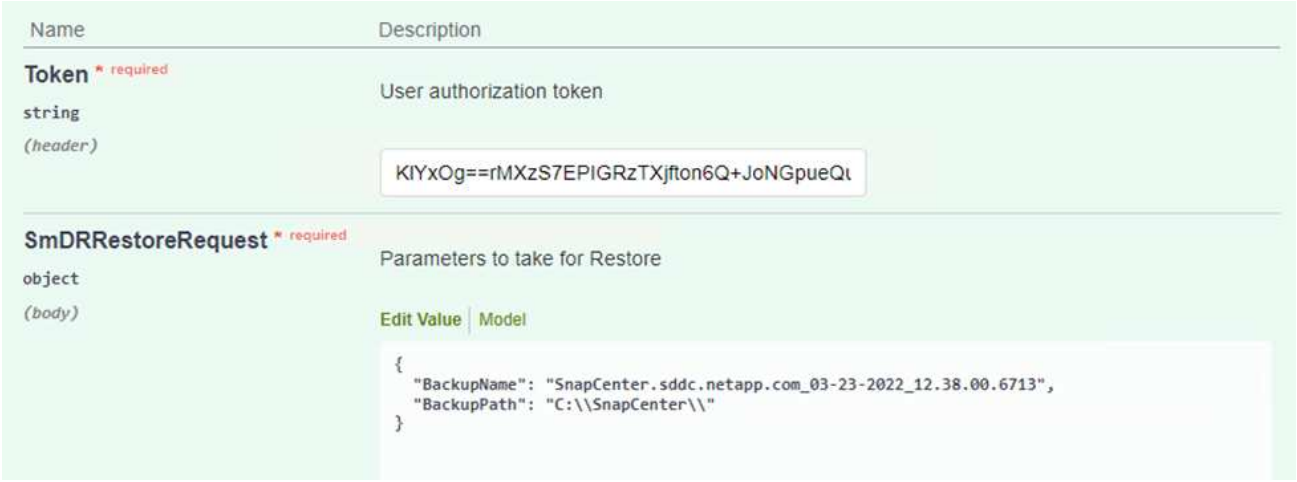
1. 断开与 FSx 集群的SnapMirror关系，这使得卷可读/写。
2. 创建 CIFS 服务器（如有必要）并创建指向克隆卷连接路径的 CIFS 共享。
3. 使用 xcopy 将备份文件复制到辅助SnapCenter系统上的本地目录。
4. 安装SnapCenter v4.6。
5. 确保SnapCenter服务器与原始服务器具有相同的 FQDN。这是数据库恢复成功所必需的。

要开始恢复过程，请完成以下步骤：

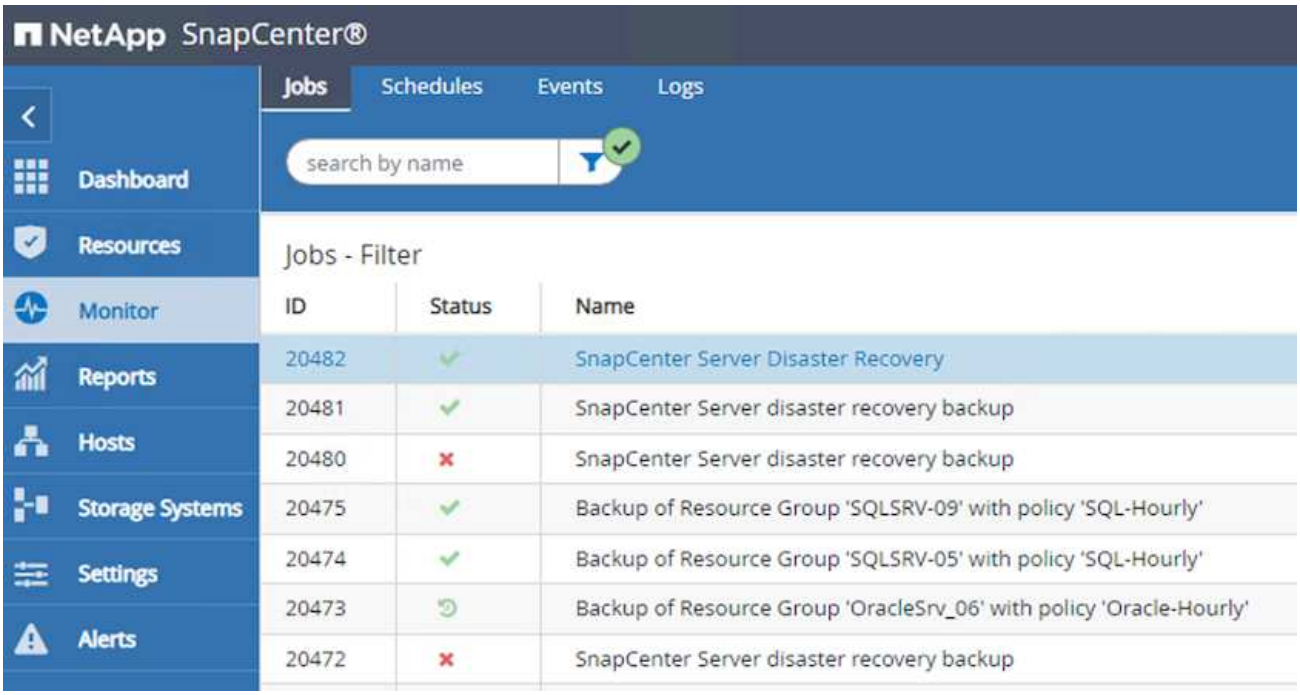
1. 导航到辅助SnapCenter服务器的 Swagger API 网页，并按照前面的说明获取授权令牌。
2. 导航到 Swagger 页面的灾难恢复部分，选择 `/4.6/disasterrecovery/server/restore`，然后单击“试用”。

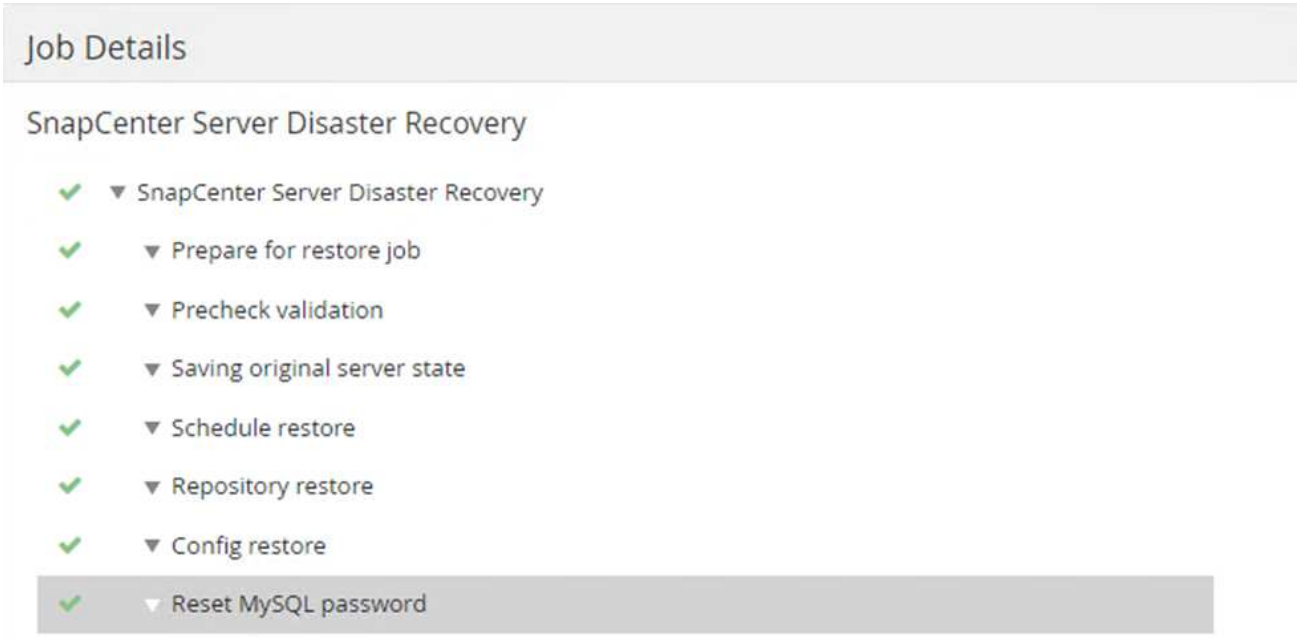


3. 粘贴您的授权令牌，并在 SmDRResterRequest 部分粘贴备份的名称和辅助SnapCenter服务器上的本地目录。



4. 选择“执行”按钮开始恢复过程。
5. 从SnapCenter导航到“监视”部分以查看还原作业的进度。





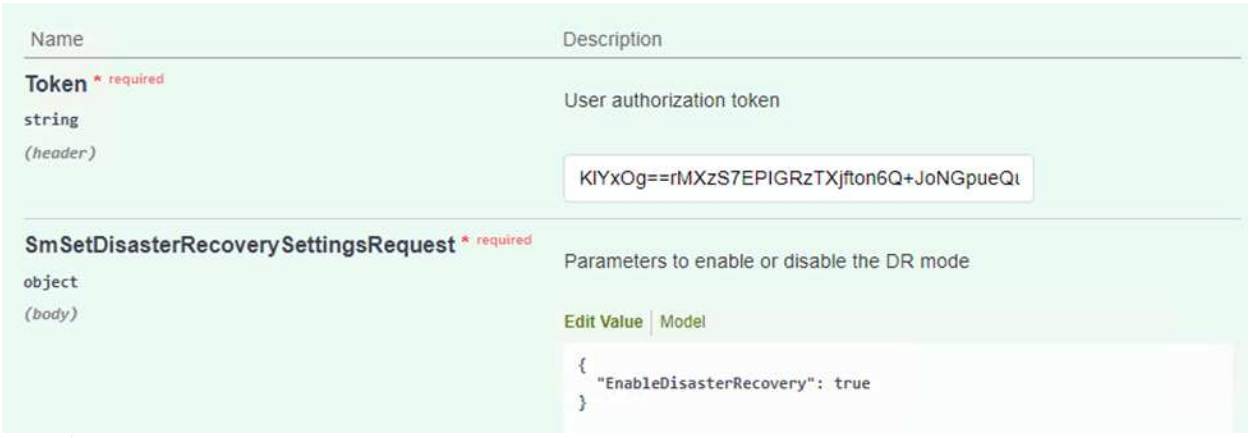
6. 要从二级存储启用 SQL Server 还原，必须将SnapCenter数据库切换到灾难恢复模式。这是作为单独的操作执行的，并在 Swagger API 网页上启动。

   a. 导航至灾难恢复部分并单击 `/4.6/disasterrecovery/storage`。

   b. 粘贴用户授权令牌。

   c. 在 SmSetDisasterRecoverySettingsRequest 部分中，更改 `EnableDisasterRecover`到 `true`。

   d. 单击“执行”以启用 SQL Server 的灾难恢复模式。



请参阅有关附加程序的评论。

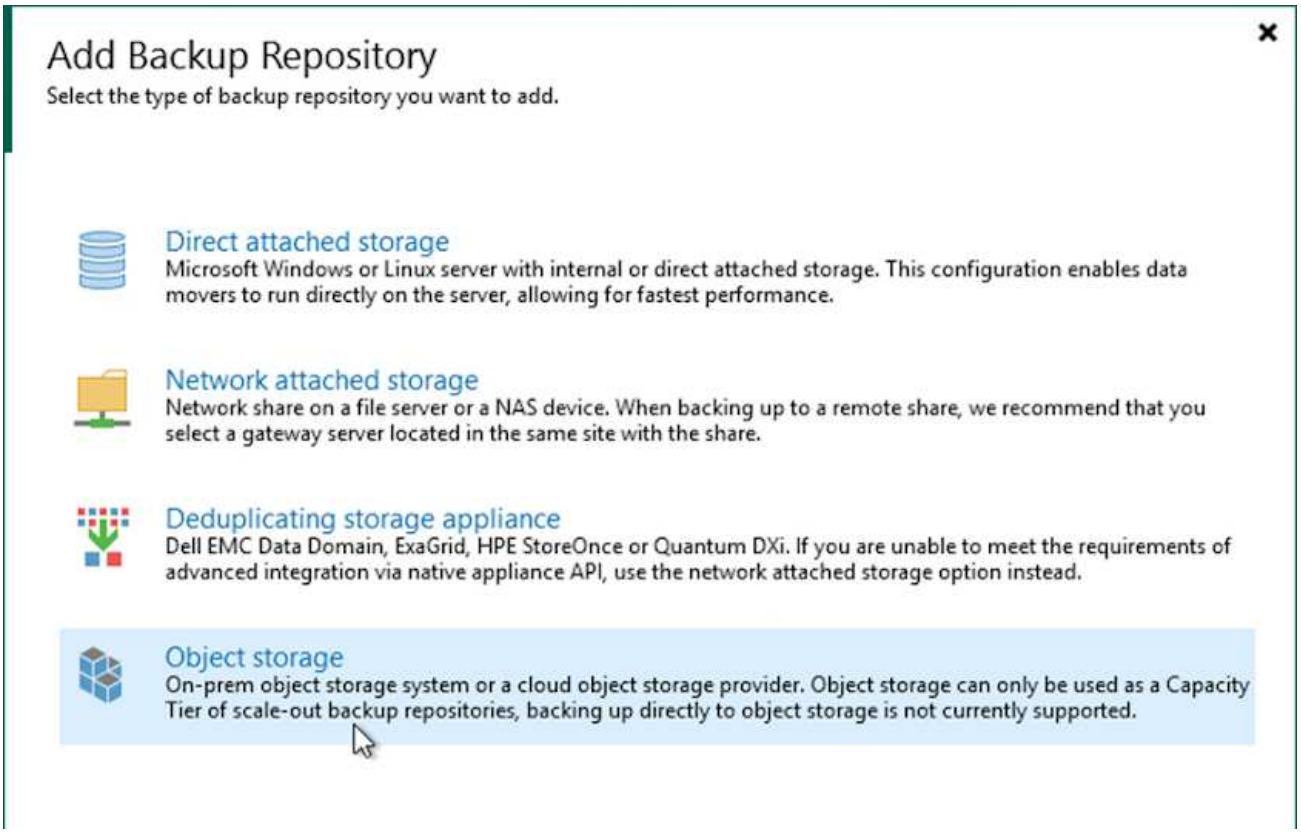
使用 **Veeam** 完整恢复功能恢复应用程序虚拟机

▼ 创建备份存储库并从 **S3** 导入备份

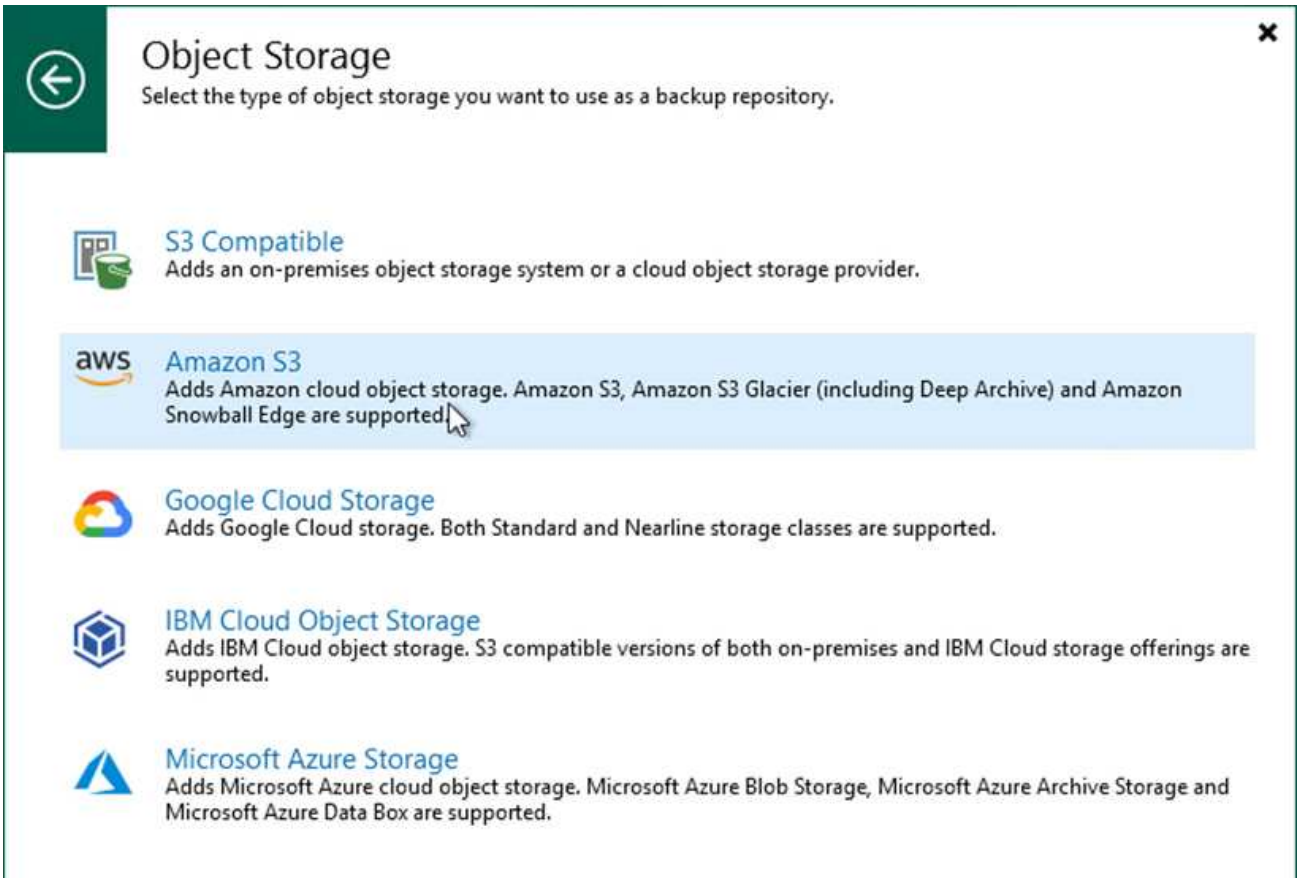
从辅助 Veeam 服务器，从 S3 存储导入备份并将 SQL Server 和 Oracle VM 还原到您的 VMware Cloud 集群。

要从属于本地扩展备份存储库的 S3 对象导入备份，请完成以下步骤：

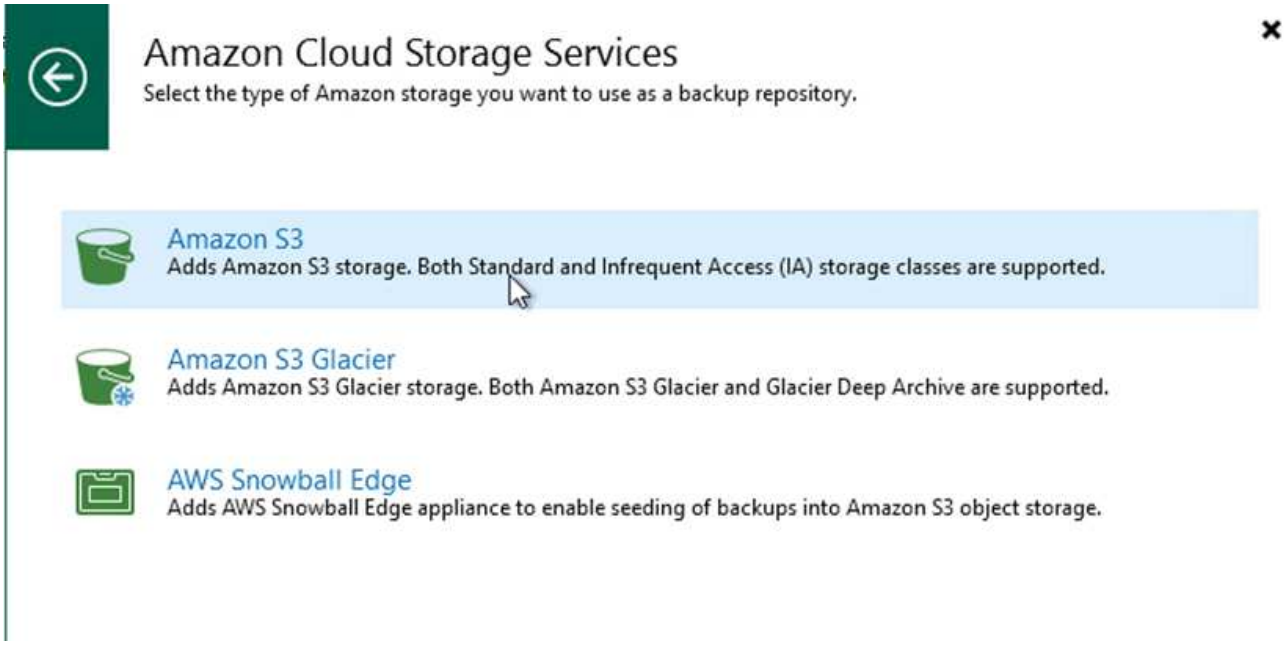
1. 转到备份存储库并单击顶部菜单中的添加存储库以启动添加备份存储库向导。在向导的第一页上，选择对象存储作为备份存储库类型。



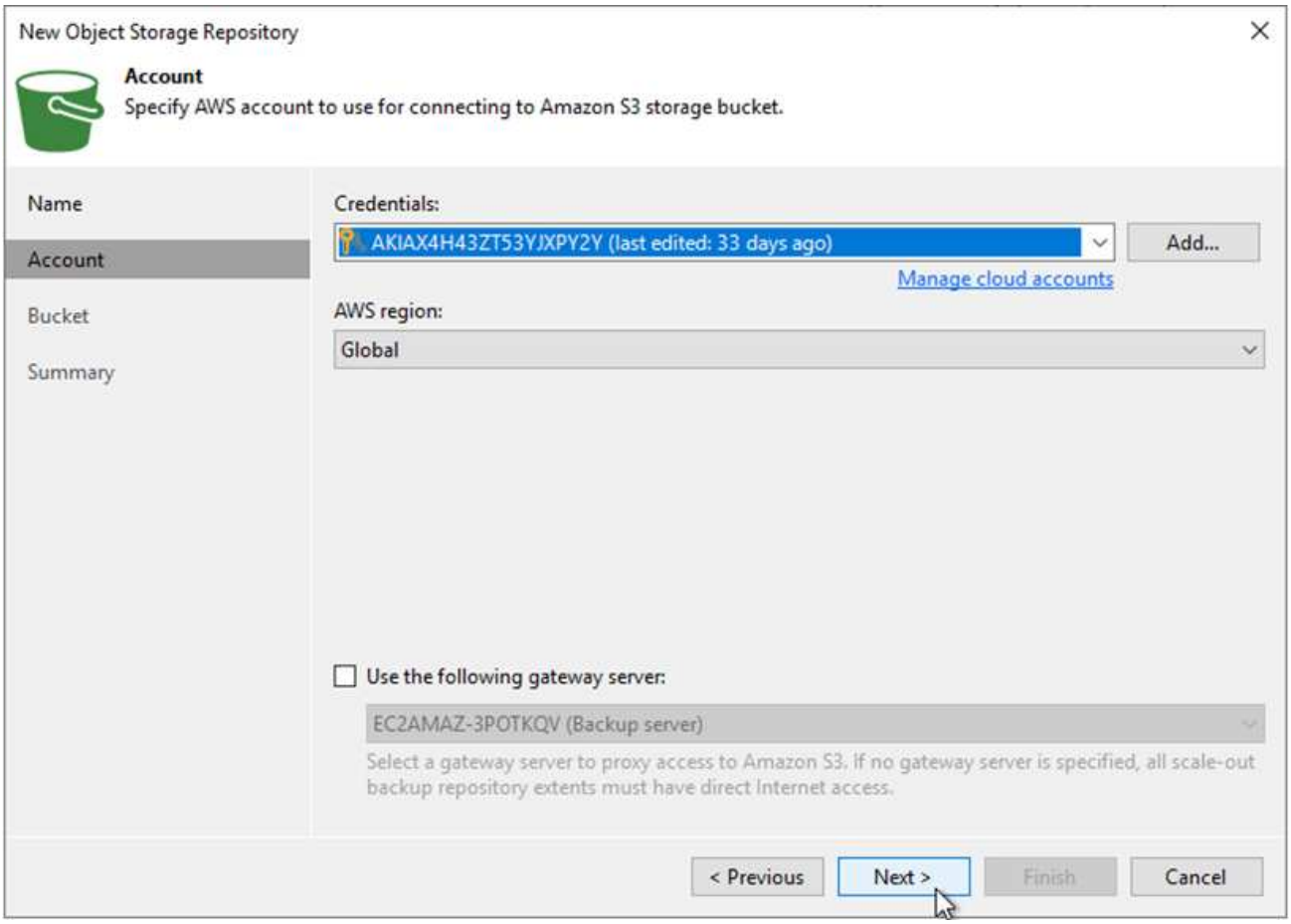
2. 选择 Amazon S3 作为对象存储类型。



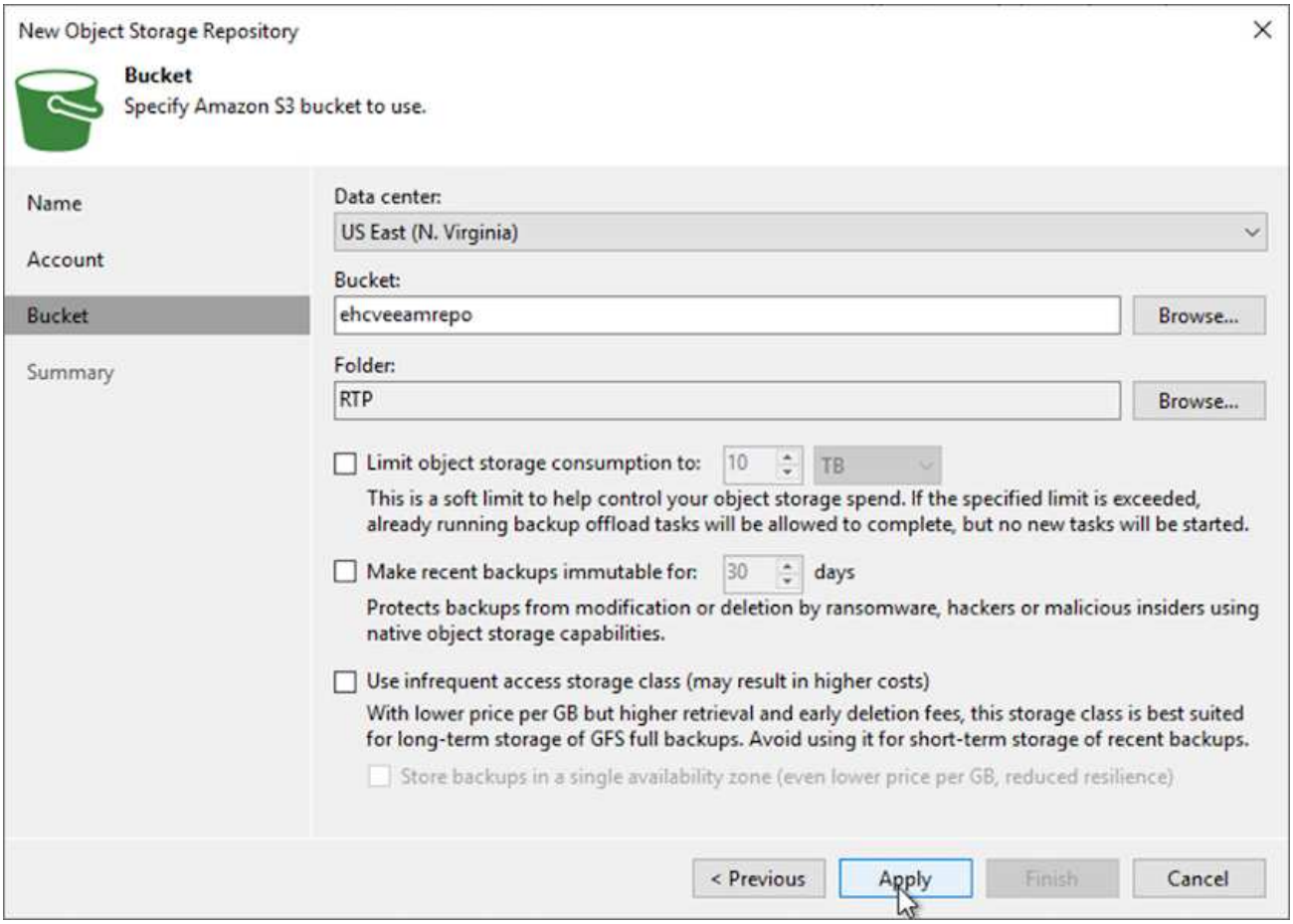
3. 从 Amazon 云存储服务列表中，选择 Amazon S3。



4. 从下拉列表中选择您预先输入的凭据或添加用于访问云存储资源的新凭据。单击“下一步”继续。



5. 在 Bucket 页面上，输入数据中心、bucket、文件夹和任何所需选项。单击“应用”。

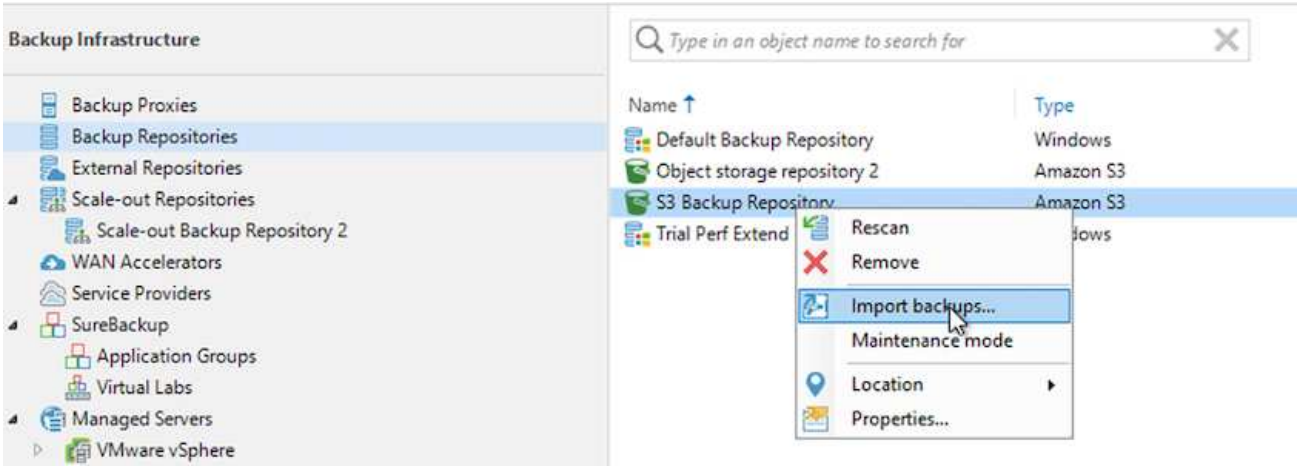


6. 最后，选择“完成”以完成该过程并添加存储库。

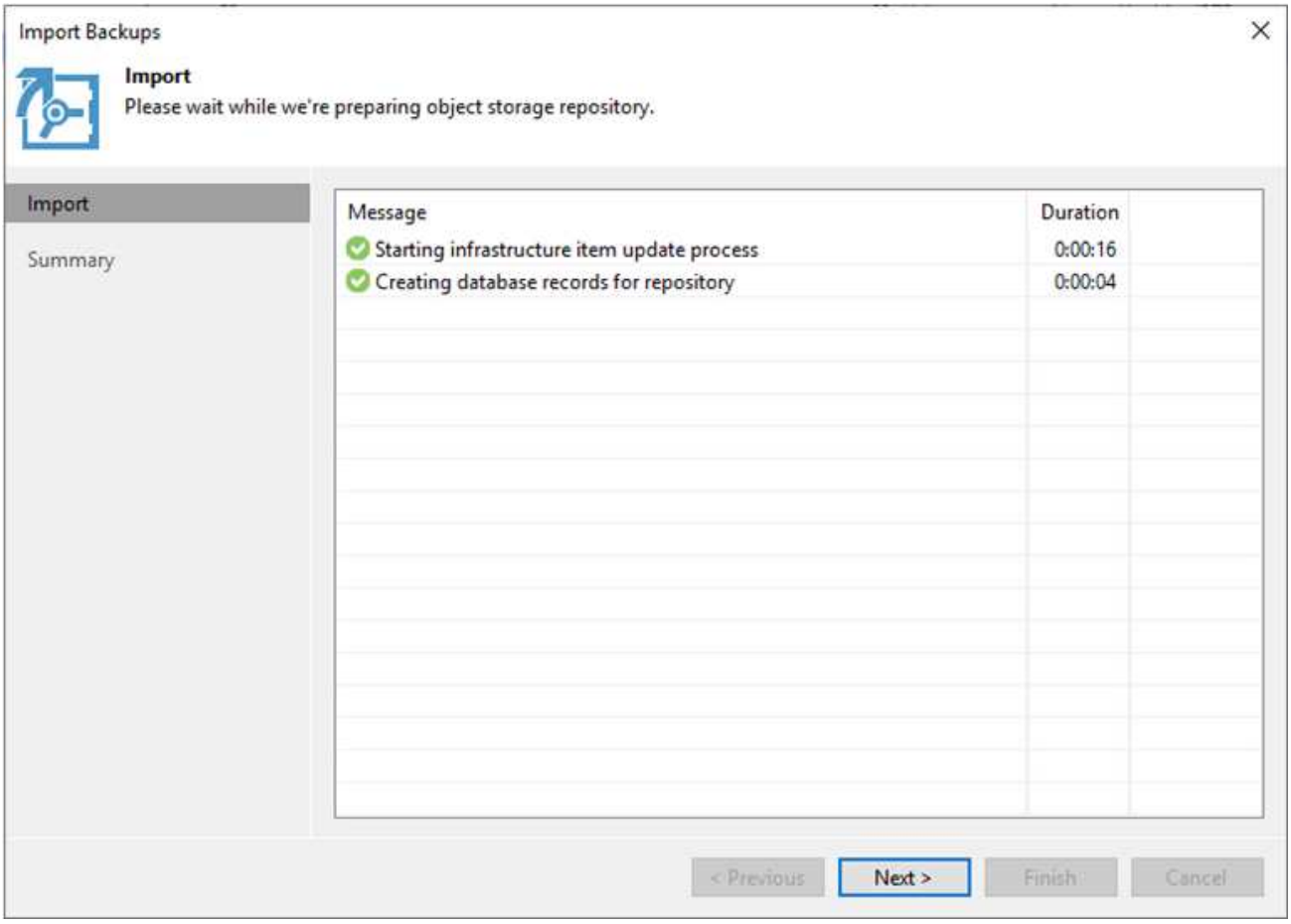
▼ 从 **S3** 对象存储导入备份

要从上一节中添加的 S3 存储库导入备份，请完成以下步骤。

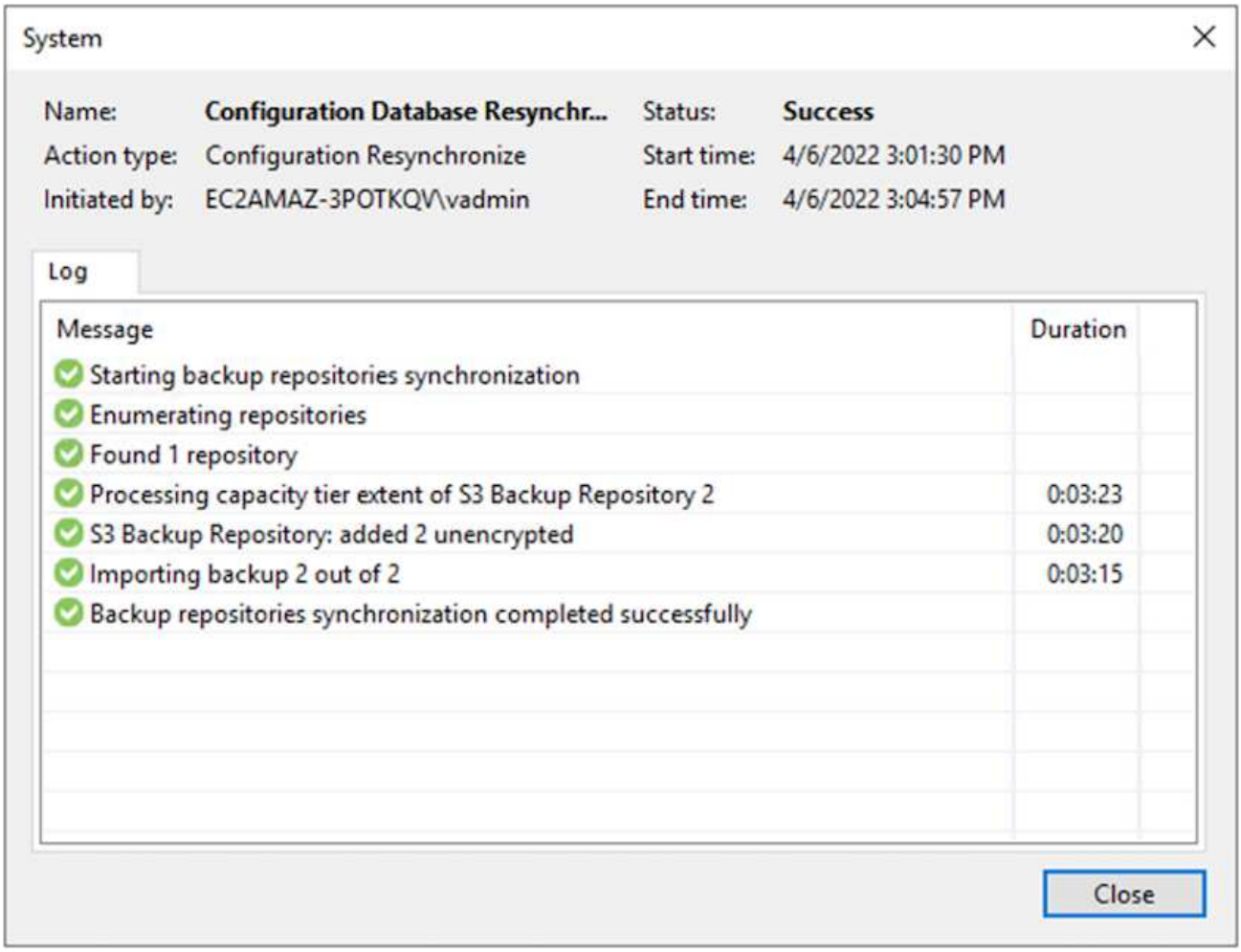
1. 从 S3 备份存储库中，选择导入备份以启动导入备份向导。



2. 创建导入的数据库记录后，选择下一步，然后在摘要屏幕上选择完成以开始导入过程。



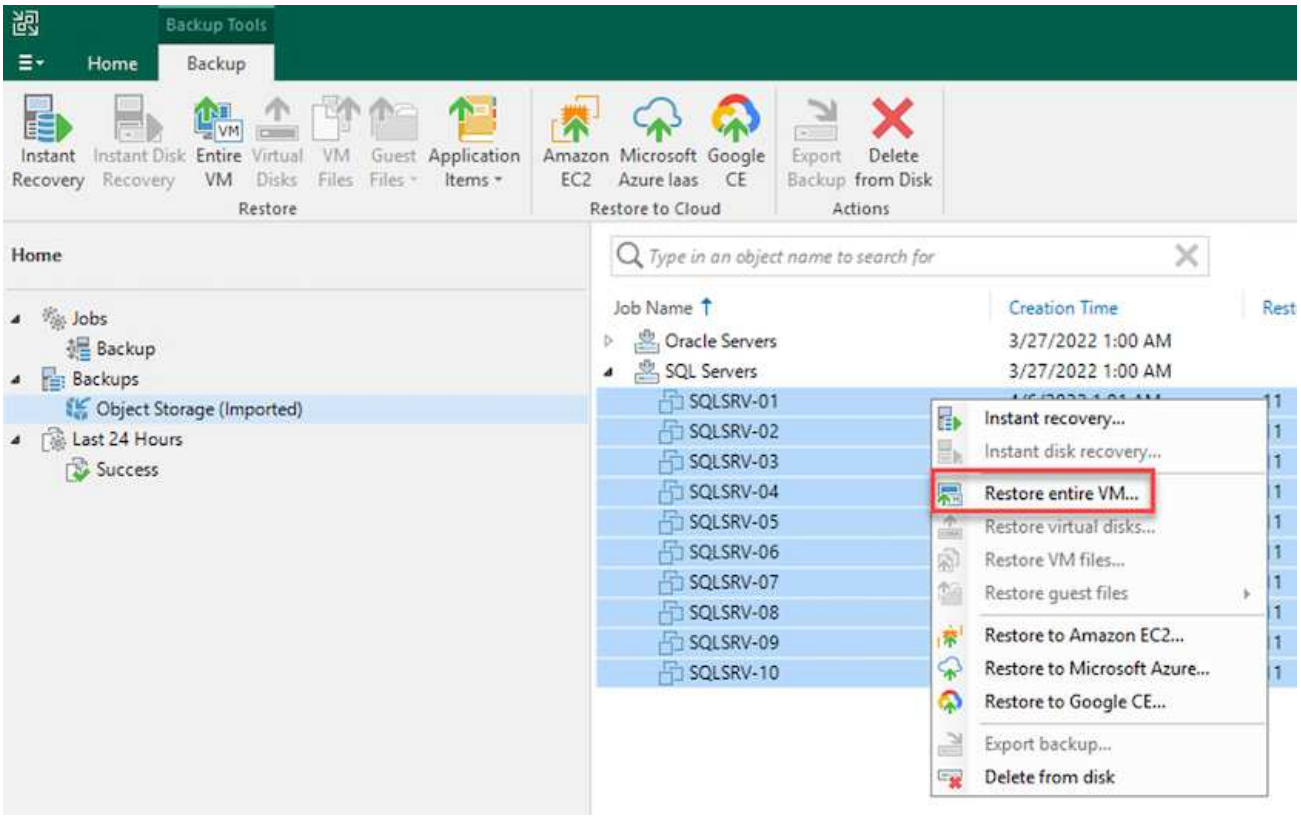
3. 导入完成后，您可以将虚拟机恢复到 VMware Cloud 集群中。



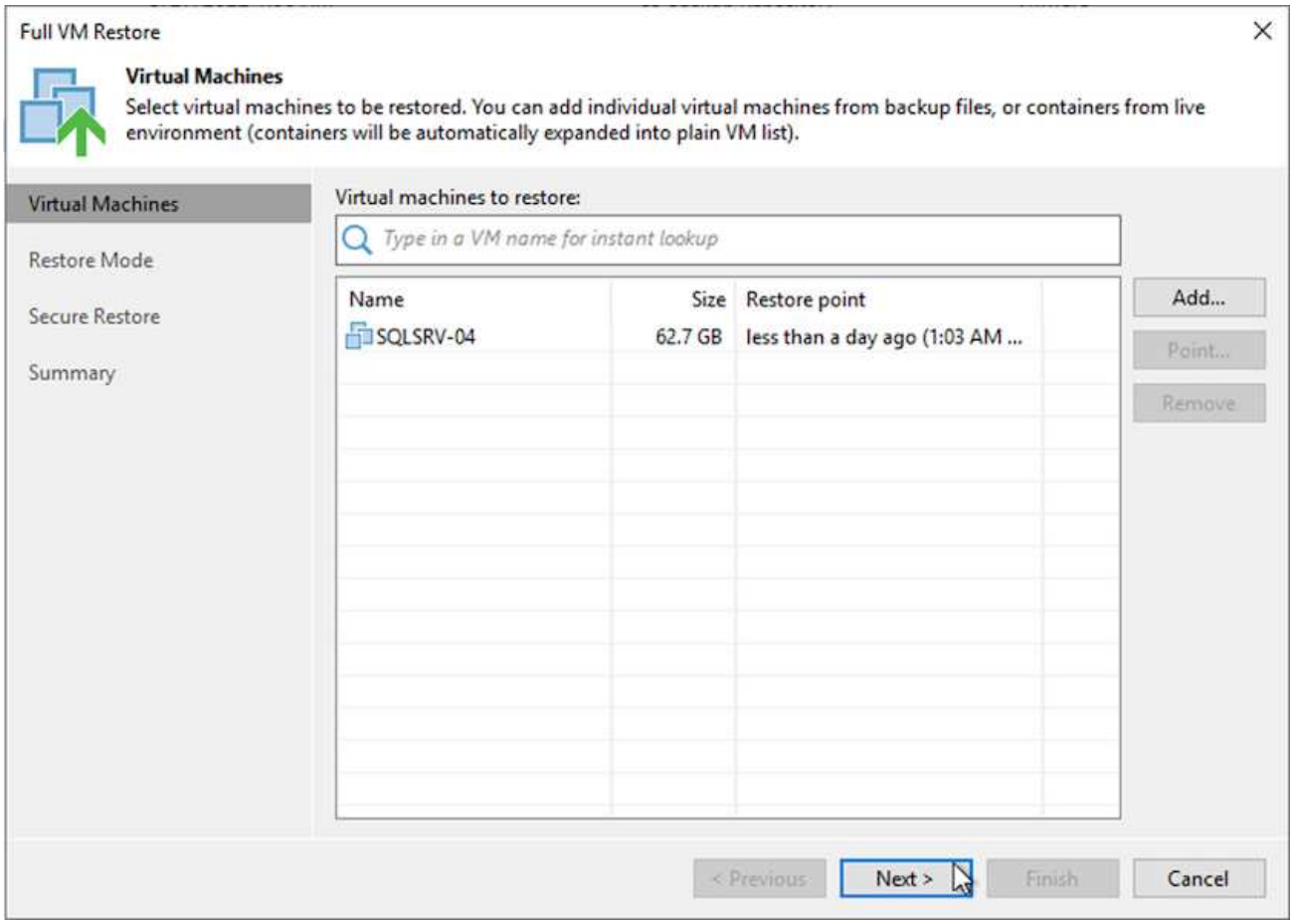
▼ 使用 **Veeam** 完整还原将应用程序虚拟机还原到 **VMware Cloud**

要将 SQL 和 Oracle 虚拟机还原到 VMware Cloud on AWS 工作负载域/集群，请完成以下步骤。

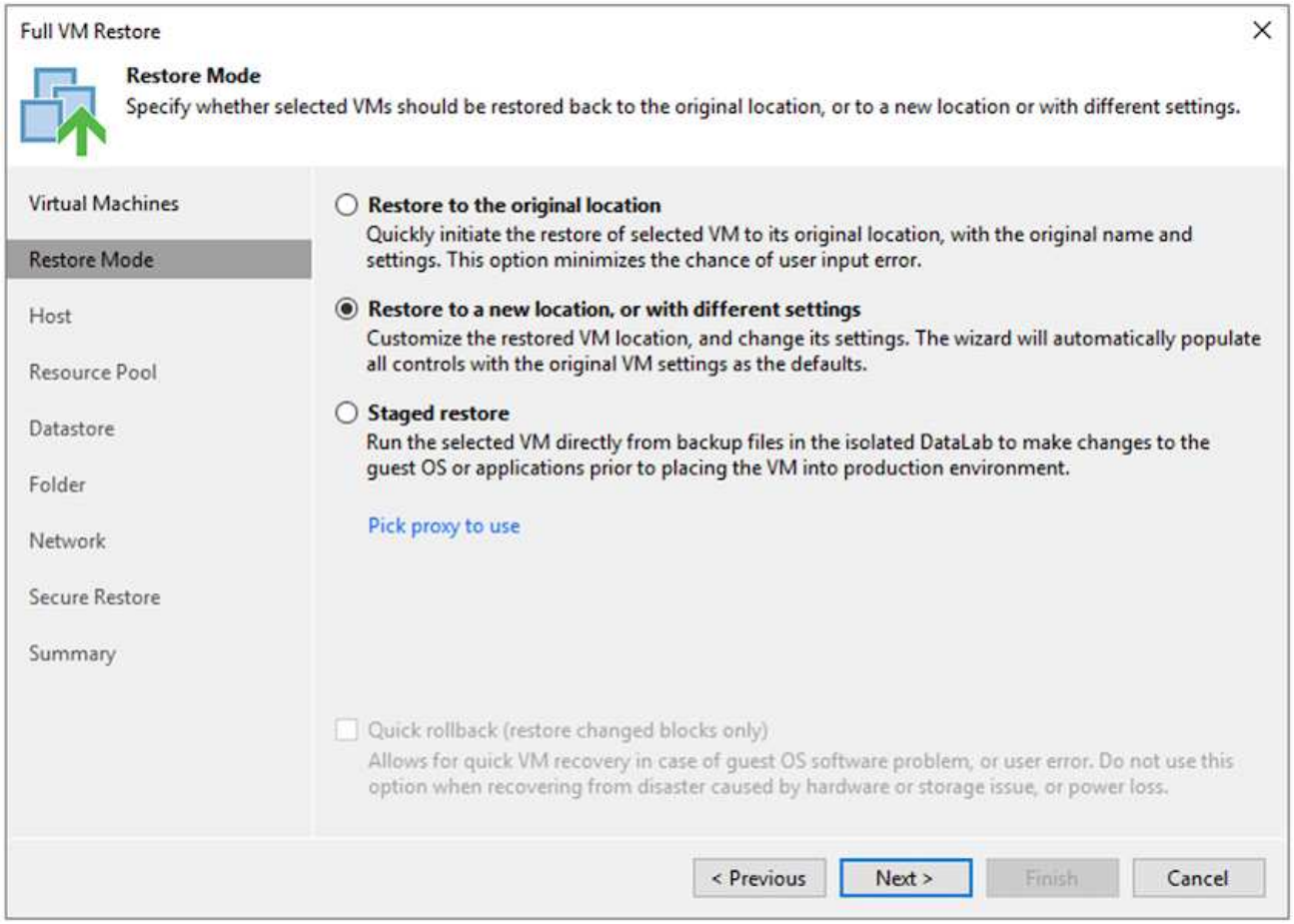
1. 从 Veeam 主页中，选择包含导入备份的对象存储，选择要恢复的虚拟机，然后右键单击并选择“恢复整个虚拟机”。



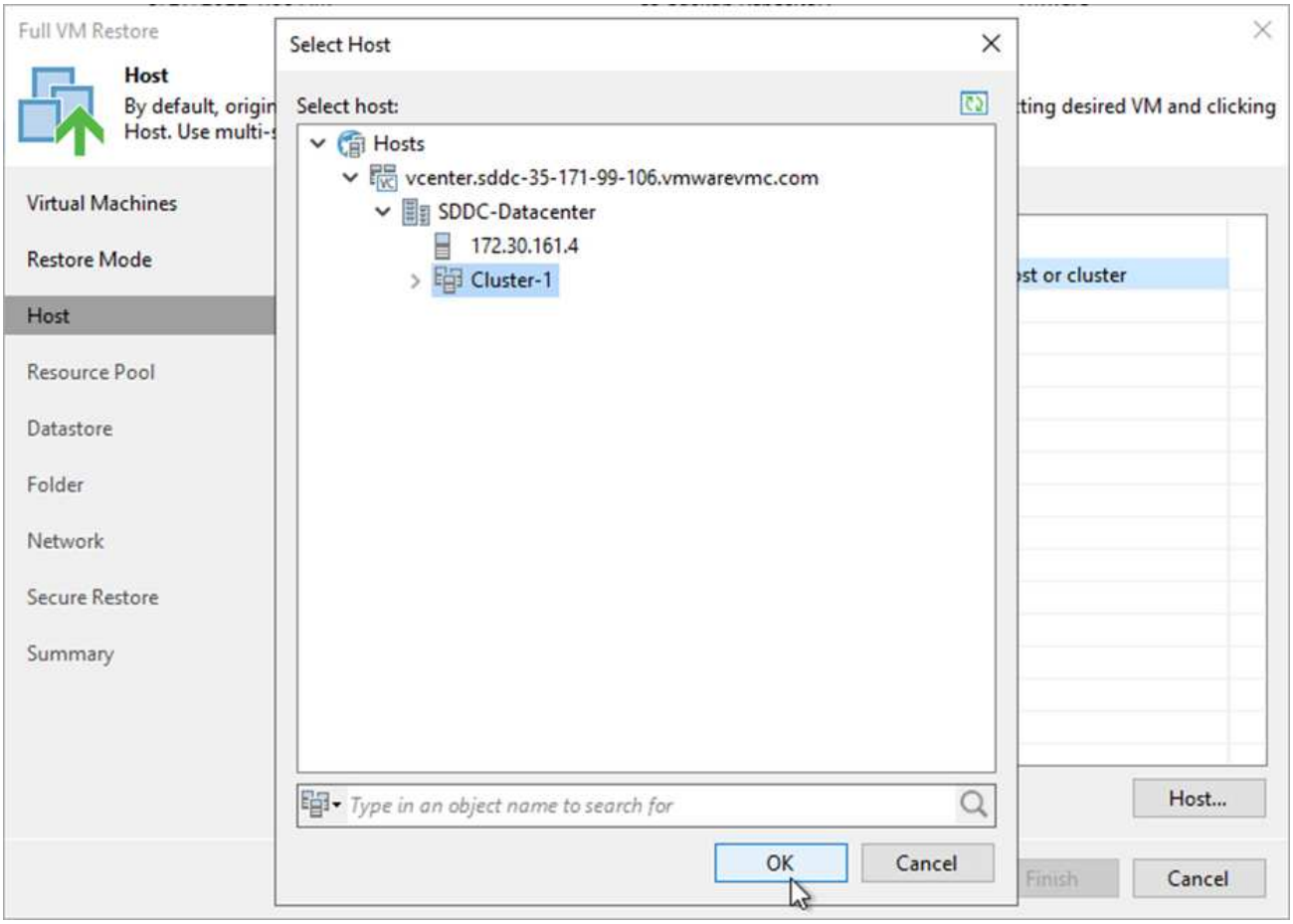
2. 在完整虚拟机还原向导的第一页上，根据需要修改要备份的虚拟机，然后选择下一步。



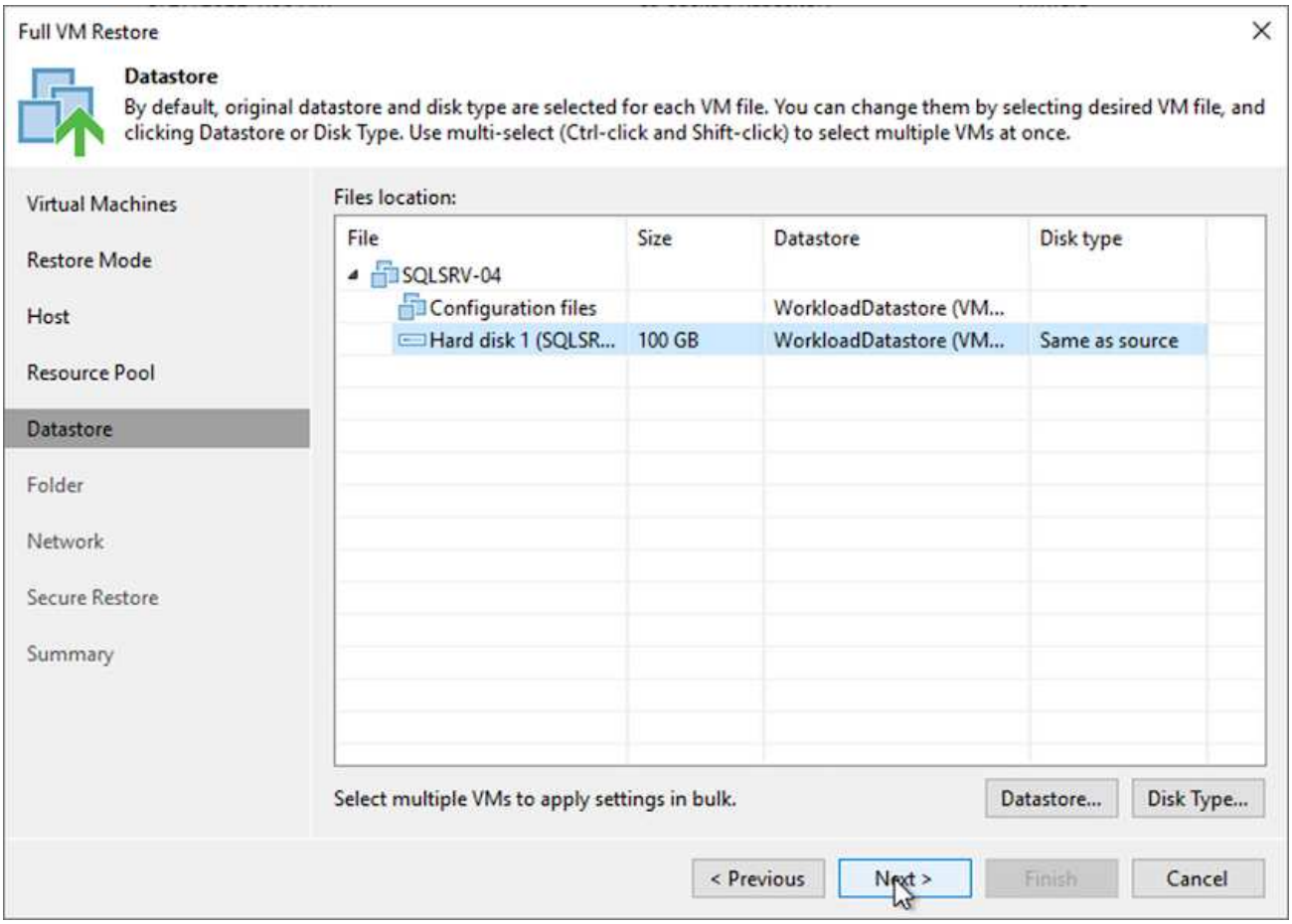
3. 在“恢复模式”页面上，选择“恢复到新位置”或“使用不同的设置”。



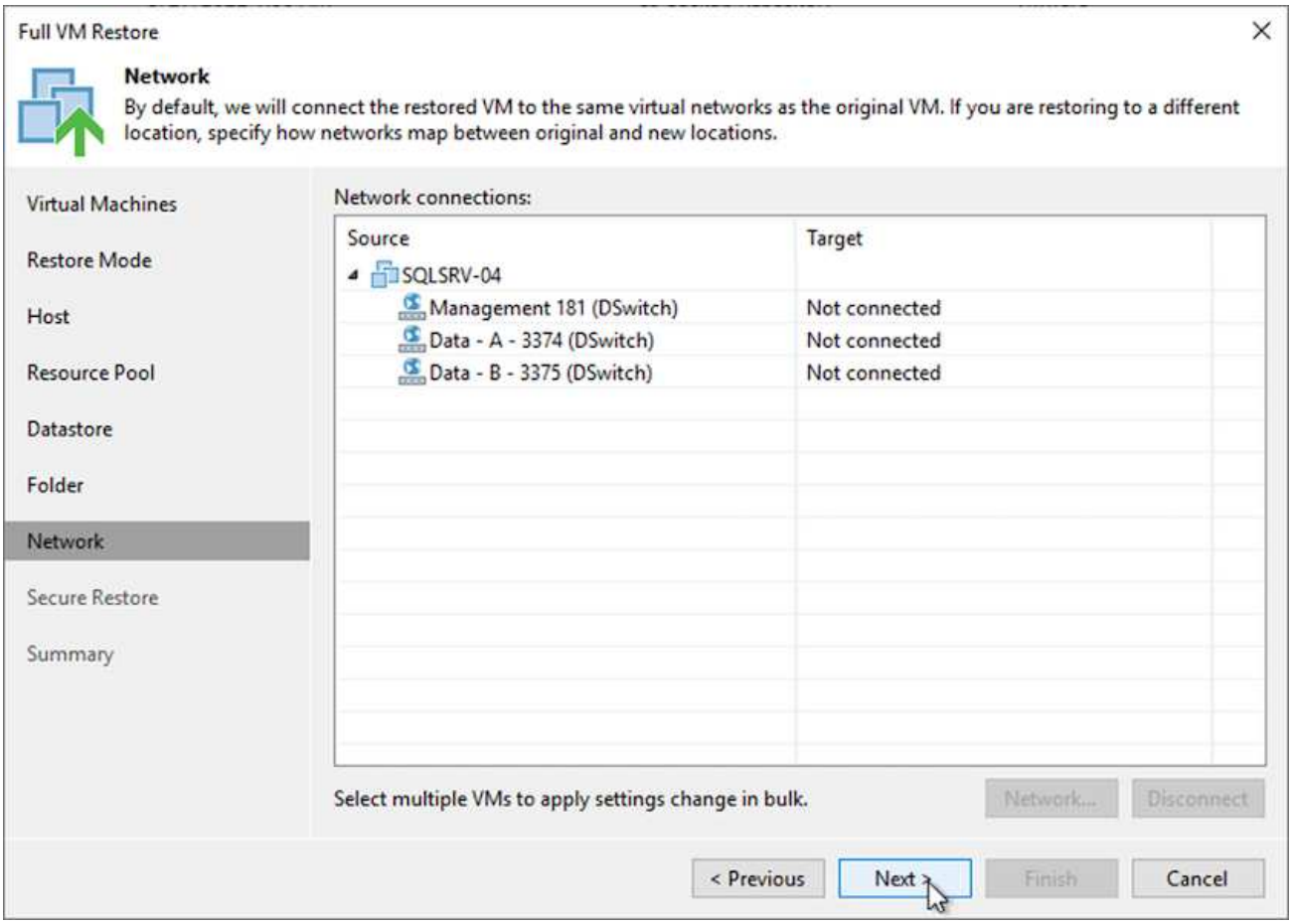
4. 在主机页面上，选择要将虚拟机还原到的目标 ESXi 主机或群集。

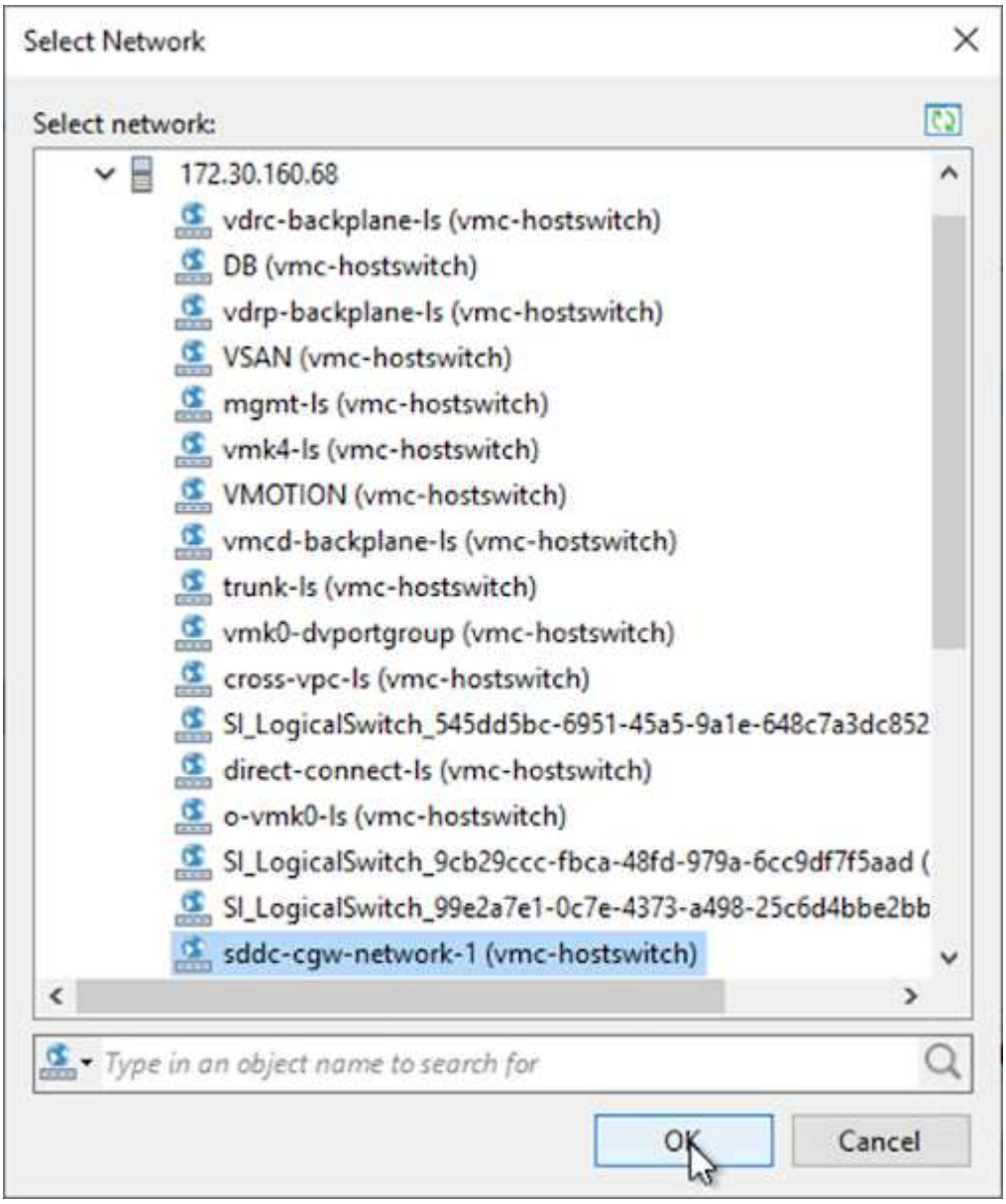


5. 在数据存储页面上，选择配置文件和硬盘的目标数据存储位置。



6. 在网络页面，将虚拟机上原有的网络映射到新目标位置的网络。


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. 选择是否扫描已恢复的虚拟机中的恶意软件，查看摘要页面，然后单击“完成”以开始恢复。

还原 **SQL Server** 应用程序数据

以下过程提供了有关在发生导致本地站点无法运行的灾难时如何在 AWS 中的 VMware Cloud Services 中恢复 SQL Server 的说明。

为了继续执行恢复步骤，假定以下先决条件已完成：

1. Windows Server VM 已使用 Veeam Full Restore 恢复到 VMware Cloud SDDC。
2. 已建立辅助SnapCenter服务器，并已使用本节中概述的步骤完成SnapCenter数据库还原和配置"SnapCenter备份和恢复过程摘要。"

▼ **VM：SQL Server VM** 的恢复后配置

虚拟机还原完成后，您必须配置网络和其他项目，以准备在SnapCenter中重新发现主机虚拟机。

1. 为管理和 iSCSI 或 NFS 分配新的 IP 地址。

2. 将主机加入 Windows 域。
3. 将主机名添加到 DNS 或SnapCenter服务器上的 hosts 文件。

> 如果使用与当前域不同的域凭据部署SnapCenter插件，则必须更改 SQL Server VM 上 Windows 服务插件的登录帐户。更改登录帐户后，重新启动SnapCenter SMCore、Windows 插件和 SQL Server 插件服务。

> 要自动重新发现SnapCenter中还原的虚拟机，FQDN 必须与最初添加到本地SnapCenter 的虚拟机相同。

▼ 配置 **FSx** 存储以进行 **SQL Server** 还原

要完成 SQL Server VM 的灾难恢复过程，您必须中断与 FSx 集群的现有SnapMirror关系并授予对该卷的访问权限。为此，请完成以下步骤。

1. 要中断 SQL Server 数据库和日志卷的现有SnapMirror关系，请从 FSx CLI 运行以下命令：

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. 通过创建包含 SQL Server Windows VM 的 iSCSI IQN 的启动器组来授予对 LUN 的访问权限：

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

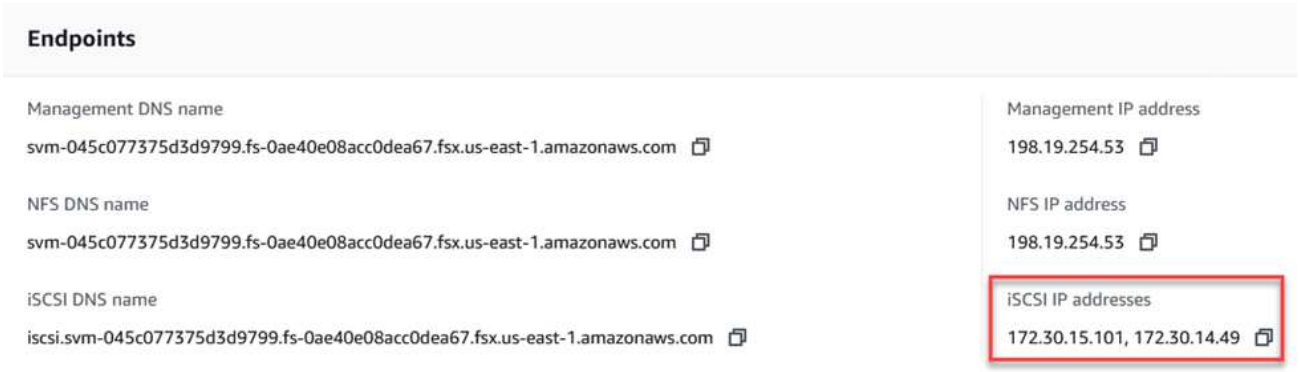
3. 最后，将 LUN 映射到刚刚创建的启动器组：

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

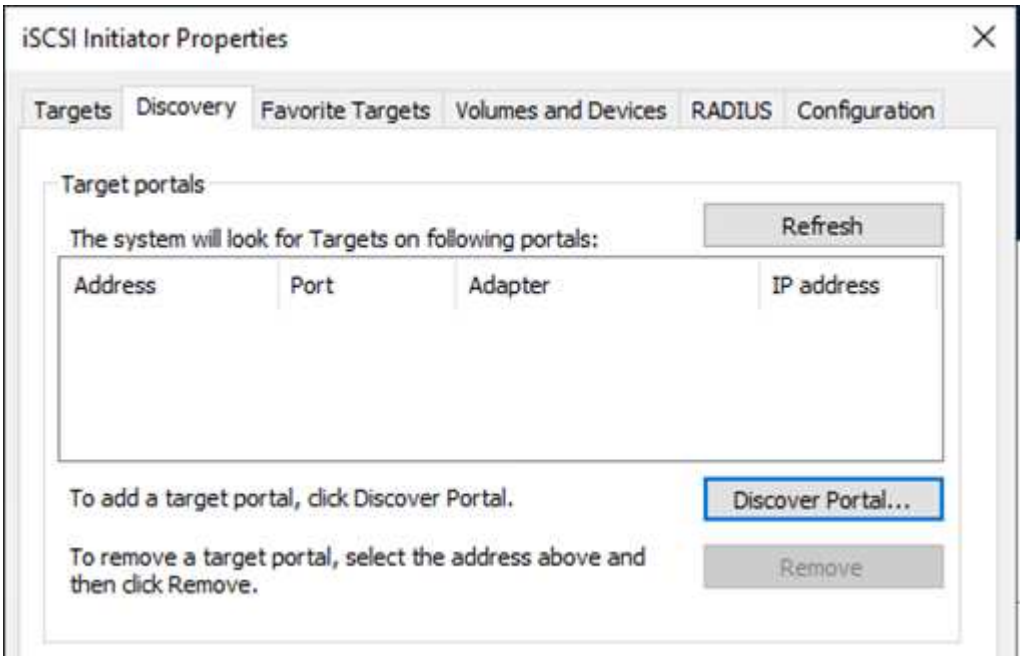
4. 要查找路径名，请运行 `lun show`命令。

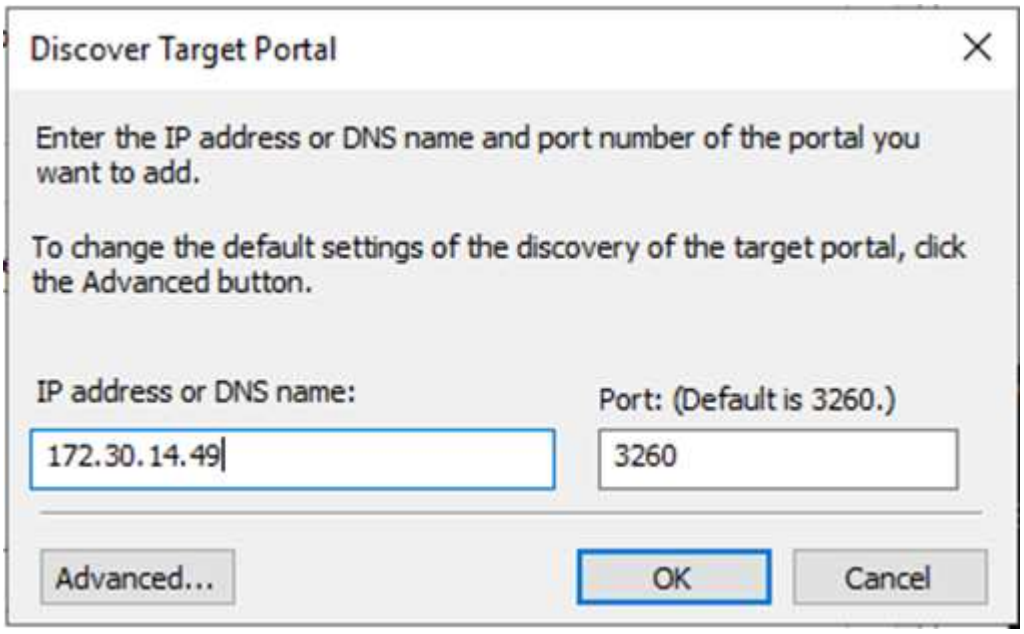
▼ 设置 **Windows VM** 以进行 **iSCSI** 访问并发现文件系统

1. 从 SQL Server VM 中，设置您的 iSCSI 网络适配器，以便在已建立与 FSx 实例上的 iSCSI 目标接口连接的 VMware 端口组上进行通信。
2. 打开 iSCSI 启动器属性实用程序并清除“发现”、“收藏目标”和“目标”选项卡上的旧连接设置。
3. 找到用于访问 FSx 实例/集群上的 iSCSI 逻辑接口的 IP 地址。这可以在 AWS 控制台的Amazon FSx > ONTAP > Storage Virtual Machines 下找到。

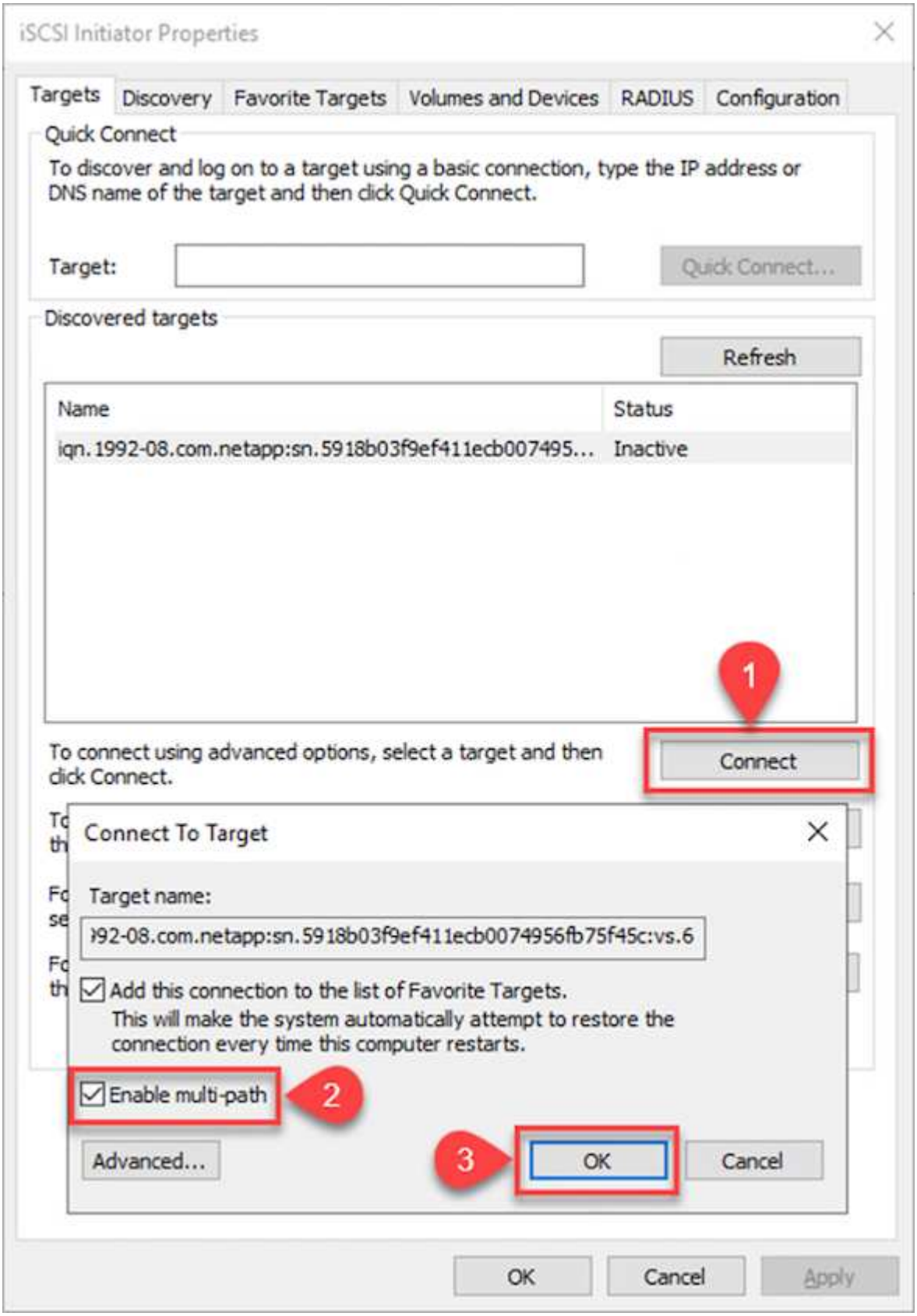


4. 在“发现”选项卡中，单击“发现门户”并输入 FSx iSCSI 目标的 IP 地址。

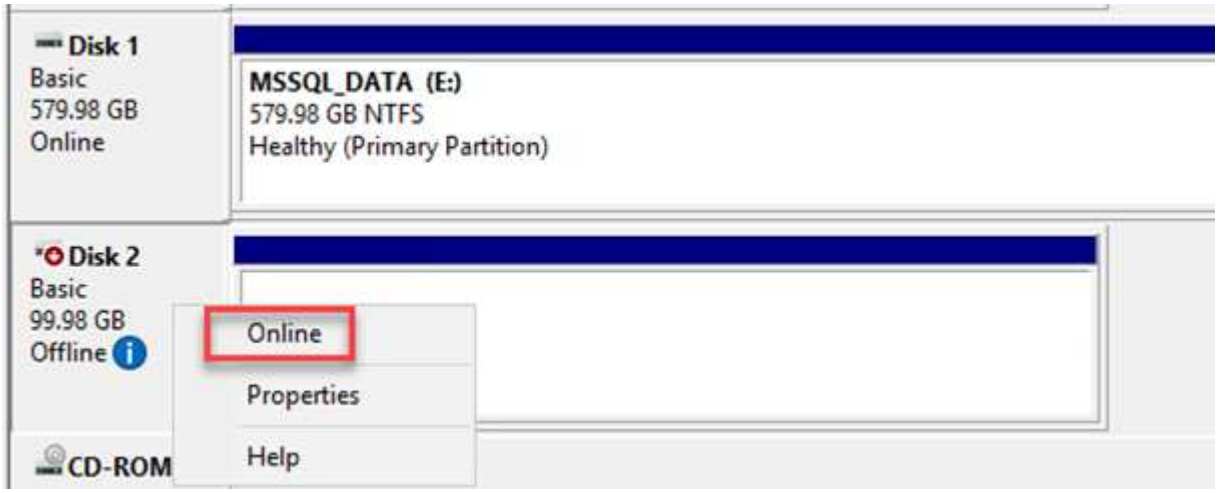




5. 在目标选项卡上，单击连接，如果适合您的配置，请选择启用多路径，然后单击确定以连接到目标。

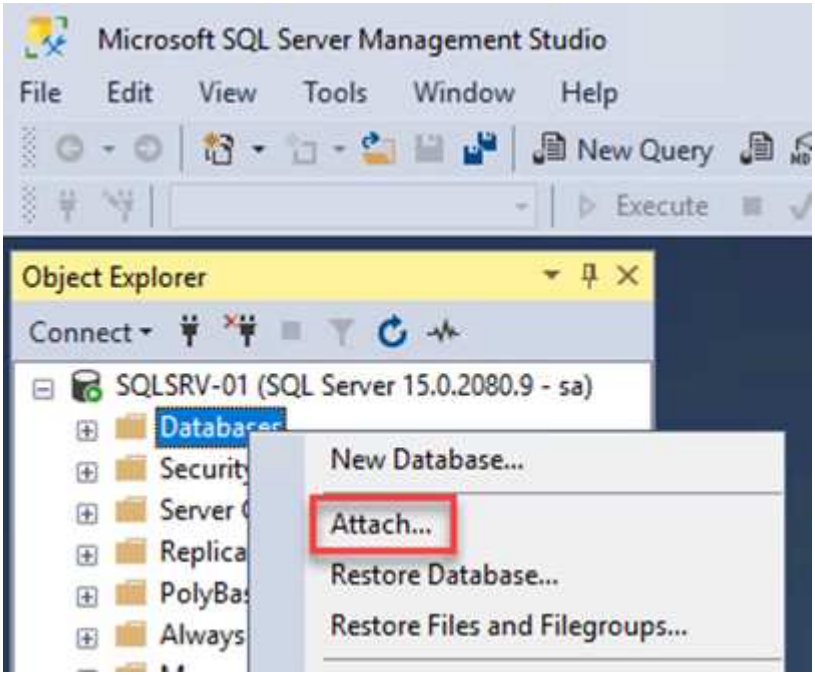


6. 打开计算机管理实用程序并使磁盘联机。验证它们是否保留了先前的相同驱动器号。

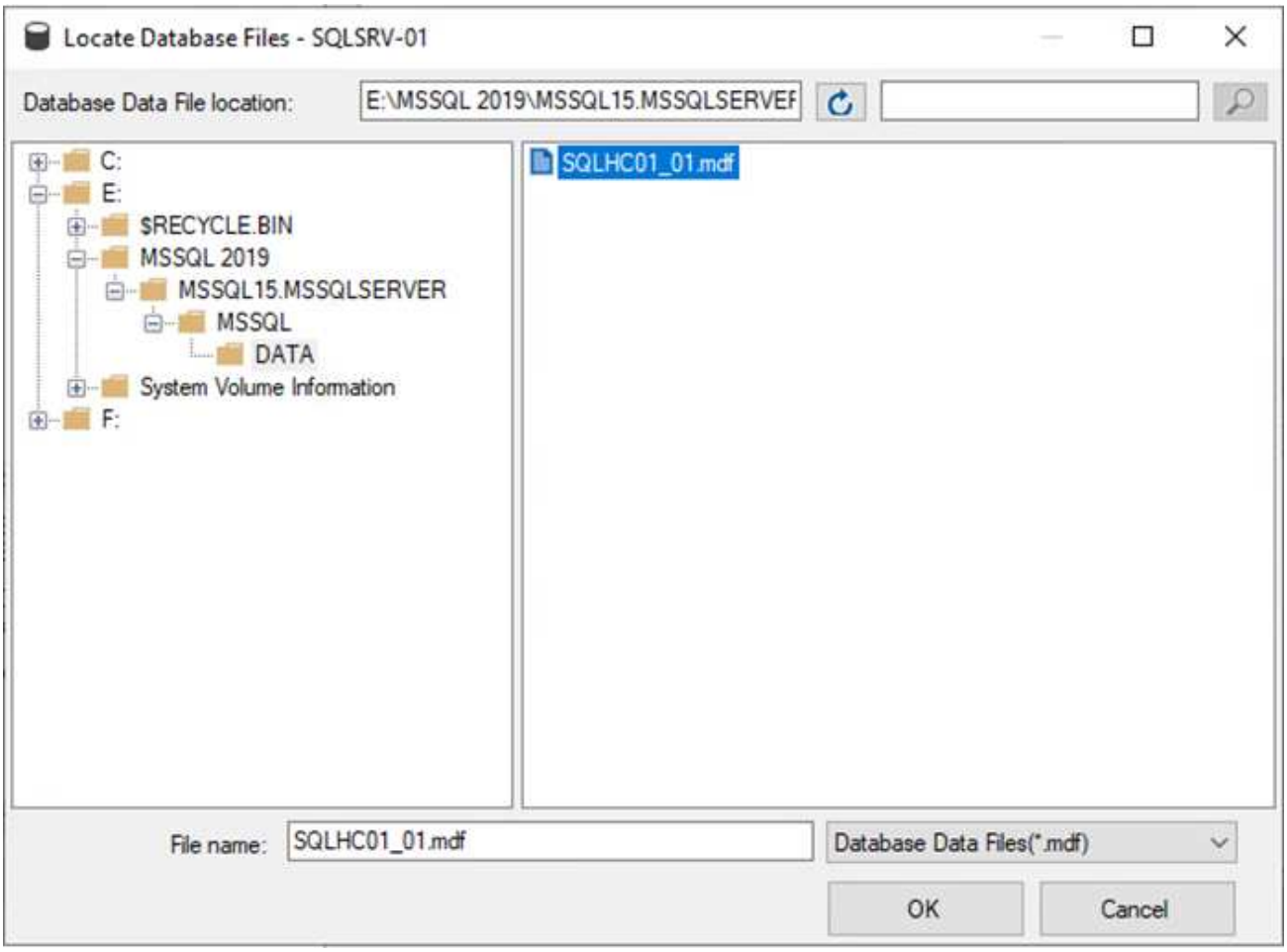


▼ 附加 **SQL Server** 数据库

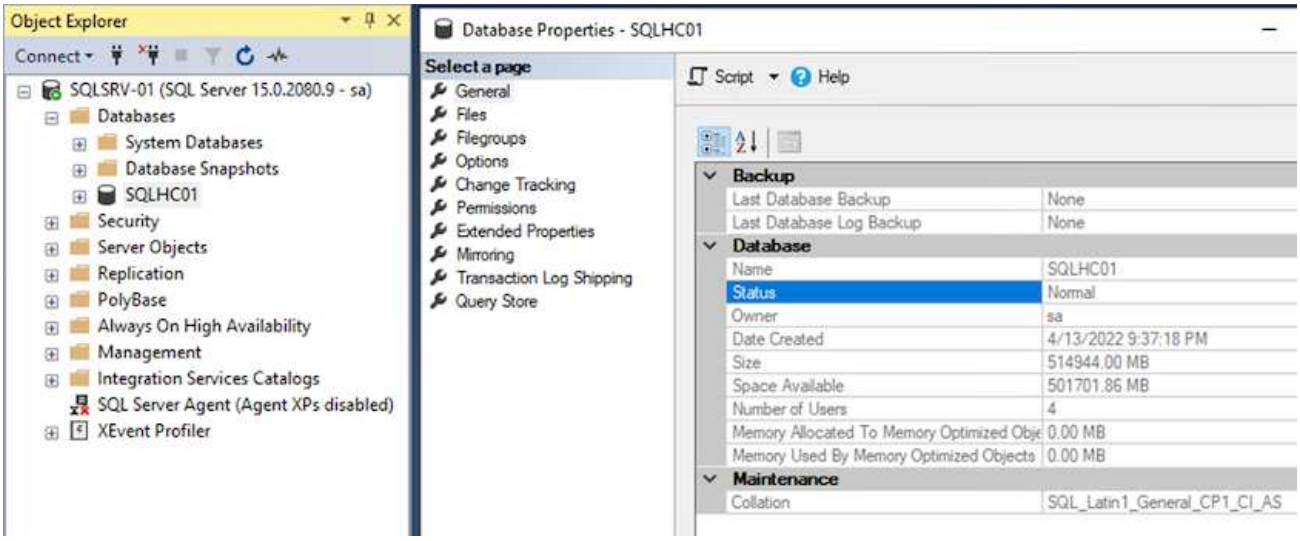
1. 从 SQL Server VM 中，打开 Microsoft SQL Server Management Studio 并选择“附加”以开始连接数据库的过程。



2. 单击“添加”并导航到包含 SQL Server 主数据库文件的文件夹，选择它，然后单击“确定”。



3. 如果事务日志位于单独的驱动器上，请选择包含事务日志的文件夹。
4. 完成后，单击“确定”以附加数据库。



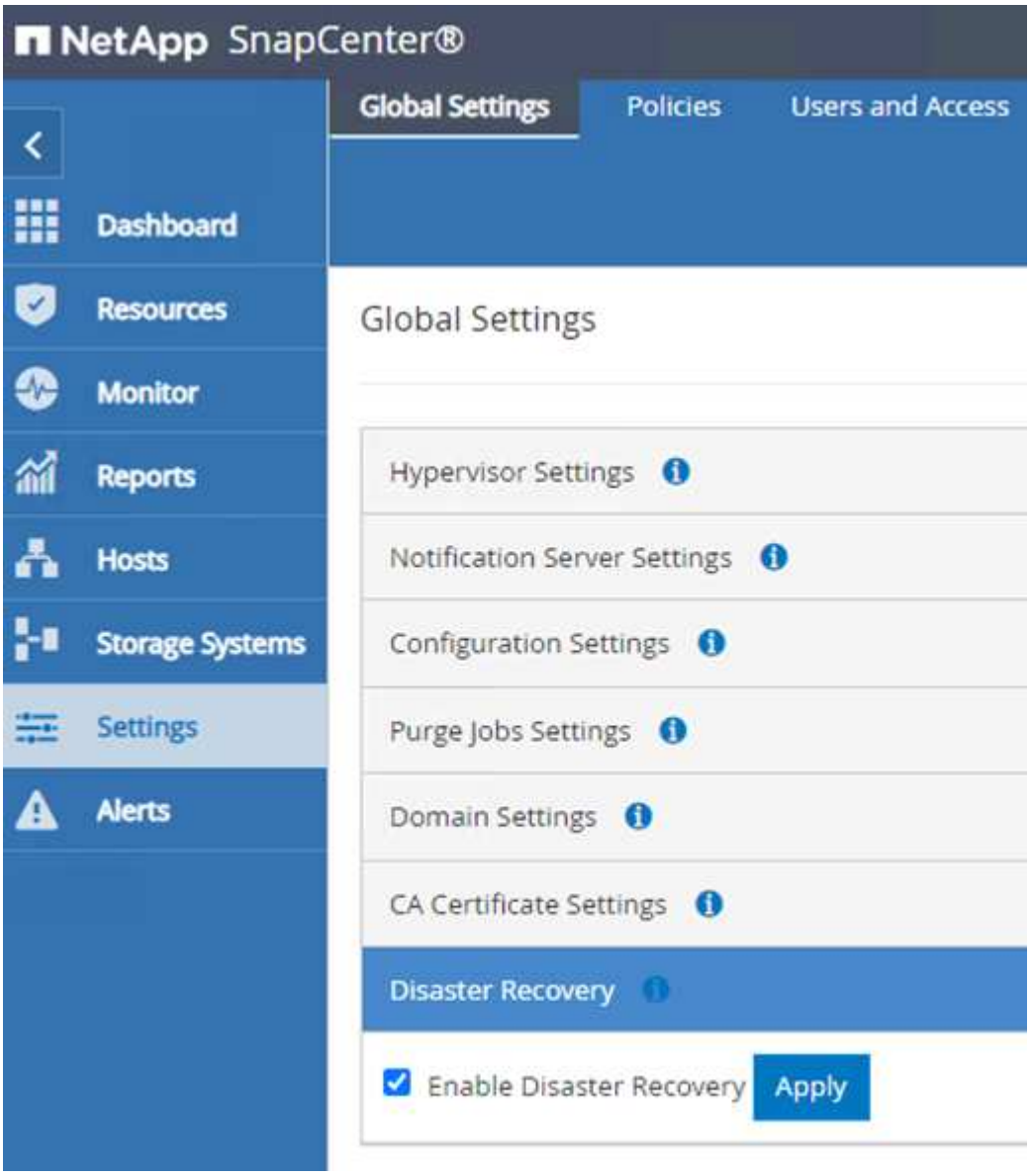
▼ 确认**SnapCenter**与 **SQL Server** 插件的通信

当SnapCenter数据库恢复到以前的状态时，它会自动重新发现 SQL Server 主机。为了使其正常工作，请记住以下先决条件：

- SnapCenter必须处于灾难恢复模式。这可以通过 Swagger API 或在灾难恢复下的全局设置中完成。

- SQL Server 的 FQDN 必须与在本地数据中心运行的实例相同。
- 必须破坏原始的SnapMirror关系。
- 必须将包含数据库的 LUN 安装到 SQL Server 实例并附加数据库。

要确认SnapCenter处于灾难恢复模式，请从SnapCenter Web 客户端导航到“设置”。转到“全局设置”选项卡，然后单击“灾难恢复”。确保启用灾难恢复复选框已启用。



恢复 **Oracle** 应用程序数据

以下流程提供了有关在发生导致本地站点无法运行的灾难时如何在 AWS 中的 VMware Cloud Services 中恢复 Oracle 应用程序数据的说明。

完成以下先决条件以继续执行恢复步骤：

1. Oracle Linux 服务器 VM 已使用 Veeam Full Restore 恢复到 VMware Cloud SDDC。
2. 已建立辅助SnapCenter服务器，并已使用本节概述的步骤恢复SnapCenter数据库和配置文件"SnapCenter备份和恢复过程摘要。"

▼ 配置 **FSx for Oracle** 还原 **–** 中断**SnapMirror**关系

要使 Oracle 服务器可以访问 FSx ONTAP实例上托管的二级存储卷，您必须首先中断现有的SnapMirror关系。

1. 登录 FSx CLI 后，运行以下命令查看按正确名称过滤的卷。

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

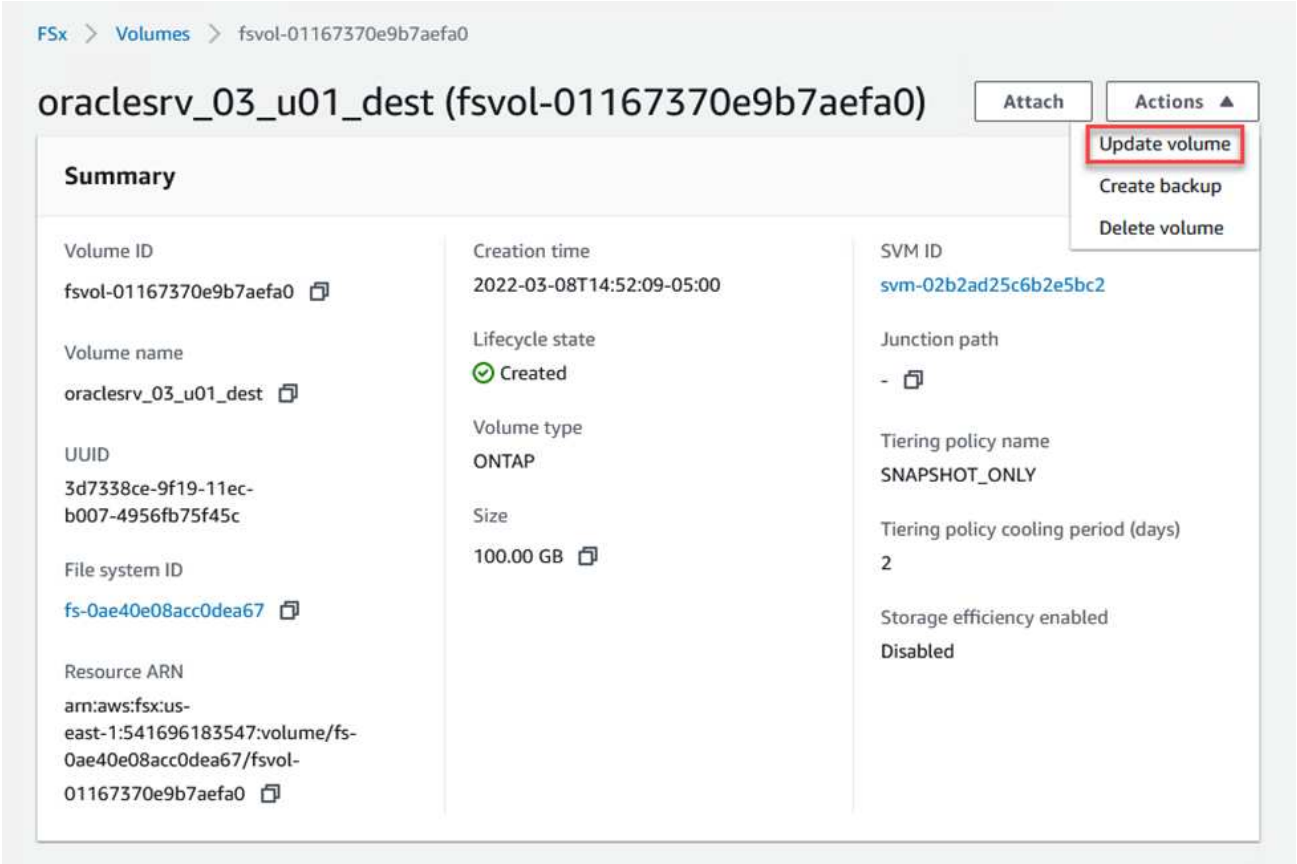
2. 运行以下命令来中断现有的SnapMirror关系。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

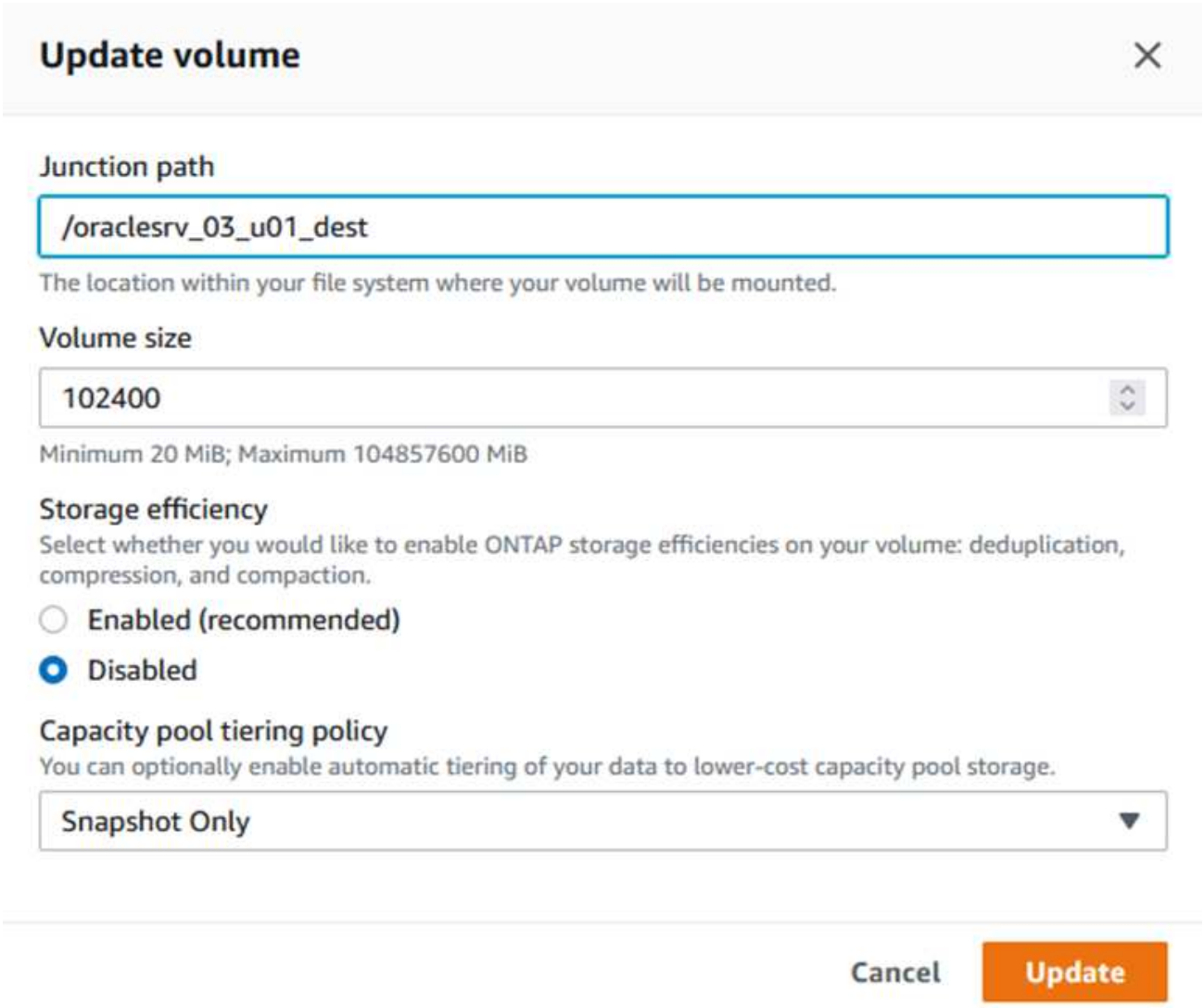
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. 更新Amazon FSx Web 客户端中的连接路径：



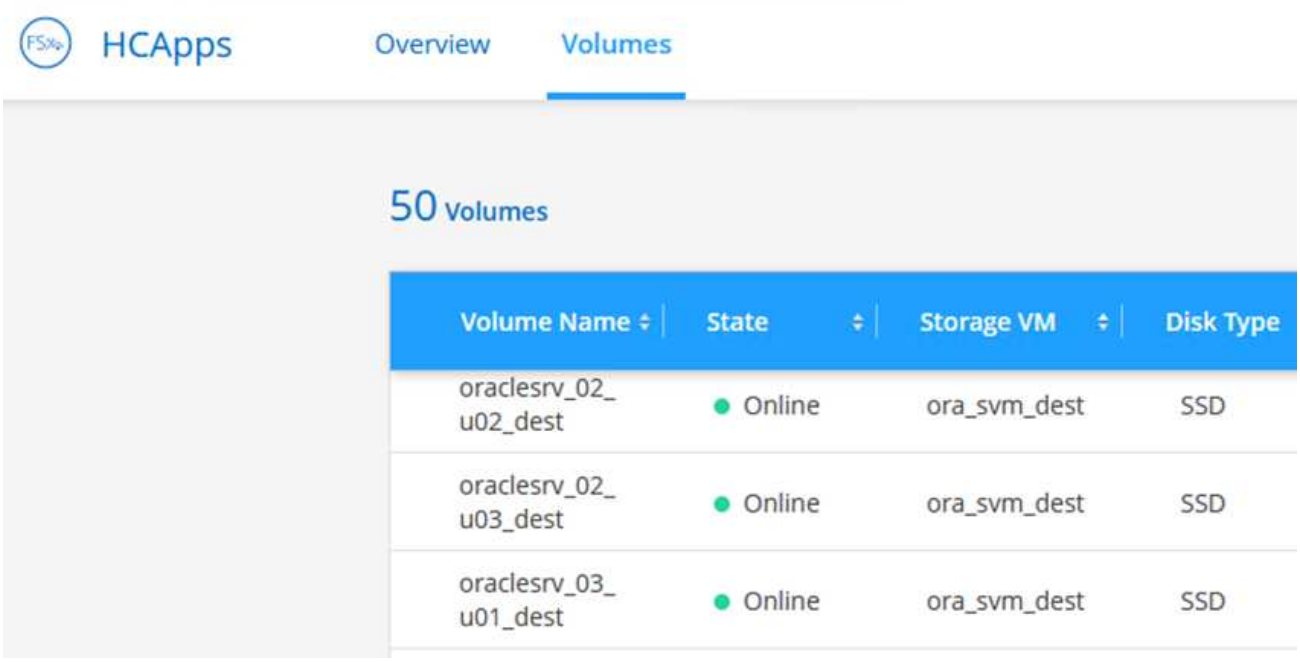
4. 添加连接路径名称并单击更新。从 Oracle 服务器挂载 NFS 卷时指定此连接路径。



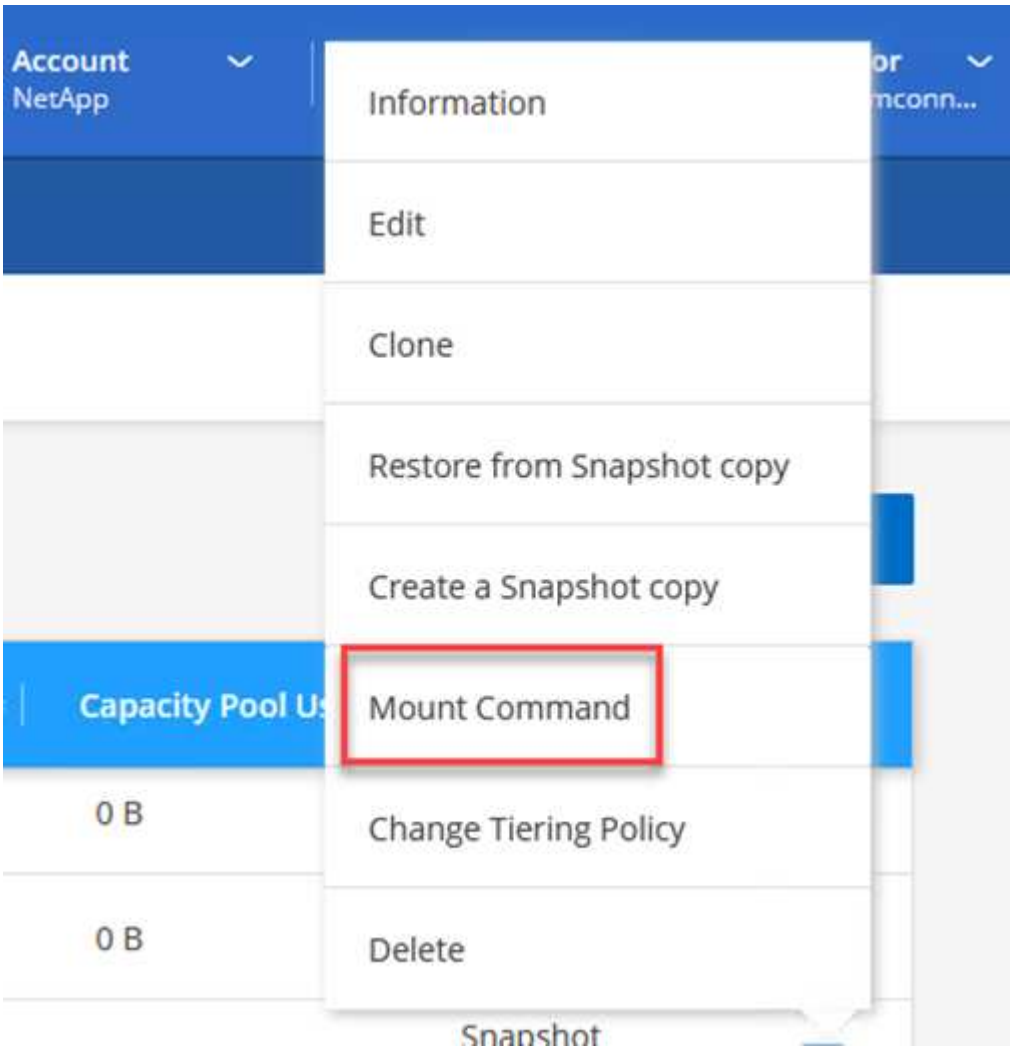
▼ 在 **Oracle** 服务器上挂载 **NFS** 卷

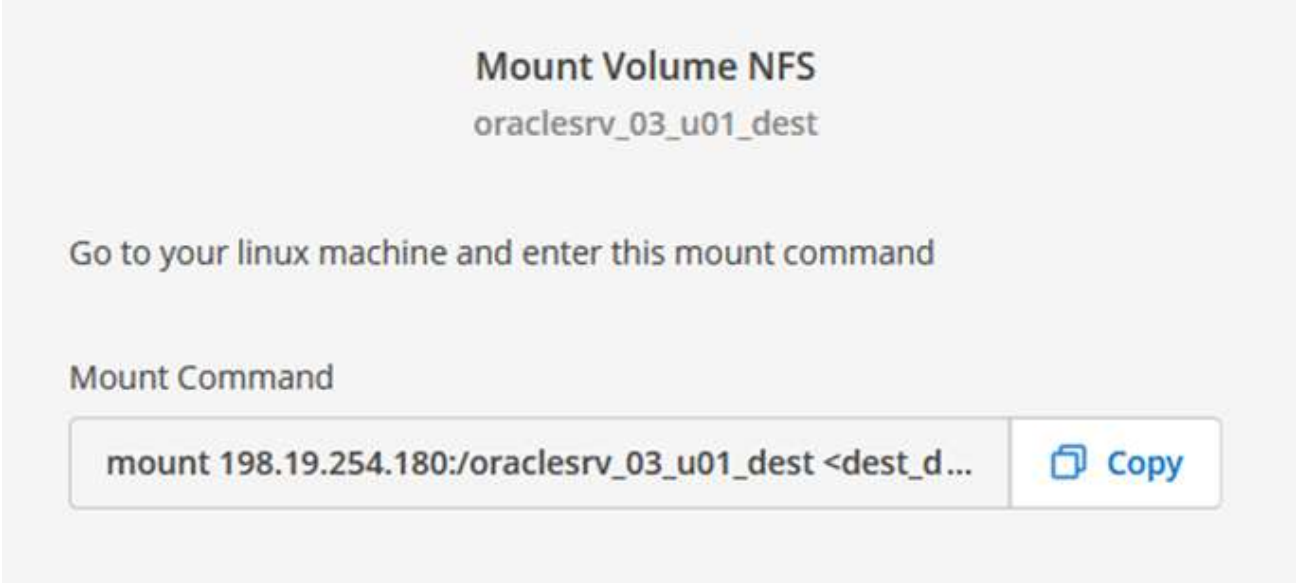
在 Cloud Manager 中，您可以获取具有正确 NFS LIF IP 地址的挂载命令，以挂载包含 Oracle 数据库文件和日志的 NFS 卷。

1. 在云管理器中，访问 FSx 集群的卷列表。



2. 从操作菜单中，选择“挂载命令”以查看和复制要在我们的 Oracle Linux 服务器上使用的挂载命令。





3. 将 NFS 文件系统挂载到 Oracle Linux 服务器。用于挂载 NFS 共享的目录已存在于 Oracle Linux 主机上。
4. 从 Oracle Linux 服务器，使用 mount 命令挂载 NFS 卷。

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

对与 Oracle 数据库关联的每个卷重复此步骤。

要使 NFS 挂载在重启后持久化，请编辑 `/etc/fstab`文件以包含挂载命令。

5. 重新启动 Oracle 服务器。 Oracle 数据库应该正常启动并可供使用。

故障回复

成功完成此解决方案中概述的故障转移过程后， SnapCenter和 Veeam 将恢复在 AWS 中运行的备份功能，并且FSx ONTAP现在被指定为主存储，与原始内部部署数据中心不存在现有的SnapMirror关系。在本地恢复正常功能后，您可以使用与本文档中概述的流程相同的流程将数据镜像回本地ONTAP存储系统。

正如本文档中概述的，您可以配置SnapCenter将应用程序数据卷从 FSx ONTAP镜像到位于本地的ONTAP存储系统。类似地，您可以配置 Veeam 使用横向扩展备份存储库将备份副本复制到 Amazon S3，以便位于本地数据中心的 Veeam 备份服务器可以访问这些备份。

故障回复超出了本文档的范围，但故障回复与此处概述的详细过程略有不同。

结束语

本文档中介绍的用例重点关注经过验证的灾难恢复技术，突出了NetApp和 VMware 之间的集成。 NetApp ONTAP存储系统提供成熟的数据镜像技术，使组织能够设计涵盖本地和领先云提供商所采用的ONTAP技术的灾难恢复解决方案。

AWS 上的 FSx ONTAP就是这样一种解决方案，它允许与SnapCenter和SyncMirror无缝集成，以将应用程序数据复制到云端。 Veeam Backup & Replication 是另一项知名技术，它与NetApp ONTAP存储系统很好地集成，

并可以为 vSphere 原生存储提供故障转移。

该解决方案提供了一种灾难恢复解决方案，使用托管 SQL Server 和 Oracle 应用程序数据的ONTAP系统的客户连接存储。带有SnapMirror的SnapCenter提供了一种易于管理的解决方案，用于保护ONTAP系统上的应用程序卷并将其复制到驻留在云中的 FSx 或 CVO。 SnapCenter是一种支持 DR 的解决方案，可将所有应用程序数据故障转移到 AWS 上的 VMware Cloud。

VMware Cloud 中的 **Veeam** 备份和还原，搭配**Amazon FSx ONTAP**

Veeam Backup & Replication 是保护 VMware Cloud 中数据的有效且可靠的解决方案。该解决方案演示了使用 Veeam Backup and Replication 备份和恢复 VMware Cloud 中 FSx ONTAP NFS 数据存储区上的应用程序虚拟机的正确设置和配置。

概述

VMware Cloud（在 AWS 中）支持使用 NFS 数据存储作为补充存储，而 FSx ONTAP对于需要为其云应用程序存储大量数据的客户来说是一种安全的解决方案，并且可以独立于 SDDC 集群中的 ESXi 主机数量进行扩展。此集成的 AWS 存储服务提供高效存储以及所有传统的NetApp ONTAP功能。

使用案例

此解决方案适用于以下用例：

- 使用 FSx ONTAP作为备份存储库，备份和恢复 VMC 中托管的 Windows 和 Linux 虚拟机。
- 使用 FSx ONTAP作为备份存储库备份和恢复 Microsoft SQL Server 应用程序数据。
- 使用 FSx ONTAP作为备份存储库备份和恢复 Oracle 应用程序数据。

使用**Amazon FSx ONTAP** 的**NFS** 数据存储

此解决方案中的所有虚拟机都驻留在 FSx ONTAP补充 NFS 数据存储上。使用 FSx ONTAP作为补充 NFS 数据存储有几个好处。例如，它允许您：

- 在云中创建可扩展且高度可用的文件系统，无需复杂的设置和管理。
- 与您现有的 VMware 环境集成，使您可以使用熟悉的工具和流程来管理您的云资源。
- 利用ONTAP提供的高级数据管理功能（例如快照和复制）来保护您的数据并确保其可用性。

▼ 解决方案部署概述

此列表提供了配置 Veeam Backup & Replication、使用 FSx ONTAP作为备份存储库执行备份和还原作业以及执行 SQL Server 和 Oracle VM 和数据库还原所需的高级步骤：

1. 创建 FSx ONTAP文件系统，用作 Veeam Backup & Replication 的 iSCSI 备份存储库。
2. 部署 Veeam Proxy 以分配备份工作负载并挂载 FSx ONTAP上托管的 iSCSI 备份存储库。
3. 配置 Veeam Backup Jobs 来备份 SQL Server、Oracle、Linux 和 Windows 虚拟机。
4. 还原 SQL Server 虚拟机和单个数据库。
5. 恢复 Oracle 虚拟机和单个数据库。

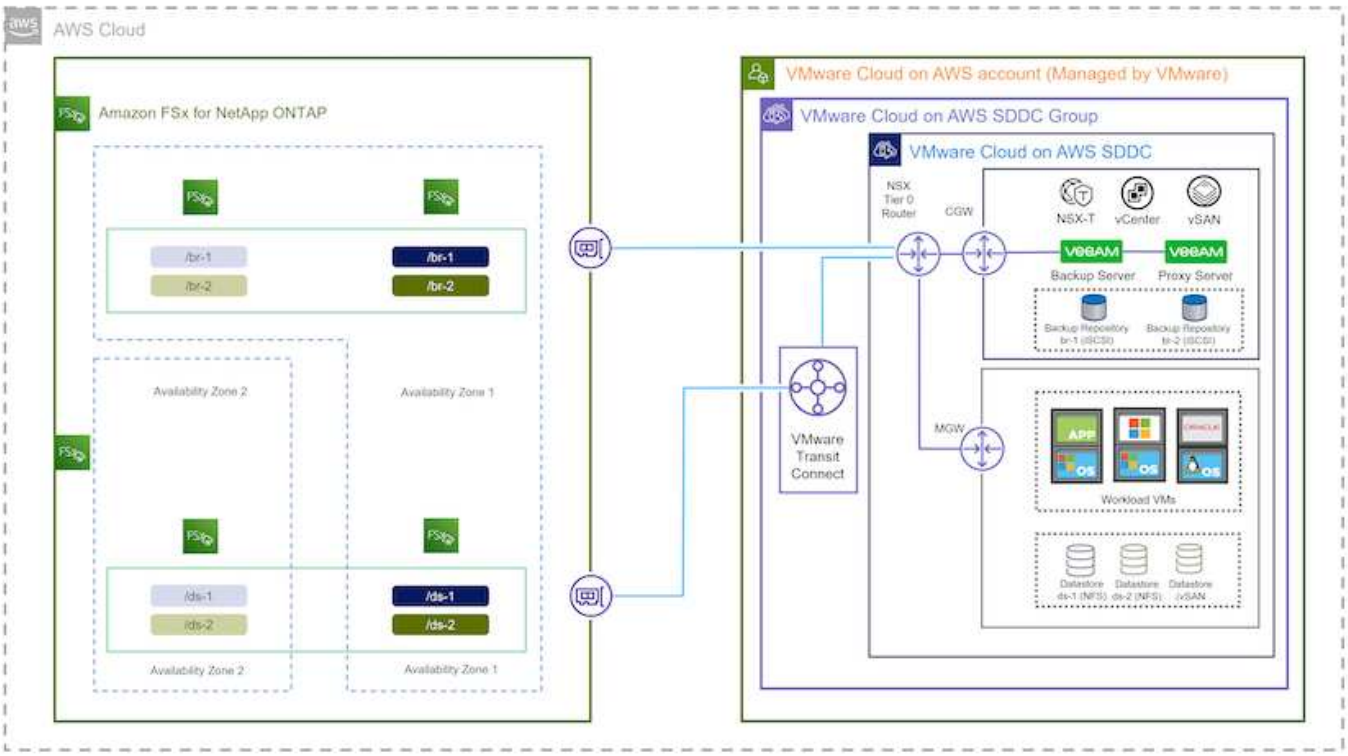
▼ 前提条件

此解决方案的目的是展示在 VMware Cloud 中运行并位于 FSx ONTAP托管的 NFS 数据存储上的虚拟机的数据保护。此解决方案假定以下组件已配置并可供使用：

1. 具有一个或多个连接到 VMware Cloud 的 NFS 数据存储的 FSx ONTAP文件系统。
2. 安装了 Veeam Backup & Replication 软件的 Microsoft Windows Server VM。
   - Veeam Backup & Replication 服务器已使用其 IP 地址或完全限定域名发现 vCenter 服务器。
3. 在解决方案部署期间，Microsoft Windows Server VM 将与 Veeam Backup Proxy 组件一起安装。
4. 带有 VMDK 和应用程序数据的 Microsoft SQL Server VM 驻留在 FSx ONTAP NFS 数据存储区上。对于此解决方案，我们在两个独立的 VMDK 上有两个 SQL 数据库。
   - 注意：最佳实践是将数据库和事务日志文件放在单独的驱动器上，因为这将提高性能和可靠性。部分原因是由于事务日志是按顺序写入的，而数据库文件是随机写入的。
5. 带有 VMDK 和应用程序数据的 Oracle 数据库虚拟机驻留在 FSx ONTAP NFS 数据存储区上。
6. 具有 VMDK 的 Linux 和 Windows 文件服务器虚拟机驻留在 FSx ONTAP NFS 数据存储区上。
7. Veeam 需要特定的 TCP 端口来实现备份环境中的服务器和组件之间的通信。在 Veeam 备份基础架构组件上，会自动创建所需的防火墙规则。有关网络端口要求的完整列表，请参阅 "适用于 VMware vSphere 的 Veeam Backup and Replication 用户指南"。

高级架构

该解决方案的测试/验证是在实验室中进行的，该实验室可能与最终部署环境匹配，也可能不匹配。欲了解更多信息，请参阅以下章节。



▼ 硬件/软件组件

此解决方案的目的是展示在 VMware Cloud 中运行并位于 FSx ONTAP托管的 NFS 数据存储上的虚拟机的数据保护。此解决方案假定以下组件已配置并可供使用：

- 位于 FSx ONTAP NFS 数据存储上的 Microsoft Windows VM
- 位于 FSx ONTAP NFS 数据存储上的 Linux (CentOS) VM
- 位于 FSx ONTAP NFS 数据存储上的 Microsoft SQL Server VM
  - 两个数据库托管在不同的 VMDK 上
- 位于 FSx ONTAP NFS 数据存储上的 Oracle VM

解决方案部署

在此解决方案中，我们提供了有关部署和验证解决方案的详细说明，该解决方案利用 Veeam Backup 和 Replication 软件在 AWS 上的 VMware Cloud SDDC 中执行 SQL Server、Oracle 以及 Windows 和 Linux 文件服务器虚拟机的备份和恢复。此解决方案中的虚拟机驻留在由 FSx ONTAP托管的补充 NFS 数据存储上。此外，单独的 FSx ONTAP文件系统用于托管将用于 Veeam 备份存储库的 iSCSI 卷。

我们将介绍 FSx ONTAP文件系统的创建、挂载 iSCSI 卷以用作备份存储库、创建和运行备份作业以及执行 VM 和数据库恢复。

有关 FSx ONTAP的详细信息，请参阅 "FSx ONTAP用户指南"。

有关 Veeam Backup and Replication 的详细信息，请参阅 "Veeam 帮助中心技术文档"地点。

有关在 VMware Cloud on AWS 上使用 Veeam Backup and Replication 时的注意事项和限制，请参阅 "VMware Cloud on AWS 和 VMware Cloud on Dell EMC 支持。注意事项和限制"。

部署 **Veeam** 代理服务器

Veeam 代理服务器是 Veeam Backup & Replication 软件的一个组件，充当源和备份或复制目标之间的中介。代理服务器通过在本地处理数据来帮助优化和加速备份作业期间的数据传输，并且可以使用不同的传输模式通过 VMware vStorage API 进行数据保护或通过直接存储访问来访问数据。

在选择 Veeam 代理服务器设计时，重要的是考虑并发任务的数量以及所需的传输模式或存储访问类型。

有关代理服务器数量及其系统要求，请参阅 "Veeam VMware vSphere 最佳实践指南"。

Veeam Data Mover 是 Veeam Proxy Server 的一个组件，它利用传输模式作为从源获取 VM 数据并将其传输到目标的方法。传输模式是在备份作业配置期间指定的。通过使用直接存储访问，可以提高 NFS 数据存储的备份效率。

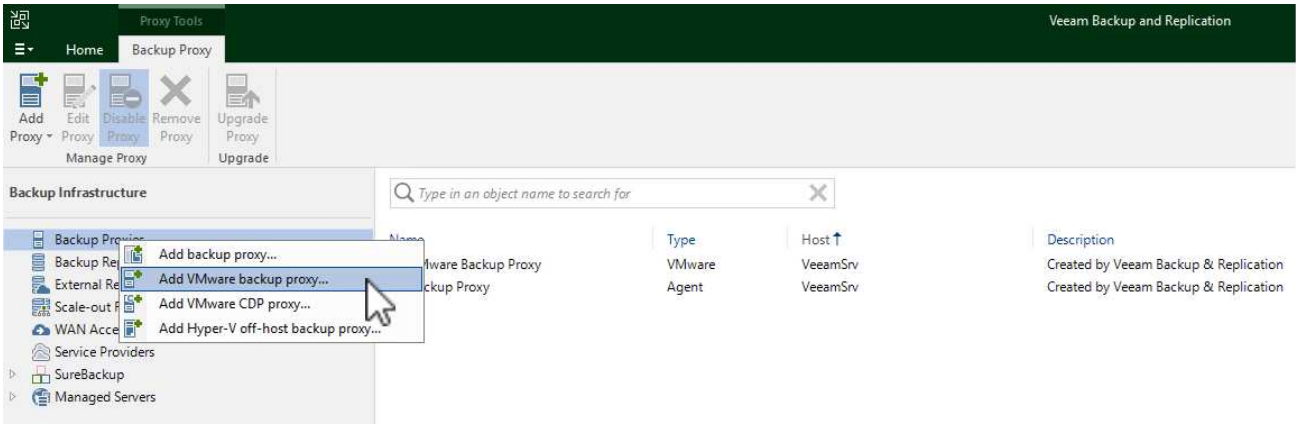
有关运输方式的更多信息，请参阅 "适用于 VMware vSphere 的 Veeam Backup and Replication 用户指南"。

在下一步中，我们将介绍在 VMware Cloud SDDC 中的 Windows VM 上部署 Veeam 代理服务器。

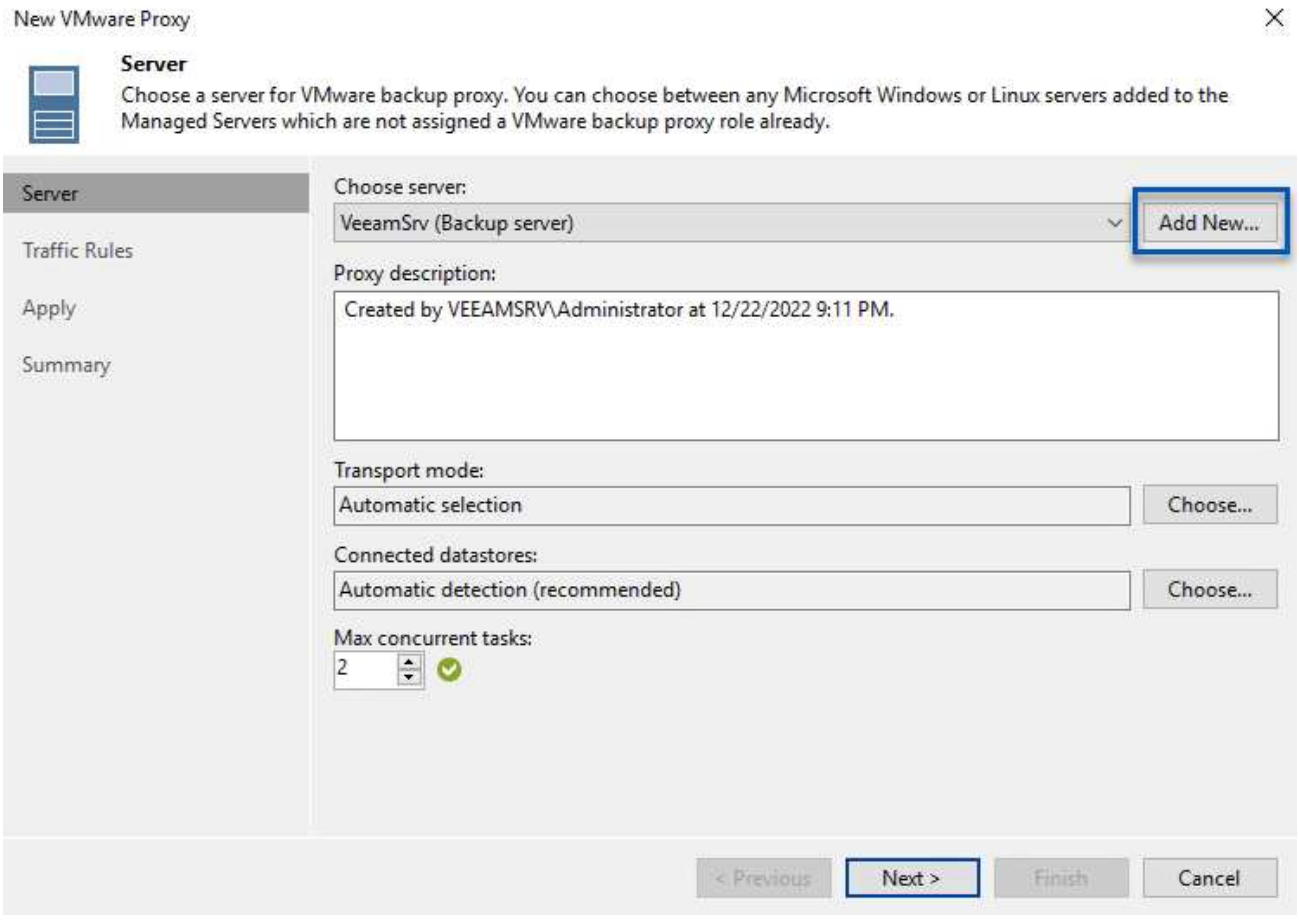
▼ 部署 **Veeam Proxy** 以分配备份工作负载

在此步骤中，Veeam Proxy 被部署到现有的 Windows VM。这允许备份作业在主 Veeam 备份服务器和 Veeam 代理之间分配。

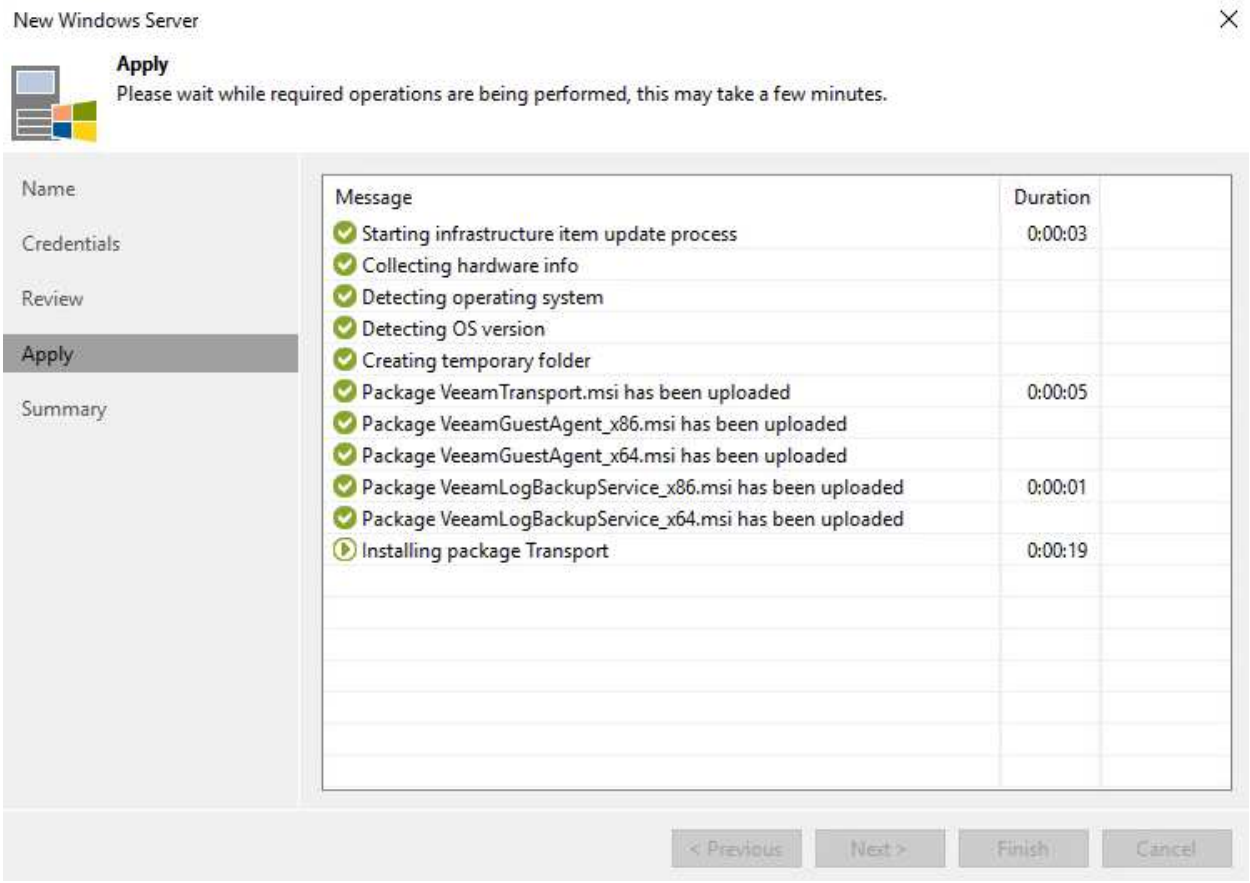
1. 在 Veeam Backup and Replication 服务器上，打开管理控制台并在左下角菜单中选择 **Backup Infrastructure**。
2. 右键单击“备份代理”，然后单击“添加 **VMware** 备份代理...”以打开向导。



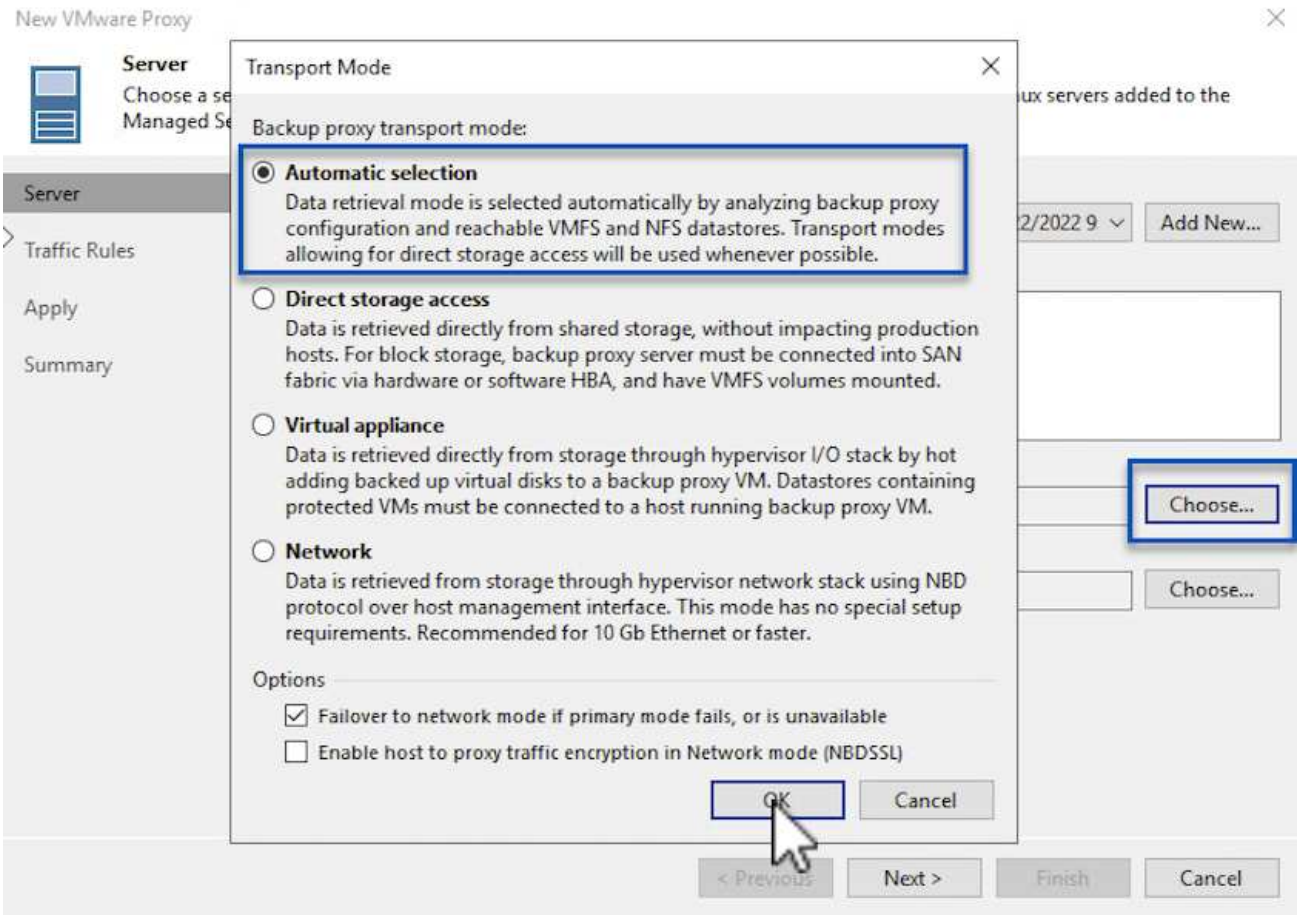
3. 在“添加 VMware 代理”向导中，单击“添加新…”按钮以添加新的代理服务器。



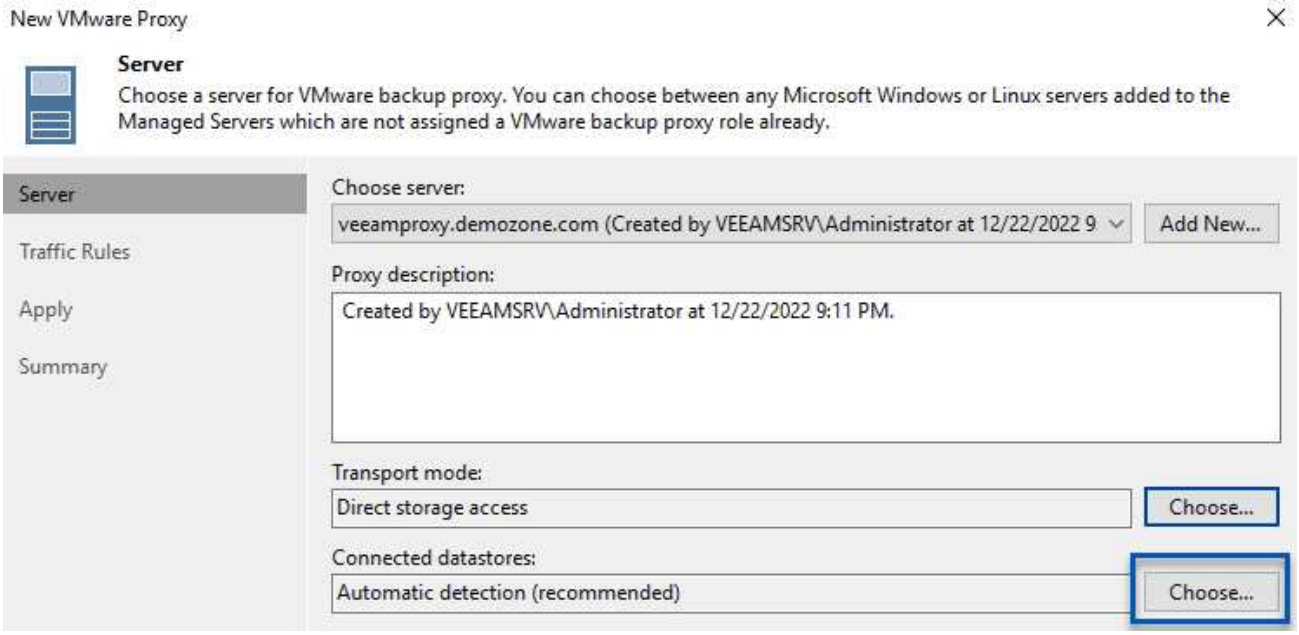
4. 选择添加Microsoft Windows并按照提示添加服务器：
   - 填写DNS名称或IP地址
   - 选择新系统上用于凭证的帐户或添加新凭证
   - 检查要安装的组件，然后单击“应用”开始部署

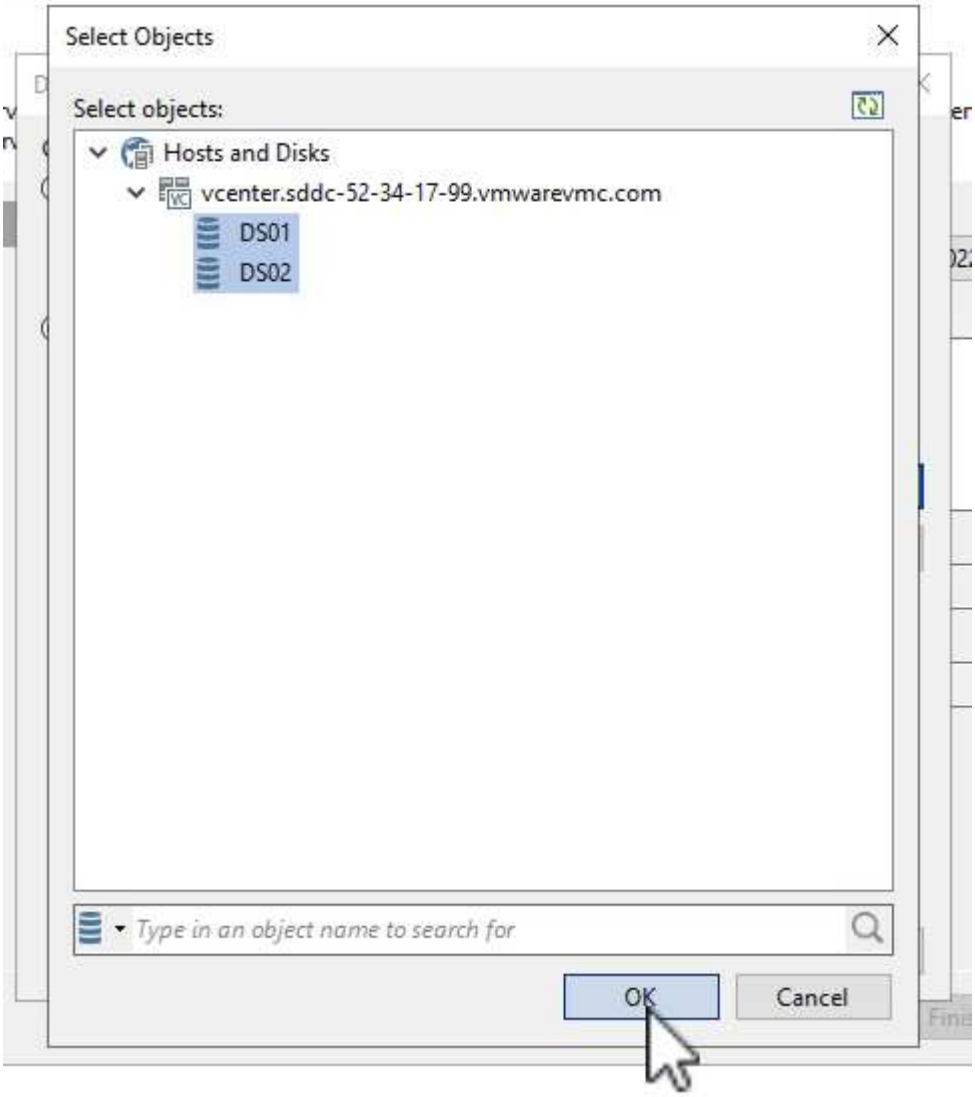


5. 返回“新建 VMware 代理”向导，选择传输模式。在我们的例子中，我们选择了*自动选择*。

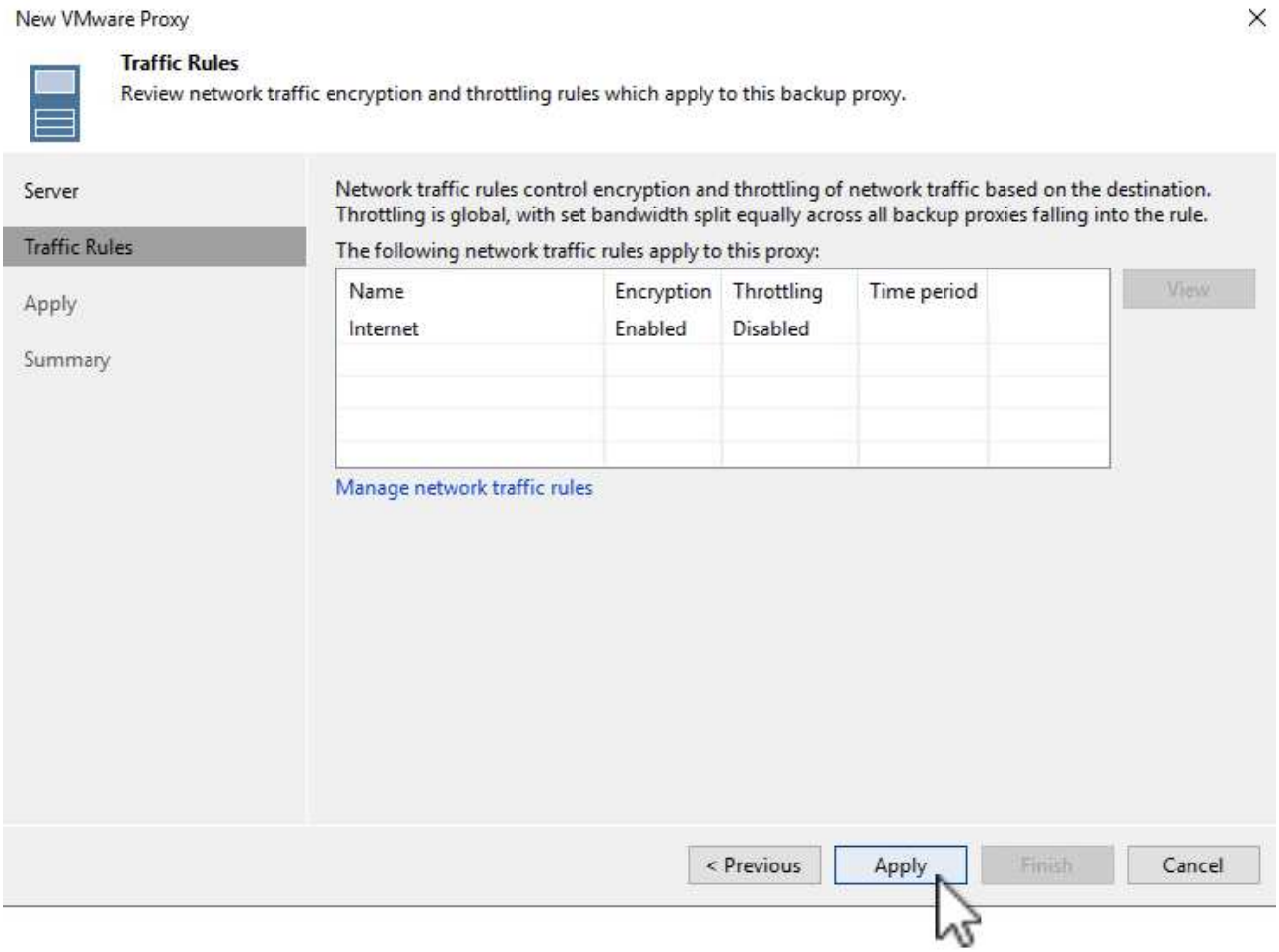


6. 选择您希望 VMware 代理直接访问的已连接数据存储。





7. 配置并应用所需的任何特定网络流量规则，例如加密或限制。完成后单击“应用”按钮即可完成部署。



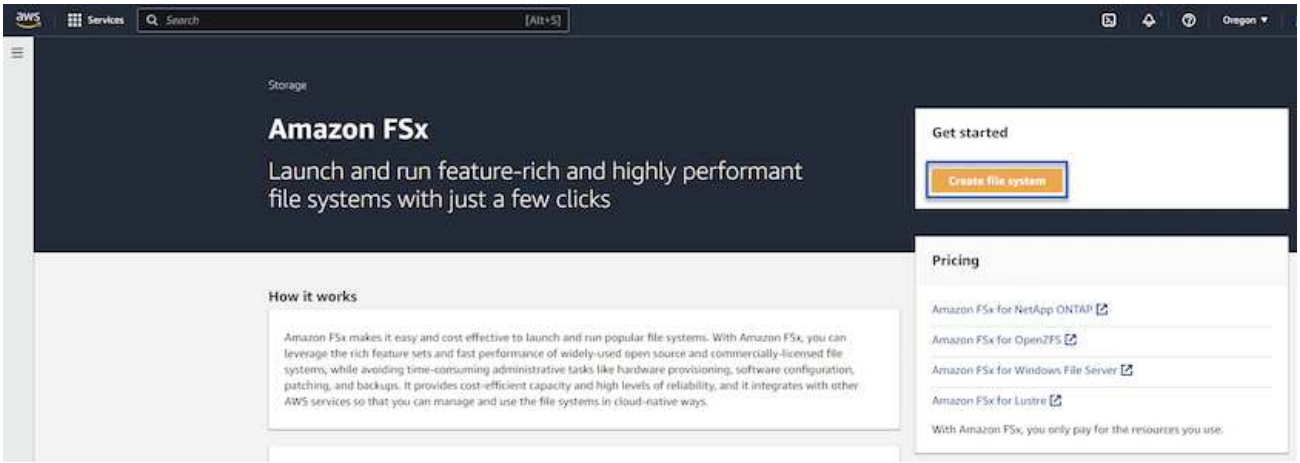
配置存储和备份存储库

主 Veeam Backup 服务器和 Veeam Proxy 服务器可以以直接连接存储的形式访问备份存储库。在本节中，我们介绍如何创建 FSx ONTAP文件系统、将 iSCSI LUN 安装到 Veeam 服务器以及创建备份存储库。

▼ 创建 **FSx ONTAP**文件系统

创建一个 FSx ONTAP文件系统，用于托管 Veeam 备份存储库的 iSCSI 卷。

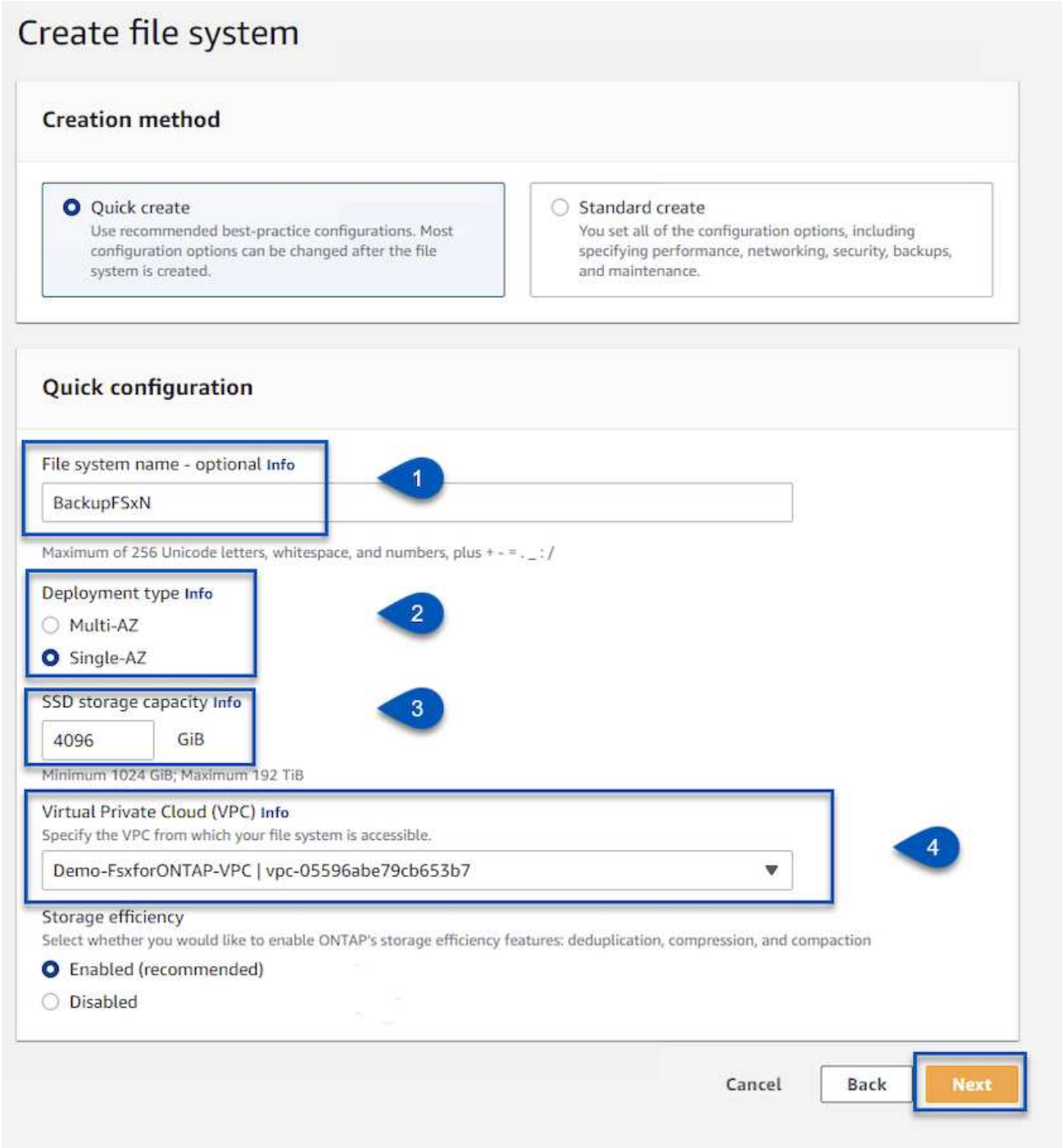
1. 在 AWS 控制台中，转到 FSx，然后 创建文件系统



2. 选择 * Amazon FSx ONTAP*，然后选择 下一步 继续。



3. 填写文件系统名称、部署类型、SSD 存储容量以及 FSx ONTAP集群所在的 VPC。这必须是配置为与 VMware Cloud 中的虚拟机网络通信的 VPC。单击“下一步”。



4. 查看部署步骤并单击*创建文件系统*开始文件系统创建过程。

▼ 配置并挂载 **iSCSI LUN**

在 FSx ONTAP上创建和配置 iSCSI LUN 并安装到 Veeam 备份和代理服务器。这些 LUN 稍后将用于创建 Veeam 备份存储库。

在 FSx ONTAP上创建 iSCSI LUN 是一个多步骤的过程。创建卷的第一步可以在Amazon FSx 控制台或使用NetApp ONTAP CLI 完成。

有关使用 FSx ONTAP 的更多信息，请参阅 "FSx ONTAP用户指南"。

1. 从NetApp ONTAP CLI 使用以下命令创建初始卷：

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. 使用上一步创建的卷创建 LUN：

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. 通过创建包含 Veeam 备份和代理服务器的 iSCSI IQN 的启动器组来授予对 LUN 的访问权限：

```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

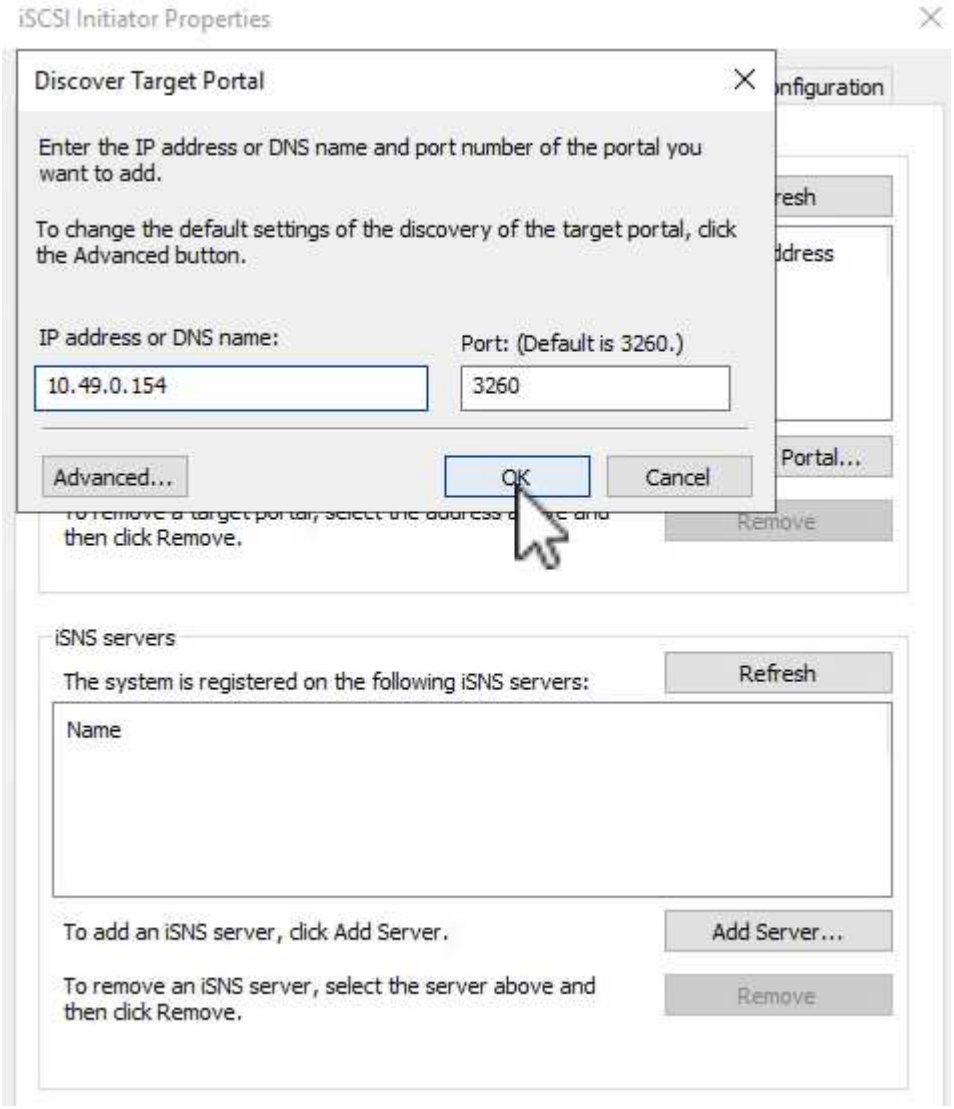


要完成前面的步骤，您需要首先从 Windows 服务器上的 iSCSI 启动器属性中检索 IQN。

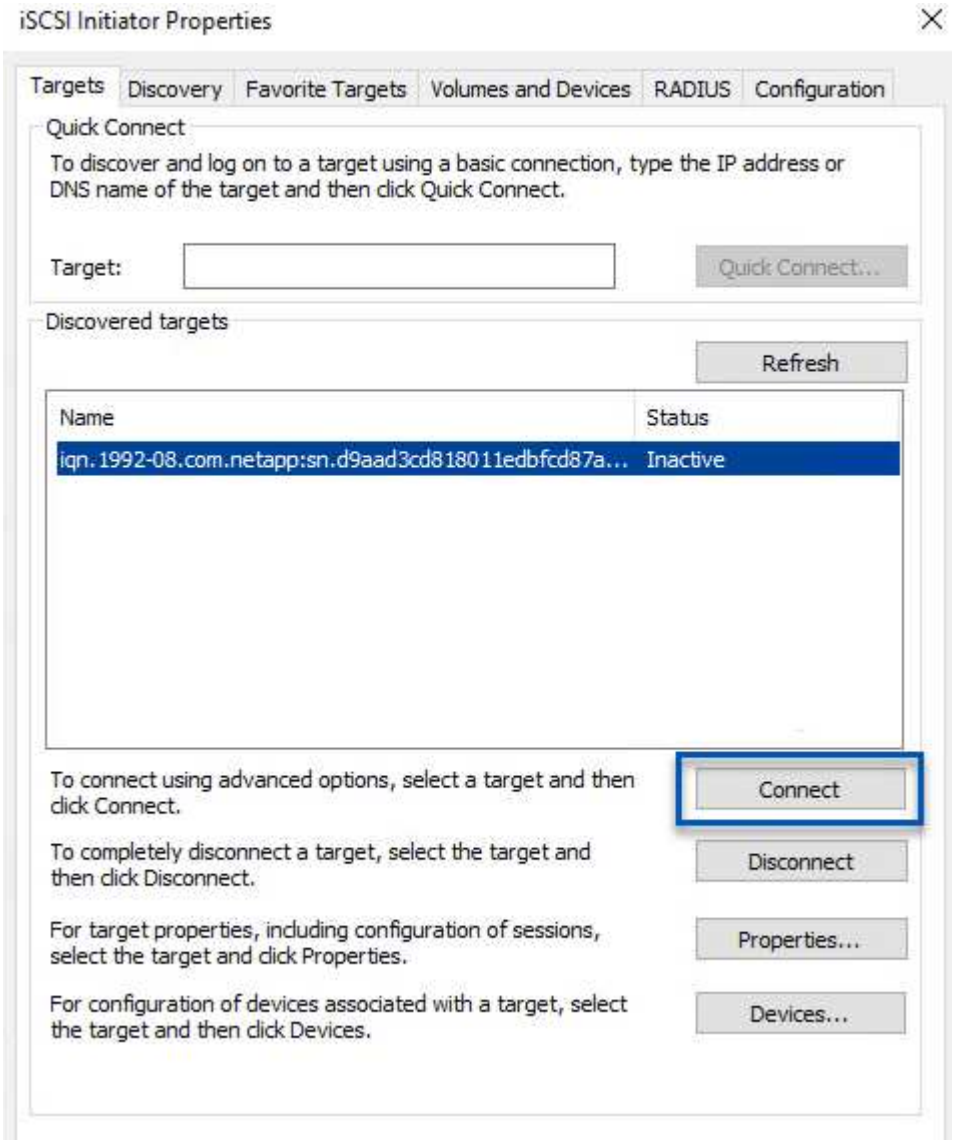
4. 最后，将 LUN 映射到刚刚创建的启动器组：

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

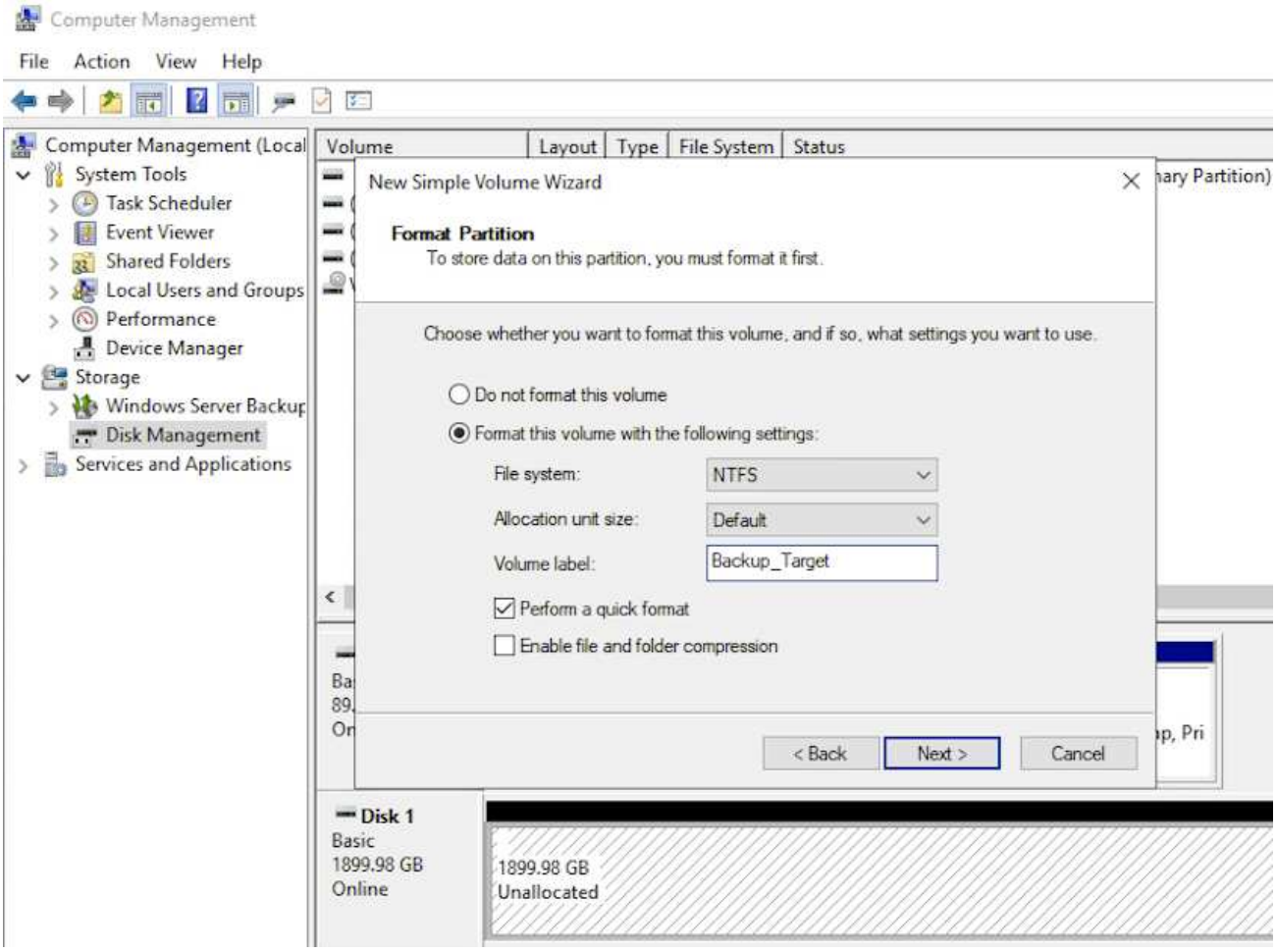
5. 要安装 iSCSI LUN，请登录 Veeam Backup & Replication Server 并打开 iSCSI Initiator Properties。转到“发现”选项卡并输入 iSCSI 目标 IP 地址。



6. 在“目标”选项卡上，突出显示非活动 LUN，然后单击“连接”。选中“启用多路径”框并单击“确定”以连接到 LUN。



7. 在磁盘管理实用程序中初始化新的 LUN 并创建具有所需名称和驱动器号的卷。选中“启用多路径”框并单击“确定”以连接到 LUN。

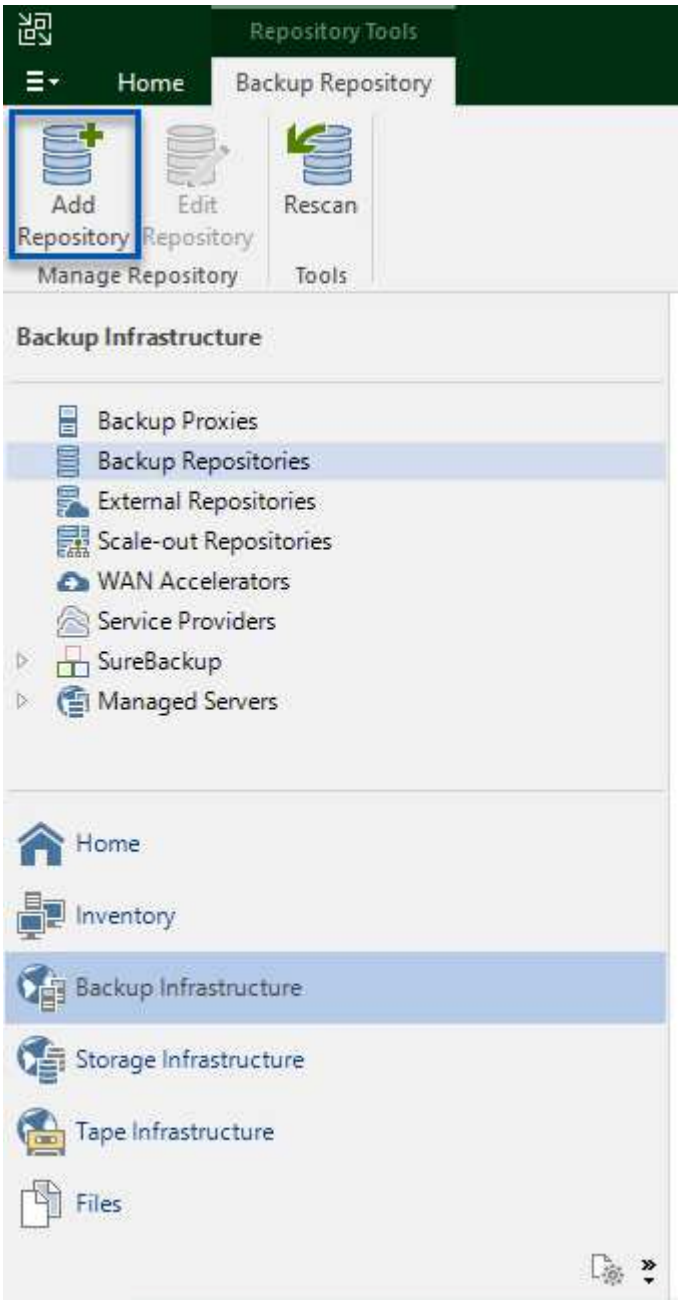


8. 重复这些步骤以在 Veeam 代理服务器上挂载 iSCSI 卷。

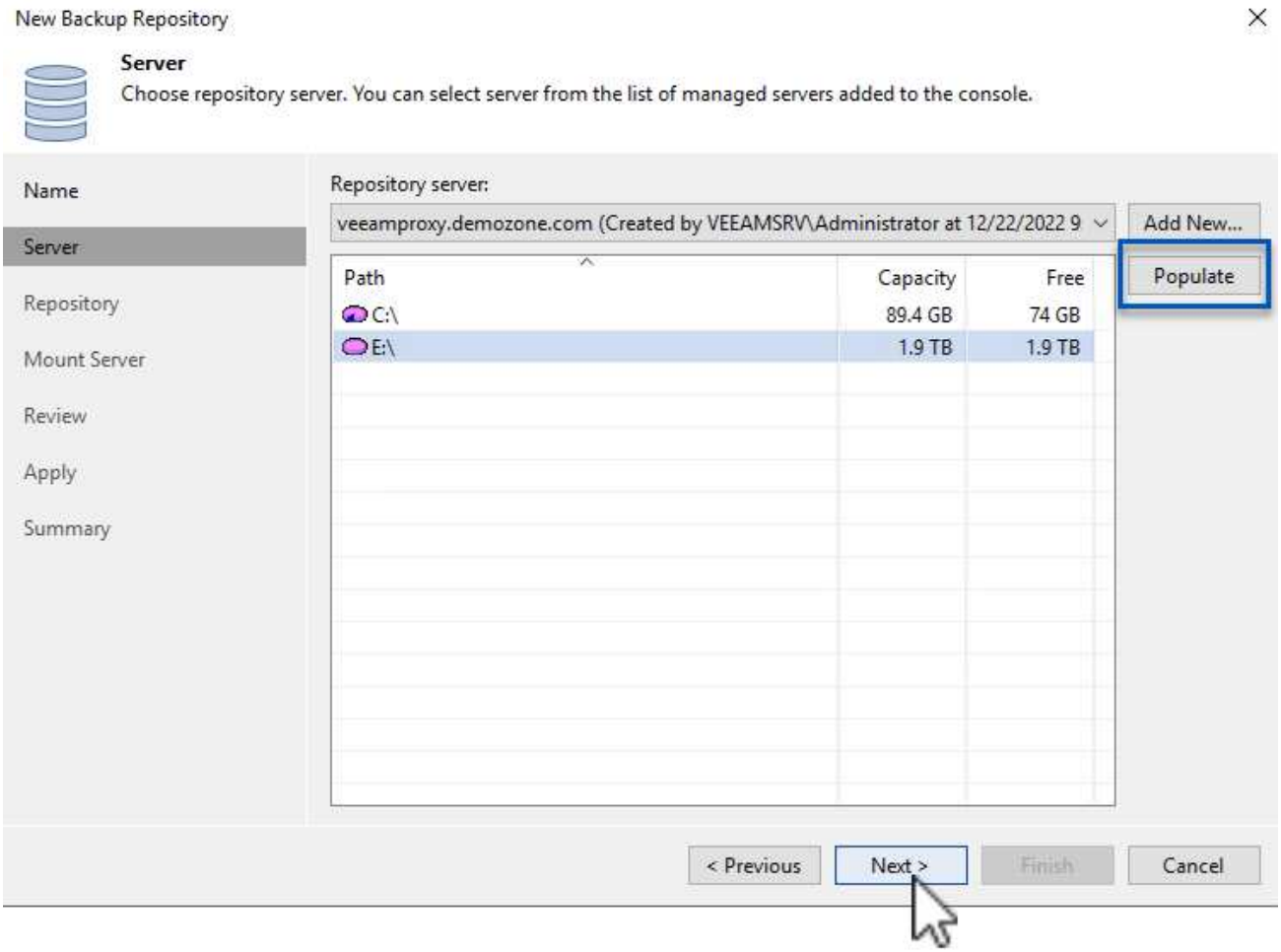
▼ 创建 **Veeam** 备份存储库

在 Veeam Backup and Replication 控制台中，为 Veeam Backup 和 Veeam Proxy 服务器创建备份存储库。这些存储库将用作虚拟机备份的备份目标。

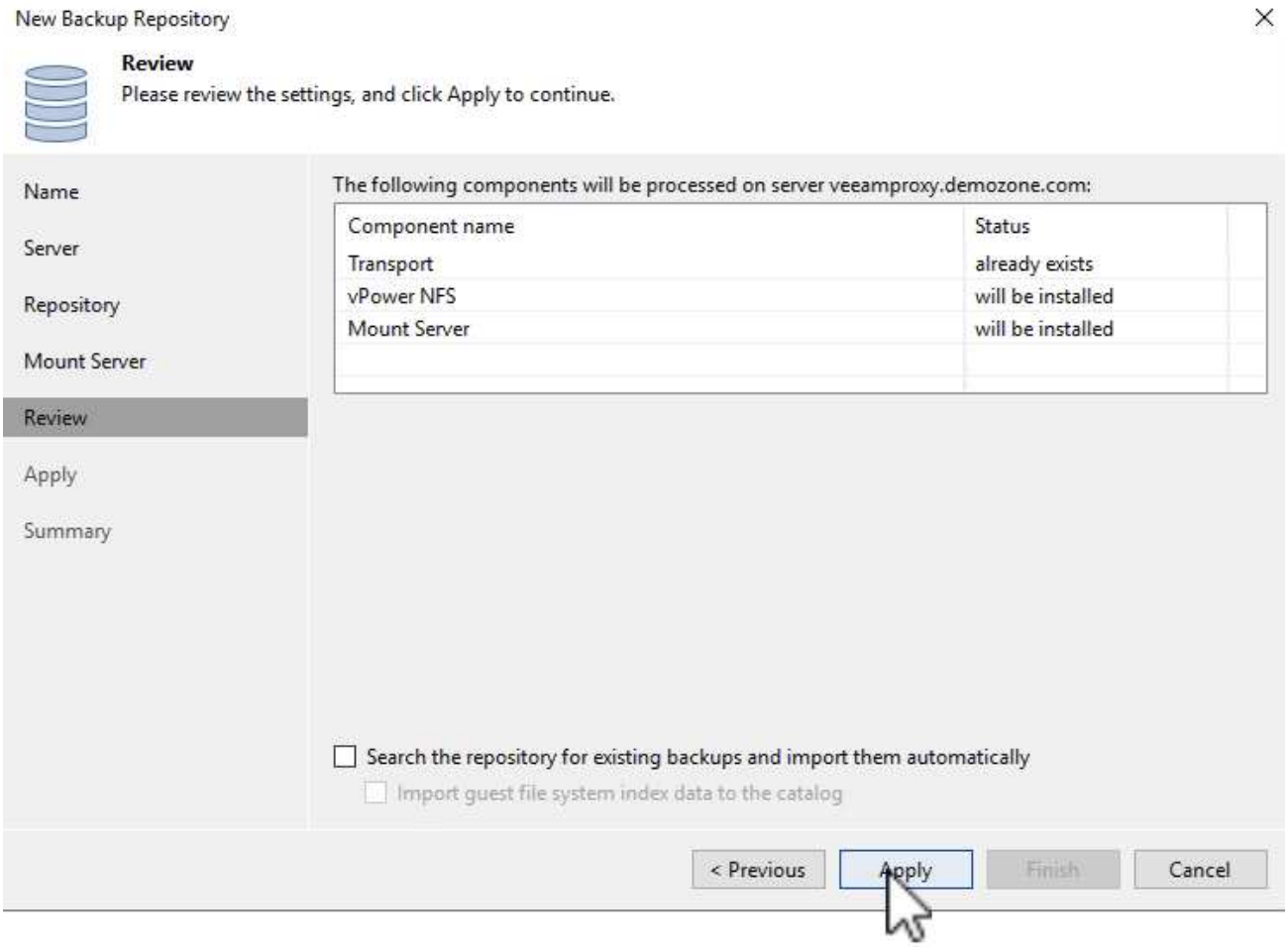
1. 在 Veeam Backup and Replication 控制台中，单击左下角的“备份基础架构”，然后选择“添加存储库”



2. 在新建备份存储库向导中，输入存储库的名称，然后从下拉列表中选择服务器，并单击*填充*按钮以选择将使用的 NTFS 卷。



3. 在下一页上，选择执行高级恢复时用于挂载备份的挂载服务器。默认情况下，这是与存储库存储连接的同一服务器。
4. 检查您的选择并单击“应用”开始创建备份存储库。



5. 对任何其他代理服务器重复这些步骤。

配置 **Veeam** 备份作业

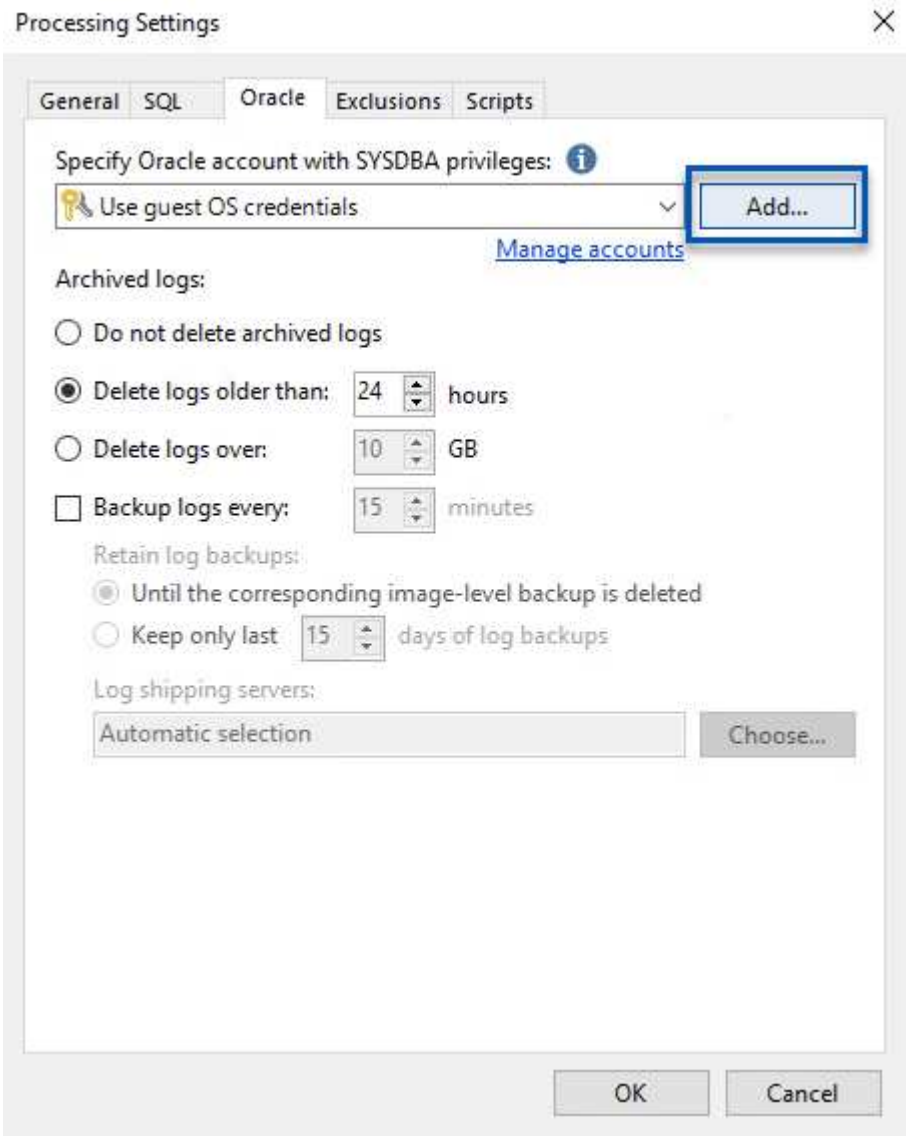
应利用上一节中的备份存储库创建备份作业。创建备份作业是任何存储管理员的正常工作的一部分，我们不会在这里介绍所有步骤。有关在 Veeam 中创建备份作业的更多完整信息，请参阅 "Veeam 帮助中心技术文档"。

在此解决方案中，为以下内容创建了单独的备份作业：

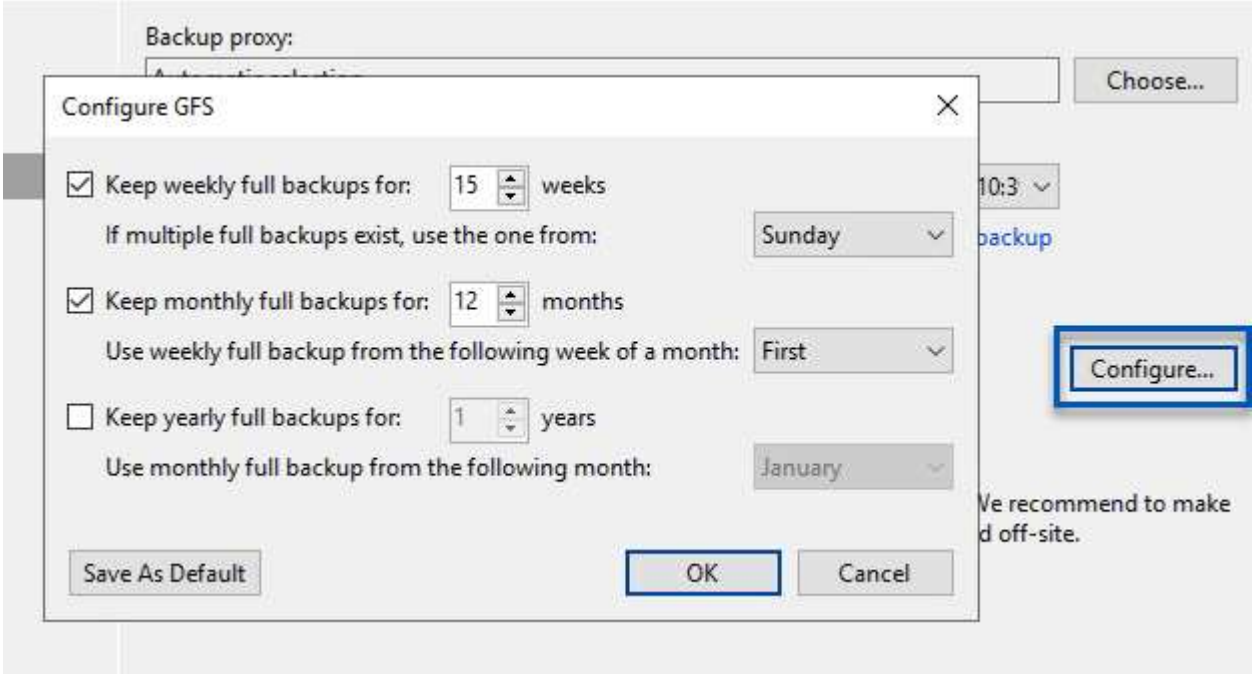
- Microsoft Windows SQL 服务器
- Oracle 数据库服务器
- Windows 文件服务器
- Linux 文件服务器

▼ 配置 **Veeam** 备份作业时的一般注意事项

1. 启用应用程序感知处理来创建一致的备份并执行事务日志处理。
2. 启用应用程序感知处理后，向应用程序添加具有管理员权限的正确凭据，因为这可能与来宾操作系统凭据不同。



3. 要管理备份的保留策略，请选中*将某些完整备份保留更长时间以用于存档目的*，然后单击*配置…*按钮来配置策略。



使用 **Veeam** 完整恢复功能恢复应用程序虚拟机

使用 Veeam 执行完整恢复是执行应用程序恢复的第一步。我们验证了虚拟机的完全恢复已启动并且所有服务均正常运行。

恢复服务器是任何存储管理员的正常工作的一部分，我们不会在这里介绍所有步骤。有关在 Veeam 中执行完整恢复的更多完整信息，请参阅 "Veeam 帮助中心技术文档"。

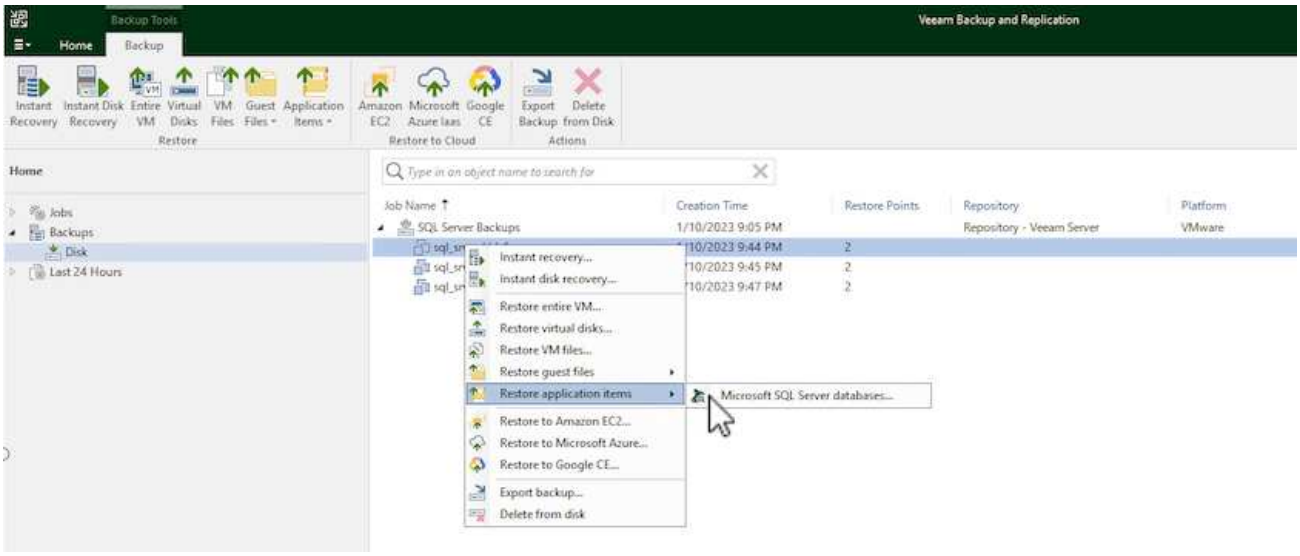
还原 **SQL Server** 数据库

Veeam Backup & Replication 提供了多种用于恢复 SQL Server 数据库的选项。为了进行此验证，我们使用具有即时恢复功能的 Veeam Explorer for SQL Server 来执行 SQL Server 数据库的恢复。 SQL Server 即时恢复功能允许您快速还原 SQL Server 数据库，而无需等待完整的数据库还原。这种快速恢复过程可最大限度地减少停机时间并确保业务连续性。工作原理如下：

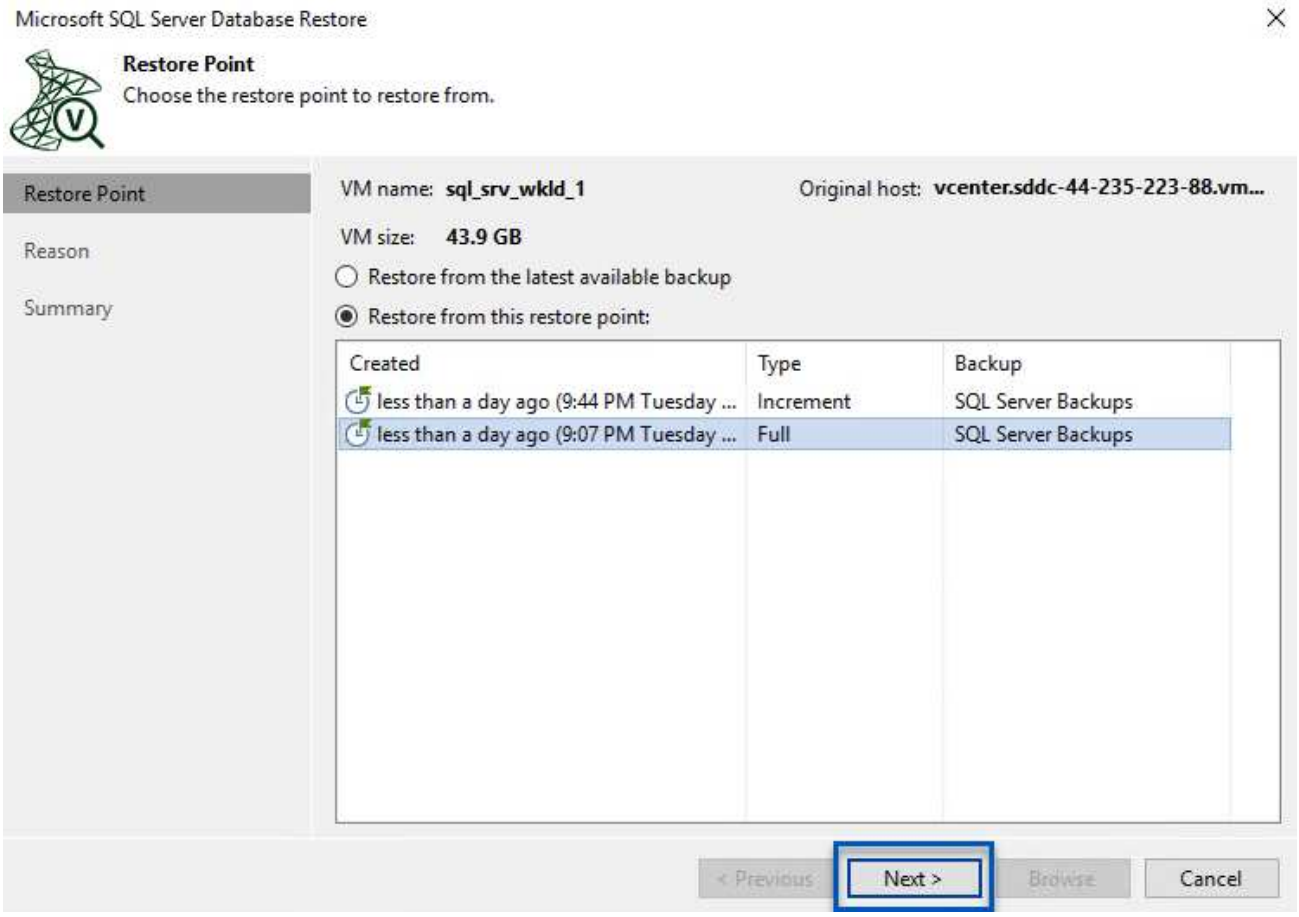
- Veeam Explorer 安装包含要恢复的 **SQL Server** 数据库的备份。
- 该软件直接从已安装的文件中*发布数据库*，使其可作为目标 SQL Server 实例上的临时数据库进行访问。
- 在使用临时数据库时，Veeam Explorer 会将用户查询重定向到该数据库，确保用户可以继续访问和使用数据。
- 在后台，Veeam 执行完整的数据库恢复，将数据从临时数据库传输到原始数据库位置。
- 一旦完整数据库恢复完成，Veeam Explorer 会将用户查询切换回原始*数据库并删除临时数据库。

▼ 使用 **Veeam Explorer Instant Recovery** 恢复 **SQL Server** 数据库

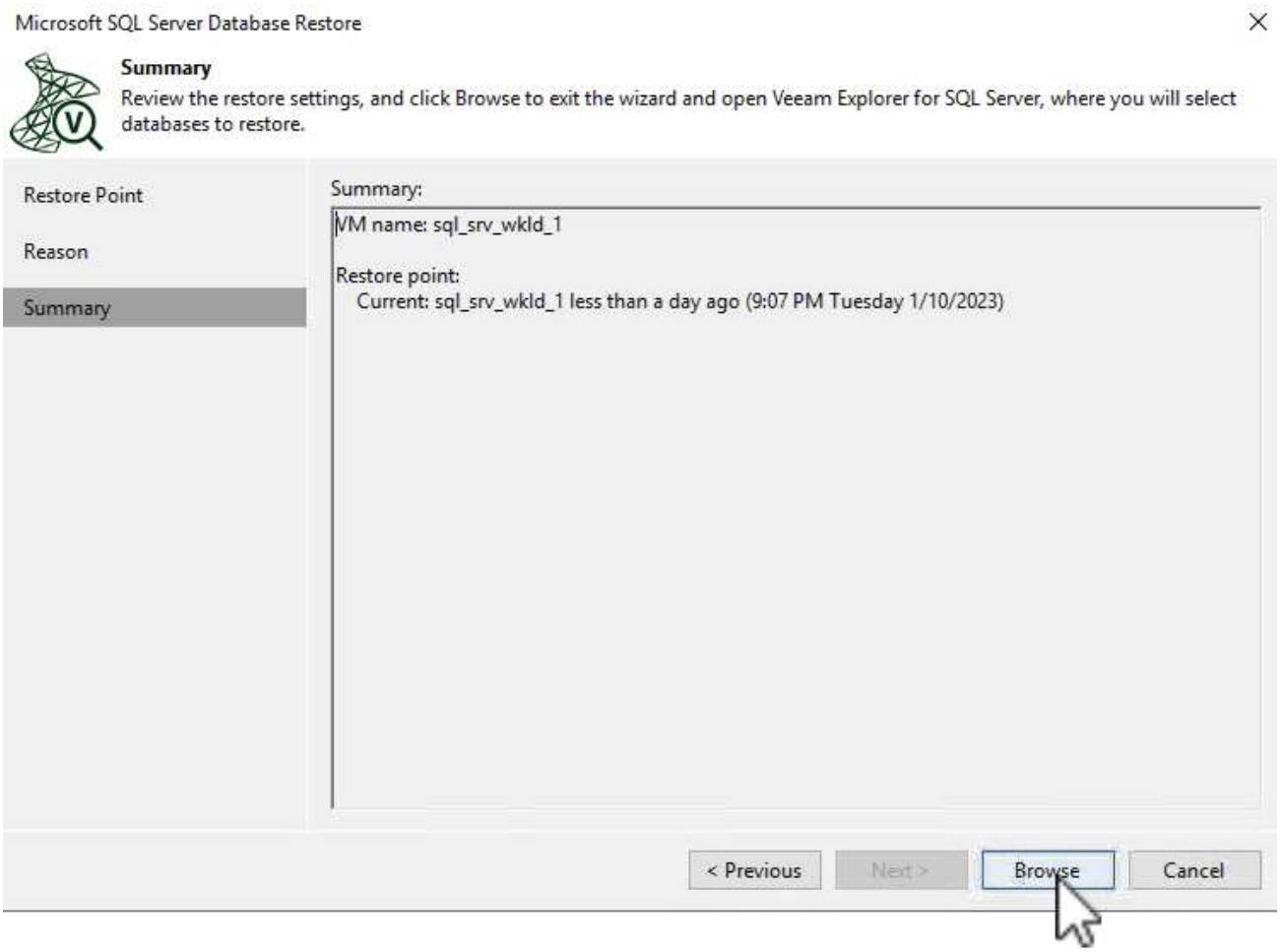
1. 在 Veeam Backup and Replication 控制台中，导航到 SQL Server 备份列表，右键单击服务器并选择 恢复应用程序项，然后选择 **Microsoft SQL Server** 数据库...。



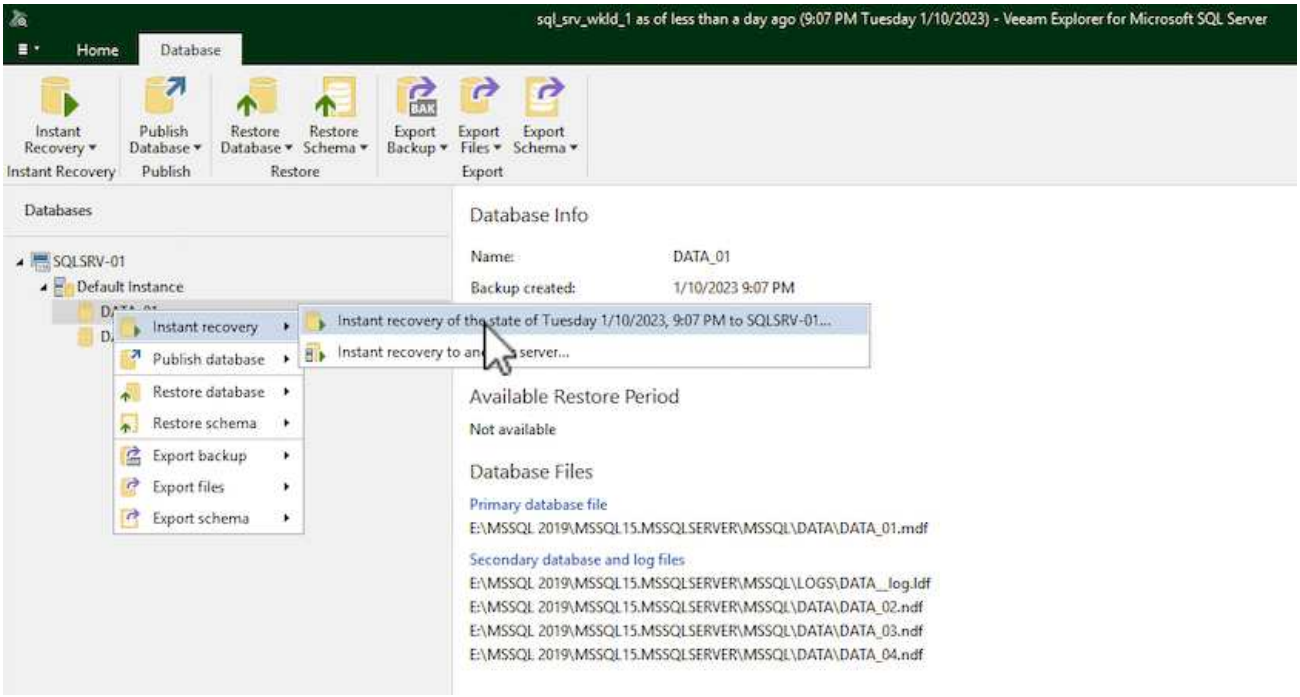
2. 在 Microsoft SQL Server 数据库还原向导中，从列表中选择一个还原点，然后单击“下一步”。



3. 如果需要，输入*恢复原因*，然后在摘要页面上，单击*浏览*按钮启动 Veeam Explorer for Microsoft SQL Server。

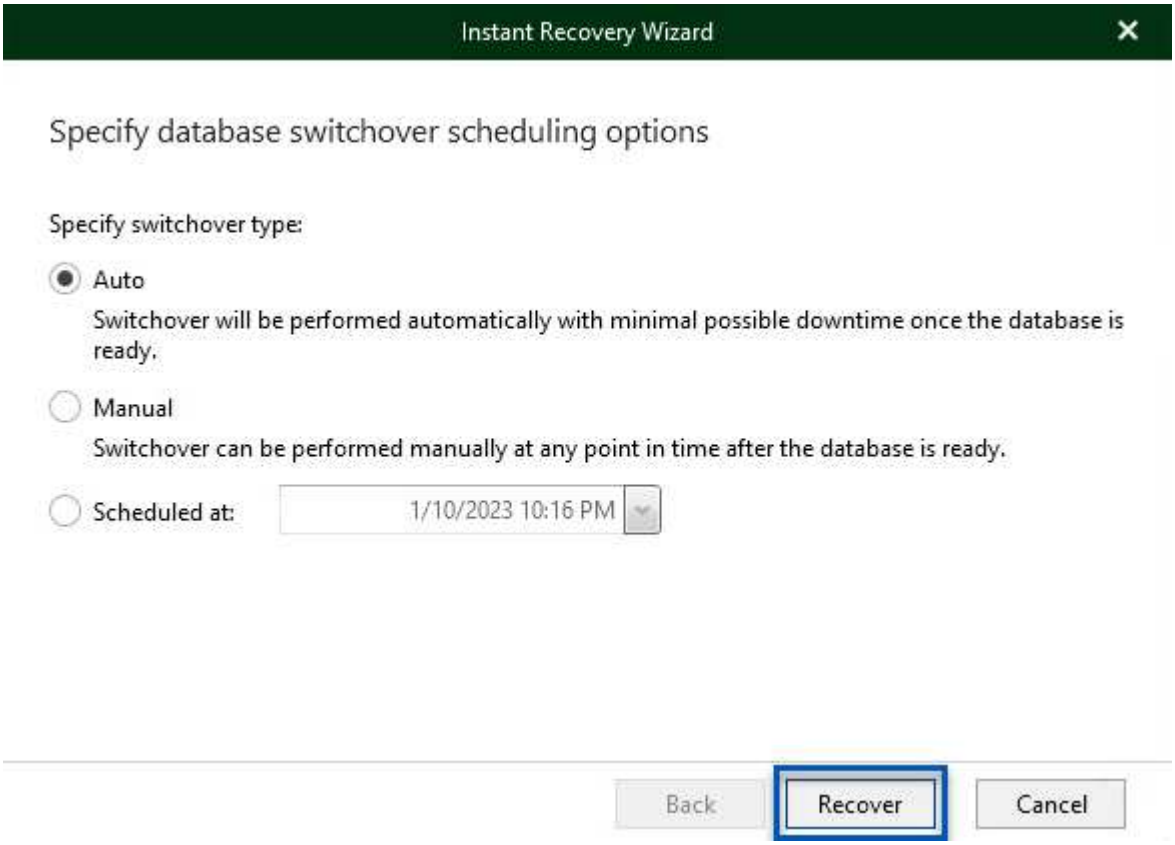


4. 在 Veeam Explorer 中展开数据库实例列表，右键单击并选择 即时恢复，然后选择要恢复到的特定还原点。

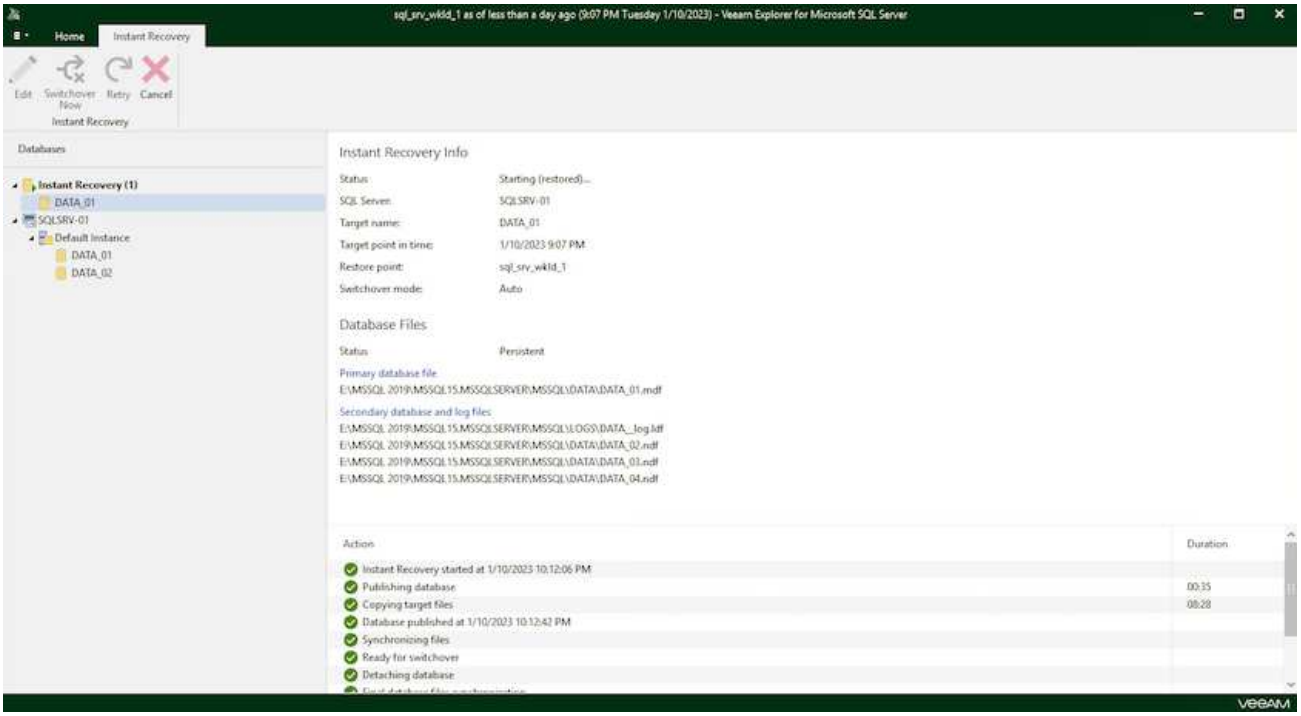


5. 在即时恢复向导中指定切换类型。这可以自动进行，停机时间最短，也可以手动进行，或者在指定时间进

行。然后单击“恢复”按钮开始恢复过程。



6. 可以从 Veeam Explorer 监控恢复过程。



有关使用 Veeam Explorer 执行 SQL Server 还原操作的更多详细信息，请参阅 "Veeam Explorers 用户指南"。

使用 **Veeam Explorer** 恢复 **Oracle** 数据库

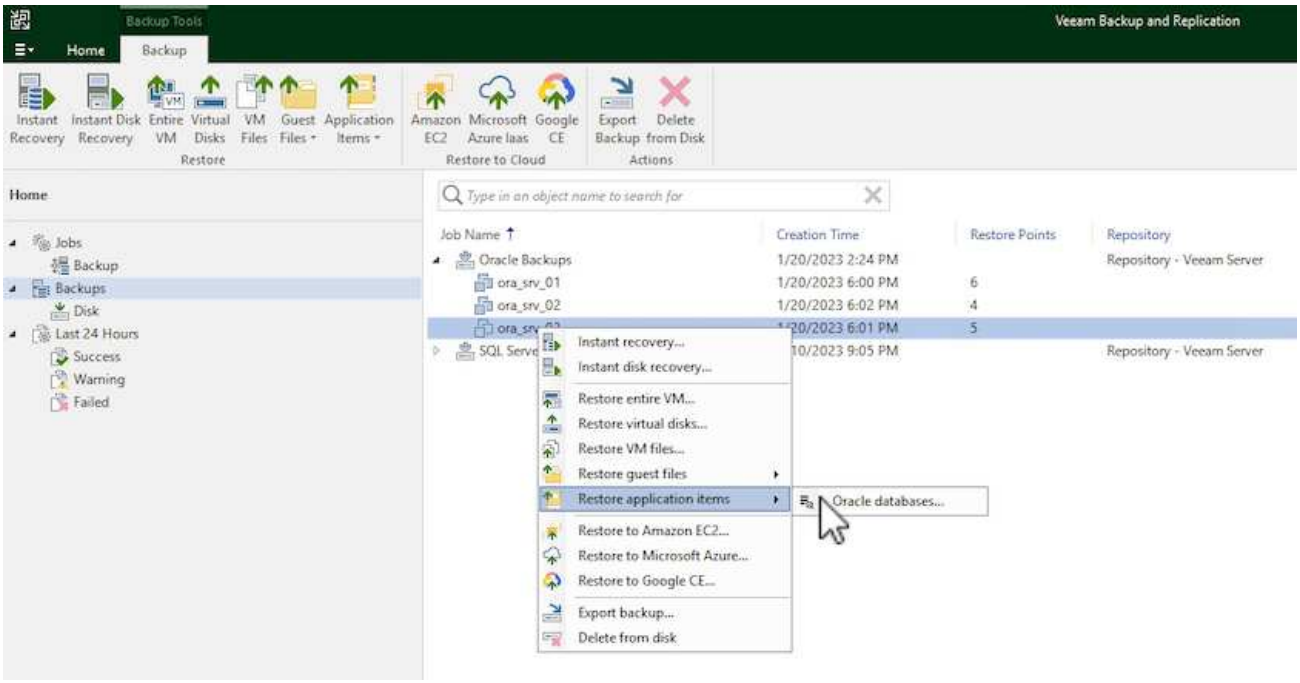
Veeam Explorer for Oracle 数据库提供了执行标准 Oracle 数据库还原或使用即时恢复进行不间断还原的能力。它还支持发布数据库以实现快速访问、恢复 Data Guard 数据库以及从 RMAN 备份中恢复。

有关使用 Veeam Explorer 执行 Oracle 数据库还原操作的更多详细信息，请参阅 "Veeam Explorers 用户指南"。

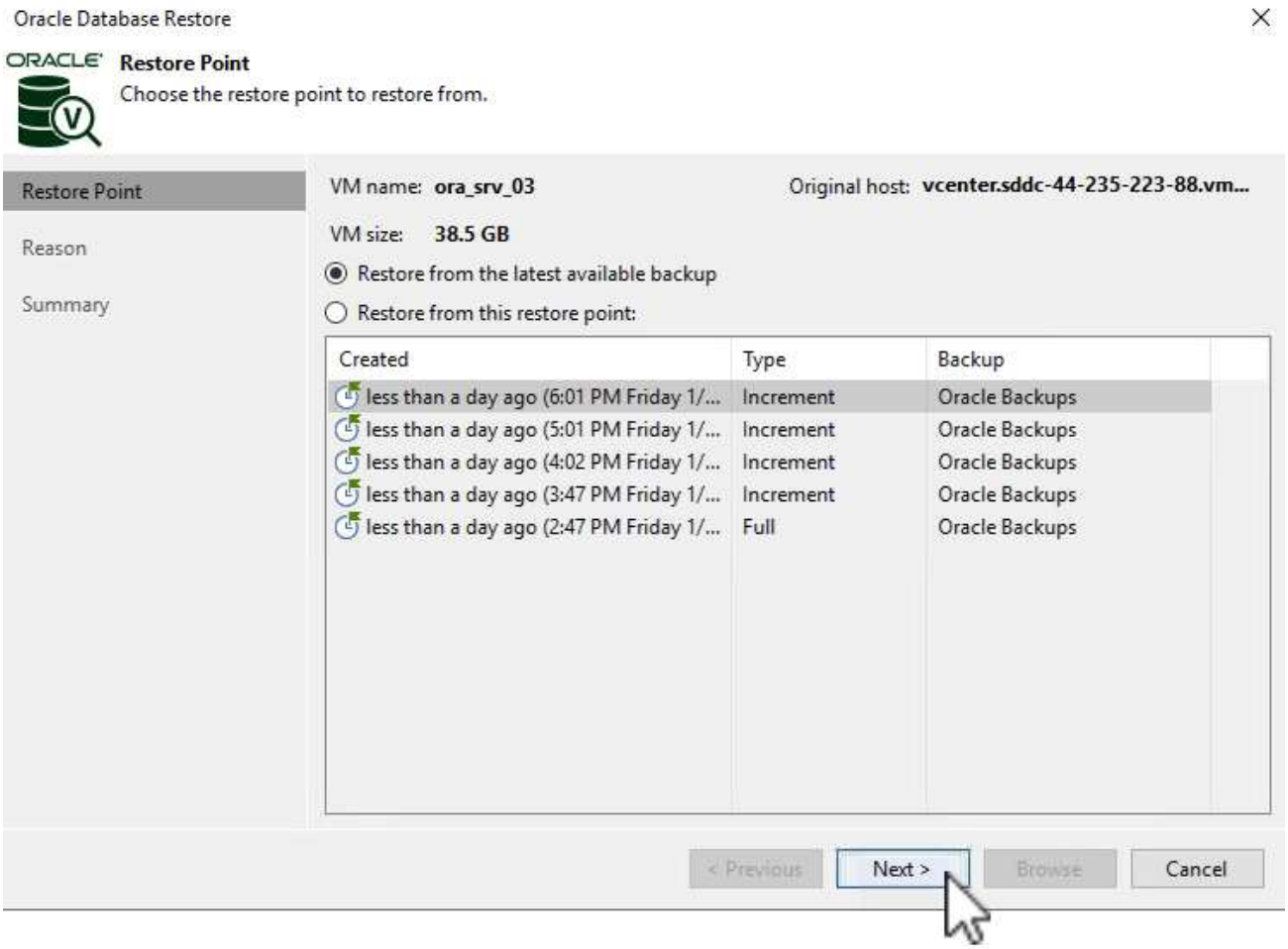
▼ 使用 **Veeam Explorer** 恢复 **Oracle** 数据库

本节介绍如何使用 Veeam Explorer 将 Oracle 数据库还原到不同的服务器。

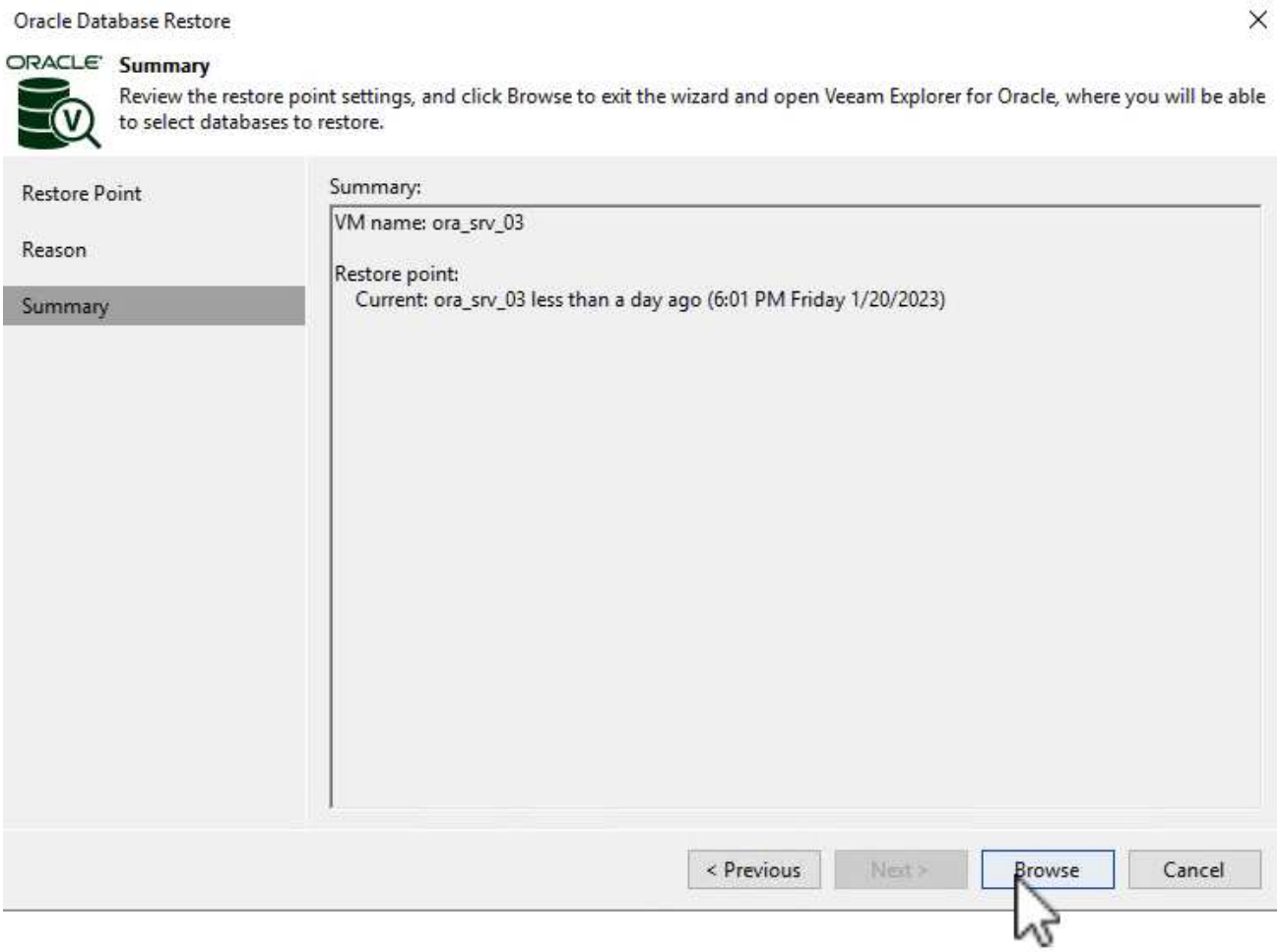
1. 在 Veeam Backup and Replication 控制台中，导航到 Oracle 备份列表，右键单击服务器并选择 恢复应用程序项，然后选择 **Oracle** 数据库...。



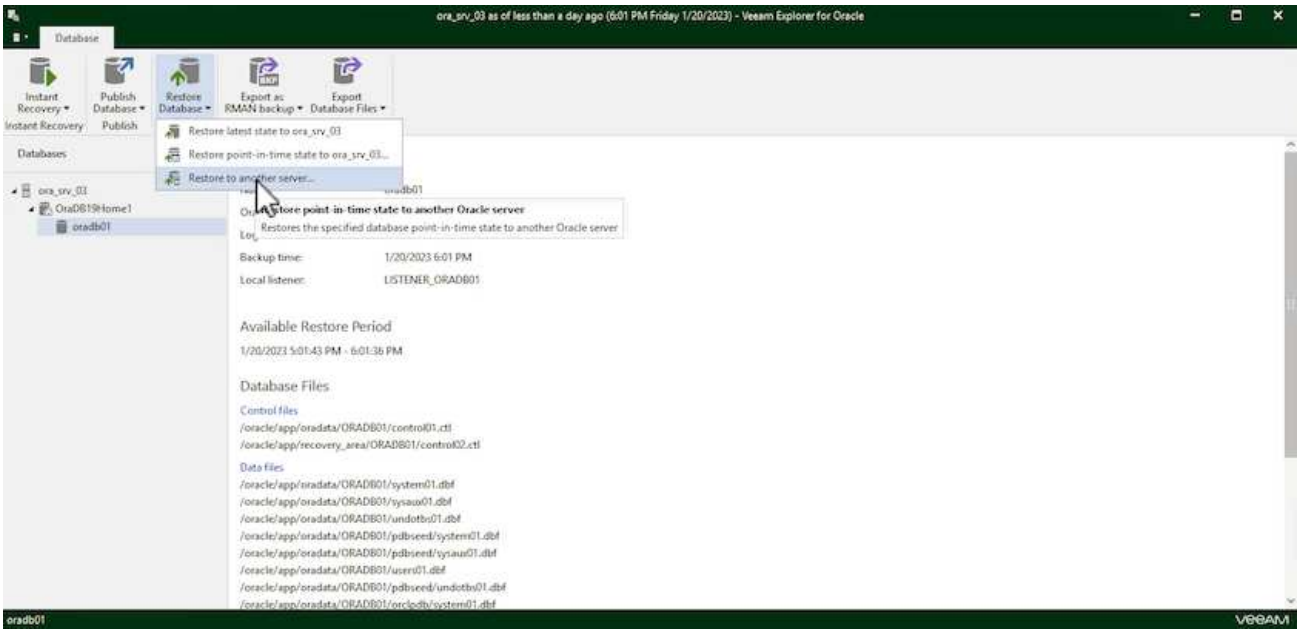
2. 在 Oracle 数据库还原向导中，从列表中选择一个还原点，然后单击“下一步”。



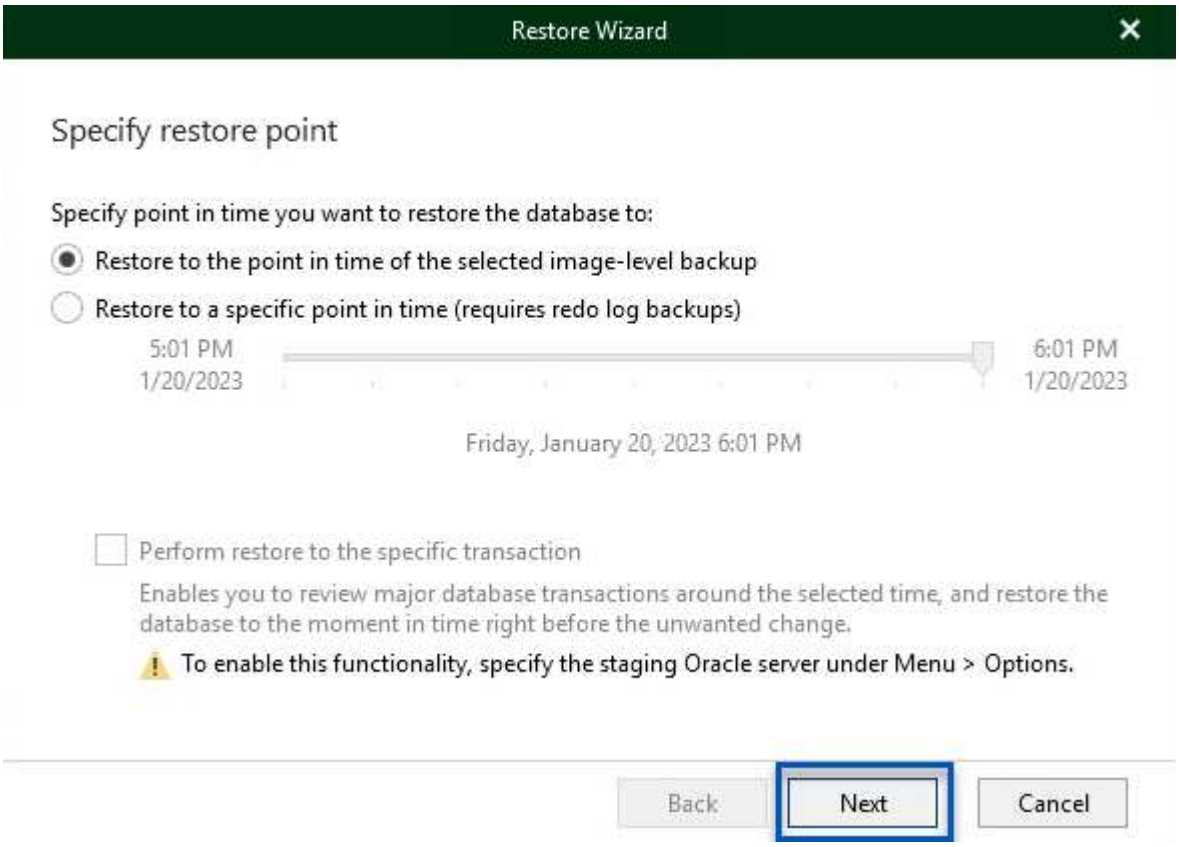
3. 如果需要，输入*恢复原因*，然后在摘要页面上，单击*浏览*按钮启动 Veeam Explorer for Oracle。



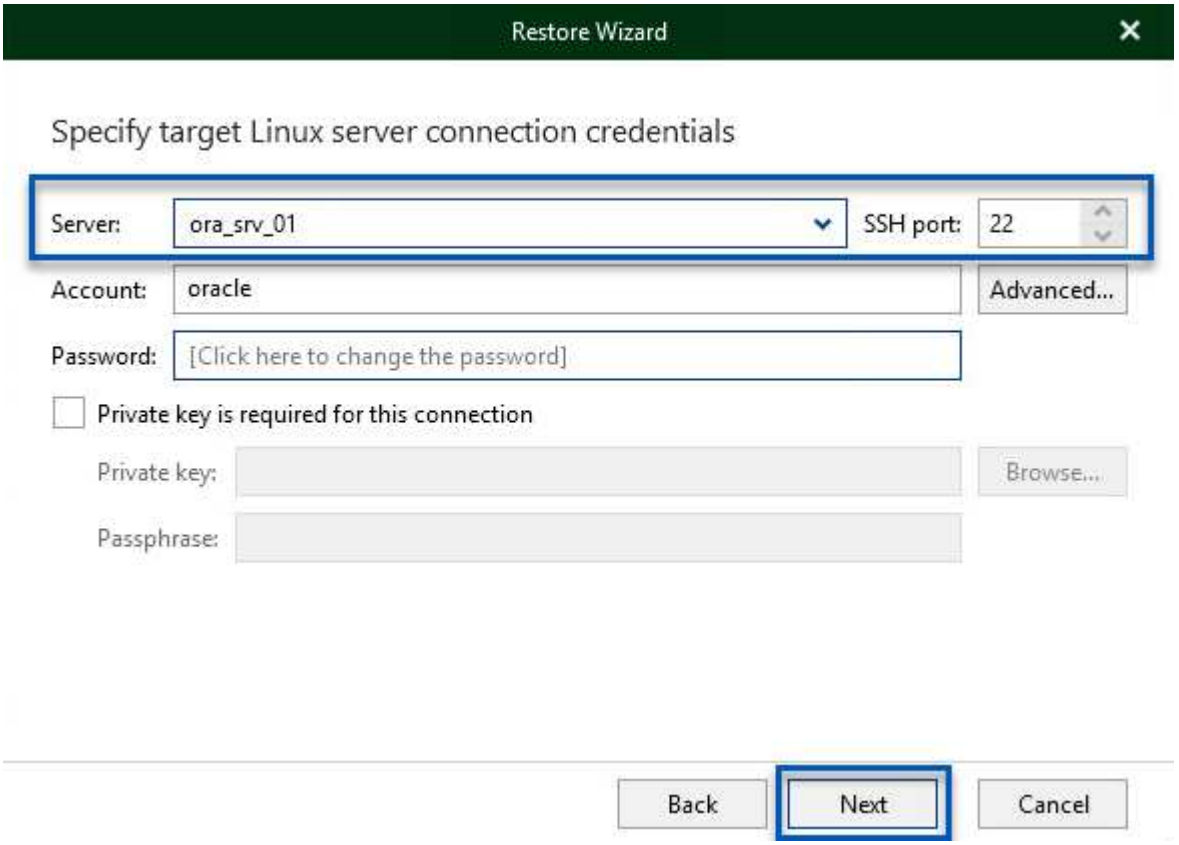
4. 在 Veeam Explorer 中展开数据库实例列表，单击要恢复的数据库，然后从顶部的 恢复数据库 下拉菜单中选择 恢复到另一台服务器...。



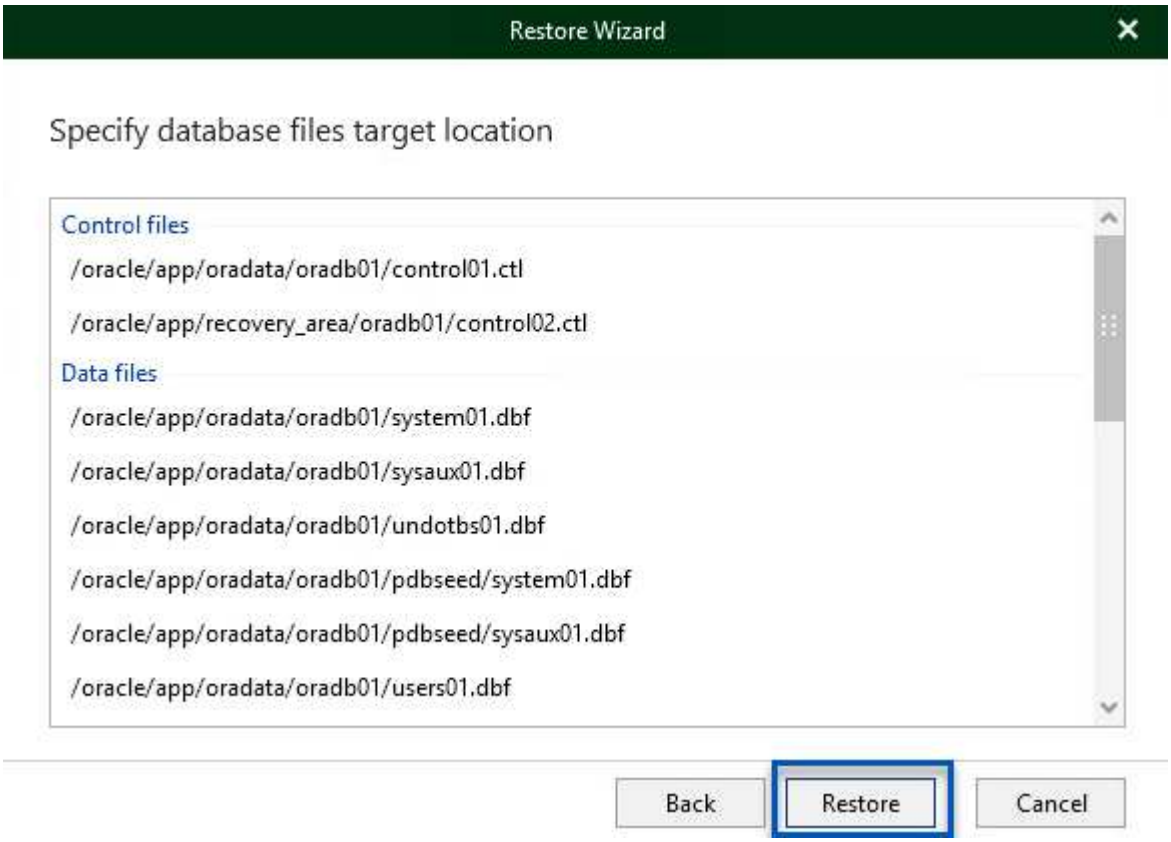
5. 在还原向导中指定要还原的还原点，然后单击“下一步”。



6. 指定数据库将恢复到的目标服务器和帐户凭据，然后单击“下一步”。



7. 最后，指定数据库文件目标位置并单击*恢复*按钮开始恢复过程。

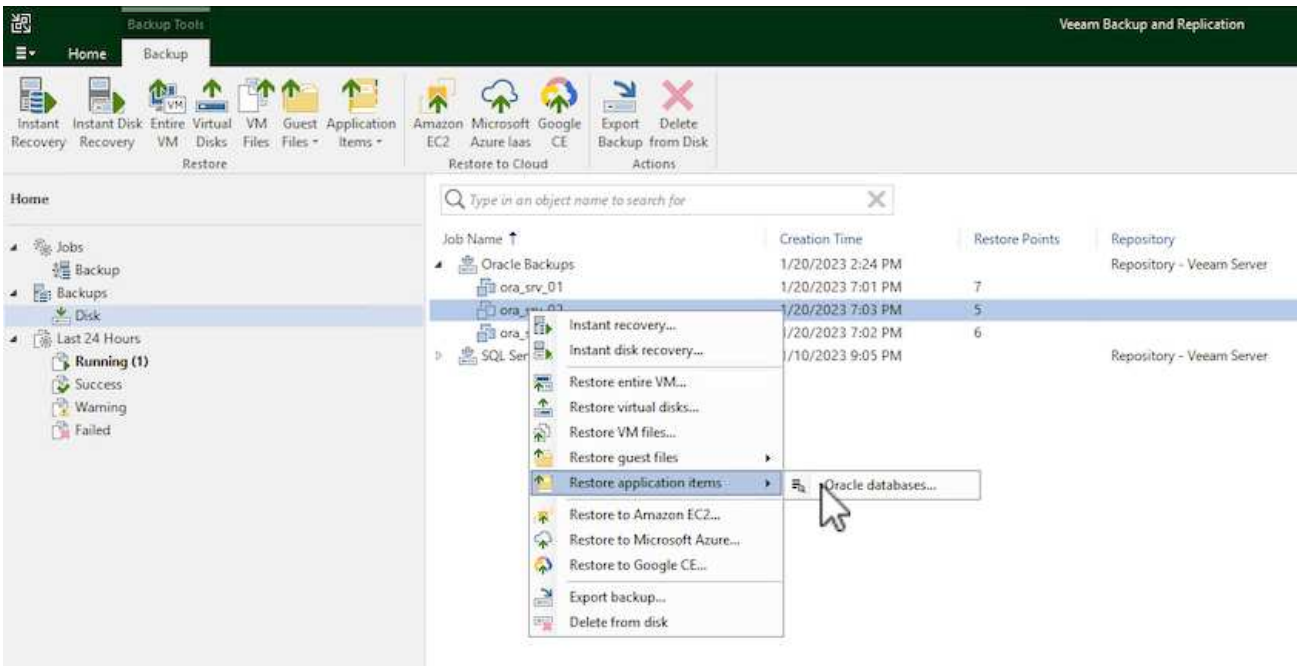


8. 数据库恢复完成后，检查 Oracle 数据库是否在服务器上正常启动。

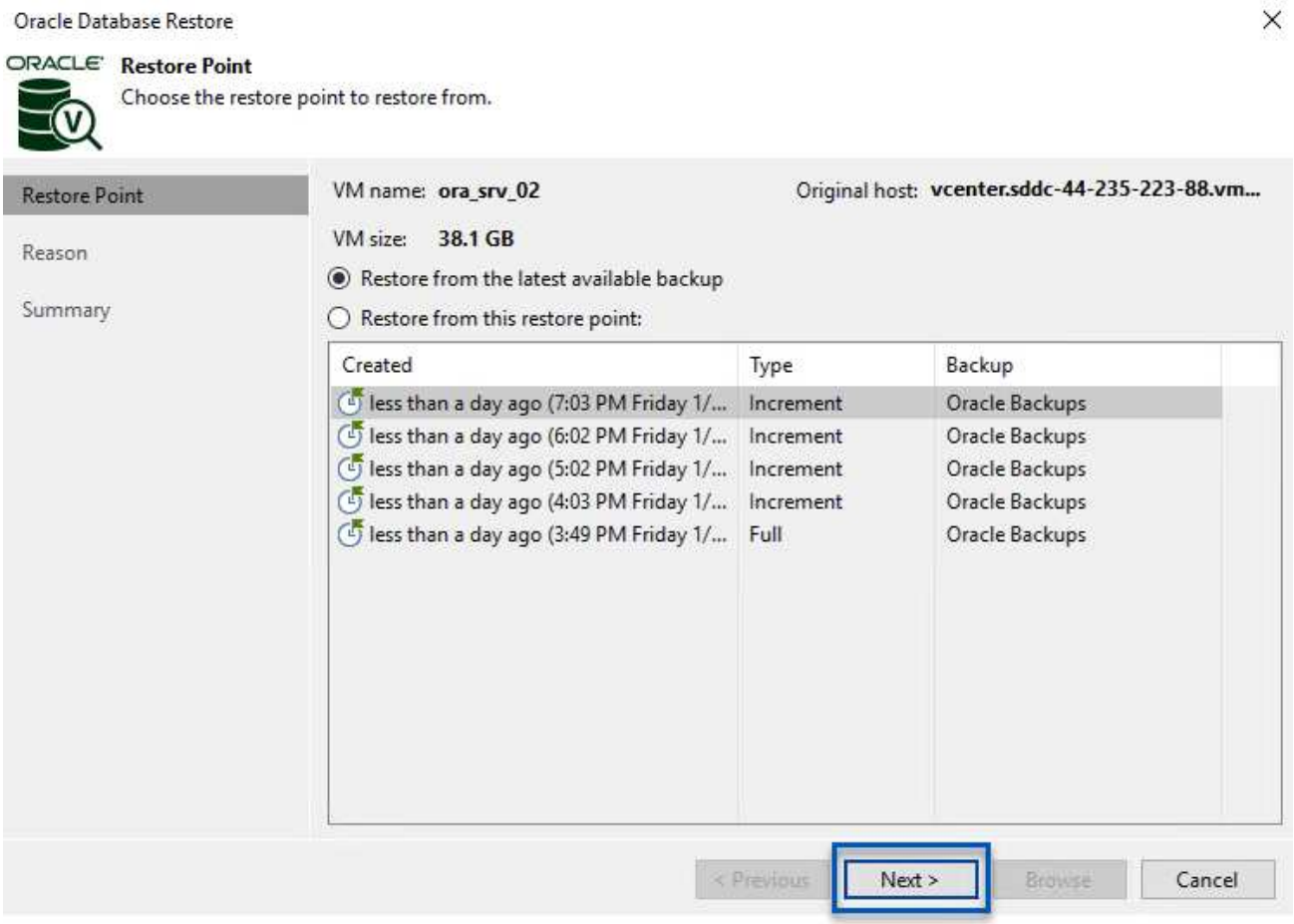
▼ 将 **Oracle** 数据库发布到备用服务器

在本节中，数据库被发布到备用服务器，以便快速访问，而无需启动完整恢复。

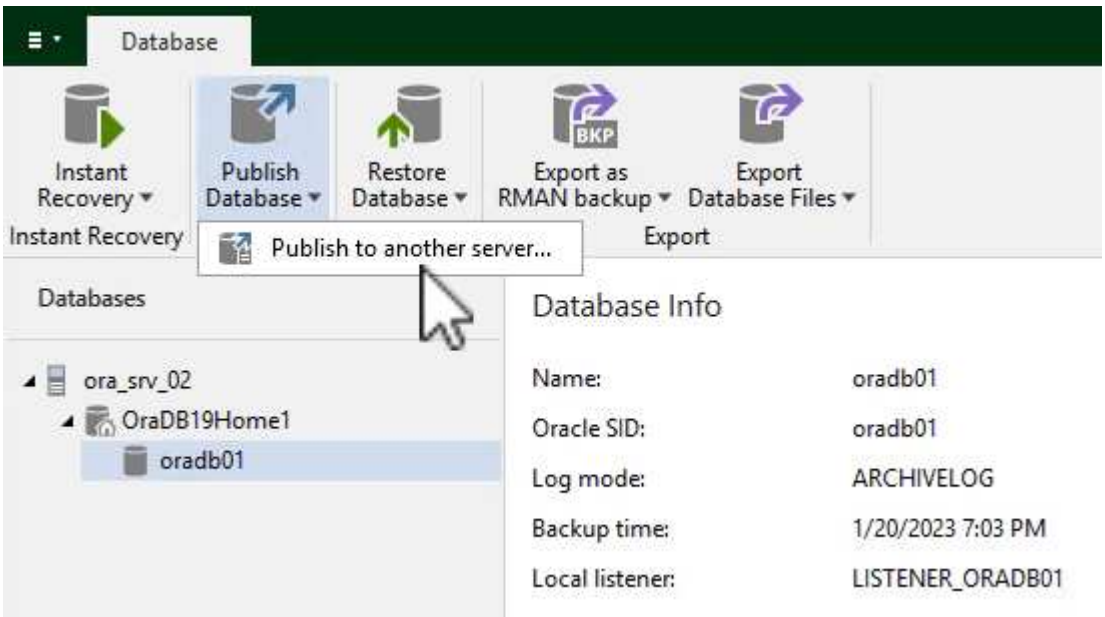
1. 在 Veeam Backup and Replication 控制台中，导航到 Oracle 备份列表，右键单击服务器并选择 恢复应用程序项，然后选择 **Oracle** 数据库…。



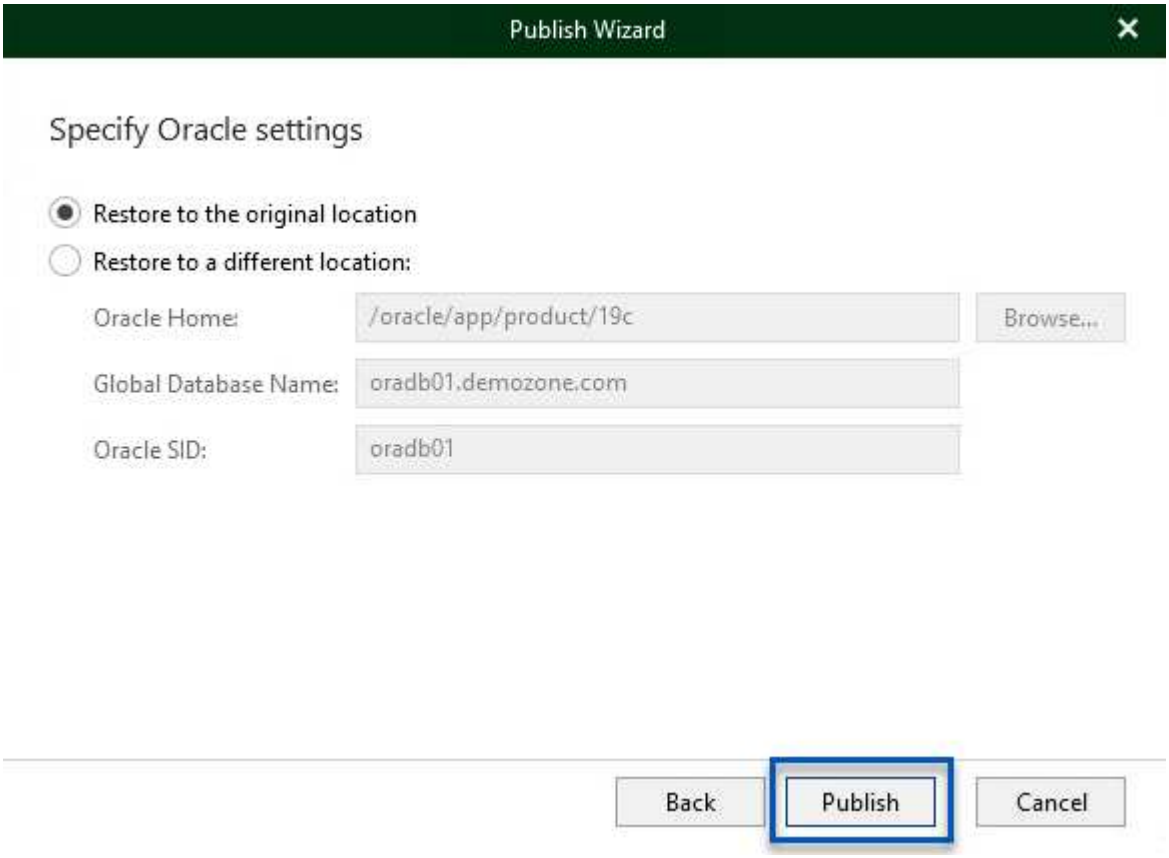
2. 在 Oracle 数据库还原向导中，从列表中选择一个还原点，然后单击“下一步”。



3. 如果需要，输入*恢复原因*，然后在摘要页面上，单击*浏览*按钮启动 Veeam Explorer for Oracle。
4. 在 Veeam Explorer 中展开数据库实例列表，单击要恢复的数据库，然后从顶部的 发布数据库 下拉菜单中选择 发布到另一台服务器...。



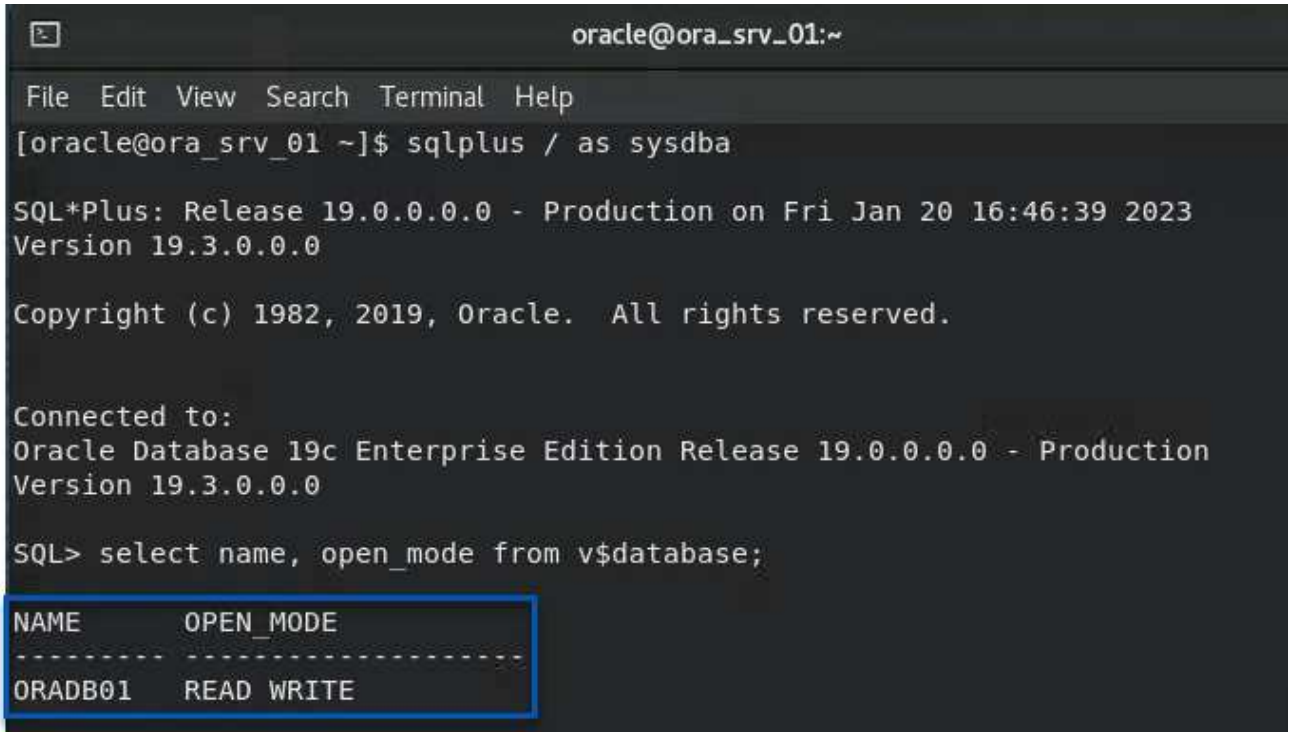
5. 在发布向导中，指定发布数据库的还原点，然后单击“下一步”。
6. 最后，指定目标 Linux 文件系统位置并单击 发布 开始恢复过程。



7. 发布完成后，登录目标服务器并运行以下命令以确保数据库正在运行：

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



结束语

VMware Cloud 是一个强大的平台，用于运行关键业务应用程序和存储敏感数据。对于依赖 VMware Cloud 来确保业务连续性并帮助防止网络威胁和数据丢失的企业来说，安全的数据保护解决方案至关重要。通过选择可靠且强大的数据保护解决方案，企业可以确信无论如何其关键数据都是安全的。

本文档中介绍的用例重点关注经过验证的数据保护技术，突出了NetApp、VMware 和 Veeam 之间的集成。 FSx ONTAP作为 AWS 中 VMware Cloud 的补充 NFS 数据存储区受支持，并用于所有虚拟机和应用程序数据。 Veeam Backup & Replication 是一款全面的数据保护解决方案，旨在帮助企业改进、自动化和简化其备份和恢复流程。 Veeam 与托管在 FSx ONTAP上的 iSCSI 备份目标卷结合使用，为驻留在 VMware Cloud 中的应用程序数据提供安全且易于管理的数据保护解决方案。

追加信息

要了解有关此解决方案中提出的技术的更多信息，请参阅以下附加信息。

- "FSx ONTAP用户指南"
- "Veeam 帮助中心技术文档"
- "VMware Cloud on AWS 支持。注意事项和限制"

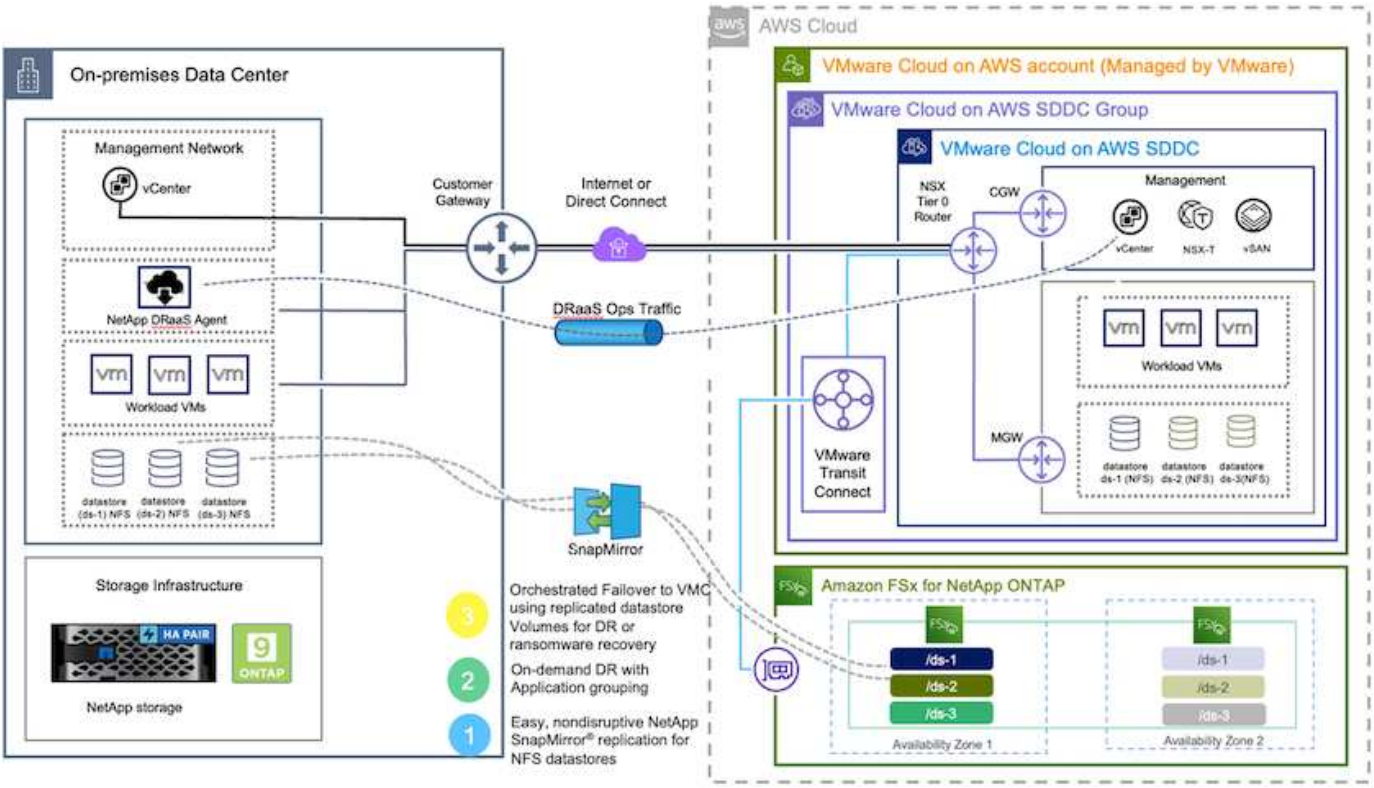
TR-4955：使用 **FSx ONTAP**和 **VMC** 进行灾难恢复 **(AWS VMware Cloud)**

灾难恢复编排器（DRO；带有 UI 的脚本解决方案）可用于无缝恢复从本地复制到 FSx ONTAP 的工作负载。 DRO 可自动执行从SnapMirror级别到 VM 注册到 VMC 再到直接在 NSX-T 上进行网络映射的恢复。所有 VMC 环境均包含此功能。

NetApp的 Niyaz Mohamed

灾难恢复到云端是一种具有弹性且经济高效的方法，可以保护工作负载免受站点中断和数据损坏事件（例如勒索软件）的影响。借助NetApp SnapMirror技术，本地 VMware 工作负载可以复制到在 AWS 中运行的 FSx ONTAP 。

灾难恢复编排器（DRO；带有 UI 的脚本解决方案）可用于无缝恢复从本地复制到 FSx ONTAP 的工作负载。DRO 可自动执行从SnapMirror级别到 VM 注册到 VMC 再到直接在 NSX-T 上进行网络映射的恢复。所有 VMC 环境均包含此功能。



入门

在 **AWS** 上部署和配置 **VMware Cloud**

"AWS 上的 VMware Cloud"为 AWS 生态系统中基于 VMware 的工作负载提供云原生体验。每个 VMware 软件定义数据中心 (SDDC) 都在 Amazon 虚拟私有云 (VPC) 中运行，并提供完整的 VMware 堆栈（包括 vCenter Server）、NSX-T 软件定义网络、vSAN 软件定义存储以及一个或多个为工作负载提供计算和存储资源的 ESXi 主机。要在 AWS 上配置 VMC 环境，请按照以下步骤操作"链接"。指示灯组也可用于 DR 目的。

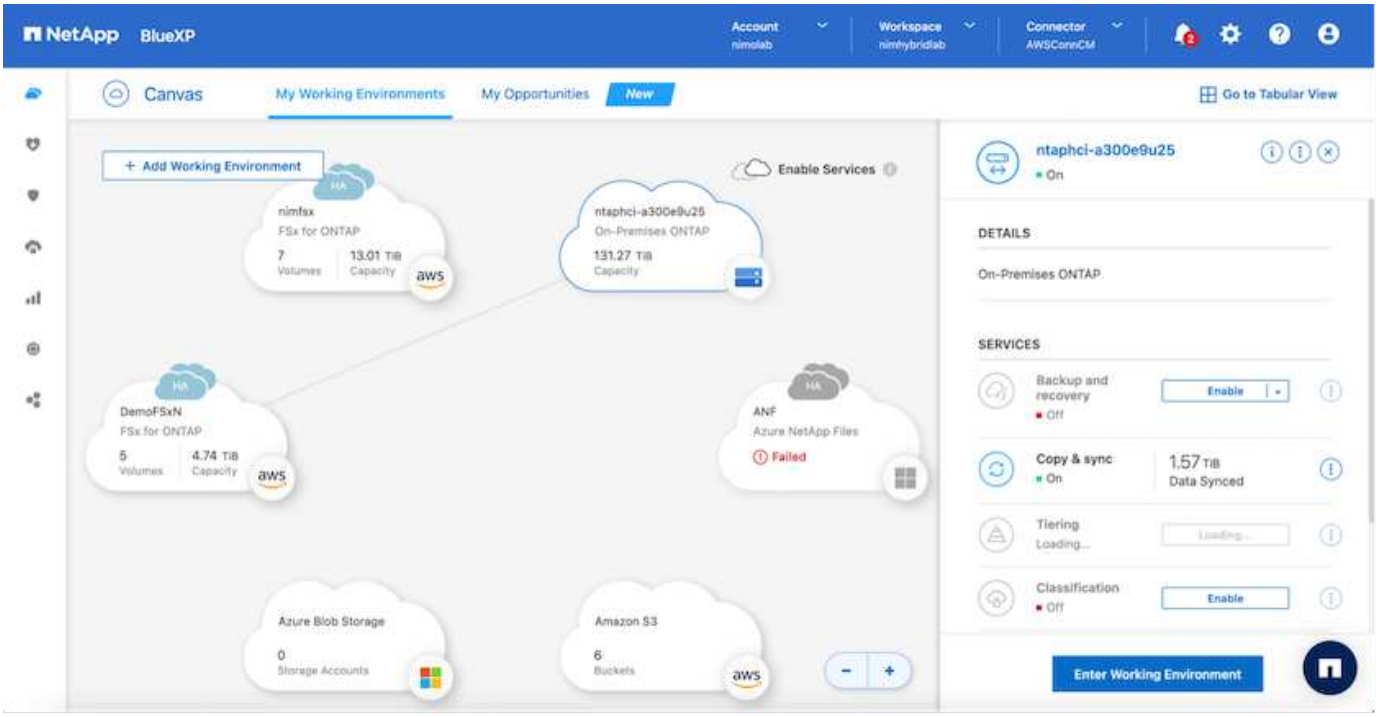
在初始版本中，DRO 支持现有的指示灯集群。按需 SDDC 创建功能将在即将发布的版本中提供。

配置 **FSx ONTAP**

Amazon FSx ONTAP是一项完全托管的服务，它基于流行的NetApp ONTAP文件系统构建，提供高度可靠、可扩展、高性能且功能丰富的文件存储。按照此处的步骤操作"链接"配置和配置 FSx ONTAP。

部署并配置SnapMirror到 FSx ONTAP

下一步是使用 NetApp Console 发现 AWS 实例上配置的 FSx ONTAP，并以适当的频率和 NetApp Snapshot 副本保留，将所需的数据存储卷从本地环境复制到 FSx ONTAP：



请按照此链接中的步骤配置 DRO。您还可以使用 NetApp ONTAP 命令行界面按照此链接安排复制。

SnapMirror关系是先决条件，必须事先创建。

DRO安装

要开始使用 DRO，请在指定的 EC2 实例或虚拟机上使用 Ubuntu 操作系统，以确保您满足先决条件。然后安装该包。

前提条件

- 确保与源和目标 vCenter 和存储系统的连接存在。
- 如果您使用 DNS 名称，则应该进行 DNS 解析。否则，您应该使用 vCenter 和存储系统的 IP 地址。
- 创建具有root权限的用户。您还可以将 sudo 与 EC2 实例一起使用。

OS 要求

- Ubuntu 20.04 (LTS)，最低配置 2GB 内存和 4 个 vCPU
- 必须在指定的代理虚拟机上安装以下软件包：
  - Docker
  - Docker-compose
  - 杰

更改权限 `docker.sock`： `sudo chmod 666 /var/run/docker.sock` 。

这 `deploy.sh`脚本执行所有必需的先决条件。

安装包

1. 在指定虚拟机上下载安装包：

```
git clone https://github.com/NetApp/DRO-AWS.git
```

该代理可以安装在本地或 AWS VPC 内。

2. 解压包，运行部署脚本，输入主机IP（例如10.10.10.10）。

```
tar xvf DRO-prereq.tar
```

3. 导航到目录并运行部署脚本，如下所示：

```
sudo sh deploy.sh
```

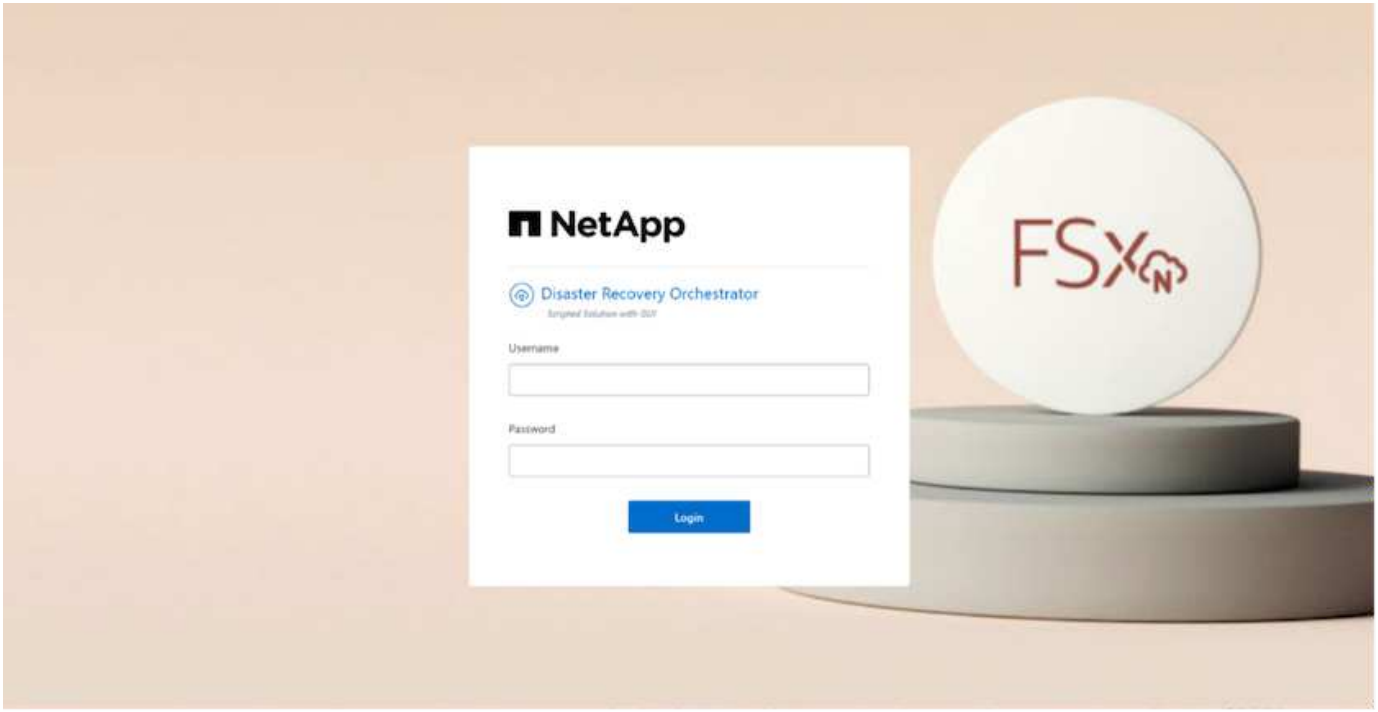
4. 使用以下方式访问 UI：

```
https://<host-ip-address>
```

使用以下默认凭据：

```
Username: admin
Password: admin
```

可以使用“更改密码”选项来更改密码。



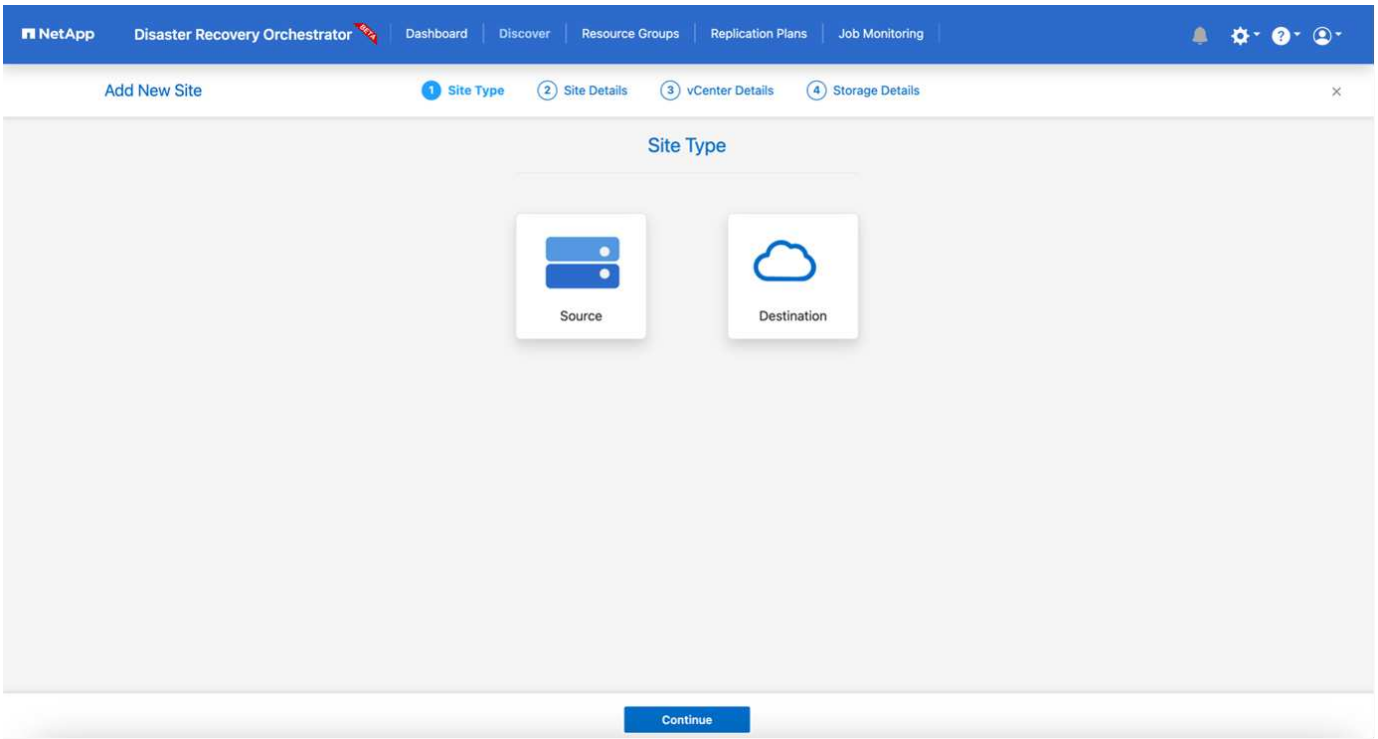
DRO 配置

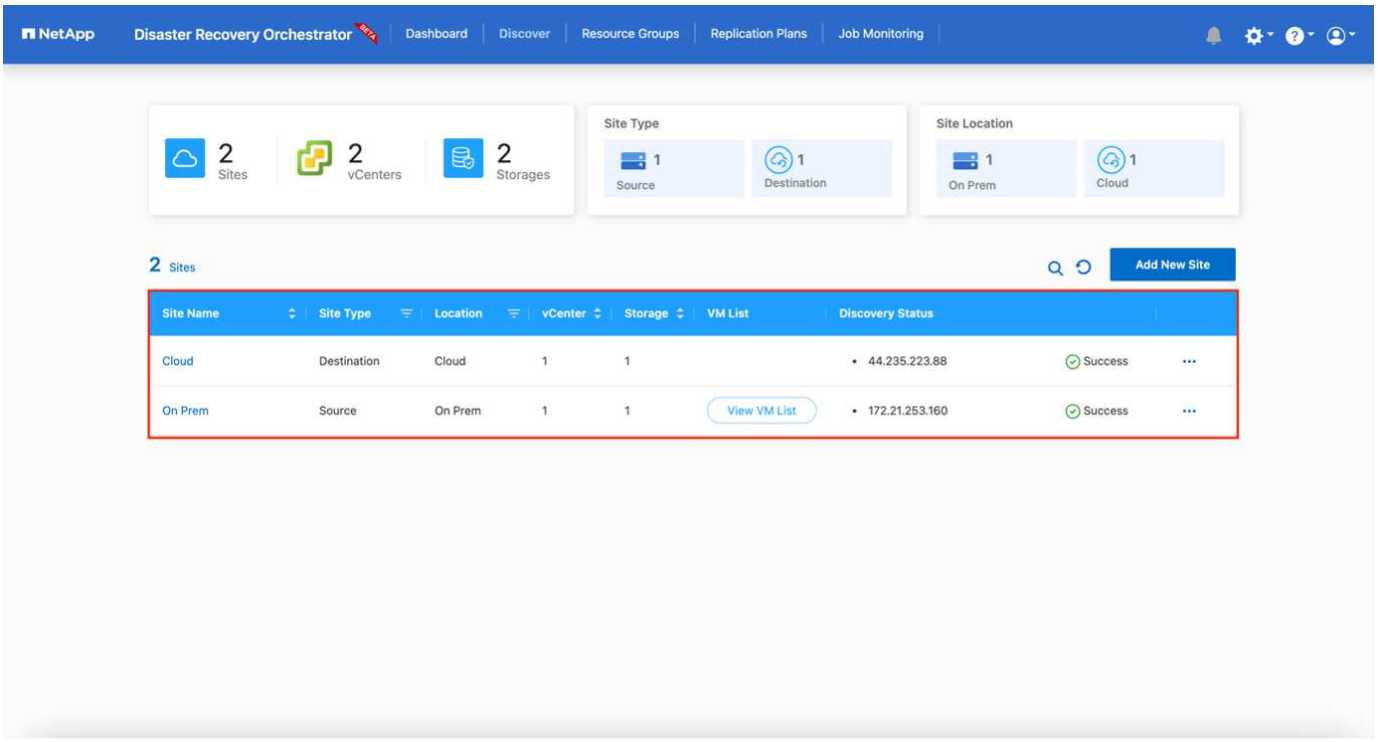
正确配置 FSx ONTAP和 VMC 后，您可以开始配置 DRO，以使用 FSx ONTAP上的只读SnapMirror副本自动将本地工作负载恢复到 VMC。

NetApp建议在 AWS 中部署 DRO 代理，并将其部署到部署 FSx ONTAP 的同一 VPC（也可以对等连接），以便 DRO 代理可以通过网络与您的内部组件以及 FSx ONTAP和 VMC 资源进行通信。

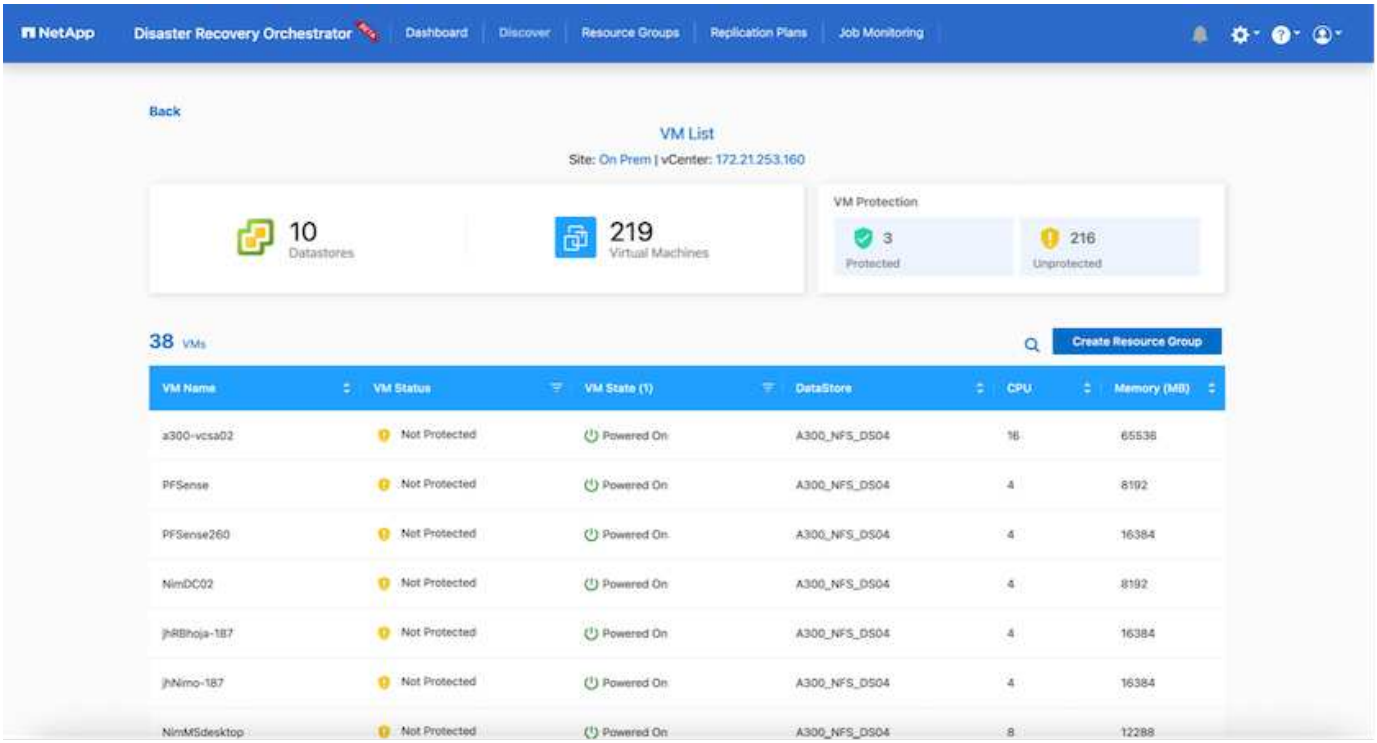
第一步是发现并将本地和云资源（vCenter 和存储）添加到 DRO。在支持的浏览器中打开 DRO 并使用默认用户名和密码（admin/admin）并添加站点。还可以使用“发现”选项添加站点。添加以下平台：

- 本地
  - 本地 vCenter
  - ONTAP存储系统
- 云
  - VMC vCenter
  - FSx ONTAP





添加后，DRO 会执行自动发现并显示从源存储到 FSx ONTAP具有相应SnapMirror副本的虚拟机。 DRO 自动检测虚拟机使用的网络和端口组并填充它们。



下一步是将所需的虚拟机分组到功能组中，作为资源组。

资源分组

添加平台后，您可以将要恢复的虚拟机分组到资源组中。 DRO 资源组允许您将一组从属虚拟机分组为逻辑组，这些逻辑组包含它们的启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

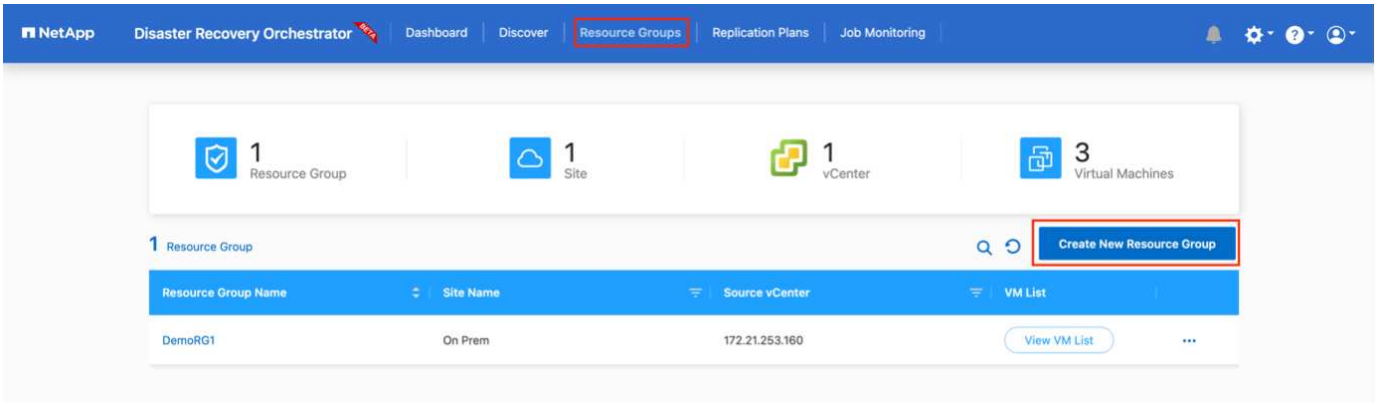
要开始创建资源组，请完成以下步骤：

1. 访问*资源组*，然后单击*创建新资源组*。
2. 在“新资源组”下，从下拉菜单中选择源站点，然后单击“创建”。
3. 提供*资源组详细信息*并单击*继续*。
4. 使用搜索选项选择适当的虚拟机。
5. 为所选虚拟机选择启动顺序和启动延迟（秒）。通过选择每个虚拟机并设置其优先级来设置开机顺序。所有虚拟机的默认值都是三。

   选项如下：

   1 – 第一个启动的虚拟机 3 – 默认 5 – 最后一个启动的虚拟机

6. 单击“创建资源组”。

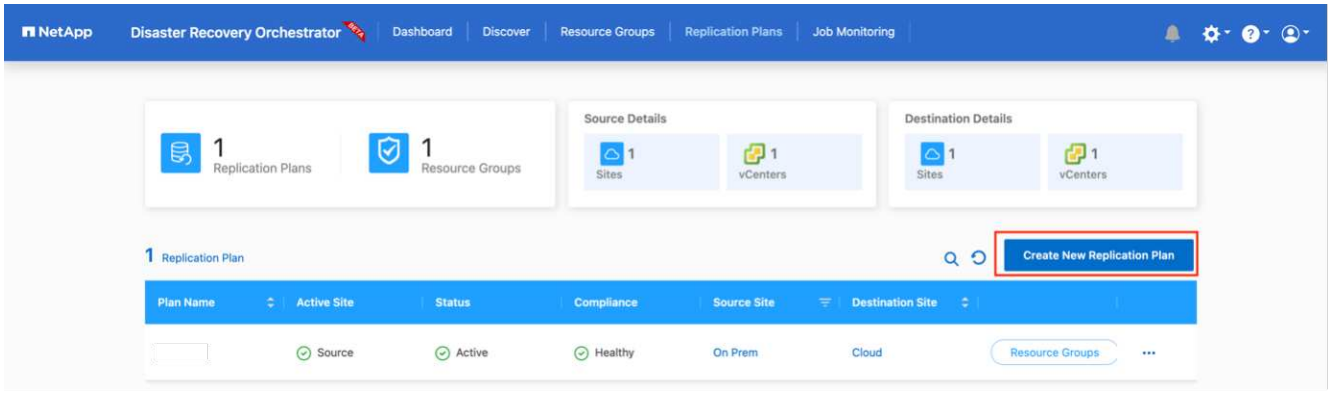


复制计划

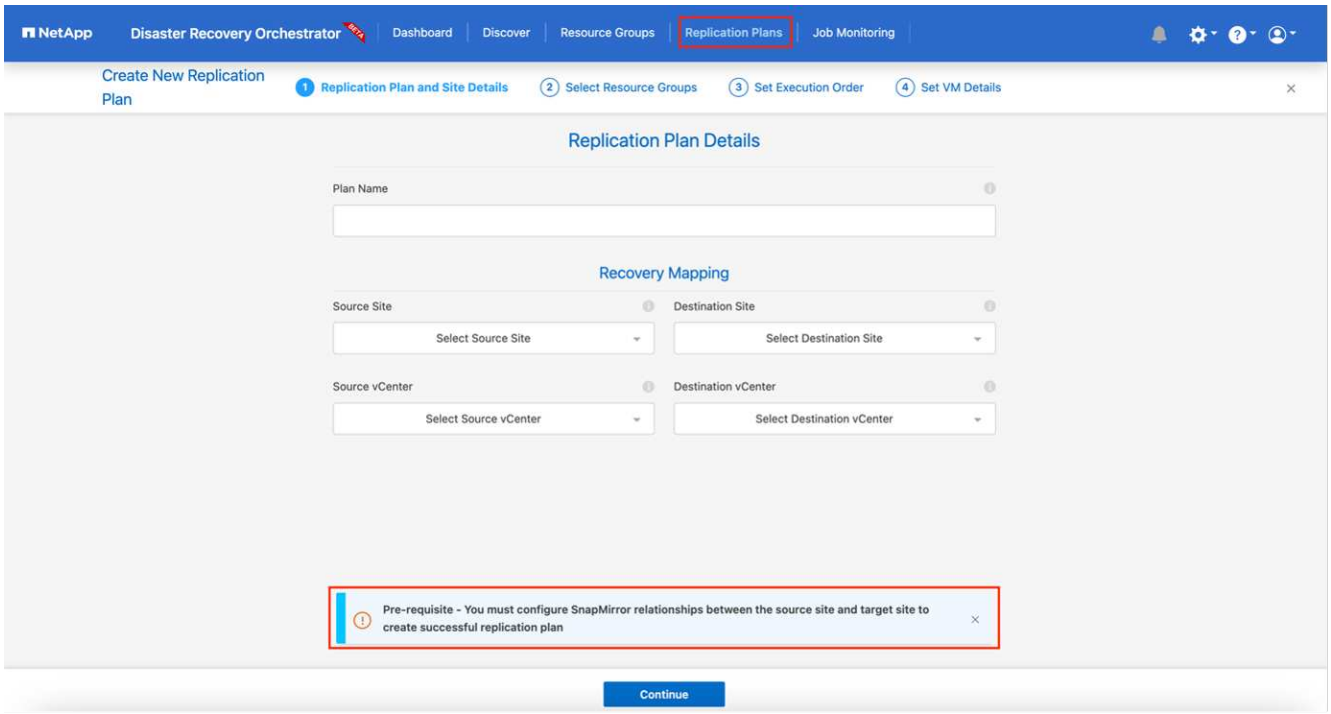
您需要一个在发生灾难时恢复应用程序的计划。从下拉菜单中选择源和目标 vCenter 平台，并选择要包含在该计划中的资源组，以及应用程序应如何恢复和启动的分组（例如，域控制器，然后是第 1 层，然后是第 2 层，等等）。此类计划有时也称为蓝图。要定义恢复计划，请导航到“复制计划”选项卡并单击“新建复制计划”。

要开始创建复制计划，请完成以下步骤：

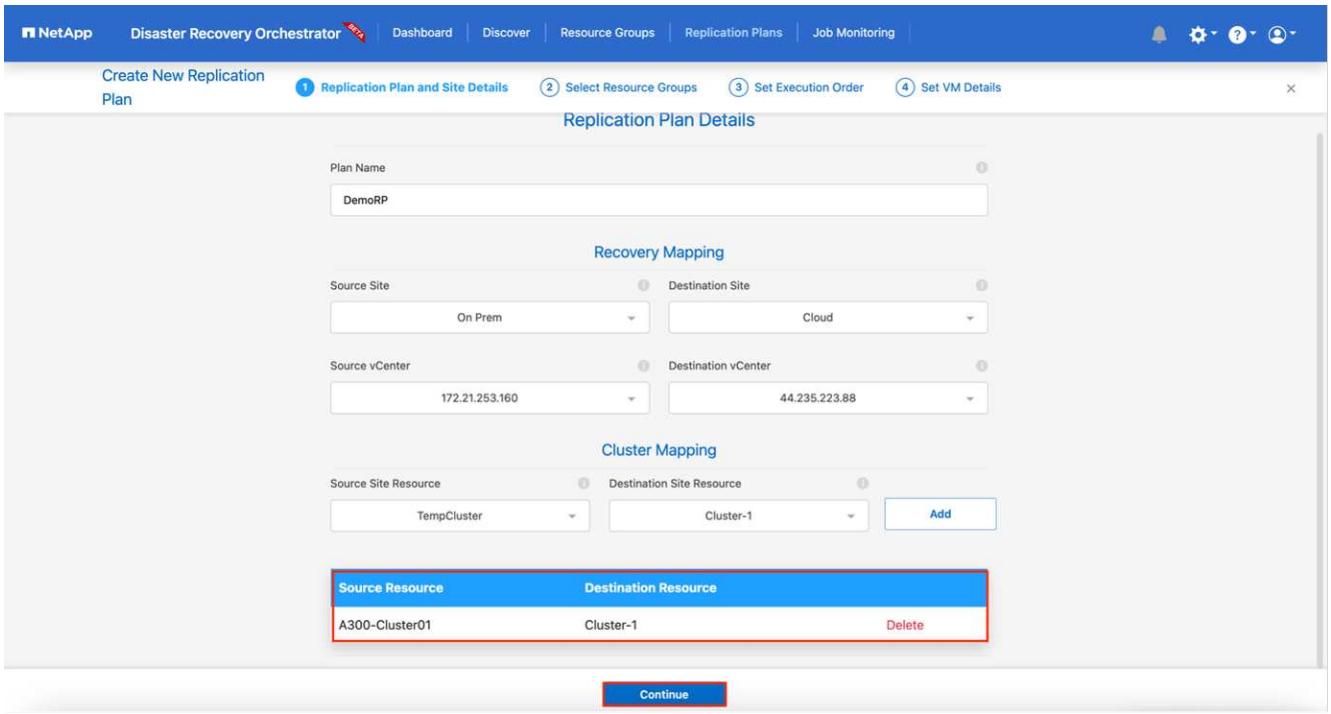
1. 访问*复制计划*，然后单击*创建新的复制计划*。



2. 在“新复制计划”下，提供计划名称并通过选择源站点、关联 vCenter、目标站点和关联 vCenter 添加恢复映射。



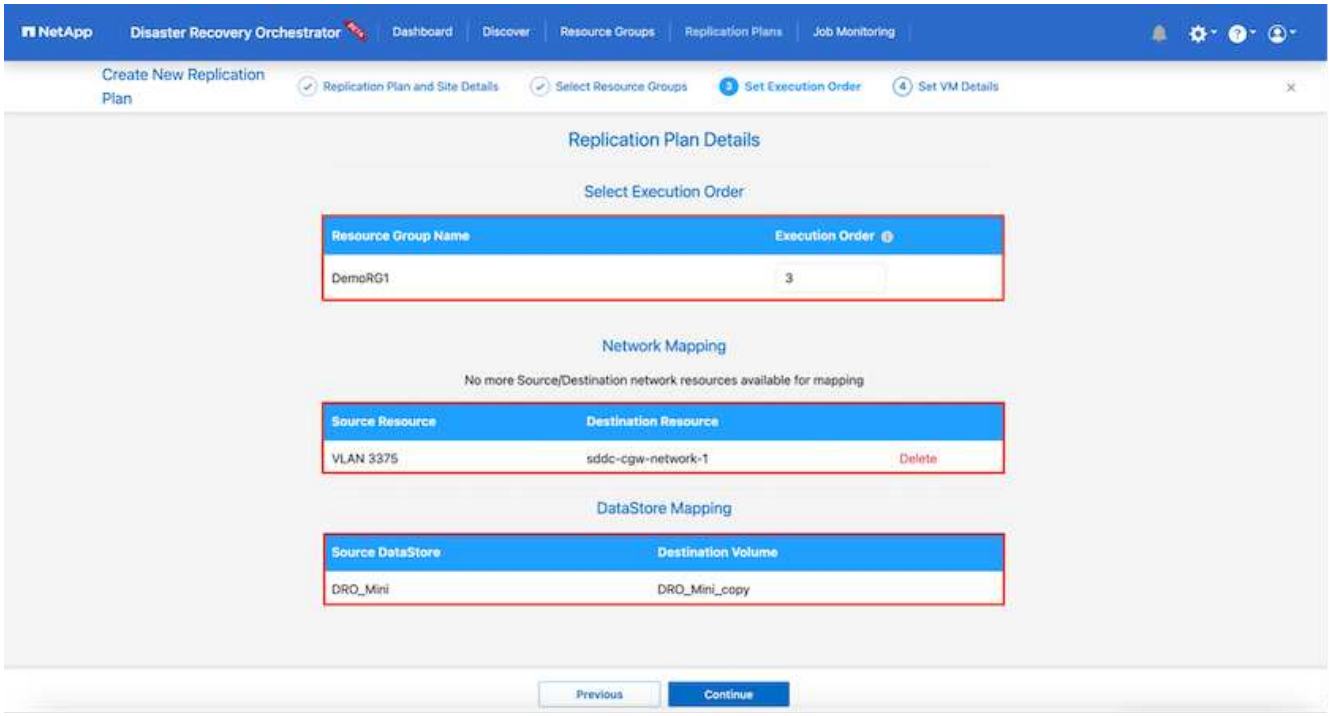
3. Recovery映射完成后，选择集群映射。



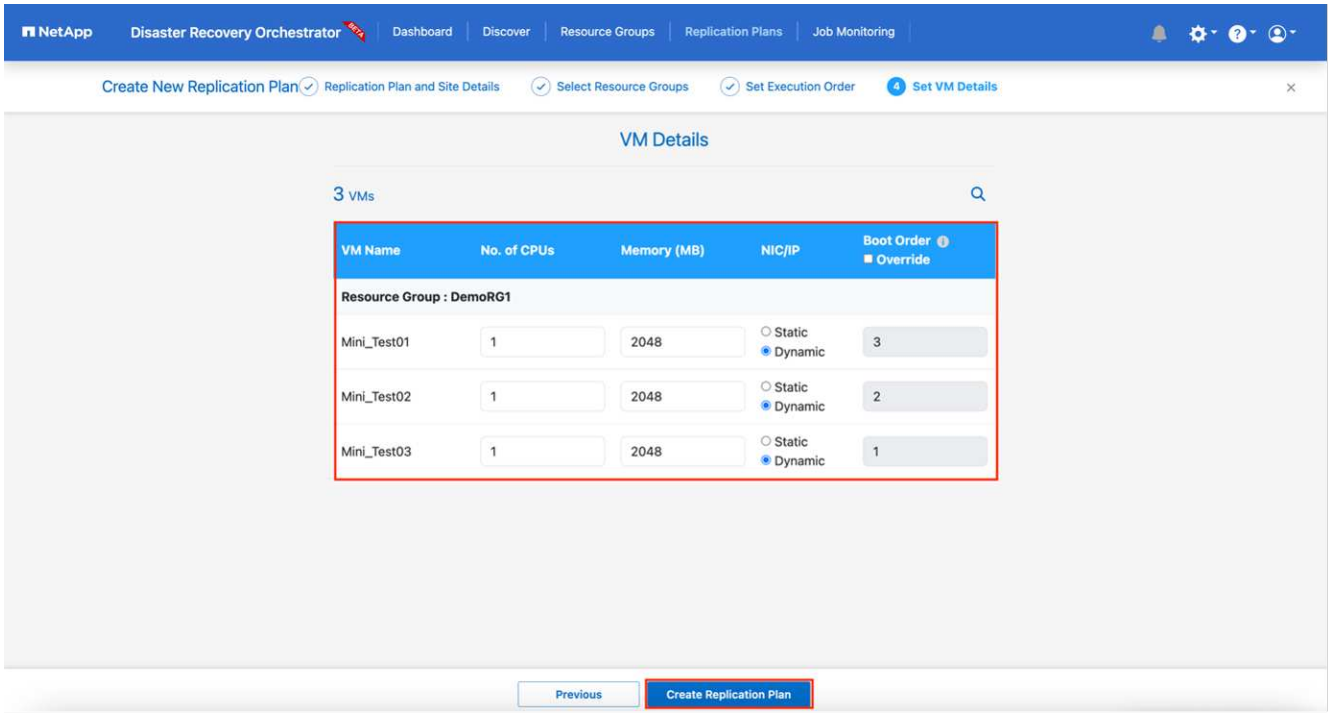
4. 选择*资源组详情*并点击*继续*。
5. 设置资源组的执行顺序。当存在多个资源组时，此选项可让您选择操作顺序。
6. 完成后，选择网络映射到适当的网段。这些段应该已经在 VMC 中配置，因此请选择适当的段来映射 VM。
7. 根据虚拟机的选择，自动选择数据存储映射。

SnapMirror处于卷级别。因此，所有虚拟机都被复制到复制目标。确保选择数据存储区中的

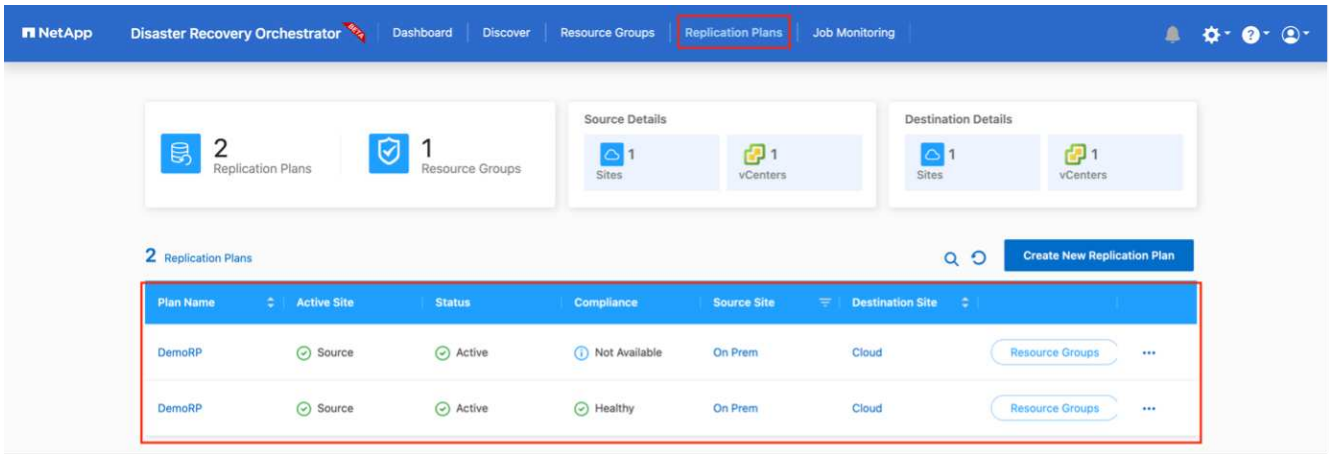
所有虚拟机。如果未选择，则仅处理复制计划中的虚拟机。



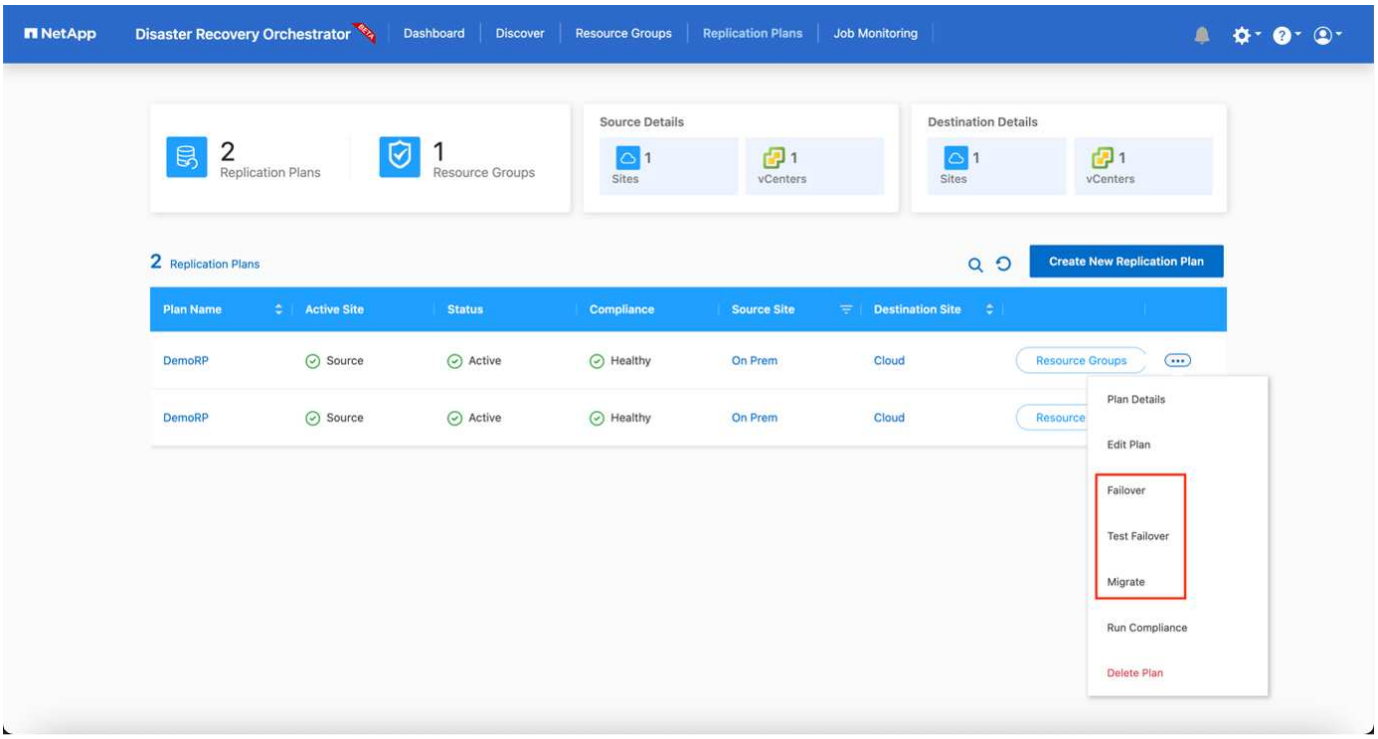
8. 在 VM 详细信息下，您可以选择调整 VM 的 CPU 和 RAM 参数的大小；当将大型环境恢复到较小的目标集群或进行 DR 测试时，这非常有用，而无需配置一对一的物理 VMware 基础架构。此外，您还可以修改资源组中所有选定虚拟机的启动顺序和启动延迟（秒）。如果需要对资源组启动顺序选择期间选择的顺序进行任何更改，则可以选择修改启动顺序。默认情况下，使用在资源组选择期间选择的启动顺序；但是，可以在此阶段执行任何修改。

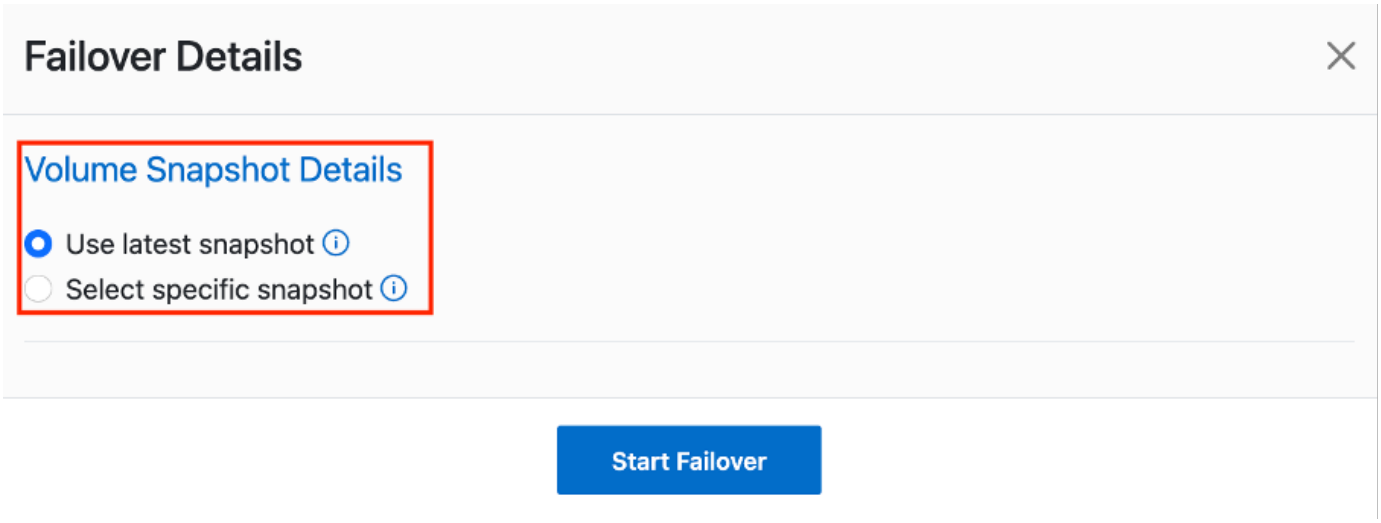


9. 单击“创建复制计划”。

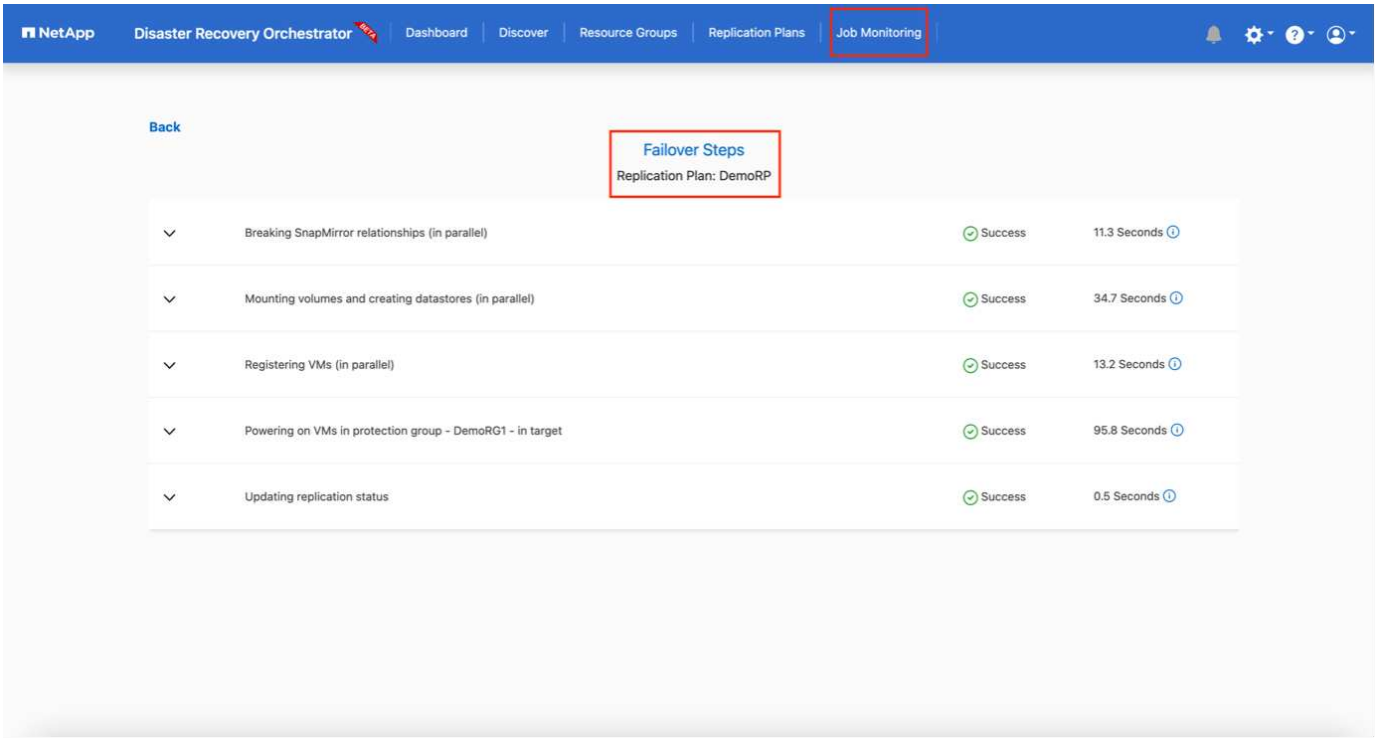


创建复制计划后，可以根据需求执行故障转移选项、测试故障转移选项或迁移选项。在故障转移和测试故障转移选项期间，使用最新的SnapMirror Snapshot 副本，或者可以从时间点 Snapshot 副本中选择特定的 Snapshot 副本（根据SnapMirror的保留策略）。如果您面临勒索软件之类的损坏事件，则时间点选项可能非常有用，其中最新的副本已被破坏或加密。 DRO 显示所有可用的时间点。要使用复制计划中指定的配置触发故障转移或测试故障转移，您可以单击“故障转移”或“测试故障转移”。

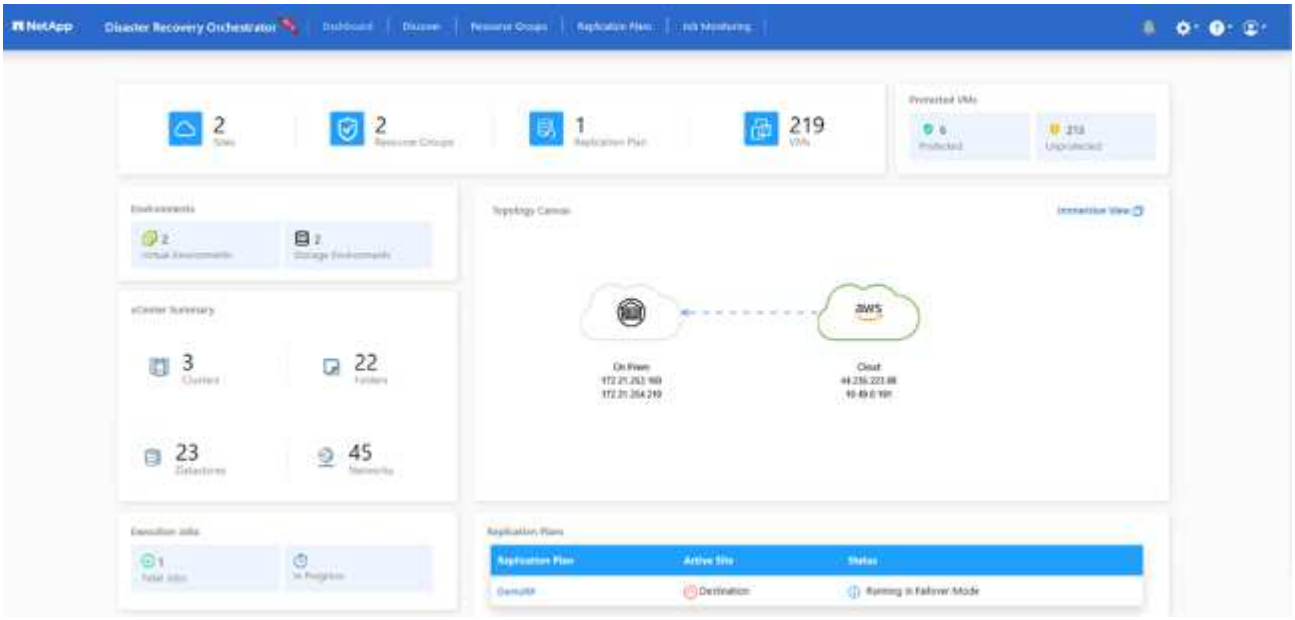




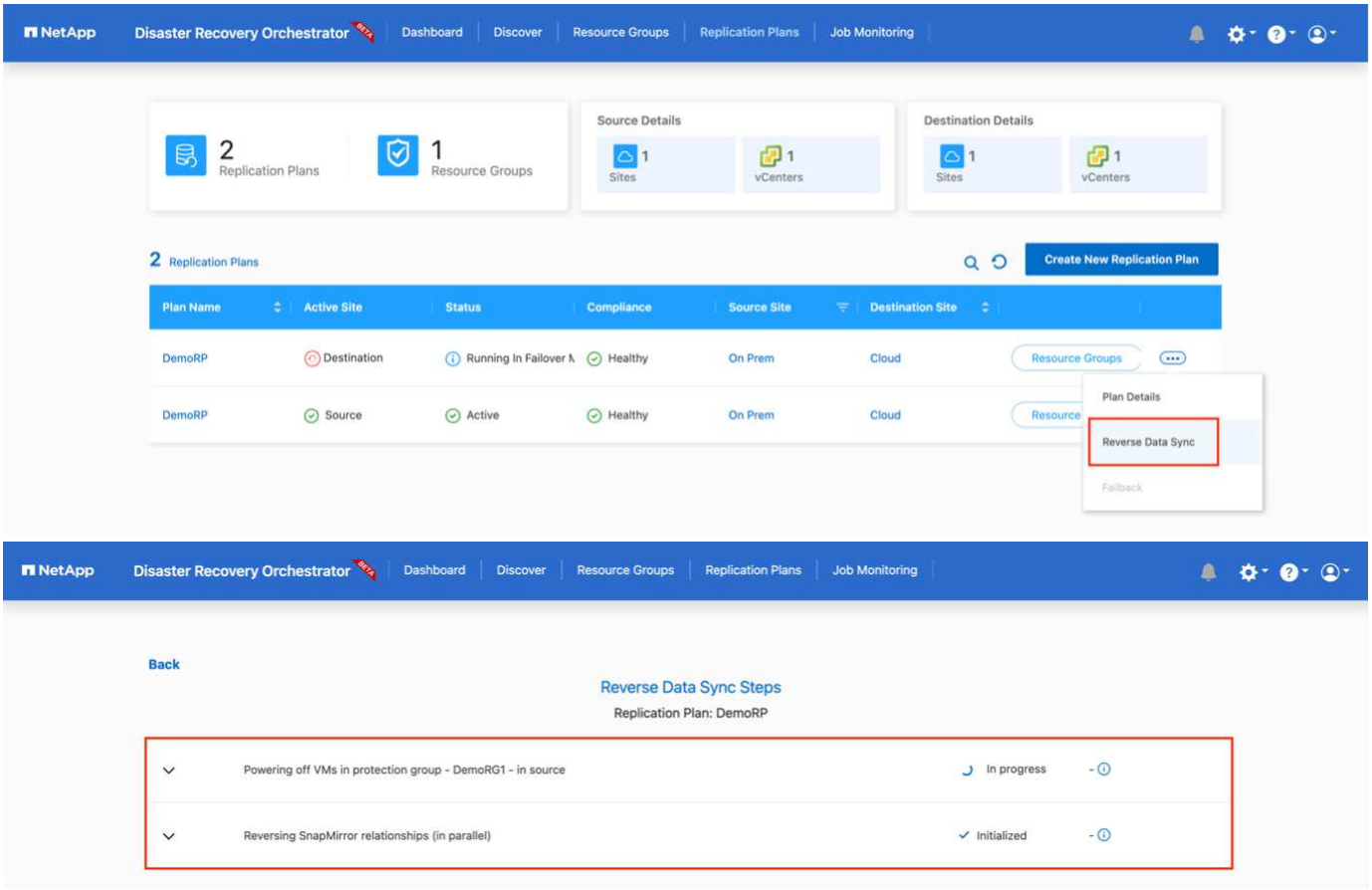
可以在任务菜单中监控复制计划：



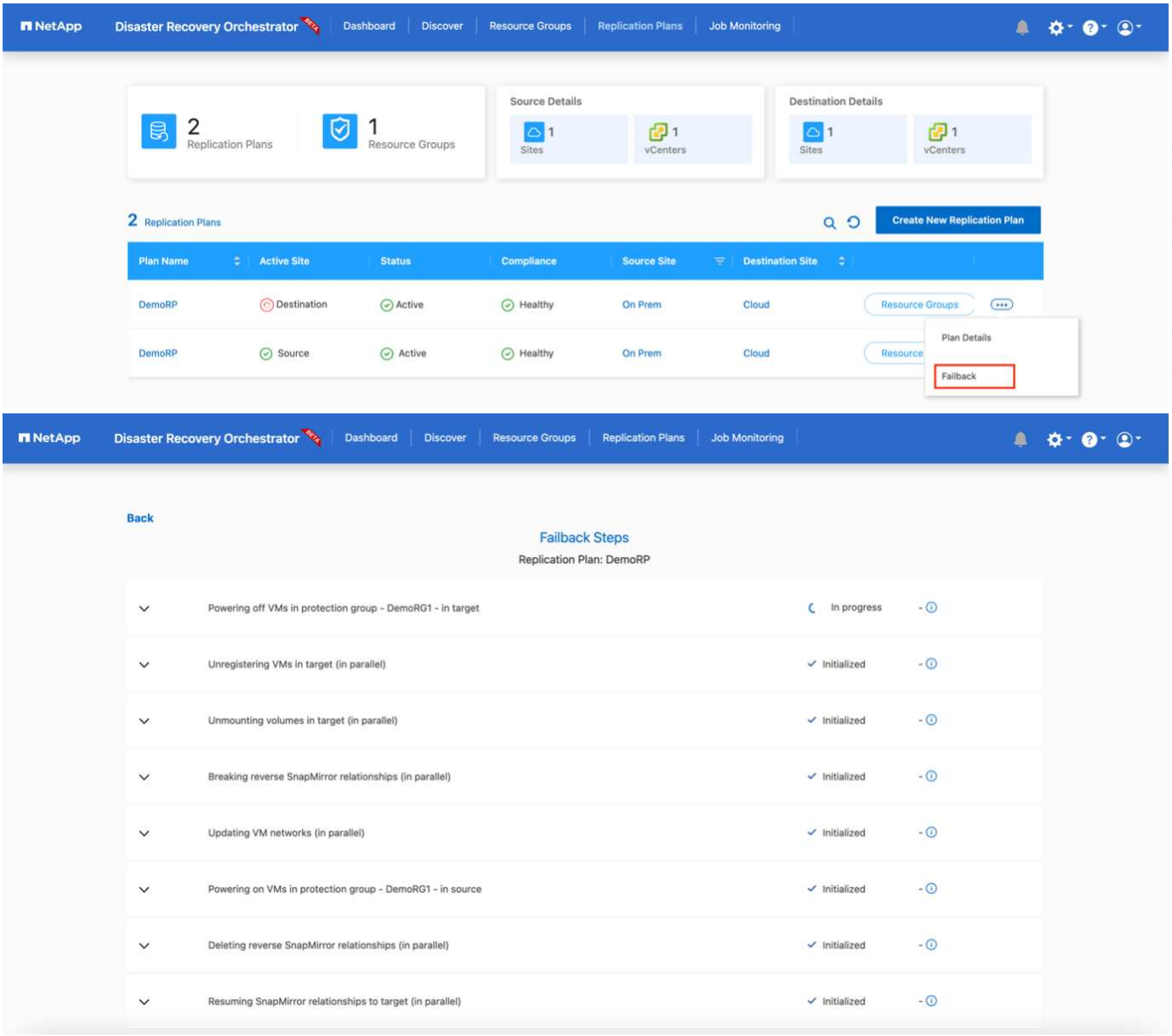
触发故障转移后，可以在 VMC vCenter（虚拟机、网络、数据存储）中看到恢复的项目。默认情况下，虚拟机将恢复到工作负载文件夹。



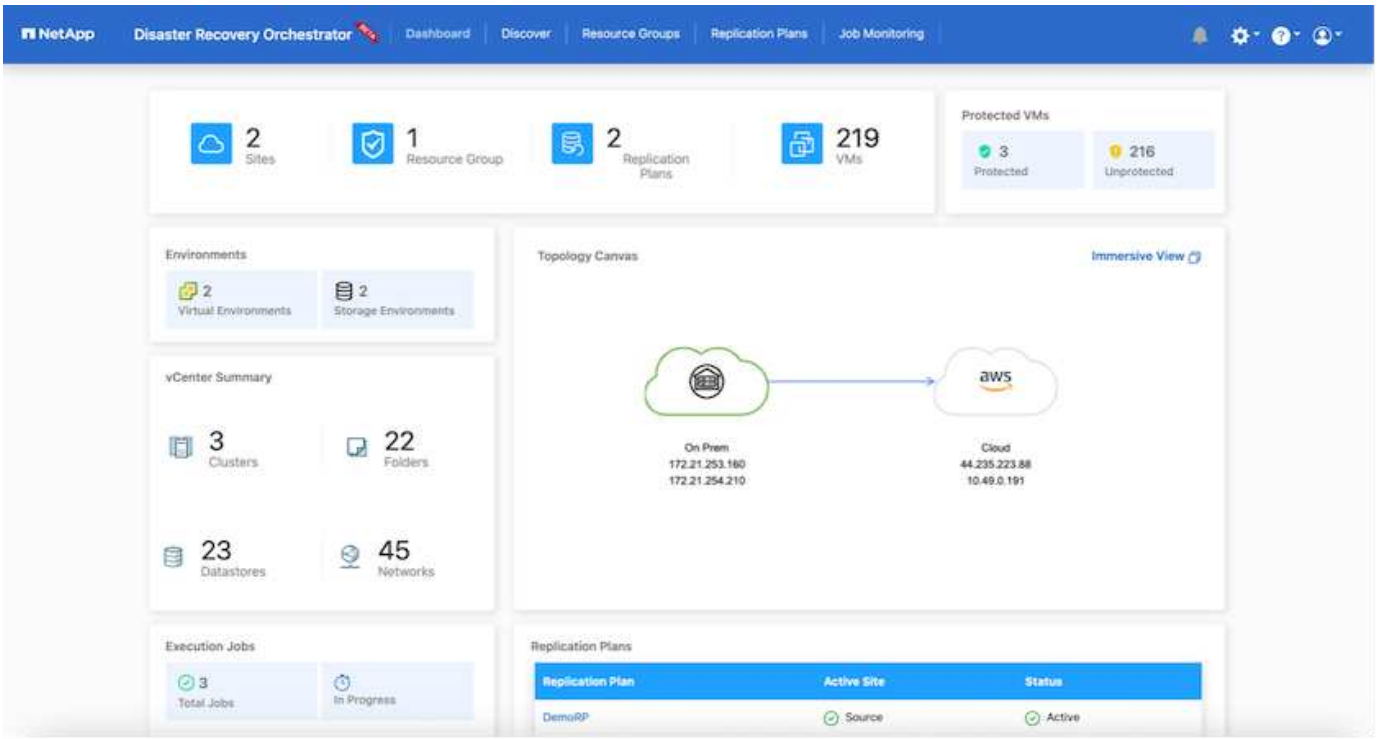
可以在复制计划级别触发故障恢复。对于测试故障转移，可使用拆除选项来回滚更改并删除FlexClone关系。与故障转移相关的故障回复是一个两步过程。选择复制计划并选择*反向数据同步*。



一旦完成后，您可以触发故障恢复以返回到原始生产站点。



从 NetApp Console 中，我们可以看到相应卷（映射到 VMC 作为读写卷的卷）的复制运行状况已中断。在测试故障转移期间，DRO 不会映射目标卷或副本卷。而是对所需的 SnapMirror（或 Snapshot）实例创建 FlexClone 副本，并公开 FlexClone 实例，该实例不会占用 FSx ONTAP 的额外物理容量。此过程可确保卷不被修改，即使在 DR 测试或分类工作流期间，副本作业也能继续运行。此外，此过程还可确保在发生错误或恢复损坏数据时，可以清理恢复操作，而不会有副本遭到销毁的风险。



勒索软件恢复

从勒索软件中恢复可能是一项艰巨的任务。具体来说，IT 组织很难确定安全的返回点，而且一旦确定，就很难保护恢复的工作负载免受休眠恶意软件或易受攻击的应用程序等的重复攻击。

DRO 可让您从任何可用时间点恢复系统，从而解决这些问题。您还可以将工作负载恢复到功能正常但隔离的网络中，以便应用程序可以在不会暴露于南北流量的位置运行并相互通信。这为您的安全团队提供了一个安全的地方来进行取证，并确保没有隐藏或休眠的恶意软件。

受益

- 使用高效且有弹性的SnapMirror复制。
- 通过 Snapshot 副本保留恢复到任何可用的时间点。
- 完全自动化从存储、计算、网络和应用程序验证步骤中恢复数百到数千台虚拟机所需的所有步骤。
- 使用ONTAP FlexClone技术进行工作负载恢复，采用的方法是不改变复制卷。
  - 避免卷或 Snapshot 副本的数据损坏风险。
  - 避免 DR 测试工作流程期间的复制中断。
  - DR 数据与云计算资源的潜在用途，可用于 DR 以外的工作流程，例如开发测试、安全测试、补丁或升级测试以及补救测试。
- 通过允许恢复到较小的计算集群，CPU 和 RAM 优化有助于降低云成本。

使用 **Veeam Replication** 和 **FSx ONTAP**实现 **VMware Cloud on AWS** 灾难恢复

Amazon FSx ONTAP与 VMware Cloud on AWS 的集成是一个 AWS 管理的外部 NFS 数据存储，它建立在 NetApp 的ONTAP文件系统上，可以连接到 SDDC 中的集群。它为客户提供灵活、高性能的虚拟化存储基础设施，可独立于计算资源进行扩展。

概述

对于希望使用 VMware Cloud on AWS SDDC 作为灾难恢复目标的客户，可以使用 FSx ONTAP数据存储区通过任何经过验证且提供 VM 复制功能的第三方解决方案从本地复制数据。通过添加 FSx ONTAP数据存储，它将实现成本优化部署，而不是在 AWS SDDC 上构建 VMware 云，并使用大量 ESXi 主机来容纳存储。

这种方法还可以帮助客户使用 VMC 中的试点灯集群以及 FSx ONTAP数据存储来托管 VM 副本。通过优雅地故障转移复制计划，相同的过程还可以扩展为到 VMware Cloud on AWS 的迁移选项。

问题陈述

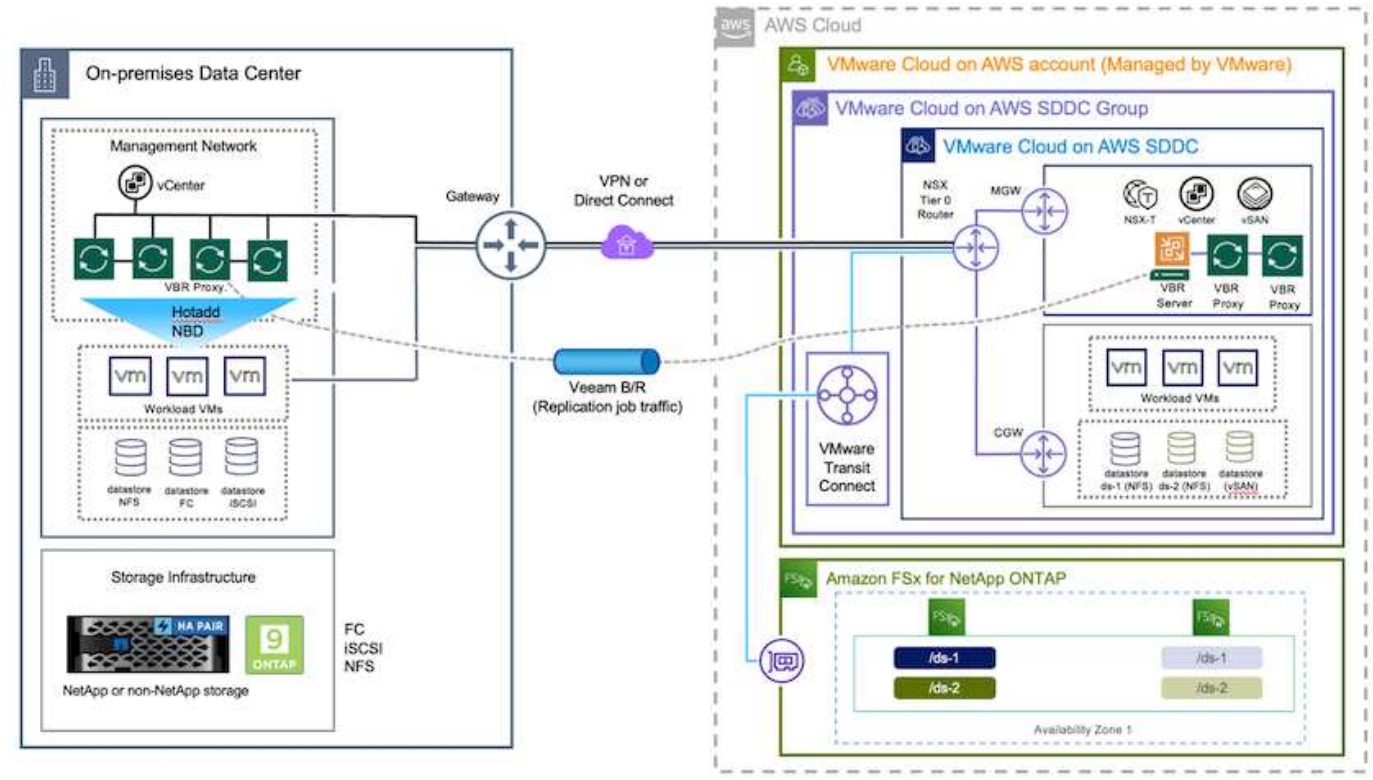
本文档介绍如何使用 FSx ONTAP数据存储和 Veeam Backup 和复制，通过 VM 复制功能为本地 VMware VM 到 VMware Cloud on AWS 设置灾难恢复。

Veeam Backup & Replication 允许现场和远程复制以实现灾难恢复 (DR)。当虚拟机被复制时，Veeam Backup & Replication 会在目标 VMware Cloud on AWS SDDC 集群上以原生 VMware vSphere 格式创建虚拟机的精确副本，并使该副本与原始虚拟机保持同步。

由于存在处于准备启动状态的 VM 副本，因此复制可提供最佳恢复时间目标 (RTO) 值。此复制机制可确保在发生灾难事件时工作负载能够在 VMware Cloud on AWS SDDC 中快速启动。 Veeam Backup & Replication 软件还优化了通过 WAN 和慢速连接进行复制的流量传输。此外，它还过滤掉重复的数据块、零数据块、交换文件和排除的 VM 客户操作系统文件，并压缩副本流量。

为了防止复制作业消耗整个网络带宽，可以实施 WAN 加速器和网络限制规则。 Veeam Backup & Replication 中的复制过程由作业驱动，这意味着复制是通过配置复制作业来执行的。如果发生灾难事件，可以触发故障转移，通过故障转移到其副本来恢复虚拟机。

当执行故障转移时，复制的虚拟机将接管原始虚拟机的角色。可以将故障转移到副本的最新状态或任何已知的良好还原点。这使得勒索软件恢复或隔离测试能够根据需要进行。在 Veeam Backup & Replication 中，故障转移和故障恢复是临时的中间步骤，需要进一步完成。 Veeam Backup & Replication 提供多种选项来处理不同的灾难恢复场景。



解决方案部署

高级步骤

1. Veeam Backup and Replication 软件在具有适当网络连接的本地环境中运行。
2. 要配置 VMware Cloud on AWS，请参阅 VMware Cloud Tech Zone 文章 "VMware Cloud on AWS 与Amazon FSx ONTAP集成部署指南" 以部署和配置 VMware Cloud on AWS SDDC，并将 FSx ONTAP 配置为 NFS 数据存储。（以最小配置设置的 pilot-light 环境可用于 DR 目的。在发生事件时，虚拟机将故障转移到此集群，并且可以添加其他节点）。
3. 设置复制作业以使用 Veeam Backup and Replication 创建 VM 副本。
4. 创建故障转移计划并执行故障转移。
5. 灾难事件结束且主站点启动后，切换回生产虚拟机。

Veeam VM 复制到 VMC 和 FSx ONTAP数据存储的先决条件

1. 确保 Veeam Backup & Replication 备份 VM 连接到源 vCenter 以及 AWS SDDC 集群上的目标 VMware 云。
2. 备份服务器必须能够解析短名称并连接到源 vCenter 和目标 vCenter。
3. 目标 FSx ONTAP数据存储必须具有足够的可用空间来存储复制虚拟机的 VMDK

有关更多信息，请参阅“注意事项和限制”"此处" 。

部署详情

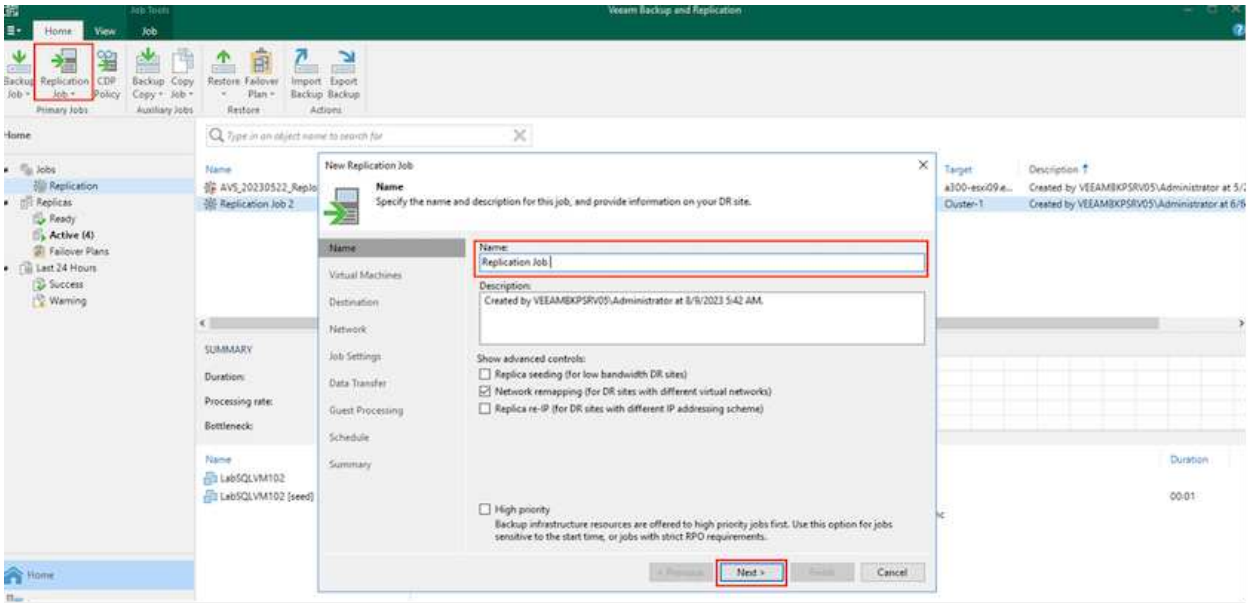
▼ 步骤 1：复制虚拟机

Veeam Backup & Replication 利用 VMware vSphere 快照功能，在复制期间，Veeam Backup & Replication

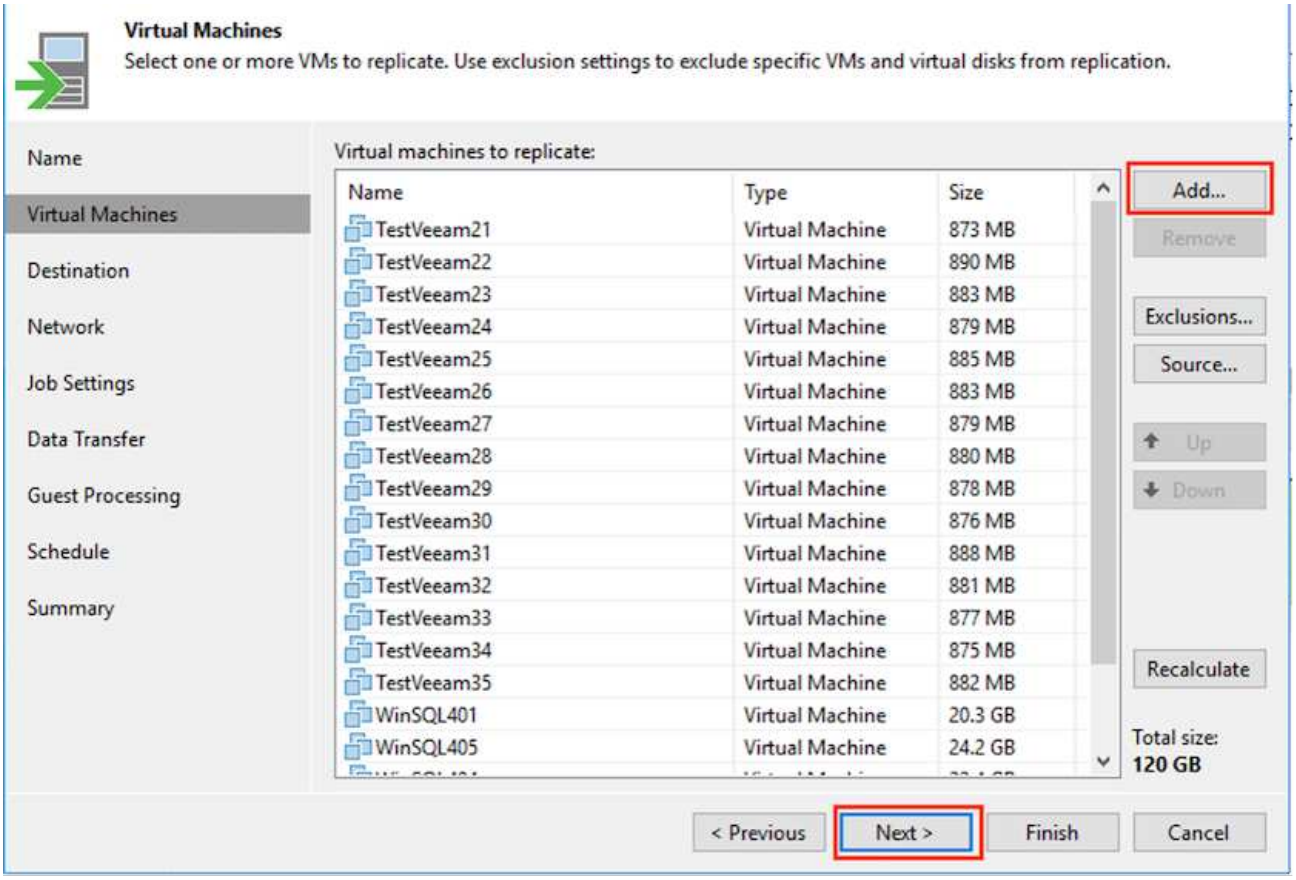
请求 VMware vSphere 创建 VM 快照。 VM 快照是 VM 的时间点副本，其中包括虚拟磁盘、系统状态、配置等。 Veeam Backup & Replication 使用快照作为复制的数据源。

要复制虚拟机，请按照以下步骤操作：

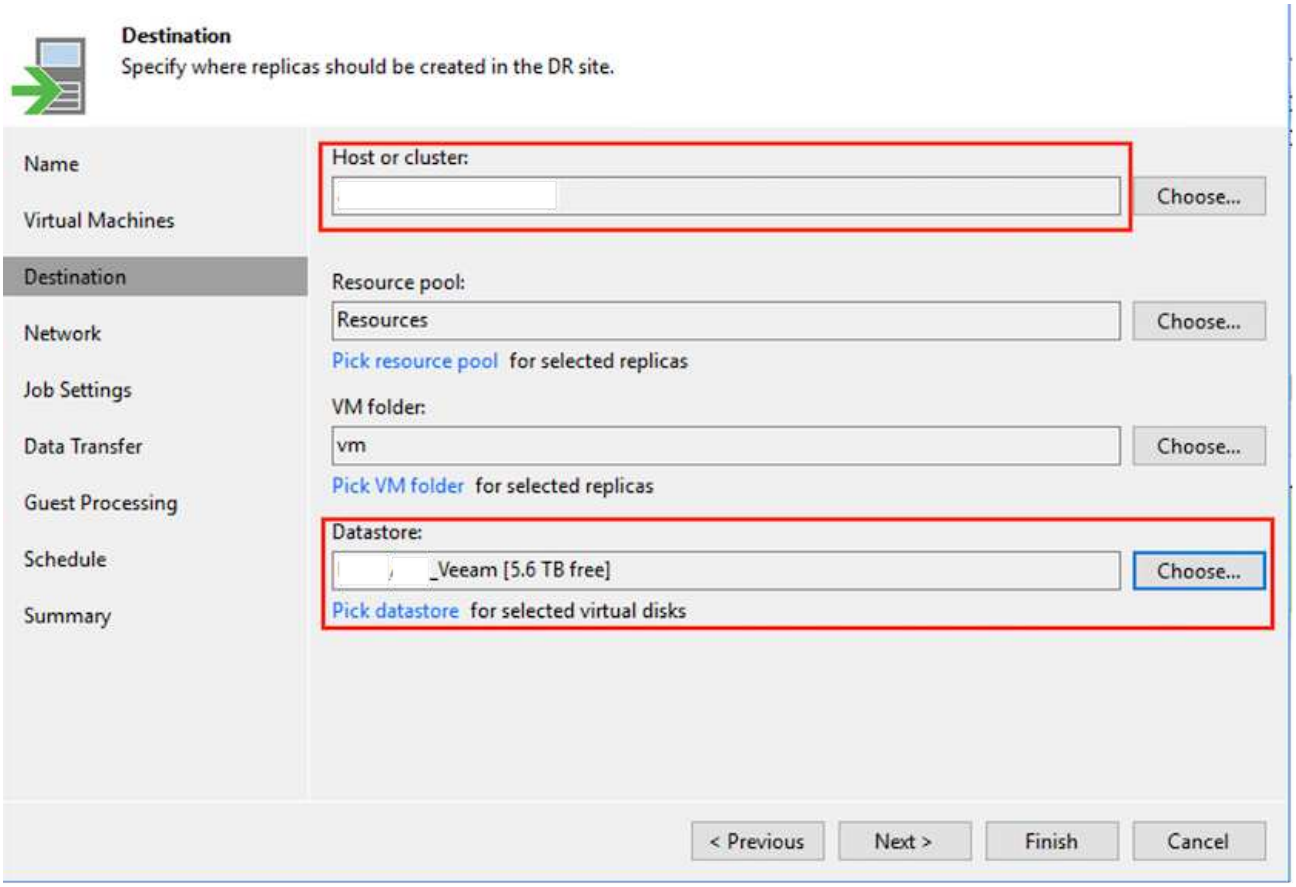
1. 打开 Veeam 备份和复制控制台。
2. 在主页视图上，选择复制作业 > 虚拟机 > VMware vSphere。
3. 指定作业名称并选择适当的高级控制复选框。单击“下一步”。
   - 如果本地和 AWS 之间的连接带宽受限，请选中“副本播种”复选框。
   - 如果 VMware Cloud on AWS SDDC 上的段与本地站点网络的段不匹配，请选中网络重新映射（针对具有不同网络的 AWS VMC 站点）复选框。
   - 如果本地生产站点中的 IP 寻址方案与 AWS VMC 站点中的方案不同，请选中副本重新 IP（对于具有不同 IP 寻址方案的 DR 站点）复选框。



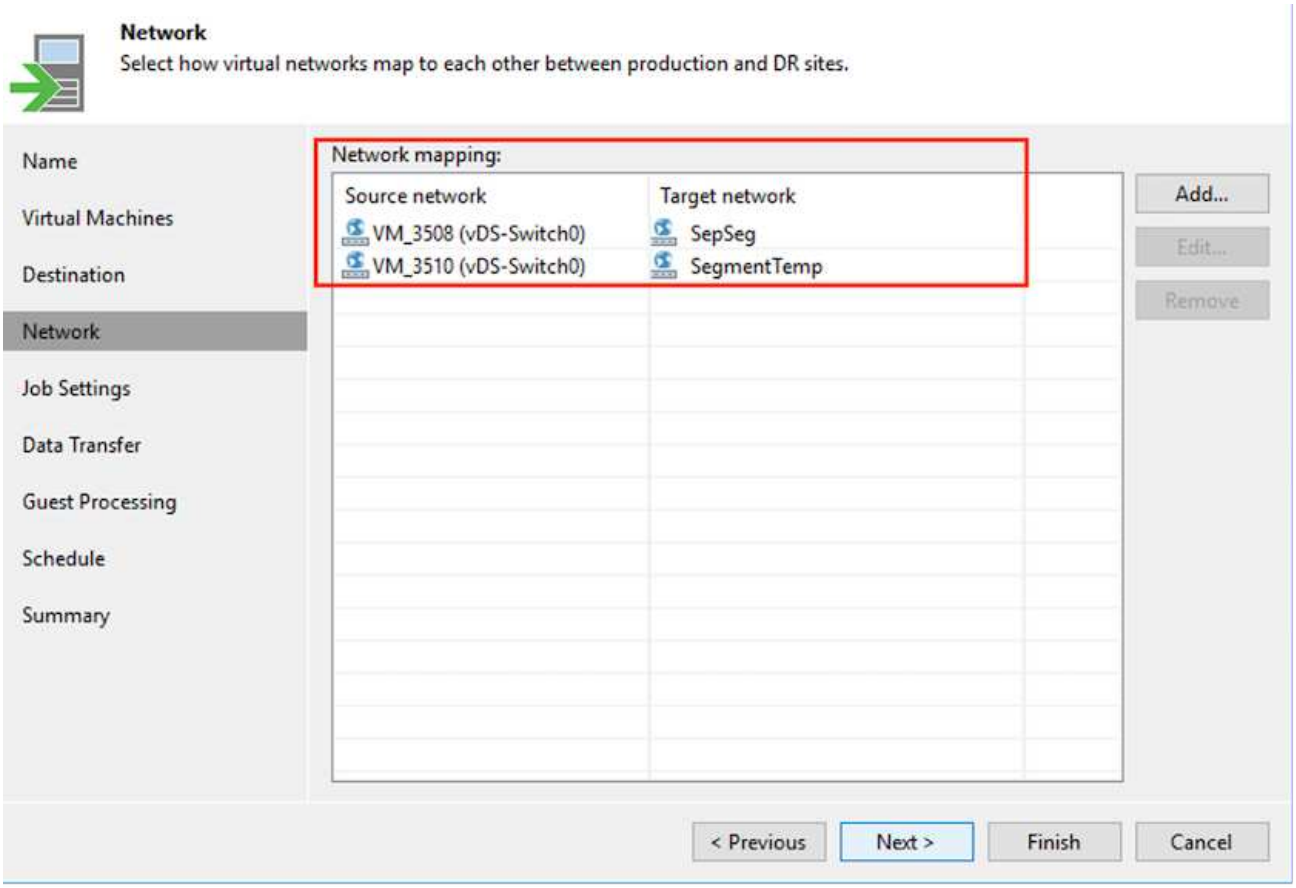
4. 在“虚拟机”步骤中选择需要复制到连接到 VMware Cloud on AWS SDDC 的 FSx ONTAP数据存储的虚拟机。可以将虚拟机放置在 vSAN 上以填充可用的 vSAN 数据存储容量。在试点集群中，3 节点集群的可用容量将受到限制。其余数据可以复制到 FSx ONTAP数据存储。单击*添加*，然后在*添加对象*窗口中选择必要的虚拟机或虚拟机容器，然后单击*添加*。单击“下一步”。



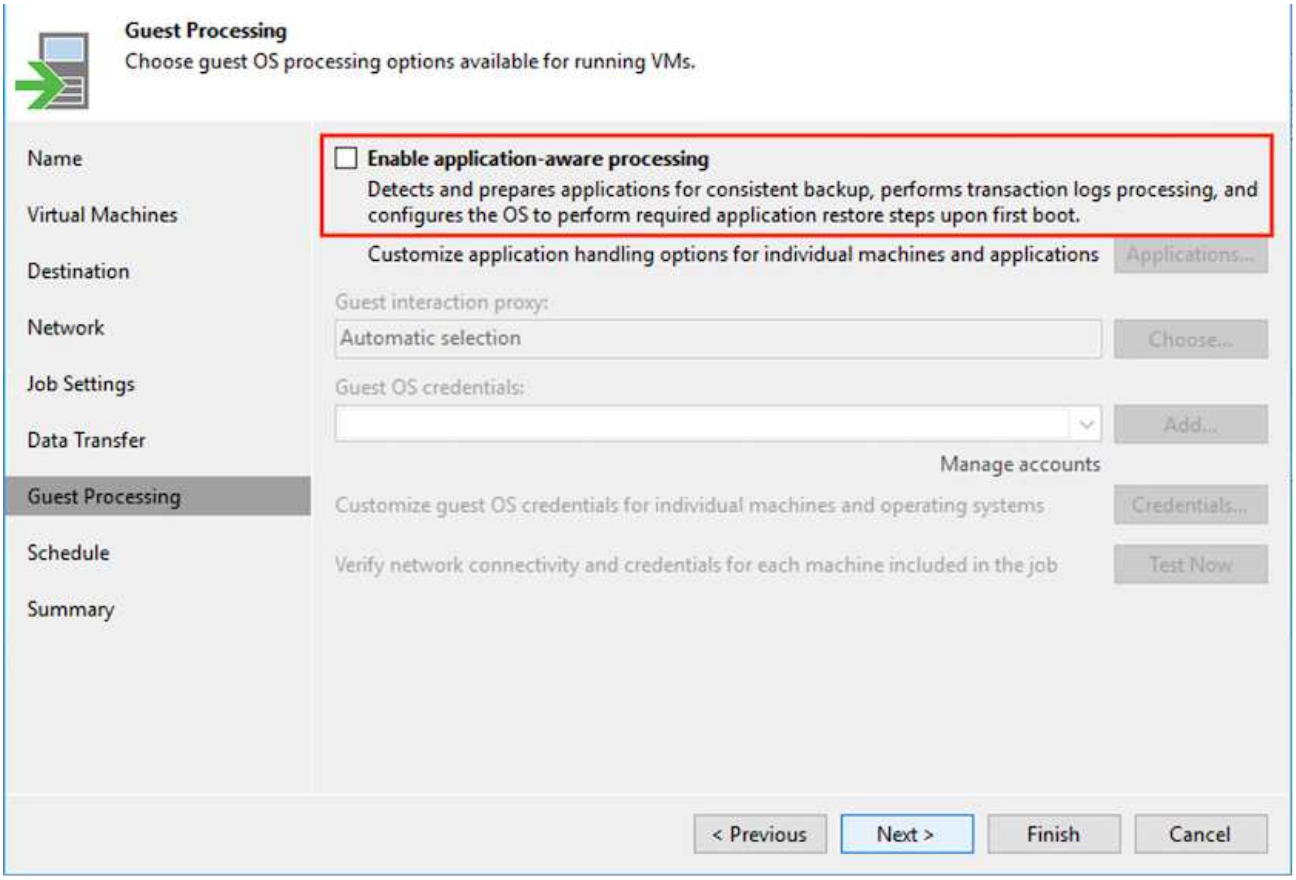
5. 之后，选择目标为 VMware Cloud on AWS SDDC 集群/主机，并选择适当的资源池、VM 文件夹和 VM 副本的 FSx ONTAP数据存储。然后单击“下一步”。



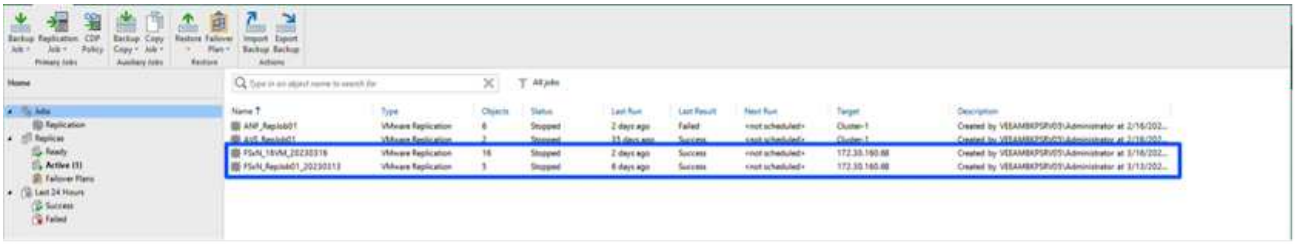
6. 下一步根据需要创建源虚拟网络和目标虚拟网络之间的映射。



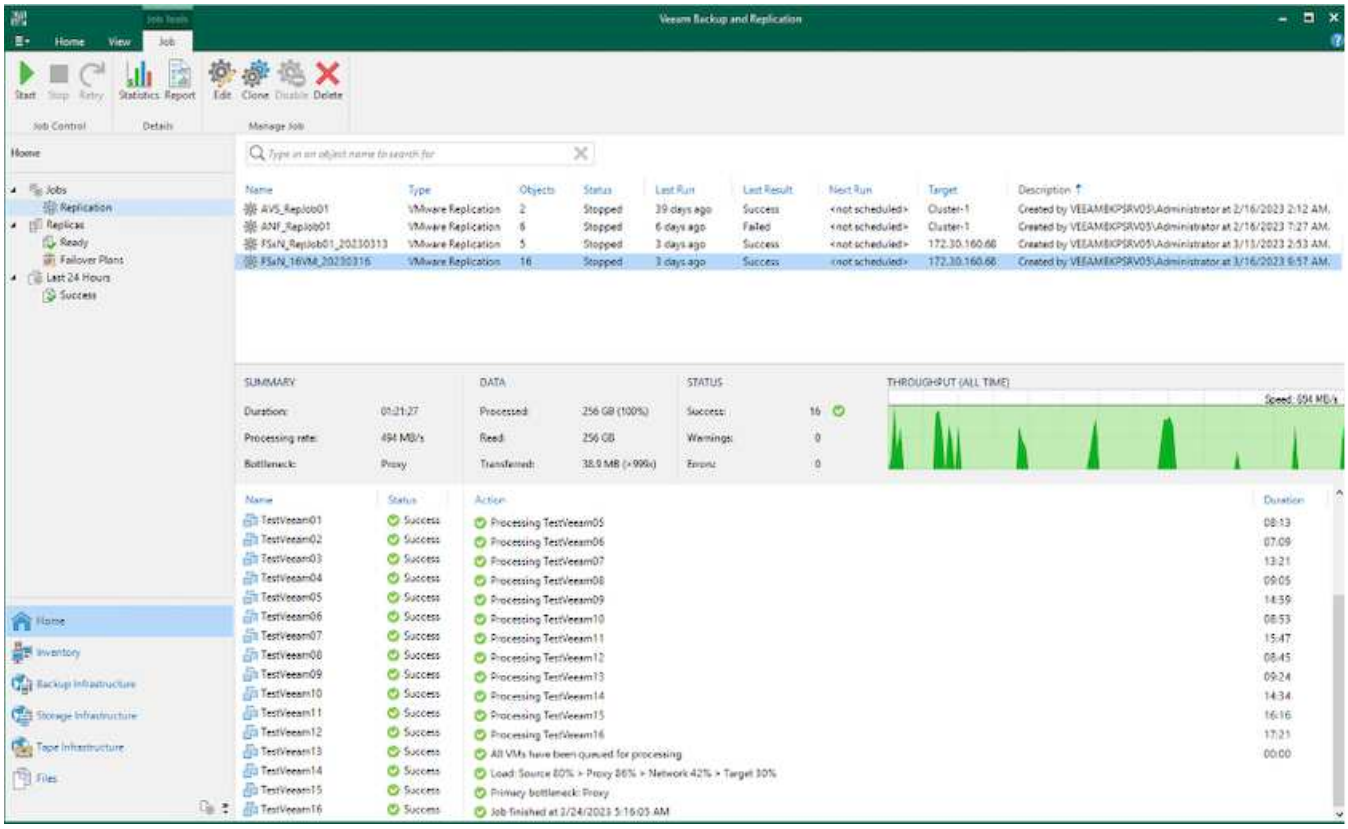
7. 在*作业设置*步骤中，指定将存储 VM 副本、保留策略等元数据的备份存储库。
8. 在*数据传输*步骤中更新*源*和*目标*代理服务器，保留*自动*选择（默认）并保持选择*直接*选项，然后单击*下一步*。
9. 在*Guest Processing*步骤中，根据需要选择*Enable application-aware processing*选项。单击“下一步”。



10. 选择复制计划来定期运行复制作业。
11. 在向导的*摘要*步骤中，查看复制作业的详细信息。要在向导关闭后立即启动作业，请选中*单击“完成”时运行作业*复选框，否则请不要选中该复选框。然后单击“完成”关闭向导。



复制作业启动后，具有指定后缀的虚拟机将填充到目标 VMC SDDC 集群/主机上。



有关 Veeam 复制的更多信息，请参阅"复制的工作原理"。

▼ 步骤 2：创建故障转移计划

初始复制或播种完成后，创建故障转移计划。故障转移计划有助于自动对从属虚拟机逐个或按组执行故障转移。故障转移计划是虚拟机处理顺序（包括启动延迟）的蓝图。故障转移计划还有助于确保关键依赖的虚拟机已经在运行。

要创建计划，请导航到名为“副本”的新子部分并选择“故障转移计划”。选择适当的虚拟机。 Veeam Backup & Replication 将查找最接近此时间点的还原点并使用它们启动 VM 副本。

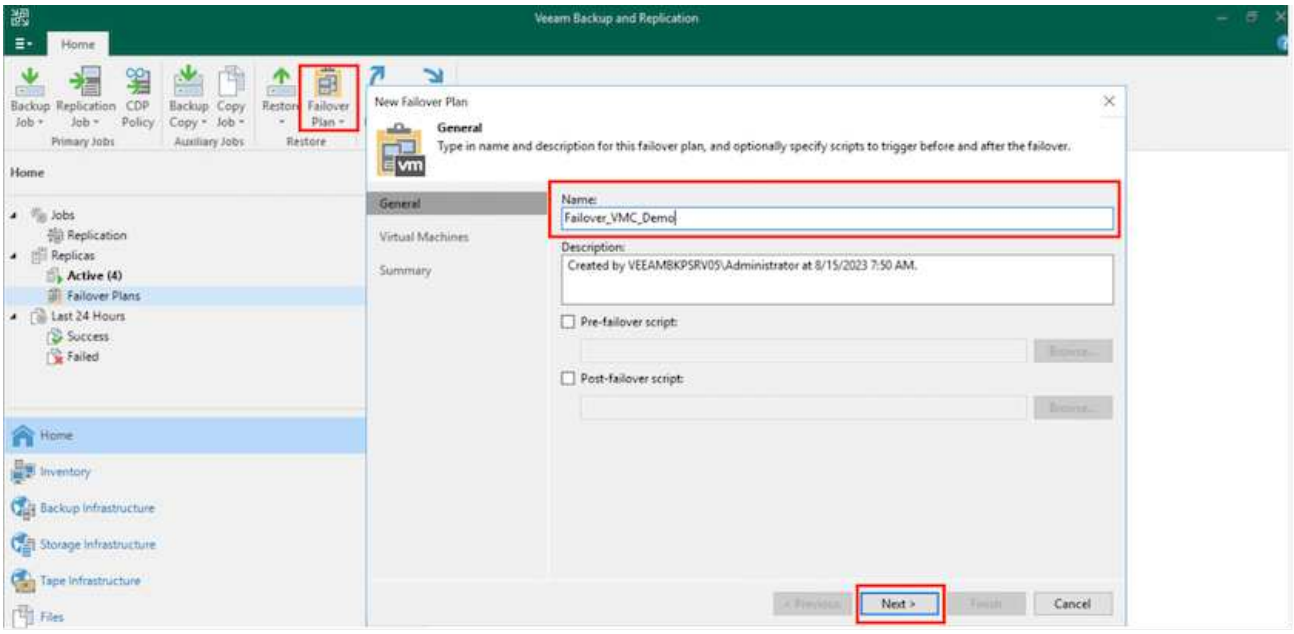
仅当初始复制完成且 VM 副本处于就绪状态后，才能添加故障转移计划。

运行故障转移计划时可同时启动的最大虚拟机数量为 10 个。

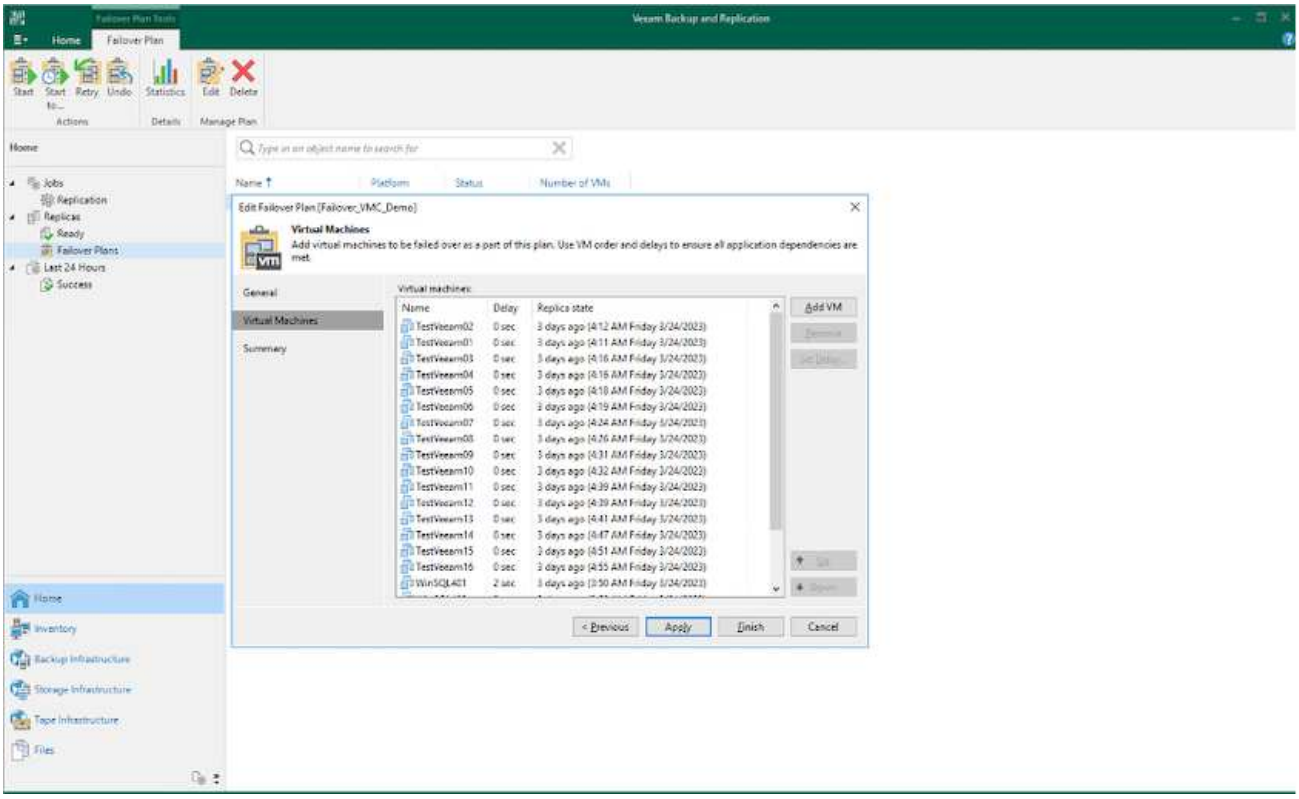
在故障转移过程中，源虚拟机不会关闭。

要创建*故障转移计划*，请执行以下操作：

1. 在主页视图上，选择“故障转移计划”>“VMware vSphere”。
2. 接下来，为计划提供名称和描述。可以根据需要添加故障转移前和故障转移后脚本。例如，在启动复制的虚拟机之前运行脚本来关闭虚拟机。



3. 将虚拟机添加到计划中，并修改虚拟机启动顺序和启动延迟以满足应用程序依赖关系。



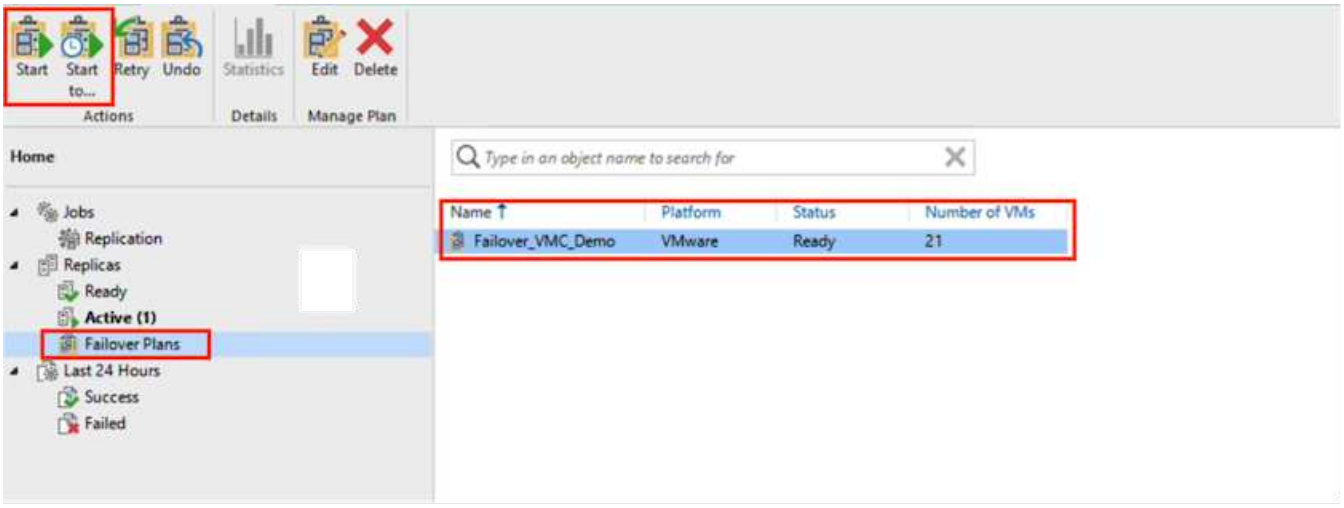
有关创建复制作业的其他信息，请参阅"创建复制作业"。

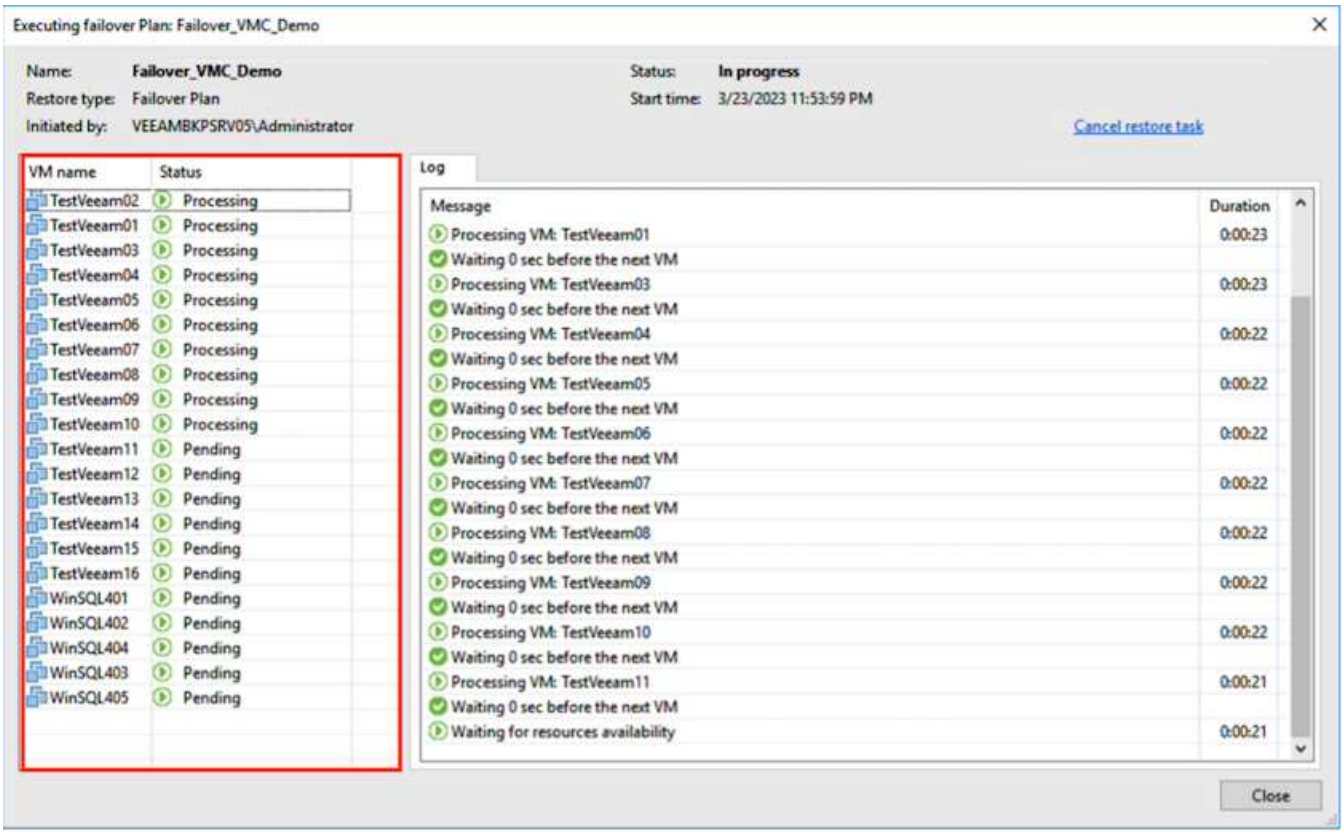
▼ 步骤 3：运行故障转移计划

在故障转移期间，生产站点中的源虚拟机将切换到灾难恢复站点上的副本。作为故障转移过程的一部分，Veeam Backup & Replication 将 VM 副本恢复到所需的恢复点，并将所有 I/O 活动从源 VM 移动到其副本。副本不仅可用于灾难发生时，还可用于模拟灾难恢复演习。在故障转移模拟期间，源虚拟机仍保持运行。一旦完成所有必要的测试，您就可以撤消故障转移并恢复正常操作。

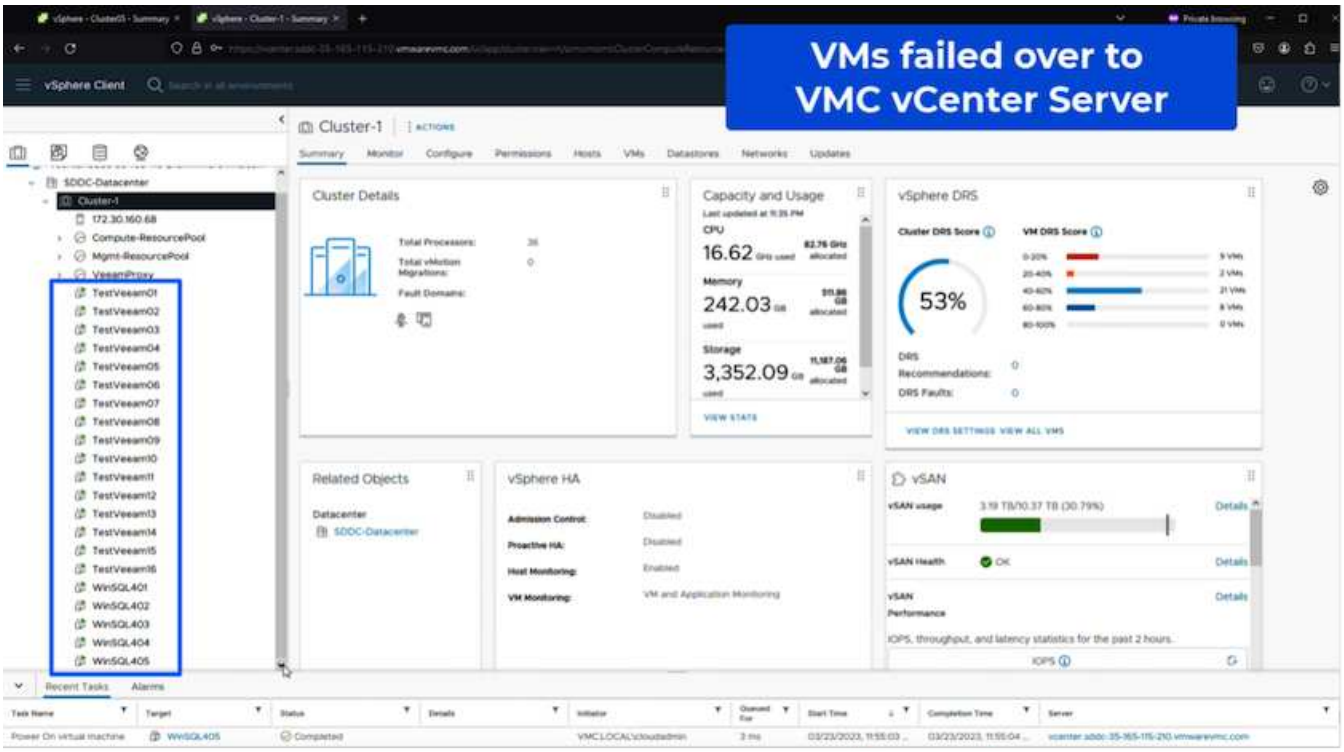
确保网络分段到位，以避免 DR 演习期间发生 IP 冲突。

要启动故障转移计划，只需单击“故障转移计划”选项卡，然后右键单击故障转移计划。选择“开始”。这将使用 VM 副本的最新还原点进行故障转移。要故障转移到 VM 副本的特定还原点，请选择*开始*。

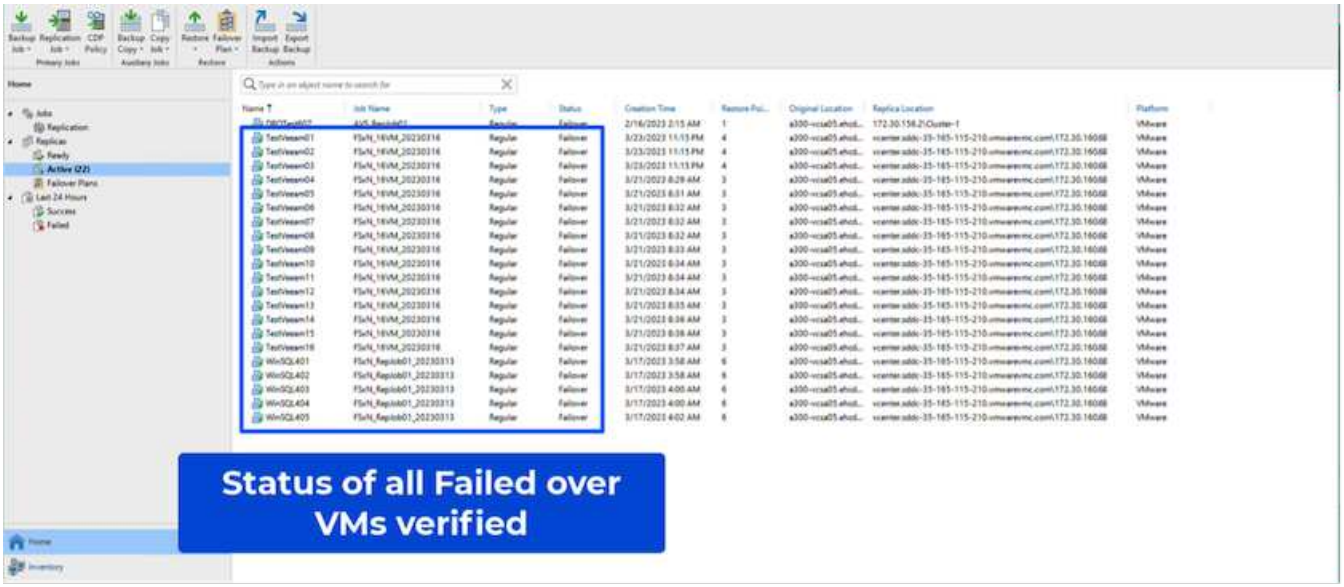




VM 副本的状态从“就绪”更改为“故障转移”，并且 VM 将在目标 VMware Cloud on AWS SDDC 集群/主机上启动。



故障转移完成后，虚拟机的状态将变为“故障转移”。



Veeam Backup & Replication 停止源 VM 的所有复制活动，直到其副本返回到就绪状态。

有关故障转移计划的详细信息，请参阅"故障转移计划"。

▼ 步骤 4：故障恢复到生产站点

当故障转移计划运行时，它被视为一个中间步骤，需要根据需求最终确定。选项包括以下内容：

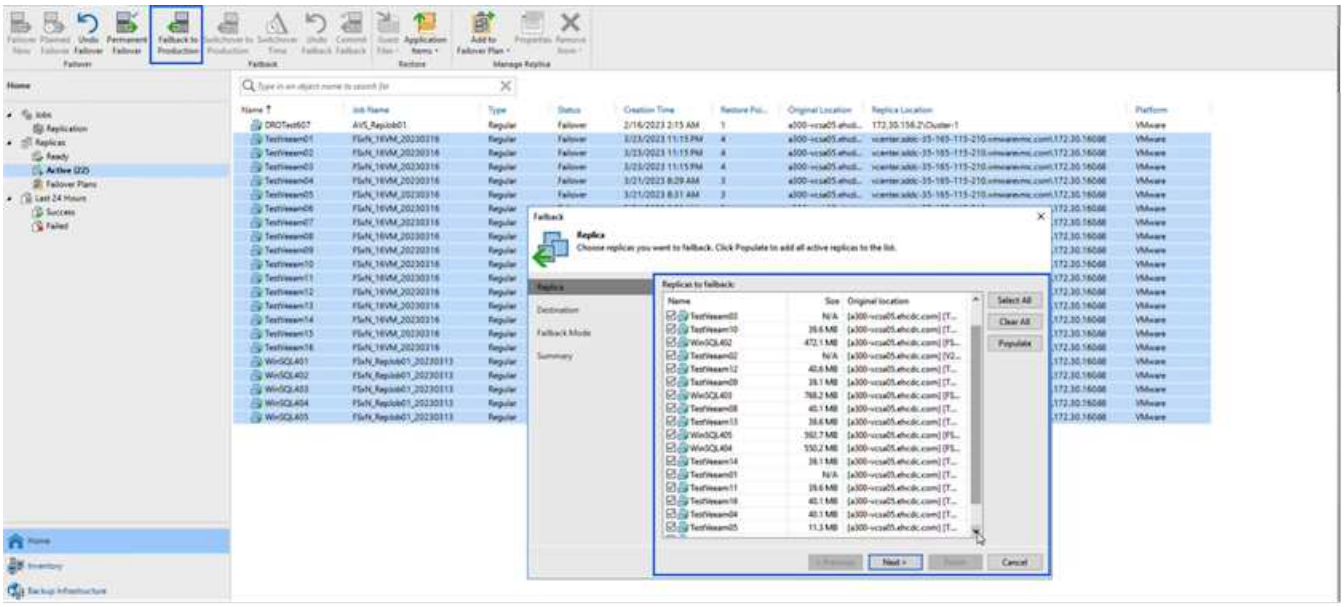
- 故障恢复到生产 - 切换回原始 VM，并将 VM 副本运行时发生的所有更改传输到原始 VM。

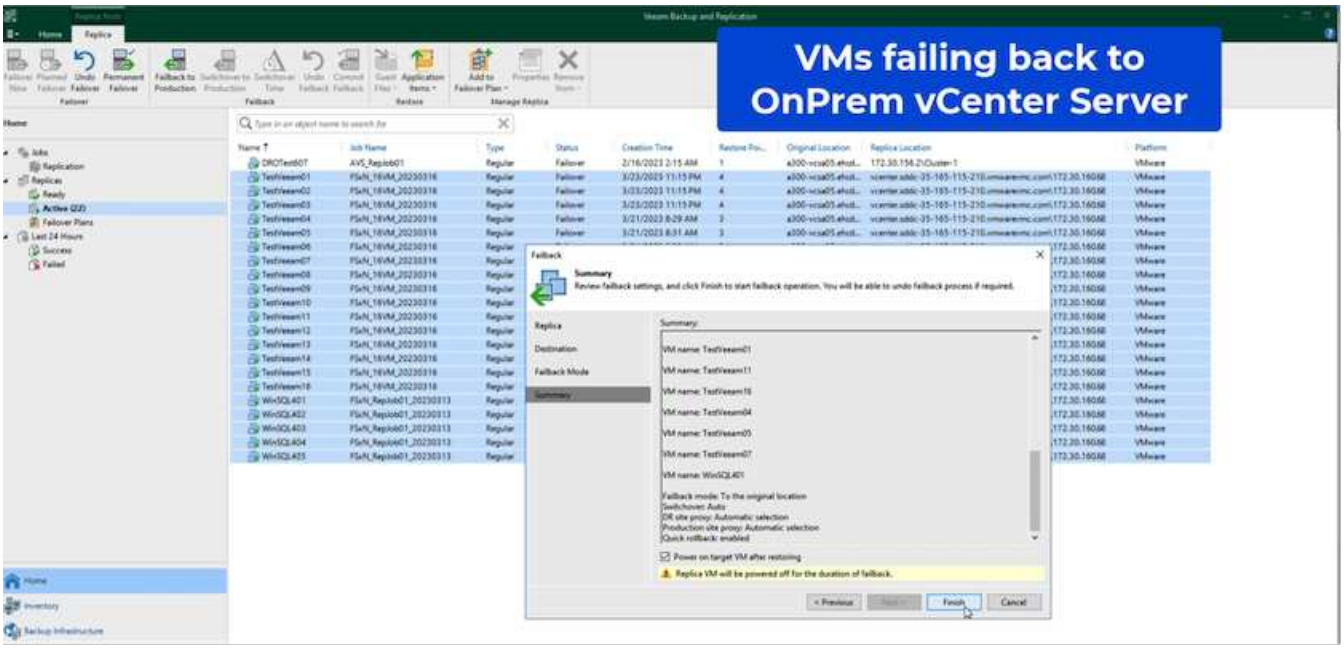
当您执行故障回复时，更改仅被传输但不会被发布。如果原始 VM 未按预期工作，请选择*提

交故障恢复*（一旦确认原始 VM 按预期工作）或*撤消故障恢复*以返回 VM 副本。

- 撤消故障转移 - 切换回原始虚拟机并放弃运行时对虚拟机副本所做的所有更改。
- 永久故障转移 - 从原始 VM 永久切换到 VM 副本，并使用此副本作为原始 VM。

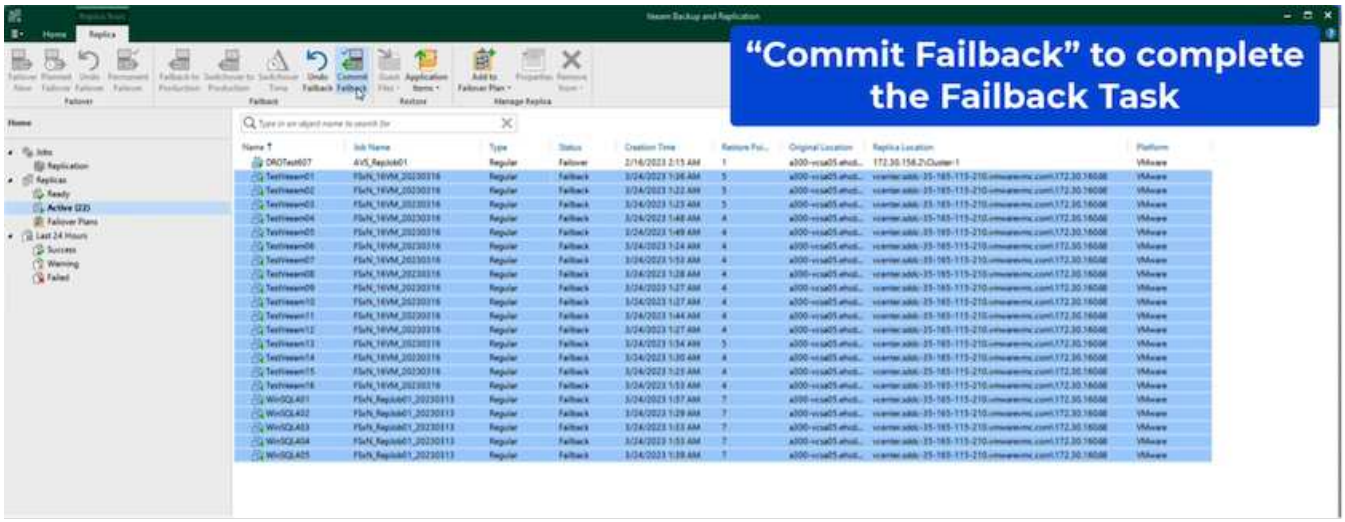
在这个演示中，选择了故障恢复到生产。在向导的目标步骤中选择了故障回复到原始虚拟机，并且启用了“恢复后启动虚拟机”复选框。

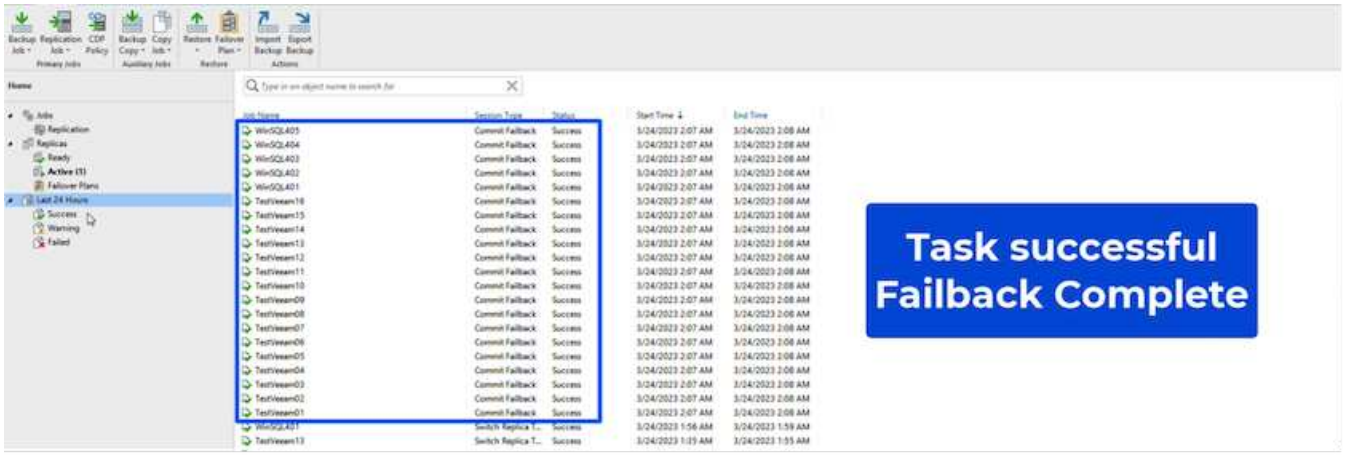




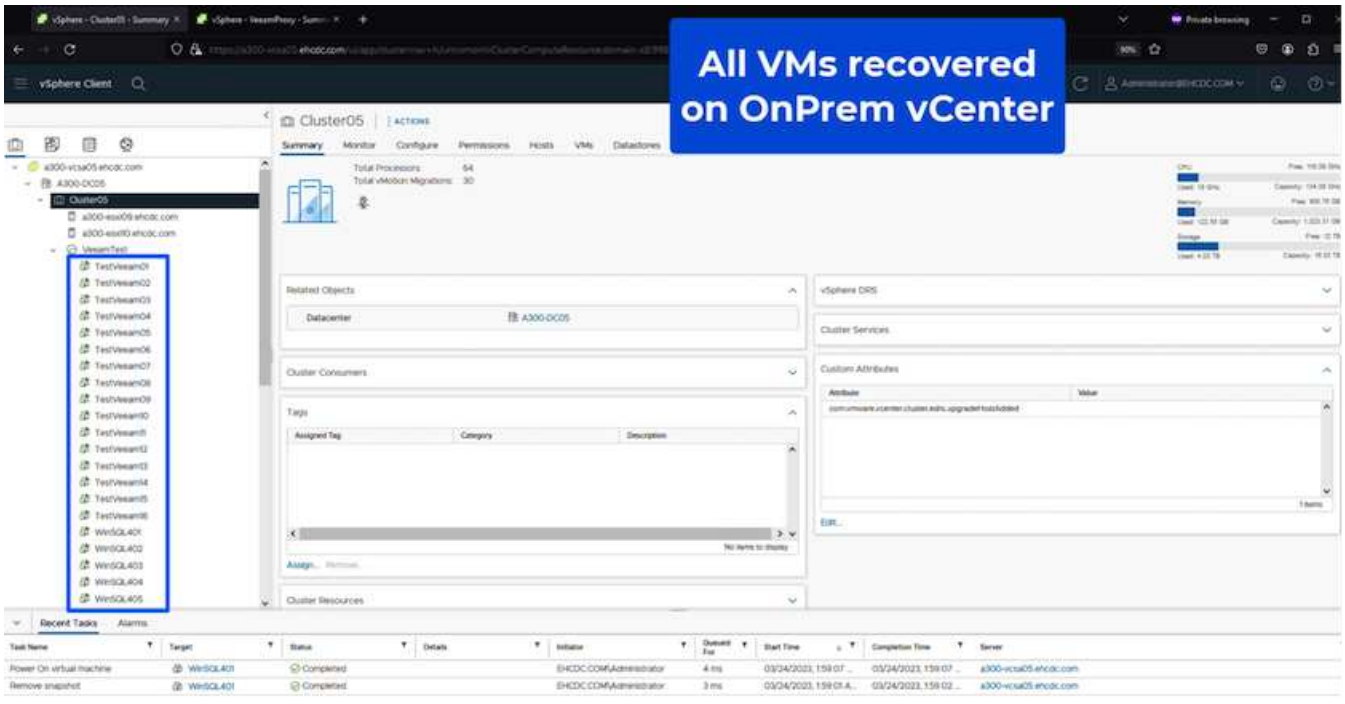
故障回复提交是完成故障回复操作的方法之一。当故障回复被提交时，它会确认发送到故障回复的虚拟机（生产虚拟机）的更改是否按预期工作。提交操作后，Veeam Backup & Replication 将恢复生产虚拟机的复制活动。

有关故障恢复过程的详细信息，请参阅 Veeam 文档"复制的故障转移和故障恢复"。





故障恢复生产成功后，所有虚拟机都将恢复到原始生产站点。



结束语

FSx ONTAP数据存储功能使 Veeam 或任何经过验证的第三方工具能够使用 Pilot Light 集群提供低成本的 DR 解决方案，而无需在集群中建立大量主机以容纳 VM 副本。这提供了一个强大的解决方案来处理量身定制的灾难恢复计划，并且还允许重复使用内部现有的备份产品来满足灾难恢复需求，从而通过退出内部灾难恢复数据中心实现基于云的灾难恢复。故障转移可以按计划进行，也可以在灾难发生时单击按钮进行故障转移，并决定激活 DR 站点。

要了解有关此过程的更多信息，请随意观看详细的演示视频。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

在 **AWS/VMC** 上迁移工作负载

TR 4942：使用 **VMware HCX** 将工作负载迁移到 **FSx ONTAP**数据存储区

Amazon Web Services (AWS) 上的 VMware Cloud (VMC) 及其在Amazon FSx ONTAP上的补充 NFS 数据存储的一个常见用例是迁移 VMware 工作负载。 VMware HCX 是一种首选方案，它提供了各种迁移方法，将在任何 VMware 支持的数据存储上运行的本地虚拟机 (VM) 及其数据移动到 VMC 数据存储，其中包括 FSx ONTAP上的补充 NFS 数据存储。

概述：使用 **VMware HCX**、**FSx ONTAP**补充数据存储区和 **VMware Cloud** 迁移虚拟机

VMware HCX 主要是一个移动平台，旨在简化跨云的工作负载迁移、工作负载重新平衡和业务连续性。它是 AWS 上 VMware Cloud 的一部分，提供多种迁移工作负载的方法，并可用于灾难恢复 (DR) 操作。

本文档提供了在本地和云数据中心端部署和配置 VMware HCX（包括其所有主要组件）的分步指导，从而实现各种 VM 迁移机制。

有关详细信息，请参阅 "VMware HCX 用户指南"和 "安装清单 B - 使用 VMware Cloud on AWS SDDC 目标环境的 HCX"。

▼ 概要步骤

此列表提供了安装和配置 VMware HCX 的高级步骤：

1. 通过 VMware Cloud Services Console 为 VMC 软件定义数据中心 (SDDC) 激活 HCX。
2. 在本地 vCenter Server 中下载并部署 HCX Connector OVA 安装程序。
3. 使用许可证密钥激活 HCX。
4. 将本地 VMware HCX Connector 与 VMC HCX Cloud Manager 配对。
5. 配置网络配置文件、计算配置文件和服务网格。
6. （可选）执行网络扩展以扩展网络并避免重新 IP。
7. 验证设备状态并确保可以迁移。
8. 迁移虚拟机工作负载。

▼ 前提条件

开始之前，请确保满足以下先决条件。有关更多信息，请参阅 "准备安装" 。在满足先决条件（包括连接性）后，通过从 VMC 的 VMware HCX 控制台生成许可证密钥来配置和激活 HCX。 HCX 激活后，vCenter 插件即被部署，可以通过 vCenter 控制台进行访问管理。

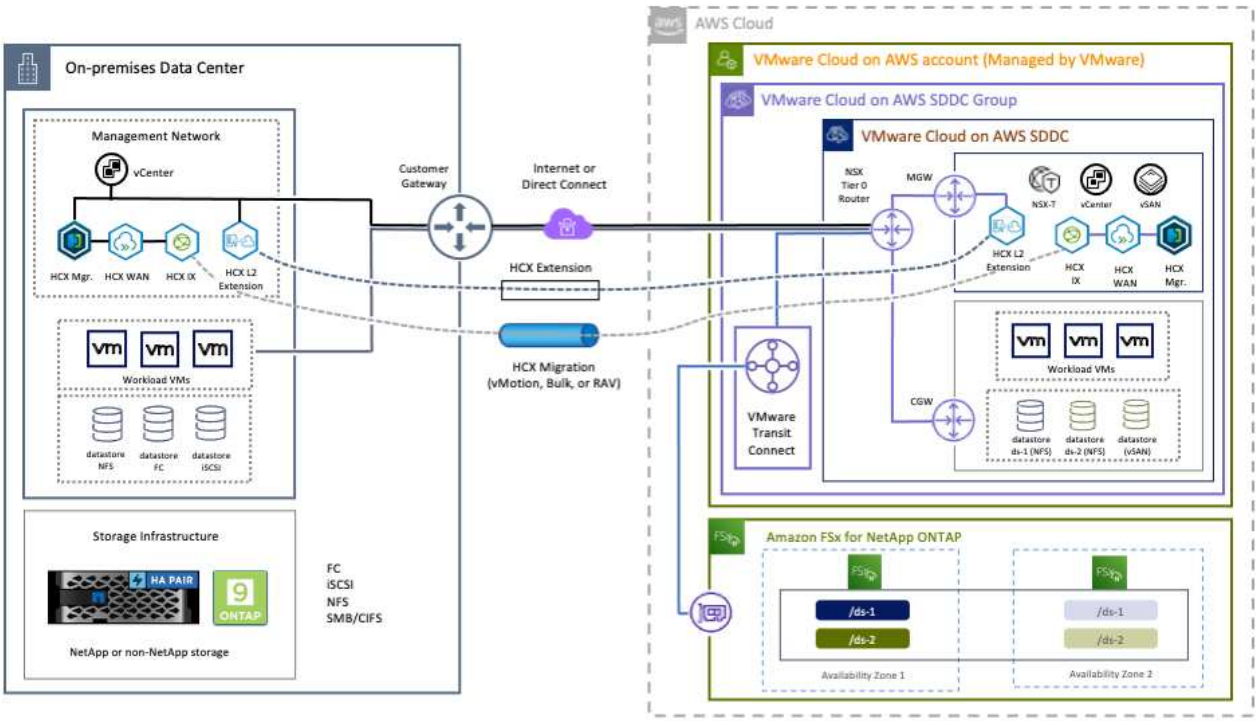
在继续 HCX 激活和部署之前，必须完成以下安装步骤：

1. 使用现有的 VMC SDDC 或按照此步骤创建新的 SDDC"NetApp链接"或者这个 "VMware 链接"。
2. 从本地 vCenter 环境到 VMC SDDC 的网络路径必须支持使用 vMotion 迁移虚拟机。
3. 确保所需的 "防火墙规则和端口"允许在本地 vCenter Server 和 SDDC vCenter 之间进行 vMotion 流量。
4. FSx ONTAP NFS 卷应作为补充数据存储安装在 VMC SDDC 中。要将 NFS 数据存储附加到适当的集群，请按照本"NetApp链接"或者这个 "VMware 链接"。

▼ 高级架构

为了测试目的，用于此验证的本地实验室环境通过站点到站点 VPN 连接到 AWS VPC，从而允许通过外部传输网关在本地连接到 AWS 和 VMware 云 SDDC。 HCX 迁移和网络扩展流量通过互联网在本地和 VMware 云目标 SDDC 之间流动。可以修改此架构以使用 Direct Connect 私有虚拟接口。

下图描述了高级架构。



解决方案部署

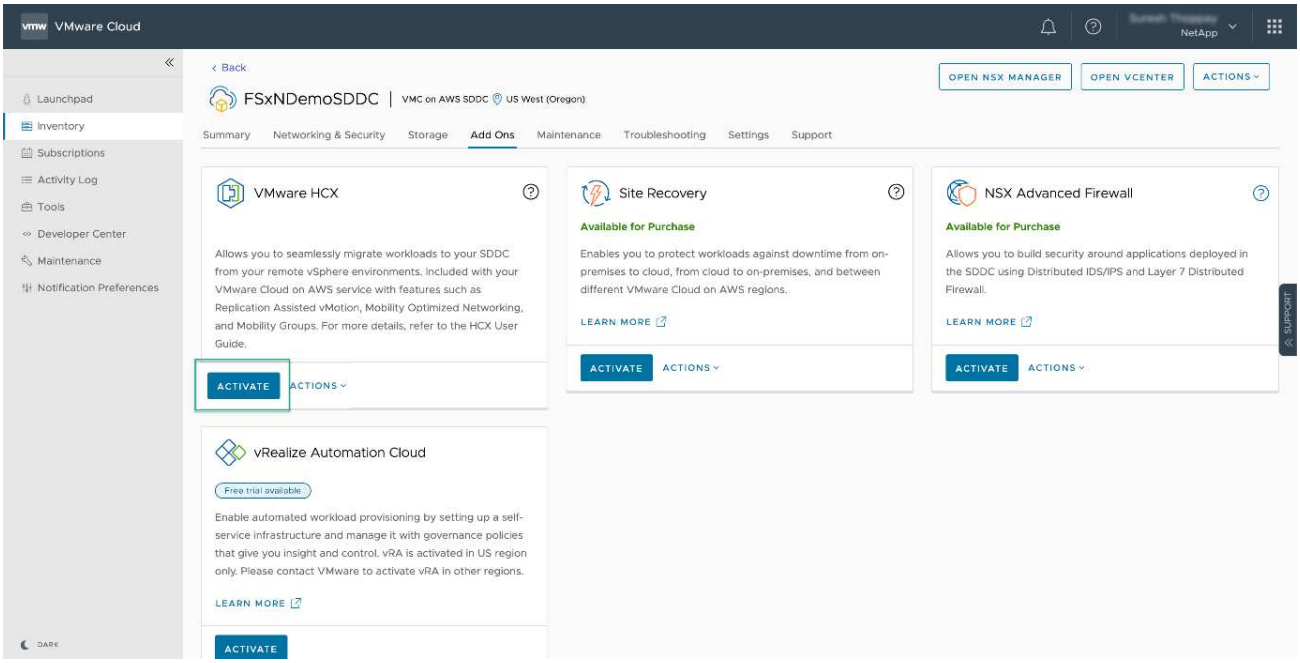
按照一系列步骤完成此解决方案的部署：

▼ 步骤 **1**：使用附加组件选项通过 **VMC SDDC** 激活 **HCX**

要执行安装，请完成以下步骤：

1. 登录到 VMC 控制台 "vmc.vmware.com"并访问库存。
2. 要选择适当的 SDDC 并访问附加组件，请单击 SDDC 上的“查看详细信息”，然后选择“附加组件”选项卡。
3. 单击“激活 VMware HCX”。

此步骤最多需要 25 分钟才能完成。

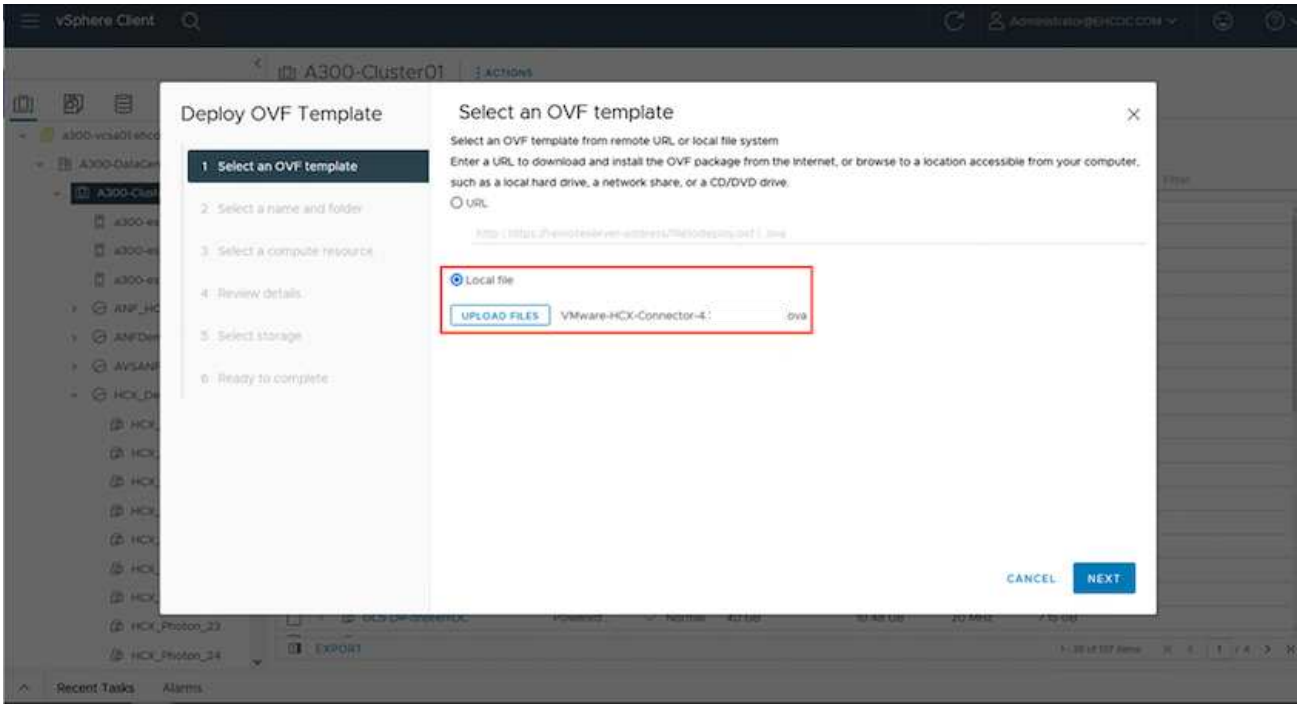


4. 部署完成后，通过确认 HCX Manager 及其相关插件在 vCenter 控制台中可用来验证部署。
5. 创建适当的管理网关防火墙以打开访问 HCX 云管理器所需的端口。HCX 云管理器现在已准备好进行 HCX 操作。

▼ 步骤 **2**：在本地 **vCenter Server** 中部署安装程序 **OVA**

为了使本地连接器能够与 VMC 中的 HCX 管理器通信，请确保在本地环境中打开了相应的防火墙端口。

1. 从 VMC 控制台导航到 HCX 仪表板，转到管理，然后选择系统更新选项卡。单击“请求下载链接”以获取 HCX 连接器 OVA 图像。
2. 下载 HCX 连接器后，在本地 vCenter Server 中部署 OVA。右键单击 vSphere 集群并选择部署 OVF 模板选项。

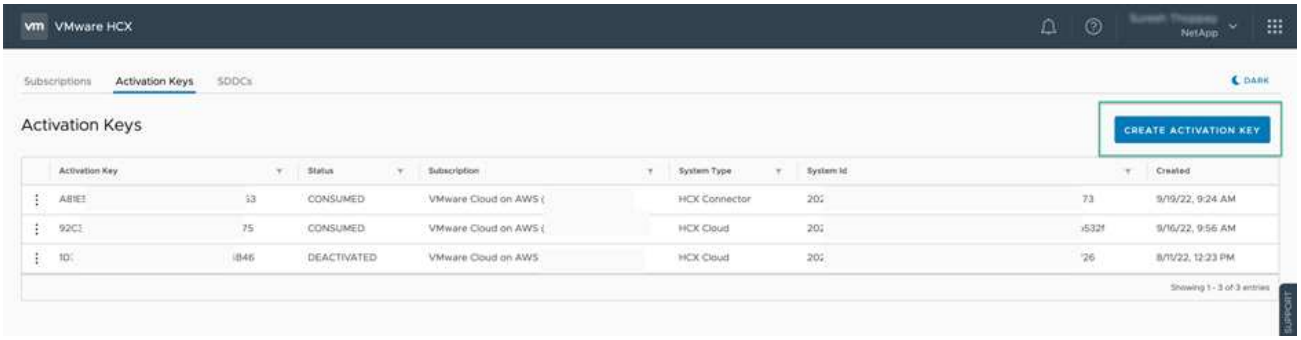


3. 在部署 OVF 模板向导中输入所需信息，单击下一步，然后单击完成以部署 VMware HCX 连接器 OVA。
4. 手动启动虚拟设备。有关分步说明，请转至 "VMware HCX 用户指南"。

▼ 步骤 3：使用许可证密钥激活 **HCX Connector**

在本地部署 VMware HCX Connector OVA 并启动设备后，请完成以下步骤以激活 HCX Connector。从 VMC 的 VMware HCX 控制台生成许可证密钥，并在 VMware HCX 连接器设置期间输入许可证。

1. 从 VMware Cloud Console 中，转到“清单”，选择 SDDC，然后单击“查看详细信息”。在“附加组件”选项卡的 VMware HCX 磁贴中，单击“打开 HCX”。
2. 在“激活密钥”选项卡中，单击“创建激活密钥”。选择系统类型为HCX连接器，然后单击确认以生成密钥。复制激活密钥。



每个在本地部署的 HCX 连接器都需要单独的密钥。

3. 登录到本地 VMware HCX 连接器，网址为 `"https://hcxconnectorIP:9443"`使用管理员凭据。

使用 OVA 部署期间定义的密码。

4. 在许可部分，输入从步骤 2 复制的激活密钥，然后单击激活。

本地 HCX 连接器必须具有 Internet 访问权限才能成功完成激活。

5. 在数据中心位置下，提供在本地安装 VMware HCX 管理器所需的位置。单击“Continue”。
6. 在系统名称下，更新名称并单击继续。
7. 选择“是”，然后“继续”。
8. 在“连接您的 vCenter”下，提供 vCenter Server 的 IP 地址或完全限定域名 (FQDN) 和凭据，然后单击“继续”。

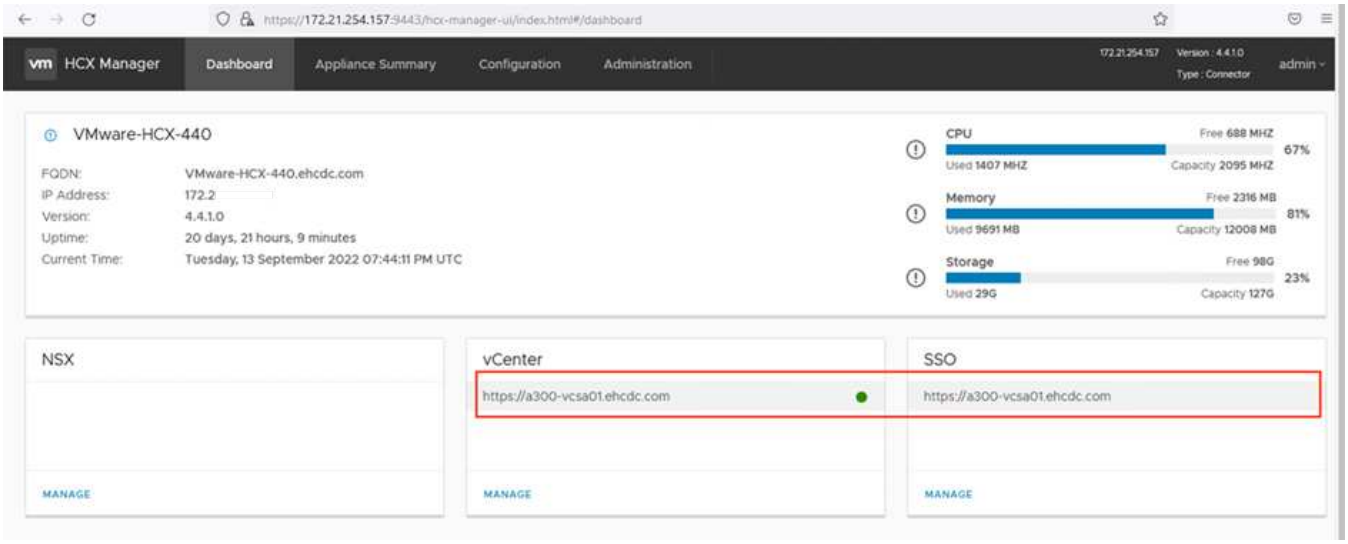
使用 FQDN 以避免以后出现通信问题。

9. 在配置 SSO/PSC 下，提供平台服务控制器的 FQDN 或 IP 地址，然后单击继续。

输入 vCenter Server 的 IP 地址或 FQDN。

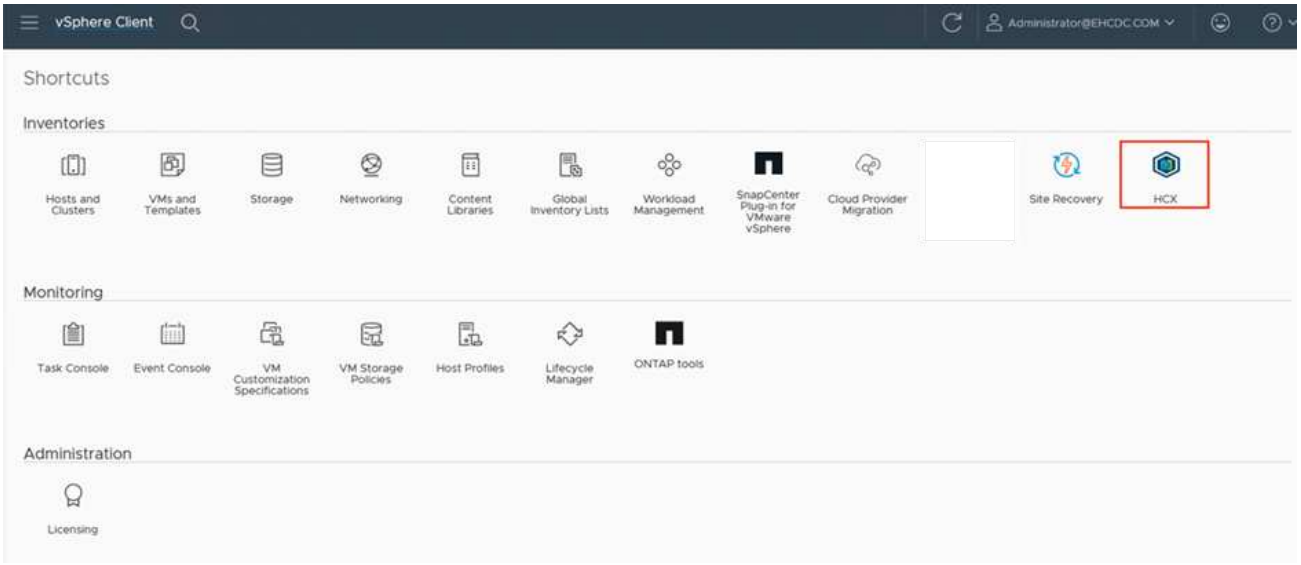
10. 验证信息输入是否正确，然后单击“重新启动”。
11. 完成后，vCenter Server 显示为绿色。 vCenter Server 和 SSO 都必须具有正确的配置参数，这些参数应与上一页相同。

此过程大约需要 10 到 20 分钟，以便将插件添加到 vCenter Server。

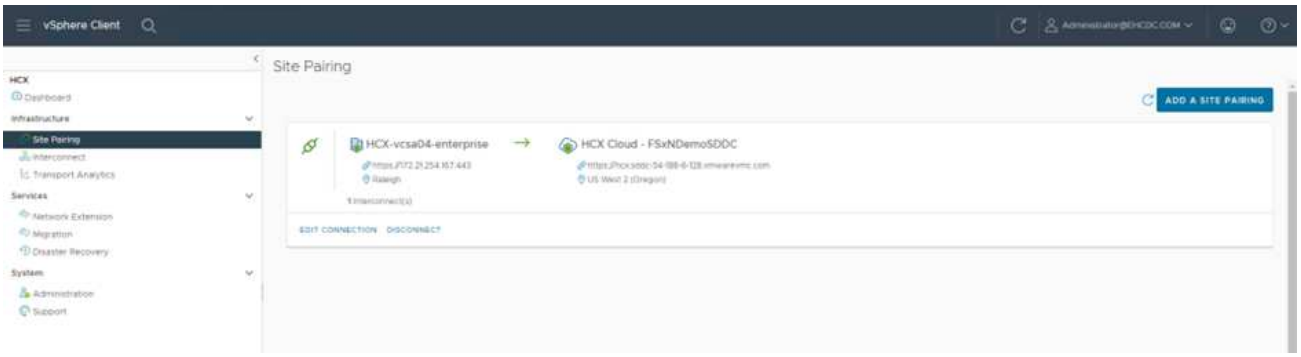


▼ 步骤 **4**：将本地 **VMware HCX Connector** 与 **VMC HCX Cloud Manager** 配对

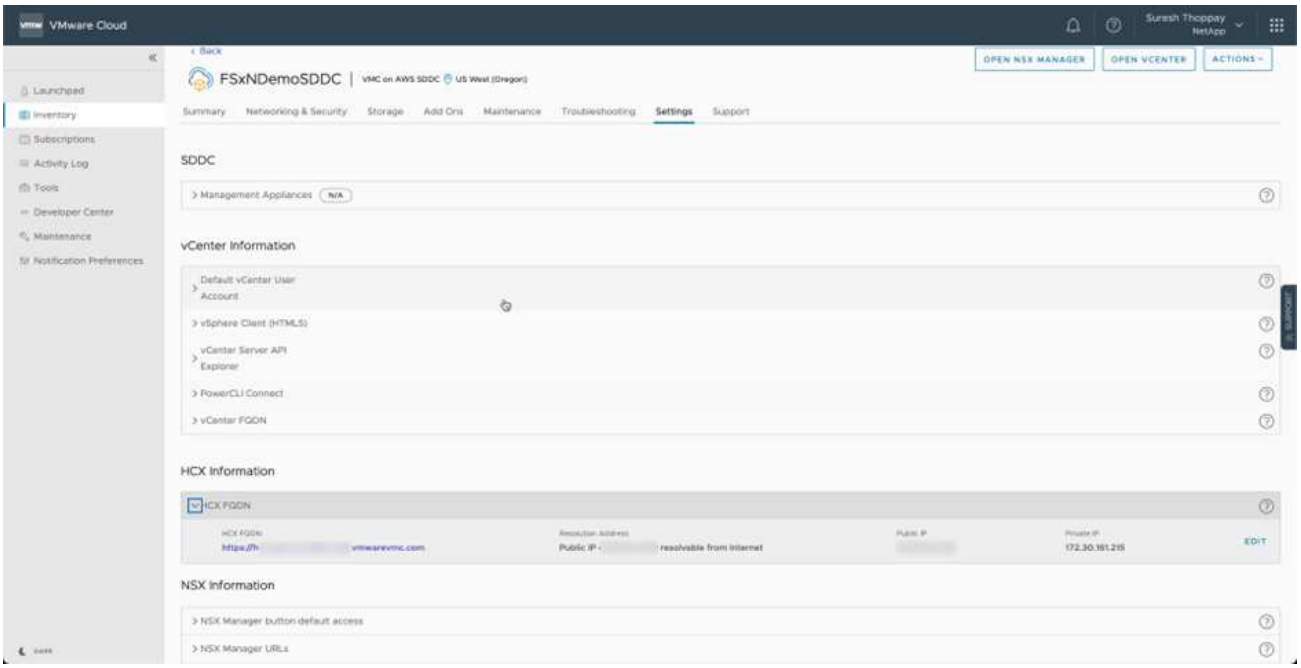
1. 要在本地 vCenter Server 和 VMC SDDC 之间创建站点对，请登录到本地 vCenter Server 并访问 HCX vSphere Web Client 插件。

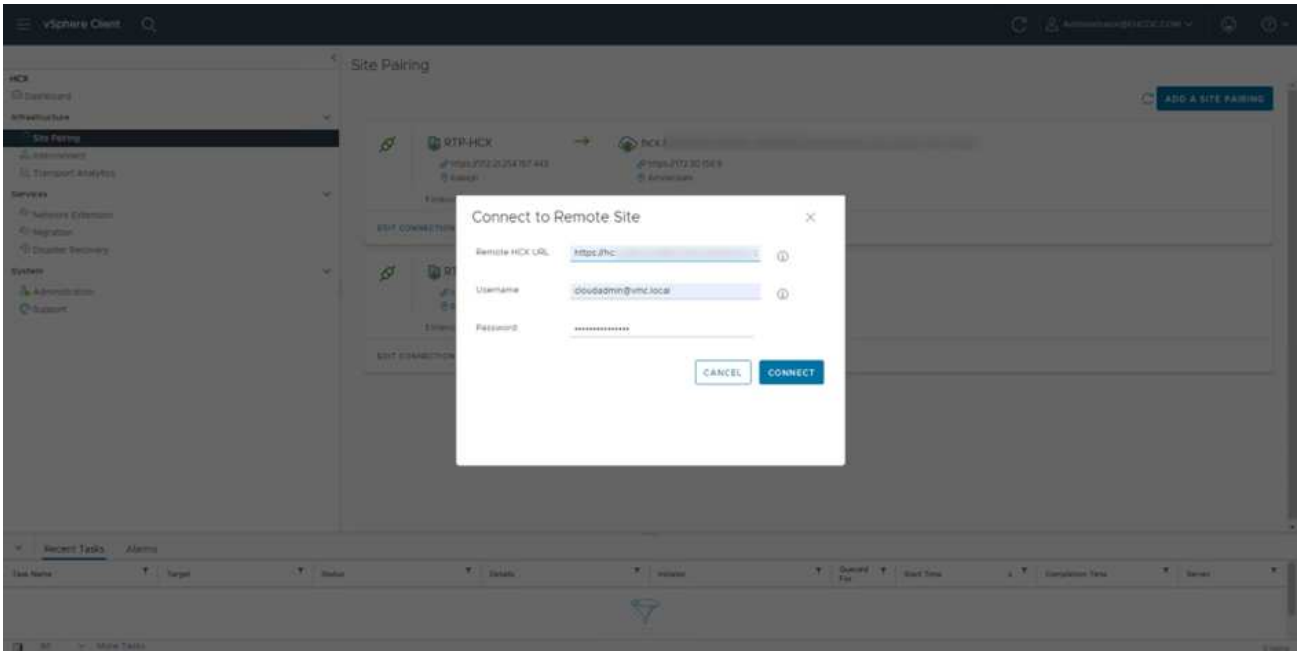


2. 在基础设施下，单击添加站点配对。要对远程站点进行身份验证，请输入 VMC HCX Cloud Manager URL 或 IP 地址以及 CloudAdmin 角色的凭据。



可以从 SDDC 设置页面检索 HCX 信息。





3. 要启动站点配对，请单击“连接”。

   VMware HCX Connector 必须能够通过端口 443 与 HCX Cloud Manager IP 通信。

4. 创建配对后，新配置的站点配对可在 HCX 仪表板上获得。

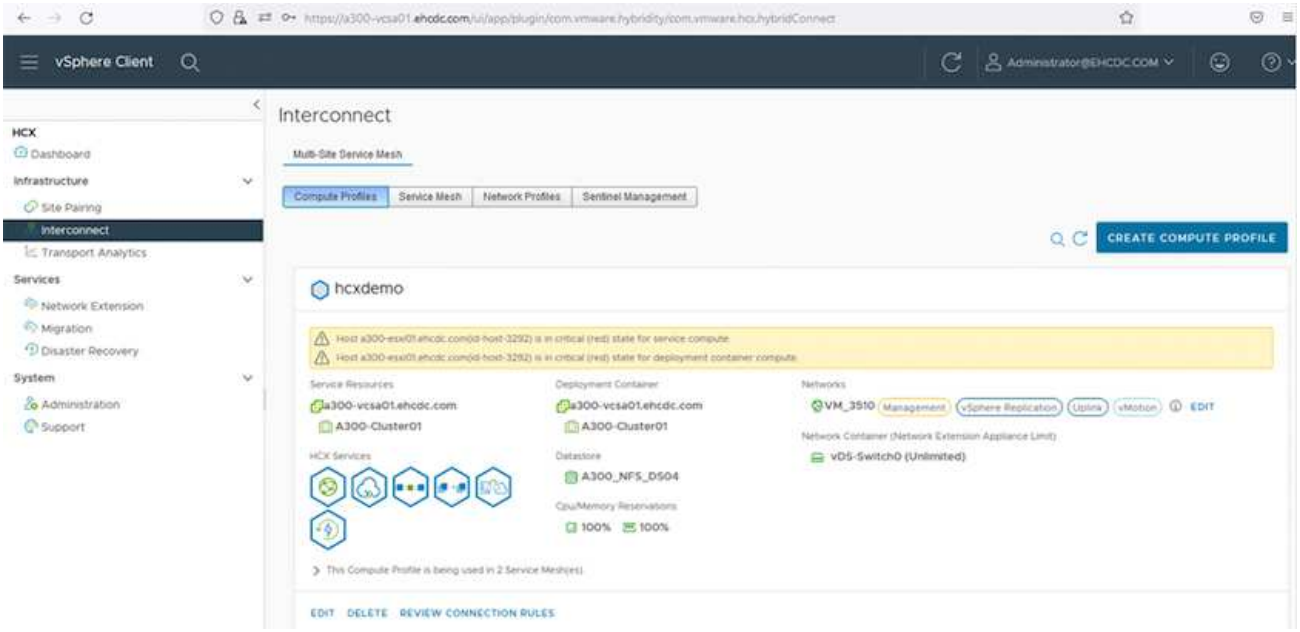
▼ 步骤 **5**：配置网络配置文件、计算配置文件和服务网格

VMware HCX Interconnect (HCX-IX) 设备通过互联网提供安全隧道功能以及与目标站点的专用连接，从而实现复制和基于 vMotion 的功能。互连提供加密、流量工程和 SD-WAN。要创建 HCI-IX 互连设备，请完成以下步骤：

1. 在“基础设施”下，选择“互连”>“多站点服务网格”>“计算配置文件”>“创建计算配置文件”。

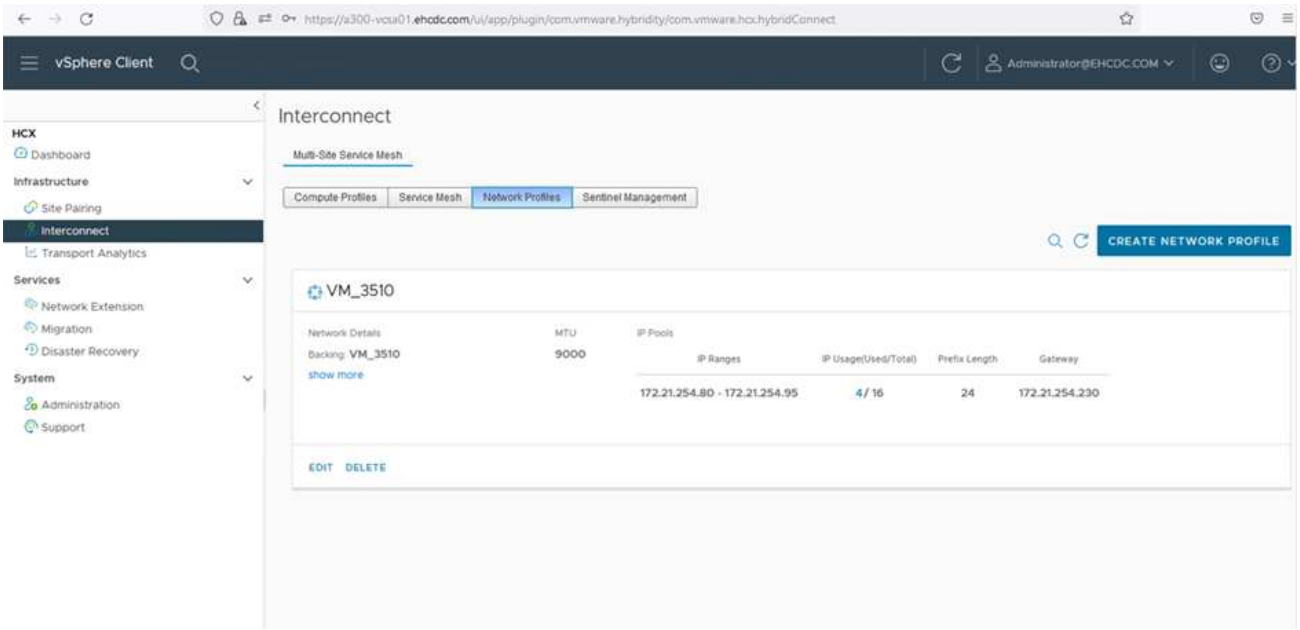
   计算配置文件包含部署互连虚拟设备所需的计算、存储和网络部署参数。他们还指定 VMware 数据中心的哪些部分可供 HCX 服务访问。

   有关详细说明，请参阅 "创建计算配置文件"。



2. 创建计算配置文件后，通过选择多站点服务网格 > 网络配置文件 > 创建网络配置文件来创建网络配置文件。
3. 网络配置文件定义了 HCX 将用于其虚拟设备的一系列 IP 地址和网络。

   这将需要两个或更多 IP 地址。这些 IP 地址将从管理网络分配给虚拟设备。

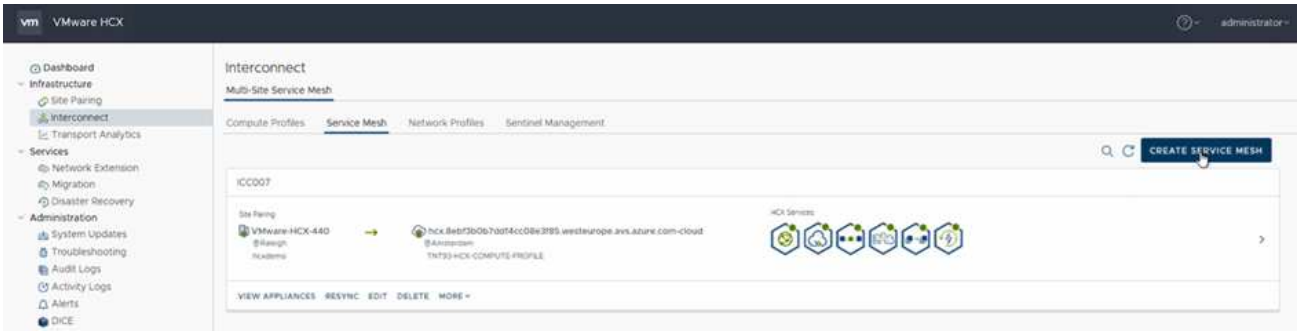


有关详细说明，请参阅 "创建网络配置文件"。

如果您通过互联网连接 SD-WAN，则必须在“网络和安全”部分下保留公共 IP。

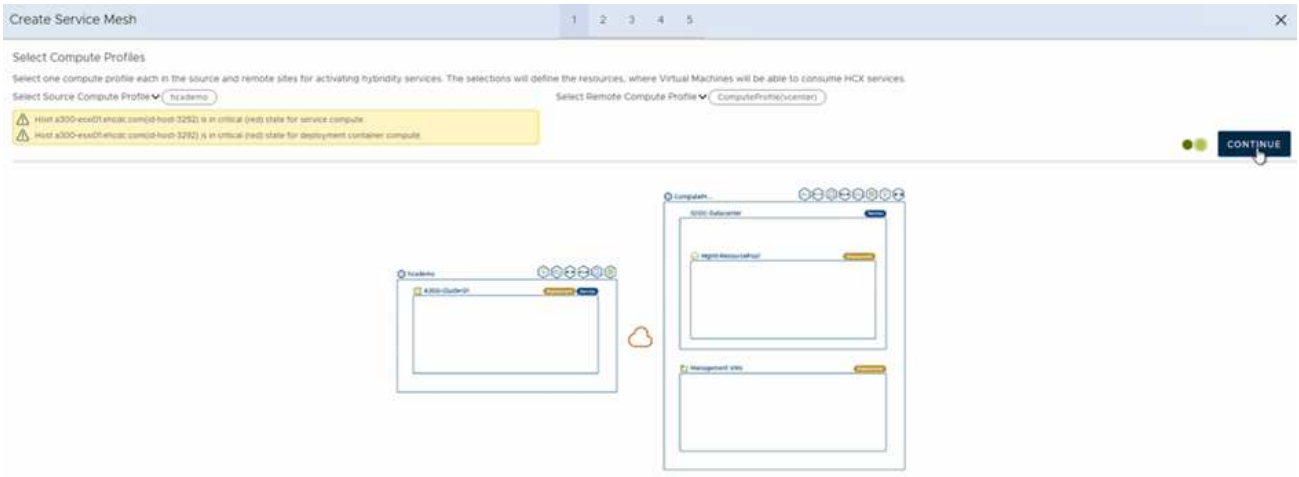
4. 要创建服务网格，请选择“互连”选项中的“服务网格”选项卡，然后选择本地和 VMC SDDC 站点。

   服务网格建立本地和远程计算和网络配置文件对。

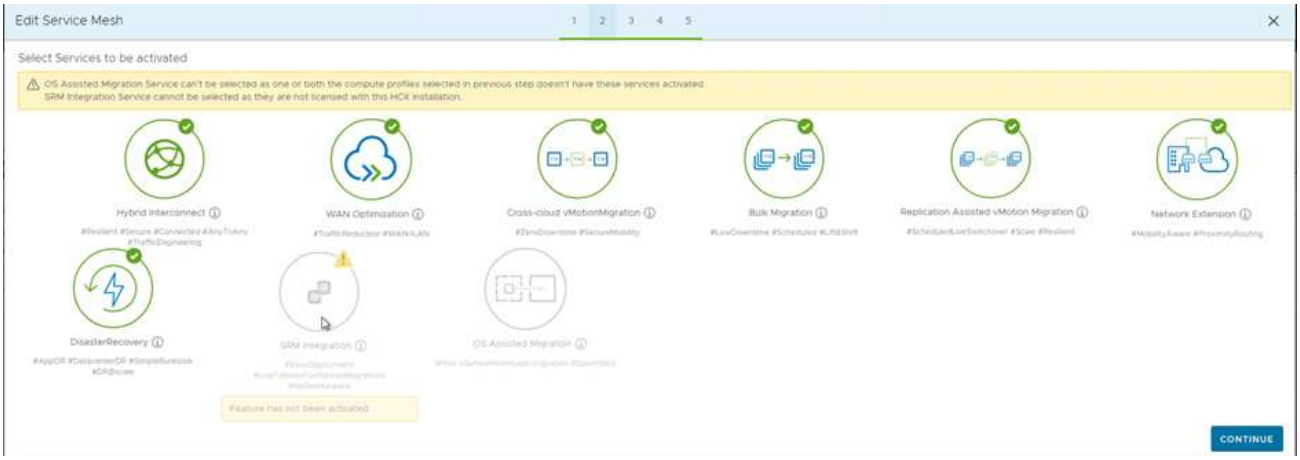


此过程的一部分涉及部署将在源站点和目标站点上自动配置的 HCX 设备，从而创建安全的传输结构。

5. 选择源和远程计算配置文件，然后单击继续。

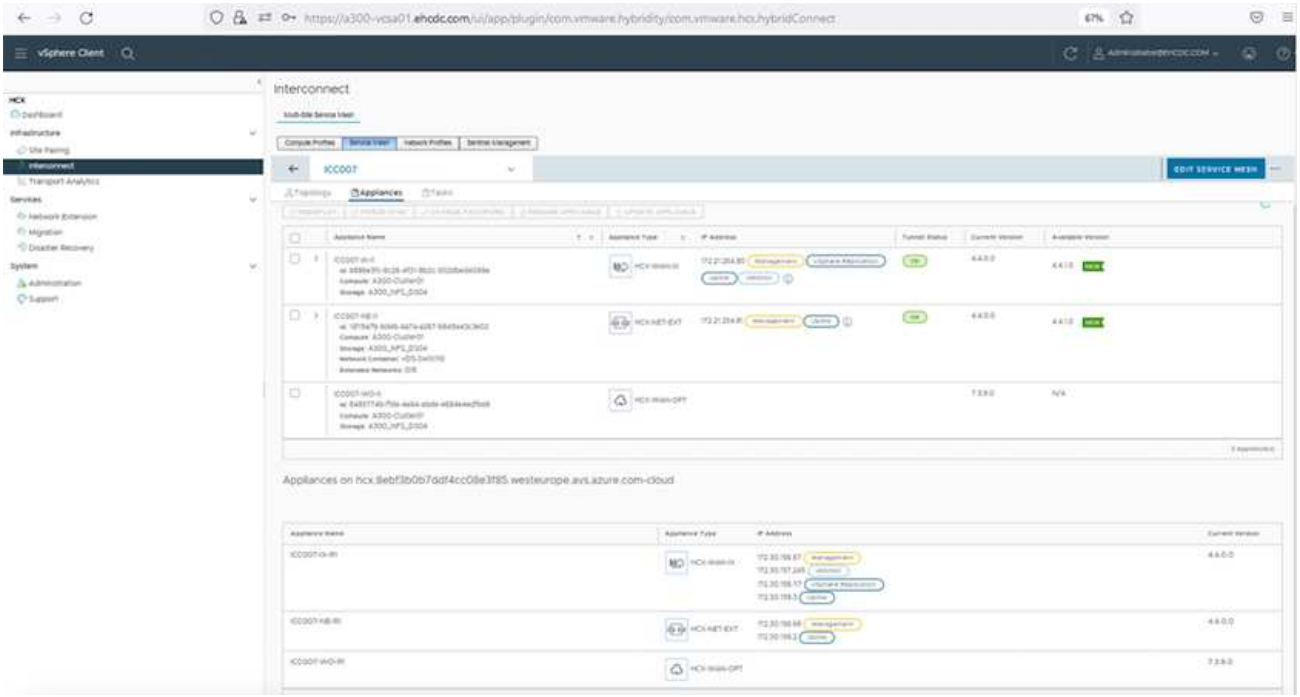


6. 选择需要激活的服务并单击继续。



复制辅助 vMotion 迁移、SRM 集成和 OS 辅助迁移需要 HCX Enterprise 许可证。

7. 为服务网格创建一个名称，然后单击“完成”开始创建过程。部署大约需要 30 分钟才能完成。配置服务网格后，迁移工作负载虚拟机所需的虚拟基础架构和网络已创建。



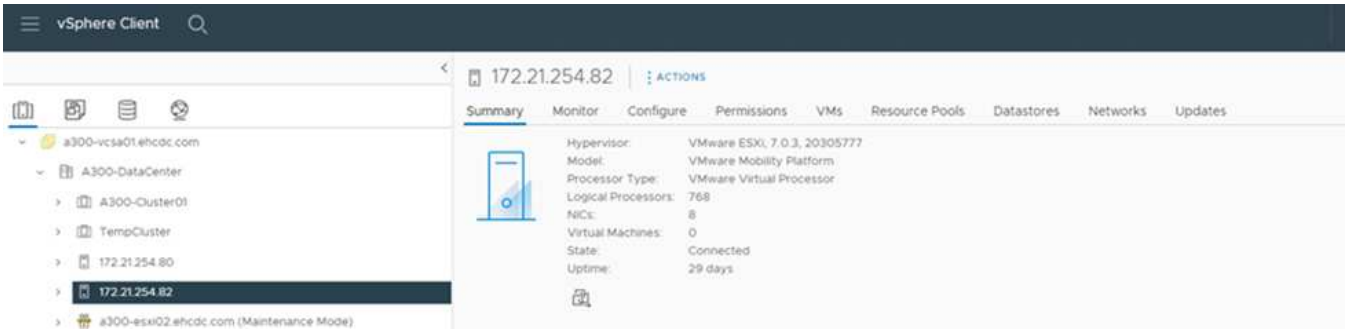
▼ 步骤 **6**：迁移工作负载

HCX 在两个或多个不同的环境（例如本地和 VMC SDDC）之间提供双向迁移服务。可以使用各种迁移技术将应用程序工作负载迁移到 HCX 激活站点和从 HCX 激活站点迁移，例如 HCX 批量迁移、HCX vMotion 、HCX 冷迁移、HCX 复制辅助 vMotion（HCX 企业版提供）和 HCX OS 辅助迁移（HCX 企业版提供）。

要了解有关可用的 HCX 迁移技术的更多信息，请参阅 "VMware HCX 迁移类型"

HCX-IX 设备使用移动代理服务执行 vMotion、Cold 和复制辅助 vMotion (RAV) 迁移。

HCX-IX 设备将移动代理服务添加为 vCenter Server 中的主机对象。此对象上显示的处理器、内存、存储和网络资源并不代表托管 IX 设备的物理虚拟机管理程序上的实际消耗。

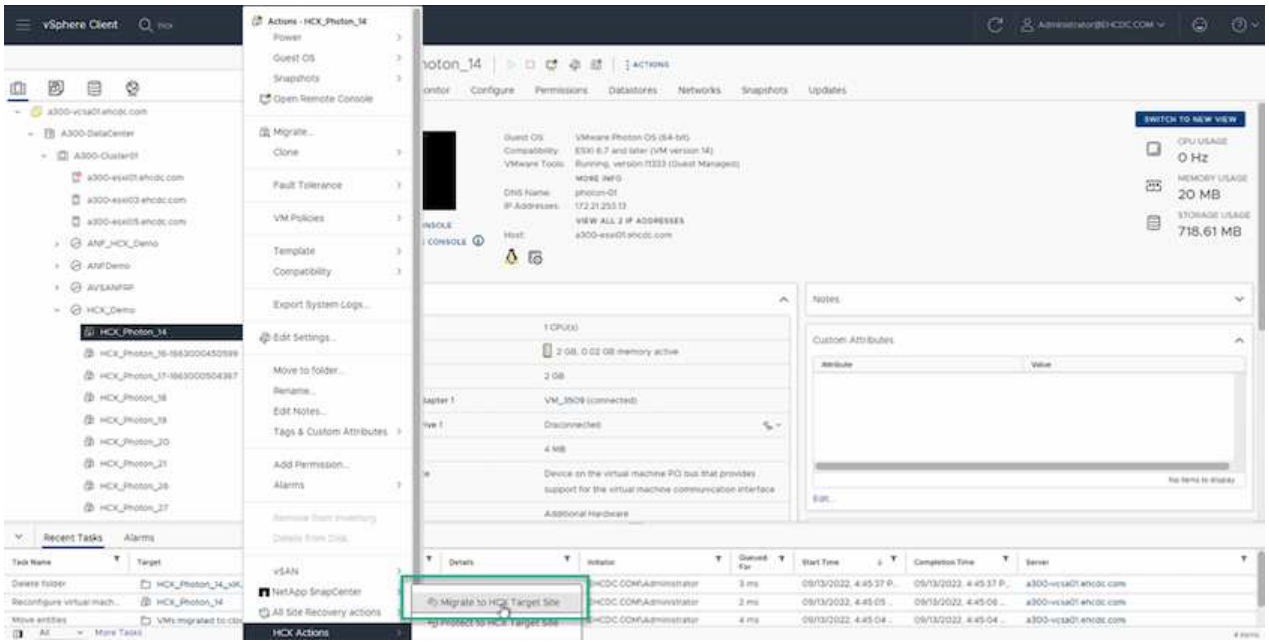


▼ **VMware HCX vMotion**

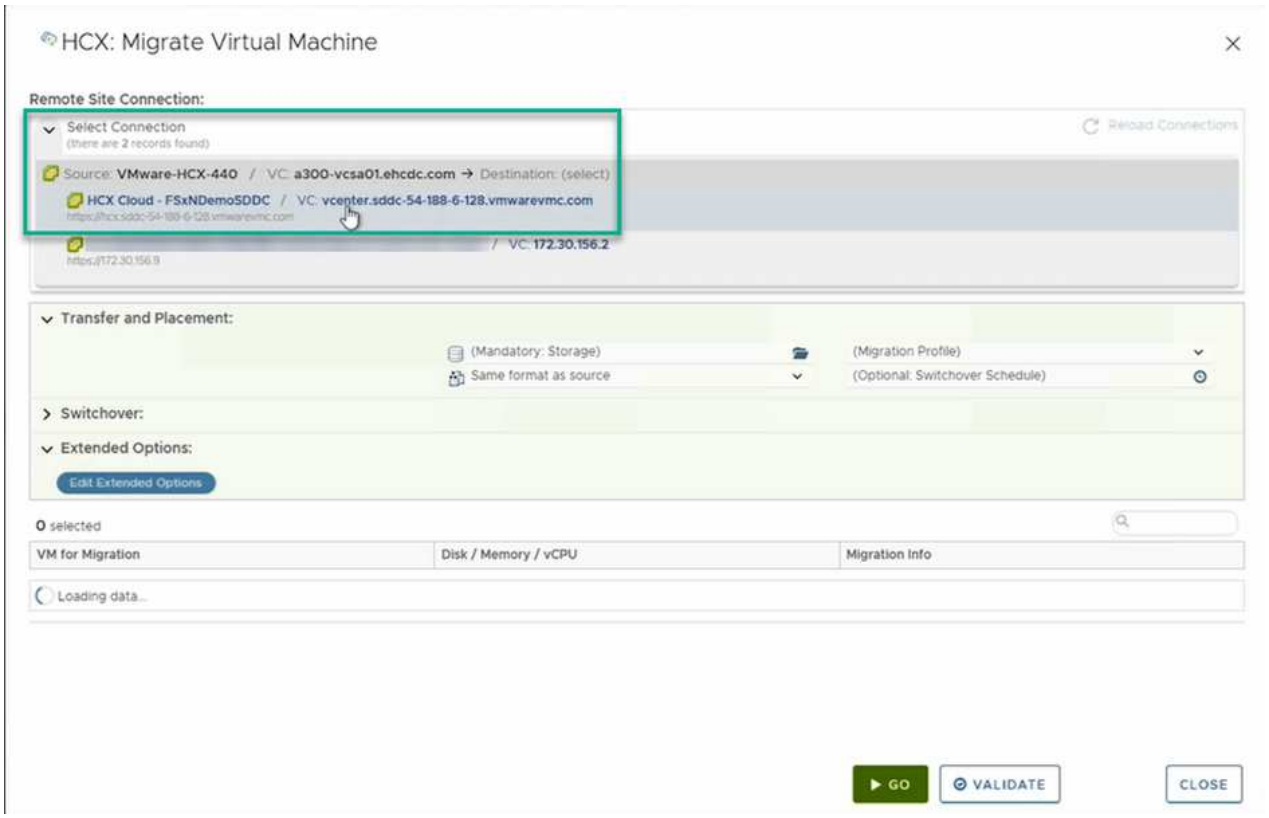
本节介绍 HCX vMotion 机制。此迁移技术使用 VMware vMotion 协议将虚拟机迁移到 VMC SDDC。vMotion 迁移选项用于一次迁移单个 VM 的 VM 状态。此迁移方法期间不会中断服务。

应该实施网络扩展（针对虚拟机所连接的端口组），以便迁移虚拟机而无需更改 IP 地址。

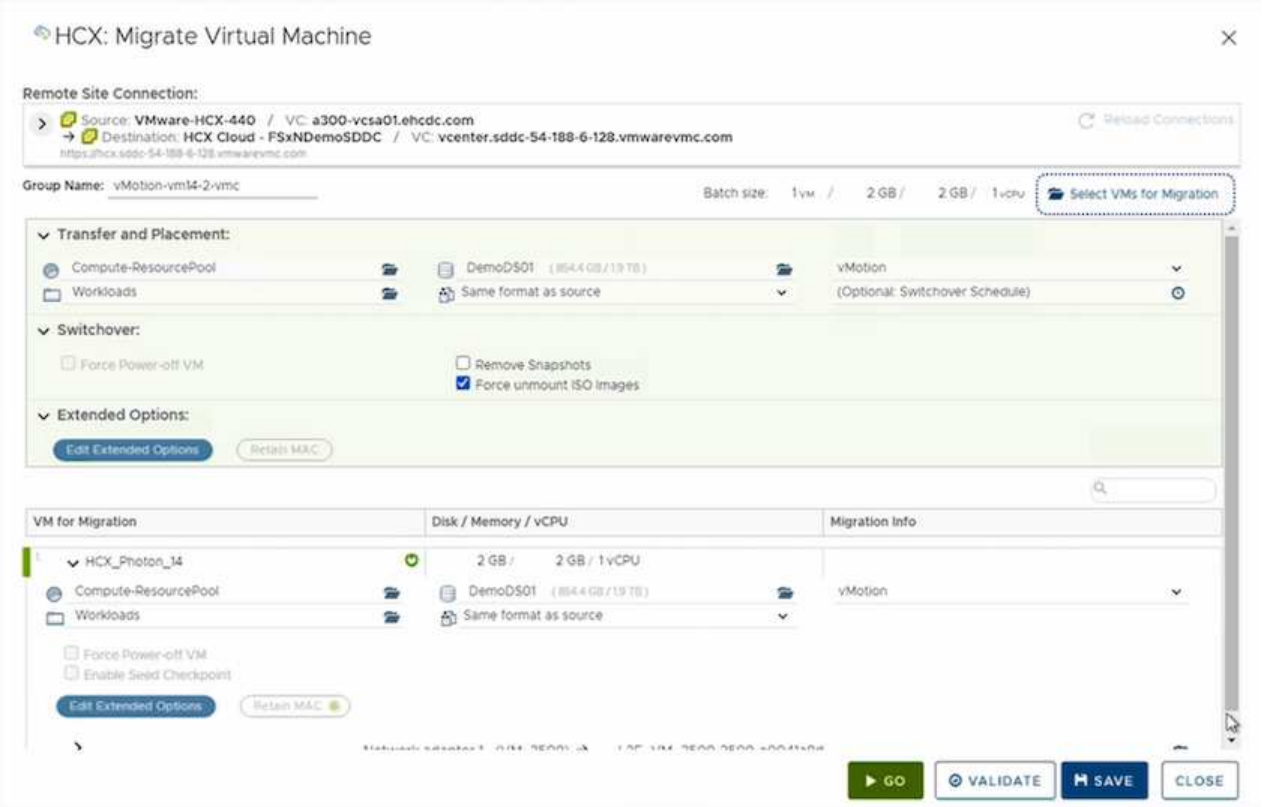
1. 从本地 vSphere 客户端，转到“清单”，右键单击要迁移的虚拟机，然后选择“HCX 操作”>“迁移到 HCX 目标站点”。



2. 在迁移虚拟机向导中，选择远程站点连接（目标 VMC SDDC）。



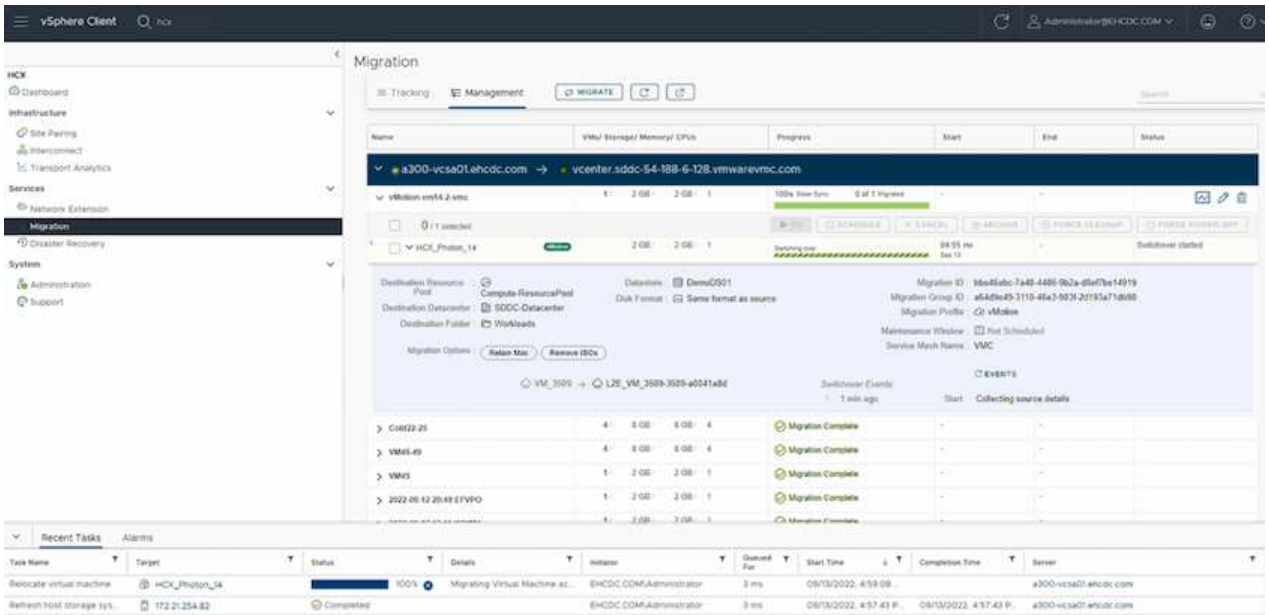
3. 添加组名，并在传输和放置下更新必填字段（集群、存储和目标网络），单击验证。



4. 验证检查完成后，单击“Go”开始迁移。

> vMotion 传输捕获 VM 活动内存、其执行状态、其 IP 地址和其 MAC 地址。有关 HCX vMotion 的要求和限制的更多信息，请参阅 "了解 VMware HCX vMotion 和冷迁移"。

5. 您可以从 HCX > 迁移仪表板监控 vMotion 的进度和完成情况。

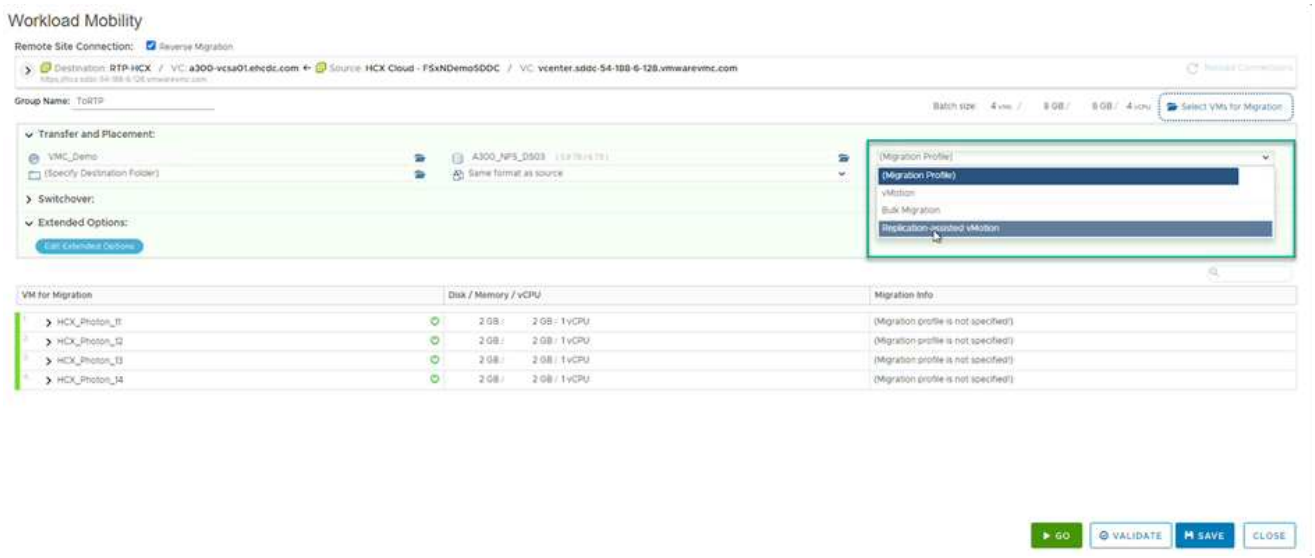


▼ **VMware 复制辅助 vMotion**

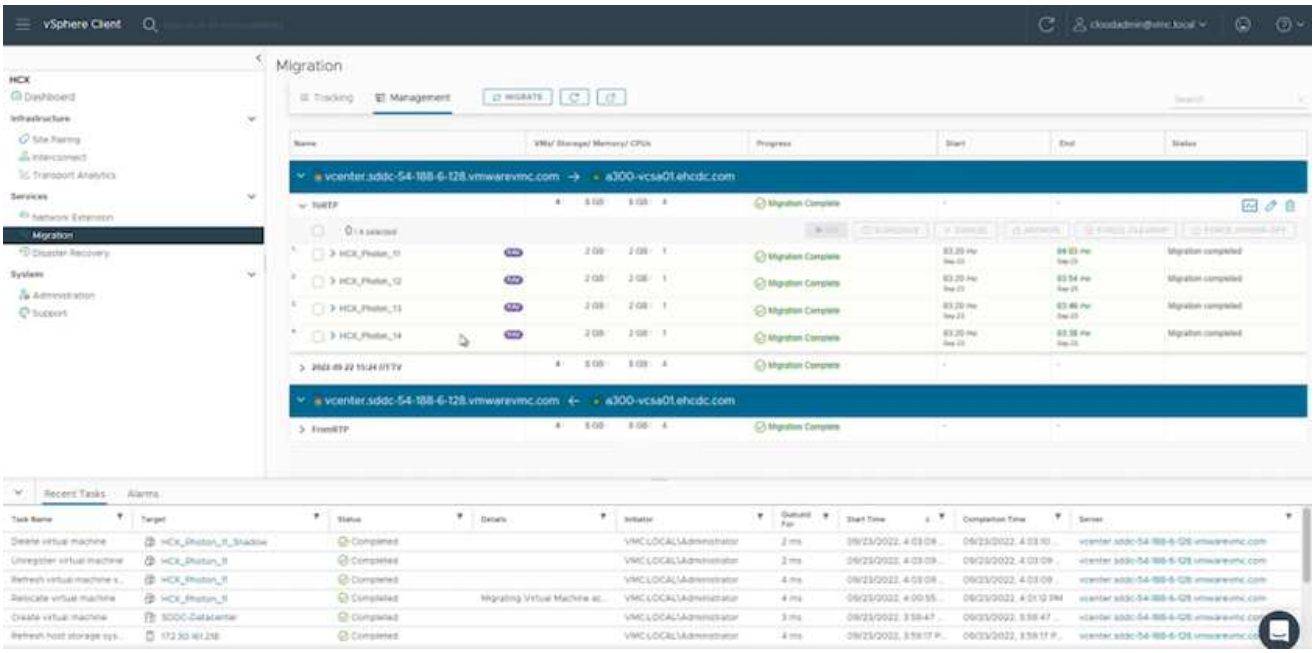
您可能从 VMware 文档中注意到，VMware HCX 复制辅助 vMotion (RAV) 结合了批量迁移和 vMotion 的优

势。批量迁移使用 vSphere Replication 并行迁移多个虚拟机 - 虚拟机在切换期间重新启动。 HCX vMotion 迁移无需停机，但它是在复制组中一次一个虚拟机地连续执行的。 RAV 并行复制虚拟机并保持同步，直到切换窗口。在切换过程中，它一次迁移一个虚拟机，且虚拟机不会停机。

以下屏幕截图显示了作为复制辅助 vMotion 的迁移配置文件。



与少量虚拟机的 vMotion 相比，复制的持续时间可能会更长。使用 RAV，仅同步增量并包含内存内容。以下是迁移状态的屏幕截图 - 它显示了迁移的开始时间相同，而每个虚拟机的结束时间不同。



有关 HCX 迁移选项以及如何使用 HCX 将工作负载从本地迁移到 VMware Cloud on AWS 的更多信息，请参阅 "VMware HCX 用户指南"。

VMware HCX vMotion 需要 100Mbps 或更高的吞吐量能力。

目标 VMC FSx ONTAP数据存储必须具有足够的空间来容纳迁移。

结束语

无论您的目标是全云还是混合云，以及驻留在本地任何类型/供应商存储上的数据， Amazon FSx ONTAP和 HCX 都提供了部署和迁移工作负载的绝佳选择，同时通过使数据要求无缝连接到应用程序层来降低 TCO。无论用例如何，选择 VMC 和 FSx ONTAP数据存储都可以快速实现云优势、跨本地和多个云的一致基础架构和操作、工作负载的双向可移植性以及企业级容量和性能。使用 VMware vSphere 复制、VMware vMotion 甚至 NFC 复制来连接存储和迁移虚拟机所采用的流程和程序相同。

总结

该文件的要点包括：

- 您现在可以将Amazon FSx ONTAP用作 VMC SDDC 的数据存储。
- 您可以轻松地将数据从任何本地数据中心迁移到使用 FSx ONTAP数据存储运行的 VMC
- 您可以轻松扩大或缩小 FSx ONTAP数据存储以满足迁移活动期间的容量和性能要求。

在哪里可以找到更多信息

要了解有关本文档中描述的信息的更多信息，请参阅以下网站链接：

- VMware Cloud 文档

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSx ONTAP文档

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX 用户指南

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

适用于 **AWS/EVS** 的**NetApp**

将 **FSx ONTAP**挂载为 **EVS** 的外部数据存储

如何将**Amazon FSx for NetApp ONTAP**挂载为 **Amazon Elastic VMware Service** 的外部数据存储

本文档将介绍创建 FSx for ONTAP文件系统并将其附加为互联网小型计算机系统接口 (iSCSI) 或网络文件系统 (NFS) 数据存储以供 Amazon EVS 使用的具体步骤。

简介

拥有现有本地 VMware 投资的组织正在寻求高效且经济高效的方式，通过在 AWS 上迁移、爆发、扩展或保护（备份、灾难恢复）副本来实现其部署的现代化，但他们面临着多项挑战。随着 Amazon Elastic VMware Service (Amazon EVS) 的发布，现在有了原生的 AWS 服务，可以直接在 Amazon Virtual Private Cloud (VPC) 中运行 VMware Cloud Foundation (VCF)。

Amazon EVS 可以将现有的 VCF 部署扩展到 AWS，在高峰使用期间爆发到 AWS 以扩展性能，并在 AWS 上完全运行 VCF 工作负载以促进现代化、数据中心退出、整合和其他使用案例。

尽管 Amazon EVS 提供了强大的优势，但默认的超融合架构将计算和存储结合在一起，从而阻止根据业务需求独立扩展其中一个或另一个。在当今以数据为中心的世界中，许多组织的存储需求高于计算需求。然而，在 VMware 超融合架构中，存储资源与计算资源是结合在一起的。这意味着只能通过添加永远不会使用的计算主机来实现存储扩展。这种情况会大大增加成本，尤其是在存储繁重的工作负载中。

为了解决这个问题，AWS 和NetApp提供Amazon FSx for NetApp ONTAP （FSx for ONTAP）作为 Amazon EVS 的外部存储服务。 FSx for ONTAP是一种 AWS 原生存储服务，可提供NetApp ONTAP软件的高性能、数据弹性和成本效益功能。通过使用 FSx for ONTAP作为外部存储，Amazon EVS 用户可以独立扩展计算和存储资源，从而实现最佳总体拥有成本 (TCO)。

概述

本文档将介绍创建 FSx for ONTAP文件系统并将其附加为互联网小型计算机系统接口 (iSCSI) 或网络文件系统 (NFS) 数据存储以供 Amazon EVS 使用的具体步骤。

本指南的目的

本指南提供了有关如何为 Amazon EVS 设置 FSx for ONTAP数据存储的说明，以及最佳实践、可支持性要求、大小考虑因素和其他信息，以帮助您规划、设计和实施集成。

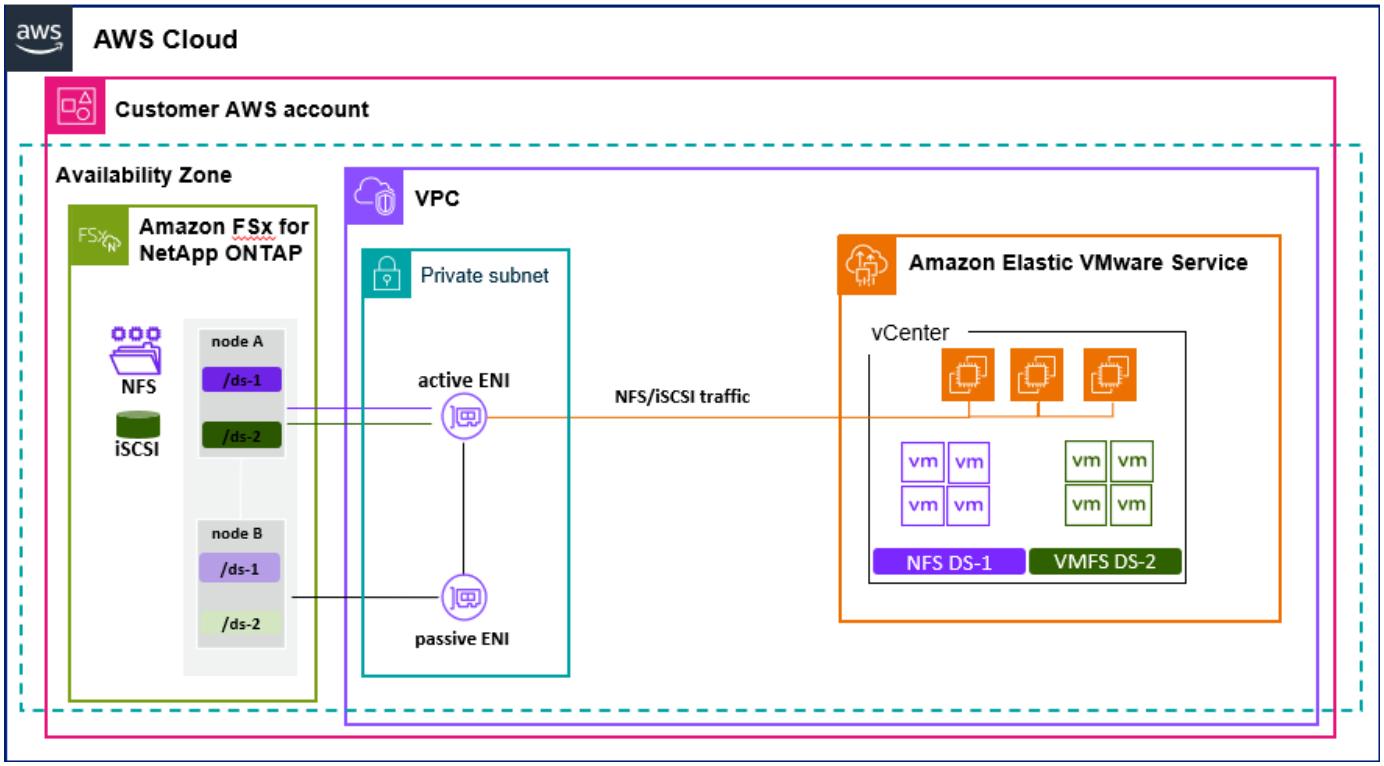
受众

本教程适用于熟悉 VMware vSphere、Amazon EVS、AWS 控制台和 FSx for ONTAP 的云架构师和云管理员。

高级架构

在本节中，我们将概述使用 FSx for ONTAP作为 Amazon EVS 数据存储的解决方案架构。

下面您可以看到 AWS VPC 内具有 Amazon EVS 环境的 FSx for ONTAP数据存储区的架构高级视图。



使用 **FSx for ONTAP**作为 **NFS** 数据存储库的部署过程

本节将展示如何将 FSx for ONTAP部署为 NFS 数据存储区的步骤。部署 iSCSI 数据存储区的步骤将在下一节中详细介绍。

高级部署步骤

部署 FSx for ONTAP文件系统作为 Amazon EVS 的 NFS 数据存储并在两种服务之间建立连接将包括以下步骤：

- 在 Amazon EVS VCF 环境所在的同一 VPC 中设置 FSx for ONTAP文件系统。
- 验证安全组和路由表。
- 连接 FSx for ONTAP存储卷以用作 Amazon EVS 的 NFS 数据存储。

前提条件

在开始将 FSx for ONTAP设置为 Amazon EVS 的 NFS 数据存储之前，应满足以下先决条件：

- Amazon EVS 虚拟化环境。有关如何执行此操作的更多信息，请参阅"Amazon EVS 入门指南"。
- 使用适当的 SSD 存储容量、预配置的 IOPS 和吞吐量为ONTAP创建单可用区 (AZ) FSx。
- 为了获得最佳性能，请将 FSx for ONTAP文件系统放置在与 Amazon EVS 实例相同的 VPC 内。请注意，当 FSx for ONTAP部署在不同 VPC 中时，也支持 VPC Peering。
- 根据性能要求，选择单可用区 FSx for ONTAP文件系统所需的正确 IOPS 和吞吐量。看"FSx for ONTAP 的性能规格详情"了解每个可用选项提供的吞吐量和 IOPS。

> 在本指南中，我们将在与服务访问子网相同的子网中部署 FSx for ONTAP文件系统。

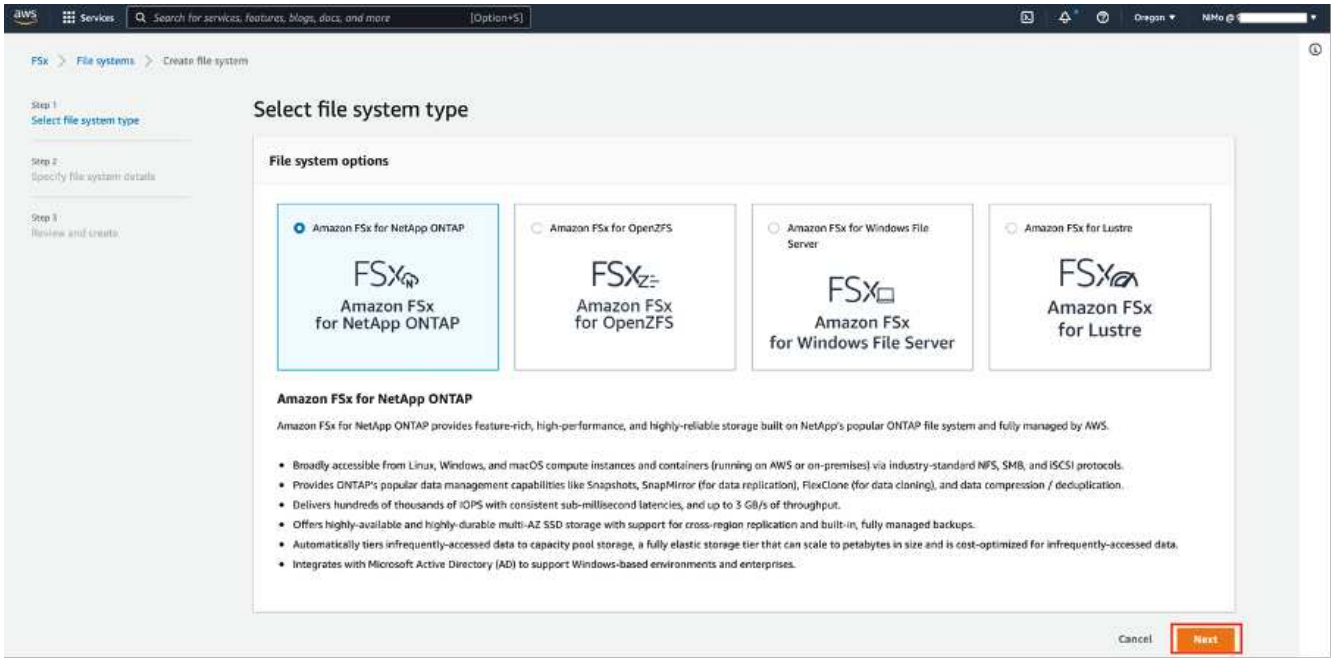
在 VPC 中部署 Amazon EVS 虚拟化环境后，您可以继续设置将用作 NFS 数据存储的单可用区 FSx for ONTAP文件系统。

> 您的 FSx for ONTAP文件系统应部署在与 Amazon EVS SDDC 相同的 AZ 中。

创建 **FSx for ONTAP**文件系统

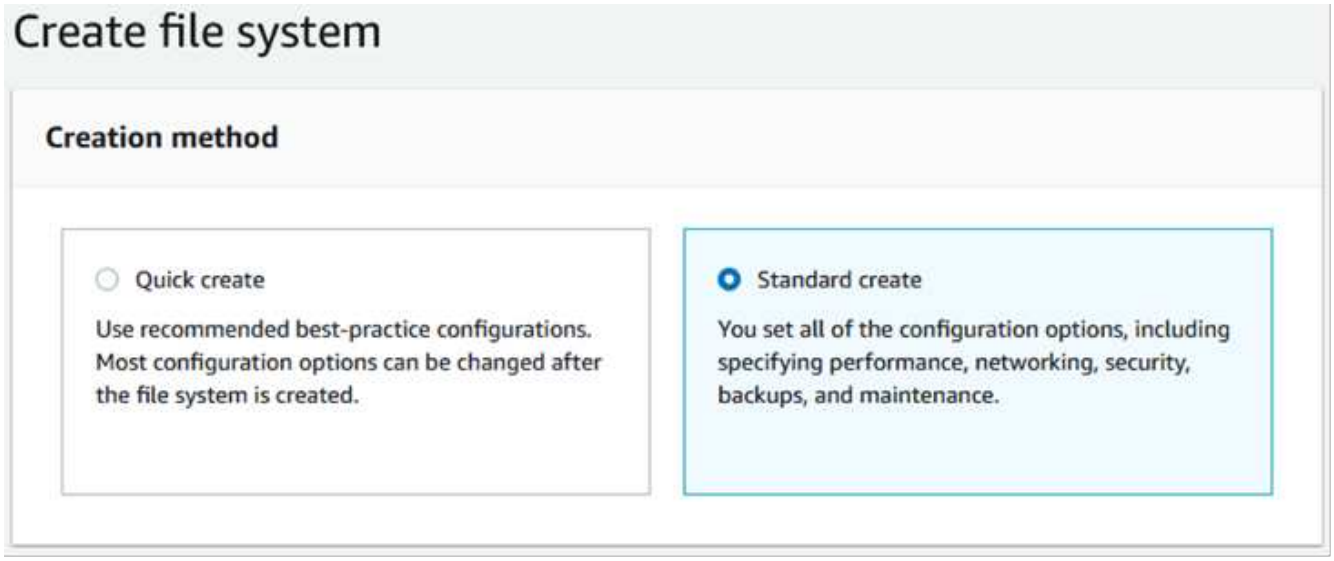
以下步骤将向您展示如何配置和挂载 FSx for ONTAP文件系统：

1. 前往Amazon FSx控制台 `https://console.aws.amazon.com/fsx/`使用您的互联网浏览器并使用您的凭据登录。
2. 在控制台中，选择创建文件系统。这将启动安装向导来创建 FSx for ONTAP文件系统。
3. 首先，选择文件系统类型。从可用的文件系统选项中，选择“Amazon FSx for NetApp ONTAP”，然后单击“下一步”按钮继续。

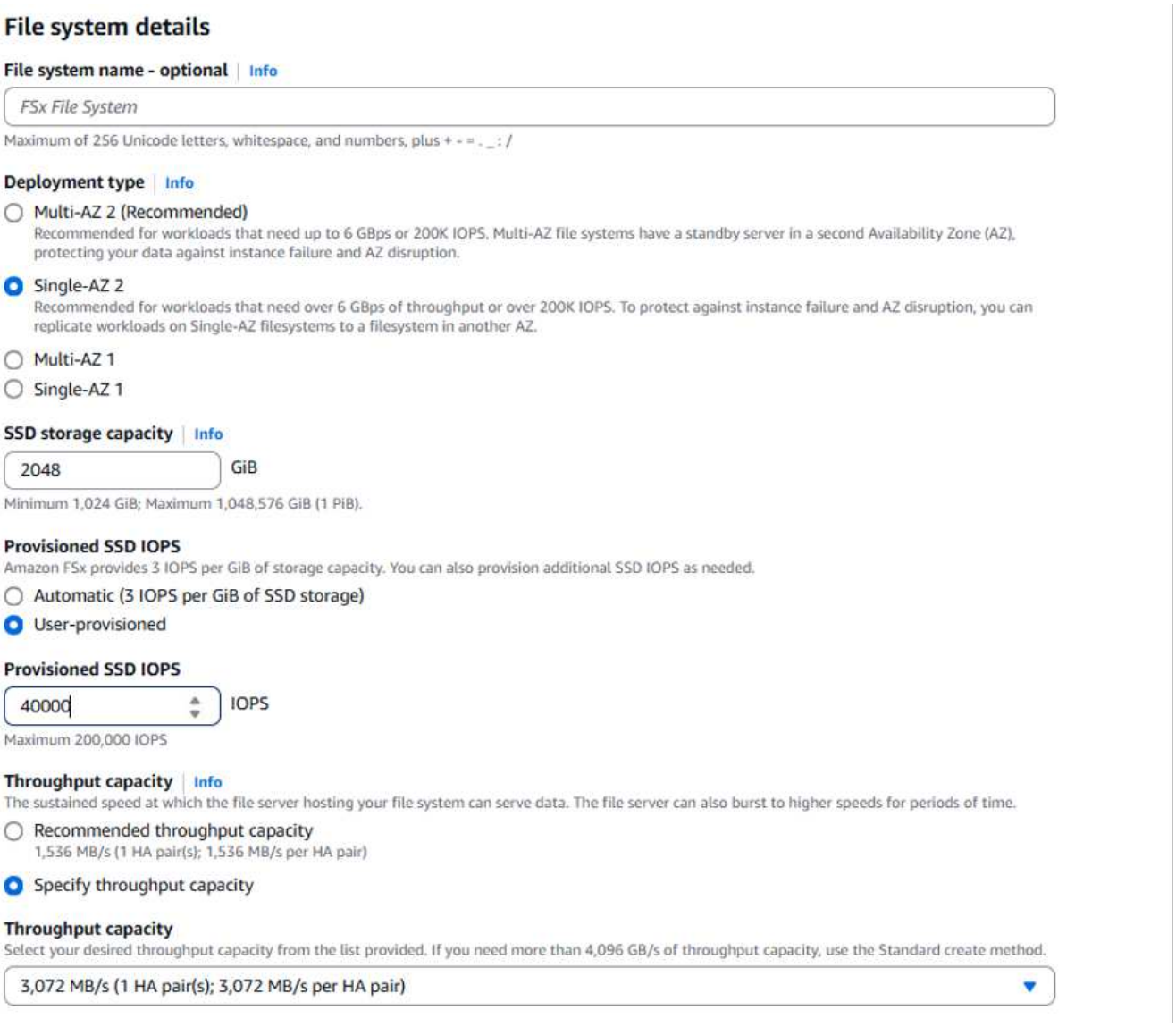


4. 您将可以在“快速创建”和“标准创建”选项之间进行选择。快速创建提供预定义配置，标准创建允许您定义自己的配置。

   选择“标准创建”选项。

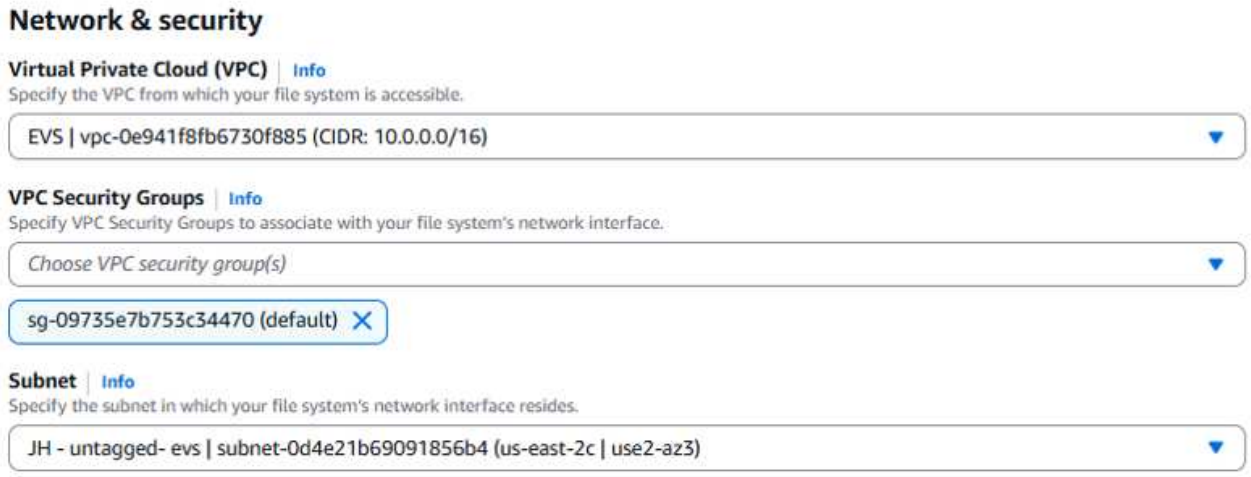


   您现在将进入标准创建文件系统设置向导。在文件系统详细信息页面中，选择并输入如下图所示的相同信息：



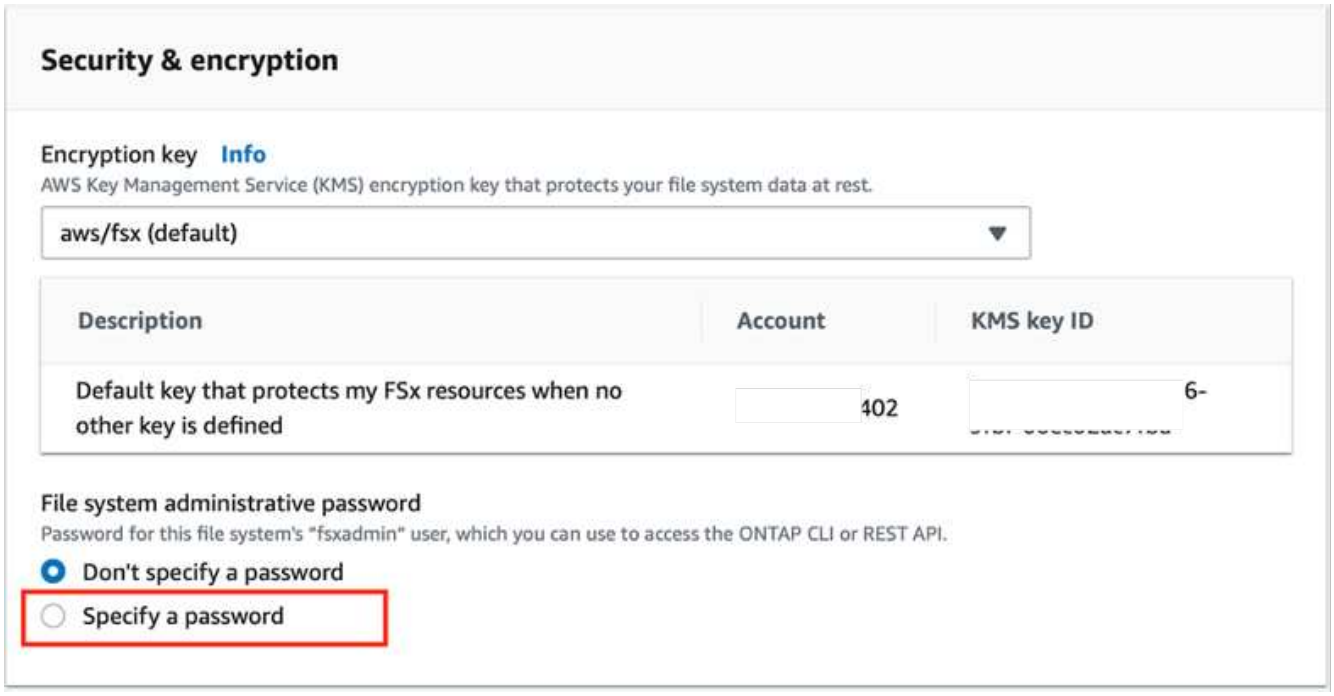
5. 向下滚动到标有“网络和安全”的部分。在本节中，您将设置子网和 VPC 的详细信息。为了本指南的目的，我们从下拉菜单中选择了“EVS-VPC”，并选择服务访问子网（未标记的 VLAN）作为 EVS 虚拟环境的子网。

> 该子网可以是 VPC 中任何未标记的私有子网。只要配置了正确的路由，它也可以位于通过 VPC Peering 连接的不同 VPC/子网中。

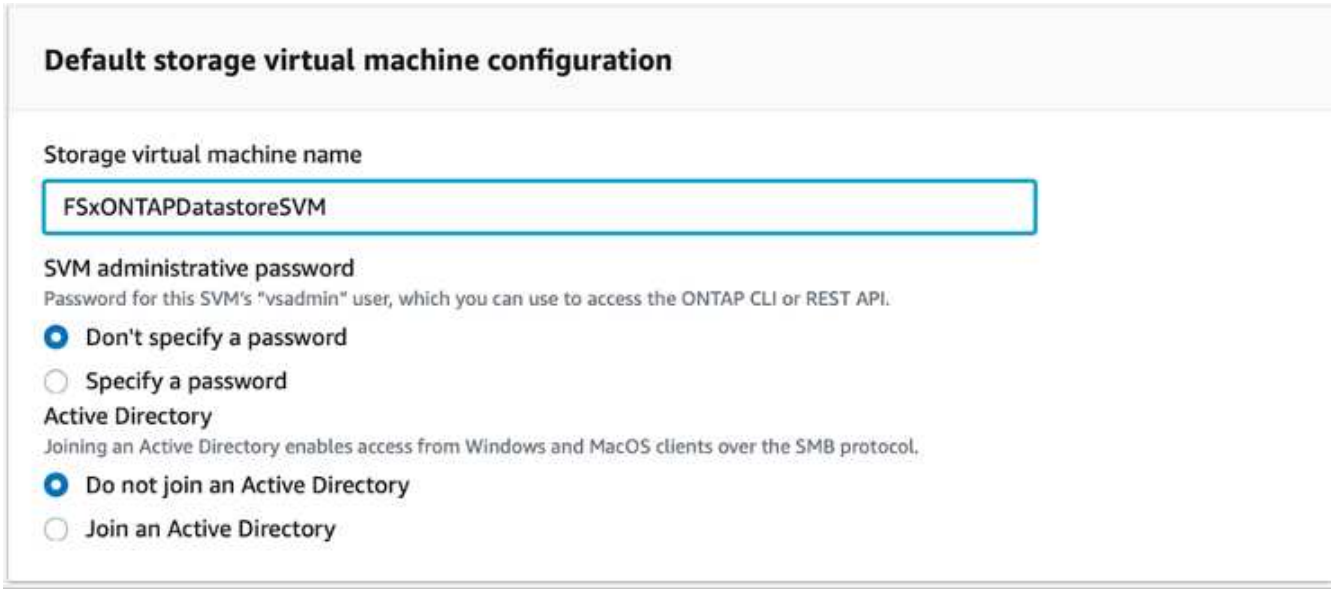


6. 向下滚动，您会找到“安全和加密”部分。在这里，从下拉菜单中选择加密密钥。这些密钥由 AWS 密钥管理服务 (AWS KMS) 提供，并将保护 FSx for ONTAP文件系统中的静态数据。

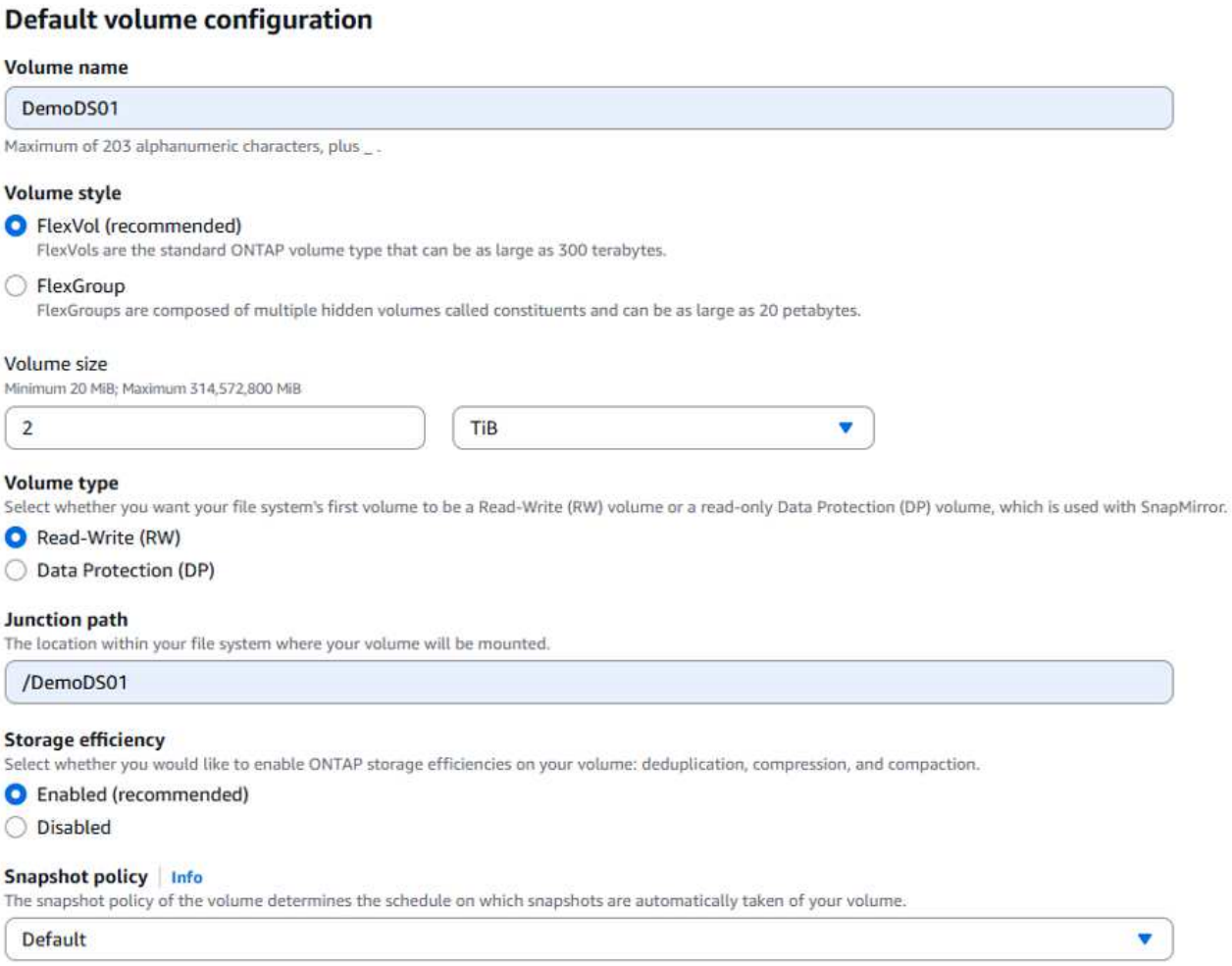
   接下来，在“文件系统管理密码”设置中，为将管理文件系统的 fsxadmin 用户指定一个唯一的密码。



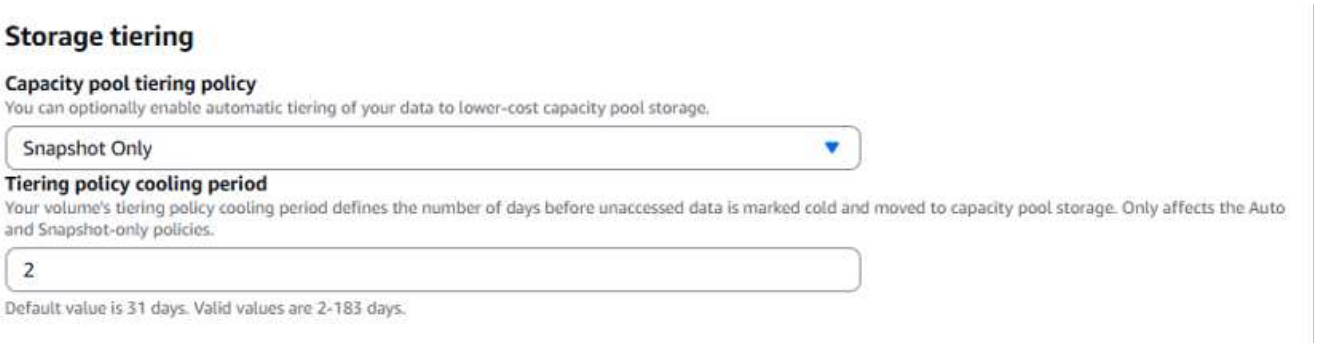
7. 接下来，您将向下滚动到标题为“默认存储虚拟机配置”的部分。在这里，您需要为存储虚拟机 (SVM) 提供一个名称。



8. 接下来，向下滚动到标题为“默认卷配置”的部分。在这里您将为卷提供名称并设置卷大小。卷协议应为 NFS v3（默认启用）。单击该选项可启用存储效率功能（压缩、重复数据删除和压缩），以减少整体存储使用量和成本。



9. 对于存储分层选项，从下拉菜单中选择“仅快照”并设置分层策略冷却期。默认值为 31 天，但对于此示例，我们设置了两天的冷却期。

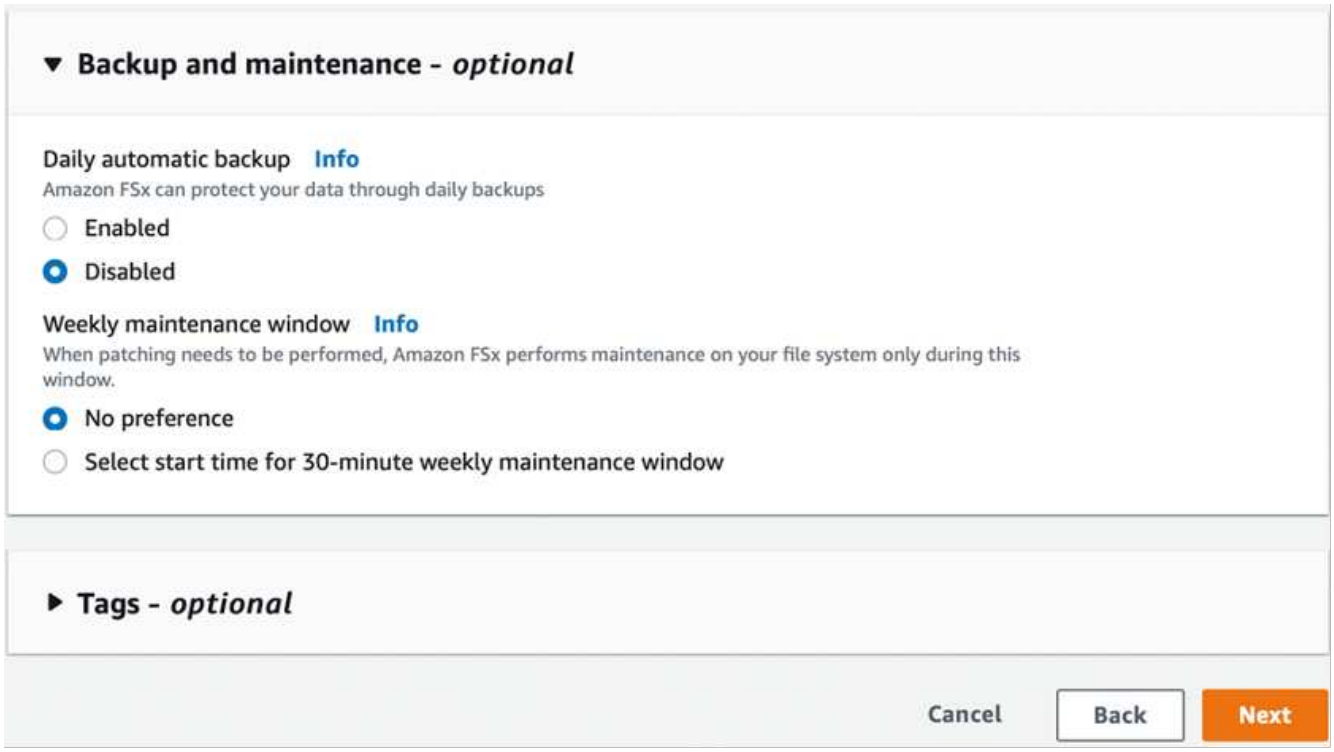


10. 创建卷后，使用ONTAP命令行界面 (ONTAP CLI) 修改以下参数：

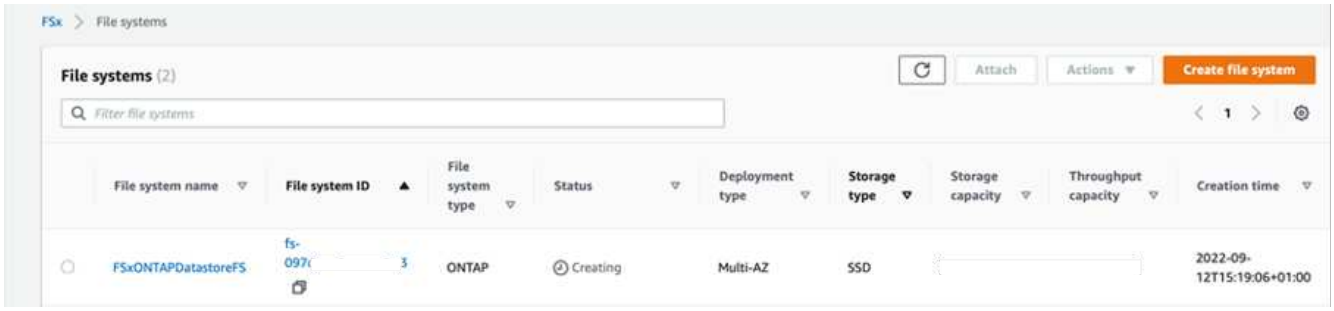
环境	配置
数量保证	无（精简配置）
部分储备	0%
snap_reserve	0%
自动调整大小	grow_shrink
存储效率	已启用
卷分层策略	仅快照
访问时间更新（-atime-update）	False
最小预读（-min-readahead）	False
Snapshot 策略	无

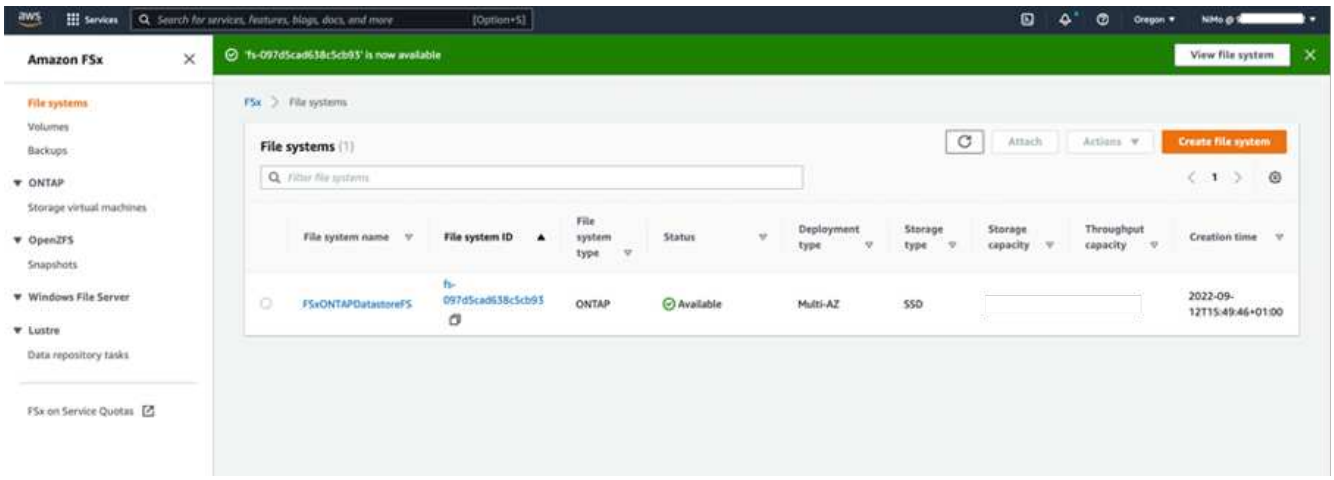
11. 在可选的“备份和维护”步骤中，禁用每日自动备份并为每周维护窗口选择“无首选项”。

    完成后单击“下一步”。



12. 现在，您将获得按照前面步骤设置的整个文件系统配置的审查。检查所有参数无误后，点击“创建文件系统”按钮完成设置。

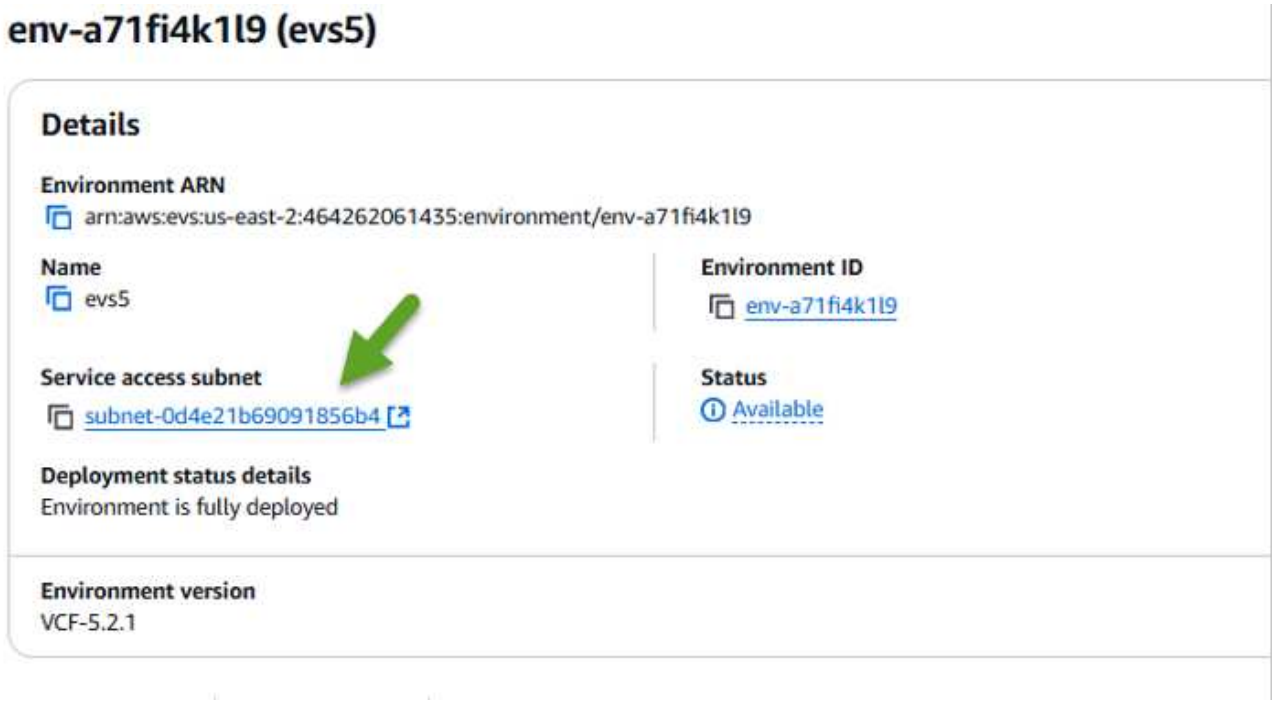




要创建额外的 FSx for ONTAP文件系统，您可以按照上面详述的步骤操作，根据需要调整影响性能和磁盘容量的值。要了解有关 FSx for ONTAP性能选项的更多信息，请参阅"此文档页面"。

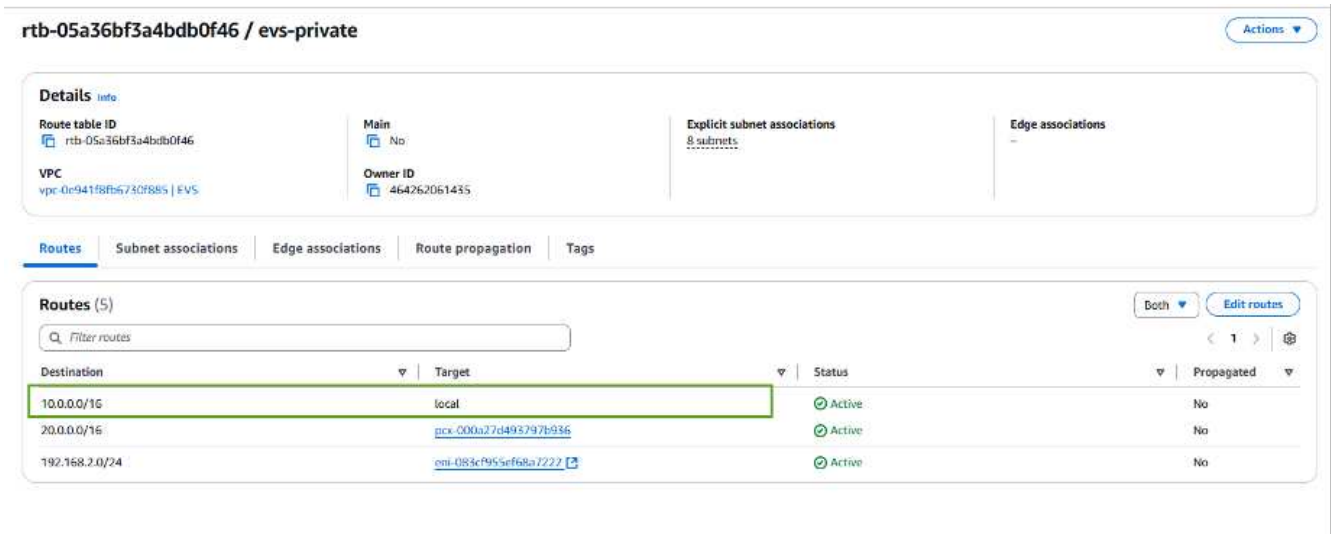
验证 VPC 和 SDDC 路由和安全组对于确保 Amazon EVS 虚拟化环境和 FSx for ONTAP文件系统组件能够正常协同工作非常重要。

1. 浏览到 Elastic VMware 服务 > 虚拟化环境 > [您的 Amazon EVS 环境] 并选择服务访问子网，如下方绿色箭头所示：

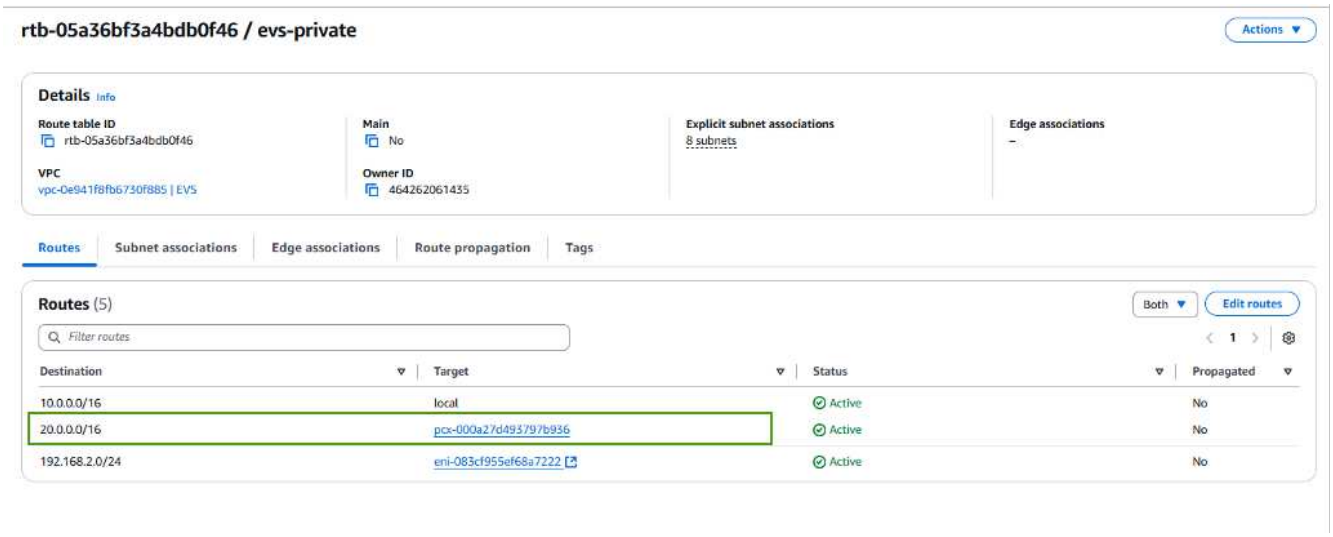


2. 这将打开子网面板。在此面板上找到路线表并单击它。

   在此示例中，FSxN ONTAP文件系统与 Amazon EVS VCF 环境位于同一 VPC 中，因此默认路由就足够了。



   如果 FSx for ONTAP文件系统位于不同的 VPC 中，则检查是否已添加至该 VPC 的路由。在此示例中，已添加 VPC Peering 到 FSx for ONTAP系统所在 VPC 的路由。

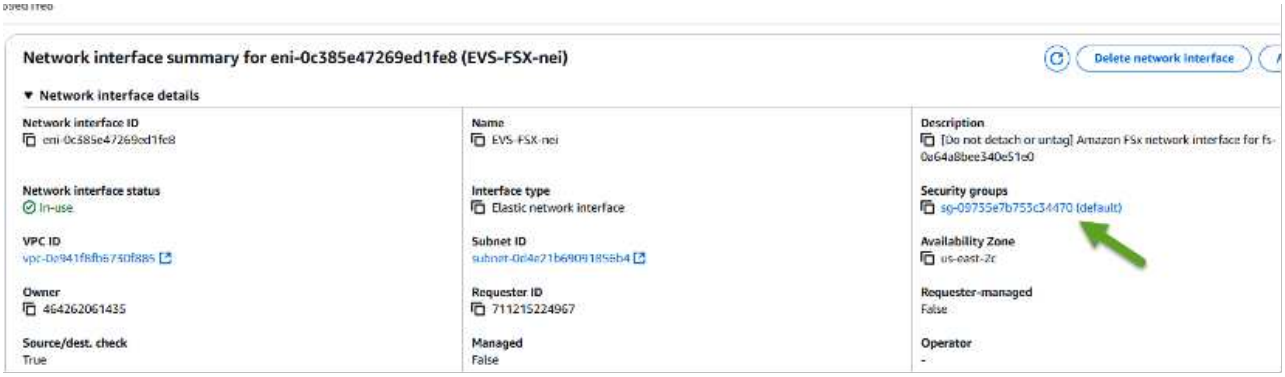


3. 接下来，您需要检查连接到 FSx for ONTAP文件系统的安全组（即连接到弹性网络接口 (ENI) 的安全组）是否允许访问 NFS 端口。

   有关 NFS 和 iSCSI 协议端口的完整列表，请参阅链接： https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html ://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]使用 Amazon VPC 文档进行文件系统访问控制]。

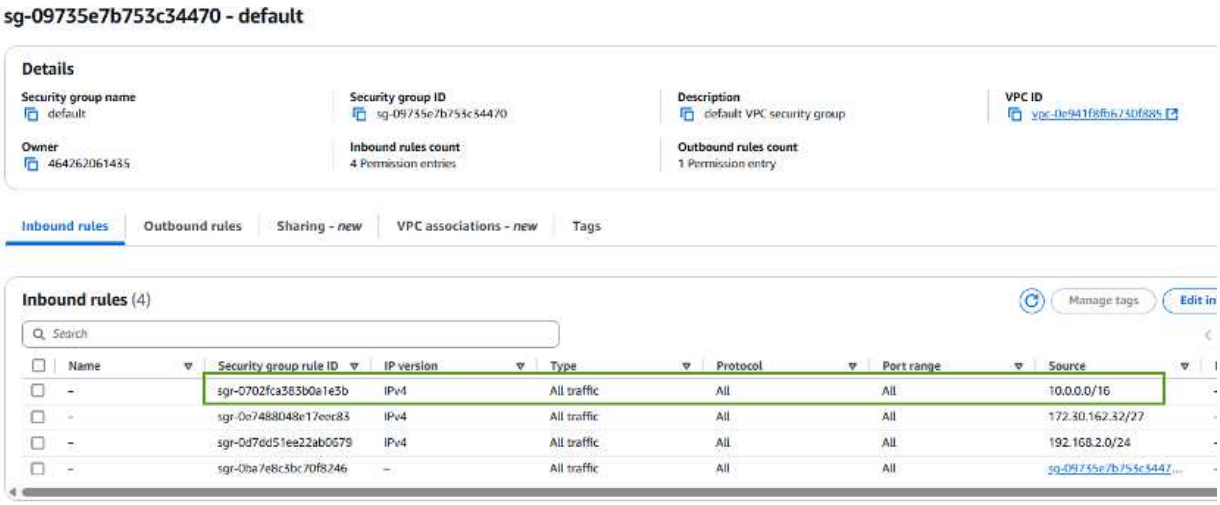
   要验证您的 FSx for ONTAP文件系统是否与安全组关联：

   a. 在 AWS 控制台中，导航到 FSx > 文件系统 > [您的 FSx for ONTAP文件系统]。
   b. 在网络和安全选项卡中，单击 ENI。
   c. 找到网络接口详细信息下列出的与 ENI 关联的安全组（如下图中的绿色箭头所示）。



   d. 验证端口。在以下屏幕所示的示例中，所有流量都被允许。但是，您可以将其限制为仅限 NFS 端口。以下是端口列表：

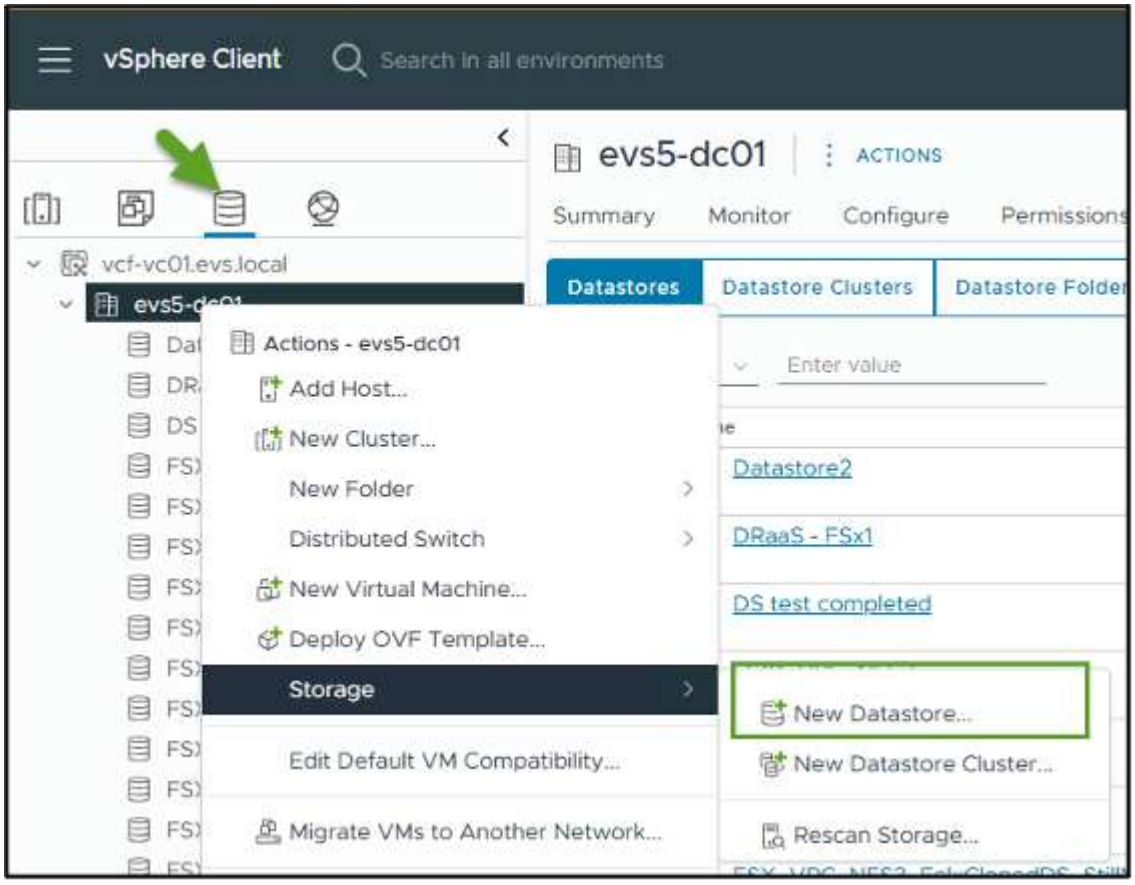
      - 端口 111 TCP：端口映射器，用于协商在 NFS 请求中使用哪些端口。
      - 端口 635 TCP：Mountd，用于接收传入的挂载请求。
      - 端口 2049 TCP：NFS，用于处理 NFS 流量。
      - 端口 4045 TCP：网络锁管理器 (NLM)，处理锁请求。
      - 端口 4046 TCP：网络状态监视器 (NSM)，当服务器重新启动以进行锁管理时，它会发送 NFS 客户端通知。



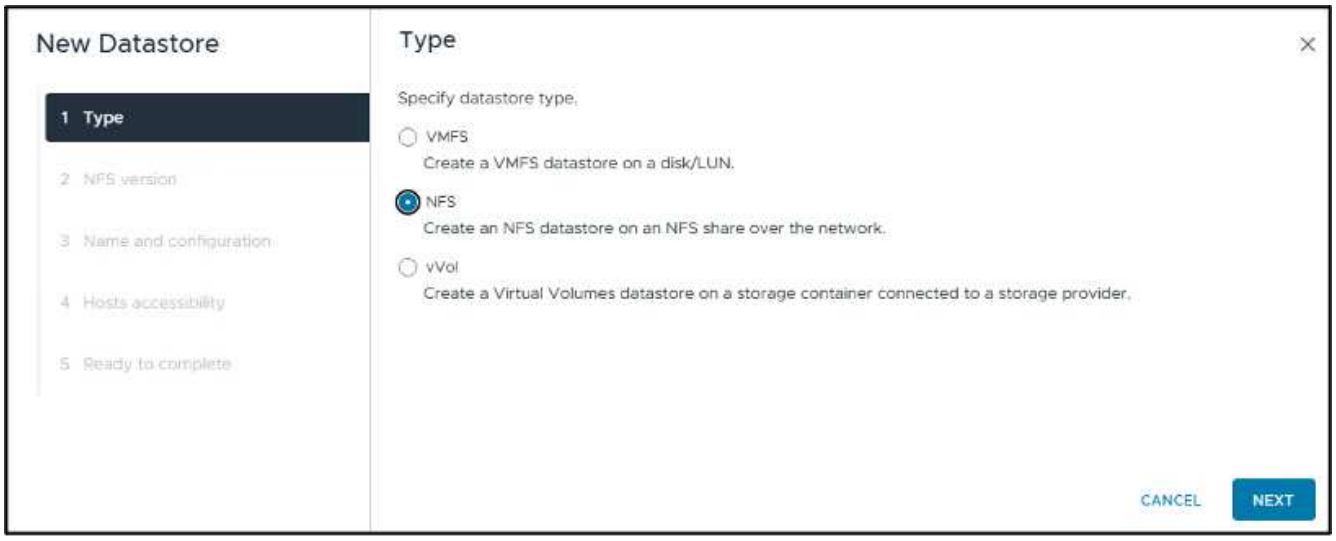
将 **FSx for ONTAP NFS** 卷附加到 **Amazon EVS** 以用作数据存储

现在您的 FSx for ONTAP文件系统已配置完毕，并且所有正确的连接参数都已验证，接下来就可以将 FSx for ONTAP存储卷附加到 Amazon EVS 了。以下步骤将展示如何访问 vCenter 并将 FSx for ONTAP卷挂载为 NFS 数据存储：

1. 在 vSphere 客户端中，转到“数据存储”选项卡。找到数据中心，导航至存储>新数据存储，如下所示：

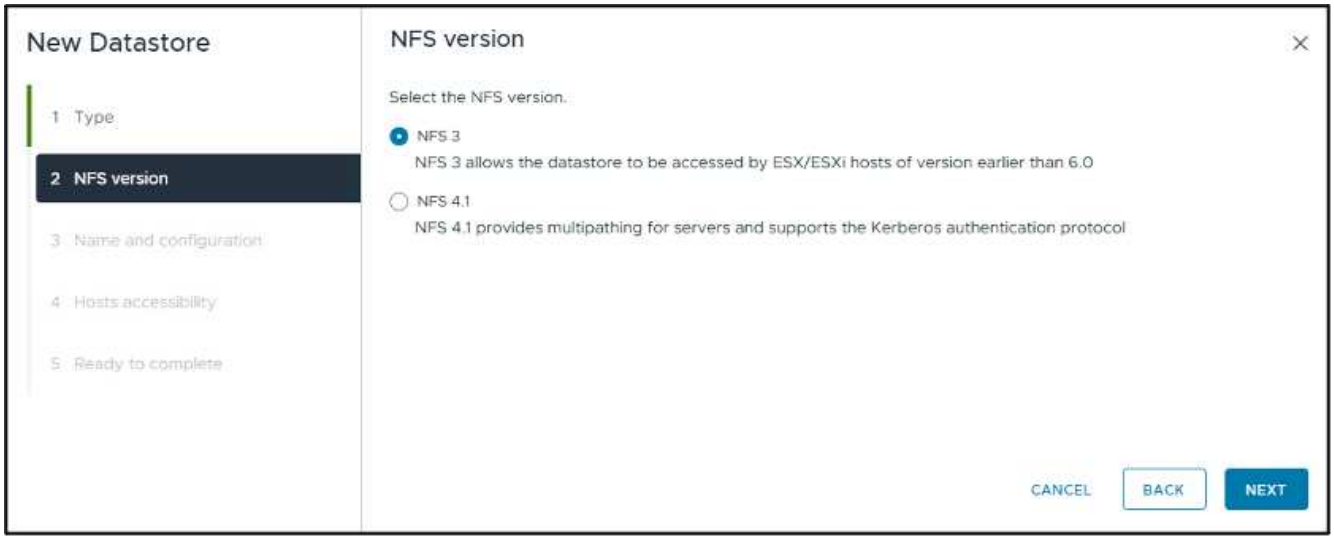


2. 您现在将进入新数据存储向导。在“类型”步骤中，您将选择数据存储类型。选择“NFS”并单击“下一步”继续。



3. 在“NFS 版本”步骤中，您将选择一个 NFS 版本。

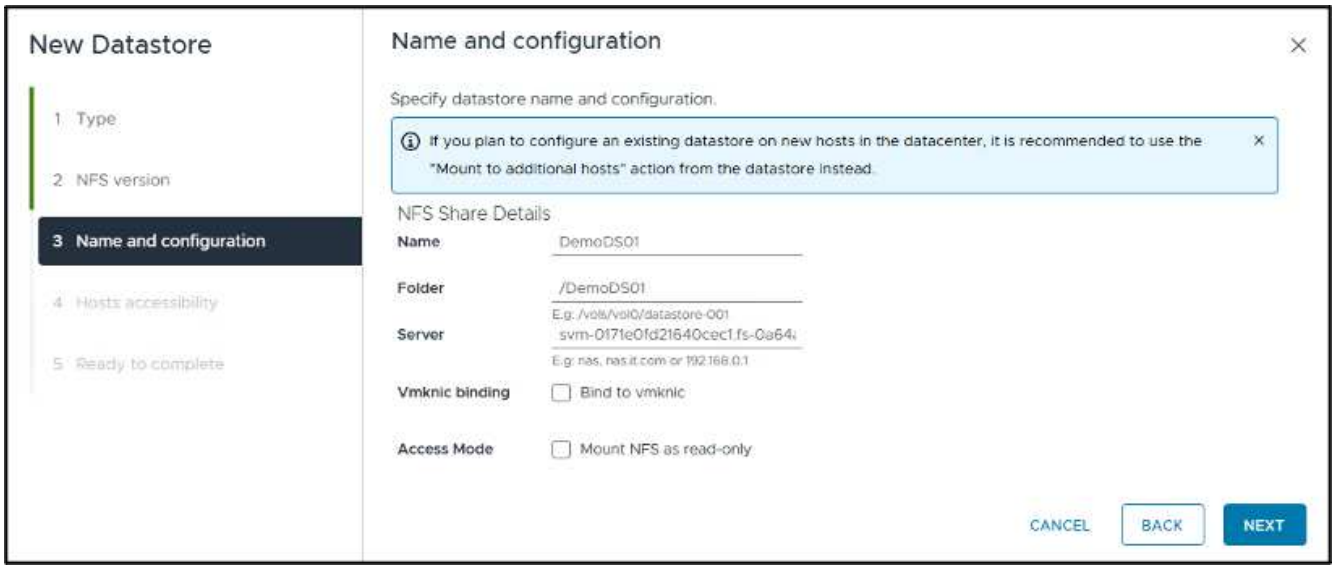
   为了本例的目的，我们将选择“NFS 3”，但请注意，也可以使用 NFS v4.1。



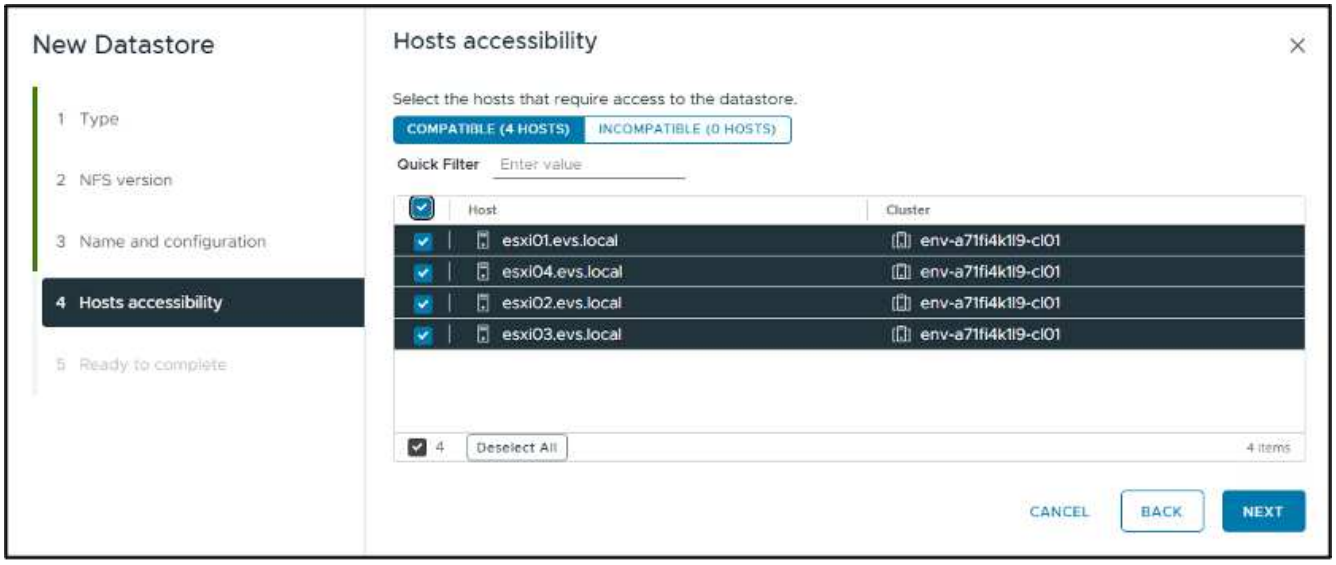
4. 在“名称和配置”步骤中，您将：

   a. 命名数据存储。
   b. 命名文件夹。使用 NFS 卷的连接路径。
   c. 命名服务器。使用 SVM 的 NFS DNS 名称或 NFS 的 IP 地址。

      单击“下一步”继续。



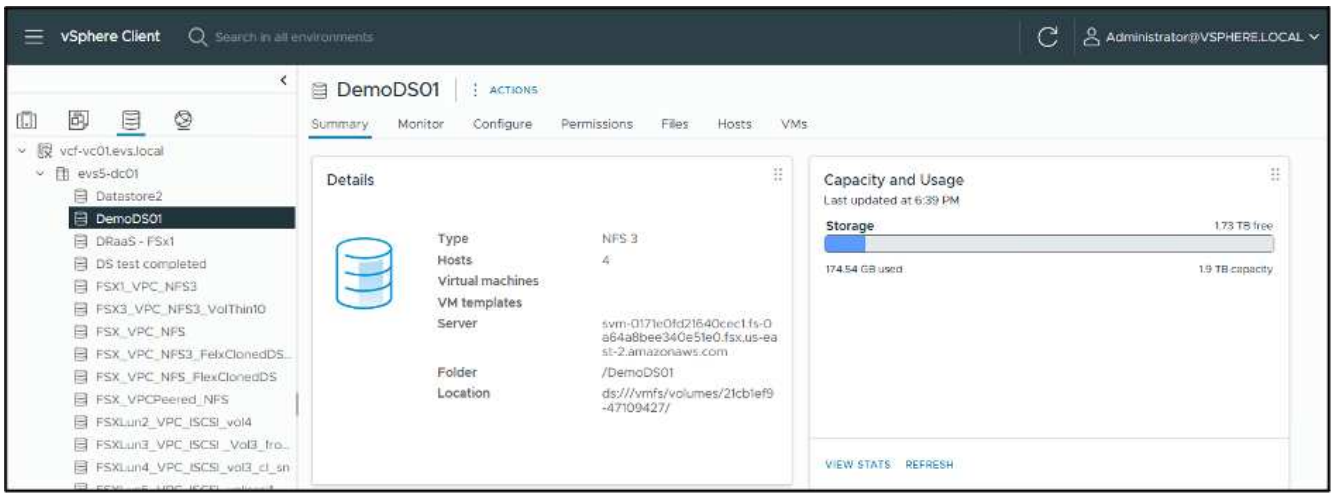
5. 在“主机可访问性”步骤中，选择所有需要访问数据存储的主机，然后单击“下一步”继续。



6. 在“准备完成”步骤中，检查数据并单击“完成”以完成设置。



7. 通过访问 vCenter 验证 NFS 数据存储是否已连接，如下所示：



使用 **FSx for ONTAP**作为 **iSCSI** 数据存储库的部署过程

本节介绍使用 FSx for ONTAP配置 iSCSI 数据存储库的步骤。

前提条件

在将 FSx for ONTAP配置并连接为 iSCSI 数据存储之前，您必须先部署 Amazon EVS 虚拟化环境。有关更多信息，请参阅《Amazon EVS 入门指南》文档。本节还假设您已经部署了 FSx for ONTAP文件系统，请参阅上面的详细方法部分了解适当的步骤。

高级部署步骤

部署 FSx for ONTAP文件系统以用作 Amazon EVS 的 iSCSI 数据存储并在两项服务之间建立连接将包括以下步骤：

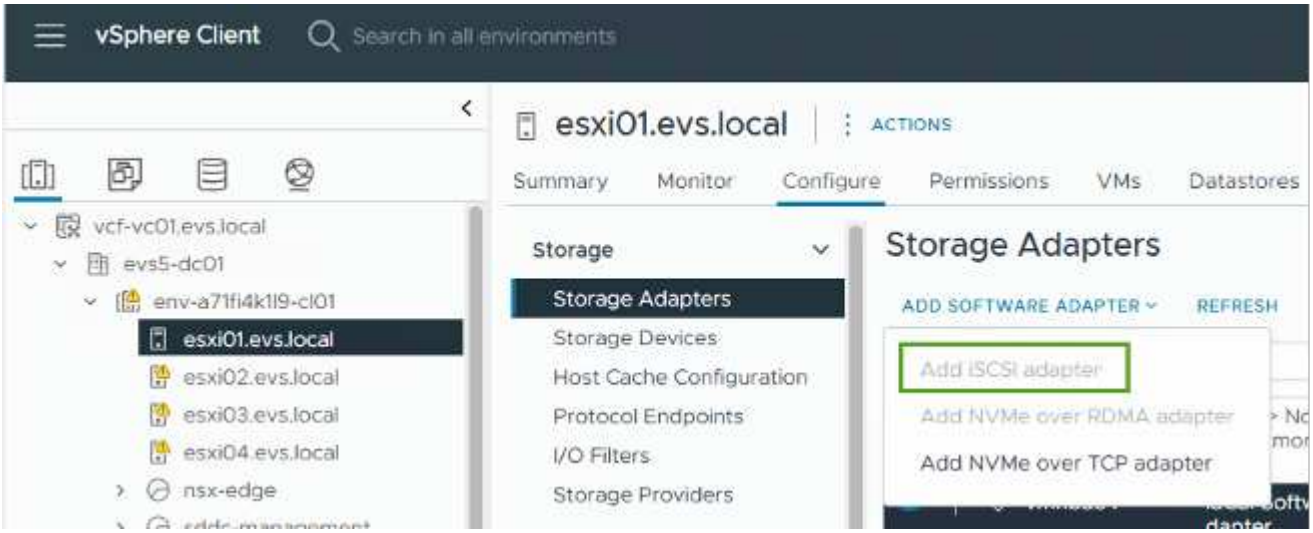
- 为每个 ESXi 主机设置一个 iSCSI 网络适配器。
- 创建和配置 FSx for ONTAP文件系统、卷、LUN 等。

- 将 ESXi 主机连接到 FSx for ONTAP文件系统服务器。
- 创建 iSCSI 数据存储虚拟机文件系统 (VMFS)。

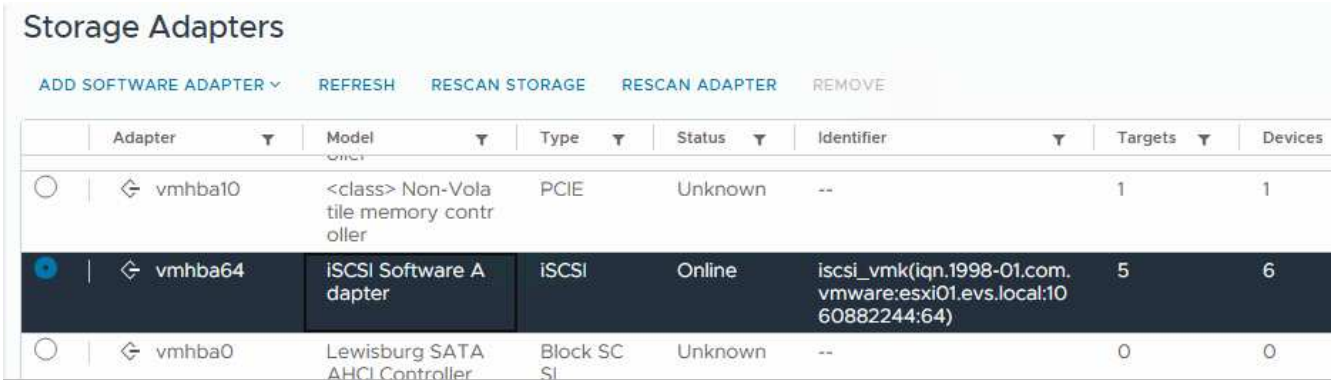
添加 **iSCSI** 网络适配器

需要在您环境中的每个 ESXi 主机上执行以下步骤。

1. 进入vSphere客户端，选择ESXi主机。在配置选项卡下，选择“添加软件适配器”，然后从下拉菜单中选择“添加 iSCSI 适配器”，如下所示：

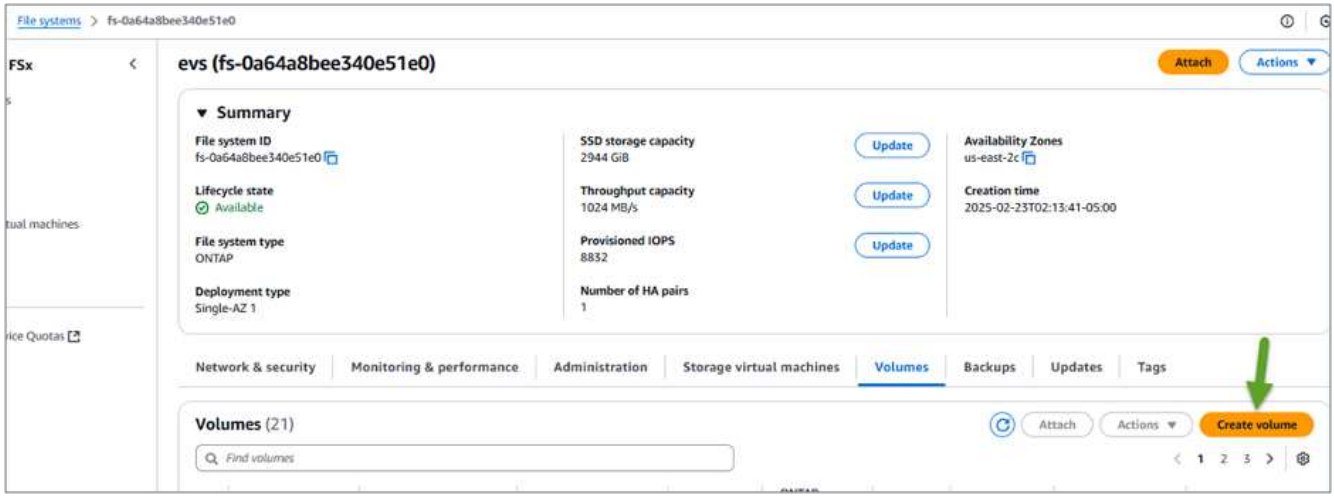


2. 安装完成后，您将进入存储适配器屏幕。从菜单栏中选择“重新扫描适配器”。记录 iSCSI 适配器的 IQN ：iqn.xxxx。该值稍后将在 LUN 映射步骤中使用。



创建 **FSx for ONTAP**卷

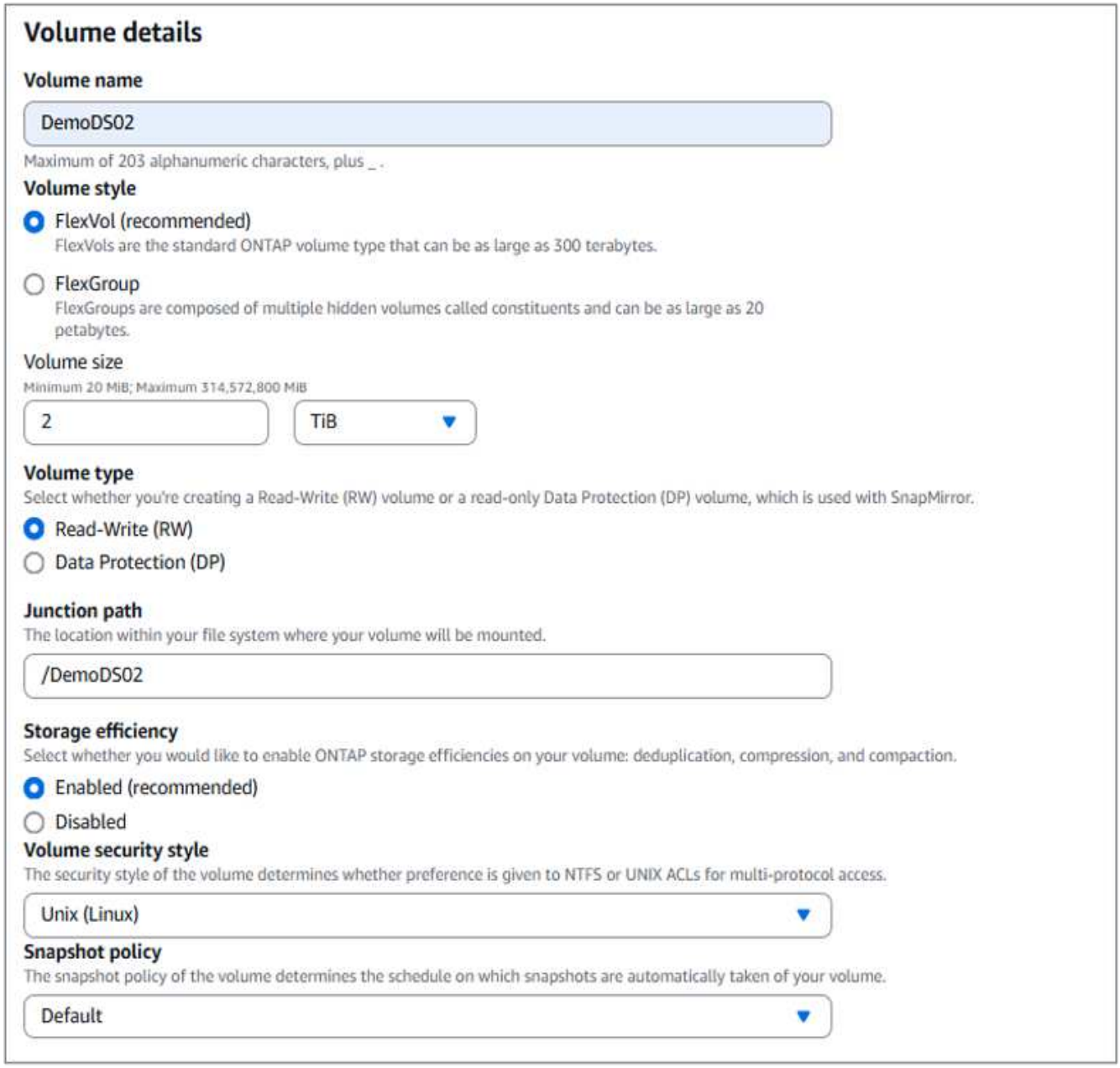
1. 转到 AWS 控制台并进入 FSx for ONTAP文件系统的页面，然后单击“创建卷”。



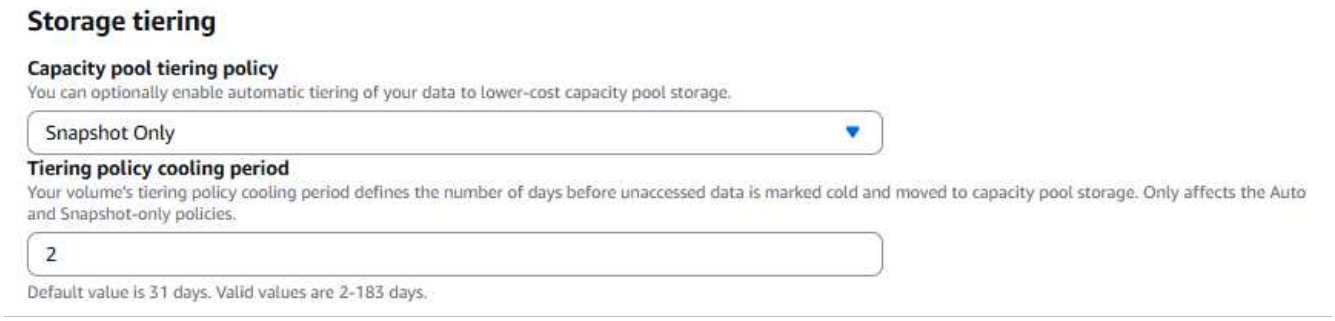
2. 选择要创建卷的 SVM。



3. 在“卷详情”页面，输入如下图所示的详情。完成后，单击“创建”来设置卷。选择“已启用”以打开ONTAP存储效率功能（压缩、重复数据删除和压缩）。



4. 对于存储分层选项，从下拉菜单中选择“仅快照”并设置分层策略冷却期。默认值为 31 天，但对于此示例，我们设置了两天的冷却期。



5. 创建卷后，使用ONTAP CLI 设置以下值：

环境	配置
数量保证	无（精简配置）
部分储备	0%
snap_reserve	0%
自动调整大小	grow_shrink
存储效率	已启用
卷分层策略	仅快照
访问时间更新（-atime-update）	False
最小预读（-min-readahead）	False
Snapshot 策略	无
LUN 空间预留	已禁用
LUN空间分配	已启用

创建 **LUN**、**igroup** 和映射 **LUN**

在本节中，我们将展示如何创建将在 vSphere 中显示为磁盘的 LUN。我们还将展示如何创建启动器组 (igroup)，它是可以访问 LUN 的启动器的列表。 igroup 将允许从 vSphere ESXi 主机访问 LUN。最后，我们将展示如何将 igroup 映射到 LUN。

1. 要访问ONTAP CLI，请通过运行以下命令在 FSx for ONTAP文件系统或 SVM 的管理端口上建立 SSH 会话：

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. 创建 LUN。确保将空间分配和空间预留设置为启用。该大小应达到卷大小的 90%：

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. 创建 igroup，并添加集群内所有 ESXi 主机的 IQN。

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. 使用以下代码映射 LUN：

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. 检查 LUN 映射并验证状态是否已更改为“已映射”。这是必要的双重检查，以确保 LUN 处于映射状态：

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

从 SVM 获取 iSCSI 配置信息

1. 运行 iSCSI show 并记录目标名称。这将用于 FSx for ONTAP磁盘的 vSphere 发现（注意：此目标名称对于您的 SVM 是唯一的）：

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. 记录 iSCSI IP 地址：

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

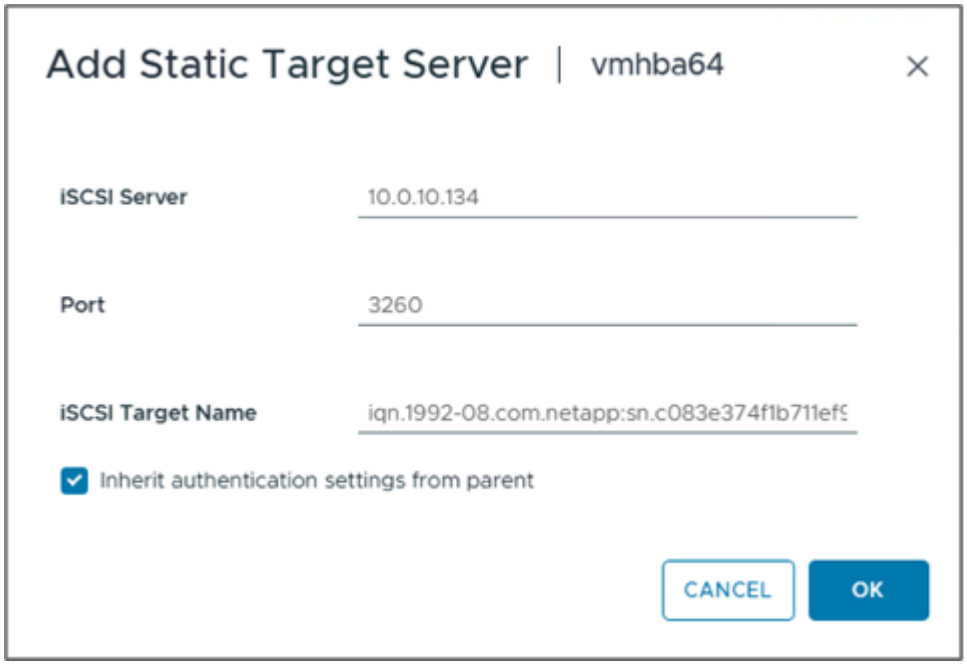
发现 FSx for ONTAP iSCSI 服务器

现在我们已经映射了 LUN，我们可以发现 SVM 的 FSx for ONTAP iSCSI 服务器。请注意，对于 SDDC 中存在的每个 ESXi 主机，您都需要重复此处列出的步骤。

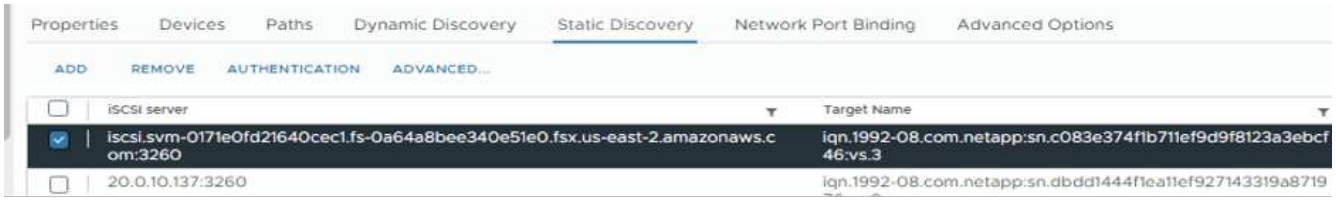
1. 首先，确保链接到 FSx for ONTAP文件系统（即连接到 ENI 的安全组）的安全组允许 iSCSI 端口。

   有关 iSCSI 协议端口的完整列表以及如何应用它们，请参阅"使用 Amazon VPC 进行文件系统访问控制"。

2. 在 vSphere Client 中，转到 ESXi 主机 > 存储适配器 > 静态发现，然后单击“添加”。
3. 输入上面的 iSCSI 服务器 IP 地址（端口为 3260）。 iSCSI 目标名称是来自 iSCSI show 命令的 IQN。单击“确定”继续。



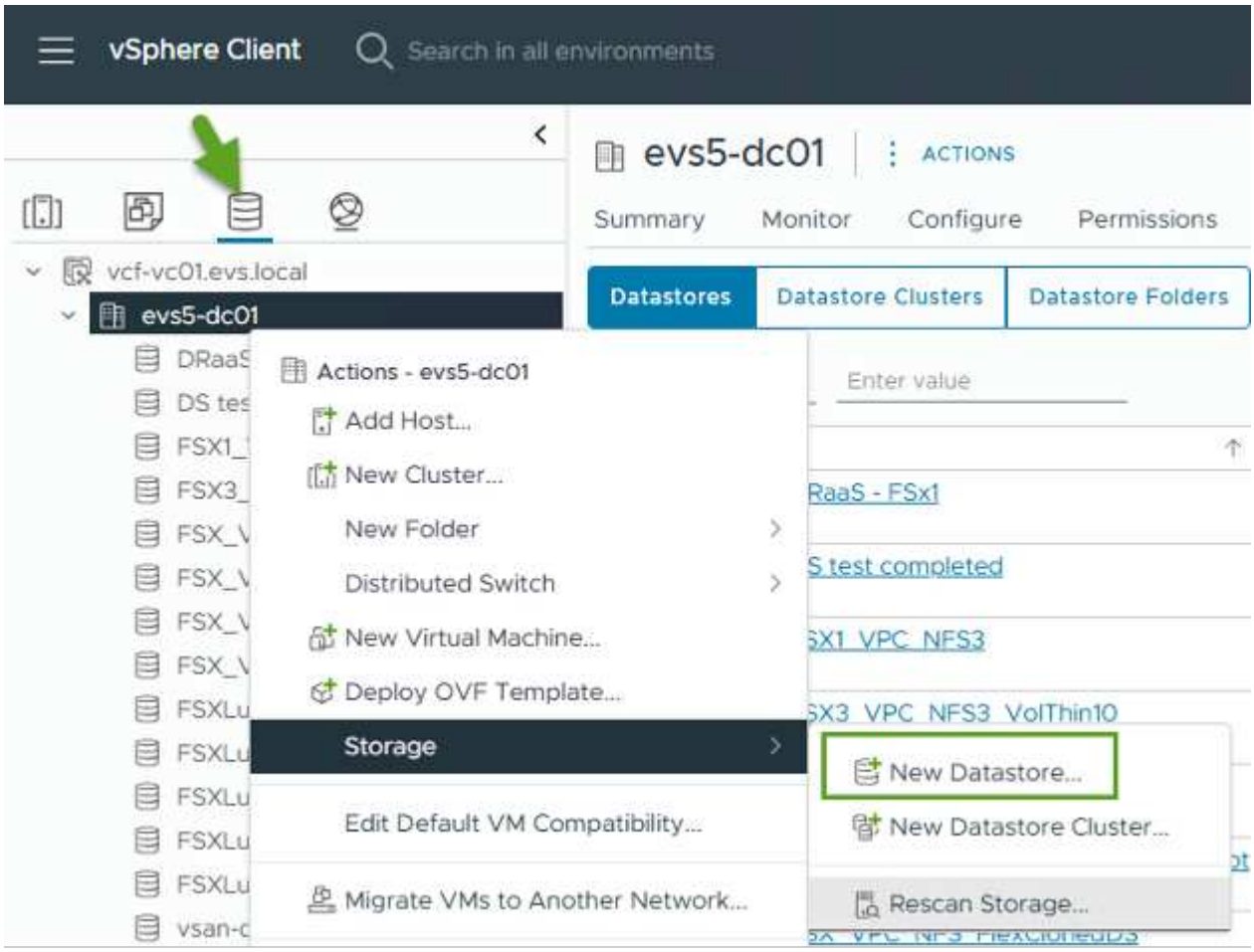
4. 向导将关闭，您将进入数据存储静态发现屏幕。在本页的表格中，您将能够验证目标是否已被发现。



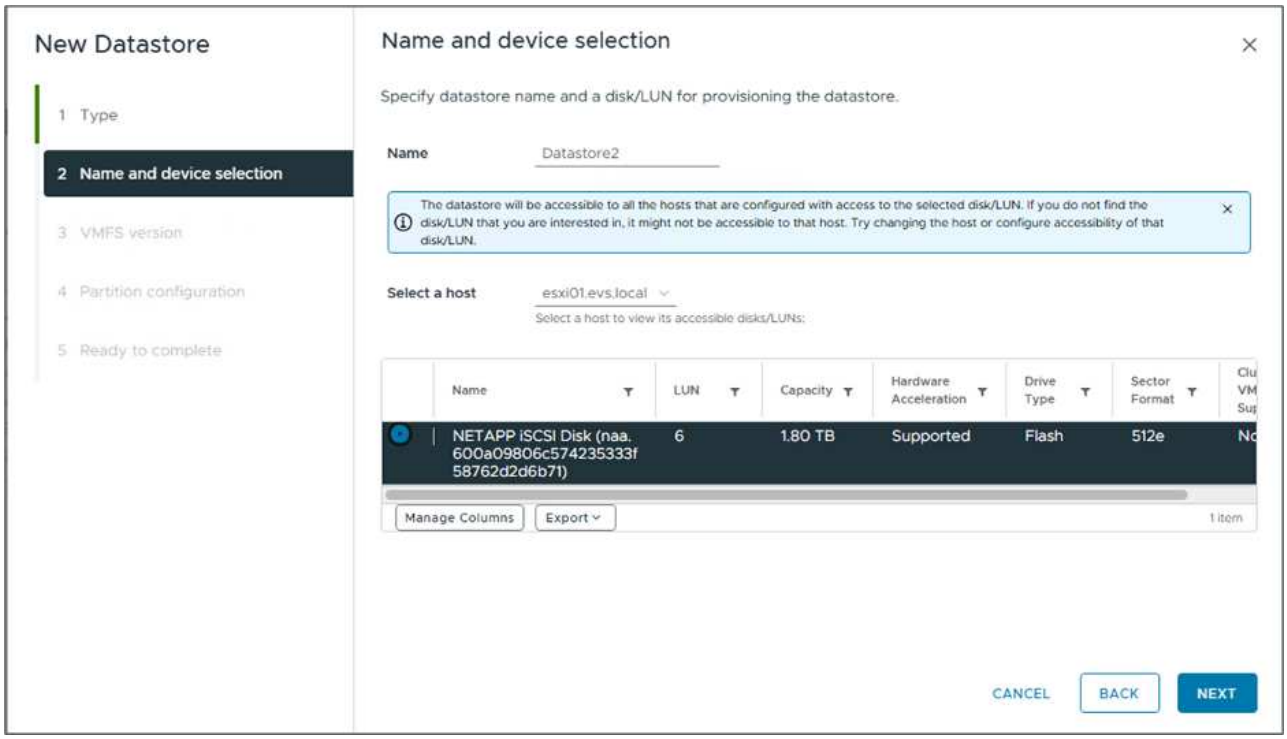
创建 **iSCSI** 数据存储

现在我们已经发现了 iSCSI 服务器，我们可以创建一个 iSCSI 数据存储。

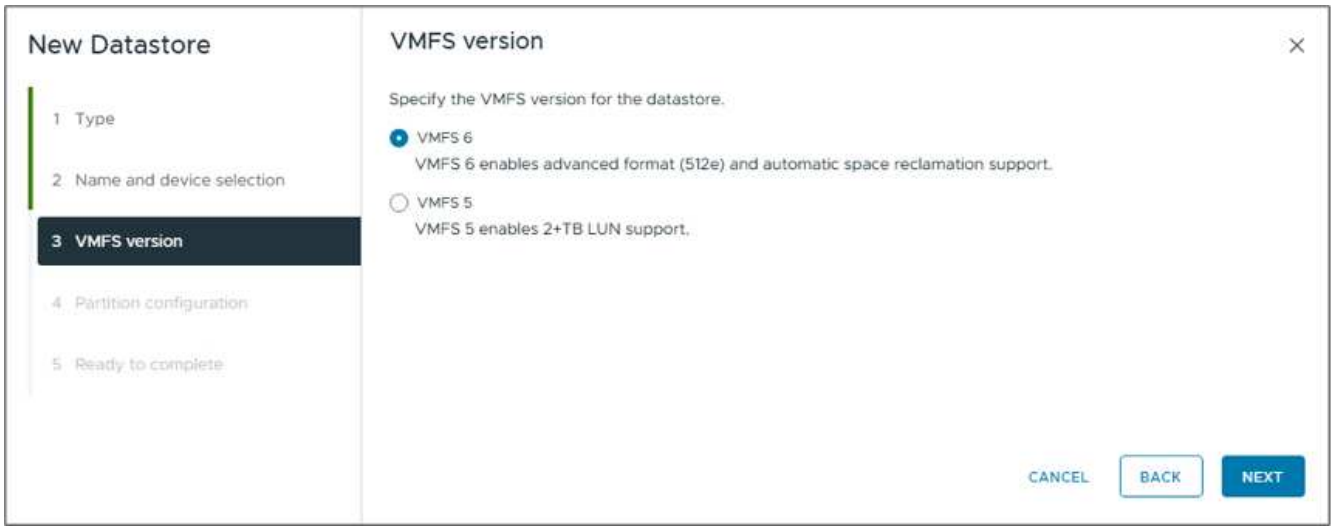
1. 在 vSphere 客户端中，转到“数据存储”选项卡，选择要部署数据存储的 SDDC。右键单击并选择存储图标（如下图屏幕截图中的绿色箭头所示），然后从下拉菜单中选择“新建数据存储”：



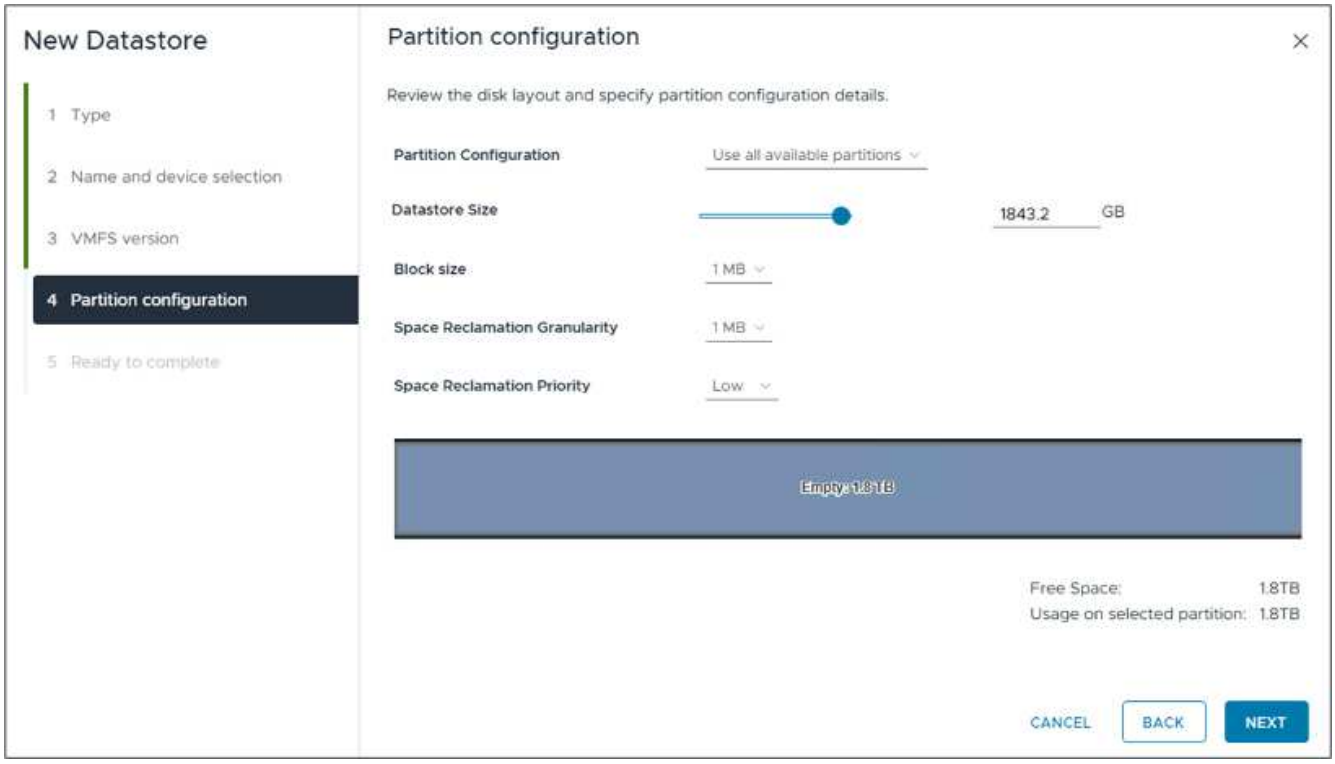
2. 您现在将进入新数据存储向导。在“类型”步骤中，选择 VMFS 选项。
3. 在“名称和设备选择”步骤中：
   a. 为您的数据存储提供一个名称。
   b. 选择要连接到数据存储的 ESXi 主机。
   c. 选择发现的磁盘（LUN），然后单击“下一步”。



4. 在“VMFS 版本”步骤中，选择“VMFS 6”。



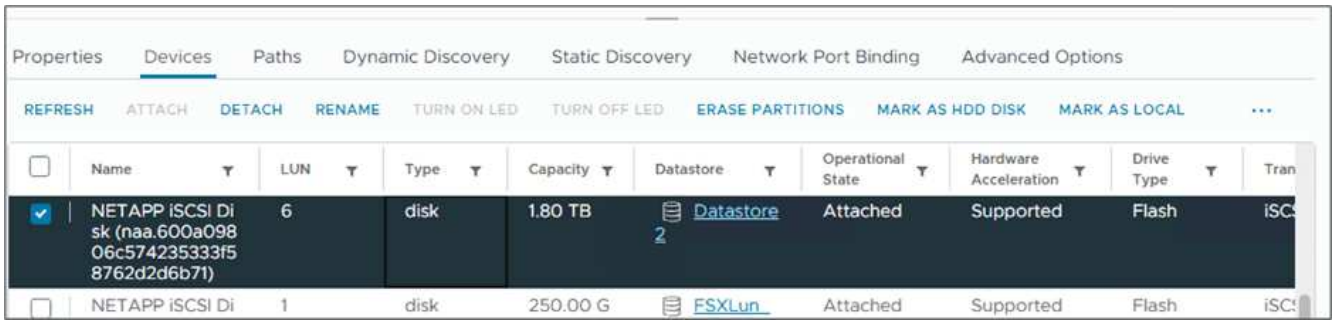
5. 在“分区配置”步骤中，保留默认设置，包括“使用所有可用分区”选项。单击“下一步”继续。



6. 在“准备完成”步骤中，确保设置正确。完成后，单击“完成”以完成设置。



7. 返回“设备”页面并验证数据存储是否已连接。



结束语

本文档提供了有关如何将 FSx for ONTAP设置为 Amazon EVS 的外部存储以便与 NFS 和 iSCSI 协议一起使用的说明。

使用 FSx for ONTAP作为 Amazon EVS 的外部存储可提供明确的运营和业务价值。它通过ONTAP技术提供更好的数据弹性、保护、复制和成本效率，并通过解耦 VMware 超融合架构保持 TCO 优化。借助 FSx for ONTAP ，Amazon EVS 用户无需添加计算资源即可扩展存储，也不会增加成本。这充分发挥了 AWS 云的弹性和规模潜力。

要了解更多信息，请阅读亚马逊新品公告："Amazon EVS 现已与 FSx for ONTAP集成"以及NetApp博客："Amazon EVS 宣布支持 FSx for ONTAP" 。

保护 **EVS** 的 **FSx ONTAP** 数据存储

如何使用 **Amazon Elastic VMware Service** 和 **NetApp SnapCenter Plug-in for VMware** 保护 **Amazon FSx for NetApp ONTAP** 数据存储

本指南将演示使用 NetApp SnapCenter® Plug-in for VMware vSphere (SCV) 备份和恢复解决方案保护 FSx for ONTAP Network File System (NFS) 和 iSCSI Amazon EVS 数据存储区及相关 VM 的简单部署方法。

简介

基于 Amazon FSx for NetApp ONTAP（FSx for ONTAP）的 Amazon Elastic VMware Service (Amazon EVS) 补充数据存储区为运行性能要求苛刻的工作负载（例如利用 nConnect、Amazon Virtual Private Cloud (Amazon VPC) 对等以及每个数据存储区挂载使用多个网络连接）和存储密集型工作负载提供了出色的解决方案。

此功能使客户能够克服虚拟存储区域网络 (vSAN) 提供的本地实例存储的局限性，独立于计算扩展存储，并降低总体拥有成本。除了总拥有成本 (TCO) 优势之外，FSx for ONTAP 提供 Amazon EVS 以及本地部署 ONTAP® 客户熟悉的企业级功能，帮助优化和简化部署。使用 FSx for ONTAP 可以访问 NetApp® Snapshot™ 、SnapMirror® 和 SnapVault® 技术，这些技术支持虚拟机 (VM)、数据存储区和虚拟机磁盘 (VMDK) 的备份和恢复操作。一个关键功能是基于 Snapshot 的保护。

概述

随着组织扩展和整合环境，保护这些工作负载和底层存储的需求变得越来越重要。SCV 可用于直接从 Amazon EVS vSphere 客户端备份数据存储区和虚拟机。

本指南的目的

本指南提供有关如何使用 SCV 保护适用于 Amazon EVS 的 FSx for ONTAP 数据存储的说明。还提供了保护 VM 和数据库以及还原的示例场景。

受众

本教程适用于熟悉 VMware vSphere、Amazon EVS、AWS 控制台和 FSx for ONTAP 的云架构师和云管理员。

部署和配置的高级步骤

以下是部署和配置 SCV 以保护 Amazon EVS 上的虚拟机和数据存储的高级步骤：

1. 下载 SCV Open Virtual Appliance (OVA)。
2. 使用 vSphere Client 凭据登录到 Amazon EVS。
3. 部署开放虚拟化格式 (OVF) 模板以启动 VMware 部署向导。
4. 要访问插件，请从菜单中选择 SnapCenter Plug-in for VMware。
5. 添加存储。
6. 创建备份策略。
7. 创建资源组。
8. 备份资源组。
9. 还原整个虚拟机或特定的虚拟磁盘或来宾文件。

适用于 **VMware** 的 **SnapCenter** 插件的设置过程

本节介绍设置适用于 VMware 的 SnapCenter 插件的步骤。

前提条件

开始之前需要满足以下先决条件：

1. 要在部署 OVA 时注册 vCenter 服务器，请指定 vCenter 的完全限定域名 (FQDN) 或 IP 地址。
2. 对于 vCenter 凭据，请使用具有最低要求权限的帐户
3. 为 vCenter Server 访问打开防火墙端口。
4. 更新运行 FSx for ONTAP 的 Amazon VPC 的安全组，以允许 SCV 访问 FSx for ONTAP。

SCV 免费提供。

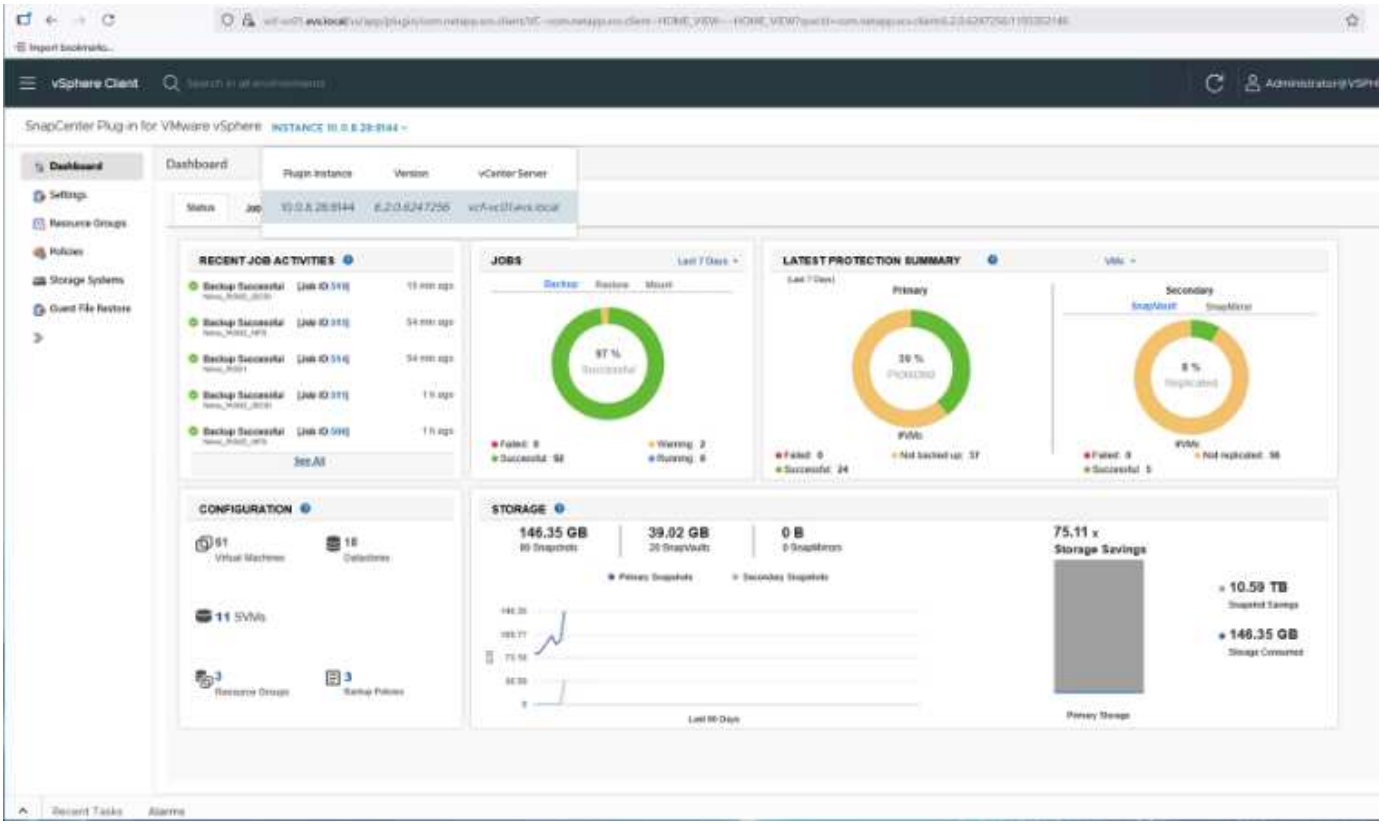
设置适用于 **VMware** 的 **SnapCenter** 插件

为了保护虚拟机和基于 NFS/iSCSI 的数据存储，必须部署 SCV。这是一个简单的 OVF 导入。

部署步骤如下：

1. 从 "NetApp 支持站点" 下载 OVA。

2. 登录到 Amazon EVS vCenter。
3. 在 vCenter 中，右键单击数据中心、文件夹、群集或主机等任何库存对象，然后选择"部署 OVF 模板"。
4. 选择正确的设置，包括存储、分段和自定义模板，以更新 vCenter 及其凭据、创建 SCV 凭据和 IP 详细信息。审核完毕后，选择"完成"。
5. 等待 OVF 导入和部署任务完成。
6. 一旦 SCV 成功部署，它将在 vCenter 中注册。
7. 要访问插件，请导航到 vCenter Web 客户端页面的左侧栏，然后选择"SnapCenter Plug-in for VMware"。



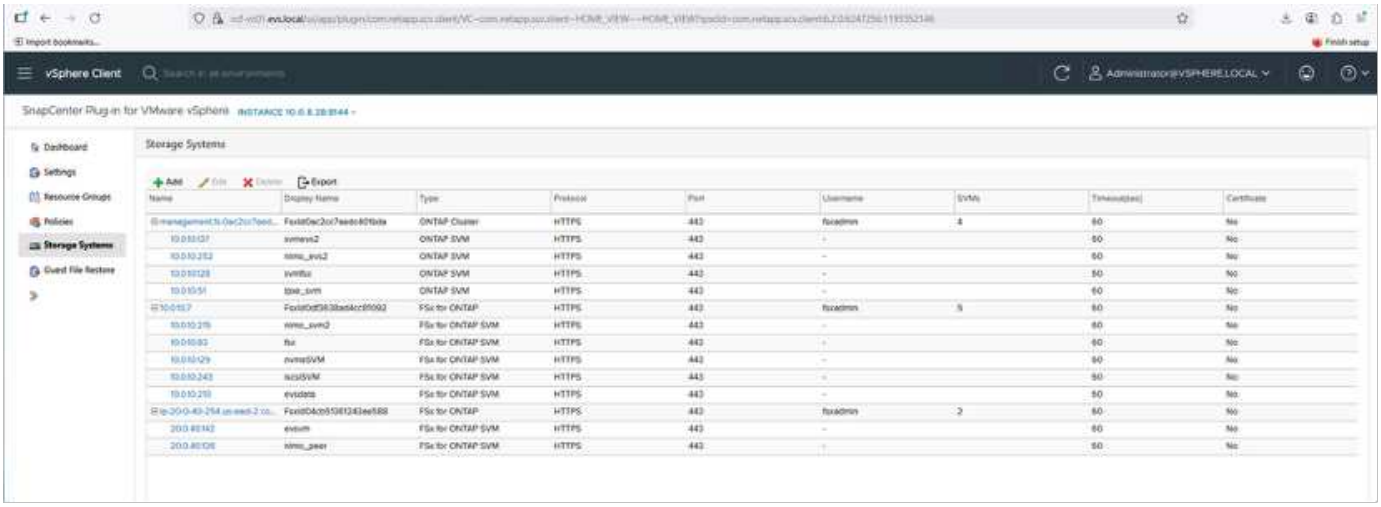
适用于 **VMware** 的 **SnapCenter Plug-in** 配置过程

本节介绍配置 SnapCenter Plug-in for VMware 的步骤。以下各节将详细介绍如何添加存储、创建备份策略以及如何创建资源组。

添加存储系统

使用 SVC 保护工作负载的下一步是添加"存储系统"。添加存储允许 SCV 检测和管理 vCenter 内的备份和还原操作。将 FSx for NetApp ONTAP 管理端点或存储虚拟机 (SVM) 管理端点 IP 作为存储系统，以启用 VM 备份和还原。

1. 从 EVS vCenter 的左侧导航菜单中，选择"SnapCenter Plug-in for VMware"。
2. 选择"Storage System"。
3. 选择"添加"以添加 FSx for ONTAP 详细信息。
4. 请使用"凭据作为身份验证"方法，并输入 FSxadmin 作为用户名和密码。然后选择"添加"以保存设置。



添加文件系统时会自动添加所有 SVM。

如果 SCV 版本为 6.2，请转到 "SCV 支持页面" 并下载 SCV 6.2P1 版本。

创建备份策略

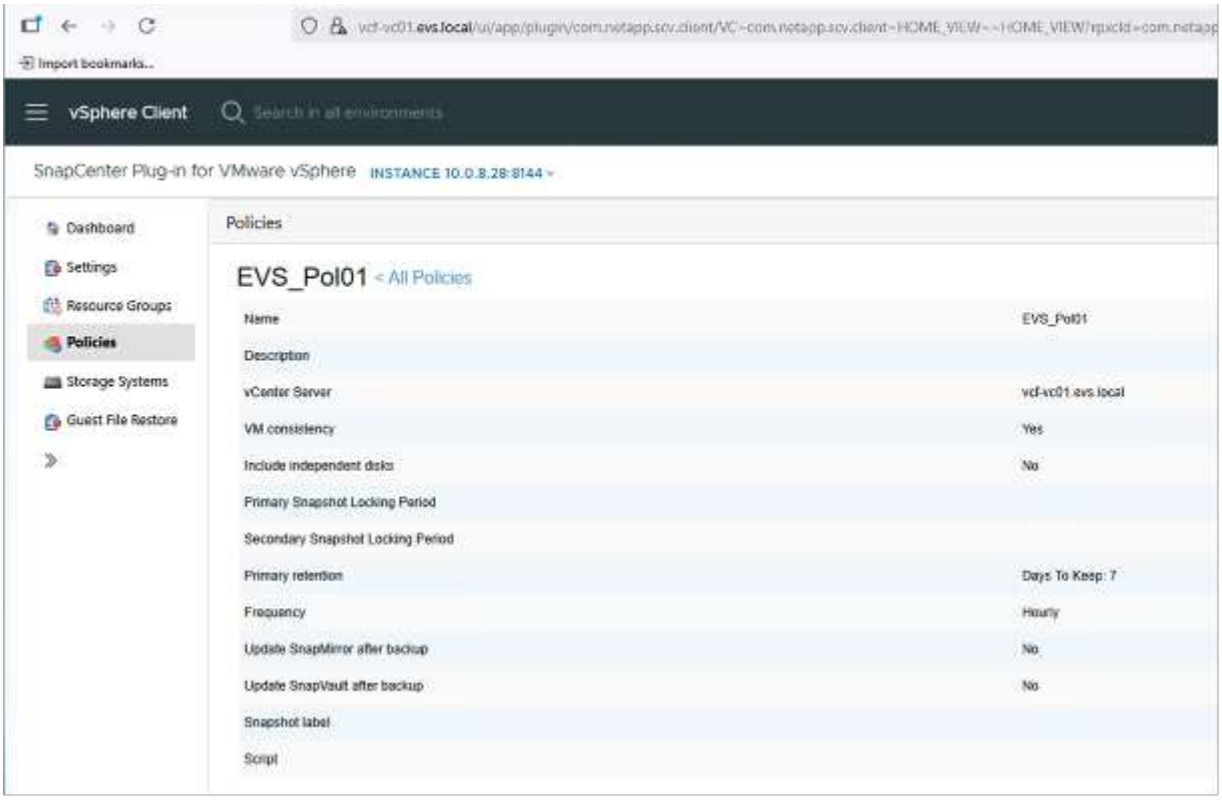
强大的备份策略应定义关键因素，例如备份计划、要备份的数据以及备份的保留期。可以按小时或按天安排快照副本，以保护整个数据存储区。通过这种方式安排备份不仅可以保护数据存储，还可以支持这些数据存储中包含的 VM 和 VMDK 的备份和恢复操作。

在为虚拟机和数据存储区启动备份之前，请创建"备份策略"和资源组。备份策略指定备份计划和保留设置等参数。

以下是创建备份策略的步骤：

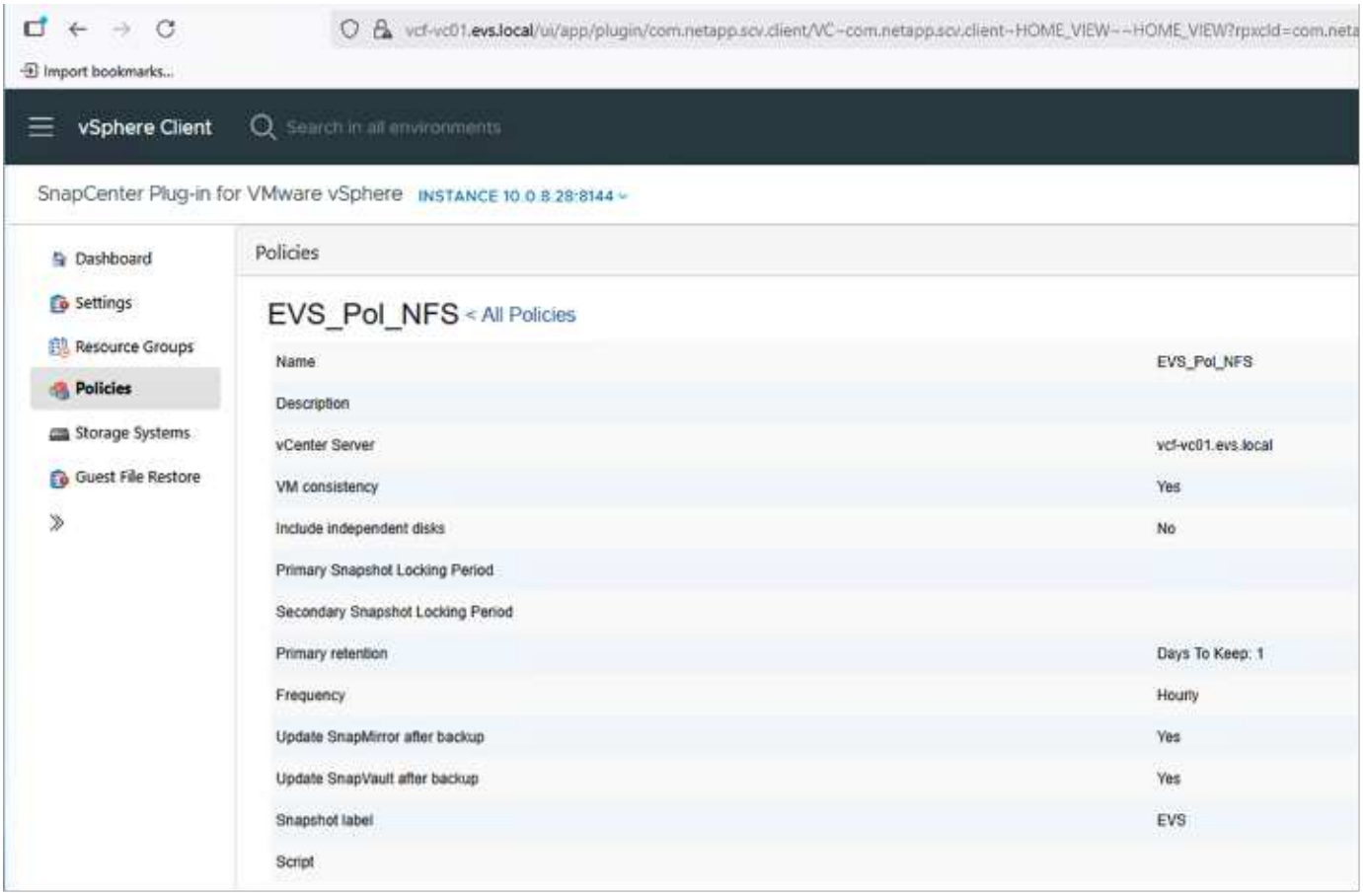
1. 转到 SCV 中的左侧导航菜单并选择"Policies"。
2. 在"策略"页面上，选择"创建"以启动向导。
3. 在"新建备份策略页面"上，输入策略的名称。
4. 指定保留期限、备份频率和复制设置。
5. 选中"Locking Period"复选框以启用 Snapshot 锁定。您可以将主要和次要 Snapshot 锁定期选择为天/月/年。

无论 SnapMirror 策略中定义的保留值如何，辅助 Snapshot 副本都将保持不变，直到指定的辅助快照锁定期到期。



要启用 VM 一致性备份，必须安装并运行 VMware 工具。当选中 VM 一致性框时，首先使 VM 静止，然后 VMware 执行 VM 一致性快照（不包括内存），然后 SCV 执行其备份操作，然后恢复 VM 操作。

要将 Snapshot 副本复制到辅助镜像或保管库文件系统，必须事先配置关系。



创建策略后，下一步是创建资源组，该资源组将定义应备份的适当 NFS 或 iSCSI 数据存储区和虚拟机。

创建资源组

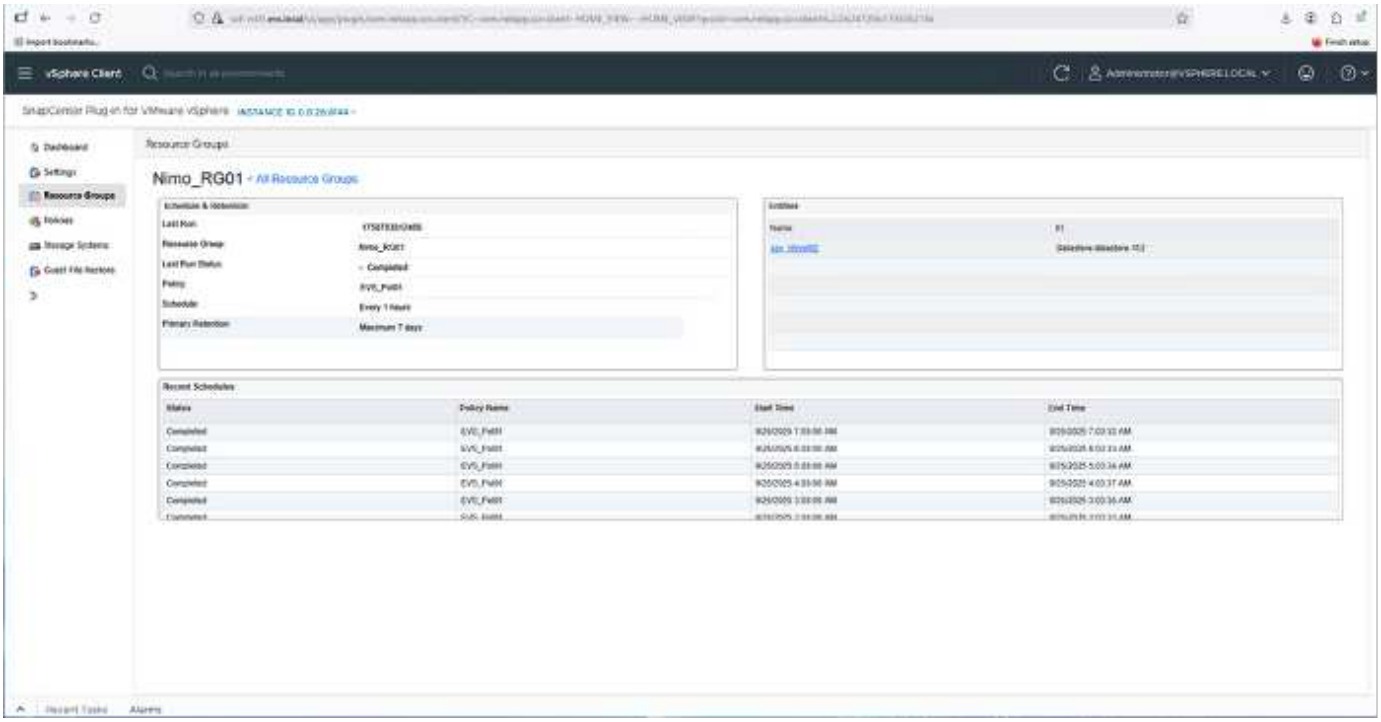
资源组用作需要保护的 VM 和数据存储的容器。资源可以随时添加到资源组或从资源组中删除，这为管理备份配置提供了灵活性。

您可以使用以下步骤创建 "资源组"：

1. 转到 SCV 中的左侧导航窗格并选择"Resource Groups"。
2. 在"资源组"页面上，选择"创建"以启动资源组创建向导。

   创建资源组的另一个选项是选择单个 VM 或数据存储区并创建仅包含该资源的资源组。

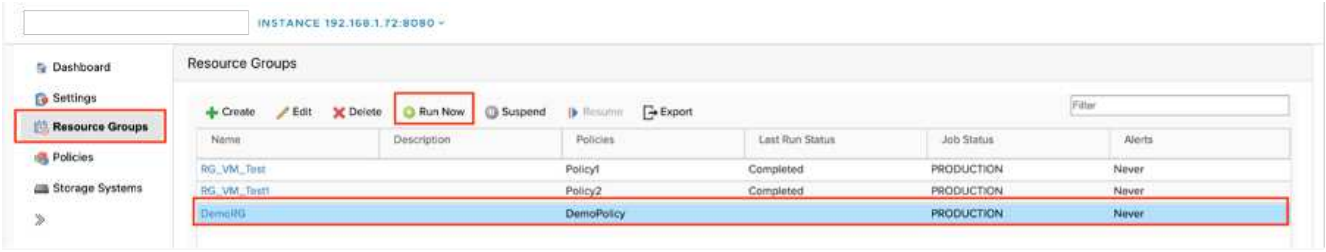
3. 在"资源"页面上，选择范围（VM 或数据存储）和数据中心。
4. 在"Spanning disks"页面上，选择"Virtual Machines with multiple VMDKs across multiple datastores"选项。
5. 接下来，关联备份策略。选择现有策略或创建新的备份策略。
6. 在"计划"页面上，为每个选定的策略配置备份计划。
7. 做出适当的选择后，选择"完成"。这将创建一个新资源组，并添加到资源组列表中。



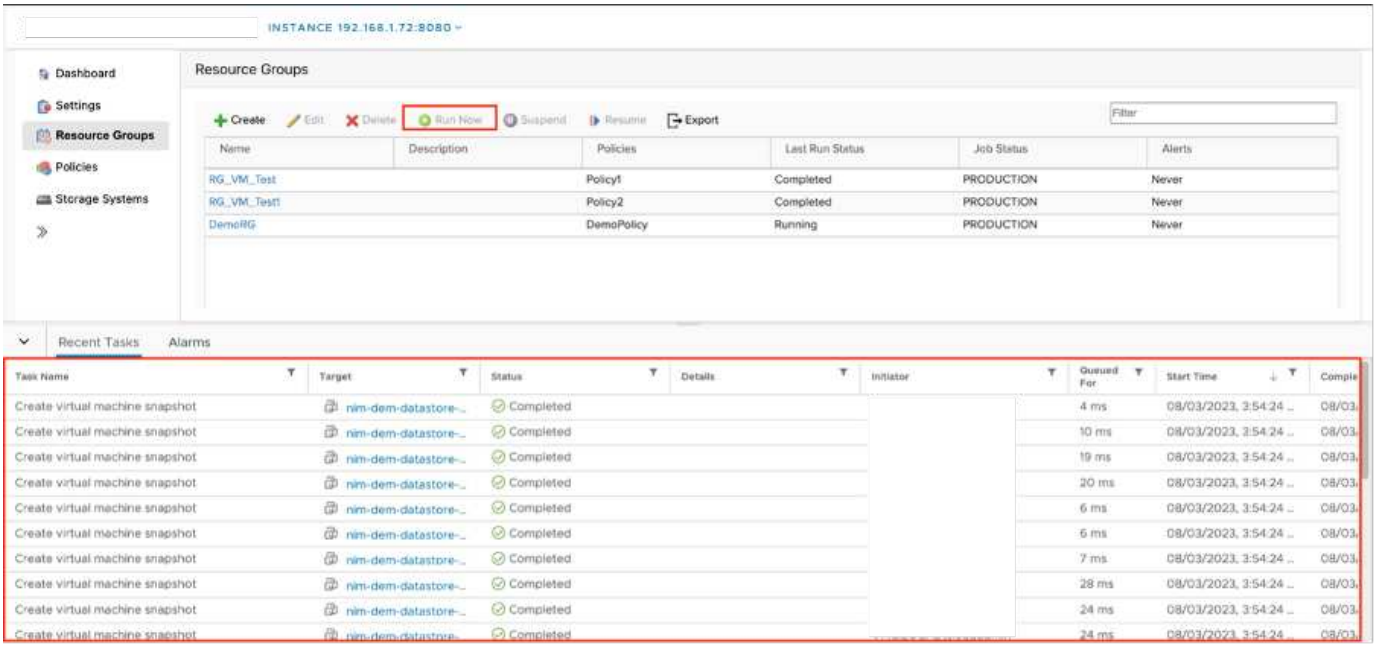
备份资源组

备份操作对资源组中定义的所有资源执行。如果资源组附加了策略并配置了计划，则会根据计划自动进行备份。

1. 在 vCenter Web 客户端页面的左侧导航中，选择"SnapCenter Plug-in for VMware"，然后选择"Resource Groups"。
2. 在资源组页面中，找到指定的资源组并选择"立即运行"以启动手动备份。



3. 如果资源组配置了多个策略，请在"立即备份"对话框中为备份操作选择策略。
4. 选择"OK"以启动备份。

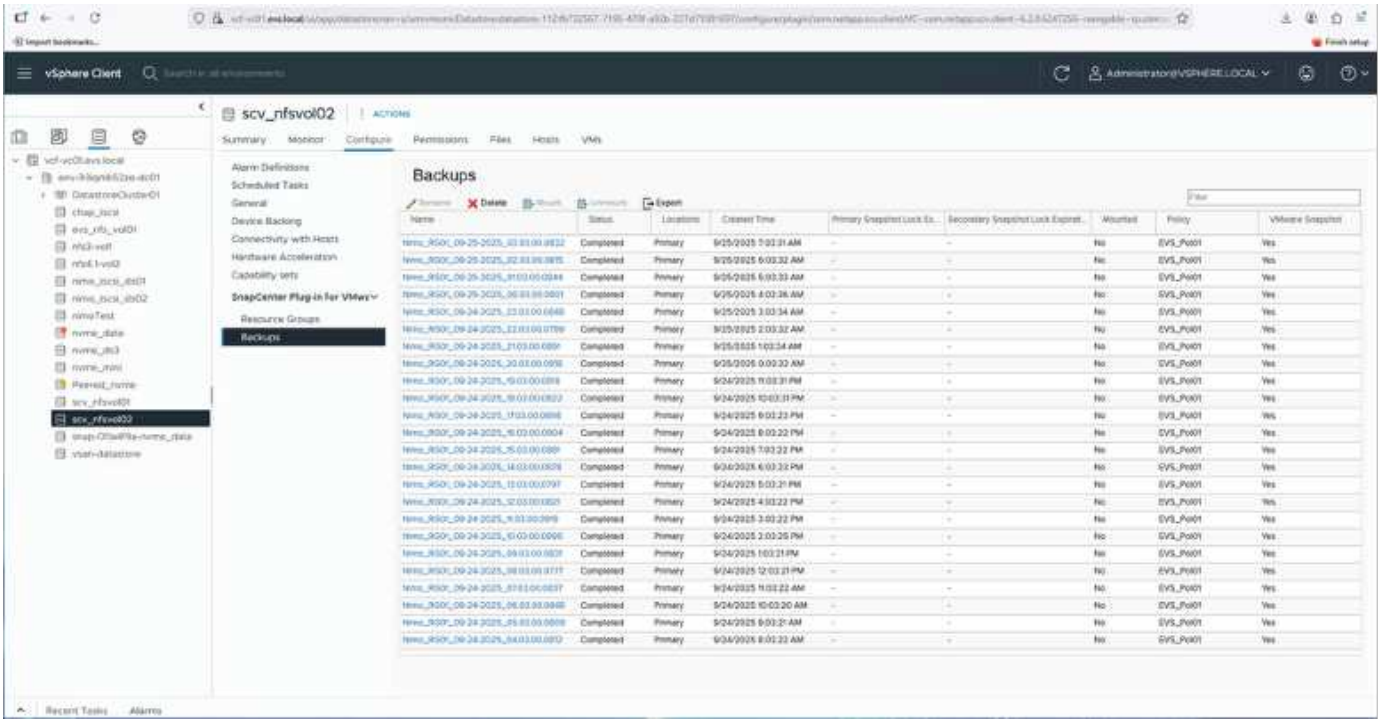


通过选择窗口底部的"最近任务"来监控操作进度，或者，有关更多详细信息，请选择仪表板上的"作业监视器"。

在不同的存储协议（包括 NFS 和 iSCSI）中，创建备份策略、配置资源组和执行备份操作的过程是一致的。

根据策略中定义的计划执行备份。

备份完成后，可以通过从下拉列表中选择"SnapCenter Plug-in for VMware vSphere"，然后选择"Restore"，在数据存储区级别或针对单个虚拟机查看备份。



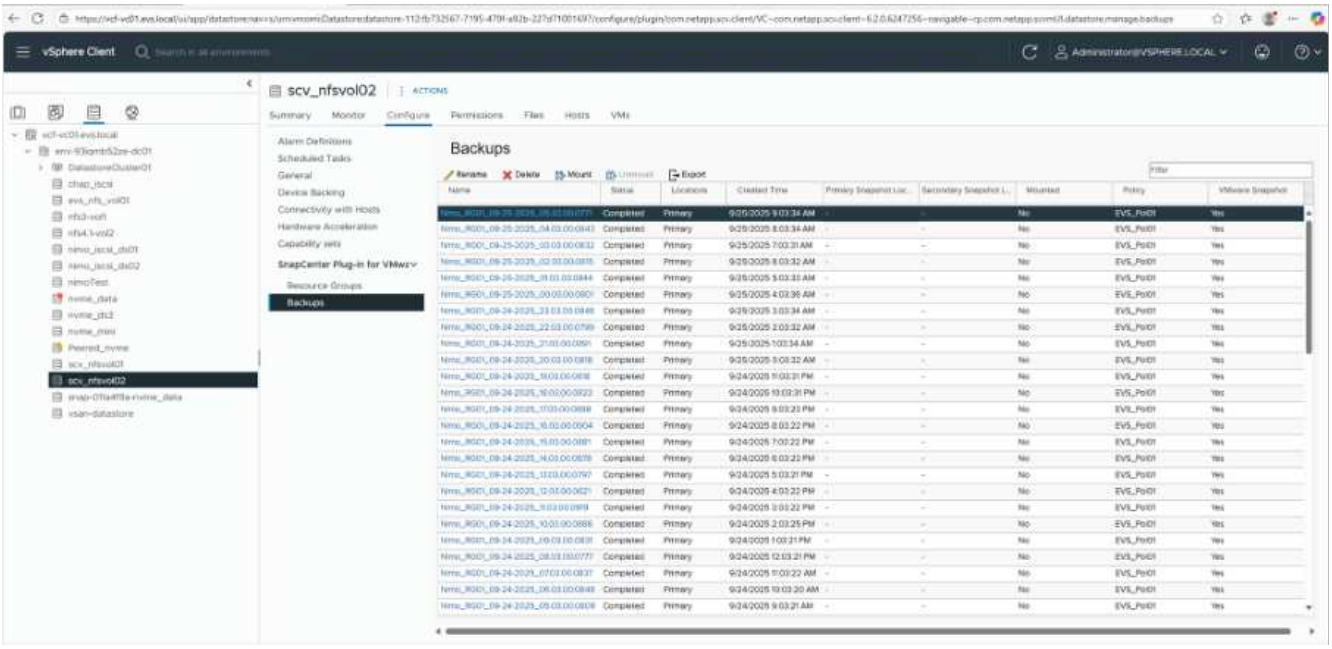
受 **SnapCenter Plug-in for VMware** 保护的虚拟机的还原过程

本节介绍从备份中恢复虚拟机的步骤。SCV 可用于恢复 vCenter 中的虚拟机，允许它们恢复到原始 ESXi 主机上的原始数据存储区（覆盖现有内容），从备份副本中恢复已删除或重命名的虚拟机，恢复到原始 ESXi 主机上的不同数据存储区，恢复到由同一 vCenter 管理的不同 ESXi 主机上的原始数据存储区，或恢复到同一 vCenter 环境中的另一台 ESXi 主机上的不同数据存储区。

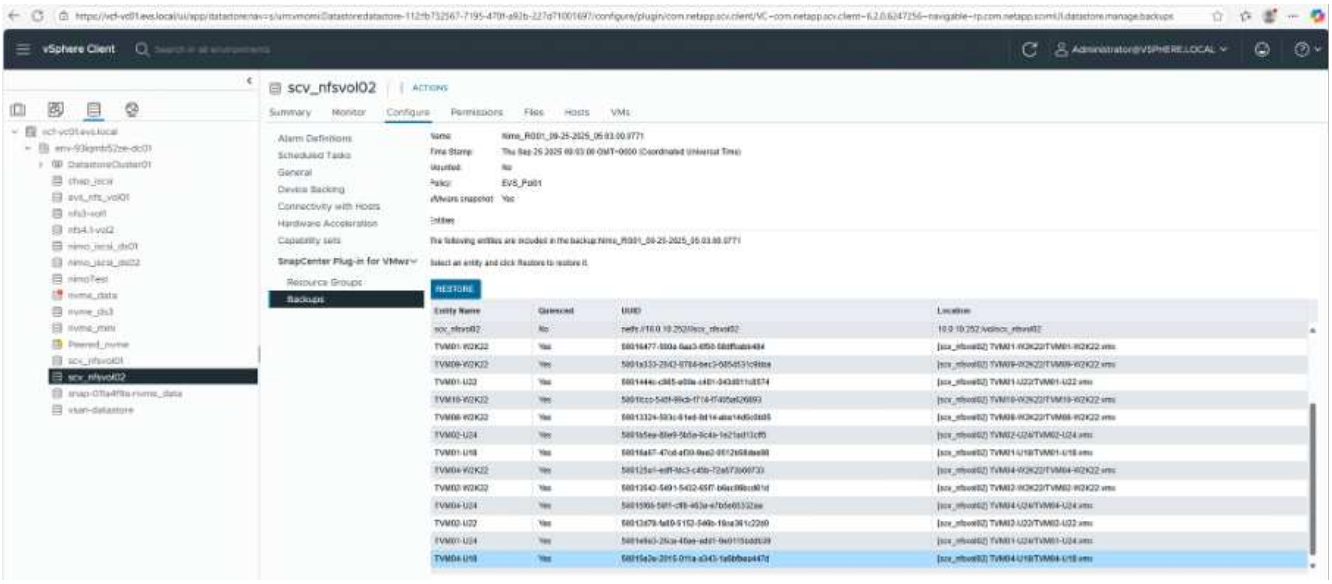
执行还原操作的步骤

要执行还原操作，请执行以下步骤：

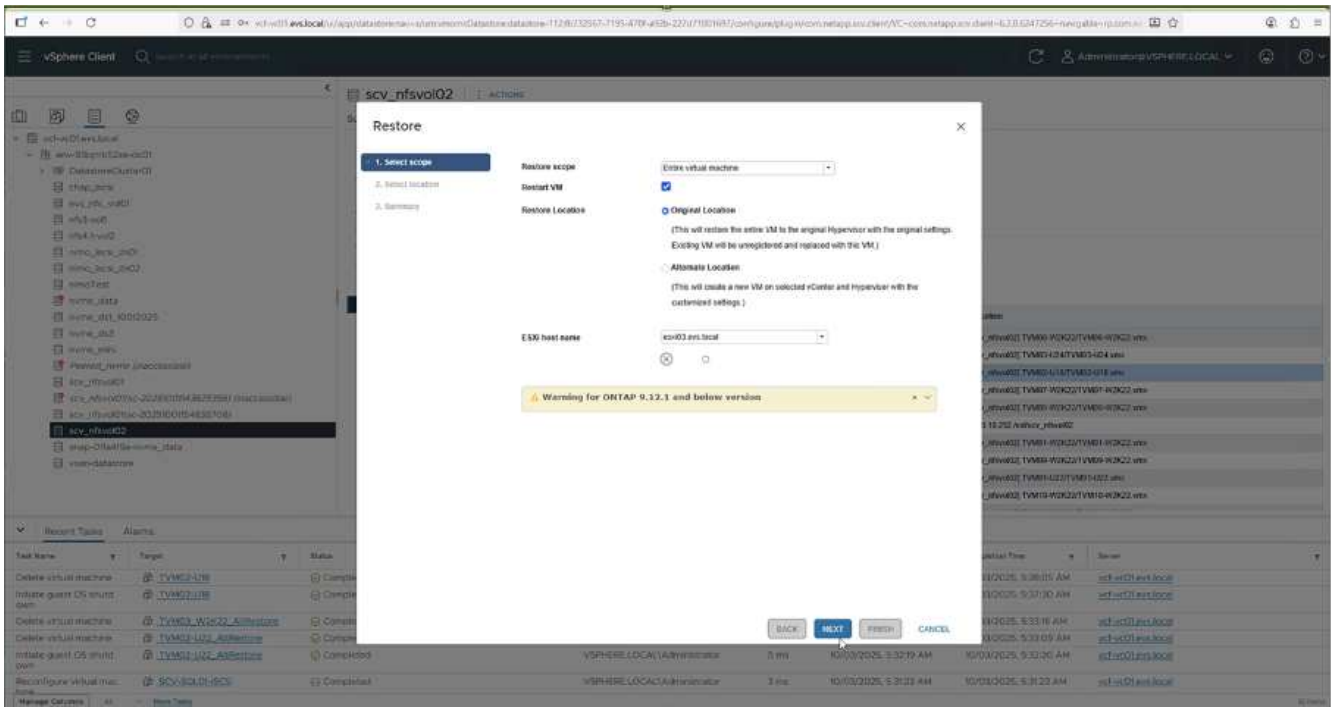
1. 在 EVS vSphere Web 客户端 GUI 中，转到**Inventory › Datastores**并选择所需的数据存储区。然后导航到"SnapCenter Plug-in for VMware vSphere"部分下的**Configure › Backups**。



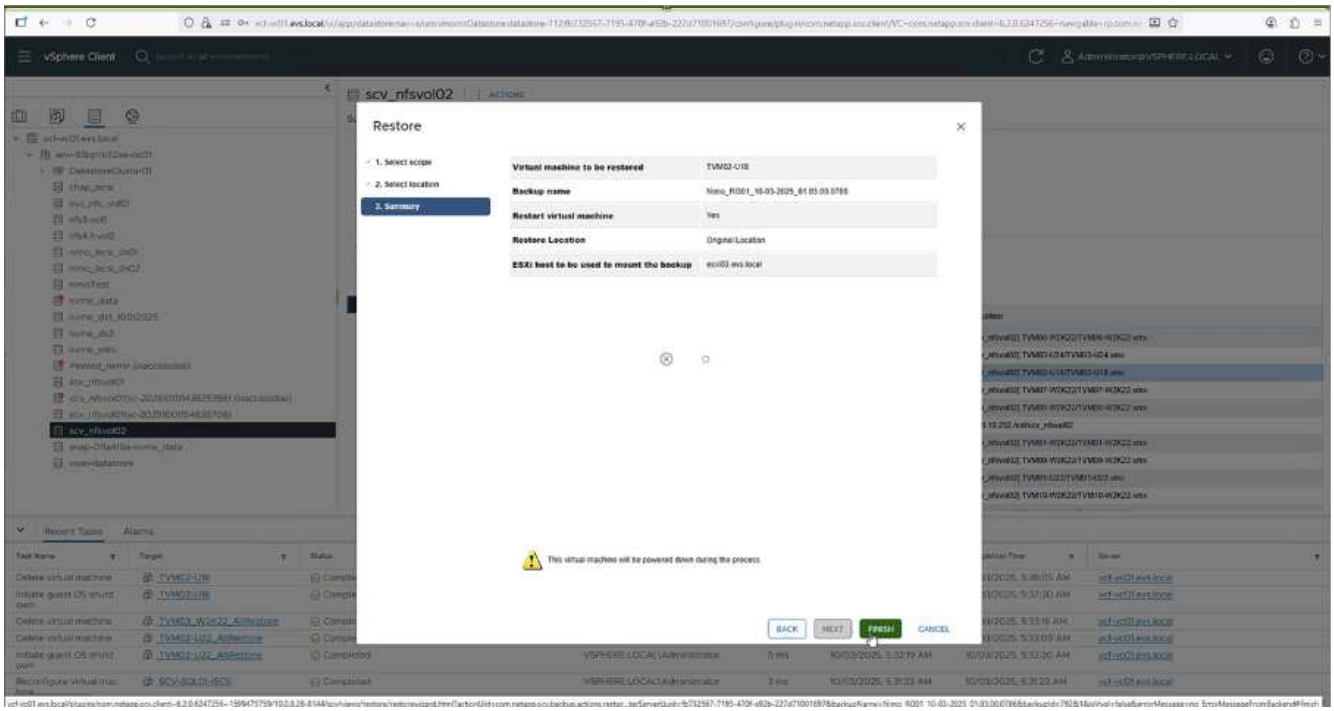
2. 双击备份以查看该备份中包含的所有虚拟机。在列表中找到要还原的虚拟机，然后选择"还原"。



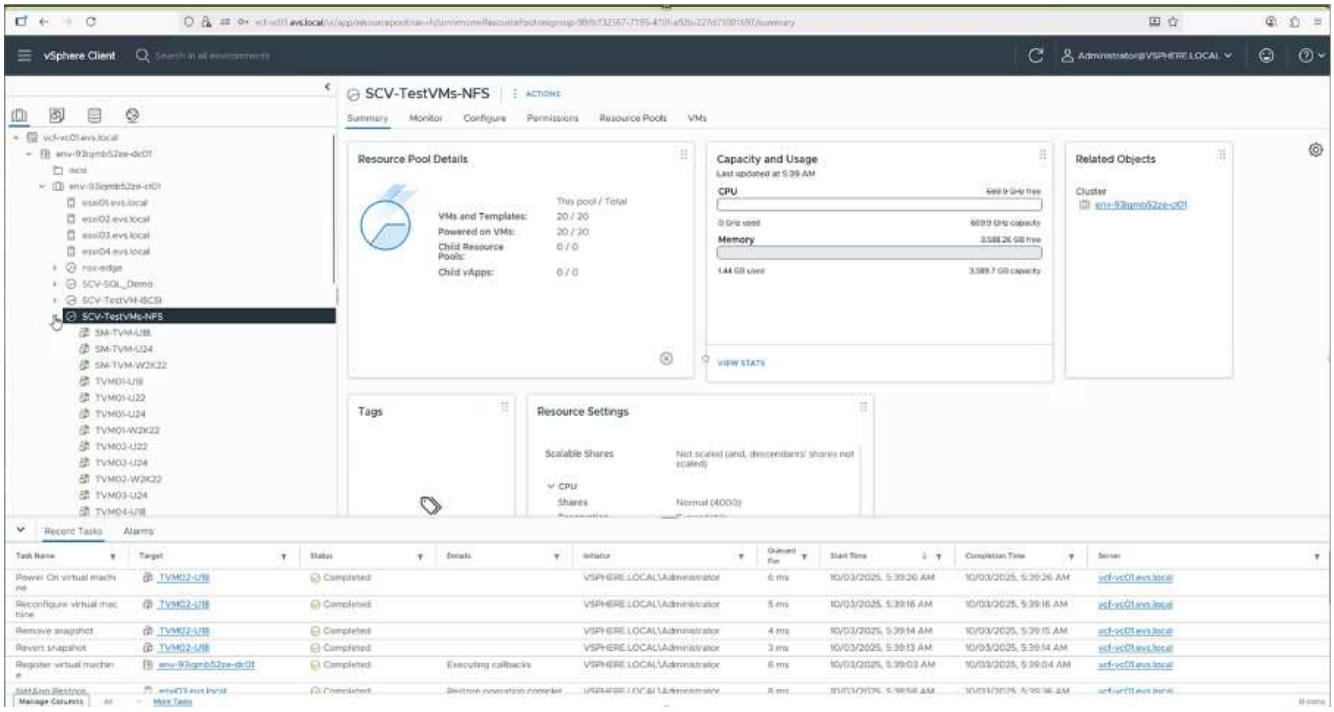
3. 在"Select Scope page"页面，在"Restore scope"字段中选择"Entire Virtual Machine"，然后选择"Restore location"，并输入应挂载备份的目标 ESXi 信息。
4. 如果还原操作后需要打开虚拟机，请启用"Restart VM"复选框。
5. 在"Select Location page"页面上，选择一个主要位置。



6. 查看"摘要"页面，然后选择"完成"。



7. 通过选择屏幕底部的"最近任务"来监控操作进度。



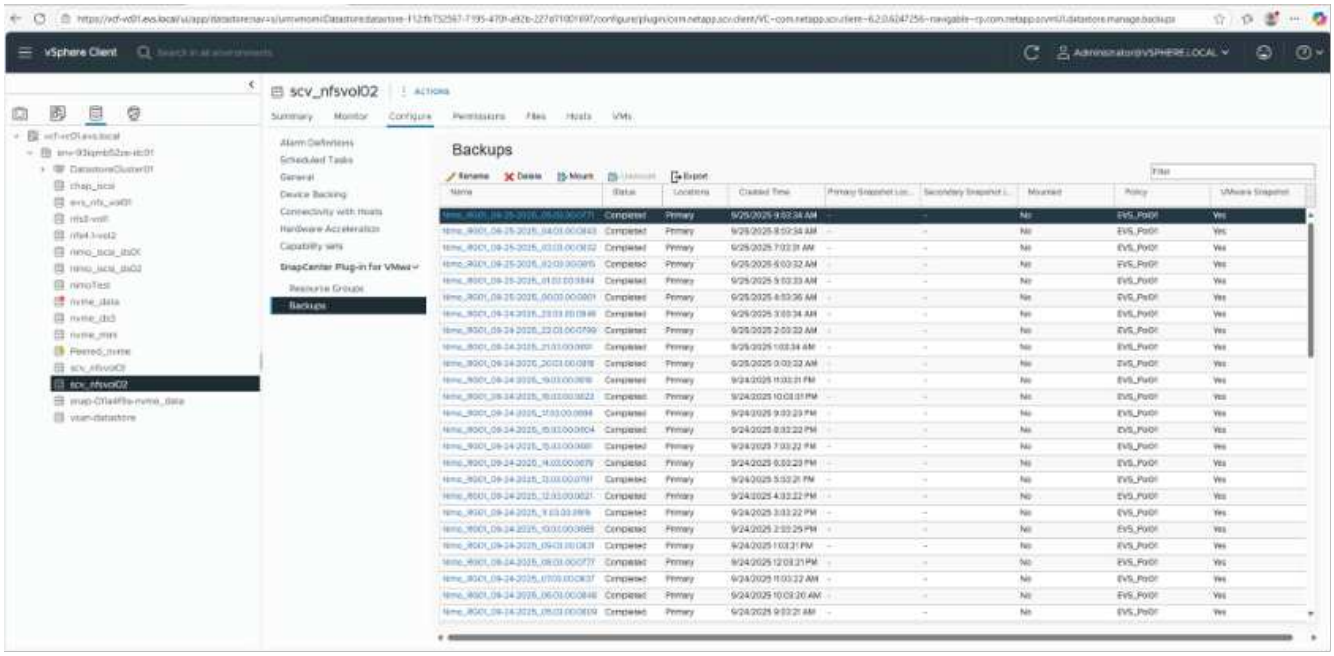
虽然 VM 已还原，但它们不会自动添加到以前的资源组中。如果要保护这些 VM，请将其手动添加到相应的资源组。

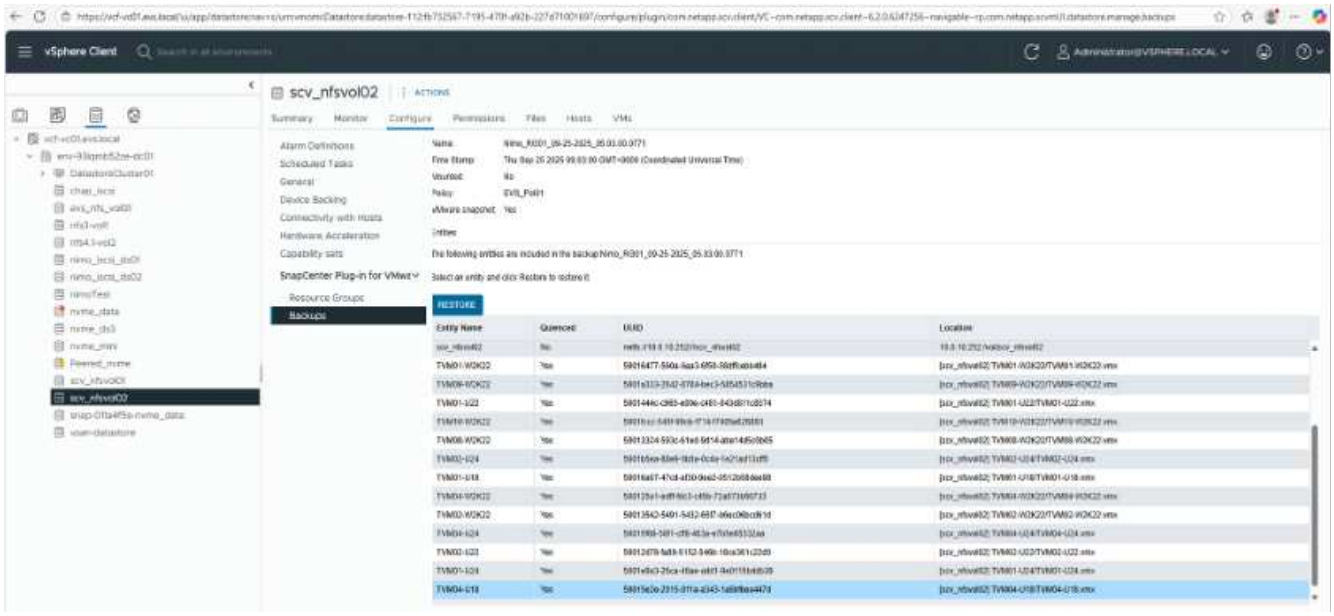
还原操作也可以从单个 VM 级别触发。

使用 SCV 还原已删除的虚拟机是一个简单的过程。

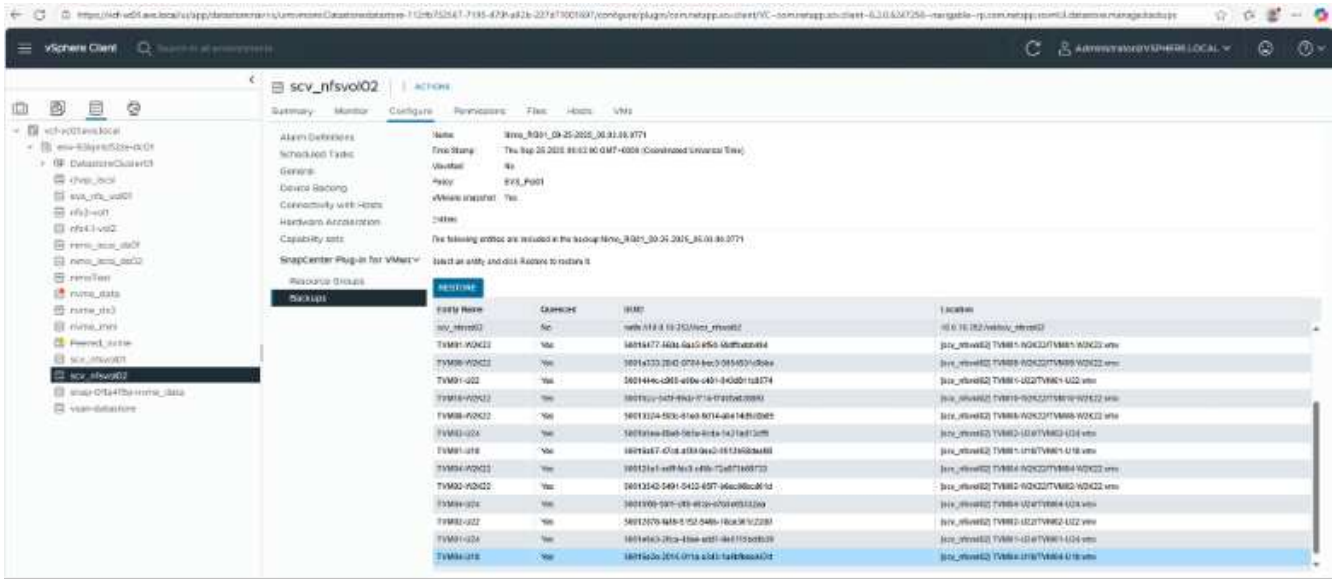
可从数据存储级别执行已删除 VM 的恢复操作。

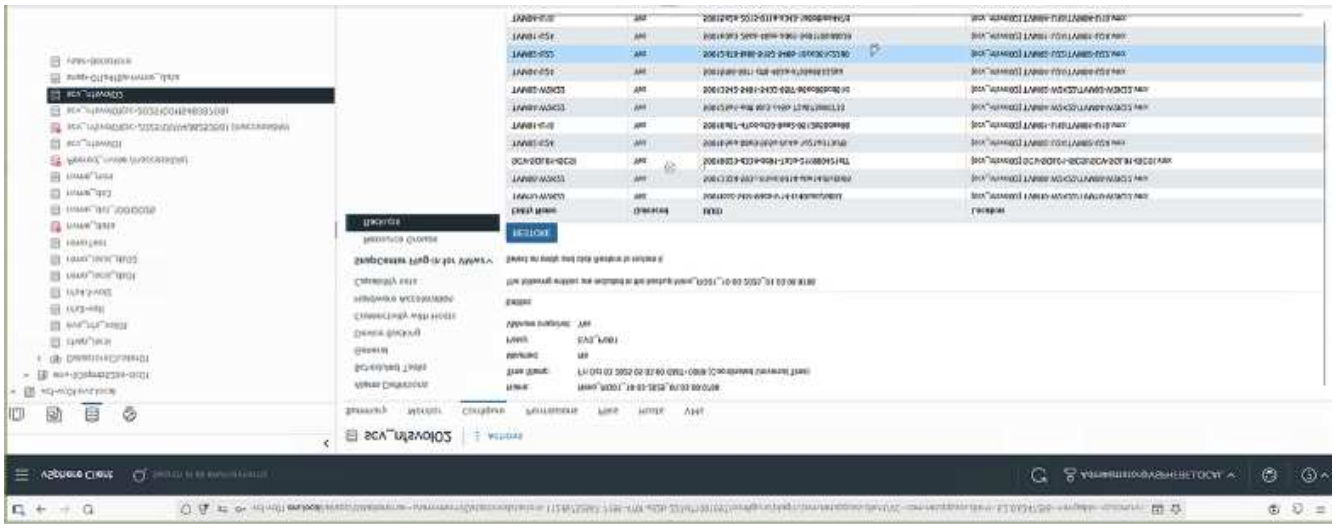
1. 转到相应的 Datastore > Configure > Backups。在那里，选择已删除的虚拟机，然后选择"Restore"。

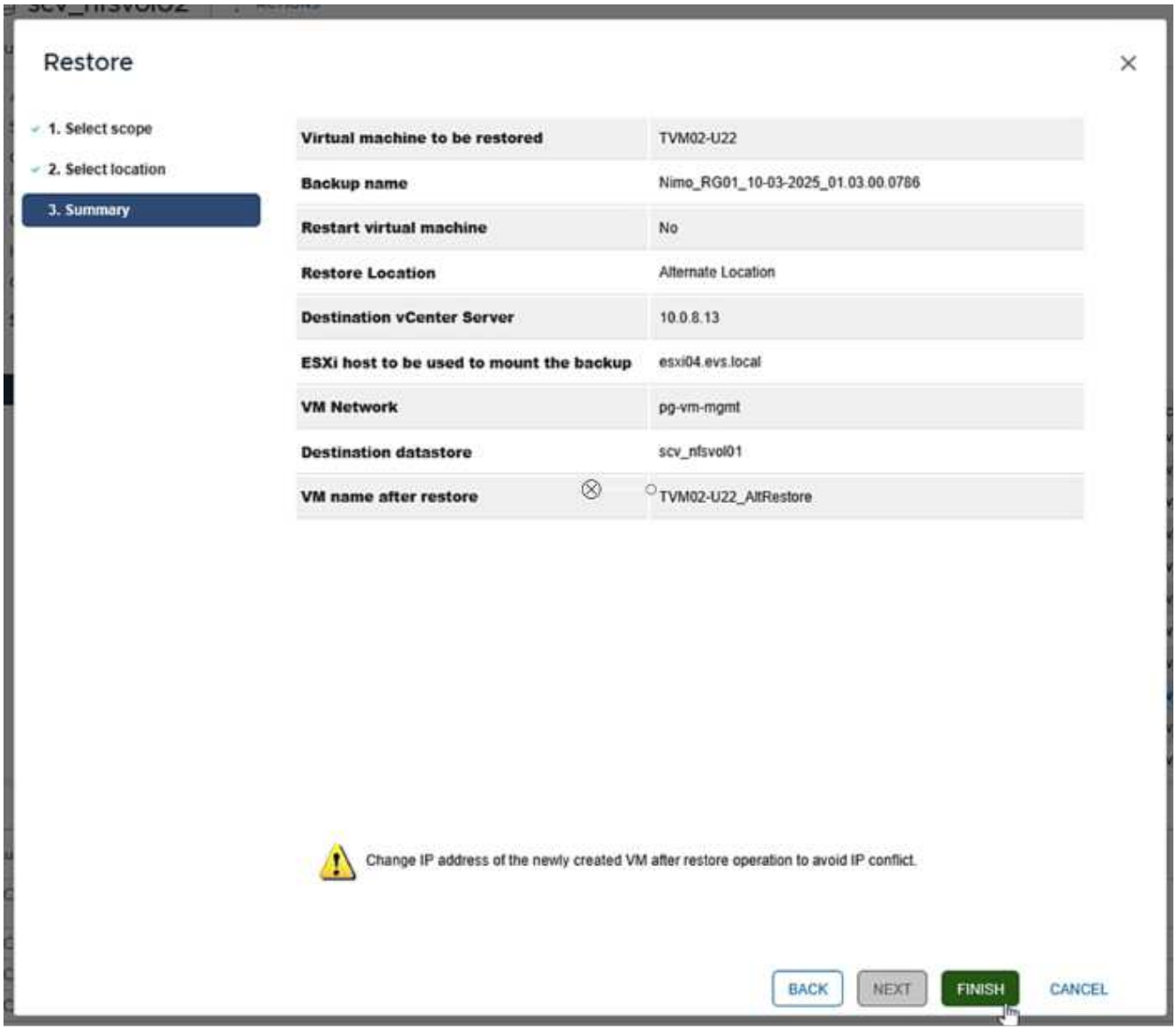


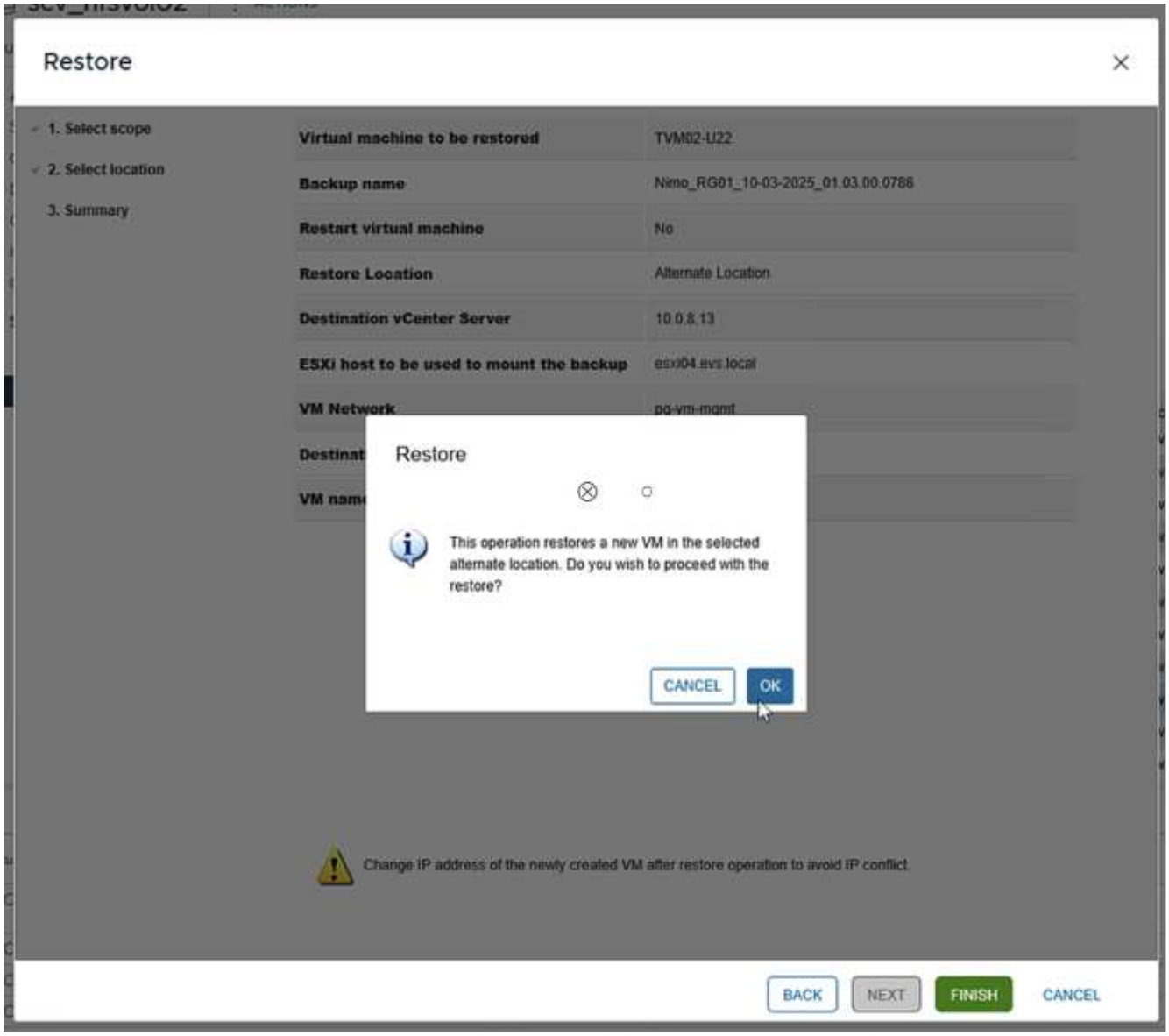


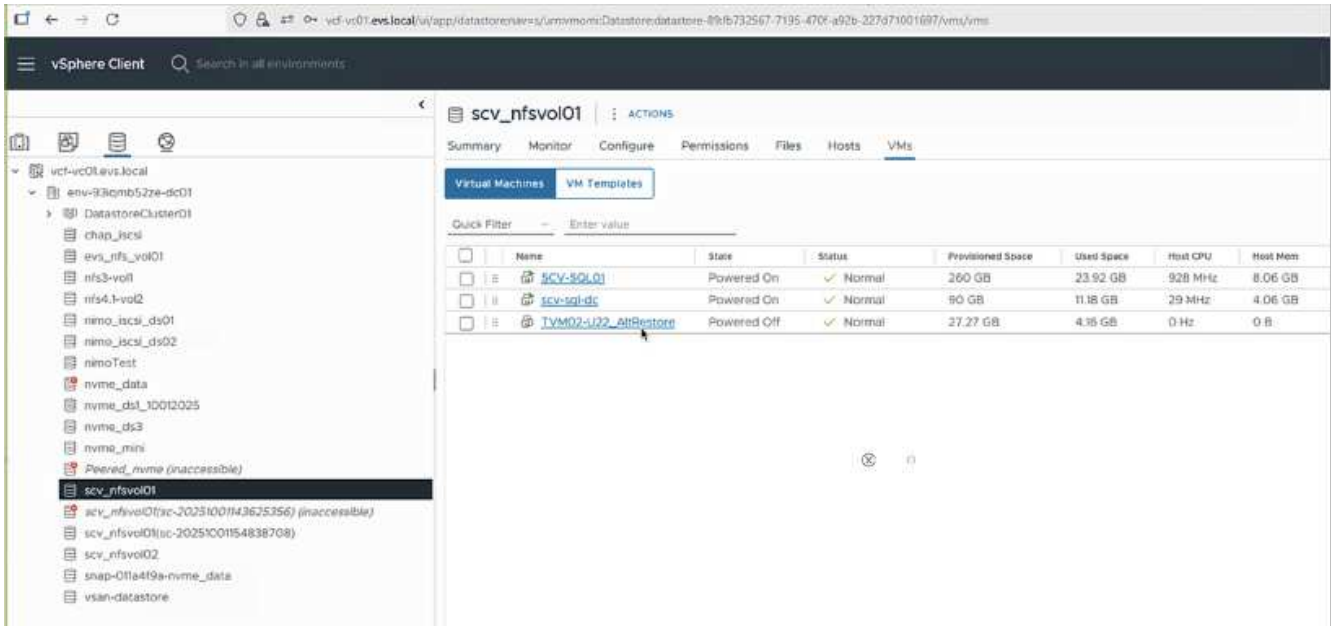
2. 下面的屏幕截图流程涵盖了将虚拟机恢复到备用 ESXi 主机和不同数据存储库的过程。


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE


vSphere Client
scv_nfsvol02
RESTORE


Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

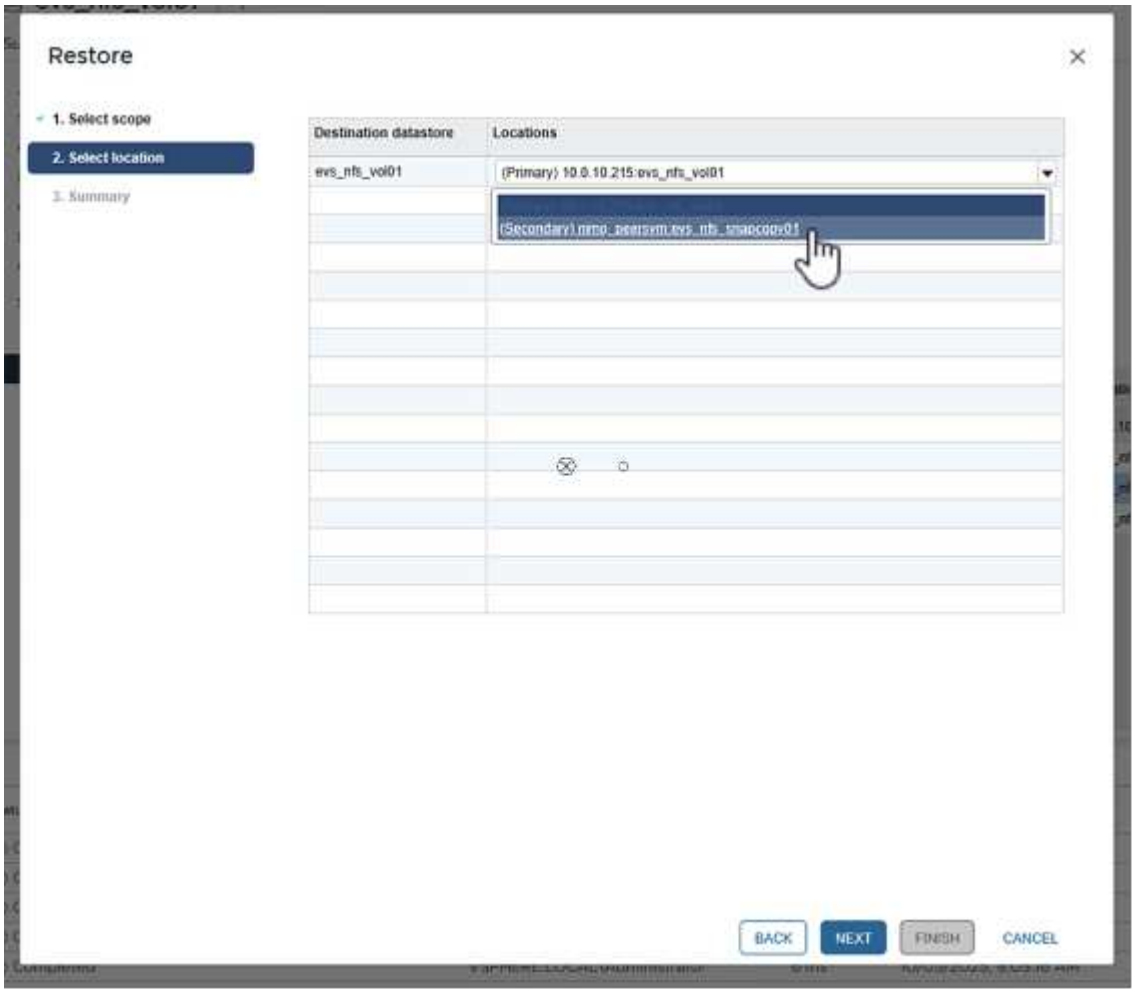

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

目标数据存储区必须具有足够的可用空间，并且在"还原到备用位置"字段中指定的 vCenter 必须是 DNS 可解析的。

为提高 NFS 环境中的还原效率，请启用 VMware vStorage API for Array Integration (VAAI)。

还原也可以从辅助位置（如 SnapMirror 目标）执行。



+

受适用于 **VMware** 的 **SnapCenter** 插件保护的来宾文件和文件夹的还原过程

以下部分演示如何从 VMDK 还原来宾文件和文件夹。

SnapCenter 仅在来宾操作系统为 Windows 时才支持从 VMDK 还原文件和文件夹。

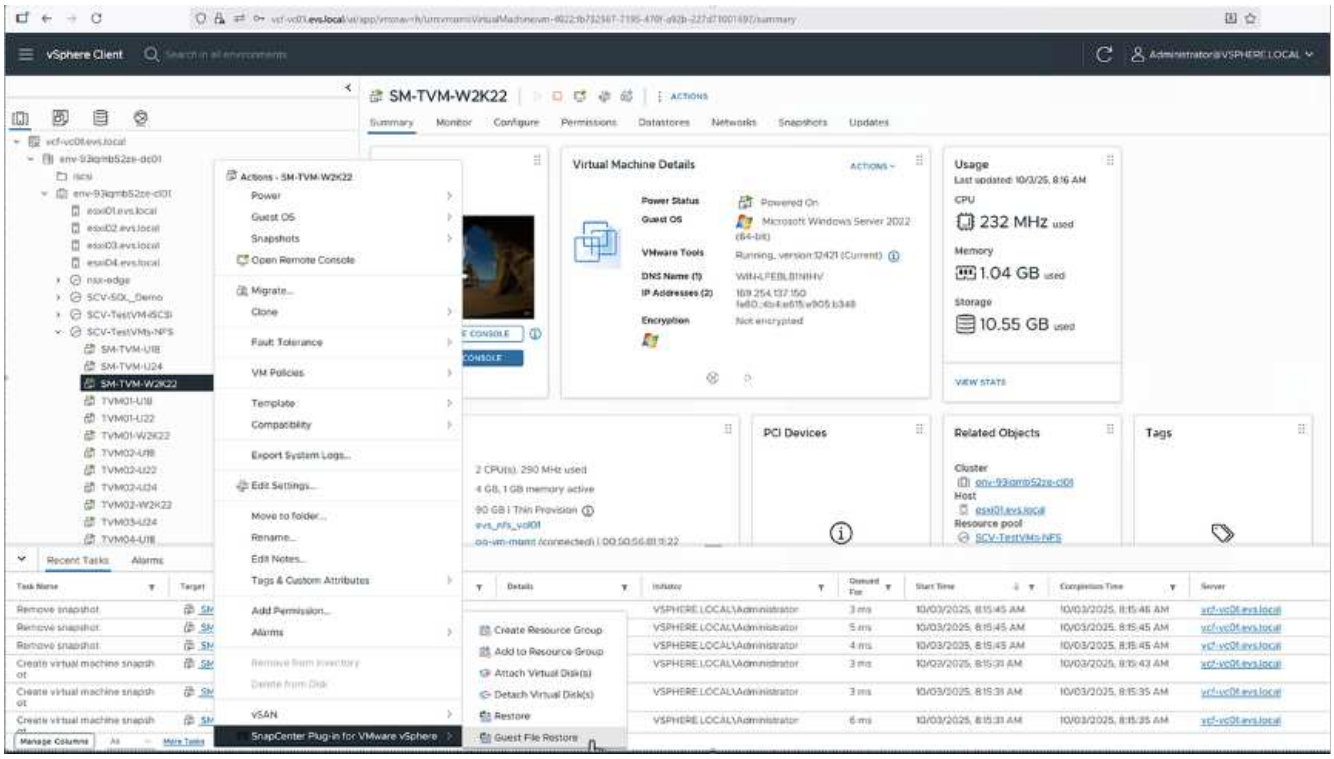
使用 SCV 还原访客文件和文件夹的注意事项：

- VMware 工具必须在 VM 上运行。
- 默认情况下，附加的 VMDK 可访问 24 小时。
- 一次只能在虚拟机上执行一个还原或附加操作。
- 可以还原系统、隐藏和加密文件，但不会保留其原始属性。

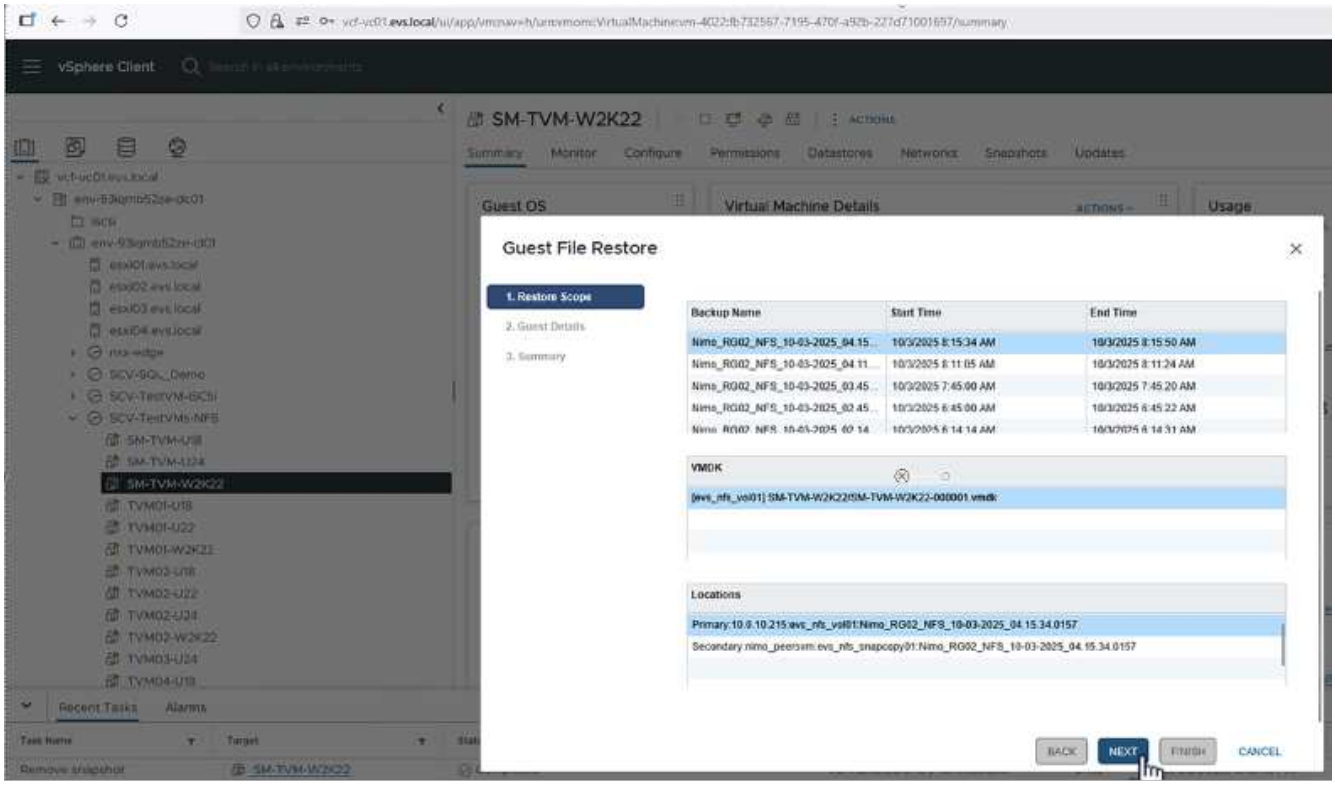
- 避免将加密文件还原到加密文件夹或覆盖系统文件。

还原来宾文件和文件夹的步骤：

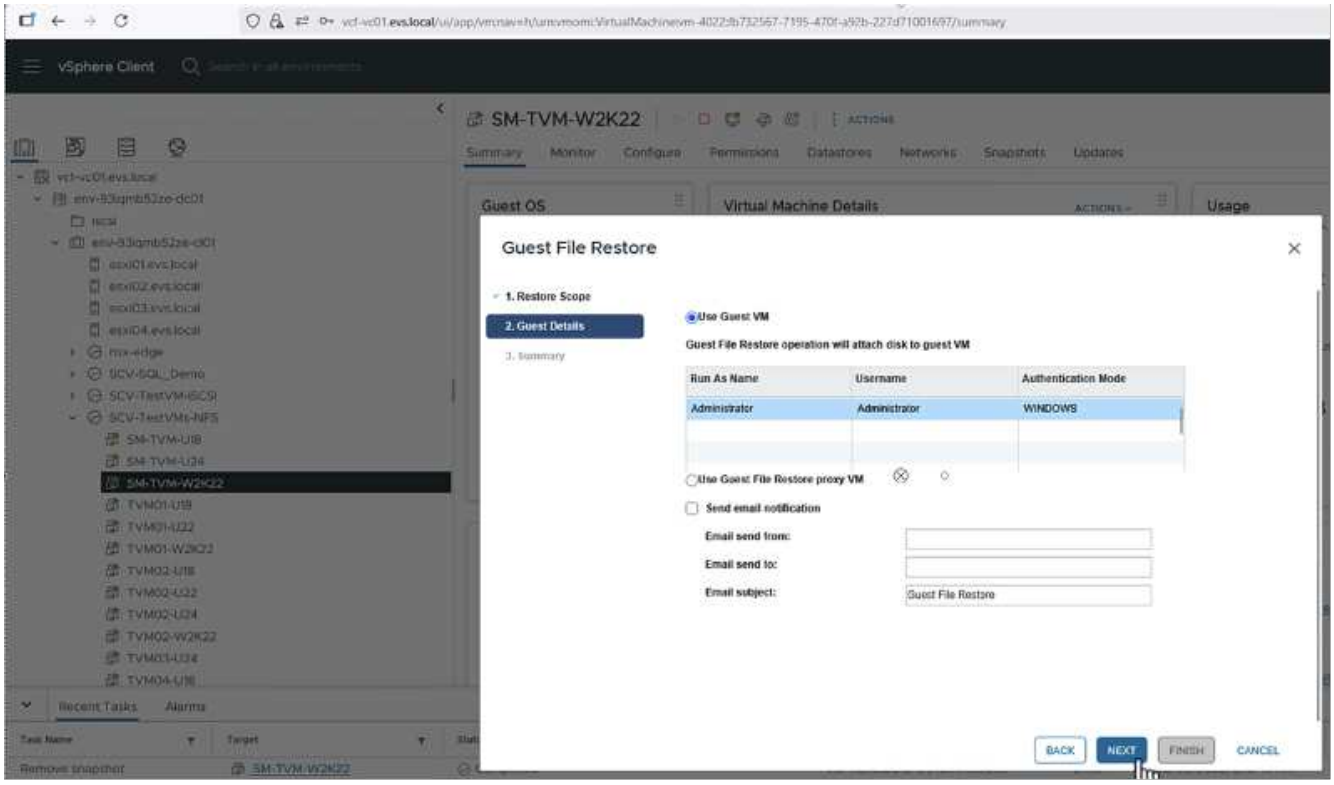
1. 右键单击目标虚拟机并选择**NetApp SnapCenter › Guest File Restore**。



2. 选择包含所需 VMDK 的备份。指定 VMDK 及其位置（主要或次要）。

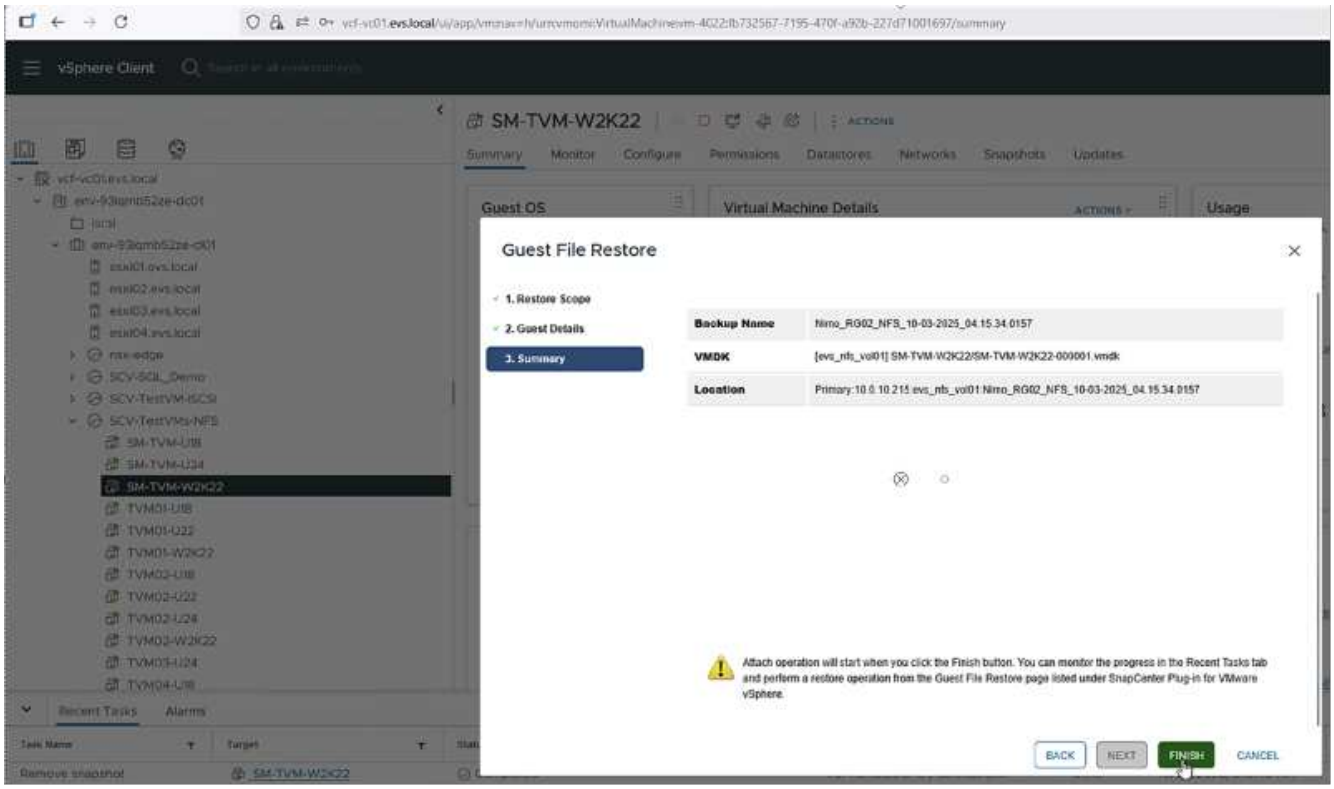


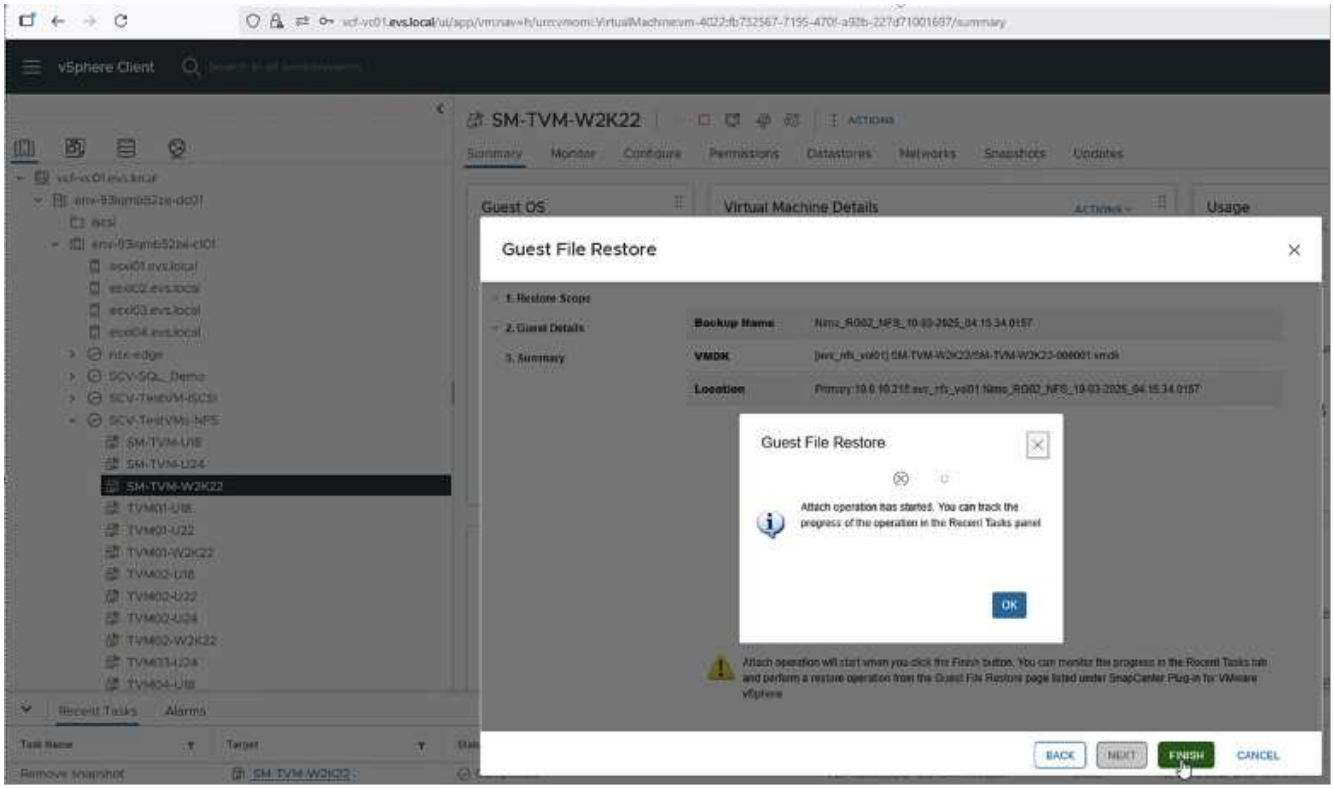
3. 选择"磁盘连接方法"。



- 来宾 VM 选项：将磁盘连接到原始 VM（需要预配置的凭据）。这是本演示中使用的选项。
- 代理 VM 选项：将磁盘连接到指定的代理 VM（必须预先配置）。

4. 等待附加操作完成，然后浏览和还原文件。操作完成后，SnapCenter 会自动创建来宾文件还原会话。





5. 在来宾文件还原会话中浏览到 VMDK，选择所需的文件或文件夹，并将其还原到指定位置。

使用 **SnapCenter for SQL (SCSQL)** 在 **VMware VMDK** 上运行的数据库的保护过程

以下部分展示了如何使用 SnapCenter for SQL (SCSQL) 保护在 VMware VMDK 上运行的数据库。

设置 **SCSQL**

使用 SCSQL 保护 VMDK 上的数据库的设置如下：

1. "安装和配置" SnapCenter 服务器。
2. 登录到 SnapCenter。
3. 配置 SnapCenter 环境：
   - "添加或分配" 存储系统连接。
   - "创建" 凭据。
4. 对于 VMware VMDK 上的 Microsoft SQL Server 数据库：
   - "部署 SCV" （已在设置部分中介绍）。
   - 向 SnapCenter 注册插件。
5. 添加 "SQL Server 主机和安装插件"：
   - "配置 SQL 插件"。
   - "配置数据库和日志的保护计划和调度"。

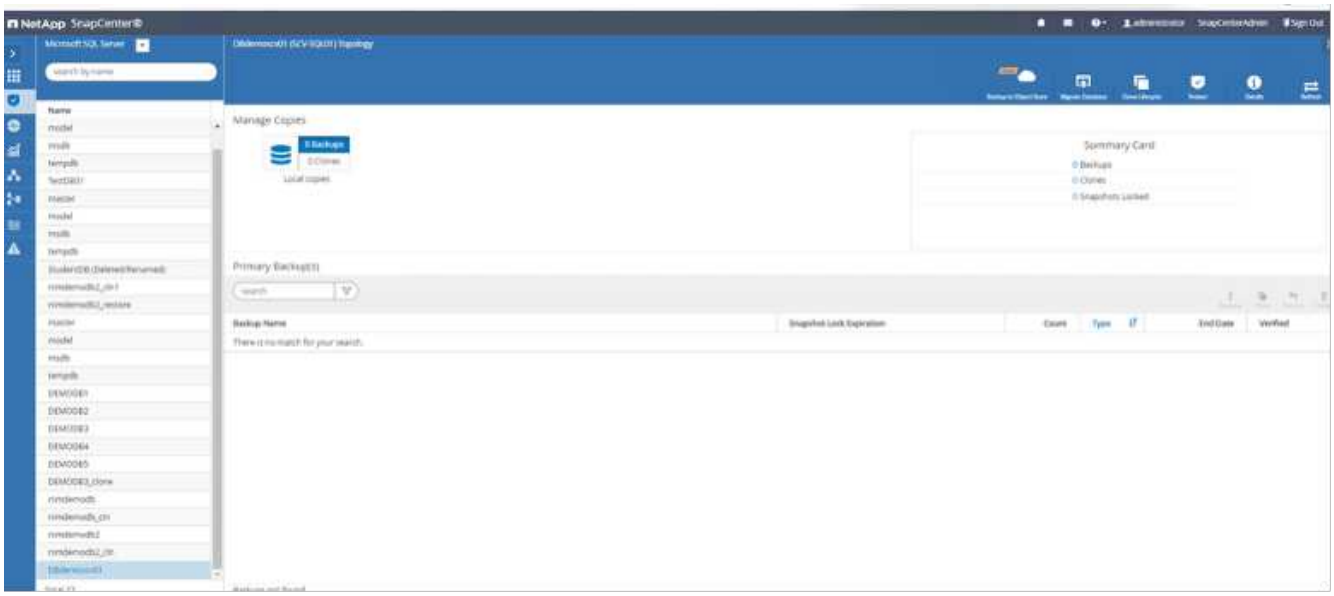


设置备份策略

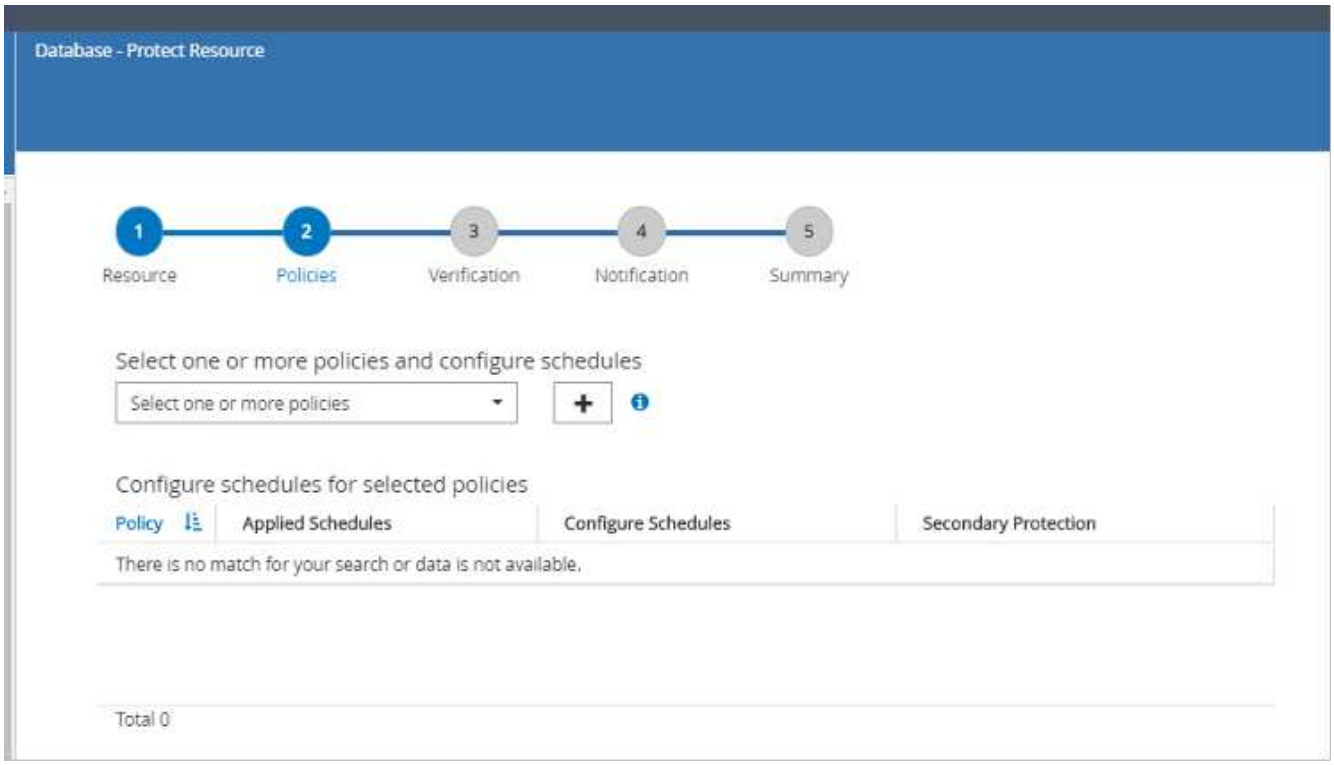
以下步骤将演示如何设置备份策略。

1. 从资源选项卡中选择数据库，然后从右上角选择"保护"。

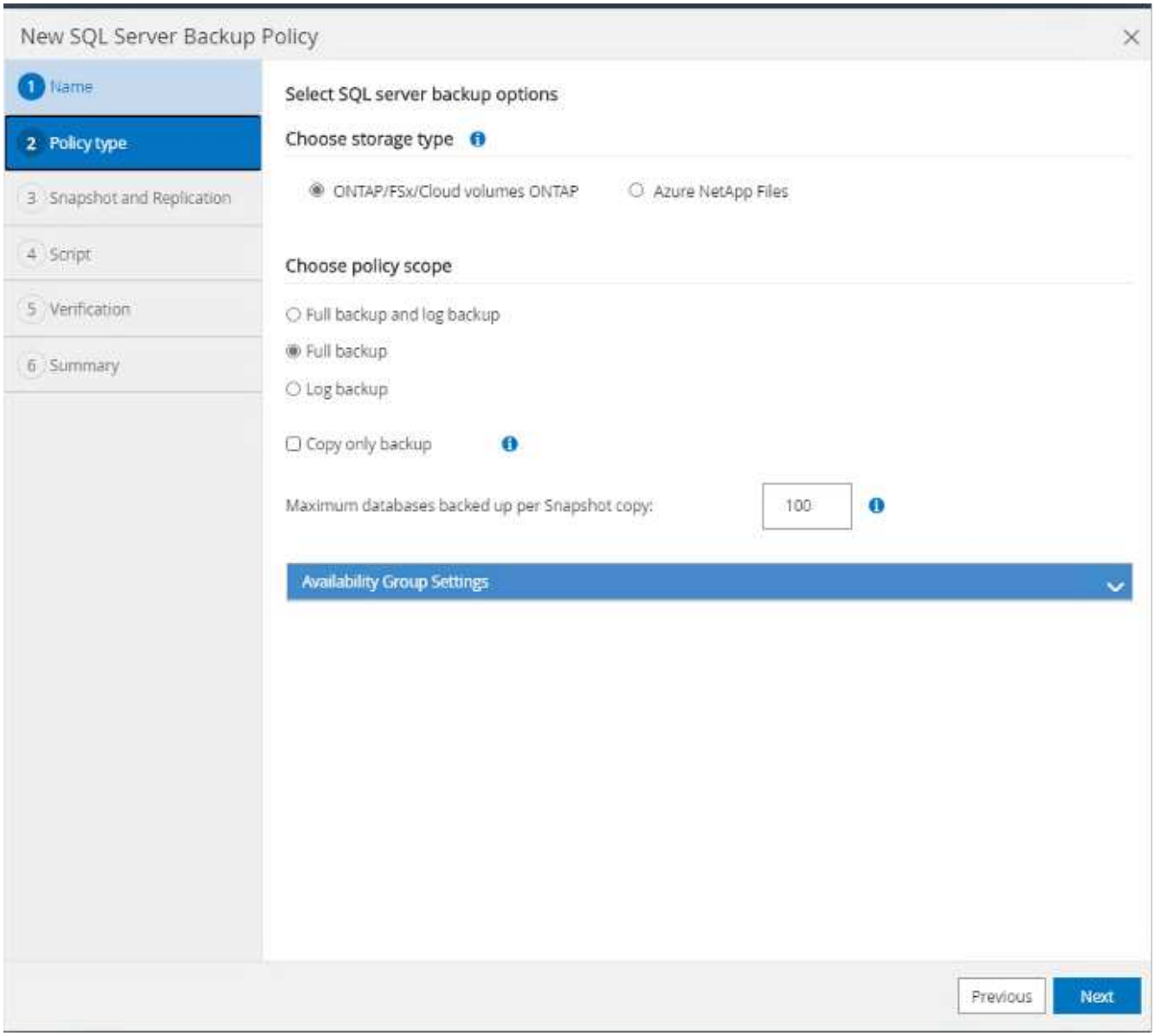
   对来宾虚拟机上运行的 SQL Server 数据库执行验证。



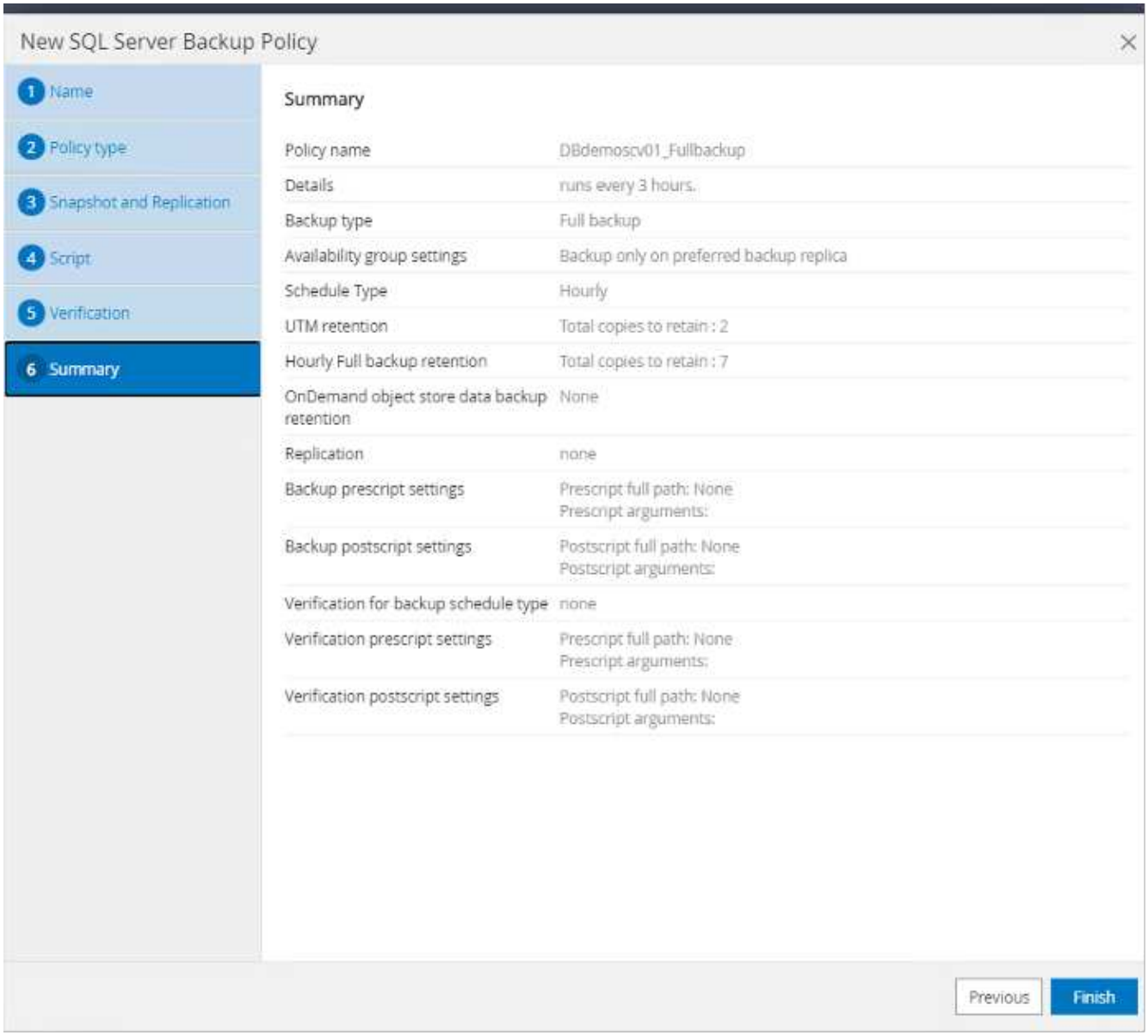
2. 单击加号图标以配置 SQL Server 备份策略。



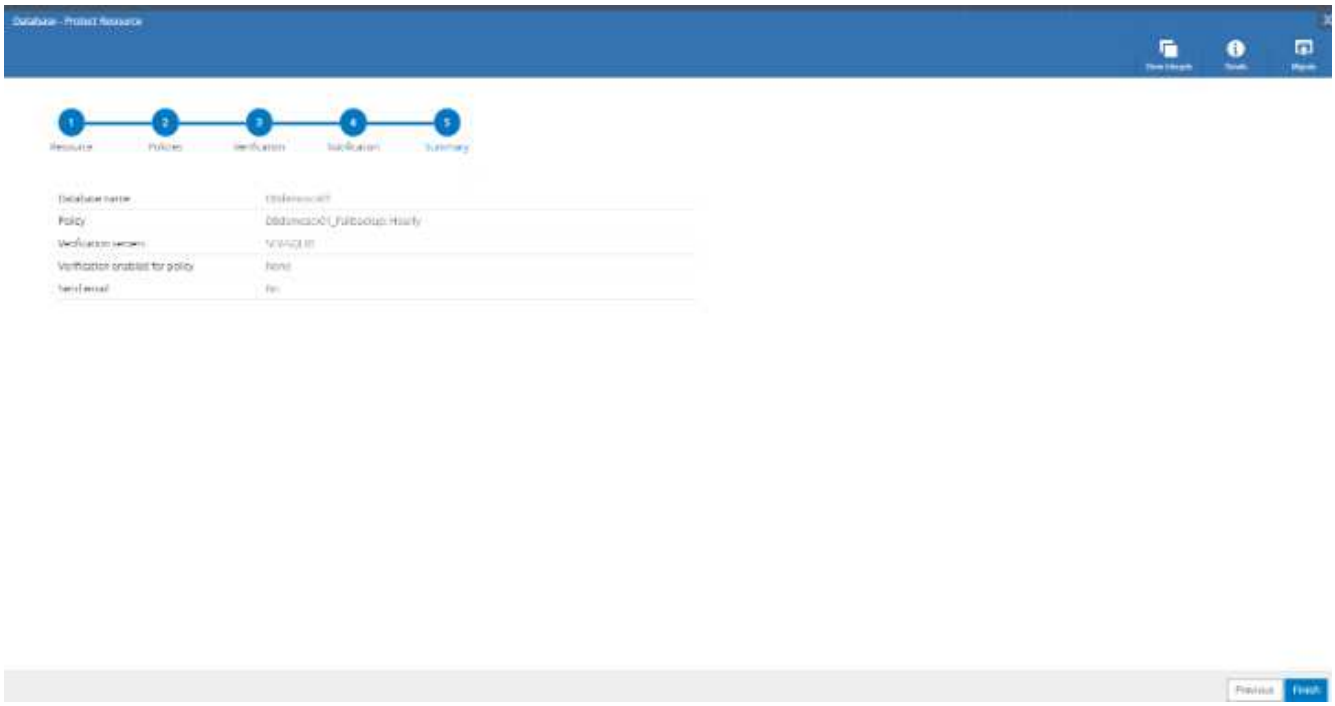
3. 在此演示中，选择"完全备份"。选择"下一步"以继续。



4. 在摘要页面上，选择 "Finish"。


New SQL Server Backup Policy
1 Name
2 Policy type
3 Snapshot and Replication
4 Script
5 Verification
6 Summary
Summary
Policy name
DBdemoscv01_Fullbackup
Details
runs every 3 hours.
Backup type
Full backup
Availability group settings
Backup only on preferred backup replica
Schedule Type
Hourly
UTM retention
Total copies to retain : 2
Hourly Full backup retention
Total copies to retain : 7
OnDemand object store data backup retention
None
Replication
none
Backup prescript settings
Prescript full path: None
Prescript arguments:
Backup postscript settings
Postscript full path: None
Postscript arguments:
Verification for backup schedule type
none
Verification prescript settings
Prescript full path: None
Prescript arguments:
Verification postscript settings
Postscript full path: None
Postscript arguments:
Previous
Finish

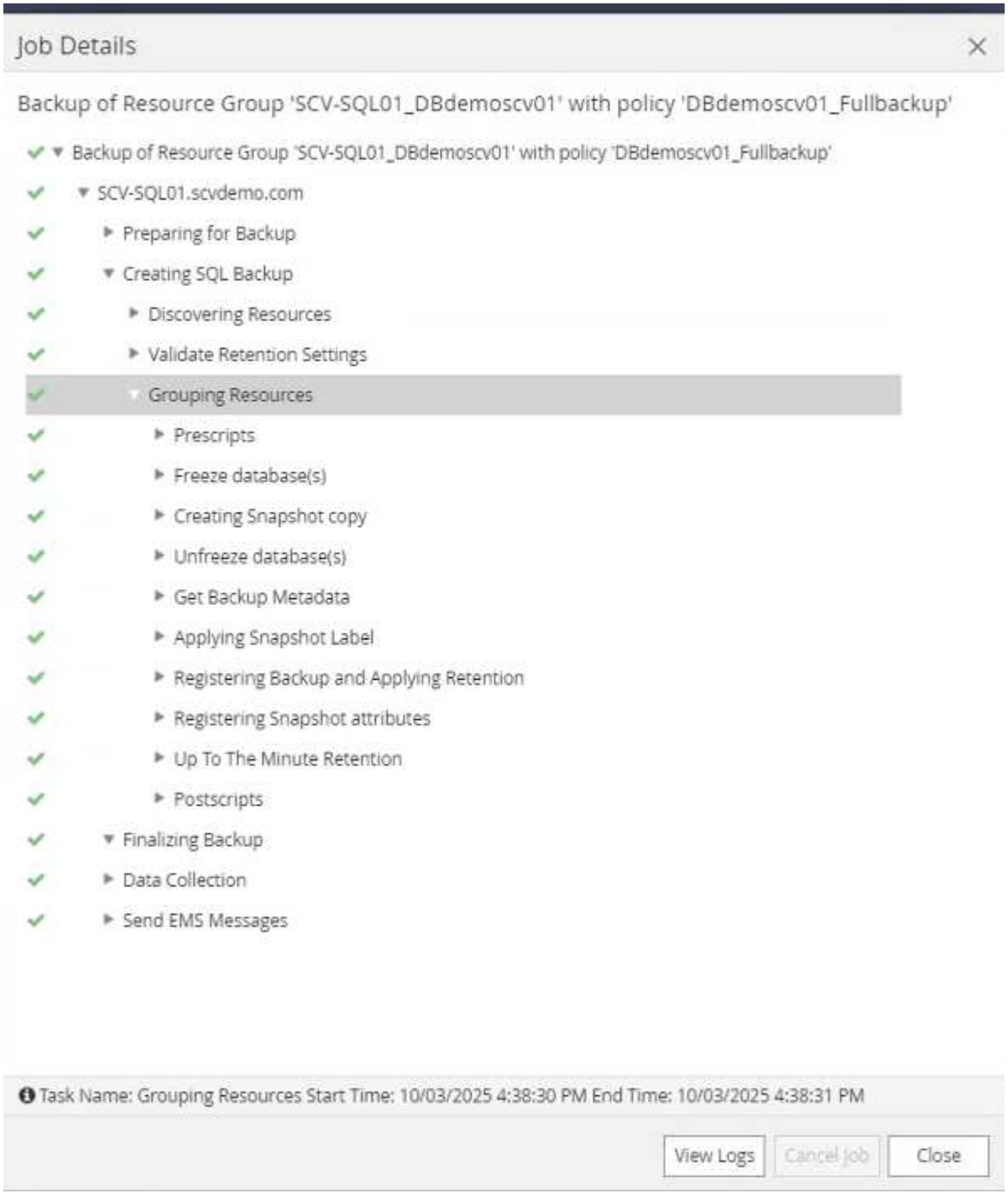
5. 继续执行"完成"。



监控备份

设置备份策略后，您可以在备份操作发生时对其进行监控。您可以通过单击"立即备份"以触发按需备份操作或等待计划备份策略启动来执行此操作。

1. 使用监控 › 作业监控作业进度。
2. 选择备份作业，然后单击"详细信息"以查看作业详细信息，如下所示。

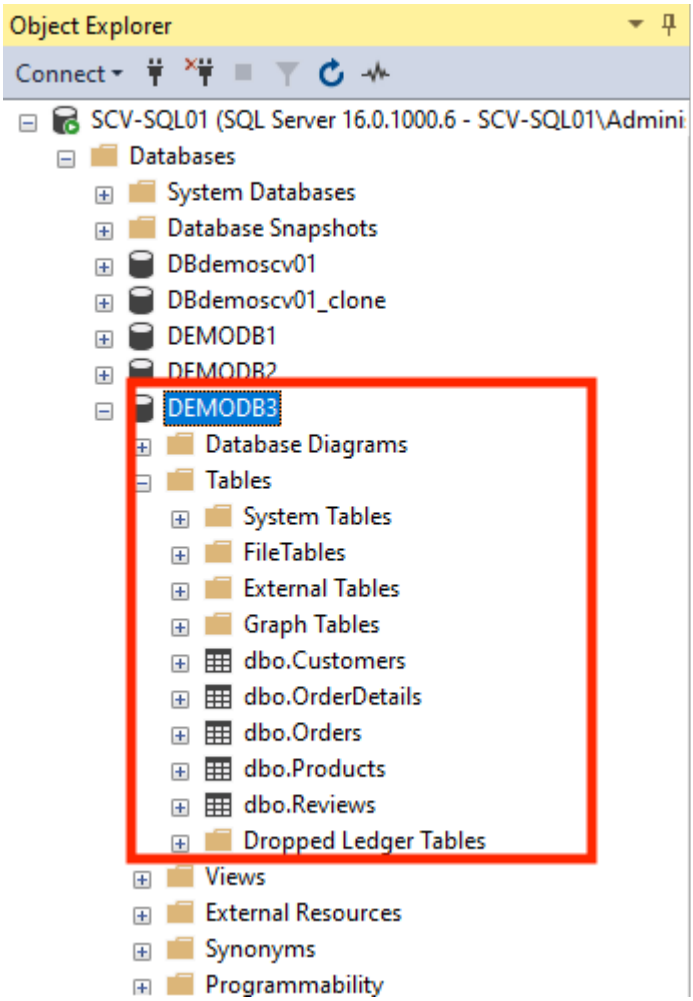


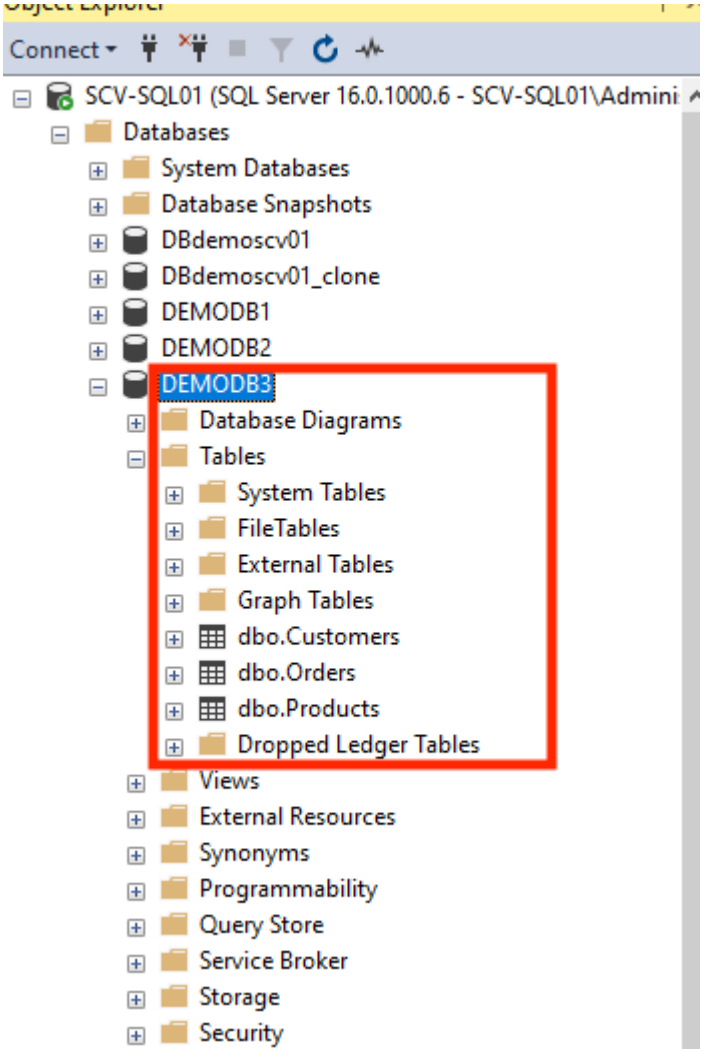
还原驻留在 **VMDK** 上的数据库

VMDK 上的数据库可以还原到特定时间点。

我们可以通过删除数据库中的一些表来模拟其重要性，然后通过执行时间点还原来更正这些表。

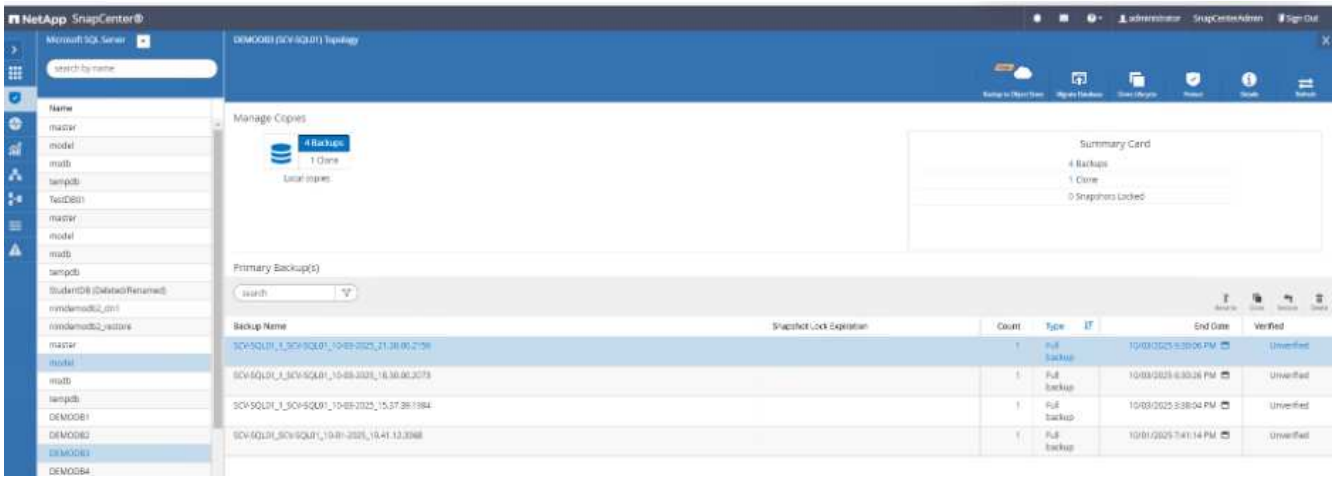
下面您可以看到，第一个屏幕截图中显示的数据库中的几个表在第二个屏幕截图中已被删除：


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

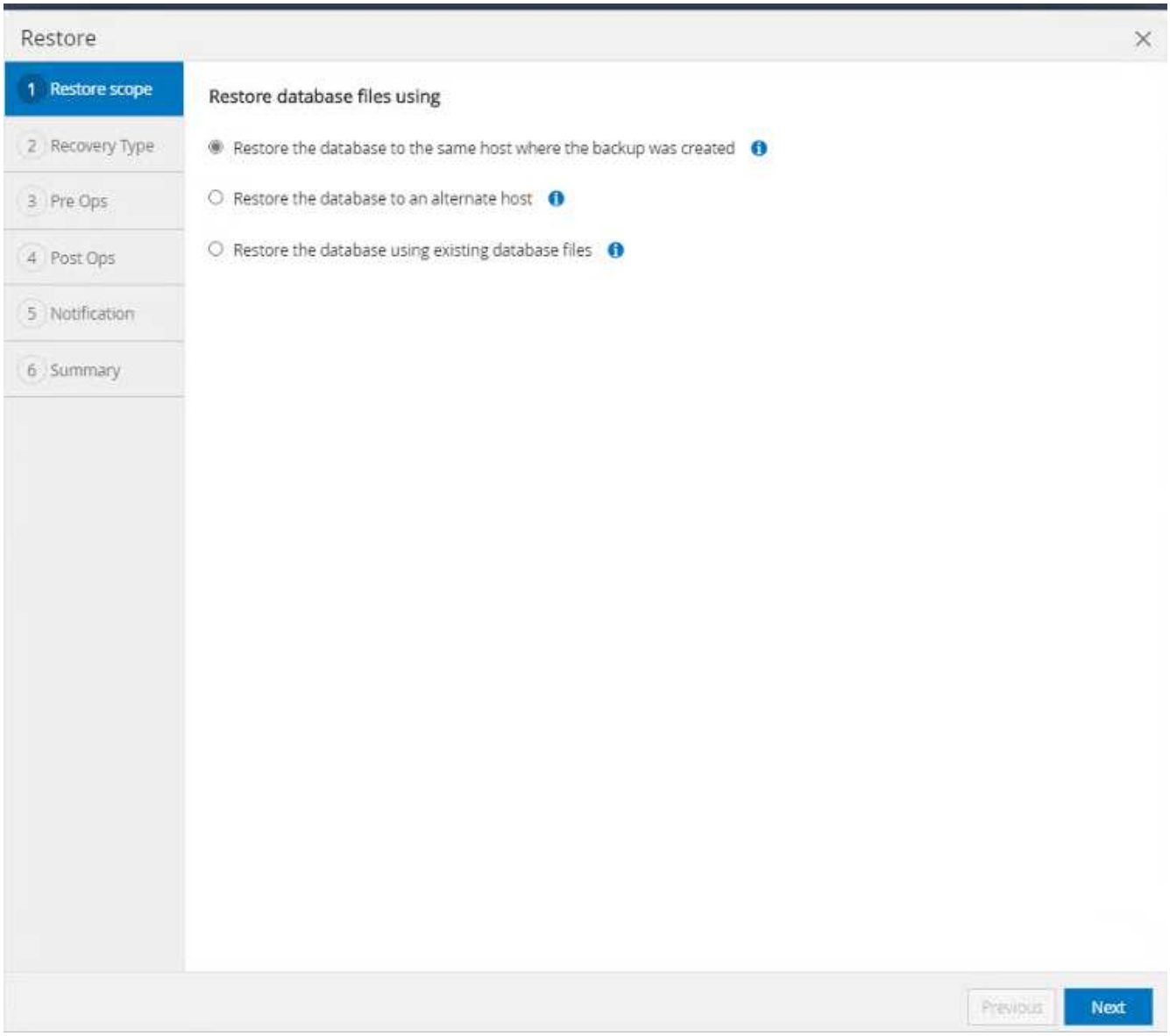


以下步骤演示如何执行还原以恢复这些已删除的表：

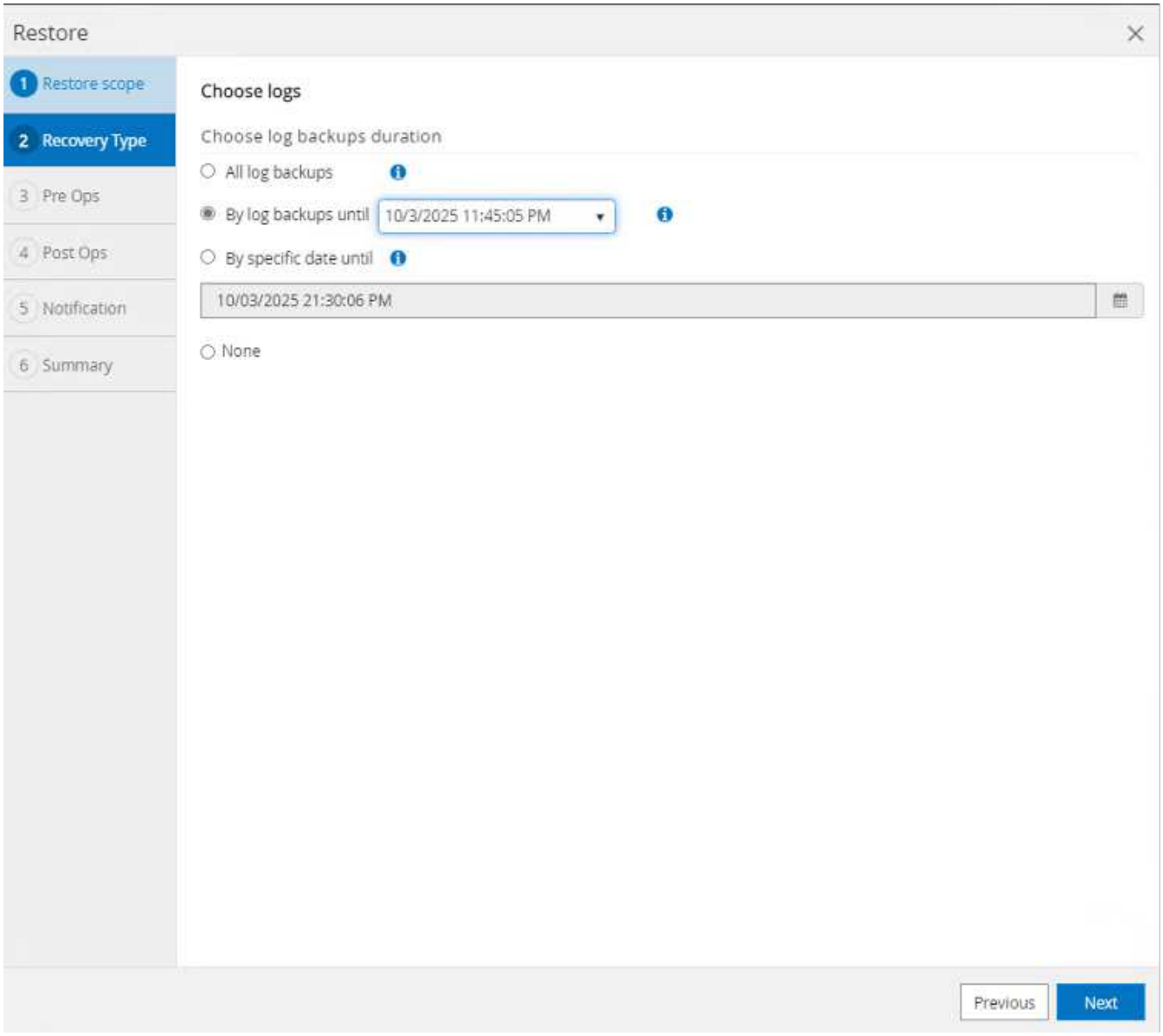
1. 从资源组中选择数据库。



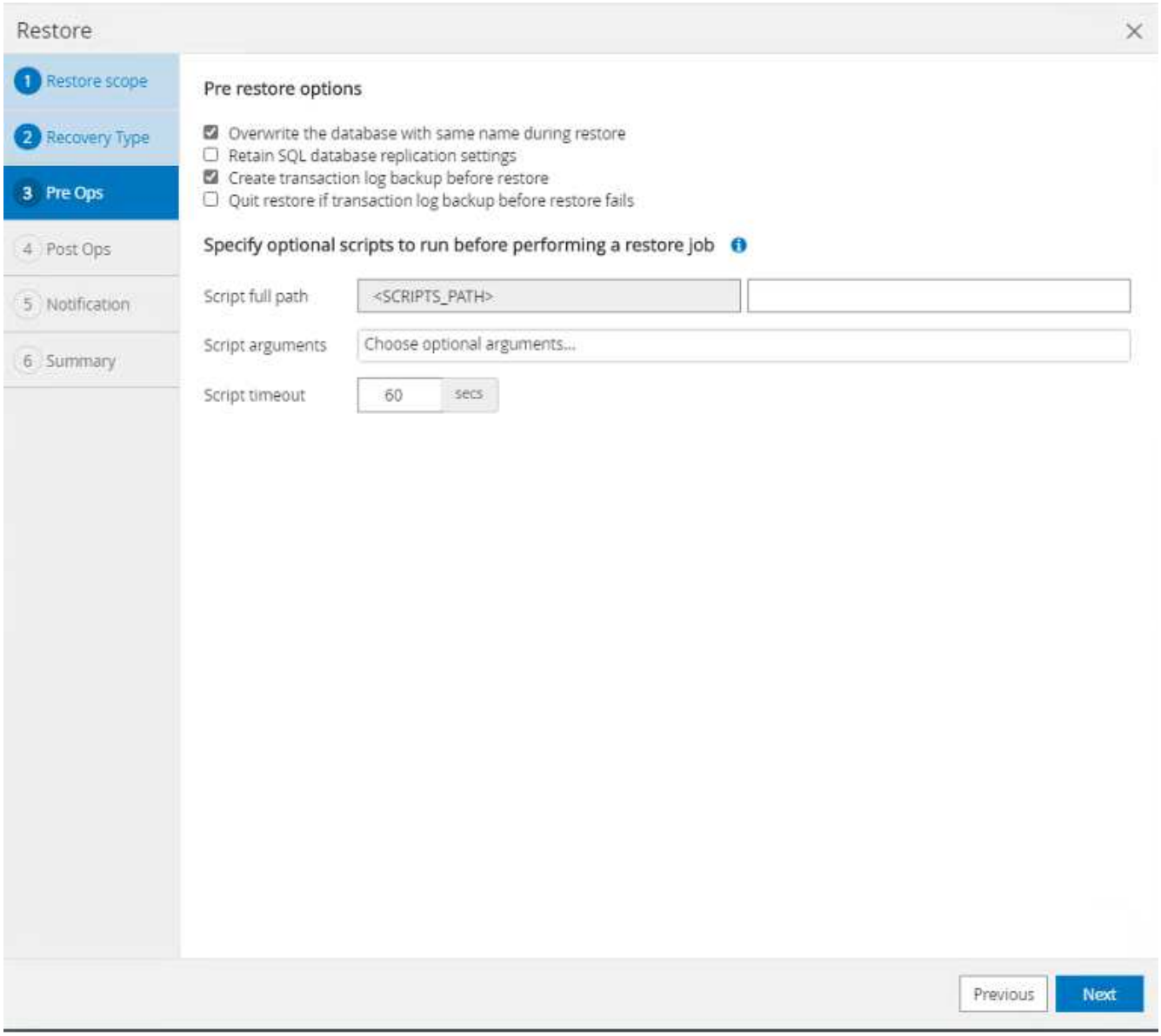
2. 在还原页面中，选择"将数据库还原到创建备份的同一主机"选项。



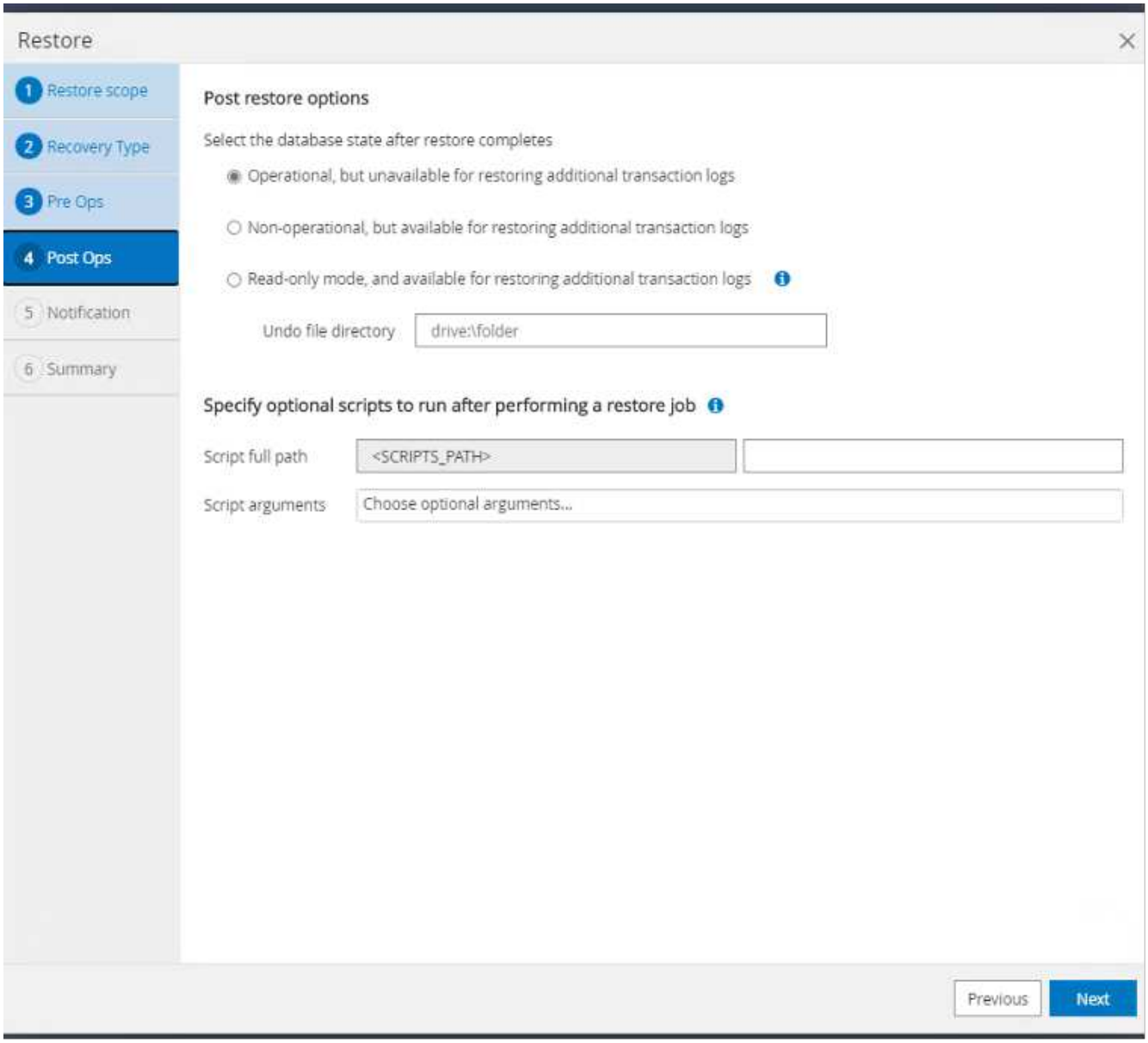
3. 选择使用日志备份到某个时间点的选项。



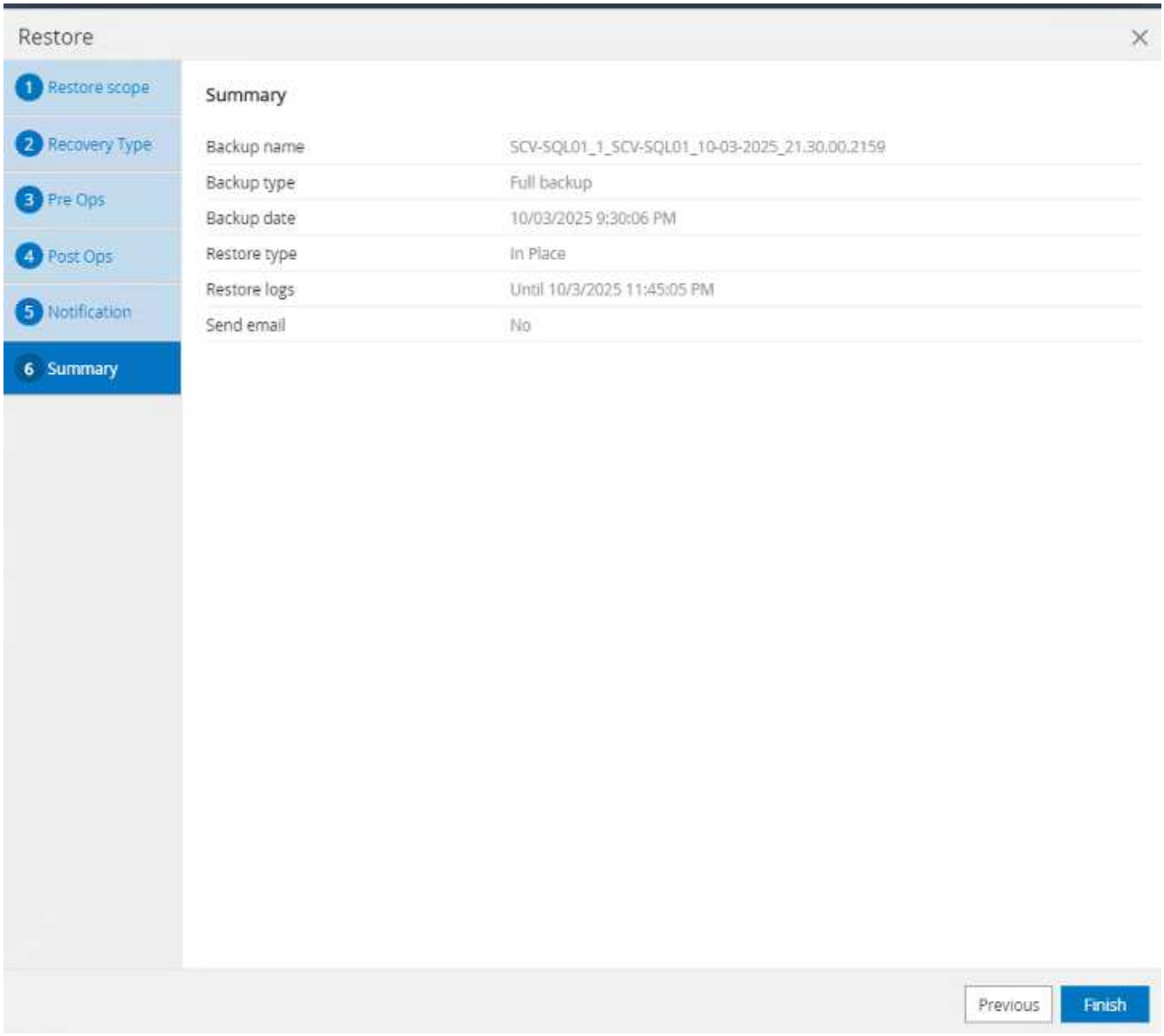
4. 选择 "Overwrite database with same name during restore, Create transaction log backup before restore"，然后选择 "Next"。



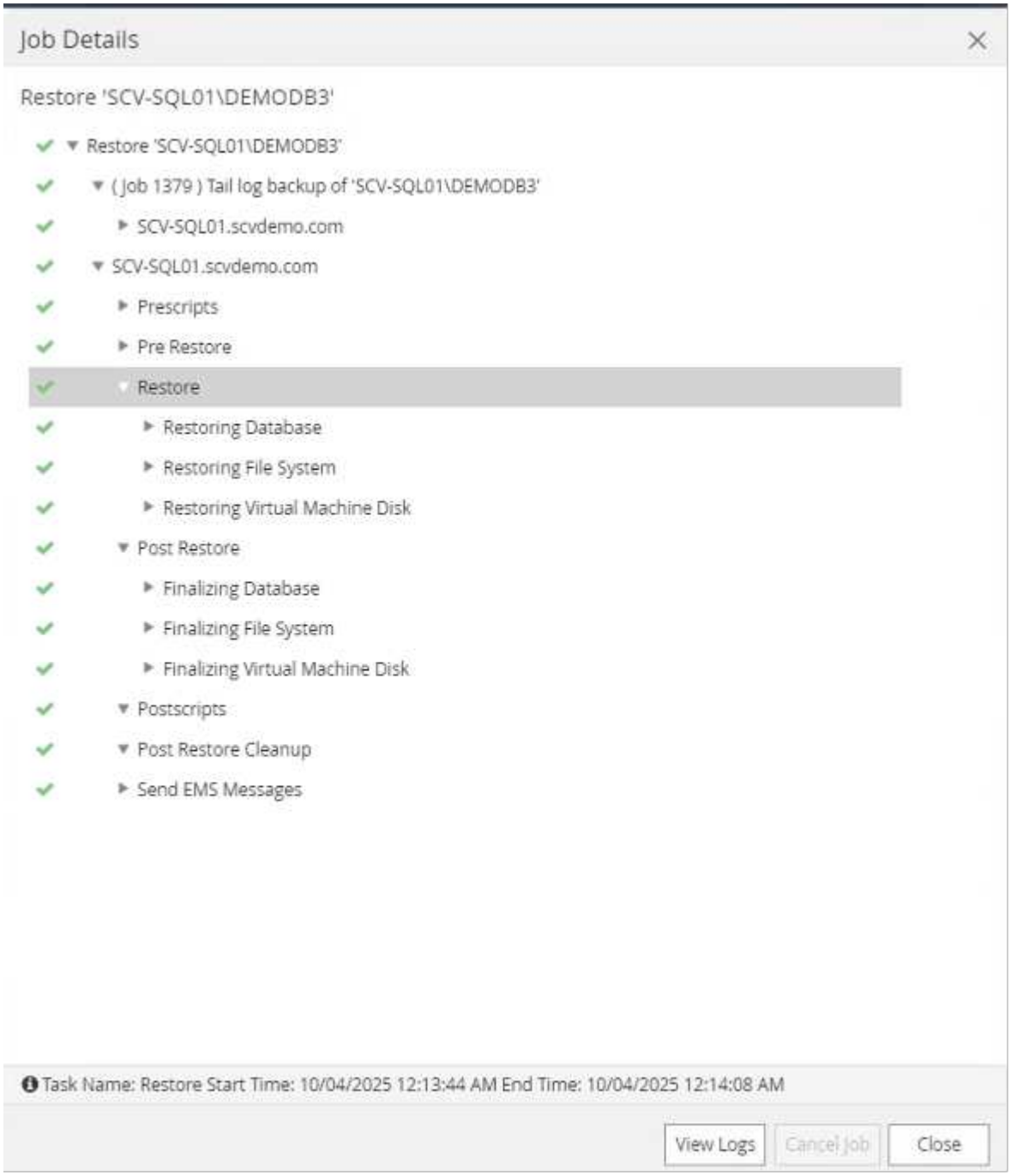
5. 从列表选项中选择您希望数据库假设的还原后状态，然后选择"下一步"。



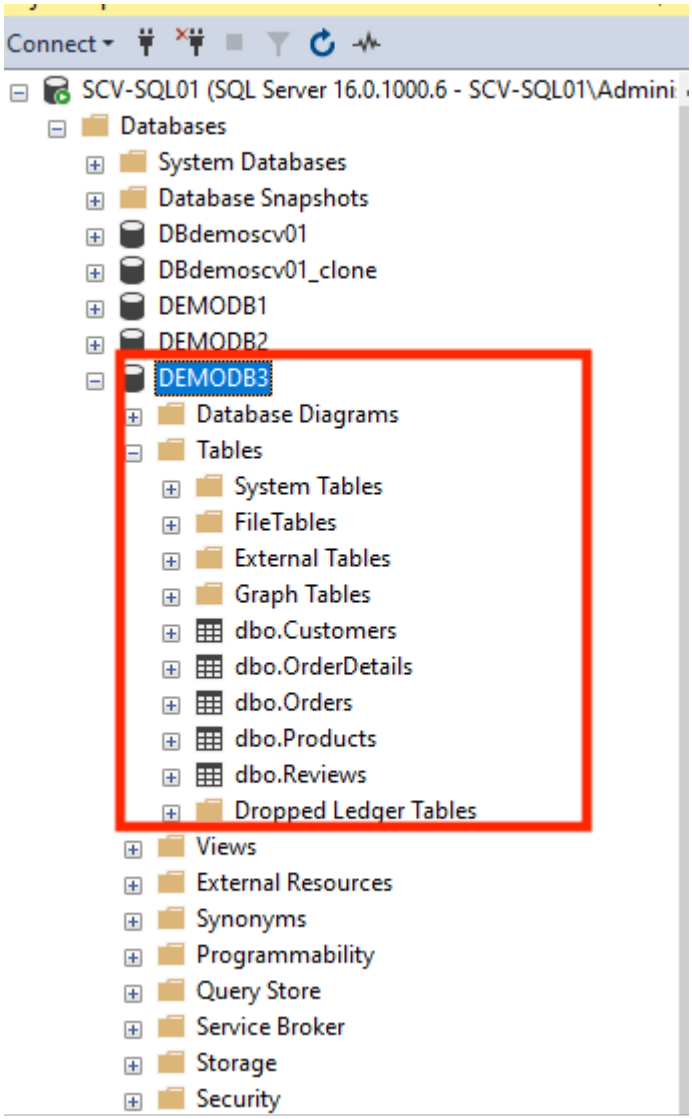
6. 在摘要页面上，选择"完成"。


Restore
1 Restore scope
2 Recovery Type
3 Pre Ops
4 Post Ops
5 Notification
6 Summary
Summary
Backup name
SCV-SQL01_1_SCV-SQL01_10-03-2025_21.30.00.2159
Backup type
Full backup
Backup date
10/03/2025 9:30:06 PM
Restore type
In Place
Restore logs
Until 10/3/2025 11:45:05 PM
Send email
No
Previous
Finish

7. 监控作业直至完成。



8. 验证已删除的表是否已成功还原。



结束语

在本文档中，我们提供了部署、配置和使用 SCV 和"SnapCenter Plug-in for SQL Server （SCSQL）"的详细分步指导，同时使用 FSx for ONTAP 作为 Amazon EVS 集群的补充数据存储区。

结束语

总而言之，当使用 FSx for ONTAP 优化 Amazon EVS 部署的 TCO 时，SCV 为备份虚拟机提供了一种简单高效的方法。它可以无缝快速地备份和恢复虚拟机，因为它依赖于 Snapshot 副本，这些副本只需几秒钟即可完成。

"立即免费试用适用于 VMware 的 SnapCenter 插件"。

NetApp适用于 Azure/AVS

NetApp的 Azure AVS 功能

详细了解NetApp为 Azure VMware 解决方案 (AVS) 带来的功能 - 从NetApp作为来宾连接

存储设备或补充 NFS 数据存储到迁移工作流、扩展/爆发到云、备份/还原和灾难恢复。

通过选择以下选项跳转到所需内容的部分：

- "在 Azure 中配置 AVS"
- "NetApp的 AVS 存储选项"
- "NetApp /VMware 云解决方案"

在 **Azure** 中配置 **AVS**

与本地一样，规划基于云的虚拟化环境对于成功创建虚拟机和迁移的生产就绪环境至关重要。

本部分介绍如何设置和管理 Azure VMware 解决方案，并将其与用于连接NetApp存储的可用选项结合使用。

来宾内存储是将Cloud Volumes ONTAP连接到 Azure VMware 解决方案的唯一支持方法。

设置过程可分为以下步骤：

- 注册资源提供者并创建私有云
- 连接到新的或现有的 ExpressRoute 虚拟网络网关
- 验证网络连接并访问私有云

查看详细信息"AVS配置步骤"。

NetApp的 **AVS** 存储选项

NetApp存储可以在 Azure AVS 中以多种方式使用 - 既可以作为猜测连接，也可以作为补充 NFS 数据存储。

请访问"支持的NetApp存储选项"了解更多信息。

Azure 支持以下配置的NetApp存储：

- Azure NetApp Files(ANF) 作为来宾连接存储
- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- Azure NetApp Files(ANF) 作为补充 NFS 数据存储

查看详细信息"AVS 的来宾连接存储选项"。查看详细信息"AVS 的补充 NFS 数据存储选项"。

解决方案用例

借助NetApp和 VMware 云解决方案，许多用例都可以在 Azure AVS 中轻松部署。针对 VMware 定义的每个云区域都定义了这些用例：

- 保护（包括灾难恢复和备份/还原）
- 延长
- 迁移

"浏览适用于 Azure AVS 的NetApp解决方案"

保护 **Azure/AVS** 上的工作负载

使用 **ANF** 和 **JetStream** 进行灾难恢复

云端灾难恢复是一种具有弹性且经济高效的方法，可以保护工作负载免受站点中断和数据损坏事件（例如勒索软件）的影响。使用 VMware VAIO 框架，可以将本地 VMware 工作负载复制到 Azure Blob 存储并进行恢复，从而实现最少或几乎无数据丢失以及接近零的 RTO。

JetStream DR 可用于无缝恢复从本地复制到 AVS 以及特别是Azure NetApp Files 的工作负载。它通过使用灾难恢复站点的最少资源和经济高效的云存储实现经济高效的灾难恢复。 JetStream DR 通过 Azure Blob Storage 自动恢复到 ANF 数据存储。 JetStream DR 根据网络映射将独立的虚拟机或相关虚拟机组恢复到恢复站点基础设施中，并提供时间点恢复以进行勒索软件保护。

本文档帮助您了解 JetStream DR 的操作原理及其主要组件。

▼ 解决方案部署概述

1. 在本地数据中心安装 JetStream DR 软件。
   a. 从 Azure 市场 (ZIP) 下载 JetStream DR 软件包，并在指定集群中部署 JetStream DR MSA (OVA)。
   b. 使用 I/O 过滤器包配置集群（安装 JetStream VIB）。
   c. 在与 DR AVS 集群相同的区域中配置 Azure Blob（Azure 存储帐户）。
   d. 部署 DRVA 设备并分配复制日志卷（来自现有数据存储或共享 iSCSI 存储的 VMDK）。
   e. 创建受保护的域（相关 VM 组）并分配 DRVA 和 Azure Blob 存储/ANF。
   f. 开始保护。
2. 在 Azure VMware 解决方案私有云中安装 JetStream DR 软件。
   a. 使用运行命令安装和配置 JetStream DR。
   b. 添加相同的 Azure Blob 容器并使用扫描域选项发现域。
   c. 部署所需的 DRVA 设备。
   d. 使用可用的 vSAN 或 ANF 数据存储创建复制日志卷。
   e. 导入受保护的域并配置 RocVA（恢复 VA）以使用 ANF 数据存储进行 VM 放置。
   f. 选择适当的故障转移选项并开始对接近零 RTO 域或虚拟机进行持续补水。
3. 在发生灾难事件期间，触发故障转移到指定 AVS DR 站点中的Azure NetApp Files数据存储。
4. 在受保护站点恢复后，调用故障回复到受保护站点。开始之前，请确保满足本 "链接"并运行 JetStream Software 提供的带宽测试工具 (BWT) 来评估与 JetStream DR 软件一起使用时 Azure Blob 存储及其复制带宽的潜在性能。满足先决条件（包括连接性）后，设置并订阅 JetStream DR for AVS "Azure 市场" 。下载软件包后，继续执行上面描述的安装过程。

在规划和启动对大量虚拟机（例如 100 多个）的保护时，请使用 JetStream DR 自动化工具包中的容量规划工具 (CPT)。提供要保护的虚拟机列表及其 RTO 和恢复组首选项，然后运行 CPT。

CPT 执行以下功能：

- 根据 RTO 将虚拟机组合到保护域中。
- 定义 DRVA 及其资源的最佳数量。
- 估计所需的复制带宽。
- 识别复制日志卷特征（容量、带宽等）。
- 估算所需的对象存储容量等等。

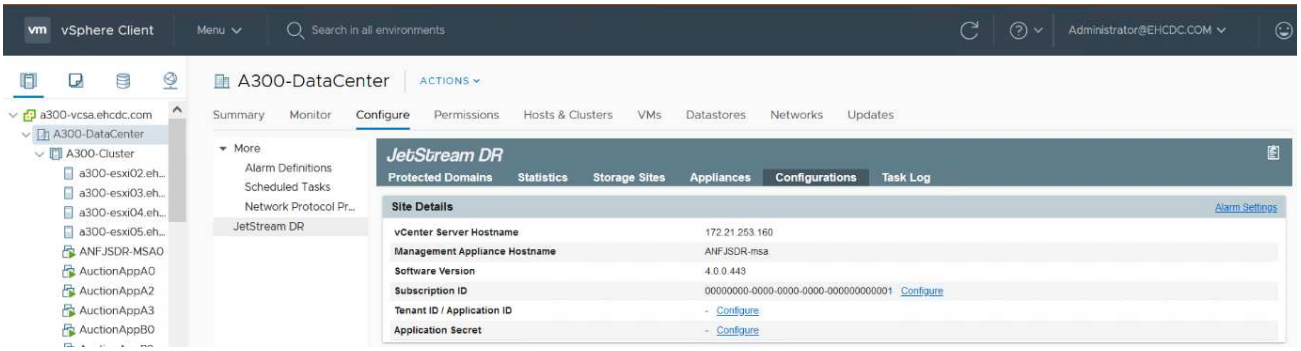
规定的域的数量和内容取决于各种 VM 特性，例如平均 IOPS、总容量、优先级（定义故障转移顺序）、RTO 等。

在本地数据中心安装 **JetStream DR**

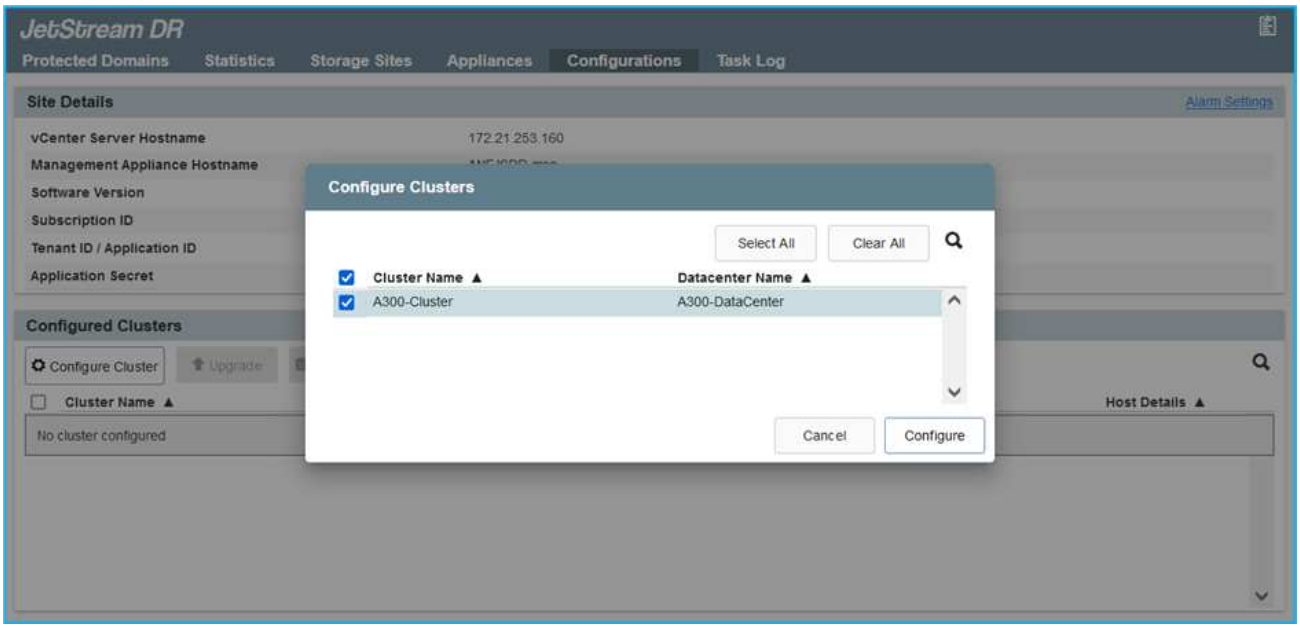
JetStream DR 软件由三个主要组件组成：JetStream DR 管理服务器虚拟设备 (MSA)、DR 虚拟设备 (DRVA) 和主机组件（I/O 筛选器包）。 MSA 用于在计算集群上安装和配置主机组件，然后管理 JetStream DR 软件。以下列表提供了安装过程的高级描述：

▼ 如何为本地安装 **JetStream DR**

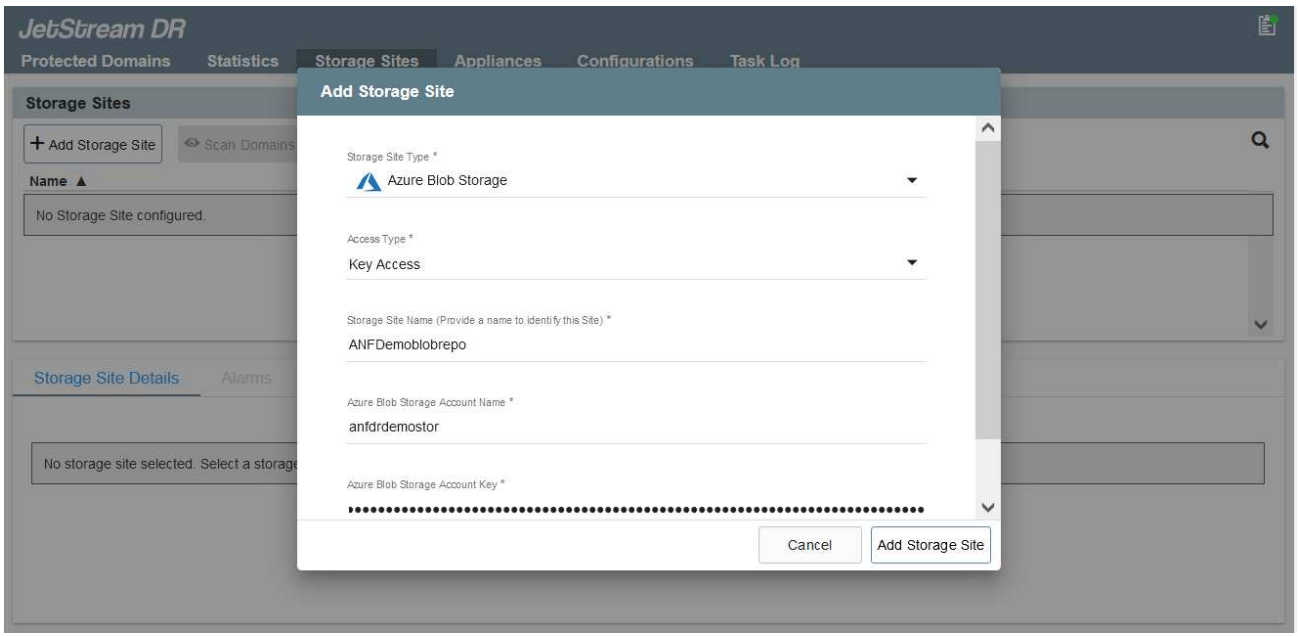
1. 检查先决条件。
2. 运行容量规划工具获取资源和配置建议（可选，但建议用于概念验证试验）。
3. 将 JetStream DR MSA 部署到指定集群中的 vSphere 主机。
4. 在浏览器中使用其 DNS 名称启动 MSA。
5. 向 MSA 注册 vCenter 服务器。要执行安装，请完成以下详细步骤：
6. 部署 JetStream DR MSA 并注册 vCenter Server 后，使用 vSphere Web Client 访问 JetStream DR 插件。这可以通过导航到数据中心 > 配置 > JetStream DR 来完成。



7. 从 JetStream DR 界面中，选择适当的集群。



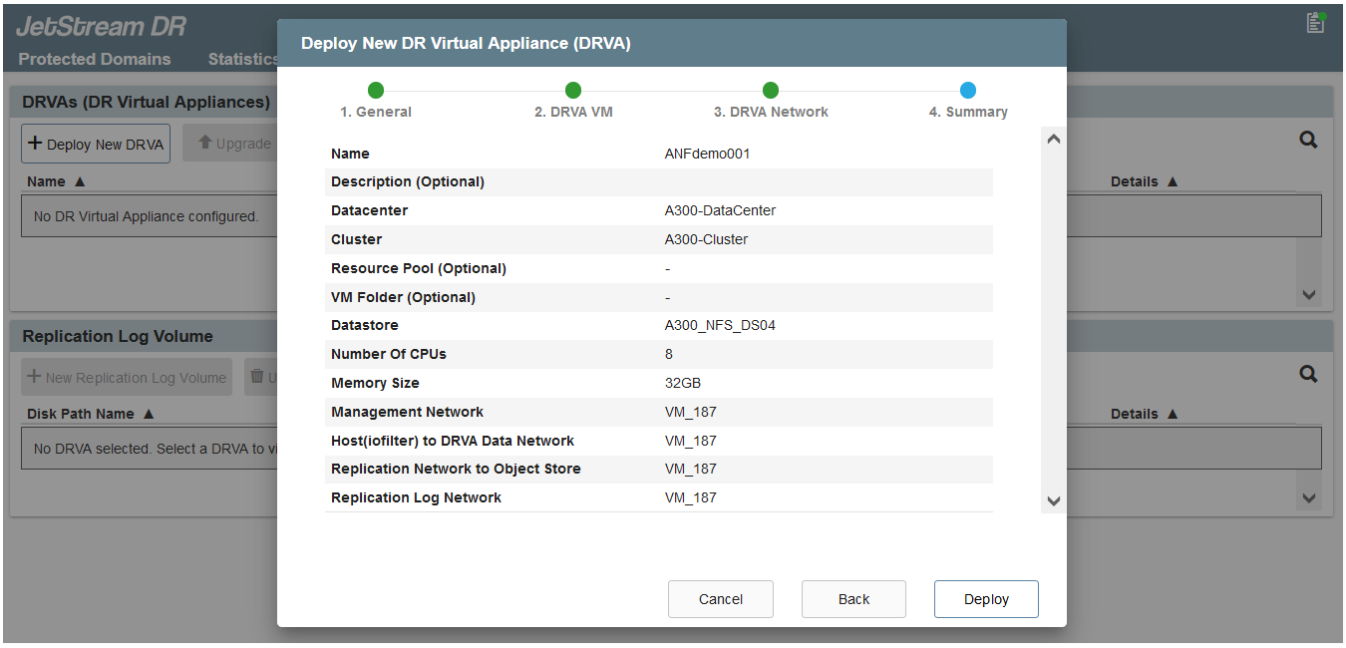
8. 使用 I/O 筛选器包配置集群。



9. 添加位于恢复站点的 Azure Blob 存储。
10. 从设备选项卡部署 DR 虚拟设备 (DRVA)。

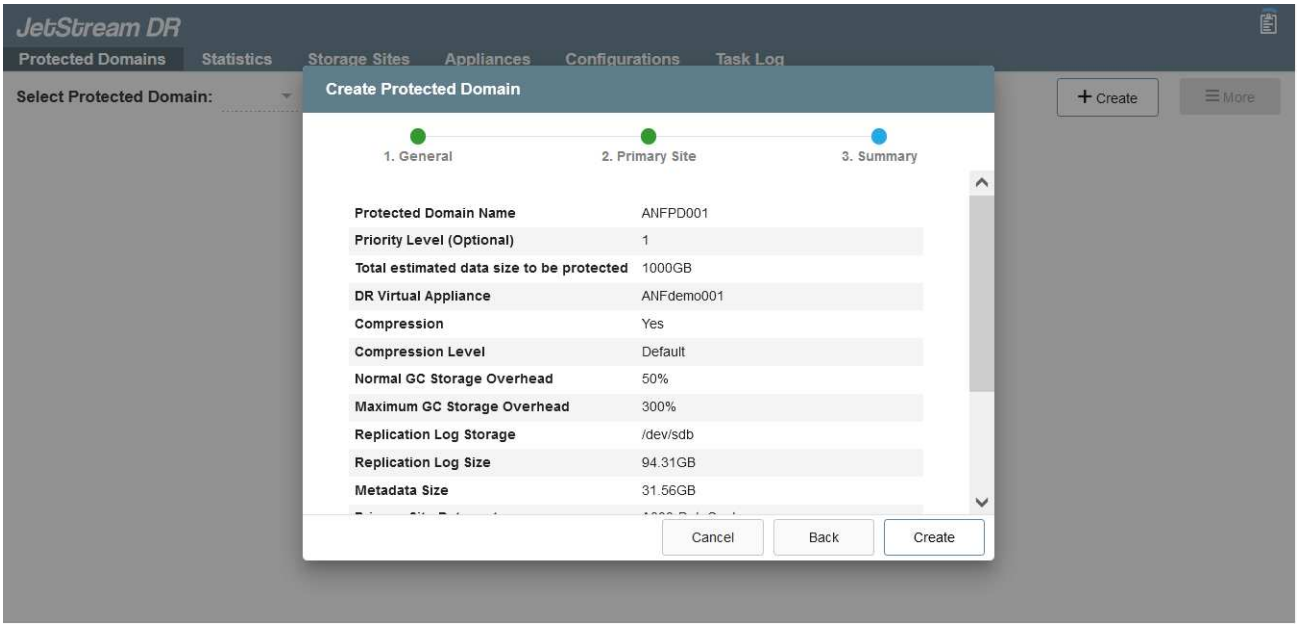
> DRVA 可以由 CPT 自动创建，但对于 POC 试验，我们建议手动配置和运行 DR 周期（启动保护 > 故障转移 > 故障恢复）。

JetStream DRVA 是一种虚拟设备，可促进数据复制过程中的关键功能。受保护的集群必须至少包含一个 DRVA，并且通常每个主机配置一个 DRVA。每个 DRVA 可以管理多个受保护域。



在此示例中，为 80 台虚拟机创建了 4 个 DRVA。

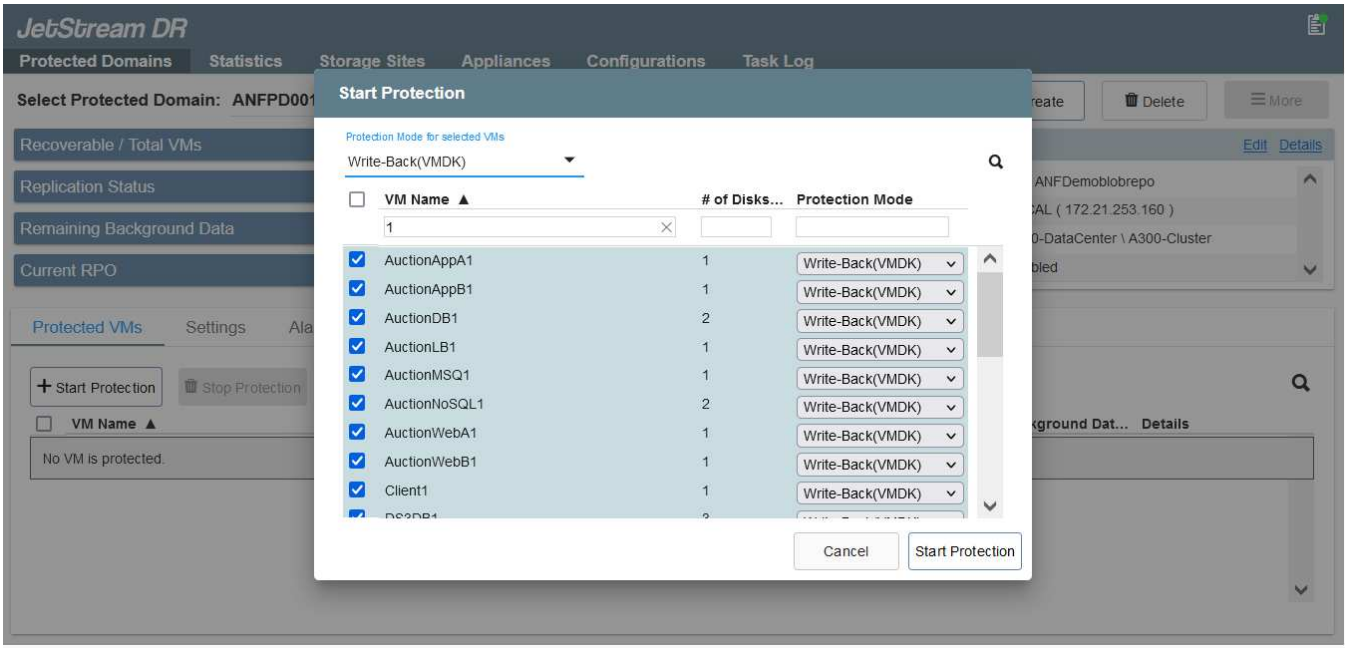
1. 使用来自可用数据存储或独立共享 iSCSI 存储池的 VMDK 为每个 DRVA 创建复制日志卷。
2. 在“受保护的域”选项卡中，使用有关 Azure Blob 存储站点、DRVA 实例和复制日志的信息创建所需数量的受保护域。受保护域定义了集群内的特定虚拟机或一组虚拟机，这些虚拟机受到共同保护，并分配了故障转移/故障回复操作的优先级顺序。



3. 选择需要保护的虚拟机，启动受保护域的虚拟机保护。这将开始将数据复制到指定的 Blob 存储。

验证受保护域中的所有虚拟机是否使用相同的保护模式。

写回（VMDK）模式可以提供更高的性能。



验证复制日志卷是否放置在高性能存储上。

> 可以配置故障转移运行手册来对虚拟机进行分组（称为恢复组）、设置启动顺序以及修改 CPU/内存设置以及 IP 配置。

使用运行命令在 **Azure VMware** 解决方案私有云中安装 **JetStream DR for AVS**

恢复站点 (AVS) 的最佳实践是提前创建一个三节点的试点灯集群。这允许预先配置恢复站点基础设施，包括以下项目：

- 目标网络段、防火墙、DHCP 和 DNS 等服务等等。
- 为 AVS 安装 JetStream DR
- 将 ANF 卷配置为数据存储，并且更多 JetStream DR 支持关键任务域的近零 RTO 模式。对于这些域，应该预先安装目标存储。在这种情况下，ANF 是推荐的存储类型。

> 应在 AVS 集群上配置包括段创建在内的网络配置以满足本地要求。

根据 SLA 和 RTO 要求，可以使用连续故障转移或常规（标准）故障转移模式。对于接近于零的 RTO，应在恢复站点开始持续补液。

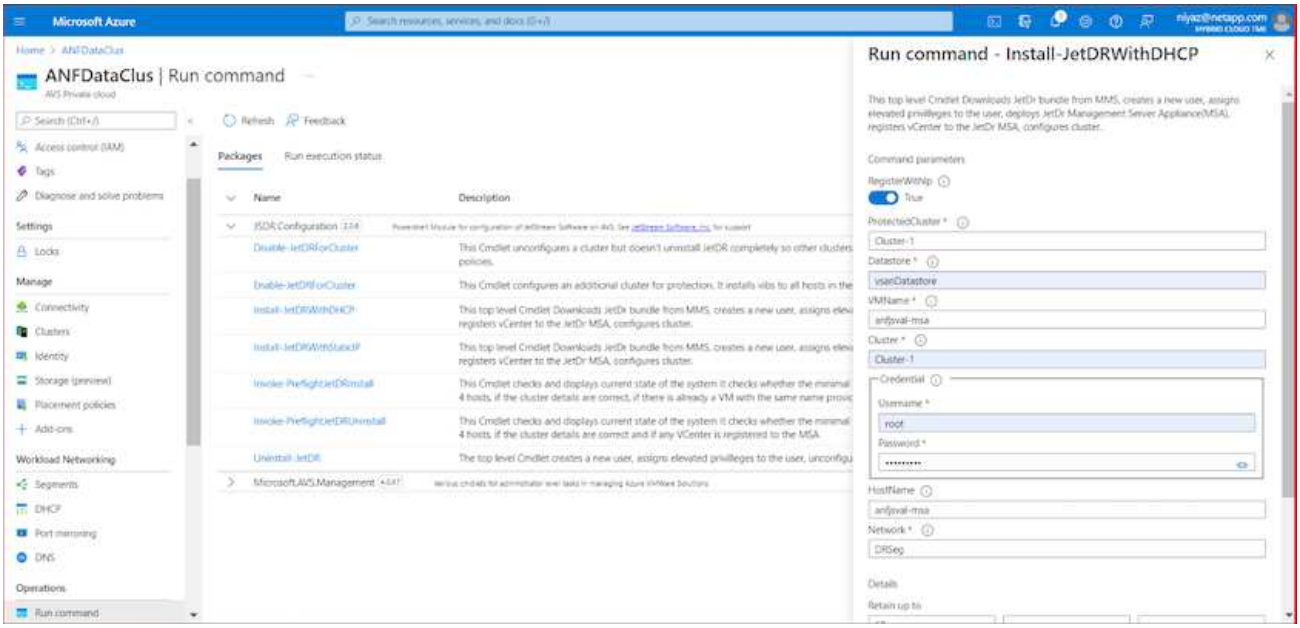
▼ 如何在私有云中安装 **JetStream DR for AVS**

要在 Azure VMware 解决方案私有云上安装 JetStream DR for AVS，请完成以下步骤：

1. 从 Azure 门户转到 Azure VMware 解决方案，选择私有云，然后选择运行命令> 包> JSDR.Configuration。

> Azure VMware 解决方案中的默认 CloudAdmin 用户没有足够的权限来为 AVS 安装 JetStream DR。 Azure VMware 解决方案通过调用 JetStream DR 的 Azure VMware 解决方案运行命令，实现了 JetStream DR 的简化和自动化安装。

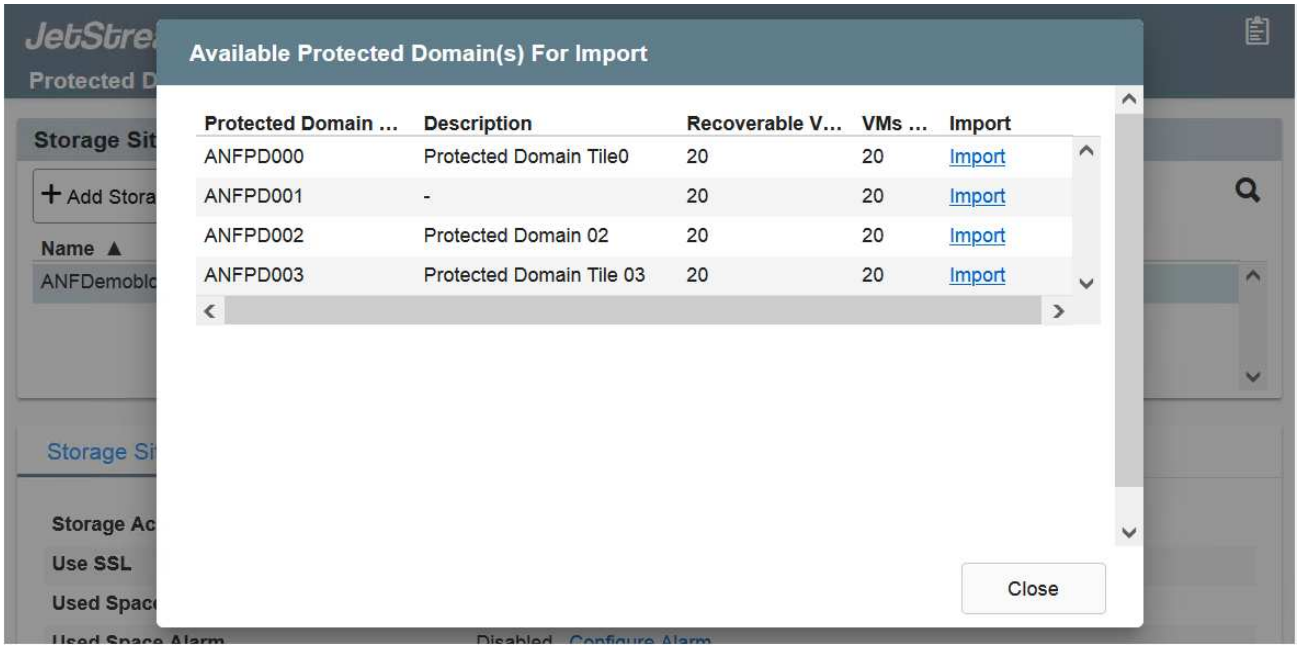
以下屏幕截图显示了使用基于 DHCP 的 IP 地址的安装。



2. JetStream DR for AVS 安装完成后，刷新浏览器。要访问 JetStream DR UI，请转到 SDDC 数据中心 > 配置 > JetStream DR。



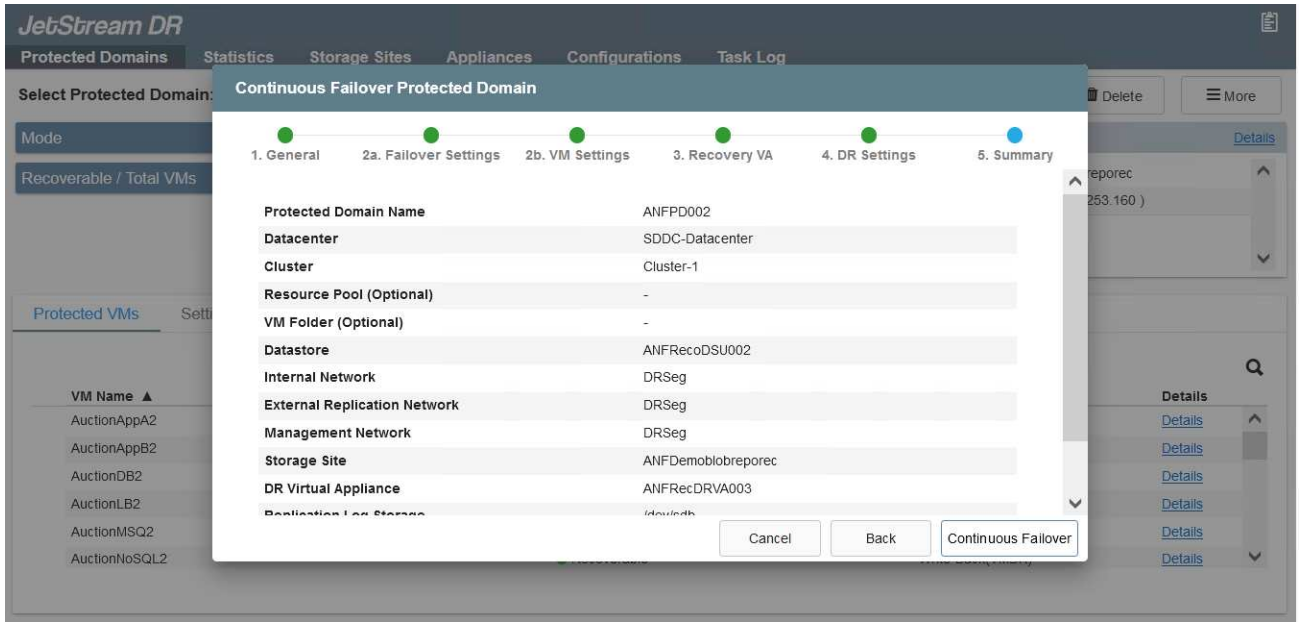
3. 从 JetStream DR 界面，添加用于保护本地集群的 Azure Blob 存储帐户作为存储站点，然后运行扫描域选项。



4. 导入受保护域后，部署 DRVA 设备。在此示例中，使用 JetStream DR UI 从恢复站点手动启动连续补水。

> 这些步骤也可以使用 CPT 创建的计划自动执行。

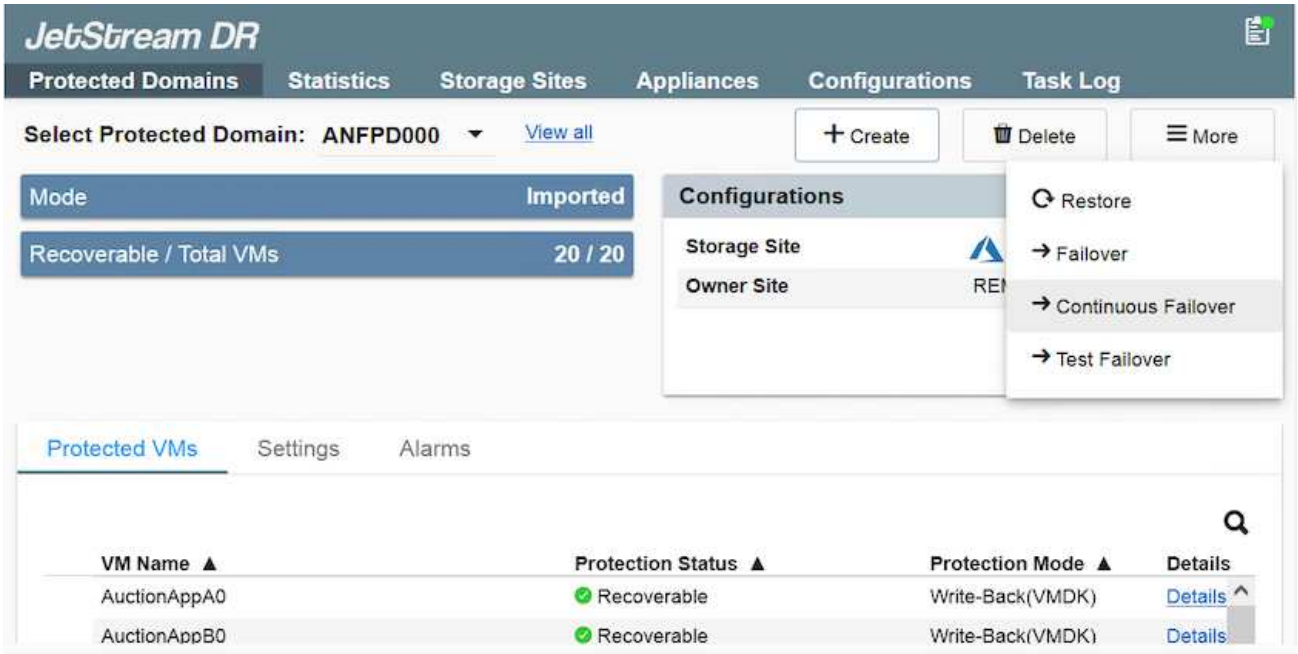
5. 使用可用的 vSAN 或 ANF 数据存储创建复制日志卷。
6. 导入受保护的域并配置恢复 VA 以使用 ANF 数据存储进行 VM 放置。



> 确保所选网段上启用了 DHCP 并且有足够的可用 IP。在域名恢复期间，暂时使用动态 IP。每个恢复的虚拟机（包括持续补水）都需要一个单独的动态 IP。恢复完成后，IP 被释放并可重复使用。

7. 选择适当的故障转移选项（连续故障转移或故障转移）。在这个例子中，选择了持续补水（持续故障转移

）。



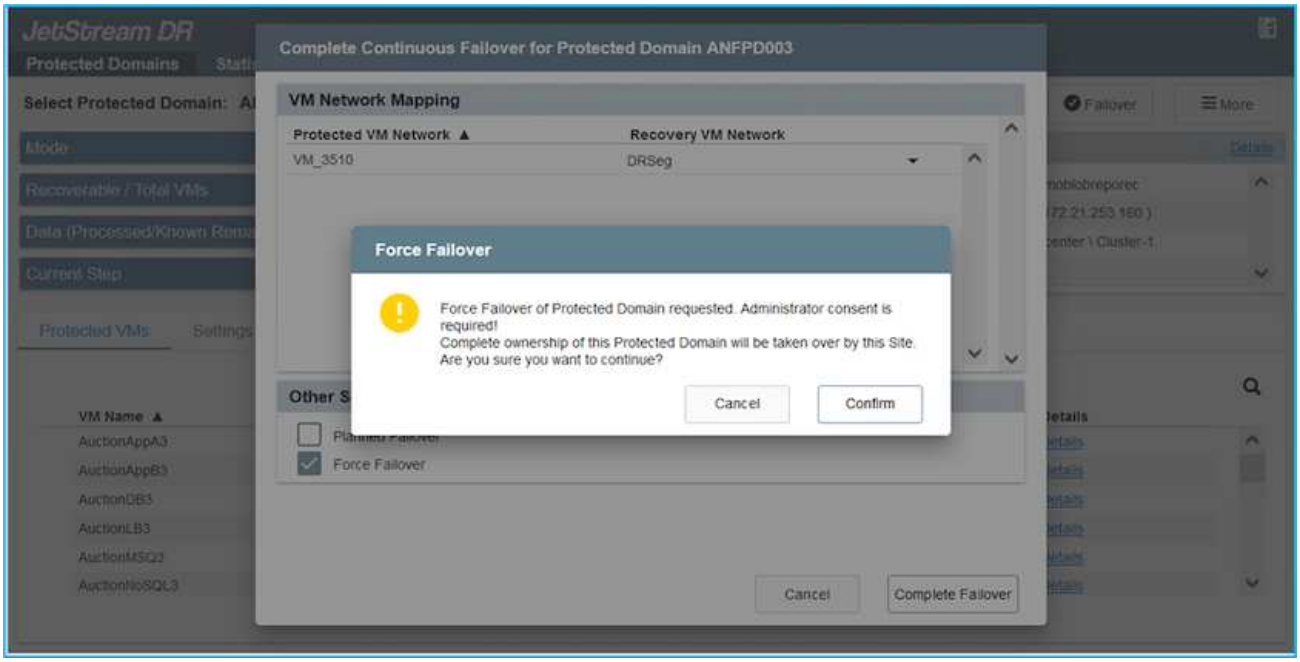
执行故障转移/故障回复

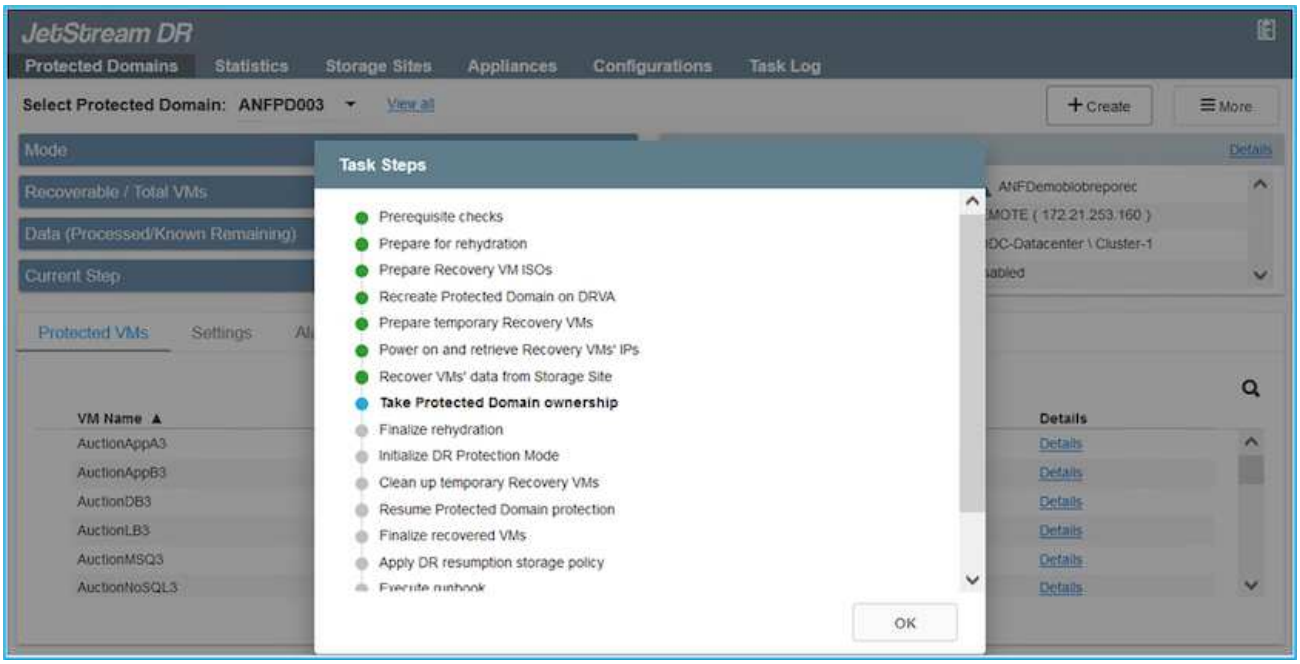
▼ 如何执行故障转移/故障恢复

1. 当本地环境受保护集群发生灾难（部分或全部故障）后，触发故障转移。

CPT 可用于执行故障转移计划，将虚拟机从 Azure Blob 存储恢复到 AVS 集群恢复站点。

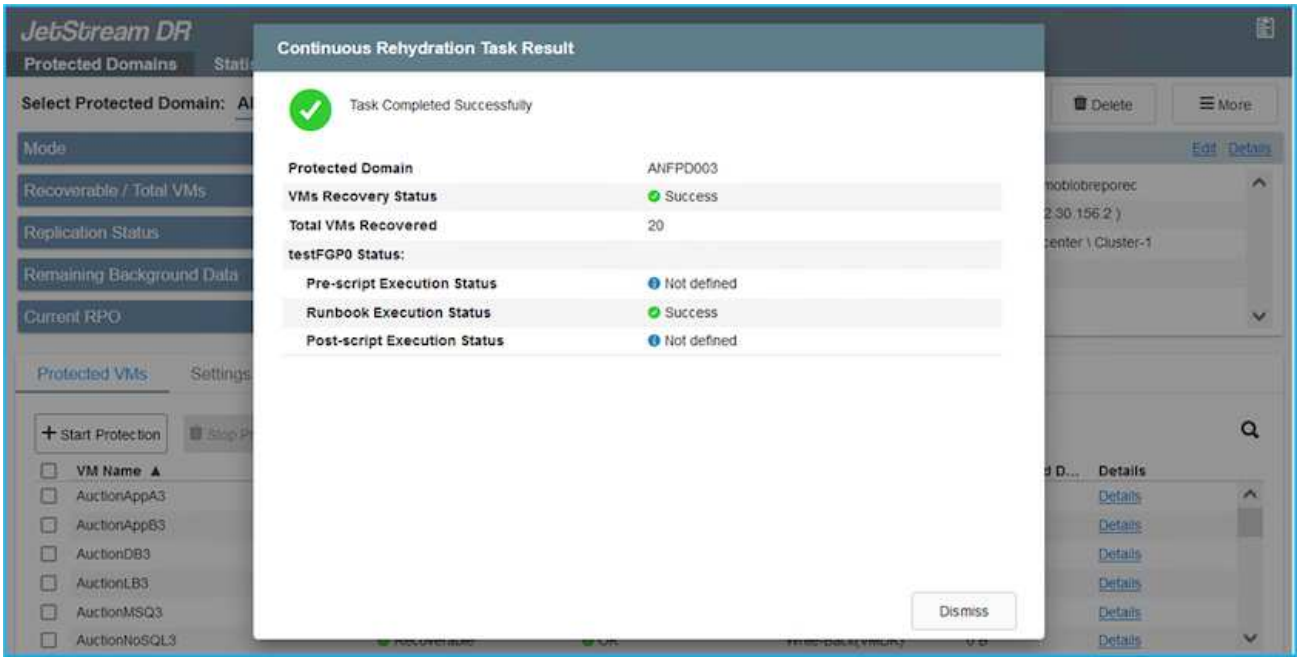
在 AVS 中启动受保护的虚拟机后进行故障转移（用于连续或标准补水），保护将自动恢复，并且 JetStream DR 将继续将其数据复制到 Azure Blob 存储中的相应/原始容器中。





任务栏显示故障转移活动的进度。

2. 任务完成后，访问恢复的虚拟机，业务继续正常进行。



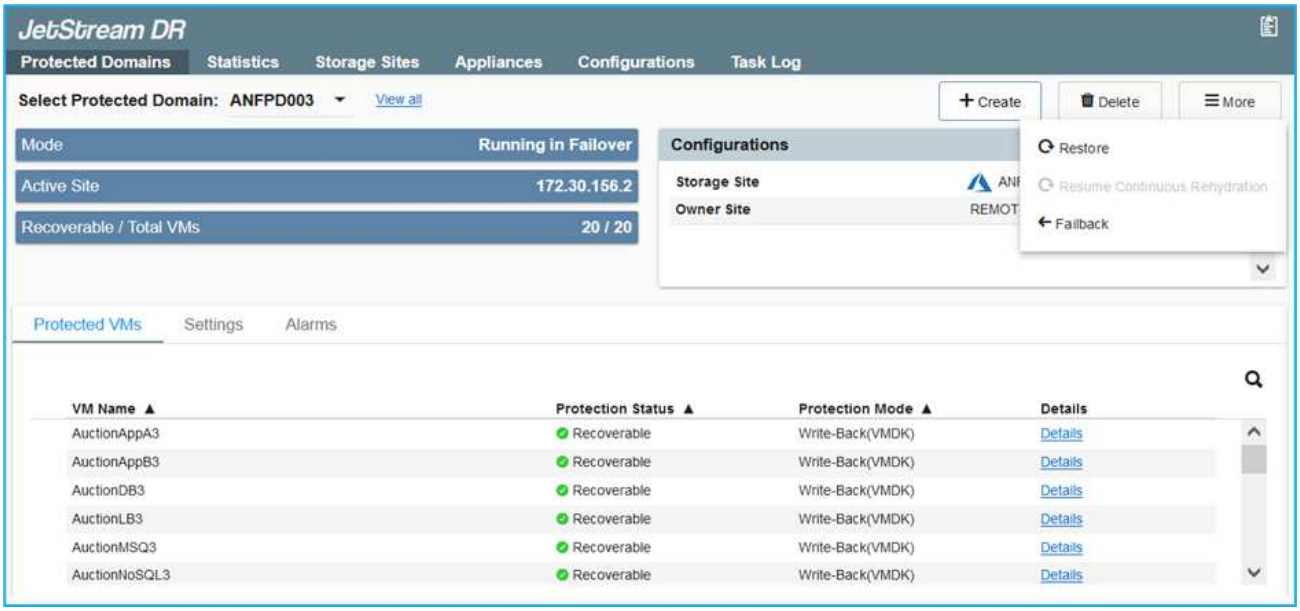
主站点重新启动并运行后，可以执行故障恢复。 VM 保护已恢复，应检查数据一致性。

3. 恢复本地环境。根据灾难事件的类型，可能需要恢复和/或验证受保护集群的配置。如有必要，可能需要重新安装 JetStream DR 软件。

> 注意： `recovery_utility_prepare_failback`自动化工具包中提供的脚本可用于帮助清理原始受保护站点中的任何过时的虚拟机、域信息等。

4. 访问恢复的本地环境，转到 Jetstream DR UI，然后选择适当的受保护域。受保护站点准备好故障恢复后

，在 UI 中选择故障恢复选项。



CPT 生成的故障恢复计划还可用于启动虚拟机及其数据从对象存储返回到原始 VMware 环境。

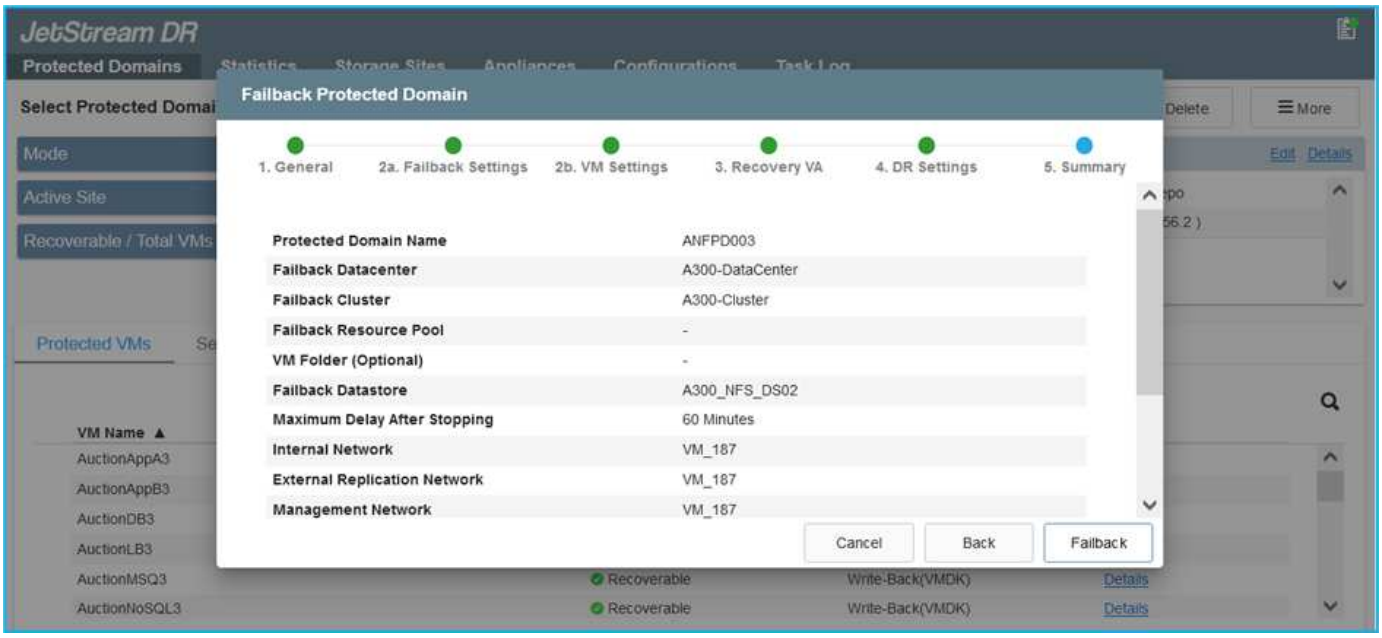
指定在恢复站点中暂停虚拟机并在受保护站点中重新启动后的最大延迟。此时间包括停止故障转移虚拟机后完成复制的时间、清理恢复站点的时间以及在受保护站点中重新创建虚拟机的时间。 NetApp建议值为 10 分钟。

完成故障恢复过程，然后确认恢复虚拟机保护和数据一致性。

勒索软件恢复

从勒索软件中恢复可能是一项艰巨的任务。具体来说，IT 组织很难确定安全的返回点，而且一旦确定，如何确保恢复的工作负载免受再次发生的攻击（来自休眠恶意软件或通过易受攻击的应用程序）。

JetStream DR for AVS 与Azure NetApp Files数据存储相结合，可以解决这些问题，允许组织从可用的时间点恢复，以便在需要时将工作负载恢复到功能齐全的隔离网络。恢复允许应用程序运行并相互通信，同时不会将它们暴露在南北流量中，从而为安全团队提供一个安全的地方来执行取证和其他必要的补救措施。



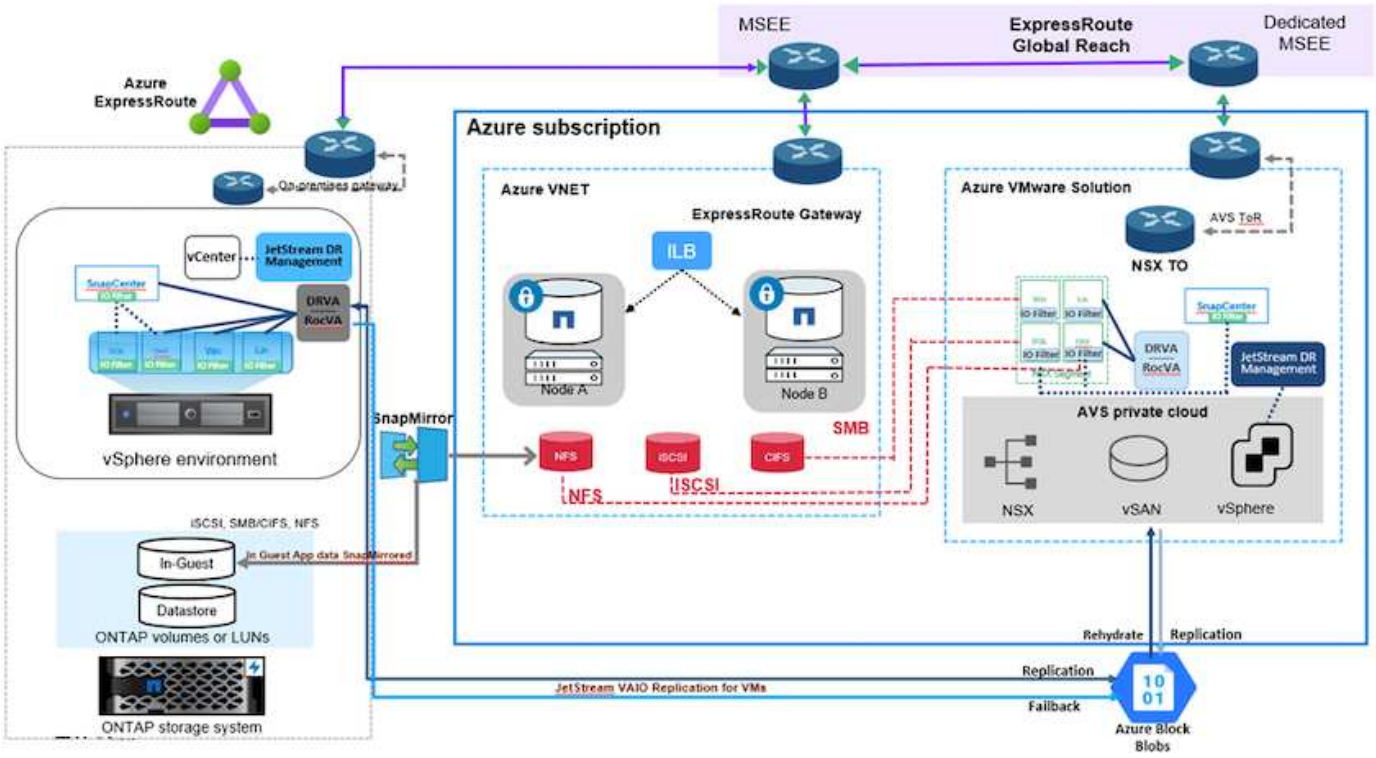
使用 **CVO** 和 **AVS**（来宾连接存储）进行灾难恢复

云端灾难恢复是一种具有弹性且经济高效的方法，可以保护工作负载免受站点中断和勒索软件等数据损坏事件的影响。借助NetApp SnapMirror，使用来宾连接存储的本地 VMware 工作负载可以复制到在 Azure 中运行的NetApp Cloud Volumes ONTAP 。

概述

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
```

本文档提供了使用NetApp SnapMirror、JetStream 和 Azure VMware 解决方案 (AVS) 设置和执行灾难恢复的分步方法。



假设

本文档重点介绍应用程序数据的客户机内存储（也称为客户机连接），我们假设本地环境使用SnapCenter进行应用程序一致性备份。

本文档适用于任何第三方备份或恢复解决方案。根据环境中使用的解决方案，遵循最佳实践来创建符合组织 SLA 的备份策略。

对于本地环境和 Azure 虚拟网络之间的连接，请使用快速路由全球覆盖或带有 VPN 网关的虚拟 WAN。应根据内部部署 vLAN 设计创建段。

将本地数据中心连接到 Azure 有多种选择，因此我们无法在本文档中概述特定的工作流程。请参阅 Azure 文档，了解适当的本地到 Azure 连接方法。

部署灾难恢复解决方案

解决方案部署概述

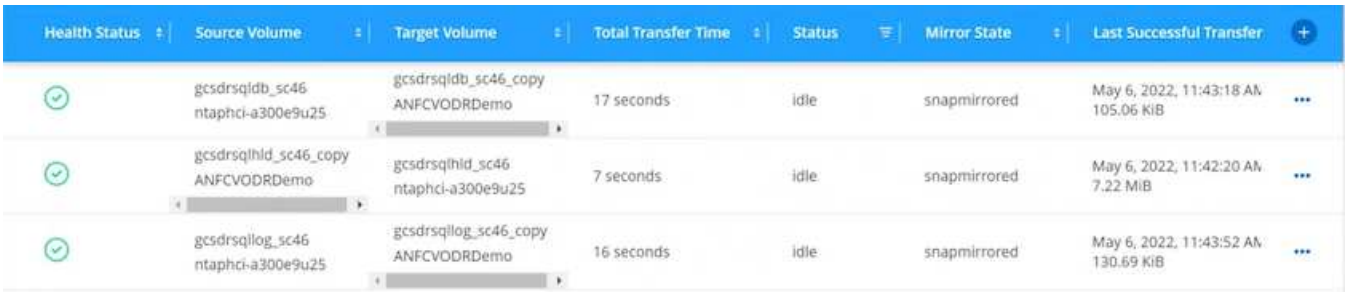
1. 确保使用SnapCenter备份应用程序数据并满足必要的 RPO 要求。
2. 使用适当的订阅和虚拟网络中的云管理器为Cloud Volumes ONTAP配置正确的实例大小。
   a. 为相关应用程序卷配置SnapMirror 。
   b. 更新SnapCenter中的备份策略以在计划的作业之后触发SnapMirror更新。
3. 在本地数据中心安装 JetStream DR 软件并启动对虚拟机的保护。
4. 在 Azure VMware 解决方案私有云中安装 JetStream DR 软件。

5. 在灾难事件期间，使用 Cloud Manager 中断SnapMirror关系并触发虚拟机到Azure NetApp Files或指定 AVS DR 站点中的 vSAN 数据存储的故障转移。
    a. 重新连接应用程序虚拟机的 ISCSI LUN 和 NFS 挂载。
6. 主站点恢复后，通过反向重新同步SnapMirror调用故障回复到受保护站点。

部署详情

▼ 在 **Azure** 上配置 **CVO** 并将卷复制到 **CVO**

第一步是在 Azure 上配置Cloud Volumes ONTAP （"链路") 并以所需的频率和快照保留将所需的卷复制到Cloud Volumes ONTAP 。



▼ 配置 **AVS** 主机和 **CVO** 数据访问

部署 SDDC 时需要考虑的两个重要因素是 Azure VMware 解决方案中 SDDC 群集的大小以及保持 SDDC 服务的时间。灾难恢复解决方案的这两个关键考虑因素有助于降低总体运营成本。 SDDC 最小可以只有三台主机，最大可以达到全面部署的多主机集群。

部署 AVS 集群的决定主要基于 RPO/RTO 要求。借助 Azure VMware 解决方案，可以及时配置 SDDC，为测试或实际灾难事件做好准备。当您不处理灾难时，及时部署的 SDDC 可以节省 ESXi 主机成本。然而，这种部署形式会在配置 SDDC 时影响 RTO 几个小时。

最常见的部署选项是让 SDDC 以始终开启、指示灯亮起的操作模式运行。此选项占用空间较小，仅需三个始终可用的主机，同时还通过为模拟活动和合规性检查提供运行基线来加快恢复操作，从而避免生产站点和 DR 站点之间出现操作偏差的风险。当需要处理实际 DR 事件时，指示灯集群可以快速扩展到所需的级别。

要配置 AVS SDDC（按需模式或指示灯模式），请参阅"在 Azure 上部署和配置虚拟化环境"。作为先决条件，请验证在建立连接后，驻留在 AVS 主机上的客户虚拟机是否能够使用来自Cloud Volumes ONTAP的数据。

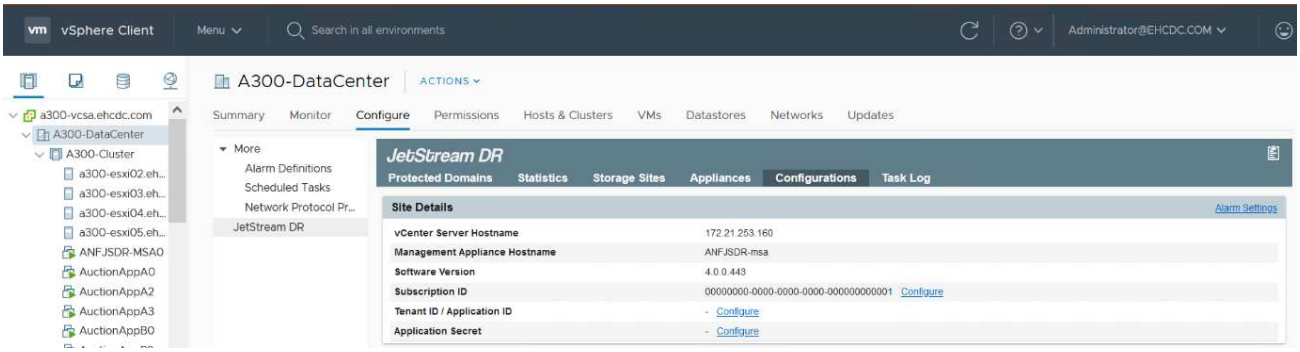
正确配置Cloud Volumes ONTAP和 AVS 后，开始配置 Jetstream，通过使用 VAIO 机制并利用SnapMirror将应用程序卷复制到Cloud Volumes ONTAP，自动将本地工作负载恢复到 AVS（具有应用程序 VMDK 的虚拟机和具有客户机内存储的虚拟机）。

▼ 在本地数据中心安装 **JetStream DR**

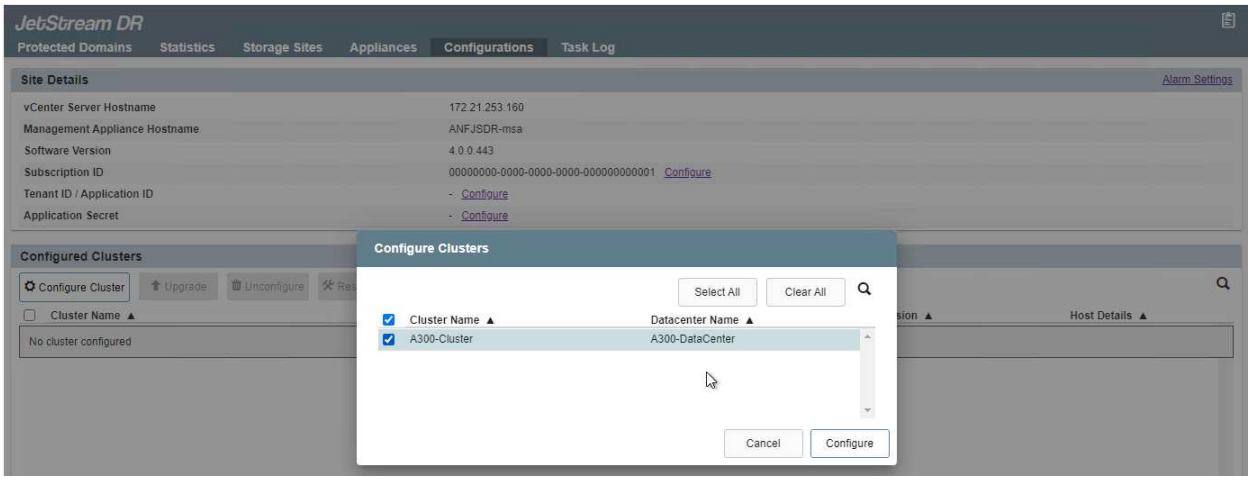
JetStream DR 软件由三个主要组件组成：JetStream DR 管理服务器虚拟设备 (MSA)、DR 虚拟设备 (DRVA) 和主机组件（I/O 过滤包）。 MSA 用于在计算集群上安装和配置主机组件，然后管理 JetStream DR 软件。安装过程如下：

1. 检查先决条件。
2. 运行容量规划工具获取资源和配置建议。
3. 将 JetStream DR MSA 部署到指定集群中的每个 vSphere 主机。
4. 在浏览器中使用其 DNS 名称启动 MSA。

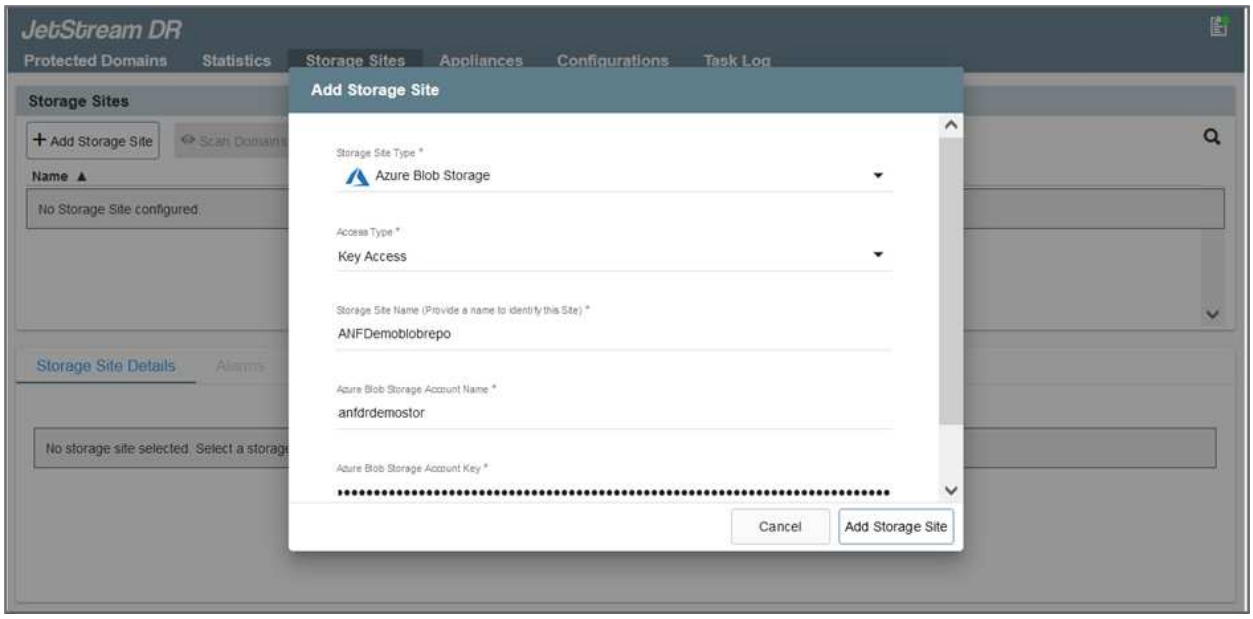
5. 向 MSA 注册 vCenter 服务器。
6. 部署 JetStream DR MSA 并注册 vCenter Server 后，使用 vSphere Web Client 导航到 JetStream DR 插件。这可以通过导航到数据中心 > 配置 > JetStream DR 来完成。



7. 从 JetStream DR 界面完成以下任务：
   a. 使用 I/O 筛选器包配置集群。



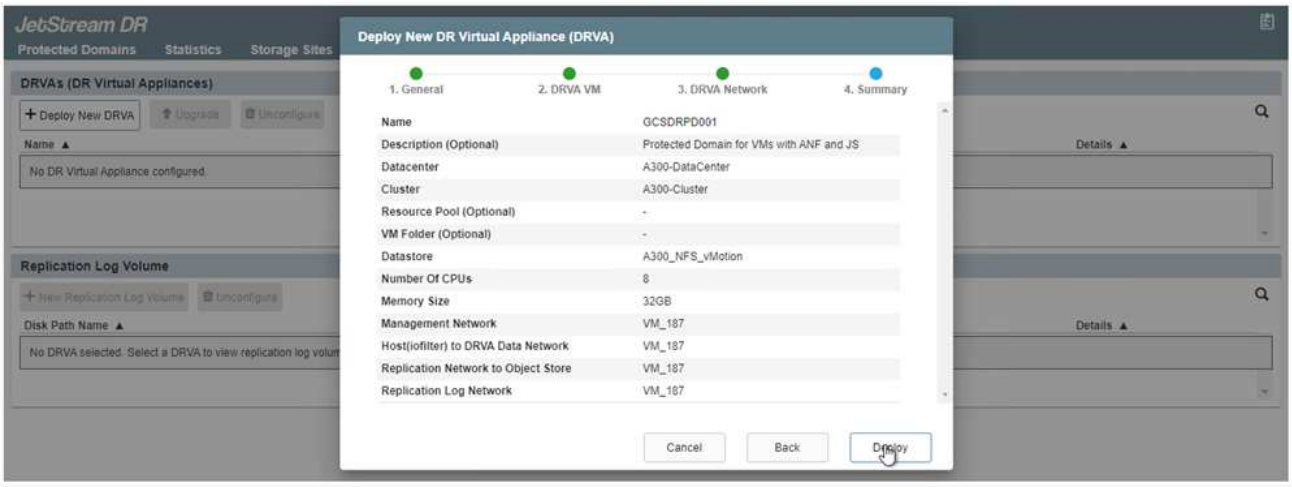
   b. 添加位于恢复站点的 Azure Blob 存储。



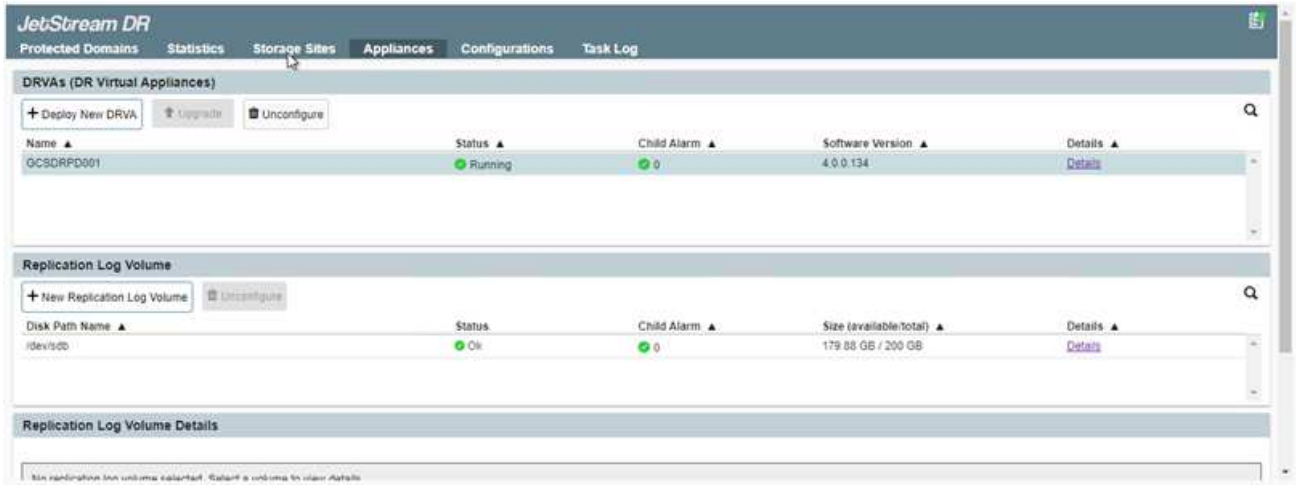
8. 从设备选项卡部署所需数量的 DR 虚拟设备 (DRVA)。

使用容量规划工具来估计所需的 DRVA 数量。

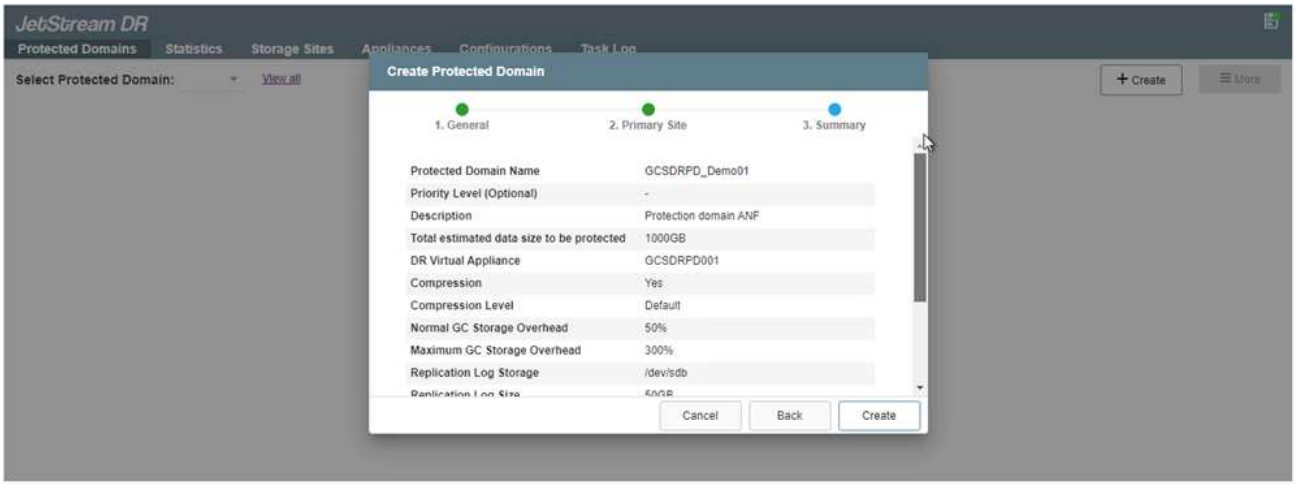


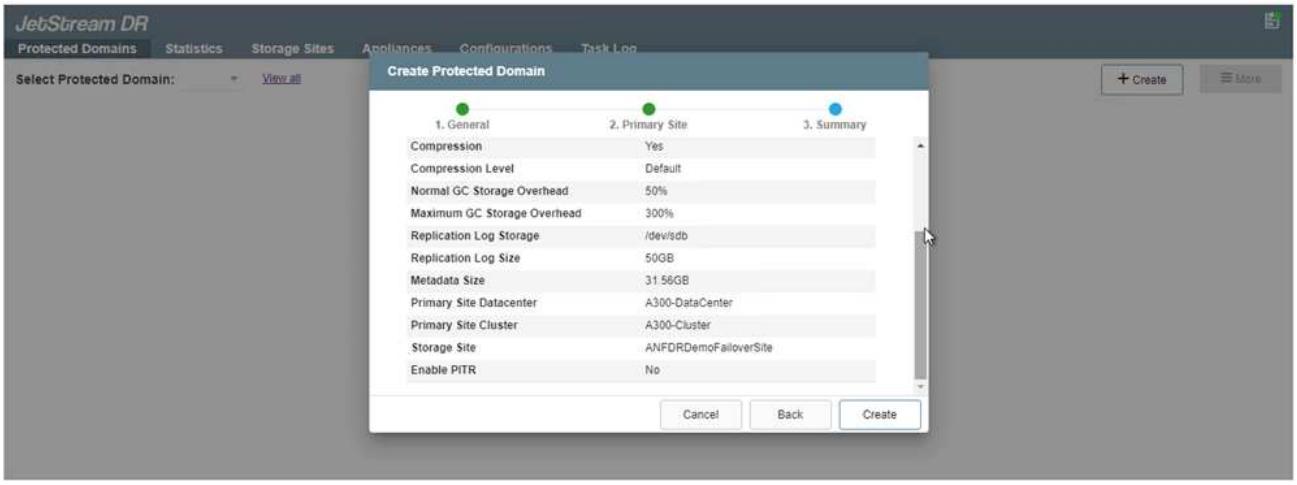


9. 使用来自可用数据存储或独立共享 iSCSI 存储池的 VMDK 为每个 DRVA 创建复制日志卷。



10. 在“受保护的域”选项卡中，使用有关 Azure Blob 存储站点、DRVA 实例和复制日志的信息创建所需数量的受保护域。受保护域定义集群内的特定虚拟机或一组应用程序虚拟机，这些虚拟机受到一起保护，并分配了故障转移/故障回复操作的优先级顺序。

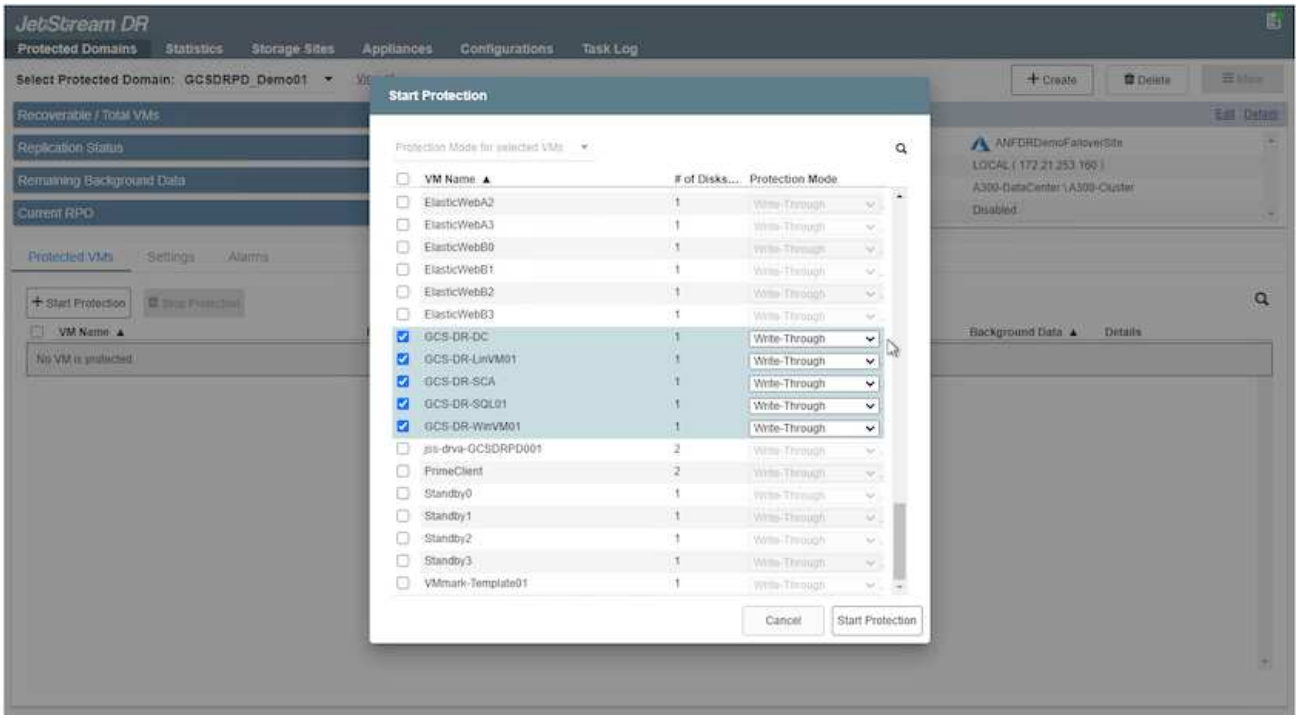




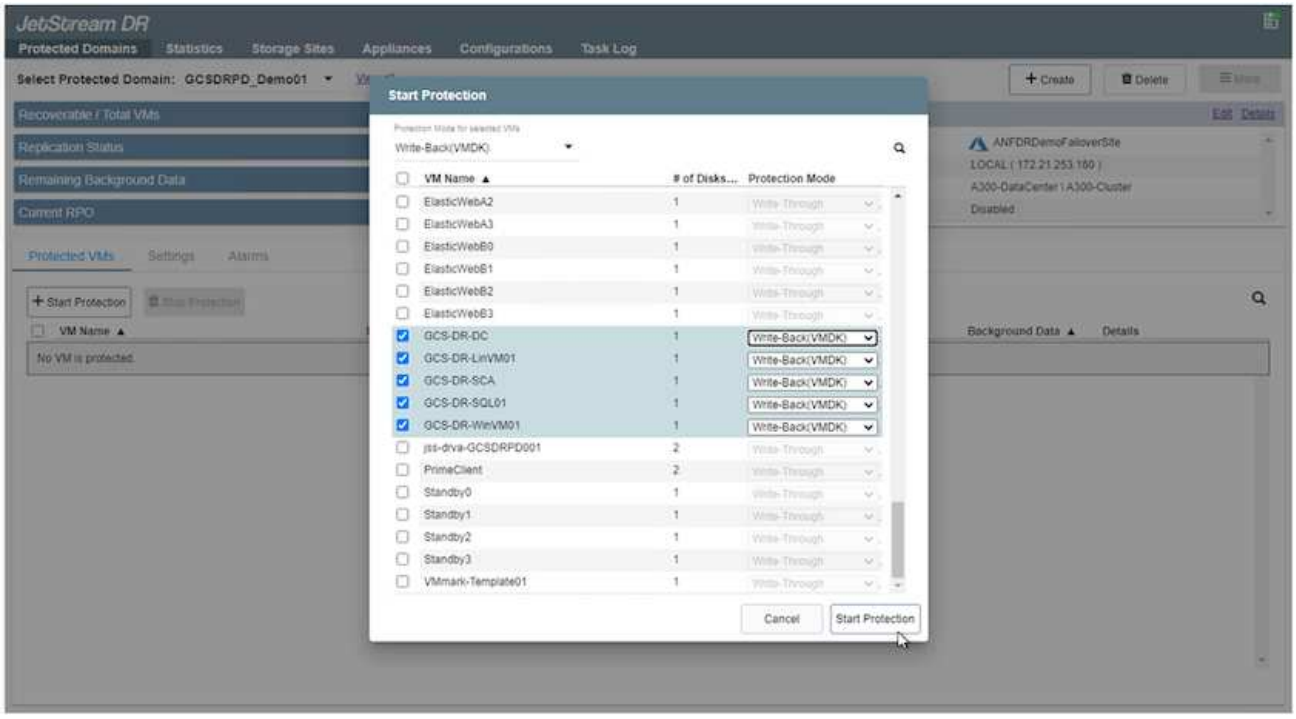
11. 选择要保护的虚拟机，并根据依赖关系将虚拟机分组到应用程序组中。应用程序定义允许您将虚拟机集分组为逻辑组，其中包含其启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

确保受保护域内的所有虚拟机使用相同的保护模式。

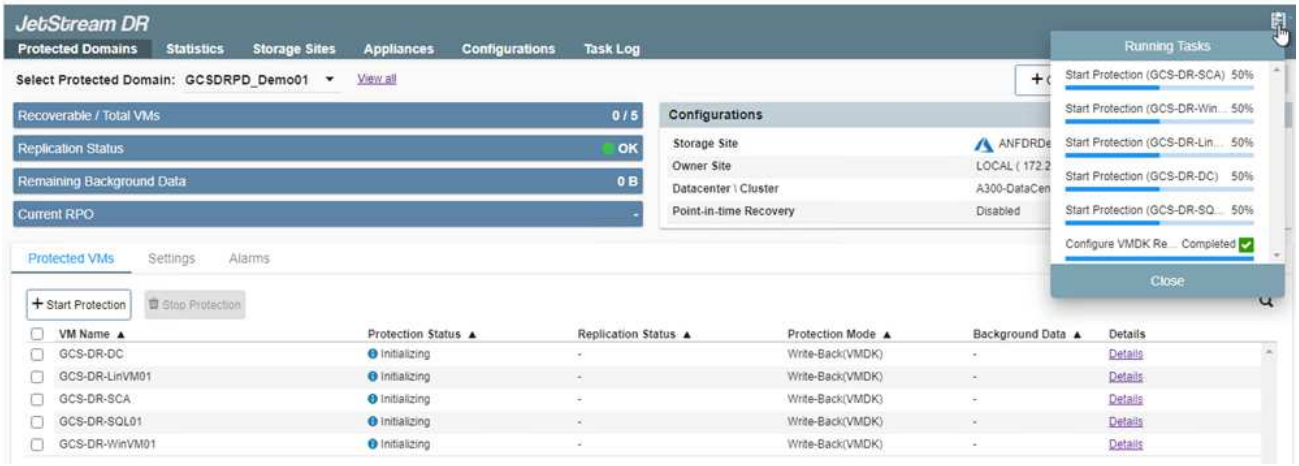
回写（VMDK）模式提供更高的性能。



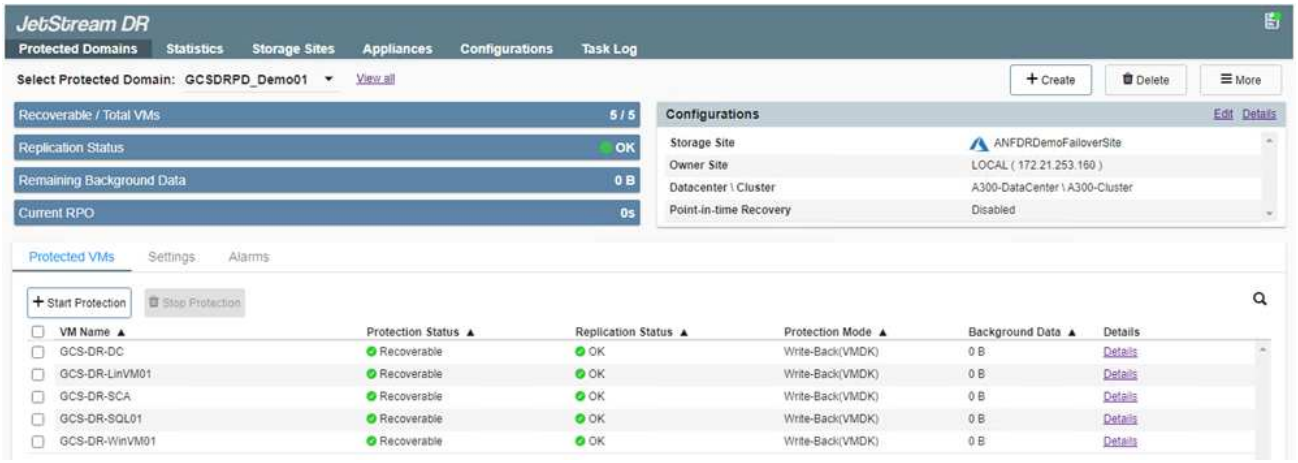
12. 确保复制日志卷放置在高性能存储上。



13. 完成后，单击“开始保护”以保护受保护的域。这将开始将选定虚拟机的数据复制到指定的 Blob 存储。



14. 复制完成后，虚拟机保护状态标记为可恢复。



> 可以配置故障转移运行手册来对虚拟机进行分组（称为恢复组）、设置启动顺序以及修改CPU/内存设置以及 IP 配置。

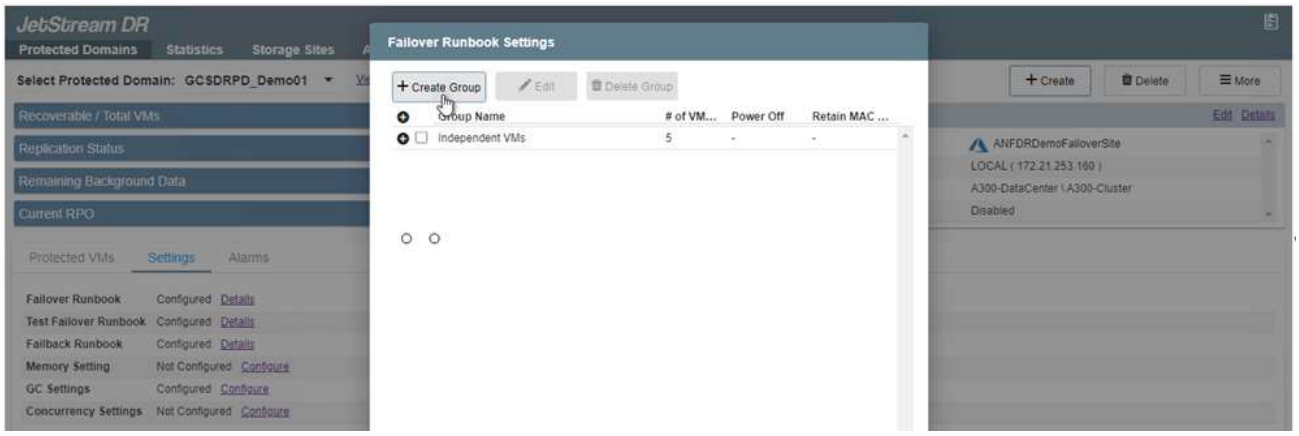
15. 单击“设置”，然后单击“运行手册配置”链接来配置运行手册组。



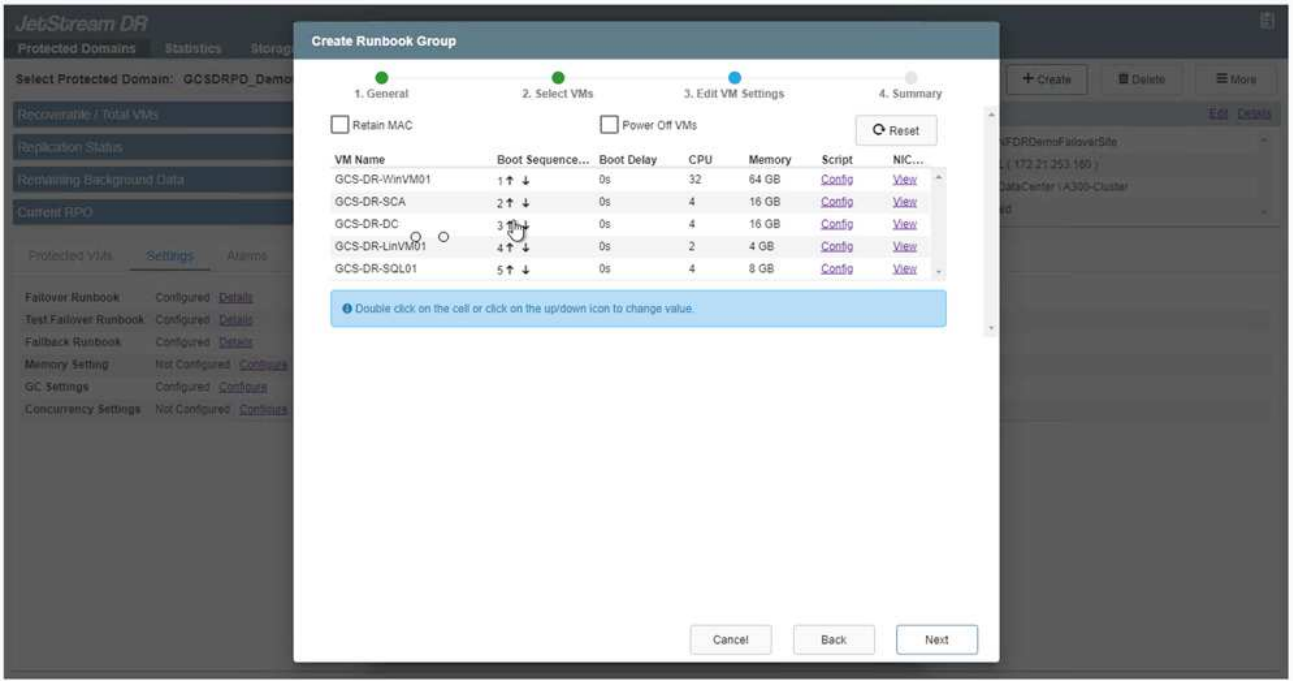
16. 单击“创建组”按钮开始创建新的运行手册组。

> 如果需要，在屏幕的下部，应用自定义前脚本和后脚本，以便在运行手册组操作之前和之

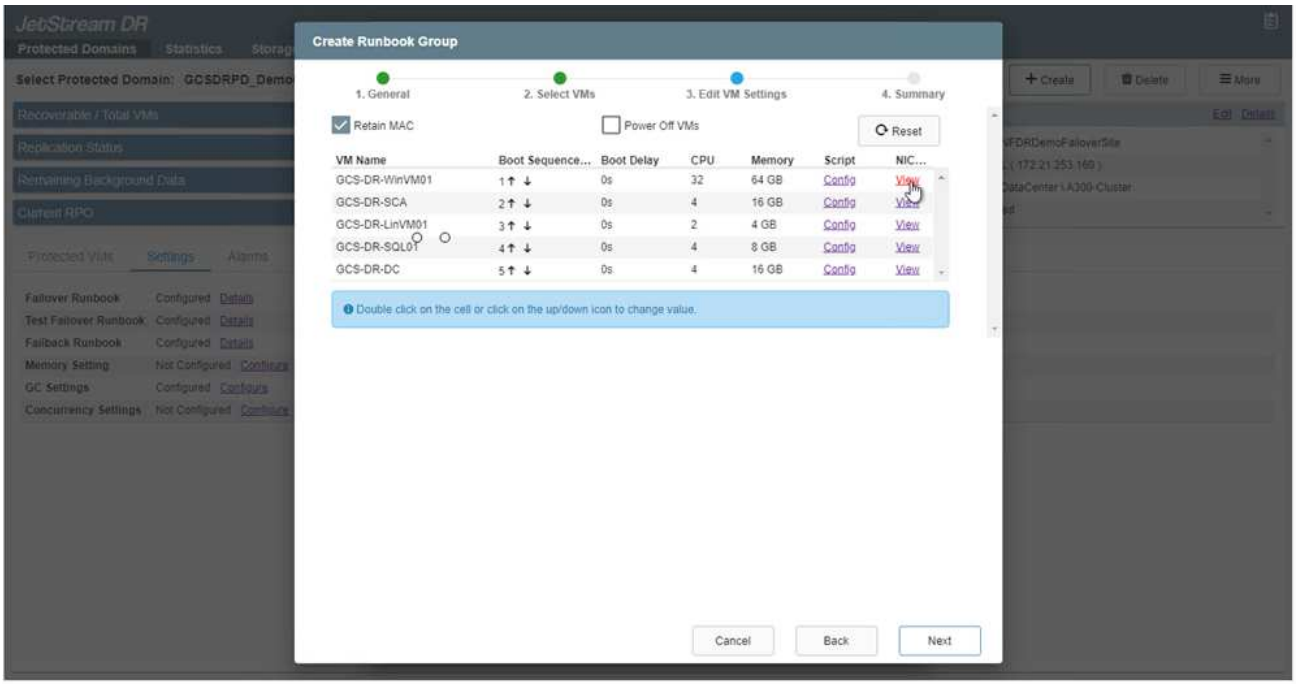
后自动运行。确保 Runbook 脚本驻留在管理服务器上。



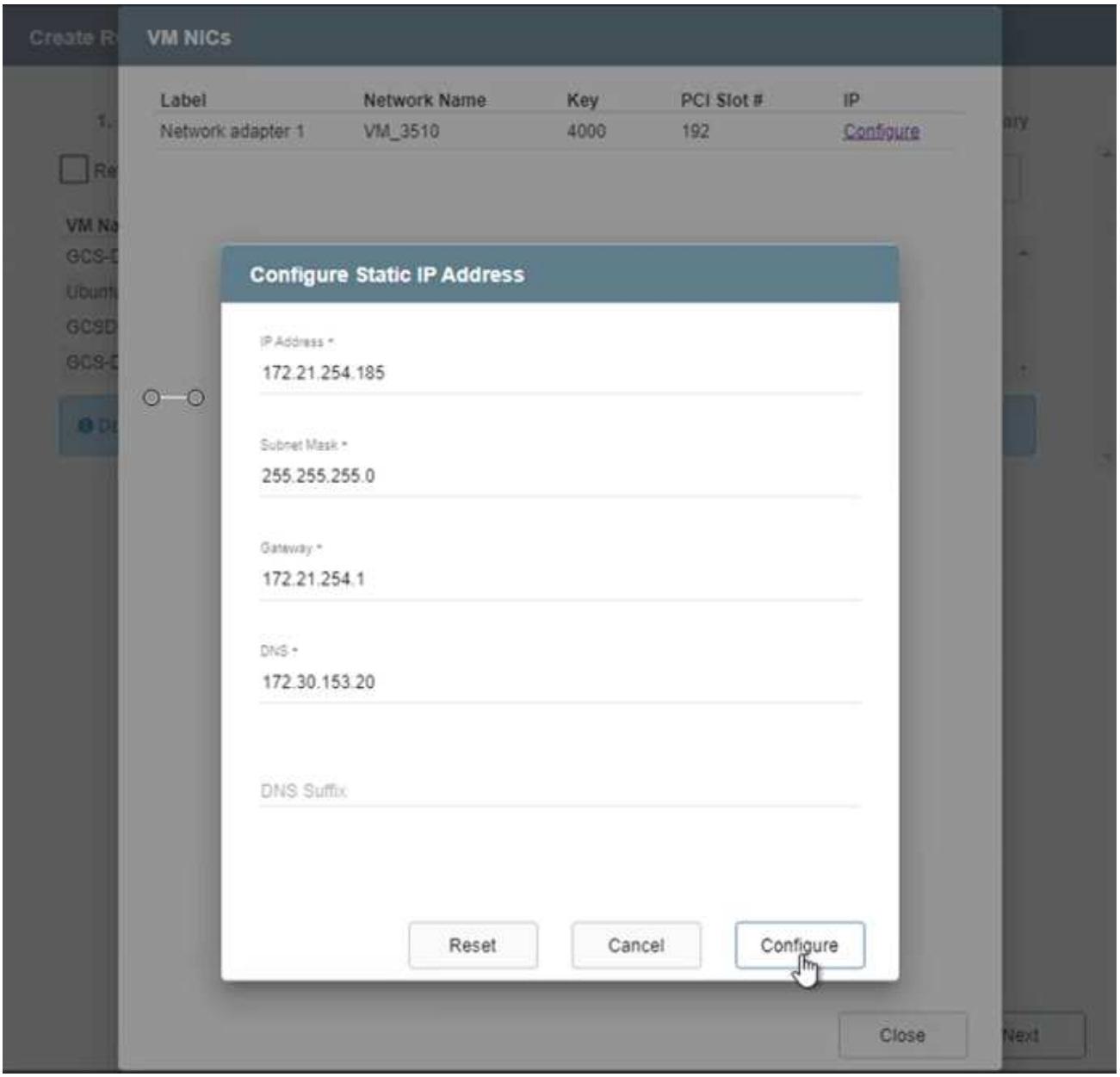
17. 根据需要编辑 VM 设置。指定恢复虚拟机的参数，包括启动顺序、启动延迟（以秒为单位）、CPU 数量以及要分配的内存量。单击向上或向下箭头更改虚拟机的启动顺序。还提供了保留 MAC 的选项。

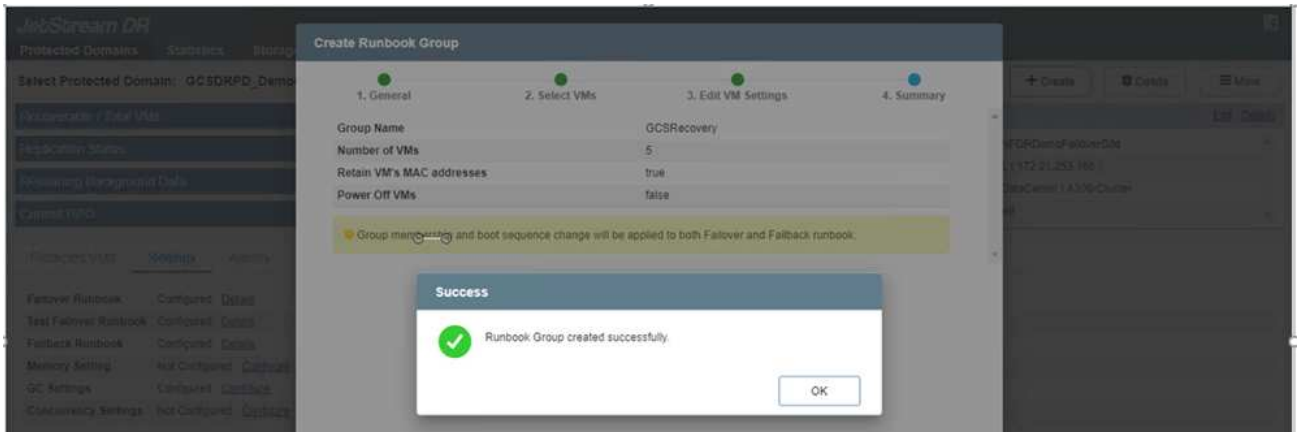


18. 可以为组中的各个虚拟机手动配置静态 IP 地址。单击虚拟机的 NIC 视图链接以手动配置其 IP 地址设置。



19. 单击配置按钮保存各个虚拟机的 NIC 设置。





故障转移和故障回复运行手册的状态现在均列为“已配置”。故障转移和故障回复运行手册组是使用相同的初始虚拟机组和设置成对创建的。如果需要，可以通过单击其各自的“详细信息”链接并进行更改来单独定制任何运行手册组的设置。

▼ 在私有云中为 **AVS** 安装 **JetStream DR**

恢复站点 (AVS) 的最佳实践是提前创建一个三节点的试点灯集群。这允许预先配置恢复站点基础设施，包括以下内容：

- 目标网络段、防火墙、DHCP 和 DNS 等服务等
- 为 AVS 安装 JetStream DR
- 将 ANF 卷配置为数据存储等

JetStream DR 支持关键任务域的接近零 RTO 模式。对于这些域，应该预先安装目标存储。在这种情况下，ANF 是推荐的存储类型。

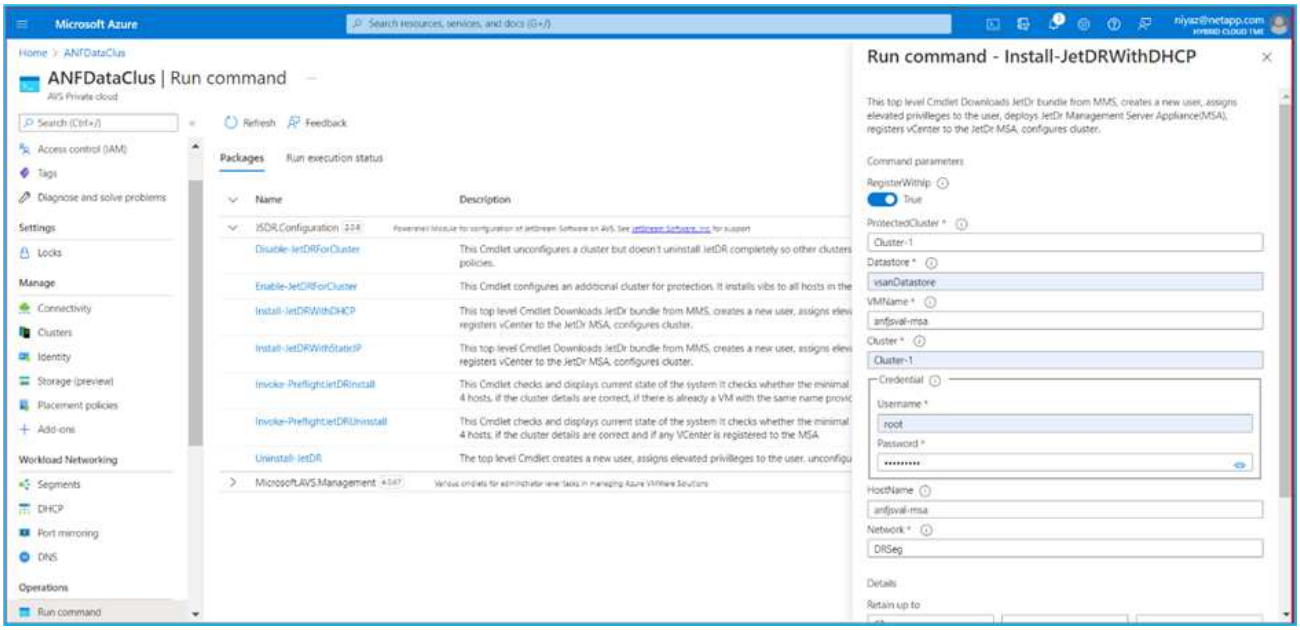
应在 AVS 集群上配置包括段创建在内的网络配置以满足本地要求。

根据 SLA 和 RTO 要求，您可以使用连续故障转移或常规（标准）故障转移模式。对于接近于零的 RTO，您应该在恢复站点开始持续补水。

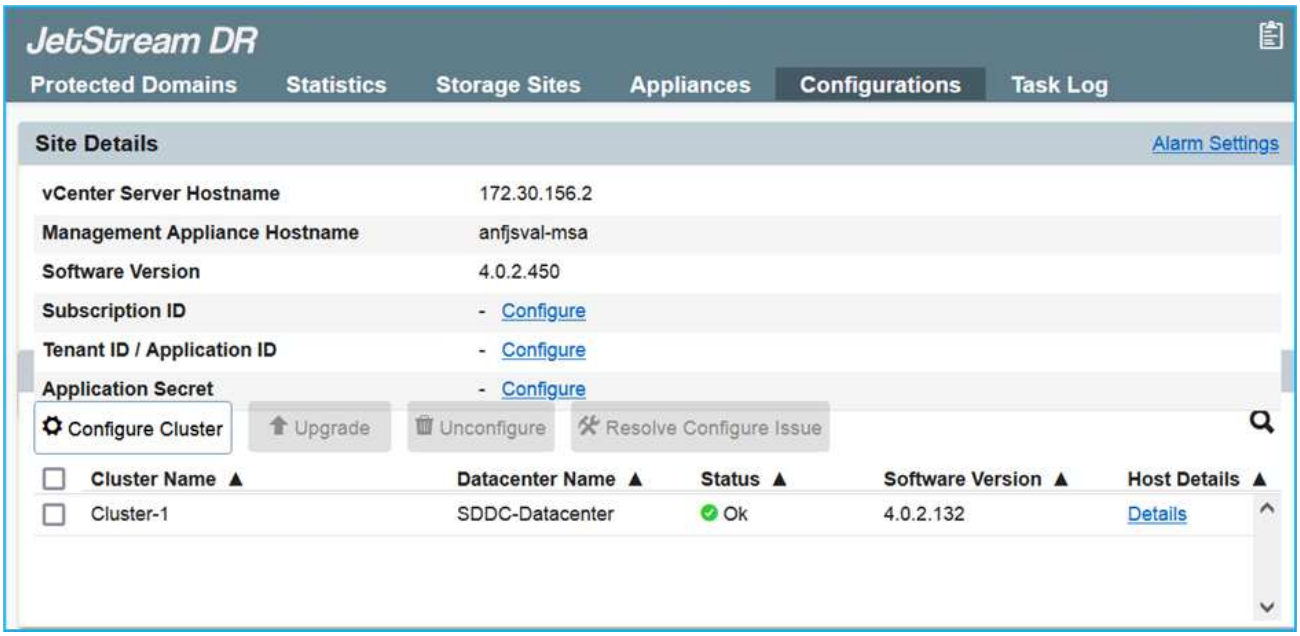
1. 要在 Azure VMware 解决方案私有云上安装 JetStream DR for AVS，请使用运行命令。从 Azure 门户转到 Azure VMware 解决方案，选择私有云，然后选择运行命令> 包> JSDR.Configuration。

   Azure VMware 解决方案的默认 CloudAdmin 用户没有足够的权限来为 AVS 安装 JetStream DR。 Azure VMware 解决方案通过调用 JetStream DR 的 Azure VMware 解决方案运行命令，实现了 JetStream DR 的简化和自动化安装。

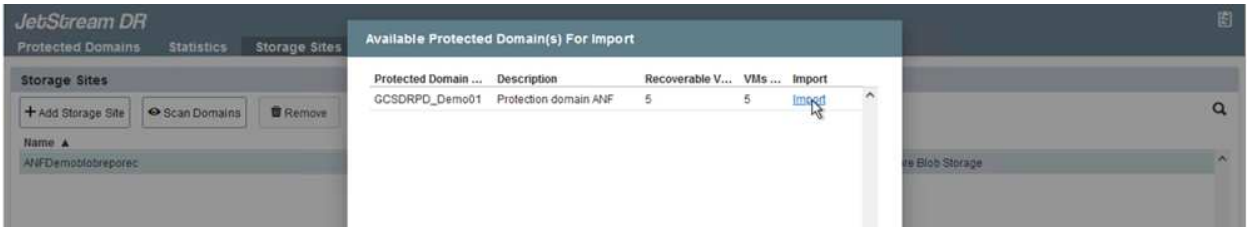
   以下屏幕截图显示了使用基于 DHCP 的 IP 地址的安装。



2. JetStream DR for AVS 安装完成后，刷新浏览器。要访问 JetStream DR UI，请转到 SDDC 数据中心 > 配置 > JetStream DR。



3. 从 JetStream DR 界面完成以下任务：
   a. 添加用于保护本地集群的 Azure Blob 存储帐户作为存储站点，然后运行扫描域选项。
   b. 在出现的弹出对话框窗口中，选择要导入的受保护域，然后单击其导入链接。



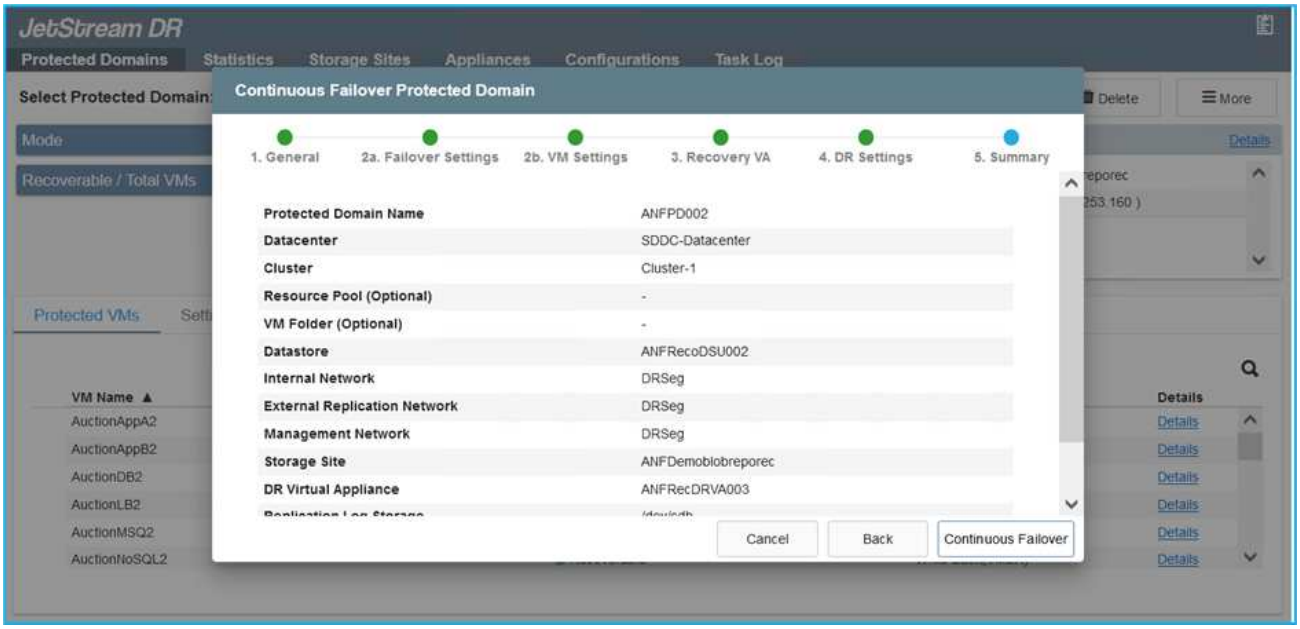
4. 该域名已导入以进行恢复。转到“受保护的域”选项卡并验证是否已选择目标域，或者从“选择受保护的域”菜单中选择所需的域。显示受保护域中可恢复的虚拟机列表。



5. 导入受保护域后，部署 DRVA 设备。

> 这些步骤也可以使用 CPT 创建的计划自动执行。

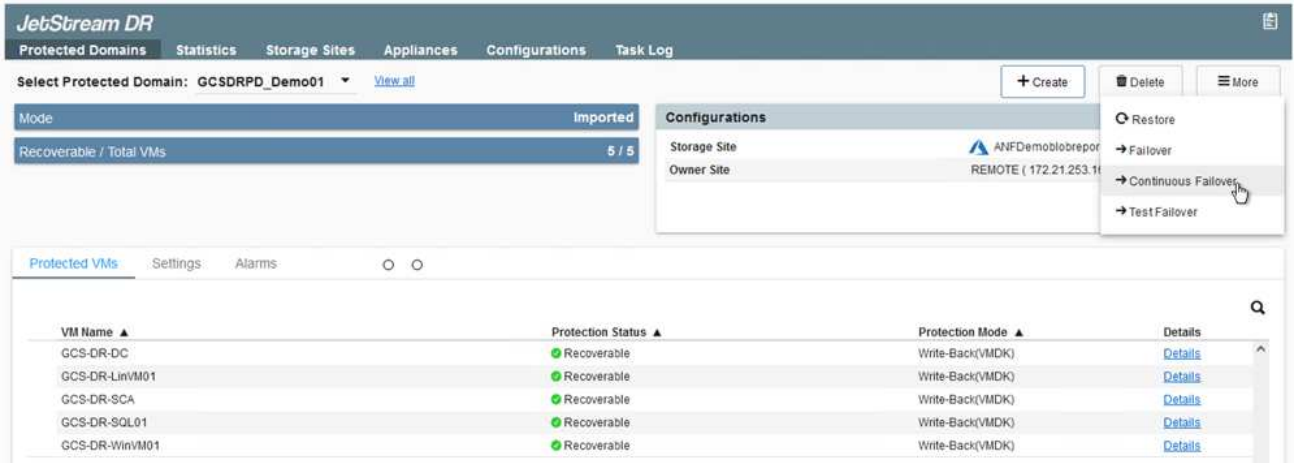
6. 使用可用的 vSAN 或 ANF 数据存储创建复制日志卷。
7. 导入受保护的域并配置恢复 VA 以使用 ANF 数据存储进行 VM 放置。



确保所选网段上启用了 DHCP，并且有足够的可用 IP。在域名恢复期间，暂时使用动态 IP。每个恢复的虚拟机（包括持续补水）都需要一个单独的动态 IP。恢复完成后，IP 被释放并可重复使用。

8. 选择适当的故障转移选项（连续故障转移或故障转移）。在这个例子中，选择了持续补水（持续故障转移）。

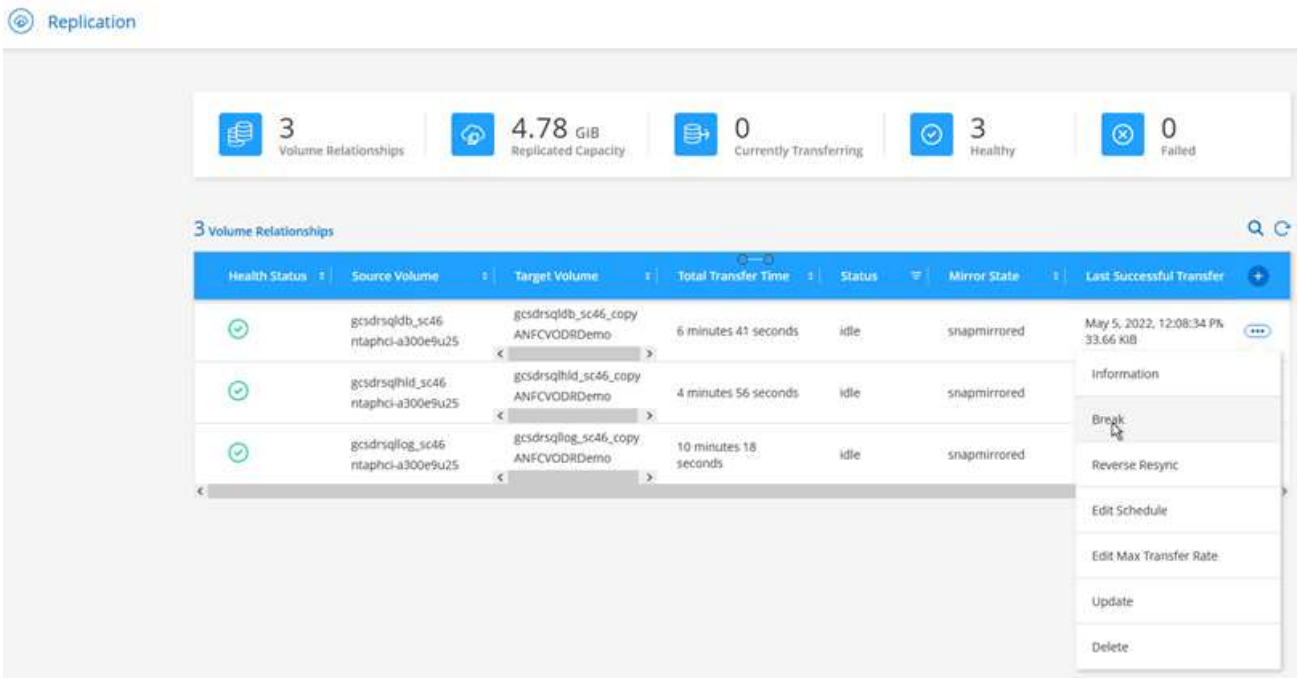
尽管连续故障转移和故障转移模式在执行配置时有所不同，但两种故障转移模式都使用相同的步骤进行配置。故障转移步骤是一起配置和执行的，以应对灾难事件。可以随时配置连续故障转移，然后允许其在正常系统运行期间在后台运行。灾难事件发生后，完成持续故障转移，立即将受保护虚拟机的所有权转移到恢复站点（接近零 RTO）。

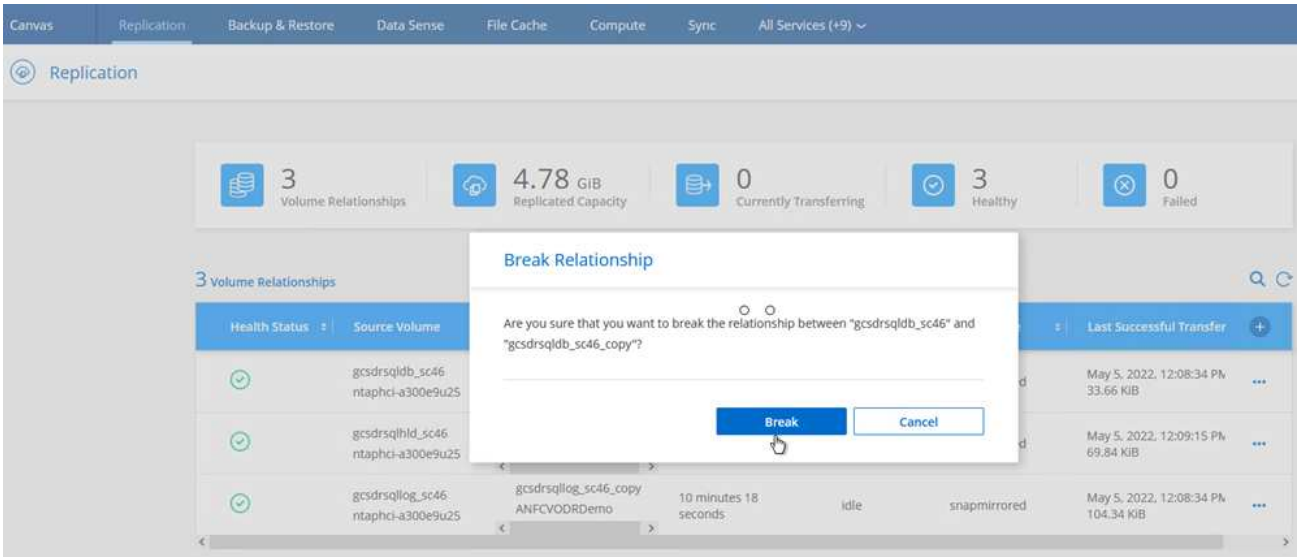


持续故障转移过程开始，并且可以从 UI 监控其进度。单击“当前步骤”部分中的蓝色图标将打开一个弹出窗口，其中显示故障转移过程当前步骤的详细信息。

▼ 故障转移和故障恢复

1. 当本地环境的受保护集群发生灾难（部分或全部故障）后，您可以在中断各个应用程序卷的SnapMirror关系后，使用 Jetstream 触发虚拟机的故障转移。

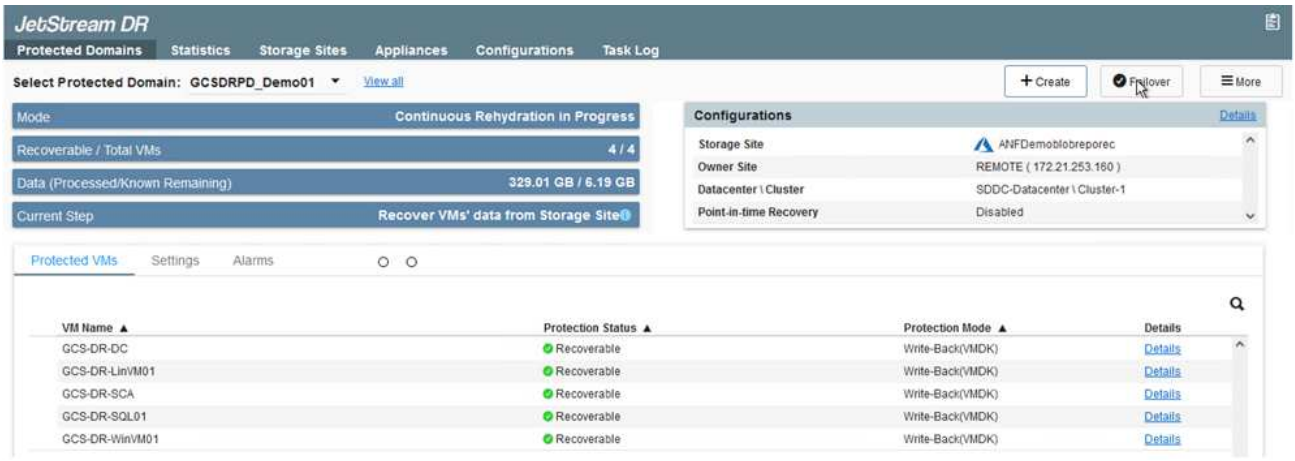


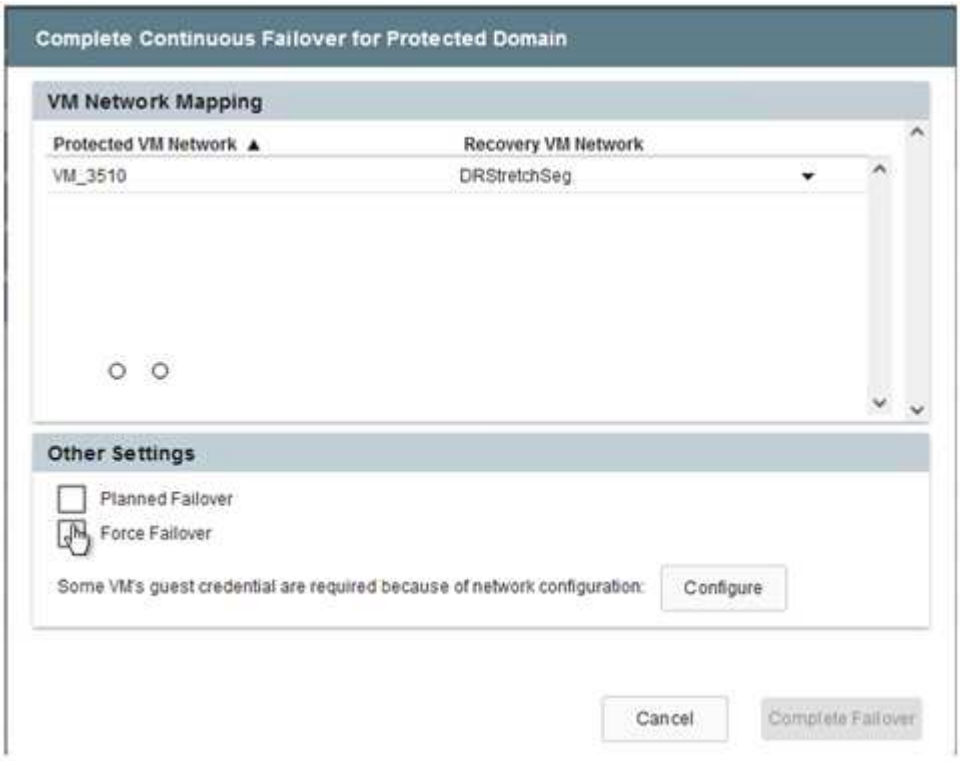


此步骤可以轻松实现自动化，以促进恢复过程。

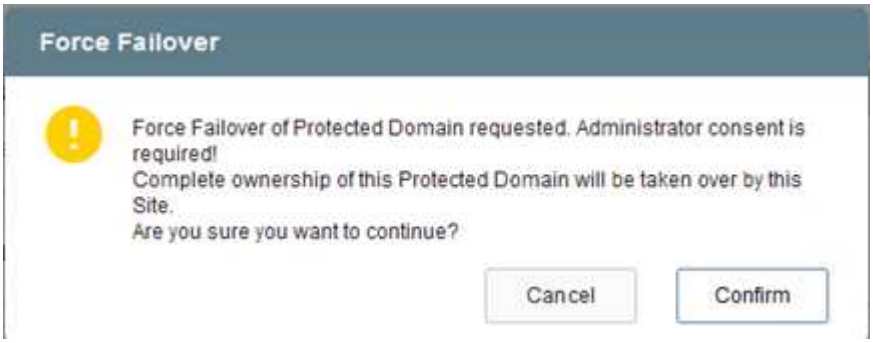
2. 访问 AVS SDDC（目标端）上的 Jetstream UI 并触发故障转移选项以完成故障转移。任务栏显示故障转移活动的进度。

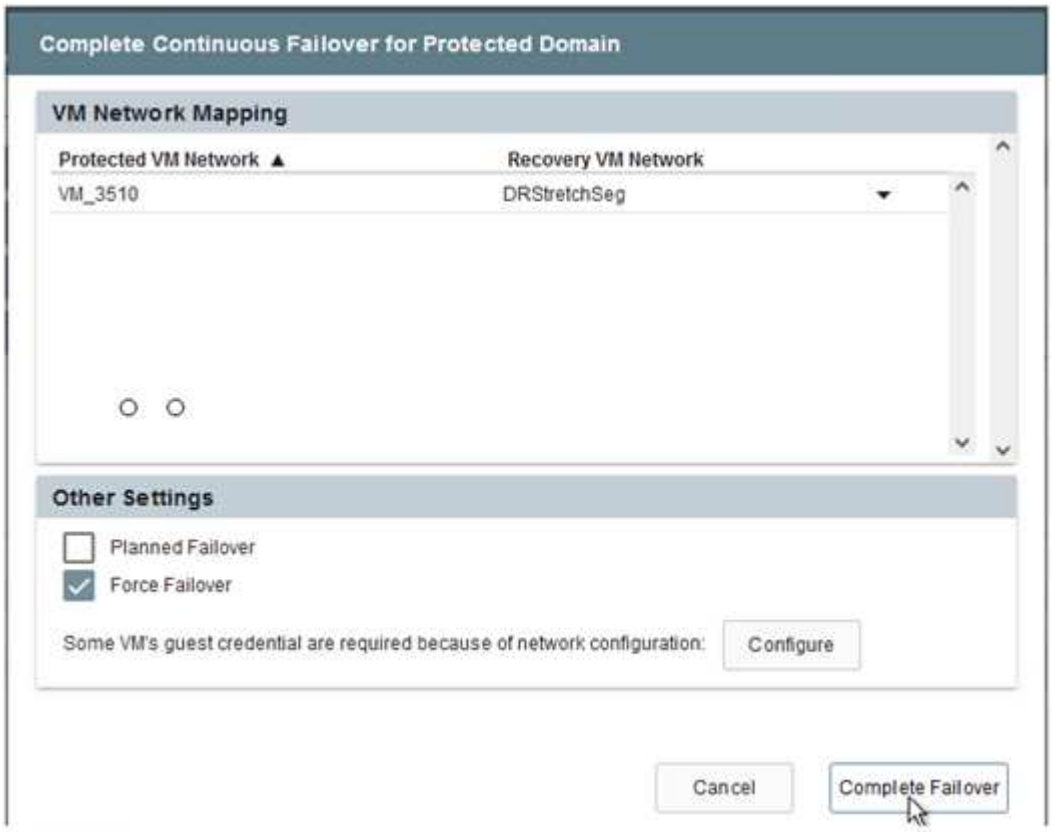
   在完成故障转移时出现的对话窗口中，可以将故障转移任务指定为计划的或假定为强制的。





强制故障转移假定主站点不再可访问，并且受保护域的所有权应由恢复站点直接承担。





3. 连续故障转移完成后，会出现一条消息确认任务完成。任务完成后，访问恢复的虚拟机以配置 ISCSI 或 NFS 会话。

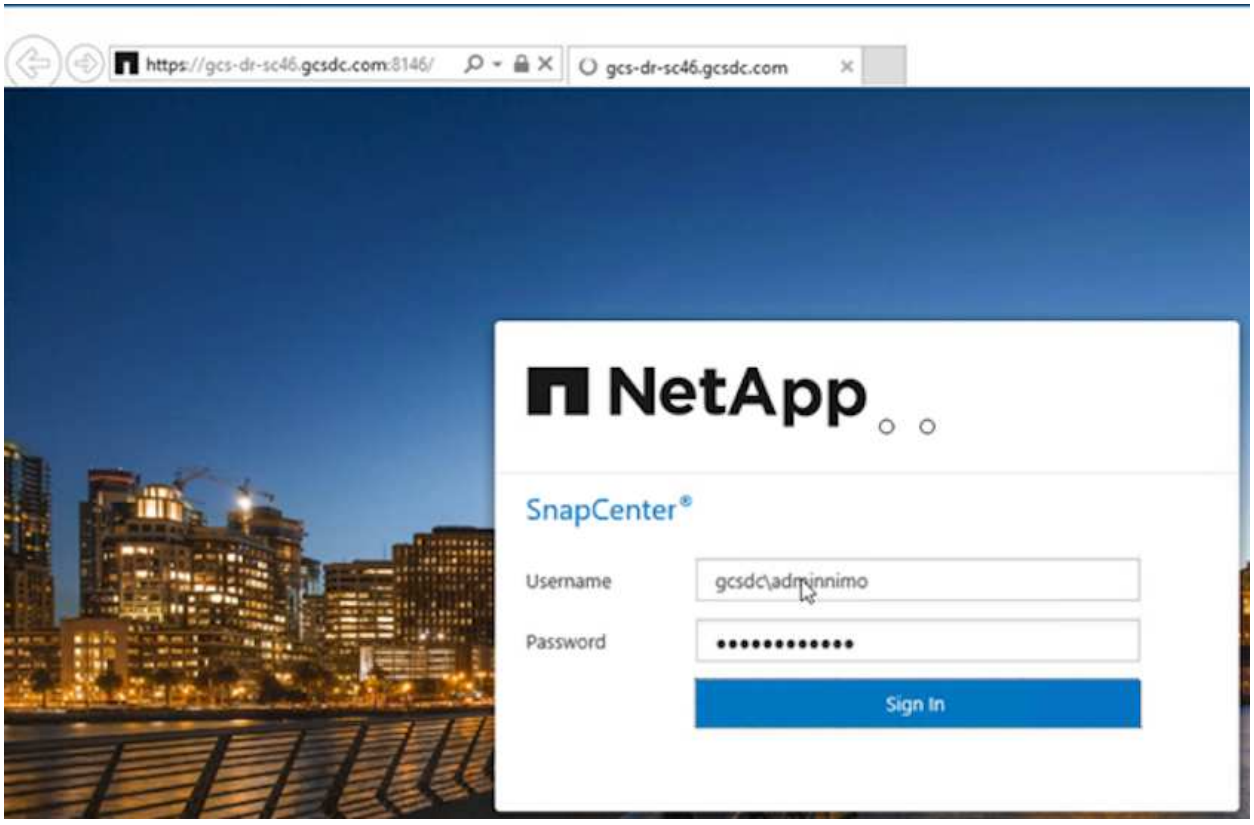
故障转移模式变为“故障转移中正在运行”，虚拟机状态变为“可恢复”。受保护域的所有虚拟机现在都在恢复站点上运行，并且处于故障转移运行手册设置指定的状态。

为了验证故障转移配置和基础设施，JetStream DR 可以在测试模式下运行（测试故障转移选项），以观察虚拟机及其数据从对象存储到测试恢复环境的恢复情况。当在测试模式下执行故障转移过程时，其操作类似于实际的故障转移过程。

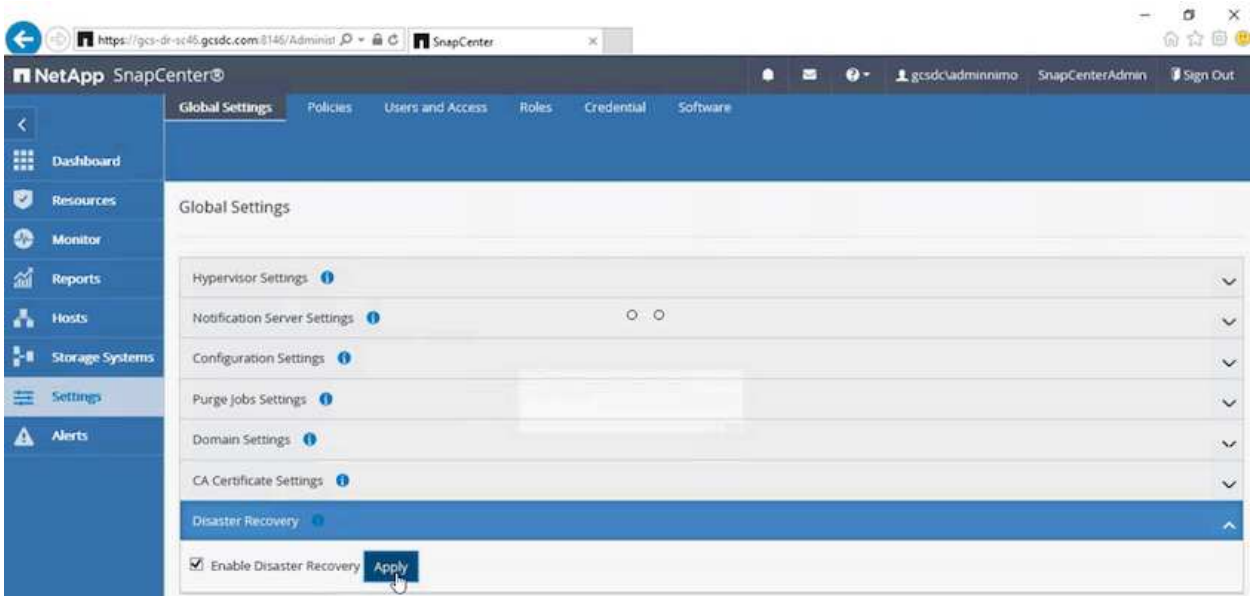


4. 虚拟机恢复后，使用存储灾难恢复进行来宾存储。为了演示此过程，本例中使用了 SQL 服务器。

5. 登录 AVS SDDC 上恢复的SnapCenter VM 并启用 DR 模式。
   a. 使用浏览器访问SnapCenter UI。



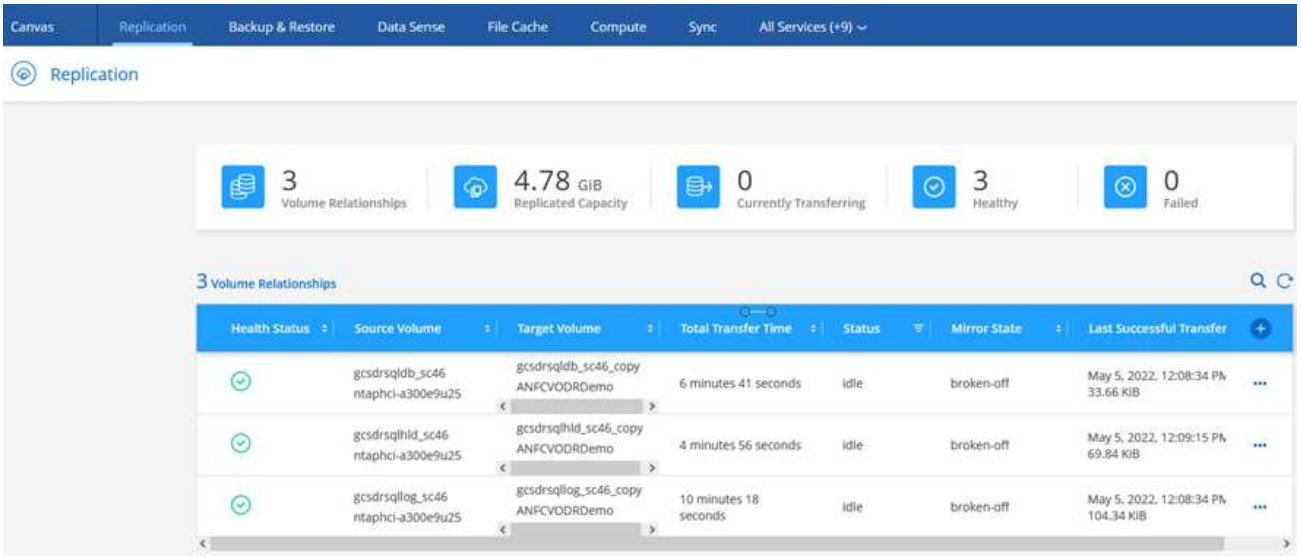
   b. 在设置页面中，导航到设置> 全局设置> 灾难恢复。
   c. 选择启用灾难恢复。
   d. 单击“应用”。



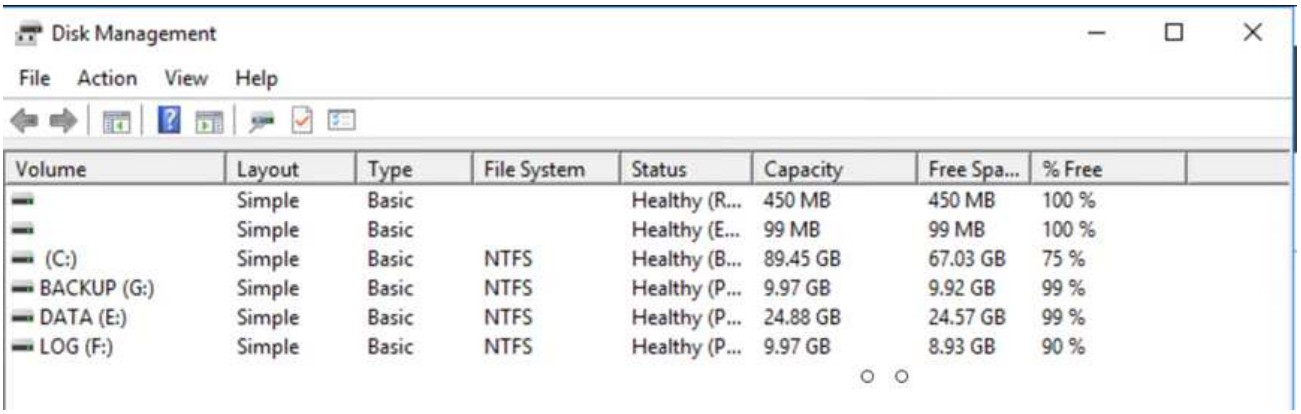
   e. 单击“监视”>“作业”来验证 DR 作业是否已启用。

应使用NetApp SnapCenter 4.6 或更高版本进行存储灾难恢复。对于以前的版本，应使用应用程序一致性快照（使用SnapMirror复制），并且应执行手动恢复，以防必须在灾难恢复站点恢复以前的备份。

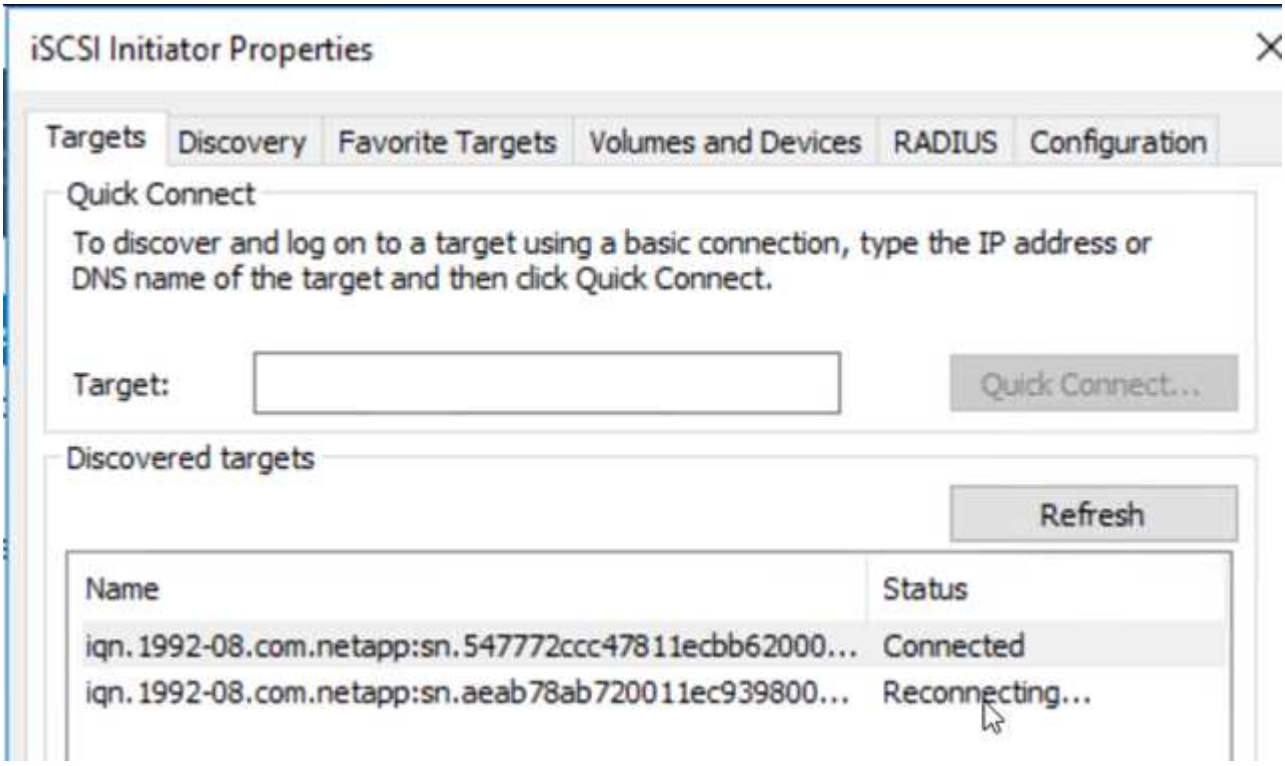
6. 确保SnapMirror关系已中断。



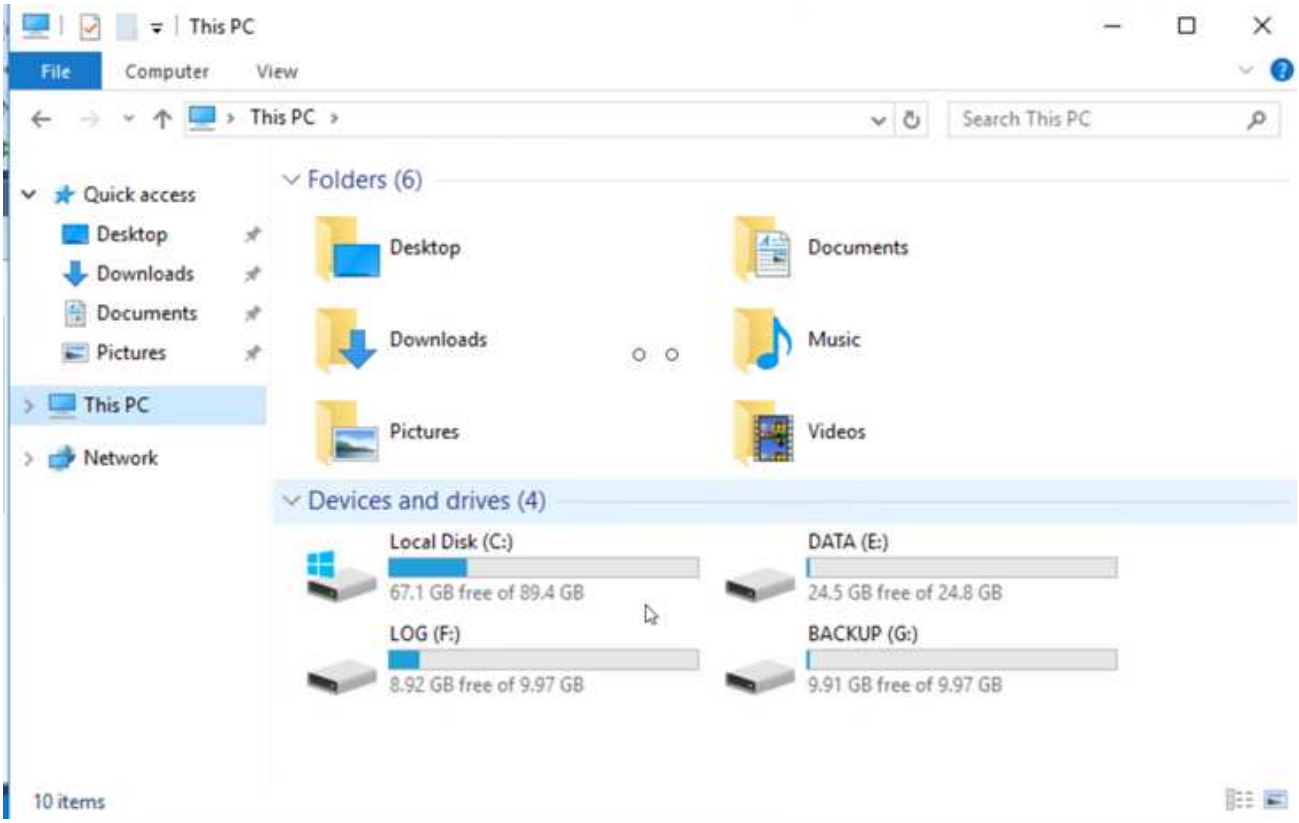
7. 将Cloud Volumes ONTAP中的 LUN 连接到具有相同驱动器号的恢复的 SQL 客户虚拟机。



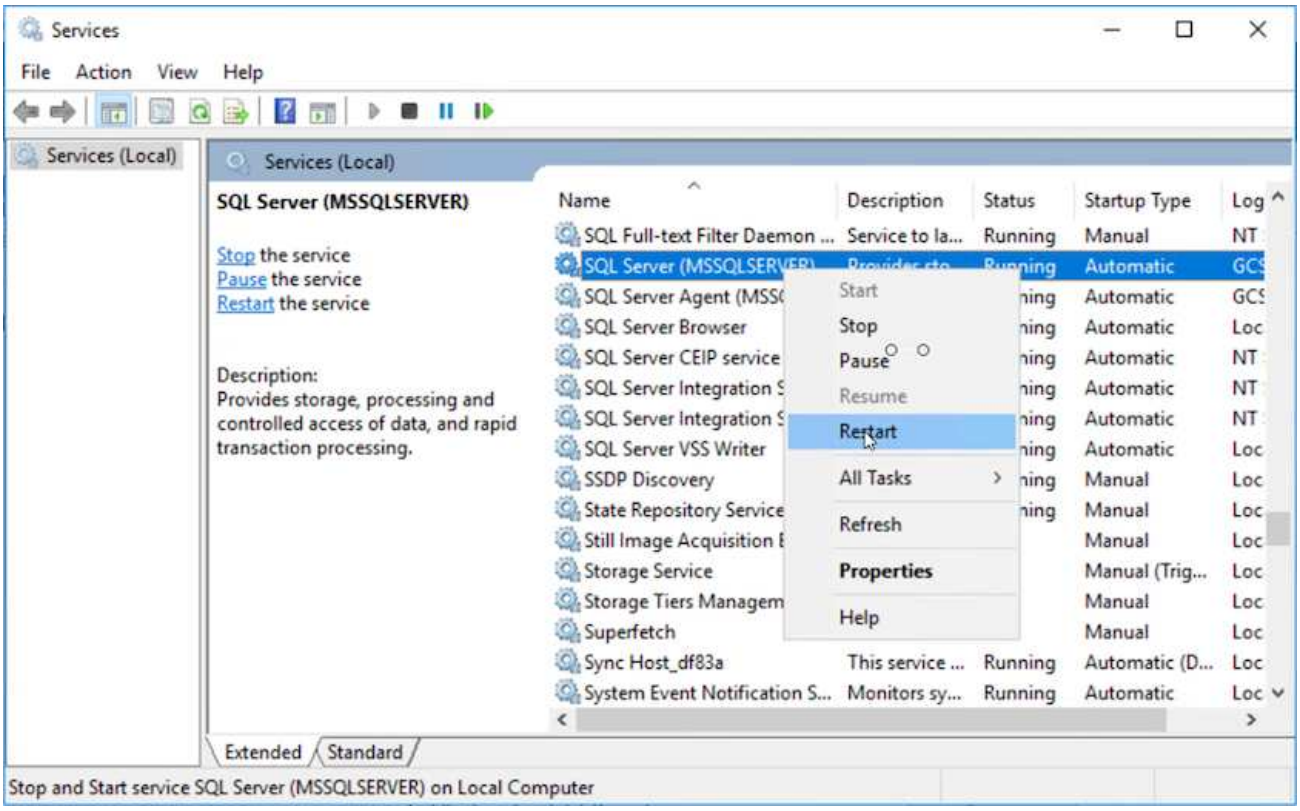
8. 打开 iSCSI 启动器，清除之前断开的会话，并为复制的Cloud Volumes ONTAP卷添加新目标以及多路径。



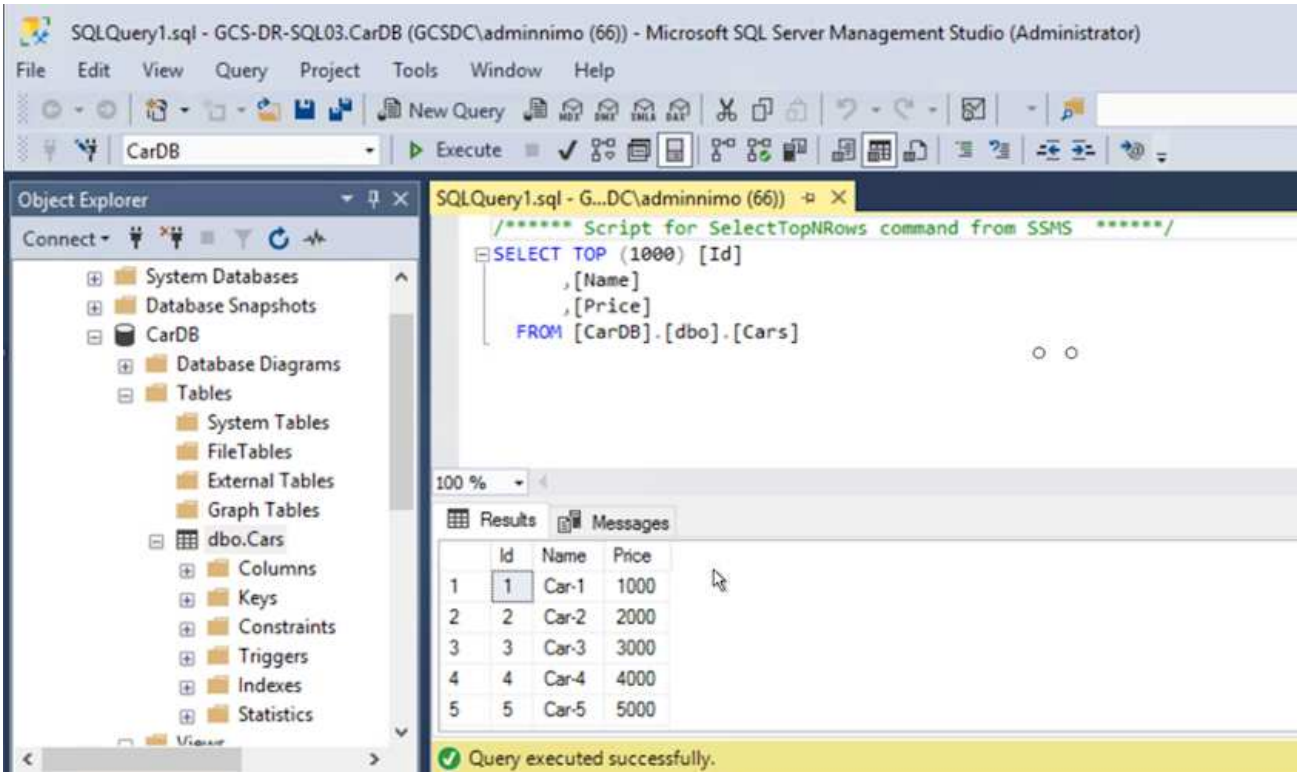
9. 确保所有磁盘都使用 DR 之前使用的相同驱动器号进行连接。



10. 重新启动 MSSQL 服务器服务。



11. 确保 SQL 资源已恢复在线。



对于 NFS，使用 mount 命令附加卷并更新 `/etc/fstab`条目。

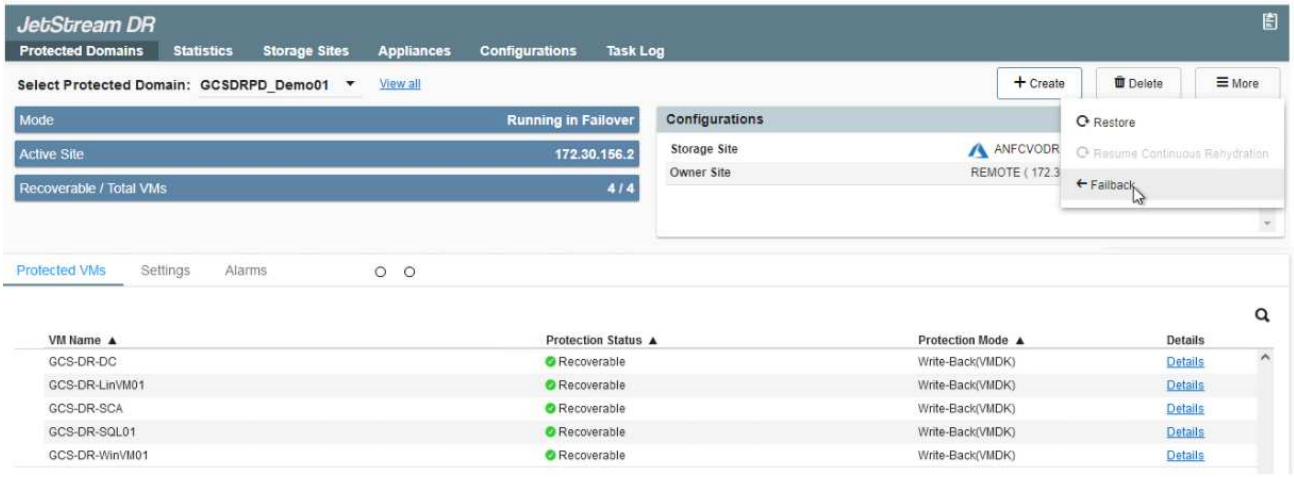
此时，操作可以运行并且业务可以继续正常进行。

在 NSX-T 端，可以创建单独的专用第 1 层网关来模拟故障转移场景。这可确保所有工作负载可以相互通信，但不会有任何流量可以路由进出环境，从而可以执行任何分类、遏制或强化任务而不会有交叉污染的风险。此操作超出了本文档的范围，但可以轻松实现模拟隔离。

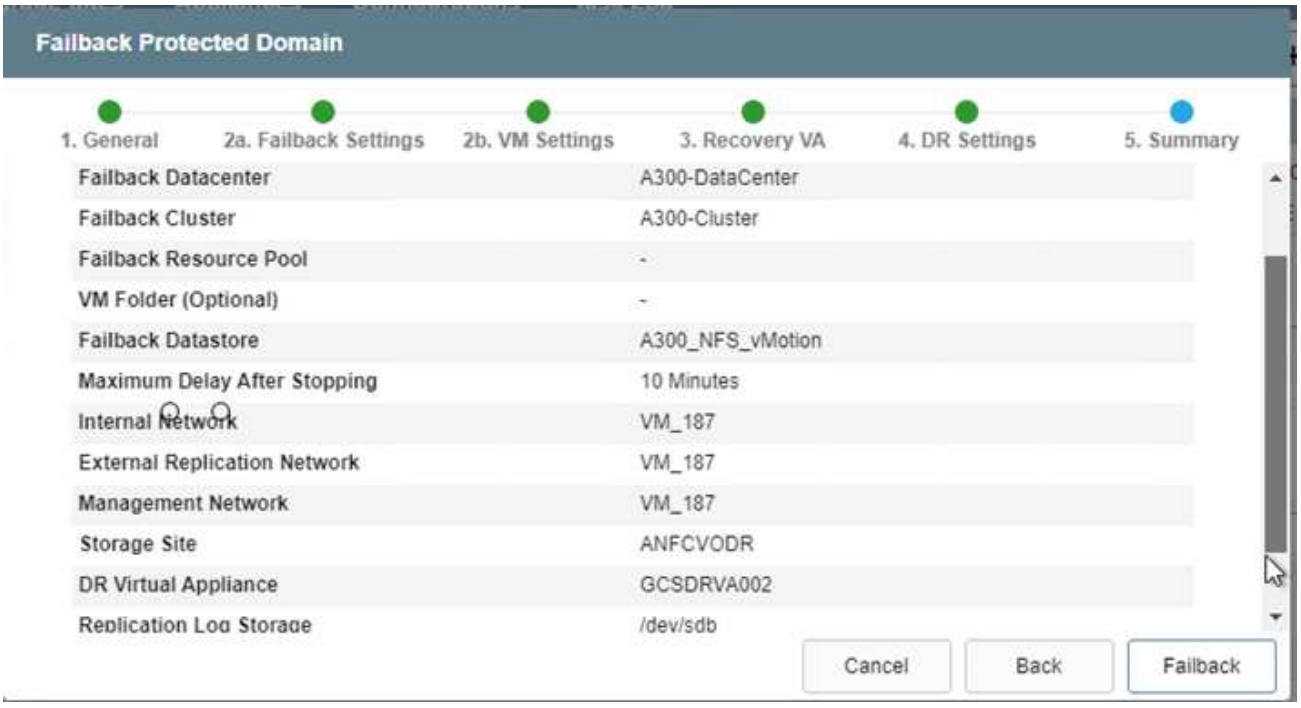
主站点重新启动并运行后，您可以执行故障恢复。 VM 保护由 Jetstream 恢复，并且必须逆转SnapMirror关系。

1. 恢复本地环境。根据灾难事件的类型，可能需要恢复和/或验证受保护集群的配置。如有必要，可能需要重新安装 JetStream DR 软件。
2. 访问恢复的本地环境，转到 Jetstream DR UI，然后选择适当的受保护域。受保护站点准备好故障恢复后，在 UI 中选择故障恢复选项。

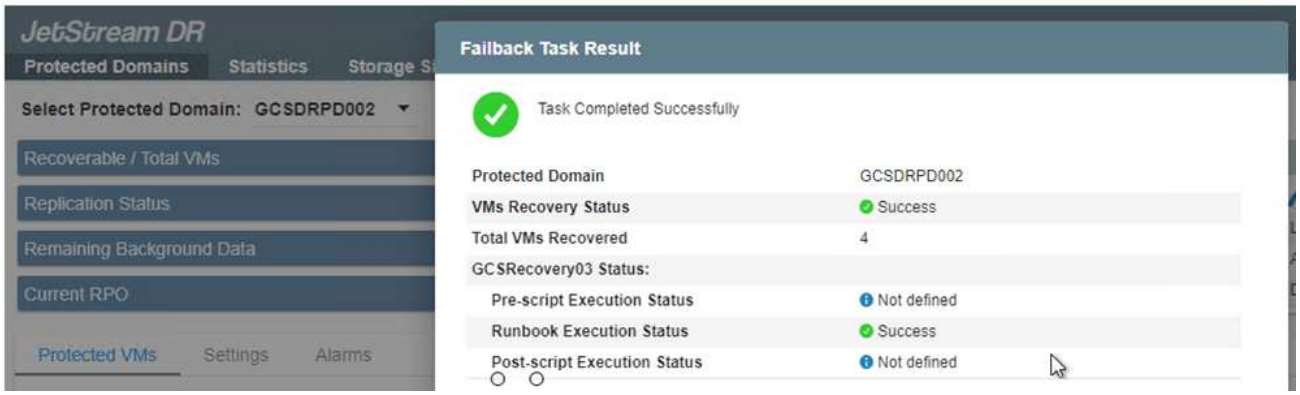
CPT 生成的故障恢复计划还可用于启动虚拟机及其数据从对象存储返回到原始 VMware 环境。



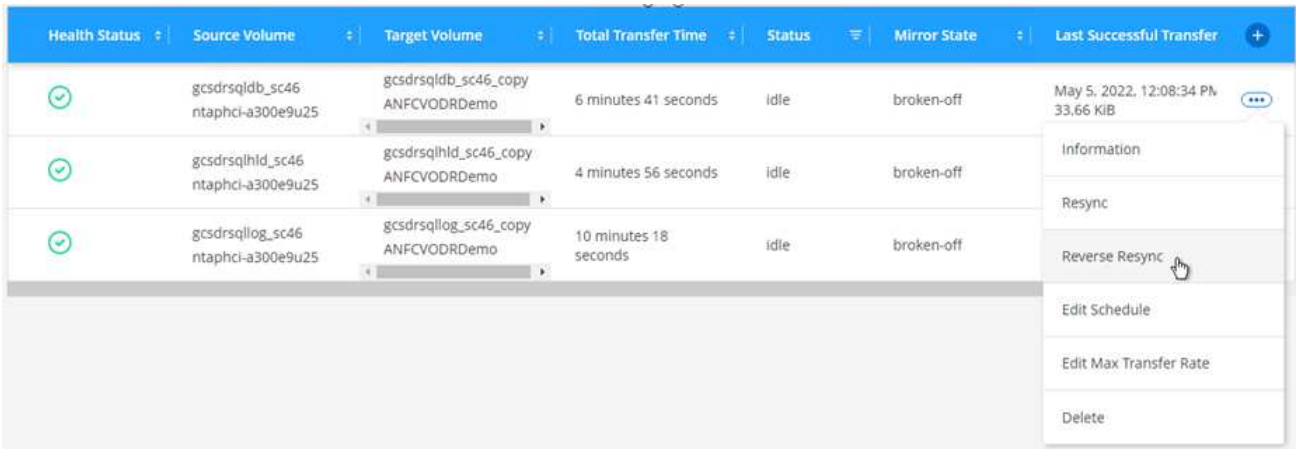
指定在恢复站点中暂停虚拟机并在受保护站点中重新启动虚拟机后的最大延迟。完成此过程所需的时间包括停止故障转移虚拟机后完成复制的时间、清理恢复站点所需的时间以及在受保护站点中重新创建虚拟机所需的时间。 NetApp建议 10 分钟。

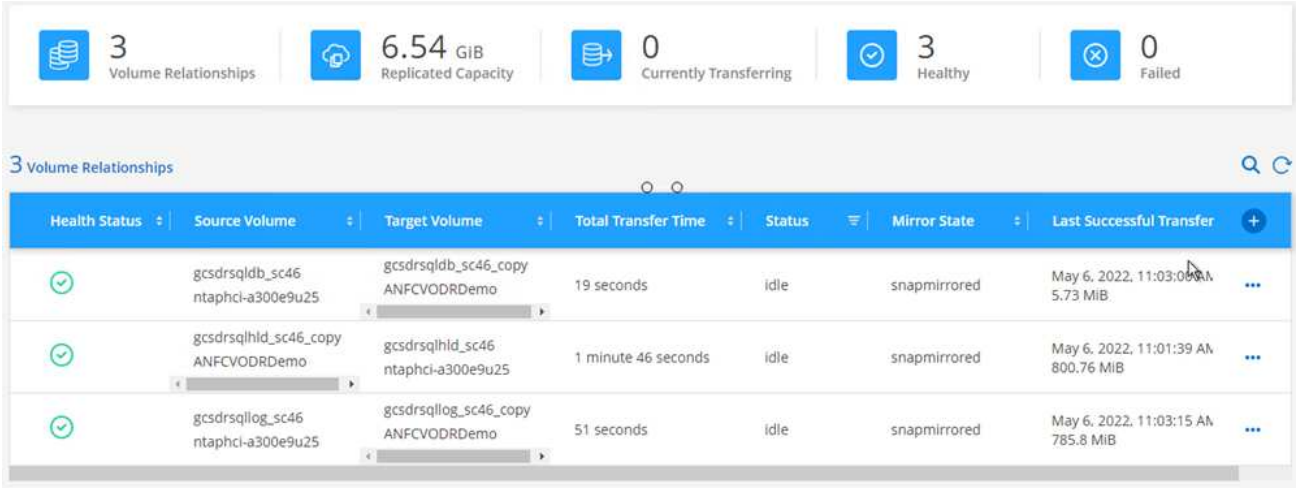


3. 完成故障恢复过程，然后确认恢复虚拟机保护和数据一致性。

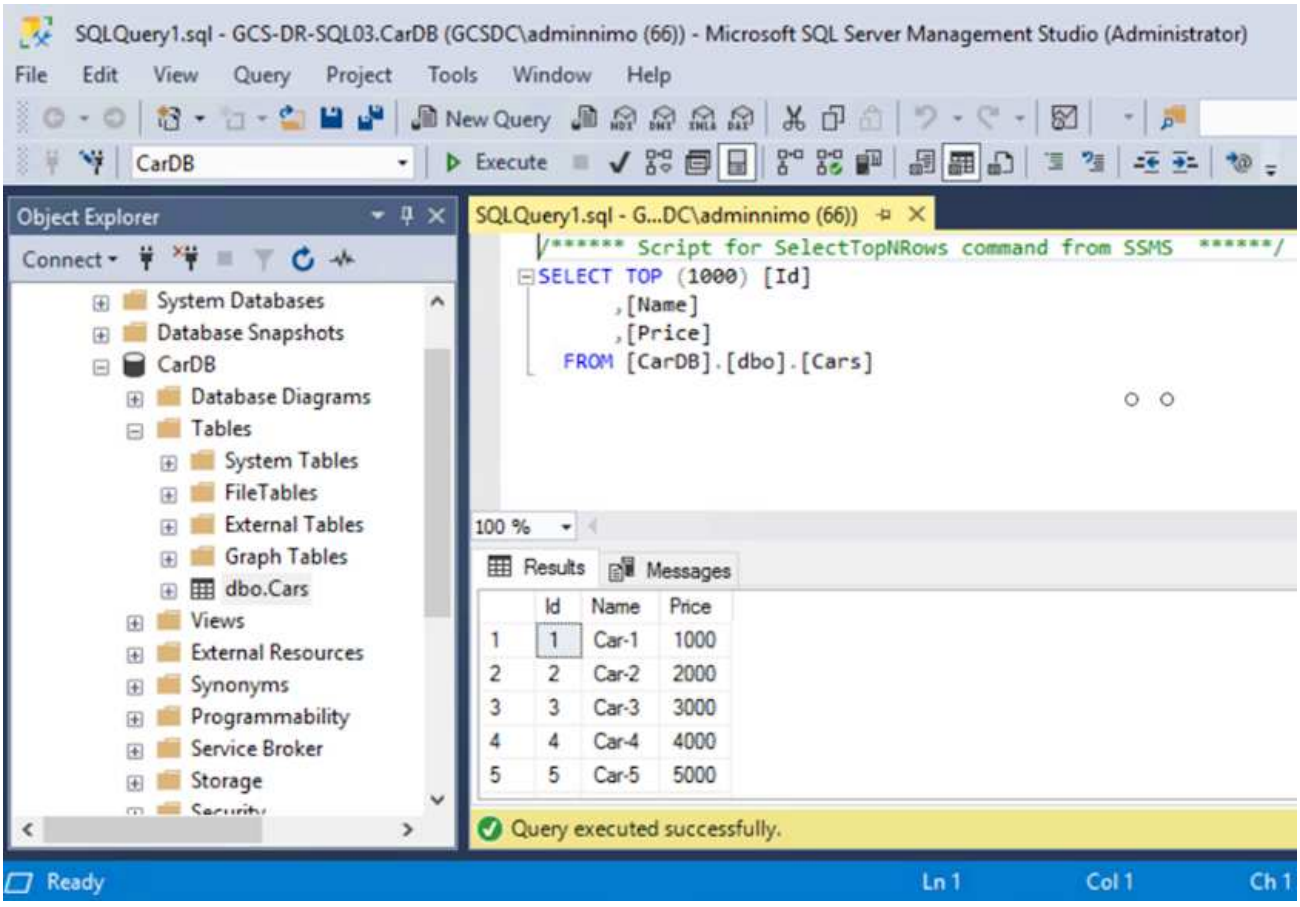


4. 虚拟机恢复后，断开辅助存储与主机的连接并连接到主存储。





5. 重新启动 MSSQL 服务器服务。
6. 验证 SQL 资源是否已恢复联机。



要故障恢复到主存储，请通过执行反向重新同步操作确保关系方向与故障转移之前保持相同。

为了在反向重新同步操作后保留主存储和辅助存储的角色，请再次执行反向重新同步操作。

此过程适用于其他应用程序，如 Oracle、类似的数据库类型以及任何其他使用来宾连接存储的应用程序。

与往常一样，在将关键工作负载转移到生产环境之前，请先测试恢复所涉及的步骤。

此解决方案的优势

- 使用SnapMirror的高效且有弹性的复制。
- 通过ONTAP快照保留恢复到任何可用的时间点。
- 从存储、计算、网络和应用程序验证步骤，恢复数百到数千台虚拟机所需的所有步骤均可实现完全自动化。
- SnapCenter使用不会改变复制卷的克隆机制。
  - 这避免了卷和快照数据损坏的风险。
  - 避免 DR 测试工作流程期间的复制中断。
  - 利用 DR 数据进行 DR 以外的工作流程，例如开发/测试、安全测试、补丁和升级测试以及补救测试。
- CPU 和 RAM 优化可以通过恢复到较小的计算集群来帮助降低云成本。

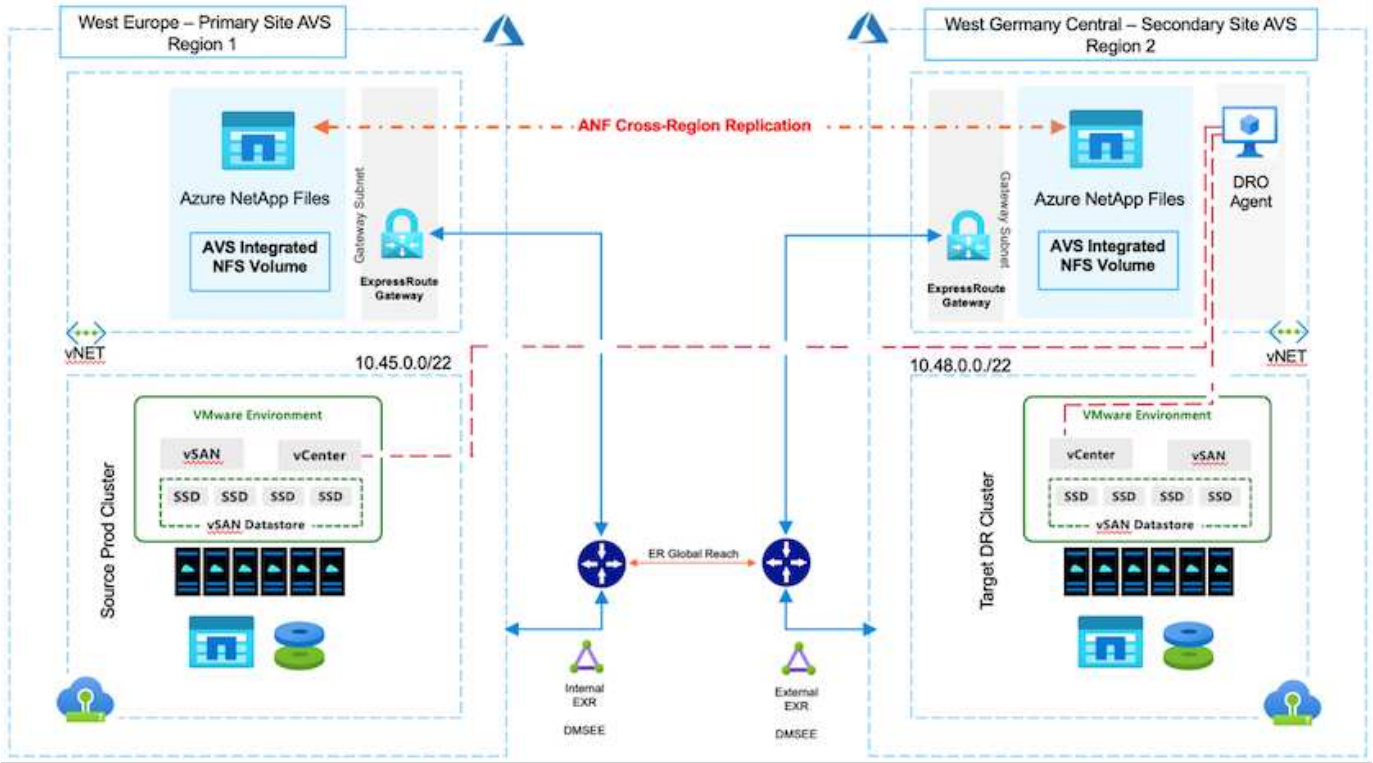
TR-4955：使用**Azure NetApp Files(ANF)** 和 **Azure VMware** 解决方案 **(AVS)** 进行灾难恢复

使用云内区域之间的块级复制进行灾难恢复是一种有弹性且经济高效的方法，可以保护工作负载免受站点中断和数据损坏事件（例如勒索软件）的影响。

概述

借助 Azure NetApp文件 (ANF) 跨区域卷复制，在 Azure VMware 解决方案 (AVS) SDDC 站点上运行的 VMware 工作负载（使用 Azure NetApp文件卷作为主 AVS 站点上的 NFS 数据存储）可以复制到目标恢复区域中的指定辅助 AVS 站点。

灾难恢复编排器 (DRO)（带有 UI 的脚本解决方案）可用于无缝恢复从一个 AVS SDDC 复制到另一个 AVS SDDC 的工作负载。 DRO 通过中断复制对等，然后将目标卷作为数据存储安装，通过 VM 注册到 AVS，再到 NSX-T 上的网络映射（包含在所有 AVS 私有云中）来实现自动恢复。



先决条件和一般建议

- 通过创建复制对等连接来验证您是否已启用跨区域复制。看 "为Azure NetApp Files创建卷复制"。
- 必须在源和目标 Azure VMware 解决方案私有云之间配置 ExpressRoute Global Reach。
- 您必须拥有可以访问资源的服务主体。
- 支持以下拓扑：主 AVS 站点到辅助 AVS 站点。
- 配置 "replication"根据业务需求和数据变化率适当地安排每个卷。

不支持级联和扇入扇出拓扑。

入门

部署 **Azure VMware** 解决方案

这 "Azure VMware 解决方案"(AVS) 是一种混合云服务，可在 Microsoft Azure 公共云中提供功能齐全的 VMware SDDC。 AVS 是使用 Azure 基础架构、完全由 Microsoft 管理和支持并经过 VMware 验证的第一方解决方案。因此，客户可以获得用于计算虚拟化的 VMware ESXi、用于超融合存储的 vSAN 以及用于网络和安全的 NSX，同时利用 Microsoft Azure 的全球影响力、一流的数据中心设施以及与丰富的原生 Azure 服务和解决方案生态系统的接近性。 Azure VMware 解决方案 SDDC 和Azure NetApp Files的组合以最小的网络延迟提供了最佳性能。

要在 Azure 上配置 AVS 私有云，请按照以下步骤操作"链接"请参阅NetApp文档以及 "链接"用于 Microsoft 文档。可以使用以最小配置设置的指示灯环境来实现 DR 目的。此设置仅包含支持关键应用程序的核心组件，并且如果发生故障转移，它可以扩展并产生更多主机来承担大部分负载。

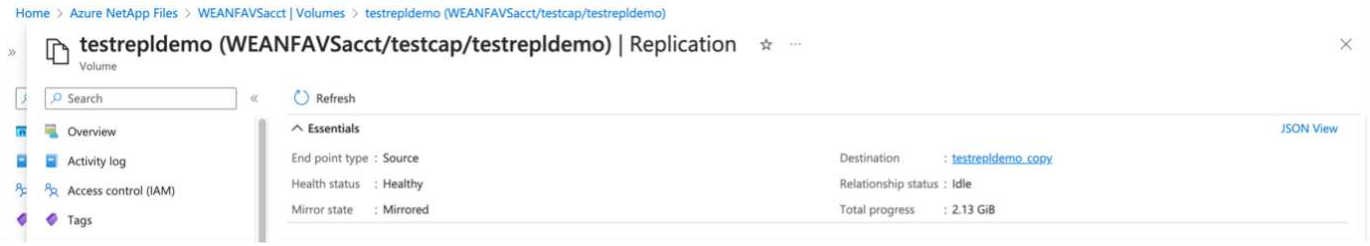
在初始版本中，DRO 支持现有的 AVS SDDC 集群。按需 SDDC 创建功能将在即将发布的版本中提供。

预配和配置Azure NetApp Files

"Azure NetApp Files"是一种高性能、企业级、计量文件存储服务。按照以下步骤操作 "链接"将Azure NetApp Files配置为 NFS 数据存储，以优化 AVS 私有云部署。

为Azure NetApp Files支持的数据存储卷创建卷复制

第一步是设置所需数据存储卷从 AVS 主站点到 AVS 辅助站点的跨区域复制，并采用适当的频率和保留。



按照以下步骤操作 "链接"通过创建复制对等来设置跨区域复制。目标容量池的服务级别可以与源容量池的服务级别匹配。但是，对于这个特定的用例，您可以选择标准服务级别，然后 "修改服务级别"在发生真实灾难或 DR 模拟时。

跨区域复制关系是先决条件，必须事先创建。

DRO安装

要开始使用 DRO，请在指定的 Azure 虚拟机上使用 Ubuntu 操作系统并确保满足先决条件。然后安装该包。

先决条件：

- 可以访问资源的服务主体。
- 确保源和目标 SDDC 以及Azure NetApp Files实例之间存在适当的连接。
- 如果您使用 DNS 名称，则应该进行 DNS 解析。否则，请使用 vCenter 的 IP 地址。

操作系统要求：

- Ubuntu Focal 20.04 (LTS)必须在指定的代理虚拟机上安装以下软件包：
- Docker
- Docker-Compose
- JqChange `docker.sock`对于这个新权限： `sudo chmod 666 /var/run/docker.sock`。

这 `deploy.sh`脚本执行所有必需的先决条件。

步骤如下：

1. 在指定虚拟机上下载安装包：

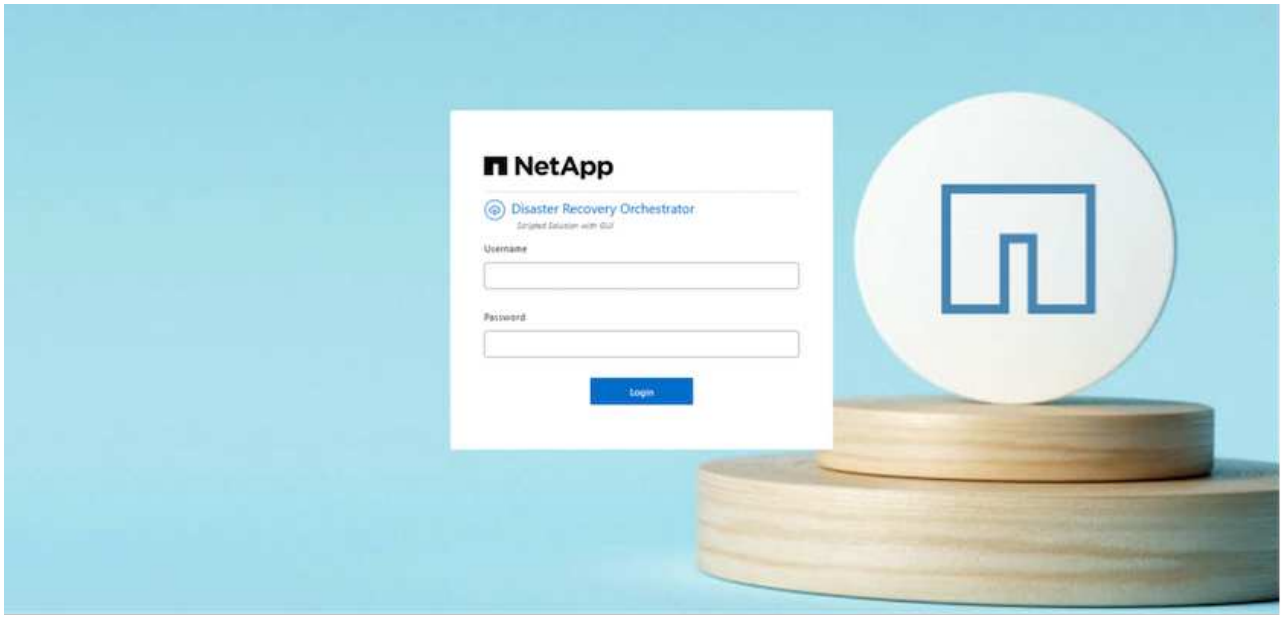
```
git clone https://github.com/NetApp/DRO-Azure.git
```

该代理必须安装在辅助 AVS 站点区域或与 SDDC 不同的 AZ 中的主 AVS 站点区域中。

2. 解压安装包，运行部署脚本，输入主机IP（例如， `10.10.10.10` ）。

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. 使用以下凭据访问 UI：
   - 用户名: `admin`
   - 密码： `admin`



DRO 配置

正确配置Azure NetApp Files和 AVS 后，您可以开始配置 DRO 以自动将工作负载从主 AVS 站点恢复到辅助 AVS 站点。 NetApp建议在辅助 AVS 站点部署 DRO 代理并配置 ExpressRoute 网关连接，以便 DRO 代理可以通过网络与适当的 AVS 和Azure NetApp Files组件进行通信。

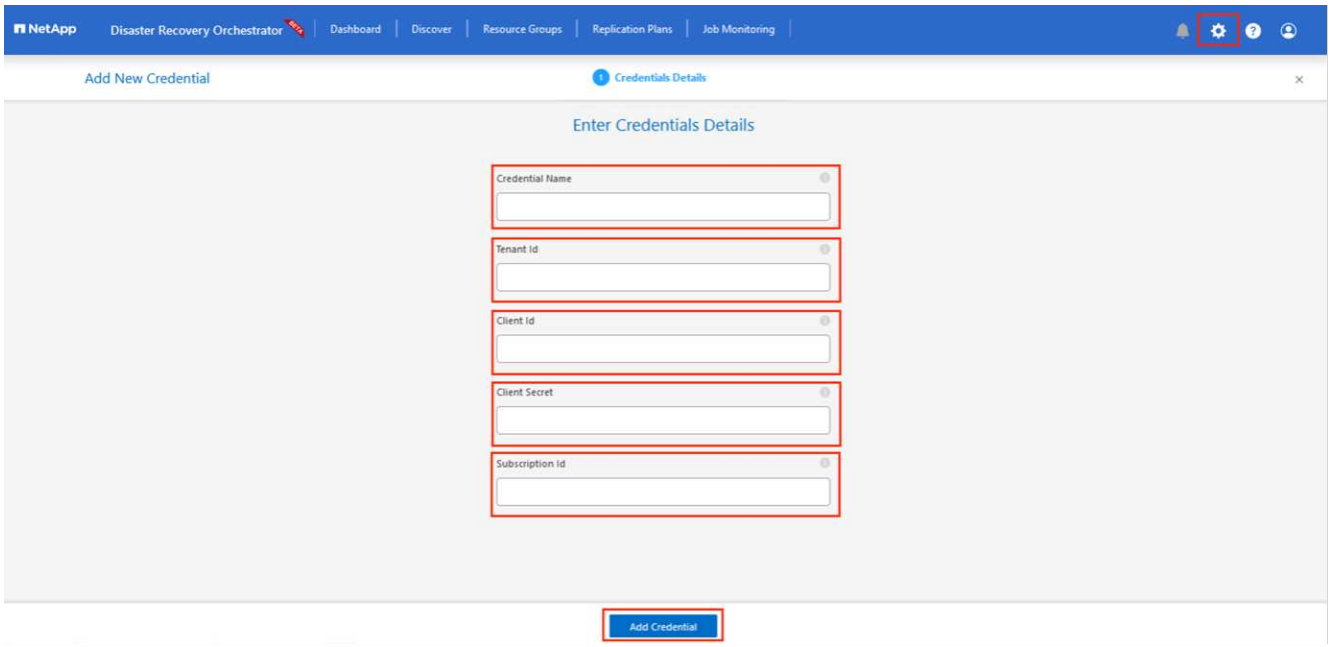
第一步是添加凭证。 DRO 需要权限才能发现Azure NetApp Files和 Azure VMware 解决方案。您可以通过创建和设置 Azure Active Directory (AD) 应用程序并获取 DRO 所需的 Azure 凭据来向 Azure 帐户授予所需的权限。您必须将服务主体绑定到您的 Azure 订阅，并为其分配具有相关所需权限的自定义角色。添加源环境和目标环境时，系统会提示您选择与服务主体关联的凭据。您需要将这些凭据添加到 DRO，然后才能单击“添加新站点”。

要执行此操作，请完成以下步骤：

1. 在支持的浏览器中打开 DRO 并使用默认用户名和密码(`admin/admin`）。首次登录后可以使用“更改密码”选项重置密码。
2. 在 DRO 控制台的右上角，单击 设置 图标，然后选择 凭据。

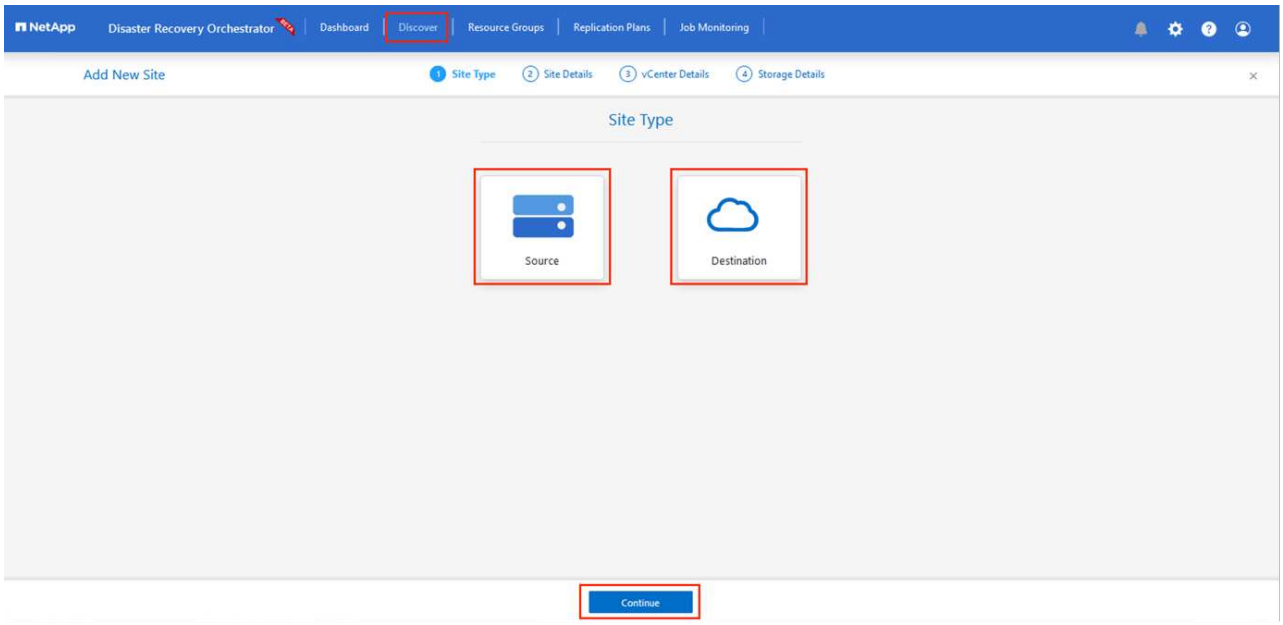
3. 单击“添加新凭据”并按照向导中的步骤进行操作。
4. 要定义凭据，请输入有关授予所需权限的 Azure Active Directory 服务主体的信息：
   - 凭证名称
   - 租户 ID
   - 客户端 ID
   - 客户端机密
   - 订阅 ID

   您应该在创建 AD 应用程序时捕获此信息。
5. 确认有关新凭证的详细信息，然后单击“添加凭证”。



添加凭据后，就可以发现并将主 AVS 站点和辅助 AVS 站点（vCenter 和 Azure NetApp文件存储帐户）添加到 DRO。要添加源站点和目标站点，请完成以下步骤：

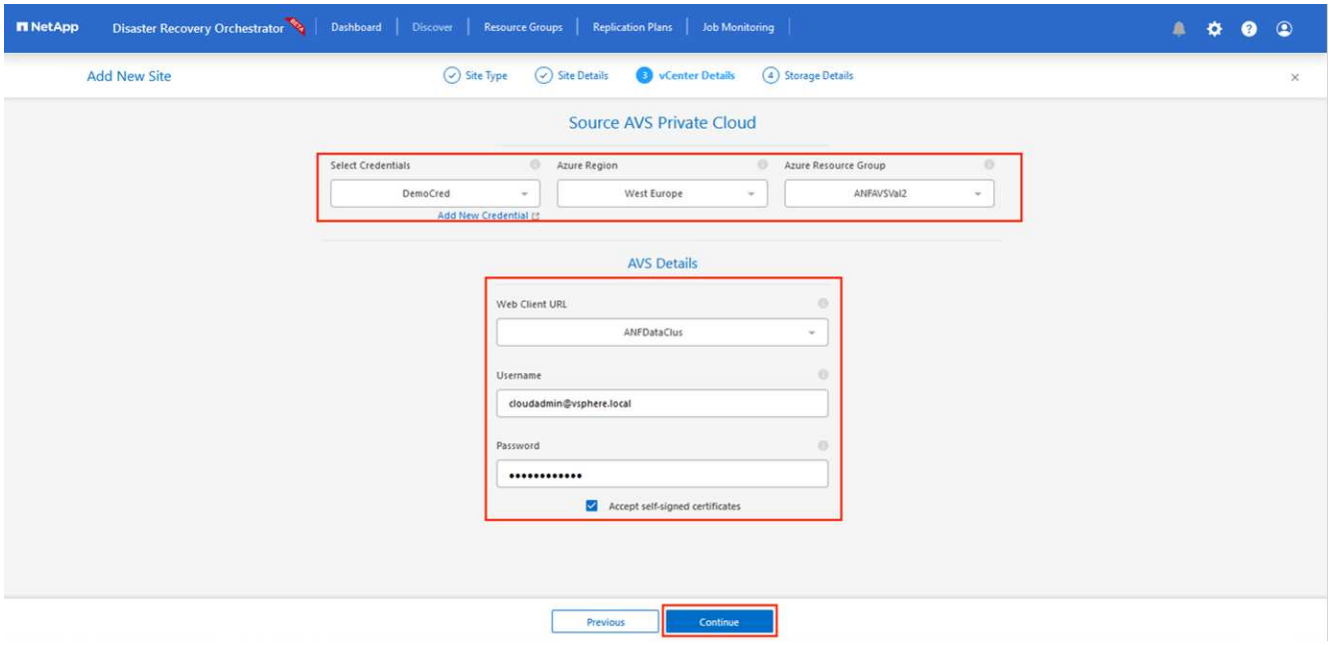
6. 转到“发现”选项卡。
7. 单击“添加新站点”。
8. 添加以下主要 AVS 站点（在控制台中指定为 源）。
   - SDDC vCenter
   - Azure NetApp Files存储帐户
9. 添加以下辅助 AVS 站点（在控制台中指定为 目标）。
   - SDDC vCenter
   - Azure NetApp Files存储帐户



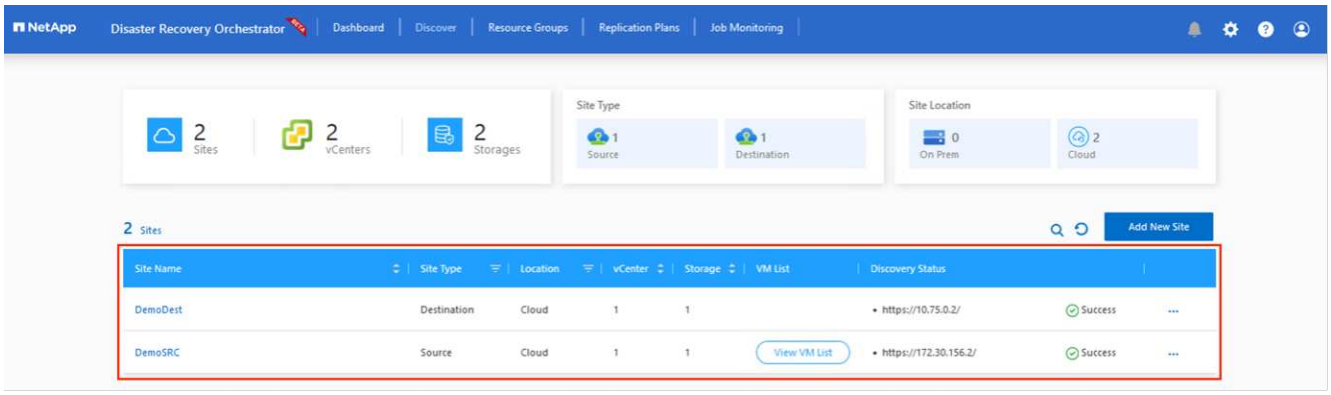
10. 通过单击“源”，输入友好的站点名称并选择连接器来添加站点详细信息。然后点击“继续”。

> 为了演示目的，本文档涵盖了添加源站点的内容。

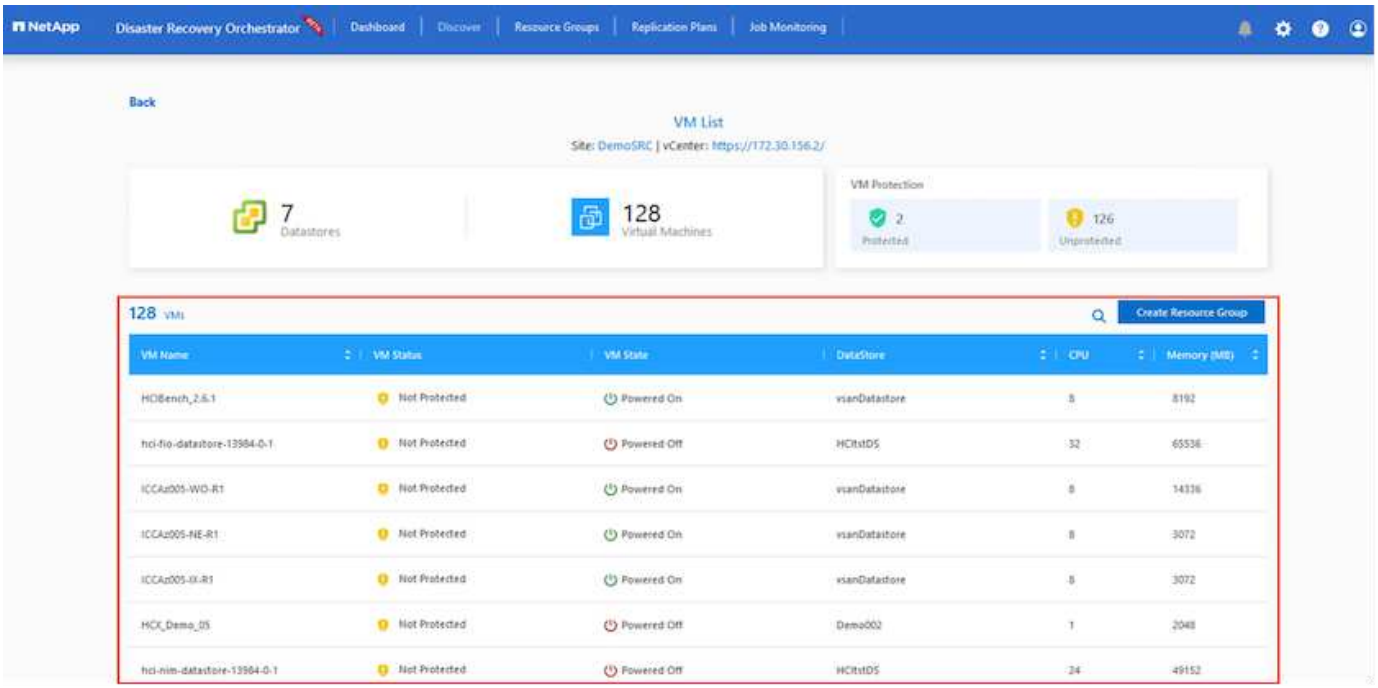
11. 更新 vCenter 详细信息。为此，请从主 AVS SDDC 的下拉列表中选择凭据、Azure 区域和资源组。
12. DRO 列出了该地区所有可用的 SDDC。从下拉菜单中选择指定的私有云 URL。
13. 输入 `cloudadmin@vsphere.local`用户凭证。可以从 Azure 门户访问。按照本文提到的步骤 "链接"。完成后，单击“继续”。



14. 通过选择 Azure 资源组和NetApp帐户来选择源存储详细信息 (ANF)。
15. 单击“创建站点”。



添加后，DRO 会执行自动发现并显示从源站点到目标站点具有相应跨区域副本的虚拟机。 DRO 自动检测虚拟机使用的网络和段并填充它们。



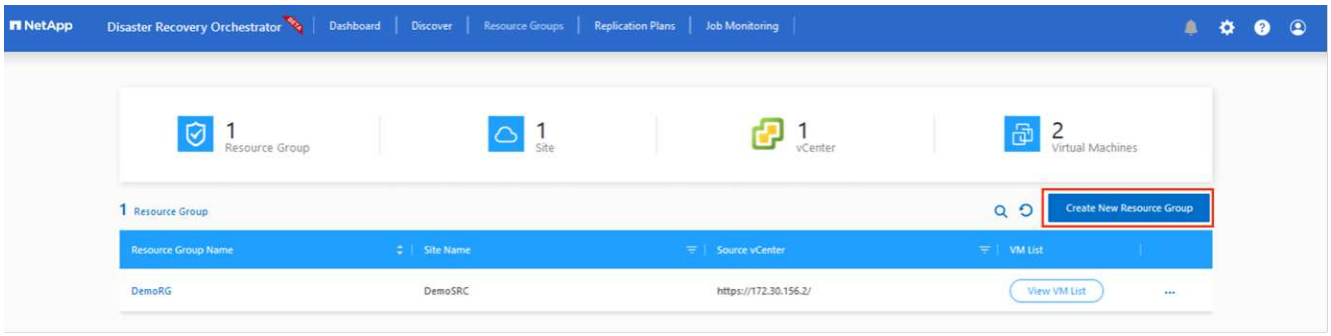
下一步是将所需的虚拟机分组到其功能组中作为资源组。

资源分组

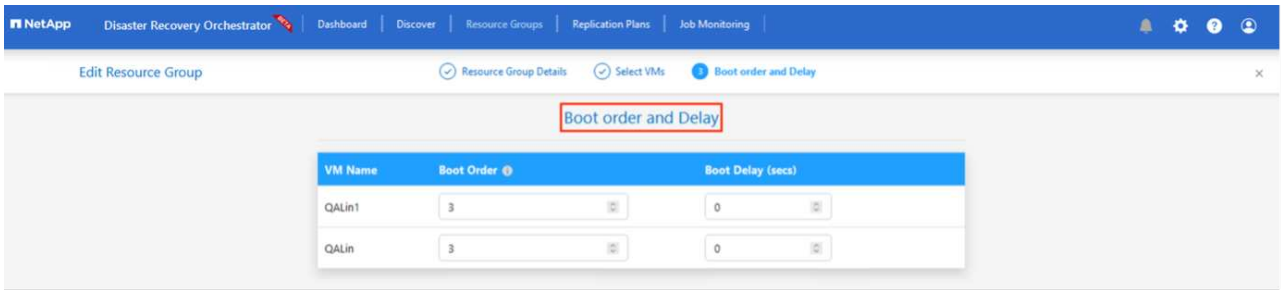
添加平台后，将要恢复的虚拟机分组到资源组中。 DRO 资源组允许您将一组从属虚拟机分组为逻辑组，这些逻辑组包含它们的启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

要开始创建资源组，请单击“创建新资源组”菜单项。

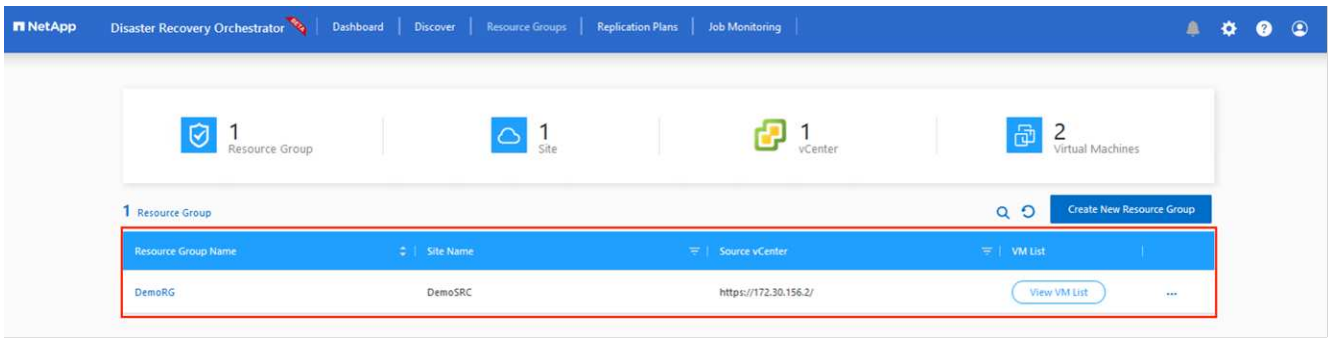
1. 访问“资源组”并单击“创建新资源组”。



2. 在新资源组下，从下拉菜单中选择源站点，然后单击*创建*。
3. 提供资源组详细信息，然后单击“继续”。
4. 使用搜索选项选择合适的虚拟机。
5. 为所有选定的虚拟机选择*启动顺序*和*启动延迟*（秒）。通过选择每个虚拟机并设置其优先级来设置开机顺序。所有虚拟机的默认值为 3。选项如下：
   - 第一个启动的虚拟机
   - 默认
   - 最后启动的虚拟机



6. 单击“创建资源组”。

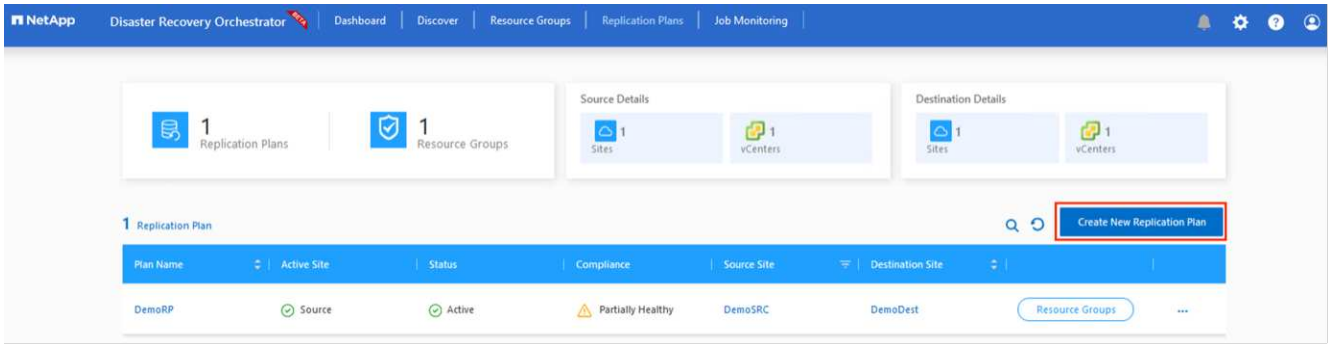


复制计划

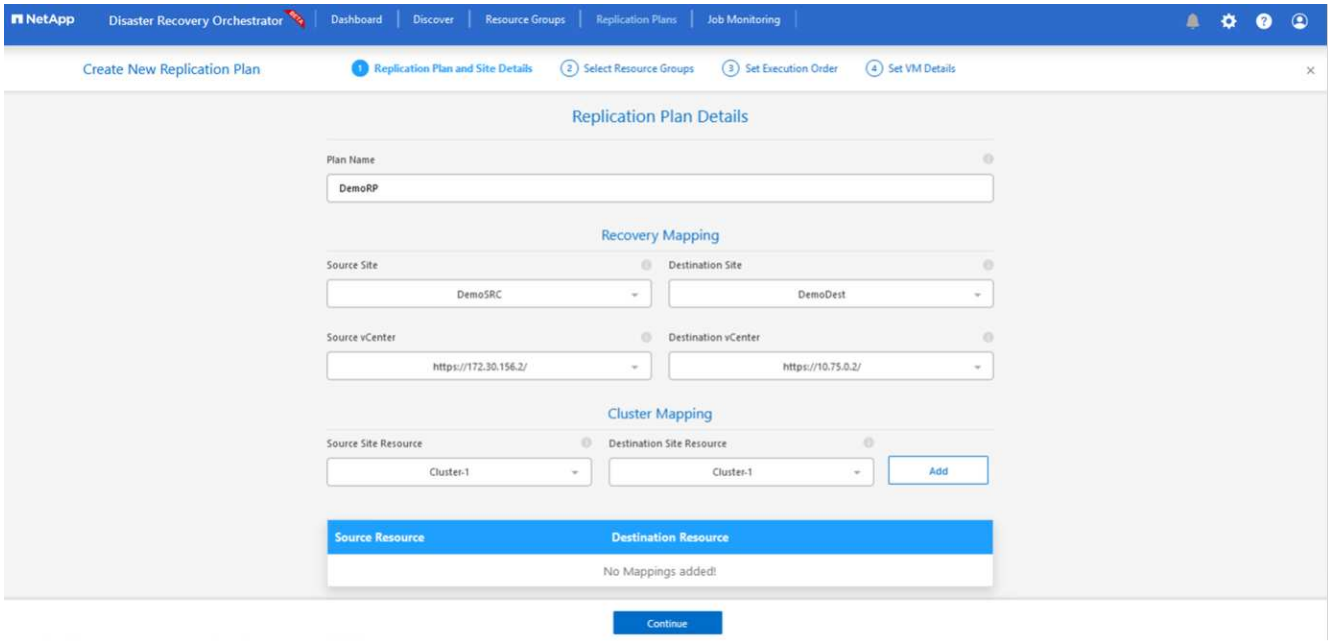
您必须制定一个在发生灾难时恢复应用程序的计划。从下拉菜单中选择源和目标 vCenter 平台，选择要包含在此计划中的资源组，还包括应用程序应如何恢复和启动的分组（例如，域控制器、第 1 层、第 2 层等）。计划通常也被称为蓝图。要定义恢复计划，请导航到“复制计划”选项卡，然后单击“新建复制计划”。

要开始创建复制计划，请完成以下步骤：

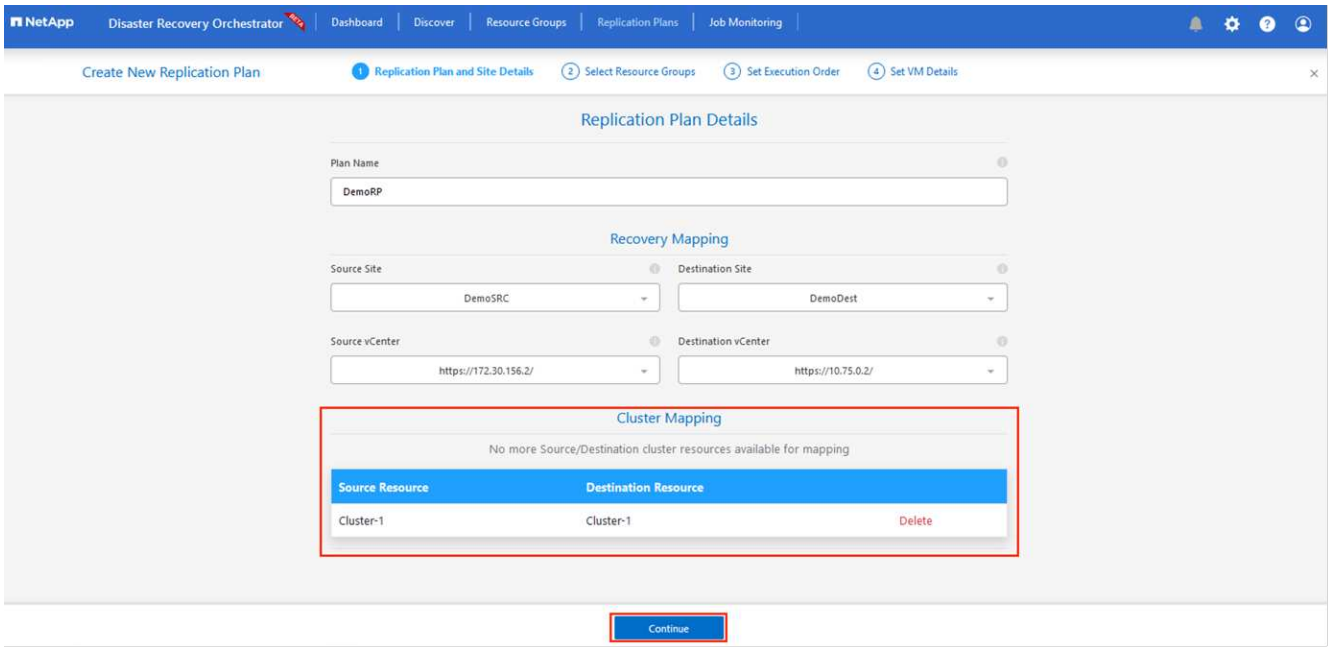
1. 导航到*复制计划*并单击*创建新复制计划*。



2. 在*新复制计划*上，提供计划名称并通过选择源站点、关联 vCenter、目标站点和关联 vCenter 来添加恢复映射。

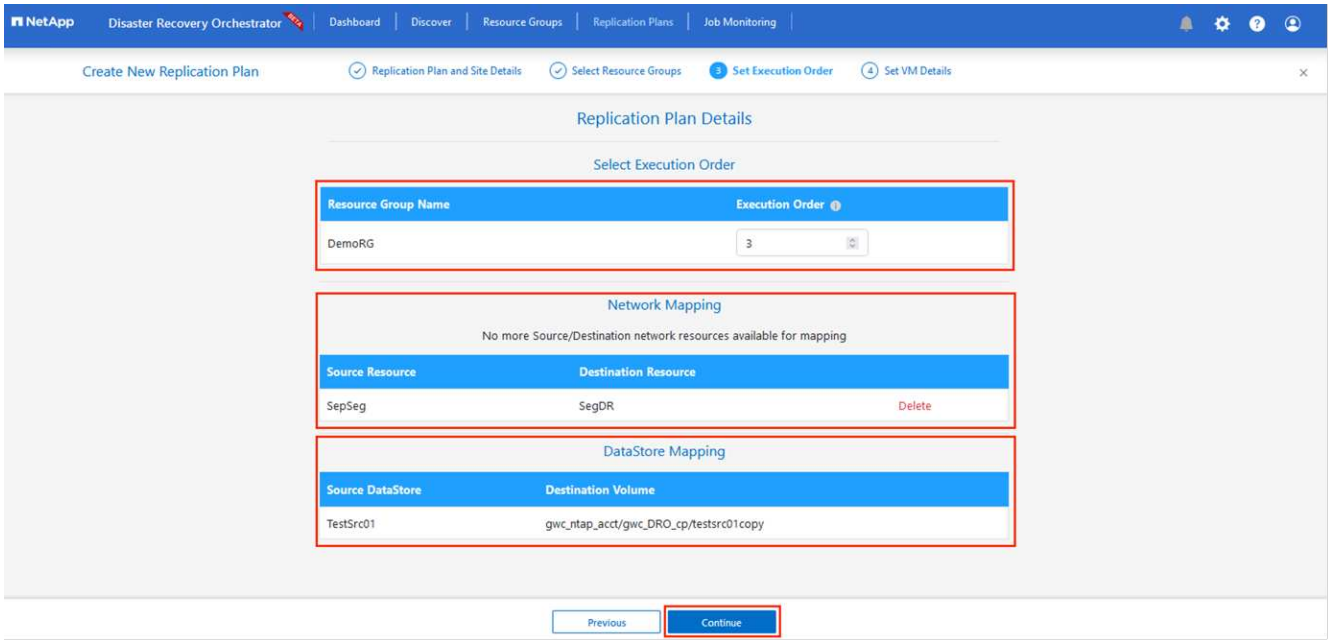


3. 恢复映射完成后，选择*集群映射*。



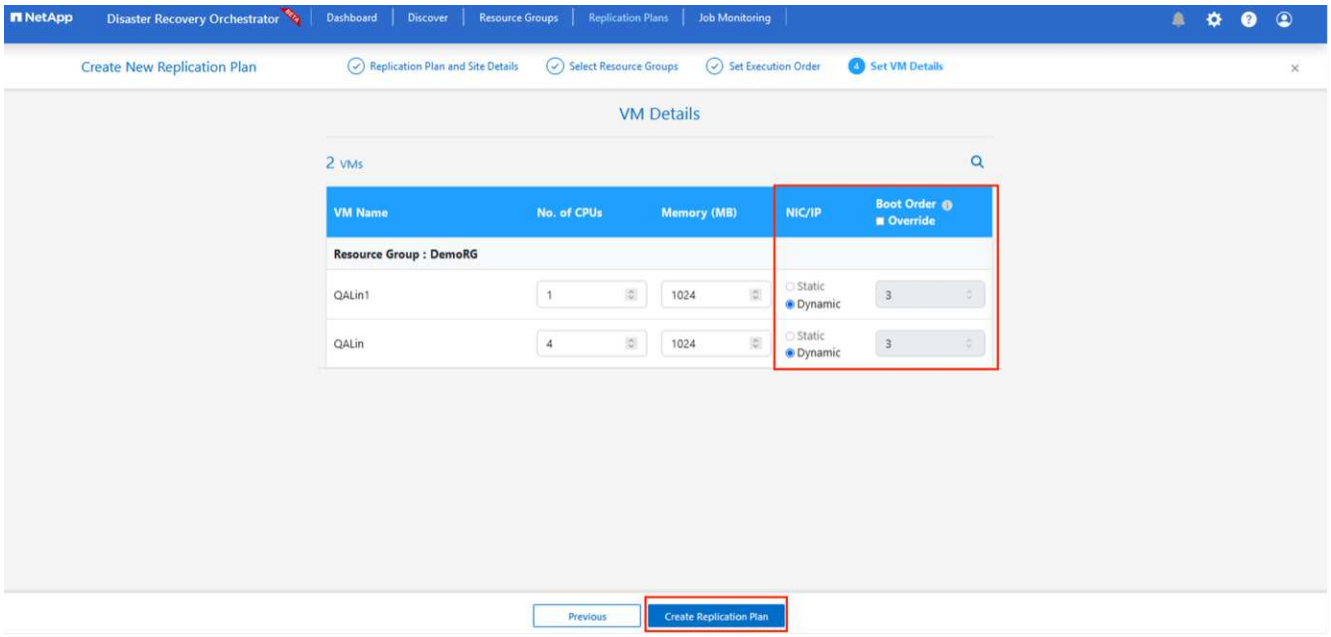
4. 选择*资源组详情*并点击*继续*。
5. 设置资源组的执行顺序。当存在多个资源组时，此选项可让您选择操作顺序。
6. 完成后，将网络映射设置到适当的段。这些段应该已经在辅助 AVS 集群上配置，并且要将虚拟机映射到这些段，请选择适当的段。
7. 根据虚拟机的选择自动选择数据存储映射。

跨区域复制（CRR）处于卷级别。因此，驻留在相应卷上的所有虚拟机都被复制到 CRR 目标。确保选择数据存储区中的所有虚拟机，因为只有复制计划中的虚拟机才会被处理。

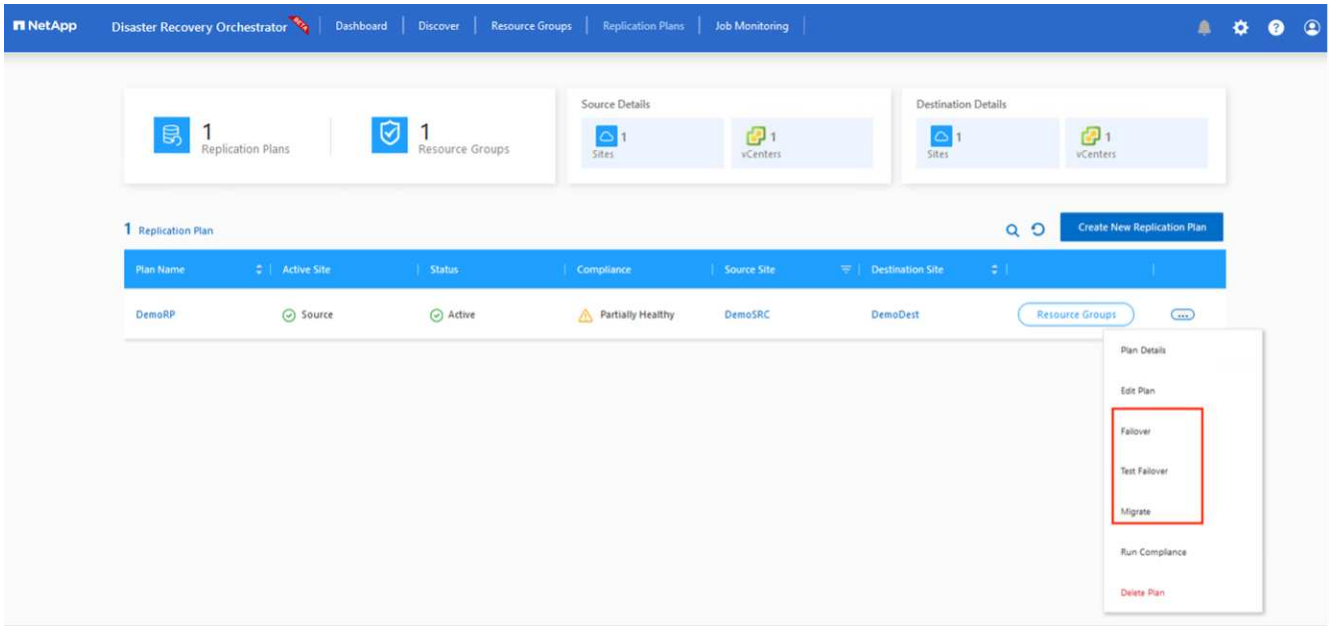


8. 在 VM 详细信息下，您可以选择调整 VM 的 CPU 和 RAM 参数。当您将大型环境恢复到较小的目标集群或进行 DR 测试而无需配置一对一的物理 VMware 基础架构时，这会非常有用。另外，修改资源组中所有选定虚拟机的启动顺序和启动延迟（秒）。如果需要对资源组启动顺序选择过程中选择的内容进行任何更改，则

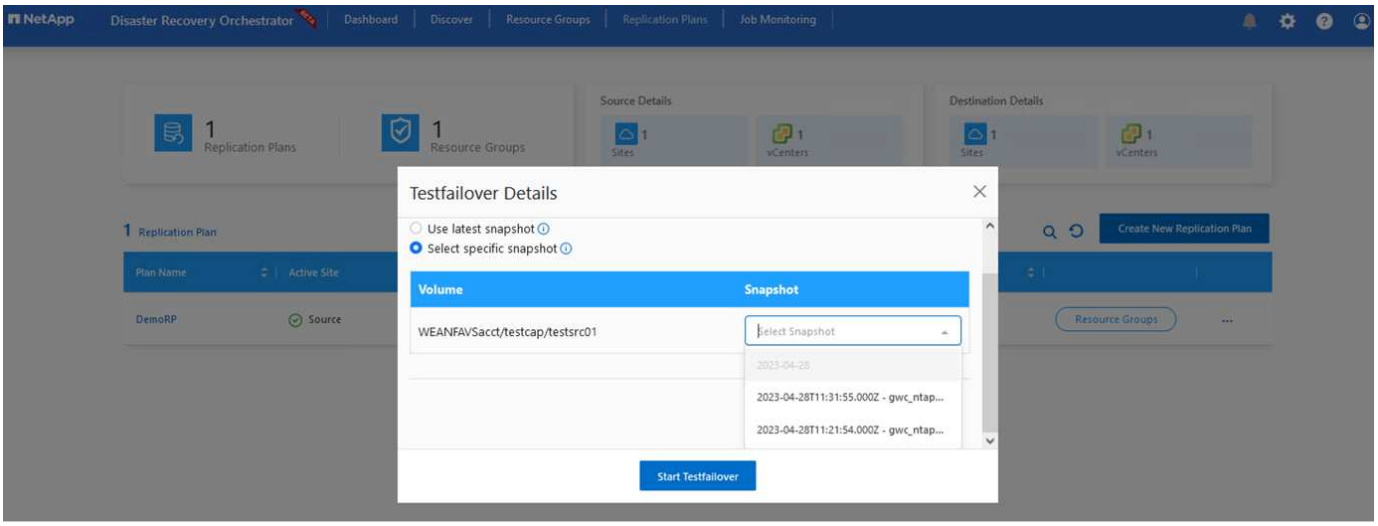
可以使用附加选项来修改启动顺序。默认情况下，使用资源组选择期间选择的启动顺序，但可以在此阶段执行任何修改。



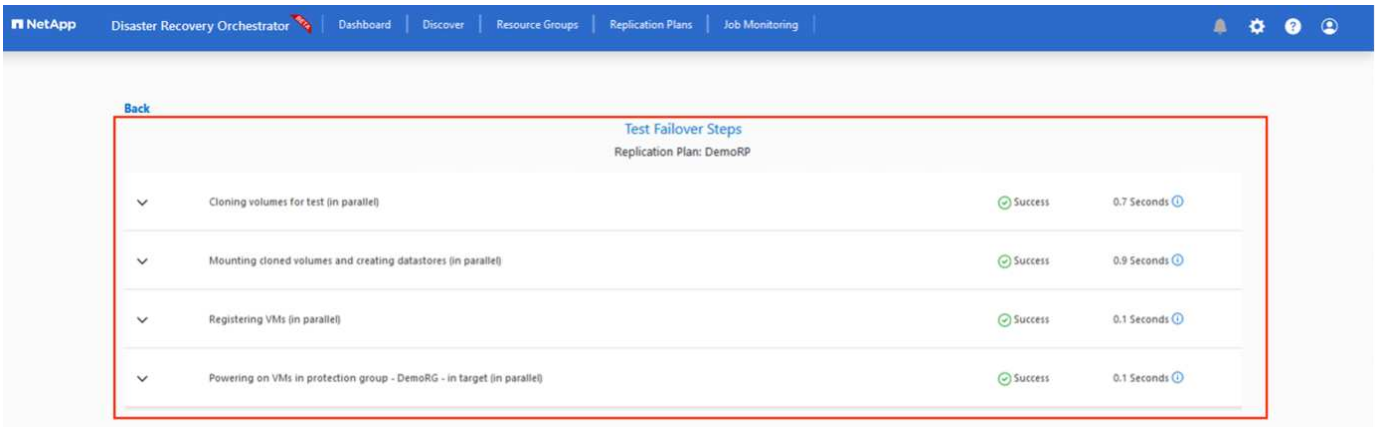
9. 单击*创建复制计划*。创建复制计划后，您可以根据需要执行故障转移、测试故障转移或迁移选项。



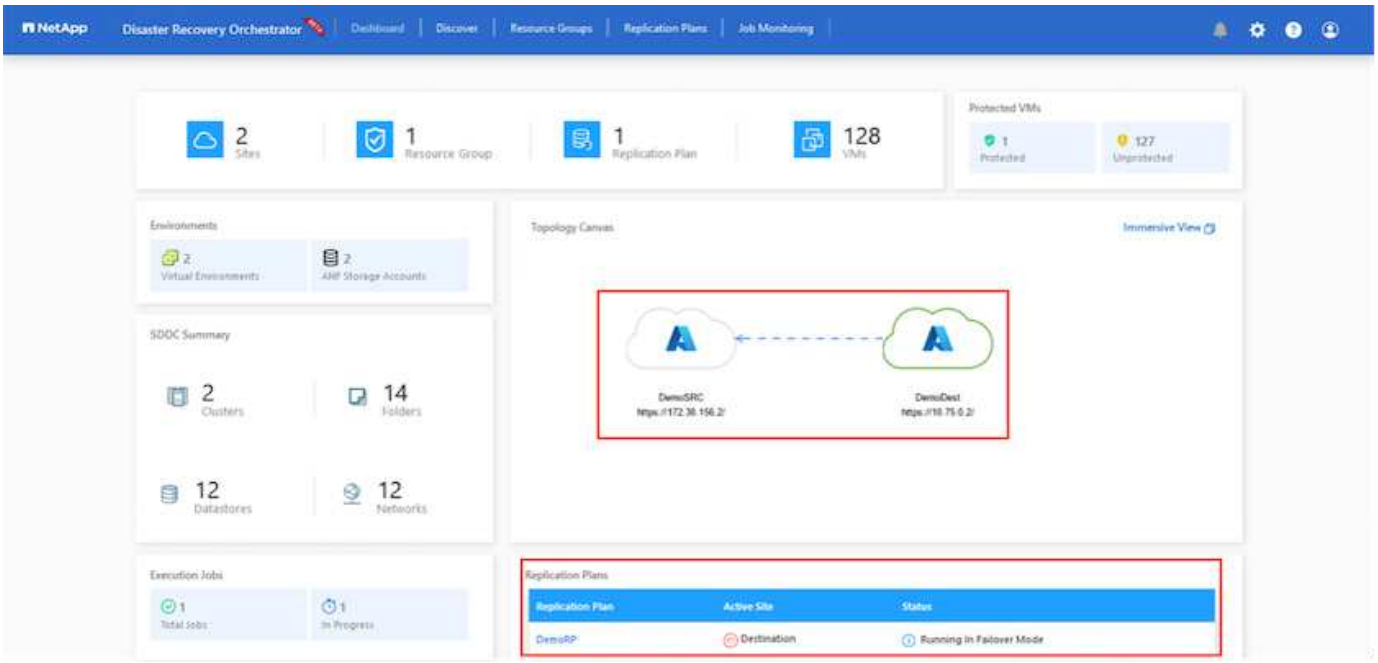
在故障转移和测试故障转移选项期间，使用最新的快照，或者可以从时间点快照中选择特定快照。如果您面临勒索软件之类的损坏事件，则时间点选项可能非常有用，其中最新的副本已被破坏或加密。 DRO 显示所有可用的时间点。



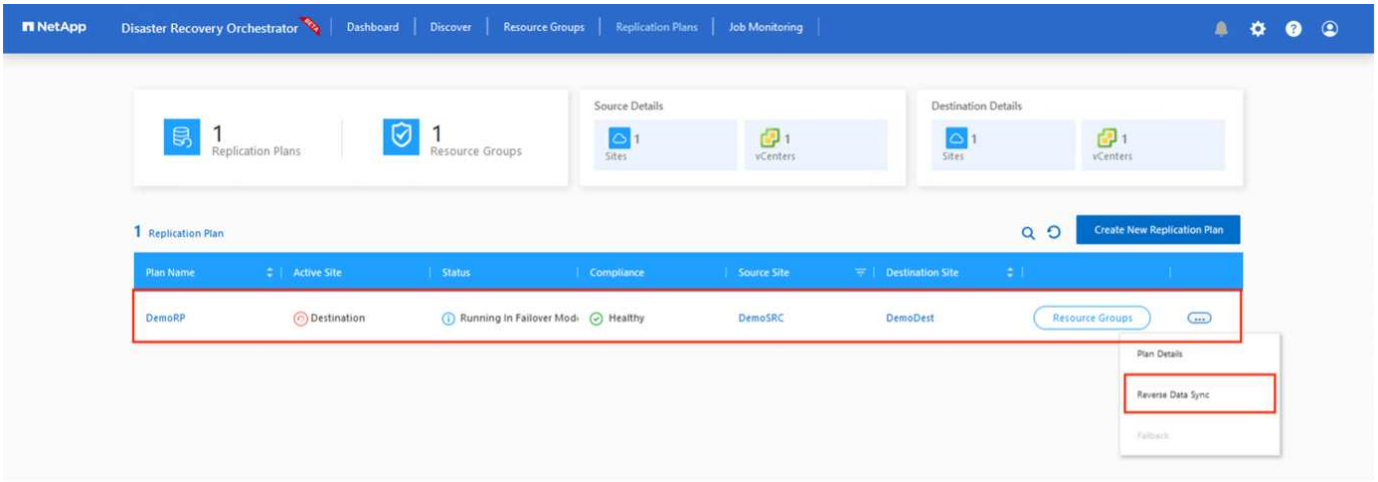
要使用复制计划中指定的配置触发故障转移或测试故障转移，您可以单击*故障转移*或*测试故障转移*。您可以在任务菜单中监控复制计划。



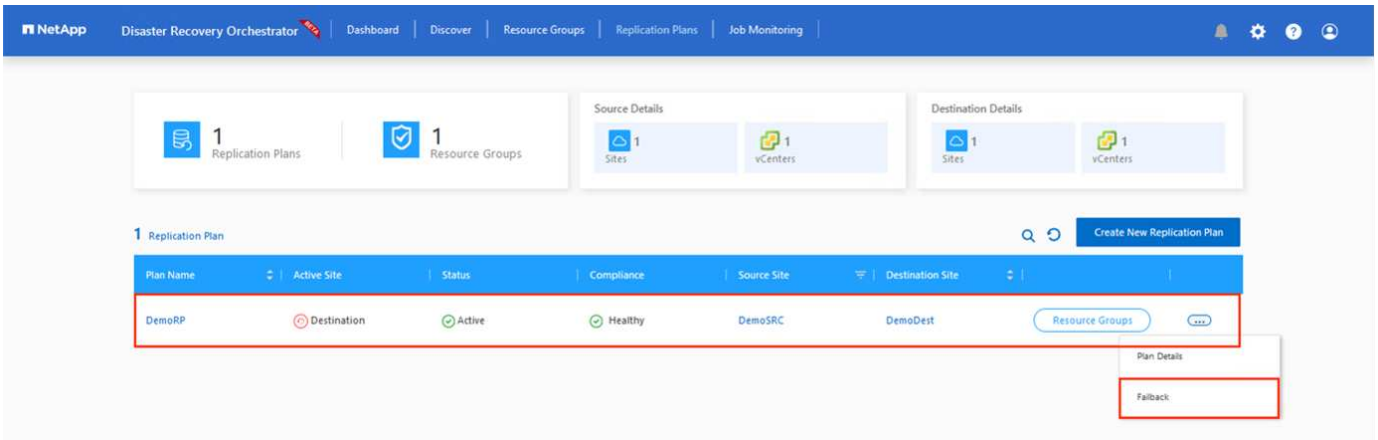
触发故障转移后，可以在辅助站点 AVS SDDC vCenter（虚拟机、网络和数据存储区）中看到恢复的项目。默认情况下，虚拟机将恢复到工作负载文件夹。

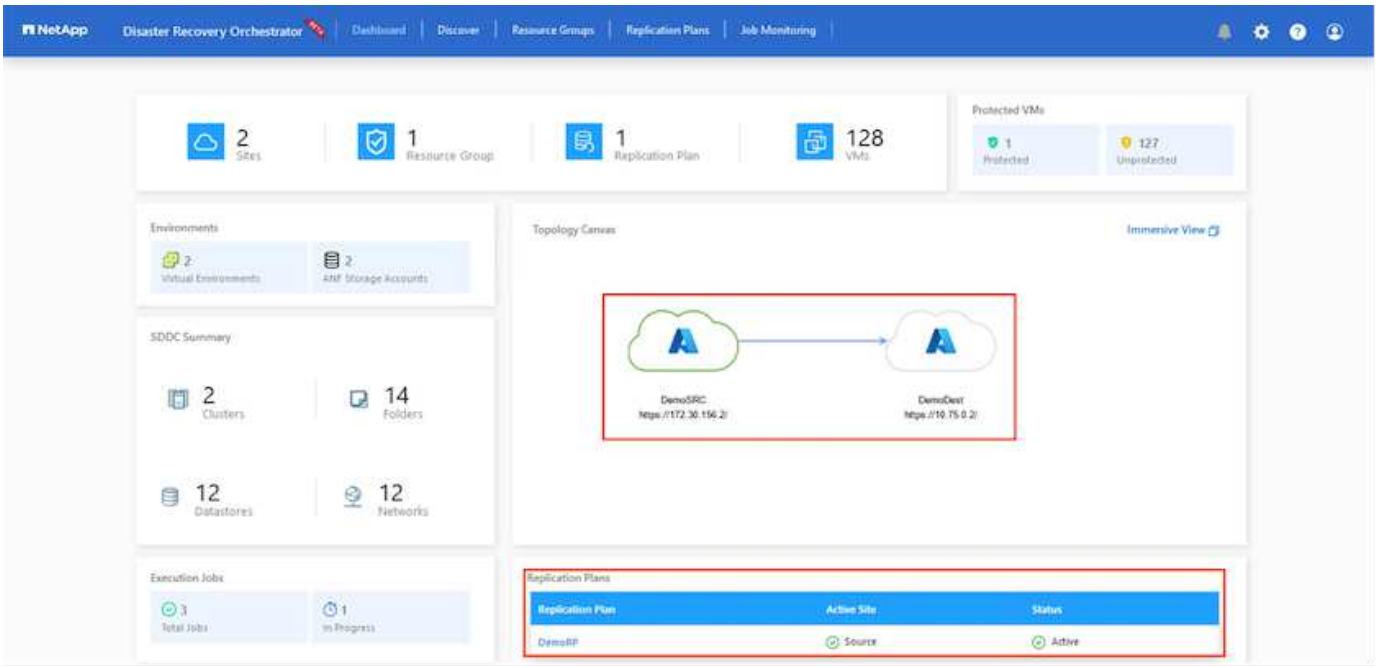


可以在复制计划级别触发故障恢复。如果发生测试故障转移，可以使用拆除选项来回滚更改并删除新创建的卷。与故障转移相关的故障回复是一个两步过程。选择复制计划并选择*反向数据同步*。



此步骤完成后，触发故障恢复以移回主 AVS 站点。





从 Azure 门户中，我们可以看到，对于作为读/写卷映射到辅助站点 AVS SDDC 的相应卷，复制运行状况已中断。在测试故障转移期间，DRO 不会映射目标卷或副本卷。相反，它会创建所需的跨区域复制快照的新卷，并将该卷公开为数据存储，这会消耗容量池中的额外物理容量并确保源卷不会被修改。值得注意的是，复制作业可以在 DR 测试或分类工作流程期间继续进行。此外，此过程可确保在发生错误或恢复损坏的数据时可以清理恢复，而不会有副本被破坏的风险。

勒索软件恢复

从勒索软件中恢复可能是一项艰巨的任务。具体来说，IT 组织很难确定安全的返回点，而且，一旦确定，如何确保恢复的工作负载免受再次发生的攻击（例如，来自休眠恶意软件或通过易受攻击的应用程序）。

DRO 通过允许组织从任何可用的时间点恢复来解决这些问题。然后将工作负载恢复到功能齐全但隔离的网络中，以便应用程序可以运行并相互通信，但不会暴露于任何南北流量。此过程为安全团队提供了一个安全的地方来进行取证并识别任何隐藏或休眠的恶意软件。

结束语

Azure NetApp Files和 Azure VMware 灾难恢复解决方案为您提供以下优势：

- 利用高效且有弹性的Azure NetApp Files跨区域复制。
- 通过快照保留恢复到任何可用的时间点。
- 完全自动化所有必需步骤，从存储、计算、网络和应用程序验证步骤中恢复数百到数千台虚拟机。
- 工作负载恢复利用“从最新的快照创建新卷”过程，该过程不会操作复制的卷。
- 避免卷或快照上的任何数据损坏风险。
- 避免 DR 测试工作流程期间的复制中断。
- 利用 DR 数据和云计算资源进行 DR 以外的工作流程，例如开发/测试、安全测试、补丁和升级测试以及补救测试。
- CPU 和 RAM 优化可以通过允许恢复到较小的计算集群来帮助降低云成本。

在哪里可以找到更多信息

要了解有关本文档中描述的信息的更多信息，请查看以下文档和/或网站：

- 为Azure NetApp Files创建卷复制

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Azure NetApp Files卷的跨区域复制

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Azure VMware 解决方案"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- 在 Azure 上部署和配置虚拟化环境

  "在 Azure 上设置 AVS"

- 部署和配置 Azure VMware 解决方案

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

使用 **Veeam Replication** 和**Azure NetApp Files**数据存储区对 **Azure VMware** 解决方案进行灾难恢复

Azure NetApp Files (ANF) 数据存储将存储与计算分离，并释放了任何组织将其工作负载转移到云端所需的灵活性。它为客户提供灵活、高性能的存储基础设施，可独立于计算资源进行扩展。 Azure NetApp Files数据存储简化并优化了与 Azure VMware 解决方案 (AVS) 一起的部署，作为本地 VMWare 环境的灾难恢复站点。

概述

基于Azure NetApp Files(ANF) 卷的 NFS 数据存储可用于使用任何经过验证的提供 VM 复制功能的第三方解决方案从本地复制数据。通过添加Azure NetApp Files数据存储，它将实现成本优化部署，而不是构建具有大量 ESXi 主机来容纳存储的 Azure VMware 解决方案 SDDC。这种方法被称为“Pilot Light Cluster”。试点灯集群是最小 AVS 主机配置（3 x AVS 节点）以及Azure NetApp Files数据存储容量。

目标是维护一个拥有所有核心组件的低成本基础设施来处理故障转移。如果发生故障转移，指示灯集群可以扩展并提供更多的 AVS 主机。一旦故障转移完成并且恢复正常操作，指示灯集群就可以缩减到低成本的运行模式。

本文件的目的

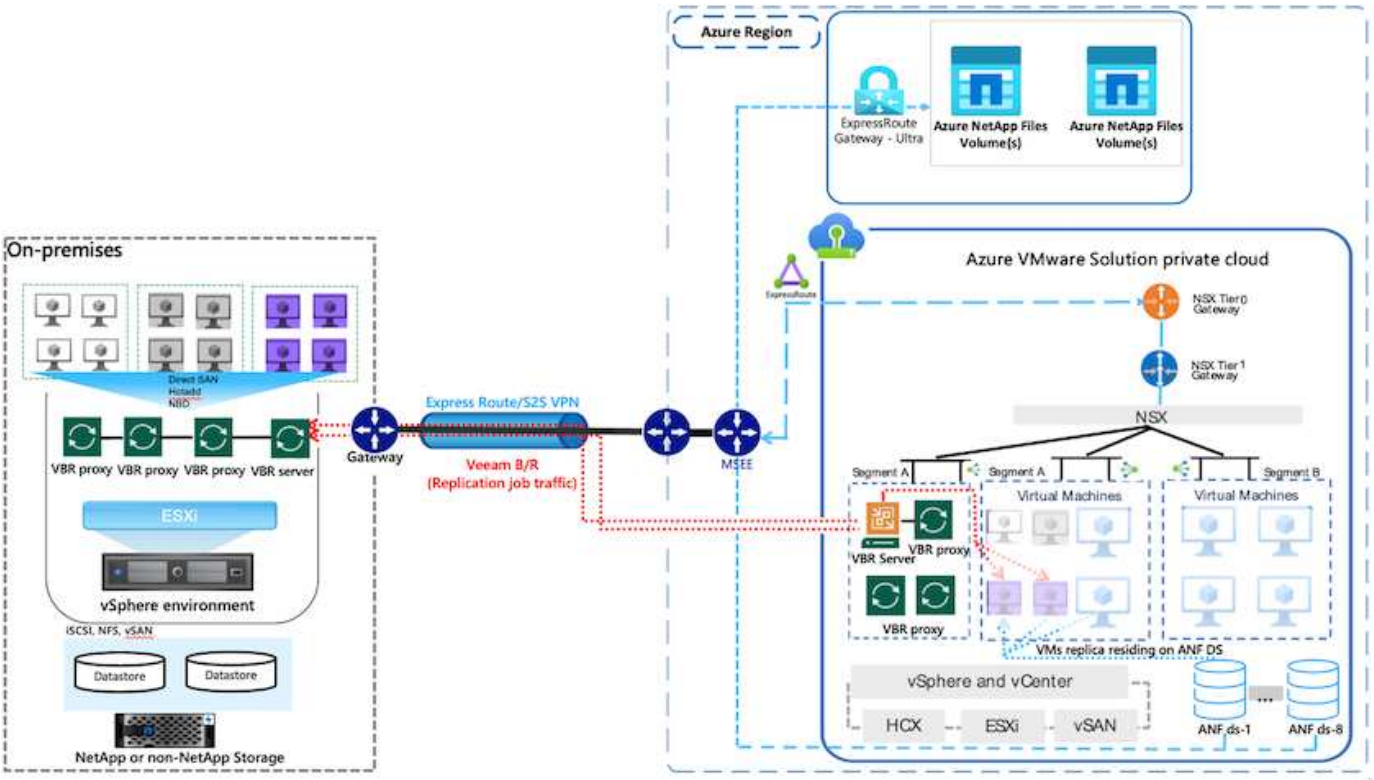
本文介绍如何将Azure NetApp Files数据存储与 Veeam Backup 和复制结合使用，以使用 Veeam VM 复制软件功能为本地 VMware VM 到 (AVS) 设置灾难恢复。

Veeam Backup & Replication 是一款用于虚拟环境的备份和复制应用程序。当虚拟机被复制时，Veeam Backup & Replication 会从 AVS 上复制，该软件将在目标 AVS SDDC 集群上以原生 VMware vSphere 格式创建虚拟机的精确副本。 Veeam Backup & Replication 将使副本与原始 VM 保持同步。复制提供了最佳的恢复时间目标 (RTO)，因为 DR 站点上有一个处于准备启动状态的 VM 的安装副本。

这种复制机制可确保在发生灾难事件时工作负载能够在 AVS SDDC 中快速启动。 Veeam Backup & Replication

软件还优化了通过 WAN 和慢速连接进行复制的流量传输。此外，它还过滤掉重复的数据块、零数据块、交换文件和“排除的 VM 客户操作系统文件”。该软件还将压缩副本流量。为了防止复制作业消耗整个网络带宽，可以利用 WAN 加速器和网络限制规则。

Veeam Backup & Replication 中的复制过程由作业驱动，这意味着复制是通过配置复制作业来执行的。如果发生灾难事件，可以触发故障转移，通过故障转移到其副本来恢复虚拟机。当执行故障转移时，复制的虚拟机将接管原始虚拟机的角色。可以执行故障转移至副本的最新状态或任何已知的良好还原点。这使得勒索软件恢复或隔离测试能够根据需要进行。 Veeam Backup & Replication 提供多种选项来处理不同的灾难恢复场景。



解决方案部署

高级步骤

1. Veeam Backup and Replication 软件在具有适当网络连接的本地环境中运行。
2. "部署 Azure VMware 解决方案 (AVS)"私有云和"附加Azure NetApp Files数据存储"到 Azure VMware 解决方案主机。

   可以使用以最小配置设置的指示灯环境来实现 DR 目的。一旦发生事故，虚拟机将故障转移到该集群，并且可以添加其他节点）。

3. 设置复制作业以使用 Veeam Backup and Replication 创建 VM 副本。
4. 创建故障转移计划并执行故障转移。
5. 灾难事件结束且主站点启动后，切换回生产虚拟机。

Veeam VM 复制到 **AVS** 和 **ANF** 数据存储区的先决条件

1. 确保 Veeam Backup & Replication 备份 VM 连接到源以及目标 AVS SDDC 集群。

2. 备份服务器必须能够解析短名称并连接到源 vCenter 和目标 vCenter。
3. 目标Azure NetApp Files数据存储必须具有足够的可用空间来存储复制的 VM 的 VMDK。

有关更多信息，请参阅“注意事项和限制”"此处" 。

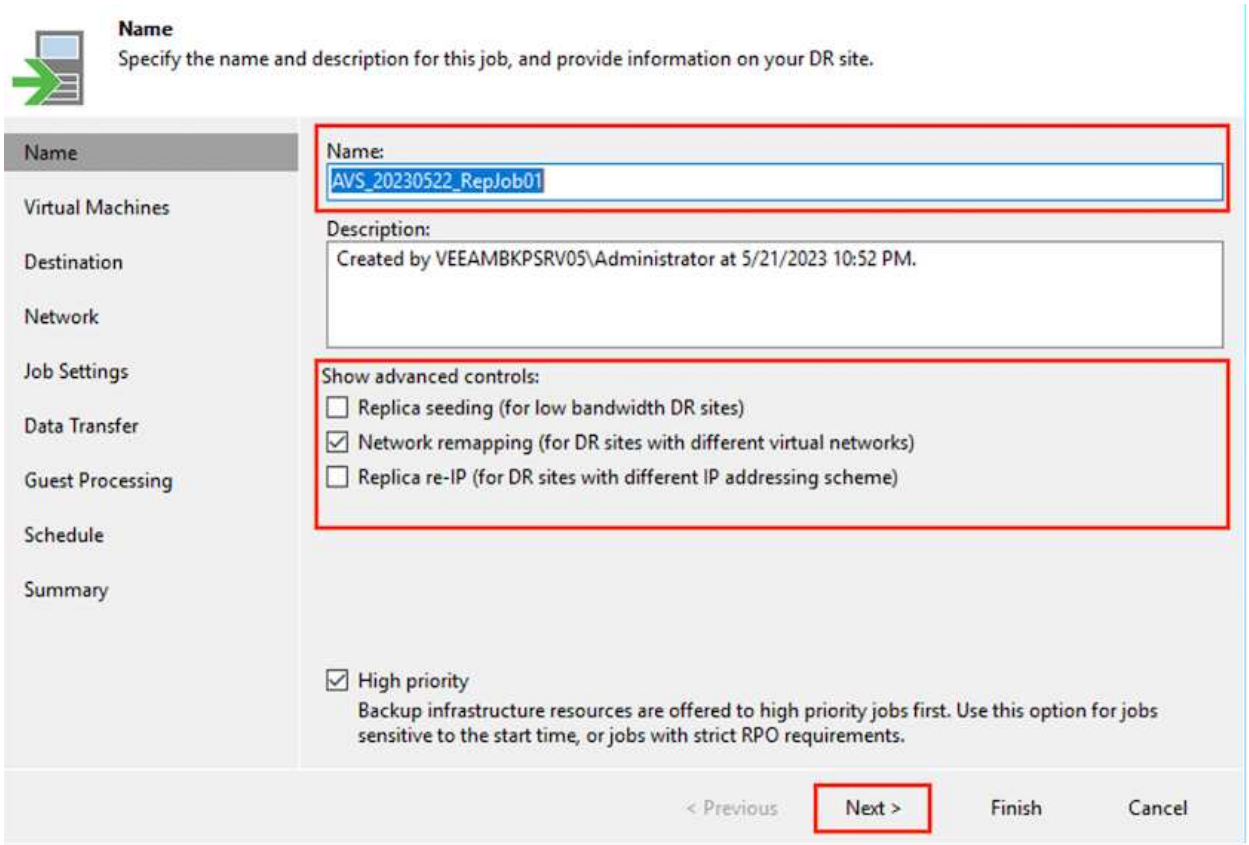
部署详情

▼ 步骤 1：复制虚拟机

Veeam Backup & Replication 利用 VMware vSphere 快照功能/在复制期间，Veeam Backup & Replication 请求 VMware vSphere 创建 VM 快照。 VM 快照是 VM 的时间点副本，其中包括虚拟磁盘、系统状态、配置和元数据。 Veeam Backup & Replication 使用快照作为复制的数据源。

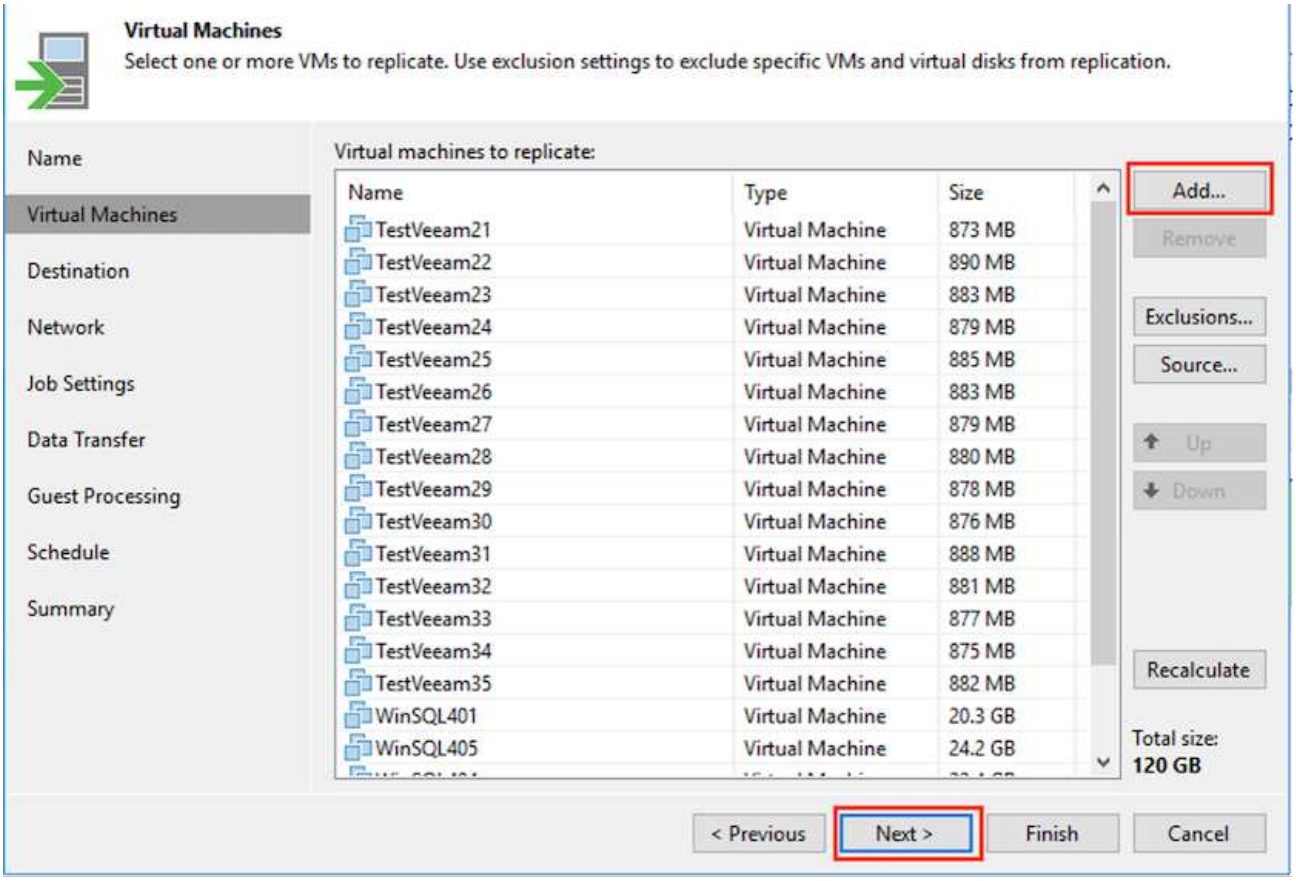
要复制虚拟机，请按照以下步骤操作：

1. 打开 Veeam 备份和复制控制台。
2. 在主页视图上。右键单击作业节点并选择复制作业>虚拟机。
3. 指定作业名称并选择适当的高级控制复选框。单击“下一步”。
   - 如果本地和 Azure 之间的连接带宽受限，请选中“副本种子”复选框。 *如果 Azure VMware 解决方案 SDDC 上的段与本地站点网络的段不匹配，请选中“网络重新映射（针对具有不同网络的 AVS SDDC 站点）”复选框。
   - 如果本地生产站点中的 IP 寻址方案与目标 AVS 站点中的方案不同，请选中“副本重新 IP（适用于具有不同 IP 寻址方案的 DR 站点）”复选框。

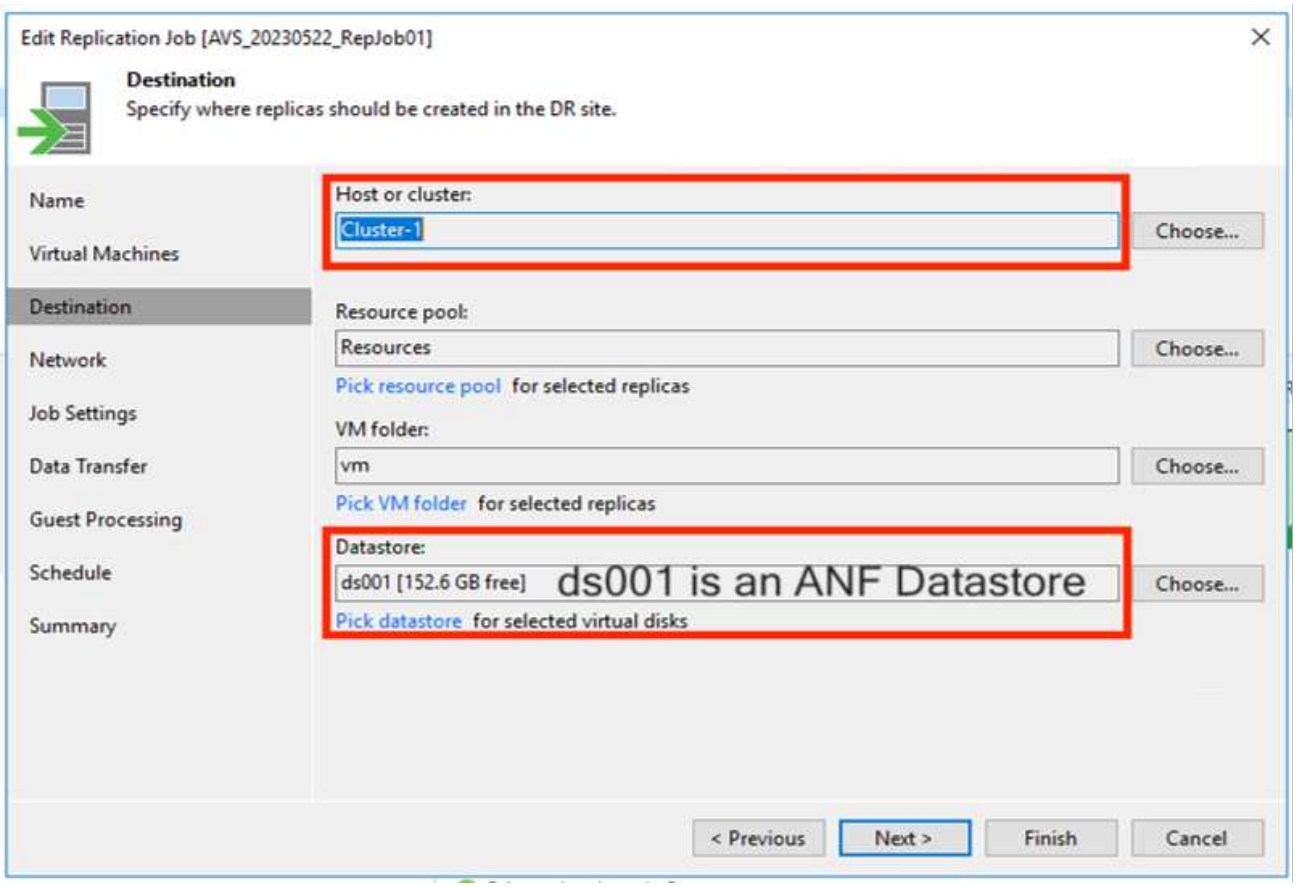


4. 在“虚拟”计算机*步骤中选择要复制到附加到 **Azure VMware** 解决方案 **SDDC**的 **Azure NetApp Files**数据存储的 **VM**。可以将虚拟机放置在 **vSAN** 上以填充可用的 **vSAN** 数据存储容量。在试点集群中，**3** 节点集

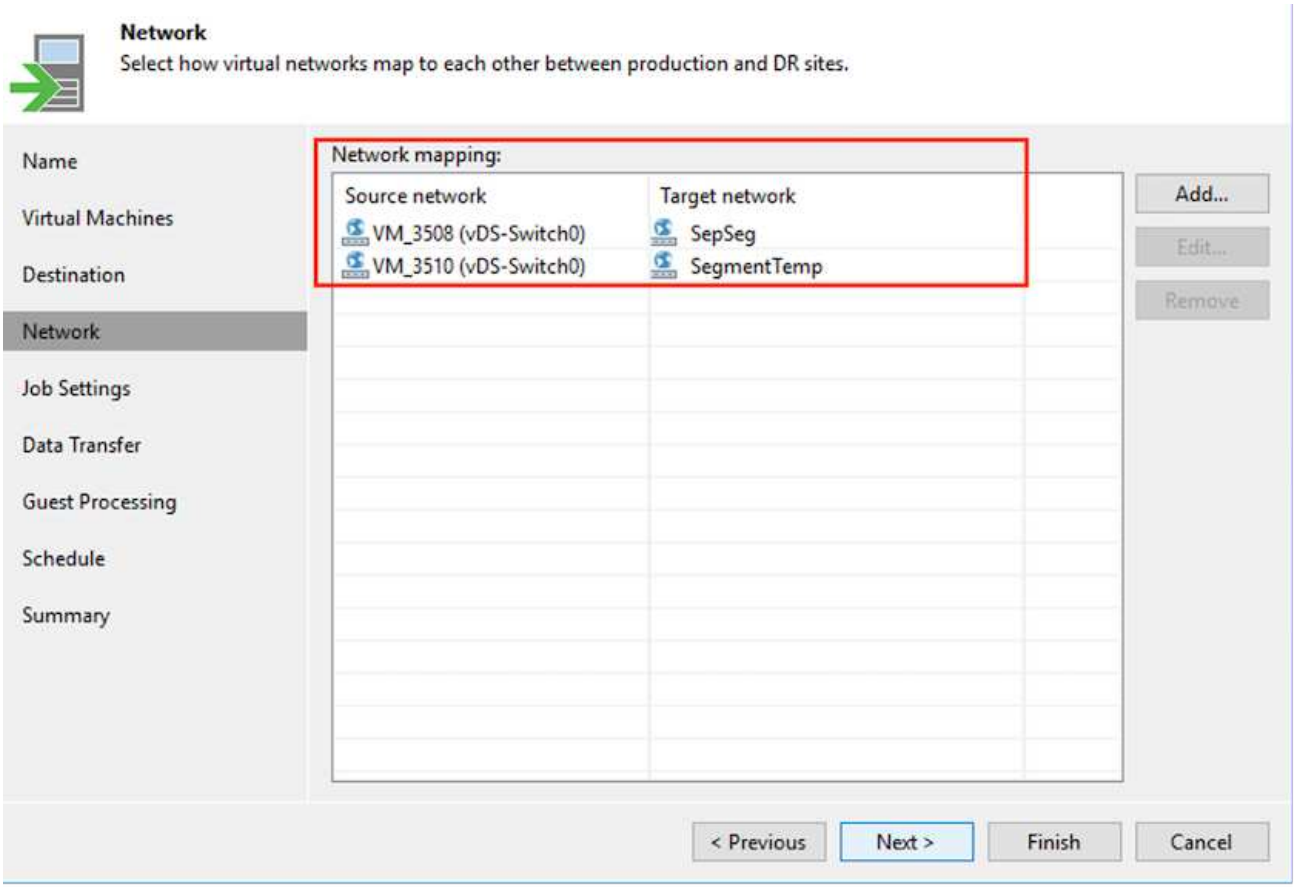
群的可用容量将受到限制。其余数据可以轻松放置在**Azure NetApp Files**数据存储中，以便可以恢复虚拟机，并且扩展集群以满足 **CPU**/内存要求。单击*添加，然后在*添加对象*窗口中选择必要的虚拟机或虚拟机容器，然后单击*添加*。单击“下一步”。



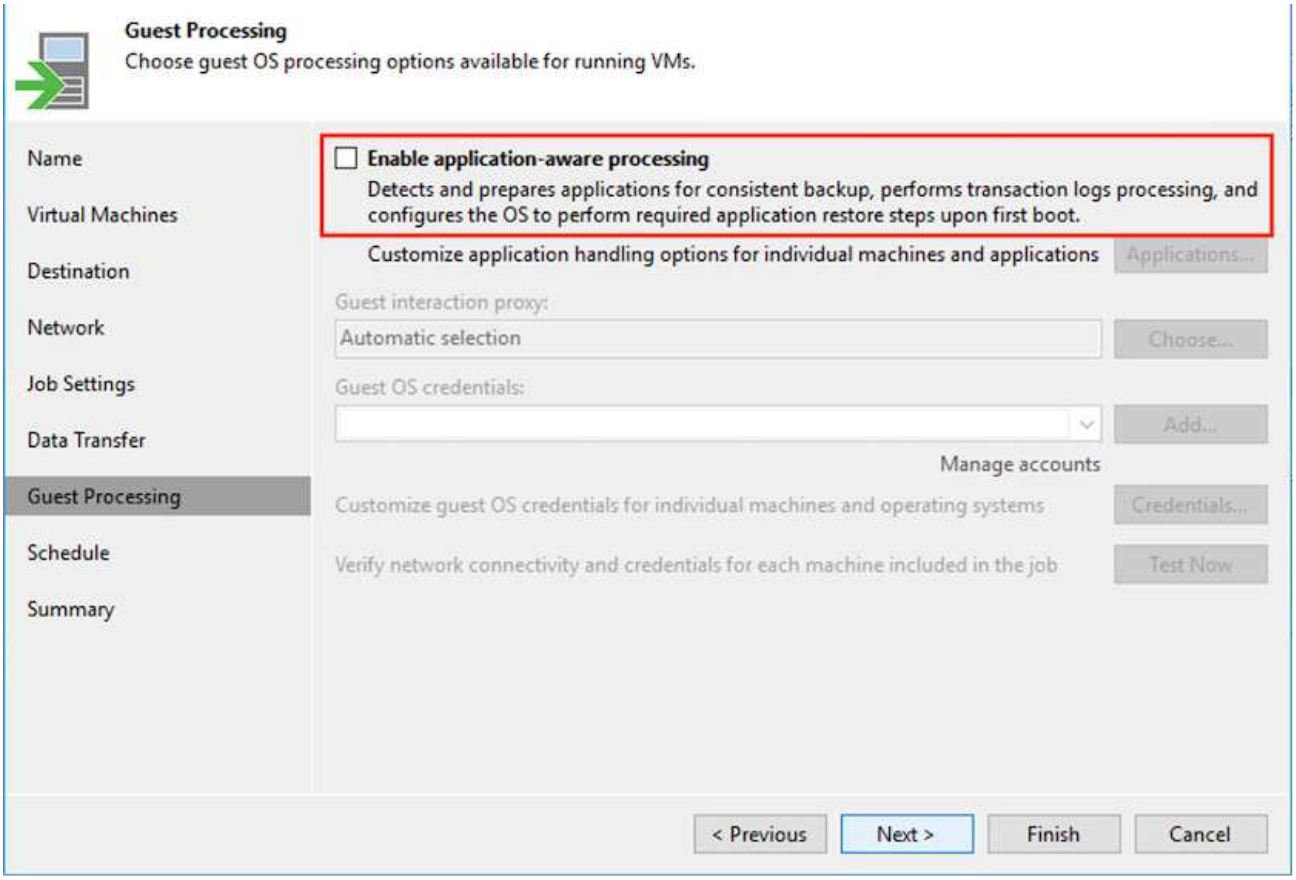
5. 之后，选择目标作为 Azure VMware 解决方案 SDDC 群集/主机，并选择适当的资源池、VM 文件夹和 VM 副本的 FSx ONTAP数据存储。然后单击“下一步”。



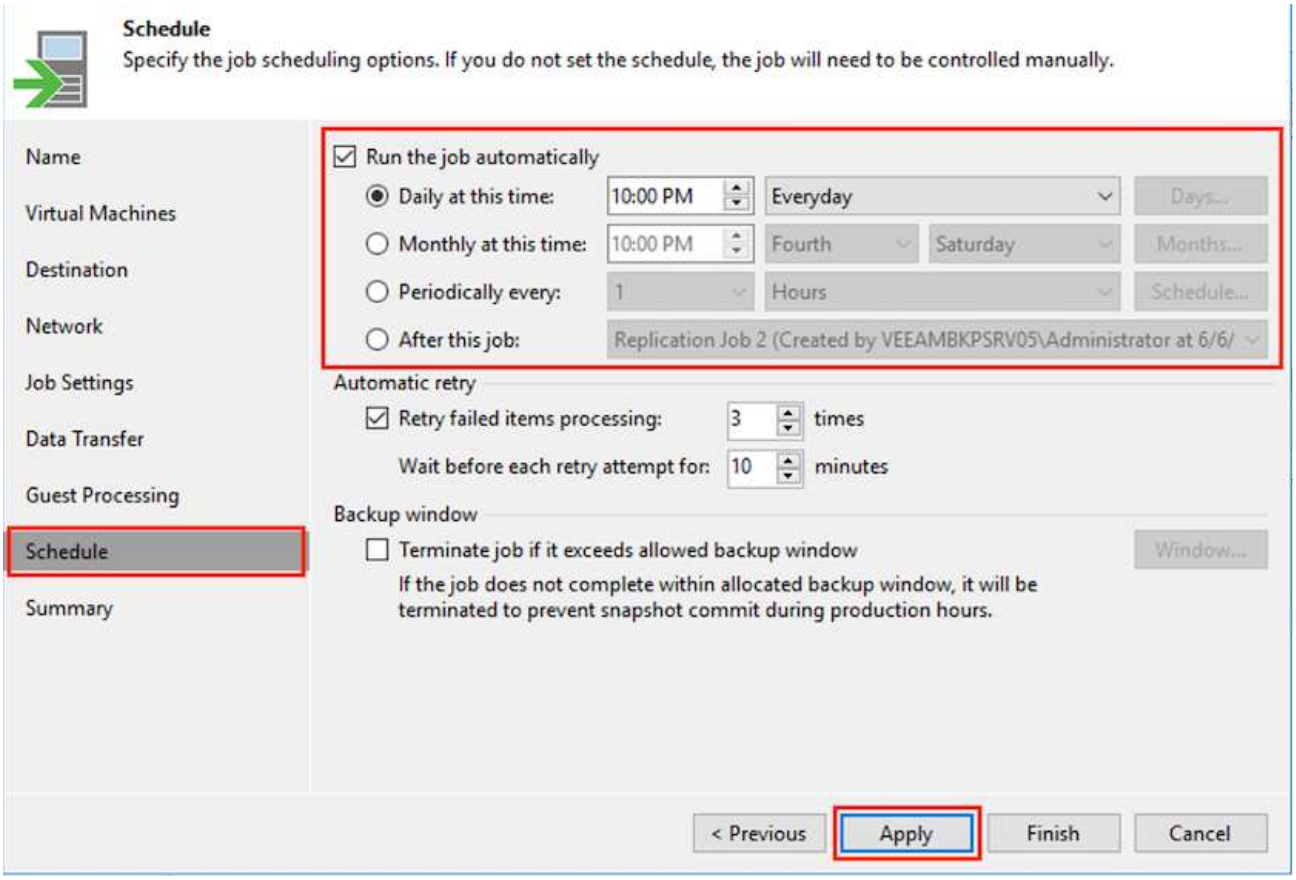
6. 下一步根据需要创建源虚拟网络和目标虚拟网络之间的映射。



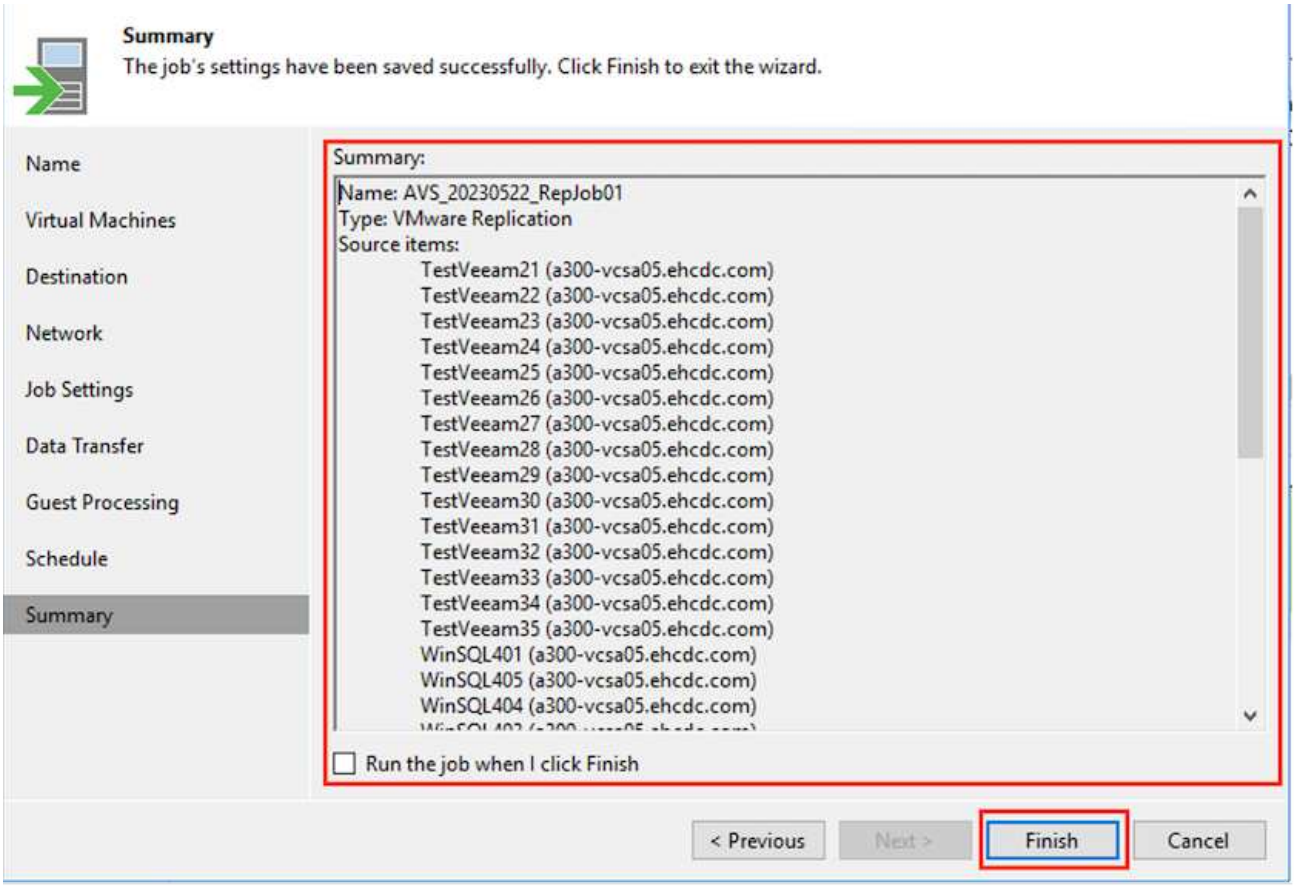
7. 在*作业设置*步骤中，指定将存储 VM 副本、保留策略等元数据的备份存储库。
8. 在*数据传输*步骤中更新*源*和*目标*代理服务器，保留*自动*选择（默认）并保持选择*直接*选项，然后单击*下一步*。
9. 在*Guest Processing*步骤中，根据需要选择*Enable application-aware processing*选项。单击“下一步”。



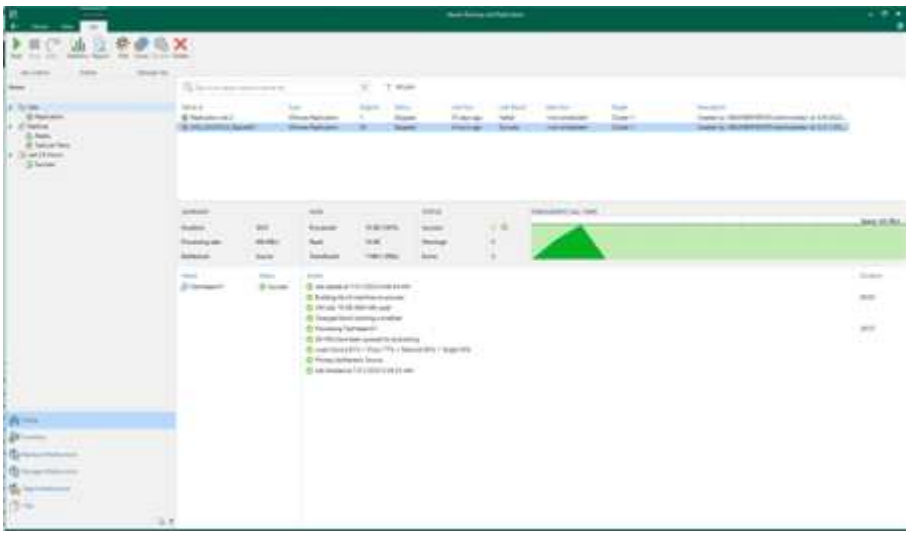
10. 选择复制计划来定期运行复制作业。



11. 在向导的*摘要*步骤中，查看复制作业的详细信息。要在向导关闭后立即启动作业，请选中*单击“完成”时运行作业*复选框，否则请不要选中该复选框。然后单击“完成”关闭向导。



复制作业启动后，具有指定后缀的虚拟机将填充到目标 AVS SDDC 集群/主机上。



有关 Veeam 复制的更多信息，请参阅"复制的工作原理"

▼ 步骤 2：创建故障转移计划

初始复制或播种完成后，创建故障转移计划。故障转移计划有助于自动对从属虚拟机逐个或按组执行故障转移。故障转移计划是虚拟机处理顺序（包括启动延迟）的蓝图。故障转移计划还有助于确保关键依赖的虚拟机已经在运行。

要创建计划，请导航到名为“副本”的新子部分并选择“故障转移计划”。选择适当的虚拟机。 Veeam Backup & Replication 将查找最接近此时间点的还原点并使用它们启动 VM 副本。

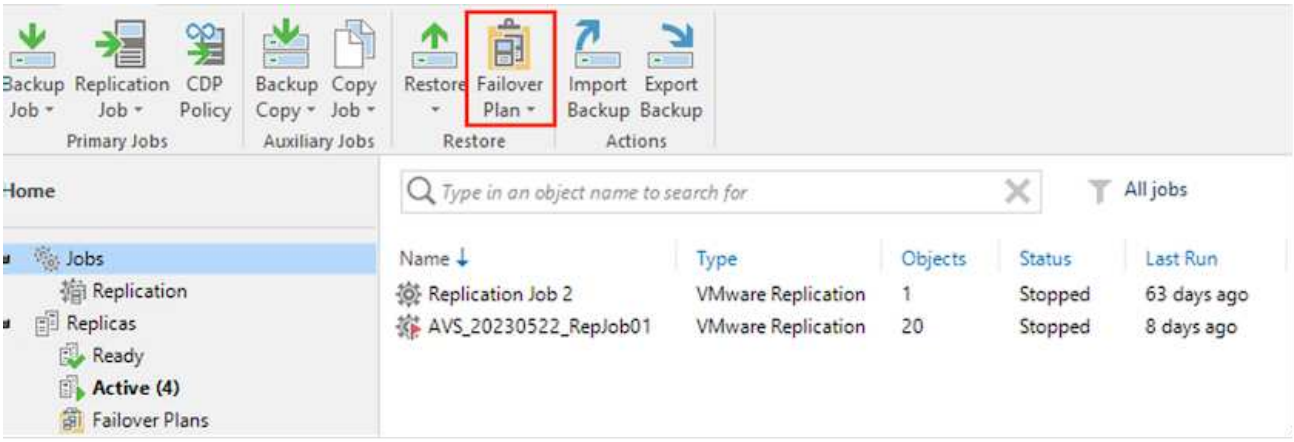
仅当初始复制完成且 VM 副本处于就绪状态后，才能添加故障转移计划。

运行故障转移计划时可同时启动的虚拟机数量上限为 10

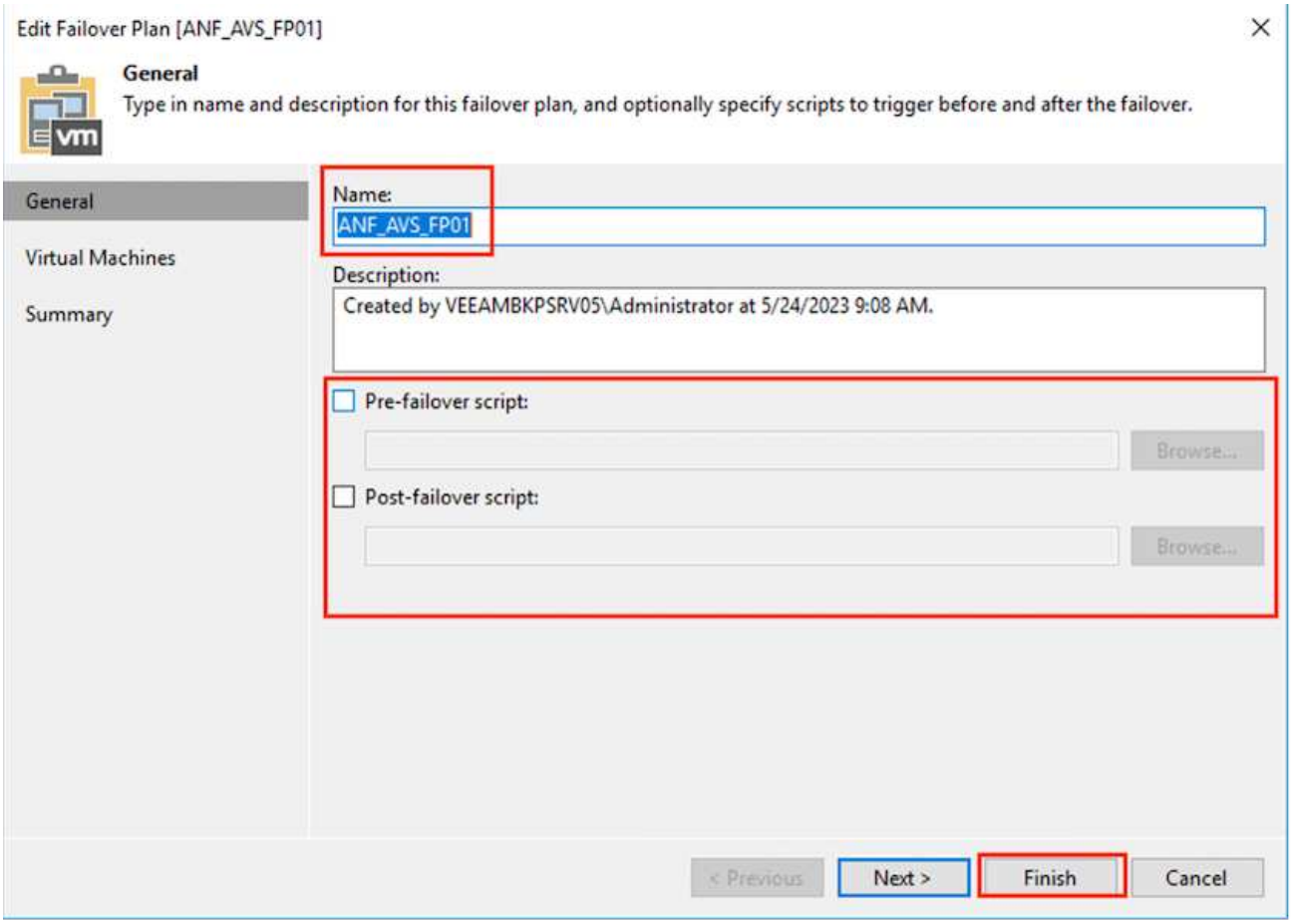
在故障转移过程中，源虚拟机不会关闭

要创建*故障转移计划*，请执行以下操作：

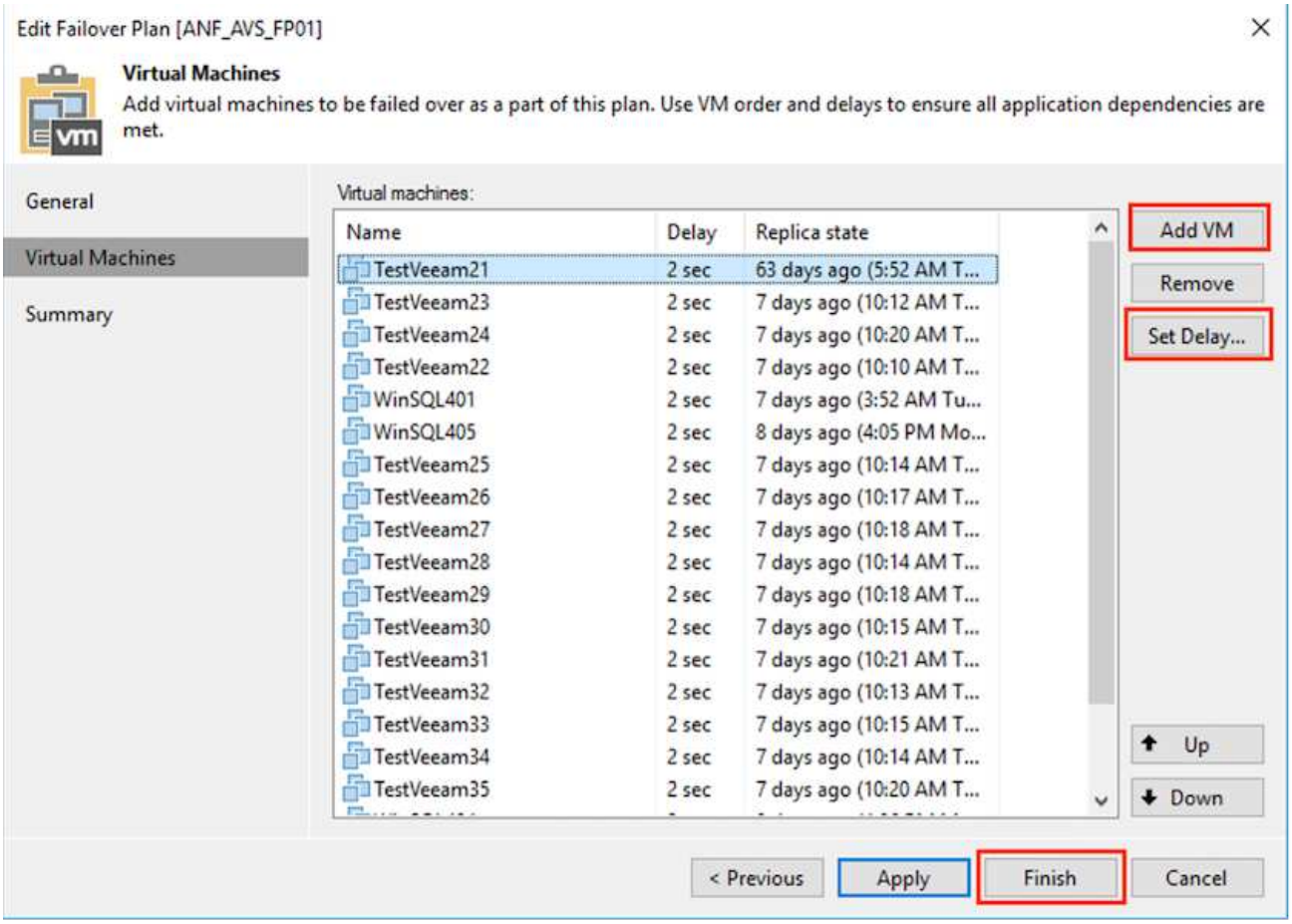
1. 在主页视图上。右键单击“副本”节点并选择“故障转移计划”>“故障转移计划”>“VMware vSphere”。



2. 接下来为计划提供名称和描述。可以根据需要添加故障转移前和故障转移后脚本。例如，在启动复制的虚拟机之前运行脚本来关闭虚拟机。



3. 将虚拟机添加到计划中，并修改虚拟机启动顺序和启动延迟以满足应用程序依赖关系。



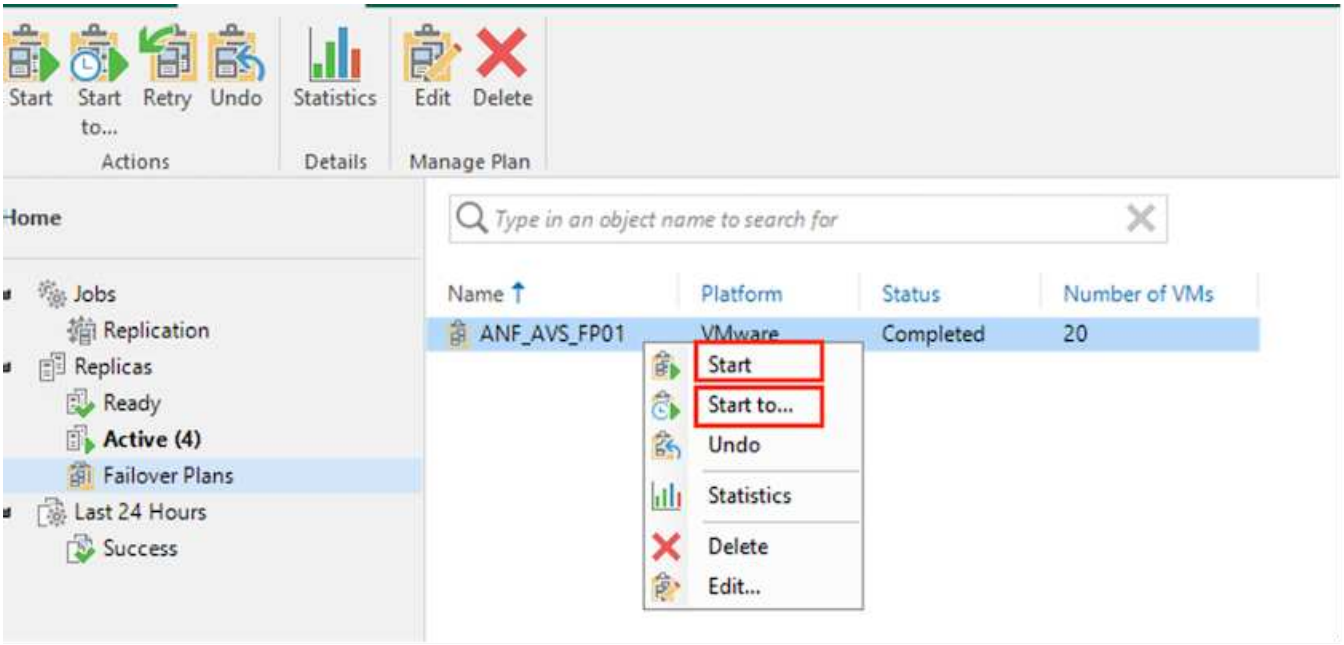
有关创建复制作业的其他信息，请参阅"创建复制作业"。

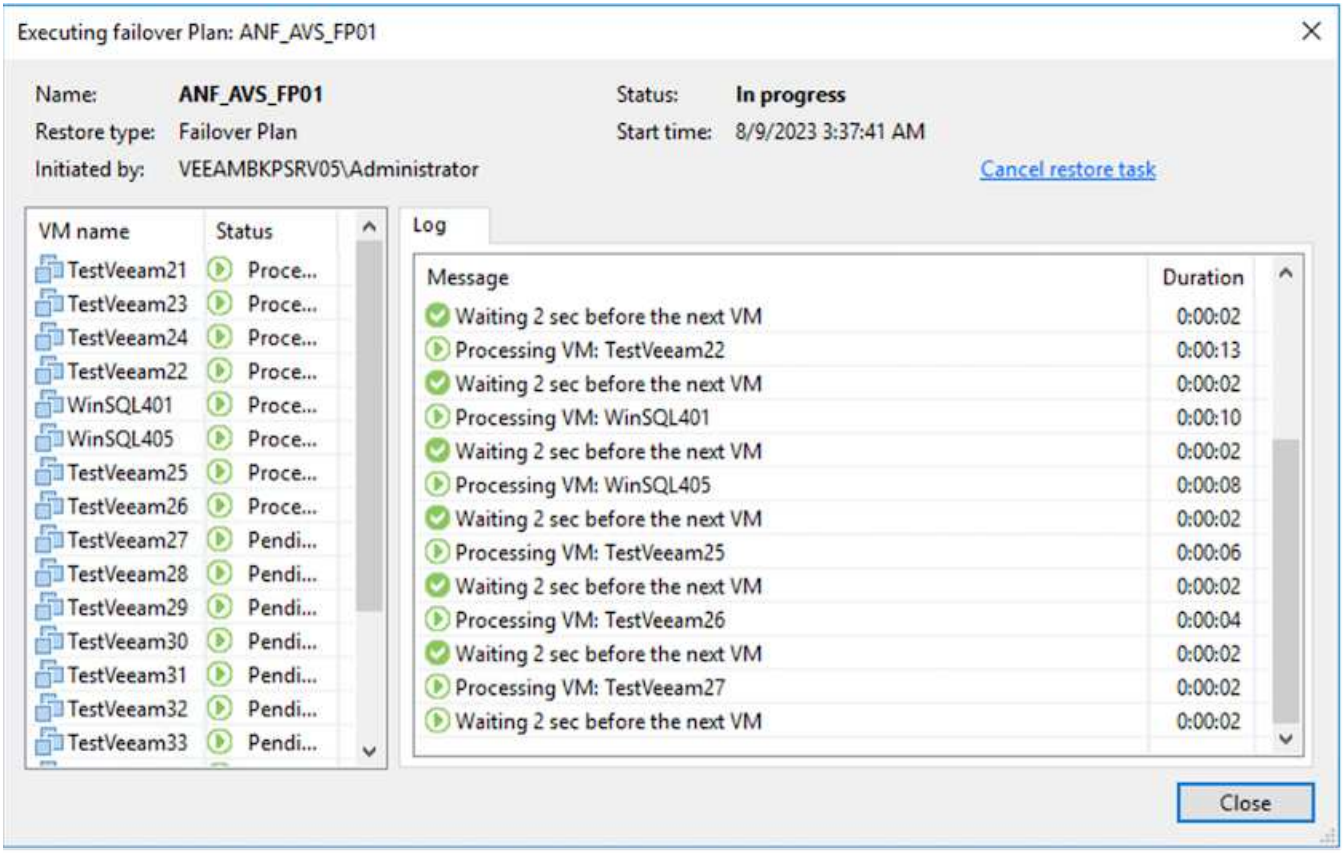
▼ 步骤 3：运行故障转移计划

在故障转移期间，生产站点中的源虚拟机将切换到灾难恢复站点上的副本。作为故障转移过程的一部分，Veeam Backup & Replication 将 VM 副本恢复到所需的恢复点，并将所有 I/O 活动从源 VM 移动到其副本。副本不仅可用于灾难发生时，还可用于模拟灾难恢复演习。在故障转移模拟期间，源虚拟机仍保持运行。一旦完成所有必要的测试，您就可以撤消故障转移并恢复正常操作。

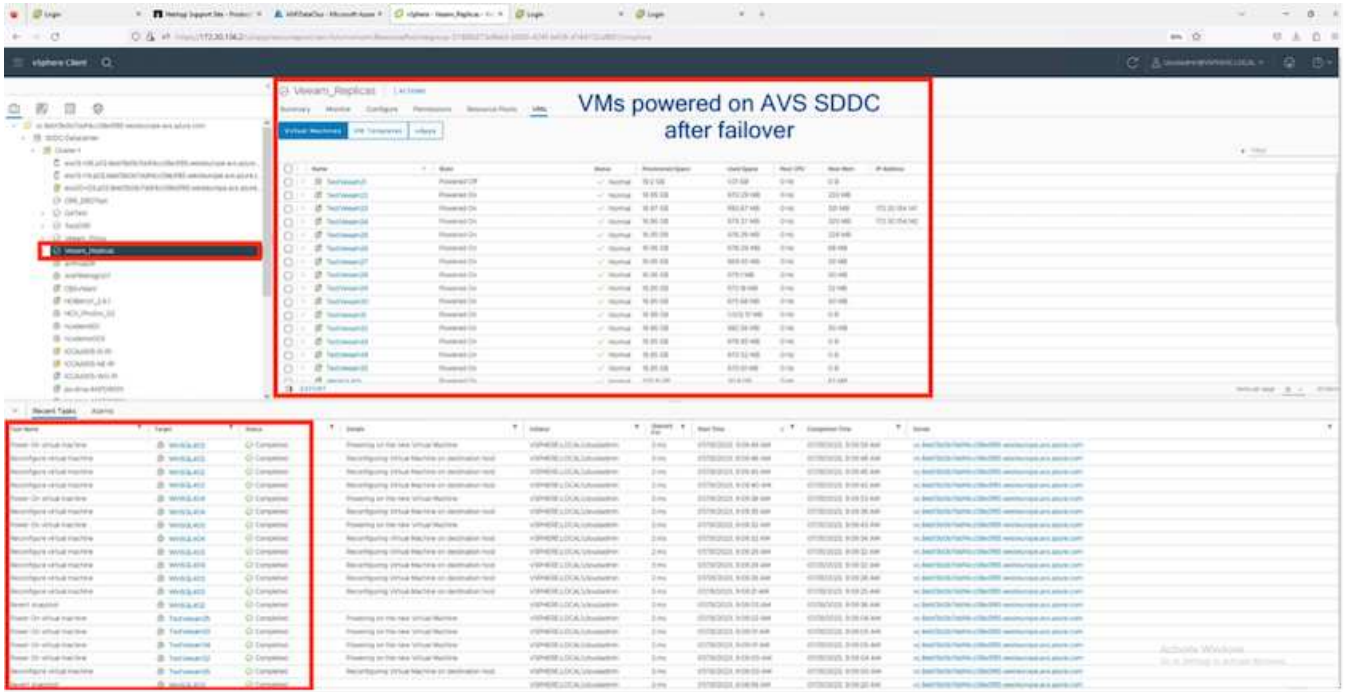
确保网络分段到位，以避免故障转移期间发生 IP 冲突。

要启动故障转移计划，只需单击“故障转移计划”选项卡，然后右键单击您的故障转移计划。选择“开始”。这将使用 VM 副本的最新还原点进行故障转移。要故障转移到 VM 副本的特定还原点，请选择*开始*。

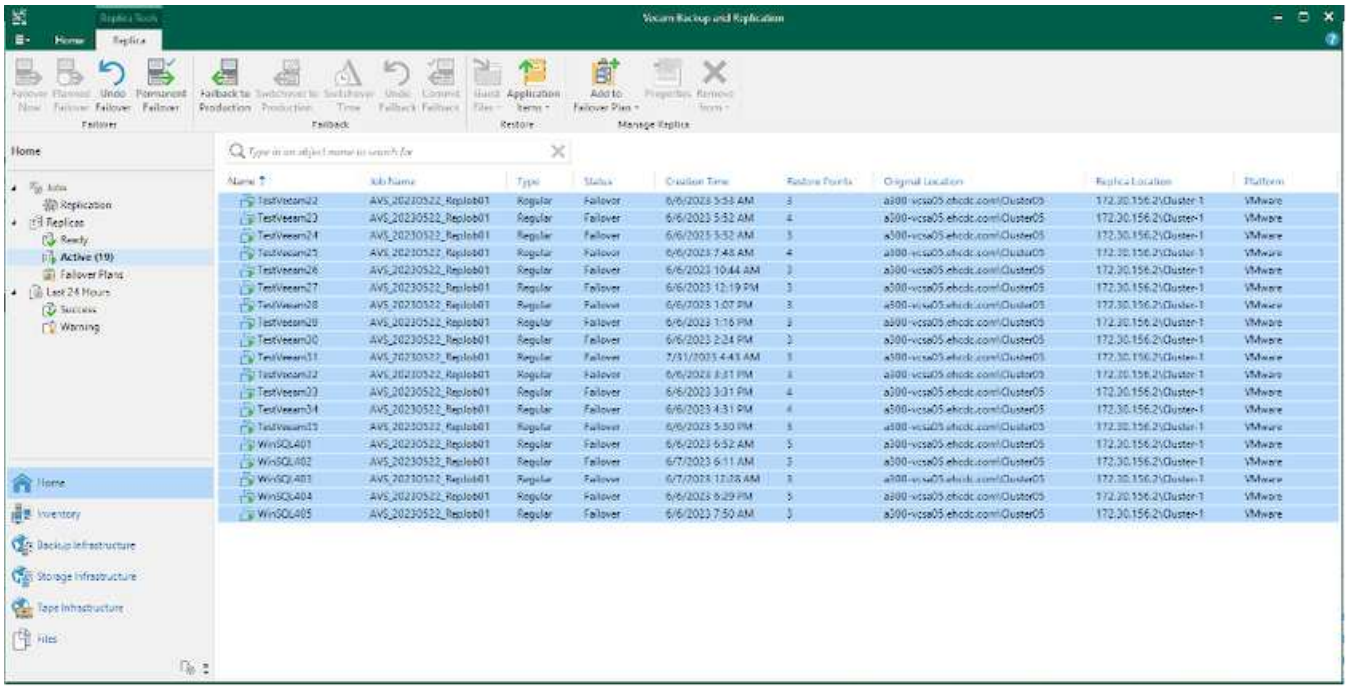




VM 副本的状态从“就绪”更改为“故障转移”，并且 VM 将在目标 Azure VMware 解决方案 (AVS) SDDC 群集/主机上启动。



故障转移完成后，虚拟机的状态将变为“故障转移”。



Veeam Backup & Replication 停止源 VM 的所有复制活动，直到其副本返回到就绪状态。

有关故障转移计划的详细信息，请参阅"故障转移计划"。

▼ 步骤 4：故障恢复到生产站点

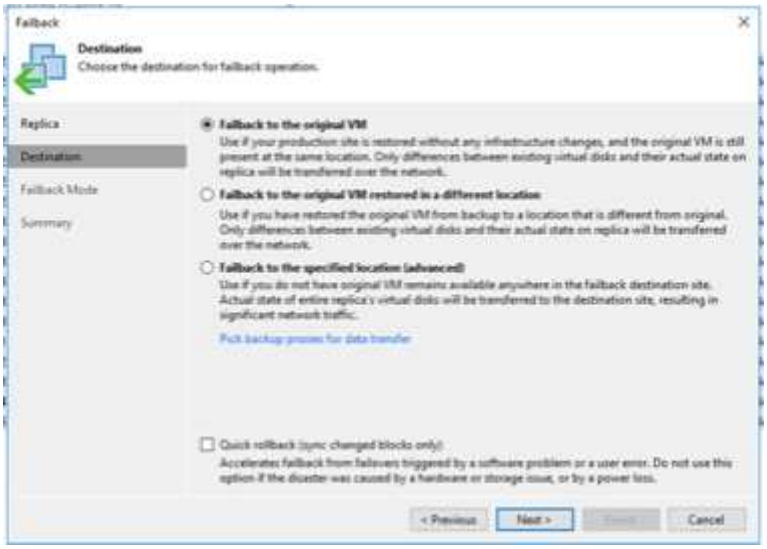
当故障转移计划运行时，它被视为一个中间步骤，需要根据需求最终确定。选项包括以下内容：

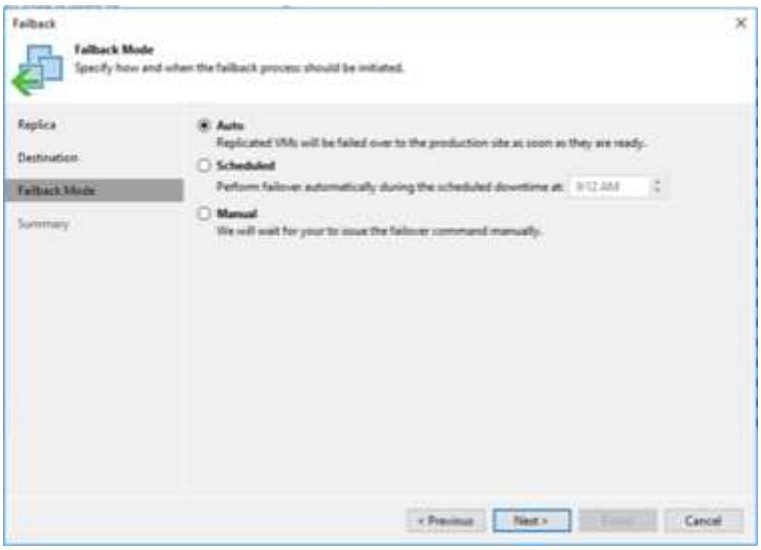
- 故障恢复到生产 - 切换回原始 VM，并将 VM 副本运行时发生的所有更改传输到原始 VM。

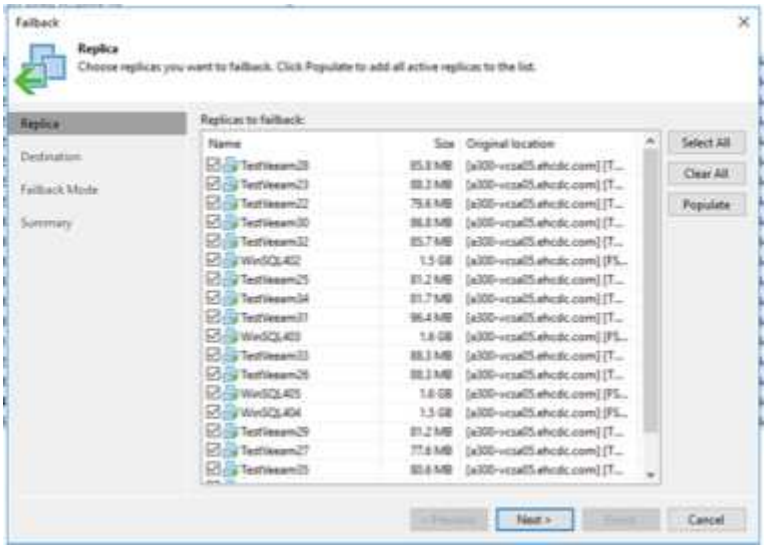
当您执行故障回复时，更改仅被传输但不会被发布。如果原始虚拟机未按预期工作，请选择*提交故障恢复*（一旦确认原始虚拟机按预期工作）或撤消故障恢复以返回虚拟机副本。

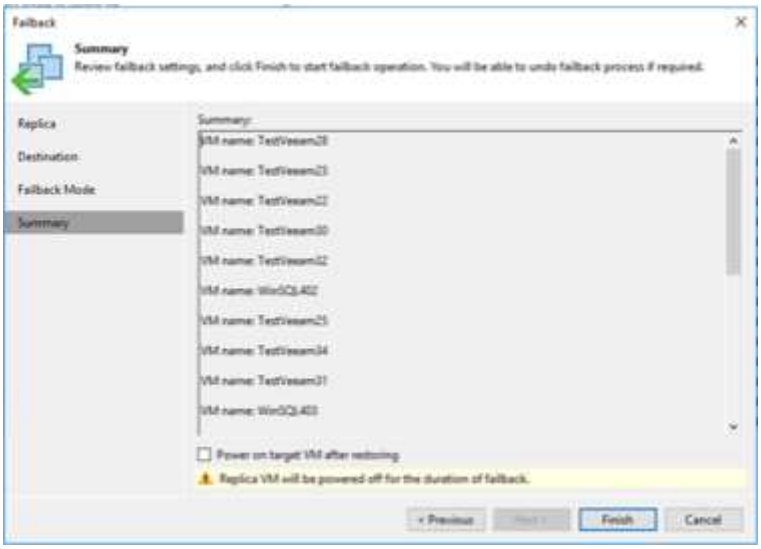
- 撤消故障转移 - 切换回原始虚拟机并放弃运行时对虚拟机副本所做的所有更改。
- 永久故障转移 - 从原始 VM 永久切换到 VM 副本，并使用此副本作为原始 VM。

在这个演示中，选择了故障恢复到生产。在向导的目标步骤中选择了故障回复到原始虚拟机，并且启用了“恢复后启动虚拟机”复选框。



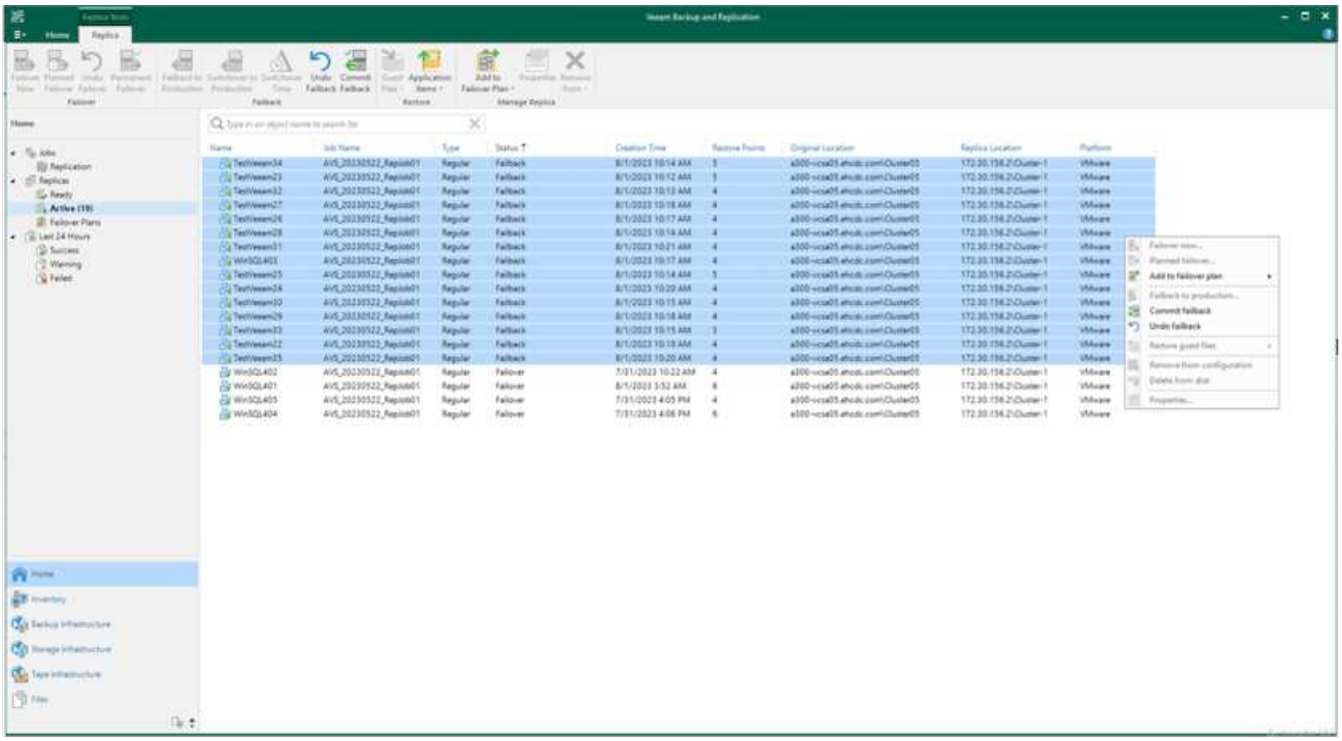




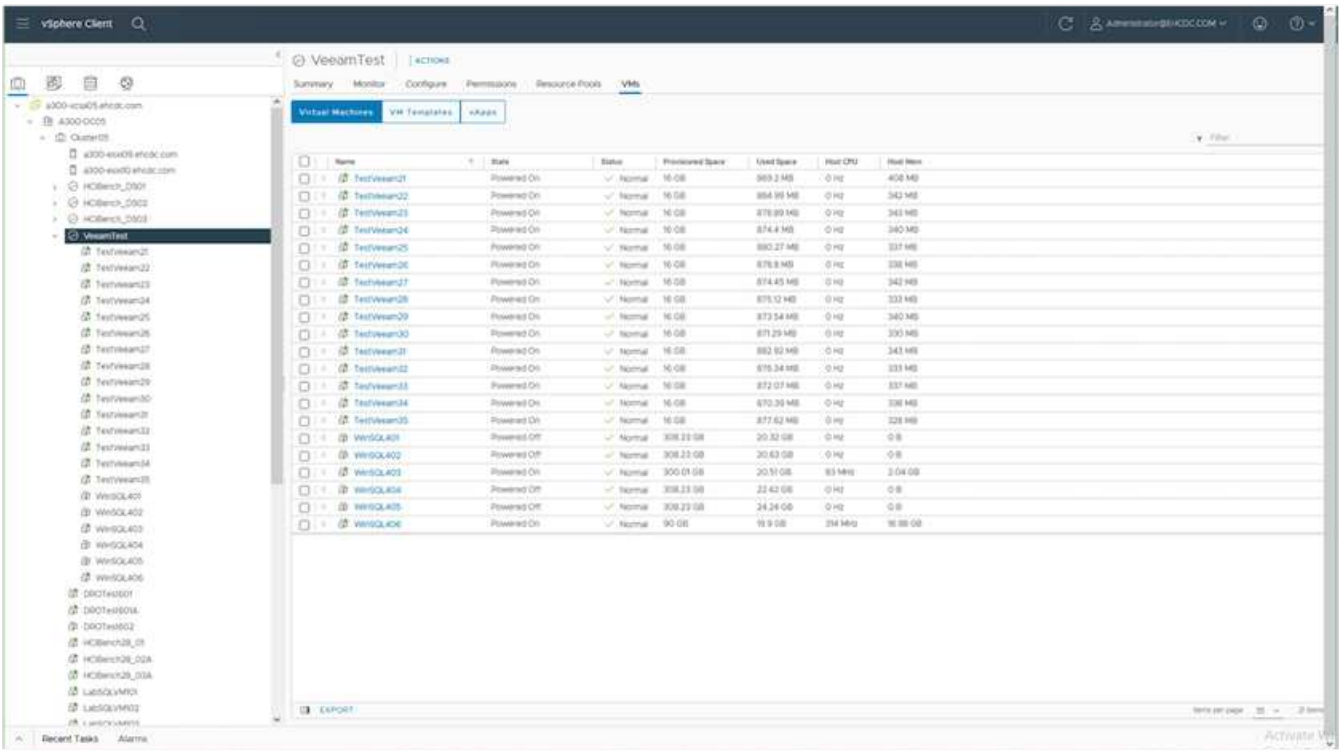


故障回复提交是完成故障回复操作的方法之一。当故障回复被提交时，它会确认发送到故障回复的虚拟机（生产虚拟机）的更改是否按预期工作。提交操作后，Veeam Backup & Replication 将恢复生产虚拟机的复制活动。

有关故障恢复过程的详细信息，请参阅 Veeam 文档"复制的故障转移和故障恢复"。



故障恢复生产成功后，所有虚拟机都将恢复到原始生产站点。



结束语

Azure NetApp Files数据存储功能使 Veeam 或任何经过验证的第三方工具能够利用 Pilot light 集群来提供低成本的 DR 解决方案，而不是仅仅为了容纳 VM 副本而建立大型集群。这提供了一种有效的方法来处理量身定制的灾难恢复计划，并重复使用内部现有的备份产品进行灾难恢复，通过退出内部灾难恢复数据中心实现基于云的灾难恢复。发生灾难时，可以通过单击按钮进行故障转移，或者在发生灾难时自动进行故障转移。

要了解有关此过程的更多信息，请随意观看详细的演示视频。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

在 **Azure/AVS** 上迁移工作负载

TR-4940：使用 **VMware HCX** 将工作负载迁移到**Azure NetApp Files**数据存储 **-** 快速入门指南

Azure VMware 解决方案和Azure NetApp Files存储最常见的用例之一是迁移 VMware 工作负载。 VMware HCX 是首选方案，它提供了各种迁移机制，可将本地虚拟机 (VM) 及其数据移动到Azure NetApp Files数据存储。

概述：使用 **VMware HCX**、 **Azure NetApp Files**数据存储和 **Azure VMware** 解决方案迁移虚拟机

VMware HCX 主要是一个迁移平台，旨在简化应用程序迁移、工作负载重新平衡甚至跨云的业务连续性。它是 Azure VMware 解决方案私有云的一部分，提供了多种迁移工作负载的方法，可用于灾难恢复 (DR) 操作。

本文档提供了配置Azure NetApp Files数据存储以及下载、部署和配置 VMware HCX 的分步指导，包括本地和 Azure VMware 解决方案端的所有主要组件（包括互连、网络扩展和 WAN 优化），以启用各种 VM 迁移机制。

> VMware HCX 适用于任何数据存储类型，因为迁移是在 VM 级别进行的。因此，本文档适用于现有NetApp客户和计划使用 Azure VMware 解决方案部署Azure NetApp Files以实现经济高效的 VMware 云部署的非NetApp客户。

▼ 概要步骤

此列表提供了在 Azure 云端安装和配置 HCX Cloud Manager 以及在本地安装 HCX Connector 所需的高级步骤：

1. 通过 Azure 门户安装 HCX。
2. 在本地 VMware vCenter Server 中下载并部署 HCX Connector Open Virtualization Appliance (OVA) 安装程序。
3. 使用许可证密钥激活 HCX。
4. 将本地 VMware HCX 连接器与 Azure VMware 解决方案 HCX 云管理器配对。
5. 配置网络配置文件、计算配置文件和服务网格。
6. （可选）执行网络扩展以避免在迁移期间重新分配 IP。
7. 验证设备状态并确保可以迁移。
8. 迁移虚拟机工作负载。

▼ 前提条件

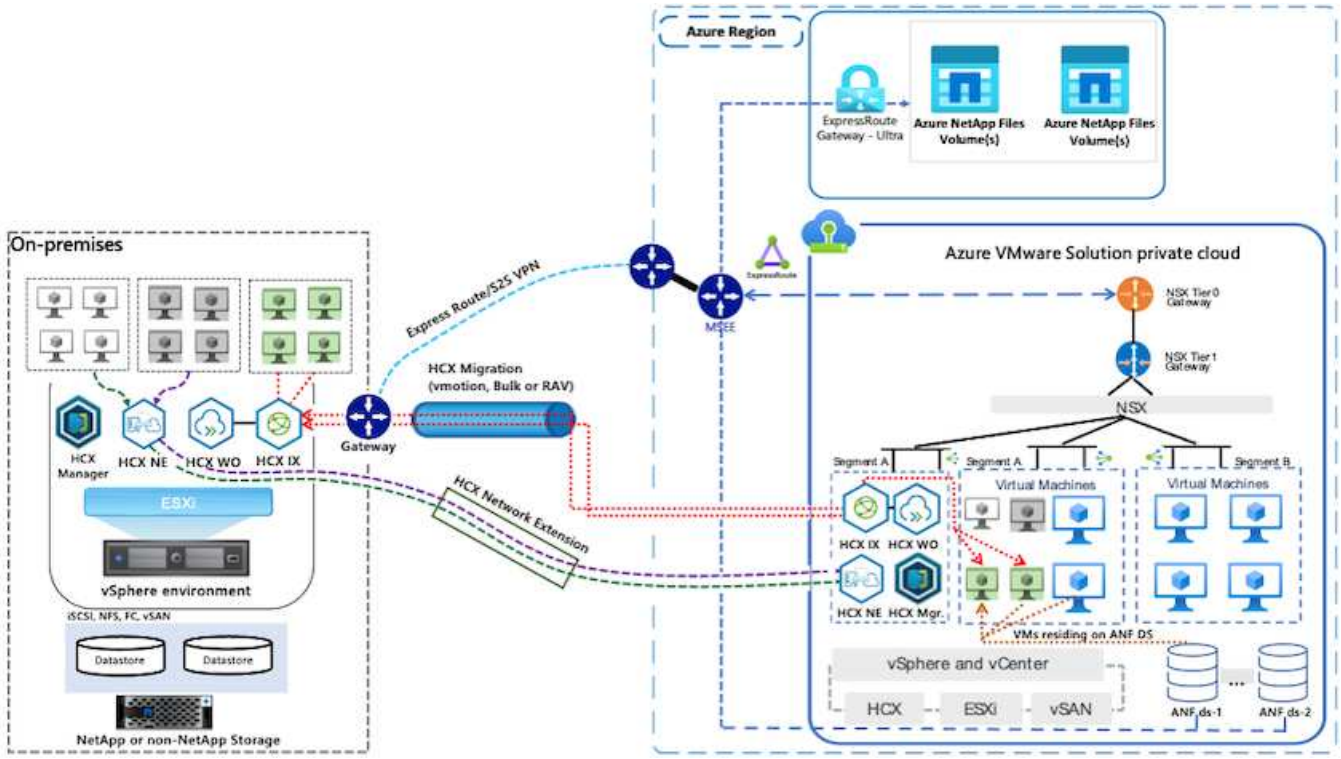
开始之前，请确保满足以下先决条件。有关详细信息，请参阅 "链接"。满足先决条件（包括连接性）后，通过从 Azure VMware 解决方案门户生成许可证密钥来配置和激活 HCX。下载 OVA 安装程序后，按照如下所述进行安装过程。

> HCX 高级版是默认选项，VMware HCX 企业版也可通过支持票获得，并且无需额外付费即可获得支持。

- 使用现有的 Azure VMware 解决方案软件定义数据中心 (SDDC) 或使用此解决方案创建私有云"NetApp链接"或者这个 "微软链接"。
- 从支持 VMware vSphere 的内部部署数据中心迁移虚拟机和相关数据需要从数据中心到 SDDC 环境的网络连接。在迁移工作负载之前， "设置站点到站点 VPN 或 Express 路由 Global Access 连接"在本地环境和相应的私有云之间。
- 从本地 VMware vCenter Server 环境到 Azure VMware 解决方案私有云的网络路径必须支持使用 vMotion 迁移 VM。
- 确保所需的 "防火墙规则和端口"允许在本地 vCenter Server 和 SDDC vCenter 之间进行 vMotion 流量。在私有云上，默认配置vMotion网络上的路由。
- Azure NetApp FilesNFS 卷应作为数据存储装载在 Azure VMware 解决方案中。按照本文中详细说明的步骤操作 "链接"将Azure NetApp Files数据存储附加到 Azure VMware 解决方案主机。

▼ 高级架构

出于测试目的，用于此验证的本地实验室环境通过站点到站点 VPN 连接，这允许本地连接到 Azure VMware 解决方案。



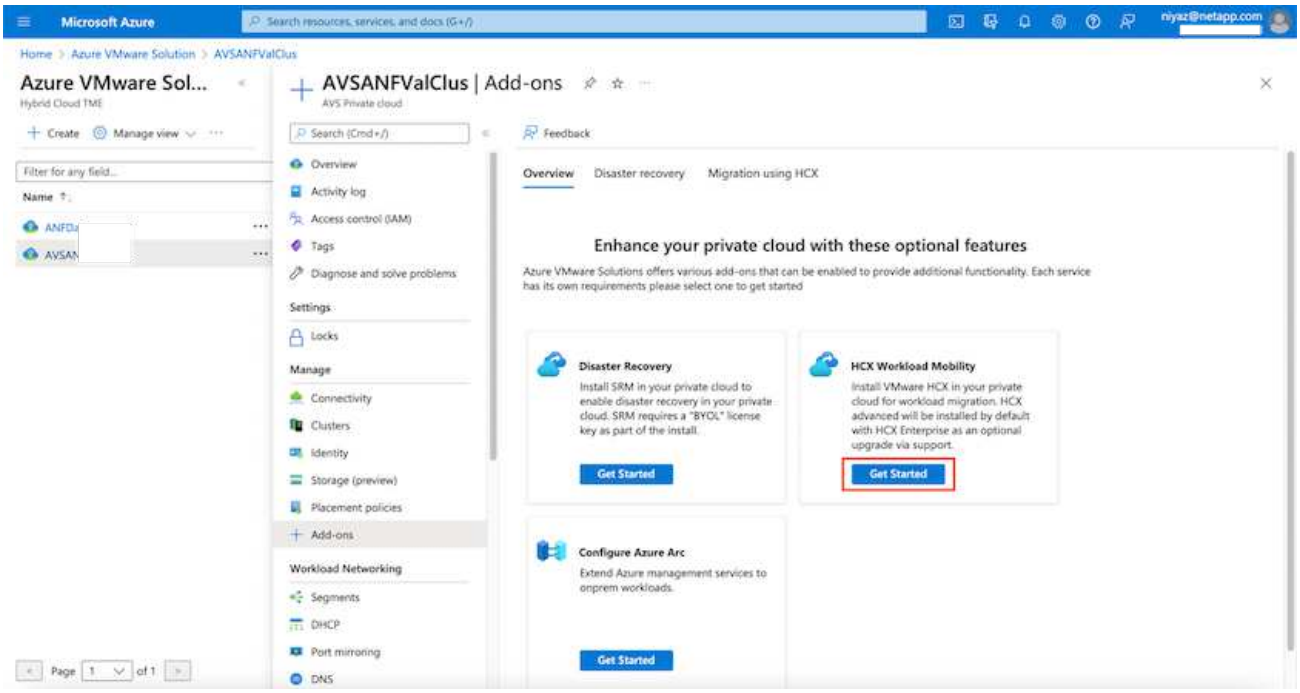
解决方案部署

按照一系列步骤完成此解决方案的部署：

▼ 步骤 **1**：使用附加组件选项通过 **Azure** 门户安装 **HCX**

要执行安装，请完成以下步骤：

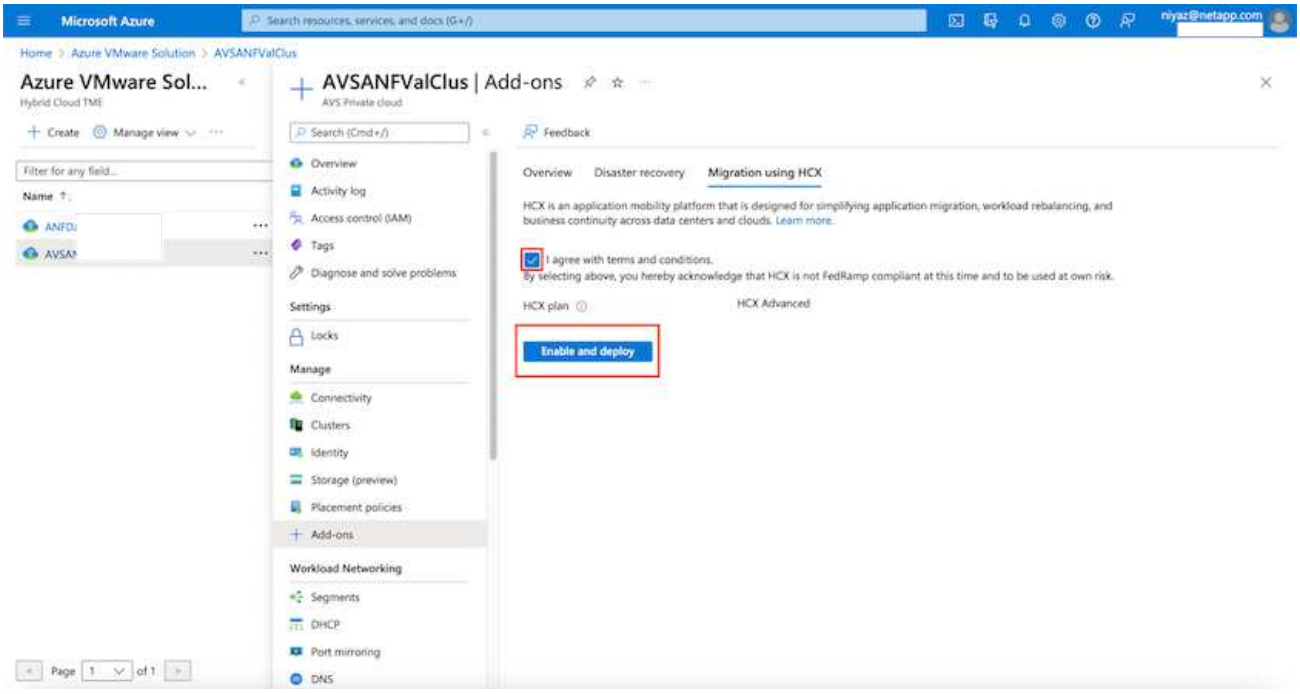
1. 登录 Azure 门户并访问 Azure VMware 解决方案私有云。
2. 选择适当的私有云并访问附加组件。这可以通过导航到*管理>附加组件*来完成。
3. 在 HCX Workload Mobility 部分，单击 开始。



4. 选择*我同意条款和条件*选项，然后单击*启用和部署*。

   默认部署是 HCX Advanced。打开支持请求以启用企业版。

   部署大约需要 25 到 30 分钟。



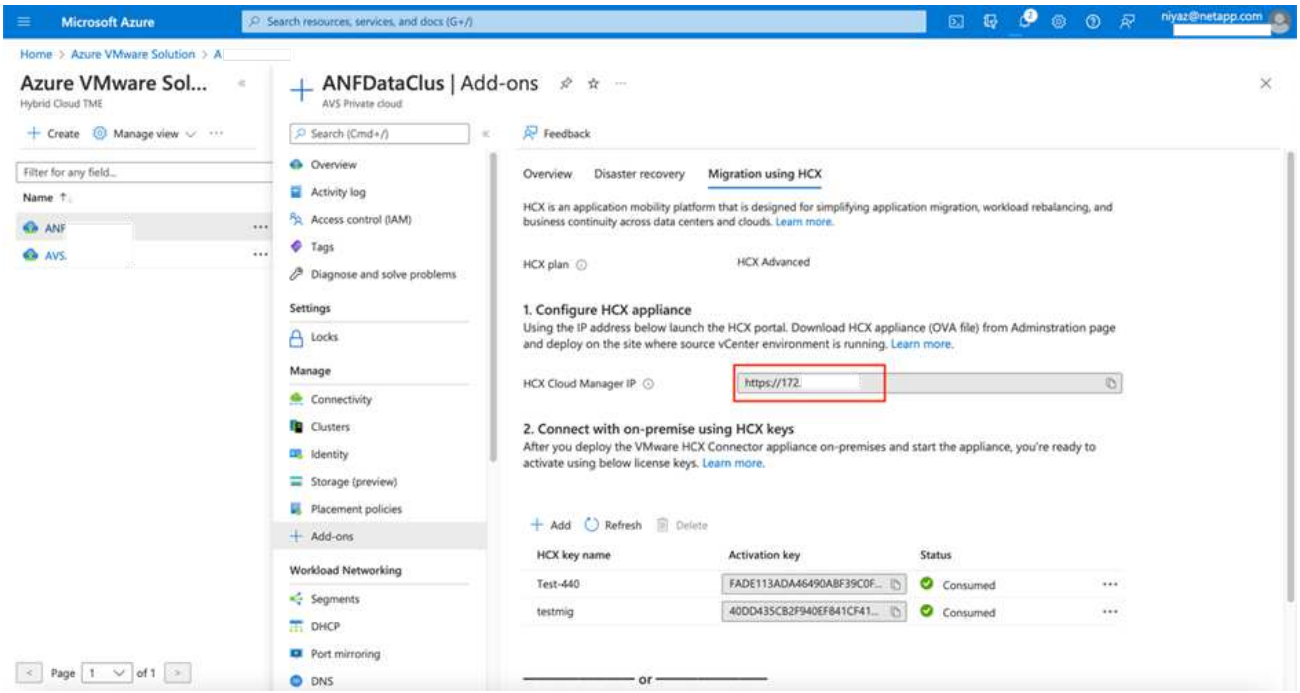
▼ 步骤 2：在本地 **vCenter Server** 中部署安装程序 **OVA**

为了使本地连接器连接到 Azure VMware 解决方案中的 HCX 管理器，请确保在本地环境中打开了相应的防火墙端口。

要在本地 vCenter Server 中下载并安装 HCX Connector，请完成以下步骤：

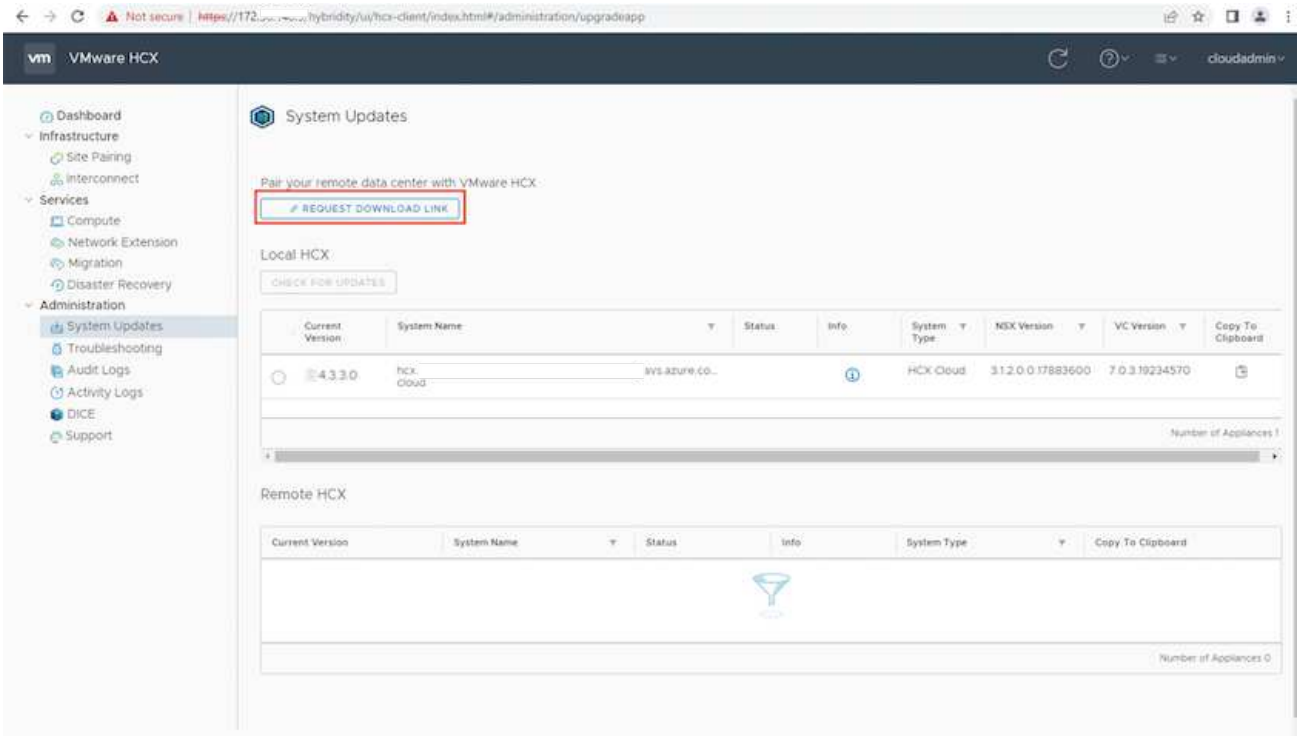
1. 从 Azure 门户转到 Azure VMware 解决方案，选择私有云，然后使用 HCX 选择 管理 > 附加组件 > 迁移，并复制 HCX 云管理器门户以下载 OVA 文件。

   使用默认 CloudAdmin 用户凭据访问 HCX 门户。

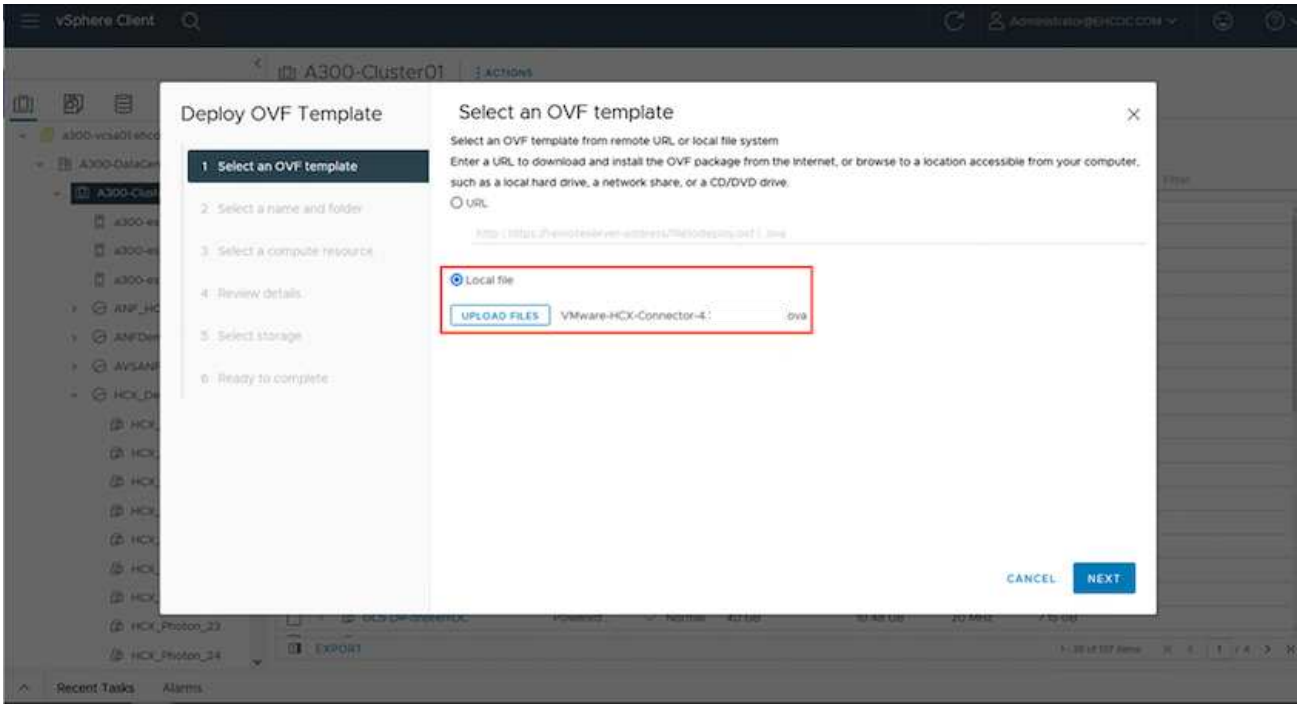


2. 使用 jumphost 通过 cloudadmin@vsphere.local 访问 HCX 门户后，导航到 管理 > 系统更新，然后单击请求下载链接。

   下载或复制 OVA 链接并将其粘贴到浏览器中，开始下载 VMware HCX Connector OVA 文件以部署在本地 vCenter Server 上。



3. 下载 OVA 后，使用 部署 **OVF** 模板 选项将其部署到本地 VMware vSphere 环境。



4. 输入 OVA 部署所需的所有信息，单击“下一步”，然后单击“完成”以部署 VMware HCX 连接器 OVA。

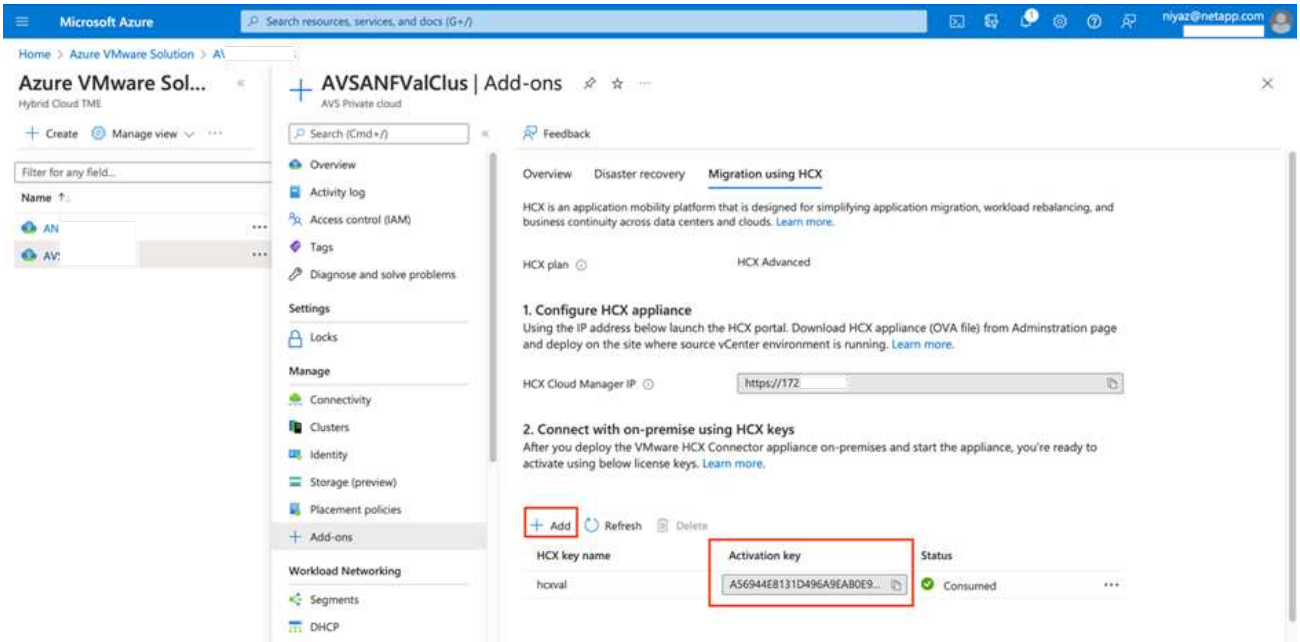
手动启动虚拟设备。

有关分步说明，请参阅 "VMware HCX 用户指南"。

▼ 步骤 3：使用许可证密钥激活 **HCX Connector**

在本地部署 VMware HCX Connector OVA 并启动设备后，请完成以下步骤以激活 HCX Connector。从 Azure VMware 解决方案门户生成许可证密钥，并在 VMware HCX 管理器中激活它。

1. 从 Azure 门户转到 Azure VMware 解决方案，选择私有云，然后选择“管理”>“附加组件”>“使用 HCX 迁移”。
2. 在*使用 HCX 密钥连接本地*下，单击*添加*并复制激活密钥。



部署的每个本地 HCX 连接器都需要单独的密钥。

3. 登录本地 VMware HCX 管理器 `"https://hcxmanagerIP:9443"`使用管理员凭据。

使用 OVA 部署期间定义的密码。

4. 在许可中，输入从步骤 3 复制的密钥，然后单击 激活。

本地 HCX 连接器应该具有互联网访问权限。

5. 在“数据中心位置”下，提供在本地安装 VMware HCX 管理器的最近位置。单击“继续”。
6. 在“系统名称”下，更新名称并单击“继续”。
7. 单击“是，继续”。
8. 在“连接您的 vCenter”下，提供 vCenter Server 的完全限定域名 (FQDN) 或 IP 地址以及相应的凭据，然后单击“继续”。

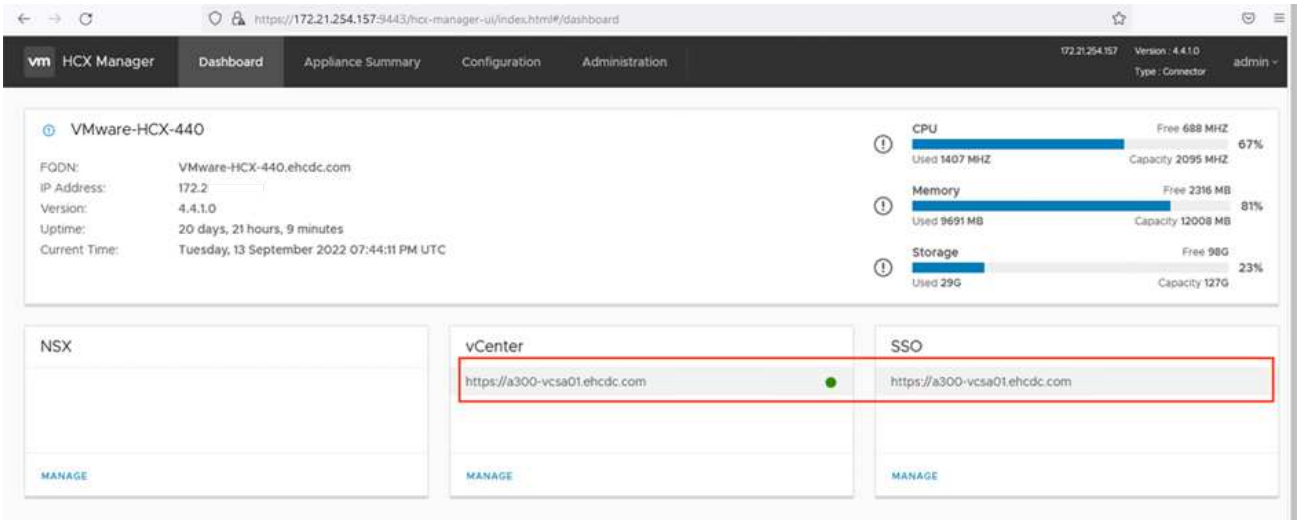
使用 FQDN 以避免以后出现连接问题。

9. 在“配置 SSO/PSC”下，提供平台服务控制器的 FQDN 或 IP 地址，然后单击“继续”。

输入 VMware vCenter Server FQDN 或 IP 地址。

10. 验证输入的信息是否正确，然后单击“重新启动”。
11. 服务重新启动后，vCenter Server 在出现的页面上显示为绿色。 vCenter Server 和 SSO 都必须具有适当的配置参数，这些参数应与上一页相同。

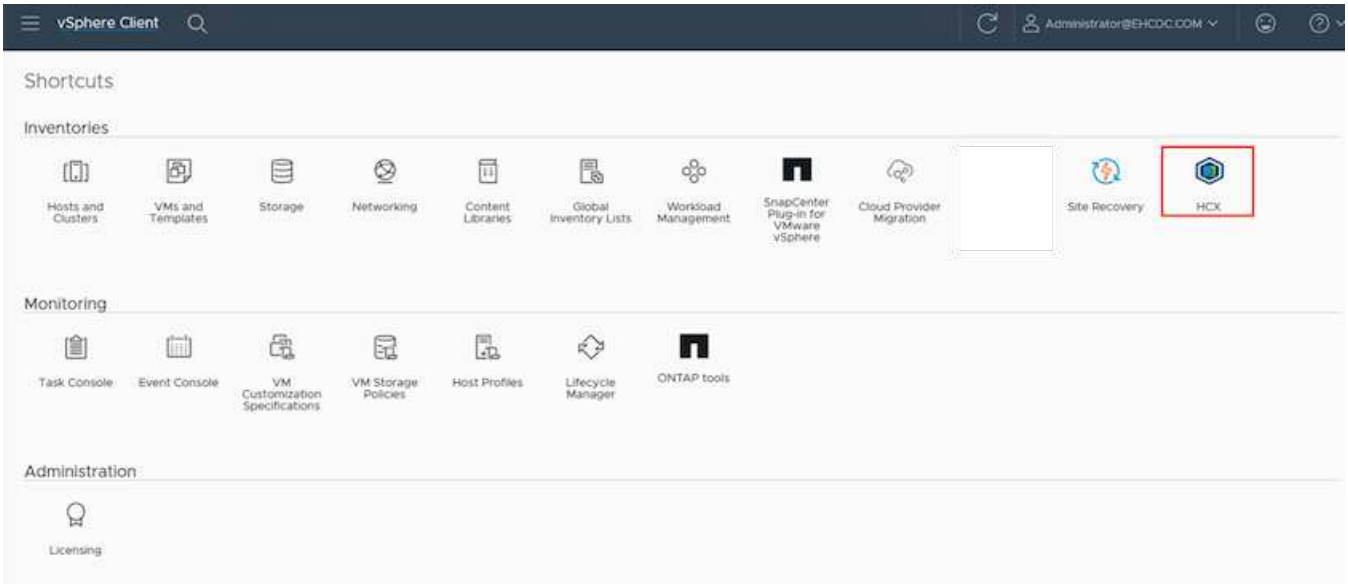
此过程大约需要 10 到 20 分钟，以便将插件添加到 vCenter Server。



▼ 步骤 4：将本地 **VMware HCX** 连接器与 **Azure VMware** 解决方案 **HCX** 云管理器配对

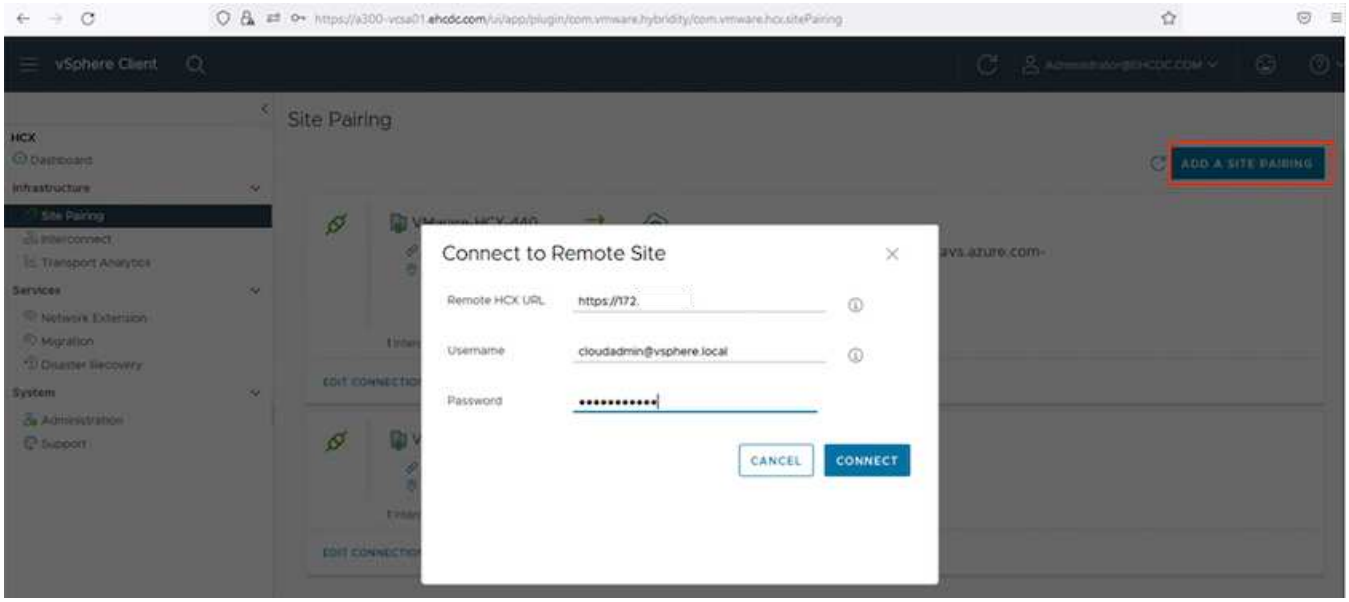
在本地和 Azure VMware 解决方案中安装 HCX 连接器后，通过添加配对为 Azure VMware 解决方案私有云配置本地 VMware HCX 连接器。要配置站点配对，请完成以下步骤：

1. 要在本地 vCenter 环境和 Azure VMware 解决方案 SDDC 之间创建站点对，请登录到本地 vCenter Server 并访问新的 HCX vSphere Web Client 插件。



1. 在基础设施下，单击*添加站点配对*。

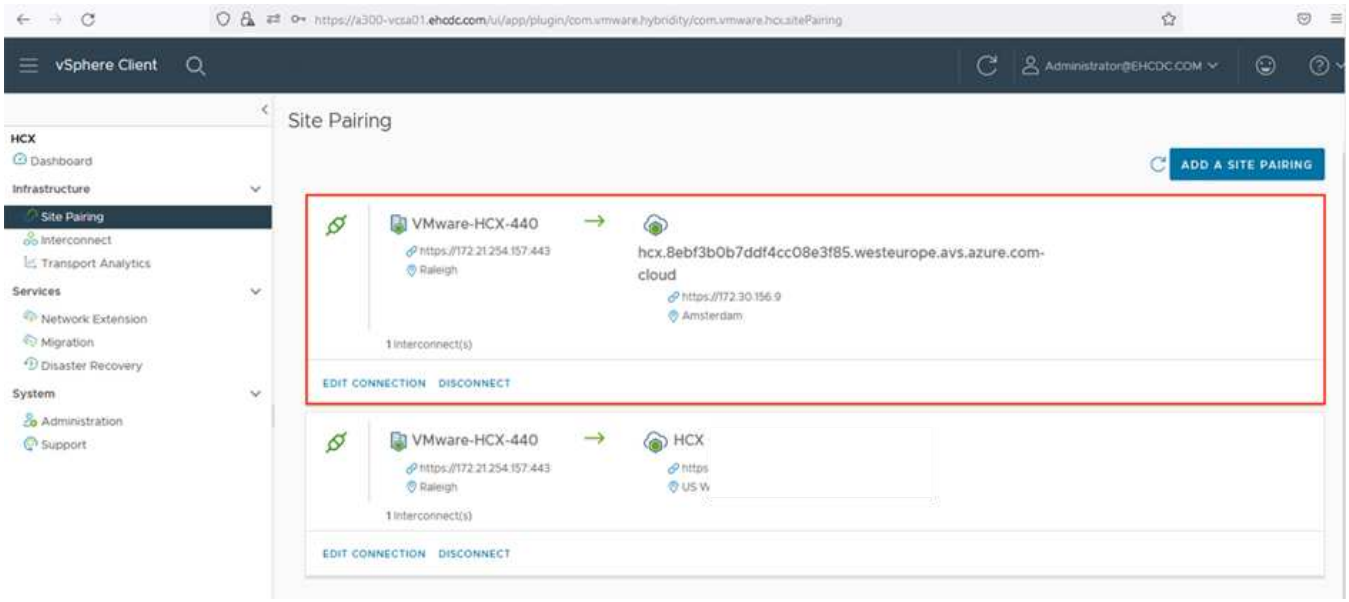
输入 Azure VMware 解决方案 HCX 云管理器 URL 或 IP 地址以及用于访问私有云的 CloudAdmin 角色的凭据。



1. 单击“连接”。

VMware HCX Connector 必须能够通过端口 443 路由到 HCX Cloud Manager IP。

1. 创建配对后，新配置的站点配对可在 HCX 仪表板上获得。

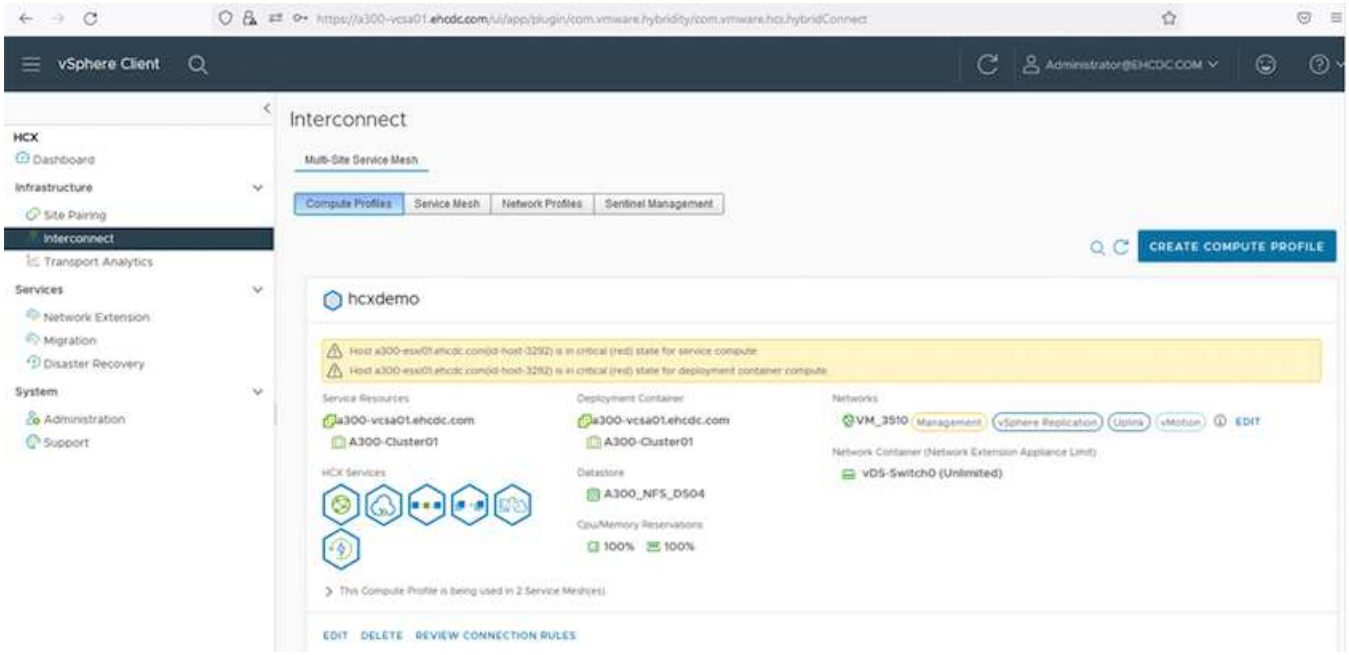


▼ 步骤 **5**：配置网络配置文件、计算配置文件和服务网格

VMware HCX Interconnect 服务设备通过互联网和与目标站点的专用连接提供复制和基于 vMotion 的迁移功能。互连提供加密、流量工程和 VM 移动性。要创建互连服务设备，请完成以下步骤：

1. 在基础设施下，选择*互连>多站点服务网格>计算配置文件>创建计算配置文件*。

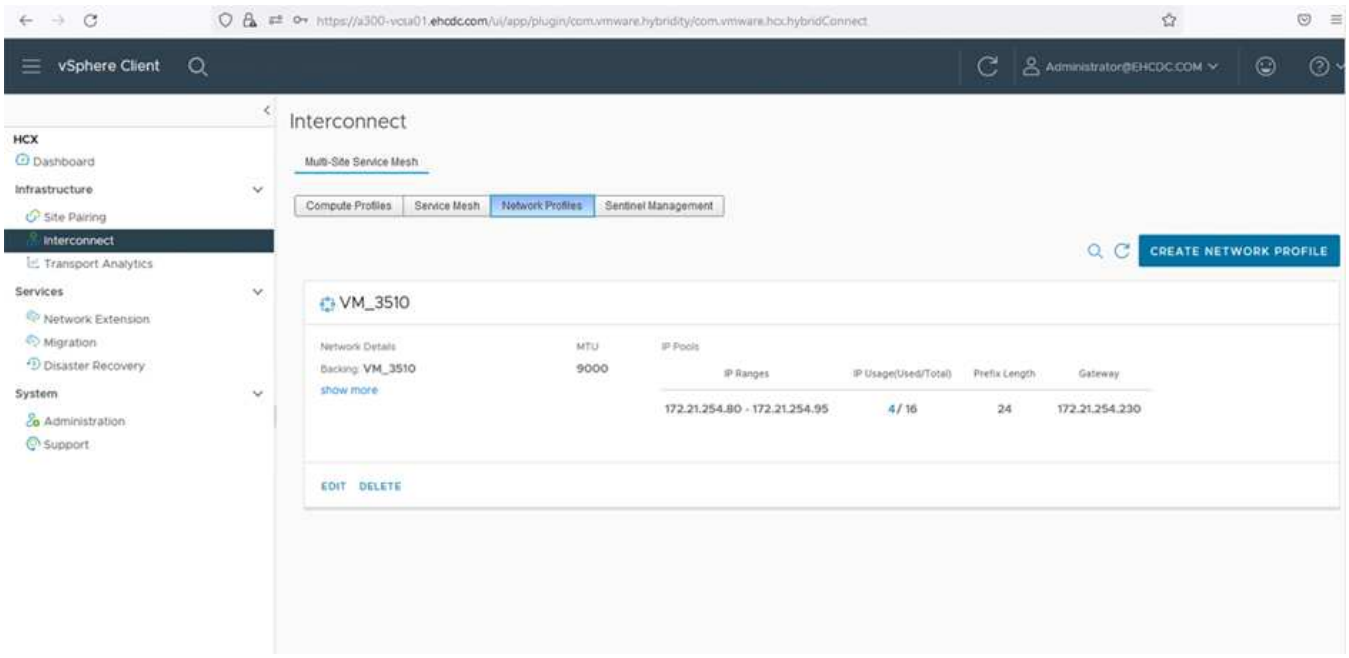
计算配置文件定义部署参数，包括部署的设备以及 VMware 数据中心的哪些部分可供 HCX 服务访问。



1. 创建计算配置文件后，通过选择“多站点服务网格”>“网络配置文件”>“创建网络配置文件”来创建网络配置文件。

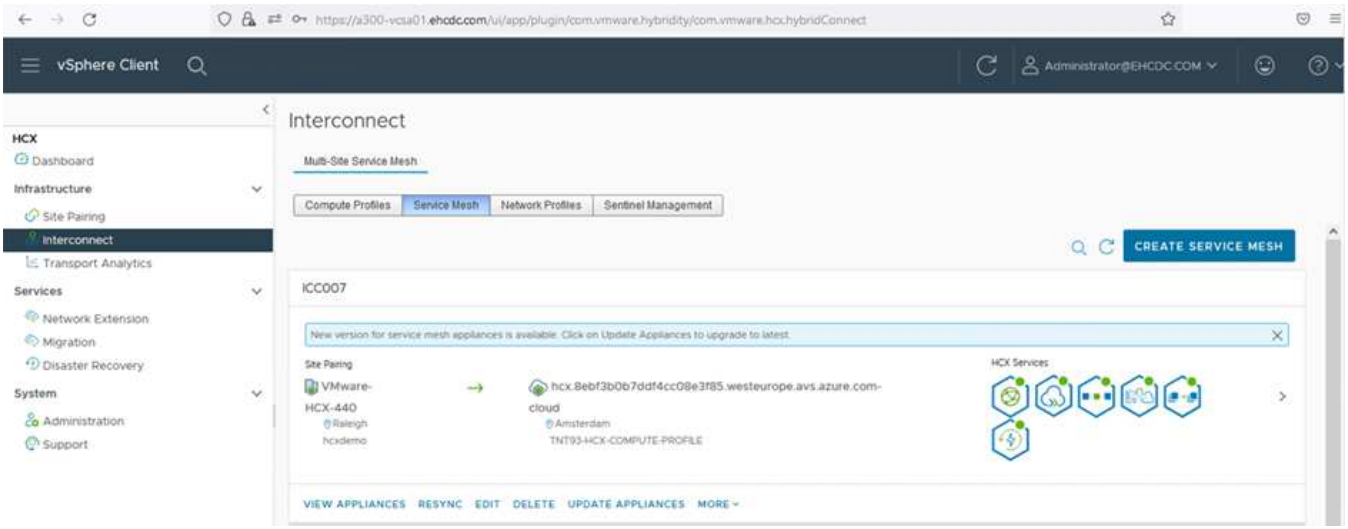
网络配置文件定义了 HCX 用于其虚拟设备的一系列 IP 地址和网络。

此步骤需要两个或更多 IP 地址。这些 IP 地址由管理网络分配给互连设备。

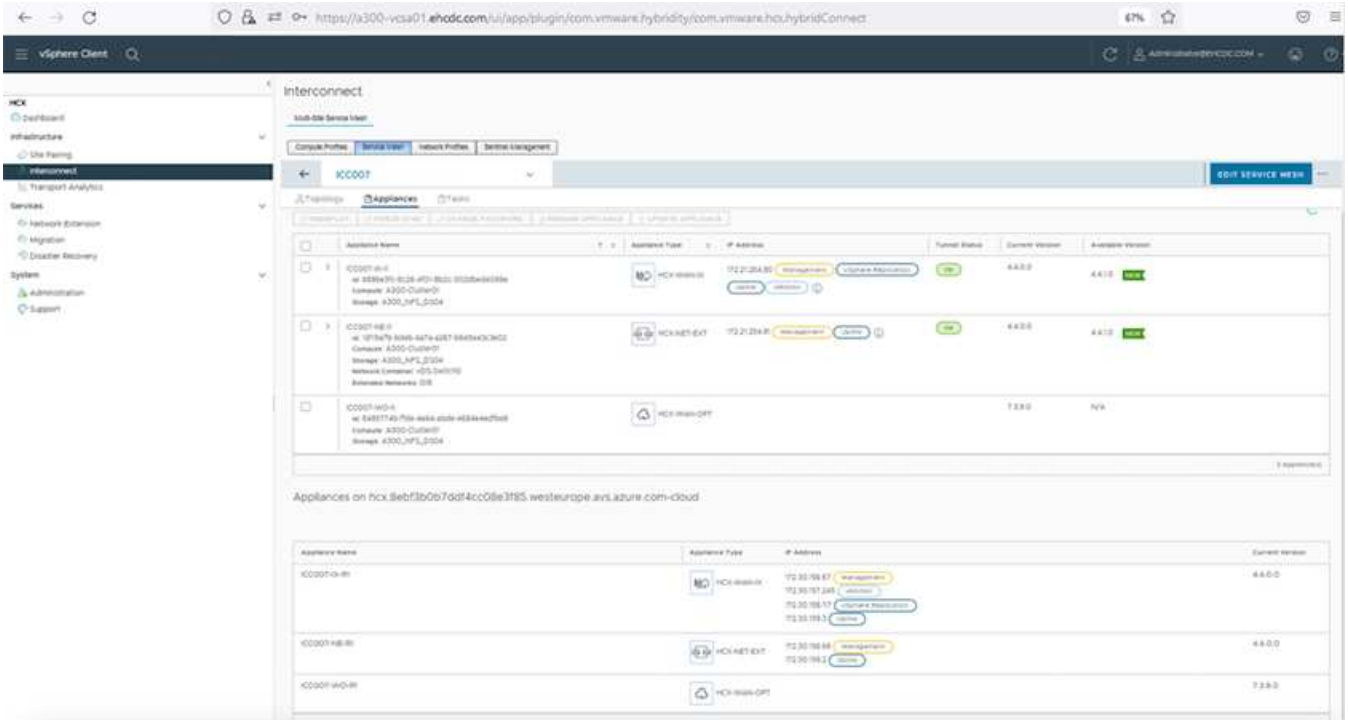


1. 此时，计算和网络配置文件已成功创建。
2. 通过选择“**Interconnect**”选项中的“**Service Mesh**”选项卡并选择本地和 Azure SDDC 站点来创建服务网格。
3. 服务网格指定本地和远程计算和网络配置文件对。

作为此过程的一部分，HCX 设备在源站点和目标站点上部署并自动配置，以创建安全的传输结构。



1. 这是配置的最后一步。完成部署大约需要 30 分钟。配置服务网格后，环境已准备就绪，并且已成功创建 IPsec 隧道来迁移工作负载虚拟机。



▼ 步骤 **6**：迁移工作负载

可以使用各种 VMware HCX 迁移技术在本地和 Azure SDDC 之间双向迁移工作负载。可以使用多种迁移技术将虚拟机移至 VMware HCX 激活的实体或从中移出，例如 HCX 批量迁移、HCX vMotion、HCX 冷迁移、HCX 复制辅助 vMotion（HCX 企业版提供）和 HCX OS 辅助迁移（HCX 企业版提供）。

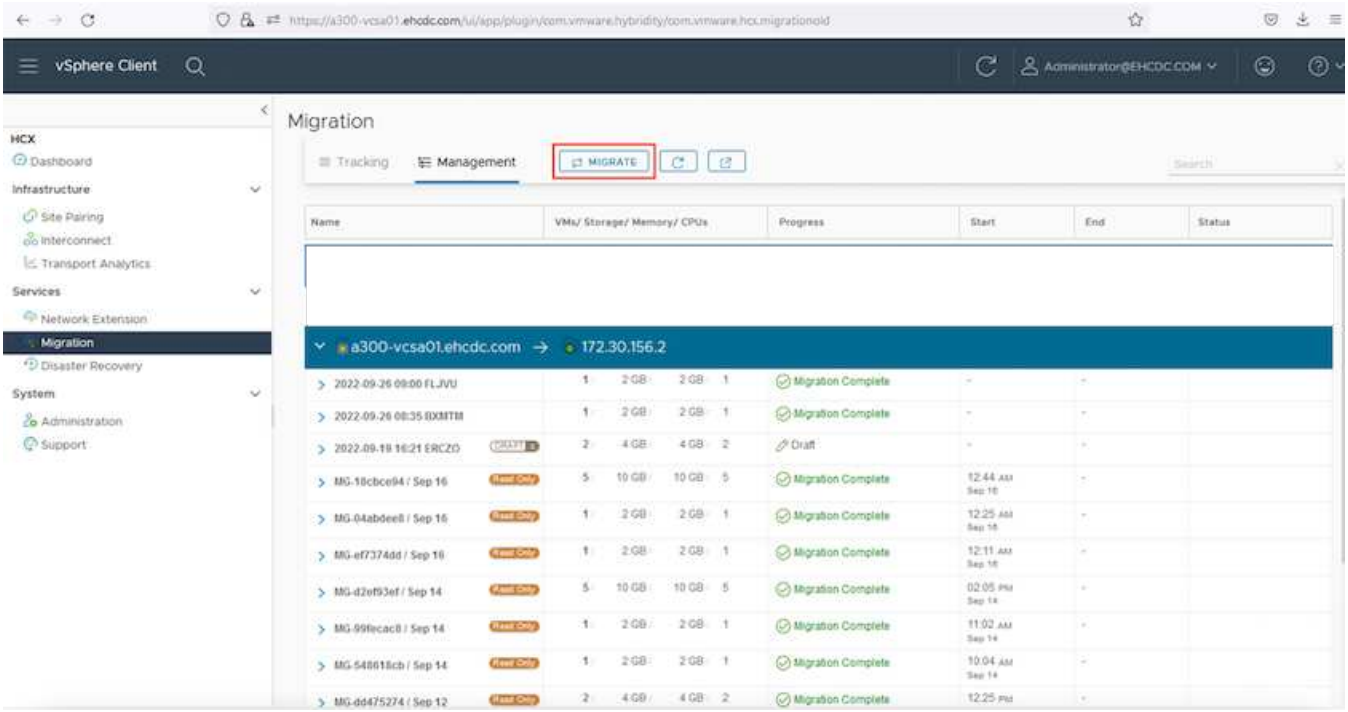
要了解有关各种 HCX 迁移机制的更多信息，请参阅 "VMware HCX 迁移类型"。

批量迁移

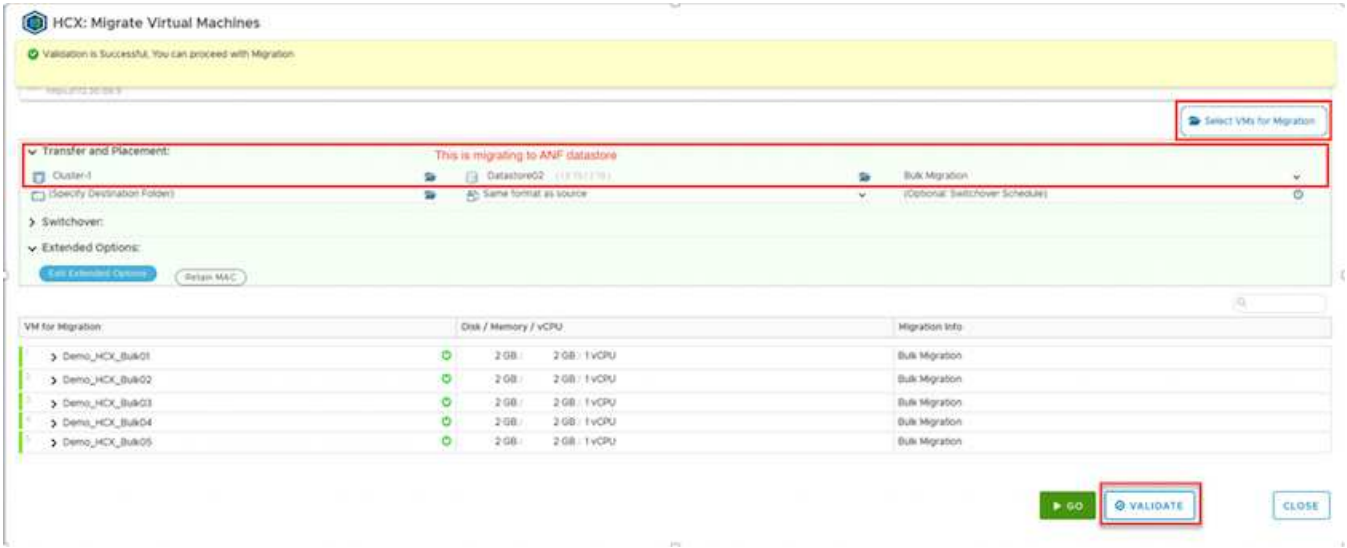
本节详细介绍批量迁移机制。在批量迁移期间，HCX 的批量迁移功能使用 vSphere Replication 迁移磁盘文件，同时在目标 vSphere HCX 实例上重新创建虚拟机。

要启动批量虚拟机迁移，请完成以下步骤：

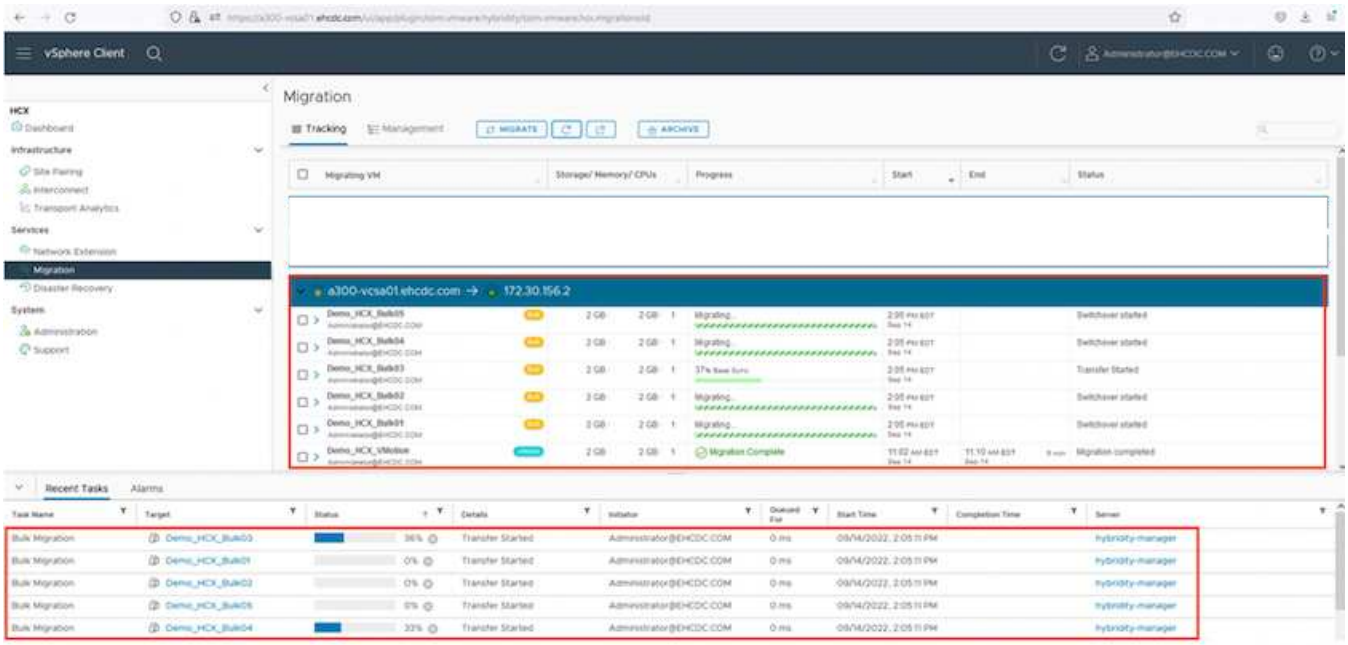
1. 访问“服务 > 迁移”下的“迁移”选项卡。



1. 在*远程站点连接*下，选择远程站点连接并选择源和目标。在此示例中，目标是 Azure VMware 解决方案 SDDC HCX 终结点。
2. 单击“选择要迁移的虚拟机”。这提供了所有本地虚拟机的列表。根据匹配：值表达式选择虚拟机，然后单击*添加*。
3. 在“传输和放置”部分中，更新必填字段（“集群*”、“存储*”、“目标*”和“网络*”），包括迁移配置文件，然后单击“验证”。

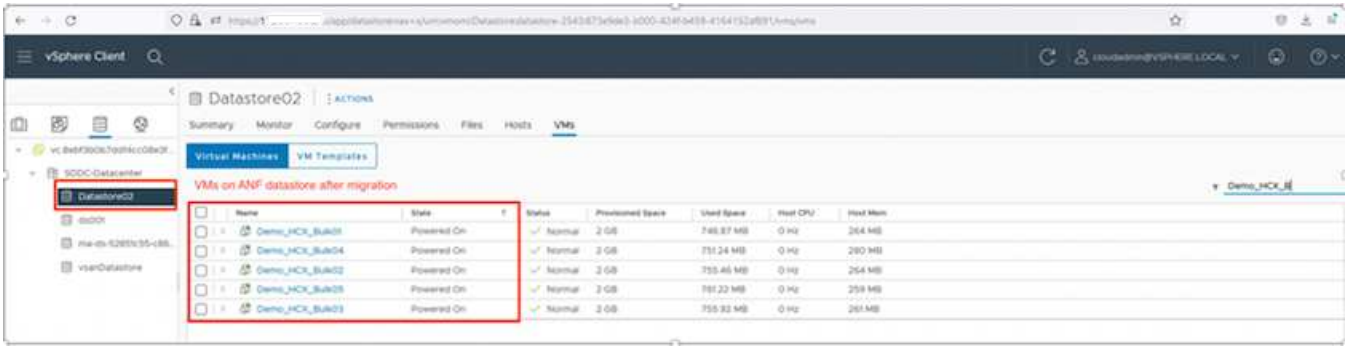


1. 验证检查完成后，单击“开始”以启动迁移。



在此迁移期间，将在目标 vCenter 内的指定Azure NetApp Files数据存储上创建一个占位磁盘，以便将源 VM 磁盘的数据复制到占位磁盘。 HBR 触发与目标的完全同步，在基线完成后，根据恢复点目标 (RPO) 周期执行增量同步。全量/增量同步完成后，除非设置特定的计划，否则会自动触发切换。

1. 迁移完成后，通过访问目标 SDDC vCenter 进行验证。

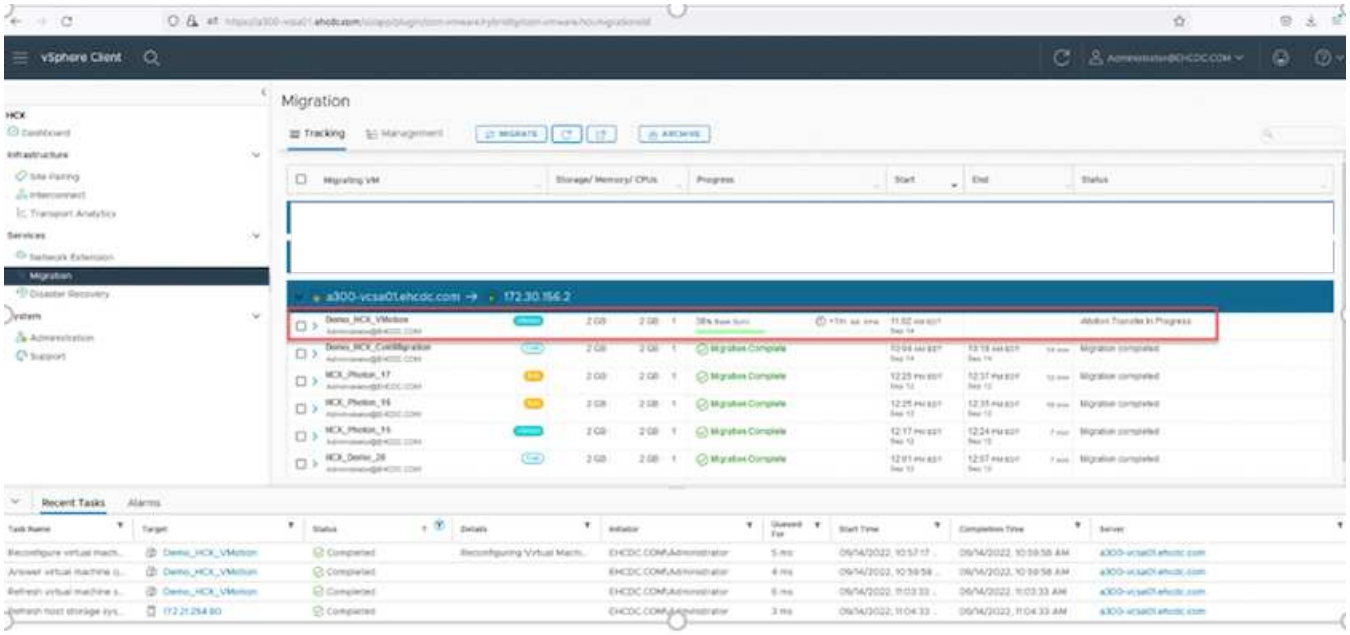


有关各种迁移选项以及如何使用 HCX 将工作负载从本地迁移到 Azure VMware 解决方案的更多详细信息，请参阅 "VMware HCX 迁移注意事项"。

要了解有关此过程的更多信息，请观看以下视频：

使用 HCX 进行工作负载迁移

这是 HCX vMotion 选项的屏幕截图。



要了解有关此过程的更多信息，请观看以下视频：

HCX vMotion

确保有足够的带宽来处理迁移。

目标 ANF 数据存储应具有足够的空间来处理迁移。

结束语

无论您的目标是全云还是混合云，以及驻留在本地任何类型/供应商存储上的数据， Azure NetApp Files和 HCX 都提供了部署和迁移应用程序工作负载的绝佳选择，同时通过使数据需求无缝连接到应用程序层来降低 TCO。无论用例如何，选择 Azure VMware 解决方案以及Azure NetApp Files都可以快速实现云优势、跨本地和多个云的一致基础架构和操作、工作负载的双向可移植性以及企业级容量和性能。使用 VMware vSphere Replication、VMware vMotion 甚至网络文件复制 (NFC) 连接存储和迁移虚拟机所使用的过程和程序相同。

总结

该文件的要点包括：

- 现在可以将Azure NetApp Files用作 Azure VMware 解决方案 SDDC 上的数据存储。
- 您可以轻松地将数据从本地迁移到Azure NetApp Files数据存储。
- 您可以轻松扩大或缩小Azure NetApp Files数据存储以满足迁移活动期间的容量和性能要求。

在哪里可以找到更多信息

要了解有关本文档中描述的信息的更多信息，请参阅以下网站链接：

- Azure VMware 解决方案文档

"https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files文档

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- VMware HCX 迁移注意事项

"https://learn.microsoft.com/en-us/azure/azure-vmware/architecture-migrate"

NetApp适用于 GCP/GCVE

NetApp针对 Google Cloud Platform GCVE 的功能

详细了解NetApp为 Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) 带来的功能 - 从NetApp作为来宾连接存储设备或补充 NFS 数据存储到迁移工作流、扩展/爆发到云、备份/恢复和灾难恢复。

通过选择以下选项跳转到所需内容的部分：

- "在 GCP 中配置 GCVE"
- "NetApp的 GCVE 存储选项"
- "NetApp /VMware 云解决方案"

在 GCP 中配置 GCVE

与本地一样，规划基于云的虚拟化环境对于成功创建虚拟机和迁移的生产就绪环境至关重要。

本节介绍如何设置和管理 GCVE，以及如何将其与可用于连接NetApp存储的选项结合使用。

> 客户机内存储是将Cloud Volumes ONTAP和Google Cloud NetApp Volumes连接到 GCVE 的唯一支持方法。

设置过程可分为以下步骤：

- 部署和配置 GCVE
- 启用对 GCVE 的私人访问

查看详细信息"GCVE 的配置步骤"。

NetApp的 GCVE 存储选项

NetApp存储在 GCP GCVE 中可以以多种方式使用 - 既可以作为猜测连接，也可以作为补充 NFS 数据存储。

请访问"支持的NetApp存储选项"了解更多信息。

Google Cloud 支持以下配置的NetApp存储：

- Cloud Volumes ONTAP (CVO) 作为来宾连接存储
- Google Cloud NetApp Volumes （NetApp Volumes）作为来宾连接存储

- Google Cloud NetApp Volumes （NetApp Volumes）作为补充 NFS 数据存储

查看详细信息"GCVE 的来宾连接存储选项"。查看详细信息"GCVE 的补充 NFS 数据存储选项"。

阅读更多"Google Cloud NetApp Volumes数据存储区支持 Google Cloud VMware Engine（NetApp博客）"或者"如何将Google Cloud NetApp Volumes用作 Google Cloud VMware Engine 的数据存储区（Google 博客）"

解决方案用例

借助NetApp和 VMware 云解决方案，许多用例都可以在 Azure AVS 中轻松部署。针对 VMware 定义的每个云区域都定义了这些用例：

- 保护（包括灾难恢复和备份/还原）
- 延长
- 迁移

"浏览适用于 Google Cloud GCVE 的NetApp解决方案"

保护 **GCP/GCVE** 上的工作负载

使用**NetApp SnapCenter**和 **Veeam Replication** 实现应用程序一致性灾难恢复

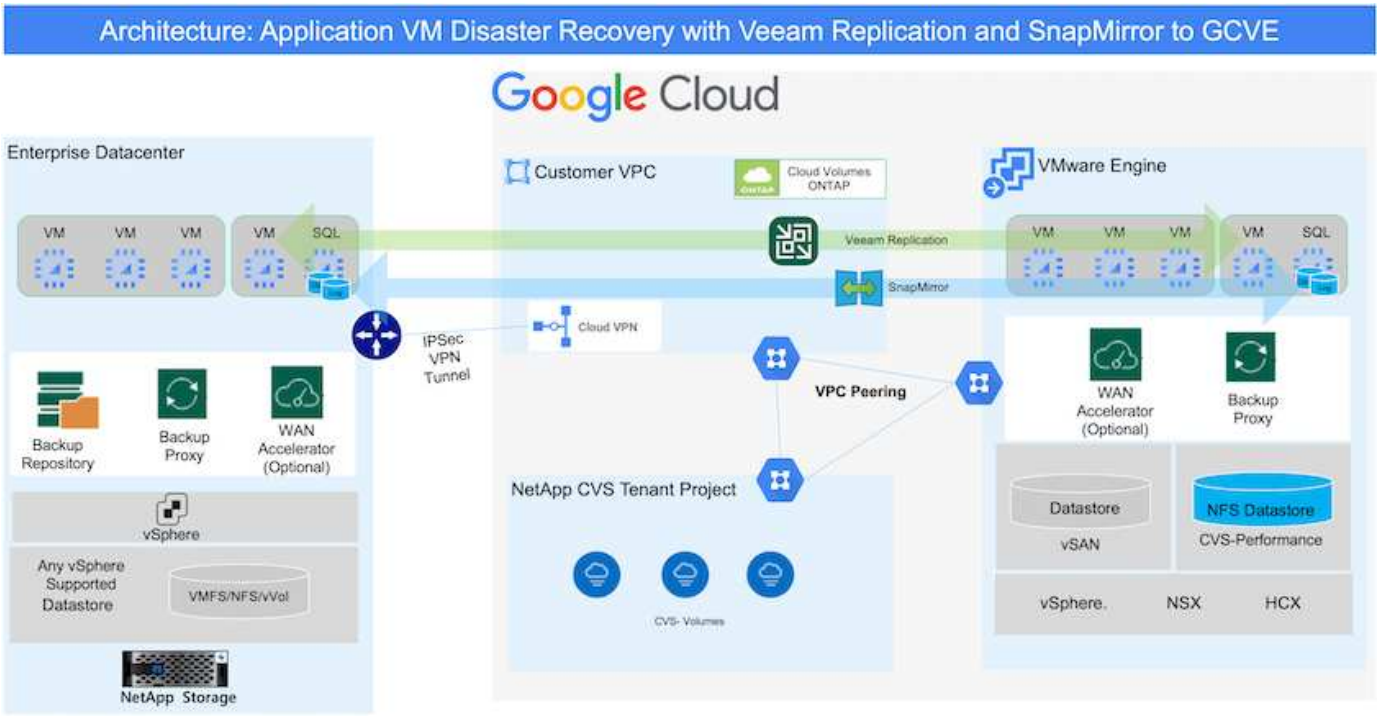
云端灾难恢复是一种具有弹性且经济高效的方法，可以保护工作负载免受站点中断和勒索软件等数据损坏事件的影响。借助NetApp SnapMirror，使用来宾连接存储的本地 VMware 工作负载可以复制到在 Google Cloud 中运行的NetApp Cloud Volumes ONTAP 。

概述

许多客户正在为托管在 VMware vSphere 上的应用程序虚拟机寻找有效的灾难恢复解决方案。他们中的许多人使用现有的备份解决方案在灾难期间进行恢复。很多时候，该解决方案会增加 RTO 并且无法满足他们的期望。为了减少 RPO 和 RTO，只要有网络连接和具有适当权限的环境，就可以利用 Veeam VM 复制，甚至可以从本地到 GCVE。注意：Veeam VM Replication 不保护 VM 客户机连接的存储设备，如客户机 VM 内的 iSCSI 或 NFS 挂载。需要单独保护它们。

为了实现 SQL VM 的应用程序一致性复制并减少 RTO，我们使用SnapCenter来协调 SQL 数据库和日志卷的 SnapMirror 操作。

本文档提供了使用NetApp SnapMirror、Veeam 和 Google Cloud VMware Engine (GCVE) 设置和执行灾难恢复的分步方法。



假设

本文档重点介绍应用程序数据的客户机内存储（也称为客户机连接），我们假设本地环境使用SnapCenter进行应用程序一致性备份。

本文档适用于任何第三方备份或恢复解决方案。根据环境中使用的解决方案，遵循最佳实践来创建符合组织 SLA 的备份策略。

对于本地环境和 Google Cloud 网络之间的连接，请使用专用互连或 Cloud VPN 等连接选项。应根据内部部署 VLAN 设计来创建段。

将本地数据中心连接到 Google Cloud 有多种选择，因此我们无法在本文档中概述特定的工作流程。请参阅 Google Cloud 文档，了解适当的本地到 Google 连接方法。

部署灾难恢复解决方案

解决方案部署概述

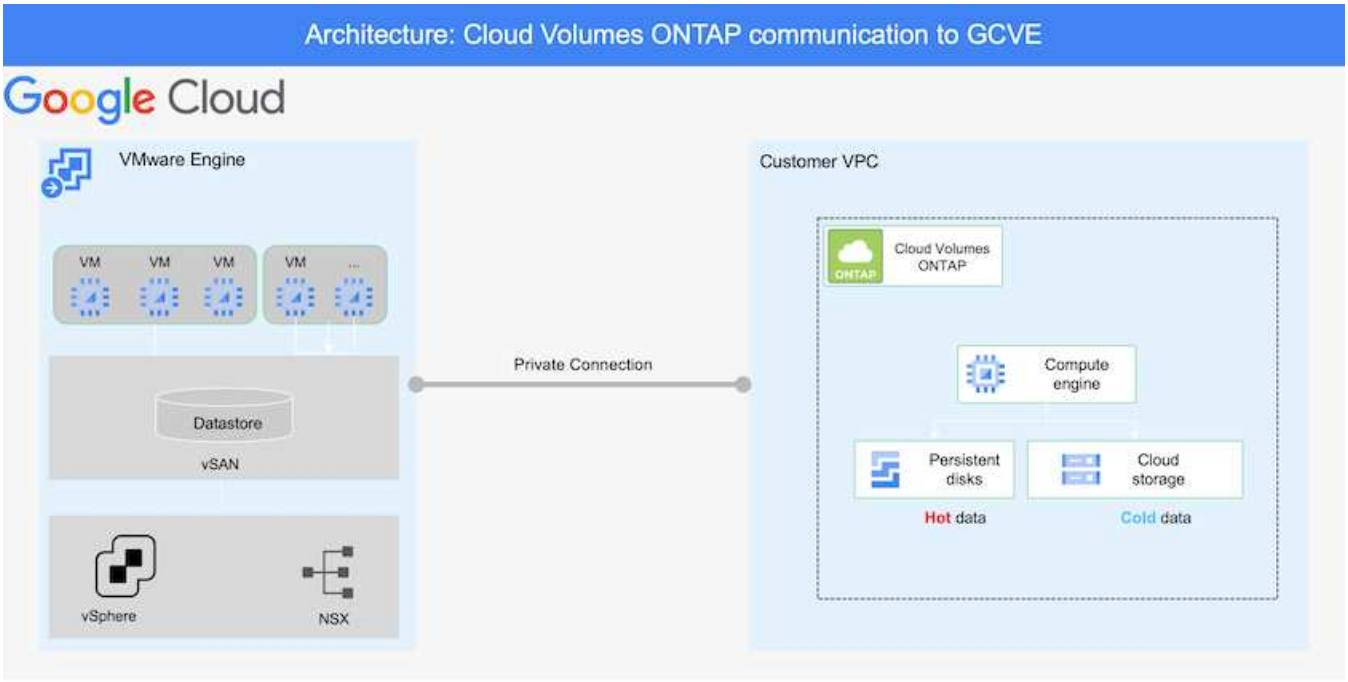
1. 确保使用SnapCenter备份应用程序数据并满足必要的 RPO 要求。
2. 使用 NetApp Console 在适当的订阅和虚拟网络中配置具有正确实例大小的 Cloud Volumes ONTAP
   a. 为相关应用程序卷配置SnapMirror 。
   b. 更新SnapCenter中的备份策略以在计划的作业之后触发SnapMirror更新。
3. 安装 Veeam 软件并开始将虚拟机复制到 Google Cloud VMware Engine 实例。
4. 在发生灾难事件时，使用 NetApp Console 中断 SnapMirror 关系，并使用 Veeam 触发虚拟机的故障转移。
   a. 重新连接应用程序虚拟机的 ISCSI LUN 和 NFS 挂载。
   b. 在网上启动应用程序。

5. 主站点恢复后，通过反向重新同步SnapMirror调用故障回复到受保护站点。

部署详情

▼ 在 **Google Cloud** 上配置 **CVO** 并将卷复制到 **CVO**

第一步是在 Google Cloud 上配置Cloud Volumes ONTAP （"克沃") 并以所需的频率和快照保留将所需的卷复制到Cloud Volumes ONTAP 。



有关设置SnapCenter和复制数据的示例分步说明，请参阅"使用SnapCenter设置复制"

使用SnapCenter审查 SQL VM 保护

▼ 配置 **GCVE** 主机和 **CVO** 数据访问

部署 SDDC 时需要考虑的两个重要因素是 GCVE 解决方案中 SDDC 集群的大小以及保持 SDDC 服务的时间。灾难恢复解决方案的这两个关键考虑因素有助于降低总体运营成本。 SDDC 最小可以只有三台主机，最大可以达到全面部署的多主机集群。

Google Cloud NetApp Volumes for NFS 数据存储区和Cloud Volumes ONTAP for SQL 数据库和日志可以部署到任何 VPC，并且 GCVE 应该具有与该 VPC 的私有连接以挂载 NFS 数据存储区并让 VM 连接到 iSCSI LUN。

要配置 GCVE SDDC，请参阅"在 Google Cloud Platform (GCP) 上部署和配置虚拟化环境"。作为先决条件，请验证在建立连接后，驻留在 GCVE 主机上的客户虚拟机是否能够使用来自Cloud Volumes ONTAP的数据。

正确配置Cloud Volumes ONTAP和 GCVE 后，开始配置 Veeam，使用 Veeam 复制功能自动将本地工作负载恢复到 GCVE（具有应用程序 VMDK 的虚拟机和具有来宾内存储的虚拟机），并利用SnapMirror将应用程序卷复制到Cloud Volumes ONTAP。

▼ 安装 **Veeam** 组件

根据部署场景，需要部署Veeam备份服务器、备份存储库和备份代理。对于这种用例，不需要为 Veeam 部署对象存储，也不需要 Scale-out 存储

库。https://helpcenter.veeam.com/docs/backup/vsphere/replication_components.html?ver=120["有关安装过程，请参阅 Veeam 文档"]欲了解更多信息，请参阅"使用 Veeam Replication 进行迁移"

▼ 使用 **Veeam** 设置虚拟机复制

本地 vCenter 和 GCVE vCenter 都需要在 Veeam 中注册。 "设置 vSphere VM 复制作业"在向导的客户机处理步骤中，选择禁用应用程序处理，因为我们将利用SnapCenter进行应用程序感知备份和恢复。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

▼ **Microsoft SQL Server VM** 的故障转移

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

此解决方案的优势

- 使用SnapMirror的高效且有弹性的复制。
- 通过ONTAP快照保留恢复到任何可用的时间点。
- 从存储、计算、网络和应用程序验证步骤，恢复数百到数千台虚拟机所需的所有步骤均可实现完全自动化。
- SnapCenter使用不会改变复制卷的克隆机制。
  - 这避免了卷和快照数据损坏的风险。
  - 避免 DR 测试工作流程期间的复制中断。
  - 利用 DR 数据进行 DR 以外的工作流程，例如开发/测试、安全测试、补丁和升级测试以及补救测试。
- Veeam Replication 允许在 DR 站点上更改 VM IP 地址。

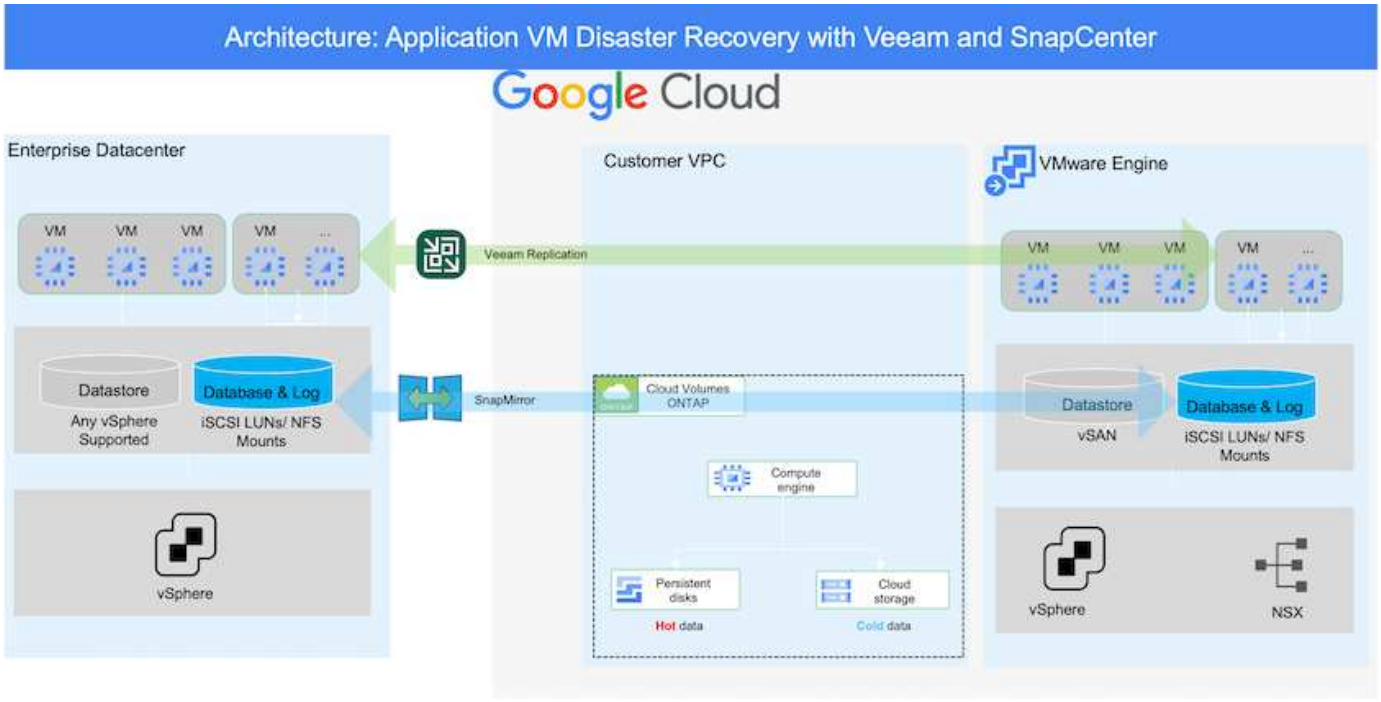
使用**SnapCenter**、 **Cloud Volumes ONTAP**和 **Veeam Replication** 实现应用程序灾难恢复

云端灾难恢复是一种具有弹性且经济高效的方法，可以保护工作负载免受站点中断和勒索软件等数据损坏事件的影响。借助NetApp SnapMirror，使用来宾连接存储的本地 VMware 工作负载可以复制到在 Google Cloud 中运行的NetApp Cloud Volumes ONTAP 。

概述

这涵盖了应用程序数据；但是，实际的虚拟机本身又如何呢？灾难恢复应涵盖所有相关组件，包括虚拟机、VMDK、应用程序数据等。为了实现此目的，可以使用SnapMirror和 Veeam 无缝恢复从本地复制到Cloud Volumes ONTAP 的工作负载，同时使用 vSAN 存储作为 VM VMDK。

本文档提供了使用NetApp SnapMirror、Veeam 和 Google Cloud VMware Engine (GCVE) 设置和执行灾难恢复的分步方法。



假设

本文档重点介绍应用程序数据的客户机内存储（也称为客户机连接），我们假设本地环境使用SnapCenter进行应用程序一致性备份。

本文档适用于任何第三方备份或恢复解决方案。根据环境中使用的解决方案，遵循最佳实践来创建符合组织 SLA 的备份策略。

对于本地环境和 Google Cloud 网络之间的连接，请使用专用互连或 Cloud VPN 等连接选项。应根据内部部署 VLAN 设计来创建段。

将本地数据中心连接到 Google Cloud 有多种选择，因此我们无法在本文档中概述特定的工作流程。请参阅 Google Cloud 文档，了解适当的本地到 Google 连接方法。

部署灾难恢复解决方案

解决方案部署概述

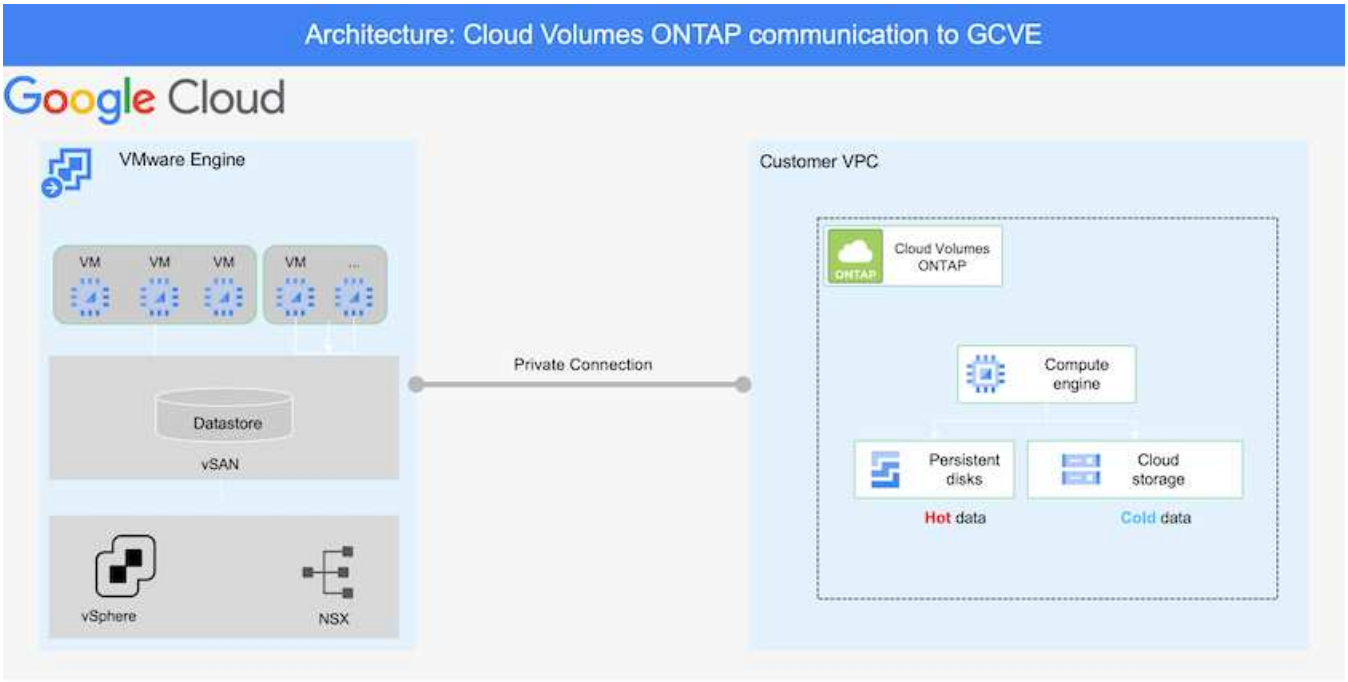
1. 确保使用SnapCenter备份应用程序数据并满足必要的 RPO 要求。
2. 使用适当的订阅和虚拟网络中的云管理器为Cloud Volumes ONTAP配置正确的实例大小。
   a. 为相关应用程序卷配置SnapMirror 。
   b. 更新SnapCenter中的备份策略以在计划的作业之后触发SnapMirror更新。
3. 安装 Veeam 软件并开始将虚拟机复制到 Google Cloud VMware Engine 实例。
4. 在灾难事件期间，使用 Cloud Manager 中断SnapMirror关系并使用 Veeam 触发虚拟机故障转移。
   a. 重新连接应用程序虚拟机的 ISCSI LUN 和 NFS 挂载。
   b. 在网上启动应用程序。

5. 主站点恢复后，通过反向重新同步SnapMirror调用故障回复到受保护站点。

部署详情

▼ 在 **Google Cloud** 上配置 **CVO** 并将卷复制到 **CVO**

第一步是在 Google Cloud 上配置Cloud Volumes ONTAP （"克沃") 并以所需的频率和快照保留将所需的卷复制到Cloud Volumes ONTAP 。



有关设置SnapCenter和复制数据的示例分步说明，请参阅"使用SnapCenter设置复制"

使用SnapCenter设置复制

▼ 配置 **GCVE** 主机和 **CVO** 数据访问

部署 SDDC 时需要考虑的两个重要因素是 GCVE 解决方案中 SDDC 集群的大小以及保持 SDDC 服务的时间。灾难恢复解决方案的这两个关键考虑因素有助于降低总体运营成本。 SDDC 最小可以只有三台主机，最大可以达到全面部署的多主机集群。

Cloud Volumes ONTAP可以部署到任何 VPC，并且 GCVE 应该与该 VPC 建立私有连接，以使 VM 连接到 iSCSI LUN。

要配置 GCVE SDDC，请参阅"在 Google Cloud Platform (GCP) 上部署和配置虚拟化环境"。作为先决条件，请验证在建立连接后，驻留在 GCVE 主机上的客户虚拟机是否能够使用来自Cloud Volumes ONTAP的数据。

正确配置Cloud Volumes ONTAP和 GCVE 后，开始配置 Veeam，使用 Veeam 复制功能自动将本地工作负载恢复到 GCVE（具有应用程序 VMDK 的虚拟机和具有来宾内存储的虚拟机），并利用SnapMirror将应用程序卷复制到Cloud Volumes ONTAP。

▼ 安装 **Veeam** 组件

根据部署场景，需要部署Veeam备份服务器、备份存储库和备份代理。对于这种用例，不需要为 Veeam 部署对象存储，也不需要 Scale-out 存储
库。https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["有关安装过程，

请参阅 Veeam 文档"]

▼ 使用 **Veeam** 设置虚拟机复制

本地 vCenter 和 GCVE vCenter 都需要在 Veeam 中注册。 "设置 vSphere VM 复制作业"在向导的客户机处理步骤中，选择禁用应用程序处理，因为我们将利用SnapCenter进行应用程序感知备份和恢复。

设置 vSphere VM 复制作业

▼ **Microsoft SQL Server VM** 的故障转移

Microsoft SQL Server VM 的故障转移

此解决方案的优势

- 使用SnapMirror的高效且有弹性的复制。
- 通过ONTAP快照保留恢复到任何可用的时间点。
- 从存储、计算、网络和应用程序验证步骤，恢复数百到数千台虚拟机所需的所有步骤均可实现完全自动化。
- SnapCenter使用不会改变复制卷的克隆机制。
  - 这避免了卷和快照数据损坏的风险。
  - 避免 DR 测试工作流程期间的复制中断。
  - 利用 DR 数据进行 DR 以外的工作流程，例如开发/测试、安全测试、补丁和升级测试以及补救测试。
- Veeam Replication 允许在 DR 站点上更改 VM IP 地址。

使用 **Veeam Replication** 和**Google Cloud NetApp Volumes**数据存储区实现 **Google Cloud VMware Engine** 的灾难恢复

在危机时刻，全面的灾难恢复计划对于企业来说至关重要。许多组织利用云计算进行日常运营和灾难恢复。这种主动的方法可以减少或消除昂贵的业务中断。

本文介绍如何使用 Veeam Backup & Replication 设置本地 VMware VM 到带有Google Cloud NetApp Volumes (NetApp Volumes) 的 Google Cloud VMware Engine (GCVE) 的灾难恢复。

概述

Google Cloud NetApp Volumes是 Google 和NetApp推出的一项存储服务，可用于 Google Cloud。 NetApp Volumes 服务提供高性能 NFS/SMB 存储。 VMware 认证的NetApp Volumes NFS 存储可用作 GCVE 中 ESXi 主机的外部数据存储。用户需要在其 GCVE 私有云和NetApp Volumes 项目之间建立对等连接。区域内的存储访问不产生任何网络费用。用户可以在 Google Cloud 控制台中创建NetApp Volumes 卷，并在将卷作为数据存储区挂载到其 ESXi 主机之前启用删除保护。

基于NetApp Volumes 的 NFS 数据存储区可用于使用任何经过验证且提供 VM 复制功能的第三方解决方案从本地复制数据。通过添加NetApp Volumes 数据存储，可以实现成本优化部署，而无需构建基于 Google Cloud VMware Engine (GCVE) 的 SDDC 并使用大量 ESXi 主机来容纳存储。这种方法被称为“Pilot Light Cluster”。试点灯集群是最小 GCVE 主机配置（3 x GCVE ESXi 主机）以及NetApp Volumes 数据存储容量，以允许独立扩展以满足容量要求。

目标是仅使用管理故障转移的核心组件来维持具有成本效益的基础设施。在发生故障转移时，指示灯集群可以扩展并添加更多 GCVE 主机。一旦故障转移得到解决并且恢复正常运行，指示灯集群就可以缩小规模，返回到低成本的运行模式。

本文件的目的

本文介绍如何使用Google Cloud NetApp Volumes数据存储和 Veeam Backup & Replication 来设置本地 VMware VM 到 GCVE 的灾难恢复（使用 Veeam VM 复制软件功能）。

Veeam Backup & Replication 是一款用于虚拟环境的备份和复制应用程序。当虚拟机被复制时，Veeam Backup & Replication 将在目标 GCVE SDDC 集群上以原生 VMware vSphere 格式创建虚拟机的精确副本。 Veeam Backup & Replication 将使副本与原始 VM 保持同步。复制提供了最佳的恢复时间目标 (RTO)，因为 DR 站点上有一个处于准备启动状态的 VM 的安装副本。

这种复制机制确保在发生灾难事件时工作负载能够在 GCVE 中快速启动。 Veeam Backup & Replication 软件还优化了通过 WAN 和慢速连接进行复制的流量传输。此外，它还过滤掉重复的数据块、零数据块、交换文件和“排除的 VM 客户操作系统文件”。该软件还将压缩副本流量。为了防止复制作业消耗整个网络带宽，可以利用 WAN 加速器和网络限制规则。

Veeam Backup & Replication 中的复制过程由作业驱动，这意味着复制是通过配置复制作业来执行的。如果发生灾难事件，可以触发故障转移，通过故障转移到其副本来恢复虚拟机。当执行故障转移时，复制的虚拟机将接管原始虚拟机的角色。可以执行故障转移至副本的最新状态或任何已知的良好还原点。这使得勒索软件恢复或隔离测试能够根据需要进行。 Veeam Backup & Replication 提供多种选项来处理不同的灾难恢复场景。

解决方案概述

该解决方案涵盖以下高级步骤：

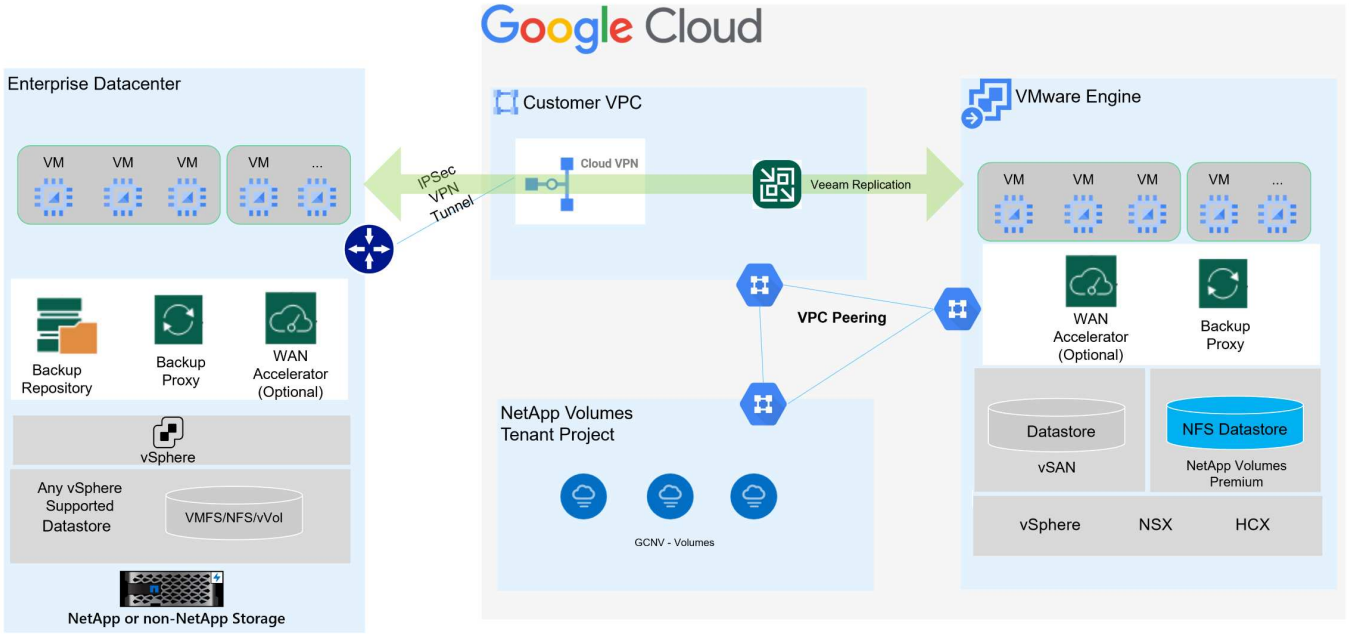
1. 使用Google Cloud NetApp Volumes创建 NFS 卷
2. 按照 GCP 流程从NetApp Volumes NFS 卷创建 GCVE 数据存储。
3. 设置复制作业以使用 Veeam Backup & Replication 创建 VM 副本。
4. 创建故障转移计划并执行故障转移。
5. 灾难事件结束且主站点启动后，切换回生产虚拟机。

> 在NetApp Volumes 中创建卷作为 GCVE 数据存储时，仅支持 NFS v3。

有关使用NetApp Volumes NFS 卷作为 GCVE 数据存储的更多信息，请查看 "使用 NFS 卷作为由Google Cloud NetApp Volumes托管的 vSphere 数据存储"。

架构

下图显示了本文档中提出的解决方案的架构。建议的最佳实践是在本地站点和 GCVE SDDC 中都安装一个 Veeam Backup & Replication 服务器。备份和恢复由内部部署的 Veeam 服务器执行和管理，复制由 GCVE SDDC 中的 Veeam 服务器管理。当主数据中心发生故障时，此架构可提供最高的可用性。



Veeam 复制到 **GCVE** 和**NetApp Volumes** 数据存储区的先决条件

此解决方案需要以下组件和配置：

1. NetApp Volumes 有一个可用的存储池，具有足够的可用容量来容纳要创建的 NFS 卷。
2. Veeam Backup and Replication 软件在具有适当网络连接的本地环境中运行。
3. 确保 Veeam Backup & Replication 备份 VM 连接到源以及目标 GCVE SDDC 集群。
4. 确保 Veeam Backup & Replication 备份 VM 连接到源和目标 GCVE 集群上的 Veeam 代理服务器 VM。
5. 备份服务器必须能够解析短名称并连接到源 vCenter 和目标 vCenter。

用户需要使用 VMware Engine Cloud 控制台 UI 中的 VPC 网络对等或私有连接页面在其 GCVE 私有云和NetApp Volumes 项目之间建立对等连接。

> 将 GCVE vCenter 服务器添加到 Veeam Backup and Replication 清单时，Veeam 需要具有提升权限的 GCVE 解决方案用户帐户。有关详细信息，请参阅 Google Cloud Platform (GCP) 文档，"提升 VMware Engine 权限"。

有关更多信息，请参阅 "注意事项和限制"在 Veeam Backup & Replication 文档中。

部署步骤

以下部分概述了使用Google Cloud NetApp Volumes创建和挂载 NFS 数据存储的部署步骤，以及使用 Veeam Backup and Replication 在本地数据中心和 Google Cloud VMware Engine 之间实施完整灾难恢复解决方案的步骤。

为 **GCVE** 创建**NetApp Volumes NFS** 卷和数据存储

参考 "使用 NFS 卷作为由Google Cloud NetApp Volumes托管的 vSphere 数据存储"了解如何将Google Cloud NetApp Volumes作为 GCVE 的数据存储的概述。

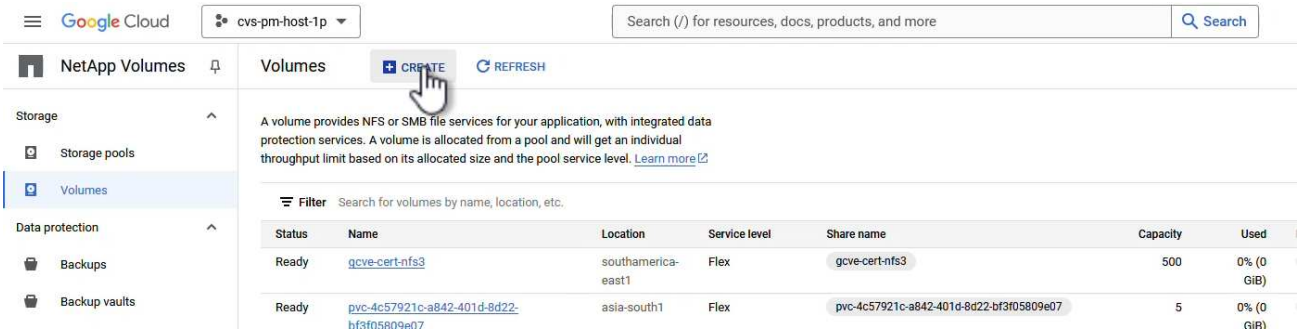
完成以下步骤以使用NetApp Volumes 为 GCVE 创建和使用 NFS 数据存储：

▼ 创建**NetApp Volumes NFS** 卷

可从 Google Cloud Platform (GCP) 控制台访问Google Cloud NetApp Volumes 。

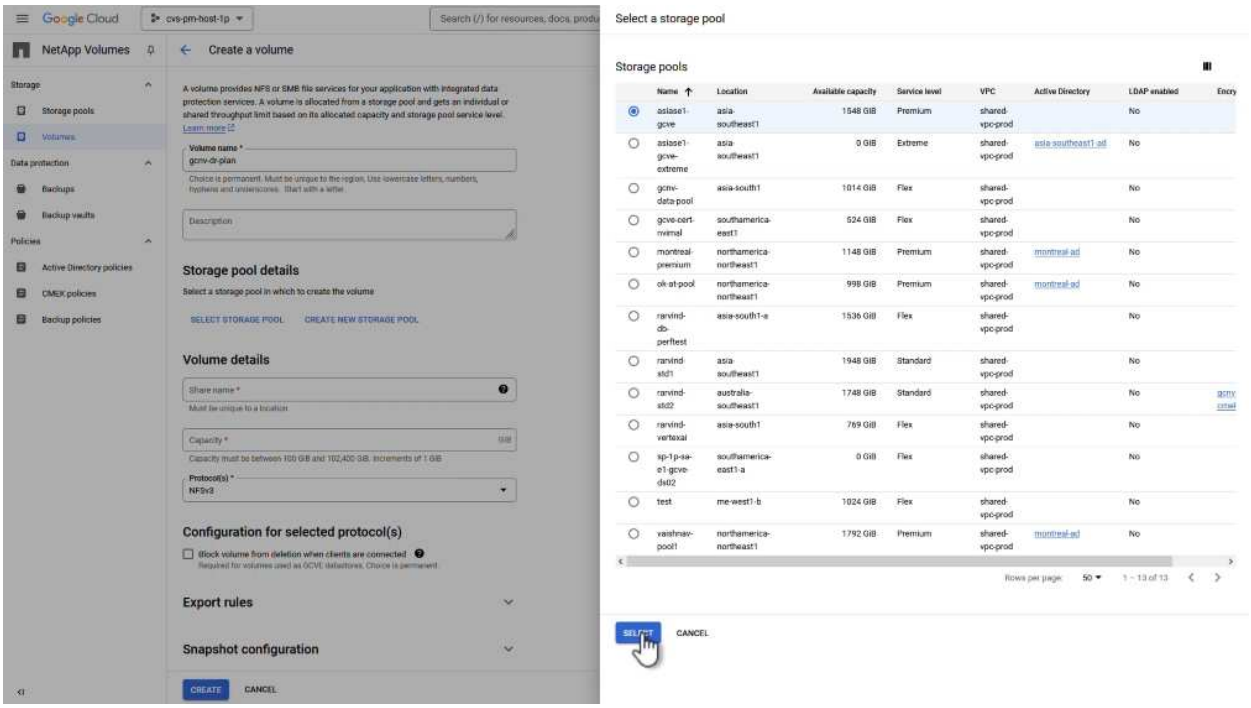
参考 "创建卷"有关此步骤的详细信息，请参阅Google Cloud NetApp Volumes文档。

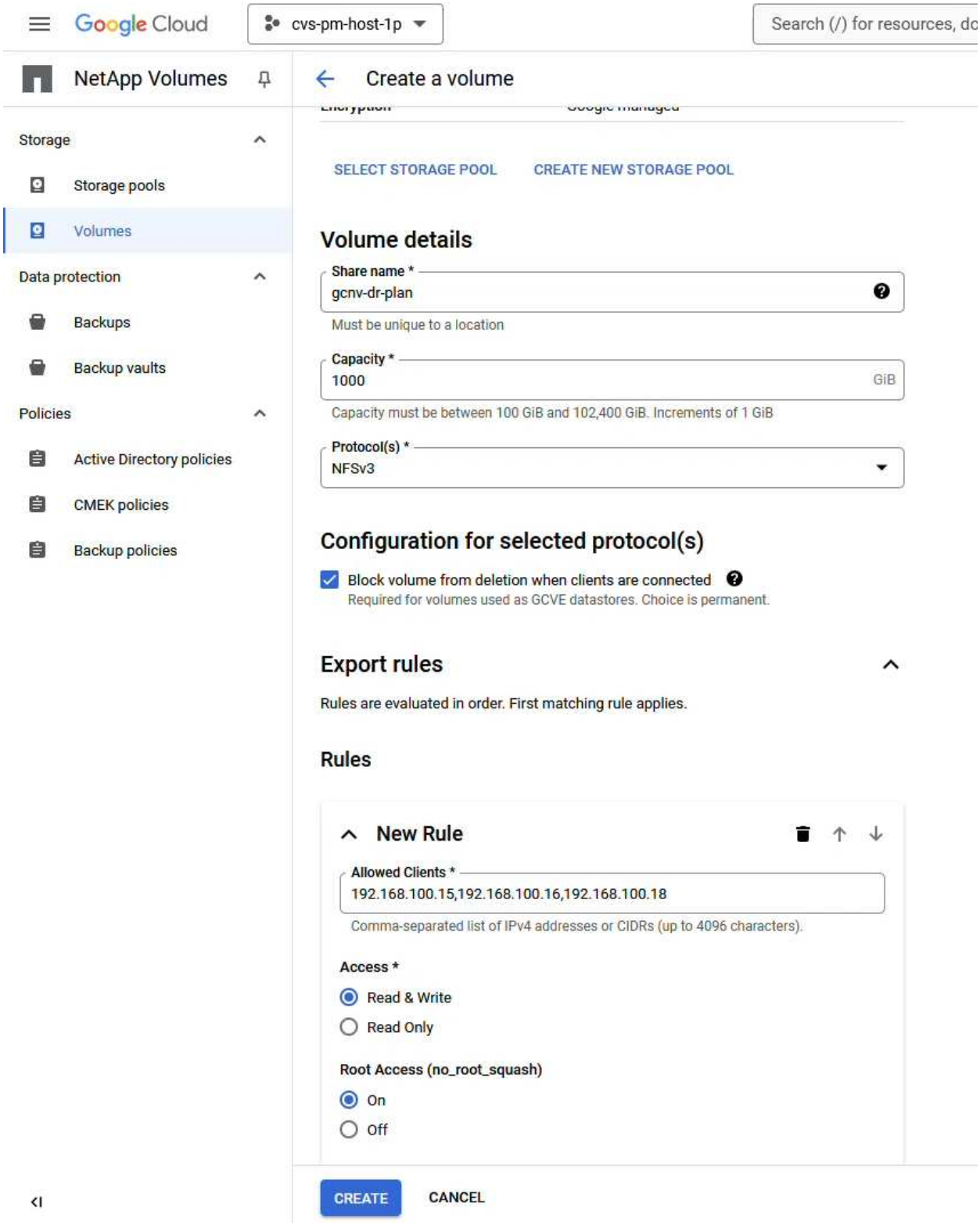
1. 在 Web 浏览器中，导航至 https://console.cloud.google.com/并登录您的 GCP 控制台。搜索 * NetApp Volumes* 开始。
2. 在* NetApp Volumes* 管理界面中，单击* Create* 开始创建 NFS 卷。



3. 在“创建卷”向导中，填写所有必需的信息：
   - 卷的名称。
   - 创建卷的存储池。
   - 挂载 NFS 卷时使用的共享名称。
   - 卷的容量（以 GiB 为单位）。
   - 要使用的存储协议。
   - 选中该框以*客户端连接时阻止删除卷*（GCVE 作为数据存储安装时需要）。
   - 访问卷的导出规则。这是 NFS 网络上 ESXi 适配器的 IP 地址。
   - 用于使用本地快照保护卷的快照计划。
   - 或者，选择备份卷和/或为卷创建标签。

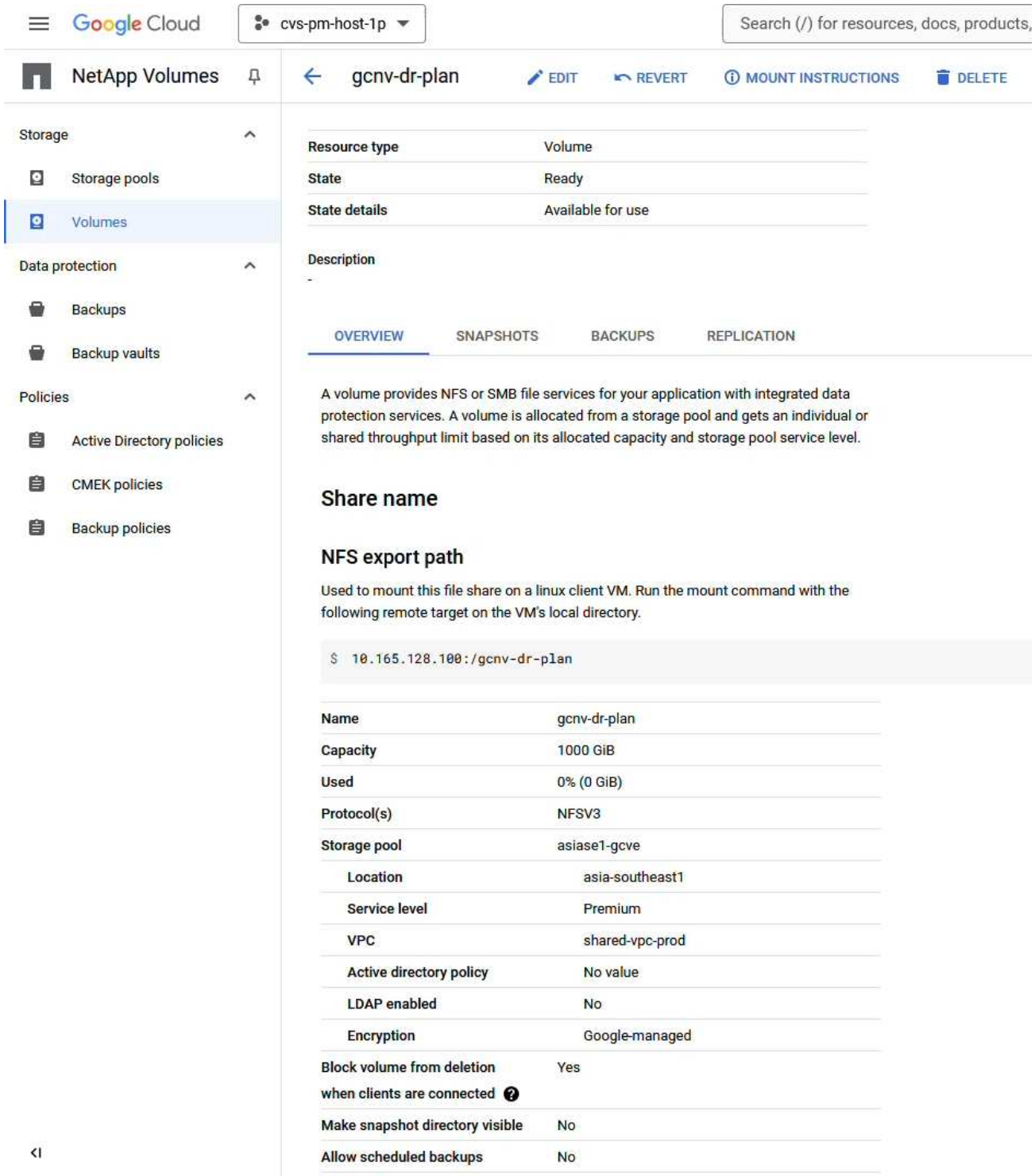
   在NetApp Volumes 中创建卷作为 GCVE 数据存储时，仅支持 NFS v3。


Google Cloud
cvs-pm-host-1p
Search (/) for resources, docs, produ
NetApp Volumes
Create a volume
Storage
Storage pools
Volumes
Data protection
Backups
Backup vaults
Policies
Active Directory policies
CMEK policies
Backup policies
A volume provides NFS or SMB file services for your application with integrated data protection services. A volume is allocated from a storage pool and gets an individual or shared throughput limit based on its allocated capacity and storage pool service level.
Learn more
Volume name *
gcnv-dr-plan
Choice is permanent. Must be unique to the region. Use lowercase letters, numbers, hyphens and underscores. Start with a letter.
Description
Storage pool details
Select a storage pool in which to create the volume
SELECT STORAGE POOL
CREATE NEW STORAGE POOL
Volume details
Share name *
Must be unique to a location
Capacity *
GiB
Capacity must be between 100 GiB and 102,400 GiB. Increments of 1 GiB
Protocol(s) *
NFSv3
Configuration for selected protocol(s)
Block volume from deletion when clients are connected
Required for volumes used as GCVE datastores. Choice is permanent.
Export rules
Snapshot configuration
CREATE
CANCEL
Select a storage pool
Storage pools
Name
Location
Available capacity
Service level
VPC
Active Directory
LDAP enabled
Encry
asiase1-gcve
asia-southeast1
1548 GiB
Premium
shared-vpc-prod
No
asiase1-gcve-extreme
asia-southeast1
0 GiB
Extreme
shared-vpc-prod
asia-southeast1-ad
No
gcnv-data-pool
asia-south1
1014 GiB
Flex
shared-vpc-prod
No
gcve-cert-nvmal
southamerica-east1
524 GiB
Flex
shared-vpc-prod
No
montreal-premium
northamerica-northeast1
1148 GiB
Premium
shared-vpc-prod
montreal-ad
No
ok-at-pool
northamerica-northeast1
998 GiB
Premium
shared-vpc-prod
montreal-ad
No
ranvind-db-perftest
asia-south1-a
1536 GiB
Flex
shared-vpc-prod
No
ranvind-std1
asia-southeast1
1948 GiB
Standard
shared-vpc-prod
No
ranvind-std2
australia-southeast1
1748 GiB
Standard
shared-vpc-prod
No
gcnv cmek
ranvind-vertexai
asia-south1
769 GiB
Flex
shared-vpc-prod
No
sp-1p-sa-e1-gcve-ds02
southamerica-east1-a
0 GiB
Flex
shared-vpc-prod
No
test
me-west1-b
1024 GiB
Flex
shared-vpc-prod
No
vaishnav-pool1
northamerica-northeast1
1792 GiB
Premium
shared-vpc-prod
montreal-ad
No
Rows per page: 50
1 – 13 of 13
SELECT
CANCEL



单击“创建”以完成卷的创建。

4. 一旦创建了卷，就可以从卷的属性页面查看挂载卷所需的 NFS 导出路径。



▼ 在 **GCVE** 中挂载 **NFS** 数据存储

在撰写本文时，在 GCVE 中挂载数据存储的过程需要打开 GCP 支持票证才能将卷挂载为 NFS 数据存储。

参考 "使用 NFS 卷作为由Google Cloud NetApp Volumes托管的 vSphere 数据存储"了解更多信息。

将虚拟机复制到 **GCVE** 并执行故障转移计划和故障回复

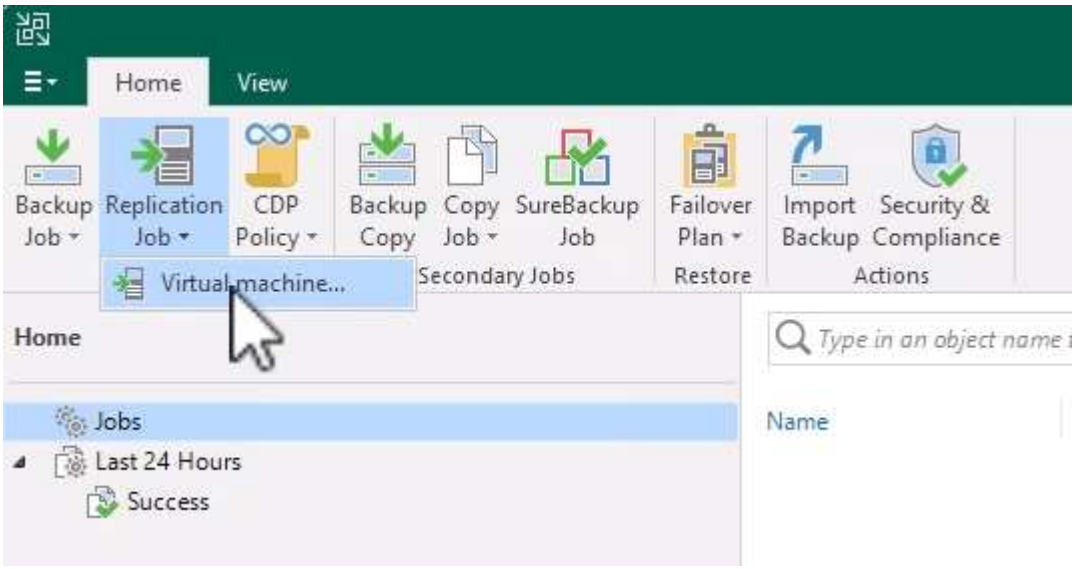
▼ 将虚拟机复制到 **GCVE** 中的 **NFS** 数据存储

Veeam Backup & Replication 在复制期间利用 VMware vSphere 快照功能，Veeam Backup & Replication 请

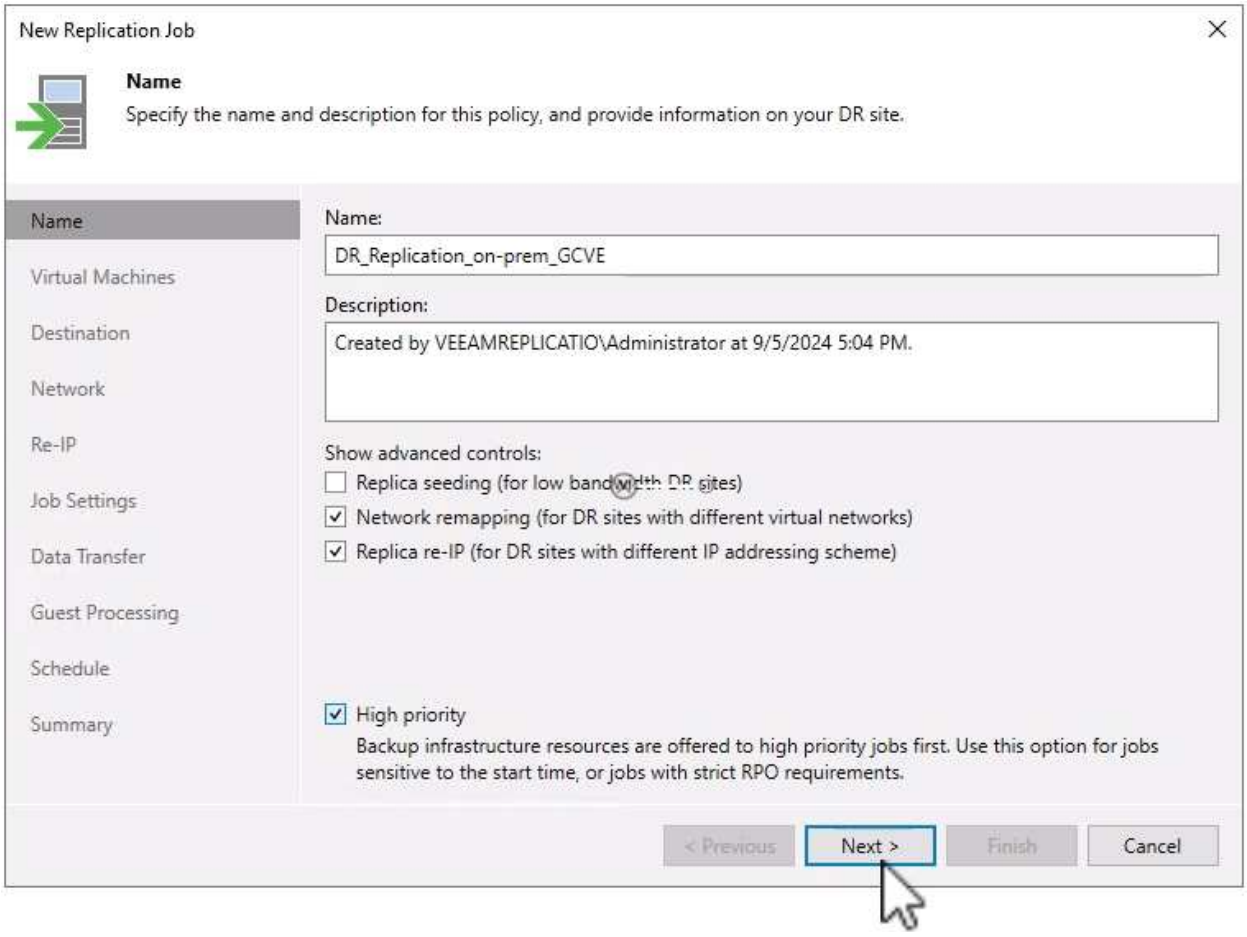
求 VMware vSphere 创建 VM 快照。 VM 快照是 VM 的时间点副本，其中包括虚拟磁盘、系统状态、配置和元数据。 Veeam Backup & Replication 使用快照作为复制的数据源。

要复制虚拟机，请完成以下步骤：

1. 打开 Veeam 备份和复制控制台。
2. 在“主页”选项卡上，单击“复制作业”>“虚拟机…”

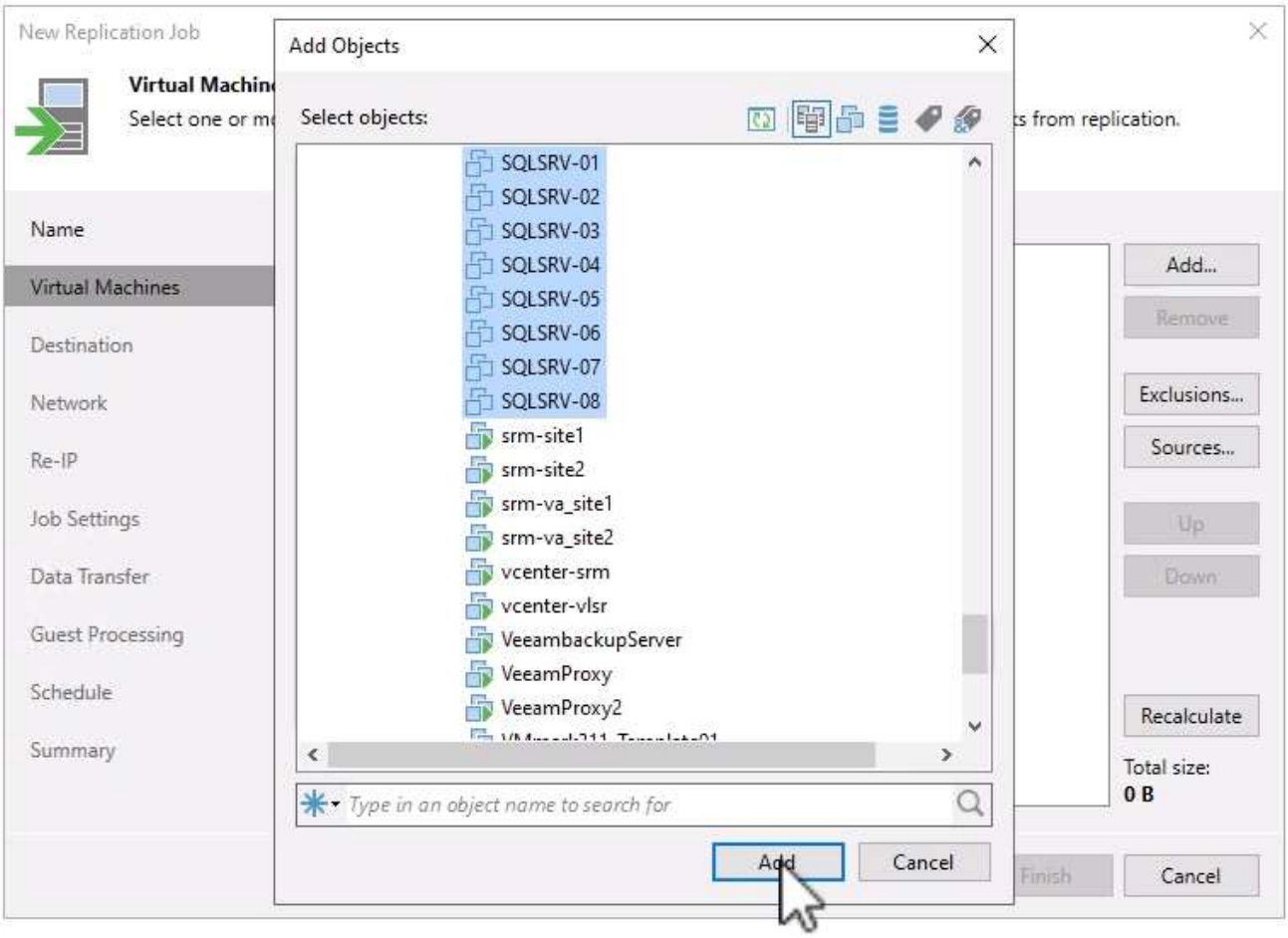


3. 在“新建复制作业”向导的“名称”页面上，指定作业名称并选择适当的高级控制复选框。
   - 如果本地和 GCP 之间的连接带宽受限，请选中“副本播种”复选框。
   - 如果 GCVE SDDC 上的段与本地站点网络的段不匹配，请选中网络重新映射（针对具有不同网络的 GCVE SDDC 站点）复选框。
   - 如果本地生产站点中的 IP 寻址方案与目标 GCVE 站点中的方案不同，请选中副本重新 IP（适用于具有不同 IP 寻址方案的 DR 站点）复选框。

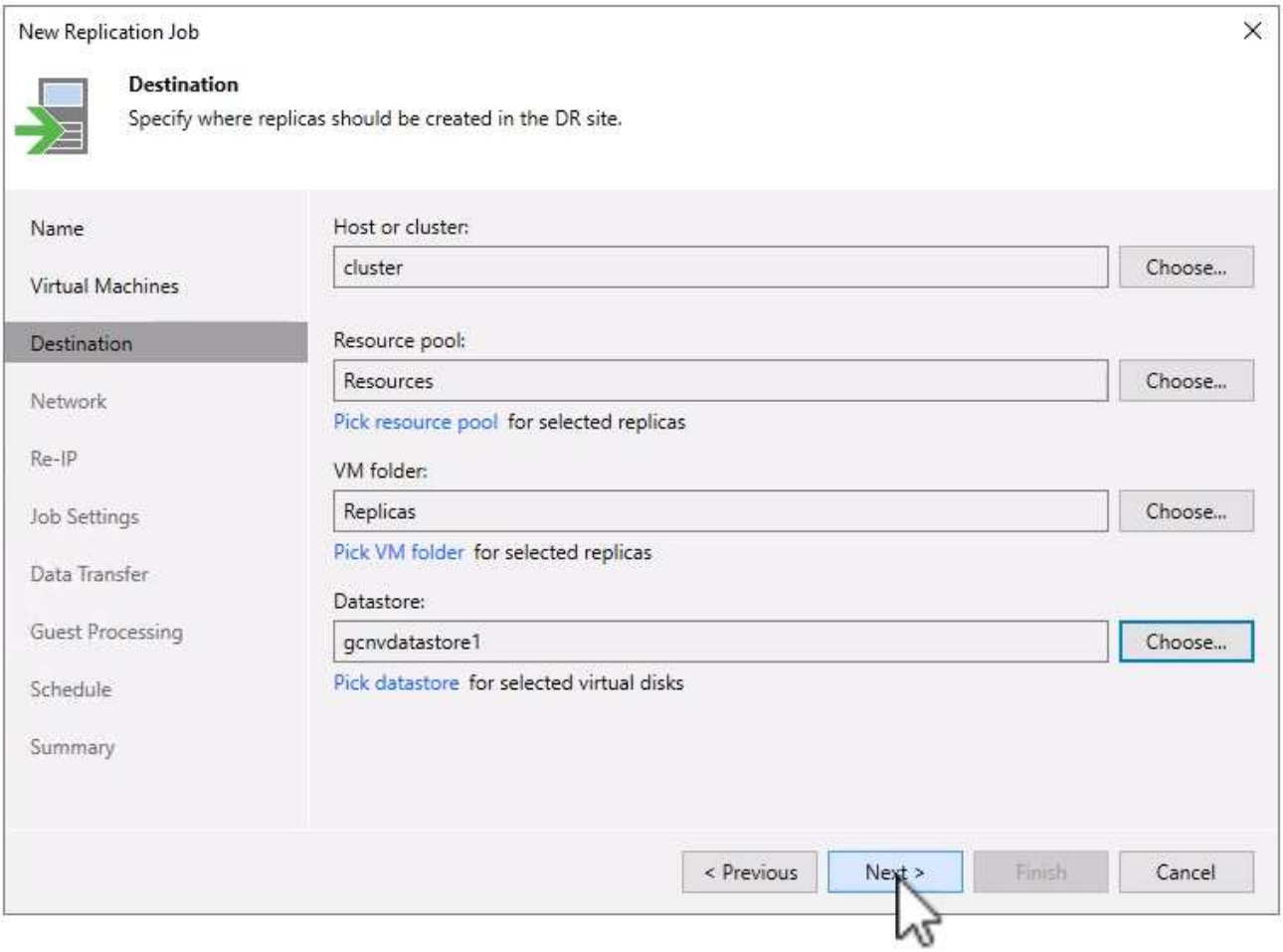


4. 在“虚拟机”页面上，选择要复制到连接到 GCVE SDDC 的NetApp卷数据存储区的虚拟机。单击*添加*，然后在*添加对象*窗口中选择必要的虚拟机或虚拟机容器，然后单击*添加*。单击“下一步”。

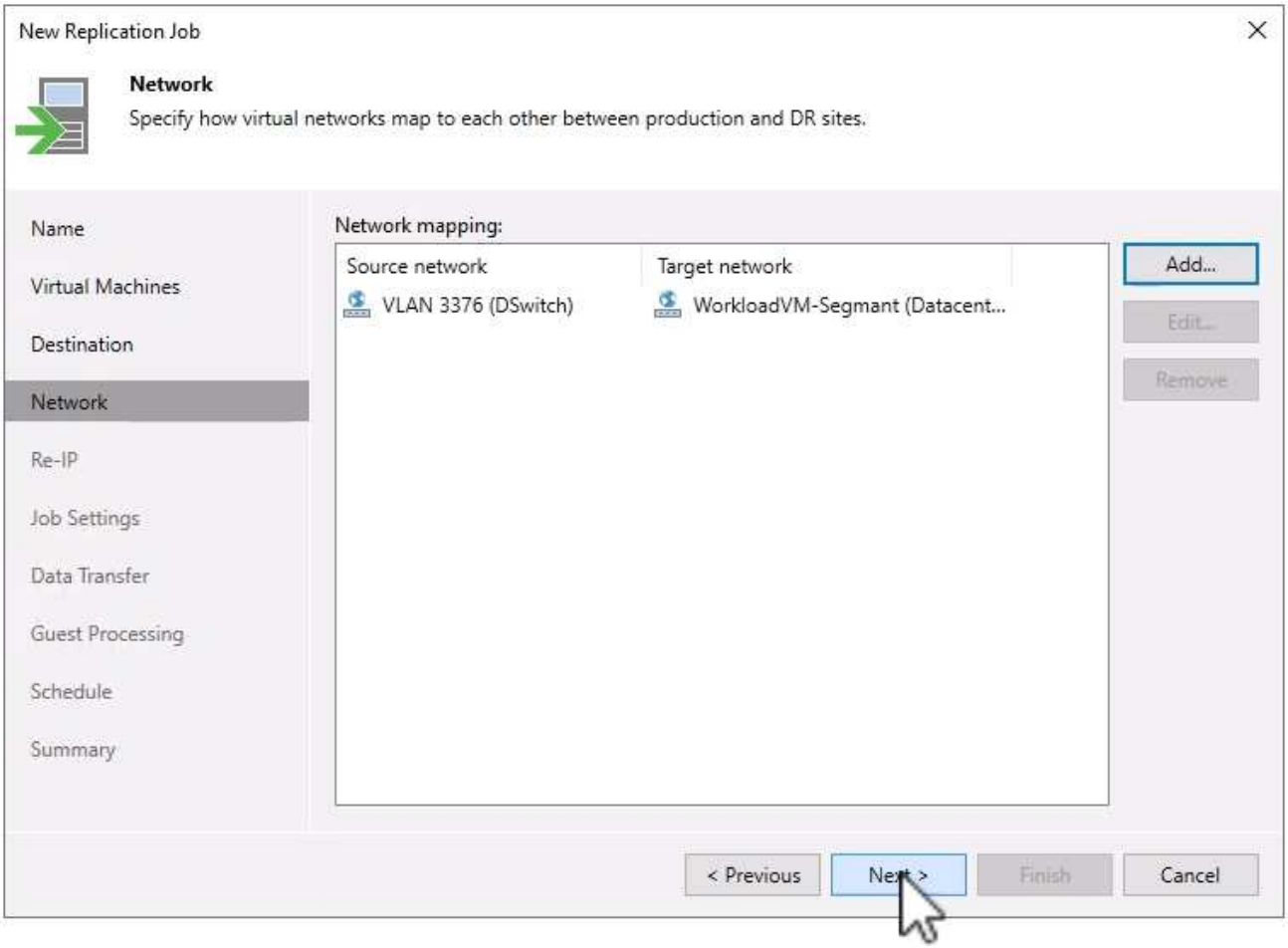
> 可以将虚拟机放置在 vSAN 上以填充可用的 vSAN 数据存储容量。在试点集群中，3 节点 vSAN 集群的可用容量将受到限制。其余数据可以轻松放置在Google Cloud NetApp Volumes数据存储中，以便可以恢复虚拟机，并且可以稍后扩展集群以满足 CPU/内存要求。



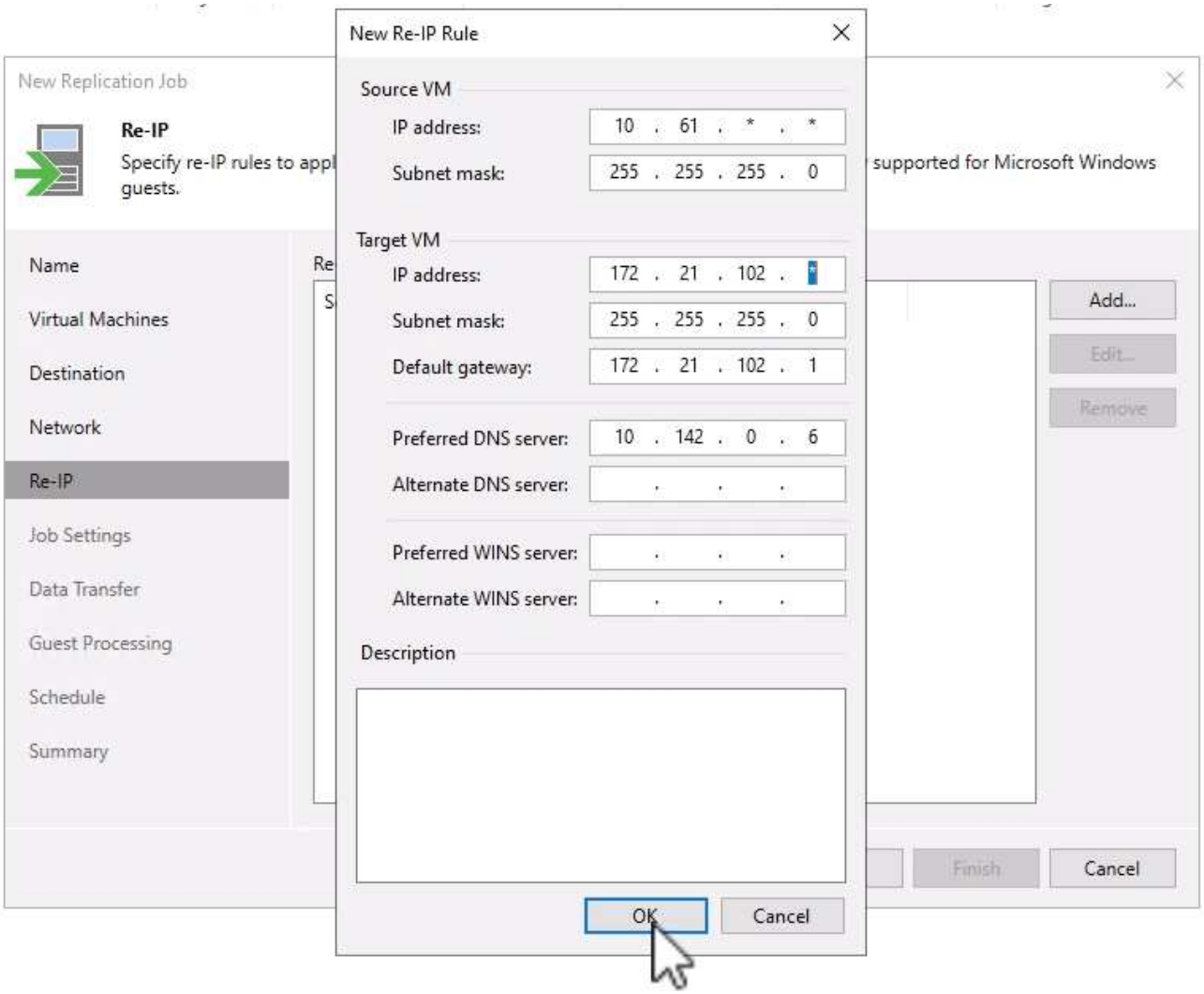
5. 在*目标*页面上，选择目标作为 GCVE SDDC 集群/主机，并为 VM 副本选择适当的资源池、VM 文件夹和NetApp Volumes 数据存储。单击“下一步”继续。



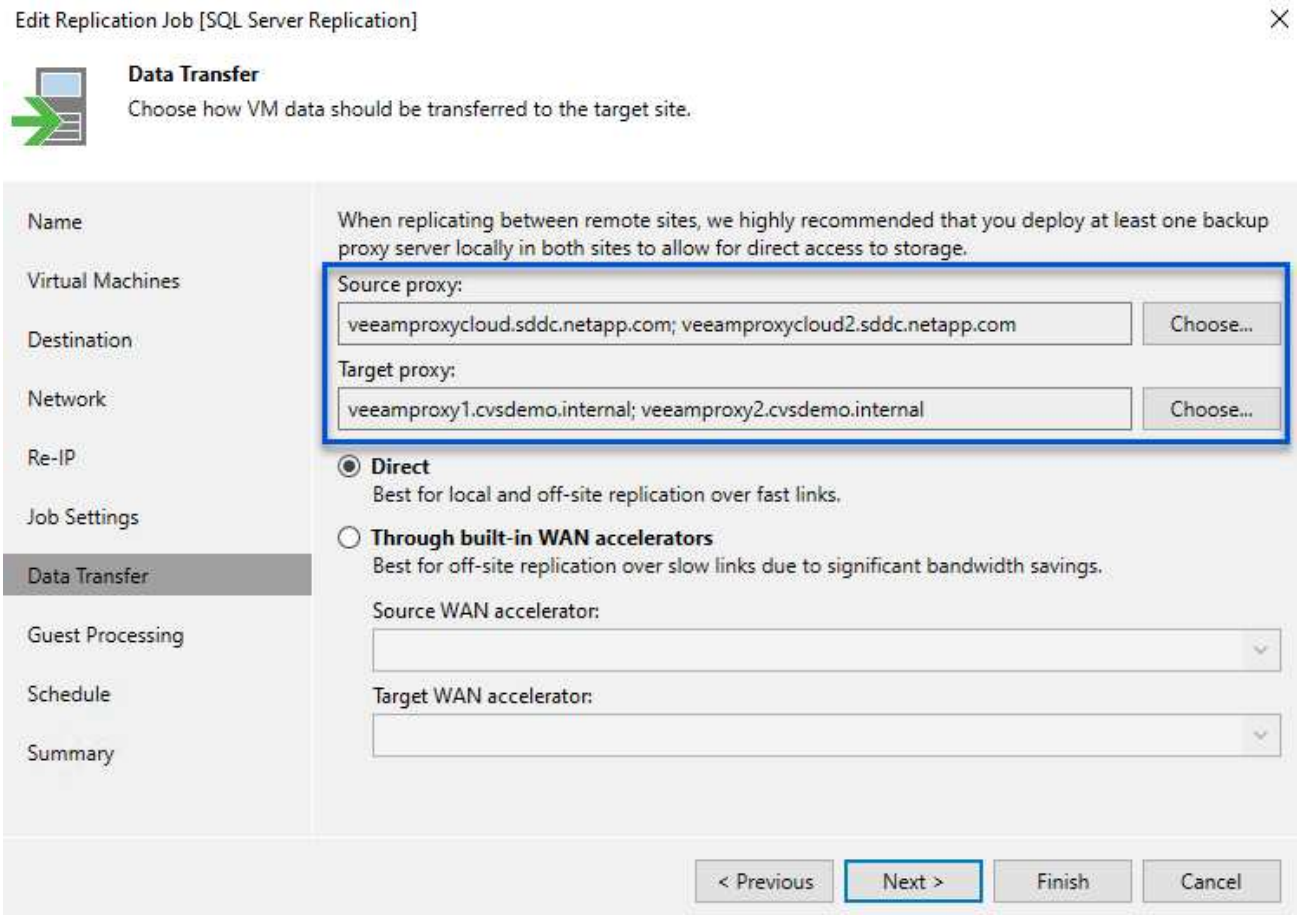
6. 在“网络”页面上，根据需要创建源虚拟网络和目标虚拟网络之间的映射。单击“下一步”继续。



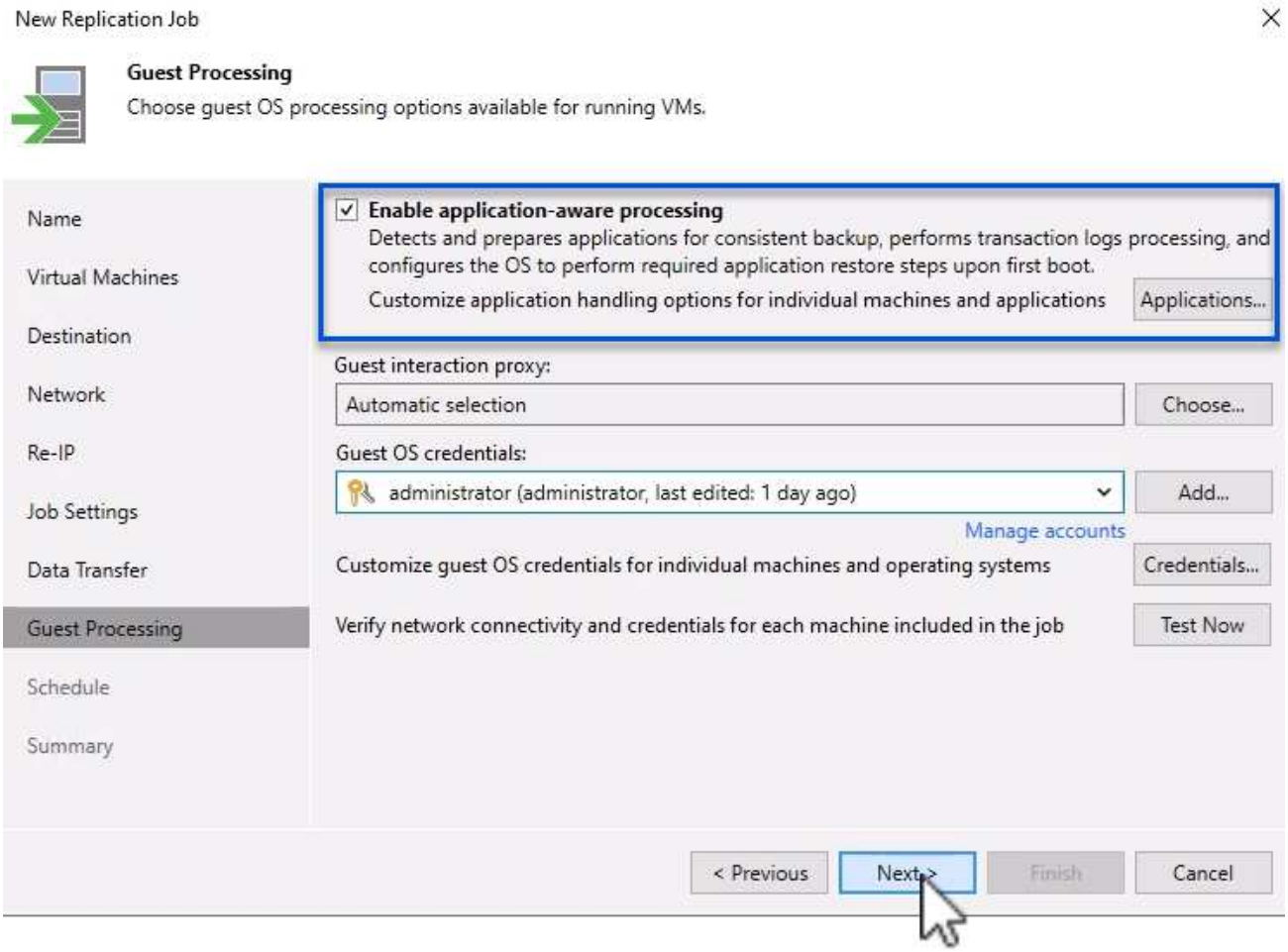
7. 在*Re-IP*页面上，单击*Add…按钮添加新的**re-ip**规则。填写源和目标虚拟机 **IP** 范围以指定在故障转移时将应用于源虚拟机的网络。使用星号来指定该八位字节的地址范围。单击“*下一步”继续。



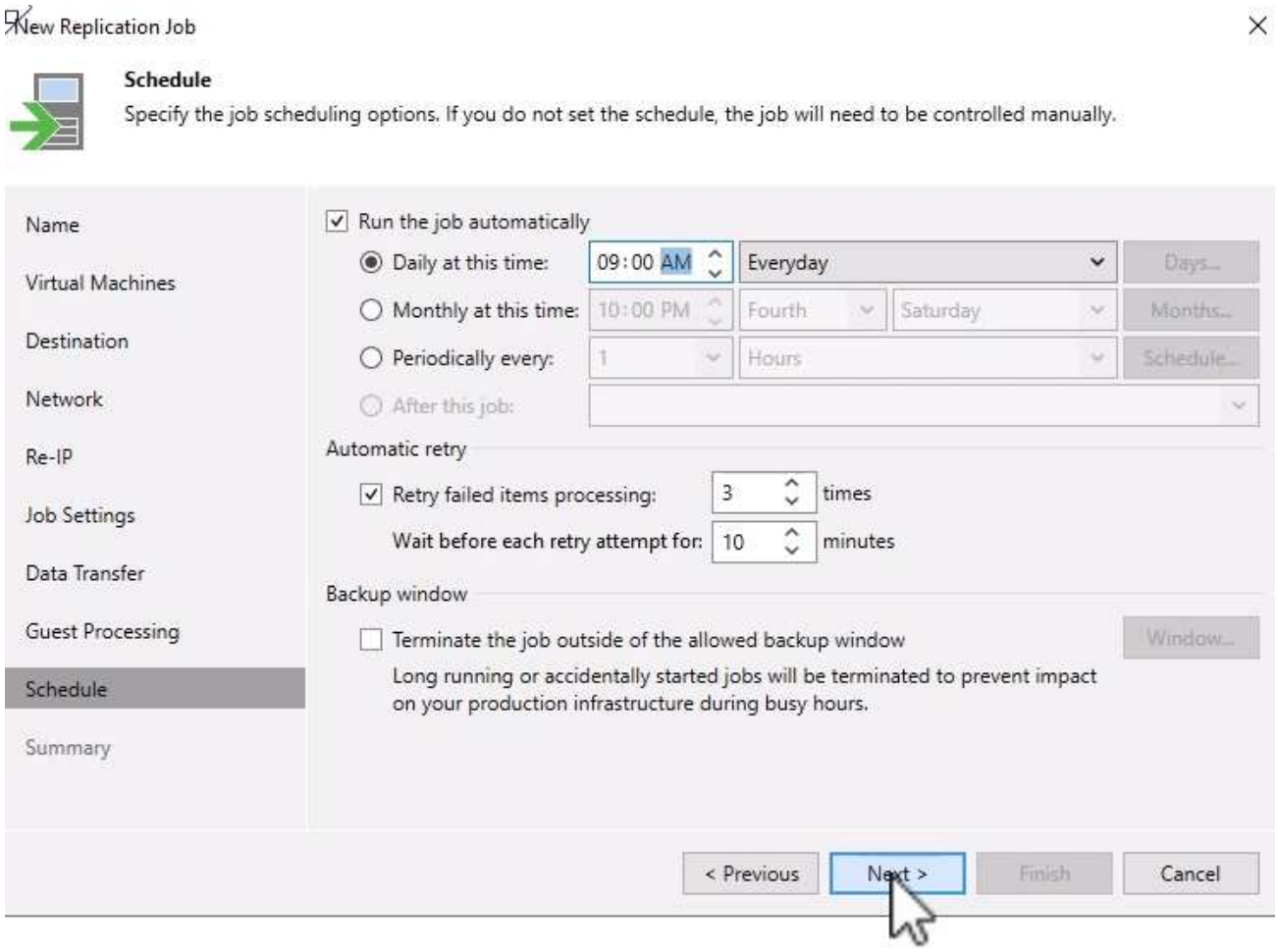
8. 在“作业设置”页面上，指定将存储 VM 副本元数据的备份存储库、保留策略，然后选择底部的“高级...”按钮以进行其他作业设置。单击“下一步”继续。
9. 在*数据传输*上，选择位于源站点和目标站点的代理服务器，并保持选择直接选项。如果配置了 WAN 加速器，也可以在这里选择。单击“下一步”继续。



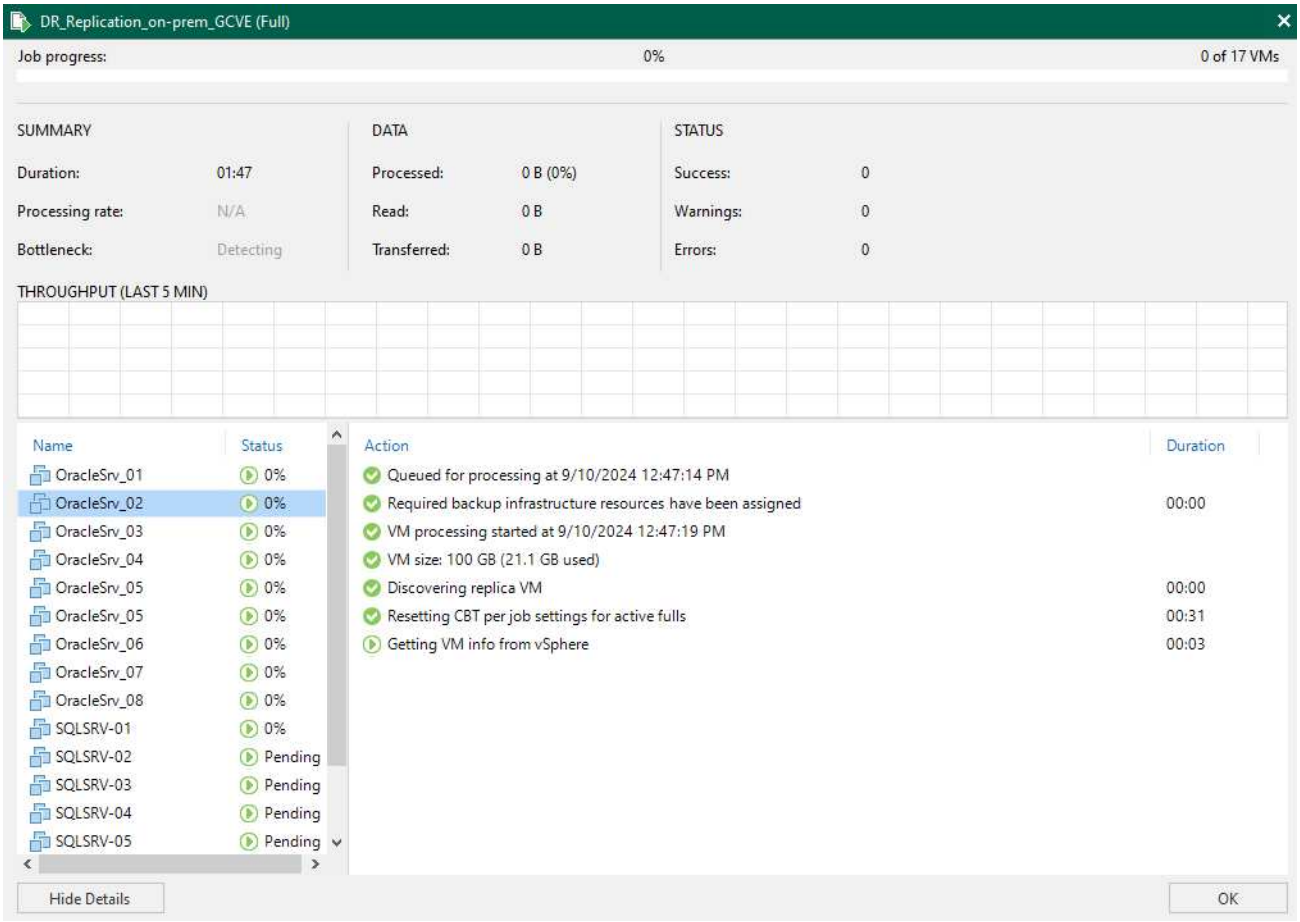
10. 在*Guest Processing*页面上，根据需要选中*Enable application-aware processing*复选框，并选择*Guest OS credentials*。单击“下一步”继续。



11. 在“计划”页面上，定义复制作业运行的时间和频率。单击“下一步”继续。



12. 最后，在*摘要*页面上检查作业设置。勾选“单击完成时运行该作业”复选框，然后单击“完成”即可完成创建复制作业。
13. 一旦运行，就可以在作业状态窗口中查看复制作业。



有关 Veeam 复制的更多信息，请参阅"复制的工作原理"

▼ 创建故障转移计划

初始复制或播种完成后，创建故障转移计划。故障转移计划有助于自动对从属虚拟机逐个或按组执行故障转移。故障转移计划是虚拟机处理顺序（包括启动延迟）的蓝图。故障转移计划还有助于确保关键依赖的虚拟机已经在运行。

完成初始复制或播种后，创建故障转移计划。该计划可作为协调依赖虚拟机（单独或作为一个组）故障转移的战略蓝图。它定义了虚拟机的处理顺序，包含了必要的启动延迟，并确保关键的依赖虚拟机在其他虚拟机之前运行。通过实施结构良好的故障转移计划，组织可以简化其灾难恢复流程，最大限度地减少停机时间并在故障转移事件期间维护相互依赖系统的完整性。

创建计划时，Veeam Backup & Replication 会自动识别并使用最新的还原点来启动 VM 副本。

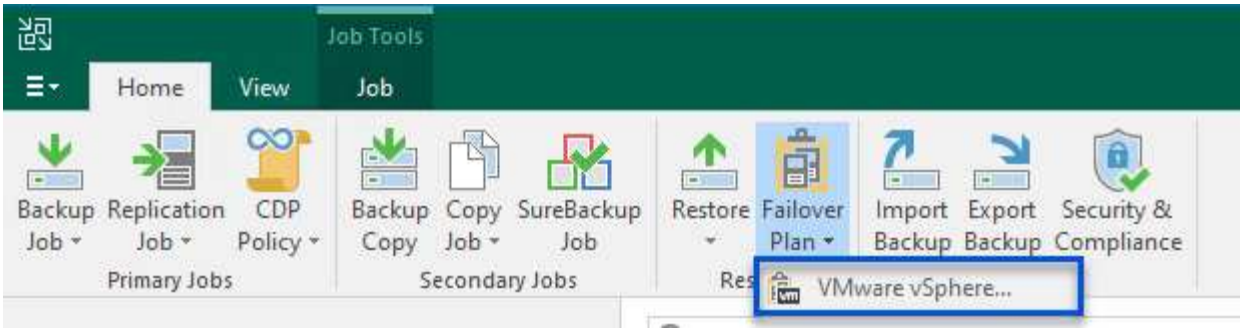
仅当初始复制完成并且 VM 副本处于就绪状态时，才能创建故障转移计划。

运行故障转移计划时可同时启动的最大虚拟机数量为 10 个。

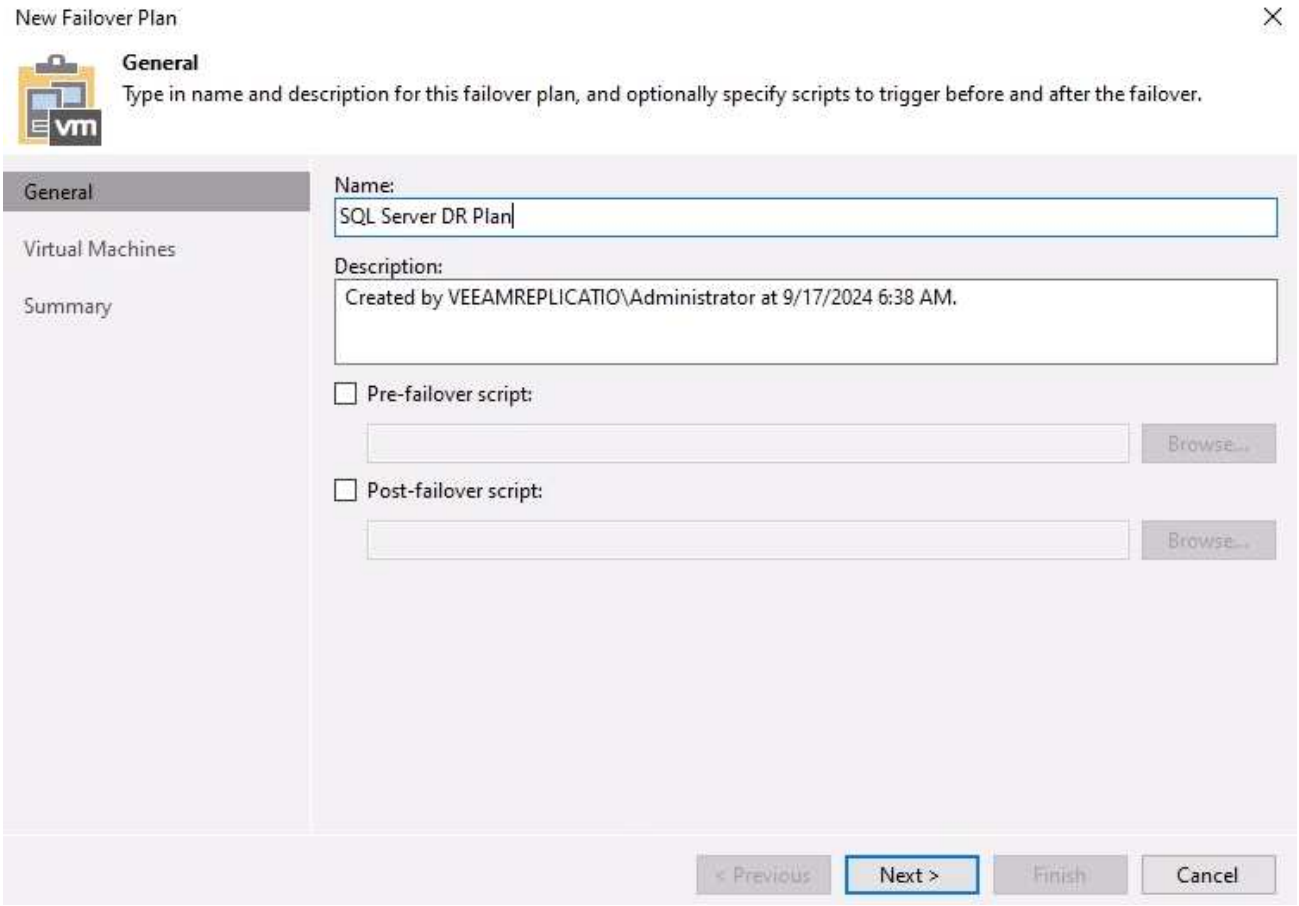
在故障转移过程中，源虚拟机不会关闭。

要创建*故障转移计划*，请完成以下步骤：

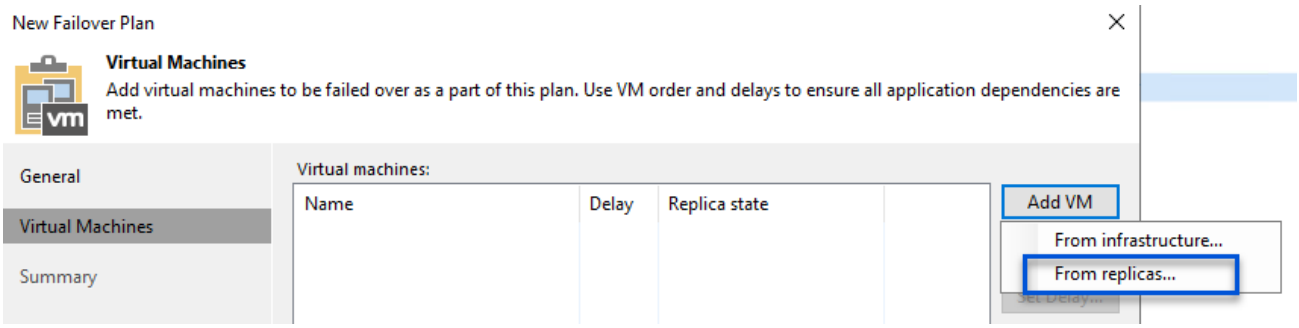
1. 在*主页*视图上，单击*恢复*部分中的*故障转移计划*按钮。在下拉菜单中，选择 **VMware vSphere...**

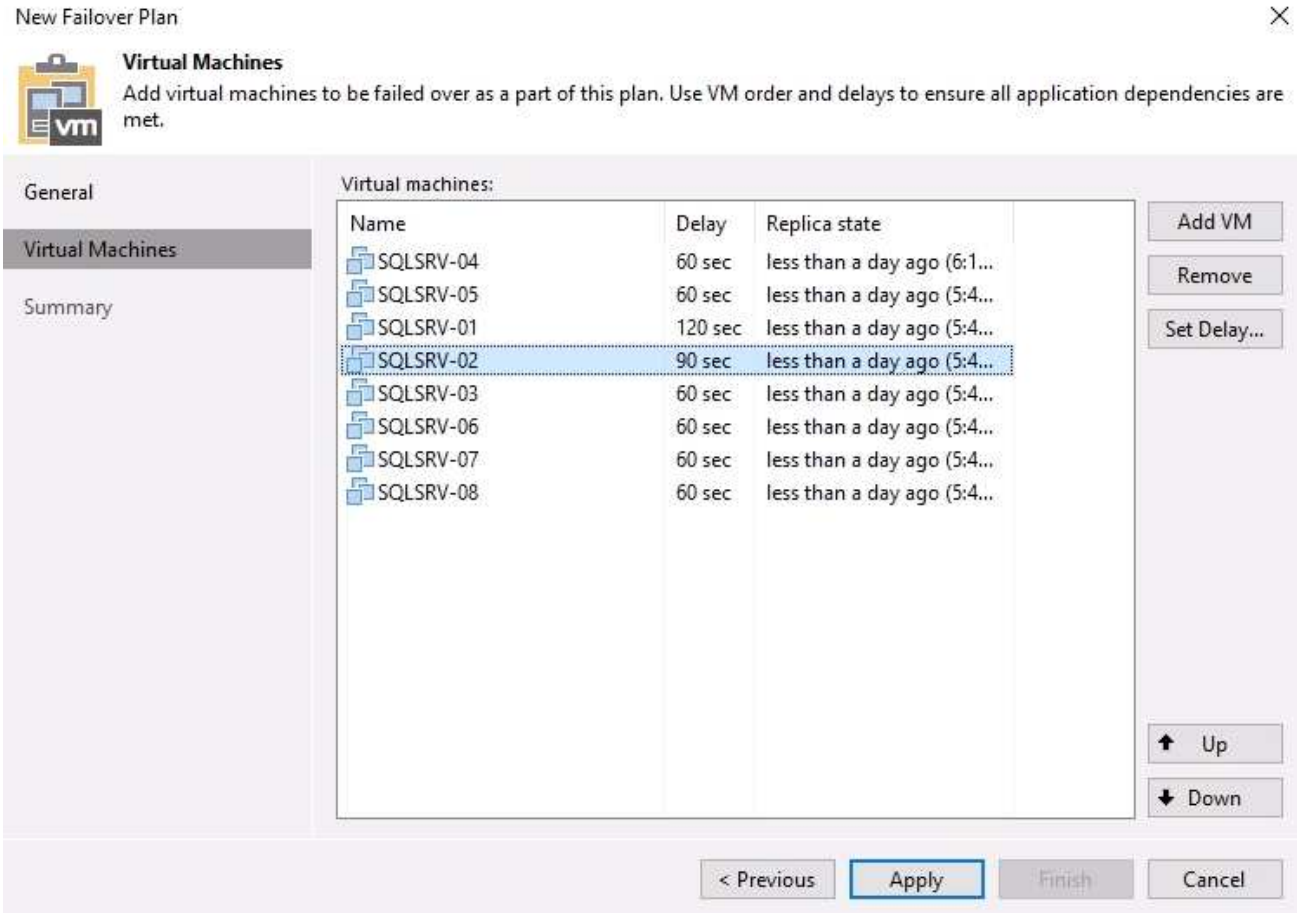


2. 在“新建故障转移计划”向导的“常规”页面上，提供计划的名称和说明。可以根据需要添加故障转移前和故障转移后脚本。例如，在启动复制的虚拟机之前运行脚本来关闭虚拟机。



3. 在“虚拟机”页面上，单击“添加虚拟机”按钮并选择“从副本…”。选择作为故障转移计划一部分的虚拟机，然后修改虚拟机启动顺序和任何所需的启动延迟以满足应用程序依赖关系。





单击“应用”继续。

4. 最后检查所有故障转移计划设置，然后单击“完成”以创建故障转移计划。

有关创建复制作业的其他信息，请参阅"创建复制作业"。

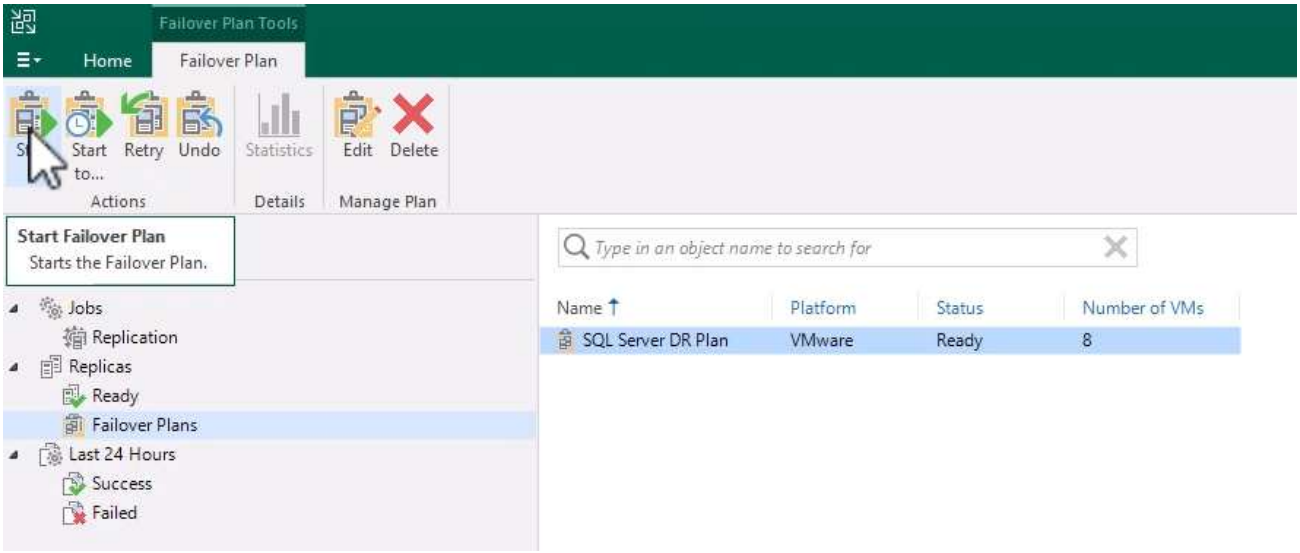
▼ 运行故障转移计划

在故障转移期间，生产站点中的源虚拟机将切换到灾难恢复站点上的副本。作为该过程的一部分，Veeam Backup & Replication 将 VM 副本恢复到所需的恢复点，并将所有 I/O 活动从源 VM 传输到其副本。复制品不仅可用于实际灾难，还可用于模拟灾难恢复演习。在故障转移模拟中，源虚拟机继续运行。完成必要的测试后，可以撤消故障转移，恢复正常操作。

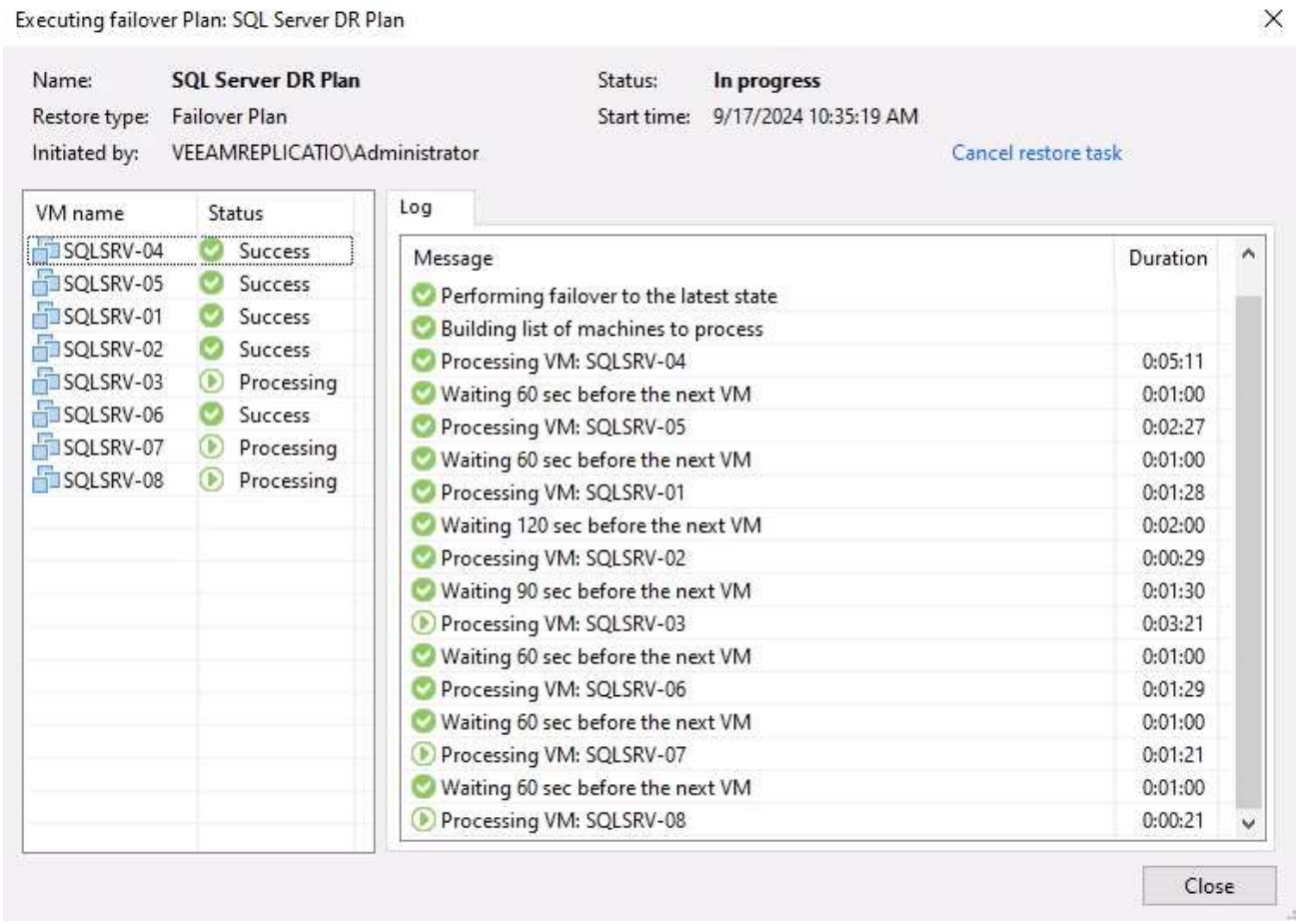
确保网络分段到位，以避免故障转移期间发生 IP 冲突。

完成以下步骤以启动故障转移计划：

1. 首先，在*主页*视图中，单击左侧菜单中的*副本 > 故障转移计划*，然后单击*开始*按钮。或者，可以使用“开始到...”按钮将故障转移到先前的还原点。



2. 在*执行故障转移计划*窗口中监控故障转移的进度。



Veeam Backup & Replication 停止源 VM 的所有复制活动，直到其副本返回到就绪状态。

有关故障转移计划的详细信息，请参阅"故障转移计划"。

▼ 故障恢复到生产站点

进行故障转移被视为中间步骤，需要根据要求最终确定。选项包括以下内容：

- 故障恢复到生产 - 恢复到原始虚拟机并将副本活动期间所做的所有修改同步回源虚拟机。

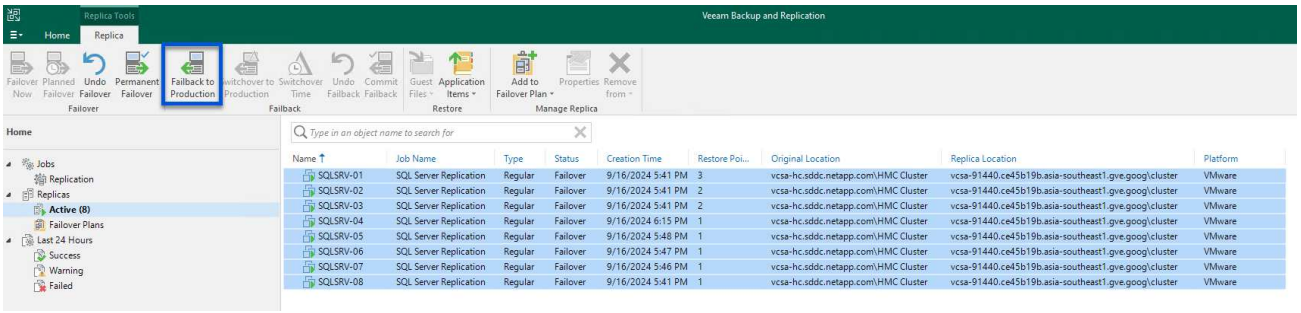
在故障恢复期间，更改会被传输但不会立即应用。验证原始虚拟机的功能后，选择“提交故障恢复”。或者，如果原始虚拟机表现出意外行为，请选择“撤消故障回复”以恢复到虚拟机副本。

- 撤消故障转移 - 恢复到原始 VM，丢弃在运行期间对 VM 副本所做的所有更改。
- 永久故障转移 - 从原始虚拟机永久切换到其副本，并将副本建立为正在进行的操作的新主虚拟机。

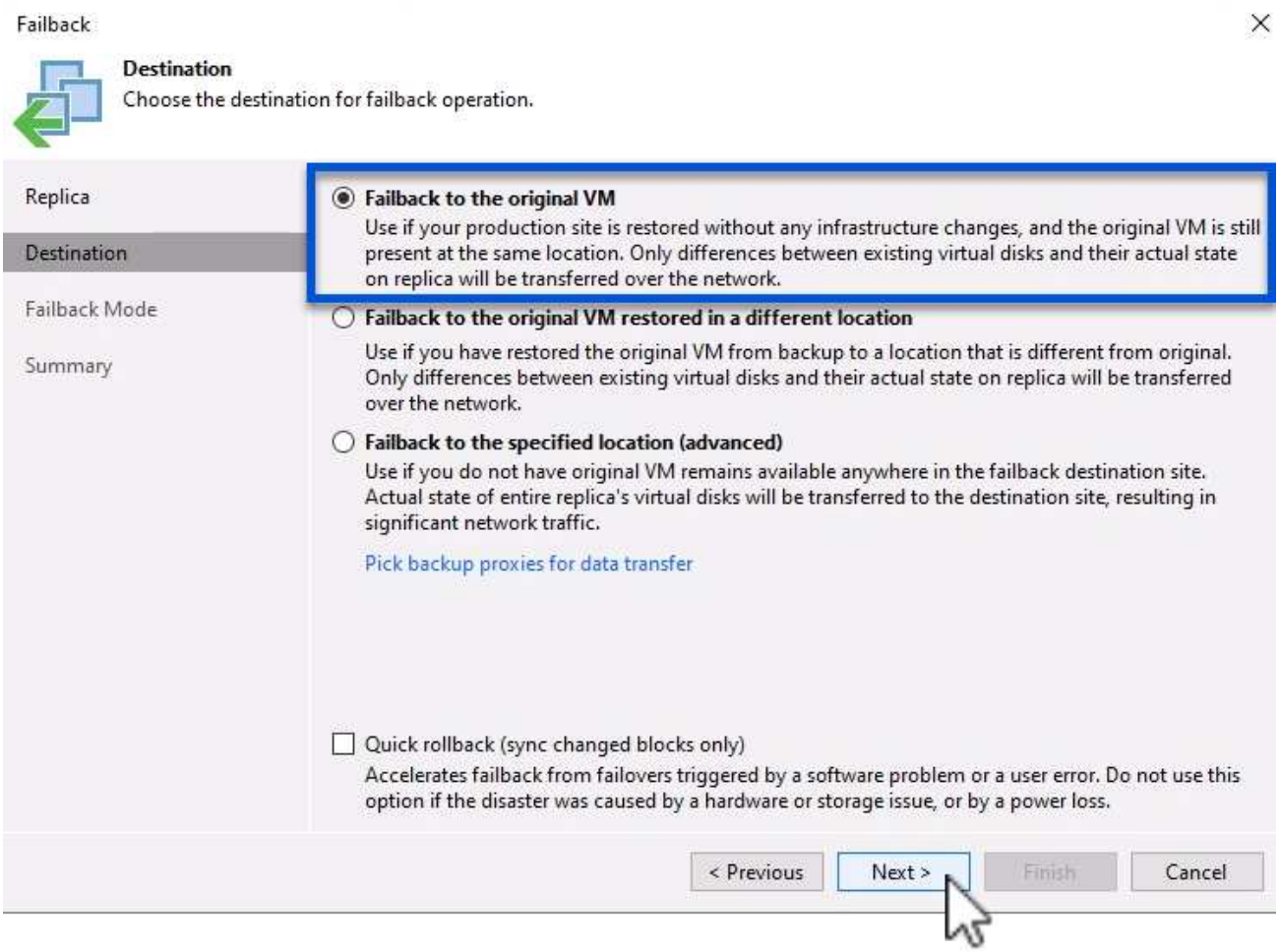
在这种情况下，选择了“故障恢复到生产”选项。

完成以下步骤以故障恢复到生产站点：

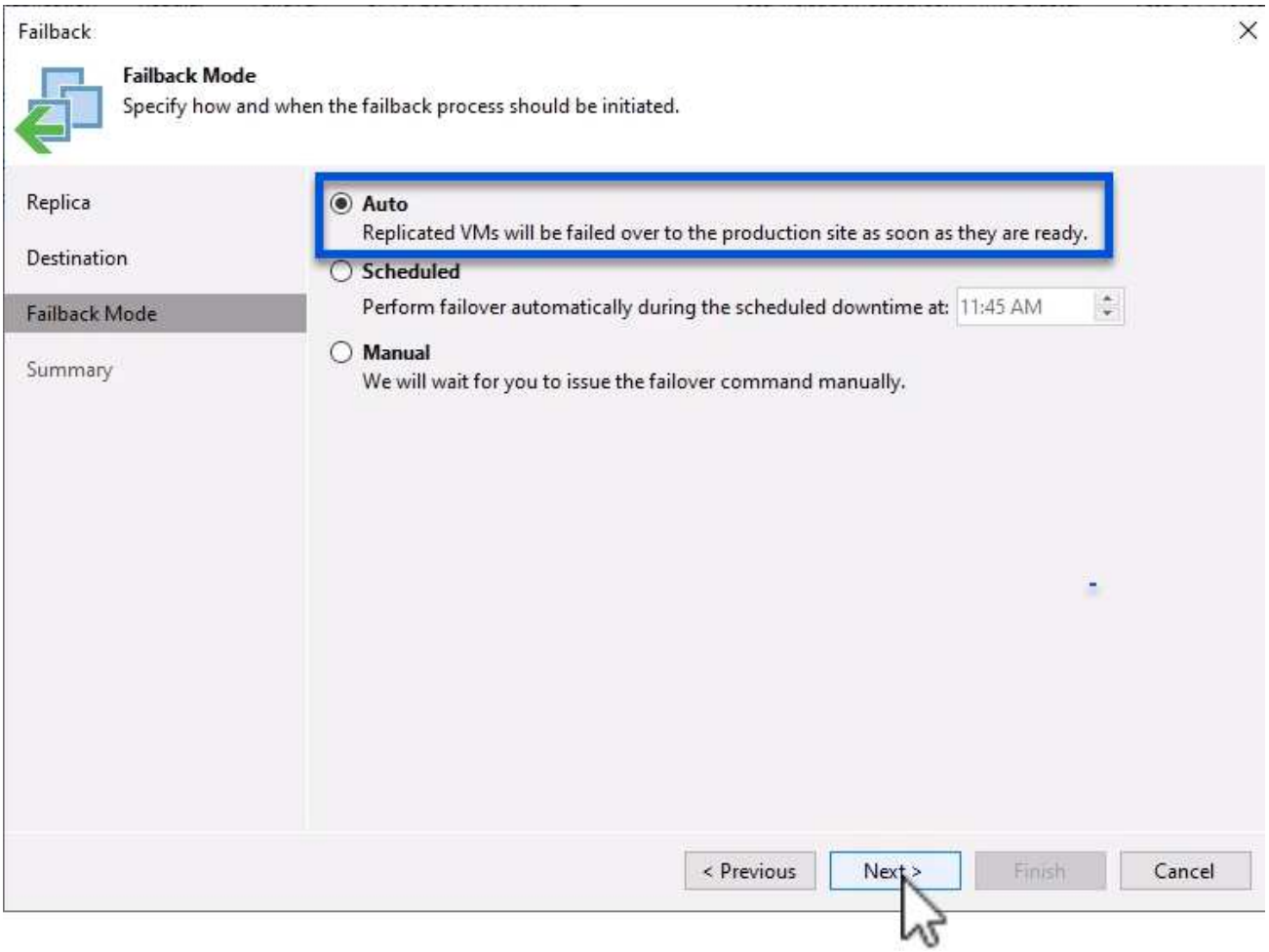
1. 从*主页*视图中，单击左侧菜单中的*副本>活动*。选择要包含的虚拟机，然后单击顶部菜单中的“故障恢复到生产”按钮。



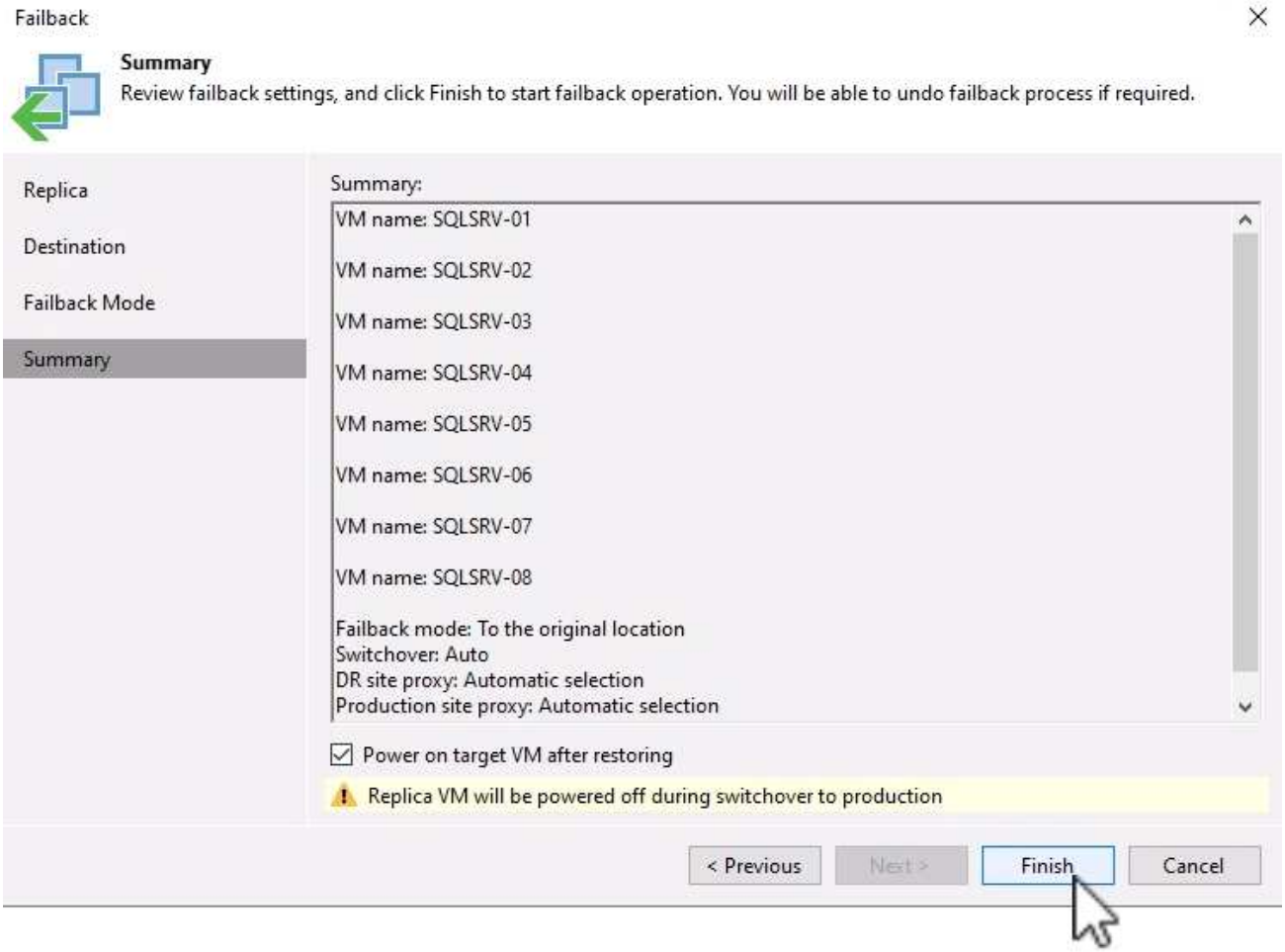
2. 在“故障回复”向导的“副本”页面上，选择要包含在故障回复作业中的副本。
3. 在*目标*页面上，选择*故障恢复到原始虚拟机*，然后单击*下一步*继续。



4. 在“故障恢复模式”页面上，选择“自动”以尽快启动故障恢复。

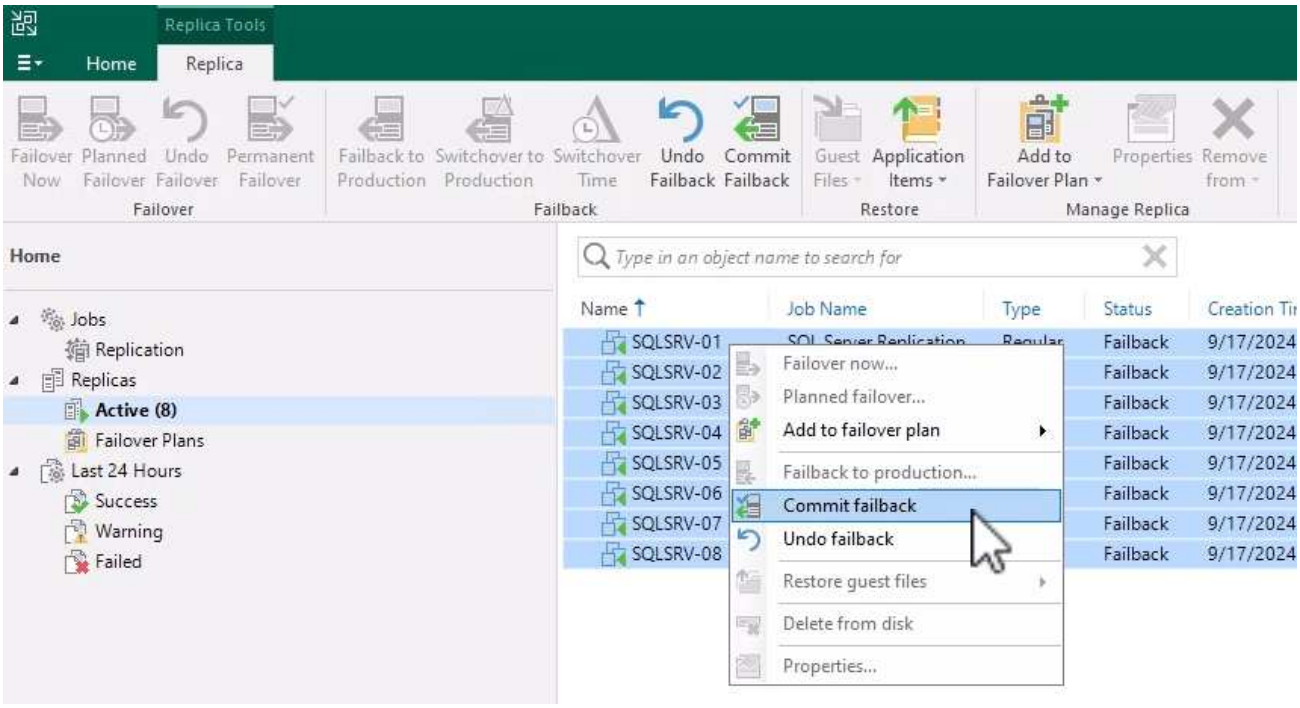


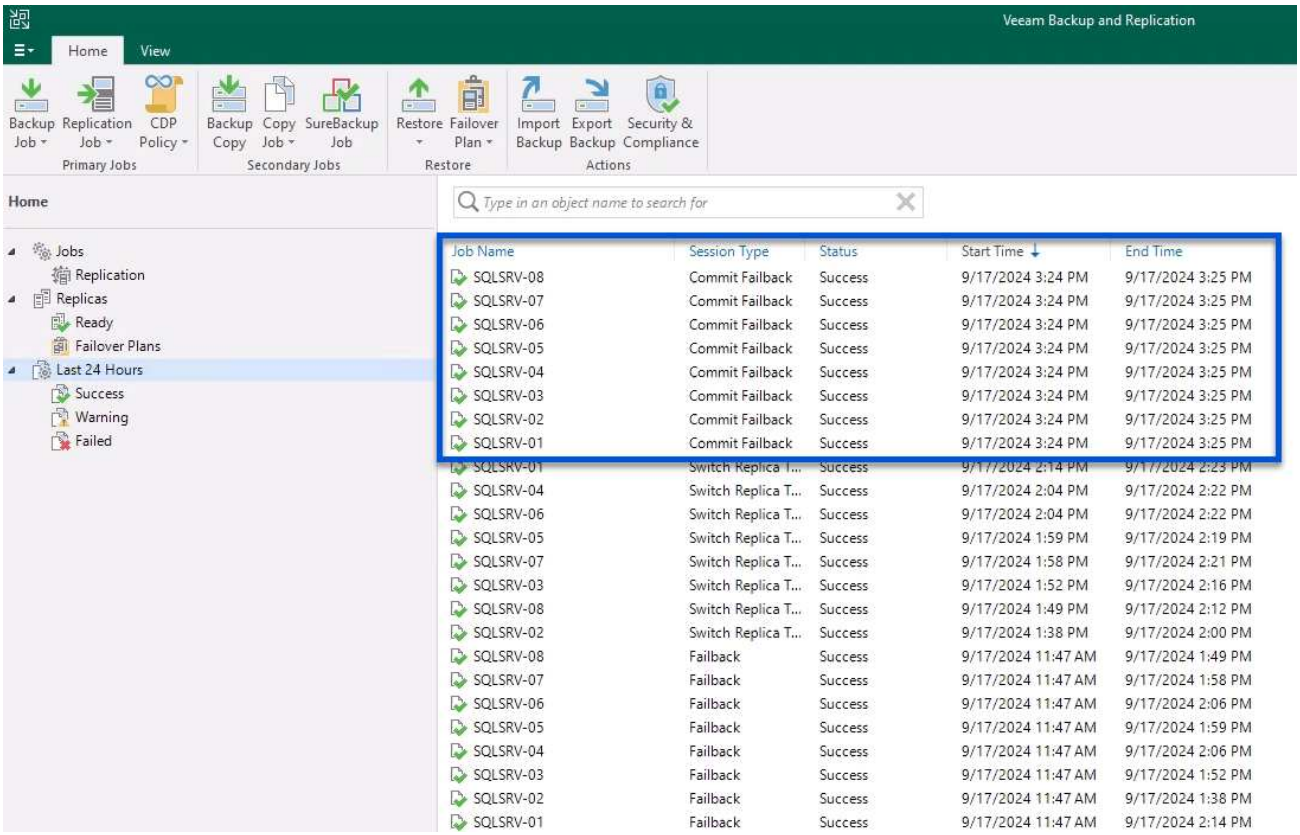
5. 在“摘要”页面上，选择是否“恢复后启动目标虚拟机”，然后单击“完成”以启动故障恢复作业。



故障回复提交完成故障回复操作，确认更改已成功集成到生产虚拟机。提交后，Veeam Backup & Replication 将恢复已恢复的生产虚拟机的常规复制活动。这会将恢复的副本的状态从_故障回复_更改为_就绪_。

1. 要提交故障回复，请导航至 **Replicas > Active**，选择要提交的虚拟机，右键单击并选择 **Commit failback**。





故障恢复到生产环境成功后，所有虚拟机都将恢复到原始生产站点。

有关故障恢复过程的详细信息，请参阅 Veeam 文档"复制的故障转移和故障恢复"。

结束语

Google Cloud NetApp Volumes数据存储功能使 Veeam 和其他经过验证的第三方工具能够提供经济高效的灾难恢复 (DR) 解决方案。通过利用 Pilot Light 集群而不是用于 VM 副本的大型专用集群，组织可以显著降低开支。这种方法可以实现定制的 DR 策略，利用现有的内部备份解决方案进行基于云的灾难恢复，从而无需额外的内部数据中心。如果发生灾难，只需单击即可启动故障转移或配置为自动发生故障转移，从而确保业务连续性并将停机时间降至最低。

要了解有关此过程的更多信息，请随意观看详细的演示视频。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

迁移 GCP/GCVE 上的工作负载

使用 **VMware HCX** 将工作负载迁移到**Google Cloud NetApp Volumes**数据存储区 - 快速入门指南

Google Cloud VMware Engine 和 Cloud Volume Service 数据存储最常见的用例之一是迁移 VMware 工作负载。 VMware HCX 是一个首选方案，它提供了各种迁移机制，可将本地虚拟机 (VM) 及其数据移动到 Cloud Volume Service NFS 数据存储。

概述：使用 **VMware HCX**、 **Google Cloud NetApp Volumes**数据存储区和 **Google Cloud VMware Engine (GCVE)** 迁移虚拟机

VMware HCX 主要是一个迁移平台，旨在简化应用程序迁移、工作负载重新平衡甚至跨云的业务连续性。它是 Google Cloud VMware Engine Private Cloud 的一部分，提供了多种迁移工作负载的方法，并可用于灾难恢复 (DR) 操作。

本文档提供了配置 Cloud Volume Service 数据存储区的分步指导，随后下载、部署和配置 VMware HCX，包括其在本地和 Google Cloud VMware Engine 端的所有主要组件（包括互连、网络扩展和 WAN 优化），以支持各种 VM 迁移机制。

> VMware HCX 适用于任何数据存储类型，因为迁移是在 VM 级别进行的。因此，本文档适用于现有NetApp客户和计划使用 Google Cloud VMware Engine 部署 Cloud Volume Service 以实现经济高效的 VMware 云部署的非NetApp客户。

▼ 概要步骤

此列表提供了将虚拟机从本地 HCX Connector 配对并迁移到 Google Cloud VMware Engine 端的 HCX Cloud Manager 所需的高级步骤：

1. 通过 Google VMware Engine 门户准备 HCX。
2. 在本地 VMware vCenter Server 中下载并部署 HCX Connector Open Virtualization Appliance (OVA) 安装程序。
3. 使用许可证密钥激活 HCX。
4. 将本地 VMware HCX Connector 与 Google Cloud VMware Engine HCX Cloud Manager 配对。
5. 配置网络配置文件、计算配置文件和服务网格。
6. （可选）执行网络扩展以避免在迁移期间重新分配 IP。
7. 验证设备状态并确保可以迁移。
8. 迁移虚拟机工作负载。

▼ 前提条件

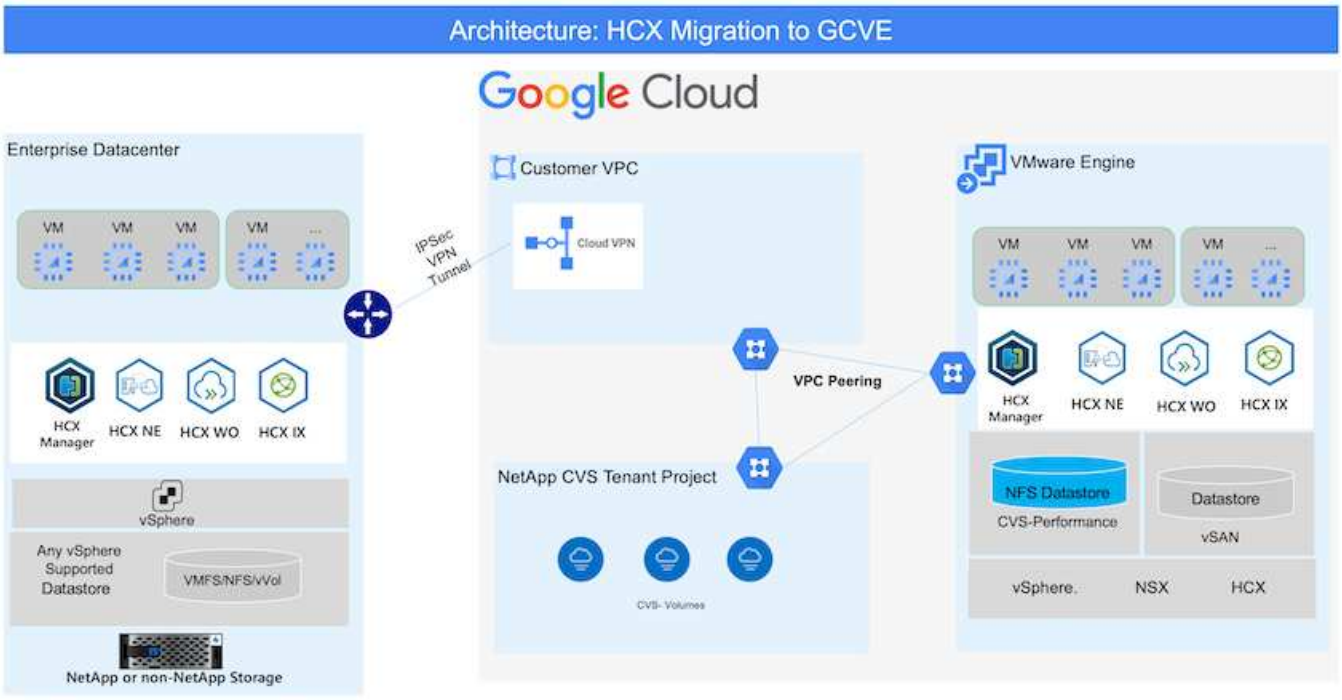
开始之前，请确保满足以下先决条件。有关详细信息，请参阅 "链接"。满足连接等先决条件后，从 Google Cloud VMware Engine 门户下载 HCX 许可证密钥。下载 OVA 安装程序后，按照如下所述进行安装过程。

HCX 高级版是默认选项，VMware HCX 企业版也可通过支持票获得，并且无需额外付费即可获得支持。参考 "此链接"

- 使用现有的 Google Cloud VMware Engine 软件定义数据中心 (SDDC) 或使用此"NetApp链接"或者这个 "谷歌链接"。
- 从支持 VMware vSphere 的内部部署数据中心迁移虚拟机和相关数据需要从数据中心到 SDDC 环境的网络连接。在迁移工作负载之前， "设置 Cloud VPN 或 Cloud Interconnect 连接"在本地环境和相应的私有云之间。
- 从本地 VMware vCenter Server 环境到 Google Cloud VMware Engine 私有云的网络路径必须支持使用 vMotion 迁移虚拟机。
- 确保所需的 "防火墙规则和端口"允许在本地 vCenter Server 和 SDDC vCenter 之间进行 vMotion 流量。
- Cloud Volume Service NFS 卷应作为数据存储安装在 Google Cloud VMware Engine 中。按照本文中详细说明的步骤操作 "链接"将 Cloud Volume Service 数据存储附加到 Google Cloud VMware Engines 主机。

▼ 高级架构

为了测试目的，用于此验证的本地实验室环境通过 Cloud VPN 连接，这允许本地连接到 Google Cloud VPC。



有关将 VMware HCX 与 Google 结合使用的更多详细信息，请参阅 "VMware 链接"

解决方案部署

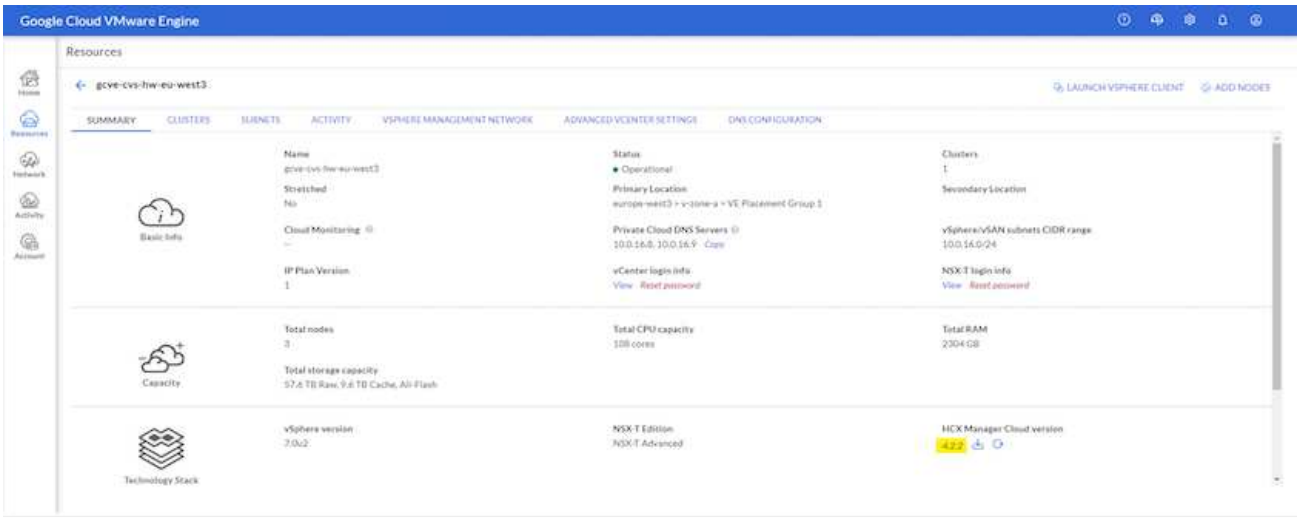
按照一系列步骤完成此解决方案的部署：

▼ 步骤 1：通过 **Google VMware Engine** 门户准备 **HCX**

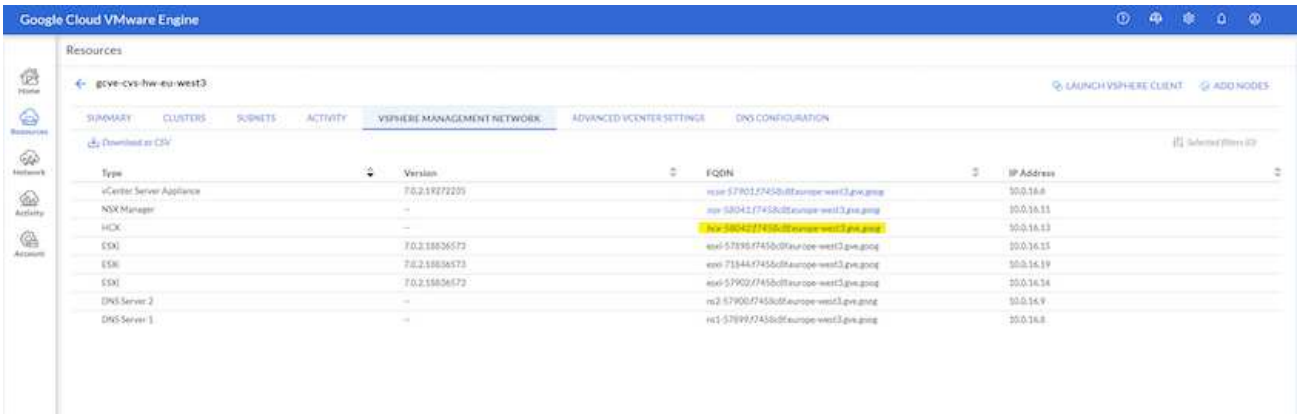
当您使用 VMware Engine 配置私有云时，HCX Cloud Manager 组件会自动安装。要准备站点配对，请完成以下步骤：

1. 登录 Google VMware Engine 门户并登录 HCX Cloud Manager。

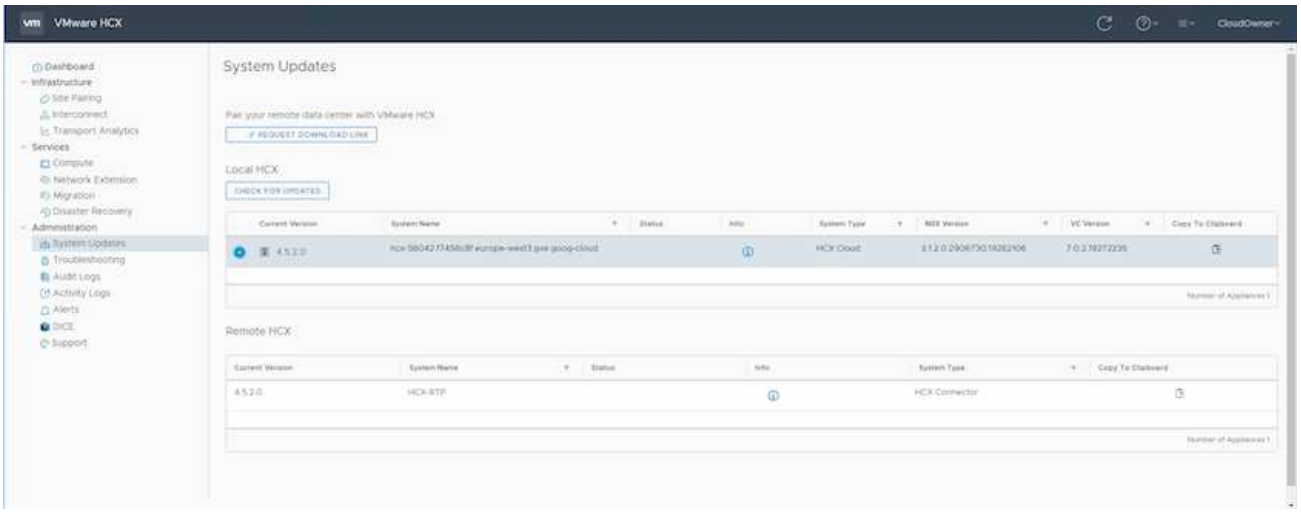
   您可以通过单击 HCX 版本链接登录 HCX 控制台



   或单击 vSphere 管理网络选项卡下的 HCX FQDN。



2. 在 HCX 云管理器中，转到“管理”>“系统更新”。
3. 单击*请求下载链接*并下载 OVA 文件。



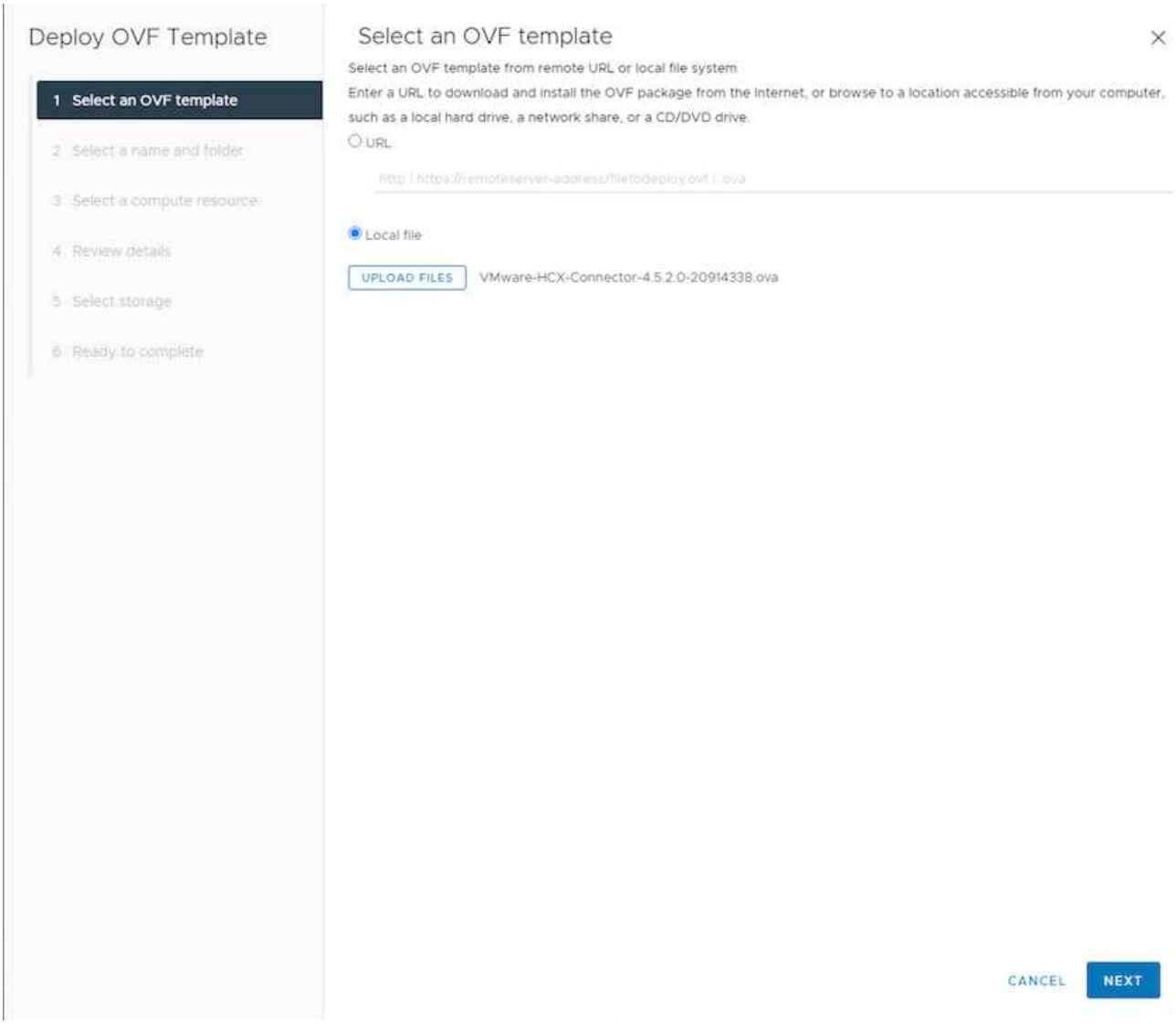
4. 将 HCX Cloud Manager 更新至 HCX Cloud Manager UI 提供的最新版本。

▼ 步骤 **2**：在本地 **vCenter Server** 中部署安装程序 **OVA**

要使本地连接器连接到 Google Cloud VMware Engine 中的 HCX 管理器，请确保在本地环境中打开了相应的防火墙端口。

要在本地 vCenter Server 中下载并安装 HCX Connector，请完成以下步骤：

1. 按照上一步所述，从 Google Cloud VMware Engine 上的 HCX 控制台下载 ova。
2. 下载 OVA 后，使用 部署 **OVF** 模板 选项将其部署到本地 VMware vSphere 环境。



3. 输入 OVA 部署所需的所有信息，单击“下一步”，然后单击“完成”以部署 VMware HCX 连接器 OVA。

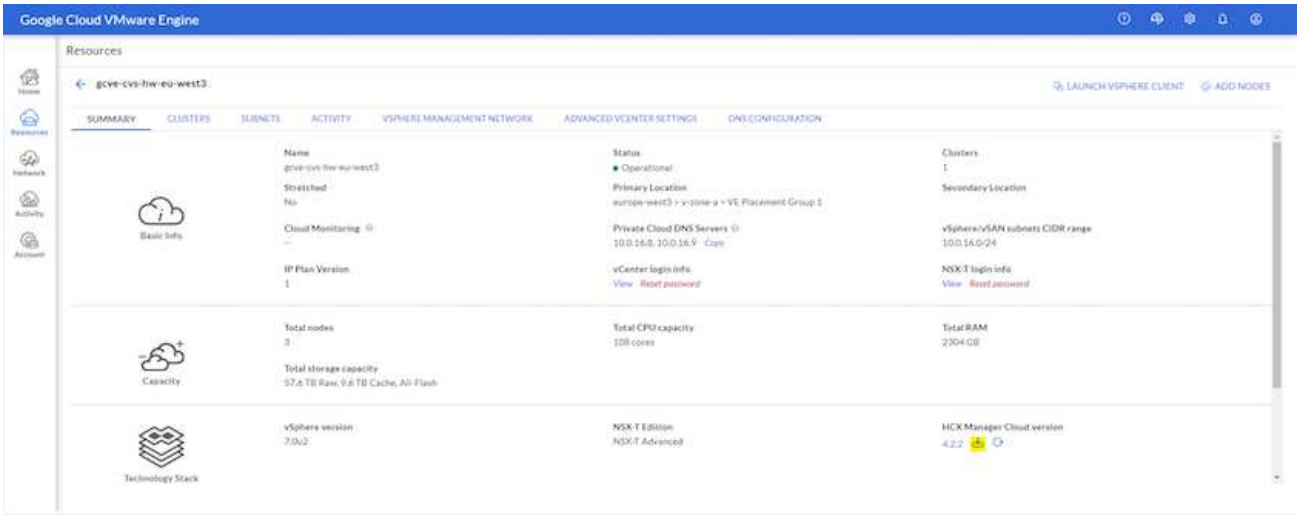
   手动启动虚拟设备。

有关分步说明，请参阅 "Google HCX 文档"。

▼ 步骤 **3**：使用许可证密钥激活 **HCX Connector**

在本地部署 VMware HCX Connector OVA 并启动设备后，完成以下步骤以激活 HCX Connector。从 Google Cloud VMware Engine 门户生成许可证密钥并在 VMware HCX Manager 中激活它。

1. 在 VMware Engine 门户中，单击“资源”，选择私有云，然后*单击“HCX Manager 云版本”下的下载图标*。



打开下载的文件并复制许可证密钥字符串。

2. 登录本地 VMware HCX 管理器 `"https://hcxmanagerIP:9443"`使用管理员凭据。

   使用 OVA 部署期间定义的 hcxmanagerIP 和密码。

3. 在许可中，输入从步骤 3 复制的密钥，然后单击 激活。

   本地 HCX 连接器应该具有互联网访问权限。

4. 在“数据中心位置”下，提供在本地安装 VMware HCX 管理器的最近位置。单击“继续”。
5. 在“系统名称”下，更新名称并单击“继续”。
6. 单击“是，继续”。
7. 在“连接您的 vCenter”下，提供 vCenter Server 的完全限定域名 (FQDN) 或 IP 地址以及相应的凭据，然后单击“继续”。

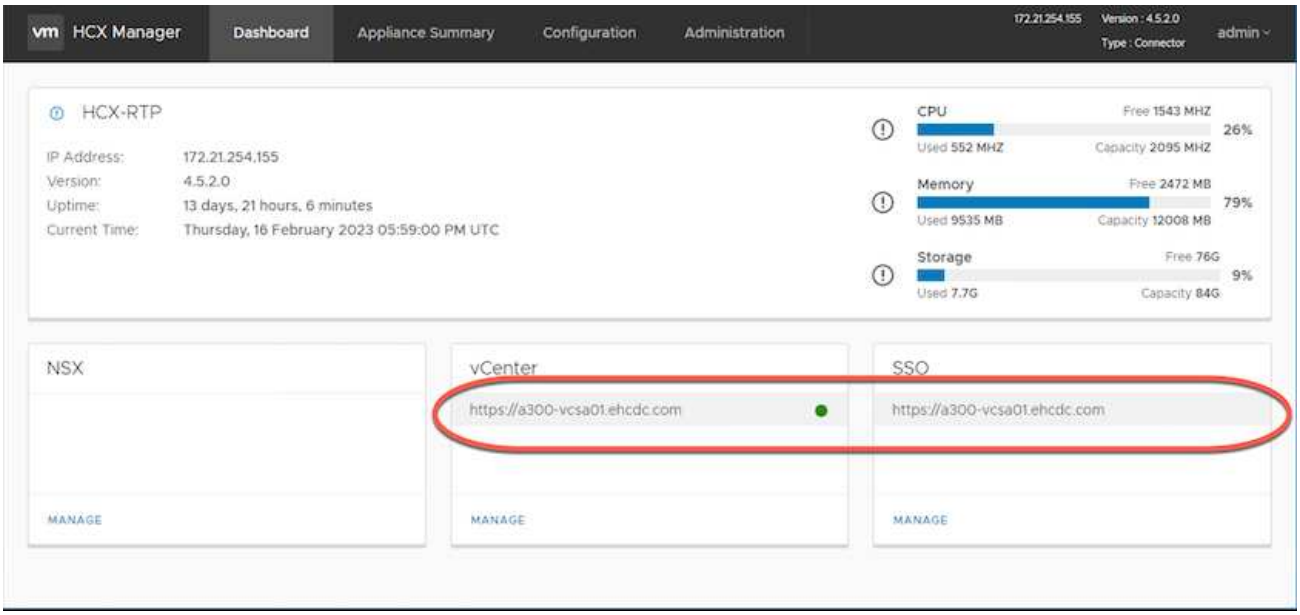
   使用 FQDN 以避免以后出现连接问题。

8. 在“配置 SSO/PSC”下，提供平台服务控制器 (PSC) 的 FQDN 或 IP 地址，然后单击“继续”。

   对于嵌入式 PSC，输入 VMware vCenter Server FQDN 或 IP 地址。

9. 验证输入的信息是否正确，然后单击“重新启动”。
10. 服务重新启动后，vCenter Server 在出现的页面上显示为绿色。 vCenter Server 和 SSO 都必须具有适当的配置参数，这些参数应与上一页相同。

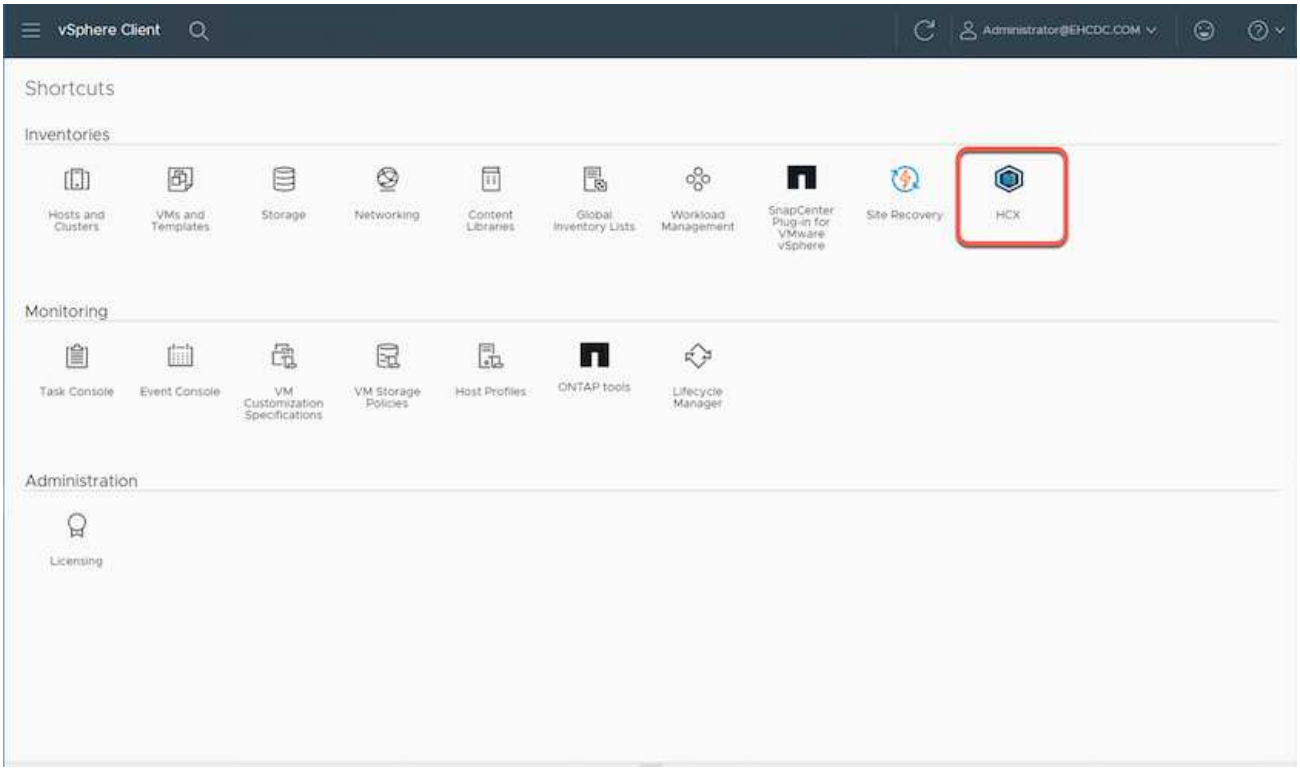
    此过程大约需要 10 到 20 分钟，以便将插件添加到 vCenter Server。



▼ 步骤 **4**：将本地 **VMware HCX** 连接器与 **Google Cloud VMware Engine HCX Cloud Manager** 配对

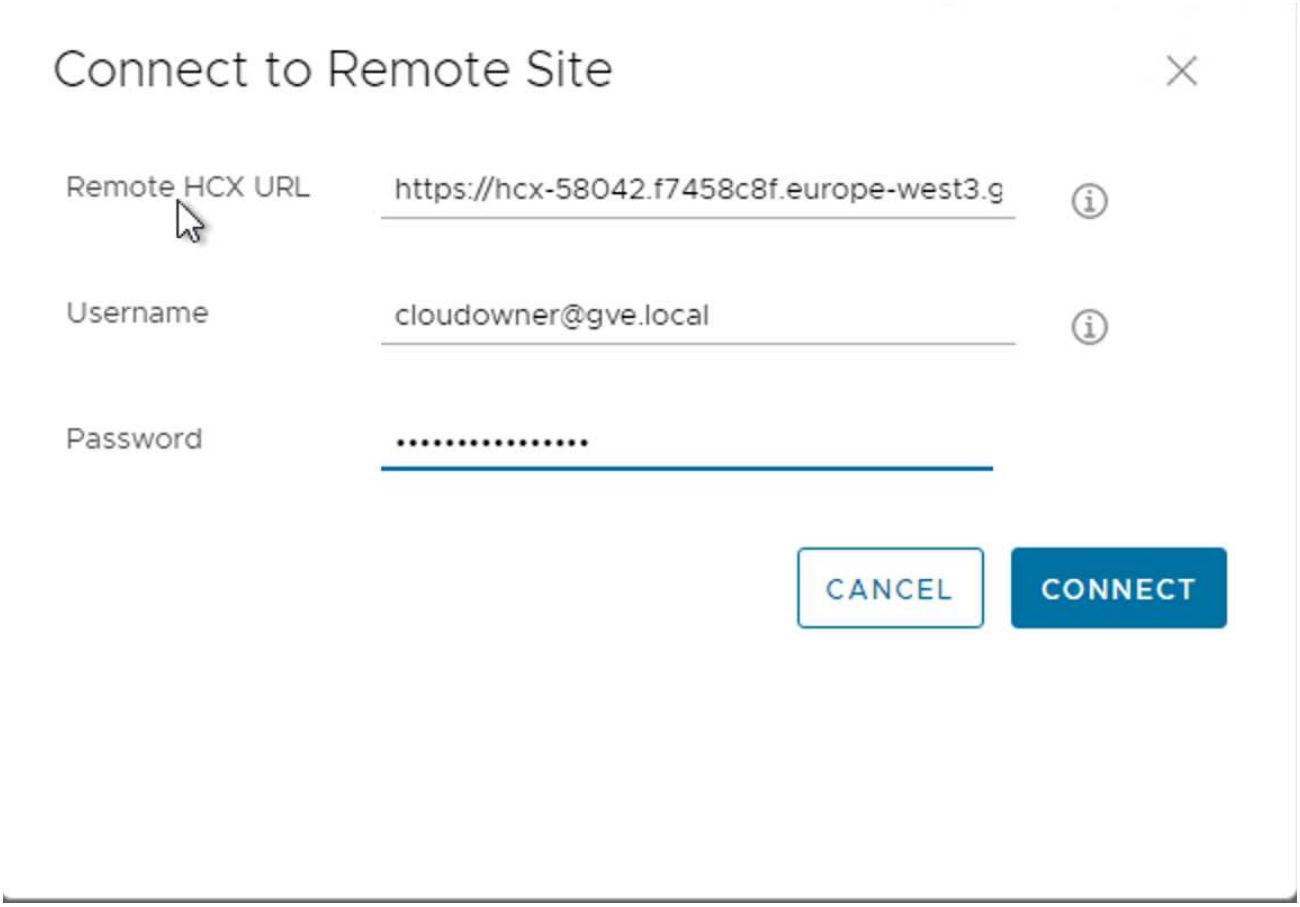
在本地 vCenter 上部署和配置 HCX Connector 后，通过添加配对建立与 Cloud Manager 的连接。要配置站点配对，请完成以下步骤：

1. 要在本地 vCenter 环境和 Google Cloud VMware Engine SDDC 之间创建站点对，请登录本地 vCenter Server 并访问新的 HCX vSphere Web Client 插件。



2. 在基础设施下，单击*添加站点配对*。

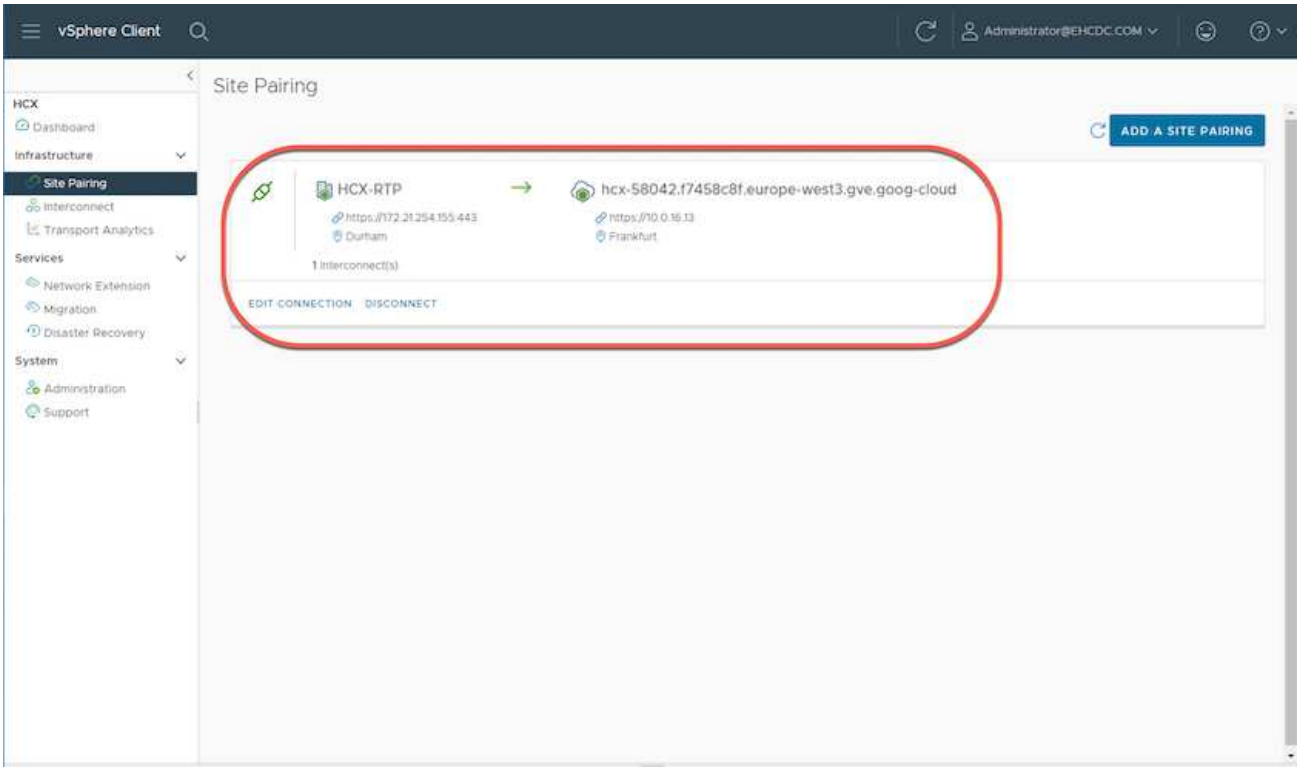
输入 Google Cloud VMware Engine HCX Cloud Manager URL 或 IP 地址以及具有 CloudOwner-Role 权限的用户访问私有云的凭据。



3. 单击“连接”。

VMware HCX Connector 必须能够通过端口 443 路由到 HCX Cloud Manager IP。

4. 创建配对后，新配置的站点配对可在 HCX 仪表板上获得。

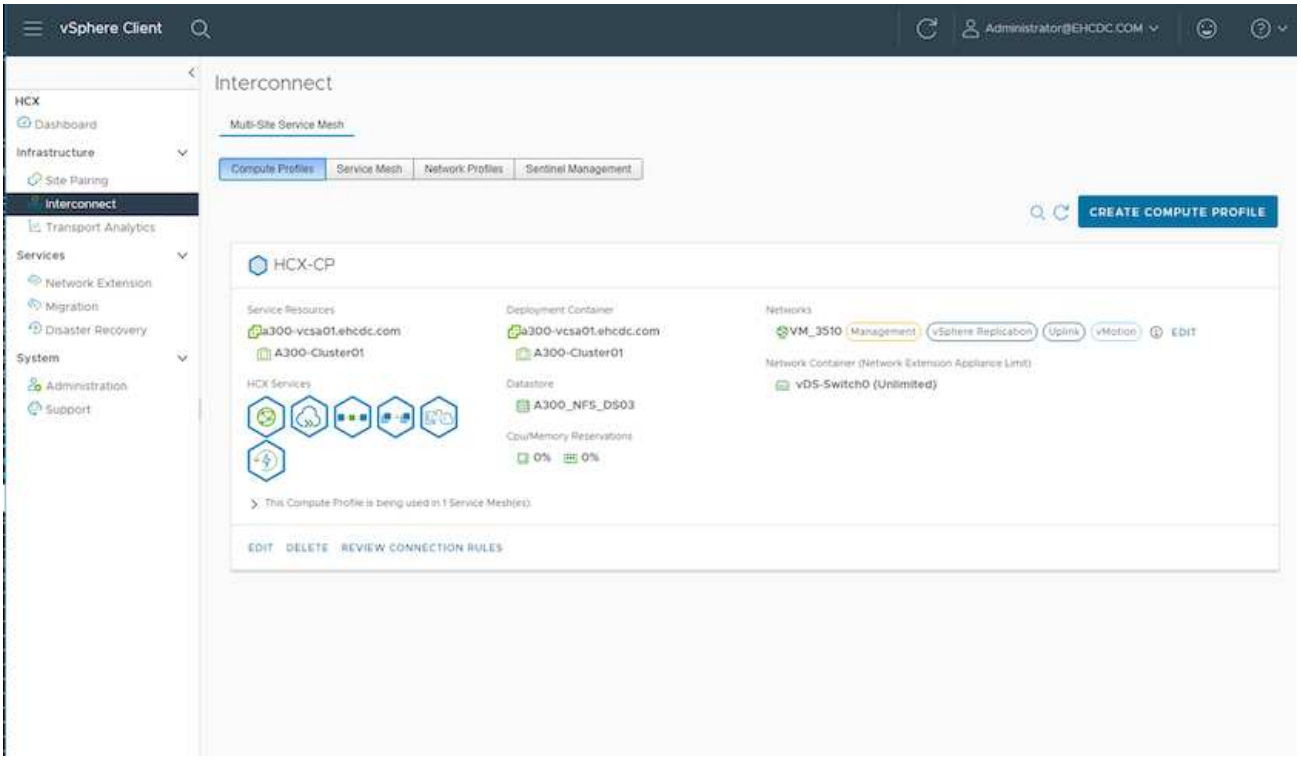


▼ 步骤 **5**：配置网络配置文件、计算配置文件和服务网格

VMware HCX Interconnect 服务设备通过互联网和与目标站点的专用连接提供复制和基于 vMotion 的迁移功能。互连提供加密、流量工程和 VM 移动性。要创建互连服务设备，请完成以下步骤：

1. 在基础设施下，选择*互连>多站点服务网格>计算配置文件>创建计算配置文件*。

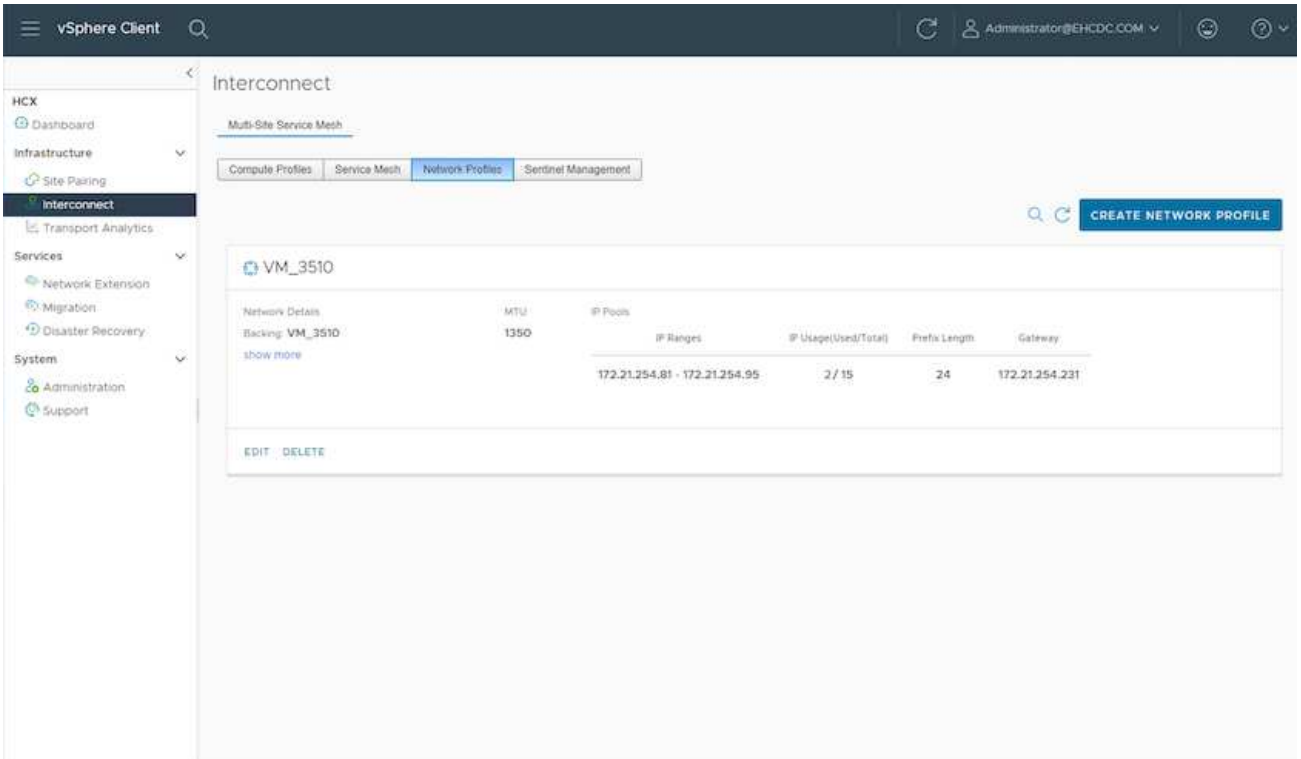
> 计算配置文件定义部署参数，包括部署的设备以及 VMware 数据中心的哪些部分可供 HCX 服务访问。



2. 创建计算配置文件后，通过选择“多站点服务网格”>“网络配置文件”>“创建网络配置文件”来创建网络配置文件。

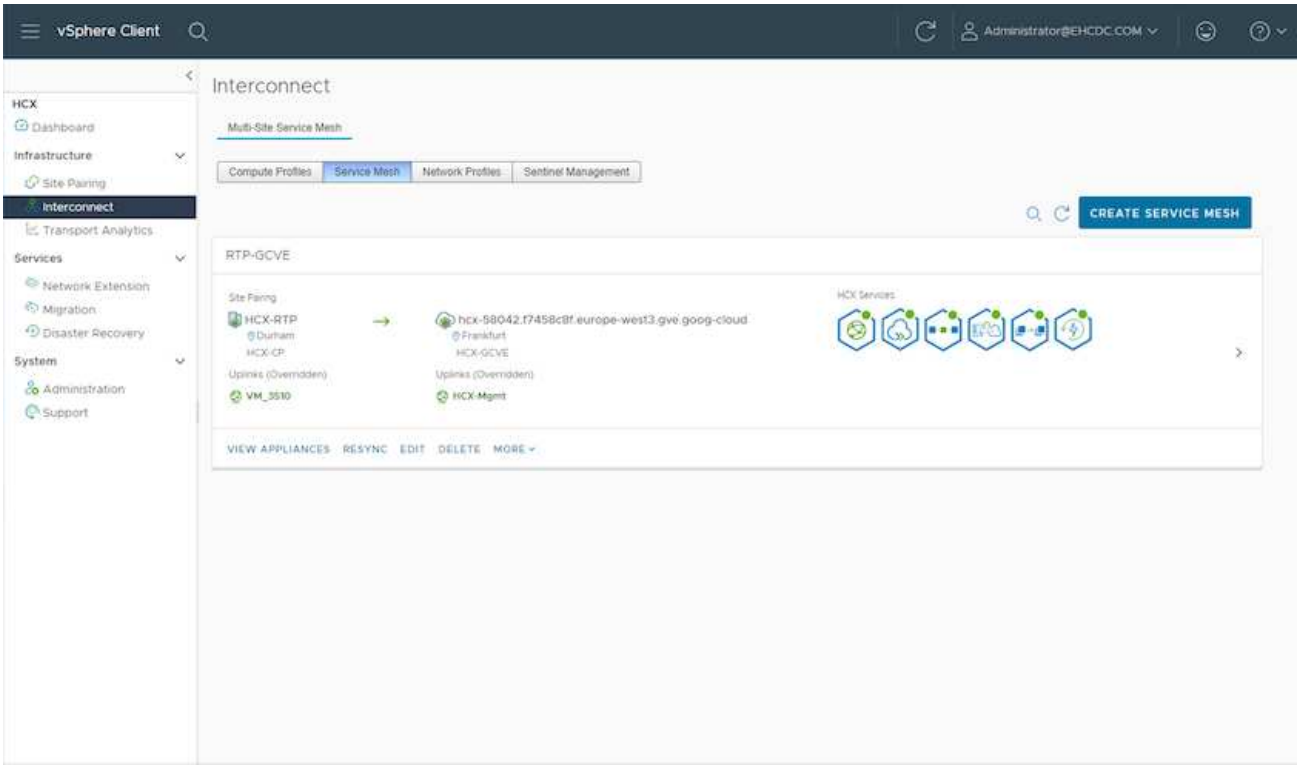
网络配置文件定义了 HCX 用于其虚拟设备的一系列 IP 地址和网络。

此步骤需要两个或更多 IP 地址。这些 IP 地址由管理网络分配给互连设备。

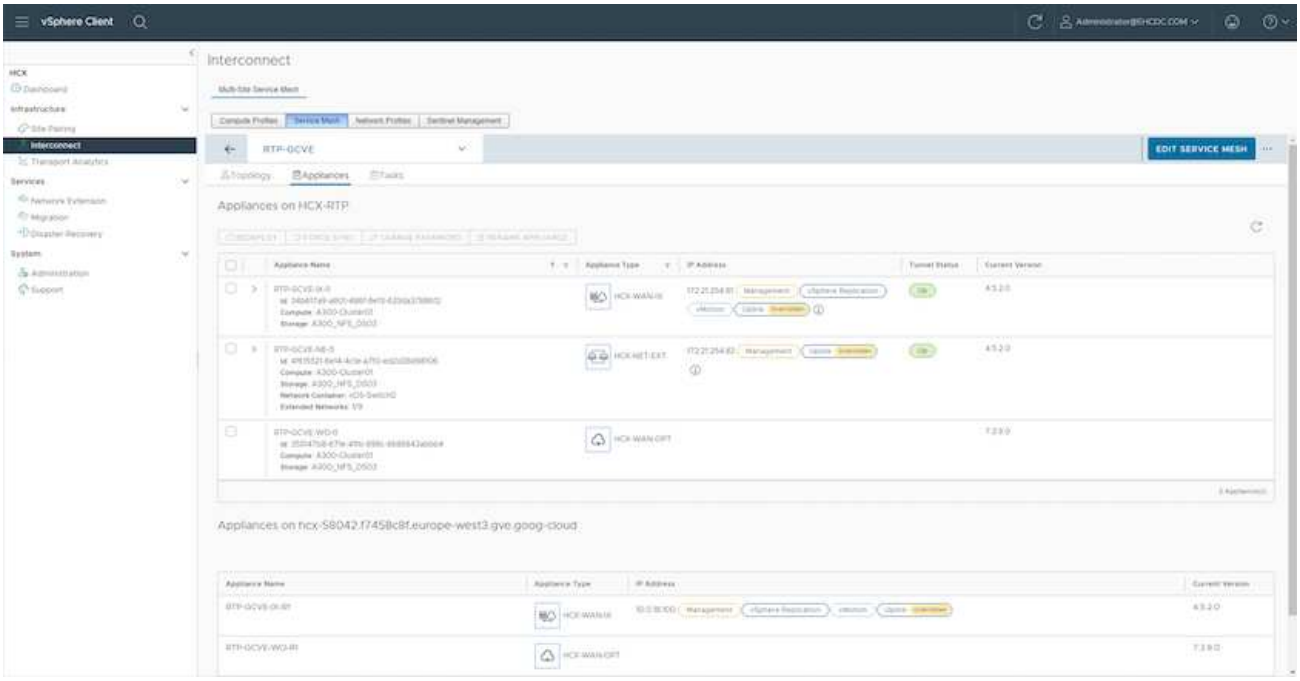


3. 此时，计算和网络配置文件已成功创建。
4. 通过选择“**Interconnect**”选项中的“**Service Mesh**”选项卡来创建服务网格，并选择本地和 GCVE SDDC 站点。
5. 服务网格指定本地和远程计算和网络配置文件对。

> 作为此过程的一部分，HCX 设备在源站点和目标站点上部署并自动配置，以创建安全的传输结构。



6. 这是配置的最后一步。完成部署大约需要 30 分钟。配置服务网格后，环境已准备就绪，并且已成功创建 IPsec 隧道来迁移工作负载虚拟机。



▼ 步骤 **6**：迁移工作负载

可以使用各种 VMware HCX 迁移技术在本地和 GCVE SDDC 之间双向迁移工作负载。可以使用多种迁移技术将虚拟机移至 VMware HCX 激活的实体或从中移出，例如 HCX 批量迁移、HCX vMotion、HCX 冷迁移、HCX 复制辅助 vMotion（HCX 企业版提供）和 HCX OS 辅助迁移（HCX 企业版提供）。

要了解有关各种 HCX 迁移机制的更多信息，请参阅 "使用 VMware HCX 文档迁移 VMware VM"。

HCX-IX 设备使用移动代理服务执行 vMotion、Cold 和复制辅助 vMotion (RAV) 迁移。

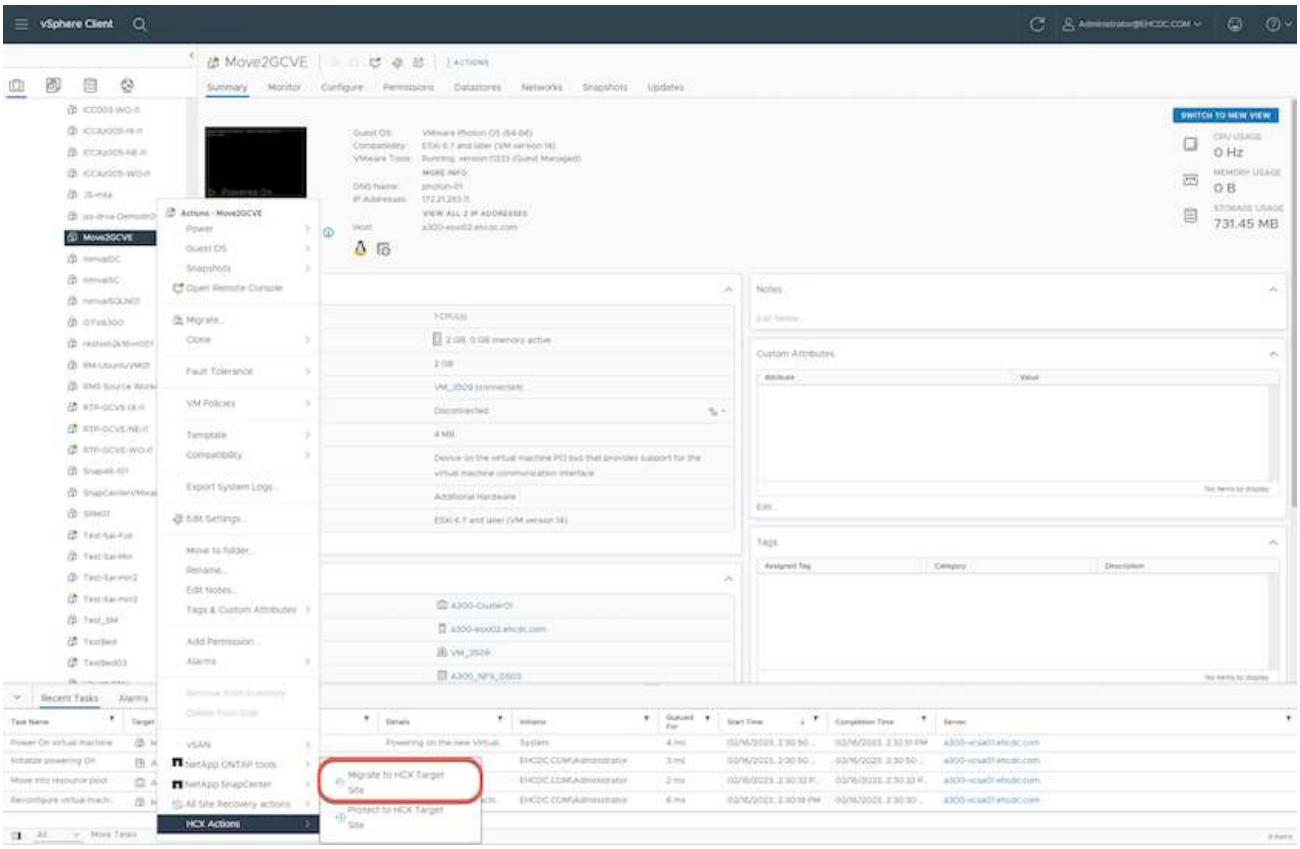
HCX-IX 设备将移动代理服务添加为 vCenter Server 中的主机对象。此对象上显示的处理器、内存、存储和网络资源并不代表托管 IX 设备的物理虚拟机管理程序上的实际消耗。

HCX vMotion

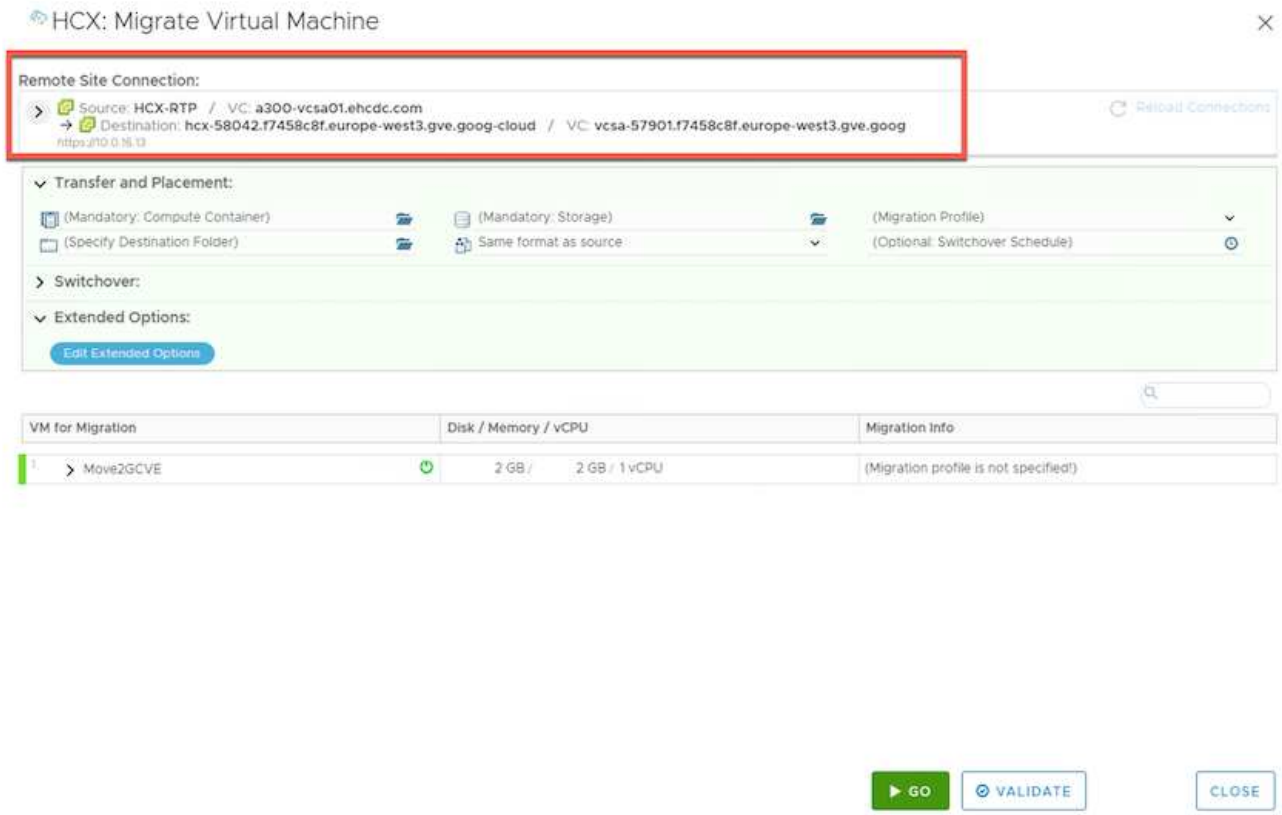
本节介绍 HCX vMotion 机制。该迁移技术使用 VMware vMotion 协议将虚拟机迁移到 GCVE。 vMotion 迁移选项用于一次迁移单个 VM 的 VM 状态。此迁移方法期间不会中断服务。

应该实施网络扩展（针对虚拟机所连接的端口组），以便迁移虚拟机而无需更改 IP 地址。

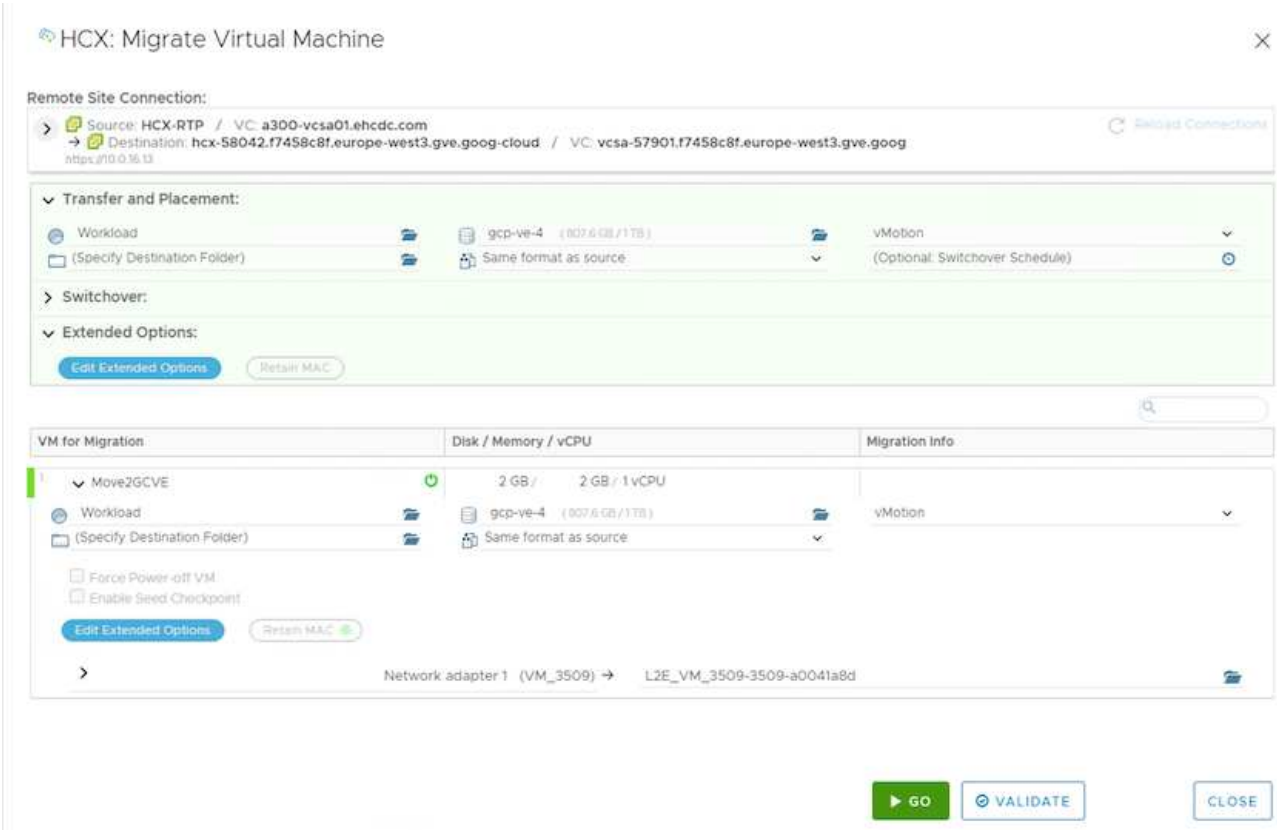
1. 从本地 vSphere 客户端，转到“清单”，右键单击要迁移的虚拟机，然后选择“HCX 操作”>“迁移到 HCX 目标站点”。



2. 在迁移虚拟机向导中，选择远程站点连接（目标 GCVE）。



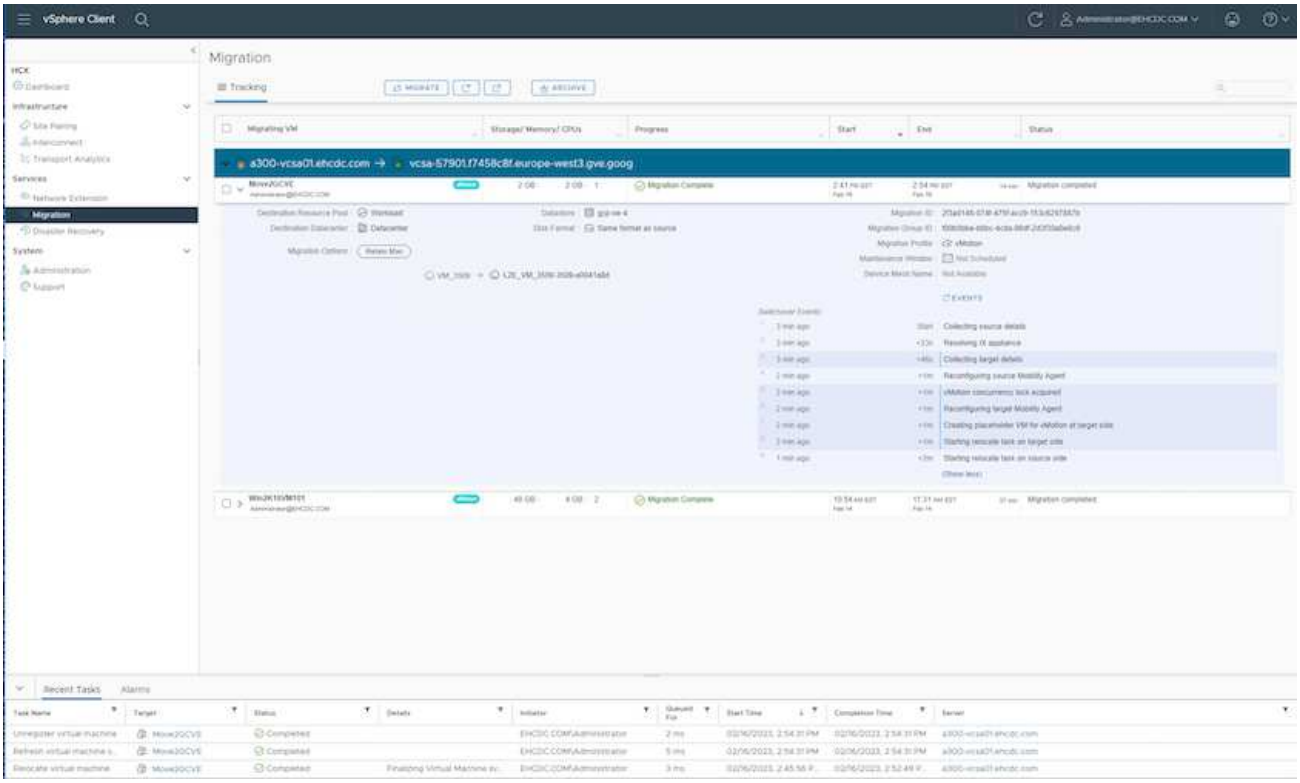
3. 更新必填字段（集群、存储和目标网络），单击验证。



4. 验证检查完成后，单击“Go”开始迁移。

> vMotion 传输捕获 VM 活动内存、其执行状态、其 IP 地址和其 MAC 地址。有关 HCX vMotion 的要求和限制的更多信息，请参阅 "了解 VMware HCX vMotion 和冷迁移"。

5. 您可以从 HCX > 迁移仪表板监控 vMotion 的进度和完成情况。



目标Google Cloud NetApp Volumes （NetApp Volumes）NFS 数据存储应具有足够的空间来处理迁移。

结束语

无论您的目标是全云还是混合云，以及驻留在本地任何类型/供应商存储上的数据，Cloud Volume Service 和 HCX 都提供了部署和迁移应用程序工作负载的绝佳选择，同时通过使数据需求无缝连接到应用程序层来降低 TCO。无论用例如何，选择 Google Cloud VMware Engine 以及 Cloud Volume Service 都可以快速实现云优势、跨本地和多云的一致基础架构和操作、工作负载的双向可移植性以及企业级容量和性能。使用 VMware vSphere Replication、VMware vMotion 甚至网络文件复制 (NFC) 连接存储和迁移虚拟机所使用的过程和程序相同。

总结

该文件的要点包括：

- 您现在可以将 Cloud Volume Service 用作 Google Cloud VMware Engine SDDC 上的数据存储。
- 您可以轻松地将数据从本地迁移到 Cloud Volume Service 数据存储。
- 您可以轻松扩大或缩小 Cloud Volume Service 数据存储以满足迁移活动期间的容量和性能要求。

参考 **Google** 和 **VMware** 的视频

▼ 来自谷歌

- "使用 GCVE 部署 HCX 连接器"
- "使用 GCVE 配置 HCX ServiceMesh"
- "将带有 HCX 的虚拟机迁移到 GCVE"

▼ 来自 **VMware**

- "适用于 GCVE 的 HCX 连接器部署"
- "GCVE 的 HCX ServiceMesh 配置"
- "HCX 工作负载迁移至 GCVE"

在哪里可以找到更多信息

要了解有关本文档中描述的信息的更多信息，请参阅以下网站链接：

- Google Cloud VMware Engine 文档

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service 文档

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- VMware HCX 用户指南

  "https://docs.vmware.com/en/VMware-HCX/index.html"

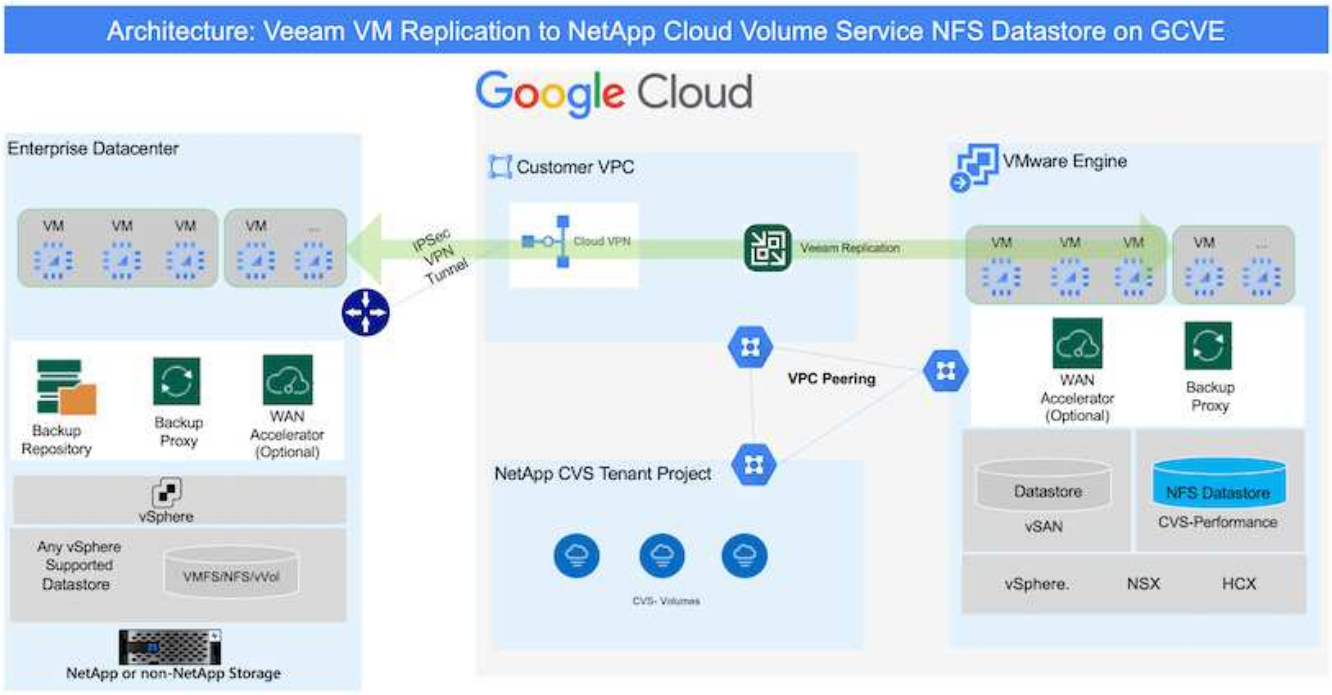
使用 **Veeam Replication** 功能将虚拟机迁移到 **Google Cloud VMware Engine** 上的**Google Cloud NetApp Volumes NFS** 数据存储区

目前使用 Veeam 满足数据保护需求的客户可以继续使用该解决方案将工作负载迁移到 GCVE，并享受Google Cloud NetApp Volumes NFS 数据存储区带来的好处。

概述

利用 Veeam Replication 功能可以将 VMware vSphere 上运行的虚拟机工作负载迁移到 Google Cloud VMware Engine (GCVE)。

本文档提供了使用Google Cloud NetApp Volumes、Veeam 和 Google Cloud VMware Engine (GCVE) 设置和执行 VM 迁移的分步方法。



假设

本文档假设您已安装 Google Cloud VPN 或 Cloud Interconnect 或其他网络选项，以建立从现有 vSphere 服务器到 Google Cloud VMware Engine 的网络连接。

> 将本地数据中心连接到 Google Cloud 有多种选择，因此我们无法在本文档中概述特定的工作流程。请参阅"Google Cloud 文档"以找到适当的本地到 Google 连接方法。

部署迁移解决方案

解决方案部署概述

1. 确保Google Cloud NetApp Volumes的 NFS 数据存储已安装在 GCVE vCenter 上。
2. 确保 Veeam Backup Recovery 部署在现有 VMware vSphere 环境中
3. 创建复制作业以开始将虚拟机复制到 Google Cloud VMware Engine 实例。
4. 执行 Veeam 复制作业的故障转移。
5. 在 Veeam 上执行永久故障转移。

部署详情

确保**Google Cloud NetApp Volumes**中的 **NFS** 数据存储已安装在 **GCVE vCenter** 上

登录 GCVE vCenter 并确保有足够空间的 NFS 数据存储可用。如果没有，请参阅"将NetApp卷挂载为 GCVE 上的 NFS 数据存储"

确保 **Veeam Backup Recovery** 部署在现有 **VMware vSphere** 环境中

请参考"Veeam 复制组件"安装所需组件的文档。

创建复制作业以开始将虚拟机复制到 **Google Cloud VMware Engine** 实例。

本地 vCenter 和 GCVE vCenter 都需要在 Veeam 中注册。"设置 vSphere VM 复制作业"这是一个视频，解释了如何"配置复制作业"。

> 副本虚拟机可以具有与源虚拟机不同的 IP，也可以连接到不同的端口组。欲了解更多详情，请查看上面的视频。

执行 **Veeam** 复制作业的故障转移

要迁移虚拟机，请执行"执行故障转移"

在 **Veeam** 上执行永久故障转移。

要将 GCVE 视为新的源环境，请执行"永久故障转移"

此解决方案的优势

- 现有的 Veeam 备份基础架构可用于迁移。
- Veeam Replication 允许更改目标站点上的 VM IP 地址。
- 能够重新映射在 Veeam 之外复制的现有数据（如 NetApp 系统的复制数据）
- 能够在目标站点上指定不同的网络端口组。
- 可以指定虚拟机的启动顺序。
- 利用 VMware 变更块跟踪来最大限度地减少通过 WAN 发送的数据量。
- 能够执行复制的前脚本和后脚本。
- 能够执行快照的前脚本和后脚本。

使用Google Cloud NetApp Volumes保护 Google Cloud 中的数据

TR-4918：安全概览 **- Google Cloud** 中的**Google Cloud NetApp Volumes**

Oliver Krause、Justin Parisi、 NetApp

安全性，特别是在基础架构不受存储管理员控制的云环境中，对于放心地将数据交由云提供商提供的服务产品至关重要。本文档概述了 "Google Cloud NetApp Volumes在 Google Cloud 中提供"提供的安全产品。

目标受众

本文档的目标受众包括但不限于以下角色：

- 云提供商
- 存储管理员
- 存储架构师
- 现场资源

- 商业决策者

如果您对本技术报告的内容有任何疑问，请参阅"联系我们。"

缩写	定义
NetApp卷-SW	Google Cloud NetApp Volumes，服务类型NetApp Volumes
NetApp卷性能	云卷服务，服务类型NetApp卷 - 性能
变压吸附	

Google Cloud 中的**Google Cloud NetApp Volumes**如何保护您的数据

Google Cloud 中的Google Cloud NetApp Volumes提供了多种方式来原生保护您的数据。

安全架构和租赁模型

Google Cloud NetApp Volumes通过将服务管理（控制平面）和数据访问（数据平面）划分到不同的端点，从而相互之间不会产生影响，从而在 Google Cloud 中提供安全架构（请参阅"Google Cloud NetApp Volumes架构"）。它使用谷歌的 "私人服务访问"（PSA）框架来提供服务。该框架区分了服务生产者（由NetApp提供和运营）和服务消费者（客户项目中的虚拟私有云 (VPC)，用于托管想要访问Google Cloud NetApp Volumes文件共享的客户端）。

在此架构中，租户（参见"租赁模型"）被定义为除非用户明确连接，否则彼此完全隔离的 Google Cloud 项目。租户可以使用Google Cloud NetApp Volumes卷平台将数据卷、外部名称服务以及解决方案的其他重要部分与其他租户完全隔离。由于Google Cloud NetApp Volumes平台通过 VPC 对等连接，因此这种隔离也适用于它。您可以使用共享 VPC 在多个项目之间共享Google Cloud NetApp Volumes卷（请参阅"共享 VPC"）。您可以对 SMB 共享和 NFS 导出应用访问控制，以限制谁或什么可以查看或修改数据集。

控制平面的强大身份管理

在进行Google Cloud NetApp Volumes配置的控制平面中，身份管理通过使用 "身份访问管理 (IAM)"。 IAM 是一项标准服务，可让您控制对 Google Cloud 项目实例的身份验证（登录）和授权（权限）。所有配置均通过使用 TLS 1.2 加密的安全 HTTPS 传输使用Google Cloud NetApp Volumes API 执行，并使用 JWT 令牌执行身份验证以增强安全性。 Google Cloud NetApp Volumes的 Google 控制台 UI 将用户输入转换为Google Cloud NetApp Volumes API 调用。

安全强化——限制攻击面

有效安全的一部分是限制服务中可用的攻击面数量。攻击面可以包括各种各样的东西，包括静态数据、动态传输数据、登录数据和数据集本身。

托管服务消除了其设计中固有的一些攻击面。基础设施管理，如本节所述"服务运营，"由专门的团队处理并实现自动化，以减少人工实际接触配置的次数，从而有助于减少有意和无意的错误。网络被隔离，以便只有必要的服务才能相互访问。加密已融入数据存储中，只有数据平面需要Google Cloud NetApp Volumes管理员的安全关注。通过将大部分管理隐藏在 API 接口后面，可以通过限制攻击面来实现安全性。

零信任模型

从历史上看，IT 安全理念一直是信任但要验证，并表现为仅依靠外部机制（如防火墙和入侵检测系统）来减轻威胁。然而，攻击和入侵已经演化成通过网络钓鱼、社会工程、内部威胁和其他提供验证的方法来绕过环境中的验证，从而进入网络并造成破坏。

零信任已成为安全领域的一种新方法，其当前的口号是“不信任任何事物，但仍然验证一切”。因此，默认情况下不允许任何内容访问。这一口号通过多种方式得到执行，包括标准防火墙和入侵检测系统 (IDS)，以及以下方法：

- 强身份验证方法（例如 AES 加密的 Kerberos 或 JWT 令牌）
- 单一强大的身份来源（例如 Windows Active Directory、轻量级目录访问协议 (LDAP) 和 Google IAM）
- 网络分段和安全多租户（默认情况下只允许租户访问）
- 使用最小特权访问策略进行细粒度访问控制
- 拥有专门的、值得信赖的管理员的小型独家名单，具有数字审计和纸质记录

在 Google Cloud 中运行的Google Cloud NetApp Volumes通过实施“不信任任何事物，验证一切”的立场来遵循零信任模型。

加密

加密静态数据（请参阅"静态数据加密") 通过使用 XTS-AES-256 密码与NetApp卷加密 (NVE) 以及"SMB 加密"或 NFS Kerberos 5p 支持。请放心，跨区域复制传输受到 TLS 1.2 加密的保护（请参阅部分链接：gcp-gcnv-security-considerations.html#Detection, Prevention and mitigation of ransomware, Malware, and viral#cross-region-replication["Cross-region replication"]）。此外，Google 网络还提供加密通信（请参阅"传输中的数据加密") 来增加一层防御攻击的保护。有关传输加密的更多信息，请参阅"Google Cloud 网络"。

数据保护和备份

安全不仅仅意味着预防攻击。它还涉及我们如何在攻击发生时恢复。该策略包括数据保护和备份。 Google Cloud NetApp Volumes提供了在发生中断时复制到其他区域的方法（请参阅"跨区域复制"）或者数据集是否受到勒索软件攻击的影响。它还可以通过以下方式将数据异步备份到Google Cloud NetApp Volumes实例之外的位置："Google Cloud NetApp Volumes备份" 。通过定期备份，缓解安全事件可以花费更少的时间，并为管理员节省金钱和精力。

利用行业领先的 **Snapshot** 副本快速缓解勒索软件

除了数据保护和备份之外， Google Cloud NetApp Volumes还支持不可变的 Snapshot 副本（请参阅"不可变的 Snapshot 副本"）允许从勒索软件攻击中恢复的卷（请参阅"服务运营") 在发现问题后的几秒钟内就能解决问题，并且干扰最小。恢复时间和效果取决于 Snapshot 计划，但您可以创建在勒索软件攻击中提供仅一小时增量的 Snapshot 副本。快照副本对性能和容量使用的影响可以忽略不计，并且是一种保护数据集的低风险、高回报的方法。

安全考虑和攻击面

了解如何保护数据的第一步是识别风险和潜在的攻击面。

这些包括（但不限于）以下内容：

- 管理和登录
- 静态数据
- 飞行中的数据
- 网络和防火墙
- 勒索软件、恶意软件和病毒

了解攻击面可以帮助您更好地保护您的环境。 Google Cloud 中的Google Cloud NetApp Volumes已经考虑了许多此类主题，并默认实现了安全功能，无需任何管理交互。

确保安全登录

在保护关键基础设施组件时，必须确保只有经过批准的用户才能登录和管理您的环境。如果不法分子破坏了您的管理凭证，那么他们就拥有了城堡的钥匙，可以做任何他们想做的事情 - 更改配置、删除卷和备份、创建后门或禁用快照计划。

Google Cloud NetApp Volumes for Google Cloud 通过混淆存储即服务 (StaaS) 来防止未经授权的管理登录。Google Cloud NetApp Volumes完全由云提供商维护，无法从外部登录。所有设置和配置操作都是完全自动化的，因此除了极少数情况外，人工管理员无需与系统进行交互。

如果需要登录，Google Cloud 中的Google Cloud NetApp Volumes通过维护一个有权登录系统的受信任管理员的极短列表来确保登录安全。这种把关有助于减少有访问权限的潜在不良行为者的数量。此外，Google Cloud 网络将系统隐藏在多层网络安全之后，只向外界公开所需的内容。有关 Google Cloud、 Google Cloud NetApp Volumes架构的信息，请参阅"Google Cloud NetApp Volumes架构。"

集群管理和升级

存在潜在安全风险的两个领域包括集群管理（如果不良行为者拥有管理员访问权限会发生什么情况）和升级（如果软件映像被泄露会发生什么情况）。

存储管理保护

作为服务提供的存储通过删除云数据中心之外的最终用户的访问权限，消除了管理员面临的额外风险。相反，唯一完成的配置是针对客户的数据访问平面。每个租户管理自己的卷，并且没有租户可以访问其他Google Cloud NetApp Volumes实例。该服务由自动化管理，只有极少数受信任的管理员可以通过本节介绍的流程访问系统"服務運作。"

NetApp Volumes-Performance 服务类型提供跨区域复制选项，以便在发生区域故障时为不同区域提供数据保护。在这些情况下， Google Cloud NetApp Volumes可以故障转移到未受影响的区域以维持数据访问。

服务升级

更新有助于保护易受攻击的系统。每次更新都提供安全性增强和错误修复，以最大限度地减少攻击面。软件更新从集中式存储库下载，并在允许更新之前进行验证，以验证是否使用了官方映像以及升级是否未被不良行为者破坏。

使用Google Cloud NetApp Volumes，更新由云提供商团队处理，通过提供精通配置和升级的专家（这些专家已经对流程进行了自动化和全面测试），从而消除了管理员团队的风险敞口。升级不会造成中断，并且Google Cloud NetApp Volumes会维护最新更新以获得最佳整体效果。

有关执行这些服务升级的管理员团队的信息，请参阅"服務運作。"

保护静态数据

当磁盘被盗、被退回或被重新利用时，静态数据加密对于保护敏感数据非常重要。 Google Cloud NetApp Volumes中的数据通过使用基于软件的加密进行静态保护。

- Google 生成的密钥用于NetApp Volumes-SW。
- 对于NetApp Volumes-Performance，每个卷的密钥都存储在Google Cloud NetApp Volumes内置的密钥管理器中，该管理器使用NetApp ONTAP CryptoMod 生成 AES-256 加密密钥。 CryptoMod 列在 CMVP FIPS

140-2 验证模块列表中。看 "FIPS 140-2 证书 #4144"。

从 2021 年 11 月开始，预览版客户管理加密 (CMEK) 功能已为NetApp Volumes-Performance 提供。此功能允许您使用托管在 Google 密钥管理服务 (KMS) 中的每个项目、每个区域的主密钥加密每个卷的密钥。 KMS 使您能够附加外部密钥管理器。

有关如何为 NetApp Volumes-Performance 配置 KMS 的详细信息， "请参阅Google Cloud NetApp Volumes文档"。

有关架构的更多信息，请参阅"Google Cloud NetApp Volumes架构。"

确保传输中的数据安全

除了保护静态数据之外，您还必须能够保护在Google Cloud NetApp Volumes实例和客户端或复制目标之间传输的数据。 Google Cloud NetApp Volumes使用加密方法（例如使用 Kerberos 的 SMB 加密、数据包的签名/密封以及用于数据传输端到端加密的 NFS Kerberos 5p）为通过 NAS 协议传输的数据提供加密。

Google Cloud NetApp Volumes卷的复制使用 TLS 1.2，它利用了 AES-GCM 加密方法。

大多数不安全的运行中协议（如 telnet、NDMP 等）默认都是禁用的。但是，DNS 并未由Google Cloud NetApp Volumes加密（不支持 DNS Sec），因此应尽可能使用外部网络加密进行加密。请参阅"传输中的数据加密"有关保护传输中数据的更多信息。

有关 NAS 协议加密的信息，请参阅"NAS 协议。"

NAS 权限的用户和组

保护云中数据安全的一部分涉及正确的用户和组身份验证，其中访问数据的用户被验证为环境中的真实用户，并且组包含有效用户。这些用户和组提供初始共享和导出访问权限，以及存储系统中文件和文件夹的权限验证。

Google Cloud NetApp Volumes使用基于标准 Active Directory 的 Windows 用户和组身份验证来实现 SMB 共享和 Windows 风格的权限。该服务还可以利用 UNIX 身份提供程序，例如用于 UNIX 用户和组的 LDAP，以进行 NFS 导出、NFSv4 ID 验证、Kerberos 身份验证和 NFSv4 ACL。

目前， Google Cloud NetApp Volumes仅支持 Active Directory LDAP 的 LDAP 功能。

检测、预防和缓解勒索软件、恶意软件和病毒

勒索软件、恶意软件和病毒对管理员来说是一个持续的威胁，检测、预防和缓解这些威胁始终是企业组织的首要任务。针对关键数据集的一次勒索软件事件就可能造成数百万美元的损失，因此尽最大努力将风险降至最低是有益的。

虽然 Google Cloud NetApp Volumes 目前不包括本机检测或预防措施，例如防病毒保护或 "自动勒索软件检测"，但可以通过启用常规快照计划来快速从勒索软件事件中恢复。快照副本是不可变的只读指针，指向文件系统中已更改的块，近乎即时，对性能影响极小，并且仅在数据更改或删除时才占用空间。您可以为快照副本设置计划，以满足所需的可接受恢复点目标 （RPO）/恢复时间目标 （RTO），每个卷最多可保留 1,024 个快照副本。

Google Cloud NetApp Volumes提供免费的快照支持（除了 Snapshot 副本保留的更改块/数据的数据存储费用之外），并且在发生勒索软件攻击时，可用于回滚到攻击发生之前的 Snapshot 副本。快照恢复只需几秒钟即可完成，然后您就可以恢复正常提供数据。有关更多信息，请参阅 "NetApp勒索软件解决方案" 。

防止勒索软件影响您的业务需要采取多层次的方法，包括以下一项或多项措施：

- 端点保护
- 通过网络防火墙防御外部威胁
- 数据异常检测
- 关键数据集的多重备份（现场和异地）
- 定期对备份进行恢复测试
- 不可变的只读NetApp Snapshot 副本
- 关键基础设施的多因素身份验证
- 系统登录安全审计

此列表远非详尽无遗，但在处理潜在的勒索软件攻击时，它是一个很好的蓝图。 Google Cloud 中的Google Cloud NetApp Volumes提供了多种方法来防范勒索软件事件并减少其影响。

不可变的 **Snapshot** 副本

Google Cloud NetApp Volumes本身提供不可变的只读 Snapshot 副本，这些副本按照可自定义的时间表进行，以便在数据删除或整个卷受到勒索软件攻击时快速进行时间点恢复。 Snapshot 恢复到以前的良好 Snapshot 副本速度很快，并且可以根据 Snapshot 计划和 RTO/RPO 的保留期最大限度地减少数据丢失。 Snapshot 技术对性能的影响微乎其微。

由于Google Cloud NetApp Volumes中的 Snapshot 副本是只读的，因此它们不会被勒索软件感染，除非勒索软件在不知不觉中扩散到数据集中，并且已经从受勒索软件感染的数据中获取了 Snapshot 副本。这就是为什么您还必须考虑基于数据异常的勒索软件检测。 Google Cloud NetApp Volumes目前不提供原生检测，但您可以使用外部监控软件。

备份和恢复

Google Cloud NetApp Volumes提供标准 NAS 客户端备份功能（例如通过 NFS 或 SMB 进行备份）。

- NetApp Volumes-Performance 提供到其他 NetApp Volumes-Performance 卷的跨区域卷复制。有关详细信息，请参见 Google Cloud NetApp Volumes 文档中的 "卷复制"。
- NetApp Volumes-SW 提供服务原生卷备份/恢复功能。有关详细信息，请参见 "云备份" Google Cloud NetApp Volumes 文档。

卷复制提供了源卷的精确副本，以便在发生灾难（包括勒索软件事件）时实现快速故障转移。

跨区域复制

NetApp Volumes-Performance 使您能够在NetApp控制的后端服务网络上使用 TLS1.2 AES 256 GCM 加密，使用在 Google 网络上运行的用于复制的特定接口，安全地跨 Google Cloud 区域复制卷以进行数据保护和存档用例。主（源）卷包含活动生产数据，并复制到辅助（目标）卷以提供主数据集的精确副本。

初始复制传输所有块，但更新仅传输主卷中更改的块。例如，如果将位于主卷上的 1TB 数据库复制到辅助卷，则在初始复制时会传输 1TB 的空间。如果该数据库在初始化和下次更新之间有几百行（假设几 MB）发生变化，则只有包含已更改行的块才会复制到辅助数据库（几 MB）。这有助于确保传输时间保持较低水平并降低复制费用。

文件和文件夹的所有权限都复制到辅助卷，但共享访问权限（例如导出策略和规则或 SMB 共享和共享 ACL）必须单独处理。在发生站点故障转移的情况下，目标站点应利用相同的名称服务和 Active Directory 域连接来提供

对用户和组身份和权限的一致处理。您可以通过中断复制关系（将辅助卷转换为读写关系）在发生灾难时将辅助卷用作故障转移目标。

卷副本是只读的，它提供了异地数据的不可变副本，以便在病毒感染数据或勒索软件加密主数据集的情况下快速恢复数据。只读数据不会被加密，但是，如果主卷受到影响并发生复制，则受感染的块也会复制。您可以使用较旧的、未受影响的 Snapshot 副本进行恢复，但根据检测到攻击的速度，SLA 可能会超出承诺的 RTO/RPO 范围。

此外，您可以使用 Google Cloud 中的跨区域复制（CRR）管理来防止恶意管理操作，例如卷删除、Snapshot 删除或 Snapshot 计划更改。这是通过创建自定义角色来实现的，这些角色将卷管理员（可以删除源卷但不能中断镜像，因此无法删除目标卷）与 CRR 管理员（不能执行任何卷操作）区分开来。有关每个管理员组允许的权限，请参阅 Google Cloud NetApp Volumes 文档中的 "安全注意事项"。

Google Cloud NetApp Volumes备份

尽管Google Cloud NetApp Volumes提供了高数据持久性，但外部事件可能会导致数据丢失。如果发生病毒或勒索软件等安全事件，备份和恢复对于及时恢复数据访问至关重要。管理员可能会意外删除Google Cloud NetApp Volumes卷。或者用户只是想将其数据的备份版本保留数月，而保留卷内的额外 Snapshot 副本空间则成为一项成本挑战。尽管 Snapshot 副本应该是保留过去几周的备份版本以从中恢复丢失数据的首选方式，但它们位于卷内，如果卷消失，它们也会丢失。

由于所有这些原因，Google Cloud NetApp Volumes 通过 "Google Cloud NetApp Volumes备份"提供备份服务。

Google Cloud NetApp Volumes备份会在 Google Cloud Storage (GCS) 上生成该卷的副本。它仅备份卷内存储的实际数据，而不是可用空间。它永远以增量方式工作，这意味着它传输一次卷内容，然后从那时起继续仅备份更改的数据。与具有多次完整备份的传统备份概念相比，它节省了大量的备份存储，从而降低了成本。由于备份空间的月费与卷相比较低，因此它是长期保存备份版本的理想场所。

用户可以使用Google Cloud NetApp Volumes备份将任何备份版本恢复到同一区域内的相同或不同卷。如果删除源卷，备份数据将保留，并且需要单独管理（例如，删除）。

Google Cloud NetApp Volumes 备份作为选项内置于 Google Cloud NetApp Volumes 中。用户可以按卷激活 Google Cloud NetApp Volumes 备份，以决定要保护哪些卷。请参阅 "Google Cloud NetApp Volumes备份文档"，了解有关备份、 "支持的最大备份版本数量"、计划和 "定价"的信息。

项目的所有备份数据都存储在 GCS 存储桶中，该存储桶由服务管理，用户不可见。每个项目使用不同的存储桶。目前，这些存储桶与Google Cloud NetApp Volumes卷位于同一区域，但正在讨论更多选项。查阅文档以了解最新状态。

从Google Cloud NetApp Volumes存储桶到 GCS 的数据传输使用带有 HTTPS 和 TLS1.2 的服务内部 Google 网络。数据使用 Google 管理的密钥进行静态加密。

要管理 Google Cloud NetApp Volumes 备份（创建、删除和还原备份），用户必须具有 "roles/netapp.admin"角色。

概述

信任云解决方案的一部分是了解其架构及其安全方式。本节介绍了 Google 中Google Cloud NetApp Volumes架构的不同方面，以帮助缓解有关数据安全方式的潜在担忧，并指出可能需要额外配置步骤才能获得最安全部署的区域。

Google Cloud NetApp Volumes的总体架构可以分为两个主要组件：控制平面和数据平面。

控制平面

Google Cloud NetApp Volumes中的控制平面是由Google Cloud NetApp Volumes管理员和NetApp原生自动化软件管理的后端基础架构。该平面对最终用户完全透明，包括网络、存储硬件、软件更新等，以帮助为Google Cloud NetApp Volumes等云驻留解决方案提供价值。

数据平面

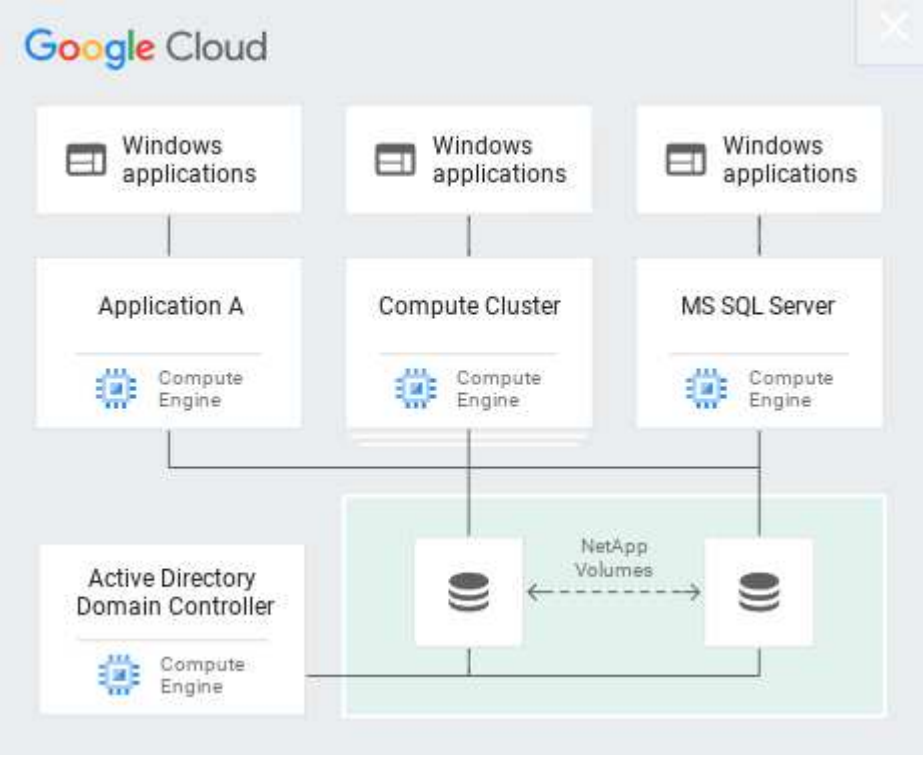
Google Cloud NetApp Volumes中的数据平面包括实际数据卷和整体Google Cloud NetApp Volumes配置（例如访问控制、Kerberos 身份验证等）。数据平面完全由Google Cloud NetApp Volumes平台的最终用户和消费者控制。

每架飞机的安全和管理方式都有明显差异。以下部分将介绍这些差异，首先介绍Google Cloud NetApp Volumes架构概述。

Google Cloud NetApp Volumes架构

与 CloudSQL、Google Cloud VMware Engine (GCVE) 和 FileStore 等其他 Google Cloud 原生服务类似， Google Cloud NetApp Volumes使用 "谷歌公益广告"来提供服务。在 PSA 中，服务是在服务生产者项目内部构建的，该项目使用 "VPC 网络对等连接"连接到服务消费者。服务生产者由NetApp提供和运营，服务消费者是客户项目中的 VPC，托管想要访问Google Cloud NetApp Volumes文件共享的客户端。

下图引用自 "Google Cloud NetApp Volumes 文档"，展示了高级视图。



虚线上方部分显示了服务的控制平面，它控制着卷的生命周期。虚线以下部分表示数据平面。左边蓝色框表示用户VPC（服务消费者），右边蓝色框表示NetApp提供的服务生产者。两者通过 VPC 对等连接。

在Google Cloud NetApp Volumes中，单个项目被视为唯一的租户。这意味着对卷、Snapshot 副本等的操作都是基于每个项目执行的。换句话说，所有卷都归创建它们的项目所有，并且默认情况下只有该项目可以管理和访问其中的数据。这被认为是服务的控制平面视图。

共享 **VPC**

在数据平面视图上， Google Cloud NetApp Volumes可以连接到共享 VPC。您可以在托管项目或连接到共享 VPC 的某个服务项目中创建卷。连接到该共享 VPC 的所有项目（主机或服务）都能够访问网络层（TCP/IP）的卷。由于共享 VPC 上具有网络连接的所有客户端都可以通过 NAS 协议访问数据，因此必须使用单个卷上的访问控制（例如用户/组访问控制列表 (ACL) 和 NFS 导出的主机名/IP 地址）来控制谁可以访问数据。

每个客户项目最多可以将Google Cloud NetApp Volumes连接到五个 VPC。在控制平面上，该项目使您能够管理所有创建的卷，无论它们连接到哪个 VPC。数据平面上，VPC之间相互隔离，每个卷只能连接到一个VPC。

对各个卷的访问由特定协议（NFS/SMB）访问控制机制控制。

换句话说，在网络层，所有连接到共享 VPC 的项目都能够看到该卷，而在管理端，控制平面只允许所有者项目看到该卷。

VPC 服务控制

VPC 服务控制在连接到互联网且可在全球范围内访问的 Google Cloud 服务周围建立访问控制边界。这些服务通过用户身份提供访问控制，但无法限制请求来自哪个网络位置。 VPC 服务控制通过引入限制对定义网络的访问的功能来弥补这一差距。

Google Cloud NetApp Volumes数据平面未连接到外部互联网，而是连接到具有明确定义的网络边界（周边）的私有 VPC。在该网络中，每个卷都使用特定于协议的访问控制。任何外部网络连接均由 Google Cloud 项目管理员明确创建。然而，控制平面不提供与数据平面相同的保护，任何人都可以从任何地方通过有效凭证进行访问（"JWT 令牌"）。

简而言之， Google Cloud NetApp Volumes数据平面提供了网络访问控制功能，而无需支持 VPC Service Controls，也不明确使用 VPC Service Controls。

数据包嗅探/跟踪注意事项

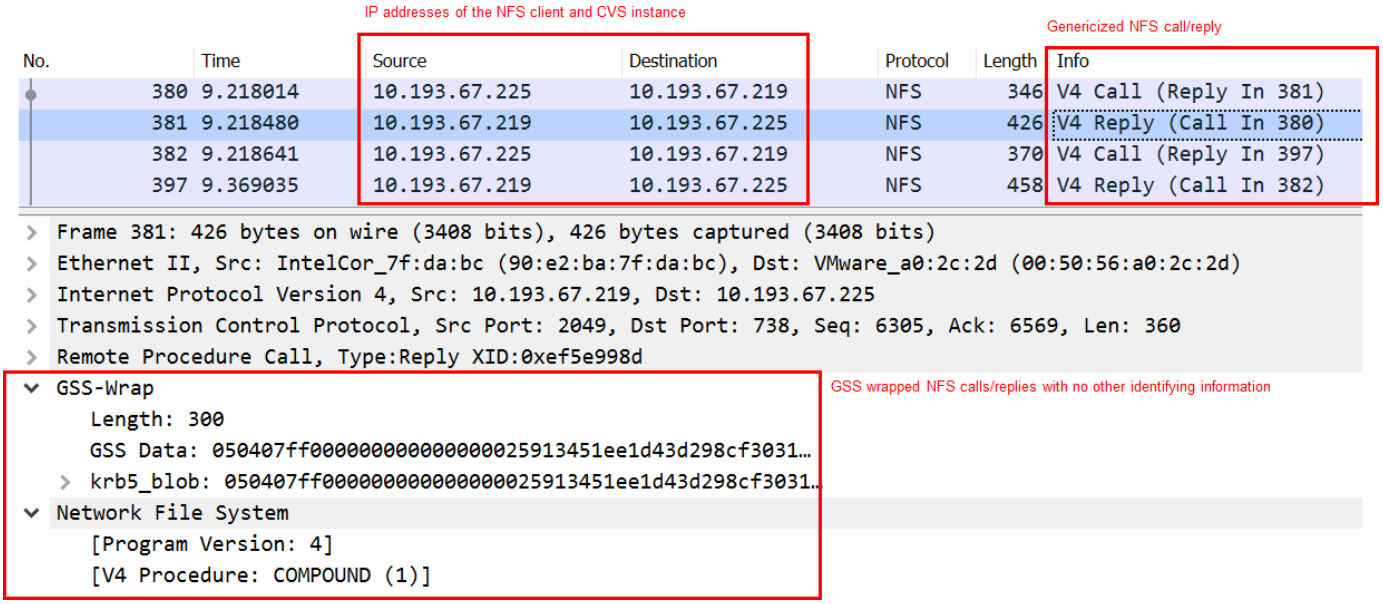
数据包捕获可用于解决网络问题或其他问题（例如 NAS 权限、LDAP 连接等），但也可能被恶意用于获取有关网络 IP 地址、MAC 地址、用户和组名称以及端点上使用的安全级别的信息。由于 Google Cloud 网络、VPC 和防火墙规则的配置方式，如果没有用户登录凭据或"JWT 令牌"进入云实例。数据包捕获仅可在端点（例如虚拟机 (VM)）上进行，并且仅可在 VPC 内部的端点上进行，除非使用共享 VPC 和/或外部网络隧道/IP 转发明确允许外部流量到端点。没有办法嗅探客户端之外的流量。

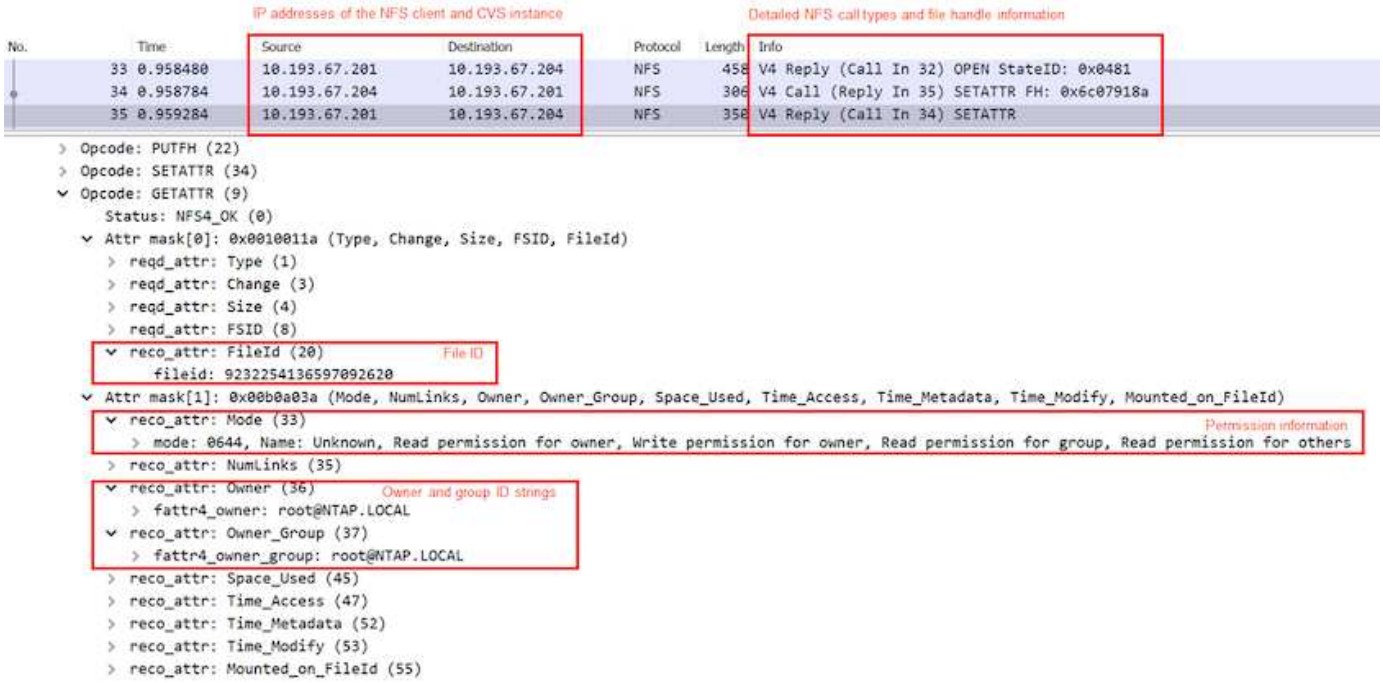
使用共享 VPC 时，使用 NFS Kerberos 和/或"SMB 加密"可以掩盖从痕迹中收集到的大量信息。然而，有些流量仍然以明文形式发送，例如"DNS"和"LDAP 查询"。下图显示了来自Google Cloud NetApp Volumes的纯文本 LDAP 查询的数据包捕获以及可能暴露的识别信息。 Google Cloud NetApp Volumes中的 LDAP 查询目前不支持加密或 LDAP over SSL。如果 Active Directory 要求， NetApp Volumes-Performance 支持 LDAP 签名。 NetApp Volumes-SW 不支持 LDAP 签名。



unixUserPassword 由 LDAP 查询，并且不是以纯文本形式发送，而是以加盐哈希形式发送。默认情况下，Windows LDAP 不会填充 unixUserPassword 字段。仅当您需要利用 Windows LDAP 通过 LDAP 交互式登录到客户端时才需要此字段。 Google Cloud NetApp Volumes不支持实例的交互式 LDAP 登录。

下图显示了从 NFS Kerberos 对话捕获的数据包以及通过 AUTH_SYS 捕获的 NFS 数据包。请注意两者之间跟踪中可用的信息有何不同，以及启用飞行中加密如何为 NAS 流量提供更高的整体安全性。





虚拟机网络接口

攻击者可能会尝试的一个技巧是向虚拟机添加新的网络接口卡 (NIC) "混杂模式" （端口镜像）或在现有 NIC 上启用混杂模式以嗅探所有流量。在 Google Cloud 中，添加新的 NIC 需要完全关闭 VM，这会创建警报，因此攻击者无法不被注意地执行此操作。

此外，NIC 根本无法设置为混杂模式，否则会在 Google Cloud 中触发警报。

控制平面架构

对Google Cloud NetApp Volumes 的所有管理操作均通过 API 完成。集成到 GCP Cloud Console 中的Google Cloud NetApp Volumes管理也使用Google Cloud NetApp Volumes API。

身份和访问管理

身份和访问管理("我是") 是一项标准服务，可让您控制对 Google Cloud 项目实例的身份验证（登录）和授权（权限）。 Google IAM 提供权限授权和删除的完整审计跟踪。目前， Google Cloud NetApp Volumes不提供控制平面审计。

授权/许可概述

IAM 为 Google Cloud NetApp Volumes 提供内置的精细权限。您可以找到 "此处有详细的权限完整列表"。

IAM 还提供了两个预定义角色，称为 `netappcloudvolumes.admin`和 `netappcloudvolumes.viewer`。这些角色可以分配给特定用户或服务帐户。

分配适当的角色和权限以允许 IAM 用户管理Google Cloud NetApp Volumes。

使用细粒度权限的示例包括：

- 构建仅具有获取/列出/创建/更新权限的自定义角色，以便用户无法删除卷。
- 使用仅具有 `snapshot.*`创建用于构建应用程序一致的快照集成的服务帐户的权限。
- 构建自定义角色以进行委派 `volumereplication.*`针对特定用户。

服务帐户

通过脚本Google Cloud NetApp Volumes "地形"，您必须使用 `roles/netappcloudvolumes.admin`角色。您可以使用此服务帐户以两种不同的方式生成验证Google Cloud NetApp Volumes API 请求所需的 JWT 令牌：

- 生成 JSON 密钥并使用 Google API 从中派生出 JWT 令牌。这是最简单的方法，但它涉及手动机密（JSON 密钥）管理。
- 使用 "服务帐户模拟"和 `roles/iam.serviceAccountTokenCreator`。代码（脚本、Terraform 等）运行 "应用程序默认凭证"并模拟服务帐户以获取其权限。这种方法体现了 Google 安全最佳实践。

有关详细信息，请参见 Google 云文档中的 "创建您的服务帐户和私钥"。

Google Cloud NetApp VolumesAPI

Google Cloud NetApp Volumes API 使用基于 REST 的 API，并使用 HTTPS (TLSv1.2) 作为底层网络传输。您可以在 "Google 云文档中的 Cloud Volumes API"找到最新的 API 定义以及有关如何使用该 API 的信息。

NetApp使用标准 HTTPS（TLSv1.2）功能来操作和保护 API 端点。

JWT 令牌

使用 JWT 承载令牌执行 API 身份验证("RFC-7519"）。必须使用 Google Cloud IAM 身份验证获取有效的 JWT 令牌。这必须通过提供服务帐户 JSON 密钥从 IAM 获取令牌来完成。

审计日志

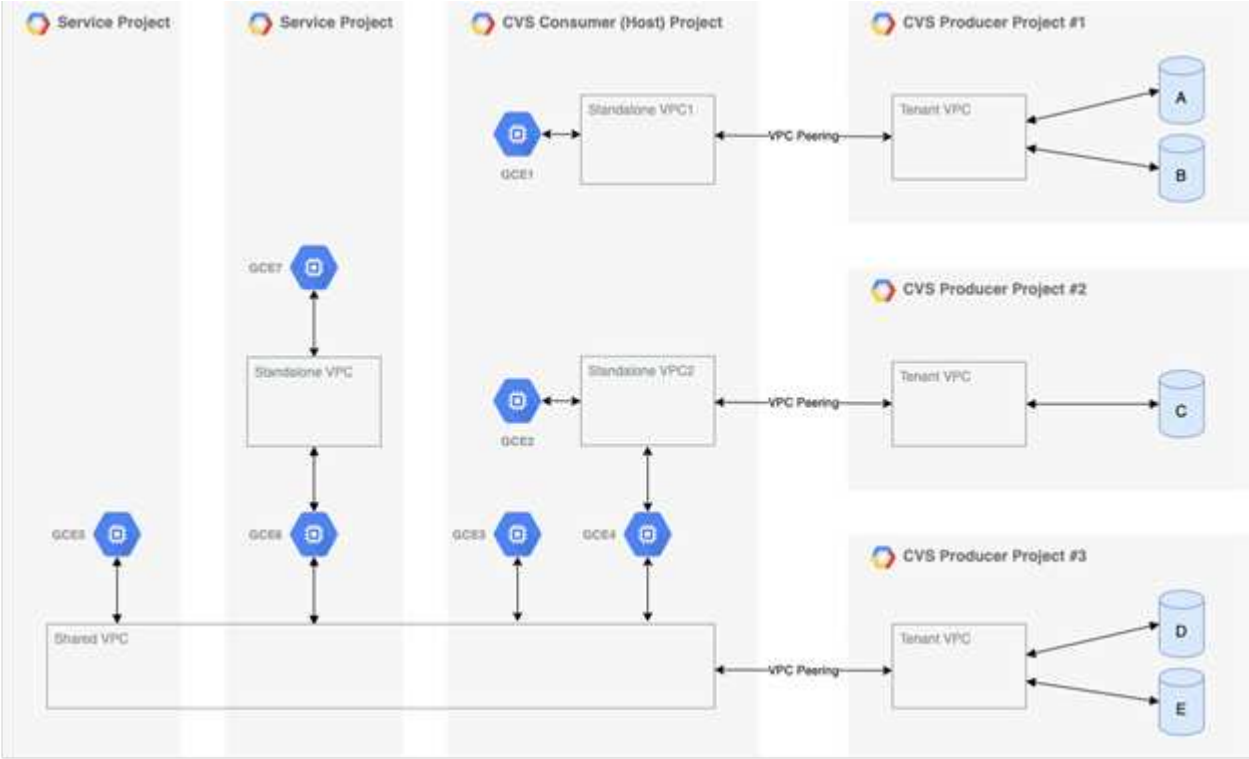
目前，没有可供用户访问的控制平面审计日志。

数据平面架构

Google Cloud NetApp Volumes for Google Cloud 利用 Google Cloud "私人服务访问"框架。在这个框架中，用户可以连接到Google Cloud NetApp Volumes。该框架像其他 Google Cloud 服务一样使用服务网络和 VPC 对等结构，确保租户之间的完全隔离。

有关适用于 Google Cloud 的 Google Cloud NetApp Volumes 的架构概述，请参见 "Google Cloud NetApp Volumes的架构"。

用户 VPC（独立或共享）与托管卷的Google Cloud NetApp Volumes管理租户项目内的 VPC 对等。



上图展示了一个项目（中间的NetApp Volumes 消费者项目），其中有三个 VPC 网络连接到Google Cloud NetApp Volumes，并且多个 Compute Engine VM（GCE1-7）共享卷：

- VPC1 允许 GCE1 访问卷 A 和 B。
- VPC2 允许 GCE2 和 GCE4 访问卷 C。
- 第三个VPC网络是共享VPC，由两个服务项目共享。它允许 GCE3、GCE4、GCE5 和 GCE6 访问卷 D 和 E。共享 VPC 网络仅支持NetApp Volumes-Performance 服务类型的卷。

GCE7 无法访问任何卷。

数据可以在Google Cloud NetApp Volumes中传输（使用 Kerberos 和/或 SMB 加密）和静止时进行加密。

传输中的数据加密

传输中的数据可以在 NAS 协议层加密，并且 Google Cloud 网络本身也经过加密，如以下部分所述。

Google Cloud 网络

Google Cloud 在网络级别加密流量，具体说明如下 "传输中加密"在 Google 文档中。正如“Google Cloud NetApp Volumes架构”部分所述， Google Cloud NetApp Volumes是由NetApp控制的 PSA 生产商项目提供的。

对于NetApp Volumes-SW，生产者租户运行 Google VM 来提供服务。用户虚拟机和Google Cloud NetApp Volumes虚拟机之间的流量由 Google 自动加密。

尽管NetApp Volumes-Performance 的数据路径在网络层上并未完全加密，但NetApp和 Google 结合使用 "IEEE 802.1AE 加密 (MACSec)"， "封装" （数据加密）和物理受限的网络来保护Google Cloud NetApp Volumes NetApp Volumes-Performance 服务类型和 Google Cloud 之间传输的数据。

NAS 协议

NFS 和 SMB NAS 协议在协议层提供可选的传输加密。

SMB 加密

"SMB 加密"提供 SMB 数据的端到端加密，并保护数据免受不受信任网络上的窃听。您可以为客户端/服务器数据连接（仅适用于支持 SMB3.x 的客户端）和服务器/域控制器身份验证启用加密。

启用 SMB 加密后，不支持加密的客户端无法访问共享。

Google Cloud NetApp Volumes支持用于 SMB 加密的 RC4-HMAC、AES-128-CTS-HMAC-SHA1 和 AES-256-CTS-HMAC-SHA1 安全密码。 SMB 协商服务器支持的最高加密类型。

NFSv4.1 Kerberos

对于 NFSv4.1， NetApp Volumes-Performance 提供 Kerberos 身份验证，如 "RFC7530"。您可以按卷启用 Kerberos。

Kerberos 目前最强大的加密类型是 AES-256-CTS-HMAC-SHA1。 Google Cloud NetApp Volumes支持 NFS 的 AES-256-CTS-HMAC-SHA1、AES-128-CTS-HMAC-SHA1、DES3 和 DES。它还支持 CIFS/SMB 流量的 ARCFOUR-HMAC (RC4)，但不支持 NFS。

Kerberos 为 NFS 挂载提供了三种不同的安全级别，可供您选择 Kerberos 安全性的强度。

根据 RedHat 的 "常见安装选项"文档：

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

一般来说，Kerberos 安全级别要做的工作越多，性能就越差，因为客户端和服务器要花时间对发送的每个数据包进行加密和解密 NFS 操作。许多客户端和 NFS 服务器都支持将 AES-NI 卸载到 CPU 以获得更好的整体体验，但 Kerberos 5p（完全端到端加密）对性能的影响明显大于 Kerberos 5（用户身份验证）的影响。

下表显示了每个级别在安全性和性能方面的差异。

安全级别	安全性	性能
NFSv3—系统	• 最不安全；带有数字用户 ID/组 ID 的纯文本 • 能够在数据包捕获中查看UID、GID、客户端IP地址、导出路径、文件名、权限	• 最适合大多数情况

安全级别	安全性	性能
NFSv4.x—系统	• 比 NFSv3 更安全（客户端 ID、名称字符串/域字符串匹配），但仍然是纯文本 • 能够查看数据包捕获中的 UID 、GID、客户端 IP 地址、名称字符串、域 ID、导出路径、文件名、权限	• 适用于顺序工作负载（例如虚拟机、数据库、大文件） • 文件数量多/元数据多时效果不佳（差 30-50%）
NFS—krb5	• 对每个 NFS 数据包中的凭证进行 Kerberos 加密 - 在 GSS 包装器中包装 RPC 调用中用户/组的 UID/GID • 请求访问挂载的用户需要有效的 Kerberos 票证（通过用户名/密码或手动密钥标签交换）；票证在指定时间段后过期，用户必须重新进行身份验证才能访问 • NFS 操作或辅助协议（如 mount/portmapper/nlm）没有加密（可以在数据包捕获中查看导出路径、IP 地址、文件句柄、权限、文件名、atime/mtime）	• 在大多数情况下，Kerberos 是最好的；比 AUTH_SYS 差
NFS—krb5i	• 对每个 NFS 数据包中的凭证进行 Kerberos 加密 - 在 GSS 包装器中包装 RPC 调用中用户/组的 UID/GID • 请求访问挂载的用户需要有效的 Kerberos 票证（通过用户名/密码或手动密钥标签交换）；票证在指定时间段后过期，用户必须重新进行身份验证才能访问 • NFS 操作或辅助协议（如 mount/portmapper/nlm）没有加密（可以在数据包捕获中查看导出路径、IP 地址、文件句柄、权限、文件名、atime/mtime） • 每个数据包都添加了 Kerberos GSS 校验和，以确保没有任何东西拦截数据包。如果校验和匹配，则允许对话。	• 比 krb5p 更好，因为 NFS 有效负载未加密；与 krb5 相比唯一增加的开销是完整性校验和。krb5i 的性能不会比 krb5 差太多，但会有一些下降。

安全级别	安全性	性能
NFS – krb5p	• 对每个 NFS 数据包中的凭证进行 Kerberos 加密 - 在 GSS 包装器中包装 RPC 调用中用户/组的 UID/GID • 请求访问挂载的用户需要有效的 Kerberos 票证（通过用户名/密码或手动密钥表交换）；票证在指定时间段后过期，用户必须重新进行身份验证才能访问 • 所有 NFS 数据包有效负载都使用 GSS 包装器加密（在数据包捕获中看不到文件句柄、权限、文件名、atime/mtime）。 • 包括完整性检查。 • NFS 操作类型可见（FSINFO 、ACCESS、GETATTR 等）。 • 辅助协议（mount、portmap 、nlm 等）未加密 - （可以看到导出路径、IP 地址）	• 安全级别性能最差；krb5p 必须进行更多加密/解密。 • 对于高文件数工作负载，性能比使用 NFSv4.x 的 krb5p 更好。

在Google Cloud NetApp Volumes中，配置的 Active Directory 服务器用作 Kerberos 服务器和 LDAP 服务器（从 RFC2307 兼容模式中查找用户身份）。不支持其他 Kerberos 或 LDAP 服务器。 NetApp强烈建议您在Google Cloud NetApp Volumes中使用 LDAP 进行身份管理。有关 NFS Kerberos 在数据包捕获中如何显示的信息，请参阅部分 "Packet sniffing/trace considers."

静态数据加密

Google Cloud NetApp Volumes中的所有卷均使用 AES-256 加密进行静态加密，这意味着写入媒体的所有用户数据都经过加密，并且只能使用每个卷的密钥解密。

- 对于NetApp Volumes-SW，使用 Google 生成的密钥。
- 对于NetApp Volumes-Performance，每个卷的密钥都存储在Google Cloud NetApp Volumes内置的密钥管理器中。

从 2021 年 11 月开始，预览客户管理加密密钥 (CMEK) 功能已推出。这使得您可以使用托管在以下位置的每个项目、每个区域的主密钥来加密每个卷密钥： "Google 密钥管理服务 (KMS)。" KMS 使您能够附加外部密钥管理器。

有关为 NetApp Volumes-Performance 配置 KMS 的信息，请参见 "设置客户管理的加密密钥"。

防火墙

Google Cloud NetApp Volumes公开多个 TCP 端口来为 NFS 和 SMB 共享提供服务：

- "NFS 访问所需的端口"
- "SMB 访问所需的端口"

此外，SMB、具有 LDAP（包括 Kerberos）的 NFS 和双协议配置都需要访问 Windows Active Directory 域。Active Directory 连接必须 "配置"基于每个区域。Active Directory 域控制器（DC）是通过使用 "基于 DNS 的 DC 发现"并使用指定的 DNS 服务器来标识的。将使用返回的任何 DC。可以通过指定 Active Directory 站点来限制符合条件的 DC 列表。

Google Cloud NetApp Volumes 使用通过 `gcloud compute address`命令分配的 CIDR 范围中的 IP 地址进行访问，同时 "加入Google Cloud NetApp Volumes"。您可以将此 CIDR 用作源地址，以配置 Active Directory 域控制器的入站防火墙。

Active Directory 域控制器必须 "如此处所述，将端口暴露给Google Cloud NetApp Volumes CIDR"。

NAS 协议概述

NAS 协议包括 NFS（v3 和 v4.1）和 SMB/CIFS（2.x 和 3.x）。这些协议是NetApp Volumes 允许跨多个 NAS 客户端共享访问数据的方式。此外， Google Cloud NetApp Volumes可以同时提供对 NFS 和 SMB/CIFS 客户端的访问（双协议），同时遵守 NAS 共享中文件和文件夹的所有身份和权限设置。为了保持最高的数据传输安全性， Google Cloud NetApp Volumes支持使用 SMB 加密和 NFS Kerberos 5p 进行飞行中的协议加密。

双协议仅适用于NetApp Volumes-Performance。

NAS 协议基础知识

NAS 协议是网络上的多个客户端访问存储系统上的相同数据的方式，例如 GCP 上的Google Cloud NetApp Volumes 。 NFS 和 SMB 是定义的 NAS 协议，在客户端/服务器基础上运行，其中Google Cloud NetApp Volumes充当服务器。客户端向服务器发送访问、读取和写入请求，服务器负责协调文件的锁定机制、存储权限以及处理身份和身份验证请求。

例如，如果 NAS 客户端想要在文件夹中创建新文件，则遵循以下一般流程。

1. 客户端向服务器询问有关目录的信息（权限、所有者、组、文件 ID、可用空间等）；如果请求的客户端和用户对父文件夹具有必要的权限，则服务器会响应该信息。
2. 如果目录的权限允许访问，客户端就会询问服务器正在创建的文件名是否已经存在于文件系统中。如果文件名已被使用，则创建失败。如果文件名不存在，服务器会让客户端知道可以继续。
3. 客户端向服务器发出调用，使用目录句柄和文件名创建文件，并设置访问和修改时间。服务器为文件发出唯一的文件 ID，以确保没有其他文件使用相同的文件 ID 创建。
4. 客户端在 WRITE 操作之前发送调用来检查文件属性。如果权限允许，客户端就会写入新文件。如果协议/应用程序使用了锁定，客户端会向服务器请求锁定，以防止其他客户端在锁定时访问文件，从而防止数据损坏。

NFS

NFS 是一种分布式文件系统协议，它是请求评论 (RFC) 中定义的开放 IETF 标准，允许任何人实现该协议。

Google Cloud NetApp Volumes中的卷通过导出客户端或一组客户端可访问的路径共享给 NFS 客户端。安装这些导出的权限由导出策略和规则定义，可由Google Cloud NetApp Volumes管理员配置。

NetApp NFS 实施被认为是该协议的黄金标准，并被应用于无数企业 NAS 环境中。以下部分介绍Google Cloud NetApp Volumes中提供的 NFS 和特定安全功能及其实现方式。

默认本地 UNIX 用户和组

Google Cloud NetApp Volumes包含几个用于各种基本功能的默认 UNIX 用户和组。目前无法修改或删除这些用户和组。目前无法将新的本地用户和组添加到Google Cloud NetApp Volumes。默认用户和组之外的 UNIX 用户和组需要由外部 LDAP 名称服务提供。

下表显示了默认用户和组及其对应的数字 ID。 NetApp建议不要在 LDAP 中或重复使用这些数字 ID 的本地客户端上创建新的用户或组。

默认用户：数字 ID	默认组：数字 ID
• 根：0 • pcuser：65534 • 无人：65535	• 根：0 • 守护进程：1 • pcuser：65534 • 无人：65535

使用 NFSv4.1 时，在 NFS 客户端上运行目录列表命令时，root 用户可能会显示为 nobody。这是由于客户端的ID域映射配置造成的。请参阅名为NFSv4.1 和 nobody 用户/组有关此问题及其解决方法的详细信息。

根用户

在 Linux 中，root 帐户可以访问基于 Linux 的文件系统中所有命令、文件和文件夹。由于此帐户的强大功能，安全最佳实践通常要求以某种方式禁用或限制根用户。在 NFS 导出中，可以通过导出策略和规则以及称为 root squash 的概念在Google Cloud NetApp Volumes中控制 root 用户对文件和文件夹的权限。

Root 压缩确保访问 NFS 挂载的 root 用户被压缩为匿名数字用户 65534（请参阅“[匿名用户] "），目前仅在使用NetApp Volumes-Performance 时可用，方法是在创建导出策略规则期间选择关闭 root 访问权限。如果 root 用户被压缩为匿名用户，则它不再具有运行 chown 或 "setuid/setgid 命令（粘滞位）"在 NFS 挂载中的文件或文件夹上，以及由 root 用户创建的文件或文件夹显示匿名 UID 作为所有者/组。此外，root 用户无法修改 NFSv4 ACL。但是，root 用户仍然可以访问 chmod 并删除其没有明确权限的文件。如果要限制对 root 用户的文件和文件夹权限的访问，请考虑使用具有 NTFS ACL 的卷，创建名为 `root`并将所需的权限应用到文件或文件夹。

匿名用户

匿名 (anon) 用户 ID 指定映射到没有有效 NFS 凭据的客户端请求的 UNIX 用户 ID 或用户名。当使用 root 压缩时，这可以包括 root 用户。 Google Cloud NetApp Volumes中的匿名用户是 65534。

此 UID 通常与用户名相关联 `nobody`或者 `nfsnobody`在 Linux 环境中。 Google Cloud NetApp Volumes也使用 65534 作为本地 UNIX 用户 `pcuser（请参阅“默认本地 UNIX 用户和组 "），当在 LDAP 中找不到有效匹配的 UNIX 用户时，它也是 Windows 到 UNIX 名称映射的默认后备用户。

由于 Linux 和Google Cloud NetApp Volumes中 UID 65534 的用户名存在差异，因此使用 NFSv4.1 时映射到 65534 的用户的名称字符串可能不匹配。因此，你可能会看到 `nobody`作为某些文件和文件夹的用户。请参阅“NFSv4.1 和 nobody 用户/组 “以获取有关此问题及其解决方法的信息。

访问控制/导出

NFS 挂载的初始导出/共享访问通过导出策略中包含的基于主机的导出策略规则进行控制。定义主机 IP、主机名、子网、网络组或域以允许访问挂载 NFS 共享以及允许对主机的访问级别。导出策略规则配置选项取决于Google Cloud NetApp Volumes级别。

对于NetApp Volumes-SW，以下选项可用于导出策略配置：

- *客户匹配。*以逗号分隔的 IP 地址列表、以逗号分隔的主机名、子网、网络组、域名列表。
- *RO/RW 访问规则。*选择读/写或只读来控制导出的访问级别。NetApp NetApp -Performance 提供以下选项：
- *客户匹配。*以逗号分隔的 IP 地址列表、以逗号分隔的主机名、子网、网络组、域名列表。
- *RO/RW 访问规则。*选择读/写或只读来控制导出的访问级别。
- *Root 访问权限（开/关）。*配置根壁球（参见“[根用户] ”以了解详情）。
- *协议类型。*这会将对 NFS 挂载的访问限制到特定的协议版本。当为卷同时指定 NFSv3 和 NFSv4.1 时，请将两者留空或选中两个框。
- *Kerberos 安全级别（选择“启用 Kerberos”时）。*提供 krb5、krb5i 和/或 krb5p 选项以进行只读或读写访问。

更改所有权（**chown**）和更改组（**chgrp**）

Google Cloud NetApp Volumes上的 NFS 仅允许 root 用户对文件和文件夹运行 chown/chgrp。其他用户看到 `Operation not permitted`错误——即使是他们自己的文件。如果你使用根南瓜（如“[根用户] "），root 被压缩为非 root 用户，并且不允许访问 chown 和 chgrp。目前， Google Cloud NetApp Volumes中没有允许非 root 用户使用 chown 和 chgrp 的解决方法。如果需要更改所有权，请考虑使用双协议卷并将安全样式设置为 NTFS 以从 Windows 端控制权限。

权限管理

Google Cloud NetApp Volumes支持模式位（例如 rwx 的 644、777 等）和 NFSv4.1 ACL，以控制使用 UNIX 安全样式的卷的 NFS 客户端权限。这些使用标准权限管理（例如 chmod、chown 或 nfs4_setfacl）并可与任何支持它们的 Linux 客户端一起使用。

此外，当使用设置为 NTFS 的双协议卷时，NFS 客户端可以利用Google Cloud NetApp Volumes名称映射到 Windows 用户，然后用于解析 NTFS 权限。这需要与Google Cloud NetApp Volumes建立 LDAP 连接以提供数字 ID 到用户名的转换，因为Google Cloud NetApp Volumes需要有效的 UNIX 用户名才能正确映射到 Windows 用户名。

为 **NFSv3** 提供细粒度的 **ACL**

模式位权限在语义上仅涵盖所有者、组和其他所有人 - 这意味着基本 NFSv3 没有细粒度的用户访问控制。Google Cloud NetApp Volumes不支持 POSIX ACL 和扩展属性（例如 chattr），因此细粒度 ACL 仅在以下使用 NFSv3 的场景中可用：

- 具有有效 UNIX 到 Windows 用户映射的 NTFS 安全样式卷（需要 CIFS 服务器）。
- 使用安装 NFSv4.1 的管理客户端应用 NFSv4.1 ACL 来应用 ACL。

两种方法都需要 LDAP 连接来进行 UNIX 身份管理，并填充有效的 UNIX 用户和组信息（请参阅"LDAP") 并且仅适用于NetApp Volumes-Performance 实例。要将 NTFS 安全样式卷与 NFS 一起使用，您必须使用双协议（SMB 和 NFSv3）或双协议（SMB 和 NFSv4.1），即使没有建立 SMB 连接。要将 NFSv4.1 ACL 与 NFSv3

挂载一起使用，您必须选择 `Both (NFSv3/NFSv4.1)`作为协议类型。

常规 UNIX 模式位不提供与 NTFS 或 NFSv4.x ACL 相同的权限粒度。下表比较了 NFSv3 模式位和 NFSv4.1 ACL 之间的权限粒度。有关 NFSv4.1 ACL 的信息，请参阅 "nfs4_acl - NFSv4 访问控制列表"。

NFSv3 模式位	**NFSv4.1 ACL**
• 执行时设置用户 ID • 执行时设置组 ID • 保存交换的文本（POSIX 中未定义） • 所有者的读取权限 • 所有者的写入权限 • 执行文件所有者的权限；或在目录中查找（搜索）所有者的权限 • 组的读取权限 • 组的写入权限 • 执行文件上的组的权限；或在目录中查找（搜索）组的权限 • 其他人的阅读权限 • 为其他人授予写入权限 • 为其他人在文件上执行权限；或在目录中查找（搜索）其他人的权限	访问控制条目 (ACE) 类型（允许/拒绝/审核）* 继承标志* 目录继承* 文件继承* 不传播继承* 仅继承 权限 * 读取数据（文件）/列出目录（目录） * 写入数据（文件）/创建文件（目录） * 附加数据（文件）/创建子目录（目录） * 执行（文件）/更改目录（目录） * 删除 * 删除子项 * 读取属性 * 写入属性 * 读取命名属性 * 写入命名属性 * 读取 ACL * 写入 ACL * 写入所有者 * 同步

最后，根据 RPC 数据包限制，NFS 组成员资格（在 NFSv3 和 NFSV4.x 中）对于 AUTH_SYS 的默认最大值限制为 16。 NFS Kerberos 提供最多 32 个组，NFSv4 ACL 通过细粒度的用户和组 ACL（每个 ACE 最多 1024 个条目）消除了限制。

此外，Google Cloud NetApp Volumes 还提供扩展组支持，可将受支持的最大组数扩展到 32 个。这需要与包含有效 UNIX 用户和组标识的 LDAP 服务器建立 LDAP 连接。有关配置此功能的详细信息，请参见 Google 文档中的 "创建和管理 NFS 卷"。

NFSv3 用户和组 **ID**

NFSv3 用户和组 ID 以数字 ID 而不是名称的形式通过网络传输。 Google Cloud NetApp Volumes不会通过 NFSv3 对这些数字 ID 进行用户名解析，而 UNIX 安全样式卷仅使用模式位。当存在 NFSv4.1 ACL 时，需要进行数字 ID 查找和/或名称字符串查找才能正确解析 ACL - 即使使用 NFSv3。对于 NTFS 安全样式卷， Google Cloud NetApp Volumes必须将数字 ID 解析为有效的 UNIX 用户，然后映射到有效的 Windows 用户以协商访问权限。

NFSv3 用户和组 **ID** 的安全限制

使用 NFSv3，客户端和服务器永远不必确认尝试使用数字 ID 进行读取或写入的用户是否是有效用户；它只是隐式地受到信任。只需伪造任何数字 ID，文件系统就有可能受到破坏。为了防止此类安全漏洞， Google Cloud NetApp Volumes提供了一些选项。

- 为 NFS 实施 Kerberos 强制用户使用用户名和密码或密钥表文件进行身份验证，以获取 Kerberos 票证以允许访问挂载。 Kerberos 适用于NetApp Volumes-Performance 实例，并且仅适用于 NFSv4.1。

- 限制导出策略规则中的主机列表会限制哪些 NFSv3 客户端可以访问Google Cloud NetApp Volumes卷。
- 使用双协议卷并将 NTFS ACL 应用于卷会强制 NFSv3 客户端将数字 ID 解析为有效的 UNIX 用户名，以正确验证访问挂载。这需要启用 LDAP 并配置 UNIX 用户和组身份。
- 压缩 root 用户可以限制 root 用户对 NFS 挂载造成的损害，但并不能完全消除风险。有关详细信息，请参阅“[根用户] “

最终，NFS 安全性受限于您所使用的协议版本所提供的功能。 NFSv3 虽然总体上比 NFSv4.1 性能更好，但却不能提供相同级别的安全性。

NFSv4.1

与 NFSv3 相比，NFSv4.1 提供了更高的安全性和可靠性，原因如下：

- 通过基于租赁的机制集成锁定
- 有状态会话
- 所有 NFS 功能均通过单个端口 (2049)
- 仅 TCP
- ID域映射
- Kerberos 集成（NFSv3 可以使用 Kerberos，但仅限于 NFS，不适用于 NLM 等辅助协议）

NFSv4.1 依赖项

由于 NFSv4.1 中增加了安全功能，因此涉及一些使用 NFSv3 时不需要的外部依赖项（类似于 SMB 需要 Active Directory 等依赖项）。

NFSv4.1 ACL

Google Cloud NetApp Volumes提供对 NFSv4.x ACL 的支持，与普通 POSIX 样式权限相比，它具有明显的优势，例如：

- 精细控制用户对文件和目录的访问
- 更好的 NFS 安全性
- 改进了与 CIFS/SMB 的互操作性
- 取消了使用 AUTH_SYS 安全性的 NFS 每个用户 16 个组的限制
- ACL 绕过了组 ID (GID) 解析的需要，从而有效地消除了 GID 限制。NFSv4.1 ACL 由 NFS 客户端控制，而不是由Google Cloud NetApp Volumes控制。要使用 NFSv4.1 ACL，请确保您的客户端的软件版本支持它们并且安装了正确的 NFS 实用程序。

NFSv4.1 ACL 与 SMB 客户端之间的兼容性

NFSv4 ACL 与 Windows 文件级 ACL（NTFS ACL）不同，但具有类似的功能。但是，在多协议 NAS 环境中，如果存在 NFSv4.1 ACL 并且您使用双协议访问（同一数据集上的 NFS 和 SMB），则使用 SMB2.0 及更高版本的客户端将无法从 Windows 安全选项卡查看或管理 ACL。

NFSv4.1 ACL 的工作原理

为供参考，定义以下术语：

- 访问控制列表 (ACL)。权限条目列表。
- 访问控制入口 (ACE)。列表中的权限条目。

当客户端在 SETATTR 操作期间在文件上设置 NFSv4.1 ACL 时， Google Cloud NetApp Volumes会在对象上设置该 ACL，替换任何现有的 ACL。如果文件上没有 ACL，则文件的模式权限将根据 OWNER@、GROUP@ 和 EVERYONE@ 计算。如果文件上存在任何现有的 SUID/SGID/STICKY 位，则它们不受影响。

当客户端在 GETATTR 操作过程中获取文件上的 NFSv4.1 ACL 时， Google Cloud NetApp Volumes会读取与该对象关联的 NFSv4.1 ACL，构建 ACE 列表，并将该列表返回给客户端。如果文件具有 NT ACL 或模式位，则由模式位构建 ACL 并返回给客户端。

如果 ACL 中存在 DENY ACE，则拒绝访问；如果存在 ALLOW ACE，则允许访问。但是，如果 ACL 中不存在任何 ACE，访问也会被拒绝。

安全描述符由安全 ACL (SACL) 和自由 ACL (DACL) 组成。 NFSv4.1与CIFS/SMB互操作时，DACL与NFSv4、CIFS是一一映射的。 DACL 由 ALLOW ACE 和 DENY ACE 组成。

如果一个基本的 `chmod`在设置了 NFSv4.1 ACL 的文件或文件夹上运行，现有用户和组 ACL 将被保留，但默认的 OWNER@、GROUP@、EVERYONE@ ACL 将被修改。

使用 NFSv4.1 ACL 的客户端可以设置和查看系统上文件和目录的 ACL。当在具有 ACL 的目录中创建新文件或子目录时，该对象将继承 ACL 中所有已使用适当标记的 ACE "继承标志" 。

如果文件或目录具有 NFSv4.1 ACL，则无论使用哪种协议访问该文件或目录，都使用该 ACL 来控制访问。

只要 ACE 标有正确的继承标志，文件和目录就会从父目录上的 NFSv4 ACL 继承 ACE（可能经过适当的修改）。

当根据 NFSv4 请求创建文件或目录时，生成的文件或目录上的 ACL 取决于文件创建请求是否包含 ACL 或仅包含标准 UNIX 文件访问权限。 ACL 还取决于父目录是否具有 ACL。

- 如果请求包含 ACL，则使用该 ACL。
- 如果请求仅包含标准 UNIX 文件访问权限，并且父目录没有 ACL，则使用客户端文件模式设置标准 UNIX 文件访问权限。
- 如果请求仅包含标准 UNIX 文件访问权限，并且父目录具有不可继承的 ACL，则会在新对象上设置基于传递到请求中的模式位的默认 ACL。
- 如果请求仅包含标准 UNIX 文件访问权限，但父目录具有 ACL，则只要 ACE 已使用适当的继承标志进行标记，父目录的 ACL 中的 ACE 就会被新文件或目录继承。

ACE 权限

NFSv4.1 ACL 权限使用一系列大写和小写字母值（例如 `rxtncy`) 来控制访问。有关这些字母值的更多信息，请参阅 "如何使用 NFSv4 ACL"。

具有 umask 和 ACL 继承的 NFSv4.1 ACL 行为

"NFSv4 ACL 提供 ACL 继承功能" 。ACL 继承意味着在设置了 NFSv4.1 ACL 的对象下创建的文件或文件夹可以

根据 "ACL 继承标志"。

"乌马斯克"用于控制无需管理员交互即可在目录中创建文件和文件夹的权限级别。默认情况下， Google Cloud NetApp Volumes允许 umask 覆盖继承的 ACL，这是根据 "RFC 5661"。

ACL 格式

NFSv4.1 ACL 具有特定的格式。以下示例是文件上的 ACE 设置：

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上述示例遵循以下 ACL 格式准则：

```
type:flags:principal:permissions
```

一种 `A`意思是“允许”。在这种情况下，不会设置继承标志，因为主体不是一个组并且不包括继承。此外，由于 ACE 不是 AUDIT 条目，因此无需设置审计标志。有关 NFSv4.1 ACL 的更多信息，请参阅 "http://linux.die.net/man/5/nfs4_acl"。

如果 NFSv4.1 ACL 设置不正确（或者客户端和服务器无法解析名称字符串），ACL 可能不会按预期运行，或者 ACL 更改可能无法应用并引发错误。

示例错误包括：

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

明确拒绝

NFSv4.1 权限可以包括 OWNER、GROUP 和 EVERYONE 的明确 DENY 属性。这是因为 NFSv4.1 ACL 是默认拒绝的，这意味着如果 ACE 未明确授予 ACL，则会被拒绝。明确的 DENY 属性将覆盖任何 ACCESS ACE，无论是否明确。

DENY ACE 的属性标签为 `D`。

在下面的示例中，GROUP@ 被允许所有读取和执行权限，但被拒绝所有写入访问权限。

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

应尽可能避免使用 DENY ACE，因为它们可能令人困惑且复杂；未明确定义的 ALLOW ACL 将被隐式拒绝。当设置了 DENY ACE 时，用户在期望获得访问权限时可能会被拒绝访问。

上述一组 ACE 相当于模式位中的 755，这意味着：

- 所有者拥有充分的权利。
- 群组具有只读权限。
- 其他人只读。

但是，即使将权限调整为 775，由于 EVERYONE 上明确设置了 DENY，访问也可能会被拒绝。

NFSv4.1 ID 域映射依赖关系

NFSv4.1 利用 ID 域映射逻辑作为安全层，帮助验证尝试访问 NFSv4.1 挂载的用户确实是他们所声称的用户。在这些情况下，来自 NFSv4.1 客户端的用户名和组名会附加一个名称字符串并将其发送到Google Cloud NetApp Volumes实例。如果用户名/组名和 ID 字符串组合不匹配，则该用户和/或组将被压缩为 `/etc/idmapd.conf`客户端上的文件。

此 ID 字符串是遵守正确权限的必要条件，尤其是在使用 NFSv4.1 ACL 和/或 Kerberos 时。因此，需要名称服务服务器依赖项（例如 LDAP 服务器）来确保客户端和Google Cloud NetApp Volumes之间的一致性，以便正确解析用户和组名身份。

Google Cloud NetApp Volumes使用静态默认 ID 域名值 `defaultv4iddomain.com`。 NFS 客户端默认使用 DNS 域名作为其 ID 域名设置，但您可以手动调整 `/etc/idmapd.conf`。

如果在Google Cloud NetApp Volumes中启用了 LDAP，则Google Cloud NetApp Volumes会自动将 NFS ID 域更改为 DNS 中搜索域的配置，并且客户端无需修改，除非它们使用不同的 DNS 域搜索名称。

当Google Cloud NetApp Volumes可以解析本地文件或 LDAP 中的用户名或组名时，将使用域字符串，而不匹配的域 ID 将被压缩为 nobody。如果Google Cloud NetApp Volumes在本地文件或 LDAP 中找不到用户名或组名，则使用数字 ID 值，并且 NFS 客户端会正确解析该名称（这类似于 NFSv3 行为）。

如果不更改客户端的 NFSv4.1 ID 域以匹配Google Cloud NetApp Volumes卷正在使用的域，您会看到以下行为：

- Google Cloud NetApp Volumes中具有本地条目的 UNIX 用户和组（例如 root，如本地 UNIX 用户和组中所定义）被压缩为 nobody 值。
- 如果 NFS 客户端和Google Cloud NetApp Volumes Volumes 之间的 DNS 域不同，则具有 LDAP 条目的 UNIX 用户和组（如果Google Cloud NetApp Volumes配置为使用 LDAP）将被压缩为 nobody。
- 没有本地条目或 LDAP 条目的 UNIX 用户和组使用数字 ID 值并解析为 NFS 客户端上指定的名称。如果客户端上不存在名称，则仅显示数字 ID。

下面显示了上述场景的结果：

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
```

```
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

当客户端和服务器 ID 域匹配时，相同的文件列表如下所示：

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

有关此问题及其解决方法的更多信息，请参阅“NFSv4.1 和 nobody 用户/组 “

Kerberos 依赖项

如果您计划将 Kerberos 与 NFS 结合使用，则必须具备以下Google Cloud NetApp Volumes：

- Kerberos 分发中心服务 (KDC) 的 Active Directory 域
- 具有用户和组属性的 Active Directory 域，其中填充了用于 LDAP 功能的 UNIX 信息（ Google Cloud NetApp Volumes中的 NFS Kerberos 需要用户 SPN 到 UNIX 用户映射才能正常运行。）
- Google Cloud NetApp Volumes实例上启用了 LDAP
- DNS 服务的 Active Directory 域

NFSv4.1 和 **nobody** 用户/组

NFSv4.1 配置中最常见的问题之一是当文件或文件夹显示在列表中时使用 `ls`归 `user:group`组合 `nobody:nobody`。

例如：

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

数字 ID 是 `99`。

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

在某些情况下，文件可能会显示正确的所有者，但 `nobody`作为团体。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

谁是没人?

这 `nobody`NFSv4.1 中的用户与 `nfsnobody`用户。您可以通过运行以下命令来查看 NFS 客户端如何查看每个用户 `id`命令：

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

使用 NFSv4.1， `nobody`用户是 `idmapd.conf`文件，可以定义为您想要使用的任何用户。

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

为什么会发生这种情况?

因为通过名称字符串映射实现的安全性是 NFSv4.1 操作的一个关键原则，所以当名称字符串不能正确匹配时，默认行为是将该用户压缩为通常无法访问用户和组所拥有的文件和文件夹的用户。

当你看到 `nobody`对于文件列表中的用户和/或组，这通常意味着 NFSv4.1 中的某些内容配置错误。这里需要区分大小写。

例如，如果 user1@CVSDEMO.LOCAL (uid 1234, gid 1234) 正在访问导出，则Google Cloud NetApp Volumes必须能够找到 user1@CVSDEMO.LOCAL (uid 1234, gid 1234)。如果Google Cloud NetApp Volumes中的用户是 USER1@CVSDEMO.LOCAL，则不会匹配（大写 USER1 与小写 user1）。在许多情况下，您可以在客户端的消息文件中看到以下内容：

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

客户端和服务器必须都同意用户确实是他们所声称的用户，因此您必须检查以下内容以确保客户端看到的用户与Google Cloud NetApp Volumes看到的用户具有相同的信息。

- NFSv4.x ID 域。客户： `idmapd.conf`文件； Google Cloud NetApp Volumes使用 `defaultv4iddomain.com`并且无法手动更改。如果将 LDAP 与 NFSv4.1 一起使用， Google Cloud NetApp Volumes会将 ID 域更改为 DNS 搜索域正在使用的域，该域与 AD 域相同。
- *用户名和数字 ID。*这确定了客户端在哪里寻找用户名，并利用名称服务交换机配置客户端：

`nsswitch.conf`和/或本地密码和组文件； Google Cloud NetApp Volumes不允许对此进行修改，但在启用时会自动将 LDAP 添加到配置中。

- *组名和数字 ID。*这确定了客户端在哪里寻找组名，并利用名称服务交换机配置客户端： `nsswitch.conf`和/或本地密码和组文件； Google Cloud NetApp Volumes不允许对此进行修改，但在启用时会自动将 LDAP 添加到配置中。

在几乎所有情况下，如果你看到 `nobody`在客户端的用户和组列表中，问题是Google Cloud NetApp Volumes和 NFS 客户端之间的用户或组名域 ID 转换。为避免这种情况，请使用 LDAP 解析客户端和Google Cloud NetApp Volumes之间的用户和组信息。

在客户端上查看 **NFSv4.1** 的名称 **ID** 字符串

如果您使用的是 NFSv4.1，则在 NFS 操作期间会发生名称字符串映射，如前所述。

除了使用 `/var/log/messages`要查找 NFSv4 ID 的问题，您可以使用 "nfsidmap -l"在 NFS 客户端上运行命令来查看哪些用户名已正确映射到 NFSv4 域。

例如，这是客户端和Google Cloud NetApp Volumes可以找到的用户访问 NFSv4.x 挂载后命令的输出：

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

当用户没有正确映射到 NFSv4.1 ID 域时（在这种情况下， `netapp-user`) 尝试访问相同的挂载并接触文件，它们被分配 `nobody:nobody`，正如预期的那样。

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

这 `nfsidmap -l`输出显示用户 `pcuser`在显示屏上，但没有 `netapp-user`；这是我们的导出策略规则中的匿名用户(65534）。

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" 是由 Microsoft 开发的网络文件共享协议，通过以太网网络为多个 SMB 客户端提供集中的用户/组身份验证、权限、锁定和文件共享。文件和文件夹通过共享呈现给客户端，共享可以配置各种共享属性，并通过共享级别权限提供访问控制。SMB 可以呈现给任何为协议提供支持的客户端，包括 Windows、Apple 和 Linux 客户端。

Google Cloud NetApp Volumes为该协议的 SMB 2.1 和 3.x 版本提供支持。

访问控制/SMB 共享

- 当 Windows 用户名请求访问Google Cloud NetApp Volumes卷时， Google Cloud NetApp Volumes会使用Google Cloud NetApp Volumes管理员配置的方法查找 UNIX 用户名。
- 如果配置了外部 UNIX 身份提供程序 (LDAP) 并且 Windows/UNIX 用户名相同，则 Windows 用户名将 1:1 映射到 UNIX 用户名，而无需任何其他配置。启用 LDAP 后，Active Directory 用于托管用户和组对象的 UNIX 属性。
- 如果 Windows 名称和 UNIX 名称不完全匹配，则必须配置 LDAP 以允许Google Cloud NetApp Volumes使用 LDAP 名称映射配置（请参阅"使用 LDAP 进行非对称名称映射"）。
- 如果未使用 LDAP，则 Windows SMB 用户将映射到名为 `pcuser`在Google Cloud NetApp Volumes中。这意味着用户在 Windows 中编写的文件映射到 `pcuser`将 UNIX 所有权显示为 `pcuser`在多协议 NAS 环境中。 `pcuser`这实际上是 `nobody`Linux 环境中的用户（UID 65534）。

在仅使用 SMB 的部署中， `pcuser`映射仍然会发生，但这并不重要，因为 Windows 用户和组所有权已正确显示，并且不允许 NFS 访问仅 SMB 卷。此外，仅 SMB 卷在创建后不支持转换为 NFS 或双协议卷。

Windows 利用 Kerberos 与 Active Directory 域控制器进行用户名身份验证，这需要与 AD DC 交换用户名/密码，而 AD DC 位于Google Cloud NetApp Volumes实例外部。当 `\\SERVERNAME`SMB 客户端使用 UNC 路径，并且以下情况属实：

- SERVERNAME 存在 DNS A/AAAA 条目
- SERVERNAME 存在用于 SMB/CIFS 访问的有效 SPN

创建Google Cloud NetApp Volumes SMB 卷时，将按照本节中的定义创建机器帐户名称"Google Cloud NetApp Volumes如何在 Active Directory 中显示。"该机器帐户名称也成为 SMB 共享访问路径，因为Google Cloud NetApp Volumes利用动态 DNS (DDNS) 在 DNS 中创建必要的 A/AAAA 和 PTR 条目，并在机器帐户主体上创建必要的 SPN 条目。

要创建 PTR 条目，DNS 服务器上必须存在Google Cloud NetApp Volumes实例 IP 地址的反向查

找区域。

例如，此Google Cloud NetApp Volumes卷使用以下 UNC 共享路径： `\\cvs-east- 433d.cvsdemo.local` 。

在 Active Directory 中，这些是Google Cloud NetApp Volumes生成的 SPN 条目：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

这是 DNS 正向/反向查找结果：

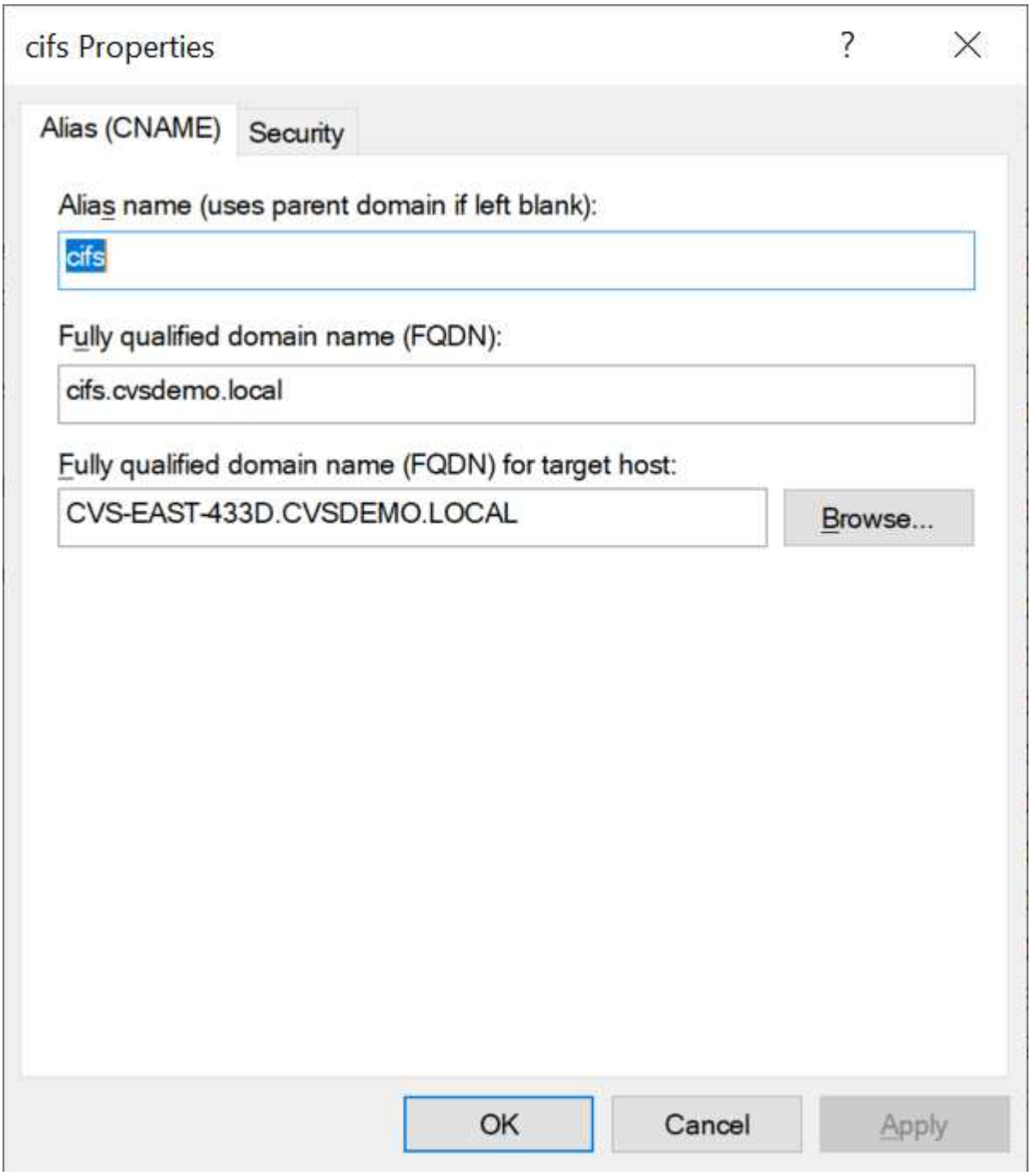
```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

或者，可以通过在Google Cloud NetApp Volumes中启用/要求 SMB 共享的 SMB 加密来应用更多访问控制。如果其中一个端点不支持 SMB 加密，则不允许访问。

使用 **SMB** 名称别名

在某些情况下，让最终用户知道Google Cloud NetApp Volumes使用的机器帐户名称可能会带来安全隐患。在其他情况下，您可能只是想为最终用户提供更简单的访问路径。在这些情况下，您可以创建 SMB 别名。

如果您想为 SMB 共享路径创建别名，您可以利用 DNS 中所谓的 CNAME 记录。例如，如果你想使用名称 `\\CIFS`访问共享而不是 `\\cvs-east- 433d.cvsdemo.local`，但您仍然想使用 Kerberos 身份验证，DNS 中指向现有 A/AAAA 记录的 CNAME 和添加到现有机器帐户的附加 SPN 可提供 Kerberos 访问。



这是添加 CNAME 之后的 DNS 正向查找结果：

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

这是添加新 SPN 后生成的 SPN 查询：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

在数据包捕获中，我们可以看到使用与 CNAME 绑定的 SPN 的会话设置请求。

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB 身份验证方言

Google Cloud NetApp Volumes支持以下 "方言"对于 SMB 身份验证：

- LM
- ntlm
- NTLMv2
- Kerberos

SMB 共享访问的 Kerberos 身份验证是您可以使用的最安全的身份验证级别。启用AES和SMB加密后，安全级别进一步提高。

Google Cloud NetApp Volumes还支持 LM 和 NTLM 身份验证的向后兼容性。当 Kerberos 配置错误时（例如创建 SMB 别名时），共享访问将回退到较弱的身份验证方法（例如 NTLMv2）。由于这些机制不太安全，因此在某些 Active Directory 环境中它们被禁用。如果禁用较弱的身份验证方法并且未正确配置 Kerberos，则共享访问将失败，因为没有有效的身份验证方法可以回退。

有关在 Active Directory 中配置/查看支持的身份验证级别的信息，请参阅 "网络安全: LAN Manager 身份验证级别"。

权限模型

NTFS/文件权限

NTFS 权限是遵循 NTFS 逻辑对文件系统中的文件和文件夹应用的权限。您可以在 `Basic`或者 `Advanced`并可设置为 `Allow`或者 `Deny`用于访问控制。

基本权限包括以下内容：

- 完全控制
- 修改
- 读取并执行
- 读取
- 写入

当您为用户或组设置权限（称为 ACE）时，它位于 ACL 中。 NTFS 权限使用与 UNIX 模式位相同的读/写/执行基础，但它们还可以扩展到更细粒度和扩展的访问控制（也称为特殊权限），例如取得所有权、创建文件夹/附加数据、写入属性等。

标准 UNIX 模式位不提供与 NTFS 权限相同级别的粒度（例如，能够在 ACL 中为单个用户和组对象设置权限或设置扩展属性）。但是，NFSv4.1 ACL 确实提供了与 NTFS ACL 相同的功能。

NTFS 权限比共享权限更具体，可以与共享权限结合使用。对于 NTFS 权限结构，适用最严格的限制。因此，在定义访问权限时，对用户或组的明确拒绝甚至会覆盖完全控制。

NTFS 权限由 Windows SMB 客户端控制。

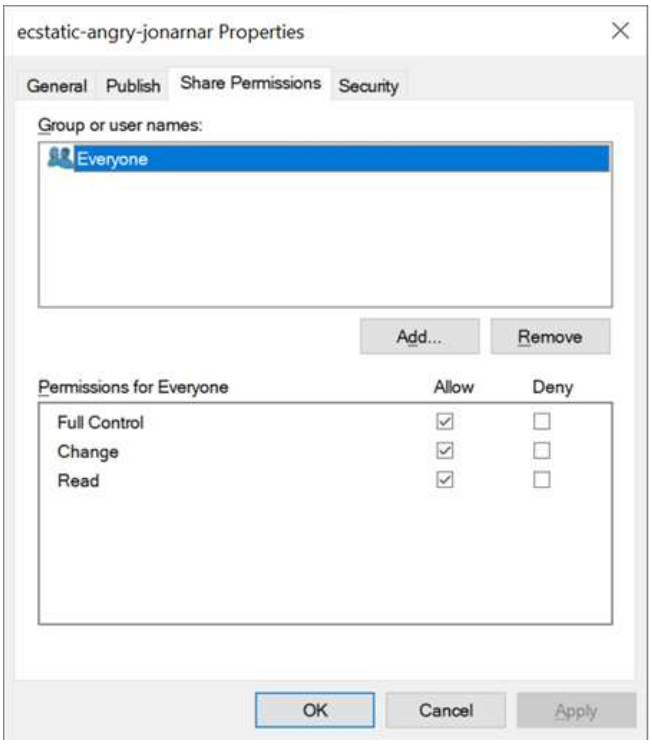
共享权限

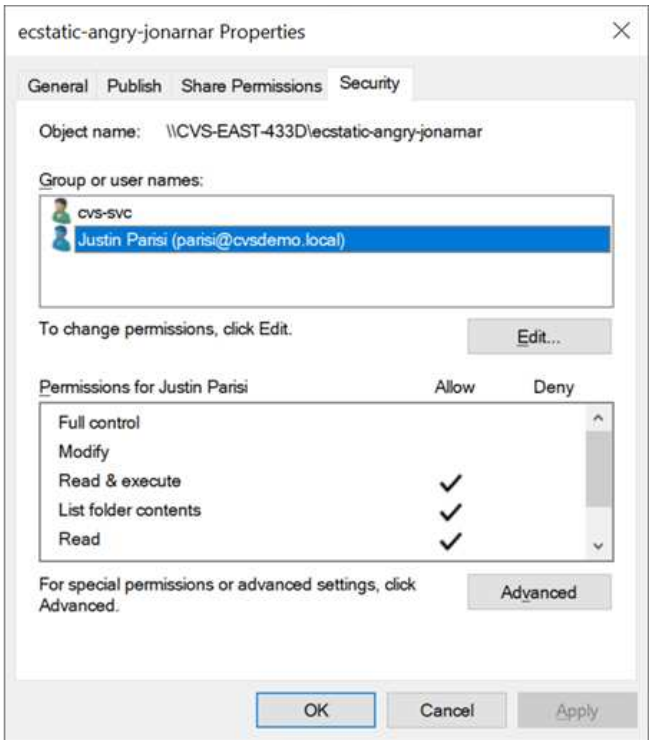
共享权限比 NTFS 权限（仅读取/更改/完全控制）更通用，并控制进入 SMB 共享的初始条目 - 类似于 NFS 导出策略规则的工作方式。

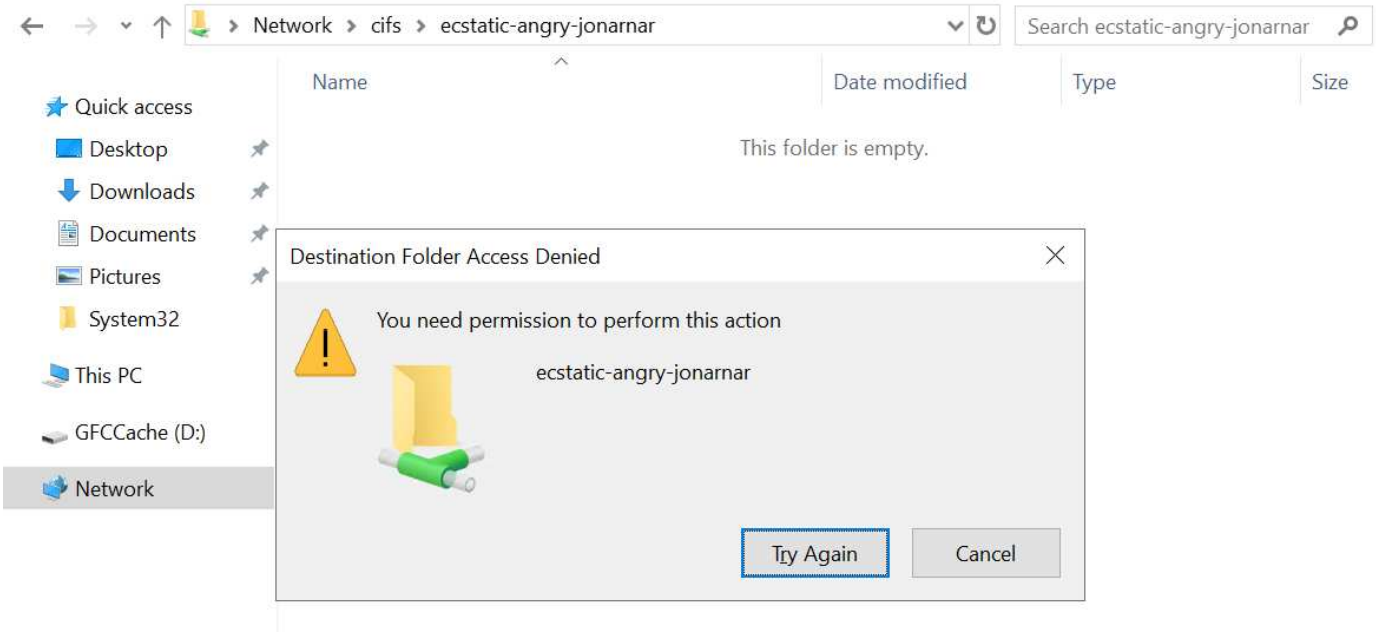
尽管 NFS 导出策略规则通过基于主机的信息（例如 IP 地址或主机名）控制访问，但 SMB 共享权限可以通过使用共享 ACL 中的用户和组 ACE 来控制访问。您可以从 Windows 客户端或Google Cloud NetApp Volumes管理 UI 设置共享 ACL。

默认情况下，共享 ACL 和初始卷 ACL 包括具有完全控制权的所有人。应该更改文件 ACL，但共享权限被共享中对象的文件权限所取代。

例如，如果用户仅被允许对Google Cloud NetApp Volumes卷文件 ACL 进行读取访问，则即使共享 ACL 设置为“具有完全控制权的所有人”，他们也将被拒绝创建文件和文件夹，如下图所示。







为了获得最佳安全效果，请执行以下操作：

- 从共享和文件 ACL 中删除所有人，并为用户或组设置共享访问权限。
- 使用组而不是单个用户进行访问控制，以便于管理，并可以通过组管理更快地删除/添加用户以共享 ACL。
- 允许对共享权限的 ACE 进行限制较少、更通用的共享访问，并锁定具有文件权限的用户和组的访问，以实现更精细的访问控制。
- 避免普遍使用显式拒绝 ACL，因为它们会覆盖允许 ACL。对于需要快速限制访问文件系统的用户或组，限制使用显式拒绝 ACL。
- 确保你注意到 "ACL 继承"修改权限时的设置；在具有大量文件数的目录或卷的顶层设置继承标志意味着该目录或卷下的每个文件都添加了继承的权限，这可能会产生不必要的行为，例如意外的访问/拒绝以及在调整每

个文件时长时间修改权限。

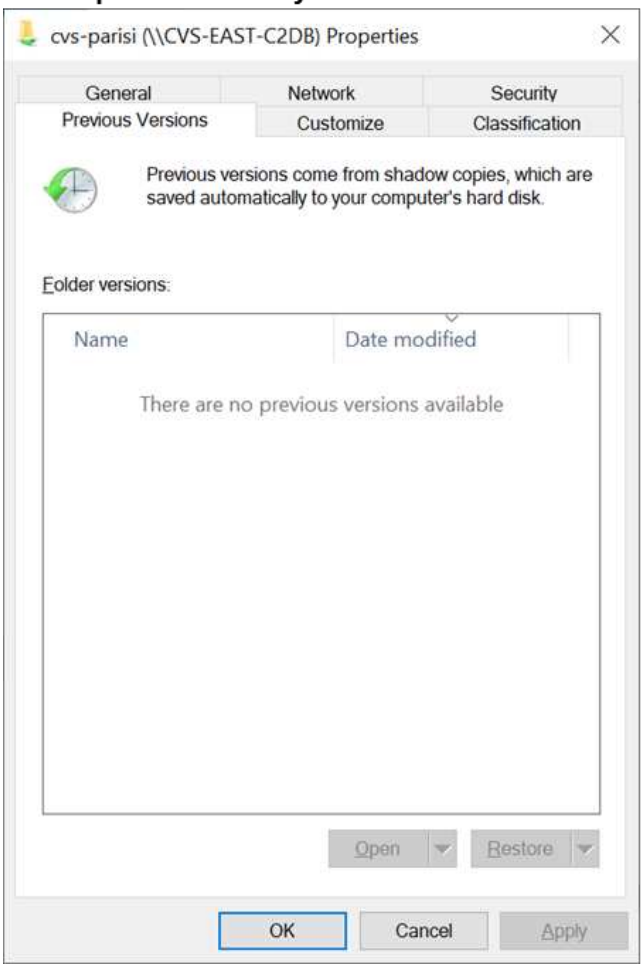
SMB 共享安全功能

当您首次在Google Cloud NetApp Volumes中创建具有 SMB 访问权限的卷时，系统会向您提供一系列用于保护该卷的选择。

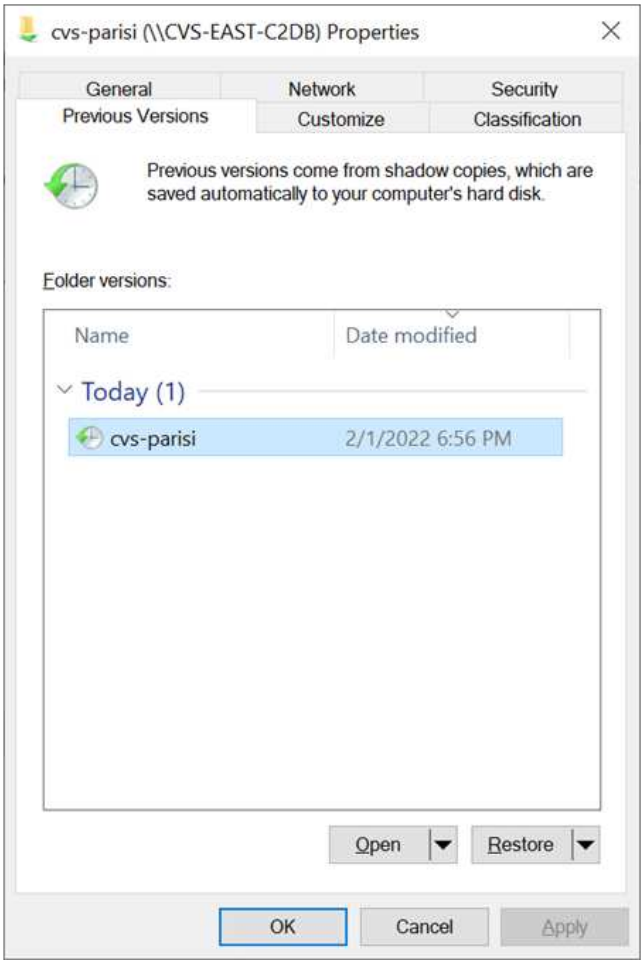
其中一些选择取决于Google Cloud NetApp Volumes级别（性能或软件），选择包括：

- *使快照目录可见（适用于NetApp Volumes-Performance 和NetApp Volumes-SW）。*此选项控制 SMB 客户端是否可以访问 SMB 共享中的快照目录(`\\server\share\~snapshot`和/或“先前版本”选项卡）。默认设置为“未选中”，这意味着卷默认隐藏并禁止访问 `~snapshot`目录，并且卷的“先前版本”选项卡中不会显示任何 Snapshot 副本。

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



出于安全原因、性能原因（隐藏这些文件夹以防 AV 扫描）或偏好，可能需要对最终用户隐藏 Snapshot 副本。Google Cloud NetApp Volumes快照是只读的，因此即使这些快照可见，最终用户也无法删除或修改快照目录中的文件。拍摄 Snapshot 副本时的文件或文件夹的文件权限适用。如果文件或文件夹的权限在 Snapshot 副本之间发生变化，则这些更改也会应用于 Snapshot 目录中的文件或文件夹。用户和组可以根据权限访问这些文件或文件夹。虽然无法删除或修改快照目录中的文件，但可以将文件或文件夹复制出快照目录。

- *启用 SMB 加密（适用于NetApp Volumes-Performance 和NetApp Volumes-SW）。*默认情况下，SMB 加密在 SMB 共享上是禁用的（未选中）。选中该框可启用 SMB 加密，这意味着 SMB 客户端和服务器之间的流量在传输过程中进行加密，并使用协商的最高支持加密级别。 Google Cloud NetApp Volumes支持对 SMB 进行高达 AES-256 的加密。启用 SMB 加密确实会带来性能损失，您的 SMB 客户端可能会或可能不

会注意到这一点 - 大约在 10-20% 的范围内。 NetApp强烈建议进行测试，以了解性能损失是否可以接受。

- *隐藏 SMB 共享（适用于NetApp Volumes-Performance 和NetApp Volumes-SW）。*设置此选项会隐藏正常浏览中的 SMB 共享路径。这意味着不知道共享路径的客户端在访问默认 UNC 路径（例如 `\\NetApp Volumes-SMB`）。选中该复选框后，只有明确知道 SMB 共享路径或具有由组策略对象定义的共享路径的客户端才能访问它（通过混淆实现安全性）。
- *启用基于访问的枚举 (ABE)（仅限NetApp Volumes-SW）。*这类似于隐藏 SMB 共享，不同之处在于共享或文件仅对没有权限访问对象的用户或组隐藏。例如，如果 Windows 用户 `joe`不允许至少通过权限读取访问权限，那么 Windows 用户 `joe`根本看不到 SMB 共享或文件。默认情况下，此功能是禁用的，您可以通过选中复选框来启用它。有关 ABE 的更多信息，请参阅NetApp知识库文章 "基于访问的枚举（ABE）如何工作？"
- 启用持续可用 **(CA)** 共享支持（仅限**NetApp Volumes-Performance**）。 "持续可用的 SMB 共享"通过在Google Cloud NetApp Volumes后端系统中的节点之间复制锁定状态，提供一种在故障转移事件期间最大限度地减少应用程序中断的方法。这不是一个安全功能，但它确实提供了更好的整体弹性。目前，只有 SQL Server 和 FSLogix 应用程序支持此功能。

默认隐藏共享

在Google Cloud NetApp Volumes中创建 SMB 服务器时， "隐藏的管理共享" （使用 $ 命名约定）除了数据卷 SMB 共享之外创建的。这些包括 C$（命名空间访问）和 IPC$（共享命名管道以用于程序之间的通信，例如用于 Microsoft 管理控制台 (MMC) 访问的远程过程调用 (RPC)）。

IPC$ 共享不包含共享 ACL，并且无法修改 - 它严格用于 RPC 调用和 "Windows 默认不允许匿名访问这些共享"。

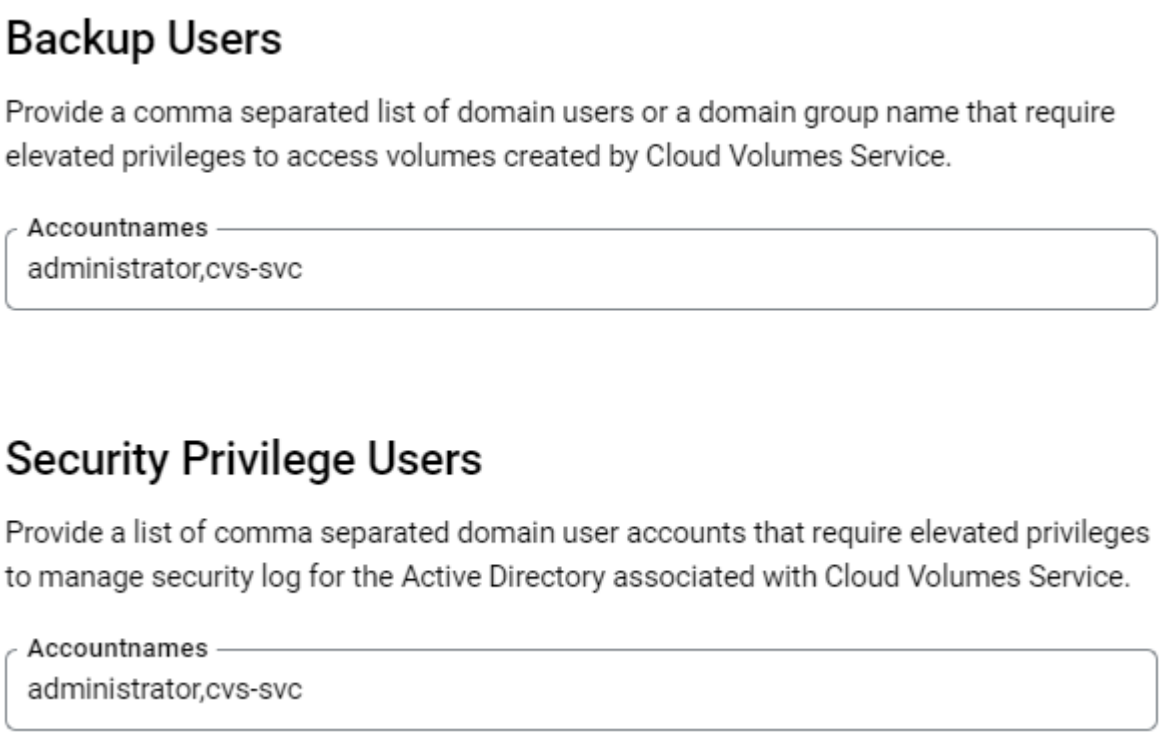
C$ 共享默认允许 BUILTIN/Administrators 访问，但Google Cloud NetApp Volumes自动化会删除共享 ACL 并且不允许任何人访问，因为访问 C$ 共享可以查看Google Cloud NetApp Volumes文件系统中所有已安装的卷。因此，尝试导航至 `\\SERVER\C$`失败。

具有本地/内置管理员/备份权限的帐户

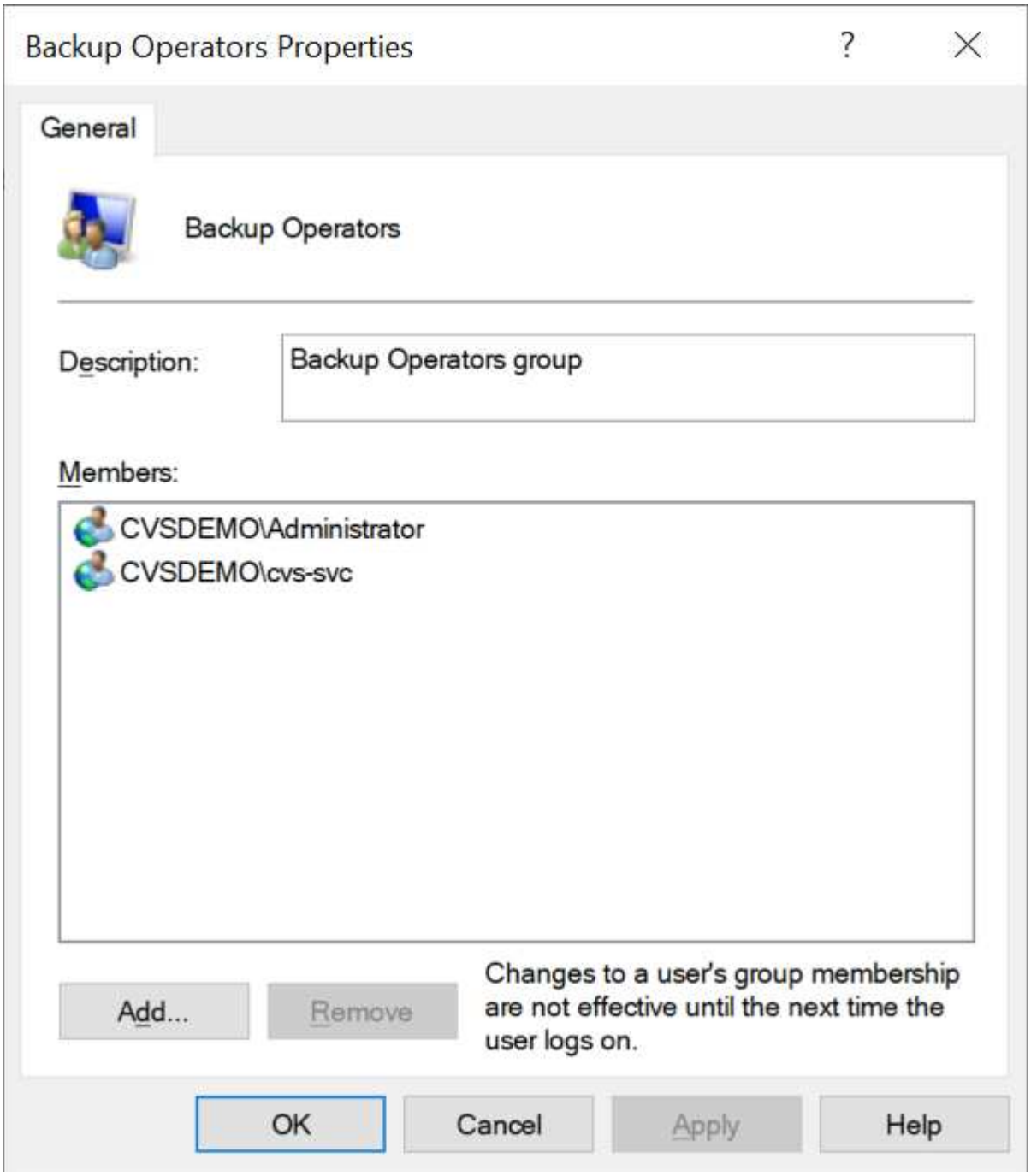
Google Cloud NetApp Volumes SMB 服务器保持与常规 Windows SMB 服务器类似的功能，即存在将访问权限应用于选定域用户和组的本地组（例如 BUILTIN\Administrators）。

当您指定要添加到备份用户中的用户时，该用户将被添加到使用该 Active Directory 连接的Google Cloud NetApp Volumes实例中的 BUILTIN\Backup Operators 组中，然后该实例将获取 "SeBackupPrivilege 和 SeRestorePrivilege"。

当您将用户添加到“安全权限用户”时，该用户将被赋予 SeSecurityPrivilege，这在某些应用程序用例中很有用，例如 "SMB 共享上的 SQL Server"。



您可以通过 MMC 以适当的权限查看Google Cloud NetApp Volumes本地组成员资格。下图显示了使用Google Cloud NetApp Volumes控制台添加的用户。

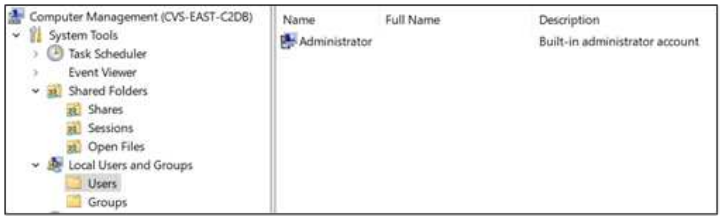


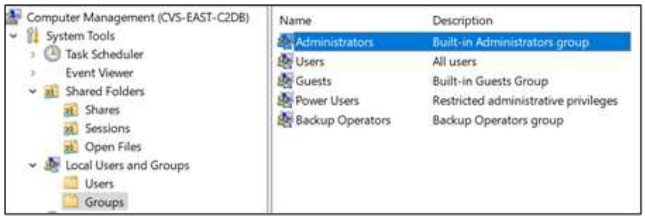
下表显示了默认的 BUILTIN 组的列表以及默认添加的用户/组。

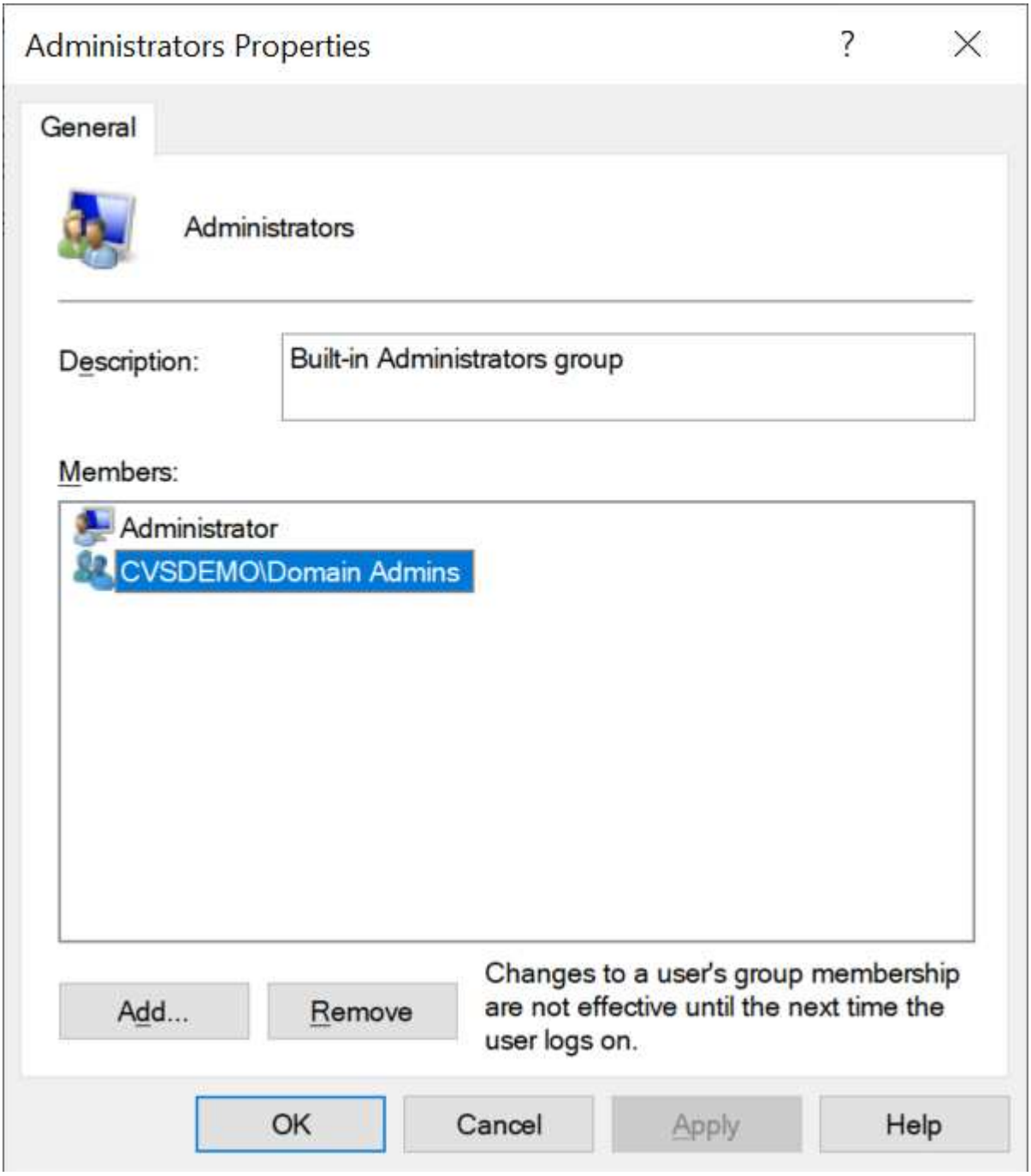
本地/内置组	默认成员
内置管理员*	域\域管理员
内置\备份操作员*	无
内置\来宾	域\域来宾
内置\高级用户	无
BUILTIN\域用户	域\域用户

- Google Cloud NetApp Volumes Active Directory 连接配置中控制的组成员资格。

您可以在 MMC 窗口中查看本地用户和组（以及组成员），但不能从此控制台添加或删除对象或更改组成员身份。默认情况下，只有域管理员组和管理员会添加到Google Cloud NetApp Volumes中的 BUILTIN\Administrators 组。目前，您无法修改此设置。







MMC/计算机管理访问

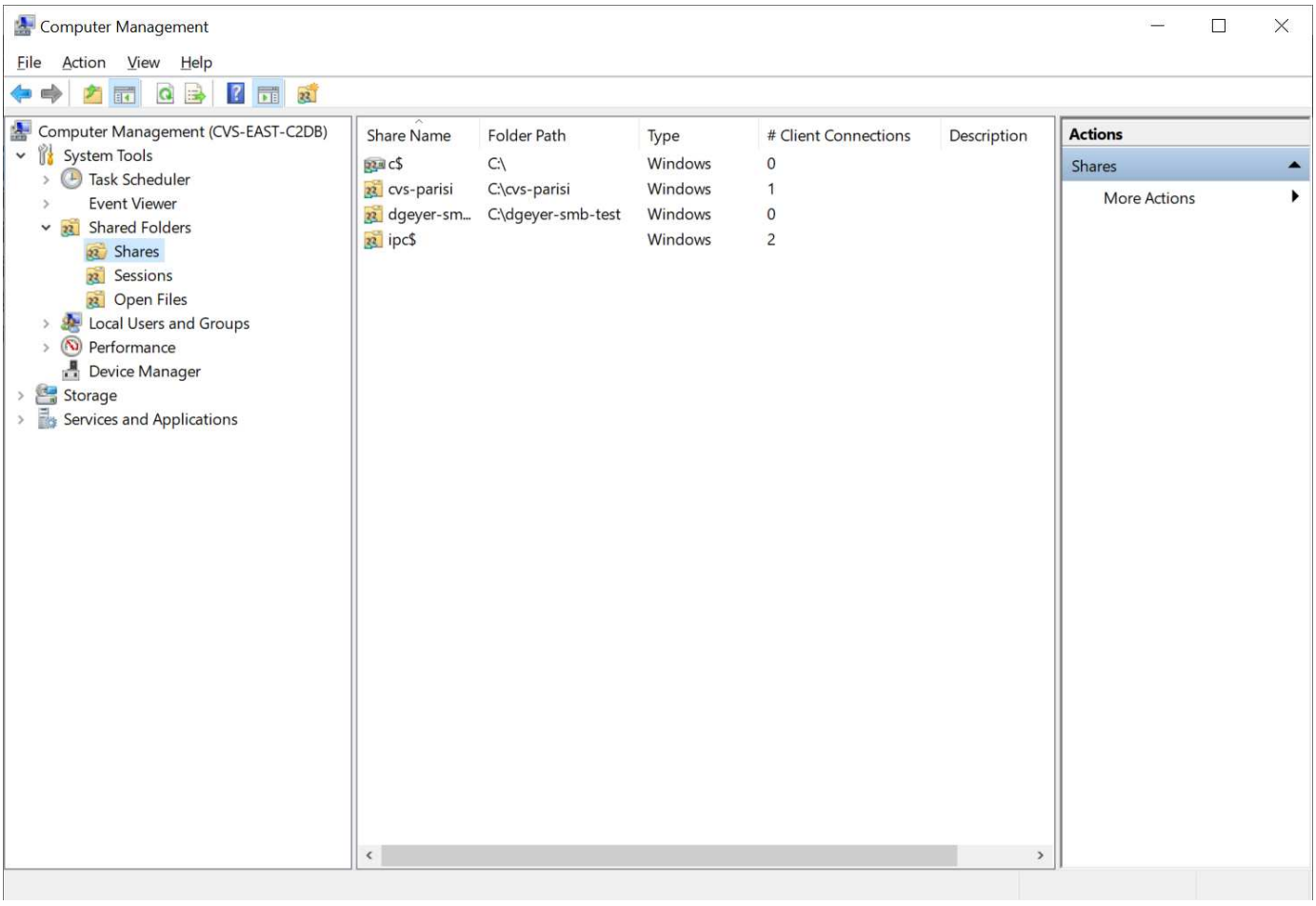
Google Cloud NetApp Volumes中的 SMB 访问提供与计算机管理 MMC 的连接，使您能够查看共享、管理共享 ACL 以及查看/管理 SMB 会话和打开文件。

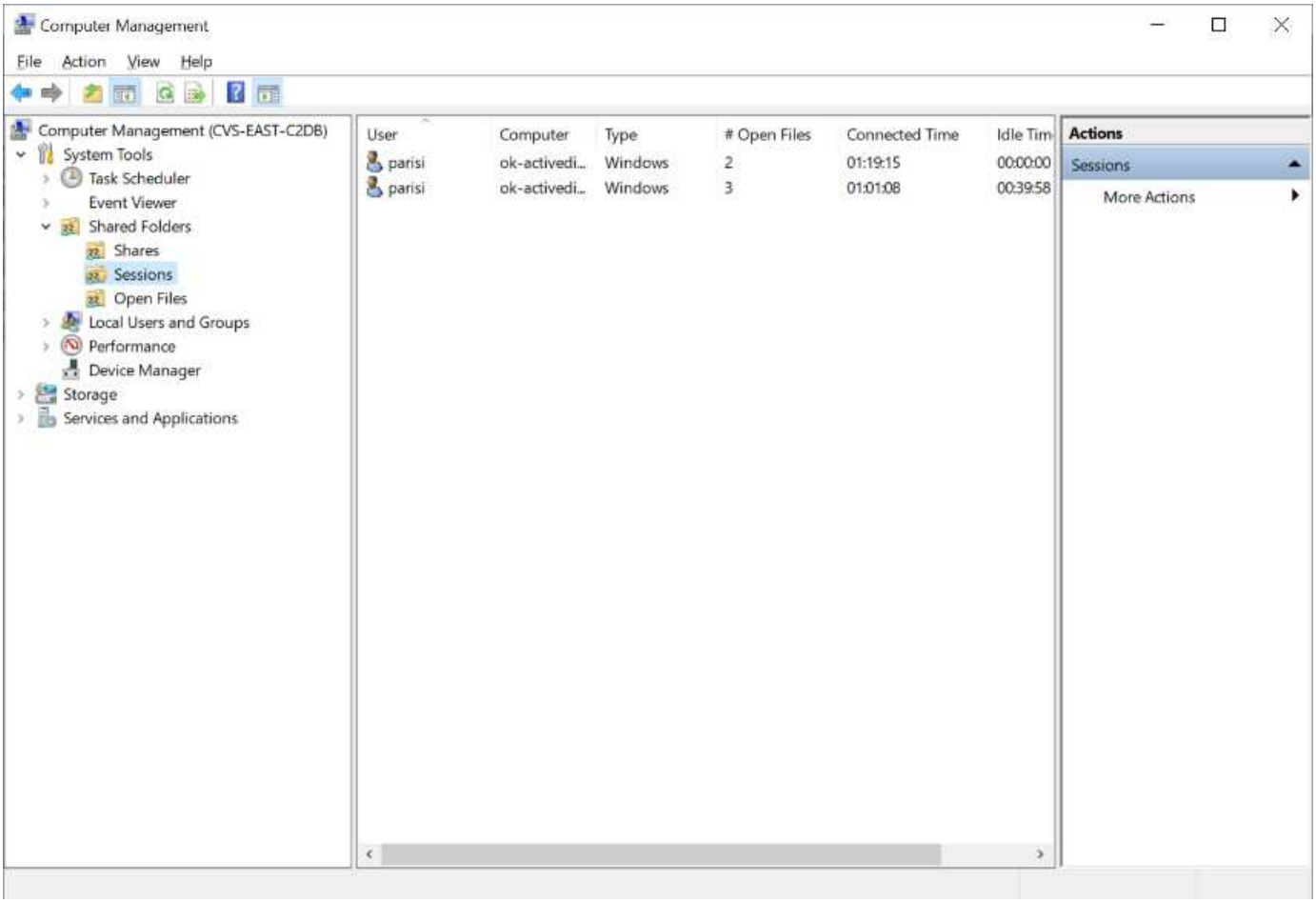
要使用 MMC 查看Google Cloud NetApp Volumes中的 SMB 共享和会话，当前登录的用户必须是域管理员。其他用户可以从 MMC 访问以查看或管理 SMB 服务器，并在尝试查看Google Cloud NetApp Volumes SMB 实例上的共享或会话时收到“您没有权限”对话框。

要连接到 SMB 服务器，请打开“计算机管理”，右键单击“计算机管理”，然后选择“连接到另一台计算机”。这将打开“选择计算机”对话框，您可以在其中输入 SMB 服务器名称（可在Google Cloud NetApp Volumes卷信息中找到）。

当您查看具有适当权限的 SMB 共享时，您会看到Google Cloud NetApp Volumes实例中共享 Active Directory 连接的所有可用共享。要控制此行为，请在Google Cloud NetApp Volumes卷实例上设置隐藏 SMB 共享选项。

请记住，每个区域只允许一个 Active Directory 连接。





下表显示了 MMC 支持/不支持的功能列表。

支持的功能	不支持的功能
• 查看分享 • 查看活动的 SMB 会话 • 查看打开的文件 • 查看本地用户和组 • 查看本地群组成员资格 • 枚举系统中的会话、文件和树连接列表 • 关闭系统中打开的文件 • 关闭开放会议 • 创建/管理共享	• 创建新的本地用户/组 • 管理/查看现有的本地用户/组 • 查看事件或性能日志 • 管理存储 • 管理服务和应用程序

SMB 服务器安全信息

Google Cloud NetApp Volumes中的 SMB 服务器使用一系列选项来定义 SMB 连接的安全策略，包括 Kerberos 时钟偏差、票证年龄、加密等。

下表包含这些选项的列表、它们的作用、默认配置以及是否可以使用Google Cloud NetApp Volumes进行修改。某些选项不适用于Google Cloud NetApp Volumes。

安全选项	它的作用	默认值	可以改嗎?
最大 Kerberos 时钟偏差（分钟）	Google Cloud NetApp Volumes与域控制器之间的最大时间偏差。如果时间偏差超过 5 分钟，Kerberos 身份验证将失败。这被设置为 Active Directory 默认值。	5	否
Kerberos 票证有效期（小时）	Kerberos 票证在需要续订之前保持有效的最长时间。如果 10 小时之前没有续订，则必须获取新票。Google Cloud NetApp Volumes会自动执行这些续订。 10 小时是 Active Directory 的默认值。	10	否
最大 Kerberos 票证更新时间（天）	在需要新的授权请求之前，Kerberos 票证可以续订的最长天数。 Google Cloud NetApp Volumes会自动更新 SMB 连接的票证。七天是 Active Directory 的默认值。	7	否
Kerberos KDC 连接超时（秒）	KDC 连接超时前的秒数。	3	否
要求对传入的 SMB 流量进行签名	设置为要求对 SMB 流量进行签名。如果设置为 true，则不支持签名的客户端将无法连接。	False	
要求本地用户帐户的密码复杂性	用于本地 SMB 用户的密码。 Google Cloud NetApp Volumes不支持本地用户创建，因此此选项不适用于Google Cloud NetApp Volumes。	True	否
使用 start_tls 进行 Active Directory LDAP 连接	用于启用 Active Directory LDAP 的启动 TLS 连接。Google Cloud NetApp Volumes目前不支持启用此功能。	False	否
是否启用 Kerberos 的 AES-128 和 AES-256 加密	这控制是否对 Active Directory 连接使用 AES 加密，并在创建/修改 Active Directory 连接时通过“为 Active Directory 身份验证启用 AES 加密”选项进行控制。	False	是

安全选项	它的作用	默认值	可以改嗎?
LM 兼容级别	Active Directory 连接支持的身份验证方言级别。请参阅“SMB 身份验证方言 ”了解更多信息。	ntlmv2-krb	否
要求对传入的 CIFS 流量进行 SMB 加密	要求所有共享都采用 SMB 加密。 Google Cloud NetApp Volumes不使用此方法；而是根据每个卷设置加密（请参阅“SMB 共享安全功能 "）。	False	否
客户端会话安全	为 LDAP 通信设置签名和/或密封。目前， Google Cloud NetApp Volumes中尚未设置该问题，但在未来的版本中可能需要解决。本节介绍了由于 Windows 补丁导致的 LDAP 身份验证问题的补救措施"LDAP 通道绑定。"。	无	否
SMB2 启用 DC 连接	使用 SMB2 进行 DC 连接。默认启用。	系统默认	否
LDAP 推荐追踪	当使用多个 LDAP 服务器时，如果在第一个服务器中找不到条目，则引用追踪允许客户端引用列表中的其他 LDAP 服务器。Google Cloud NetApp Volumes目前不支持此功能。	False	否
使用 LDAPS 实现安全的 Active Directory 连接	允许使用 LDAP over SSL。目前不受Google Cloud NetApp Volumes支持。	False	否
直流连接需要加密	需要加密才能成功连接 DC。在Google Cloud NetApp Volumes中默认禁用。	False	否

双协议/多协议

Google Cloud NetApp Volumes 能够与 SMB 和 NFS 客户端共享相同的数据集，同时保持适当的访问权限 ("双协议" ）。这是通过协调协议之间的身份映射并使用集中式后端 LDAP 服务器向 Google Cloud NetApp Volumes 提供 UNIX 身份来实现的。您可以使用 Windows Active Directory 提供 Windows 和 UNIX 用户，以便于使用。

访问控制

- *共享访问控制。*确定哪些客户端和/或用户和组可以访问 NAS 共享。对于 NFS，导出策略和规则控制客户端对导出的访问。 NFS 导出由Google Cloud NetApp Volumes实例管理。 SMB 利用 CIFS/SMB 共享和共享 ACL 在用户和组级别提供更精细的控制。您只能通过使用https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html [MMC/Computer Management^] 和在Google Cloud NetApp Volumes实例上具有管理员权限的帐户从 SMB 客户端配置共享级 ACL（请参阅部分链接：gcp-gcnv-smb.html#Accounts with local/BUILTIN administrator/backup rights["Accounts with local/BUILTIN administrator/backup rights."]）。
- *文件访问控制。*控制文件或文件夹级别的权限，并始终从 NAS 客户端进行管理。 NFS 客户端可以使用传统模式位 (rwx) 或 NFSv4 ACL。 SMB 客户端利用 NTFS 权限。

向 NFS 和 SMB 提供数据的卷的访问控制取决于所使用的协议。有关双协议权限的信息，请参阅“[权限模型] “

用户映射

当客户端访问卷时， Google Cloud NetApp Volumes会尝试将传入用户映射到相反方向的有效用户。这对于跨协议确定正确的访问权限以及确保请求访问的用户确实是他们所声称的用户来说是必要的。

例如，如果 Windows 用户名为 `joe`尝试通过 SMB 访问具有 UNIX 权限的卷，然后Google Cloud NetApp Volumes执行搜索以查找名为 `joe`。如果存在，则以 Windows 用户身份写入 SMB 共享的文件 `joe`显示为 UNIX 用户 `joe`来自 NFS 客户端。

或者，如果 UNIX 用户名为 `joe`尝试使用 Windows 权限访问Google Cloud NetApp Volumes卷，则 UNIX 用户必须能够映射到有效的 Windows 用户。否则，将拒绝访问该卷。

当前，使用 LDAP 的外部 UNIX 标识管理仅支持 Active Directory。有关配置此服务的访问权限的详细信息，请参见 "创建 AD 连接"。

权限模型

使用双协议设置时， Google Cloud NetApp Volumes会利用卷的安全样式来确定 ACL 的类型。这些安全样式是根据指定的 NAS 协议设置的，或者在双协议的情况下，是在创建Google Cloud NetApp Volumes卷时做出的选择。

- 如果您仅使用 NFS， Google Cloud NetApp Volumes卷将使用 UNIX 权限。
- 如果您仅使用 SMB， Google Cloud NetApp Volumes卷将使用 NTFS 权限。

如果您正在创建双协议卷，则可以在创建卷时选择 ACL 样式。此决定应根据所需的权限管理做出。如果您的用户从 Windows/SMB 客户端管理权限，请选择 NTFS。如果您的用户更喜欢使用 NFS 客户端和 chmod/chown，请使用 UNIX 安全样式。

创建 **Active Directory** 连接的注意事项

Google Cloud NetApp Volumes可以将您的Google Cloud NetApp Volumes实例连接到外部 Active Directory 服务器，以便为 SMB 和 UNIX 用户进行身份管理。需要创建 Active Directory 连接才能在Google Cloud NetApp Volumes中使用 SMB。

该配置提供了几个需要考虑安全性的选项。外部 Active Directory 服务器可以是本地实例或云原生实例。如果您使用的是本地 Active Directory 服务器，请不要将域暴露给外部网络（例如使用 DMZ 或外部 IP 地址）。相反，使用安全的私有隧道或 VPN、单向林信任或专用网络连接到本地网络 "私人 Google 访问权限"。有关更多信息，请参阅 Google Cloud 文档 "在 Google Cloud 中使用 Active Directory 的最佳实践"。

NetApp Volumes-SW 要求 Active Directory 服务器位于同一区域。如果在NetApp Volumes-SW 中尝试建立到另一个区域的 DC 连接，则尝试会失败。使用NetApp Volumes-SW 时，请确保创建包含 Active Directory DC 的 Active Directory 站点，然后在Google Cloud NetApp Volumes中指定站点，以避免跨区域 DC 连接尝试。

Active Directory 凭据

启用 SMB 或 LDAP for NFS 后， Google Cloud NetApp Volumes会与 Active Directory 控制器交互以创建用于身份验证的机器帐户对象。这与 Windows SMB 客户端加入域并需要对 Active Directory 中的组织单位 (OU) 具有相同的访问权限的方式没有什么不同。

在许多情况下，安全组不允许在外部服务器（例如Google Cloud NetApp Volumes）上使用 Windows 管理员帐户。在某些情况下，为了确保最佳安全措施，Windows 管理员用户会被完全禁用。

创建 **SMB** 机器帐户所需的权限

要将Google Cloud NetApp Volumes机器对象添加到 Active Directory，需要具有域管理权限或具有 "委派创建和修改计算机帐户对象的权限"需要指定 OU。您可以使用 Active Directory 中的控制委派向导来执行此操作，方法是创建自定义任务，该任务为用户提供创建/删除计算机对象的权限，并提供以下访问权限：

- 读写
- 创建/删除所有子对象
- 读/写所有属性
- 更改/重置密码

这样做会自动将定义的用户的安全 ACL 添加到 Active Directory 中的 OU，并最大限度地减少对 Active Directory 环境的访问。委派用户后，可在此窗口中提供该用户名和密码作为 Active Directory 凭据。

传递给 Active Directory 域的用户名和密码在机器帐户对象查询和创建期间利用 Kerberos 加密来增强安全性。

Active Directory 连接详细信息

`https://docs.cloud.google.com/netapp/volumes/docs/configure-and-use/active-directory/about-ad["Active Directory` 连接详细信息 `"^]`为管理员提供指导，以便为计算机帐户放置提供特定的 `Active Directory` 架构信息，例如：

- Active Directory 连接类型。用于指定区域中的 Active Directory 连接是否用于Google Cloud NetApp Volumes或NetApp Volumes-Performance 服务类型的卷。如果在现有连接上设置不正确，则使用或编辑时可能无法正常工作。
- 领域。 Active Directory 域名。
- *站点。*将 Active Directory 服务器限制到特定站点以确保安全性和性能 "注意事项"。当多个 Active Directory 服务器跨区域时，这是必要的，因为 Google Cloud NetApp Volumes 当前不支持允许 Active Directory 身份验证请求到与 Google Cloud NetApp Volumes 实例不同区域中的 Active Directory 服务器。（例如，Active Directory 域控制器位于仅 NetApp Volumes-Performance 支持的区域，但您希望在 NetApp Volumes-SW 实例中使用 SMB 共享。）

- DNS 服务器。用于名称查找的 DNS 服务器。
- NetBIOS 名称（可选）。如果需要，服务器的 NetBIOS 名称。这是使用 Active Directory 连接创建新机器帐户时使用的内容。例如，如果 NetBIOS 名称设置为NetApp Volumes-EAST，则机器帐户名称将为NetApp Volumes-EAST-{1234}。请参阅"Google Cloud NetApp Volumes如何在 Active Directory 中显示"了解更多信息。
- 组织单位 (OU)。创建计算机帐户的特定 OU。如果您将机器帐户的控制权委托给特定 OU 的用户，这将非常有用。
- *AES 加密。*您还可以选中或取消选中“为 AD 身份验证启用 AES 加密”复选框。为 Active Directory 身份验证启用 AES 加密可为用户和组查找期间Google Cloud NetApp Volumes与 Active Directory 的通信提供额外的安全性。启用此选项之前，请与域管理员核实，以确认 Active Directory 域控制器支持 AES 身份验证。

> 默认情况下，大多数 Windows 服务器不会禁用较弱的密码（例如 DES 或 RC4-HMAC），但如果您选择禁用较弱的密码，请确认Google Cloud NetApp Volumes Active Directory 连接已配置为启用 AES。否则，身份验证将失败。启用 AES 加密不会禁用较弱的密码，而是向Google Cloud NetApp Volumes SMB 机器帐户添加对 AES 密码的支持。

Kerberos 领域详细信息

此选项不适用于 SMB 服务器。相反，它用于为Google Cloud NetApp Volumes系统配置 NFS Kerberos。填充这些详细信息后，将配置 NFS Kerberos 领域（类似于 Linux 上的 krb5.conf 文件），并在Google Cloud NetApp Volumes卷创建上指定 NFS Kerberos 时使用，因为 Active Directory 连接充当 NFS Kerberos 分发中心 (KDC)。

> 非 Windows KDC 当前不支持与Google Cloud NetApp Volumes一起使用。

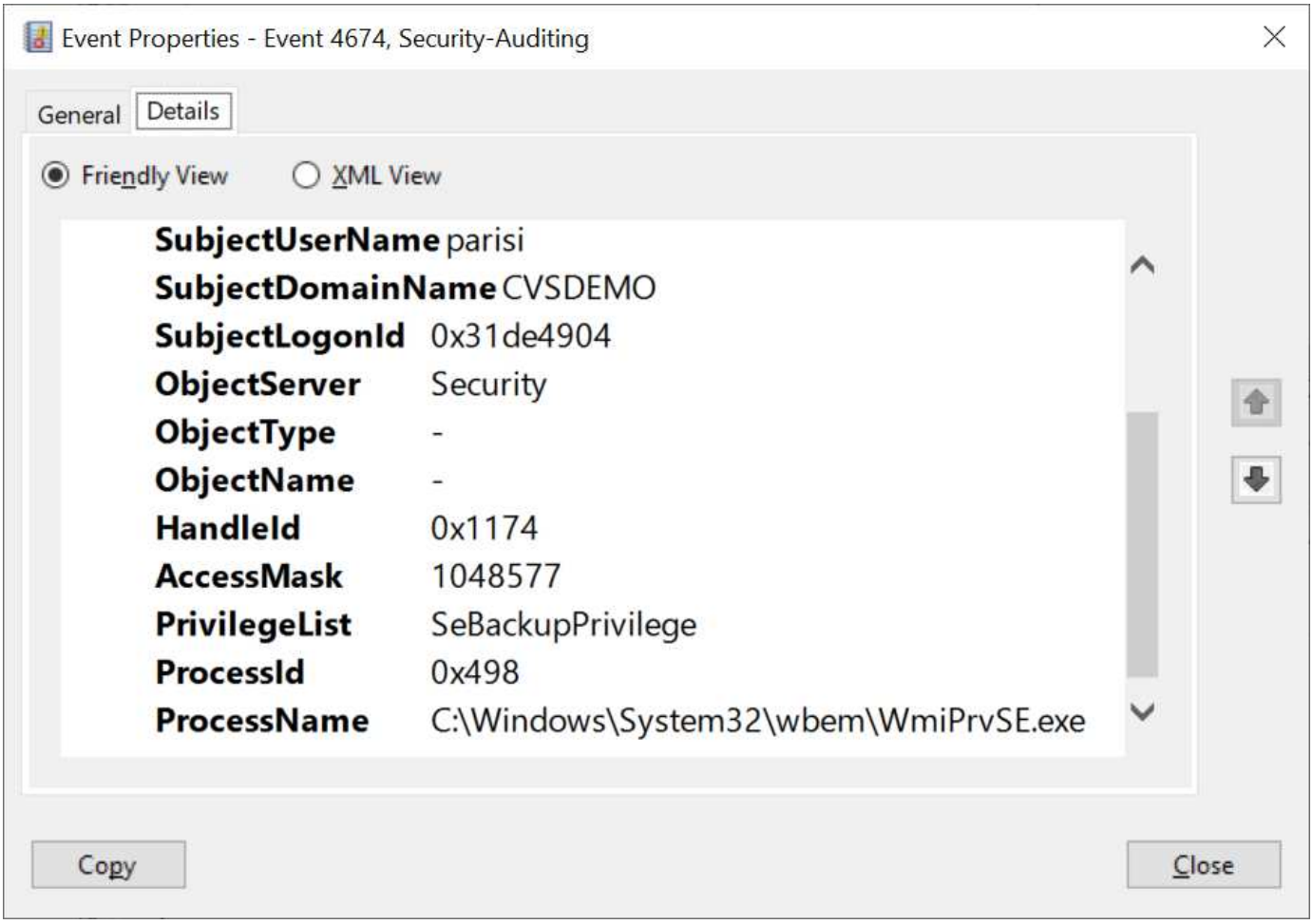
地区

通过区域，您可以指定 Active Directory 连接所在的位置。该区域必须与Google Cloud NetApp Volumes卷位于同一区域。

- *具有 LDAP 的本地 NFS 用户。*在本节中，还有一个选项允许本地 NFS 用户使用 LDAP。如果您想要扩展 UNIX 用户组成员资格支持，使其超出 NFS（扩展组）的 16 个组限制，则必须取消选择此选项。但是，使用扩展组需要为 UNIX 身份配置 LDAP 服务器。如果您没有 LDAP 服务器，请不要选择此选项。如果您有 LDAP 服务器并且还想使用本地 UNIX 用户（例如 root），请选择此选项。

备份用户

此选项使您能够指定对Google Cloud NetApp Volumes卷具有备份权限的 Windows 用户。某些应用程序需要备份权限（SeBackupPrivilege）才能正确备份和恢复 NAS 卷中的数据。此用户对卷中的数据具有高级别访问权限，因此您应该考虑 "启用该用户访问的审计"。启用后，审计事件将显示在事件查看器 > Windows 日志 > 安全中。



安全特权用户

通过此选项，您可以指定对Google Cloud NetApp Volumes卷具有安全修改权限的 Windows 用户。某些应用程序需要安全权限（SeSecurityPrivilege）("例如 SQL Server") 在安装过程中正确设置权限。管理安全日志需要此权限。虽然此权限不如 SeBackupPrivilege 强大，NetApp建议 "审计用户的用户访问"如果需要的话，可以使用此权限级别。

有关更多信息，请参阅 "分配给新登录的特殊权限" 。

Google Cloud NetApp Volumes如何在 **Active Directory** 中显示

Google Cloud NetApp Volumes在 Active Directory 中显示为普通机器帐户对象。命名约定如下。

- CIFS/SMB 和 NFS Kerberos 创建单独的机器帐户对象。
- 启用 LDAP 的 NFS 在 Active Directory 中为 Kerberos LDAP 绑定创建一个机器帐户。
- 具有 LDAP 的双协议卷共享 LDAP 和 SMB 的 CIFS/SMB 机器帐户。
- CIFS/SMB 机器帐户使用 NAME-1234 的命名约定（随机四位 ID，在 <10 个字符的名称后附加连字符）。您可以通过 Active Directory 连接上的 NetBIOS 名称设置来定义 NAME（请参阅“Active Directory 连接详细信息 ")。
- NFS Kerberos 使用 NFS-NAME-1234 作为命名约定（最多 15 个字符）。如果使用超过 15 个字符，则名称为 NFS-TRUNCATED-NAME-1234。
- 启用 LDAP 的仅 NFS NetApp Volumes-Performance 实例会创建一个 SMB 机器帐户，以与 CIFS/SMB 实

例具有相同的命名约定来绑定到 LDAP 服务器。

- 创建 SMB 机器帐户时，默认隐藏的管理共享（请参阅"默认隐藏共享"）也被创建（c$、admin$、ipc$），但这些共享没有分配 ACL，因此无法访问。
- 默认情况下，机器帐户对象放在 CN=Computers 中，但您可以在必要时指定不同的 OU。请参阅“创建 SMB 机器帐户所需的权限 “有关添加/删除Google Cloud NetApp Volumes的机器帐户对象所需的访问权限的信息。

当Google Cloud NetApp Volumes将 SMB 机器帐户添加到 Active Directory 时，将填充以下字段：

- cn（带有指定的 SMB 服务器名称）
- dNSHostName（使用 SMBserver.domain.com）
- msDS-SupportedEncryptionTypes（如果未启用 AES 加密，则允许使用 DES_CBC_MD5、RC4_HMAC_MD5；如果启用了 AES 加密，则允许使用 DES_CBC_MD5、RC4_HMAC_MD5、AES128_CTS_HMAC_SHA1_96、AES256_CTS_HMAC_SHA1_96 与 SMB 的机器帐户进行 Kerberos 票证交换）
- 名称（使用 SMB 服务器名称）
- sAMAccountName（带有 SMBserver$）
- servicePrincipalName（对于 Kerberos，使用 host/smbserver.domain.com 和 host/smbserver SPN）

如果要在计算机帐户上禁用较弱的 Kerberos 加密类型 (enctype)，您可以将计算机帐户上的 msDS-SupportedEncryptionTypes 值更改为下表中的值之一，以仅允许 AES。

msDS-SupportedEncryptionTypes 值	已启用 **Enctype**
2	DES_CBC_MD5
4	RC4_HMAC
8	仅限 AES128_CTS_HMAC_SHA1_96
16	仅限 AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 和 AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5、RC4_HMAC、AES128_CTS_HMAC_SHA1_96 和 AES256_CTS_HMAC_SHA1_96

要为 SMB 机器帐户启用 AES 加密，请在创建 Active Directory 连接时单击为 AD 身份验证启用 AES 加密。

要为 NFS Kerberos 启用 AES 加密， "请参阅Google Cloud NetApp Volumes文档"。

其他 **NAS** 基础设施服务依赖项（**KDC**、**LDAP** 和 **DNS**）

当使用Google Cloud NetApp Volumes进行 NAS 共享时，可能需要外部依赖项才能正常发挥作用。这些依赖关系在特定情况下发挥作用。下表显示了各种配置选项以及所需的依赖项（如果有）。

配置	所需依赖项
仅限 NFSv3	无

配置	所需依赖项
仅限 NFSv3 Kerberos	Windows 活动目录：* KDC * DNS * LDAP
仅限 NFSv4.1	客户端 ID 映射配置（/etc/idmap.conf）
仅限 NFSv4.1 Kerberos	• 客户端 ID 映射配置（/etc/idmap.conf） • Windows 活动目录：KDC DNS LDAP
仅限 SMB	活动目录：* KDC * DNS
多协议 NAS（NFS 和 SMB）	• 客户端 ID 映射配置（仅限 NFSv4.1；/etc/idmap.conf） • Windows 活动目录：KDC DNS LDAP

机器帐户对象的 **Kerberos** 密钥表轮换/密码重置

使用 SMB 机器帐户， Google Cloud NetApp Volumes会为 SMB 机器帐户安排定期重置密码。这些密码重置使用 Kerberos 加密进行，并按照每月第四个星期日晚上 11 点到凌晨 1 点之间的随机时间进行。这些密码重置会更改 Kerberos 密钥版本，轮换存储在Google Cloud NetApp Volumes系统上的密钥表，并帮助为在Google Cloud NetApp Volumes中运行的 SMB 服务器维持更高级别的安全性。机器帐户密码是随机的，管理员不知道。

对于 NFS Kerberos 机器帐户，仅当创建/与 KDC 交换新的密钥表时才会重置密码。目前，在Google Cloud NetApp Volumes中无法执行此操作。

用于 **LDAP** 和 **Kerberos** 的网络端口

使用 LDAP 和 Kerberos 时，您应该确定这些服务使用的网络端口。您可以在 "Google Cloud NetApp Volumes有关安全注意事项的文档"中找到 Google Cloud NetApp Volumes 正在使用的端口的完整列表。

LDAP

Google Cloud NetApp Volumes充当 LDAP 客户端，并使用标准 LDAP 搜索查询来查找 UNIX 身份的用户和组。如果您打算使用Google Cloud NetApp Volumes提供的标准默认用户之外的用户和组，则 LDAP 是必需的。如果您计划将 NFS Kerberos 与用户主体（例如 user1@domain.com）一起使用，则 LDAP 也是必需的。目前仅支持使用 Microsoft Active Directory 的 LDAP。

要将 Active Directory 用作 UNIX LDAP 服务器，您必须在要用于 UNIX 身份的用户和组上填充必要的 UNIX 属性。 Google Cloud NetApp Volumes使用默认 LDAP 模式模板，该模板根据以下信息查询属性 "RFC-2307-bis"。因此，下表显示了用户和组需要填充的最低限度的 Active Directory 属性以及每个属性的用途。

有关在 Active Directory 中设置 LDAP 属性的详细信息，请参见 "管理双协议访问。"

属性	它的作用
uid*	指定 UNIX 用户名
uid编号*	指定 UNIX 用户的数字 ID
gid编号*	指定 UNIX 用户的主要组数字 ID
对象类*	指定正在使用的对象类型； Google Cloud NetApp Volumes要求将“用户”包含在对象类列表中（默认情况下包含在大多数 Active Directory 部署中）。

属性	它的作用
name	有关帐户的一般信息（真实姓名、电话号码等 - 也称为 gecos）
unix用户密码	无需设置此项；不用于 NAS 身份验证的 UNIX 身份查找。设置此项将把配置的 unixUserPassword 值以纯文本形式放置。
unix主目录	当用户从 Linux 客户端针对 LDAP 进行身份验证时，定义 UNIX 主目录的路径。如果您想要使用 LDAP 实现 UNIX 主目录功能，请设置此项。
登录外壳	当用户通过 LDAP 进行身份验证时，定义 Linux 客户端的 bash/profile shell 路径。

*表示该属性是Google Cloud NetApp Volumes正常功能所必需的。其余属性仅供客户端使用。

属性	它的作用
cn*	指定 UNIX 组名。当使用 Active Directory 进行 LDAP 时，这是在首次创建对象时设置的，但以后可以更改。此名称不能与其他对象相同。例如，如果您的 UNIX 用户 user1 属于 Linux 客户端上名为 user1 的组，则 Windows 不允许两个对象具有相同 cn 属性。要解决此问题，请将 Windows 用户重命名为唯一名称（例如 user1-UNIX）； Google Cloud NetApp Volumes中的 LDAP 使用 uid 属性作为 UNIX 用户名。
gid编号*	指定 UNIX 组数字 ID。
对象类*	指定正在使用的对象类型； Google Cloud NetApp Volumes要求将组包含在对象类列表中（默认情况下，此属性包含在大多数 Active Directory 部署中）。
会员ID	指定哪些 UNIX 用户是 UNIX 组的成员。使用Google Cloud NetApp Volumes中的 Active Directory LDAP，此字段不是必需的。 Google Cloud NetApp Volumes LDAP 模式使用成员字段来表示组成员身份。
成员*	对于组成员身份/次要 UNIX 组是必需的。通过将 Windows 用户添加到 Windows 组来填充此字段。但是，如果 Windows 组没有填充 UNIX 属性，则它们不会包含在 UNIX 用户的组成员资格列表中。任何需要在 NFS 中可用的组都必须填充此表中列出的所需 UNIX 组属性。

*表示该属性是Google Cloud NetApp Volumes正常功能所必需的。其余属性仅供客户端使用。

LDAP 绑定信息

要查询 LDAP 中的用户， Google Cloud NetApp Volumes必须绑定（登录）到 LDAP 服务。此登录具有只读权限，用于查询 LDAP UNIX 属性以进行目录查找。目前，只有使用 SMB 机器帐户才可以进行 LDAP 绑定。

只能为以下对象启用 LDAP `NetApp Volumes-Performance`实例并将其用于 NFSv3、NFSv4.1 或双协议卷。必须在与Google Cloud NetApp Volumes卷相同的区域建立 Active Directory 连接才能成功部署启用 LDAP 的卷。

启用LDAP后，在特定场景下会出现以下情况。

- 如果Google Cloud NetApp Volumes项目仅使用 NFSv3 或 NFSv4.1，则会在 Active Directory 域控制器中创建一个新的机器帐户，并且Google Cloud NetApp Volumes中的 LDAP 客户端将使用机器帐户凭据绑定到 Active Directory。没有为 NFS 卷创建 SMB 共享，并且默认隐藏管理共享（请参阅"默认隐藏共享") 已删除共享 ACL。
- 如果Google Cloud NetApp Volumes项目使用双协议卷，则仅使用为 SMB 访问创建的单个机器帐户将Google Cloud NetApp Volumes中的 LDAP 客户端绑定到 Active Directory。不创建额外的机器帐户。
- 如果单独创建专用的 SMB 卷（在启用带有 LDAP 的 NFS 卷之前或之后），则 LDAP 绑定的机器帐户将与 SMB 机器帐户共享。
- 如果还启用了 NFS Kerberos，则会创建两个机器帐户 - 一个用于 SMB 共享和/或 LDAP 绑定，一个用于 NFS Kerberos 身份验证。

LDAP 查询

尽管 LDAP 绑定是加密的，但 LDAP 查询仍通过使用通用 LDAP 端口 389 以纯文本形式通过网络传递。目前无法在Google Cloud NetApp Volumes中更改此知名端口。因此，有权访问网络中的数据包嗅探器的人可以看到用户和组名称、数字 ID 和组成员身份。

但是，Google Cloud VM 无法嗅探其他 VM 的单播流量。只有主动参与 LDAP 流量（即能够绑定）的虚拟机才能看到来自 LDAP 服务器的流量。有关Google Cloud NetApp Volumes中的数据包嗅探的更多信息，请参阅"数据包嗅探/跟踪注意事项。"

LDAP 客户端配置默认设置

在Google Cloud NetApp Volumes实例中启用 LDAP 时，默认情况下会使用特定的配置详细信息创建 LDAP 客户端配置。在某些情况下，选项不适用于Google Cloud NetApp Volumes （不受支持）或不可配置。

LDAP 客户端选项	它的作用	默认值	可以改嗎?
LDAP 服务器列表	设置用于查询的 LDAP 服务器名称或 IP 地址。这不适用于Google Cloud NetApp Volumes。相反，Active Directory 域用于定义 LDAP 服务器。	未设置	否
Active Directory 域	设置用于 LDAP 查询的 Active Directory 域。Google Cloud NetApp Volumes利用 DNS 中 LDAP 的 SRV 记录来查找域中的 LDAP 服务器。	设置为 Active Directory 连接中指定的 Active Directory 域。	否
首选 Active Directory 服务器	设置用于 LDAP 的首选 Active Directory 服务器。不受Google Cloud NetApp Volumes支持。相反，使用 Active Directory 站点来控制 LDAP 服务器选择。	未设置。	否

LDAP 客户端选项	它的作用	默认值	可以改嗎?
使用 SMB 服务器凭据绑定	使用 SMB 机器帐户绑定到 LDAP。目前， Google Cloud NetApp Volumes中唯一支持的 LDAP 绑定方法。	True	否
架构模板	用于 LDAP 查询的架构模板。	MS-AD-BIS	否
LDAP 服务器端口	用于 LDAP 查询的端口号。 Google Cloud NetApp Volumes目前仅使用标准 LDAP 端口 389。LDAPS/端口 636 当前不受支持。	389	否
LDAPS 是否已启用	控制是否使用安全套接字层 (SSL) 上的 LDAP 进行查询和绑定。目前不受Google Cloud NetApp Volumes支持。	False	否
查询超时（秒）	查询超时。如果查询时间超过指定值，则查询失败。	3	否
最低绑定身份验证级别	支持的最低绑定级别。由于Google Cloud NetApp Volumes使用机器帐户进行 LDAP 绑定，而 Active Directory 默认不支持匿名绑定，因此此选项对于安全性不起作用。	匿名的	否
绑定 DN	使用简单绑定时用于绑定的用户/专有名称 (DN)。Google Cloud NetApp Volumes使用机器账户进行 LDAP 绑定，目前不支持简单绑定身份验证。	未设置	否
基础 DN	用于 LDAP 搜索的基本 DN。	用于 Active Directory 连接的 Windows 域，采用 DN 格式（即 DC=domain 、DC=local）。	否
基本搜索范围	基本 DN 搜索的搜索范围。值可以包括 base 、onelevel 或 subtree。Google Cloud NetApp Volumes仅支持子树搜索。	子树	否

LDAP 客户端选项	它的作用	默认值	可以改嗎?
用户 DN	定义用户开始搜索 LDAP 查询的 DN。目前不支持Google Cloud NetApp Volumes，因此所有用户搜索都从基本 DN 开始。	未设置	否
用户搜索范围	用户 DN 搜索的搜索范围。值可以包括 base 、onelevel 或 subtree。Google Cloud NetApp Volumes不支持设置用户搜索范围。	子树	否
组 DN	定义 LDAP 查询的组搜索开始的 DN。目前不支持Google Cloud NetApp Volumes，因此所有组搜索都从基本 DN 开始。	未设置	否
群组搜索范围	组 DN 搜索的搜索范围。值可以包括 base 、onelevel 或 subtree。Google Cloud NetApp Volumes不支持设置组搜索范围。	子树	否
网络组 DN	定义网络组搜索 LDAP 查询的起始 DN。目前不支持Google Cloud NetApp Volumes，因此所有网络组搜索都从基本 DN 开始。	未设置	否
网络组搜索范围	网络组 DN 搜索的搜索范围。值可以包括 base 、onelevel 或 subtree。Google Cloud NetApp Volumes不支持设置网络组搜索范围。	子树	否
通过 LDAP 使用 start_tls	利用 Start TLS 通过端口 389 建立基于证书的 LDAP 连接。目前不受Google Cloud NetApp Volumes支持。	False	否
启用按主机查找网络组	启用按主机名查找网络组，而不是扩展网络组来列出所有成员。目前不受Google Cloud NetApp Volumes支持。	False	否

LDAP 客户端选项	它的作用	默认值	可以改嗎?
按主机 DN 划分的网络组	定义 LDAP 查询的 netgroup-by-host 搜索开始的 DN。 Google Cloud NetApp Volumes目前不支持 Netgroup-by-host。	未设置	否
Netgroup-by-host 搜索范围	按主机 DN 搜索的网络组搜索范围。值可以包括 base、onelevel 或 subtree。 Google Cloud NetApp Volumes目前不支持 Netgroup-by-host。	子树	否
客户端会话安全	定义 LDAP 使用的会话安全级别（签名、印章或无）。如果 Active Directory 请求， NetApp Volumes-Performance 支持 LDAP 签名。 NetApp Volumes-SW 不支持 LDAP 签名。对于这两种服务类型，目前不支持密封。	无	否
LDAP 引用追踪	当使用多个 LDAP 服务器时，如果在第一个服务器中找不到条目，则引用追踪允许客户端引用列表中的其他 LDAP 服务器。 Google Cloud NetApp Volumes目前不支持此功能。	False	否
群组成员资格过滤器	提供自定义 LDAP 搜索过滤器，用于从 LDAP 服务器查找组成员身份。目前不支持Google Cloud NetApp Volumes。	未设置	否

使用 **LDAP** 进行非对称名称映射

默认情况下， Google Cloud NetApp Volumes会双向映射具有相同用户名的 Windows 用户和 UNIX 用户，无需特殊配置。只要Google Cloud NetApp Volumes可以找到有效的 UNIX 用户（使用 LDAP），就会发生 1:1 名称映射。例如，如果 Windows 用户 `johnsmith`然后，如果Google Cloud NetApp Volumes可以找到名为 `johnsmith`在 LDAP 中，该用户的名称映射成功，由该用户创建的所有文件/文件夹 `johnsmith`显示正确的用户所有权，以及所有影响的 ACL `johnsmith`无论使用何种 NAS 协议，都将受到尊重。这被称为对称名称映射。

非对称名称映射是指 Windows 用户和 UNIX 用户身份不匹配的情况。例如，如果 Windows 用户 `johnsmith` 具有 `UNIX 身份 `jsmith`， Google Cloud NetApp Volumes需要一种方法来获知这一变化。由于Google Cloud NetApp Volumes目前不支持创建静态名称映射规则，因此必须使用 LDAP 来查找 Windows 和 UNIX 身份的用户身份，以确保文件和文件夹的正确所有权和预期权限。

默认情况下， Google Cloud NetApp Volumes包含 `LDAP`在名称映射数据库实例的 ns-switch 中，以便通过使用 LDAP 为非对称名称提供名称映射功能，您只需修改一些用户/组属性以反映Google Cloud NetApp Volumes所寻找的内容。

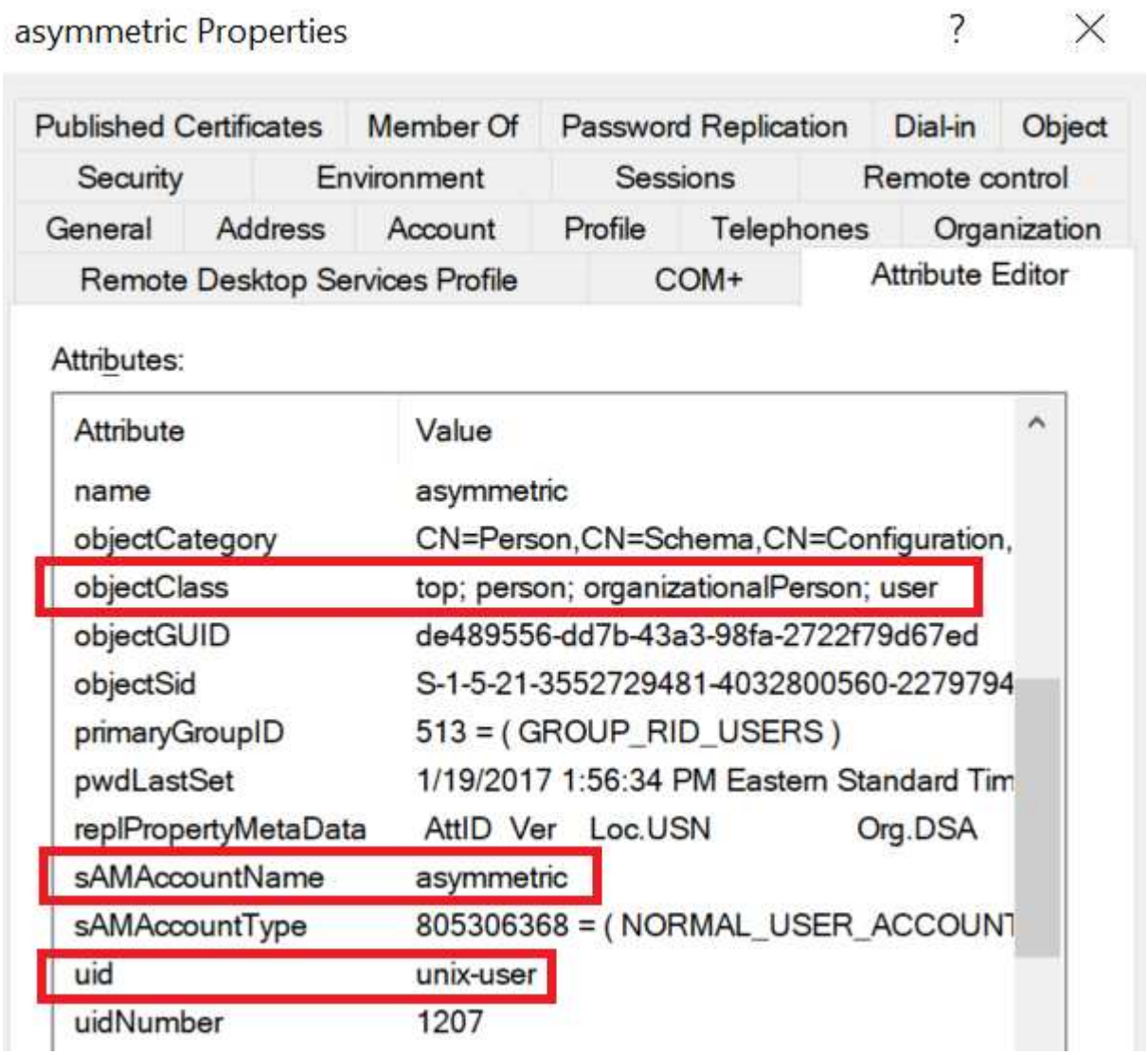
下表显示了 LDAP 中必须填充哪些属性才能实现非对称名称映射功能。大多数情况下，Active Directory 已经配置为执行此操作。

Google Cloud NetApp Volumes属性	它的作用	**Google Cloud NetApp Volumes**用于名称映射的值
Windows 到 UNIX 对象类	指定正在使用的对象的类型。 （即用户、组、posixAccount 等）	必须包含用户（如果需要，可以包含多个其他值。）
Windows 到 UNIX 属性	在创建时定义 Windows 用户名。 Google Cloud NetApp Volumes使用它来进行 Windows 到 UNIX 的查找。	这里不需要更改；sAMAccountName 与 Windows 登录名相同。
UID	定义 UNIX 用户名。	所需的 UNIX 用户名。

Google Cloud NetApp Volumes目前在 LDAP 查找中不使用域前缀，因此多域 LDAP 环境无法正常进行 LDAP 名称映射查找。

以下示例显示了具有 Windows 名称的用户 `asymmetric`，UNIX 名称 `unix-user`，以及从 SMB 和 NFS 写入文件时遵循的行为。

下图显示了 LDAP 属性在 Windows 服务器上的样子。



从 NFS 客户端，您可以查询 UNIX 名称，但不能查询 Windows 名称：

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

当文件从 NFS 写入时 `unix-user`，以下是来自 NFS 客户端的结果：

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

从 Windows 客户端，您可以看到文件的所有者已设置为正确的 Windows 用户：

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

相反，Windows 用户创建的文件 `asymmetric`从 SMB 客户端显示正确的 UNIX 所有者，如下文所示。

中小企业：

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS：

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP 通道绑定

由于 Windows Active Directory 域控制器存在漏洞， "Microsoft 安全公告 ADV190023"改变 DC 允许 LDAP 绑定的方式。

对Google Cloud NetApp Volumes的影响与对任何 LDAP 客户端的影响相同。 Google Cloud NetApp Volumes目前不支持通道绑定。由于Google Cloud NetApp Volumes通过协商默认支持 LDAP 签名，因此 LDAP 通道绑定应该不是问题。如果您在启用通道绑定的情况下确实遇到 LDAP 绑定问题，请按照 ADV190023 中的修复步骤操作，以允许Google Cloud NetApp Volumes的 LDAP 绑定成功。

DNS

Active Directory 和 Kerberos 都依赖 DNS 来实现主机名到 IP/IP 到主机名的解析。 DNS 要求端口 53 处于打开状态。 Google Cloud NetApp Volumes不会对 DNS 记录进行任何修改，目前也不支持使用 "动态 DNS"在网络接口上。

您可以配置 Active Directory DNS 来限制哪些服务器可以更新 DNS 记录。有关更多信息，请参阅 "安全 Windows DNS" 。

请注意，Google 项目内的资源默认使用 Google Cloud DNS，它与 Active Directory DNS 无关。使用 Cloud DNS 的客户端无法解析Google Cloud NetApp Volumes返回的 UNC 路径。加入 Active Directory 域的 Windows 客户端配置为使用 Active Directory DNS，并且可以解析此类 UNC 路径。

若要将客户端加入 Active Directory，必须将其 DNS 配置配置为使用 Active Directory DNS。或者，您可以将 Cloud DNS 配置为将请求转发到 Active Directory DNS。有关详细信息，请参见 "为什么我的客户端无法解析 SMB NetBIOS 名称？ "。

Google Cloud NetApp Volumes目前不支持 DNSSEC，DNS 查询以纯文本形式执行。

文件访问审计

目前不支持Google Cloud NetApp Volumes。

防病毒保护

您必须在 NAS 共享客户端的Google Cloud NetApp Volumes中执行防病毒扫描。目前， Google Cloud NetApp Volumes尚未实现本机防病毒集成。

服务运营

Google Cloud NetApp Volumes团队管理 Google Cloud 中的后端服务，并使用多种策略来保护平台安全并防止不必要的访问。

每个客户都有自己独特的子网，默认情况下，该子网的访问权限与其他客户隔离，并且Google Cloud NetApp Volumes中的每个租户都有自己的命名空间和 VLAN，以实现完全的数据隔离。用户通过身份验证后，服务交付引擎 (SDE) 只能读取特定于该租户的配置数据。

物理安全

经过适当的预先批准，只有现场工程师和带有NetApp标志的现场支持工程师 (FSE) 才能进入笼子和机架进行物理工作。不允许存储和网络管理。只有这些现场资源能够执行硬件维护任务。

对于现场工程师，将提出工作说明书 (SOW) 的票证，其中包括机架 ID 和设备位置 (RU)，所有其他详细信息都包含在票证中。对于NetApp FSE，必须向 COLO 提出现场访问票，票上应包含访客的详细信息、日期和时间，以供审计。 FSE 的 SOW 在内部传达给NetApp。

运营团队

Google Cloud NetApp Volumes的运营团队由Google Cloud NetApp Volumes的生产工程和站点可靠性工程师 (SRE) 以及硬件的NetApp现场支持工程师和合作伙伴组成。所有运营团队成员均已获得在 Google Cloud 工作的认证，并且每张提出的工单都会保留详细的工作记录。此外，还制定了严格的变更控制和批准流程，以确保每个决策都经过适当的审查。

SRE 团队管理控制平面以及如何将数据从 UI 请求路由到Google Cloud NetApp Volumes中的后端硬件和软件。SRE 团队还管理系统资源，例如卷和 inode 最大值。 SRE 不得与客户数据交互或访问客户数据。 SRE 还提供与退货授权 (RMA) 的协调，例如后端硬件的新磁盘或内存更换请求。

客户责任

Google Cloud NetApp Volumes的客户管理其组织的 Active Directory 和用户角色管理以及卷和数据操作。客户可以拥有管理角色，并可以使用NetApp和 Google Cloud 提供的两个预定义角色（管理员和查看者）将权限委托给同一 Google Cloud 项目内的其他最终用户。

管理员可以将客户项目中的任何 VPC 与客户认为合适的Google Cloud NetApp Volumes对等连接。客户有责任管理对其 Google Cloud 市场订阅的访问以及管理有权访问数据平面的 VPC。

恶意 **SRE** 保护

可能出现的一个问题是， Google Cloud NetApp Volumes如何防范恶意 SRE 或 SRE 凭证被泄露的情况?

只有有限数量的 SRE 个人可以访问生产环境。管理权限进一步限制于少数经验丰富的管理员。 Google Cloud NetApp Volumes生产环境中任何人执行的所有操作都会被记录下来，并且我们的安全信息和事件管理 (SIEM) 威胁情报平台会检测到基线异常或可疑活动。因此，可以在对Google Cloud NetApp Volumes后端造成太大损害之前跟踪和缓解恶意行为。

卷生命周期

Google Cloud NetApp Volumes仅管理服务内的对象，而不是卷内的数据。只有访问卷的客户端才能管理数据、ACL、文件所有者等。这些卷中的数据在静止时是加密的，并且访问权限仅限于Google Cloud NetApp Volumes实例的租户。

Google Cloud NetApp Volumes的卷生命周期是创建-更新-删除。卷会保留卷的 Snapshot 副本，直到卷被删除，并且只有经过验证的Google Cloud NetApp Volumes管理员才能删除Google Cloud NetApp Volumes中的卷。当管理员请求删除卷时，需要额外输入卷名称来验证删除。卷被删除后，该卷将消失并且无法恢复。

如果Google Cloud NetApp Volumes合同终止， NetApp会在特定时间段后将卷标记为删除。在该时间段到期之前，您可以根据客户的要求恢复卷。

认证

Google Cloud NetApp Volumes for Google Cloud 目前已通过 ISO/IEC 27001:2013 和 ISO/IEC 27018:2019 标准认证。该服务最近还收到了 SOC2 Type I 认证报告。有关NetApp对数据安全和隐私的承诺，请参阅 "合规性：数据安全和数据隐私"。

GDPR

我们对隐私和遵守 GDPR 的承诺在我们的许多 "客户合同"中均有体现，例如我们的 "客户Data Processing附录"，其中包括欧盟委员会提供的 "标准合同条款"。我们还在隐私政策中做出了这些承诺，并以公司行为准则中规定的核心价值观为后盾。

附加信息和联系信息

要了解有关本文档中描述的信息的更多信息，请查看以下文档和/或网站：

- Google Google Cloud NetApp Volumes Cloud 文档

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Google 私人服务访问

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp产品文档

  "https://www.netapp.com/support-and-training/documentation/"

- 加密验证模块程序 - NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- NetApp勒索软件解决方案

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616： ONTAP中的 NFS Kerberos

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

联系我们

敬请提出宝贵意见和建议，帮助我们改进本技术报告。

请通过 doccomments@netapp.com 联系我们。在主题行中包含技术报告 4918。

NetApp Disaster Recovery

针对 **VMware** 的 **3-2-1** 数据保护：使用 **SnapCenter** 插件和 **NetApp Backup and Recovery** 保护 **VMware** 工作负载

3-2-1 备份策略是业界认可的数据保护方法，它提供了一种全面的方法来保护宝贵的数据。这种策略是可靠的，并确保即使发生一些意外的灾难，仍然可以提供数据的副本。

概述

该策略由三条基本规则组成：

1. 至少保留三份数据副本。这样可以确保即使一个副本丢失或损坏，您仍然至少有两个副本可以依靠。
2. 将两个备份存储在不同的存储介质或设备上。多样化的存储介质有助于防止特定于设备或特定于介质的故障。如果一个设备损坏或一种介质出现故障，另一个备份副本不会受到影响。
3. 最后，确保至少有一个备份副本位于异地。异地存储可以作为防止火灾或洪水等局部灾害的故障保护措施，因为这些灾害可能会导致现场副本无法使用。

本解决方案文档涵盖 3-2-1 备份解决方案，使用 SnapCenter Plug-in for VMware vSphere（SCV）为我们的本地虚拟机创建主备份和辅助备份，并使用 NetApp Backup and Recovery for virtual machines 将我们的数据副本备份到云存储或 StorageGRID。

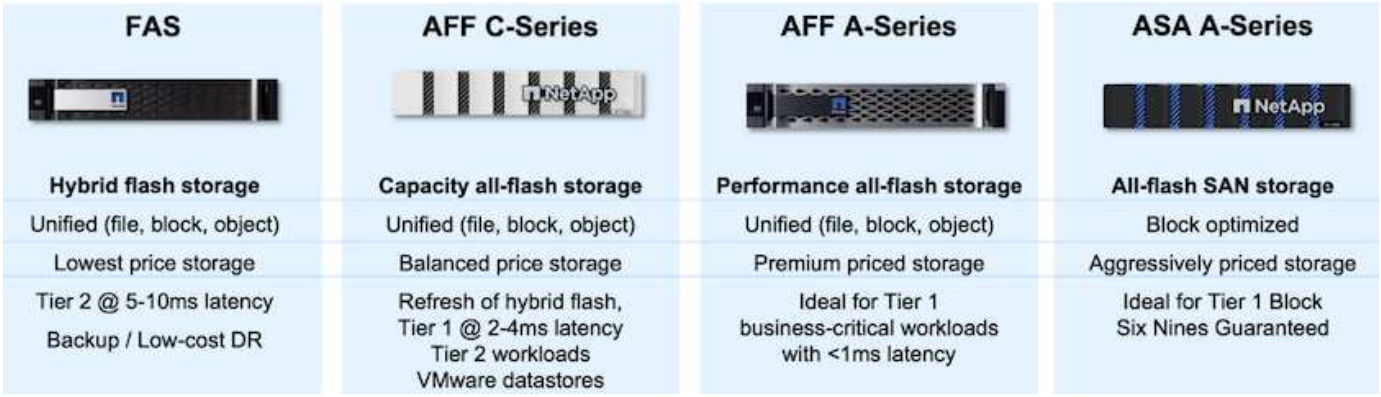
使用案例

此解决方案适用于以下用例：

- 使用适用于SnapCenter Plug-in for VMware vSphere备份和还原本地虚拟机和数据存储区。
- 本地虚拟机和数据存储的备份和还原，托管在 ONTAP 集群上，并使用用于虚拟机的 NetApp Backup and Recovery 备份到对象存储。

NetApp ONTAP数据存储

ONTAP是 NetApp 业界领先的存储解决方案，无论您通过 SAN 还是 NAS 协议访问，它都能提供统一存储。 3-2-1 备份策略确保本地数据在多种媒体类型上受到保护，并且NetApp提供从高速闪存到低成本媒体的平台。



有关 NetApp 所有硬件平台的更多信息，请查看 "NetApp数据存储"。

适用于 **VMware vSphere** 的 **SnapCenter** 插件

VMware vSphere 的SnapCenter插件是一种数据保护产品，它与 VMware vSphere 紧密集成，可以轻松管理虚拟机的备份和恢复。作为该解决方案的一部分， SnapMirror提供了一种快速可靠的方法，可以在二级ONTAP存储集群上创建虚拟机数据的第二个不可变备份副本。有了这种架构，就可以从主备份位置或辅助备份位置轻松启动虚拟机恢复操作。

SCV 使用 OVA 文件部署为 Linux 虚拟设备。该插件现在使用远程插件架构。远程插件在 vCenter 服务器之外运行，并托管在 SCV 虚拟设备上。

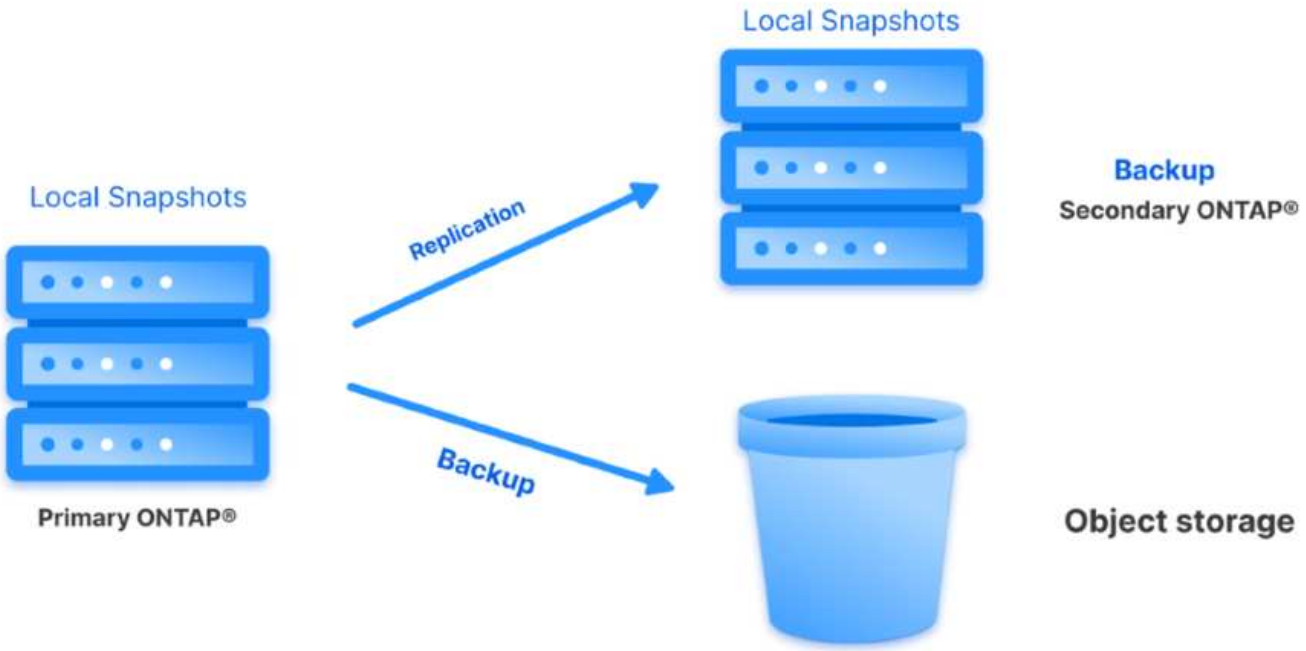
有关 SCV 的详细信息，请参阅 "SnapCenter Plug-in for VMware vSphere文档"。

NetApp Backup and Recovery 用于保护 **VMware** 工作负载

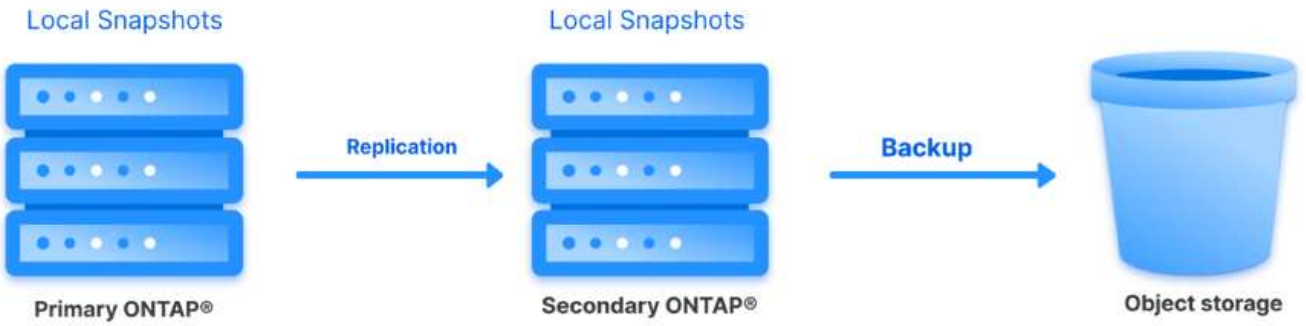
NetApp Backup and Recovery 是一种基于云的数据管理工具，可为本地和云环境中的各种备份和恢复操作提供单一控制平面。NetApp Backup and Recovery for VM 套件的一部分是一项与 SnapCenter Plugin for VMware vSphere（本地）集成的功能，可将数据副本扩展到云中的对象存储。这会建立异地数据的第三个副本，该副本来自主存储备份或二级存储备份。NetApp Backup and Recovery for VMs 使您可以轻松设置存储策略，从这两个本地位置中的任何一个传输数据副本。

在 NetApp Backup and Recovery 中选择主备份或二级备份作为源将导致实施以下两种拓扑之一：

扇出拓扑 – 当 SnapCenter Plug-in for VMware vSphere 启动备份时，将立即创建本地快照。然后，SCV 启动 SnapMirror 操作，将最新的快照复制到二级 ONTAP 集群。在 NetApp Backup and Recovery 中，策略将主 ONTAP 集群指定为源，以便将数据的快照副本传输到您选择的云提供商中的对象存储。



级联拓扑 – 使用 SCV 创建主数据副本和辅助数据副本与上述扇出拓扑完全相同。但是，这次在 NetApp Backup and Recovery 中创建了一个策略，指定对象存储的备份将来自辅助 ONTAP 集群。



NetApp Backup and Recovery 可以将本地 ONTAP 快照的备份副本创建到 AWS Glacier、Azure Blob 和 GCP 存档存储。



AWS Glacier and Deep Glacier



Azure Blob Archive



GCP Archive Storage

此外，您可以使用NetApp StorageGRID作为对象存储备份目标。有关StorageGRID 的更多信息，请参阅 "StorageGRID登录页面"。

▼ 解决方案部署概述

此列表提供了配置此解决方案以及从 SCV 和 NetApp Console 执行备份和还原操作所需的高级步骤：

1. 配置ONTAP集群之间的SnapMirror关系以用于主数据和辅助数据副本。
2. 为 VMware vSphere 配置SnapCenter插件。
   a. 添加存储系统
   b. 创建备份策略
   c. 创建资源组
   d. 运行备份第一个备份作业
3. 为虚拟机配置 NetApp Backup and Recovery
   a. 添加工作环境
   b. 发现 SCV 和 vCenter 设备
   c. 创建备份策略
   d. 激活备份
4. 使用 SCV 从主存储和辅助存储恢复虚拟机。
5. 使用 NetApp Console 从对象存储还原虚拟机。

▼ 前提条件

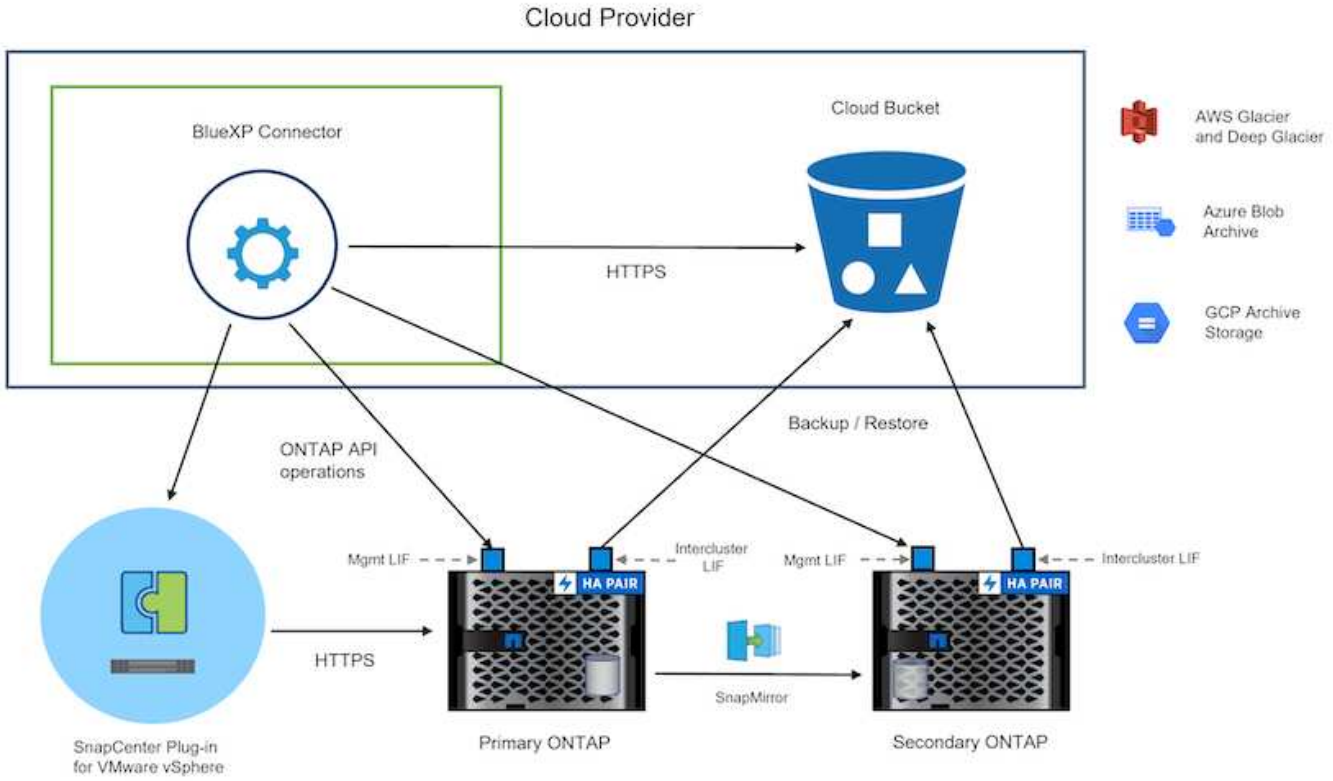
此解决方案的目的是展示在 VMware vSphere 中运行并位于由NetApp ONTAP托管的 NFS 数据存储上的虚拟机的数据保护。此解决方案假定以下组件已配置并可供使用：

1. 具有连接到 VMware vSphere 的 NFS 或 VMFS 数据存储的ONTAP存储集群。 NFS 和 VMFS 数据存储均受支持。此解决方案采用了 NFS 数据存储。
2. 为用于 NFS 数据存储库的卷建立了具有SnapMirror关系的辅助ONTAP存储集群。
3. 为用于对象存储备份的云提供商安装的控制台代理。
4. 要支持的虚拟机位于主ONTAP存储集群上的 NFS 数据存储库上。

5. 控制台代理和本地 ONTAP 存储集群管理接口之间的网络连接。
6. 控制台代理和本地 SCV 设备 VM 之间，以及控制台代理和 vCenter 之间的网络连接。
7. 本地ONTAP集群间 LIF 与对象存储服务之间的网络连接。
8. 为主ONTAP存储集群和辅助 ONTAP 存储集群上的管理 SVM 配置的 DNS。更多信息请参阅 "配置 DNS 以进行主机名解析"。

高级架构

该解决方案的测试/验证是在实验室中进行的，该实验室可能与最终部署环境匹配，也可能不匹配。



解决方案部署

在此解决方案中，我们提供了有关部署和验证解决方案的详细说明，该解决方案利用 SnapCenter Plug-in for VMware vSphere 以及备份和恢复，来执行位于本地数据中心的 VMware vSphere 集群中的 Windows 和 Linux 虚拟机的备份和恢复。此设置中的虚拟机存储在由 ONTAP A300 存储集群托管的 NFS 数据存储中。此外，单独的 ONTAP A300 存储集群用作使用 SnapMirror 复制的卷的二级目标。此外，在 Amazon Web Services 和 Azure Blob 上托管的对象存储被用作第三个数据副本的目标。

我们将介绍如何为由 SCV 管理的备份的辅助副本创建 SnapMirror 关系，以及在 SCV 和 NetApp Console 中配置备份作业。

有关适用SnapCenter Plug-in for VMware vSphere的详细信息，请参阅 "SnapCenter Plug-in for VMware vSphere文档"。

有关备份和恢复的详细信息，请参见 "备份和恢复文档"。

SnapCenter Plug-in for VMware vSphere使用ONTAP SnapMirror技术来管理二级SnapMirror和/或SnapVault副本到二级ONTAP集群的传输。

SCV 备份策略可以选择使用SnapMirror或SnapVault关系。主要区别在于，当使用SnapMirror选项时，策略中为备份配置的保留计划在主位置和辅助位置将是相同的。 SnapVault专为归档而设计，使用此选项时，可以使用SnapMirror关系为二级ONTAP存储集群上的快照副本建立单独的保留计划。

设置 SnapMirror 关系可以在 NetApp Console 中完成，其中许多步骤是自动化的，也可以使用 System Manager 和 ONTAP CLI 完成。下面将讨论所有这些方法。

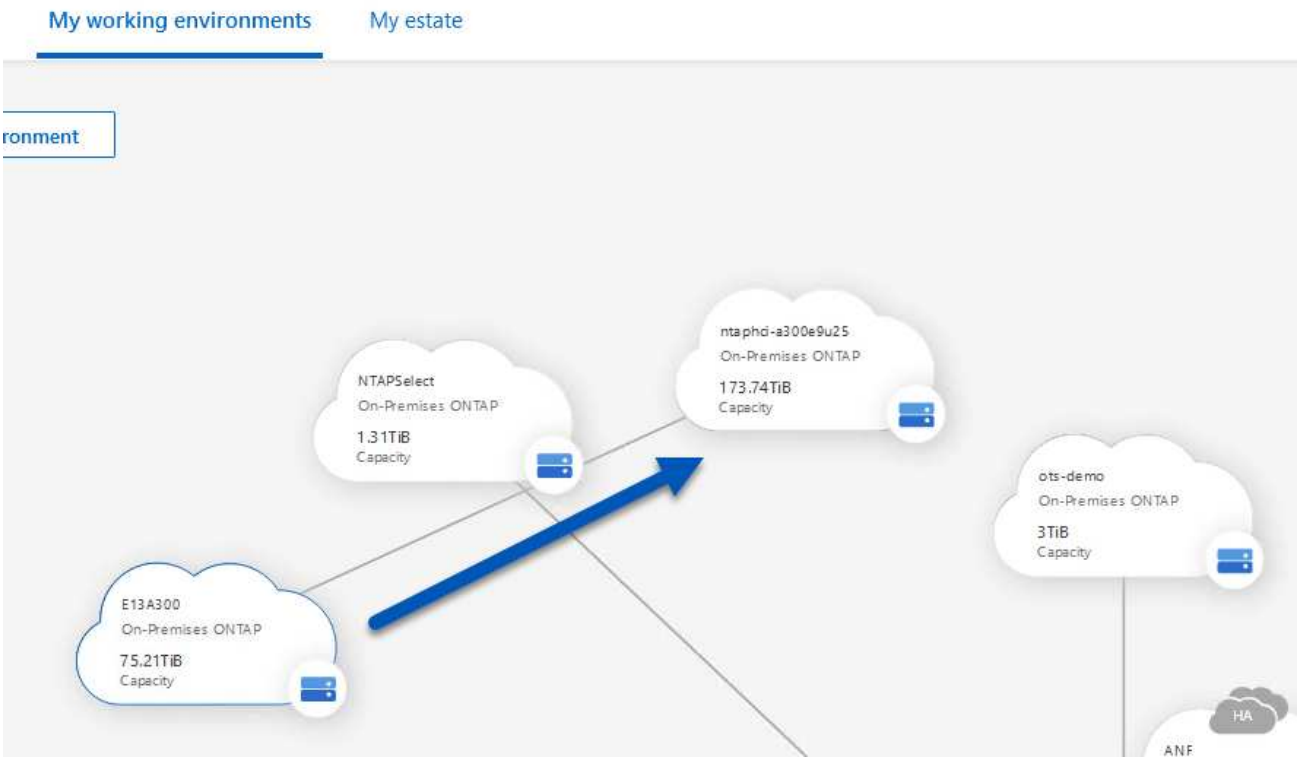
使用 **NetApp Console** 建立 **SnapMirror** 关系

必须从 NetApp Console 完成以下步骤：

▼ 主 **ONTAP** 存储系统和辅助**ONTAP**存储系统的复制设置

首先登录 NetApp Console 并导航到系统。

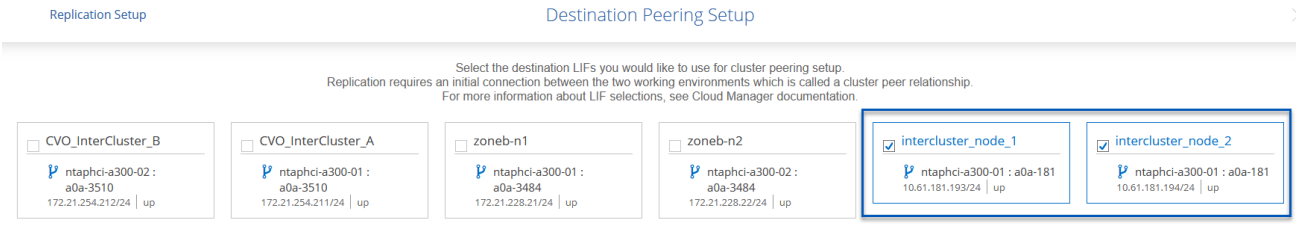
1. 将源（主） ONTAP存储系统拖放到目标（辅助） ONTAP存储系统上。



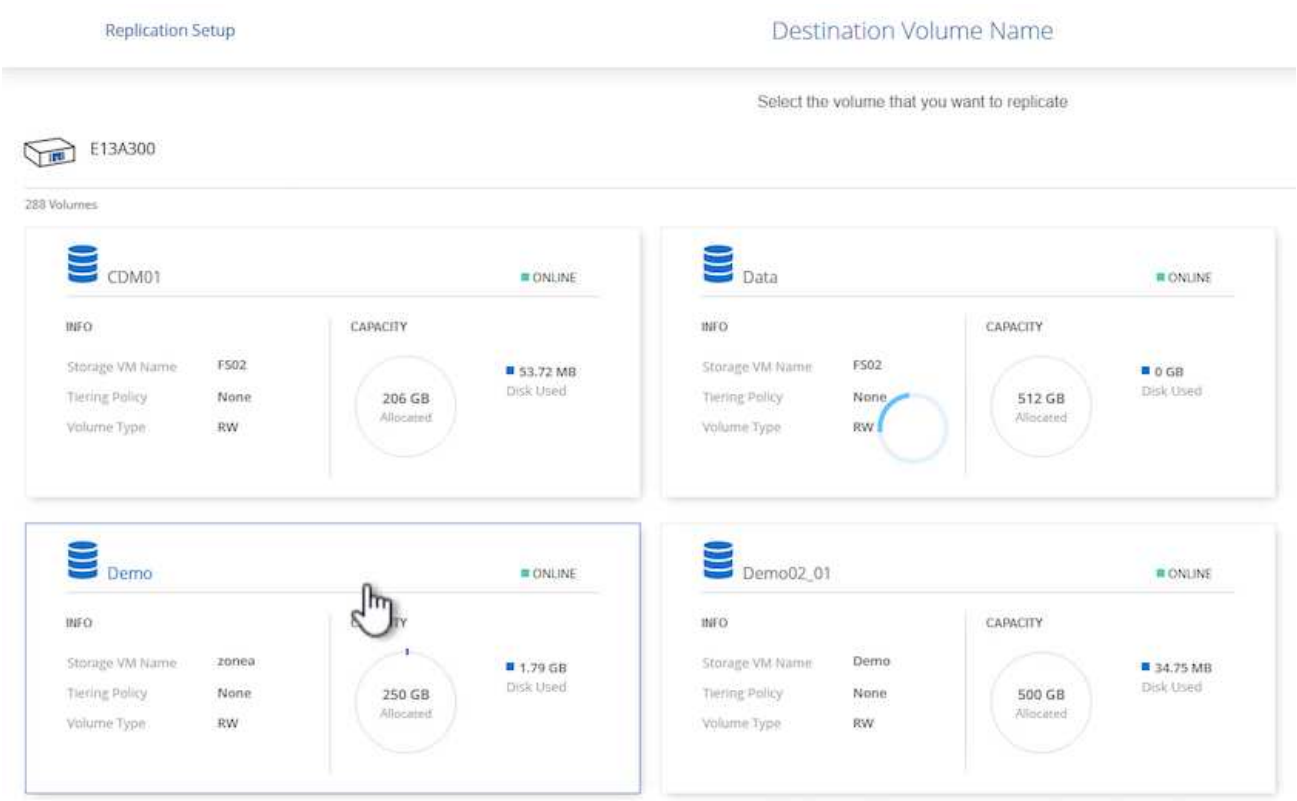
2. 从出现的菜单中选择*复制*。



3. 在“目标对等设置”页面上，选择用于存储系统之间连接的目标集群间 LIF。

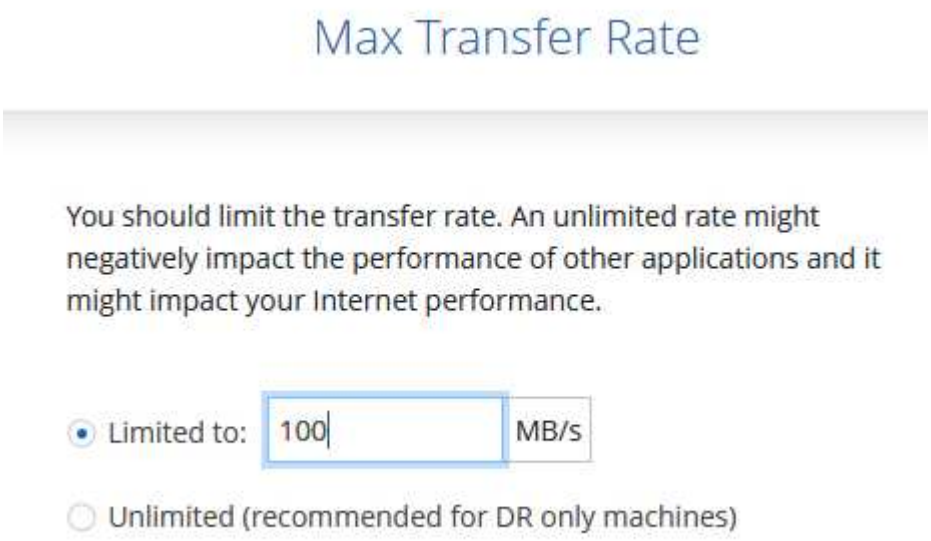


4. 在“目标卷名称”页面上，首先选择源卷，然后填写目标卷名称并选择目标 SVM 和聚合。单击“下一步”继续。

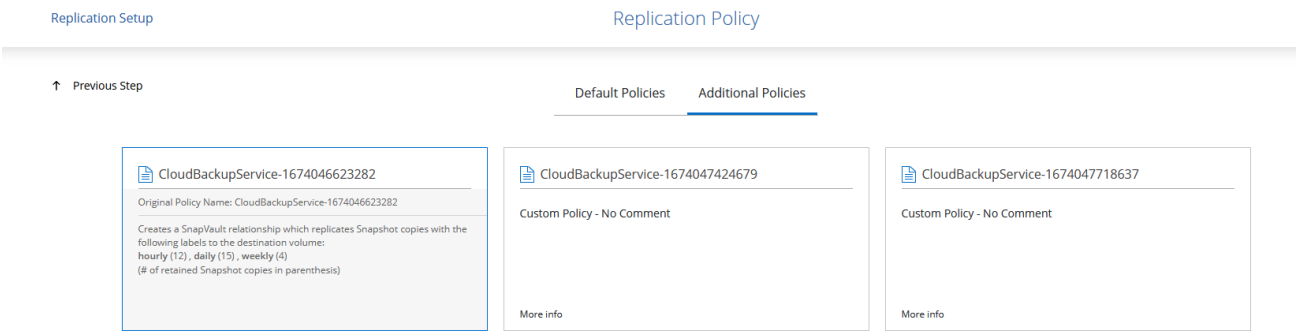




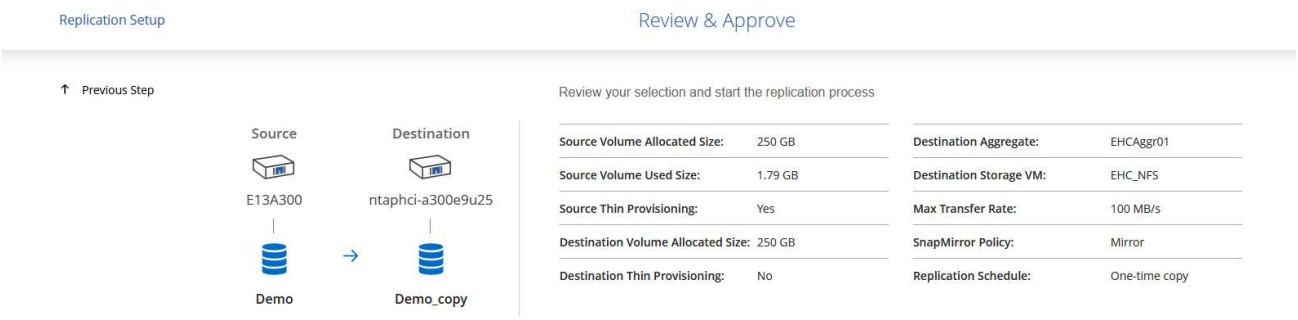
5. 选择进行复制的最大传输速率。



6. 选择确定二次备份保留计划的策略。此策略可以预先创建（请参阅下面*创建快照保留策略*步骤中的手动过程），也可以在需要时在事后进行更改。



7. 最后，检查所有信息并单击“**Go**”按钮开始复制设置过程。



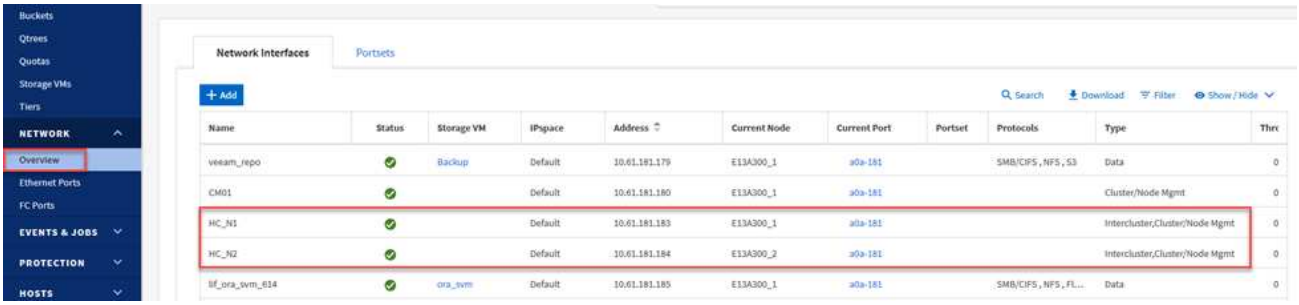
使用 **System Manager** 和**ONTAP CLI** 建立**SnapMirror**关系

建立SnapMirror关系所需的所有步骤都可以通过 System Manager 或ONTAP CLI 完成。以下部分提供了这两种方法的详细信息：

▼ 记录源和目标集群间逻辑接口

对于源和目标ONTAP集群，您可以从系统管理器或 CLI 检索集群间 LIF 信息。

1. 在ONTAP系统管理器中，导航到网络概览页面并检索配置为与安装了 FSx 的 AWS VPC 通信的类型：集群间的 IP 地址。



2. 要使用 CLI 检索集群间 IP 地址，请运行以下命令：

```
ONTAP-Dest::> network interface show -role intercluster
```

▼ 在**ONTAP**集群之间建立集群对等连接

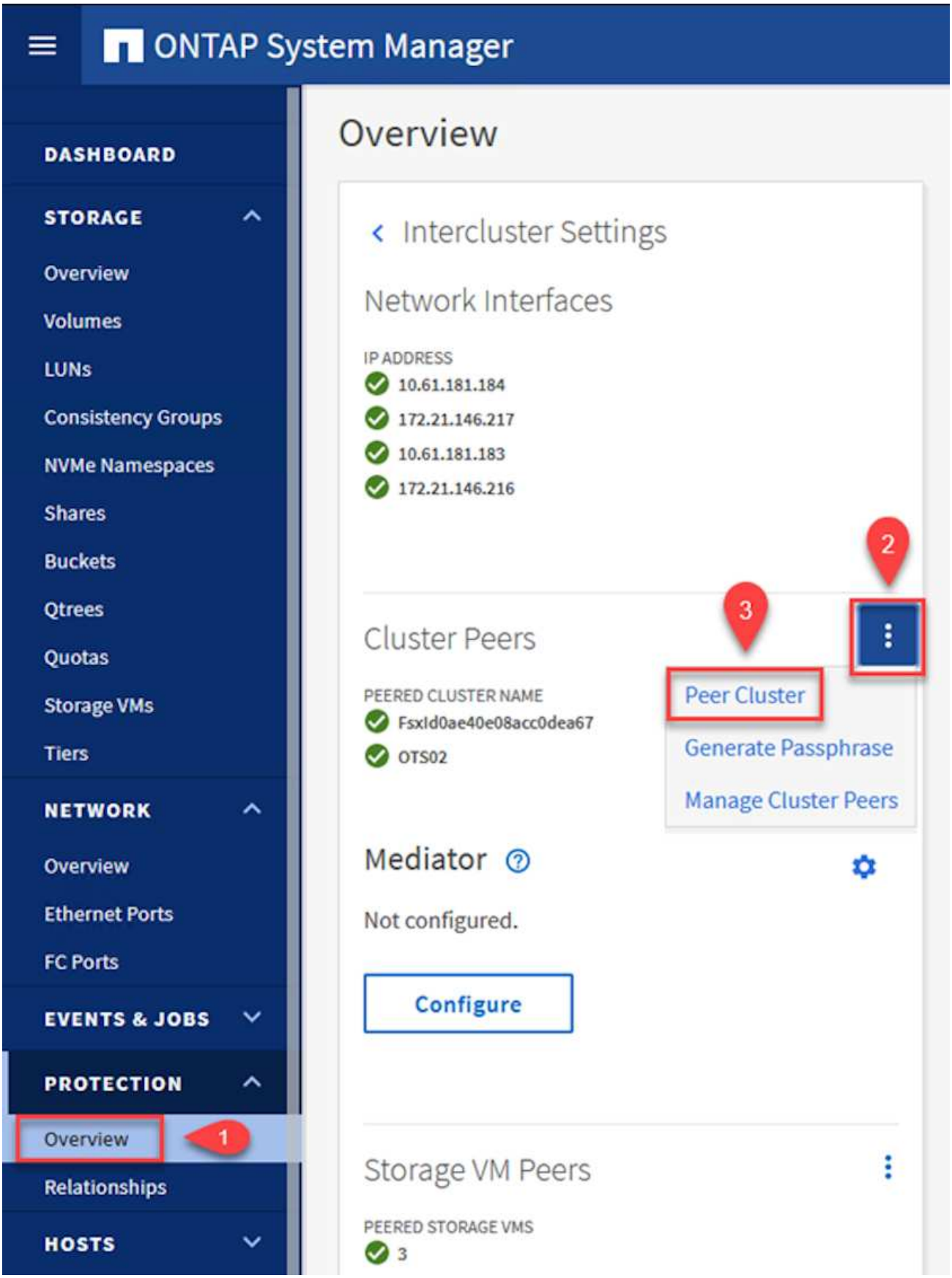
要在ONTAP集群之间建立集群对等连接，必须在另一个对等集群中确认在启动ONTAP集群中输入的唯一密

码。

1. ONTAP `cluster peer create`命令。出现提示时，请输入稍后在源集群上使用的唯一密码来完成创建过程。

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. 在源集群中，您可以使用ONTAP系统管理器或 CLI 建立集群对等关系。从ONTAP系统管理器中，导航到“保护”>“概览”，然后选择“对等集群”。

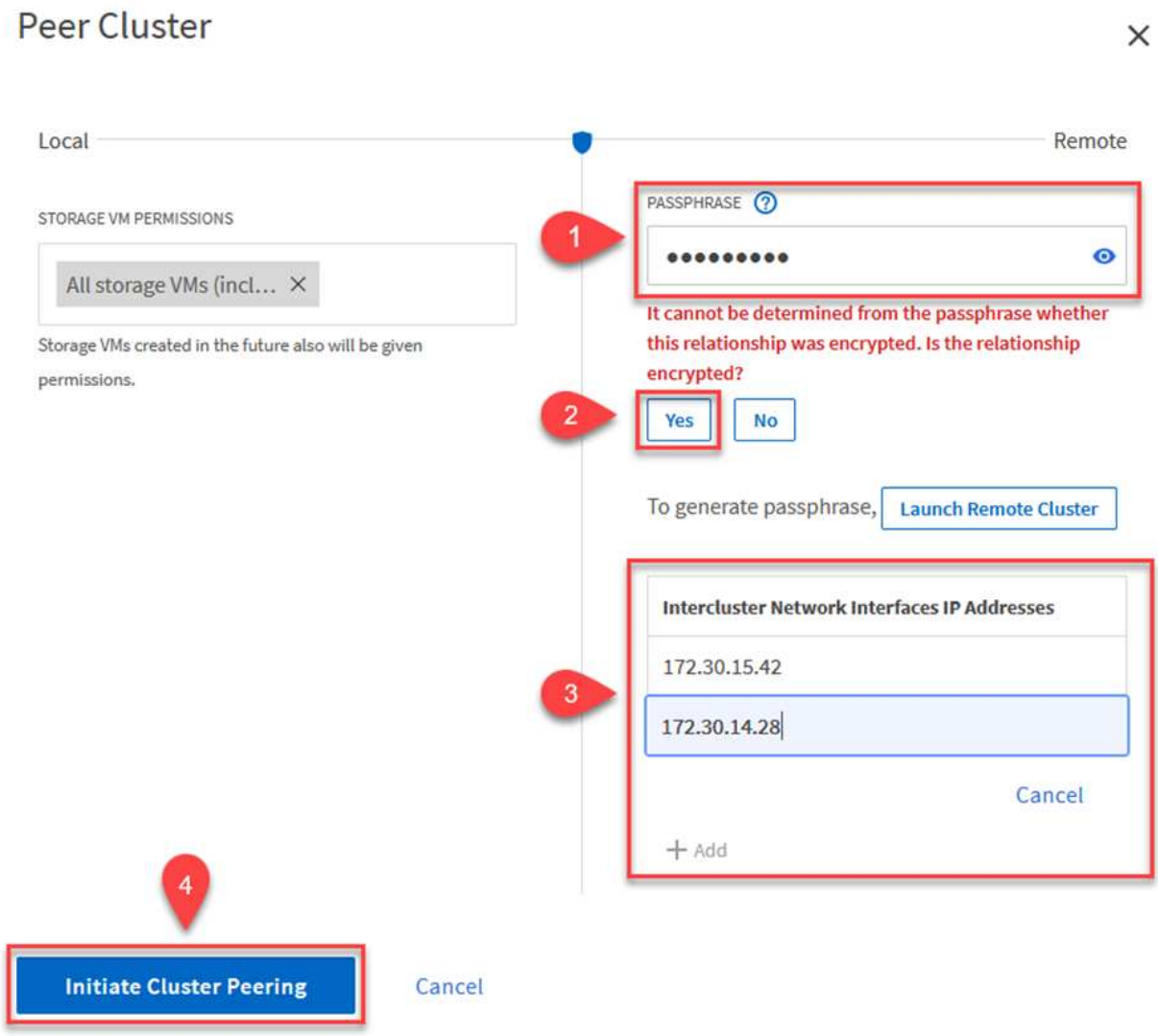


3. 在对等集群对话框中，填写所需信息：
   a. 输入用于在目标ONTAP集群上建立对等集群关系的密码。

b. 选择 `Yes`建立加密关系。

c. 输入目标ONTAP集群的集群间 LIF IP 地址。

d. 单击“启动集群对等”以完成该过程。



4. 使用以下命令从目标ONTAP集群验证集群对等关系的状态：

```
ONTAP-Dest::> cluster peer show
```

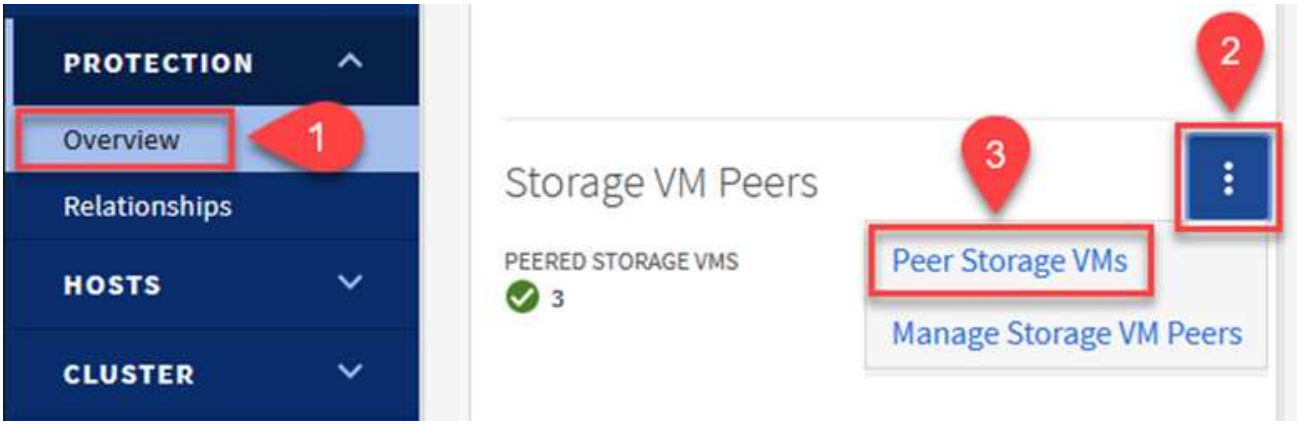
▼ 建立 **SVM** 对等关系

下一步是在包含将处于SnapMirror关系中的卷的目标存储虚拟机和源存储虚拟机之间建立 SVM 关系。

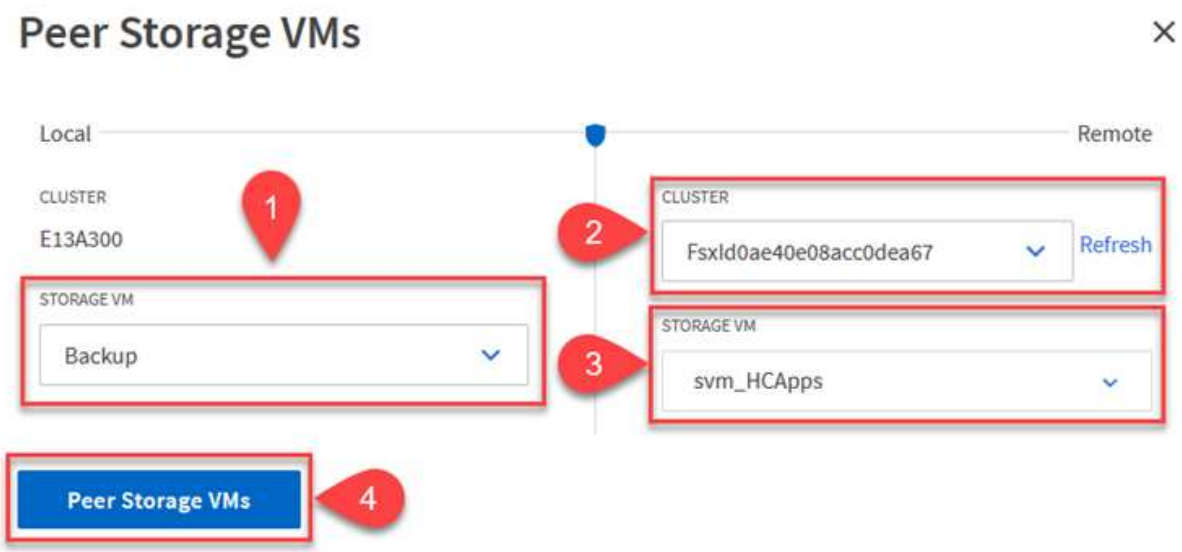
1. 从目标ONTAP集群，使用 CLI 中的以下命令创建 SVM 对等关系：

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 从源ONTAP集群，使用ONTAP系统管理器或 CLI 接受对等关系。
3. 从ONTAP系统管理器中，转到“保护”>“概览”，然后选择“存储虚拟机对等体”下的“对等存储虚拟机”。



4. 在对等存储虚拟机的对话框中，填写必填字段：
   - 源存储虚拟机
   - 目标集群
   - 目标存储虚拟机



5. 单击“对等存储虚拟机”以完成 SVM 对等连接过程。

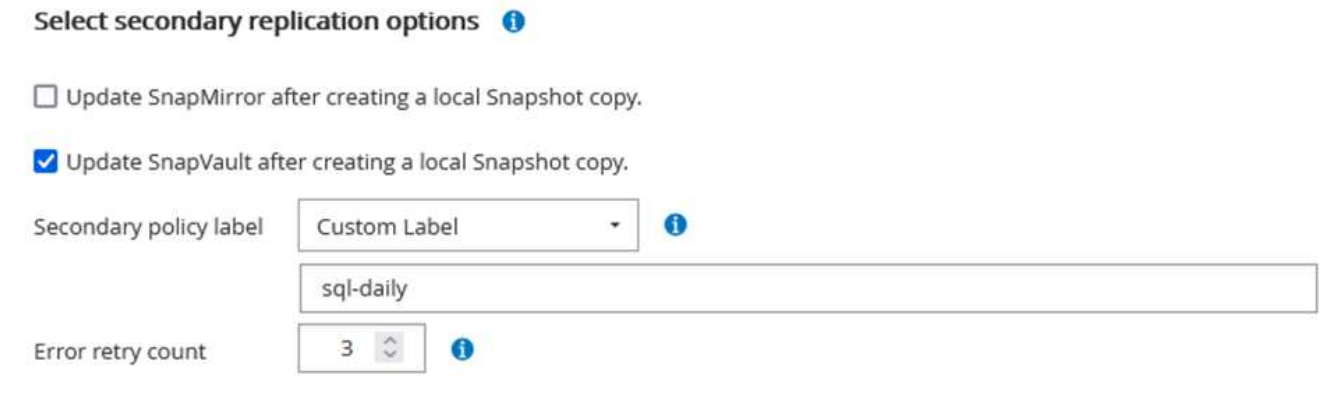
▼ 创建快照保留策略

SnapCenter管理主存储系统上作为快照副本存在的备份的保留计划。这是在SnapCenter中创建策略时建立的。 SnapCenter不管理保留在二级存储系统上的备份的保留策略。这些策略通过在辅助 FSx 集群上创建的SnapMirror策略单独进行管理，并与与源卷具有SnapMirror关系的目标卷相关联。

创建SnapCenter策略时，您可以选择指定一个辅助策略标签，该标签将添加到执行SnapCenter备份时生成的每个快照的SnapMirror标签中。

在二级存储上，这些标签与目标卷相关的策略规则相匹配，以强制保留快照。

以下示例显示了一个SnapMirror标签，该标签存在于作为用于 SQL Server 数据库和日志卷的每日备份的策略的一部分生成的所有快照上。



有关为 SQL Server 数据库创建SnapCenter策略的更多信息，请参阅 "SnapCenter文档"。

您必须首先创建一个SnapMirror策略，其中包含规定要保留的快照副本数量的规则。

1. 在 FSx 集群上创建SnapMirror策略。

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. 向具有与SnapCenter策略中指定的二级策略标签匹配的SnapMirror标签的策略添加规则。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

以下脚本提供了可以添加到策略的规则示例：

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

ⓘ 为每个SnapMirror标签和要保留的快照数量（保留期）创建附加规则。

▼ 创建目标卷

要在ONTAP上创建将作为源卷快照副本接收者的目标卷，请在目标ONTAP集群上运行以下命令：

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

▼ 在源卷和目标卷之间创建**SnapMirror**关系

要在源卷和目标卷之间创建SnapMirror关系，请在目标ONTAP集群上运行以下命令：

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

▼ 初始化**SnapMirror**关系

初始化 SnapMirror 关系。此过程启动从源卷生成的新快照并将其复制到目标卷。

要创建卷，请在目标ONTAP集群上运行以下命令：

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

SnapCenter Plug-in for VMware vSphere

安装后，可以从 vCenter Server Appliance 管理界面访问SnapCenter Plug-in for VMware vSphere。 SCV 将管理安装到 ESXi 主机并包含 Windows 和 Linux VM 的 NFS 数据存储的备份。

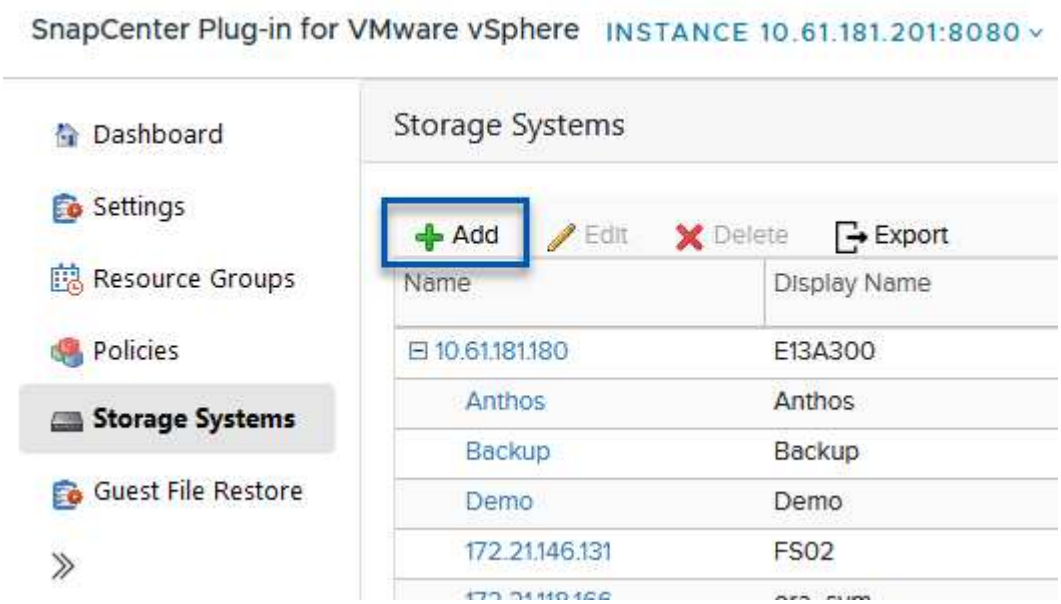
回顾 "数据保护工作流程"有关配置备份所涉及的步骤的更多信息，请参阅 SCV 文档的部分。

要配置虚拟机和数据存储的备份，需要从插件界面完成以下步骤。

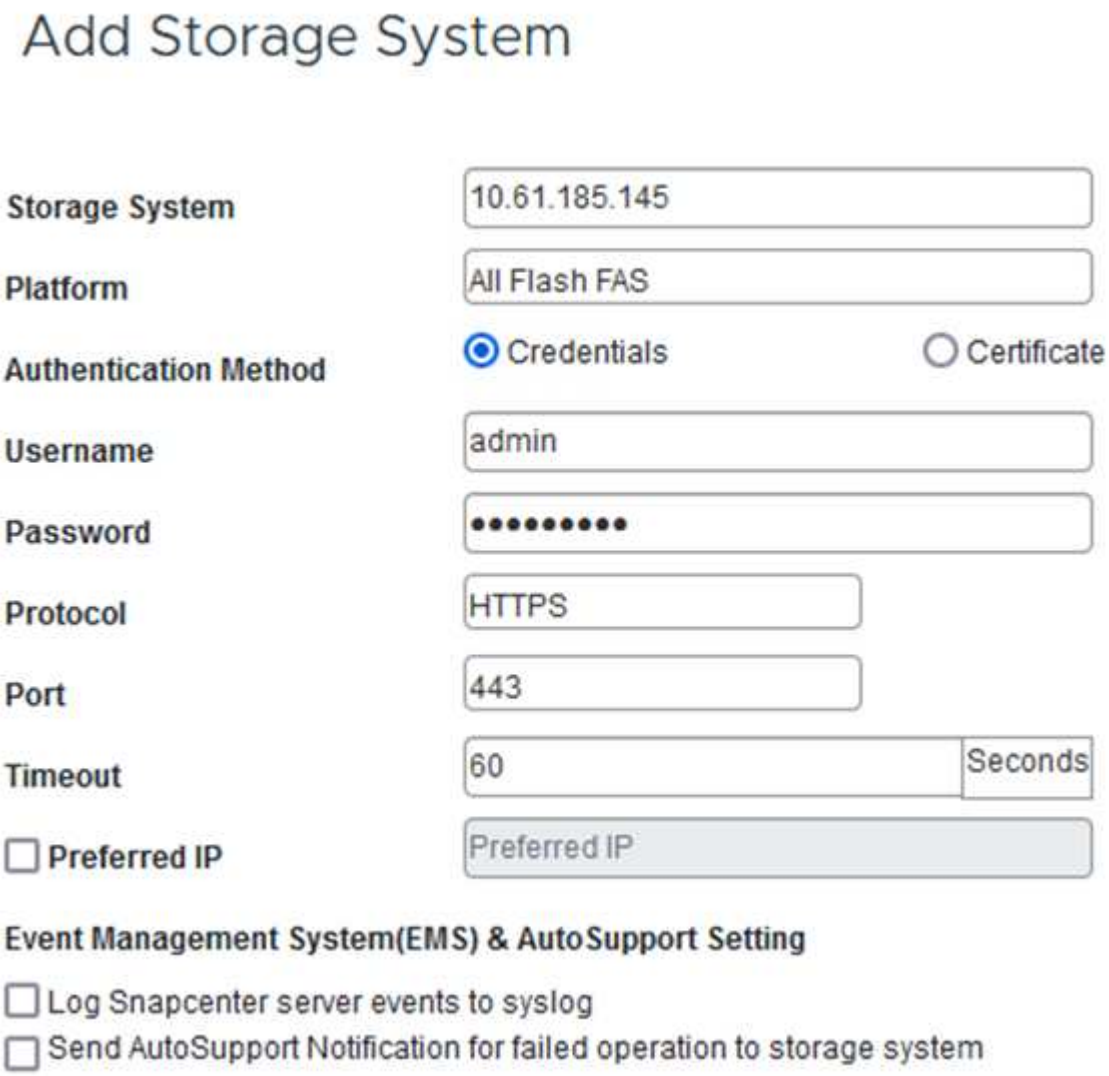
▼ **Discovery ONTAP**存储系统

发现用于主备份和辅助备份的ONTAP存储集群。

1. 在SnapCenter Plug-in for VMware vSphere中，导航到左侧菜单中的“存储系统”，然后单击“添加”按钮。



2. 填写主ONTAP存储系统的凭据和平台类型，然后单击“添加”。



3. 对辅助ONTAP存储系统重复此过程。

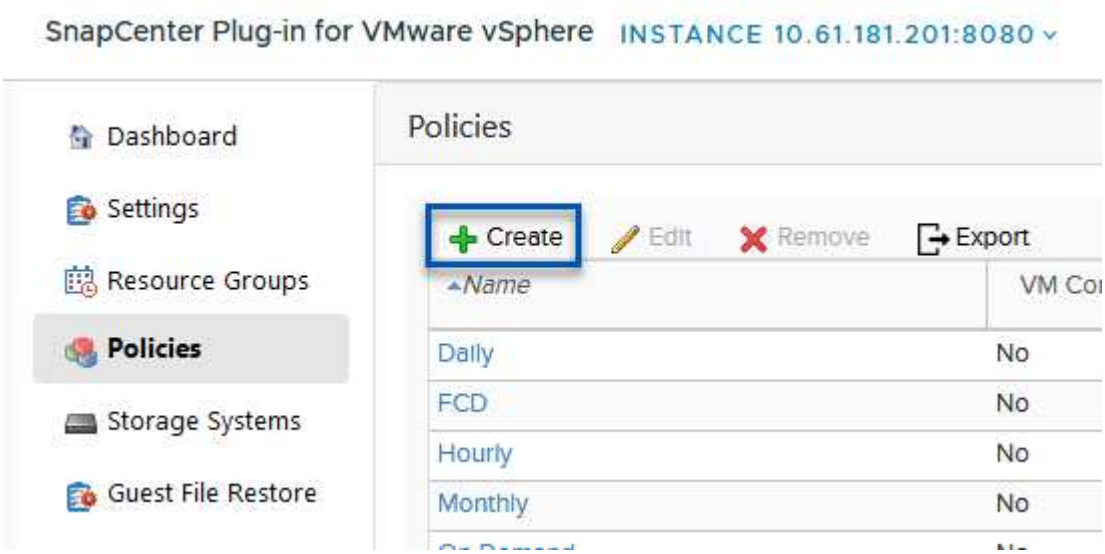
▼ 创建 **SCV** 备份策略

策略指定 SCV 管理的备份的保留期、频率和复制选项。

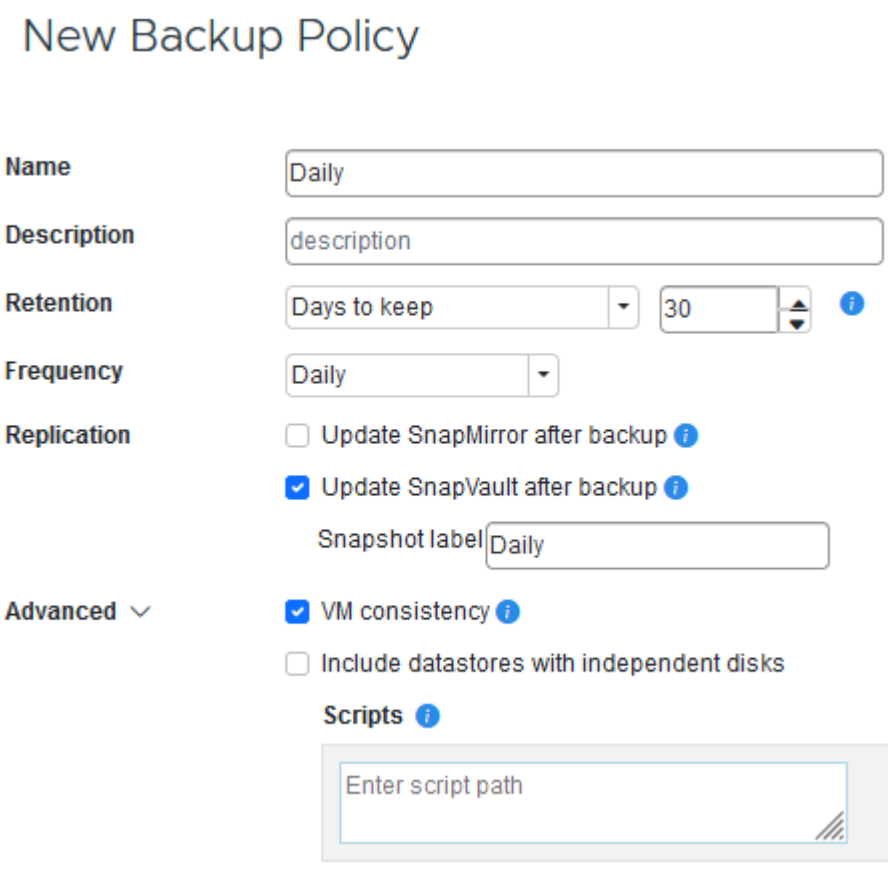
回顾 "为虚拟机和数据存储创建备份策略"请参阅文档部分以获取更多信息。

要创建备份策略，请完成以下步骤：

1. 在SnapCenter Plug-in for VMware vSphere中，导航到左侧菜单中的“策略”，然后单击“创建”按钮。



2. 指定策略的名称、保留期、频率和复制选项以及快照标签。



在SnapCenter插件中创建策略时，您将看到SnapMirror和SnapVault的选项。如果您选择SnapMirror，则策略中指定的保留计划对于主快照和辅助快照将相同。如果您选择SnapVault，则辅助快照的保留计划将基于使用SnapMirror关系实施的单独计划。当您希望延长二次备份的保留期时，这很有用。

快照标签非常有用，因为它们可用于为复制到辅助 ONTAP 集群的 SnapVault 副本制定具有特定保留期的策略。当 SCV 与 NetApp Data Services 一起使用时，快照标签字段必须

为空或[underline]#匹配#备份策略中指定的标签。

3. 对每个所需的策略重复该过程。例如，针对每日、每周和每月备份制定单独的策略。

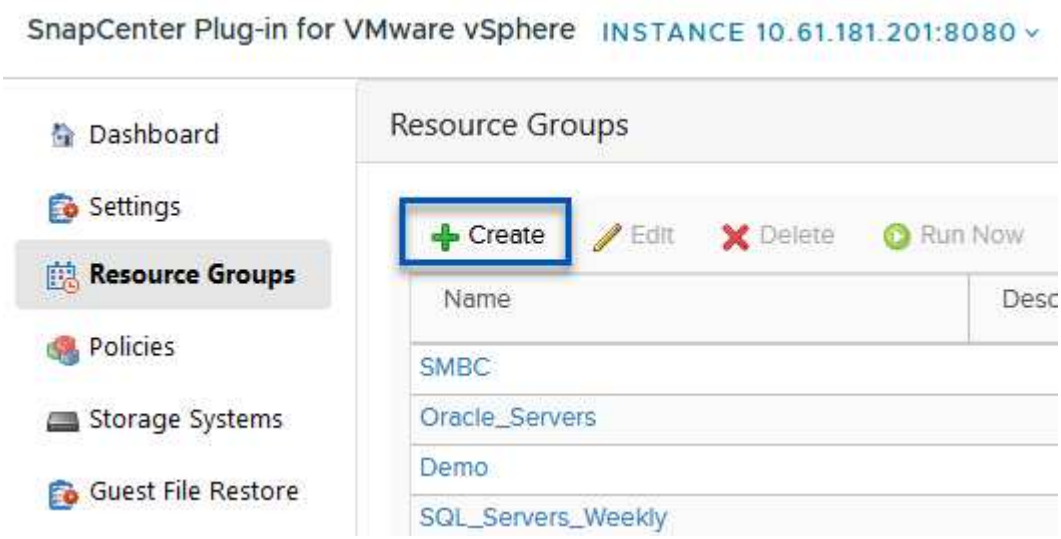
▼ 创建资源组

资源组包含要包含在备份作业中的数据存储区和虚拟机，以及相关的策略和备份计划。

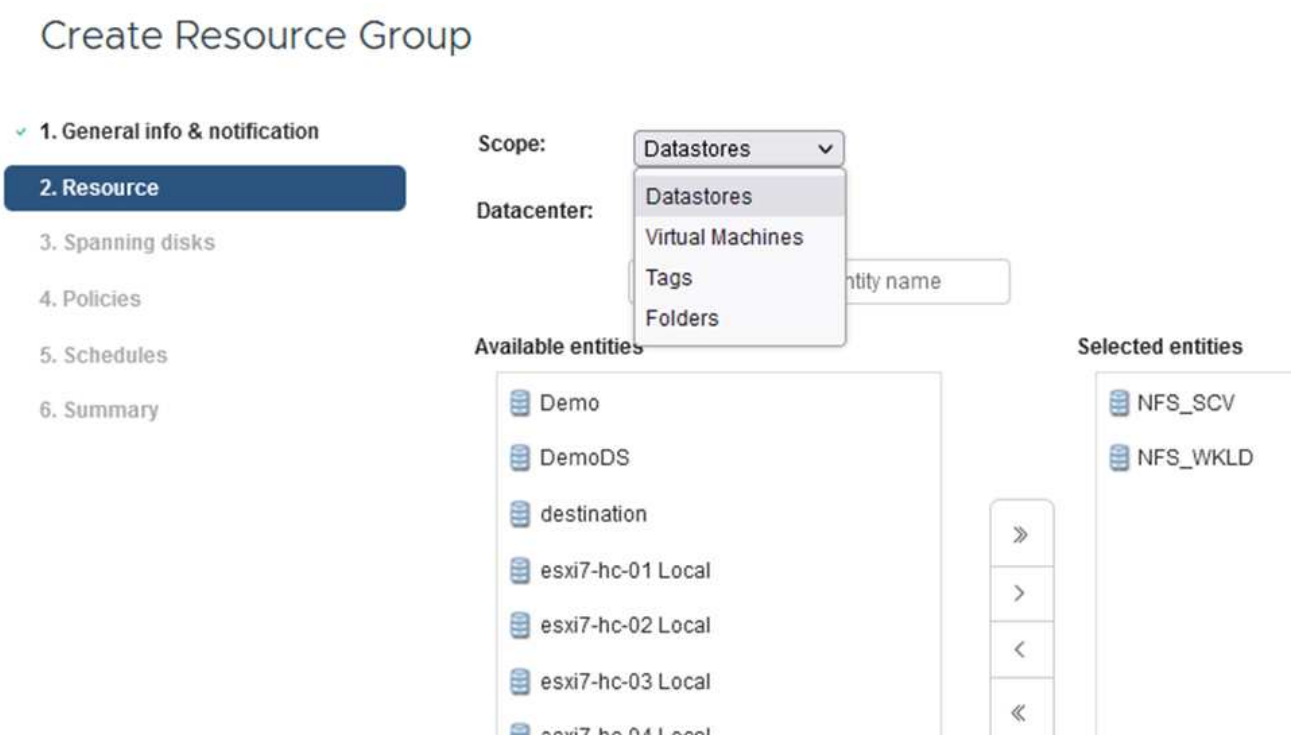
回顾 "创建资源组"请参阅文档部分以获取更多信息。

要创建资源组，请完成以下步骤。

1. 在SnapCenter Plug-in for VMware vSphere中，导航到左侧菜单中的“资源组”，然后单击“创建”按钮。

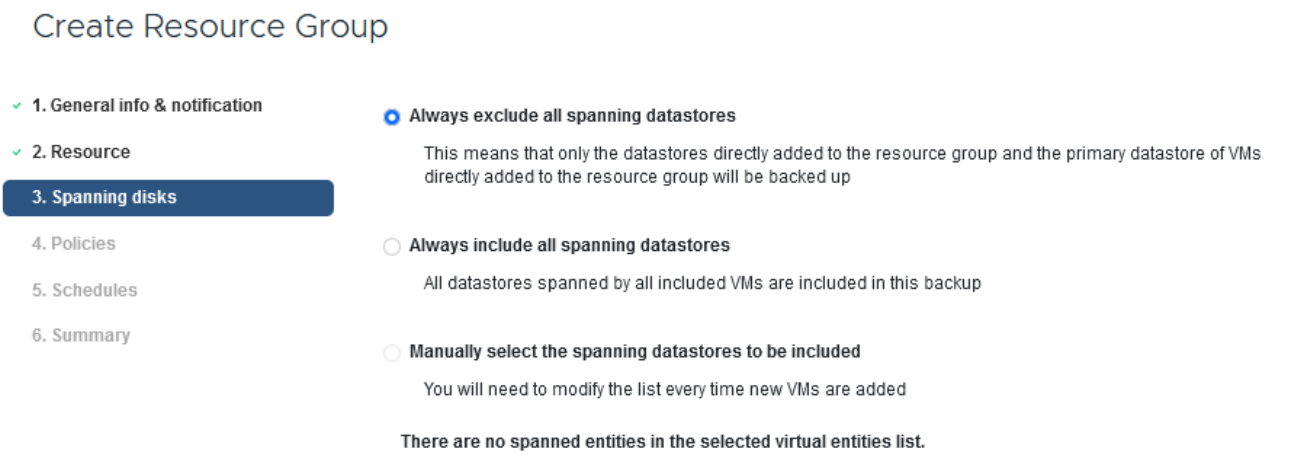


2. 在创建资源组向导中，输入组的名称和描述，以及接收通知所需的信息。点击“下一步”
3. 在下一页上，选择希望包含在备份作业中的数据存储和虚拟机，然后单击“下一步”。



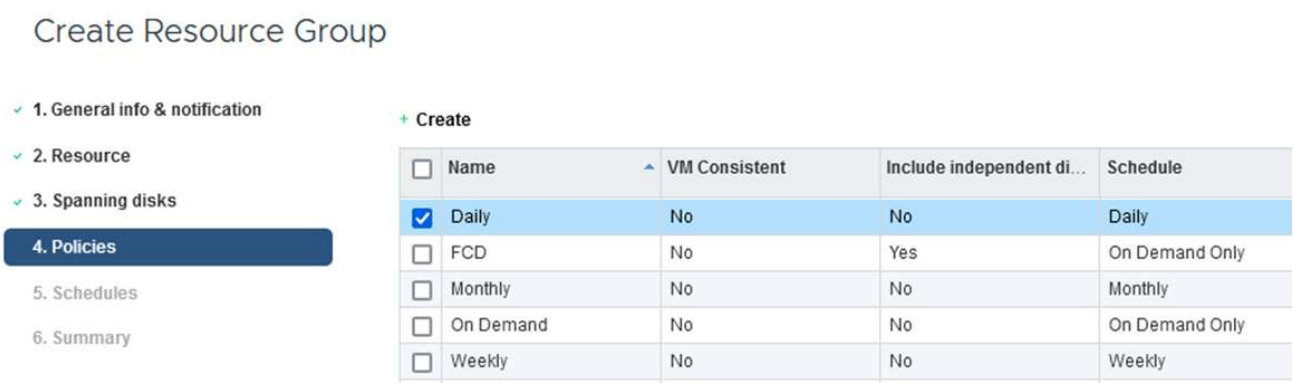
您可以选择特定的虚拟机或整个数据存储。无论您选择哪种方式，整个卷（和数据存储）都会被备份，因为备份是拍摄底层卷快照的结果。在大多数情况下，选择整个数据存储是最简单的。但是，如果您希望在恢复时限制可用虚拟机的列表，则可以仅选择一部分虚拟机进行备份。

4. 选择跨位于多个数据存储上的 VMDK 的虚拟机的数据存储选项，然后单击“下一步”。



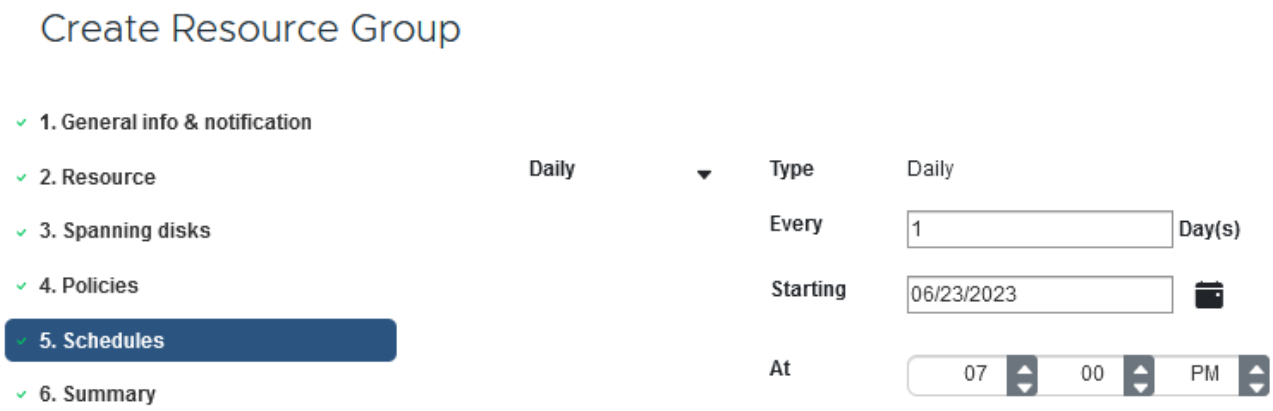
用于保护 VMware 工作负载的备份和恢复当前不支持备份具有跨多个数据存储的 VMDK 的虚拟机。

5. 在下一页上，选择与资源组关联的策略，然后单击“下一步”。



使用备份和恢复将 SCV 管理的快照备份到对象存储时，每个资源组只能与单个策略关联。

6. 选择一个计划来确定备份的运行时间。单击“下一步”。

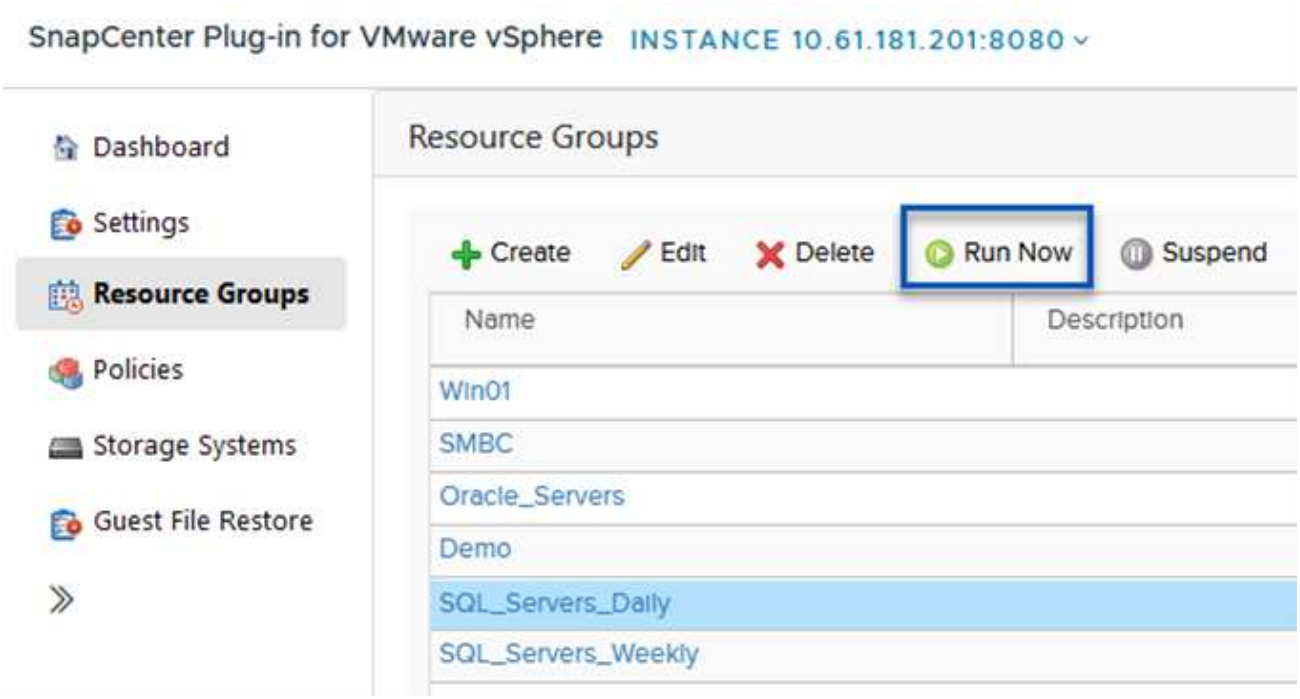


7. 最后，查看摘要页面，然后单击“完成”以完成资源组创建。

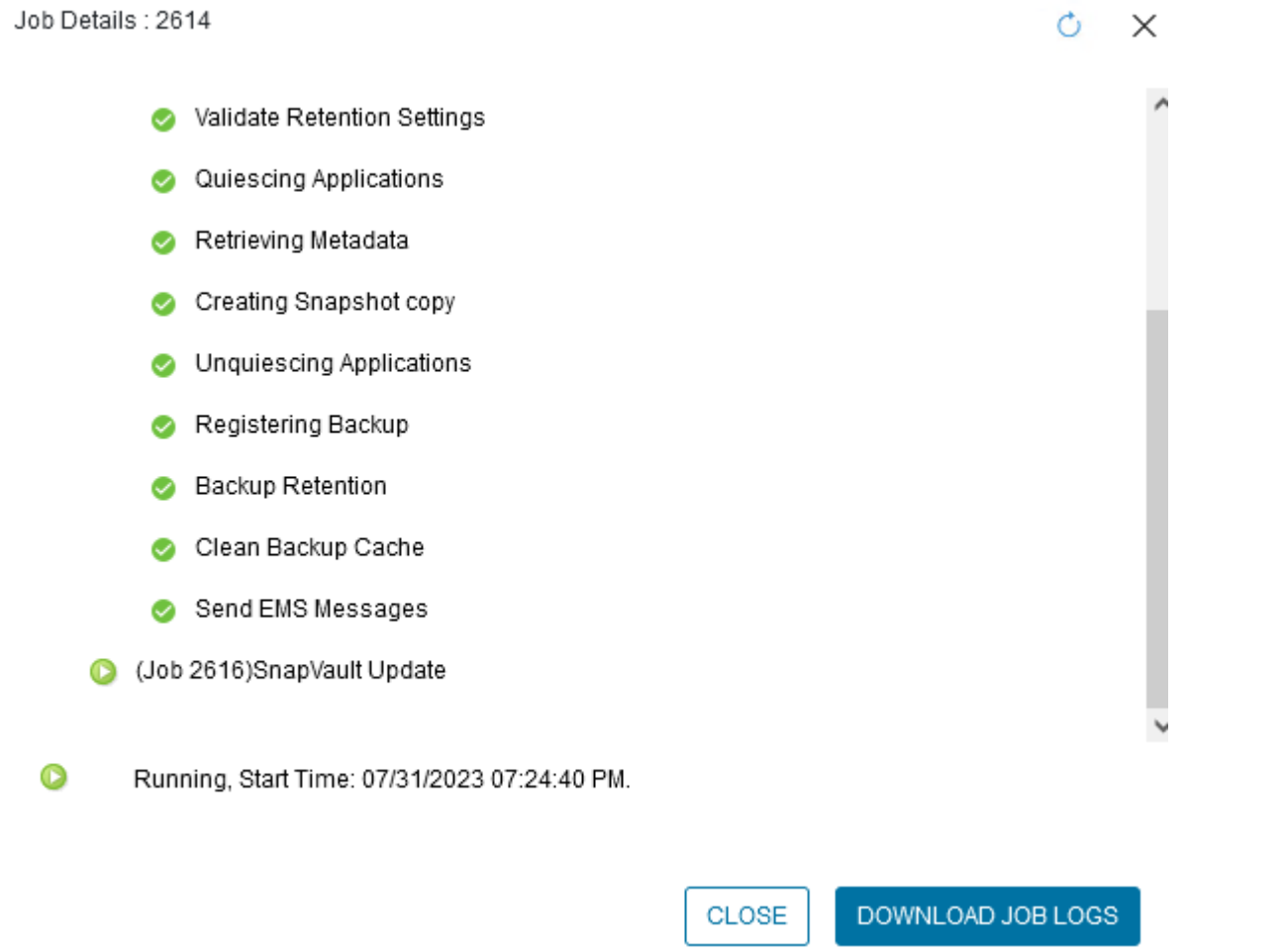
▼ 运行备份作业

在最后一步中，运行备份作业并监控其进度。必须至少在 SCV 中成功完成一个备份作业，然后才能从 NetApp Console 发现资源。

1. 在SnapCenter Plug-in for VMware vSphere中，导航到左侧菜单中的“资源组”。
2. 要启动备份作业，请选择所需的资源组并单击*立即运行*按钮。



3. 要监控备份作业，请导航至左侧菜单上的“仪表板”。在“最近的工作活动”下单击工作 ID 号来监控工作进度。



为了使 NetApp Console 能够有效地管理数据基础架构，需要事先安装 Console 代理。Console 代理执行发现资源和管理数据操作所涉及的操作。

有关 Console 代理的更多信息，请参见 NetApp Console 文档中的 "了解控制台代理"。

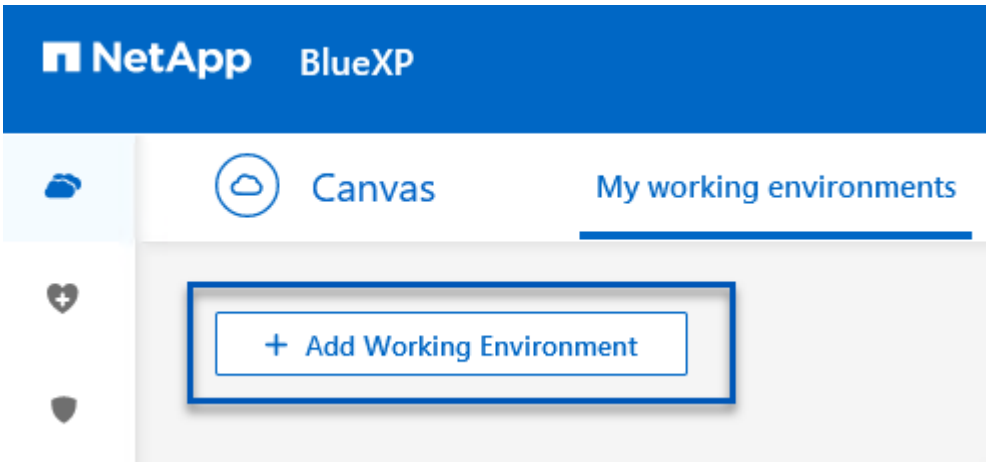
为正在使用的云提供商安装代理后，将可从系统查看对象存储的图形表示。

要配置 Backup and Recovery 以备份由本地 SCV 管理的数据，请完成以下步骤：

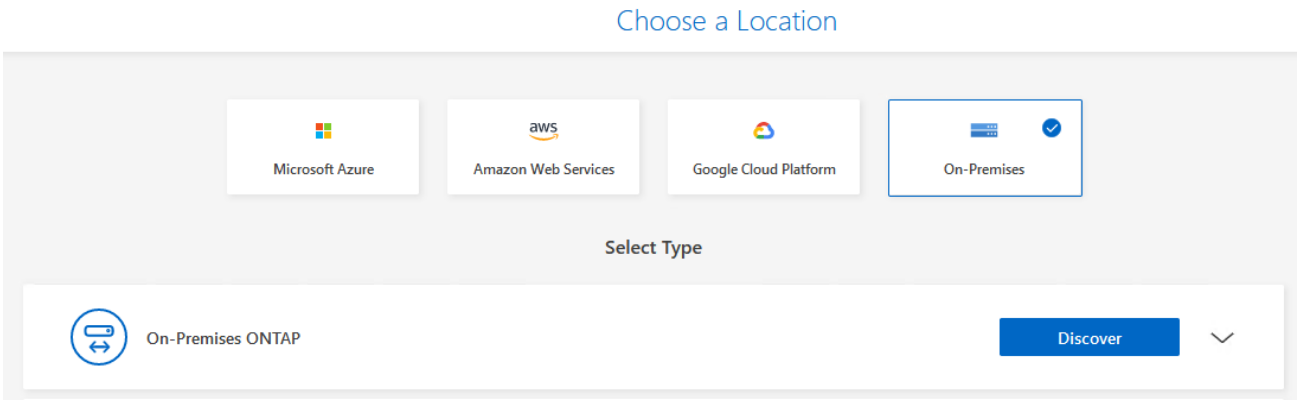
▼ 将 **ONTAP** 存储系统添加到系统

第一步是将本地 ONTAP 存储系统添加到 NetApp Console。

1. 从系统单击 **+** 添加 开始。



2. 从位置选择中选择*On-Premises*，然后单击*Discover*按钮。



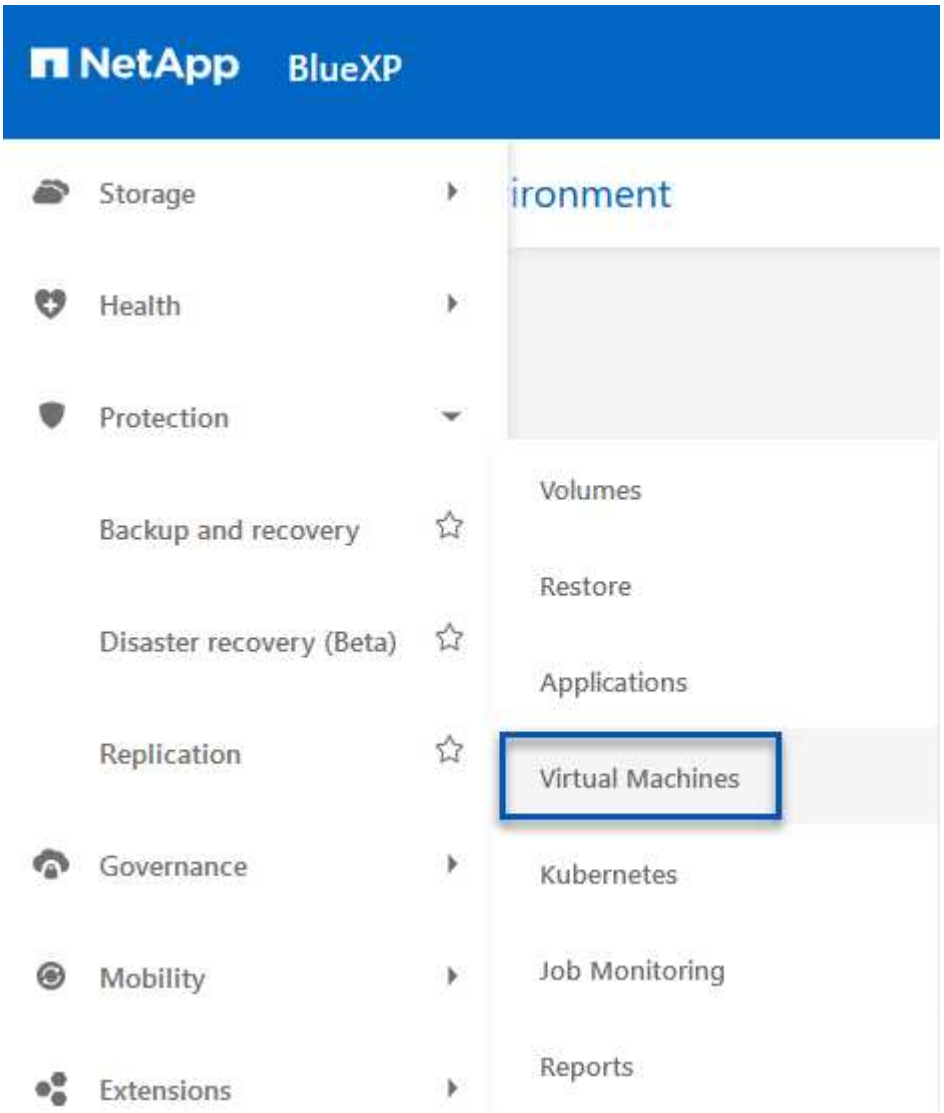
3. 填写ONTAP存储系统的凭据，然后单击 发现 按钮添加工作环境。



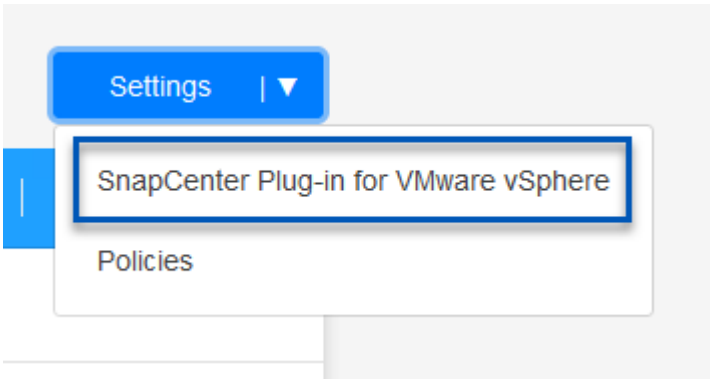
▼ 发现本地 **SCV** 设备和 **vCenter**

要发现本地数据存储和虚拟机资源，请添加 SCV 数据代理的信息和 vCenter 管理设备的凭据。

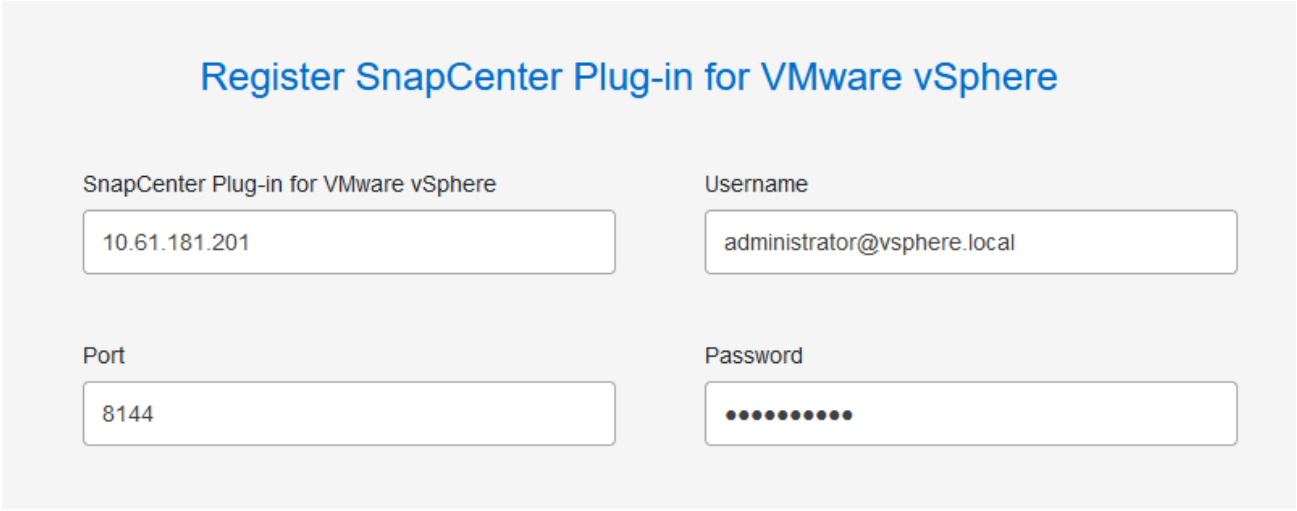
1. 从 NetApp Console 左侧菜单选择 保护 **>** 备份和恢复 **>** 工作负载 **> VMware**



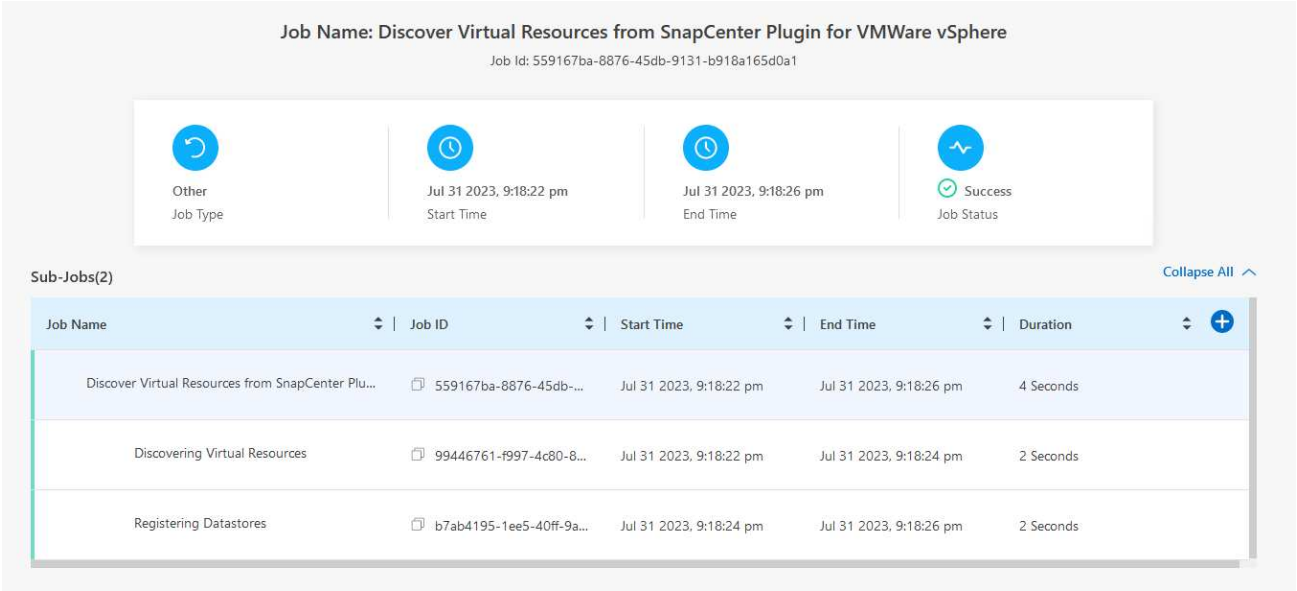
2. 从虚拟机主屏幕访问*设置*下拉菜单并选择*SnapCenter Plug-in for VMware vSphere*。



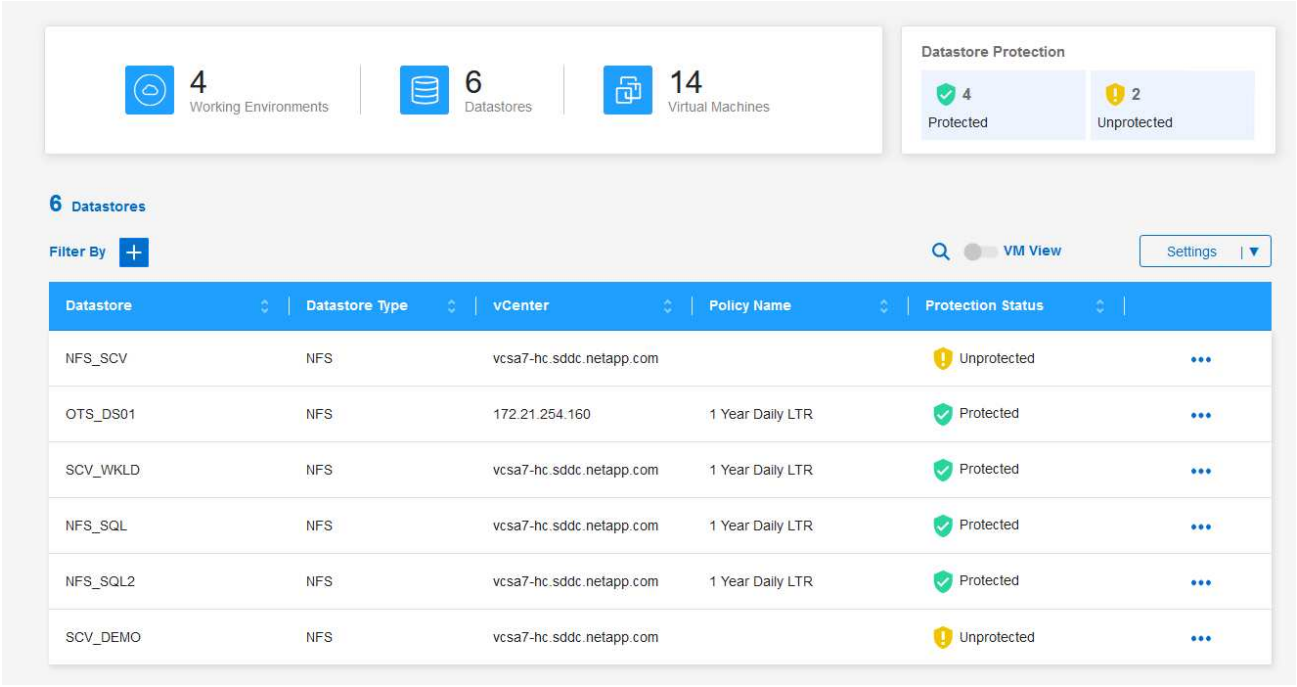
3. 单击*注册*按钮，然后输入SnapCenter插件设备的 IP 地址和端口号以及 vCenter 管理设备的用户名和密码。单击“注册”按钮开始发现过程。



4. 您可以从“作业监控”选项卡监控作业的进度。



5. 一旦发现完成，您将能够查看所有已发现的 SCV 设备上的数据存储和虚拟机。

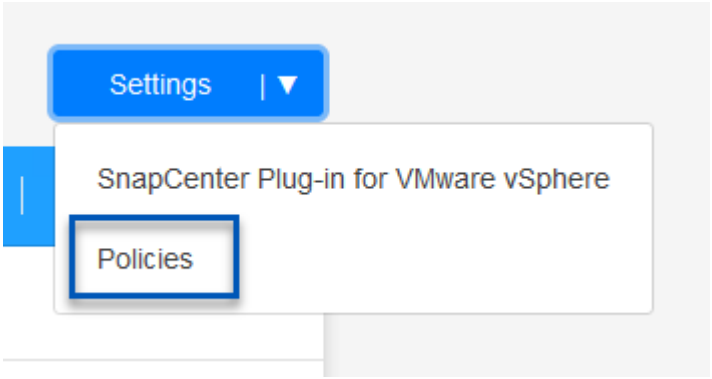


▼ 创建备份策略

在适用于虚拟机的 NetApp Backup and Recovery 中，创建策略以指定保留期限、备份源和归档策略。

有关创建保护组的详细信息，请参阅 "创建保护组"。

1. 从适用于虚拟机的 NetApp Backup and Recovery 主页，访问*设置*下拉菜单并选择*策略*。



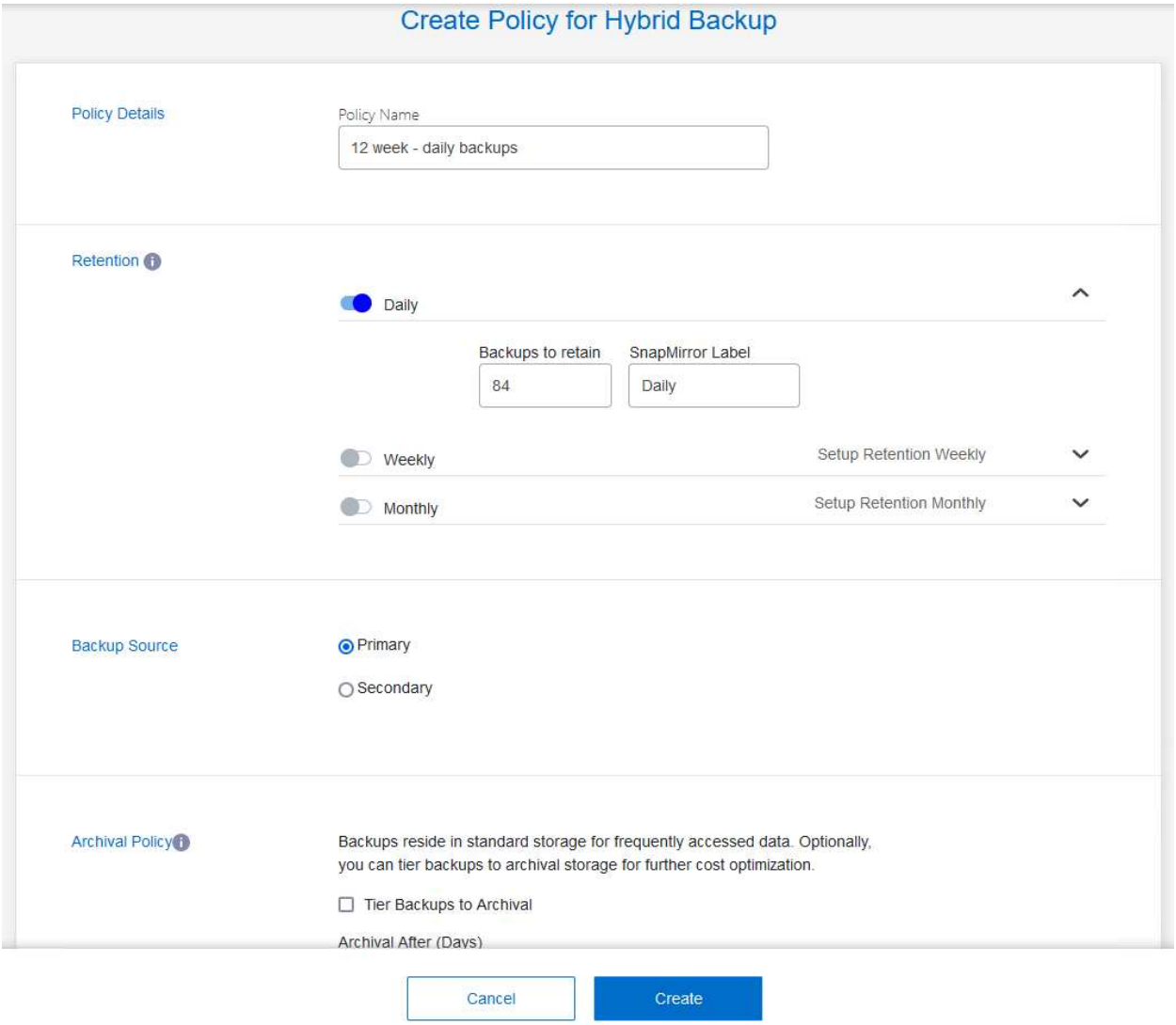
2. 单击“创建策略”以访问“创建混合备份策略”窗口。

   a. 添加策略名称

   b. 选择所需的保留期限

   c. 选择备份是否来自主或辅助本地ONTAP存储系统

   d. 或者，指定在多长时间后将备份分层到档案存储以节省更多成本。



此处输入的SnapMirror标签用于标识要应用该策略的备份。标签名称必须与相应的本地 SCV 策略中的标签名称匹配。

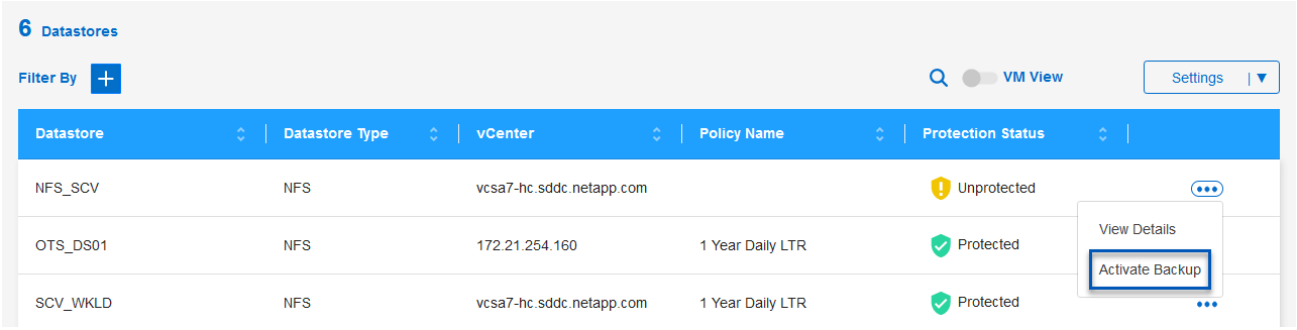
3. 单击“创建”完成策略创建。

▼ 将数据存储备份到 **Amazon Web Services**

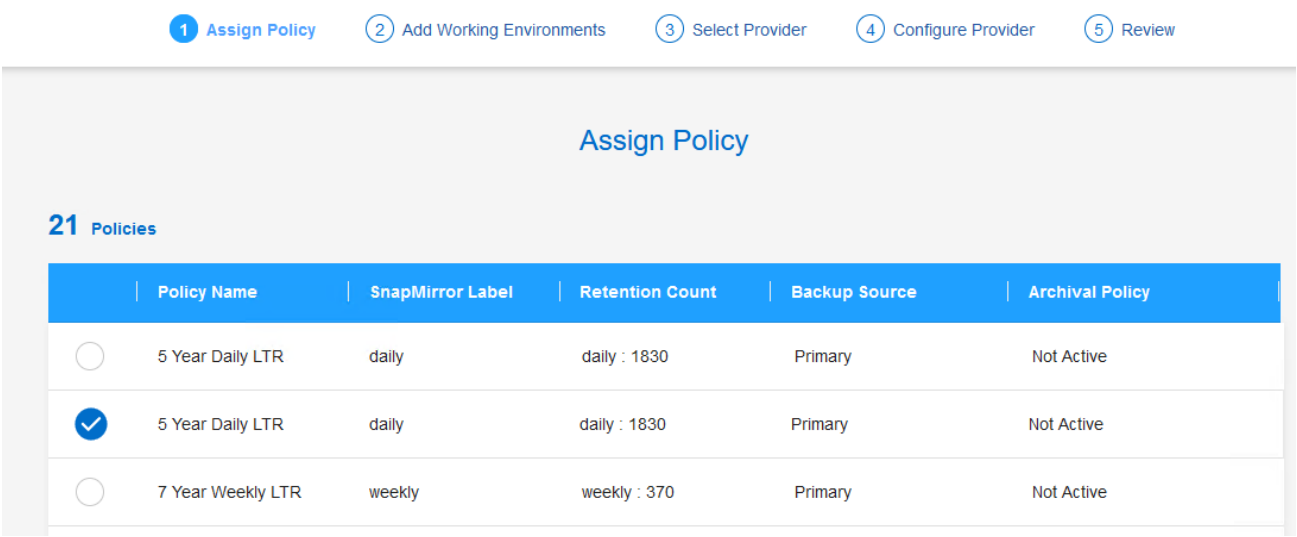
最后一步是激活各个数据存储区和虚拟机的数据保护。以下步骤概述了如何激活 AWS 备份。

有关更多信息，请参阅 "备份 VMware 工作负载"。

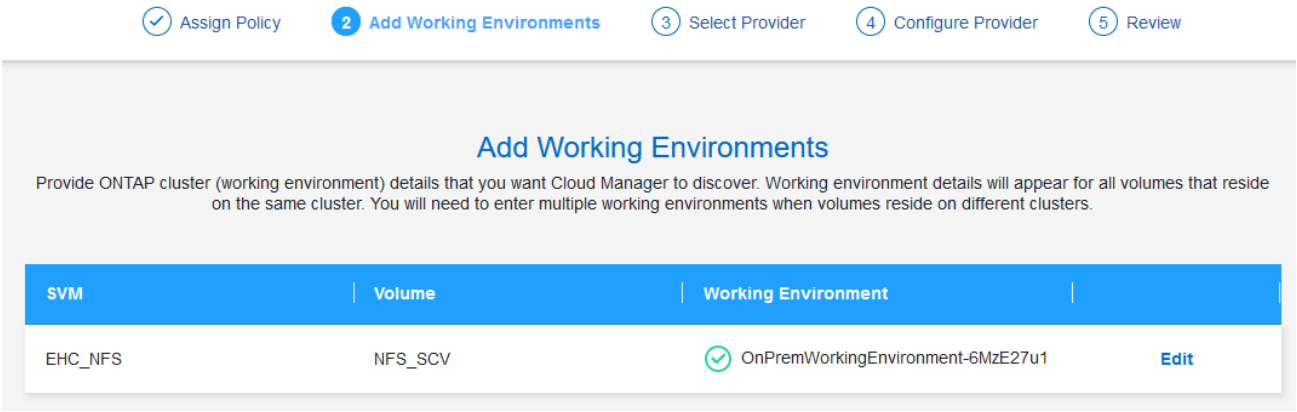
1. 从 NetApp Backup and Recovery for Virtual Machines 主页，访问要备份的数据存储的设置下拉菜单，然后选择*激活备份*。



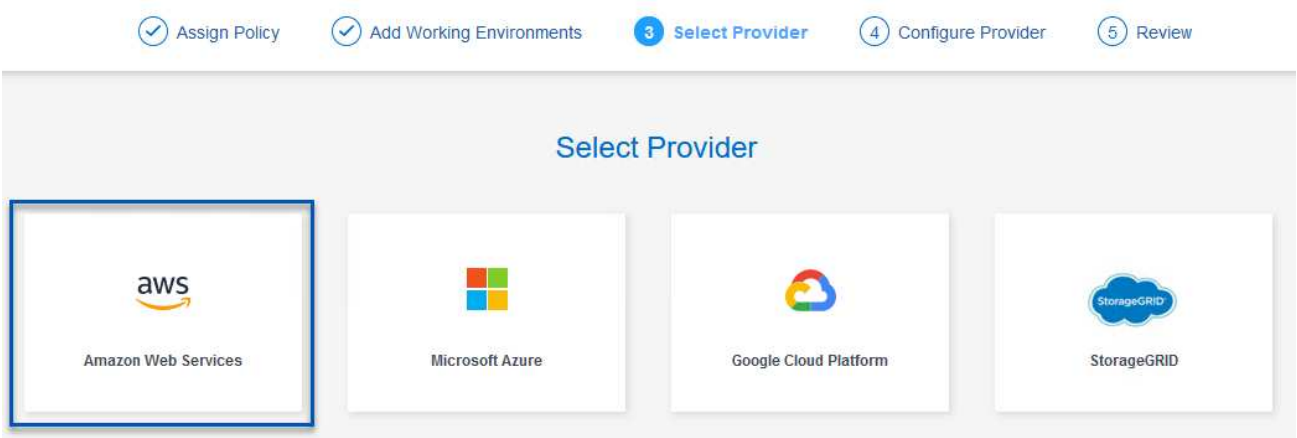
2. 分配用于数据保护操作的策略，然后单击“下一步”。



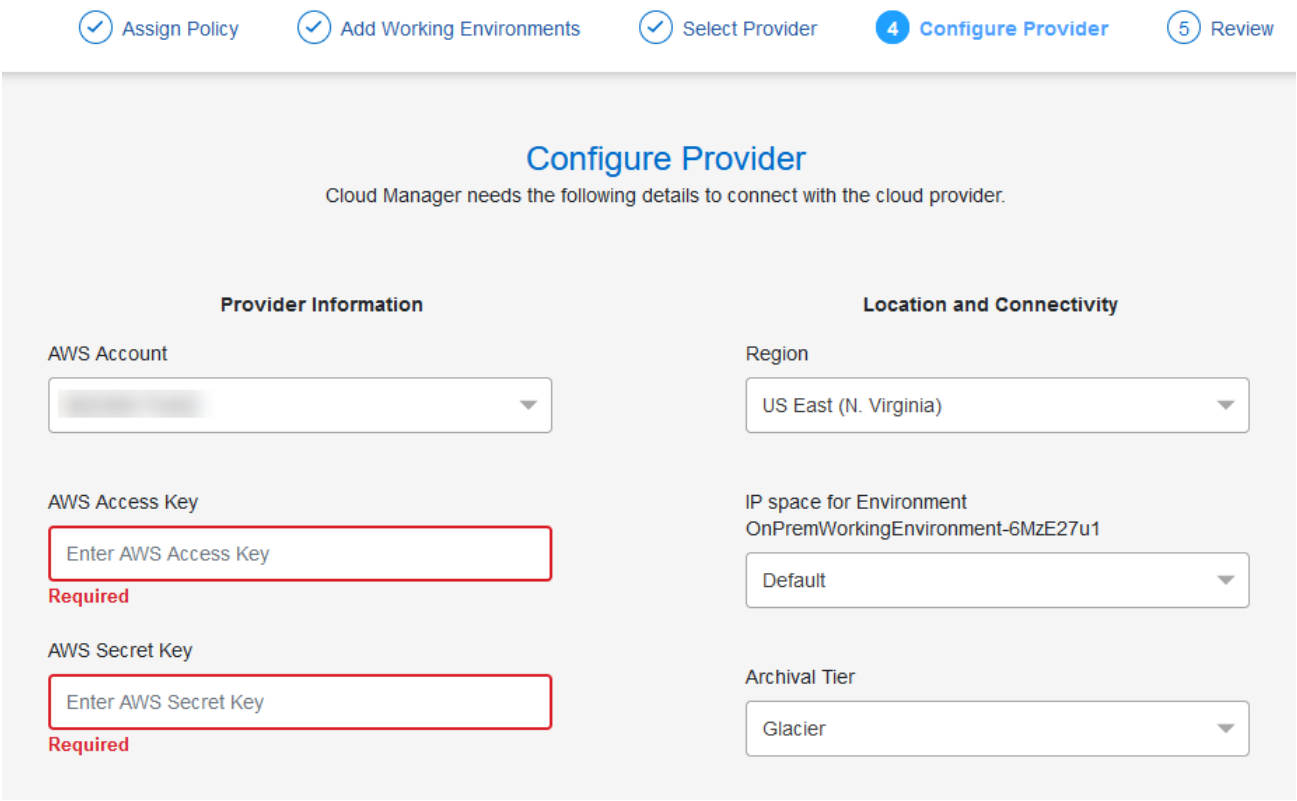
3. 如果之前已经发现了工作环境，则在“添加工作环境”页面上应该会出现带有复选标记的数据存储和工作环境。如果之前没有发现工作环境，您可以在这里添加它。单击“下一步”继续。



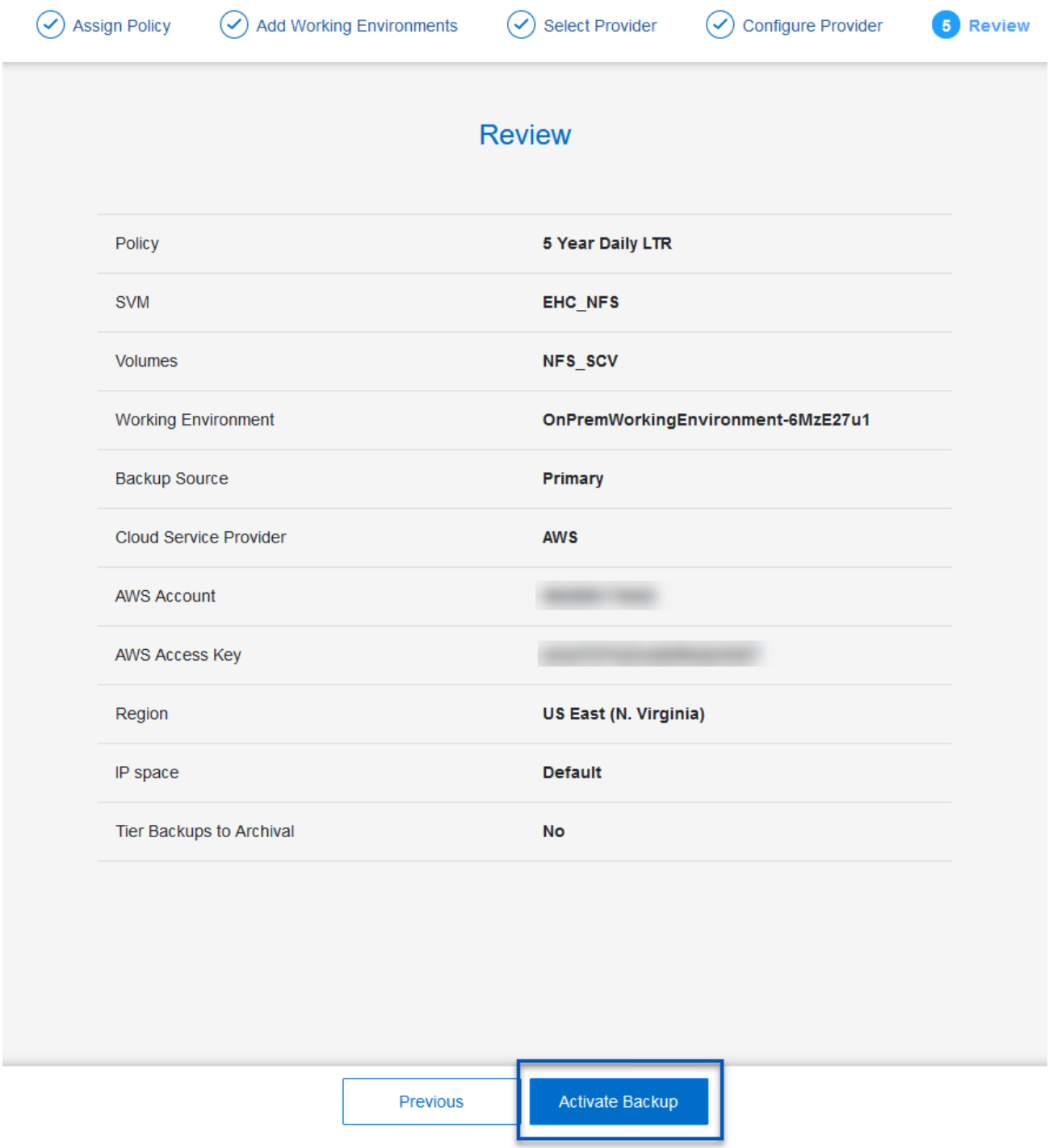
4. 在*选择提供商*页面上单击 AWS，然后单击*下一步*按钮继续。



5. 填写 AWS 提供商特定的凭证信息，包括要使用的 AWS 访问密钥和密钥、区域和存档层。此外，还要为本地ONTAP存储系统选择ONTAP IP 空间。单击“下一步”。



6. 最后，查看备份作业详细信息，然后单击“激活备份”按钮以启动数据存储的数据保护。



此时，数据传输可能不会立即开始。NetApp Backup and Recovery 每小时扫描一次任何未完成的快照，然后将其传输到对象存储。

数据丢失时恢复虚拟机

确保数据的安全只是全面数据保护的一个方面。同样重要的是，在发生数据丢失或勒索软件攻击时能够从任何位置迅速恢复数据。此功能对于维持无缝业务运营和满足恢复点目标至关重要。

NetApp提供高度适应性的 3-2-1 策略，可对主存储、辅助存储和对象存储位置的保留计划进行定制控制。该策略提供了灵活性，可以根据特定需求定制数据保护方法。

本节概述了从 SnapCenter Plug-in for VMware vSphere 和针对虚拟机的 NetApp Backup and Recovery 恢复数据的过程。

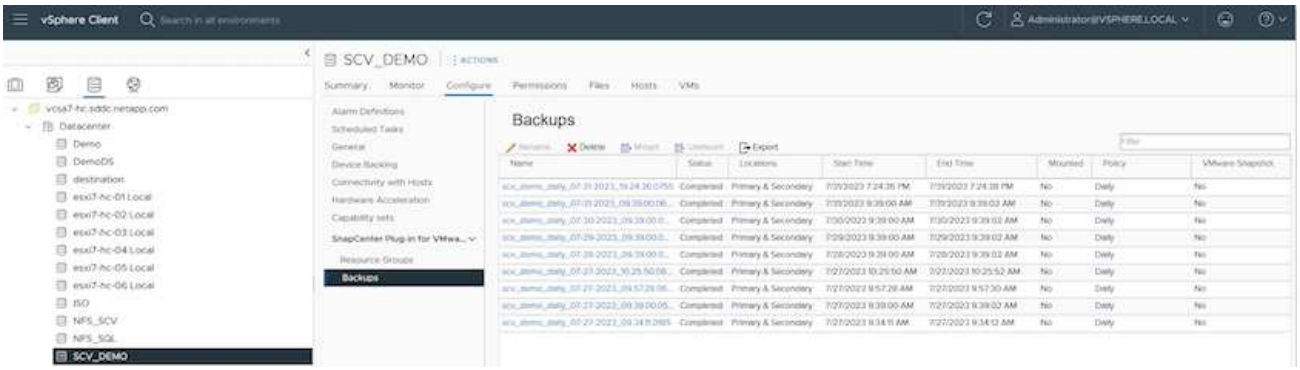
从**SnapCenter Plug-in for VMware vSphere**还原虚拟机

对于此解决方案，虚拟机被恢复到原始位置和备用位置。该解决方案并未涵盖 SCV 数据恢复功能的所有方面。有关 SCV 提供的所有服务的详细信息，请参阅 "从备份还原虚拟机"在产品文档中。

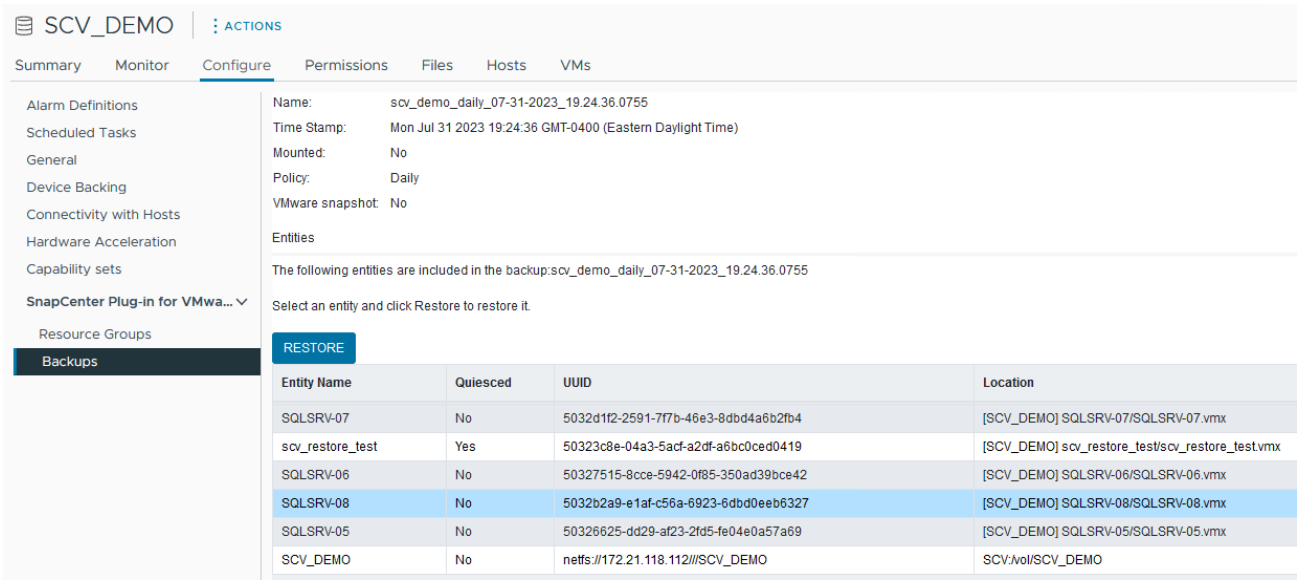
▼ 从 **SCV** 还原虚拟机

完成以下步骤以从主存储或辅助存储恢复虚拟机。

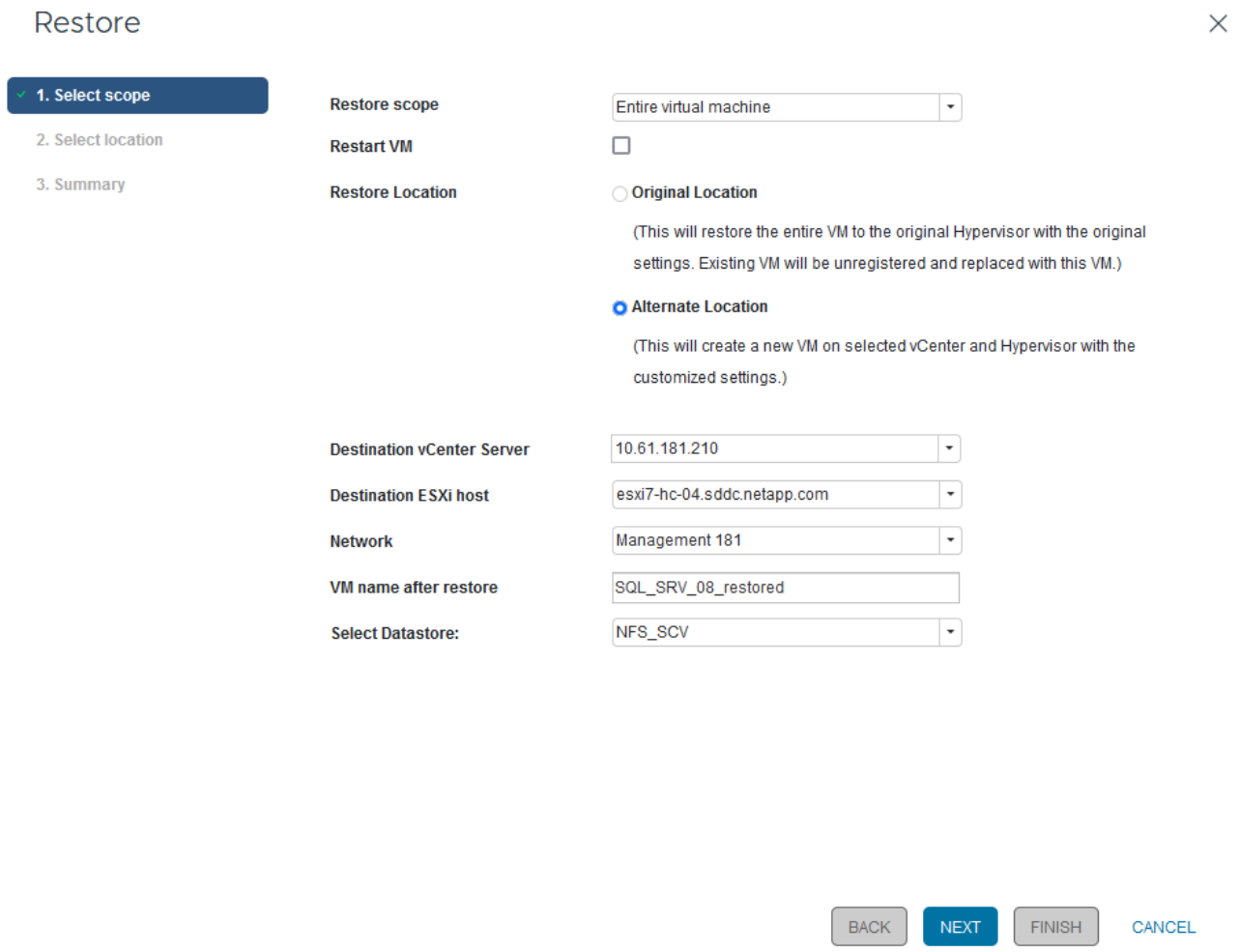
1. 从 vCenter 客户端导航到 **Inventory > Storage**，然后单击包含要还原的虚拟机的数据存储。
2. 从“配置”选项卡单击“备份”以访问可用备份列表。



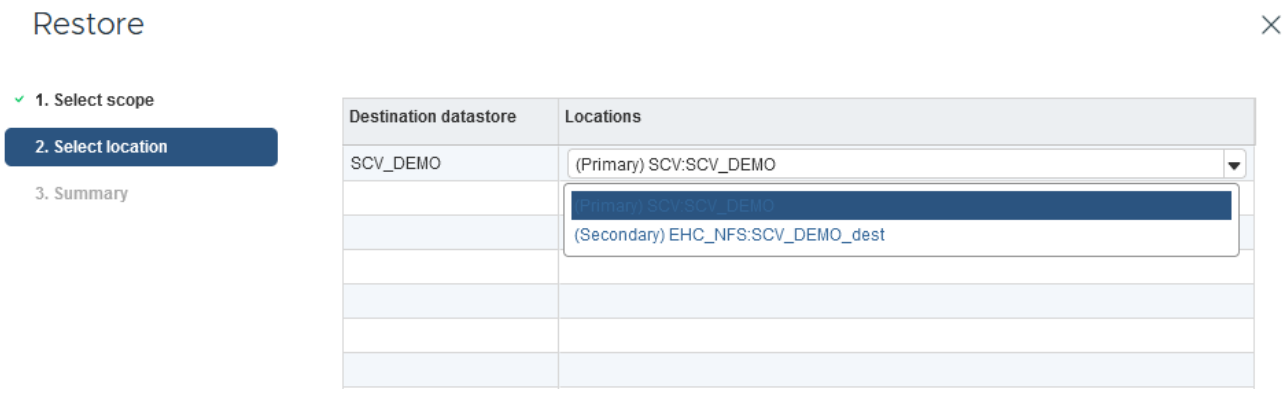
3. 单击备份以访问虚拟机列表，然后选择要恢复的虚拟机。点击*恢复*。



4. 从还原向导中选择还原整个虚拟机或特定的 VMDK。选择安装到原始位置或备用位置，提供恢复后的虚拟机名称和目标数据存储。单击“下一步”。



5. 选择从主存储位置或辅助存储位置备份。



6. 最后，查看备份作业的摘要并单击“完成”以开始恢复过程。

从 **NetApp Backup and Recovery for Virtual Machines** 还原虚拟机

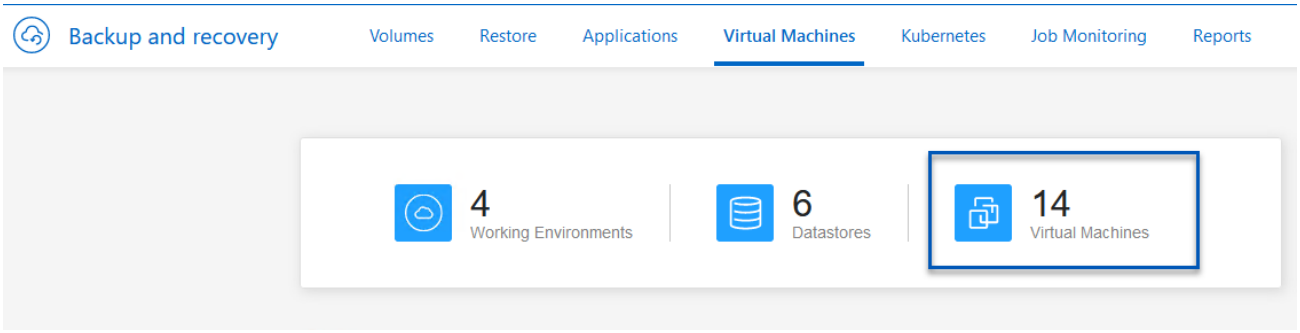
适用于虚拟机的 NetApp Backup and Recovery 允许将虚拟机还原到其原始位置。可以通过 NetApp Backup and Recovery Web 控制台访问还原功能。

有关详细信息，请参阅 "从云端恢复虚拟机数据"。

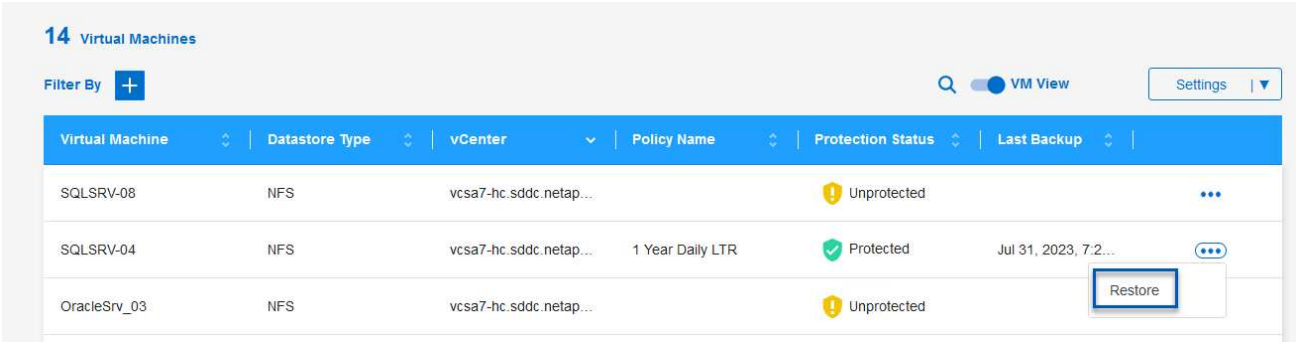
▼ 从 **NetApp Backup and Recovery** 还原虚拟机

要从 NetApp Backup and Recovery 还原虚拟机，请完成以下步骤。

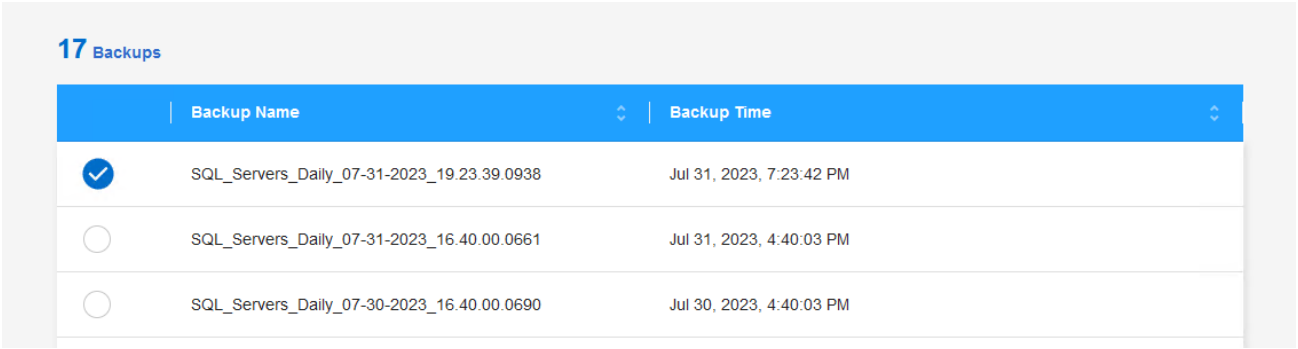
1. 导航到*保护>备份和恢复>虚拟机*，然后单击虚拟机以查看可恢复的虚拟机列表。



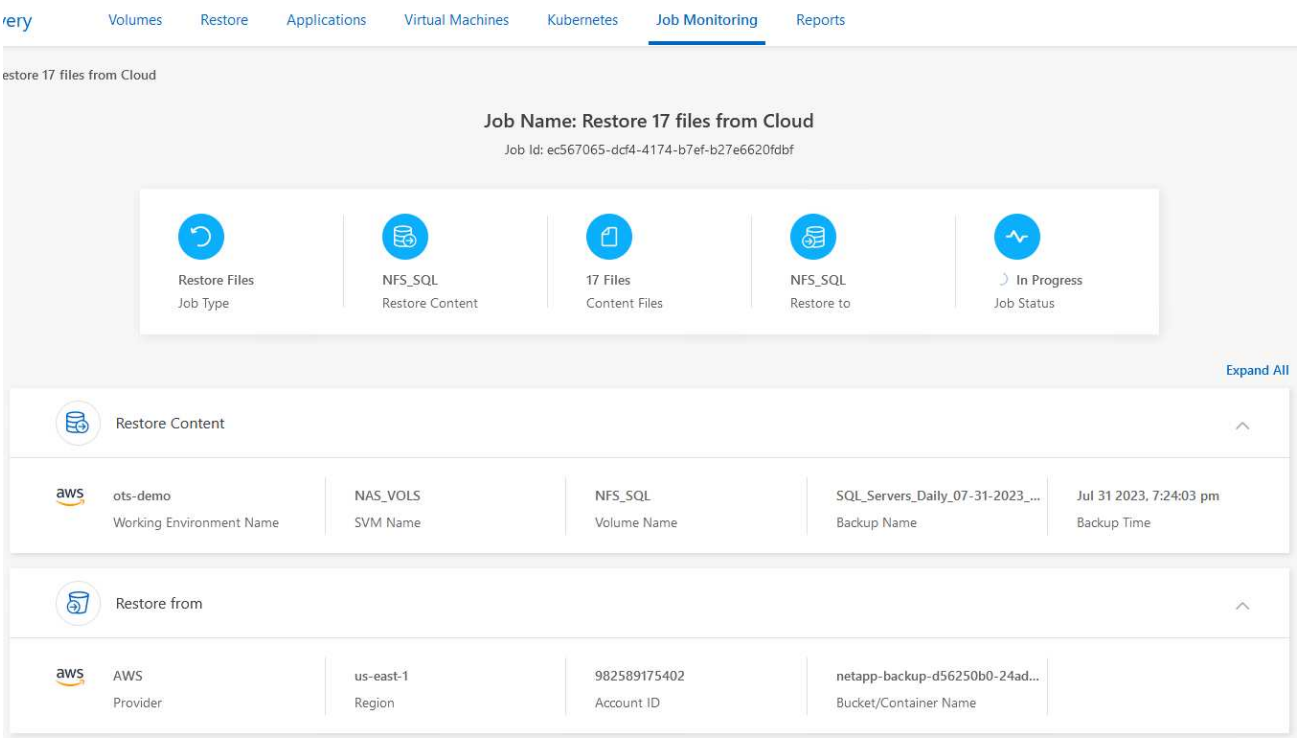
2. 访问要恢复的虚拟机的设置下拉菜单并选择



3. 选择要恢复的备份，然后单击“下一步”。



4. 查看备份作业的摘要，然后单击“恢复”开始恢复过程。
5. 从“作业监控”选项卡监控恢复作业的进度。



结束语

当与 SnapCenter Plug-in for VMware vSphere 和适用于虚拟机的 NetApp Backup and Recovery 一起实施时，3-2-1 备份策略可为数据保护提供强大、可靠且经济高效的解决方案。这种策略不仅确保了数据冗余和可访问性，而且还提供了从任何位置以及从本地 ONTAP 存储系统和基于云的对象存储恢复数据的灵活性。

本文档中介绍的使用案例侧重于经过验证的数据保护技术，这些技术突出了 NetApp、VMware 与领先的云提供商之间的集成。SnapCenter Plug-in for VMware vSphere 提供了与 VMware vSphere 的无缝集成，允许对数据保护操作进行高效的集中管理。这种集成简化了虚拟机的备份和恢复流程，在 VMware 生态系统中实现了轻松的计划、监控和灵活的恢复操作。适用于虚拟机的 NetApp Backup and Recovery 通过将虚拟机数据安全、气隙隔离地备份到基于云的对象存储，提供了 3-2-1 策略中的“1”。直观的界面和逻辑工作流程为关键数据的长期归档提供了一个安全的平台。

追加信息

要了解有关此解决方案中提出的技术的更多信息，请参阅以下附加信息。

- "SnapCenter Plug-in for VMware vSphere文档"
- "NetApp Console 文档"

NetApp Disaster Recovery

概述

灾难恢复是每个 VMware 管理员最关心的问题。因为 VMware 将整个服务器封装到一系列组成虚拟机的文件中；管理员利用基于块存储的技术（如克隆、快照和副本）来保护这些虚拟机。ONTAP 阵列提供内置复制以将卷数据从一个站点传输到另一个站点，从而将驻留在指定数据存储 LUN 上的虚拟机传输到另一个站点。NetApp Disaster Recovery 与 vSphere 集成并自动化整个工作流程，以便在发生灾难时实现无缝故障转移和故障回复。

通过将存储复制与智能自动化相结合，管理员现在不仅可以配置、自动化和测试灾难恢复计划，还可以在发生灾难时轻松运行这些计划。

VMware vSphere 环境中 DR 故障转移最耗时的部分是在 DR 站点执行清点、注册、重新配置和启动虚拟机所需的步骤。理想的解决方案既具有低 RPO（以分钟为单位），又具有低 RTO（以分钟到小时为单位）。 DR 解决方案中经常被忽视的一个因素是定期有效地测试 DR 解决方案的能力。

要构建 DR 解决方案，请牢记以下因素：

- 恢复时间目标 (RTO)。 RTO 是指企业从灾难中恢复的速度，或者更具体地说，是执行恢复过程以使业务服务再次可用所需的时间。
- 恢复点目标 (RPO)。 RPO 是指恢复的数据相对于灾难发生的时间而言，可供使用的时间。
- 可扩展性和适应性。该因素包括随着需求的增加而逐步增加存储资源的能力。

有关可用解决方案的更多技术信息，请参阅：

- "NFS 数据存储的 NetApp Disaster Recovery"
- "VMFS 数据存储的 NetApp Disaster Recovery"

NFS 数据存储的 NetApp Disaster Recovery

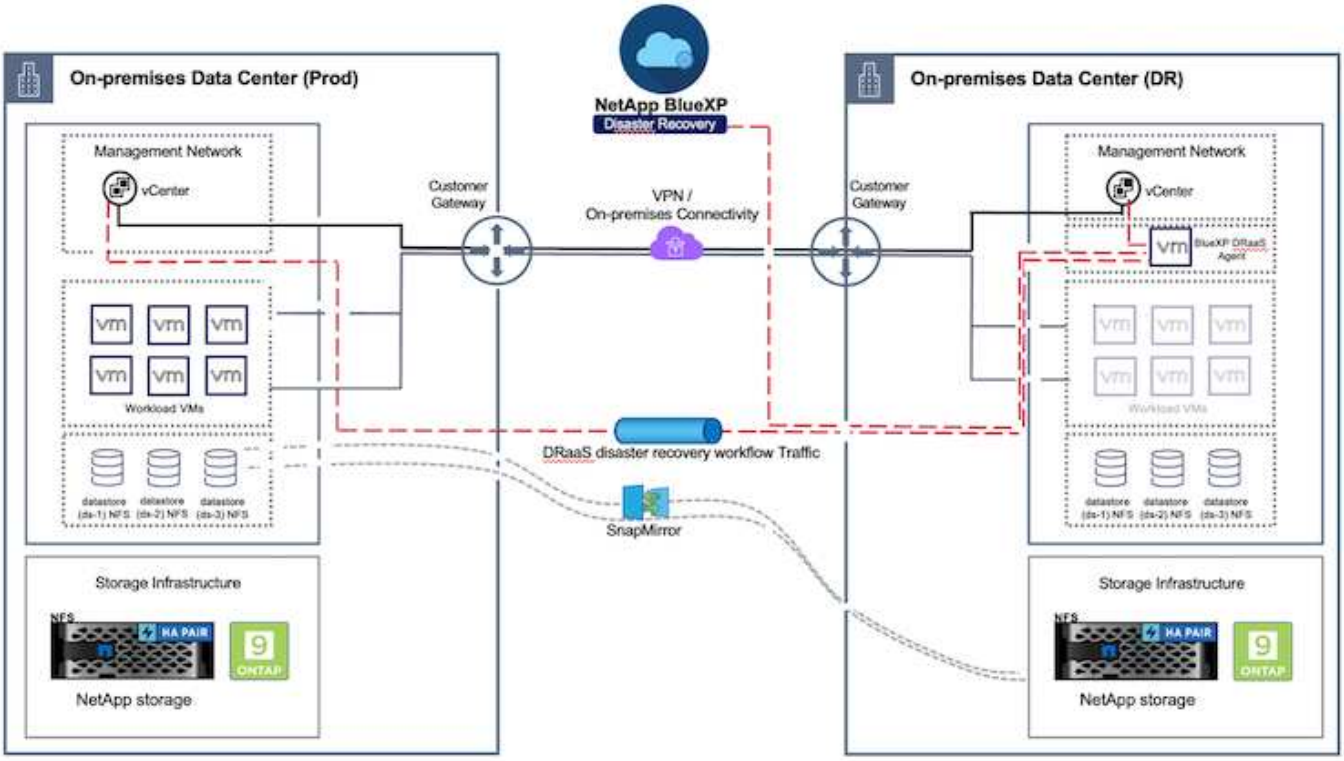
NFS 数据存储的 NetApp Disaster Recovery

通过从生产站点到灾难恢复站点的块级复制来实现灾难恢复是一种有弹性且经济高效的方法，可以保护工作负载免受站点中断和数据损坏事件（例如勒索软件攻击）的影响。使用NetApp SnapMirror复制，在具有 NFS 数据存储的本地ONTAP系统上运行的 VMware 工作负载可以复制到位于指定恢复数据中心的另一个ONTAP存储系统，该数据中心也部署了 VMware。

本文档的这一部分描述了 NetApp Disaster Recovery 的配置，以便为本地 VMware 虚拟机设置到另一个指定站点的灾难恢复。作为此设置的一部分，控制台代理将载入 ONTAP 阵列、定义站点并关联 VMware vCenter。此外，本文档详细介绍了如何配置站点之间的复制以及如何设置和测试恢复计划。最后一部分包含有关执行完整站点故障转移的说明，以及如何在主站点恢复并重新上线时进行故障恢复。

利用灾难恢复（NetApp Data Services 的一部分），公司可以轻松发现其本地 VMware vCenters 和 ONTAP 存储。然后，组织可以创建资源组、创建灾难恢复计划、将其与资源组关联，以及测试或执行故障转移和故障回复。SnapMirror 提供存储级块复制，以使两个站点通过增量更改保持最新，从而实现最多 5 分钟的恢复点目标（RPO）。此外，还可以模拟灾难恢复过程，而不会影响生产或产生额外的存储成本。

灾难恢复利用 ONTAP 的 FlexClone 技术从灾难恢复站点上的上次复制快照创建 NFS 数据存储的节省空间的副本。完成灾难恢复测试后，客户可以轻松删除测试环境，而不会影响实际复制的生产资源。在实际故障转移的情况下，灾难恢复会协调所有必要的步骤，只需单击几下即可在指定的灾难恢复站点上自动启动受保护的虚拟机。该服务还将反转与主站点的 SnapMirror 关系，并在需要时将任何更改从辅助站点复制到主站点，以进行故障回复操作。与其他众所周知的替代方案相比，所有这些功能的成本仅为一小部分。

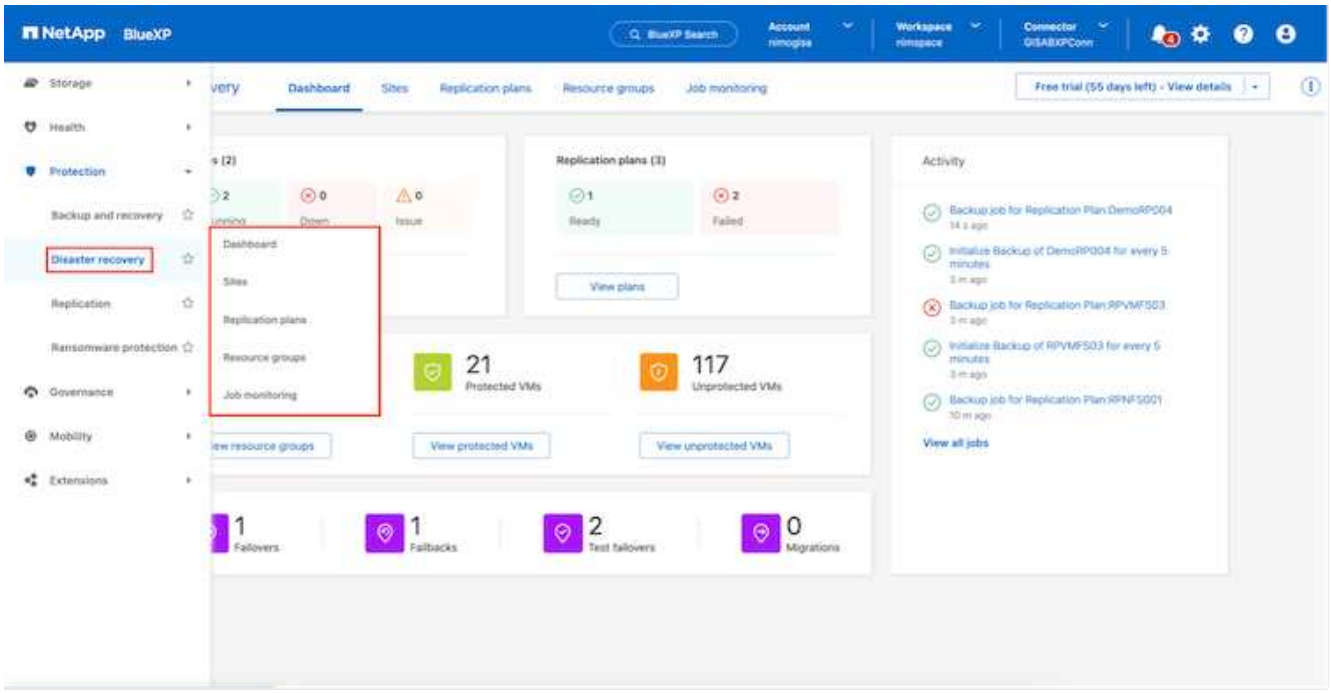


有关用于灾难恢复的 vCenter Server、ESXi 和 ONTAP 的最新信息和支持版本，请参见 "灾难恢复支持的配置"。

入门

要开始使用 NetApp Disaster Recovery，请使用 NetApp Console，然后访问该服务。

1. 登录到 Console。
2. 从控制台左侧导航栏中，选择保护 > 灾难恢复。
3. 此时将显示灾难恢复仪表板。

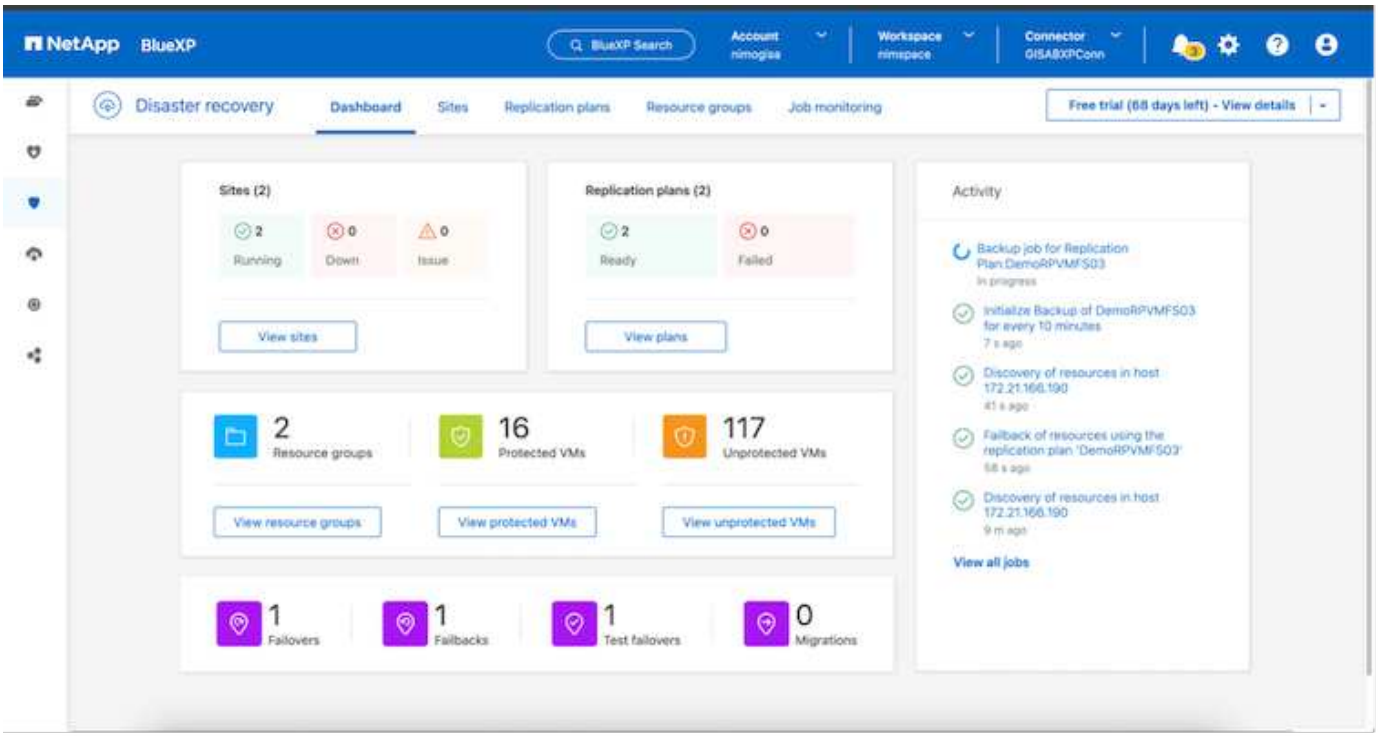


在配置灾难恢复计划之前，请确保满足以下先决条件：

- 已部署控制台代理。
- 代理具有到源和目标 vCenter 以及存储系统的连接。
- 具有启用 NFS 服务的 SVM 的 ONTAP 集群可用。
- 在控制台中添加了托管适用于 VMware 的 NFS 数据存储的本地 NetApp 存储系统。
- 使用 DNS 名称时应该进行 DNS 解析。否则，请使用 vCenter 的 IP 地址。
- SnapMirror复制是为指定的基于 NFS 的数据存储库卷配置的。
- 确保环境具有受支持的 vCenter Server 和 ESXi 服务器版本。

一旦源站点和目标站点之间建立了连接，请继续执行配置步骤，这需要几次点击和大约 3 到 5 分钟的时间。

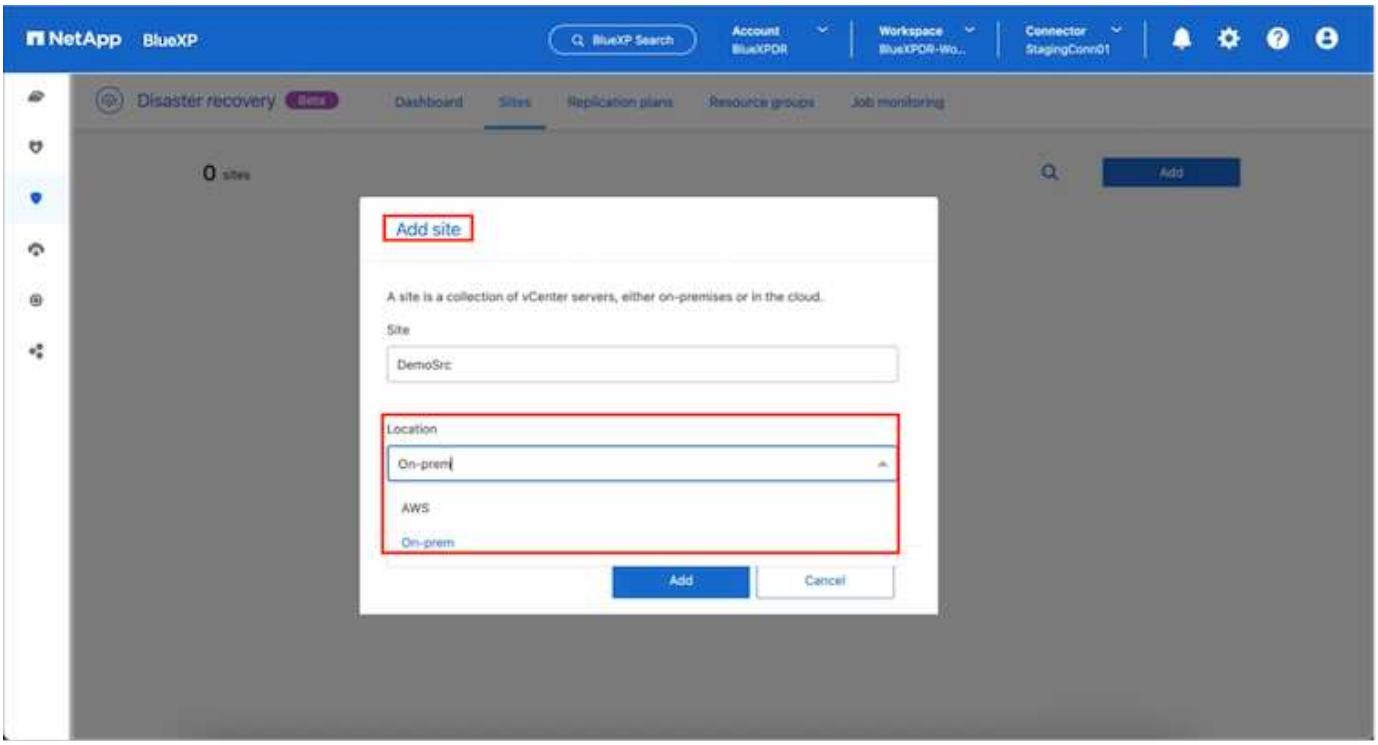
NetApp 建议在目标站点或第三个站点中部署控制台代理，以便控制台代理可以通过网络与源和目标资源进行通信。



NetApp Disaster Recovery 配置

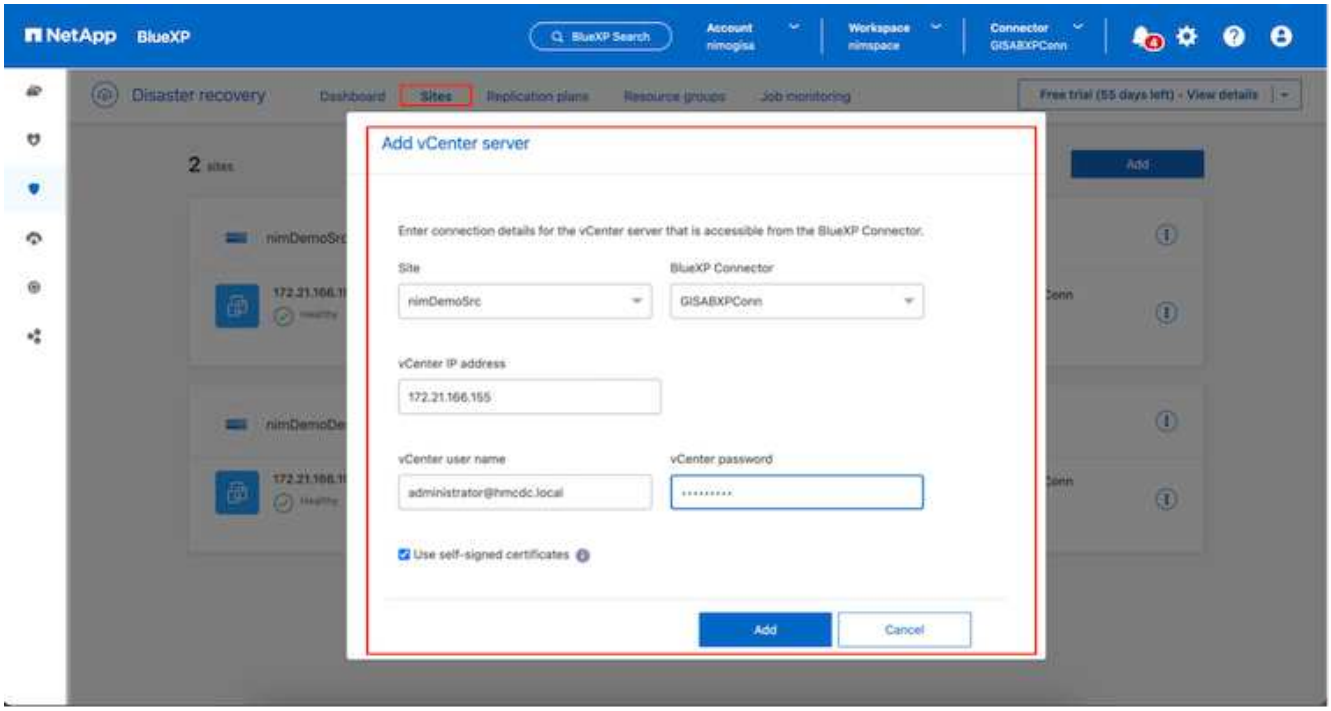
准备灾难恢复的第一步是发现本地 vCenter 和存储资源并将其添加到 NetApp Disaster Recovery。

打开控制台，然后从左侧导航中选择 保护 **>** 灾难恢复。单击 站点，提供名称并选择位置类型。然后，单击 添加 **vCenter** 按钮。

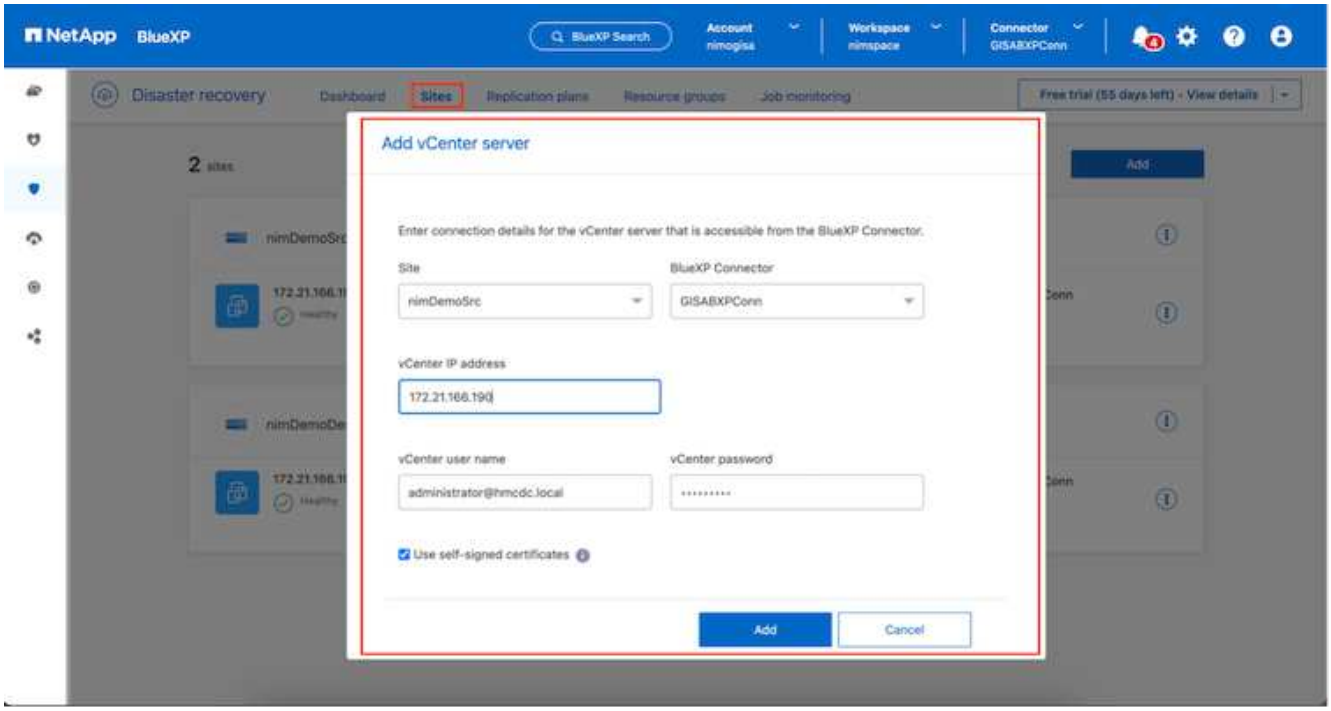


添加以下平台：

- 来源。本地 vCenter。



- 目的地。 VMC SDDC vCenter。



一旦添加了 vCenter，就会触发自动发现。

配置源站点阵列和目标站点阵列之间的存储复制

SnapMirror 在 NetApp 环境中提供数据复制功能。SnapMirror 复制基于 NetApp Snapshot 技术构建，效率极高，因为它仅复制自上次更新以来已更改或新增的块。SnapMirror 可通过 NetApp OnCommand System Manager 或 ONTAP CLI 轻松配置。NetApp Data Services 还会创建 SnapMirror 关系，前提是事先配置了集群和 SVM 对

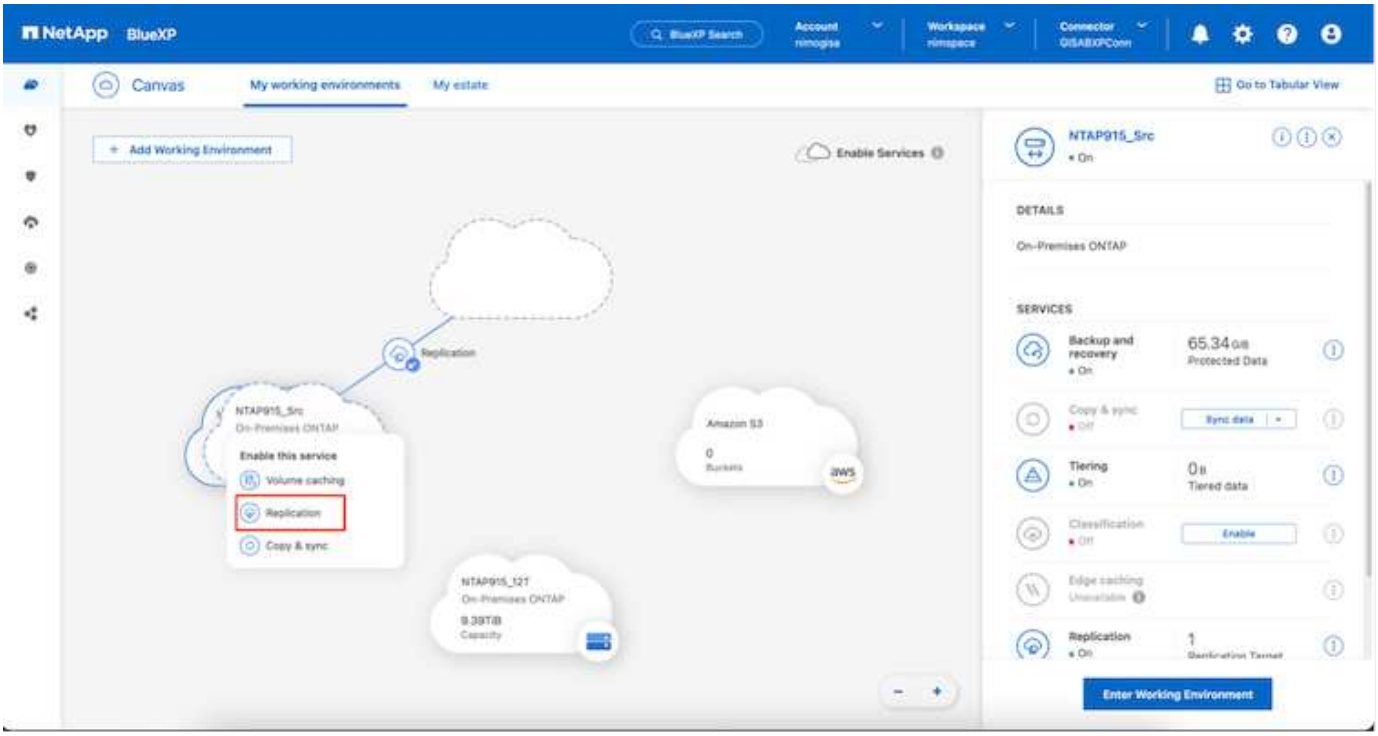
等关系。

对于主存储未完全丢失的情况，SnapMirror 提供了一种重新同步主站点和灾难恢复站点的有效方法。SnapMirror 可以重新同步两个站点，只需简单地反转 SnapMirror 关系，即可将更改或新数据从灾难恢复站点传回主站点。这意味着灾难恢复中的复制计划可以在故障切换后向任一方向重新同步，而无需重新复制整个卷。如果反向重新同步关系，则仅将自上次成功同步快照副本后写入的新数据发送回目标。

如果已通过 CLI 或 System Manager 为该卷配置 SnapMirror 关系，NetApp Data Services 将提取该关系并继续其余的工作流操作。

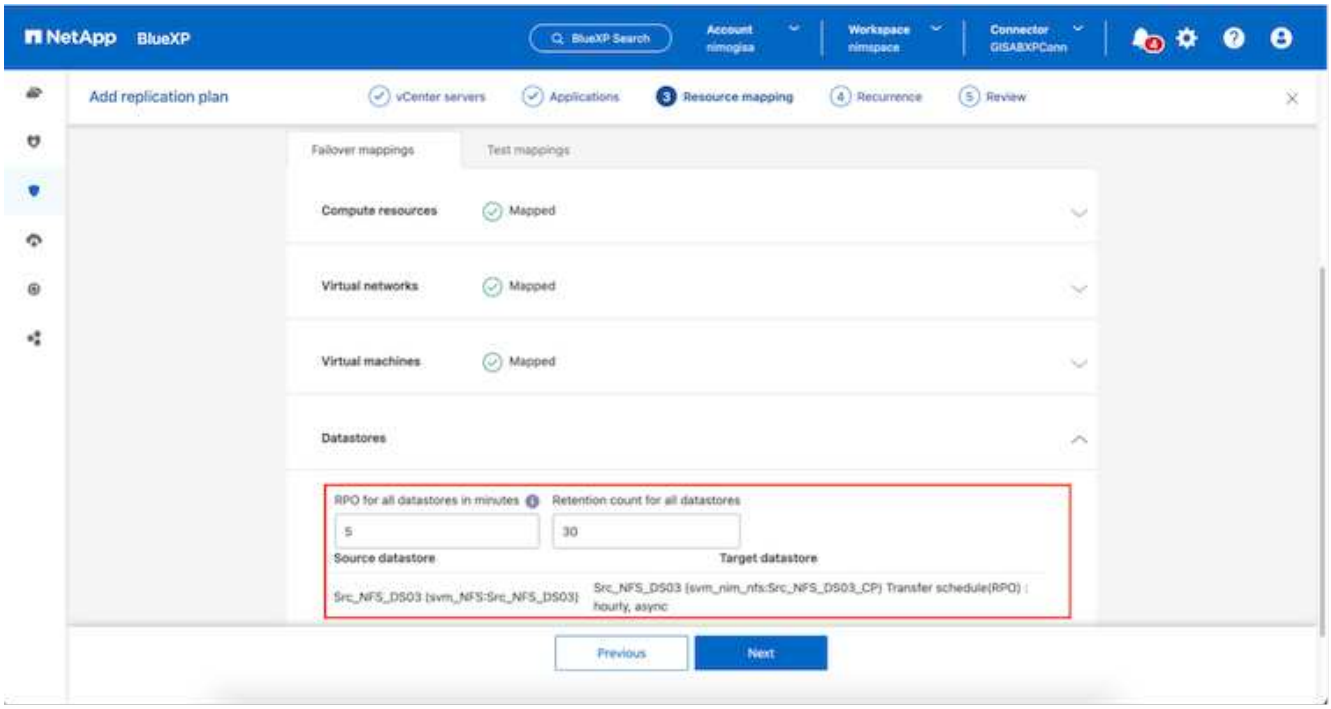
如何设置 **VMware** 灾难恢复

对于任何给定应用程序，创建 SnapMirror 复制的过程保持不变。该过程可以是手动或自动的。最简单的方法是利用 NetApp Console，通过将环境中的源 ONTAP 系统简单地拖放到目标上来配置 SnapMirror 复制，从而触发向导以指导完成其余过程。



如果满足以下两个条件，灾难恢复也可以自动执行相同的操作：

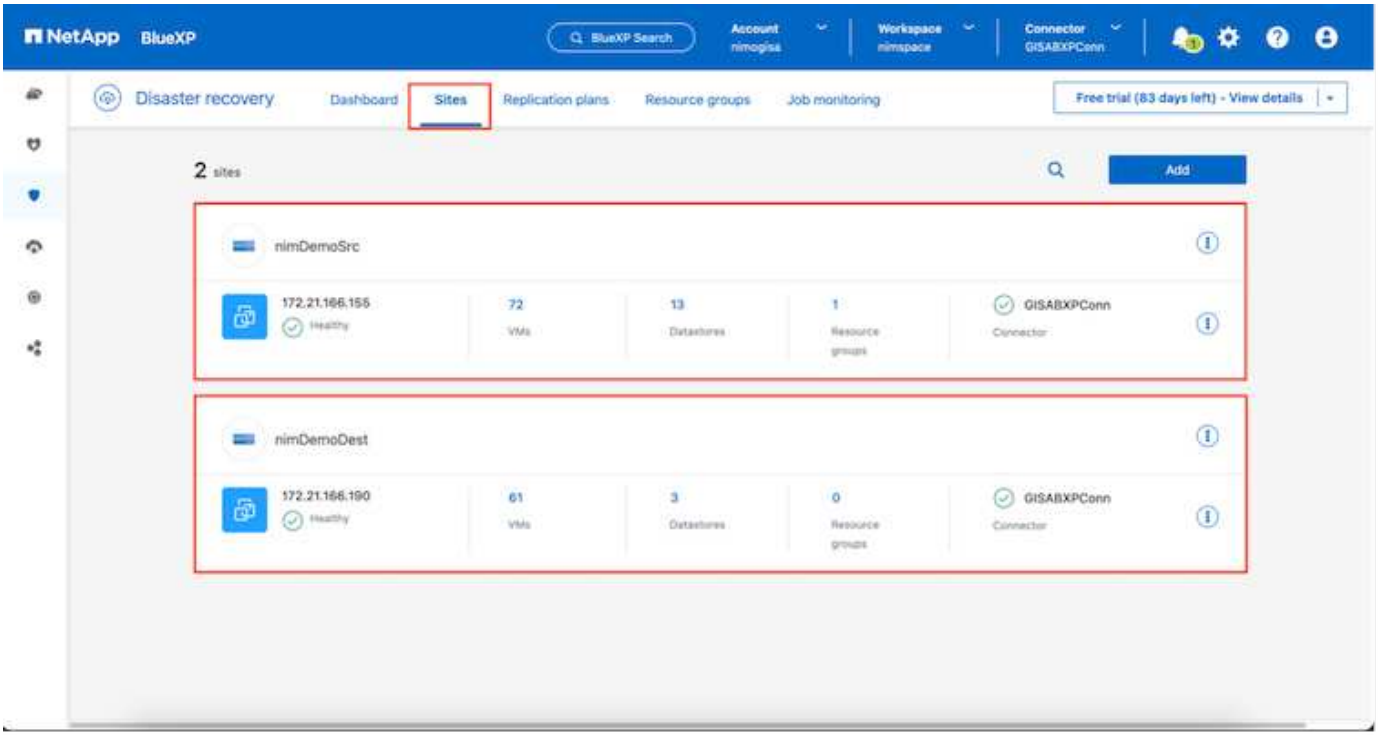
- 源集群和目标集群具有对等关系。
- 源 SVM 和目标 SVM 具有对等关系。



如果已通过 CLI 为该卷配置了 SnapMirror 关系，灾难恢复将提取该关系并继续其余的工作流操作。

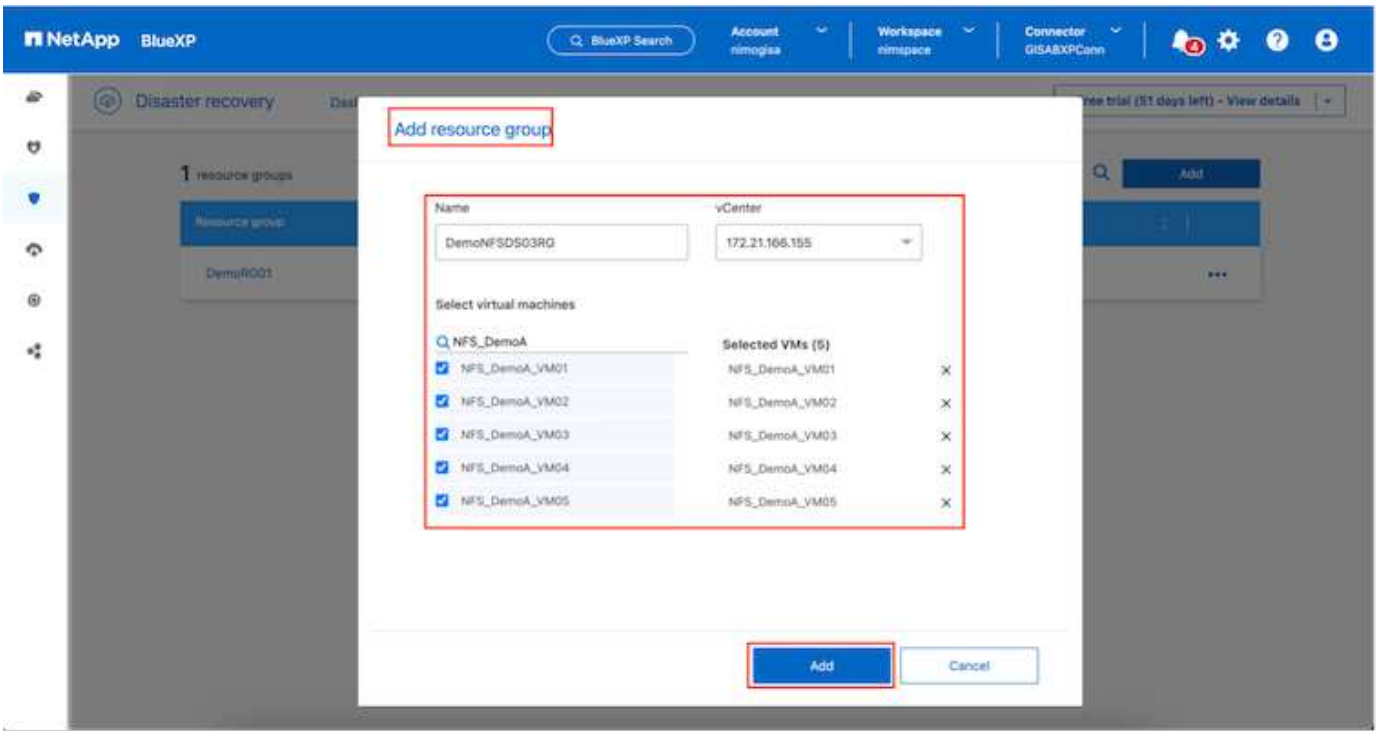
灾难恢复可以为您做些什么？

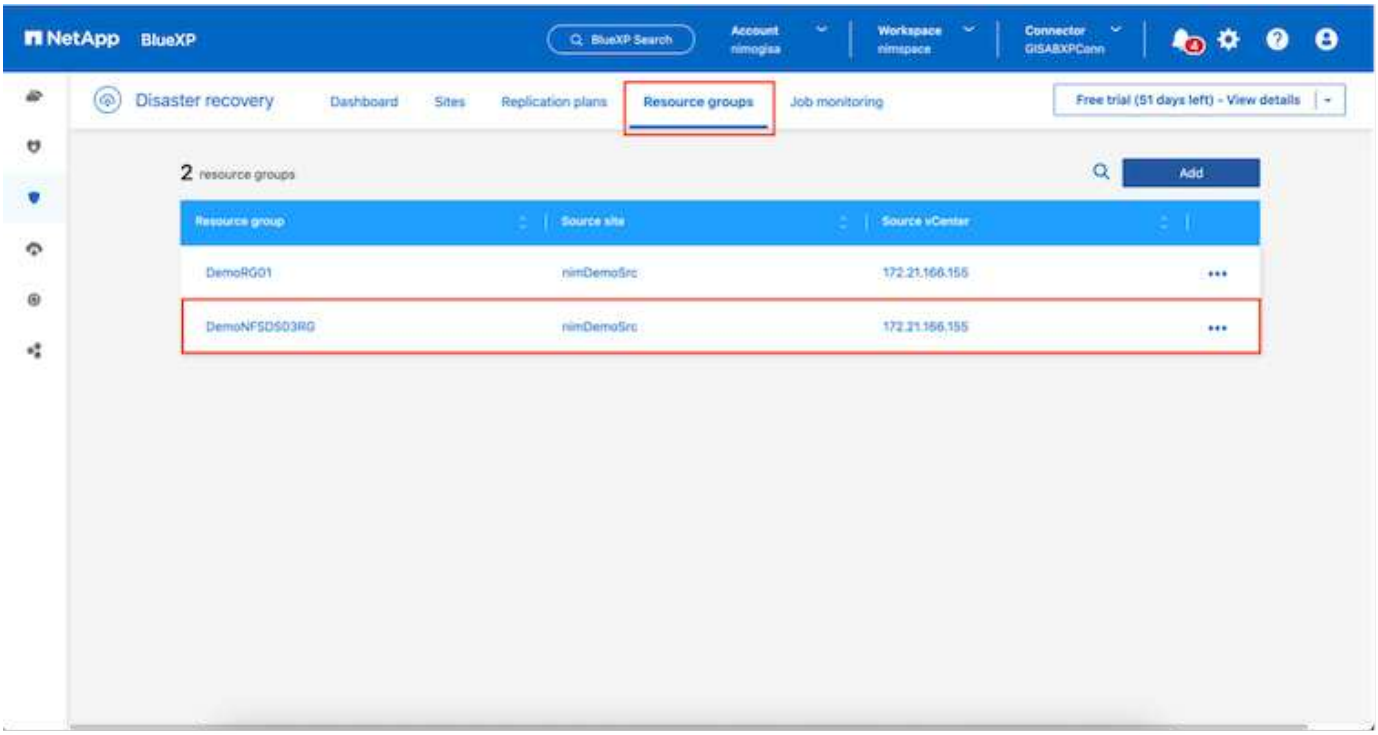
添加源站点和目标站点后，灾难恢复将执行自动深度发现并显示虚拟机以及关联的元数据。灾难恢复还会自动检测虚拟机使用的网络和端口组，并填充它们。



添加站点后，可以将 VM 分组到资源组中。灾难恢复资源组允许您将一组从属虚拟机分组到包含其启动顺序和启

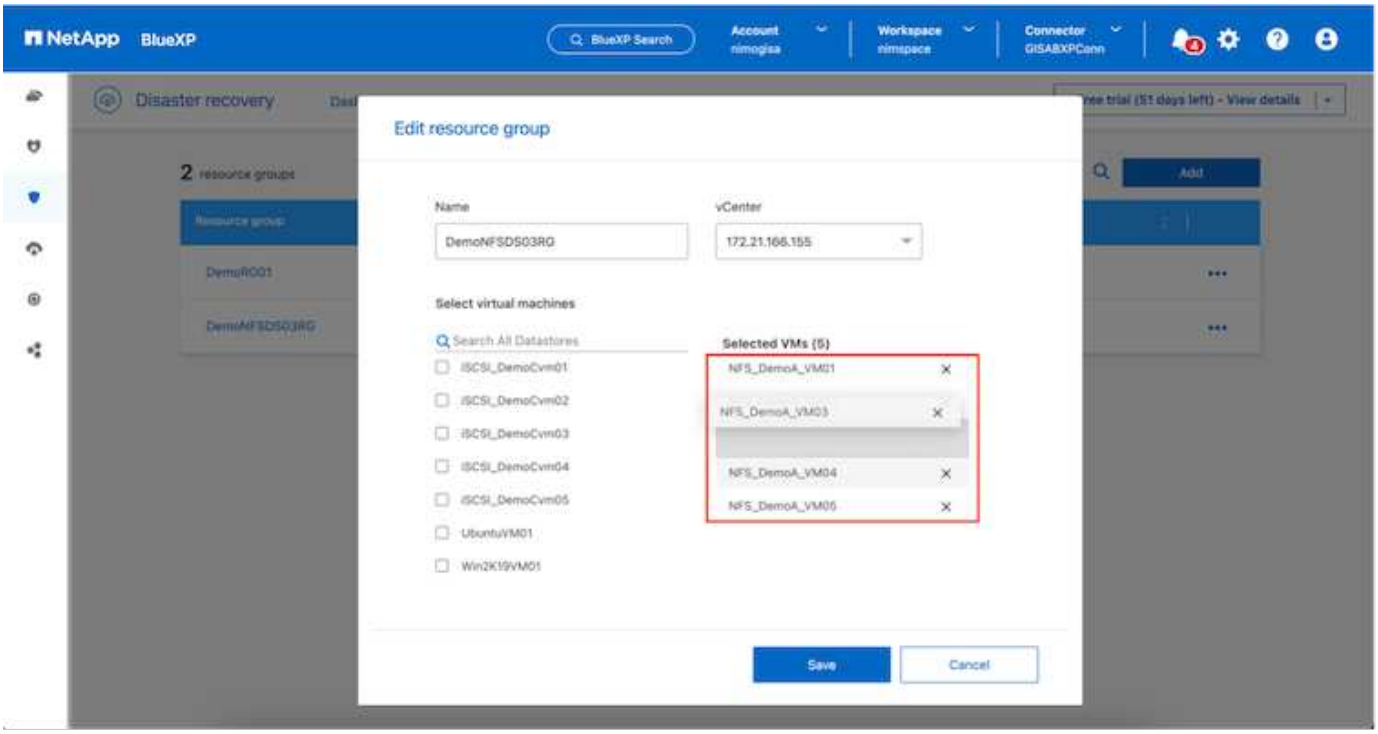
动延迟的逻辑组中，这些启动顺序和启动延迟可在恢复时执行。要开始创建资源组，请导航到*资源组*，然后单击*创建新资源组*。



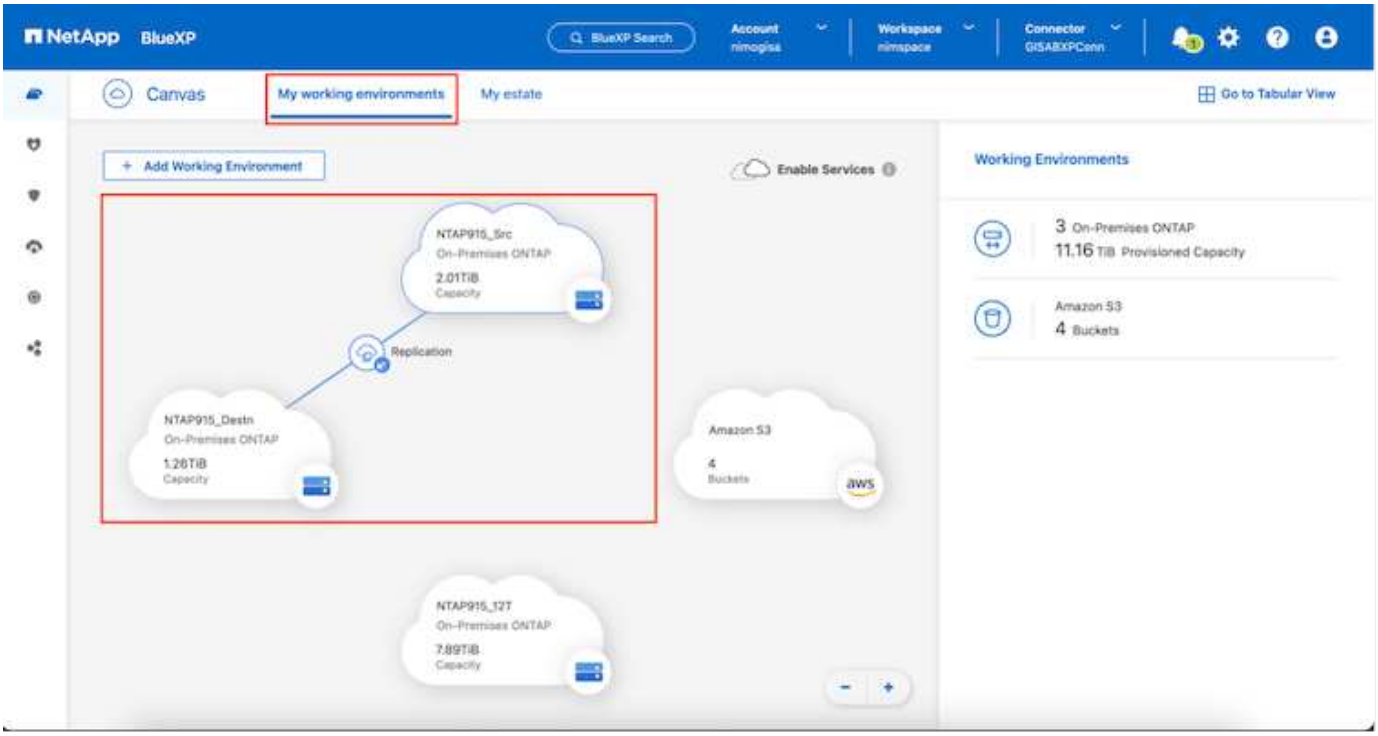


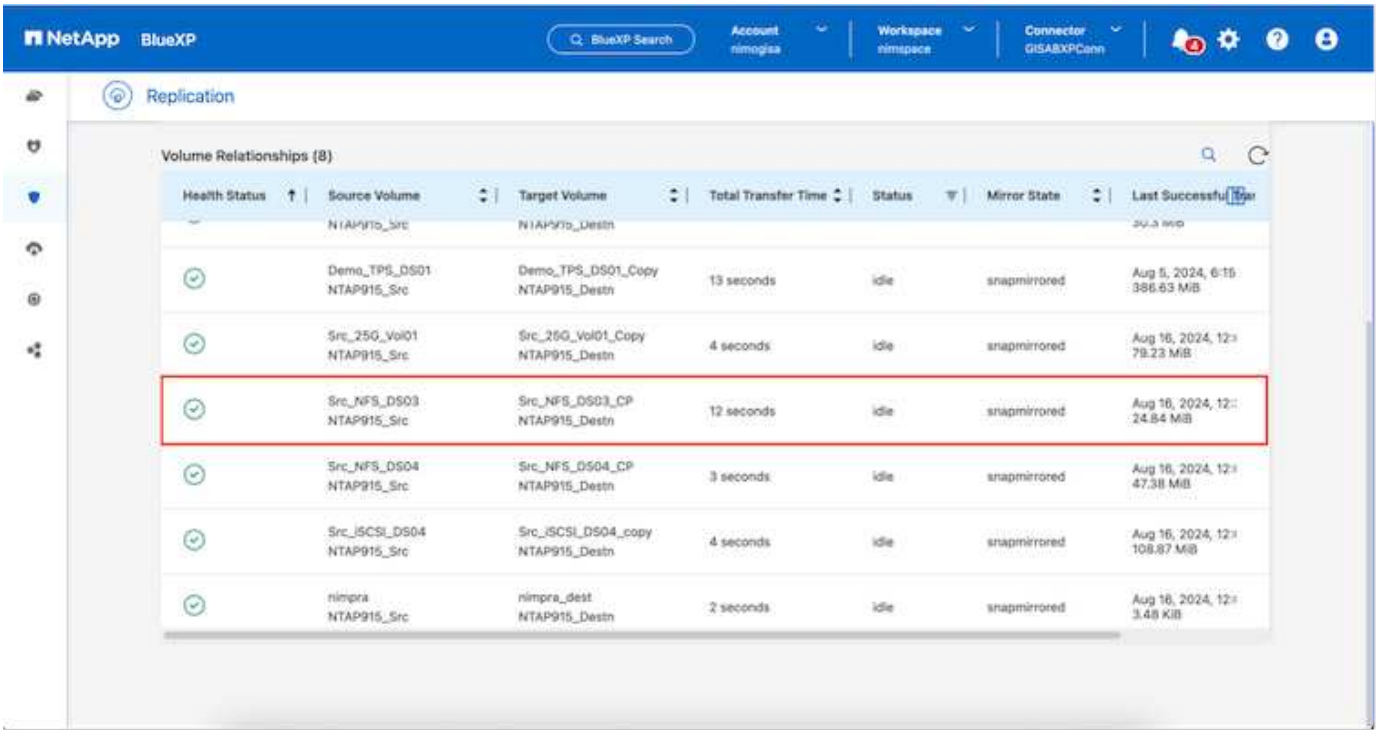
在创建复制计划时也可以创建资源组。

可以通过简单的拖放机制在创建资源组期间定义或修改虚拟机的启动顺序。



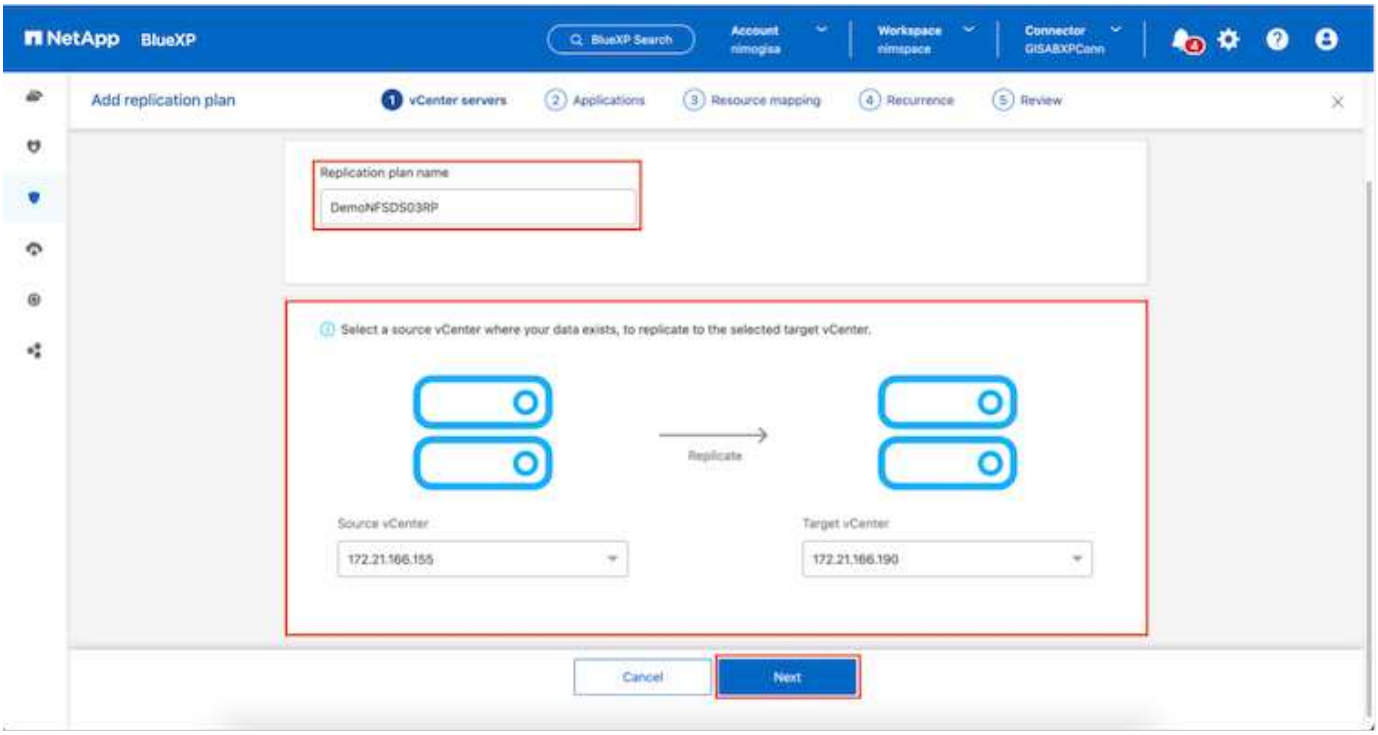
创建资源组后，下一步是创建执行蓝图或在发生灾难时恢复虚拟机和应用程序的计划。如先决条件中所述，可以预先配置SnapMirror复制，或者 DRaaS 可以使用在创建复制计划期间指定的 RPO 和保留计数来配置它。



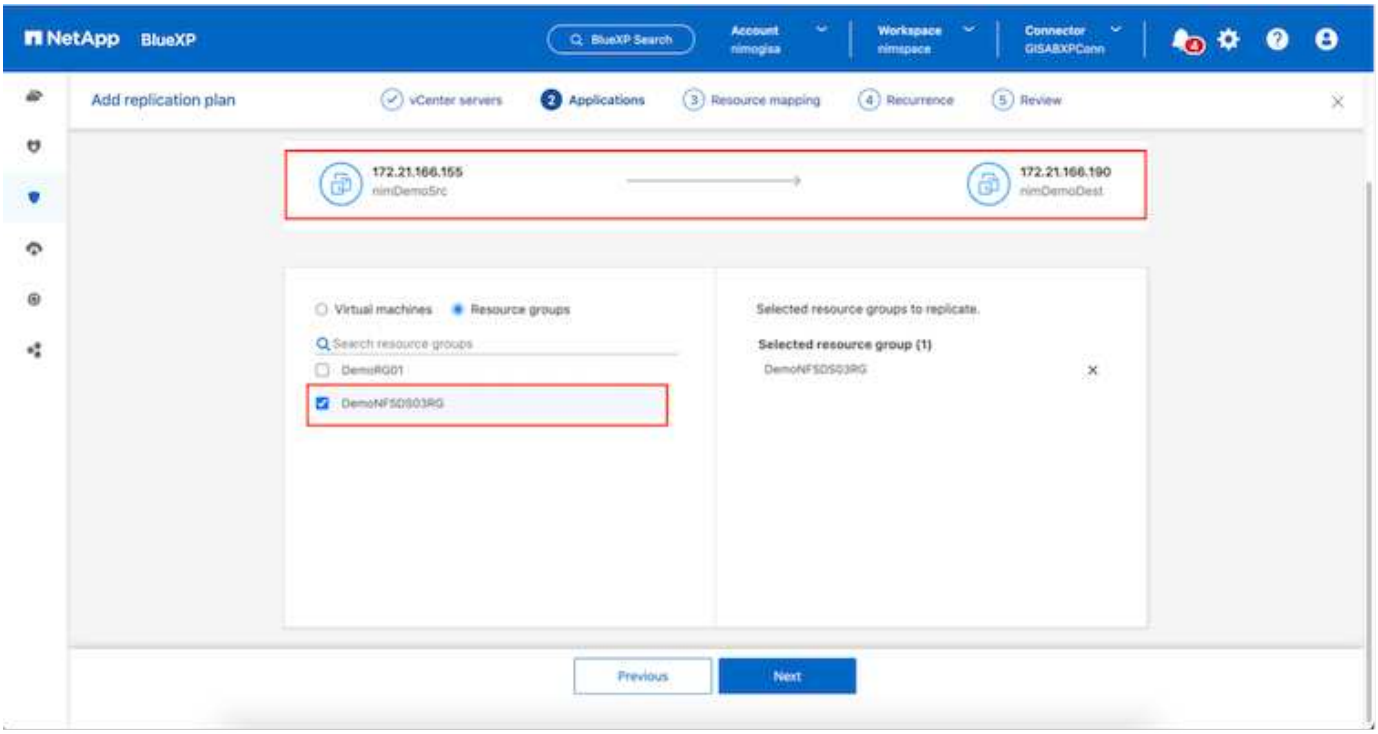


通过从下拉菜单中选择源和目标 vCenter 平台来配置复制计划，并选择要包含在计划中的资源组，以及如何恢复和启动应用程序的分组以及集群和网络的映射。要定义恢复计划，请导航到“复制计划”选项卡并单击“添加计划”。

首先，选择源 vCenter，然后选择目标 vCenter。



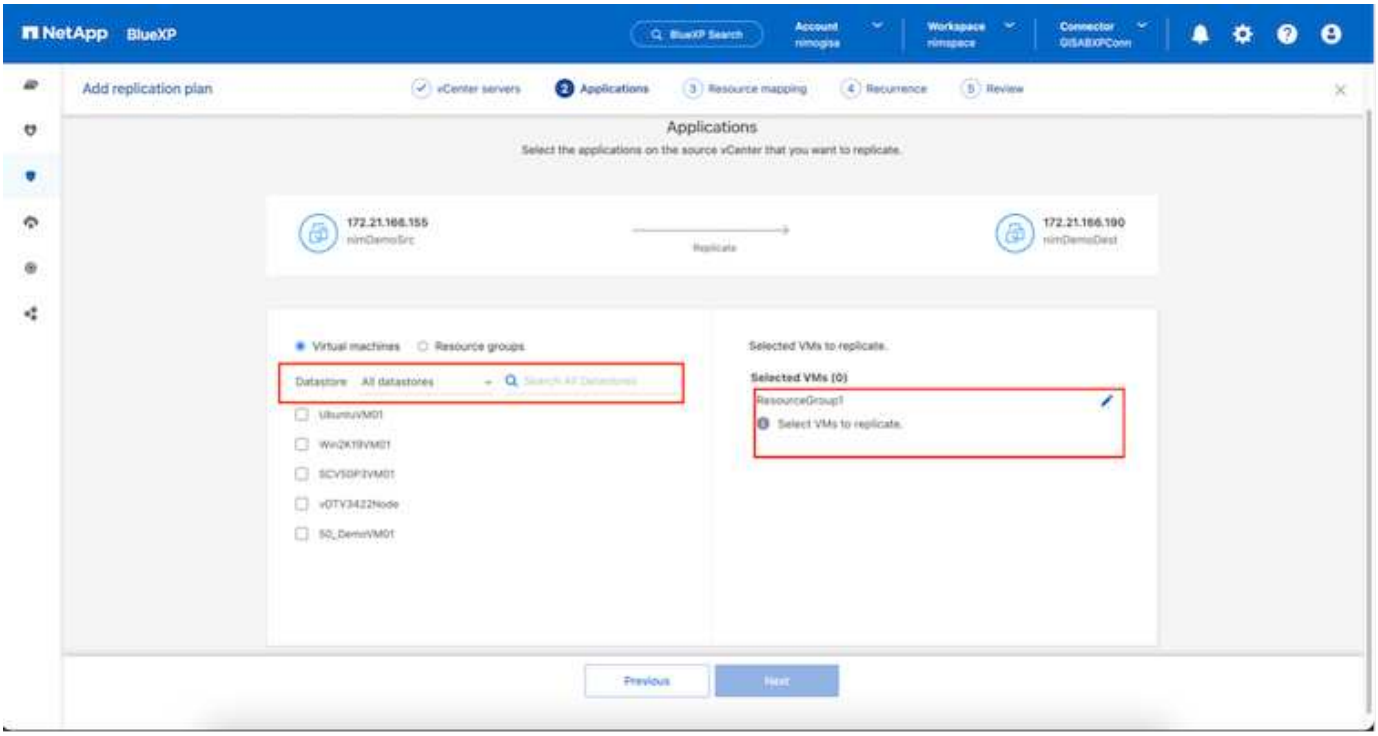
下一步是选择现有的资源组。如果没有创建资源组，则向导将帮助根据恢复目标对所需的虚拟机进行分组（基本上创建功能资源组）。这也有助于定义如何恢复应用程序虚拟机的操作顺序。



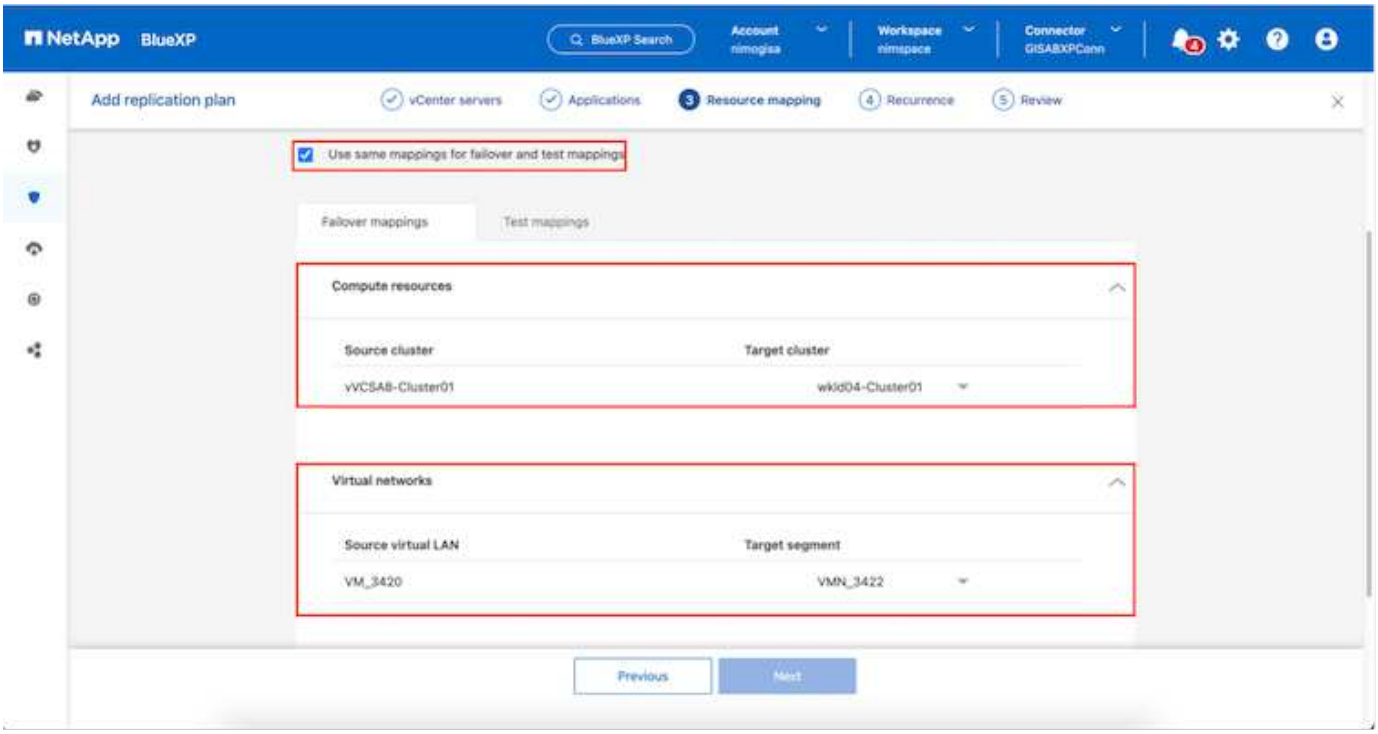
资源组允许使用拖放功能设置启动顺序。它可用于轻松修改恢复过程中虚拟机的启动顺序。

资源组内的各个虚拟机按照顺序依次启动。两个资源组并行启动。

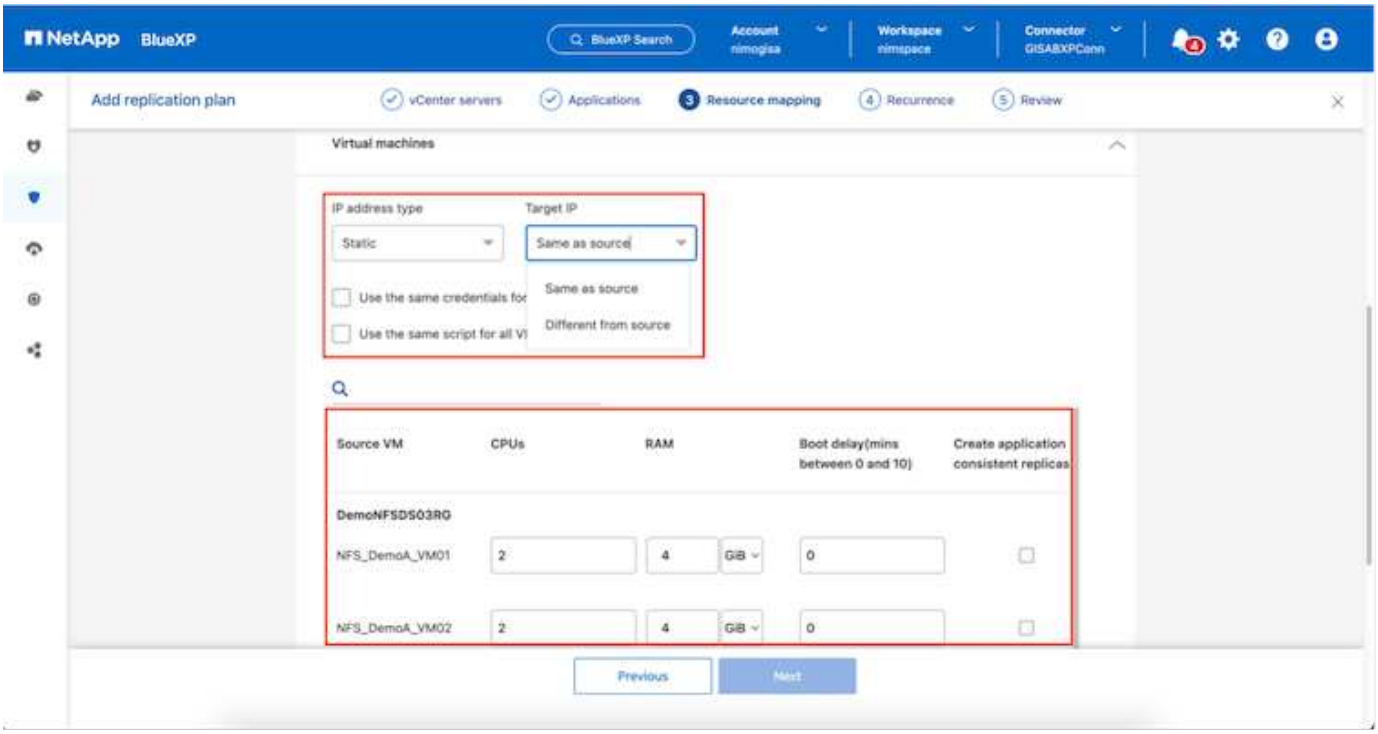
如果未事先创建资源组，则以下屏幕截图显示了根据组织要求过滤虚拟机或特定数据存储的选项。



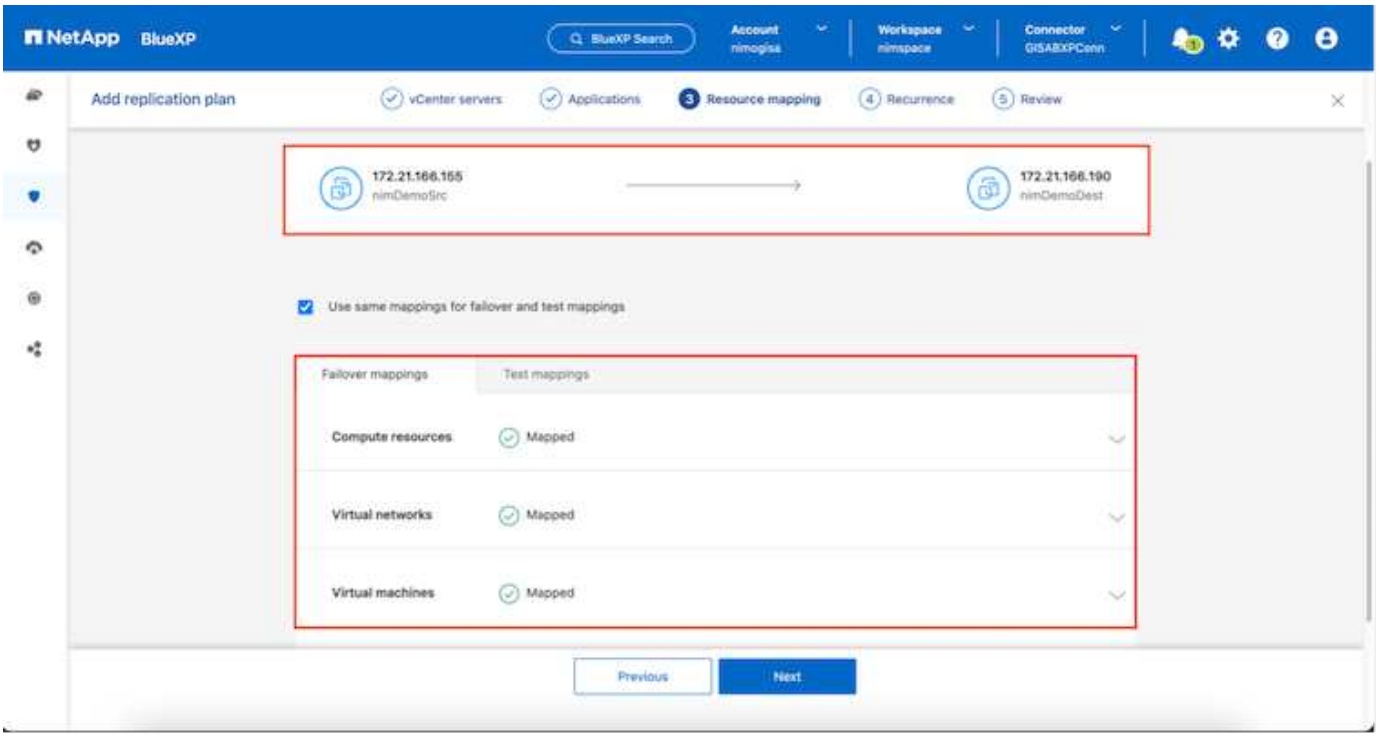
选择资源组后，创建故障转移映射。在此步骤中，指定源环境中的资源如何映射到目标。这包括计算资源、虚拟网络。IP 定制、前置和后置脚本、引导延迟、应用程序一致性等。有关详细信息，请参阅 "创建复制计划"。



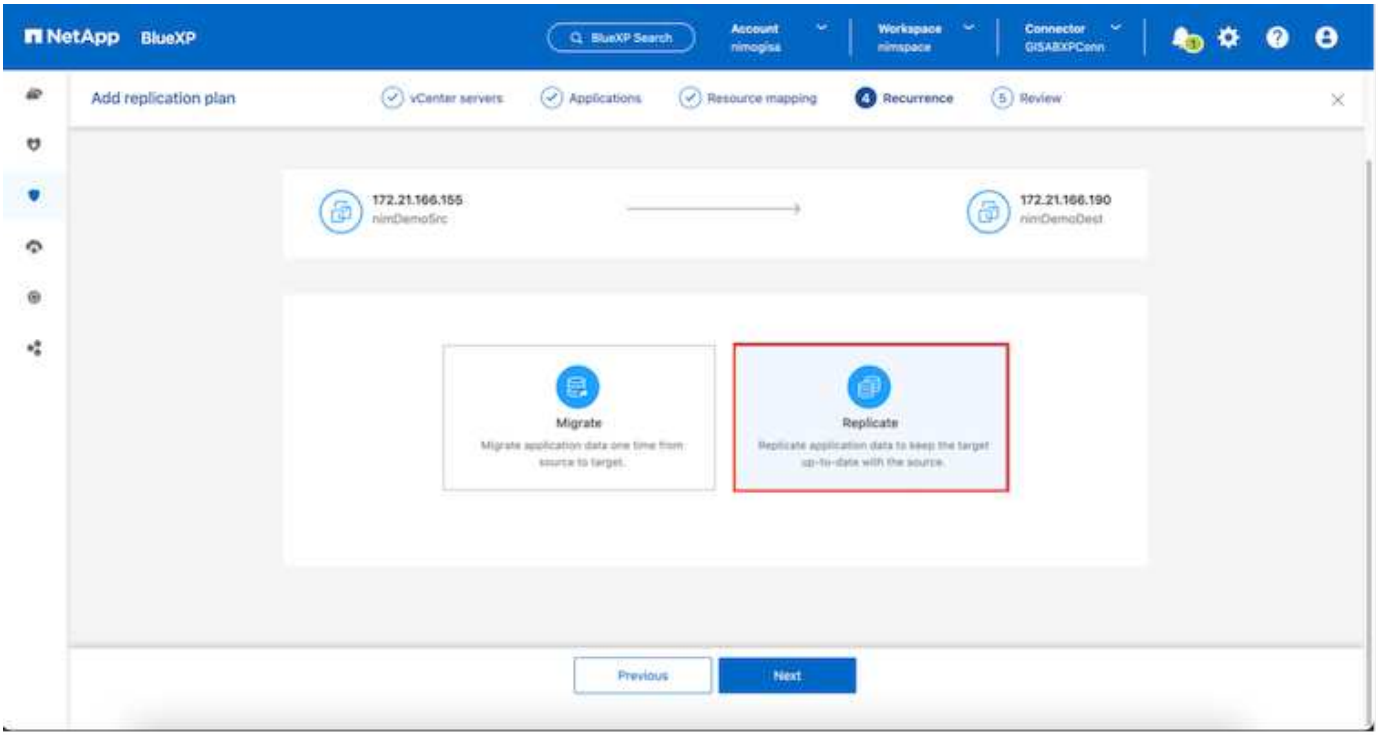
默认情况下，测试和故障转移操作使用相同的映射参数。要为测试环境设置不同的映射，请取消选中复选框后选择测试映射选项，如下所示：



资源映射完成后，单击下一步。

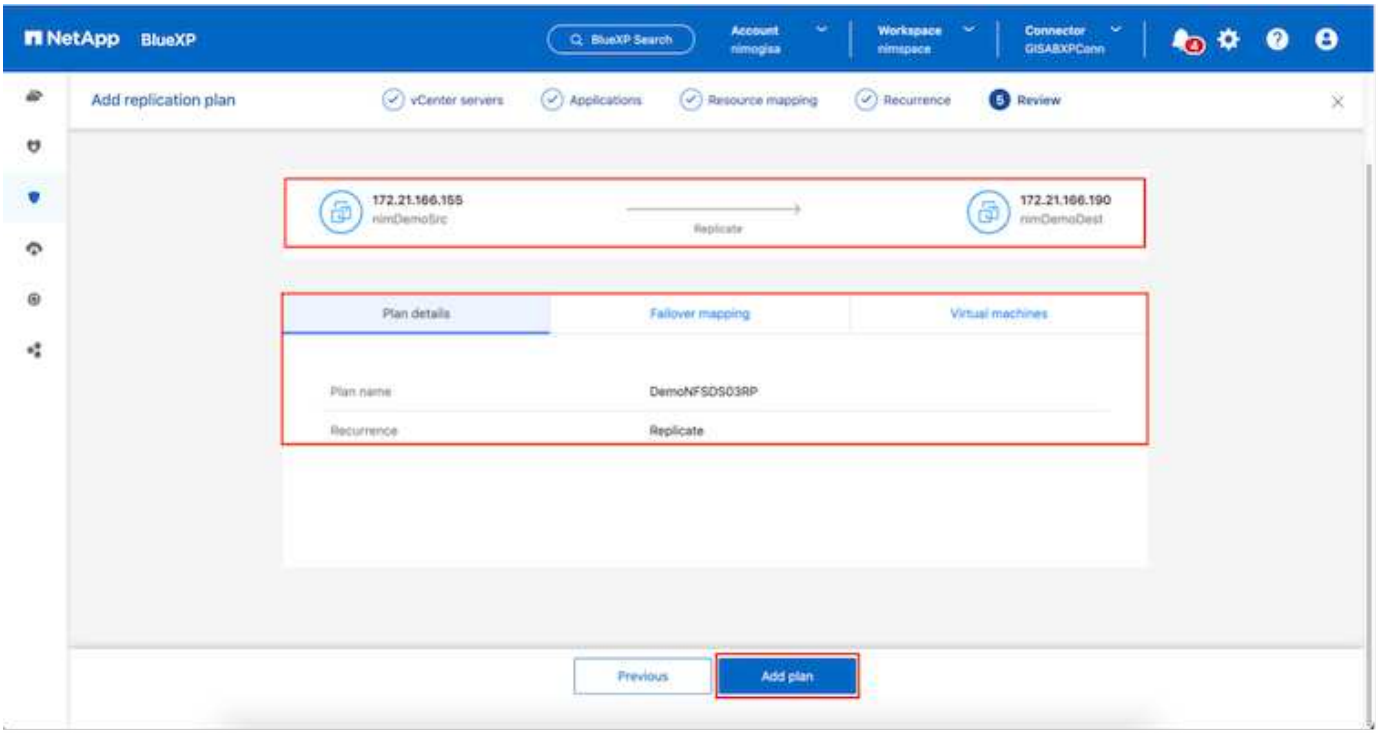


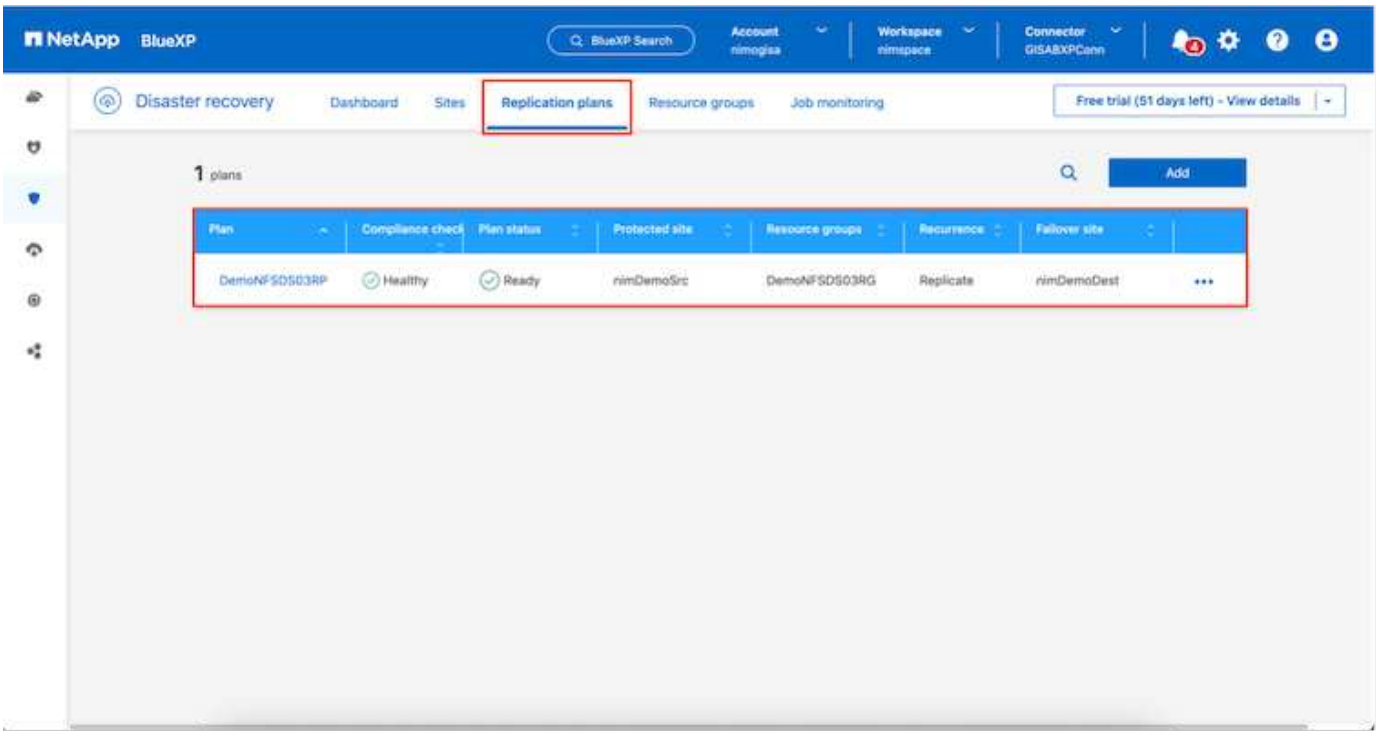
选择重复类型。简单来说，选择迁移（使用故障转移的一次性迁移）或重复连续复制选项。在本演练中，选择了“复制”选项。



完成后，检查创建的映射，然后单击*添加计划*。

来自不同卷和 SVM 的 VM 可以包含在复制计划中。根据 VM 的放置位置（无论是在同一卷上，还是在同一 SVM 中的不同卷上，亦或是在不同 SVM 上的不同卷上），灾难恢复会创建一个一致性组快照。



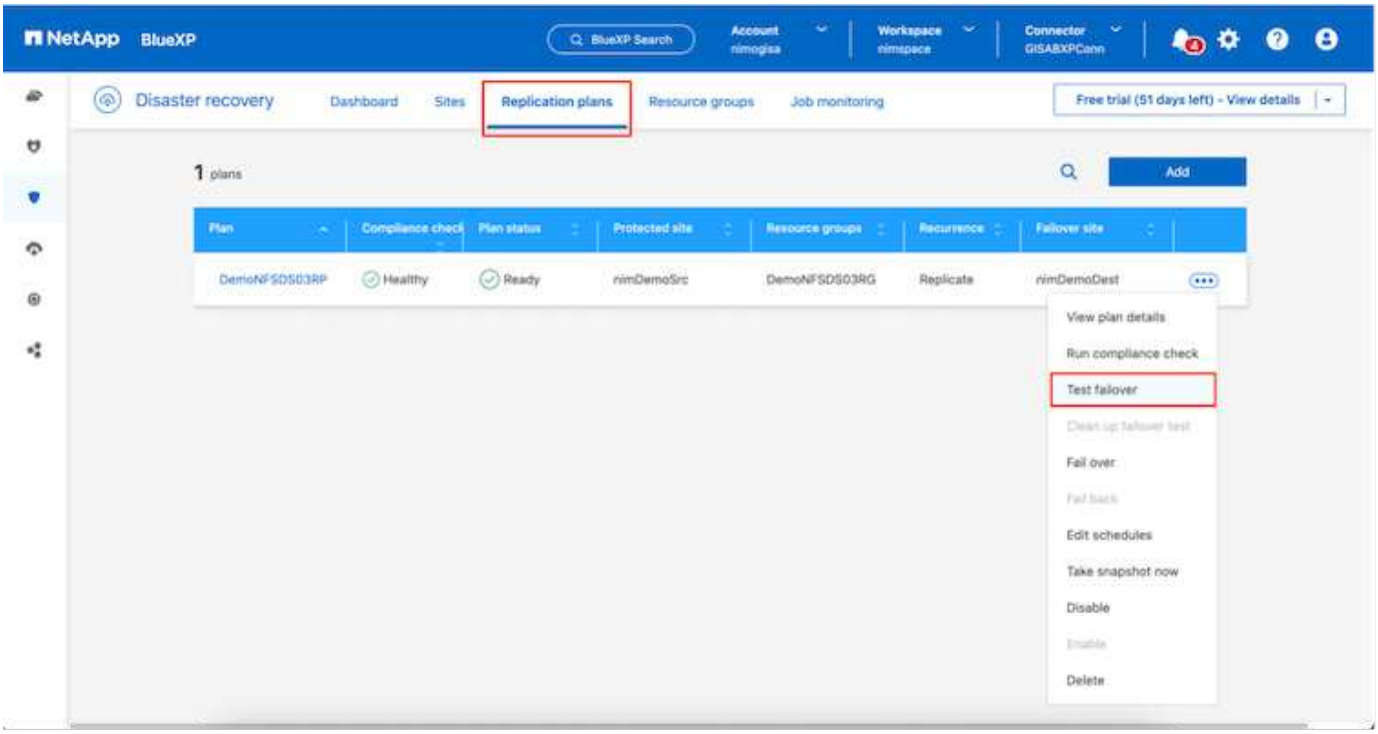


灾难恢复包括以下工作流：

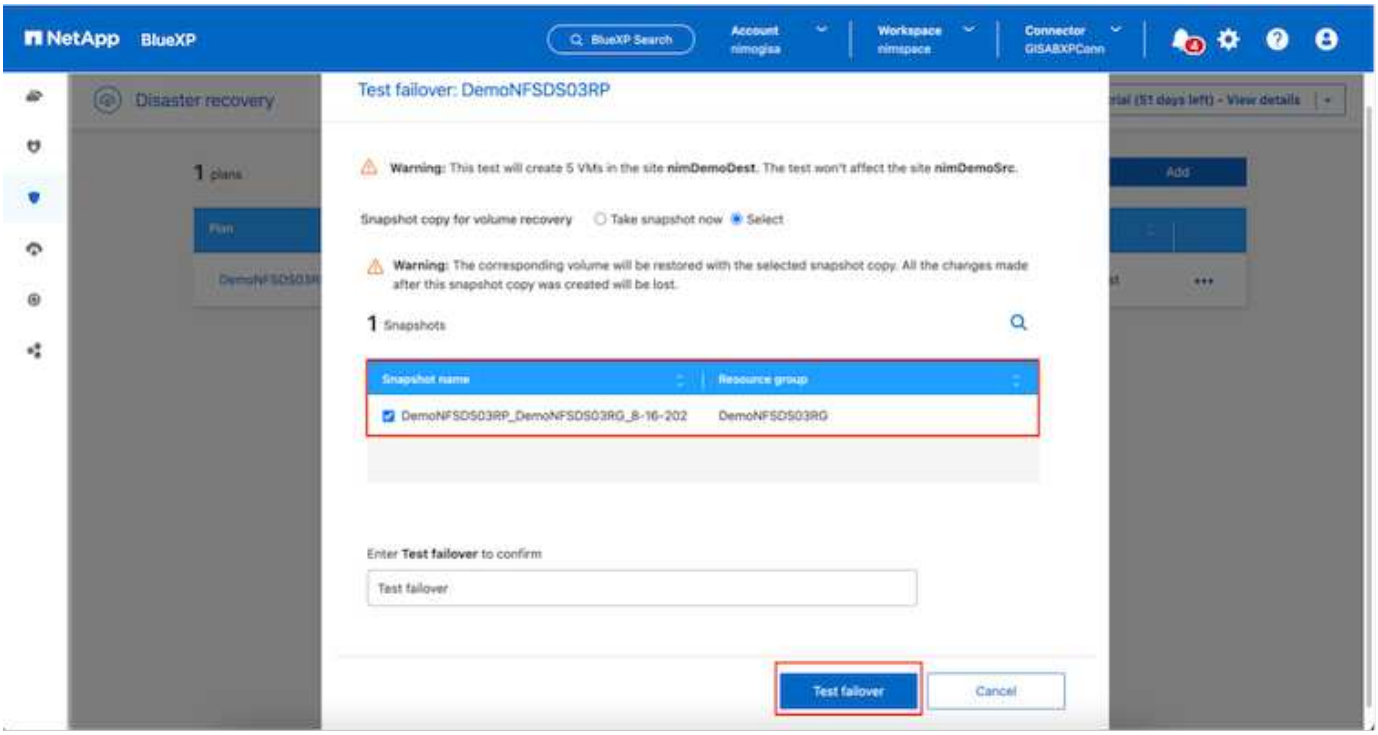
- 测试故障转移（包括定期自动模拟）
- 清理故障转移测试
- 故障转移
- 故障回复

测试故障转移

灾难恢复中的测试故障转移是一种操作过程，允许 VMware 管理员在不中断其生产环境的情况下完全验证其恢复计划。在测试故障转移期间，灾难恢复会在 DR 存储系统上创建复制的 NFS 数据存储卷的节省空间的 NetApp FlexClone 副本。然后将这些 FlexClone 卷挂载到 DR 站点的 ESXi 主机上，并在隔离的测试网络中开启虚拟机电源。此过程允许管理员验证其灾难恢复计划在发生实际灾难时能否按预期运行。

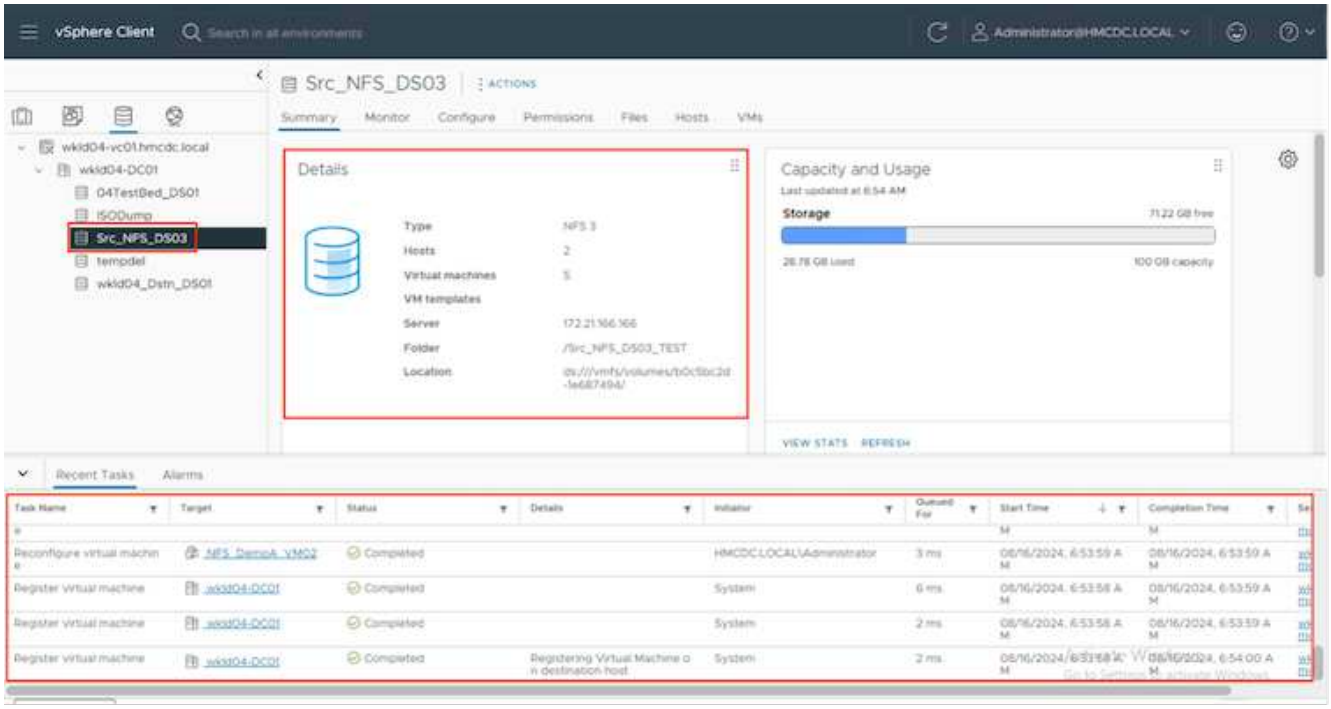


灾难恢复在测试故障转移操作中加入了选择快照这一可选功能。此功能允许 VMware 管理员验证最近在环境中所做的任何更改是否已复制到目标站点，从而确保这些更改在测试期间存在。此类更改包括虚拟机客户机操作系统的补丁



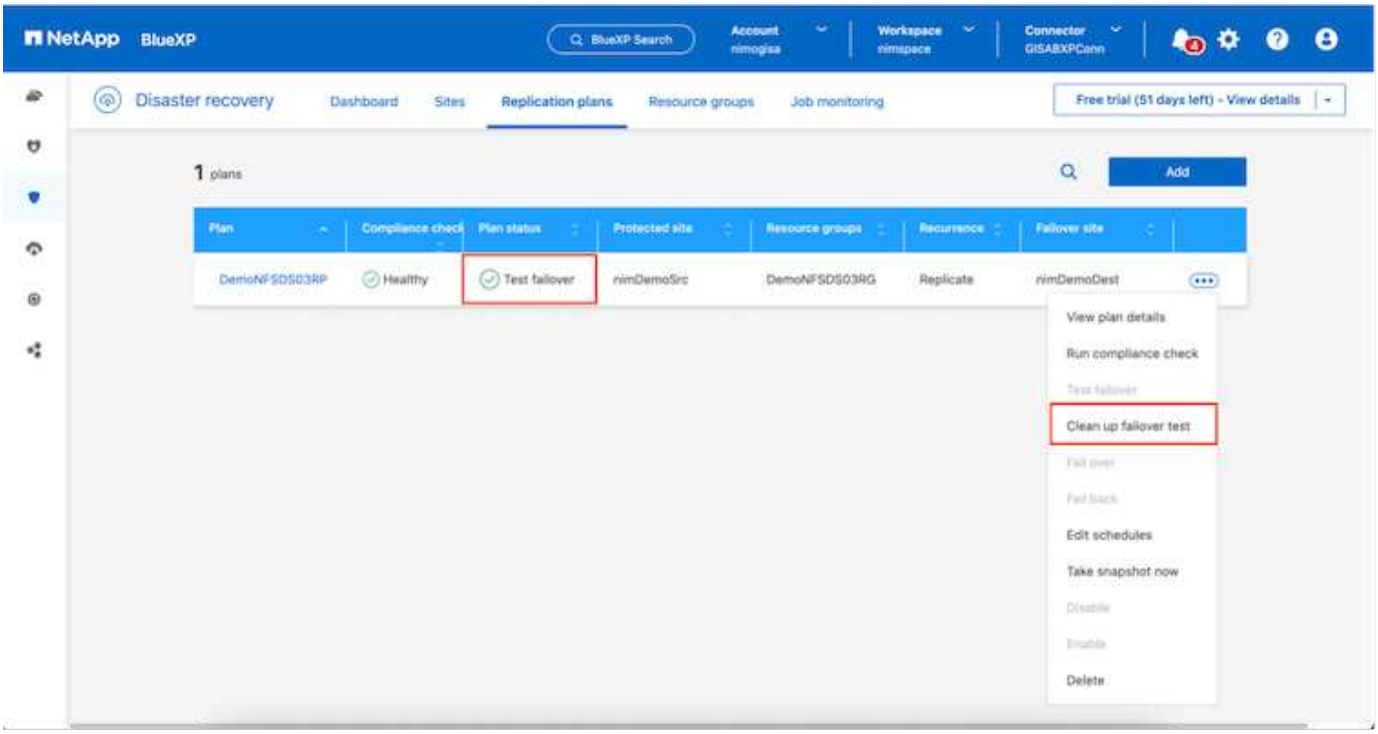
当 VMware 管理员运行测试故障切换操作时，灾难恢复会自动执行以下任务：

- 触发SnapMirror关系，使用生产站点上所做的任何最新更改来更新目标站点上的存储。
- 在 DR 存储阵列上创建FlexVol卷的NetApp FlexClone卷。
- 将FlexClone卷中的 NFS 数据存储库连接到 DR 站点的 ESXi 主机。
- 将虚拟机网络适配器连接到映射期间指定的测试网络。
- 按照 DR 站点的网络定义重新配置 VM 客户操作系统网络设置。
- 执行复制计划中存储的任何自定义命令。
- 按照复制计划中定义的顺序启动虚拟机。



清理故障转移测试操作

清理故障转移测试操作在复制计划测试完成并且 VMware 管理员响应清理提示后发生。



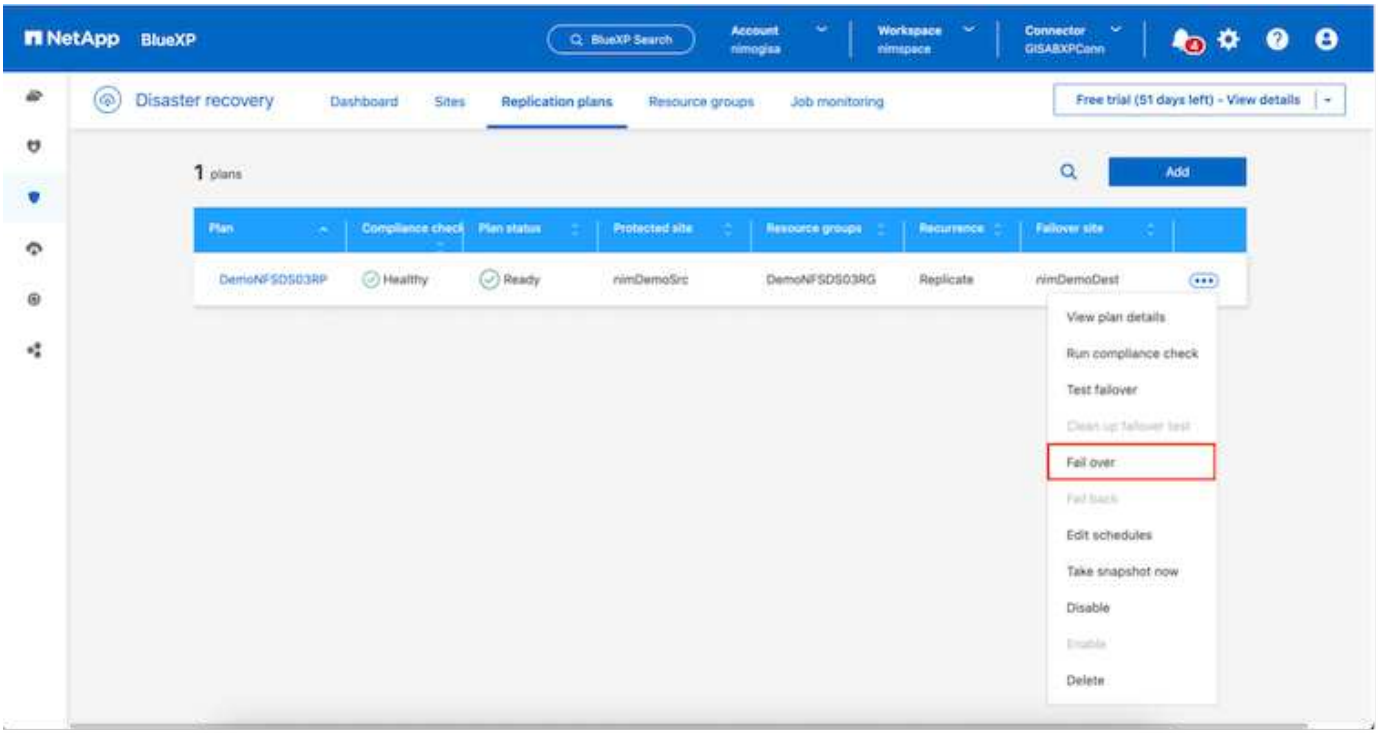
此操作将虚拟机 (VM) 和复制计划的状态重置为就绪状态。

当 VMware 管理员执行恢复操作时，灾难恢复将完成以下过程：

1. 它关闭用于测试的FlexClone副本中的每个恢复的虚拟机。
2. 它会删除在测试期间用于呈现恢复的虚拟机的 FlexClone卷。

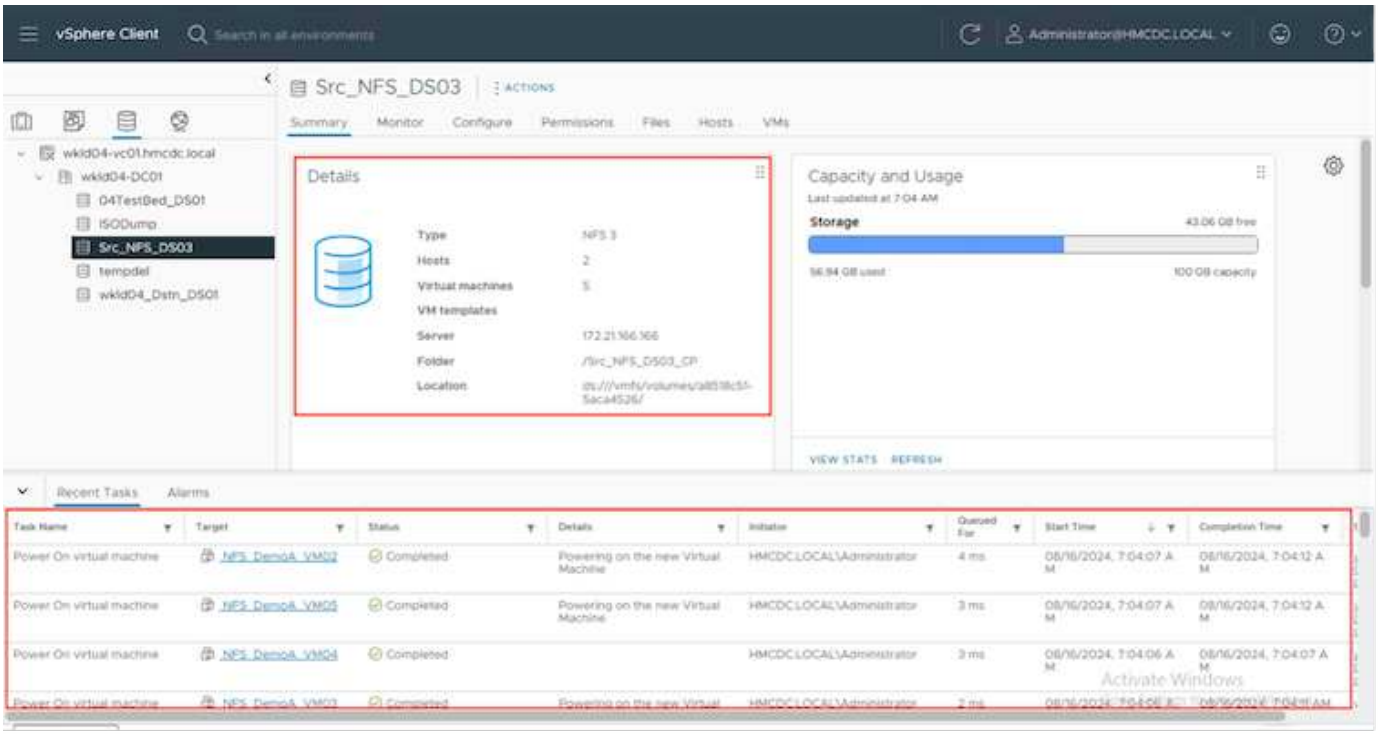
计划迁移和故障转移

灾难恢复有两种执行真正故障转移的方法：计划迁移和故障转移。第一种方法，即计划迁移，将虚拟机关闭和存储复制同步纳入流程，以恢复或有效地将虚拟机移动到目标站点。计划迁移需要访问源站点。第二种方法，即故障转移，是一种计划内/计划外故障转移，其中虚拟机在目标站点从能够完成的最后一个存储复制间隔进行恢复。根据解决方案中设计的 RPO，在 DR 场景中可能会出现一定程度的数据丢失。



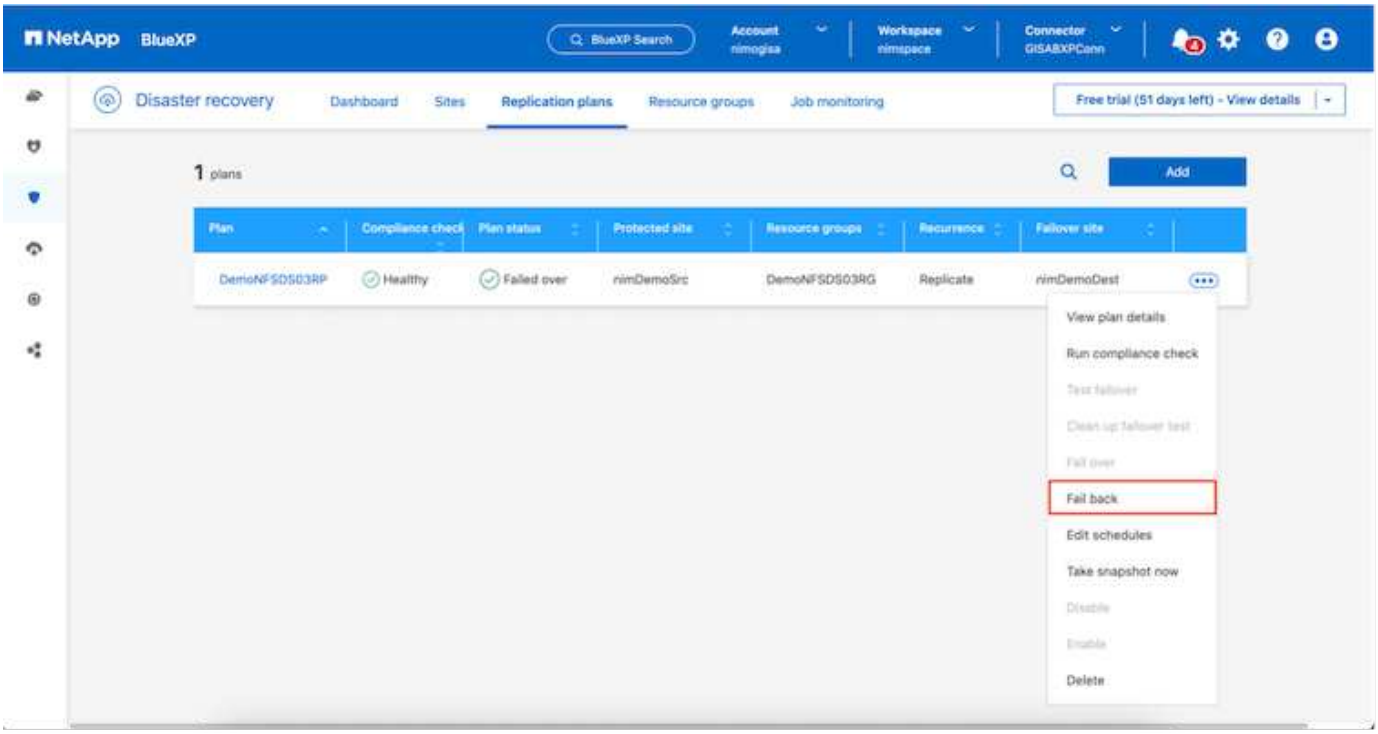
当 VMware 管理员执行故障切换操作时，灾难恢复会自动执行以下任务：

- 中断并故障转移NetApp SnapMirror关系。
- 将复制的 NFS 数据存储连接到 DR 站点的 ESXi 主机。
- 将 VM 网络适配器连接到适当的目标站点网络。
- 按照目标站点的网络定义重新配置 VM 客户操作系统网络设置。
- 执行复制计划中存储的任何自定义命令（如果有）。
- 按照复制计划中定义的顺序启动虚拟机。



故障回复

故障回复是一种可选过程，可在恢复后恢复源站点和目标站点的原始配置。



当 VMware 管理员准备将服务恢复到原始源站点时，他们可以配置并运行故障回复程序。

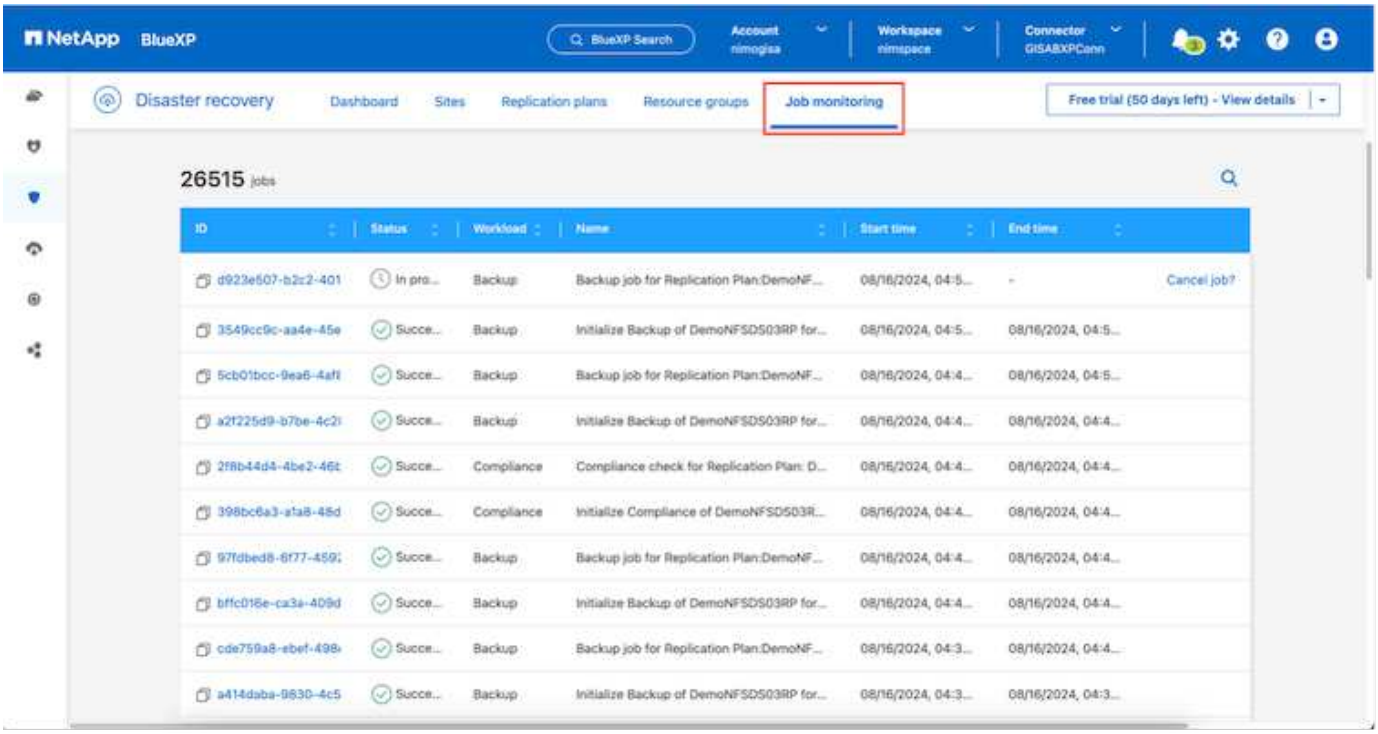
注意： 灾难恢复在反转复制方向之前，将任何更改复制（重新同步）回原始源虚拟机。此过程从已完成故障转移到目标的关系开始，涉及以下步骤：

- 关闭并取消注册虚拟机，并卸载目标站点上的卷。
- 打破原始源上的SnapMirror关系，使其变为读/写。
- 重新同步SnapMirror关系以逆转复制。
- 在源上安装卷，启动并注册源虚拟机。

有关访问和配置灾难恢复的详细信息，请参见 "了解适用于 VMware 的 NetApp Disaster Recovery"。

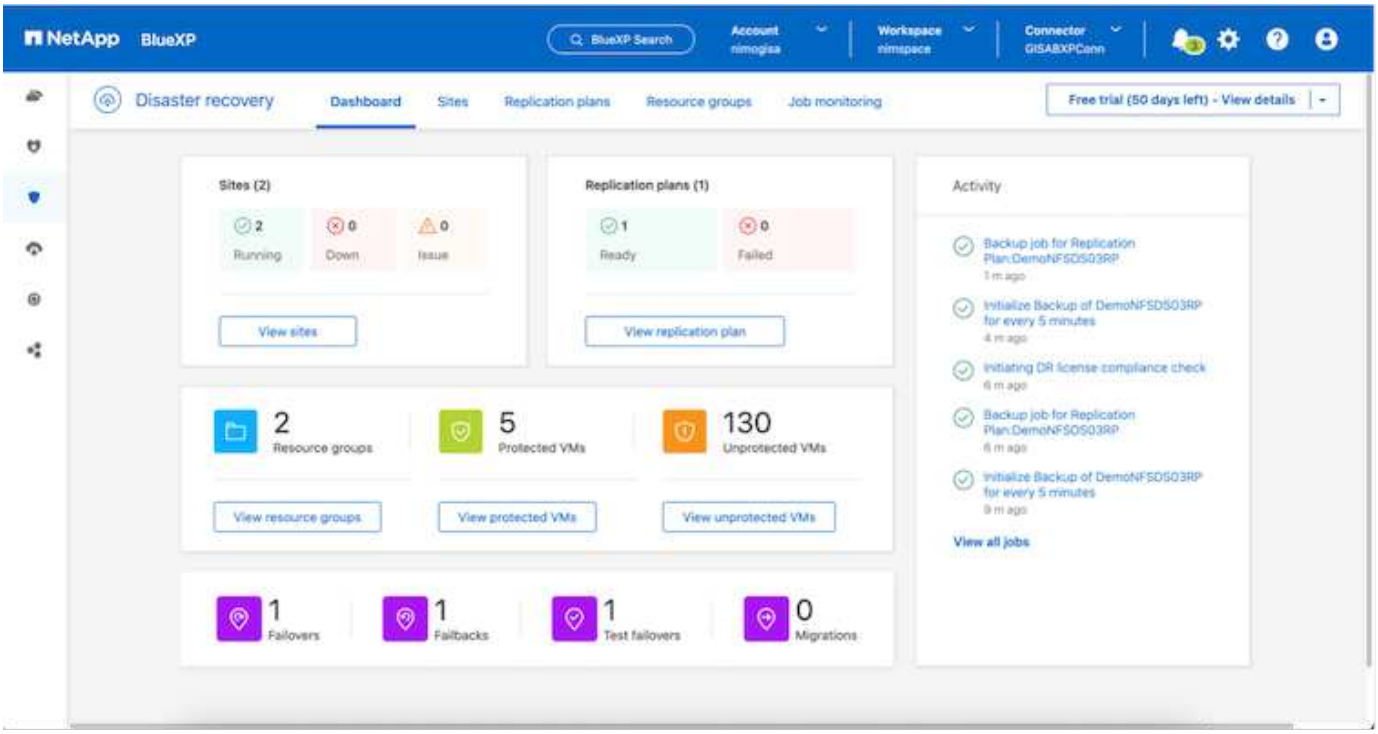
监控和仪表板

从控制台或 ONTAP 命令行界面中，您可以监控相应数据存储卷的复制健康状态，并且可以通过作业监控跟踪故障切换或测试故障切换的状态。



如果某项工作当前正在进行或排队，而您希望停止它，则可以选择取消它。

使用灾难恢复仪表板，自信地评估灾难恢复站点和复制计划的状态。这使管理员能够快速识别健康、断开连接或降级的站点和计划。



这为处理量身定制的灾难恢复计划提供了强大的解决方案。当发生灾难并决定激活 DR 站点时，可以按计划进行故障转移或单击按钮进行故障转移。

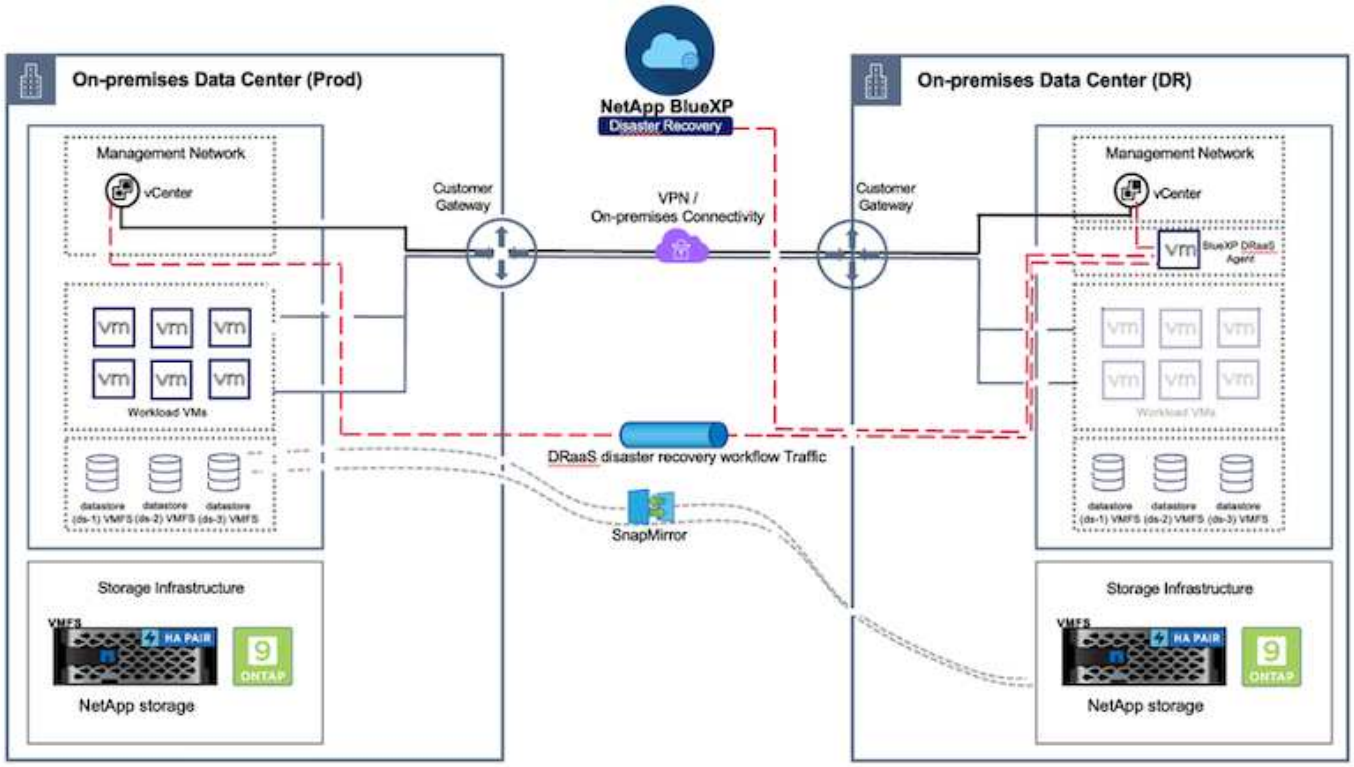
要了解有关此过程的更多信息，请随意观看详细的演示视频或使用"解决方案模拟器"。

VMFS 数据存储的 **NetApp Disaster Recovery**

使用从生产站点到灾难恢复站点的块级复制进行灾难恢复是一种有弹性且经济高效的方法，可以保护工作负载免受站点中断和数据损坏事件（如勒索软件攻击）的影响。借助NetApp SnapMirror复制，使用 VMFS 数据存储区运行本地ONTAP系统的 VMware 工作负载可以复制到 VMware 所在的指定恢复数据中心的另一个ONTAP存储系统

本文档的这一部分描述了 NetApp Disaster Recovery 的配置，以便为本地 VMware VM 设置到另一个指定站点的灾难恢复。作为此设置的一部分，包括 Console 代理、载入 ONTAP 阵列、定义站点以及关联 VMware vCenter。此外，本文档详细介绍了如何配置站点之间的复制以及如何设置和测试恢复计划。最后一部分包含有关执行完整站点故障转移的说明，以及如何在主站点恢复并重新上线时进行故障恢复。

利用灾难恢复（NetApp Data Services 的一部分），客户可以发现其本地 VMware vCenters 以及 ONTAP 存储，创建资源分组，创建灾难恢复计划，将其与资源组相关联，并测试或执行故障转移和故障恢复。SnapMirror 提供存储级块复制，以使两个站点保持最新的增量更改，从而实现长达 5 分钟的 RPO。也可以将 DR 过程模拟为常规演练，而不会影响生产和复制数据存储，也不会产生额外的存储成本。NetApp Data Services 利用 ONTAP 的 FlexClone 技术，从 DR 站点上最后复制的 Snapshot 创建 VMFS 数据存储的节省空间的副本。DR 测试完成后，客户只需删除测试环境，同样不会对实际复制的生产资源产生任何影响。当需要（计划内或计划外）进行实际故障转移时，只需单击几下，灾难恢复将协调在指定的灾难恢复站点上自动启动受保护虚拟机所需的所有步骤。该服务还将反转与主站点的 SnapMirror 关系，并在需要时复制从辅助站点到主站点的任何更改，以进行故障恢复操作。与其他众所周知的替代方案相比，所有这些都可以以极低的成本实现。

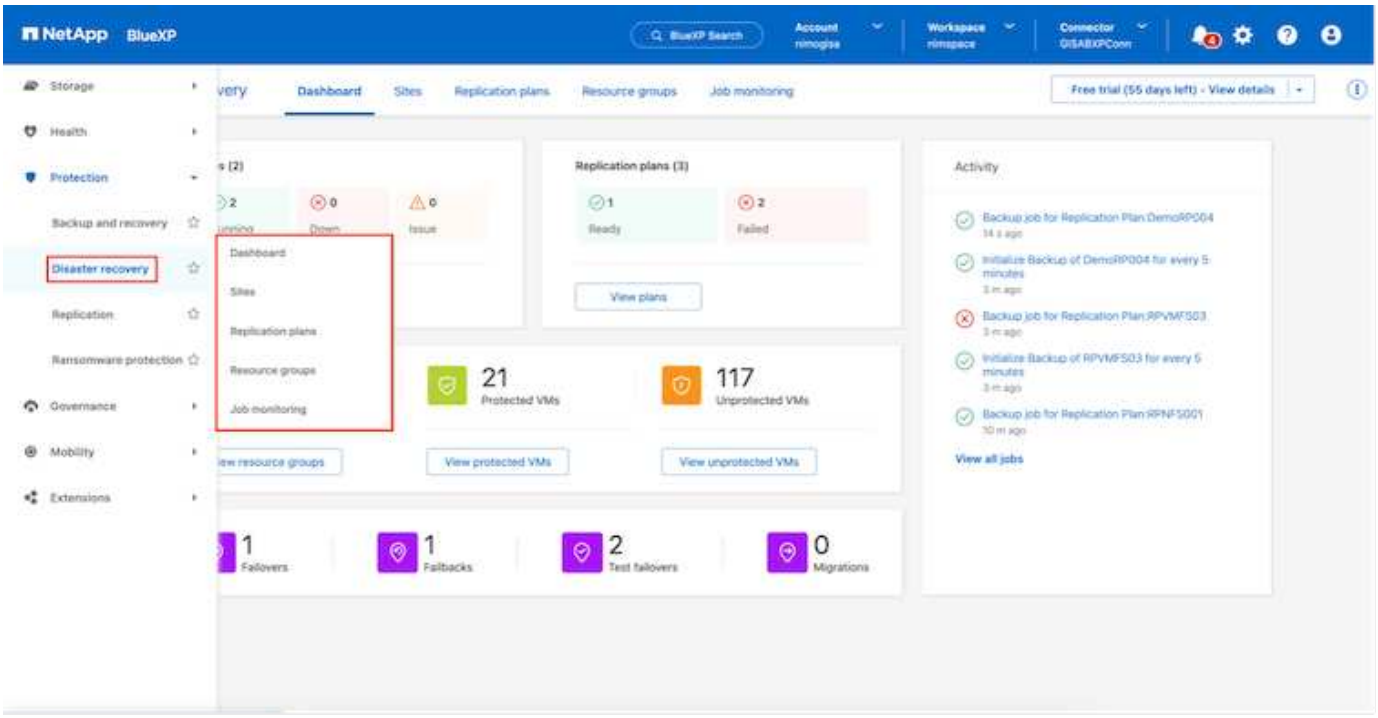


有关用于灾难恢复的 vCenter Server、ESXi 和 ONTAP 的最新信息和支持版本，请参见 "灾难恢复支持的配置"。

入门

要开始使用灾难恢复，请使用 NetApp Console，然后访问服务。

1. 登录到 Console。
2. 在控制台左侧导航栏中，选择“保护” > “灾难恢复”。
3. 此时将显示灾难恢复仪表板。

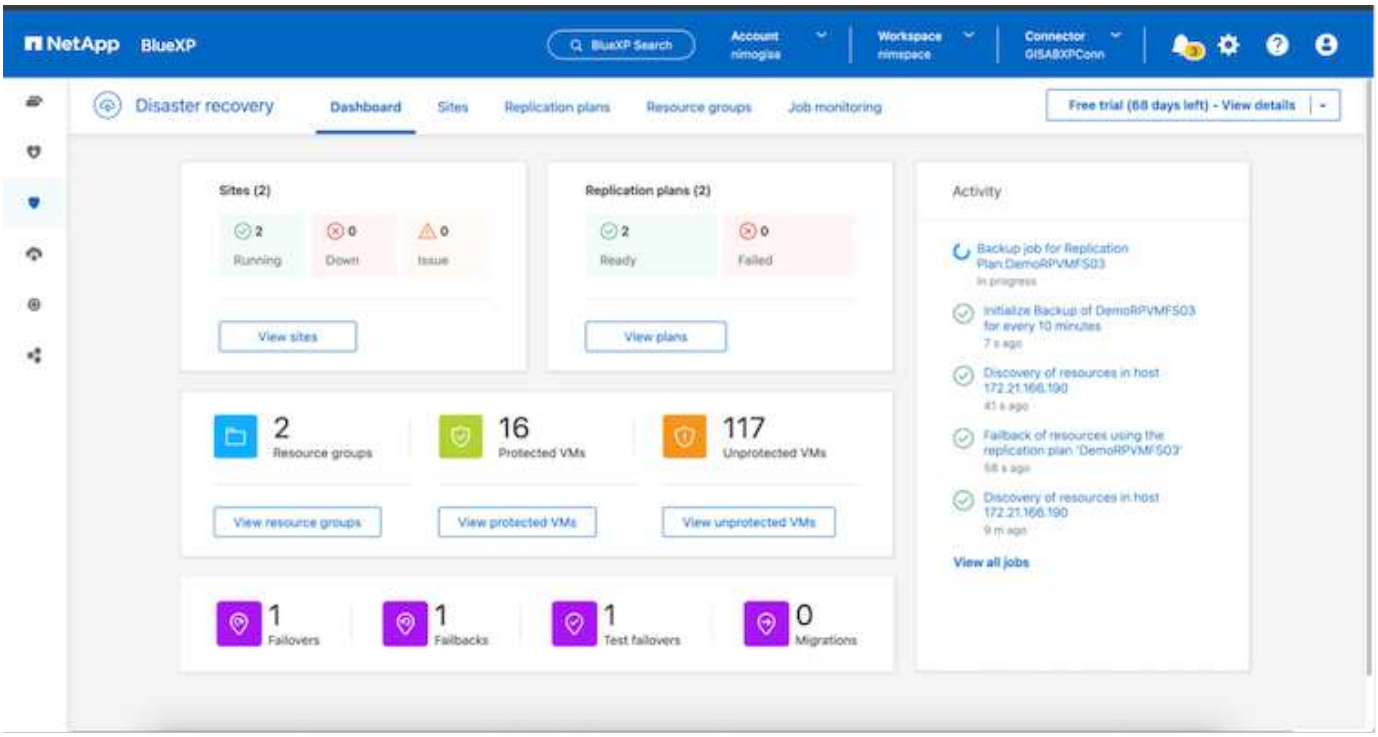


配置灾难恢复计划之前，请确保满足以下先决条件：

- 控制台代理部署在 AWS VPC 中。
- 控制台代理实例具有到源和目标 vCenter 以及存储系统的连接。
- 在控制台中添加了托管适用于 VMware 的 VMFS 数据存储的本地 NetApp 存储系统。
- 使用 DNS 名称时应该进行 DNS 解析。否则，请使用 vCenter 的 IP 地址。
- SnapMirror复制是为指定的基于 VMFS 的数据存储卷配置的。

一旦源站点和目标站点之间建立连接，请继续执行配置步骤，这大约需要 3 到 5 分钟。

NetApp 建议在灾难恢复站点或第三个站点中部署控制台代理，以便控制台代理在实际中断或自然灾害期间可以通过网络与源和目标资源进行通信。

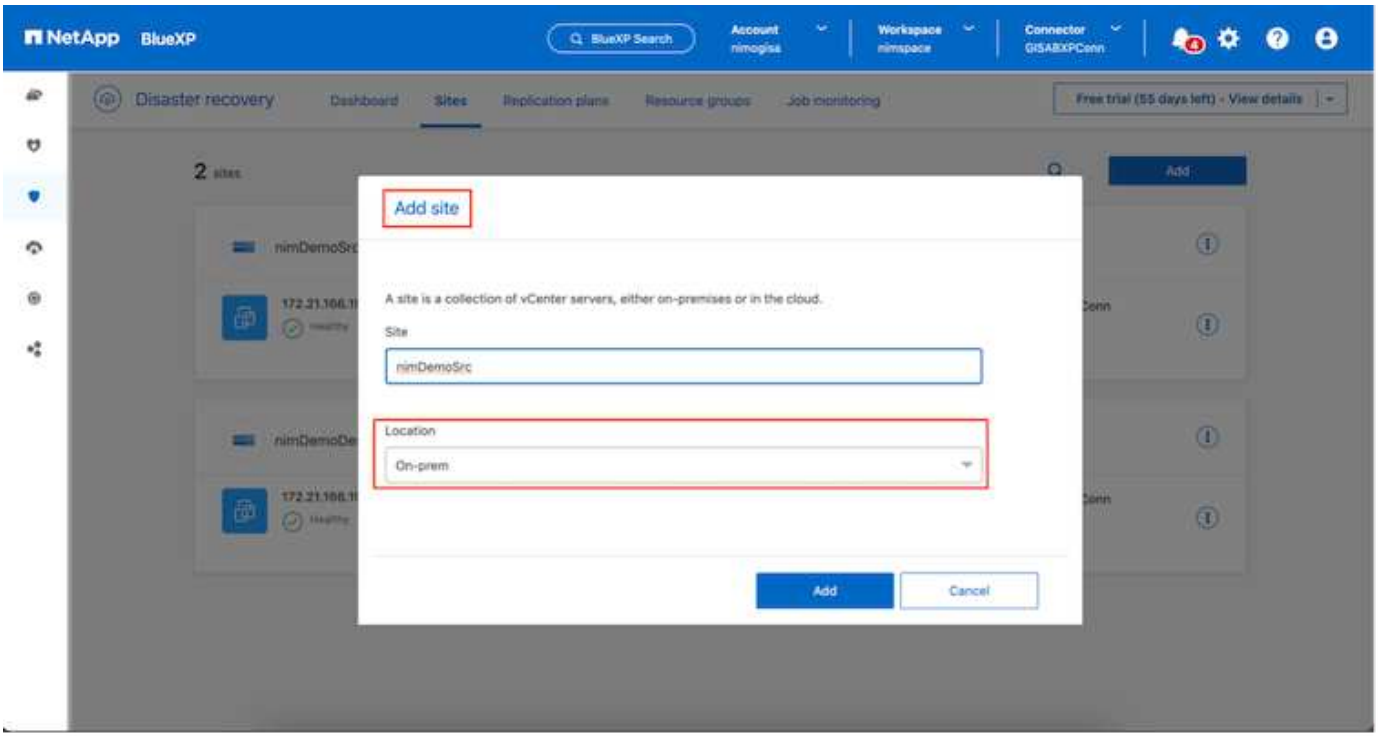


在撰写本文档时，对本地到本地 VMFS 数据存储的支持处于技术预览阶段。基于 FC 和 ISCSI 协议的 VMFS 数据存储均支持该功能。

灾难恢复配置

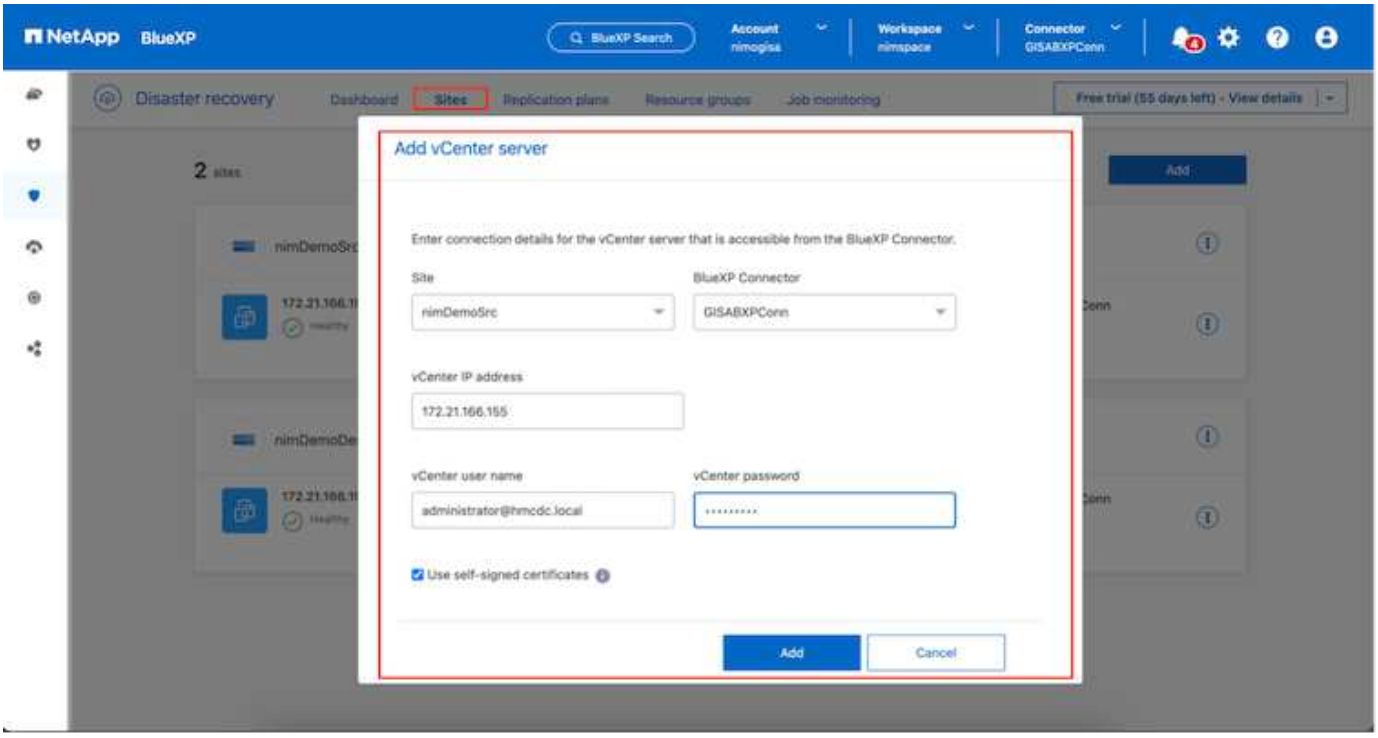
准备灾难恢复的第一步是发现本地 vCenter 和存储资源并将其添加到灾难恢复。

确保 ONTAP 存储系统已添加到画布内的工作环境中。打开控制台，然后从左侧导航中选择 保护 > 灾难恢复。选择 发现 **vCenter** 服务器 或使用顶部菜单，选择 站点 > 添加 > 添加 **vCenter**。

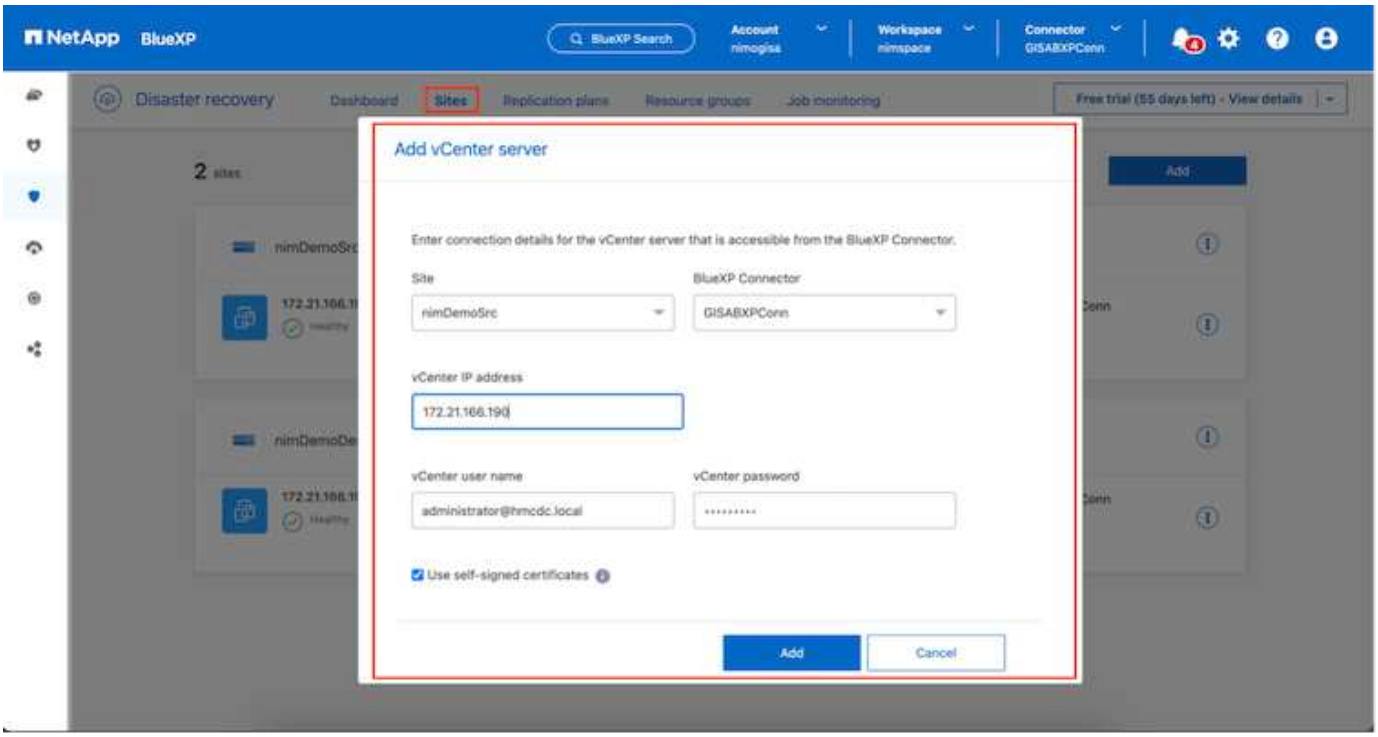


添加以下平台：

- 来源。本地 vCenter。



- 目的地。 VMC SDDC vCenter。



一旦添加了 vCenter，就会触发自动发现。

配置源站点和目标站点之间的存储复制

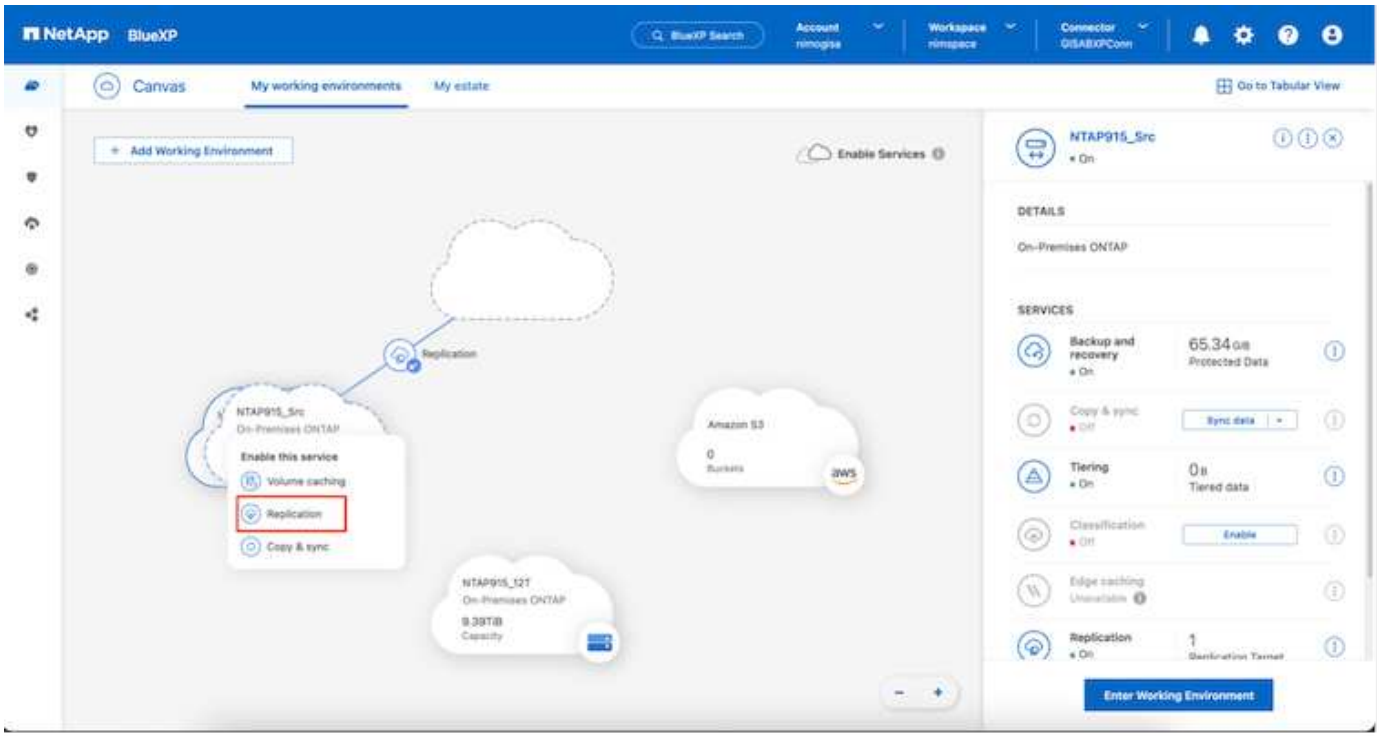
SnapMirror利用ONTAP快照来管理从一个位置到另一个位置的数据传输。首先，基于源卷快照的完整副本被复制到目标位置以执行基线同步。当源处发生数据变化时，会创建一个新的快照并将其与基线快照进行比较。然后将发现已更改的块复制到目标位置，其中较新的快照成为当前基线或最新的公共快照。这使得该过程可以重复，并且增量更新可以发送到目的地。

建立SnapMirror关系后，目标卷处于联机只读状态，因此仍然可访问。 SnapMirror与物理存储块一起工作，而不是在文件或其他逻辑级别上工作。这意味着目标卷是源的相同副本，包括快照、卷设置等。如果源卷正在使用ONTAP空间效率功能（例如数据压缩和重复数据删除），则复制的卷将保留这些优化。

中断SnapMirror关系会使目标卷变得可写，并且通常在使用SnapMirror将数据同步到 DR 环境时用于执行故障转移。 SnapMirror足够复杂，可以允许故障转移站点上更改的数据有效地重新同步回主系统（如果主系统稍后恢复在线），然后允许重新建立原始的SnapMirror关系。

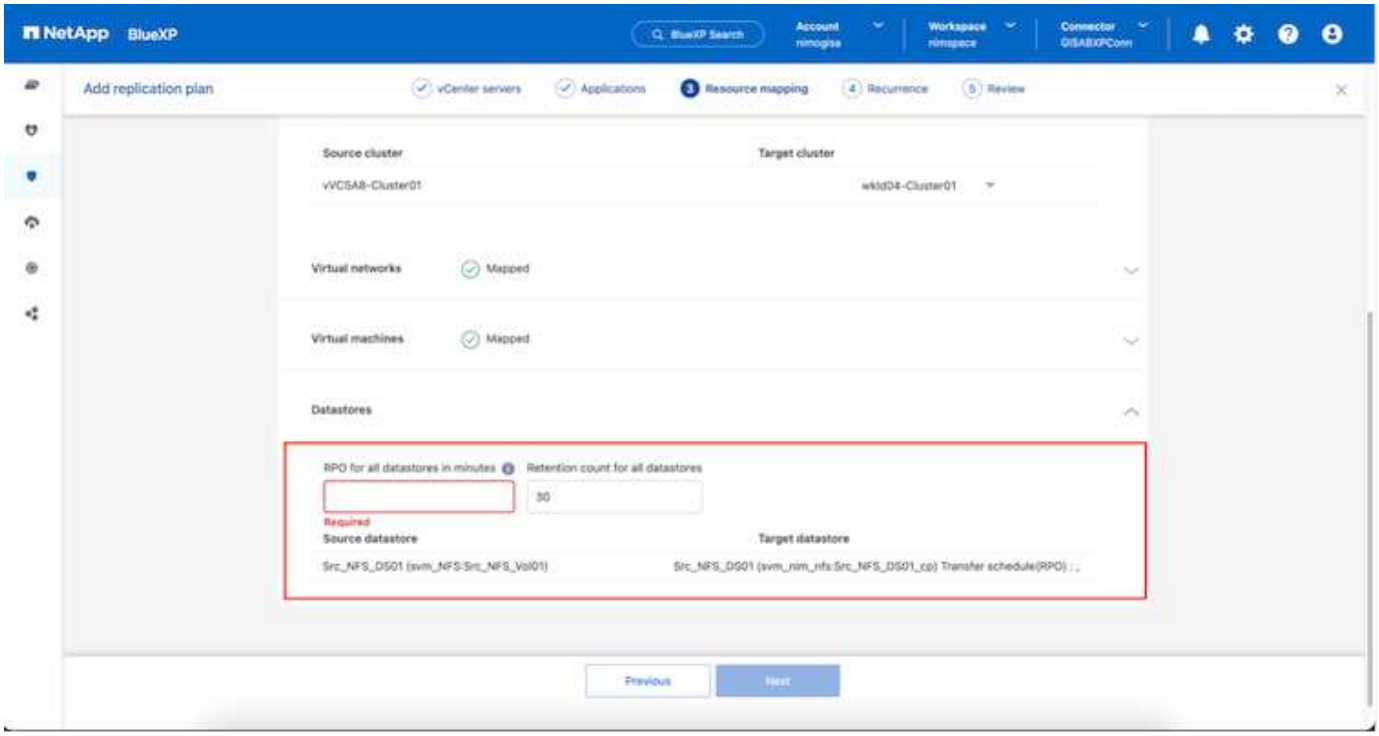
如何设置 **VMware** 灾难恢复

对于任何给定应用程序，创建 SnapMirror 复制的过程保持不变。该过程可以是手动或自动的。最简单的方法是利用控制台，通过将环境中的源 ONTAP 系统简单地拖放到目标上来配置 SnapMirror 复制，从而触发向导以指导完成剩余过程。



NetApp Data Services 也可以自动执行相同的操作，前提是满足以下两个条件：

- 源集群和目标集群具有对等关系。
- 源 SVM 和目标 SVM 具有对等关系。

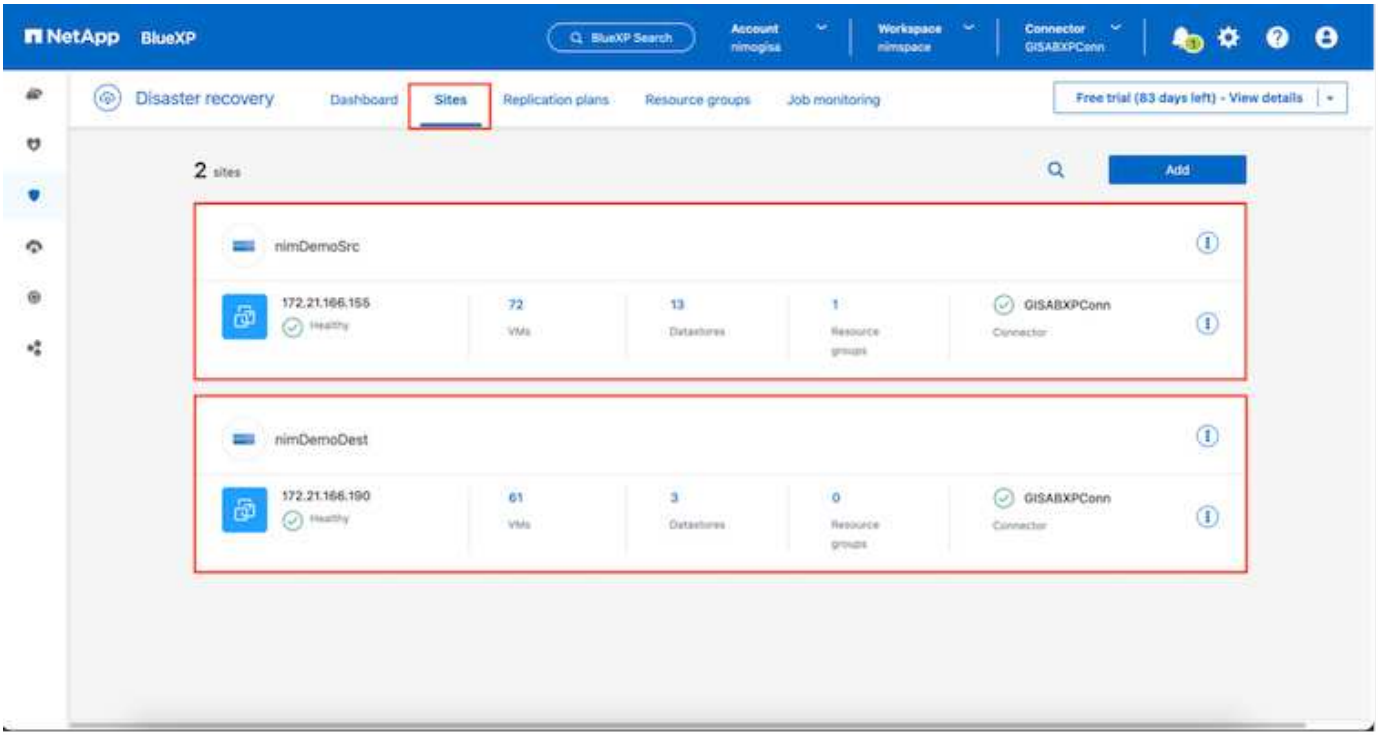


如果已通过 CLI 为该卷配置了 SnapMirror 关系，Console 将提取该关系并继续其余的工作流操作。

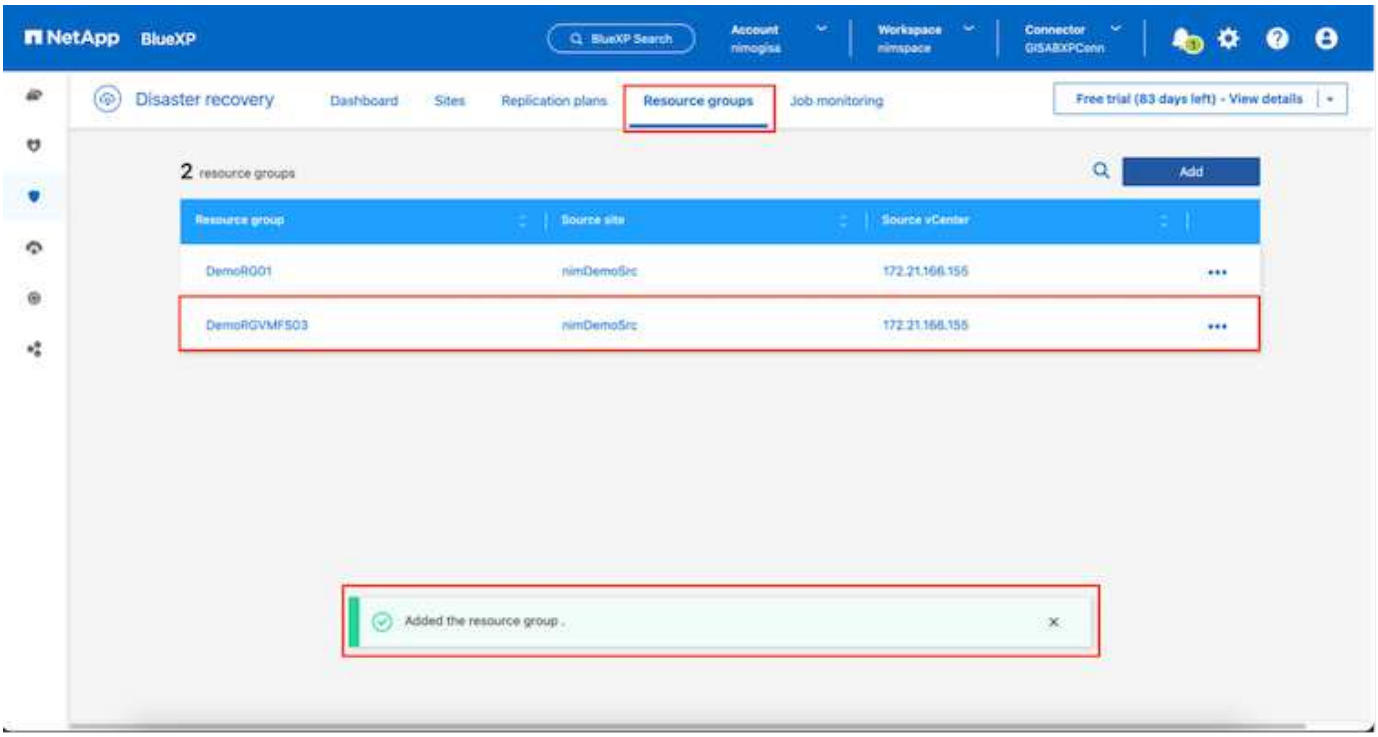
除了上述方法外，还可以通过 ONTAP CLI 或 System Manager 创建 SnapMirror 复制。无论使用哪种方法通过 SnapMirror 同步数据，灾难恢复都会协调工作流程，以实现无缝且高效的灾难恢复操作。

灾难恢复可以为您做些什么？

添加源站点和目标站点后，灾难恢复将执行自动深度发现并显示虚拟机以及关联的元数据。灾难恢复还会自动检测虚拟机使用的网络和端口组，并填充它们。

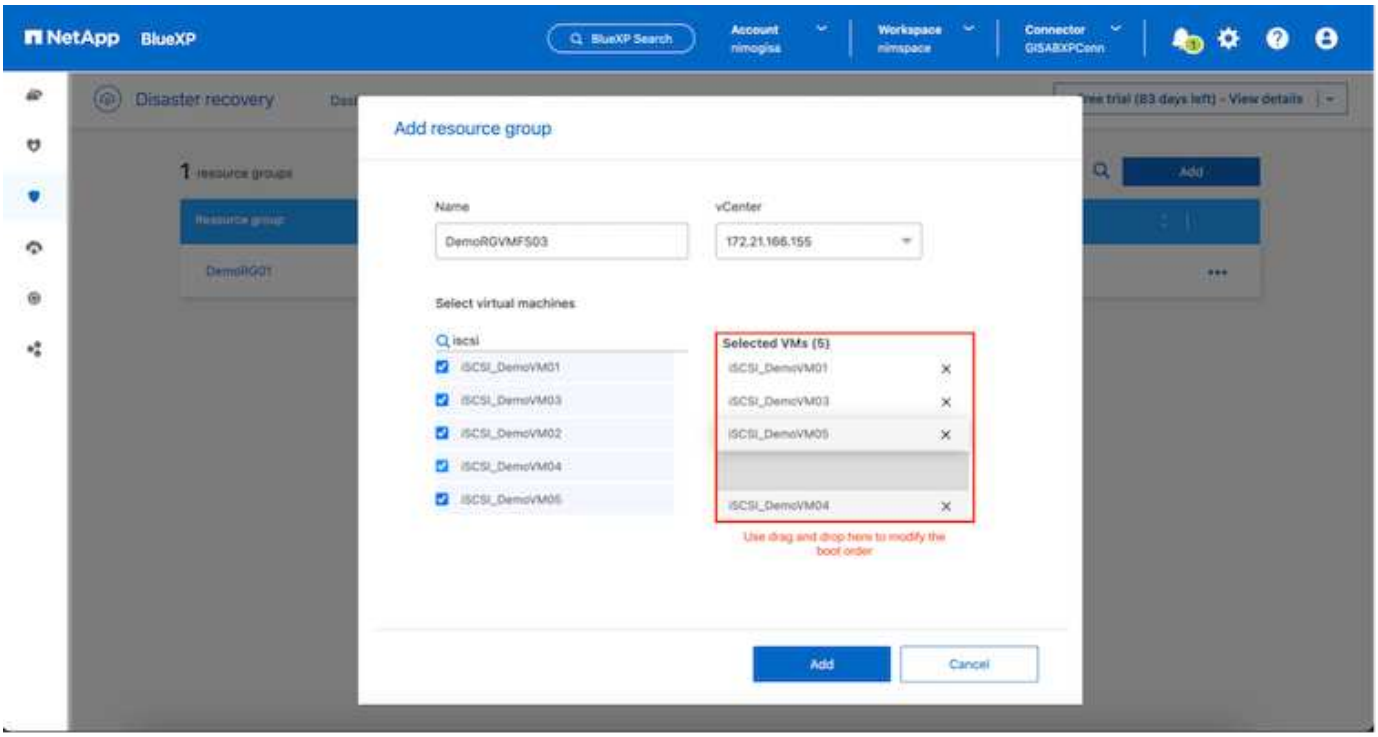


添加站点后，可以将 VM 分组到资源组中。灾难恢复资源组允许您将一组从属虚拟机分组到包含其启动顺序和启动延迟的逻辑组中，这些启动顺序和启动延迟可在恢复时执行。要开始创建资源组，请导航到*资源组*，然后单击*创建新资源组*。

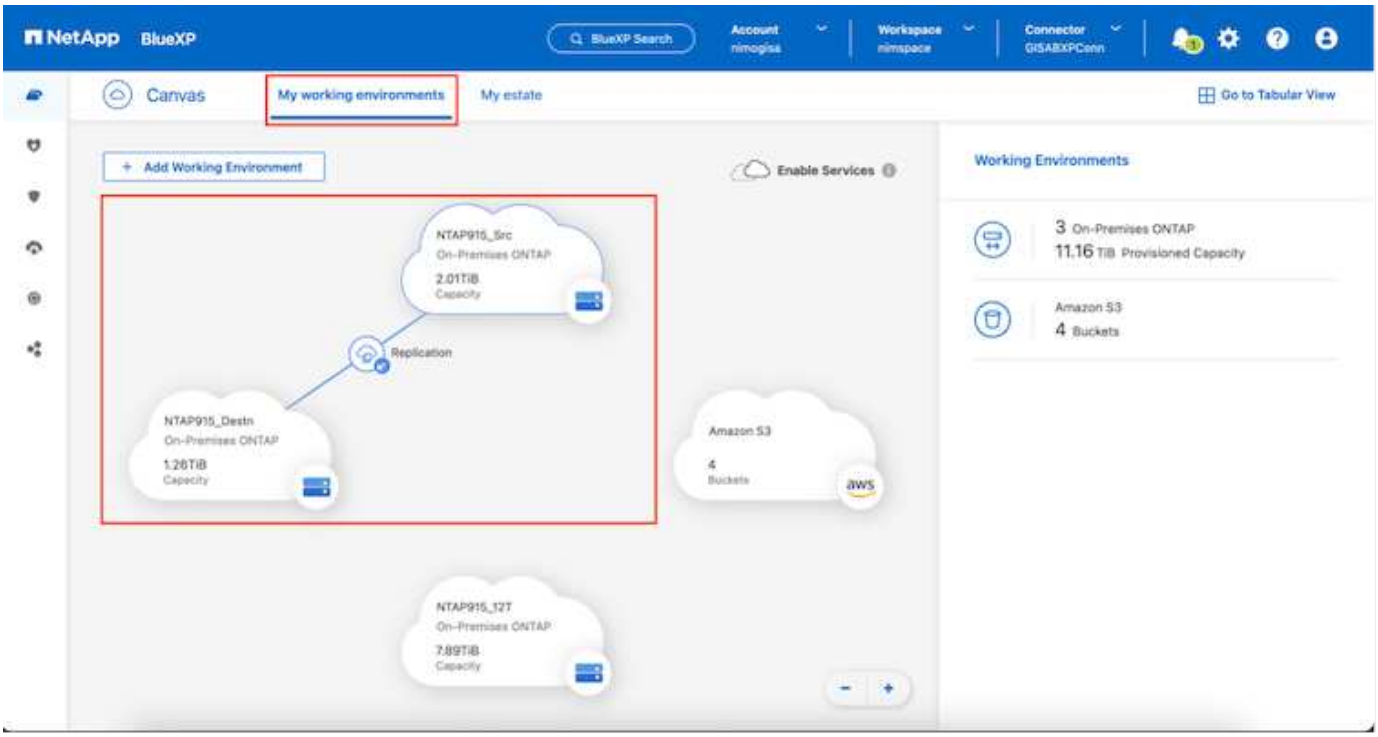


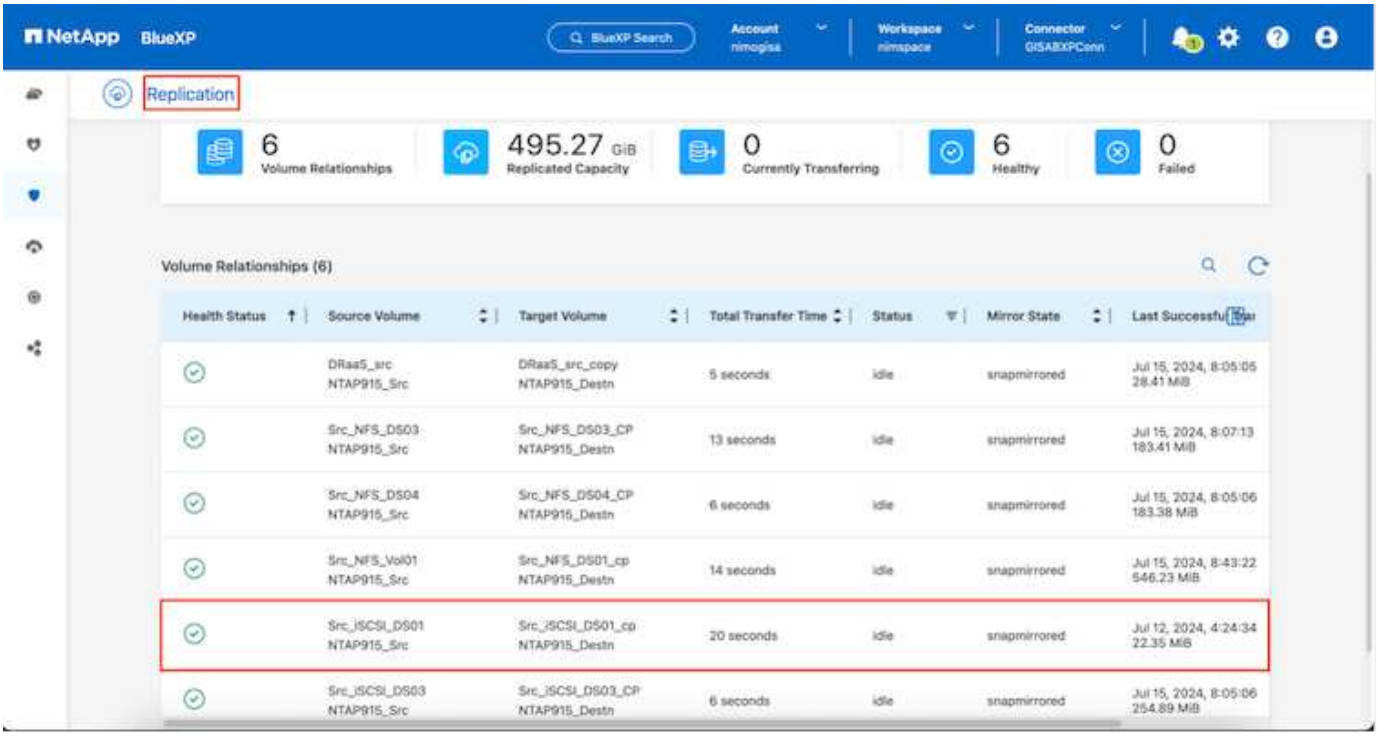
在创建复制计划时也可以创建资源组。

可以通过简单的拖放机制在创建资源组期间定义或修改虚拟机的启动顺序。



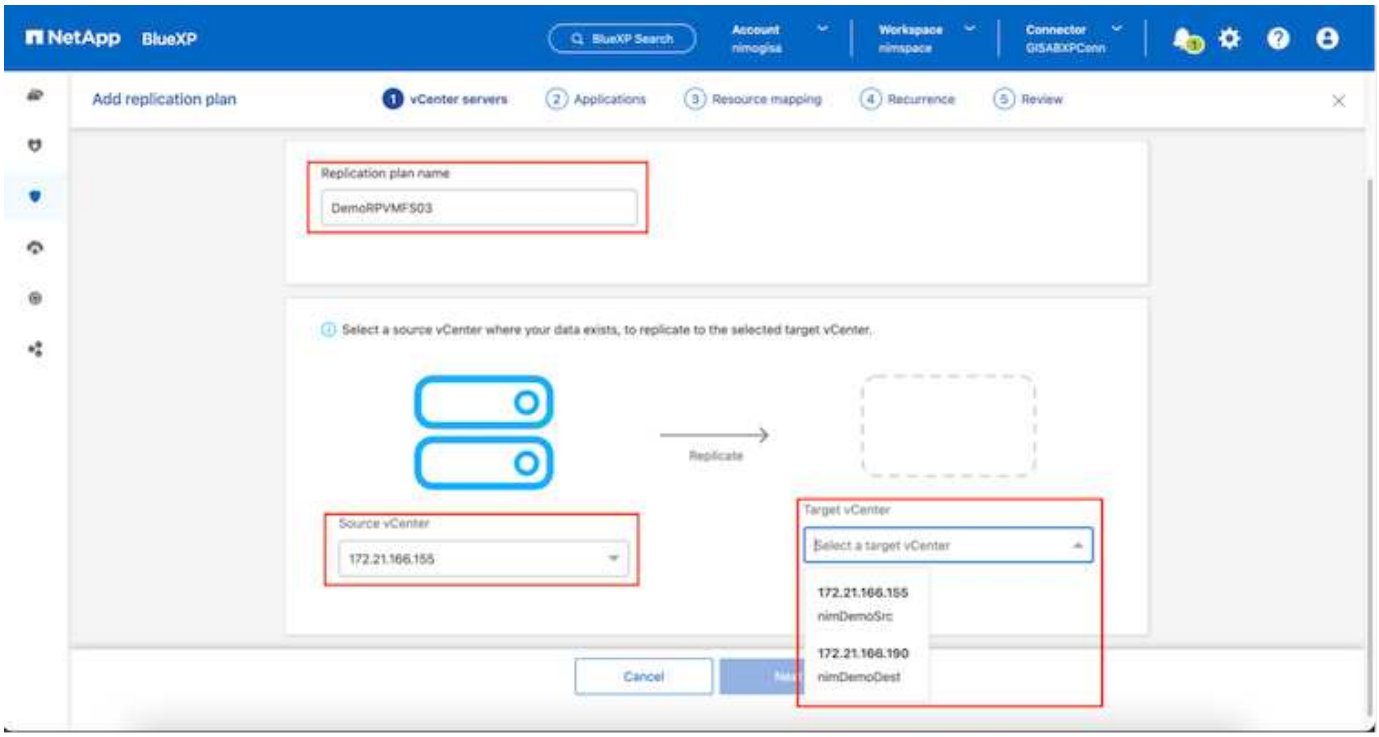
创建资源组后，下一步是创建执行蓝图或在发生灾难时恢复虚拟机和应用程序的计划。如先决条件中所述，可以预先配置SnapMirror复制，或者 DRaaS 可以使用在创建复制计划期间指定的 RPO 和保留计数来配置它。



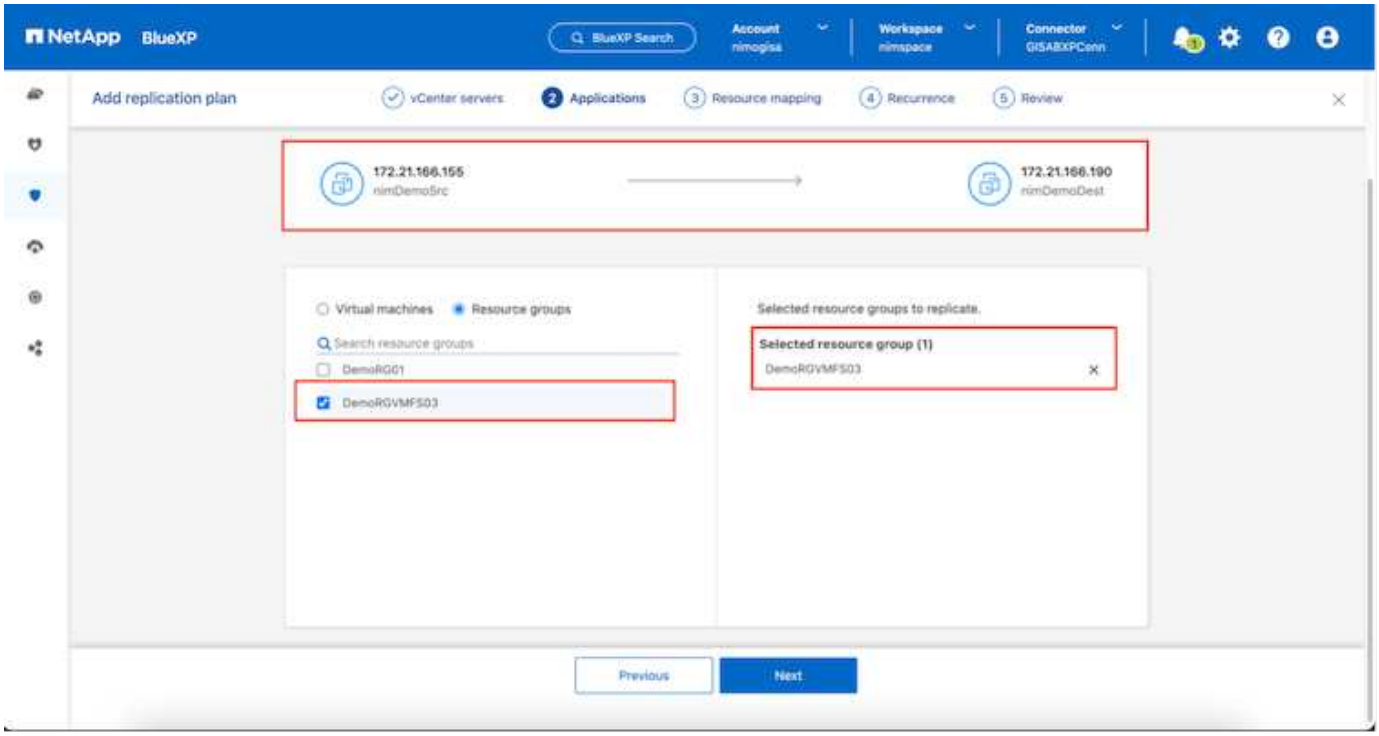


通过从下拉菜单中选择源和目标 vCenter 平台来配置复制计划，并选择要包含在计划中的资源组，以及如何恢复和启动应用程序的分组以及集群和网络的映射。要定义恢复计划，请导航到“复制计划”选项卡并单击“添加计划”。

首先，选择源 vCenter，然后选择目标 vCenter。



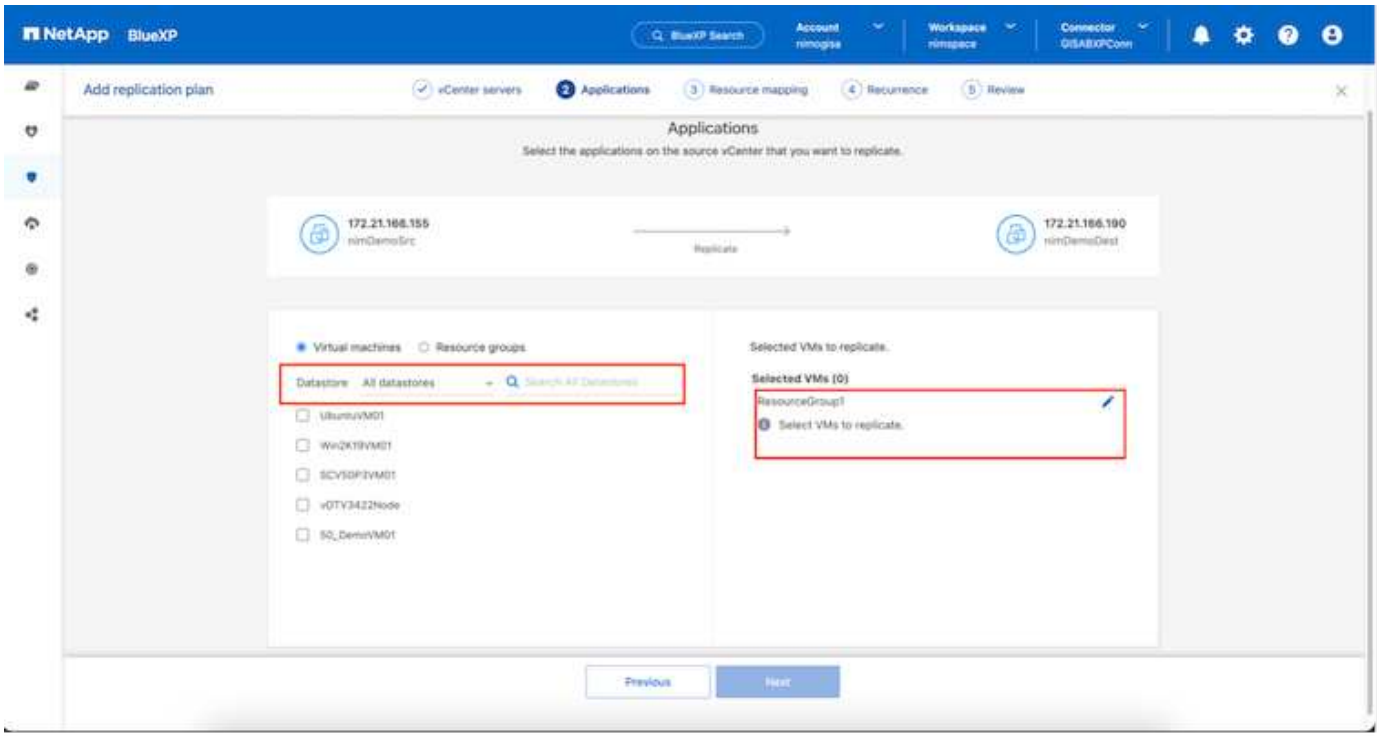
下一步是选择现有的资源组。如果没有创建资源组，则向导将帮助根据恢复目标对所需的虚拟机进行分组（基本上创建功能资源组）。这也有助于定义如何恢复应用程序虚拟机的操作顺序。



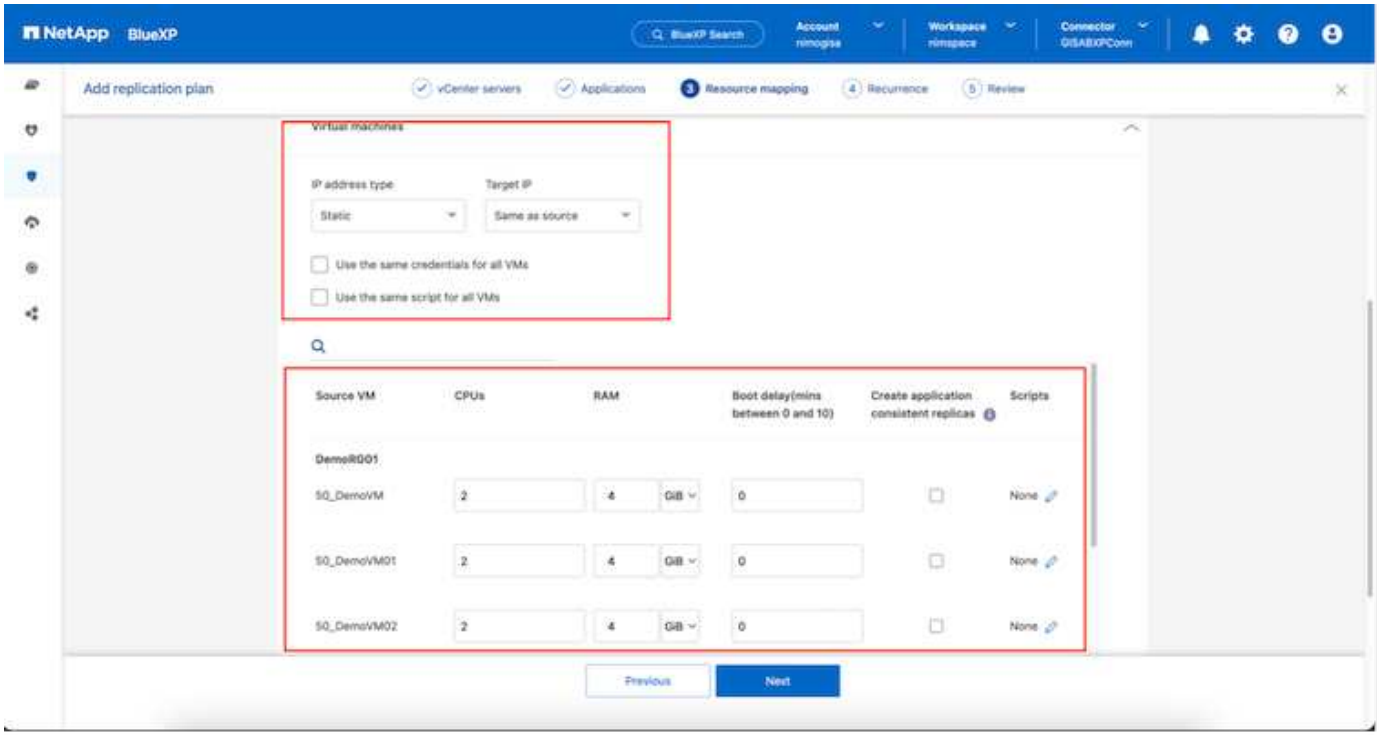
资源组允许使用拖放功能设置启动顺序。它可用于轻松修改恢复过程中虚拟机的启动顺序。

资源组内的各个虚拟机按照顺序依次启动。两个资源组并行启动。

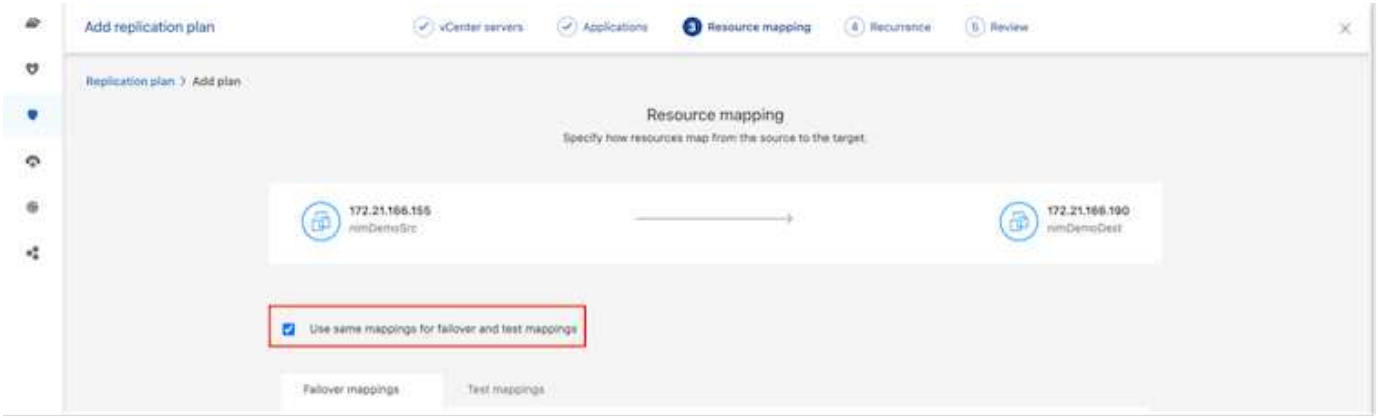
如果未事先创建资源组，则以下屏幕截图显示了根据组织要求过滤虚拟机或特定数据存储的选项。



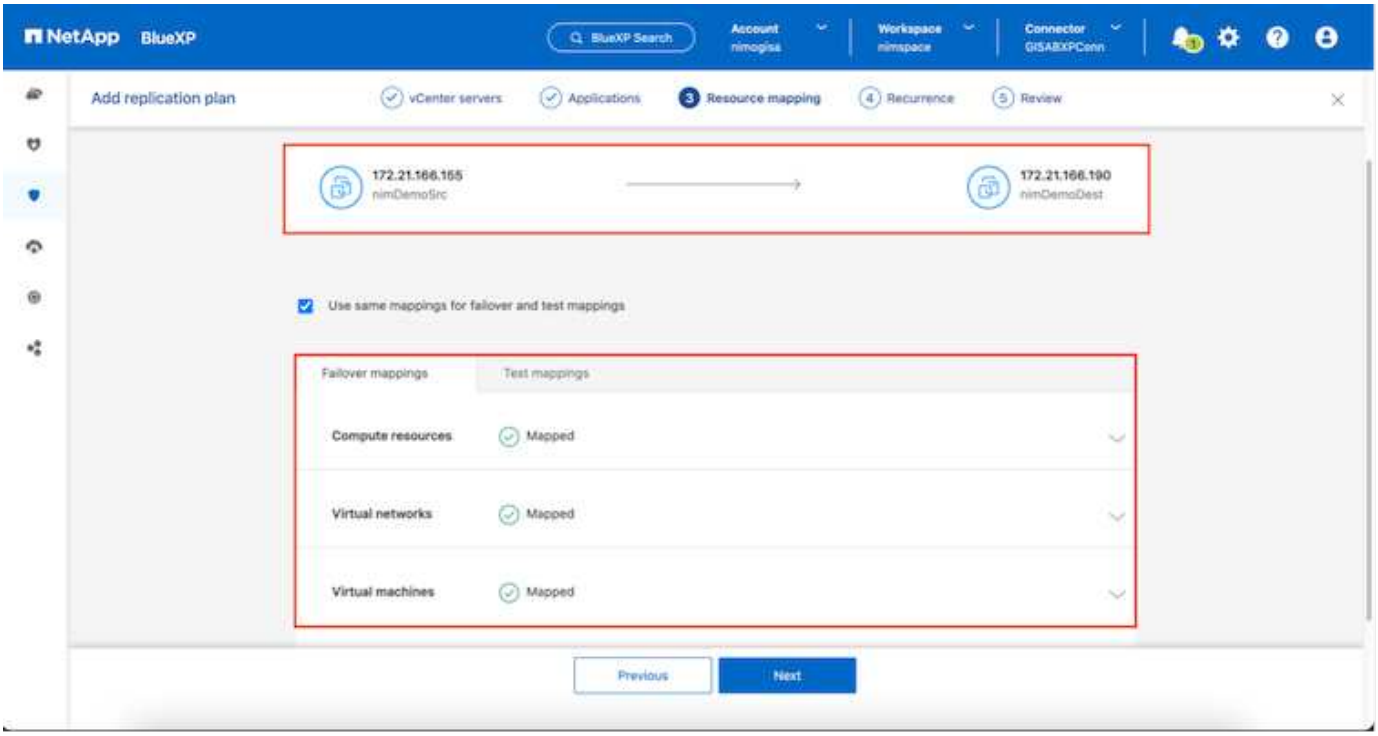
选择资源组后，创建故障转移映射。在此步骤中，指定源环境的资源如何映射到目标。这包括计算资源、虚拟网络。IP 定制、前置和后置脚本、启动延迟、应用程序一致性等。有关详细信息，请参阅 "创建复制计划"。



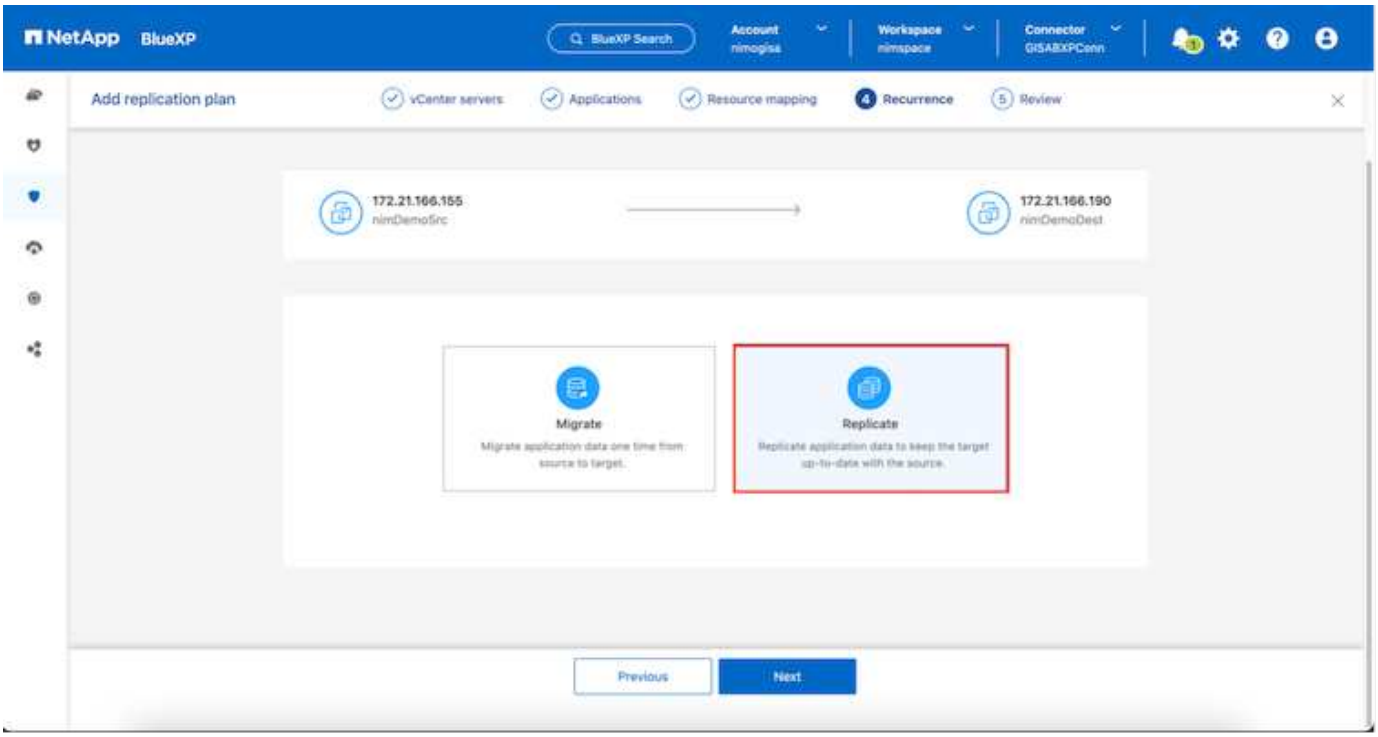
默认情况下，测试和故障转移操作使用相同的映射参数。要对测试环境应用不同的映射，请取消选中复选框后选择测试映射选项，如下所示：



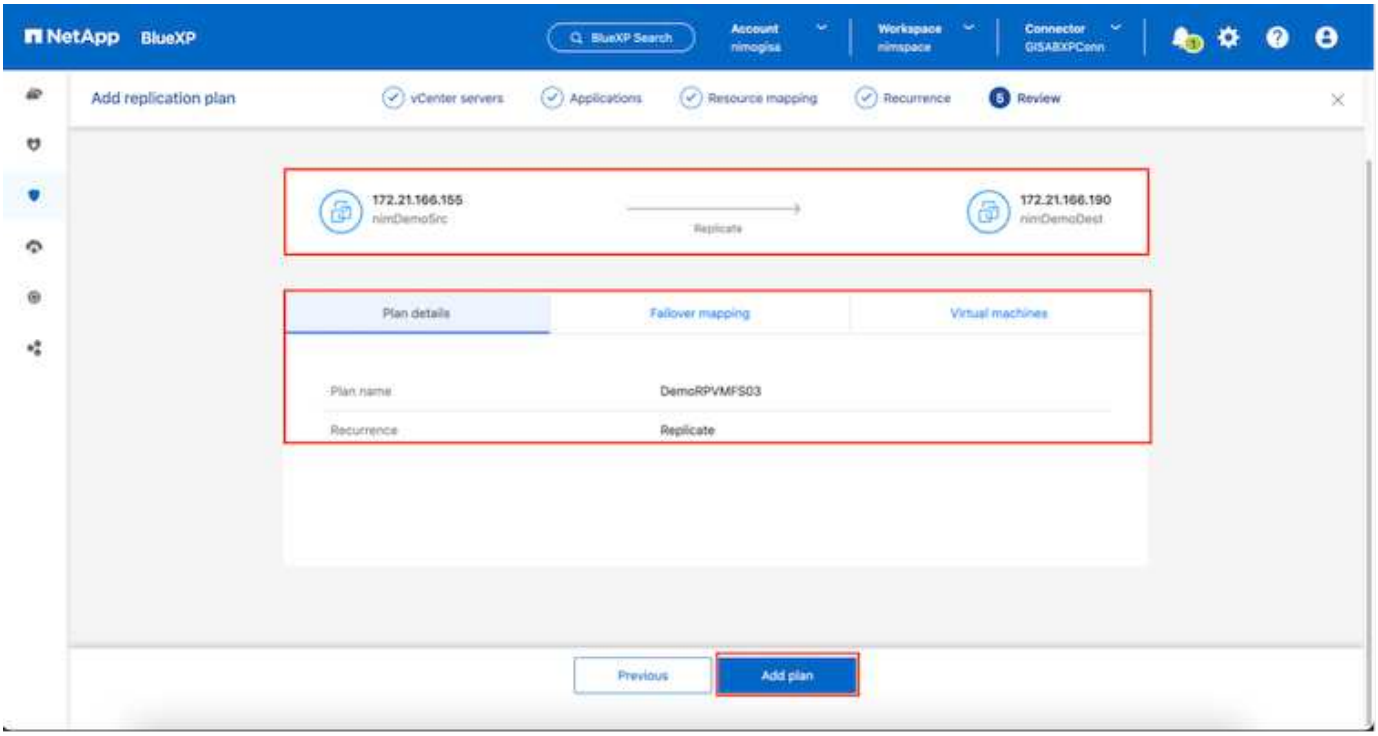
资源映射完成后，单击下一步。

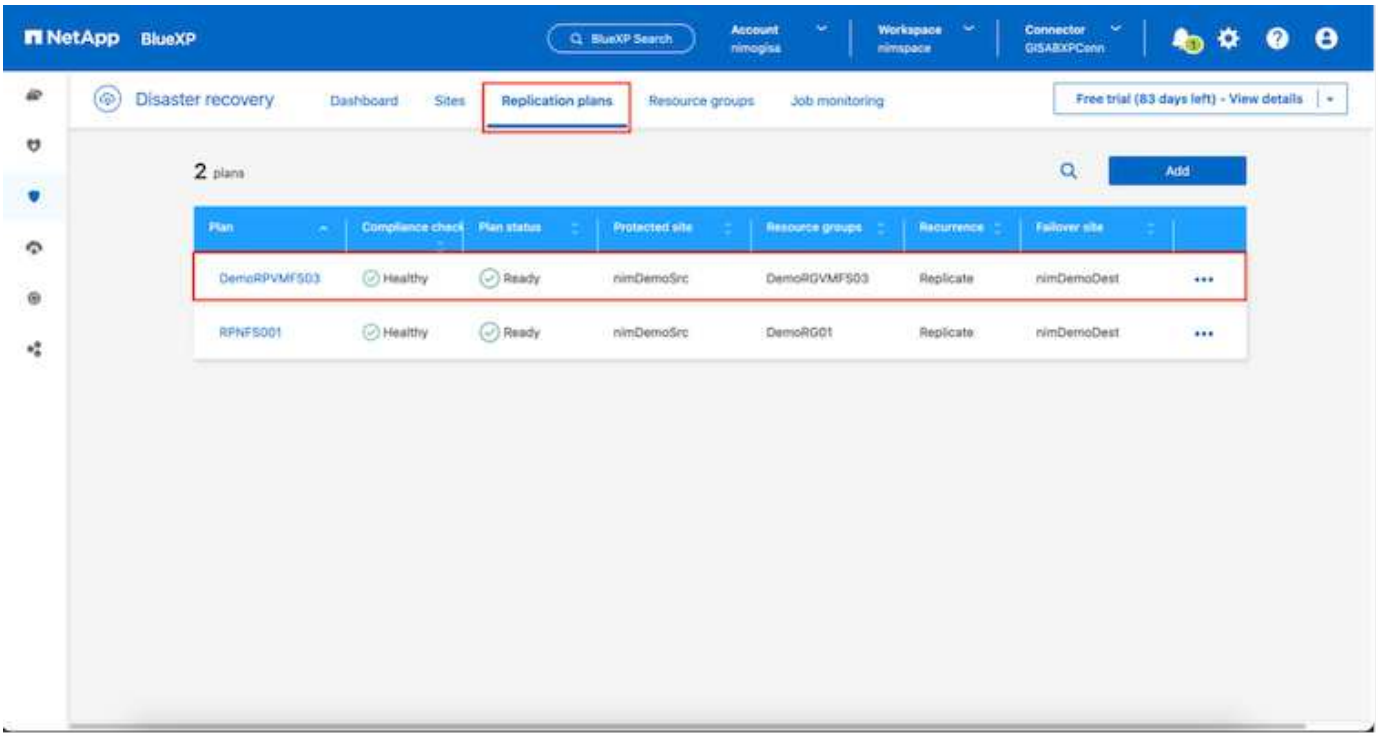


选择重复类型。简单来说，选择迁移（使用故障转移的一次性迁移）或重复连续复制选项。在本演练中，选择了“复制”选项。

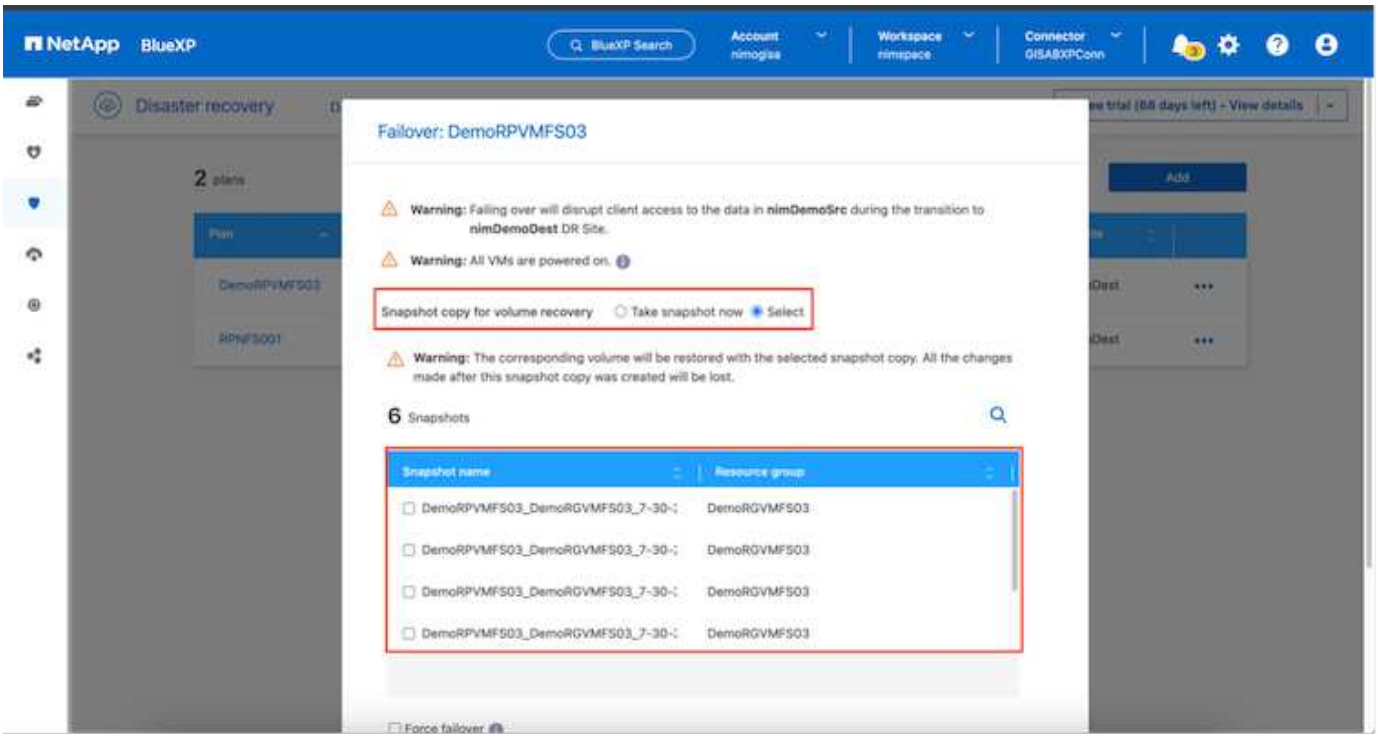


完成后，检查创建的映射，然后单击添加计划。

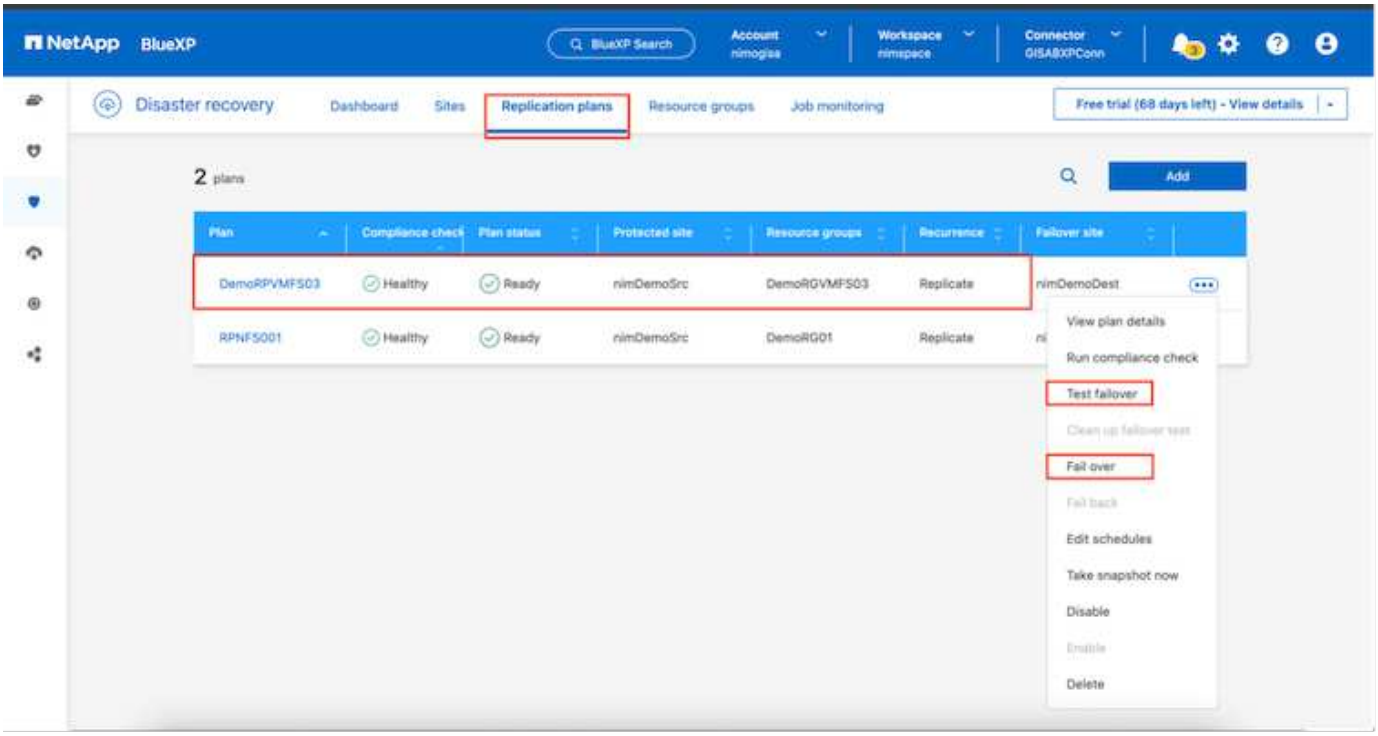




创建复制计划后，可以根据要求通过选择故障转移选项、测试故障转移选项或迁移选项来执行故障转移。灾难恢复可确保每 30 分钟根据计划执行一次复制过程。在故障转移和测试故障转移选项期间，您可以使用最新的 SnapMirror Snapshot 副本，也可以从时间点 Snapshot 副本中选择特定的 Snapshot 副本（根据 SnapMirror 的保留策略）。如果发生勒索软件等损坏事件，并且最新的副本已被破坏或加密，则时间点选项非常有用。灾难恢复显示所有可用的恢复点。



要使用复制计划中指定的配置触发故障转移或测试故障转移，请单击“故障转移”或“测试故障转移”。

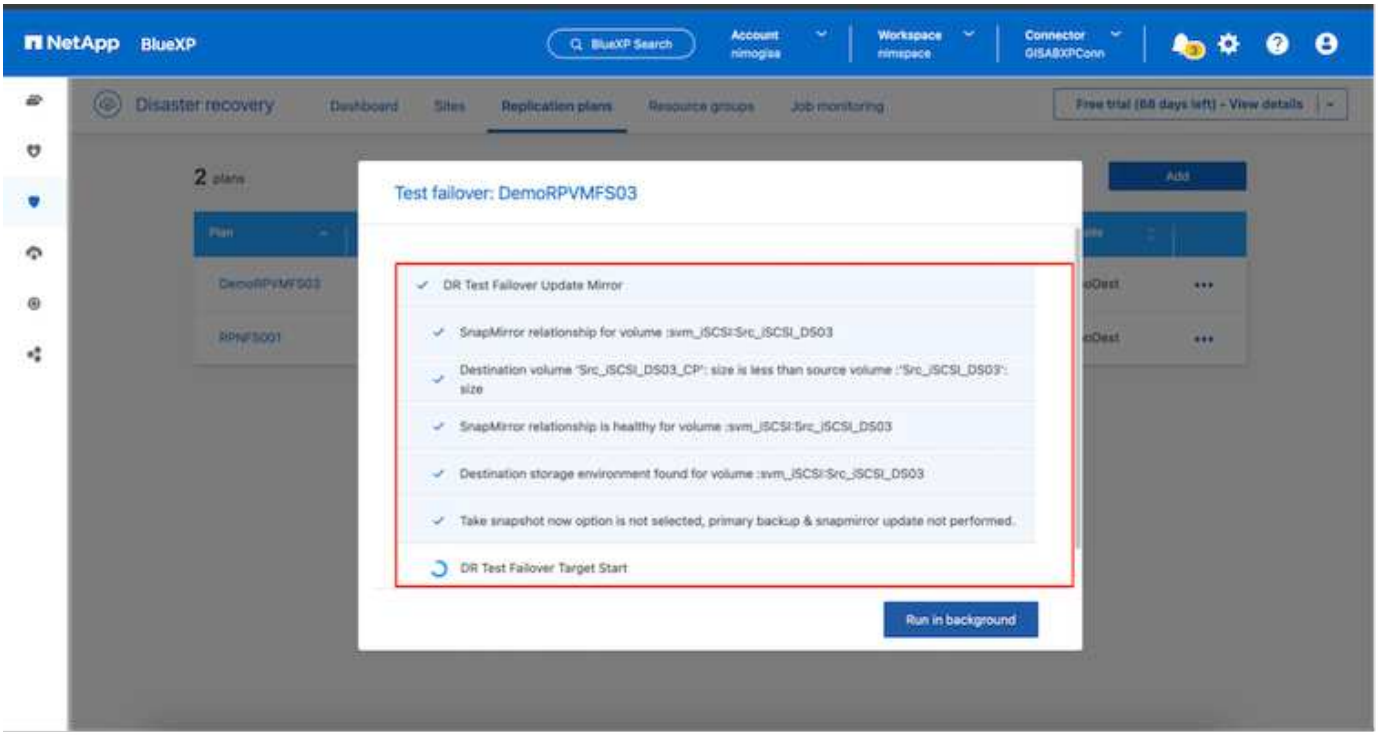


故障转移或测试故障转移操作期间会发生什么？

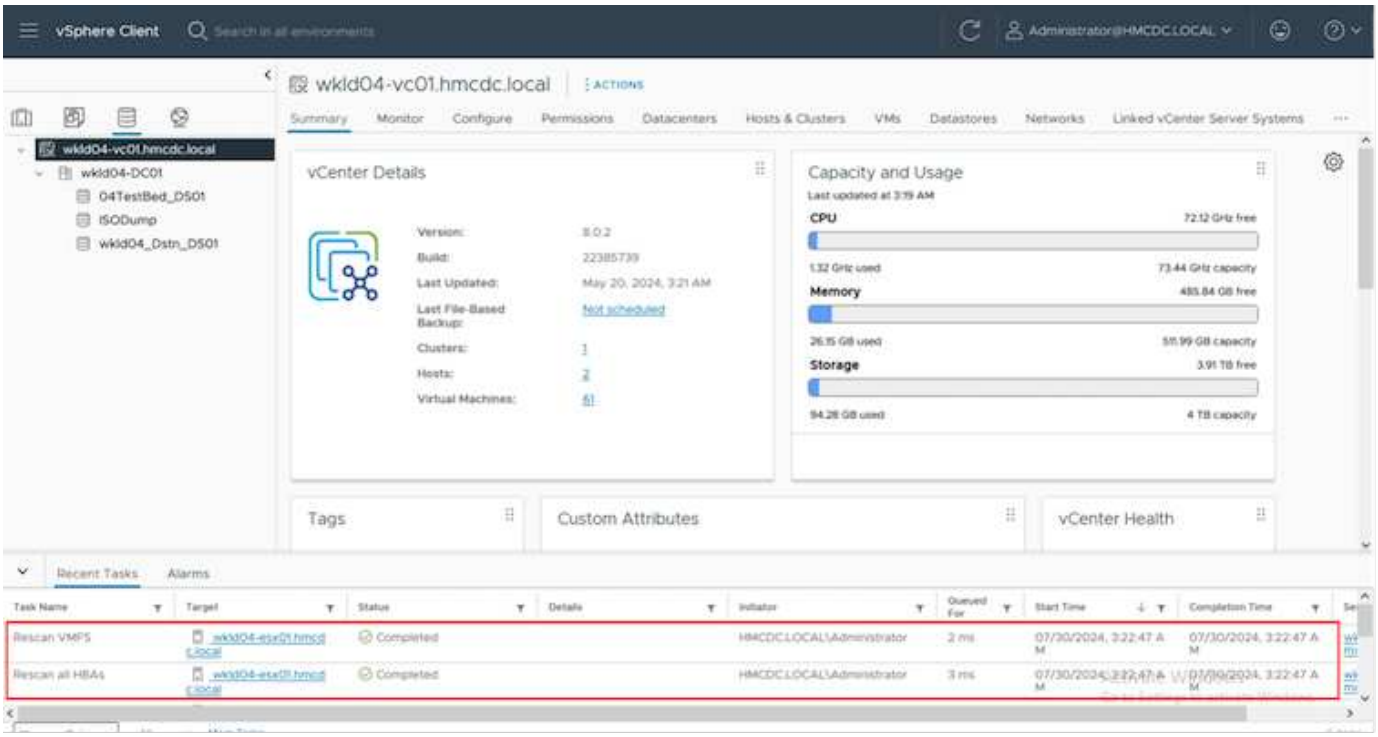
在测试故障转移操作期间，灾难恢复将使用最新的快照副本或目标卷的选定快照，在目标 ONTAP 存储系统上创建一个 FlexClone 卷。

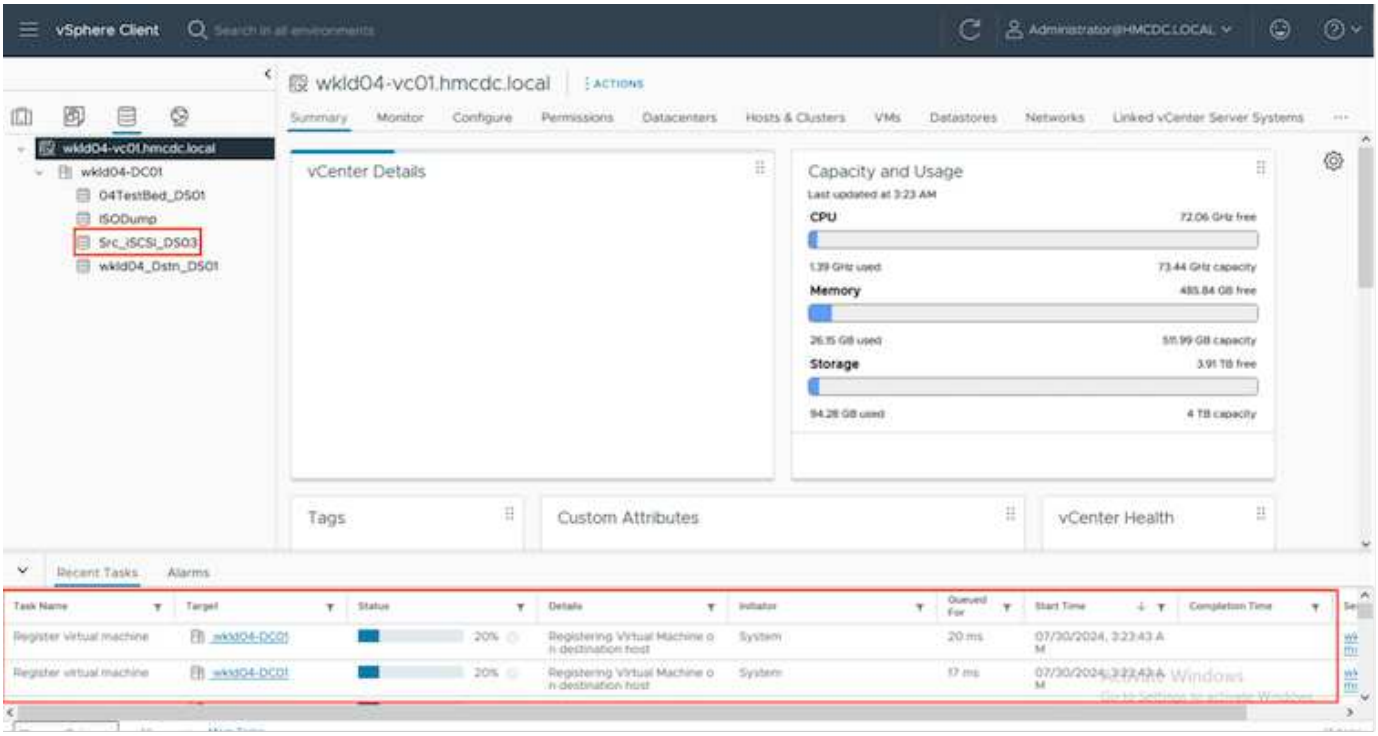
测试故障转移操作会在目标ONTAP存储系统上创建克隆卷。

运行测试恢复操作不会影响SnapMirror复制。



在此过程中，灾难恢复不会映射原始目标卷。相反，它会从选定的快照创建一个新的 FlexClone 卷，并将支持该 FlexClone 卷的临时数据存储映射到 ESXi 主机。



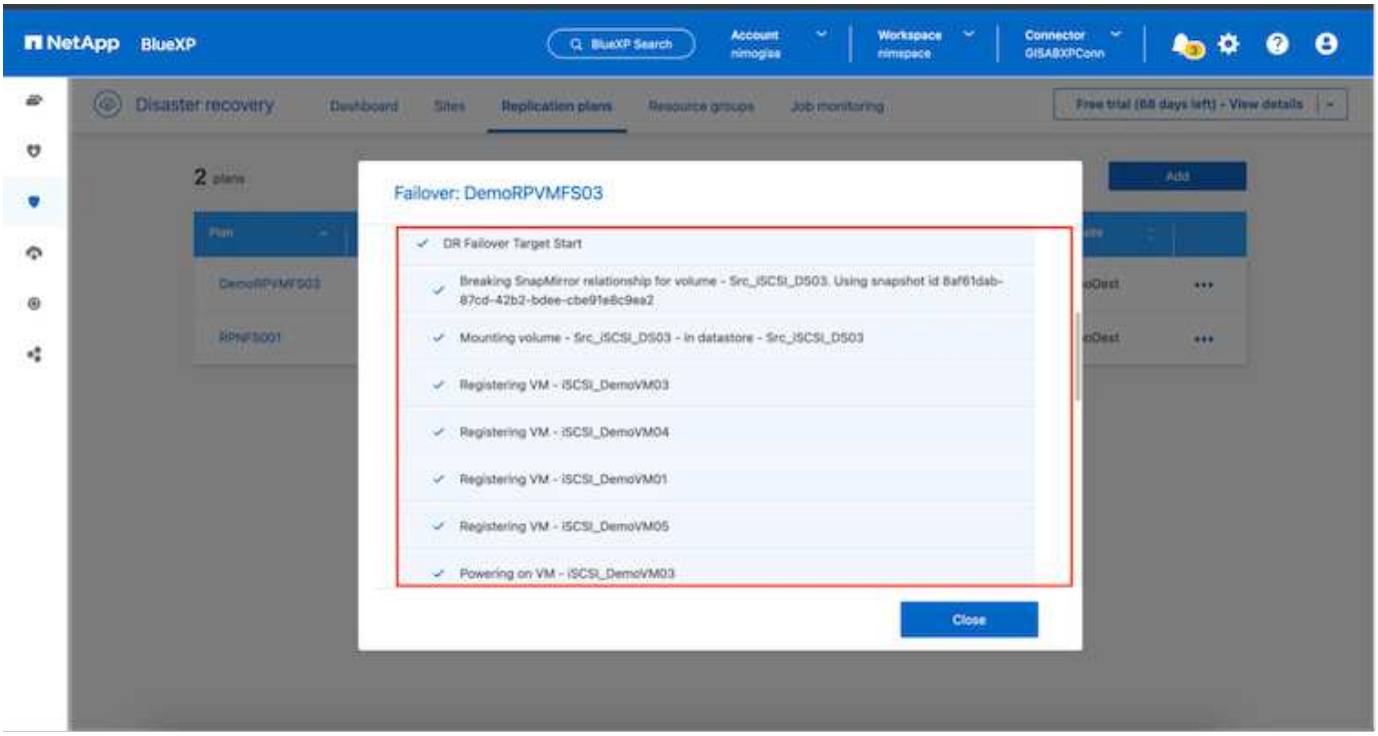


当测试故障转移操作完成时，可以使用 "清理故障转移测试" 触发清理操作。在此操作期间，灾难恢复会销毁此操作中使用的 FlexClone 卷。

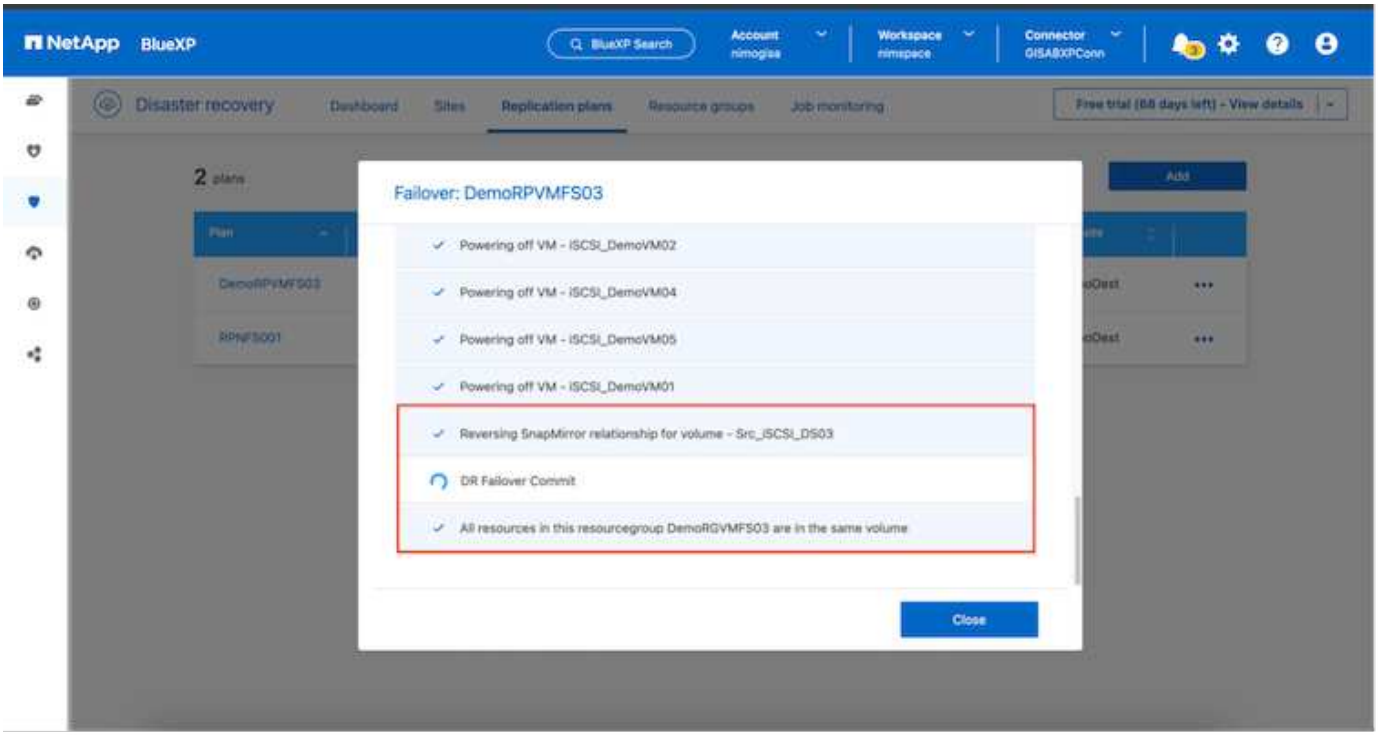
如果发生真正的灾难事件，Disaster Recovery 将执行以下步骤：

1. 中断站点之间的SnapMirror关系。

2. 重新签名后挂载 VMFS 数据存储卷以供立即使用。
3. 注册虚拟机
4. 启动虚拟机



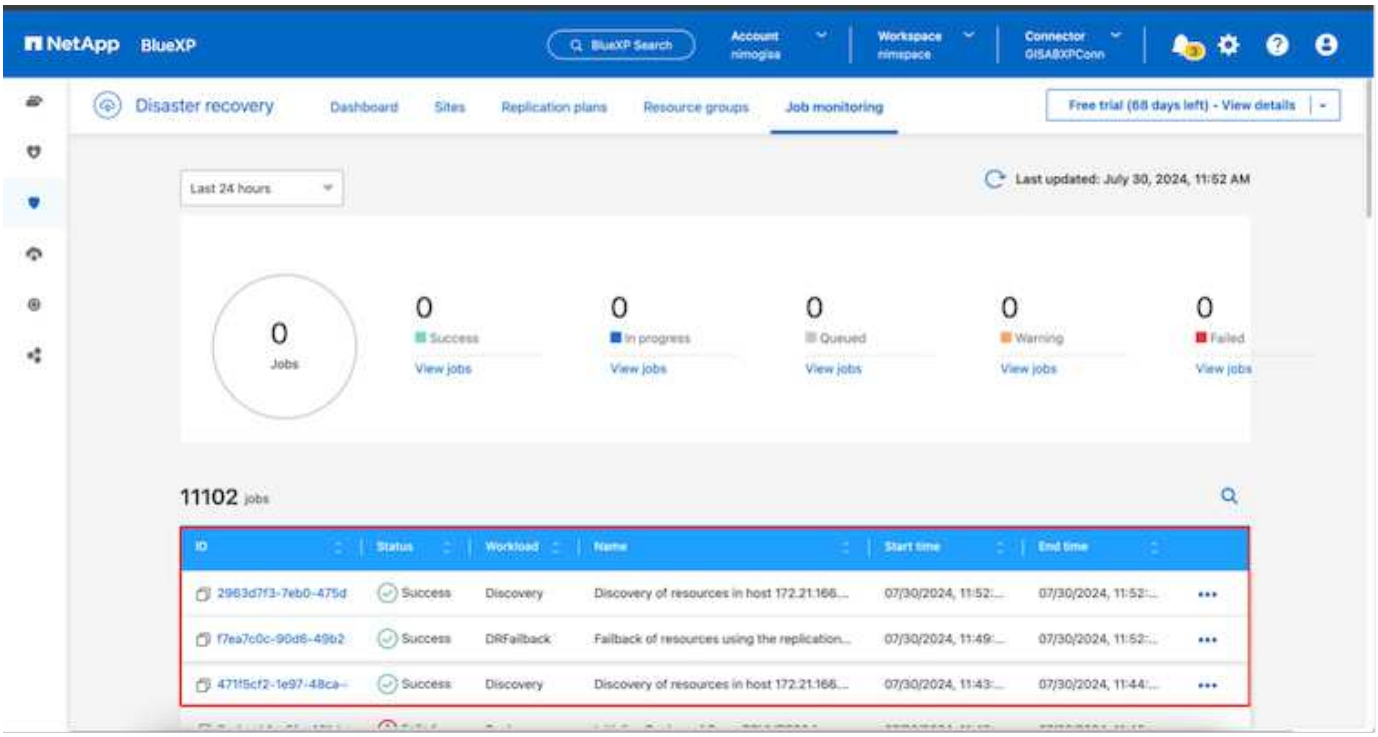
主站点启动并运行后，灾难恢复将为 SnapMirror 启用反向重新同步并启用故障恢复，同样只需单击按钮即可执行此操作。



如果选择迁移选项，则它将被视为计划内的故障转移事件。在这种情况下，将触发额外的步骤，即关闭源站点的

虚拟机。其余步骤与故障转移事件相同。

从控制台或 ONTAP 命令行界面中，您可以监控相应数据存储卷的复制健康状态，并且可以通过作业监控跟踪故障切换或测试故障切换的状态。



这为处理量身定制的灾难恢复计划提供了强大的解决方案。当发生灾难并决定激活 DR 站点时，可以按计划进行故障转移或单击按钮进行故障转移。

要了解有关此过程的更多信息，请随意观看详细的演示视频或使用"解决方案模拟器"。

NetApp混合多云与 Red Hat OpenShift 容器工作负载

开始使用

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

NetApp发现，越来越多的客户正在对其传统企业应用程序进行现代化改造，并使用围绕 Kubernetes 构建的容器和编排平台来构建新的应用程序。 Red Hat OpenShift Container Platform 就是我们看到许多客户采用的一个例子。

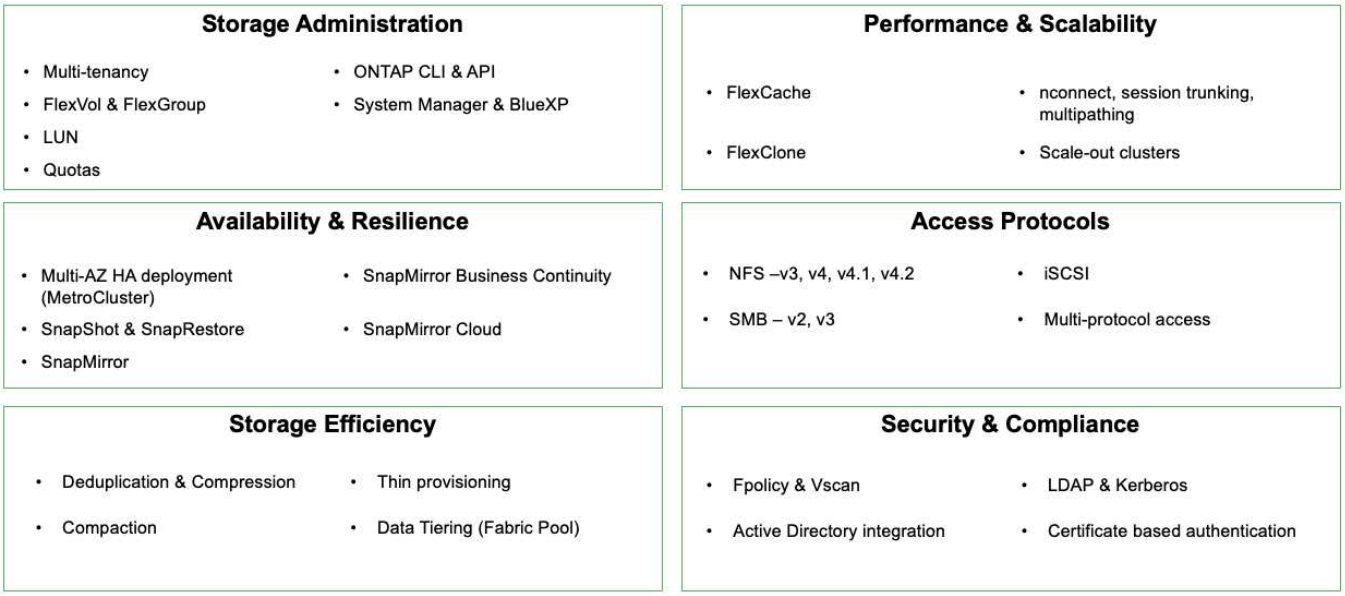
概述

随着越来越多的客户开始在其企业内采用容器， NetApp完全有能力帮助满足其有状态应用程序的持久存储需求以及数据保护、数据安全和数据迁移等经典数据管理需求。然而，这些需求可以通过不同的策略、工具和方法来满足。

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

- 本地自我管理存储：
  - NetApp光纤连接存储 (FAS)、 NetApp全闪存FAS阵列 (AFF)、 NetApp全 SAN 阵列 (ASA) 和ONTAP Select
- 本地提供商管理的存储：
  - NetApp Keystone提供存储即服务 (STaaS)
- 云端自我管理存储：
  - NetApp Cloud Volumes ONTAP（CVO）在超大规模数据中心中提供自管理存储
- 云中的提供商管理存储：
  - Amazon FSx for NetApp ONTAP、 Azure NetApp Files和Google Cloud NetApp Volumes在云中提供基于文件的存储。

ONTAP feature highlights

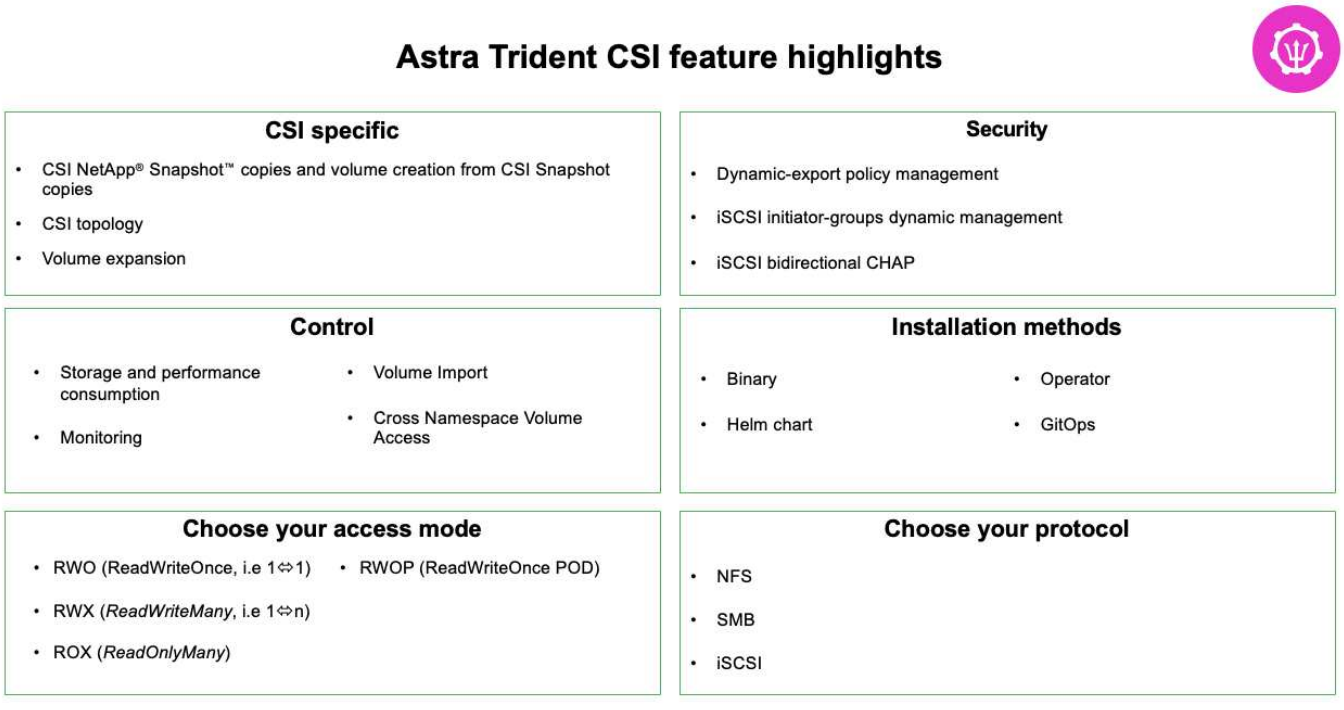


NetApp Console 使您能够从单一控制平面/界面管理所有存储和数据资产。

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

- NetApp Trident** 是一款符合 CSI 标准的存储编排器，可以快速轻松地使用由上述各种NetApp存储选项支持的持久存储。它是由NetApp维护和支持的开源软件。

Astra Trident CSI feature highlights



业务关键型容器工作负载需要的不仅仅是持久卷。他们的数据管理要求也需要保护和迁移应用程序 Kubernetes 对象。

应用程序数据除了用户数据之外，还包括 kubernetes 对象：以下是一些示例： - kubernetes 对象，例如 pod 规范、PVC、部署、服务 - 自定义配置对象，例如配置映射和机密 - 持久数据，例如 Snapshot 副本、备份、克隆 - 自定义资源，例如 CR 和 CRD

NetApp Trident Protect，作为 NetApp Trident 的免费附加组件，提供先进的应用程序数据管理功能，增强由 NetApp ONTAP 存储系统支持的有状态 Kubernetes 应用程序的功能和可用性。Trident Protect 简化了跨公共云和本地环境的容器化工作负载的管理、保护和移动。它还通过其 API 和 CLI 提供强大的自动化功能。

该参考文档提供了使用Trident Protect 在 RedHat OpenShift 平台上部署的基于容器的应用程序的数据保护验证。此外，该解决方案还提供了有关部署和使用 Red Hat Advanced Cluster Management (ACM) 管理容器平台的高级详细信息。该文档还重点介绍了使用Trident CSI 配置器将NetApp存储与 Red Hat OpenShift 容器平台集成的细节。

NetApp混合多云解决方案针对 Red Hat OpenShift 容器工作负载的价值主张

大多数客户不会在没有任何现有基础设施的情况下开始构建基于 Kubernetes 的环境。也许他们是一家传统的 IT 商店，在虚拟机上运行大多数企业应用程序（例如在大型 VMware 环境中）。然后，他们开始构建基于小型容器的环境来满足现代应用程序开发团队的需求。这些举措通常从小处开始，随着团队学习这些新技术和技能并开始认识到采用它们的诸多好处，它们开始变得更加普遍。对于客户来说，好消息是NetApp可以满足这两种环境的需求。这套采用 Red Hat OpenShift 的混合多云解决方案将使NetApp客户能够采用现代云技术和服务，而无需彻底改造其整个基础设施和组织。无论客户应用程序和数据托管在本地、云端、虚拟机上运行还是容器上， NetApp都能提供一致的数据管理、保护、安全性和可移植性。借助这些新解决方案， NetApp数十年来在本地数据中心环境中提供的相同价值将在整个企业数据范围内提供，而无需进行大量投资来重新装备、获取新技能或组建新团队。无论客户处于云之旅的哪个阶段， NetApp都能够帮助客户解决这些业务挑战。

NetApp混合多云与 Red Hat Openshift：

- 为客户提供经过验证的设计和实践，展示客户在使用基于NetApp 的Red Hat OpenShift 存储解决方案时管理、保护、保护和迁移其数据和应用程序的最佳方法。
- 为在 VMware 环境、裸机基础架构或两者结合中运行 Red Hat OpenShift 和NetApp存储的客户提供最佳实践。
- 展示本地和云环境以及两者混合环境的策略和选项。

NetApp混合多云支持 Red Hat OpenShift 容器工作负载的解决方案

该解决方案使用 OpenShift 容器平台（OCP）、OpenShift 高级集群管理器（ACM）、NetApp ONTAP、NetApp Console 和 NetApp Trident Protect 测试和验证迁移和集中式数据保护。

对于此解决方案， NetApp已测试并验证了以下场景。该解决方案根据以下特点分为多个场景：

- 本地
- cloud
  - 自我管理的 OpenShift 集群和自我管理的NetApp存储

- 提供商管理的 OpenShift 集群和提供商管理的NetApp存储

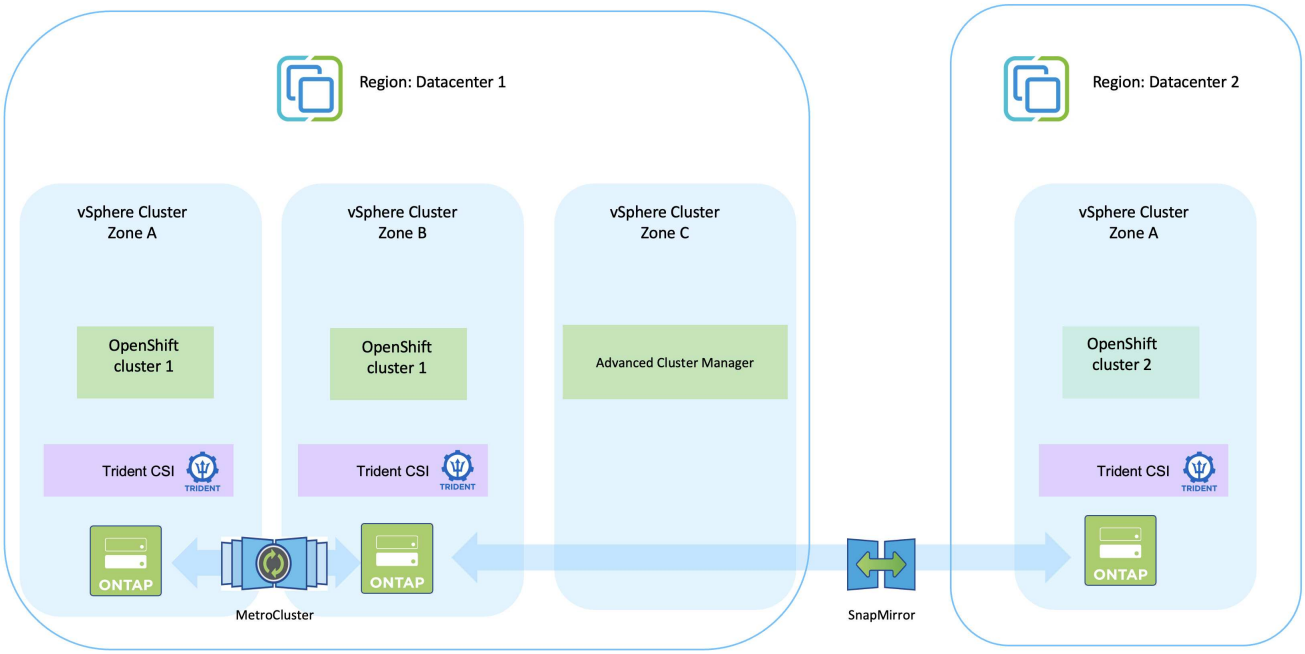
我们将在未来构建更多解决方案和用例。

场景 **1**：使用**Trident Protect** 在本地环境中进行数据保护和迁移

本地：自我管理的 **OpenShift** 集群和自我管理的**NetApp**存储

- 使用 Trident Protect 保护应用程序并支持本地集群之间的迁移。

场景 **1**

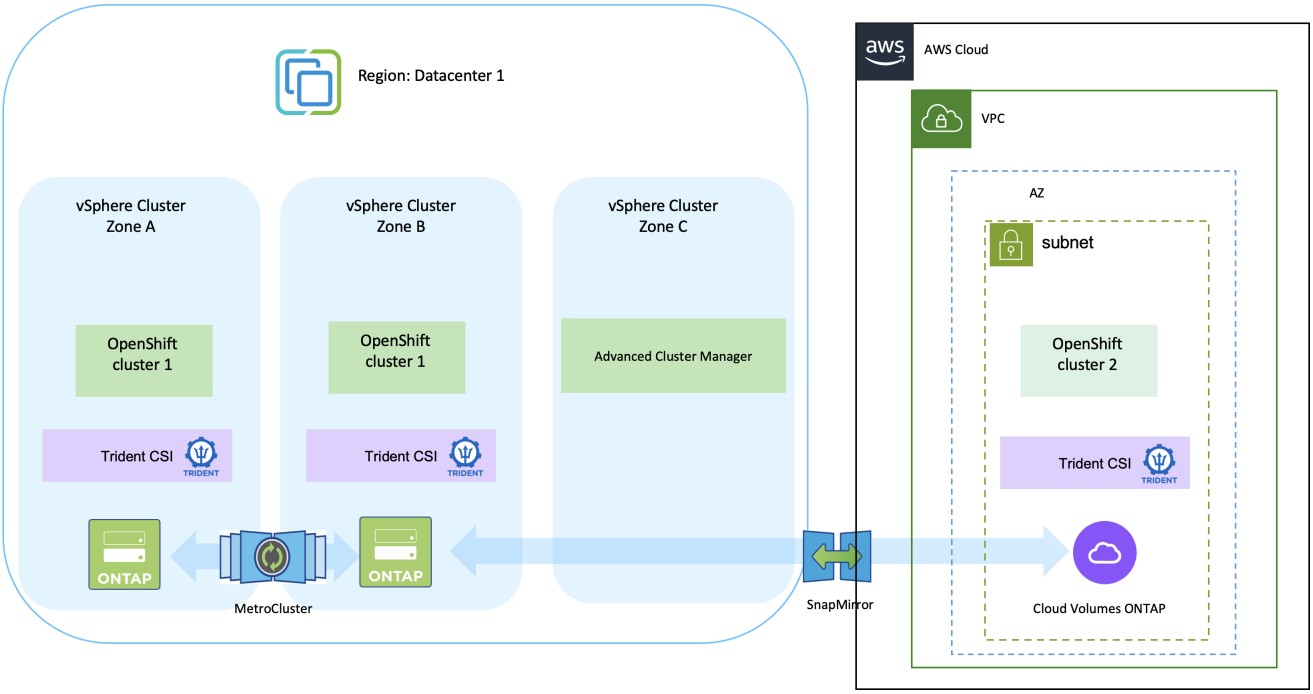


场景 **2**：使用**Trident Protect** 进行数据保护以及从本地环境到 **AWS** 环境的迁移

本地：自管理 **OpenShift** 集群和自管理存储 **AWS** 云：自管理 **OpenShift** 集群和自管理存储

- 使用 Trident Protect 保护应用程序，并支持本地集群和 AWS 中自管理 OpenShift 集群之间的迁移。

场景 **2**

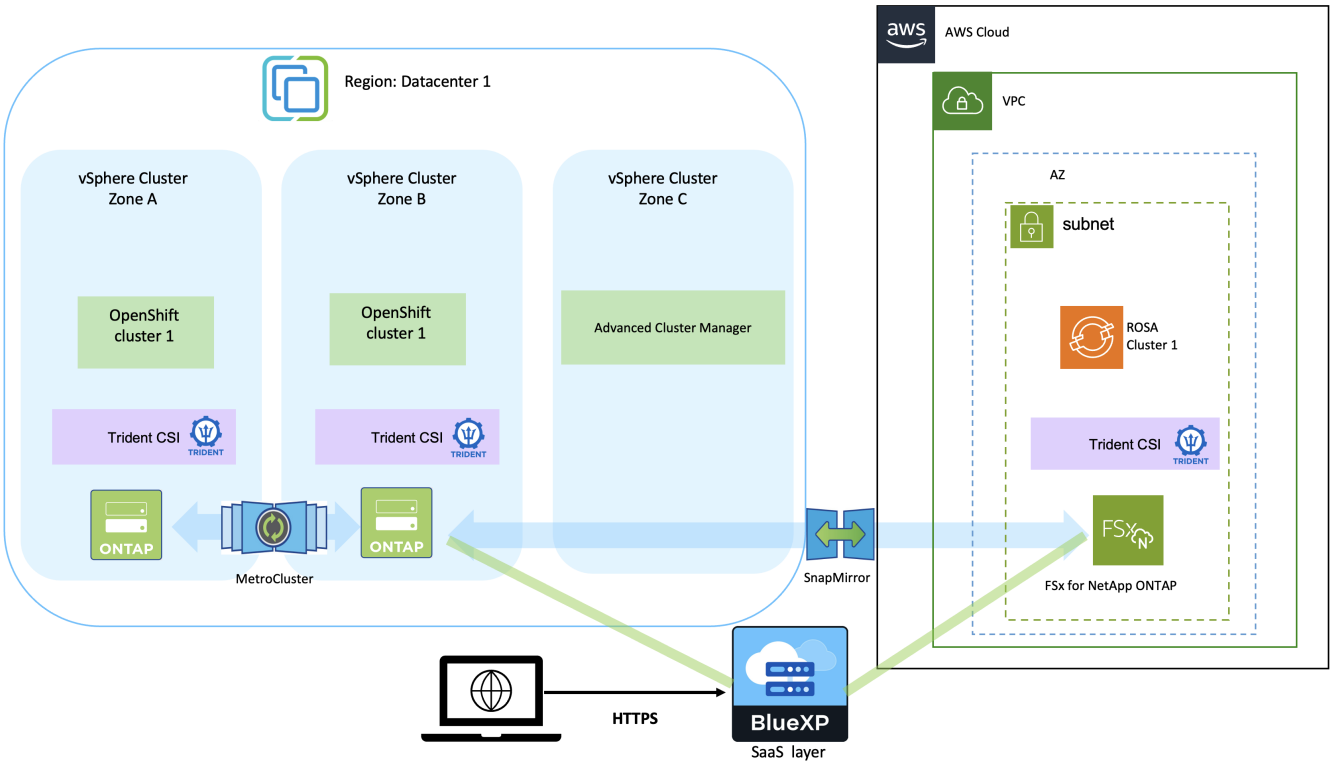


场景 **3**：数据保护以及从本地环境到 **AWS** 环境的迁移

本地：自管理 **OpenShift** 集群和自管理存储 **AWS** 云：提供商管理的 **OpenShift** 集群 **(ROSA)** 和提供商管理的存储 **(FSx ONTAP)**

- 使用 NetApp Console，执行持久卷（FSx ONTAP）的复制。
- 使用 OpenShift GitOps 重新创建应用程序元数据。

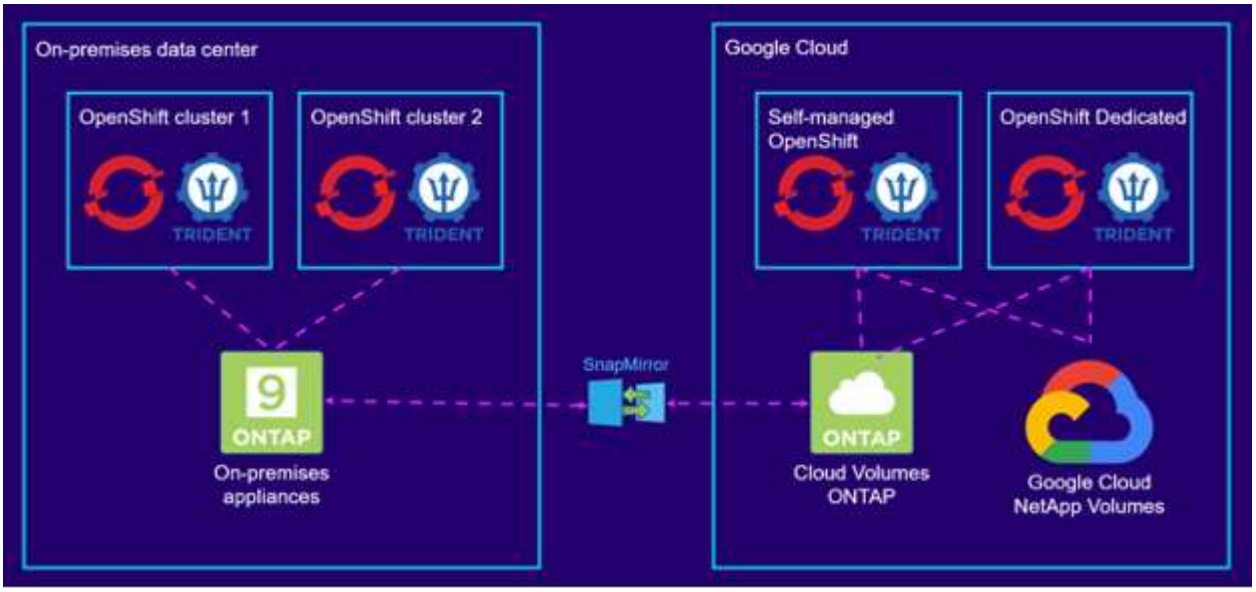
场景 **3**



场景 4：使用**Trident Protect** 进行数据保护以及从本地环境到 **GCP** 环境的迁移

本地：自管理 **OpenShift** 集群和自管理存储 **Google Cloud**：自管理 **OpenShift** 集群和自管理存储

- 使用 Trident Protect 保护应用程序，并支持本地集群和 Google Cloud OpenShift 集群之间的迁移。

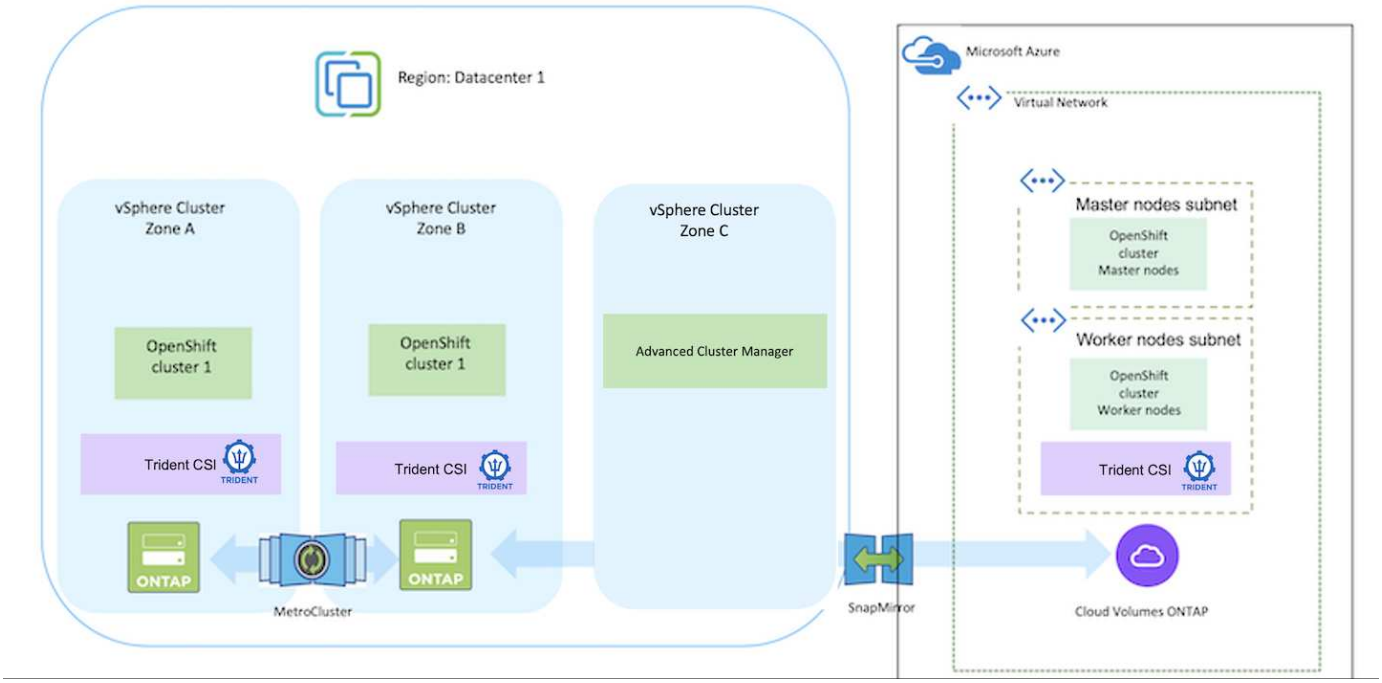


有关在MetroCluster配置中使用ONTAP时的注意事项，请参阅"此处"。

场景 5：使用**Trident Protect** 进行数据保护以及从本地环境到 **Azure** 环境的迁移

本地：自管理 **OpenShift** 集群和自管理存储 **Azure** 云：自管理 **OpenShift** 集群和自管理存储

- 使用 Trident Protect 保护应用程序并支持本地和 Azure 中的 OpenShift 集群之间的迁移。



有关在MetroCluster配置中使用ONTAP时的注意事项，请参阅"此处"。

解决方案验证中使用的各种组件的版本

该解决方案使用 OpenShift 容器平台、OpenShift Advanced Cluster Manager、 NetApp ONTAP和NetApp Trident Protect 测试并验证迁移和集中数据保护。

解决方案的场景 1、2 和 3 使用下表所示的版本进行验证：

成分	版本
VMware	vSphere Client 版本 8.0.0.10200 VMware ESXi，8.0.0，20842819
枢纽集群	OpenShift 4.11.34
源集群和目标集群	OpenShift 4.12.9 本地和 AWS
NetApp Trident	Trident服务器和客户端 23.04.0
* NetApp Trident保护*	Trident Protect 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1
AWS FSx ONTAP	单个 AZ

解决方案的场景 4 使用下表所示的版本进行了验证：

成分	版本
VMware	vSphere Client 版本 8.0.2.00000 VMware ESXi，8.0.2，22380479

枢纽集群	OpenShift 4.13.13
源集群和目标集群	OpenShift 4.13.12 本地和 Google Cloud 中
NetApp Trident	Trident服务器和客户端 23.07.0
NetApp ONTAP	ONTAP 9.12.1
* Cloud Volumes ONTAP*	单可用区，单节点，9.14.0

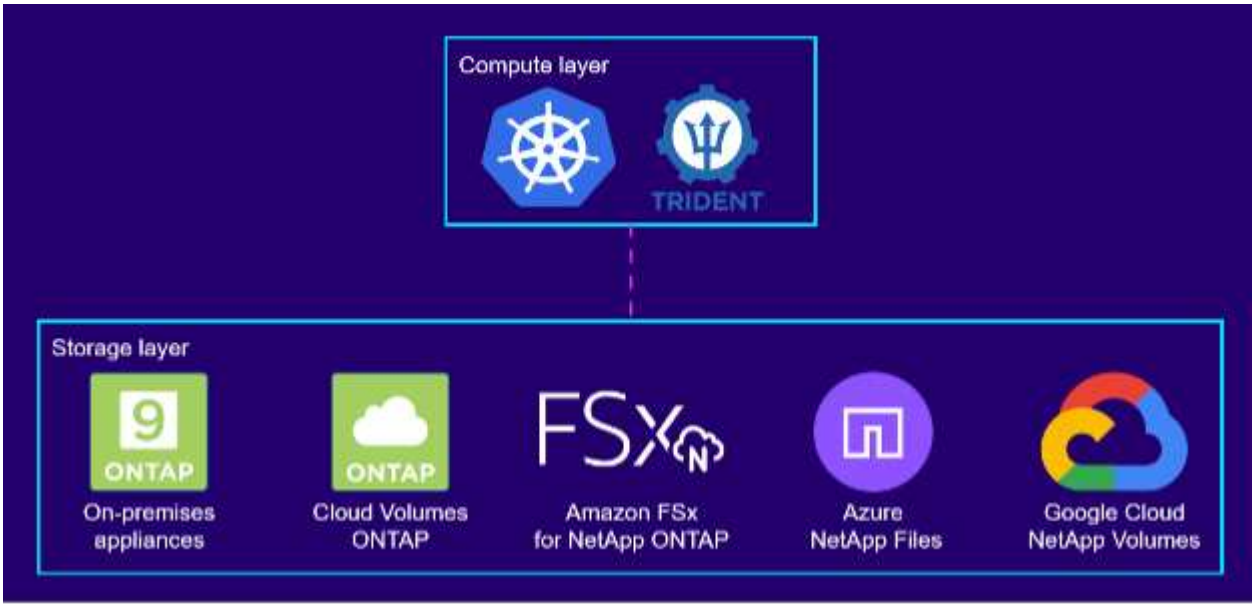
解决方案的场景 5 使用下表所示的版本进行了验证：

成分	版本
VMware	vSphere Client 版本 8.0.2.00000 VMware ESXi，8.0.2，22380479
源集群和目标集群	OpenShift 4.13.25 本地和 Azure
NetApp Trident	Trident Server 和 Client 23.10.0
* NetApp Trident保护*	Trident Protect 23.10
NetApp ONTAP	ONTAP 9.12.1
* Cloud Volumes ONTAP*	单可用区，单节点，9.14.0

支持**NetApp Storage** 与 **Red Hat OpenShift Containers** 的集成

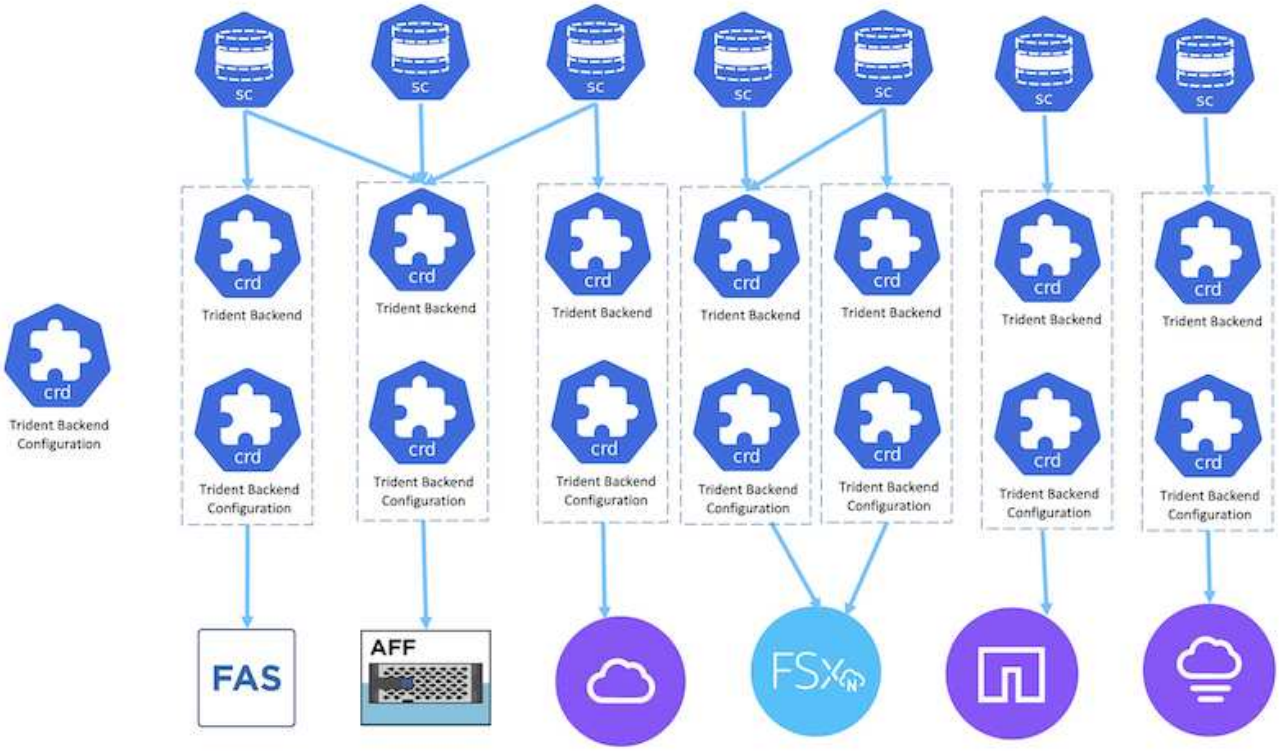
无论 Red Hat OpenShift 容器是在 VMware 上运行还是在超大规模环境中运行， NetApp Trident都可以用作其支持的各种类型的后端NetApp存储的 CSI 配置器。

下图描述了可使用NetApp Trident与 OpenShift 集群集成的各种后端NetApp存储。



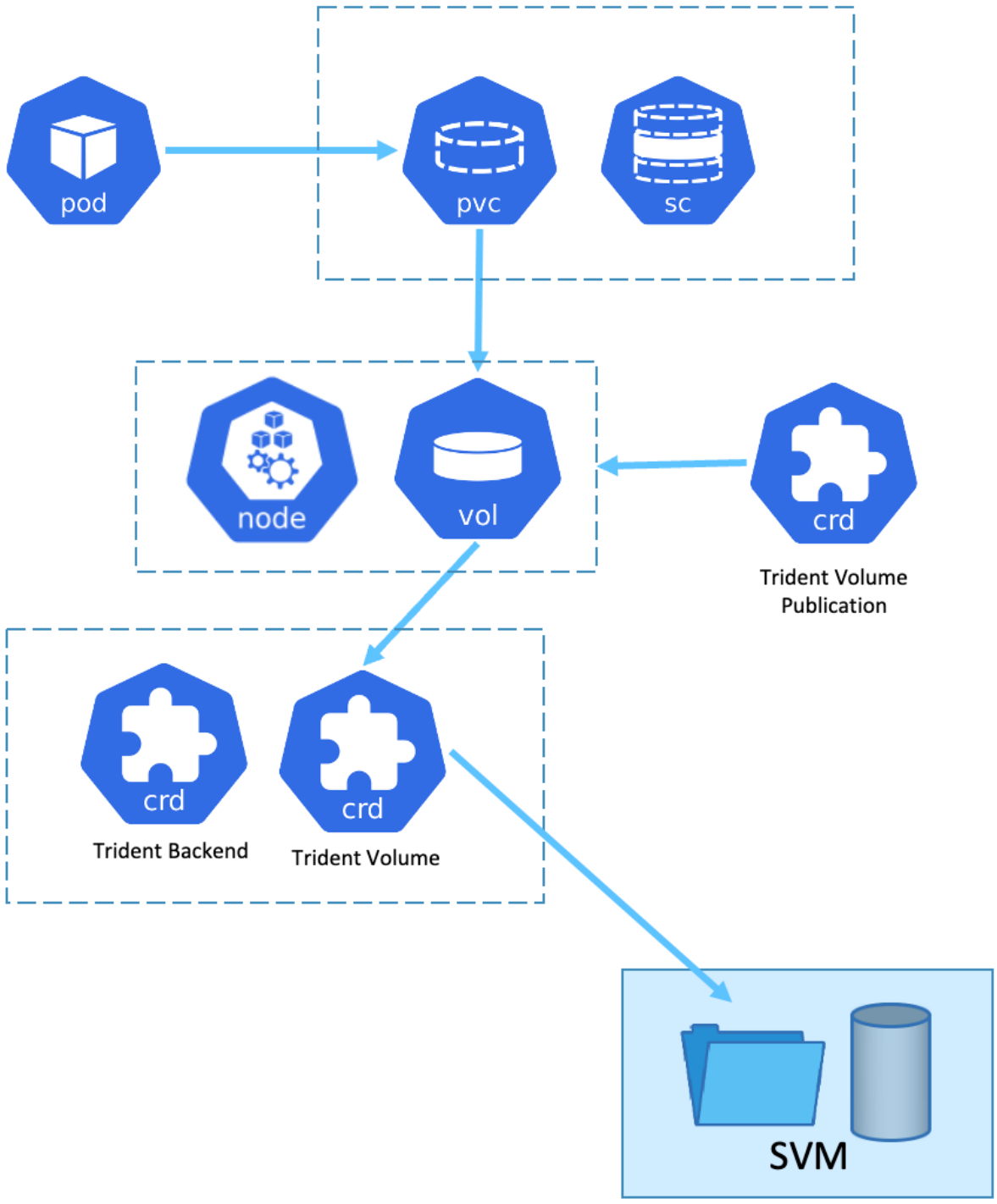
ONTAP存储虚拟机 (SVM) 提供安全的多租户。单个 OpenShift 集群可以连接到单个 SVM 或多个 SVM，甚至多个ONTAP集群。存储类根据参数或标签过滤后端存储。存储管理员使用 trident 后端配置定义连接到存储系统的参数。成功建立连接后，它会创建 trident 后端并填充存储类可以过滤的信息。

storageclass和backend的关系如下图所示。



应用程序所有者请求使用存储类的持久卷。存储类过滤后端存储。

pod与后端存储的关系如下图所示。



容器存储接口 **(CSI)** 选项

在 vSphere 环境中，客户可以选择 VMware CSI 驱动程序和/或Trident CSI 与ONTAP集成。使用 VMware CSI 时，持久卷将作为本地 SCSI 磁盘使用，而使用Trident时，它将与网络一起使用。

由于 VMware CSI 不支持ONTAP的 RWX 访问模式，因此如果需要 RWX 模式，应用程序需要使用Trident CSI。对于基于 FC 的部署，VMware CSI 是首选，而SnapMirror业务连续性 (SMBC) 可提供区域级别的高可用性。

VMware CSI 支持

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

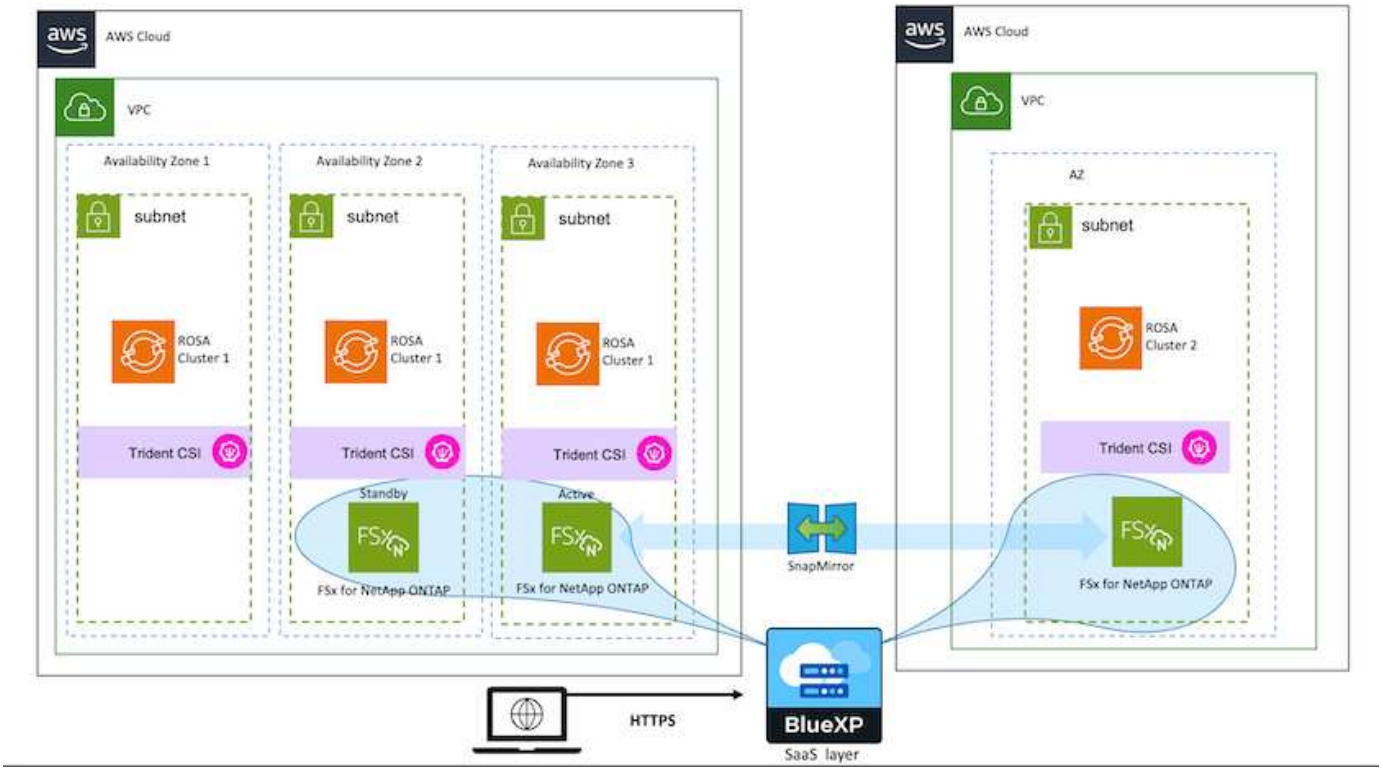
Trident有以下驱动程序支持ONTAP

- ontap-san（专用卷）
- ontap-san-economy（共享卷）
- ontap-nas（专用卷）
- ontap-nas-economy（共享卷）
- ontap-nas-flexgroup（专用大规模卷）

对于 VMware CSI 和Trident CSI， ONTAP支持 NFS 的 nconnect、会话中继、kerberos 等以及块协议的多路径、chap 身份验证等。

在 AWS 中， Amazon FSx for NetApp ONTAP （FSx ONTAP）可以部署在单个可用区（AZ）或多可用区中。对于需要高可用性的生产工作负载，与单可用区相比，多可用区提供区域级容错能力并具有更好的 NVMe 读取缓存。欲了解更多信息，请查看"AWS 性能指南"。

为了节省灾难恢复站点的成本，可以使用单 AZ FSx ONTAP
。



有关 FSx ONTAP支持的 SVM 数量，请参阅"管理 FSx ONTAP存储虚拟机"

其他文档

以下是一些可供参考的附加文档：

1. "VMware vSphere"
2. "OpenShift Container 平台产品文档"
3. "安装 OpenShift 容器平台集群"
4. "高级集群管理产品文档"
5. "使用 ACM 创建集群"
6. "在 OpenShift 上部署 Red Hat Quay"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda" - Verda（开源）为流行的云原生数据密集型应用程序提供了一系列参考执行挂钩
10. "NetApp 数据服务"
11. "AWS 上的 Red Hat OpenShift Service 经典架构"
12. "Amazon FSx ONTAP"
13. "在 GCP 上安装 OpenShift 集群"
14. "在 Azure 上安装 OpenShift 集群"

Openshift 适用于本地

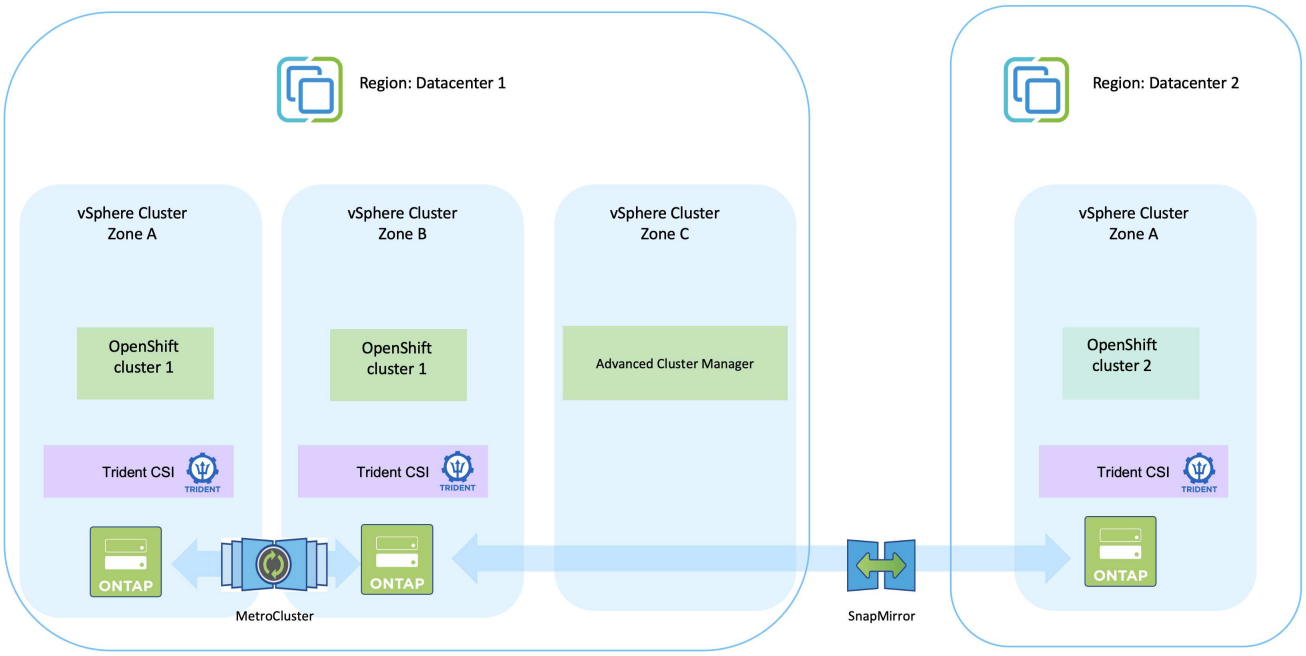
NetApp解决方案与 VMware 上的 Red Hat OpenShift Container 平台工作负载

如果客户需要在其私有数据中心的基础设施上运行现代容器化应用程序，他们可以这样做。他们应该规划和部署 Red Hat OpenShift 容器平台 (OCP)，以便成功构建可用于生产的环境来部署他们的容器工作负载。他们的 OCP 集群可以部署在 VMware 或裸机上。

NetApp ONTAP存储为容器部署提供数据保护、可靠性和灵活性。 Trident作为动态存储配置器，为客户的有状态应用程序使用持久性ONTAP存储。 NetApp Trident Protect 可用于满足有状态应用程序的多种数据管理需求，例如数据保护、迁移和业务连续性。

借助 VMware vSphere， NetApp ONTAP工具提供了可用于配置数据存储区的 vCenter 插件。应用标签并将其与 OpenShift 一起使用来存储节点配置和数据。基于 NVMe 的存储提供更低的延迟和高性能。

使用**Trident Protect** 为 **OpenShift Container** 工作负载提供数据保护和迁移解决方案

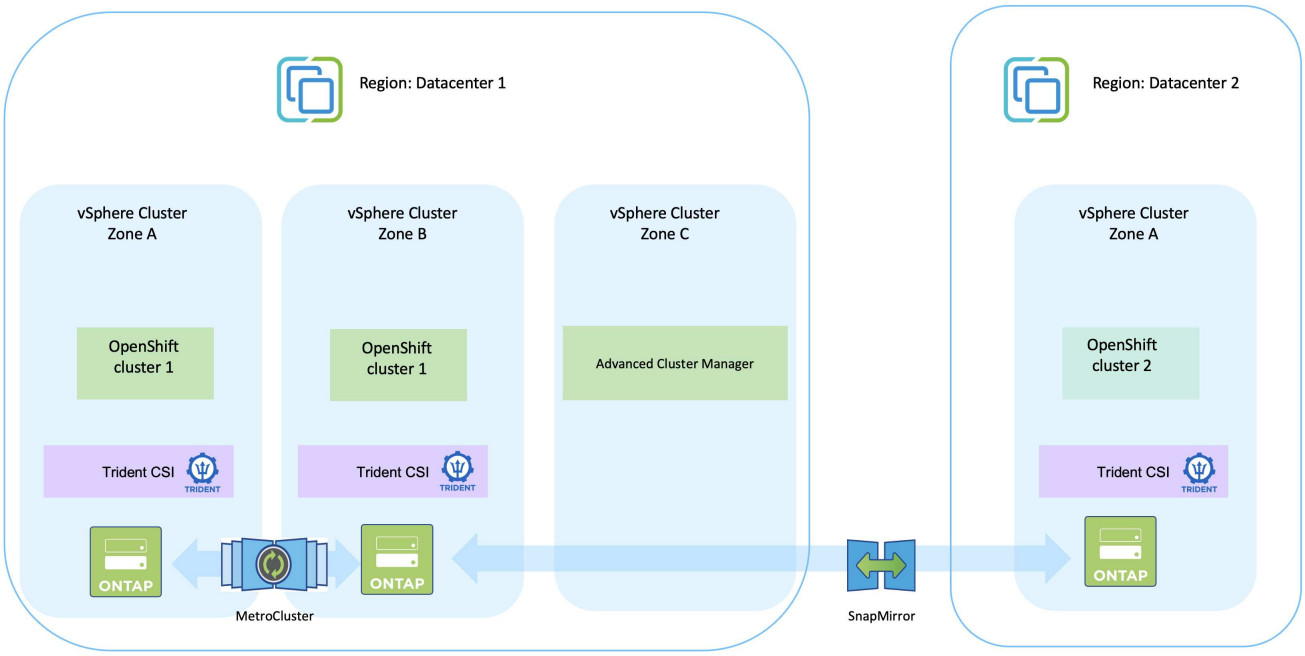


在 **VMware** 上部署和配置 **Red Hat OpenShift Container** 平台

本节介绍了如何设置和管理 OpenShift 集群以及管理其上的有状态应用程序的高级工作流程。它展示了如何使用NetApp ONTAP存储阵列借助Trident来提供持久卷。

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

下面是描述数据中心内 VMware 上部署的集群的图表。



设置过程可分为以下步骤：

▼ 部署并配置 **CentOS VM**

- 它部署在VMware vSphere环境中。
- 该虚拟机用于为解决方案部署一些组件，例如NetApp Trident和NetApp Trident Protect。
- 安装期间，此虚拟机上配置了一个 root 用户。

▼ 在 **VMware vSphere**（**Hub Cluster**）上部署和配置 **OpenShift Container Platform** 集群

请参阅有关部署 OCP 集群的 "协助部署" 方法的说明。

请记住以下内容： - 创建 ssh 公钥和私钥以提供给安装程序。如果需要，这些密钥将用于登录主节点和工作节点。 - 从辅助安装程序下载安装程序。该程序用于启动您在 VMware vSphere 环境中为主节点和工作节点创建的虚拟机。 - 虚拟机应具备最低 CPU、内存和硬盘要求。 （请参阅 vm create 命令"这"提供此信息的主节点和工作节点的页面） - 应在所有虚拟机上启用 diskUUID。 - 为 master 创建至少 3 个节点，为 worker 创建至少 3 个节点。 - 一旦安装程序发现它们，请打开 VMware vSphere 集成切换按钮。

▼ 在 **Hub** 集群上安装高级集群管理

这是使用 Hub 集群上的高级集群管理操作员安装的。参考说明"此处"。

▼ 安装两个额外的 **OCP** 集群（源和目标）

- 可以使用 Hub 集群上的 ACM 部署附加集群。
- 请参见说明 "此处"。

▼ 配置**NetApp ONTAP**存储

- 在 VMWare 环境中安装与 OCP VM 连接的ONTAP集群。

- 创建 SVM。
- 配置 NAS 数据生命周期以访问 SVM 中的存储。

▼ 在 **OCP** 集群上安装**NetApp Trident**

- 在所有三个集群上安装NetApp Trident： 中心集群、源集群和目标集群
- 请参见说明 "此处"。
- 为 ontap-nas 创建存储后端。
- 为 ontap-nas 创建存储类。
- 参考说明"此处"。

▼ 在源集群上部署应用程序

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

下一步是使用Trident Protect 进行数据保护和从源集群到目标集群的数据迁移。参考"此处"以获取说明。

使用**Trident Protect** 进行数据保护

本页面展示了在 VMware vSphere 上运行的 Red Hat OpenShift 容器化应用程序使用 Trident Protect 的数据保护选项。

随着用户开始使用 Red Hat OpenShift 对其应用程序进行现代化改造，应制定数据保护策略，以防止意外删除或任何其他人为错误。通常还需要出于监管或合规目的制定保护策略，以保护其数据免受灾难影响。

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

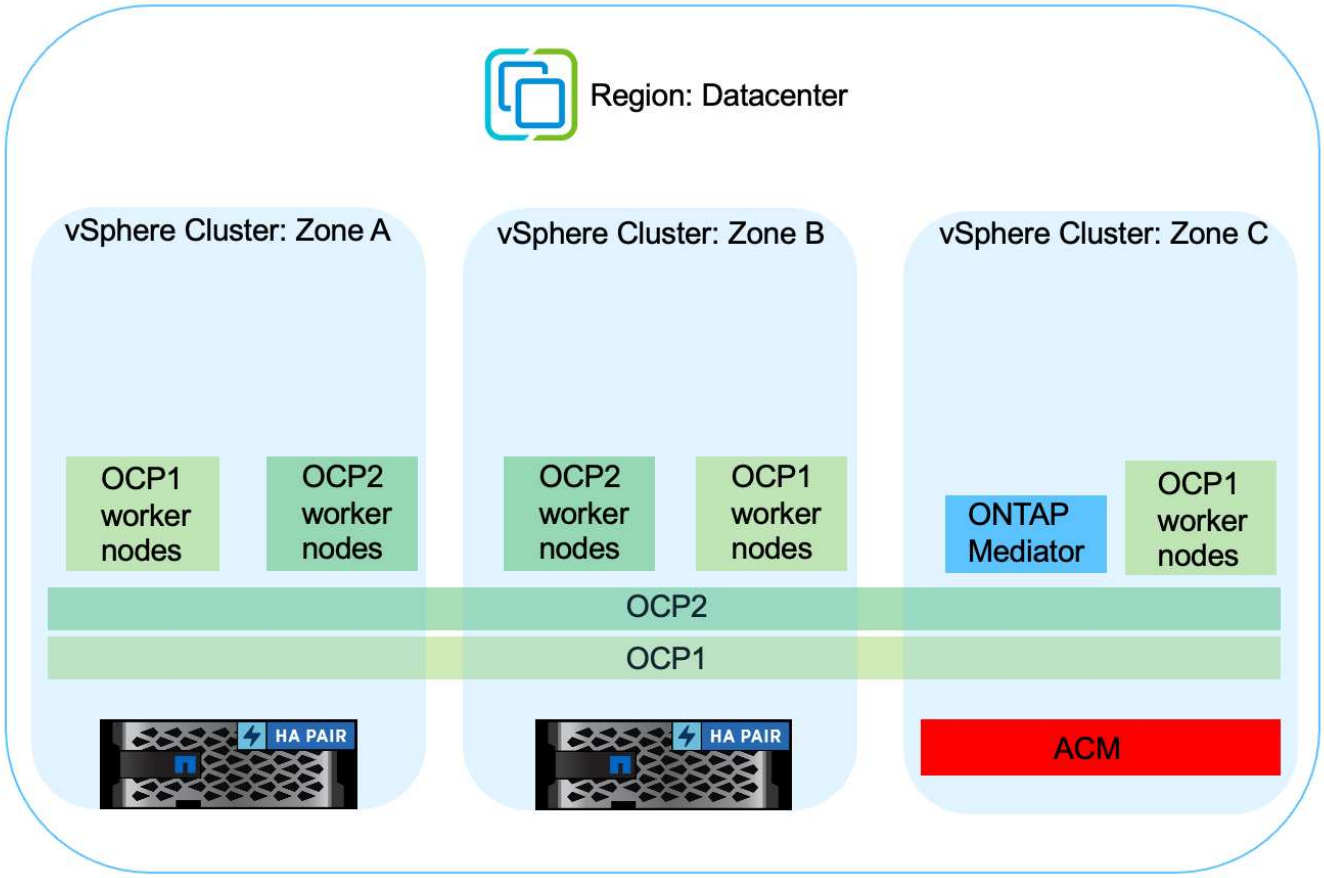
有关使用 Trident Protect 保护和迁移容器工作负载的详细信息，请查看以下部分： - "使用 Trident Protect 保护和迁移容器应用程序"

利用**MetroCluster**实现业务连续性

我们的大多数ONTAP硬件平台都具有高可用性功能，可以防止设备故障，避免执行灾难恢复。但为了防止火灾或任何其他灾难，并以零 RPO 和低 RTO 继续开展业务，通常会使用MetroCluster解决方案。

当前拥有ONTAP系统的客户可以通过在距离限制内添加支持的ONTAP系统来扩展到MetroCluster ，以提供区域级灾难恢复。 Trident，CSI（容器存储接口）支持NetApp ONTAP，ONTAPMetroCluster配置以及其他选项，如Cloud Volumes ONTAP、 Azure NetApp Files、AWS FSx ONTAP等。Trident 为Trident提供了五种存储驱动程序选项，并且所有选项都支持MetroCluster配置。参考"此处"有关Trident支持的ONTAP存储驱动程序的更多详细信息。

MetroCluster解决方案需要第 2 层网络扩展或从两个故障域访问相同网络地址的能力。一旦MetroCluster配置到位，该解决方案对于应用程序所有者来说是透明的，因为MetroCluster svm 中的所有卷都受到保护并获得SyncMirror （零 RPO）的好处。



对于Trident后端配置 (TBC)，使用MetroCluster配置时请勿指定 dataLIF 和 SVM。为 managementLIF 指定 SVM 管理 IP 并使用 vsadmin 角色凭据。

有关 Trident Protect 数据保护功能的详细信息"此处"。

具有自管理组件的混合云

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

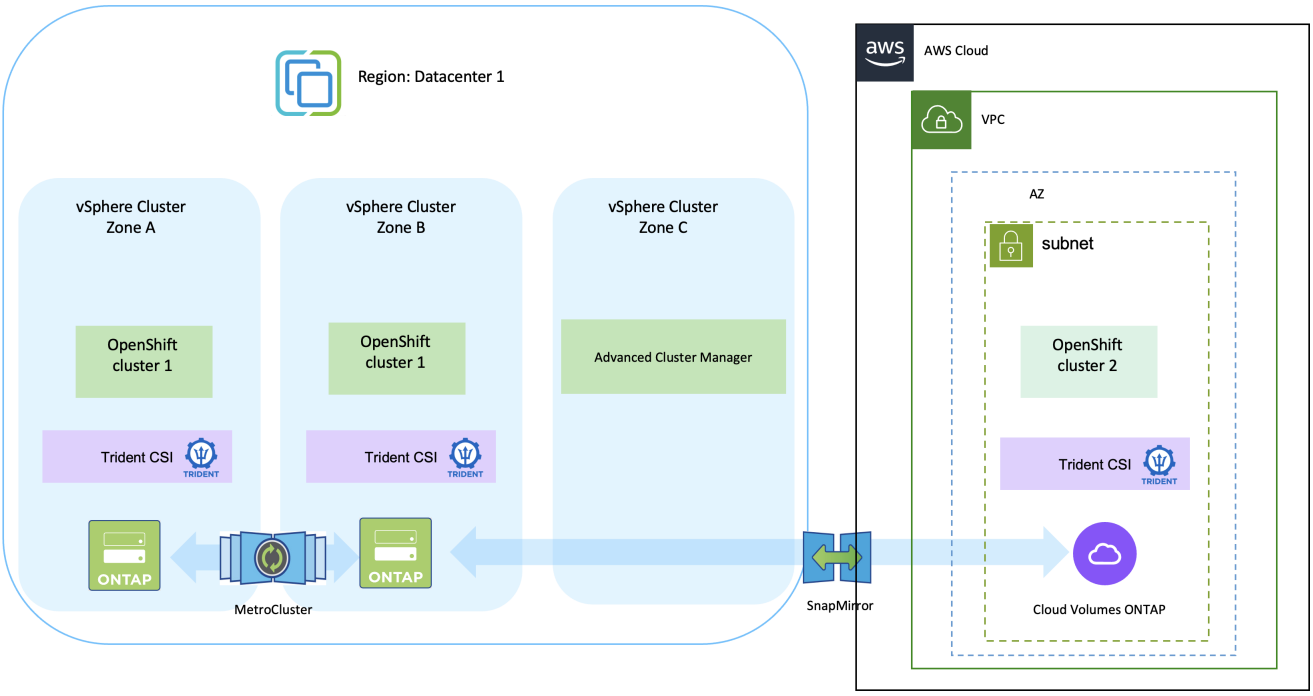
当客户准备将部分选定的工作负载或所有工作负载从数据中心迁移到云端时，他们可能正处于现代化转型的某个阶段。他们可能出于各种原因选择在云中使用自管理的 OpenShift 容器和自管理的NetApp存储。他们应该在云中规划和部署 Red Hat OpenShift 容器平台 (OCP)，以便成功构建一个可用于生产的环境，以便从数据中心迁移容器工作负载。他们的 OCP 集群可以在其数据中心部署在 VMware 或 Bare Metal 上，也可以在云环境中部署在 AWS、Azure 或 Google Cloud 上。

NetApp Cloud Volumes ONTAP 存储为 AWS、Azure 和 Google Cloud 中的容器部署提供数据保护、可靠性和灵活性。Trident 充当动态存储配置程序，为客户的有状态应用程序使用持久的 Cloud Volumes ONTAP 存储。Trident Protect 可用于数据保护、迁移和业务连续性等有状态应用的数据管理要求。

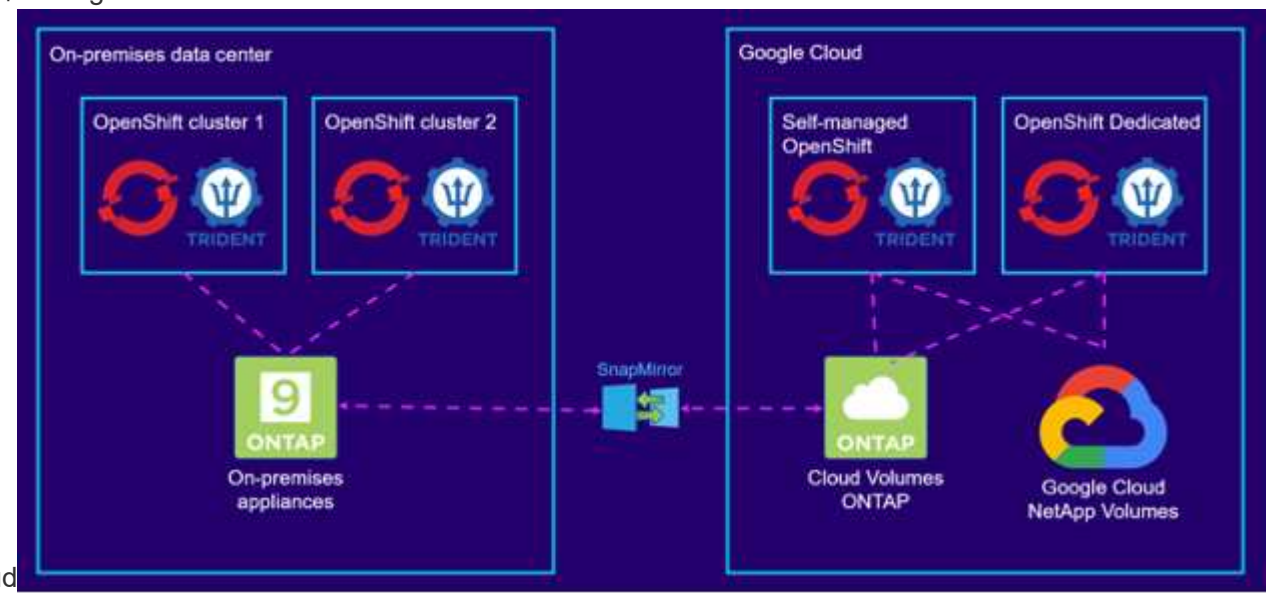
使用**Trident Protect** 为混合云中的 **OpenShift Container** 工作负载提供数据保护和迁移解决方案

本地和

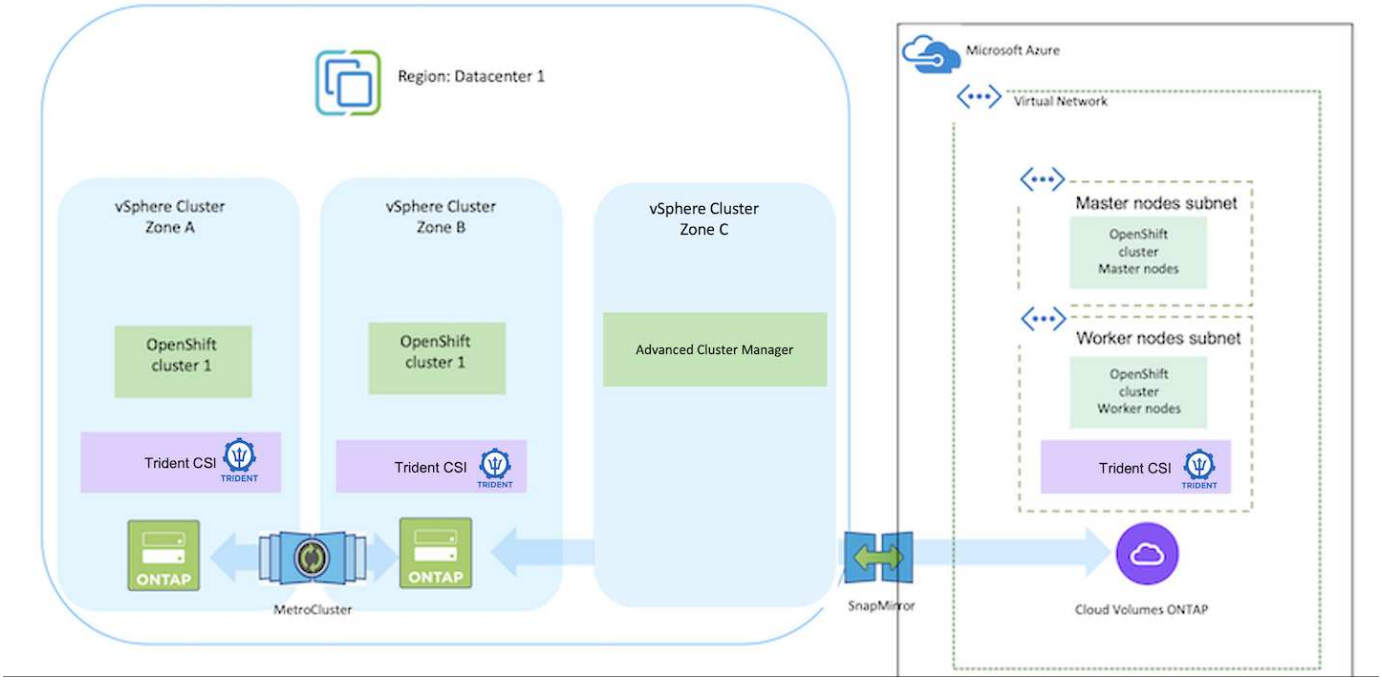
AWS



本地和 Google Cloud



本地和 Azure 云

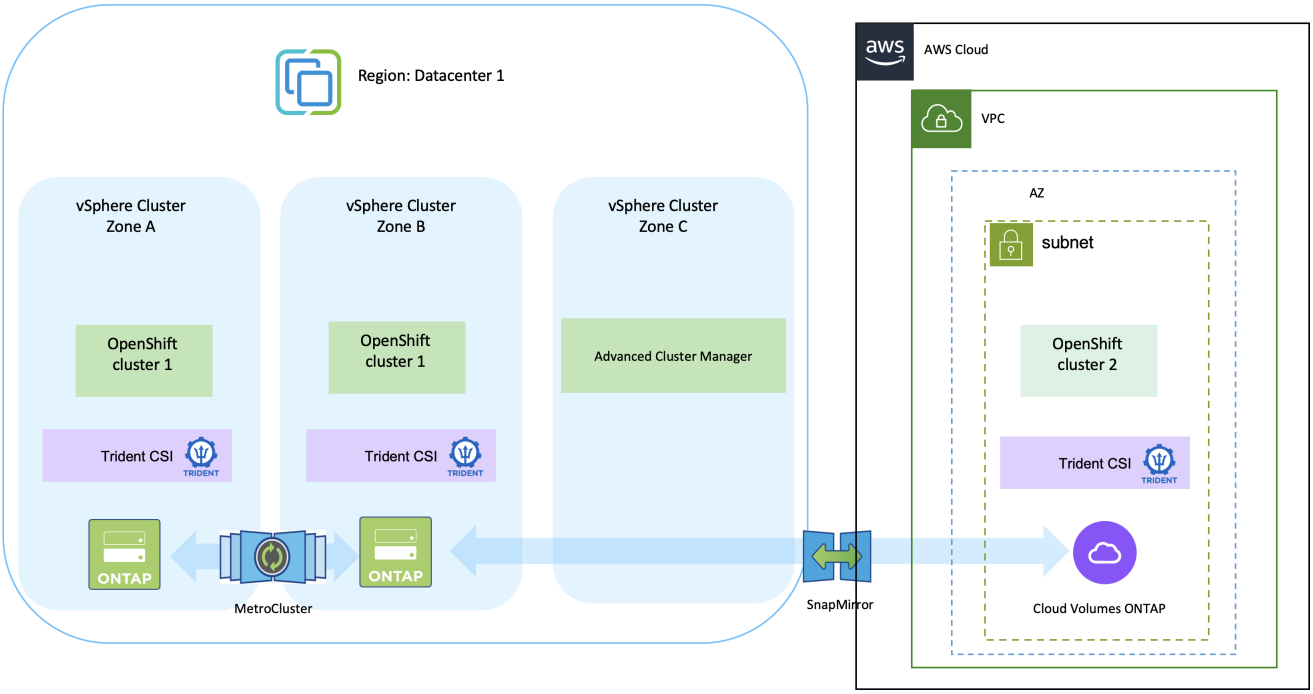


在 **AWS** 上部署和配置 **Red Hat OpenShift Container** 平台

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

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

下图描述了部署在 AWS 上并使用 VPN 连接到数据中心的集群。



设置过程可分为以下步骤：

▼ 从高级集群管理在 **AWS** 上安装 **OCP** 集群。

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

从 Advanced Cluster Management （ACM） 向导在 AWS 上创建 OpenShift 集群。请参阅说明 "此处"。

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

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

▼ 使用 **NetApp Console** 在 **AWS** 中部署 **Cloud Volumes ONTAP**。

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

该连接器也可以安装在云环境中。参考"此处"了解更多信息。

▼ 在 **OCP** 集群中安装**Trident**

- 使用 Helm 部署 Trident Operator。请参见说明 "此处"

- 创建后端和存储类。参考说明"此处"。

使用**Trident**的 **CSI** 拓扑功能实现多区域架构

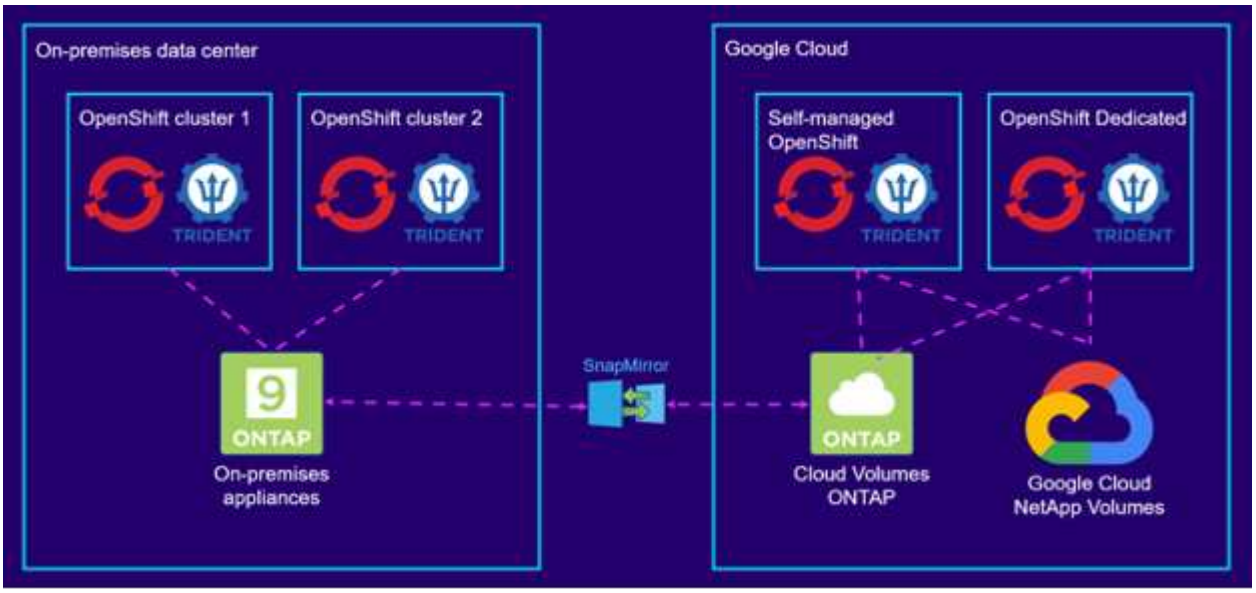
如今，云提供商使 Kubernetes/OpenShift 集群管理员能够生成基于区域的集群节点。节点可以位于一个区域内的不同可用区，也可以跨多个区域。为了方便在多区域架构中为工作负载配置卷， Trident使用了 CSI 拓扑。使用 CSI 拓扑功能，可以根据区域和可用区域将对卷的访问限制到节点子集。参考"此处"了解更多详细信息。

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

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

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

下图显示了在 GCP 上部署并使用 VPN 连接到数据中心的集群。



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

设置过程可分为以下步骤：

从 **CLI** 在 **GCP** 上安装 **OCP** 集群

- 确保您已满足 "此处" 所述的所有先决条件。
- 为了实现本地和 GCP 之间的 VPN 连接，我们创建并配置了一个 pfSense VM。有关说明，请参阅 "此处"。

- 只有在 Google Cloud Platform 中创建 VPN 网关后，才能配置 pfSense 中的远程网关地址。
- 只有在 OpenShift 集群安装程序运行并创建集群的基础架构组件后，才能配置第 2 阶段的远程网络 IP 地址。
- 只有在安装程序创建集群的基础架构组件后，才能配置 Google Cloud 中的 VPN。

- 现在在 GCP 上安装 OpenShift 集群。
  - 获取安装程序和 pull secret，并按照文档中提供的步骤部署集群 "此处"。
  - 安装在 Google Cloud Platform 中创建一个 VPC 网络。它还在 Cloud DNS 中创建一个私有区域并添加 A 记录。
    - 使用VPC网络的CIDR块地址配置pfSense并建立VPN连接。确保防火墙设置正确。
    - 使用 Google Cloud DNS 的 A 记录中的 IP 地址在本地环境的 DNS 中添加 A 记录。
  - 集群安装完成，会提供一个kubeconfig文件以及登录集群控制台的用户名和密码。

部署**Google Cloud NetApp Volumes**

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

使用 **NetApp Console** 在 **GCP** 中部署 **Cloud Volumes ONTAP**

- 在 Google Cloud 中安装控制台代理。请参见说明 "此处"。
- 使用代理在 Google Cloud 中部署 CVO 实例。请参阅说明 "此处"。

在 **GCP** 中的 **OCP** 集群中安装**Trident**

- 如图所示，部署 Trident 的方法有很多 "此处"。
- 对于此项目，Trident 是按照说明手动部署 Trident Operator 来安装的 "此处"。
- 创建后端和存储类。参考说明"此处"。

使用**Trident**的 **CSI** 拓扑功能实现多区域架构

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

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

演示视频

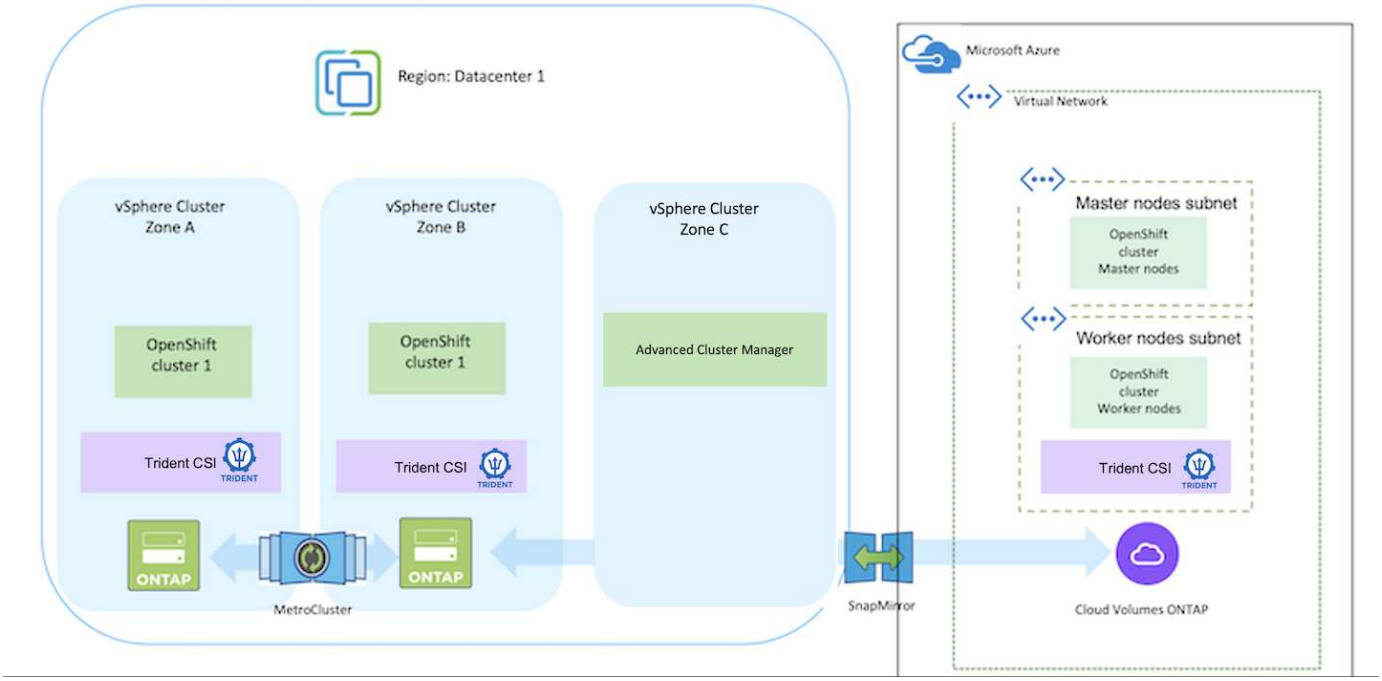
在 Google Cloud Platform 上安装 OpenShift 集群

将 OpenShift 集群导入Trident Protect

在 **Azure** 上部署和配置 **Red Hat OpenShift** 容器平台

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

下图显示了在 Azure 上部署并使用 VPN 连接到数据中心的集群。



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

设置过程可分为以下步骤：

▼ 从 **CLI** 在 **Azure** 上安装 **OCP** 群集。

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

下面给出了一个示例 install-config.yaml 文件。

```
apiVersion: v1
baseDomain: sddc.netapp.com
```

```
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
```

```
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

▼ 使用 **NetApp Console** 在 **Azure** 中部署 **Cloud Volumes ONTAP**。

- 在 Azure 中安装 NetApp Console 代理。请参见说明 "此处"。
- 使用代理在 Azure 中部署 CVO 实例。请参阅说明"此处"。

使用**Trident**的 **CSI** 拓扑功能实现多区域架构

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

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

使用**Trident Protect** 进行数据保护

有关使用 Trident Protect 保护和迁移容器工作负载的详细信息，请查看以下部分： - "使用 Trident Protect 保护和迁移容器应用程序"

具有提供商管理组件的混合云

具有托管 **Red Hat OpenShift** 容器平台工作负载的**NetApp**解决方案

客户可能“诞生于云端”，或者正处于现代化历程的某个阶段，准备将部分选定的工作负载或所有工作负载从数据中心迁移到云端。他们可以选择在云中使用提供商管理的 OpenShift 容器和提供商管理的NetApp存储来运行他们的工作负载。他们应该在云中规划和部署托管的 Red Hat OpenShift 容器集群，以便为他们的容器工作负载提供成功的生产

就绪环境。 NetApp为三大领先公共云中的托管 Red Hat 解决方案提供完全托管的存储产品。

Amazon FSx for NetApp ONTAP (FSx ONTAP)

FSx ONTAP为 AWS 中的容器部署提供数据保护、可靠性和灵活性。 Trident作为动态存储供应器，为客户的有状态应用程序使用持久性 FSx ONTAP存储。

由于 ROSA 可以在 HA 模式下部署，并且控制平面节点分布在多个可用区域，因此 FSx ONTAP还可以配置多可用区选项，以提供高可用性并防止可用区故障。

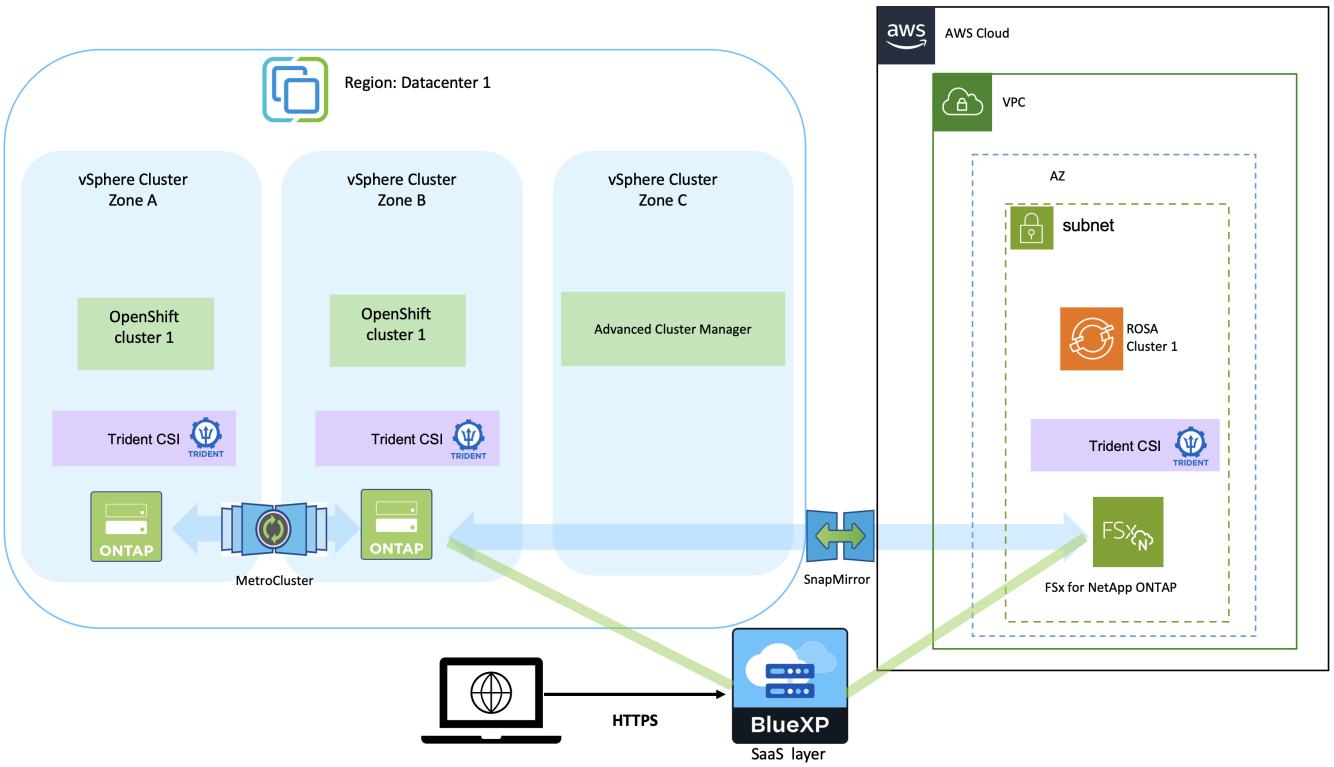
- Google Cloud NetApp Volumes*

Red Hat OpenShift Dedicated 是一个完全托管的应用程序平台，使您能够在混合云中快速构建、部署和扩展应用程序。 Google Cloud NetApp Volumes提供持久卷，将 ONTAP 的全套企业数据管理功能带入 Google Cloud 中的 OpenShift 部署。

在 **AWS** 上部署和配置托管 **Red Hat OpenShift** 容器平台

本节介绍在 AWS（ROSA）上设置托管 Red Hat OpenShift 集群的高级工作流。它展示了 Trident 使用托管的 Amazon FSx for NetApp ONTAP（FSx ONTAP）作为存储后端来提供持久卷。其中提供了有关使用 NetApp Console 在 AWS 上部署 FSx ONTAP 的详细信息。此外，还提供了有关使用 NetApp Console 和 OpenShift GitOps（Argo CD）为 ROSA 集群上的有状态应用程序执行数据保护和迁移活动的详细信息。

下图描述了部署在 AWS 上并使用 FSx ONTAP作为后端存储的 ROSA 集群。



该解决方案通过在AWS的两个VPC中使用两个ROSA集群进行了验证。每个 ROSA 集群都使

用Trident与 FSx ONTAP集成。在 AWS 中部署 ROSA 集群和 FSx ONTAP有几种方法。此设置的高级描述提供了所使用的特定方法的文档链接。您可以参考"资源部分"。

设置过程可分为以下步骤：

安装**ROSA**集群

- 创建两个 VPC 并在 VPC 之间建立 VPC 对等连接。
- 请参阅 "此处" 获取安装 ROSA 集群的说明。

安装 **FSx ONTAP**

- 从 NetApp Console 在 VPC 上安装 FSx ONTAP。有关创建 NetApp Console 帐户并开始使用的信息，请参阅 "此处"。有关安装 FSx ONTAP 的信息，请参阅 "此处"。有关在 AWS 中创建连接器以管理 FSx ONTAP 的信息，请参阅 "此处"。
- 使用 AWS 部署 FSx ONTAP 。参考"此处"使用 AWS 控制台进行部署。

在 **ROSA** 集群上安装**Trident** （使用 **Helm** 图表）

- 使用 Helm chart 在 ROSA 集群上安装 Trident。请参见文档链接：https://docs.netapp.com/us-en/trident/trident-install/kubernetes-deploy-helm.html[此处^]。

FSx ONTAP与Trident集成用于 ROSA 集群

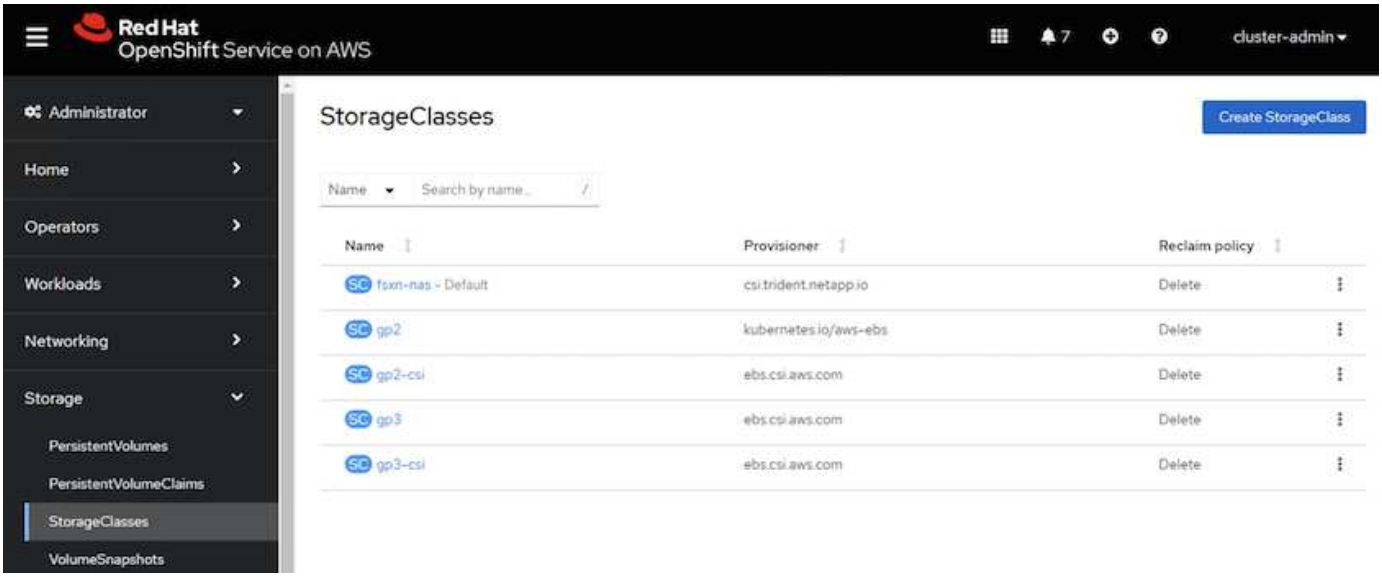
OpenShift GitOps 可用于将Trident CSI 部署到所有托管集群，因为它们使用 ApplicationSet 注册到 ArgoCD。

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```



使用**Trident**创建后端和存储类（适用于 **FSx ONTAP**）

- 参考"此处"有关创建后端和存储类的详细信息。
- 从 OpenShift 控制台将使用Trident CSI 为 FsxN 创建的存储类设为默认。请参阅下面的截图：



使用 **OpenShift GitOps**（**Argo CD**）部署应用程序

- 在集群上安装 OpenShift GitOps operator。请参阅说明 "此处"。
- SetUp 集群的新 Argo CD 实例。请参阅说明 "此处"。

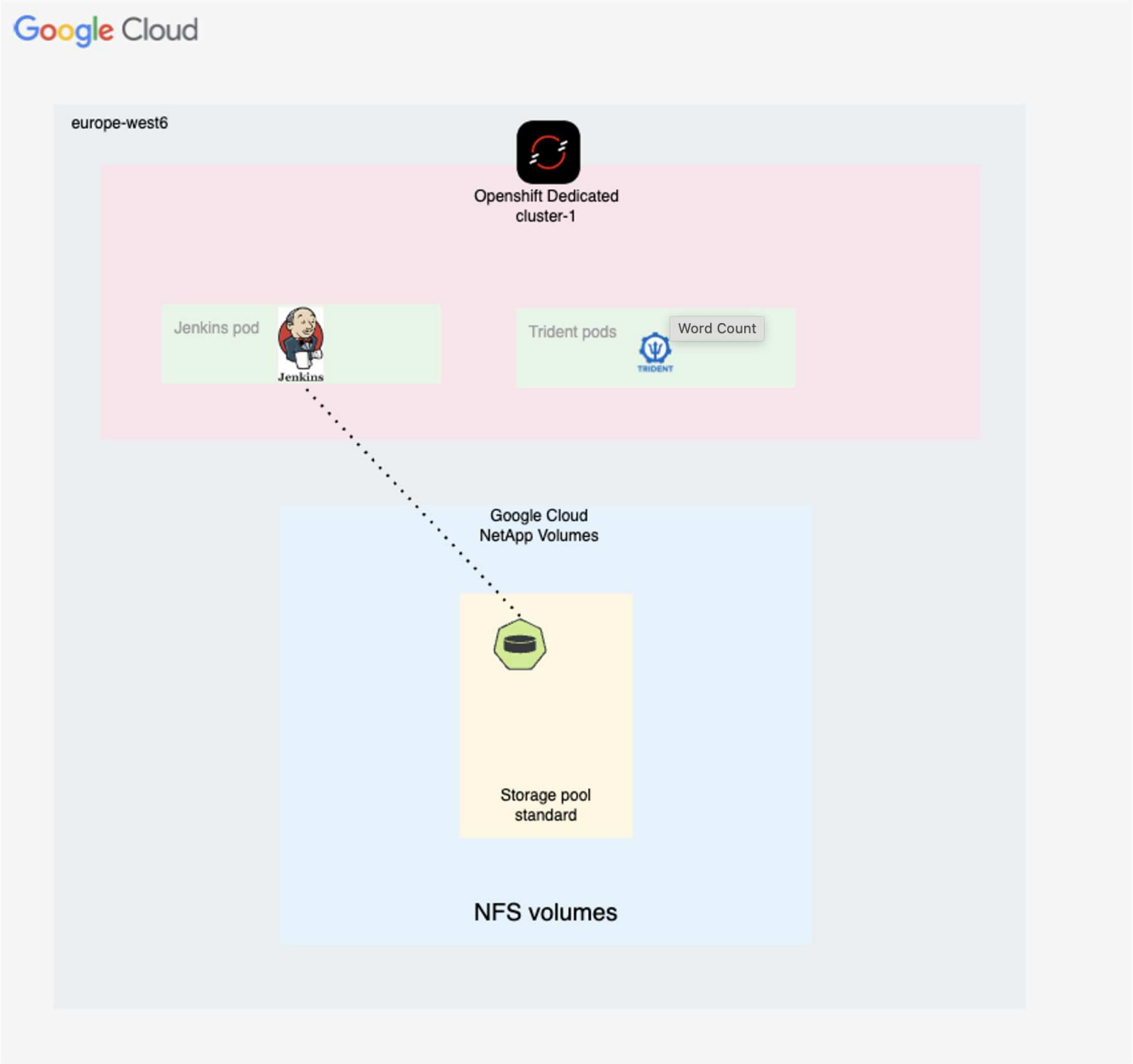
打开 Argo CD 的控制台并部署应用。例如，您可以使用带有 Helm Chart 的 Argo CD 部署 Jenkins 应用程序。创建应用程序时，提供了以下详细信息：Project：default cluster：'https://kubernetes.default.svc'[]（不带引号）Namespace：Jenkins Helm Chart 的 URL：'https://charts.bitnami.com/bitnami'[]（不带引号）

Helm 参数：global.storageClass: fsxn-nas

使用**Google Cloud NetApp Volumes**在 **Google Cloud** 上部署和配置 **OpenShift Dedicated**

本节介绍在 Google Cloud 平台上设置 OpenShift Dedicated (OSD) 集群的高级工作流程。它显示NetApp Trident使用Google Cloud NetApp Volumes作为存储后端，为使用 Kubernetes 运行的有状态应用程序提供持久卷。

下图描述了部署在 Google Cloud 上并使用NetApp Volumes 作为后端存储的 OSD 集群。



设置过程可分为以下步骤：

在 **Google Cloud** 中安装 **OSD** 集群

- 如果您希望为集群使用现有的 VPC，则必须为 OSD 集群创建 VPC、两个子网、一个云路由器和两个 GCP 云 NAT。参考"此处"以获取说明。
- 请参阅"此处"获取有关使用客户云订阅（CCS）计费模型在 GCP 上安装 OSD 集群的说明。OSD 也包含在 Google Cloud Marketplace 中。有关如何使用 Google Cloud Marketplace 解决方案安装 OSD 的视频位于"此处"。

启用**Google Cloud NetApp Volumes**

- 参考"此处"有关设置对Google Cloud NetApp Volumes 的访问权限的信息。遵循所有步骤，包括
- 创建存储池。参考"此处"有关如何在Google Cloud NetApp Volumes上设置存储池的信息。将在存储池内创建在 OSD 上运行的有状态 Kubernetes 应用程序的卷。

在 **OSD** 集群上安装**Trident** （使用 **Helm** 图表）

- 使用 Helm 图表在 OSD 集群上安装 Trident。有关如何安装 Helm Chart 的说明，请参阅 "此处"。

将**NetApp Volumes** 与**NetApp Trident**集成用于 **OSD** 集群

使用Trident创建后端和存储类（适用于Google Cloud NetApp Volumes）

- 有关创建后端的详细信息，请参阅此处。
- 如果 kubernetes 中的任何当前存储类被标记为默认，请通过编辑存储类来删除该注释。
- 使用Trident CSI 配置程序为NetApp卷创建至少一个存储类。使用注释将其中一个存储类设为默认存储类。当 PVC 清单中未明确调用时，这将允许 PVC 使用此存储类。下面显示了一个带有注释的示例。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

使用 **OpenShift GitOps**（**Argo CD**）部署应用程序

- 在集群上安装 OpenShift GitOps operator。请参阅说明 "此处"。
- SetUp 集群的新 Argo CD 实例。请参阅说明 "此处"。

打开 Argo CD 的控制台并部署应用。例如，您可以使用带有 Helm Chart 的 Argo CD 部署 Jenkins 应用程序。创建应用程序时，提供了以下详细信息：Project：default cluster：'https://kubernetes.default.svc'[]（不带引号）Namespace：Jenkins Helm Chart 的 URL：'https://charts.bitnami.com/bitnami'[]（不带引号）

数据保护

有关使用 Trident Protect 保护和迁移容器工作负载的详细信息，请查看以下部分： - "使用 Trident Protect 保护和迁移容器应用程序"

适用于 **Red Hat OpenShift** 工作负载的其他**NetApp**混合多云解决方案

请参见以下解决方案：

- "Red Hat OpenShift Container 本地解决方案"
- "AWS 上的 Red Hat OpenShift Service 容器解决方案"
- "本地 Red Hat OpenShift 虚拟化解决方案"
- "Red Hat OpenShift Service on AWS 虚拟化解决方案"

使用Trident Protect 保护数据

使用 Trident Protect 为 OpenShift Container Platform 中的 Container Apps 提供数据保护

参考文档的这一部分提供了使用 Trident Protect 创建容器应用程序的快照和备份的详细信息。NetApp Trident Protect 提供高级应用程序数据管理功能，可增强由 NetApp ONTAP 存储系统和 NetApp Trident CSI 存储配置程序支持的有状态 Kubernetes 应用程序的功能和可用性。Trident Protect 创建应用程序快照和备份。这意味着不仅要为持久卷中的应用程序数据创建快照和备份，还要为应用程序元数据创建快照和备份。Trident Protect 创建的快照和备份可以存储在以下任何对象存储中，并在稍后从中恢复。

- AWS S3
- Azure Blob 存储
- Google Cloud Storage
- ONTAP S3
- 存储网格
- 任何其他与 S3 兼容的存储

Trident Protect 使用基于角色的访问控制 (RBAC) 的 Kubernetes 模型。默认情况下，Trident Protect 提供称为 trident-protect 的单个系统命名空间及其关联的默认服务帐户。如果您的组织有很多用户或特定的安全需求，您可以使用 Trident Protect 的 RBAC 功能对资源和命名空间的访问进行更精细的控制。

有关 Trident Protect 中的 RBAC 的更多信息，请参见 "Trident Protect 文档"

> 集群管理员可以访问默认的 trident-protect 命名空间中的资源，也可以访问所有其他命名空间中的资源。用户无法在 trident-protect 命名空间中创建应用程序数据管理自定义资源 (CR)，如快照和备份 CR。作为最佳实践，用户需要在应用程序命名空间中创建这些 CR。

Trident Protect 可以使用文档中提供的说明进行安装"此处"。本节将显示使用 Trident Protect 的容器应用程序的数据保护和应用程序恢复的工作流程。1.快照创建（按需或预定）2.从快照还原（还原到相同和不同的命名空间）3.备份创建 4.从备份还原

▼ 前提条件

在为应用程序创建快照和备份之前，必须在 Trident Protect 中配置对象存储以存储快照和备份。这是使用 bucket CR 完成的。只有管理员可以创建 bucket CR 并进行配置。bucket CR 在 Trident Protect 中称为 AppVault。AppVault 对象是存储桶的声明性 Kubernetes 工作流表示。AppVault CR 包含在保护操作中使用存储桶所需的配置，例如备份、快照、还原操作和 SnapMirror 复制。

在本示例中，我们将演示使用 ONTAP S3 作为对象存储。以下是为 ONTAP S3 创建 AppVault CR 的工作流程：1.在 ONTAP 集群的 SVM 中创建 S3 对象存储服务器。2.在对象存储服务器中创建存储桶。3.在 SVM 中创建 S3 用户。请将访问密钥和秘密密钥存放在安全的地方。4.在 OpenShift 中，创建一个密钥来存储 ONTAP S3 凭据。5.为 ONTAP S3 创建 AppVault 对象

为 **ONTAP S3** 配置 **Trident Protect AppVault**

使用 **ONTAP S3** 作为 **AppVault** 配置 **Trident Protect** 的示例 **YAML** 文件

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
```

```
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

用于安装 **postgresql** 应用程序的示例 **yaml** 文件

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
```

```
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

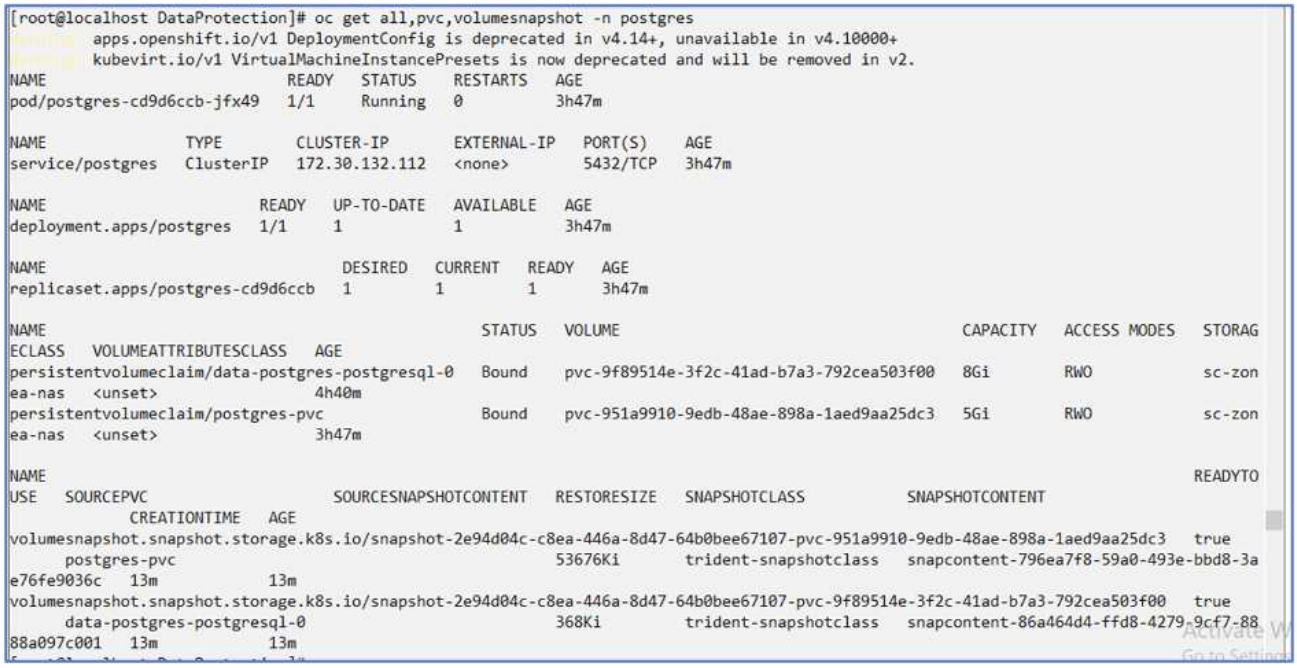
```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ 创建快照

创建按需快照

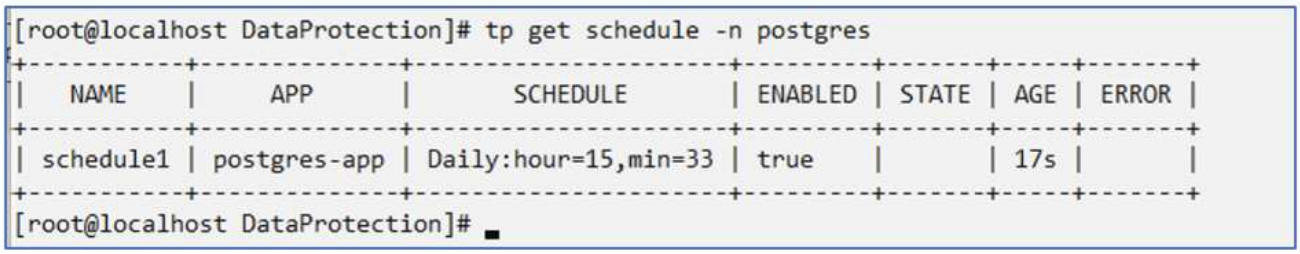
```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+----------------+--------------+-----------+-----+-------+
|      NAME      |   APP REF    |   STATE   | AGE | ERROR |
+----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```



创建计划 使用以下命令，将每天 15:33 创建快照，并保留两个快照和备份。

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```



使用 **yaml** 创建计划

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
```

```
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

您可以看到按照此计划创建的快照。

```
[root@localhost DataProtection]# tp get snap -n postgres
+----------------------------+--------------+-----------+-------+-------+
|            NAME            |   APP REF    |   STATE   |  AGE  | ERROR |
+----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1             | postgres-app | Completed | 1h25m |       |
+----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

还创建了卷快照。

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                  READYTOUSE   SOURCEPVC
                                CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ 删除应用程序以模拟应用程序丢失

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ 从快照恢复到同一命名空间

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |     APPVAULT       |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

应用程序及其 PVC 恢复到同一个命名空间。

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                     READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                 Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ 从快照还原到不同的命名空间

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-
3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n
postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |      APPVAULT      |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

您可以看到应用程序已恢复到新的命名空间。

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                  Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ 创建备份

创建按需备份

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300  | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300  | postgres-app | Completed | 36m27s |       |
| postgres-backup1             | postgres-app | Completed | 6m19s  |       |
+------------------------------+--------------+-----------+--------+-------+
```

创建备份计划

上面列表中的每日和每小时备份是根据之前设置的计划创建的。

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily --hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ 从备份恢复

删除应用程序和 **PVC** 以模拟数据丢失。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

恢复到相同的命名空间 #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir" created。

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

应用程序和 PVC 在同一个命名空间中恢复。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w     1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                  Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

恢复到不同的命名空间 创建一个新的命名空间。从备份恢复到新的命名空间。

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                       READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p   1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                 Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ 迁移应用程序

若要将应用程序克隆或迁移到其他群集（执行跨群集克隆），请在源群集上创建备份，然后将备份还原到其他群集。确保已在目标集群上安装 Trident Protect。

在源集群上，执行下图所示的步骤：

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

从源集群，将上下文切换到目标集群。然后，确保可以从目标集群上下文访问 AppVault，并从目标集群获取 AppVault 内容。

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+---------------+--------------+--------+----------------------------+--------------------------+-----------------------------------
-----------------------------------------------------------------------------------------------+
|    CLUSTER    |     APP      |  TYPE  |            NAME            |        TIMESTAMP         |
                      PATH                                                                     |
+---------------+--------------+--------+----------------------------+--------------------------+-----------------------------------
-----------------------------------------------------------------------------------------------+
| ocp-cluster11 | bbox         | backup | bboxbackup1                | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                                 |
| ocp-cluster11 | postgres-app | backup | backup1                    | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3                             |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300 | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd           |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300 | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d           |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc          |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031          |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1   | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3             |
```

使用列表中的备份路径并创建一个备份恢复 CR 对象，如下面的命令所示。

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|           NAME           |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

现在您可以看到应用程序 pod 和 PVC 已在目标集群中创建。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                    READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                  Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

使用 **Trident Protect** 保护 **Red Hat OpenShift Virtualization** 中的虚拟机

使用快照和备份在 OpenShift Virtualization 中保护虚拟机。此过程包括使用 ONTAP S3 对

象存储创建 AppVault，配置 Trident Protect 以捕获虚拟机数据，包括 Kubernetes 资源对象、持久卷和内部映像，并在必要时恢复数据。

OpenShift 虚拟化环境中的虚拟机是在 OpenShift 容器平台的工作节点中运行的容器化应用程序。保护虚拟机元数据以及虚拟机的持久磁盘非常重要，以便在它们丢失或损坏时可以恢复它们。

OpenShift Virtualization VM 的持久磁盘可以由使用 "Trident犯罪现场调查" 集成到 OpenShift 集群的 ONTAP 存储提供支持。在本节中，我们使用 "Trident Protect" 创建 VM 的快照和备份，包括其数据卷到 ONTAP 对象存储。

然后，我们在需要时从快照或备份中恢复。

Trident Protect 支持 OpenShift 集群上的应用程序和 VM 的快照、备份、恢复和灾难恢复。对于 OpenShift Virtualization VM，可以使用 Trident Protect 保护的数据包括与 VM 关联的 Kubernetes 资源对象、持久卷和内部映像。

以下是本节示例使用的各个组件的版本

- "OpenShift 集群 4.17"
- "通过 Red Hat 提供的 OpenShift Virtualization Operator 安装 OpenShift Virtualization"
- "Trident25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

为对象存储创建 **AppVault**

▼ 创建 **AppVault**

在为应用程序或 VM 创建快照和备份之前，必须在 Trident Protect 中配置对象存储以存储快照和备份。这是使用 bucket CR 完成的。只有管理员可以创建 bucket CR 并对其进行配置。bucket CR 在 Trident Protect 中称为 AppVault。AppVault 对象是存储桶的声明性 Kubernetes 工作流表示。AppVault CR 包含在保护操作中使用存储桶所需的配置，例如备份、快照、还原操作和 SnapMirror 复制。

在本示例中，我们将演示使用 ONTAP S3 作为对象存储。以下是为 ONTAP S3 创建 AppVault CR 的工作流程：1.在 ONTAP 集群的 SVM 中创建 S3 对象存储服务器。2.在对象存储服务器中创建存储桶。3.在 SVM 中创建 S3 用户。请将访问密钥和秘密密钥存放在安全的地方。4.在 OpenShift 中，创建一个密钥来存储 ONTAP S3 凭据。5.为 ONTAP S3 创建 AppVault 对象

为 **ONTAP S3** 配置 **Trident Protect AppVault**

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
```

```
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+--------------------+----------+-----------+-------+---------+-------+
|        NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+--------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault  | OntapS3  | Available |       |         | 8d17h |
+--------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

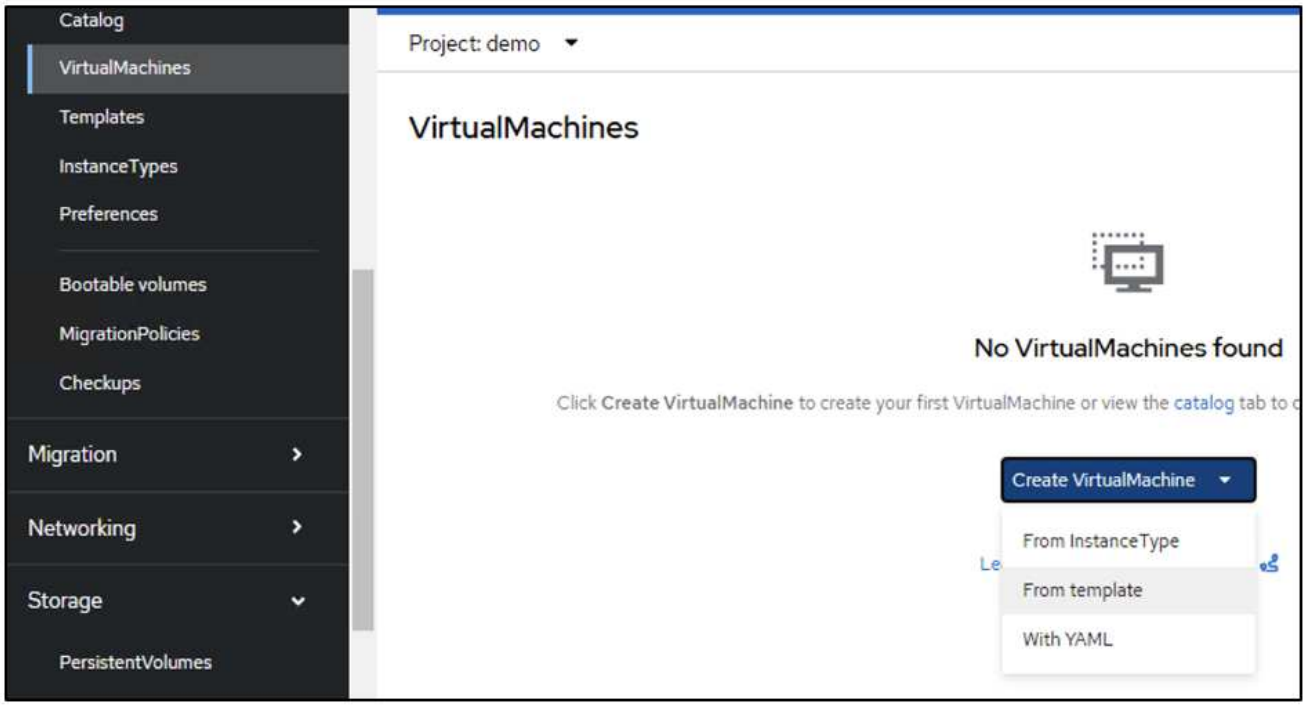
在 **OpenShift Virtualization** 中创建 **VM**

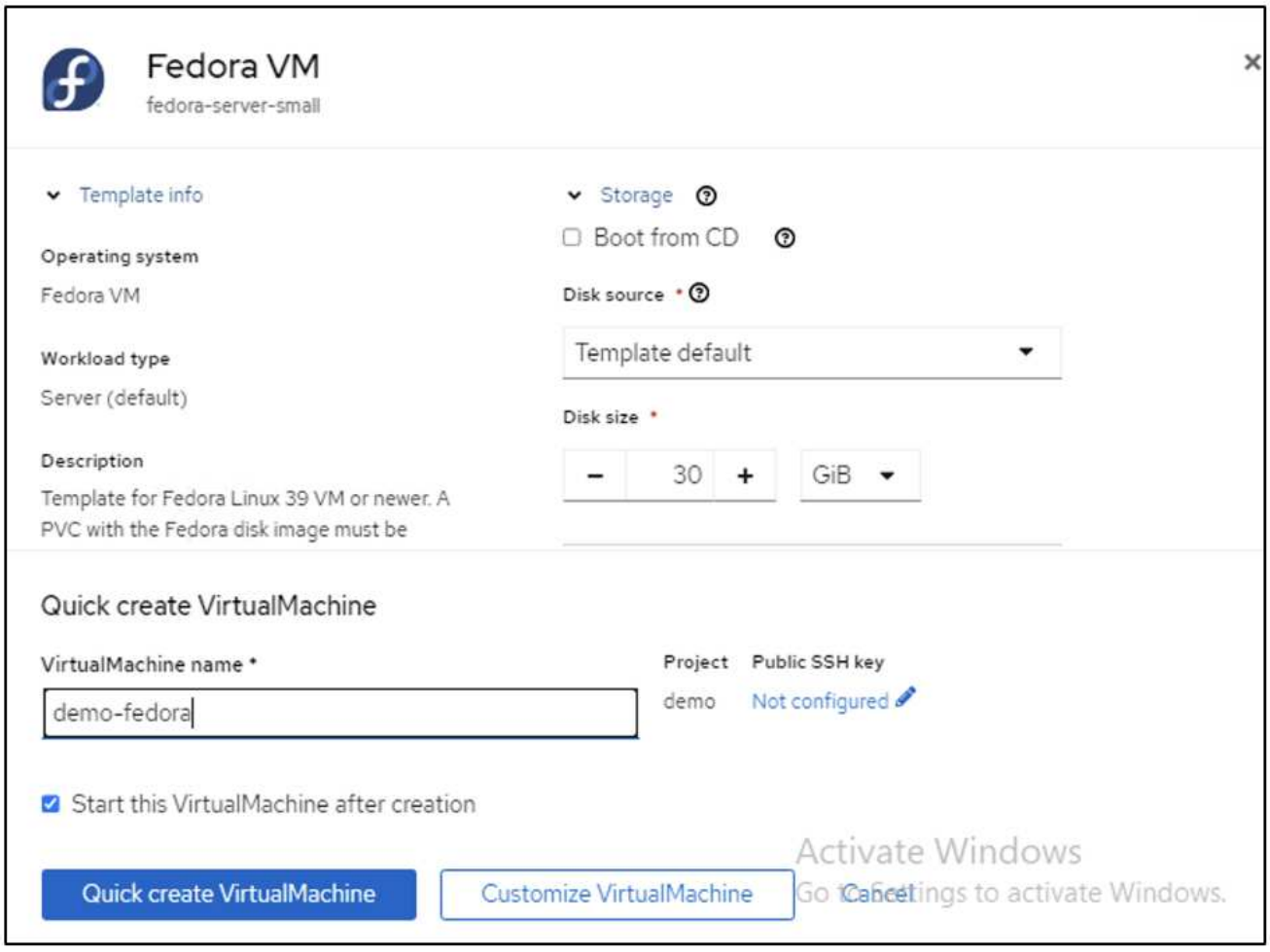
▼ 在 **OpenShift Virtualization** 中创建 **VM**

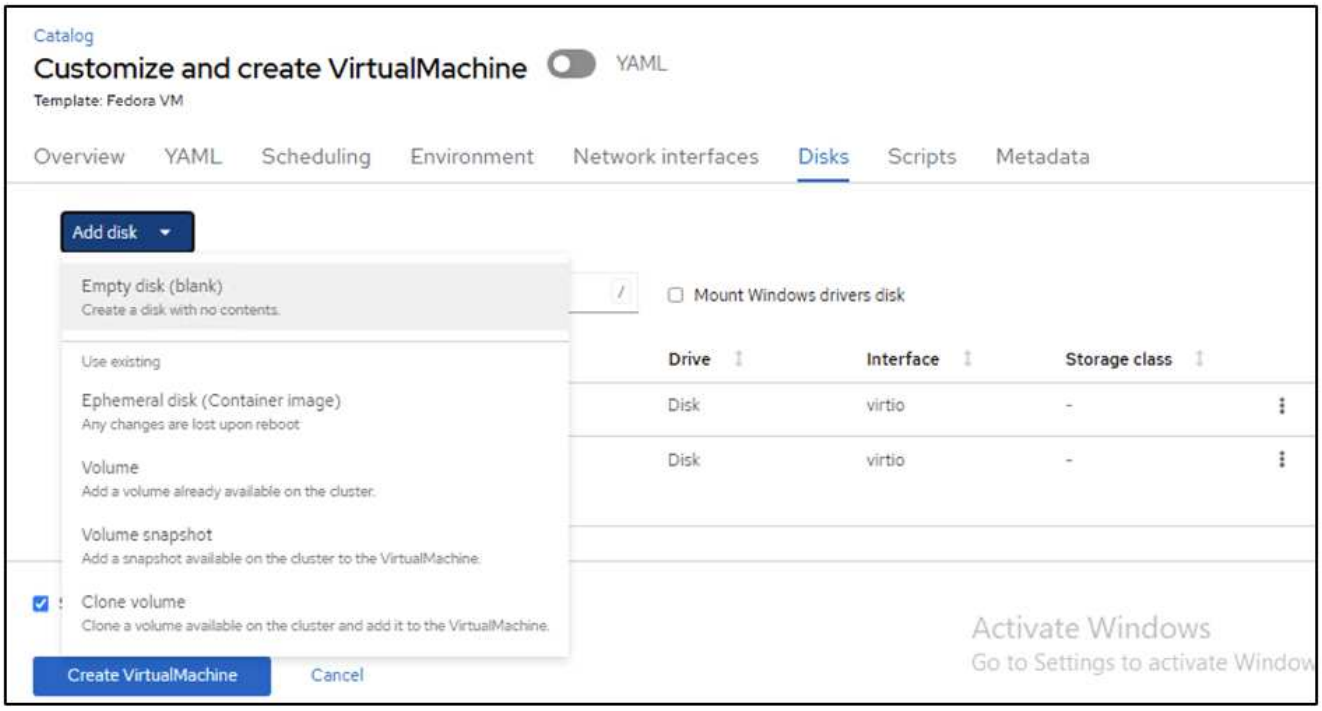
以下屏幕截图显示了使用模板从控制台创建 VM（命名空间 demo 中的 demo-fedora）。根磁盘会自动选择默认存储类别，因此，请验证默认存储类别是否设置得当。在此设置中，默认存储类是**sc-zonea-san**。确保在创建附加磁盘时选择存储类 sc-zonea-san 并选中“应用优化存储设置”复选框。这会将访问模式设置为 RWX，将卷模式设置为阻止。

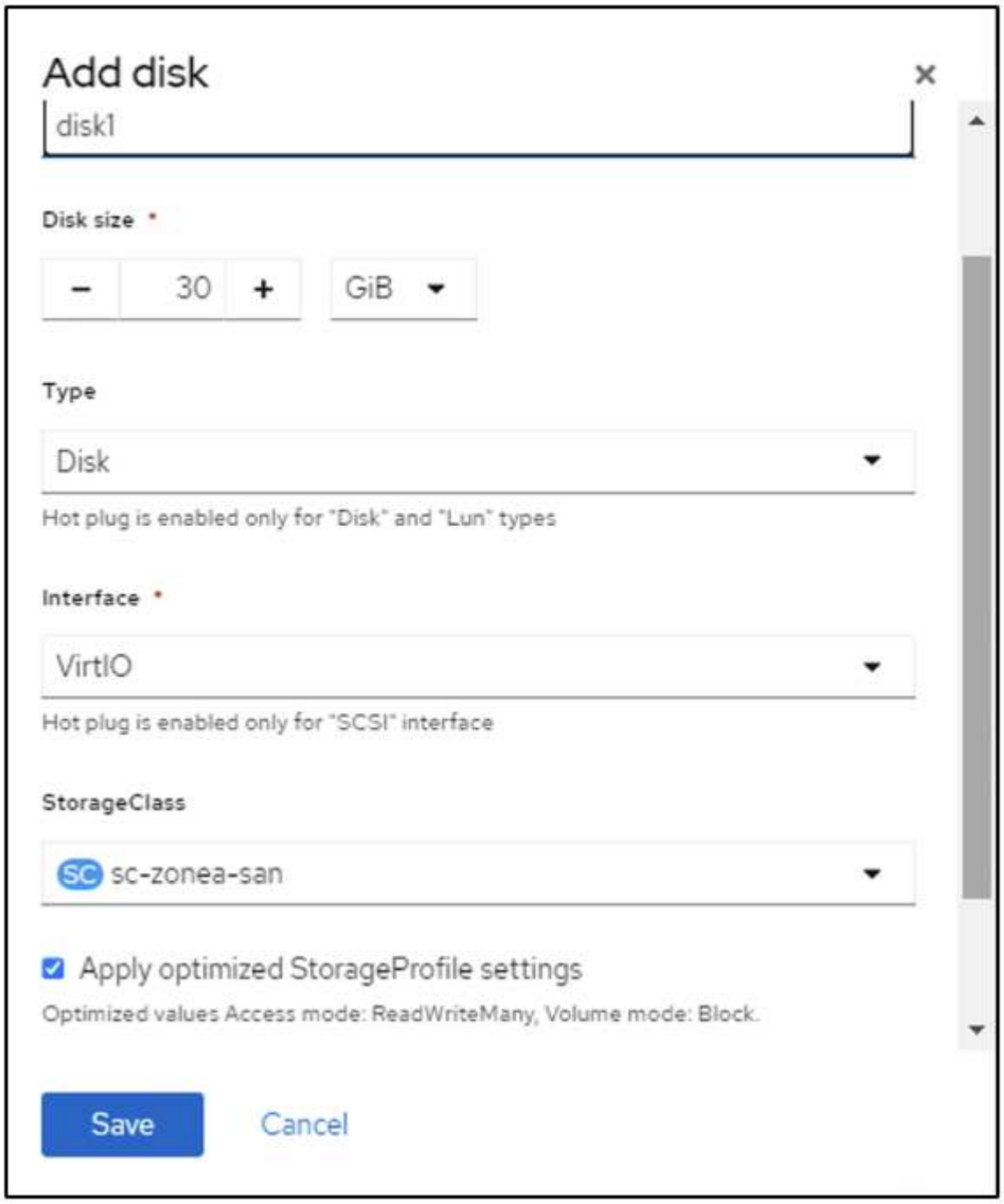
> Trident支持 SAN（iSCSI、NVMe/TCP 和 FC）块卷模式下的 RWX 访问模式。 （这是NAS的默认访问模式）。如果您稍后需要对虚拟机进行实时迁移，则需要 RWX 访问模式。

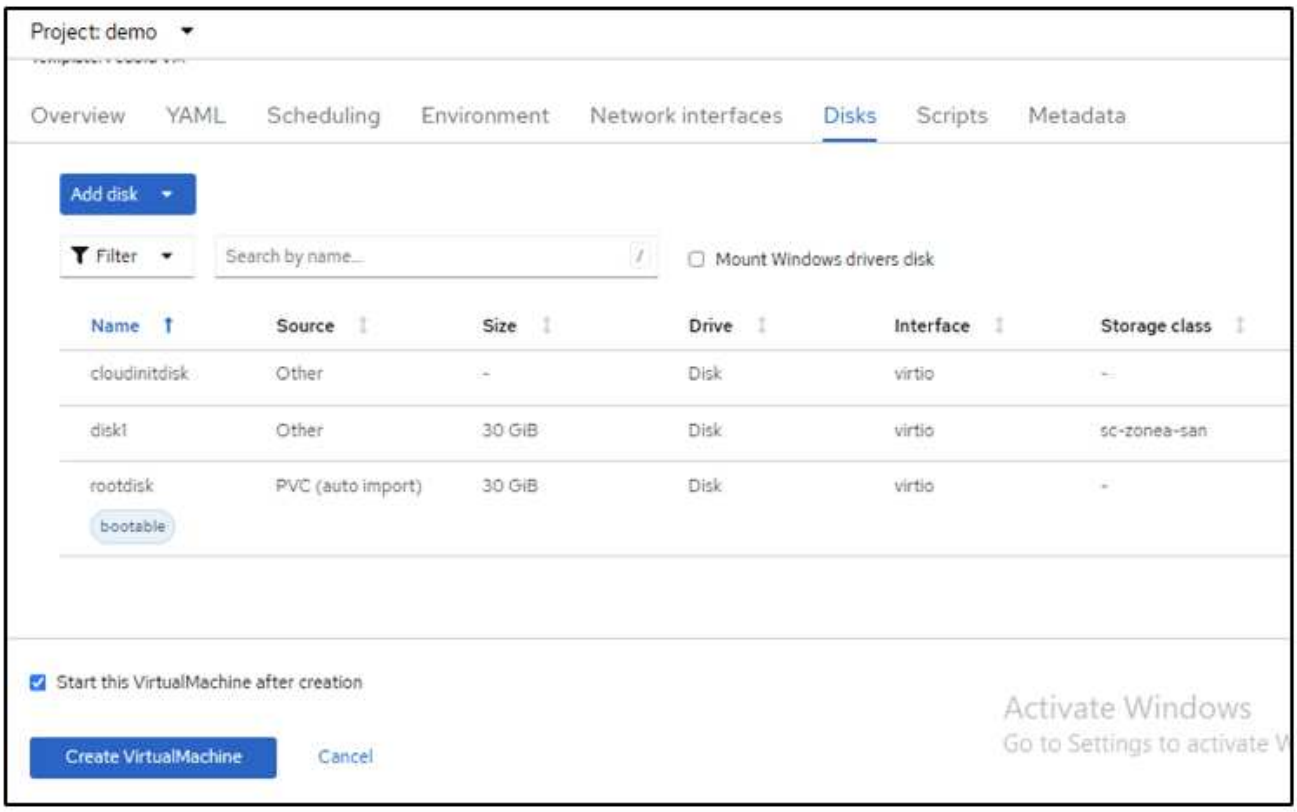



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Quick create VirtualMachine
Customize VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows.


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

创建应用程序

▼ 创建应用程序

为虚拟机创建 **Trident Protect** 应用程序

在示例中，demo 命名空间有一个 VM，并且在创建应用程序时包含命名空间的所有资源。

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
  namespace: demo
```

```
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

通过创建备份来保护应用程序

▼ 创建备份

创建按需备份

为之前创建的应用程序（demo-vm）创建一个备份，其中包括 demo 命名空间中的所有资源。提供将存储备份的 appvault 名称。

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

按计划创建备份

创建备份计划，指定要保留的备份粒度和数量。

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

从备份还原

▼ 从备份还原

将虚拟机恢复到相同的命名空间

在示例中，备份 demo-vm-backup-on-demand 包含 fedora VM 的 demo-app 备份。

首先，删除虚拟机，并确保 PVC、pod 和虚拟机对象从命名空间“demo”中删除

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                  STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

现在，创建一个就地备份恢复对象。

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

验证虚拟机、Pod 和 PVC 是否已恢复

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

将虚拟机还原到不同的命名空间

首先创建一个要将应用程序恢复到的新命名空间，在本例中为 demo2。然后创建备份恢复对象

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  conditions: null
```

```
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

验证是否在新命名空间 demo2 中创建了 VM、pod 和 pvc。

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

使用快照保护应用程序

▼ 创建快照

创建按需快照 为应用程序创建快照并指定需要存储它的 appvault。

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
```

```
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

为快照创建计划 为快照创建计划。指定要保留的粒度和快照数量。

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-------------------------------------------+---------+----------------+-----------+-------+--------+
|                   NAME                    |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand                 | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000               | demo-vm | Delete         | Completed |       | 1m29s  |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

从快照还原

▼ 从快照还原

将虚拟机从快照恢复到同一个命名空间 从 demo2 命名空间中删除虚拟机 demo-fedora。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

从虚拟机的快照创建快照就地恢复对象。

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
```

```
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+-----------------------------------+-------------------+-----------+-------+--------+
|               NAME                |     APPVAULT      |   STATE   | ERROR |  AGE   |
+-----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+-----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

验证虚拟机及其 PVC 是否在 demo 命名空间中创建。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    5m17s   Running   True

NAME                                                  STATUS   VOLUME
persistentvolumeclaim/demo-fedora                     Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

将虚拟机从快照还原到不同的命名空间

删除先前从备份中恢复的 demo2 命名空间中的虚拟机。

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora    3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr  1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc  1/1     Running   0          3m11s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                     Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                     Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

从快照创建快照恢复对象并提供命名空间映射。

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-----------------------------------+------------------+-----------+-------+--------+
|               NAME                |     APPVAULT     |   STATE   | ERROR |  AGE   |
+-----------------------------------+------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-----------------------------------+------------------+-----------+-------+--------+
```

验证虚拟机及其 PVC 是否在新的命名空间 demo2 中恢复。

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                        STATUS   VOLUME
STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                           Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san     <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san     <unset>                 29h
[root@localhost RedHat]#
```

恢复特定虚拟机

▼ 选择命名空间中的特定虚拟机来创建快照/备份和恢复

在前面的例子中，我们在命名空间内有一个虚拟机。通过将整个命名空间包含在备份中，可以捕获与该虚拟机相关的所有资源。在下面的示例中，我们将另一个 VM 添加到同一个命名空间，并使用标签选择器为这个新 VM 创建一个应用程序。

在 **demo** 命名空间中创建一个新的虚拟机（**demo-centos vm**）

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora    81m     Running   True

NAME                                  READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g   1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          81m

NAME                                                        STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                           Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                           Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

标记 **demo-centos vm** 及其相关资源

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

验证 **demo-centos vm** 和 **pvcs** 是否已获得标签

```
[root@localhost VM-DataProtection]# oc get vm --show-labels -n demo
NAME          AGE     STATUS    READY   LABELS
demo-centos   6m31s   Running   True    app=demo-centos,category=protect-demo-centos,kubevirt.io/dynamic-credentials-support=true,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=centos-stream9-server-small
demo-fedora   85m     Running   True    app=demo-fedora,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=fedora-server-small
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get pvc --show-labels -n demo
NAME                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE     LABELS
demo-centos                         Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san   <unset>                 7m41s   app.kubernetes.io/component=storage,app.kubernetes
.io/managed-by=cdi-controller,app.kubernetes.io/part-of=hyperconverged-cluster,app.kubernetes.io/version=4.17.5,app=containerized-data-importer,category=protect-demo-centos,instancetype.kubevirt.io/default-instanc
etype=u1.medium,instancetype.kubevirt.io/default-preference=centos.stream9,kubevirt.io/created-by=a6a7b49c-669a-4e21-aa78-20743671b284
demo-fedora                         Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san   <unset>                 86m     app.kubernetes.io/component=storage,app.kubernetes
.io/managed-by=cdi-controller,app.kubernetes.io/part-of=hyperconverged-cluster,app.kubernetes.io/version=4.17.5,app=containerized-data-importer,instancetype.kubevirt.io/default-instancetype=u1.medium,instancetype.
kubevirt.io/default-preference=fedora,kubevirt.io/created-by=7d5184e9-22f0-4456-9afe-3d1904c430f9
dv-demo-centos-lavender-tortoise-34   Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san   <unset>                 7m41s   app.kubernetes.io/component=storage,app.kubernetes
.io/managed-by=cdi-controller,app.kubernetes.io/part-of=hyperconverged-cluster,app.kubernetes.io/version=4.17.5,app=containerized-data-importer,category=protect-demo-centos,kubevirt.io/created-by=a6a7b49c-669a-4e2
1-aa78-20743671b284
dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246a63f8   30Gi       RWX            sc-zonea-san   <unset>                 86m     app.kubernetes.io/component=storage,app.kubernetes
.io/managed-by=cdi-controller,app.kubernetes.io/part-of=hyperconverged-cluster,app.kubernetes.io/version=4.17.5,app=containerized-data-importer,kubevirt.io/created-by=7d51B4e9-22f0-4456-9afe-3d1904c430f9
[root@localhost VM-DataProtection]#
```

使用标签选择器仅为特定虚拟机（**demo-centos**）创建应用程序

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+-----------------+------------+-------+------+
|      NAME       | NAMESPACES | STATE | AGE  |
+-----------------+------------+-------+------+
| demo-centos-app | demo       | Ready | 56s  |
| demo-vm         | demo       | Ready | 4h6m |
+-----------------+------------+-------+------+
```

按需和按计划创建备份和快照的方法与前面所示的相同。由于用于创建快照或备份的 trident-protect 应用程序仅包含来自命名空间的特定 VM，因此从它们恢复只会恢复特定的 VM。下面显示了一个备份/恢复操作的示例。

使用其对应的应用程序创建命名空间中特定虚拟机的备份

在前面的步骤中，使用标签选择器创建了一个应用程序，以仅包含演示命名空间中的 centos vm。为此应用程序创建备份（在本例中为按需备份）。

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+------------------------------+-----------------+----------------+-----------+-------+--------+
|             NAME             |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand     | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500  | demo-vm         | Retain         | Completed |       | 56m17s |
+------------------------------+-----------------+----------------+-----------+-------+--------+
```

将特定的 **VM** 恢复到同一个命名空间 使用相应的应用程序创建了特定的 VM（centos）的备份。如果从此创建了备份就地恢复或备份恢复，则仅恢复此特定的 VM。删除 Centos VM。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora   4m27s   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                    STATUS   VOLUME
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

从 demo-centos-backup-on-demand 创建备份就地恢复并验证 centos VM 是否已重新创建。

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-
demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore  | ontap-s3-appvault  | Completed |       | 57m9s |
| demo-fedora-restore  | ontap-s3-appvault  | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

将特定的 **VM** 恢复到不同的命名空间 从 demo-centos-backup-on-demand 创建到不同命名空间 (demo3) 的备份恢复，并验证 centos VM 是否已重新创建。

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-
demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault  | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

视频演示

以下视频演示了如何使用快照保护虚拟机

保护虚拟机

使用第三方工具保护容器应用

使用 **OpenShift API for Data Protection (OADP)** 为 **OpenShift Container Platform** 中的容器应用提供数据保护

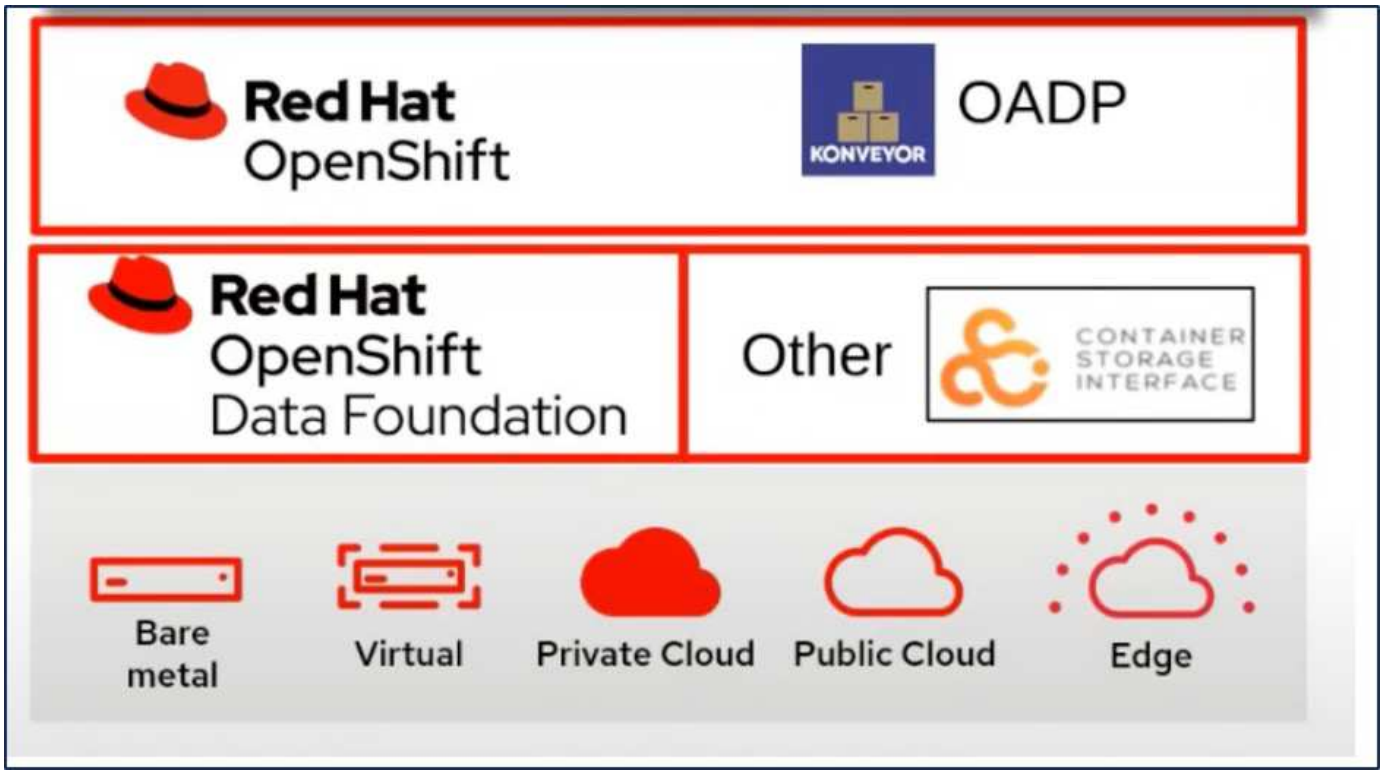
参考文档的此部分提供了在NetApp ONTAP S3 或NetApp StorageGRID S3 上使用 Velero 的 OpenShift API for Data Protection (OADP) 创建容器应用程序备份的详细信息。使用 CSI Trident Snapshots 创建应用程序的命名空间范围资源（包括持久卷 (PV)）的备份。

容器应用的持久存储可由使用 "Trident犯罪现场调查" 集成到 OpenShift 集群的 ONTAP 存储提供支持。在本节中，我们使用 "OpenShift 数据保护 API (OADP)" 将应用程序（包括其数据卷）备份到

- ONTAP对象存储
- 存储网格

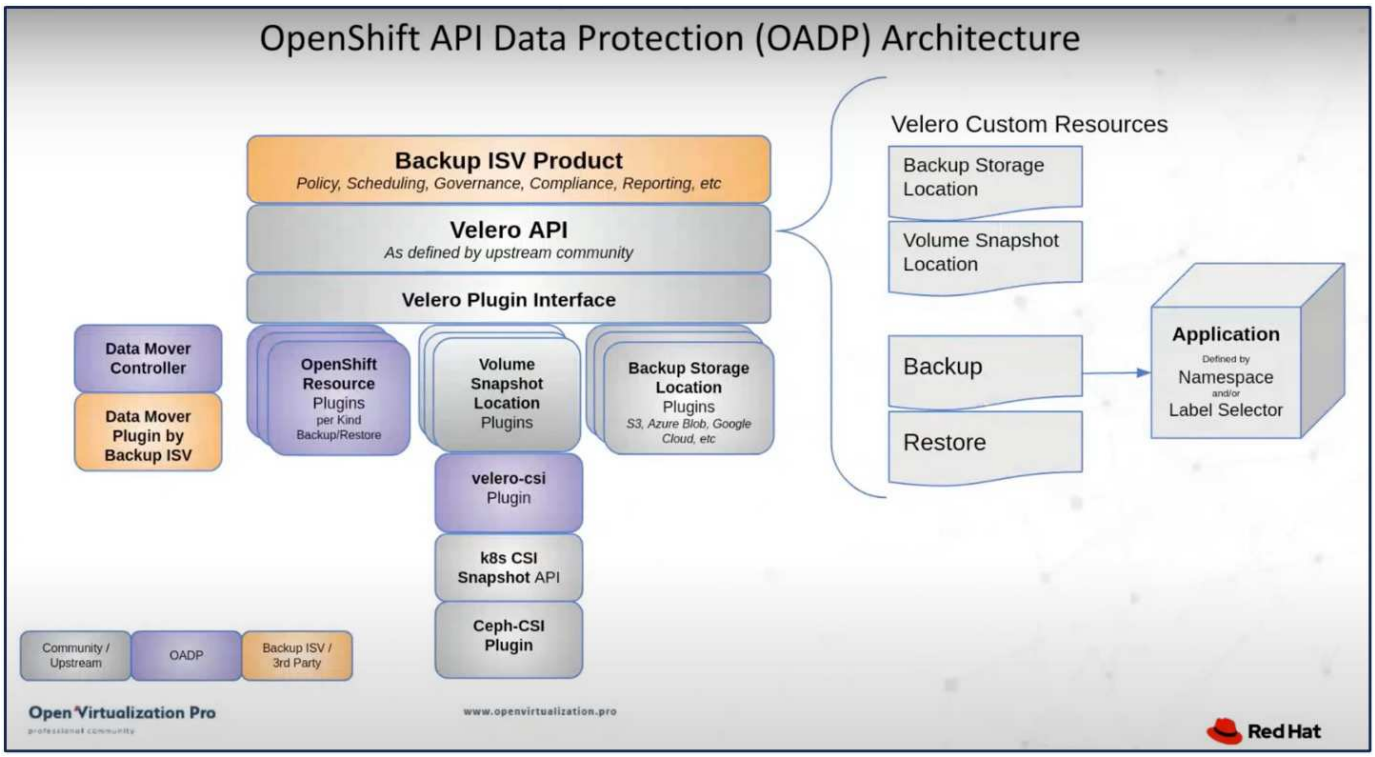
然后我们在需要时从备份中恢复。请注意，应用程序只能恢复到创建备份的集群。

OADP 支持 OpenShift 集群上应用程序的备份、还原和灾难恢复。可以使用 OADP 保护的数据包括 Kubernetes 资源对象、持久卷和内部图像。



Red Hat OpenShift 利用开源社区开发的解决方案来保护数据。"维莱罗"是一个开源工具，用于安全地备份和恢复、执行灾难恢复以及迁移 Kubernetes 集群资源和持久卷。为了轻松使用 Velero，OpenShift 开发了 OADP 操

作符和 Velero 插件以与 CSI 存储驱动程序集成。所公开的 OADP API 的核心基于 Velero API。安装 OADP 操作器并配置后，可以执行的备份/恢复操作基于 Velero API 公开的操作。



OADP 1.3 可从 OpenShift 集群 4.12 及更高版本的操作员中心获得。它有一个内置的数据移动器，可以将 CSI 卷快照移动到远程对象存储。通过在备份期间将快照移动到对象存储位置，这提供了可移植性和耐用性。灾难发生后，快照可用于恢复。

以下是本节示例使用的各个组件的版本

- OpenShift 集群 4.14
- Red Hat 提供的 OADP Operator 1.13
- 适用于 Linux 的 Velero CLI 1.13
- Trident24.02
- ONTAP 9.12
- 使用 helm 安装 postgresql。

"Trident犯罪现场调查" "OpenShift 数据保护 API (OADP)" "维莱罗"

OpenShift API for Data Protection (OADP) Operator 的安装

本节概述了 OpenShift API for Data Protection (OADP) Operator 的安装。

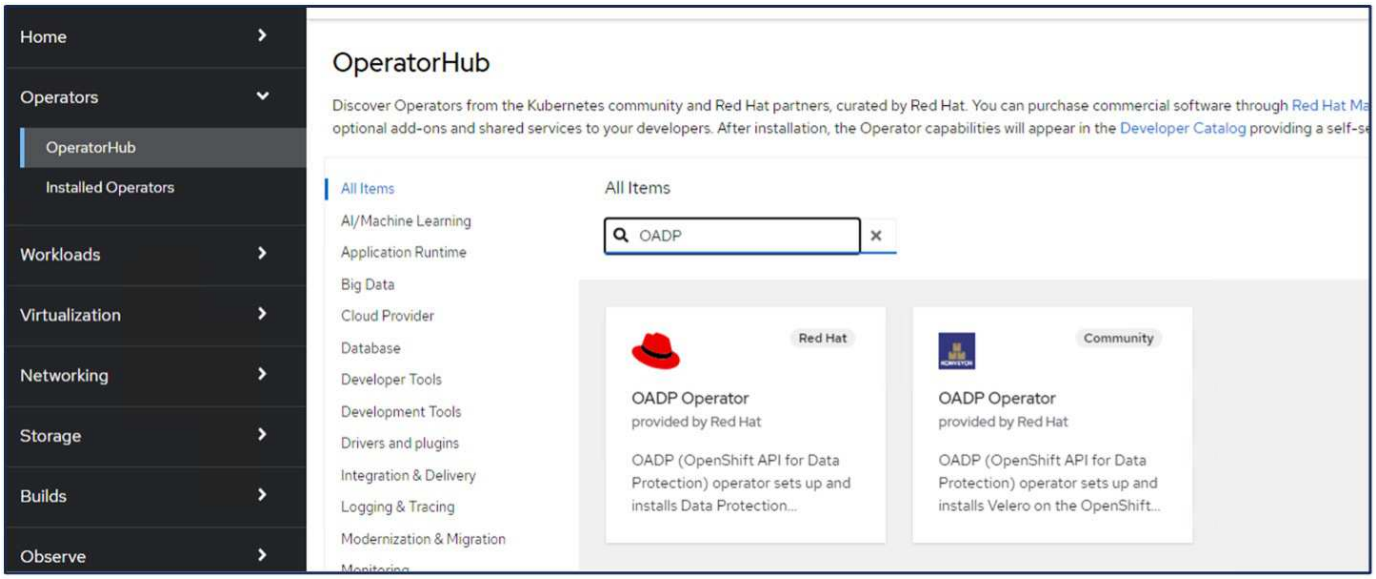
前提条件

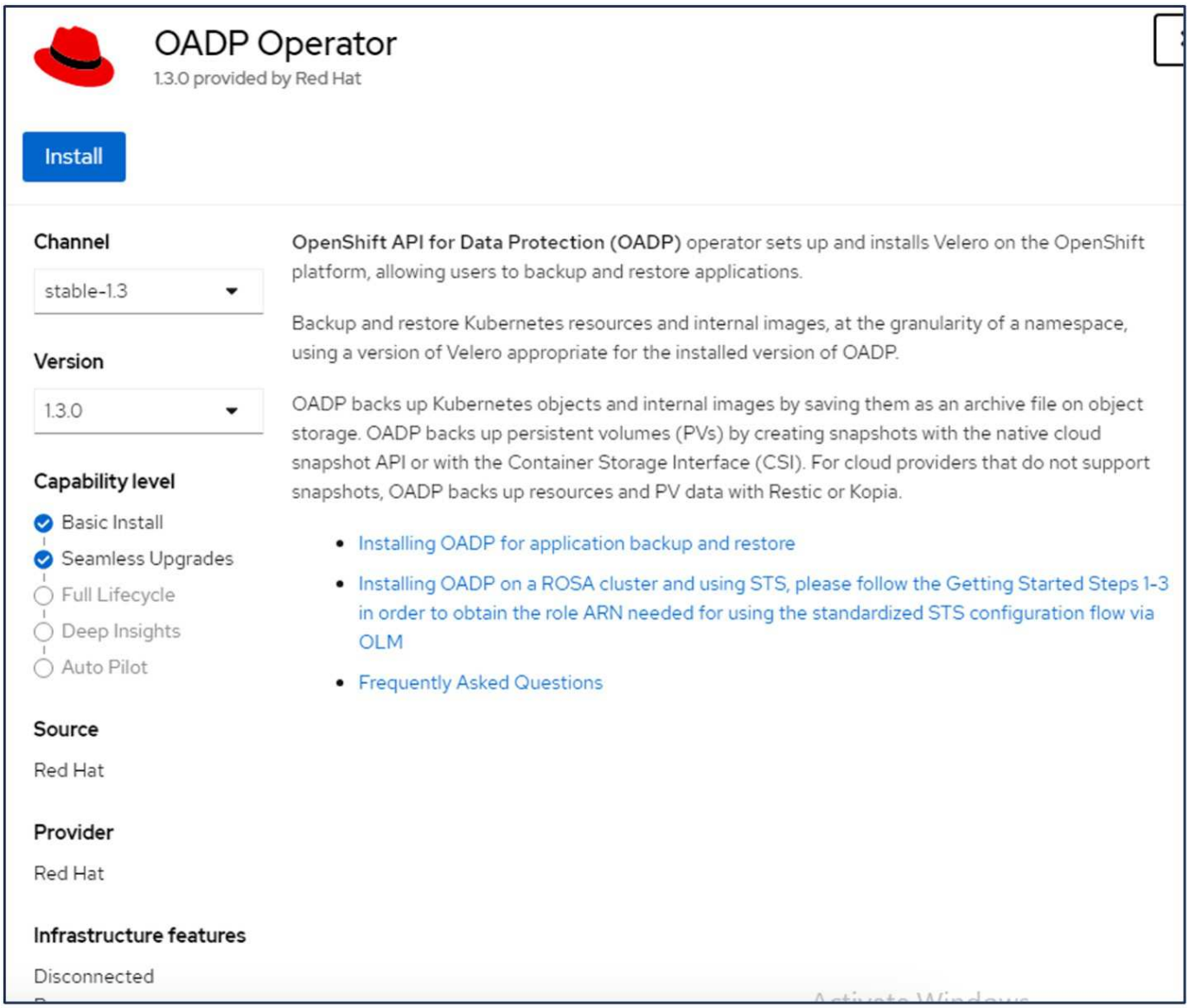
- 安装在裸机基础架构上并带有 RHCOS 工作节点的 Red Hat OpenShift 集群（高于 4.12 版本）
- 使用Trident与集群集成的NetApp ONTAP集群

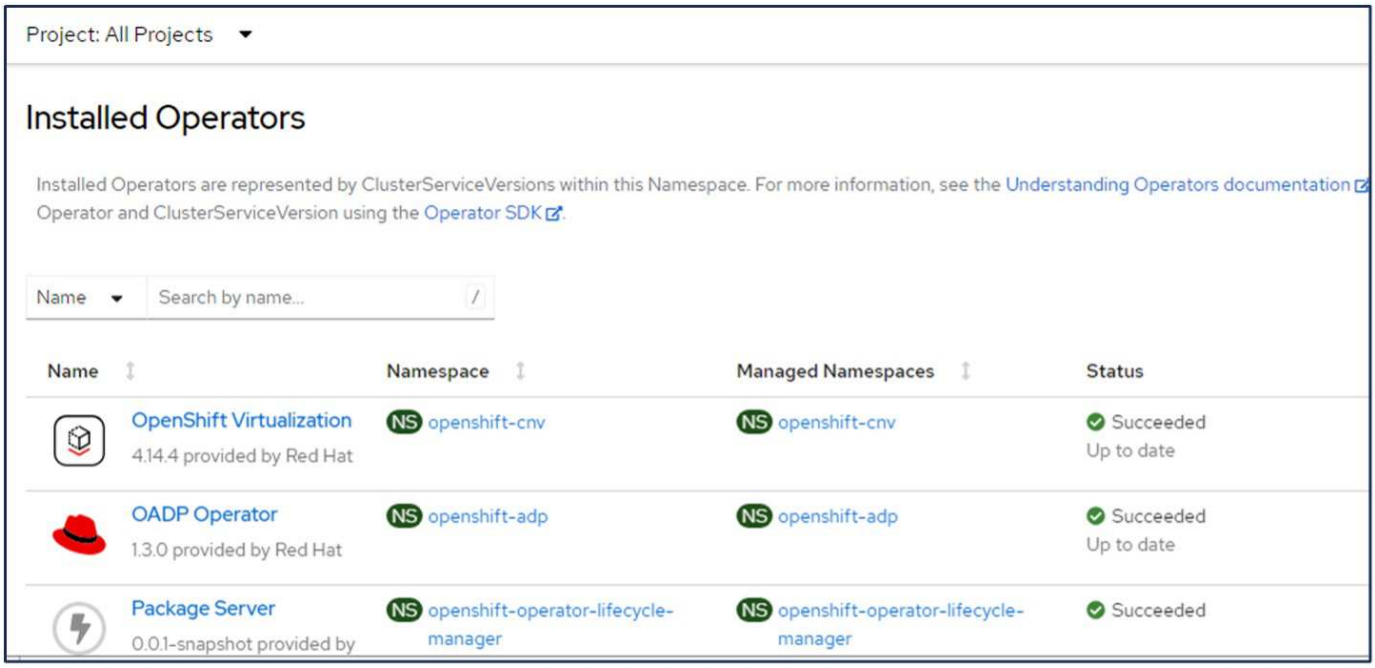
- 在ONTAP集群上配置了 SVM 的Trident后端
- 在 OpenShift 集群上配置 StorageClass，并使用Trident作为配置器
- 在集群上创建的Trident Snapshot 类
- 集群管理员访问 Red Hat OpenShift 集群
- NetApp ONTAP集群的管理员访问权限
- 部署在集群上的应用程序，例如 postgresql
- 安装了 tridentctl 和 oc 工具并添加到 $PATH 的管理员工作站

安装 **OADP Operator** 的步骤

1. 进入集群的 Operator Hub，选择 Red Hat OADP 操作员。在安装页面中，使用所有默认选择并单击安装。在下一页上，再次使用所有默认设置并单击“安装”。 OADP 操作员将安装在命名空间 openshift-adp 中。




OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions


Project: All Projects
Installed Operators
Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation
Operator and ClusterServiceVersion using the Operator SDK
Name
Search by name...
Name
Namespace
Managed Namespaces
Status
OpenShift Virtualization
4.14.4 provided by Red Hat
openshift-cnv
openshift-cnv
Succeeded
Up to date
OADP Operator
1.3.0 provided by Red Hat
openshift-adp
openshift-adp
Succeeded
Up to date
Package Server
0.0.1-snapshot provided by
openshift-operator-lifecycle-manager
openshift-operator-lifecycle-manager
Succeeded

使用 **Ontap S3** 详细信息进行 **Velero** 配置的先决条件

操作员安装成功后，配置Velero的实例。 Velero 可以配置为使用 S3 兼容的对象存储。使用所示步骤配置ONTAP S3"ONTAP文档的对象存储管理部分" 。您将需要ONTAP S3 配置中的以下信息才能与 Velero 集成。

- 可用于访问 S3 的逻辑接口 (LIF)
- 访问 S3 的用户凭证，包括访问密钥和秘密访问密钥
- S3 中用于备份的存储桶名称，具有用户访问权限
- 为了安全访问对象存储，应在对象存储服务器上安装 TLS 证书。

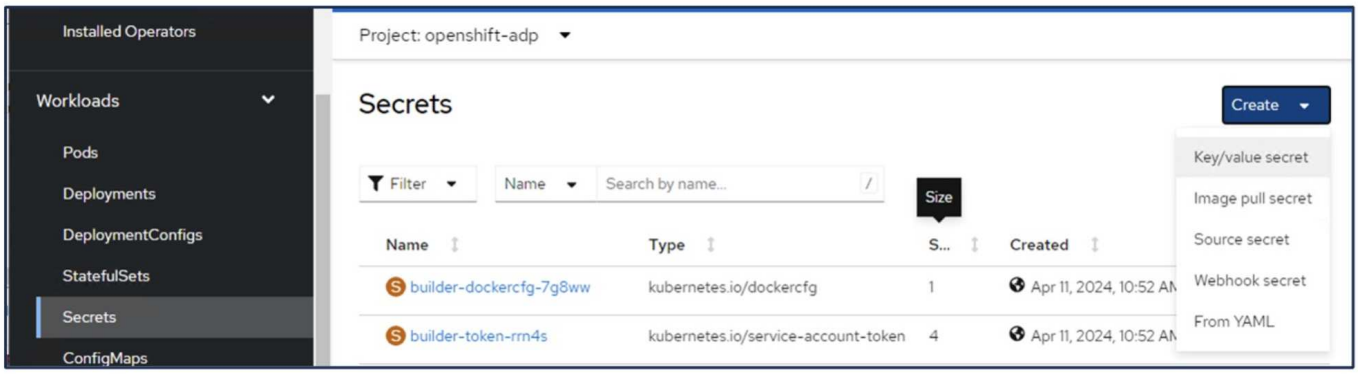
使用 **StorageGrid S3** 详细信息进行 **Velero** 配置的先决条件

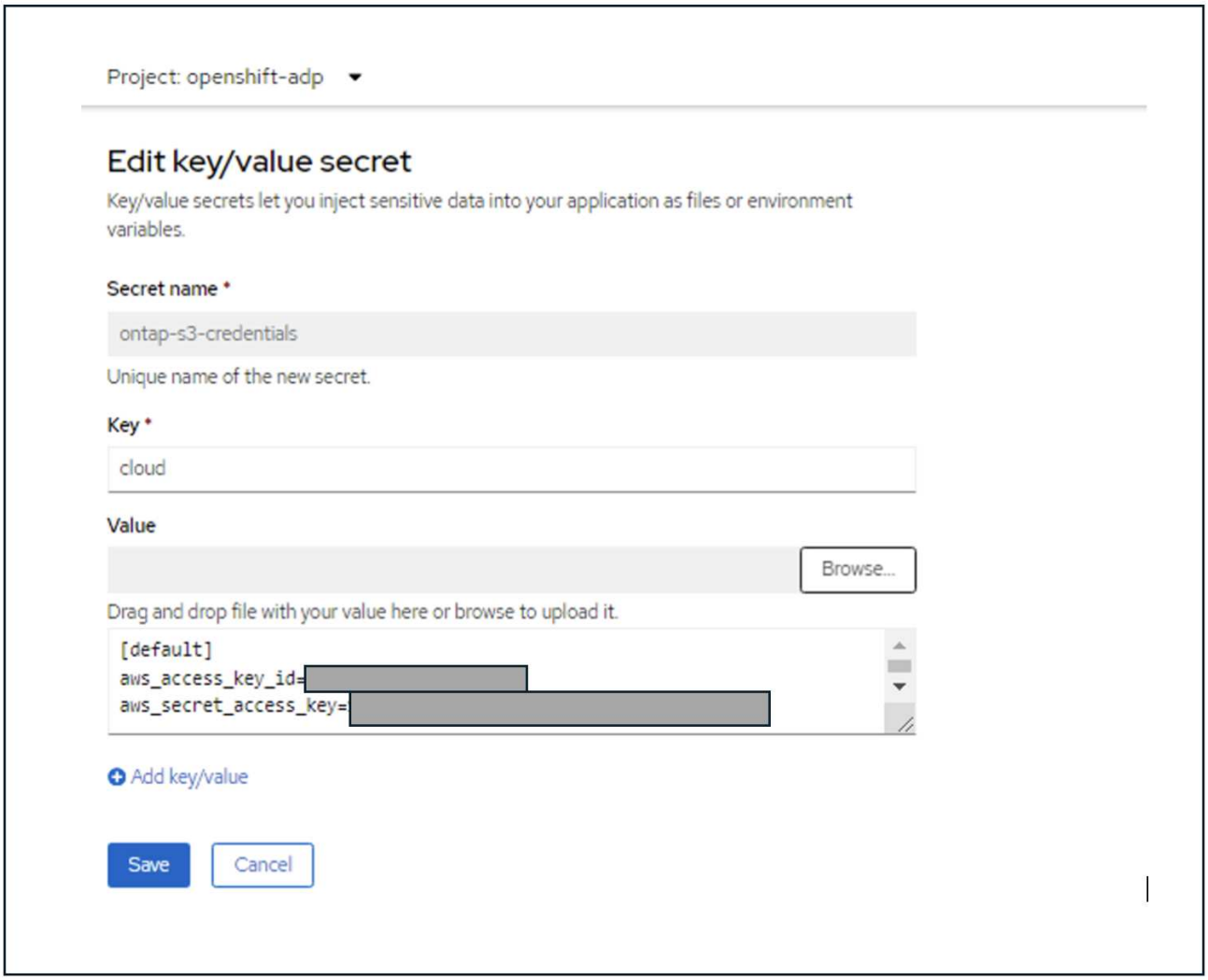
Velero 可以配置为使用 S3 兼容的对象存储。您可以使用以下所示的步骤配置 StorageGrid S3"StorageGrid 文档" 。您将需要 StorageGrid S3 配置中的以下信息才能与 Velero 集成。

- 可用于访问 S3 的端点
- 访问 S3 的用户凭证，包括访问密钥和秘密访问密钥
- S3 中用于备份的存储桶名称，具有用户访问权限
- 为了安全访问对象存储，应在对象存储服务器上安装 TLS 证书。

配置 **Velero** 的步骤

- 首先，为ONTAP S3 用户凭证或 StorageGrid Tenant 用户凭证创建一个密钥。这将用于稍后配置 Velero。您可以从 CLI 或 Web 控制台创建机密。要从 Web 控制台创建密钥，请选择“密钥”，然后单击“键/值密钥”。提供凭证名称、密钥和值的值，如下所示。请务必使用您的 S3 用户的访问密钥 ID 和秘密访问密钥。为秘密指定一个合适的名称。在下面的示例中，创建了一个名为 ontap-s3-credentials 的具有ONTAP S3 用户凭据的密钥。





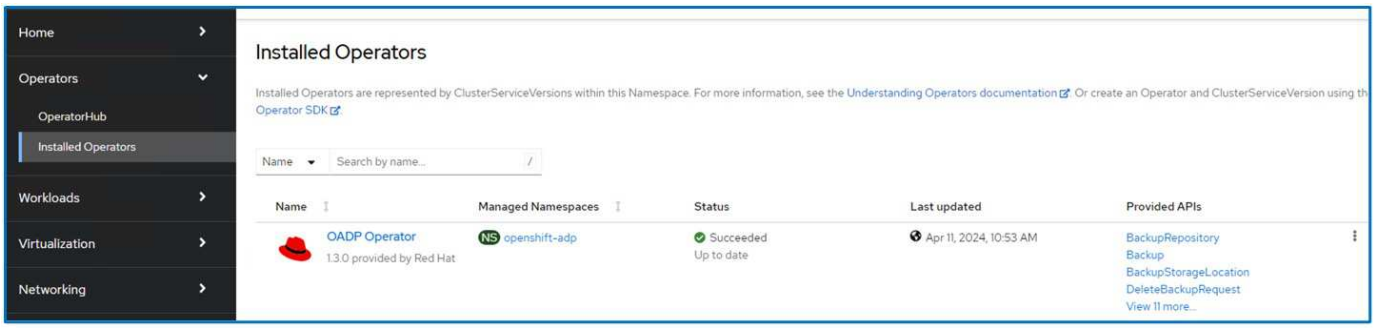
要从 CLI 创建名为 sg-s3-credentials 的密钥，您可以使用以下命令。

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

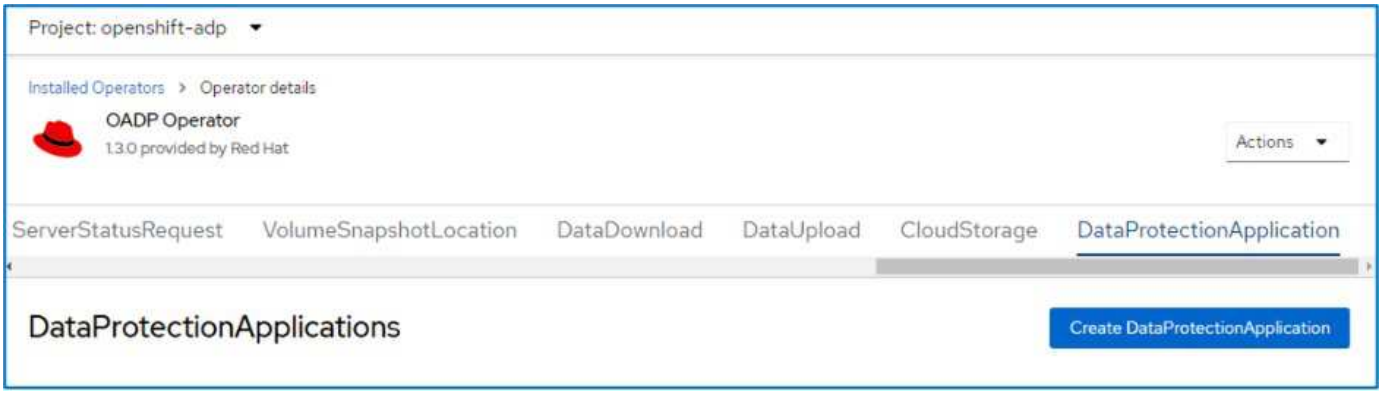
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- 接下来，要配置 Velero，请从 Operators 下的菜单项中选择 Installed Operators，单击 OADP 操作员，然后选择 **DataProtectionApplication** 选项卡。



单击创建 DataProtectionApplication。在表单视图中，为数据保护应用程序提供一个名称或使用默认名称。



现在转到 YAML 视图并替换规范信息，如下面的 yaml 文件示例所示。

使用**ONTAP S3** 作为备份位置配置 **Velero** 的示例 **yaml** 文件

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
```

```
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

使用 **StorageGrid S3** 作为备份位置来配置 **Velero** 的示例 **yaml** 文件

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

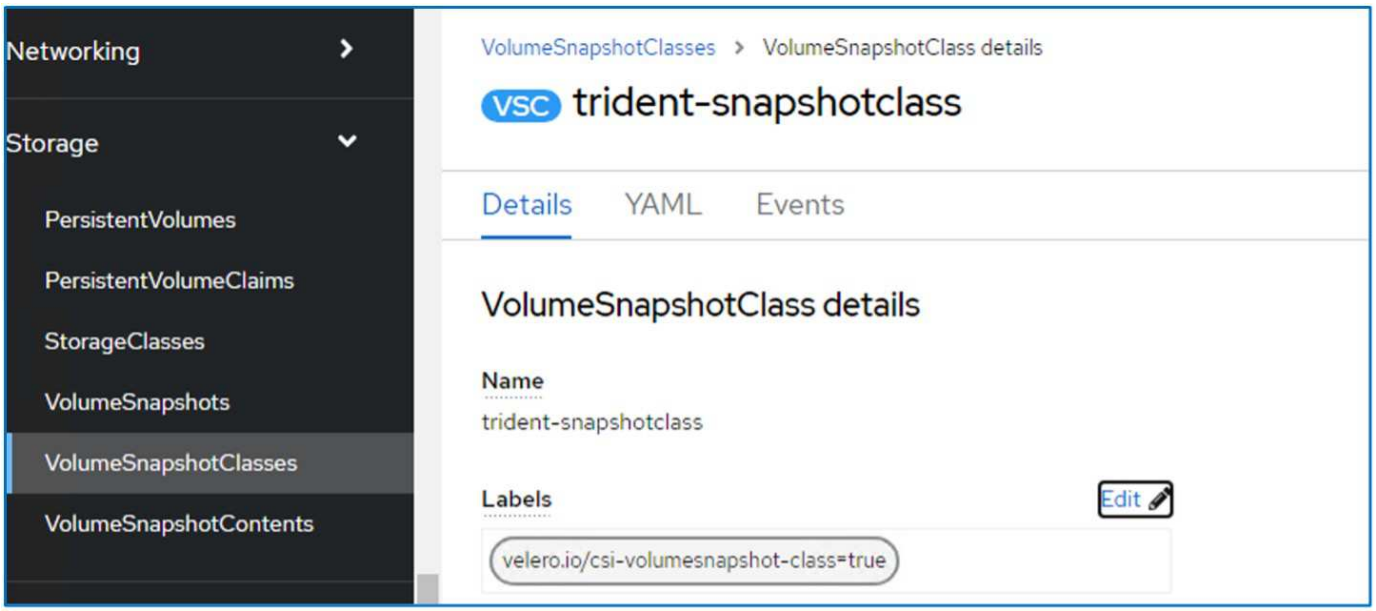
yaml 文件中的 spec 部分应针对类似于上述示例的以下参数进行适当配置

backupLocations ONTAP S3 或 StorageGrid S3（其凭据和其他信息如 yaml 中所示）配置为 velero 的默认 BackupLocation。

snapshotLocations 如果您使用容器存储接口 (CSI) 快照，则无需指定快照位置，因为您将创建 VolumeSnapshotClass CR 来注册 CSI 驱动程序。在我们的示例中，您使用Trident CSI，并且之前已使用Trident CSI 驱动程序创建了 VolumeSnapShotClass CR。

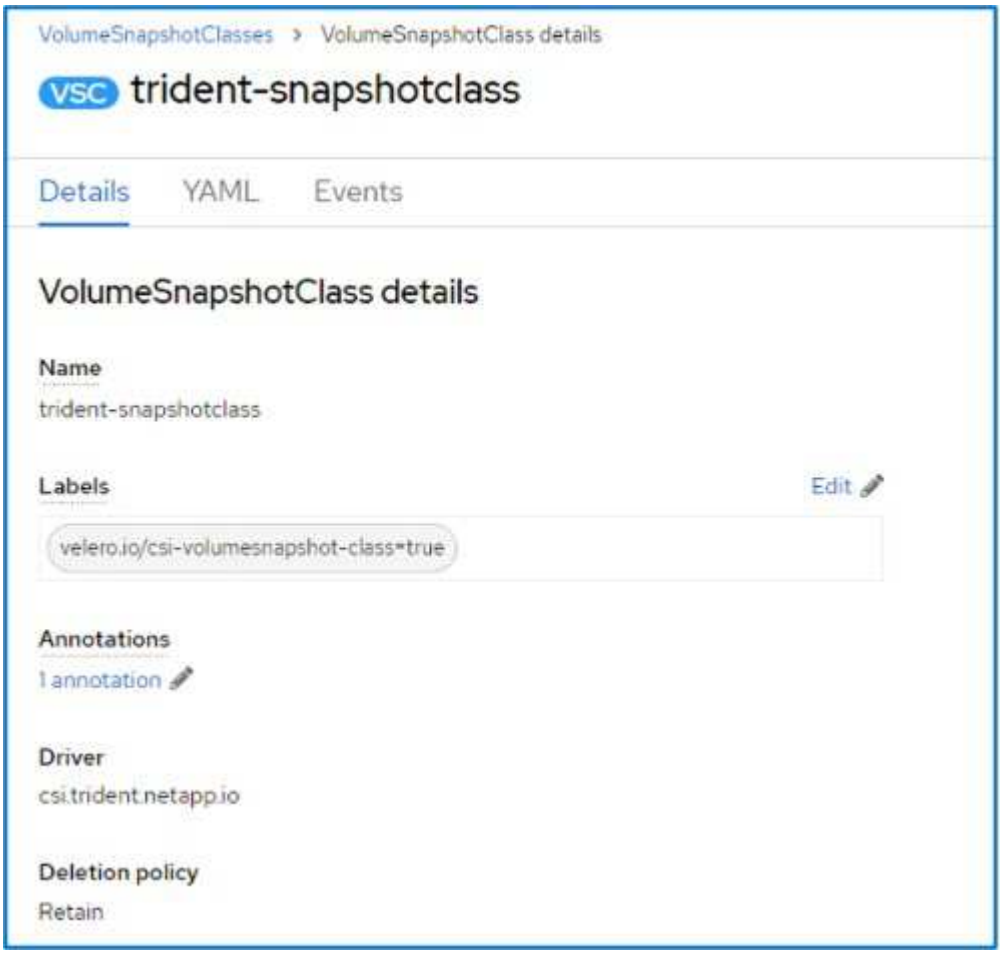
启用 **CSI** 插件 将 csi 添加到 Velero 的默认插件中，以使用 CSI 快照备份持久卷。 Velero CSI 插件用于备份 CSI 支持的 PVC，它将选择集群中设置了 **velero.io/csi-volumesnapshot-class** 标签的 VolumeSnapshotClass。为了这

- 您必须创建 trident VolumeSnapshotClass。
- 编辑 trident-snapshotclass 的标签，并将其设置为 **velero.io/csi-volumesnapshot-class=true**，如下所示。

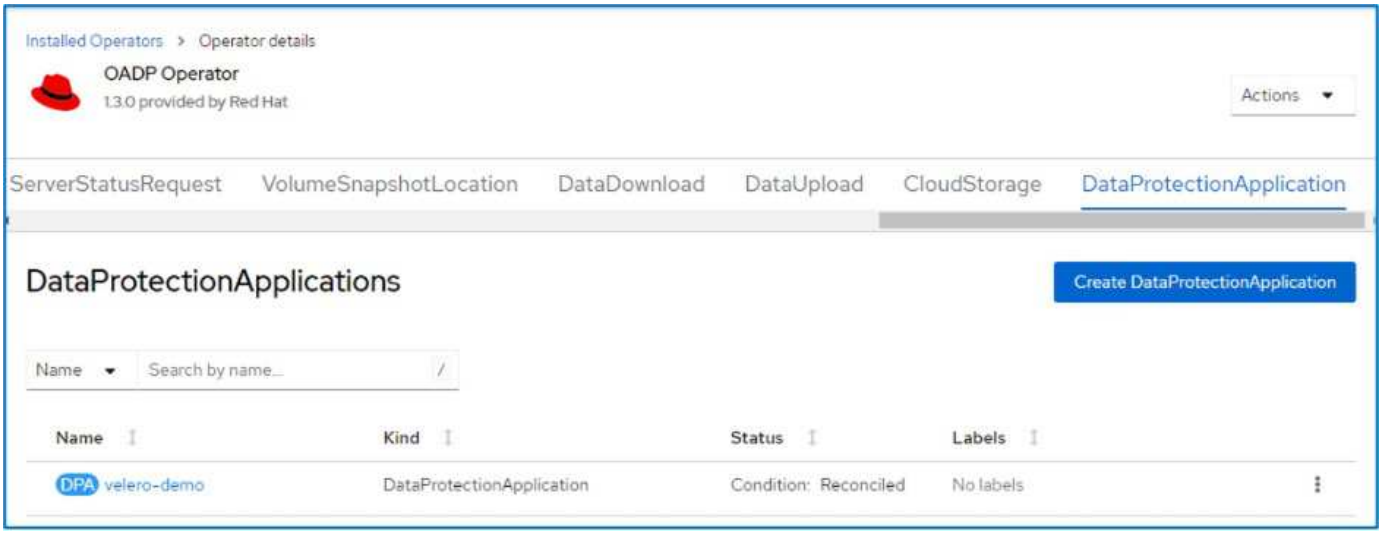


确保即使 VolumeSnapshot 对象被删除，快照也能保留。这可以通过将 **deletionPolicy** 设置为 Retain 来实现。如果不是，删除命名空间将完全丢失其中备份的所有 PVC。

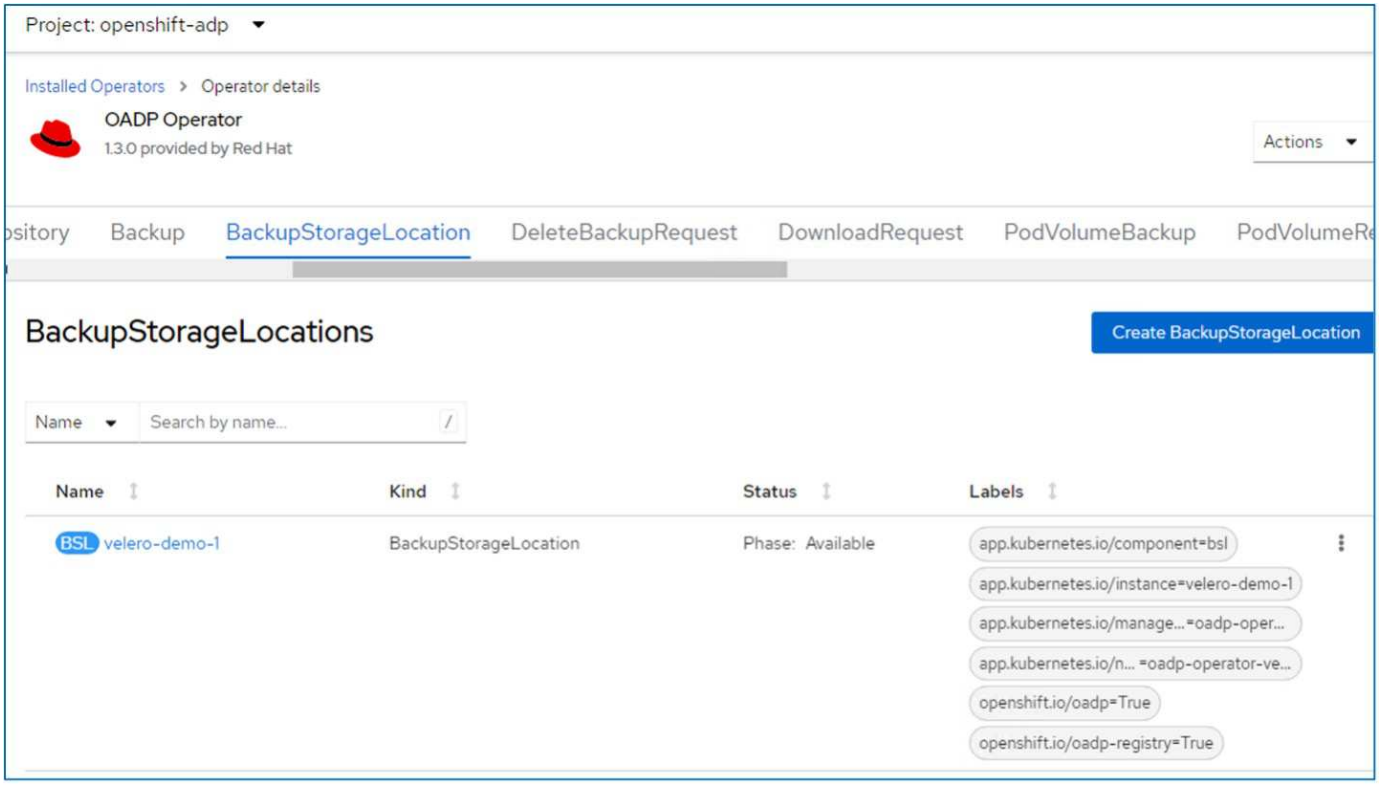
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



确保 DataProtectionApplication 已创建并且处于“状态：Reconciled”。



OADP 操作员将创建相应的 BackupStorageLocation。这将在创建备份时使用。



在 OpenShift Container Platform 中为应用程序创建按需备份

本节概述如何在 OpenShift Virtualization 中为虚拟机创建按需备份。

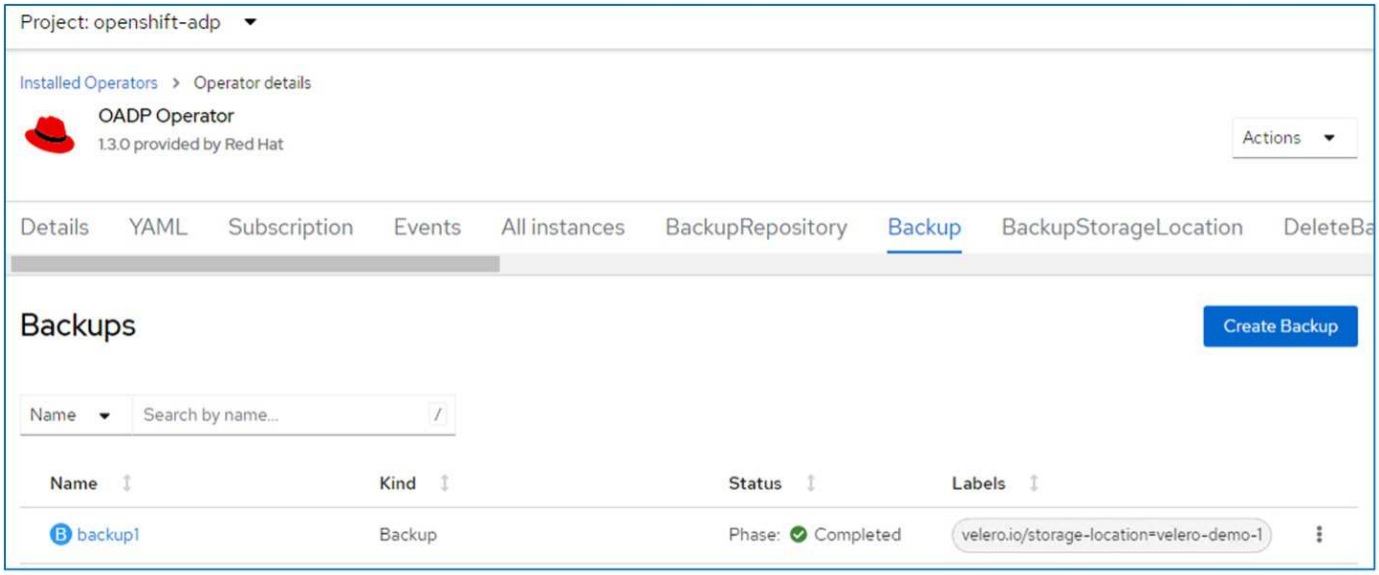
创建应用程序备份的步骤

要创建应用程序的按需备份（应用程序元数据和应用程序的持久卷），请点击 备份 选项卡以创建备份自定义资源（CR）。提供了一个示例 yaml 来创建备份 CR。使用此 yaml，将备份指定命名空间中的应用程序及其持久存储。可以设置其他参数，如 "文档" 中所示。

CSI 将创建指定命名空间中的持久卷和应用程序资源的快照。此快照将存储在 yaml 中指定的备份位置。备份将按照 ttl 的规定在系统中保留 30 天。

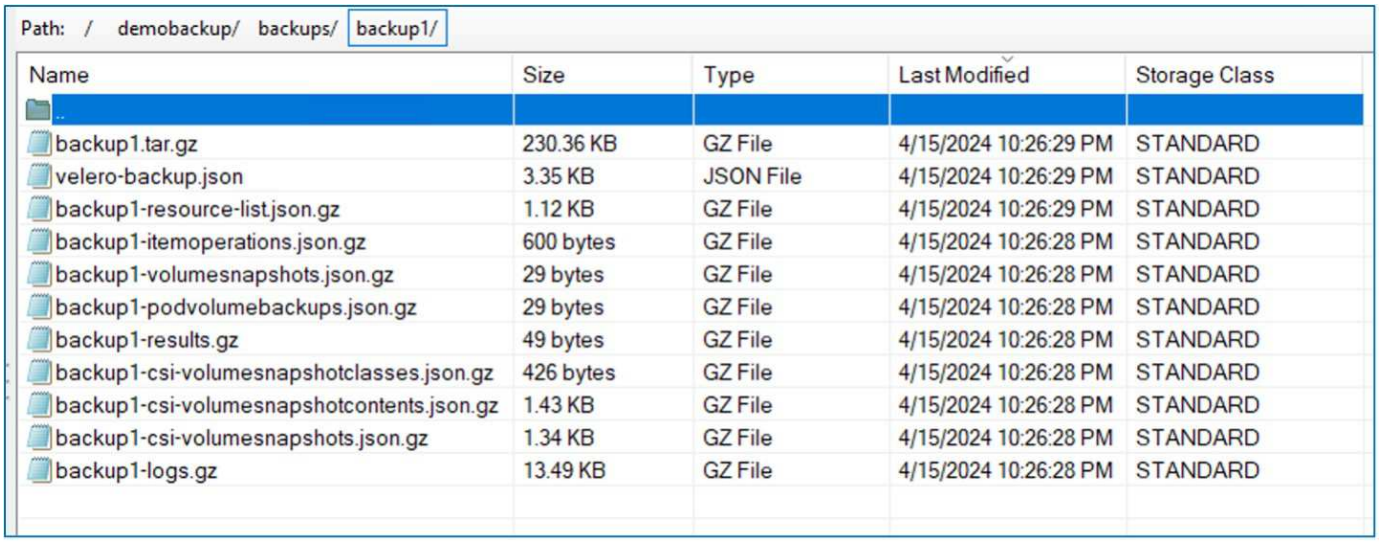
```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
  ttl: 720h0m0s
```

备份完成后，其阶段将显示为已完成。



您可以借助 S3 浏览器应用程序检查对象存储中的备份。备份路径显示在配置的存储桶中，前缀名称为（velero/container-demo-backup）。您可以看到备份的内容包括卷快照、日志和应用程序的其他元数据。

在 StorageGrid 中，您还可以使用租户管理器提供的 S3 控制台来查看备份对象。



为应用程序创建计划备份

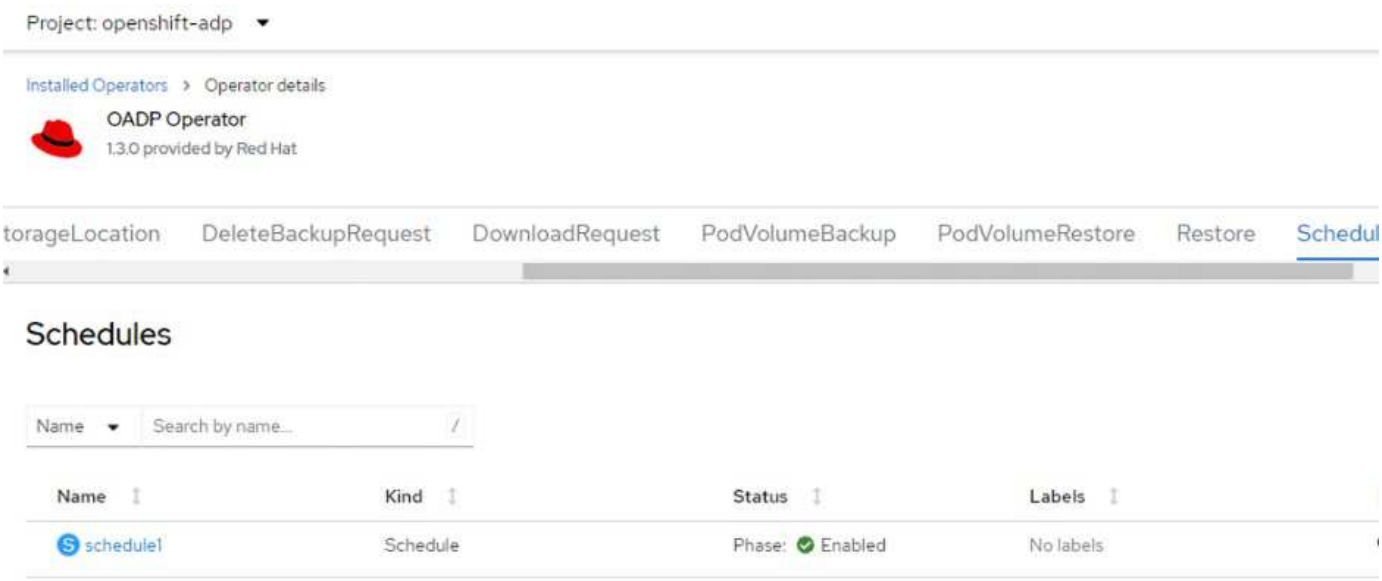
要按计划创建备份，您需要创建计划 CR。该计划只是一个 Cron 表达式，允许您指定要创建备份的时间。下面显示了创建 Schedule CR 的示例 yaml。

```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
```

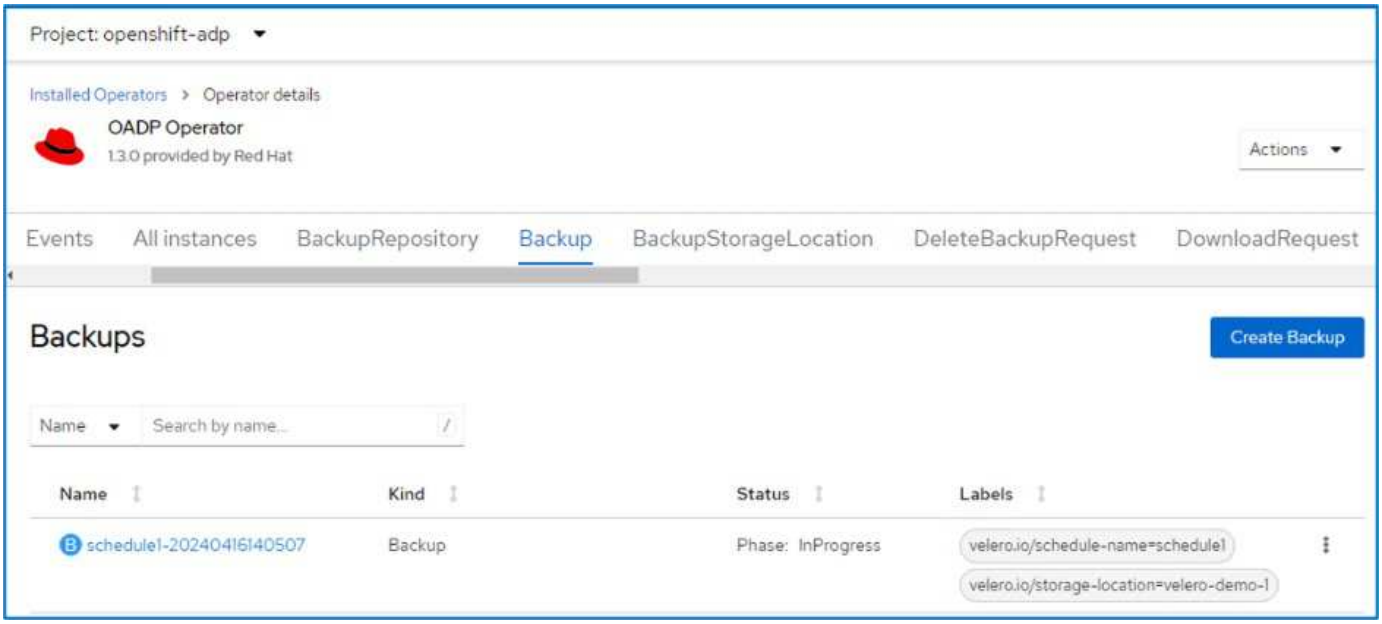
```
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

Cron表达式 0 7 * * * 表示每天7:00创建备份。还指定了要包含在备份中的命名空间和备份的存储位置。因此，不是使用备份 CR，而是使用计划 CR 在指定的时间和频率创建备份。

一旦创建了计划，它将被启用。



备份将根据此计划创建，并可从“备份”选项卡中查看。



将应用程序从一个集群迁移到另一个集群

Velero 的备份和恢复功能使其成为在集群之间迁移数据的有价值的工具。本节介绍如何将

应用程序从一个集群迁移到另一个集群，方法是在一个集群的对象存储中创建应用程序的备份，然后将应用程序从同一对象存储还原到另一个集群。。

▼ 从第一个集群备份

集群 **1** 的先决条件

- 必须在集群上安装Trident 。
- 必须创建 trident 后端和存储类。
- 必须在集群上安装 OADP 操作员。
- 应该配置 DataProtectionApplication。

使用以下规范来配置 DataProtectionApplication 对象。

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

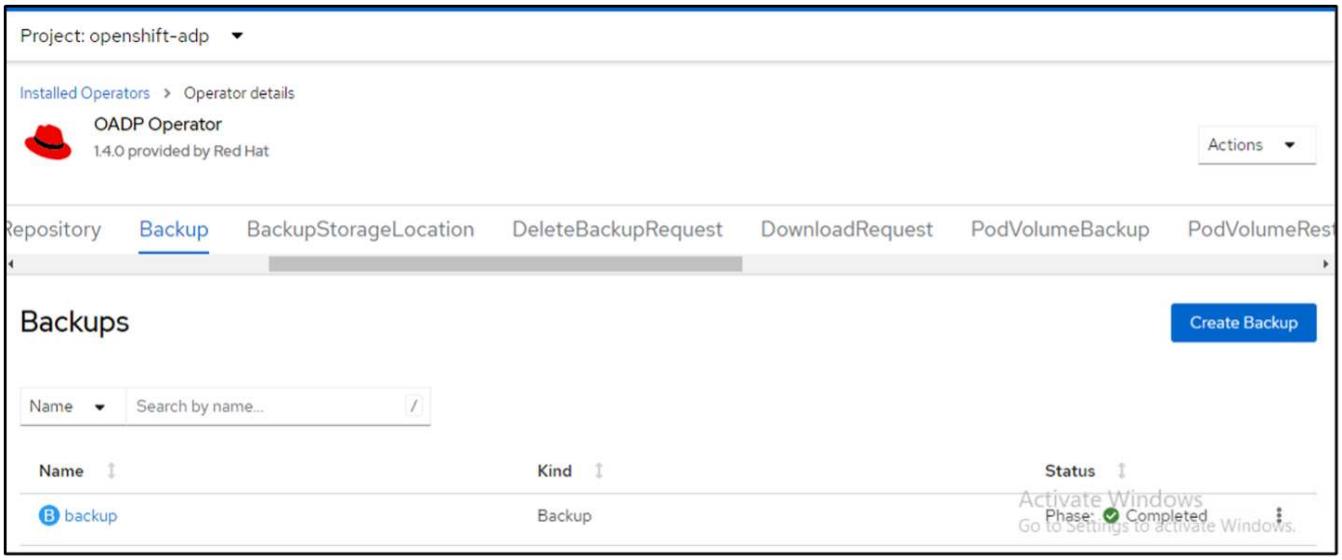
- 在集群上创建一个应用程序并备份该应用程序。例如，安装一个 postgres 应用程序。

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE     VERSION
ocp6-master1   Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-master2   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-master3   Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-worker1   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker2   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker3   Ready    control-plane,master   3d12h   v1.27.15+6147456
[root@localhost ~]# helm install postgresql bitnami/postgresql -n postgresql --create namespace^C
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          4h53m
[root@localhost ~]# oc get pvc -n postgresql
NAME              STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            ontap-nas      4h53m
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                       STORAGECLASS
REASON   AGE
pvc-2e9e982f-54a4-4e7b-8eae-a589e0d9d819   1Gi        RWO            Delete           Bound    trident/basic               ontap-nas
         4h55m
pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         4h53m
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

- 对备份 CR 使用以下规范：

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



您可以点击所有实例选项卡来查看正在创建的不同对象，它们经过不同的阶段，最终进入备份完成阶段。

命名空间 postgresql 中的资源备份将存储在 OADP 规范中的 backupLocation 中指定的对象存储位置 (ONTAP S3) 中。

▼ 恢复到第二个集群

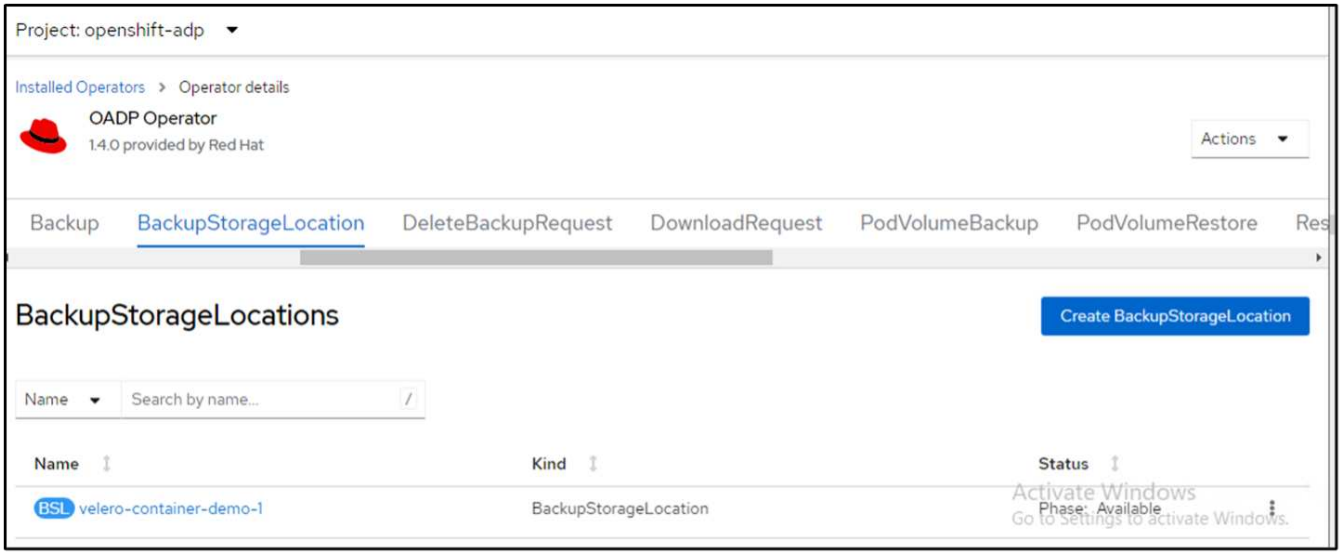
集群 **2** 的先决条件

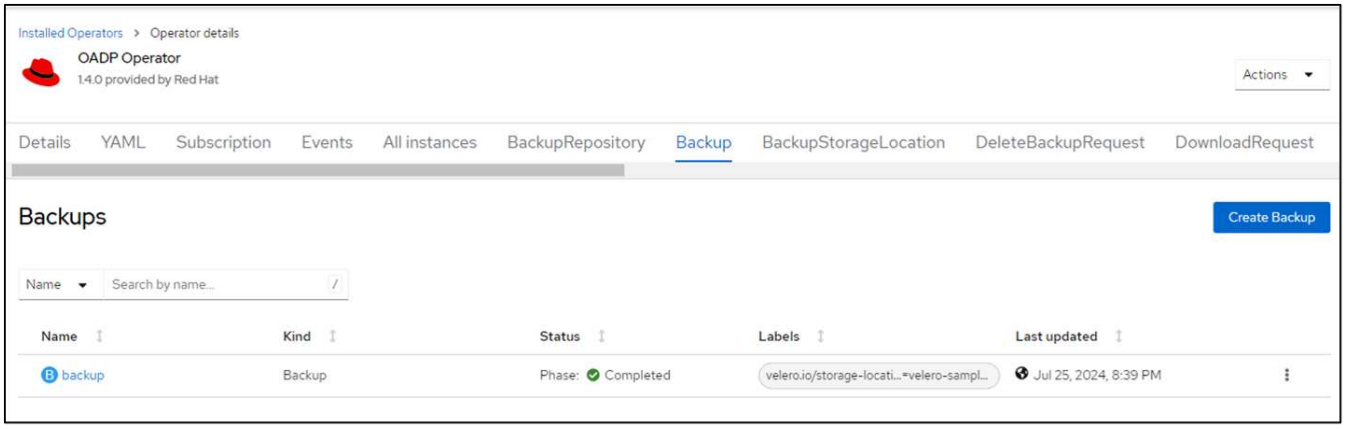
- 必须在集群 2 上安装Trident 。
- postgresql 应用程序一定不能已经安装在 postgresql 命名空间中。
- OADP 操作员必须安装在集群 2 上，并且 BackupStorage Location 必须指向存储第一个集群的备份的相同对象存储位置。
- 备份 CR 必须对第二个集群可见。

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker               3d    v1.27.15+6147456
ocp7-worker2   Ready    worker               3d    v1.27.15+6147456
ocp7-worker3   Ready    worker               3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM              STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic      ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc   vsphere-sc              2d7
h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

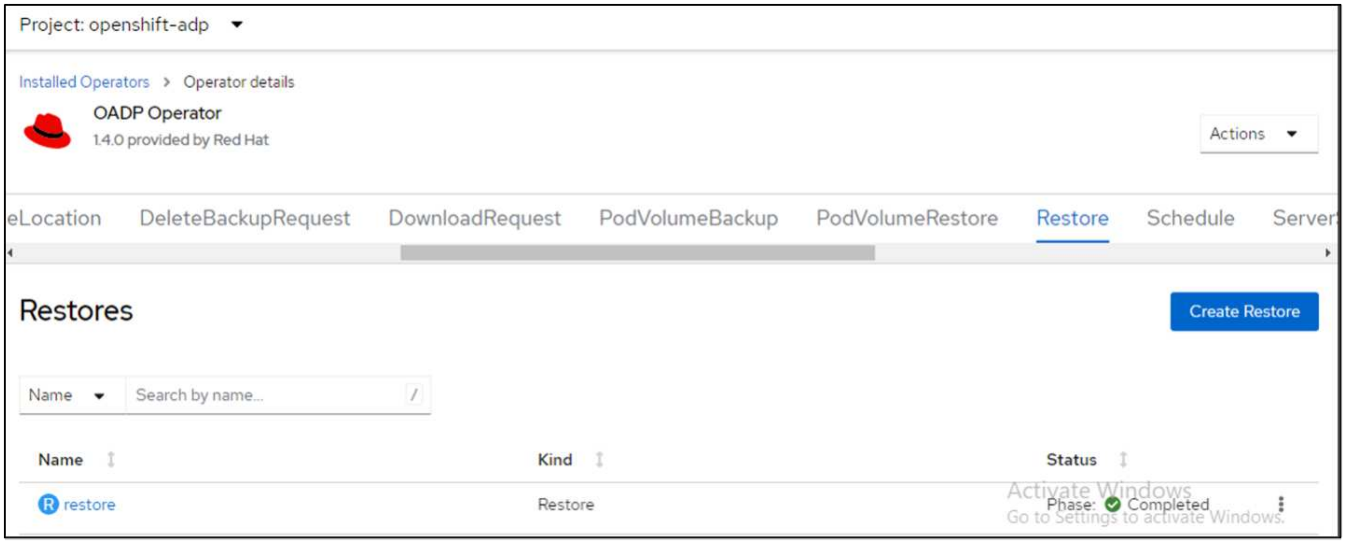


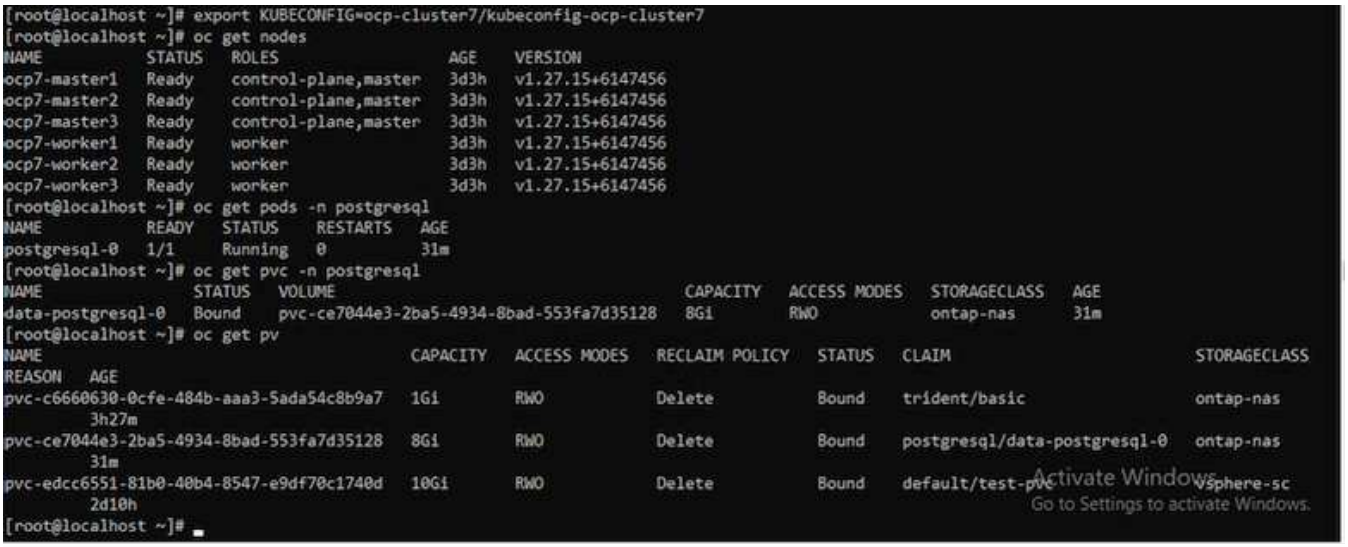


从备份恢复此集群上的应用程序。使用以下 yaml 创建 Restore CR。

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
```

恢复完成后，您将看到 postgresql 应用程序正在此集群上运行，并与 pvc 和相应的 pv 相关联。应用程序的状态与备份时的状态相同。



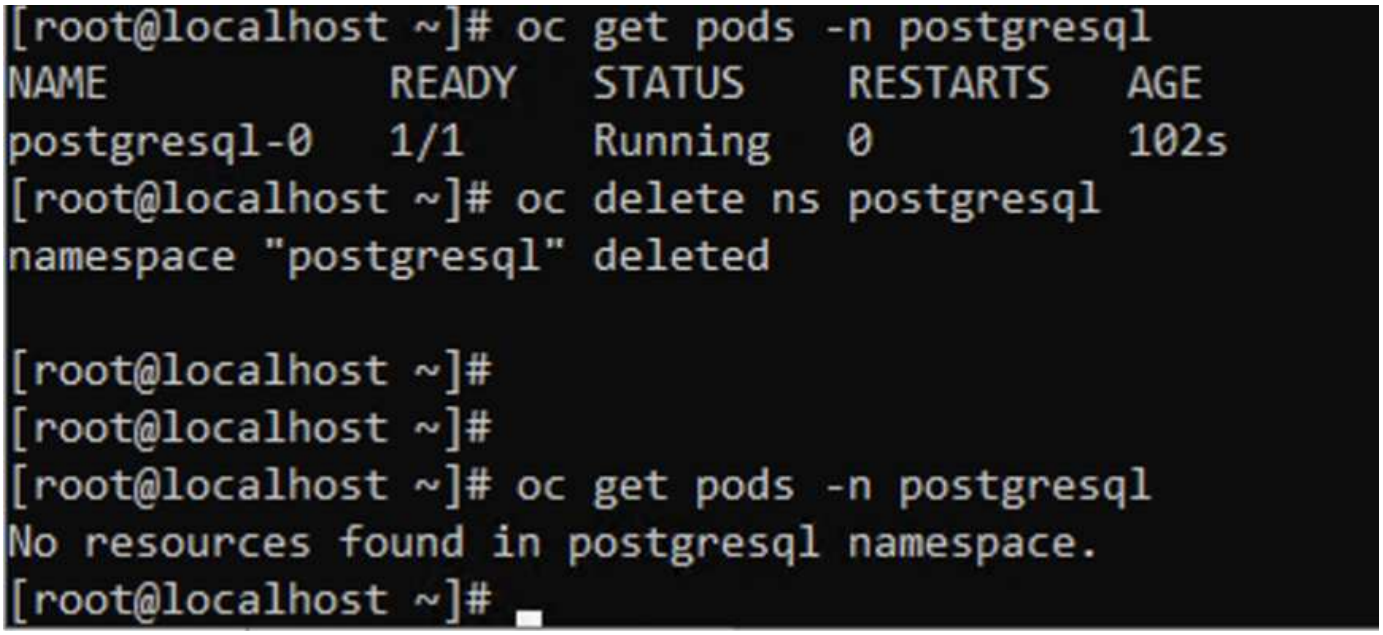


从备份恢复应用程序

本节介绍如何从备份恢复应用程序。

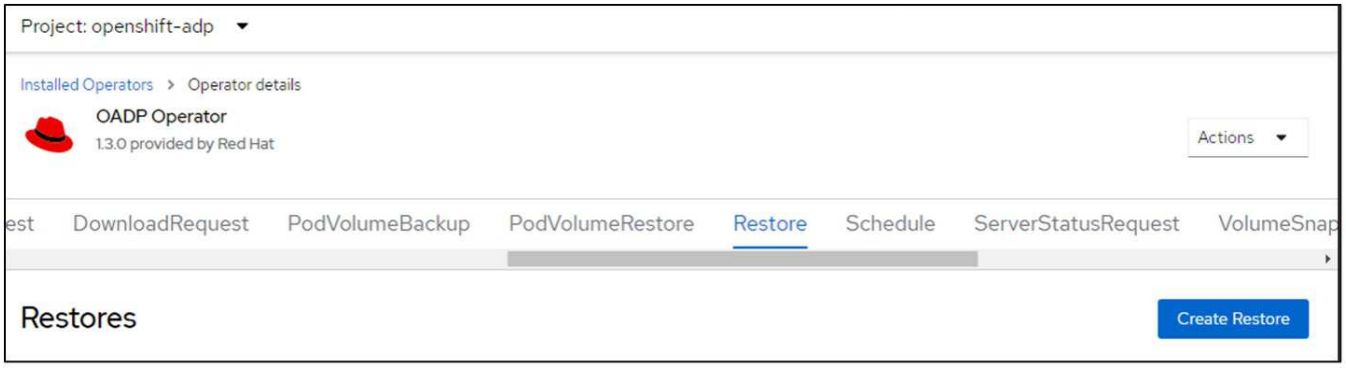
前提条件

为了从备份中恢复，我们假设应用程序所在的命名空间被意外删除了。



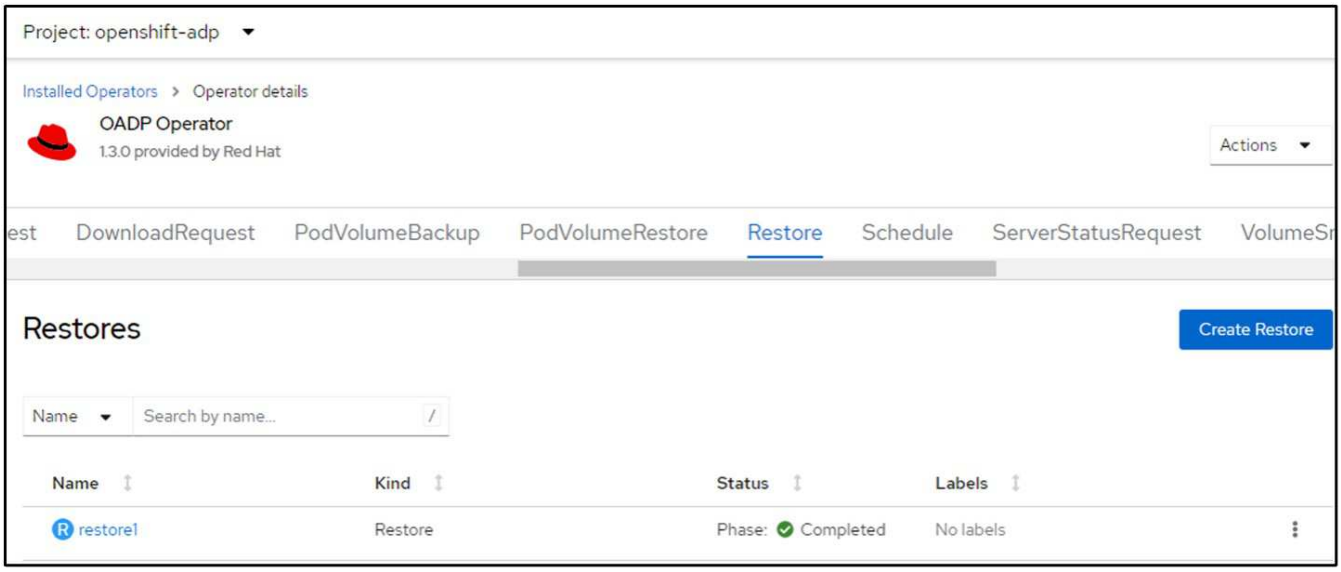
▼ 还原到同一命名空间

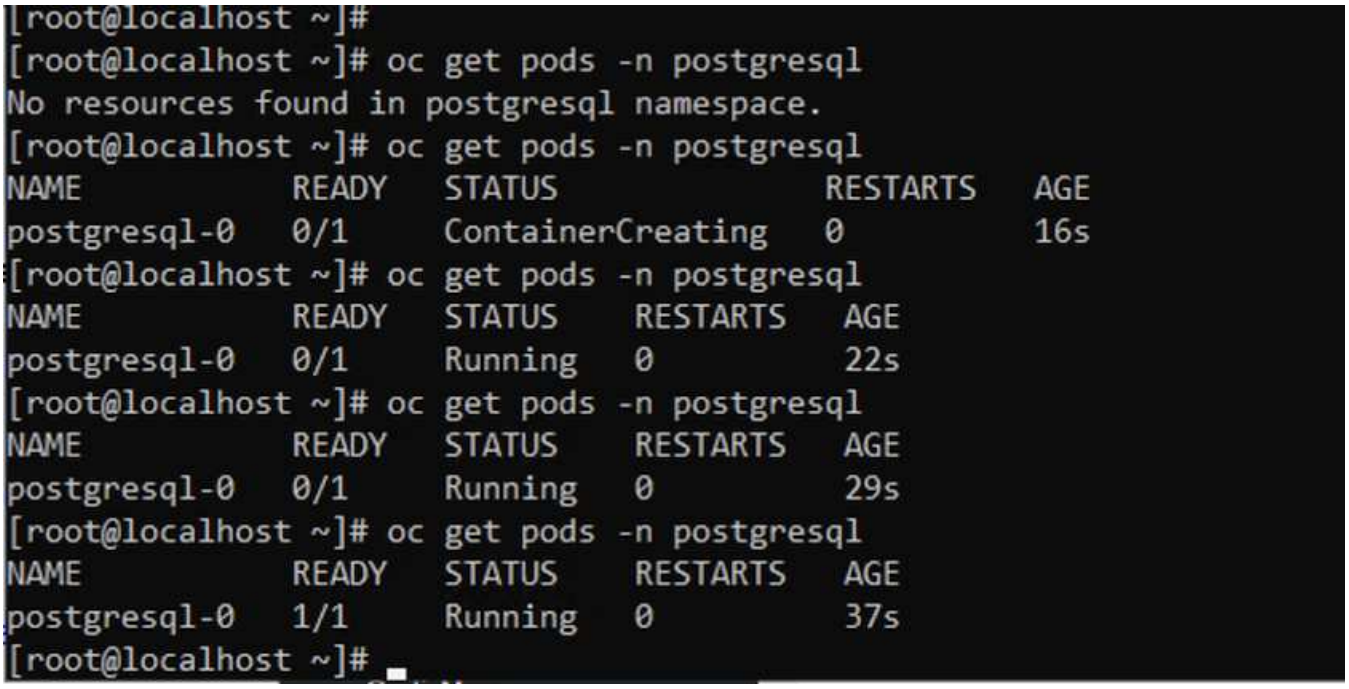
要从我们刚刚创建的备份还原，我们需要创建一个还原自定义资源（CR）。我们需要提供一个名称，提供要从中还原的备份的名称，并将 restorePVs 设置为 true。可以设置其他参数，如 "文档" 中所示。单击“创建”按钮。




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

当阶段显示完成时，您可以看到应用程序已恢复到拍摄快照时的状态。应用程序恢复到相同的命名空间。





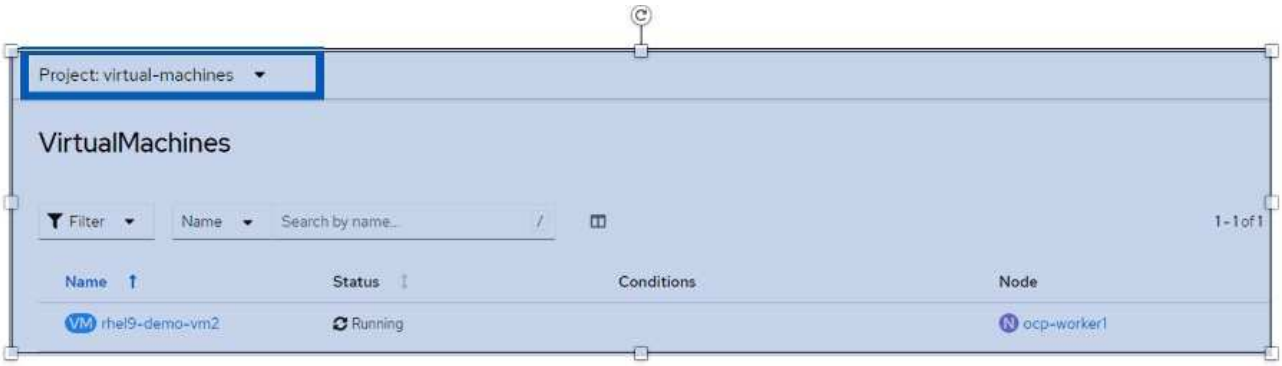
▼ 还原到不同的命名空间

要将应用程序恢复到不同的命名空间，您可以在 Restore CR 的 yaml 定义中提供 namespaceMapping。

以下示例 yaml 文件创建一个 Restore CR，以将应用程序及其持久存储从 postgresql 命名空间恢复到新的命名空间 postgresql-restored。

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

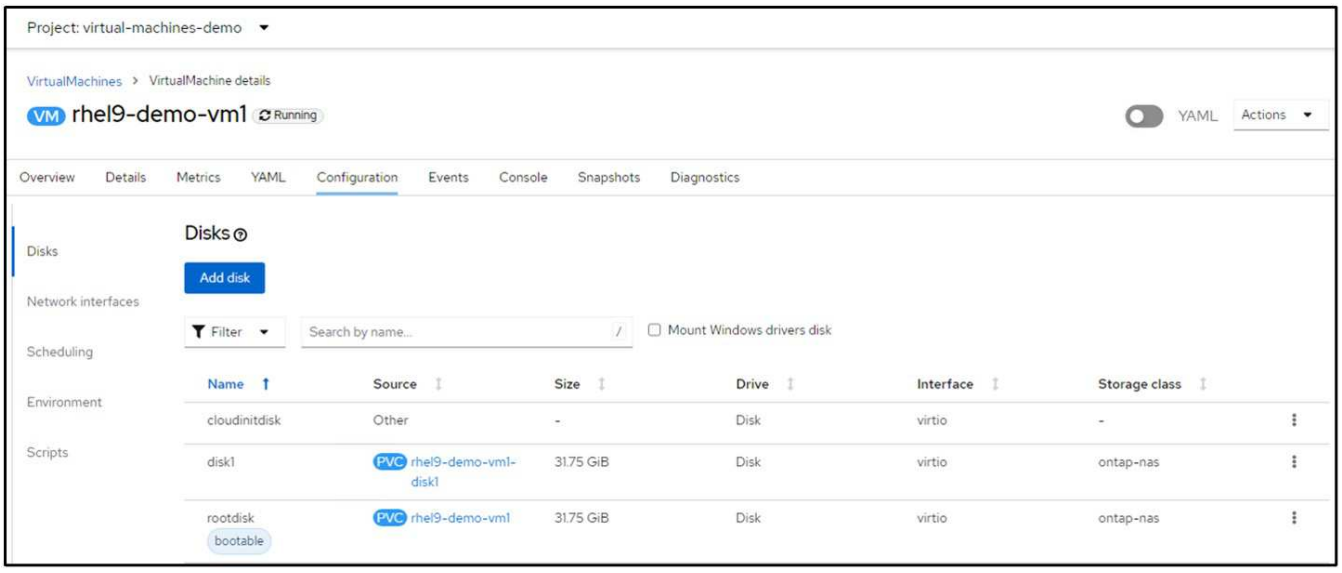
当阶段显示完成时，您可以看到应用程序已恢复到拍摄快照时的状态。应用程序将恢复到 yaml 中指定的不同命名空间。

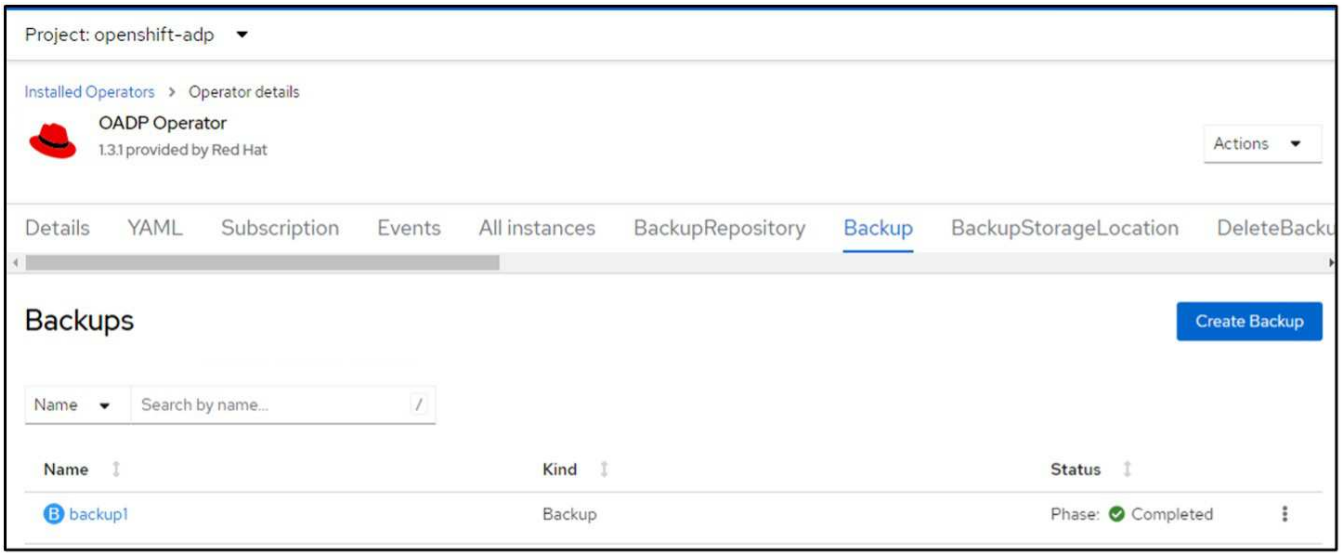


▼ 还原到不同的存储类别

Velero 提供了通过指定 json 补丁来修改恢复期间资源的通用功能。在恢复资源之前，json 补丁会应用到资源上。 json 补丁在 configmap 中指定，并且在 restore 命令中引用该 configmap。此功能使您能够使用不同的存储类别进行恢复。

在下面的示例中，应用程序在部署期间使用 ontap-nas 作为其持久卷的存储类。创建了名为backup-postgresql-ontaps3的应用程序备份。





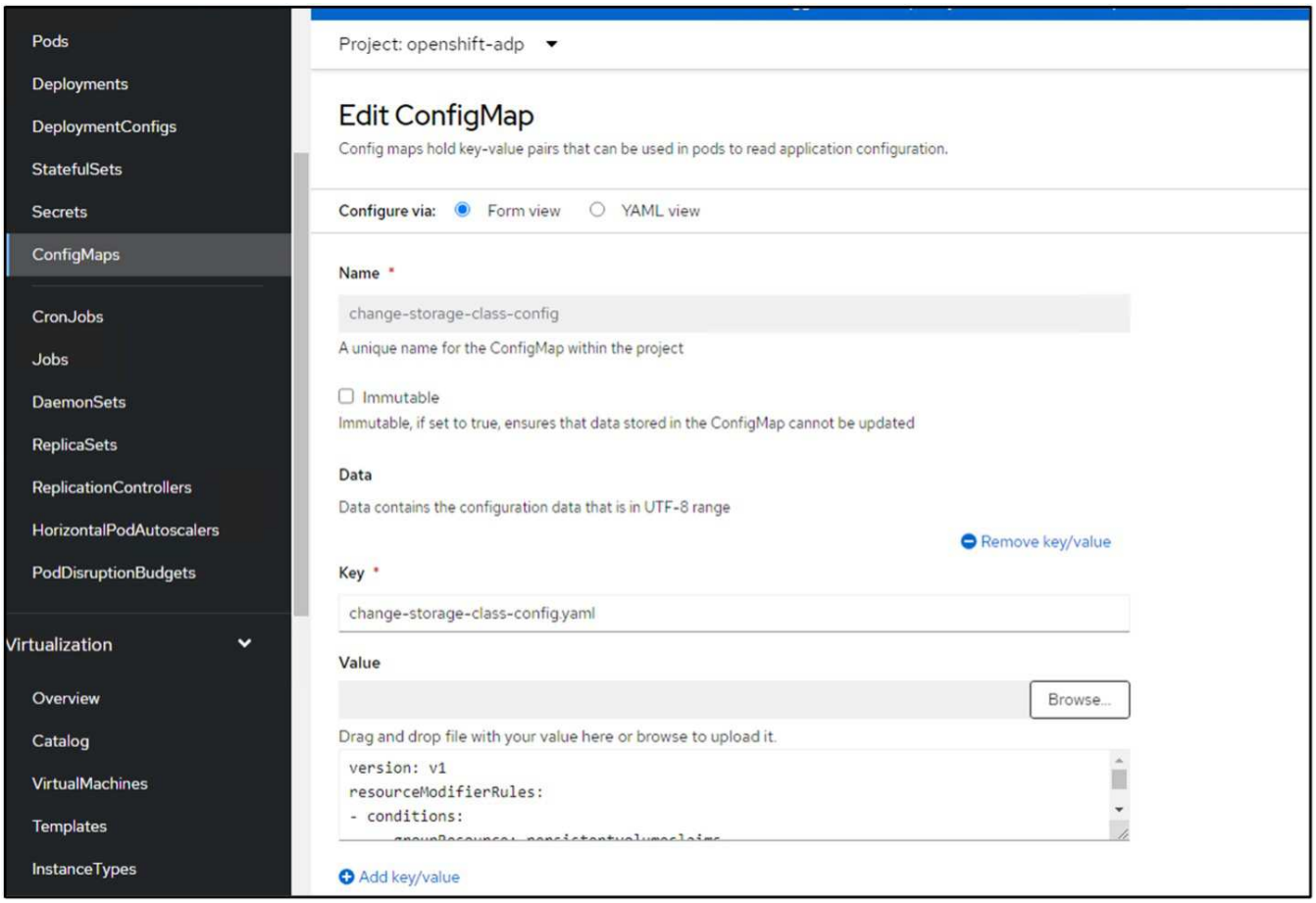
通过卸载应用程序来模拟应用程序的丢失。

要使用不同的存储类（例如 ontap-nas-eco 存储类）恢复虚拟机，您需要执行以下两个步骤：

步骤 **1**

在 openshift-adp 命名空间中创建一个配置映射（控制台），如下所示： 填写屏幕截图中显示的详细信息： 选择命名空间：openshift-adp 名称：change-ontap-sc（可以是任意名称） 键：change-ontap-sc-config.yaml ： 值：

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



生成的配置映射对象应如下所示（CLI）：

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"



BinaryData
====

Events:  <none>
```

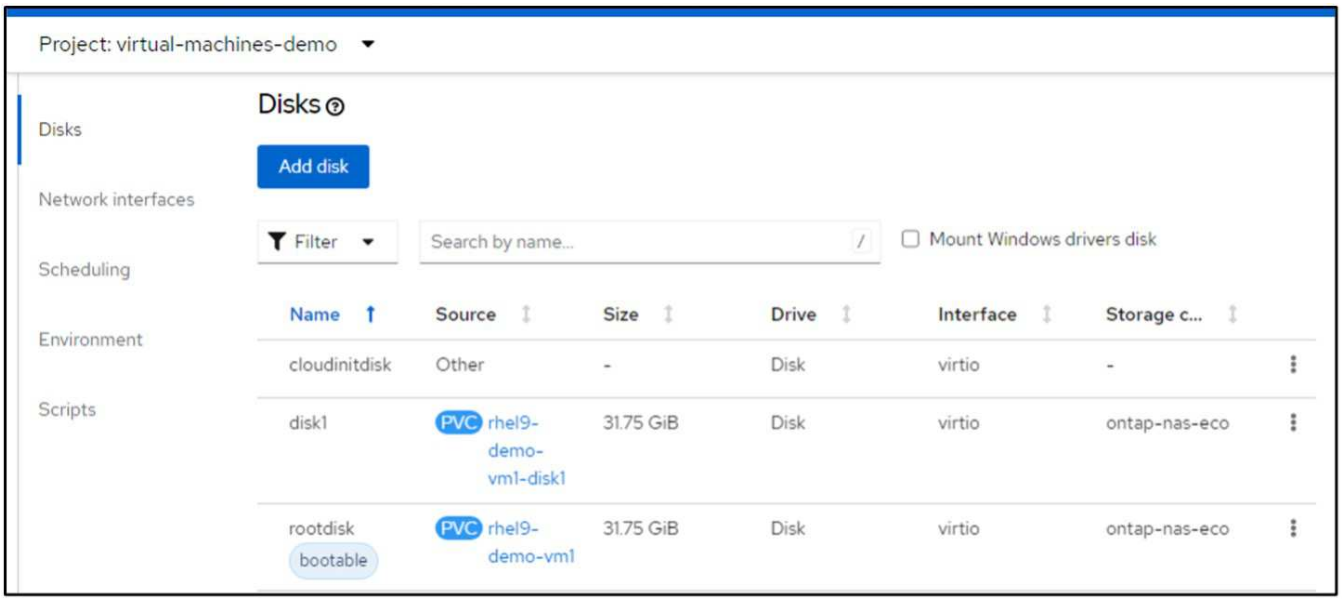
此配置图将在创建恢复时应用资源修改规则。将应用补丁程序将以 rhel 开头的所有持久卷声明的存储类名称替换为 ontap-nas-eco。

步骤 **2**

要恢复虚拟机，请使用 Velero CLI 中的以下命令：

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

该应用程序在使用存储类 ontap-nas-eco 创建的持久卷声明的同一命名空间中恢复。



使用 **Velero** 删除备份和恢复

本节概述如何使用 Velero 删除 OpenShift 容器平台中应用程序的备份和恢复。

列出所有备份

您可以使用 OC CLI 工具或 Velero CLI 工具列出所有备份 CR。按照说明下载 Velero CLI"Velero 文档" 。

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

删除备份

您可以使用 OC CLI 工具删除备份 CR，而不删除对象存储数据。备份将从 CLI/控制台输出中删除。但是，由于相应的备份没有从对象存储中删除，它将重新出现在 CLI/控制台输出中。

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                           AGE
backup-postgresql-ontaps3      23h
schedule1-20240717070005       6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                           AGE
backup-postgresql-ontaps3      23h
backup2                        24s
schedule1-20240717070005       6h50m
[root@localhost ~]#
```

如果您想删除备份 **CR** 和相关的对象存储数据，您可以使用 **Velero CLI** 工具来执行此操作。

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                           STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3      Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                        Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005       Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                           STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3      Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005       Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

删除还原

您可以使用 OC CLI 或 Velero CLI 删除恢复 CR 对象

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                   STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                   STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

观看有关NetApp混合多云解决方案的视频和演示

观看有关使用NetApp的 Amazon Web Services 混合多云解决方案的视频

探索 NetApp 的综合视频库，其中包含NetApp针对 AWS 的混合多云解决方案。观看有关 VMware Cloud on AWS 和Amazon FSx for ONTAP的客户机连接存储、TCO 节省、补充数据存储和迁移工作流程的视频，包括 Windows 和 Linux 场景。

来宾连接存储

使用 iSCSI 的 Windows 客户机连接存储与 FSx ONTAP

使用 NFS 连接 Linux 客户机和 FSx ONTAP 的存储

TCO 和补充数据存储

VMware Cloud on AWS 使用Amazon FSx ONTAP节省 TCO

VMware Cloud on AWS 补充数据存储（带有Amazon FSx ONTAP）

迁移工作流程 (HCX)

VMC 的 VMware HCX 部署和配置设置

使用 VMware HCX for VMC 和 FSx ONTAP进行 vMotion 迁移演示

使用 VMware HCX for VMC 和 FSx ONTAP进行冷迁移演示

观看有关使用NetApp的 Azure VMware 云的混合多云解决方案的视频

探索 NetApp 的综合视频库，其中包含NetApp针对 Azure VMware 解决方案 (AVS) 的混合多云解决方案。该系列包括有关补充数据存储、灾难恢复和迁移工作流程的视频。

补充数据存储

Azure VMware 解决方案补充数据存储概述（包含Azure NetApp Files）

灾难恢复

带有Cloud Volumes ONTAP、 SnapCenter和 JetStream 的 Azure VMware 解决方案 DR

迁移工作流程 (HCX)

使用 VMware HCX 进行 AVS 和 ANF 冷迁移演示

使用 VMware HCX 进行 AVS 和 ANF 的 vMotion 演示

使用 VMware HCX 进行 AVS 和 ANF 批量迁移演示

观看有关NetApp的 Red Hat OpenShift 混合多云解决方案的视频

探索 NetApp 的综合视频库，其中包含NetApp为 Red Hat OpenShift 提供的混合多云解决方案。该集合包括使用 FSx ONTAP对 AWS 上的 OpenShift (ROSA) 进行快照和恢复的演示、与Trident 的集成、应用程序的故障转移和故障恢复，以及使用 Ansible 在FlexPod上自动部署 Oracle RAC。

快照和恢复

使用Amazon FSx ONTAP存储为 AWS (ROSA) 集群上的 Red Hat OpenShift Service 应用程序进行快照/还原

存储集成

FSx ONTAP与Trident的集成

故障转移和故障恢复

使用 FSx ONTAP在 ROSA 上实现应用程序的故障转移和故障恢复

解决方案自动化



使用 **Ansible** 在**FlexPod**上自动部署 **Oracle 19c RAC**

阅读NetApp专家的云解决方案博客

阅读博客，了解有关将ONTAP存储与NetApp云解决方案集成的实用指导和最佳实践。

VMware 与 AWS 和Amazon FSx for ONTAP 的集成

- "使用 Amazon EC2 和Amazon FSx ONTAP iSCSI 协议将 VMware VM 迁移到 AWS"
- "Amazon EVS 现已与 FSx for ONTAP集成"
- "Amazon EVS 宣布支持 FSx for ONTAP"
- "使用 VMware HCX 配置带有 FSx ONTAP和 VMware Cloud on AWS SDDC 的混合云"

Azure VMware 解决方案

- "优化任何云中的存储和数据密集型 VMware 工作负载"
- "VMware 工作负载迁移到 Azure VMware Solution？请先阅读此内容。"

Google Cloud VMware 引擎

- "Google Cloud NetApp Volumes数据存储区支持 Google Cloud VMware Engine (NetApp)"
- "如何将NetApp Volumes 用作 Google Cloud VMware Engine 的数据存储区（Google）"
- "NetApp博客 - 将存储丰富的应用程序迁移到 Google Cloud 的更好方法"

数据保护和管理

- "使用 SnapCenter 插件和适用于虚拟机的 NetApp Backup and Recovery 为 VMware 提供 3-2-1 数据保护"
- "利用NetApp Cloud Insights实现现代数据中心的可观察性"

NetApp适用于 OpenShift 容器工作负载

- "NetApp ONTAP兼作 Red Hat OpenShift 容器平台中的日志存储"

VMware 主权云

- "推出全新主权云计划"

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 徽标和NetApp商标页面上列出的标志是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。

"https://www.netapp.com/company/legal/trademarks/"

专利

NetApp拥有的专利的最新列表可以在以下位置找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

版权信息

版权所有 © 2026 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。