公共云和混合云

NetApp Solutions

NetApp
May 10, 2024

目录

公共云和混合云

采用VMware解决方案的NetApp混合多云

适用于公有云的 VMware

NetApp混合多云与VMware概述

大多数 IT 组织都采用混合云优先的方法。这些组织处于转型阶段，客户正在评估其当前 IT 环境，然后根据评估和发现练习将工作负载迁移到云。

客户迁移到云的因素包括弹性和突发，数据中心退出，数据中心整合，寿命终结情形，合并， 采集等。迁移的原因可能因组织及其各自的业务优先级而异。迁移到混合云时，在云中选择合适的存储对于充分发挥云部署和弹性的潜能非常重要。

公有云中的 VMware 云选项

本节介绍每个云提供商如何在其各自的公共云产品中支持VMware软件定义的数据中心(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，支持在 Microsoft Azure 公有云中实现完全正常运行的 VMware SDDC 。Azure VMware 解决方案是由 Microsoft 全面管理和支持的第一方解决方案，由 VMware 利用 Azure 基础架构进行验证。这意味着，在部署 Azure VMware 解决方案时，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 ， 和 NSX 实现网络连接和安全性，同时充分利用 Microsoft Azure 的全球影响力，一流的数据中心设施以及邻近丰富的原生 Azure 服务和解决方案生态系统的优势。

基于 **AWS** 的 **VMware Cloud**

基于 AWS 的 VMware 云通过优化对原生 AWS 服务的访问，将 VMware 企业级 SDDC 软件引入 AWS 云。VMware Cloud on AWS 由 VMware Cloud Foundation 提供支持，它将 VMware 的计算，存储和网络虚拟化产品（ VMware vSphere ， VMware vSAN 和 VMware NSX ）与 VMware vCenter Server 管理相集成，并经过优化，可在专用的弹性裸机 AWS 基础架构上运行。

Google Cloud VMware 引擎

Google Cloud VMware Engine 是一款基础架构即服务（ Infrastructure-as-a-Service ， IaaS ）产品，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 ）构建此服务支持快速迁移到云，将现有 VMware 工作负载从内部环境无缝迁移或扩展到 Google Cloud Platform ，而无需花费成本，精力或风险来重新构建应用程序或重新调整操作。这是一项由 Google 销售和支持的服务，与 VMware 密切合作。

SDDC 私有云和 NetApp Cloud Volumes 主机代管功能可提供最佳性能，并将网络延迟降至最低。

您知道吗？

无论使用何种云，在部署 VMware SDDC 时，初始集群都包括以下产品：

- 用于计算虚拟化的 VMware ESXi 主机，以及用于管理的 vCenter Server 设备
- VMware vSAN 超融合存储，整合了每个 ESXi 主机的物理存储资产
- VMware NSX 用于虚拟网络连接和安全性，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的 VMware 解决方案上横向扩展的客户，默认的超融合基础架构要求扩展应同时位于计算和存储资源上。

通过与 Azure NetApp Files ，适用于 NetApp ONTAP 的 Amazon FSx ，适用于所有三种主要超大规模云产品的 Cloud Volumes ONTAP 以及适用于 Google Cloud 的 Cloud Volumes Service 等 NetApp Cloud Volumes 相集成，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。

注释：

- VMware 不建议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 TCO 增加。
- 只能使用一个 vSAN 环境。因此，所有存储流量都将直接与生产工作负载竞争。
- 无法提供多个性能层来满足应用程序要求，性能和成本要求。
- 很容易达到基于集群主机构建的 vSAN 的存储容量限制。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永久性存储。

Azure NetApp Files ，适用于 NetApp ONTAP 的 Amazon FSx ， Cloud Volumes ONTAP （在所有三个主要超大规模企业中均有提供）和适用于 Google Cloud 的 Cloud Volumes Service 可与子虚拟机结合使用。此混合存储架构由一个 vSAN 数据存储库组成，用于存放子操作系统和应用程序二进制数据。应用程序数据通过基于子系统的 iSCSI 启动程序或 NFS/SMB 挂载连接到 VM ，这些启动程序或挂载可分别直接与适用于 NetApp ONTAP 的 Amazon FSx ， Cloud Volume ONTAP ， Azure NetApp Files 和适用于 Google Cloud 的 Cloud Volumes Service 进行通信。此配置可让您轻松克服存储容量方面的挑战，就像使用 vSAN 一样，可用空间取决于可宽空间和所使用的存储策略。

我们来考虑一下 AWS 上的 VMware Cloud 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 10 TB ）。
- 在添加其他主机之前要保留的可宽空间 = 25% = （ .25 x 31.1TB ） = 7.6 TB 。
- 可宽空间扣除后的可用原始容量 = 23.4TB
- 有效可用空间取决于应用的存储策略。

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 = 17.5 TB （可用原始容量 /1.33 ）

因此，使用 NetApp Cloud Volumes 作为子系统连接的存储有助于扩展存储和优化 TCO ，同时满足性能和数据保护要求。

在编写本文档时，来宾存储是唯一可用的选项。 随着NFS数据存储库支持的补充提供、我们将提供其他文档 "此处"。

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 数据存储库上，以满足任何特定延迟要求，因为它们是主机本身的一部分且位于邻近位置。对事务处理延迟可接受的任何工作负载 VM 使用来宾机制。
- 使用 NetApp SnapMirror ® 技术将工作负载数据从内部 ONTAP 系统复制到 Cloud Volumes ONTAP 或 Amazon FSx for NetApp ONTAP ，以便使用块级机制轻松迁移。这不适用于 Azure NetApp Files 和 Cloud Volumes 服务。要将数据迁移到Azure NetApp Files或Cloud Volumes Services、请根据使用的文件协议使用NetApp XCP、BlueXP复制和同步、rysnc或Robocopy。
- 测试显示，从相应 SDDC 访问存储时会出现 2 到 4 毫秒的额外延迟。在映射存储时，将此额外延迟考虑到应用程序要求。
- 要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 启动程序，更新 SMB 共享的 DNS 以及在 fstab 中更新 NFS 挂载点。
- 确保已在 VM 中正确配置来宾系统内 Microsoft 多路径 I/O （ MPIO ），防火墙和磁盘超时注册表设置。

此适用场景子系统仅连接存储。

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，提高计算到存储的密度。
- 可用于减少主机数量，从而降低总 TCO 。
- 计算节点故障不会影响存储性能。
- 借助 Azure NetApp Files 的卷重塑和动态服务级别功能，您可以根据稳定状态工作负载进行规模估算，从而防止过度配置，从而优化成本。
- Cloud Volumes ONTAP 的存储效率，云分层和实例类型修改功能可以提供最佳的存储添加和扩展方式。
- 防止过度配置存储资源仅在需要时添加。
- 通过高效的 Snapshot 副本和克隆，您可以快速创建副本，而不会对性能造成任何影响。
- 通过从 Snapshot 副本快速恢复来帮助解决勒索软件攻击。
- 提供基于增量块传输的高效区域灾难恢复以及跨区域的集成备份块级别，从而提供更好的 RPO 和 RTO 。

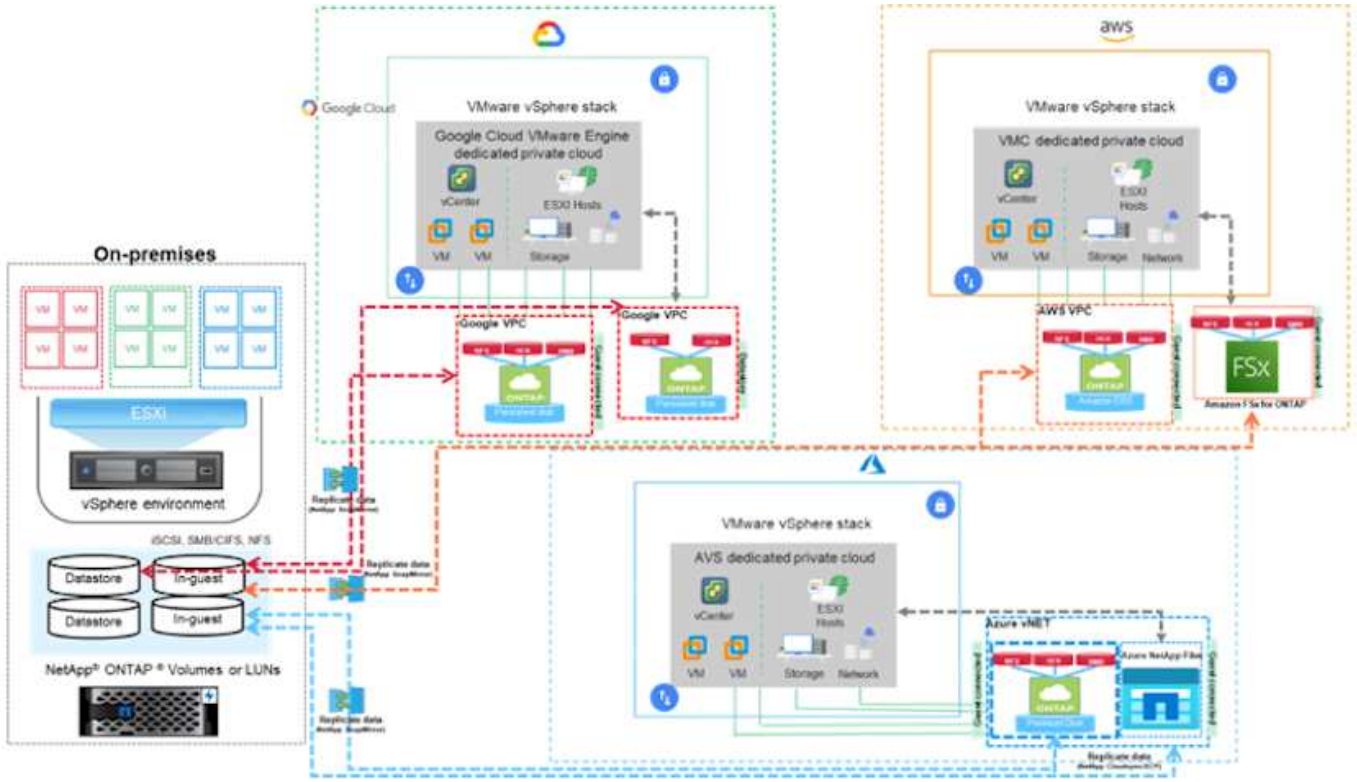
假设

- 已启用 SnapMirror 技术或其他相关数据迁移机制。从内部环境到任何超大规模云，有许多连接选项可供选择。使用适当的路径并与相关网络团队合作。
- 在编写本文档时，来宾存储是唯一可用的选项。 随着NFS数据存储库支持的补充提供、我们将提供其他文档"此处"。

请联系 NetApp 解决方案架构师和相应的超大规模云架构师来规划和估算存储以及所需数量的主机。NetApp 建议先确定存储性能要求，然后再使用 Cloud Volumes ONTAP 规模估算器以正确的吞吐量最终确定存储实例类型或相应的服务级别。

详细的架构

从高层面来看、此架构(如下图所示)介绍了如何使用NetApp Cloud Volumes ONTAP 、Cloud Volumes Service for Google Cloud和Azure NetApp Files 作为额外的子系统内存储选项、在多个云提供商之间实现混合多云连接和应用程序可移植性。



适用于超大规模云提供商的 **VMware** 的 **NetApp** 解决方案

详细了解NetApp为三(3)个主要超大规模提供商提供的功能—从NetApp作为子系统连接存储设备或补充NFS数据存储库、到迁移工作流、扩展/突发云、备份/还原和灾难恢复。

选择您的云，让 NetApp 完成其余工作！

要查看特定超大规模提供商的功能，请单击该超大规模提供商的相应选项卡。

从以下选项中选择，跳至所需内容部分：

- "超大规模部署中的 VMware"
- "NetApp 存储选项"
- "NetApp/VMware云解决方案"

超大规模部署中的 **VMware**

与内部部署一样，规划基于云的虚拟化环境对于成功创建 VM 和迁移生产就绪环境至关重要。

AWS/VMC

本节介绍如何在 AWS SDDC 上设置和管理 VMware Cloud ，并将其与连接 NetApp 存储的可用选项结合使用。

只支持使用来宾存储将Cloud Volumes ONTAP 连接到AWS VMC。

设置过程可细分为以下步骤：

- 部署和配置适用于AWS的VMware Cloud
- 将 VMware Cloud 连接到 FSX ONTAP

查看详细信息 "VMC的配置步骤"。

Azure / AVS

本节介绍如何设置和管理 Azure VMware 解决方案并将其与连接 NetApp 存储的可用选项结合使用。

来宾存储是将Cloud Volumes ONTAP 连接到Azure VMware解决方案 的唯一受支持方法。

设置过程可细分为以下步骤：

- 注册资源提供商并创建私有云
- 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的配置步骤"。

GCP / GCVE

本节介绍如何设置和管理 GCVE ，并将其与连接 NetApp 存储的可用选项结合使用。

来宾存储是将 Cloud Volumes ONTAP 和云卷服务连接到 GCVE 的唯一受支持方法。

设置过程可细分为以下步骤：

- 部署和配置 GCVE
- 启用对 GCVE 的私有访问

查看详细信息 "GCVE的配置步骤"。

NetApp 存储选项

NetApp存储可以通过多种方式在3个主要超大规模主机中的每一个上作为子系统连接或作为补充NFS数据存储库加以利用。

请访问 "支持的 NetApp 存储选项" 有关详细信息 …

AWS/VMC

AWS 支持以下配置中的 NetApp 存储：

- FSX ONTAP 作为子系统连接的存储
- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- FSX ONTAP 作为补充NFS数据存储库

查看详细信息 "VMC的子系统连接存储选项"。查看详细信息 "VMC的补充NFS数据存储库选项"。

Azure / AVS

Azure 支持以下配置中的 NetApp 存储：

- Azure NetApp Files （ ANF ）作为子系统连接的存储
- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- Azure NetApp Files (ANF)作为补充NFS数据存储库

查看详细信息 "AVS的子系统连接存储选项"。查看详细信息 "AVS的补充NFS数据存储库选项"。

GCP / GCVE

Google Cloud 支持以下配置中的 NetApp 存储：

- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- Cloud Volumes Service （ CVS ）作为子系统连接的存储
- Cloud Volumes Service (CVS)作为补充NFS数据存储库

查看详细信息 "GCVE的子系统连接存储选项"。

了解更多信息 "适用于Google Cloud VMware Engine的NetApp Cloud Volumes Service 数据存储库支持(NetApp博客)" 或 "如何使用NetApp CVS作为Google Cloud VMware Engine的数据存储库(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部署到您选择的超大规模云提供商中。VMware将主要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
- 扩展

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"

GCP / GCVE

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

支持采用**VMware**的**NetApp**混合多云配置

了解主要超大规模提供商中的 NetApp 存储支持组合。

	已连接子系统	补充**NFS**数据存储库
* AWS *	CVO FSX ONTAP"详细信息"	FSX ONTAP"详细信息"
* Azure *	CVO ANF"详细信息"	ANF"详细信息"
* GCP*	CVO CVS"详细信息"	CVS"详细信息"

在云提供商中配置虚拟化环境

此处详细介绍了如何在每个受支持的超大规模主机中配置虚拟化环境。

AWS/VMC

本节介绍如何在 AWS SDDC 上设置和管理 VMware Cloud ，并将其与连接 NetApp 存储的可用选项结合使用。

只支持使用来宾存储将Cloud Volumes ONTAP 连接到AWS VMC。

设置过程可细分为以下步骤：

- 部署和配置适用于AWS的VMware Cloud
- 将 VMware Cloud 连接到 FSX ONTAP

查看详细信息 "VMC的配置步骤"。

Azure / AVS

本节介绍如何设置和管理 Azure VMware 解决方案并将其与连接 NetApp 存储的可用选项结合使用。

来宾存储是将Cloud Volumes ONTAP 连接到Azure VMware解决方案 的唯一受支持方法。

设置过程可细分为以下步骤：

- 注册资源提供商并创建私有云
- 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的配置步骤"。

GCP / GCVE

本节介绍如何设置和管理 GCVE ，并将其与连接 NetApp 存储的可用选项结合使用。

来宾存储是将 Cloud Volumes ONTAP 和云卷服务连接到 GCVE 的唯一受支持方法。

设置过程可细分为以下步骤：

- 部署和配置 GCVE
- 启用对 GCVE 的私有访问

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

与内部部署一样，在 AWS 上规划 VMware Cloud 对于成功打造可随时投入生产的环境以创建 VM 和迁移至关重要。

本节介绍如何在 AWS SDDC 上设置和管理 VMware Cloud ，并将其与连接 NetApp 存储的可用选项结合使用。

目前、只有来宾存储是将Cloud Volumes ONTAP (CVO)连接到AWS VMC的唯一受支持方法。

设置过程可细分为以下步骤：

部署和配置适用于 **AWS** 的 **VMware Cloud**

"基于 AWS 的 VMware Cloud" 为 AWS 生态系统中基于 VMware 的工作负载提供 Cloud 原生体验。每个 VMware 软件定义的数据中心（ SDDC ）均在 Amazon Virtual Private Cloud （ VPC ）中运行，并提供完整的 VMware 堆栈（包括 vCenter Server ）， NSX-T 软件定义的网络连接， vSAN 软件定义的存储以及一个或多个 ESXi 主机，这些主机可为您的工作负载提供计算和存储资源。

本节介绍如何在 AWS 上设置和管理 VMware Cloud ，并将其与适用于 NetApp ONTAP 的 Amazon FSX 和 / 或在 AWS 上使用子系统内存储的 Cloud Volumes ONTAP 结合使用。

目前、只有来宾存储是将Cloud Volumes ONTAP (CVO)连接到AWS VMC的唯一受支持方法。

设置过程可分为三部分：

注册**AWS**帐户

注册 "Amazon Web Services 帐户"。

您需要一个 AWS 帐户才能开始使用，前提是尚未创建一个 AWS 帐户。无论新的还是现有的，您都需要在帐户中拥有管理权限才能执行此操作步骤中的许多步骤。请参见此内容 "链接。" 有关 AWS 凭据的详细信息。

注册**"**我的**VMware**帐户**"**

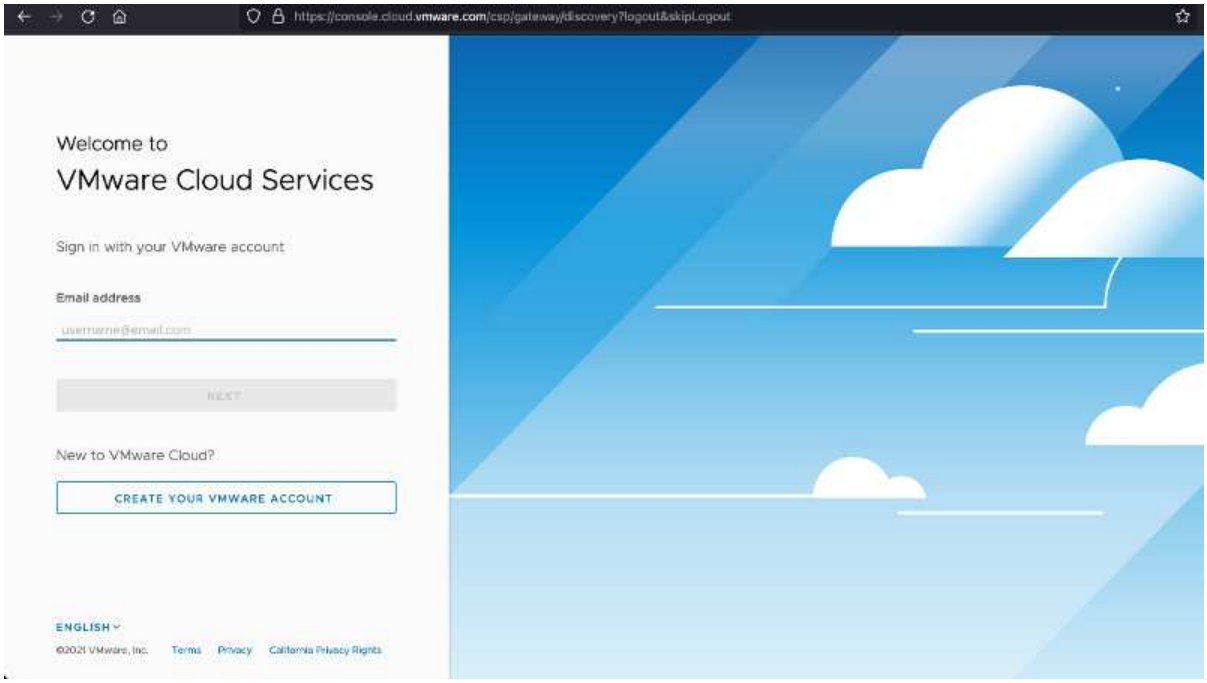
注册 "我的 VMware" 帐户。

要访问 VMware 的云产品组合（包括基于 AWS 的 VMware Cloud ），您需要 VMware 客户帐户或 My VMware 帐户。如果尚未创建 VMware 帐户，请创建此帐户 "此处"。

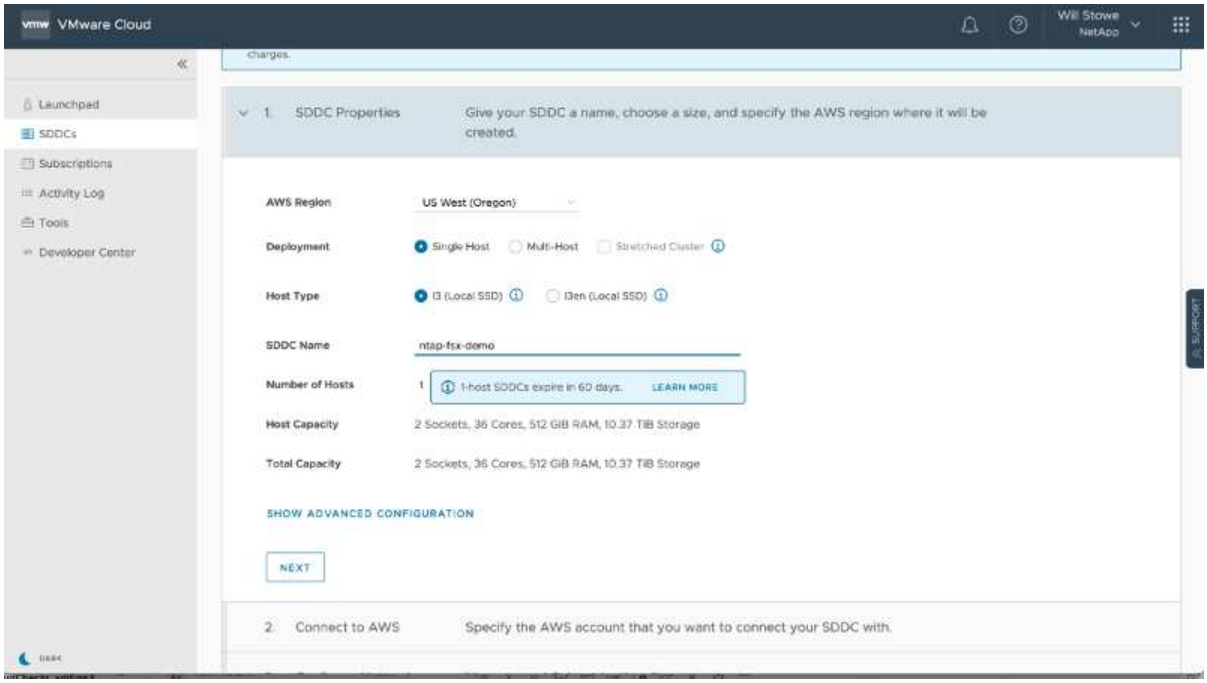
在 **VMware Cloud** 中配置 **SDDC**

配置 VMware 帐户并执行适当的规模估算后，部署软件定义的数据中心显然是使用 VMware Cloud on AWS 服务的下一步。要创建 SDDC ，请选择要托管它的 AWS 区域，为 SDDC 指定一个名称，并指定希望 SDDC 包含的 ESXi 主机数。如果您还没有 AWS 帐户，则仍可以创建一个包含单个 ESXi 主机的入门级配置 SDDC 。

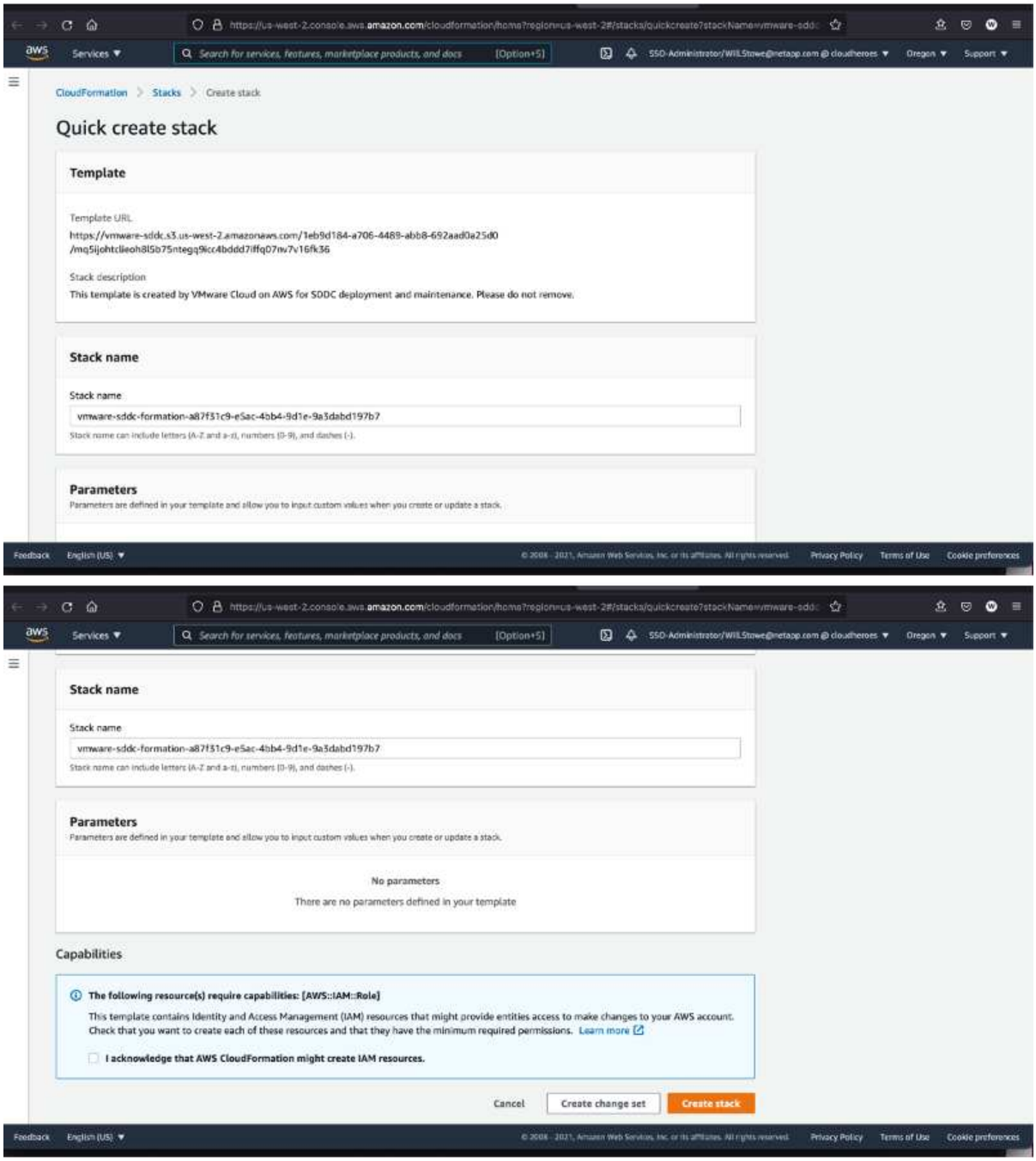
1. 使用现有或新创建的 VMware 凭据登录到 VMware Cloud Console 。



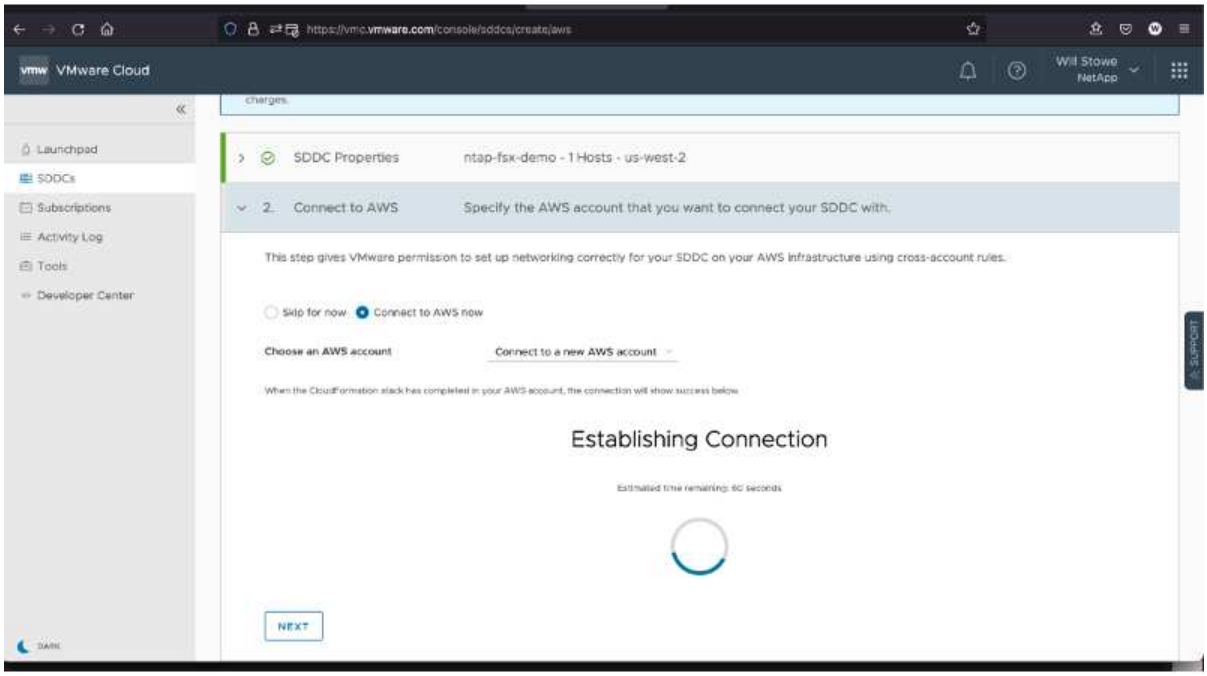
2. 配置 AWS 区域，部署和主机类型以及 SDDC 名称：

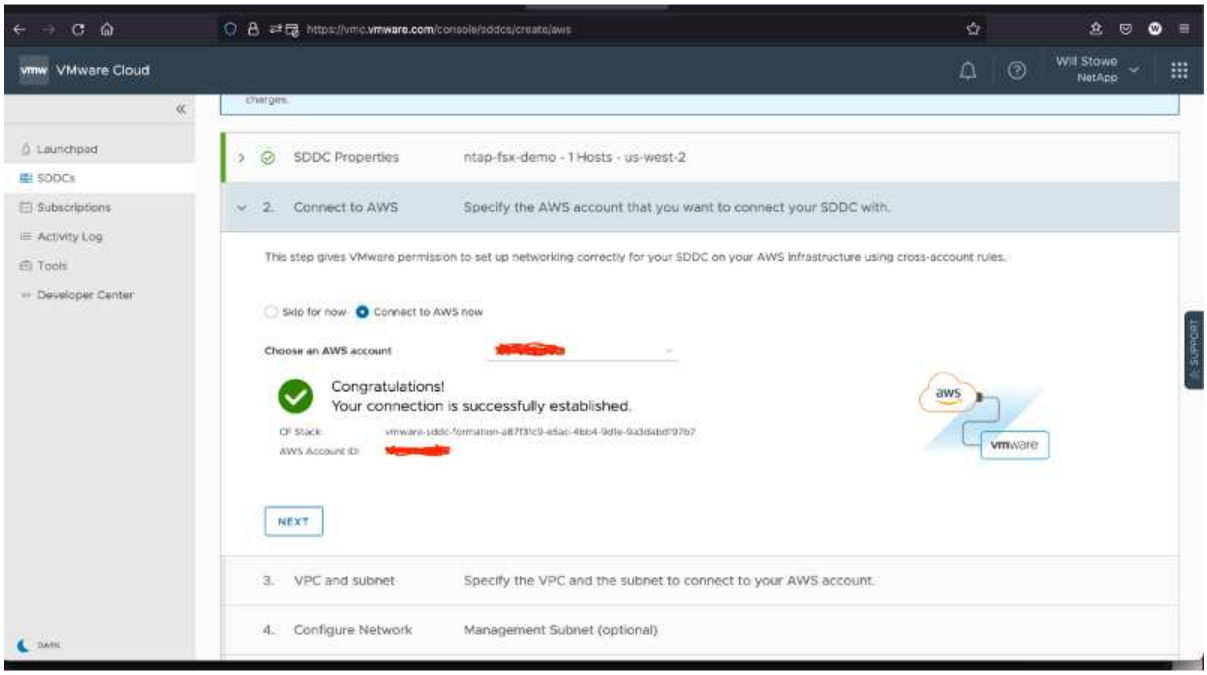


3. 连接到所需的 AWS 帐户并执行 AWS Cloud Formation 堆栈。


CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ijohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences

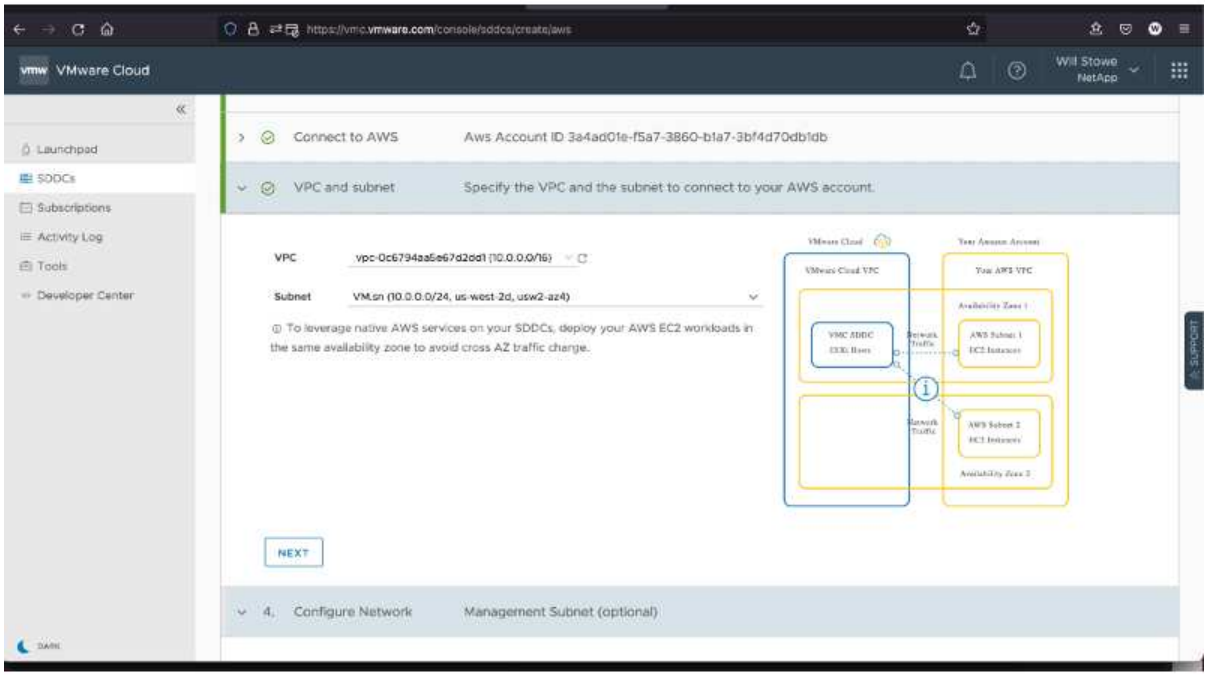
Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There 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
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences



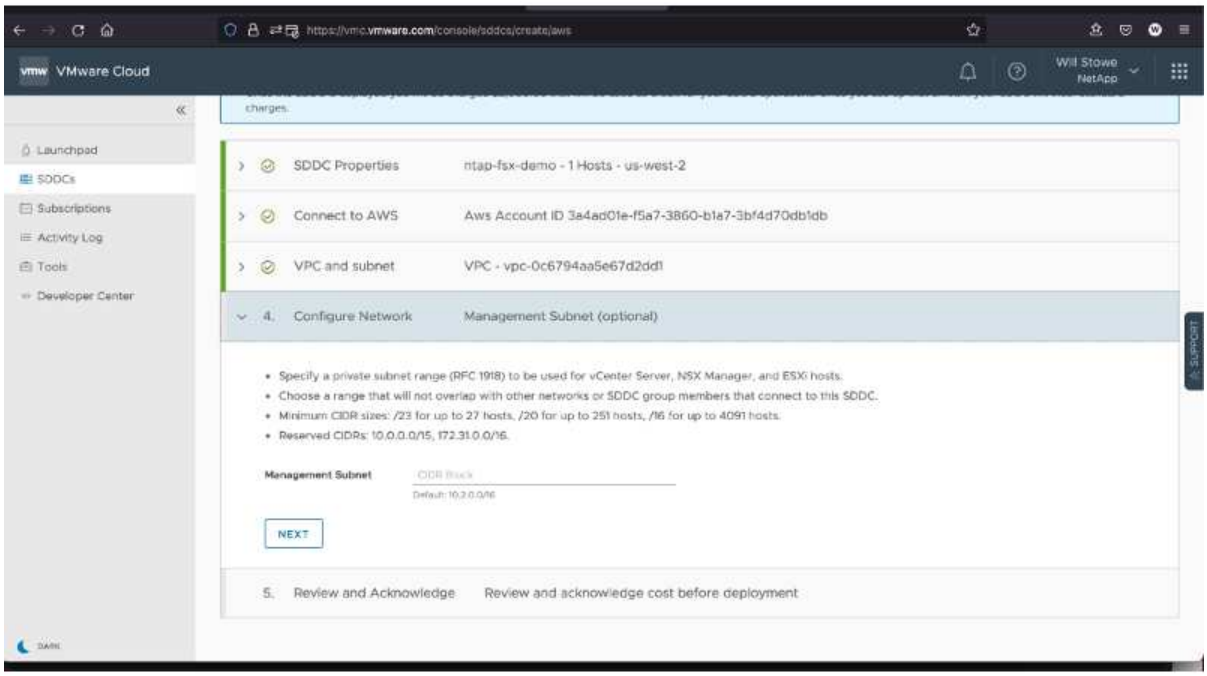


此验证使用单主机配置。

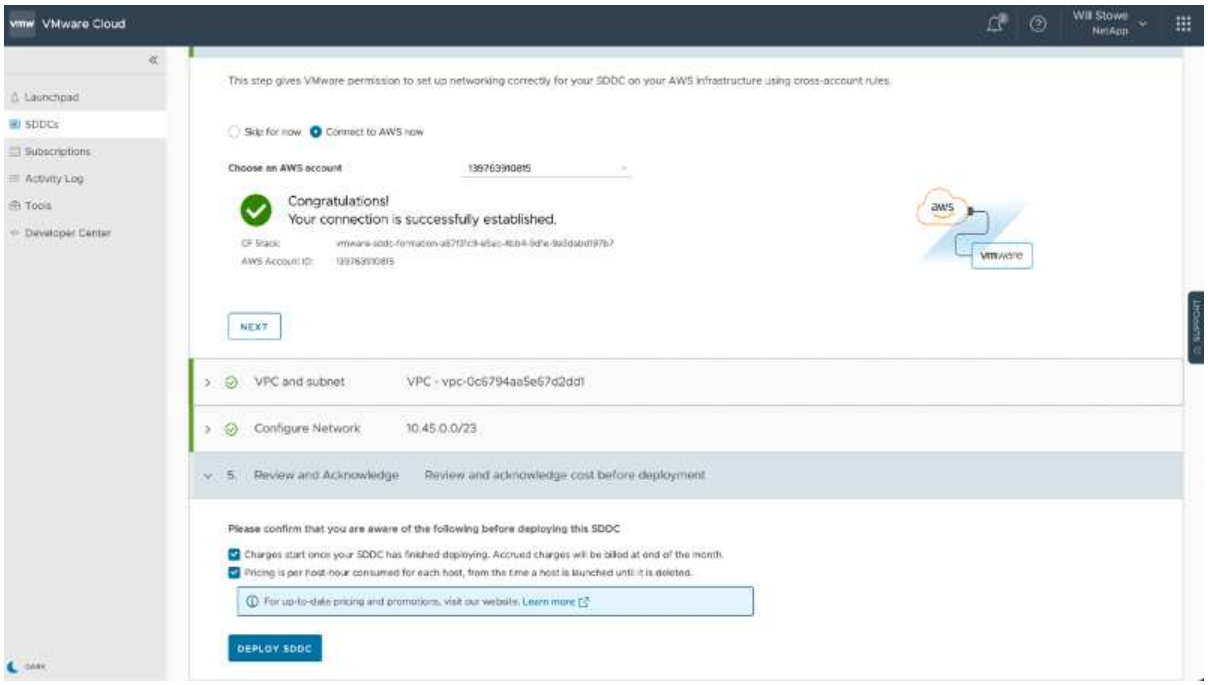
4. 选择所需的 AWS VPC 以连接 VMC 环境。



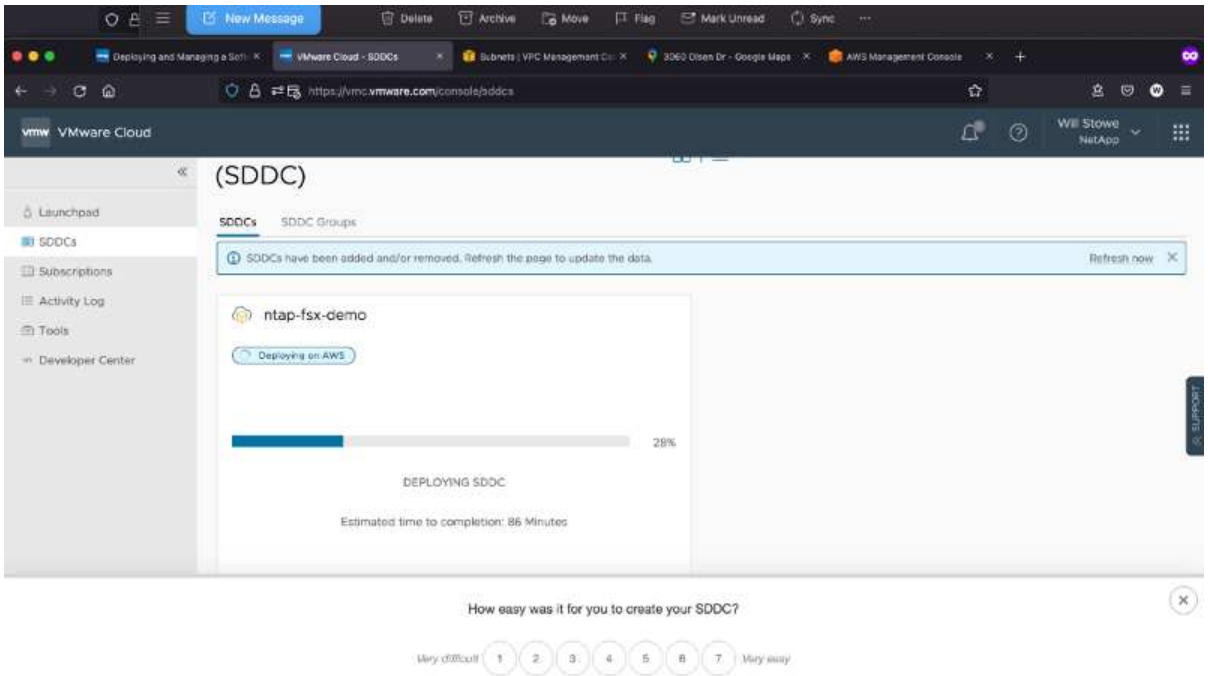
5. 配置 VMC 管理子网；此子网包含 vCenter ， NSX 等 VMC 管理的服务。请勿选择与任何其他需要连接到 SDDC 环境的网络重叠的地址空间。最后，请遵循下面标注的 CIDR 大小建议。



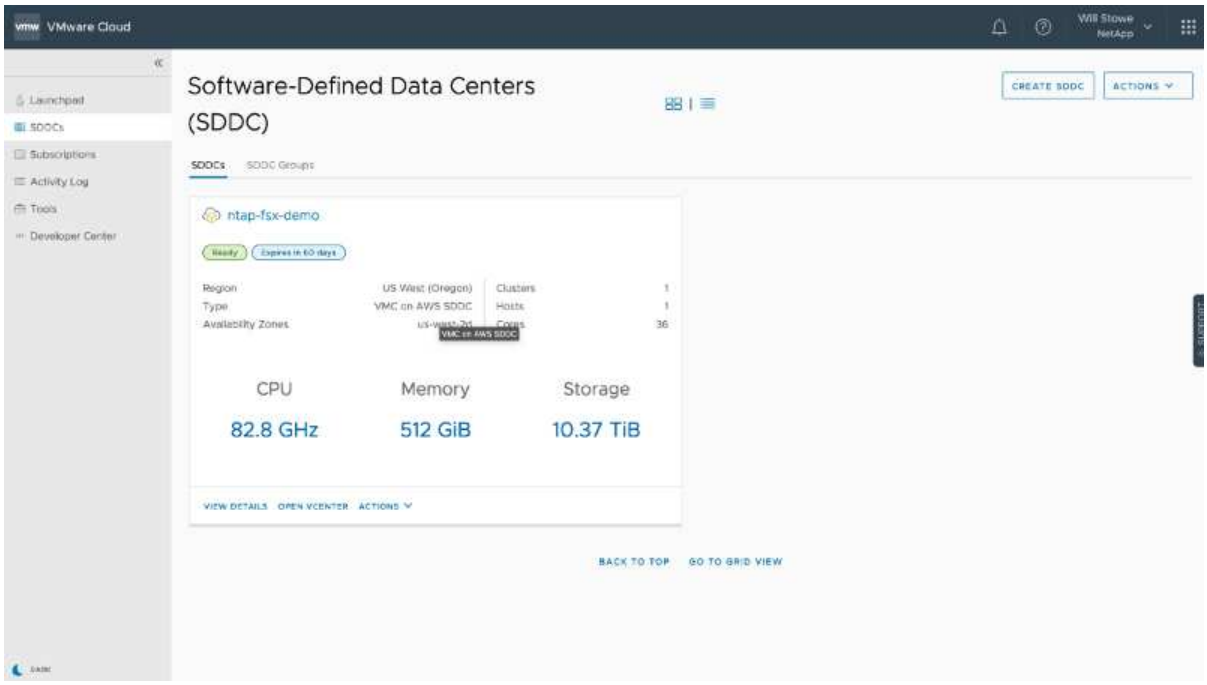
6. 查看并确认 SDDC 配置，然后单击 Deploy the SDDC 。



完成部署过程通常需要大约两个小时。



7. 完成后， SDDC 即可使用。

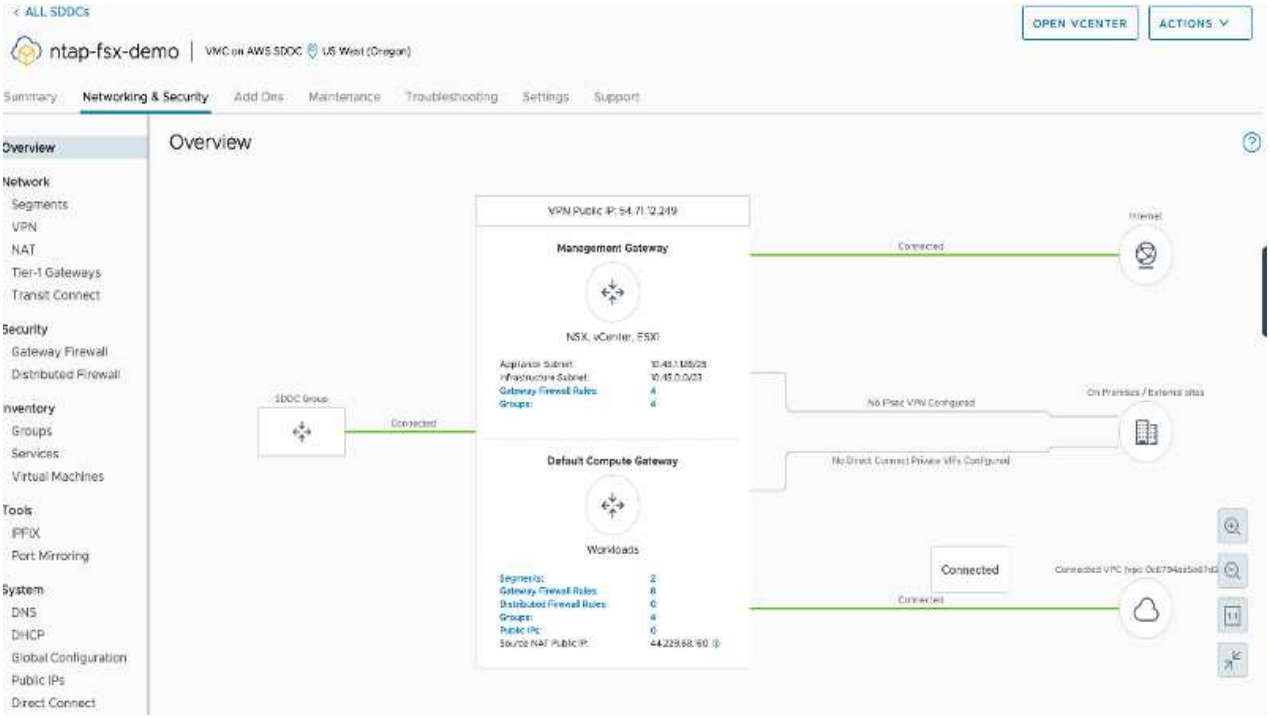


有关 SDDC 部署的分步指南，请参见 "从 VMC 控制台部署 SDDC"。

将 **VMware Cloud** 连接到 **FSX ONTAP**

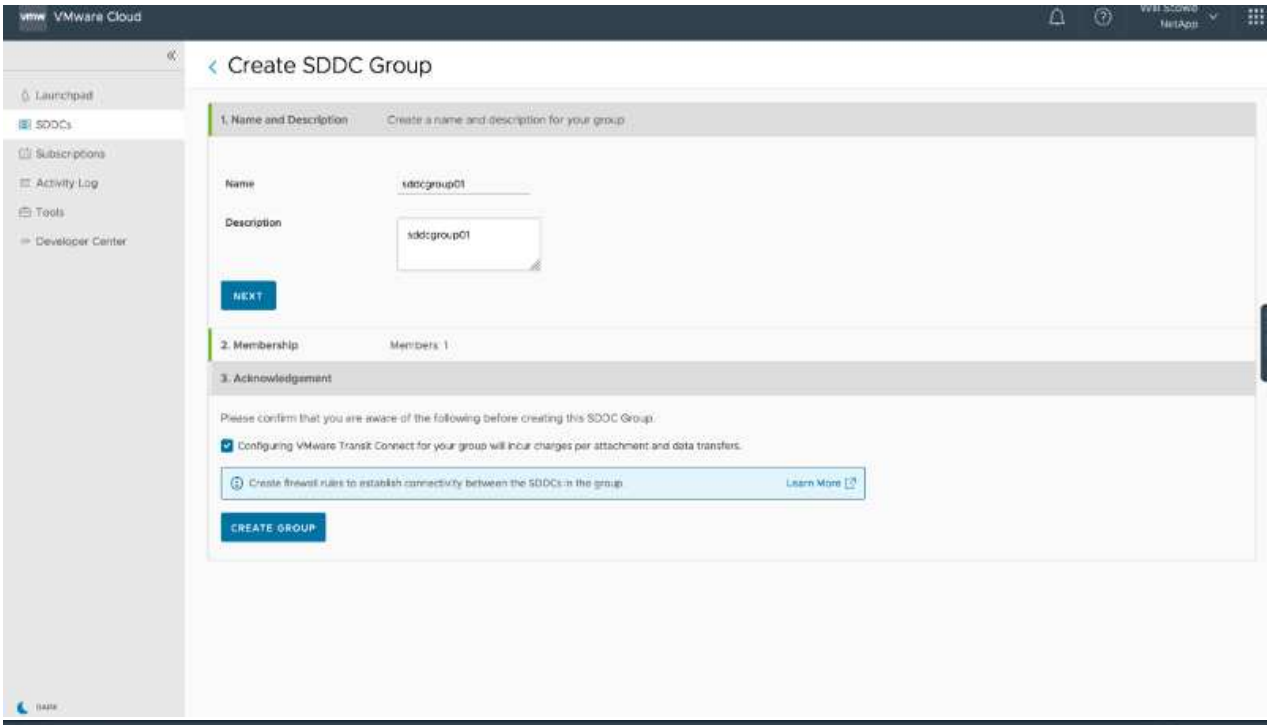
要将 VMware Cloud 连接到 FSX ONTAP ，请完成以下步骤：

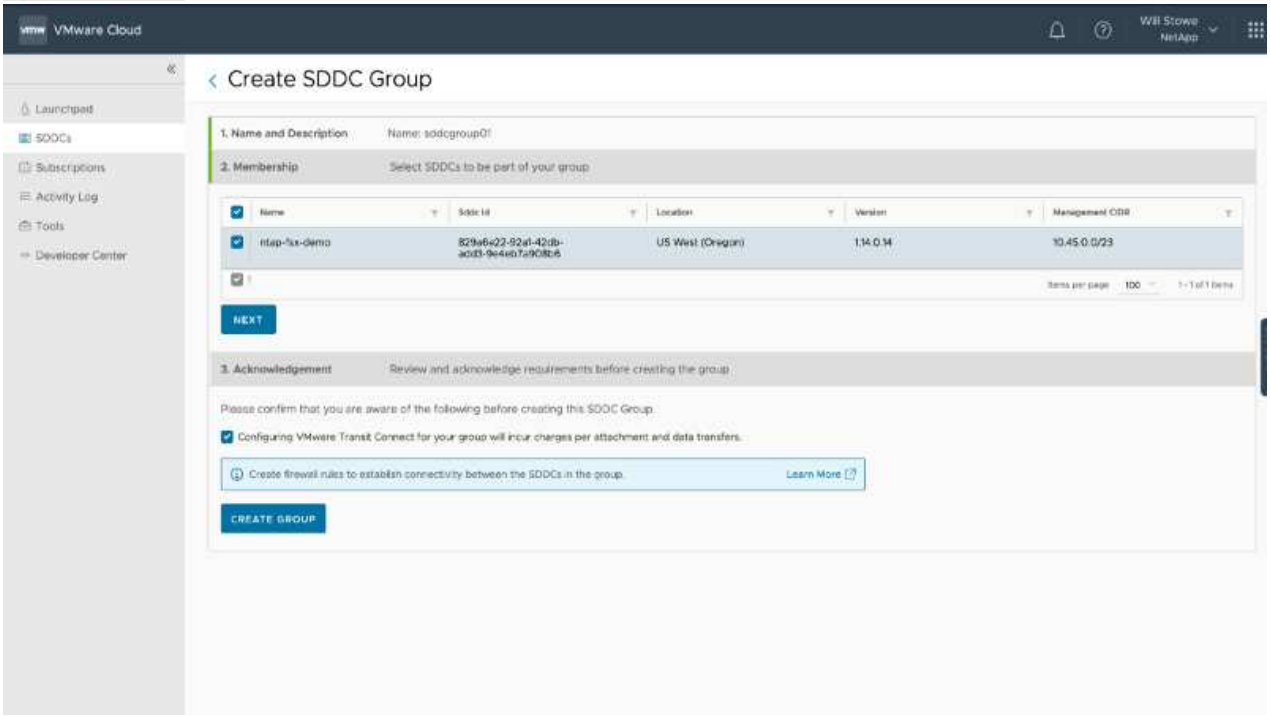
1. 完成 VMware Cloud 部署并连接到 AWS VPC 后，您必须将适用于 NetApp ONTAP 的 Amazon FSx 部署到新的 VPC 中，而不是原始连接的 VPC 中（请参见下面的屏幕截图）。如果在连接的 VPC 中部署了 FSX （ NFS 和 SMB 浮动 IP ），则无法访问它。请注意， Cloud Volumes ONTAP 等 iSCSI 端点在连接的 VPC 上运行正常。

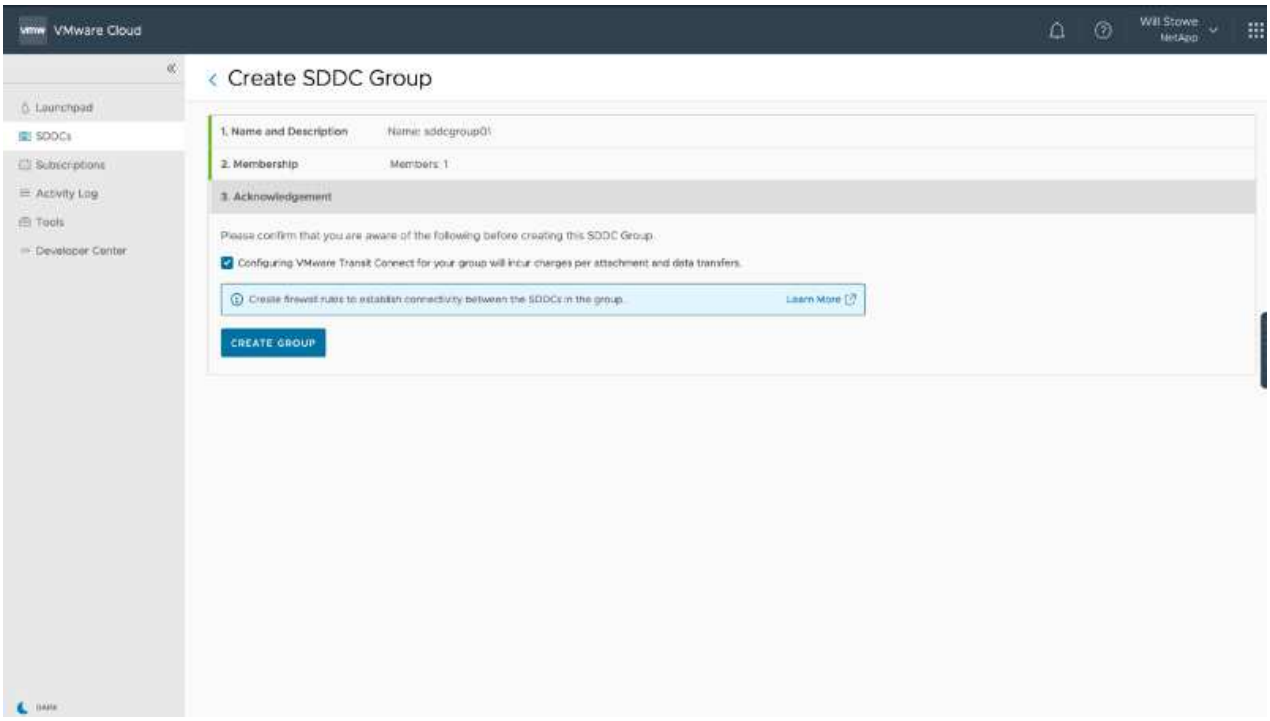


2. 在同一地区部署一个额外的 VPC ，然后将适用于 NetApp ONTAP 的 Amazon FSx 部署到新的 VPC 中。

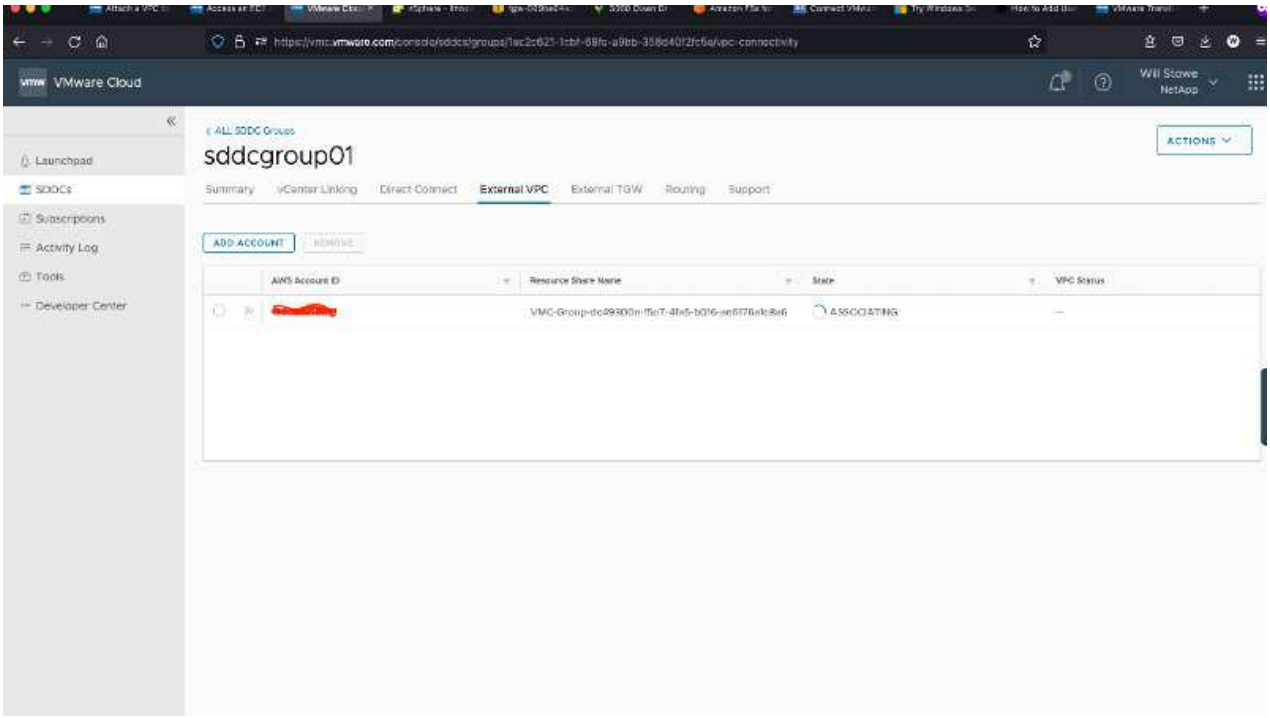
   通过在 VMware Cloud 控制台中配置 SDDC 组，可以使用所需的网络配置选项连接到部署了 FSX 的新 VPC 。在第 3 步中，验证是否已选中 " 为组配置 VMware Transit Connect 将在每个附件和数据传输中产生费用 " ，然后选择创建组。完成此过程可能需要几分钟时间。

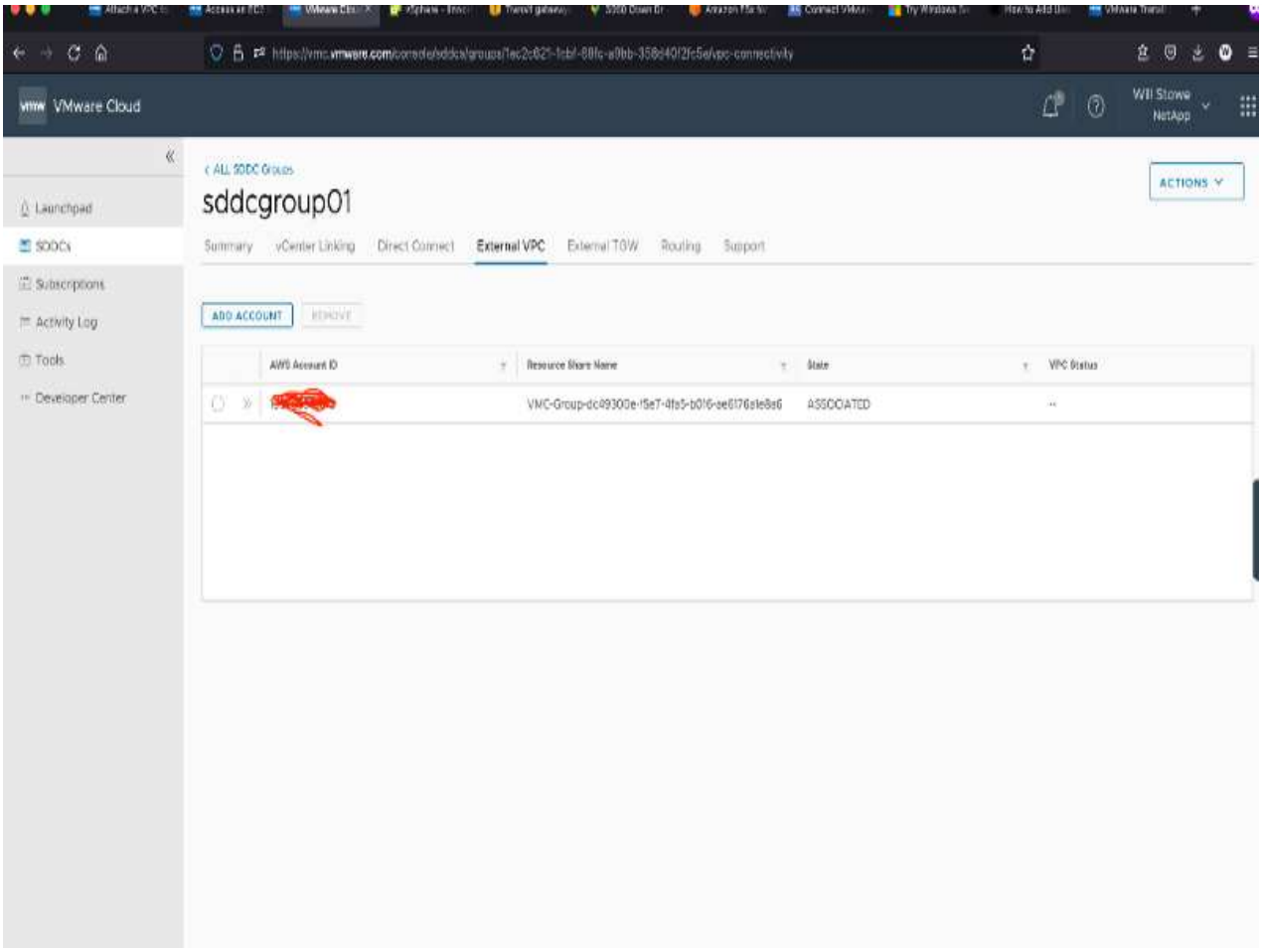

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP


VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6e22-92a1-42db-
acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page
100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

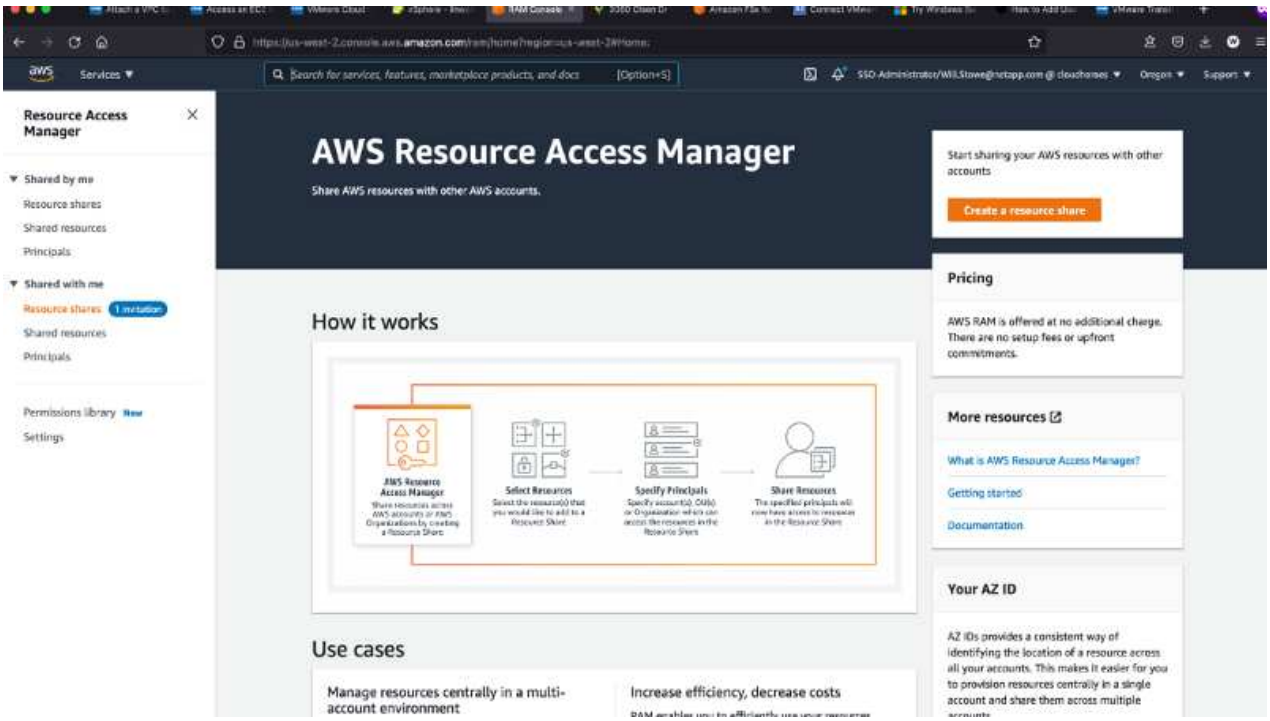


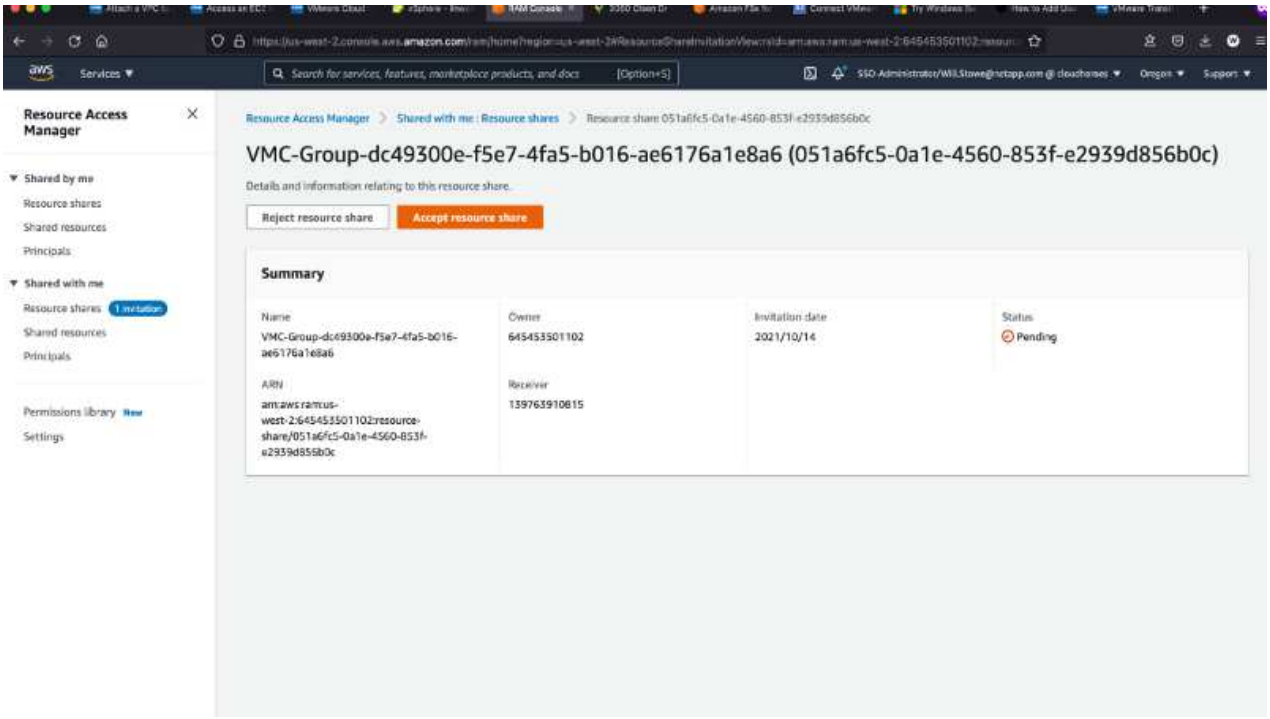
3. 将新创建的 VPC 附加到刚刚创建的 SDDC 组。选择外部 VPC 选项卡，然后按照进行操作 "连接外部 VPC 的说明" 组。完成此过程可能需要 10 到 15 分钟。



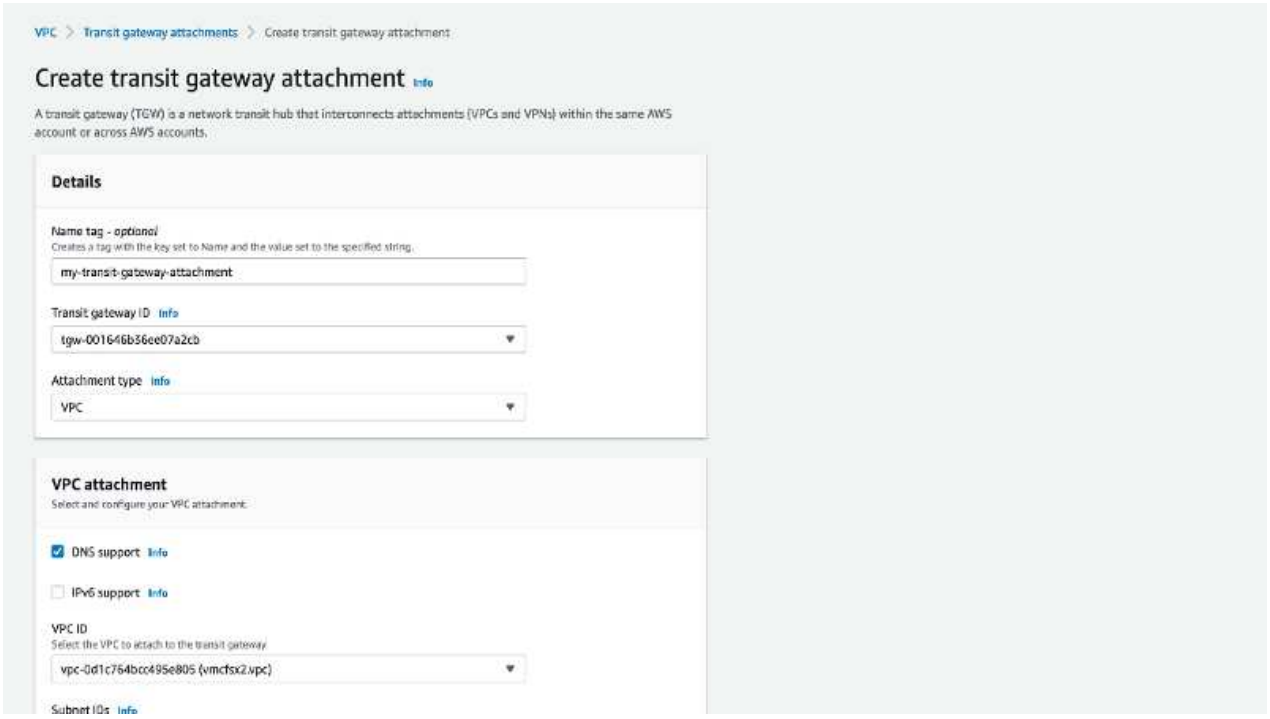


4. 在外部 VPC 过程中，系统会通过 AWS 控制台通过资源访问管理器提示您访问新的共享资源。共享资源为 "AWS 传输网关" 由 VMware Transit Connect 管理。

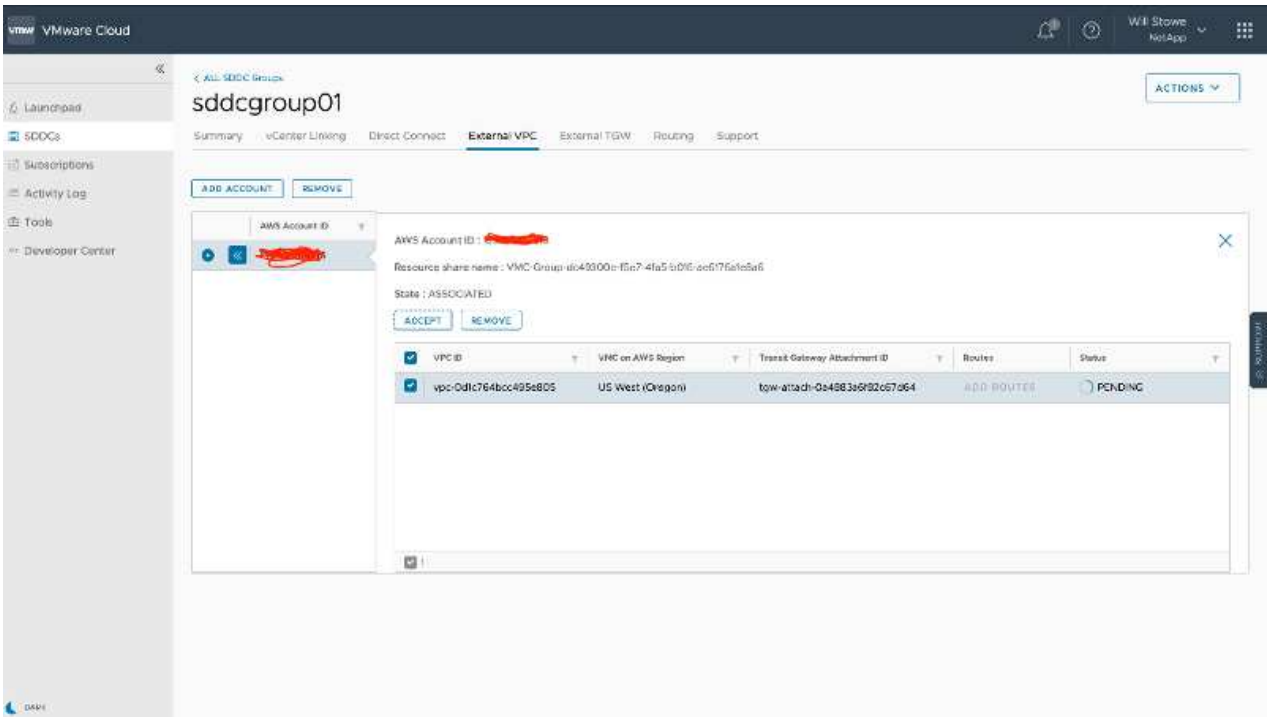




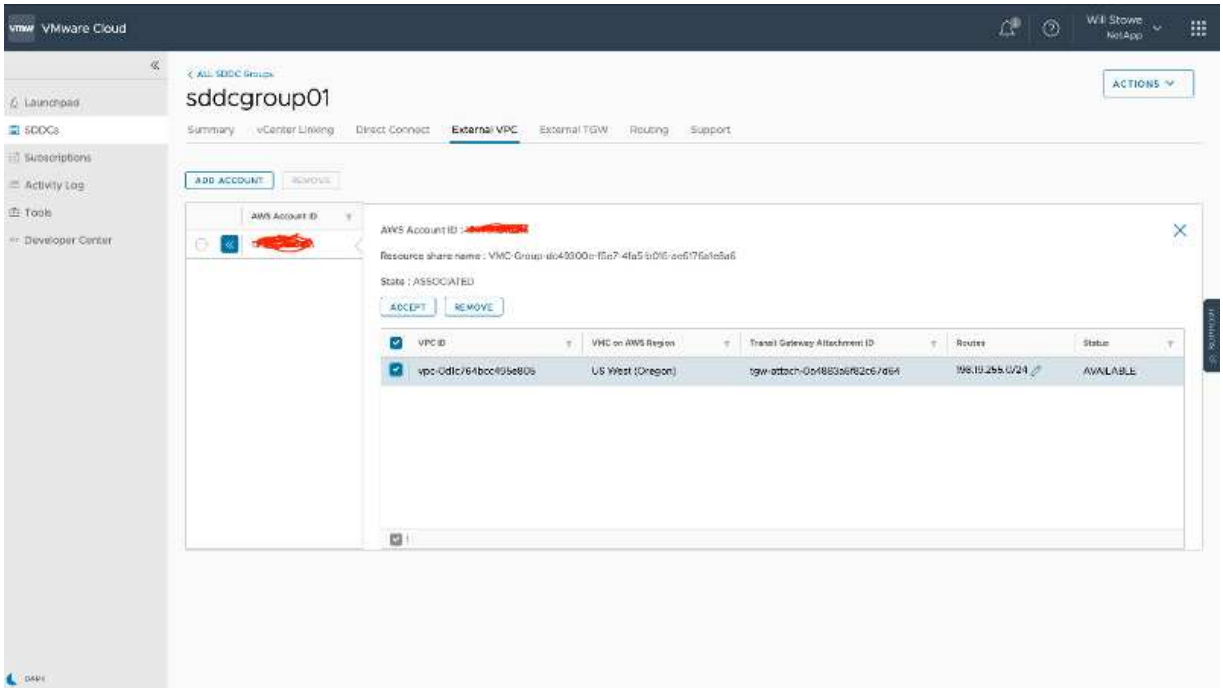
5. 创建传输网关附件。



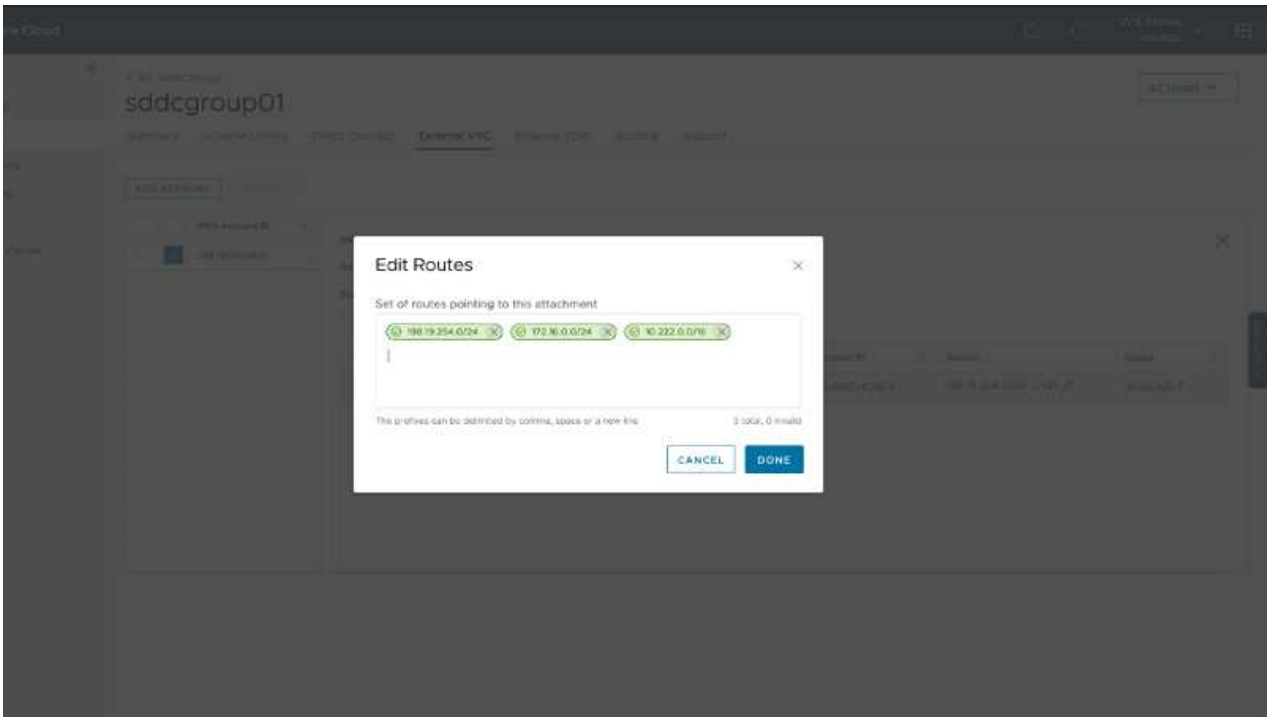
6. 返回 VMC 控制台，接受 VPC 连接。完成此过程大约需要 10 分钟。



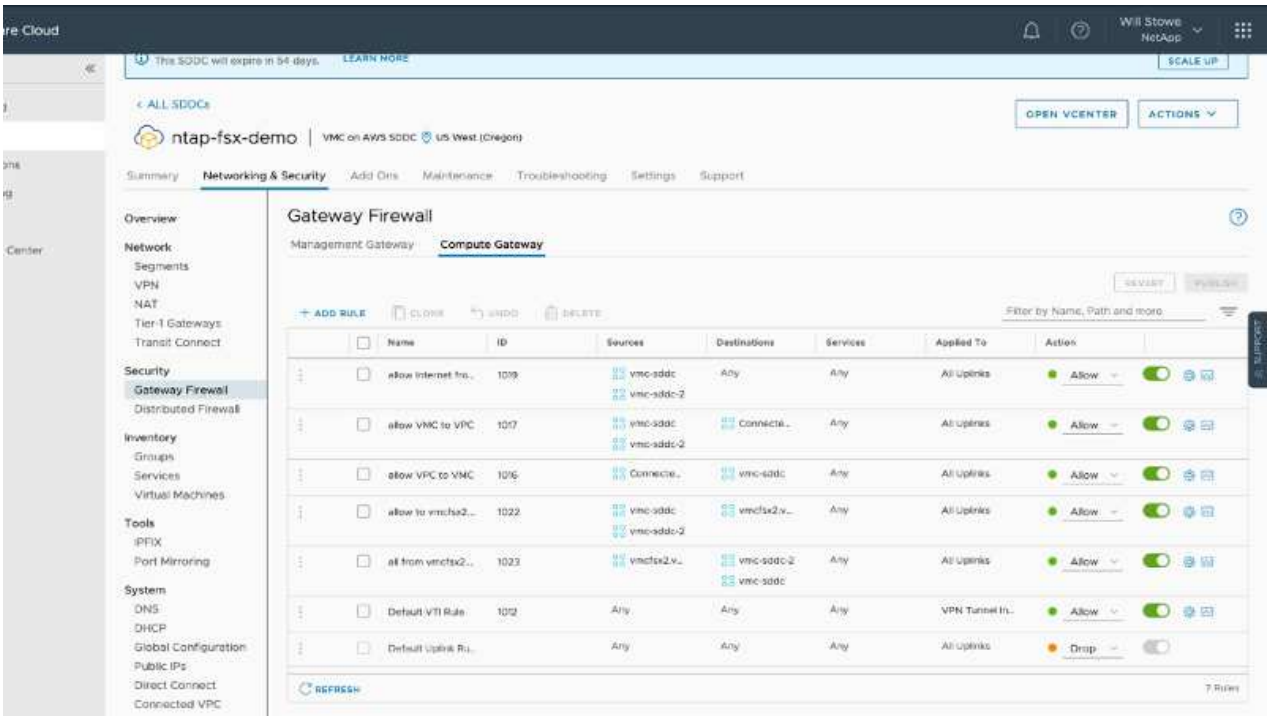
7. 在外部 VPC 选项卡中，单击路由列中的编辑图标，然后添加以下所需的路由：
   - 适用于 NetApp ONTAP 的 Amazon FSX 的浮动 IP 范围的路由 "浮动 IP"。
   - Cloud Volumes ONTAP 的浮动 IP 范围的路由（如果适用）。
   - 新创建的外部 VPC 地址空间的路由。



8. 最后，允许双向流量 "防火墙规则" 用于访问 FSX/CVO 。请按照以下说明操作 "详细步骤" 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：



下一步是验证是否已根据您的需求配置 Amazon FSX ONTAP 或 Cloud Volumes ONTAP ，以及是否已配置卷以从 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

与内部部署一样，规划 Azure VMware 解决方案对于成功创建 VM 和迁移生产就绪环境至关重要。

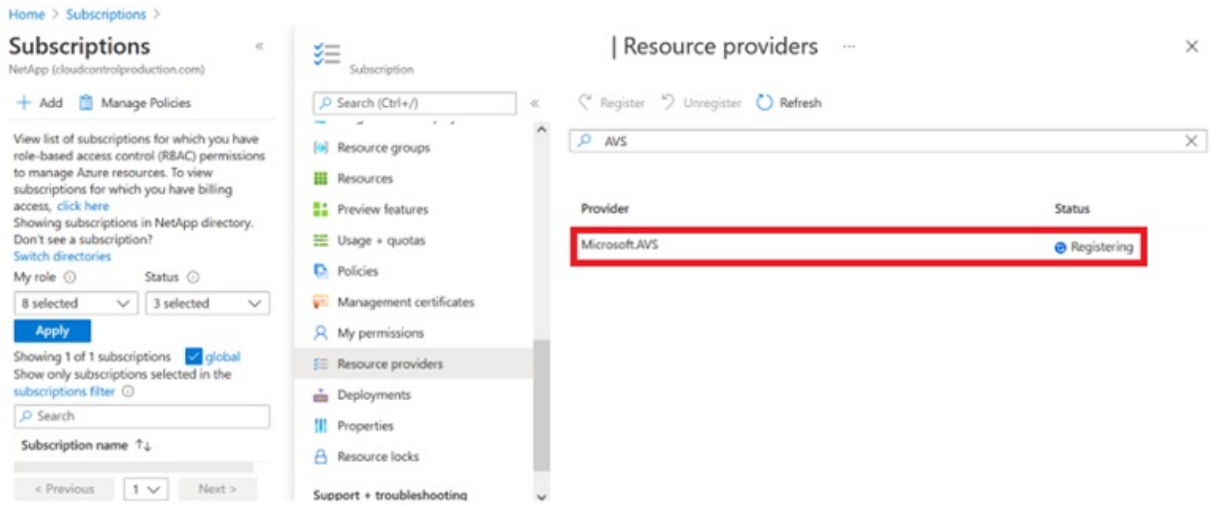
本节介绍如何设置和管理 Azure VMware 解决方案并将其与连接 NetApp 存储的可用选项结合使用。

设置过程可细分为以下步骤：

注册资源提供商并创建私有云

要使用 Azure VMware 解决方案，请先在标识的订阅中注册资源提供程序：

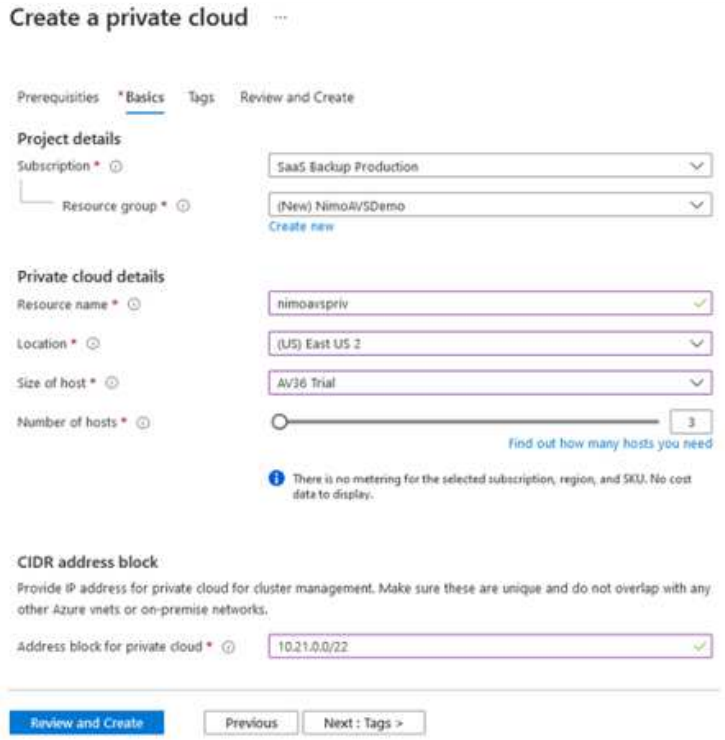
1. 登录到 Azure 门户。
2. 在 Azure 门户菜单上，选择所有服务。
3. 在所有服务对话框中，输入订阅，然后选择订阅。
4. 要查看此订阅，请从订阅列表中选择此订阅。
5. 选择资源提供程序，然后在搜索中输入 microsoft.AVS 。
6. 如果资源提供程序未注册，请选择注册。



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. 登录到 Azure 门户。
9. 选择创建新资源。
10. 在 Search the Marketplace 文本框中，输入 Azure VMware 解决方案并从结果中选择它。
11. 在 Azure VMware 解决方案页面上，选择创建。
12. 在基础选项卡的字段中输入值，然后选择查看 + 创建。

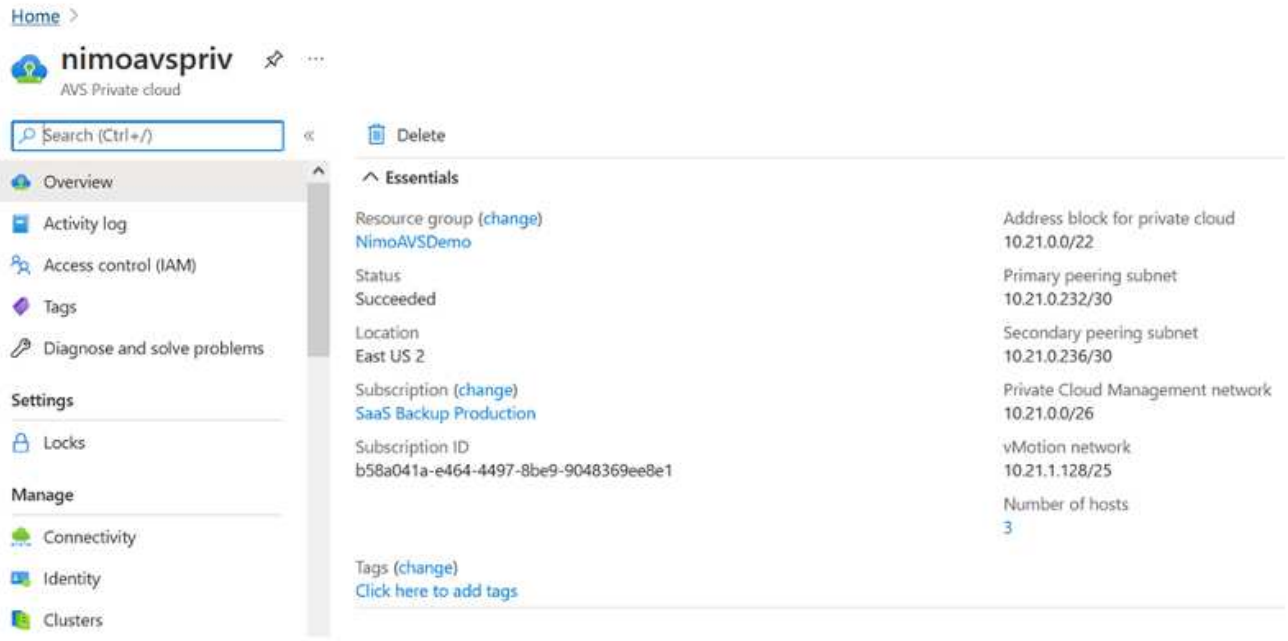
注释：

- 要快速入门，请在规划阶段收集所需信息。
- 选择现有资源组或为私有云创建新资源组。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，不会与其他 Azure 虚拟网络或内部网络重叠。CIDR 表示私有云管理网络，并用于 vCenter Server 和 NSX-T Manager 等集群管理服务。NetApp 建议使用 22 地址空间。在此示例中，使用了 10.21.0.0/22 。



配置过程大约需要 4 – 5 小时。此过程完成后，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，系统将显示状态 " 成功 " 。

Azure VMware 解决方案私有云需要 Azure 虚拟网络。由于 Azure VMware 解决方案不支持内部 vCenter ，因此需要执行其他步骤才能与现有内部环境集成。此外，还需要设置 ExpressRoute 电路和虚拟网络网关。在等待集群配置完成时，创建新的虚拟网络或使用现有虚拟网络连接到 Azure VMware 解决方案。



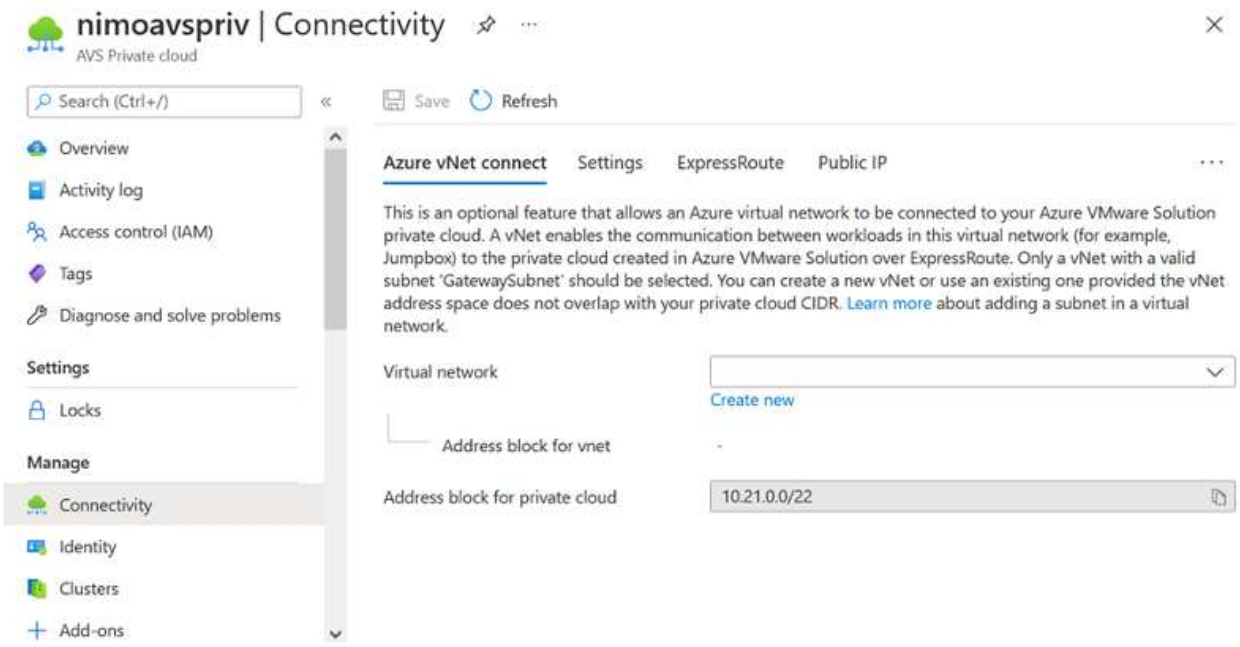
连接到新的或现有的 **ExpressRoute** 虚拟网络网关

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：

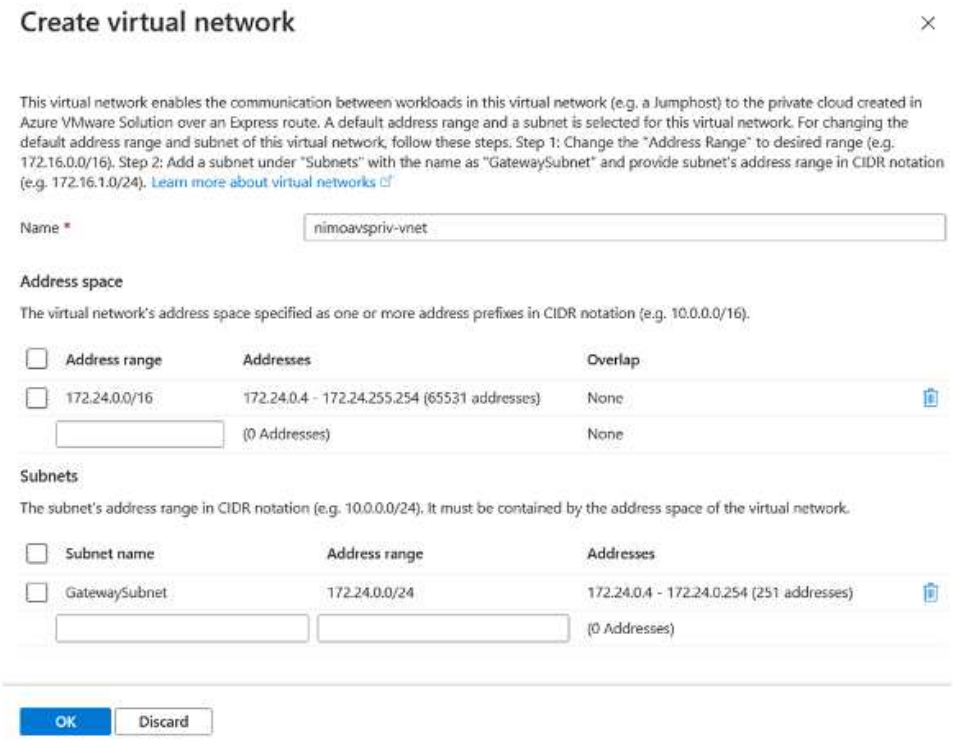
1. 转到 Azure VMware 解决方案私有云，然后在管理选项下访问连接。
2. 选择 Azure vNet Connect 。
3. 要创建新的 vNet ，请选择 Create New 选项。

   通过此功能，可以将 vNet 连接到 Azure VMware 解决方案私有云。vNet 可通过自动创建所需组件（例如跳转盒， Azure NetApp Files 等共享服务和 Cloud Volume ONTAP ）并通过 ExpressRoute 在 Azure VMware 解决方案中创建的私有云来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，然后选择确定。

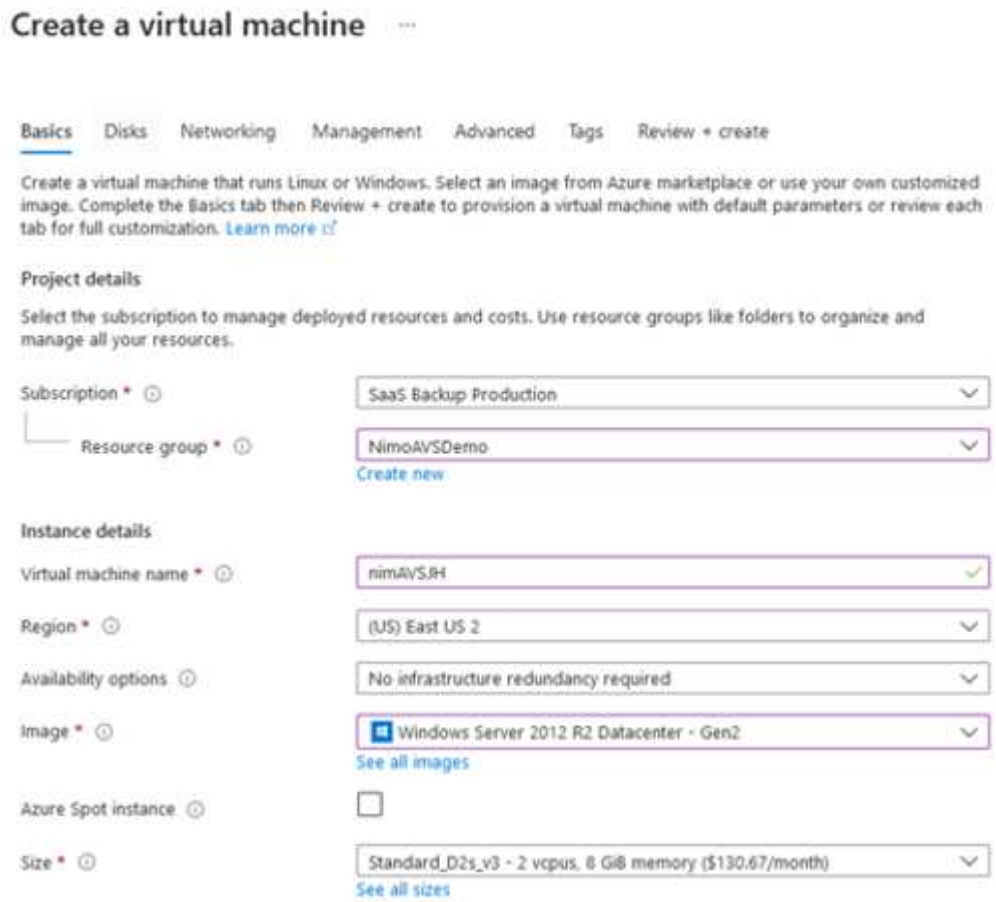


将在指定的订阅和资源组中创建具有提供的地址范围和网关子网的 vNet 。

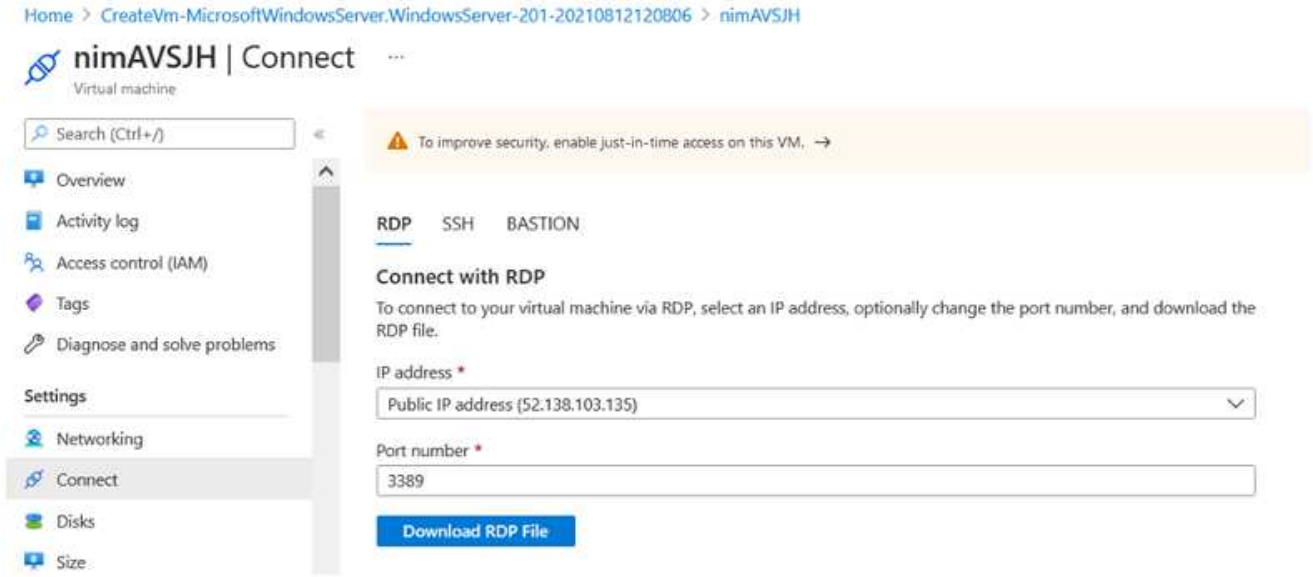
如果您手动创建 vNet ，请创建一个虚拟网络网关，并将相应的 SKU 和 ExpressRoute 作为网关类型。部署完成后，使用授权密钥将 ExpressRoute 连接到包含 Azure VMware 解决方案私有云的虚拟网络网关。有关详细信息，请参见 "在 Azure 中为 VMware 私有云配置网络连接"。

验证连接到 **Azure VMware** 解决方案私有云的网络和访问权限

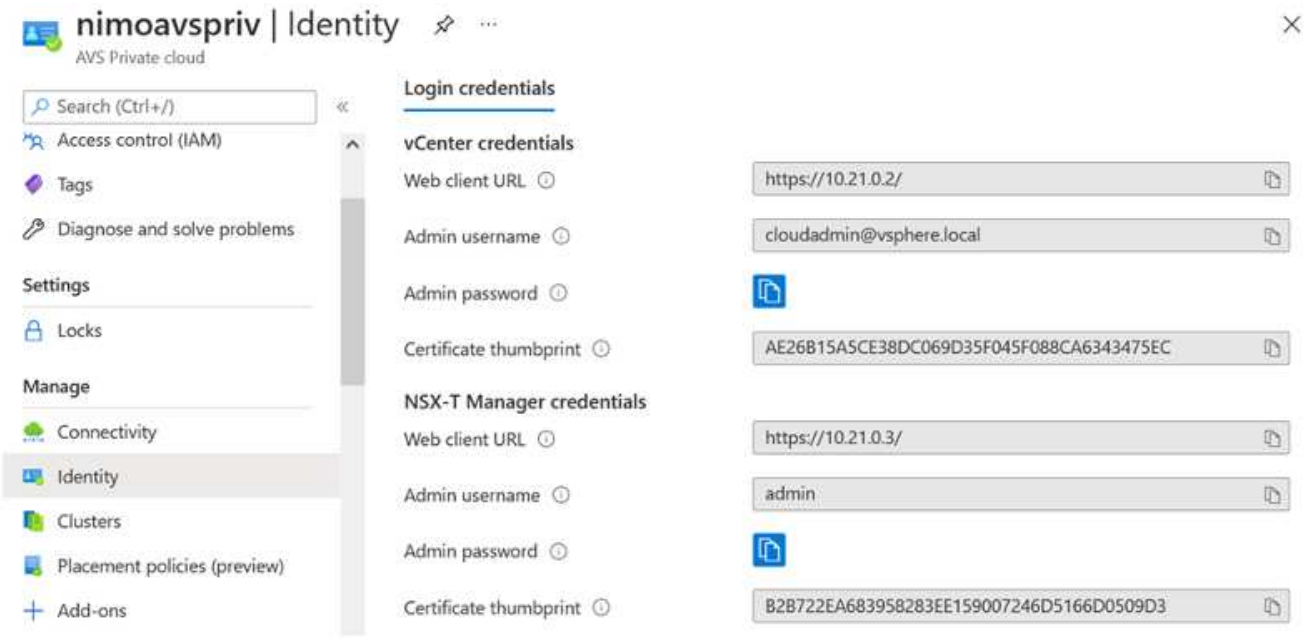
Azure VMware 解决方案不允许您使用内部 VMware vCenter 管理私有云。而是需要跳转主机才能连接到 Azure VMware 解决方案 vCenter 实例。在指定资源组中创建一个跳转主机，然后登录到 Azure VMware 解决方案 vCenter 。此跳转主机应是为连接而创建的同一虚拟网络上的 Windows VM ，并应提供对 vCenter 和 NSX Manager 的访问权限。



配置虚拟机后，使用 Connect 选项访问 RDP 。

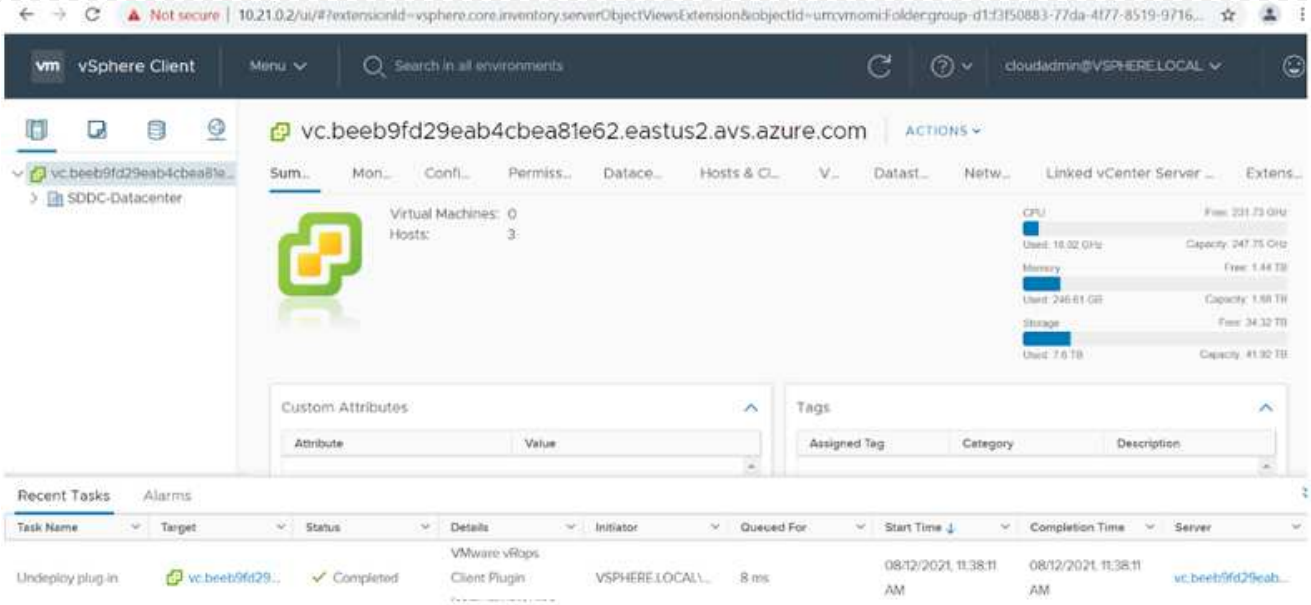


使用云管理员用户从此新创建的跳转主机虚拟机登录到 vCenter 。要访问凭据，请转到 Azure 门户并导航到身份（位于私有云中的 Manage 选项下）。可以从此处复制私有云 vCenter 和 NSX-T Manager 的 URL 和用户凭据。



在 Windows 虚拟机中，打开浏览器并导航到 vCenter Web 客户端 URL 并使用管理员用户名 * 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 管理器并使用管理员用户名并粘贴复制的密码以创建新分段或修改现有分层网关。

对于配置的每个 SDDC ， Web 客户端 URL 都不同。



现在， Azure VMware 解决方案 SDDC 已部署和配置。利用 ExpressRoute Global Reach 将内部环境连接到 Azure VMware 解决方案私有云。有关详细信息，请参见 "将内部环境与 Azure VMware 解决方案建立对等关系"。

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

与内部部署一样，规划 Google Cloud VMware Engine （ GCVE ）对于成功创建虚拟机和迁移可随时投入生产的环境至关重要。

本节介绍如何设置和管理 GCVE ，并将其与连接 NetApp 存储的可用选项结合使用。

设置过程可细分为以下步骤：

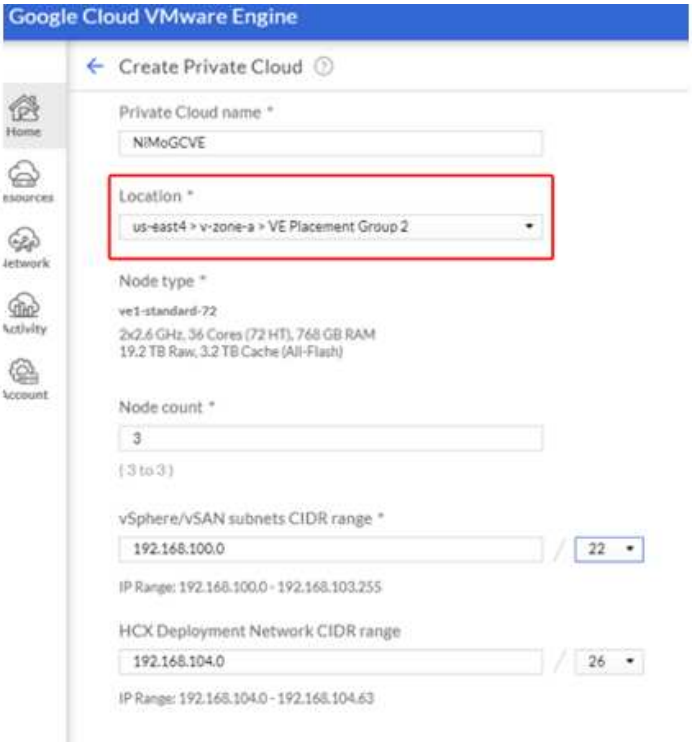
部署和配置 **GCVE**

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

单击 " 新建私有云 " 按钮，然后输入所需的 GCVE 私有云配置。在 " 位置 " 上，确保在部署 CVS/CVO 的同一区域 / 区域部署私有云，以确保最佳性能和最低延迟。

前提条件：

- 设置 VMware 引擎服务管理员 IAM 角色
- "启用 VMware 引擎 API 访问和节点配额"
- 确保 CIDR 范围不会与任何内部或云子网重叠。CIDR 范围必须为 /27 或更高。



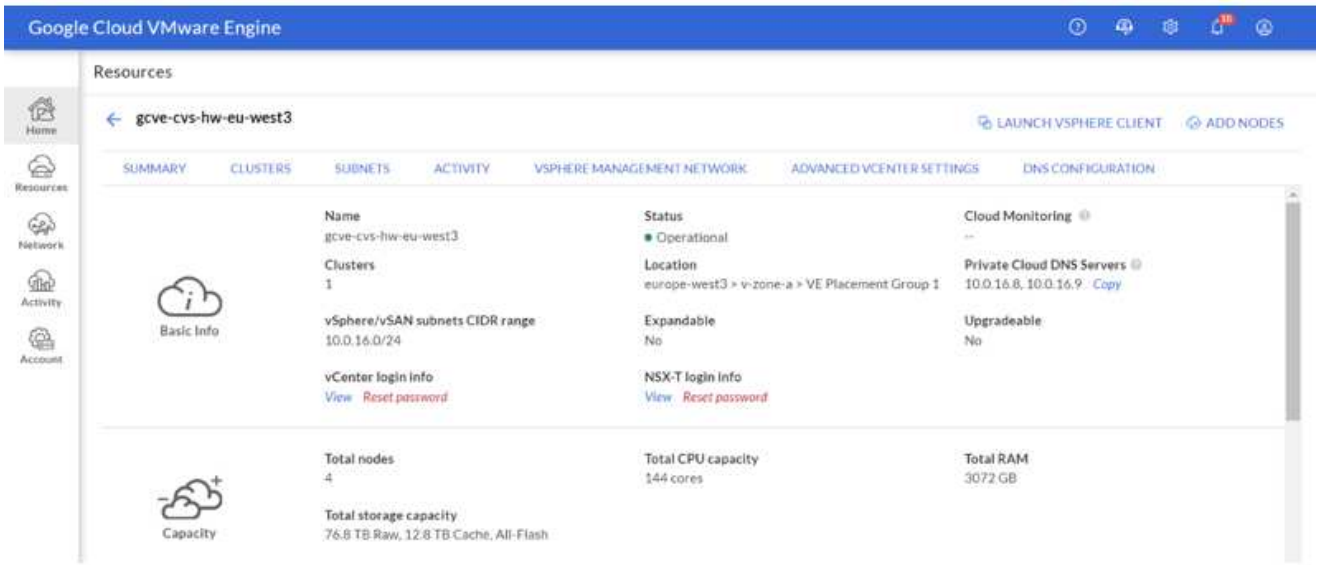
注意：创建私有云可能需要 30 分钟到 2 小时。

配置私有云后，配置对私有云的私有访问，以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。要执行此操作，请按照 "GCP 文档"。对于云卷服务，通过在租户主机项目之间执行一次性对等操作，在 VMware 引擎和 Cloud Volumes Service 之间建立连接。有关详细步骤，请按照此步骤进行操作 "链接。"。

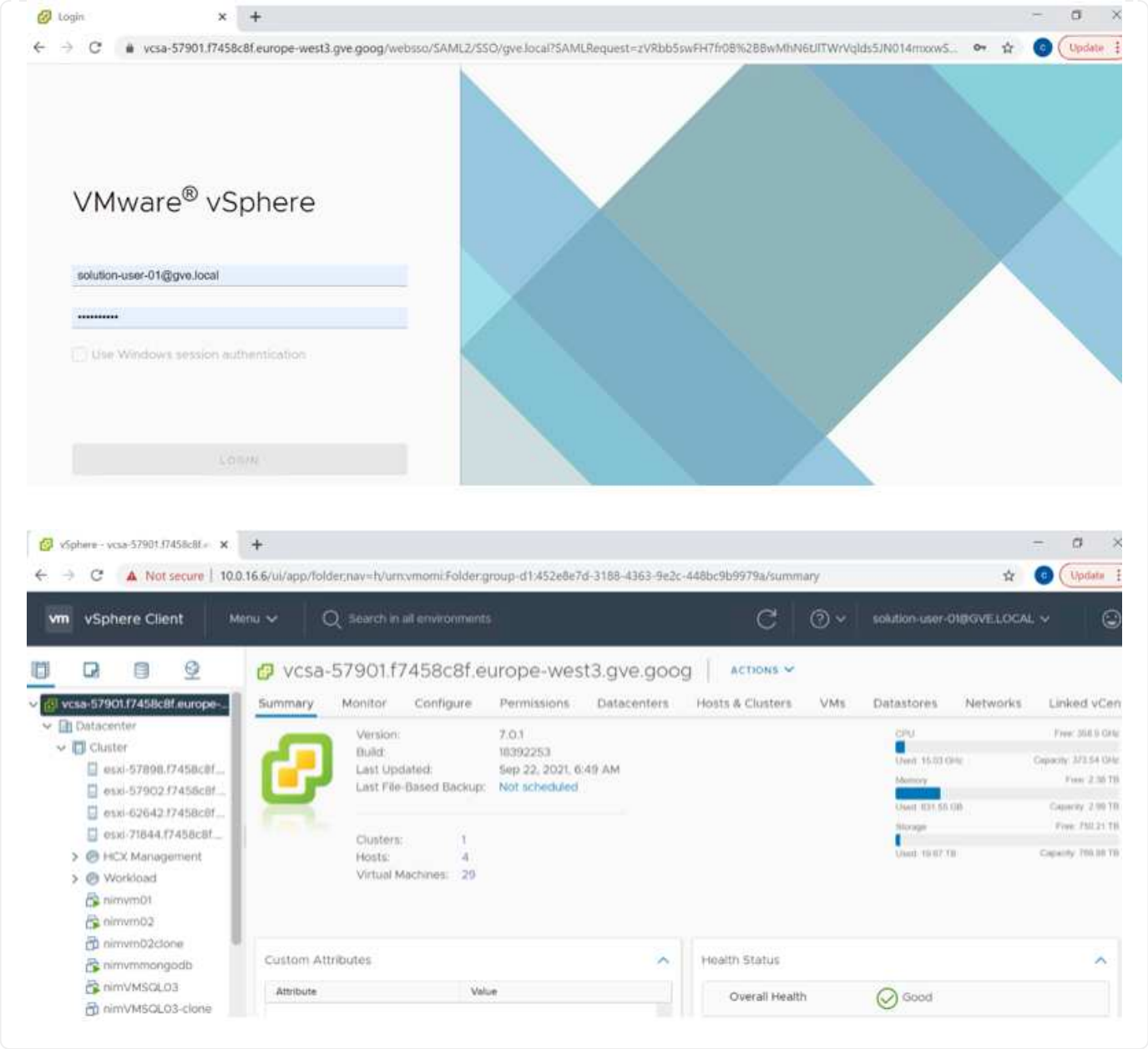
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

使用 CloudOwner@gve.local 用户登录到 vCenter 。要访问凭据，请转到 VMware 引擎门户，转到资源并选择相应的私有云。在基本信息部分中，单击 vCenter 登录信息（ vCenter Server ， HCX Manager ）或 NSX-T 登录信息（ NSX Manager ）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 并使用 admin 用户名 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 并使用管理员用户名并粘贴复制的密码以创建新分段或修改现有分层网关。

要从内部网络连接到 VMware Engine 私有云，请利用云 VPN 或 Cloud Interconnect 实现适当的连接，并确保所需端口处于打开状态。有关详细步骤，请按照此步骤进行操作 "链接。"。



将**NetApp**云卷服务补充数据存储库部署到**GCVe**

请参见 "操作步骤使用NetApp CVS将补充NFS数据存储库部署到GCVE"

适用于公有云提供商的 **NetApp** 存储选项

了解 NetApp 在三大超大规模提供商中作为存储的各种选项。

AWS/VMC

AWS 支持以下配置中的 NetApp 存储：

- FSX ONTAP 作为子系统连接的存储
- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- FSX ONTAP 作为补充NFS数据存储库

查看详细信息 "VMC的子系统连接存储选项"。查看详细信息 "VMC的补充NFS数据存储库选项"。

Azure / AVS

Azure 支持以下配置中的 NetApp 存储：

- Azure NetApp Files （ ANF ）作为子系统连接的存储
- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- Azure NetApp Files (ANF)作为补充NFS数据存储库

查看详细信息 "AVS的子系统连接存储选项"。查看详细信息 "AVS的补充NFS数据存储库选项"。

GCP / GCVE

Google Cloud 支持以下配置中的 NetApp 存储：

- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- Cloud Volumes Service （ CVS ）作为子系统连接的存储
- Cloud Volumes Service (CVS)作为补充NFS数据存储库

查看详细信息 "GCVE的子系统连接存储选项"。

了解更多信息 "适用于Google Cloud VMware Engine的NetApp Cloud Volumes Service 数据存储库支持(NetApp博客)" 或 "如何使用NetApp CVS作为Google Cloud VMware Engine的数据存储库(Google博客)"

TR-4938：将**Amazon FSX for ONTAP** 作为**NFS**数据存储库挂载到**AWS**上的**VMware Cloud**中

NetApp 公司 Niyaz Mohamed

简介

每个成功的组织都在转型和现代化的道路上。在此过程中、企业通常会利用现有的VMware投资来利用云优势、并探索如何尽可能无缝地迁移、突发、扩展和提供灾难恢复。迁移到云的客户必须评估弹性和突发、数据中心退出、数据中心整合、寿命终结情形、合并、 采集等。

虽然基于AWS的VMware Cloud是大多数客户的首选选项、因为它可以为客户提供独特的混合功能、但有限的原生 存储选项限制了它对存储工作负载繁重的组织的有用性。由于存储与主机直接相关、因此扩展存储的唯一方法是添加更多主机、这样对于存储密集型工作负载、成本可能会增加35-40%或更多。这些工作负载需要额外的存储和隔离的性能、而不是额外的功率、而是需要为额外的主机付费。这就是 "近期集成" 适用于ONTAP 的FSX可通过AWS上的VMware Cloud方便地用于存储和性能密集型工作负载。

我们来考虑以下情形：客户需要八台主机来提供功率(vCPU/vMem)、但他们也需要大量存储。根据他们的评

估、他们需要16台主机来满足存储要求。这样可以提高总体TCO、因为他们必须购买所有这些额外的动力、而他们真正需要的只是更多的存储。这适用于任何使用情形、包括迁移、灾难恢复、突发、开发/测试、 等等。

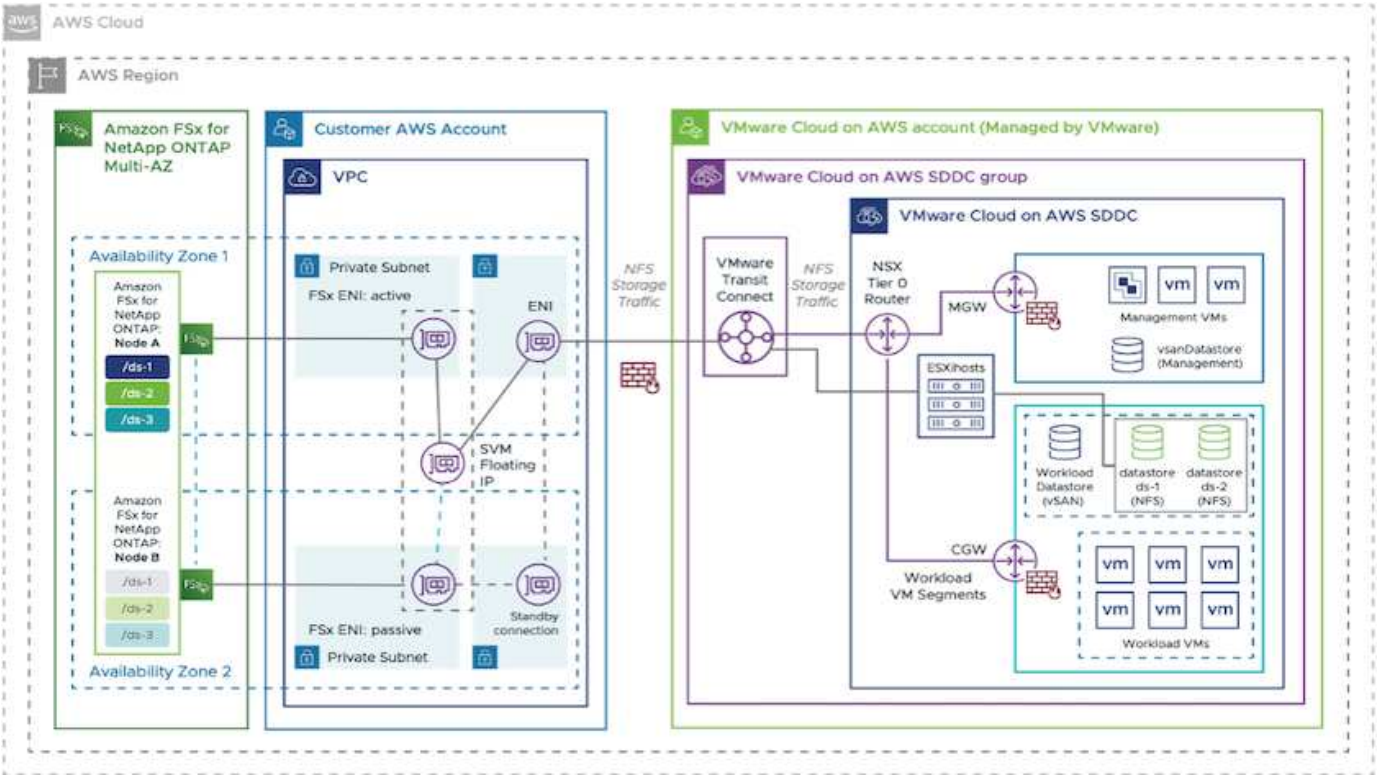
本文档将指导您完成在AWS上将适用于ONTAP 的FSX配置和连接为适用于VMware Cloud的NFS数据存储库所需的步骤。

VMware也提供了此解决方案。请访问 "VMware云技术区" 有关详细信息 …

连接选项

基于AWS的VMware Cloud支持适用于ONTAP 的FSX的多AZ和单AZ部署。

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



高级部署步骤如下：

1. 在新的指定VPC中创建适用于ONTAP 的Amazon FSx。
2. 创建SDDC组。
3. 创建VMware Transit Connect和Tgw.
4. 配置路由(AWS VPC和SDDC)和安全组。
5. 将NFS卷作为数据存储库连接到SDDC集群。

在将适用于ONTAP 的FSX配置和连接为NFS数据存储库之前、您必须先设置云SDDC环境或将现有SDDC升级到v1.20或更高版本。有关详细信息，请参见 "在AWS上开始使用VMware Cloud"。

延伸型集群当前不支持适用于ONTAP 的FSX。

结论

本文档介绍了在AWS上为适用于ONTAP 的Amazon FSX配置VMware云所需的步骤。Amazon FSX for ONTAP 提供了出色的选项、可用于部署和管理应用程序工作负载以及文件服务、同时通过将数据需求无缝地传输到应用程序层来降低TCO。无论使用何种情形、均可选择基于AWS的VMware云以及适用于ONTAP 的Amazon FSx、以快速实现云优势、从内部环境到AWS的一致基础架构和运营、工作负载的双向可移植性以及企业级容量和性能。这是用于连接存储的熟悉过程。请记住、随新名称一起更改的只是数据的位置；工具和流程都保持不变、Amazon FSx for ONTAP 有助于优化整体部署。

要了解有关此过程的更多信息、请随时观看详细的演练视频。

适用于ONTAP VMware Cloud的Amazon FSx

适用于 **AWS** 的 **NetApp** 子系统连接存储选项

AWS支持使用原生 FSX服务(FSX ONTAP)或Cloud Volumes ONTAP (CVO)的子系统连接NetApp存储。

FSX ONTAP

Amazon FSX for NetApp ONTAP 是一项完全托管的服务、可提供基于NetApp常用ONTAP 文件系统构建的高度可靠、可扩展、高性能和功能丰富的文件存储。FSX for ONTAP 将NetApp文件系统的常见特性、性能、功能和API操作与完全托管的AWS服务的灵活性、可扩展性和精简性相结合。

FSX for ONTAP 提供功能丰富、快速且灵活的共享文件存储、可从AWS或内部运行的Linux、Windows和macOS计算实例广泛访问。适用于ONTAP 的FSX可提供具有亚毫秒级延迟的高性能固态驱动器(SSD)存储。借助适用于ONTAP 的FSX、您可以为工作负载实现SSD级别的性能、而只需为一小部分数据购买SSD存储即可。

只需单击一个按钮、即可使用适用于ONTAP 的FSX轻松管理数据、因为您可以创建文件快照、克隆和复制文件。此外、适用于ONTAP 的FSX会自动将数据分层到成本较低的弹性存储中、从而减少配置或管理容量的需求。

此外、适用于ONTAP 的FSX还可通过完全托管的备份提供高可用性和持久性存储、并支持跨区域灾难恢复。为了更轻松地保护和保护数据、适用于ONTAP 的FSx支持常见的数据安全和防病毒应用程序。

FSX ONTAP 作为子系统连接的存储

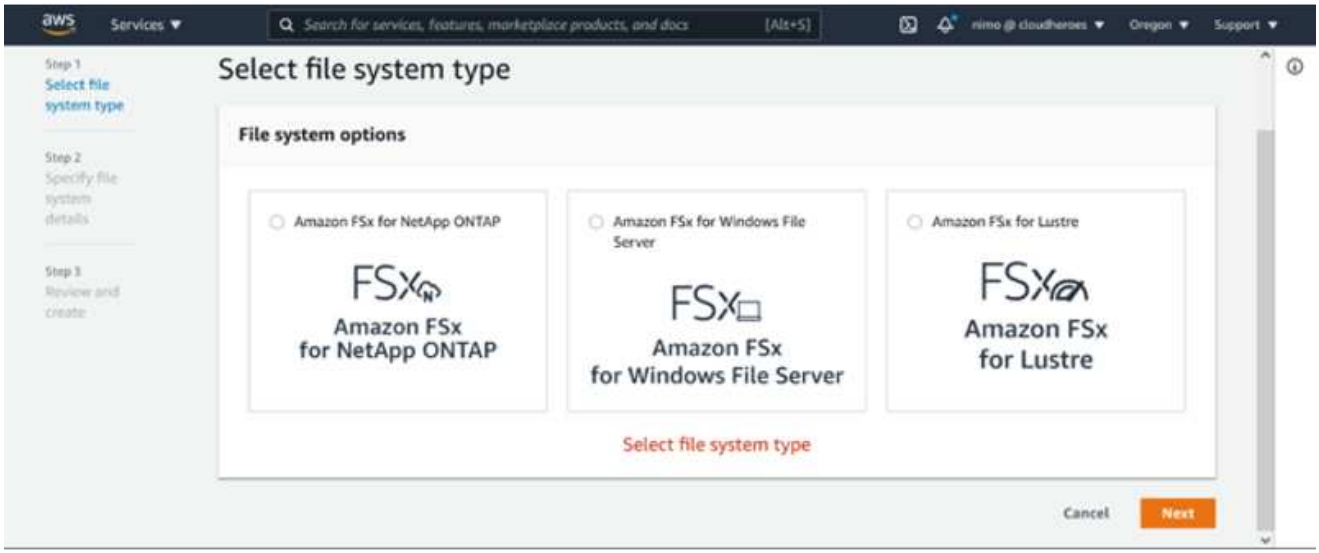
在 **AWS** 上为适用于 **NetApp ONTAP** 的 **Amazon FSX** 配置 **VMware Cloud**

Amazon FSX for NetApp ONTAP 文件共享和 LUN 可以从 AWS 上的 VMware Cloud 的 VMware SDDC 环境中创建的 VM 挂载。此外，还可以使用 NFS 或 SMB 协议在 Linux 客户端上挂载这些卷并将其映射到 Windows 客户端上，通过 iSCSI 挂载 LUN 时，可以在 Linux 或 Windows 客户端上以块设备的形式访问这些 LUN 。可通过以下步骤快速设置适用于 NetApp ONTAP 文件系统的 Amazon FSX 。

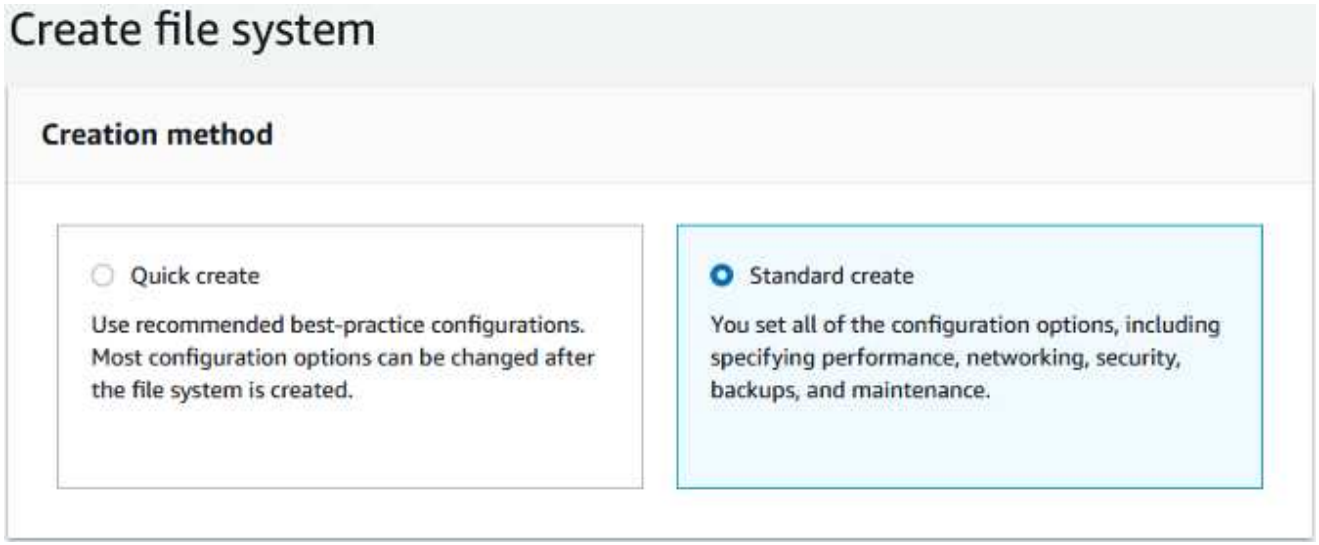
适用于 NetApp ONTAP 的 Amazon FSx 和基于 AWS 的 VMware Cloud 必须位于同一可用性区域中，才能提高性能并避免在可用性区域之间传输数据。

要创建和挂载适用于 NetApp ONTAP 的 Amazon FSX 文件系统，请完成以下步骤：

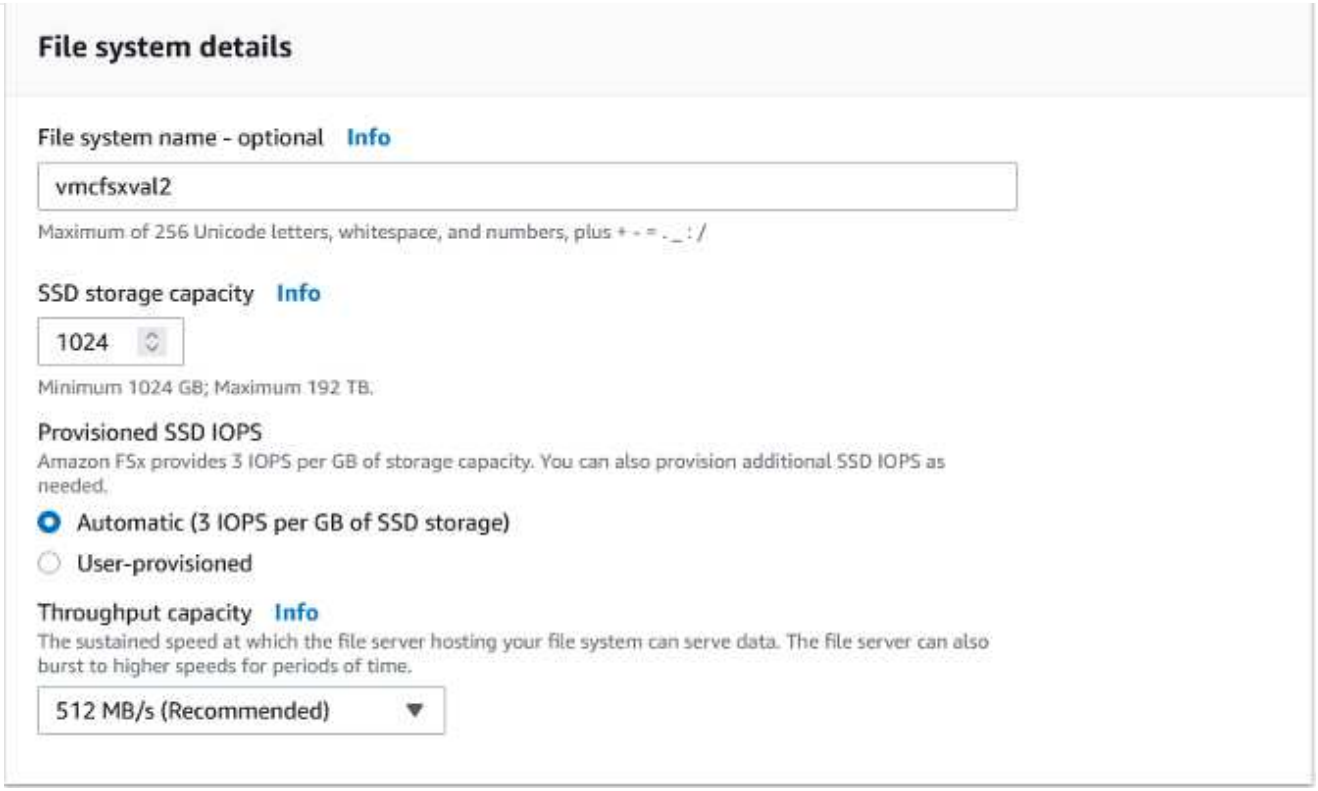
1. 打开 "Amazon FSX 控制台" 并选择创建文件系统以启动文件系统创建向导。
2. 在选择文件系统类型页面上，选择适用于 NetApp ONTAP 的 Amazon FSx ，然后选择下一步。此时将显示创建文件系统页面。



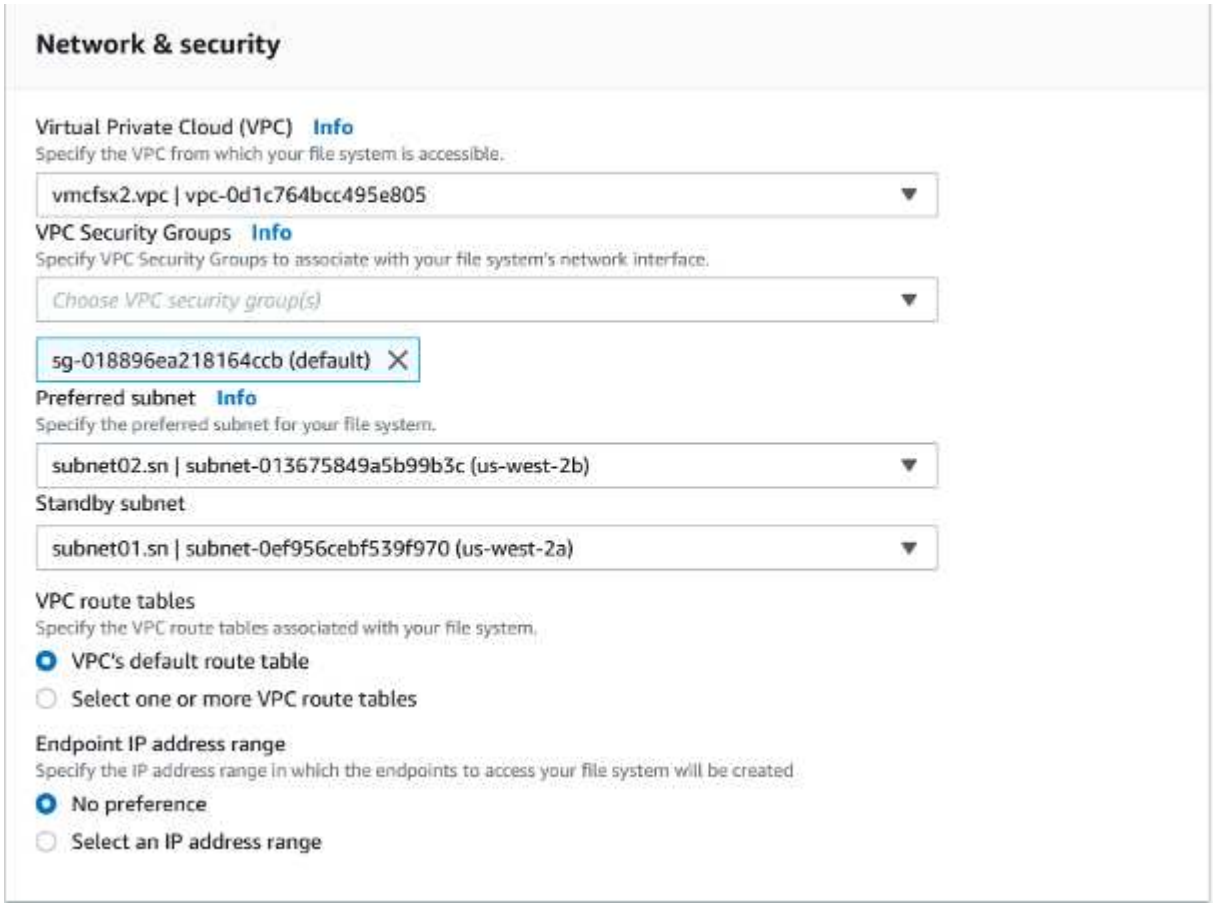
1. 在网络部分中，对于虚拟私有云（ Virtual Private Cloud ， VPC ），选择适当的 VPC 和首选子网以及路由表。在这种情况下，将从下拉列表中选择 vmcfsx2.vPC 。



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。

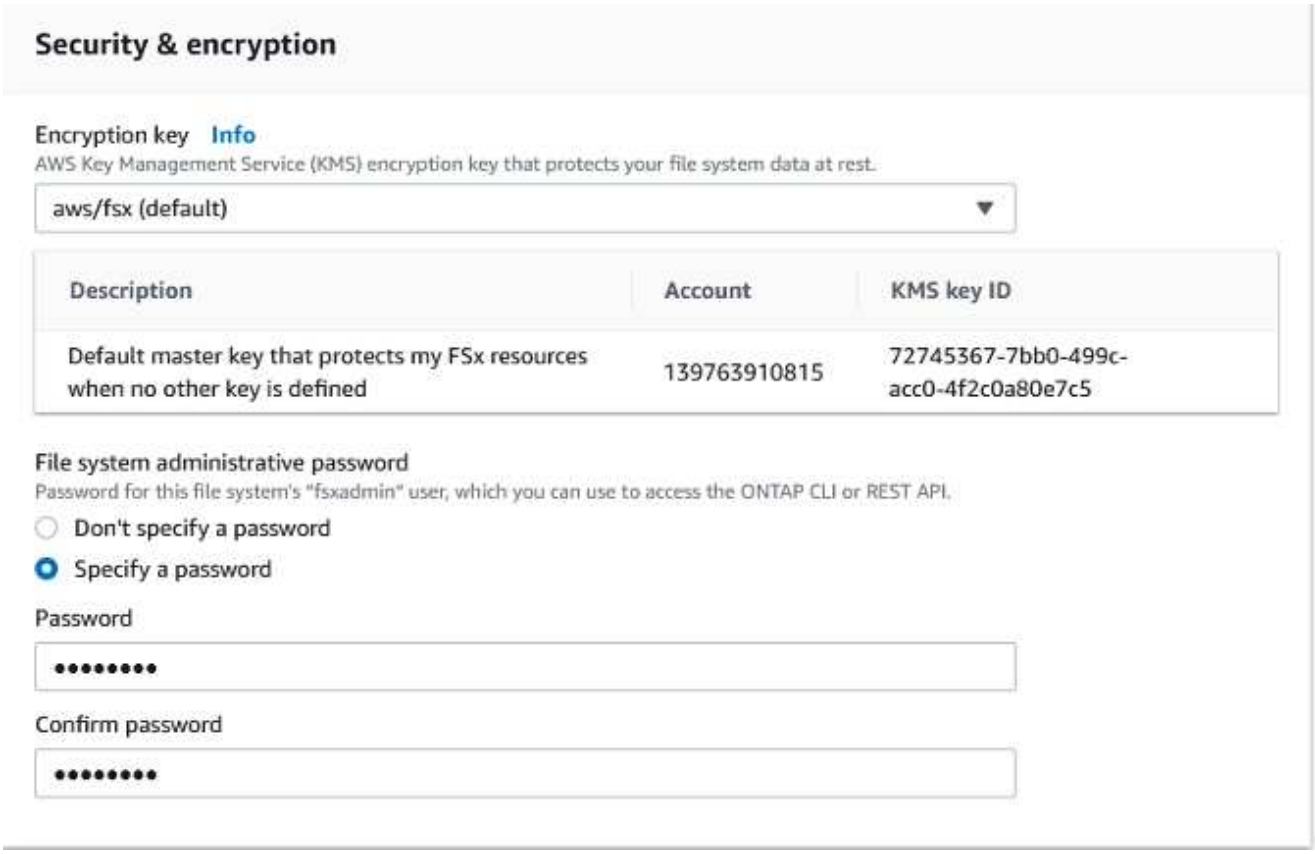


1. 在网络部分中，对于虚拟私有云（ Virtual Private Cloud ， VPC ），选择适当的 VPC 和首选子网以及路由表。在这种情况下，将从下拉列表中选择 vmcfsx2.vPC 。

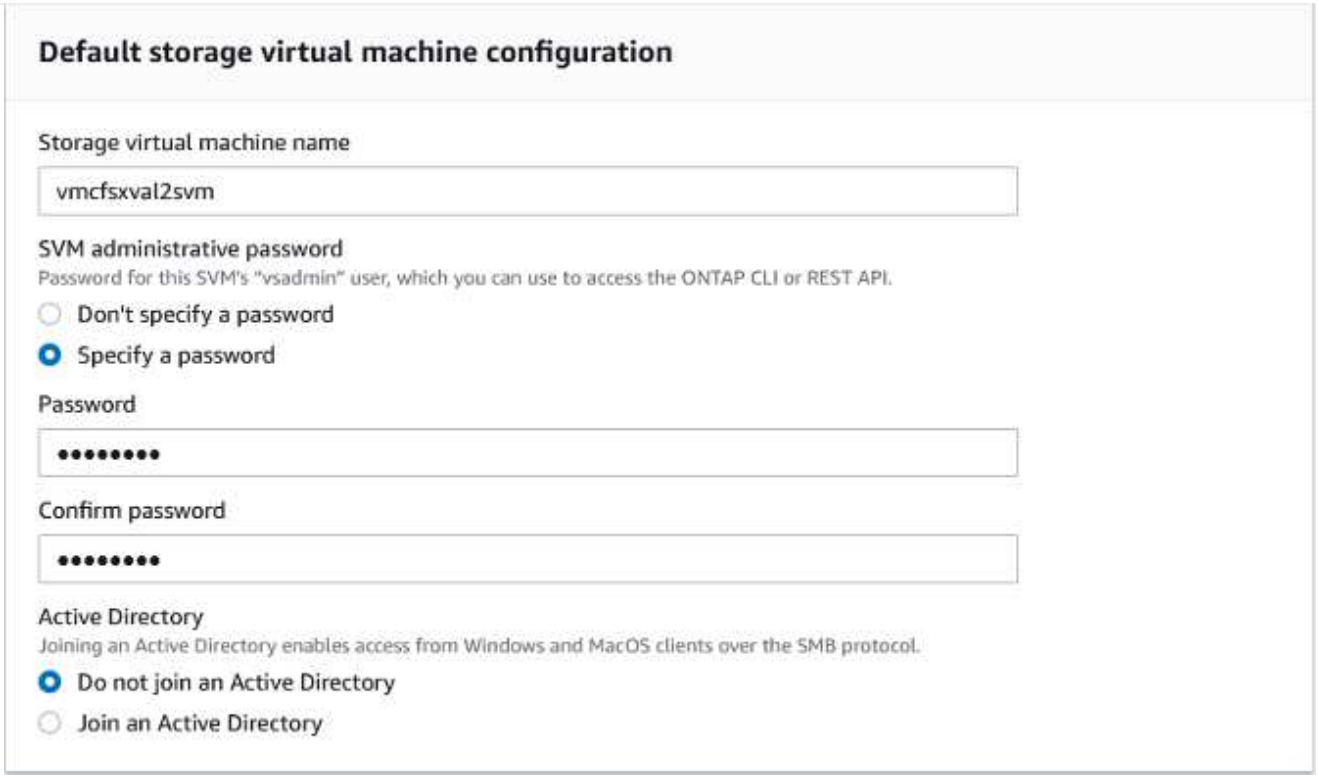


在网络部分中，对于虚拟私有云（ Virtual Private Cloud ， VPC ），选择适当的 VPC 和首选子网以及路由表。在这种情况下，将从下拉列表中选择 vmcfsx2.vPC 。

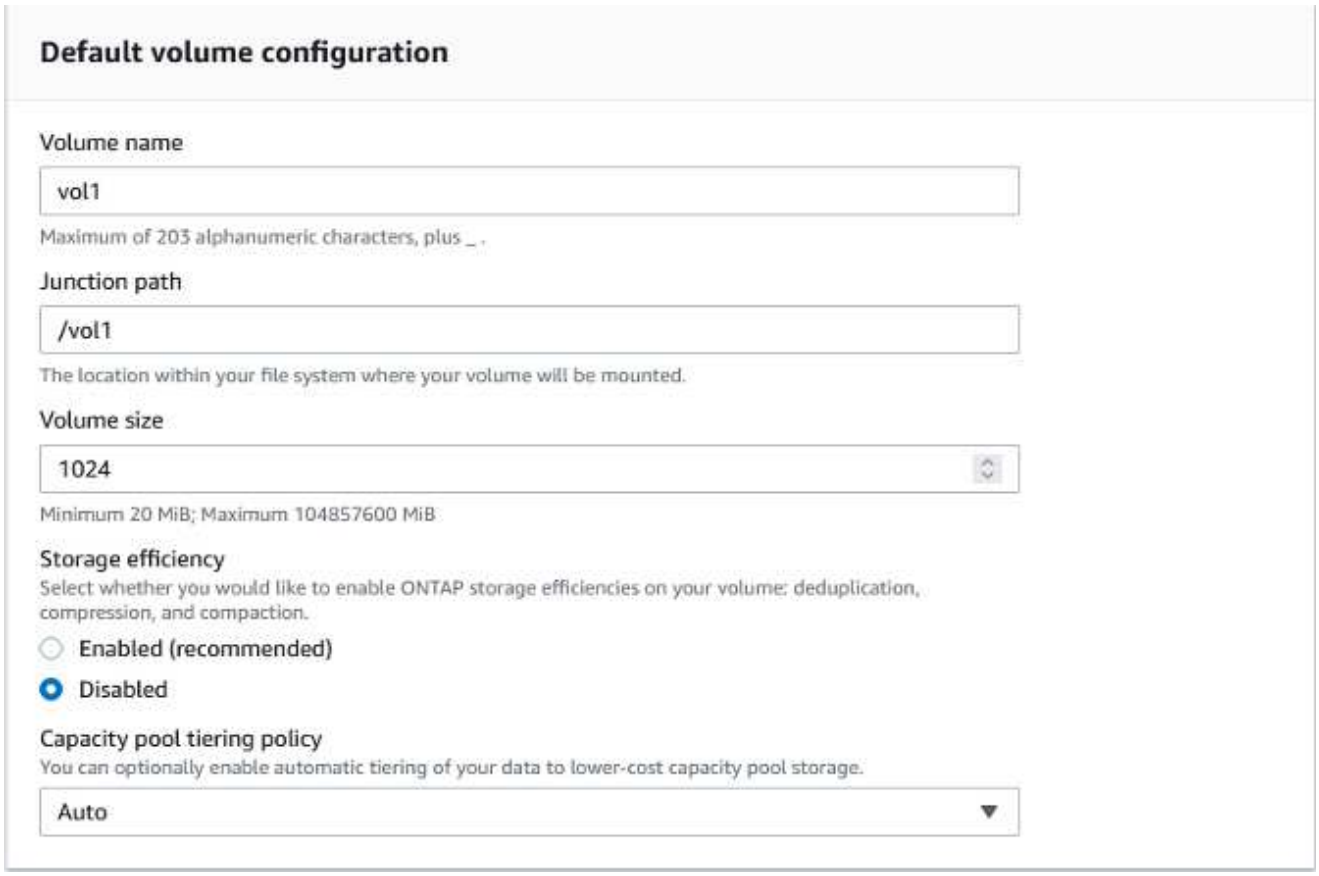
1. 在安全性和加密部分中，对于加密密钥，选择用于保护文件系统空闲数据的 AWS 密钥管理服务（ AWS KMS ）加密密钥。对于文件系统管理密码，输入 fsxadmin 用户的安全密码。



1. 在虚拟机中，并指定与 vsadmin 结合使用的密码，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 SVM 以配置 SMB 共享。在默认 Storage Virtual Machine 配置部分中，在此验证中提供存储的名称， SMB 共享使用自管理的 Active Directory 域进行配置。

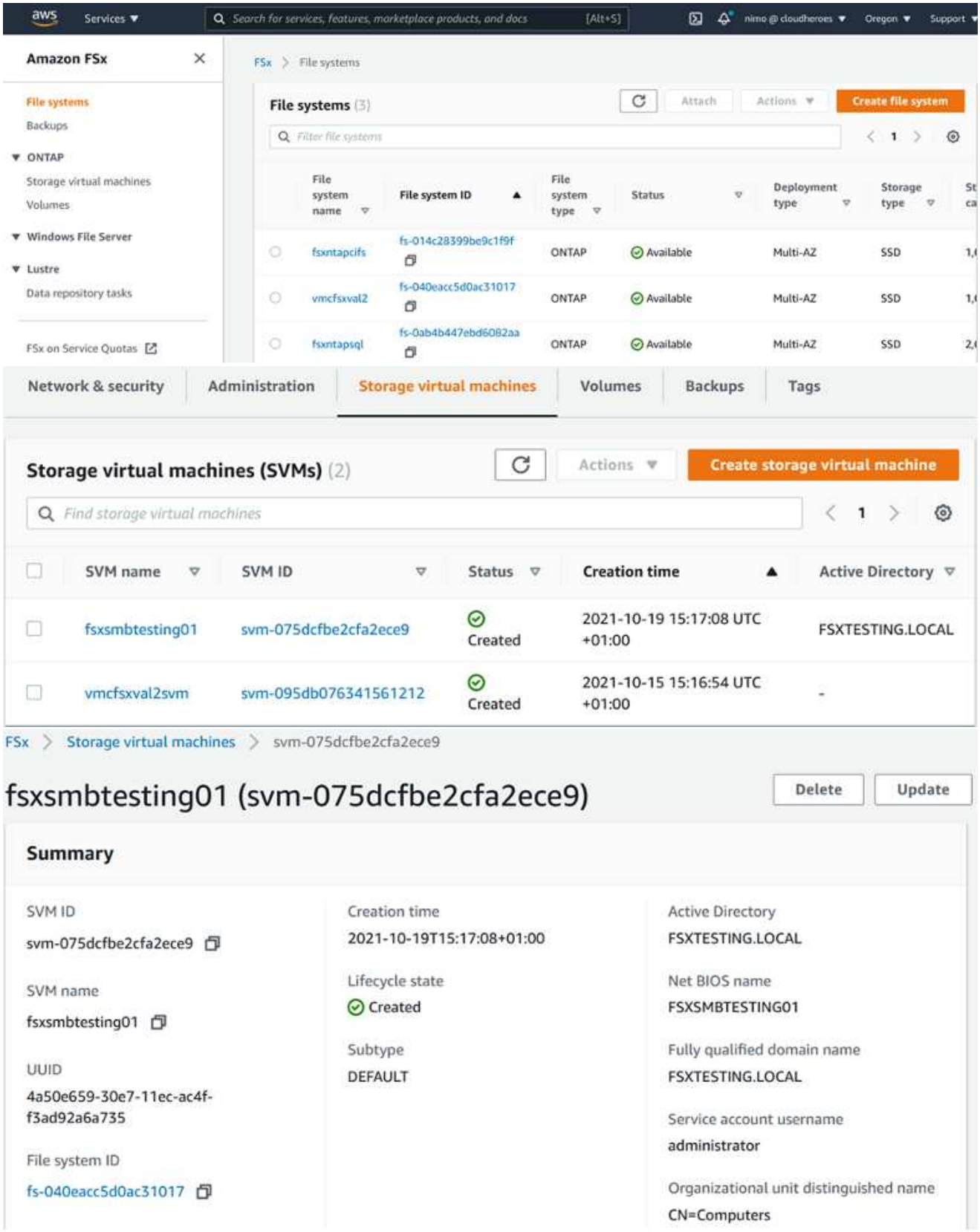


1. 在默认卷配置部分中，指定卷名称和大小。这是一个 NFS 卷。对于存储效率，请选择启用以启用 ONTAP 存储效率功能（数据压缩，重复数据删除和数据缩减），或者选择禁用以禁用这些功能。



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。



有关更多详细信息，请参见 "适用于 NetApp ONTAP 的 Amazon FSX 入门"。

按上述方式创建文件系统后，使用所需的大小和协议创建卷。

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. 此时将显示创建卷对话框。

出于演示目的，本节创建了一个 NFS 卷，可以轻松地挂载在 AWS 上的 VMware 云上运行的 VM 上。nfsdemovol01 创建如下：

在 **Linux** 客户端上挂载 **FSX ONTAP** 卷

挂载上一步中创建的 FSX ONTAP 卷。在 AWS SDDC 上 VMC 中的 Linux VM 中，完成以下步骤：

1. 连接到指定的 Linux 实例。
2. 使用安全 Shell （ SSH ）在实例上打开一个终端，并使用相应的凭据登录。
3. 使用以下命令为卷的挂载点创建一个目录：

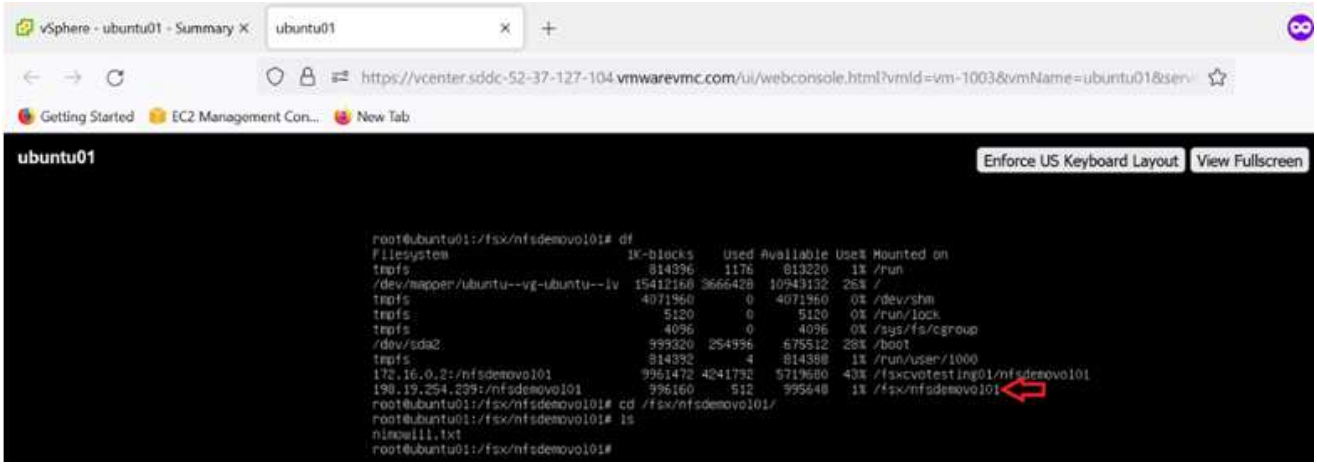
```
 $ sudo mkdir /fsx/nfsdemovol01
```

. 将适用于 NetApp ONTAP NFS 的 Amazon FSX 卷挂载到上一步创建的目录中。

```
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 命令以验证挂载。

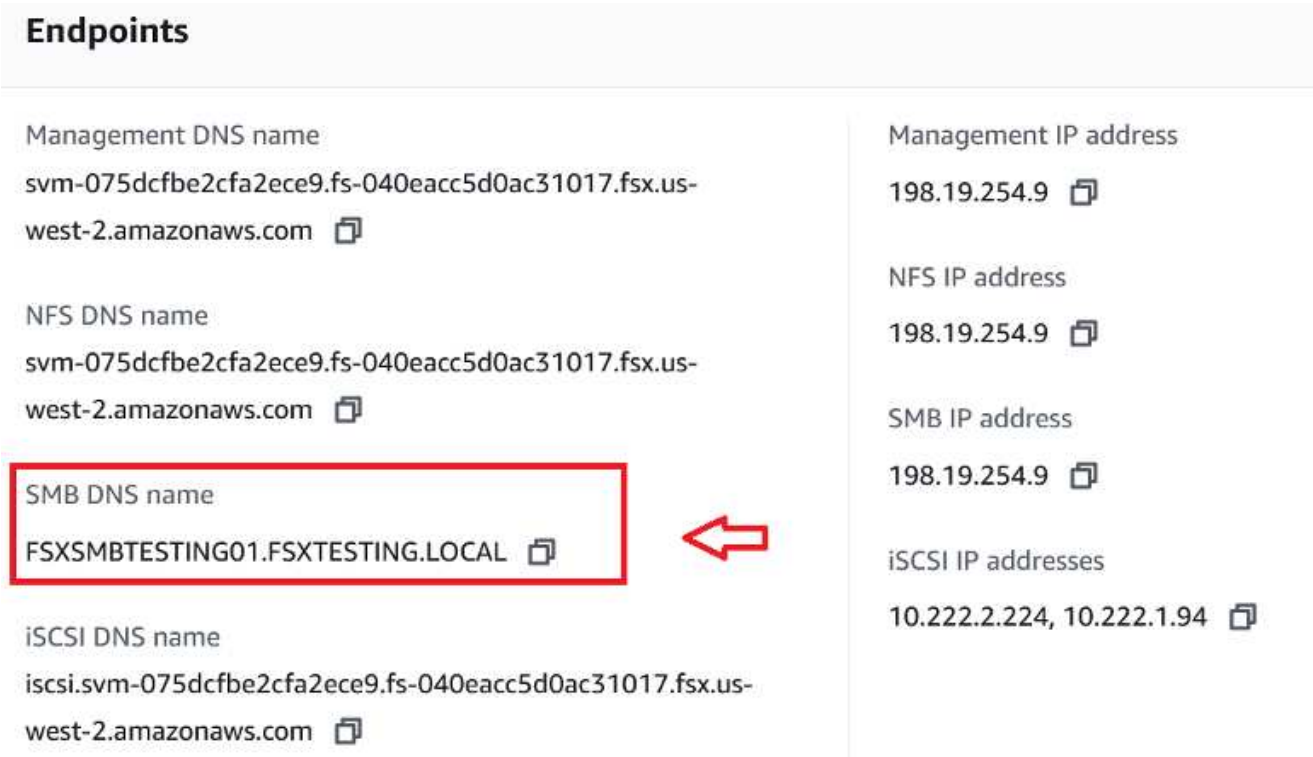


在 Linux 客户端上挂载 FSX ONTAP 卷

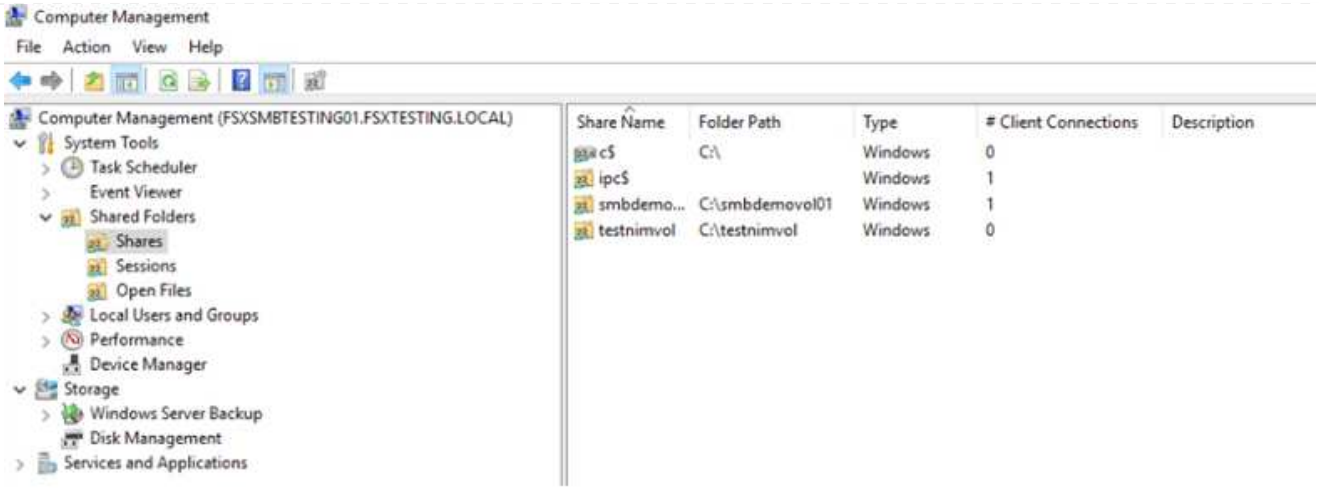
要管理和映射 Amazon FSX 文件系统上的文件共享，必须使用共享文件夹图形用户界面。

1. 打开 " 开始 " 菜单，然后使用以管理员身份运行来运行 fsmgmt.msc 。这样将打开共享文件夹 GUI 工具。
2. 单击操作 > 所有任务，然后选择连接到另一台计算机。
3. 对于另一台计算机，输入 Storage Virtual Machine （ SVM ）的 DNS 名称。例如，在此示例中使用了 FSXSMBTESTING01.FSXTESTING.local 。

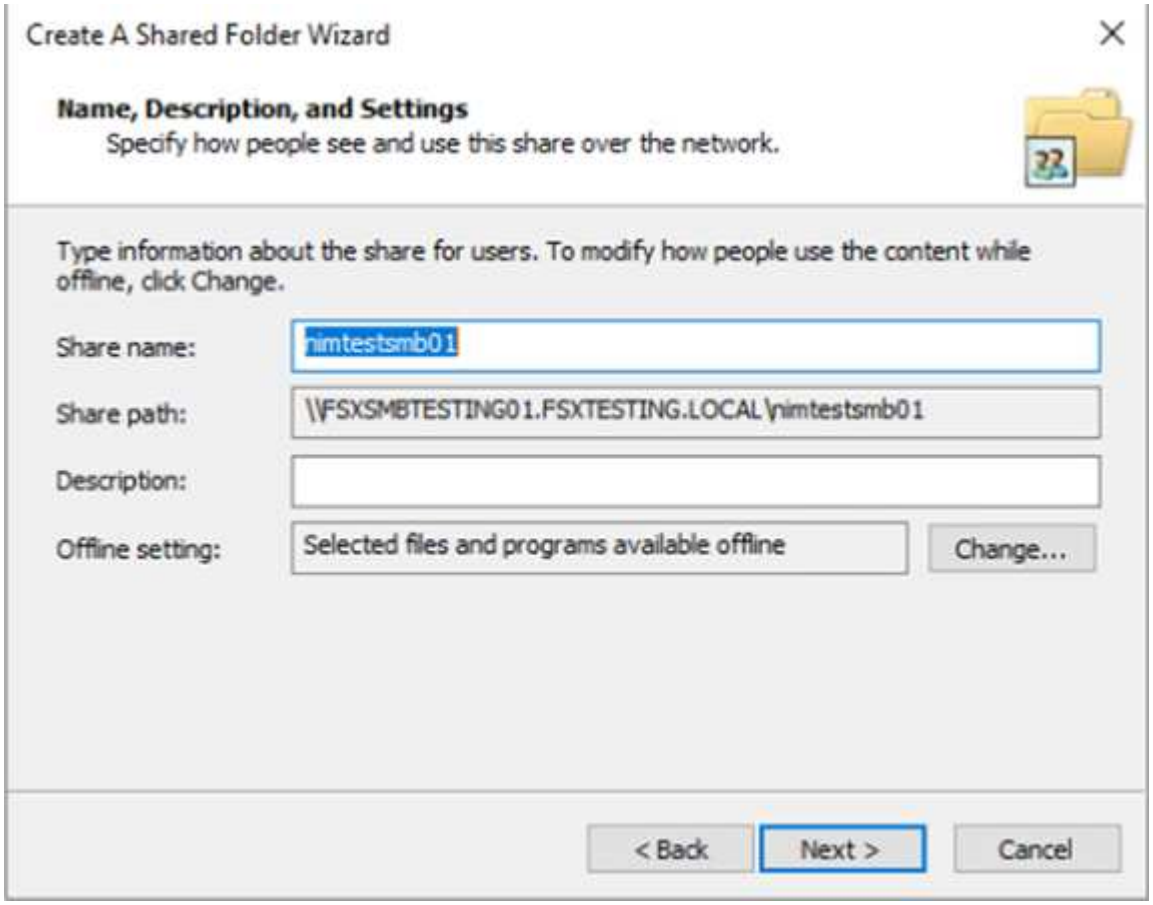
TP 可在 Amazon FSX 控制台上找到 SVM 的 DNS 名称，选择 Storage Virtual Machine ，选择 SVM ，然后向下滚动到端点以查找 SMB DNS 名称。单击确定。Amazon FSX 文件系统将显示在共享文件夹列表中。



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

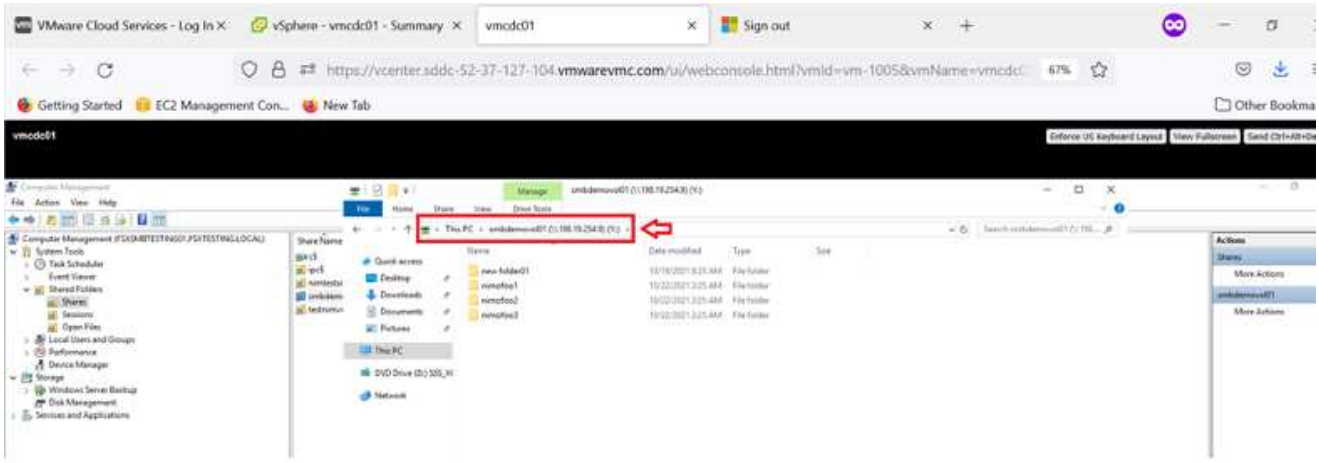


1. 现在，选择一个新共享并完成创建共享文件夹向导。



要了解有关在 Amazon FSX 文件系统上创建和管理 SMB 共享的详细信息，请参见 "创建 SMB 共享"。

1. 建立连接后，可以连接 SMB 共享并将其用于应用程序数据。为此，请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 上在 VMware Cloud 上运行的虚拟机上。



使用 iSCSI 将适用于 NetApp ONTAP LUN 的 FSX 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 。要在适用于 NetApp ONTAP 的 Amazon FSX 中配置 LUN ，请按照找到的文档进行操作 "此处"。

在 Linux 客户端上，确保 iSCSI 守护进程正在运行。配置 LUN 后，请参见有关使用 Ubuntu 配置 iSCSI 的详细指南（示例） "此处"。

本文介绍了如何将 iSCSI LUN 连接到 Windows 主机：

在适用于 **NetApp ONTAP** 的 **FSX** 中配置 **LUN**：

1. 使用 ONTAP 文件系统的 FSX 管理端口访问 NetApp ONTAP 命令行界面。
2. 按照规模估算输出所示，使用所需大小创建 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 以控制哪些主机可以访问特定 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
```

此时将显示两个条目。

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
```

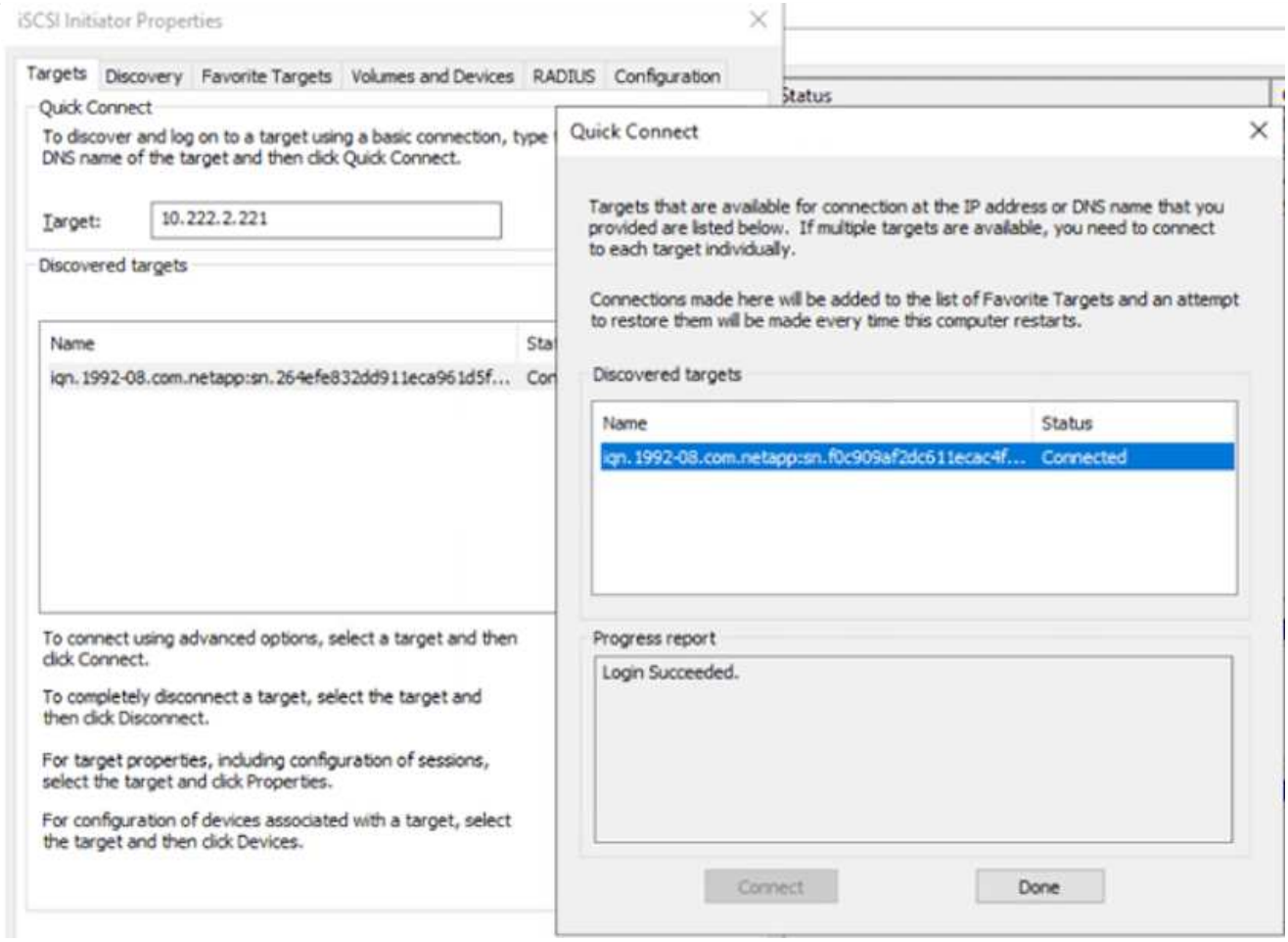
此时将显示两个条目。

1. 将新配置的 LUN 连接到 Windows VM：

要将新 LUN 连接到 AWS SDDC 上 VMware 云上的 Windows 主机，请完成以下步骤：

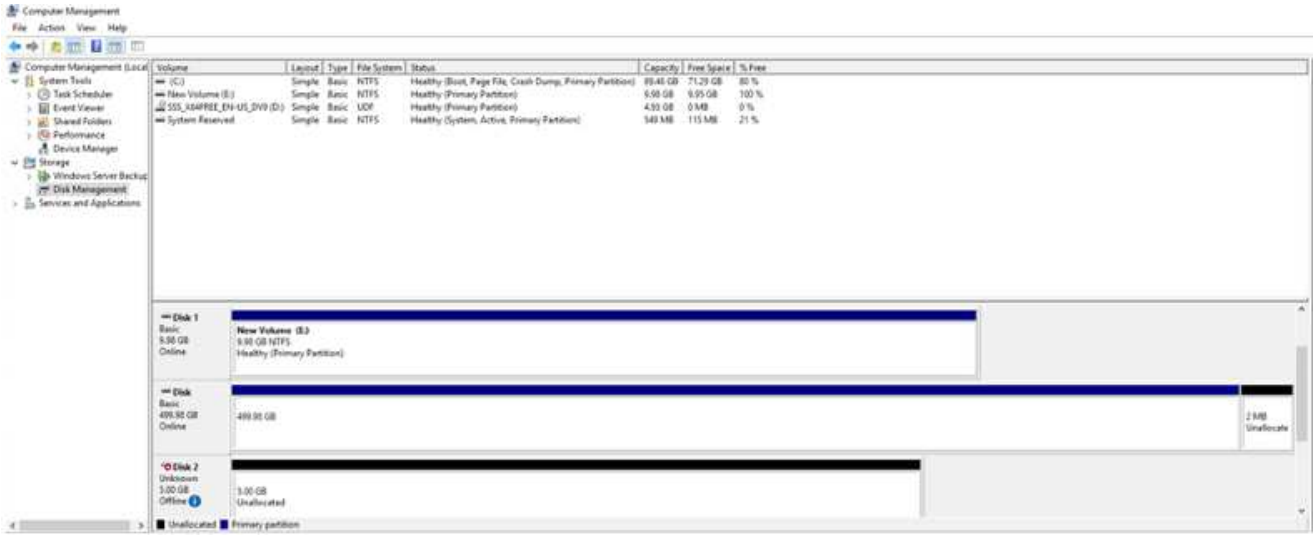
1. RDP 到 AWS SDDC 上 VMware Cloud 上托管的 Windows VM 。
2. 导航到服务器管理器 > 信息板 > 工具 > iSCSI 启动程序以打开 iSCSI 启动程序属性对话框。
3. 在发现选项卡中，单击发现门户或添加门户，然后输入 iSCSI 目标端口的 IP 地址。
4. 从目标选项卡中，选择已发现的目标，然后单击登录或连接。
5. 选择启用多路径，然后选择 " 计算机启动时自动还原此连接 " 或 " 将此连接添加到收藏目标列表 " 。单击高级。

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



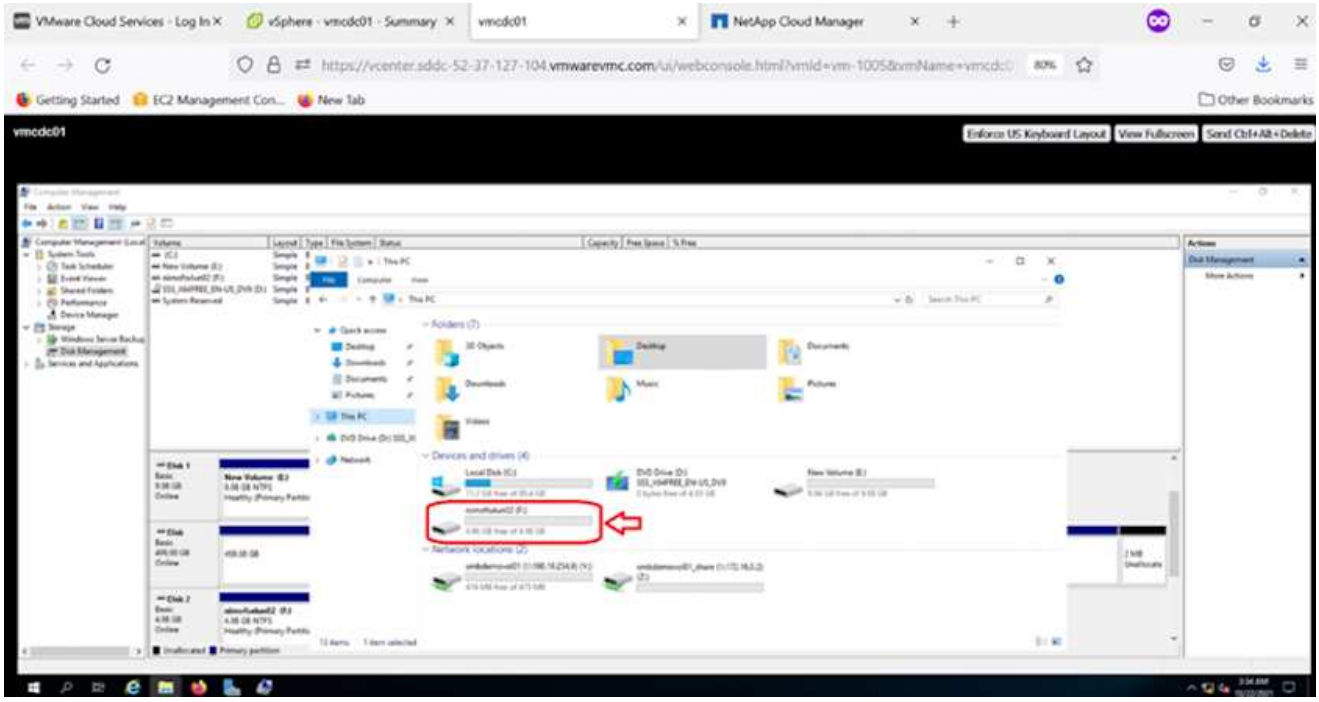
Storage Virtual Machine （ SVM ）上的 LUN 在 Windows 主机中显示为磁盘。主机不会自动发现添加的任何新磁盘。通过完成以下步骤触发手动重新扫描以发现磁盘：

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。



当新 LUN 首次由 Windows 主机访问时，它没有分区或文件系统。通过完成以下步骤初始化 LUN ，并可选择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，驱动器 F ： 已挂载。



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP 是行业领先的云数据管理解决方案 、基于NetApp的ONTAP 存储软件构建、可在Amazon Web Services (AWS)、Microsoft Azure和Google Cloud Platform (GCP)上本机获得。

它是ONTAP 的软件定义版本、使用云原生存储、可以在云端和内部环境中使用相同的存储软件、从而减少了对IT员工进行全新数据管理方法培训的需求。

借助CVO、客户可以无缝地将数据从边缘、数据中心、云和云端来回移动、从而将混合云整合在一起—所有这些都通过一个单一窗格管理控制台NetApp Cloud Manager进行管理。

按照设计、CVO可提供极致性能和高级数据管理功能、甚至可以满足云中要求最苛刻的应用程序的需求

Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储

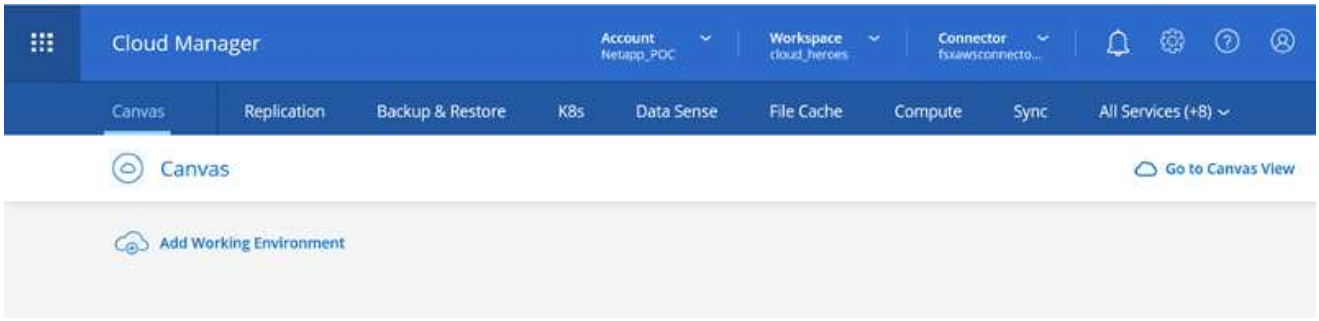
在 **AWS** 中部署新的 **Cloud Volumes ONTAP** 实例（自行操作）

可以从 AWS SDDC 环境中的 VMware 云中创建的 VM 挂载 Cloud Volumes ONTAP 共享和 LUN 。这些卷还可以挂载在原生 AWS VM Linux Windows 客户端上，并且在通过 iSCSI 挂载时，可以在 Linux 或 Windows 客户端上以块设备的形式访问 LUN ，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。

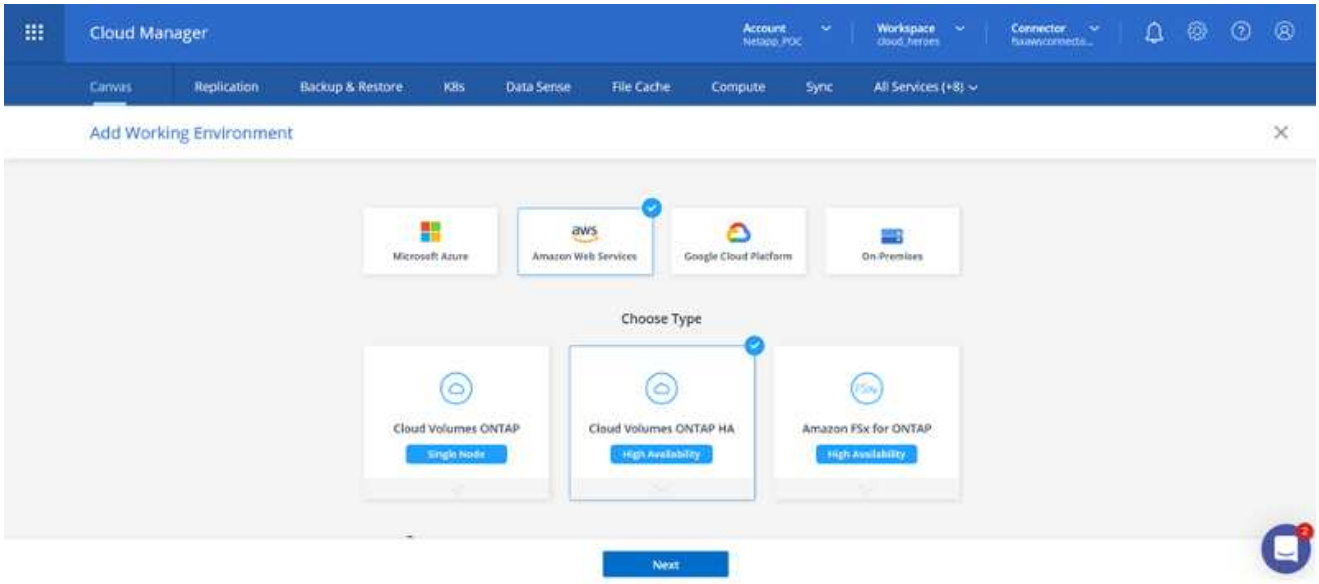
要将卷从内部环境复制到云以实现灾难恢复或迁移，请使用站点到站点 VPN 或 DirectConnect 与 AWS 建立网络连接。将数据从内部复制到 Cloud Volumes ONTAP 不在本文档的讨论范围之内。要在内部系统和 Cloud Volumes ONTAP 系统之间复制数据，请参见 "在系统之间设置数据复制"。

使用 "Cloud Volumes ONTAP 规模估算工具" 以准确估算 Cloud Volumes ONTAP 实例的大小。此外，还可以监控内部性能，以用作 Cloud Volumes ONTAP 规模估算器中的输入。

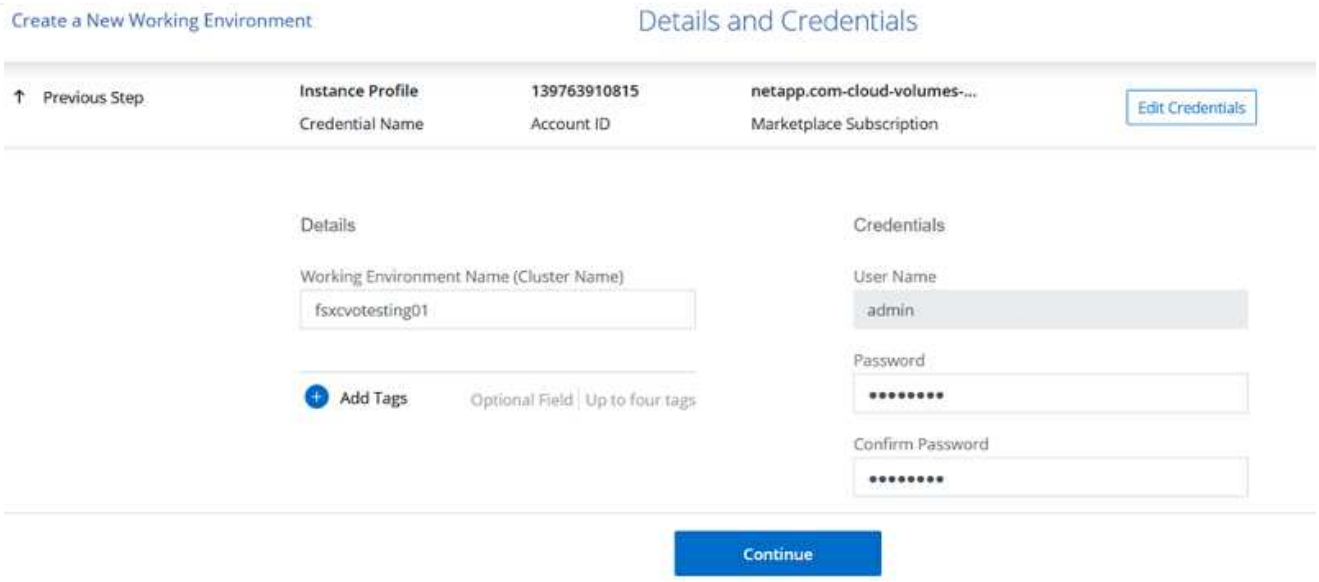
1. 登录到 NetApp Cloud Central ；此时将显示 Fabric View 屏幕。找到 Cloud Volumes ONTAP 选项卡，然后选择转到 Cloud Manager 。登录后，将显示 " 画布 " 屏幕。



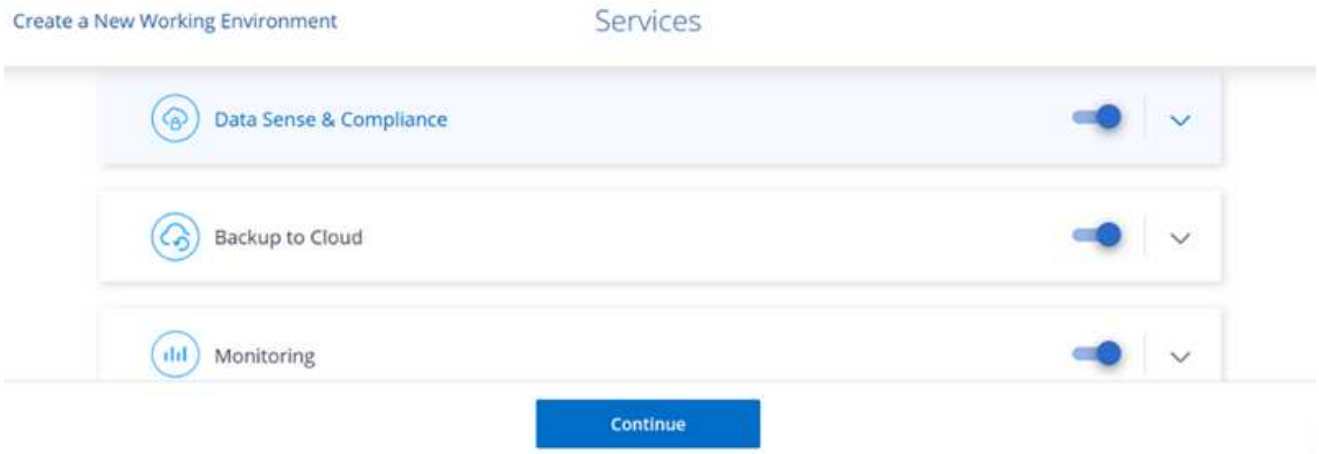
1. 在 Cloud Manager 主页上，单击添加工作环境，然后选择 AWS 作为云以及系统配置的类型。



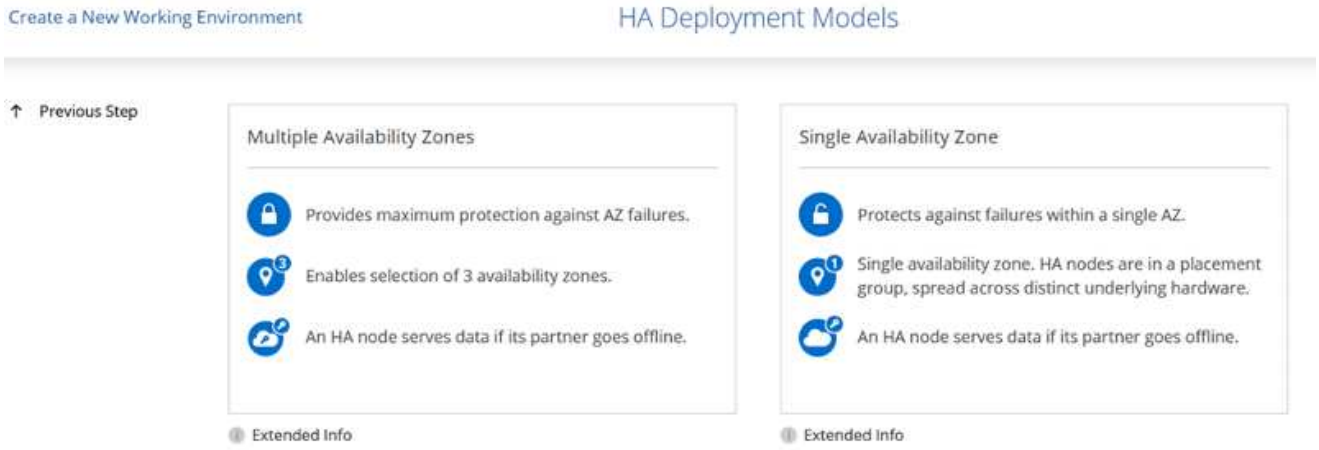
1. 提供要创建的环境的详细信息，包括环境名称和管理员凭据。单击 Continue （继续）。



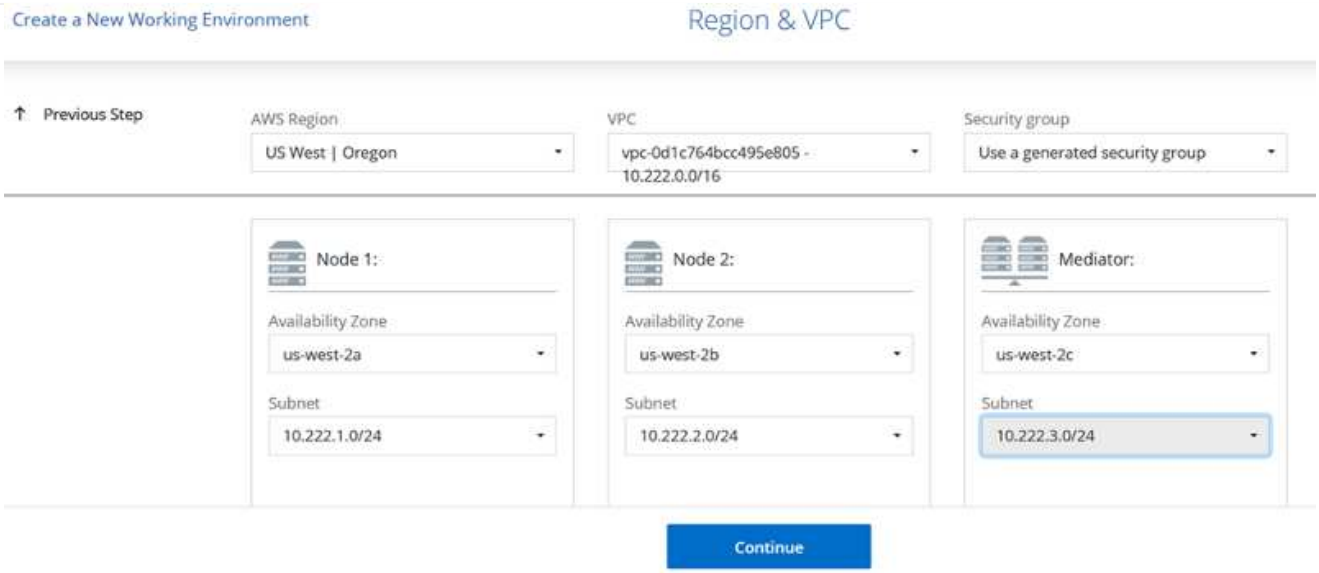
1. 为Cloud Volumes ONTAP部署选择附加服务、包括BlueXP分类、BlueXP备份和恢复以及Cloud Insights。单击 Continue （继续）。



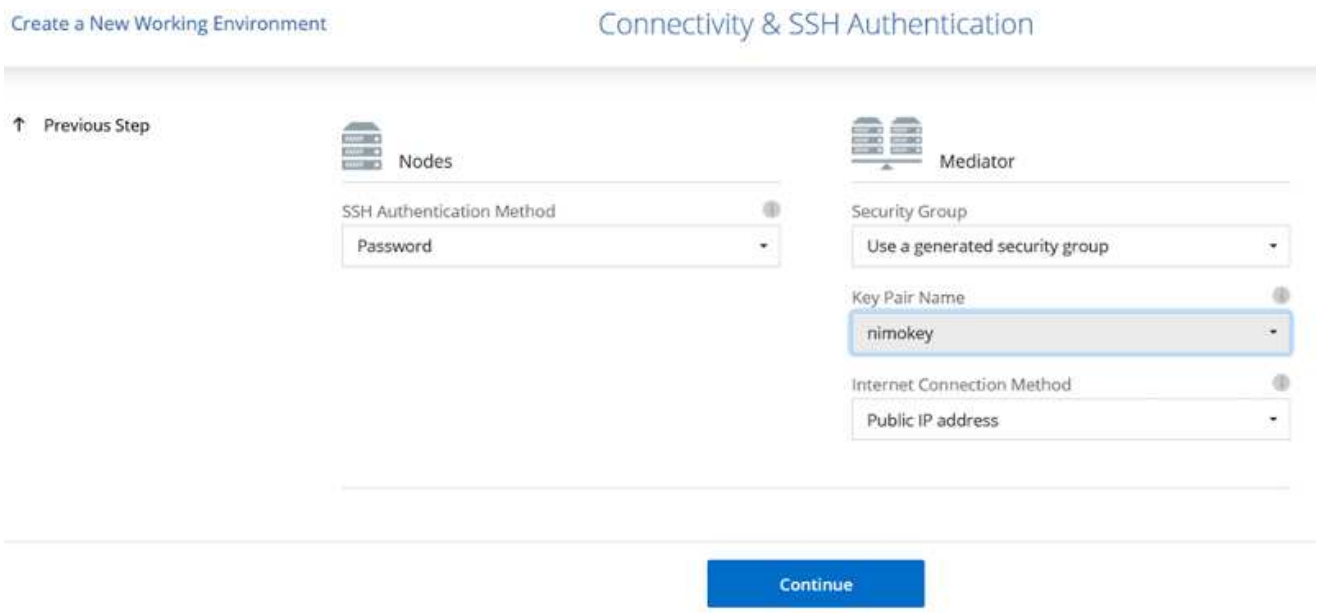
1. 在 HA 部署模式页面上，选择多个可用性区域配置。



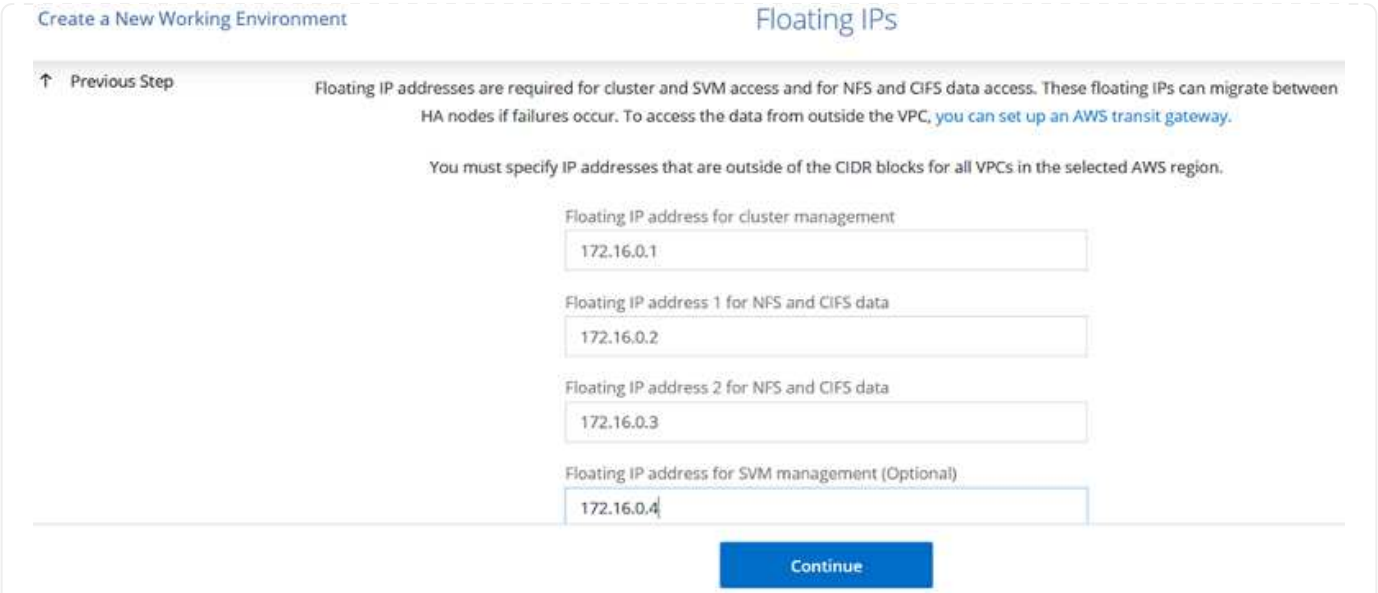
1. 在区域和 VPC 页面上，输入网络信息，然后单击继续。



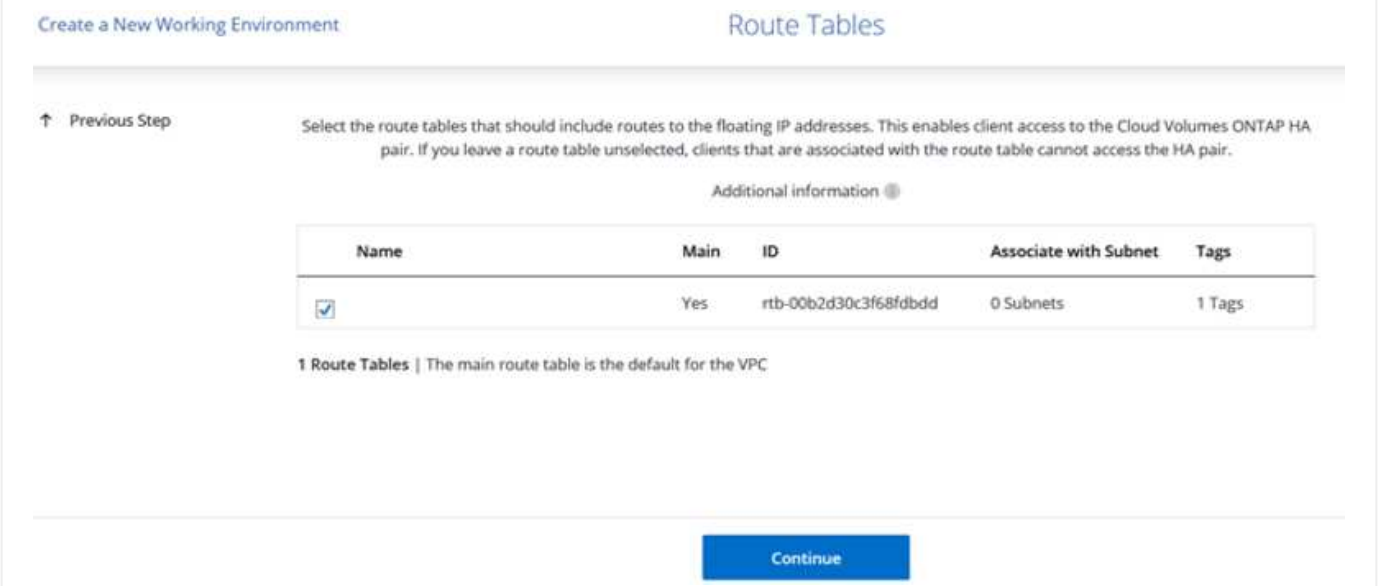
1. 在“ Connectivity and SSH Authentication ”（连接和 SSH 身份验证）页上、为 HA 对和调解器选择连接方法。



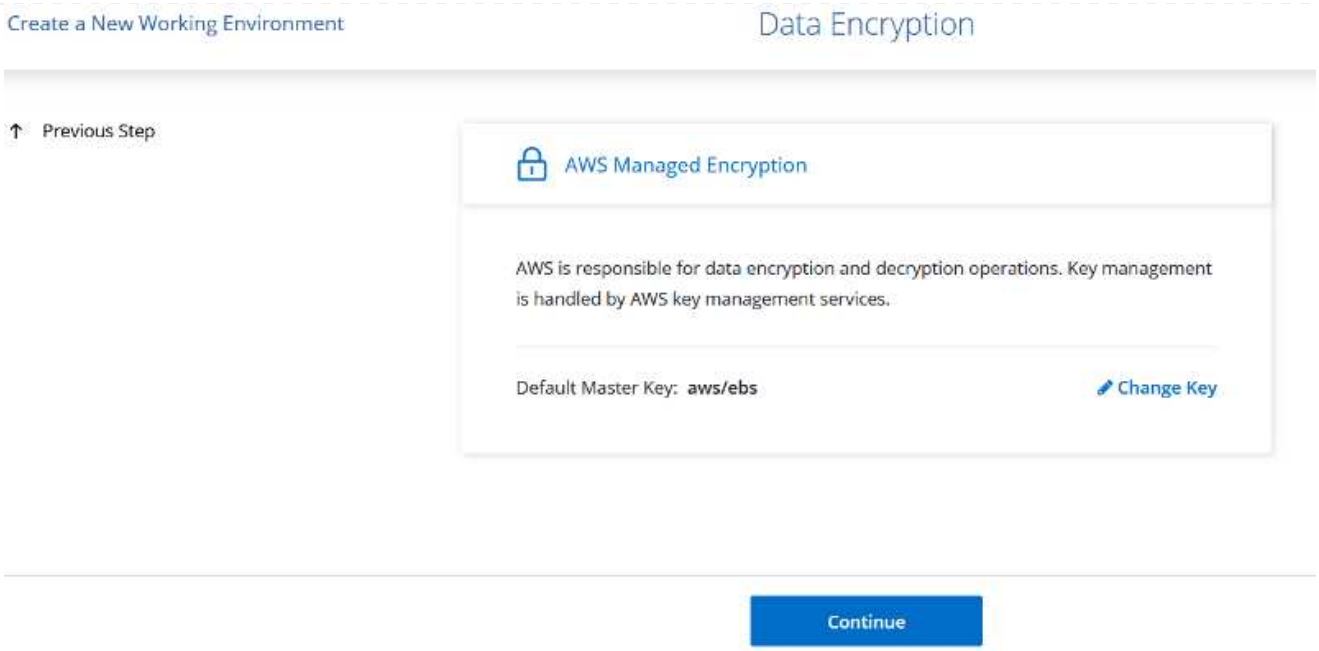
1. 指定浮动 IP 地址，然后单击继续。



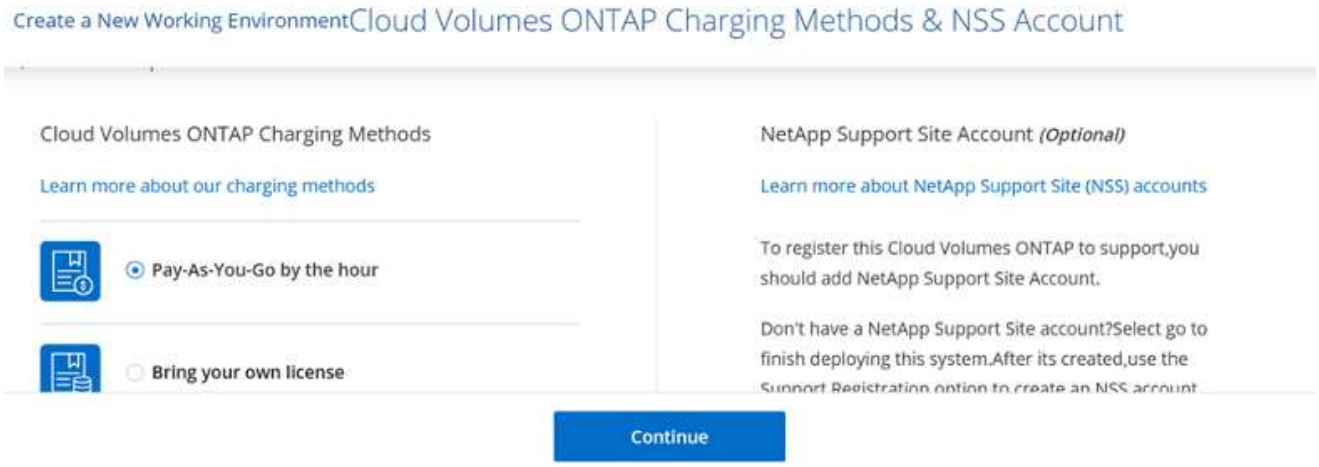
1. 选择适当的路由表以包含指向浮动 IP 地址的路由，然后单击继续。



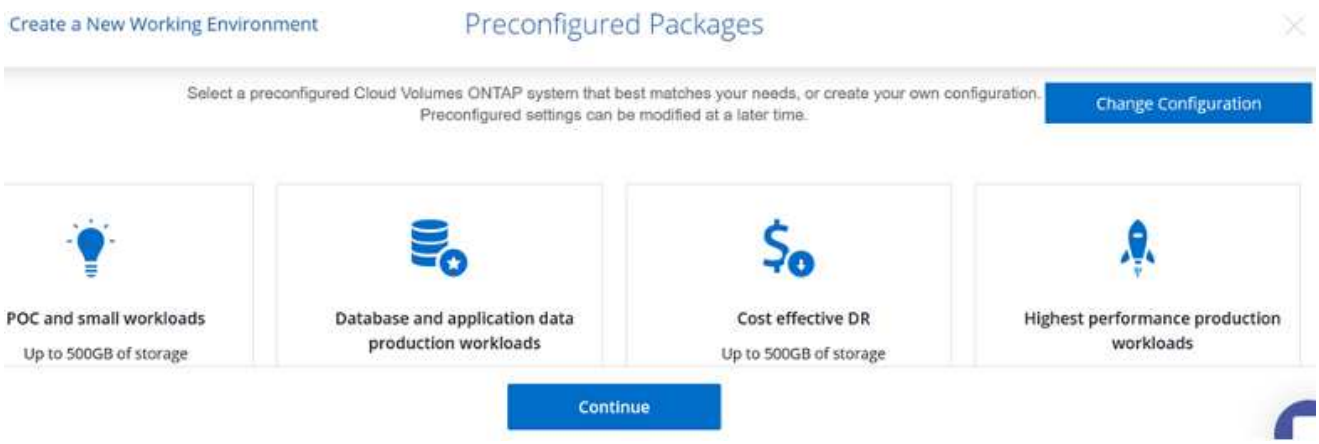
1. 在数据加密页面上，选择 AWS 管理的加密。



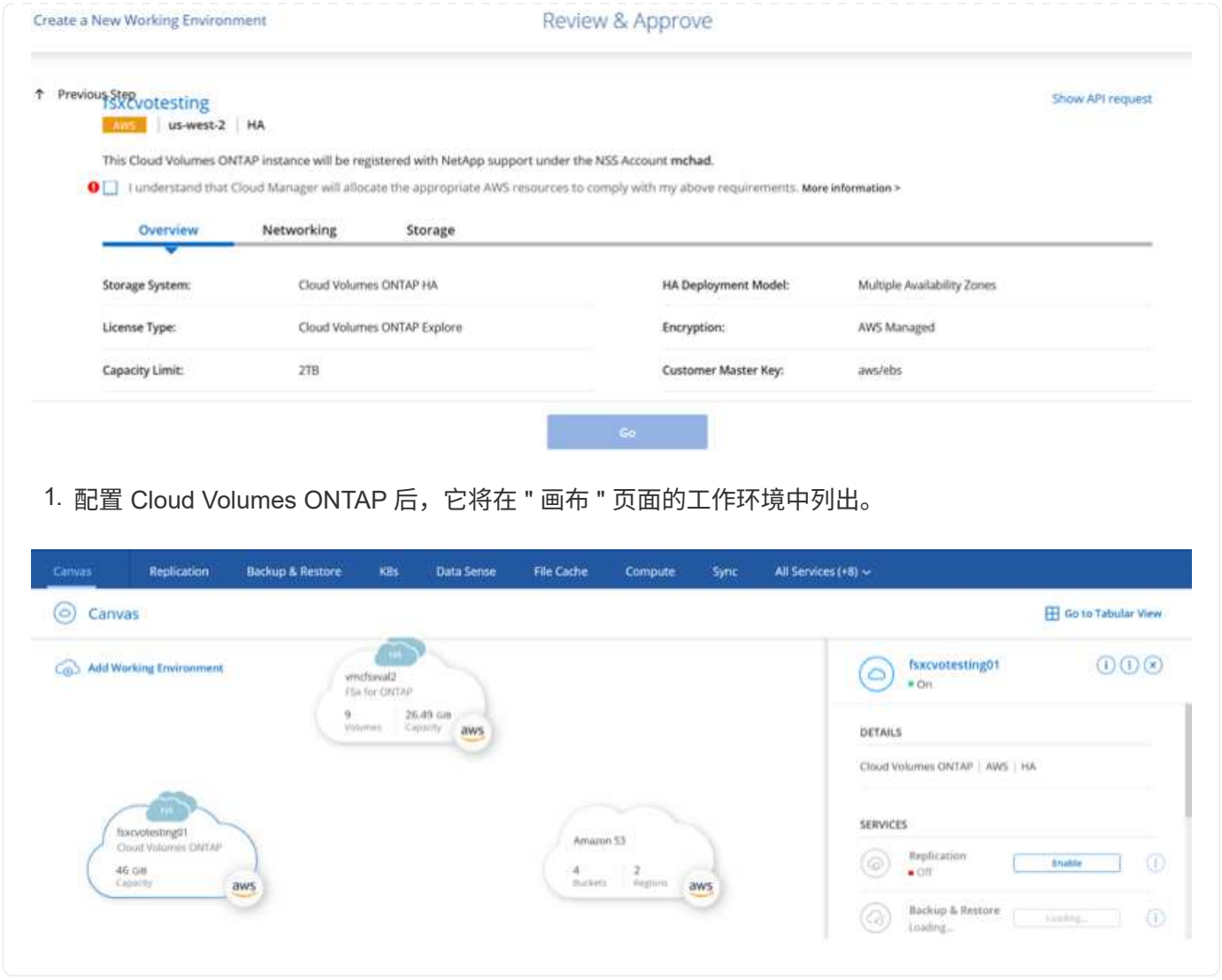
1. 选择许可证选项：按需购买或自带许可证以使用现有许可证。在此示例中，将使用按需购买选项。



1. 根据要在 AWS SDDC 上的 VMware 云上运行的 VM 上部署的工作负载类型，在多个预配置的软件包之间进行选择。



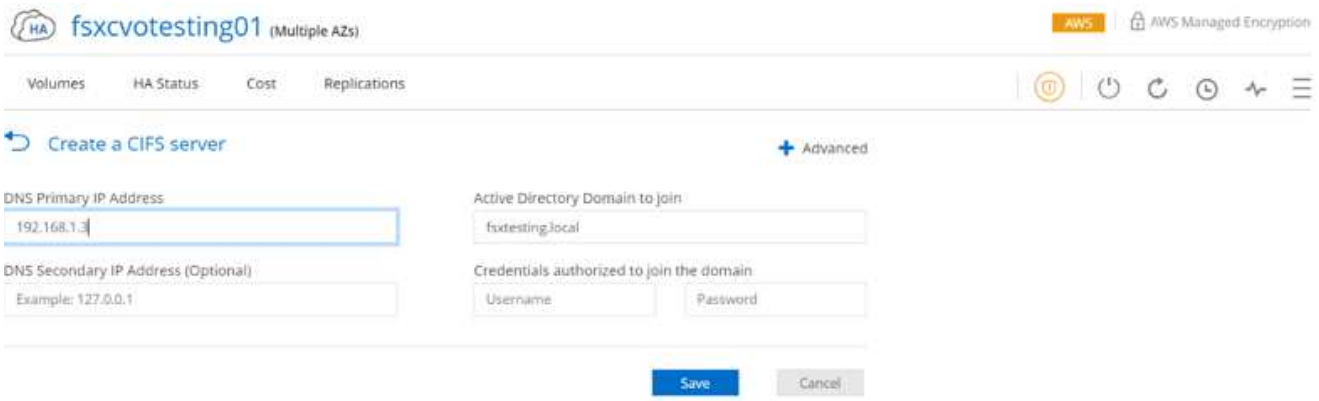
1. 在审核和批准页面上，查看并确认所做的选择。要创建 Cloud Volumes ONTAP 实例，请单击执行。



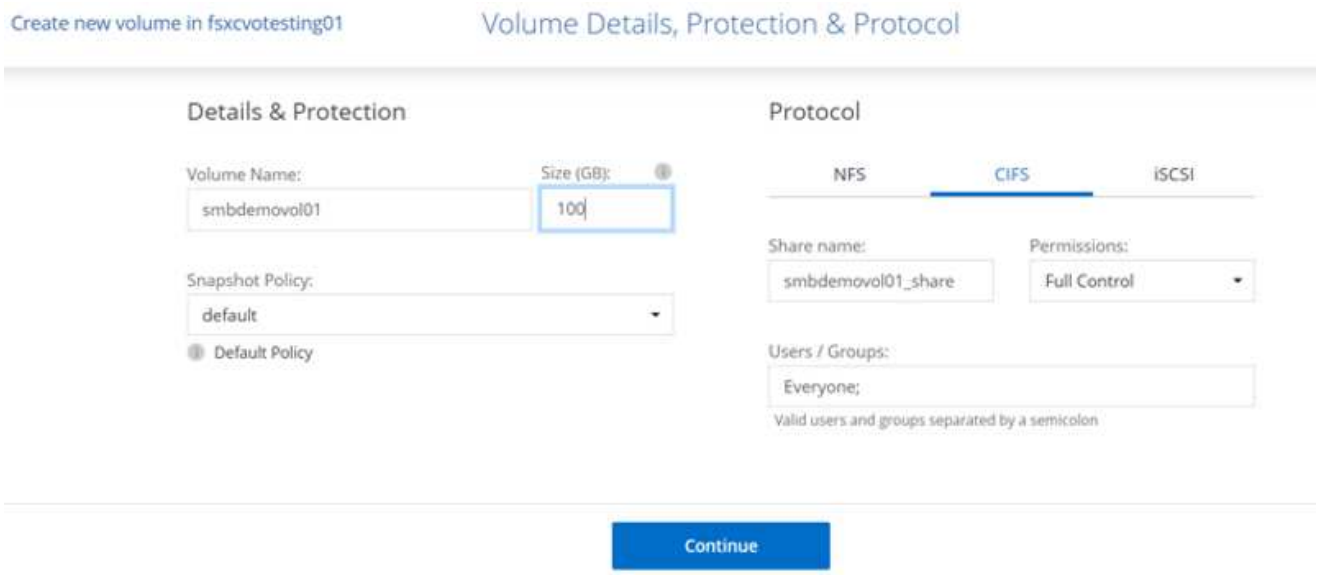
1. 配置 Cloud Volumes ONTAP 后，它将在 " 画布 " 页面的工作环境中列出。

SMB 卷的其他配置

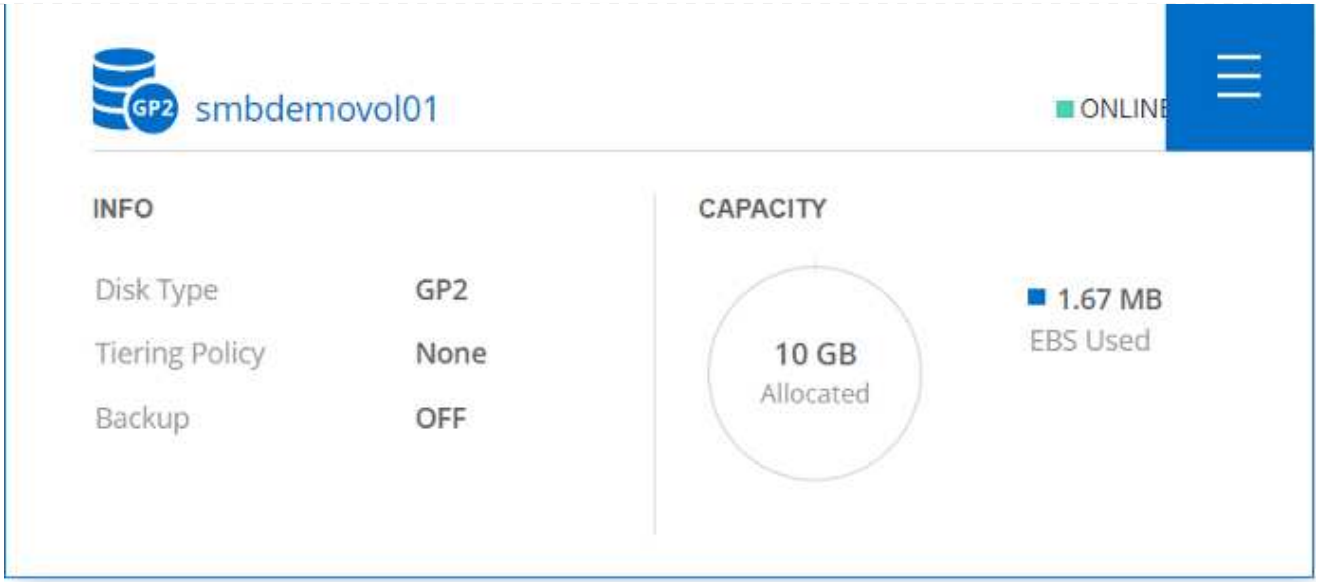
1. 准备好工作环境后，请确保为 CIFS 服务器配置了适当的 DNS 和 Active Directory 配置参数。要创建 SMB 卷，必须执行此步骤。



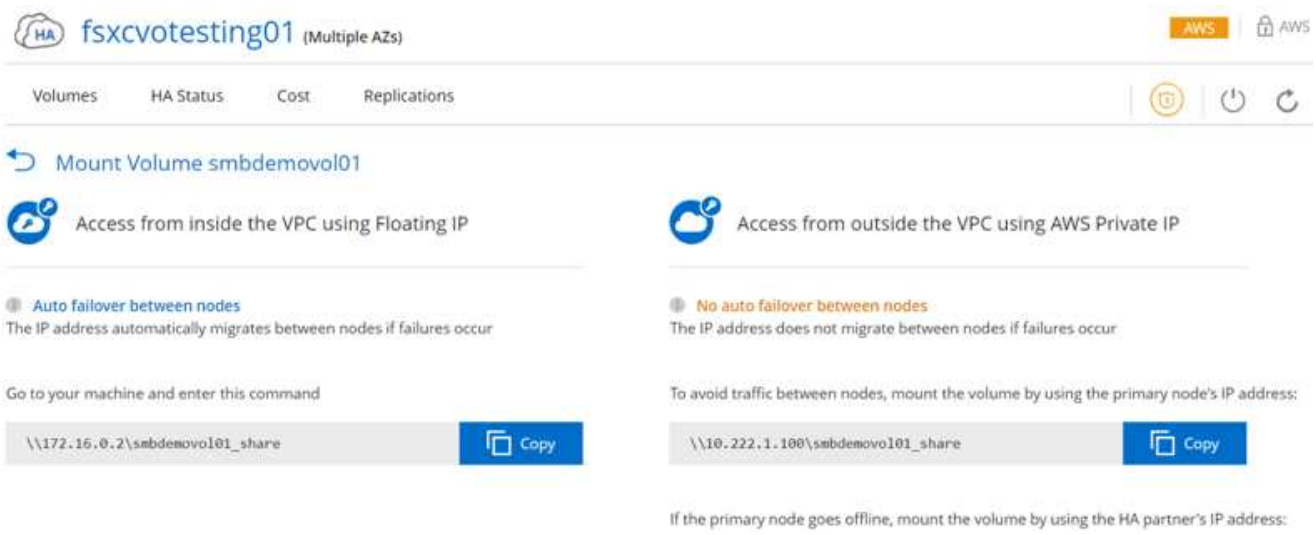
1. 选择要创建卷的 CVO 实例，然后单击创建卷选项。选择适当的大小， Cloud Manager 选择包含的聚合或使用高级分配机制将其放置在特定聚合上。在此演示中，选择 SMB 作为协议。

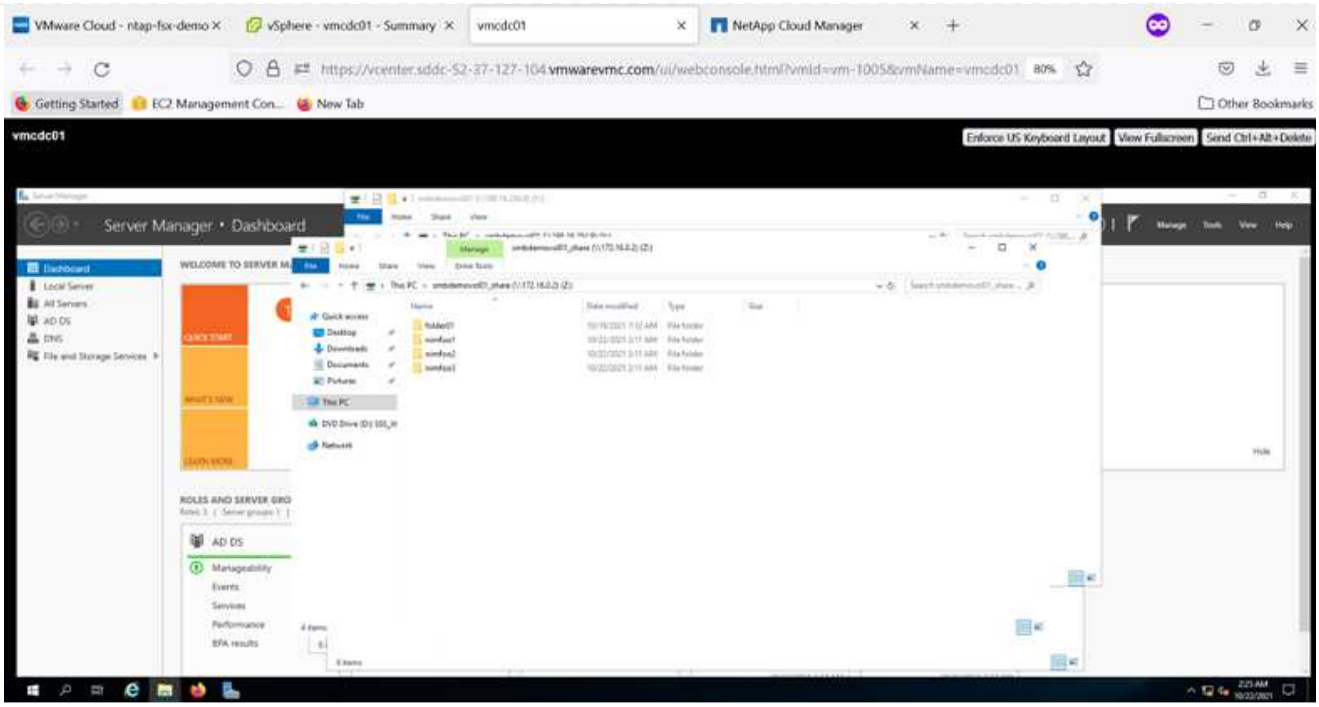


1. 配置卷后，此卷将显示在卷窗格下。由于已配置 CIFS 共享，因此您应向用户或组授予对文件和文件夹的权限，并验证这些用户是否可以访问此共享并创建文件。



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。

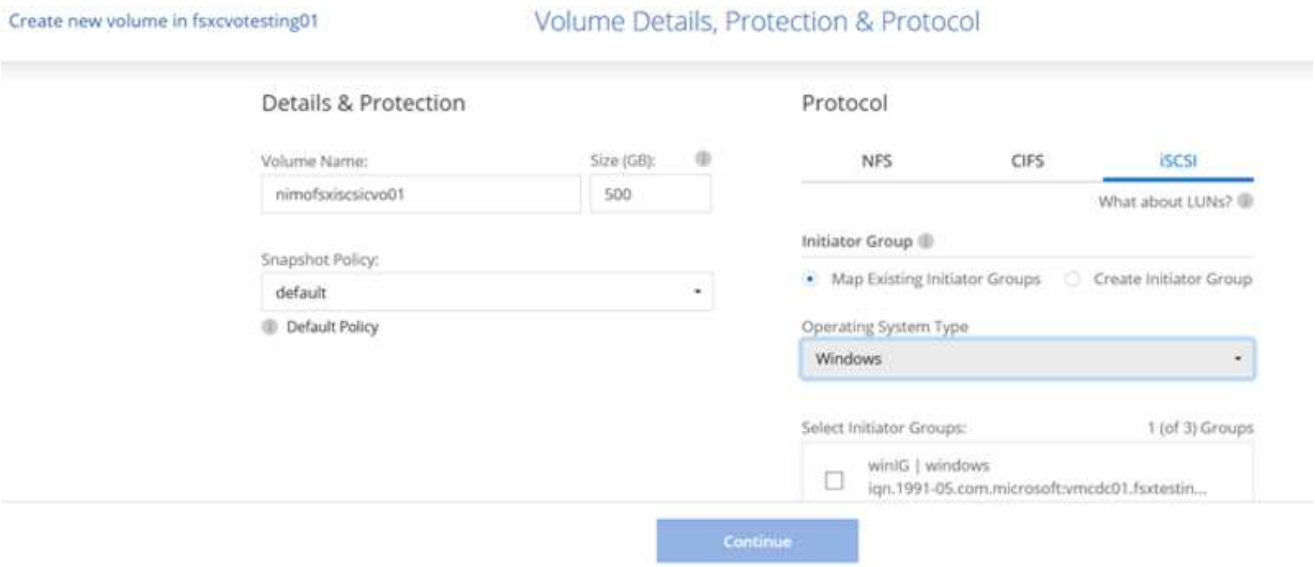


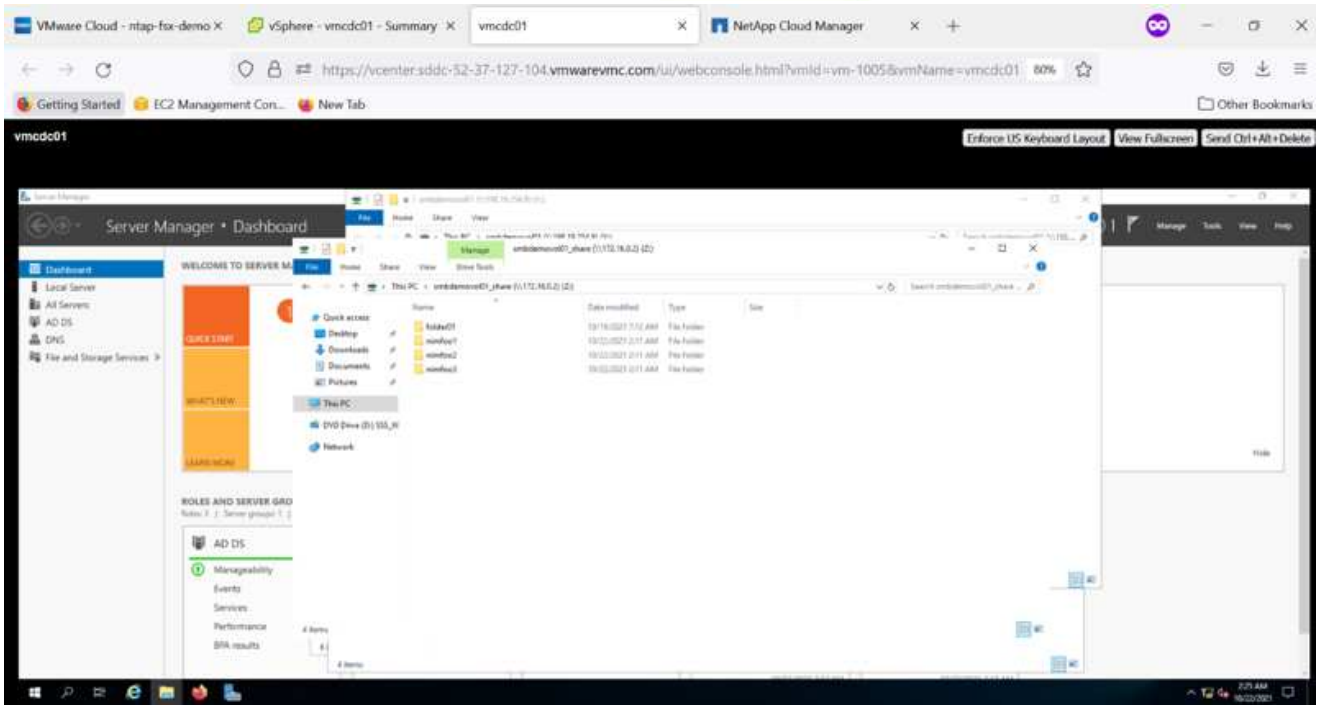

VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Dashboard
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER GROUPS
AD DS
Manageability
Events
Services
Performance
BPA results
This PC
Network
Quick access
Desktop
Downloads
Documents
Pictures
DVD Drive (D:) SSS_X
Manage
Tools
View
Help
Hide

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 的 " 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 > 新建卷，选择 iSCSI ，然后单击创建启动程序组。单击 Continue （继续）。





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

要对位于 AWS SDDC 上的 VMware Cloud 上的主机执行相同操作，请完成以下步骤：

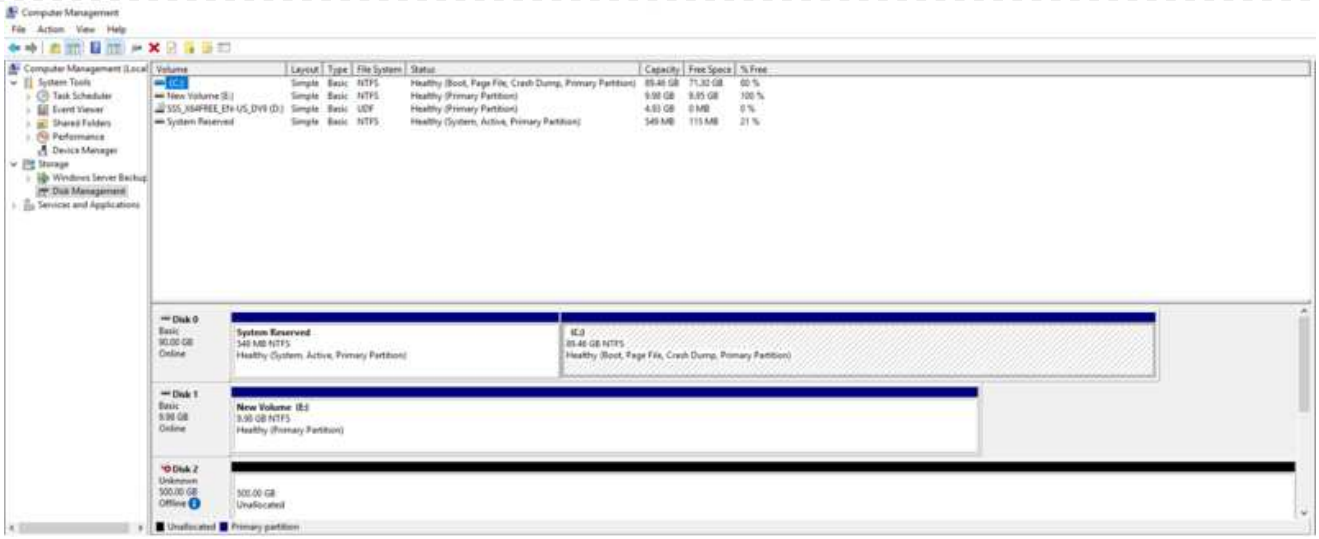
1. RDP 到 AWS 上 VMware 云上托管的 VM 。
2. 打开 iSCSI 启动程序属性对话框：服务器管理器 > 信息板 > 工具 > iSCSI 启动程序。

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，选择已发现的目标，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还原此连接或将此连接添加到收藏目标列表。单击高级。

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

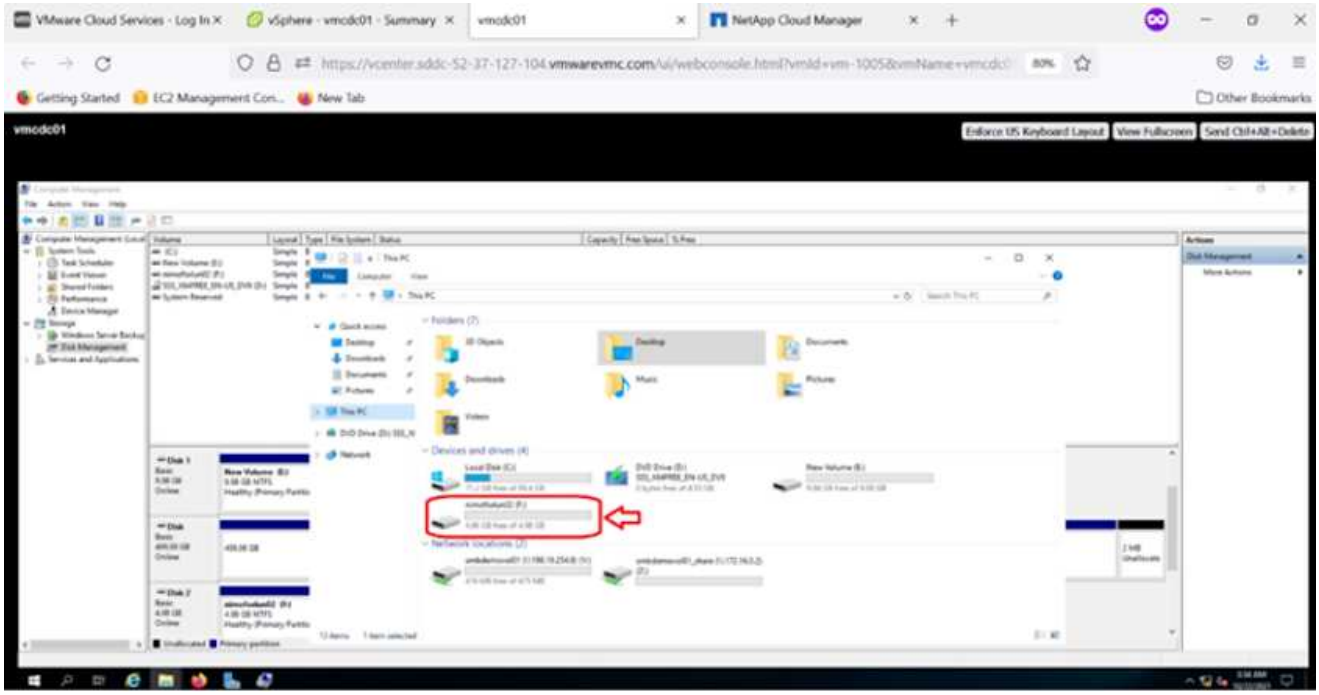
SVM 中的 LUN 在 Windows 主机中显示为磁盘。主机不会自动发现添加的任何新磁盘。通过完成以下步骤触发手动重新扫描以发现磁盘：

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。



当新 LUN 首次由 Windows 主机访问时，它没有分区或文件系统。初始化 LUN ； 也可以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，驱动器 F ： 已挂载。



在 Linux 客户端上，确保 iSCSI 守护进程正在运行。配置 LUN 后，请参阅有关适用于 Linux 分发版的 iSCSI 配置的详细指导。例如，可以找到 Ubuntu iSCSI 配置 "此处"。要进行验证，请从 shell 运行 lsblk cmd 。

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

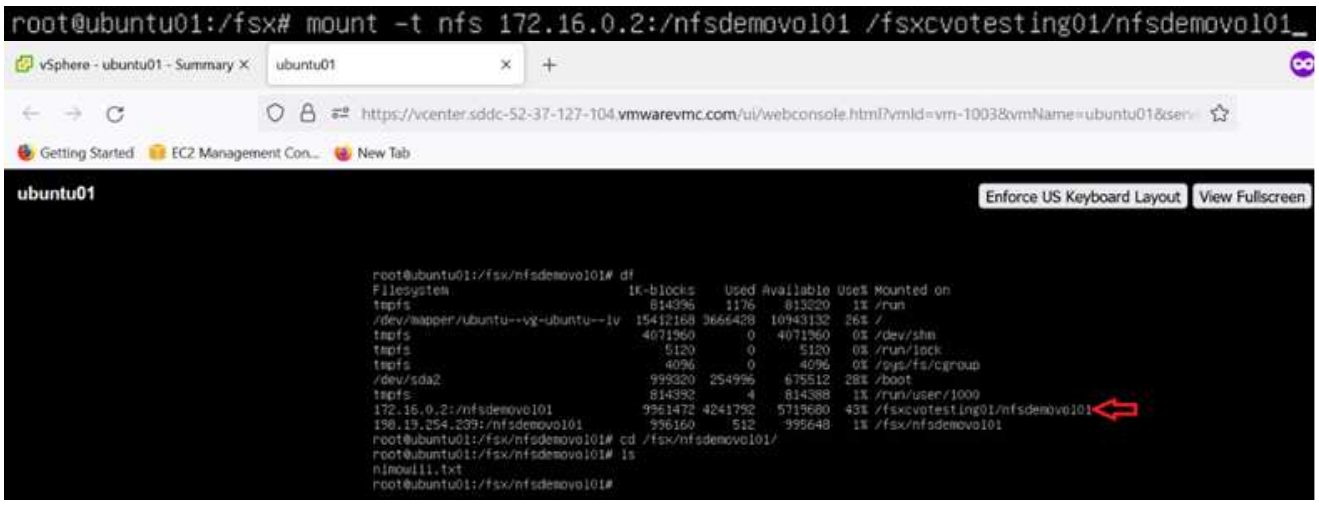
要从 AWS SDDC 上 VMC 内的 VM 挂载 Cloud Volumes ONTAP （ DIY ）文件系统，请完成以下步骤：

1. 连接到指定的 Linux 实例。
2. 使用安全 Shell （ SSH ）在实例上打开一个终端，并使用相应的凭据登录。
3. 使用以下命令为卷的挂载点创建一个目录。

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
```

. 将适用于 NetApp ONTAP NFS 的 Amazon FSX 卷挂载到上一步创建的目录中。

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



ANF数据存储库解决方案概述

每个成功的组织都在转型和现代化的道路上。在此过程中、企业通常会利用现有的VMware投资、同时利用云优势、并探索如何尽可能无缝地迁移、突发、扩展和灾难恢复过程。迁移到云的客户必须评估弹性和突发、数据中心退出、数据中心整合、寿命终结情形、合并、收购等问题。每个组织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、选择一个具有适当性能且最大程度减少障碍的低成本模式是一个关键目标。除了选择合适的平台之外、存储和工作流编排对于充分发挥云部署和弹性的潜能尤其重要。

用例

虽然Azure VMware解决方案 为客户提供了独特的混合功能、但有限的原生 存储选项限制了它对存储负载繁重的组织的有用性。由于存储与主机直接相关、因此扩展存储的唯一方法是添加更多主机、这样对于存储密集型工作负载、成本可能会增加35-40%或更多。这些工作负载需要额外的存储、而不是额外的功率、但这意味着需要为额外的主机付费。

我们来考虑以下情形：客户需要六台主机来提供功率(vCPU/vMem)、但他们也需要大量存储。根据他们的评估、他们需要12台主机来满足存储要求。这样可以提高总体TCO、因为他们必须购买所有这些额外的动力、而他们真正需要的只是更多的存储。这适用于任何使用情形、包括迁移、灾难恢复、突发、开发/测试、 等等。

Azure VMware解决方案 的另一个常见使用情形是灾难恢复(DR)。大多数企业都没有防虚灾难恢复策略、或者可能难以为灾难恢复运行虚影数据中心。管理员可以使用轻型试点集群或按需集群探索零占用空间灾难恢复选项。然后、他们可以在不添加额外主机的情况下扩展存储、这可能是一个极具吸引力的选择。

因此、概括地说、使用情形可以分为两种分类方式：

- 使用ANF数据存储库扩展存储容量
- 在软件定义的数据中心(SDDC)之间、将ANF数据存储库用作从内部或Azure区域进行成本优化的恢复工作流的灾难恢复目标。本指南深入介绍如何使用Azure NetApp Files 为数据存储库提供优化的存储(当前处于公有预览模式) 除了Azure VMware解决方案 中同类最佳的数据保护和灾难恢复功能之外、您还可以通过此功能从vSAN存储中卸载存储容量。

有关如何使用ANF数据存储库的信息、请联系您所在地区的NetApp或Microsoft解决方案 架构师以获取追加信息。

Azure中的**VMware Cloud**选项

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公有 云中提供功能完备的VMware SDDC。AVS是由Microsoft全面管理和支持并经过VMware验证的第一方解决方案 、它使用Azure基础架构。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以及用于网络连接和安全的NSX、同时充分利用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邻近性。Azure VMware解决方案 SDDC与Azure NetApp Files 相结合、可提供最佳性能、同时将网络延迟降至最低。

无论使用何种云、在部署VMware SDDC时、初始集群都包括以下组件：

- 用于计算虚拟化的VMware ESXi主机、以及用于管理的vCenter Server设备。
- VMware vSAN超融合存储、整合了每个ESXi主机的物理存储资产。
- VMware NSX用于虚拟网络连接和安全性、并使用NSX Manager集群进行管理。

结论

无论您是以全云还是混合云为目标、Azure NetApp Files 都可以提供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、同时通过将数据需求无缝地迁移到应用程序层来降低TCO。无论使用何种情形、都可以选择Azure VMware解决方案 和Azure NetApp Files 、以快速实现云优势、跨内部和多个云实现一致的基础架构和运营、并实现工作负载双向可移植性以及企业级容量和性能。这是用于连接存储的熟悉过程。请记住、随新名称一起更改的只是数据的位置；工具和流程都保持不变、Azure NetApp Files 有助于优化整体部署。

要点总结

本文档的要点包括：

- 现在、您可以在AVS SDDC上使用Azure NetApp Files 作为数据存储库。
- 加快应用程序响应速度并提高可用性、以便在需要时随时随地访问工作负载数据。

- 通过简单的即时调整大小功能简化vSAN存储的整体复杂性。
- 利用动态重塑功能为任务关键型工作负载提供有保障的性能。
- 如果Azure VMware解决方案 Cloud是目标、则Azure NetApp Files 是最适合优化部署的存储解决方案。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请访问以下网站链接：

- 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 数据存储库连接到Azure VMware解决方案 主机(预览)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

适用于 **Azure** 的 **NetApp** 子系统连接存储选项

Azure支持使用 原生 Azure NetApp Files (ANF)服务或Cloud Volumes ONTAP (CVO)的子系统连接NetApp存储。

Azure NetApp 文件 **(ANF)**

Azure NetApp Files 为Azure提供了企业级数据管理和存储、让您可以轻松管理工作负载和应用程序。将工作负载迁移到云并在不影响性能的情况下运行这些工作负载。

Azure NetApp Files 消除了各种障碍、因此您可以将所有基于文件的应用程序迁移到云。这是您第一次不必重新构建应用程序、而是为应用程序提供了不复杂的持久存储。

由于此服务是通过Microsoft Azure门户提供的、因此用户将在其Microsoft企业协议中体验到完全托管的服务。由Microsoft管理的一流支持让您高枕无忧。通过这一个解决方案 、您可以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、即使对于传统环境也是如此。

Azure NetApp Files （ **ANF** ）作为子系统连接的存储

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

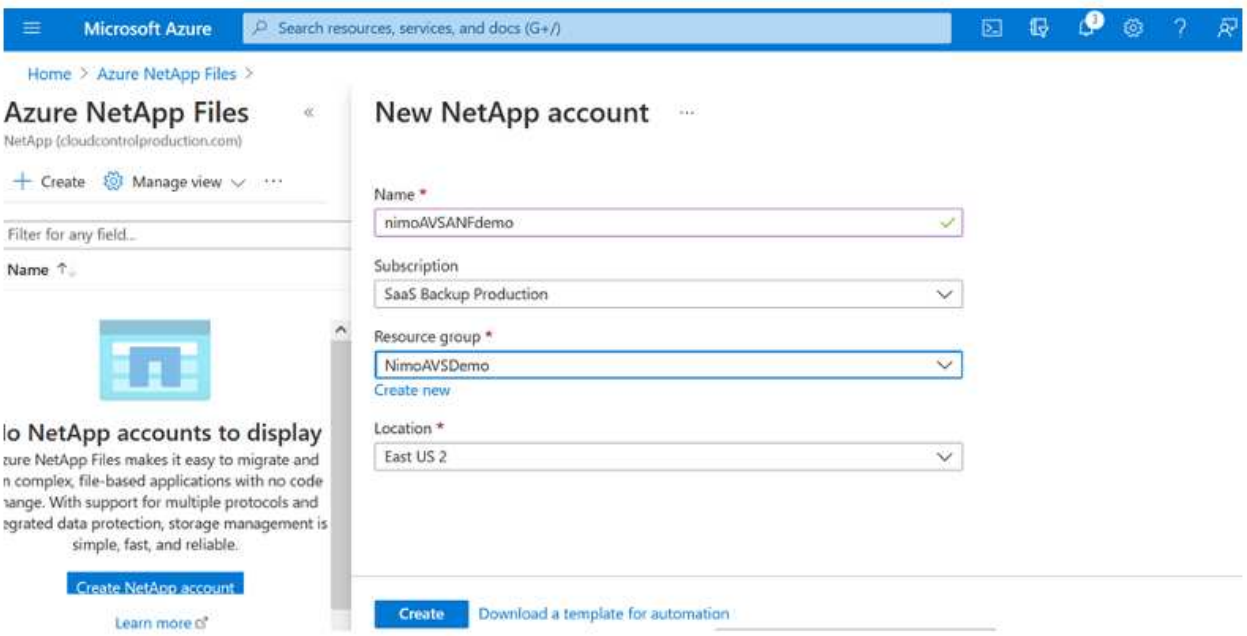
可以从 Azure VMware 解决方案 SDDC 环境中创建的虚拟机挂载 Azure NetApp Files 共享。由于 Azure NetApp Files 支持 SMB 和 NFS 协议，因此这些卷也可以挂载到 Linux 客户端并映射到 Windows 客户端。只需五个简单步骤即可设置 Azure NetApp Files 卷。

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

要创建和挂载 Azure NetApp Files 卷，请完成以下步骤：

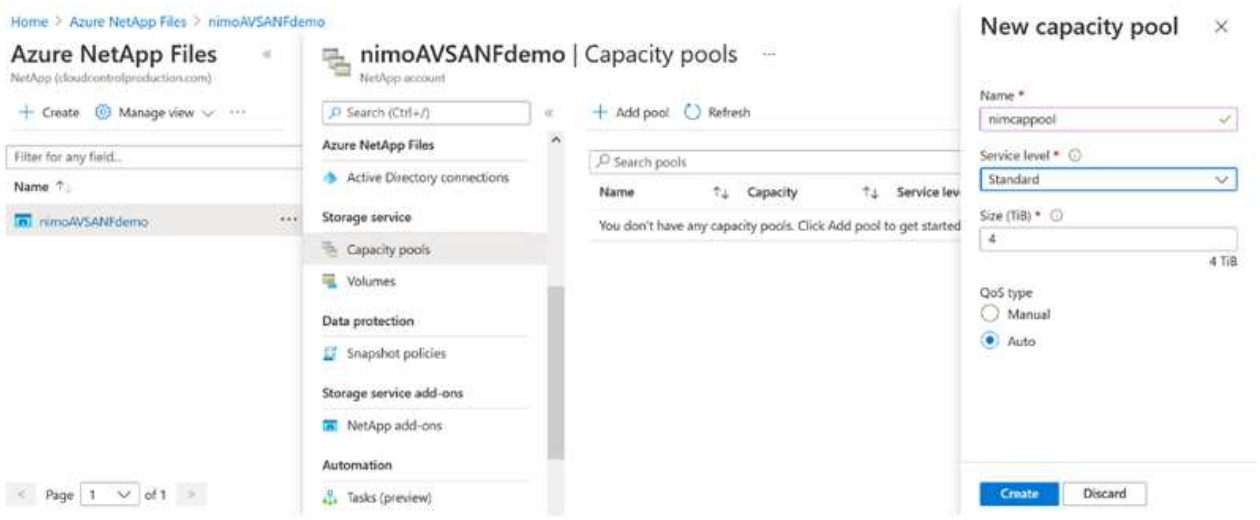
1. 登录到 Azure 门户并访问 Azure NetApp Files 。使用 _az provider register -namespace Microsoft.NetApp – wait 命令验证对 Azure NetApp Files 服务的访问并注册 Azure NetApp Files 资源提供程序。注册完成后，创建一个 NetApp 帐户。

   有关详细步骤，请参见 "Azure NetApp Files 共享"。此页面将引导您逐步完成此过程。

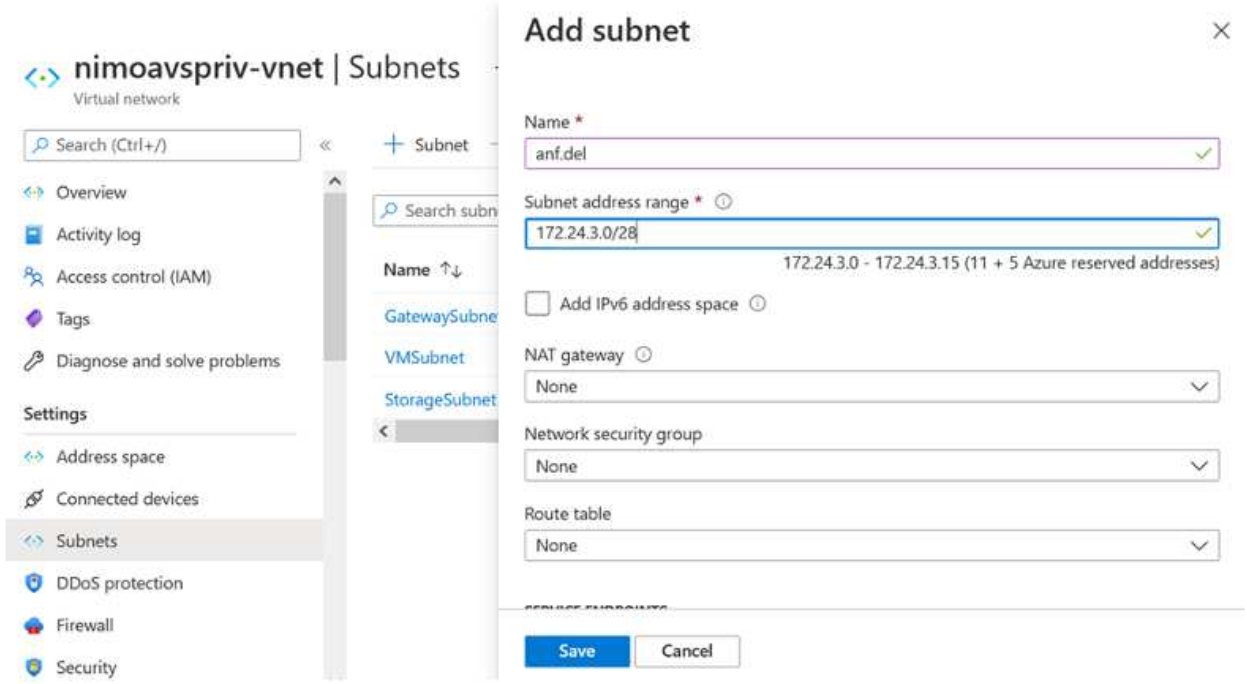


2. 创建 NetApp 帐户后，使用所需的服务级别和大小设置容量池。

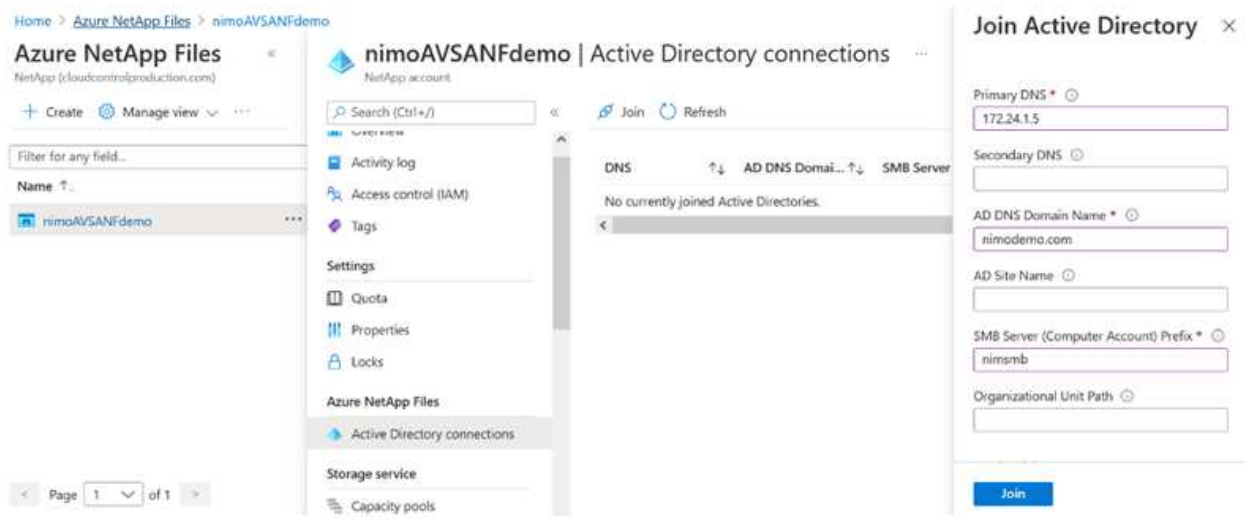
   有关详细信息，请参见 "设置容量池"。



3. 为 Azure NetApp Files 配置委派子网，并在创建卷时指定此子网。有关创建委派子网的详细步骤，请参见 "Delegate a subnet to Azure NetApp Files"。

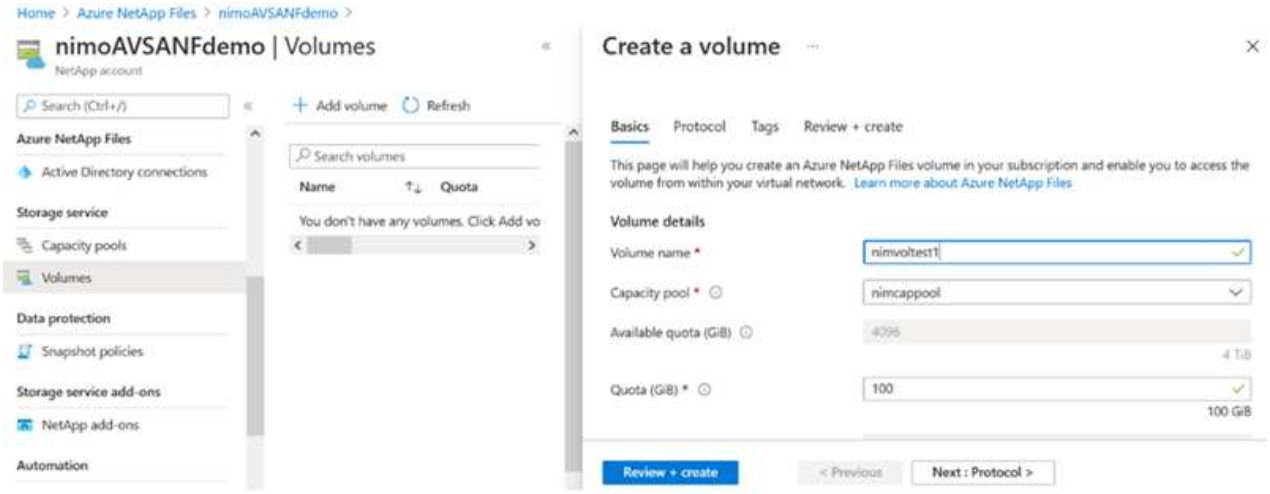


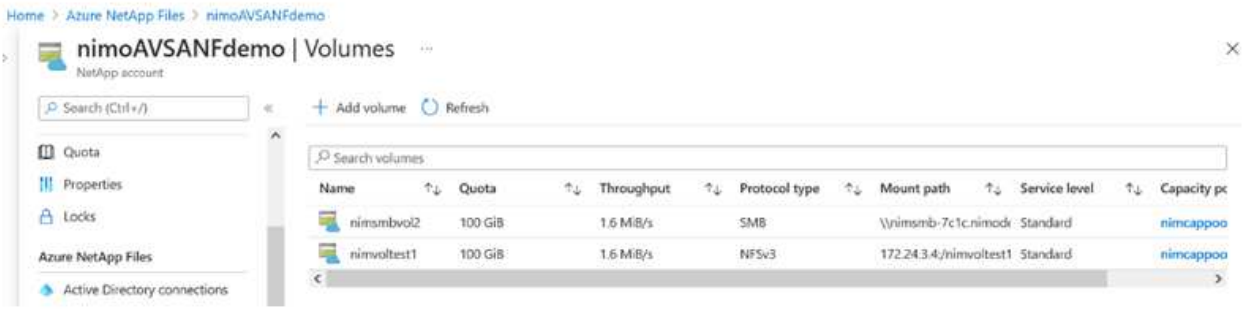
4. 使用容量池刀片下的卷刀片添加 SMB 卷。确保在创建 SMB 卷之前已配置 Active Directory 连接器。



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。

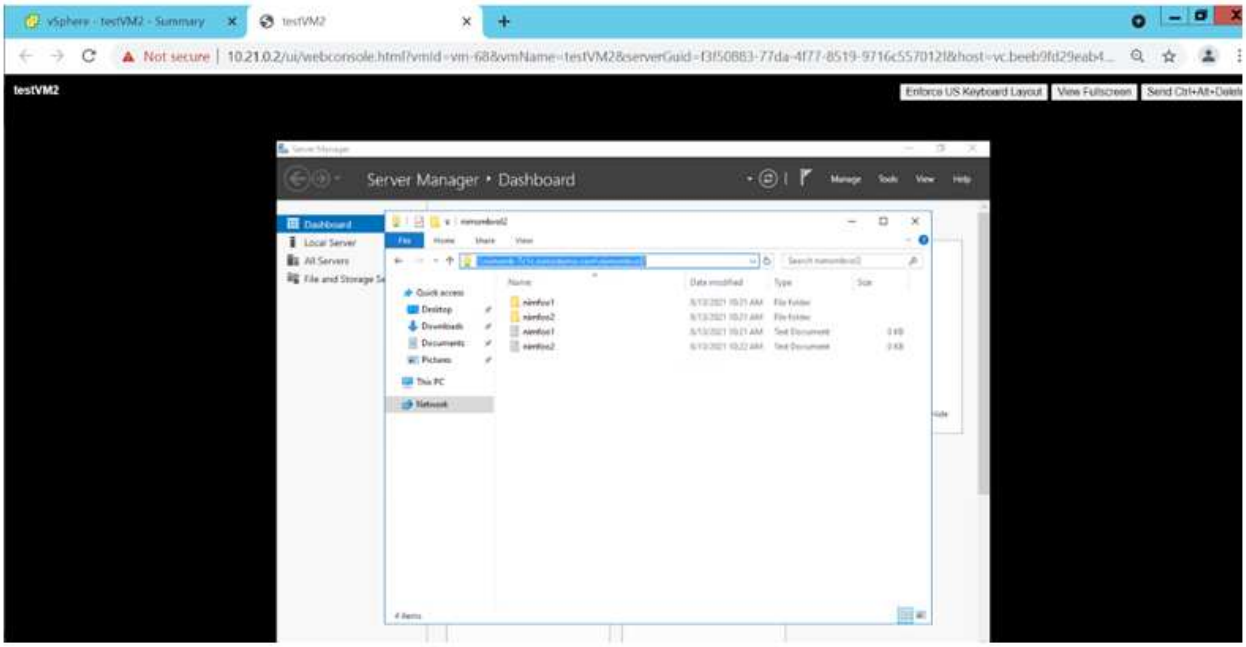


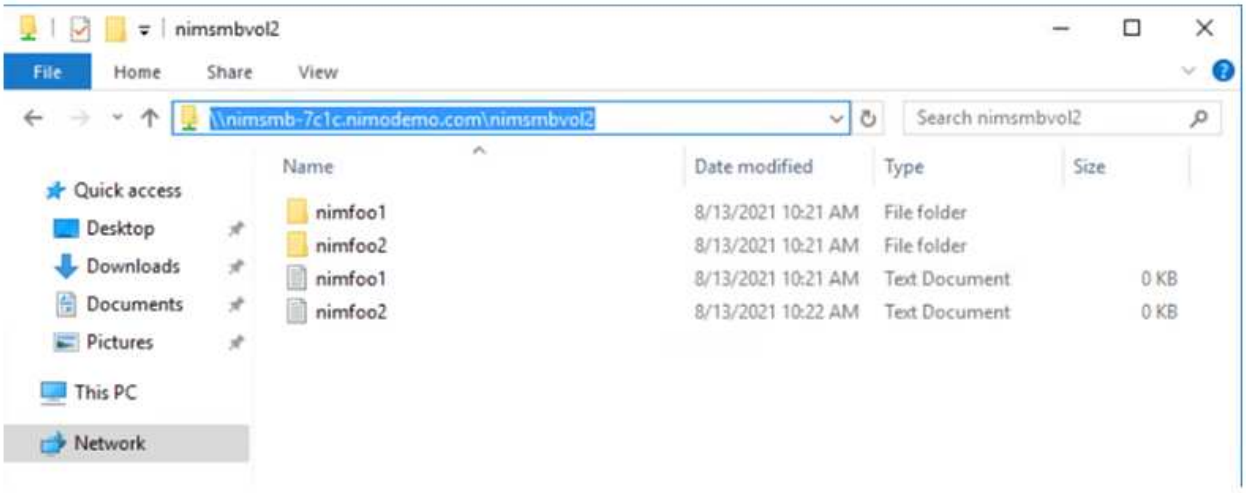


要了解有关按大小或配额显示的 Azure NetApp Files 卷性能的详细信息，请参见 "Azure NetApp Files 的性能注意事项"。

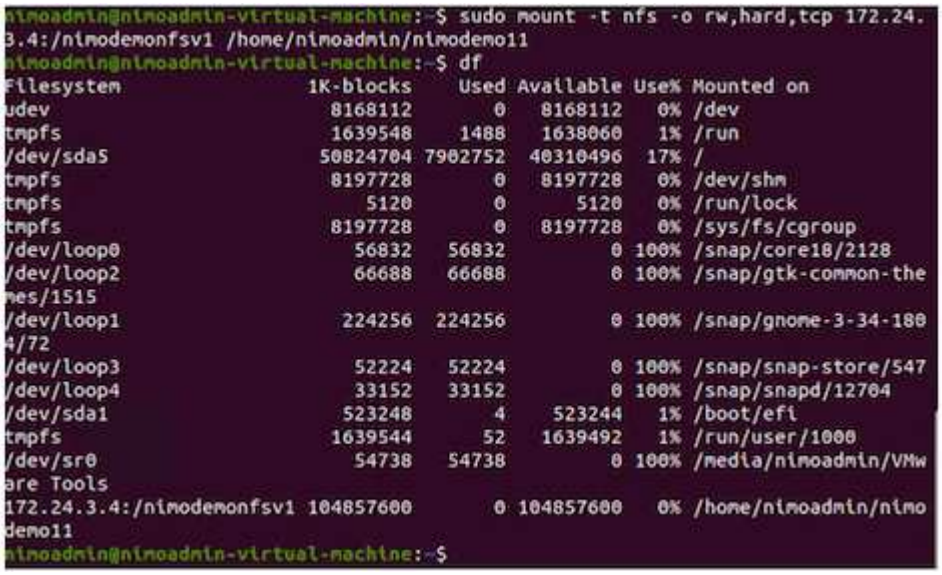
6. 建立连接后，可以挂载此卷并将其用于应用程序数据。

要完成此操作，请从 Azure 门户中单击卷刀片，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挂载到 Azure VMware 解决方案 SDDC 上运行的虚拟机上。





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



有关详细信息，请参见 "动态更改卷的服务级别"。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP 是行业领先的云数据管理解决方案 、基于NetApp的ONTAP 存储软件构建、可在Amazon Web Services (AWS)、Microsoft Azure和Google Cloud Platform (GCP)上本机获得。

它是ONTAP 的软件定义版本、使用云原生存储、可以在云端和内部环境中使用相同的存储软件、从而减少了对IT员工进行全新数据管理方法培训的需求。

借助CVO、客户可以无缝地将数据从边缘、数据中心、云和云端来回移动、从而将混合云整合在一起—所有这些都通过一个单一窗格管理控制台NetApp Cloud Manager进行管理。

按照设计、CVO可提供极致性能和高级数据管理功能、甚至可以满足云中要求最苛刻的应用程序的需求

Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储

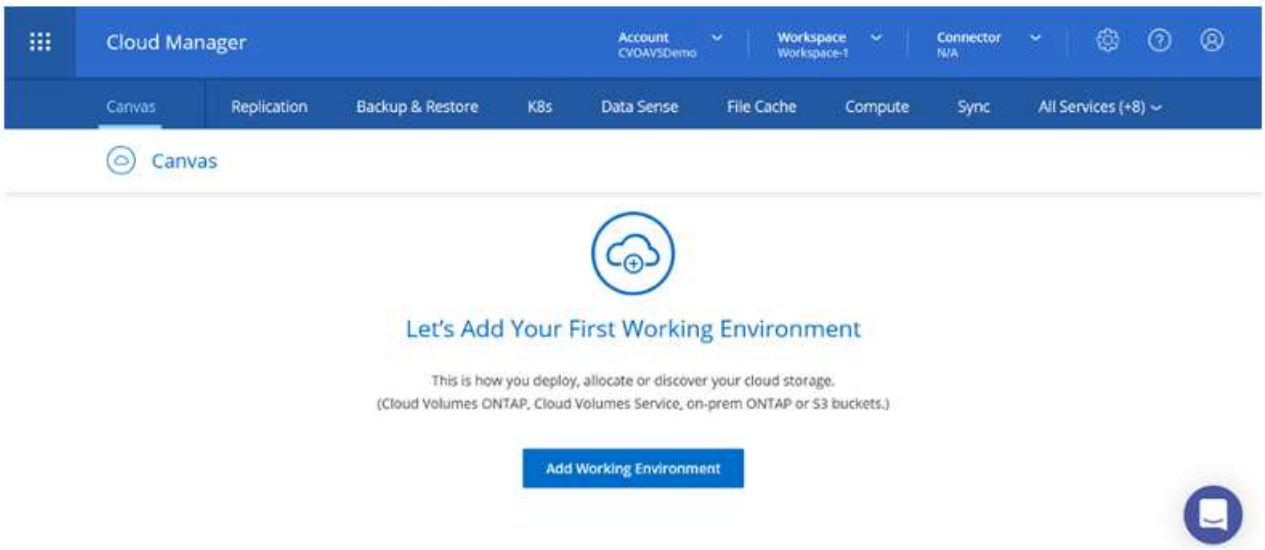
在 Azure 中部署新 Cloud Volumes ONTAP

可以从 Azure VMware 解决方案 SDDC 环境中创建的 VM 挂载 Cloud Volumes ONTAP 共享和 LUN 。这些卷也可以挂载到 Linux 客户端和 Windows 客户端上，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。

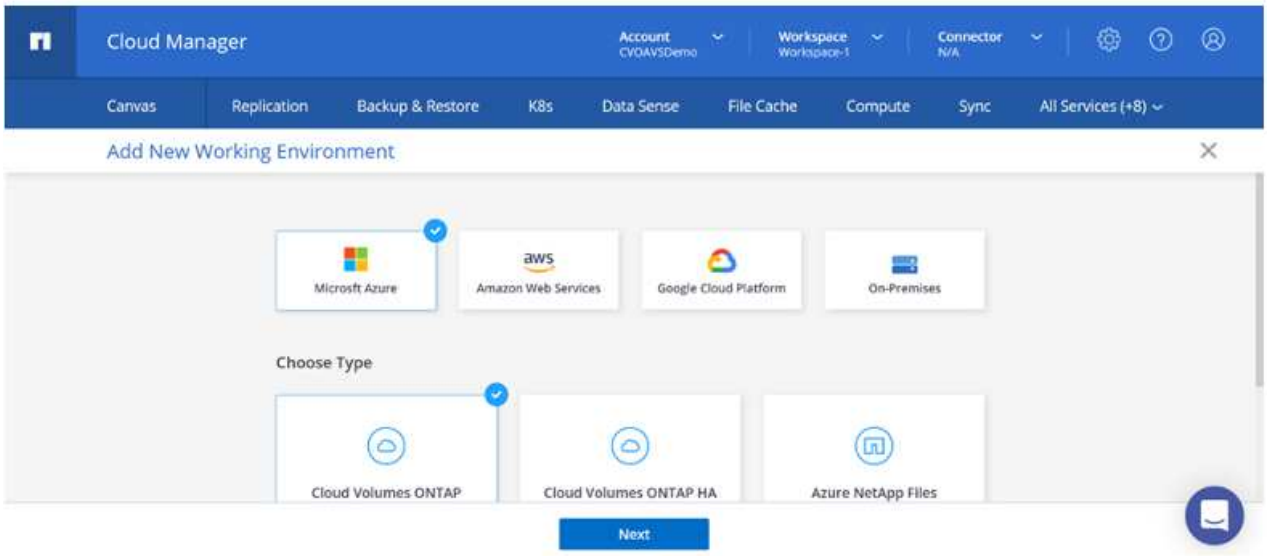
要将卷从内部环境复制到云以实现灾难恢复或迁移，请使用站点到站点 VPN 或 ExpressRoute 与 Azure 建立网络连接。将数据从内部复制到 Cloud Volumes ONTAP 不在本文档的讨论范围之内。要在内部系统和 Cloud Volumes ONTAP 系统之间复制数据，请参见 "在系统之间设置数据复制"。

使用 … "Cloud Volumes ONTAP 规模估算工具" 以准确估算 Cloud Volumes ONTAP 实例的大小。此外，还可以监控内部性能，以用作 Cloud Volumes ONTAP 规模估算器中的输入。

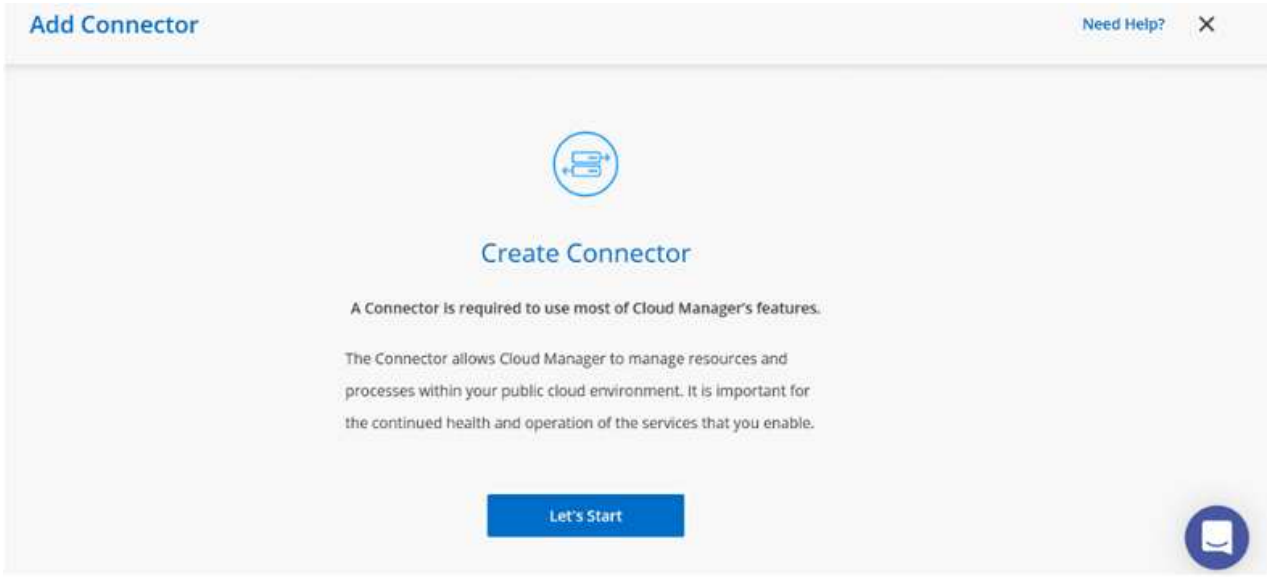
1. 登录到 NetApp Cloud Central —此时将显示 Fabric View 屏幕。找到 Cloud Volumes ONTAP 选项卡，然后选择转到 Cloud Manager 。登录后，将显示 " 画布 " 屏幕。



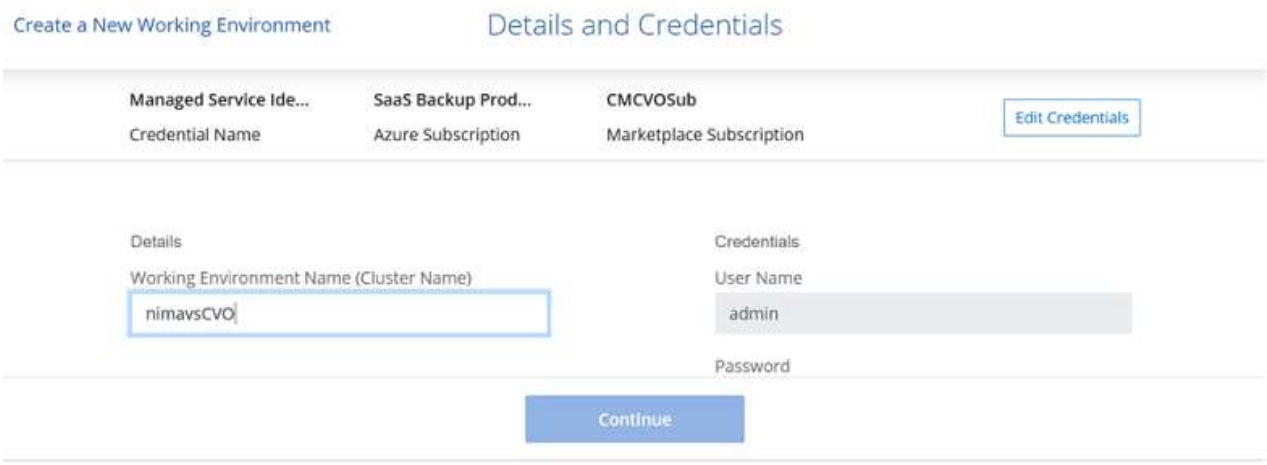
2. 在 Cloud Manager 主页上，单击添加工作环境，然后选择 Microsoft Azure 作为云以及系统配置的类型。



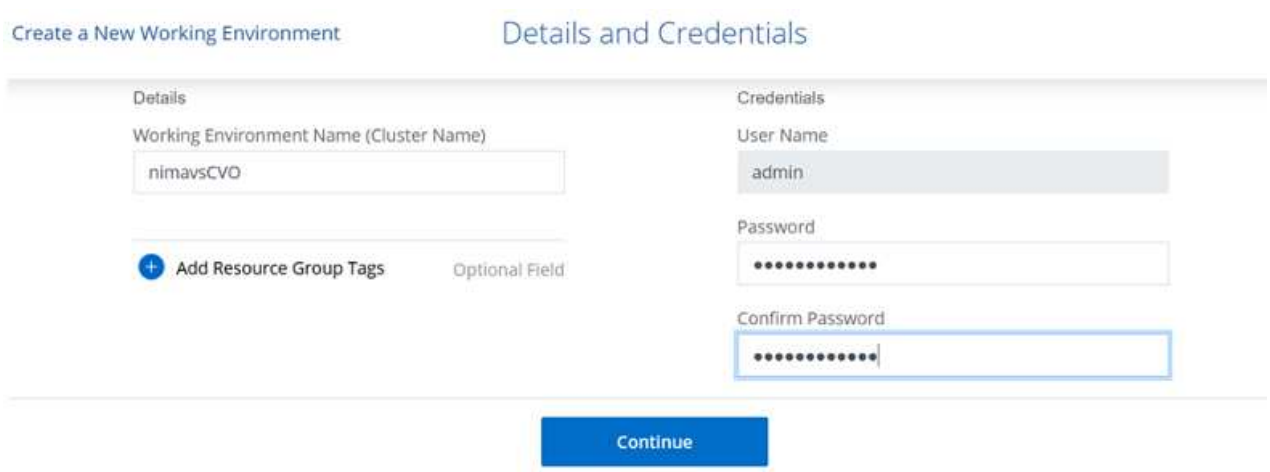
3. 在创建第一个 Cloud Volumes ONTAP 工作环境时， Cloud Manager 会提示您部署连接器。



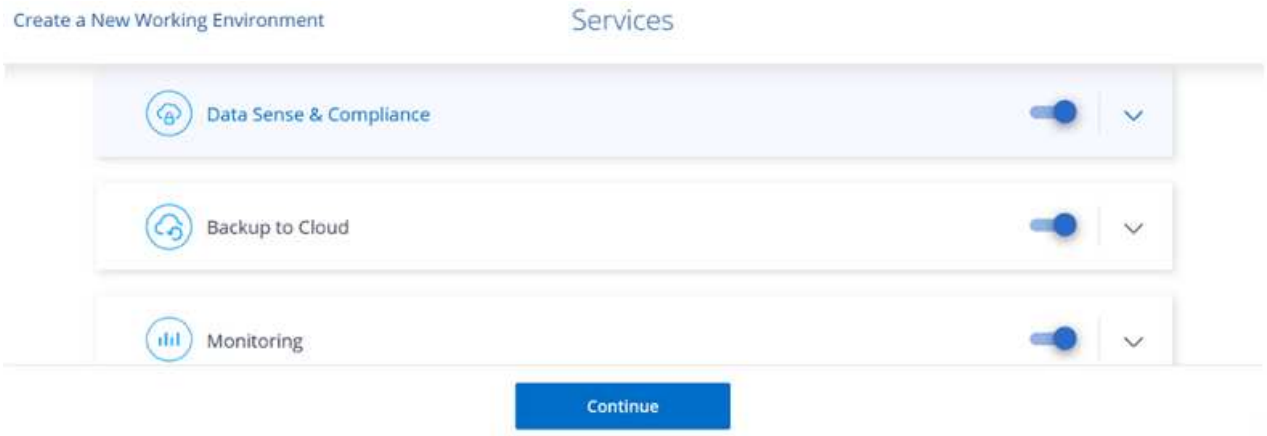
4. 创建连接器后，更新详细信息和凭据字段。



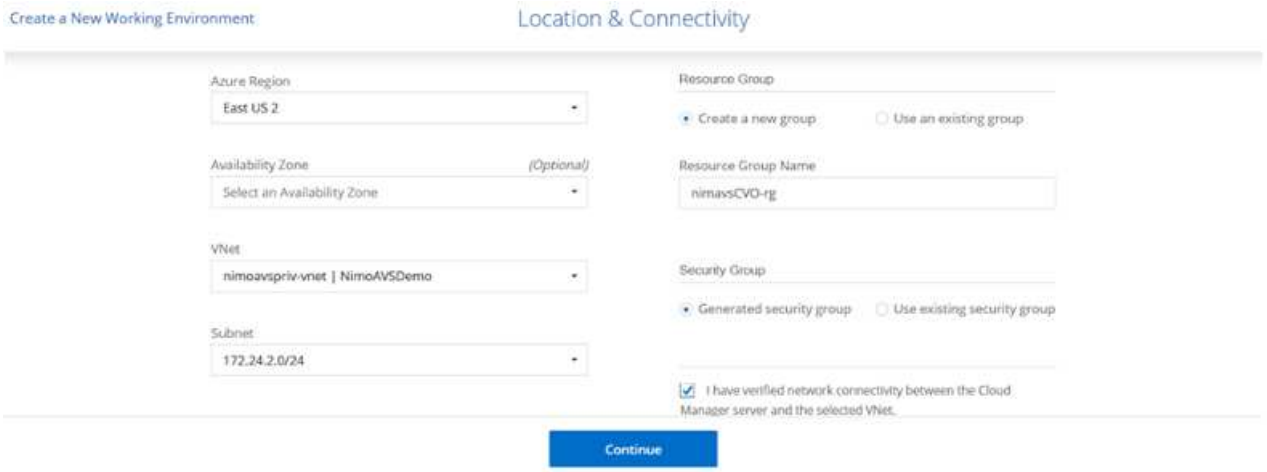
5. 提供要创建的环境的详细信息，包括环境名称和管理员凭据。为 Azure 环境添加资源组标记作为可选参数。完成后，单击 Continue 。



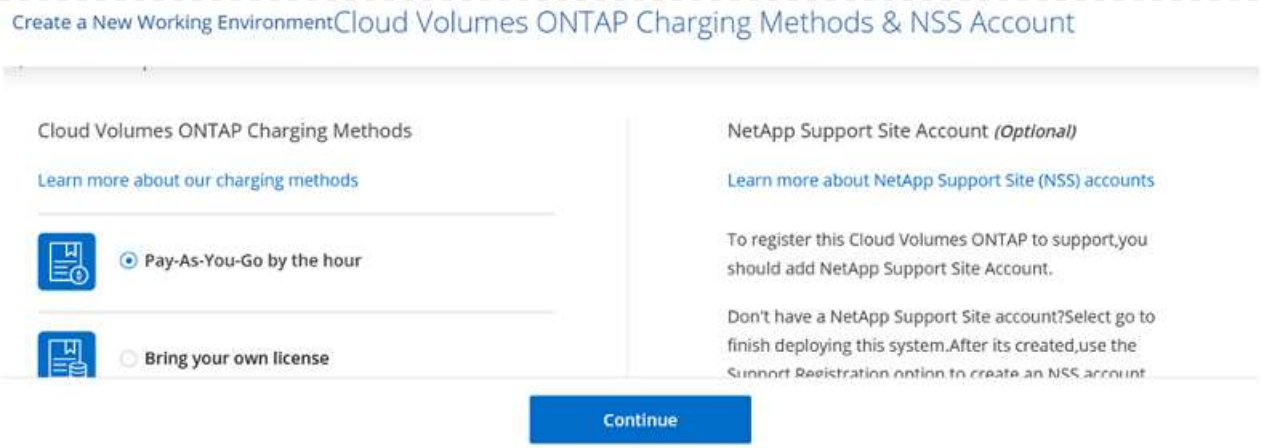
6. 为Cloud Volumes ONTAP部署选择附加服务、包括BlueXP分类、BlueXP备份和恢复以及Cloud Insights。选择服务，然后单击继续。



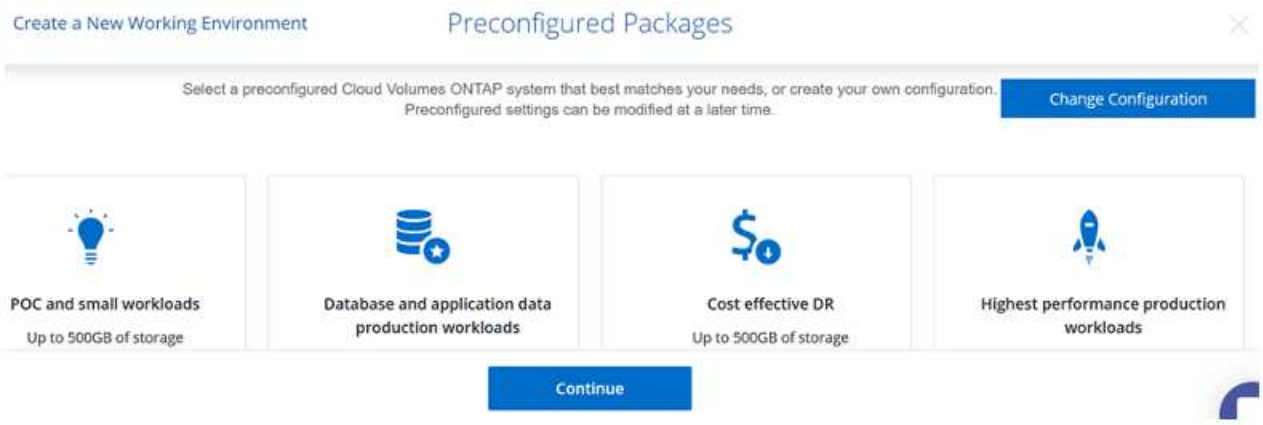
7. 配置 Azure 位置和连接。选择要使用的 Azure 区域，资源组， vNet 和子网。



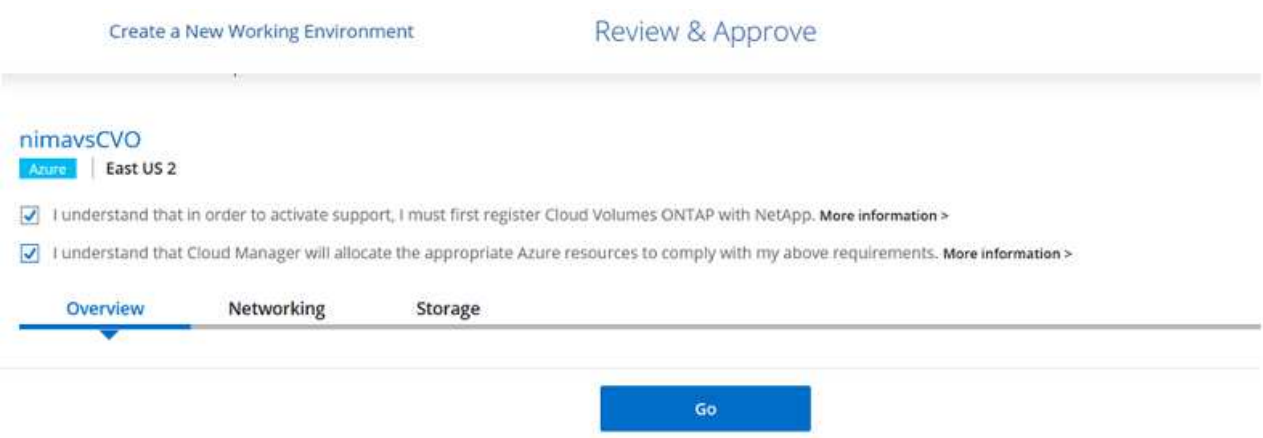
8. 选择许可证选项：按需购买或自带许可证以使用现有许可证。在此示例中，使用按需购买选项。



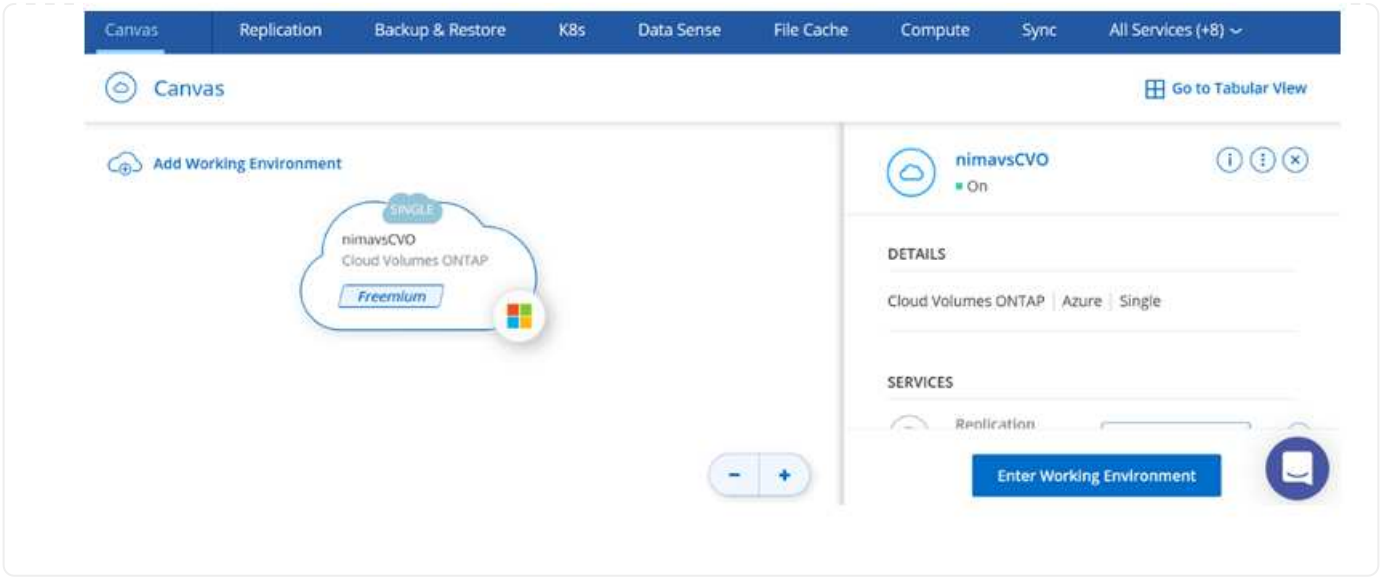
9. 在可用于各种工作负载类型的多个预配置软件包之间进行选择。



10. 接受有关激活 Azure 资源支持和分配的两个协议。要创建 Cloud Volumes ONTAP 实例，请单击 " 转到 " 。

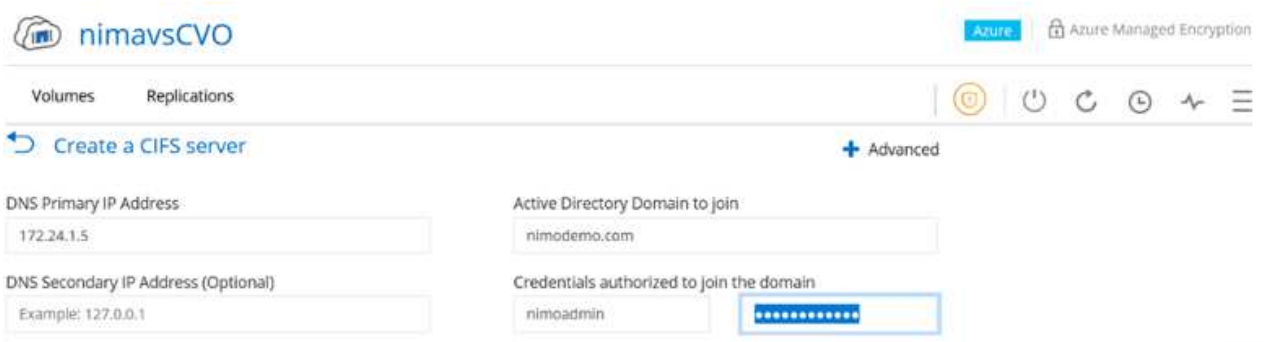


11. 配置 Cloud Volumes ONTAP 后，它将在 " 画布 " 页面的工作环境中列出。

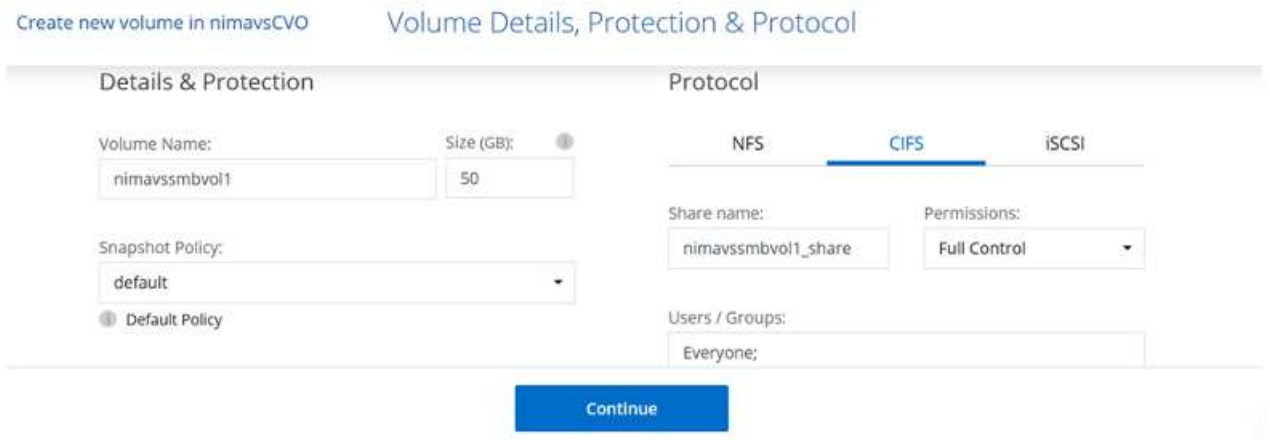

Canvas
Replication
Backup & Restore
K8s
Data Sense
File Cache
Compute
Sync
All Services (+8)
Canvas
Go to Tabular View
Add Working Environment
SINGLE
nimavsCVO
Cloud Volumes ONTAP
Freemium
nimavsCVO
On
DETAILS
Cloud Volumes ONTAP | Azure | Single
SERVICES
Replication
Enter Working Environment

SMB 卷的其他配置

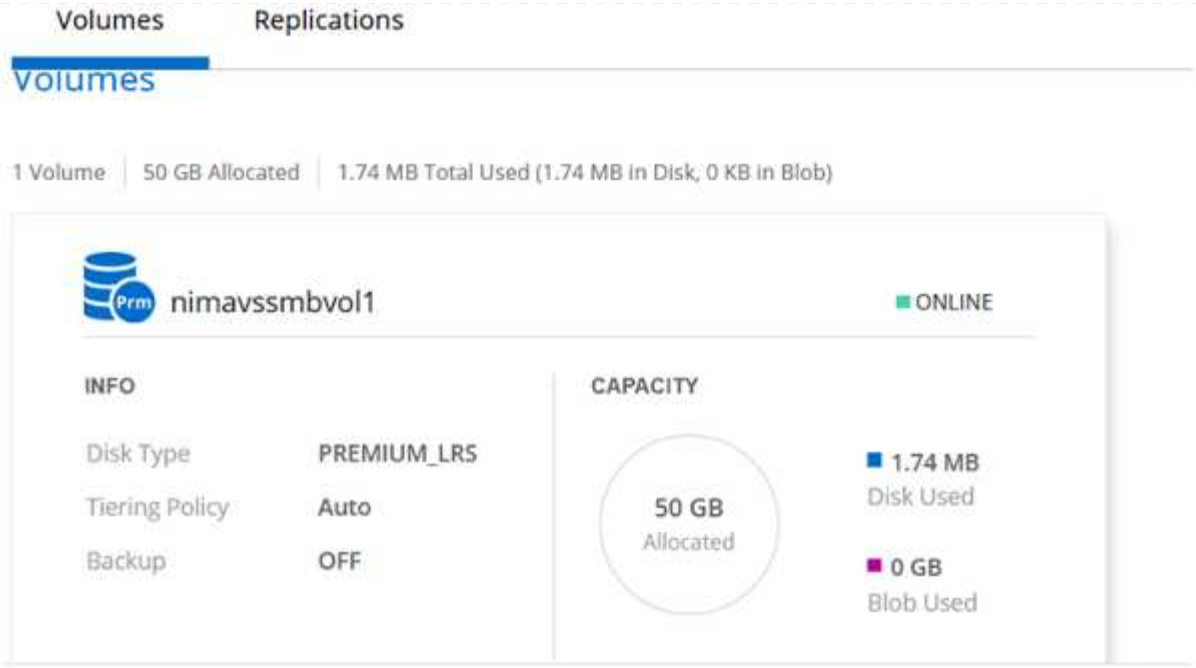
1. 准备好工作环境后，请确保为 CIFS 服务器配置了适当的 DNS 和 Active Directory 配置参数。要创建 SMB 卷，必须执行此步骤。



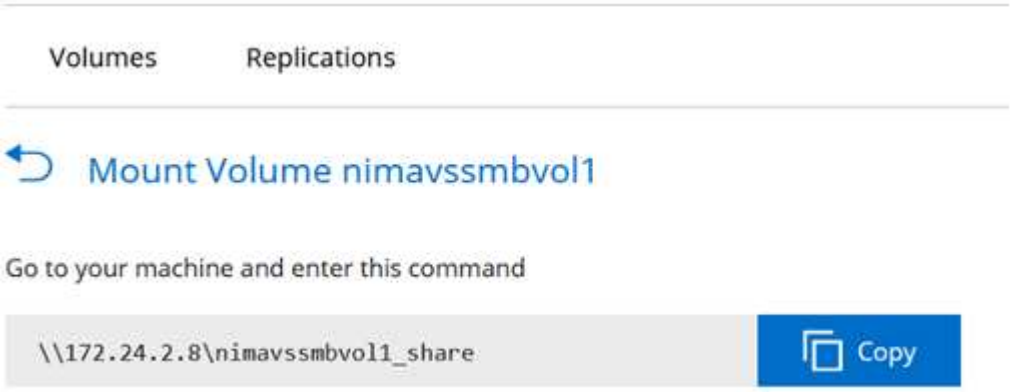
2. 创建 SMB 卷的过程非常简单。选择要创建卷的 CVO 实例，然后单击创建卷选项。选择适当的大小，Cloud Manager 选择包含的聚合或使用高级分配机制将其放置在特定聚合上。在此演示中，选择 SMB 作为协议。

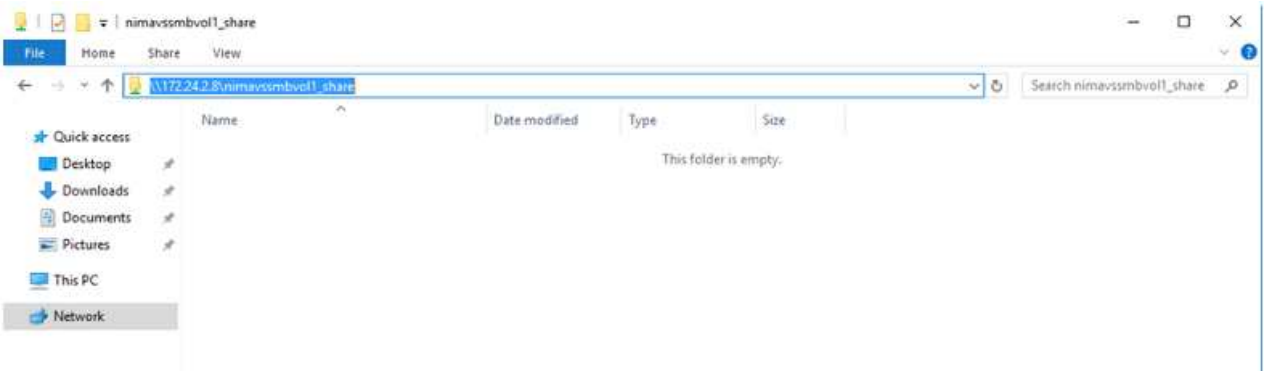


3. 配置卷后，卷将显示在卷窗格下。由于已配置 CIFS 共享，因此请为用户或组授予对文件和文件夹的权限，并验证这些用户是否可以访问此共享并创建文件。如果从内部环境复制卷，则不需要执行此步骤，因为文件和文件夹权限均会在 SnapMirror 复制过程中保留。



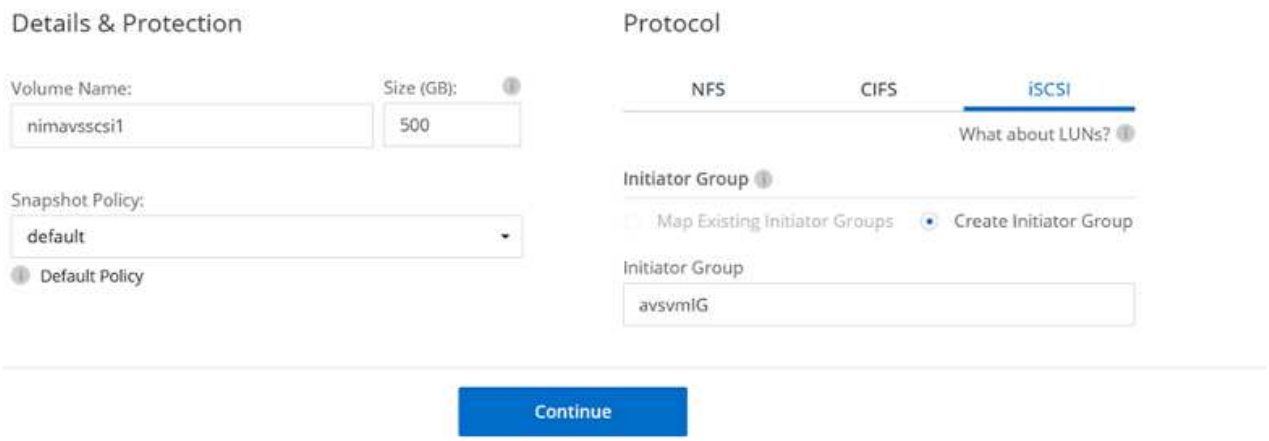
4. 创建卷后，使用 mount 命令从 Azure VMware 解决方案 SDDC 主机上运行的虚拟机连接到共享。
5. 复制以下路径并使用映射网络驱动器选项将卷挂载到 Azure VMware 解决方案 SDDC 上运行的虚拟机上。





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 "Add Volume" （添加卷） >"New Volume" （新卷），然后选择 "iSCSI" ，然后单击 "Create Initiator Group" （单击 Continue （继续）。



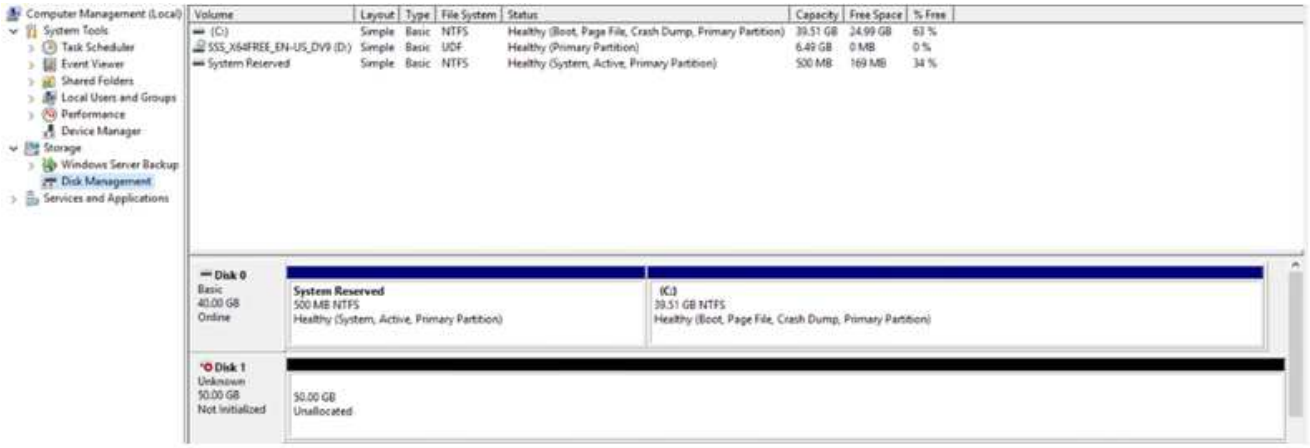
3. 配置卷后，选择卷，然后单击目标 IQN 。要复制 iSCSI 限定名称（ IQN ），请单击复制。设置从主机到 LUN 的 iSCSI 连接。

   要对 Azure VMware 解决方案 SDDC 上的主机执行相同操作，请执行以下操作：

   a. RDP 到 Azure VMware 解决方案 SDDC 上托管的虚拟机。
   b. 打开 iSCSI 启动程序属性对话框：服务器管理器 > 信息板 > 工具 > iSCSI 启动程序。
   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，选择已发现的目标，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还原此连接或将此连接添加到收藏目标列表。单击高级。
      - 注： * Windows 主机必须与集群中的每个节点建立 iSCSI 连接。原生 DSM 会选择要使用的最佳路径。

Storage Virtual Machine （ SVM ）上的 LUN 在 Windows 主机中显示为磁盘。主机不会自动发现添加的任何新磁盘。通过完成以下步骤触发手动重新扫描以发现磁盘：

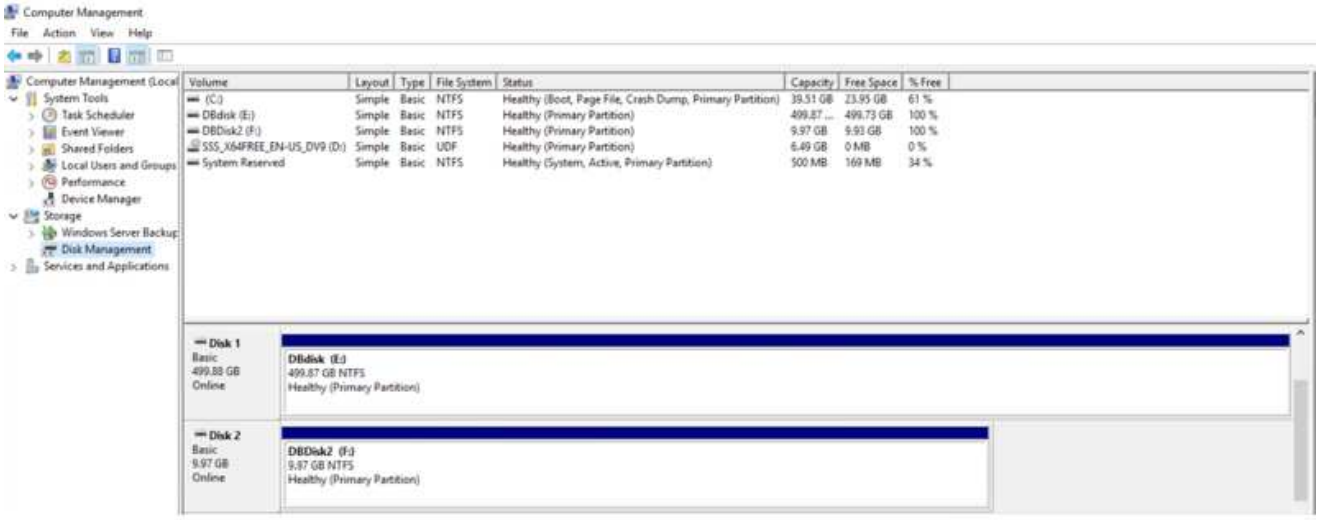
1. 打开 Windows 计算机管理实用程序：开始 > 管理工具 > 计算机管理。
2. 在导航树中展开存储节点。
3. 单击磁盘管理。
4. 单击操作 > 重新扫描磁盘。

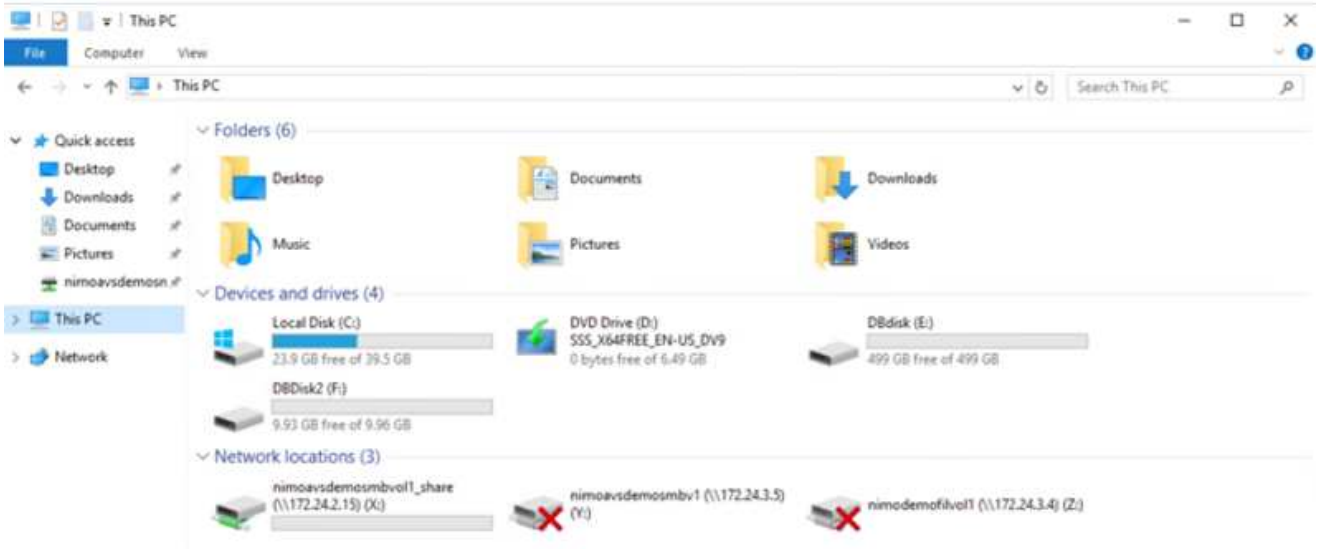


当新 LUN 首次由 Windows 主机访问时，它没有分区或文件系统。初始化 LUN ；也可以通过完成以下步骤使用文件系统格式化 LUN ：

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，驱动器 E： 已挂载



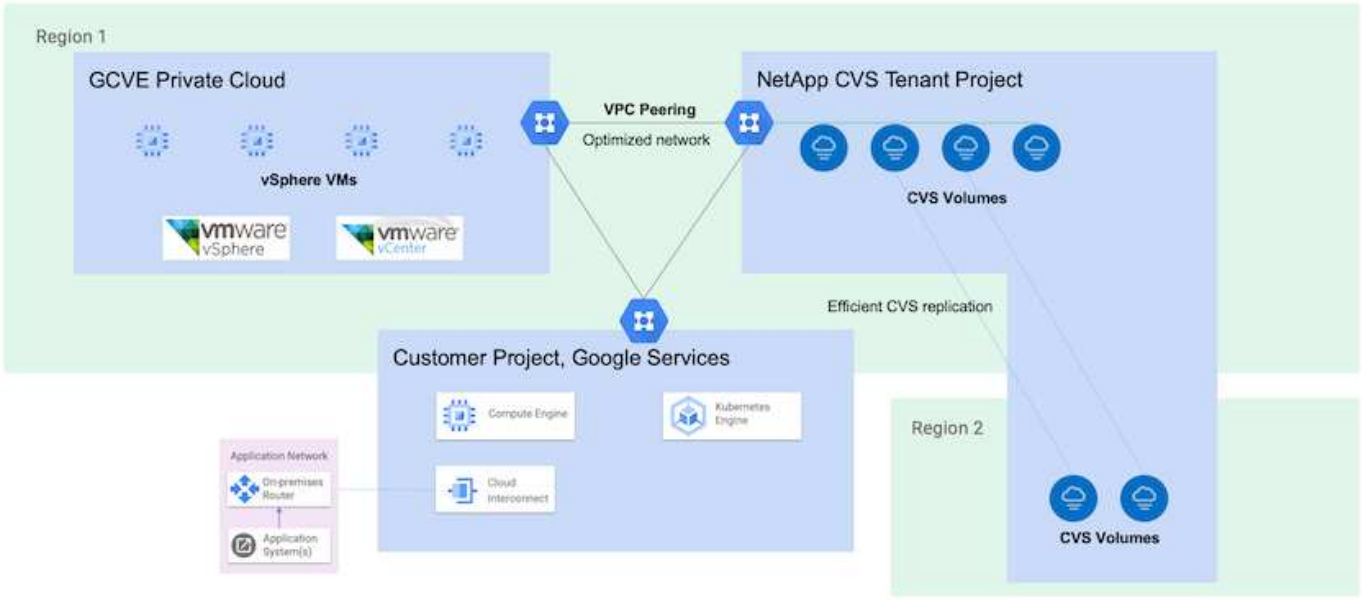


Google Cloud VMware引擎使用**NetApp**云卷服务补充**NFS**数据存储库

概述

作者：NetApp公司Suresh ThopPay

如果客户需要在其Google Cloud VMware Engine (GCVe)环境中增加存储容量、则可以使用NetApp云卷服务挂载为补充NFS数据存储库。
通过将数据存储在NetApp云卷服务上、客户可以在不同区域之间进行复制、以防止灾难。



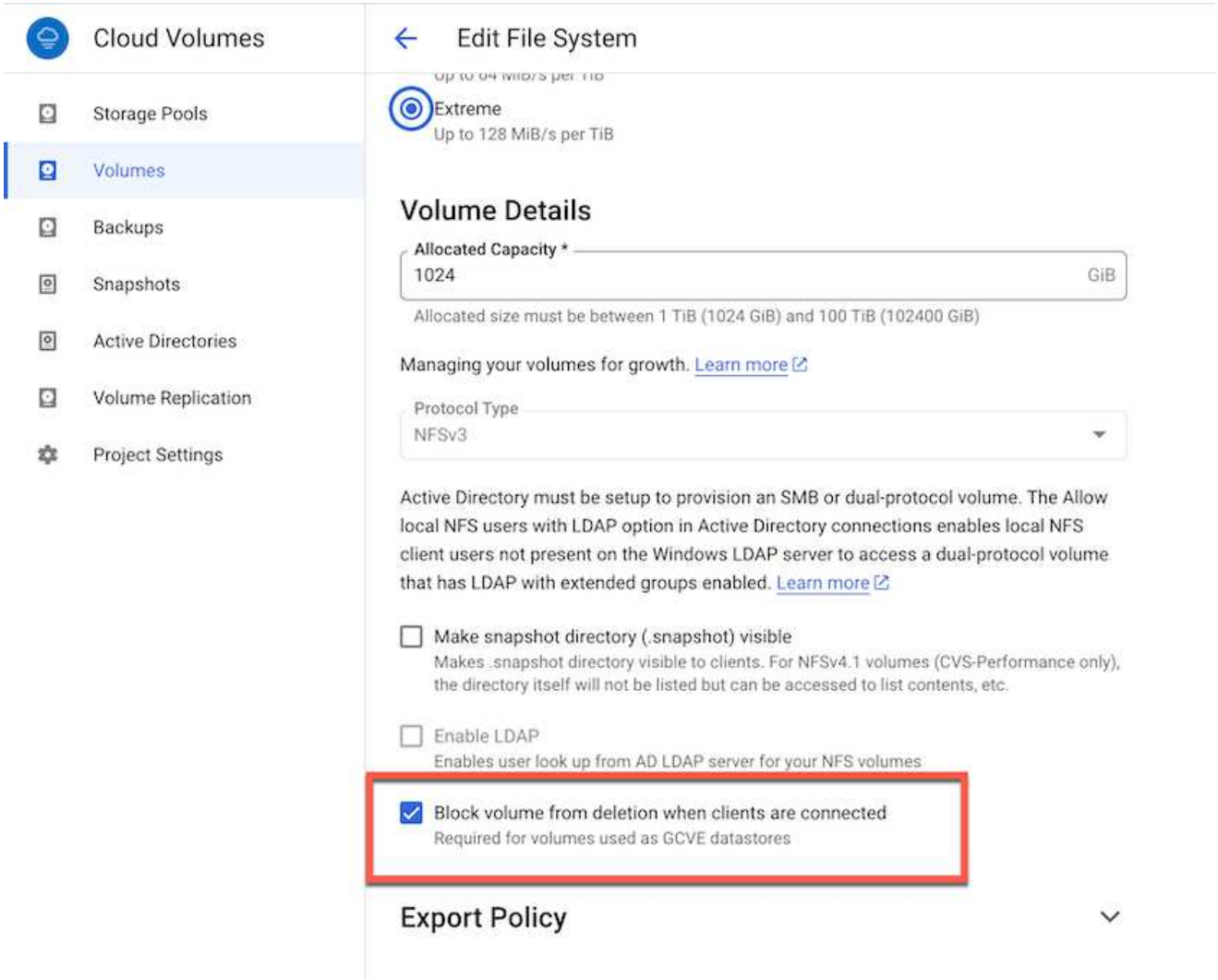
从**NetApp CVS**在**GCVE)**上挂载**NFS**数据存储库的部署步骤

配置**CVS**性能卷

NetApp云卷服务卷可以通过进行配置
"使用Google Cloud Console"
"使用NetApp BlueXP门户或API"

将该**CVS**卷标记为不可删除

为了避免在VM运行期间意外删除卷、请确保将此卷标记为不可删除、如下面的屏幕截图所示。



有关详细信息、请参见 "正在创建NFS卷" 文档。

确保**NetApp CVS**租户**VPC**在**GCVA**上存在专用连接。

要挂载NFS数据存储库、GCVA和NetApp CVS项目之间应存在专用连接。
有关详细信息、请参见 "如何设置专用服务访问"

挂载**NFS**数据存储库

有关如何在GCVE)上挂载NFS数据存储库的说明，请参阅 "如何使用NetApp CVS创建NFS数据存储库"

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

借助**NetApp**云卷服务实现节省

要详细了解NetApp云卷服务可为您的GCVe存储需求节省的空间、请查看 "NetApp ROI计算器"

参考链接

- "Google博客—如何使用NetApp CVS作为Google Cloud VMware Engine的数据存储库"
- "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支持使用Cloud Volumes ONTAP (CVO)或Cloud Volumes Service (CVS)的子系统连接的NetApp存储。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP 是行业领先的云数据管理解决方案 、基于NetApp的ONTAP 存储软件构建、可在Amazon Web Services (AWS)、Microsoft Azure和Google Cloud Platform (GCP)上本机获得。

它是ONTAP 的软件定义版本、使用云原生存储、可以在云端和内部环境中使用相同的存储软件、从而减少了对IT员工进行全新数据管理方法培训的需求。

借助CVO、客户可以无缝地将数据从边缘、数据中心、云和云端来回移动、从而将混合云整合在一起—所有这些都通过一个单一窗格管理控制台NetApp Cloud Manager进行管理。

按照设计、CVO可提供极致性能和高级数据管理功能、甚至可以满足云中要求最苛刻的应用程序的需求

Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储

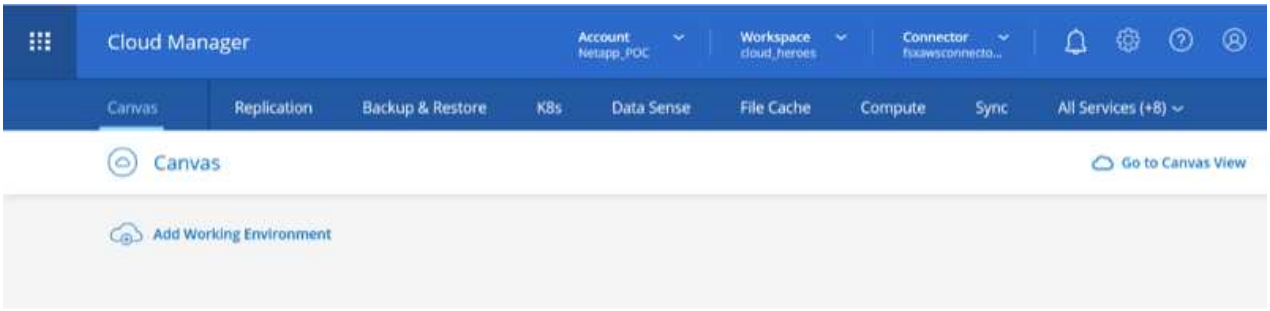
在 **Google Cloud** 中部署 **Cloud Volumes ONTAP** （自行部署）

可以从在 GCVE 私有云环境中创建的 VM 挂载 Cloud Volumes ONTAP 共享和 LUN 。这些卷还可以挂载到 Linux 客户端和 Windows 客户端上，并且在通过 iSCSI 挂载时，可以在 Linux 或 Windows 客户端上以块设备的形式访问 LUN ，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。

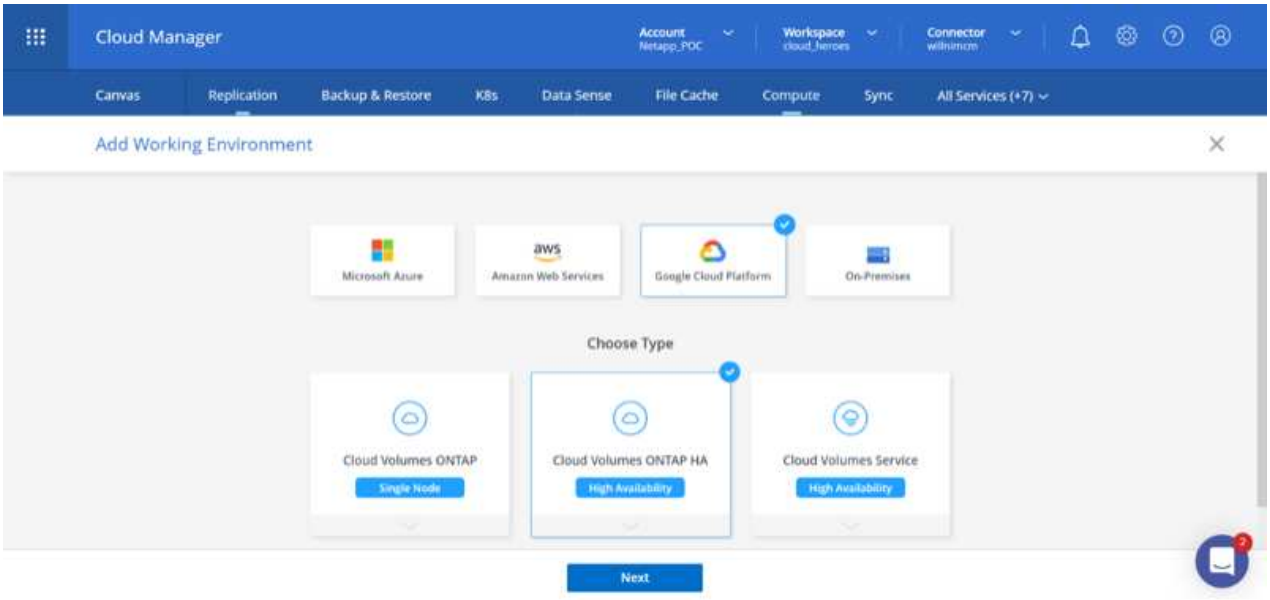
要将卷从内部环境复制到云以实现灾难恢复或迁移，请使用站点到站点 VPN 或云互连建立与 Google Cloud 的网络连接。将数据从内部复制到 Cloud Volumes ONTAP 不在本文档的讨论范围之内。要在内部系统和 Cloud Volumes ONTAP 系统之间复制数据，请参见 xref:./ehc/"在系统之间设置数据复制"。

使用 … "Cloud Volumes ONTAP 规模估算工具" 以准确估算 Cloud Volumes ONTAP 实例的大小。此外，还可以监控内部性能，以用作 Cloud Volumes ONTAP 规模估算器中的输入。

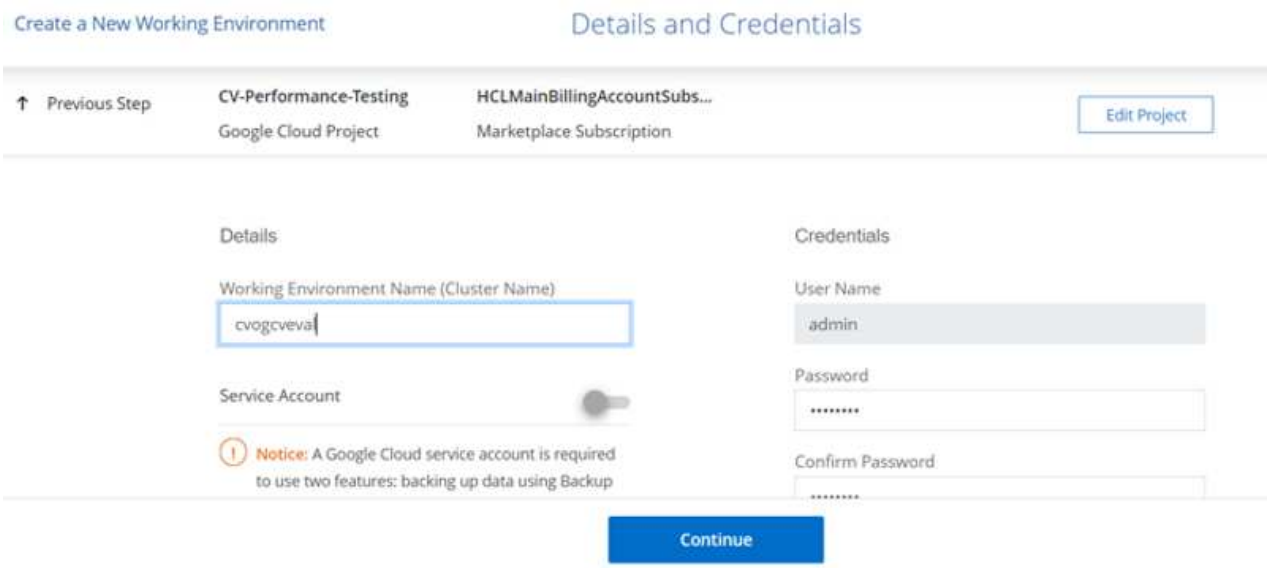
1. 登录到 NetApp Cloud Central —此时将显示 Fabric View 屏幕。找到 Cloud Volumes ONTAP 选项卡，然后选择转到 Cloud Manager 。登录后，将显示 " 画布 " 屏幕。



2. 在 Cloud Manager 的 " 画布 " 选项卡上，单击添加工作环境，然后选择 Google Cloud Platform 作为云以及系统配置的类型。然后，单击下一步。

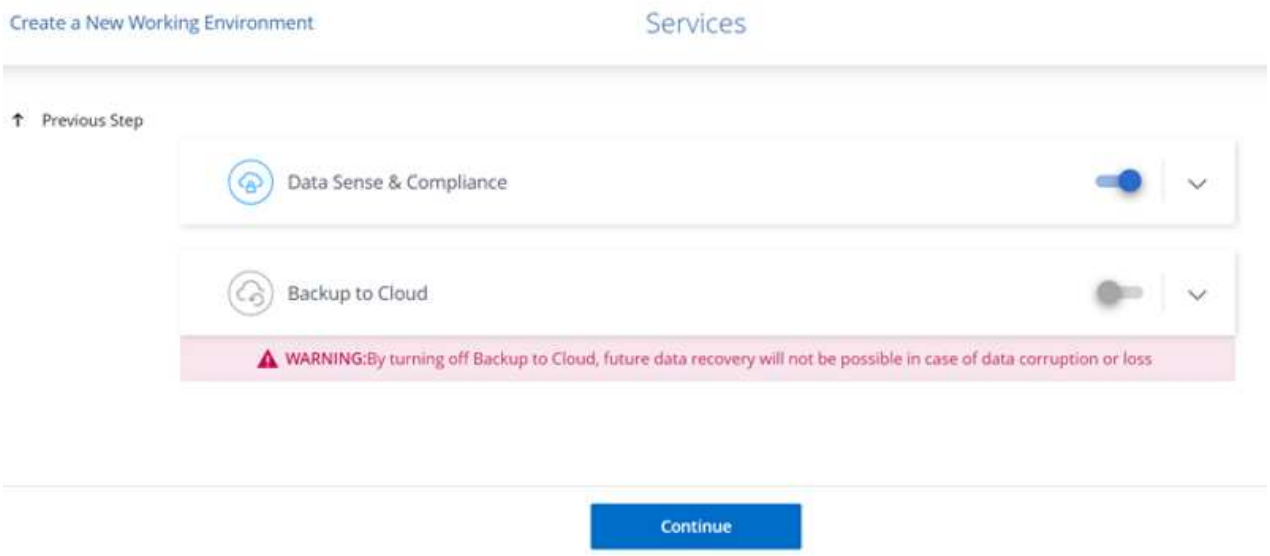


3. 提供要创建的环境的详细信息，包括环境名称和管理员凭据。完成后，单击 Continue 。

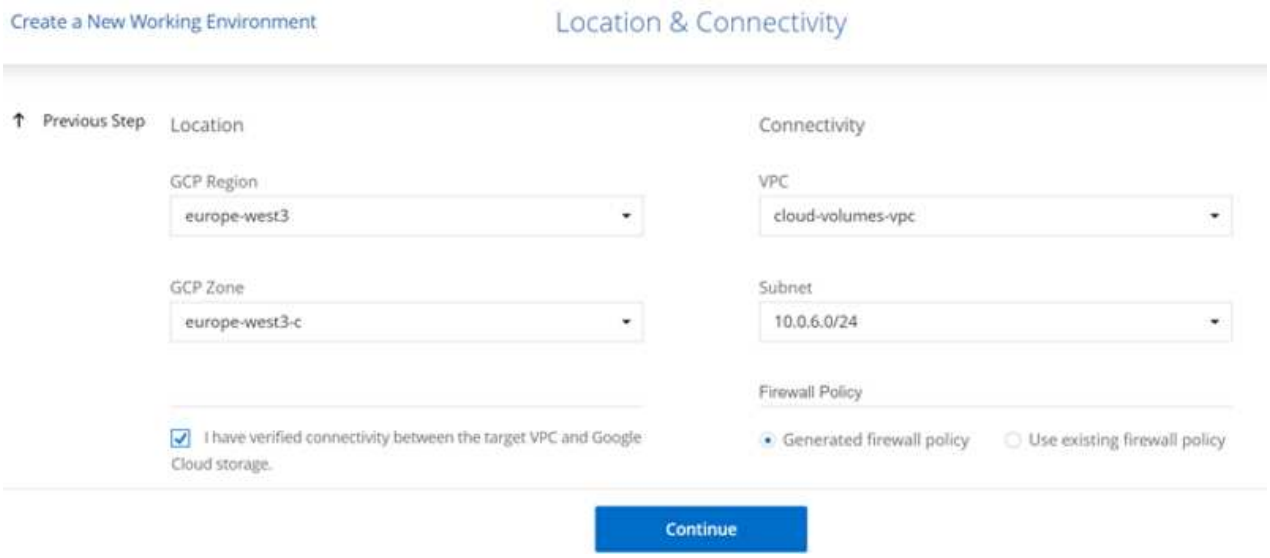


4. 选择或取消选择 Cloud Volumes ONTAP 部署的附加服务，包括数据感知与合规性或备份到云。然后，单击 Continue 。

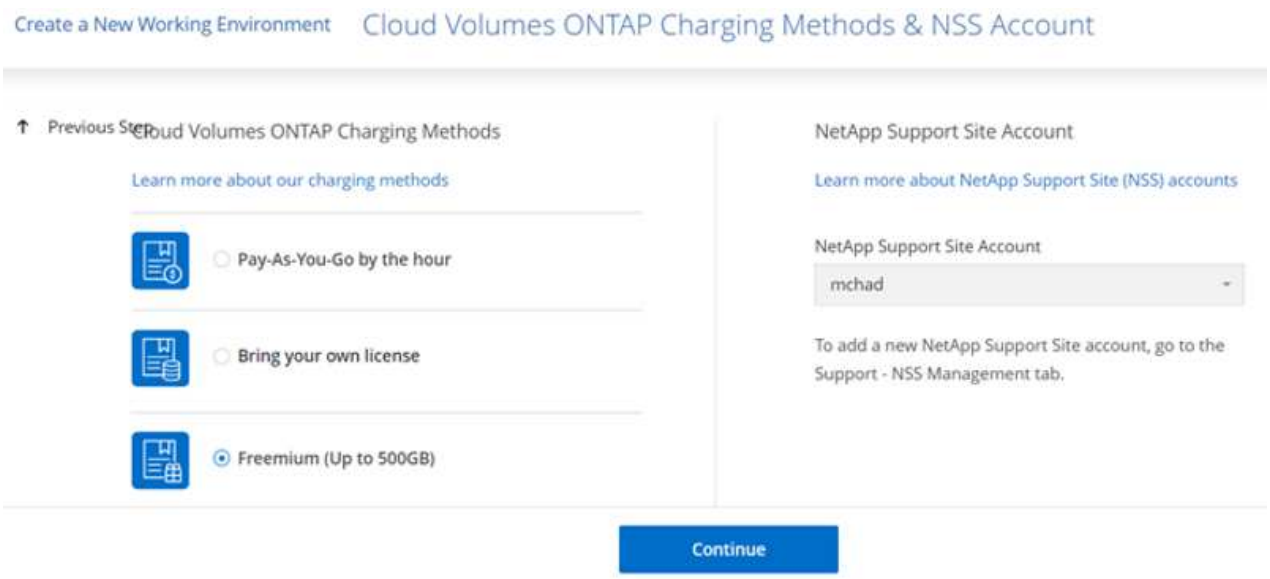
   提示：停用附加服务时，将显示验证弹出消息。可以在部署 CVO 后添加 / 删除附加服务，如果不需要，请考虑从一开始就取消选择这些附加服务，以避免成本。



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

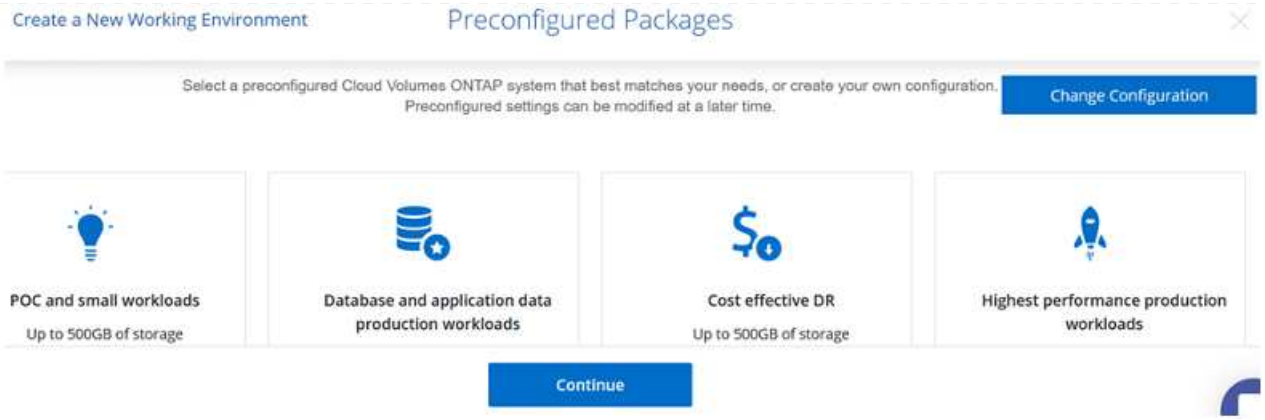


6. 选择许可证选项：按需购买或自带许可证以使用现有许可证。在此示例中，使用了 freemium 选项。然后，单击 Continue 。

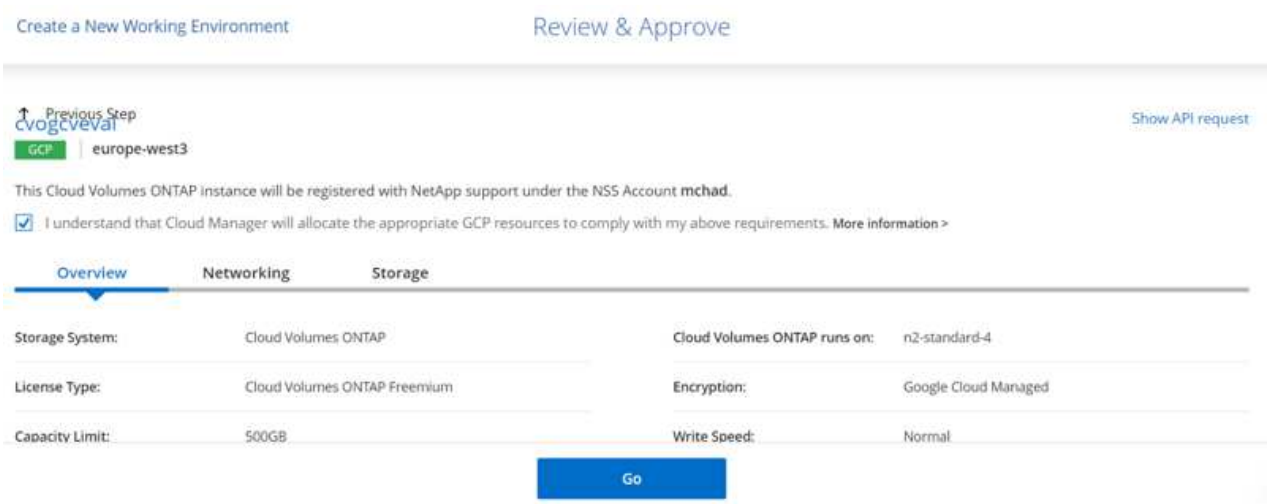


7. 根据要部署在 AWS SDDC 上的 VMware 云上运行的 VM 上的工作负载类型，在多个预配置的软件包之间进行选择。

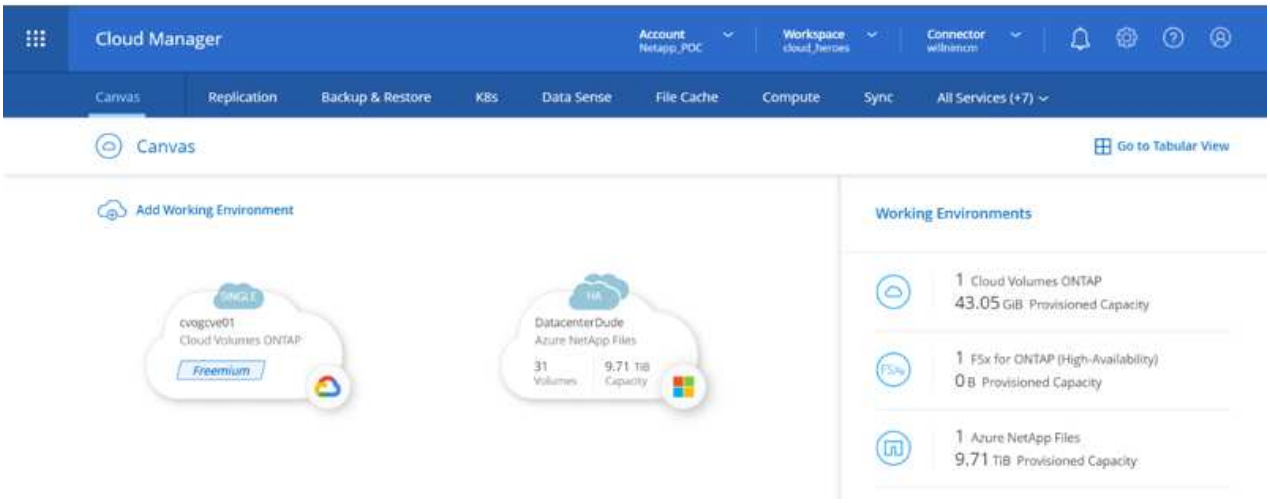
   提示：将鼠标悬停在图块上可查看详细信息，或者单击更改配置来自定义 CVO 组件和 ONTAP 版本。



8. 在审核和批准页面上，查看并确认所做的选择。要创建 Cloud Volumes ONTAP 实例，请单击执行。



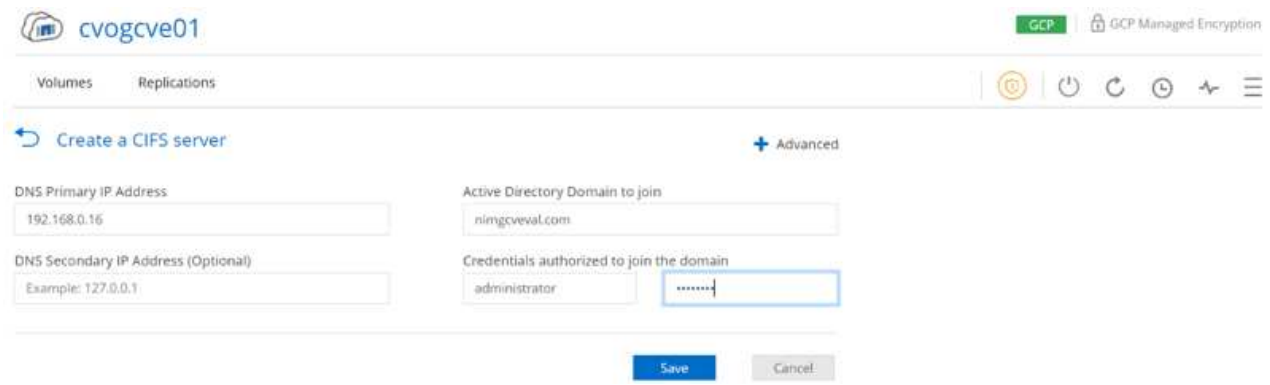
9. 配置 Cloud Volumes ONTAP 后，它将在 " 画布 " 页面的工作环境中列出。



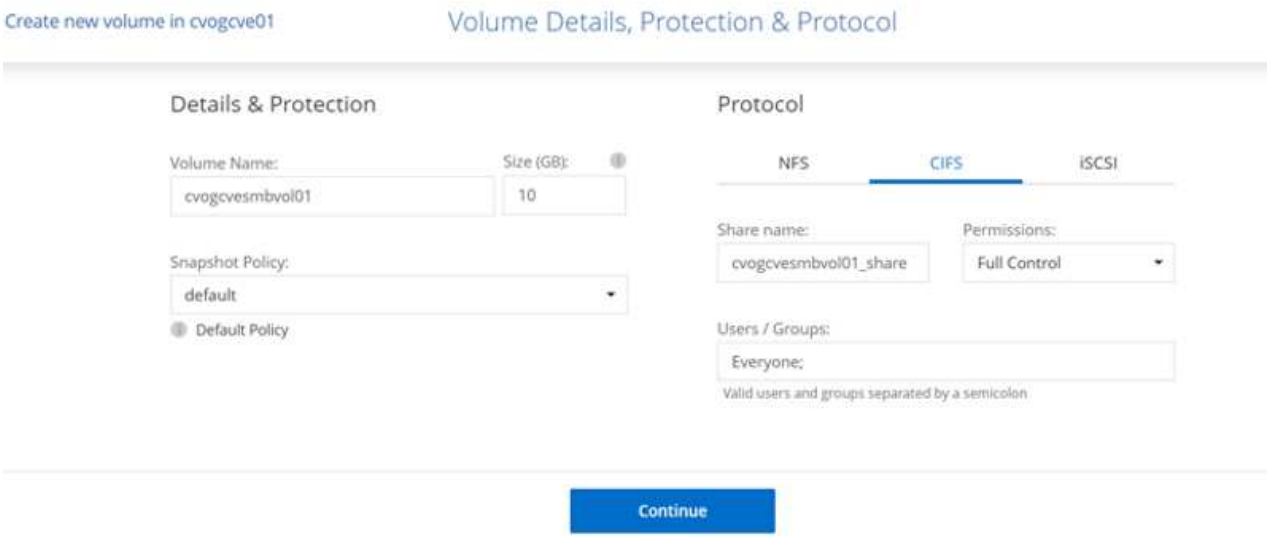
SMB 卷的其他配置

1. 准备好工作环境后，请确保为 CIFS 服务器配置了适当的 DNS 和 Active Directory 配置参数。要创建 SMB 卷，必须执行此步骤。

   提示：单击菜单图标（⁰），选择高级以显示更多选项，然后选择 CIFS 设置。



2. 创建 SMB 卷的过程非常简单。在 " 画布 " 中，双击 Cloud Volumes ONTAP 工作环境以创建和管理卷，然后单击创建卷选项。选择适当的大小， Cloud Manager 选择包含的聚合或使用高级分配机制将其放置在特定聚合上。在此演示中，选择 CIFS/SMB 作为协议。

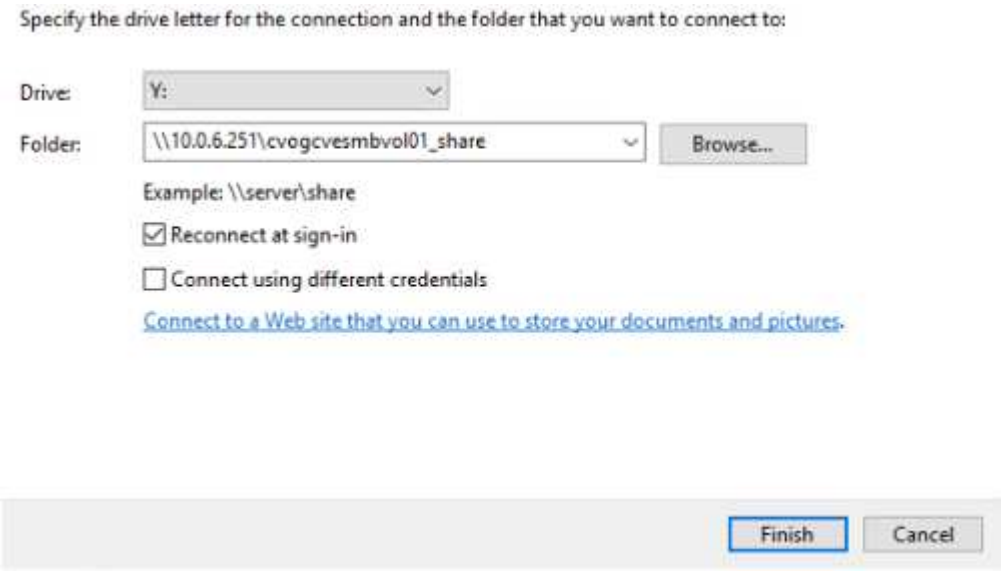


3. 配置卷后，卷将显示在卷窗格下。由于已配置 CIFS 共享，因此请为用户或组授予对文件和文件夹的权限，并验证这些用户是否可以访问此共享并创建文件。如果从内部环境复制卷，则不需要执行此步骤，因为文件和文件夹权限均会在 SnapMirror 复制过程中保留。

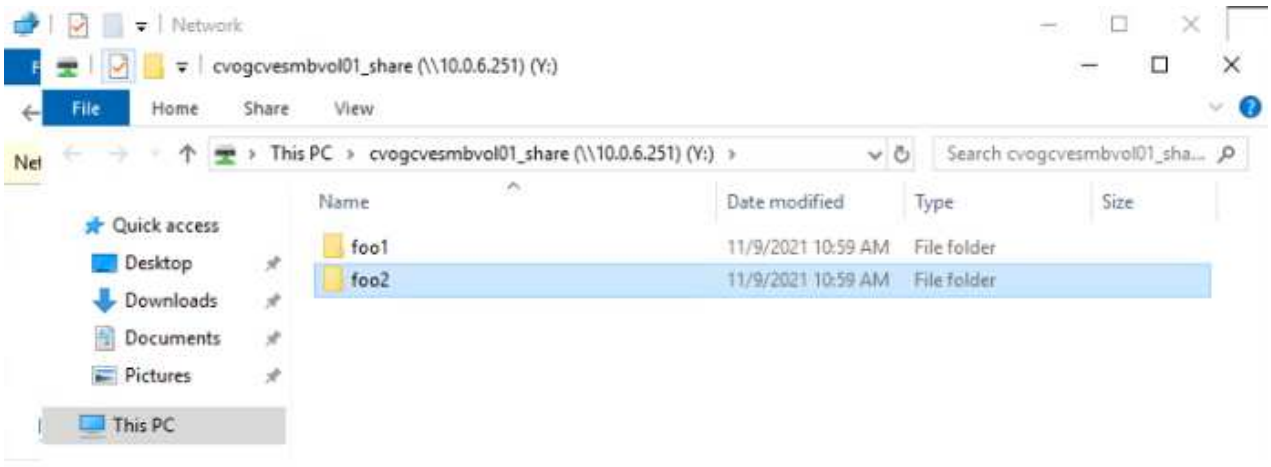
   提示：单击卷菜单（⁰）可显示其选项。

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 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挂载到 Google Cloud VMware 引擎上运行的虚拟机上。



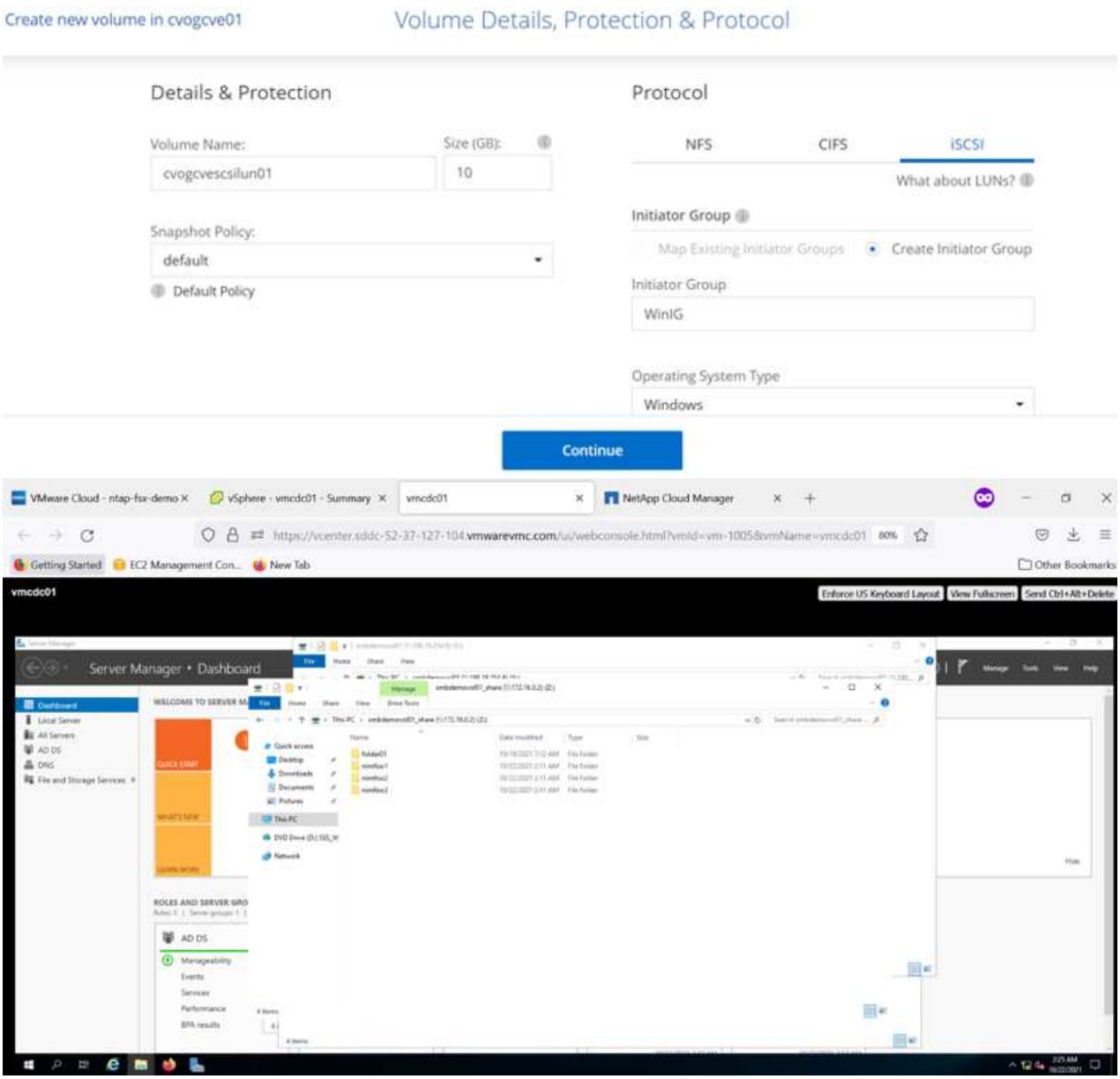
映射后，可以轻松访问该文件，并相应地设置 NTFS 权限。



将 **Cloud Volumes ONTAP** 上的 **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 " 画布 " 页面上，双击 Cloud Volumes ONTAP 工作环境以创建和管理卷。
2. 单击 "Add Volume" （添加卷） >"New Volume" （新卷），然后选择 "iSCSI" ，然后单击 "Create Initiator Group" （单击 Continue （继续）。



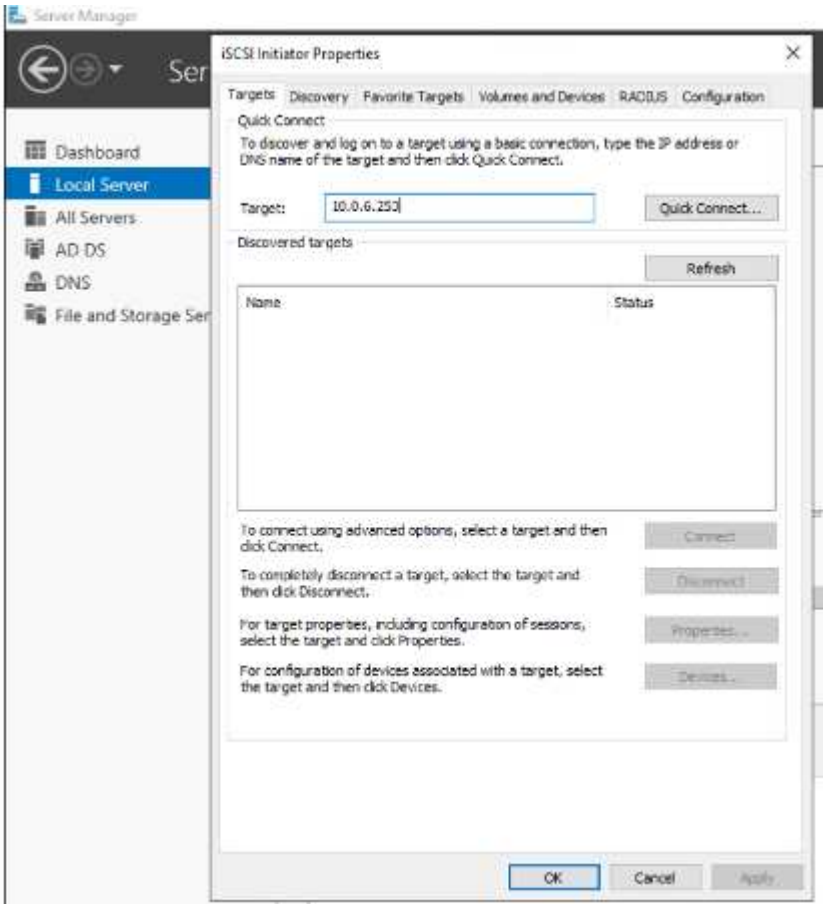
3. 配置卷后，选择卷菜单（ º ），然后单击目标 IQN 。要复制 iSCSI 限定名称（ IQN ），请单击复制。设置从主机到 LUN 的 iSCSI 连接。

要对驻留在 Google Cloud VMware Engine 上的主机执行相同操作，请执行以下操作：

1. RDP 到 Google Cloud VMware Engine 上托管的 VM 。
2. 打开 iSCSI 启动程序属性对话框：服务器管理器 > 信息板 > 工具 > iSCSI 启动程序。

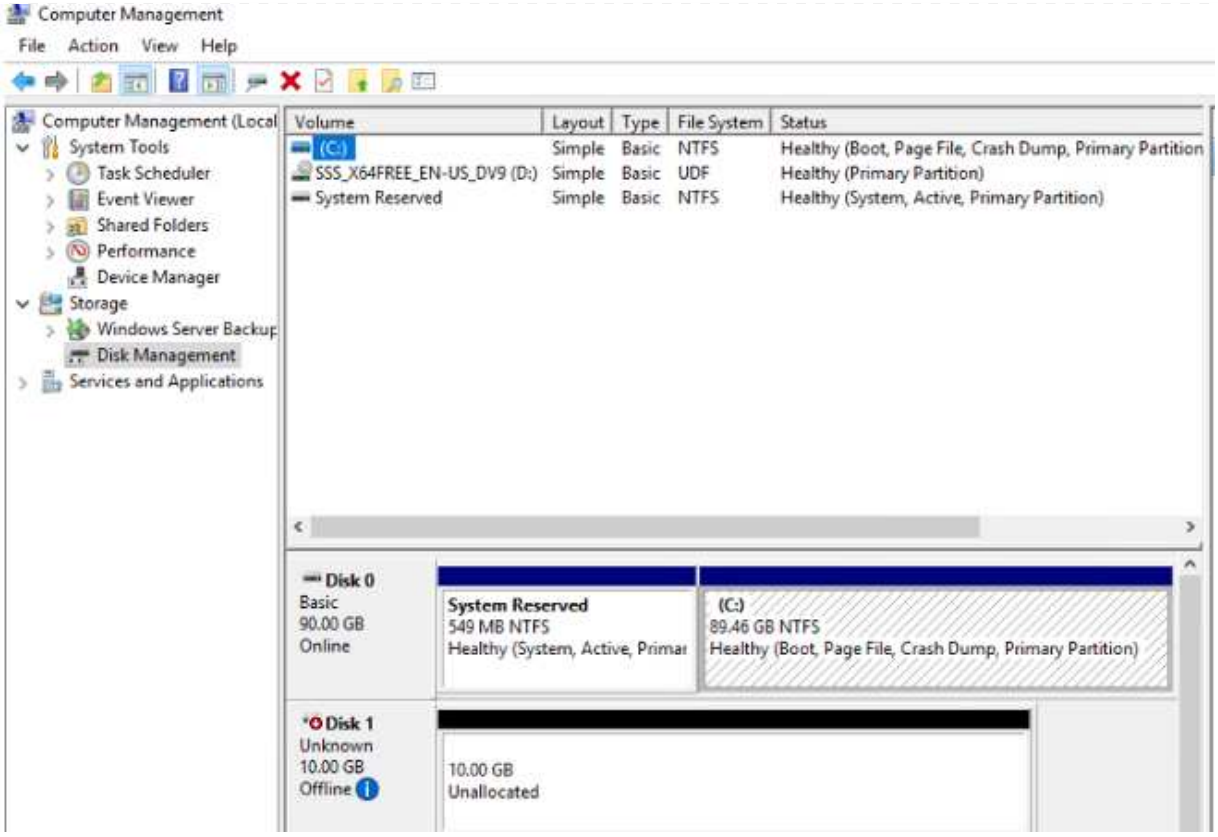
3. 在发现选项卡中，单击发现门户或添加门户，然后输入 iSCSI 目标端口的 IP 地址。
4. 从目标选项卡中，选择已发现的目标，然后单击登录或连接。
5. 选择启用多路径，然后选择计算机启动时自动还原此连接或将此连接添加到收藏目标列表。单击高级。

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



Storage Virtual Machine （SVM）上的 LUN 在 Windows 主机中显示为磁盘。主机不会自动发现添加的任何新磁盘。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。

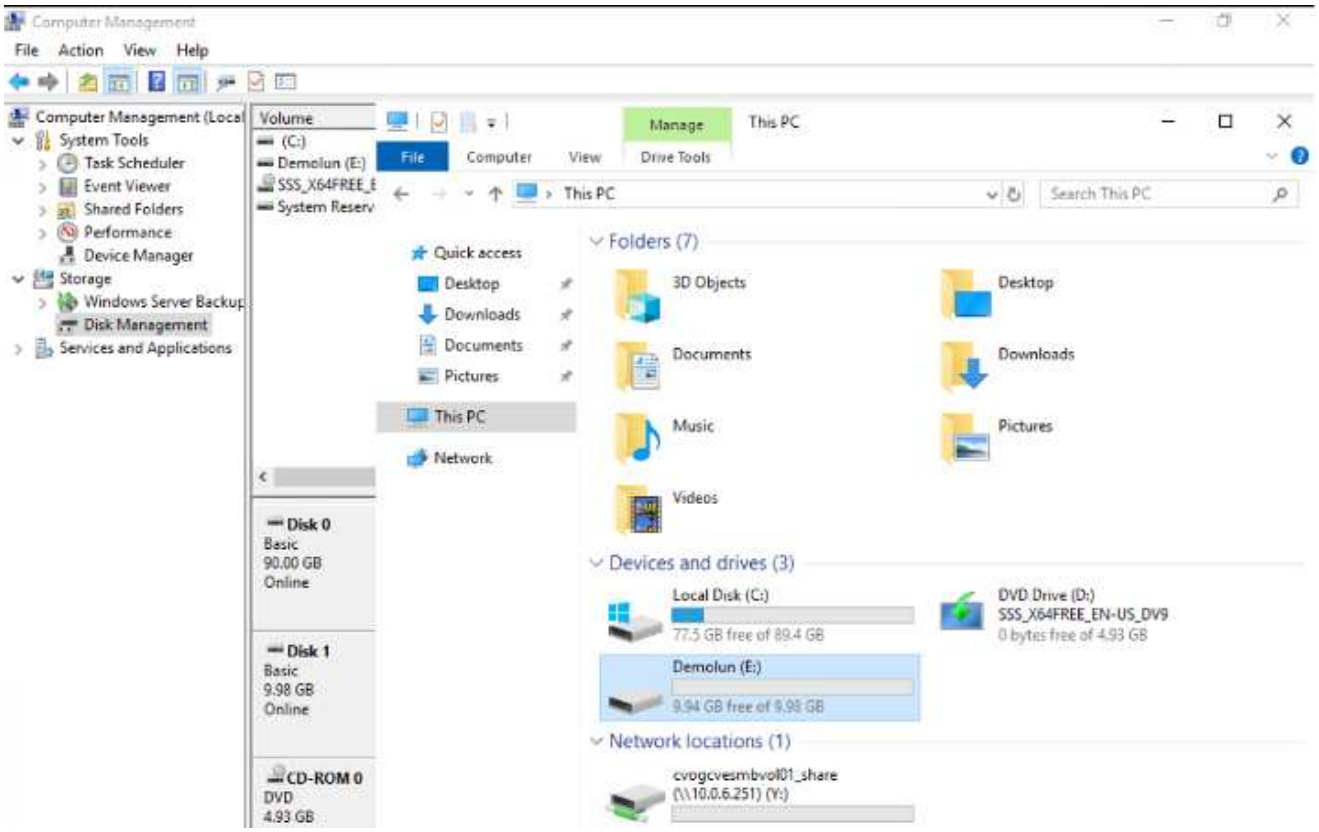


当新 LUN 首次由 Windows 主机访问时，它没有分区或文件系统。初始化 LUN ； 也可以通过完成以下步骤使用文件系统格式化 LUN ：

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，驱动器 F ： 已挂载。



在 Linux 客户端上，确保 iSCSI 守护进程正在运行。配置 LUN 后，请参见有关使用 Ubuntu 进行 iSCSI 配置的详细指南，作为示例。要进行验证，请从 shell 运行 lsblk cmd 。

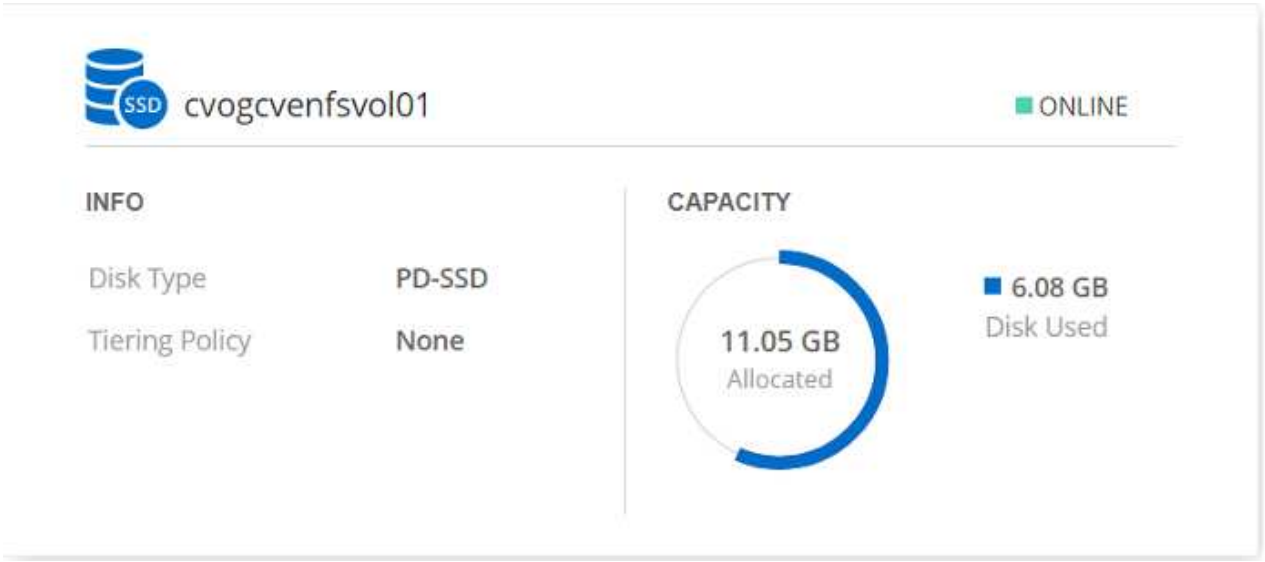
```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    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

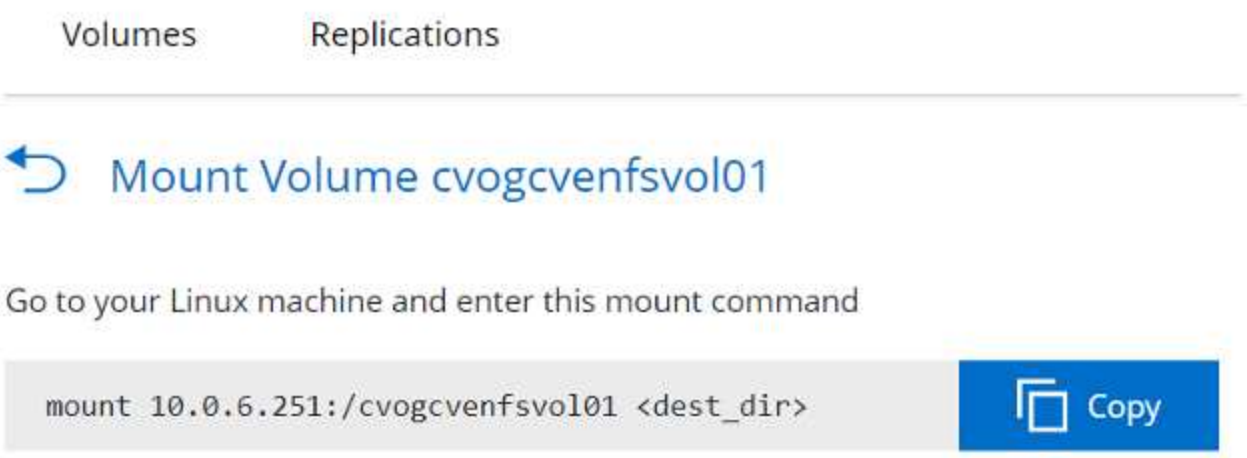
要从 Google Cloud VMware 引擎中的 VM 挂载 Cloud Volumes ONTAP （ DIY ）文件系统，请执行以下步骤：

按照以下步骤配置卷

1. 在 Volumes （卷）选项卡中，单击 Create New Volume （创建新卷）。
2. 在 "Create New Volume" 页面上，选择卷类型：



3. 在卷选项卡中，将鼠标光标置于卷上方，选择菜单图标（ ° ），然后单击挂载命令。



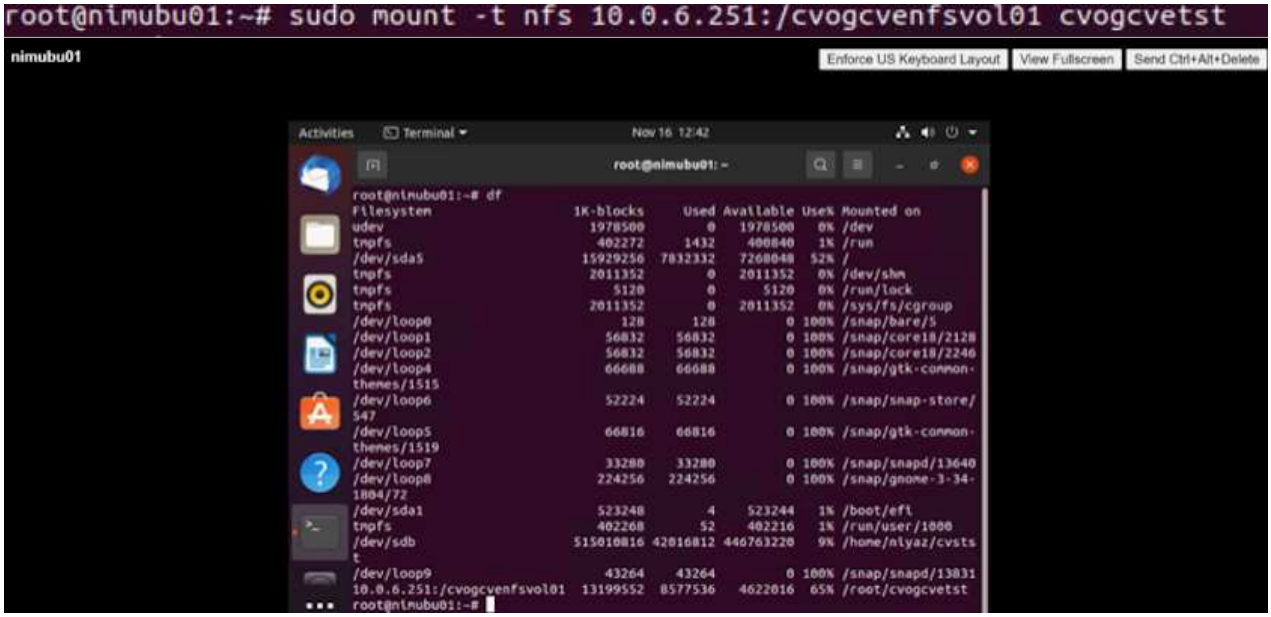
4. 单击复制。
5. 连接到指定的 Linux 实例。
6. 使用安全 Shell （ SSH ）在实例上打开一个终端，并使用相应的凭据登录。
7. 使用以下命令为卷的挂载点创建一个目录。

```
$ 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
```



Cloud Volumes Service (CVS)

Cloud Volumes Services (CVS)是一套完整的数据服务产品组合、可提供高级云解决方案。Cloud Volumes Services支持为主要云提供商提供多种文件访问协议(NFS和SMB支持)。

其他优势和功能包括：使用Snapshot进行数据保护和还原；在内部或云端复制、同步和迁移数据目标的特殊功能；以及在专用闪存存储系统级别实现一致的高性能。

Cloud Volumes Service （ CVS ）作为子系统连接的存储

使用 **VMware** 引擎配置 **Cloud Volumes Service**

可以从 VMware 引擎环境中创建的 VM 挂载 Cloud Volumes Service 共享。由于 Cloud Volumes Service 支持 SMB 和 NFS 协议，因此这些卷也可以挂载到 Linux 客户端并映射到 Windows 客户端。可以通过简单的步骤设置 Cloud Volumes Service 卷。

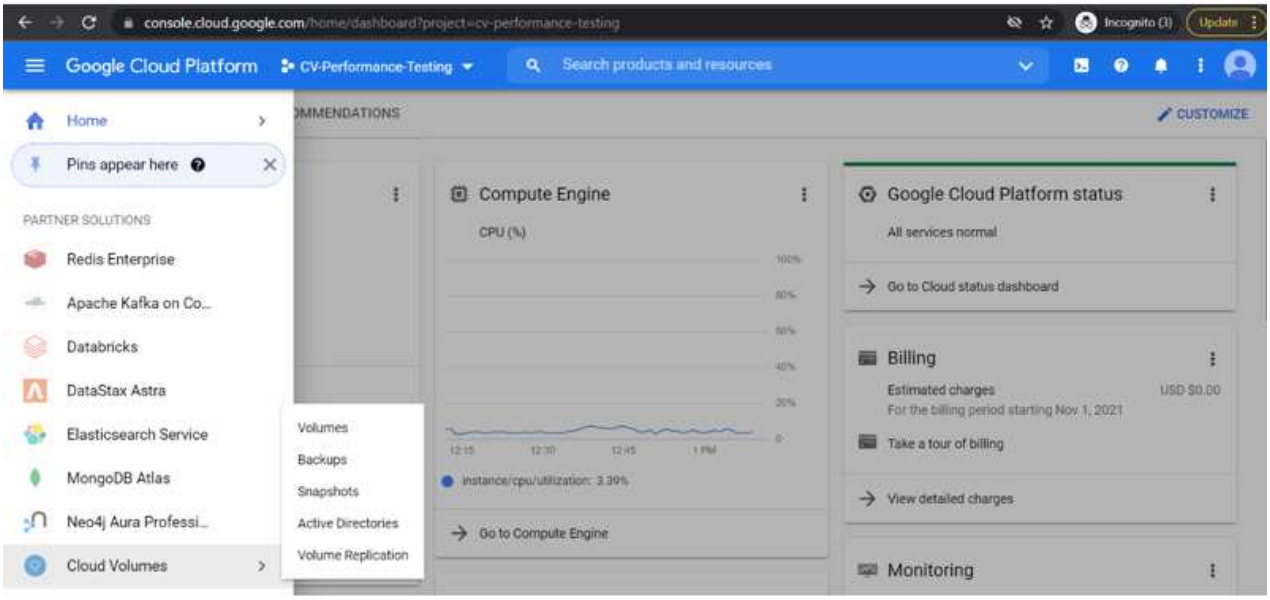
Cloud Volume Service 和 Google Cloud VMware Engine 私有云必须位于同一区域。

要从 Google 云市场购买，启用和配置适用于 Google Cloud 的 NetApp Cloud Volumes Service ，请按照以下详细信息进行操作 "指南"。

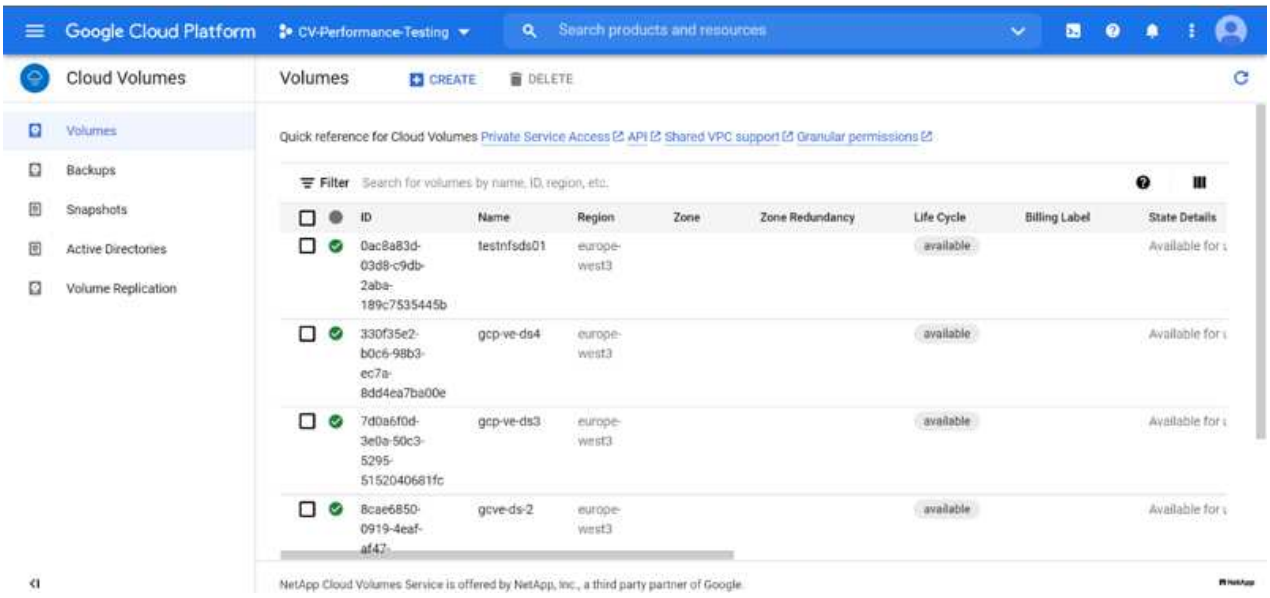
创建一个 **CVS NFS** 卷到 **GCVE** 私有云

要创建和挂载 NFS 卷，请完成以下步骤：

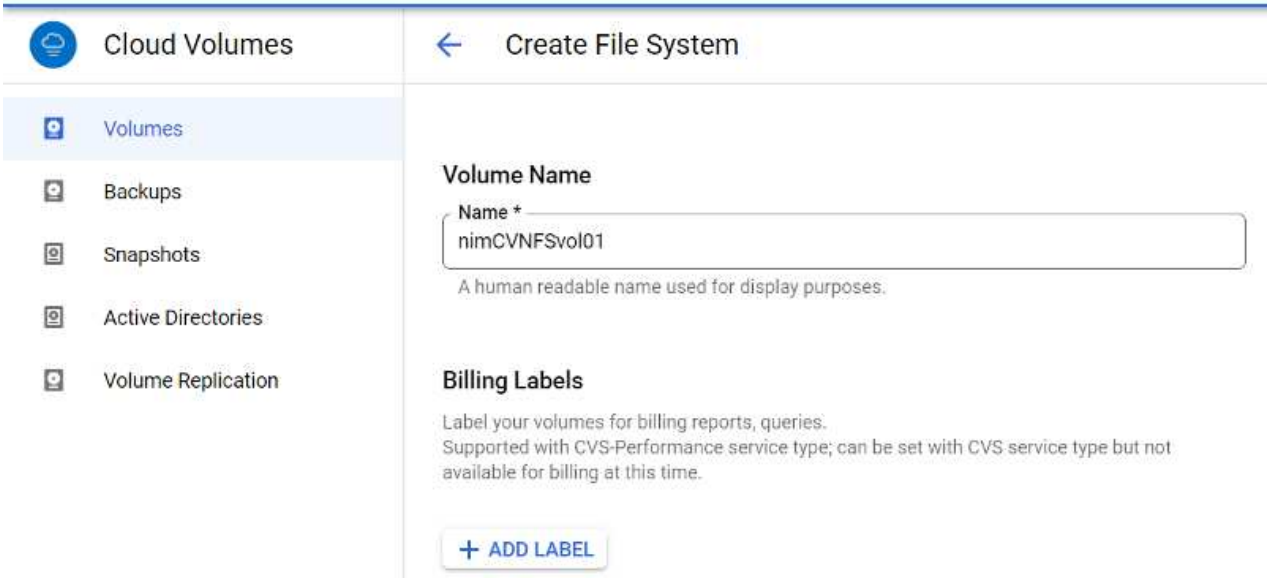
1. 从 Google 云控制台中的合作伙伴解决方案访问 Cloud Volumes 。



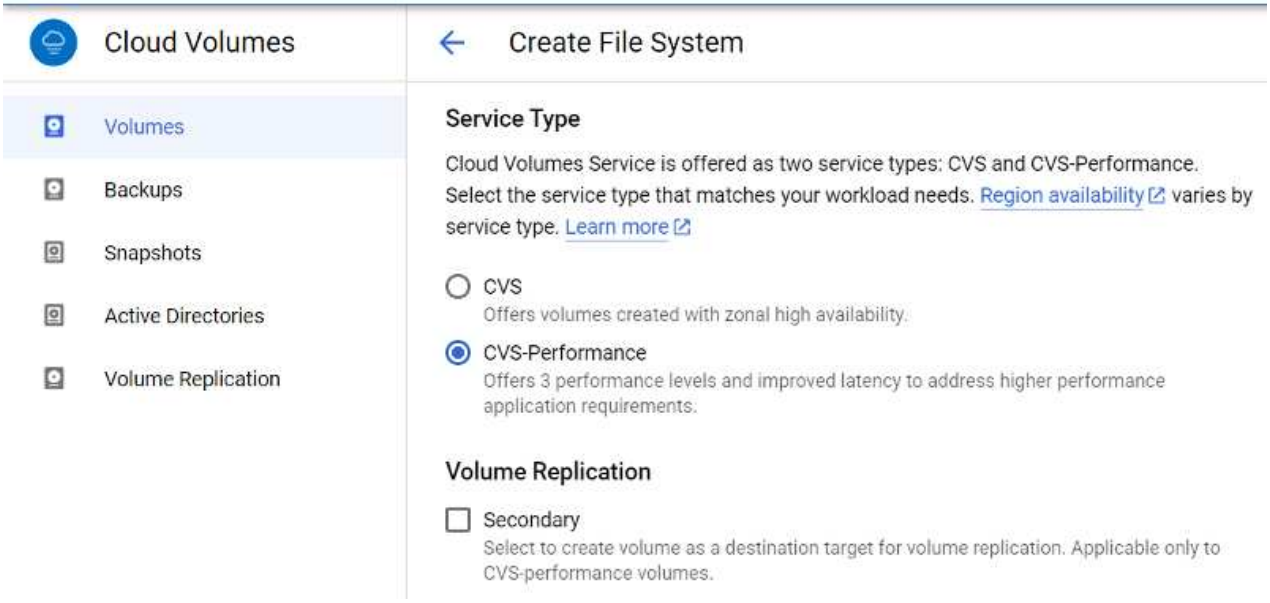
2. 在 Cloud Volumes Console 中，转到 Volumes 页面，然后单击 Create 。



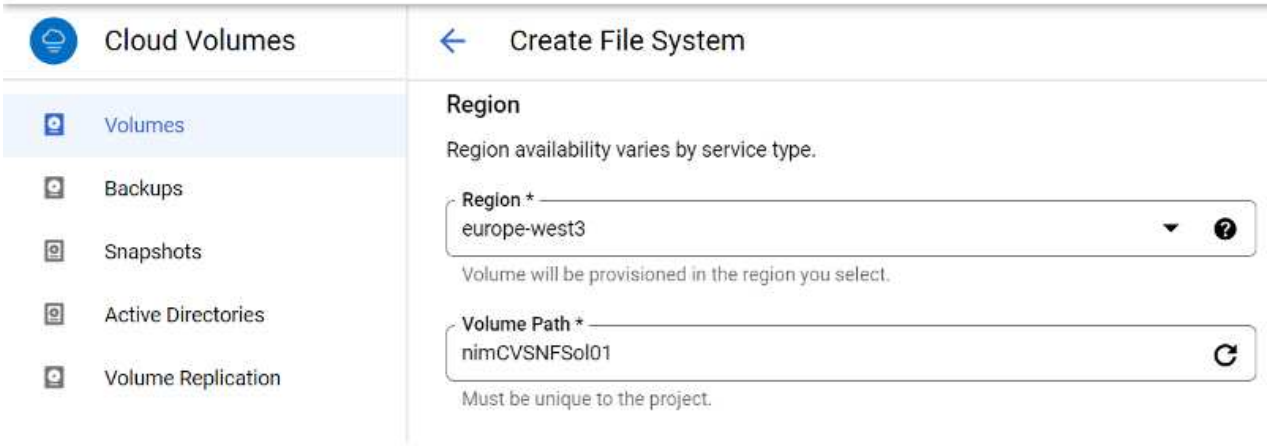
3. 在创建文件系统页面上，根据成本分摊机制的需要指定卷名称和计费标签。



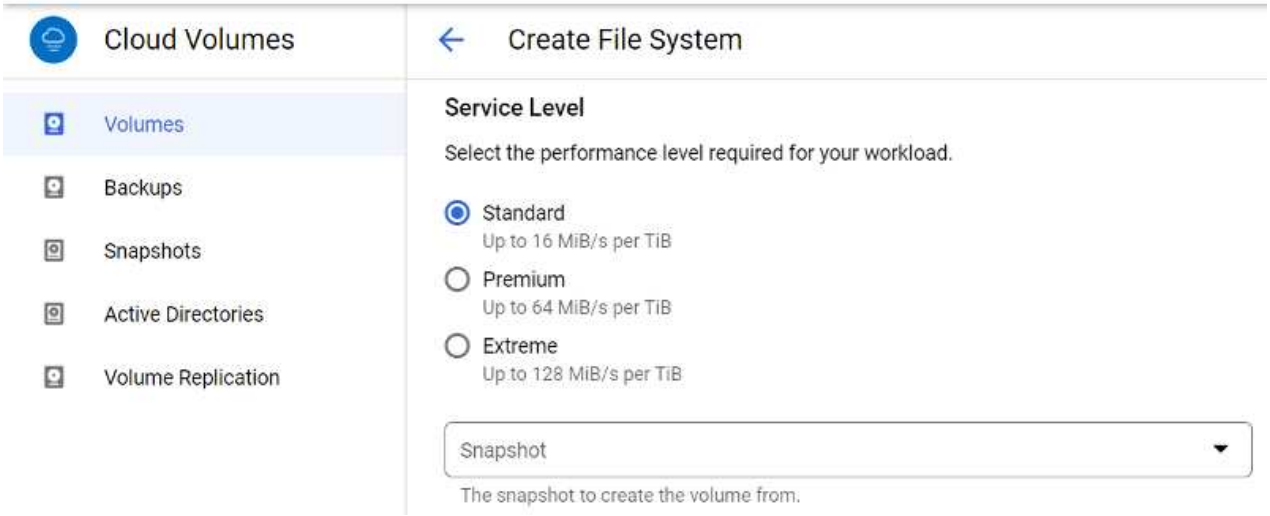
4. 选择相应的服务。对于 GCVE ，请选择 CVS-Performance 和所需的服务级别，以根据应用程序工作负载要求提高延迟和性能。



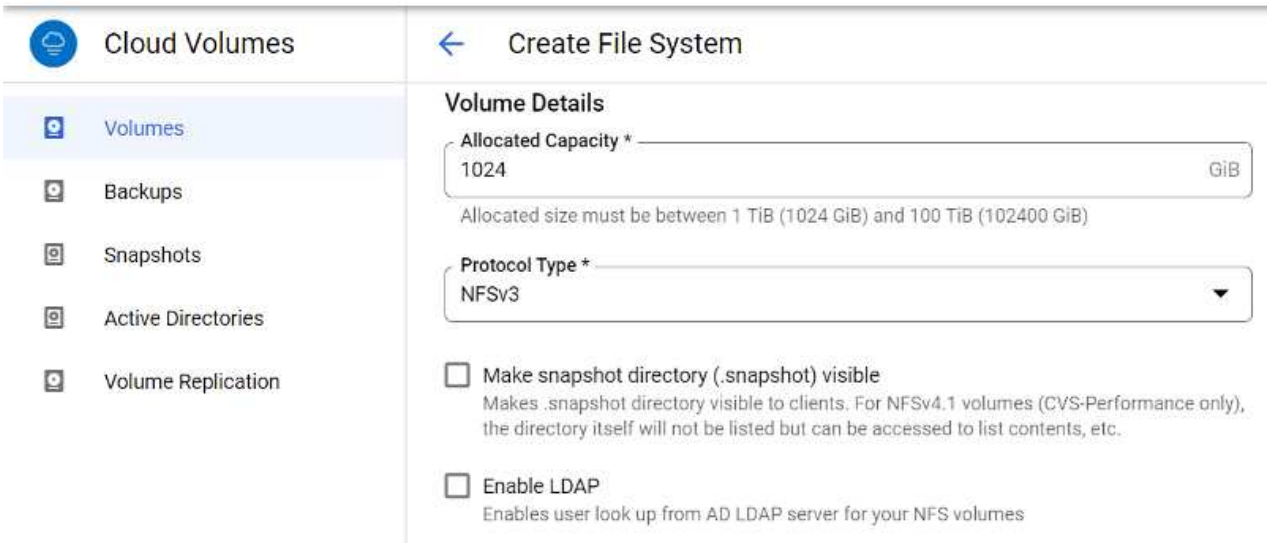
5. 为卷和卷路径指定 Google Cloud 区域（卷路径必须在项目中的所有云卷之间是唯一的）



6. 选择卷的性能级别。

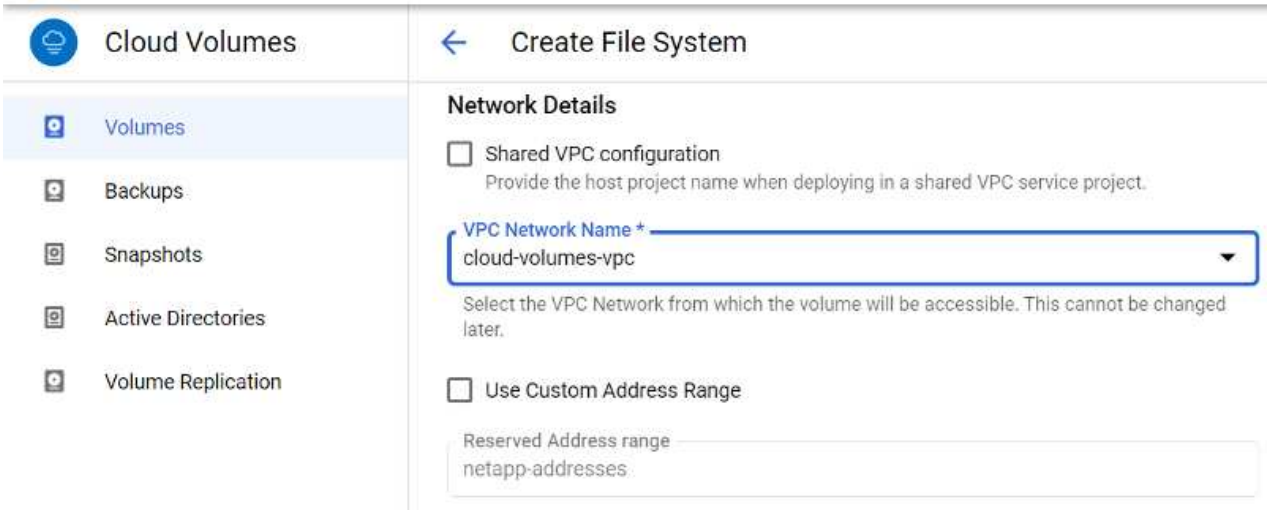


7. 指定卷的大小和协议类型。在此测试中，将使用 NFSv3 。



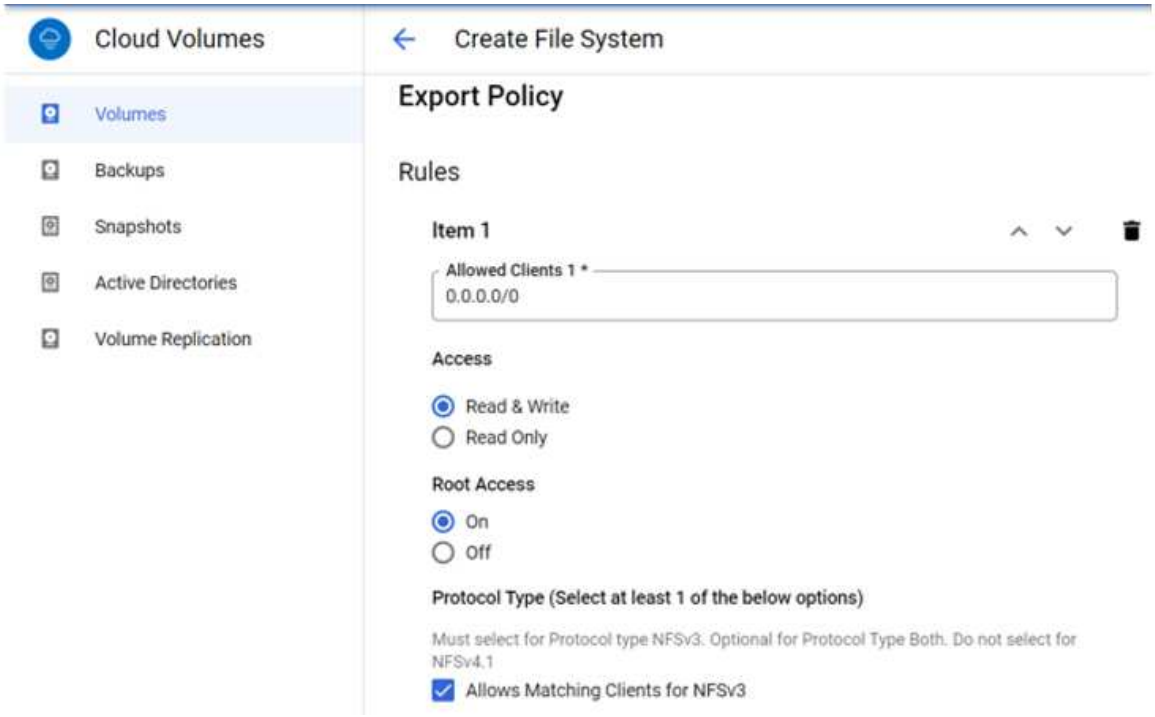
8. 在此步骤中，选择可从中访问卷的 VPC 网络。确保已建立 VPC 对等关系。

提示：如果尚未建立 VPC 对等关系，则会显示一个弹出按钮，用于指导您完成对等命令。打开 Cloud Shell 会话并执行相应的命令，将您的 VPC 与 Cloud Volumes Service 生产者建立对等关系。如果您决定事先准备 VPC 对等关系，请参见以下说明。



9. 通过添加相应的规则来管理导出策略规则，然后选中相应 NFS 版本对应的复选框。

   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** 引擎上运行的 **VM**

在准备挂载 NFS 卷之前，请确保专用连接的对等状态列为 "Active" 。状态为 "Active" 后，请使用 mount 命令。

要挂载 NFS 卷，请执行以下操作：

1. 在 Cloud Console 中，转至 Cloud Volumes > Volumes 。
2. 转到卷页面
3. 单击要挂载 NFS 导出的 NFS 卷。
4. 向右滚动，在显示更多下，单击挂载说明。

要从 VMware VM 的子操作系统中执行挂载过程，请执行以下步骤：

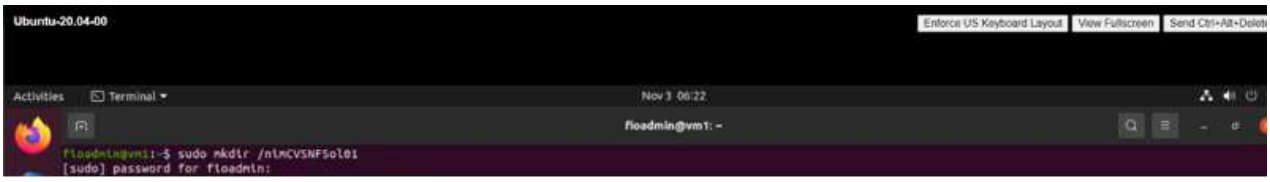
1. 对虚拟机使用 SSH 客户端和 SSH 。
2. 在实例上安装 NFS 客户端。
   a. 在 Red Hat Enterprise Linux 或 SUSE Linux 实例上：

```
 sudo yum install -y nfs-utils
.. 在 Ubuntu 或 Debian 实例上：
```

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

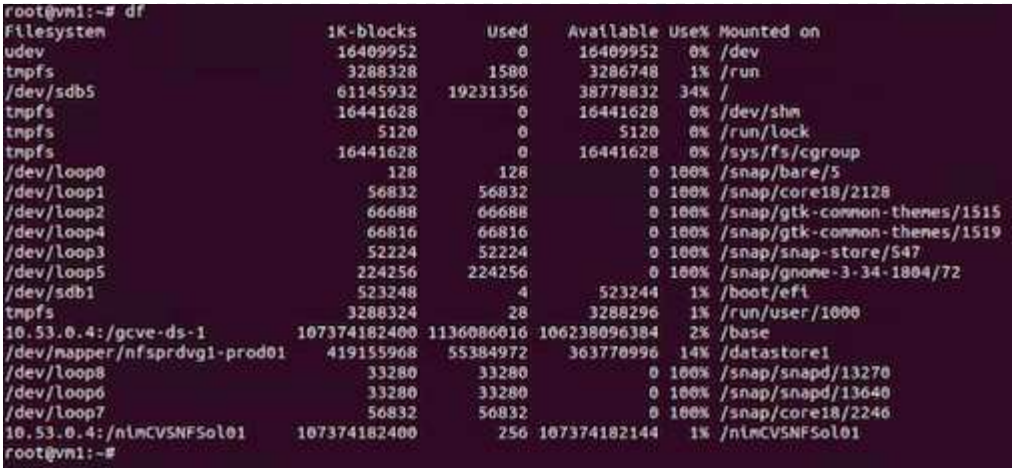
3. 在实例上创建新目录，例如 "/nimCVSNFSol01" ：

```
sudo mkdir /nimCVSNFSol01
```



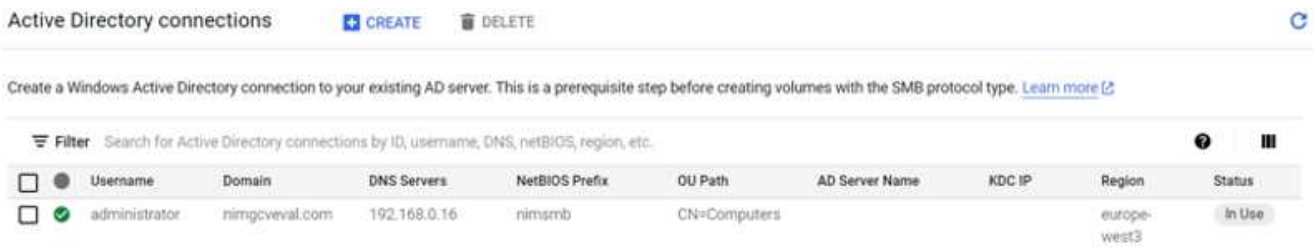
4. 使用相应的命令挂载卷。以下是实验室命令示例：

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



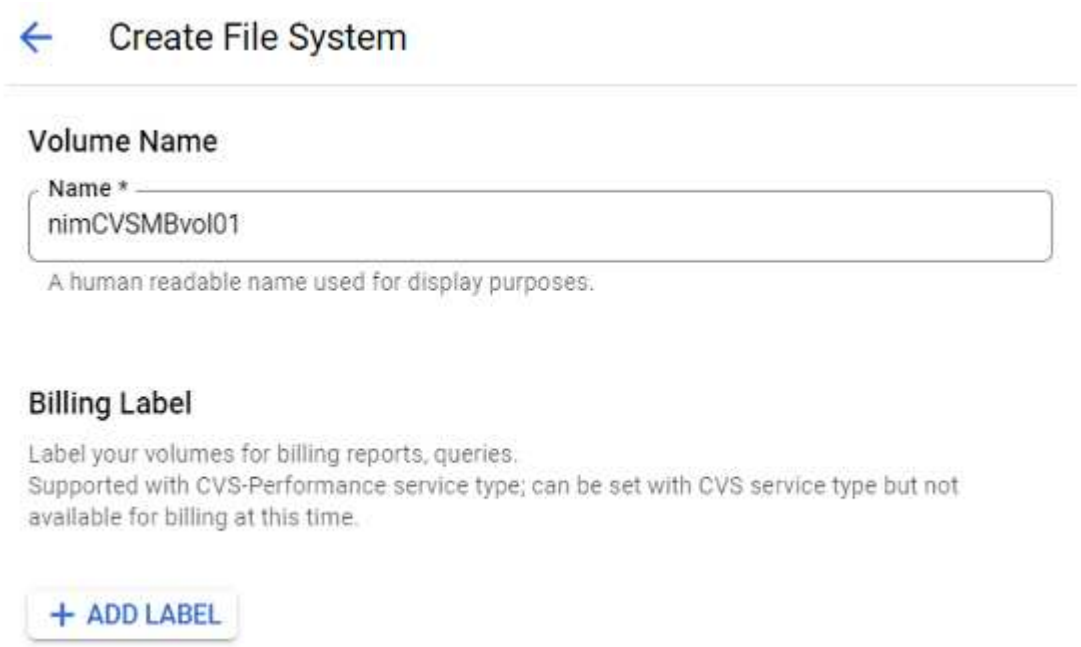
```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     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:/nlmCVSNFSol01      107374182400         256 107374182144   1% /nlmCVSNFSol01
root@vm1:~#
```

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

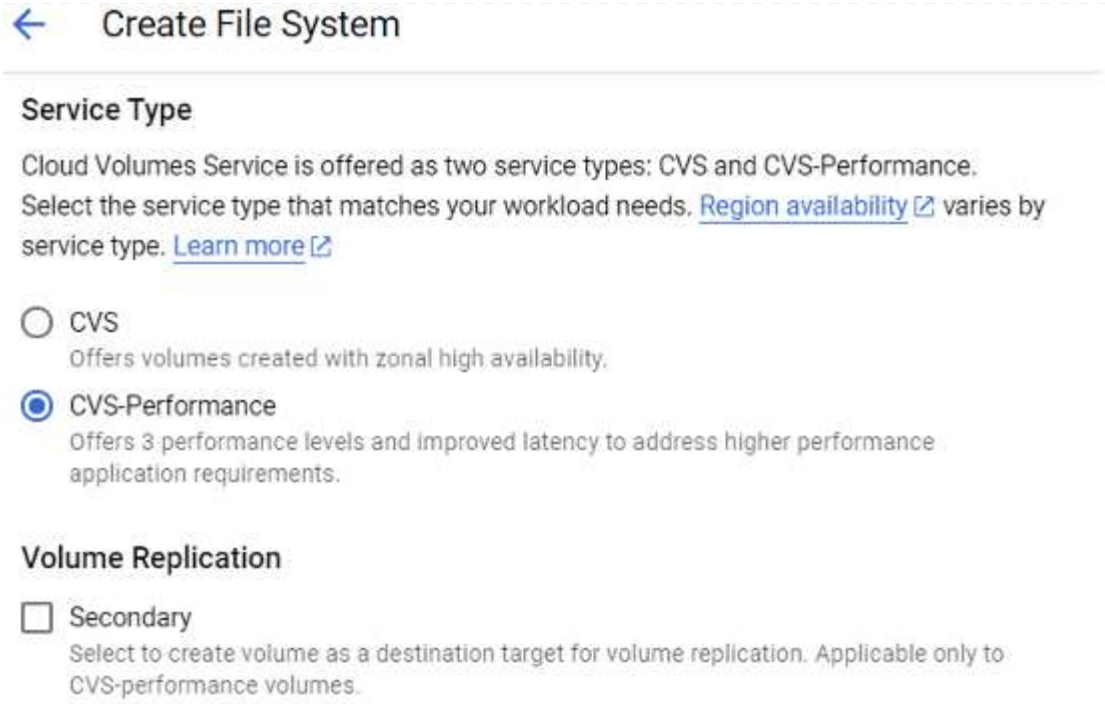


建立 AD 连接后，创建具有所需服务级别的卷。除了选择适当的协议之外，这些步骤与创建 NFS 卷类似。

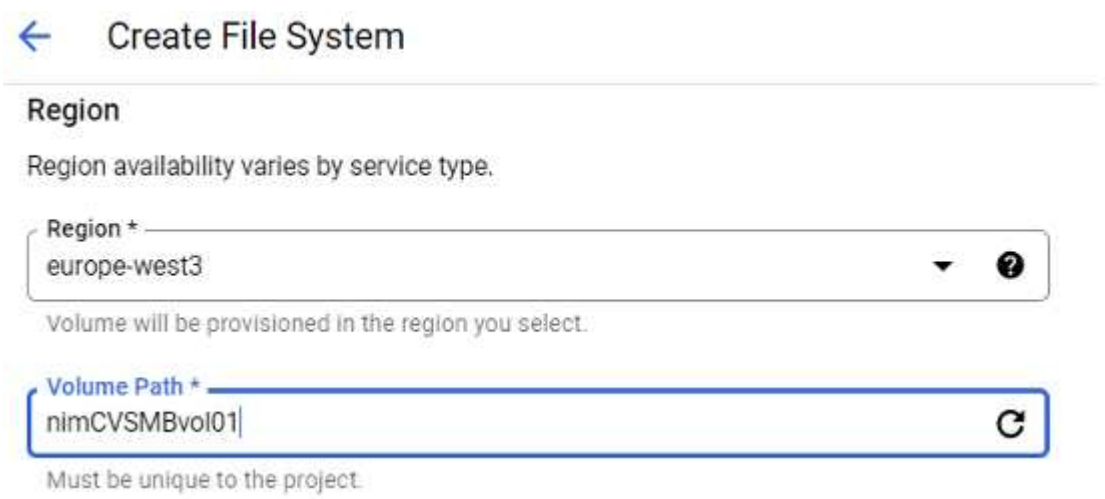
1. 在 Cloud Volumes Console 中，转到 Volumes 页面，然后单击 Create 。
2. 在创建文件系统页面上，根据成本分摊机制的需要指定卷名称和计费标签。



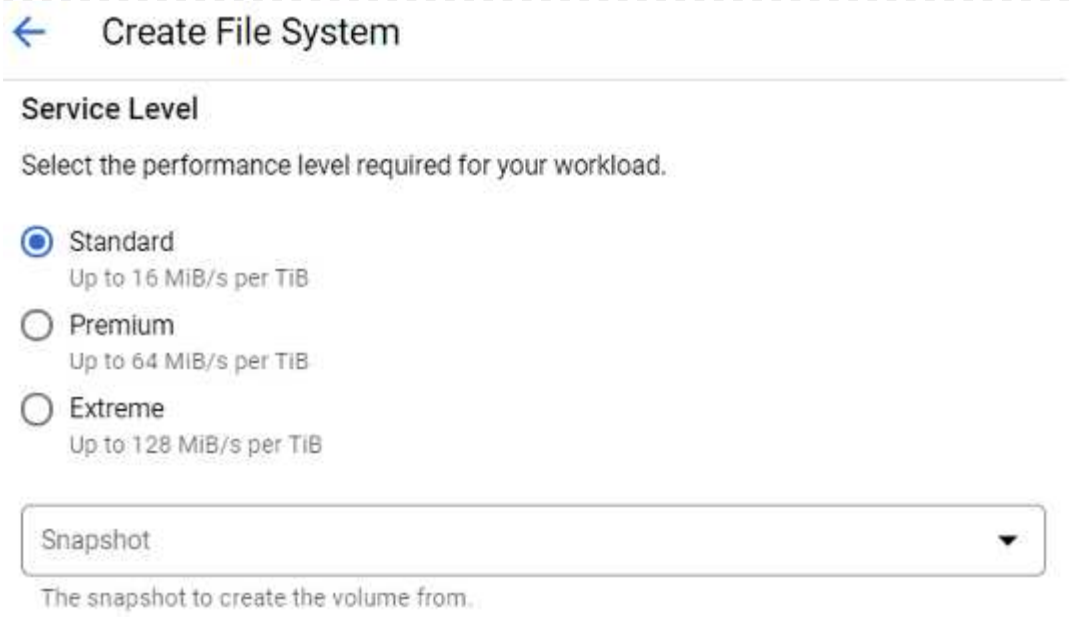
3. 选择相应的服务。对于 GCVE ，请选择 CVS-Performance 和所需的服务级别，以根据工作负载要求提高延迟和性能。



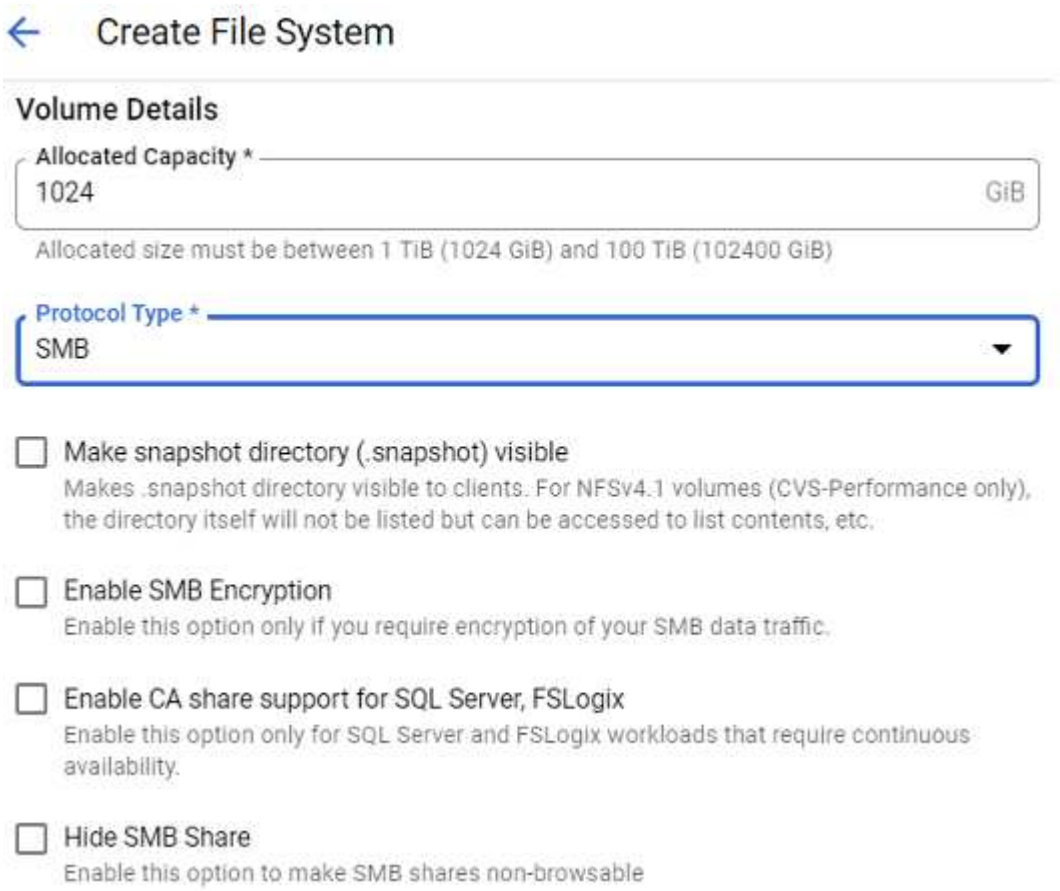
4. 为卷和卷路径指定 Google Cloud 区域（卷路径必须在项目中的所有云卷之间是唯一的）



5. 选择卷的性能级别。

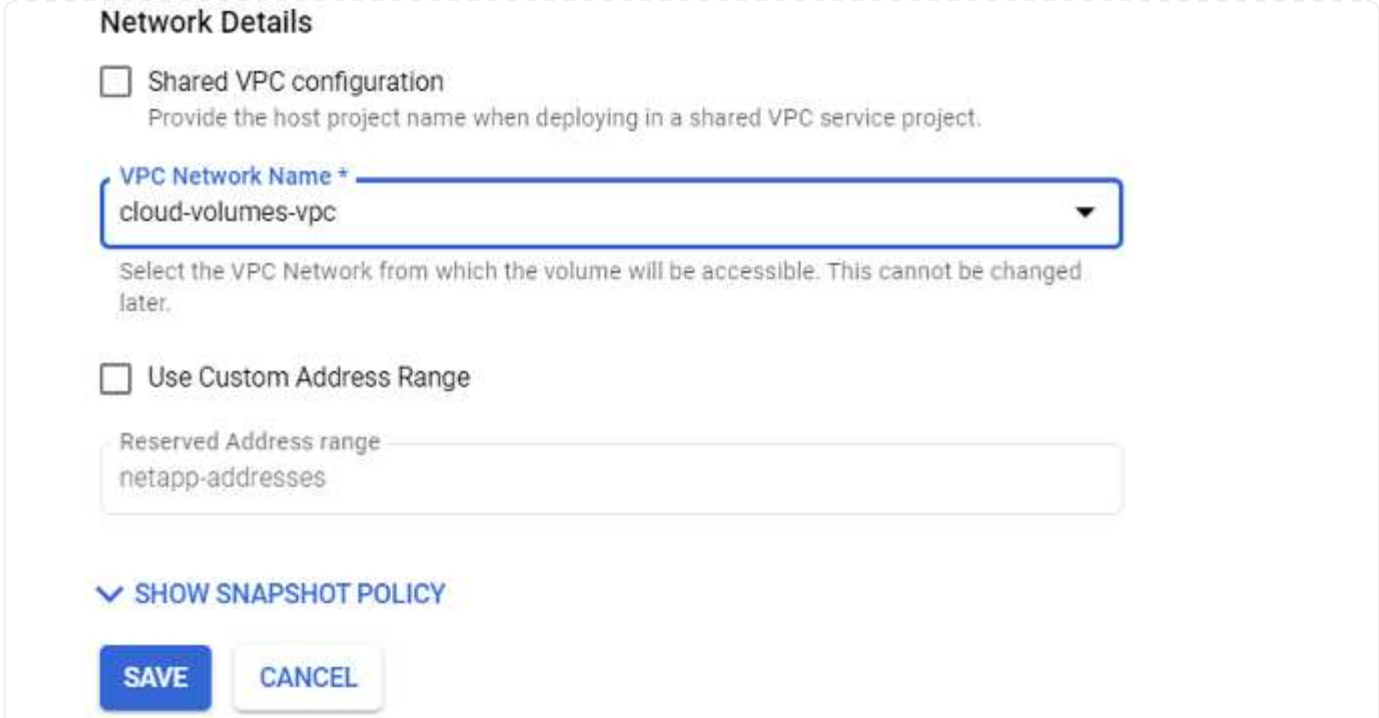


6. 指定卷的大小和协议类型。在此测试中，使用 SMB 。



7. 在此步骤中，选择可从中访问卷的 VPC 网络。确保已建立 VPC 对等关系。

   提示：如果尚未建立 VPC 对等关系，则会显示一个弹出按钮，用于指导您完成对等命令。打开 Cloud Shell 会话并执行相应的命令，将您的 VPC 与 Cloud Volumes Service 生产者建立对等关系。如果您决定事先准备 VPC 对等关系，请参见以下内容 "说明"。



8. 单击保存以创建卷。

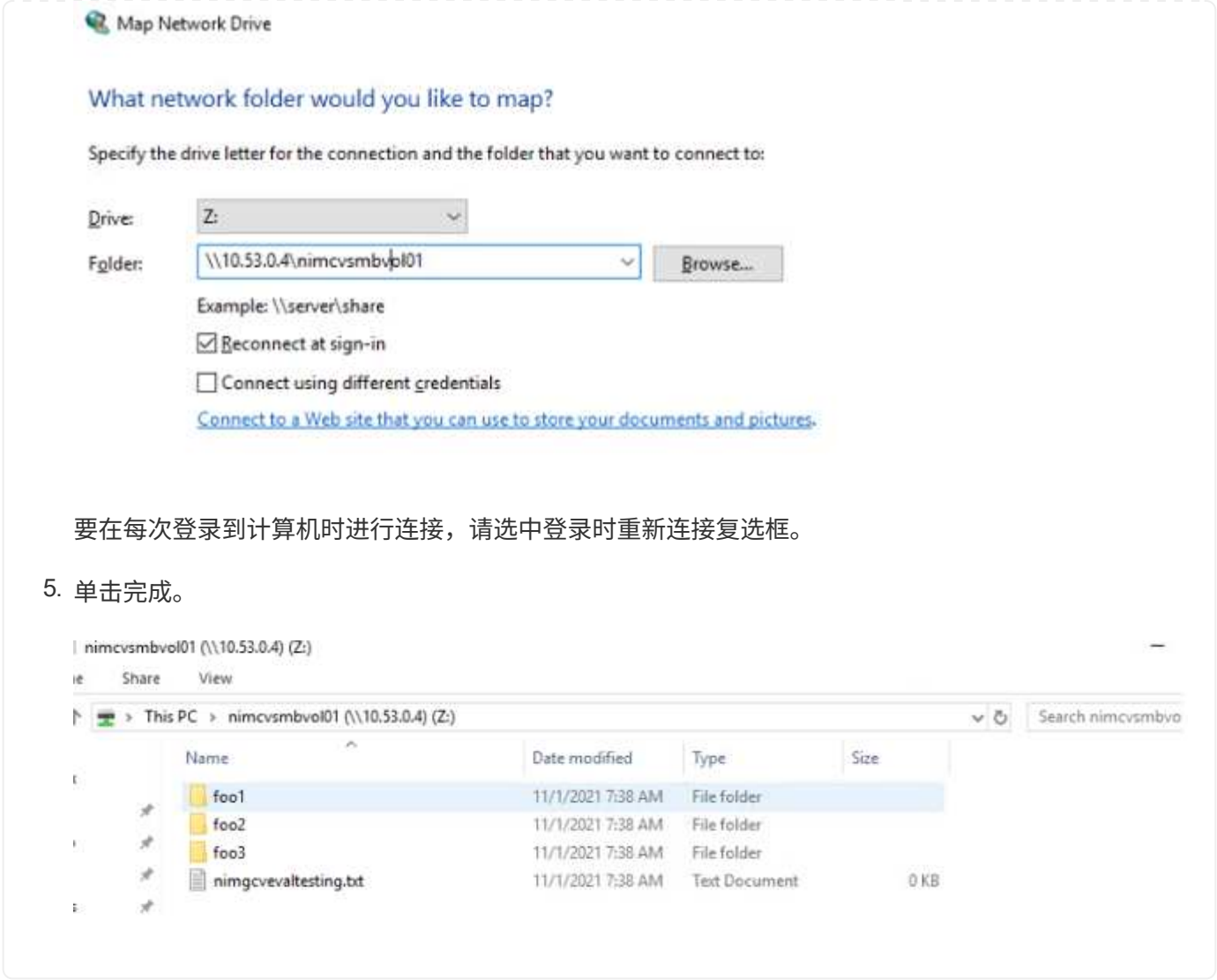
要挂载 SMB 卷，请执行以下操作：

1. 在 Cloud Console 中，转至 Cloud Volumes > Volumes 。
2. 转到卷页面
3. 单击要映射 SMB 共享的 SMB 卷。
4. 向右滚动，在显示更多下，单击挂载说明。

要从 VMware VM 的 Windows 子操作系统中执行挂载过程，请执行以下步骤：

1. 单击 "Start （开始） " 按钮，然后单击 "Computer" （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盘符。
4. 在文件夹框中，键入：

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



要在每次登录到计算机时进行连接，请选中登录时重新连接复选框。

5. 单击完成。

AWS、**Azure**和**GCP**上的补充**NFS**数据存储库的区域可用性

详细了解全球地区对AWS、Azure和Google Cloud Platform (GCP)上的补充NFS数据存储库的支持。

AWS区域可用性

AWS/VMC上的补充NFS数据存储库的可用性由Amazon定义。首先、您需要确定VMC和FSxN是否在指定区域中可用。接下来、您需要确定该区域是否支持FSxN补充NFS数据存储库。

- 检查VMC的可用性 "此处"。
- Amazon的定价指南提供了有关FSxN (FSX ONTAP)的可用位置的信息。您可以找到这些信息 "此处"。
- VMC的FSxN补充NFS数据存储库即将推出。

虽然信息仍在发布中、但下图将当前对VMC、FSxN和FSxN的支持标识为一个补充NFS数据存储库。

美洲

* AWS地区*	* VMC可用性*	* FSX ONTAP 可用性*	* NFS数据存储库可用性*
美国东部(北弗吉尼亚)	是的。	是的。	是的。
美国东部（俄亥俄州）	是的。	是的。	是的。
美国西部(北加利福尼亚)	是的。	否	否
US West （俄勒冈州）	是的。	是的。	是的。
GovCloud (美国西部)	是的。	是的。	是的。
加拿大（中部）	是的。	是的。	是的。
南美(圣保罗)	是的。	是的。	是的。

最后更新日期：2022年6月2日。

欧洲、中东和非洲

* AWS地区*	* VMC可用性*	* FSX ONTAP 可用性*	* NFS数据存储库可用性*
欧洲(爱尔兰)	是的。	是的。	是的。
欧洲(伦敦)	是的。	是的。	是的。
欧洲(法兰克福)	是的。	是的。	是的。
欧洲(巴黎)	是的。	是的。	是的。
欧洲(米兰)	是的。	是的。	是的。
欧洲（斯德哥尔摩）	是的。	是的。	是的。

最后更新日期：2022年6月2日。

亚太地区

* AWS地区*	* VMC可用性*	* FSX ONTAP 可用性*	* NFS数据存储库可用性*
Asia Pacific (Sydney)	是的。	是的。	是的。
亚太地区(东京)	是的。	是的。	是的。
亚太地区(日本、日本)	是的。	否	否
亚太地区(新加坡)	是的。	是的。	是的。
亚太地区(首尔)	是的。	是的。	是的。
亚太地区(孟买)	是的。	是的。	是的。
亚太地区(雅加达)	否	否	否
亚太地区(香港)	是的。	是的。	是的。

最后更新日期：2022年9月28日。

Azure区域可用性

Azure / AVS上的补充NFS数据存储库的可用性由Microsoft定义。首先、您需要确定AVS和ANF是否在特定区域可用。接下来、您需要确定该区域是否支持ANF补充NFS数据存储库。

- 检查AVS和ANF的可用性 "此处"。
- 检查ANF补充NFS数据存储库的可用性 "此处"。

GCP地区可用性

当GCP进入公有 可用性状态时、将发布GCP区域可用性。

总结和结论：为什么要将**NetApp**混合多云与**VMware**结合使用

NetApp Cloud Volumes 以及适用于主要超大规模企业的 VMware 解决方案为希望利用混合云的企业提供了巨大的潜力。本节其余部分将介绍有关集成NetApp Cloud Volumes以实现真正的混合多云功能的使用情形。

用例 **1** ： 优化存储

在使用 RVtools 输出执行规模估算练习时，显而易见，功率（ vCPU/vMem ）与存储是并行的。企业往往会发现自己处于存储空间所需的驱动器大小远远超出所需的容量的情况。

通过集成 NetApp Cloud Volumes ，企业可以通过简单的迁移方法实现基于 vSphere 的 Cloud 解决方案，无需重新整合，无需 IP 更改，也无需架构更改。此外，通过这种优化，您可以扩展存储占用空间，同时将主机数量保持在 vSphere 所需的最低水平，但不会更改可用的存储层次结构，安全性或文件。这样，您可以优化部署并将总 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

企业面临着将应用程序从内部数据中心迁移到公有云的压力，原因有多种：即将到期的租约；从资本支出（ capex ）支出迁移到运营支出（ opex ）支出的财务指令；或者只是自上而下的要求，将所有内容迁移到云。

速度至关重要时，只有简化的迁移方法才可行，因为要适应云的特定 IaaS 平台，重新整合和重构应用程序的速度缓慢且成本高昂，通常需要数月时间。将 NetApp Cloud Volumes 与为子系统连接的存储（包括 RDM 以及应用程序一致的 Snapshot 副本和 HCX ）提供的高效带宽 SnapMirror 复制相结合，从而实现云特定的迁移（例如 Azure Migrate ）或用于复制 VM 的第三方产品），这种过渡比依赖耗时的 I/O 筛选器机制更容易。

用例 **3** ： 数据中心扩展

当数据中心因季节性需求峰值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 是一项轻松的解决方案。利用 NetApp Cloud Volumes ，可以跨可用性区域提供高可用性并提供动态扩展功能，从而轻松创建，复制和扩展存储。利用 NetApp Cloud Volumes 可以消除对延伸型集群的需求，从而最大限度地减少主机集群容量。

用例 **4** ： 灾难恢复到云

在传统方法中，如果发生灾难，则复制到云的 VM 需要先转换到云自己的虚拟机管理程序平台，然后才能还原，而不是在危机期间处理的任务。

通过使用内部 SnapCenter 和 SnapMirror 复制以及公有云虚拟化解决方案将 NetApp Cloud Volumes 用于子系统连接的存储，可以设计一种更好的灾难恢复方法，以便在完全一致的 VMware SDDC 基础架构上恢复 VM 副

本以及云专用恢复工具（例如 Azure Site Recovery ）或 Veeam 等第三方工具。此外，您还可以通过此方法快速执行灾难恢复演练并从勒索软件中恢复。这样，您还可以通过按需添加主机来扩展到完全生产环境，以供测试或在灾难期间使用。

用例 **5** ： 应用程序现代化

应用程序进入公有云后，企业将希望利用数百种功能强大的云服务来实现现代化和扩展。借助 NetApp Cloud Volumes ，现代化过程非常简单，因为应用程序数据不会锁定在 vSAN 中，并允许数据在包括 Kubernetes 在内的各种用例中移动。

结论

无论您是以全云还是混合云为目标， NetApp Cloud Volumes 都可以提供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，同时通过将数据需求无缝地迁移到应用程序层来降低 TCO 。

无论使用何种情形，都可以选择您最喜欢的云 / 超大规模云提供商以及 NetApp Cloud Volumes ，快速实现云优势，跨内部和多个云实现一致的基础架构和运营，工作负载的双向可移植性以及企业级容量和性能。

这是用于连接存储的熟悉过程。请记住，这只是数据位置随新名称而变化；工具和流程都保持不变， NetApp Cloud Volumes 有助于优化整体部署。

VMware Hybrid Cloud 用例

采用**VMware**的**NetApp**混合多云的用例

概述在规划混合云或云优先部署时对 IT 组织至关重要的使用情形。

常见使用情形

使用情形包括：

- 灾难恢复，
- 在数据中心维护期间托管工作负载， * 快速激增，需要额外的资源，但不能满足本地数据中心的配置要求。
- VMware 站点扩展，
- 快速迁移到云，
- 开发 / 测试，和
- 利用云补充技术实现应用程序现代化。

在本文档中、我们将使用VMware用例详细介绍云工作负载参考。这些用例包括：

- 保护(包括灾难恢复和备份/还原)
- 迁移
- 扩展

IT 发展历程中的一个过程

大多数企业都在经历转型和现代化之旅。在这一过程中，各家公司正在尝试利用现有的 VMware 投资，同时利用云优势并探索尽可能无缝地迁移过程的方法。这种方法将使他们的现代化工作变得非常简单，因为数据已经在

云中。

在这种情况下，最简单的问题解答是每个超大规模提供商中的 VMware 产品。与 NetApp ® Cloud Volumes 一样， VMware 提供了一种将内部 VMware 环境迁移或扩展到任何云的方法，使您可以在云中本机运行工作负载的同时保留现有内部资产，技能和工具。这样可以降低风险，因为不会发生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在内部执行操作。这样可以加快云迁移速度、并更平稳地过渡到混合多云架构。

了解补充**NFS**存储选项的重要性

尽管VMware在任何云中都能为每个客户提供独特的混合功能、但有限的补充NFS存储选项限制了它对存储负载繁重的组织的有用性。由于存储与主机直接相关，因此扩展存储的唯一方法是添加更多主机，这样对于存储密集型工作负载，成本可能会增加 35% – 40% 或更多。这些工作负载只需要额外的存储，而不是额外的功率。但这意味着需要为额外的主机付费。

我们来考虑一下这种情况：

客户只需要五台主机来满足 CPU 和内存需求，但需要大量存储需求，并需要 12 台主机来满足存储需求。这一要求最终确实会让财务规模大得多，因为他们只需要增加存储即可购买额外的动力。

在规划云采用和迁移时，始终需要评估最佳方法并采取最简单的方法来减少总投资。对于任何应用程序迁移，最常见且最简单的方法是重新托管（也称为提升和移动），在这种情况下不会进行虚拟机（ VM ）或数据转换。在将 NetApp Cloud Volumes 与 VMware 软件定义的数据中心（ SDDC ）结合使用的同时，还可以作为 vSAN 的补充，从而提供一个轻松的升降和移动选项。

适用于 **Amazon VMware Managed Cloud** （ **VMC** ）的 **NetApp** 解决方案

详细了解NetApp为AWS提供的解决方案。

VMware将云工作负载定义为以下三个类别之一：

- 保护(包括灾难恢复和备份/还原)
- 迁移
- 扩展

在以下各节中浏览可用的解决方案。

保护

- "在AWS上使用VMC进行灾难恢复(已连接子系统)"
- "使用FSx for ONTAP 在VMC中执行Veeam备份和还原()"
- "使用适用于ONTAP 和VMC的FSX进行灾难恢复(DRO)"
- "使用Veeam Replication和FSx for ONTAP将灾难恢复到AWS上的VMware Cloud"

迁移

- "使用VMware HCX将工作负载迁移到FSxN数据存储库"

扩展

即将推出！！

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

详细了解NetApp为Azure提供的解决方案。

VMware将云工作负载定义为以下三个类别之一：

- 保护(包括灾难恢复和备份/还原)
- 迁移
- 扩展

在以下各节中浏览可用的解决方案。

保护

- "使用ANF和Jetstream (补充NFS数据存储库)进行灾难恢复"
- "使用ANF和CVO (子系统连接存储)进行灾难恢复"
- "借助ANF和AVS实现灾难恢复(Disaster Recovery、DRO)"
- "使用Veeam复制和Azure NetApp Files数据存储库将灾难恢复到Azure VMware解决方案"

迁移

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

扩展

即将推出！！

适用于**Google Cloud**的**NetApp**解决方案**VMware**引擎**(GCVe)**

详细了解NetApp为GCP提供的解决方案。

VMware将云工作负载定义为以下三个类别之一：

- 保护(包括灾难恢复和备份/还原)
- 迁移
- 扩展

在以下各节中浏览可用的解决方案。

保护

- "使用SnapCenter 、Cloud Volumes ONTAP 和Veeam复制实现应用程序灾难恢复"
- "通过NetApp SnapCenter和Veeam复制到GCVE上的NetApp CVS实现应用程序一致的灾难恢复"

迁移

- "使用VMware HCX将工作负载迁移到NetApp Cloud Volume Service NFS数据存储库"
- "使用Veeam将VM复制到NetApp云卷服务NFS数据存储库"

扩展

即将推出！！

适用于 **AWS VMC** 的 **NetApp** 功能

详细了解NetApp为AWS VMware Cloud (VMC)提供的功能—从作为子系统连接存储设备或补充NFS数据存储库的NetApp到迁移工作流、扩展/突发到云、备份/还原和灾难恢复。

从以下选项中选择，跳至所需内容部分：

- "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**

与内部部署一样，规划基于云的虚拟化环境对于成功创建 VM 和迁移生产就绪环境至关重要。

本节介绍如何在 AWS SDDC 上设置和管理 VMware Cloud ，并将其与连接 NetApp 存储的可用选项结合使用。

只支持使用来宾存储将Cloud Volumes ONTAP 连接到AWS VMC。

设置过程可细分为以下步骤：

- 部署和配置适用于AWS的VMware Cloud
- 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存储可以通过多种方式在AWS VMC中用作guess connected或作为补充NFS数据存储库。

请访问 "支持的 NetApp 存储选项" 有关详细信息 …

AWS 支持以下配置中的 NetApp 存储：

- FSX ONTAP 作为子系统连接的存储
- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- FSX ONTAP 作为补充NFS数据存储库

查看详细信息 "VMC的子系统连接存储选项"。查看详细信息 "VMC的补充NFS数据存储库选项"。

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部署在 AWS VMC 中。为VMware定义的每个云区域定义了使用情形：

- 保护(包括灾难恢复和备份/还原)
- 扩展
- 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：《在**Amazon Web Services**和**Guest Connect**上使用**VMware Cloud**进行灾难恢复》

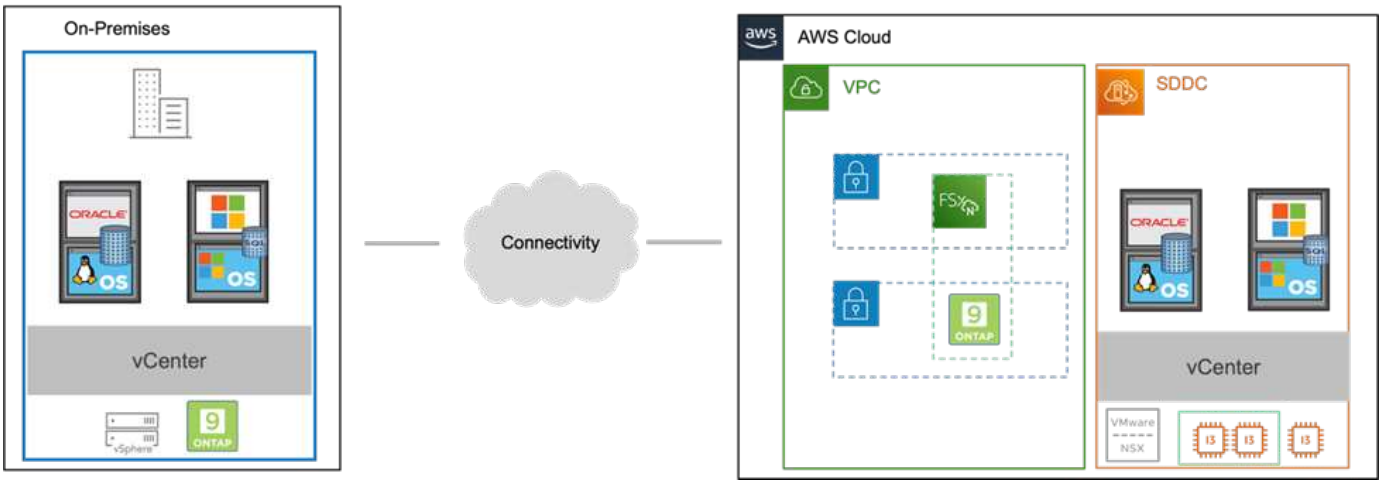
作者：Chris Reno、Josh Powell和Suresh ThopPay—NetApp解决方案工程部

概述

对于确保在发生重大中断时快速恢复业务关键型应用程序的企业来说、成熟可靠的灾难恢复(Disaster Recovery、DR)环境和计划至关重要。本解决方案 重点展示灾难恢复使用情形、重点介绍内部部署和AWS上的VMware云中的VMware和NetApp技术。

NetApp与VMware集成的历史很长、成千上万的客户选择NetApp作为其虚拟化环境的存储合作伙伴就证明了这一点。这种集成将继续与云中的子系统连接选项进行、并在近期与NFS数据存储库进行集成。本解决方案 重点介绍通常称为子系统连接存储的使用情形。

在子系统连接的存储中、子系统VMDK部署在VMware配置的数据存储库上、应用程序数据存储在iSCSI或NFS上并直接映射到虚拟机。Oracle和MS SQL应用程序用于演示灾难恢复场景、如下图所示。



假设、前提条件和组件概述

在部署此解决方案 之前、请查看组件概述、部署解决方案 所需的前提条件以及在记录此解决方案 时所做的假设。

"DR解决方案 要求、要求和规划"

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、可在内部AFF 和FSX ONTAP 集群之间提供高速数据复制。此外、Veeam Backup & Replication还为我们的虚拟机提供备份和还原功能。

在本节中、我们将介绍用于备份和还原的SnapCenter 、SnapMirror和Veeam的配置。

以下各节介绍了在二级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(主存储系统>镜像)和二级存储系统(主存储系统>存储)中的SnapMirror关系、以便进行长期归档和保留。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。

源和目标ONTAP 系统必须位于使用Amazon VPC对等、传输网关、AWS Direct Connect或AWS VPN建立对等关系的网络中。

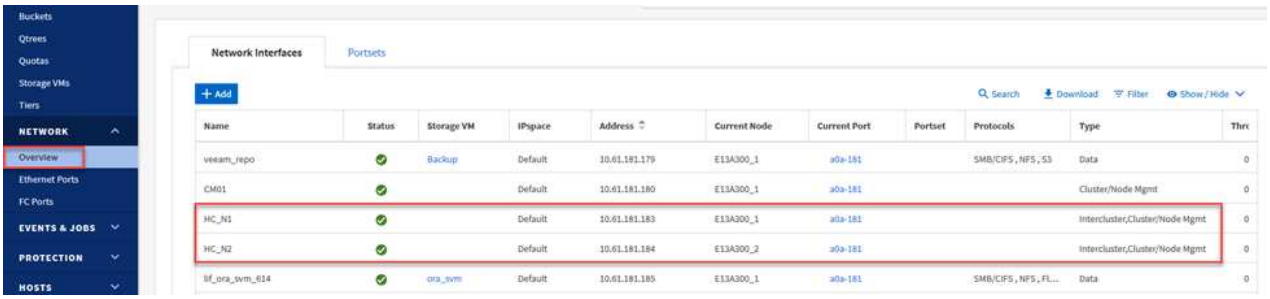
要在内部ONTAP 系统和FSX ONTAP 之间设置SnapMirror关系、需要执行以下步骤：

> 请参见 "适用于ONTAP 的FSx—ONTAP 用户指南" 有关使用FSX创建SnapMirror关系的详细信息、请参见。

记录源和目标集群间逻辑接口

对于驻留在内部的源ONTAP 系统、您可以从System Manager或命令行界面检索集群间LIF信息。

1. 在ONTAP 系统管理器中、导航到"网络概述"页面、然后检索类型为"集群间"的IP地址、这些IP地址配置为与安装了FSX的AWS VPC进行通信。



2. 要检索FSX的集群间IP地址、请登录到命令行界面并运行以下命令：

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

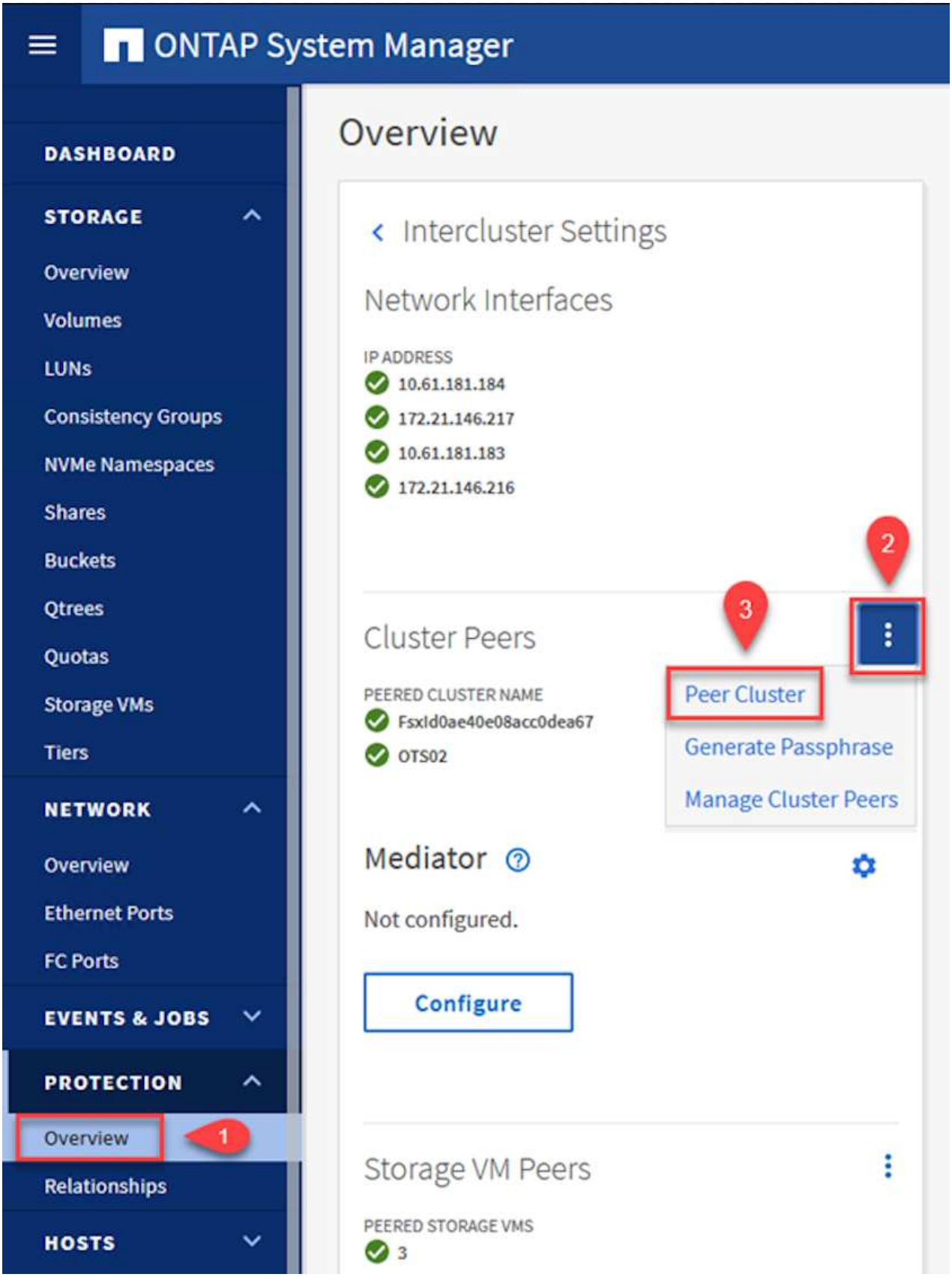
```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
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.
```

要在ONTAP 集群之间建立集群对等关系、必须在另一对等集群中确认在发起ONTAP 集群上输入的唯一密码短语。

1. 使用`cluster peer create`命令在目标FSX集群上设置对等关系。出现提示时、输入一个唯一的密码短语、稍后在源集群上使用该密码短语以完成创建过程。

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

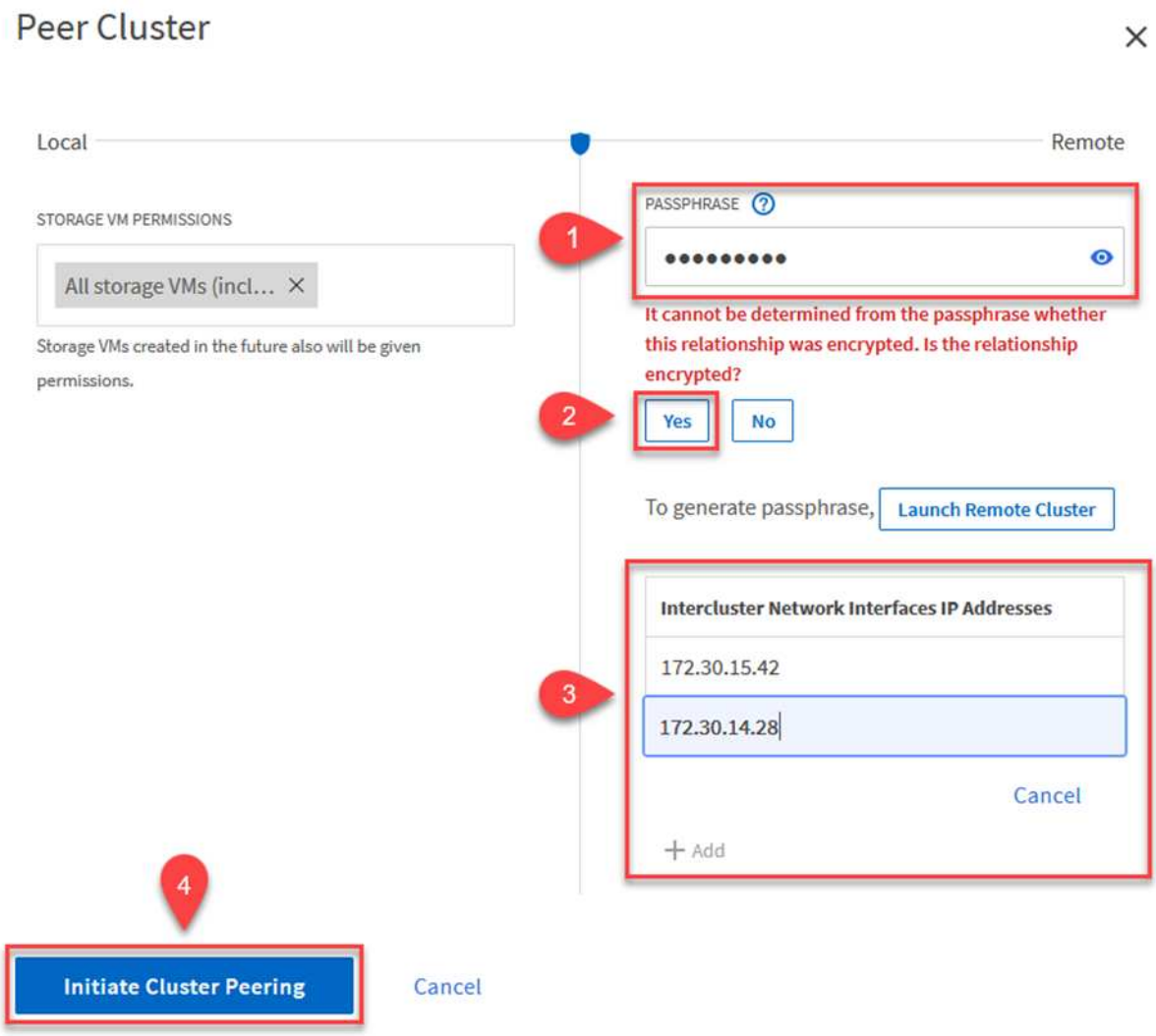
2. 在源集群上、您可以使用ONTAP 系统管理器或命令行界面建立集群对等关系。在ONTAP 系统管理器中、导航到"保护">"概述"、然后选择"对等集群"。



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短语。
   b. 选择`是`以建立加密关系。

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此过程。



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
```

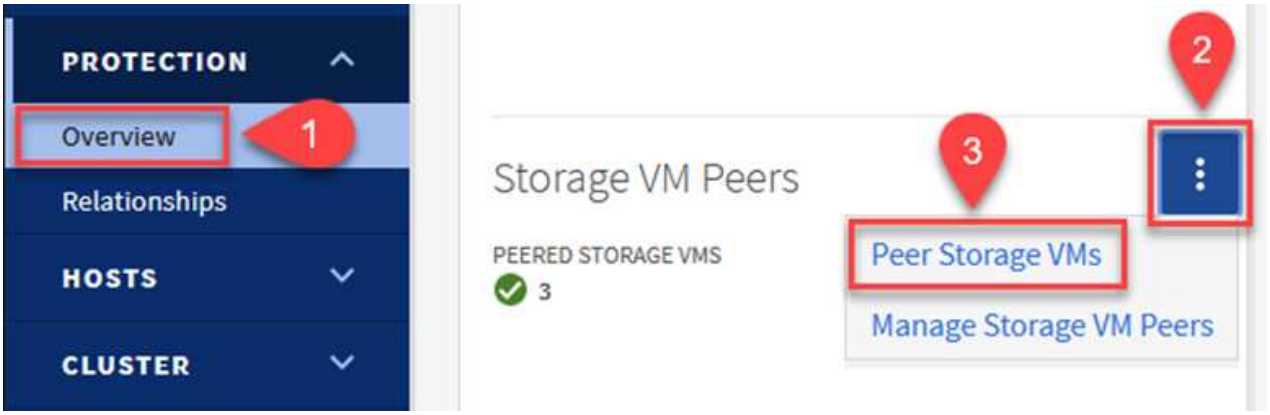
```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

下一步是在目标和源Storage Virtual Machine之间设置SVM关系、这些虚拟机包含将处于SnapMirror关系中的卷。

1. 在源FSX集群中、从CLI使用以下命令创建SVM对等关系：

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

2. 在源ONTAP 集群中、接受与ONTAP 系统管理器或命令行界面的对等关系。
3. 在ONTAP 系统管理器中、转到"保护">"概述"、然后在"Storage VM对等方"下选择"对等Storage VM"。



4. 在对等Storage VM的对话框中、填写必填字段：
   - 源Storage VM
   - 目标集群
   - 目标Storage VM

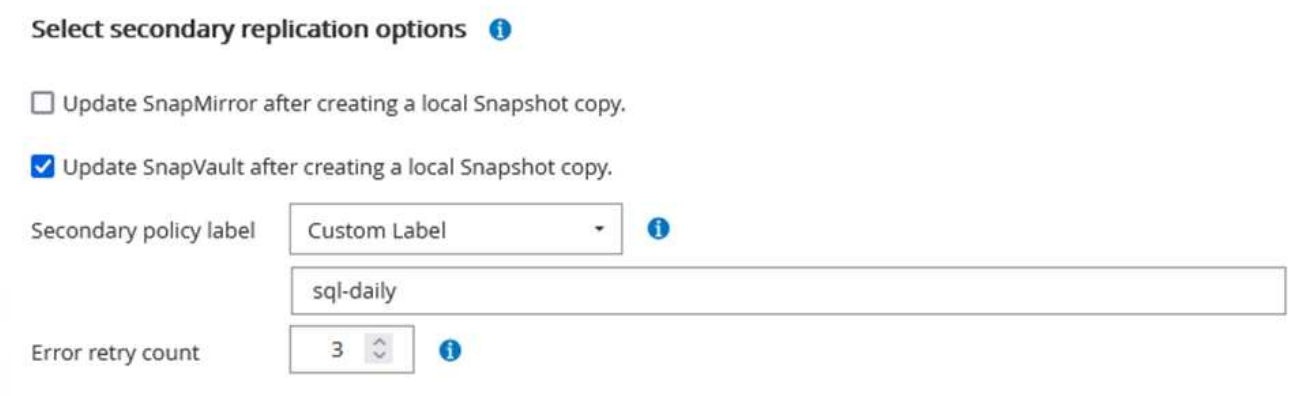
5. 单击对等Storage VM以完成SVM对等过程。

SnapCenter 管理主存储系统上作为Snapshot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 不会管理二级存储系统上保留的备份的保留策略。这些策略通过在二级FSX集群上创建的SnapMirror策略单独管理、并与与与源卷具有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二级策略标签、该标签将添加到创建SnapCenter 备份时生成的每个快照的SnapMirror标签中。

在二级存储上、这些标签与与与目标卷关联的策略规则匹配、以便强制保留快照。

以下示例显示了一个SnapMirror标签、该标签位于作为SQL Server数据库和日志卷每日备份策略一部分生成的所有快照上。



有关为SQL Server数据库创建SnapCenter 策略的详细信息、请参见 "SnapCenter 文档"。

您必须先创建一个SnapMirror策略、其中包含指定要保留的Snapshot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. 向策略添加SnapMirror标签与SnapCenter 策略中指定的二级策略标签匹配的规则。

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

以下脚本提供了可添加到策略中的规则示例：

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

为每个SnapMirror标签以及要保留的快照数量(保留期限)创建其他规则。

创建目标卷

要在FSX上创建一个目标卷、使其成为源卷中Snapshot副本的收件人、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。此过程将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
```

在内部部署和配置**Windows SnapCenter** 服务器。

在内部部署**Windows SnapCenter** 服务器

此解决方案 使用NetApp SnapCenter 为SQL Server和Oracle数据库创建应用程序一致的备份。与用于备份虚拟机VMDK的Veeam备份和复制相结合、可为内部和基于云的数据中心提供全面的灾难恢复解决方案。

SnapCenter 软件可从NetApp支持站点获得、并可安装在位于域或工作组中的Microsoft Windows系统上。有关详细的规划指南和安装说明、请参见 "NetApp文档中心"。

SnapCenter 软件可从获取 "此链接。"。

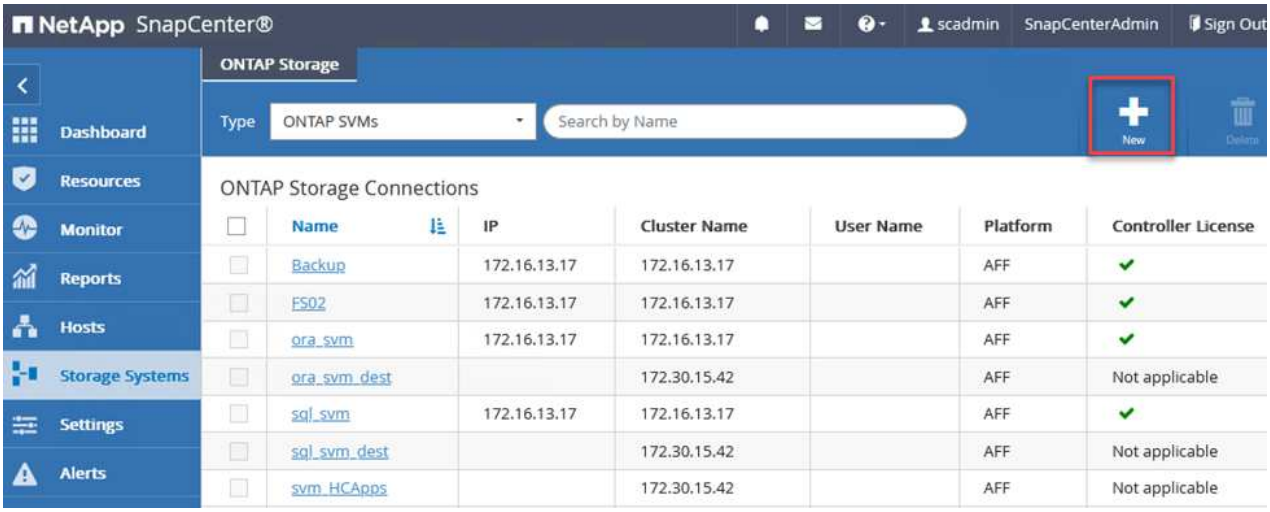
安装后、您可以使用 {\https://Virtual_Cluster_IP_or_FQDN:8146_} 从Web浏览器访问SnapCenter 控制台。

登录到控制台后、必须为备份SQL Server和Oracle数据库配置SnapCenter。

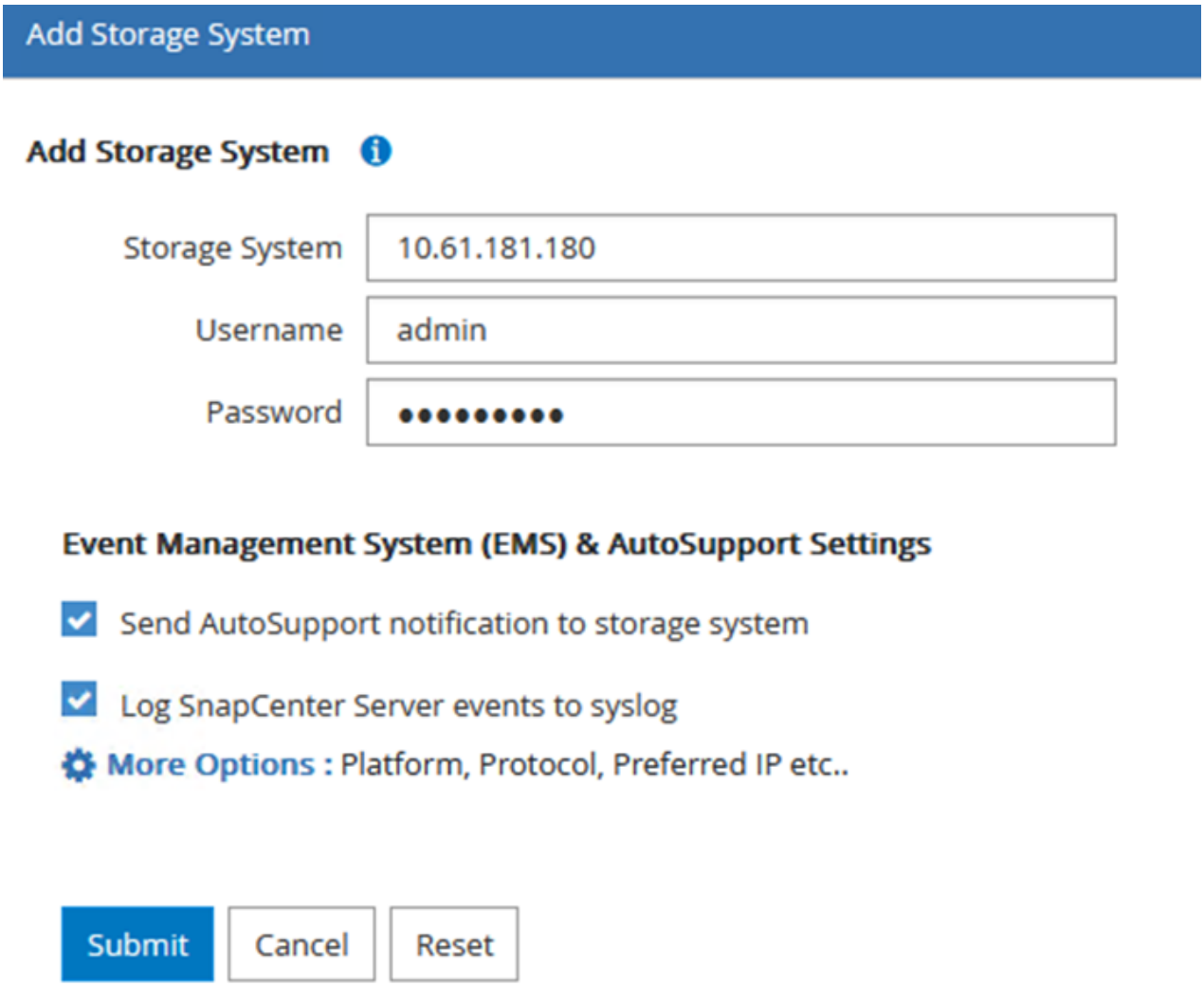
将存储控制器添加到**SnapCenter**

要将存储控制器添加到SnapCenter 、请完成以下步骤：

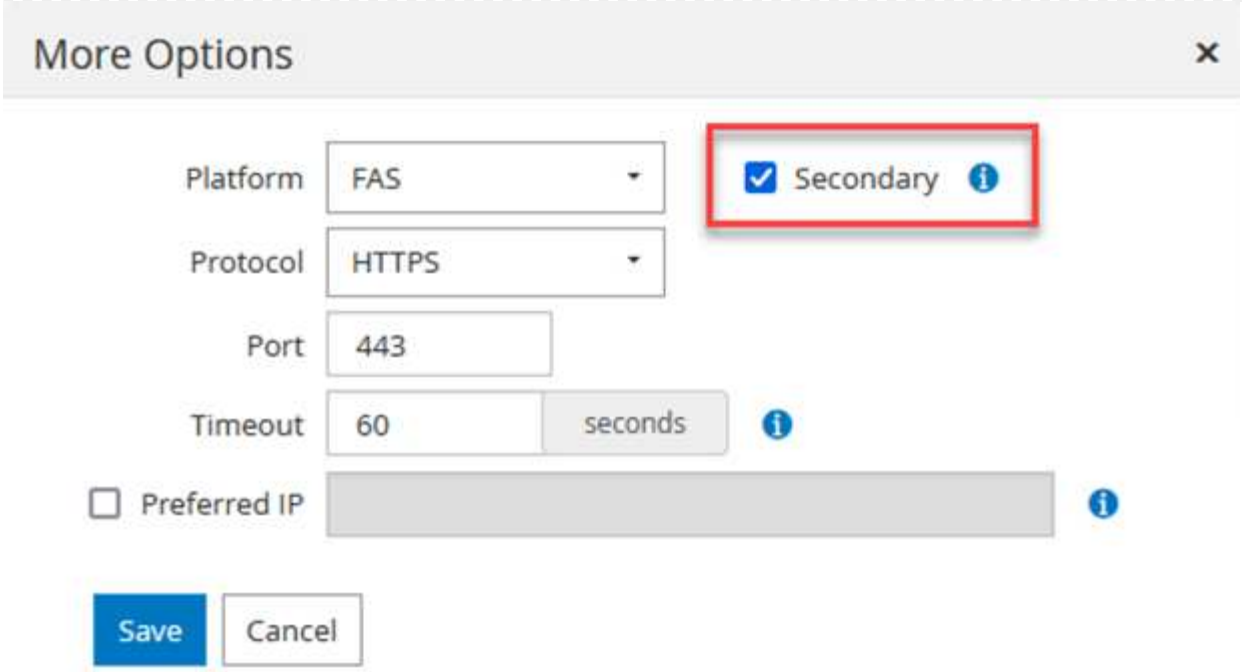
1. 从左侧菜单中、选择存储系统、然后单击新建开始将存储控制器添加到SnapCenter 的过程。



2. 在添加存储系统对话框中、添加本地内部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。



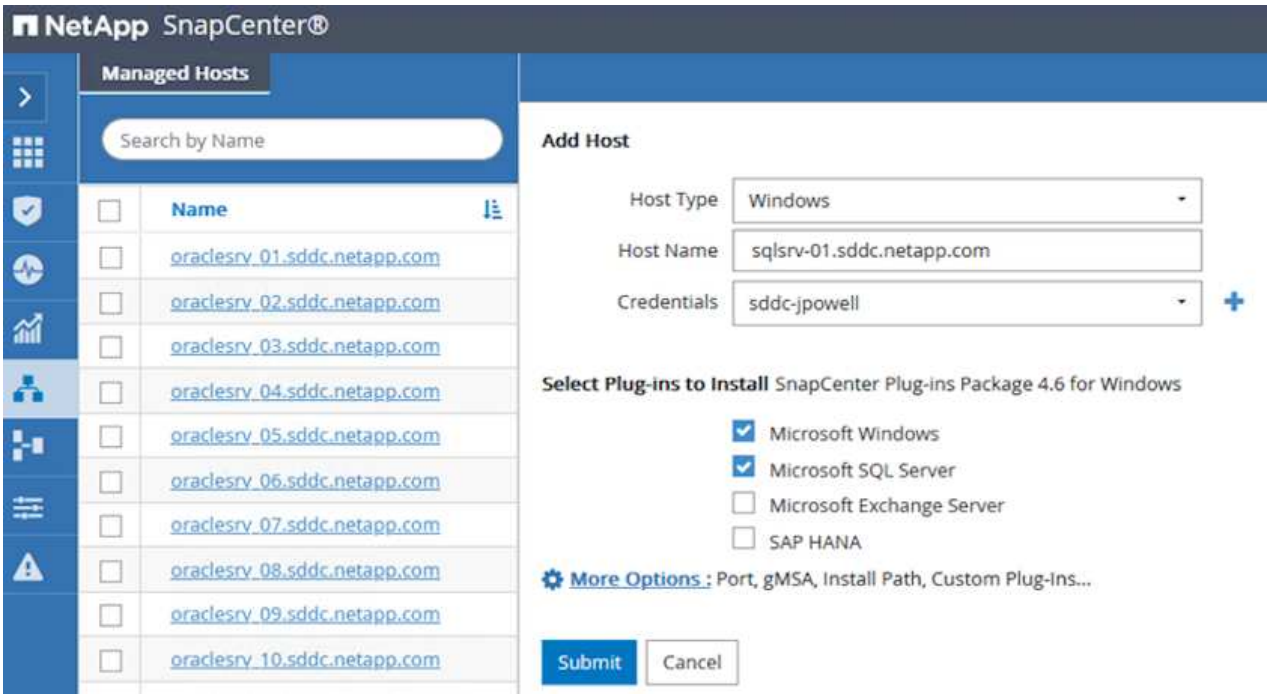
3. 重复此过程将FSX ONTAP 系统添加到SnapCenter。在这种情况下、请选择添加存储系统窗口底部的更多选项、然后单击二级复选框、将FSX系统指定为使用SnapMirror副本或主备份快照更新的二级存储系统。



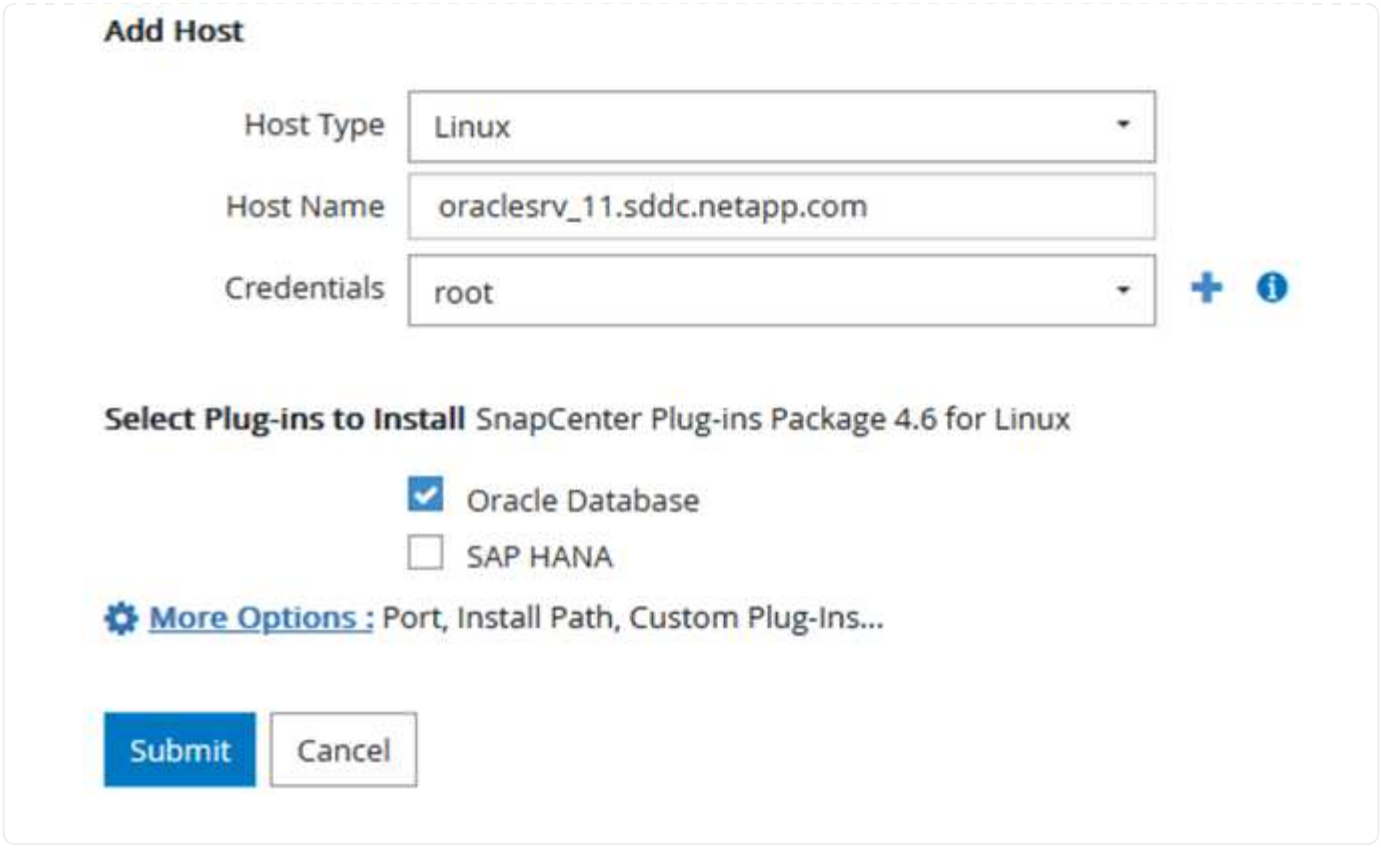
有关向SnapCenter 添加存储系统的详细信息、请参见中的文档 "此链接。"。

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

1. 从左侧菜单中、选择主机、然后单击添加开始向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。

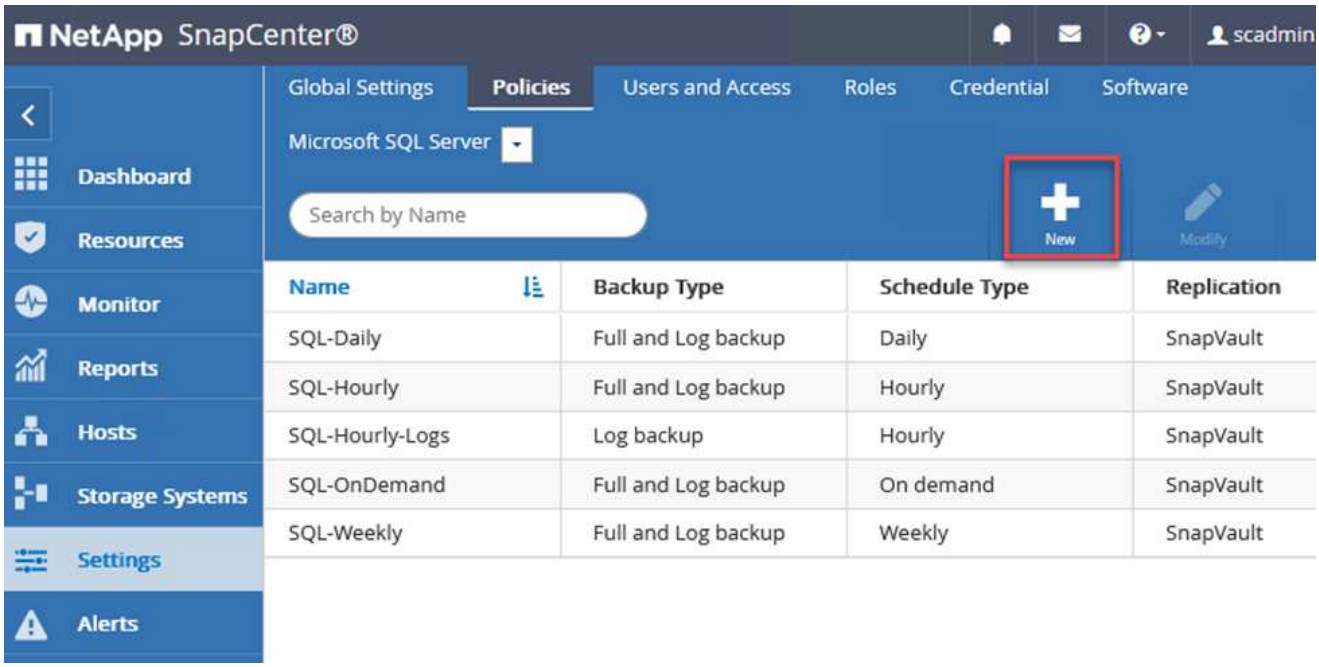


3. 对于Oracle、请在添加主机对话框中填写必填字段、然后选中Oracle数据库插件对应的复选框。然后、单击提交开始发现过程、并将主机添加到SnapCenter。


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

策略用于建立备份作业要遵循的特定规则。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。

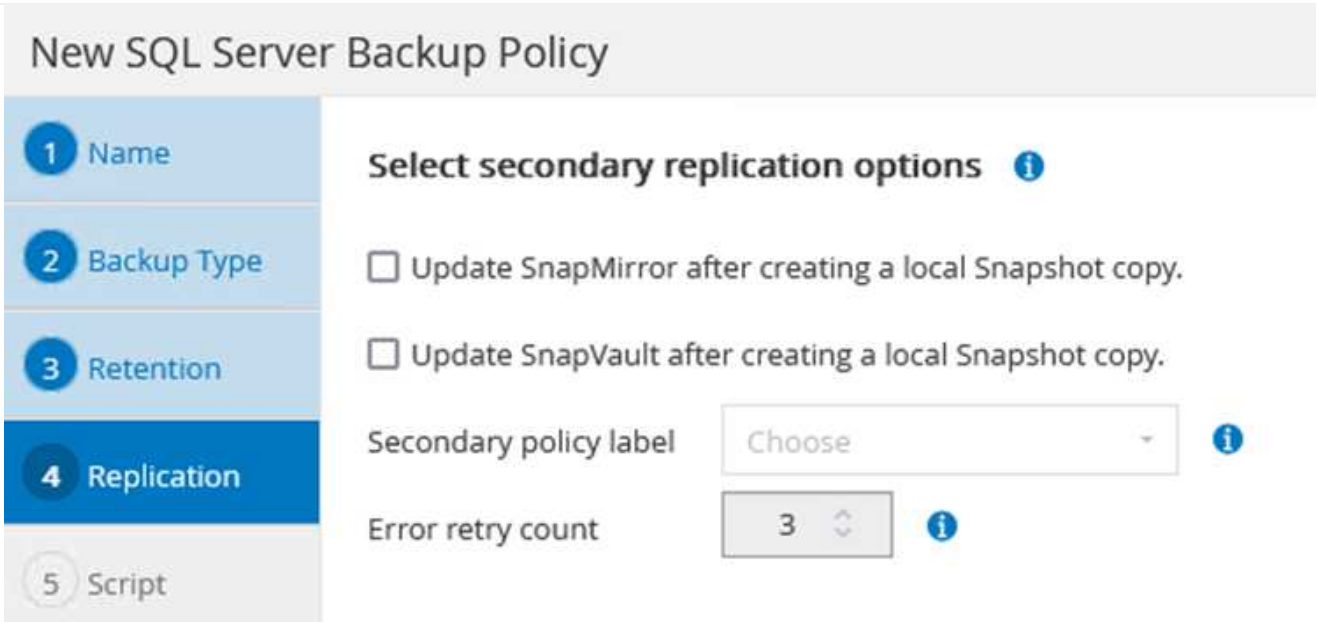


有关为SQL Server备份创建策略的完整信息、请参见 "SnapCenter 文档"。

有关为Oracle备份创建策略的完整信息、请参见 "SnapCenter 文档"。

- 注： *
- 在执行策略创建向导期间、请特别注意"复制"部分。在本节中、您将指定要在备份过程中创建的二级SnapMirror副本的类型。
- "创建本地Snapshot副本后更新SnapMirror"设置是指在同一集群中的两个Storage Virtual Machine之间存在SnapMirror关系时更新此关系。
- "创建本地快照副本后更新Snapmirror "设置用于更新两个独立集群之间以及内部ONTAP 系统与Cloud Volumes ONTAP 或FSxN之间的SnapVault 关系。

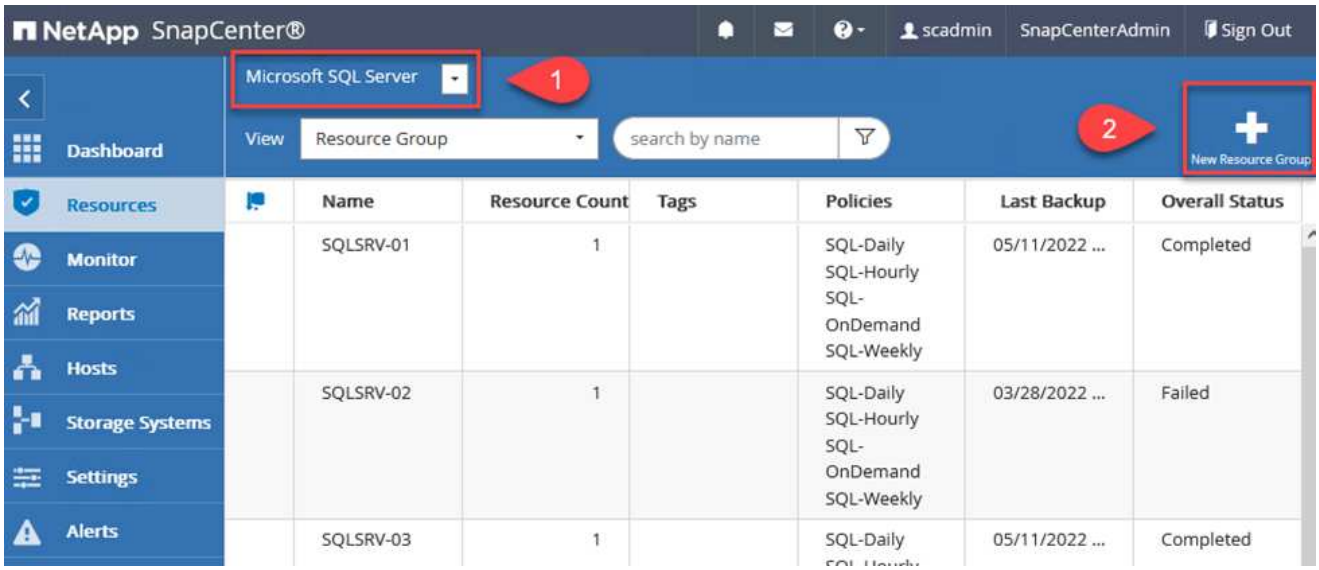
下图显示了上述选项及其在备份策略向导中的显示方式。



创建**SnapCenter** 资源组

通过资源组、您可以选择要包含在备份中的数据库资源以及这些资源所遵循的策略。

1. 转到左侧菜单中的"Resources"部分。
2. 在窗口顶部、选择要使用的资源类型(此处为Microsoft SQL Server)、然后单击新建资源组。



SnapCenter 文档介绍了为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 Backup Server**

解决方案 中使用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(SVBR)将备份副本归档到Amazon S3存储分段。Veeam部署在此解决方案 的Windows服务器上。有关部署Veeam的具体指导、请参见 "Veeam帮助中心技术文档"。

配置**Veeam**横向扩展备份存储库

部署并许可软件后、您可以创建横向扩展备份存储库(SVBR)作为备份作业的目标存储。此外、还应包括一个S3存储分段作为异地VM数据的备份、以便进行灾难恢复。

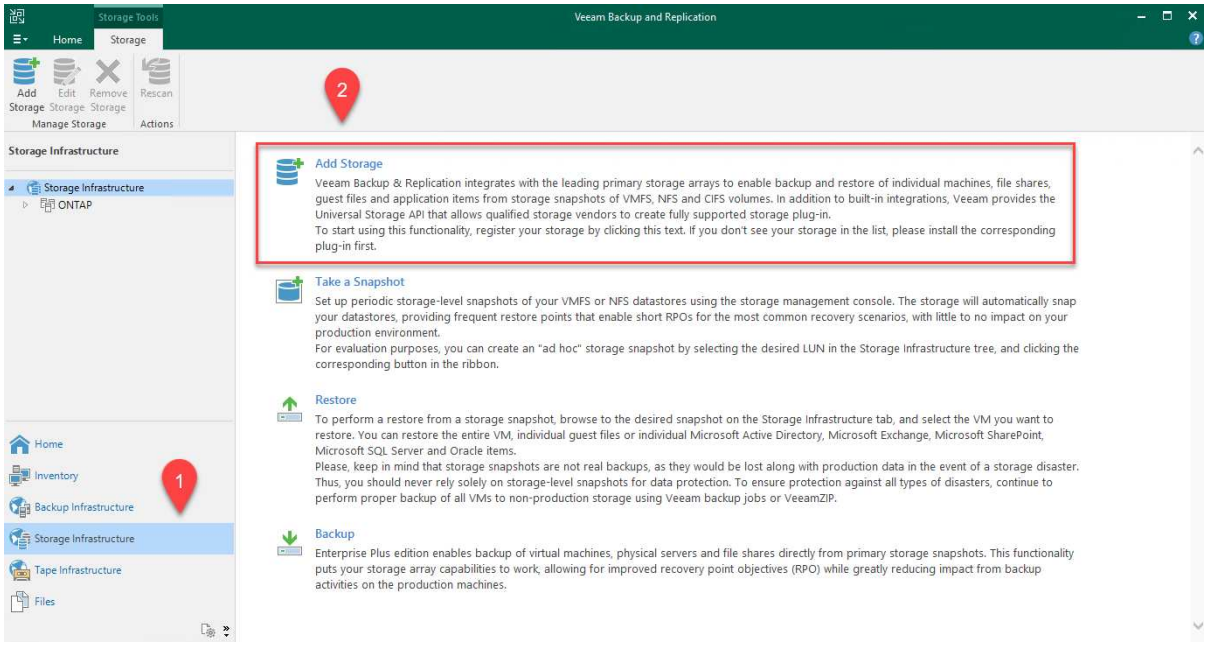
开始使用前、请参见以下前提条件。

1. 在内部ONTAP 系统上创建SMB文件共享、作为备份的目标存储。
2. 创建要包含在SOBR中的Amazon S3存储分段。这是用于异地备份的存储库。

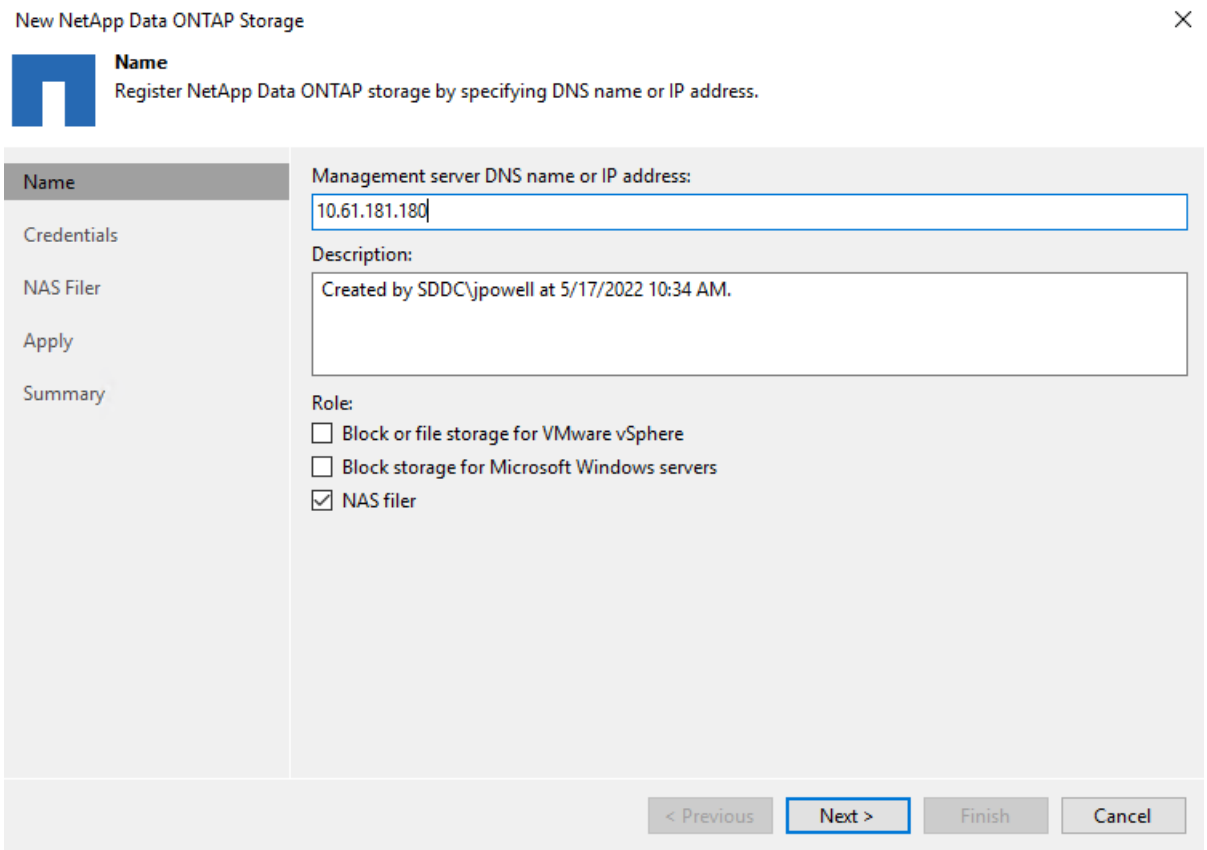
将ONTAP 存储添加到Veeam

首先、在Veeam中将ONTAP 存储集群和关联的SMB/NFS文件系统添加为存储基础架构。

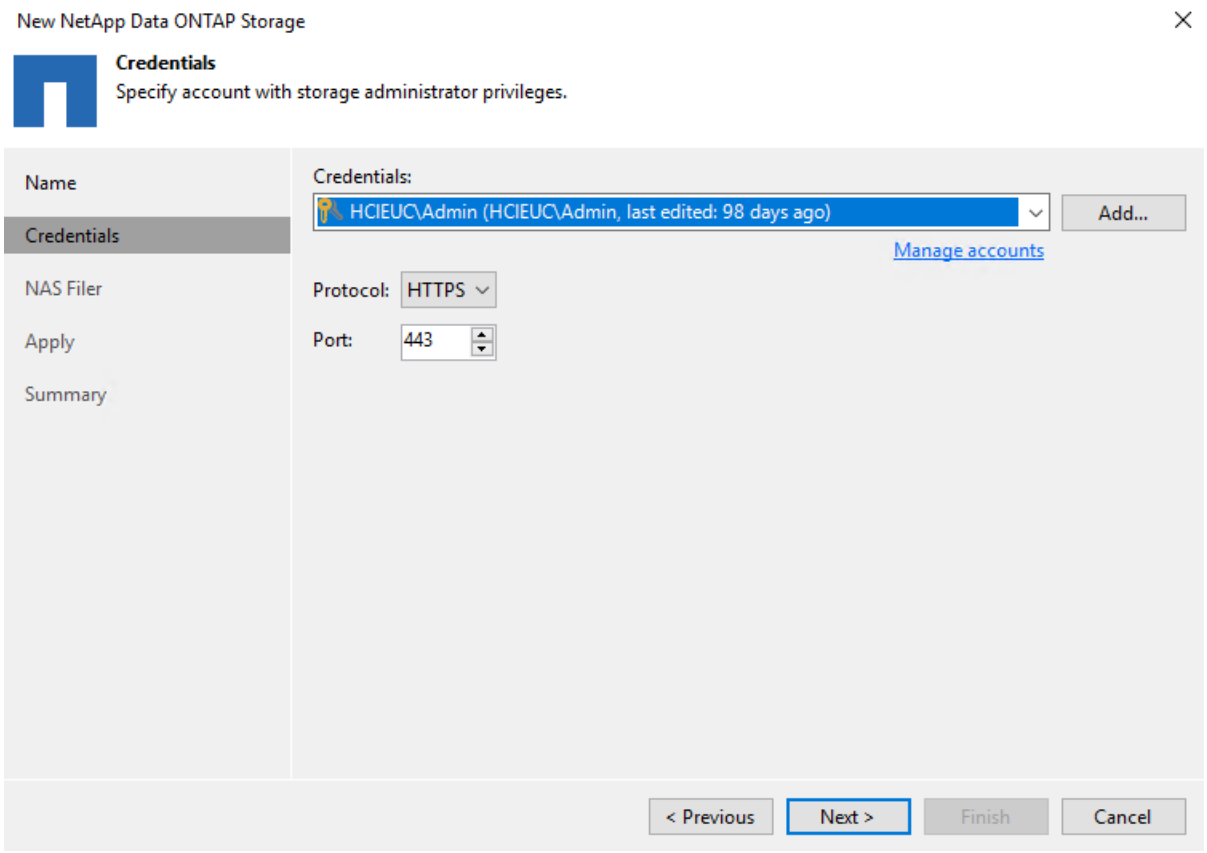
1. 打开Veeam控制台并登录。导航到存储基础架构、然后选择添加存储。



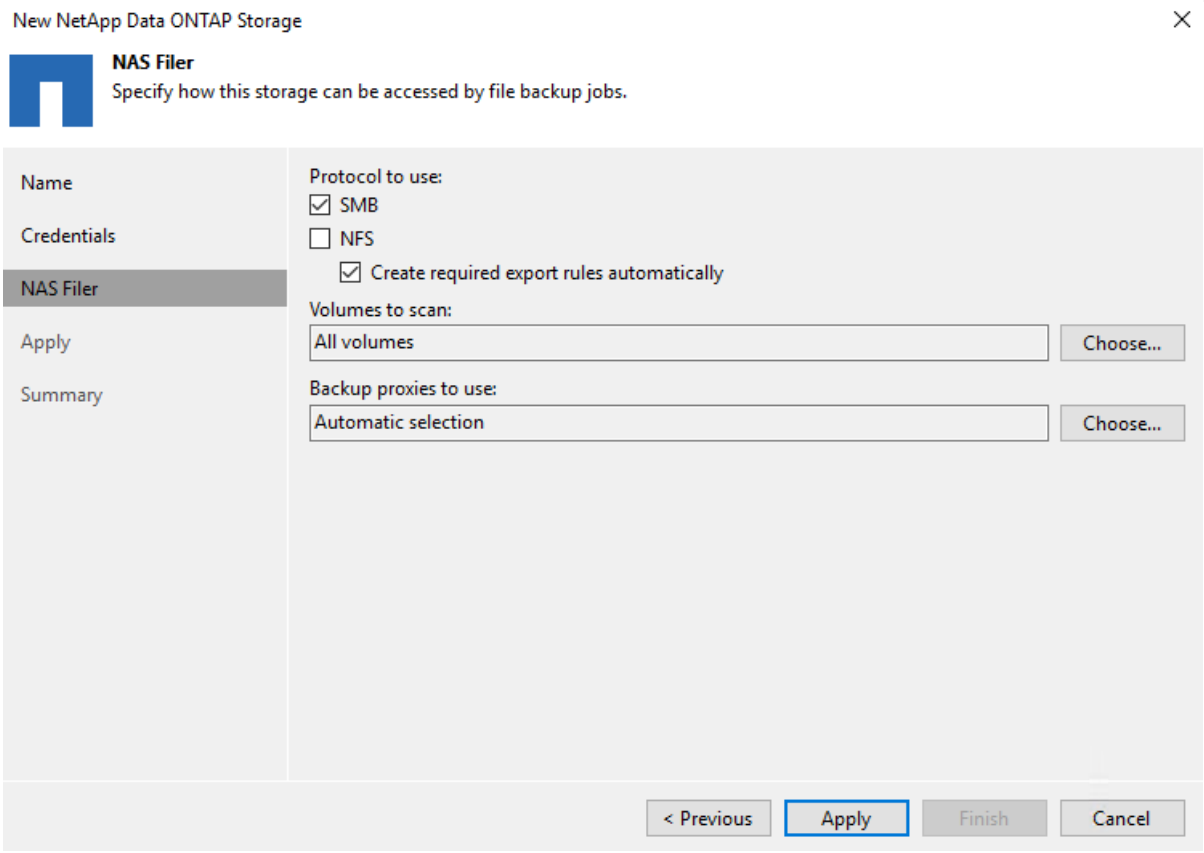
2. 在添加存储向导中、选择NetApp作为存储供应商、然后选择Data ONTAP。
3. 输入管理IP地址并选中NAS文件器复选框。单击下一步。



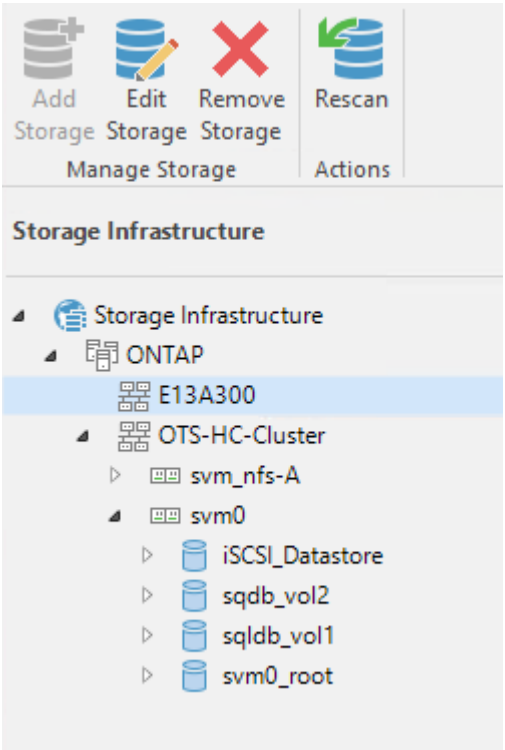
4. 添加凭据以访问ONTAP 集群。



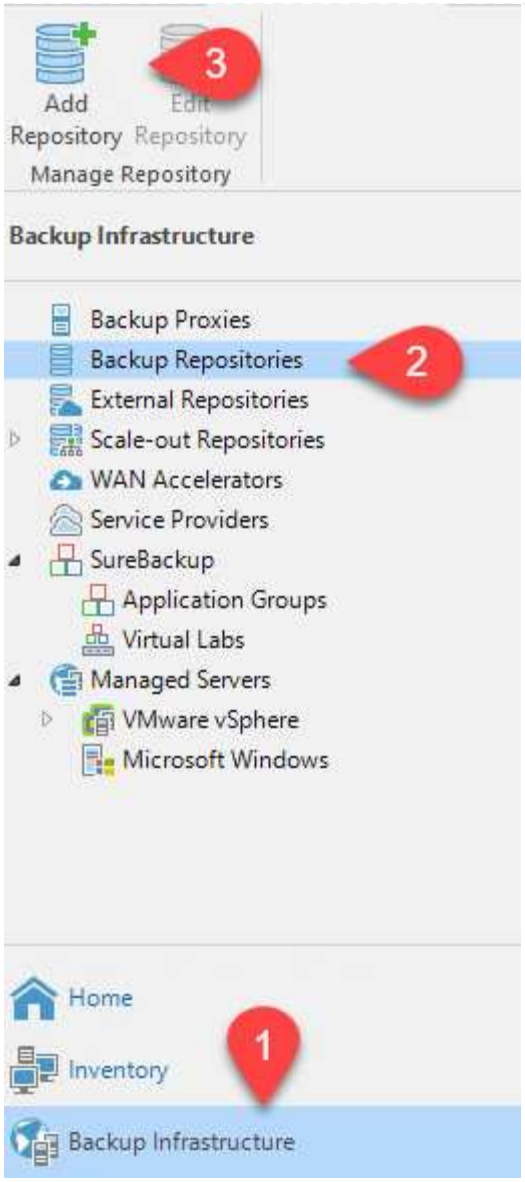
5. 在NAS文件管理器页面上、选择要扫描的协议、然后选择下一步。



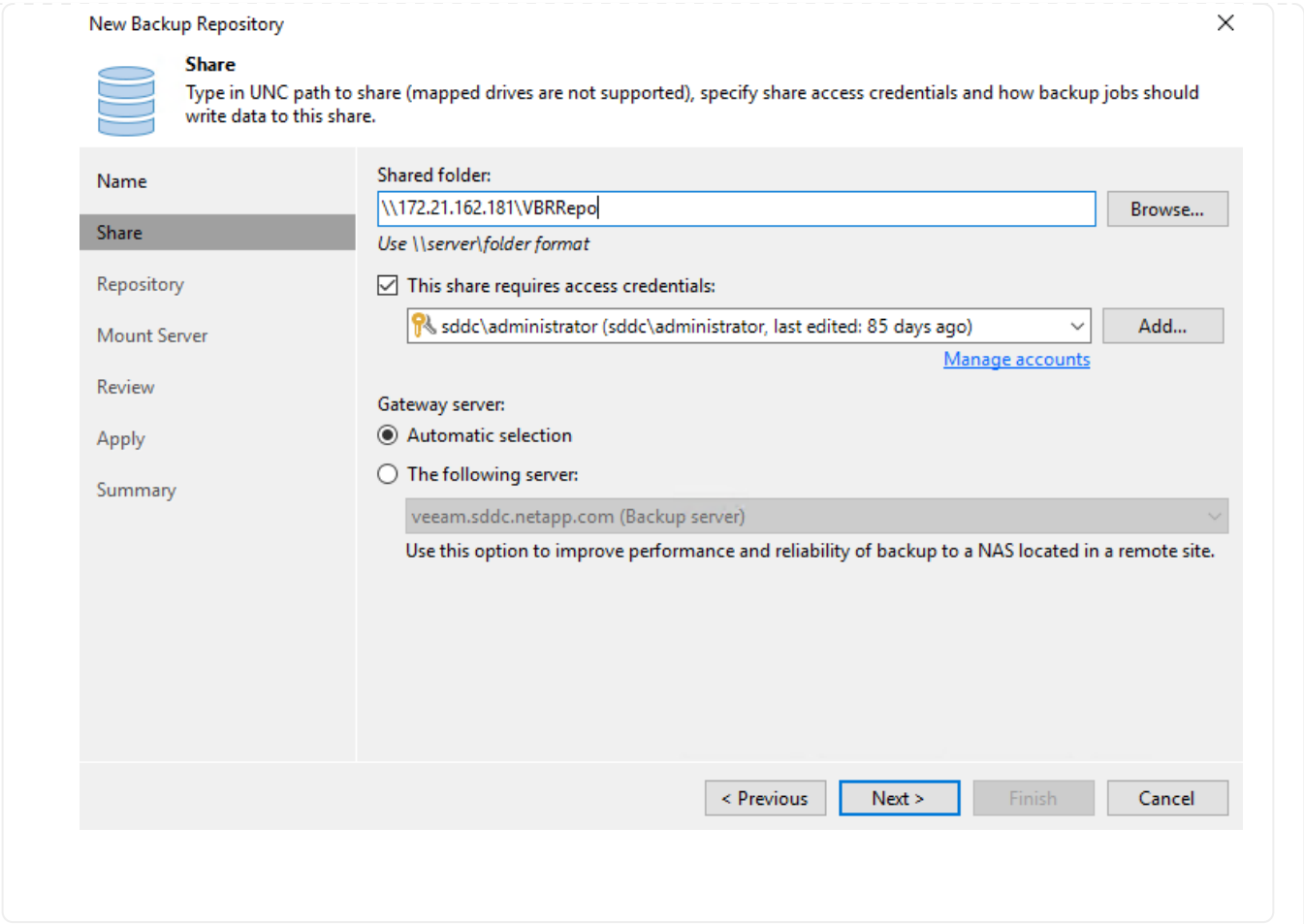
6. 完成向导的"Apply"和"Summary"页面、然后单击"Finish"开始存储发现过程。扫描完成后、ONTAP 集群将与NAS存储器一起添加为可用资源。



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、然后单击添加存储库菜单项。



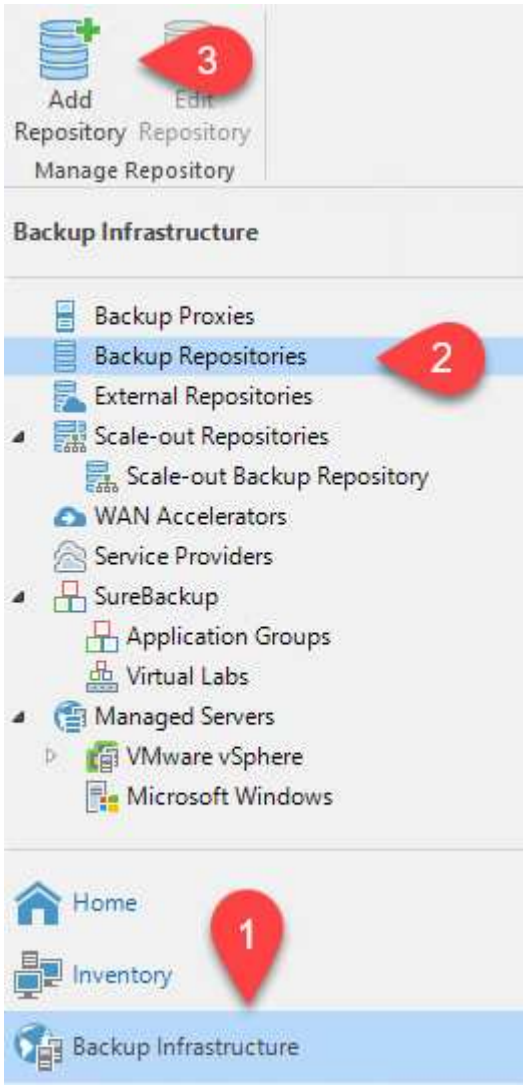
8. 按照"新建备份存储库向导"中的所有步骤创建存储库。有关创建Veeam备份存储库的详细信息、请参见 "Veeam文档"。


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

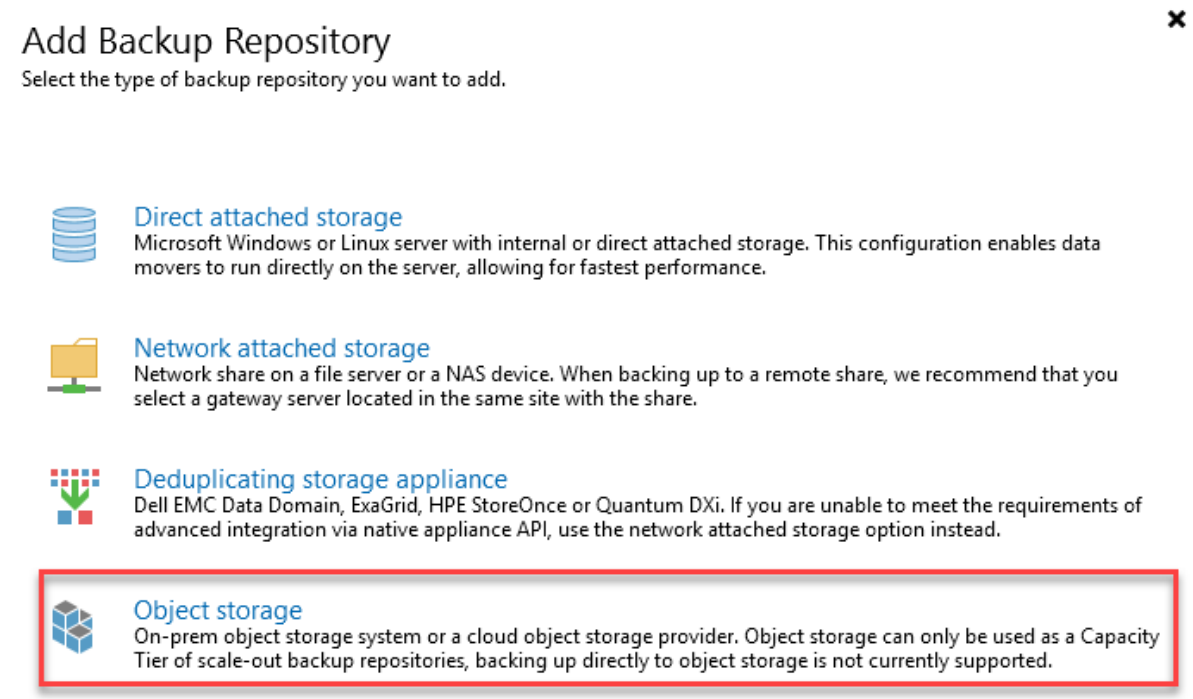
将**Amazon S3**存储分段添加为备份存储库

下一步是将Amazon S3存储添加为备份存储库。

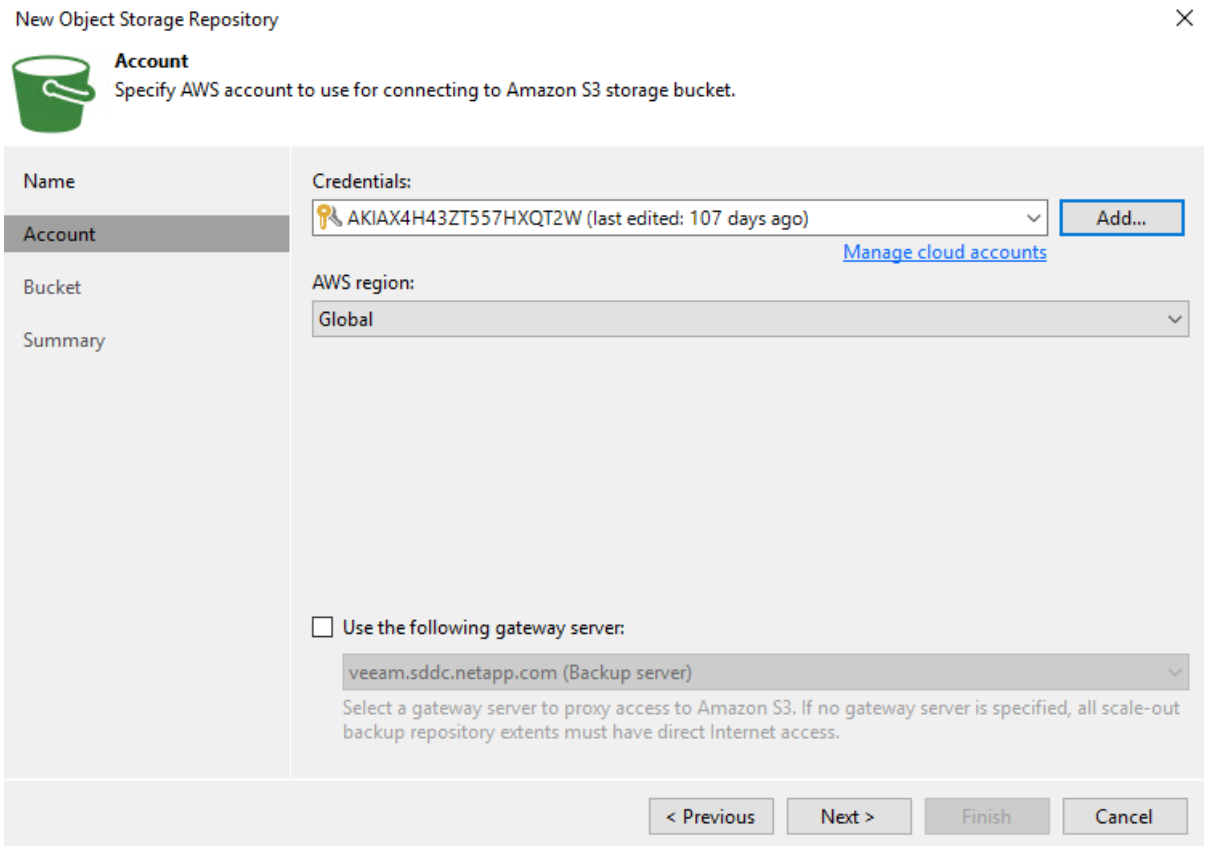
1. 导航到备份基础架构>备份存储库。单击添加存储库。



2. 在添加备份存储库向导中、选择对象存储、然后选择Amazon S3。此时将启动"新建对象存储库"向导。



3. 提供对象存储库的名称、然后单击下一步。
4. 在下一节中、提供您的凭据。您需要AWS访问密钥和机密密钥。

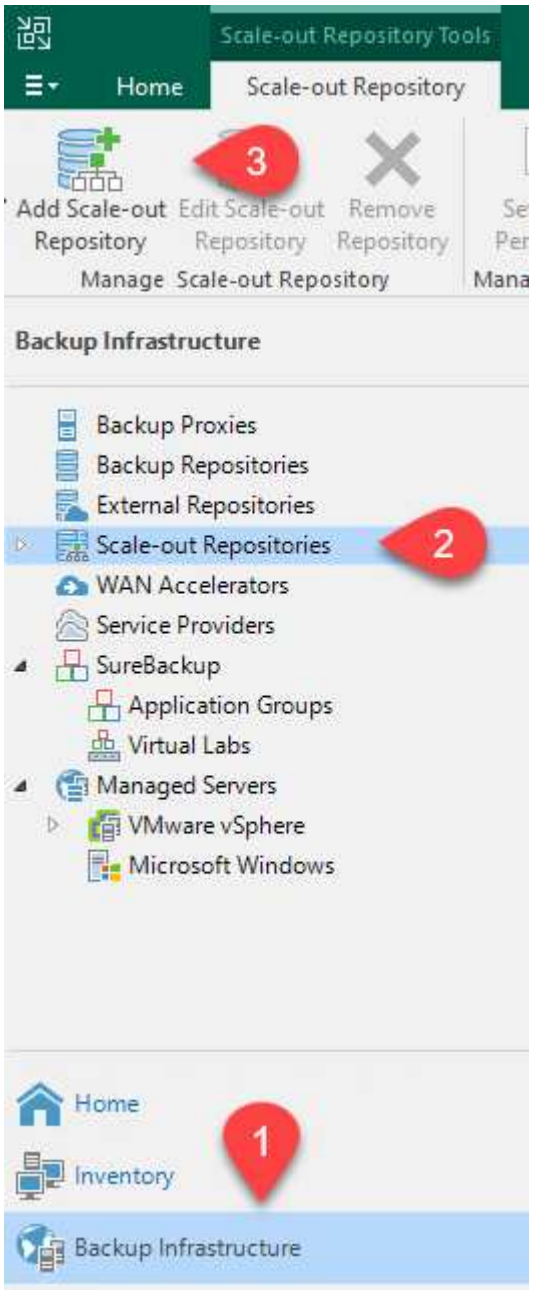


5. 加载Amazon配置后、选择您的数据中心、存储分段和文件夹、然后单击应用。最后、单击完成以关闭向导。

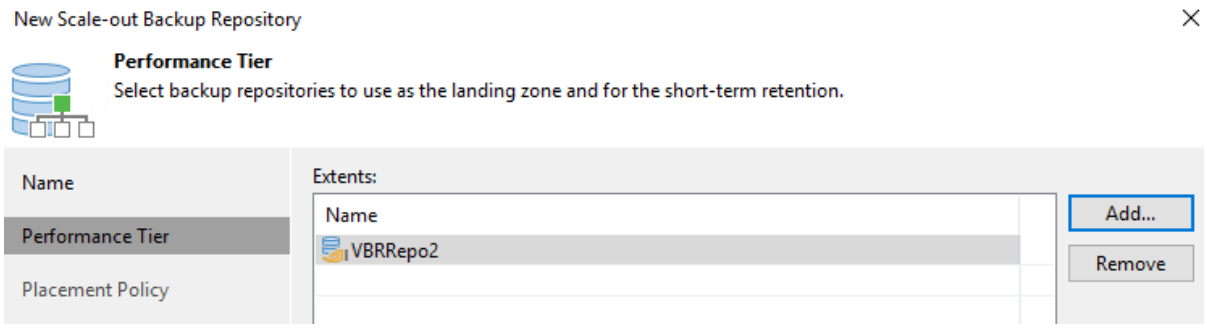
创建横向扩展备份存储库

现在、我们已将存储库添加到Veeam中、我们可以创建SOBR、以便自动将备份副本分层到异地Amazon S3对象存储以进行灾难恢复。

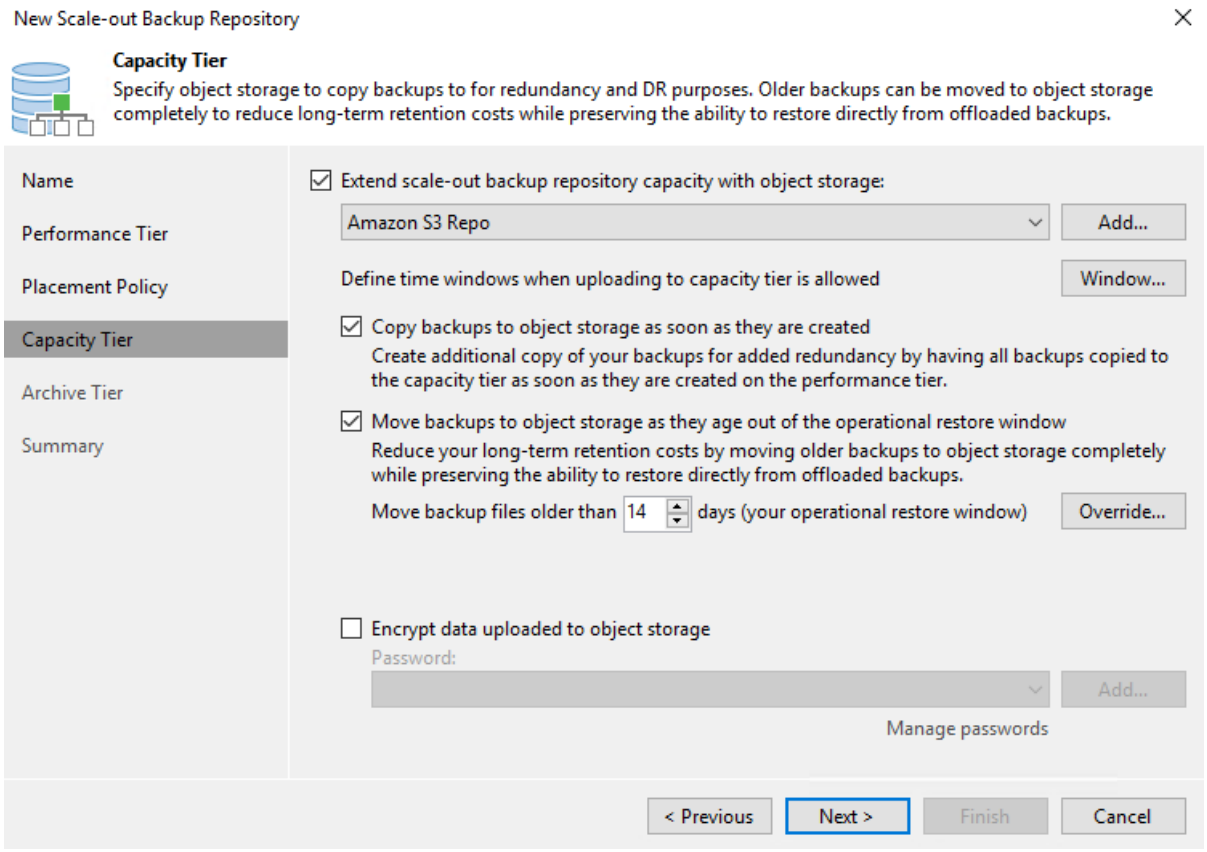
1. 在备份基础架构中、选择横向扩展存储库、然后单击添加横向扩展存储库菜单项。



2. 在New Scale-Out Backup Repository中、为SOBR提供一个名称、然后单击Next。
3. 对于性能层、选择包含驻留在本地ONTAP 集群上的SMB共享的备份存储库。



4. 对于放置策略、根据您的要求选择数据位置或性能。选择"下一步"。
5. 对于容量层、我们使用Amazon S3对象存储扩展了SOBR。为了实现灾难恢复、请在创建备份后立即选择将其复制到对象存储、以确保及时交付我们的二级备份。



6. 最后、选择应用并完成以完成创建SOBR。

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任务的正常组成部分、我们不会介绍此处的详细步骤。有关在Veeam中创建备份作业的详细信息、请参见 "Veeam帮助中心技术文档"。

BlueXP备份和恢复工具及配置

要将应用程序VM和数据库卷故障转移到AWS中运行的VMware云卷服务、您必须安装并配置SnapCenter 服务器和Veeam备份和复制服务器的正在运行的实例。故障转移完成后、您还必须配置这些工具以恢复正常备份操作、直到计划并执行到内部数据中心的故障恢复为止。

部署二级**Windows SnapCenter** 服务器

SnapCenter 服务器部署在VMware云SDDC中或安装在VPC中的EC2实例上、并通过网络连接到VMware云环境。

SnapCenter 软件可从NetApp支持站点获得、并可安装在位于域或工作组中的Microsoft Windows系统上。有关详细的规划指南和安装说明、请参见 "NetApp文档中心"。

您可以在以下位置找到SnapCenter 软件： "此链接。"。

配置二级**Windows SnapCenter** 服务器

要还原镜像到FSX ONTAP 的应用程序数据、您必须先完全还原内部SnapCenter 数据库。此过程完成后、将重新建立与VM的通信、现在可以使用FSX ONTAP 作为主存储来恢复应用程序备份。

为此、您必须在SnapCenter 服务器上完成以下各项：

1. 将计算机名称配置为与原始内部SnapCenter 服务器相同。
2. 配置网络以与VMware Cloud和FSX ONTAP 实例进行通信。
3. 完成操作步骤 以还原SnapCenter 数据库。
4. 确认SnapCenter 处于灾难恢复模式、以确保FSX现在成为备份的主存储。
5. 确认已与还原的虚拟机重新建立通信。

部署二级**Veeam Backup & amp**；复制服务器

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。有关详细的实施指导、请参见 "Veeam帮助中心技术文档"。

配置二级**Veeam Backup & amp**；复制服务器

要还原已备份到Amazon S3存储的虚拟机、您必须在Windows服务器上安装Veeam服务器、并将其配置为与VMware Cloud、FSX ONTAP 和包含原始备份存储库的S3存储分段进行通信。此外、还必须在FSX ONTAP 上配置一个新的备份存储库、以便在虚拟机还原后对其执行新备份。

要执行此过程、必须完成以下各项：

1. 配置网络以与VMware Cloud、FSX ONTAP 和包含原始备份存储库的S3存储分段进行通信。
2. 将FSX ONTAP 上的SMB共享配置为新的备份存储库。
3. 在内部挂载用作横向扩展备份存储库一部分的原始S3存储分段。
4. 还原VM后、建立新的备份作业以保护SQL和Oracle VM。

有关使用Veeam还原VM的详细信息、请参见一节 "使用Veeam Full Restore还原应用程序VM"。

用于灾难恢复的**SnapCenter** 数据库备份

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。对于解决方案 、我们在VPC中的AWS EC2实例上恢复了SnapCenter 数据库和配置。有关此步骤的详细信息、请参见 "此链接。"。

SnapCenter 备份前提条件

SnapCenter 备份需要满足以下前提条件：

- 在内部ONTAP 系统上创建的卷和SMB共享、用于查找备份的数据库和配置文件。
- 内部ONTAP 系统与AWS帐户中的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。
- Windows Server安装在云帐户中、可以安装在EC2实例上、也可以安装在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

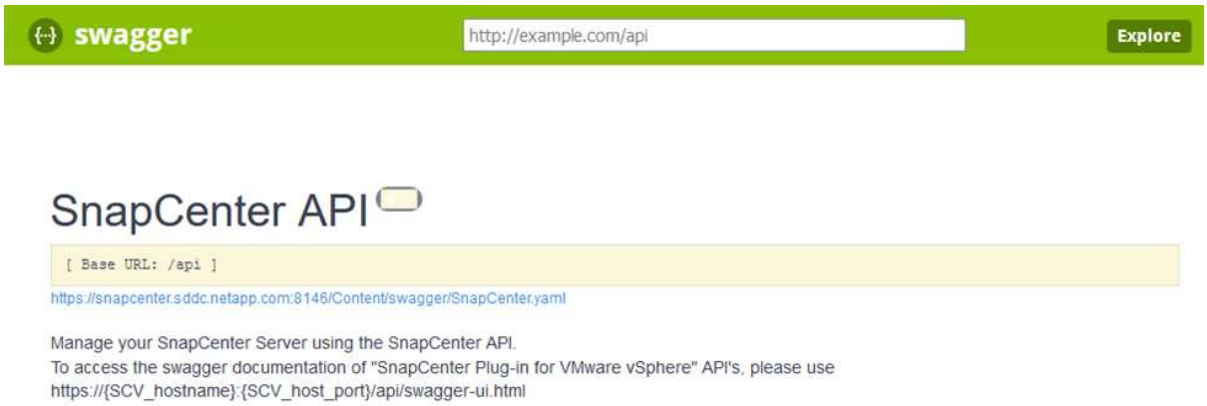
- 在内部ONTAP 系统上创建一个卷、用于托管备份数据库和配置文件。
- 在内部部署和FSX/CVO之间设置SnapMirror关系。
- 挂载SMB共享。
- 检索用于执行API任务的Swagger授权令牌。
- 启动数据库还原过程。
- 使用xcopy实用程序将数据库和配置文件本地目录复制到SMB共享。
- 在FSX上、创建ONTAP 卷的克隆(通过SnapMirror从内部复制)。
- 将SMB共享从FSX挂载到EC2/VMware Cloud。
- 将还原目录从SMB共享复制到本地目录。
- 从Swagger运行SQL Server还原过程。

SnapCenter 提供了一个Web客户端界面、用于执行REST API命令。有关通过Swagger访问REST API的信息、请参见SnapCenter 文档、网址为 "此链接。"。

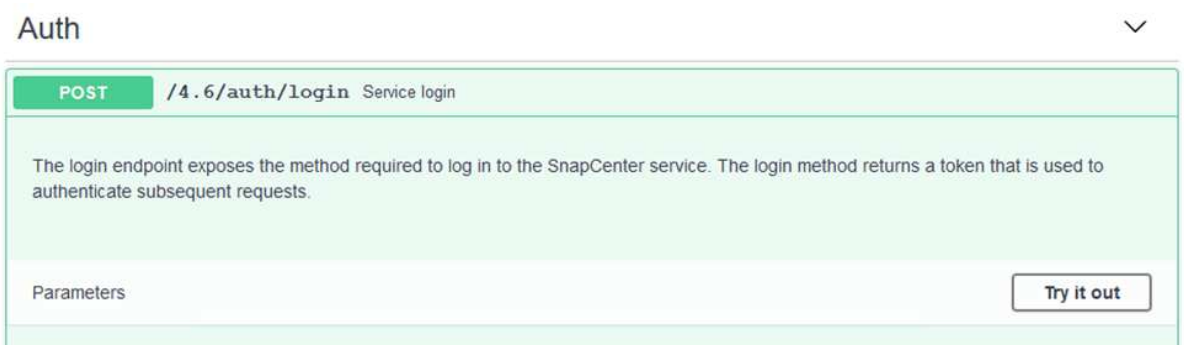
登录到**Swagger**并获取授权令牌

导航到Swagger页面后、您必须检索授权令牌以启动数据库还原过程。

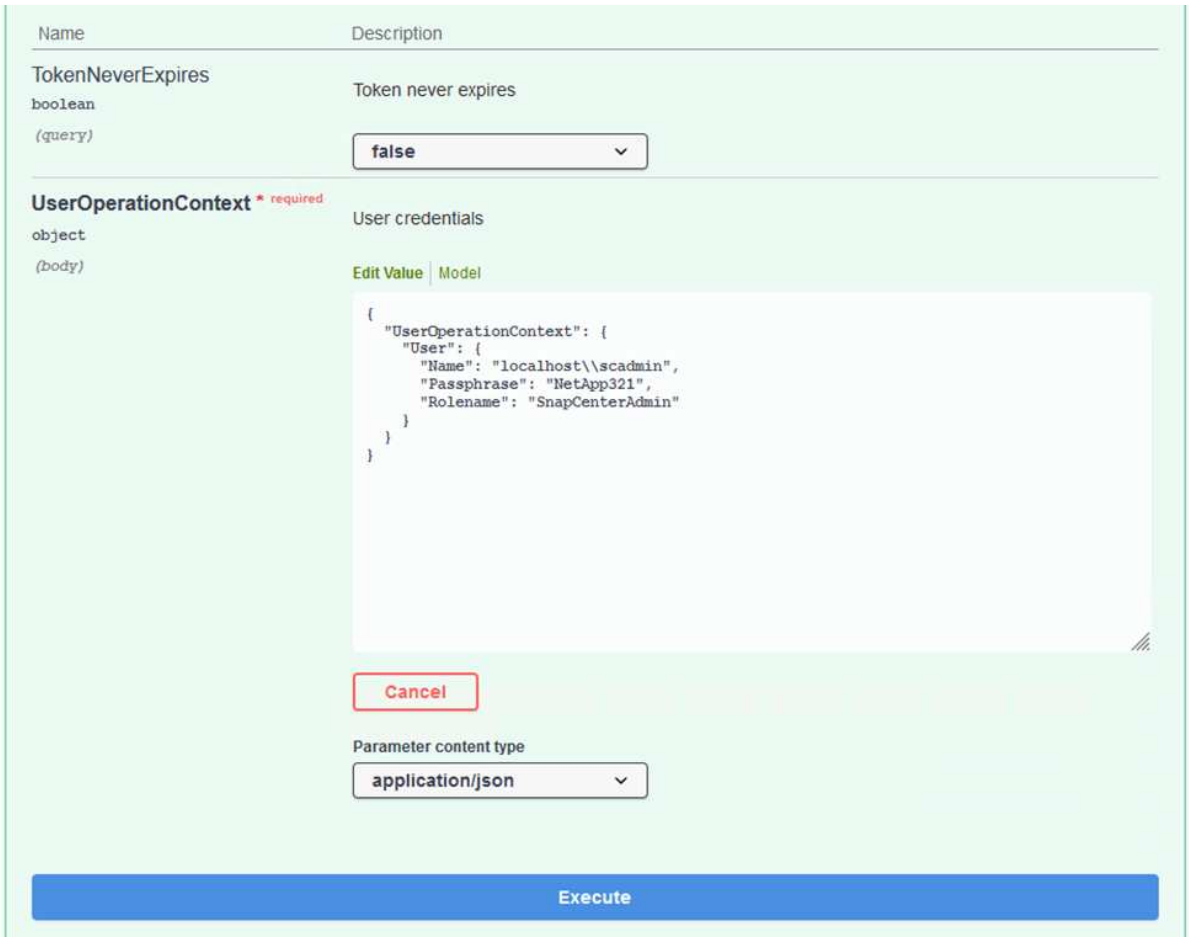
1. 访问SnapCenter Swagger API网页、网址为：//https://<SnapCenter Server IP>：8146/swagger/_。



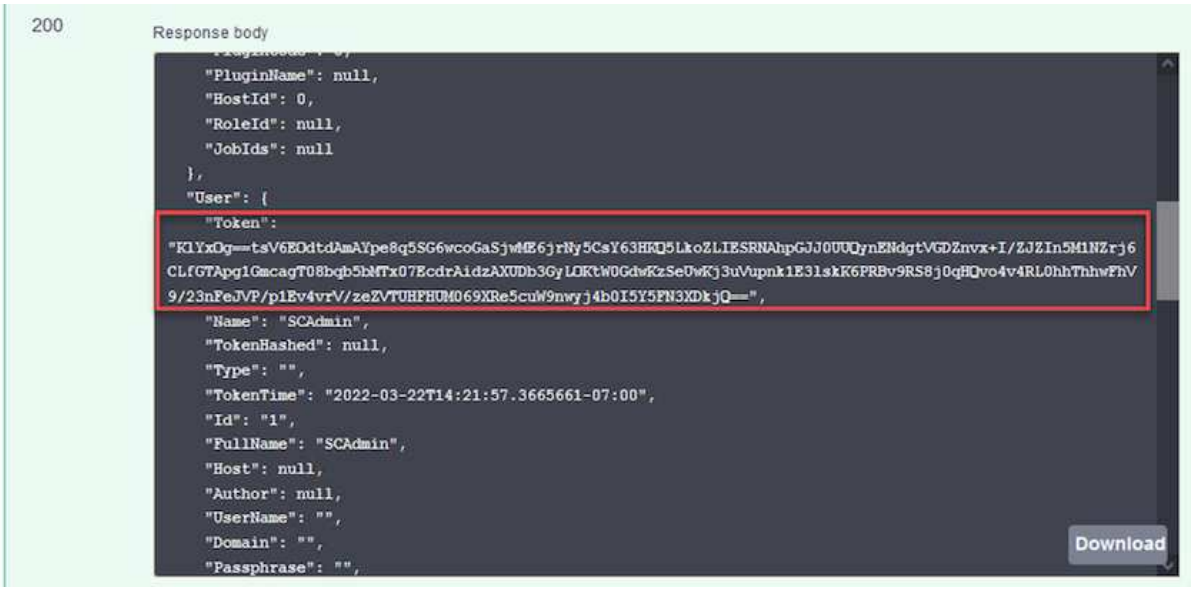
2. 展开"Auth"部分、然后单击Try it out。



3. 在用户操作文本区域中、填写SnapCenter 凭据和角色、然后单击执行。



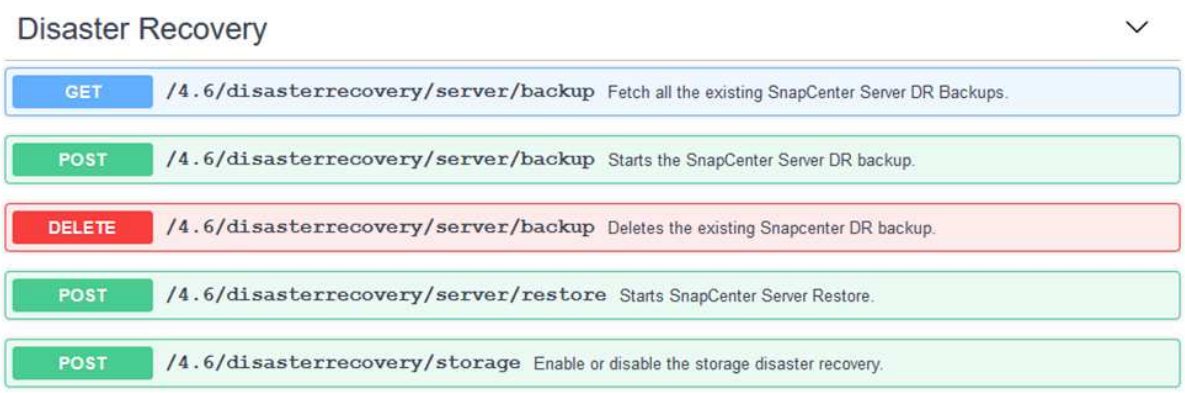
4. 在下面的响应正文中、您可以看到令牌。执行备份过程时、复制令牌文本以进行身份验证。



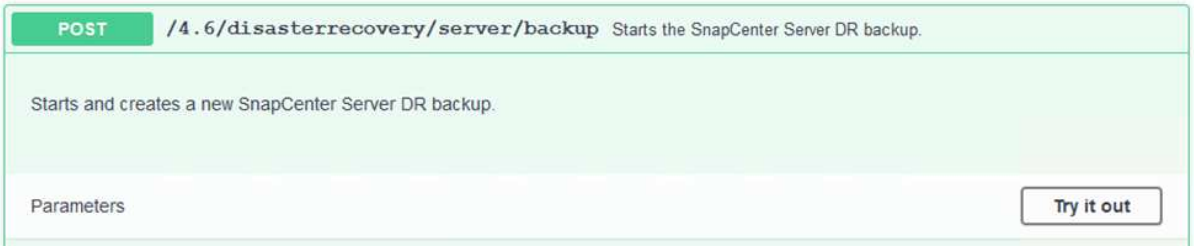
执行**SnapCenter** 数据库备份

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

1. 单击"Disaster Recovery"区域、将其展开。

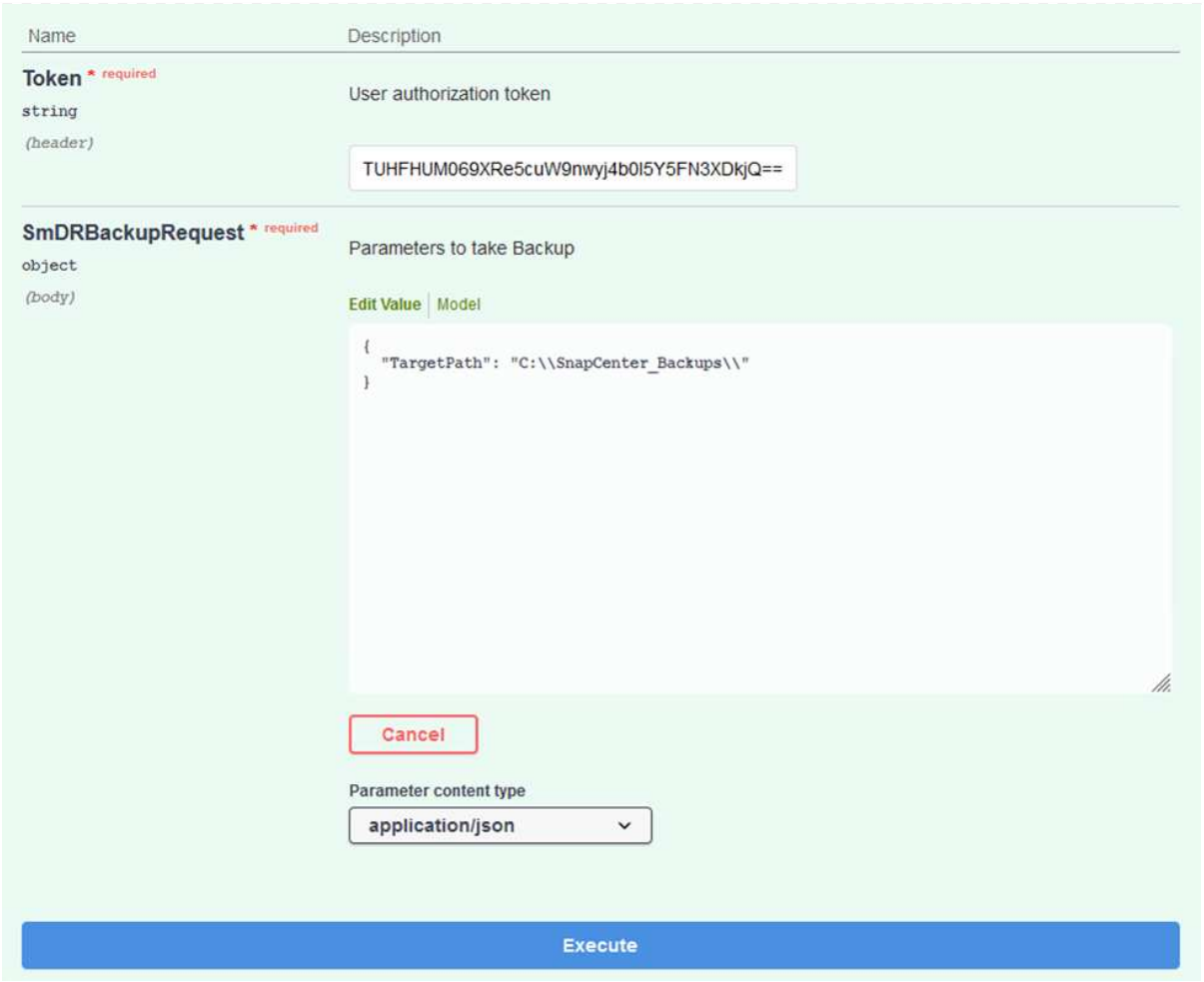


2. 展开`/4.6/disasterrecovery/server/backup`部分、然后单击Try it out。



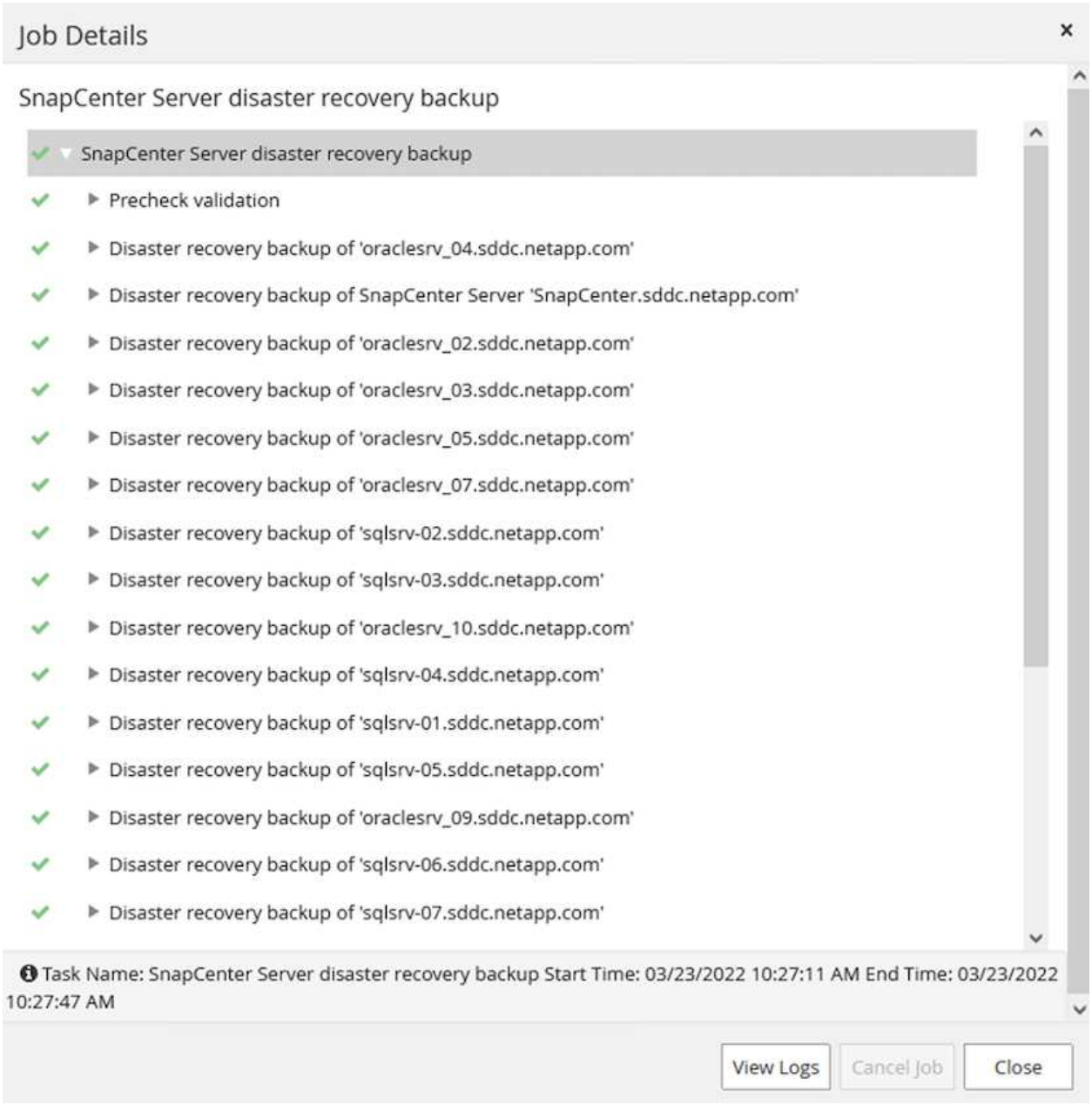
3. 在SmDRBackupRequest部分中、添加正确的本地目标路径并选择执行以启动SnapCenter 数据库和配置的备份。

备份过程不允许直接备份到NFS或CIFS文件共享。


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

从**SnapCenter** 监控备份作业

在启动数据库还原过程时、登录到SnapCenter 以查看日志文件。在"Monitor"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用于SnapMirror将数据复制到AWS中FSX实例上的二级位置的CIFS共享。使用带有保留文件权限的特定选项的xcopy。

以管理员身份打开命令提示符。在命令提示符处、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
```

故障转移

主站点发生灾难

对于主内部数据中心发生的灾难、我们的方案包括使用VMware Cloud on AWS故障转移到位于Amazon Web Services基础架构上的二级站点。我们假定虚拟机和内部ONTAP 集群不再可访问。此外、SnapCenter 和Veeam虚拟机将无法再访问、必须在我们的二级站点上进行重建。

本节将介绍基础架构故障转移到云的问题、我们将介绍以下主题：

- SnapCenter 数据库还原。建立新的SnapCenter 服务器后、请还原MySQL数据库和配置文件、并将数据库切换到灾难恢复模式、以使二级FSX存储成为主存储设备。
- 使用Veeam Backup & Replication还原应用程序虚拟机。连接包含VM备份的S3存储、导入备份并将其还原到AWS上的VMware Cloud。
- 使用SnapCenter 还原SQL Server应用程序数据。
- 使用SnapCenter 还原Oracle应用程序数据。

SnapCenter 数据库还原过程

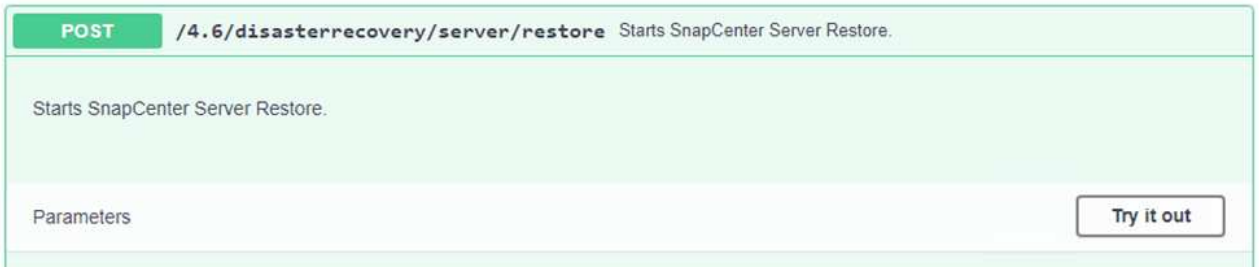
SnapCenter 允许备份和还原其MySQL数据库和配置文件、从而支持灾难恢复场景。这样、管理员便可以在内部数据中心对SnapCenter 数据库进行定期备份、然后将该数据库还原到二级SnapCenter 数据库。

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

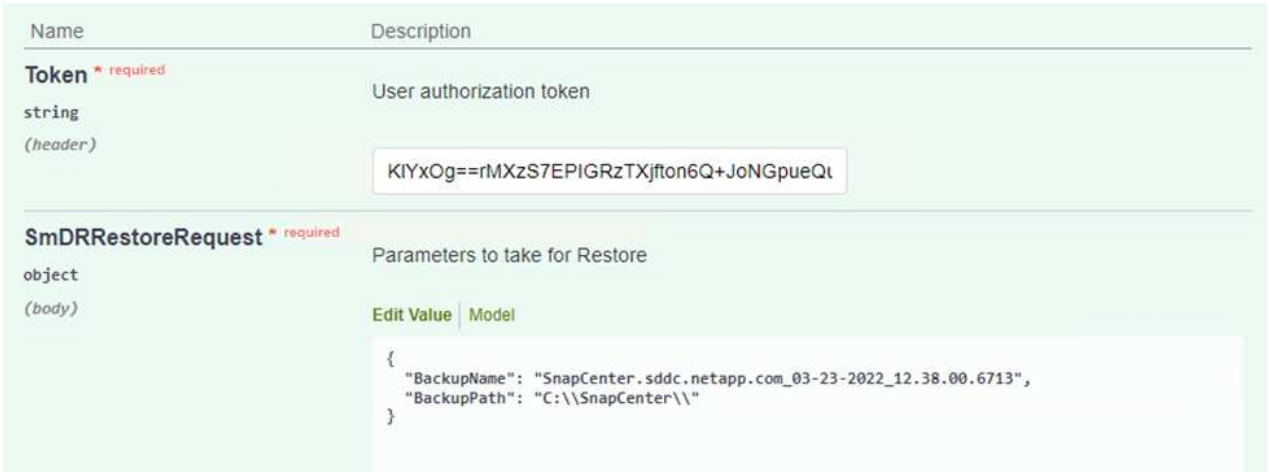
1. 从FSX集群中断SnapMirror关系、从而使卷变为读/写卷。
2. 创建CIFS服务器(如有必要)并创建指向克隆卷的接合路径的CIFS共享。
3. 使用xcopy将备份文件复制到二级SnapCenter 系统上的本地目录。
4. 安装SnapCenter v4.6。
5. 确保SnapCenter 服务器与原始服务器具有相同的FQDN。要成功还原数据库、必须执行此操作。

要启动还原过程、请完成以下步骤：

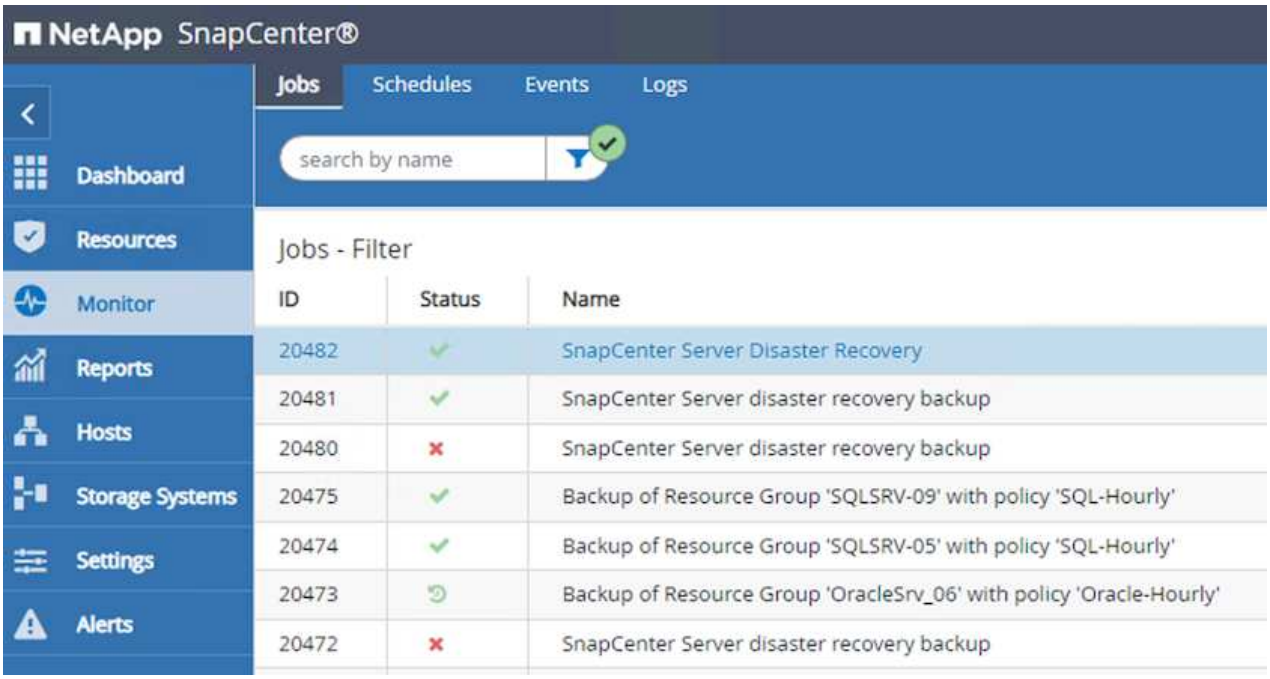
1. 导航到二级SnapCenter 服务器的Swagger API网页、然后按照前面的说明获取授权令牌。
2. 导航到Swagger页面的Disaster Recovery部分、选择`/4.6/disasterrecovery/server/restore`、然后单击Try it out。

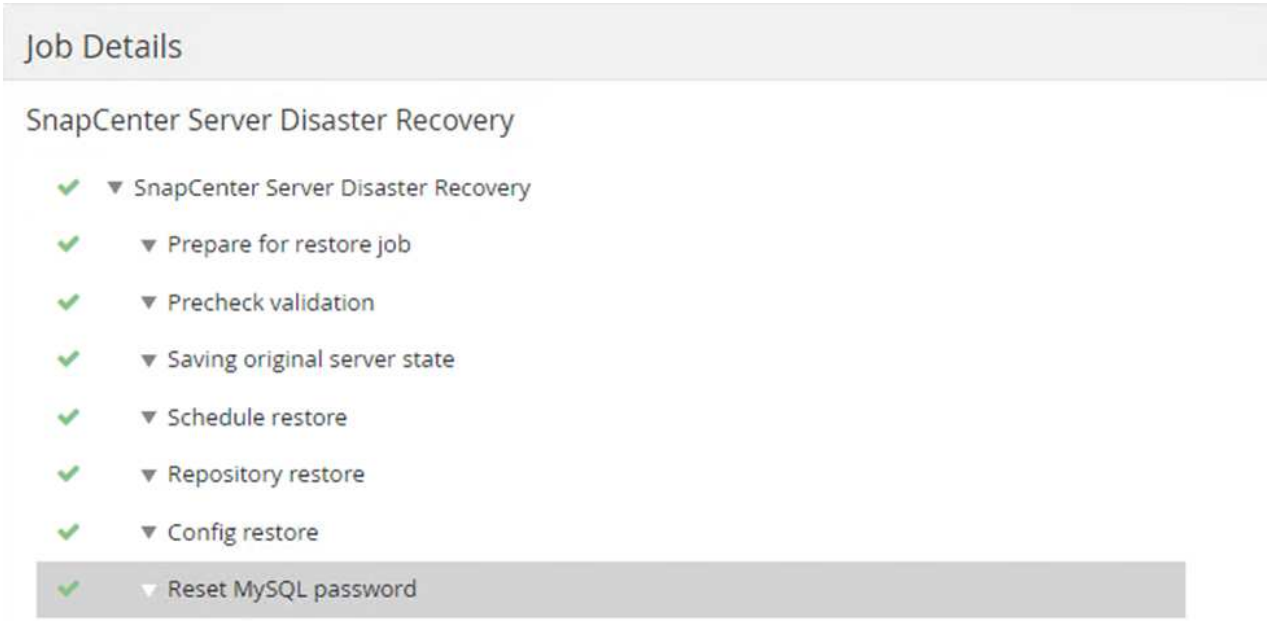


3. 粘贴您的授权令牌、然后在"SmDRResterRequest"部分中、将备份名称和二级SnapCenter 服务器上的本地目录粘贴。



4. 选择执行按钮以启动还原过程。
5. 在SnapCenter 中、导航到Monitor部分以查看还原作业的进度。





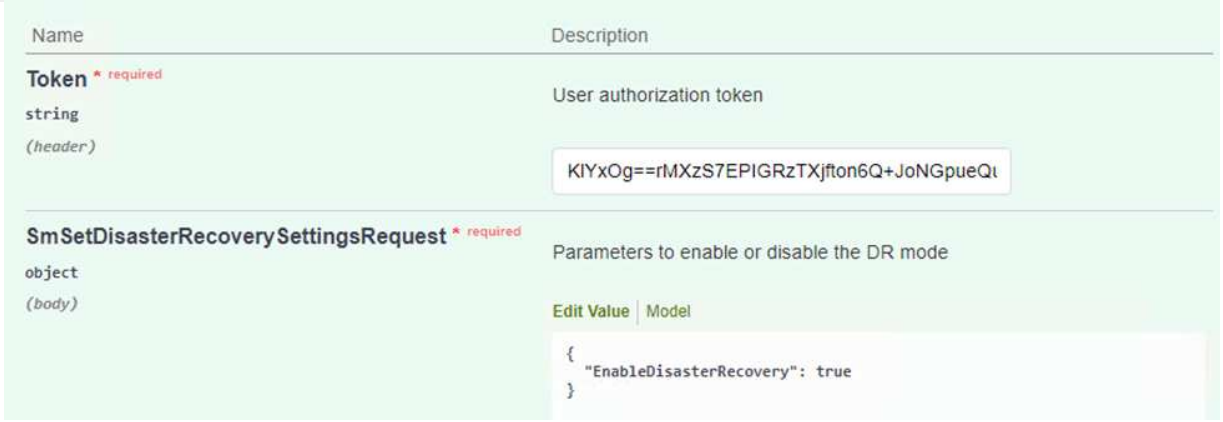
6. 要从二级存储启用SQL Server还原、必须将SnapCenter 数据库切换为灾难恢复模式。此操作将作为单独的操作执行、并在Swagger API网页上启动。

   a. 导航到Disaster Recovery部分、然后单击`/4.6/disasterrecovery/storage`。

   b. 粘贴用户授权令牌。

   c. 在SmSetDisasterRecoverySettingsRequest部分中、将`EnableDisasterRecover`更改为`true`。

   d. 单击执行为SQL Server启用灾难恢复模式。



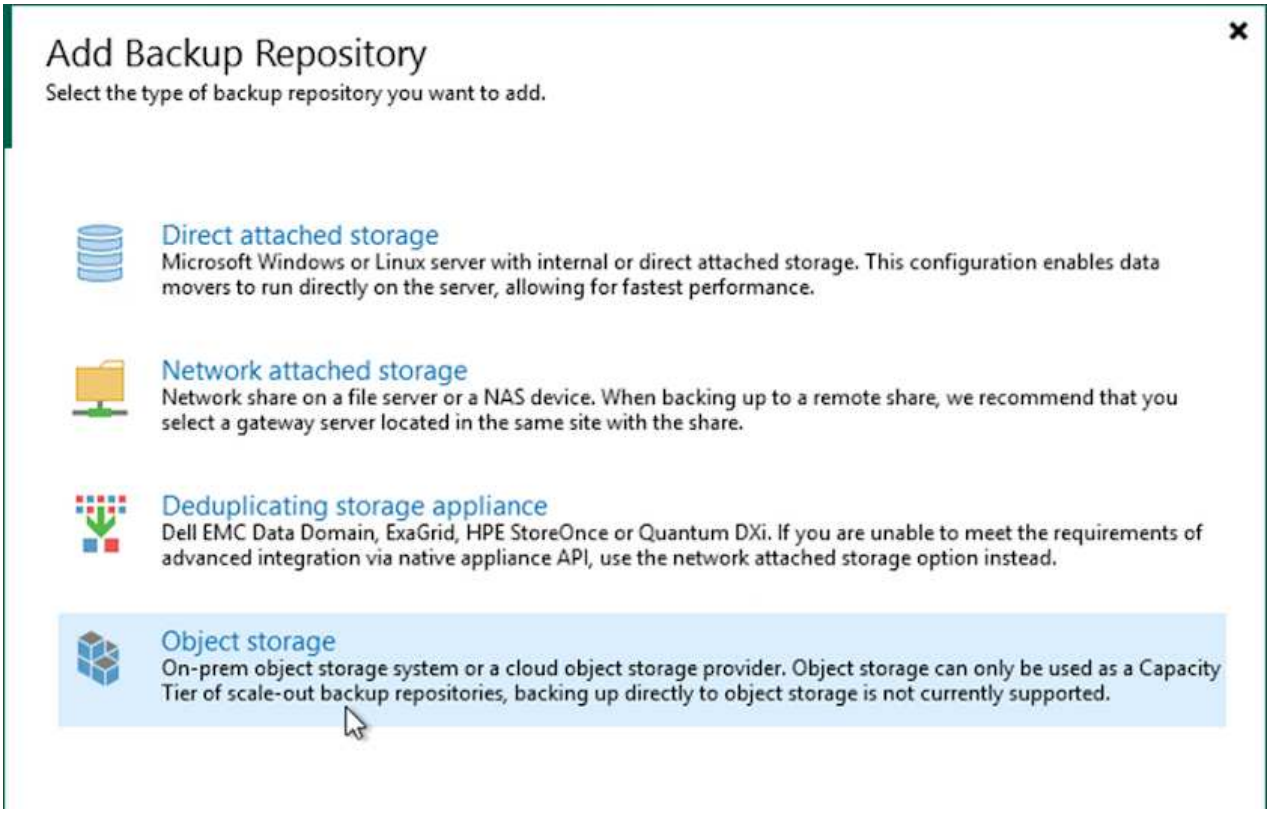
请参见有关其他过程的注释。

使用**Veeam**完全还原还原应用程序**VM**

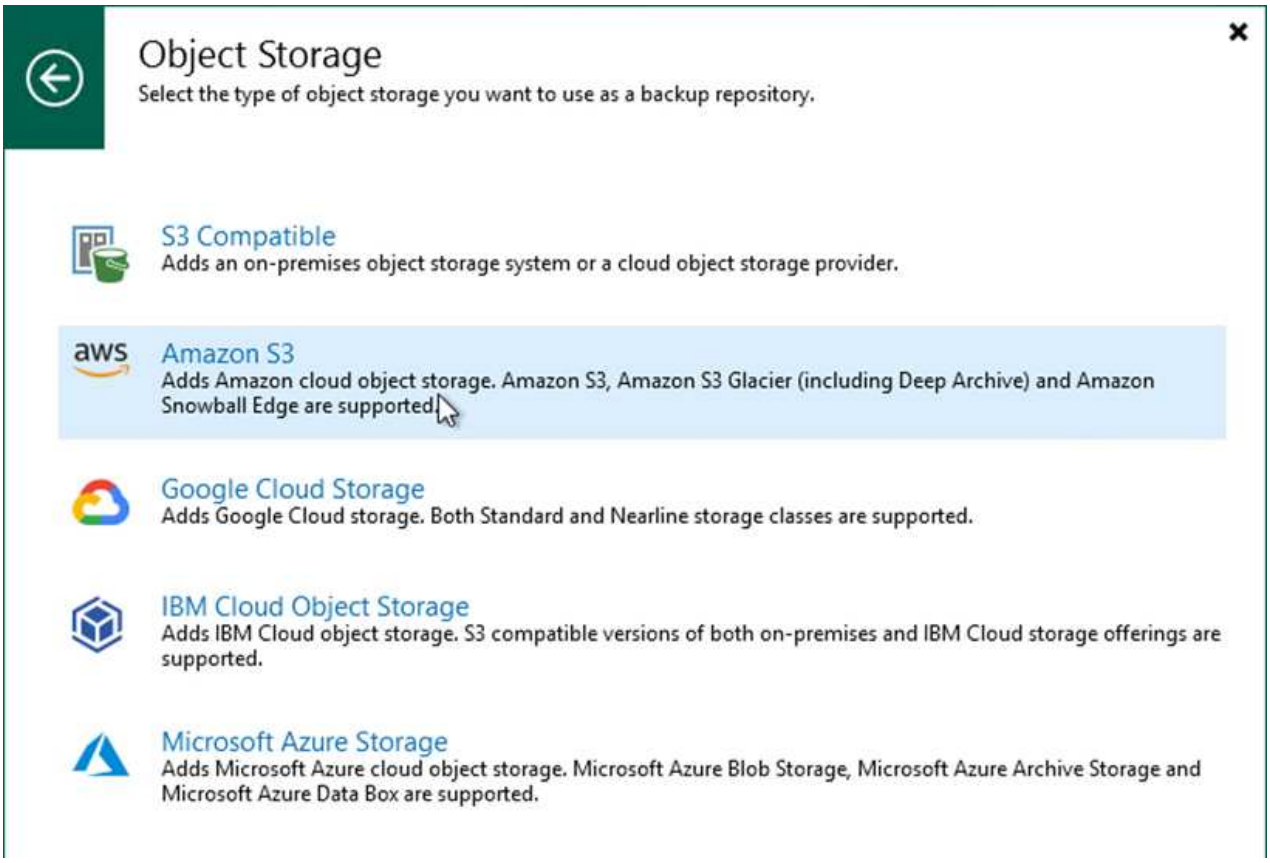
从二级Veeam服务器导入S3存储的备份、并将SQL Server和Oracle VM还原到VMware Cloud集群。

要从内部横向扩展备份存储库中的S3对象导入备份、请完成以下步骤：

1. 转到备份存储库、然后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。

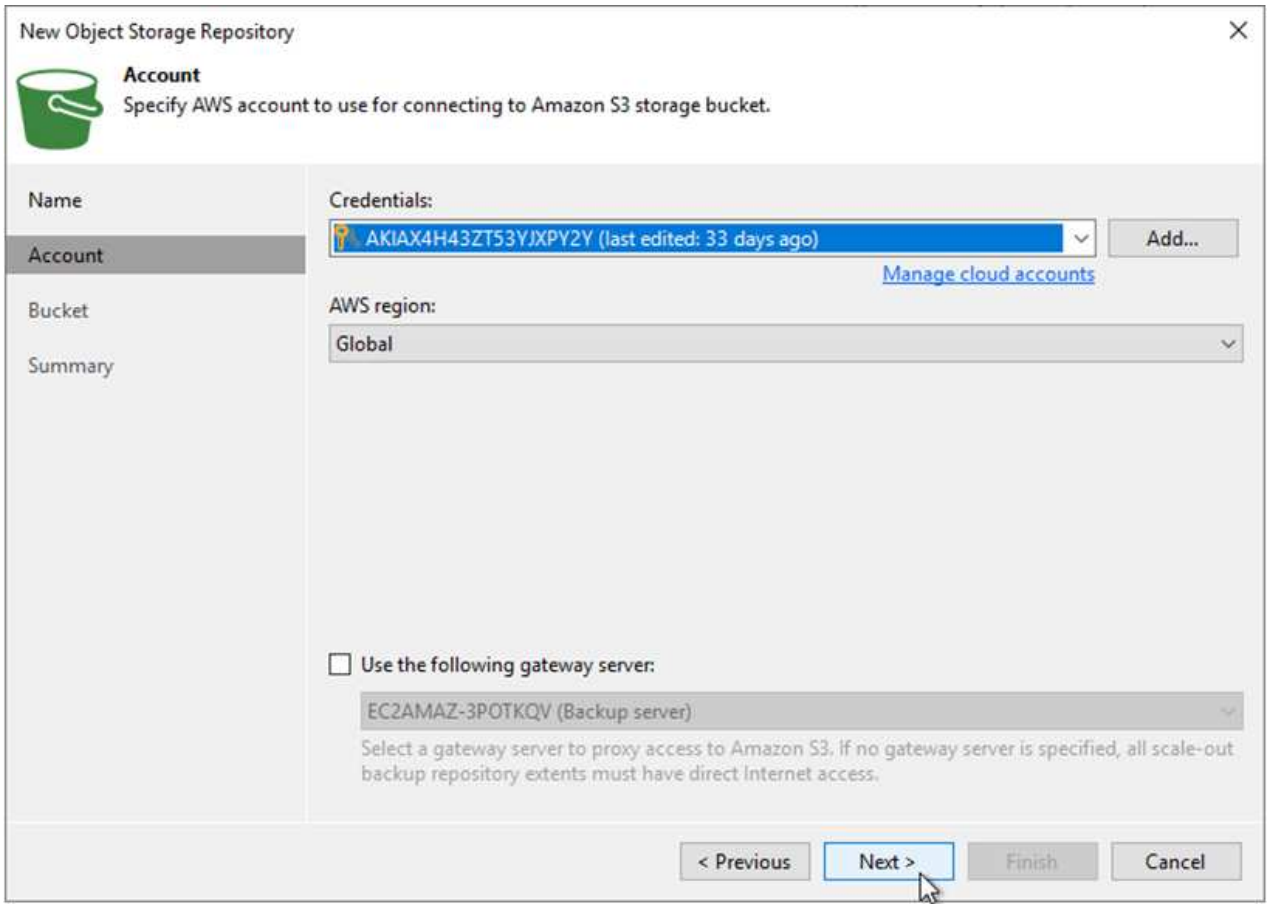


2. 选择Amazon S3作为对象存储类型。

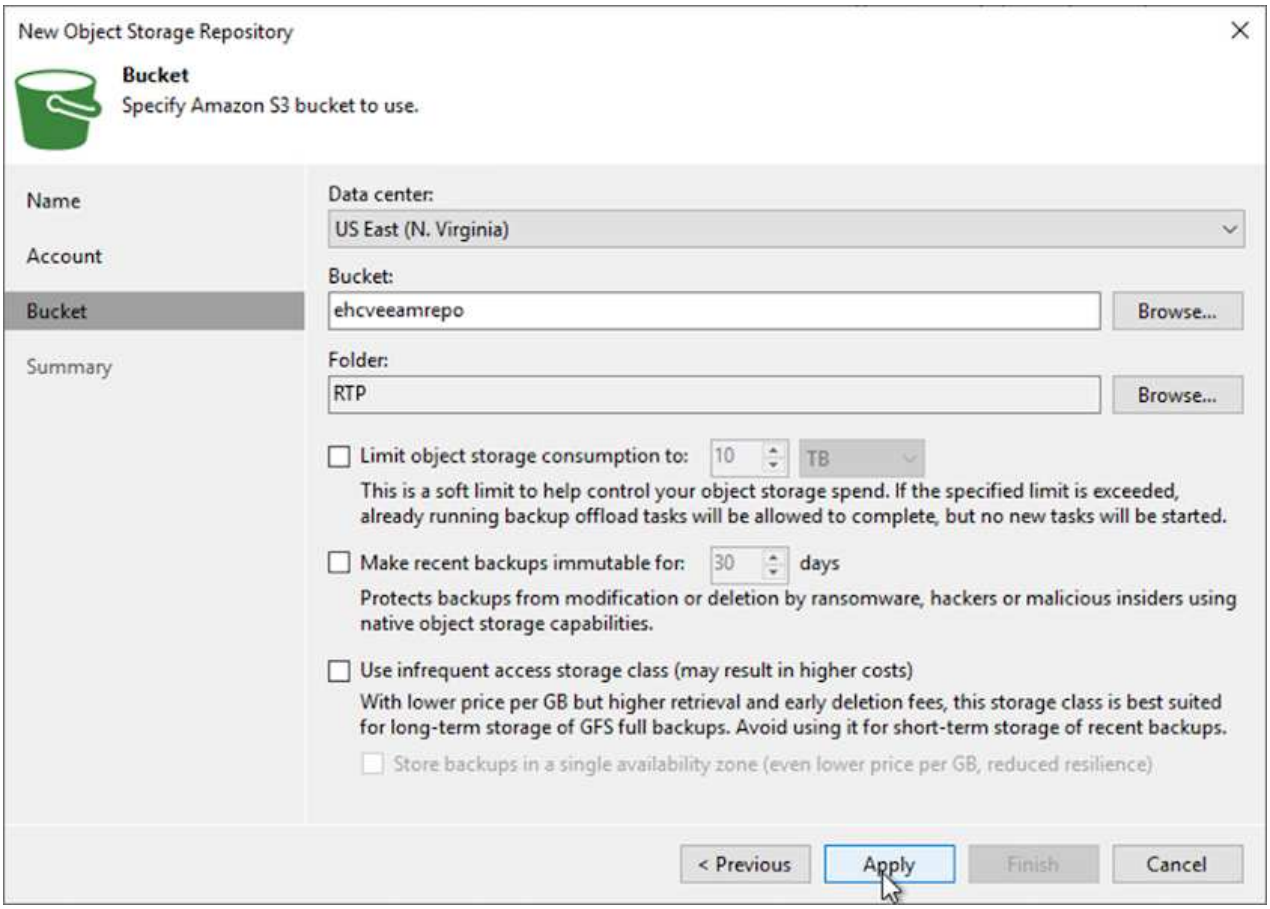


3. 从Amazon Cloud Storage Services列表中、选择Amazon S3。

4. 从下拉列表中选择预先输入的凭据、或者添加用于访问云存储资源的新凭据。单击下一步继续。



5. 在存储分段页面上、输入数据中心、存储分段、文件夹以及任何所需选项。单击应用。

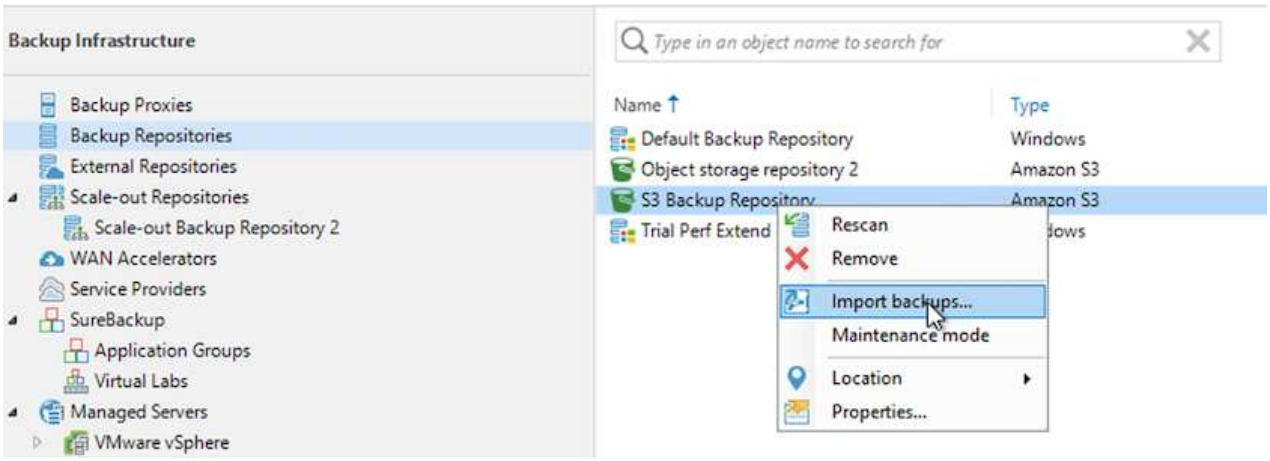


6. 最后、选择完成以完成此过程并添加存储库。

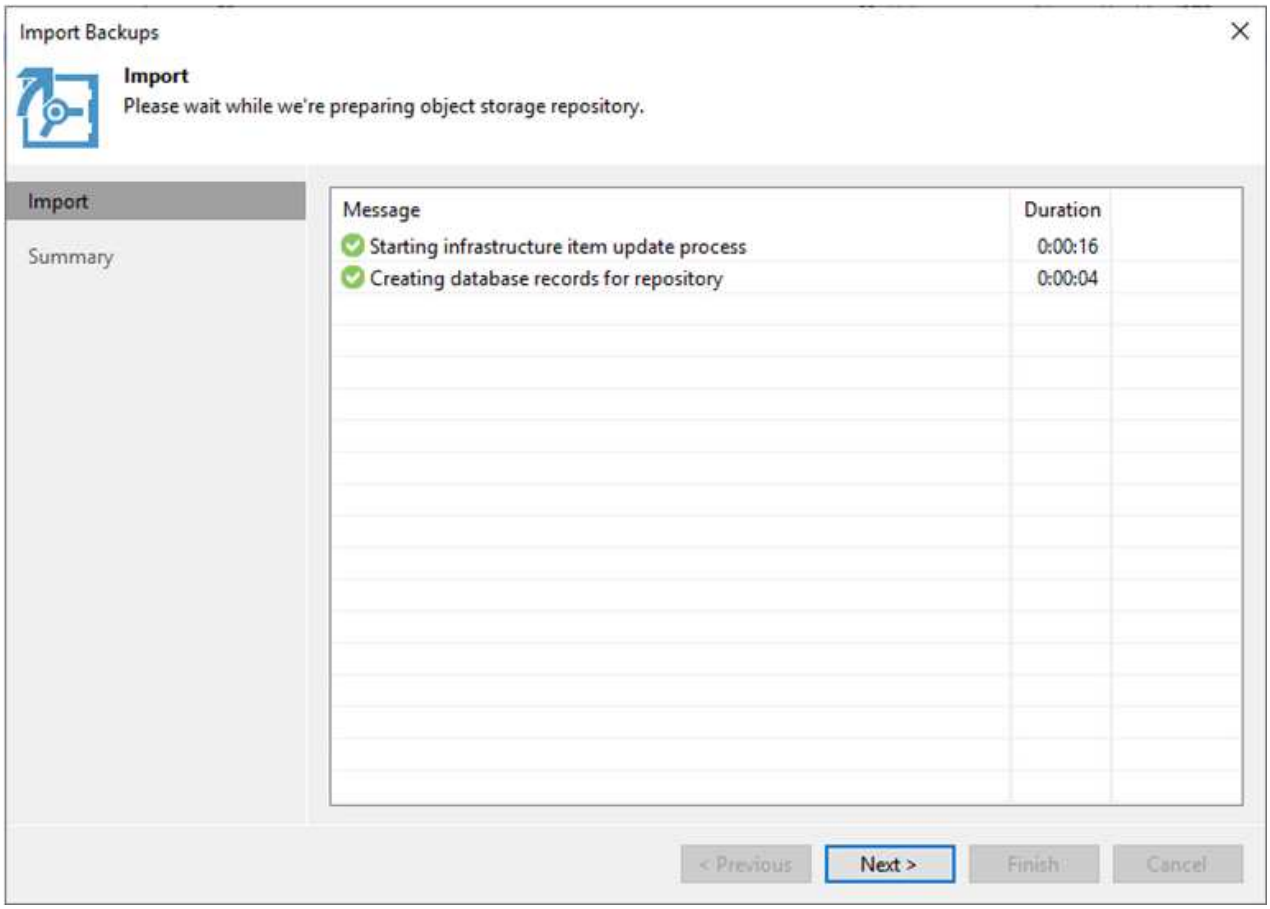
从**S3**对象存储导入备份

要从上一节中添加的S3存储库导入备份、请完成以下步骤。

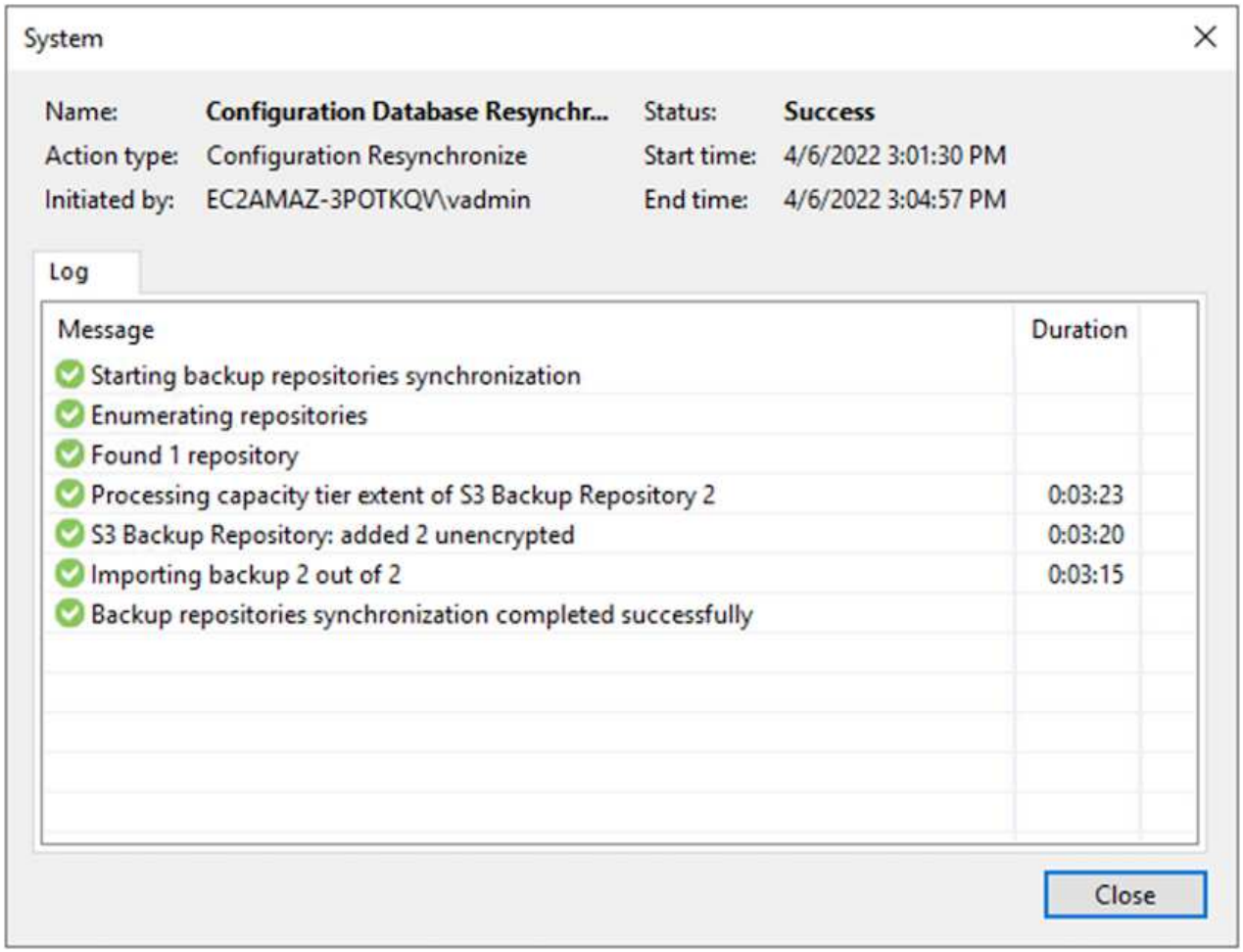
1. 在S3备份存储库中、选择导入备份以启动导入备份向导。



2. 为导入创建数据库记录后、在摘要屏幕上选择下一步、然后选择完成以启动导入过程。



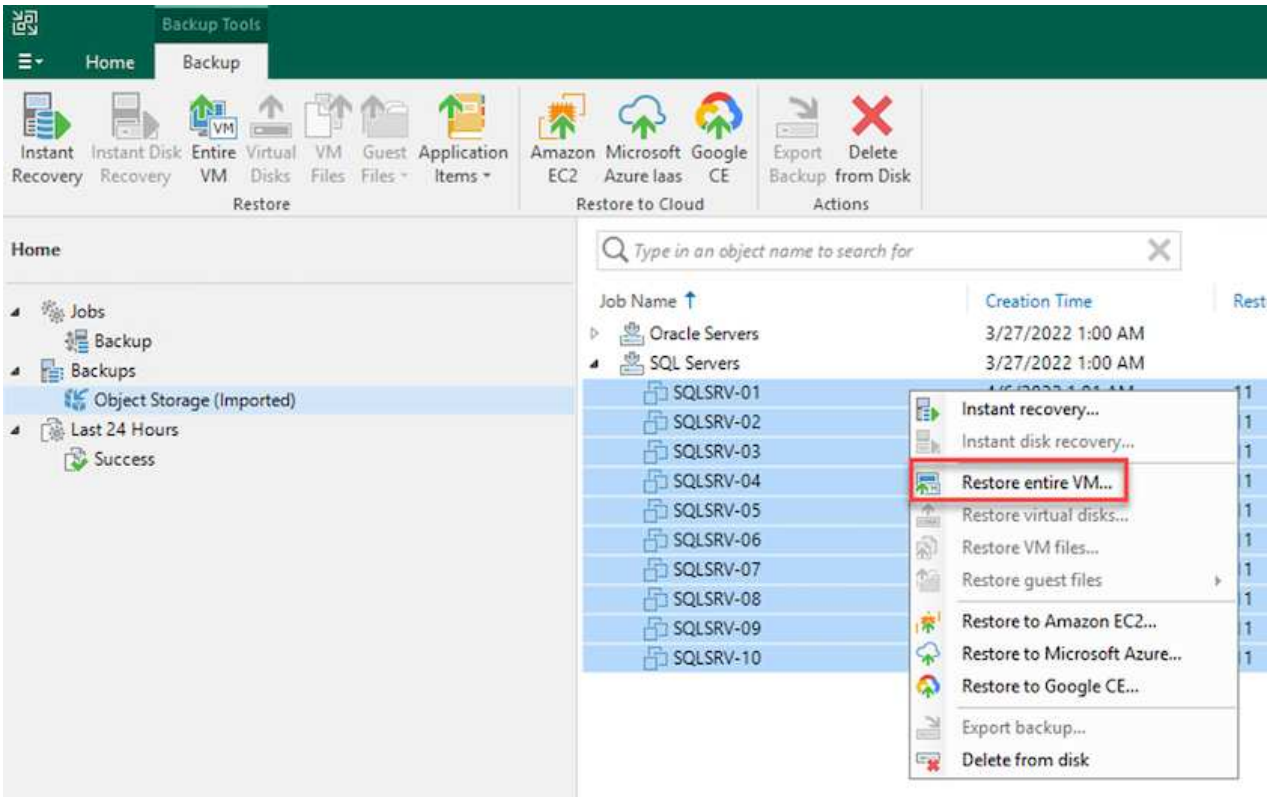
3. 导入完成后、您可以将虚拟机还原到VMware Cloud集群中。


System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

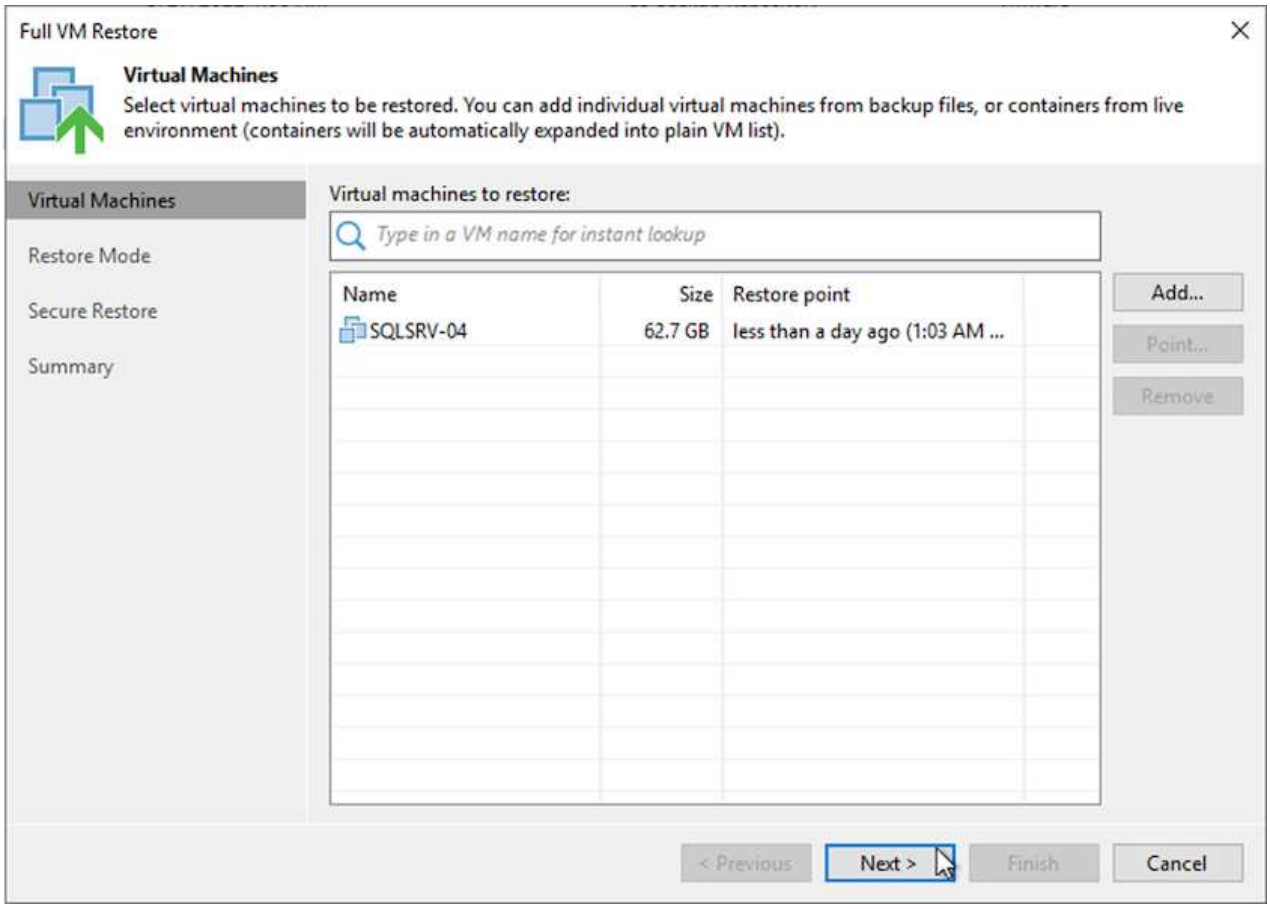
通过Veeam完全还原到VMware Cloud来还原应用程序VM

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

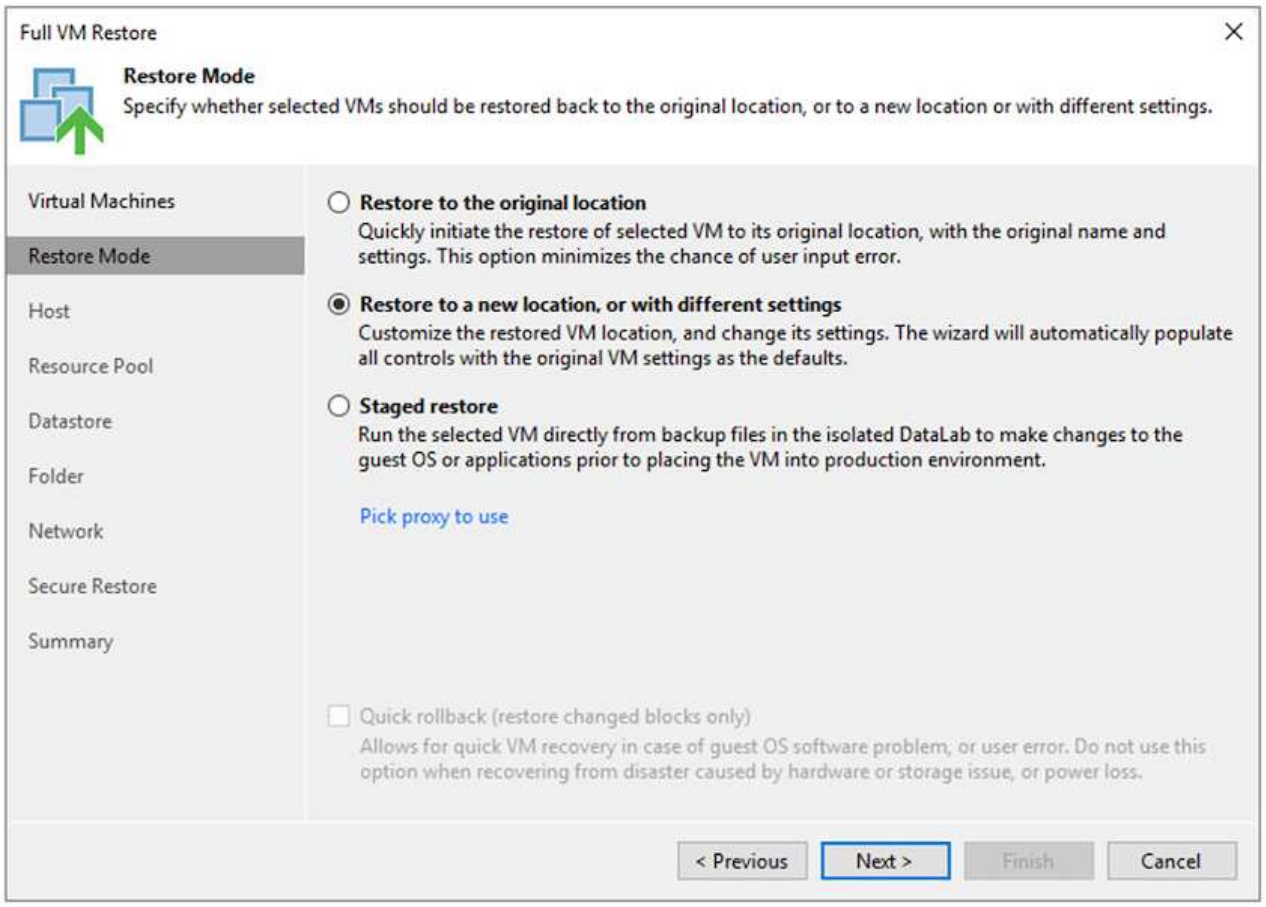
1. 从Veeam主页页面中、选择包含导入备份的对象存储、选择要还原的VM、然后右键单击并选择还原整个VM。



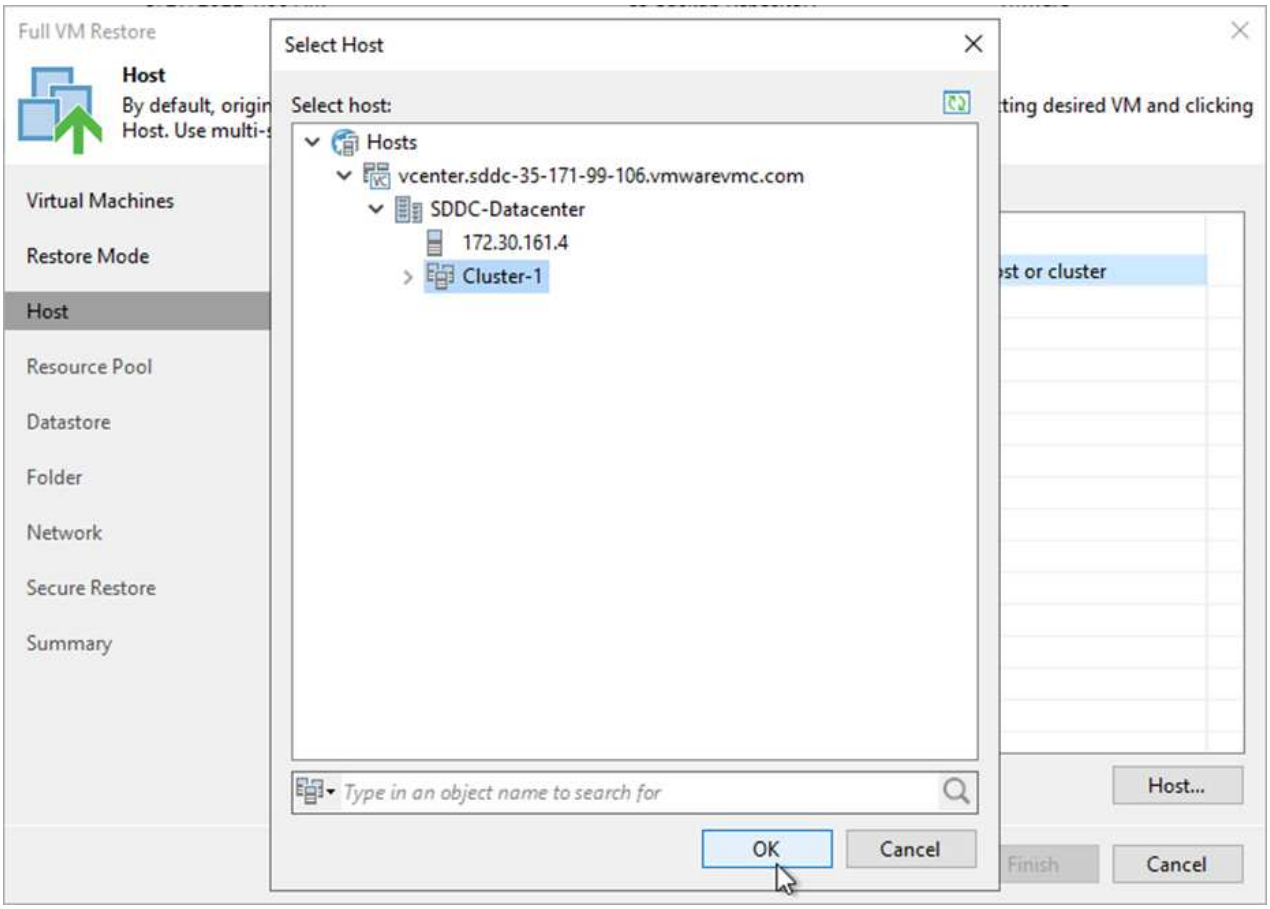
2. 在完整虚拟机还原向导的第一页上、根据需要修改要备份的虚拟机、然后选择下一步。



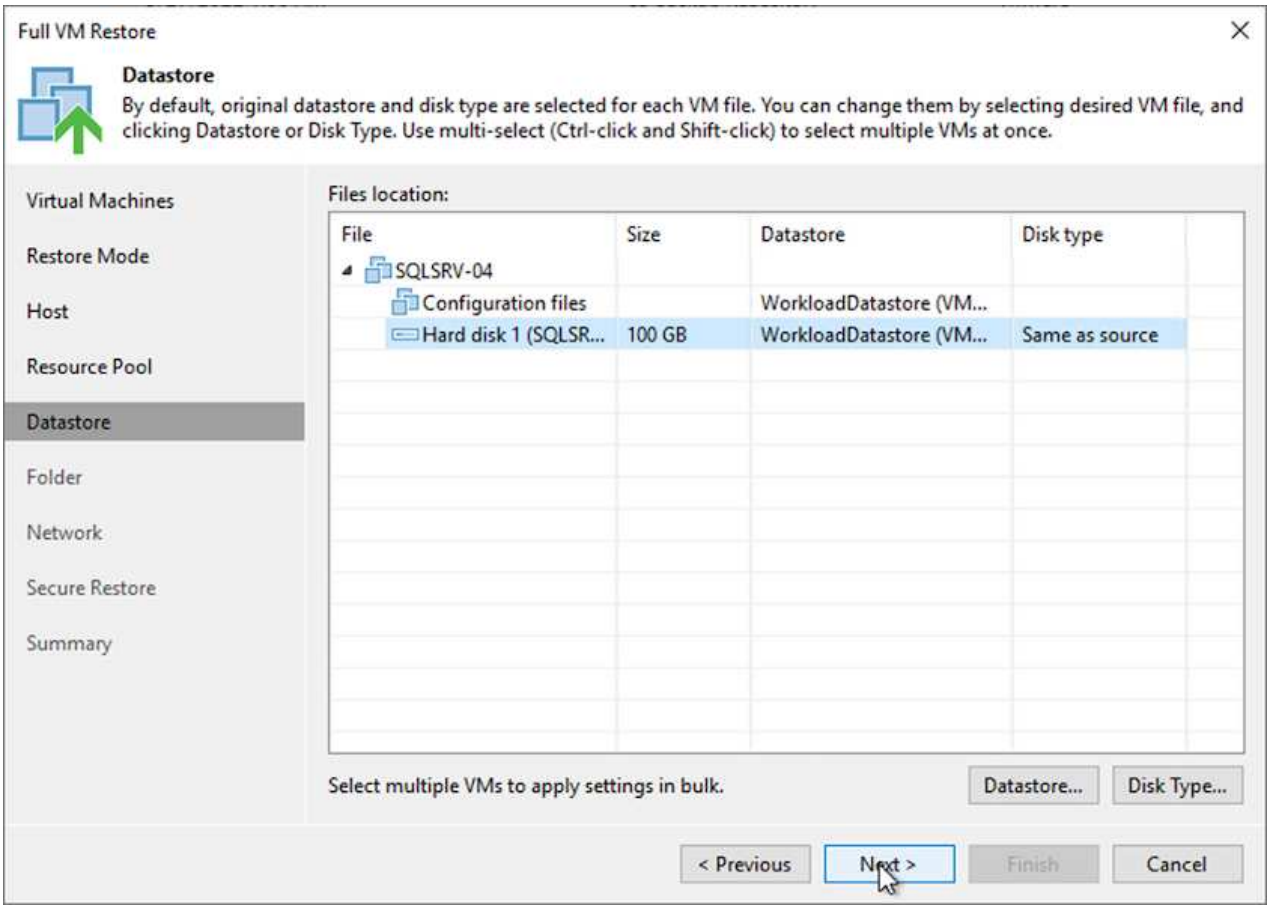
3. 在还原模式页面上、选择还原到新位置或使用不同设置。



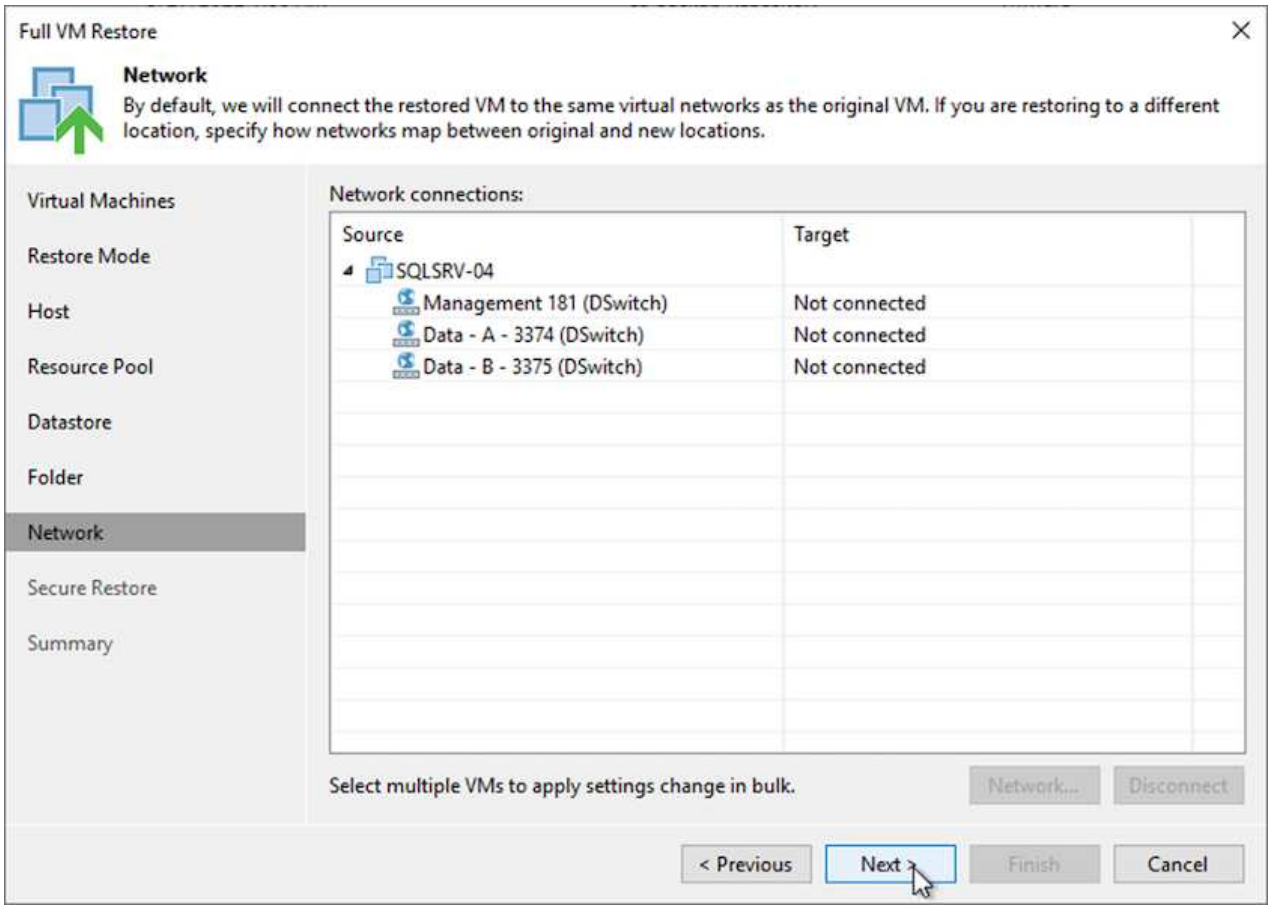
4. 在主机页面上、选择要将虚拟机还原到的目标ESXi主机或集群。

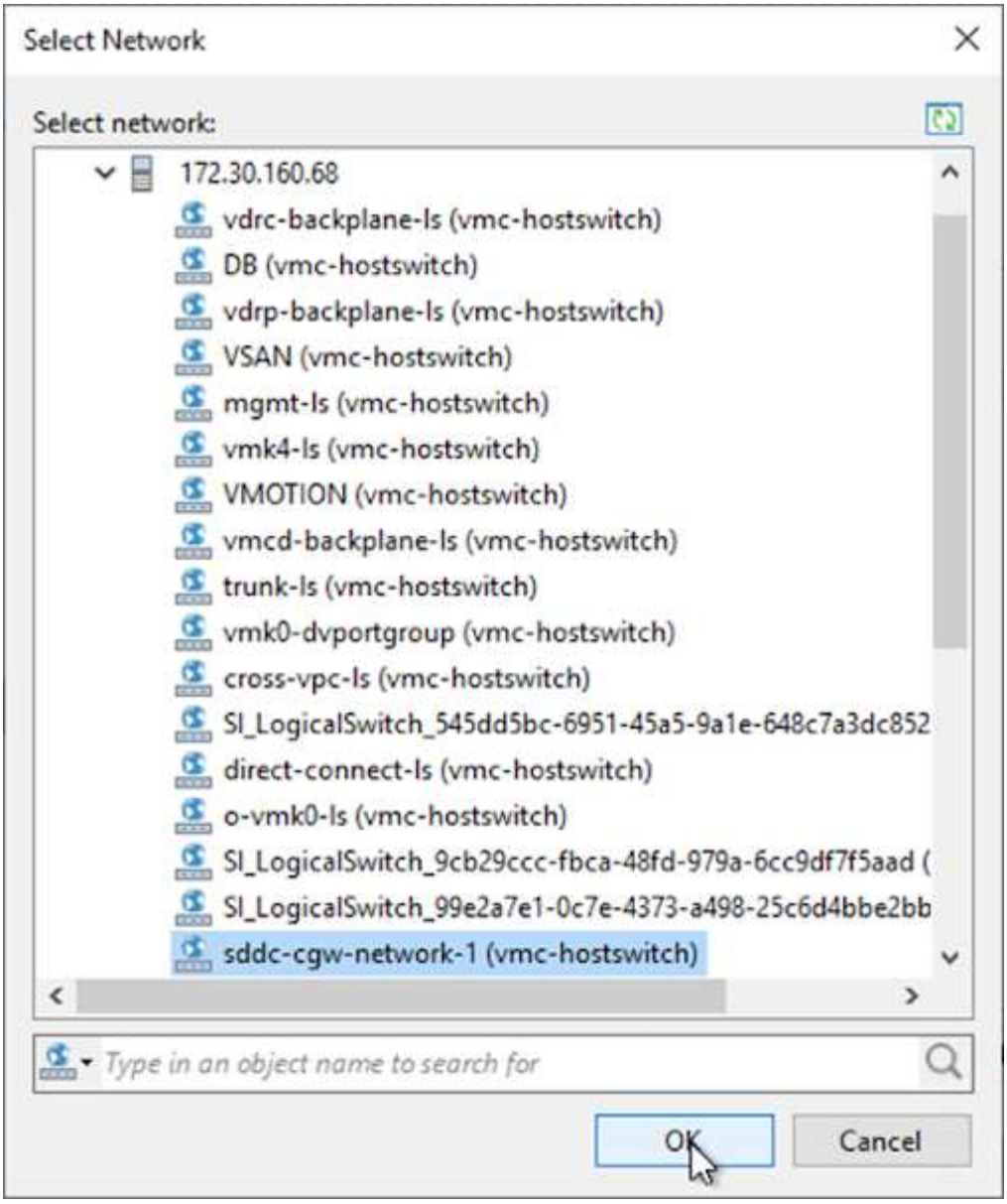


5. 在Datastores页面上、为配置文件和硬盘选择目标数据存储库位置。



6. 在网络页面上、将虚拟机上的原始网络映射到新目标位置中的网络。


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. 选择是否扫描已还原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还原。

还原**SQL Server**应用程序数据

以下过程提供了有关在发生灾难导致内部站点无法运行时如何在AWS的VMware云服务中恢复SQL Server的说明。

假定已完成以下前提条件、才能继续执行恢复步骤：

1. 已使用Veeam Full Restore将Windows Server VM还原到VMware Cloud SDDC。
2. 已建立二级SnapCenter 服务器、并已使用一节中所述的步骤完成SnapCenter 数据库还原和配置 "SnapCenter 备份和还原过程摘要。"

VM：SQL Server VM的还原后配置

虚拟机还原完成后、您必须配置网络连接和其他项目、以便在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文件中。

如果部署SnapCenter 插件时使用的域凭据与当前域不同、则必须在SQL Server VM上更改适用于Windows服务的插件的登录帐户。更改登录帐户后、重新启动SnapCenter SMCore、适用于Windows的插件和适用于SQL Server的插件服务。

要在SnapCenter 中自动重新发现还原的VM、FQDN必须与最初添加到内部SnapCenter 中的VM相同。

为SQL Server还原配置FSX存储

要完成SQL Server VM的灾难恢复还原过程、您必须断开与FSX集群的现有SnapMirror关系并授予对卷的访问权限。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命令行界面运行以下命令：

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

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

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

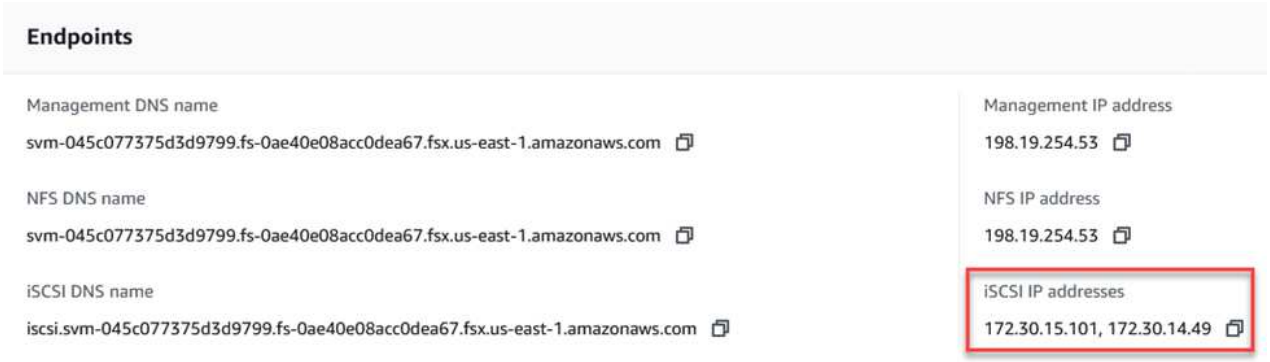
3. 最后、将LUN映射到刚刚创建的启动程序组：

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

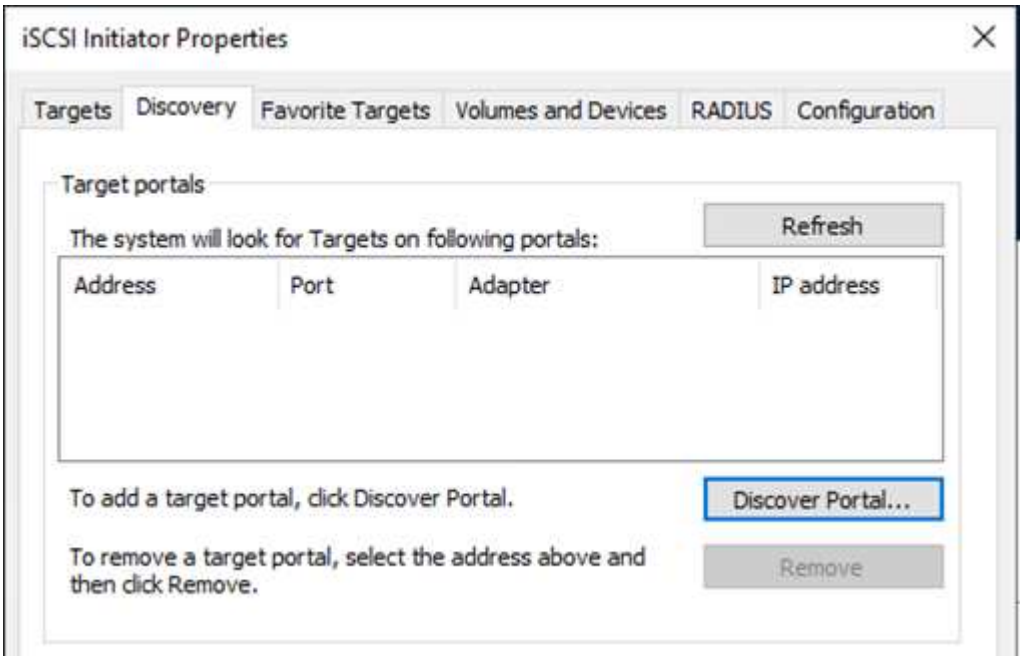
4. 要查找路径名称、请运行`lun show`命令。

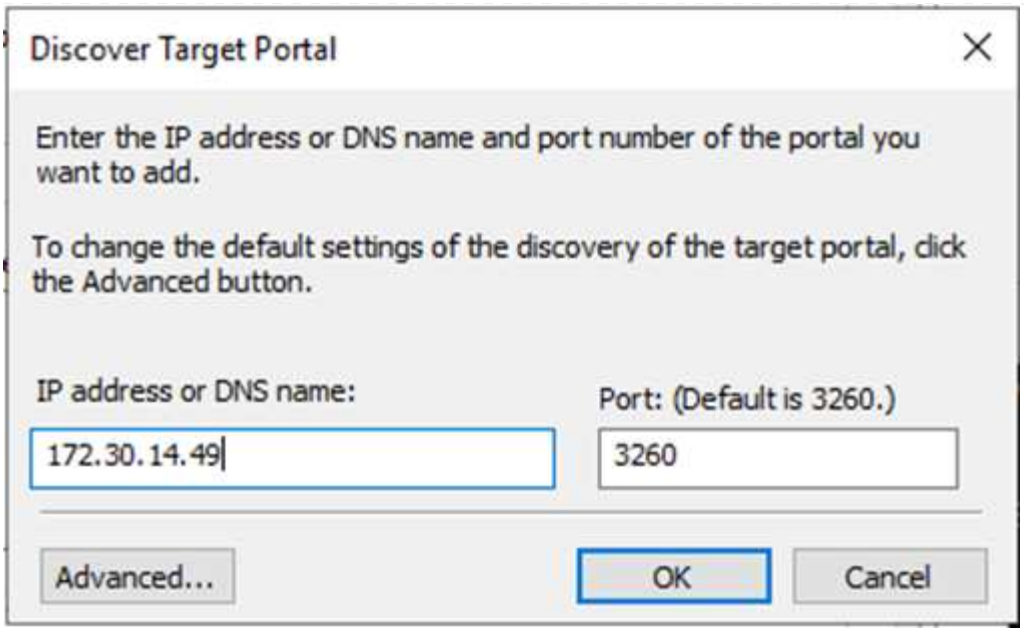
设置**Windows VM**以进行**iSCSI**访问并发现文件系统

1. 在SQL Server VM中、设置iSCSI网络适配器、以便在VMware端口组上进行通信、该端口组已建立、并可连接到FSX实例上的iSCSI目标接口。
2. 打开iSCSI启动程序属性实用程序、并清除发现、收藏的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。您可以在AWS控制台中的Amazon FSx > ONTAP > Storage Virtual Machine下找到此选项。

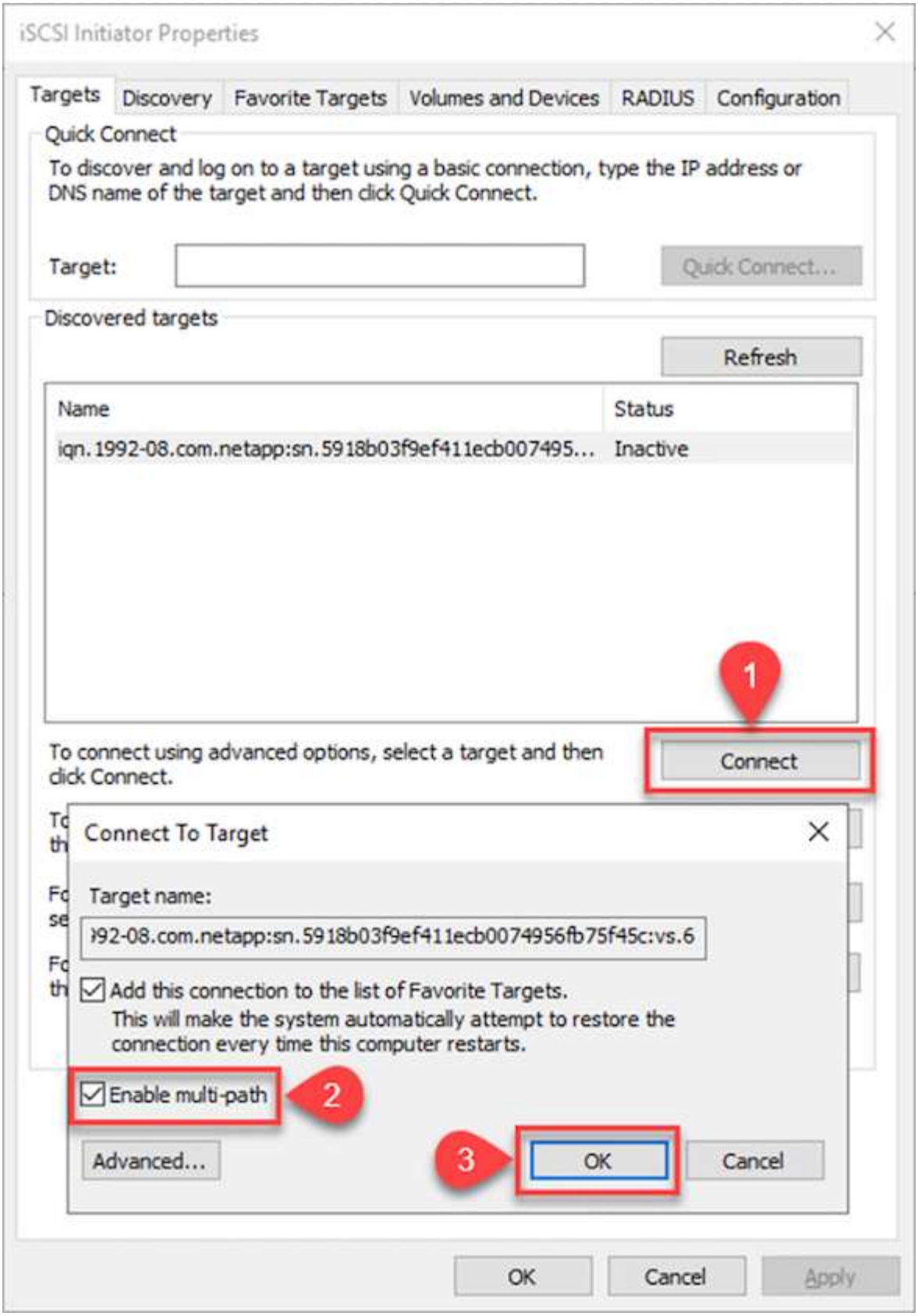


4. 在发现选项卡中、单击发现门户、然后输入FSX iSCSI目标的IP地址。

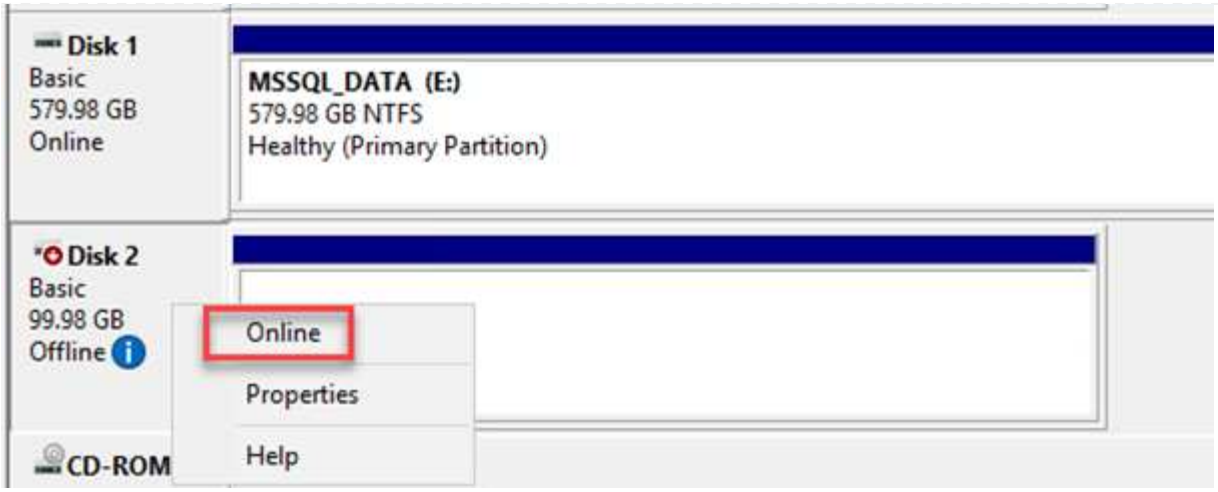




5. 在目标选项卡上、单击连接、根据您的配置选择启用多路径、然后单击确定连接到目标。

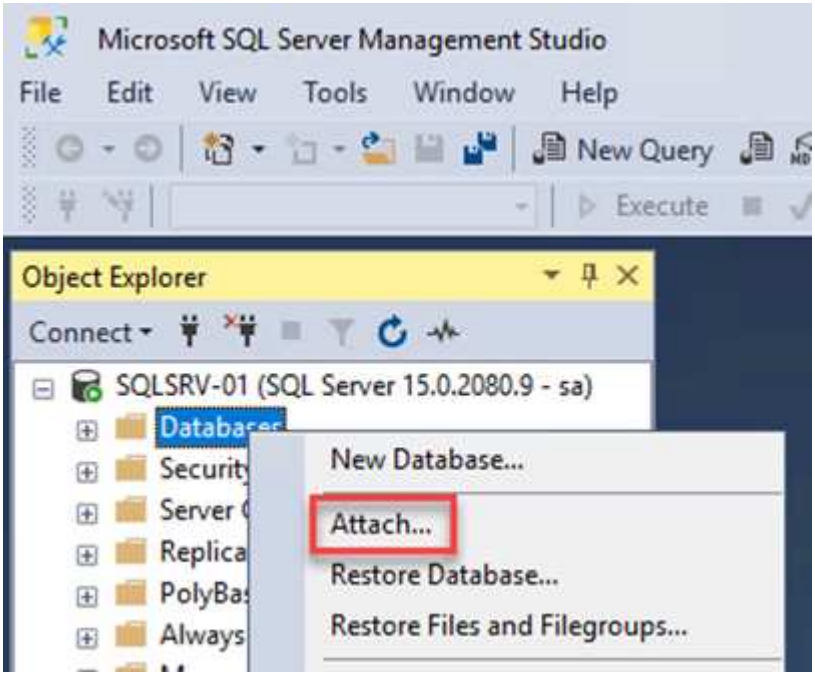


6. 打开计算机管理实用程序并使磁盘联机。确认它们保留的驱动器号与先前相同。

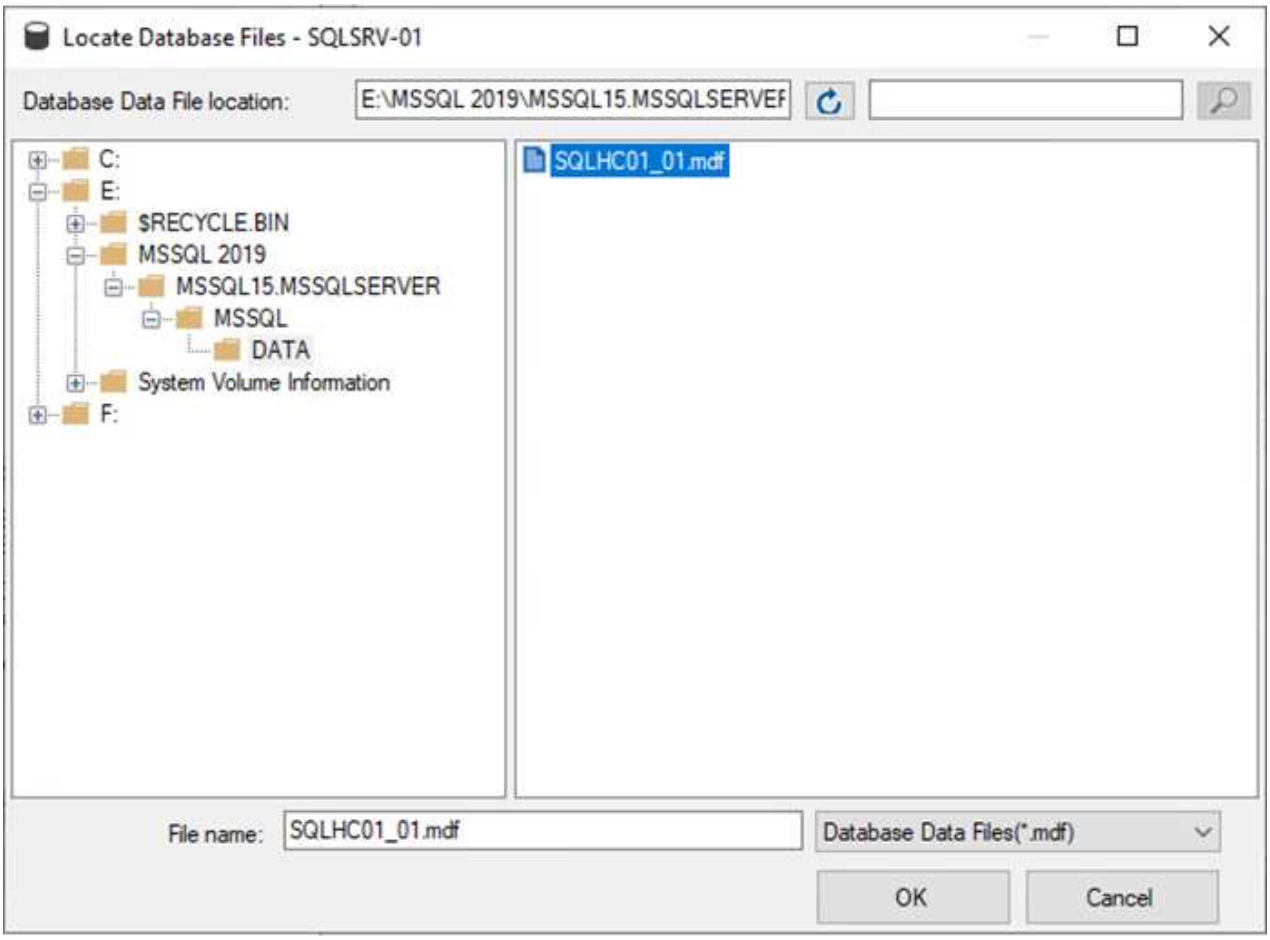

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

连接**SQL Server**数据库

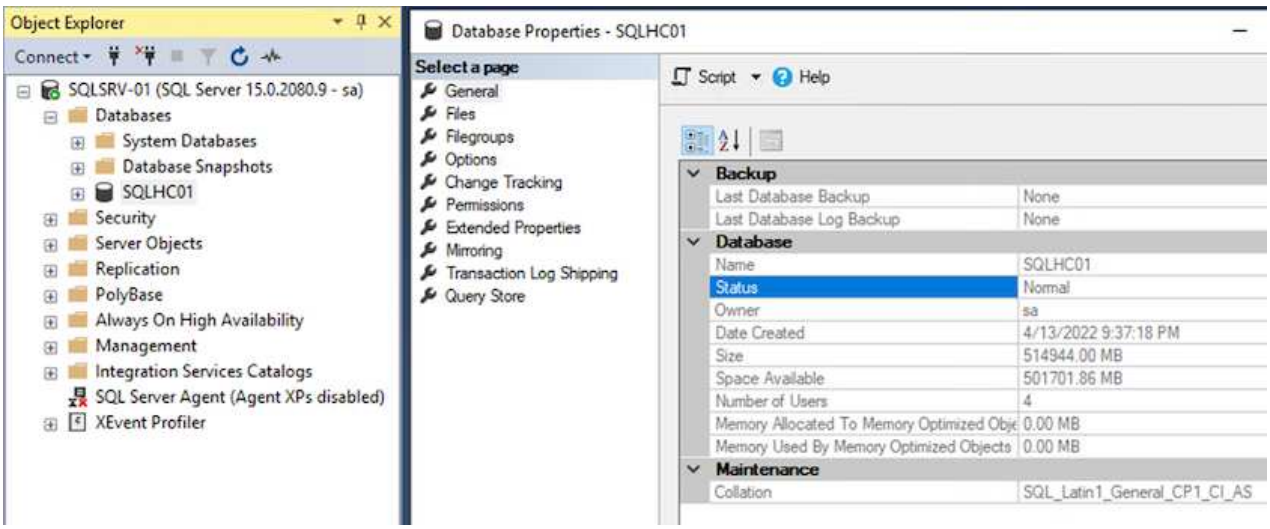
1. 从SQL Server VM中、打开Microsoft SQL Server Management Studio并选择Attach以开始连接到数据库的过程。



2. 单击添加并导航到包含SQL Server主数据库文件的文件夹、将其选中、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、单击确定以连接数据库。

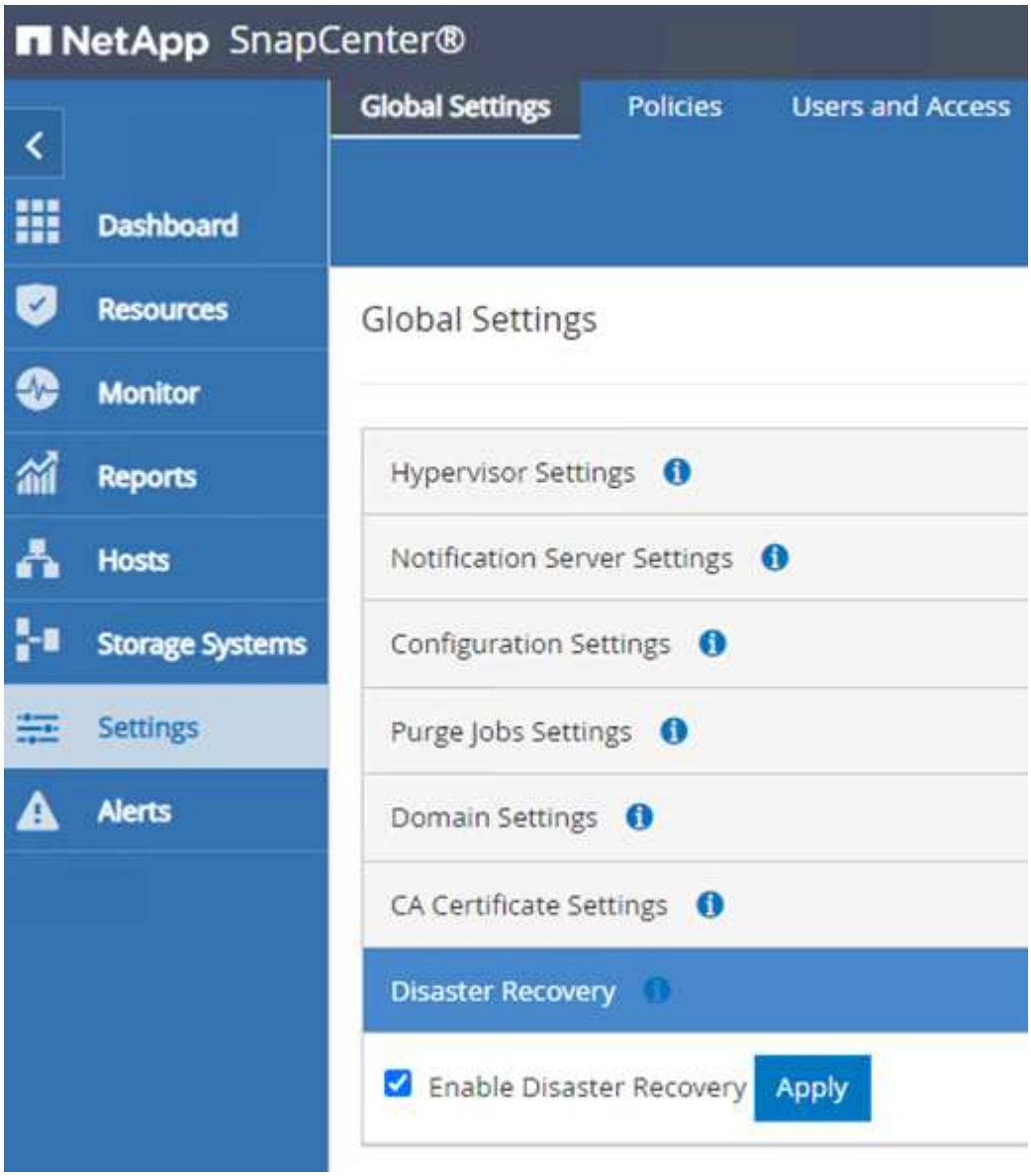


确认**SnapCenter** 与**SQL Server**插件的通信

将SnapCenter 数据库还原到其先前状态后、它会自动重新发现SQL Server主机。要使此操作正常运行、请记住以下前提条件：

- 必须将SnapCenter 置于灾难恢复模式。可以通过Swagger API或Disaster Recovery下的Global Settings实现此目的。
- SQL Server的FQDN必须与内部数据中心中运行的实例相同。
- 必须断开原始SnapMirror关系。
- 必须将包含数据库的LUN挂载到SQL Server实例、并连接数据库。

要确认SnapCenter 处于灾难恢复模式、请在SnapCenter Web客户端中导航到设置。转到全局设置选项卡、然后单击灾难恢复。确保启用"启用灾难恢复"复选框。



还原**Oracle**应用程序数据

以下过程提供了有关在发生灾难导致内部站点无法运行时如何在AWS的VMware云服务中恢复Oracle应用程序数据的说明。

完成以下前提条件以继续执行恢复步骤：

1. Oracle Linux服务器VM已使用Veeam Full Restore还原到VMware Cloud SDDC。
2. 已建立二级SnapCenter 服务器、并已使用本节所述的步骤还原SnapCenter 数据库和配置文件 "SnapCenter 备份和还原过程摘要。"

为Oracle还原配置FSX—中断SnapMirror关系

要使FSxN实例上托管的二级存储卷可供Oracle服务器访问、必须先中断现有的SnapMirror关系。

1. 登录到FSX命令行界面后、运行以下命令以查看使用正确名称筛选的卷。

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

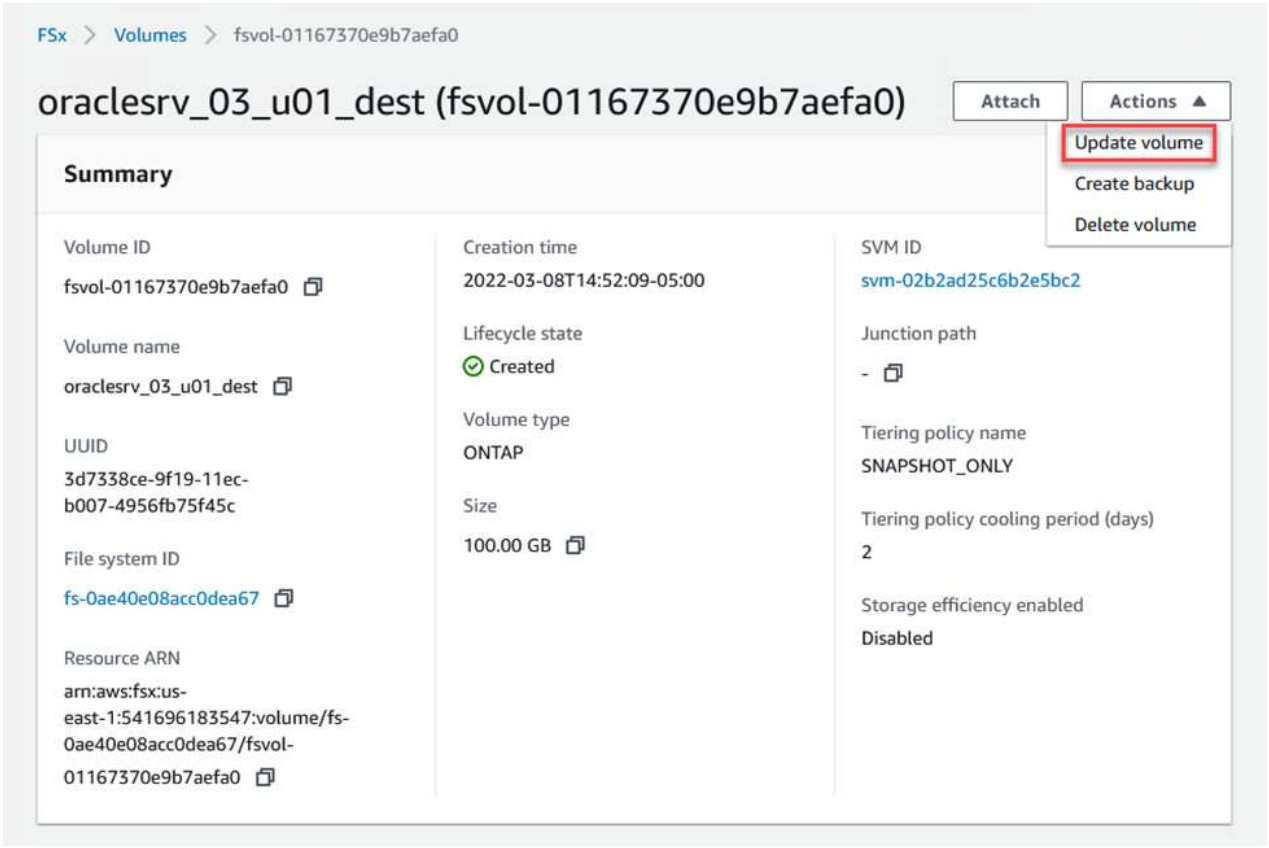
```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        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. 运行以下命令以中断现有SnapMirror关系。

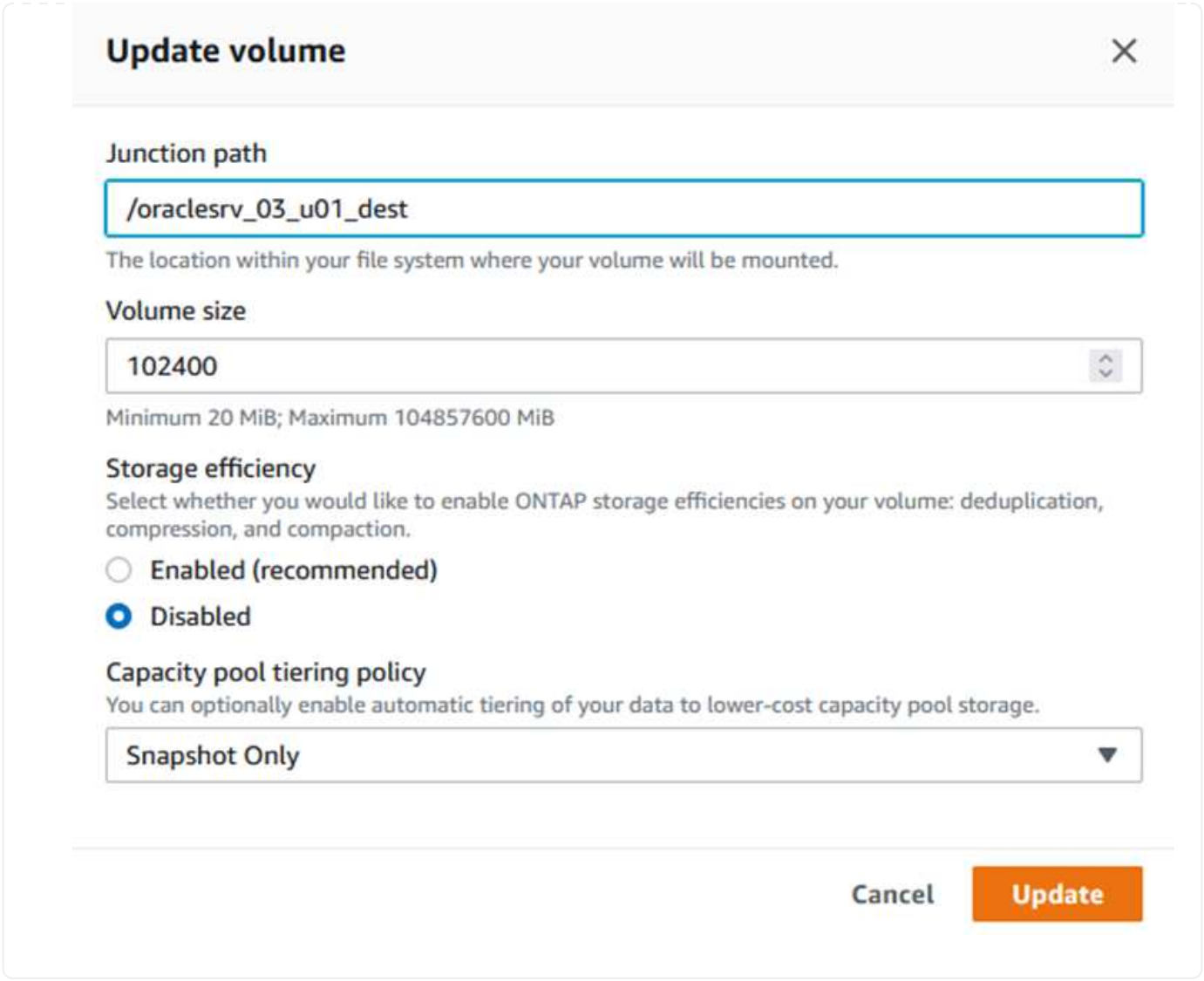
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
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客户端中的接合路径：



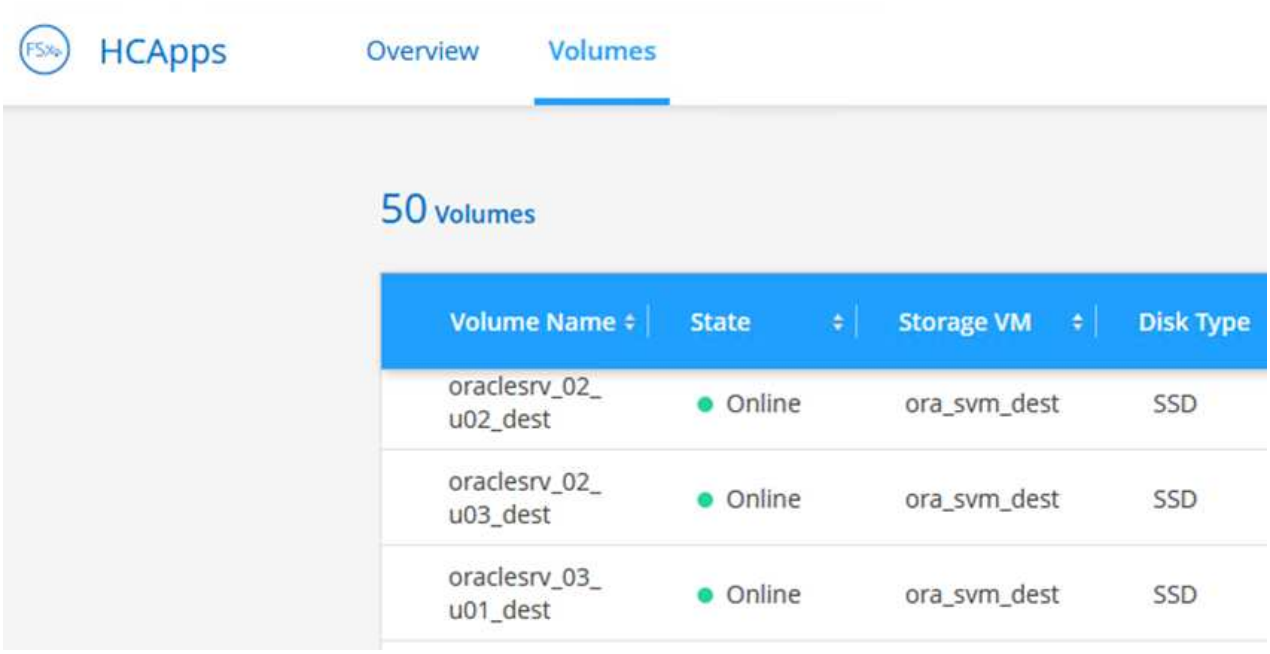
4. 添加接合路径名称、然后单击更新。从Oracle服务器挂载NFS卷时、请指定此接合路径。


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

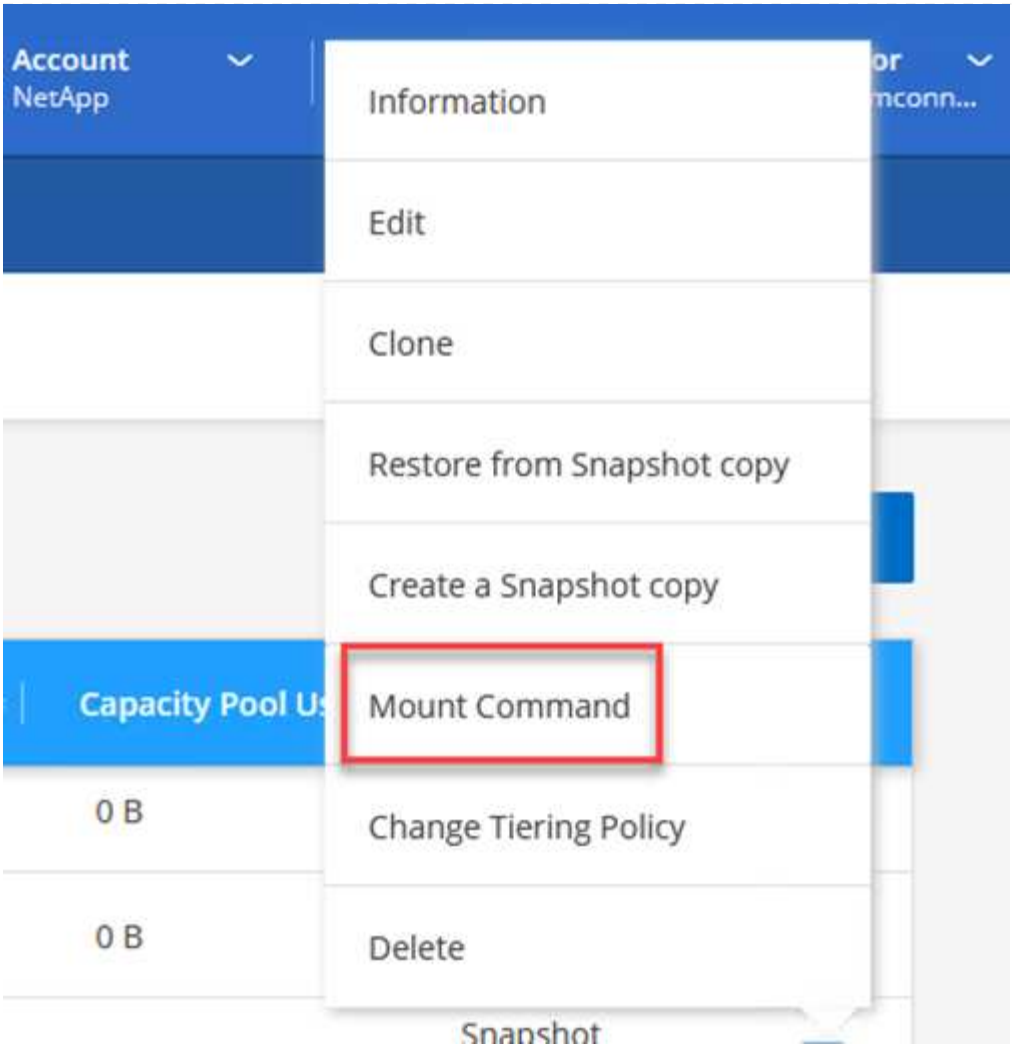
在**Oracle Server**上挂载**NFS**卷

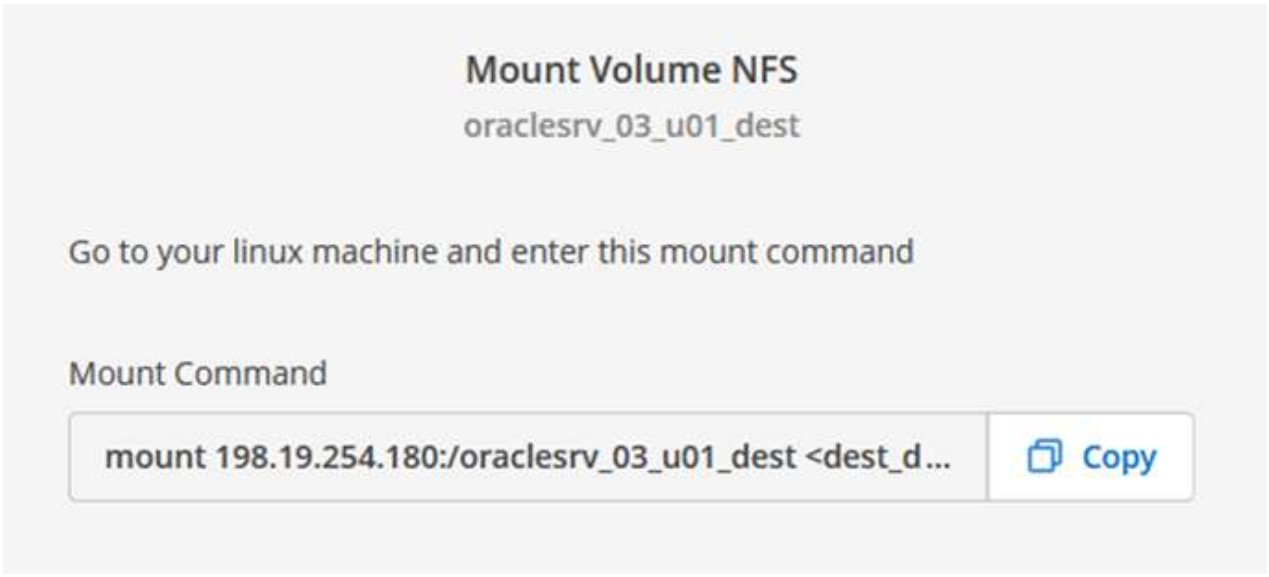
在Cloud Manager中、您可以使用正确的NFS LIF IP地址获取mount命令、以便挂载包含Oracle数据库文件和日志的NFS卷。

1. 在Cloud Manager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并复制要在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 Server。Oracle Linux主机上已存在用于挂载NFS共享的目录。
4. 在Oracle Linux服务器上、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。

要在重新启动时使NFS挂载持久、请编辑`/etc/fstab`文件以包含mount命令。

5. 重新启动Oracle服务器。Oracle数据库应正常启动并可供使用。

故障恢复

成功完成此解决方案 中所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、而适用于ONTAP 的FSX现在已指定为主存储、并且与原始内部数据中心没有SnapMirror关系。在内部恢复正常功能后、您可以使用与本文档所述过程相同的过程将数据镜像回内部ONTAP 存储系统。

如本文档中所述、您还可以配置SnapCenter 、以便将应用程序数据卷从适用于ONTAP 的FSx镜像到驻留在内部的ONTAP 存储系统。同样、您也可以将Veeam配置为使用横向扩展备份存储库将备份副本复制到Amazon S3、以便驻留在内部数据中心的Veeam备份服务器可以访问这些备份。

故障恢复不在本文档的讨论范围内、但故障恢复与此处所述的详细过程差别不大。

结论

本文档中介绍的使用情形侧重于经过验证的灾难恢复技术、这些技术突出了NetApp与VMware之间的集成。NetApp ONTAP 存储系统提供经验证的数据镜像技术、使企业能够设计涵盖领先云提供商所采用的内部和ONTAP 技术的灾难恢复解决方案。

AWS上的ONTAP FSX就是这样一种解决方案 、它可以与SnapCenter 和SyncMirror 无缝集成、以便将应用程序数据复制到云。Veeam备份和复制是另一项众所周知的技术、可与NetApp ONTAP 存储系统完美集成、并可提供到vSphere原生 存储的故障转移。

此解决方案 使用托管SQL Server和Oracle应用程序数据的ONTAP 系统中的子系统连接存储提供了一个灾难恢复解决方案。采用SnapMirror的SnapCenter 提供了一个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 是一种支持灾难恢复的解决方案 、用于将所有应用程序数据故障转移到AWS上的VMware Cloud。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- 指向解决方案 文档的链接

  "采用VMware解决方案的NetApp混合多云"

  "NetApp 解决方案"

VMware Cloud中的**Veeam**备份和还原、采用**Amazon FSx for ONTAP**

作者：Jsh Powell—NetApp解决方案工程部

概述

Veeam Backup & Replication是一款高效可靠的解决方案 、用于保护VMware Cloud中的数据。此解决方案 演示了使用Veeam备份和复制在VMware Cloud中备份和还原FSx for ONTAP NFS数据存储库上的应用程序VM的正确设置和配置。

VMware Cloud (在AWS中)支持使用NFS数据存储库作为补充存储、而FSx for NetApp ONTAP 是一款安全解决方案 、适用于需要为云应用程序存储大量数据的客户、该数据存储库可以独立于SDDC集群中的ESXi主机数量进行扩展。这项集成的AWS存储服务可提供具有所有传统NetApp ONTAP 功能的高效存储。

用例

此解决方案 可解决以下使用情形：

- 使用FSx for NetApp ONTAP 作为备份存储库、备份和还原VMC中托管的Windows和Linux虚拟机。
- 使用FSx for NetApp ONTAP 作为备份存储库来备份和还原Microsoft SQL Server应用程序数据。
- 使用FSx for NetApp ONTAP 作为备份存储库来备份和还原Oracle应用程序数据。

使用**Amazon FSx for ONTAP** 的**NFS**数据存储库

此解决方案 中的所有虚拟机都位于FSx上、用于ONTAP 补充NFS数据存储库。使用FSx for ONTAP 作为补充NFS数据存储库具有若干优势。例如、它允许您：

- 在云中创建可扩展且高度可用的文件系统、而无需复杂的设置和管理。
- 与现有VMware环境集成、支持您使用熟悉的工具和流程来管理云资源。
- 利用ONTAP 提供的高级数据管理功能(例如快照和复制)保护数据并确保其可用性。

解决方案 部署概述

此列表简要介绍了配置Veeam备份和复制、使用FSx for ONTAP 作为备份存储库执行备份和还原作业以及还原SQL Server和Oracle VM和数据库所需的步骤：

1. 创建FSx for ONTAP 文件系统、用作Veeam Backup & Replication的iSCSI备份存储库。
2. 部署Veeam代理以分布备份工作负载并挂载FSx for ONTAP 上托管的iSCSI备份存储库。
3. 配置Veeam备份作业以备份SQL Server、Oracle、Linux和Windows虚拟机。
4. 还原SQL Server虚拟机和各个数据库。
5. 还原Oracle虚拟机和各个数据库。

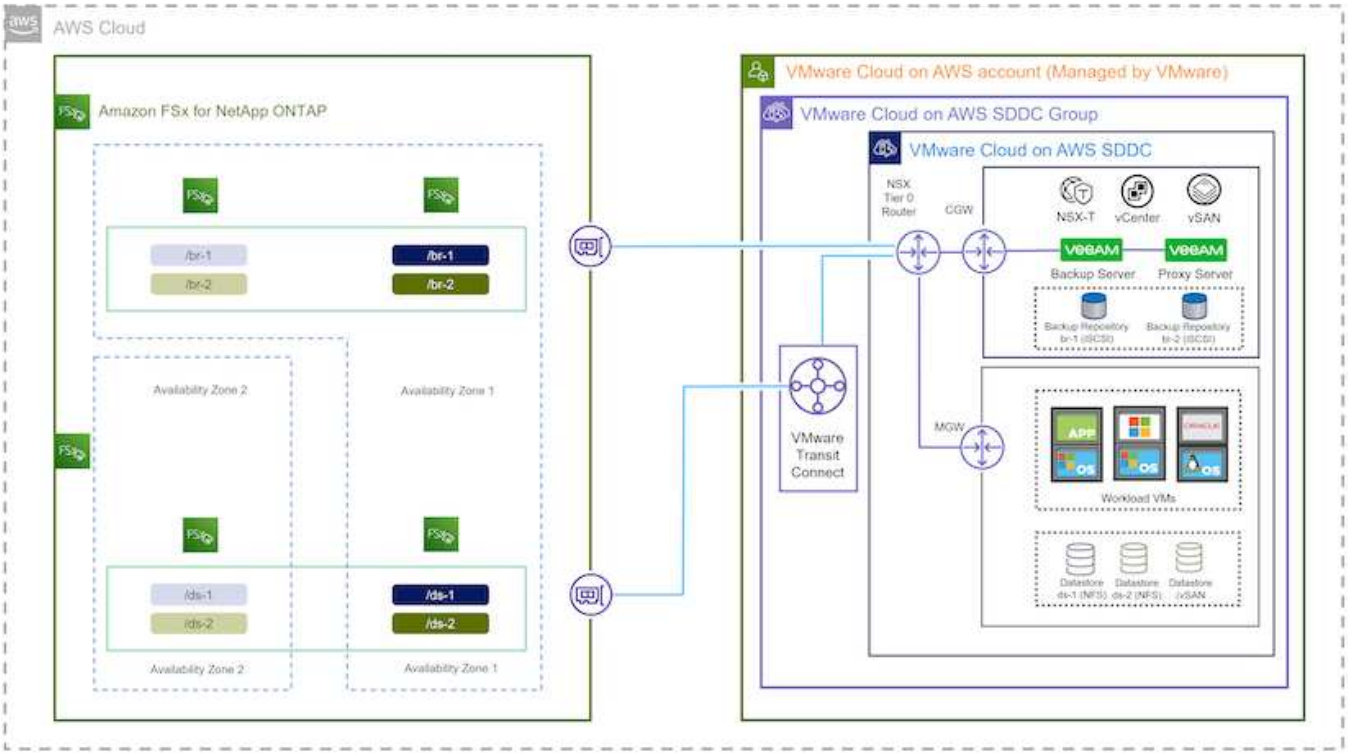
前提条件

本解决方案 的目的是演示在VMware Cloud中运行的虚拟机以及由FSx for NetApp ONTAP 托管的NFS数据存储库中的虚拟机的数据保护。此解决方案 假定已配置以下组件并可供使用：

1. 一个或多个NFS数据存储库连接到VMware Cloud的FSx for 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 Server。
3. 在解决方案 部署期间、要与Veeam备份代理组件一起安装的Microsoft Windows Server VM。
4. VMDK和应用程序数据驻留在FSx for ONTAP NFS数据存储库上的Microsoft SQL Server VM。对于此解决方案 、我们在两个单独的VMDK上有两个SQL数据库。
   - 注意：作为最佳实践、数据库和事务日志文件应放置在单独的驱动器上、因为这样可以提高性能和可靠性。这部分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. 包含VMDK和应用程序数据的Oracle数据库VM驻留在FSx上、用于ONTAP NFS数据存储库。
6. VMDK驻留在FSx上的Linux和Windows文件服务器VM、用于ONTAP NFS数据存储库。
7. Veeam需要使用特定的TCP端口在备份环境中的服务器和组件之间进行通信。在Veeam备份基础架构组件上、系统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、请参阅的端口部分 "适用于VMware vSphere的Veeam备份和复制用户指南"。

高级架构

此解决方案 的测试/验证是在可能与最终部署环境匹配或可能不匹配的实验室中执行的。有关详细信息、请参见以下各节。



硬件/软件组件

本解决方案 的目的是演示在VMware Cloud中运行的虚拟机以及由FSx for NetApp ONTAP 托管的NFS数据存储库中的虚拟机的数据保护。此解决方案 假定已配置以下组件并可供使用：

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

解决方案 部署

在本解决方案 中、我们详细说明了如何使用Veeam备份和复制软件部署和验证解决方案 、以便在AWS上的VMware Cloud SDDC中对SQL Server、Oracle以及Windows和Linux文件服务器虚拟机执行备份和恢复。此解决方案 中的虚拟机位于FSx for ONTAP 托管的补充NFS数据存储库中。此外、还会使用一个单独的FSx for ONTAP 文件系统来托管要用于Veeam备份存储库的iSCSI卷。

我们将通过FSx创建ONTAP 文件系统、挂载要用作备份存储库的iSCSI卷、创建和运行备份作业以及执行VM和数据库还原。

有关FSx for NetApp ONTAP 的详细信息、请参见 "FSx for ONTAP 用户指南"。

有关Veeam备份和复制的详细信息、请参见 "Veeam帮助中心技术文档" 站点

有关将Veeam Backup and Replication与VMware Cloud on AWS结合使用时的注意事项和限制、请参见 "基于AWS的VMware Cloud和基于Dell EMC支持的VMware Cloud。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、充当源与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、请务必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的规模估算及其系统要求、请参见 "Veeam VMware vSphere最佳实践指南"。

Veeam Data Mover是Veeam代理服务器的一个组件、它利用传输模式从源获取VM数据并将其传输到目标。传输模式是在配置备份作业期间指定的。通过使用直接存储访问、可以提高从NFS数据存储库备份的效率。

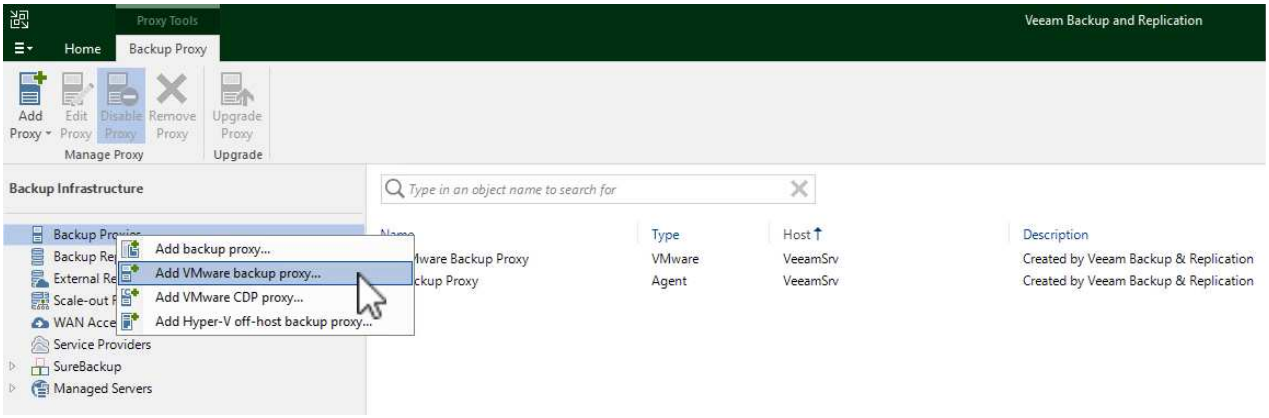
有关运输模式的详细信息、请参阅 "适用于VMware vSphere的Veeam备份和复制用户指南"。

在下面的步骤中、我们将介绍如何在VMware Cloud SDDC中的Windows VM上部署Veeam代理服务器。

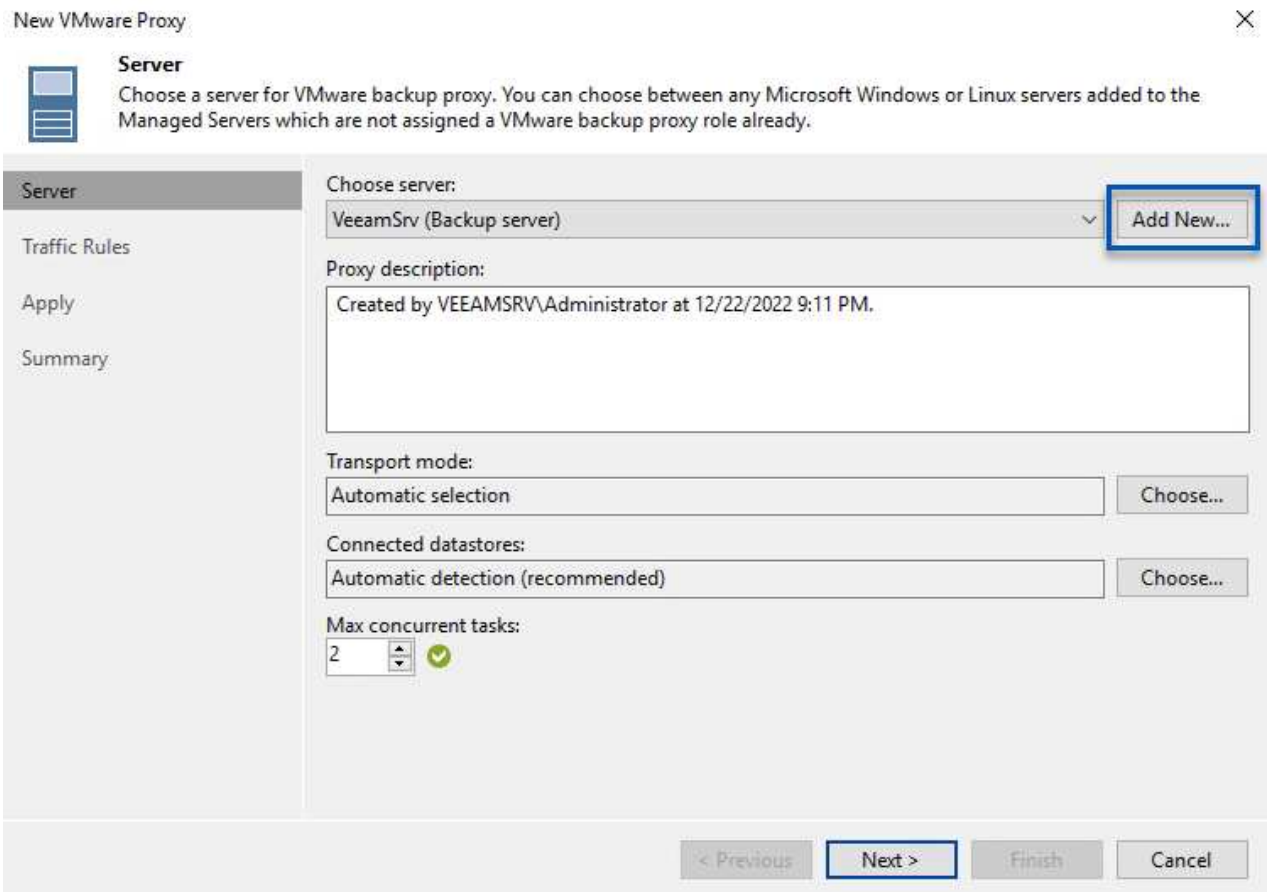
部署**Veeam**代理以分布备份工作负载

在此步骤中、Veeam代理将部署到现有Windows VM。这样便可在主Veeam备份服务器和Veeam代理之间分布备份作业。

1. 在Veeam Backup and Replication服务器上、打开管理控制台并选择左下方菜单中的*备份基础架构*。
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。

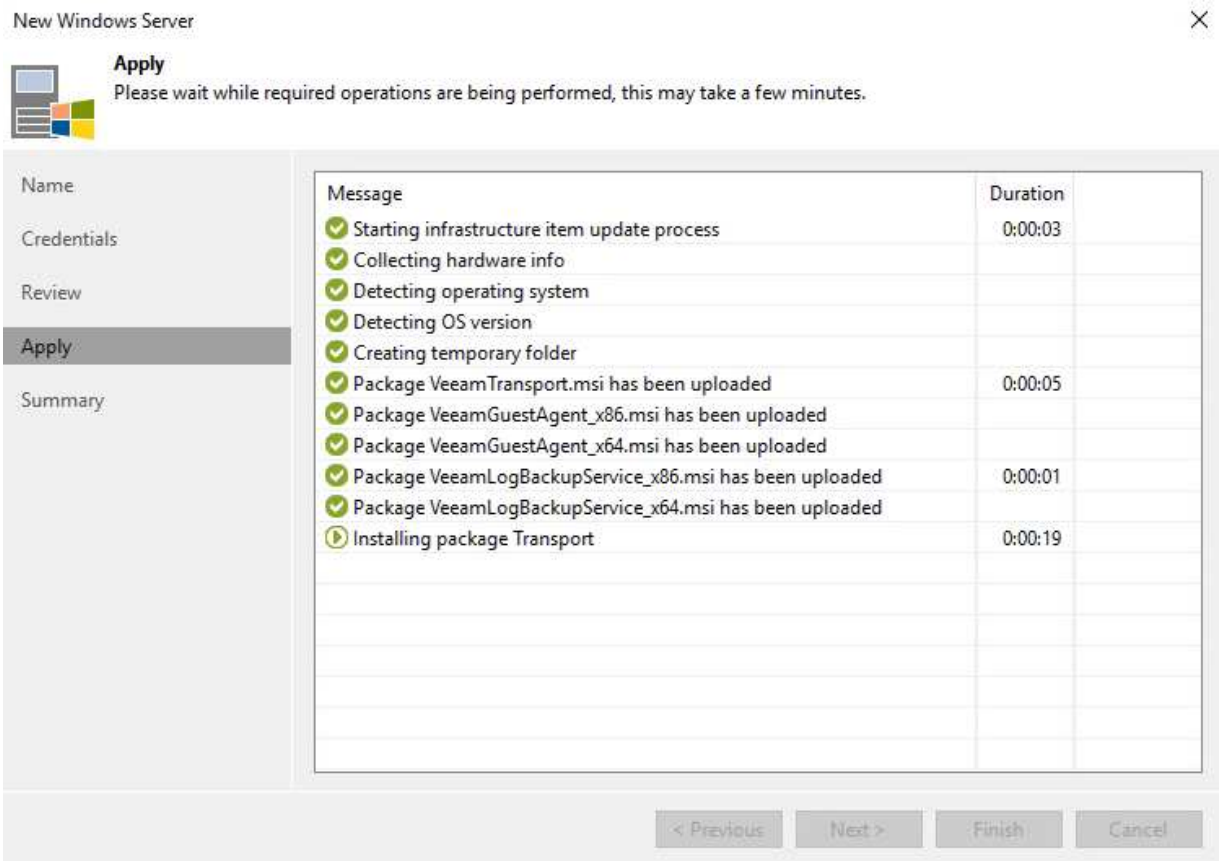


3. 在*Add VMware Proxy*向导中，单击*Add New…*按钮以添加新的代理服务器。

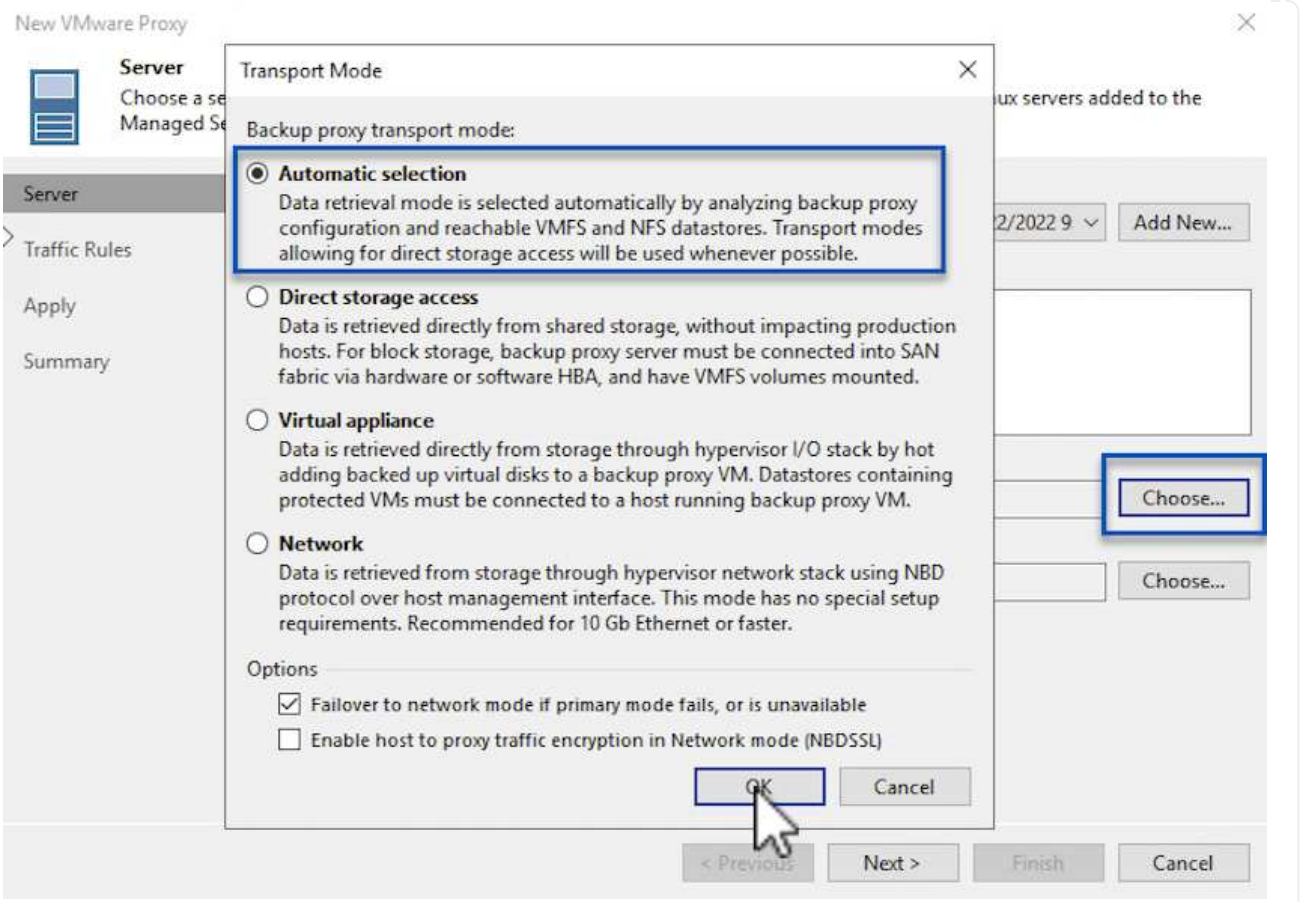


4. 选择以添加Microsoft Windows、然后按照提示添加服务器：
   - 填写DNS名称或IP地址

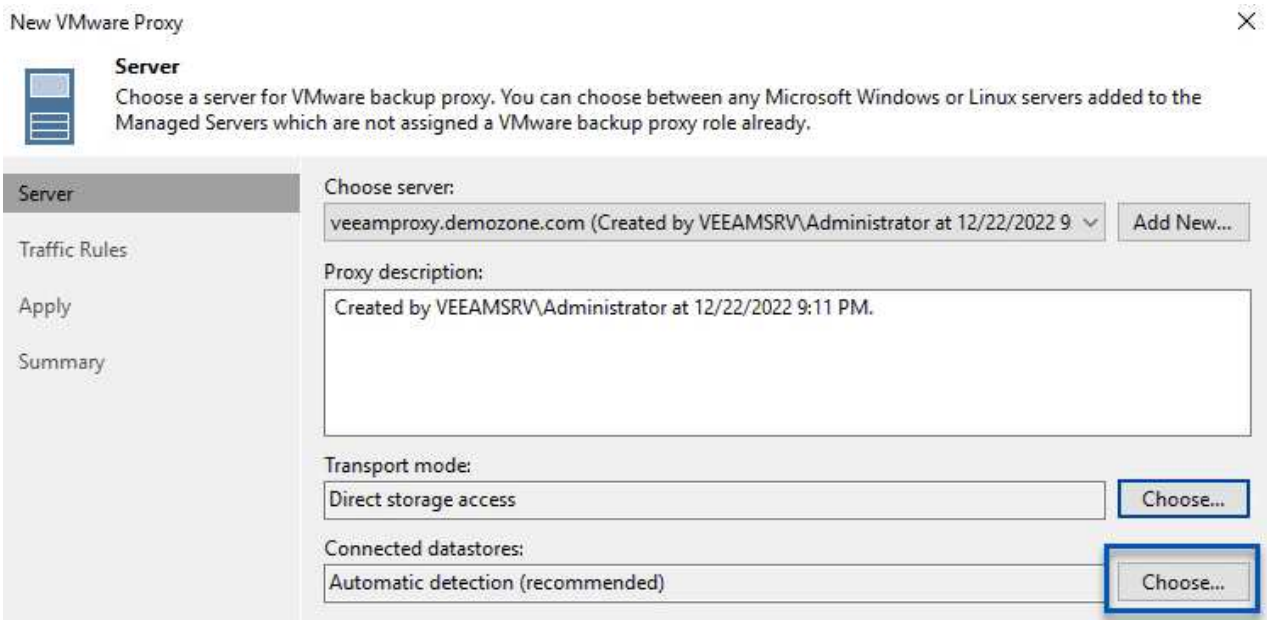
- 选择要用于新系统上的凭据的帐户或添加新凭据
- 查看要安装的组件，然后单击*Apply*开始部署

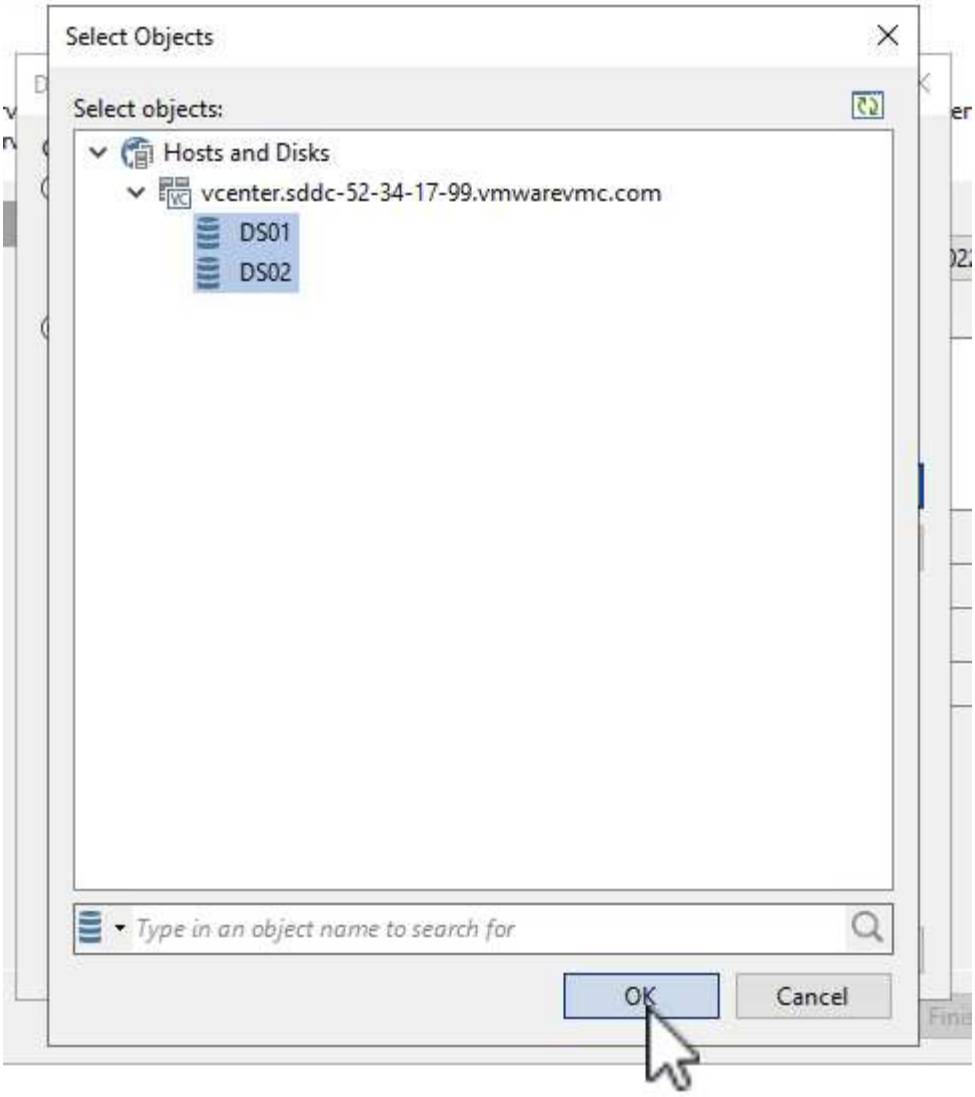


5. 返回“新建**VMware**代理”向导，选择传输模式。在本例中，我们选择了*自动选择*。

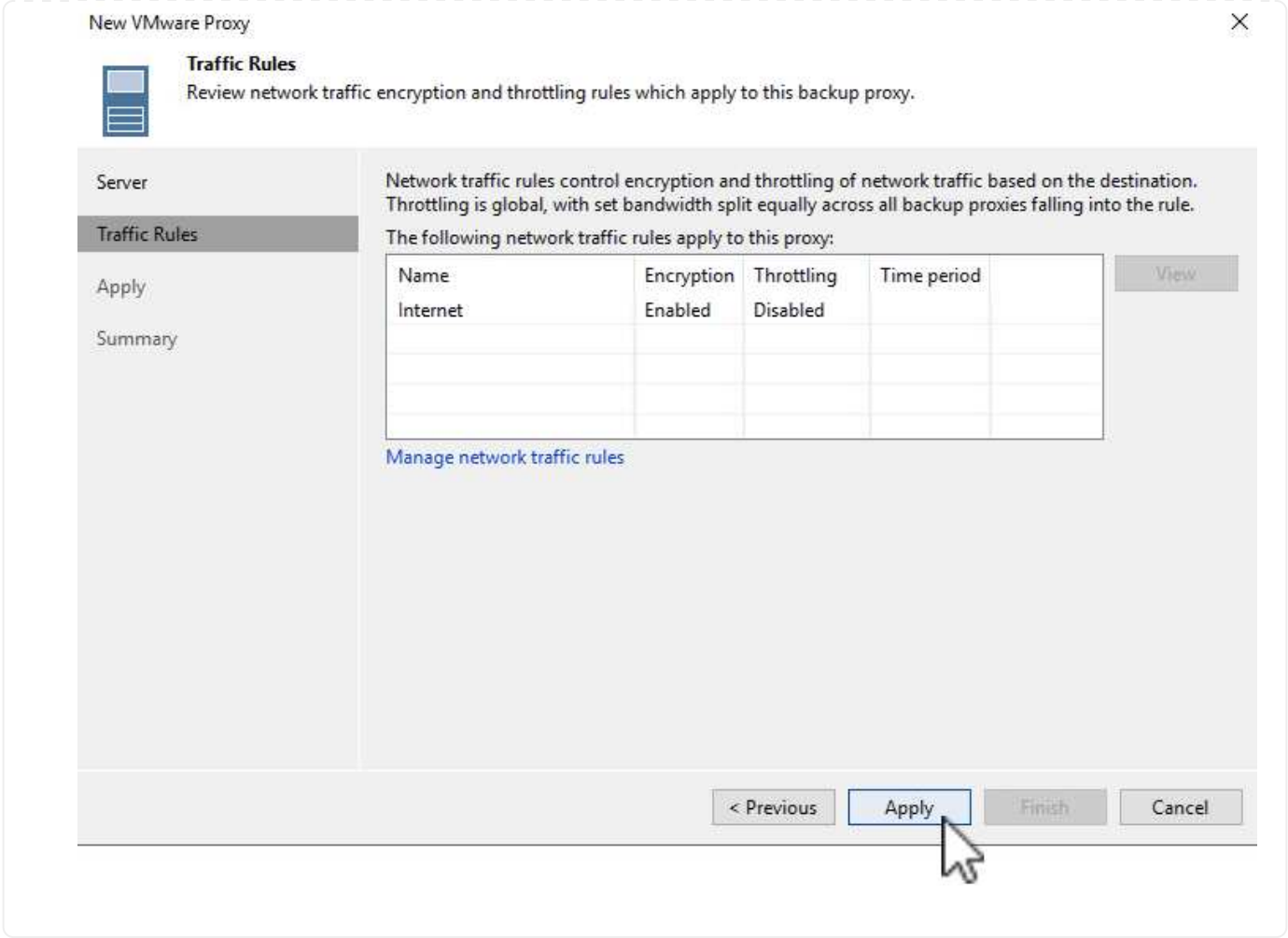


6. 选择希望VMware代理直接访问的已连接数据存储库。





7. 根据需要配置和应用任何特定网络流量规则、例如加密或限制。完成后，单击*Apply*按钮完成部署。



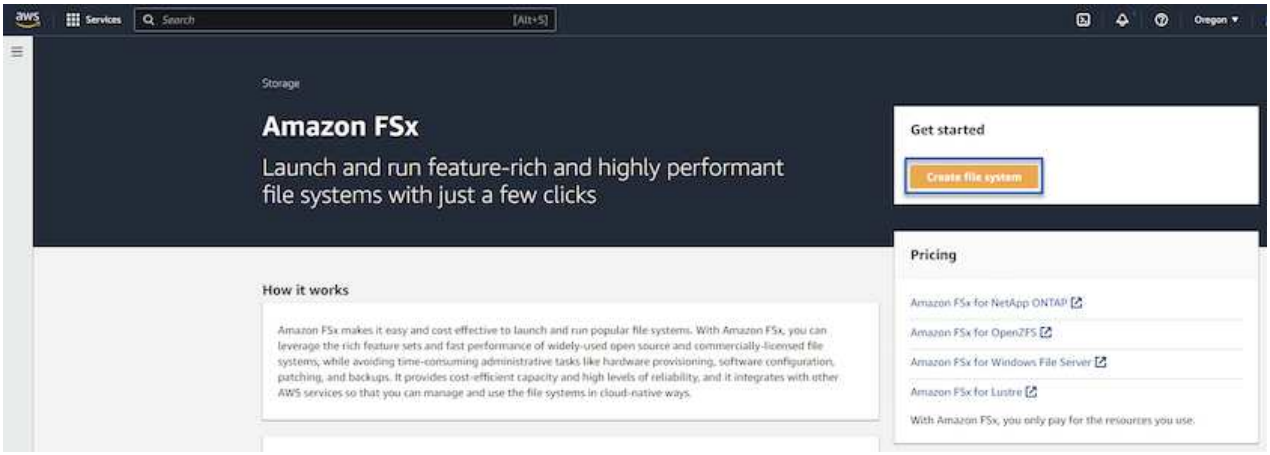
配置存储和备份存储库

主Veeam备份服务器和Veeam代理服务器可访问直连存储形式的备份存储库。在本节中、我们将介绍如何创建适用于ONTAP 文件系统的FSx、如何将iSCSI LUN挂载到Veeam服务器以及如何创建备份存储库。

为ONTAP 文件系统创建FSx

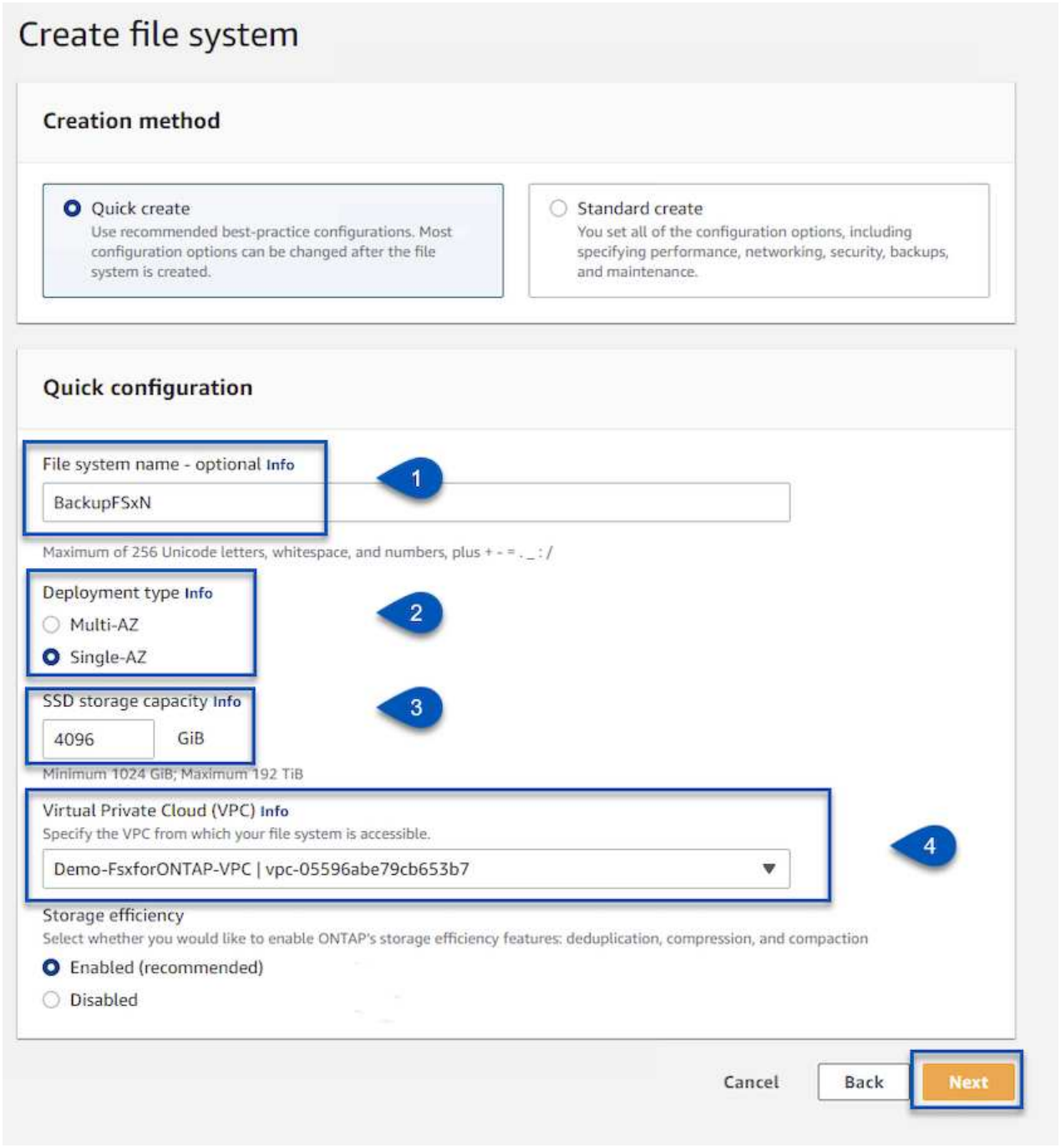
创建FSx for ONTAP 文件系统、用于托管Veeam备份存储库的iSCSI卷。

1. 在AWS控制台中，转到FSx，然后选择*Create file system*



2. 选择*Amazon FSx for NetApp ONTAP FS*，然后选择*Next*继续。

3. 填写文件系统名称、部署类型、SSD存储容量以及FSx for ONTAP 集群将驻留的VPC。此VPC必须配置为与VMware Cloud中的虚拟机网络进行通信。单击“下一步”。



4. 查看部署步骤，然后单击*Create File System*开始文件系统创建过程。

配置和挂载iSCSI LUN

在FSx for ONTAP 上创建和配置iSCSI LUN、然后挂载到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 for ONTAP 上创建iSCSI LUN是一个多步骤过程。创建卷的第一步可以在Amazon FSx控制台中完成、也可以使用NetApp ONTAP 命令行界面完成。

> 有关使用FSx for ONTAP 的详细信息、请参见 "FSx for ONTAP 用户指南"。

1. 在NetApp ONTAP 命令行界面中、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. 使用上一步中创建的卷创建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的启动程序组来授予对LUN的访问权限：

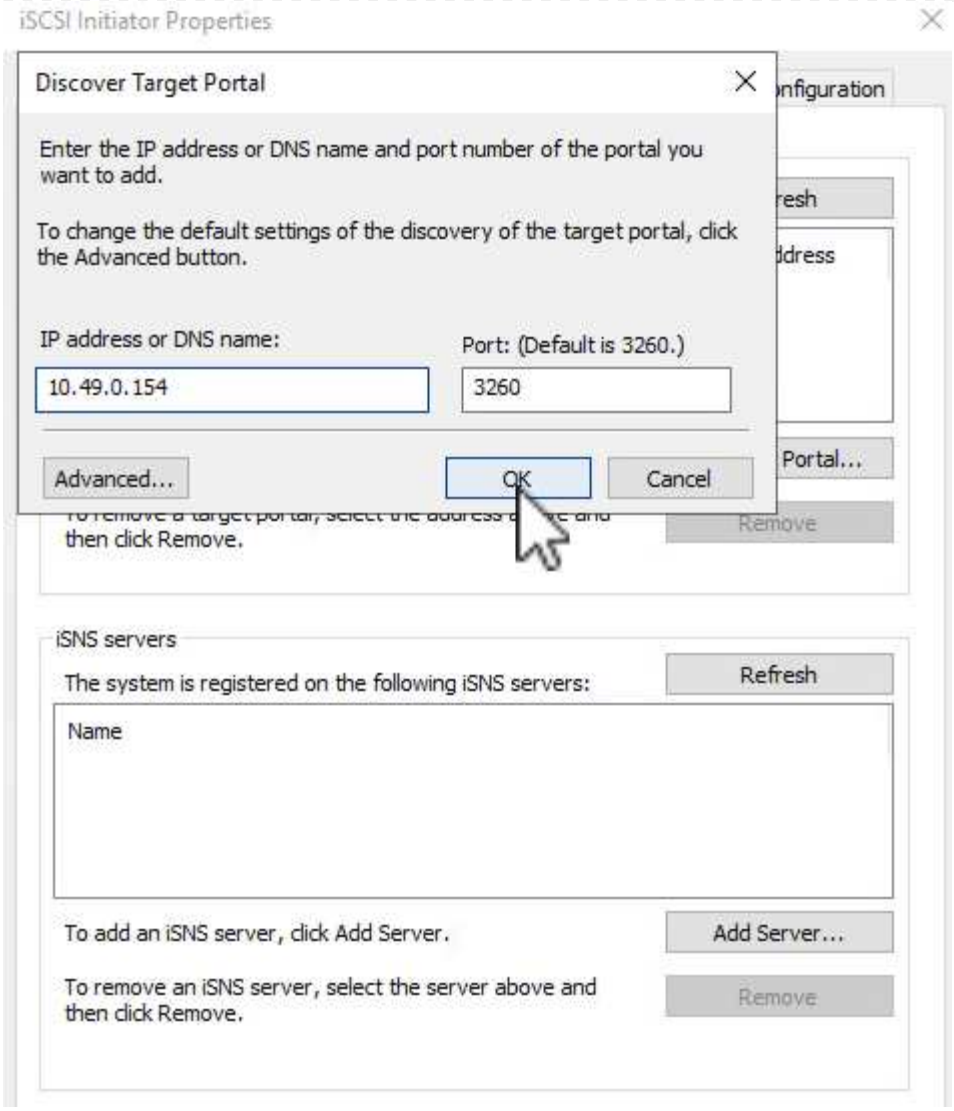
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

> 要完成上述步骤、您需要先从Windows服务器上的iSCSI启动程序属性检索IQN。

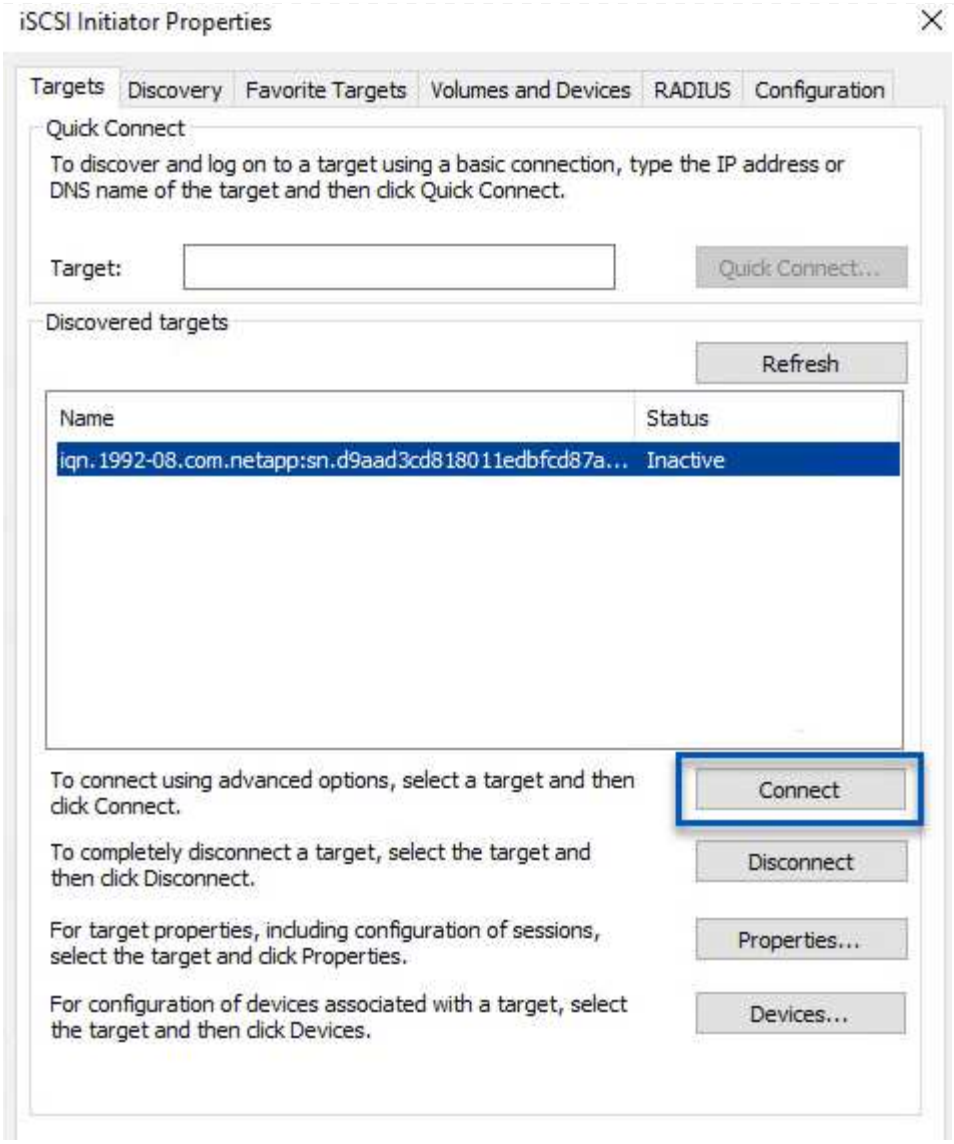
4. 最后、将LUN映射到刚刚创建的启动程序组：

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

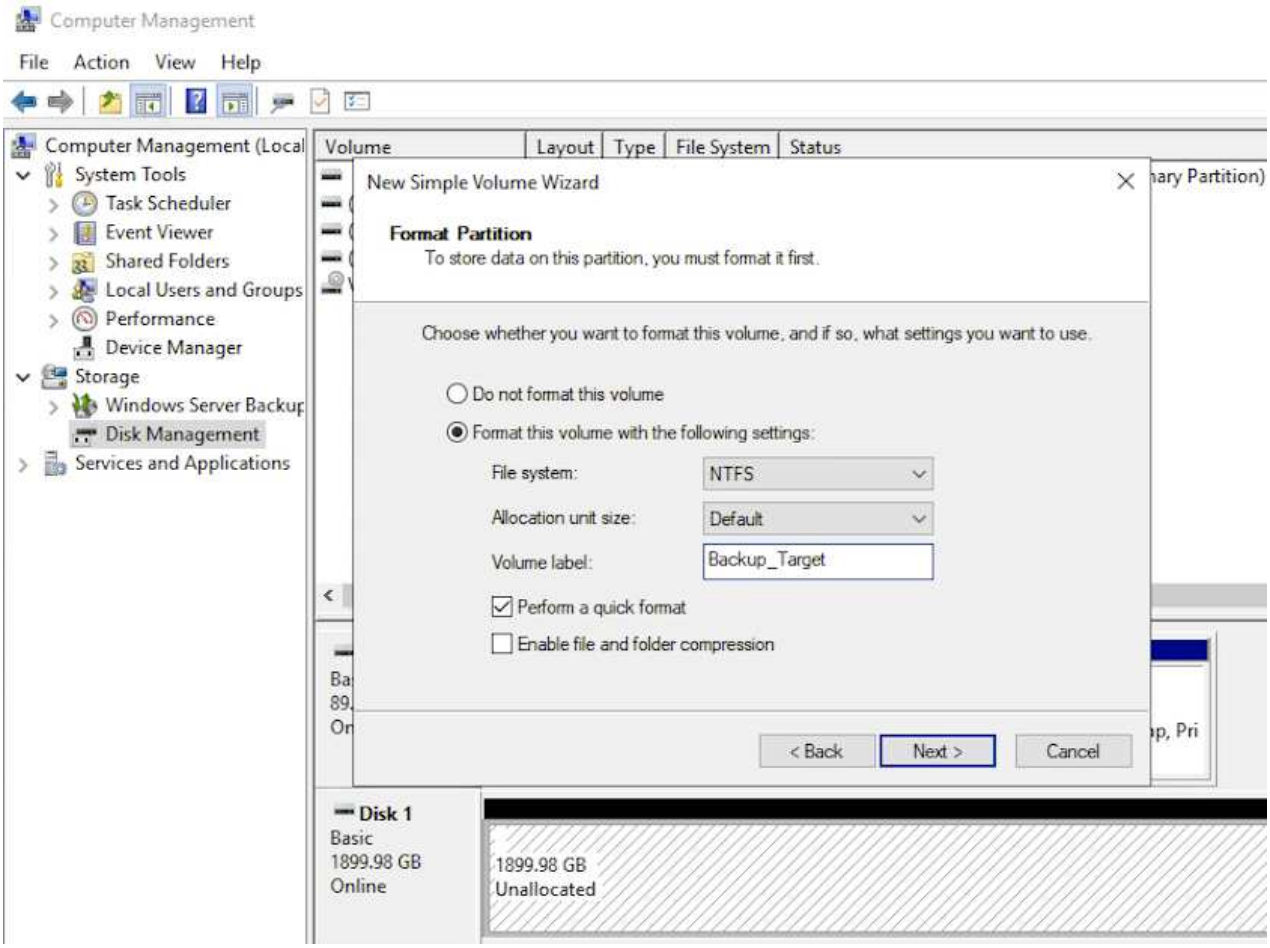
5. 要挂载iSCSI LUN、请登录到Veeam Backup & Replication Server并打开iSCSI启动程序属性。进入*Discover (*发现)*选项卡并输入iSCSI目标IP地址。



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



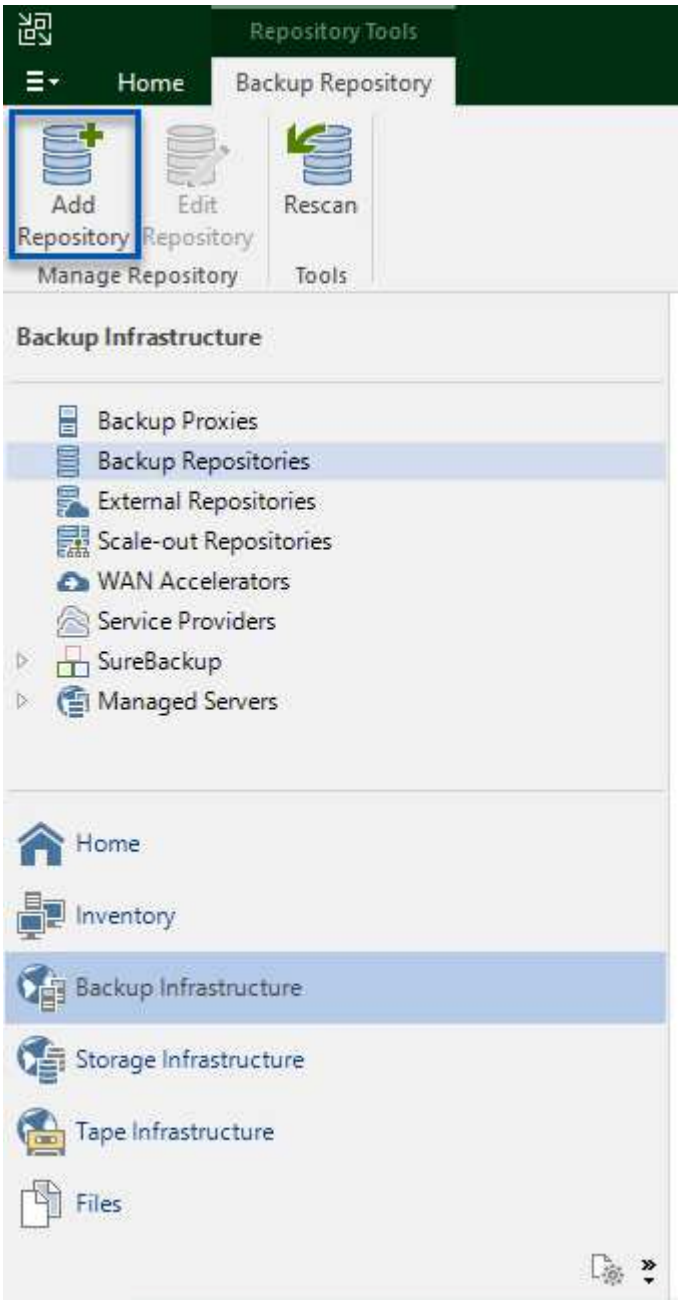
7. 在磁盘管理实用程序中、初始化新的LUN并使用所需的名称和驱动器盘符创建卷。选中*启用多路径*框，然后单击*确定*以连接到LUN。



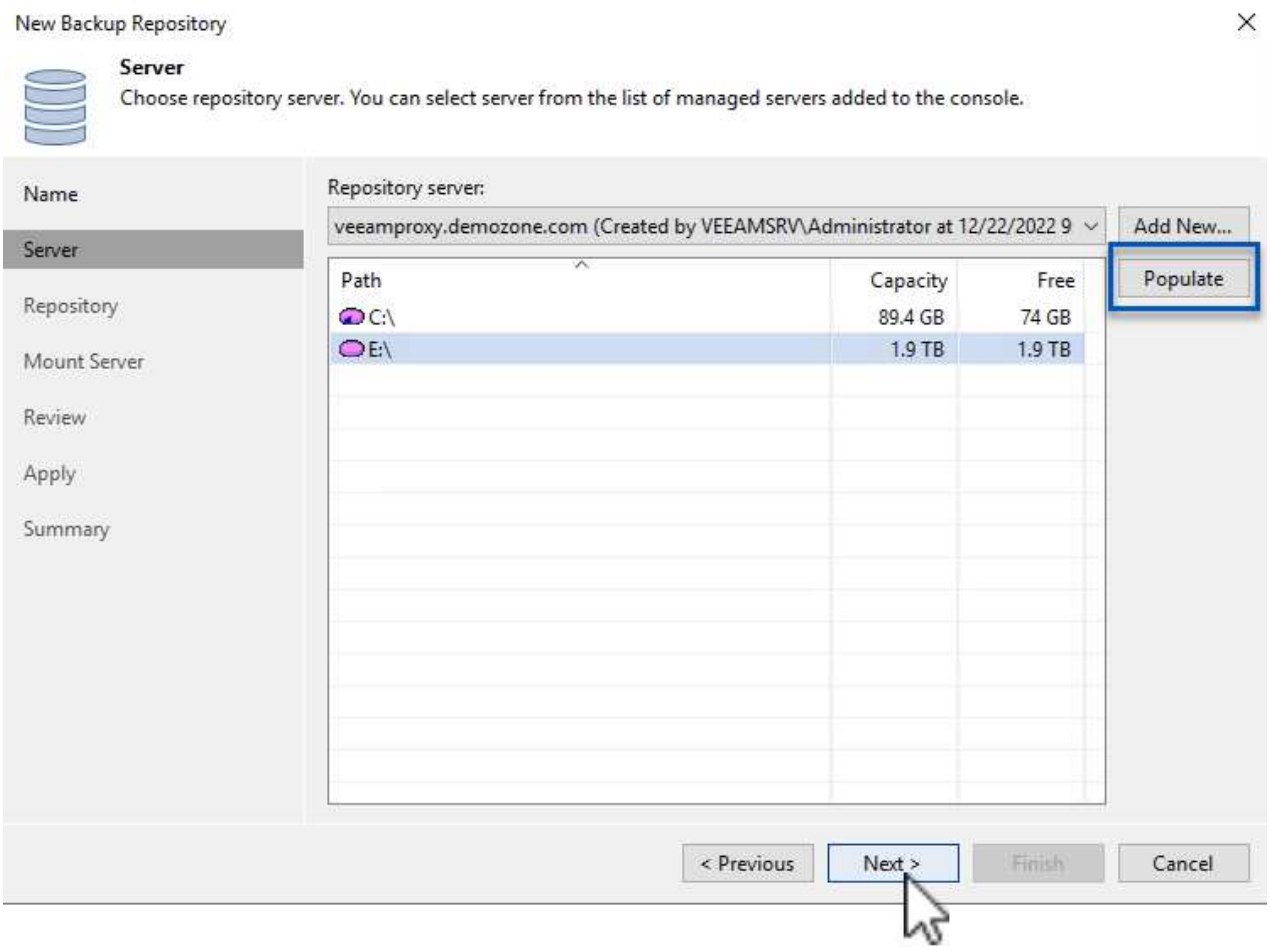
8. 重复上述步骤、将iSCSI卷挂载到Veeam代理服务器上。

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。

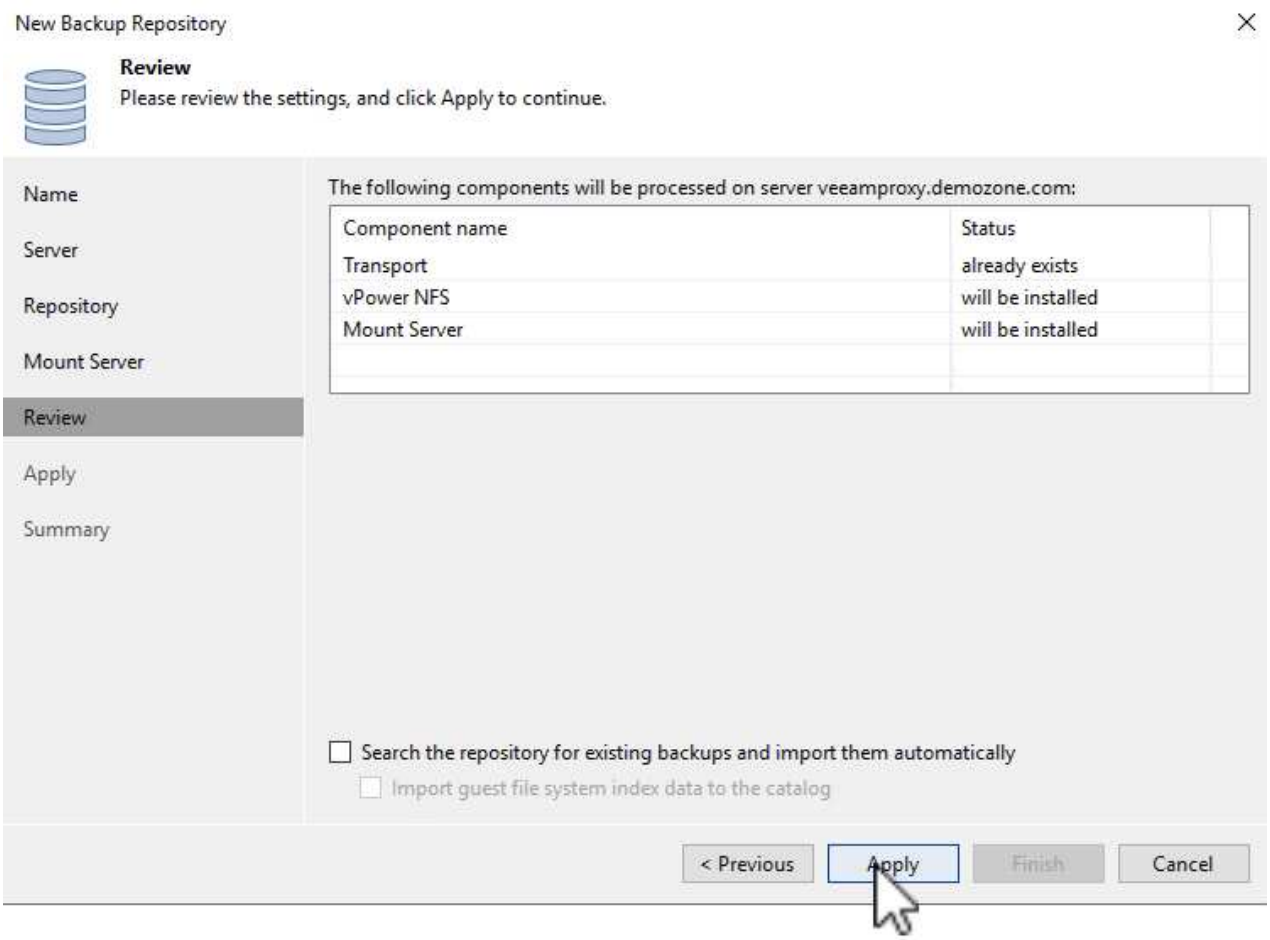
1. 在Veeam Backup and Replication控制台中、单击左下方的*备份基础架构*、然后选择*添加存储库*



2. 在"New Backup Repository (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*按钮以选择要使用的NTFS卷。



3. 在下一页上、选择执行高级还原时用于挂载备份的挂载服务器。默认情况下、此服务器与存储库存储连接在一起。
4. 查看您的选择，然后单击*Apply*开始创建备份存储库。



5. 对任何其他代理服务器重复上述步骤。

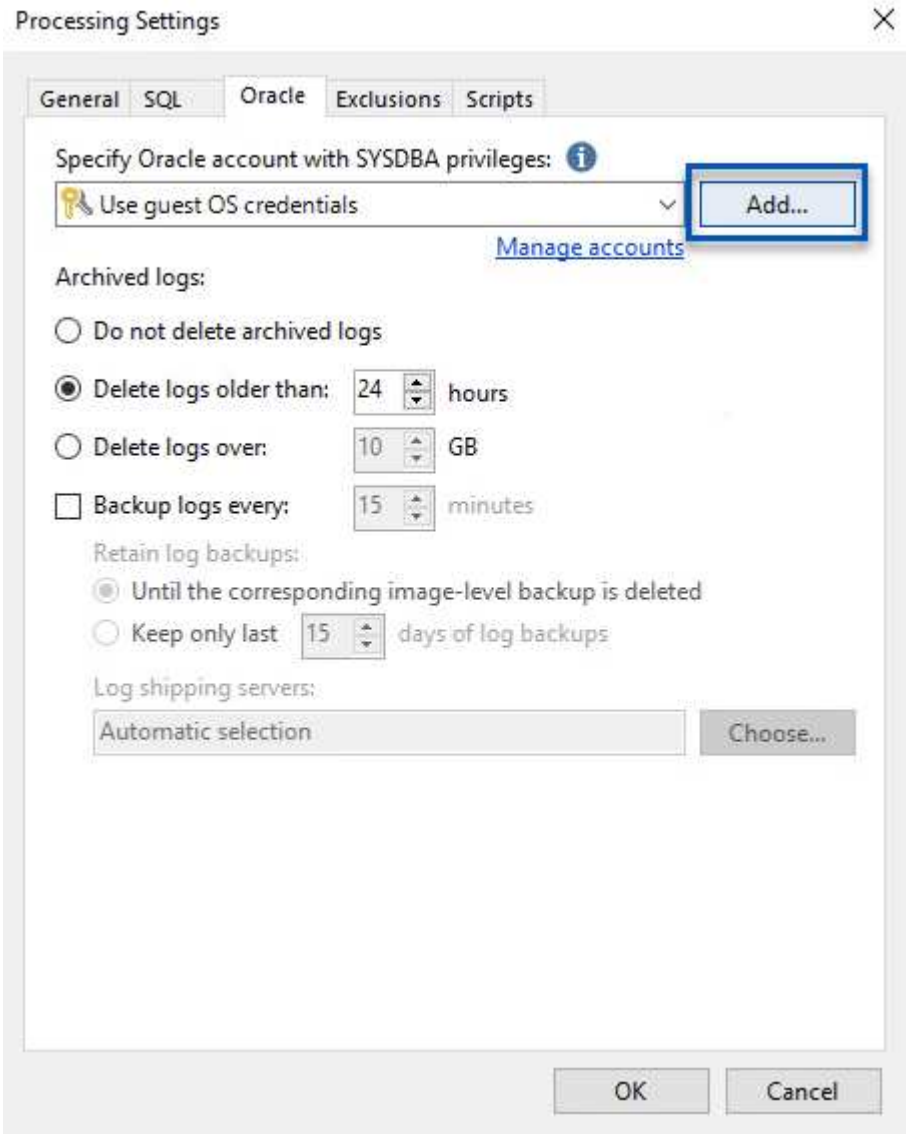
配置**Veeam**备份作业

应使用上一节中的备份系统信息栏创建备份作业。创建备份作业是任何存储管理员的常规任务、此处不会介绍所有步骤。有关在Veeam中创建备份作业的详细信息、请参见 "Veeam帮助中心技术文档"。

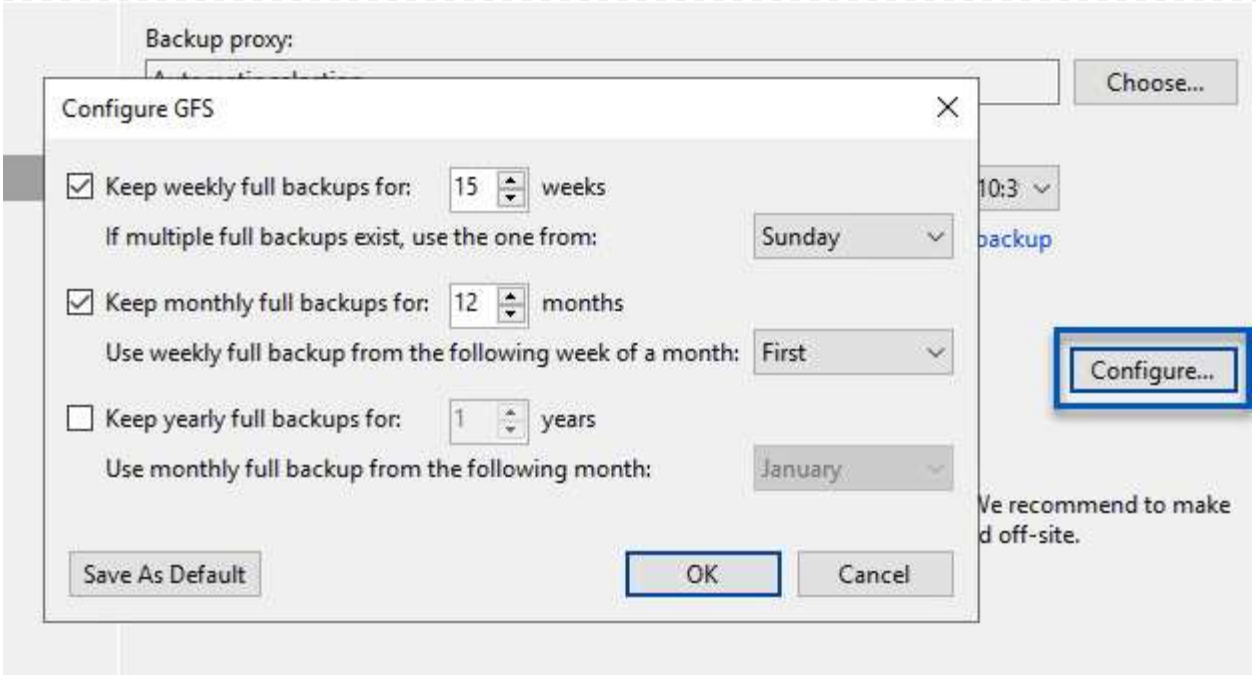
在此解决方案 中、为以下项创建了单独的备份作业：

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

1. 启用应用程序感知型处理、以创建一致的备份并执行事务日志处理。
2. 启用应用程序感知型处理后、请向应用程序添加具有管理员权限的正确凭据、因为此凭据可能与子操作系统凭据不同。



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的时间以供归档使用*，然后单击*配置…*按钮以配置策略。



使用**Veeam**完全恢复还原应用程序**VM**

使用Veeam执行完全还原是执行应用程序还原的第一步。我们验证了已启动的VM的完全恢复以及所有服务均正常运行。

还原服务器是任何存储管理员职责的正常组成部分、此处不会介绍所有步骤。有关在Veeam中执行完全恢复的更多完整信息、请参见 "Veeam帮助中心技术文档"。

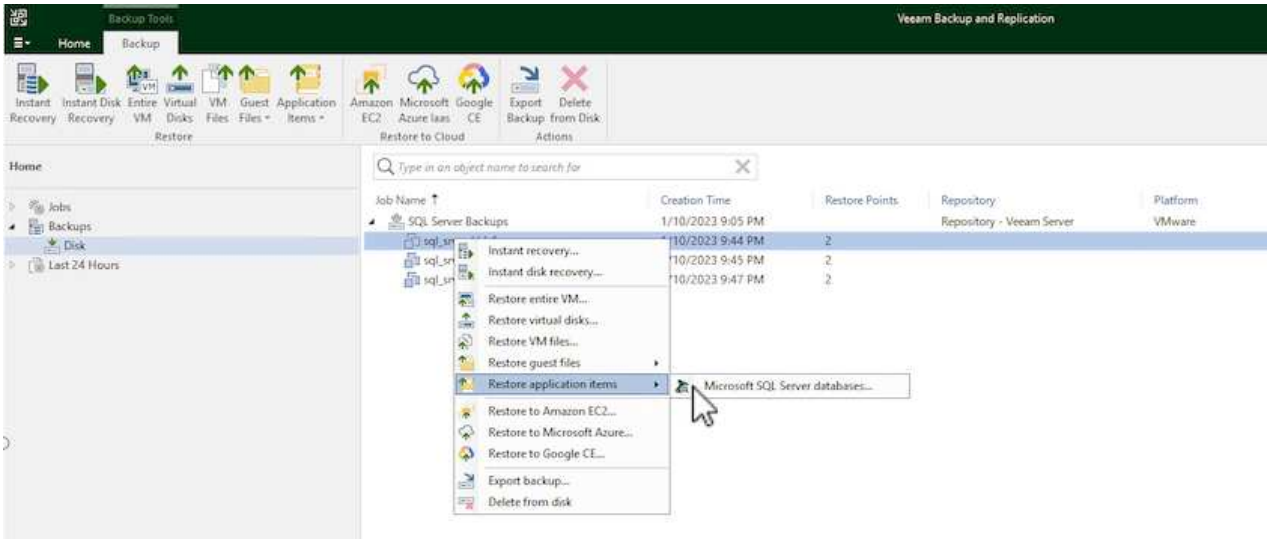
还原**SQL Server**数据库

Veeam Backup & Replication提供了多种还原SQL Server数据库的选项。在此验证中、我们使用Veeam Explorer for SQL Server with Instant Recovery执行SQL Server数据库还原。SQL Server即时恢复是一项功能、可用于快速还原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：

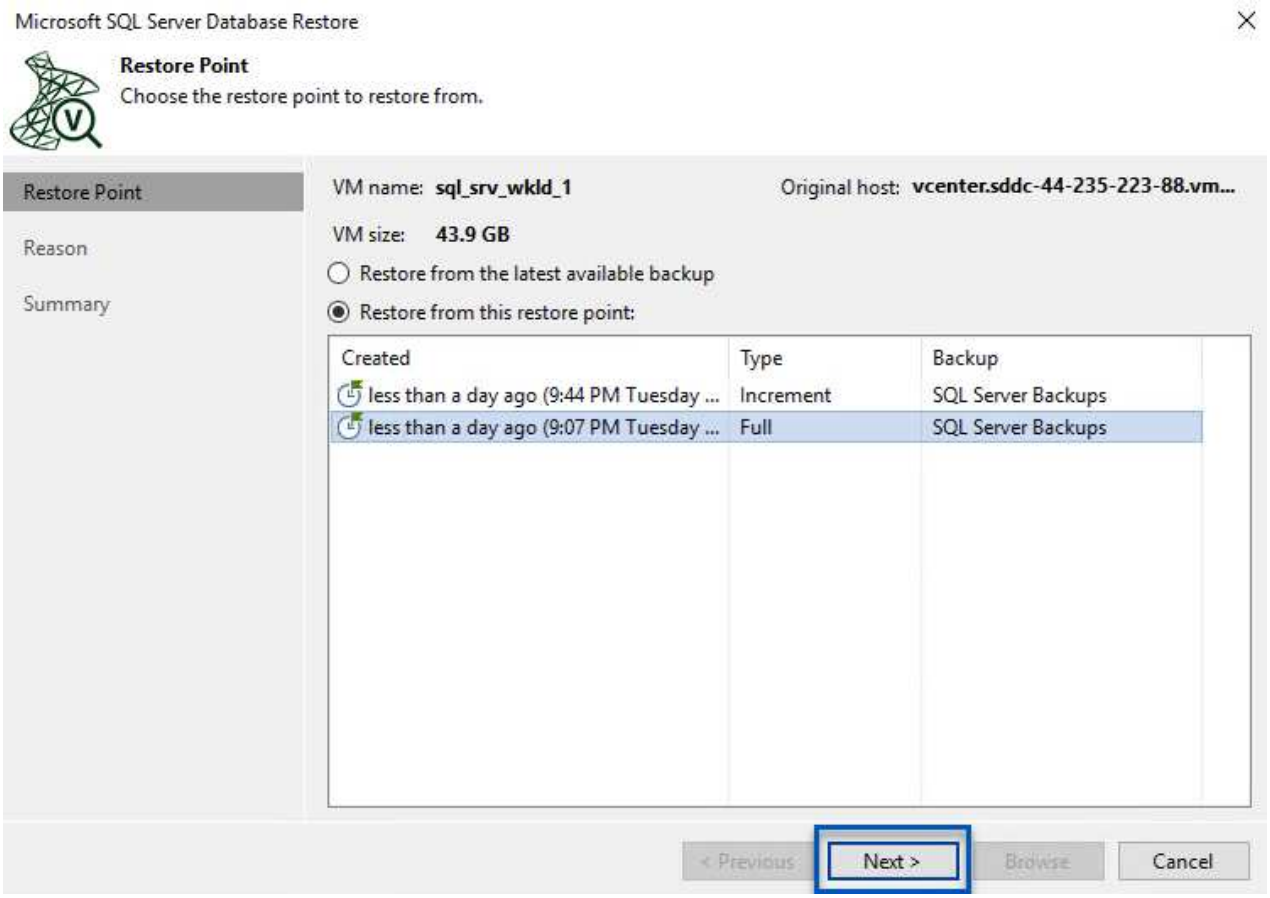
- Veeam Explorer 挂载包含要还原的**SQL Server**数据库的备份。
- 软件*直接从装载的文件发布数据库*，使其可作为目标SQL Server实例上的临时数据库访问。
- 在使用临时数据库时、Veeam Explorer *将用户查询*重定向到此数据库、以确保用户可以继续访问和使用数据。
- 在后台、Veeam 执行完整数据库还原、将数据从临时数据库传输到原始数据库位置。
- 完整数据库还原完成后、Veeam Explorer *将用户查询切换回原始*数据库并删除临时数据库。

使用**Veeam Explorer**即时恢复还原**SQL Server**数据库

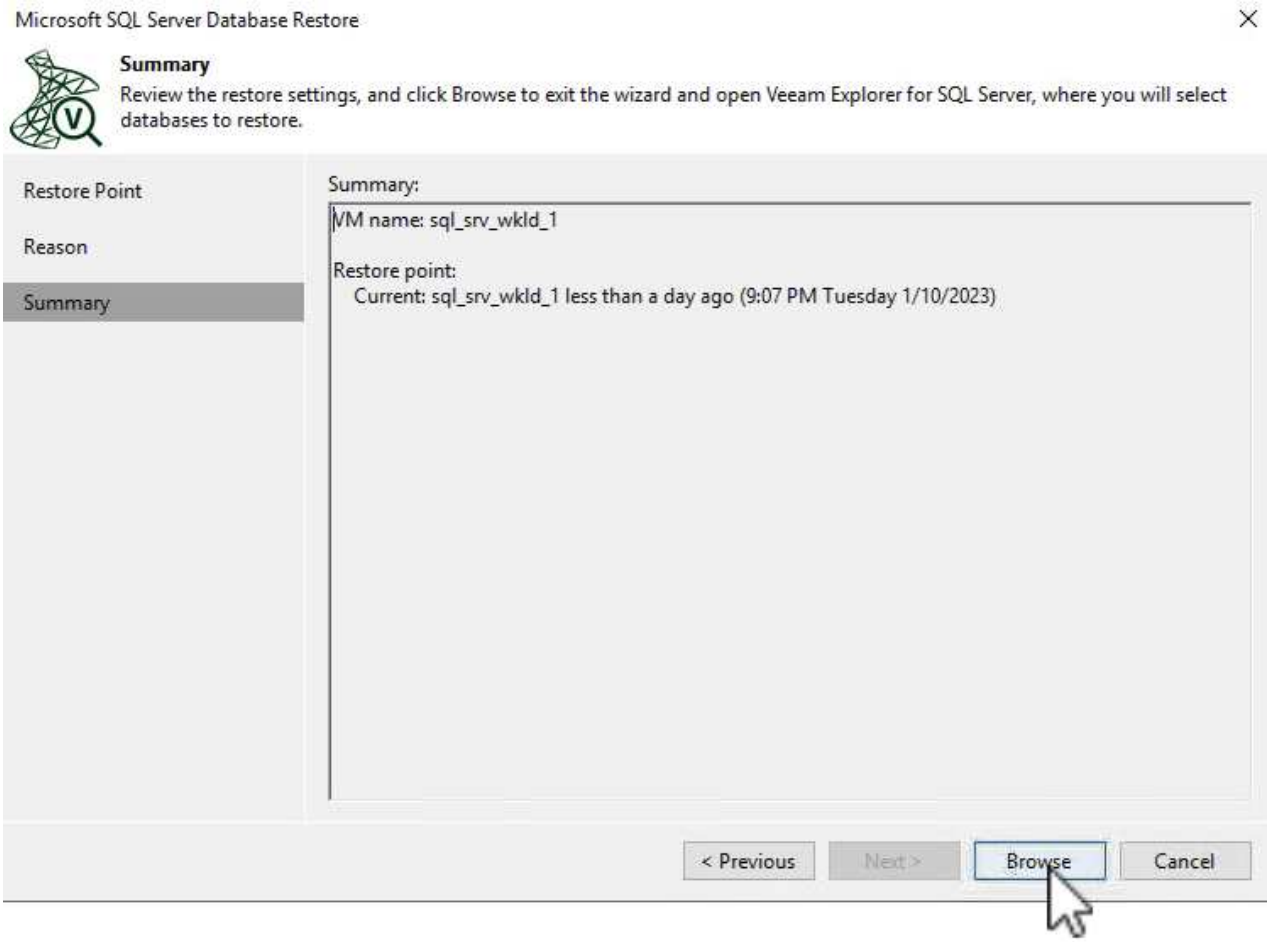
1. 在Veeam备份和复制控制台中、导航到SQL Server备份列表、右键单击某个服务器并选择*还原应用程序项*、然后选择* Microsoft SQL Server数据库…*。



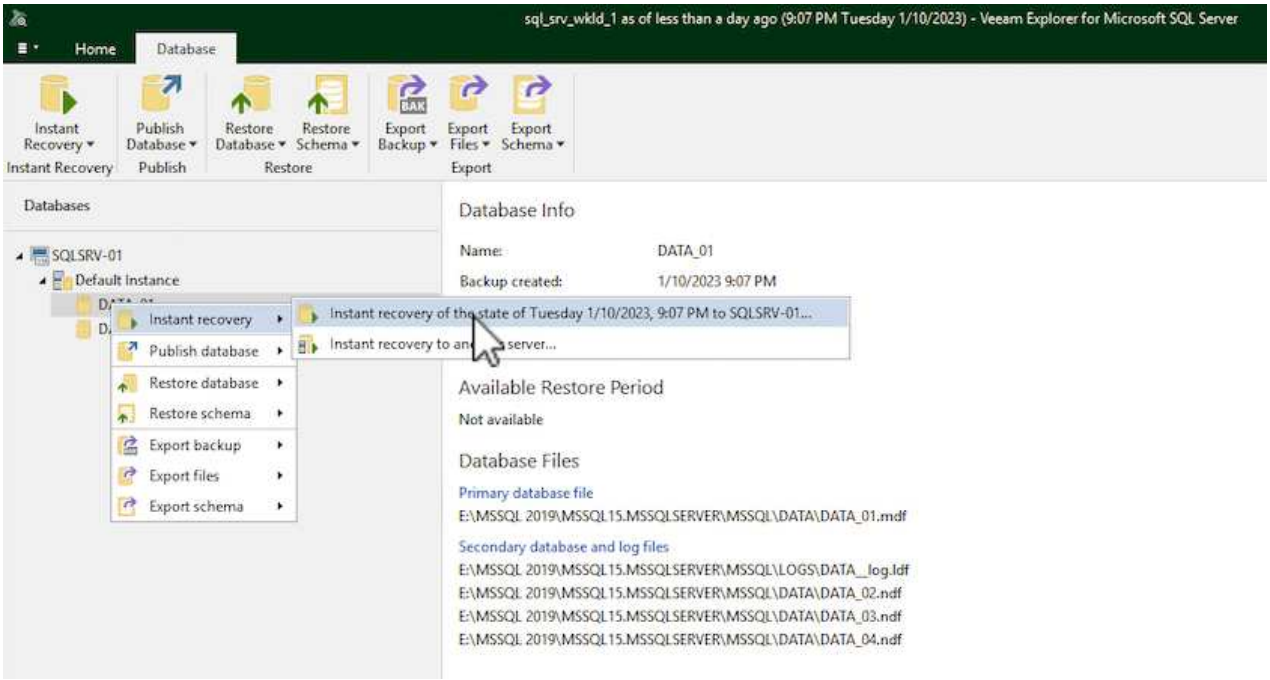
2. 在Microsoft SQL Server数据库还原向导中，从列表中选择还原点，然后单击*Next*。



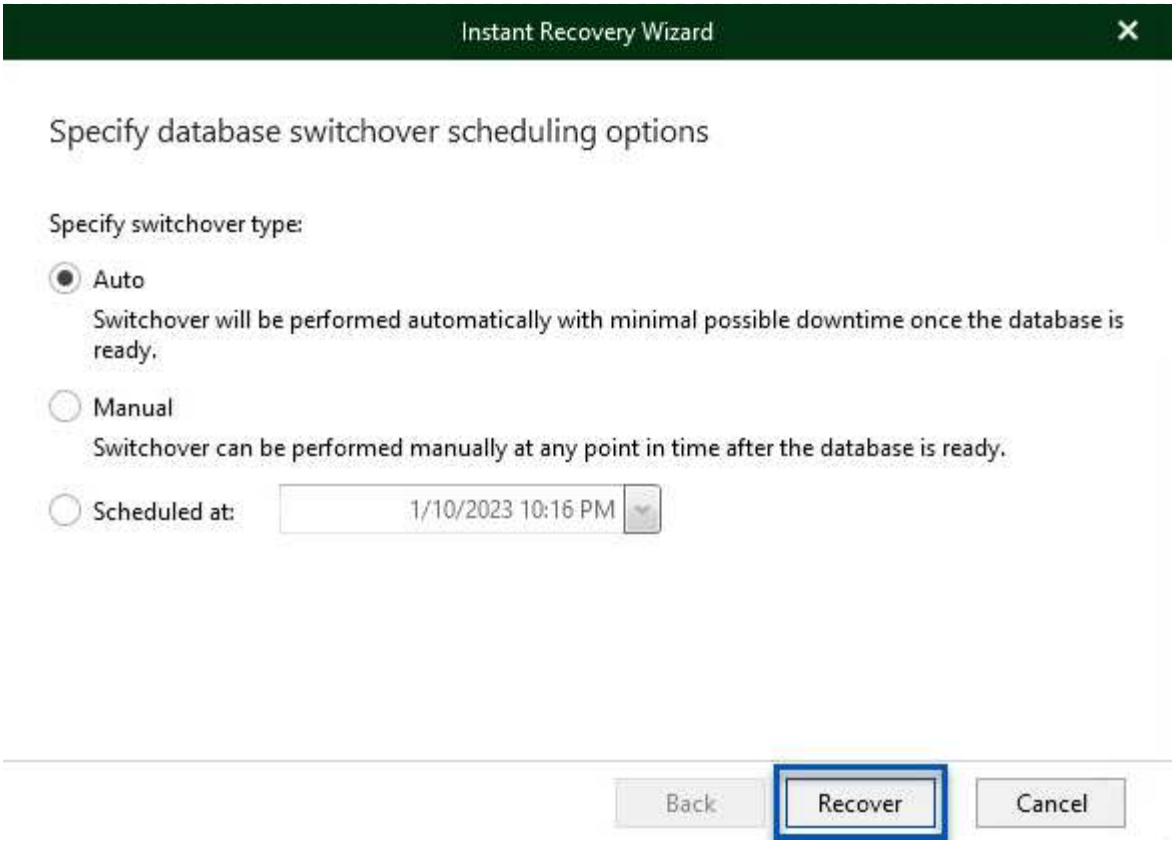
3. 如果需要、输入*恢复原因*、然后在摘要页面上、单击*浏览*按钮以启动Veeam Explorer for Microsoft SQL Server。



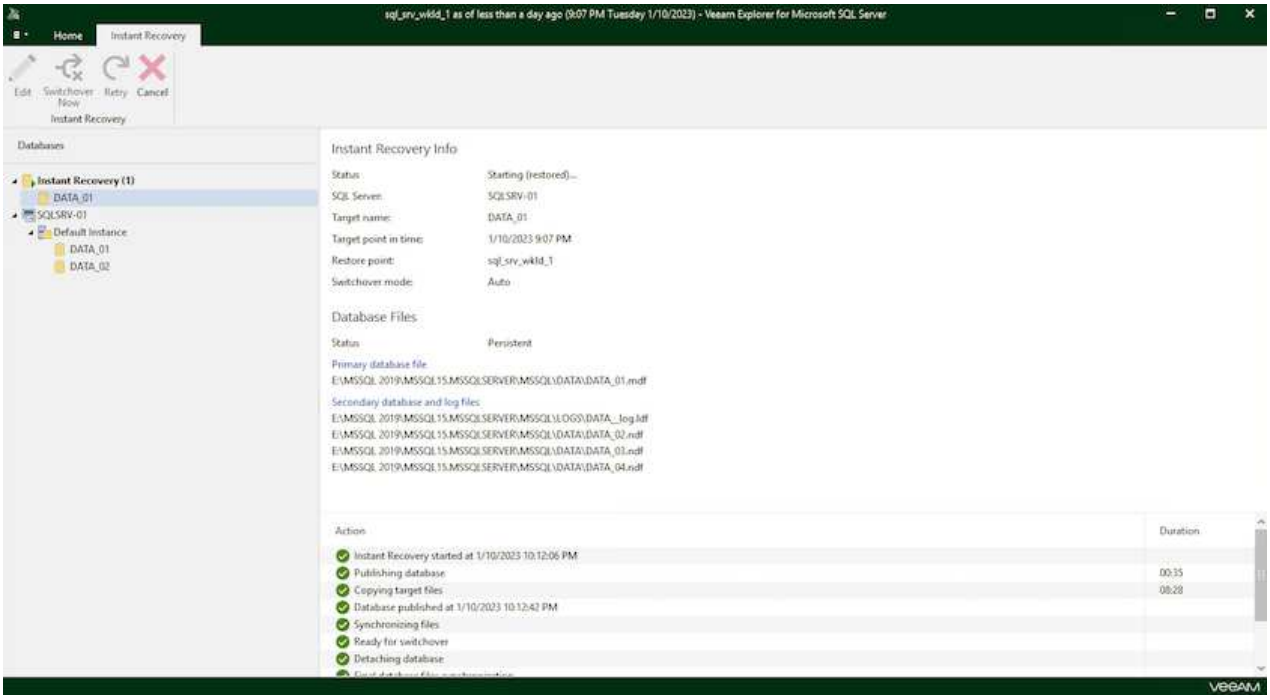
4. 在Veeam Explorer中展开数据库实例列表、右键单击并选择*即时恢复*、然后选择要恢复到的特定还原点。



5. 在即时恢复向导中、指定切换类型。这可以是自动执行的、停机时间最短、也可以是手动执行的、也可以是在指定时间执行的。然后单击*recover (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还原操作的详细信息、请参阅中的Microsoft SQL Server一节 "《Veeam Explorers用户指南》"。

使用**Veeam Explorer**还原**Oracle**数据库

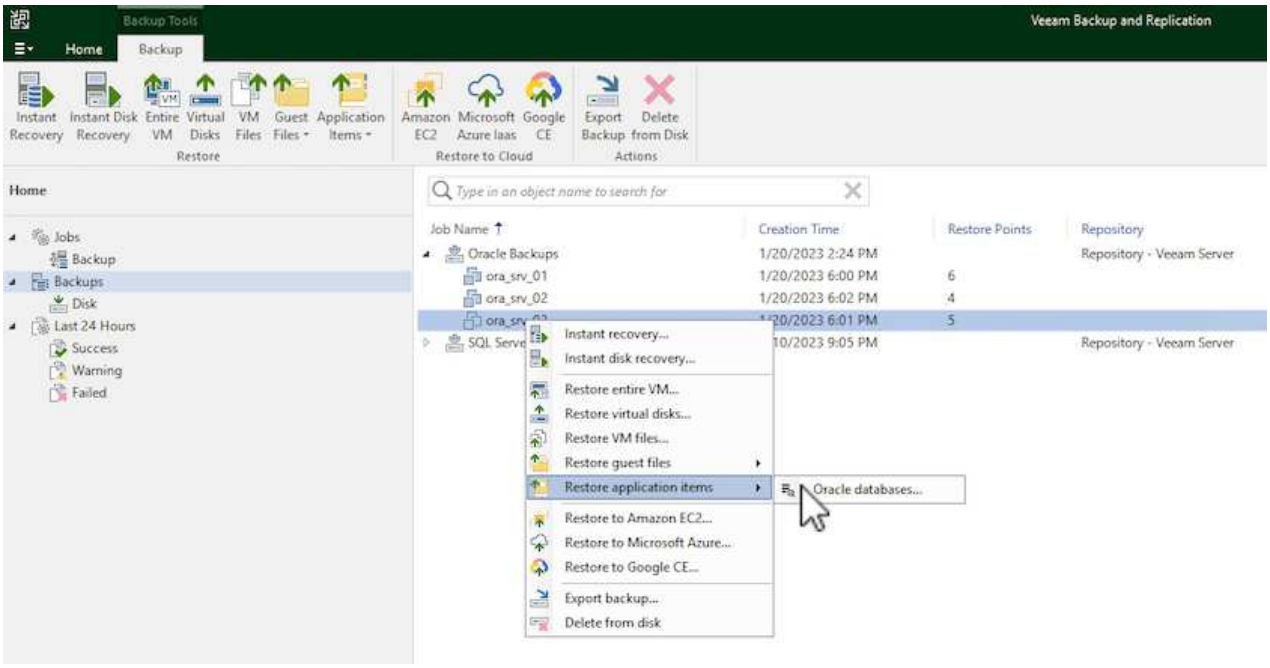
Veeam Explorer for Oracle数据库支持使用即时恢复执行标准Oracle数据库还原或无中断还原。它还支持发布数据库、以便快速访问、恢复Data Guard数据库以及从RMAN备份中恢复。

有关使用Veeam Explorer执行Oracle数据库还原操作的详细信息、请参阅中的Oracle一节 "《Veeam Explorers用户指南》"。

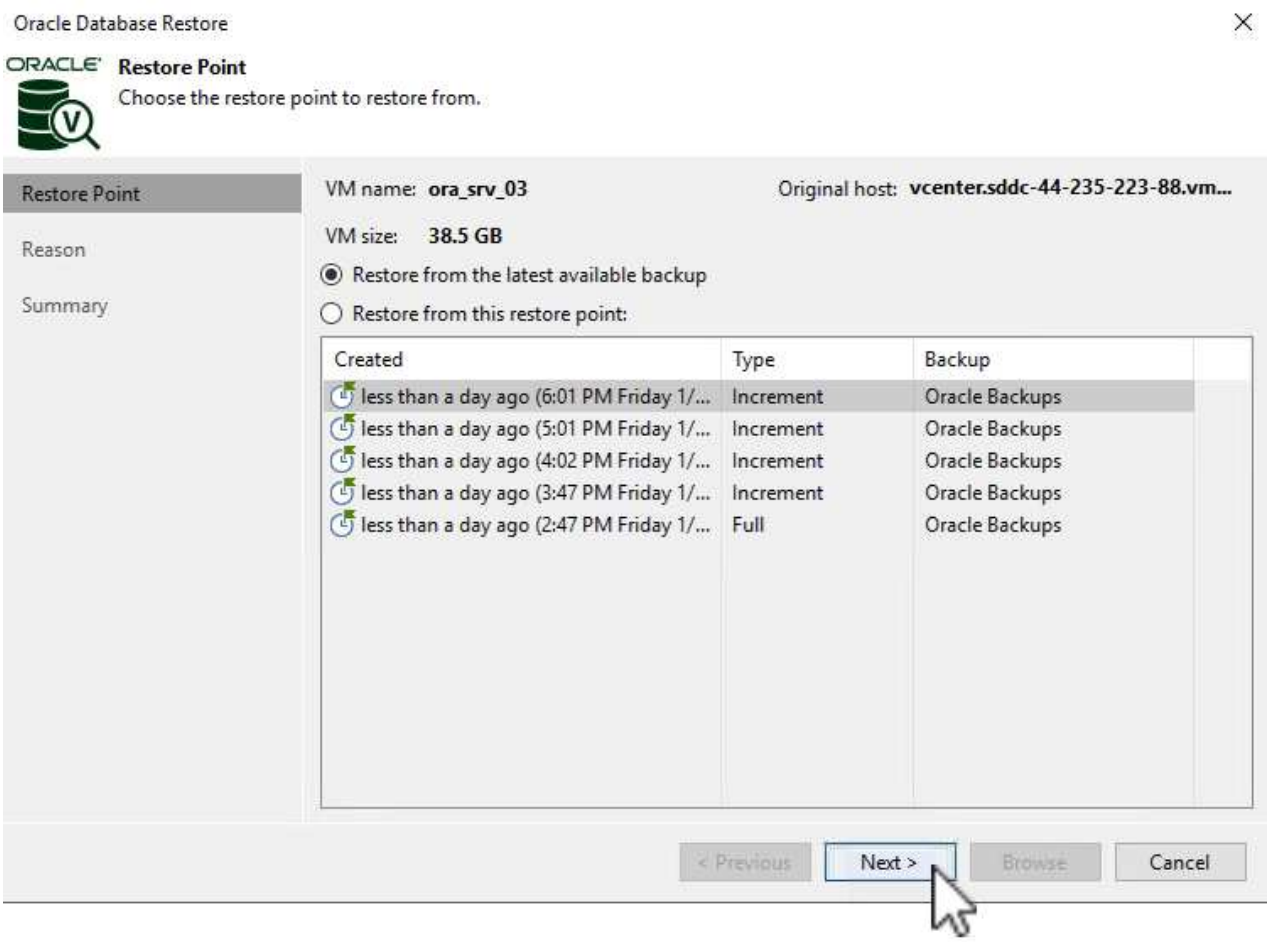
使用**Veeam Explorer**还原**Oracle**数据库

本节将介绍如何使用Veeam Explorer将Oracle数据库还原到其他服务器。

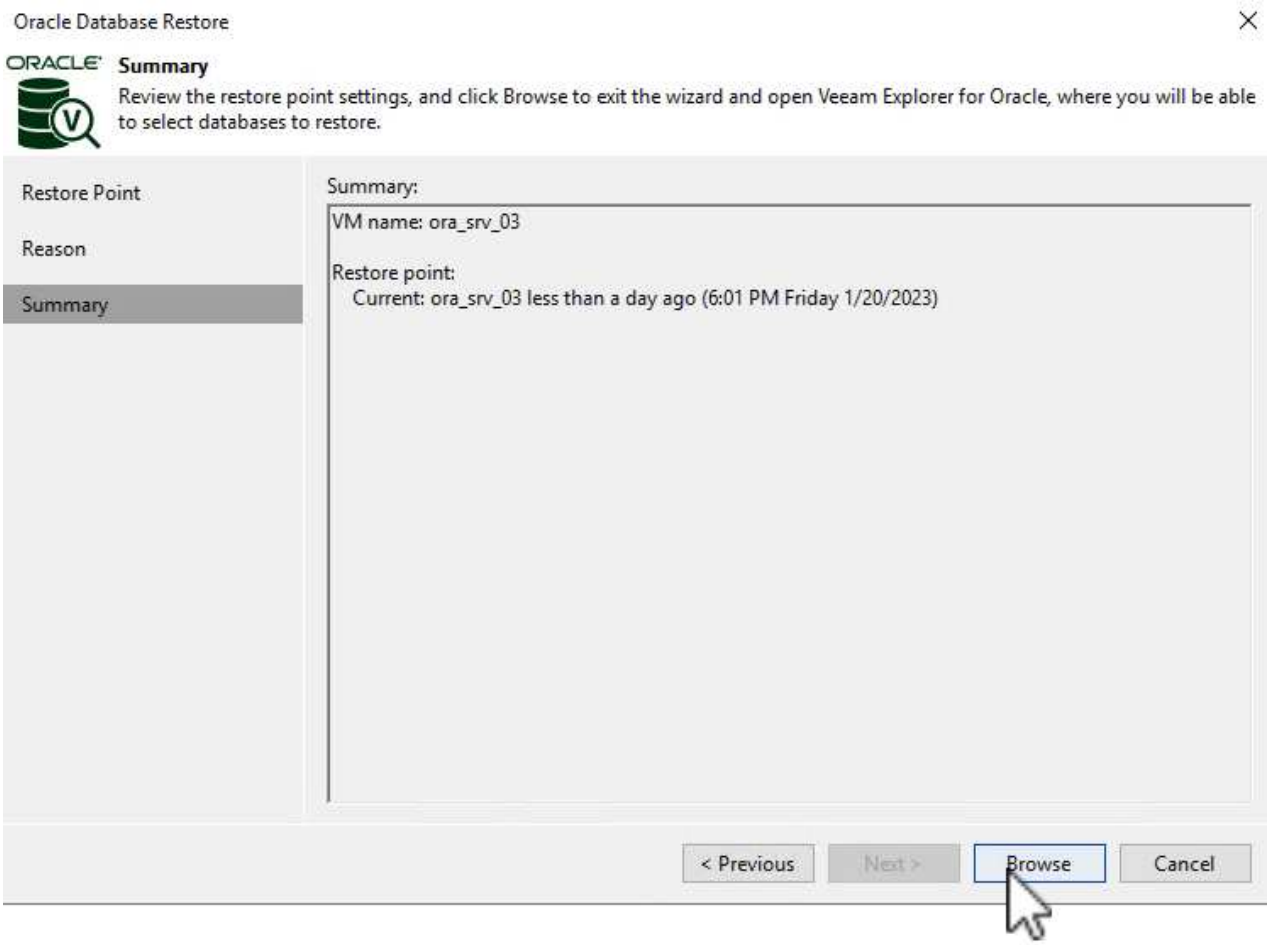
1. 在Veeam Backup and Replication控制台中、导航到Oracle备份列表、右键单击某个服务器并选择*还原应用程序项*、然后选择* Oracle数据库…*。



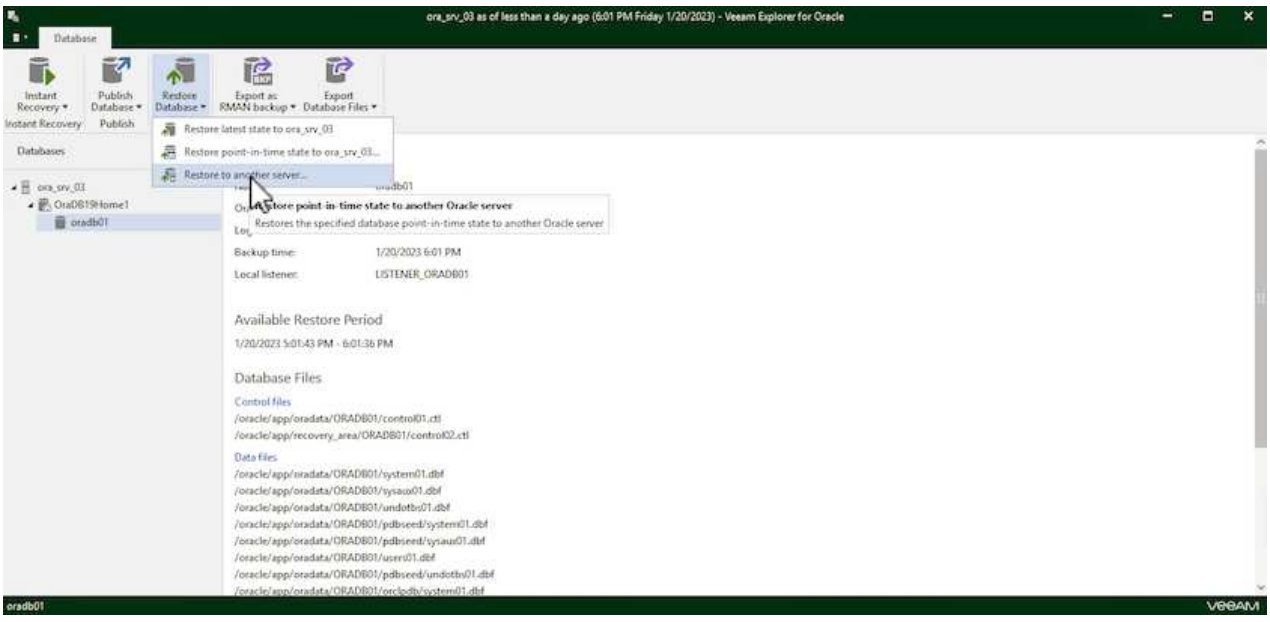
2. 在Oracle数据库恢复向导中，从列表中选择一个还原点，然后单击*Next*。



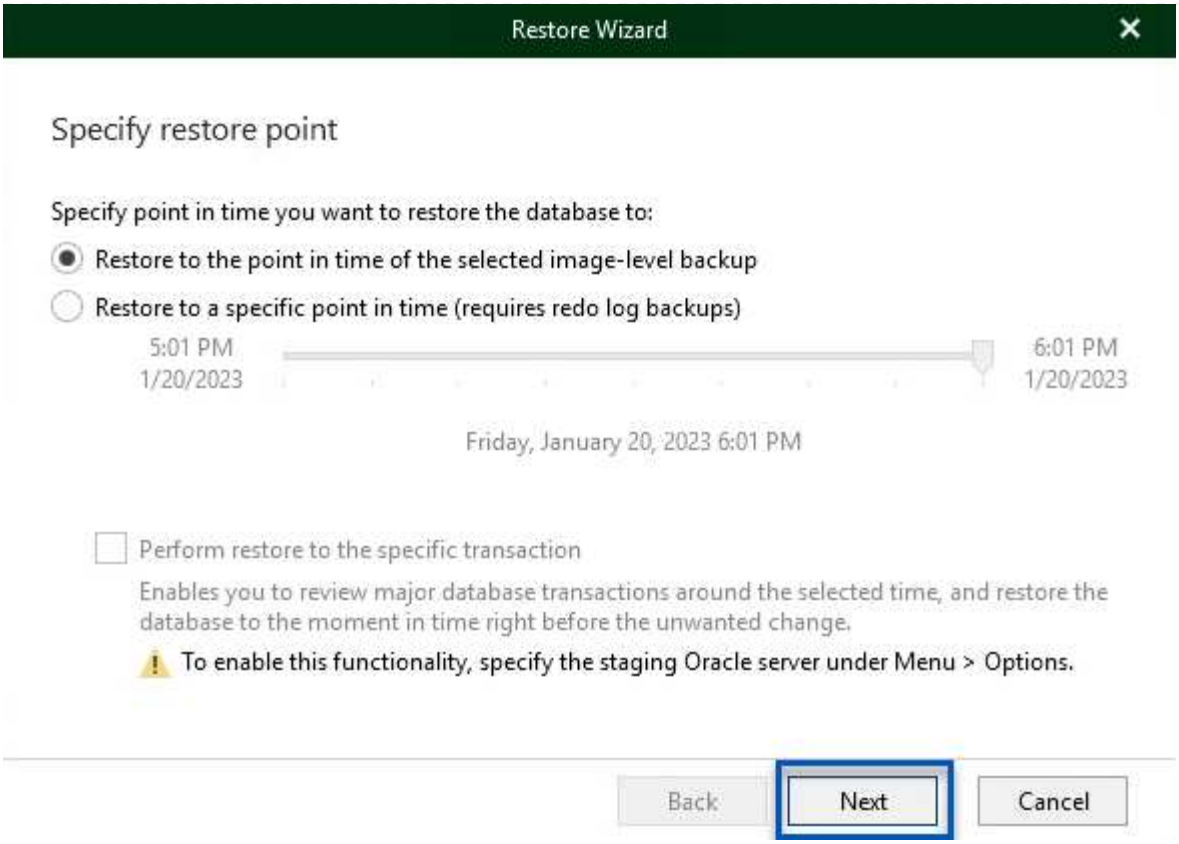
3. 如果需要、输入*恢复原因*、然后在摘要页面上、单击*浏览*按钮以启动Veeam Explorer for Oracle。



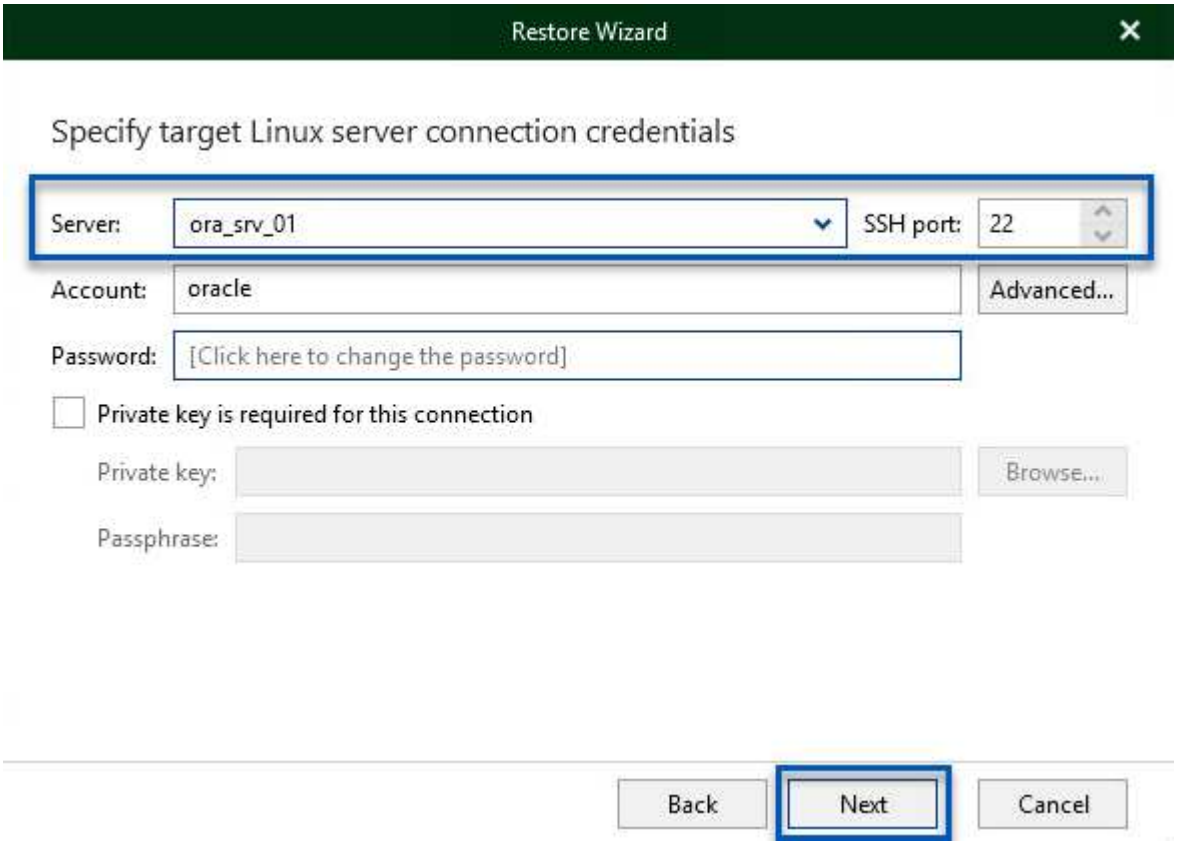
4. 在Veeam Explorer中展开数据库实例列表、单击要还原的数据库、然后从顶部的*还原数据库*下拉菜单中选择*还原到另一台服务器…*。



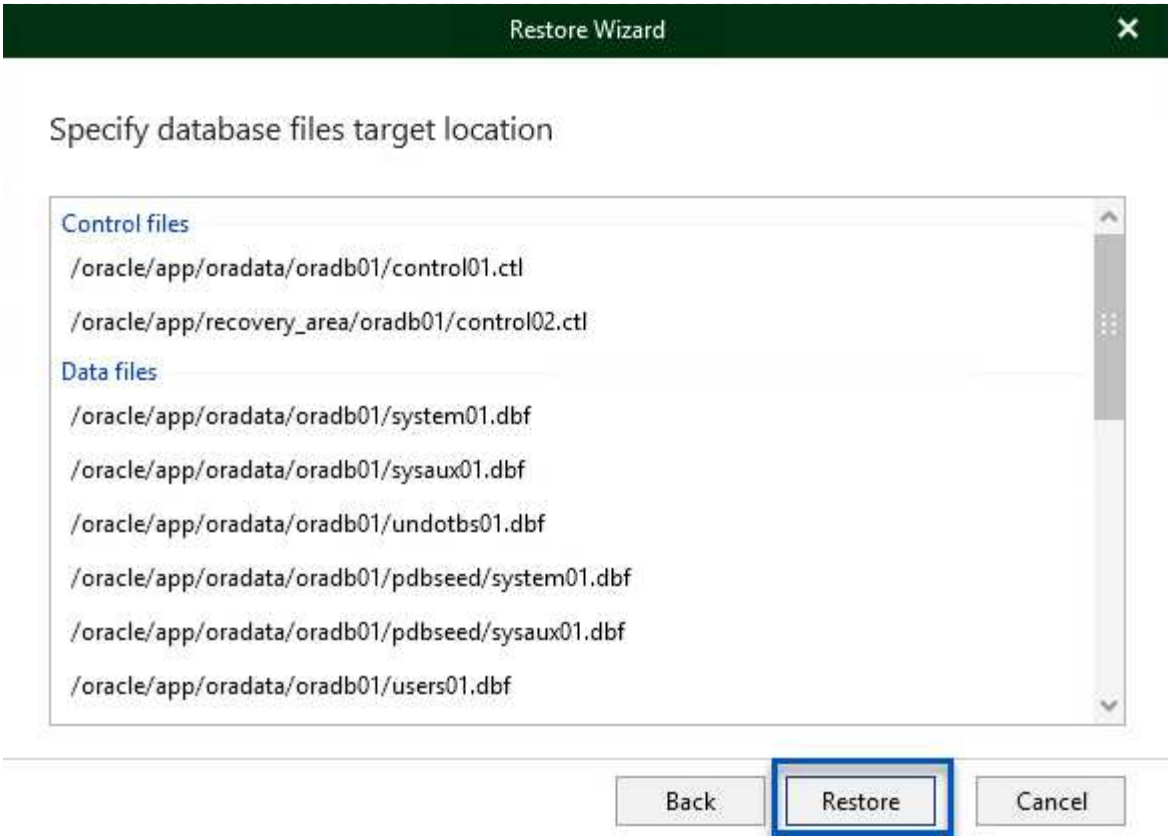
5. 在“恢复向导”中，指定要从中恢复的还原点，然后单击“下一步”。



6. 指定数据库将还原到的目标服务器和帐户凭据，然后单击*Next*。



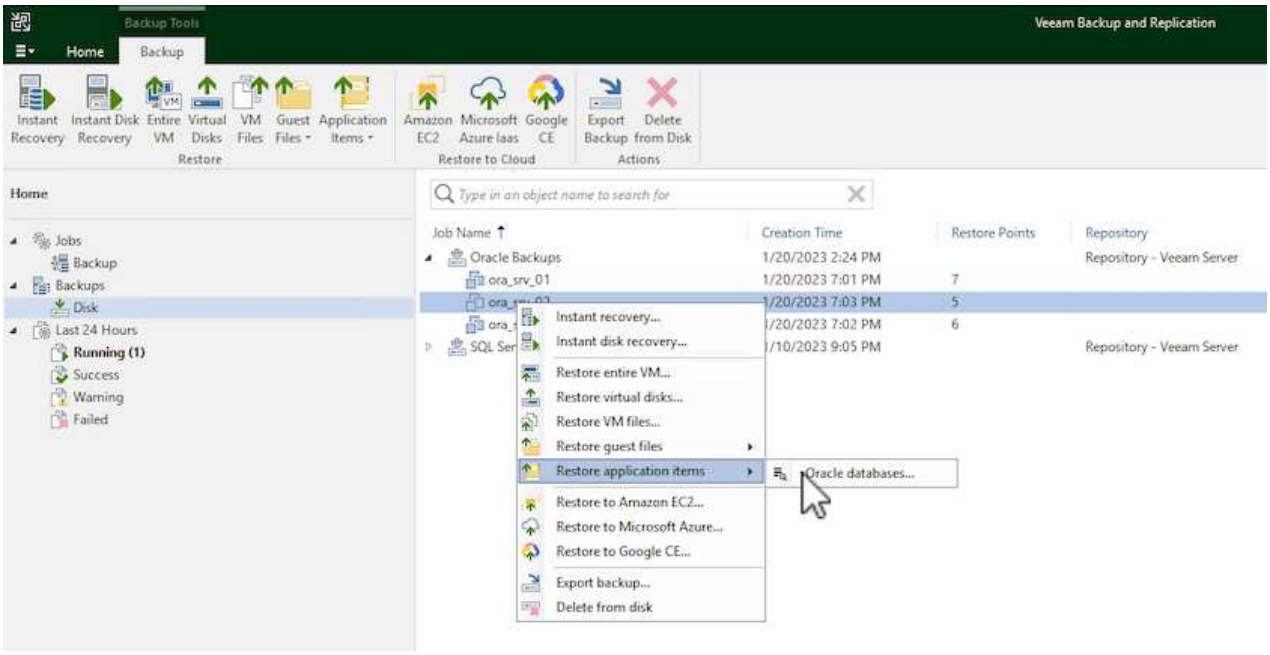
7. 最后，指定数据库文件的目标位置，然后单击*Restore*按钮开始恢复过程。



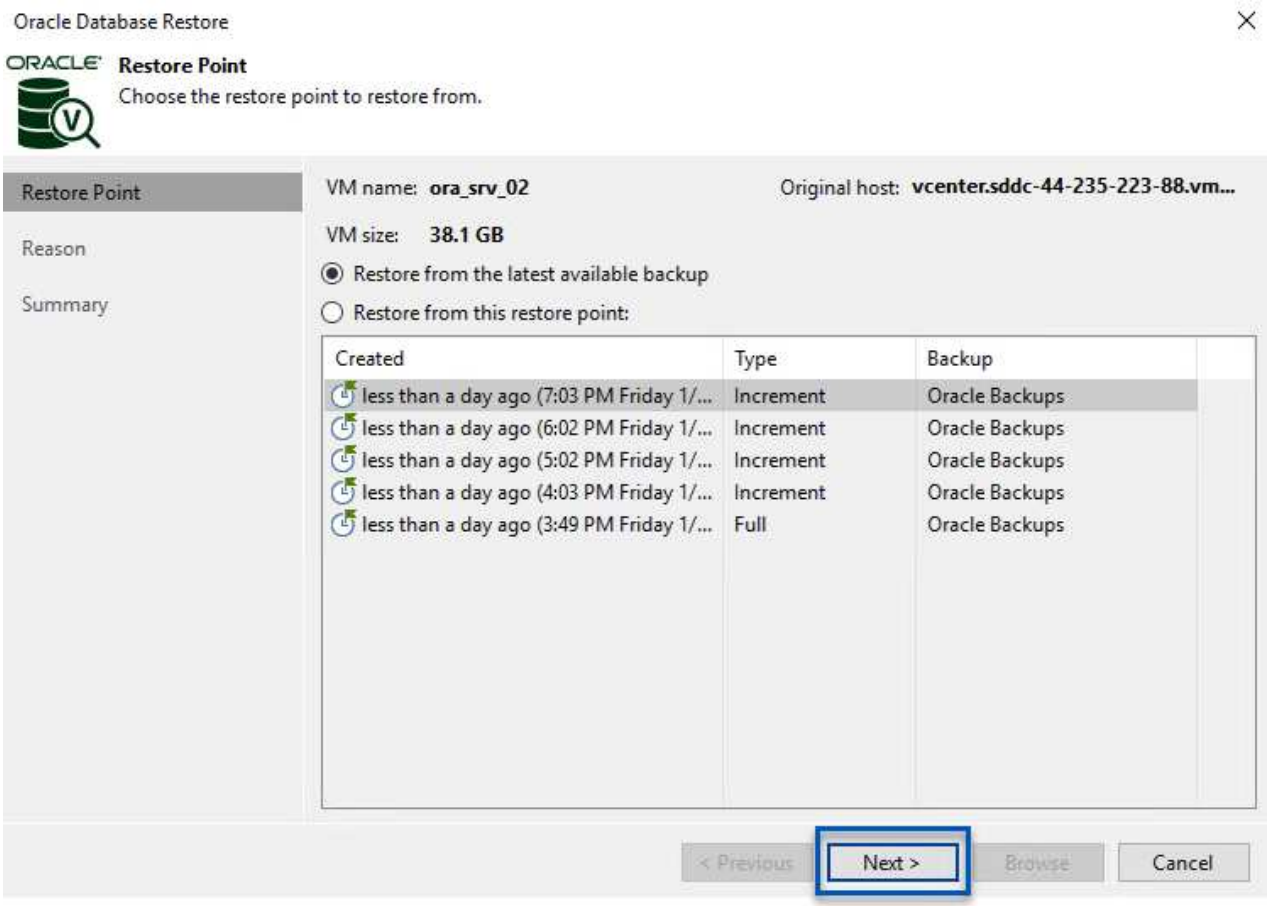
8. 数据库恢复完成后、请检查Oracle数据库是否在服务器上正确启动。

在本节中、数据库会发布到备用服务器、以便在不启动完全还原的情况下快速访问。

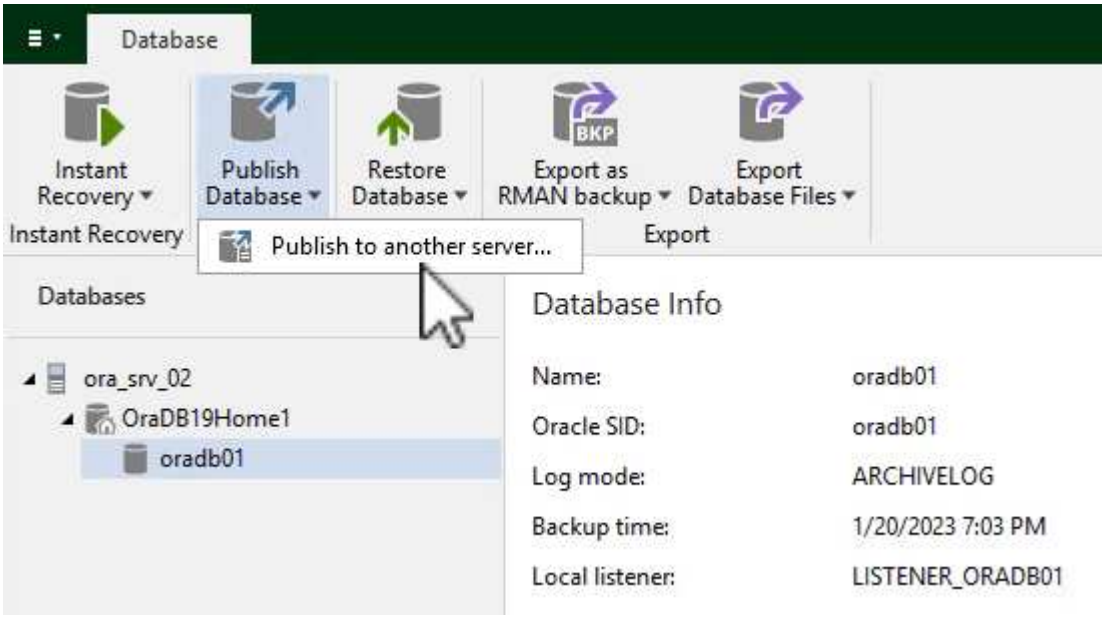
1. 在Veeam Backup and Replication控制台中、导航到Oracle备份列表、右键单击某个服务器并选择*还原应用程序项*、然后选择* Oracle数据库…*。



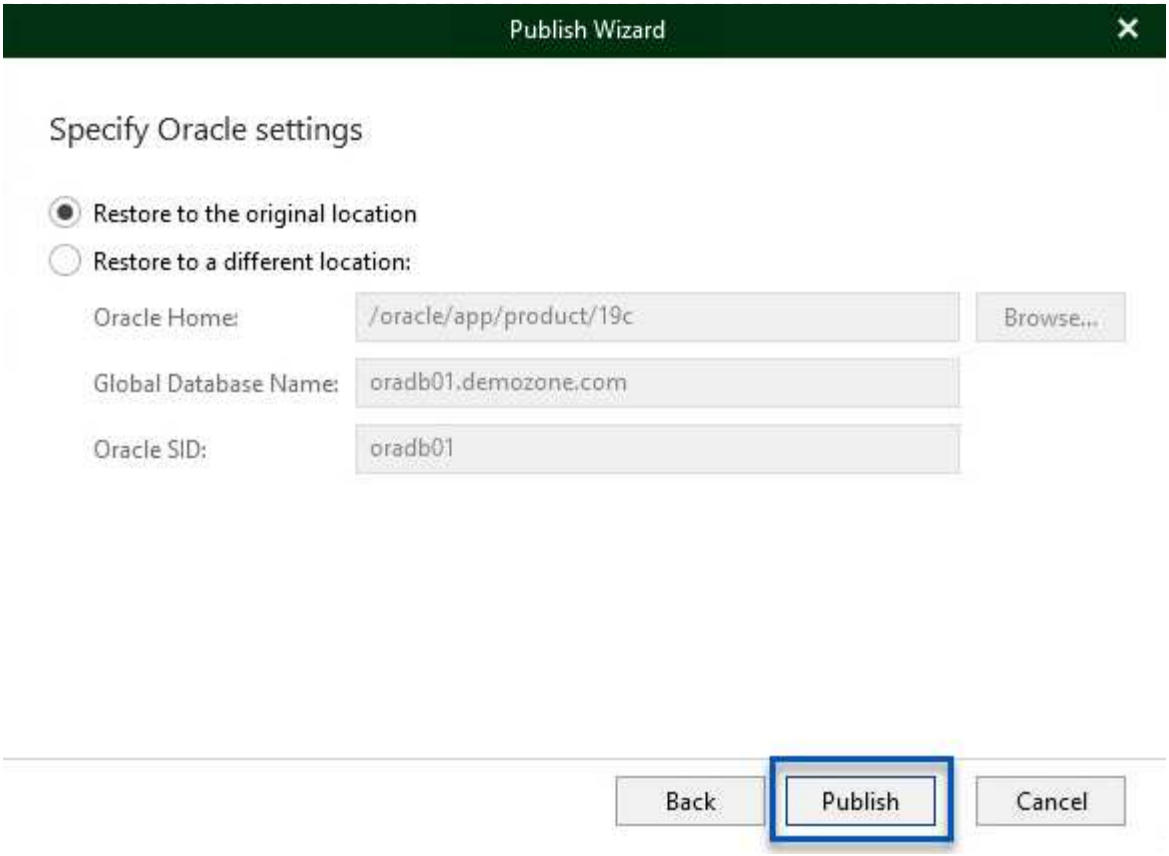
2. 在Oracle数据库恢复向导中，从列表中选择一个还原点，然后单击*Next*。



3. 如果需要、输入*恢复原因*、然后在摘要页面上、单击*浏览*按钮以启动Veeam Explorer for Oracle。
4. 在Veeam Explorer中展开数据库实例列表、单击要还原的数据库、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…*。



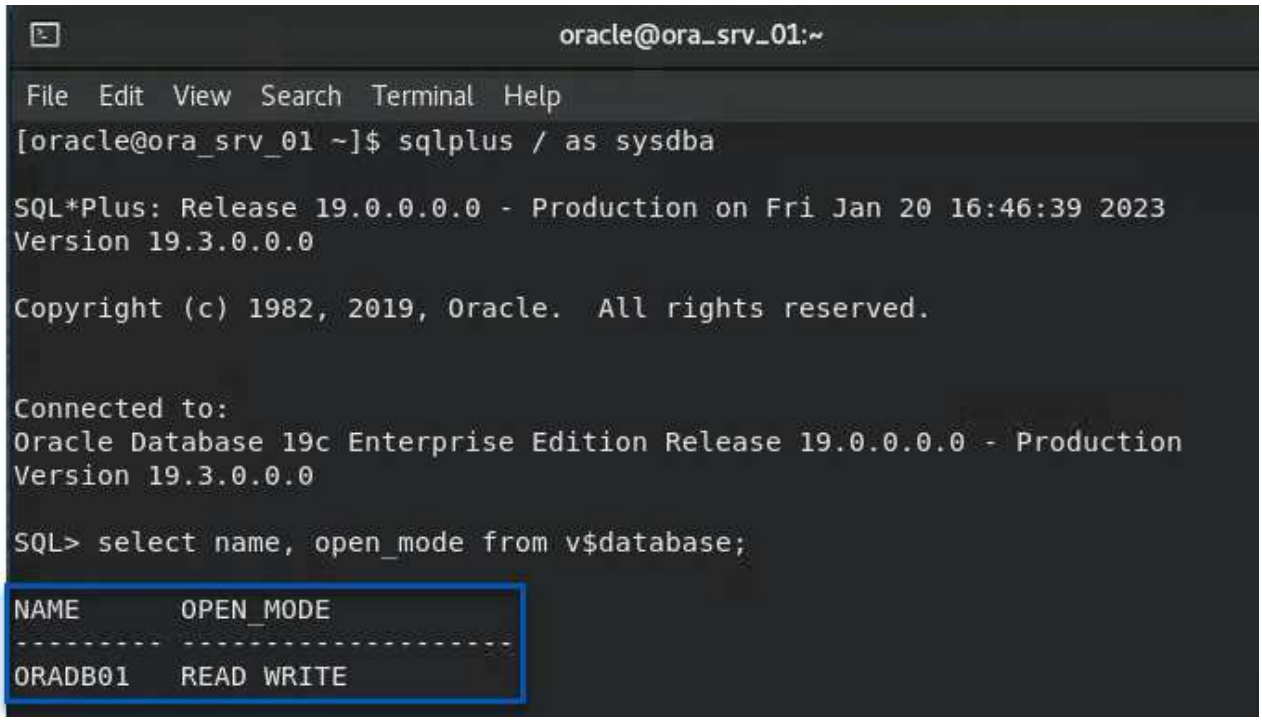
5. 在发布向导中，指定发布数据库的还原点，然后单击*Next*。
6. 最后，指定目标Linux文件系统位置，然后单击*发布*开始恢复过程。



7. 发布完成后、登录到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;
```



结论

VMware Cloud是一个功能强大的平台、用于运行业务关键型应用程序和存储敏感数据。对于依赖VMware Cloud的企业来说、安全的数据保护解决方案 对于确保业务连续性并帮助抵御网络威胁和数据丢失至关重要。通过选择可靠且强大的数据保护解决方案 、企业可以确信无论什么情况、其关键数据都是安全可靠的。

本文档中提供的使用情形重点介绍经验证的数据保护技术、这些技术重点介绍了NetApp、VMware和Veeam之间的集成。在AWS中、FSx for ONTAP 可用作VMware Cloud的补充NFS数据存储库、并可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、自动化和简化备份和恢复流程。Veeam可与FSx for ONTAP 上托管的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

要详细了解此解决方案 中提供的技术、请参阅以下追加信息。

- "FSx for 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"

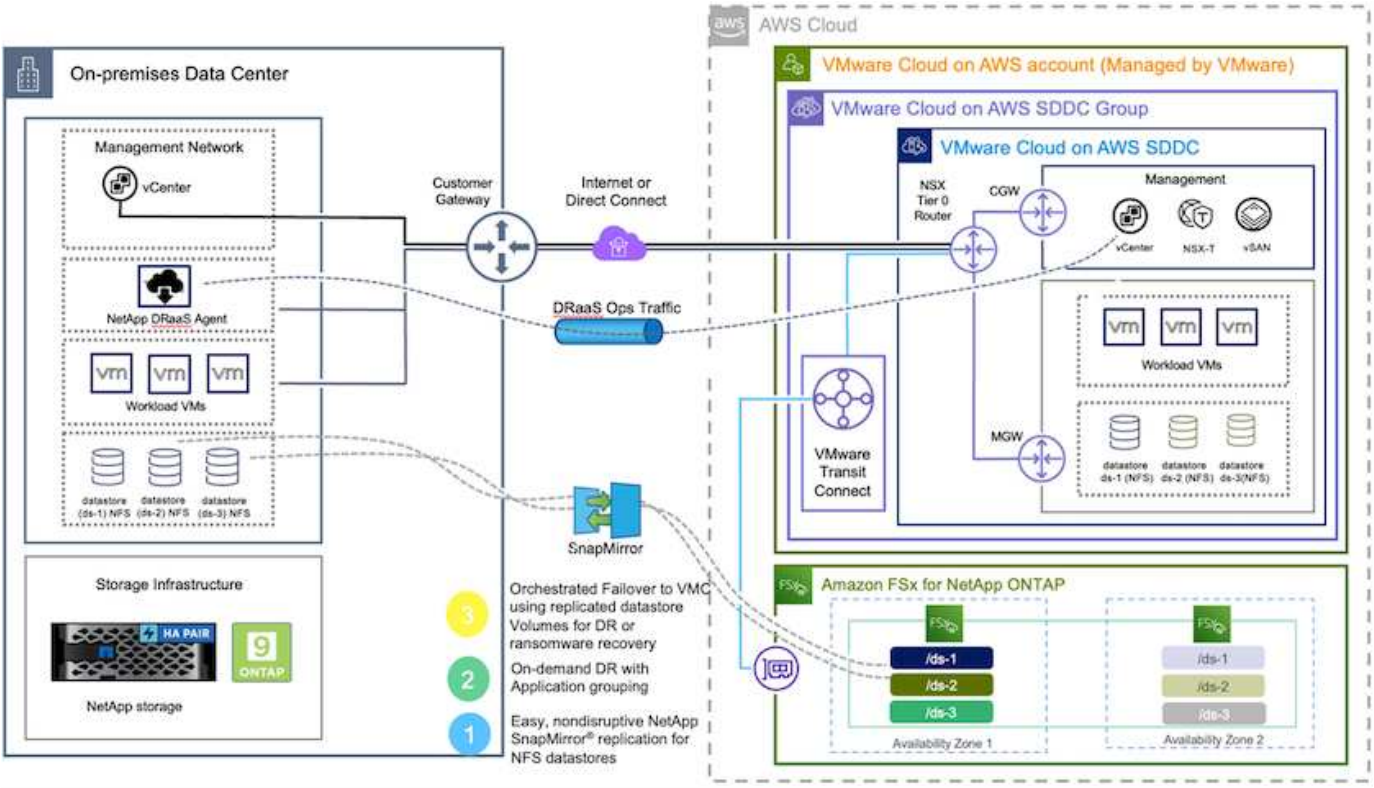
TR-4955：使用适用于**ONTAP** 和**VMC**的**FSX**进行灾难恢复**(AWS VMware Cloud)**

NetApp 公司 Niyaz Mohamed

概述

将灾难恢复到云是一种弹性且经济高效的方式、可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、可以将内部VMware工作负载复制到在AWS中运行的FSX for ONTAP。

可以使用灾难恢复协调器(DRO；具有UI的脚本式解决方案)无缝恢复从内部复制到FSX for ONTAP 的工作负载。DRO可通过VM注册到VMC自动从SnapMirror级别恢复到直接在NSX-T上进行的网络映射所有VMC环境都包含此功能。



入门

在**AWS**上部署和配置**VMware Cloud**

"基于 AWS 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软件定义的数据中心(SDDC)均在Amazon Virtual Private Cloud (VPC)中运行、并提供完整的VMware堆栈(包括vCenter Server)、NSX-T软件定义的网络连接、vSAN软件定义的存储以及一个或多个ESXi主机、这些主机可为工作负载提供计算和存储资源。要在AWS上配置VMC环境、请按照此处的步骤进行操作 "链接。"。此外、还可以使用引导灯集群进行灾难恢复。

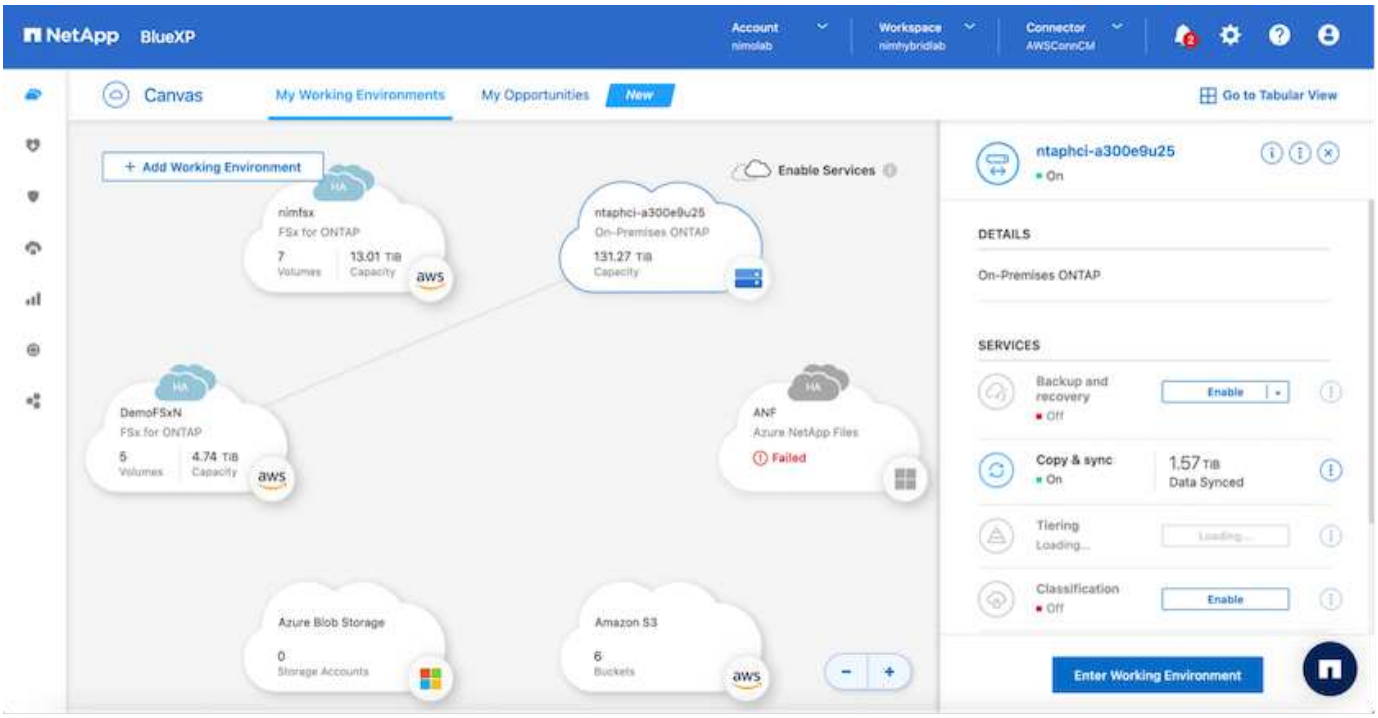
在初始版本中、DRO支持现有的试用集群。即将发布的版本将提供按需创建SDDC的功能。

为**ONTAP** 配置和配置**FSX**

适用于NetApp ONTAP 的Amazon FSX是一种完全托管的服务、可提供基于常见NetApp ONTAP 文件系统构建的高度可靠、可扩展、高性能和功能丰富的文件存储。请按照此处的步骤进行操作 "链接。" 为ONTAP 配置和配置FSX。

为适用于**ONTAP** 的**FSX**部署和配置**SnapMirror**

下一步是使用NetApp BlueXP并发现在AWS实例上为ONTAP 配置的FSX、并以适当的频率将所需的数据存储库卷从内部环境复制到适用于ONTAP 的FSX并保留NetApp Snapshot副本：



按照此链接中的步骤配置BlueXP。您也可以使用NetApp ONTAP 命令行界面计划通过此链接进行复制。

SnapMirror关系是前提条件、必须事先创建。

DRO安装

要开始使用DRO、请在指定EC2实例或虚拟机上使用Ubuntu操作系统、以确保满足前提条件。然后安装软件包。

前提条件

- 确保与源和目标vCenter以及存储系统建立连接。
- 如果使用的是DNS名称、则应进行DNS解析。否则、您应使用vCenter和存储系统的IP地址。
- 创建具有root权限的用户。您也可以将sudo与EC2实例结合使用。

操作系统要求

- Ubuntu 20.04 (LTS)、至少具有2 GB和4个vCPU
- 指定代理VM上必须安装以下软件包：
  - Docker
  - Docker构成
  - JQ

更改上的权限 `docker.sock`： `sudo chmod 666 /var/run/docker.sock`。

。 `deploy.sh` 此脚本将执行所有必需的前提条件。

安装软件包

1. 在指定虚拟机上下载安装包：

```
git clone https://github.com/NetApp/DRO-AWS.git
```

该代理可以安装在内部环境中、也可以安装在AWS VPC中。

2. 解压缩软件包、运行部署脚本、然后输入主机IP (例如10.10.10.10)。

```
tar xvf DRO-prereq.tar
```

3. 导航到目录并按如下所示运行Deploy脚本：

```
sudo sh deploy.sh
```

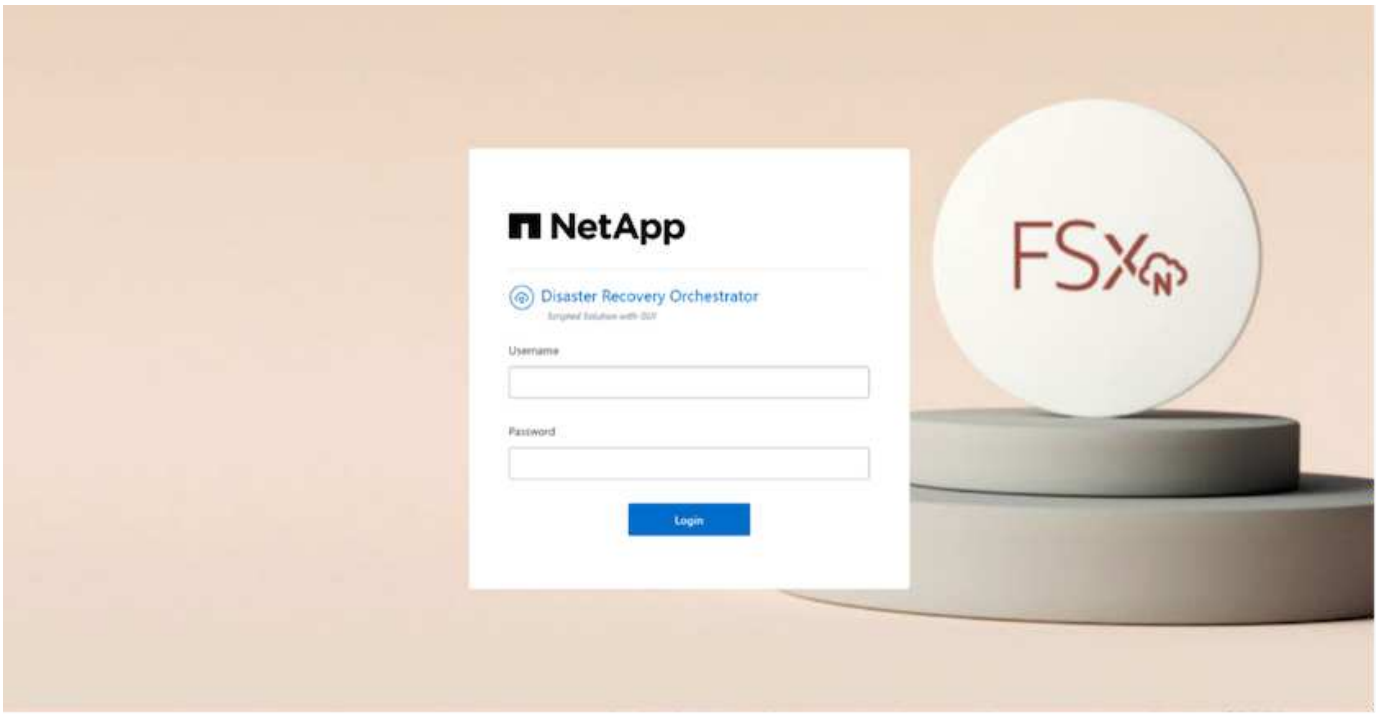
4. 使用以下命令访问UI：

```
https://<host-ip-address>
```

使用以下默认凭据：

```
Username: admin
Password: admin
```

可以使用"更改密码"选项更改密码。



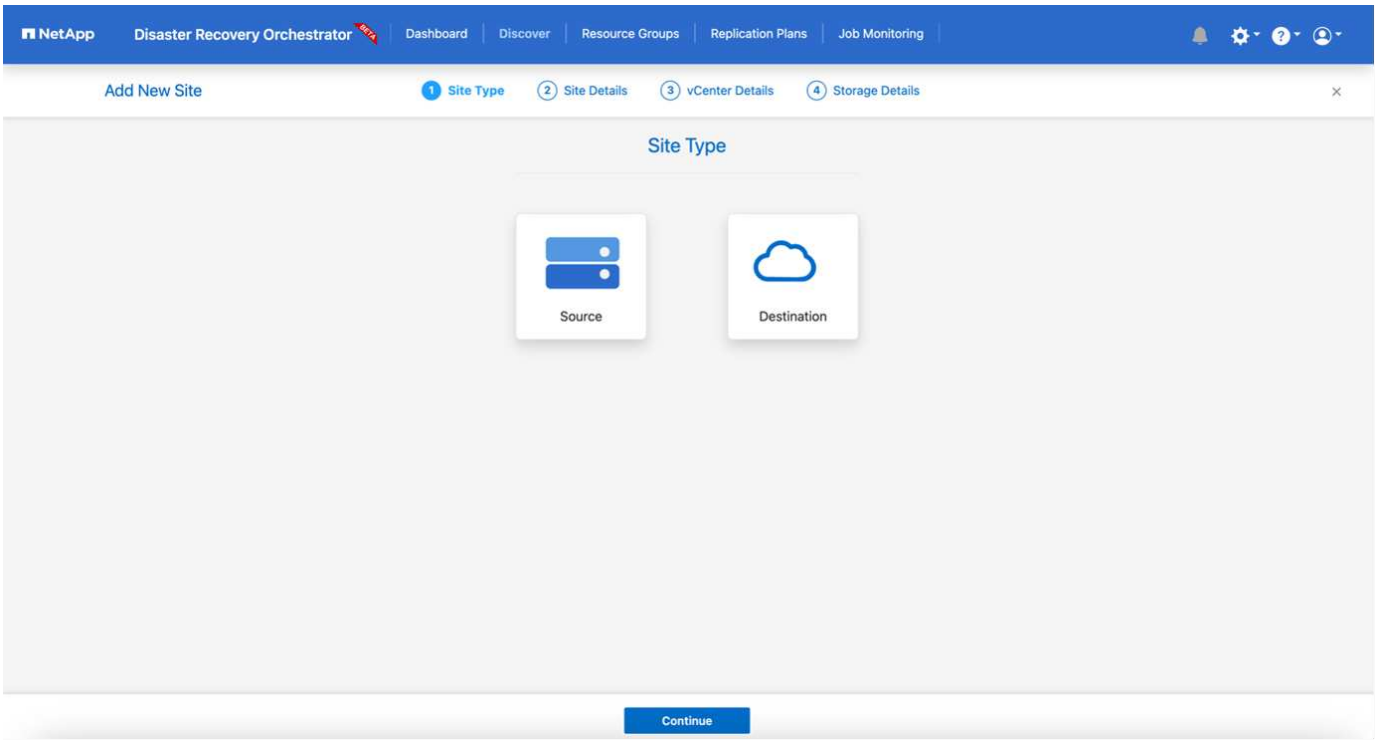
DRO配置

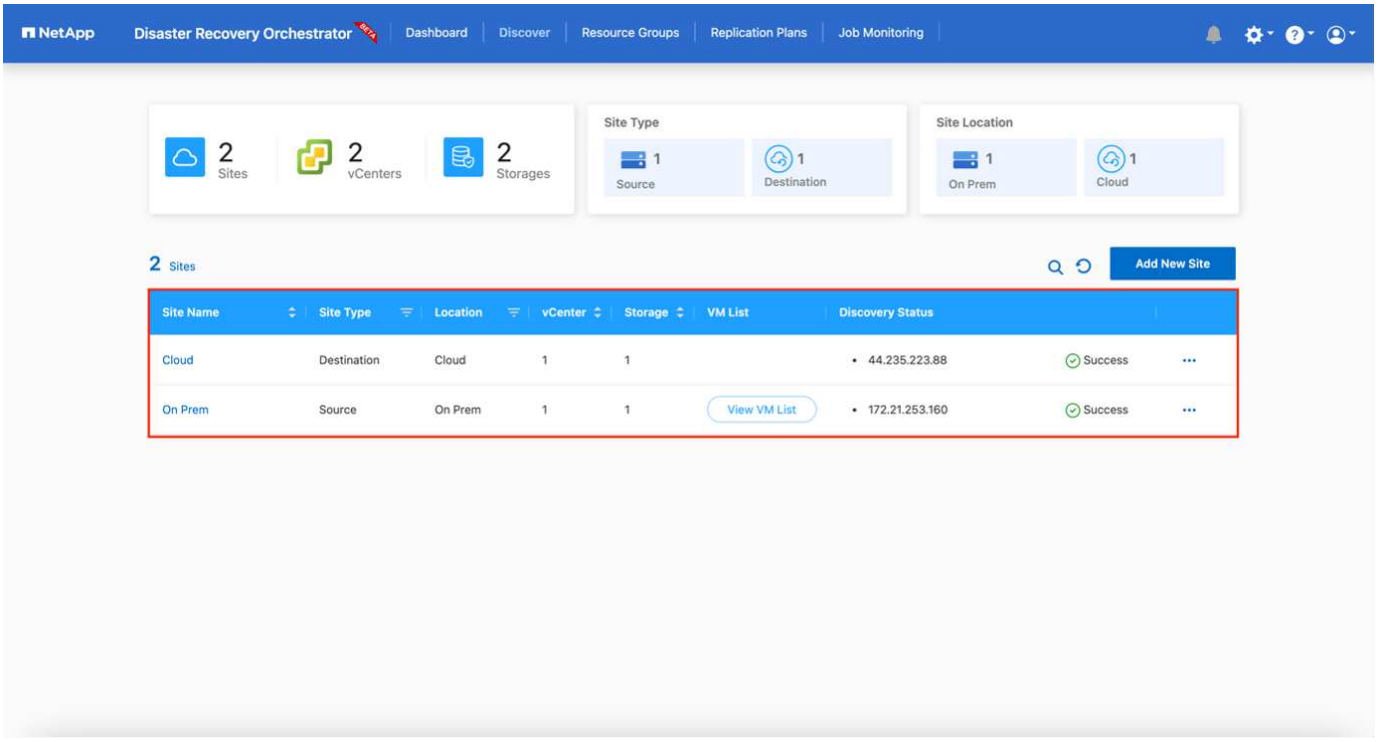
正确配置适用于ONTAP 的FSX和VMC之后、您可以开始配置DRO、以便使用适用于ONTAP 的FSX上的只读SnapMirror副本自动将内部工作负载恢复到VMC。

NetApp建议在AWS中部署DRO代理、并将其部署到部署了FSX for ONTAP 的同一VPC上(也可以通过对等连接)。这样、DRO代理便可通过网络与内部组件以及适用于ONTAP 的FSX和VMC资源进行通信。

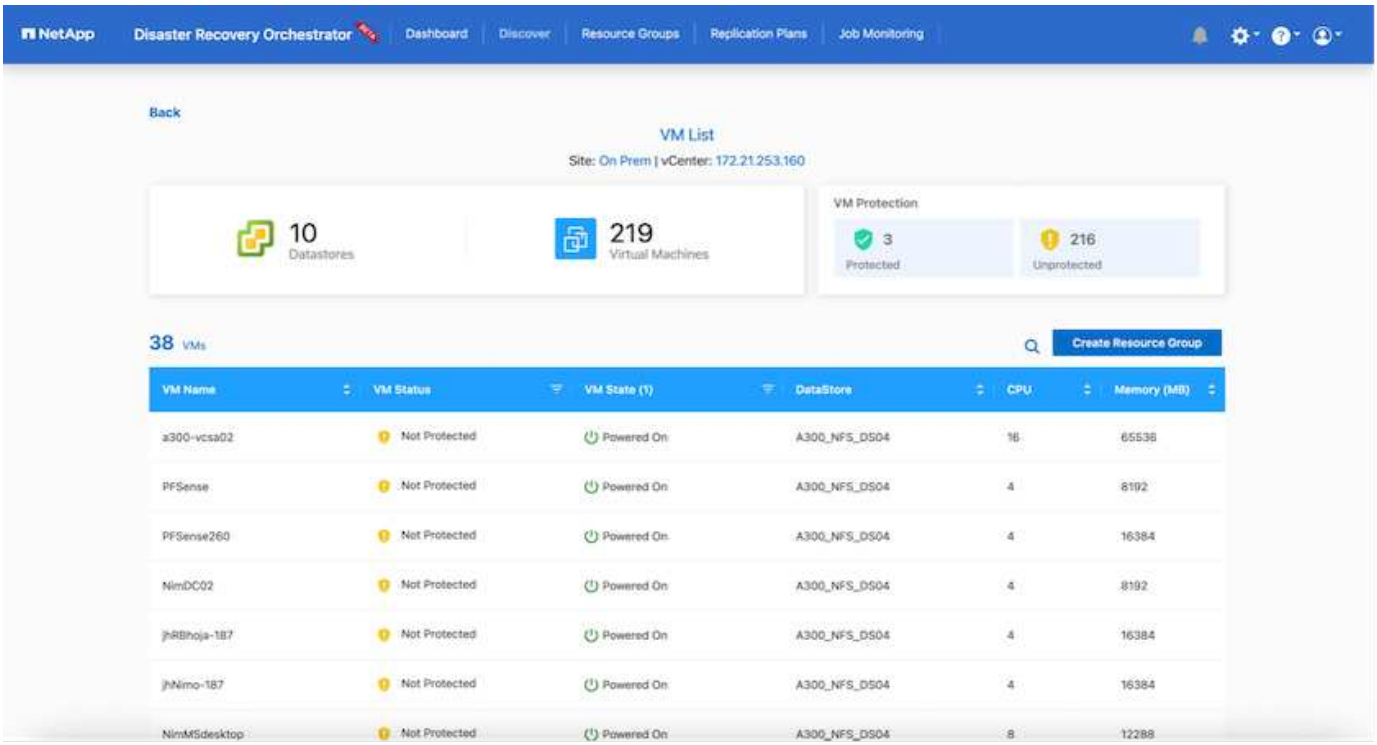
第一步是发现内部资源和云资源(vCenter和存储)并将其添加到DRO中。在支持的浏览器中打开DRO、并使用默认用户名和密码(admin/admin)以及添加站点。也可以使用发现选项添加站点。添加以下平台：

- 内部部署
  - 内部vCenter
  - ONTAP 存储系统
- 云
  - VMC vCenter
  - 适用于 ONTAP 的 FSX





添加后、DRO将执行自动发现、并显示具有从源存储到适用于ONTAP 的FSX的相应SnapMirror副本的VM。DRO会自动检测VM使用的网络和端口组并对其进行填充。



下一步是将所需的VM分组到功能组中、以用作资源组。

资源分组

添加平台后、您可以将要恢复的VM分组到资源组中。使用DRO资源组、您可以将一组依赖虚拟机分组到逻辑组中、这些逻辑组包含启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

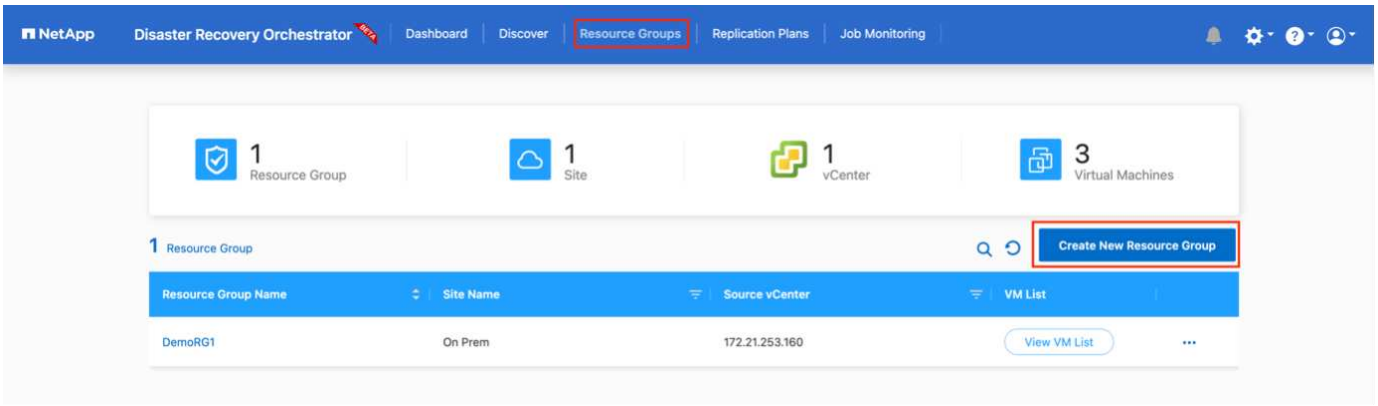
要开始创建资源组、请完成以下步骤：

1. 访问*资源组*、然后单击*创建新资源组*。
2. 在*新建资源组*下、从下拉列表中选择源站点、然后单击*创建*。
3. 提供*资源组详细信息*并单击*继续*。
4. 使用搜索选项选择相应的VM。
5. 选择选定虚拟机的启动顺序和启动延迟(秒)。通过选择每个VM并设置其优先级来设置启动顺序。所有VM的默认值均为3。

   选项如下：

   1—第一个启动的虚拟机3—默认值5—最后一个启动的虚拟机

6. 单击*创建资源组*。

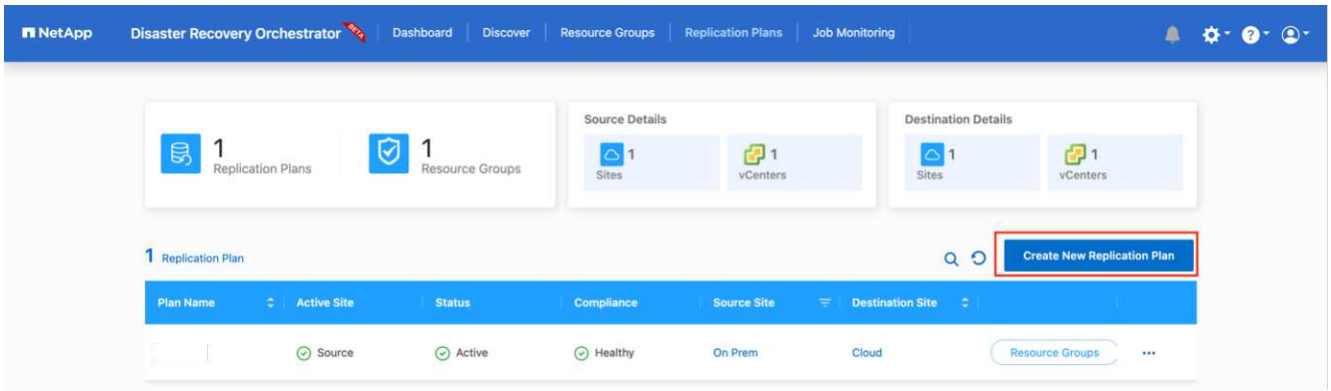


复制计划

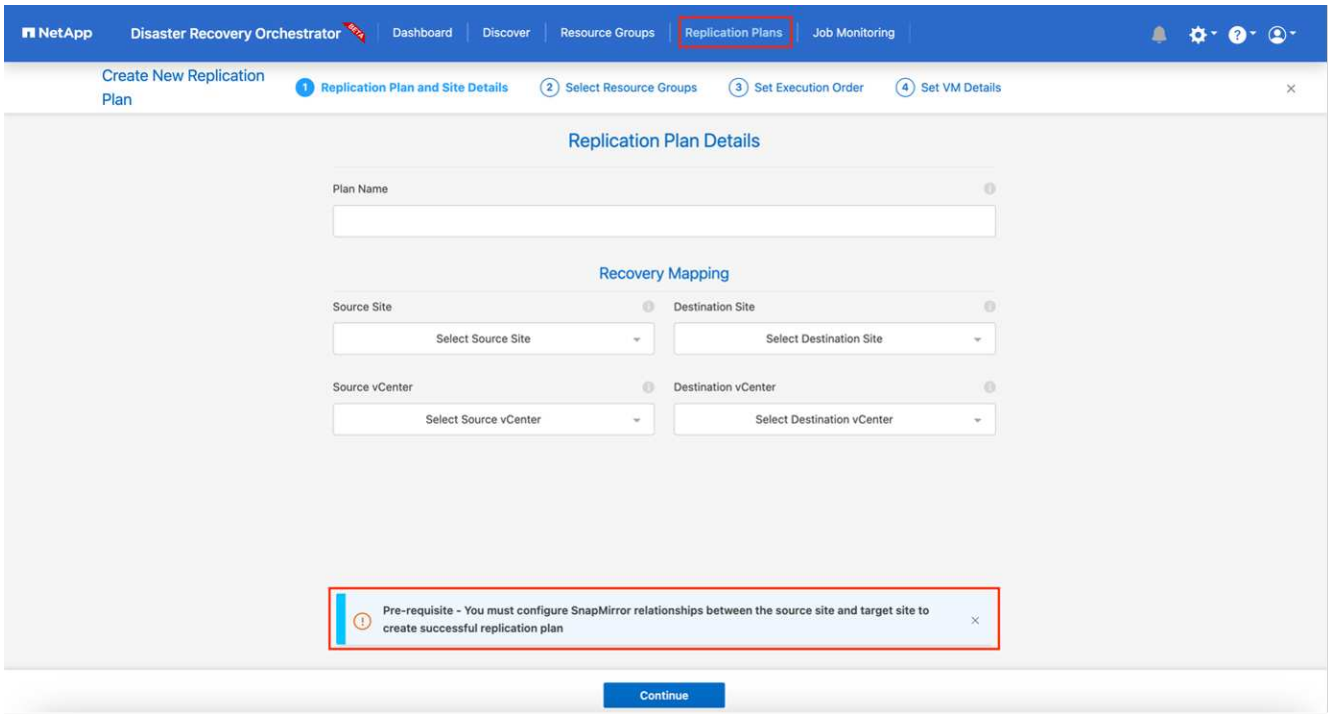
您需要制定计划、以便在发生灾难时恢复应用程序。从下拉列表中选择源和目标vCenter平台、然后选择要包含在此计划中的资源组、以及应用程序应如何还原和启动的分组(例如、域控制器、第1层、第2层等)。此类计划有时也称为蓝图。要定义恢复计划、请导航到*复制计划*选项卡、然后单击*新建复制计划*。

要开始创建复制计划、请完成以下步骤：

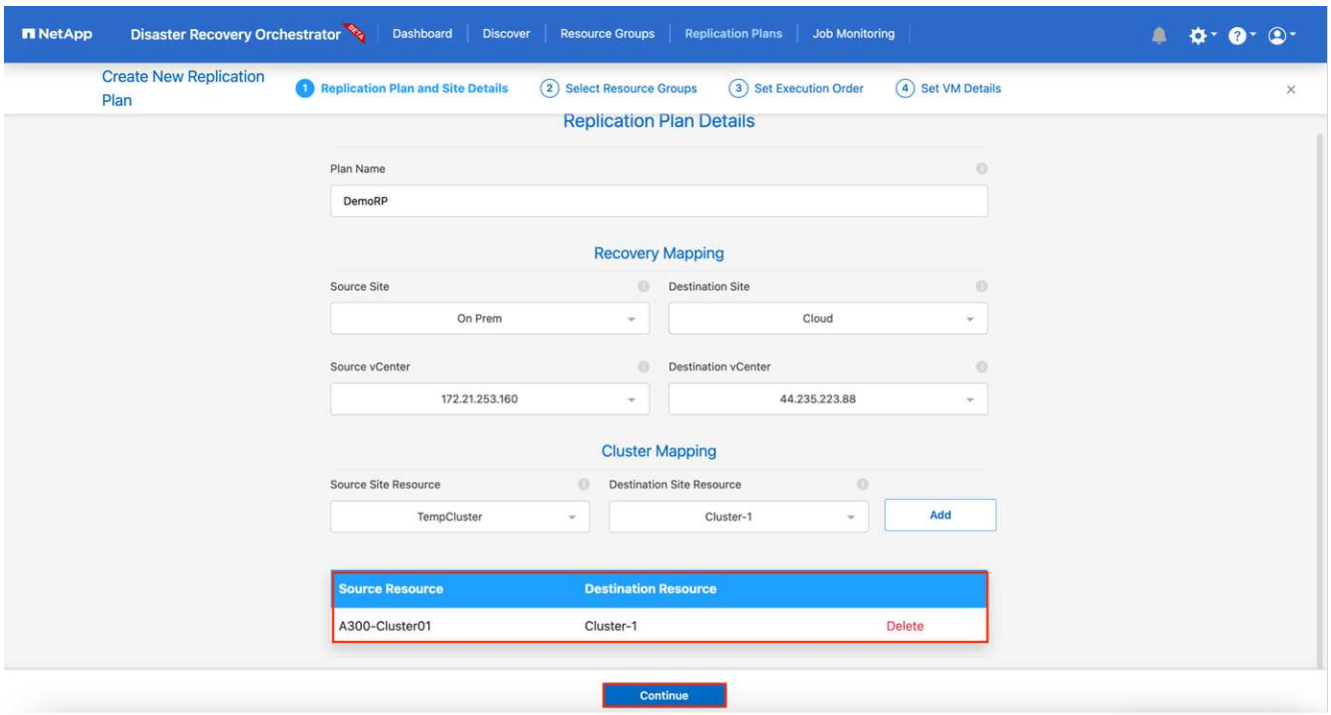
1. 访问*复制计划*、然后单击*创建新复制计划*。



2. 在*新复制计划*下、为计划提供一个名称、并通过选择源站点、关联的vCenter、目标站点和关联的vCenter来添加恢复映射。

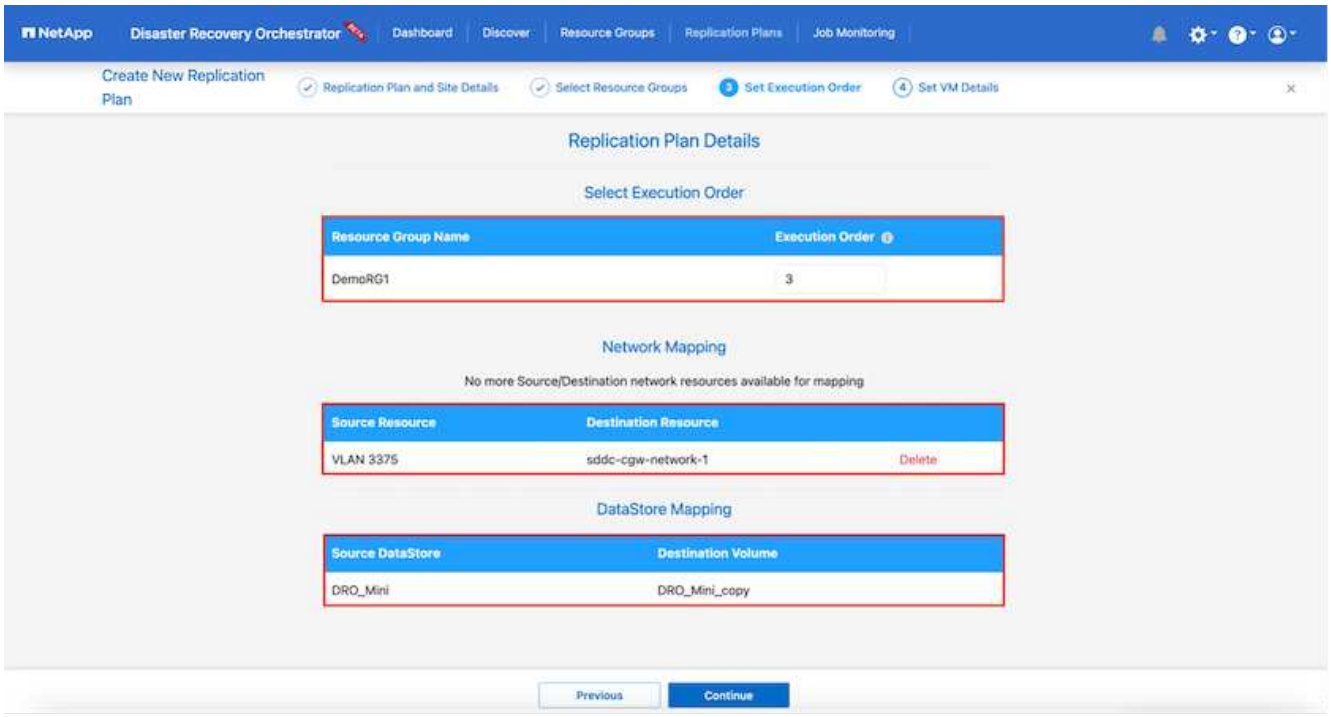


3. 恢复映射完成后、选择集群映射。

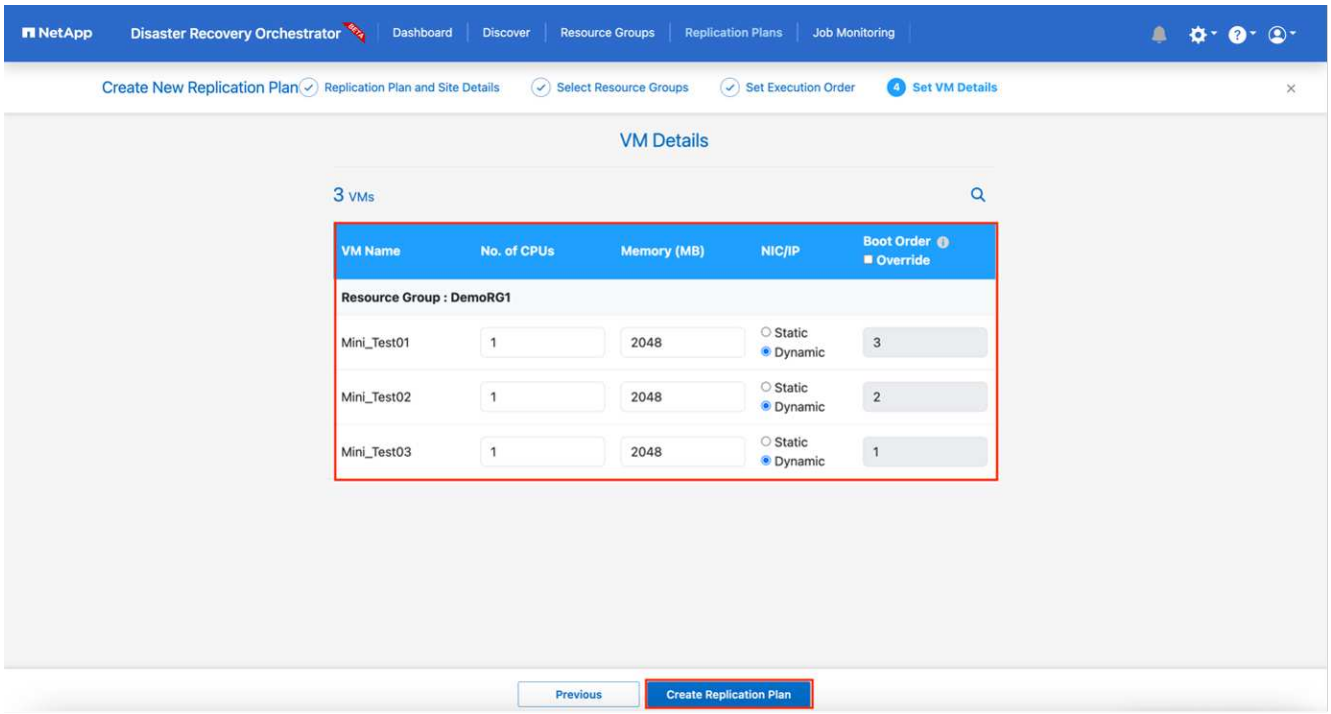


4. 选择*资源组详细信息*、然后单击*继续*。
5. 设置资源组的执行顺序。使用此选项可以选择存在多个资源组时的操作顺序。
6. 完成后、选择指向相应网段的网络映射。应已在VMC中配置这些区块、因此请选择适当的区块以映射虚拟机。
7. 根据VM的选择、系统会自动选择数据存储库映射。

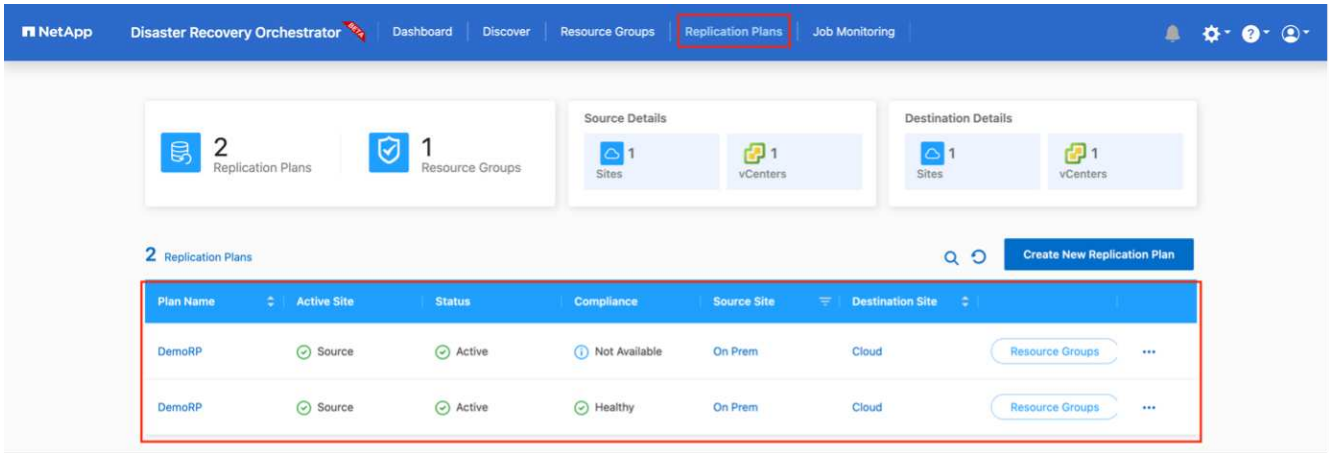
SnapMirror处于卷级别。因此、所有VM都会复制到复制目标。确保选择属于数据存储库的所有VM。如果未选择这些虚拟机、则仅会处理属于复制计划的虚拟机。



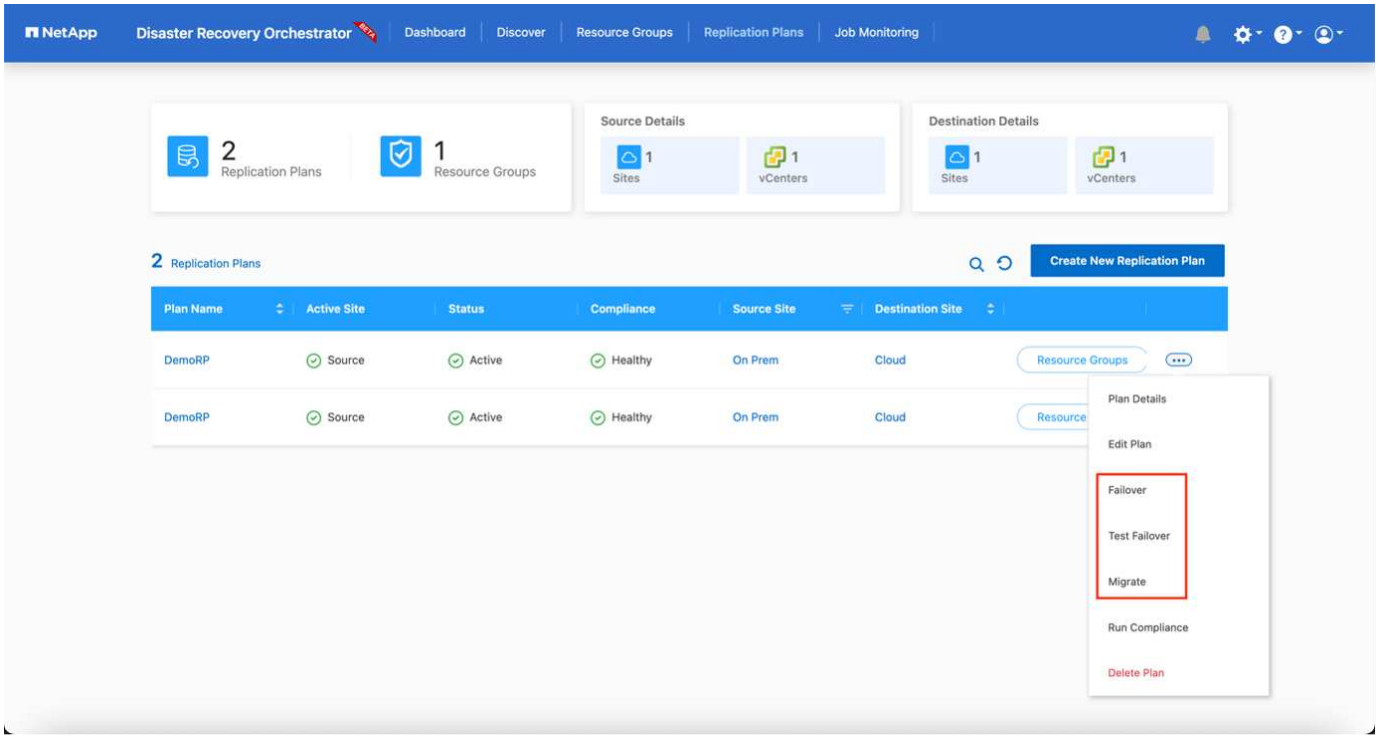
8. 在VM详细信息下、您可以选择调整VM的CPU和RAM参数大小；在将大型环境恢复到较小的目标集群或执行灾难恢复测试而无需配置一对一物理VMware基础架构时、这会非常有用。此外、您还可以修改资源组中所有选定虚拟机的启动顺序和启动延迟(秒)。如果需要对资源组启动顺序选择期间选择的启动顺序进行任何更改、还可以选择修改启动顺序。默认情况下、系统会使用在选择资源组期间选择的启动顺序；但是、在此阶段可以执行任何修改。

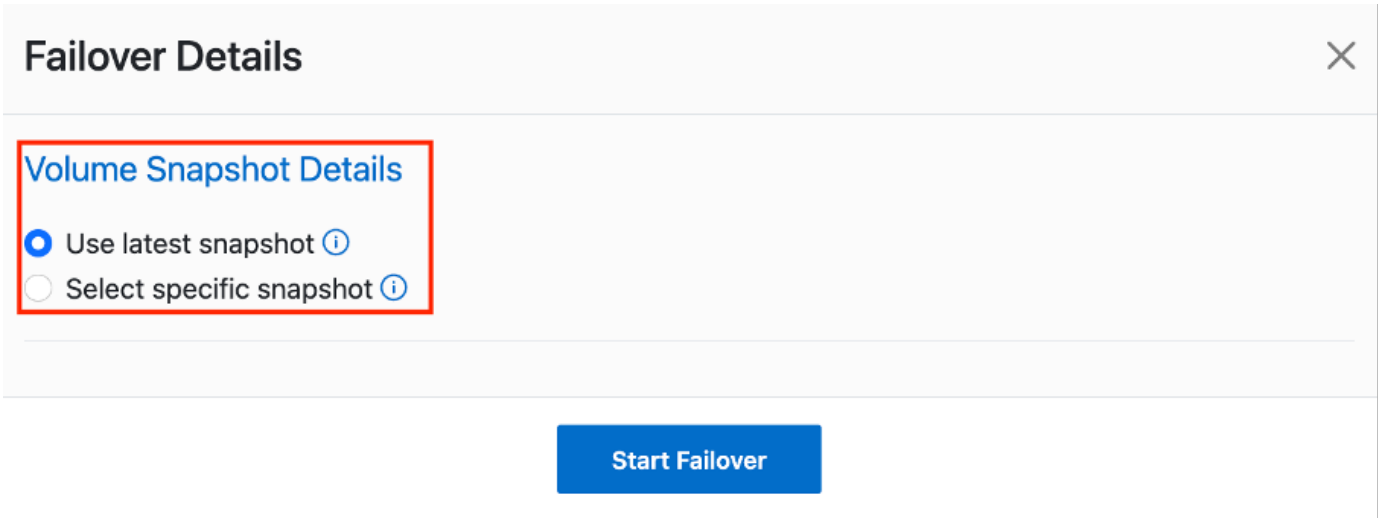


9. 单击*创建复制计划*。

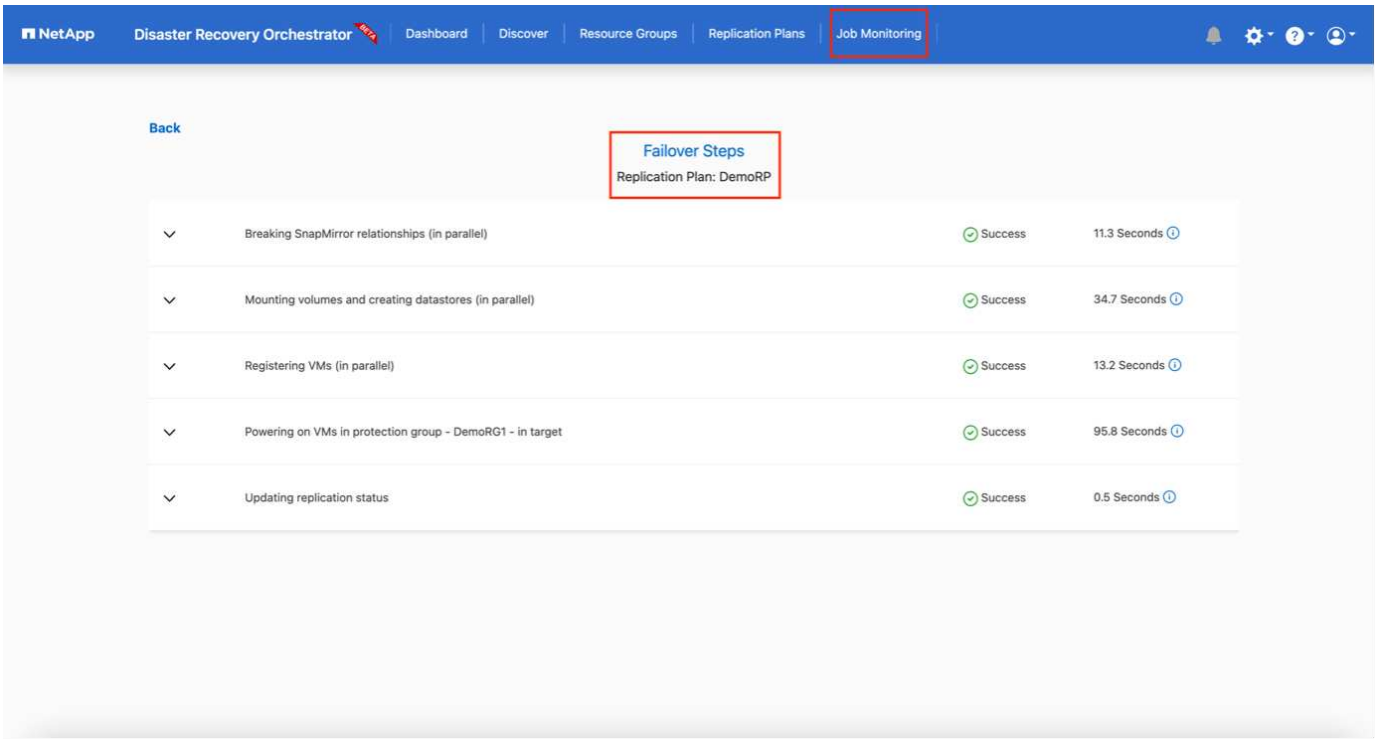


创建复制计划后、可以根据需要使用故障转移选项、test-failover选项或migrate选项。在故障转移和测试-故障转移选项期间、将使用最新的SnapMirror Snapshot副本、或者可以从时间点Snapshot副本中选择特定的Snapshot副本(按照SnapMirror的保留策略)。如果您遇到勒索软件等损坏事件、而最新副本已被泄露或加密、则时间点选项可能会非常有用。DRO显示所有可用时间点。要使用复制计划中指定的配置触发故障转移或测试故障转移、可以单击*故障转移*或*测试故障转移*。

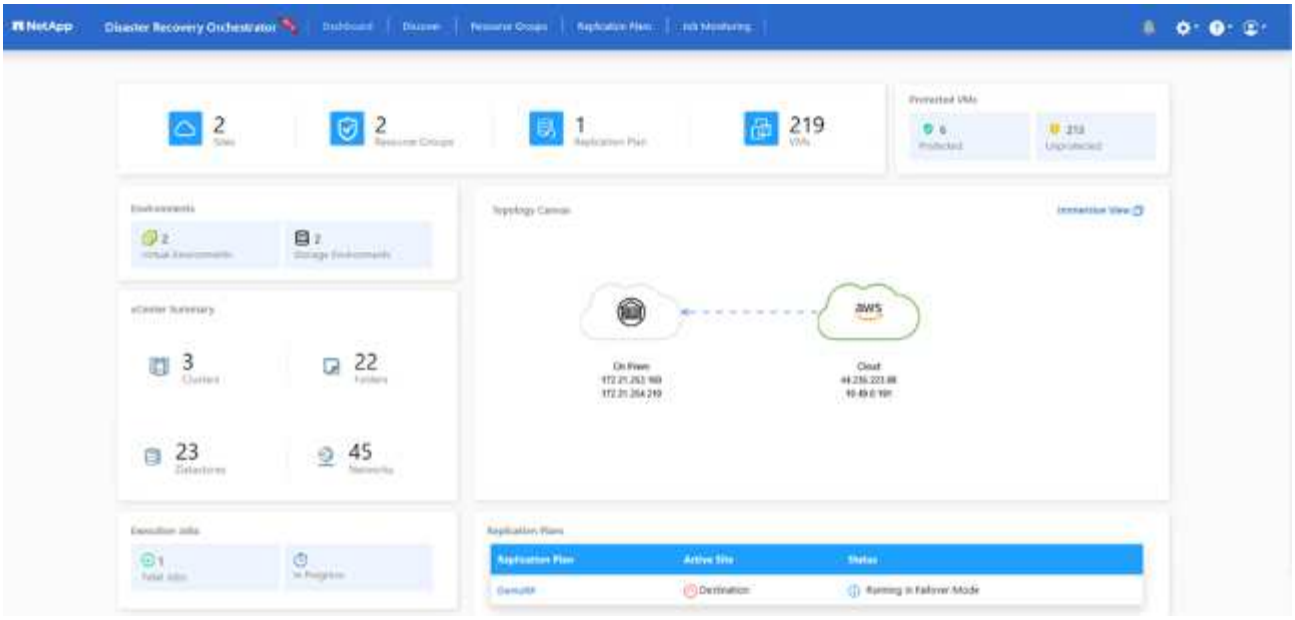




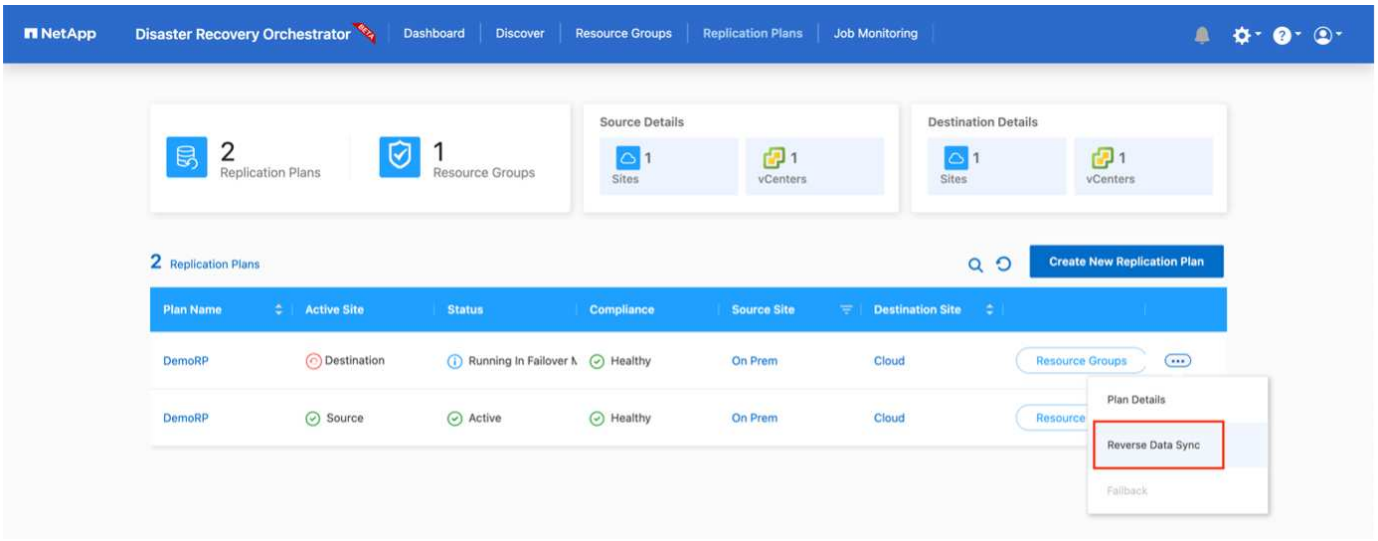
可以在任务菜单中监控复制计划：

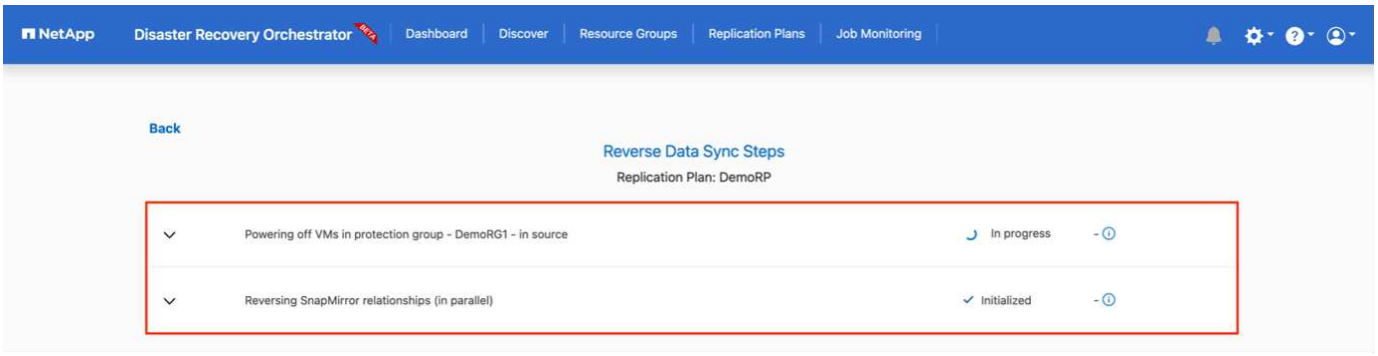


触发故障转移后、可以在VMC vCenter中看到恢复的项目(VM、网络、数据存储库)。默认情况下、VM将恢复到工作负载文件夹。

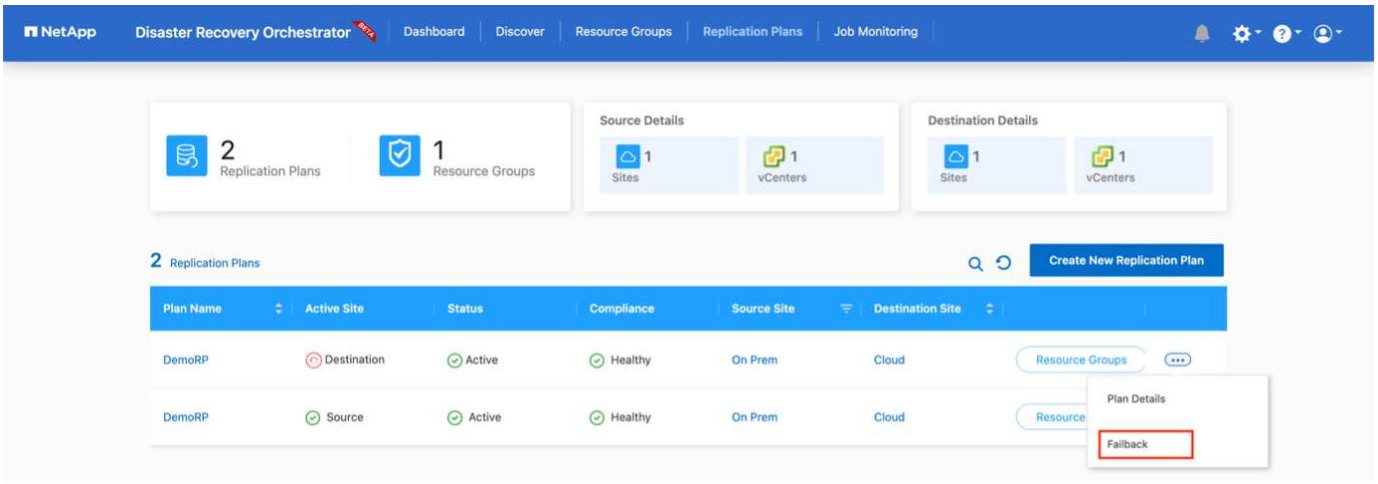


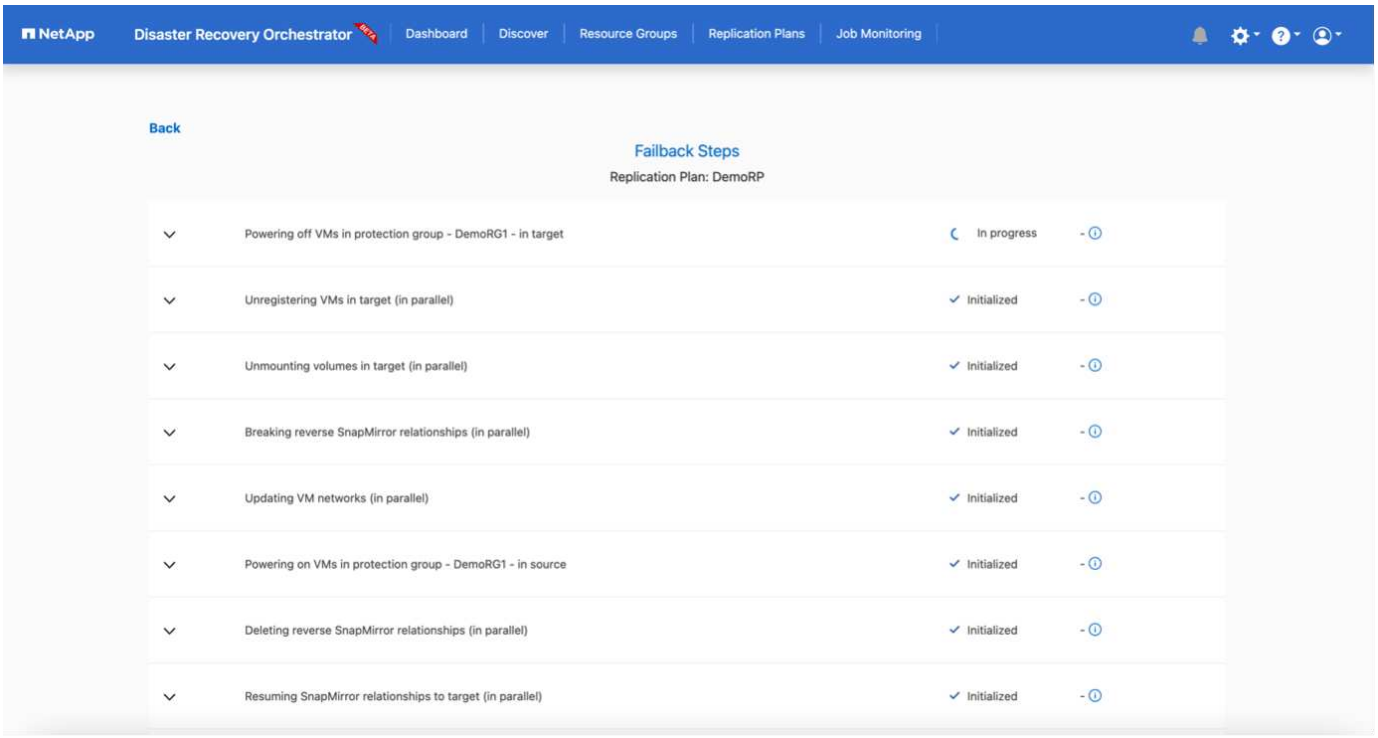
可以在复制计划级别触发故障恢复。对于测试故障转移、可以使用卸载选项回滚更改并删除FlexClone关系。与故障转移相关的故障恢复过程分为两步。选择复制计划并选择*反向数据同步*。



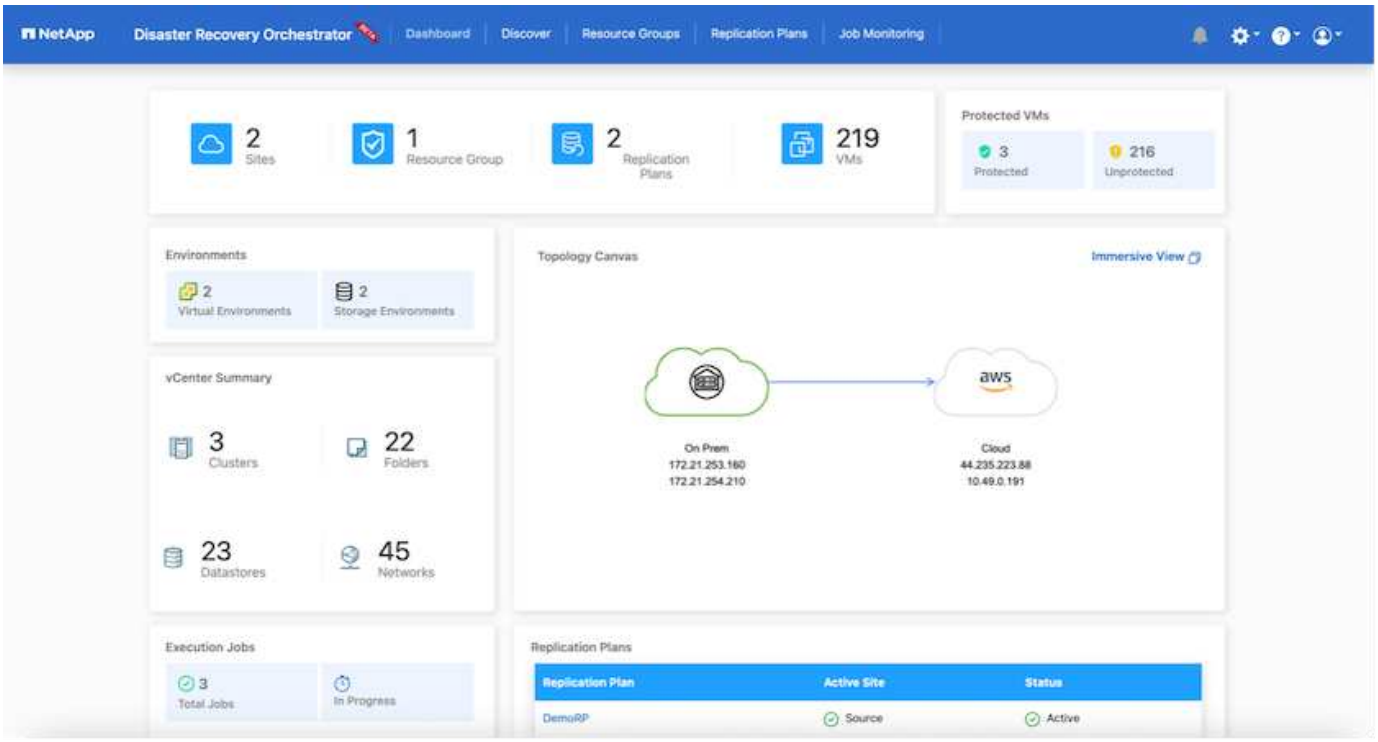


完成后、您可以触发故障恢复以移回原始生产站点。





在NetApp BlueXP中、我们可以看到相应卷(已映射到VMC的读写卷)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。相反、它会为所需的SnapMirror (或Snapshot)实例创建一个FlexClone副本、并公开FlexClone实例、这样不会占用适用于ONTAP 的FSX的额外物理容量。此过程可确保卷不会被修改、并且即使在灾难恢复测试或鉴别工作流期间、副本作业也可以继续执行。此外、此过程还可确保在发生错误或恢复损坏的数据时、可以清理恢复过程、而不会造成副本被销毁的风险。



勒索软件恢复

从勒索软件中恢复可能是一项艰巨的任务。具体而言、IT组织很难确定安全的返回点、一旦确定、就很难保护已恢复的工作负载、防止再次发生攻击、例如、休眠的恶意软件或容易受到攻击的应用程序。

DRO可帮助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正常运行且彼此隔离的网络、以便应用程序可以在不受北-南流量影响的位置彼此运行和通信。这样、您的安全团队就可以安全地进行取证、并确保没有隐藏或休眠的恶意软件。

优势

- 使用高效且具有故障恢复能力的SnapMirror复制。
- 使用Snapshot副本保留功能恢复到任何可用时间点。
- 完全自动化执行从存储、计算、网络和应用程序验证步骤中恢复成百上千个VM所需的所有步骤。
- 使用ONTAP FlexClone技术执行工作负载恢复、方法不会更改复制的卷。
  - 避免卷或Snapshot副本发生数据损坏的风险。
  - 在灾难恢复测试工作流期间避免复制中断。
  - 将灾难恢复数据与云计算资源一起用于灾难恢复以外的工作流、例如DevTest、安全测试、修补或升级测试以及修复测试。
- CPU和RAM优化、可通过恢复到较小的计算集群来帮助降低云成本。

使用**Veeam Replication**和**FSx for ONTAP**将灾难恢复到**AWS**上的**VMware Cloud**

作者：Niyaz Mohamed - NetApp解决方案工程部

概述

Amazon FSx for NetApp ONTAP与AWS上的VMware Cloud集成是一个AWS管理的外部NFS数据存储库、该数据存储库基于NetApp的ONTAP文件系统构建、可以连接到SDDC中的集群。它为客户提供了灵活的高性能虚拟化存储基础架构、该基础架构可独立于计算资源进行扩展。

对于希望将基于AWS SDDC的VMware Cloud用作灾难恢复目标的客户、可以使用FSx for ONTAP数据存储库通过任何经过验证的第三方从内部复制数据、此类解决方案可提供VM复制功能。通过添加FSx for ONTAP数据存储库、与在AWS SDDC上使用大量ESXi主机来容纳存储相比、它将实现成本优化的部署。

此方法还有助于客户在VMC中使用试点轻型集群以及FSx for ONTAP数据存储库来托管VM副本。通过妥善地对复制计划进行故障转移、也可以将同一过程作为一个迁移选项扩展到AWS上的VMware Cloud。

问题陈述

本文档介绍如何使用FSx for ONTAP数据存储库以及Veeam备份和复制功能为内部VMware VM设置灾难恢复、并将其恢复到AWS上的VMware Cloud。

Veeam Backup & Replication支持通过现场和远程复制实现灾难恢复(Disaster Recovery、DR)。复制虚拟机时、Veeam Backup & Replication会在AWS SDDC集群上的目标VMware Cloud上以本机VMware vSphere格式创建VM的精确副本、并使该副本与原始VM保持同步。

复制可提供最佳恢复时间目标(Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time 此复制机制可确保在发生灾难事件时、工作负载可以在AWS SDDC上的VMware Cloud中快速启动。Veeam Backup & Replication软件还可以优化流量传输、以便通过WAN和慢速连接进行复制。此外、它还会筛选出重复的数据块、将数据块置零、交换文件和排除的VM子操作系统文件、并压缩副本流量。

为了防止复制作业占用整个网络带宽、可以设置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、则可以通过故障转移到VM副本来触发故障转移以恢复VM。

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正常的还原点。这样便可根据需要进行勒索软件恢复或隔离测试。在Veeam Backup & Replication中、故障转移和故障恢复是临时的中间步骤、应进一步完成。Veeam Backup & Replication提供了多种选项来处理不同的灾难恢复场景。

[使用Veeam Replication和FSx ONTAP for VMC的灾难恢复场景示意图]

解决方案 部署

高级步骤

1. Veeam Backup and Replication软件正在具有适当网络连接的内部环境中运行。
2. 配置基于AWS的VMware Cloud、请参见VMware Cloud Tech Zone文章 "《VMware Cloud on AWS与Amazon FSx for NetApp ONTAP集成部署指南》" 要进行部署、请将基于AWS SDDC的VMware Cloud和适用于ONTAP的FSx配置为NFS数据存储库。(采用最低配置设置的指示灯环境可用于灾难恢复。发生意外事件时、VM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. 灾难事件完成且主站点启动后、切换回生产VM。

将**Veeam VM**复制到适用于**ONTAP**数据存储库的**VMC**和**FSx**的前提条件

1. 确保Veeam Backup & Replication备份VM已连接到源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和目标vCenter。
3. 适用于ONTAP数据存储库的目标FSx必须具有足够的可用空间来存储已复制VM的VMDK

对于追加信息、请参阅介绍的"注意事项和限制" "此处"。

部署详细信息

第**1**步：复制**VM**

Veeam Backup & Replication利用VMware vSphere快照功能、在复制期间、Veeam Backup & Replication会请求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使用快照作为复制数据源。

要复制VM、请执行以下步骤：

1. 打开Veeam Backup & Replication Console。
2. 在主页视图中、选择复制作业>虚拟机> VMware vSphere。
3. 指定作业名称并选中相应的高级控制复选框。单击下一步。
   - 如果内部和AWS之间的连接带宽受限、请选中副本传播复选框。
   - 如果AWS SDDC上VMware Cloud上的区块与内部站点网络不匹配、请选中网络重新映射(适用于具有不同网络的AWS VMC站点)复选框。
   - 如果内部生产站点中的IP地址方案与AWS VMC站点中的方案不同、请选中"副 本重新IP (适用于具有不同IP地址方案的灾难恢复站点)"复选框。

     [灾难恢复Veeam FSx版本2] | *dr-veeam-fsx-image2.png*
4. 在*虚拟机*步骤中、选择需要复制到连接到AWS SDDC上的VMware Cloud的FSx for ONTAP数据存储库的VM。可以将虚拟机放置在vSAN上、以填满可用的vSAN数据存储库容量。在指示灯集群中、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 for ONTAP数据存储库。单击*Add*，然后在*Add Object*窗口中选择所需的VM或VM容器，然后单击*Add*。单击 * 下一步 * 。

   [灾难恢复Veeam FSx版本3] | *dr-veeam-fsx-image3.png*
5. 之后、选择目标作为AWS SDDC上的VMware Cloud集群/主机、并为VM副本选择相应的资源池、VM文件夹和FSx for ONTAP数据存储库。然后单击*Next*。

   [灾难恢复Veeam FSx版本4] | *dr-veeam-fsx-image4.png*
6. 在下一步中、根据需要创建源虚拟网络与目标虚拟网络之间的映射。

   [灾难恢复Veeam FSx版本5] | *dr-veeam-fsx-image5.png*
7. 在*作业设置*步骤中，指定要存储VM副本元数据、保留策略等的备份存储库。
8. 在“数据传输”步骤中更新*Source*和*Target*代理服务器，保留“自动*选择”(默认)并保持“*直接”选项处于选中状态，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 * 。

   [灾难恢复Veeam FSx版本6] | *dr-veeam-fsx-image6.png*
10. 选择复制计划以定期运行复制作业。
11. 在向导的*摘要*步骤中，查看复制作业的详细信息。要在关闭向导后立即启动作业，请选中*单击完成时运行作业*复选框，否则不要选中该复选框。然后单击*完成*关闭向导。

    [灾难恢复Veeam FSx版本7] | *dr-veeam-fsx-image7.png*

复制作业启动后、目标VMC SDDC集群/主机上将填充具有指定后缀的VM。

[灾难恢复Veeam FSx版本8] | *dr-veeam-fsx-image8.png*

有关追加信息for Veeam复制的信息、请参见 "复制的工作原理"。

第**2**步：创建故障转移计划

初始复制或传播完成后、创建故障转移计划。故障转移计划有助于逐个或以组的形式自动对相关VM执行故障转移。故障转移计划是VM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的相关VM已在运行。

要创建计划、请导航到名为副本的新子部分、然后选择故障转移计划。选择适当的VM。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。

只有在初始复制完成且虚拟机副本处于就绪状态时、才能添加故障转移计划。

在运行故障转移计划时、最多可同时启动10个VM。

在故障转移过程中、源VM不会关闭。

要创建*故障转移计划*，请执行以下操作：

1. 在主页视图中，选择*故障转移计划> VMware vSphere。
2. 接下来、提供计划的名称和问题描述。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VM之前、请运行一个脚本来关闭VM。

   [灾难恢复Veeam FSx版本9] | *dr-veeam-fsx-image9.png*

3. 将VM添加到计划中、并修改VM启动顺序和启动延迟、以满足应用程序依赖关系。

   [灾难恢复Veeam FSx版本10] | *dr-veeam-fsx-image10.png*

有关用于创建复制作业的追加信息、请参见 "正在创建复制作业"。

第**3**步：运行故障转移计划

在故障转移期间、生产站点中的源VM将切换到灾难恢复站点上的副本。在故障转移过程中、Veeam Backup & Replication会将VM副本还原到所需的还原点、并将所有I/O活动从源VM移至其副本。不仅可以在发生灾难时使用副本、还可以用于模拟灾难恢复演练。在模拟故障转移期间、源VM将保持运行状态。执行完所有必要的测试后、您可以撤消故障转移并恢复正常操作。

确保网络分段到位、以避免灾难恢复期间发生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 * 。此操作将使用虚拟机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*Start to *。

[灾难恢复Veeam FSx image11] | *dr-veeam-fsx-image11.png*

[DR Veeam FSx版本12] | *dr-veeam-fsx-image12.png*

VM副本的状态将从"准备就绪"更改为"故障转移"、VM将在AWS SDDC集群/主机上的目标VMware Cloud上启动。

[灾难恢复Veeam FSx版本13.] | *dr-veeam-fsx-image13.png*

故障转移完成后、VM的状态将更改为"故障转移"。

[DR Veeam FSx版本14.] | *dr-veeam-fsx-image14.png*

Veeam Backup & Replication会停止源VM的所有复制活动、直到其副本恢复到就绪状态为止。

有关故障转移计划的详细信息、请参见 "故障转移计划"。

第**4**步：故障恢复到生产站点

当故障转移计划正在运行时、它会被视为一个中间步骤、需要根据需要最终确定。选项包括：

- 故障恢复到生产环境-切换回原始虚拟机并将虚拟机副本运行期间发生的所有更改传输至原始虚拟机。

> 执行故障恢复时、只会传输更改、但不会发布更改。如果原始虚拟机未按预期工作，请选择*commit failback*(确认原始虚拟机按预期工作后)或*Undo failback*(撤消故障恢复)返回到虚拟机副本。

- 撤消故障转移-切换回原始虚拟机并放弃在虚拟机副本运行期间对其所做的所有更改。
- 永久故障转移-从原始虚拟机永久切换到虚拟机副本，并将此副本用作原始虚拟机。

在此演示中、我们选择了故障恢复到生产环境。在向导的目标步骤中选择了故障恢复到原始虚拟机、并启用了"Power On VM after Restoring"(还原后启动虚拟机)复选框。

[灾难恢复Veeam FSx版本15] | *dr-veeam-fsx-image15.png*

[DR Veeam FSx版本16] | *dr-veeam-fsx-image16.png*

提交故障恢复是完成故障恢复操作的方法之一。提交故障恢复后、它会确认发送到故障恢复虚拟机(生产虚拟机)的更改是否按预期工作。完成提交操作后、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、请参见的Veeam文档 "故障转移和故障恢复以进行复制"。

[DR Veeam FSx版本17.] | *dr-veeam-fsx-image17.png*

[DR Veeam FSx版本18.] | *dr-veeam-fsx-image18.png*

成功故障恢复到生产环境后、所有VM都会还原回原始生产站点。

[DR Veeam FSx版本19] | *dr-veeam-fsx-image19.png*

结论

借助FSx for ONTAP数据存储库功能、Veeam或任何经过验证的第三方工具可以使用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来容纳VM副本。这样可以提供一个功能强大的解决方案来处理定制的自定义灾难恢复计划、还可以重复使用内部现有备份产品来满足灾难恢复需求、从而通过在内部部署现有灾难恢复数据中心实现基于云的灾难恢复。发生灾难时、只需单击一个按钮、即可按计划进行故障转移或故障转移、并决定激活灾难恢复站点。

要了解有关此过程的更多信息、请随时观看详细的演练视频。

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

作者：NetApp Solutions Engineering

概述：迁移具有**VMware HCX**、**FSX ONTAP** 补充数据存储库和**VMware Cloud**的虚拟机

迁移VMware工作负载是Amazon Web Services (AWS)上的VMware Cloud (VMC)及其在Amazon FSx for NetApp ONTAP 上的补充NFS数据存储库的一个常见使用情形。VMware HCX是首选选项、它提供了多种迁移方法、用于将在任何VMware支持的数据存储库上运行的内部虚拟机(VM)及其数据移动到VMC数据存储库、其中包括适用于ONTAP 的FSX上的补充NFS数据存储库。

VMware HCX主要是一个移动平台、旨在简化工作负载迁移、工作负载重新平衡以及跨云的业务连续性。它作为VMware Cloud on AWS的一部分提供、可通过多种方式迁移工作负载、并可用于灾难恢复(DR)操作。

本文档提供了部署和配置VMware HCX的分步指导、其中包括其所有主要组件、内部部署和云数据中心端、从而支持各种VM迁移机制。

有关详细信息，请参见 "HCX部署简介" 和 "安装检查清单B—在AWS SDDC目标环境中使用VMware Cloud的HCX"。

高级步骤

此列表概括介绍了安装和配置VMware HCX的步骤：

1. 通过VMware Cloud Services Console为VMC软件定义的数据中心(SDDC)激活HCX。
2. 在内部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. 将内部部署的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进行迁移。
8. 迁移VM工作负载。

前提条件

开始之前、请确保满足以下前提条件。有关详细信息，请参见 "准备安装HCX"。具备连接等前提条件后、可从VMC的VMware HCX控制台生成许可证密钥来配置和激活HCX。激活HCX后、将部署vCenter插件、并可使用vCenter控制台进行访问以进行管理。

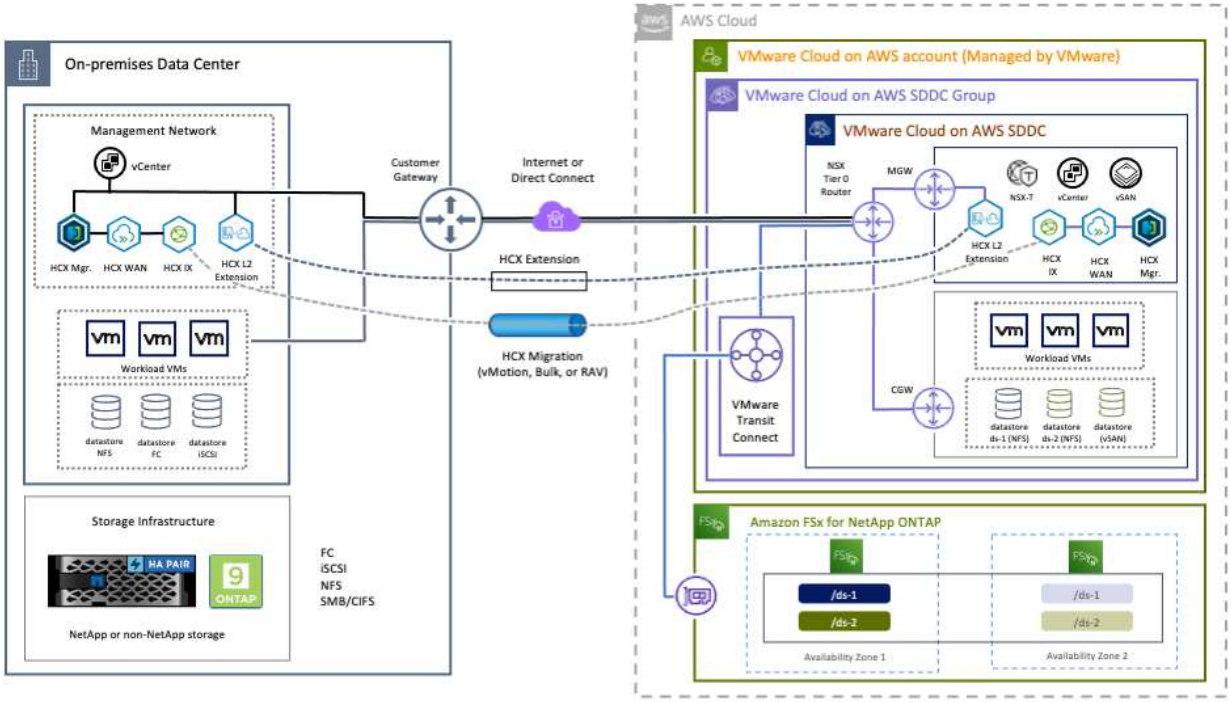
在继续执行HCX激活和部署之前、必须完成以下安装步骤：

1. 使用现有VMC SDDC或根据此操作创建新的SDDC "NetApp链接" 或这一点 "VMware链接"。
2. 从内部vCenter环境到VMC SDDC的网络路径必须支持使用vMotion迁移VM。
3. 确保满足所需 "防火墙规则和端口" 允许用于内部vCenter Server与SDDC vCenter之间的vMotion流量。
4. 适用于ONTAP NFS的FSX卷应作为补充数据存储库挂载到VMC SDDC中。 要将NFS数据存储库连接到相应的集群、请按照本节中所述的步骤进行操作 "NetApp链接" 或这一点 "VMware链接"。

高级架构

出于测试目的、用于此验证的内部实验室环境通过站点到站点VPN连接到AWS VPC、从而可以通过外部传输网关在内部连接到AWS和VMware云SDDC。内部部署和VMware云目标SDDC之间的HCX迁移和网络扩展流量通过Internet传输。可以修改此架构以使用Direct Connect专用虚拟接口。

下图展示了高级架构。



解决方案 部署

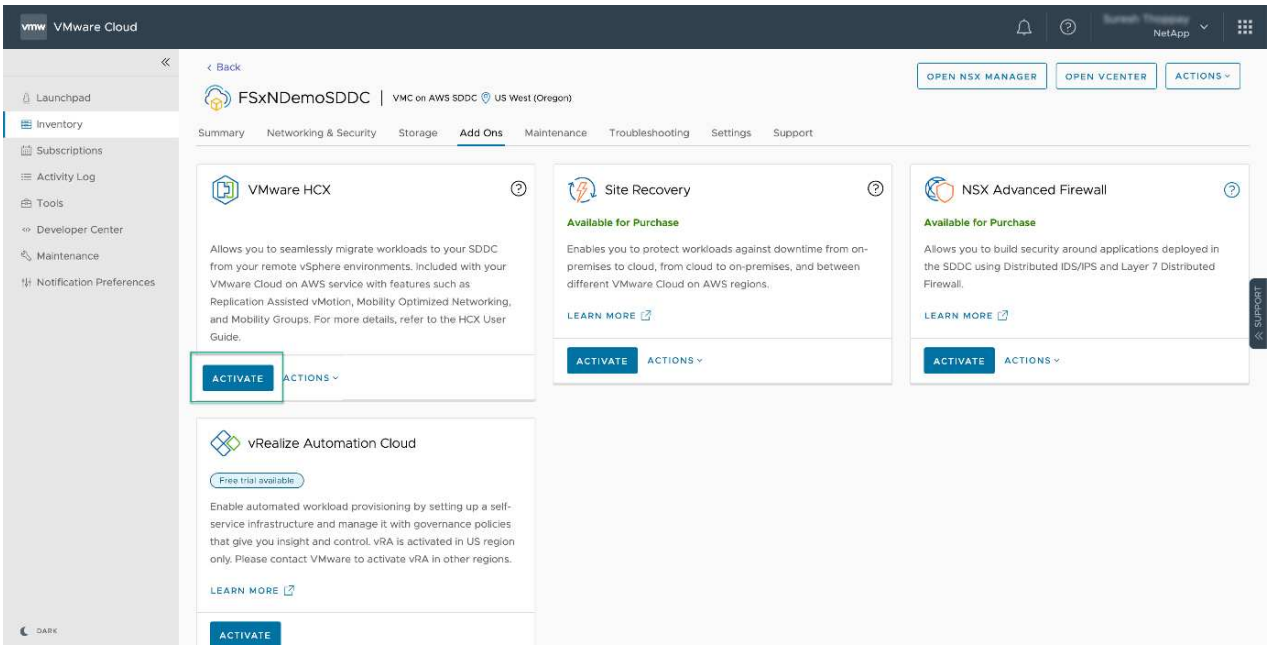
按照一系列步骤完成此解决方案 的部署：

第1步：使用Add-ons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" 并访问清单。
2. 要选择适当的SDDC并访问附加项、请单击SDDC上的查看详细信息、然后选择添加项选项卡。
3. 单击激活VMware HCX。

   完成此步骤最多需要25分钟。

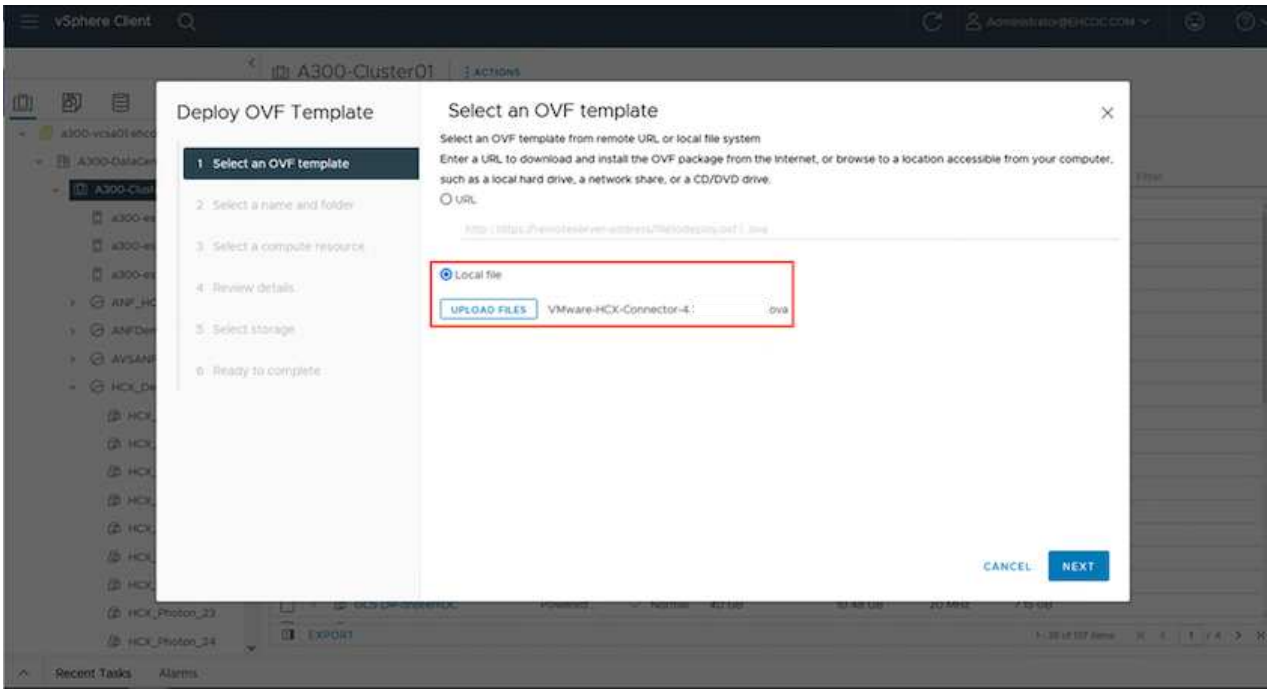


4. 部署完成后、通过确认HCX Manager及其关联插件在vCenter Console中可用来验证部署。
5. 创建适当的管理网关防火墙、以打开访问HCX Cloud Manager所需的端口。HCX Cloud Manager现在已准备就绪、可以执行HCX操作。

第2步：在内部vCenter Server中部署安装程序OVA

要使内部连接器能够与VMC中的HCX Manager进行通信、请确保在内部环境中打开相应的防火墙端口。

1. 在VMC控制台中、导航到HCX信息板、转到管理、然后选择系统更新选项卡。单击"Request a Download Link"以获取HCX Connector OVA映像。
2. 下载HCX Connector后、在内部vCenter Server中部署OVA。右键单击vSphere集群并选择部署OVF模板选项。

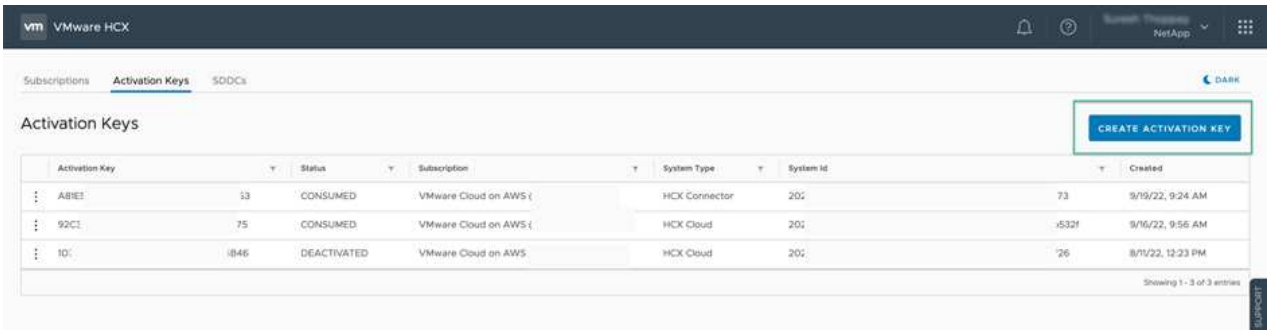


3. 在Deploy OVF Template向导中输入所需信息、单击Next、然后单击Finish以部署VMware HCX Connector OVA。
4. 手动启动虚拟设备。有关分步说明、请转至 "《VMware HCX用户指南》"。

第3步：使用许可证密钥激活HCX Connector

在内部部署VMware HCX Connector OVA并启动设备后、请完成以下步骤以激活HCX Connector。从VMC上的VMware HCX控制台生成许可证密钥、并在设置VMware HCX Connector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"Add Ons"选项卡的VMware HCX磁贴中、单击Open HCX。
2. 从激活密钥选项卡中、单击创建激活密钥。选择System Type作为HCX Connector、然后单击Confirm以生成密钥。复制激活密钥。



> 部署在内部的每个HCX连接器都需要一个单独的密钥。

3. 登录到内部部署的VMware HCX Connector、网址为 "https://hcxconnectorIP:9443" 使用管理员凭据。

> 使用在OVA部署期间定义的密码。

4. 在许可部分中、输入从步骤2复制的激活密钥、然后单击激活。

> 要成功完成激活、内部HCX Connector必须能够访问Internet。

5. 在数据中心位置下、提供在内部安装VMware HCX Manager所需的位置。单击 Continue （继续）。
6. 在System Name下、更新此名称并单击Continue。
7. 选择是、然后继续。
8. 在连接vCenter下、提供vCenter Server的IP地址或完全限定域名(FQDN)以及凭据、然后单击继续。

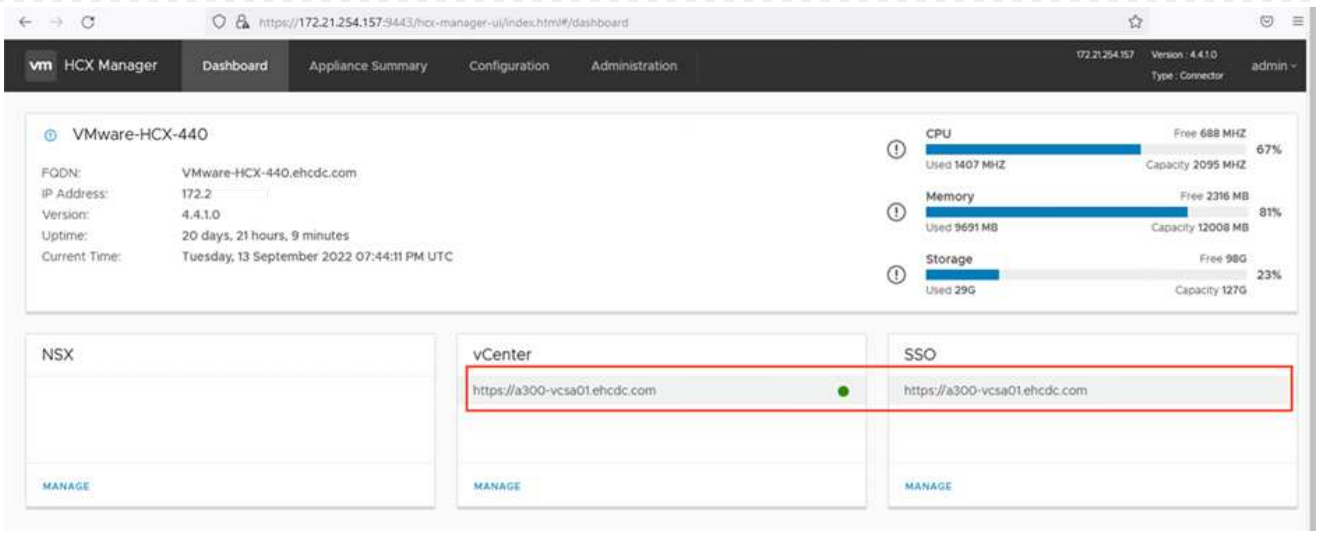
> 使用FQDN以避免稍后出现通信问题。

9. 在配置SSA/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。

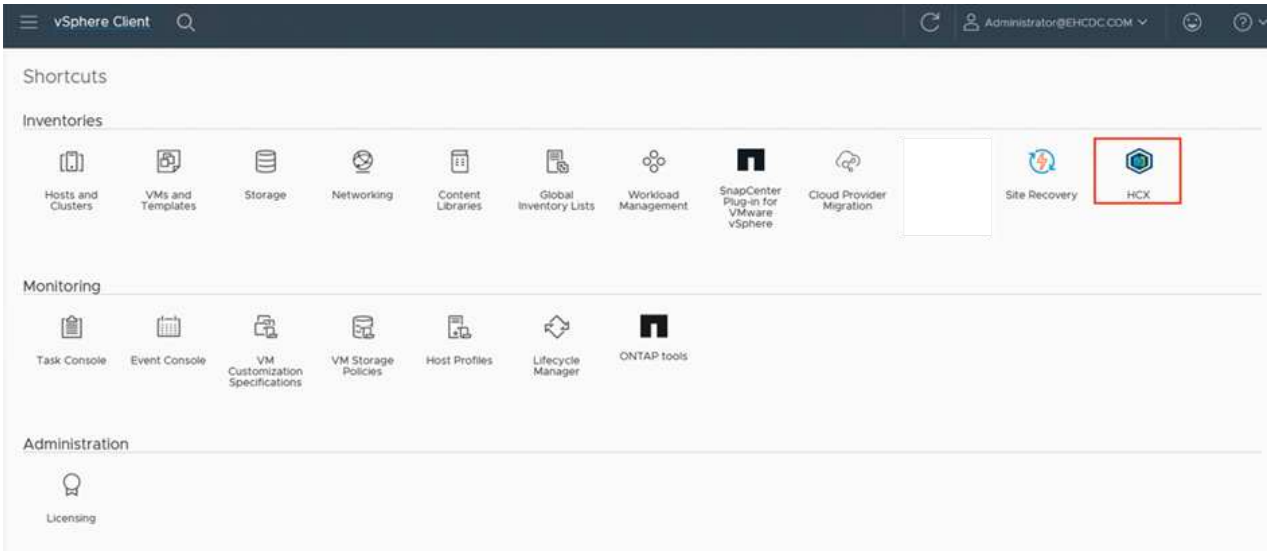
10. 验证输入的信息是否正确、然后单击Restart。
11. 完成后、vCenter Server将显示为绿色。vCenter Server和SSO都必须具有正确的配置参数、这些参数应与上一页相同。

> 此过程大约需要10–20分钟、并且要将此插件添加到vCenter Server中。

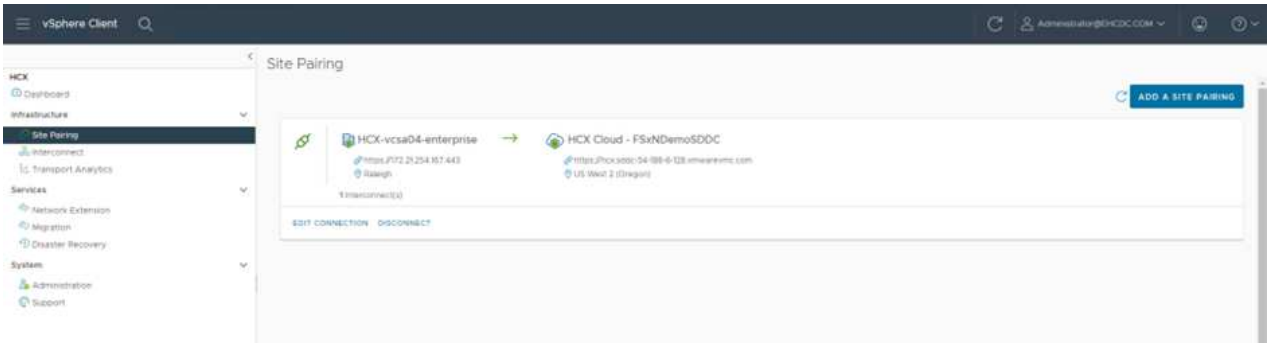

https://172.21.254.157:9443/hcx-manager-ui/index.html#/dashboard
HCX Manager
Dashboard
Appliance Summary
Configuration
Administration
172.21.254.157
Version : 4.4.1.0
Type : Connector
admin
VMware-HCX-440
FQDN: VMware-HCX-440.ehcdc.com
IP Address: 172.2
Version: 4.4.1.0
Uptime: 20 days, 21 hours, 9 minutes
Current Time: Tuesday, 13 September 2022 07:44:11 PM UTC
CPU
Free 688 MHZ
Used 1407 MHZ
Capacity 2095 MHZ
67%
Memory
Free 2316 MB
Used 9691 MB
Capacity 12008 MB
81%
Storage
Free 98G
Used 29G
Capacity 127G
23%
NSX
MANAGE
vCenter
https://a300-vcsa01.ehcdc.com
MANAGE
SSO
https://a300-vcsa01.ehcdc.com
MANAGE

第4步：将内部**VMware HCX Connector**与**VMC HCX Cloud Manager**配对

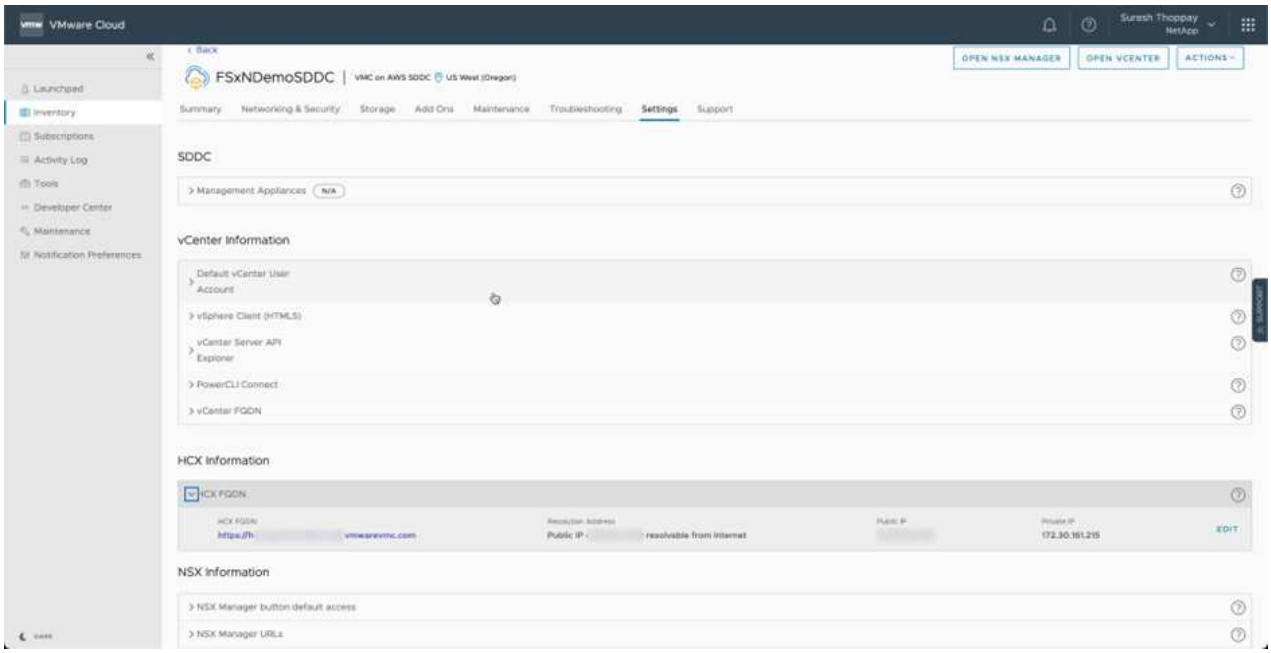
1. 要在内部vCenter Server和VMC SDDC之间创建站点对、请登录到内部vCenter Server并访问HCX vSphere Web Client插件。

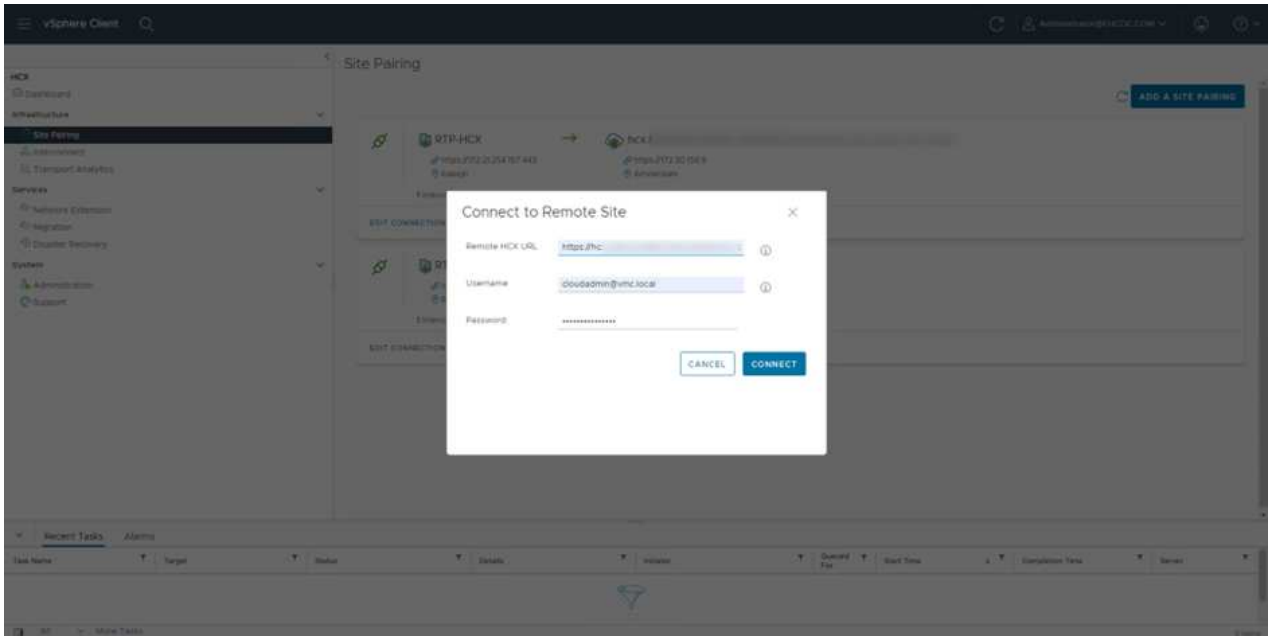


2. 在基础架构下、单击添加站点配对。要对远程站点进行身份验证、请输入VMC HCX Cloud Manager URL或IP地址以及CloudAdmin角色的凭据。



可以从SDDC设置页面检索HCX信息。





3. 要启动站点配对、请单击Connect。

   VMware HCX Connector必须能够通过端口443与HCX Cloud Manager IP进行通信。

4. 创建配对后、新配置的站点配对将显示在HCX信息板上。

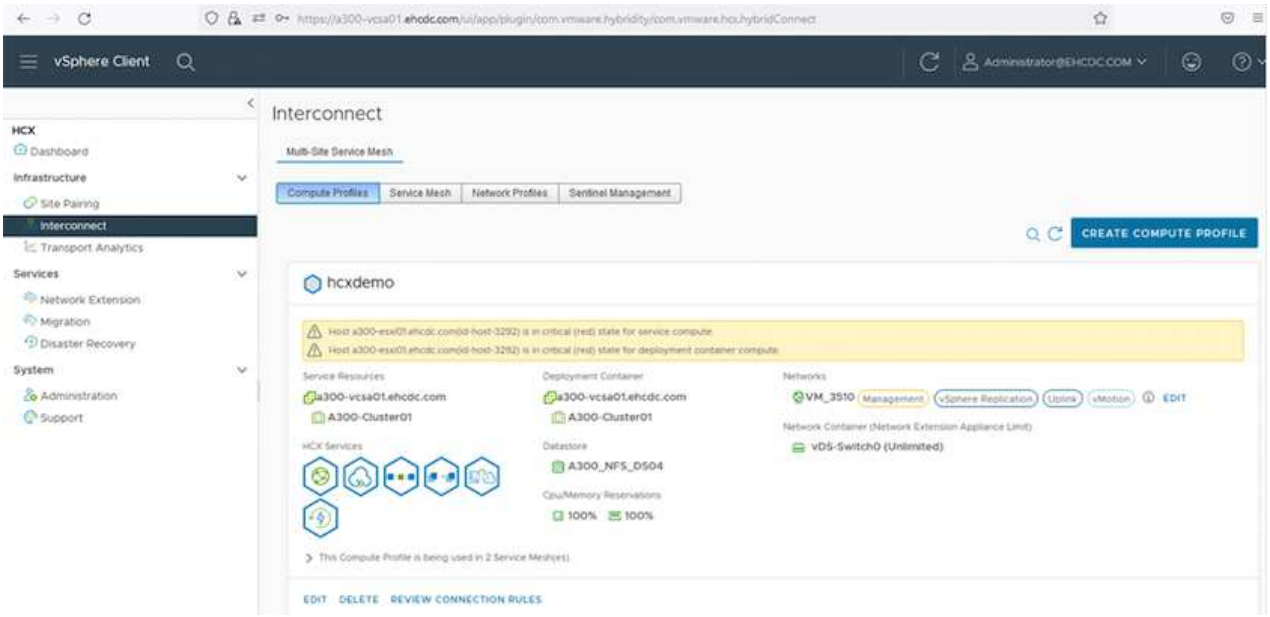
第**5**步：配置网络配置文件、计算配置文件和服务网格

VMware HCX互连(HCX-IX)设备可通过Internet提供安全通道功能、并可通过专用连接到目标站点、从而实现复制和基于vMotion的功能。互连可提供加密、流量工程和SD-WAN。要创建HCI-IX互连设备、请完成以下步骤：

1. 在基础架构下、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。

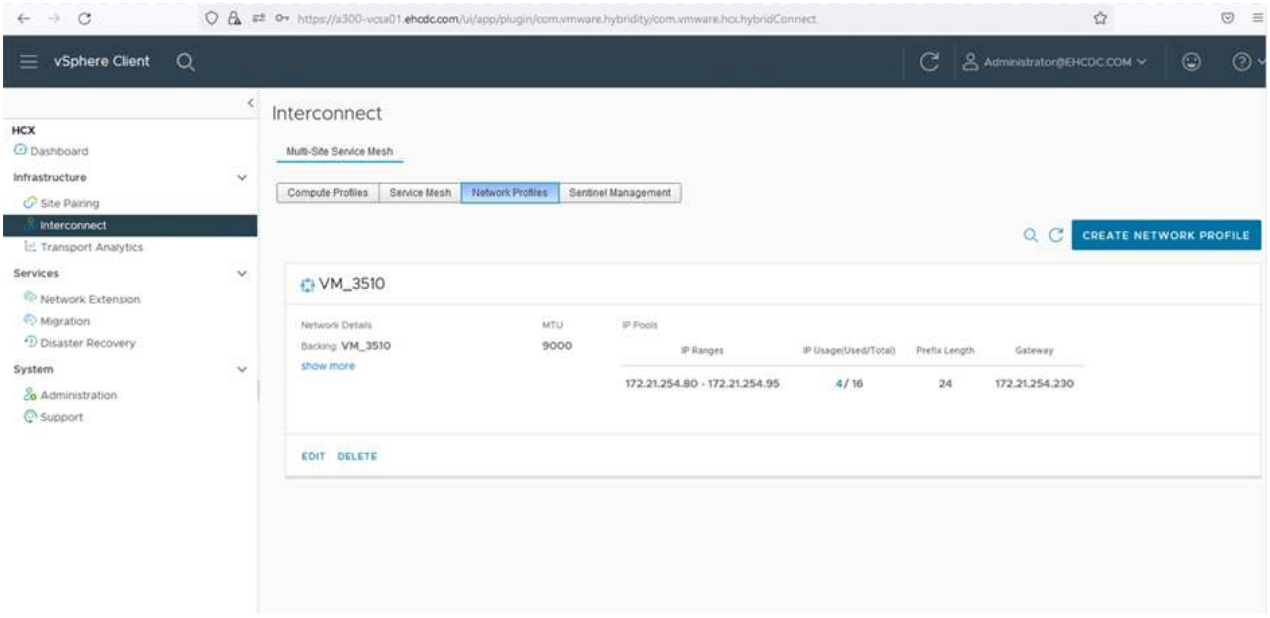
   计算配置文件包含部署互连虚拟设备所需的计算、存储和网络部署参数。它们还会指定HCX服务可访问VMware数据中心的哪个部分。

   有关详细说明、请参见 "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一个IP地址和网络范围、HCX将使用这些地址和网络作为其虚拟设备。

   这需要两个或更多IP地址。这些IP地址将从管理网络分配给虚拟设备。

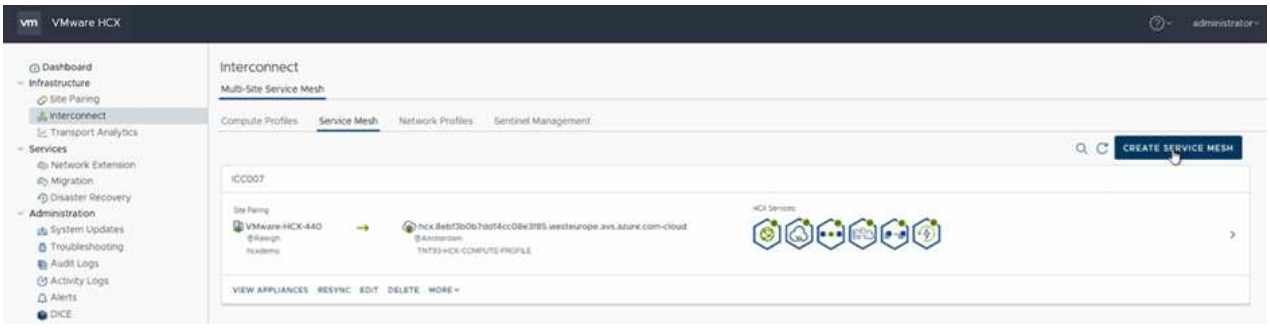


有关详细说明、请参见 "创建网络配置文件"。

如果您要通过Internet连接到SD-WAN、则必须在"网络连接和安全"部分下预留公有 IP。

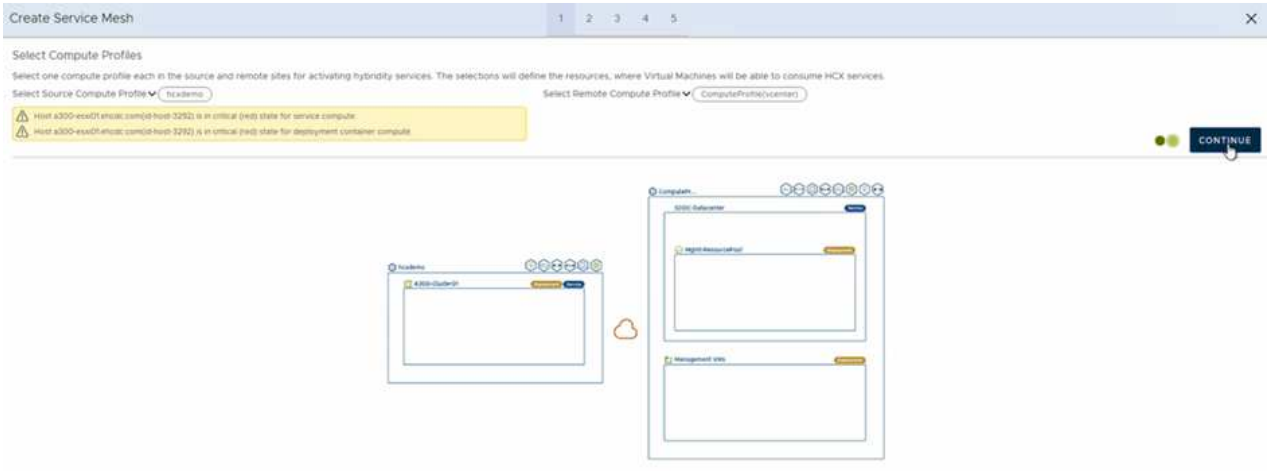
4. 要创建服务网格、请在互连选项中选择服务网格选项卡、然后选择内部和VMC SDDC站点。

   服务网格建立一个本地和远程计算和网络配置文件对。

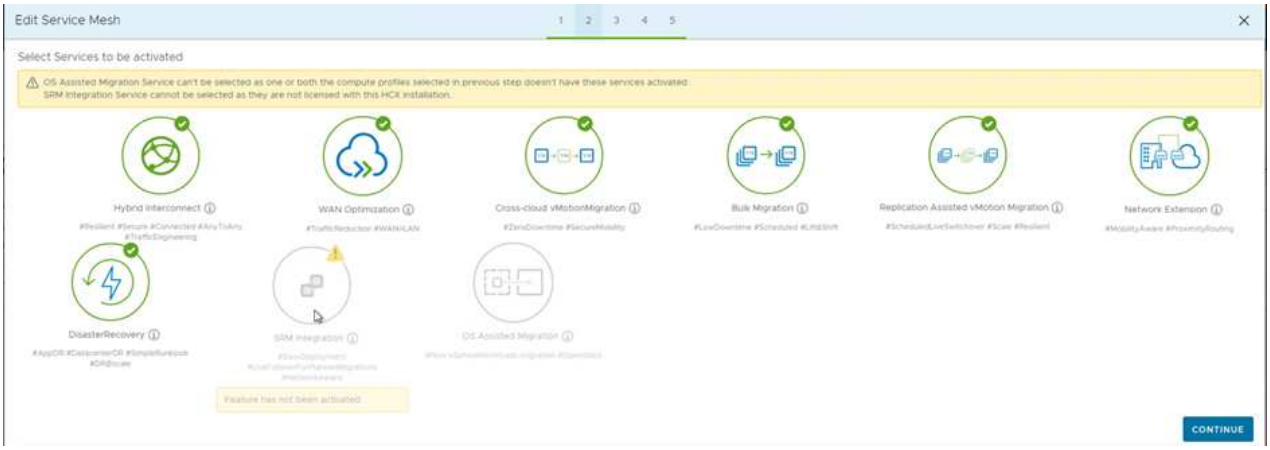


此过程的一部分涉及部署将在源站点和目标站点上自动配置的HCX设备、从而创建安全的传输网络结构。

5. 选择源和远程计算配置文件、然后单击Continue。

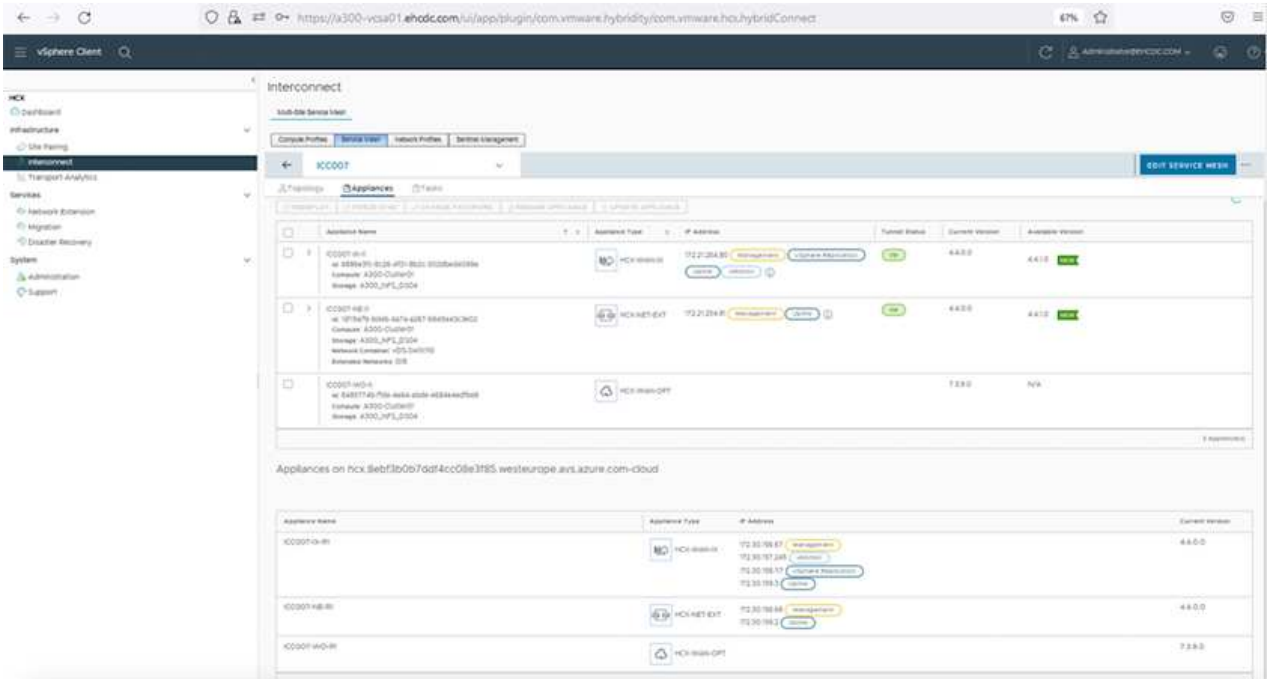


6. 选择要激活的服务、然后单击Continue。



复制辅助vMotion迁移、SRM集成和操作系统辅助迁移需要HCX Enterprise许可证。

7. 为服务网格创建一个名称、然后单击完成以开始创建过程。完成部署大约需要30分钟。配置服务网格后、便创建了迁移工作负载VM所需的虚拟基础架构和网络。


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

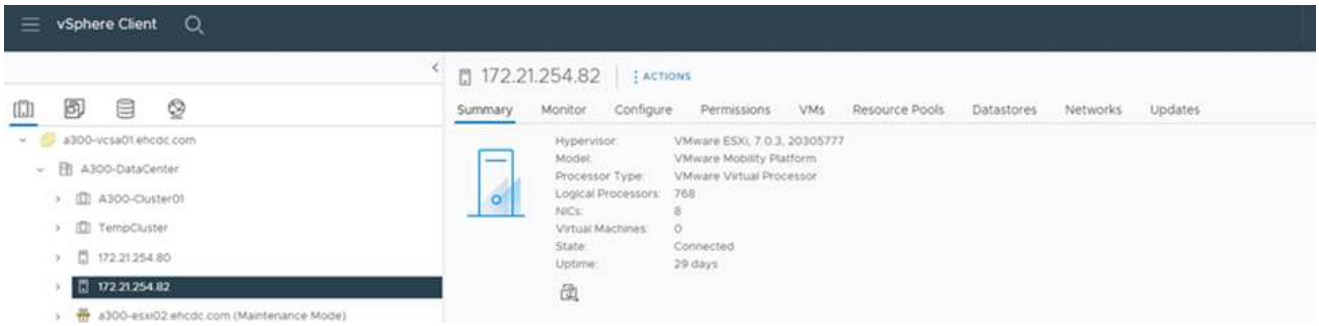
第**6**步：迁移工作负载

HCX可在内部环境和VMC SDDC等两个或更多不同环境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激活的站点或从这些站点迁移到这些站点、例如HCX批量迁移、HCX vMotion、HCX冷迁移、HCX复制辅助vMotion (适用于HCX Enterprise版本)以及HCX操作系统辅助迁移(适用于HCX Enterprise版本)。

要了解有关可用HCX迁移技术的更多信息、请参见 "VMware HCX迁移类型"

HCX-IX设备使用移动代理服务执行vMotion、冷迁移和复制辅助vMotion (RAV)迁移。

HCX-IX设备会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表示托管IX设备的物理虚拟机管理程序上的实际消耗量。

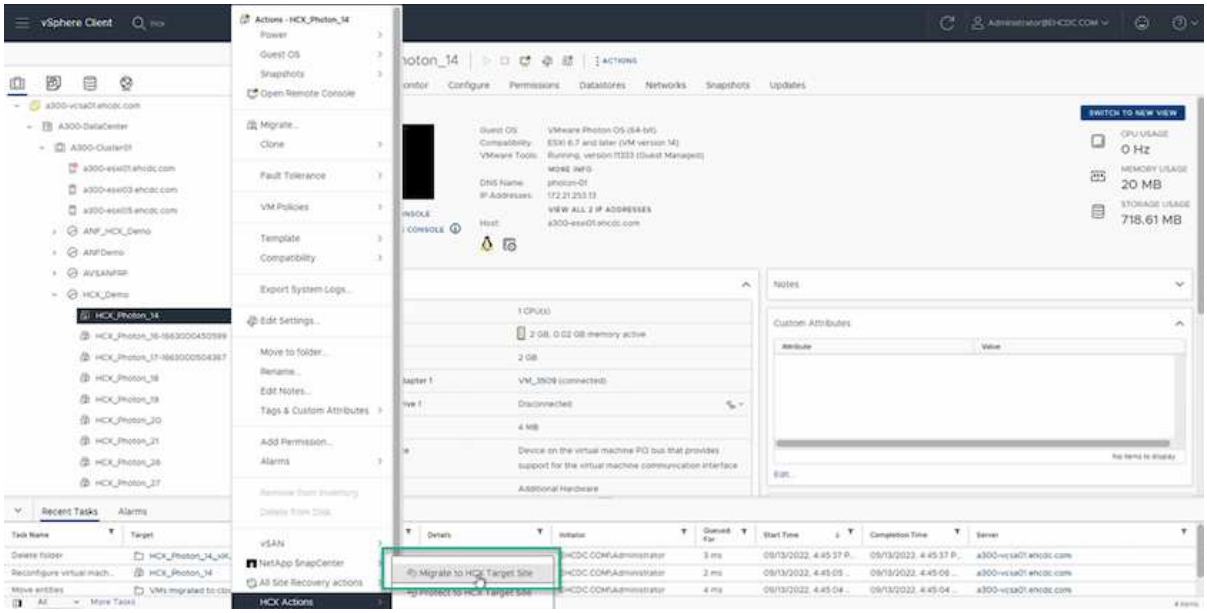


VMware HCX vMotion

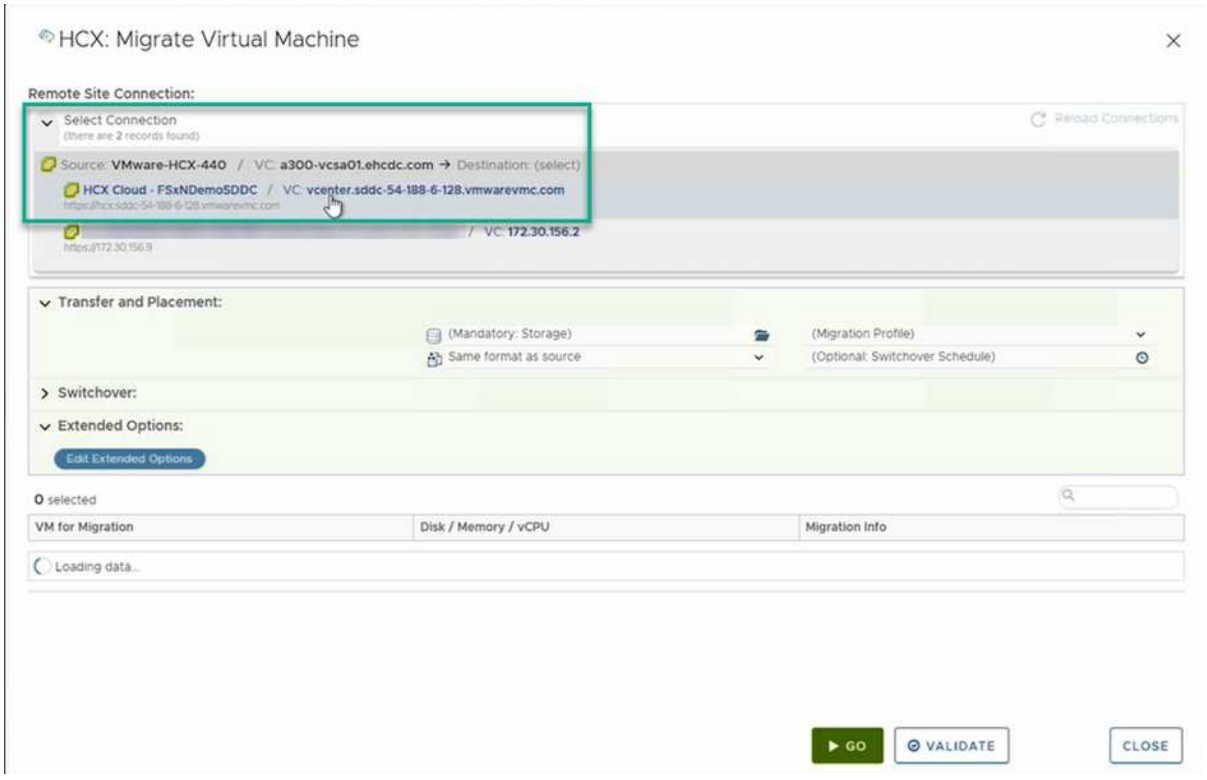
本节介绍HCX vMotion机制。此迁移技术使用VMware vMotion协议将VM迁移到VMC SDDC 。vMotion迁移选项用于一次迁移单个VM的VM状态。此迁移方法期间不会发生服务中断。

应设置网络扩展(对于VM所连接的端口组)、以便在不更改IP地址的情况下迁移VM。

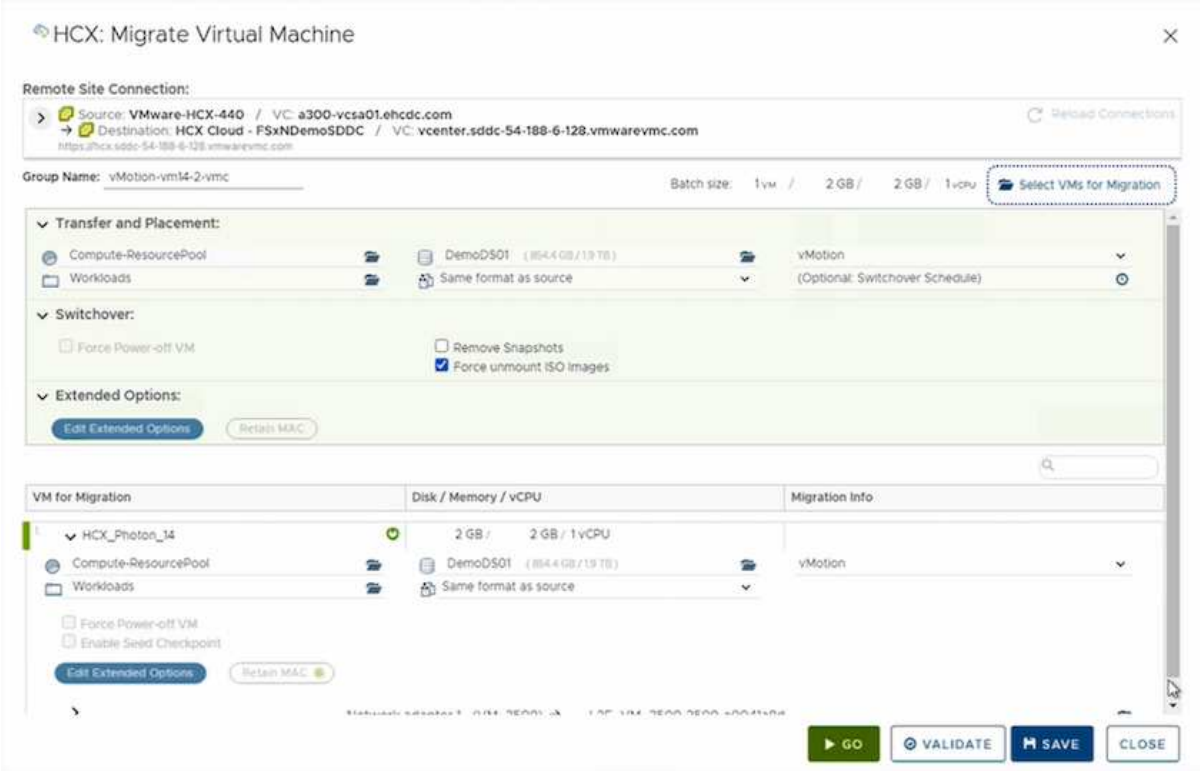
1. 从内部vSphere客户端中、转到清单、右键单击要迁移的虚拟机、然后选择HCX操作>迁移到HCX目标站点。



2. 在迁移虚拟机向导中、选择远程站点连接(目标VMC SDDC)。



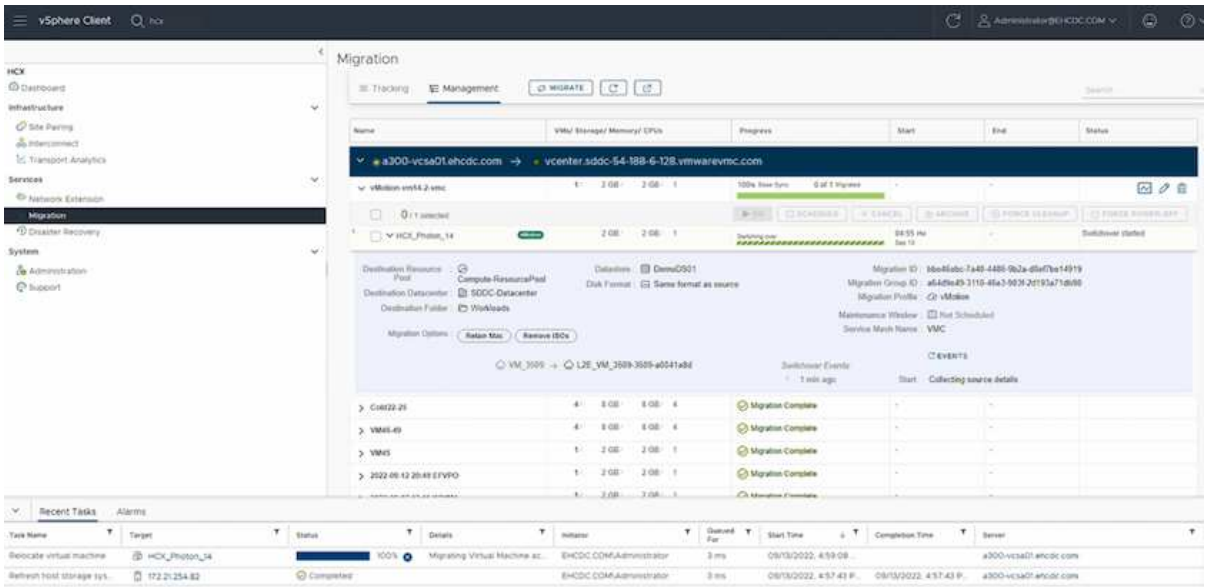
3. 添加组名称、然后在传输和放置下更新必填字段(集群、存储和目标网络)、然后单击验证。



4. 验证检查完成后、单击"Go"启动迁移。

> vMotion传输会捕获VM活动内存、其执行状态、IP地址及其MAC地址。有关HCX vMotion的要求和限制的详细信息、请参见 "了解VMware HCX vMotion和冷迁移"。

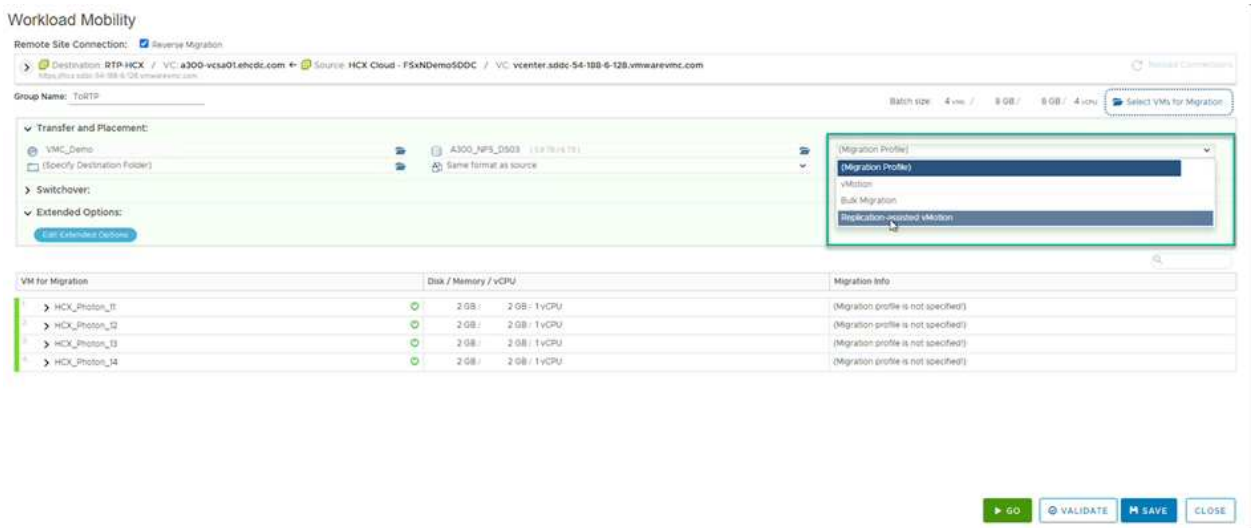
5. 您可以从"HCX">"迁移"信息板监控vMotion的进度和完成情况。



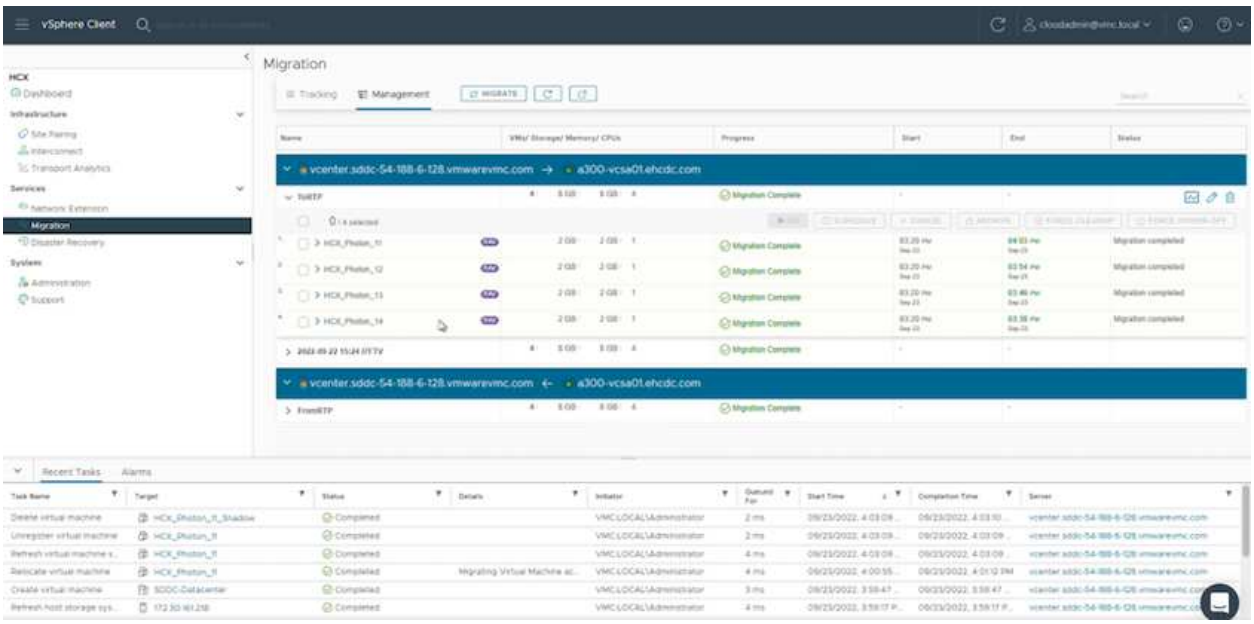
VMware复制辅助vMotion

正如您从VMware文档中可能注意到的那样、VMware HCX Replication Assised 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VM—VM会在切换期间重新启动。HCX vMotion无需停机即可迁移、但它会在一个复制组中按顺序逐个虚拟机执行。RAV会并行复制虚拟机、并使其保持同步、直到切换窗口为止。在切换过程中、它一次迁移一个虚拟机、而不会造成虚拟机停机。

以下屏幕截图将迁移配置文件显示为复制辅助vMotion。



与少数虚拟机的vMotion相比、复制持续时间可能会更长。使用RAV时、请仅同步增量并包含内存内容。以下是迁移状态的屏幕截图—显示了每个虚拟机的迁移开始时间是如何相同的、结束时间是如何不同的。



有关追加信息 的HCX迁移选项以及如何使用HCX将工作负载从内部迁移到AWS上的VMware Cloud的信息、请参见 "《VMware HCX用户指南》"。

VMware HCX vMotion需要100 Mbps或更高的吞吐量功能。

ONTAP 数据存储库的目标VMC FSx必须具有足够的空间来容纳迁移。

结论

无论您是针对全云还是混合云、以及驻留在内部任何类型/供应商存储上的数据、Amazon FSx for NetApp ONTAP 以及HCX均可提供出色的选项来部署和迁移工作负载、同时通过将数据需求无缝迁移到应用程序层来降低TCO。无论使用何种情形、都可以选择VMC以及适用于ONTAP 数据存储库的FSx、以便快速实现云优势、一致的基础架构以及跨内部和多个云的操作、工作负载的双向可移植性以及企业级容量和性能。使用VMware vSphere复制、VMware vMotion甚至是NFCs副本连接存储和迁移VM所使用的过程与步骤相同。

要点总结

本文档的要点包括：

- 现在、您可以使用Amazon FSX ONTAP 作为VMC SDDC的数据存储库。
- 您可以轻松地将数据从任何内部数据中心迁移到使用FSX for ONTAP 数据存储库运行的VMC
- 您可以轻松地扩展和缩减FSX ONTAP 数据存储库、以满足迁移活动期间的容量和性能要求。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请访问以下网站链接：

- VMware Cloud文档

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSX for NetApp ONTAP 文档

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  《VMware HCX用户指南》

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

区域可用性—**VMC**的补充**NFS**数据存储库

AWS/VMC上的补充NFS数据存储库的可用性由Amazon定义。首先、您需要确定VMC和FSxN是否在指定区域中可用。接下来、您需要确定该区域是否支持FSxN补充NFS数据存储库。

- 检查VMC的可用性 "此处"。
- Amazon的定价指南提供了有关FSxN (FSX ONTAP)的可用位置的信息。您可以找到这些信息 "此处"。
- VMC的FSxN补充NFS数据存储库即将推出。

虽然信息仍在发布中、但下图将当前对VMC、FSxN和FSxN的支持标识为一个补充NFS数据存储库。

美洲

* AWS地区*	* VMC可用性*	* FSX ONTAP 可用性*	* NFS数据存储库可用性*
美国东部(北弗吉尼亚)	是的。	是的。	是的。
美国东部（俄亥俄州）	是的。	是的。	是的。
美国西部(北加利福尼亚)	是的。	否	否
US West （俄勒冈州）	是的。	是的。	是的。
GovCloud (美国西部)	是的。	是的。	是的。
加拿大（中部）	是的。	是的。	是的。
南美(圣保罗)	是的。	是的。	是的。

最后更新日期：2022年6月2日。

欧洲、中东和非洲

* AWS地区*	* VMC可用性*	* FSX ONTAP 可用性*	* NFS数据存储库可用性*
欧洲(爱尔兰)	是的。	是的。	是的。
欧洲(伦敦)	是的。	是的。	是的。
欧洲(法兰克福)	是的。	是的。	是的。
欧洲(巴黎)	是的。	是的。	是的。
欧洲(米兰)	是的。	是的。	是的。
欧洲（斯德哥尔摩）	是的。	是的。	是的。

最后更新日期：2022年6月2日。

亚太地区

* AWS地区*	* VMC可用性*	* FSX ONTAP 可用性*	* NFS数据存储库可用性*
Asia Pacific (Sydney)	是的。	是的。	是的。
亚太地区(东京)	是的。	是的。	是的。
亚太地区(日本、日本)	是的。	否	否
亚太地区(新加坡)	是的。	是的。	是的。
亚太地区(首尔)	是的。	是的。	是的。
亚太地区(孟买)	是的。	是的。	是的。
亚太地区(雅加达)	否	否	否
亚太地区(香港)	是的。	是的。	是的。

最后更新日期：2022年9月28日。

适用于 **Azure AVS** 的 **NetApp** 功能

详细了解NetApp为Azure VMware解决方案 (AVS)提供的功能—从作为子系统连接存储设备或补充NFS数据存储库的NetApp到迁移工作流、扩展/突发到云、备份/还原和灾难恢复。

从以下选项中选择，跳至所需内容部分：

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

在 **Azure** 中配置 **AVS**

与内部部署一样，规划基于云的虚拟化环境对于成功创建 VM 和迁移生产就绪环境至关重要。

本节介绍如何设置和管理 Azure VMware 解决方案并将其与连接 NetApp 存储的可用选项结合使用。

来宾存储是将Cloud Volumes ONTAP 连接到Azure VMware解决方案 的唯一受支持方法。

设置过程可细分为以下步骤：

- 注册资源提供商并创建私有云
- 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的配置步骤"。

适用于 **AVS** 的 **NetApp** 存储选项

NetApp存储可以通过多种方式在Azure AVS中用作guess connected或作为补充NFS数据存储库。

请访问 "支持的 NetApp 存储选项" 有关详细信息 …

Azure 支持以下配置中的 NetApp 存储：

- Azure NetApp Files （ ANF ）作为子系统连接的存储
- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- Azure NetApp Files (ANF)作为补充NFS数据存储库

查看详细信息 "AVS的子系统连接存储选项"。查看详细信息 "AVS的补充NFS数据存储库选项"。

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部署在 Azure AVS 中。为VMware定义的每个云区域定义了SE案例：

- 保护(包括灾难恢复和备份/还原)

- 扩展
- 迁移

"浏览适用于 Azure AVS 的 NetApp 解决方案"

保护**AzAzure / AVS**上的工作负载

使用**ANF**和**Jetstream**进行灾难恢复

将灾难恢复到云是一种弹性且经济高效的方式、可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、可以将内部VMware工作负载复制到Azure Blob存储并进行恢复、从而最大限度地减少或接近无数据丢失、并实现近乎零的RTO。

可以使用Jetstream DR无缝恢复从内部复制到AVS、特别是复制到Azure NetApp Files 的工作负载。它通过在灾难恢复站点使用最少的资源和经济高效的云存储来实现经济高效的灾难恢复。Jetstream DR可通过Azure Blob Storage自动恢复到ANF数据存储库。Jetstream灾难恢复可根据网络映射将独立的VM或相关VM组恢复到恢复站点基础架构中、并提供时间点恢复以实现勒索软件保护。

本文档介绍了Jetstream灾难恢复的操作原理及其主要组件。

1. 在内部数据中心安装Jetstream DR软件。
   a. 从Azure Marketplace (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筛选器软件包配置集群(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(来自现有数据存储库或共享iSCSI存储的VMDK)。
   e. 创建受保护域(相关VM的组)并分配DRBA和Azure Blob Storage/ANF。
   f. 启动保护。
2. 在Azure VMware解决方案 私有云中安装Jetstream DR软件。
   a. 使用Run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数据存储库创建复制日志卷。
   e. 导入受保护域并配置RocVA (恢复VA)、以便使用ANF数据存储库放置VM。
   f. 选择相应的故障转移选项、并为接近零的RTO域或VM启动持续重新融合。
3. 在发生灾难事件期间、触发故障转移到指定AVS灾难恢复站点中的Azure NetApp Files 数据存储库。
4. 在受保护站点恢复后调用故障恢复到受保护站点。在启动之前、请确保满足此中所述的前提条件 "链接。" 此外、还可以运行Jetstream Software提供的带宽测试工具(BWT)来评估Azure Blob存储在与Jetstream DR软件结合使用时的潜在性能及其复制带宽。在具备包括连接在内的前提条件后、从设置并订阅Jetstream DR for AVS "Azure Marketplace"。下载软件包后、继续执行上述安装过程。

在为大量VM (例如100多个)规划和启动保护时、请使用Jetstream DR Automation Toolkit中的容量规划工具(CPT)。提供要保护的VM列表及其RTO和恢复组首选项、然后运行CPT。

CPT可执行以下功能：

- 根据虚拟机的RTO将其组合到保护域中。
- 定义最佳的DRBA数及其资源。
- 估计所需的复制带宽。
- 确定复制日志卷的特征(容量、带宽等)。
- 估计所需的对象存储容量等。

规定的域数量和内容取决于各种VM特征、例如平均IOPS、总容量、优先级(用于定义故障转移顺序)、RTO等。

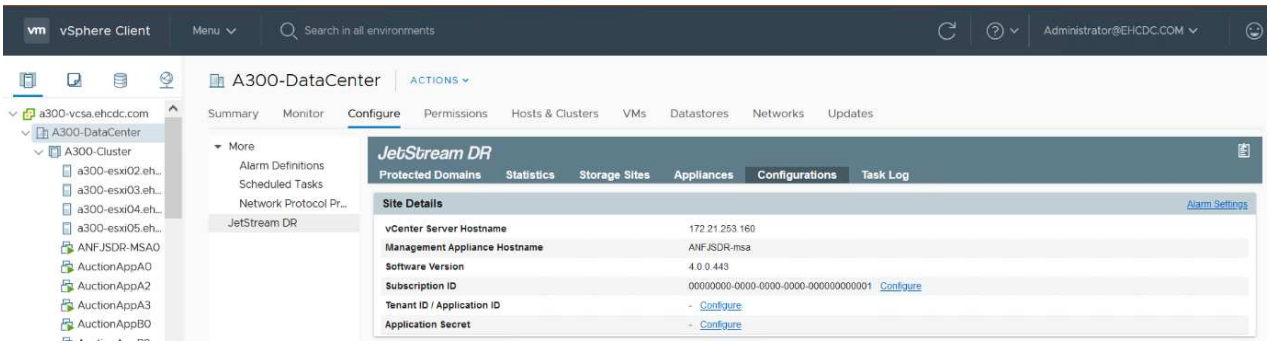
在内部数据中心中安装**Jetstream DR**

Jetstream灾难恢复软件由三个主要组件组成：Jetstream灾难恢复管理服务器虚拟设备(Virtual Appliance、MSA)、灾难恢复虚拟设备(DR Virtual Appliance、DRVA)和主机组件(I/O筛选器软件包)。MSA用于在计算集群

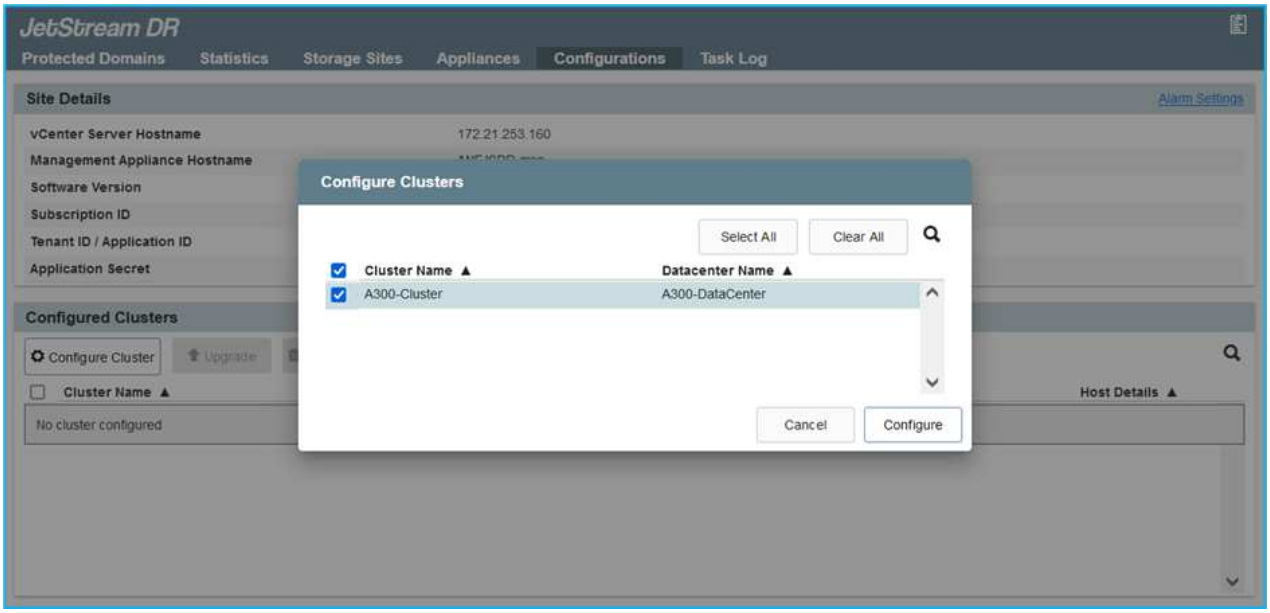
上安装和配置主机组件、然后管理Jetstream DR软件。以下列表提供了安装过程的高级问题描述：

如何为内部环境安装**Jetstream DR**

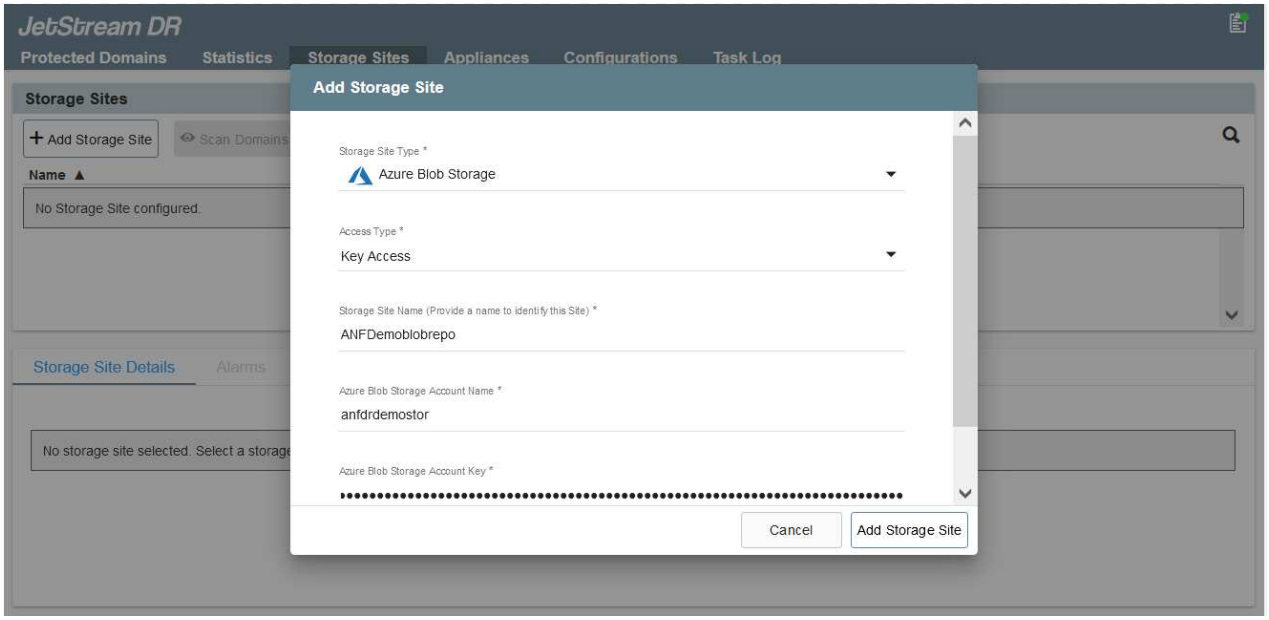
1. 检查前提条件。
2. 运行容量规划工具以获取资源和配置建议(可选、但建议用于概念验证试用)。
3. 将Jetstream DR MSA部署到指定集群中的vSphere主机。
4. 在浏览器中使用其DNS名称启动MSA。
5. 向MSA注册vCenter Server。要执行安装、请完成以下详细步骤：
6. 部署Jetstream DR MSA并注册vCenter Server后、请使用vSphere Web Client访问Jetstream DR插件。可通过导航到"数据中心">"配置">"Jetstream DR"来完成此操作。



7. 从Jetstream灾难恢复界面中、选择相应的集群。



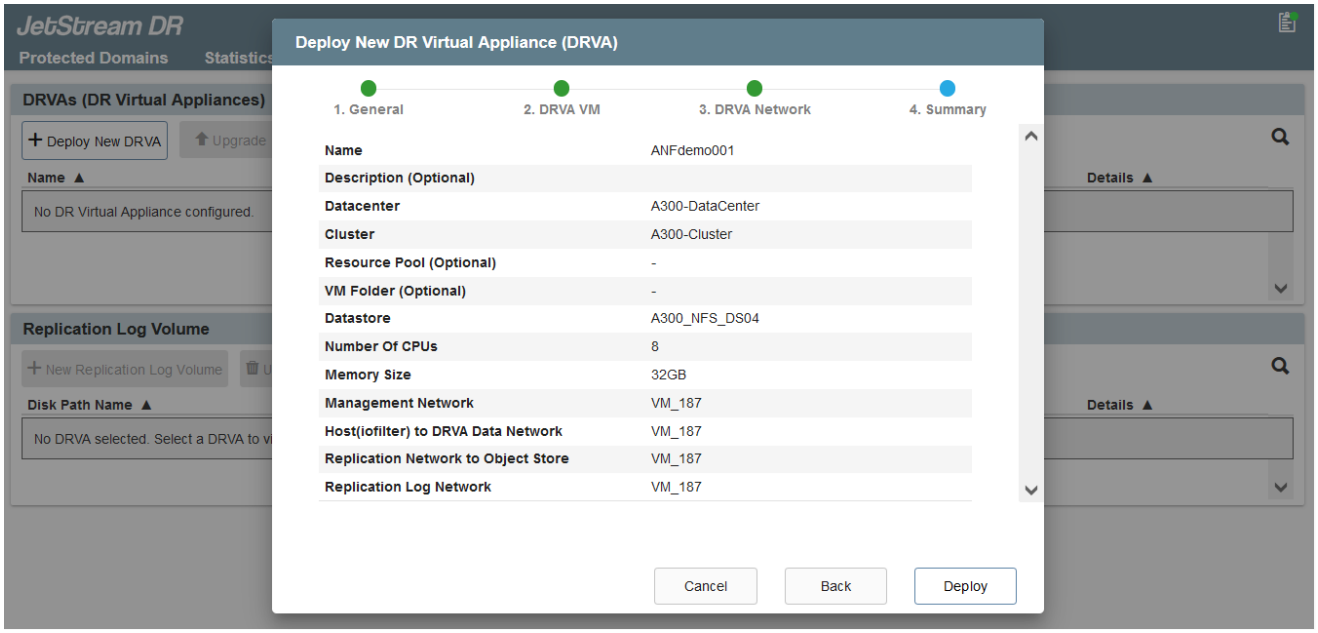
8. 使用I/O筛选器软件包配置集群。



9. 添加位于恢复站点的Azure Blob Storage。
10. 从设备选项卡部署灾难恢复虚拟设备(DR Virtual Appliance、DRVA)。

> DvA可以由CPT自动创建、但对于POC试用、我们建议手动配置和运行灾难恢复周期(启动保护>故障转移>故障恢复)。

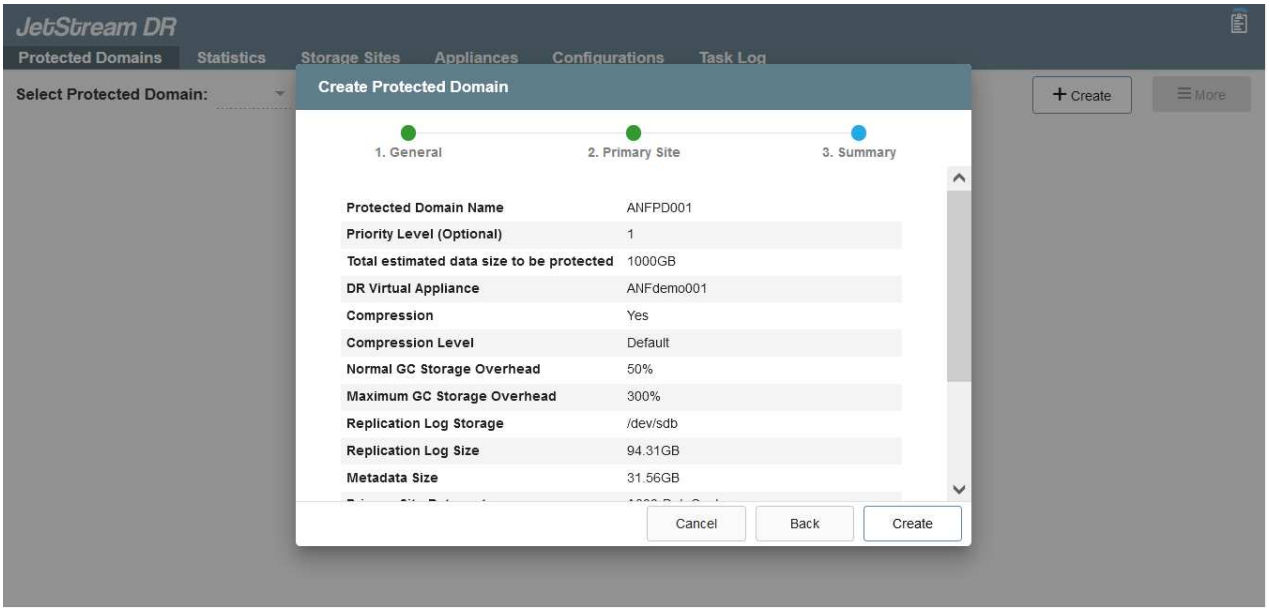
Jetstream DRVA是一个虚拟设备、可促进数据复制过程中的关键功能。受保护集群必须至少包含一个DRVA、通常每个主机配置一个DRVA。每个DRVA都可以管理多个受保护域。



在此示例中、为80个虚拟机创建了四个DRVA。

1. 使用VMDK从可用的数据存储库或独立的共享iSCSI存储池为每个DRVA创建复制日志卷。
2. 在受保护域选项卡中、使用Azure Blob Storage站点、DRVA实例和复制日志的相关信息创建所需数量的受保护域。受保护域定义集群中一个或一组一起受保护的特定虚拟机、并为故障转移/故障恢复操作

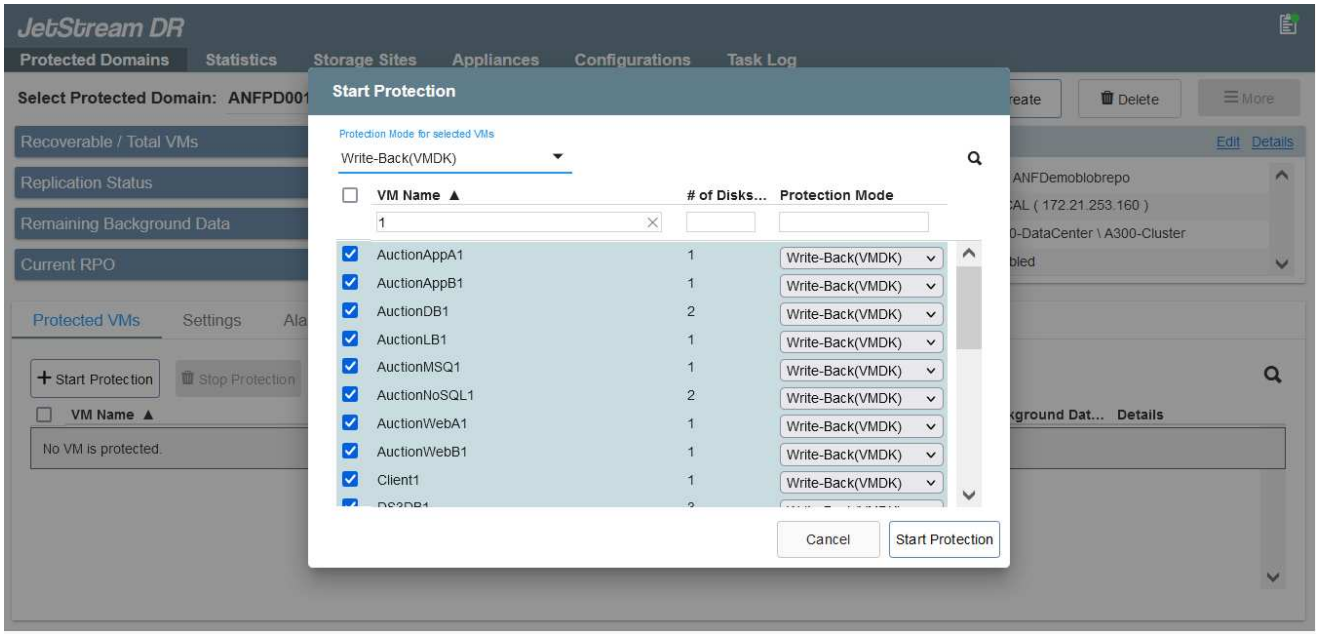
分配优先级顺序。



3. 选择要保护的VM并启动受保护域的VM保护。此时将开始向指定的Blob Store复制数据。

验证受保护域中的所有VM是否使用相同的保护模式。

回写(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。

可以对故障转移运行手册进行配置、以便对VM (称为恢复组)进行分组、设置启动顺序以及修改CPU/内存设置和IP配置。

使用**Run**命令在**Azure VMware**解决方案 私有云中安装**Jetstream DR for AVS**

恢复站点(AVS)的一个最佳实践是、提前创建一个三节点的试用集群。这样可以对恢复站点基础架构进行预配置、其中包括以下各项：

- 目标网络分段、防火墙、DHCP和DNS等服务等。
- 安装适用于AVS的Jetstream DR
- 将ANF卷配置为数据存储库、并且moreJetStream DR支持任务关键型域的RTO模式接近零。对于这些域、应预安装目标存储。在这种情况下、建议使用ANF存储类型。

应在AVS集群上配置网络配置、包括创建网段、以满足内部部署要求。

根据SLA和RTO要求、可以使用持续故障转移或常规(标准)故障转移模式。对于接近零的RTO、应在恢复站点启动持续再融合。

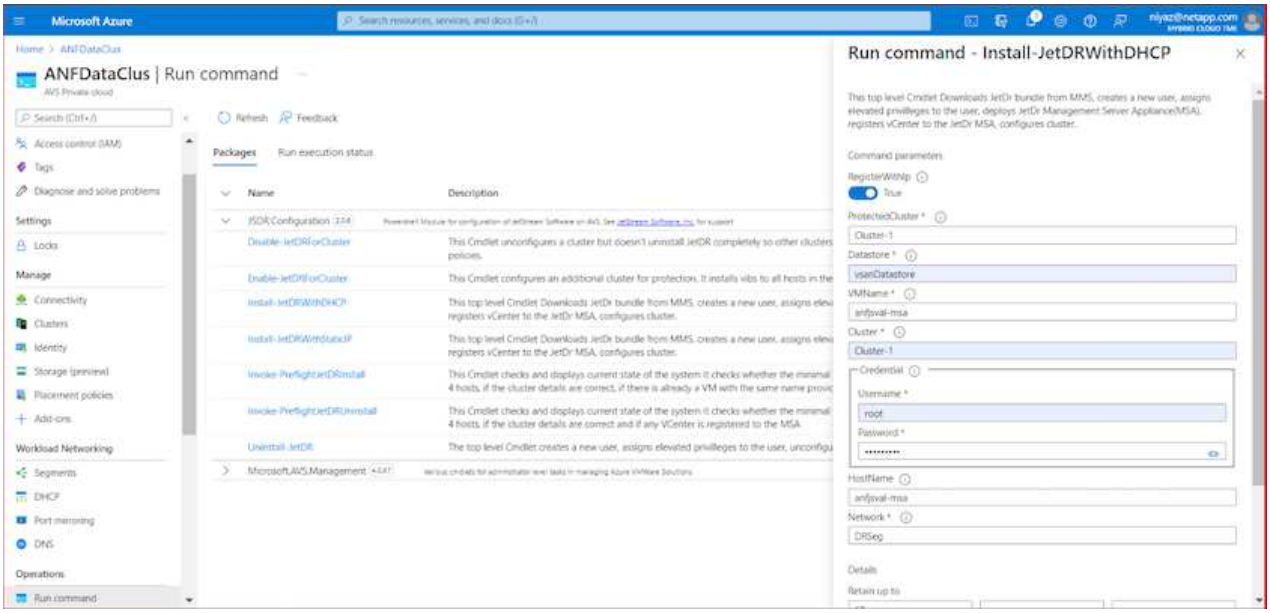
如何在私有云中安装**Jetstream DR for AVS**

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：

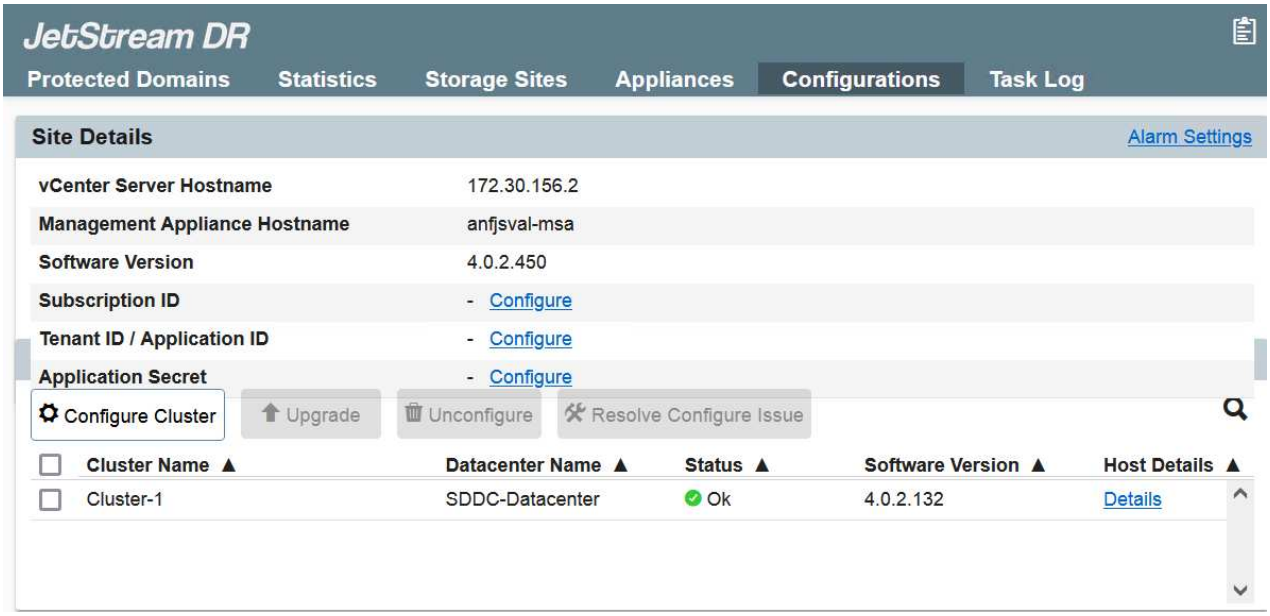
1. 从Azure门户中、转到Azure VMware解决方案 、选择私有云、然后选择运行命令>软件包> JSDR.Configuration。

> Azure VMware解决方案 中的默认CloudAdmin用户没有足够的权限来安装适用于AVS的Jetstream DR。Azure VMware解决方案 通过调用适用于Jetstream DR的Azure VMware解决方案 Run命令、可以简化并自动安装Jetstream DR。

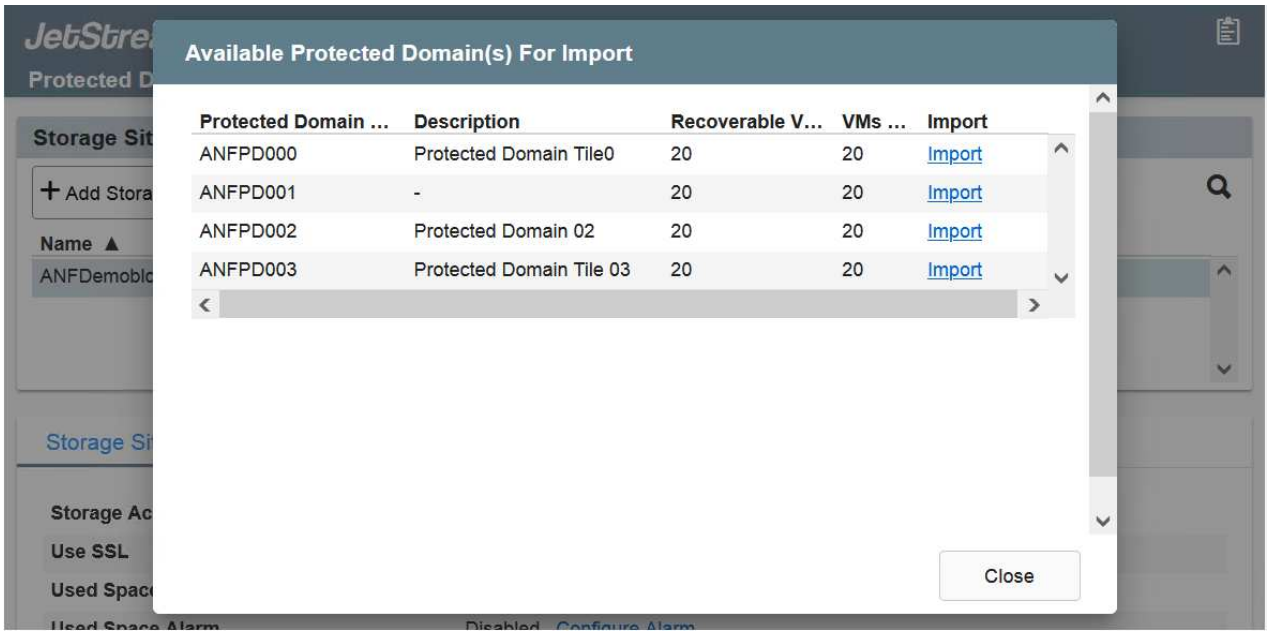
以下屏幕截图显示了使用基于DHCP的IP地址进行安装的情况。



2. 完成适用于AVS的Jetstream DR安装后、刷新浏览器。要访问Jetstream DR UI、请转到SDDC Datacenter >配置> Jetstream DR。



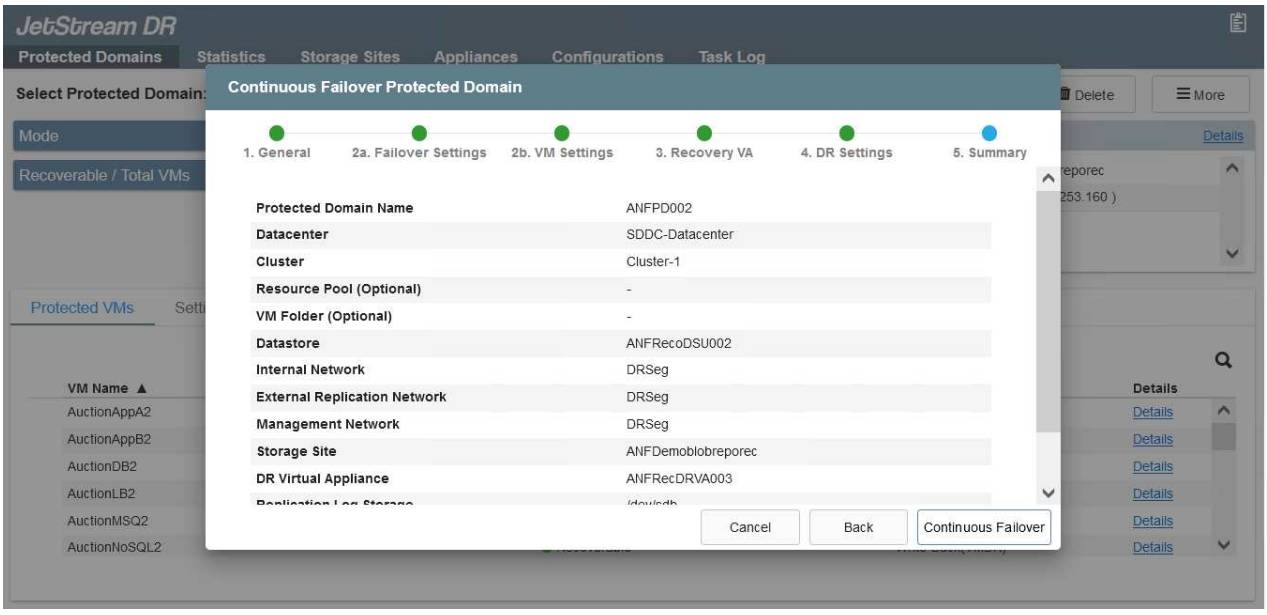
3. 从Jetstream DR界面中、添加用于将内部集群作为存储站点进行保护的Azure Blob Storage帐户、然后运行扫描域选项。



4. 导入受保护域后、部署DRVA设备。在此示例中、可以使用Jetstream DR UI从恢复站点手动启动持续再水化。

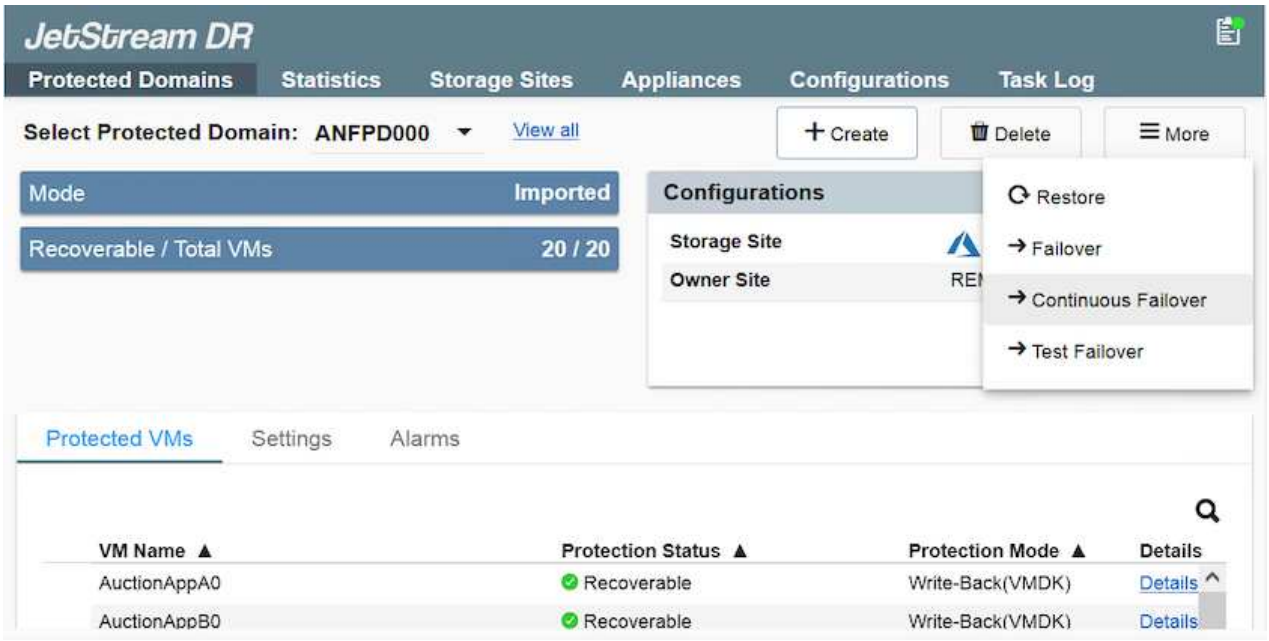
> 也可以使用CPT创建的计划自动执行这些步骤。

5. 使用可用的vSAN或ANF数据存储库创建复制日志卷。
6. 导入受保护域并配置恢复VA以使用ANF数据存储库放置VM。



> 确保选定网段上已启用DHCP、并且有足够的可用IP。在恢复域时、系统会临时使用动态IP。每个正在恢复的VM (包括持续重新融合)都需要一个单独的动态IP。恢复完成后、此IP将被释放并可重复使用。

7. 选择相应的故障转移选项(持续故障转移或故障转移)。在此示例中、选择了持续再融合(持续故障转移)。



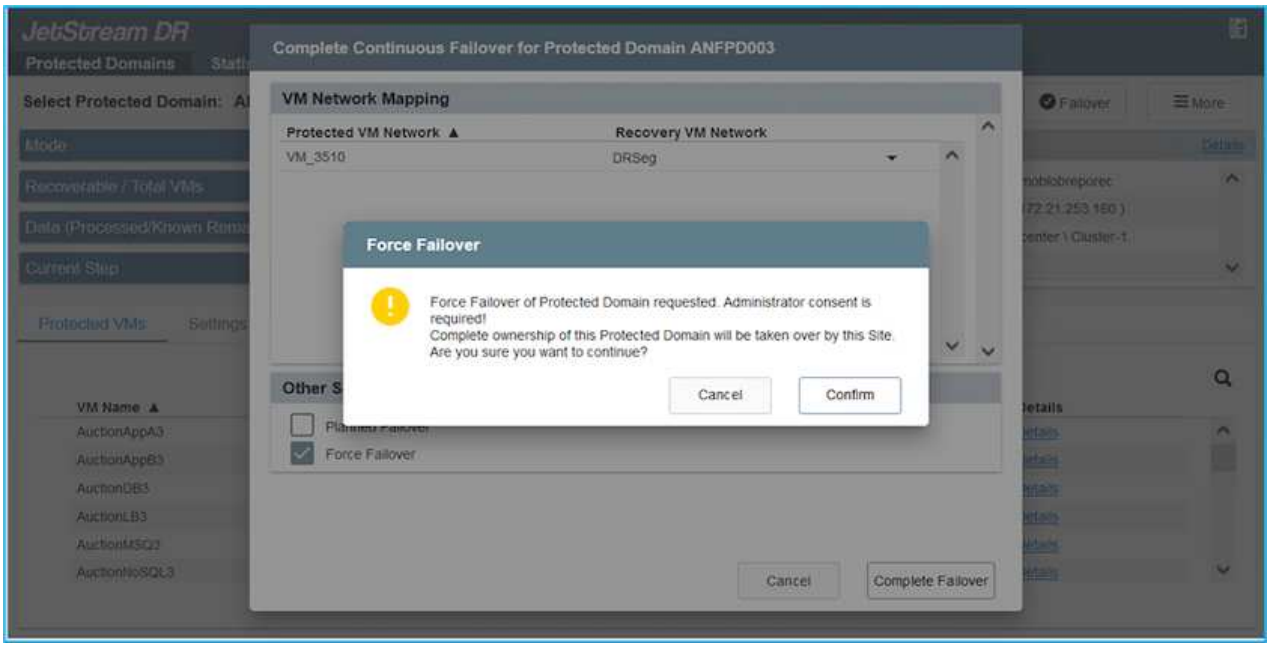
正在执行故障转移/故障恢复

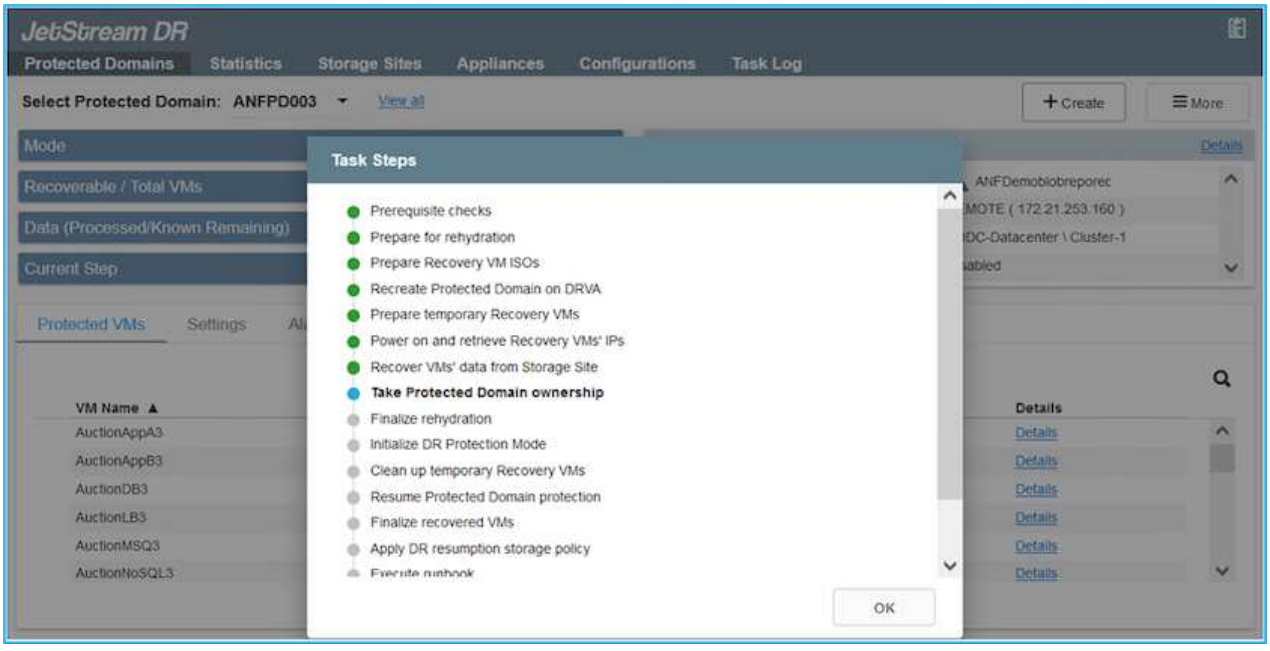
如何执行故障转移/故障恢复

1. 在内部环境的受保护集群发生灾难(部分或完全故障)后、触发故障转移。

   CPT可用于执行故障转移计划、以便将虚拟机从Azure Blob Storage恢复到AVS集群恢复站点。

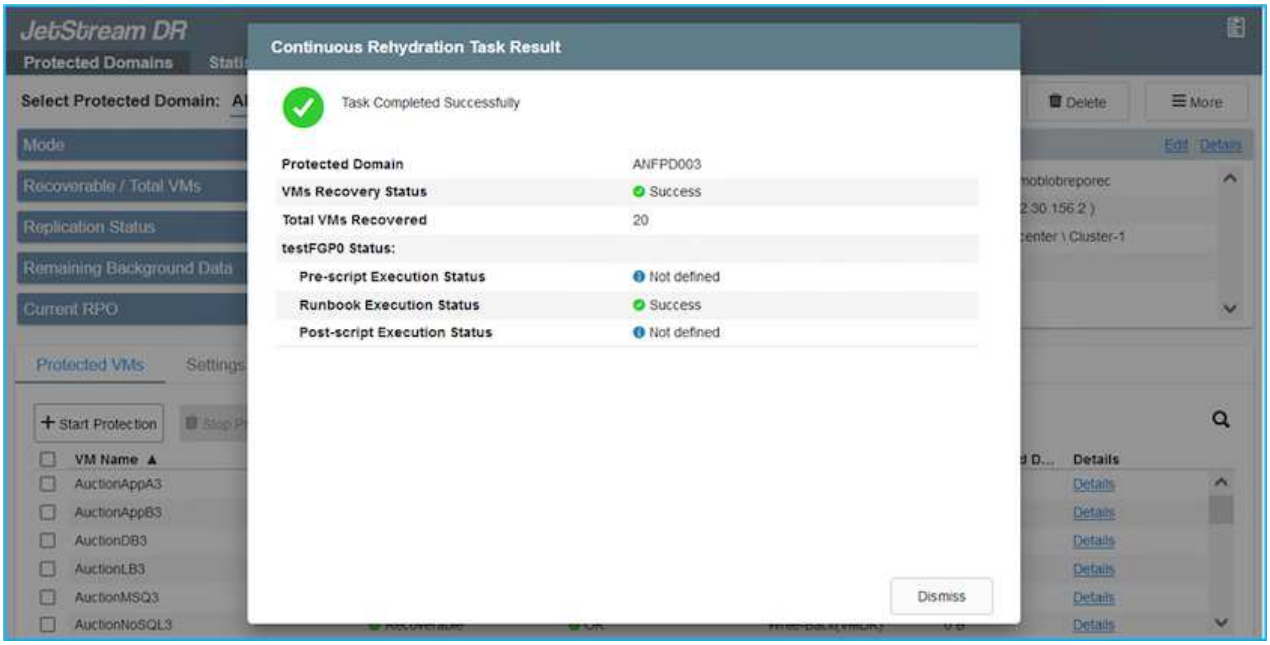
   在AVS中启动受保护的VM后进行故障转移(针对持续或标准再融合)、保护将自动恢复、Jetstream DR将继续将其数据复制到Azure Blob Storage中的相应/原始容器中。





   任务栏显示故障转移活动的进度。

2. 任务完成后、访问已恢复的VM、业务将继续正常进行。

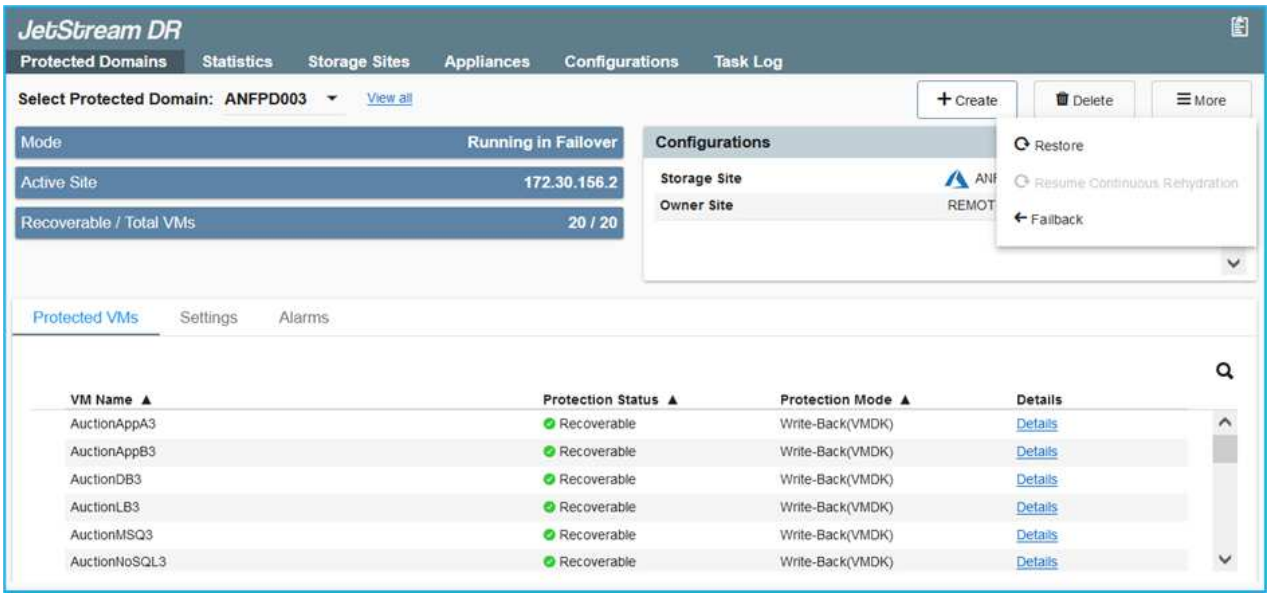


主站点启动并重新运行后、可以执行故障恢复。VM保护将恢复、应检查数据一致性。

3. 还原内部环境。根据灾难意外事件的类型、可能需要还原和/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：可使用Automation Toolkit中提供的`recovery_utility_prepare_failback`脚本帮助清理原始受保护站点中任何废弃的VM、域信息等。

4. 访问已还原的内部环境、转到Jetstream DR UI、然后选择相应的受保护域。受保护站点准备好进行故障恢复后、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VM及其数据从对象存储返回到原始VMware环境的操作。

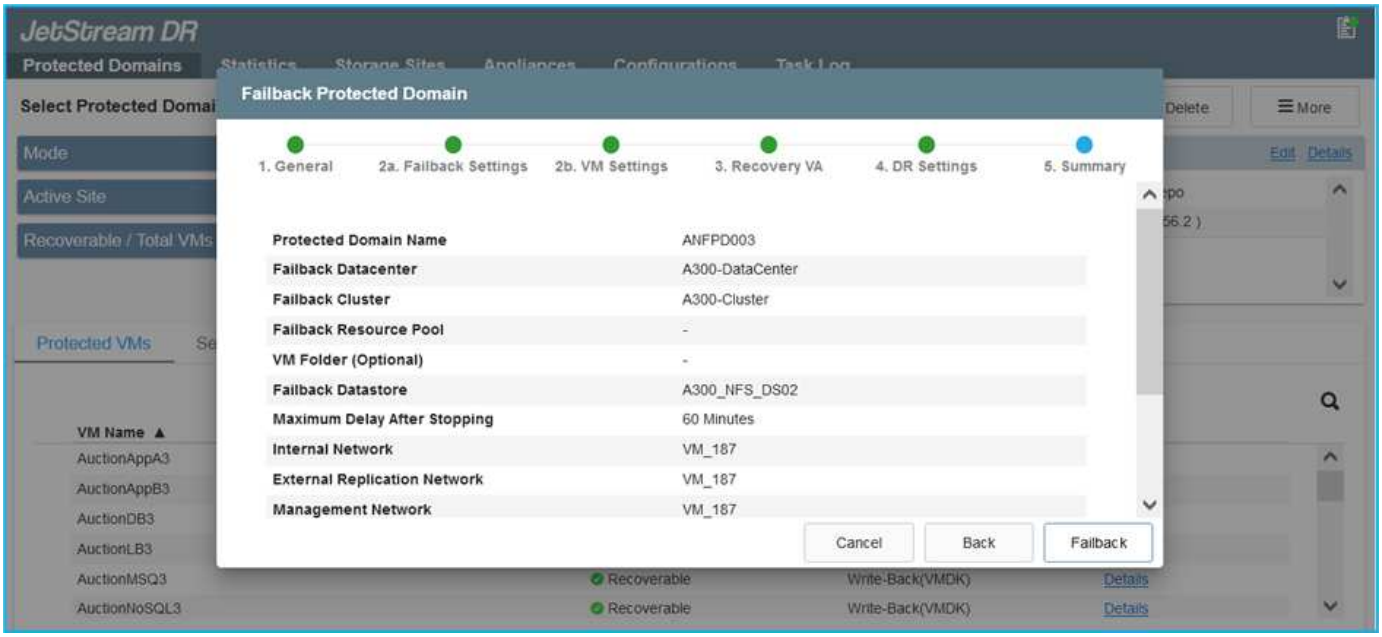
指定在恢复站点暂停VM并在受保护站点重新启动后的最大延迟。这包括在停止故障转移VM后完成复制、清理恢复站点的时间以及在受保护站点中重新创建VM的时间。NetApp建议值为10分钟。

完成故障恢复过程、然后确认虚拟机保护和数据一致性的恢复。

Ransomware恢复

从勒索软件中恢复可能是一项艰巨的任务。具体而言、IT组织很难确定安全的返回点、一旦确定、如何确保恢复的工作负载免受再次发生的攻击(来自休眠的恶意软件或通过容易受到攻击的应用程序)。

Jetstream DR for AVS与Azure NetApp Files 数据存储库可通过允许组织从可用时间点恢复来解决这些问题、以便在需要时将工作负载恢复到正常运行的隔离网络。通过恢复、应用程序可以相互运行并进行通信、同时不会使它们暴露在北-南流量中、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修复。



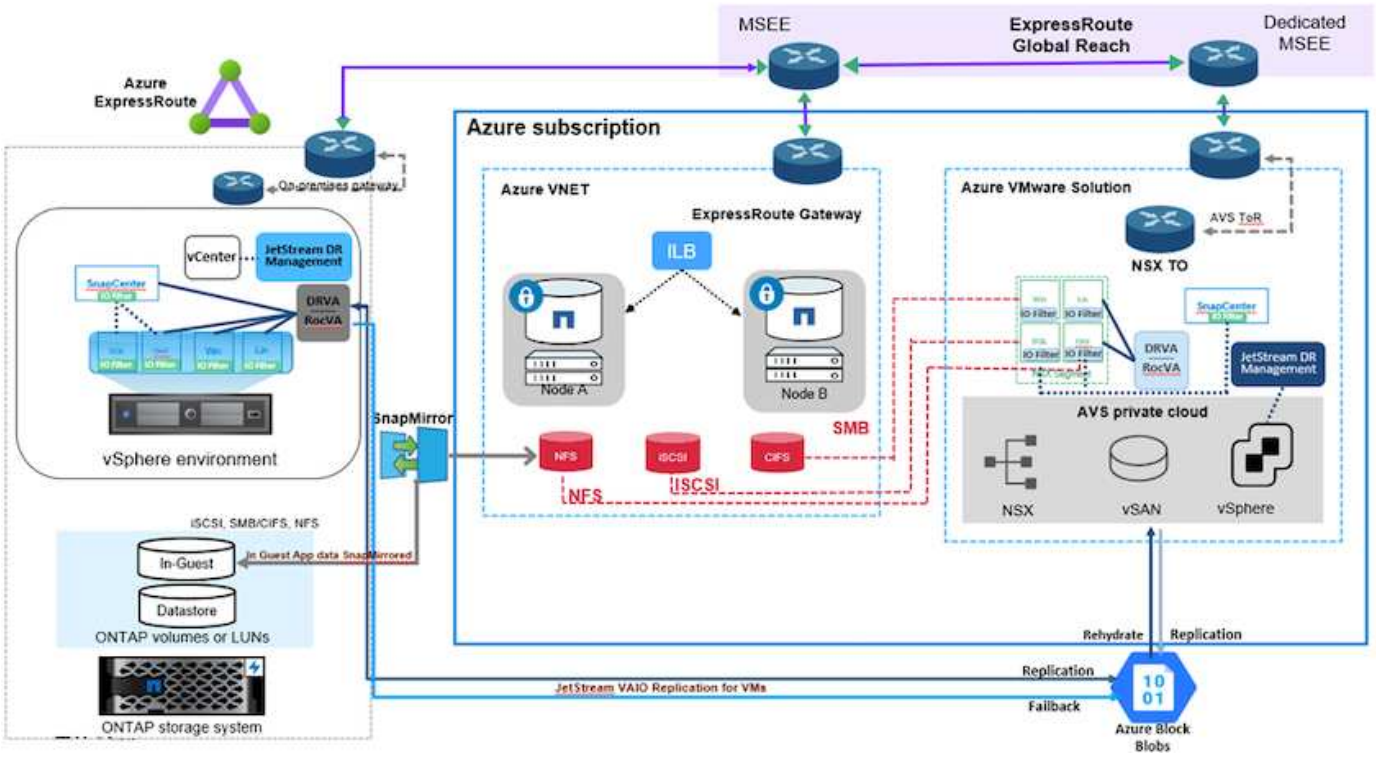
使用**CVO**和**AVS**进行灾难恢复(来宾连接存储)

概述

作者：NetApp公司Ravi BCB和Niyaz Mohamed

将灾难恢复到云是一种具有弹性且经济高效的方式、可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、可以将使用来宾连接存储的内部VMware工作负载复制到在Azure中运行的NetApp Cloud Volumes ONTAP。其中包括应用程序数据；但是、实际VM本身又如何。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。为此、可以使用SnapMirror以及Jetstream无缝恢复从内部复制到Cloud Volumes ONTAP 的工作负载、同时对VM VMDK使用vSAN存储。

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子系统内存储(也称为子系统连接)、我们假定内部环境正在使用SnapCenter 进行应用程序一致的备份。

本文档将对任何第三方备份或恢复解决方案 进行适用场景。根据环境中使用的解决方案 、按照最佳实践创建符合组织SLA的备份策略。

要在内部环境与Azure虚拟网络之间建立连接、请使用Express route全局访问或具有VPN网关的虚拟WAN。应根据内部VLAN设计创建分段。

将内部数据中心连接到Azure有多种选项、这使我们无法在本文档中概述特定的工作流。有关适当的内部到Azure连接方法、请参见Azure文档。

部署**DR**解决方案

解决方案 部署概述

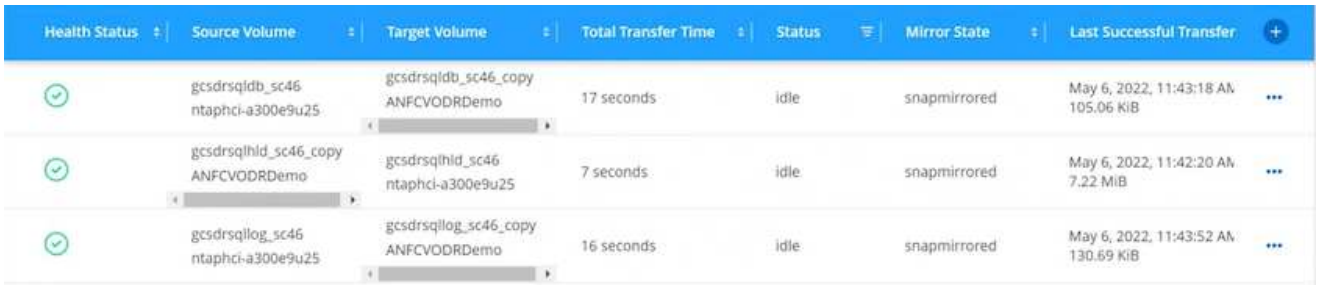
1. 确保使用具有必要RPO要求的SnapCenter 备份应用程序数据。
2. 在相应的订阅和虚拟网络中使用Cloud Manager使用正确的实例大小配置Cloud Volumes ONTAP。
   a. 为相关应用程序卷配置SnapMirror。
   b. 更新SnapCenter 中的备份策略、以便在计划作业完成后触发SnapMirror更新。
3. 在内部数据中心安装Jetstream灾难恢复软件、并启动虚拟机保护。
4. 在Azure VMware解决方案 私有云中安装Jetstream DR软件。

5. 在灾难事件期间、使用Cloud Manager中断SnapMirror关系、并触发虚拟机故障转移到指定AVS灾难恢复站点中的Azure NetApp Files 或vSAN数据存储库。
   a. 重新连接应用程序VM的iSCSI LUN和NFS挂载。
6. 在主站点恢复之后、通过反向重新同步SnapMirror来调用对受保护站点的故障恢复。

部署详细信息

在**Azure**上配置**CVO**并将卷复制到**CVO**

第一步是Cloud Volumes ONTAP在Azure ("链接。")并使用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集群的大小以及SDDC的持续运行时间。对于灾难恢复解决方案 、这两个主要注意事项有助于降低整体运营成本。SDDC可以小至三台主机、在整个规模的部署中一直到多主机集群。

部署AVS集群的决定主要取决于RPO/RTO要求。借助Azure VMware解决方案 、可以及时配置SDDC、以便为测试或实际灾难事件做好准备。及时部署的SDDC可在您不应对灾难时节省ESXi主机成本。但是、在配置SDDC时、这种部署形式会影响RTO几小时。

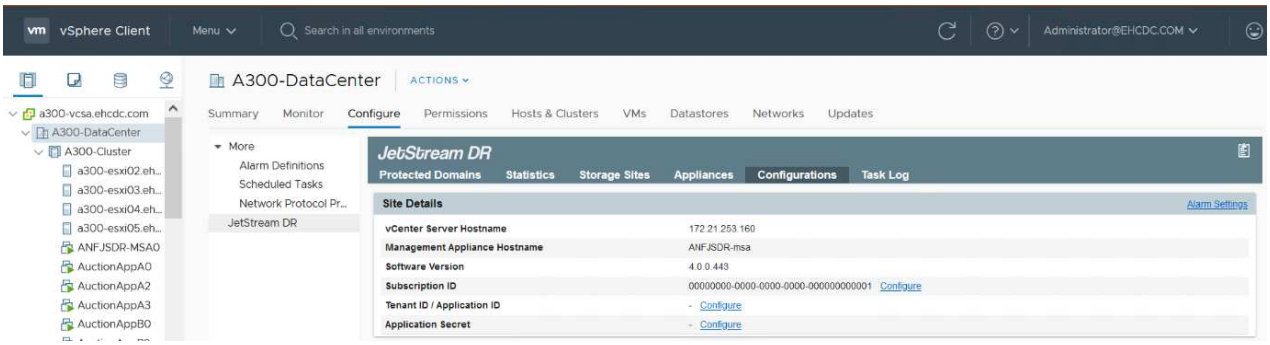
最常见的部署选项是、SDDC以无中断的引导模式运行。此选项占用的空间很小、可容纳三台始终可用的主机、还可以通过为模拟活动和合规性检查提供运行基线来加快恢复操作的速度、从而避免生产站点和灾难恢复站点之间发生操作偏差的风险。当需要处理实际灾难恢复事件时、可以快速将引导灯集群扩展到所需的级别。

要配置AVS SDDC (无论是按需配置还是在指示灯模式下配置)、请参见 "在 Azure 上部署和配置虚拟化环境"。前提条件是、在建立连接后、验证AVS主机上的子虚拟机是否能够使用Cloud Volumes ONTAP 中的数据。

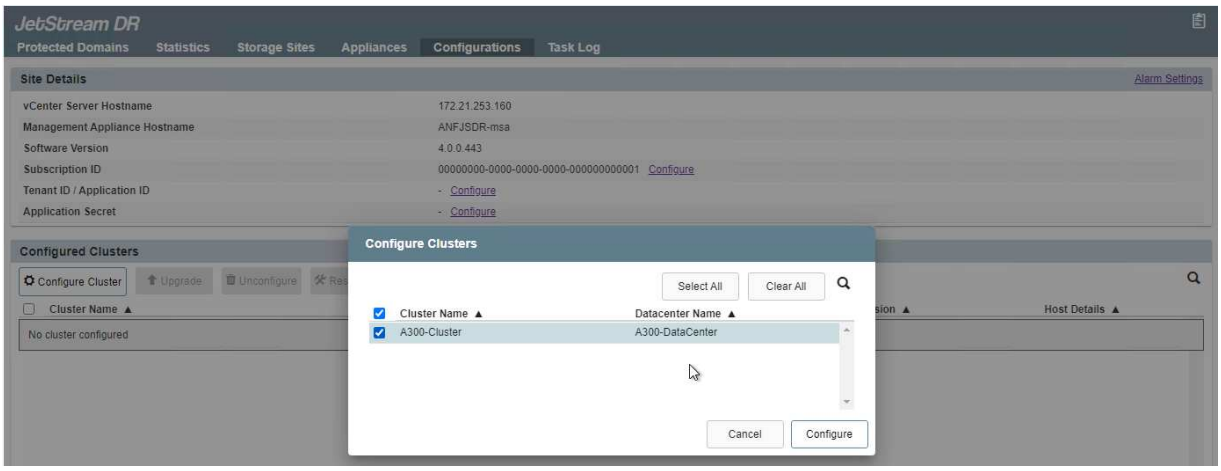
正确配置Cloud Volumes ONTAP 和AVS后、请使用VAIO机制并利用SnapMirror将应用程序卷副本复制到Cloud Volumes ONTAP 、开始配置Jetstream、以便自动将内部工作负载恢复到AVS (具有应用程序VMDK的VM和具有来宾存储的VM)。

Jetstream灾难恢复软件由三个主要组件组成：Jetstream灾难恢复管理服务器虚拟设备(Virtual Appliance、MSA)、灾难恢复虚拟设备(DR Virtual Appliance、DRVA)和主机组件(I/O筛选器软件包)。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：

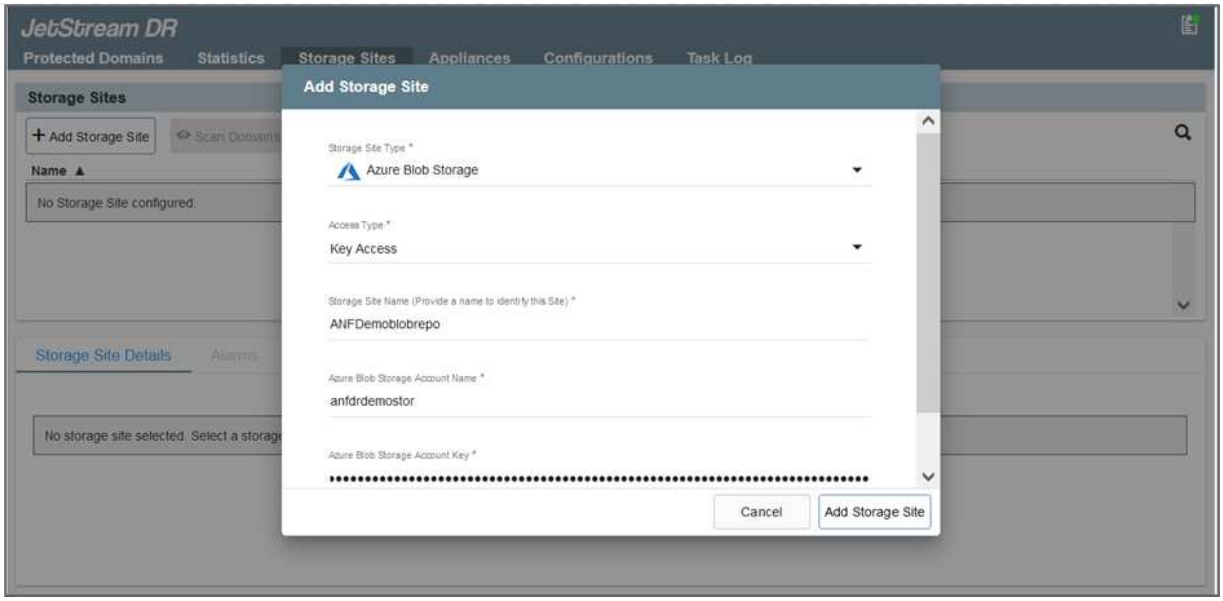
1. 检查前提条件。
2. 运行容量规划工具以获取资源和配置建议。
3. 将Jetstream DR MSA部署到指定集群中的每个vSphere主机。
4. 在浏览器中使用其DNS名称启动MSA。
5. 向MSA注册vCenter Server。
6. 部署Jetstream DR MSA并注册vCenter Server后、导航到vSphere Web Client中的Jetstream DR插件。可通过导航到"数据中心">"配置">"Jetstream DR"来完成此操作。



7. 在Jetstream DR界面中、完成以下任务：
   a. 使用I/O筛选器软件包配置集群。

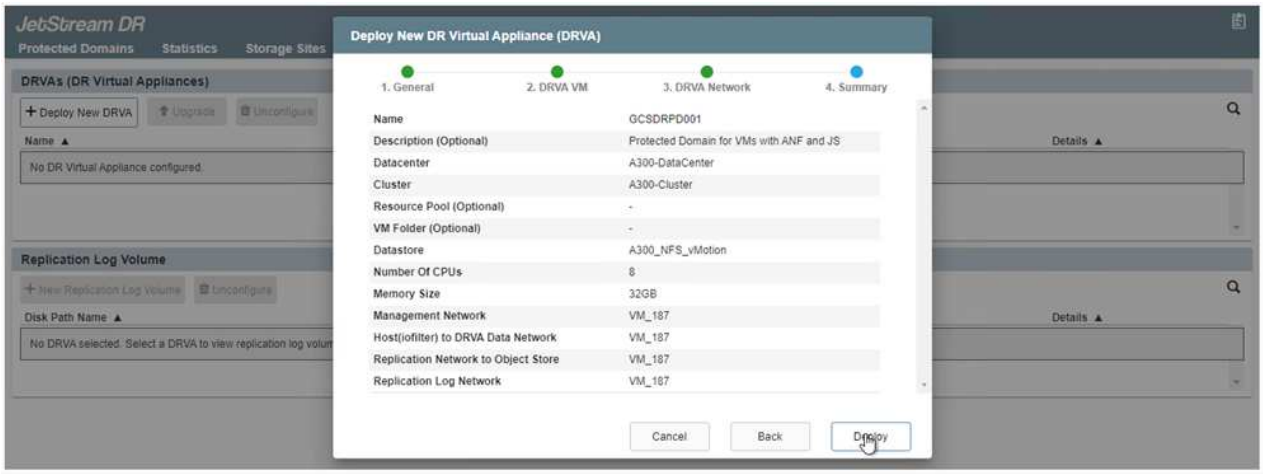


   b. 添加位于恢复站点的Azure Blob存储。

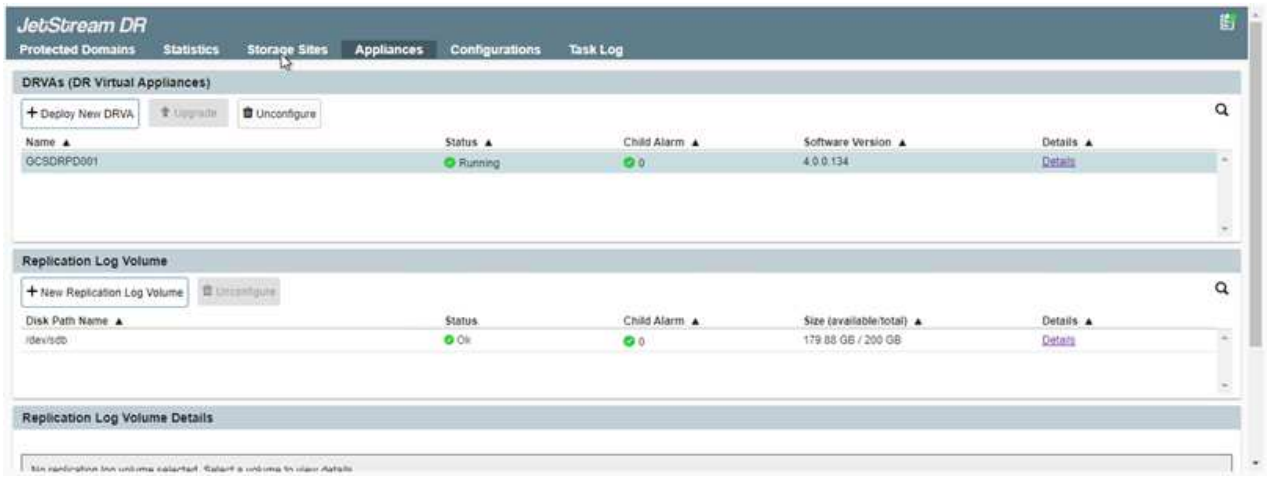


8. 从设备选项卡部署所需数量的灾难恢复虚拟设备(DR Virtual Appliances、DRVA)。

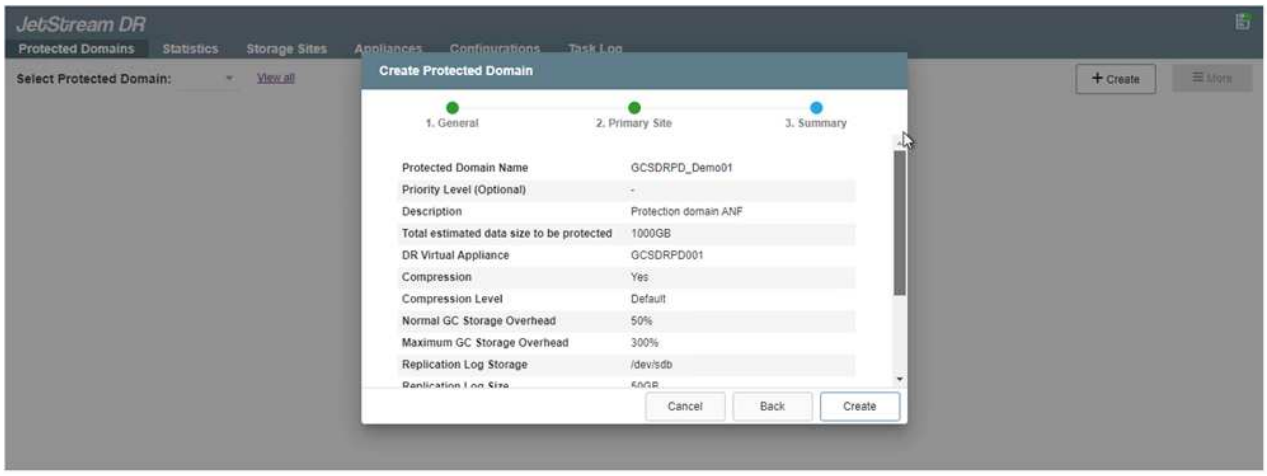
使用容量规划工具估计所需的DRBA数量。

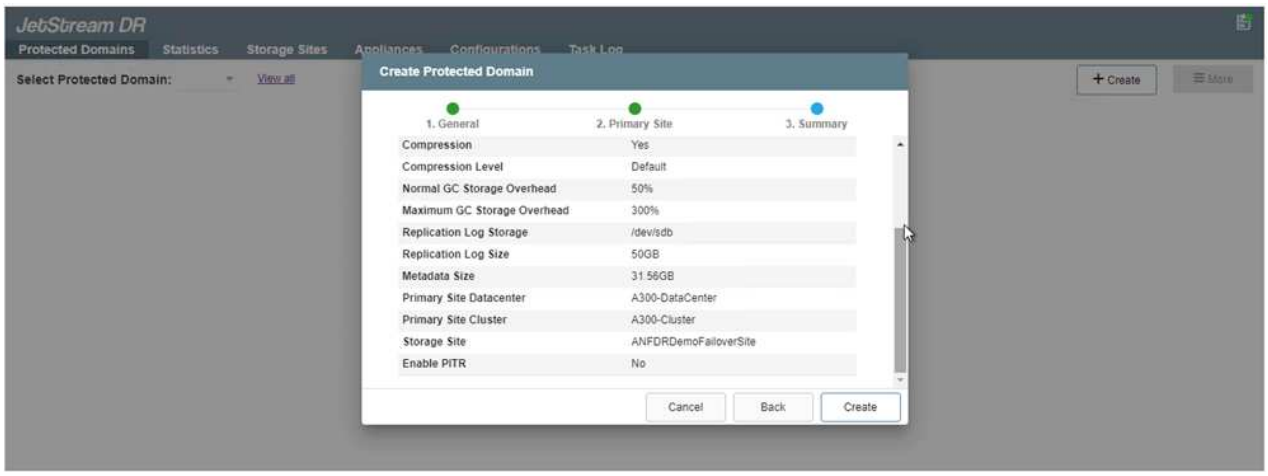


9. 使用可用数据存储库或独立的共享iSCSI存储池中的VMDK为每个DRVA创建复制日志卷。



10. 在受保护域选项卡中、使用Azure Blob Storage站点、DRVA实例和复制日志的相关信息创建所需数量的受保护域。受保护域定义集群中一个或一组同时受保护的应用程序VM、并为故障转移/故障恢复操作分配优先级顺序。

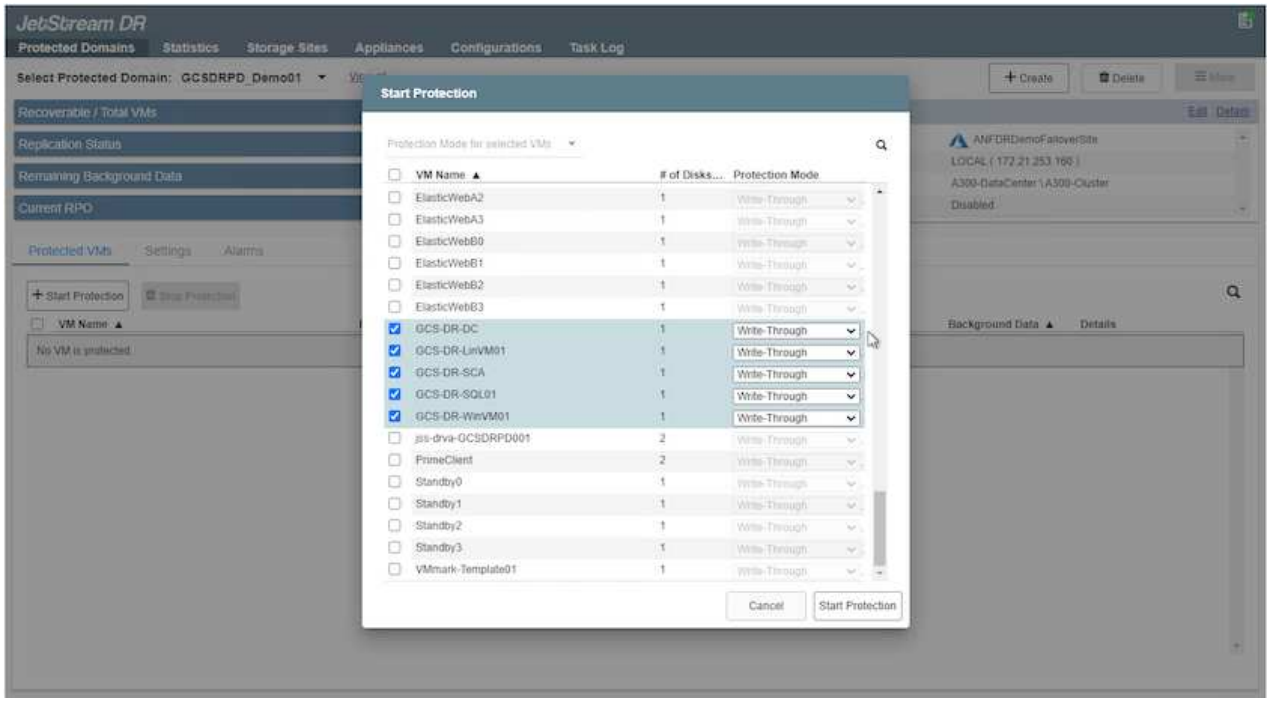




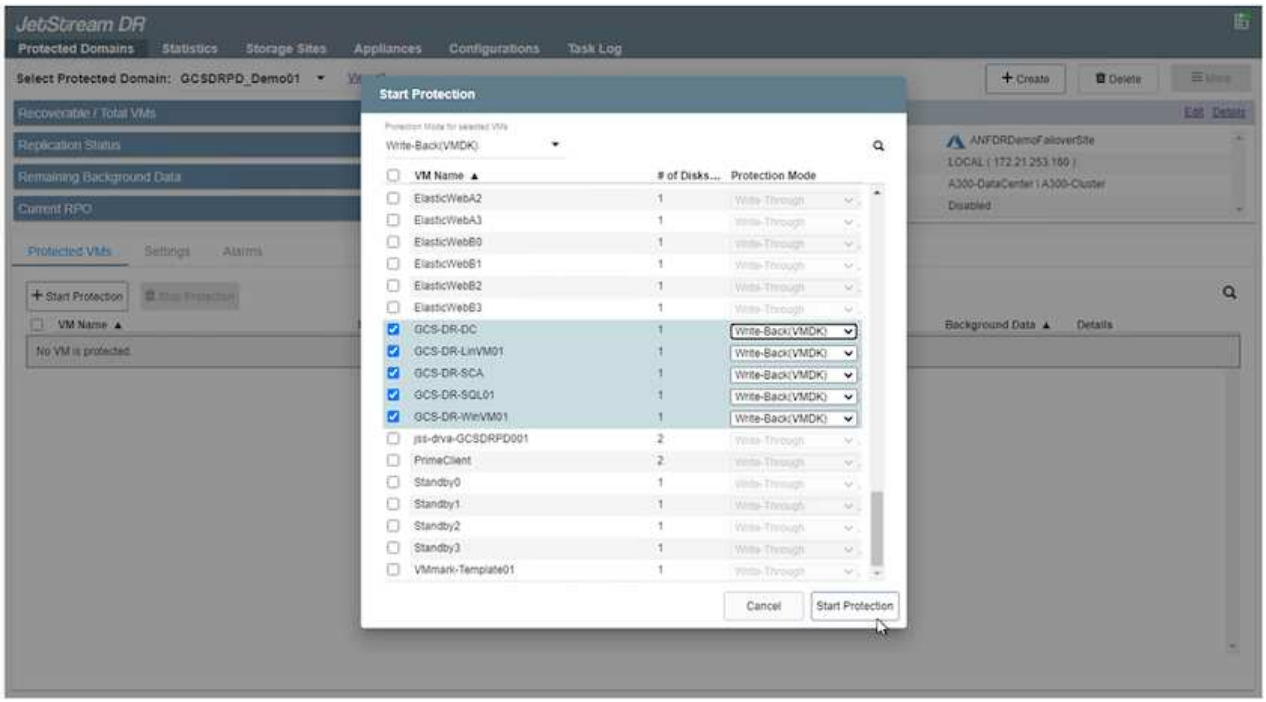
11. 选择要保护的VM、并根据依赖关系将这些VM分组到应用程序组中。通过应用程序定义、您可以将VM集分组到逻辑组中、这些逻辑组包含其启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

确保对受保护域中的所有VM使用相同的保护模式。

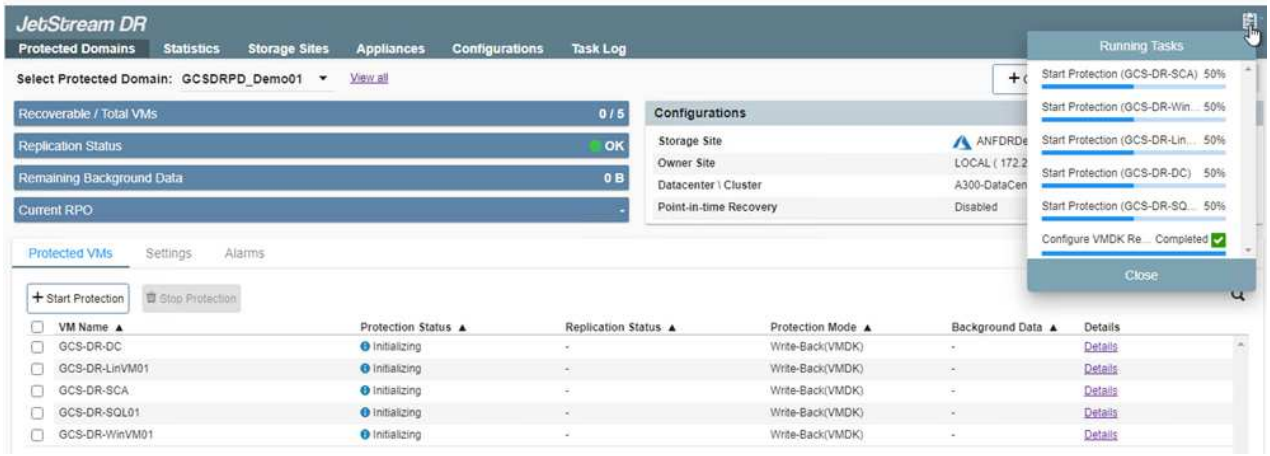
回写(VMDK)模式可提供更高的性能。



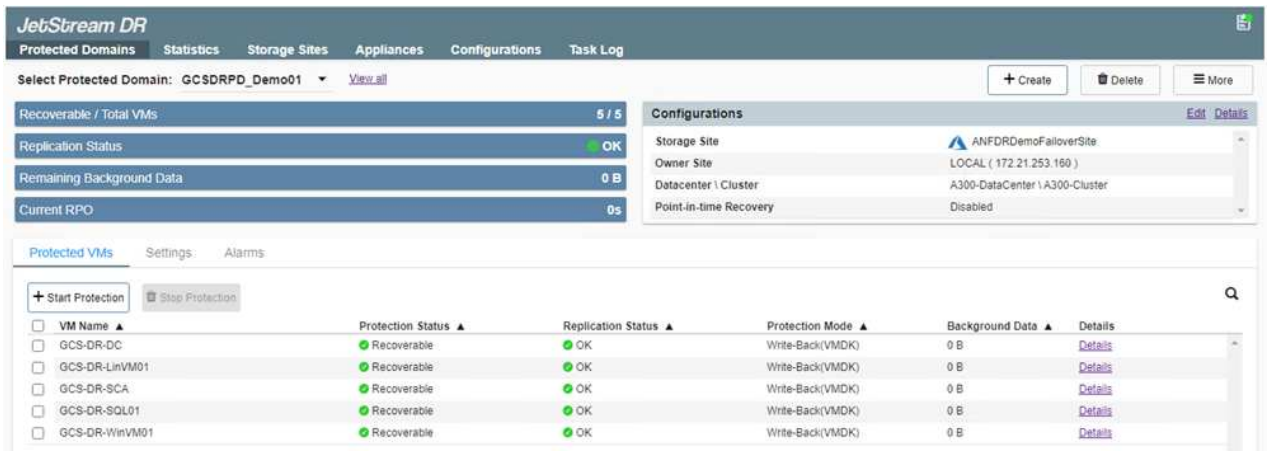
12. 确保将复制日志卷放置在高性能存储上。



13. 完成后、单击受保护域的开始保护。此时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、虚拟机保护状态将标记为可恢复。

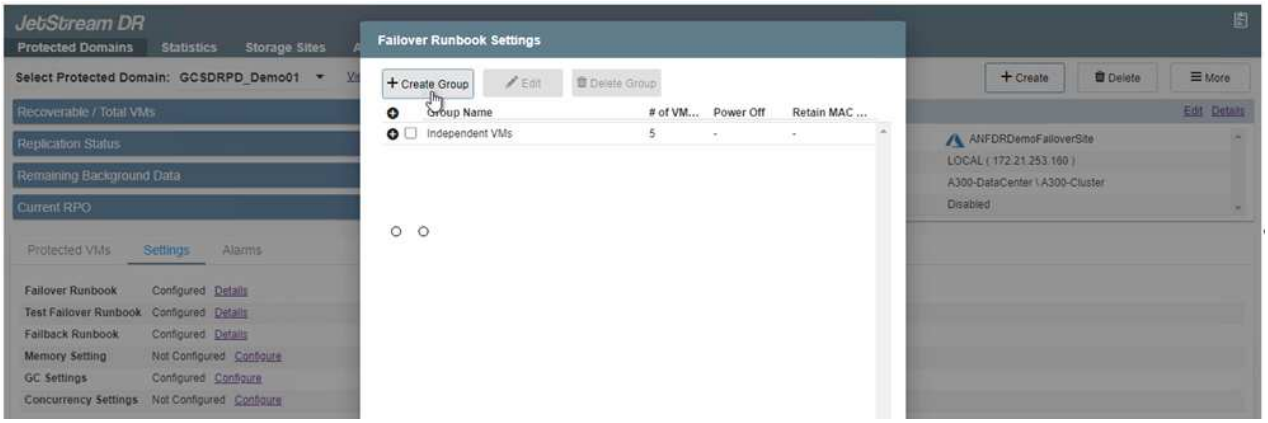


可以对故障转移运行手册进行配置、以便对VM (称为恢复组)进行分组、设置启动顺序以及修改CPU/内存设置以及IP配置。

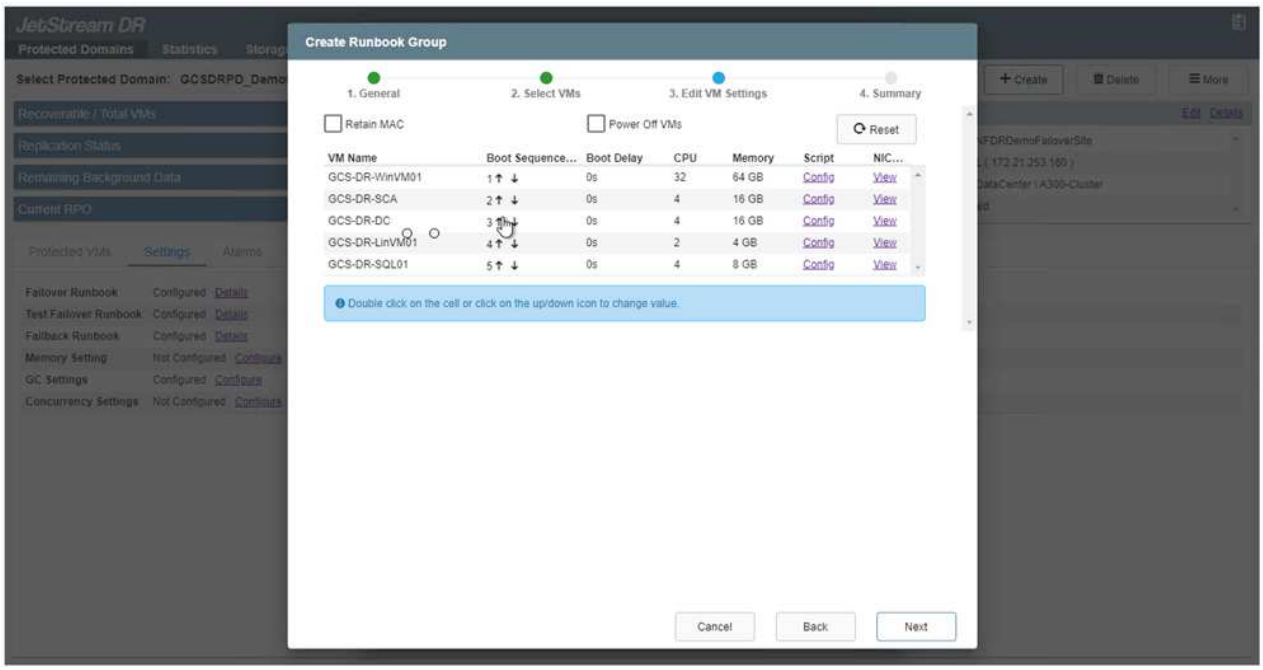
15. 单击设置、然后单击运行手册配置链接以配置运行手册组。

16. 单击创建组按钮开始创建新的运行手册组。

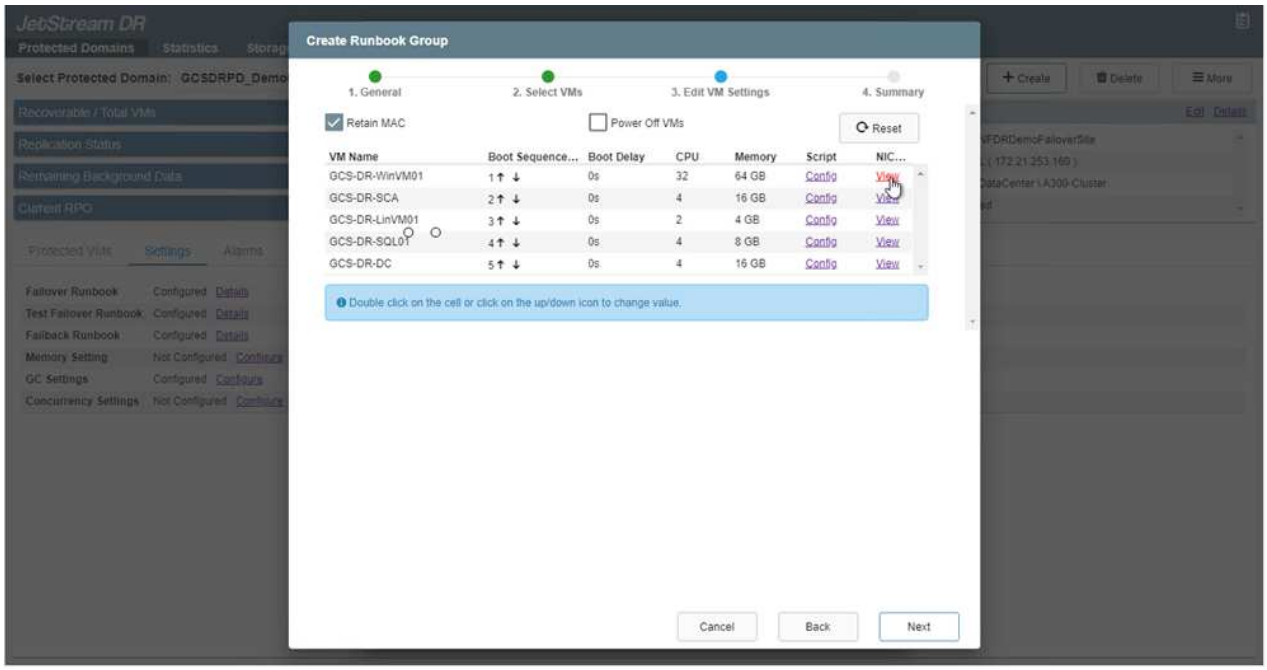
如果需要、请在屏幕下部应用自定义预脚本和后脚本、以便在运行手册组执行操作之前和之后自动运行。确保Runbook脚本驻留在管理服务器上。



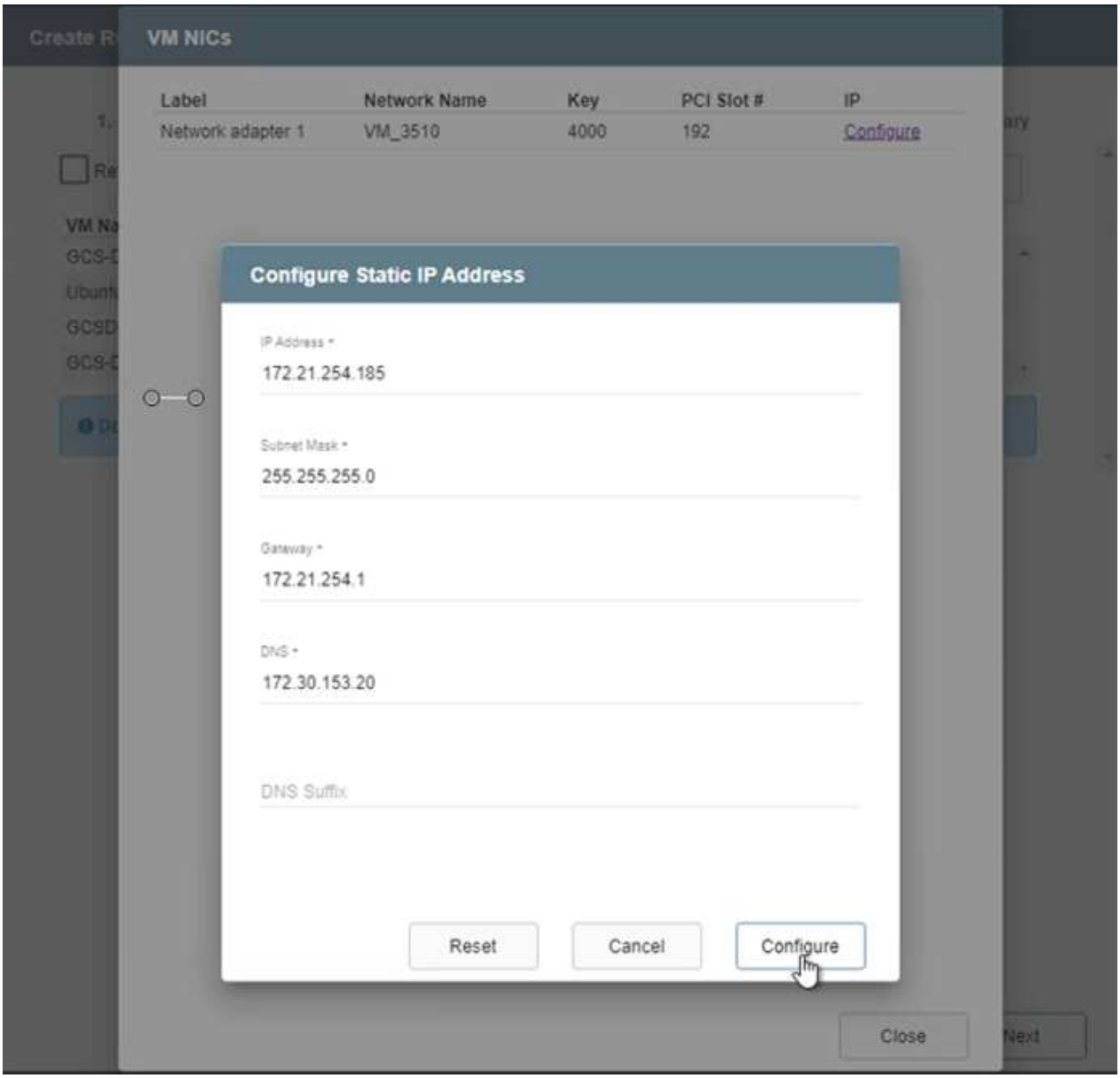
17. 根据需要编辑VM设置。指定用于恢复VM的参数、包括启动顺序、启动延迟(以秒为单位指定)、CPU数量以及要分配的内存量。单击向上或向下箭头更改VM的启动顺序。此外、还提供了用于保留MAC的选项。

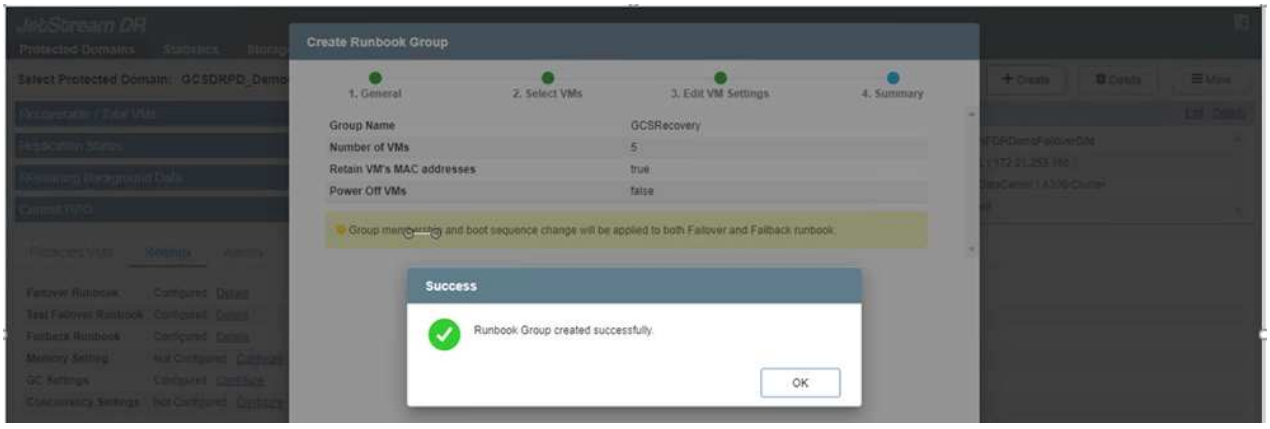


18. 可以为组中的各个VM手动配置静态IP地址。单击虚拟机的NIC视图链接以手动配置其IP地址设置。



19. 单击配置按钮以保存相应虚拟机的NIC设置。





现在、故障转移和故障恢复运行手册的状态均列为已配置。故障转移和故障恢复操作手册组会使用相同的初始VM和设置成对创建。如有必要、可以通过单击相应的详细信息链接并进行更改来单独自定义任何运行手册组的设置。

在私有云中安装**Jetstream DR for AVS**

恢复站点(AVS)的一个最佳实践是、提前创建一个三节点的试用集群。这样可以对恢复站点基础架构进行预配置、其中包括以下内容：

- 目标网络分段、防火墙、DHCP和DNS等服务等
- 安装适用于AVS的Jetstream DR
- 将ANF卷配置为数据存储库等

Jetstream DR支持任务关键型域采用接近零的RTO模式。对于这些域、应预安装目标存储。在这种情况下、建议使用ANF存储类型。

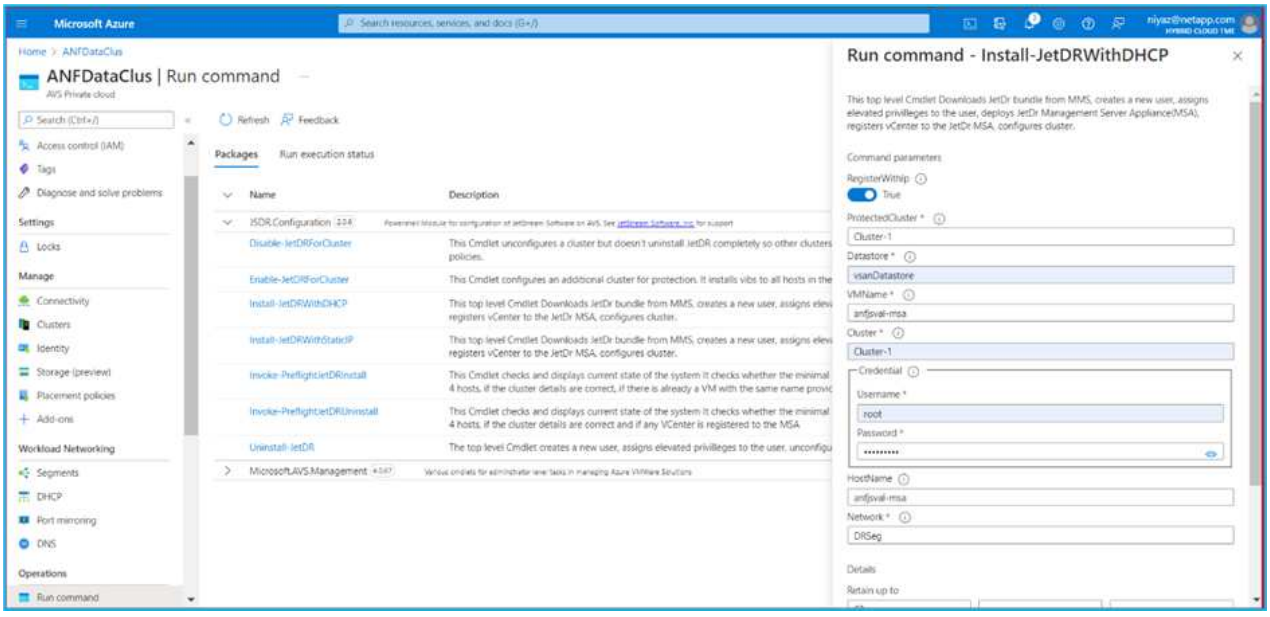
应在AVS集群上配置网络配置、包括创建网段、以满足内部部署要求。

根据SLA和RTO要求、您可以使用持续故障转移或常规(标准)故障转移模式。对于接近零的RTO、您应在恢复站点开始持续重新水化。

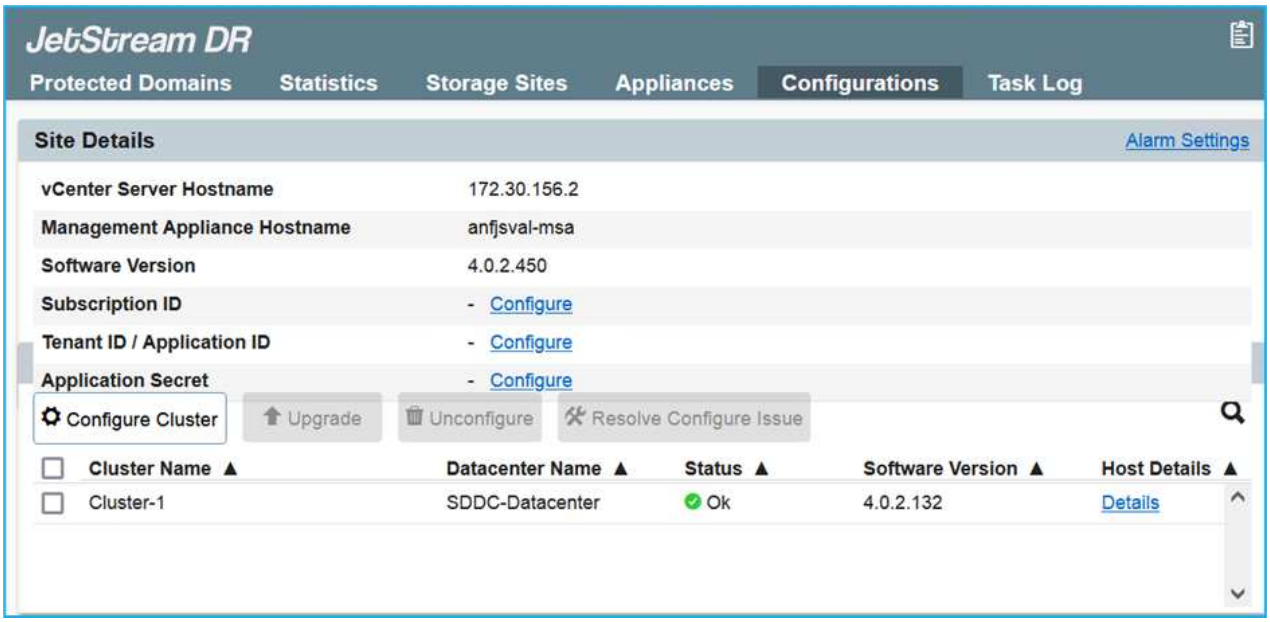
1. 要在Azure VMware解决方案 私有云上安装Jetstream DR for AVS、请使用Run命令。从Azure门户中、转到Azure VMware解决方案 、选择私有云、然后选择运行命令>软件包> JSDR.Configuration。

   Azure VMware解决方案 的默认CloudAdmin用户没有足够的权限来安装适用于AVS的Jetstream DR。Azure VMware解决方案 通过调用适用于Jetstream DR的Azure VMware解决方案 Run命令、可以简化并自动安装Jetstream DR。

   以下屏幕截图显示了使用基于DHCP的IP地址进行安装的情况。

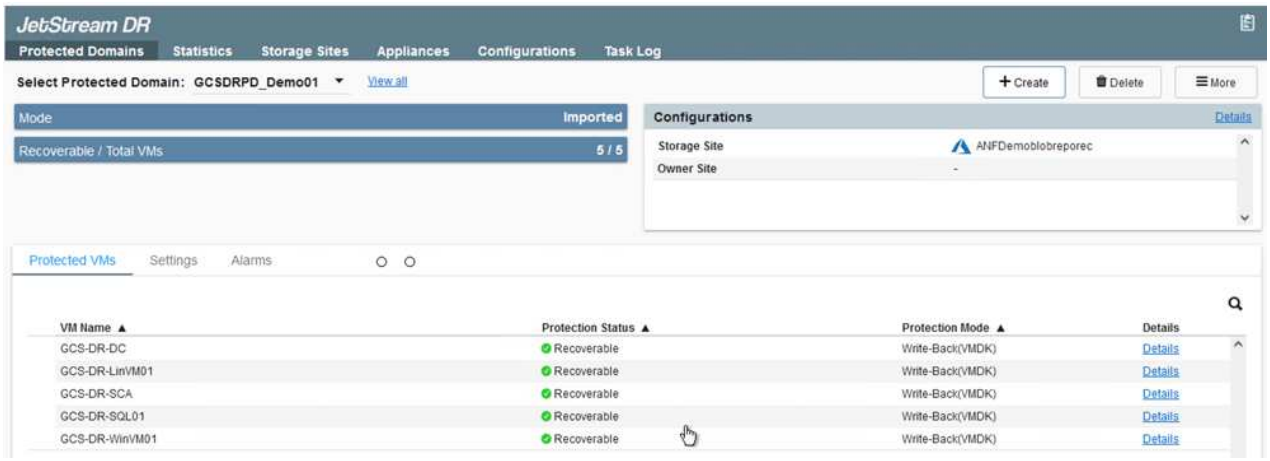


2. 完成适用于AVS的Jetstream DR安装后、刷新浏览器。要访问Jetstream DR UI、请转到SDDC Datacenter >配置> Jetstream DR。



3. 在Jetstream DR界面中、完成以下任务：
   a. 添加用于将内部集群作为存储站点进行保护的Azure Blob Storage帐户、然后运行扫描域选项。
   b. 在显示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。

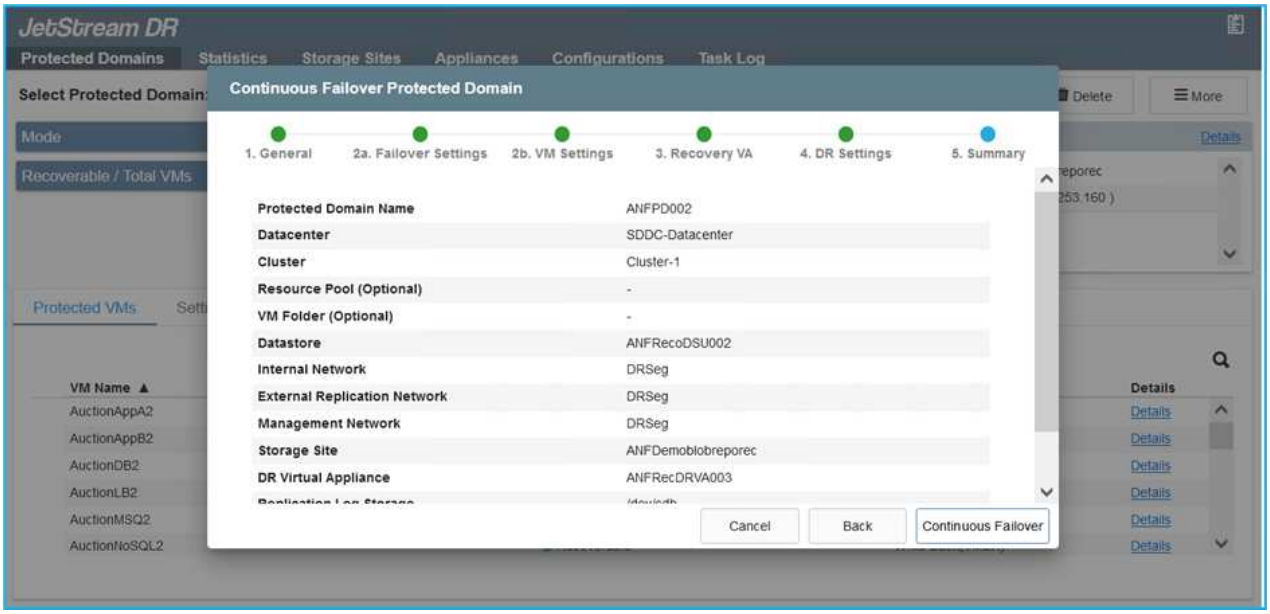
4. 已导入此域以进行恢复。转到"受保护域"选项卡并验证是否已选择目标域、或者从"选择受保护域"菜单中选择所需域。此时将显示受保护域中可恢复的VM列表。



5. 导入受保护域后、部署DRVA设备。

> 也可以使用CPT创建的计划自动执行这些步骤。

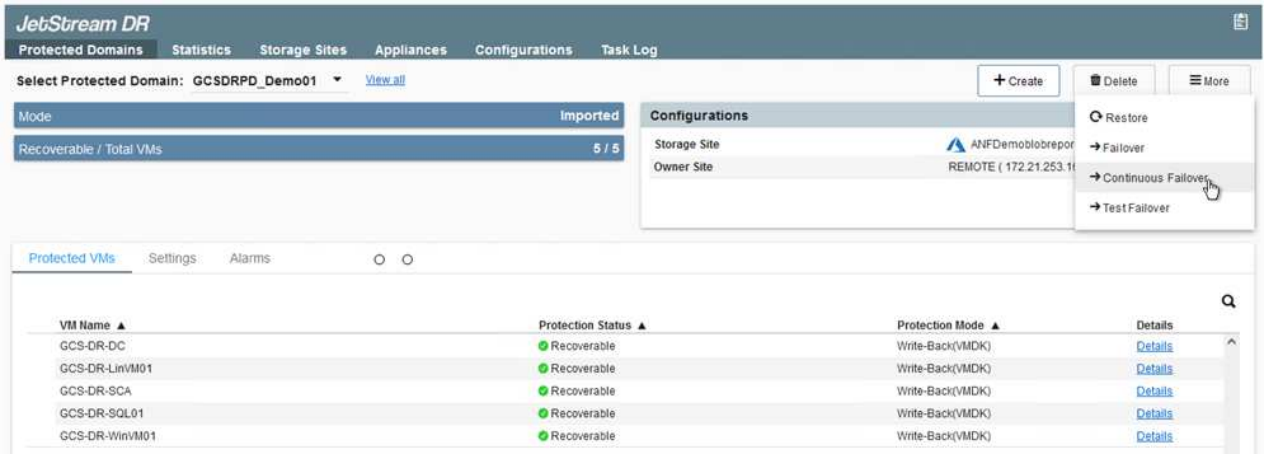
6. 使用可用的vSAN或ANF数据存储库创建复制日志卷。
7. 导入受保护域并配置恢复VA以使用ANF数据存储库放置VM。



确保选定网段上已启用DHCP、并且有足够的可用IP。在恢复域时、系统会临时使用动态IP。每个正在恢复的VM (包括持续重新融合)都需要一个单独的动态IP。恢复完成后、此IP将被释放并可重复使用。

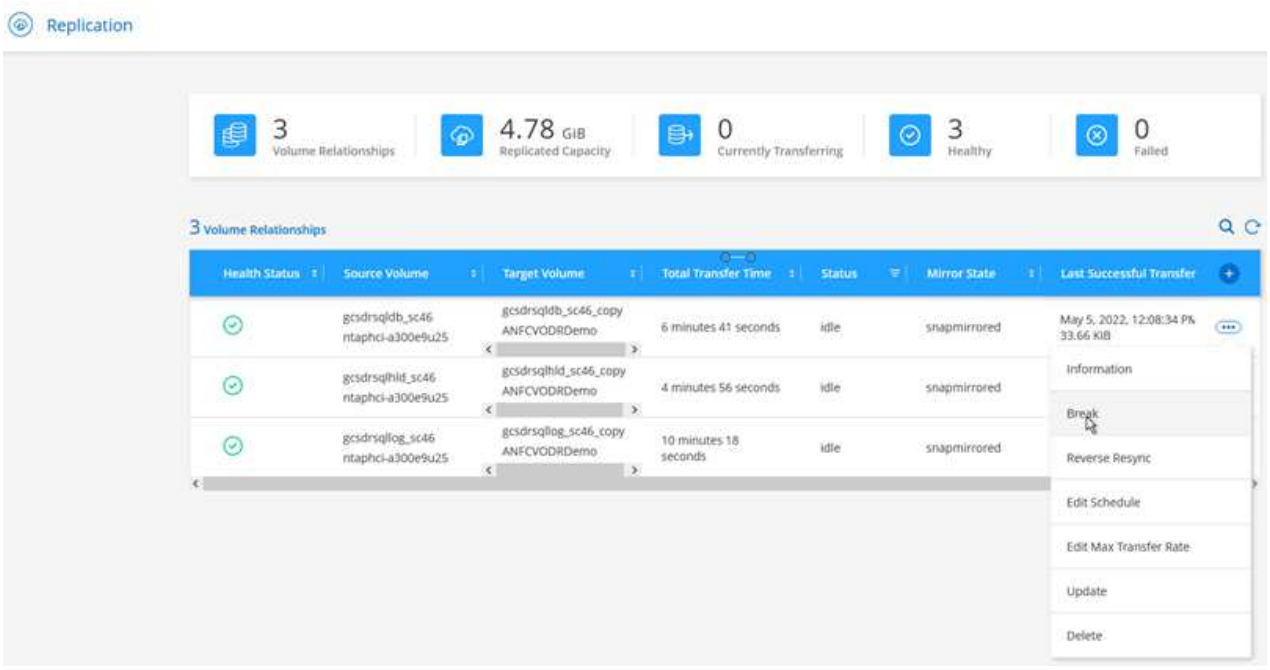
8. 选择相应的故障转移选项(持续故障转移或故障转移)。在此示例中、选择了持续再融合(持续故障转移)。

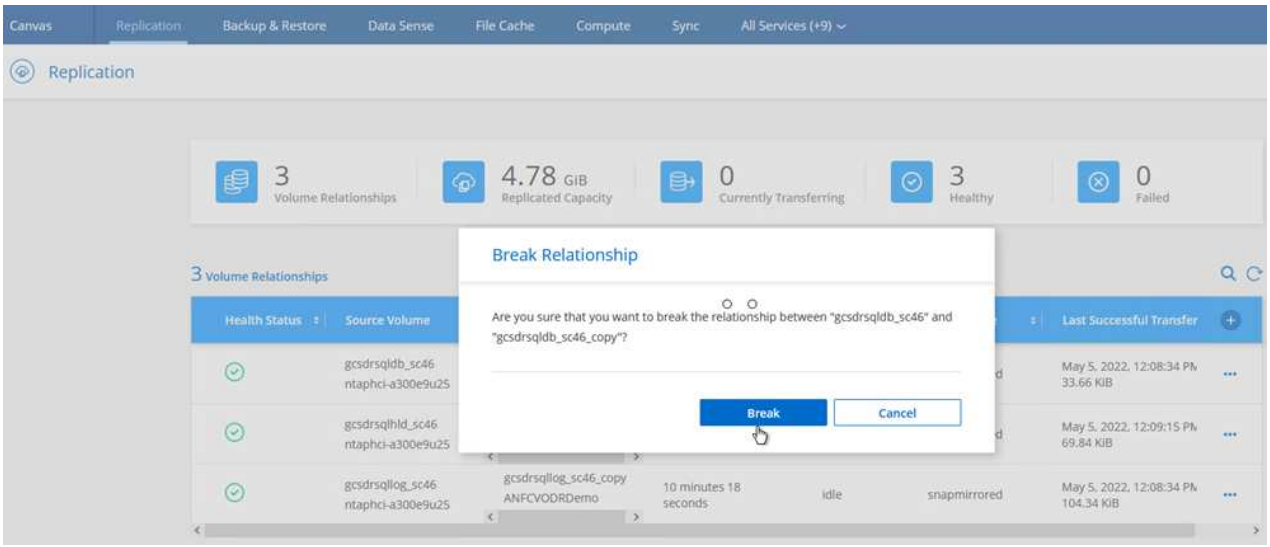
尽管执行配置时的持续故障转移和故障转移模式有所不同、但这两种故障转移模式都使用相同的步骤进行配置。在发生灾难事件时、可以同时配置和执行故障转移步骤。可以随时配置持续故障转移、然后允许在正常系统运行期间在后台运行。发生灾难事件后、将完成持续故障转移、以便立即将受保护VM的所有权转移到恢复站点(接近零的RTO)。



持续故障转移过程开始、可从UI监控其进度。单击当前步骤部分中的蓝色图标将显示一个弹出窗口、其中显示了故障转移过程当前步骤的详细信息。

1. 在内部环境的受保护集群发生灾难(部分或完整故障)后、您可以在中断相应应用程序卷的SnapMirror关系后使用Jetstream为VM触发故障转移。

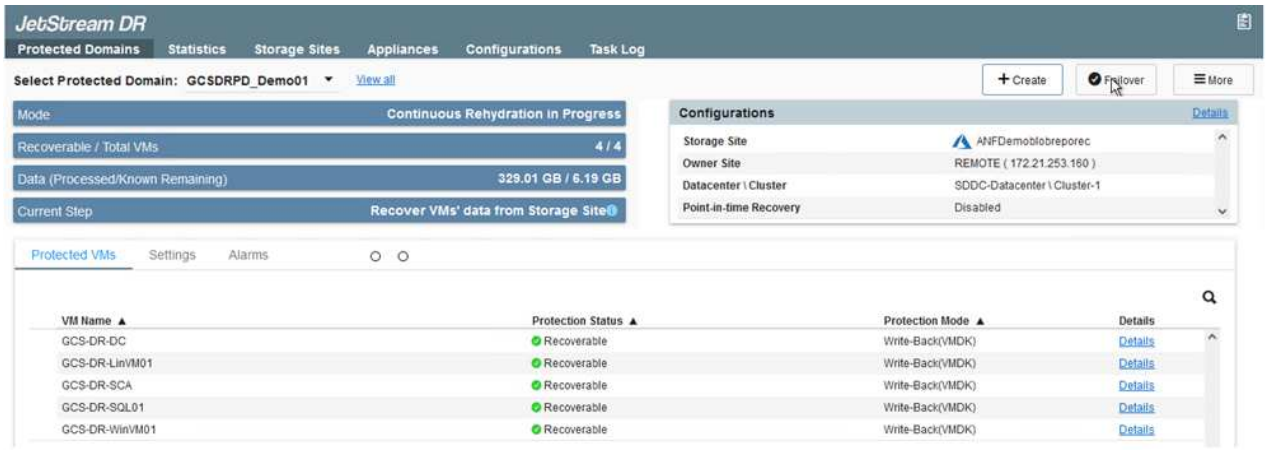


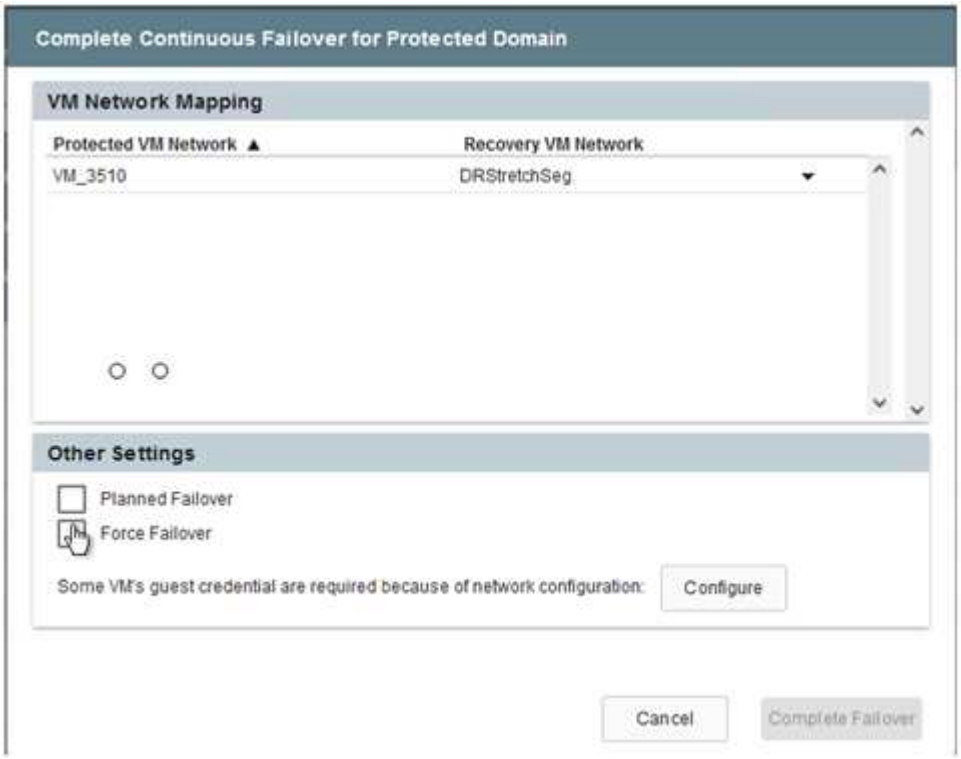


此步骤可以轻松地自动执行、以便于恢复过程。

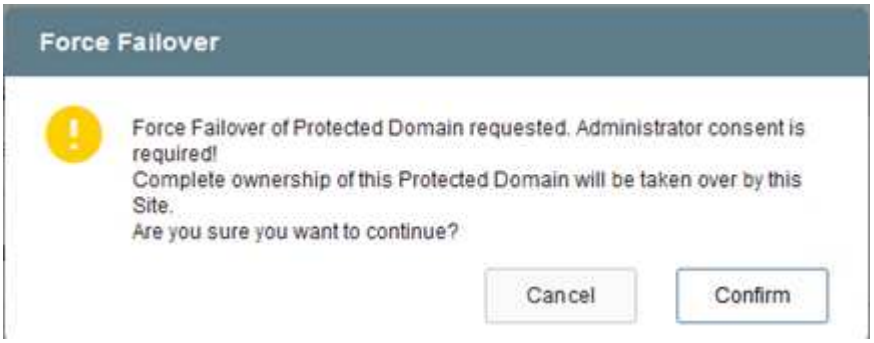
2. 在AVS SDDC (目标端)上访问Jetstream UI并触发故障转移选项以完成故障转移。任务栏将显示故障转移活动的进度。

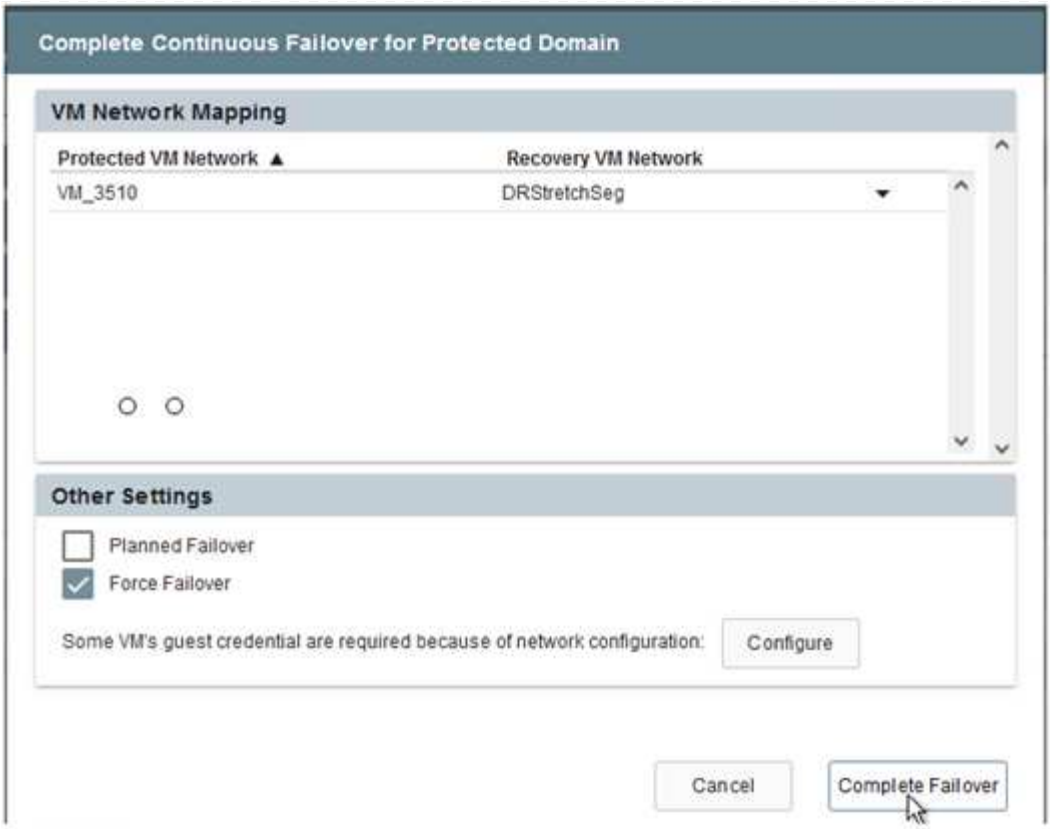
   在完成故障转移时显示的对话框窗口中、可以按计划或假定强制指定故障转移任务。





强制故障转移假定主站点不再可访问、并且恢复站点应直接接管受保护域的所有权。





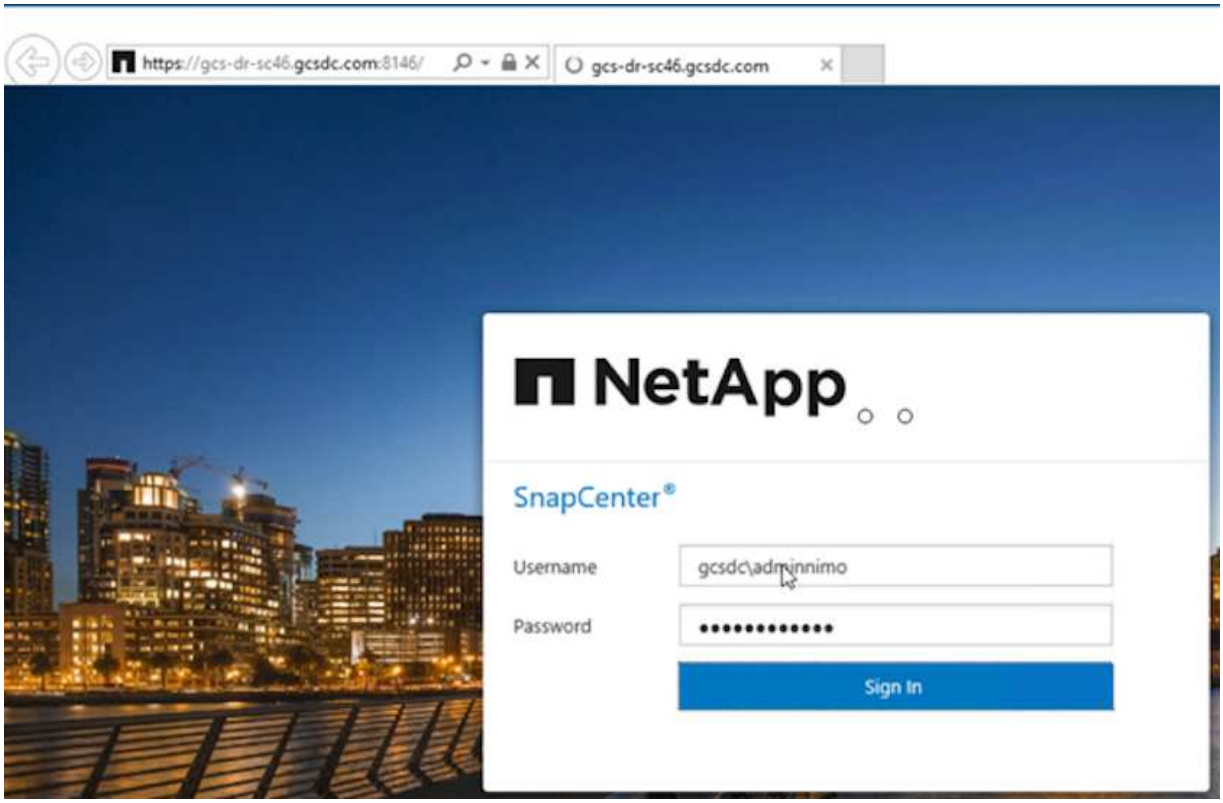
3. 持续故障转移完成后、将显示一条消息、确认任务完成。任务完成后、访问已恢复的VM以配置iSCSI或NFS会话。

故障转移模式将更改为在故障转移中运行、并且VM状态可恢复。受保护域中的所有VM现在都在恢复站点上以故障转移操作手册设置指定的状态运行。

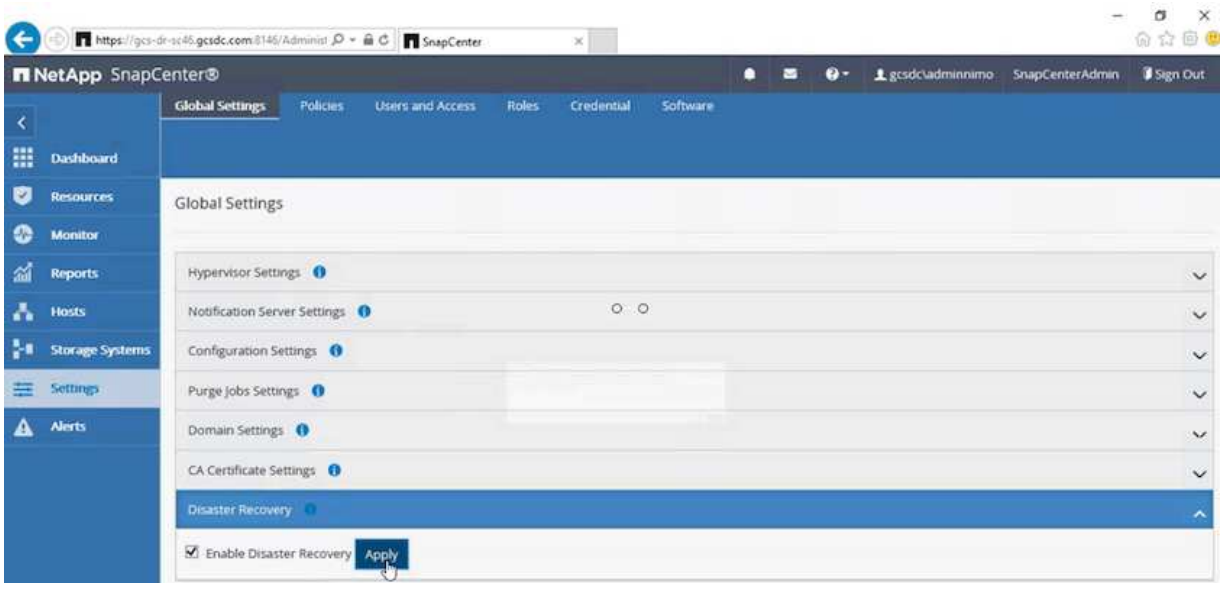
要验证故障转移配置和基础架构、可以在测试模式(测试故障转移选项)下运行Jetstream DR、以观察虚拟机及其数据从对象存储恢复到测试恢复环境的过程。在测试模式下执行故障转移操作步骤 时、其操作类似于实际的故障转移过程。

4. 恢复虚拟机后、请对子系统中的存储使用存储灾难恢复。要演示此过程、请在此示例中使用SQL Server。

5. 登录到AVS SDDC上已恢复的SnapCenter VM并启用灾难恢复模式。
   a. 使用browserN访问SnapCenter UI。



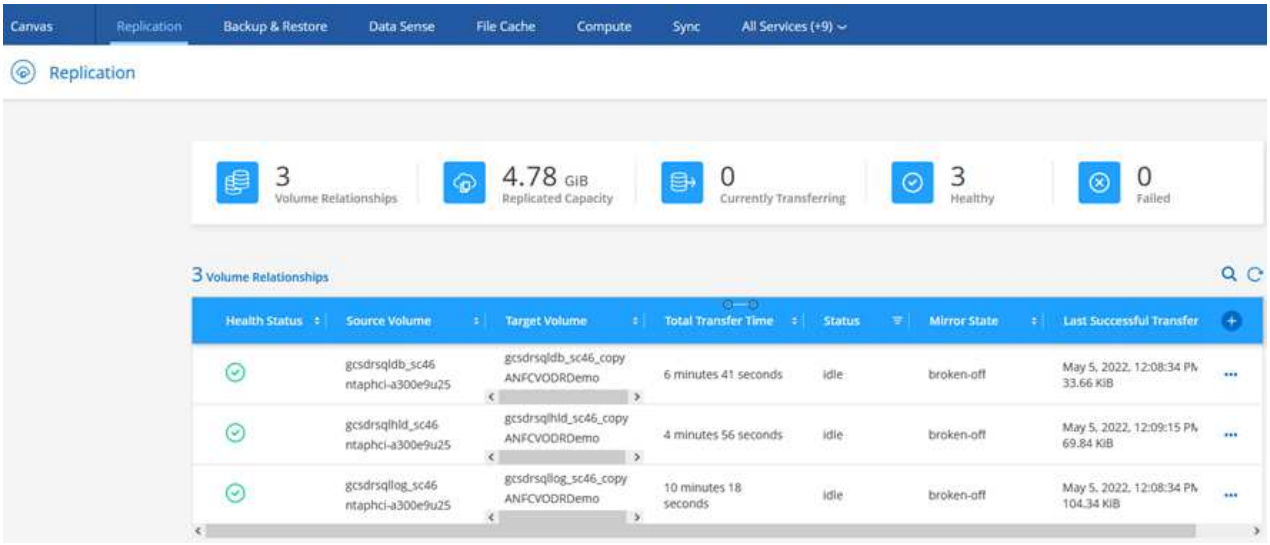
   b. 在设置页面中、导航到设置>全局设置>灾难恢复。
   c. 选择启用灾难恢复。
   d. 单击应用。



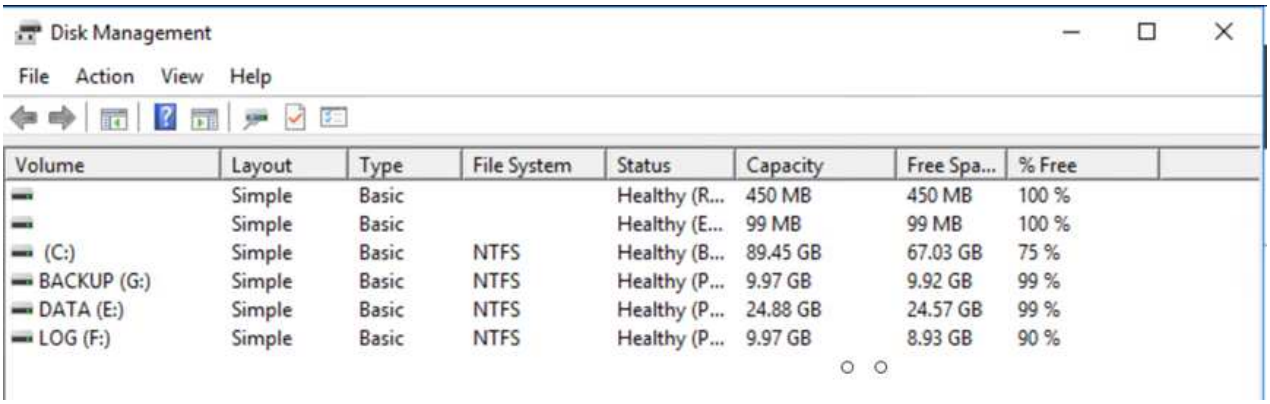
   e. 单击"监控">"作业"以验证是否已启用灾难恢复作业。

应使用NetApp SnapCenter 4.6或更高版本进行存储灾难恢复。对于先前版本、应使用应用程序一致的快照(使用SnapMirror复制)、如果必须在灾难恢复站点中恢复先前的备份、则应执行手动恢复。

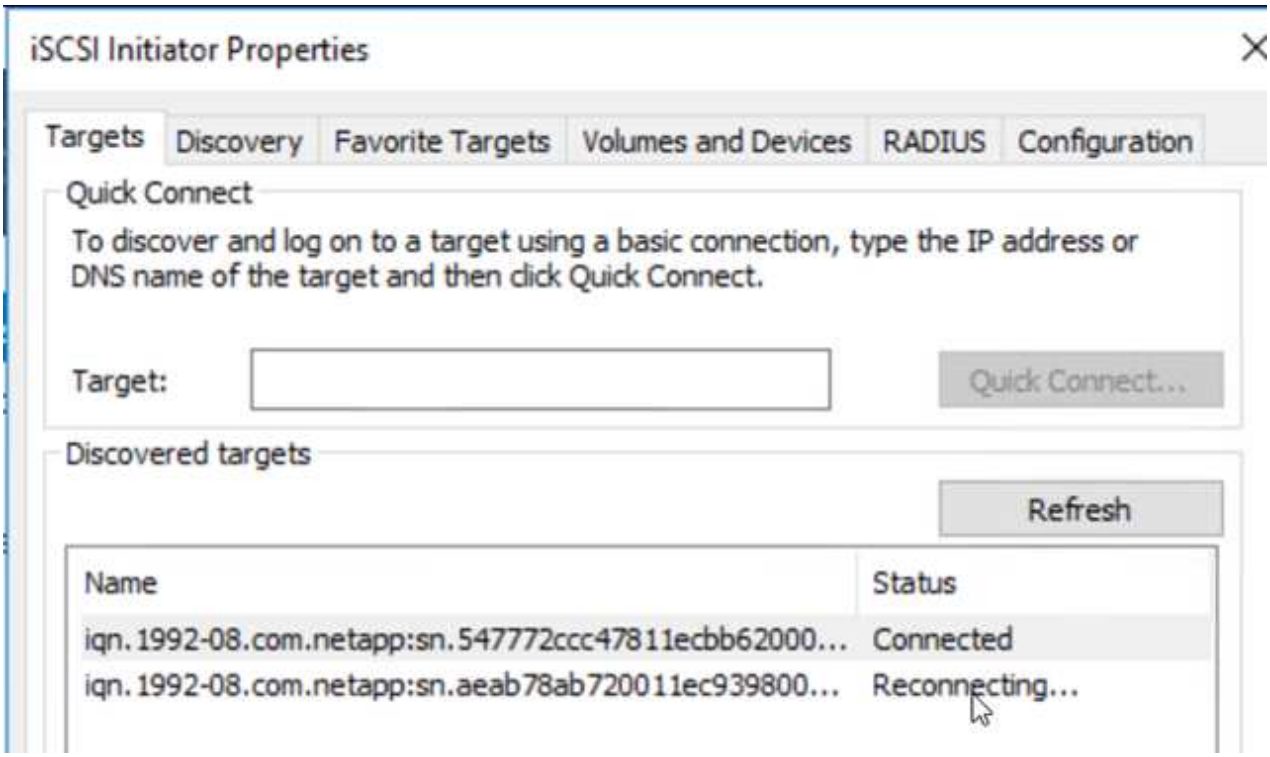
6. 确保SnapMirror关系已断开。



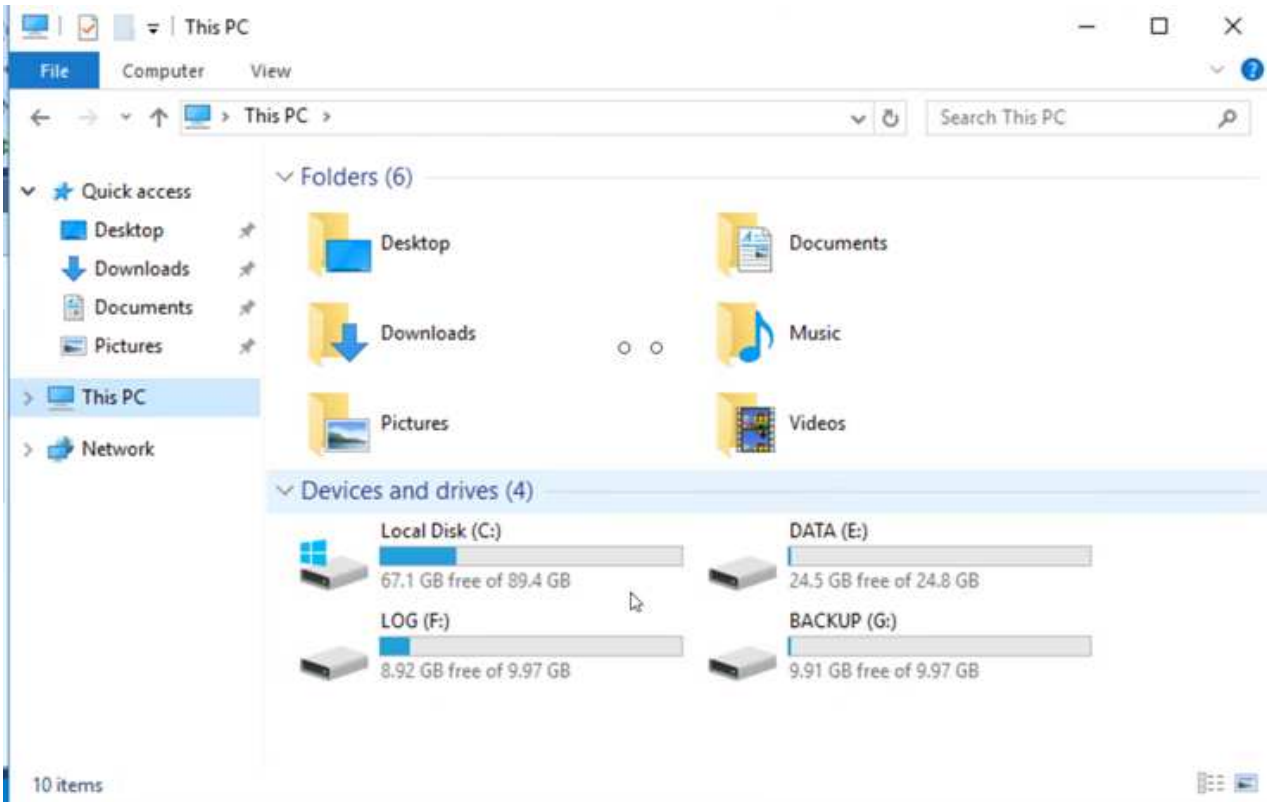
7. 使用相同的驱动器号将LUN从Cloud Volumes ONTAP 连接到已恢复的SQL子虚拟机。



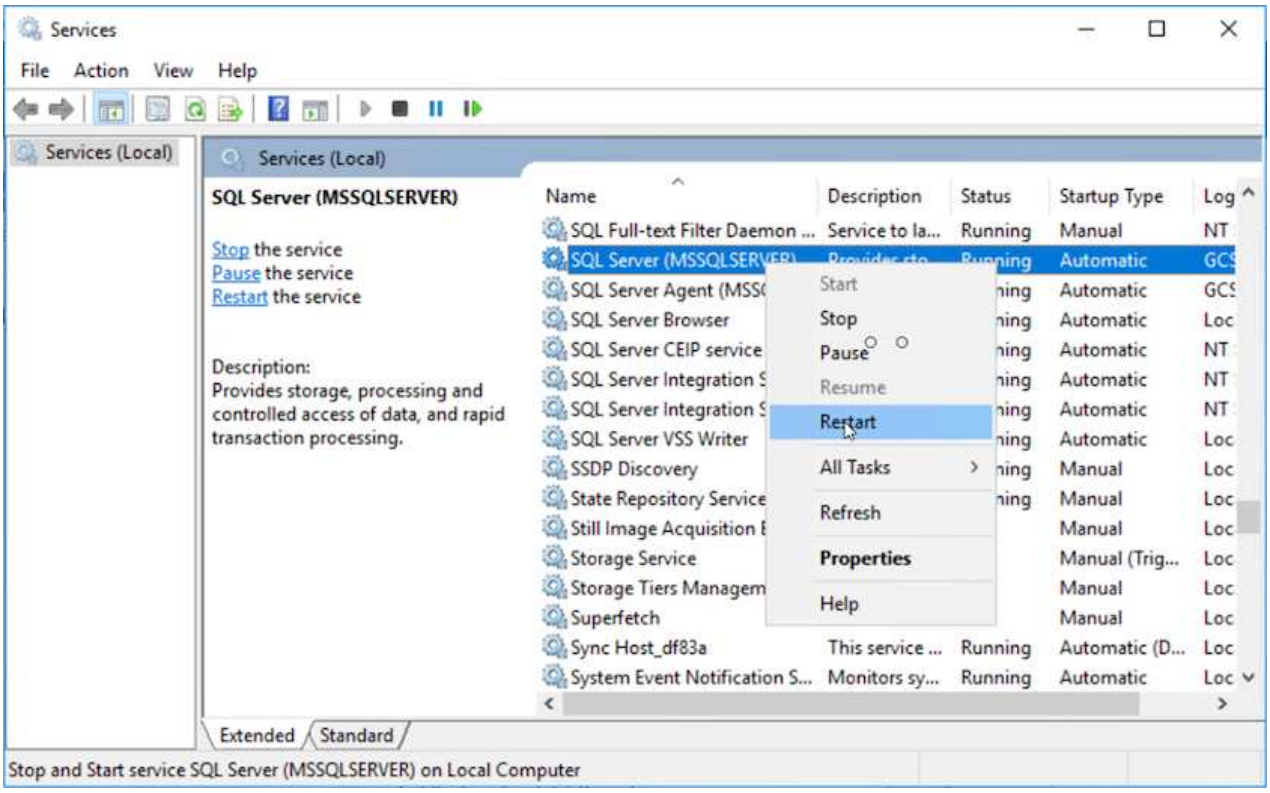
8. 打开iSCSI启动程序、清除先前已断开连接的会话、然后为复制的Cloud Volumes ONTAP 卷添加新目标以及多路径。



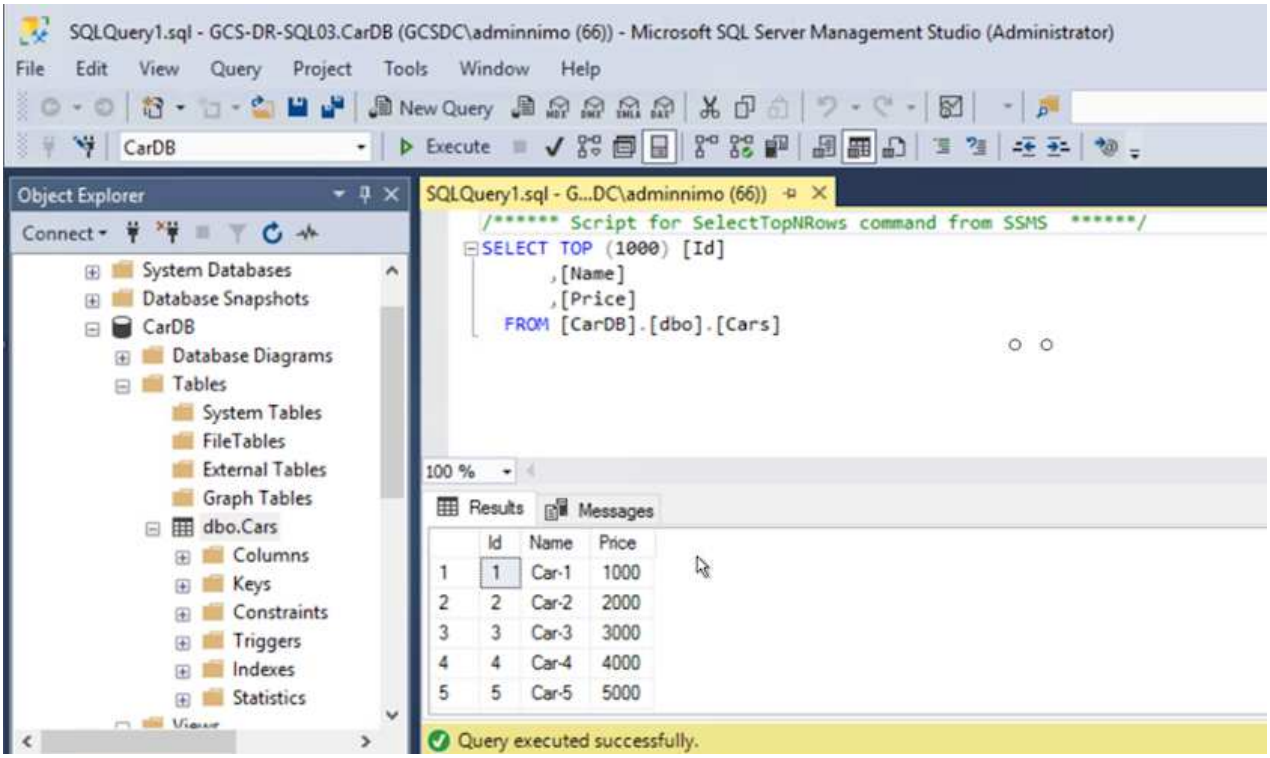
9. 确保使用DR之前使用的相同驱动器盘符连接所有磁盘。



10. 重新启动MSSQL服务器服务。



11. 确保SQL资源重新联机。



对于NFS、请使用mount命令连接卷并更新`/etc/fstab`条目。

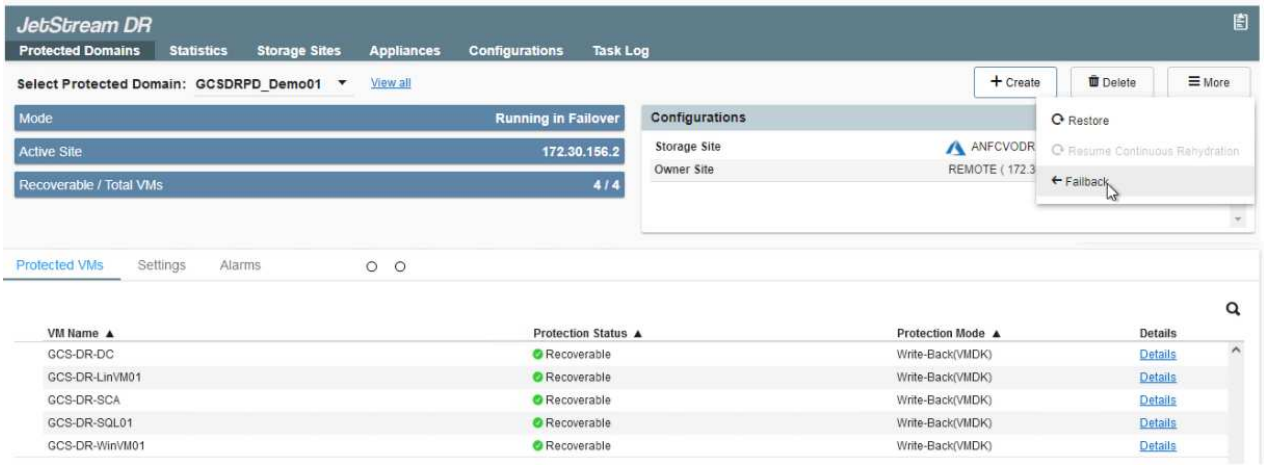
此时、可以正常运行运营并继续正常运营。

在NSX-T端、可以创建一个单独的专用第1层网关来模拟故障转移场景。这样可以确保所有工作负载可以相互通信、但任何流量都不能路由到环境或从环境中路由出来、这样、执行任何鉴别、控制或强化任务都不会面临交叉感染的风险。此操作不在本文档的讨论范围内、但在模拟隔离时可以轻松完成。

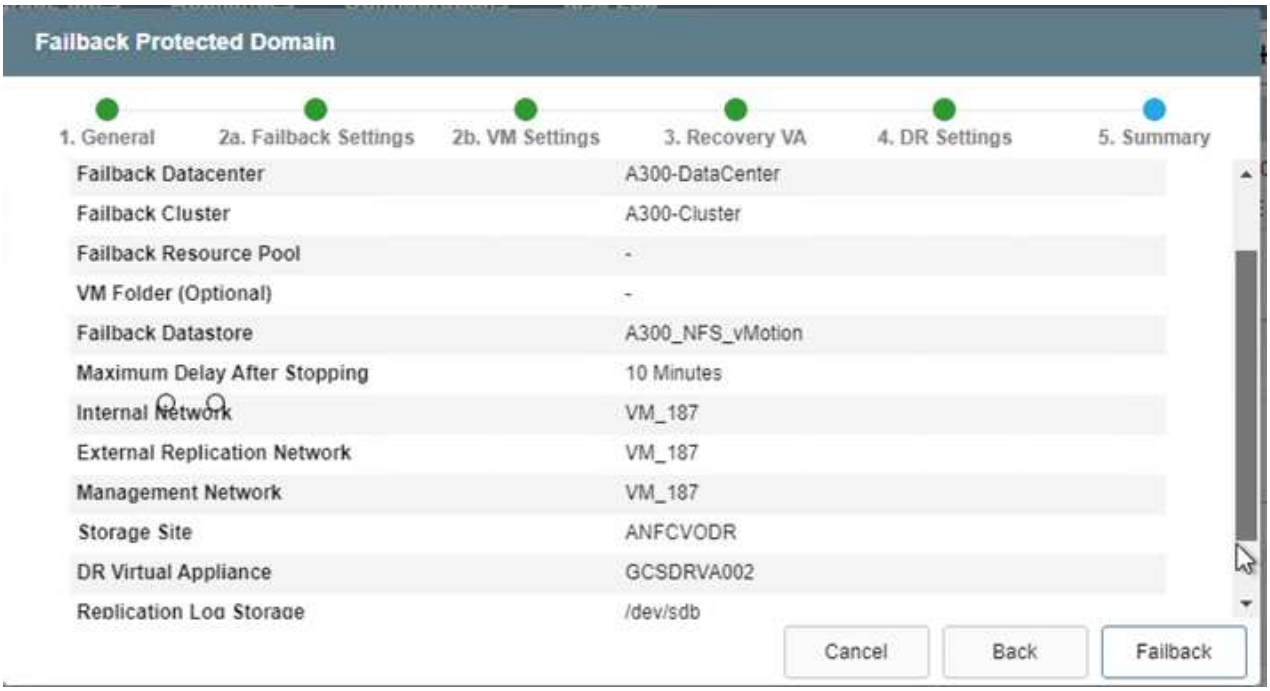
主站点启动并重新运行后、您可以执行故障恢复。Jetstream将恢复VM保护、并且必须反转SnapMirror关系。

1. 还原内部环境。根据灾难意外事件的类型、可能需要还原和/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. 访问已还原的内部环境、转到Jetstream DR UI、然后选择相应的受保护域。受保护站点准备好进行故障恢复后、在UI中选择故障恢复选项。

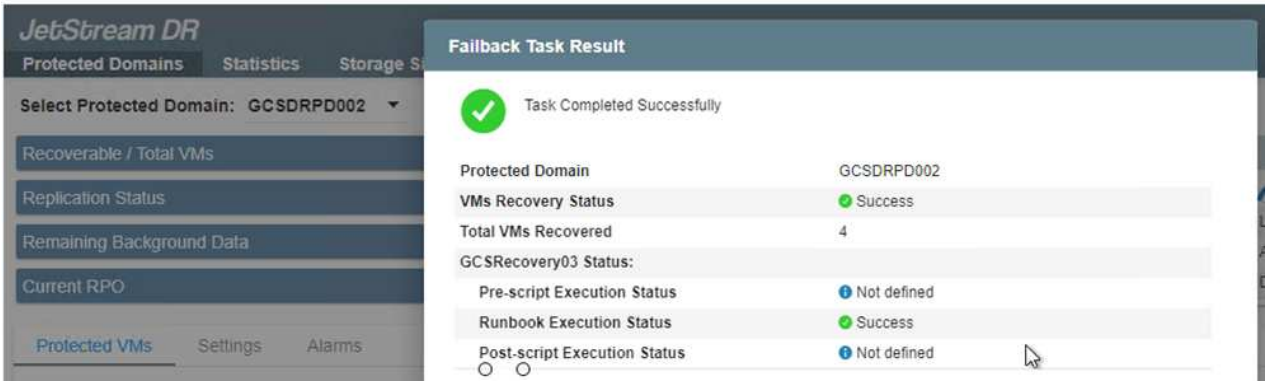
CPT生成的故障恢复计划还可用于启动VM及其数据从对象存储返回到原始VMware环境的操作。



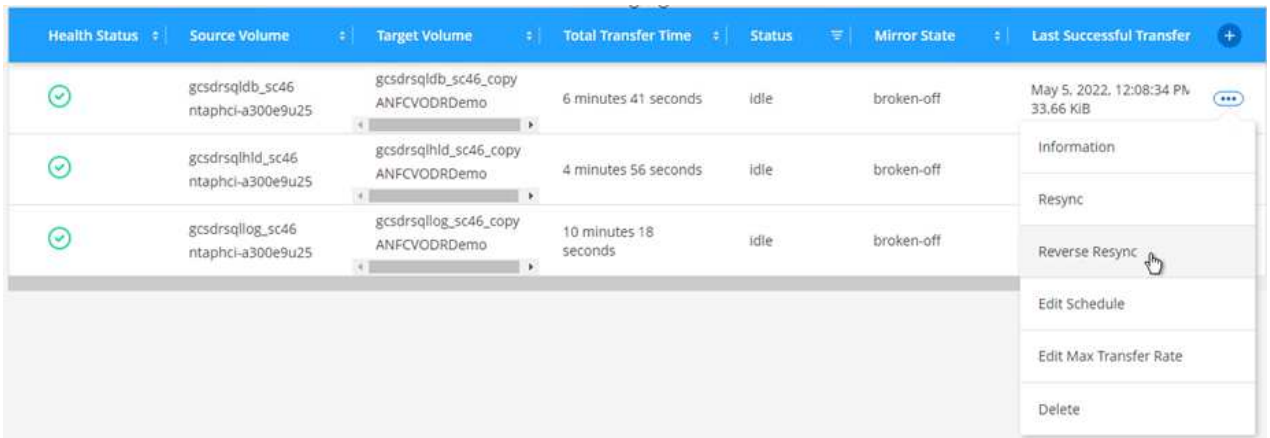
指定暂停恢复站点中的VM并在受保护站点中重新启动VM后的最大延迟。完成此过程所需的时间包括：停止故障转移VM后完成复制、清理恢复站点所需的时间以及在受保护站点中重新创建VM所需的时间。NetApp建议10分钟。

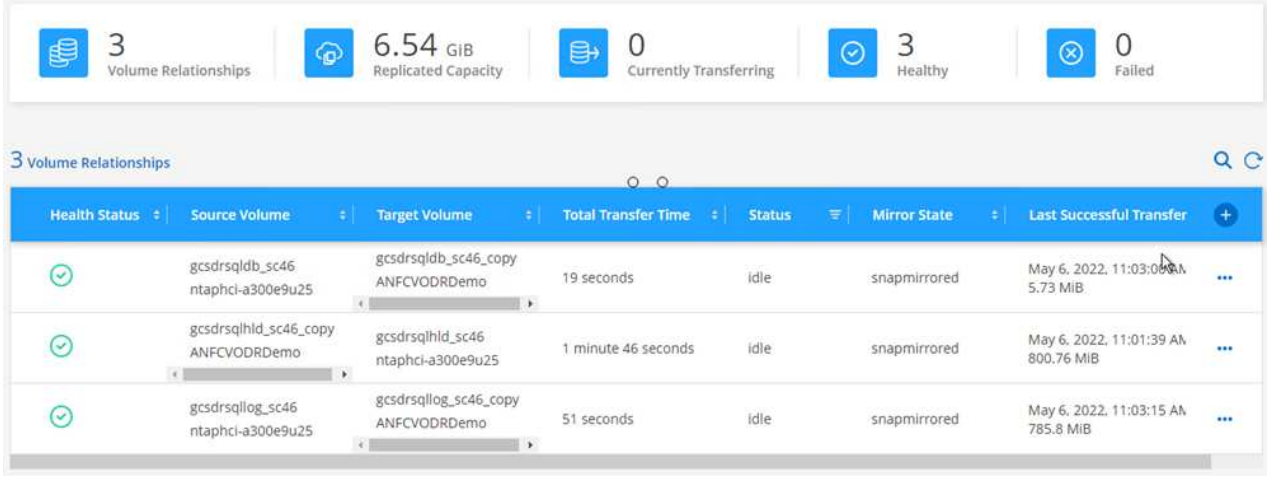


3. 完成故障恢复过程、然后确认虚拟机保护恢复和数据一致性。

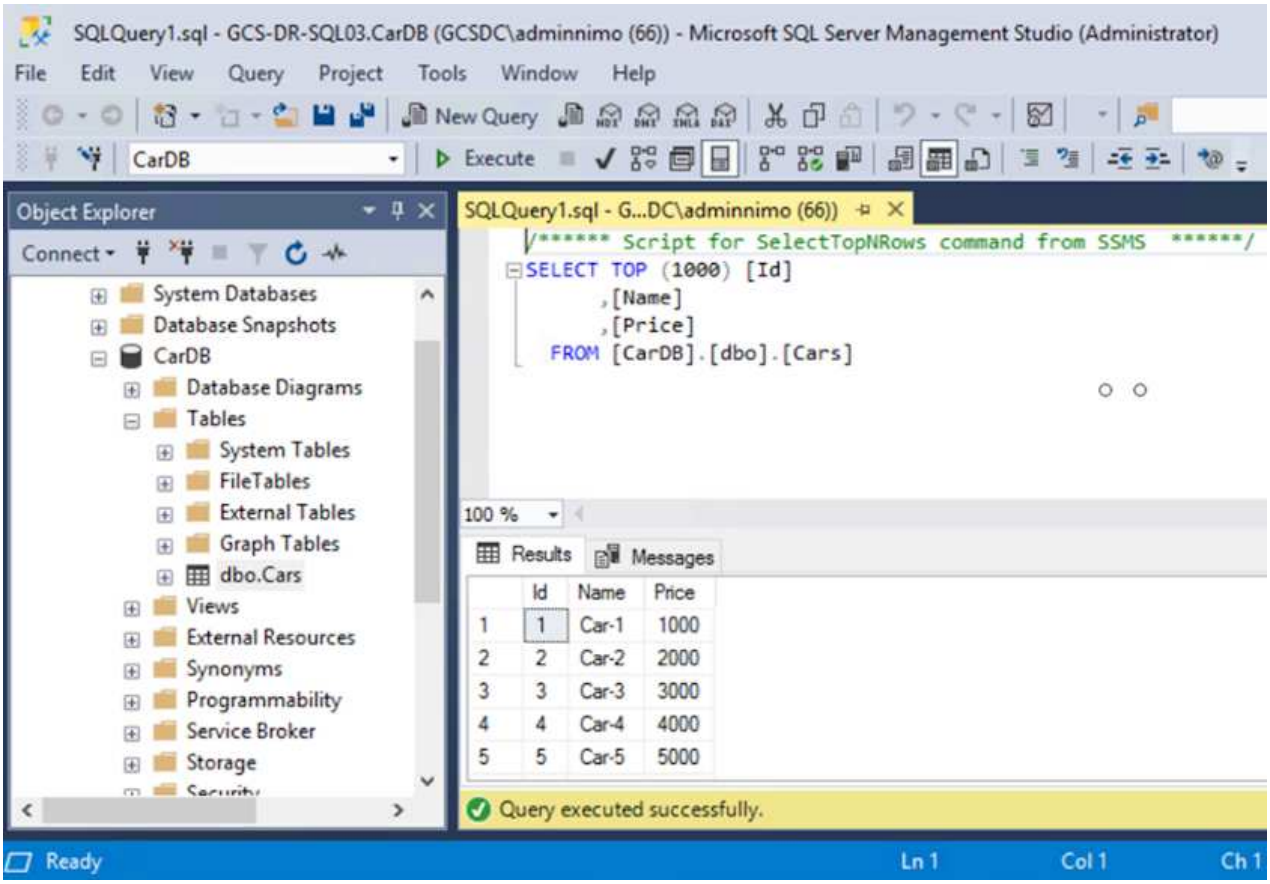


4. 恢复VM后、断开二级存储与主机的连接并连接到主存储。





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、请执行反向重新同步操作、以确保关系方向与故障转移前的关系方向保持一致。

要在执行反向重新同步操作后保留主存储和二级存储的角色、请再次执行反向重新同步操作。

此过程适用于Oracle等其他应用程序、类似的数据库模式以及使用来宾连接存储的任何其他应用程序。

在将关键工作负载迁移到生产环境之前、请始终测试恢复这些工作负载所涉及的步骤。

此解决方案 的优势

- 使用高效且具有故障恢复能力的SnapMirror复制。
- 使用ONTAP 快照保留功能恢复到任何可用时间点。
- 从存储、计算、网络和应用程序验证步骤中恢复成百上千个VM所需的所有步骤均可实现完全自动化。
- SnapCenter 使用的克隆机制不会更改复制的卷。
  - 这样可以避免卷和快照的数据损坏风险。
  - 在灾难恢复测试工作流期间避免复制中断。
  - 将灾难恢复数据用于灾难恢复以外的工作流、例如开发/测试、安全测试、修补和升级测试以及修复测试。
- CPU和RAM优化可通过恢复到较小的计算集群来帮助降低云成本。

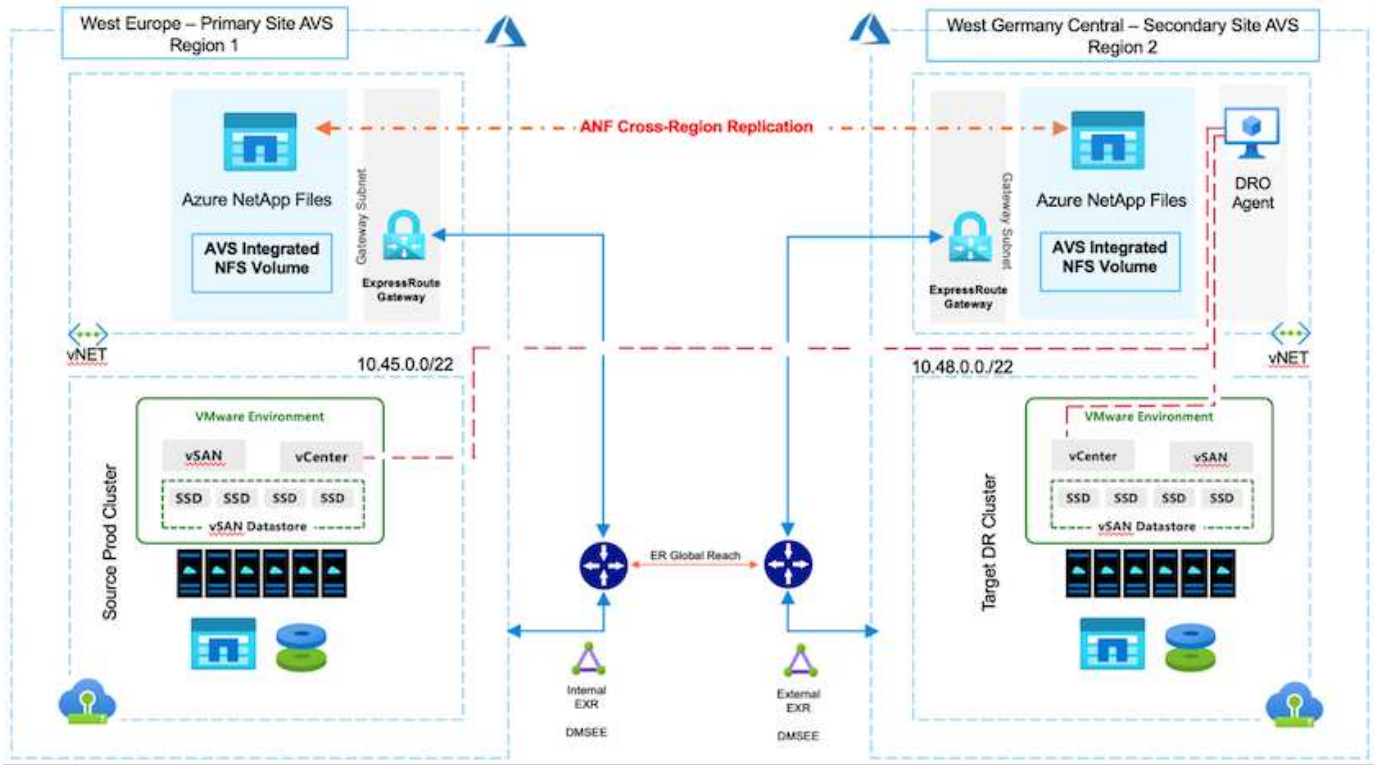
TR-4955：《使用**Azure NetApp Files (ANF)**和**Azure VMware**解决方案 **(AVS)**进行灾难恢复》

作者：Niyaz Mohamed、NetApp解决方案工程部

概述

在云中的各个区域之间使用块级复制进行灾难恢复、是一种具有故障恢复能力且经济高效的方法、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。通过Azure NetApp Files (ANF)跨区域卷复制、可以将在Azure VMware解决方案 (AVS) SDDC站点上使用Azure NetApp Files 卷作为主AVS站点上的NFS数据存储库运行的VMware工作负载复制到目标恢复区域中的指定二级AVS站点。

灾难恢复编排程序(Disaster Recovery Orchestrator、DRO)(一种具有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可通过中断复制对等关系、然后将目标卷挂载为数据存储库、通过向AVS注册VM、直接在NSX-T (包括在所有AVS私有云中)上映射网络来自动恢复。



前提条件和一般建议

- 通过创建复制对等来验证是否已启用跨区域复制。请参见 "为Azure NetApp Files 创建卷复制"。
- 您必须在源Azure VMware解决方案 私有云和目标Azure VMware私有云之间配置ExpressRoute全局范围。
- 您必须具有可访问资源的服务主体。
- 支持以下拓扑：主AVS站点到辅AVS站点。
- 配置 "复制" 根据业务需求和数据变更率为每个卷制定适当的计划。

不支持级联和扇入及扇出拓扑。

入门

部署**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公共云中提供功能全面的VMware SDDC。AVS是由Microsoft全面管理和支持并经过VMware验证的第一方解决方案 、它使用Azure基础架构。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以及用于网络连接和安全的NSX、同时充分利用Microsoft Azure的全球影响力、同类领先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邻近性。Azure VMware解决方案 SDDC与Azure NetApp Files 相结合、可提供最佳性能、同时将网络延迟降至最低。

要在Azure上配置AVS私有云、请按照中的步骤进行操作 "链接。" 适用于NetApp文档和本 "链接。" 了解Microsoft文档。 采用最低配置设置的指示灯环境可用于灾难恢复。 此设置仅包含支持关键应用程序的核心组件、并且可以横向扩展并生成更多主机、以便在发生故障转移时承担大部分负载。

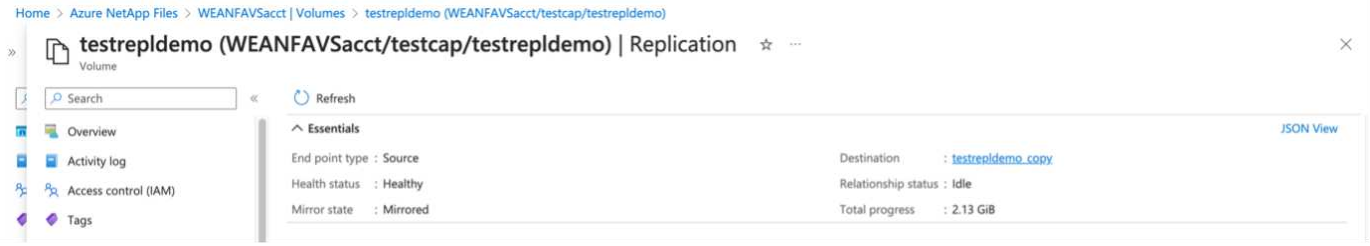
在初始版本中、DRO支持现有AVS SDDC集群。即将发布的版本将提供按需创建SDDC的功能。

配置和配置Azure NetApp Files

"Azure NetApp Files" 是一种高性能的企业级计量文件存储服务。按照中的步骤进行操作 "链接。" 配置Azure NetApp Files 并将其配置为NFS数据存储库、以优化AVS私有云部署。

为Azure NetApp Files提供支持的数据存储库卷创建卷复制

第一步是使用适当的频率和保留值为所需的数据存储库卷设置从AVS主站点到AVS二级站点的跨区域复制。



按照中的步骤进行操作 "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、对于此特定使用情形、您可以选择标准服务级别、然后选择 "修改服务级别" 发生实际灾难或灾难恢复模拟时。

跨区域复制关系是前提条件、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、并确保满足前提条件。然后安装软件包。

前提条件：

- 可以访问资源的服务主体。
- 确保与源和目标SDDC以及Azure NetApp Files 实例建立了适当的连接。
- 如果使用的是DNS名称、则应进行DNS解析。否则、请使用vCenter的IP地址。

操作系统要求：

- Ubuntu Focal 20.04 (LTS)指定的代理虚拟机上必须安装以下软件包：
- Docker
- Docker—编写
- JqChange `docker.sock` 对此新权限： `sudo chmod 666 /var/run/docker.sock`。

。 `deploy.sh` 脚本会执行所有必需的前提条件。

步骤如下：

1. 在指定虚拟机上下载安装包：

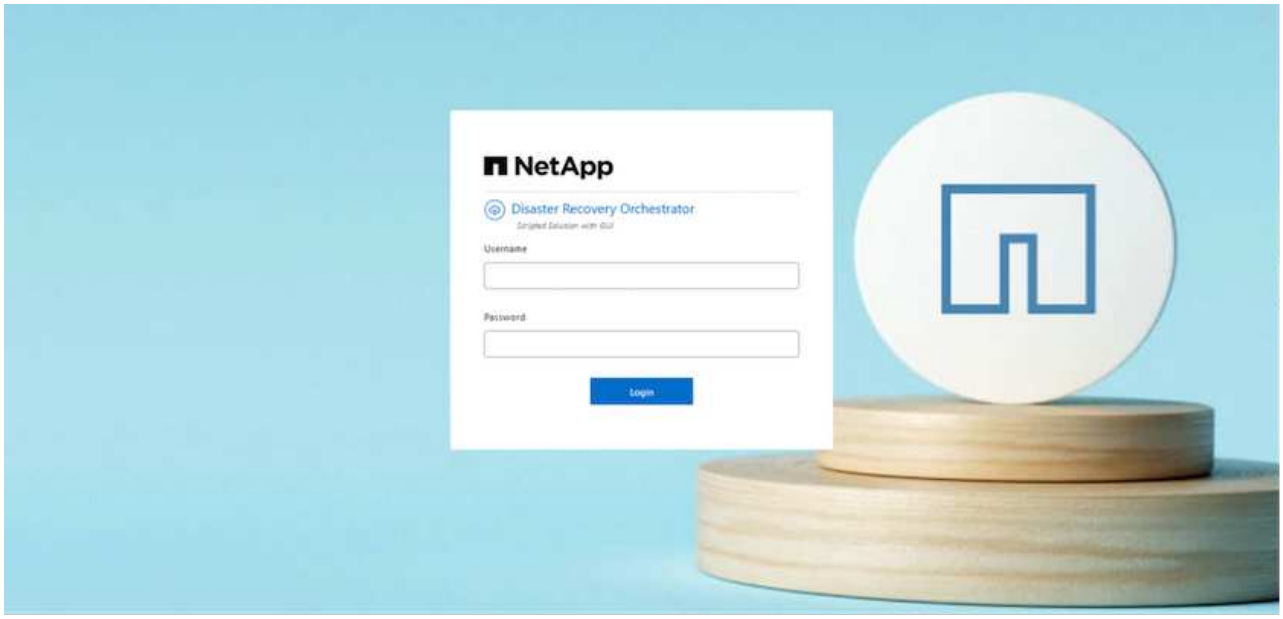
```
git clone https://github.com/NetApp/DRO-Azure.git
```

代理必须安装在二级AVS站点区域或主AVS站点区域中、其AZ不能与SDDC相同。

2. 解压缩软件包、运行部署脚本、然后输入主机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、以便自动将工作负载从主AVS站点恢复到二级AVS站点。NetApp建议在二级AVS站点中部署DRO代理并配置ExpressRoute网关连接、以便DRO代理可以通过网络与相应的AVS和Azure NetApp Files 组件进行通信。

第一步是添加凭据。DRO需要具有发现Azure NetApp Files 和Azure VMware解决方案 的权限。您可以通过创建和设置Azure Active Directory (AD)应用程序以及获取DRO所需的Azure凭据来为Azure帐户授予所需权限。您必须将服务主体绑定到Azure订阅、并为其分配具有所需相关权限的自定义角色。添加源和目标环境时、系统会提示您选择与服务主体关联的凭据。您需要先将这些凭据添加到DRO、然后才能单击添加新站点。

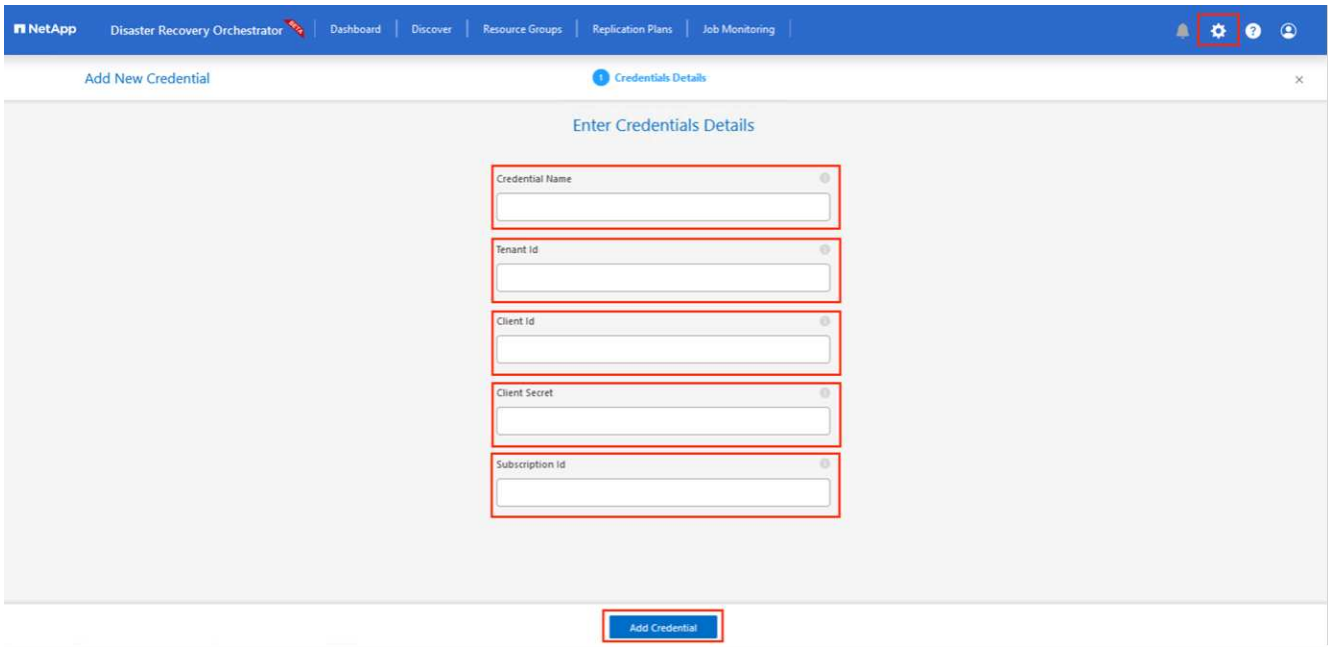
要执行此操作、请完成以下步骤：

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*Settings*图标，然后选择*凭 据*。
3. 单击Add New凭据、然后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：
   - 凭据名称
   - 租户ID
   - 客户端 ID
   - 客户端密钥
   - 订阅ID

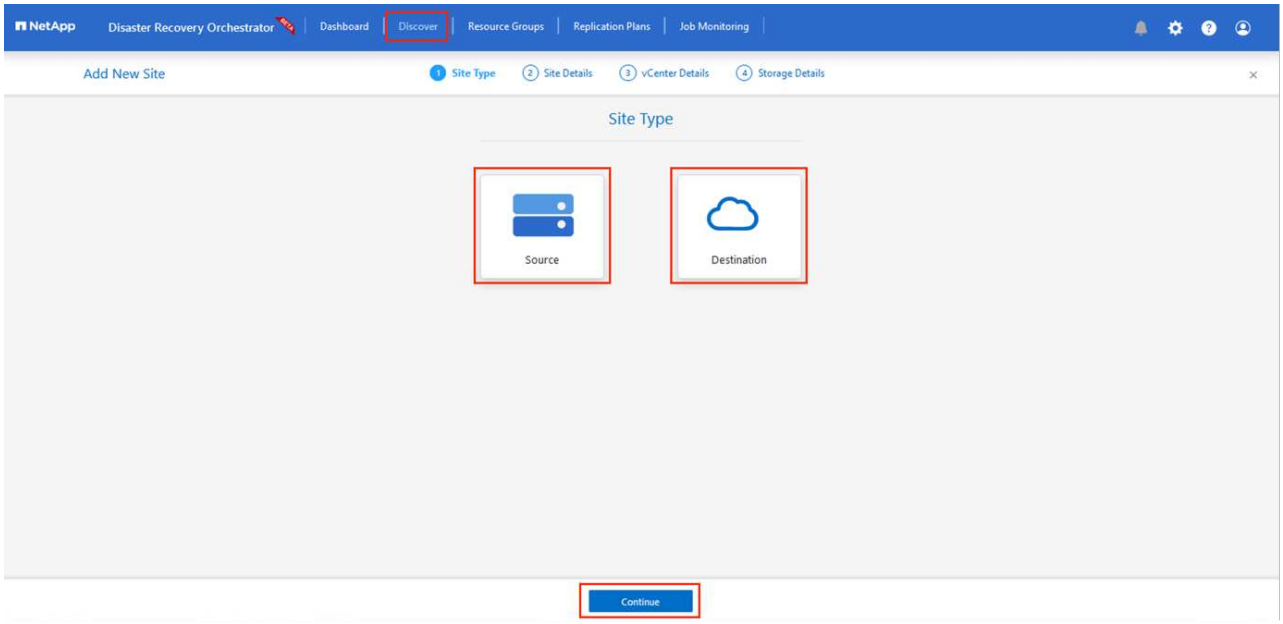
     创建AD应用程序时、您应已捕获此信息。

5. 确认有关新凭据的详细信息、然后单击添加凭据。



添加凭据后、即可发现主AVS站点和二级AVS站点(vCenter和Azure NetApp Files 存储帐户)并将其添加到DRO中。要添加源站点和目标站点、请完成以下步骤：

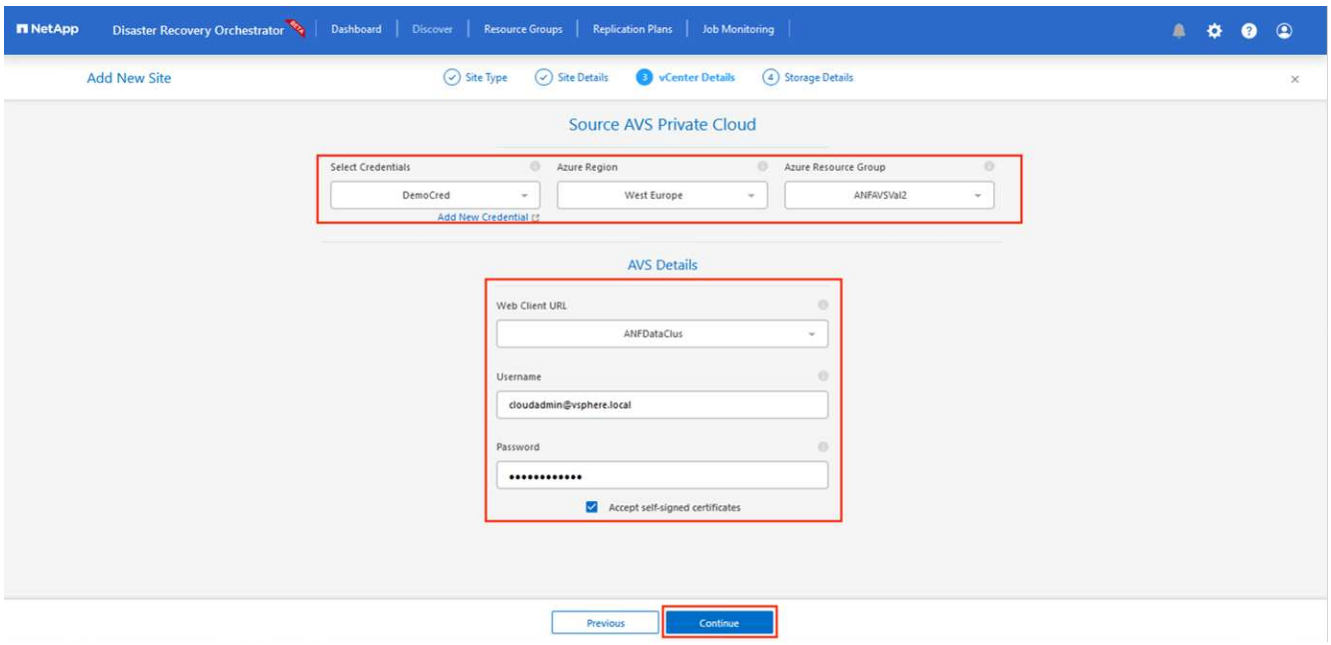
6. 转到*Discover (发现)*选项卡。
7. 单击*添加新站点*。
8. 添加以下主AVS站点(在控制台中指定为*Source*)。
   - SDDC vCenter
   - Azure NetApp Files 存储帐户
9. 添加以下二级AVS站点(在控制台中指定为*目标*)。
   - SDDC vCenter
   - Azure NetApp Files 存储帐户



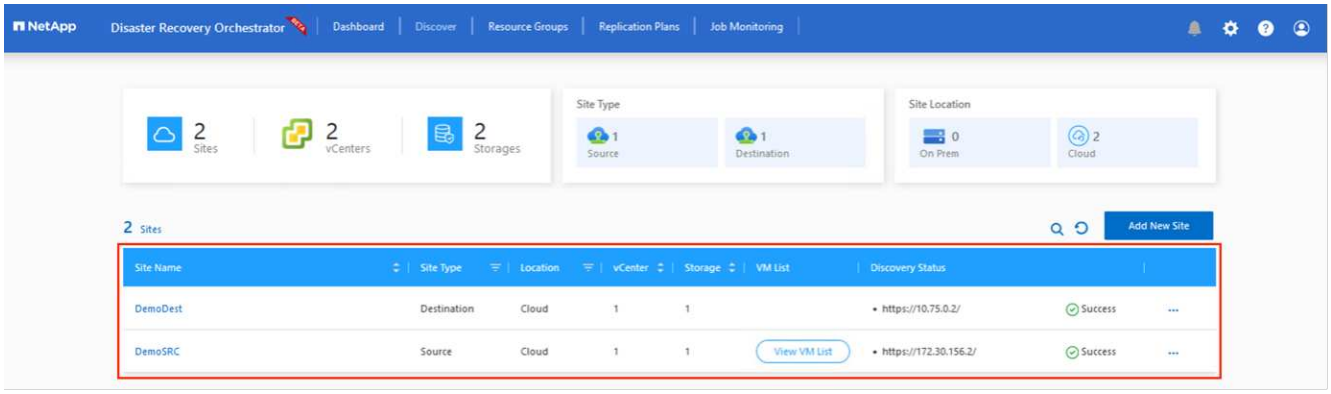
10. 通过单击*源*添加站点详细信息，输入友好的站点名称，然后选择连接器。然后单击 * 继续 * 。

> 为了便于演示、本文档将介绍如何添加源站点。

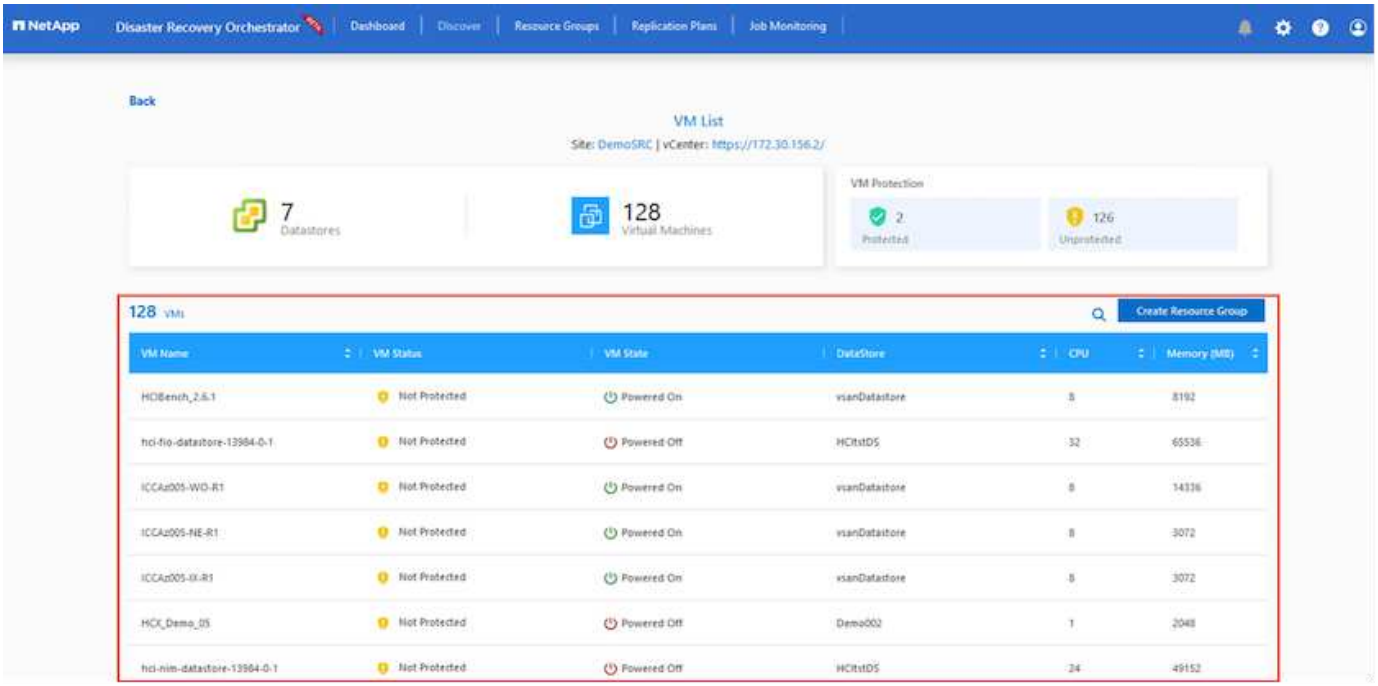
11. 更新vCenter详细信息。为此、请从主AVS SDDC的下拉列表中选择凭据、Azure区域和资源组。
12. DRO列出了该区域内的所有可用SDDC。从下拉列表中选择指定的私有云URL。
13. 输入 `cloudadmin@vsphere.local` 用户凭据。可从Azure门户访问此内容。请按照本中所述的步骤进行操作 "链接。"。完成后，单击*继续*。



14. 通过选择Azure资源组和NetApp帐户、选择源存储详细信息(ANF)。
15. 单击*创建站点*。



添加后、DRO将执行自动发现、并显示具有从源站点到目标站点的相应跨区域副本的VM。DRO会自动检测VM使用的网络和网段并将其填充。



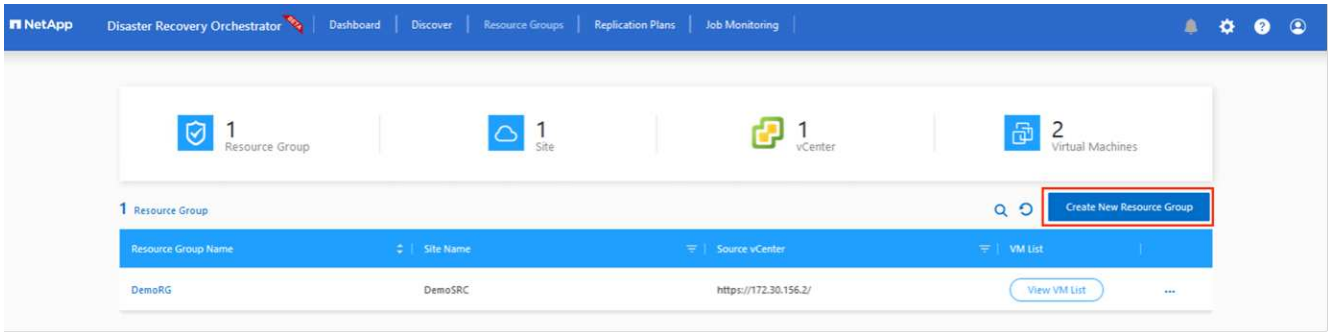
下一步是将所需的VM作为资源组分组到其功能组中。

资源分组

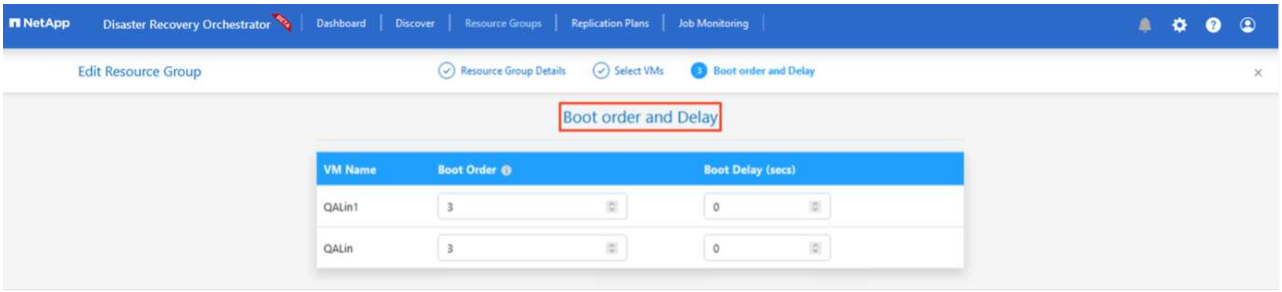
添加平台后、将要恢复的VM分组到资源组中。使用DRO资源组、您可以将一组依赖虚拟机分组到逻辑组中、这些逻辑组包含启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

要开始创建资源组，请单击*Create New Resource Group*菜单项。

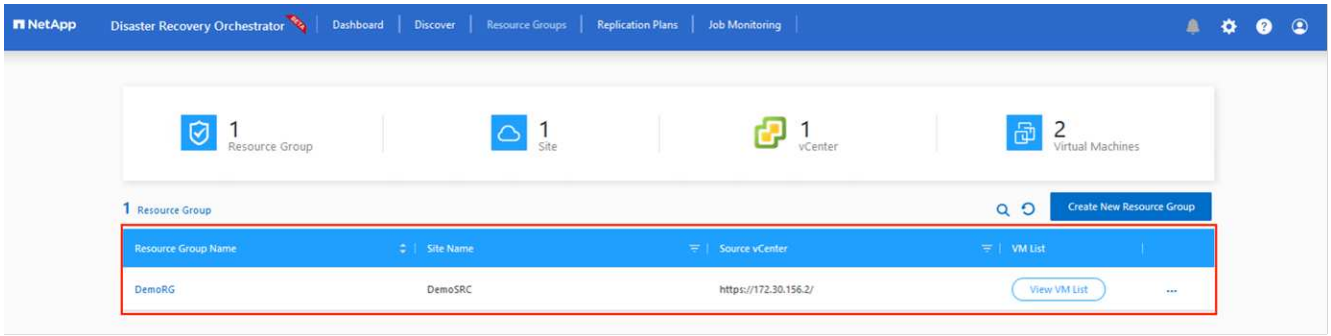
1. 访问*Resource Group*ps并单击*Create New Resource Group*。



2. 在“新建资源组”下，从下拉列表中选择源站点，然后单击*Create*。
3. 提供资源组详细信息，然后单击*Continue*。
4. 使用搜索选项选择适当的VM。
5. 为所有选定虚拟机选择*引导顺序*和*引导延迟*(秒)。通过选择每个虚拟机并设置其优先级来设置启动顺序。所有虚拟机的默认值均为3。选项如下：
   - 要启动的第一个虚拟机
   - Default
   - 要启动的最后一个虚拟机



6. 单击*创建资源组*。

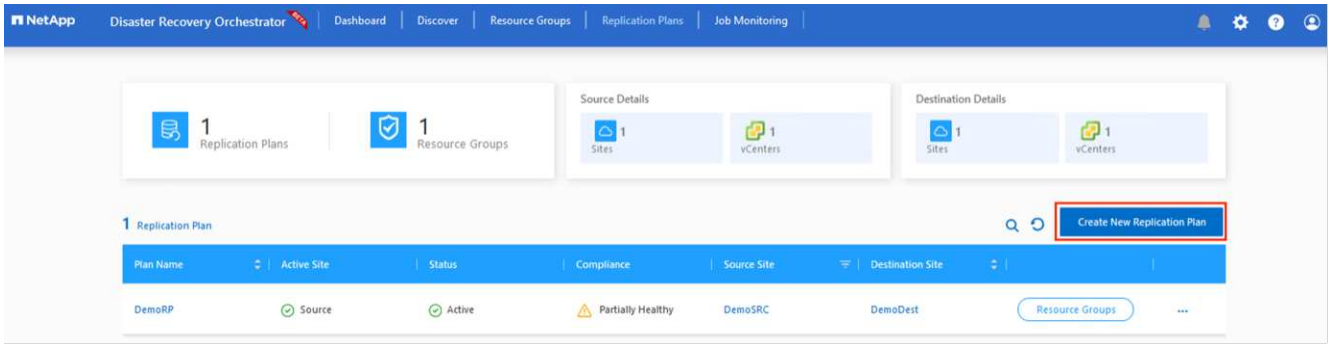


复制计划

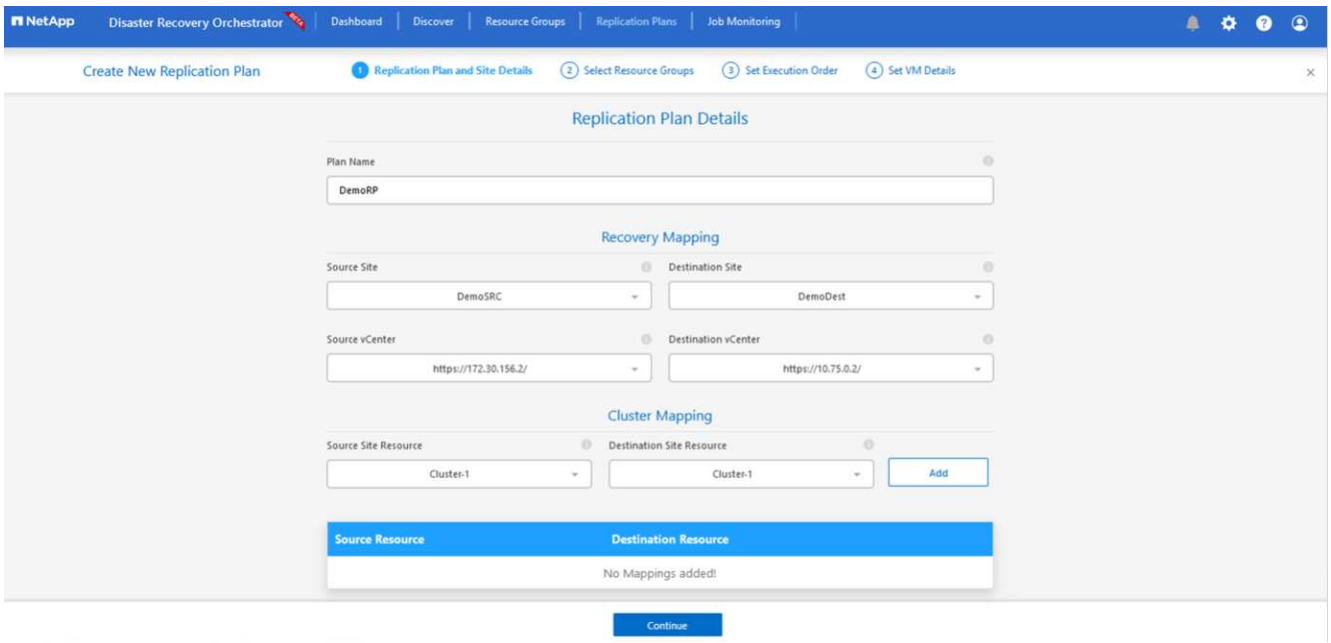
您必须制定在发生灾难时恢复应用程序的计划。从下拉列表中选择源和目标vCenter平台、选择要包含在此计划中的资源组、同时还包括应用程序应如何还原和启动的分组(例如、域控制器、第1层、第2层等)。计划通常也称为蓝图。要定义恢复计划，请导航到“复制计划”选项卡，然后单击*New Replication Plan*。

要开始创建复制计划、请完成以下步骤：

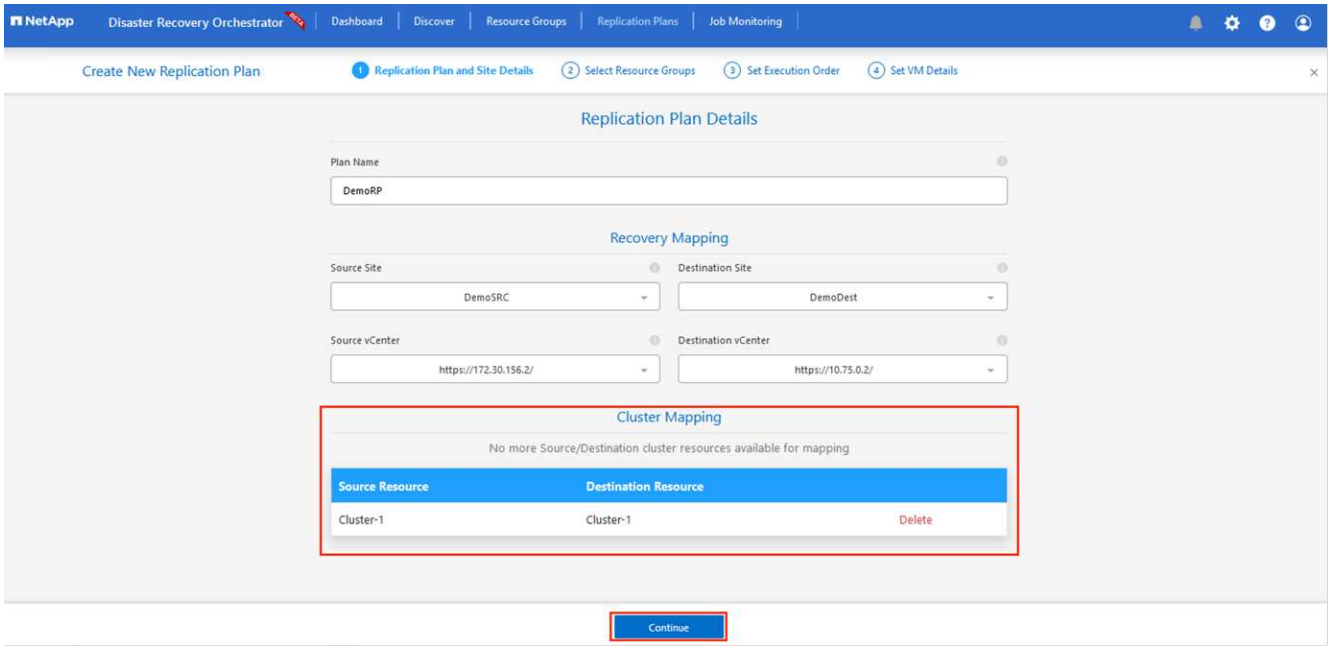
1. 导航到*复制计划*，然后单击*创建新复制计划*。



2. 在*New Replication Plan*上，为该计划提供一个名称，并通过选择源站点、关联的vCenter、目标站点和关联的vCenter来添加恢复映射。

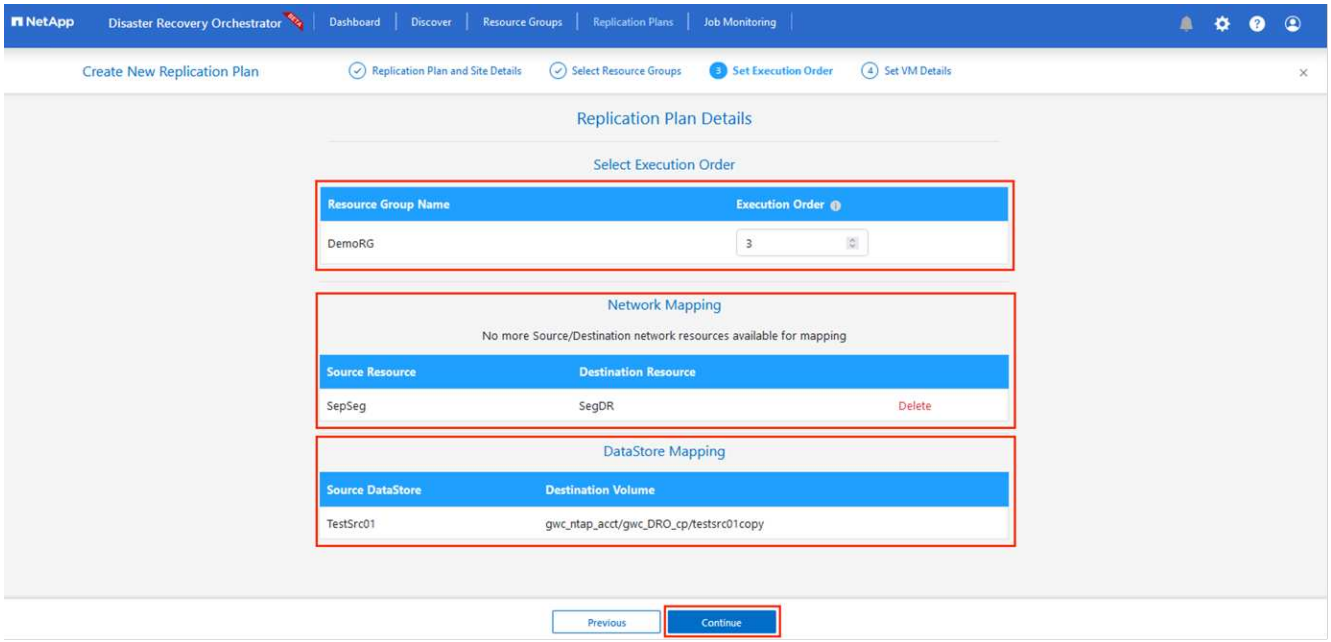


3. 恢复映射完成后，选择*Cluster Mapping*。



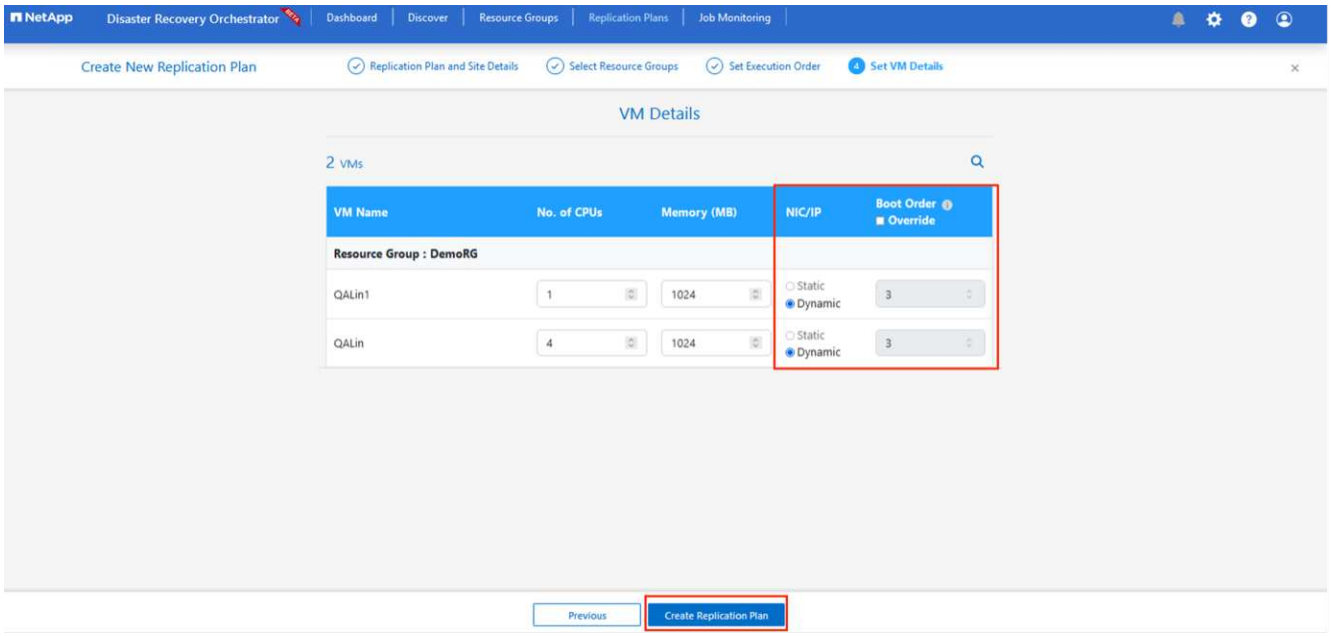
4. 选择*资源组详细信息*、然后单击*继续*。
5. 设置资源组的执行顺序。使用此选项可以选择存在多个资源组时的操作顺序。
6. 完成后、将网络映射设置为相应的网段。区块应已在二级AVS集群上配置、要将虚拟机映射到这些区块、请选择适当的区块。
7. 系统会根据所选虚拟机自动选择数据存储库映射。

跨区域复制(CRR)在卷级别进行。因此、驻留在相应卷上的所有VM都会复制到CRR目标。请确保选择属于数据存储库的所有虚拟机、因为只会处理属于复制计划的虚拟机。

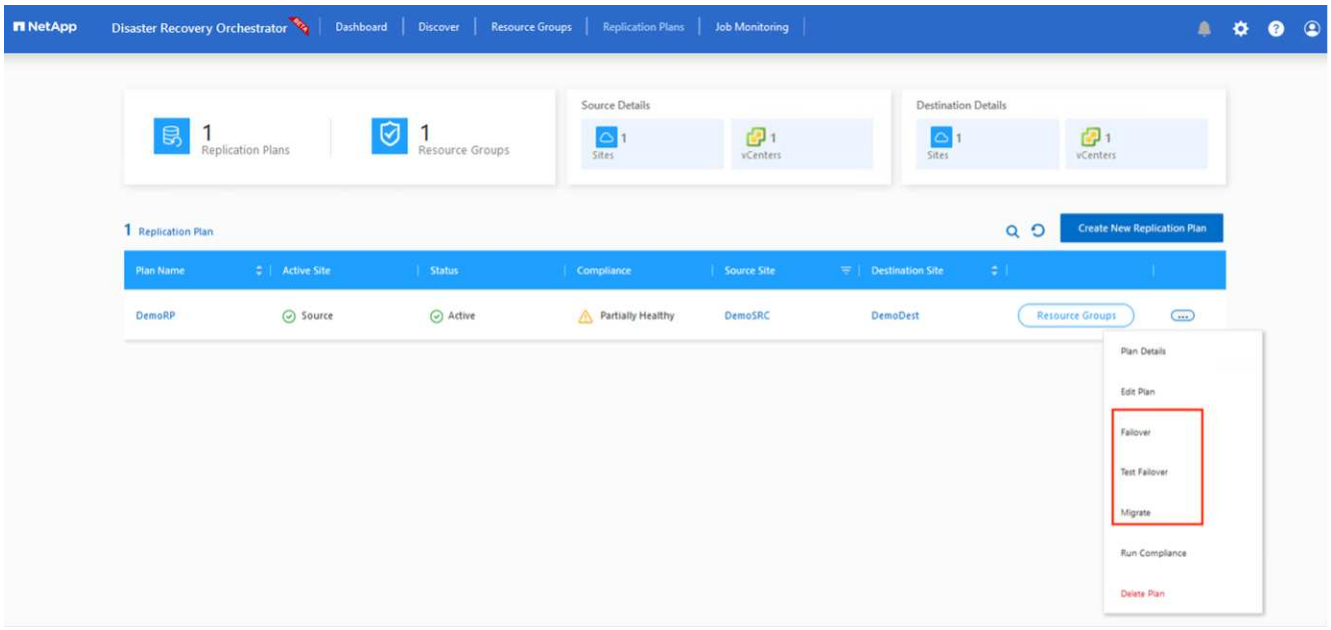


8. 在VM详细信息下、您可以选择调整VM CPU和RAM参数的大小。如果您要将大型环境恢复到较小的目标集群、或者在执行灾难恢复测试时无需配置一对一物理VMware基础架构、则此功能非常有用。此外、还可以修改资源组中所有选定VM的启动顺序和启动延迟(秒)。如果需要对您在资源组引导顺序选择期间选择的内容

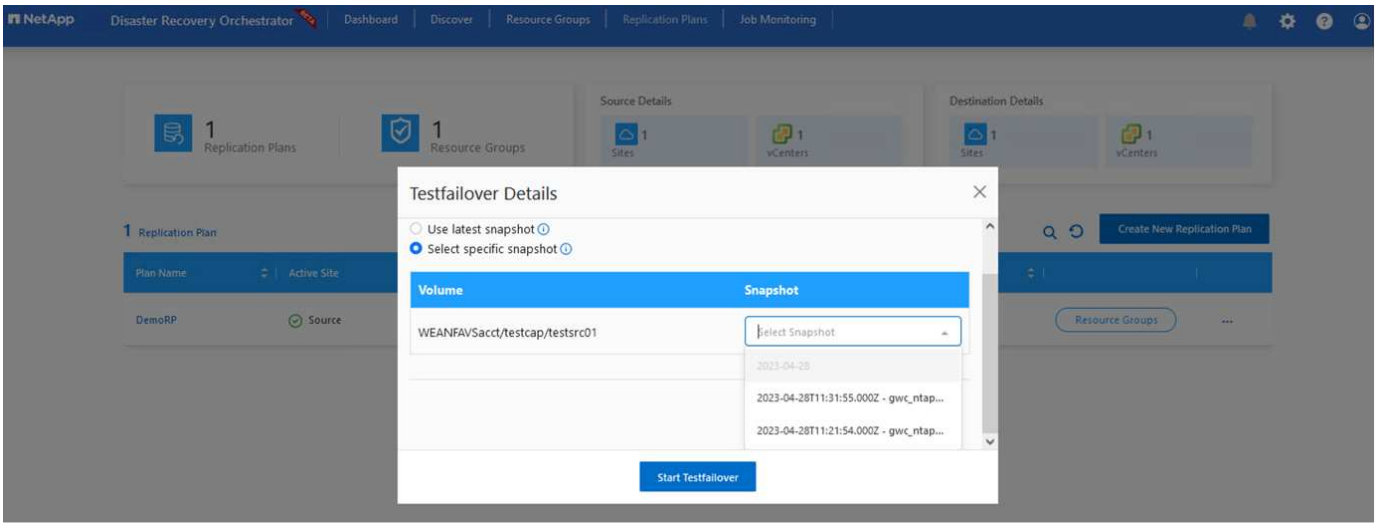
进行任何更改，则还可以使用一个附加选项来修改引导顺序。默认情况下、系统会使用在资源组选择期间选择的引导顺序、但在此阶段可以执行任何修改。



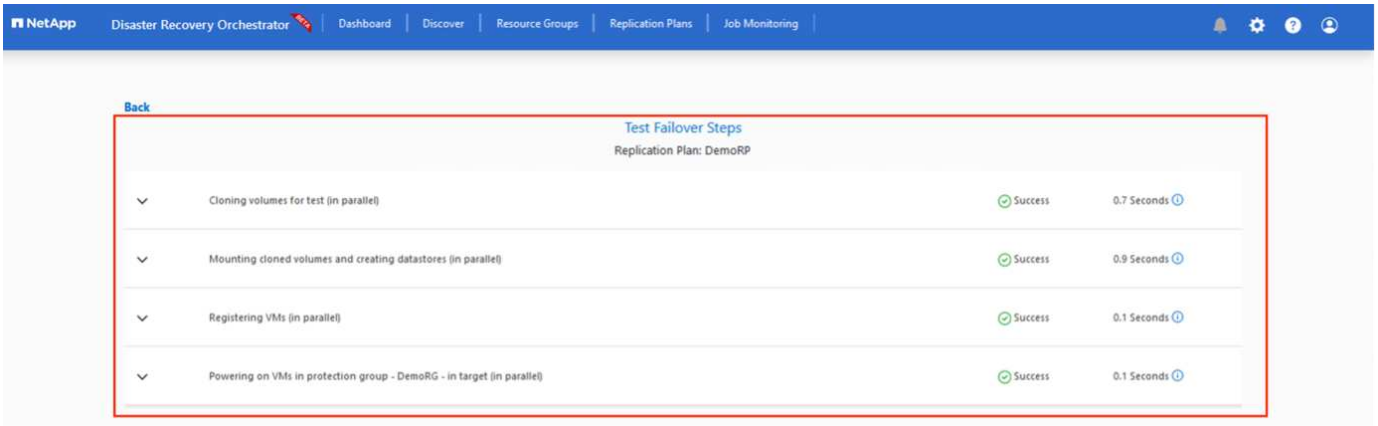
9. 单击*创建复制计划*。创建复制计划后，您可以根据需要执行故障转移、测试故障转移或迁移选项。



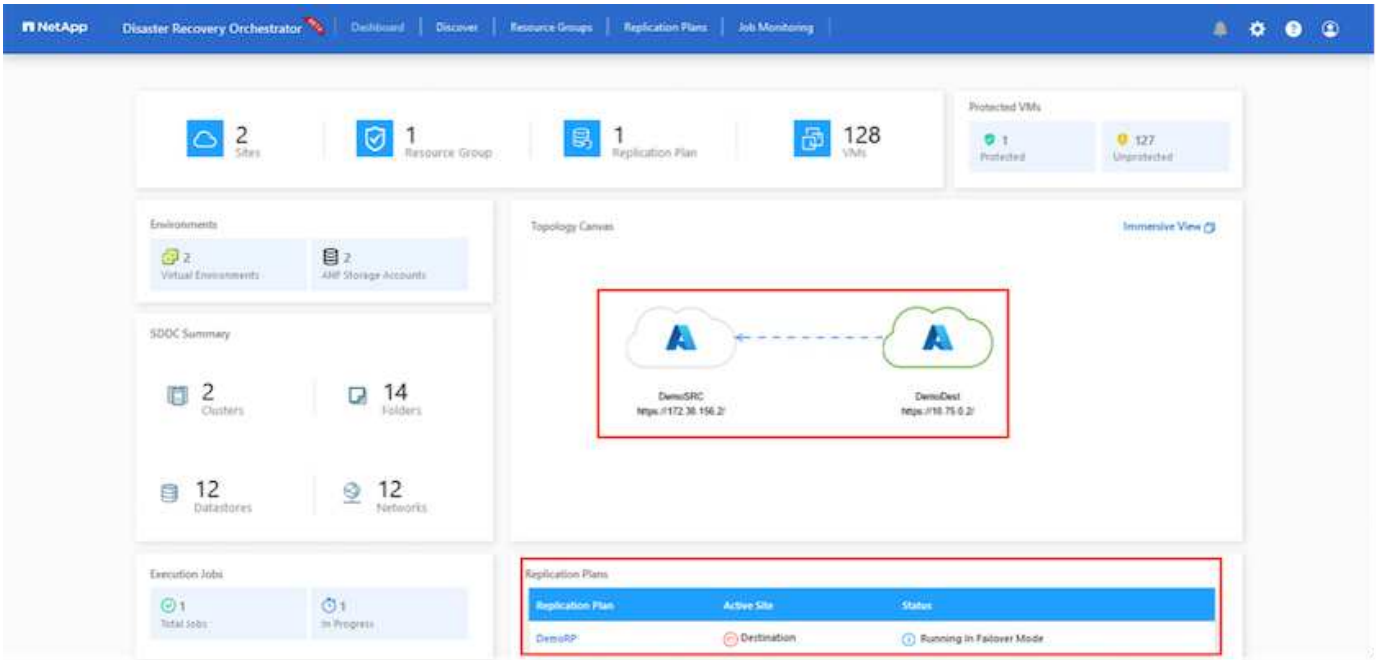
在故障转移和测试故障转移选项期间、将使用最新的快照、或者可以从时间点快照中选择特定快照。如果您正面临勒索软件等损坏事件、其中最新副本已被泄露或加密、则时间点选项非常有用。DRO显示所有可用的时间点。



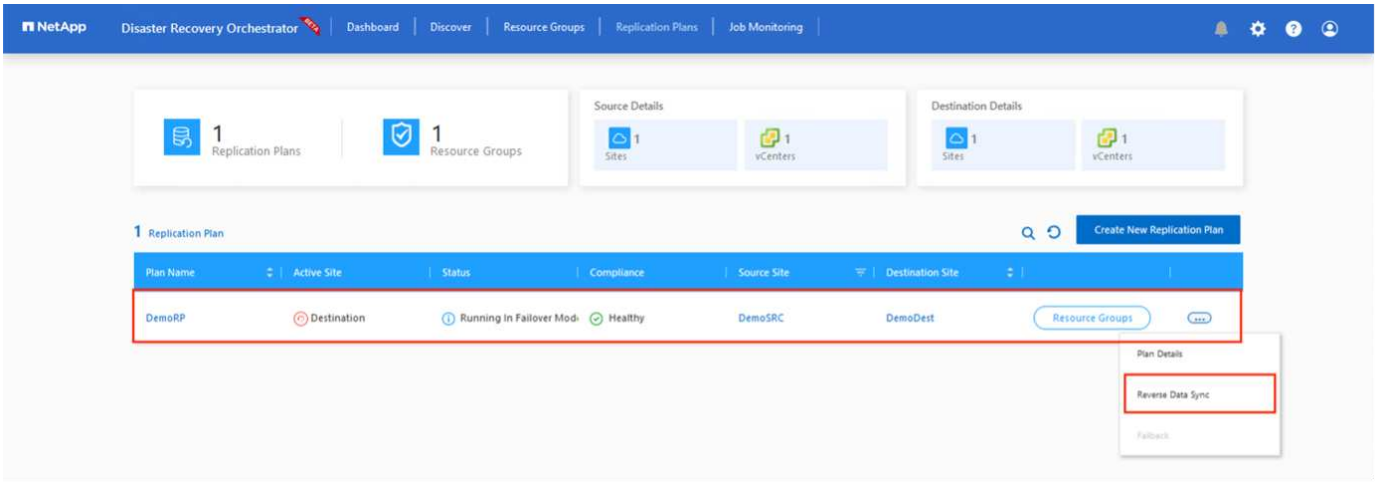
要使用复制计划中指定的配置触发故障转移或测试故障转移，可以单击*Failover或*Test Failover。您可以在任务菜单中监控复制计划。



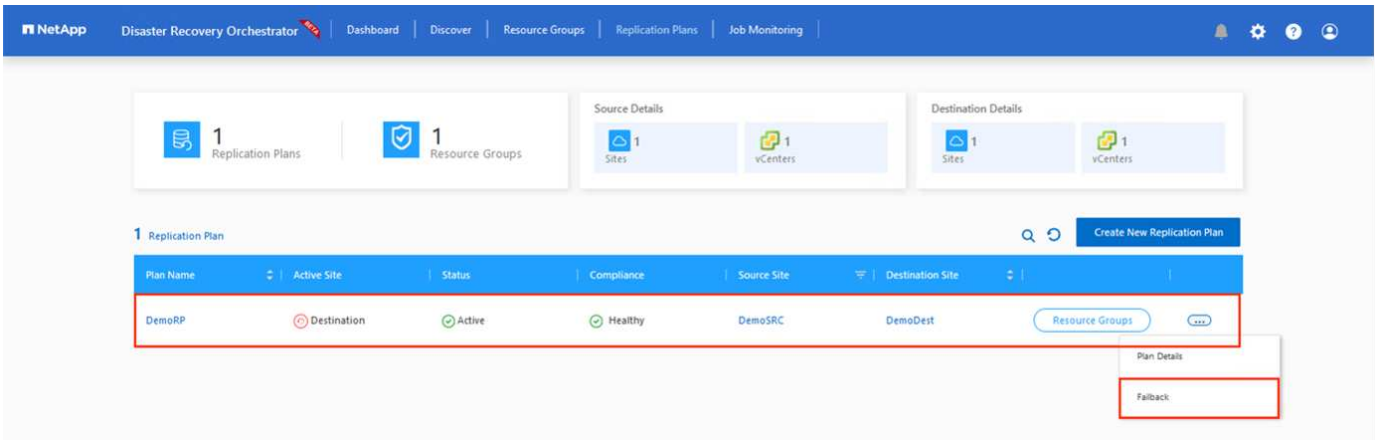
触发故障转移后、可以在二级站点AVS SDDC vCenter (VM、网络和数据存储库)中看到恢复的项目。默认情况下、VM会恢复到工作负载文件夹。

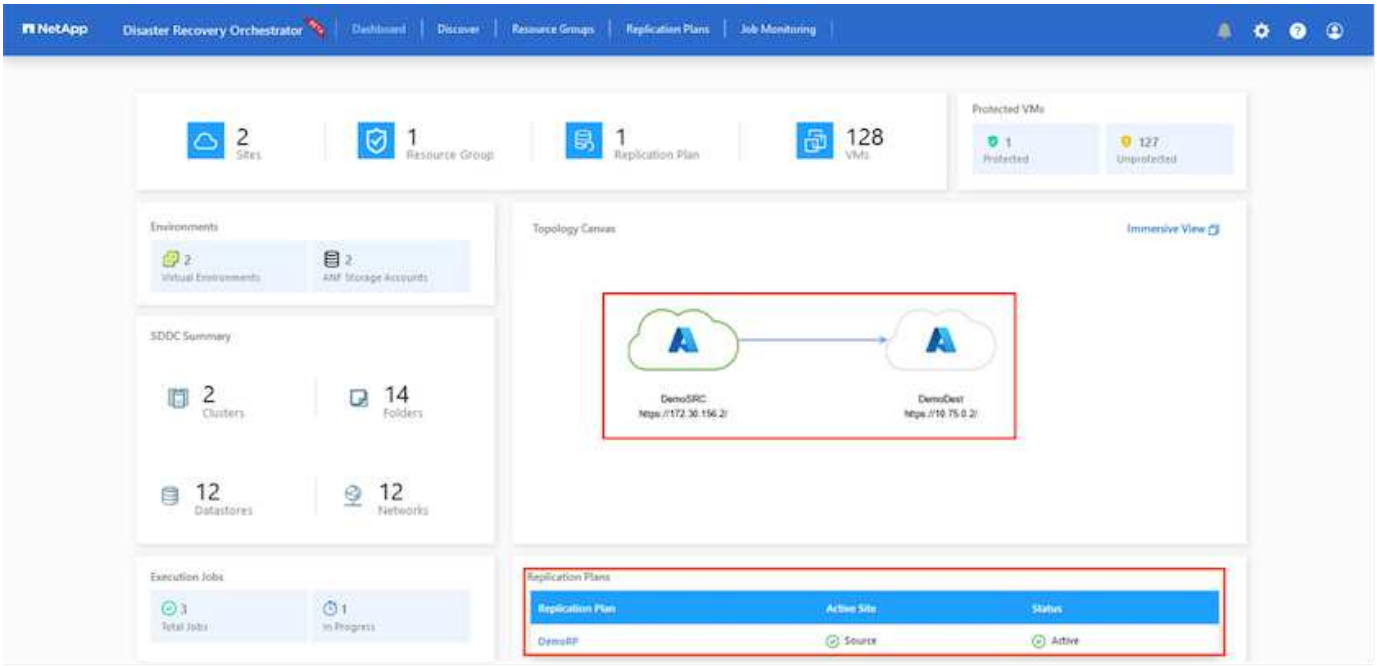


可以在复制计划级别触发故障恢复。如果发生测试故障转移、可使用拆卸选项回滚更改并删除新创建的卷。与故障转移相关的故障恢复过程分为两步。选择复制计划并选择*反向数据同步*。



完成此步骤后、触发故障恢复以移回主AVS站点。





从Azure门户中、我们可以看到、已将作为读/写卷映射到二级站点AVS SDDC的相应卷的复制运行状况已断开。在测试故障转移期间、DRO不会映射目标卷或副本卷。相反、它会为所需的跨区域复制快照创建一个新卷、并将该卷公开为数据存储库、这样会占用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、复制作业可以在灾难恢复测试或鉴别工作流期间继续运行。此外、此过程还可确保在发生错误或恢复损坏的数据时、可以清除恢复、而不会造成副本被销毁的风险。

勒索软件恢复

从勒索软件中恢复可能是一项艰巨的任务。具体而言、IT组织可能难以确定安全返回点、以及在确定安全返回点后、如何确保恢复的工作负载不会再次受到攻击(例如、恶意软件休眠或通过易受攻击的应用程序)。

DRO允许组织从任何可用时间点进行恢复、从而解决了这些问题。然后、工作负载将恢复到正常运行但又孤立的网络、以便应用程序可以正常运行并相互通信、但不会受到任何南北流量的影响。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。

结论

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。
- 通过保留快照恢复到任何可用时间点。
- 完全自动执行所有必要步骤、以便从存储、计算、网络和应用程序验证步骤中恢复成百上千个VM。
- 工作负载恢复利用"从最新快照创建新卷"过程、但不会处理复制的卷。
- 避免卷或快照上的任何数据损坏风险。
- 在灾难恢复测试工作流期间避免复制中断。
- 将灾难恢复数据和云计算资源用于灾难恢复之外的工作流、例如开发/测试、安全测试、修补和升级测试以及修复测试。
- CPU和RAM优化支持恢复到较小的计算集群、有助于降低云成本。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- 为Azure NetApp Files 创建卷复制

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- 跨区域复制Azure NetApp Files 卷

  "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**复制和**Azure NetApp Files**数据存储库将灾难恢复到**Azure VMware**解决方案

作者：Niyaz Mohamed - NetApp解决方案工程部

概述

Azure NetApp Files (ANF)数据存储库可将存储与计算分离、并为任何组织提供将其工作负载迁移到云所需的灵活性。它为客户提供了灵活的高性能存储基础架构、可独立于计算资源进行扩展。Azure NetApp Files数据存储库可简化并优化Azure VMware解决方案(AVS)作为内部VMware环境灾难恢复站点的部署。

可以使用基于Azure NetApp Files (ANF)卷的NFS数据存储库通过任何经过验证的第三方解决方案从内部复制数据、从而提供VM复制功能。通过添加Azure NetApp Files数据存储库、与构建具有大量ESXi主机来容纳存储的Azure VMware解决方案SDDC相比、它可以实现成本优化部署。这种方法称为“导向灯组”。试点轻型集群是一种最低的AVS主机配置(3个AVS节点)以及Azure NetApp Files数据存储库容量。

其目标是维护一个具有所有核心组件的低成本基础架构、以处理故障转移。如果确实发生故障转移、试点轻型集群可以横向扩展并配置更多AVS主机。一旦完成故障转移并恢复正常操作、试点指示灯集群就可以向下扩展到低成本的操作模式。

本文档的目的

本文介绍如何将Azure NetApp Files数据存储库与Veeam备份和复制结合使用、以便使用Veeam VM复制软件功能为内部VMware VM设置灾难恢复(AVS)。

Veeam Backup & Replication是一款适用于虚拟环境的备份和复制应用程序。在复制虚拟机时、Veeam Backup & Replication会从AVS上进行复制、该软件将在目标AVS SDDC集群上以本机VMware vSphere格式创建VM的精确副本。 Veeam Backup & Replication将使副本与原始虚拟机保持同步。复制可提供最佳恢复时间目标(Recovery Time客观、Recovery Time目标、Recovery Time目标、Recovery Time目标、Recovery Time目

标、Recovery Time目标)、因为灾难恢复站点上已挂载VM副本、并且处于随时可启动的状态。

此复制机制可确保在发生灾难事件时、工作负载可以在AVS SDDC中快速启动。Veeam Backup & Replication软件还可以优化流量传输、以便通过WAN和慢速连接进行复制。此外、它还会筛选出重复的数据块、零数据块、交换文件和"排除的VM子操作系统文件"。软件还将压缩副本流量。为了防止复制作业占用整个网络带宽、可以使用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、则可以通过故障转移到VM副本来触发故障转移以恢复VM。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正常的还原点。这样便可根据需要进行勒索软件恢复或隔离测试。Veeam Backup & Replication提供了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内部环境中运行。
2. "部署Azure VMware解决方案(AVS)" 私有云和 "连接Azure NetApp Files数据存储库" Azure VMware解决方案主机。

   采用最低配置设置的指示灯环境可用于灾难恢复。发生意外事件时、VM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. 灾难事件完成且主站点启动后、切换回生产VM。

Veeam VM复制到**AVS**和**ANF**数据存储库的前提条件

1. 确保Veeam Backup & Replication备份VM已连接到源和目标AVS SDDC集群。
2. 备份服务器必须能够解析短名称并连接到源和目标vCenter。
3. 目标Azure NetApp Files数据存储库必须具有足够的可用空间来存储已复制VM的VMDK。

对于追加信息、请参阅介绍的"注意事项和限制" "此处"。

部署详细信息

第**1**步：复制**VM**

Veeam Backup & Replication利用VMware vSphere快照功能/在复制期间、Veeam Backup & Replication会请求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使用快照作为复制数据源。

要复制VM、请执行以下步骤：

1. 打开Veeam Backup & Replication Console。
2. 在主页视图中。右键单击作业节点、然后选择复制作业>虚拟机。
3. 指定作业名称并选中相应的高级控制复选框。单击下一步。
   - 如果内部和Azure之间的连接带宽受限、请选中"副本传播"复选框。
     *如果Azure VMware解决方案SDDC上的分段与内部站点网络不匹配、请选中"网络重新映射(适用于具有不同网络的AVS SDDC站点)"复选框。
   - 如果内部生产站点中的IP地址方案与目标AVS站点中的方案不同、请选中"副 本重新IP (适用于IP地址方案不同的灾难恢复站点)"复选框。

     []
4. 在*Virtual* Machines*步骤中，选择要复制到连接到Azure VMware解决方案SDDC的Azure NetApp Files数据存储库的VM。可以将虚拟机放置在vSAN上、以填满可用的vSAN数据存储库容量。在指示灯集群中、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数据存储库中、以便恢复VM、并可扩展集群以满足CPU/内存要求。单击*Add*，然后在*Add Object*窗口中选择所需的VM或VM容器，然后单击*Add*。单击 * 下一步 * 。

   []
5. 之后、选择目标作为Azure VMware解决方案SDDC集群/主机、并为VM副本选择相应的资源池、VM文件夹和FSx for ONTAP数据存储库。然后单击 * 下一步 * 。

   []
6. 在下一步中、根据需要创建源虚拟网络与目标虚拟网络之间的映射。

   []
7. 在*作业设置*步骤中，指定要存储VM副本元数据、保留策略等的备份存储库。
8. 在“数据传输”步骤中更新*Source*和*Target*代理服务器，保留“自动*选择”**(**默认**)**并保持“*直接”选项处于选中状态，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. 选择复制计划以定期运行复制作业。

    []
11. 在向导的*摘要*步骤中，查看复制作业的详细信息。要在关闭向导后立即启动作业，请选中*单击完成时运行作业*复选框，否则不要选中该复选框。然后单击*完成*关闭向导。

[]

复制作业启动后、目标AVS SDDC集群/主机上将填充具有指定后缀的VM。

[]

有关追加信息for Veeam复制的信息、请参见 "复制的工作原理"

第**2**步：创建故障转移计划

初始复制或传播完成后、创建故障转移计划。故障转移计划有助于逐个或以组的形式自动对相关VM执行故障转移。故障转移计划是VM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的相关VM已在运行。

要创建计划，请导航到名为*RELIG副 本*的新子部分，然后选择*Failover Plan*。选择适当的VM。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。

只有在初始复制完成且虚拟机副本处于就绪状态时、才能添加故障转移计划。

在运行故障转移计划时、最多可同时启动10个VM

在故障转移过程中、源VM不会关闭

要创建*故障转移计划*，请执行以下操作：

1. 在主页视图中。右键单击副本节点、然后选择故障转移计划>故障转移计划> VMware vSphere。

   []

2. 接下来、提供计划的名称和问题描述。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VM之前、请运行一个脚本来关闭VM。

   []

3. 将VM添加到计划中、并修改VM启动顺序和启动延迟、以满足应用程序依赖关系。

   []

有关用于创建复制作业的追加信息、请参见 "正在创建复制作业"。

第**3**步：运行故障转移计划

在故障转移期间、生产站点中的源VM将切换到灾难恢复站点上的副本。在故障转移过程中、Veeam Backup & Replication会将VM副本还原到所需的还原点、并将所有I/O活动从源VM移至其副本。不仅可以在发生灾难时使用副本、还可以用于模拟灾难恢复演练。在模拟故障转移期间、源VM将保持运行状态。执行完所有必要的测试后、您可以撤消故障转移并恢复正常操作。

确保已建立网络分段、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。此操作将使用虚拟机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*Start to *。

[]

[]

VM副本的状态将从"准备就绪"更改为"故障转移"、VM将在目标Azure VMware解决方案(AVS) SDDC集群/主机上启动。

[]

故障转移完成后、VM的状态将更改为"故障转移"。

[]

Veeam Backup & Replication会停止源VM的所有复制活动、直到其副本恢复到就绪状态为止。

有关故障转移计划的详细信息、请参见 "故障转移计划"。

第**4**步：故障恢复到生产站点

当故障转移计划正在运行时、它会被视为一个中间步骤、需要根据需要最终确定。选项包括：

- 故障恢复到生产环境-切换回原始虚拟机并将虚拟机副本运行期间发生的所有更改传输至原始虚拟机。

> 执行故障恢复时、只会传输更改、但不会发布更改。选择*Commit failback*(确认原始虚拟机按预期工作后)或Undo failback (撤消故障恢复)以返回到虚拟机副本(如果原始虚拟机未按预期工作)。

- 撤消故障转移-切换回原始虚拟机并放弃在虚拟机副本运行期间对其所做的所有更改。
- 永久故障转移-从原始虚拟机永久切换到虚拟机副本，并将此副本用作原始虚拟机。

在此演示中、我们选择了故障恢复到生产环境。在向导的目标步骤中选择了故障恢复到原始虚拟机、并启用了"Power On VM after Restoring"(还原后启动虚拟机)复选框。

[]

[]

[]

[]

提交故障恢复是完成故障恢复操作的方法之一。提交故障恢复后、它会确认发送到故障恢复虚拟机(生产虚拟机)的更改是否按预期工作。完成提交操作后、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、请参见的Veeam文档 "故障转移和故障恢复以进行复制"。

[]

成功故障恢复到生产环境后、所有VM都会还原回原始生产站点。

[]

结论

借助Azure NetApp Files数据存储库功能、Veeam或任何经过验证的第三方工具可以利用试点轻型集群来提供低成本的灾难恢复解决方案、而不是仅仅通过建立大型集群来容纳VM副本。这样可以高效地处理定制的自定义灾难恢复计划、并重复使用内部现有备份产品进行灾难恢复、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。如果发生灾难、可以通过单击按钮进行故障转移、如果发生灾难、则可以自动进行故障转移。

要了解有关此过程的更多信息、请随时观看详细的演练视频。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

在**AzAzure / AVS**上迁移工作负载

作者：NetApp Solutions Engineering

概述：迁移具有**VMware HCX**、**Azure NetApp Files** 数据存储库和**Azure VMware**解决方案 的虚拟机

Azure VMware解决方案 和Azure NetApp Files 数据存储库最常见的使用情形之一是迁移VMware工作负载。VMware HCX是首选选项、它提供了各种迁移机制、可将内部虚拟机(VM)及其数据移动到Azure NetApp Files 数据存储库。

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、甚至跨云实现业务连续性。它作为Azure VMware解决方案 私有云的一部分提供、可通过多种方式迁移工作负载、并可用于灾难恢复(DR)操作。

本文档提供了配置Azure NetApp Files 数据存储库以及下载、部署和配置VMware HCX的分步指导、其中包括内部部署和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、用于启用各种VM迁移机制。

VMware HCX可用于任何数据存储库类型、因为迁移是在VM级别进行的。因此、本文档适用于计划在Azure VMware解决方案 中部署Azure NetApp Files 以实现经济高效的VMware云部署的现有NetApp客户和非NetApp客户。

高级步骤

此列表概括介绍了在Azure云端安装和配置HCX Cloud Manager以及在内部安装HCX Connector所需的步骤：

1. 通过Azure门户安装HCX。
2. 在内部部署的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. 将内部部署的VMware HCX连接器与Azure VMware解决方案 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进行IP。
7. 验证设备状态并确保可以进行迁移。
8. 迁移VM工作负载。

前提条件

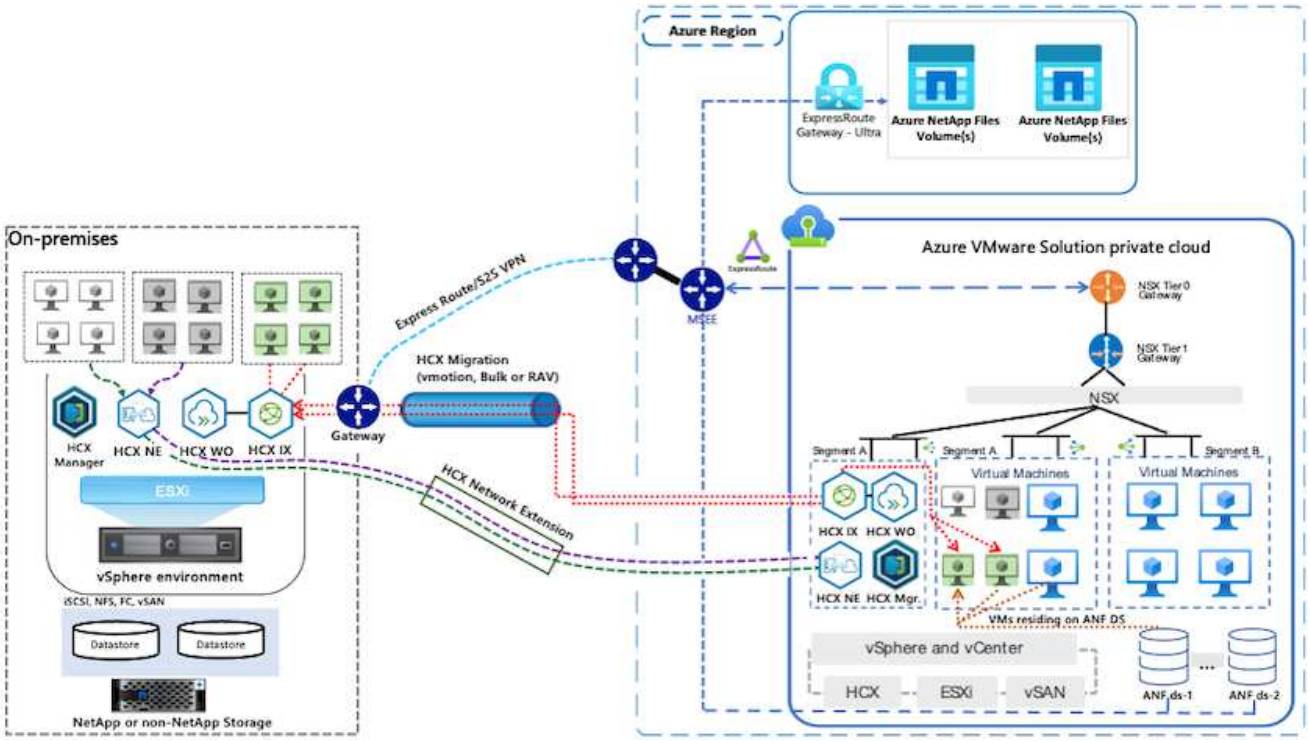
开始之前、请确保满足以下前提条件。有关详细信息，请参见此 "链接。"。在满足包括连接在内的前提条件后、通过从Azure VMware解决方案 门户生成许可证密钥来配置和激活HCX。下载OVA安装程序后、按如下所述继续安装过程。

默认选项为HCX高级版、VMware HCX Enterprise版本也可通过支持服务单获得、并且无需额外付费。

- 使用现有Azure VMware解决方案 软件定义的数据中心(SDDC)或使用此功能创建私有云 "NetApp链接" 或这一点 "Microsoft链接"。
- 从启用了VMware vSphere的内部数据中心迁移VM和关联数据需要从数据中心到SDDC环境的网络连接。迁移工作负载之前、 "设置站点到站点VPN或快速路由全局访问连接" 在内部环境和相应的私有云之间。
- 从内部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。
- 确保满足所需 "防火墙规则和端口" 允许内部vCenter Server与SDDC vCenter之间的vMotion流量。在私有云上、默认情况下会在vMotion网络上配置路由。
- Azure NetApp Files NFS卷应挂载为Azure VMware解决方案 中的数据存储库。请按照本节中详细介绍的步骤进行操作 "链接。" 将Azure NetApp Files 数据存储库连接到Azure VMware解决方案主机。

高级架构

出于测试目的、用于此验证的内部实验室环境通过站点到站点VPN进行连接、从而可以在内部连接到Azure VMware解决方案。



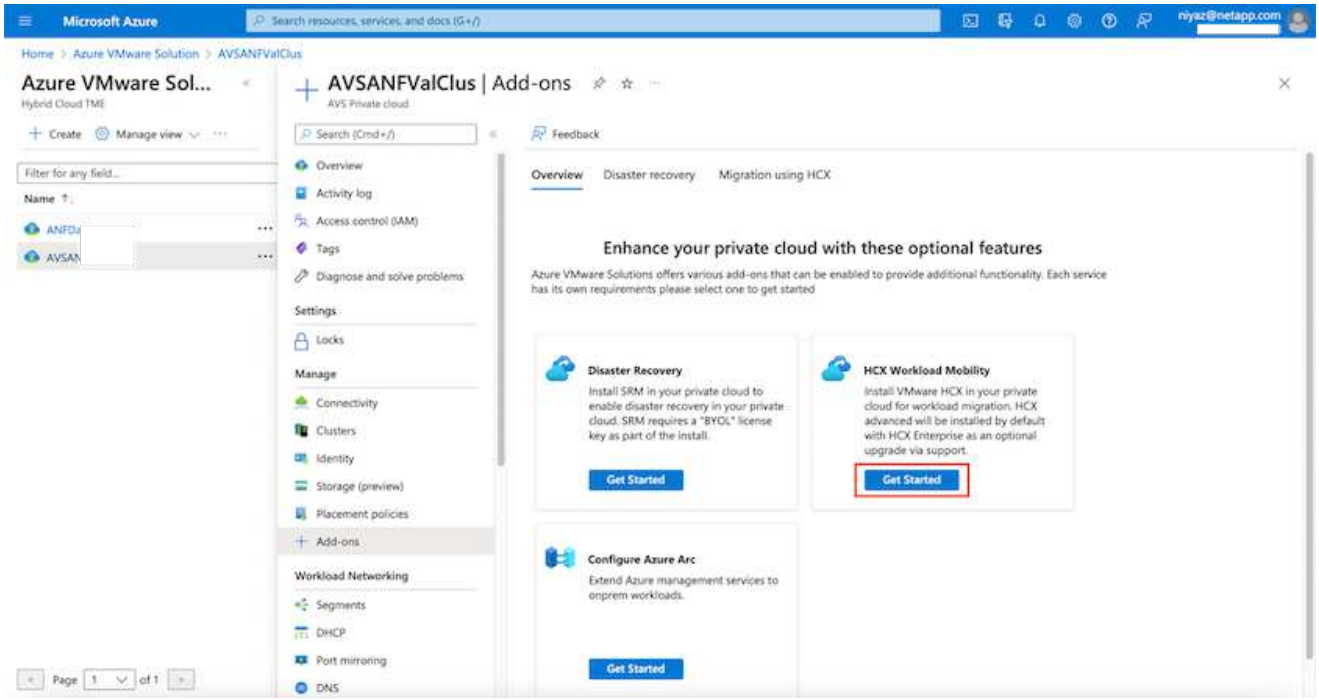
解决方案 部署

按照一系列步骤完成此解决方案 的部署：

第1步：使用加载项选项通过Azure门户安装HCX

要执行安装、请完成以下步骤：

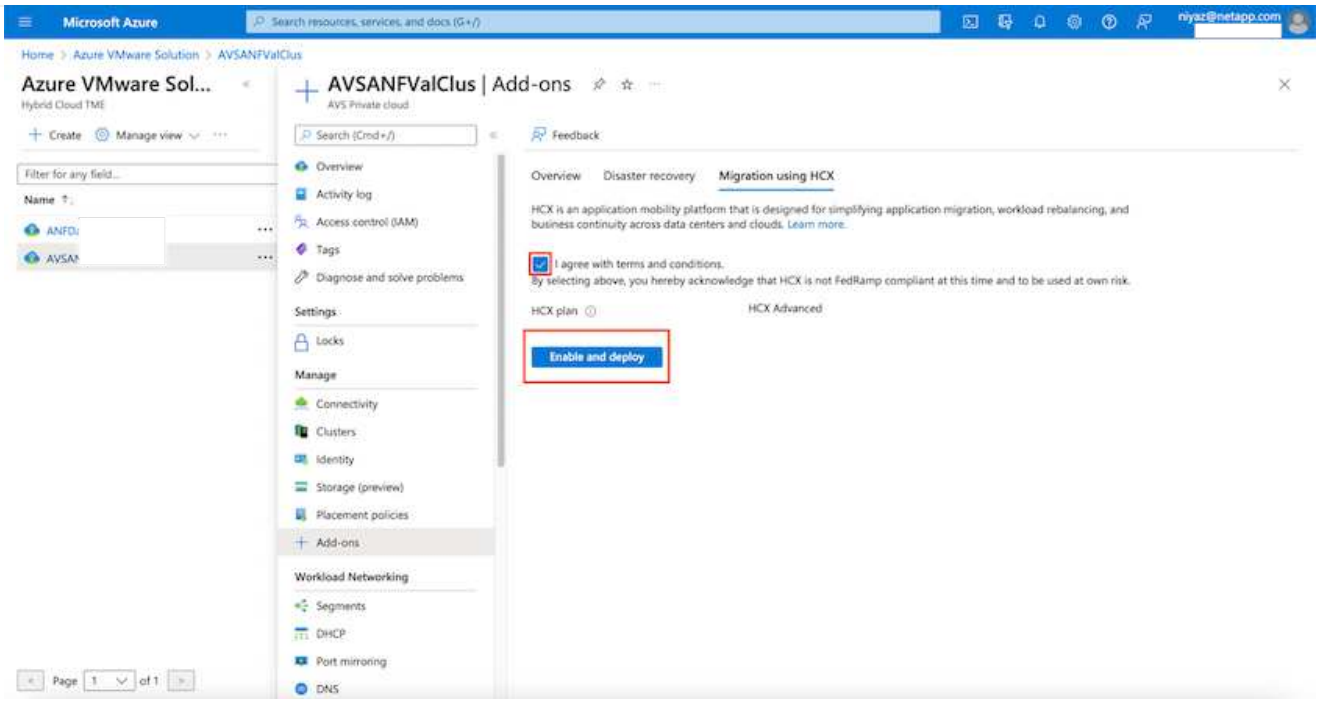
1. 登录到Azure门户并访问Azure VMware解决方案 私有云。
2. 选择适当的私有云并访问附加项。可通过导航到*管理>加载项*来完成此操作。
3. 在HCX工作负载移动性部分中、单击*开始使用*。



1. 选择*我同意条款和条件*选项、然后单击*启用并部署*。

默认部署为HCX Advanced。打开支持请求以启用Enterprise版本。

部署大约需要25到30分钟。


Microsoft Azure
Search resources, services, and docs (G+/)
niyaz@netapp.com
Home > Azure VMware Solution > AVSANFValClus
Azure VMware Sol...
Hybrid Cloud TME
Create
Manage view
Filter for any field...
Name
ANFDu
AVSAN
Page 1 of 1
AVSANFValClus | Add-ons
AVS Private cloud
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Clusters
Identity
Storage (preview)
Placement policies
Add-ons
Workload Networking
Segments
DHCP
Port mirroring
DNS
Feedback
Overview
Disaster recovery
Migration using HCX
HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. Learn more.
I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.
HCX plan
HCX Advanced
Enable and deploy

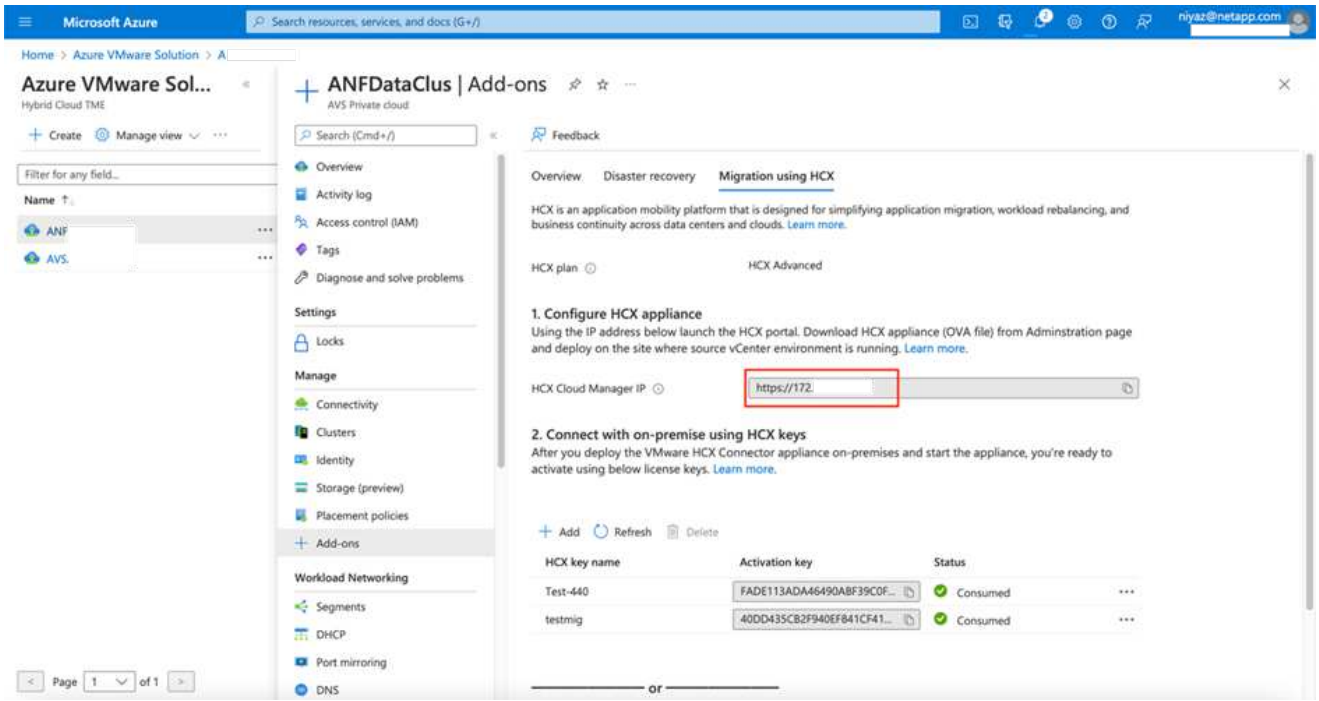
第2步：在内部vCenter Server中部署安装程序OVA

要使内部连接器连接到Azure VMware解决方案 中的HCX管理器、请确保在内部环境中打开相应的防火墙端口。

要在内部vCenter Server中下载并安装HCX Connector、请完成以下步骤：

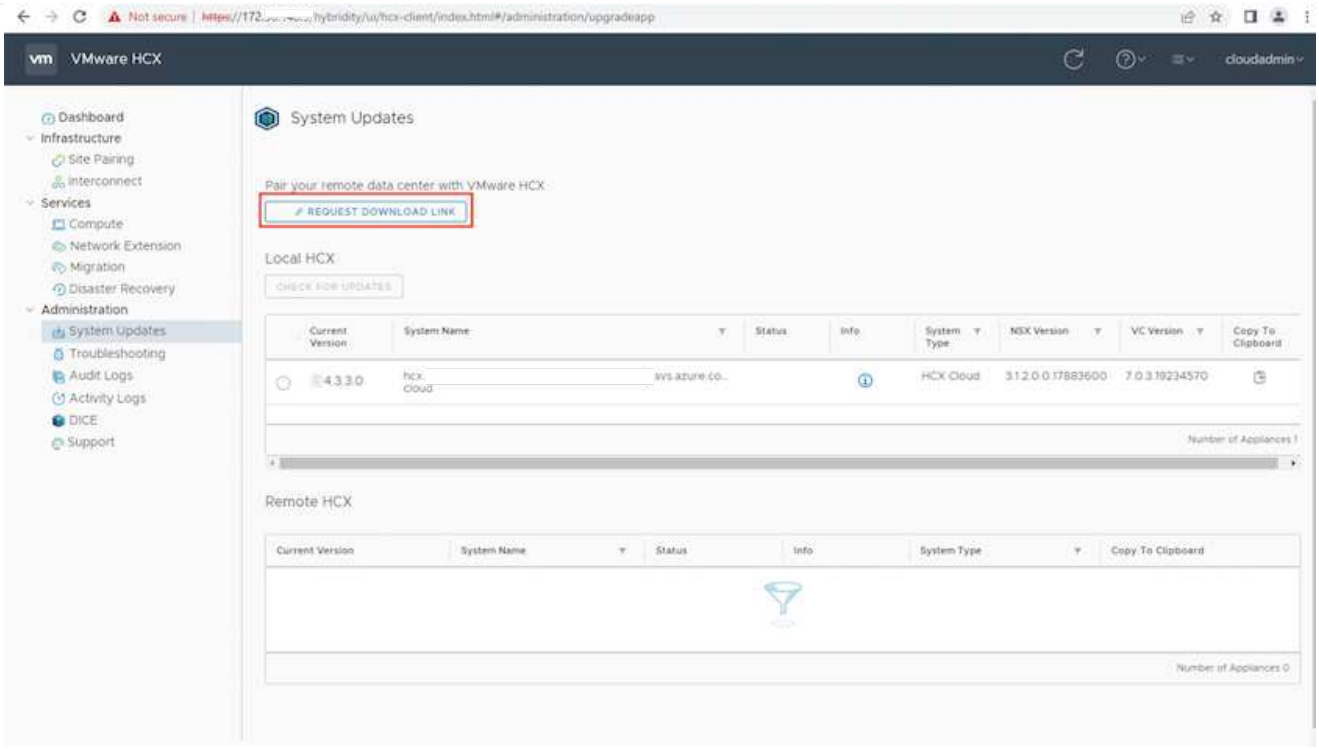
1. 从Azure门户中、转到Azure VMware解决方案 、选择私有云、然后使用HCX选择*管理>加载项>迁移*、并复制HCX Cloud Manager门户以下载OVA文件。

使用默认CloudAdmin用户凭据访问HCX门户。

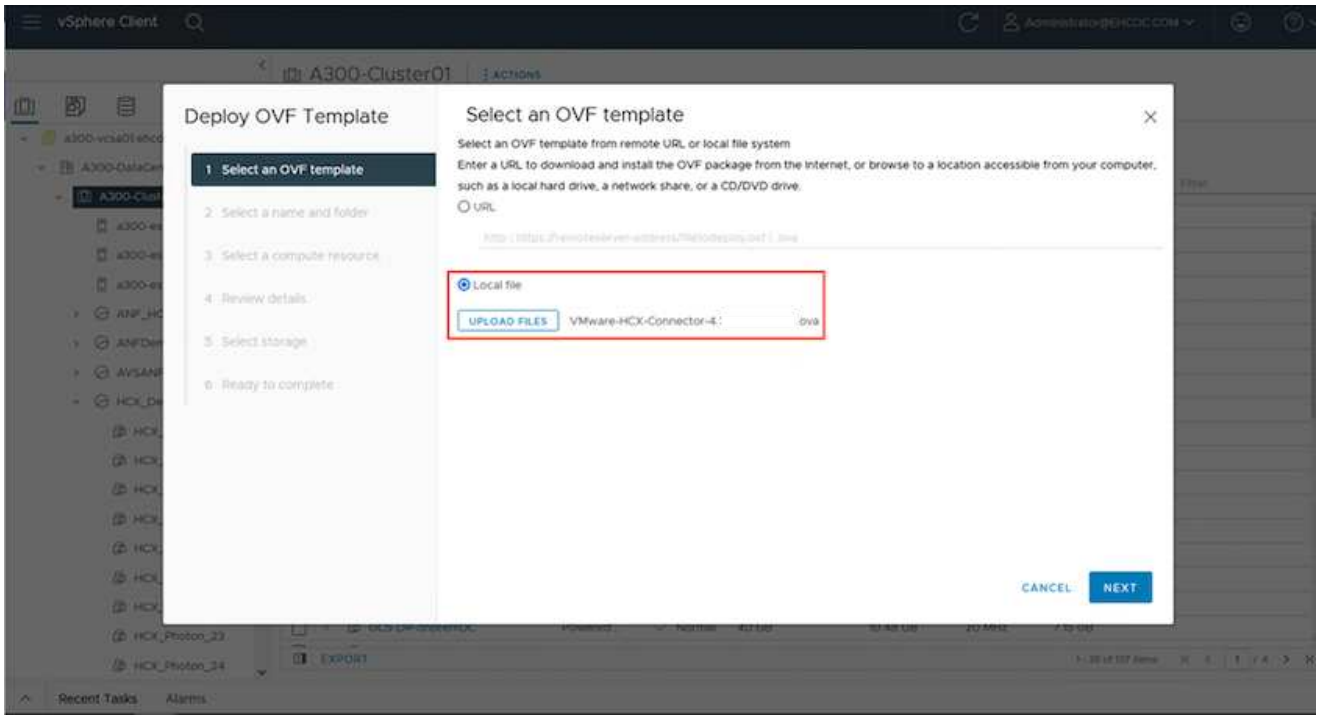


1. 使用jumphost通过mailto：cloudadmin@vsphere.local[cloudadmin@vsphere.local^]访问HCX门户后、导航到*管理>系统更新*、然后单击*请求下载链接*。

下载或复制到OVA的链接并将其粘贴到浏览器中、以开始下载要部署在内部vCenter Server上的VMware HCX Connector OVA文件。



1. 下载OVA后、使用*部署OVF模板*选项将其部署到内部VMware vSphere环境中。



1. 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。

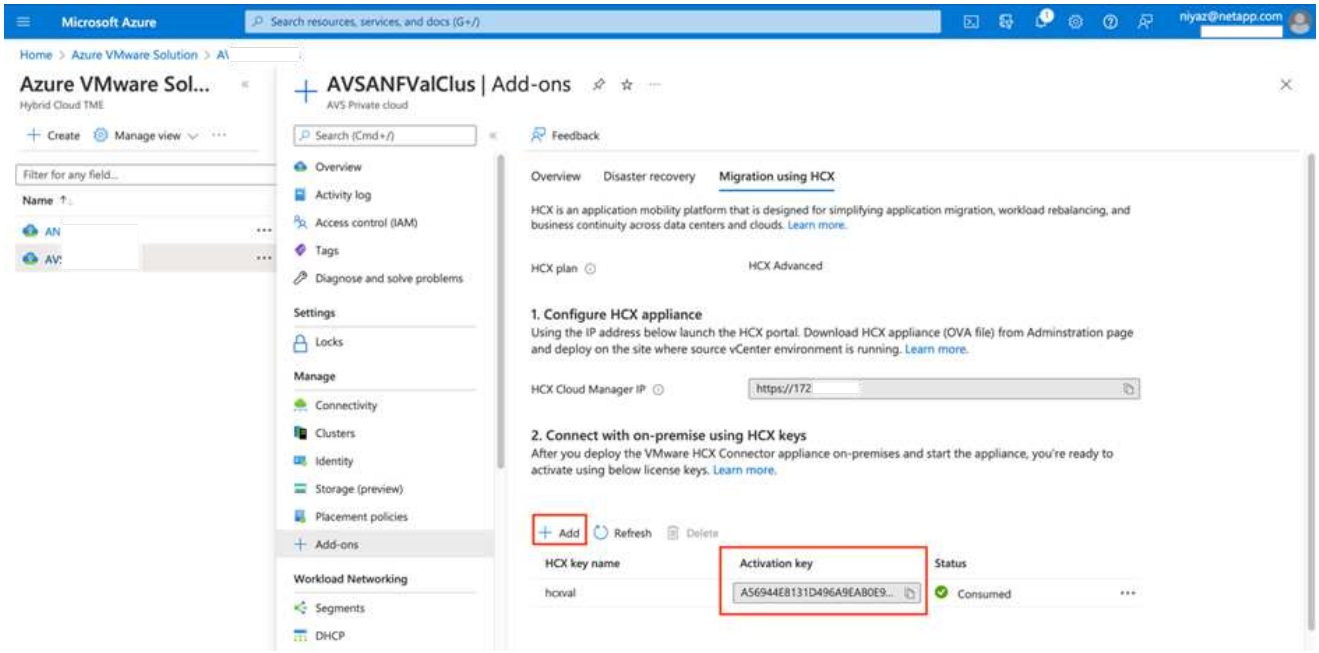
手动启动虚拟设备。

有关分步说明、请参见 "《VMware HCX用户指南》"。

第3步：使用许可证密钥激活HCX Connector

在内部部署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 HCL Manager中激活它。

1. 从Azure门户中、转到Azure VMware解决方案 、选择私有云、然后选择*管理>加载项>使用HCX*迁移。
2. 在*使用HCX密钥与内部环境连接*下、单击*添加*并复制激活密钥。



部署的每个内部HCX连接器都需要一个单独的密钥。

1. 登录到内部部署的VMware HCX Manager、网址为 "https://hcxmanagerIP:9443" 使用管理员凭据。

使用在OVA部署期间定义的密码。

1. 在许可中、输入从步骤3复制的密钥、然后单击*激活*。

内部HCX连接器应可访问Internet。

1. 在*数据中心位置*下、提供最近的位置、以便在内部安装VMware HCX Manager。单击 * 继续 * 。
2. 在*系统名称*下、更新名称并单击*继续*。
3. 单击*是、继续*。
4. 在*连接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。

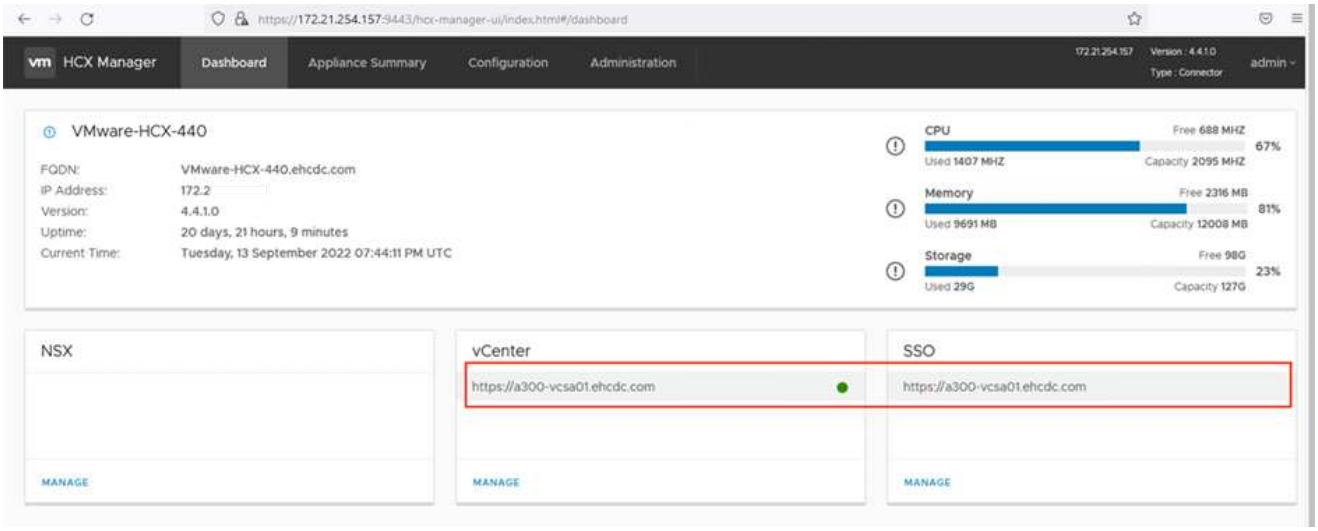
使用FQDN以避免稍后出现连接问题。

1. 在*配置SSA/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。

1. 验证输入的信息是否正确、然后单击*重新启动*。
2. 服务重新启动后、vCenter Server将在显示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。

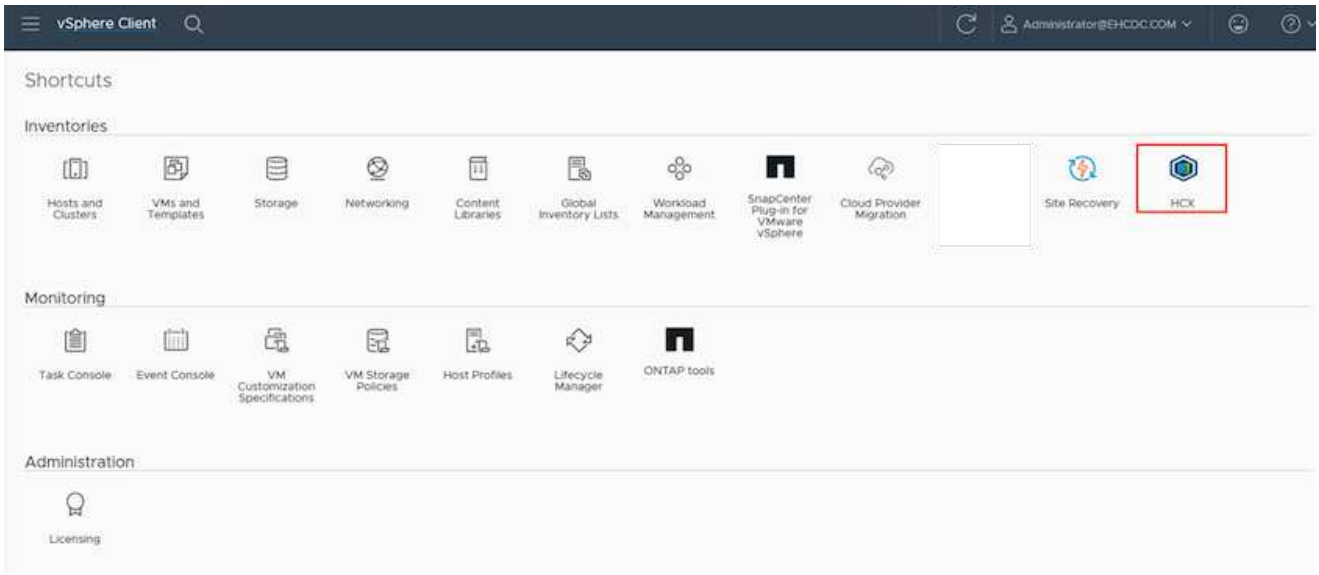
此过程大约需要10到20分钟、并且需要将此插件添加到vCenter Server中。



第4步：将内部**VMware HCX Connector**与**Azure VMware**解决方案 **HCX Cloud Manager**配对

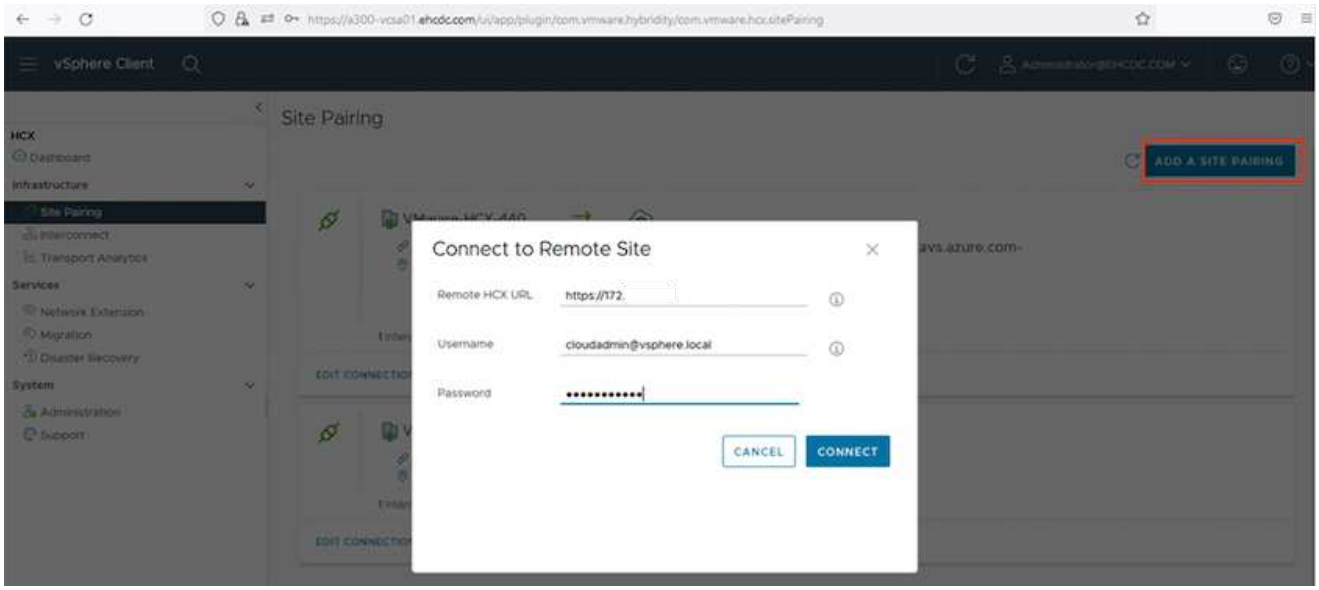
在内部部署和Azure VMware解决方案 中安装HCX Connector后、通过添加配对来配置适用于Azure VMware解决方案 私有云的内部部署VMware HCX Connector。要配置站点配对、请完成以下步骤：

1. 要在内部vCenter环境和Azure VMware解决方案 SDDC之间创建站点对、请登录到内部vCenter Server并访问新的HCX vSphere Web Client插件。



1. 在基础架构下、单击*添加站点配对*。

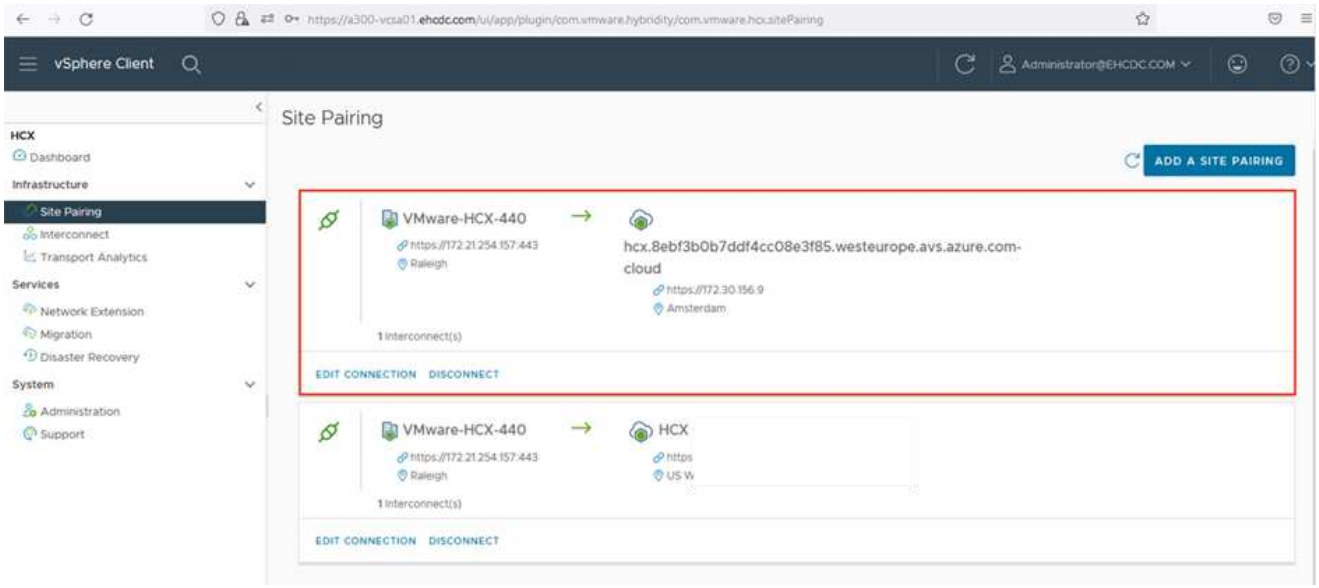
输入Azure VMware解决方案 HCX Cloud Manager URL或IP地址以及CloudAdmin角色访问私有云的凭据。



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、新配置的站点配对将显示在HCX信息板上。

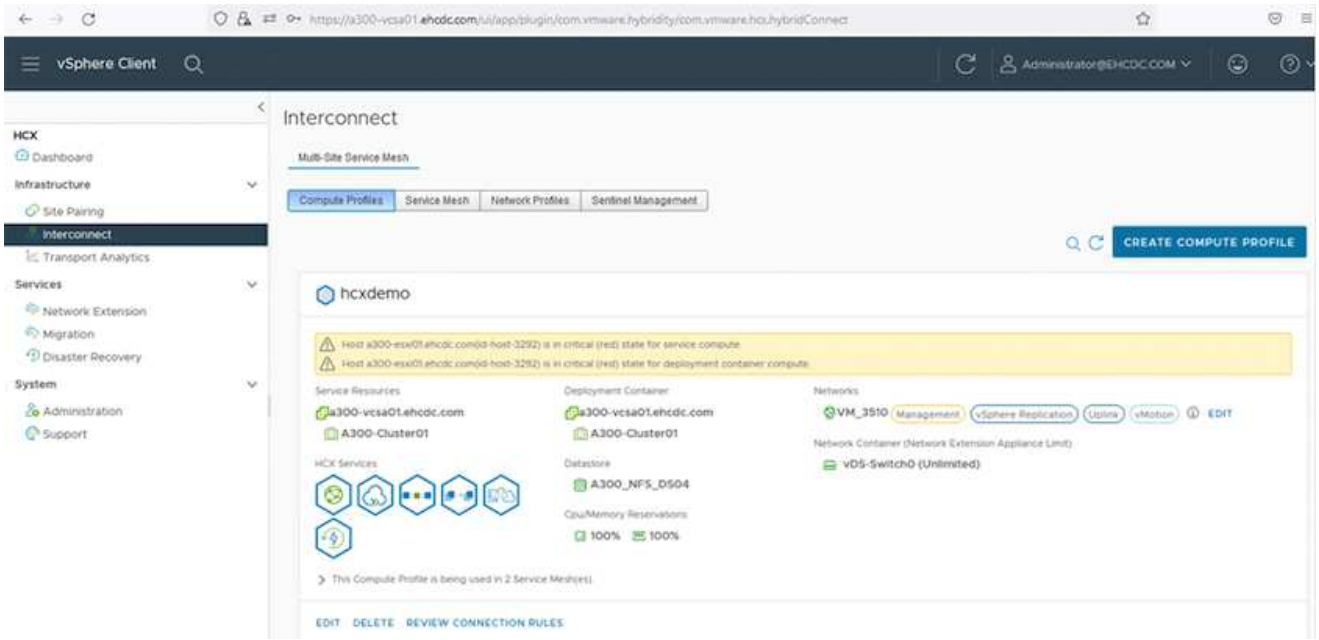


第**5**步：配置网络配置文件、计算配置文件和服务网格

VMware HCX互连服务设备可通过Internet以及与目标站点的专用连接提供复制和基于vMotion的迁移功能。互连可提供加密、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. 在基础架构下、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*。

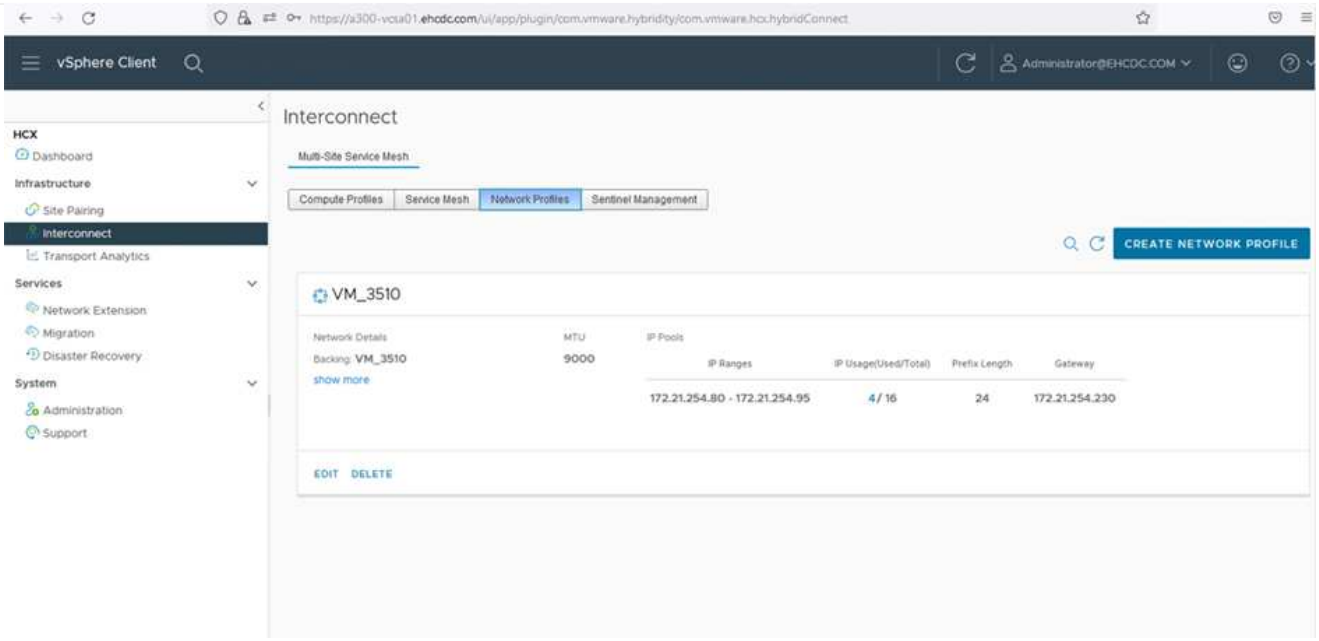
计算配置文件定义了部署参数、包括部署的设备以及HCL服务可访问的VMware数据中心的哪个部分。



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。

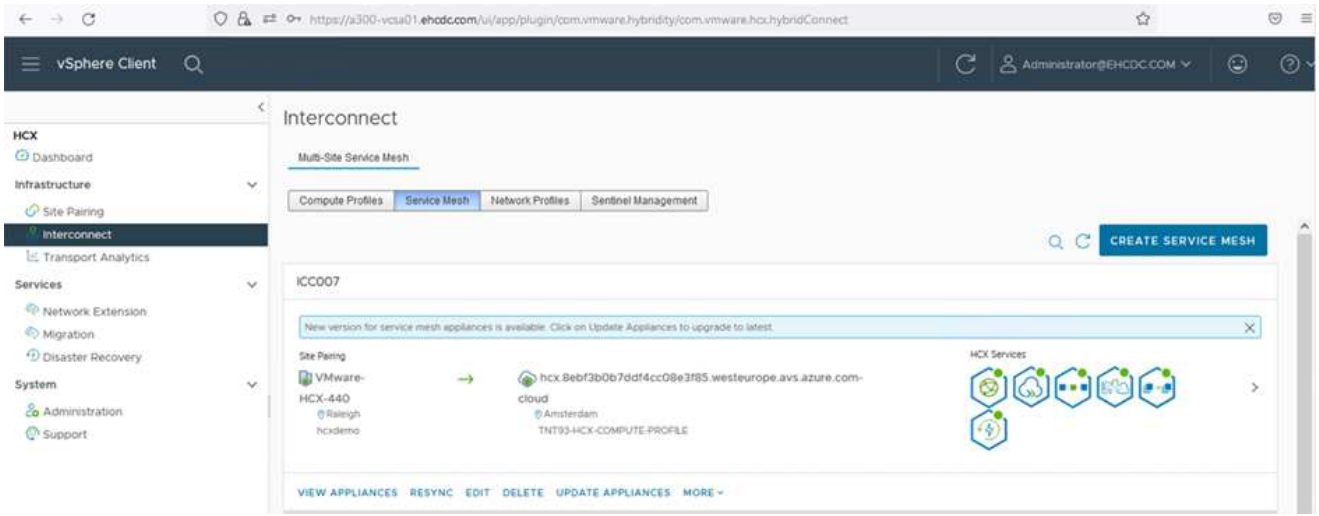
网络配置文件定义了HCX用于其虚拟设备的IP地址和网络范围。

此步骤需要两个或更多IP地址。这些IP地址将从管理网络分配给互连设备。

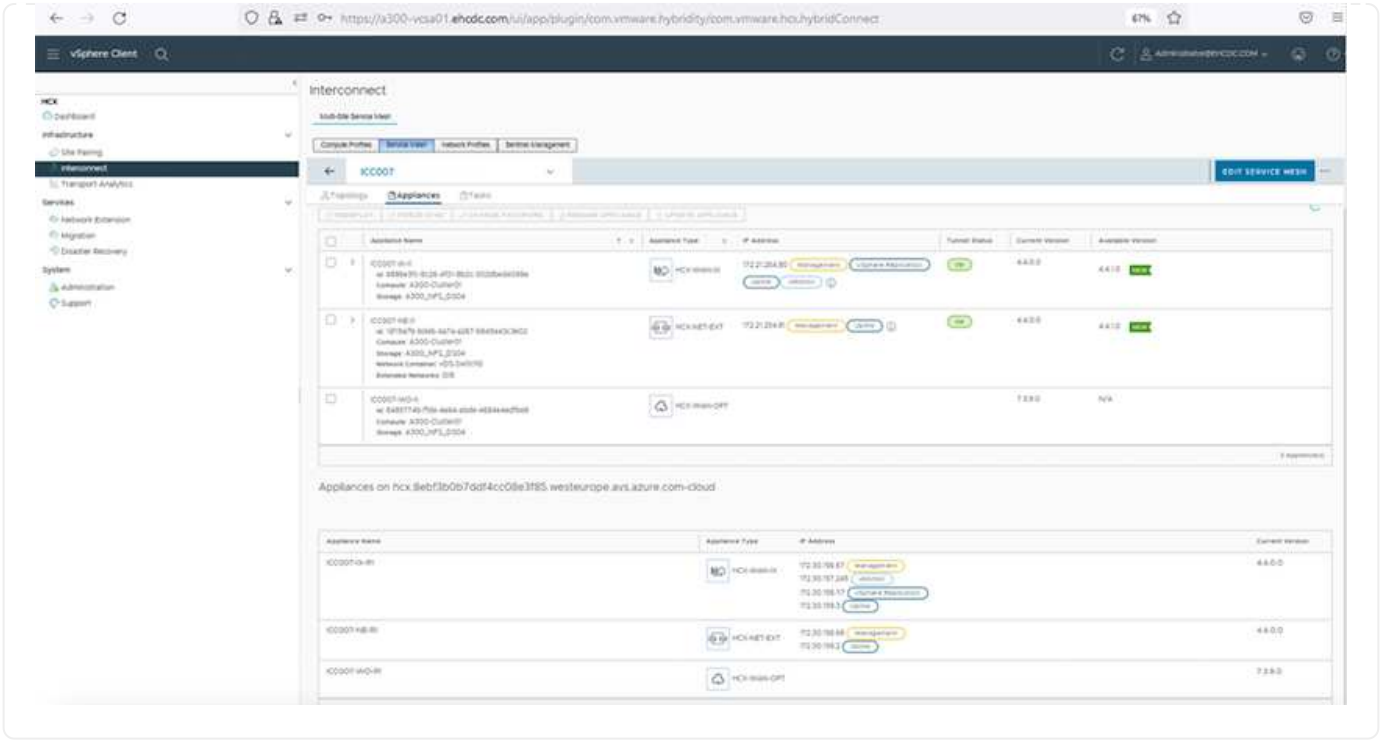


1. 此时、已成功创建计算和网络配置文件。
2. 在*互连*选项中选择*服务网格*选项卡以创建服务网格、然后选择内部和Azure SDDC站点。
3. 服务网格用于指定本地和远程计算和网络配置文件对。

在此过程中、源站点和目标站点都会部署并自动配置HCX设备、以便创建安全的传输网络结构。



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、环境便已准备就绪、可以成功创建IPsec通道来迁移工作负载VM。


vSphere Client
Interconnect
EDIT SERVICE MESH
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

第6步：迁移工作负载

可以使用各种VMware HCX迁移技术在内部部署和Azure SDDC之间双向迁移工作负载。可以使用多种迁移技术将VM移入和移出VMware HCX激活的实体、例如HCX批量迁移、HCX vMotion、HCX冷迁移、HCX复制辅助vMotion (适用于HCX Enterprise版本)和HCX操作系统辅助迁移(适用于HCX Enterprise版本)。

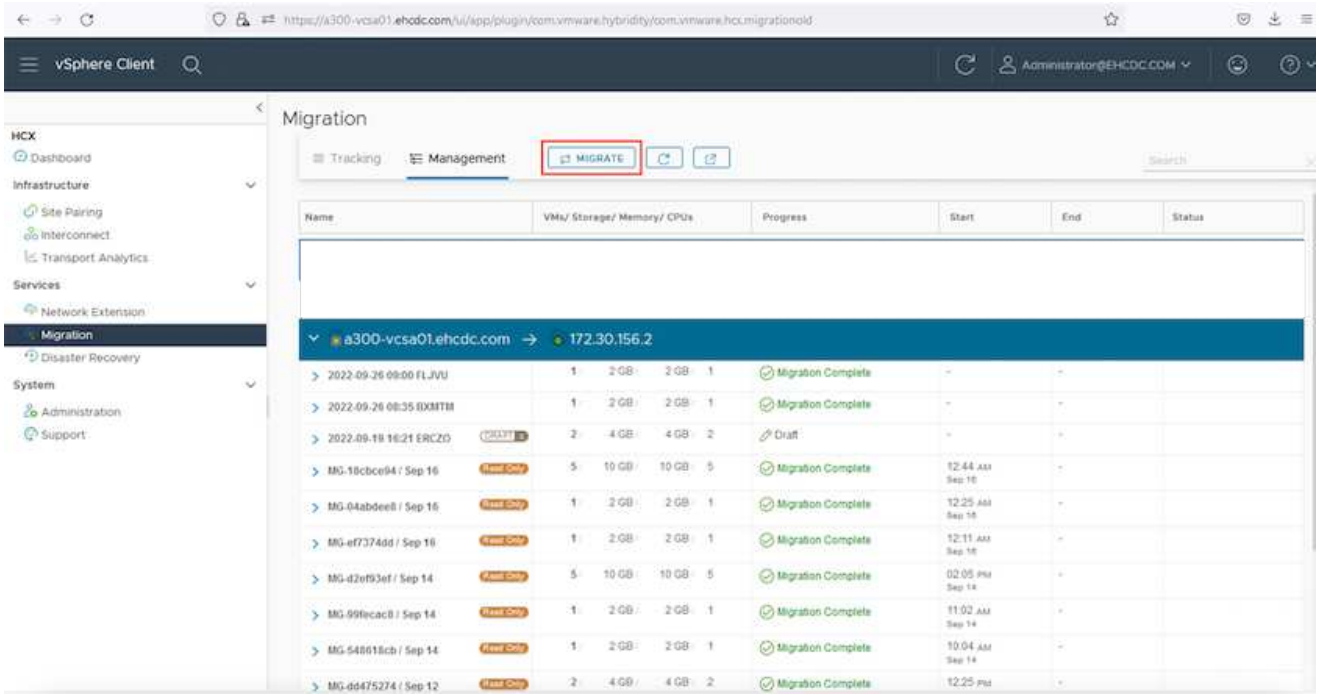
要了解有关各种HCX迁移机制的更多信息、请参见 "VMware HCX迁移类型"。

批量迁移

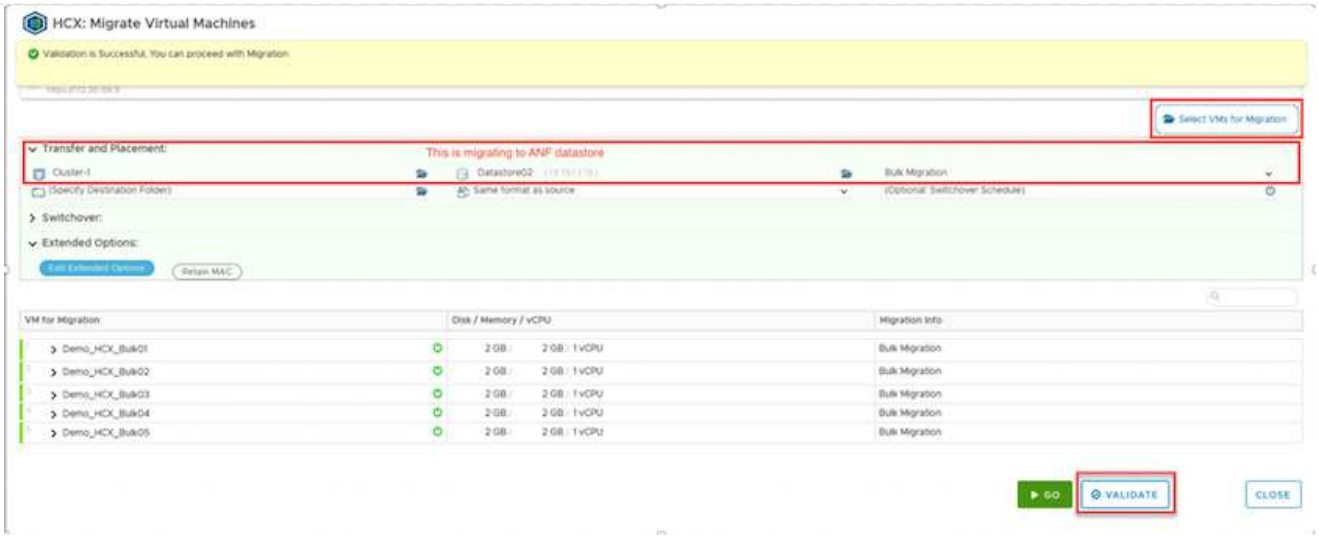
本节详细介绍了批量迁移机制。在批量迁移期间、HCX的批量迁移功能使用vSphere复制迁移磁盘文件、同时在目标vSphere HCX实例上重新创建VM。

要启动批量VM迁移、请完成以下步骤：

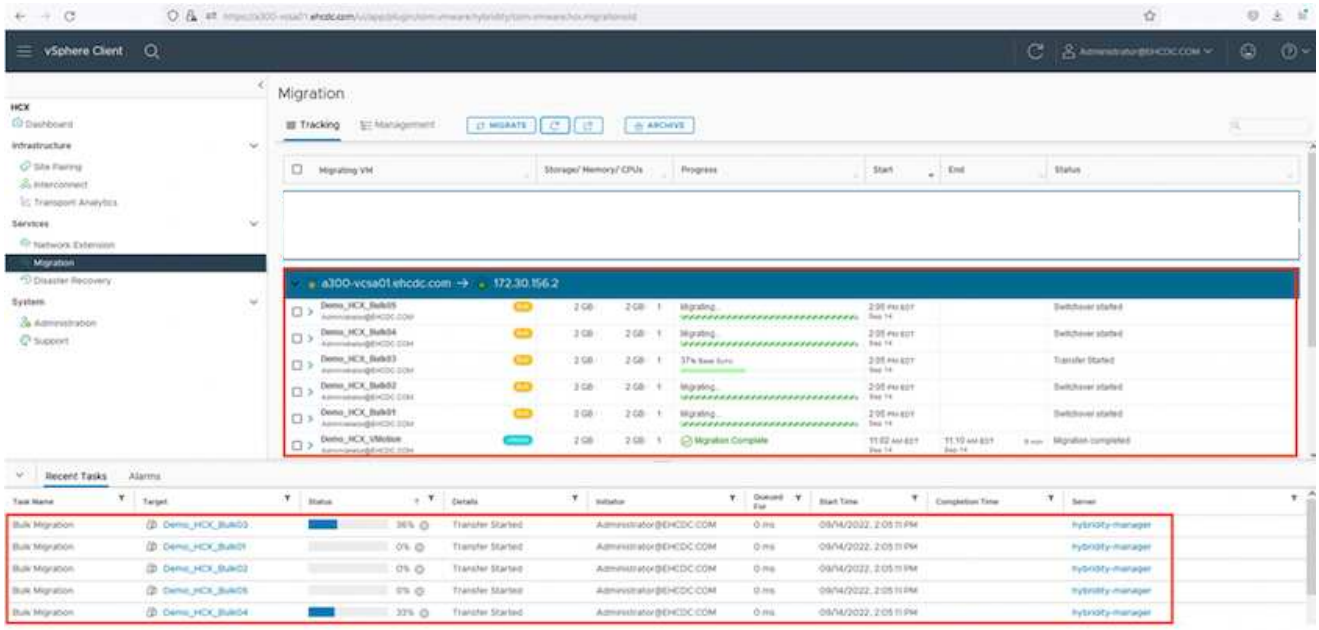
1. 访问*服务>迁移*下的*迁移*选项卡。



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、目标为Azure VMware解决方案 SDDC HCX端点。
2. 单击*选择要迁移的虚拟机*。此操作将列出所有内部VM。根据match：value表达式选择VM、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*。

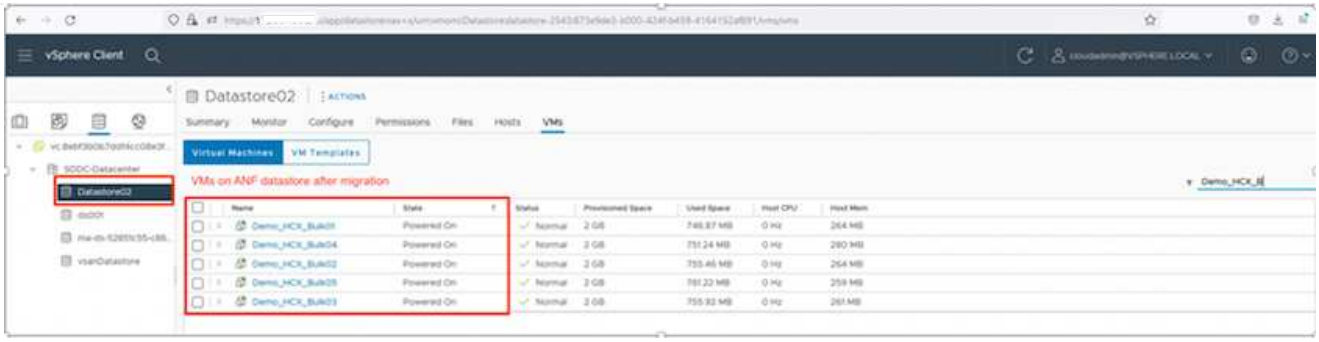


1. 验证检查完成后、单击*执行*以启动迁移。



在此迁移期间、会在目标vCenter中的指定Azure NetApp Files 数据存储库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。系统会触发HBR以与目标完全同步、在基线完成后、将根据恢复点目标(RPO)周期执行增量同步。完整/增量同步完成后、除非设置了特定计划、否则会自动触发切换。

1. 迁移完成后、通过访问目标SDDC vCenter来验证相同的。

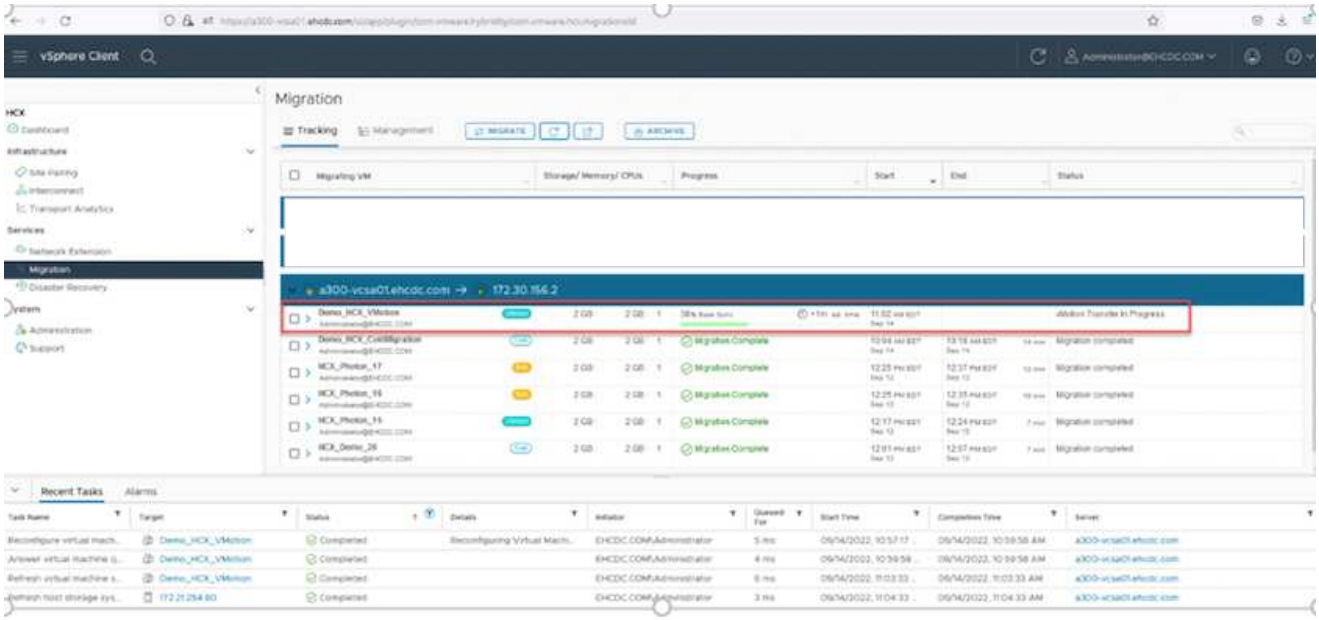


有关各种迁移选项以及如何使用HCX将工作负载从内部迁移到Azure VMware解决方案 的其他详细信息、请参见 "《VMware HCX用户指南》"。

要了解有关此过程的更多信息、请随时观看以下视频：

使用HCX迁移工作负载

下面是HCX vMotion选项的屏幕截图。



要了解有关此过程的更多信息、请随时观看以下视频：

HCX vMotion

确保有足够的带宽来处理迁移。

目标ANF数据存储库应具有足够的空间来处理迁移。

结论

无论您的目标是全云还是混合云、以及驻留在内部任何类型/供应商存储上的数据、Azure NetApp Files 和HCX都可以提供出色的选项来部署和迁移应用程序工作负载、同时通过将数据需求无缝地迁移到应用程序层来降

低TCO。无论使用何种情形、都可以选择Azure VMware解决方案 和Azure NetApp Files 、以快速实现云优势、跨内部和多个云实现一致的基础架构和运营、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甚至网络文件复制(Network File Copy、NFCs)连接存储和迁移VM时、使用的过程与步骤相同。

要点总结

本文档的要点包括：

- 现在、您可以将Azure NetApp Files 用作Azure VMware解决方案 SDDC上的数据存储库。
- 您可以轻松地将数据从内部迁移到Azure NetApp Files 数据存储库。
- 您可以轻松地扩展和缩减Azure NetApp Files 数据存储库、以满足迁移活动期间的容量和性能要求。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请访问以下网站链接：

- 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用户指南》

"https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

区域可用性—适用于**ANF**的补充**NFS**数据存储库

Azure / AVS上的补充NFS数据存储库的可用性由Microsoft定义。首先、您需要确定AVS和ANF是否在特定区域可用。接下来、您需要确定该区域是否支持ANF补充NFS数据存储库。

- 检查AVS和ANF的可用性 "此处"。
- 检查ANF补充NFS数据存储库的可用性 "此处"。

适用于 **Google Cloud Platform GCVE** 的 **NetApp** 功能

详细了解NetApp为Google云平台(GCP) Google Cloud VMware Engine (GCVe)带来的功能—从作为子系统连接存储设备或补充NFS数据存储库的NetApp、到迁移工作流、扩展/扩充到云、备份/还原和灾难恢复。

从以下选项中选择，跳至所需内容部分：

- "在 GCP 中配置 GCVE"
- "适用于 GCVE 的 NetApp 存储选项"

- "NetApp/VMware云解决方案"

在 GCP 中配置 GCVE

与内部部署一样，规划基于云的虚拟化环境对于成功创建 VM 和迁移生产就绪环境至关重要。

本节介绍如何设置和管理 GCVE ，并将其与连接 NetApp 存储的可用选项结合使用。

来宾存储是将 Cloud Volumes ONTAP 和云卷服务连接到 GCVE 的唯一受支持方法。

设置过程可细分为以下步骤：

- 部署和配置 GCVE
- 启用对 GCVE 的私有访问

查看详细信息 "GCVE的配置步骤"。

适用于 GCVE 的 NetApp 存储选项

NetApp存储可以通过多种方式在GCP GCVE中用作guess connected或作为补充NFS数据存储库。

请访问 "支持的 NetApp 存储选项" 有关详细信息 …

Google Cloud 支持以下配置中的 NetApp 存储：

- Cloud Volumes ONTAP （ CVO ）作为子系统连接的存储
- Cloud Volumes Service （ CVS ）作为子系统连接的存储
- Cloud Volumes Service (CVS)作为补充NFS数据存储库

查看详细信息 "GCVE的子系统连接存储选项"。

了解更多信息 "适用于Google Cloud VMware Engine的NetApp Cloud Volumes Service 数据存储库支持(NetApp博客)" 或 "如何使用NetApp CVS作为Google Cloud VMware Engine的数据存储库(Google博客)"

解决方案用例

借助 NetApp 和 VMware 云解决方案，许多用例都可以轻松部署在 Azure AVS 中。为VMware定义的每个云区域定义了SE案例：

- 保护(包括灾难恢复和备份/还原)
- 扩展
- 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

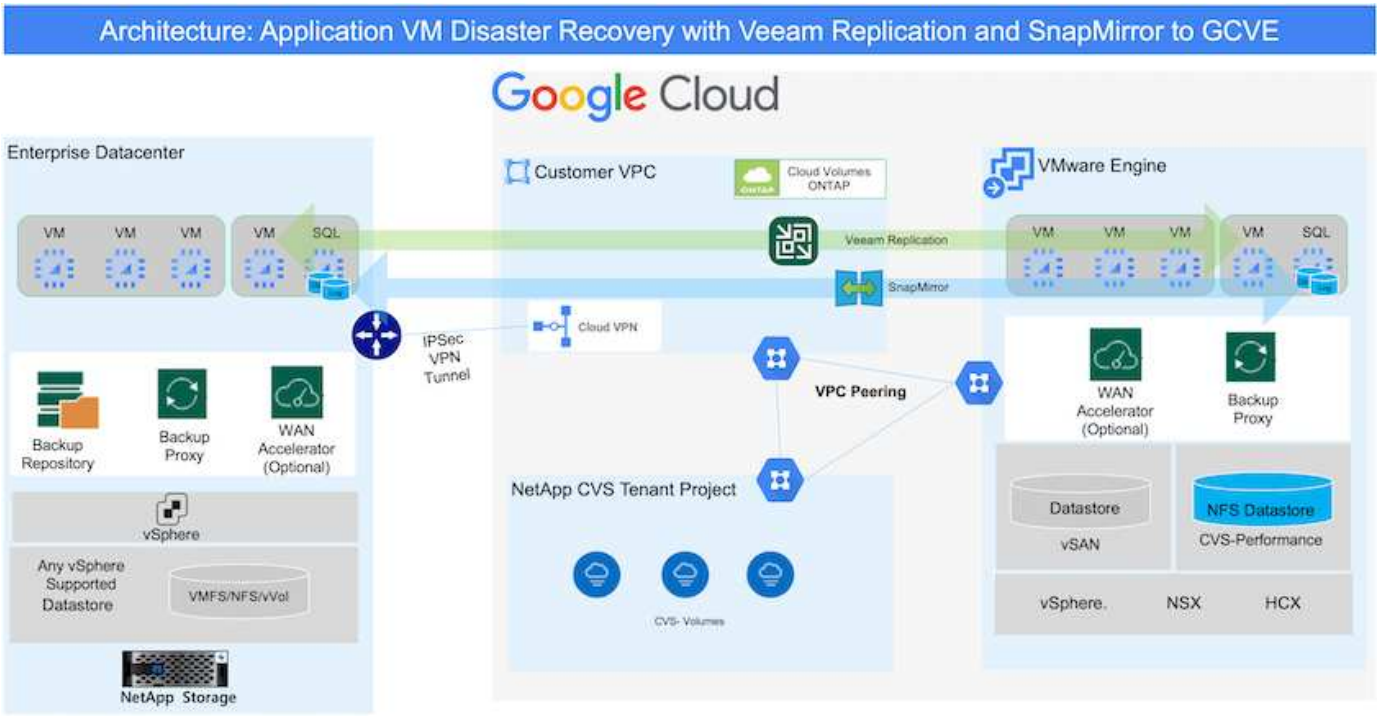
作者：NetApp公司Suresh ThopPay

概述

许多客户都在为VMware vSphere上托管的应用程序VM寻找有效的灾难恢复解决方案。其中许多企业使用现有备份解决方案在灾难期间执行恢复。
解决方案多次增加了RTO、但并未达到他们的期望。为了减少RPO和RTO、只要具有适当权限的网络连接和环境可用、即使从内部复制到GCVE)也可以使用Veeam VM复制。
注意：Veeam VM Replication不会保护与VM子系统连接的存储设备、例如子系统VM中的iSCSI或NFS挂载。需要单独保护这些数据。

为了实现SQL VM的应用程序一致复制并减少RTO、我们使用SnapCenter来编排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子系统内存储(也称为子系统连接)、我们假定内部环境正在使用SnapCenter 进行应用程序一致的备份。

> 本文档将对任何第三方备份或恢复解决方案 进行适用场景。根据环境中使用的解决方案 、按照最佳实践创建符合组织SLA的备份策略。

要在内部环境与Google Cloud网络之间建立连接、请使用专用互连或Cloud VPN等连接选项。应根据内部VLAN设计创建分段。

将内部数据中心连接到Google Cloud有多种方式、这使我们无法在本文档中概述特定工作流。有关适当的内部到Google连接方法、请参见Google Cloud文档。

部署**DR**解决方案

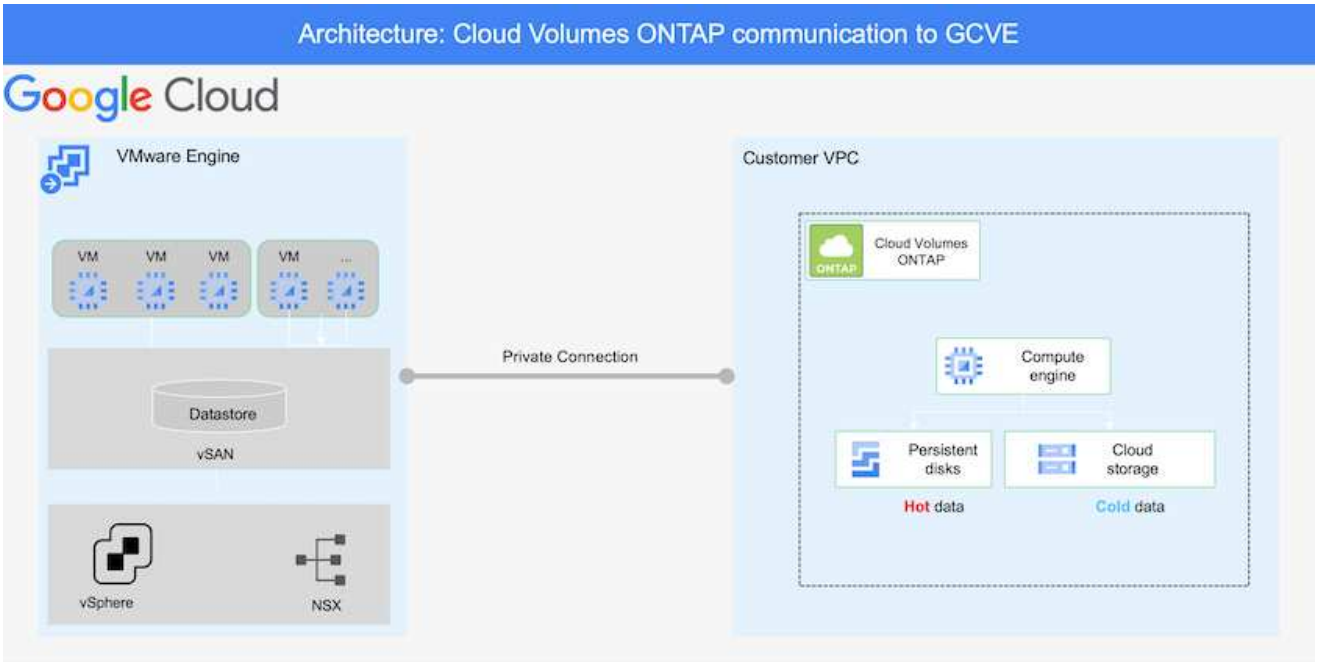
解决方案 部署概述

1. 确保使用具有必要RPO要求的SnapCenter 备份应用程序数据。
2. 在适当的订阅和虚拟网络中使用BlueXP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、以便在计划作业完成后触发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. 发生灾难事件时、请使用BlueXP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VM的iSCSI LUN和NFS挂载。
   b. 使应用程序联机。
5. 在主站点恢复之后、通过反向重新同步SnapMirror来调用对受保护站点的故障恢复。

部署详细信息

在**Google Cloud**上配置**CVO**并将卷复制到**CVO**

第一步是Cloud Volumes ONTAP在Google Cloud ("CVO")并使用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 和复制数据的分步说明示例、请参见 "使用SnapCenter 设置复制"

查看使用SnapCenter保护SQL VM的情况

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SDDC的持续运行时间。对于灾难恢复解决方案 、这两个主要注意事项有助于降低整体运营成本。SDDC可以小至三台主机、在整个规模的部署中一直到多主机集群。

可以将适用于NFS数据存储库的NetApp云卷服务以及适用于SQL的Cloud Volumes ONTAP数据库和日志部署到任何VPC、并且GCVe应与该VPC建立专用连接、以便挂载NFS数据存储库并使VM连接到iSCSI LUN。

要配置GCVE SDDC、请参见 "在 Google Cloud Platform （ GCP ）上部署和配置虚拟化环境"。前提条件是、在建立连接后、验证位于GCVE主机上的子虚拟机是否能够使用Cloud Volumes ONTAP 中的数据。

正确配置Cloud Volumes ONTAP 和GCVE后、请使用Veeam复制功能并利用SnapMirror将应用程序卷副本复制到Cloud Volumes ONTAP 、开始配置Veeam、以便自动将内部工作负载恢复到GCVE (具有应用程序VMDK的VM和具有来宾存储的VM)。

安装**Veeam**组件

根据部署场景、需要部署的Veeam备份服务器、备份存储库和备份代理。在此使用情形下、无需为Veeam部署对象存储、也不需要横向扩展存储库。
"有关安装操作步骤 的信息、请参见Veeam文档"
有关追加信息、请参见 "使用Veeam Replication进行迁移"

使用**Veeam**设置**VM**复制

内部vCenter和GCVE vCenter都需要向Veeam注册。 "设置vSphere VM复制作业" 在向导的子系统处理步骤中、选择禁用应用程序处理、因为我们将利用SnapCenter 进行应用程序感知型备份和恢复。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Microsoft SQL Server VM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

- 使用高效且具有故障恢复能力的SnapMirror复制。
- 使用ONTAP 快照保留功能恢复到任何可用时间点。
- 从存储、计算、网络和应用程序验证步骤中恢复成百上千个VM所需的所有步骤均可实现完全自动化。
- SnapCenter 使用的克隆机制不会更改复制的卷。
  - 这样可以避免卷和快照的数据损坏风险。
  - 在灾难恢复测试工作流期间避免复制中断。
  - 将灾难恢复数据用于灾难恢复以外的工作流、例如开发/测试、安全测试、修补和升级测试以及修复测试。
- Veeam复制允许更改灾难恢复站点上的VM IP地址。

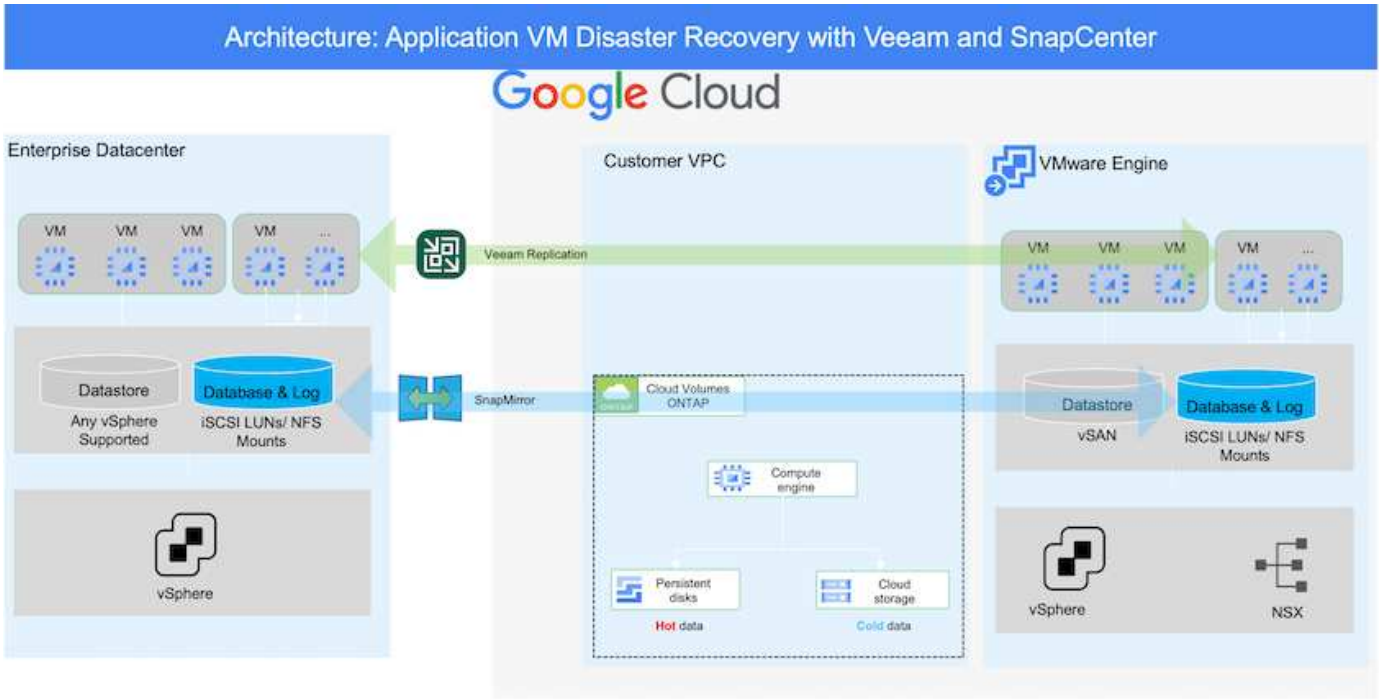
使用**SnapCenter** 、**Cloud Volumes ONTAP** 和**Veeam**复制实现应用程序灾难恢复

作者：NetApp公司Suresh ThopPay

概述

将灾难恢复到云是一种具有弹性且经济高效的方式、可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、可以将使用来宾连接存储的内部VMware工作负载复制到在Google Cloud中运行的NetApp Cloud Volumes ONTAP。其中包括应用程序数据；但是、实际VM本身又如何。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。为此、可以使用SnapMirror和Veeam无缝恢复从内部复制到Cloud Volumes ONTAP 的工作负载、同时对VM VMDK使用vSAN存储。

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子系统内存储(也称为子系统连接)、我们假定内部环境正在使用SnapCenter 进行应用程序一致的备份。

本文档将对任何第三方备份或恢复解决方案 进行适用场景。根据环境中使用的解决方案 、按照最佳实践创建符合组织SLA的备份策略。

要在内部环境与Google Cloud网络之间建立连接、请使用专用互连或Cloud VPN等连接选项。应根据内部VLAN设计创建分段。

将内部数据中心连接到Google Cloud有多种方式、这使我们无法在本文档中概述特定工作流。有关适当的内部到Google连接方法、请参见Google Cloud文档。

部署**DR**解决方案

解决方案 部署概述

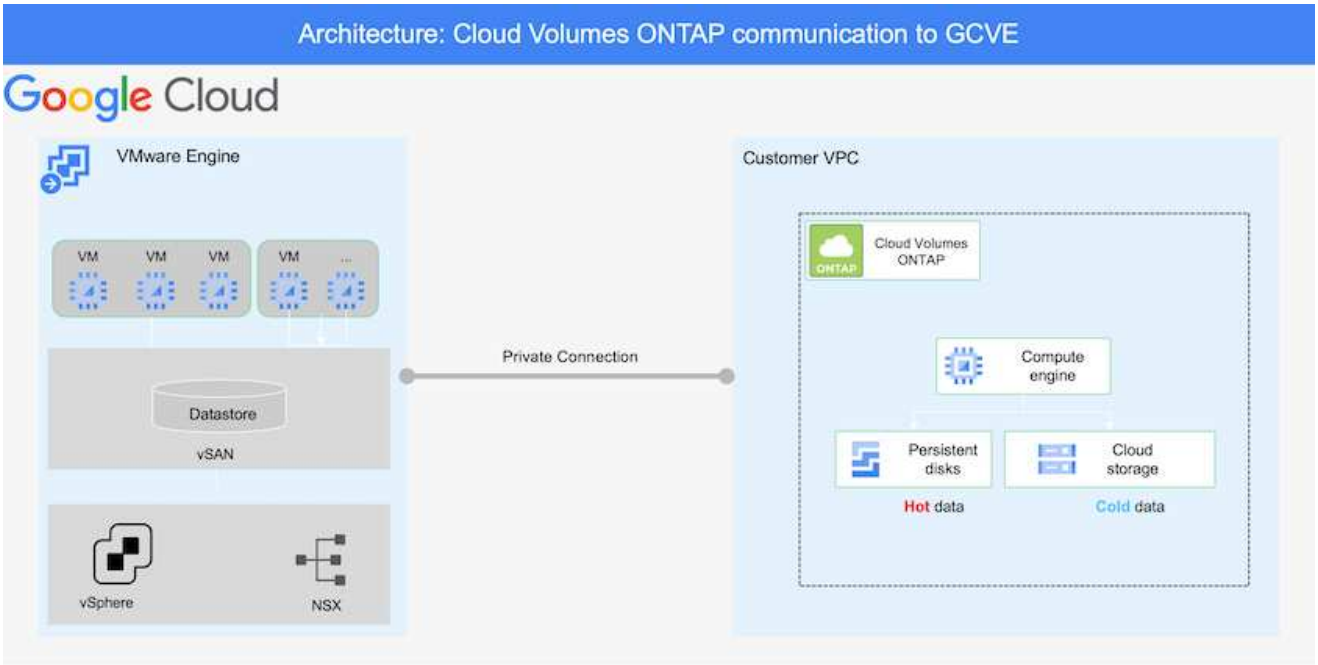
1. 确保使用具有必要RPO要求的SnapCenter 备份应用程序数据。
2. 在相应的订阅和虚拟网络中使用Cloud Manager使用正确的实例大小配置Cloud Volumes ONTAP。
   a. 为相关应用程序卷配置SnapMirror。
   b. 更新SnapCenter 中的备份策略、以便在计划作业完成后触发SnapMirror更新。
3. 安装Veeam软件并开始将虚拟机复制到Google Cloud VMware Engine实例。
4. 发生灾难事件时、使用Cloud Manager中断SnapMirror关系、并触发Veeam虚拟机故障转移。
   a. 重新连接应用程序VM的iSCSI LUN和NFS挂载。
   b. 使应用程序联机。

5. 在主站点恢复之后、通过反向重新同步SnapMirror来调用对受保护站点的故障恢复。

部署详细信息

在**Google Cloud**上配置**CVO**并将卷复制到**CVO**

第一步是Cloud Volumes ONTAP在Google Cloud ("CVO")并使用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 和复制数据的分步说明示例、请参见 "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SDDC的持续运行时间。对于灾难恢复解决方案 、这两个主要注意事项有助于降低整体运营成本。SDDC可以小至三台主机、在整个规模的部署中一直到多主机集群。

可以将Cloud Volumes ONTAP 部署到任何VPC、并且CVE应与该VPC建立专用连接、以便VM连接到iSCSI LUN。

要配置GCVE SDDC、请参见 "在 Google Cloud Platform （ GCP ）上部署和配置虚拟化环境"。前提条件是、在建立连接后、验证位于GCVE主机上的子虚拟机是否能够使用Cloud Volumes ONTAP 中的数据。

正确配置Cloud Volumes ONTAP 和GCVE后、请使用Veeam复制功能并利用SnapMirror将应用程序卷副本复制到Cloud Volumes ONTAP 、开始配置Veeam、以便自动将内部工作负载恢复到GCVE (具有应用程序VMDK的VM和具有来宾存储的VM)。

安装**Veeam**组件

根据部署场景、需要部署的Veeam备份服务器、备份存储库和备份代理。在此使用情形下、无需为Veeam部署对象存储、也不需要横向扩展存储库。https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["有关安装操作步骤 的信息、请参见Veeam文档"]

使用**Veeam**设置**VM**复制

内部vCenter和GCVE vCenter都需要向Veeam注册。 "设置vSphere VM复制作业" 在向导的子系统处理步骤中、选择禁用应用程序处理、因为我们将利用SnapCenter 进行应用程序感知型备份和恢复。

设置vSphere VM复制作业

Microsoft SQL Server VM故障转移

Microsoft SQL Server VM故障转移

此解决方案 的优势

- 使用高效且具有故障恢复能力的SnapMirror复制。
- 使用ONTAP 快照保留功能恢复到任何可用时间点。
- 从存储、计算、网络和应用程序验证步骤中恢复成百上千个VM所需的所有步骤均可实现完全自动化。
- SnapCenter 使用的克隆机制不会更改复制的卷。
  - 这样可以避免卷和快照的数据损坏风险。
  - 在灾难恢复测试工作流期间避免复制中断。
  - 将灾难恢复数据用于灾难恢复以外的工作流、例如开发/测试、安全测试、修补和升级测试以及修复测试。
- Veeam复制允许更改灾难恢复站点上的VM IP地址。

在**GCP/GCVE)**上迁移工作负载

使用**VMware HCX -**快速入门指南将工作负载迁移到**Google Cloud VMware Engine**上的**NetApp Cloud Volume Service**数据存储库

作者：NetApp Solutions Engineering

概述：迁移具有**VMware HCX**、**NetApp Cloud Volume Service**数据存储库和**Google Cloud VMware Engine (GCVE)**的虚拟机

Google Cloud VMware引擎和Cloud Volume Service数据存储库最常见的使用情形之一是迁移VMware工作负载。VMware HCX是首选选项、可通过各种迁移机制将内部虚拟机(VM)及其数据移动到Cloud Volume Service NFS数据存储库。

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、甚至跨云实现业务连续性。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、可用于灾难恢

复(DR)操作。

本文档分步指导您配置Cloud Volume Service数据存储库、然后下载、部署和配置VMware HCX、包括内部部署和Google Cloud VMware Engine端的所有主要组件、包括互连、网络扩展和WAN优化、以启用各种VM迁移机制。

VMware HCX可用于任何数据存储库类型、因为迁移是在VM级别进行的。因此、本文档适用于计划通过Google Cloud VMware Engine部署Cloud Volume Service以实现经济高效的VMware云部署的现有NetApp客户和非NetApp客户。

高级步骤

此列表概括介绍了将VM与内部HCX Connector配对并迁移到Google Cloud VMware Engine端的HCX Cloud Manager所需的步骤：

1. 通过Google VMware引擎门户准备HCX。
2. 在内部部署的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. 将内部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进行IP。
7. 验证设备状态并确保可以进行迁移。
8. 迁移VM工作负载。

前提条件

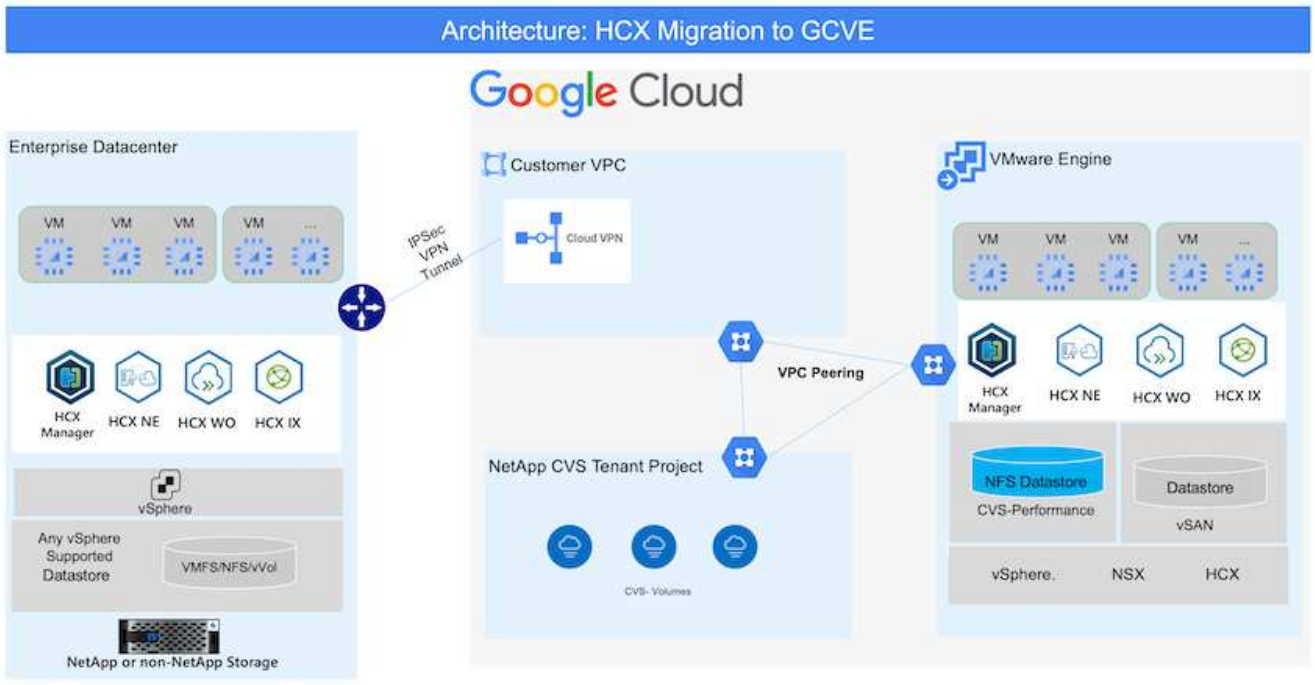
开始之前、请确保满足以下前提条件。有关详细信息，请参见此 "链接。"。满足包括连接在内的前提条件后、从Google Cloud VMware Engine门户下载HCX许可证密钥。下载OVA安装程序后、按如下所述继续安装过程。

> 默认选项为HCX高级版、VMware HCX Enterprise版本也可通过支持服务单获得、并且无需额外付费。请参见 "此链接。"

- 使用现有Google Cloud VMware Engine软件定义的数据中心(SDDC)或使用此功能创建私有云 "NetApp链接" 或这一点 "Google链接"。
- 从启用了VMware vSphere的内部数据中心迁移VM和关联数据需要从数据中心到SDDC环境的网络连接。迁移工作负载之前、 "设置Cloud VPN或Cloud Interconnect连接" 在内部环境和相应的私有云之间。
- 从内部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VM。
- 确保满足所需 "防火墙规则和端口" 允许内部vCenter Server与SDDC vCenter之间的vMotion流量。
- Cloud Volume Service NFS卷应作为数据存储库挂载到Google Cloud VMware Engine中。请按照本节中详细介绍的步骤进行操作 "链接。" 将Cloud Volume Service数据存储库连接到Google Cloud VMware Engines主机。

高级架构

出于测试目的、用于此验证的内部实验室环境通过云VPN进行连接、从而可以在内部连接到Google Cloud VPC。



有关HCX的更多详细图表、请参见 "VMware链接"

解决方案 部署

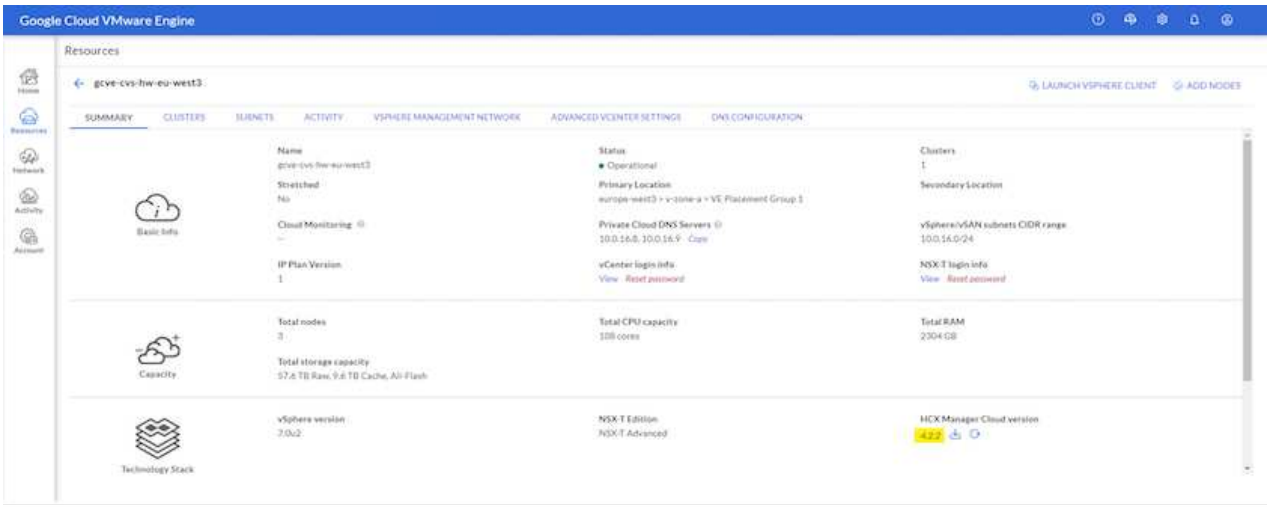
按照一系列步骤完成此解决方案 的部署：

第1步：通过Google VMware引擎门户准备HCX

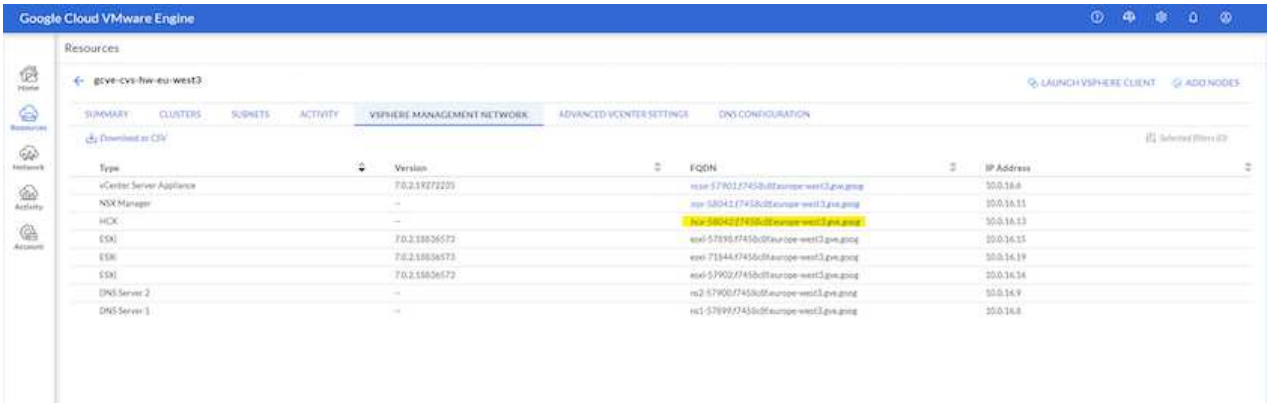
在使用VMware Engine配置私有云时、会自动安装HCX Cloud Manager组件。要准备站点配对、请完成以下步骤：

1. 登录到Google VMware引擎门户并登录到HCX Cloud Manager。

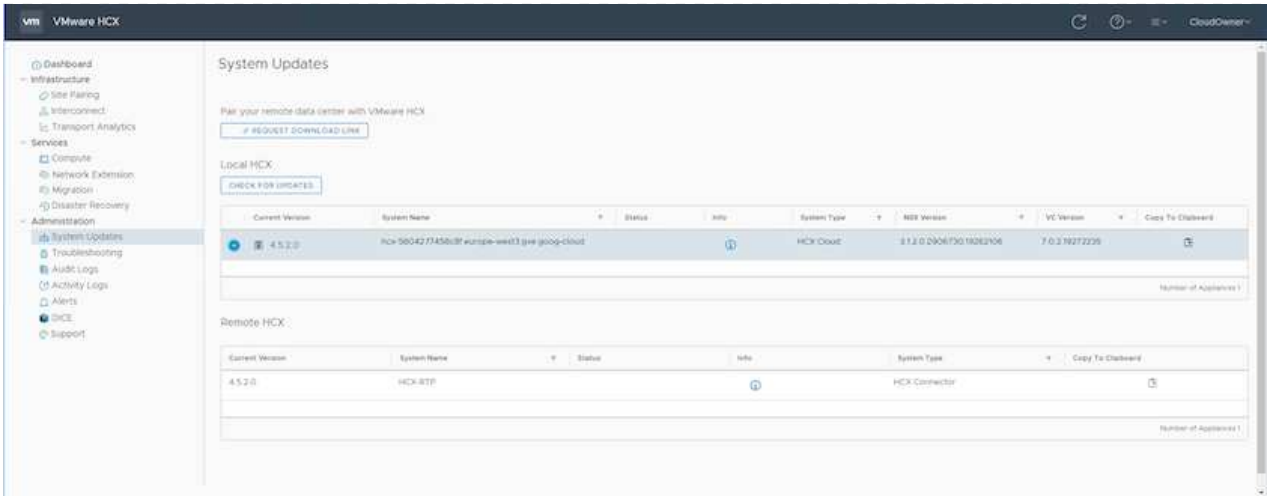
   您可以通过单击HCX版本链接登录到HCX控制台



   或者单击vSphere Management Network选项卡下的HCX FQDN。



2. 在HCX Cloud Manager中、转到*管理>系统更新*。
3. 单击*请求下载链接*并下载OVA文件。



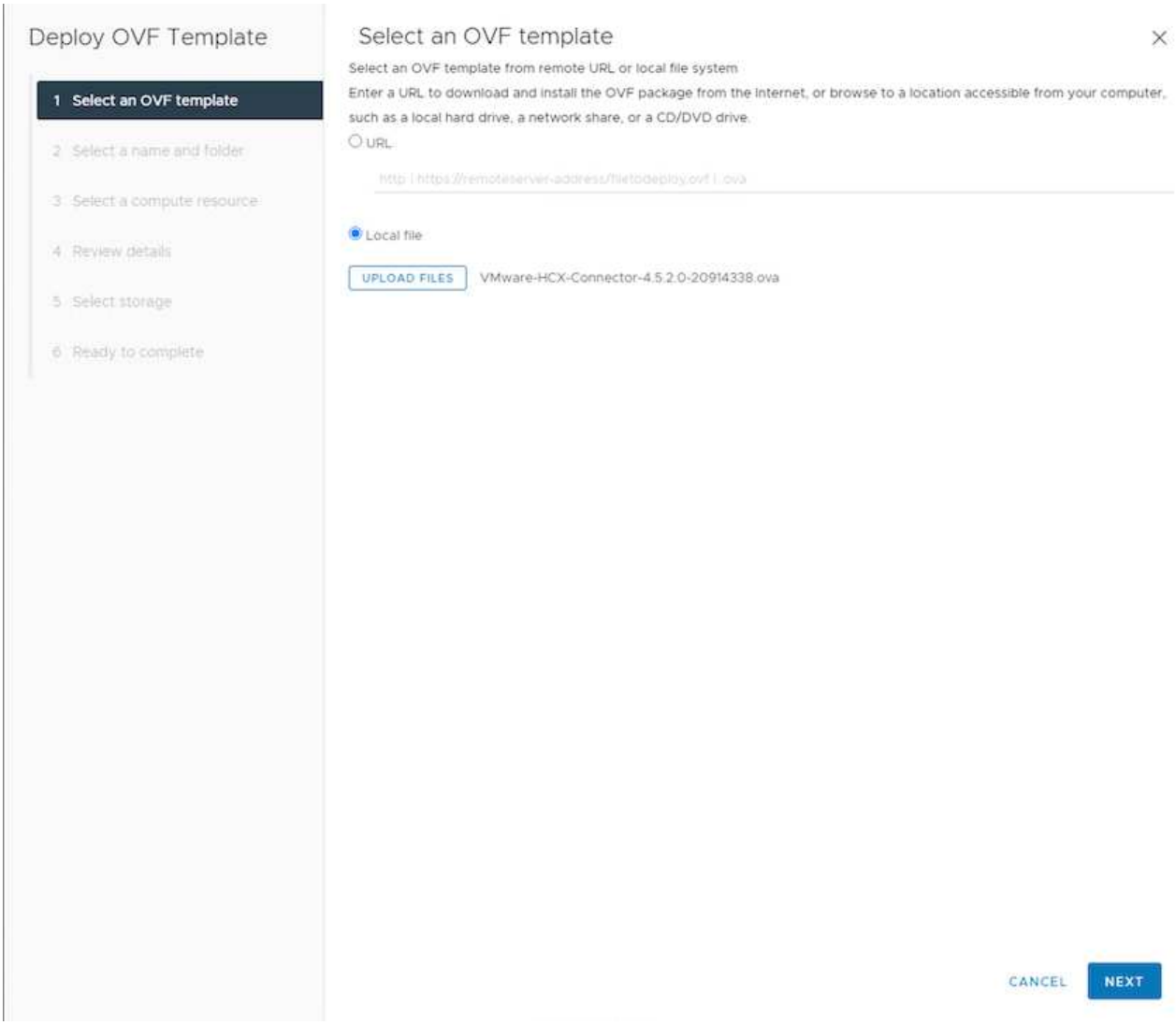
4. 将HCX Cloud Manager更新为可从HCX Cloud Manager UI获得的最新版本。

第2步：在内部vCenter Server中部署安装程序OVA

要使内部连接器连接到Google Cloud VMware Engine中的HCX Manager、请确保在内部环境中打开相应的防火墙端口。

要在内部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*选项将其部署到内部VMware vSphere环境中。



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。

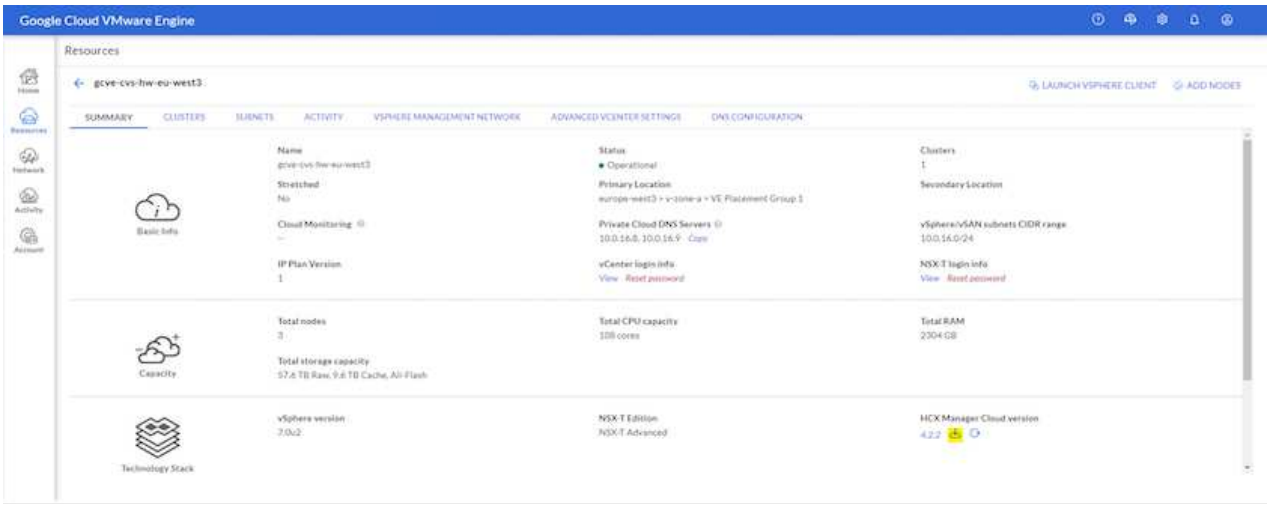
手动启动虚拟设备。

有关分步说明、请参见 "《VMware HCX用户指南》"。

第3步：使用许可证密钥激活HCX Connector

在内部部署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引擎门户中、单击资源、选择私有云、然后*单击HCX Manager Cloud Version*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. 登录到内部部署的VMware HCX Manager、网址为 "https://hcxmanagerIP:9443" 使用管理员凭据。

   使用在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*。

   内部HCX连接器应可访问Internet。

4. 在*数据中心位置*下、提供最近的位置、以便在内部安装VMware HCX Manager。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。

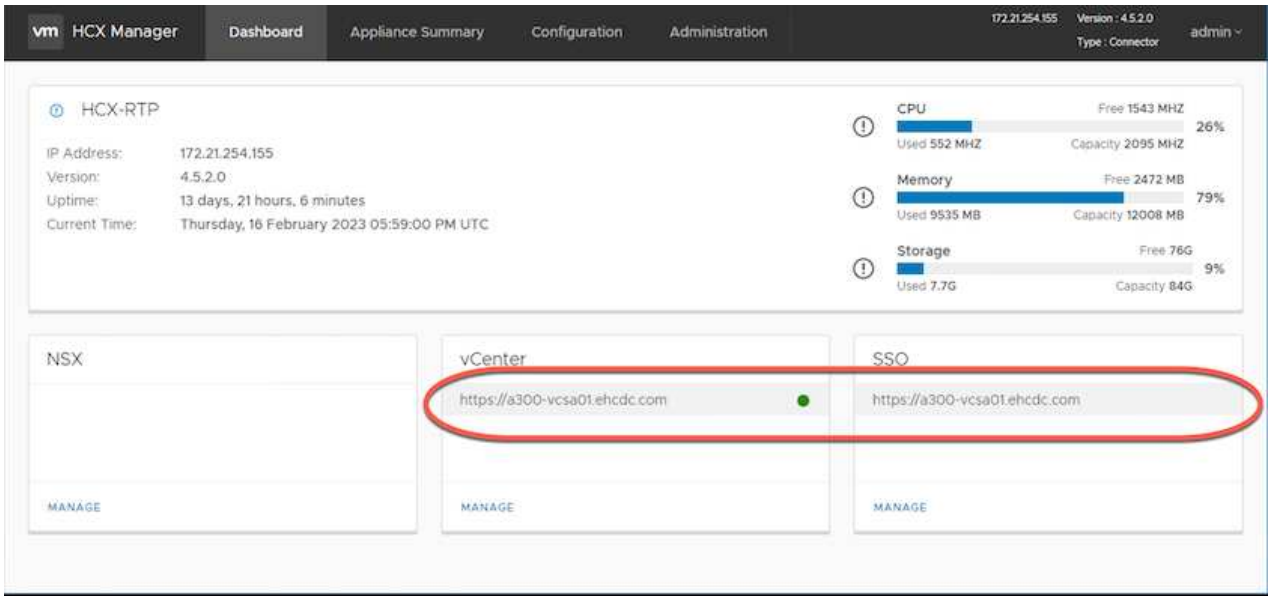
   使用FQDN以避免稍后出现连接问题。

8. 在*配置SSE/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将在显示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。

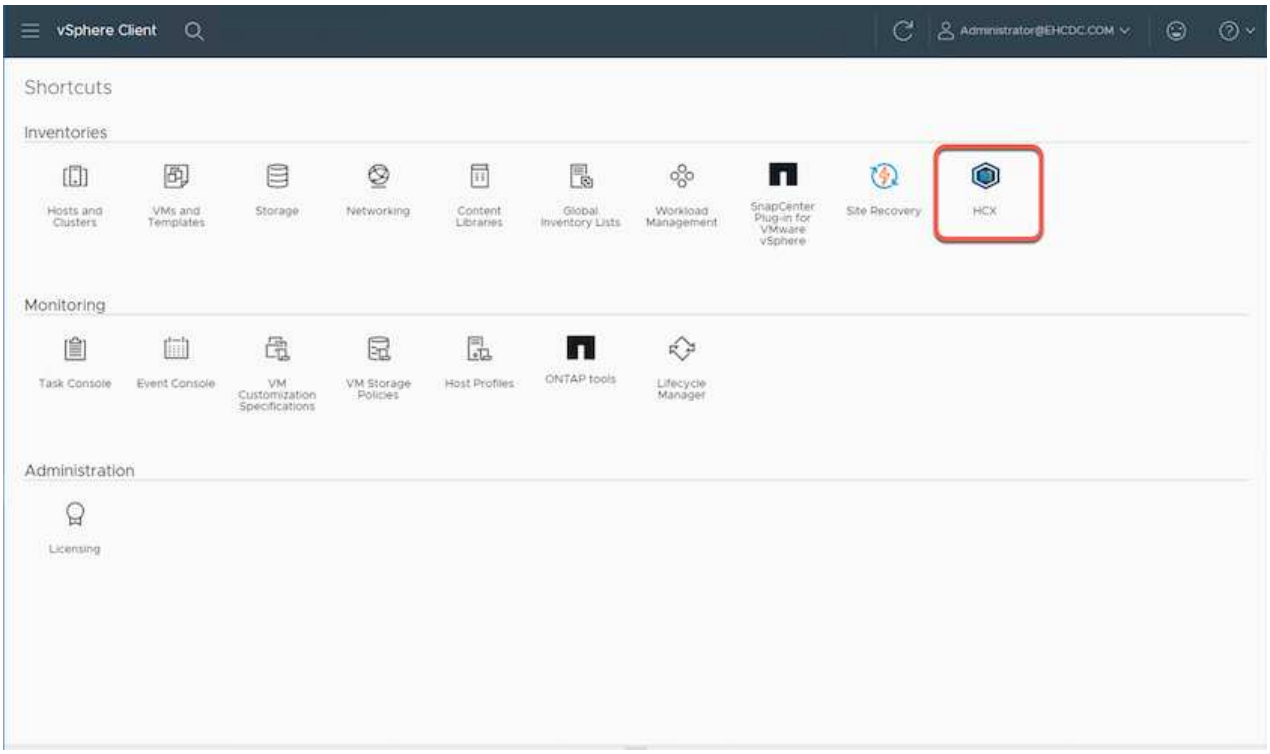
    此过程大约需要10到20分钟、并且需要将此插件添加到vCenter Server中。


vm HCX Manager
Dashboard
Appliance Summary
Configuration
Administration
172.21.254.155
Version : 4.5.2.0
Type : Connector
admin
HCX-RTP
IP Address: 172.21.254.155
Version: 4.5.2.0
Uptime: 13 days, 21 hours, 6 minutes
Current Time: Thursday, 16 February 2023 05:59:00 PM UTC
CPU
Free 1543 MHZ
26%
Used 552 MHZ
Capacity 2095 MHZ
Memory
Free 2472 MB
79%
Used 9535 MB
Capacity 12008 MB
Storage
Free 76G
9%
Used 7.7G
Capacity 84G
NSX
vCenter
https://a300-vcsa01.ehcdc.com
SSO
https://a300-vcsa01.ehcdc.com
MANAGE
MANAGE
MANAGE

第4步：将内部**VMware HCX Connector**与**Google Cloud VMware Engine HCX Cloud Manager**配对

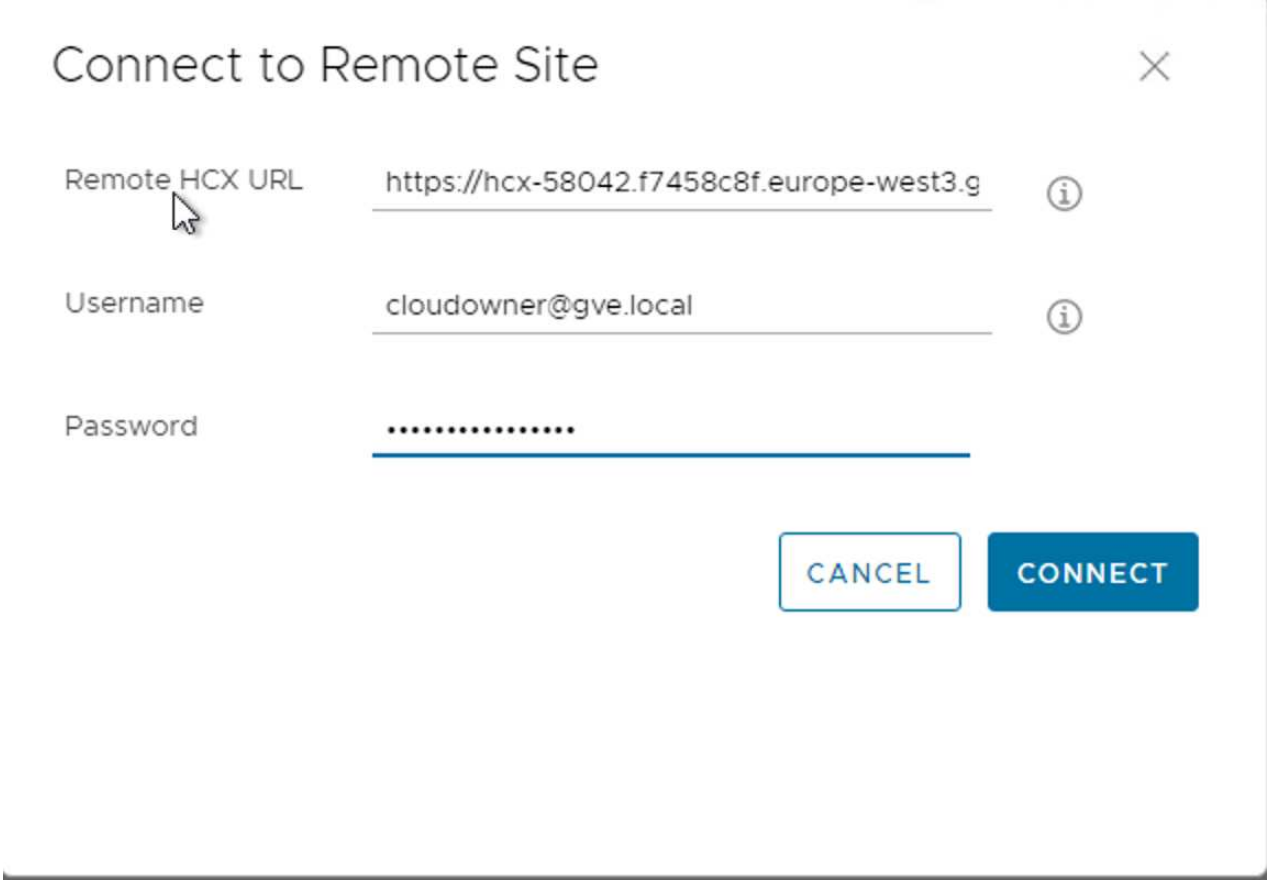
在内部vCenter上部署和配置HCX Connector后、通过添加配对来建立与Cloud Manager的连接。要配置站点配对、请完成以下步骤：

1. 要在内部vCenter环境和Google Cloud VMware Engine SDDC之间创建站点对、请登录到内部vCenter Server并访问新的HCX vSphere Web Client插件。



2. 在基础架构下、单击*添加站点配对*。

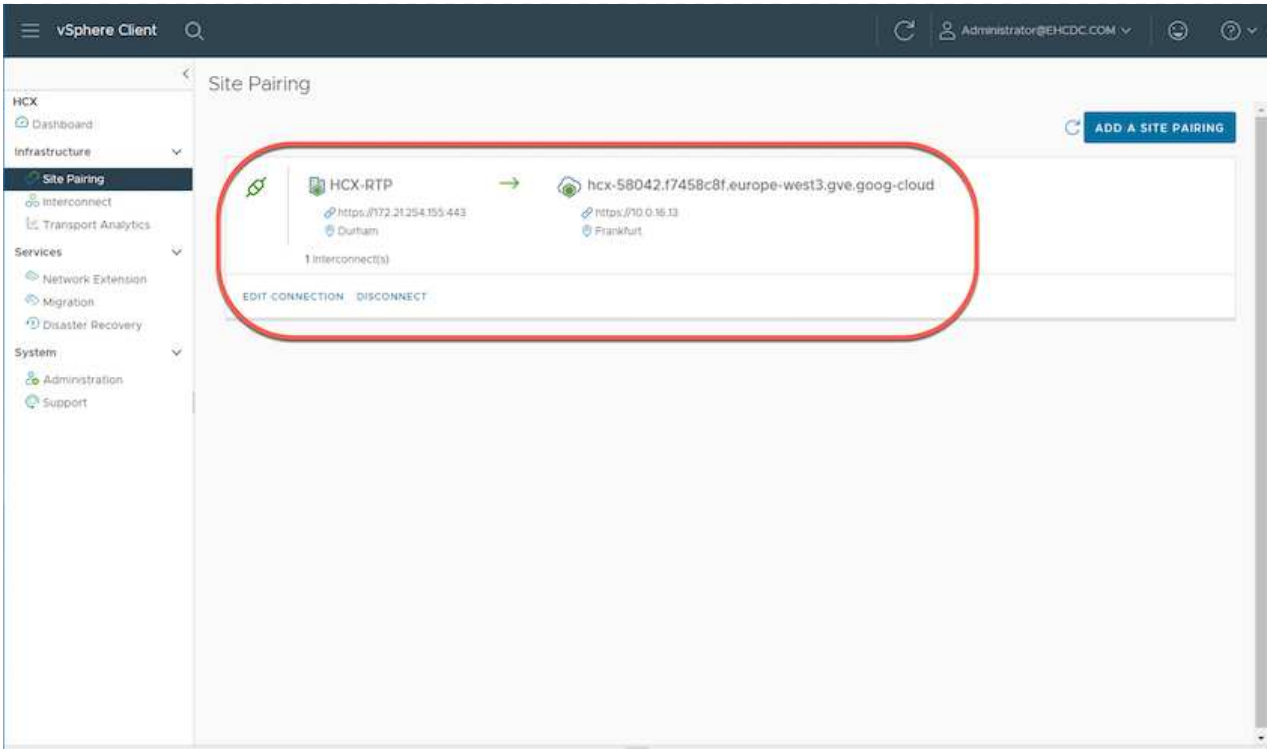
输入拥有云所有者角色特权的用户访问私有云的Google Cloud VMware Engine HCX Cloud Manager URL或IP地址以及凭据。



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、新配置的站点配对将显示在HCX信息板上。

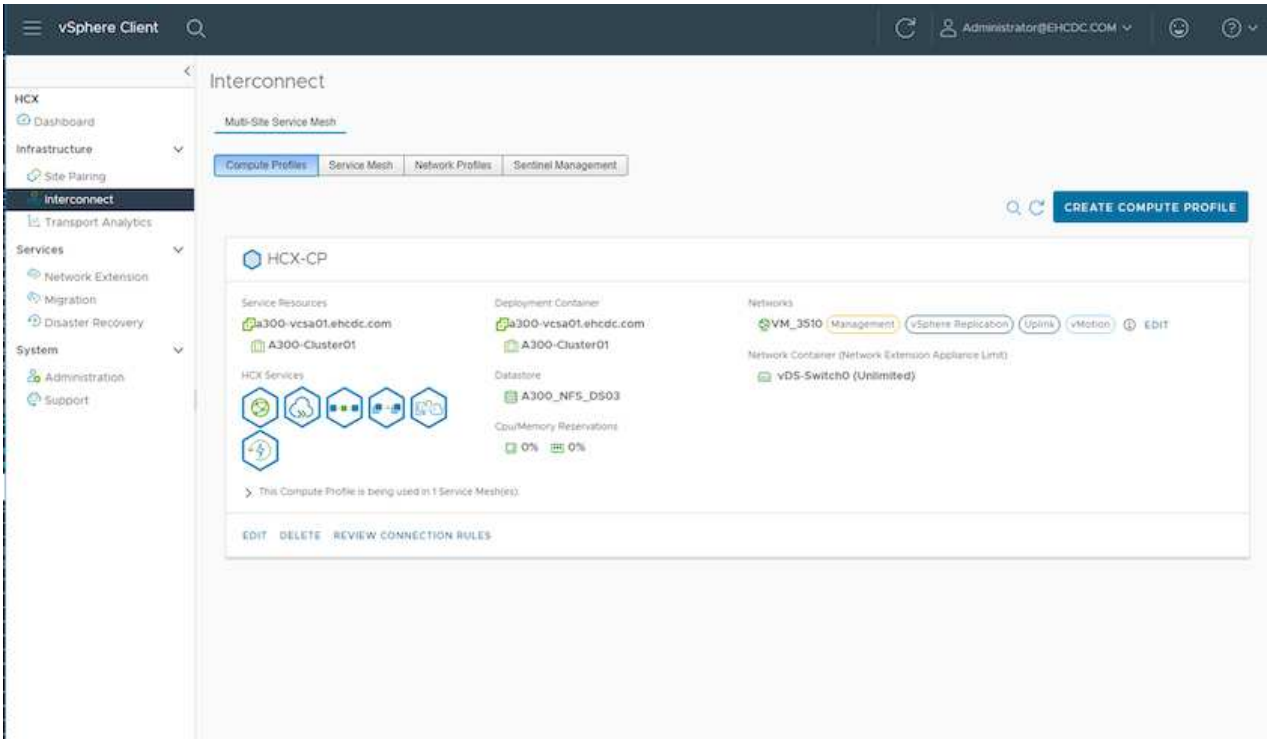

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

第**5**步：配置网络配置文件、计算配置文件和服务网格

VMware HCX互连服务设备可通过Internet以及与目标站点的专用连接提供复制和基于vMotion的迁移功能。互连可提供加密、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. 在基础架构下、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*。

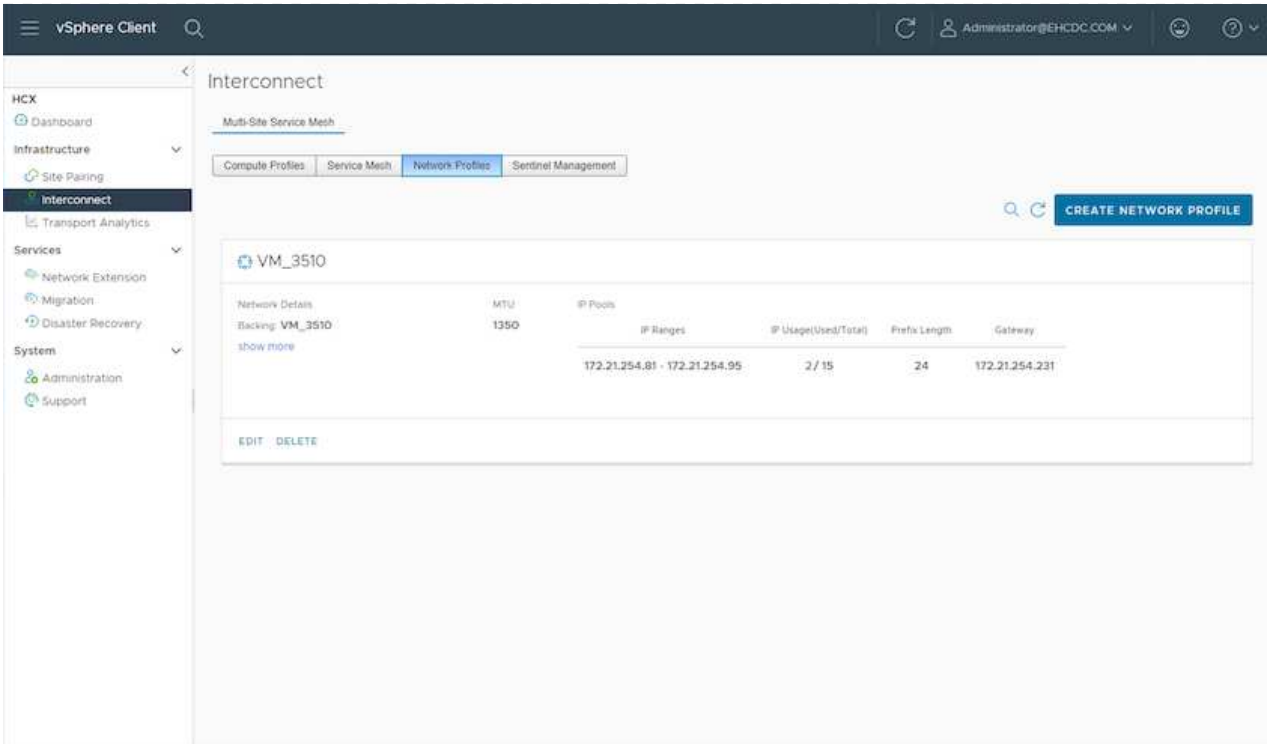
   计算配置文件定义了部署参数、包括部署的设备以及HCL服务可访问的VMware数据中心的哪个部分。



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。

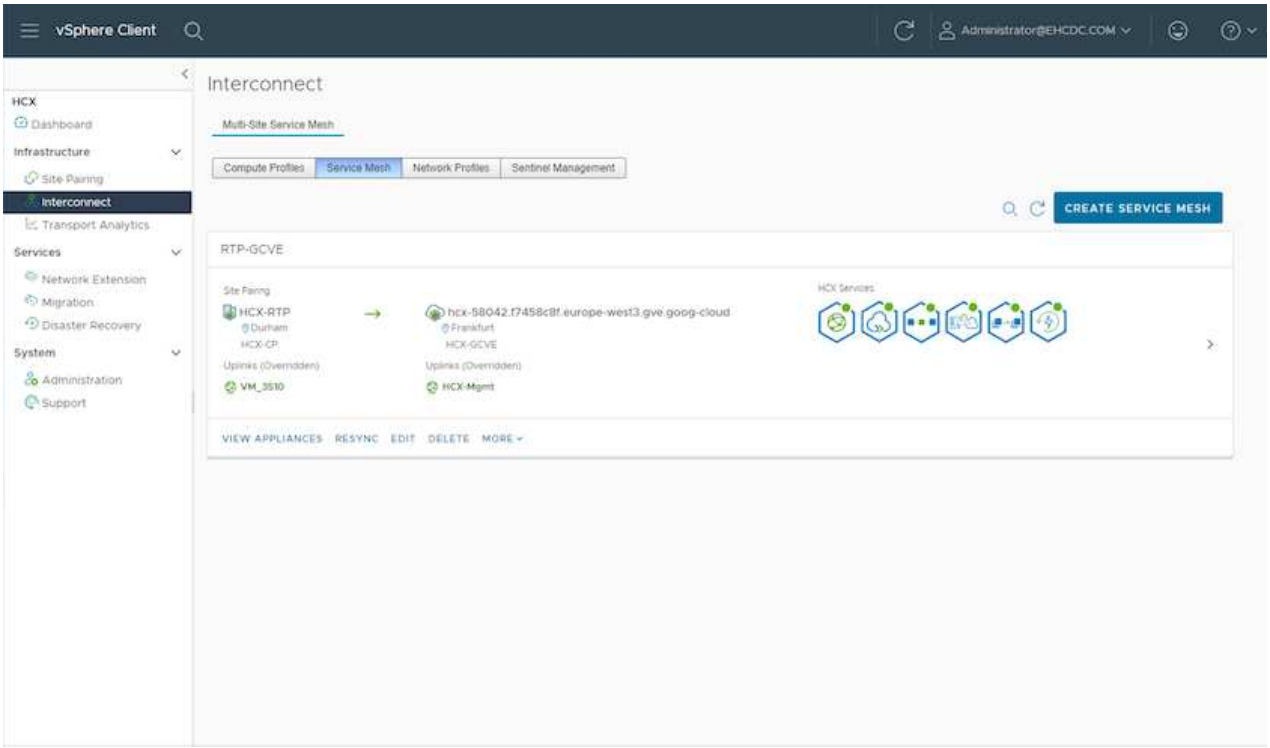
   网络配置文件定义了HCX用于其虚拟设备的IP地址和网络范围。

   此步骤需要两个或更多IP地址。这些IP地址将从管理网络分配给互连设备。

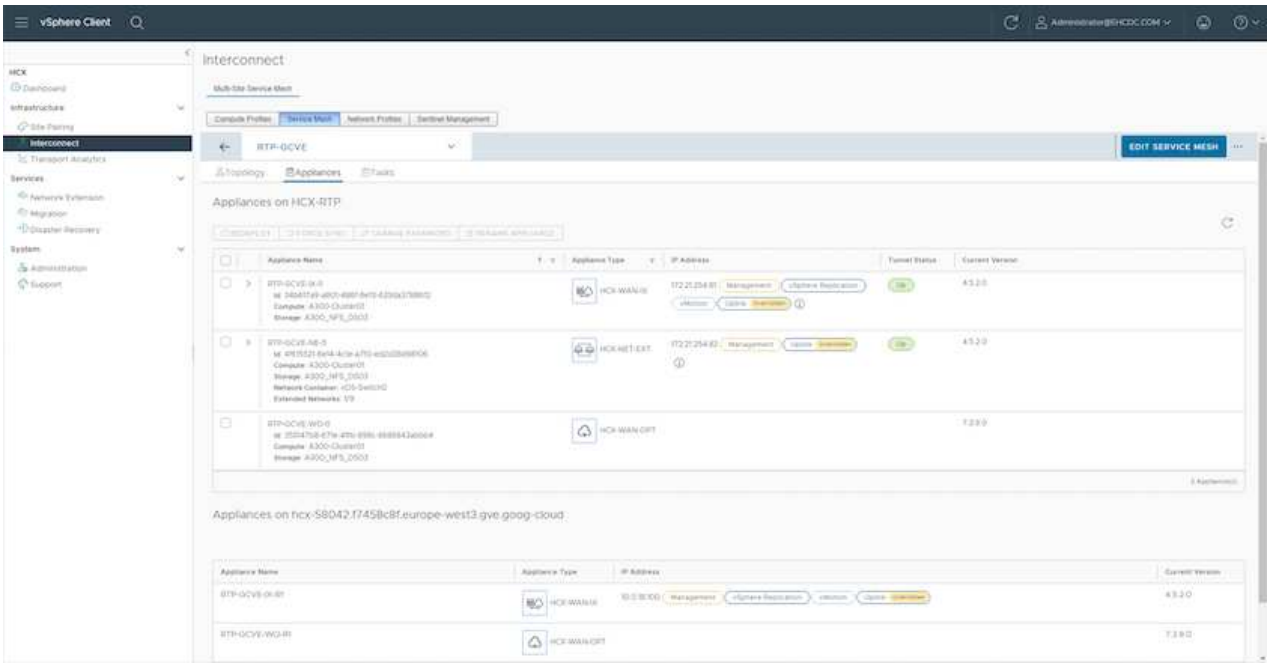


3. 此时、已成功创建计算和网络配置文件。
4. 在*互连*选项中选择*服务网格*选项卡以创建服务网格、然后选择内部站点和GCVE SDDC站点。
5. 服务网格用于指定本地和远程计算和网络配置文件对。

> 在此过程中、源站点和目标站点都会部署并自动配置HCX设备、以便创建安全的传输网络结构。



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、环境便已准备就绪、可以成功创建IPsec通道来迁移工作负载VM。



第6步：迁移工作负载

可以使用各种VMware HCX迁移技术在内部部署和GCVE SDDC之间双向迁移工作负载。可以使用多种迁移技术将VM移入和移出VMware HCX激活的实体、例如HCX批量迁移、HCX vMotion、HCX冷迁移、HCX复制辅助vMotion (适用于HCX Enterprise版本)和HCX操作系统辅助迁移(适用于HCX Enterprise版本)。

要了解有关各种HCX迁移机制的更多信息、请参见 "VMware HCX迁移类型"。

HCX-IX设备使用移动代理服务执行vMotion、冷迁移和复制辅助vMotion (RAV)迁移。

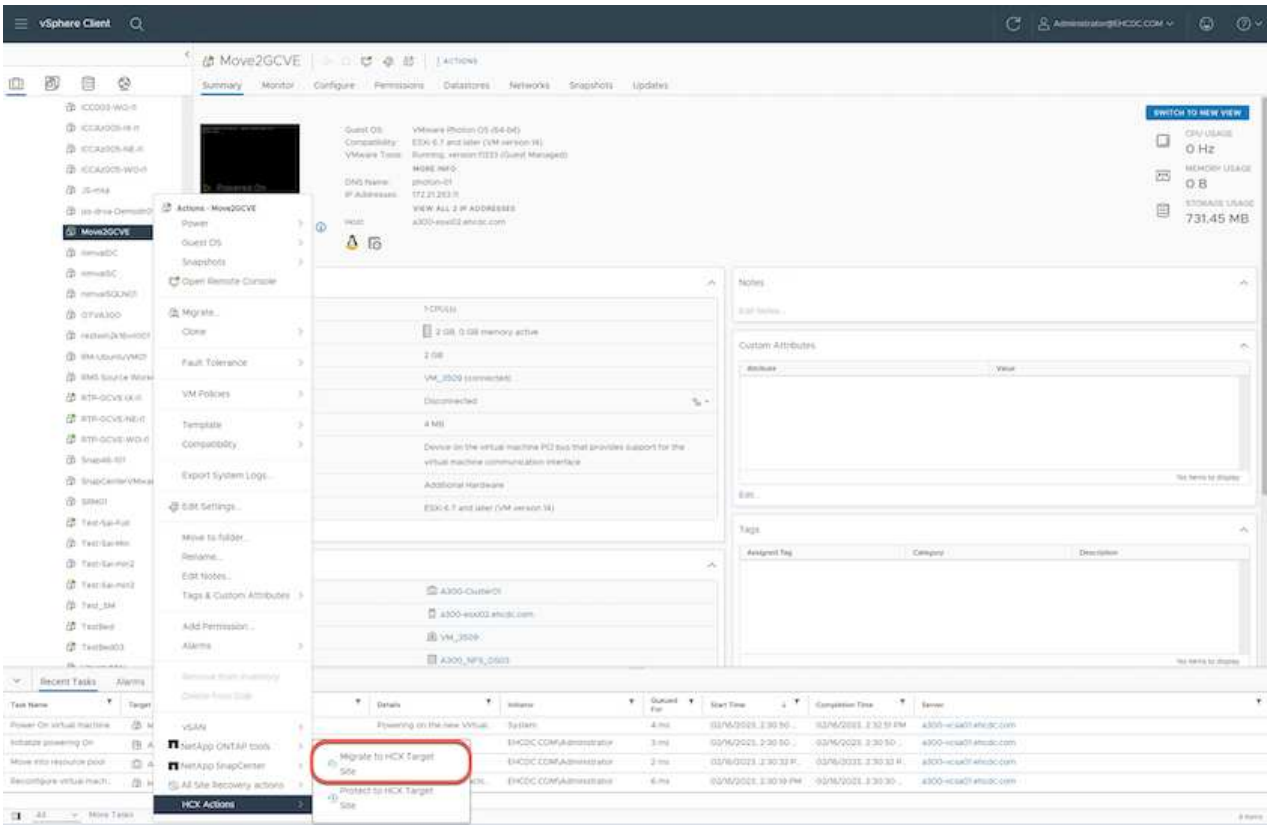
HCX-IX设备会将移动代理服务添加为vCenter Server中的主机对象。此对象上显示的处理器、内存、存储和网络资源并不表示托管IX设备的物理虚拟机管理程序上的实际消耗量。

- HCX vMotion*

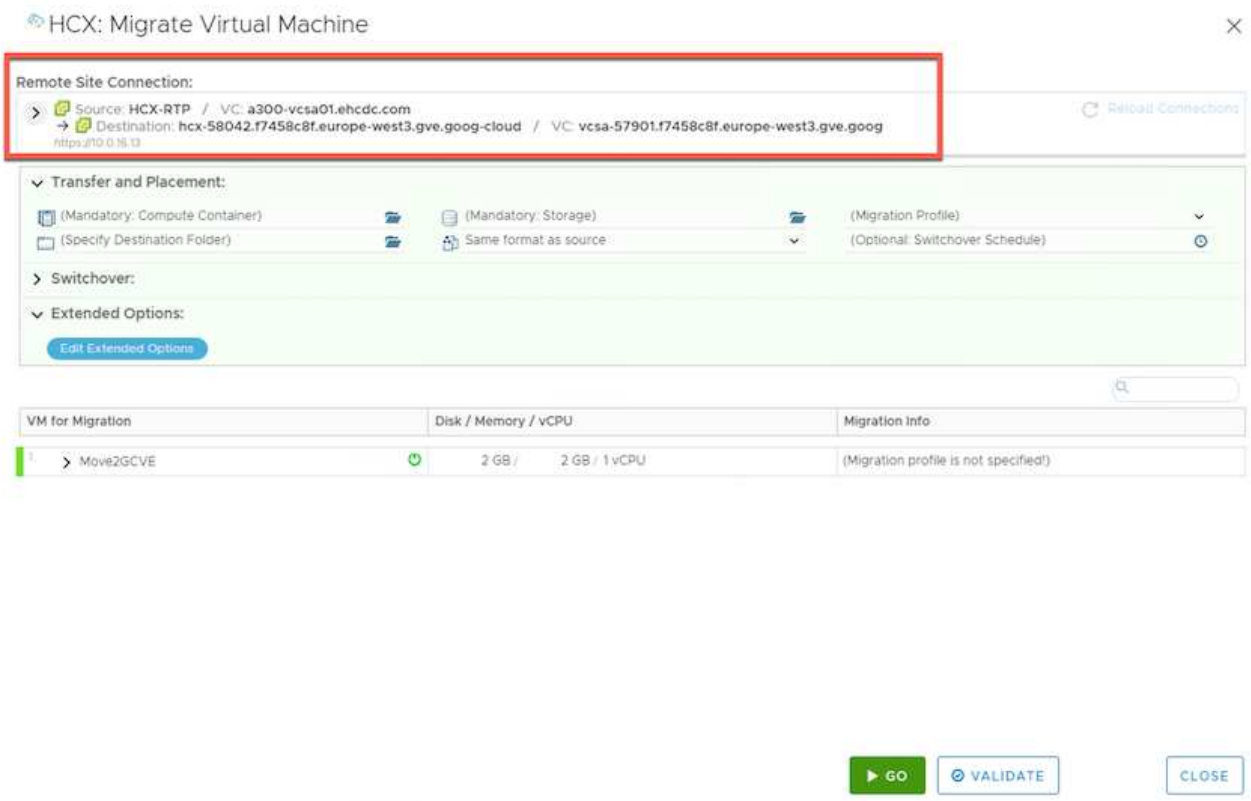
本节介绍HCX vMotion机制。此迁移技术使用VMware vMotion协议将VM迁移到GCVE。vMotion迁移选项用于一次迁移单个VM的VM状态。此迁移方法期间不会发生服务中断。

应设置网络扩展(对于VM所连接的端口组)、以便在不更改IP地址的情况下迁移VM。

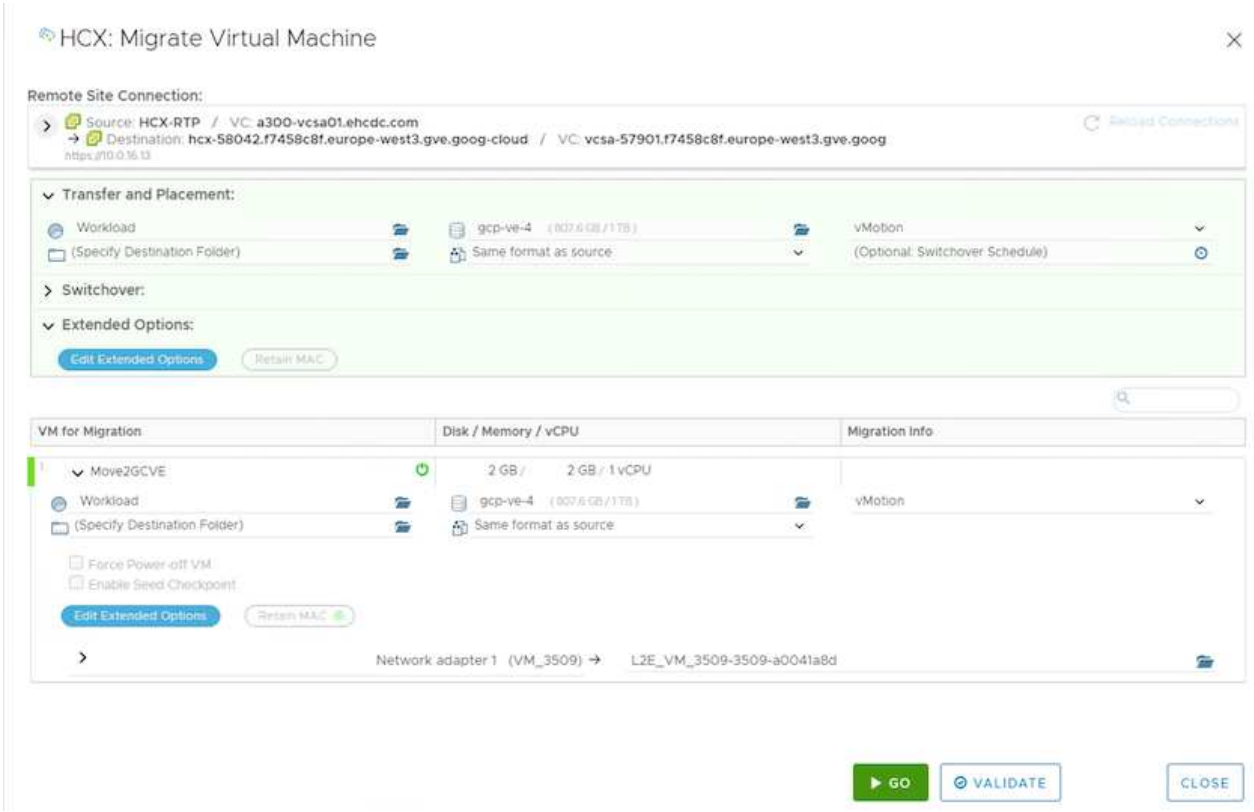
1. 从内部vSphere客户端中、转到清单、右键单击要迁移的虚拟机、然后选择HCX操作>迁移到HCX目标站点。



2. 在迁移虚拟机向导中、选择远程站点连接(目标GCVE)。



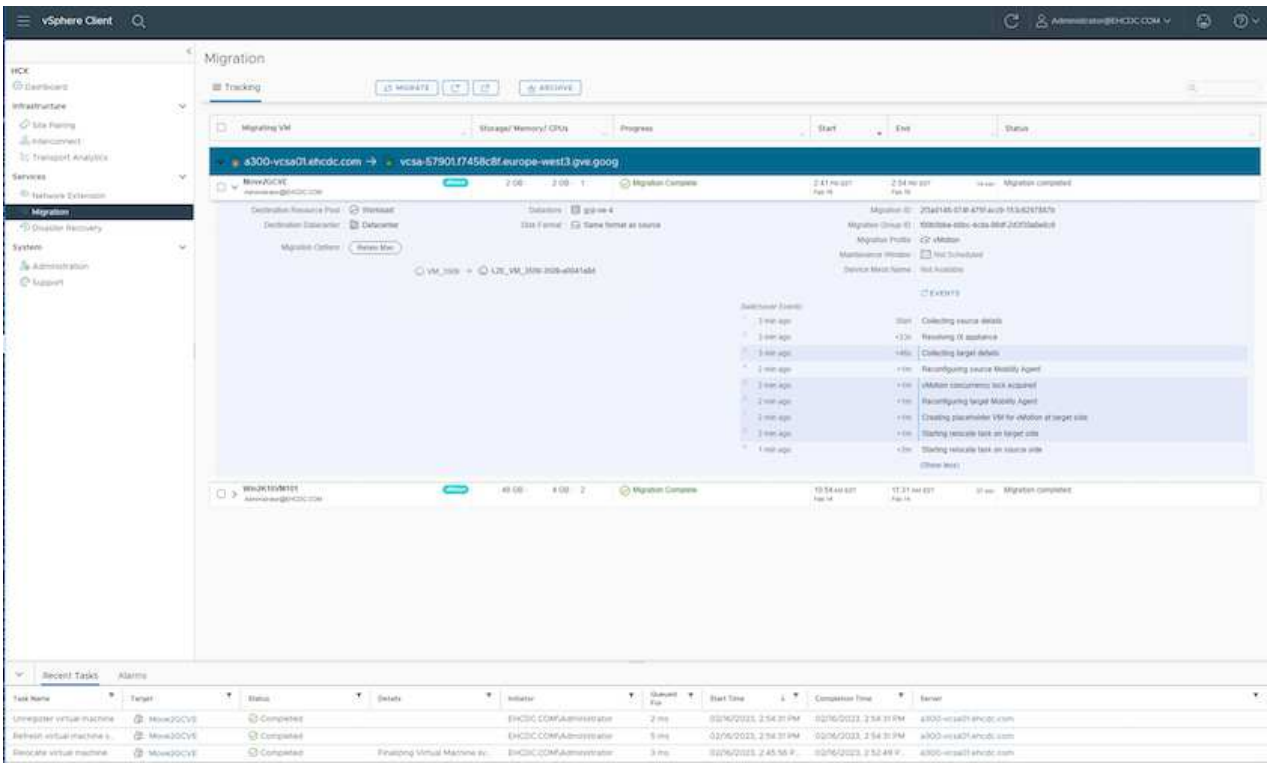
3. 更新必填字段(集群、存储和目标网络)、然后单击验证。



4. 验证检查完成后、单击"Go"启动迁移。

vMotion传输会捕获VM活动内存、其执行状态、IP地址及其MAC地址。有关HCX vMotion的要求和限制的详细信息、请参见 "了解VMware HCX vMotion和冷迁移"。

5. 您可以从"HCX">"迁移"信息板监控vMotion的进度和完成情况。



目标CVS NFS数据存储库应具有足够的空间来处理迁移。

结论

无论您的目标是全云还是混合云、以及驻留在内部任何类型/供应商存储上的数据、Cloud Volume Service和HCX都可以提供出色的选项来部署和迁移应用程序工作负载、同时通过将数据需求无缝地迁移到应用程序层来降低TCO。无论使用何种情形、都可以选择Google Cloud VMware Engine以及Cloud Volume Service、以便快速实现云优势、一致的基础架构以及跨内部和多个云的运营、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甚至网络文件复制(Network File Copy、NFCs)连接存储和迁移VM时、使用的过程与步骤相同。

要点总结

本文档的要点包括：

- 现在、您可以在Google Cloud VMware Engine SDDC上使用Cloud Volume Service作为数据存储库。
- 您可以轻松地将数据从内部迁移到Cloud Volume Service数据存储库。
- 您可以轻松地扩展和缩减Cloud Volume Service数据存储库、以满足迁移活动期间的容量和性能要求。

Google和VMware提供的视频供参考

来自**Google**

- "使用GCVE部署HCX Connector"
- "使用GCVE配置HCX ServiceMesh"
- "将具有HCX的VM迁移到GCVE"

来自**VMware**

- "适用于GCVE的HCX Connector部署"
- "适用于GCVE的HCX ServiceMeshy配置"
- "HCX工作负载迁移到GCVE"

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请访问以下网站链接：

- Google Cloud VMware Engine文档

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service文档

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- 《VMware HCX用户指南》

  "https://docs.vmware.com/en/VMware-HCX/index.html"

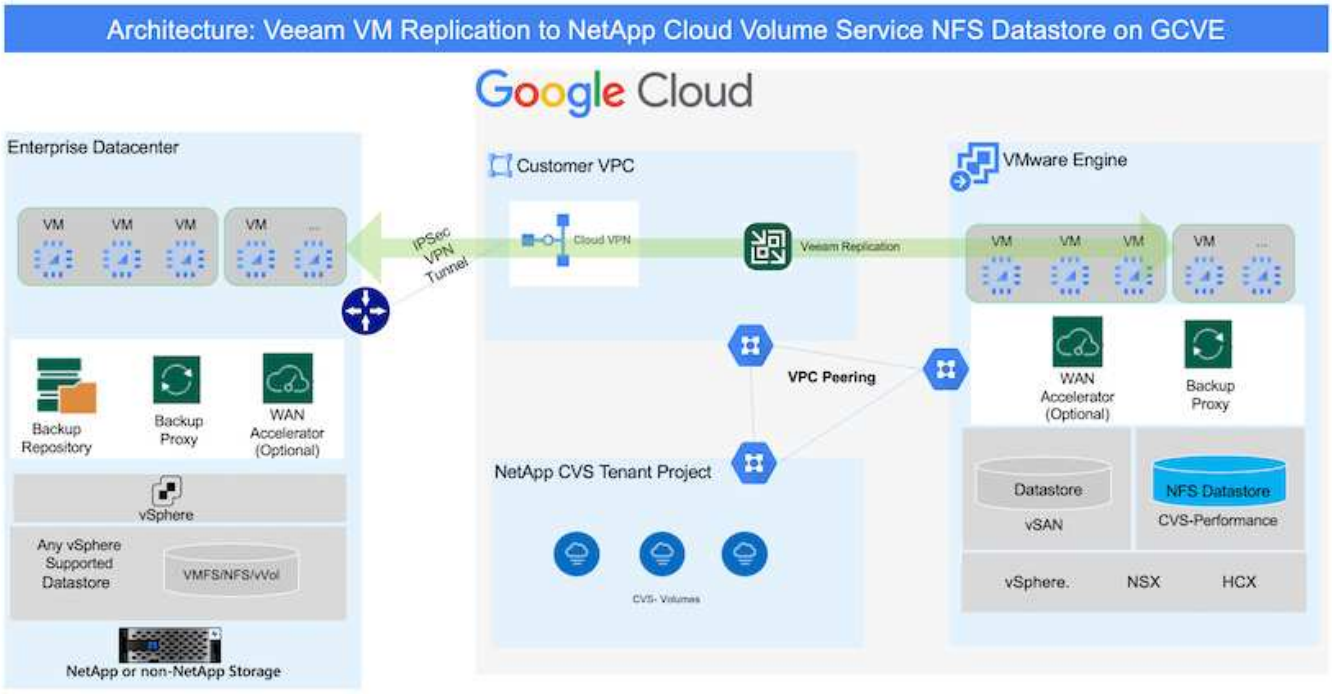
使用**Veeam**复制功能将**VM**迁移到**Google Cloud VMware Engine**上的**NetApp**云卷服务**NFS**数据存储库

概述

作者：NetApp公司Suresh ThopPay

可以利用Veeam复制功能将VMware vSphere上运行的VM工作负载迁移到Google Cloud VMware Engine (GCVE)。

本文档提供了一种使用NetApp云卷服务、Veeam和Google Cloud VMware引擎(GCVe)设置和执行VM迁移的分步方法。



假设

本文档假设您已具备Google Cloud VPN或Cloud Inter连 或其他网络选项、可用于建立从现有vSphere服务器到Google Cloud VMware Engine的网络连接。

> 将内部数据中心连接到Google Cloud有多种方式、这使我们无法在本文档中概述特定工作流。请参见 "Google Cloud文档" 了解适当的内部到Google连接方法。

部署迁移解决方案

解决方案 部署概述

1. 确保NetApp云卷服务中的NFS数据存储库已挂载到GCVe vCenter上。
2. 确保在现有VMware vSphere环境中部署Veeam Backup Recovery
3. 创建复制作业以开始将虚拟机复制到Google Cloud VMware Engine实例。
4. 对Veeam复制作业执行故障转移。
5. 在Veeam上执行永久故障转移。

部署详细信息

确保**NetApp**云卷服务中的**NFS**数据存储库已挂载到**GCVe vCenter**上

登录到GCVEvCenter并确保具有足够空间的NFS数据存储库可用。
如果不是、请参见 "将NetApp CVS挂载为GCVE)上的NFS数据存储库"

确保在现有**VMware vSphere**环境中部署**Veeam Backup Recovery**

请参阅 "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。

内部vCenter和GCVE vCenter都需要向Veeam注册。 "设置vSphere VM复制作业"
下面是一个介绍如何操作的视频
"配置复制作业"。

副本VM可以与源VM具有不同的IP、也可以连接到不同的端口组。有关更多详细信息、请观看上面的视频。

对**Veeam**复制作业执行故障转移

要迁移VM、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

- 可以利用现有Veeam备份基础架构进行迁移。
- Veeam Replication允许更改目标站点上的VM IP地址。
- 能够重新映射从Veeam外部复制的现有数据(例如从BlueXP复制的数据)
- 能够在目标站点上指定不同的网络端口组。
- 可以指定VM的启动顺序。
- 利用VMware变更块跟踪最大限度地减少通过WAN发送的数据量。
- 能够执行复制前和后脚本。
- 能够为快照执行前处理脚本和后处理脚本。

区域可用性—**Google Cloud Platform (GCP)**的补充**NFS**数据存储库

NetApp云卷服务支持GCVe的补充NFS数据存储库。

GCVENFS数据存储库只能使用CVS性能卷。
有关可用位置、请参见 "全球区域地图"

Google Cloud VMware Engine可从以下位置获得
为了最大限度地减少延迟、NetApp CVS卷和要挂载该卷的GCVe应位于同一可用性区域。
与Google和NetApp 解决方案 架构师合作、实现可用性和TCO优化。

安全概述—Google Cloud中的NetApp Cloud Volumes Service (CVS)

TR-4918：安全概述—**Google Cloud**中的**NetApp Cloud Volumes Service**

NetApp公司Justin Parisi的Oliver Krause

文档范围

安全性、尤其是在基础架构不受存储管理员控制的云环境中、对于将数据信任到云提供商提供的服务产品至关重要。本文档概述了NetApp提供的安全产品 "Cloud Volumes Service 在Google Cloud中提供"。

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
- 业务决策者

如果您对本技术报告的内容有任何疑问、请参见一节 ""联系我们。""

缩写	定义
CVS-SW	Cloud Volumes Service 、服务类型CVS
CVS 性能	Cloud Volume Service、服务类型CVS-Performance
PSA	

Google Cloud中的**Cloud Volumes Service** 如何保护您的数据安全

Google Cloud中的Cloud Volumes Service 提供了多种本机保护数据安全的方法。

安全架构和租户模式

Cloud Volumes Service 通过在不同端点之间分段服务管理(控制平面)和数据访问(数据平面)、在Google Cloud中提供一个安全的架构、这样两者都不会影响另一端(请参见一节) "Cloud Volumes Service 架构"）。它使用Google "私有服务访问" (PSA)提供服务的框架。此框架区分由NetApp提供和运营的服务生产者和客户项目中托管要访问Cloud Volumes Service 文件共享的客户端的虚拟私有云(Virtual Private Cloud、VPC)服务使用者。

在此架构中、租户(请参见第节 ""租户模式"")定义为除非用户明确连接、否则彼此完全隔离的Google Cloud项目。通过租户、可以使用Cloud Volumes Service 卷平台将数据卷、外部名称服务以及解决方案 的其他基本部分与其他租户完全隔离。由于Cloud Volumes Service 平台是通过VPC对等连接的、因此这种隔离也会对其进行适用场景。您可以使用共享VPC在多个项目之间共享Cloud Volumes Service 卷(请参见一节) ""共享VPC""）。您可以对SMB共享和NFS导出应用访问控制、以限制可以查看或修改数据集的用户或对象。

为控制平台提供强大的身份管理功能

在进行Cloud Volumes Service 配置的控制平面中、身份管理通过进行管理 "身份访问管理(IAM)"。IAM是一项标

准服务、可用于控制对Google Cloud项目实例的身份验证(登录)和授权(权限)。所有配置都使用Cloud Volumes Service API通过使用TLS 1.2加密的安全HTTPS传输执行、而身份验证则使用JWT令牌执行、以提高安全性。适用于Cloud Volumes Service 的Google控制台UI可将用户输入转换为Cloud Volumes Service API调用。

安全强化—限制攻击面

有效安全性的一部分是限制服务中可用的攻击面数。攻击面可能包括各种内容、包括空闲数据、正在传输的数据、登录信息以及数据集本身。

托管服务可从其设计中消除某些固有的攻击面。基础架构管理、如一节所述 ""服务操作"、" 由专门的团队处理、并可自动执行、以减少人员实际接触配置的次数、从而有助于减少有意和无意的错误数量。网络隔离、以便只有必要的服务才能彼此访问。加密会插入到数据存储中、只有数据平面需要Cloud Volumes Service 管理员的安全注意。通过隐藏API接口背后的大部分管理内容、可通过限制攻击面来实现安全性。

零信任模式

过去、IT安全理念一直是信任、但要进行验证、这种理念表现为仅依靠外部机制(例如防火墙和入侵检测系统)来缓解威胁。但是、攻击和违规行为演变成通过网络钓鱼、社交工程、内部威胁以及其他验证方法绕过环境中的验证、从而进入网络并造成严重破坏。

Zero Trust已成为一种全新的安全方法、目前的口号是"不信任任何内容、但仍需验证一切"。 因此、默认情况下不允许访问任何内容。此命令可通过多种方式实施、包括标准防火墙和入侵检测系统(IDS)以及以下方法：

- 强大的身份验证方法(例如AES加密的Kerberos或JWT令牌)
- 单一强身份源(例如Windows Active Directory、轻型目录访问协议(LDAP)和Google IAM)
- 网络分段和安全多租户(默认情况下仅允许租户访问)
- 采用最低特权访问策略的粒度访问控制
- 拥有数字审核和纸质跟踪的一小部分专属管理员

在Google Cloud中运行的Cloud Volumes Service 通过实施"不信任、不验证一切"的立场、遵循零信任模式。

加密

对空闲数据进行加密(请参见一节 ""空闲数据加密"") ""SMB加密"" 或NFS Kerberos 5p支持。您可以轻松了解跨区域复制传输是否受TLS 1.2加密保护(请参见一节 ""跨区域复制"") 。此外、Google网络还提供加密通信(请参见一节 ""传输中的数据加密"")、以添加抵御攻击的保护层。有关传输加密的详细信息、请参见一节 ""Google Cloud network""。

数据保护和备份

安全性不仅仅是为了防止攻击。此外、还需要了解我们如何从发生的攻击中恢复。此策略包括数据保护和备份。Cloud Volumes Service 提供了在发生中断时复制到其他区域的方法(请参见一节 ""跨区域复制"")或数据集受勒索软件攻击影响时。此外、它还可以使用将数据异步备份到Cloud Volumes Service 实例以外的位置 "Cloud Volumes Service 备份"。通过定期备份、减少安全事件所需的时间、为管理员节省资金并提高效率。

利用行业领先的**Snapshot**副本快速减少勒索软件

除了数据保护和备份之外、Cloud Volumes Service 还支持不可变的Snapshot副本(请参见一节) ""不可变的Snapshot副本"")允许从勒索软件攻击中恢复的卷(请参见一节 ""服务操作"")在发现问题描述 后数秒内完成、中断最少。恢复时间和影响取决于Snapshot计划、但您可以创建Snapshot副本、在勒索软件攻击中只能提供一小时的增量。Snapshot副本对性能和容量使用的影响微乎其微、是一种低风险、高回报的数据集保护方法。

了解如何保护数据安全的第一步是识别风险和潜在的攻击面。

其中包括(但不限于)以下内容：

- 管理和登录
- 空闲数据
- 数据正在传输
- 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环境。Google Cloud中的Cloud Volumes Service 已经考虑了其中许多主题、并在默认情况下实施了安全功能、而无需任何管理交互。

确保安全登录

在保护关键基础架构组件安全时、必须确保只有经过批准的用户才能登录和管理您的环境。如果不良行为者违反您的管理凭据、则他们将拥有存储区的密钥、并可以执行所需的任何操作—更改配置、删除卷和备份、创建后台或禁用Snapshot计划。

Cloud Volumes Service for Google Cloud可通过将存储即服务(StaaS)混淆来防止未经授权的管理登录。Cloud Volumes Service 由云提供商完全维护、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、除了极少数情况之外、人工管理员不必与系统进行交互。

如果需要登录、Google Cloud中的Cloud Volumes Service 会保留一个非常短的可访问登录到系统的可信管理员列表、从而确保登录安全。这种关守有助于减少具有访问权限的潜在不良行为者的数量。此外、Google Cloud网络还会将系统隐藏在网络层安全的基础之上、并仅向外部环境公开所需的内容。有关Google Cloud、Cloud Volumes Service 架构的信息、请参见一节 "Cloud Volumes Service 架构。"

集群管理和升级

存在潜在安全风险的两个方面包括集群管理(如果不良者拥有管理员访问权限会发生什么情况)和升级(如果软件映像受到影响会发生什么情况)。

存储管理保护

以服务形式提供的存储可通过删除云数据中心以外的最终用户的访问权限、消除管理员面临的额外风险。而是只为客户的数据访问平面进行配置。每个租户都管理自己的卷、任何租户都无法访问其他Cloud Volumes Service 实例。此服务通过自动化进行管理、只需一小部分受信任管理员即可通过本节所述的流程访问系统 ""服务操作"。"

CVS-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其他区域提供数据保护。在这种情况下、可以将Cloud Volumes Service 故障转移到不受影响的区域以保持数据访问。

服务升级

更新有助于保护容易受到攻击的系统。每个更新都提供了安全增强功能和错误修复、可最大限度地减少攻击面。软件更新会从中央存储库下载并进行验证、然后才允许更新、以验证是否使用了官方映像、以及升级是否不会受到不良行为者的影响。

借助Cloud Volumes Service 、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来消除管理员团队面临的风险、这些专家已经对流程进行了自动化和全面测试。升级不会造成中断、Cloud Volumes Service 会维护最新的更新、以获得最佳的整体效果。

有关执行这些服务升级的管理员团队的信息、请参见一节 ""服务操作"。"

保护空闲数据的安全

空闲数据加密对于在磁盘被盗、退回或重新利用时保护敏感数据非常重要。Cloud Volumes Service 中的数据通过基于软件的加密在空闲时受到保护。

- Google生成的密钥用于CVS-SW。
- 对于CVS-Performance、每个卷的密钥存储在Cloud Volumes Service 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。请参见 "FIPS 140-2证书#4144"。

自2021年11月起、CVS-Performance提供了客户管理的预览加密(CMEK)功能。通过此功能、您可以使用Google密钥管理服务(KMS)中托管的每个项目、每个区域的主密钥对每个卷的密钥进行加密。您可以通过Kms连接外部密钥管理器。

有关如何为KMS配置CVS-Performance的详细信息、 "请参见Cloud Volumes Service 文档"。

有关架构的详细信息、请参见一节 "Cloud Volumes Service 架构。"

保护传输中的数据安全

除了保护空闲数据之外、当数据在Cloud Volumes Service 实例与客户端或复制目标之间传输时、您还必须能够保护数据的安全。Cloud Volumes Service 通过使用加密方法(例如使用Kerberos进行SMB加密、对数据包进行签名/密封以及对数据传输进行端到端加密的NFS Kerberos 5p)为通过NAS协议传输的数据提供加密。

Cloud Volumes Service 卷的复制使用TLS 1.2、它会利用AES-GCM加密方法。

默认情况下、大多数不安全的传输中协议(例如telnet、NDMP等)都处于禁用状态。但是、Cloud Volumes Service 不会对DNS进行加密(不支持DNS安全)、应尽可能使用外部网络加密进行加密。请参见一节 ""传输中的数据加密"" 有关保护传输中数据的详细信息、请参见。

有关NAS协议加密的信息、请参见一节 ""NAS协议"。"

NAS权限的用户和组

在云中保护数据的一部分工作涉及到正确的用户和组身份验证、其中、访问数据的用户会作为环境中的实际用户进行验证、而组包含有效用户。这些用户和组可为存储系统中的文件和文件夹提供初始共享和导出访问权限以及权限验证。

Cloud Volumes Service 对SMB共享和Windows模式权限使用基于Active Directory的标准Windows用户和组身份验证。该服务还可以利用UNIX身份提供程序、例如用于UNIX用户的LDAP以及用于NFS导出的组、NFSv4 ID验证、Kerberos身份验证和NFSv4 ACL。

目前、Cloud Volumes Service 仅支持Active Directory LDAP功能。

检测、防止和缓解勒索软件、恶意软件和病毒

勒索软件、恶意软件和病毒是管理员面临的持久威胁、企业组织始终将检测、预防和缓解这些威胁作为头等大事。关键数据集上的一个勒索软件事件可能会导致数百万美元的损失、因此您可以尽最大可能降低风险。

尽管Cloud Volumes Service 目前不包括防病毒保护或等原生 检测或预防措施 "自动检测勒索软件"、通过启用定期Snapshot计划、可以快速从勒索软件事件中恢复。Snapshot副本是指向文件系统中已更改块的不可变和只读指针、它们接近瞬时、对性能的影响最小、并且仅在更改或删除数据时才会占用空间。您可以为Snapshot副本设置计划、使其与所需的可接受恢复点目标(RPO)/恢复时间目标(RTO)相匹配、并且每个卷最多可保留1、024个Snapshot副本。

Snapshot支持包括在Cloud Volumes Service 中、无需额外费用(对于Snapshot副本所保留的更改块/数据收取的数据存储费用除外)、如果发生勒索软件攻击、可以在攻击发生之前使用它回滚到Snapshot副本。快照还原只需几秒钟即可完成、然后您可以恢复正常提供数据。有关详细信息，请参见 "适用于勒索软件的NetApp解决方案"。

要防止勒索软件影响您的业务、需要采用多层方法、其中包括以下一项或多项：

- 端点保护
- 通过网络防火墙防止外部威胁
- 检测数据异常
- 对关键数据集进行多个备份(现场和异地)
- 定期对备份进行还原测试
- 不可变的只读NetApp Snapshot副本
- 关键基础架构的多因素身份验证
- 系统登录的安全审核

此列表远非详尽无遗、但在应对潜在的勒索软件攻击时、是一个理想的蓝图。Google Cloud中的Cloud Volumes Service 提供了多种方法来防止勒索软件事件并减少其影响。

不可变的**Snapshot**副本

Cloud Volumes Service 本机提供不可变的只读Snapshot副本、这些副本会按照可自定义的计划创建、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。根据Snapshot计划和RTO /RO的保留期限、将Snapshot还原到先前的正常Snapshot副本速度非常快、并可最大程度地减少数据丢失。Snapshot技术对性能的影响可以忽略不计。

由于Cloud Volumes Service 中的Snapshot副本为只读副本、因此、除非勒索软件在未经注意的情况下激增到数据集中、并且已为受勒索软件感染的数据创建Snapshot副本、否则它们不会受到勒索软件的感染。因此、您还必须考虑根据数据异常检测勒索软件。Cloud Volumes Service 目前不提供本机检测功能、但您可以使用外部监控软件。

备份和还原

Cloud Volumes Service 提供标准NAS客户端备份功能(例如通过NFS或SMB进行备份)。

- CVS-Performance可跨区域卷复制到其他CVS-Performance卷。有关详细信息，请参见 "卷复制" 在Cloud Volumes Service 文档中。
- CVS-SW提供服务本机卷备份/还原功能。有关详细信息，请参见 "云备份" 在Cloud Volumes Service 文档

中。

卷复制可提供源卷的精确副本、以便在发生灾难(包括勒索软件事件)时快速进行故障转移。

跨区域复制

通过CVS-Performance、您可以在NetApp控制的后端服务网络上使用用于在Google网络上运行复制的特定接口使用TLS1.2 AES 256 GCM加密功能、在Google Cloud区域之间安全地复制卷、以实现数据保护和归档使用情形。主(源)卷包含活动生产数据、并复制到二级(目标)卷、以提供主数据集的精确副本。

初始复制会传输所有块、但更新仅传输主卷中发生更改的块。例如、如果将主卷上的1 TB数据库复制到二级卷、则在初始复制时会传输1 TB的空间。如果该数据库中有几百行(假设有几MB)在初始化和下次更新之间发生变化、则只有包含更改行的块才会复制到二级(几MB)。这有助于确保传输时间保持较短、并降低复制成本。

文件和文件夹上的所有权限都会复制到二级卷、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时、目标站点应利用相同的名称服务和Active Directory域连接、以便一致地处理用户和组身份和权限。如果发生灾难、您可以使用二级卷作为故障转移目标、方法是中断复制关系、从而将二级卷转换为读写卷。

卷副本为只读副本、可为异地数据提供不可变的副本、以便在病毒已感染数据或勒索软件已对主数据集进行加密的情况下快速恢复数据。只读数据不会加密、但如果主卷受到影响并发生复制、则受感染的块也会进行复制。您可以使用不受影响的旧Snapshot副本进行恢复、但SLA可能会超出承诺的RTO /RRPO范围、具体取决于检测到攻击的速度。

此外、您还可以通过在Google Cloud中进行跨区域复制(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、这些角色会将卷管理员分隔开、这些管理员可以删除源卷、但不会中断镜像、因此无法从无法执行任何卷操作的CRR管理员中删除目标卷。请参见 "安全注意事项" 在Cloud Volumes Service 文档中、了解每个管理员组允许的权限。

Cloud Volumes Service 备份

虽然Cloud Volumes Service 可提供较高的数据持久性、但外部事件可能会导致发生原因 数据丢失。在发生病毒或勒索软件等安全事件时、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Cloud Volumes Service 卷。或者、用户只希望将数据的备份版本保留数月、而在卷中保留额外的Snapshot副本空间将成为一项成本难题。虽然Snapshot副本应该是在过去几周内保留备份版本以恢复其丢失的数据的首选方式、但它们位于卷中、如果卷消失、它们将丢失。

出于所有这些原因、NetApp Cloud Volumes Service 均通过提供备份服务 "Cloud Volumes Service 备份"。

Cloud Volumes Service 备份会在Google云存储(GCS)上生成卷的副本。它只会备份存储在卷中的实际数据、而不会备份可用空间。它始终以增量形式运行、也就是说、它会一次性传输卷内容、并在上继续备份更改的数据。与具有多个完整备份的传统备份概念相比、它可以节省大量备份存储、从而降低成本。由于与卷相比、备份空间的每月价格更低、因此、它是延长备份版本的理想之选。

用户可以使用Cloud Volumes Service 备份将任何备份版本还原到同一区域内的相同或不同卷。如果删除了源卷、则备份数据会保留下来、需要单独管理(例如删除)。

Cloud Volumes Service 备份内置在Cloud Volumes Service 中作为选项。用户可以通过激活每个卷的Cloud Volumes Service 备份来确定要保护的卷。请参见 "Cloud Volumes Service 备份文档" 有关备份的信息、请参见 "支持的最大备份版本数"、计划和 "定价"。

项目的所有备份数据都存储在GCS存储分段中、此存储分段由服务管理、用户无法看到。每个项目使用不同的存储分段。目前、存储分段与Cloud Volumes Service 卷位于同一区域、但正在讨论更多选项。有关最新状态、

请参见文档。

从Cloud Volumes Service 存储分段到GCS的数据传输使用具有HTTPS和TLS1.2的服务内部Google网络。数据会使用Google管理的密钥在空闲时进行加密。

要管理Cloud Volumes Service 备份(创建、删除和还原备份)、用户必须具有 "角色/netappcloudvolumes.admin" 角色。

架构

概述

信任云解决方案 的一部分是了解架构及其安全保护方式。本节将介绍Google中Cloud Volumes Service 架构的不同方面、以帮助缓解对数据安全保护的潜在担忧、并指出可能需要执行其他配置步骤才能实现最安全的部署。

Cloud Volumes Service 的通用架构可细分为两个主要组件：控制平面和数据平面。

控制面板

Cloud Volumes Service 中的控制平台是由Cloud Volumes Service 管理员和NetApp原生 自动化软件管理的后端基础架构。此平台对最终用户完全透明、并包括网络、存储硬件、软件更新等、可帮助为Cloud Volumes Service 等驻留在云中的解决方案 提供价值。

数据平面

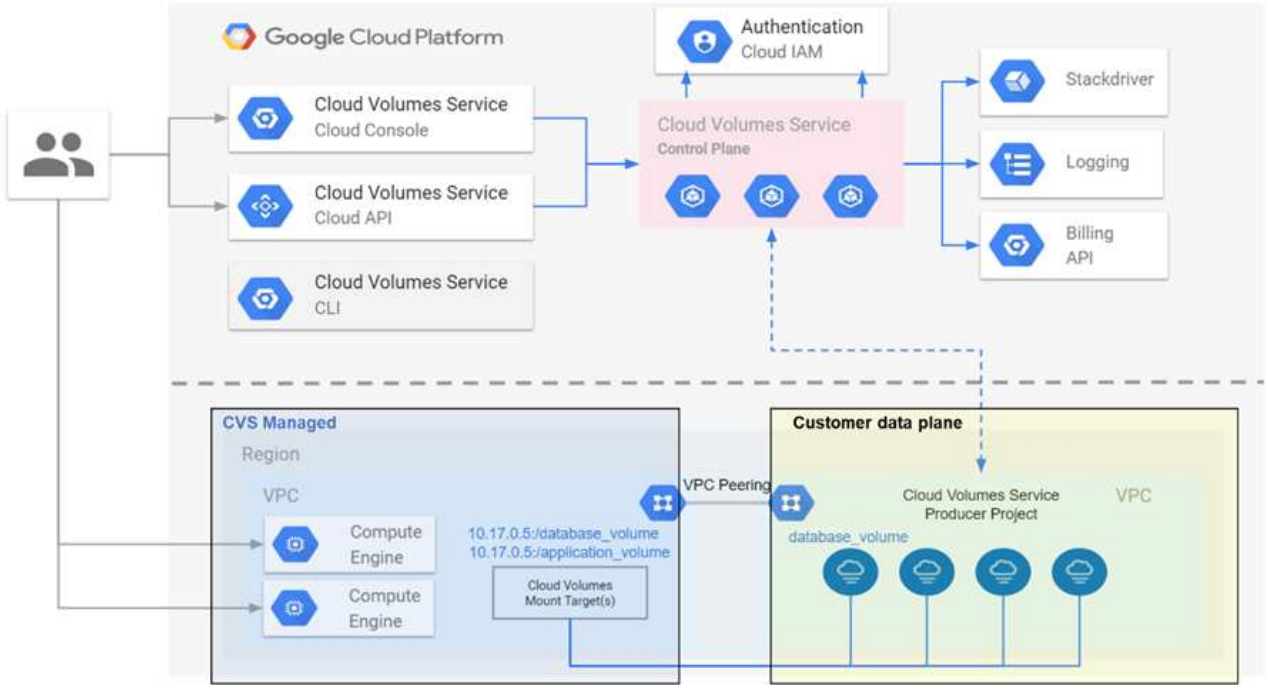
Cloud Volumes Service 中的数据平面包括实际数据卷和整体Cloud Volumes Service 配置(例如访问控制、Kerberos身份验证等)。数据平面完全由Cloud Volumes Service 平台的最终用户和使用者控制。

每个平面的安全保护和管理方式各不相同。以下各节将从Cloud Volumes Service 架构概述开始介绍这些差异。

Cloud Volumes Service 架构

Cloud Volumes Service 采用与其他Google Cloud原生 服务类似的方式、例如CloudSQL、Google Cloud VMware引擎(GCVE)和文件存储库 "Google PSA" 交付服务。在PSA中、服务构建在服务生产者项目中、该项目使用 "VPC网络对等" 以连接到服务使用者。服务生产者由NetApp提供和运营、服务使用者是客户项目中的VPC、负责托管要访问Cloud Volumes Service 文件共享的客户端。

下图、引用自 "架构部分" 显示了Cloud Volumes Service 文档的概要视图。



虚线上方的部分显示服务的控制平面、控制卷生命周期。虚线下方的部分显示数据平面。左侧蓝色框表示用户VPC (服务使用者)、右侧蓝色框表示NetApp提供的服务生产者。两者均通过VPC对等连接。

租户模式

在Cloud Volumes Service 中、各个项目被视为唯一租户。这意味着、卷、Snapshot副本等操作是按项目执行的。换言之、所有卷均归在中创建它们的项目所有、默认情况下、只有该项目才能管理和访问其中的数据。这被视为服务的控制面板视图。

共享 **vPC**

在数据平面视图中、Cloud Volumes Service 可以连接到共享VPC。您可以在托管项目中或连接到共享VPC的某个服务项目中创建卷。连接到此共享VPC的所有项目(主机或服务)均可访问网络层(TCP/IP)上的卷。由于共享VPC上具有网络连接的所有客户端都可能通过NAS协议访问数据、因此必须使用单个卷上的访问控制(例如、NFS导出的用户/组访问控制列表(ACL)和主机名/IP地址)来控制谁可以访问数据。

每个客户项目最多可以将Cloud Volumes Service 连接到五个vPC。在控制平面上、您可以通过该项目管理所有已创建的卷、无论这些卷连接到哪个VPC。在数据平面上、VPC彼此隔离、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。

换言之、在网络层、连接到共享VPC的所有项目都能够看到卷、而在管理端、控制平面仅允许所有者项目查看卷。

VPC服务控制

VPC服务控制功能可围绕连接到互联网且可在全球访问的Google Cloud服务建立访问控制边界。这些服务可通过用户身份提供访问控制、但不能限制发出哪些网络位置请求。VPC服务控制通过引入限制对定义的网络的访问的功能来缩小这一差距。

Cloud Volumes Service 数据平面不会连接到外部Internet、而是连接到具有明确定义的网络边界(边界)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。但是、控制平面不提供与数据平面相同的保护、任何人都可以使用有效凭据("JWT令牌"）。

简而言之、Cloud Volumes Service 数据平面可提供网络访问控制功能、无需支持VPC服务控制、也不明确使用VPC服务控制。

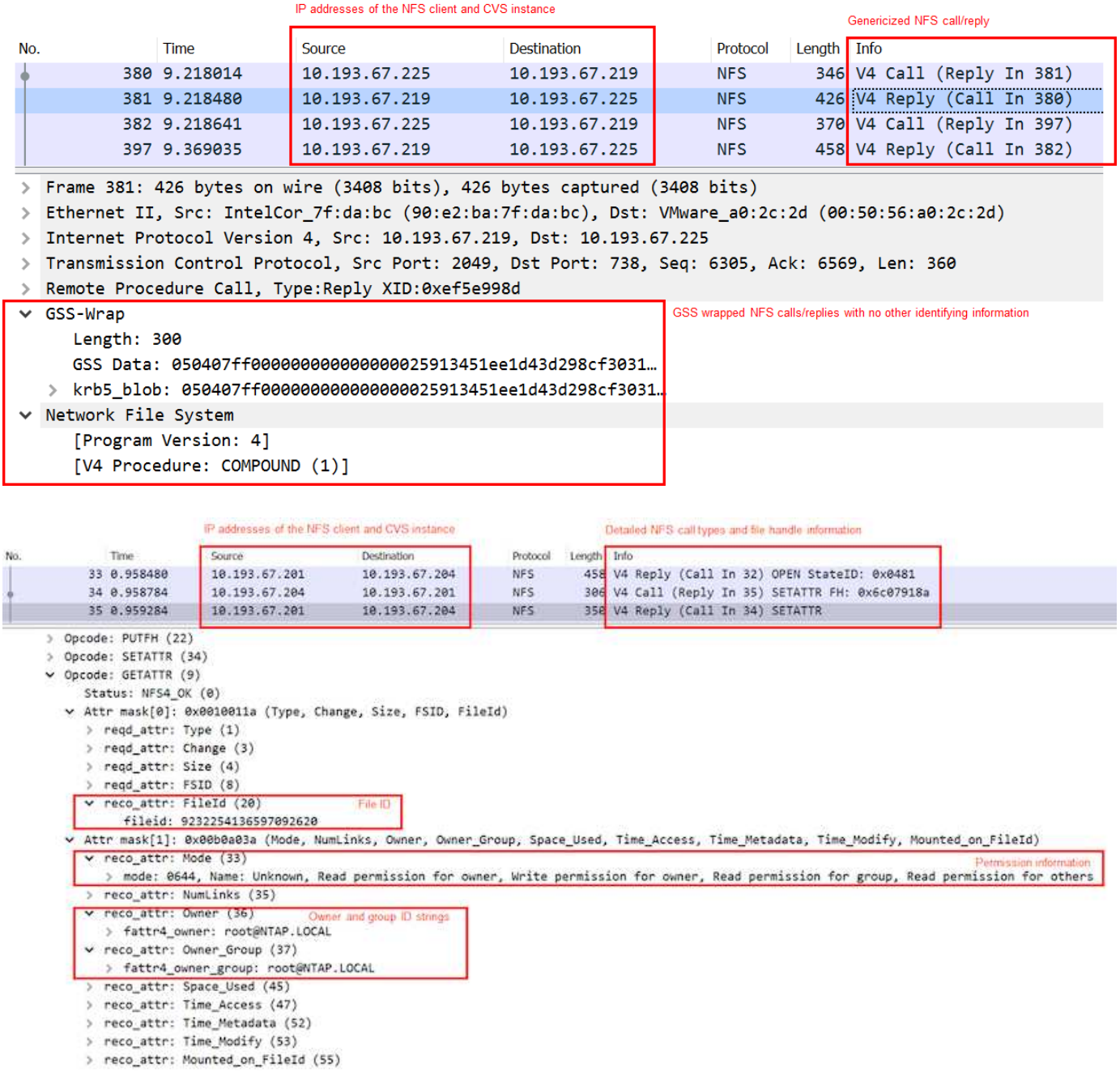
数据包嗅探/跟踪注意事项

数据包捕获对于解决网络问题或其他问题(例如NAS权限、LDAP连接等)非常有用、但也可以恶意使用数据包捕获来获取有关网络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。由于配置Google Cloud网络、VPC和防火墙规则的方式、如果没有用户登录凭据或、则很难获取对网络数据包的不必要访问 "JWT令牌" 迁移到云实例。只有端点(如虚拟机(VM))才可以捕获数据包、只有VPC内部的端点才可以捕获数据包、除非使用共享VPC和/或外部网络通道/IP转发明确允许外部流量传输到端点。无法嗅探客户端外部的流量。

使用共享VPC时、使用NFS Kerberos和/或进行动态加密 "SMB加密" 可以屏蔽从跟踪中获取的大部分信息。但是、某些流量仍以纯文本形式发送、例如 "DNS" 和 "LDAP查询"。下图显示了从Cloud Volumes Service 发起的纯文本LDAP查询中捕获的数据包以及公开的潜在标识信息。Cloud Volumes Service 中的LDAP查询当前不支持加密或基于SSL的LDAP。如果Active Directory请求、CVS-Performance支持LDAP签名。CVS-SW不支持LDAP签名。

unixUserPassword由LDAP查询、不会以纯文本形式发送、而是以盐哈希形式发送。默认情况下、Windows LDAP不会填充unixUserPassword字段。只有在需要利用Windows LDAP通过LDAP交互式登录到客户端时、才需要此字段。Cloud Volumes Service 不支持对实例进行交互式LDAP登录。

下图显示了通过AUTH_SYS捕获NFS旁边的NFS Kerberos对话中的数据包捕获。请注意、跟踪中提供的信息在这两者之间有何不同、以及启用动态加密如何为NAS流量提供更高的整体安全性。



VM网络接口

攻击者可能会尝试的一个技巧是、在中向虚拟机添加新的网络接口卡(Network Interface Card、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需要完全关闭虚拟机、这样会创建警报、因此攻击者无法在无人察觉的情况下执行此操作。

此外、NIC根本无法设置为混杂模式、并会在Google Cloud中触发警报。

控制平面架构

对Cloud Volumes Service 执行的所有管理操作均通过API完成。集成到GCP云控制台的Cloud Volumes Service 管理也使用Cloud Volumes Service API。

身份和访问管理

身份和访问管理 ("IAM")是一项标准服务、可用于控制对Google Cloud项目实例的身份验证(登录)和授权(权限)。Google IAM可提供权限授权和删除的完整审核跟踪。目前、Cloud Volumes Service 不提供控制平面审核。

授权/权限概述

IAM为Cloud Volumes Service 提供内置的粒度权限。您可以找到 "在此填写粒度权限列表"。

IAM还提供了两个预定义角色、称为`netappcloudvolumes.admin`和`netappcloudvolumes.viewer`。可以将这些角色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Cloud Volumes Service。

使用粒度权限的示例包括：

- 仅使用获取/列表/创建/更新权限构建自定义角色、以使用户无法删除卷。
- 使用仅具有`snapshot.*`权限的自定义角色创建用于构建应用程序一致的Snapshot集成的服务帐户。
- 构建自定义角色、将`volumereplication *`委派给特定用户。

服务帐户

通过脚本或进行Cloud Volumes Service API调用 "Terraform"、您必须创建一个具有`角色/netappcloudvolumes.admin`角色的服务帐户。您可以使用此服务帐户通过两种不同的方式生成对Cloud Volumes Service API请求进行身份验证所需的JWT令牌：

- 生成JSON密钥并使用Google API从该密钥派生JWT令牌。这是最简单的方法、但涉及手动密钥(JSON密钥)管理。
- 使用 … "服务帐户模拟" 使用`Roles/iam.serviceAccountTokenCreator`。代码(脚本、Terraform等)运行 "应用程序默认凭据" 并模拟服务帐户以获取其权限。此方法反映了Google的安全最佳实践。

请参见 "正在创建服务帐户和私钥" 有关详细信息、请参见Google云文档。

Cloud Volumes Service API

Cloud Volumes Service API使用基于REST的API、并使用HTTPS (TLSv1.2)作为底层网络传输。您可以找到最新的API定义 "此处" 以及有关如何使用API的信息、请参见 "Google云文档中的Cloud Volumes API"。

API端点由NetApp使用标准HTTPS (TLSv1.2)功能进行操作和保护。

JWT令牌

使用JWT承载令牌对API进行身份验证 ("RFC-7519"）。必须使用Google Cloud IAM身份验证获取有效的JWT令牌。必须通过提供服务帐户JSON密钥从IAM提取令牌来完成此操作。

审核日志记录

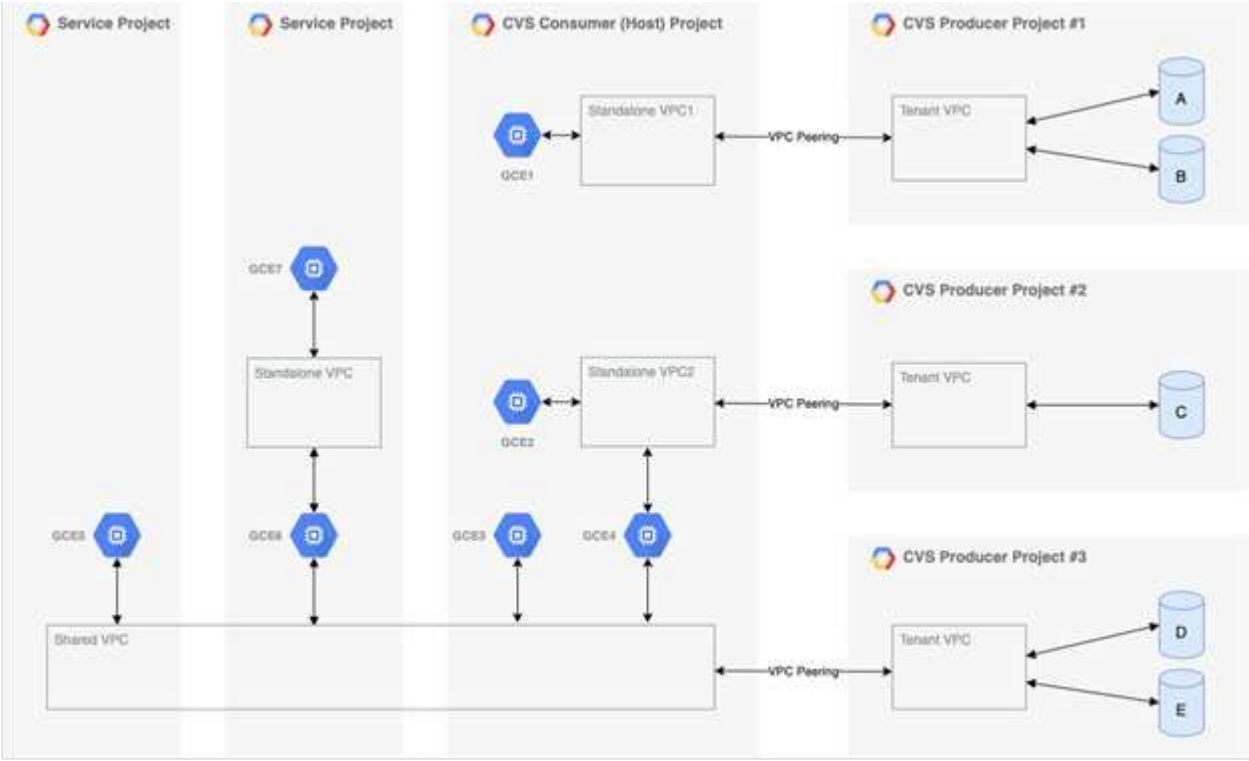
目前、没有用户可访问的控制平面审核日志。

数据平台架构

适用于Google Cloud的Cloud Volumes Service 利用了Google Cloud "私有服务访问" 框架。在此框架中、用户可以连接到Cloud Volumes Service。此框架像使用其他Google Cloud服务一样使用服务网络和VPC对等结构、确保租户之间完全隔离。

有关适用于Google Cloud的Cloud Volumes Service 架构概述、请参见 "适用于Cloud Volumes Service 的架构"。

用户vPC (独立或共享)与托管卷的Cloud Volumes Service 托管租户项目中的vPC建立对等关系。



上图显示了一个项目(中间为CVS使用者项目)、其中三个VPC网络连接到Cloud Volumes Service 、多个计算引擎VM (GCE1-7)共享卷：

- VC1允许GCE1访问卷A和B
- VPC2允许GCE2和GCE4访问卷C
- 第三个VPC网络是一个共享VPC、与两个服务项目共享。它允许GCE3、GCE4、GCE5和GCE6访问卷D和E只有CVS-Performance服务类型的卷才支持共享VPC网络。

GCE7无法访问任何卷。

可以在Cloud Volumes Service 中对传输中(使用Kerberos和/或SMB加密)和空闲数据进行加密。

传输中的数据加密

传输中的数据可以在NAS协议层进行加密、Google Cloud网络本身也会进行加密、如以下各节所述。

Google Cloud网络

Google Cloud按中所述在网络级别对流量进行加密 "传输中加密" 在Google文档中。如"云卷服务架构"一节所述、Cloud Volumes Service 是通过NetApp控制的PSA生产商项目交付的。

对于CVS-SW、生产者租户运行Google VM来提供服务。Google会自动对用户VM和Cloud Volumes Service VM之间的流量进行加密。

虽然在网络层上、CVS-Performance的数据路径未完全加密、但NetApp和Google会结合使用 "IEEE 802.1AE加密(MAC秒)"， "封装" (数据加密)和受物理限制的网络、用于保护Cloud Volumes Service CVS-Performance服务类型与Google Cloud之间传输的数据。

NAS协议

NFS和SMB NAS协议可在协议层提供可选的传输加密。

SMB加密

"SMB加密" 为SMB数据提供端到端加密、并防止数据在不可信的网络上被窃听。您可以同时为客户端/服务器数据连接(仅适用于具有SMB3.x功能的客户端)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将无法访问共享。

Cloud Volumes Service 支持使用RC4 HMAC、AES-128-CTS-HMAC-SHA1和AES-256-CTS-HMAC-SHA1安全密码进行SMB加密。SMB协商到服务器支持的最高加密类型。

NFSv4.1 Kerberos

对于NFSv4.1、CVS-Performance可提供Kerberos身份验证、如中所述 "RFC7530"。您可以按卷启用Kerberos。

当前最强的Kerberos加密类型为AES-256-CTS-HMAC-SHA1。NetApp Cloud Volumes Service 支持适用于NFS的AES-256-CTS-HMAC-SHA1、AES-128-CTS-HMAC-SHA1、DES3和DES。它还支持对CIFS/SMB流量使用ARCFOUR-HMAC (RC4)、但不支持对NFS使用。

Kerberos为NFS挂载提供了三种不同的安全级别、这些安全级别可以选择Kerberos安全性的强程度。

根据RedHat的要求 "通用挂载选项" 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安全级别必须执行的操作越多、性能就越差、因为客户端和服务器会花费时间对发送的每个数据包的NFS操作进行加密和解密。许多客户端和NFS服务器都支持将AES-NI负载分流到CPU、以获得更好的

整体体验、但Kerberos 5p (完全端到端加密)的性能影响远远大于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	• 安全性最低；纯文本、包含数字用户ID/组ID • 能够查看UID、GID、客户端IP地址、导出路径、文件名、 数据包捕获中的权限	• 最适合大多数情况
NFSv4.x—系统	• 比NFSv3 (客户端ID、名称字符串/域字符串匹配)更安全、但仍为纯文本 • 能够查看UID、GID、客户端IP地址、名称字符串、域ID、 数据包捕获中的导出路径、文件名和权限	• 适用于顺序工作负载(如VM、数据库、大型文件) • 错误、文件数量较多/元数据较高(较差30-50%)
NFS—krb5	• 对每个NFS数据包中的凭据进行Kerberos加密—在GSS包装程序中的RPC调用中封装用户/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/密码或手动密钥选项卡交换)；票证将在指定时间段后过期、用户必须重新进行身份验证才能进行访问 • 对于NFS操作或挂载/端口映射程序/NLM等辅助协议、不进行加密(可以查看导出路径、IP地址、文件句柄、权限、文件名、数据包捕获中的atime/mtime)	• 大多数情况下最适合使用Kerberos；比AUTH_SYS更差

安全级别	安全性	性能
NFS—krb5i	• 对每个NFS数据包中的凭据进行Kerberos加密—在GSS包装程序中的RPC调用中封装用户/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/密码或手动密钥选项卡交换)；票证将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 • 对于NFS操作或挂载/端口映射程序/NLM等辅助协议、不进行加密(可以查看导出路径、IP地址、文件句柄、权限、文件名、数据包捕获中的atime/mtime) • 每个数据包都会添加Kerberos GSS校验和、以确保不会截获任何数据包。如果校验和匹配、则允许对话。	• 优于krb5p、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差得多、但会有所下降。
NFS—krb5p	• 对每个NFS数据包中的凭据进行Kerberos加密—在GSS包装程序中的RPC调用中封装用户/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)；票证将在指定时间段后过期、用户必须重新进行身份验证才能进行访问 • 所有NFS数据包有效负载都使用GSS包装程序进行加密(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操作类型是可见的(fsINFO、access、getattr等)。 • 辅助协议(挂载、端口映射、NLM等)未加密-(可以查看导出路径、IP地址)	• 安全级别的性能最差；krb5p必须对更多内容进行加密/解密。 • 对于文件数量较多的工作负载、性能优于使用NFSv4.x时的krb5p。

在Cloud Volumes Service 中、配置的Active Directory服务器用作Kerberos服务器和LDAP服务器(从RFC2307兼容模式查找用户身份)。不支持其他Kerberos或LDAP服务器。NetApp强烈建议您在Cloud Volumes Service 中使用LDAP进行身份管理。有关NFS Kerberos在数据包捕获中的显示方式的信息、请参见一节 "《数据包嗅探/跟踪注意事项》。"

空闲数据加密

Cloud Volumes Service 中的所有卷都使用AES-256加密进行空闲加密、这意味着写入介质的所有用户数据都将进行加密、并且只能使用每个卷的密钥进行解密。

- 对于CVS-SW、使用Google生成的密钥。
- 对于CVS-Performance、每个卷的密钥存储在Cloud Volumes Service 中内置的密钥管理器中。

自2021年11月起、提供了预览客户管理的加密密钥(CMEK)功能。这样、您就可以使用中托管的每个项目的每个区域主密钥对每个卷的密钥进行加密 "Google密钥管理服务(KMS)。" 您可以通过Kms连接外部密钥管理器。

有关为KMS配置CVS-Performance的信息、请参见 "设置客户管理的加密密钥"。

防火墙：

Cloud Volumes Service 公开多个TCP端口以提供NFS和SMB共享：

- "NFS访问所需的端口"
- "SMB访问所需的端口"

此外、SMB、包含Kerberos的LDAP NFS以及双协议配置都需要访问Windows Active Directory域。Active Directory连接必须为 "已配置" 按区域计算。Active Directory域控制器(DC)通过使用进行标识 "基于DNS的DC发现" 使用指定的DNS服务器。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域控制器列表。

Cloud Volumes Service 会通过分配给的CIDR范围内的IP地址进行访问 `gcloud compute address` 命令 "加入Cloud Volumes Service"。您可以使用此CIDR作为源地址来为Active Directory域控制器配置入站防火墙。

Active Directory域控制器必须 "将端口公开到此处所述的Cloud Volumes Service CIDR中"。

NAS协议

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CVS允许在多个NAS客户端之间共享访问数据的方式。此外、Cloud Volumes Service 还可以同时提供对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。为了保持尽可能高的数据传输安全性、Cloud Volumes Service 支持使用SMB加密和NFS Kerberos 5p进行协议加密。

双协议仅适用于CVS-Performance。

NAS协议基础知识

NAS协议是一个网络上的多个客户端访问存储系统上相同数据的方法、例如GCP上的Cloud Volumes Service。NFS和SMB是定义的NAS协议、在客户端/服务器基础上运行、Cloud Volumes Service 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客户端要在文件夹中创建新文件、则遵循以下常规过程。

1. 客户端要求服务器提供有关目录的信息(权限、所有者、组、文件ID、可用空间、 等)；如果发出请求的客户端和用户对父文件夹具有必要的权限、则服务器将使用此信息进行响应。
2. 如果目录上的权限允许访问、则客户端会询问服务器所创建的文件名是否已存在于文件系统中。如果文件名已在使用中、则创建将失败。如果文件名不存在、服务器会让客户端知道它可以继续。
3. 客户端调用服务器以使用目录句柄和文件名创建文件、并设置访问和修改时间。服务器会向文件发出唯一的文件ID、以确保不会使用相同的文件ID创建其他文件。
4. 在执行写入操作之前、客户端会发送一个调用来检查文件属性。如果权限允许、客户端将写入新文件。如果协议/应用程序使用锁定、则客户端会要求服务器提供锁定、以防止其他客户端在锁定期间访问文件、以防止数据损坏。

NFS

NFS是一种分布式文件系统协议、它是在Request for Comments (RFC)中定义的开放式IETF标准、允许任何人实施该协议。

通过导出客户端或一组客户端可访问的路径、可以将Cloud Volumes Service 中的卷共享到NFS客户端。挂载这些导出的权限由导出策略和规则定义、这些策略和规则可由Cloud Volumes Service 管理员配置。

NetApp NFS实施被视为该协议的黄金标准、用于无数企业级NAS环境。以下各节介绍了Cloud Volumes Service 中提供的NFS和特定安全功能及其实施方式。

默认本地**UNIX**用户和组

Cloud Volumes Service 包含多个用于各种基本功能的默认UNIX用户和组。当前无法修改或删除这些用户和组。当前无法将新的本地用户和组添加到Cloud Volumes Service 中。默认用户和组以外的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中或在重新使用这些数字ID的本地客户端上创建新用户或组。

默认用户：数字**ID**	默认组：数值**ID**
• 根：0 • pcuser：65534 • nobody：65535	• 根：0 • 守护进程：1. • pcuser：65534 • nobody：65535

使用NFSv4.1时、root用户在NFS客户端上运行目录列出命令时可能会显示为nobody。这是因为客户端的ID域映射配置。请参见名为的部分 NFSv4.1和nobody用户/组 有关此问题描述 以及如何解决此问题的详细信息、请参见。

root用户

在Linux中、root帐户可以访问基于Linux的文件系统中的所有命令、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root用户。在NFS导出中、可以通过导出策略和规则以及称为根强制转换的概念在Cloud Volumes Service 中控制root用户对文件和文件夹的能力。

根强制转换可确保访问NFS挂载的root用户被强制转换为匿名数字用户65534 (请参见第节[匿名用户]")、并且当前仅在使用CVS-Performance时可用、方法是在创建导出策略规则期间选择off作为root访问权限。如果root用户被强制转换为匿名用户、则它将无法再运行chown或 "setuid/setgid命令(粘滞位)" 对于NFS挂载中的文件或文件夹、以及root用户创建的文件或文件夹、将anon UID显示为所有者/组。此外、root用户无法修改NFSv4 ACL。但是、root用户仍可访问其没有显式权限的chmod和已删除的文件。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`的Windows用户并将所需权限应用于文件或文件夹。

匿名用户

匿名(anon)用户ID指定映射到未使用有效NFS凭据的客户端请求的UNIX用户ID或用户名。使用root用户强制转换时、这可能包括root用户。Cloud Volumes Service 中的anon用户为65534。

在Linux环境中、此UID通常与用户名`nobody`或`nfsnobody`关联。Cloud Volumes Service 还使用65534作为本地UNIX用户` pcuser`(请参见第节默认本地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名称映射的默认回退用户。

由于Linux和Cloud Volumes Service 中UID 65534的用户名不同、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、在某些文件和文件夹上、您可能会看到`nobody`作为用户。请参见第节"NFSv4.1和nobody用户/组有关此问题描述 以及如何解决此问题的信息、请参见。

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。定义了主机IP、主机名、子网、网络组或域、以允许访问挂载NFS共享以及主机允许的访问级别。导出策略规则配置选项取决于Cloud Volumes Service 级别。

对于CVS-SW、导出策略配置可使用以下选项：

- 客户端匹配。 IP地址列表以逗号分隔、主机名、子网、网络组和域名列表以逗号分隔。
- * RO/RW访问规则。*选择读/写或只读以控制对导出的访问级别。cvs-Performance提供了以下选项：
- 客户端匹配。 IP地址列表以逗号分隔、主机名、子网、网络组和域名列表以逗号分隔。
- * RO或RW访问规则。*选择读/写或只读以控制导出的访问级别。
- *根访问(开/关)。*配置根强制转换(请参见一节[root用户]"了解详细信息)。
- *协议类型。*此操作会将对NFS挂载的访问限制为特定协议版本。为卷同时指定NFSv3和NFSv4.1时、请将这两个字段留空或同时选中这两个框。
- * Kerberos安全级别(选择启用Kerberos时)。*提供了krb5、krb5i和/或krb5p选项、用于只读或读写访问。

更改所有权**(chown)**和更改组**(chgrp)**

Cloud Volumes Service 上的NFS仅允许root用户对文件和文件夹运行chown/chgrp。其他用户会看到`Operation not permitted`错误、即使是在其拥有的文件上也是如此。如果使用root squash (如第节中所述)[root用户]")、根卷将被强制转换为非root用户、并且不允许访问chown和chgrp。目前、Cloud Volumes Service 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模式设置为NTFS、以便从Windows端控制权限。

权限管理

Cloud Volumes Service 同时支持模式位(例如rwx的6444、777等)和NFSv4.1 ACL、以控制使用UNIX安全模式的卷在NFS客户端上的权限。标准权限管理用于这些对象(例如chmod、chown或nfs4_setfacl)、并可用于支持这

些对象的任何Linux客户端。

此外、使用设置为NTFS的双协议卷时、NFS客户端可以利用Cloud Volumes Service 名称映射到Windows用户、然后使用该映射来解析NTFS权限。这需要通过LDAP连接到Cloud Volumes Service 来提供数字ID到用户名的转换、因为Cloud Volumes Service 需要有效的UNIX用户名才能正确映射到Windows用户名。

为NFSv3提供粒度ACL

模式位权限仅涵盖语义中的所有者、组和其他所有人、这意味着基本NFSv3没有粒度用户访问控制。Cloud Volumes Service 既不支持POSIX ACL、也不支持扩展属性(例如chattr)、因此、只有在使用NFSv3的以下情况下、才可以使用粒度ACL：

- 具有有效UNIX到Windows用户映射的NTFS安全模式卷(需要CIFS服务器)。
- 使用挂载NFSv4.1的管理客户端应用NFSv4.1 ACL以应用ACL。

这两种方法都需要使用LDAP连接进行UNIX身份管理、并填充有效的UNIX用户和组信息(请参见一节 ""LDAP"")、并且仅适用于CVS-Performance实例。要对NFS使用NTFS安全模式卷、必须使用双协议(SMB和NFSv3)或双协议(SMB和NFSv4.1)、即使未建立SMB连接也是如此。要对NFSv3挂载使用NFSv4.1 ACL、必须选择`both (NFSv3/NFSv4.1)`作为协议类型。

常规UNIX模式位提供的权限粒度级别与NTFS或NFSv4.x ACL提供的权限级别不同。下表对NFSv3模式位和NFSv4.1 ACL之间的权限粒度进行了比较。有关NFSv4.1 ACL的信息、请参见 "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(未在POSIX中定义) • 所有者的读取权限 • 所有者的写入权限 • 对文件执行所有者权限；或者在目录中查找(搜索)所有者权限 • 组的读取权限 • 组的写入权限 • 对文件中的组执行权限；或者在目录中查找(搜索)组权限 • 其他人的读取权限 • 其他人的写入权限 • 对其他人对文件执行权限；或者在目录中查找(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*无传播-继承*仅继承 权限*读取数据(文件)/列表目录(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*删除子目录*读取属性*写入属性*读取命名属性*写入ACL *写入所有者*写入ACL *写入操作

最后、根据RPC数据包限制、对于AUTH_SYS、NFS组成员资格(在NFSv3和NFSv4.x中)限制为默认最大16个。NFS Kerberos最多可提供32个组、NFSv4 ACL可通过粒度用户和组ACL (每个ACE最多1024个条目)来消除此限制。

此外、Cloud Volumes Service 还提供了扩展的组支持、可将支持的最大组数扩展到32个。这需要通过LDAP连接到包含有效UNIX用户和组身份的LDAP服务器。有关配置此的详细信息、请参见 "创建和管理NFS卷" 在Google文档中。

NFSv3用户和组ID

NFSv3用户和组ID以数字ID而非名称的形式通过网线传输。Cloud Volumes Service 使用NFSv3无法解析这些数字ID的用户名、而UNIX安全模式卷仅使用模式位。如果存在NFSv4.1 ACL、则需要进行数字ID查找和/或名称字符串查找才能正确解析此ACL、即使使用NFSv3也是如此。对于NTFS安全模式卷、Cloud Volumes Service 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时、客户端和服务器无需确认尝试使用数字ID进行读写的用户是否为有效用户；这只是隐式信任。这样、只需欺骗任何数字ID即可使文件系统不受潜在漏洞的影响。为了防止出现此类安全漏洞、Cloud Volumes Service 提供了一些选项。

- 实施适用于NFS的Kerberos会强制用户使用用户名和密码或keytab文件进行身份验证、以获取Kerberos票证以允许访问挂载。Kerberos可用于CVS-Performance实例、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Cloud Volumes Service 卷。
- 使用双协议卷并对卷应用NTFS ACL会强制NFSv3客户端将数字ID解析为有效的UNIX用户名、以便正确进行身份验证以访问挂载。这需要启用LDAP并配置UNIX用户和组身份。
- 将root用户强制转换会限制root用户对NFS挂载可能造成的损害、但不会完全消除风险。有关详细信息、请参见"[root用户]。 "

最终、NFS安全性仅限于您所使用的协议版本。虽然NFSv3的总体性能优于NFSv4.1、但提供的安全性级别不同。

NFSv4.1

与NFSv3相比、NFSv4.1的安全性和可靠性更高、原因如下：

- 通过基于租赁的机制实现集成锁定
- 有状态会话
- 通过单个端口提供所有NFS功能(2049)
- 仅限TCP
- ID域映射
- Kerberos集成(NFSv3可以使用Kerberos、但只能用于NFS、而不能用于辅助协议、例如NLM)

NFSv4.1依赖关系

由于NFSv4.1中的额外安全功能、因此、使用NFSv3时不需要涉及一些外部依赖关系(类似于SMB需要依赖关系的方式、例如Active Directory)。

NFSv4.1 ACL

Cloud Volumes Service 支持NFSv4.x ACL、与正常的POSIX模式权限相比、这些ACL具有明显的优势、例如：

- 精细控制用户对文件和目录的访问
- 提高 NFS 安全性
- 改进了与CIFS/SMB的互操作性
- 取消了使用AUTH_SYS安全性时每个用户16个组的NFS限制
- ACL不需要进行组ID (GID)解析、从而有效地消除了GID限制NFSv4.1 ACL由NFS客户端控制、而不是通过Cloud Volumes Service 控制。要使用NFSv4.1 ACL、请确保您的客户端软件版本支持这些ACL、并安装了正确的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、而您使用的是双协议访问(同一数据集中的NFS和SMB)、则使用SMB2.0及更高版本的客户端将无法通过Windows安全选项卡查看或管理ACL。

NFSv4.1 ACL的工作原理

定义了以下术语以供参考：

- *访问控制列表(ACL)。*权限条目的列表。
- *访问控制条目(ACE)。*列表中的一个权限条目。

当客户端在SETATTR操作期间为文件设置NFSv4.1 ACL时、Cloud Volumes Service 会在对象上设置此ACL、以替换任何现有ACL。如果文件没有ACL、则文件的模式权限将通过所有者@、组@和所有人@计算得出。如果文件上存在任何现有的SUID/SGID/粘滞位、它们不会受到影响。

如果客户端在getattr操作期间获取文件的NFSv4.1 ACL、则Cloud Volumes Service 将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、则会使用模式位构建ACL并将其返回给客户端。

如果ACL中存在拒绝ACE、则拒绝访问；如果存在允许ACE、则授予访问权限。但是、如果ACL中不存在任何ACE、则访问也会被拒绝。

安全描述符由一个安全ACL (SACL)和一个随机ACL (DACL)组成。如果NFSv4.1与CIFS/SMB互操作、则DACL将与NFSv4和CIFS进行一对一映射。DACL由ALLOW ACE和DENY ACE组成。

如果在设置了NFSv4.1 ACL的文件或文件夹上运行基本的`chmod`、则会保留现有用户和组ACL、但会修改默认所有者@、组@、每个人@ ACL。

使用NFSv4.1 ACL的客户端可以为系统上的文件和目录设置和查看ACL。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中已标记为相应的所有ACE "继承标志"。

如果文件或目录具有NFSv4.1 ACL、则无论使用哪个协议访问文件或目录、都可以使用该ACL来控制访问。

只要父目录上的NFSv4 ACL为ACE添加了正确的继承标志、文件和目录就会继承这些ACE (可能需要进行适当修改)。

在根据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包含ACL还是仅包含标准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 ，则会使用该 ACL 。

- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录没有 ACL ，则会使用客户端文件模式设置标准 UNIX 文件访问权限。
- 如果此请求仅包含标准UNIX文件访问权限、并且父目录具有不可继承的ACL、则会根据传递给此请求的模式位为新对象设置默认ACL。
- 如果此请求仅包含标准 UNIX 文件访问权限，但父目录具有 ACL ，则只要父目录的 ACL 中的 ACE 已使用适当的继承标志进行标记，新文件或目录就会继承这些 ACE 。

ACE权限

NFSv4.1 ACL权限使用一系列大小写字母值(例如`rxtncy`)来控制访问。有关这些字母值的详细信息、请参见 "如何：使用NFSv4 ACL"。

具有**umask**和**ACL**继承的**NFSv4.1 ACL**行为

"NFSv4 ACL可提供ACL继承功能"。ACL继承是指在设置了NFSv4.1 ACL的对象下创建的文件或文件夹可以根据的配置继承ACL "ACL继承标志"。

"umask" 用于控制在目录中创建文件和文件夹而无需管理员干预的权限级别。默认情况下、Cloud Volumes Service 允许umask覆盖继承的ACL、这是预期的行为 "RFC 5661"。

ACL格式化

NFSv4.1 ACL采用特定格式。以下示例是对文件设置的ACE：

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上述示例遵循以下ACL格式准则：

```
type:flags:principal:permissions
```

类型`a`表示"允许"。 在这种情况下、不会设置继承标志、因为主体不是组、并且不包括继承。此外、由于ACE不是审核条目、因此无需设置审核标志。有关NFSv4.1 ACL的详细信息、请参见 "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)、则ACL可能无法按预期运行、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.
```

显式拒绝

NFSv4.1权限可以包括所有者、组和所有人的显式拒绝属性。这是因为NFSv4.1 ACL为default-deny、这意味着如果ACE未明确授予ACL、则会拒绝该ACL。显式拒绝属性会覆盖任何访问ACE、无论显式还是非显式。

deny ACE使用属性标记`D`设置。

在以下示例中、组@允许所有读取和执行权限、但拒绝所有写入访问。

```
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
```

应尽可能避免拒绝ACE、因为它们可能会造成混乱和复杂；不明确定义的允许ACL会被隐式拒绝。如果设置了拒绝ACE、则在用户希望获得访问权限时、可能会拒绝其访问。

上述一组ACE相当于模式位中的755、这意味着：

- 所有者拥有完全权限。
- 组具有只读。
- 其他用户只读。

但是、即使权限调整为775等效权限、访问也可能会因为对Everyone设置了显式拒绝而被拒绝。

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挂载的用户是否确实是他们所宣称的身份。在这些情况下、NFSv4.1客户端的用户名和组名称会附加一个名称字符串并将其发送到Cloud Volumes Service实例。如果此用户名/组名称和ID字符串组合不匹配、则此用户和/或组将被强制转换为客户端上的`/etc/idmapd.conf`文件中指定的默认nobody用户。

要确保正确遵守权限、需要使用此ID字符串、尤其是在使用NFSv4.1 ACL和/或Kerberos时。因此、要确保客户端和Cloud Volumes Service 之间的一致性、以正确解析用户和组名称身份、必须具有LDAP服务器等名称服务服务器依赖关系。

Cloud Volumes Service 使用静态默认ID域名值`defaultv4iddomain.com`。NFS客户端的ID域名设置默认为DNS域名、但您可以在`/etc/idmapd.conf`中手动调整ID域名。

如果在Cloud Volumes Service 中启用了LDAP、则Cloud Volumes Service 会自动将NFS ID域更改为DNS中为搜索域配置的内容、并且客户端不需要修改、除非它们使用不同的DNS域搜索名称。

如果Cloud Volumes Service 可以解析本地文件或LDAP中的用户名或组名称、则会使用域字符串、而不匹配的域ID将强制转换为nobody。如果Cloud Volumes Service 在本地文件或LDAP中找不到用户名或组名称、则会使用数字ID值、NFS客户端会正确解析此名称(这类似于NFSv3行为)。

如果不更改客户端的NFSv4.1 ID域以匹配Cloud Volumes Service 卷正在使用的内容、您将看到以下行为：

- 在Cloud Volumes Service 中具有本地条目的UNIX用户和组(如在本地UNIX用户和组中定义的root)将被强制转换为nobody值。

- 如果NFS客户端和Cloud Volumes Service 之间的DNS域不同、则具有LDAP条目的UNIX用户和组(如果Cloud Volumes Service 配置为使用LDAP)将强制转换为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任何名称、则仅显示数字ID。

下面显示了上述情形的结果：

```
# 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
```

如果客户端ID域和服务器ID域匹配、则相同文件列表的显示方式如下：

```
# 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
```

有关此问题描述 以及如何解决此问题的详细信息、请参见"NFSv4.1和nobody用户/组。 "

Kerberos依赖关系

如果您计划对NFS使用Kerberos、则Cloud Volumes Service 必须具有以下配置：

- Kerberos分发中心服务(KDC)的Active Directory域
- Active Directory域、其中用户和组属性填充了有关LDAP功能的UNIX信息(Cloud Volumes Service 中的NFS Kerberos需要用户SPN到UNIX用户映射才能正常运行。)
- 已在Cloud Volumes Service 实例上启用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、如果列表中使用`ls`显示的文件或文件夹属于`user：group` combination of `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为`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、但会显示组`nobody`。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

谁不是谁?

NFSv4.1中的`nobody`用户与`nfsnobody`用户不同。您可以运行`id`命令来查看NFS客户端如何识别每个用户：

```
# 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时、`nobody`用户是由`idmapd.conf`文件定义的默认用户、可定义为要使用的任何用户。

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

为什么会发生这种情况?

由于通过名称字符串映射实现安全性是NFSv4.1操作的关键要素、因此、如果名称字符串不匹配、则默认行为是将该用户强制转换为通常无法访问用户和组所拥有的文件和文件夹的用户。

如果您在文件列表中看到用户和/或组的`nobody`、则这通常意味着NFSv4.1中的某些内容配置不当。区分大小写可以在此处发挥作用。

例如、如果user1@CVSDEMO.LOCAL (uid 1234、gid 1234)正在访问导出、则Cloud Volumes Service 必须能够找到user1@CVSDEMO.LOCAL (uid 1234、gid 1234)。如果Cloud Volumes Service 中的用户为USER1@CVSDEMO.LOCAL、则不匹配(大写用户1与小写用户1)。在许多情况下、您可以在客户端上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'
```

客户端和服务器都必须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Cloud Volumes Service 看到的用户具有相同的信息。

- * NFSv4.x ID域。*客户端：`idmapd.conf` file；Cloud Volumes Service 使用`defaultv4iddomain.com`、无法手动更改。如果将LDAP与NFSv4.1结合使用、则Cloud Volumes Service 会将ID域更改为DNS搜索域所使用的域、该域与AD域相同。
- *用户名和数字ID。*这决定了客户端查找用户名的位置、并利用名称服务开关配置—client：`nsswitch.conf`和/或本地passwd和group文件；Cloud Volumes Service 不允许修改此设置、但在启用LDAP后会自动将其添加到配置中。
- *组名称和数字ID。*这决定了客户端查找组名称的位置、并利用名称服务开关配置—client：`nsswitch.conf`和/或本地passwd和group文件；Cloud Volumes Service 不允许修改此设置、但会在启用LDAP后自动将其添加到配置中。

在几乎所有情况下、如果您在客户端的用户和组列表中看到`nobody`、则问题描述 将在Cloud Volumes Service和NFS客户端之间进行用户或组名称域ID转换。要避免这种情况、请使用LDAP在客户端和Cloud Volumes Service 之间解析用户和组信息。

查看客户端上**NFSv4.1**的名称**ID**字符串

如果您使用的是NFSv4.1、则会在NFS操作期间进行名称-字符串映射、如上所述。

除了使用`/var/log/messages`查找具有NFSv4 ID的问题描述 之外、您还可以使用 "nfsidmap -l" 命令以查看哪些用户名已正确映射到NFSv4域。

例如、这是客户端发现的用户以及Cloud Volumes Service 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
```

如果某个用户未正确映射到NFSv4.1 ID域(在本例中为`netapp-user`)、则会尝试访问同一挂载并触摸某个文件、系统会按预期为其分配`nobody：nobody`。

```
# 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
```

`nfsidmap -l`输出会在屏幕上显示用户`pcuser`、但不会显示`netapp-user`；这是我们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Microsoft开发的一种网络文件共享协议、可通过以太网为多个SMB客户端提供集中式用户/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可以提供给提供协议支持的任何客户端、包括Windows、Apple和Linux客户端。

Cloud Volumes Service 支持SMB 2.1和3.x版本的协议。

访问控制/SMB共享

- 当Windows用户名请求访问Cloud Volumes Service 卷时、Cloud Volumes Service 会使用Cloud Volumes Service 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这些UNIX属性。
- 如果Windows名称和UNIX名称不匹配、则必须将LDAP配置为允许Cloud Volumes Service 使用LDAP名称映射配置(请参见一节) ""使用LDAP进行非对称名称映射""）。

- 如果未使用LDAP、则Windows SMB用户会映射到Cloud Volumes Service 中名为`pcuser`的默认本地UNIX用户。这意味着在多协议NAS环境中、映射到`pcuser`的用户在Windows中写入的文件将UNIX所有权显示为`pcuser`。`pcuser`此处是Linux环境中的`nobody`用户(UID 65534)。

在仅使用SMB的部署中、仍会进行`pcuser`映射、但这无关紧要、因为Windows用户和组所有权会正确显示、并且不允许对仅使用SMB的卷进行NFS访问。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进行用户名/密码交换、AD DC位于Cloud Volumes Service 实例外部。如果SMB客户端使用`\\servername` UNC路径且满足以下条件、则会使用Kerberos身份验证：

- 服务器名称存在DNS A/AAAA条目
- 服务器名称存在有效的SMB/CIFS访问SPN

创建Cloud Volumes Service SMB卷时、系统会按照一节中的定义创建计算机帐户名称 "《Cloud Volumes Service 在Active Directory中的显示方式》。" 该计算机帐户名称也会成为SMB共享访问路径、因为Cloud Volumes Service 利用动态DNS (DDNS)在DNS中创建必要的A/AAAA和PTR条目、并在计算机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Cloud Volumes Service 实例IP地址的反向查找区域。

例如、此Cloud Volumes Service 卷使用以下UNC共享路径：`\\cvs-east- 433d.cvsdema.local`。

在Active Directory中、这些是Cloud Volumes Service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 CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-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:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

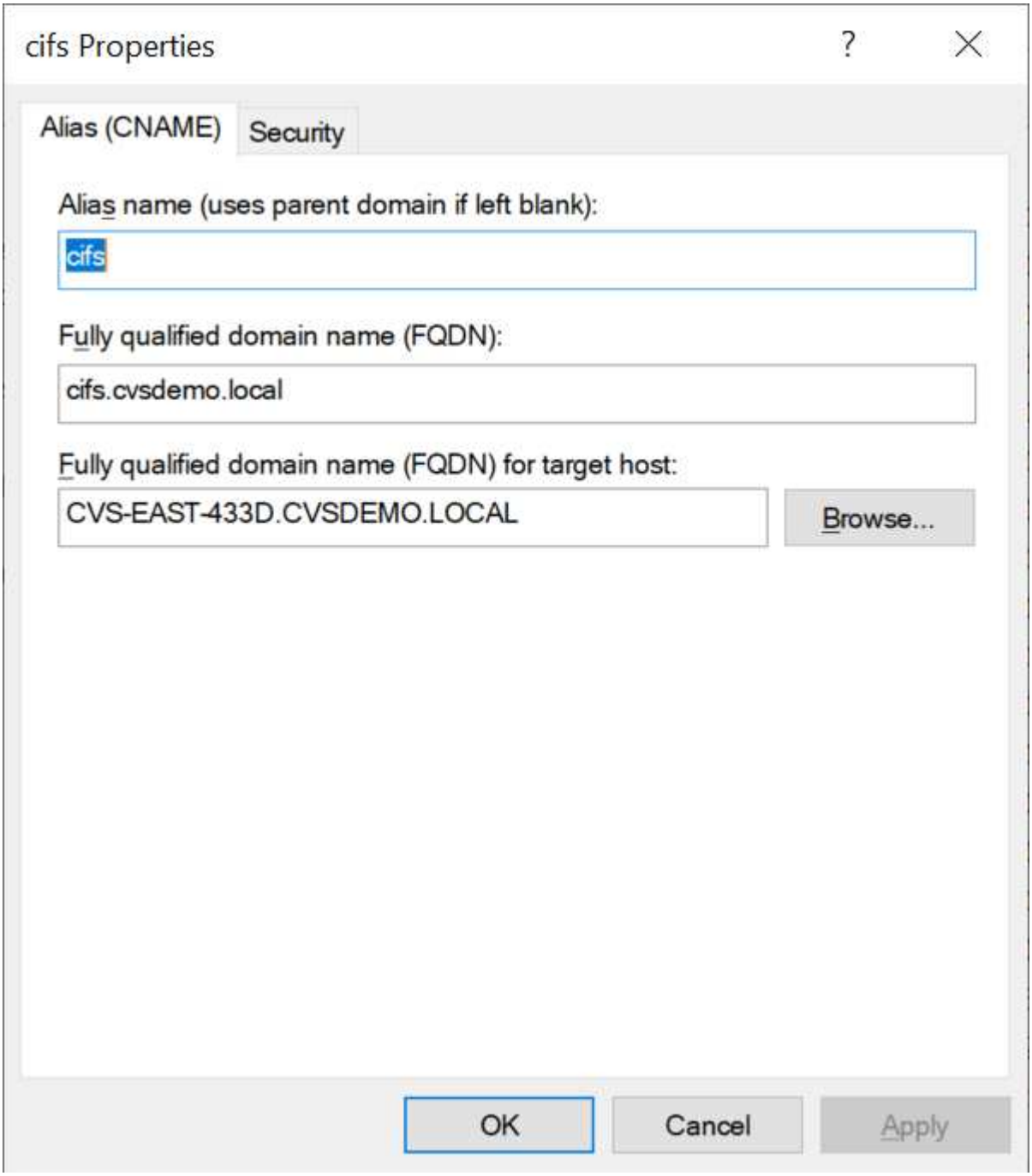
或者、可以通过在Cloud Volumes Service 中为SMB共享启用/要求SMB加密来应用更多访问控制。如果其中一个端点不支持SMB加密、则不允许访问。

使用**SMB**名称别名

在某些情况下、如果最终用户知道Cloud Volumes Service 使用的计算机帐户名称、则可能会出于安全考虑。在

其他情况下、您可能只想为最终用户提供一个更简单的访问路径。在这种情况下、您可以创建SMB别名。

如果要为SMB共享路径创建别名、可以利用DNS中的CNAME记录。例如、如果您要使用名称`\\cifs`来访问共享、而不是`\\cvs-east- 433d.cvsdema.local`、但您仍要使用Kerberos身份验证、则DNS中指向现有A/AAAA记录的CNAME以及添加到现有计算机帐户的其他SPN可提供Kerberos访问。



这是添加CNAME后生成的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:    CVS-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、我们可以使用与CNAME绑定的SPN查看会话设置请求。

```
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

Cloud Volumes Service 支持以下功能 "方言" 对于SMB身份验证：

- LM
- NTLM
- NTLMv2
- Kerberos

用于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、安全级别将进一步提高。

Cloud Volumes Service 还支持LM和NTLM身份验证的向后兼容性。如果Kerberos配置不当(例如创建SMB别名)、则共享访问会回退到身份验证方法较弱的位置(例如NTLMv2)。由于这些机制的安全性较低、因此在某些Active Directory环境中会禁用它们。如果禁用了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、因为没有可回退的有效身份验证方法。

有关在Active Directory中配置/查看受支持的身份验证级别的信息、请参见 "网络安全：LAN Manager身份验证级别"。

权限模式

NTFS/文件权限

NTFS权限是指应用于符合NTFS逻辑的文件系统中的文件和文件夹的权限。您可以在`基本`或`高级`中应用NTFS权限、并可设置为`允许`或`D允许`来进行访问控制。

基本权限包括：

- 完全控制
- 修改
- 读取和执行
- 读取
- 写入

为用户或组(称为ACE)设置权限时、该用户或组驻留在ACL中。NTFS权限使用与UNIX模式位相同的读/写/执行基础知识、但也可以扩展到更精细的扩展访问控制(也称为"特殊权限")、例如"获取所有权"、"创建文件夹/附加数据"、"写入属性"等。

标准UNIX模式位提供的粒度级别与NTFS权限不同(例如、能够为ACL中的各个用户和组对象设置权限或设置扩展属性)。但是、NFSv4.1 ACL提供的功能与NTFS ACL相同。

NTFS权限比共享权限更具体、可与共享权限结合使用。对于NTFS权限结构、限制性最强。因此、在定义访问权限时、显式拒绝用户或组甚至会覆盖"完全控制"。

NTFS权限由Windows SMB客户端控制。

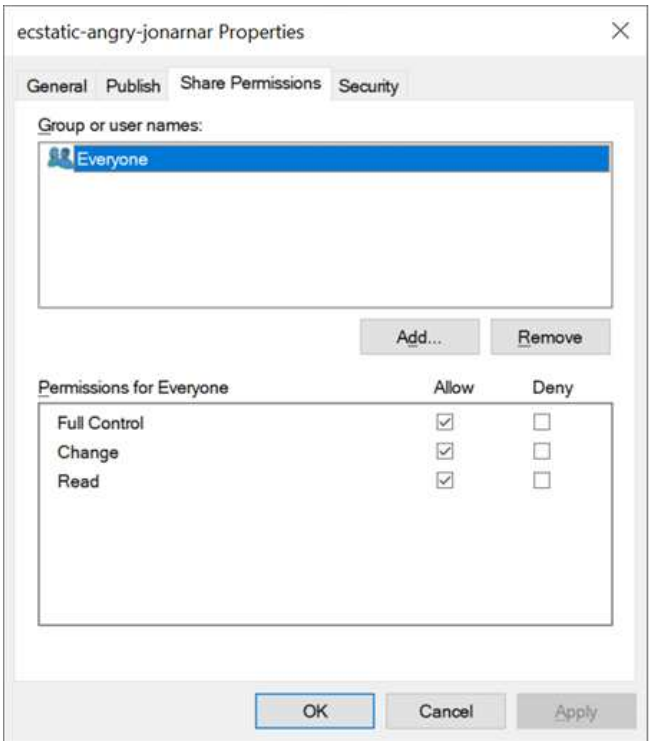
共享权限

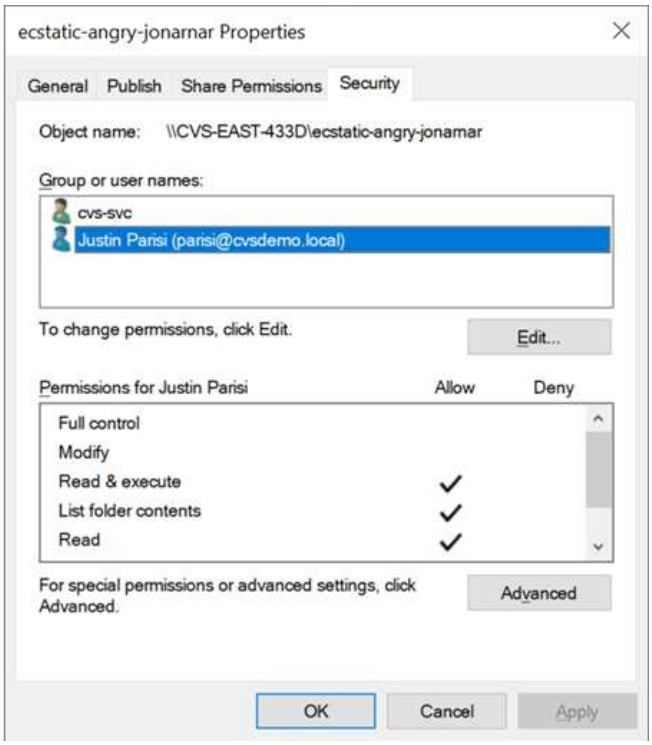
共享权限比NTFS权限更常规(仅限读取/更改/完全控制)、并可控制SMB共享的初始条目、类似于NFS导出策略规则的工作方式。

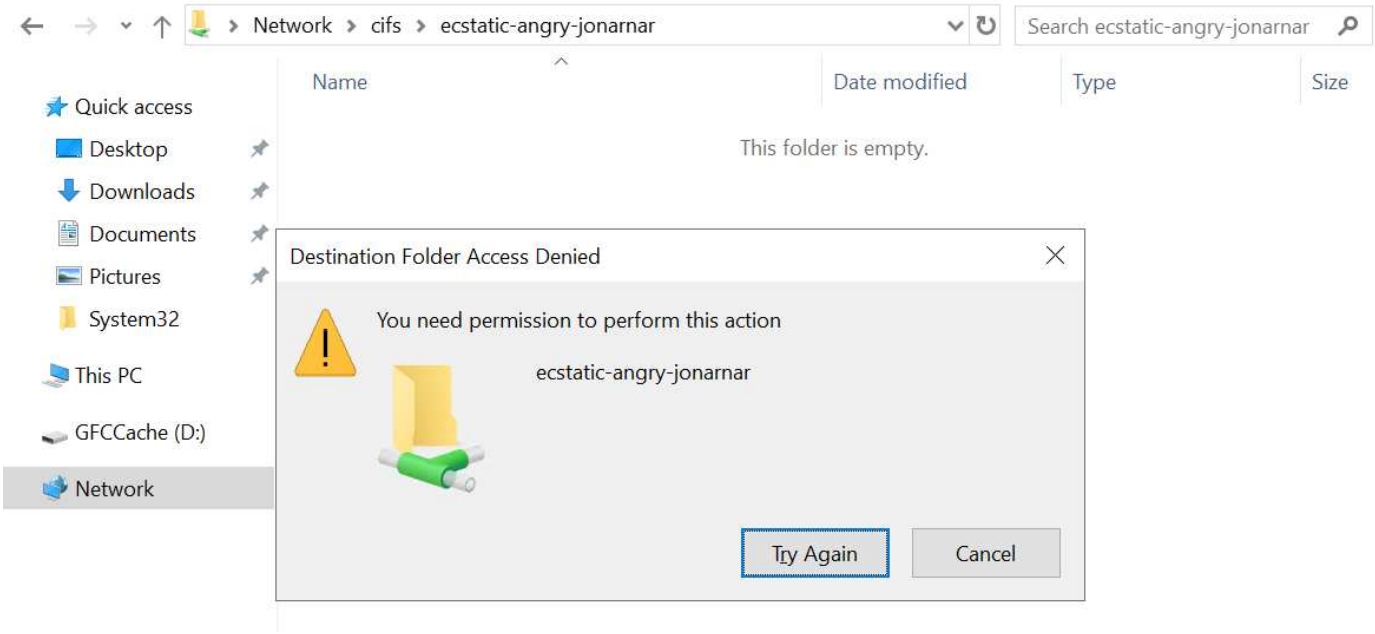
虽然NFS导出策略规则通过IP地址或主机名等基于主机的信息来控制访问、但SMB共享权限可以通过使用共享ACL中的用户和组ACE来控制访问。您可以从Windows客户端或Cloud Volumes Service 管理UI设置共享ACL。

默认情况下、共享ACL和初始卷ACL包括具有完全控制的Everyone。应更改文件ACL、但共享权限会被共享中对象的文件权限所取代。

例如、如果仅允许用户读取Cloud Volumes Service 卷文件ACL、则即使共享ACL设置为"具有完全控制的所有人"、也会拒绝用户访问创建文件和文件夹、如下图所示。







要获得最佳安全性结果、请执行以下操作：

- 从共享和文件ACL中删除Everyone、而是为用户或组设置共享访问权限。
- 使用组进行访问控制、而不是使用单个用户、以便于管理、并加快删除/添加用户的速度、以便通过组管理共享ACL。
- 允许对共享权限上的ACE进行限制性更低的常规共享访问、并锁定对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。
- 避免常规使用显式拒绝ACL、因为它们会覆盖允许ACL。限制需要限制的用户或组快速访问文件系统时使用显式拒绝ACL。
- 请务必注意 "ACL继承" 修改权限时的设置；在文件数量较多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权限、 这可能会在调整每个文件时产生不必要的行为、例如意外访问/拒绝以及长时间更改权限。

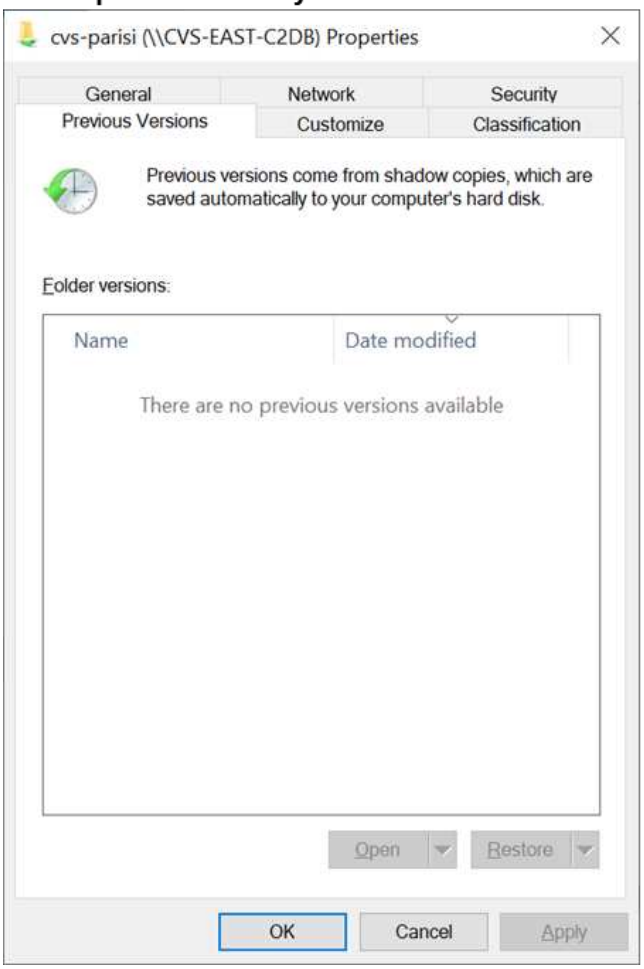
SMB共享安全功能

首次在Cloud Volumes Service 中创建具有SMB访问权限的卷时、系统会为您提供一系列用于保护该卷的选项。

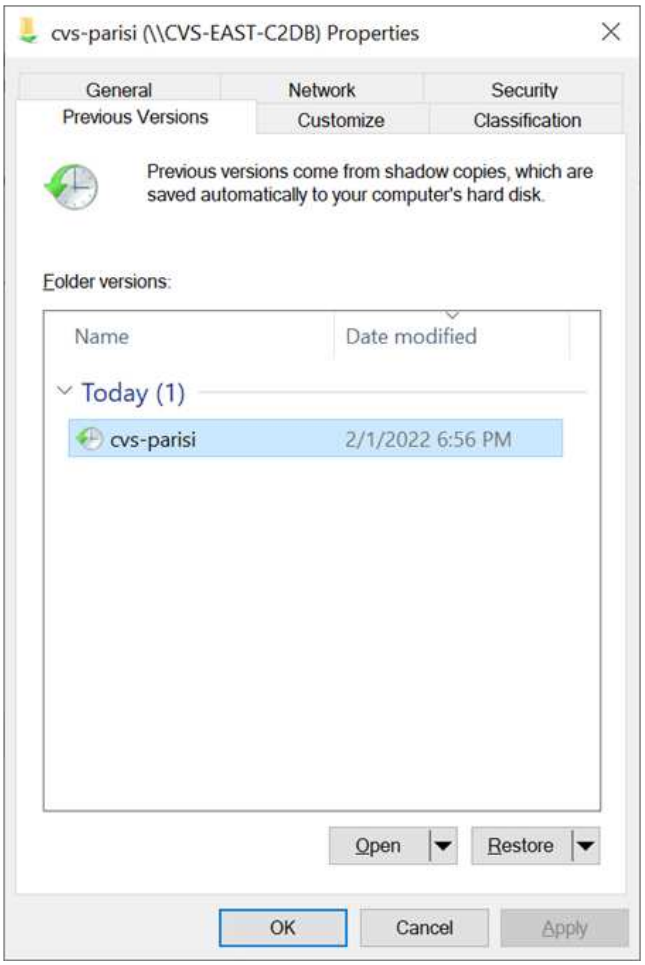
其中一些选项取决于Cloud Volumes Service 级别(性能或软件)、选项包括：

- *使Snapshot目录可见(可用于CVS-Performance和CVS-SW)。*此选项控制SMB客户端是否可以访问SMB共享中的Snapshot目录(`\\server\share~snapshot`和/或先前版本选项卡)。默认设置不会选中、这意味着卷默认隐藏和禁止访问~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(从AV扫描中隐藏这些文件夹)或偏好、可能需要向最终用户隐藏Snapshot副本。Cloud Volumes Service 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Snapshot目录中的文件。创建Snapshot副本时对文件或文件夹的文件权限将适用。如果文件或文件夹在Snapshot副本之间的权限发生变化、则所做的更改也会应用于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Snapshot目录中的文件、但可以从Snapshot目录中复制文件或文件夹。

- *启用SMB加密(可用于CVS-Performance和CVS-SW)。*默认情况下、SMB共享上禁用SMB加密(未选中)。选中此复选框可启用SMB加密、这意味着SMB客户端和服务器之间的流量将使用协商的最高支持加密级别进行动态加密。Cloud Volumes Service 最多支持对SMB进行AES-256加密。启用SMB加密确实会对SMB客户端造成性能降低、这种降低可能会也可能不会对SMB客户端造成明显影响、大致处于10-20%的范围

内。NetApp强烈建议通过测试来确定性能降低是否可接受。

- *隐藏SMB共享(可用于CVS-Performance和CVS-SW)。*设置此选项可在正常浏览时隐藏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`\\CVS-SMB`)时无法看到共享。选中此复选框后、只有明确知道SMB共享路径或具有组策略对象定义的共享路径的客户端才能访问此路径(通过混淆实现安全性)。
- *启用基于访问的枚举(ABE)(仅限CVS-SW)。*这与隐藏SMB共享类似、只是共享或文件仅对无权访问对象的用户或组隐藏。例如、如果至少不允许Windows用户`Joe`通过权限进行读取访问、则Windows用户`Joe`根本看不到SMB共享或文件。默认情况下、此选项处于禁用状态、您可以通过选中此复选框来启用它。有关ABE的详细信息、请参见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**CVS-Performance)**。 "持续可用的SMB共享" 通过在Cloud Volumes Service 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。这不是一项安全功能、但可以提供更好的整体故障恢复能力。目前、此功能仅支持SQL Server和FSLogix应用程序。

默认隐藏共享

在Cloud Volumes Service 中创建SMB服务器时、会显示 "隐藏的管理共享" (使用$命名约定)。其中包括C$(命名空间访问)和IPC$(共享命名管道以在程序之间进行通信、例如用于Microsoft管理控制台(MMC)访问的远程操作步骤 调用(RPC))。

ipc$共享不包含共享ACL、无法修改—它严格用于RPC调用和 "默认情况下、Windows不允许匿名访问这些共享"。

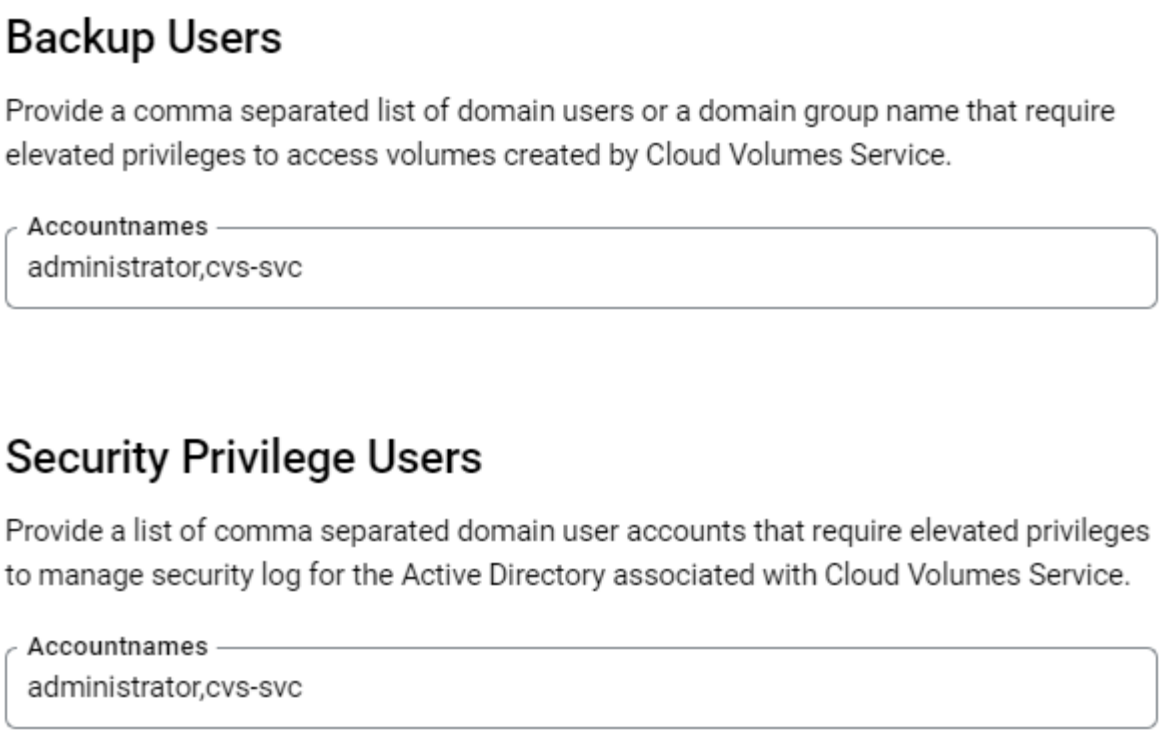
默认情况下、C$共享允许BUILTIN/Administrators访问、但Cloud Volumes Service 自动化会删除共享ACL、并且不允许任何人访问、因为访问C$共享可以查看Cloud Volumes Service 文件系统中所有已挂载的卷。因此、尝试导航到`\\Server\C$`失败。

具有本地**/BUILTIN**管理员/备份权限的帐户

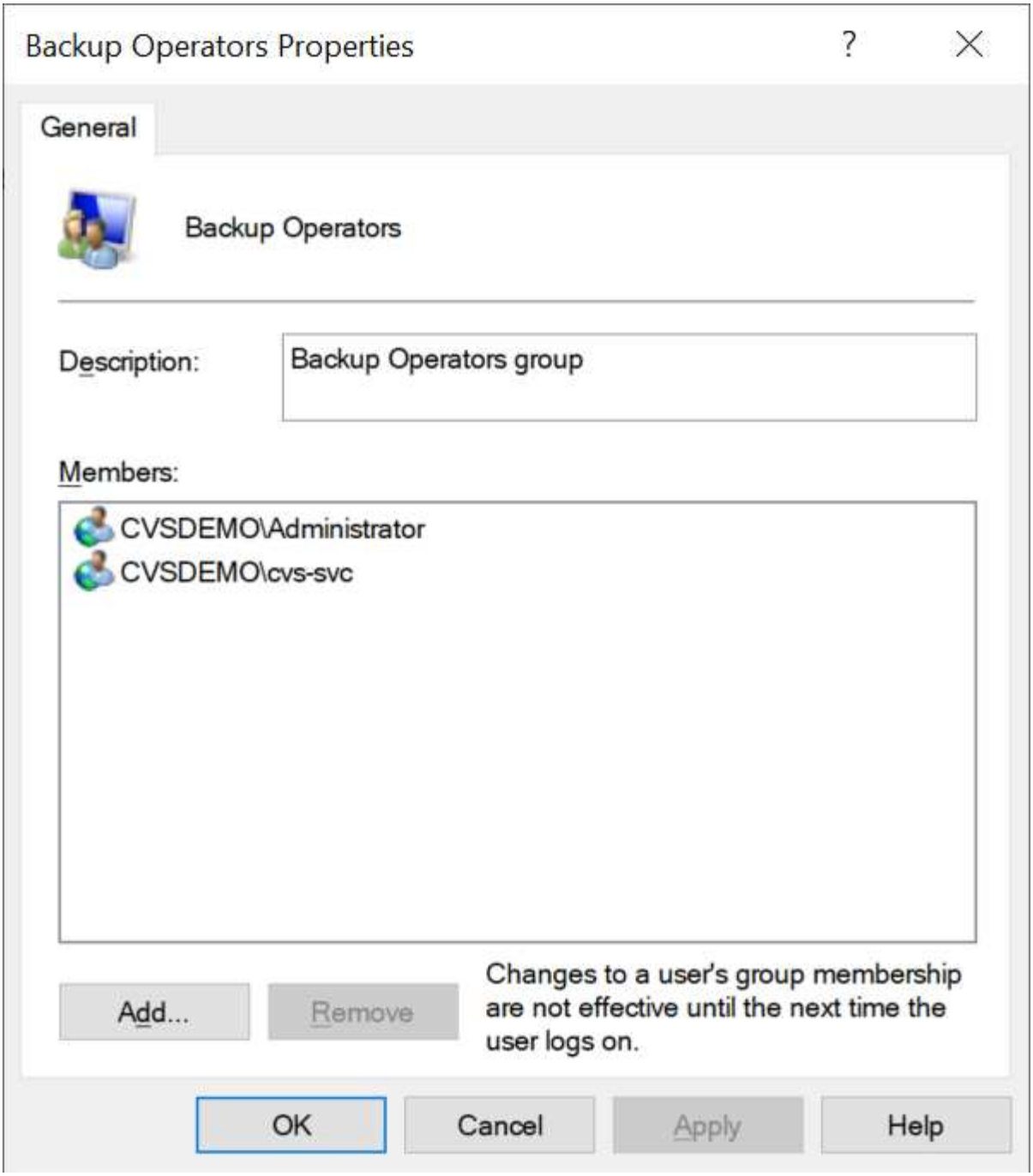
Cloud Volumes Service SMB服务器与常规Windows SMB服务器具有类似的功能、因为有本地组(例如BUILTIN\Administrators)会将访问权限应用于选定域用户和组。

指定要添加到备份用户的用户时、该用户将添加到使用该Active Directory连接的Cloud Volumes Service 实例中的BUILTIN\Backup Operators组中、然后该组将获取 "SeBackupPrivilege和SeRestorePrivilege"。

将用户添加到安全权限用户时、系统会为该用户授予SeSecurityPrivilege、这在某些应用程序使用情形下非常有用、例如 "SMB共享上的SQL Server"。



您可以使用适当的权限通过MMC查看Cloud Volumes Service 本地组成员资格。下图显示了已使用Cloud Volumes Service 控制台添加的用户。

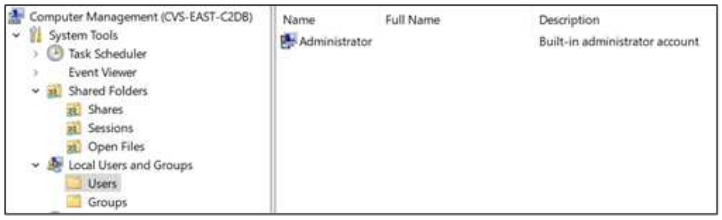


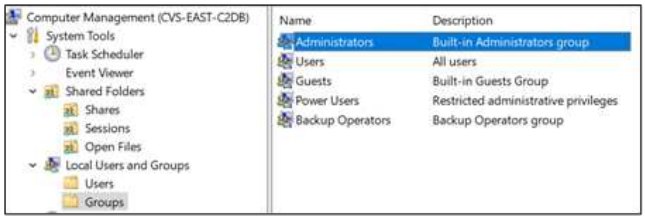
下表显示了默认BUILTIN组的列表以及默认添加的用户/组。

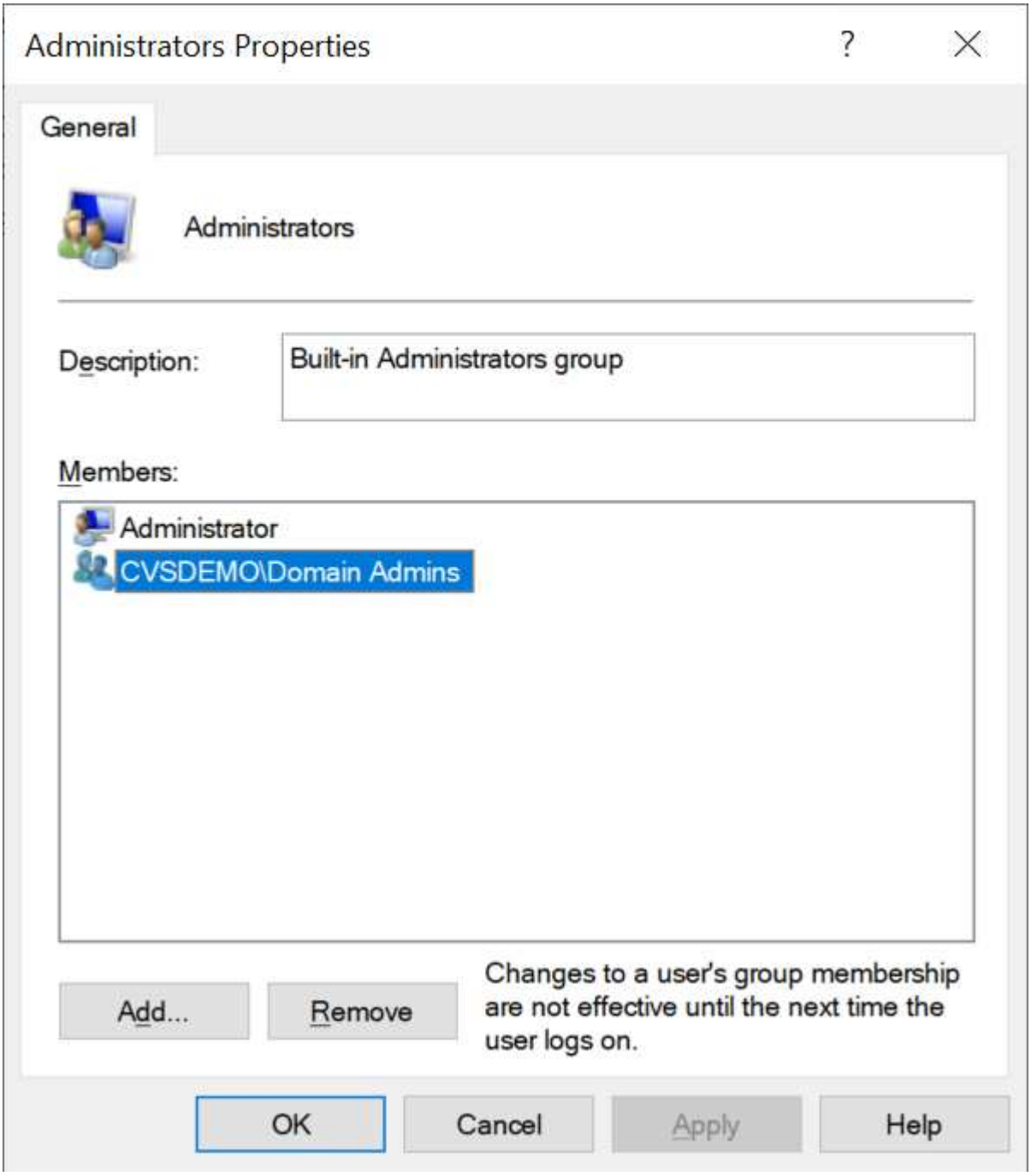
本地/**BUILTIN**组	默认成员
BUILTIN\Administrators *	域\域管理员
BUILTIN\Backup Operators*	无
BUILTIN\guests	域\域子系统
BUILTIN\Power Users	无
BUILTIN\Domain用户	域\域用户

*组成员资格在Cloud Volumes Service Active Directory连接配置中控制。

您可以在MMC窗口中查看本地用户和组(以及组成员)、但不能在此控制台中添加或删除对象或更改组成员资格。默认情况下、只有域管理员组和管理员才会添加到Cloud Volumes Service 中的BUILTIN\Administrators组。目前、您无法修改此设置。







MMC/计算机管理访问

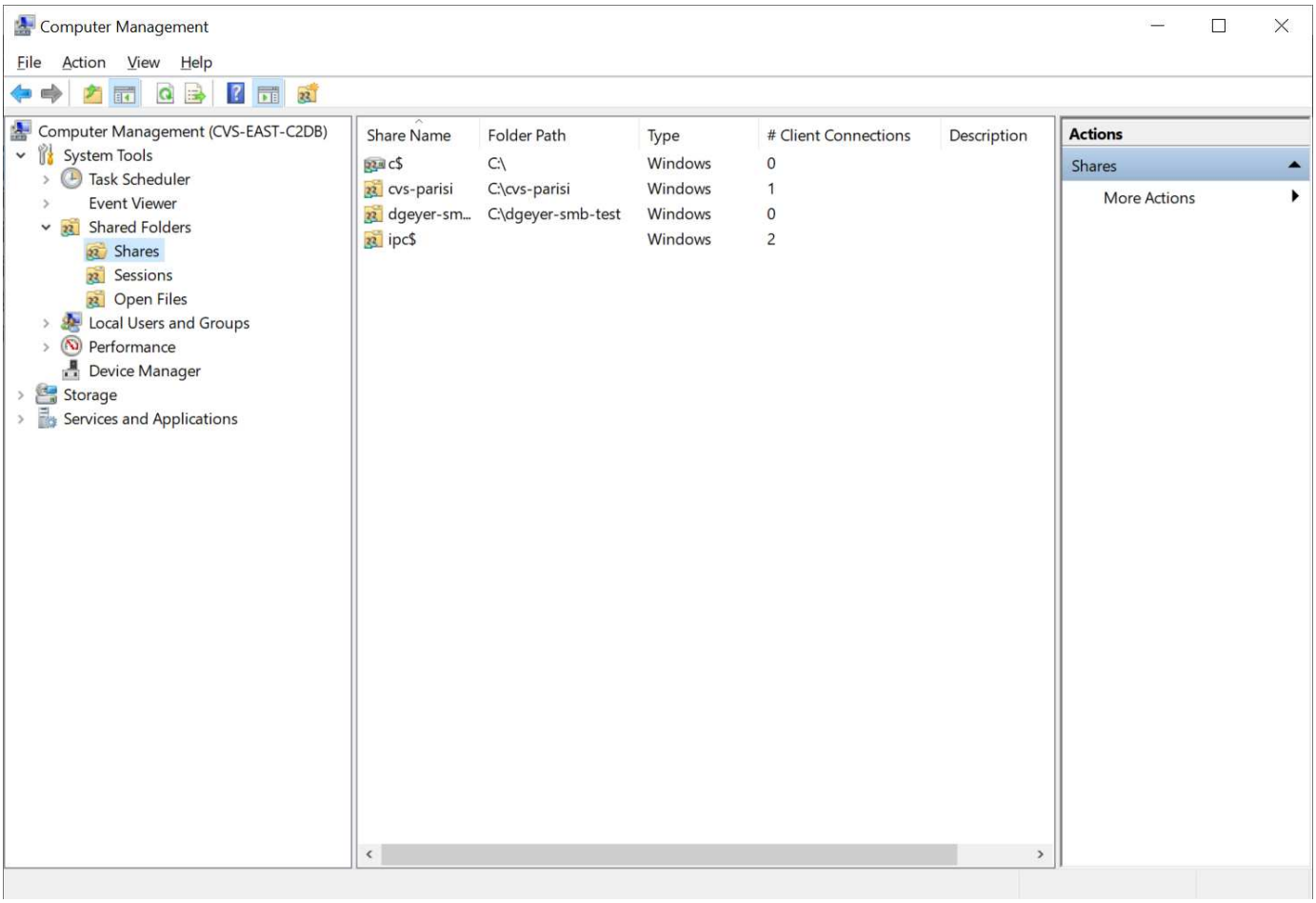
通过Cloud Volumes Service 中的SMB访问、您可以连接到计算机管理MMC、从而可以查看共享、管理共享ACL、以及查看/管理SMB会话和打开的文件。

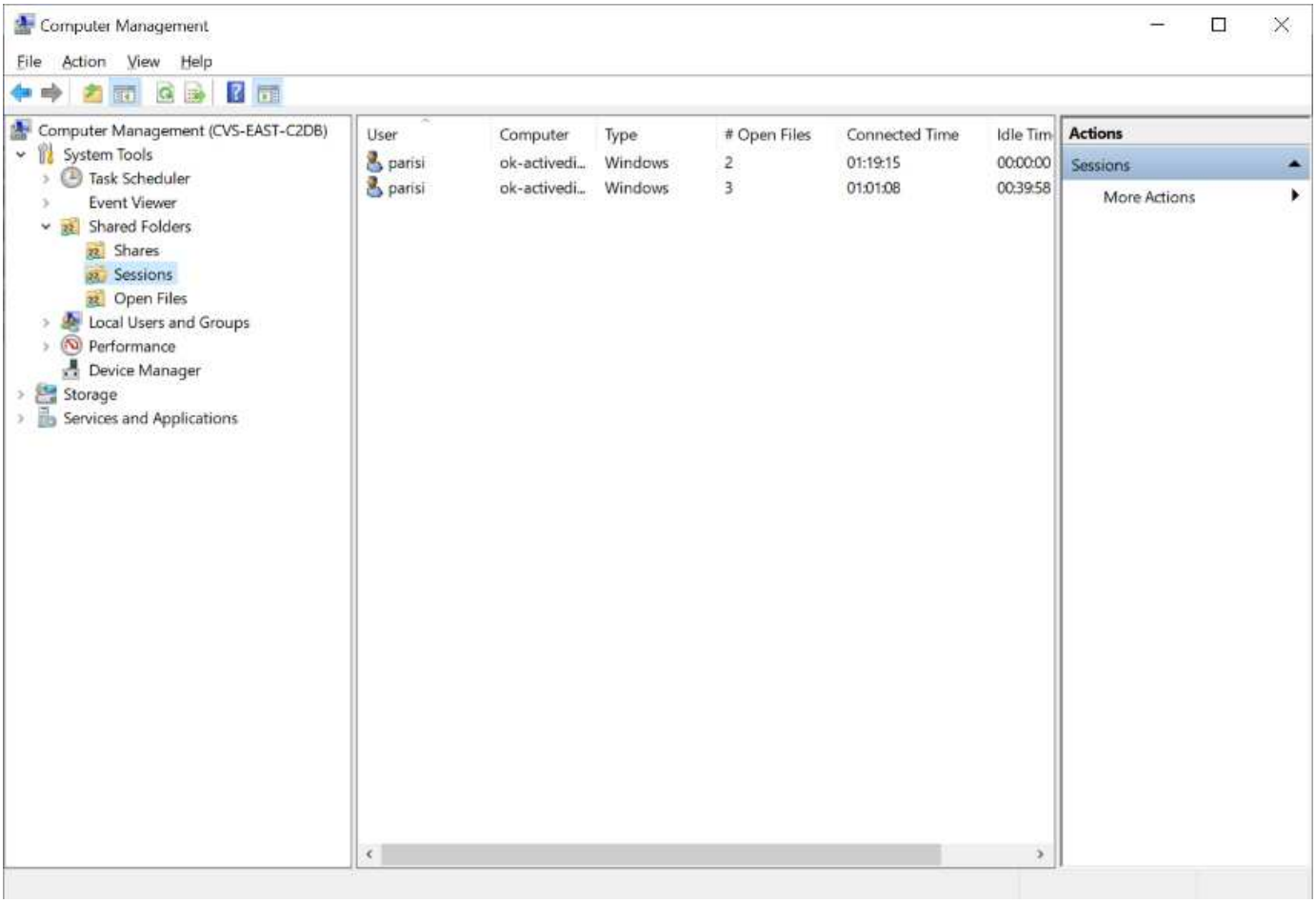
要使用MMC在Cloud Volumes Service 中查看SMB共享和会话、登录的用户当前必须是域管理员。其他用户可以通过MMC查看或管理SMB服务器、并在尝试查看Cloud Volumes Service SMB实例上的共享或会话时收到"您没有权限"对话框。

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。此时将打开选择计算机对话框、在此可以输入SMB服务器名称(可在Cloud Volumes Service 卷信息中找到)。

查看具有适当权限的SMB共享时、您会看到Cloud Volumes Service 实例中共享Active Directory连接的所有可用共享。要控制此行为、请在Cloud Volumes Service 卷实例上设置隐藏SMB共享选项。

请记住、每个区域仅允许一个Active Directory连接。





下表列出了MMC支持/不支持的功能。

支持的功能	不支持的功能
• 查看共享 • 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 • 关闭系统中已打开的文件 • 关闭打开的会话 • 创建 / 管理共享	• 创建新的本地用户 / 组 • 管理/查看现有本地用户/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

Cloud Volumes Service 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、票证期限、加密等。

下表列出了这些选项、它们的功能、默认配置以及是否可以使用Cloud Volumes Service 进行修改。某些选项不

适用于Cloud Volumes Service。

安全选项	功能	默认值	是否可以更改?
最大Kerberos时钟间隔(分钟)	Cloud Volumes Service 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、则Kerberos身份验证将失败。此值设置为Active Directory默认值。	5.	否
Kerberos票证生命周期(小时)	在要求续订之前、Kerberos票证保持有效的最长时间。如果在10小时之前未发生续订、您必须获取新的服务单。Cloud Volumes Service 会自动执行这些续订。Active Directory默认值为10小时。	10	否
Kerberos票证续订上限(天)	在需要新的授权请求之前可以续订Kerberos票证的最长天数。Cloud Volumes Service 会自动续订SMB连接的服务单。Active Directory默认值为七天。	7.	否
Kerberos KDC连接超时(秒)	KDC连接超时前的秒数。	3.	否
传入SMB流量需要签名	设置为SMB流量需要签名。如果设置为true、则不支持签名的客户端连接将失败。	false	
本地用户帐户需要密码复杂度	用于本地SMB用户的密码。Cloud Volumes Service 不支持创建本地用户、因此此选项不适用于Cloud Volumes Service。	true	否
对Active Directory LDAP连接使用start_tls	用于为Active Directory LDAP启用启动TLS连接。Cloud Volumes Service 当前不支持启用此功能。	false	否
已启用适用于Kerberos的AES-128和AES-256加密	此选项用于控制是否对Active Directory连接使用AES加密、并在创建/修改Active Directory连接时使用为Active Directory身份验证启用AES加密选项进行控制。	false	是的。

安全选项	功能	默认值	是否可以更改?
LM兼容性级别	Active Directory连接支持的身份验证方言级别。请参见第节"SMB身份验证方言"了解更多信息。	NTLMv2-KRB	否
传入CIFS流量需要SMB加密	所有共享都需要SMB加密。Cloud Volumes Service 不会使用此功能；而是按卷设置加密(请参见一节SMB共享安全功能")。	false	否
客户端会话安全性	为LDAP通信设置签名和/或密封。目前未在Cloud Volumes Service 中设置此选项、但在未来版本中可能需要执行此操作。本节将介绍由于Windows修补程序而导致的LDAP身份验证问题的修复方法 ""LDAP通道绑定。""。	无	否
SMB2为DC连接启用	使用SMB2进行DC连接。默认情况下处于启用状态。	系统默认值	否
LDAP转介跟踪	使用多个LDAP服务器时、如果在第一个服务器中找不到条目、则转介跟踪功能允许客户端引用列表中的其他LDAP服务器。Cloud Volumes Service 目前不支持此功能。	false	否
使用LDAPS实现安全Active Directory连接	启用基于SSL的LDAP。Cloud Volumes Service 目前不支持。	false	否
DC连接需要加密	要成功建立DC连接、需要加密。默认情况下、在Cloud Volumes Service 中处于禁用状态。	false	否

双协议/多协议

通过Cloud Volumes Service 、可以向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以及使用中央后端LDAP服务器向Cloud Volumes Service 提供UNIX身份来实现的。您可以使用Windows Active Directory为Windows和UNIX用户提供方便易用的功能。

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导出可通过Cloud Volumes Service 实例进行管理。SMB使用CIFS/SMB共享和共享ACL、在用户和组级别提供更精细的控制。您只能使用从SMB客户端配置共享级ACL "MMC/计算机管理"具有Cloud Volumes Service 实例管理员权限的帐户(请参见一节 ""具有本地/BUILTIN管理员/备份权限的帐户。""）。
- *文件访问控制。*在文件或文件夹级别控制权限、并且始终从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。

为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、请参见"[权限模型]。 "

用户映射

当客户端访问卷时、Cloud Volumes Service 会尝试反向将传入用户映射到有效用户。这一点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宣称的用户是必不可少的。

例如、如果名为`joe`的Windows用户尝试通过SMB访问具有UNIX权限的卷、则Cloud Volumes Service 将执行搜索以查找名为`joe`的相应UNIX用户。如果存在一个、则以Windows用户`joe`的身份写入SMB共享的文件在NFS客户端中显示为UNIX用户`joe`。

或者、如果名为`Joe`的UNIX用户尝试使用Windows权限访问Cloud Volumes Service 卷、则UNIX用户必须能够映射到有效的Windows用户。否则、将拒绝对卷的访问。

目前、只有Active Directory支持使用LDAP进行外部UNIX身份管理。有关配置对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、Cloud Volumes Service 会使用卷的安全模式来确定ACL的类型。这些安全模式是根据指定的NAS协议设置的、对于双协议、则是在创建Cloud Volumes Service 卷时选择的。

- 如果您仅使用NFS、则Cloud Volumes Service 卷将使用UNIX权限。
- 如果您仅使用SMB、则Cloud Volumes Service 卷将使用NTFS权限。

如果要创建双协议卷、则可以在创建卷时选择ACL模式。应根据所需的权限管理来做出此决策。如果您的用户从Windows/SMB客户端管理权限、请选择NTFS。如果您的用户希望使用NFS客户端和chmod/chown、请使用UNIX安全模式。

创建**Active Directory**连接的注意事项

通过Cloud Volumes Service 、可以将Cloud Volumes Service 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。要在Cloud Volumes Service 中使用SMB、需要创建Active Directory连接。

此配置提供了多个选项、需要在一定程度上考虑安全性。外部Active Directory服务器可以是内部实例或云原生。如果您使用的是内部Active Directory服务器、请勿将域公开到外部网络(例如使用DMZ或外部IP地址)。而是使用安全专用通道或VPN、单向林信任或专用网络连接到内部网络 "私有 Google 访问"。有关的详细信息、请参见Google Cloud文档 "在Google Cloud中使用Active Directory的最佳实践"。

CVS-SW要求Active Directory服务器位于同一区域。如果尝试在CVS-SW中与另一个区域建立DC连接、则尝试将失败。使用CVS-SW时、请务必创建包含Active Directory DC的Active Directory站点、然后在Cloud Volumes Service 中指定站点、以避免尝试跨区域DC连接。

Active Directory凭据

启用SMB或LDAP for NFS后、Cloud Volumes Service 将与Active Directory控制器进行交互、以创建用于身份验证的计算机帐户对象。这与Windows SMB客户端加入域的方式并要求对Active Directory中的组织单位(OU)具有相同的访问权限没有区别。

在许多情况下、安全组不允许在Cloud Volumes Service 等外部服务器上使用Windows管理员帐户。在某些情况下、作为安全最佳实践、Windows管理员用户将被完全禁用。

创建SMB计算机帐户所需的权限

要将Cloud Volumes Service 计算机对象添加到Active Directory、此帐户对域具有管理权限或具有管理权限 "用于创建和修改计算机帐户对象的委派权限" 指定的OU为必填项。您可以使用Active Directory中的"控制委派向导"执行此操作、方法是创建一个自定义任务、使用户能够使用提供的以下访问权限创建/删除计算机对象：

- 读 / 写
- 创建/删除所有子对象
- 读/写所有属性
- 更改/重置密码

这样会自动将定义的用户的安全ACL添加到Active Directory中的OU中、并最大限度地减少对Active Directory环境的访问。委派用户后、可以在此窗口中将此用户名和密码作为Active Directory凭据提供。

传递到Active Directory域的用户名和密码会在计算机帐户对象查询和创建期间利用Kerberos加密来提高安全性。

Active Directory连接详细信息

。 "Active Directory连接详细信息" 为管理员提供字段、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*用于指定某个区域中的Active Directory连接是用于Cloud Volumes Service 服务类型的卷还是CVS-Performance服务类型的卷。如果在现有连接上设置不正确、则在使用或编辑时可能无法正常工作。
- 域。 Active Directory域名。
- *站点*为了保证安全性和性能、将Active Directory服务器限制为特定站点 "注意事项"。如果多个Active Directory服务器跨越多个区域、则必须执行此操作、因为Cloud Volumes Service 目前不支持向Cloud Volumes Service 实例以外的其他区域的Active Directory服务器发出Active Directory身份验证请求。(例如、Active Directory域控制器所在的区域仅支持CVS-Performance、但您希望在CVS-SW实例中使用SMB共享。)
- * DNS服务器。*要在名称查找中使用的DNS服务器。
- * NetBIOS名称(可选)。*如果需要、则为服务器指定NetBIOS名称。这是使用Active Directory连接创建新计算机帐户时使用的。例如、如果NetBIOS名称设置为cvs-East、则计算机帐户名称将为cvs-East-｛1234｝。请参见一节 "Cloud Volumes Service 在Active Directory中的显示方式" 有关详细信息 …

- *组织单位(OU)。*用于创建计算机帐户的特定OU。如果要将计算机帐户的控制权委派给特定OU的用户、则此功能非常有用。
- * AES加密。*您也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加密可在用户和组查找期间为Cloud Volumes Service 到Active Directory的通信提供额外的安全性。启用此选项之前、请与域管理员联系以确认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、请确认已将Cloud Volumes Service Active Directory连接配置为启用AES。否则、身份验证将失败。启用AES加密不会禁用较弱的密码、而是会向Cloud Volumes Service SMB计算机帐户添加对AES密码的支持。

Kerberos域详细信息

此选项不适用于SMB服务器。而是在为Cloud Volumes Service 系统配置NFS Kerberos时使用。填充这些详细信息后、将配置NFS Kerberos域(类似于Linux上的krb5.conf文件)、并在创建Cloud Volumes Service 卷时指定NFS Kerberos时使用此域、因为Active Directory连接充当NFS Kerberos分发中心(KDC)。

> 目前不支持将非Windows KDC与Cloud Volumes Service 结合使用。

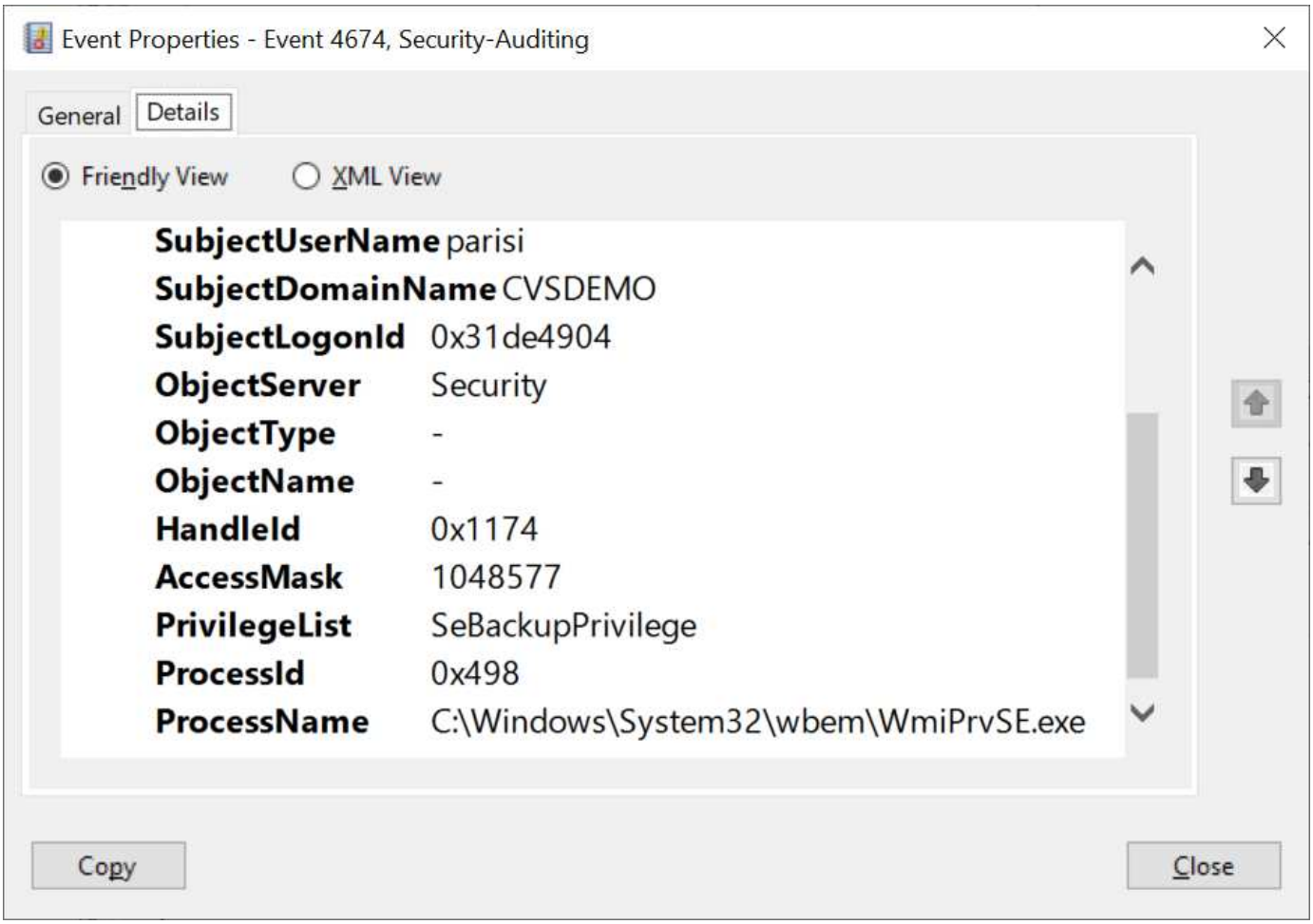
Region

使用区域可以指定Active Directory连接所在的位置。此区域必须与Cloud Volumes Service 卷所在的区域相同。

- *使用LDAP的本地NFS用户。*本节还提供了一个允许使用LDAP的本地NFS用户的选项。如果要将UNIX用户组成员资格支持扩展到NFS (扩展组)的16组限制之外、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、请取消选择此选项。如果您有LDAP服务器、并且还希望使用本地UNIX用户(例如root)、请选择此选项。

备份用户

使用此选项可以指定对Cloud Volumes Service 卷具有备份权限的Windows用户。某些应用程序需要使用备份特权(SeBackupPrivilege)来正确备份和还原NAS卷中的数据。此用户对卷中的数据具有较高的访问权限、因此您应考虑这一点 "启用对该用户访问的审核"。启用后、审核事件将显示在事件查看器> Windows日志>安全性中。



安全权限用户

使用此选项可以指定对Cloud Volumes Service 卷具有安全修改权限的Windows用户。某些应用程序需要安全特权(SeSecurityPrivilege) ("例如SQL Server")以在安装期间正确设置权限。管理安全日志需要此权限。虽然此特权的功能不如SeBackupPrivilege强大、但NetApp建议这样做 "审核用户的访问权限" 如果需要、则使用此权限级别。

有关详细信息，请参见 "分配给新登录的特殊权限"。

Cloud Volumes Service 在Active Directory中的显示方式

Cloud Volumes Service 在Active Directory中显示为普通计算机帐户对象。命名约定如下。

- CIFS/SMB和NFS Kerberos会创建单独的计算机帐户对象。
- 启用了LDAP的NFS会在Active Directory中为Kerberos LDAP绑定创建一个计算机帐户。
- 使用LDAP的双协议卷共享LDAP和SMB的CIFS/SMB计算机帐户。
- CIFS/SMB计算机帐户的命名约定为name-1234 (随机四位ID、并在< 10个字符名称后附加连字符)。您可以通过Active Directory连接上的NetBIOS名称设置来定义名称(请参见一节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)。如果使用的字符数超过15个、则名称为nfs-truncated-name-1234。
- 启用了LDAP的仅NFS CVS-Performance实例创建一个SMB计算机帐户、以便使用与CIFS/SMB实例相同的命名约定绑定到LDAP服务器。

- 创建SMB计算机帐户时、默认隐藏的管理共享(请参见一节 ""默认隐藏共享"")也会创建(c$、admin$、ipc$)、但这些共享没有分配ACL、因此无法访问。
- 默认情况下、计算机帐户对象放置在CN=Computers中、但您可以在必要时指定其他OU。请参见第节"创建SMB计算机帐户所需的权限有关为Cloud Volumes Service 添加/删除计算机帐户对象所需的访问权限的信息。

当Cloud Volumes Service 将SMB计算机帐户添加到Active Directory时、将填充以下字段：

- cn (使用指定的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、则允许使用计算机Kerberos帐户使用DES_CBC_MD5、RC4_HMAC_MD5、AES128_CTS_HMAC_SHA1_96、AES256_CTS_HMAC_SHA1_96)
- 名称(使用SMB服务器名称)
- sAMAccountName (使用SMBserver$)
- servicePrincipalName (具有用于Kerberos的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)、则可以将计算机帐户上的MSDS-SupportedEncryptionTypes值更改为下表中的一个值、以便仅允许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 个	DES_CBC_MD5、RC4_HMAC、AES128_CTS_HMAC_SHA1_96和AES256_CTS_HMAC_SHA1_96

要为SMB计算机帐户启用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。

为NFS Kerberos启用AES加密、 "请参见Cloud Volumes Service 文档"。

其他**NAS**基础架构服务依赖关系**(KDC**、**LDAP**和**DNS)**

在对NAS共享使用Cloud Volumes Service 时、可能需要外部依赖关系才能正常运行。这些依赖关系在特定情况下起作用。下表显示了各种配置选项以及需要哪些依赖关系(如果有)。

Configuration	需要依赖关系
仅限NFSv3	无
仅限NFSv3 Kerberos	Windows Active Directory：* KDC * DNS * LDAP

Configuration	需要依赖关系
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 Active Directory：KDC DNS LDAP
仅SMB	Active Directory：* 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 Active Directory：KDC DNS LDAP

计算机帐户对象的**Kerberos keytab**轮换/密码重置

对于SMB计算机帐户、Cloud Volumes Service 会为SMB计算机帐户计划定期密码重置。这些密码重置会使用Kerberos加密进行、并按每第四个星期日的计划在晚上11点到凌晨1点之间随机运行。这些密码重置会更改Kerberos密钥版本、轮换存储在Cloud Volumes Service 系统上的密钥选项卡、并帮助保持在Cloud Volumes Service 中运行的SMB服务器的更高级别安全性。计算机帐户密码是随机设置的、管理员不知道这些密码。

对于NFS Kerberos计算机帐户、只有在与KDC创建/交换新的keytab时、才会发生密码重置。目前、在Cloud Volumes Service 中无法执行此操作。

用于**LDAP**和**Kerberos**的网络端口

使用LDAP和Kerberos时、您应确定这些服务正在使用的网络端口。您可以在中找到Cloud Volumes Service 正在使用的端口的完整列表 "有关安全注意事项的Cloud Volumes Service 文档"。

LDAP

Cloud Volumes Service 充当LDAP客户端、并使用标准LDAP搜索查询来查找用户和组的UNIX身份。如果要使用Cloud Volumes Service 提供的标准默认用户之外的用户和组、则需要使用LDAP。如果您计划将NFS Kerberos与用户主体(如user1@domain.com)结合使用、也需要LDAP。目前、仅支持使用Microsoft Active Directory的LDAP。

要使用Active Directory作为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。Cloud Volumes Service 使用默认LDAP模式模板、根据查询属性 "RFC-2307-bis"。因此、下表显示了为用户和组填充所需的最小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	功能
UID*	指定UNIX用户名
uidNumber*	指定UNIX用户的数字ID
gidNumber*	指定UNIX用户的主组数字ID
objectclass*	指定正在使用的对象类型；Cloud Volumes Service 要求在对象类列表中包含"用户"(默认情况下、大多数Active Directory部署都包含此用户)。

属性	功能
name	有关帐户的常规信息(真实姓名、电话号码等、也称为gecos)
unixUserPassword	无需设置此参数；不会在用于NAS身份验证的UNIX身份查找中使用。如果设置此选项、则会将配置的unixUserPassword值设置为纯文本。
unixHomeDirectory	定义用户从Linux客户端根据LDAP进行身份验证时UNIX主目录的路径。如果要使用LDAP for UNIX主目录功能、请设置此选项。
loginShell	定义用户根据LDAP进行身份验证时Linux客户端的bash/配置文件Shell的路径。

*表示要在Cloud Volumes Service 中正常运行、必须具有属性。其余属性仅供客户端使用。

属性	功能
CN*	指定UNIX组名称。使用Active Directory进行LDAP时、会在首次创建对象时设置此值、但可以稍后更改。此名称不能与其他对象相同。例如、如果名为user1的UNIX用户属于Linux客户端上名为user1的组、则Windows不允许两个具有相同CN属性的对象。要解决此问题、请将Windows用户重命名为唯一名称(例如user1-unix)；Cloud Volumes Service 中的LDAP将使用UID属性作为UNIX用户名。
gidNumber*	指定UNIX组数字ID。
objectclass*	指定正在使用的对象类型；Cloud Volumes Service 要求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)。
memberUID	指定哪些UNIX用户是UNIX组的成员。对于Cloud Volumes Service 中的Active Directory LDAP、不需要此字段。Cloud Volumes Service LDAP模式使用成员字段作为组成员资格。
成员*	组成员资格/二级UNIX组必需。此字段通过向Windows组添加Windows用户来填充。但是、如果Windows组未填充UNIX属性、则这些属性不会包含在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。

*表示要在Cloud Volumes Service 中正常运行、必须具有属性。其余属性仅供客户端使用。

LDAP绑定信息

要在LDAP中查询用户、Cloud Volumes Service 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属性以查找目录。目前、LDAP绑定只能使用SMB计算机帐户。

您只能为`CVS-Performance`实例启用LDAP、并将其用于NFSv3、NFSv4.1或双协议卷。要成功部署已启用LDAP的卷、必须在与Cloud Volumes Service 卷相同的区域建立Active Directory连接。

启用LDAP后、在特定情况下会发生以下情况。

- 如果Cloud Volumes Service 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计算机帐户、并且Cloud Volumes Service 中的LDAP客户端会使用计算机帐户凭据绑定到Active Directory。不会为NFS卷和默认隐藏管理共享创建SMB共享(请参见一节 ""默认隐藏共享"")已删除共享ACL。
- 如果Cloud Volumes Service 项目使用双协议卷、则只会使用为SMB访问创建的单个计算机帐户将Cloud Volumes Service 中的LDAP客户端绑定到Active Directory。不会创建其他计算机帐户。
- 如果专用SMB卷是单独创建的(在启用具有LDAP的NFS卷之前或之后)、则用于LDAP绑定的计算机帐户将与SMB计算机帐户共享。
- 如果还启用了NFS Kerberos、则会创建两个计算机帐户—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绑定已加密、但LDAP查询仍会使用通用LDAP端口389以纯文本形式通过网线进行传递。目前无法在Cloud Volumes Service 中更改此众所周知的端口。因此、有权在网络中嗅探数据包的用户可以查看用户和组名称、数字ID以及组成员资格。

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VM才能看到LDAP服务器的流量。有关在Cloud Volumes Service 中嗅探数据包的详细信息、请参见一节 "《数据包嗅探/跟踪注意事项》。"

LDAP客户端配置默认值

在Cloud Volumes Service 实例中启用LDAP后、默认情况下会创建一个LDAP客户端配置、其中包含特定的配置详细信息。在某些情况下、选项不适用于Cloud Volumes Service (不受支持)或不可配置。

LDAP客户端选项	功能	默认值	是否可以更改?
LDAP服务器列表	设置要用于查询的LDAP服务器名称或IP地址。这不适用于Cloud Volumes Service。而是使用Active Directory域定义LDAP服务器。	未设置	否
Active Directory域	设置用于LDAP查询的Active Directory域。Cloud Volumes Service 利用DNS中LDAP的SRV记录在域中查找LDAP服务器。	设置为在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。Cloud Volumes Service 不支持。而是使用Active Directory站点控制LDAP服务器选择。	未设置。	否
使用SMB服务器凭据绑定	使用SMB计算机帐户绑定到LDAP。目前、Cloud Volumes Service 中唯一支持的LDAP绑定方法。	true	否

LDAP客户端选项	功能	默认值	是否可以更改?
模式模板	用于LDAP查询的模式模板。	MS-AD-BIS	否
LDAP服务器端口	用于LDAP查询的端口号。Cloud Volumes Service 当前仅使用标准LDAP端口389。目前不支持LDAPS/端口636。	389.	否
是否已启用LDAPS	控制是否对查询和绑定使用基于安全套接字层的LDAP (SSL)。Cloud Volumes Service 目前不支持。	false	否
查询超时(秒)	查询超时。如果查询所用时间超过指定值、则查询将失败。	3.	否
最低绑定身份验证级别	支持的最低绑定级别。由于Cloud Volumes Service使用计算机帐户进行LDAP绑定、并且默认情况下Active Directory不支持匿名绑定、因此出于安全考虑、此选项不起作用。	匿名	否
绑定 DN	使用简单绑定时用于绑定的用户/可分辨名称(DN)。Cloud Volumes Service使用计算机帐户进行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搜索的基础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	基础DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service仅支持子树搜索。	子树	否
用户DN	定义LDAP查询的用户搜索开始位置的DN。目前Cloud Volumes Service不支持、因此所有用户搜索均从基础DN开始。	未设置	否

LDAP客户端选项	功能	默认值	是否可以更改?
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。Cloud Volumes Service 不支持设置用户搜索范围。	子树	否
组DN	定义为LDAP查询开始组搜索的DN。目前Cloud Volumes Service 不支持、因此所有组搜索均从基础DN开始。	未设置	否
组搜索范围	组DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service 不支持设置组搜索范围。	子树	否
网络组DN	定义为LDAP查询启动网络组搜索的DN。目前Cloud Volumes Service 不支持、因此所有网络组搜索均从基础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。Cloud Volumes Service 不支持设置网络组搜索范围。	子树	否
使用基于LDAP的start_tls	利用Start TLS通过端口389建立基于证书的LDAP连接。Cloud Volumes Service 目前不支持。	false	否
启用netgroup-by-host查找	启用按主机名查找网络组、而不是扩展网络组以列出所有成员。Cloud Volumes Service 目前不支持。	false	否
按主机的网络组DN	定义在LDAP查询中按主机搜索网络组的起始DN。Cloud Volumes Service 当前不支持按主机进行网络组。	未设置	否
netgroup-by-host搜索范围	netgroup-by-host DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service 当前不支持按主机进行网络组。	子树	否

LDAP客户端选项	功能	默认值	是否可以更改?
客户端会话安全性	定义LDAP使用的会话安全级别(签名、签章或无)。如果Active Directory请求、CVS-Performance支持LDAP签名。CVS-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转介跟踪	使用多个LDAP服务器时、如果在第一个服务器中找不到条目、则转介跟踪功能允许客户端引用列表中的其他LDAP服务器。Cloud Volumes Service 目前不支持此功能。	false	否
组成员资格筛选器	提供了一个自定义LDAP搜索筛选器、用于从LDAP服务器查找组成员资格。Cloud Volumes Service 当前不支持。	未设置	否

使用**LDAP**进行非对称名称映射

默认情况下、Cloud Volumes Service 会双向映射用户名相同的Windows用户和UNIX用户、而无需特殊配置。只要Cloud Volumes Service 可以找到有效的UNIX用户(使用LDAP)、就会进行1：1名称映射。例如、如果使用了Windows用户`johnsmith`、则如果Cloud Volumes Service 在LDAP中找到名为`johnsmith`的UNIX用户、则该用户的名称映射将成功、则由`johnsmith`创建的所有文件/文件夹将显示正确的用户所有权、 而且、无论使用何种NAS协议、影响`johnsmith`的所有ACL都将得到遵守。这称为对称名称映射。

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`的UNIX身份为`jsmith`、则Cloud Volumes Service 需要了解此变体。由于Cloud Volumes Service 当前不支持创建静态名称映射规则、因此必须使用LDAP查找用户的身份以获取Windows和UNIX身份、以确保文件和文件夹的所有权以及所需权限正确无误。

默认情况下、Cloud Volumes Service 在名称映射数据库的实例的ns-switch中包含`ldap`、因此、要通过对非对称名称使用LDAP来提供名称映射功能、您只需修改某些用户/组属性以反映Cloud Volumes Service 的查找内容即可。

下表显示了为实现非对称名称映射功能、必须在LDAP中填充哪些属性。在大多数情况下、Active Directory已配置为执行此操作。

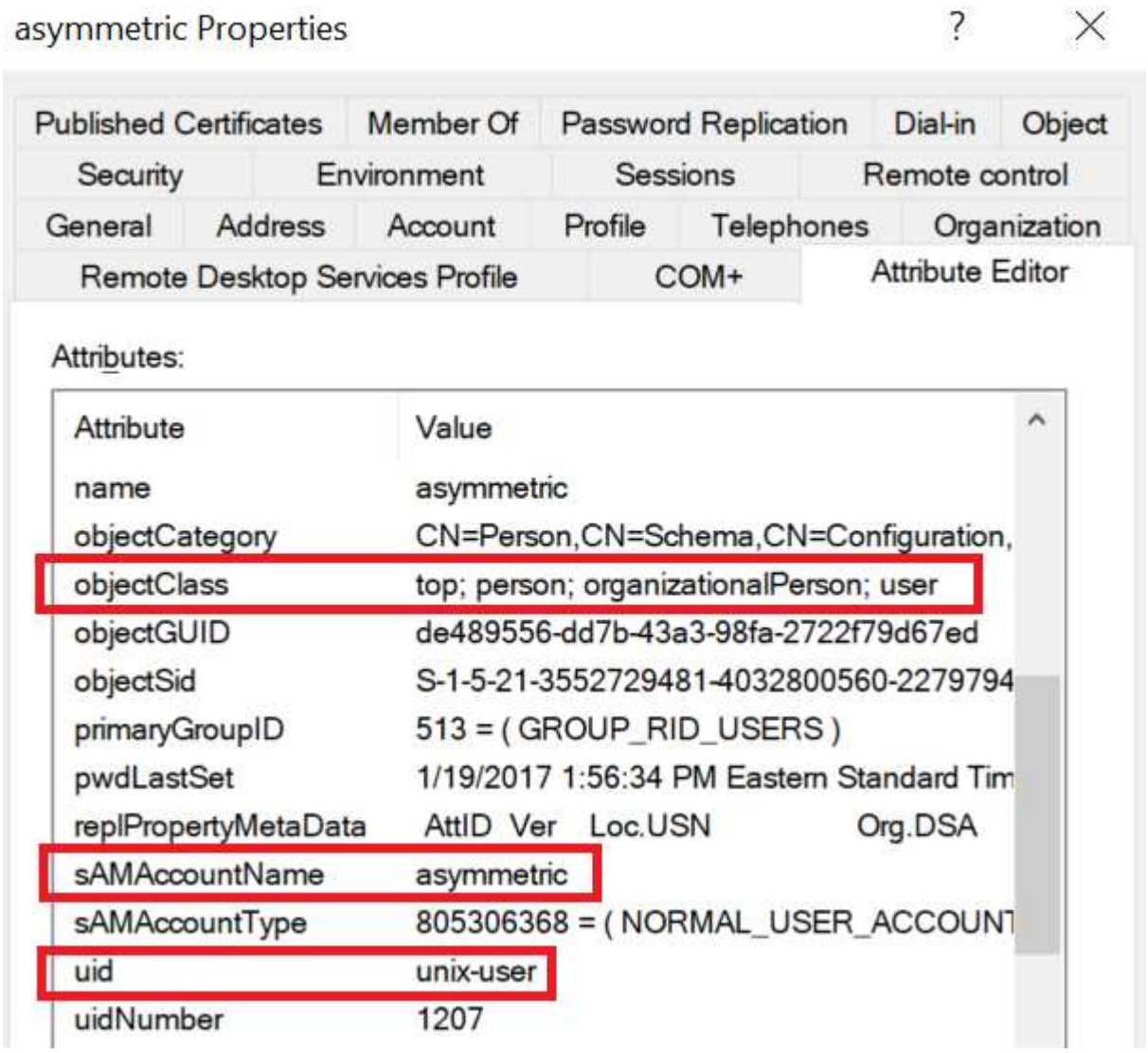
Cloud Volumes Service 属性	功能	**Cloud Volumes Service** 用于名称映射的值
Windows到UNIX对象类	指定要使用的对象类型。(即用户、组、posixAccount等)	必须包括用户(如果需要、可以包含多个其他值。)
Windows到UNIX属性	用于在创建时定义Windows用户名。Cloud Volumes Service 将此功能用于Windows到UNIX查找。	此处无需更改；sAMAccountName与Windows登录名相同。

Cloud Volumes Service 属性	功能	Cloud Volumes Service 用于名称映射的值
UID	定义UNIX用户名。	所需的UNIX用户名。

Cloud Volumes Service 当前不会在LDAP查找中使用域前缀、因此多域LDAP环境无法在LDAP命名映射查找中正常运行。

以下示例显示了一个名为`unymmetric`、UNIX名为`unix-user`的用户、以及从SMB和NFS写入文件时的行为。

下图显示了LDAP属性在Windows服务器中的外观。



在NFS客户端中、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
```

从NFS写入文件时、如果为`unix-user`、则NFS客户端会生成以下结果：

```
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)
```

在Windows客户端中、您可以看到文件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`非对称`从SMB客户端创建的文件将显示正确的UNIX所有者、如以下文本所示。

SMB：

```
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域控制器存在一个漏洞、 "Microsoft安全建议ADV190023" 更改DC允许LDAP绑定的方式。

对Cloud Volumes Service 的影响与对任何LDAP客户端的影响相同。Cloud Volumes Service 当前不支持通道绑定。由于Cloud Volumes Service 默认通过协商支持LDAP签名、因此LDAP通道绑定不应是问题描述。如果在启用了通道绑定的情况下绑定到LDAP时确实存在问题、请按照ADV190023中的修复步骤操作、以允许从Cloud Volumes Service 进行LDAP绑定。

DNS

Active Directory和Kerberos都依赖于DNS来进行主机名到IP/IP到主机名解析。DNS要求端口53处于打开状态。Cloud Volumes Service 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以限制哪些服务器可以更新DNS记录。有关详细信息，请参见 "保护Windows DNS的安全"。

请注意、Google项目中的资源默认使用Google Cloud DNS、而Google Cloud DNS未连接到Active Directory DNS。使用云DNS的客户端无法解析Cloud Volumes Service 返回的UNC路径。加入Active Directory域的Windows客户端已配置为使用Active Directory DNS、并且可以解析此类UNC路径。

要将客户端加入Active Directory、必须将其DNS配置为使用Active Directory DNS。或者、您也可以配置云DNS以将请求转发到Active Directory DNS。请参见 "为什么我的客户端无法解析SMB NetBIOS名称？"有关详细信息…

Cloud Volumes Service 当前不支持DNSSEC、DNS查询以纯文本形式执行。

文件访问审核

目前不支持Cloud Volumes Service。

防病毒保护

您必须在客户端的Cloud Volumes Service 中对NAS共享执行防病毒扫描。目前未将原生 防病毒与Cloud Volumes Service 集成。

服务操作

Cloud Volumes Service 团队负责管理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。

每个客户都获得自己的唯一子网、默认情况下、该子网的访问会与其他客户隔离、而Cloud Volumes Service 中的每个租户都获得自己的命名空间和VLAN以实现整体数据隔离。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。

物理安全性

经过适当的预先批准后、只有现场工程师和具有NetApp徽标的现场支持工程师(Field Support Engineer、FSE)才能访问固定框架和机架进行物理工作。不允许进行存储和网络管理。只有这些现场资源才能执行硬件维护任务。

对于现场工程师、将为工作说明书(SOW)提交一个服务单、其中包括机架ID和设备位置(RU)、所有其他详细信息均包含在服务单中。对于NetApp现场服务工程师、必须向Colo提交现场访问服务单、此服务单应包含访客的详细信息、日期和时间、以供审核。FSE的SOW会在内部传达给NetApp。

运营团队

Cloud Volumes Service 运营团队由生产工程和云卷服务站点可靠性工程师(SRE)以及NetApp现场支持工程师和硬件合作伙伴组成。所有运营团队成员都获得了在Google Cloud中工作的认证、并为提交的每个服务单维护详细的工作记录。此外、我们还制定了严格的变更控制和批准流程、以确保对每项决策进行适当审查。

SRE团队负责管理控制平台以及如何将数据从UI请求路由到Cloud Volumes Service 中的后端硬件和软件。SRE团队还负责管理系统资源、例如卷和索引节点最大值。不允许SRES与客户数据进行交互或访问客户数据。此外、SRES还可以与退回材料授权(Return Material Authorizations、RMA)进行协调、例如为后端硬件请求新磁盘或内存更换请求。

客户责任

Cloud Volumes Service 的客户负责管理其组织的Active Directory和用户角色管理以及卷和数据操作。客户可以具有管理角色、并可以使用NetApp和Google Cloud提供的两个预定义角色(管理员和查看器)将权限委派给同一Google Cloud项目中的其他最终用户。

管理员可以将客户项目中的任何VPC与客户确定合适的Cloud Volumes Service 建立对等关系。客户有责任管理对其Google Cloud Marketplace订阅的访问权限、并管理有权访问数据平面的VPC。

恶意**SRE**保护

可能会出现的一个问题是、Cloud Volumes Service 如何防止出现恶意SRE或SRE凭据受到损坏的情况?

只能由有限数量的SRE人员访问生产环境。管理权限进一步限制为少数经验丰富的管理员。我们的安全信息和事件管理(Cloud Volumes Service)威胁情报平台会记录任何人在生产环境中执行的所有操作、并检测到基线异常或可疑活动。因此、在对Cloud Volumes Service 后端造成过多损坏之前、可以跟踪和缓解恶意操作。

卷生命周期

Cloud Volumes Service 仅管理服务中的对象、而不管理卷中的数据。只有访问卷的客户端才能管理数据、ACL、文件所有者等。这些卷中的数据会在空闲时进行加密、并且只能由Cloud Volumes Service 实例的租户访问。

Cloud Volumes Service 的卷生命周期为create-update-delete。卷会保留卷的Snapshot副本、直到删除卷为止、只有经过验证的Cloud Volumes Service 管理员才能删除Cloud Volumes Service 中的卷。当管理员请求删除卷时、还需要输入卷名称来验证删除操作。删除卷后、该卷将消失、无法恢复。

如果Cloud Volumes Service 合同终止、NetApp会在特定时间段后标记要删除的卷。在该时间段到期之前、您可以根据客户的请求恢复卷。

认证

适用于Google Cloud的Cloud Volumes Services目前已通过ISO/IEC 27001：2013和ISO/IEC 27018：2019标准的认证。该服务最近还收到了其SOC2 I类证明报告。有关NetApp对数据安全和隐私的承诺的信息、请参见 "合规性：数据安全和数据隐私"。

GDPR

我们的许多公司都承诺遵守GDPR并遵守隐私规定 "客户合同"、例如我们的 "客户数据处理附录"、其中包括 "标准合同条款" 由欧盟委员会提供。我们还会在隐私政策中做出这些承诺、并以我们公司行为准则中规定的核心价值为后盾。

追加信息和联系信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- 适用于Cloud Volumes Service 的Google Cloud文档

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google私有服务访问

  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/"

- 加密验证模块计划—NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- 适用于勒索软件的NetApp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

请联系我们

请告诉我们如何改进本技术报告。

联系我们、电子邮件地址为：mailto：doccomments@netapp.com^ doccomments@netapp.com。在主题行中包含技术报告4918。

BlueXP备份和恢复

适用于**VM**的**BlueXP**备份和恢复

3-2-1使用**SnapCenter**插件和适用于**VM**的**BlueXP**备份和恢复为**VMware**提供数据保护

作者：Jsh Powell—NetApp解决方案工程部

概述

3-2-1备份策略是行业认可的数据保护方法、可提供全面的方法来保护有价值的数据。 此策略非常可靠、可确保即使发生意外灾难、仍有可用数据的副本。

该战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、您仍至少有两个剩余副本可供回退。
2. 将两个备份副本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设备或介质特定的故障。如果一个设备损坏或一种介质发生故障、另一个备份副本不受影响。
3. 最后、确保至少有一个备份副本位于异地。异地存储可防止发生火灾或洪水等本地灾难、这些灾难可能会导致现场副本不可用。

本解决方案文档介绍解决方案了使用适用于VMware vSphere的SnapCenter插件(SCV)为内部虚拟机创建主备份和二级备份的3-2-1备份、以及使用BlueXP备份和恢复为虚拟机将数据副本备份到云存储或StorageGRID。

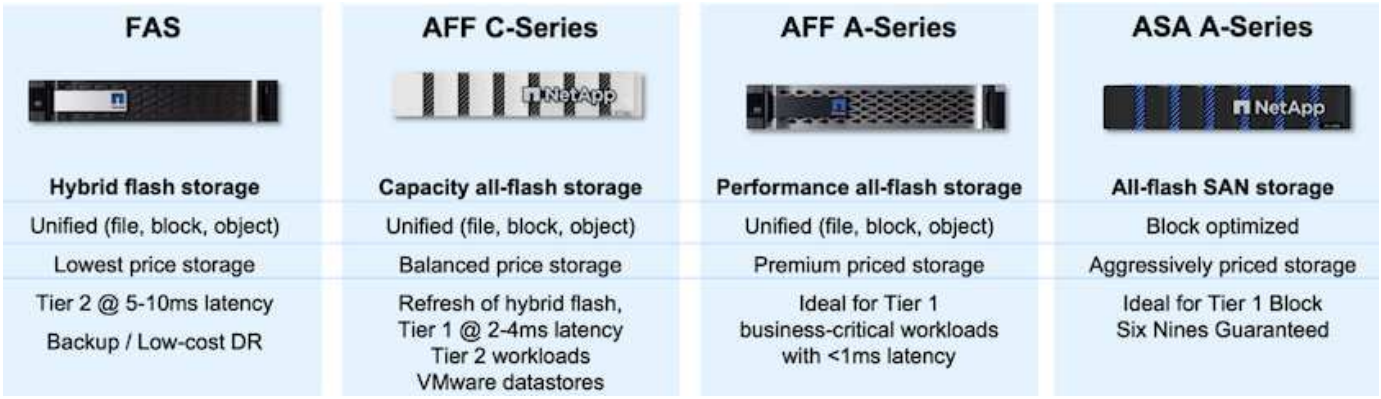
用例

此解决方案 可解决以下使用情形：

- 使用适用于VMware vSphere的SnapCenter插件备份和还原内部虚拟机和数据存储库。
- 备份和还原ONTAP集群上托管的内部虚拟机和数据存储库、并使用适用于虚拟机的BlueXP备份和恢复功能备份到对象存储。

NetApp ONTAP数据存储

ONTAP是NetApp行业领先的存储解决方案、无论您是通过SAN还是NAS协议访问、它都能提供统一存储。3-2-1备份策略可确保内部数据在多种介质类型上受到保护、NetApp提供的平台从高速闪存到低成本介质不等。



有关NetApp所有硬件平台的详细信息、请查看 "NetApp数据存储"。

适用于 **VMware vSphere** 的 **SnapCenter** 插件

适用于VMware vSphere的SnapCenter插件是一款数据保护产品、与VMware vSphere紧密集成、可轻松管理虚拟机的备份和还原。作为解决方案的一部分、SnapMirror提供了一种快速可靠的方法、可在二级ONTAP存储集群上为虚拟机数据创建第二个不可变化的备份副本。采用此架构后、可以轻松地从主备份位置或二级备份位置启动虚拟机还原操作。

SCV使用OVA文件部署为Linux虚拟设备。现在、此插件将使用远程插件
架构。远程插件在vCenter Server外部运行、并托管在SCV虚拟设备上。

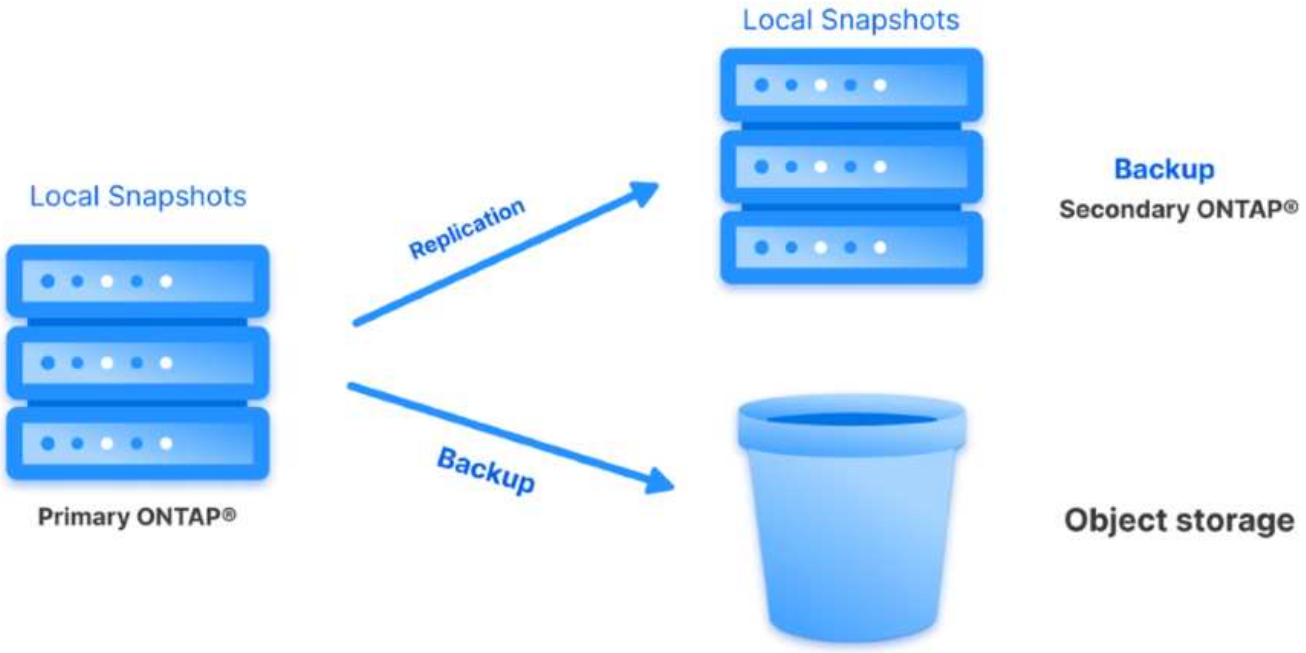
有关选择控制阀的详细信息，参见 "适用于 VMware vSphere 的 SnapCenter 插件文档"。

适用于虚拟机的**BlueXP**备份和恢复

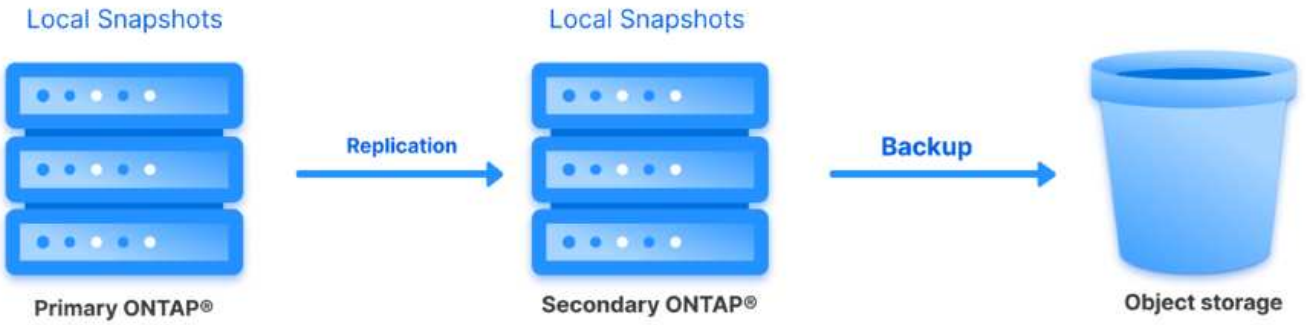
BlueXP备份和恢复是一款基于云的数据管理工具、可为内部和云环境中的各种备份和恢复操作提供单一控制平台。NetApp BlueXP备份和恢复套件的一部分是一项与适用于VMware vSphere的SnapCenter插件(内部)集成的功能、用于将数据副本扩展到云中的对象存储。这样可以为来自主存储备份或二级存储备份的异地数据创建第三个副本。通过BlueXP备份和恢复、您可以轻松设置存储策略、以便从这两个内置位置中的任何一个位置传输数据副本。

在BlueXP备份和恢复中选择主备份和二级备份作为源将导致实施以下两种拓扑之一：

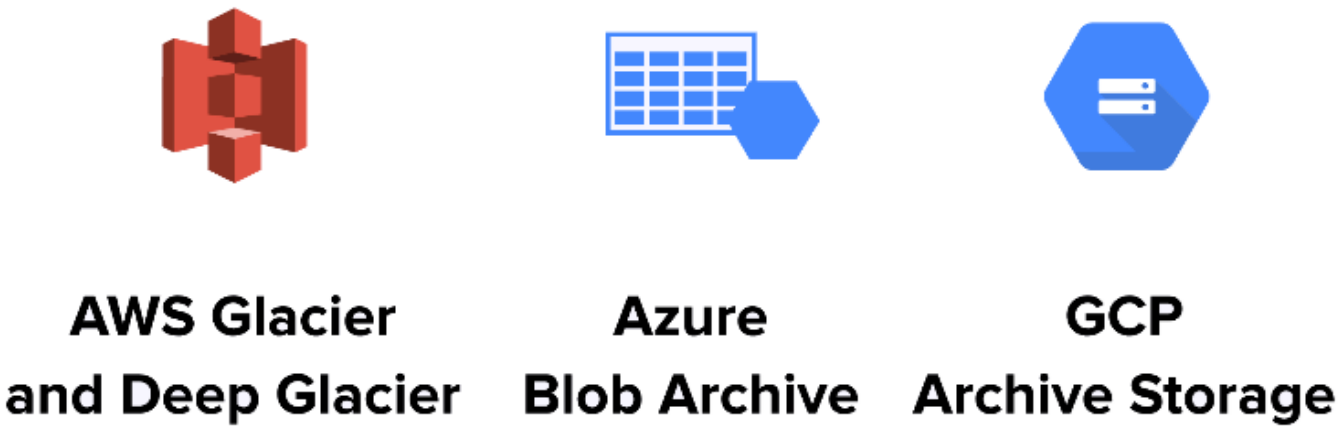
扇出拓扑—适用于VMware vSphere的SnapCenter插件启动备份时，会立即创建本地快照。然后、SCV启动SnapMirror操作、将最新的快照复制到二级ONTAP集群。在BlueXP备份和恢复中、策略会将主ONTAP集群指定为要传输到所选云提供商中的对象存储的数据Snapshot副本的源。



级联拓扑–使用SCV创建主数据副本和二级数据副本与上述扇出拓扑相同。但是、这一次在BlueXP备份和恢复中创建一个策略、指定对象存储备份将源自二级ONTAP集群。



BlueXP备份和恢复可以为内部ONTAP快照创建备份副本、并将其备份到AWS Glacie、Azure Blb和GCP归档存储。



此外、您还可以使用NetApp StorageGRID作为对象存储备份目标。有关StorageGRID的详细信息、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BlueXP备份和恢复执行备份和恢复操作所需的高级步骤：

1. 在要用于主数据副本和二级数据副本的ONTAP集群之间配置SnapMirror关系。
2. 配置适用于VMware vSphere的SnapCenter插件。
    a. 添加存储系统
    b. 创建备份策略
    c. 创建资源组
    d. 运行备份优先备份作业
3. 为虚拟机配置BlueXP备份和恢复
    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从主存储和二级存储还原虚拟机。
5. 使用BlueXP备份和还原从对象存储还原虚拟机。

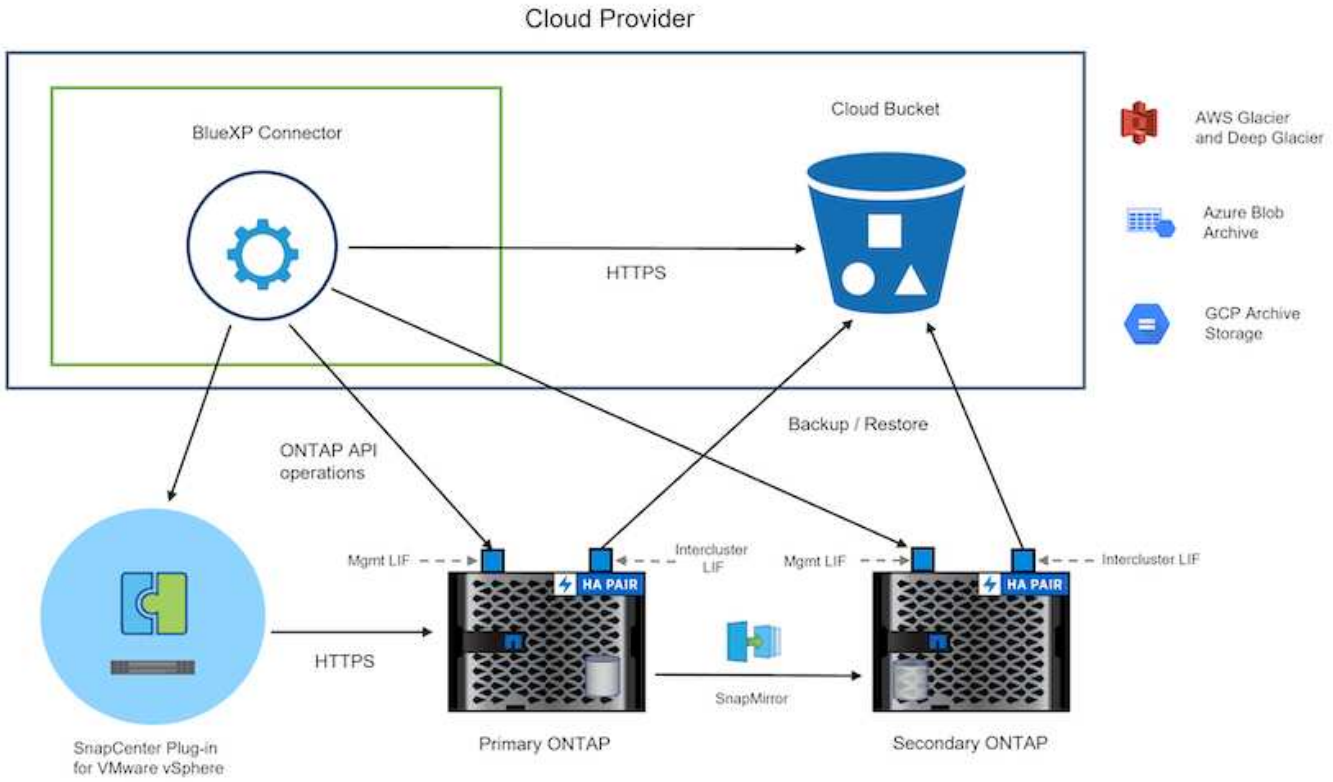
前提条件

此解决方案的目的是演示对在VMware vSphere中运行且位于由NetApp ONTAP托管的NFS数据存储库上的虚拟机的数据保护。此解决方案 假定已配置以下组件并可供使用：

1. 使用NFS或VMFS数据存储库连接到VMware vSphere的ONTAP存储集群。支持NFS和VMFS数据存储库。此解决方案使用了NFS数据存储库。
2. 为用于NFS数据存储库的卷建立SnapMirror关系的二级ONTAP存储集群。
3. 为用于对象存储备份的云提供程序安装了BlueXP连接器。
4. 要备份的虚拟机位于主ONTAP存储集群上的NFS数据存储库中。
5. BlueXP连接器和内部ONTAP存储集群管理接口之间的网络连接。
6. BlueXP连接器和内部SCV设备VM之间以及BlueXP连接器和vCenter之间的网络连接。
7. 内部ONTAP集群间LUN和对象存储服务之间的网络连接。
8. 在主和二级ONTAP存储集群上为管理SVM配置了DNS。有关详细信息、请参见 "配置 DNS 以进行主机名解析"。

高级架构

此解决方案 的测试/验证是在可能与最终部署环境匹配或可能不匹配的实验室中执行的。



解决方案 部署

在本解决方案中、我们详细说明了如何部署和验证解决方案、该利用适用于VMware vSphere的SnapCenter插件以及BlueXP备份和恢复功能、在内部数据中心的VMware vSphere集群中执行Windows和Linux虚拟机的备份和恢复。此设置中的虚拟机存储在ONTAP A300存储集群托管的NFS数据存储库中。此外、一个单独的ONTAP A300存储集群可用作使用SnapMirror复制的卷的二级目标。此外、Amazon Web Services和Azure Blb上托管的对象存储也用作数据第三个副本的目标。

我们将继续为SCV管理的备份的二级副本创建SnapMirror关系、并在SCV和BlueXP备份和恢复中配置备份作业。

有关适用于VMware vSphere的SnapCenter插件的详细信息、请参见 "适用于 VMware vSphere 的 SnapCenter 插件文档"。

有关BlueXP备份和恢复的详细信息、请参阅 "BlueXP备份和恢复文档"。

在**ONTAP**集群之间建立**SnapMirror**关系

适用于VMware vSphere的SnapCenter插件使用ONTAP SnapMirror技术管理将二级SnapMirror和/或SnapVault副本传输到二级ONTAP集群的过程。

选择控制阀备份策略可以选择使用SnapMirror或SnapVault关系。主要区别在于、使用SnapMirror选项时、在策略中为备份配置的保留计划在主位置和二级位置将相同。SnapVault专为归档而设计、使用此选项时、可以通过SnapMirror关系为二级ONTAP存储集群上的Snapshot副本建立单独的保留计划。

可以在BlueXP中自动执行许多步骤来设置SnapMirror关系、也可以使用System Manager和ONTAP命令行界面来设置SnapMirror关系。下面将讨论所有这些方法。

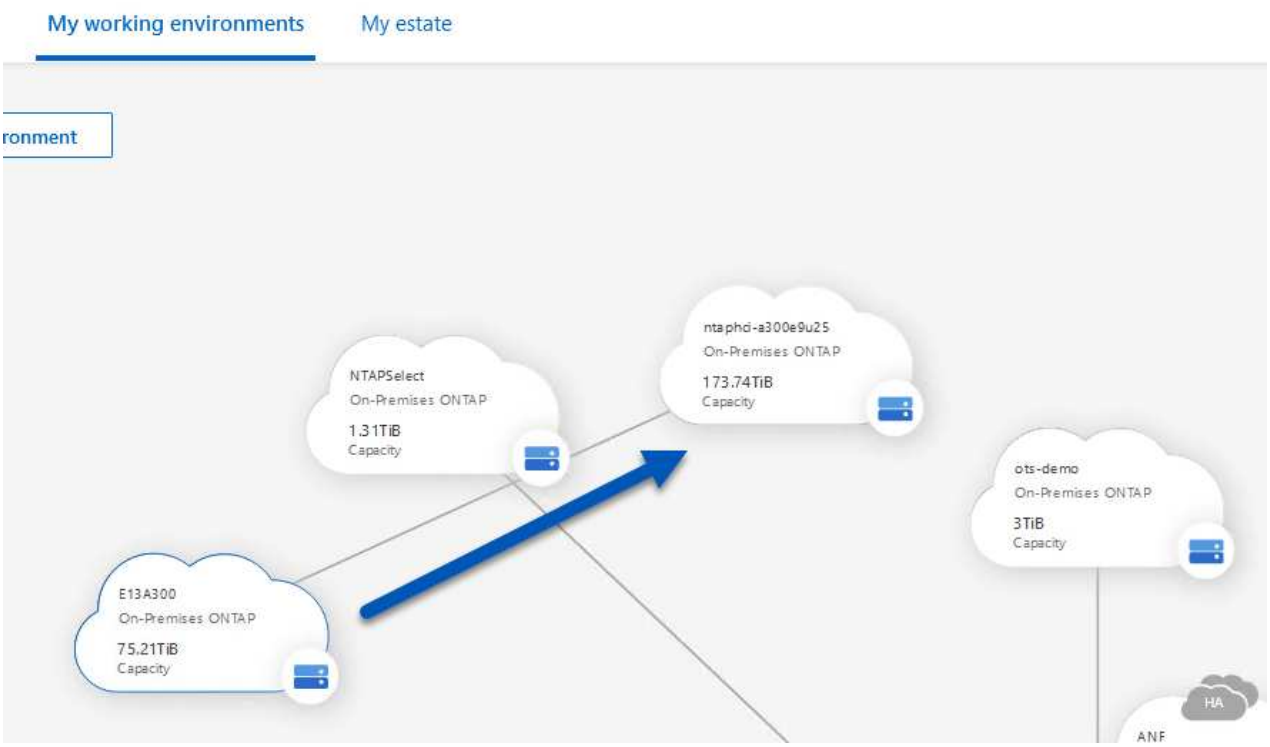
与**BlueXP**建立**SnapMirror**关系

必须从BlueXP Web控制台完成以下步骤：

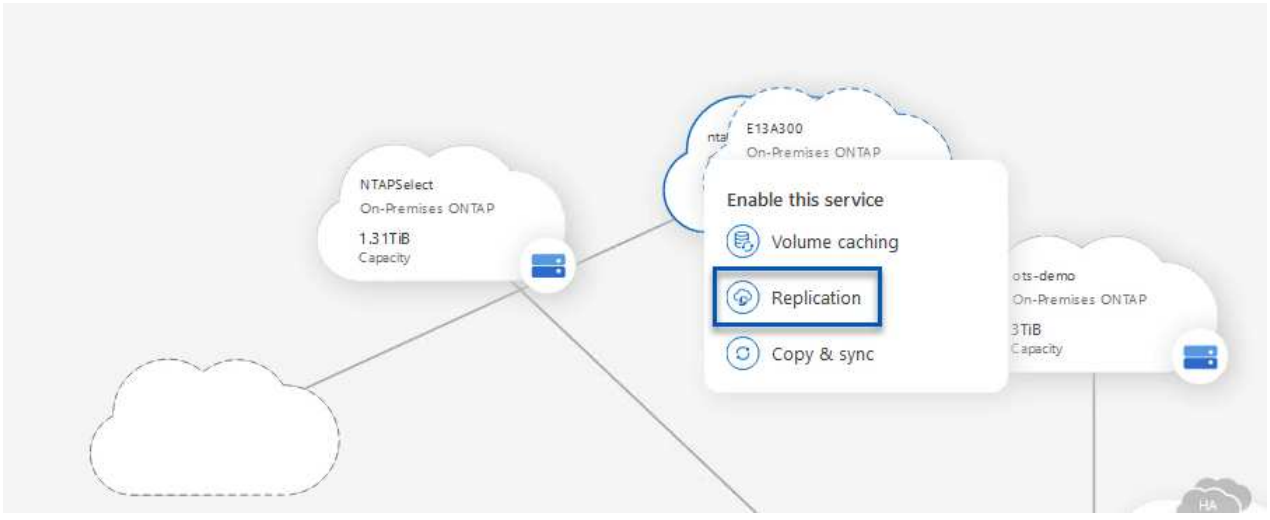
主和二级**ONTAP**存储系统的复制设置

首先登录到BlueXP Web控制台并导航到Canvas。

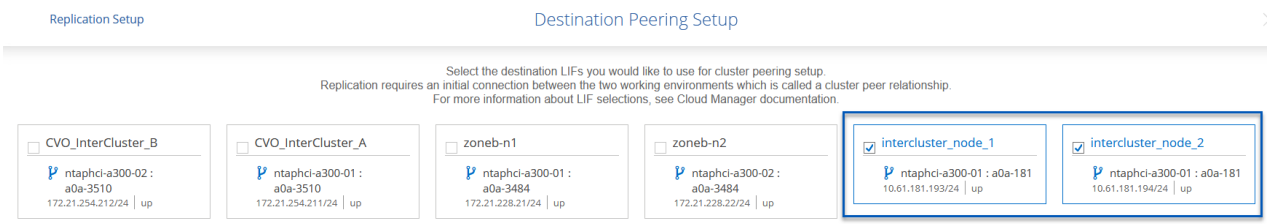
1. 将源(主) ONTAP存储系统拖放到目标(二级) ONTAP存储系统上。



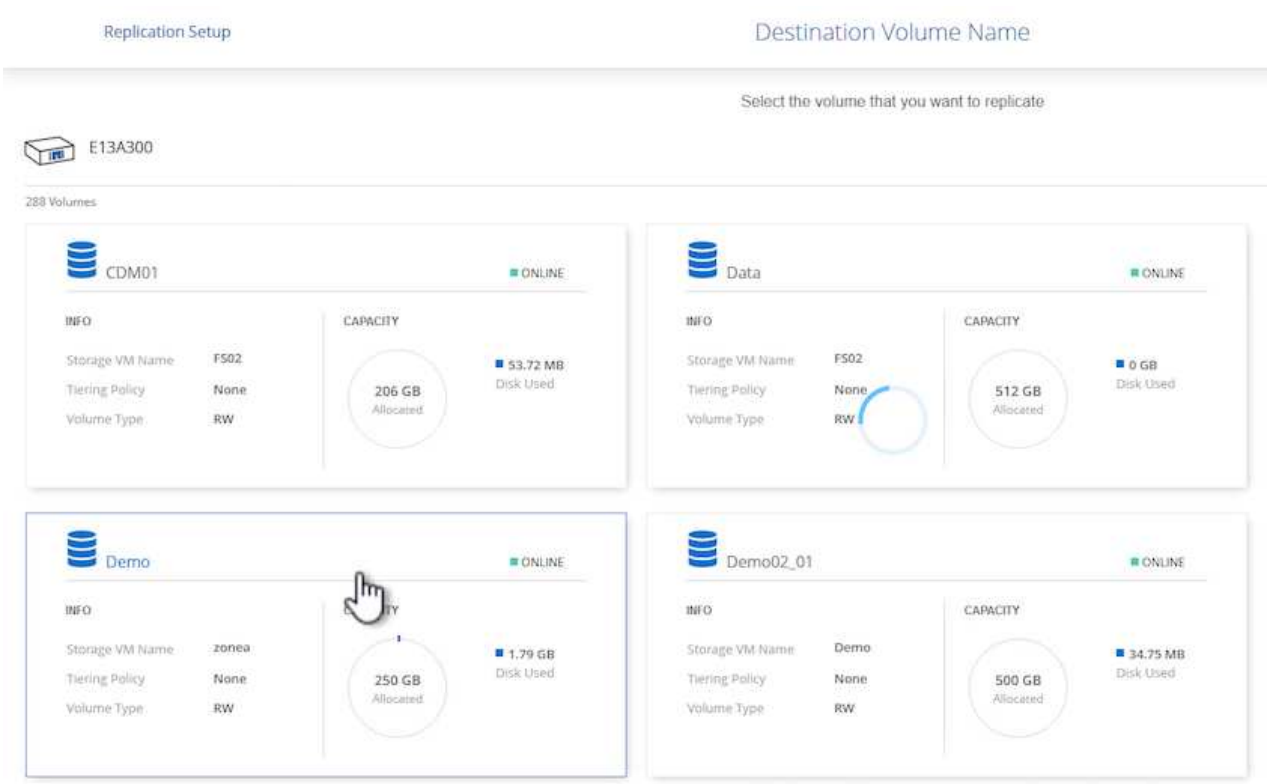
2. 从显示的菜单中选择*复制*。



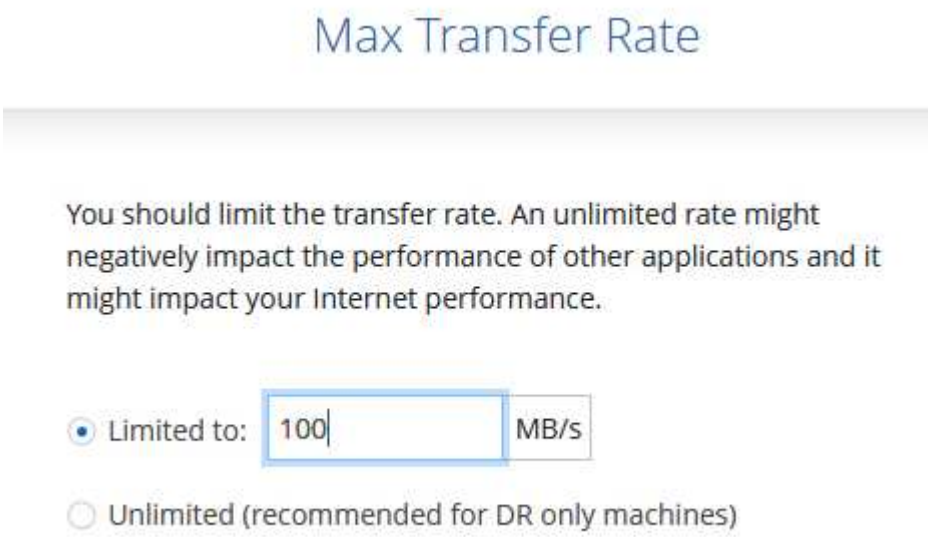
3. 在*目标对等设置*页面上、选择要用于存储系统之间连接的目标集群间Lifs。



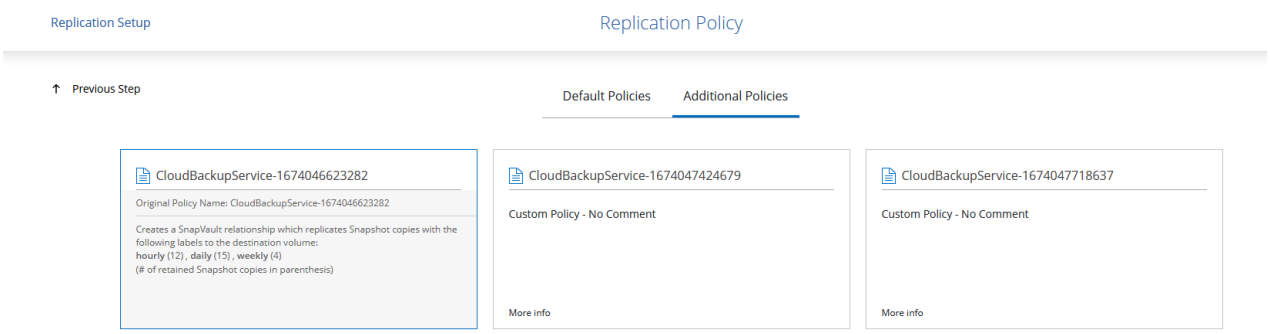
4. 在*目标卷名称*页面上、首先选择源卷、然后填写目标卷名称并选择目标SVM和聚合。单击“下一步”继续。



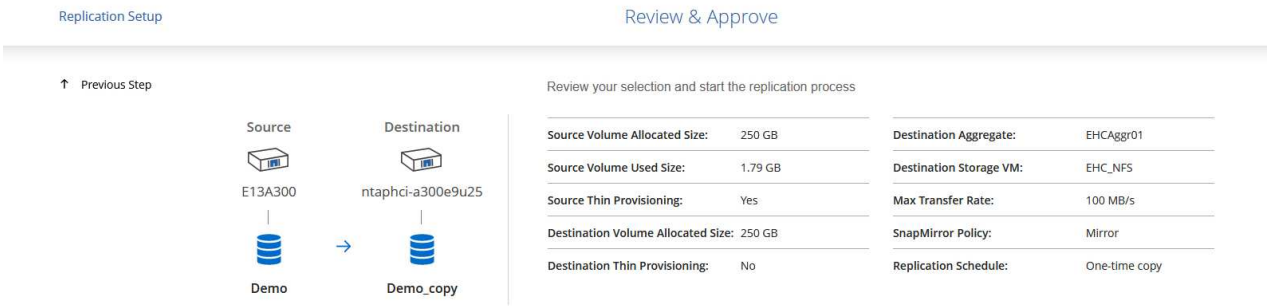
5. 选择进行复制的最大传输速率。



6. 选择用于确定二级备份的保留计划的策略。此策略可以事先创建(请参见下面的*创建快照保留策略*步骤中的手动过程)，也可以在创建后根据需要进行更改。



7. 最后，查看所有信息，然后单击*go *按钮开始复制设置过程。



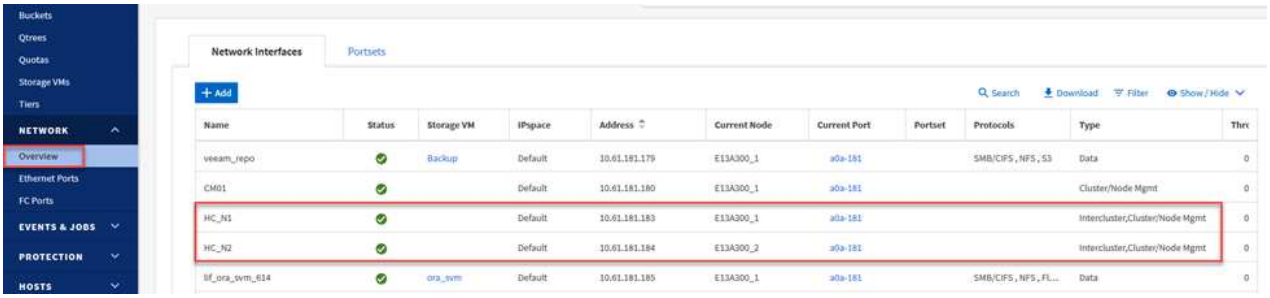
使用System Manager和ONTAP命令行界面建立SnapMirror关系

可以使用System Manager或ONTAP命令行界面完成建立SnapMirror关系所需的所有步骤。下一节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System Manager或命令行界面检索集群间LIF信息。

1. 在ONTAP 系统管理器中、导航到"网络概述"页面、然后检索类型为"集群间"的IP地址、这些IP地址配置为与安装了FSX的AWS VPC进行通信。



2. 要使用命令行界面检索集群间IP地址、请运行以下命令：

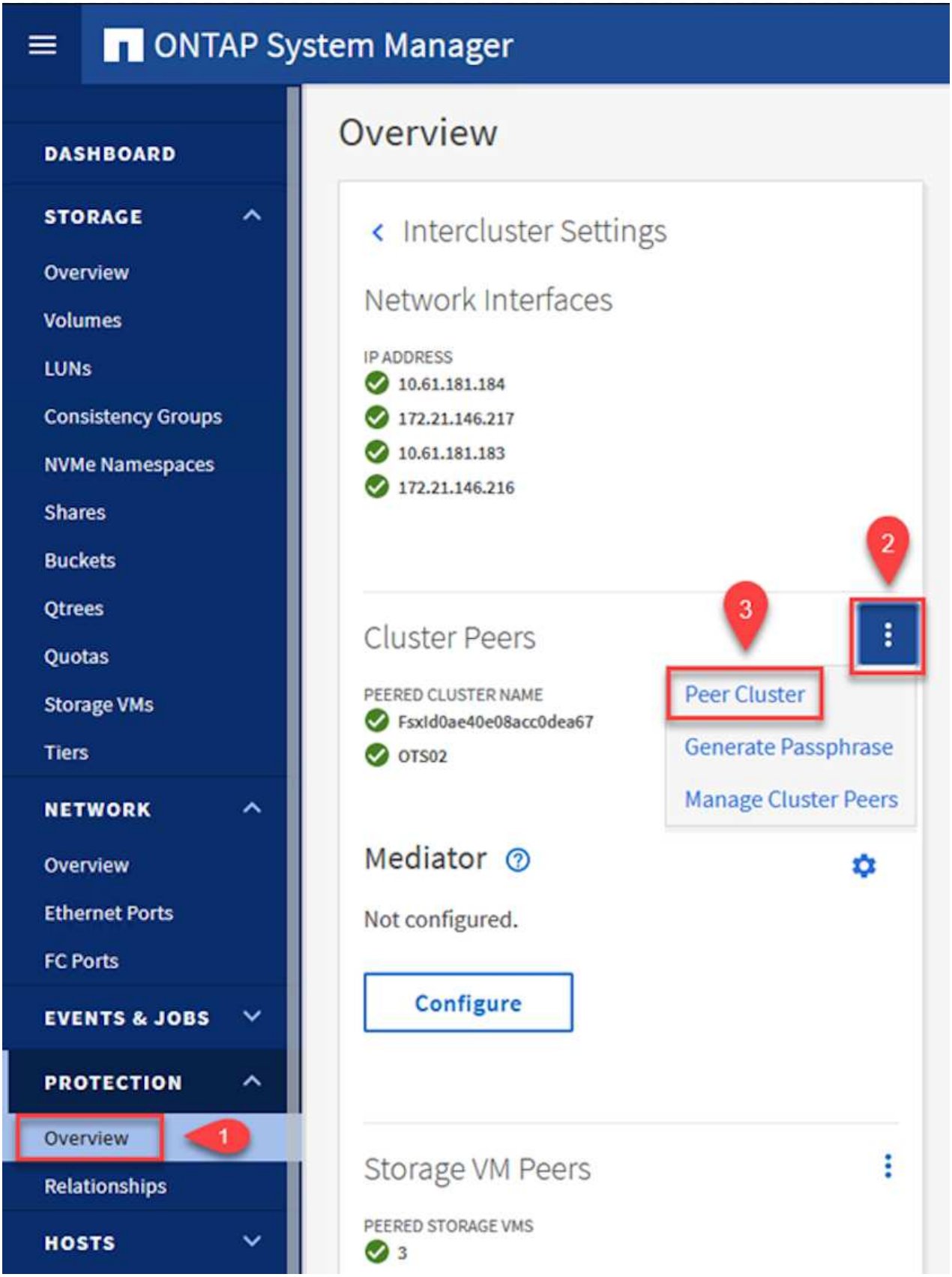
```
ONTAP-Dest::> network interface show -role intercluster
```

要在ONTAP 集群之间建立集群对等关系、必须在另一对等集群中确认在发起ONTAP 集群上输入的唯一密码短语。

1. 使用在目标ONTAP集群上设置对等关系 `cluster peer create` 命令：出现提示时、输入一个唯一的密码短语、稍后在源集群上使用该密码短语以完成创建过程。

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

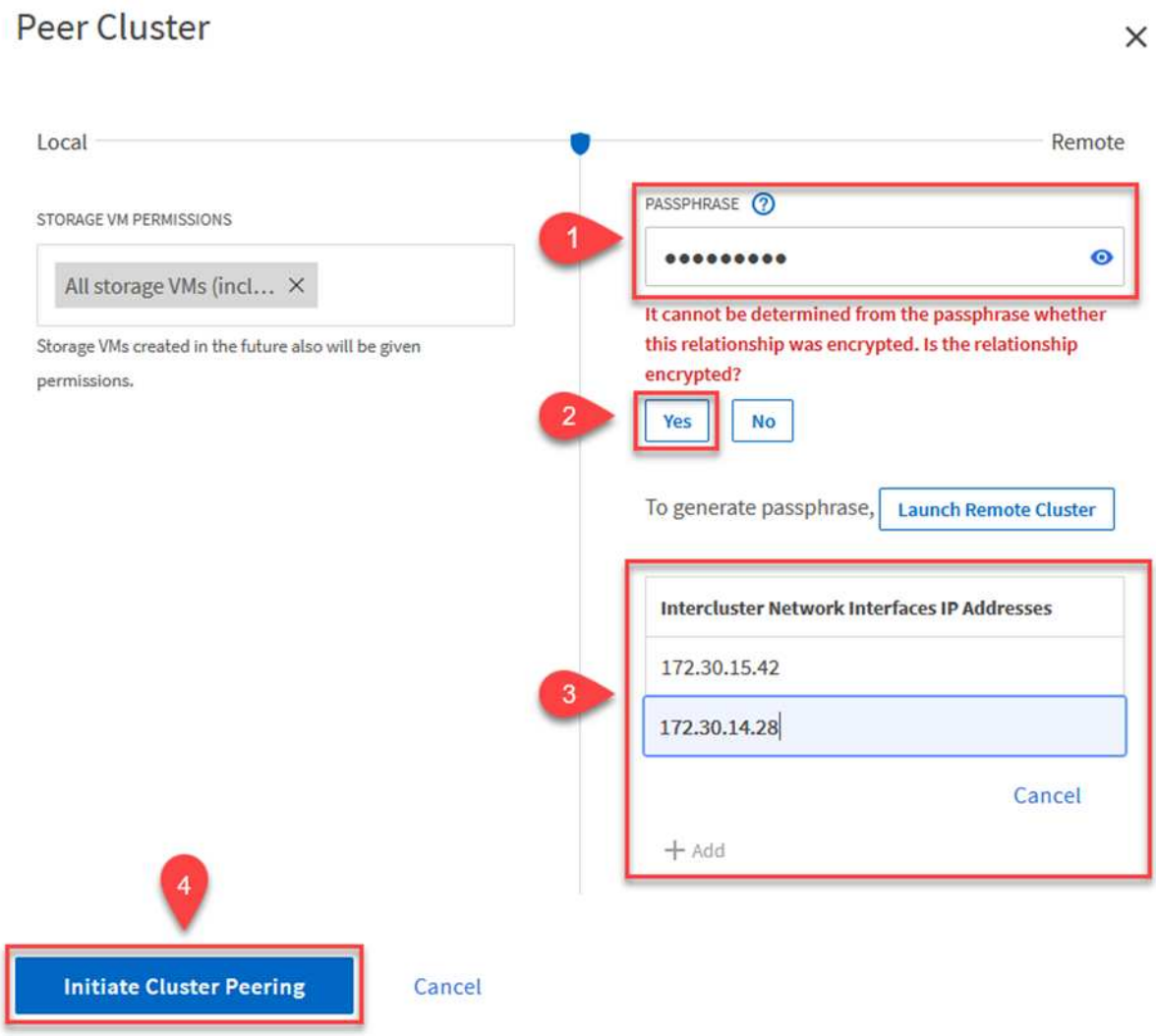
2. 在源集群上、您可以使用ONTAP 系统管理器或命令行界面建立集群对等关系。在ONTAP 系统管理器中、导航到"保护">"概述"、然后选择"对等集群"。



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短语。
   b. 选择`是`以建立加密关系。

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此过程。



4. 使用以下命令验证目标ONTAP集群的集群对等关系的状态：

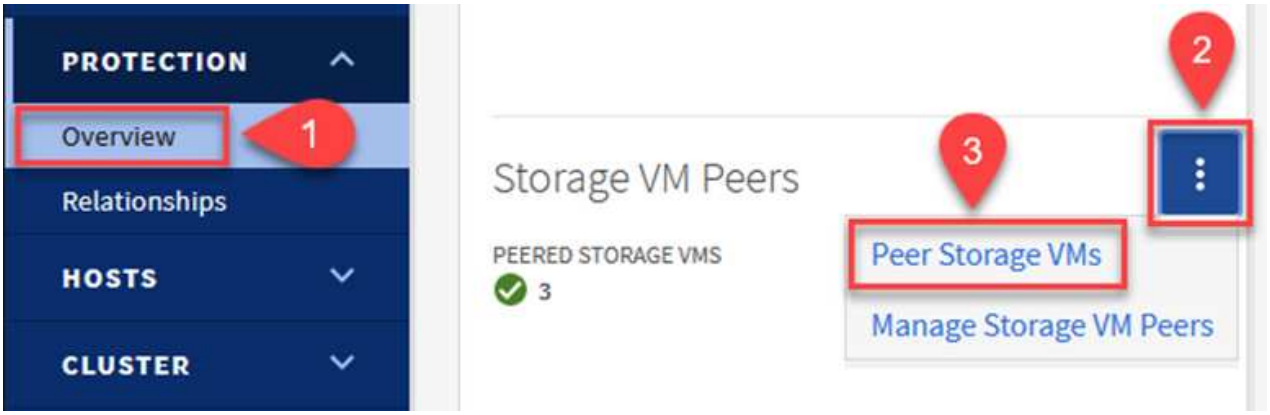
```
ONTAP-Dest::> cluster peer show
```

下一步是在目标和源Storage Virtual Machine之间设置SVM关系、这些虚拟机包含将处于SnapMirror关系中的卷。

1. 在目标ONTAP集群中、从命令行界面使用以下命令创建SVM对等关系：

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

2. 在源ONTAP 集群中、接受与ONTAP 系统管理器或命令行界面的对等关系。
3. 在ONTAP 系统管理器中、转到"保护">"概述"、然后在"Storage VM对等方"下选择"对等Storage VM"。



4. 在对等Storage VM的对话框中、填写必填字段：
   - 源Storage VM
   - 目标集群
   - 目标Storage VM

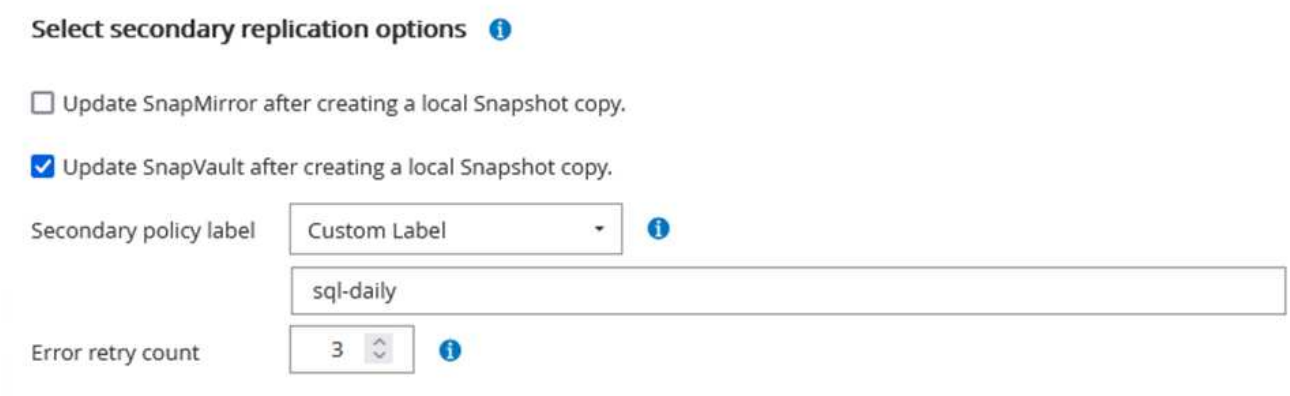
5. 单击对等Storage VM以完成SVM对等过程。

SnapCenter 管理主存储系统上作为Snapshot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 不会管理二级存储系统上保留的备份的保留策略。这些策略通过在二级FSX集群上创建的SnapMirror策略单独管理、并与与与源卷具有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二级策略标签、该标签将添加到创建SnapCenter 备份时生成的每个快照的SnapMirror标签中。

在二级存储上、这些标签与与与目标卷关联的策略规则匹配、以便强制保留快照。

以下示例显示了一个SnapMirror标签、该标签位于作为SQL Server数据库和日志卷每日备份策略一部分生成的所有快照上。



有关为SQL Server数据库创建SnapCenter 策略的详细信息、请参见 "SnapCenter 文档"。

您必须先创建一个SnapMirror策略、其中包含指定要保留的Snapshot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. 向策略添加SnapMirror标签与SnapCenter 策略中指定的二级策略标签匹配的规则。

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

以下脚本提供了可添加到策略中的规则示例：

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

为每个SnapMirror标签以及要保留的快照数量(保留期限)创建其他规则。

创建目标卷

要在ONTAP上创建目标卷、以便接收源卷的Snapshot副本、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。此过程将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
```

配置适用于**VMware vSphere**的**SnapCenter**插件

安装后、可从vCenter Server设备管理界面访问适用于VMware vSphere的SnapCenter插件。SCV将管理装载到ESXi主机且包含Windows和Linux VM的NFS数据存储库的备份。

查看 "数据保护工作流" 有关配置备份所涉及步骤的详细信息，请参阅选择控制阀文档的一节。

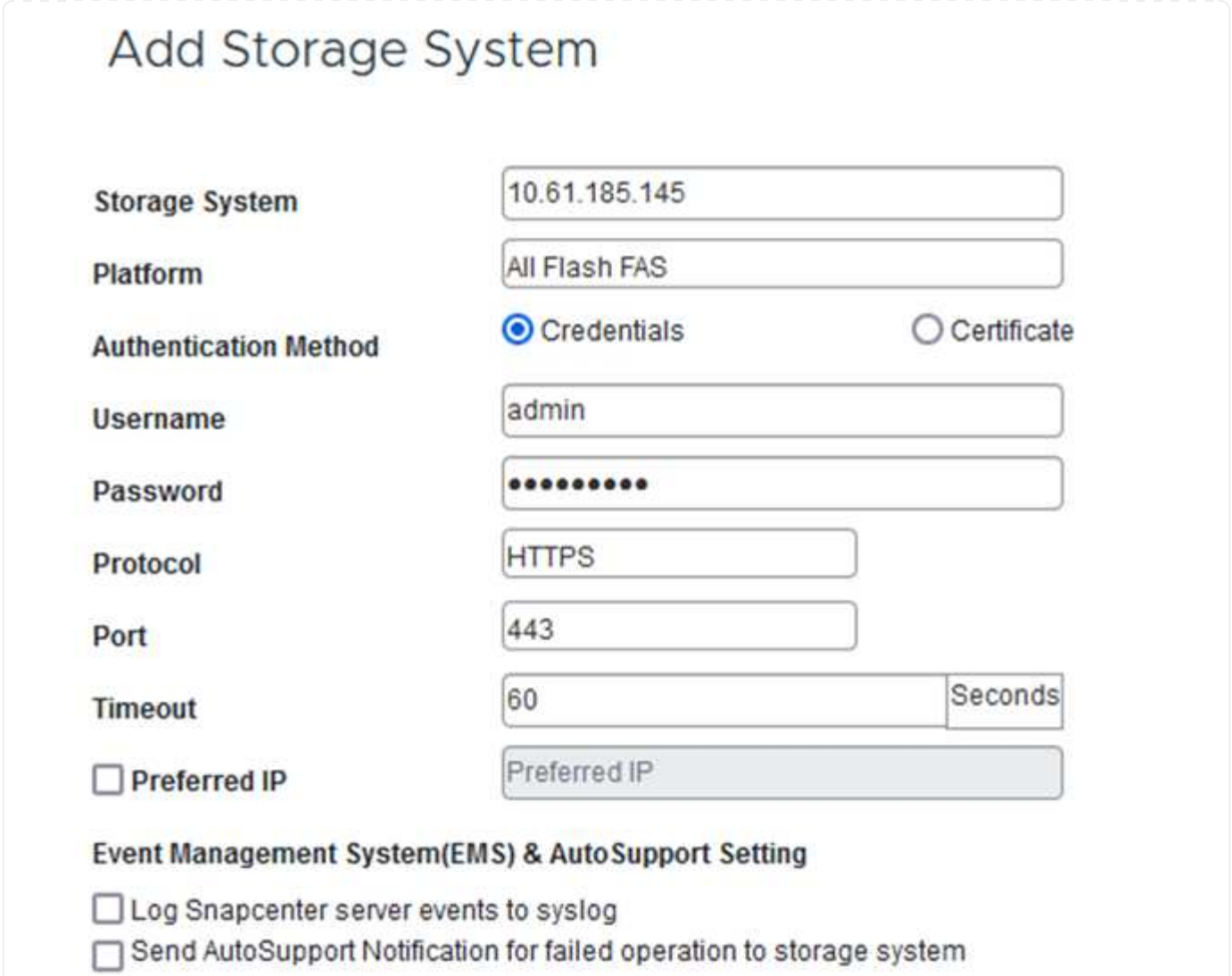
要配置虚拟机和数据存储库的备份、需要从插件界面完成以下步骤。

Discovery ONTAP存储系统

发现要用于主备份和二级备份的ONTAP存储集群。

1. 在适用于VMware vSphere的SnapCenter插件中，导航到左侧菜单中的*存储系统*，然后单击*Add*按钮。

2. 填写主ONTAP存储系统的凭据和平台类型，然后单击*Add*。



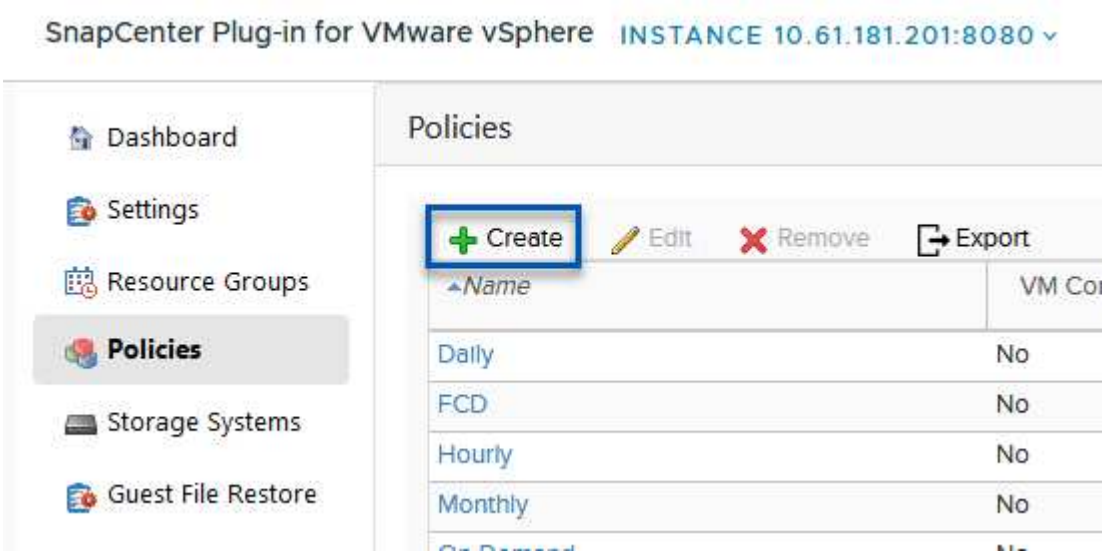
3. 对二级ONTAP存储系统重复此操作步骤。

策略用于为SCV管理的备份指定保留期限、频率和复制选项。

查看 "为 VM 和数据存储库创建备份策略" 有关详细信息、请参见文档中的第节。

要创建备份策略、请完成以下步骤：

1. 在适用于VMware vSphere的SnapCenter插件中、导航到左侧菜单中的*策略*、然后单击*创建*按钮。



2. 指定策略名称、保留期限、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。如果选择SnapMirror、则主快照和二级快照在策略中指定的保留计划将相同。如果选择SnapVault、则二级快照的保留计划将基于通过SnapMirror关系实施的单独计划。如果您希望二级备份的保留期限更长、则此功能非常有用。

Snapshot标签非常有用、因为它们可用于为复制到二级ONTAP集群的SnapVault副本制定具有特定保留期限的策略。如果将SCV与BlueXP备份和还原结合使用、则Snapshot标签字段必须为空、或者[Underline]#Match#是BlueXP备份策略中指定的标签。

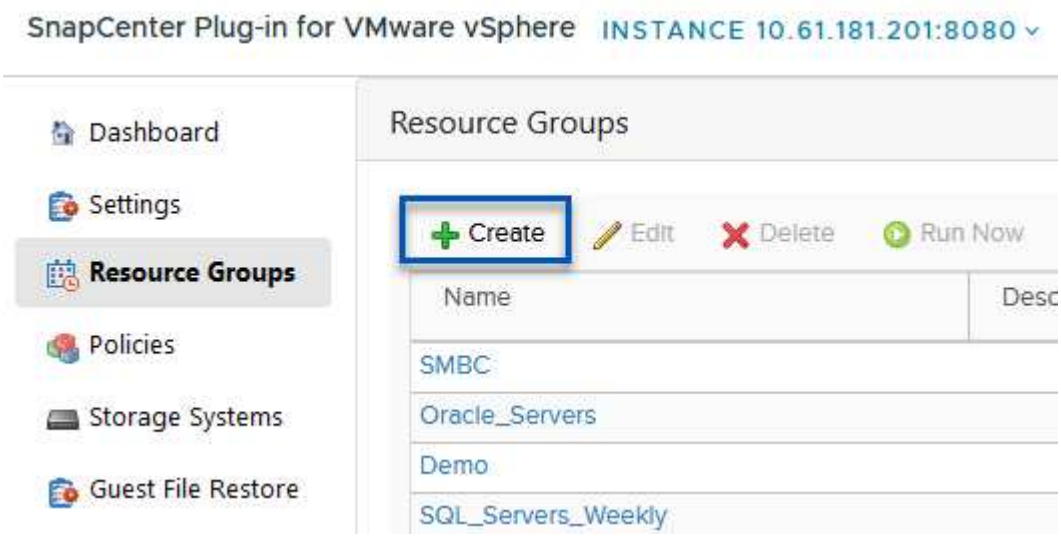
3. 对所需的每个策略重复操作步骤。例如、为每日、每周和每月备份分别设置策略。

资源组包含要包含在备份作业中的数据存储库和虚拟机、以及关联的策略和备份计划。

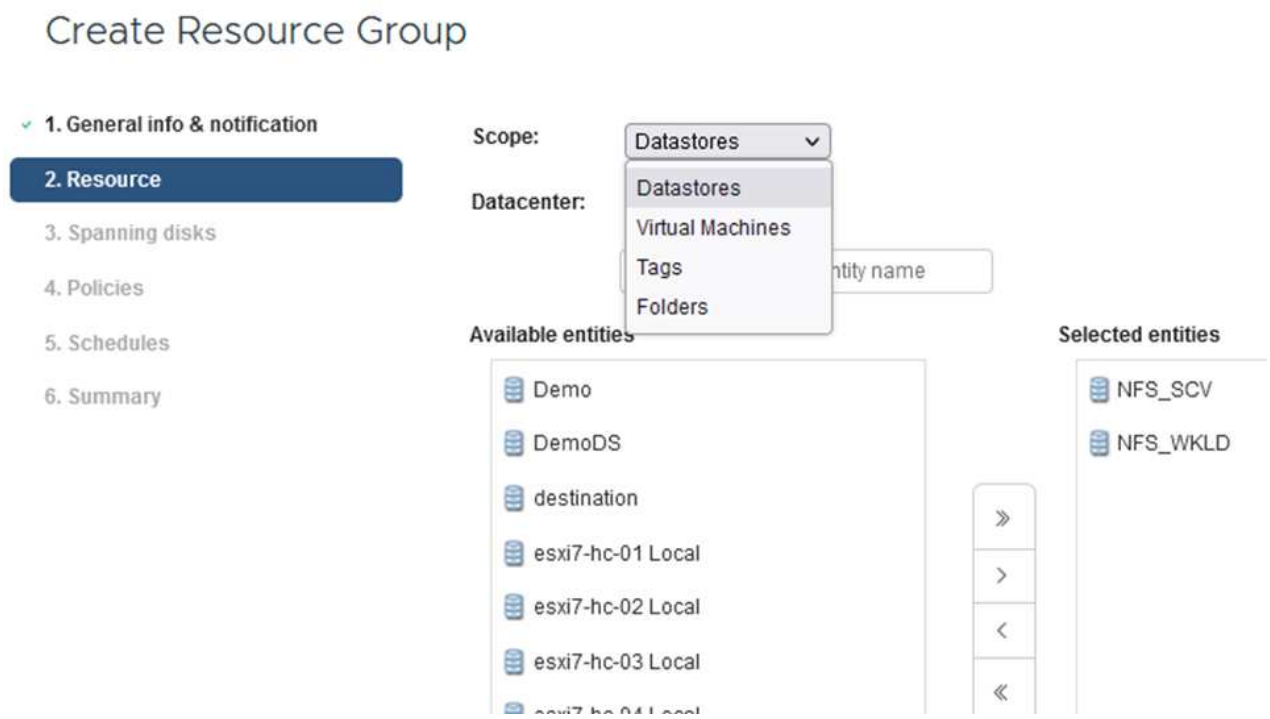
查看 "创建资源组" 有关详细信息、请参见文档中的第节。

要创建资源组，请完成以下步骤。

1. 在适用于VMware vSphere的SnapCenter插件中、导航到左侧菜单中的*资源组*、然后单击*创建*按钮。

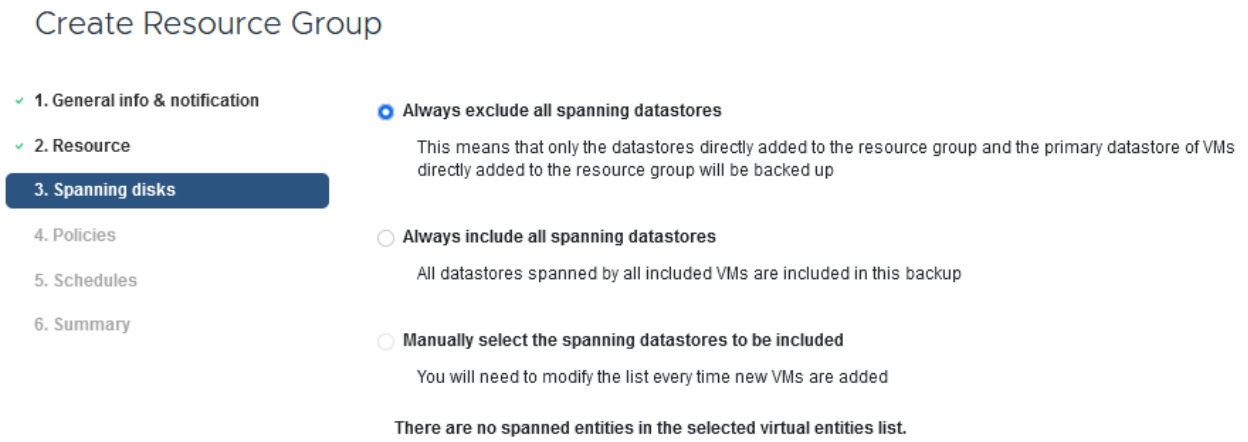


2. 在创建资源组向导中、输入组的名称和问题描述以及接收通知所需的信息。单击“下一步”
3. 在下一页上、选择要包含在备份作业中的数据存储库和虚拟机、然后单击*下一步*。



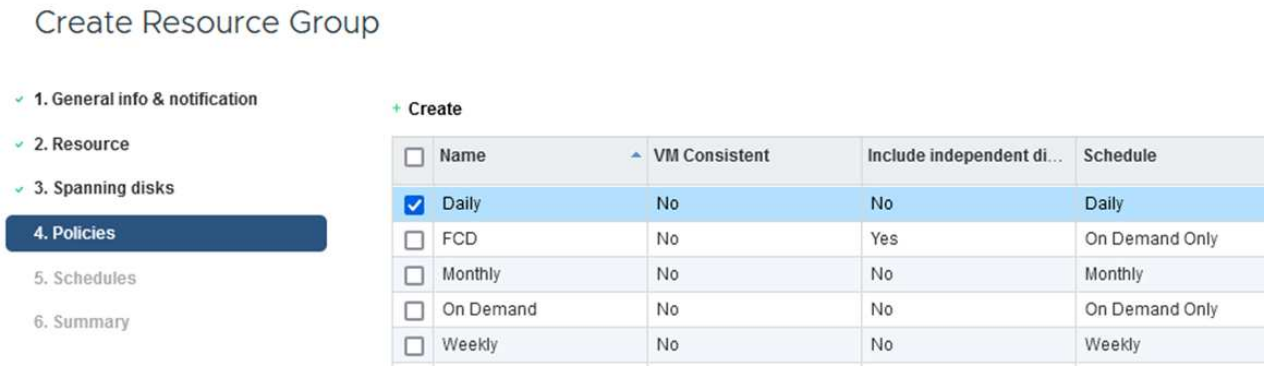
您可以选择特定虚拟机或整个数据存储库。无论选择哪种方式、都会备份整个卷(和数据存储库)、因为备份是通过为底层卷创建快照来完成的。在大多数情况下、最简单的方法是选择整个数据存储库。但是、如果要在还原时限制可用VM的列表、则只能选择一部分VM进行备份。

4. 为VMDK位于多个数据存储库上的VM选择跨数据存储库选项、然后单击*下一步*。



BlueXP备份和恢复目前不支持使用跨多个数据存储库的VMDK备份VM。

5. 在下一页中，选择要与资源组关联的策略，然后单击*Next*。



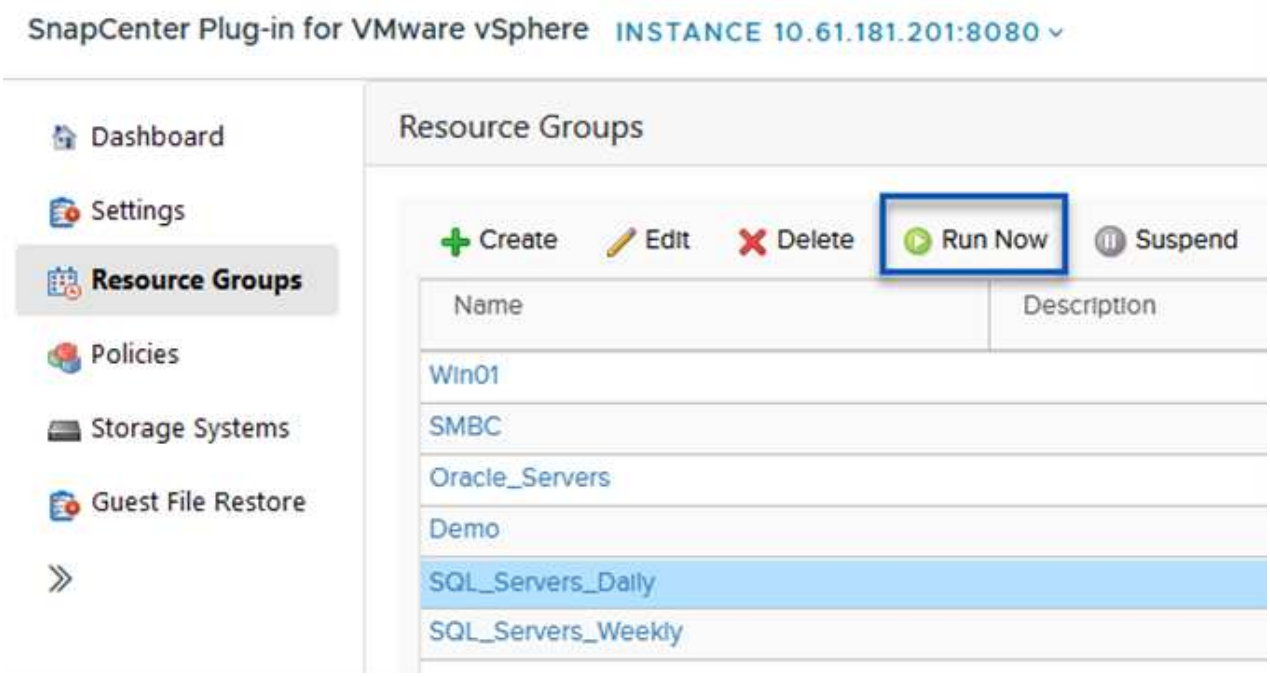
使用BlueXP备份和恢复将SCV管理的快照备份到对象存储时、每个资源组只能与一个策略相关联。

6. 选择一个计划、以确定备份的运行时间。单击“下一步”。

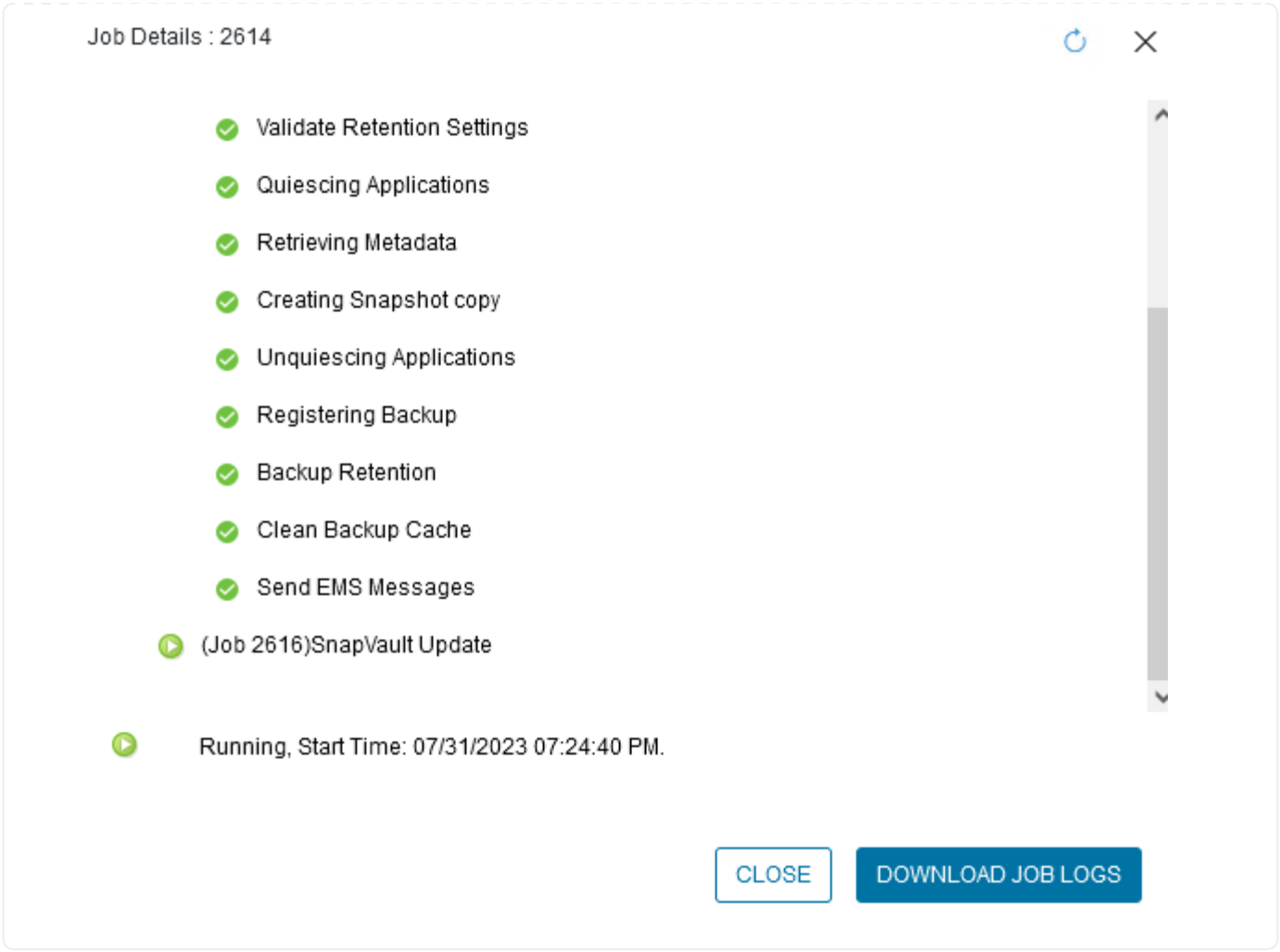
7. 最后，查看摘要页，然后在*Finish (完成)*上完成资源组的创建。

在最后一步中、运行备份作业并监控其进度。必须在SCV中至少成功完成一个备份作业、然后才能从BlueXP备份和恢复中发现资源。

1. 在适用于VMware vSphere的SnapCenter插件中、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，然后单击*立即运行*按钮。



3. 要监控备份作业，请导航至左侧菜单中的*Dashboard。在*近期工作活动*下，单击工作ID号以监视工作进度。



在**BlueXP**备份和恢复中配置对象存储备份

要使BlueXP有效管理数据基础架构、需要事先安装Connector。Connector执行发现资源和管理数据操作所涉及的操作。

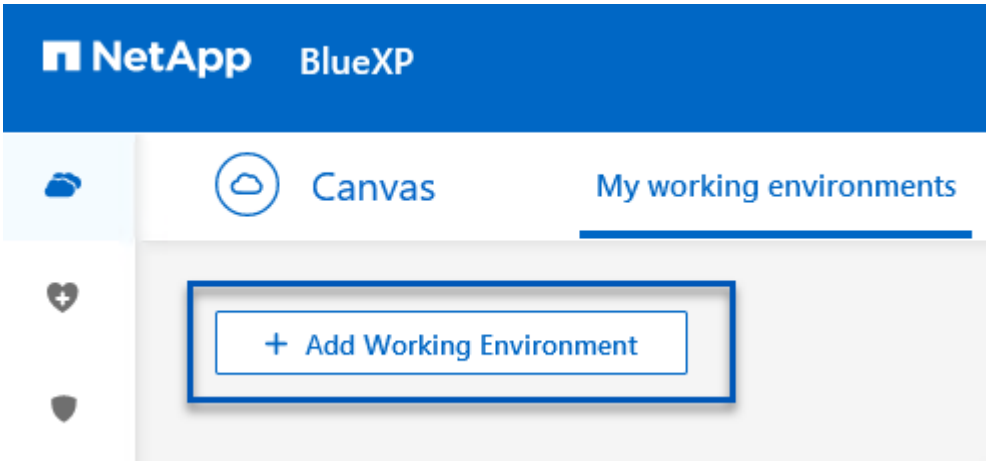
有关BlueXP Connector的详细信息、请参阅 "了解连接器" BlueXP文档中的。

为正在使用的云提供程序安装连接器后、可以从Canvas中查看对象存储的图形表示。

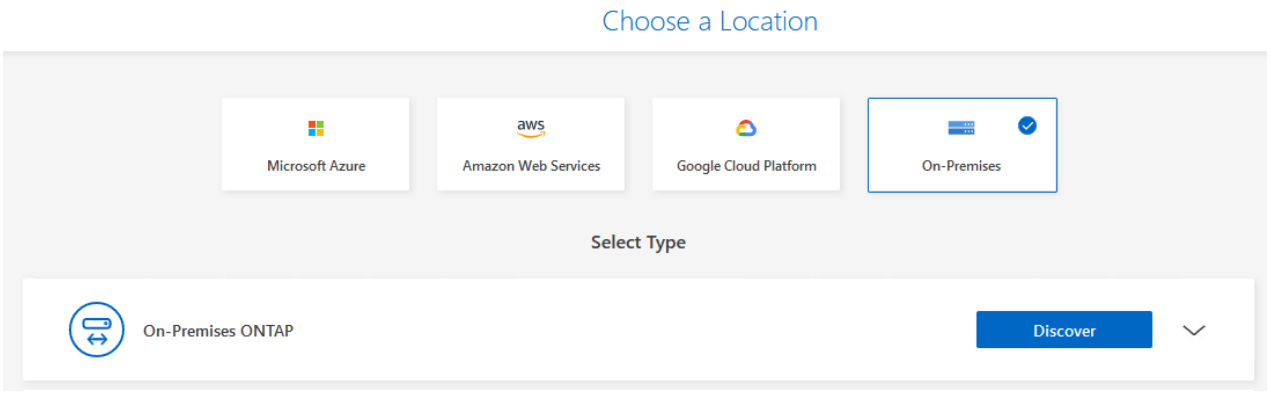
要将BlueXP备份和恢复配置为备份由内部SCV管理的数据、请完成以下步骤：

第一步是将内部ONTAP存储系统添加到BlueXP

1. 从“画布”中选择*添加工作环境*开始。



2. 从所选位置中选择*内部*，然后单击*发现*按钮。



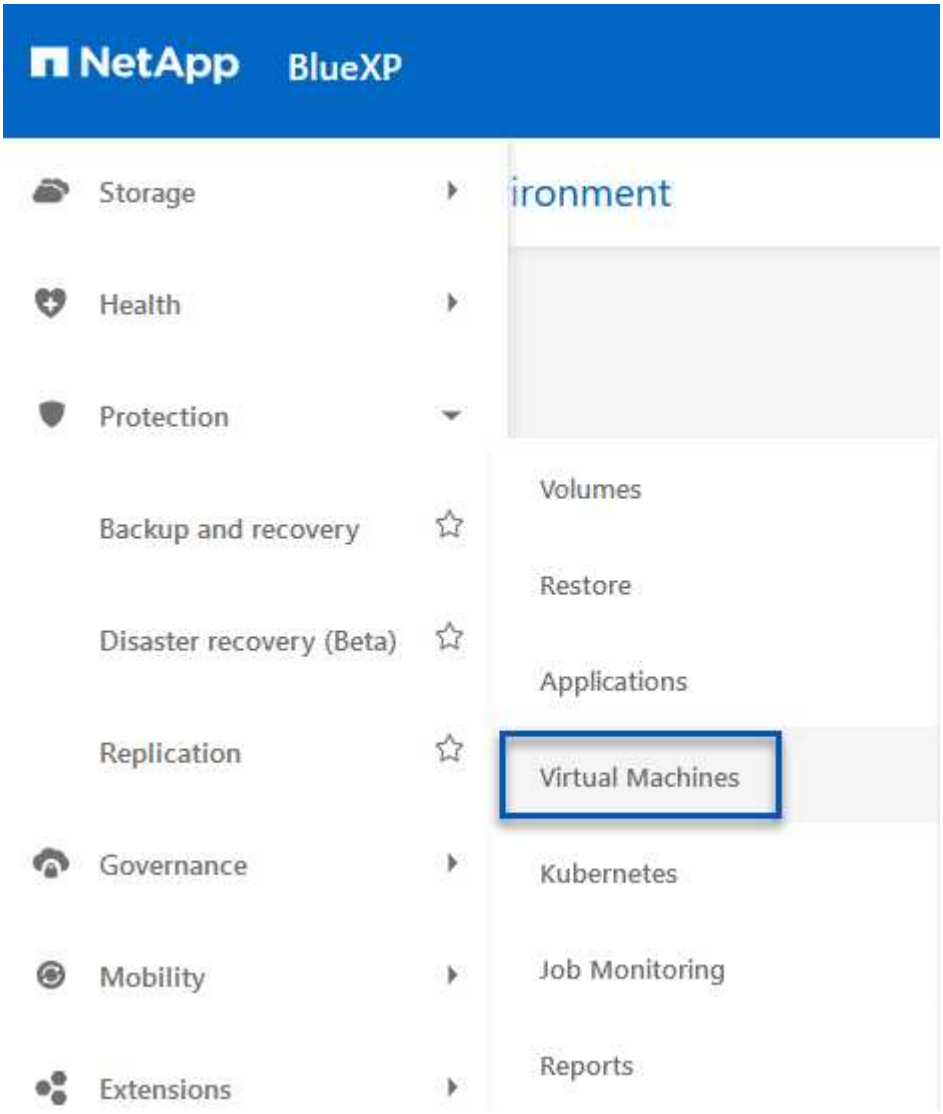
3. 填写ONTAP存储系统的凭据，然后单击*Discover (发现)*按钮以添加工作环境。


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

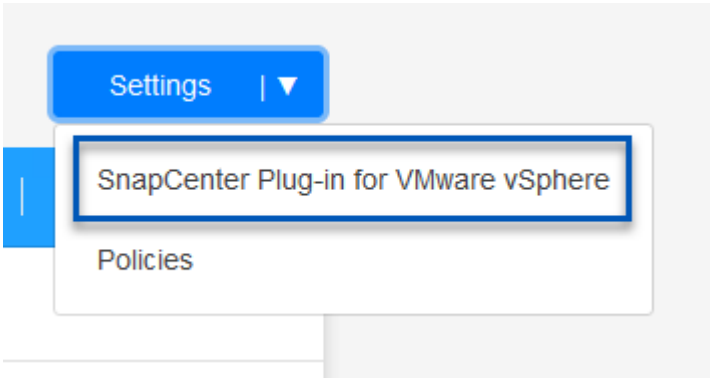
了解内部**SCV**设备和**vCenter**

要发现内部数据存储库和虚拟机资源、请添加SCV数据代理的信息以及vCenter管理设备的凭据。

1. 从BlueXP左侧菜单中选择*保护>备份和恢复>虚拟机*

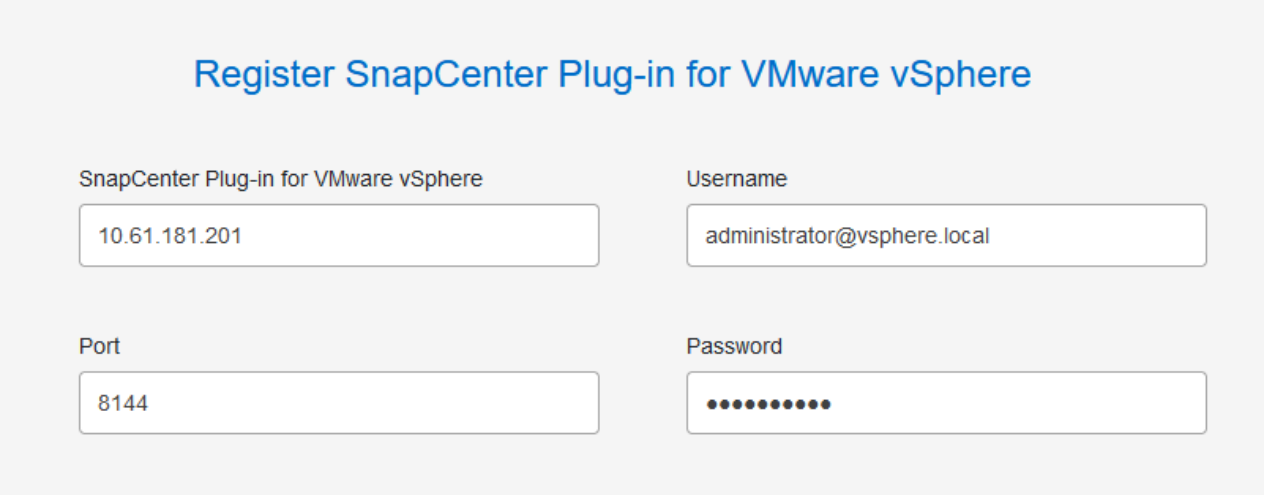


2. 从虚拟机主屏幕访问*设置*下拉菜单并选择*适用于VMware vSphere的SnapCenter插件*。

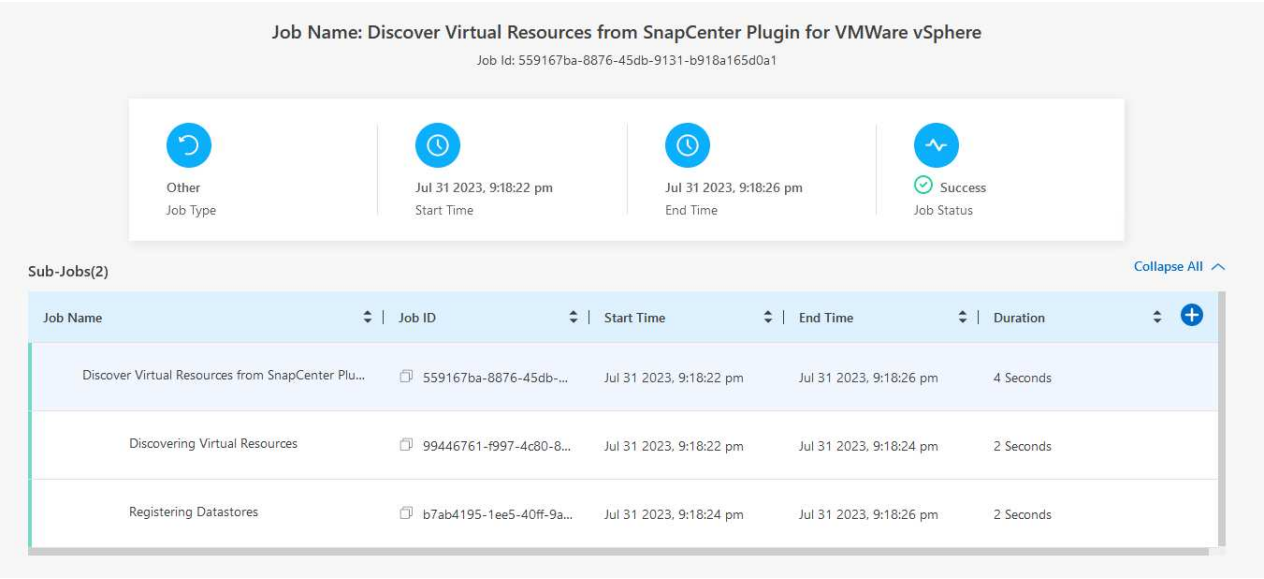


3. 单击*注册*按钮、然后输入SnapCenter插件设备的IP地址和端口号以及vCenter管理设备的用户名和密

码。单击*注册*按钮开始发现过程。



4. 可以通过作业监控选项卡监控作业进度。



5. 发现完成后、您将能够查看所有已发现的SCV设备中的数据存储库和虚拟机。

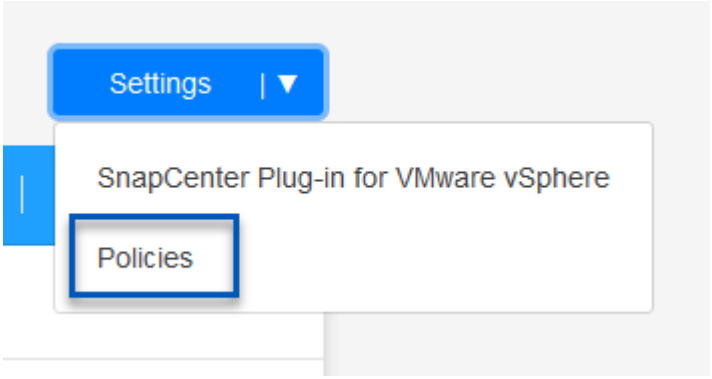
图像：： bxp-SCV hyby-23.png[查看可用资源]

创建**BlueXP**备份策略

在适用于虚拟机的BlueXP备份和恢复中、创建策略以指定保留期限、备份源和归档策略。

有关创建策略的详细信息、请参见 "创建一个策略以备份数据存储库"。

1. 从虚拟机的BlueXP备份和恢复主页中、访问*设置*下拉菜单并选择*策略*。



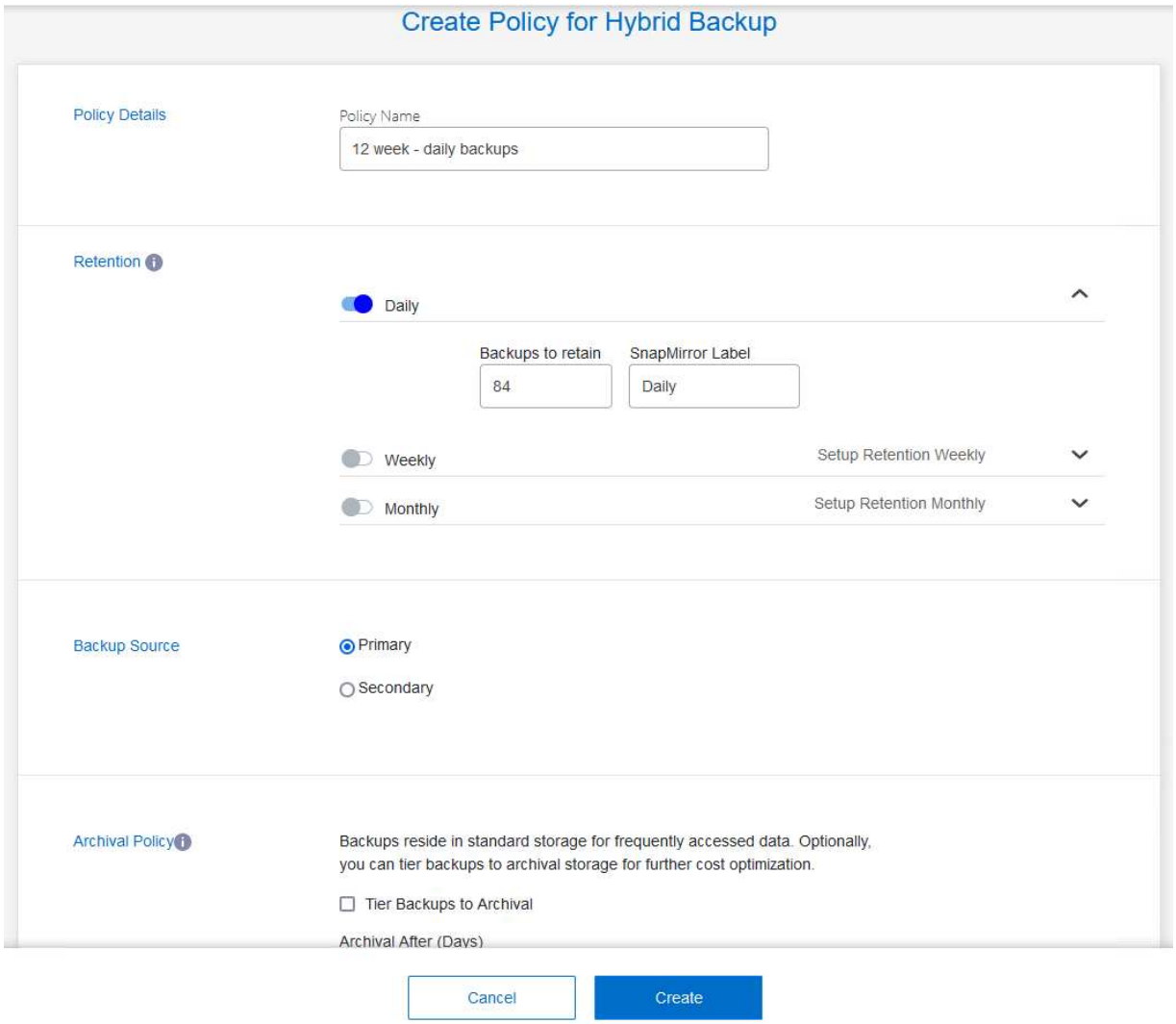
2. 单击*创建策略*以访问*为混合备份创建策略*窗口。

   a. 为策略添加名称

   b. 选择所需的保留期限

   c. 选择是从内部ONTAP主存储系统还是从二级存储系统获取备份

   d. (可选)指定备份分层到归档存储的时间期限、以节省更多成本。



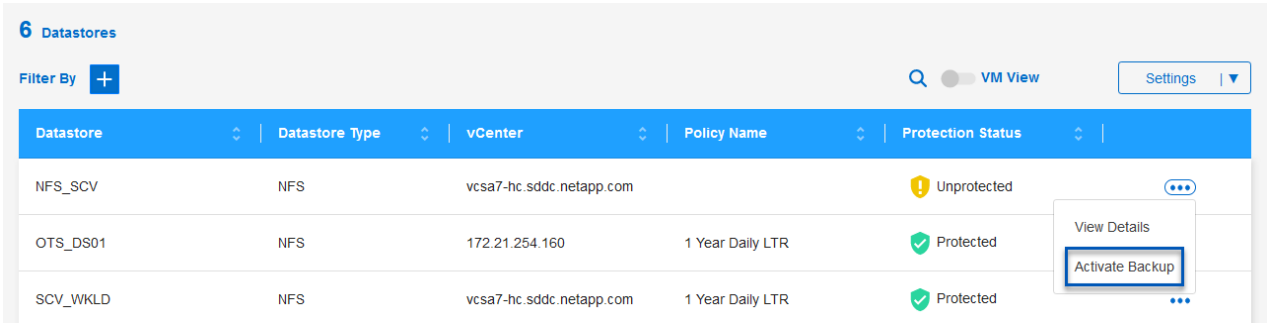
此处输入的SnapMirror标签用于标识要应用此策略的备份。标签名称必须与相应的内部SCV策略中的标签名称匹配。

3. 单击*创建*以完成策略创建。

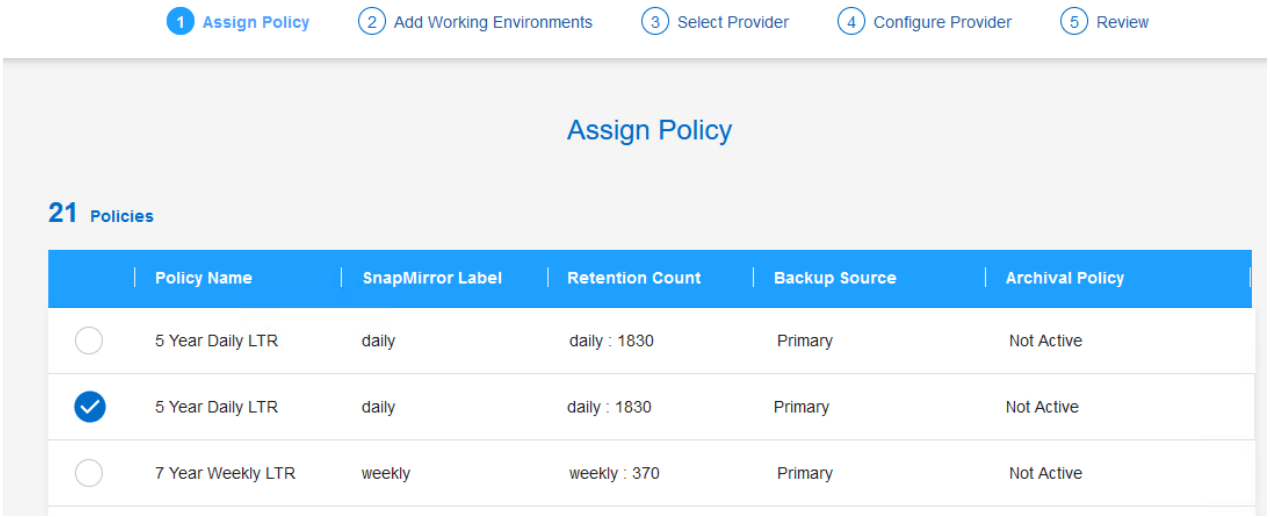
最后一步是为各个数据存储库和虚拟机激活数据保护。以下步骤概述了如何激活备份到AWS。

有关详细信息、请参见 "将数据存储库备份到Amazon Web Services"。

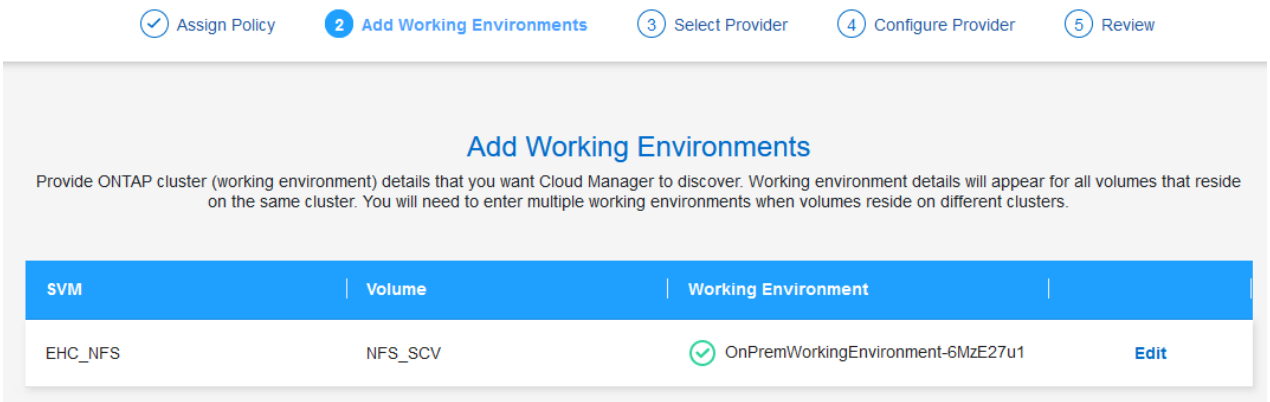
1. 从虚拟机的BlueXP备份和恢复主页中，访问要备份的数据存储库的设置下拉列表，然后选择*Activate Backup*。



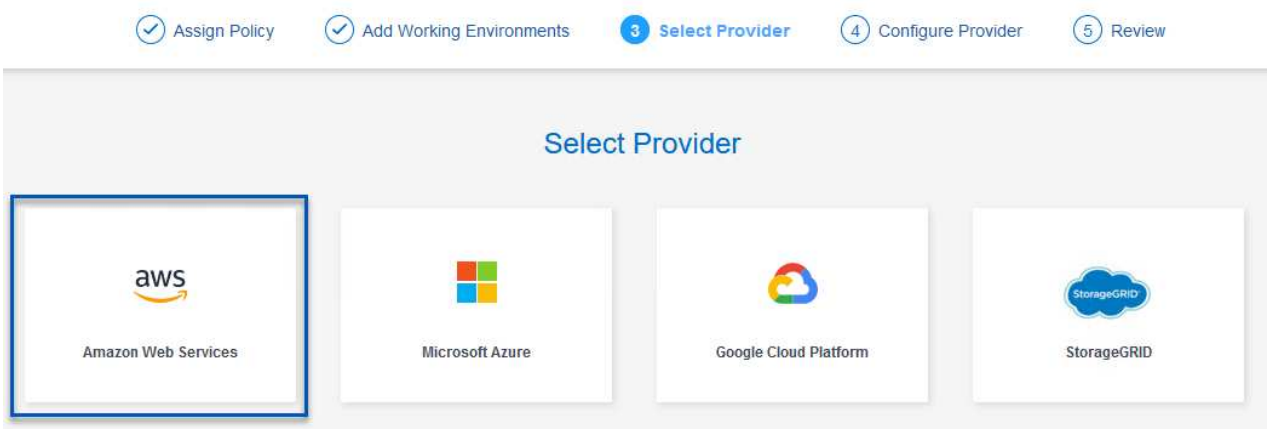
2. 分配要用于数据保护操作的策略，然后单击*Next*。



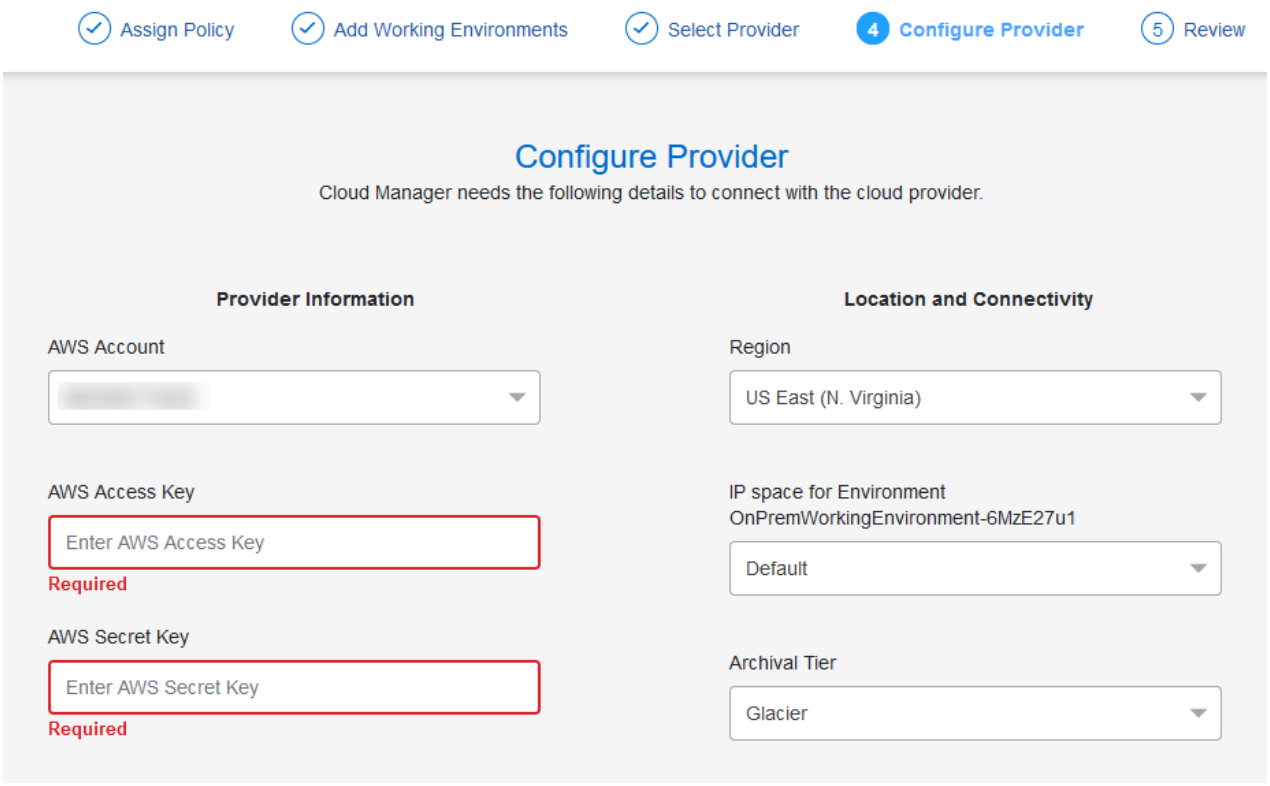
3. 如果先前已发现数据存储库和工作环境，则会在“添加工作环境”页面上显示带有复选标记的数据存储库和工作环境。如果以前未发现工作环境、您可以在此处添加它。单击“*下一步”继续。



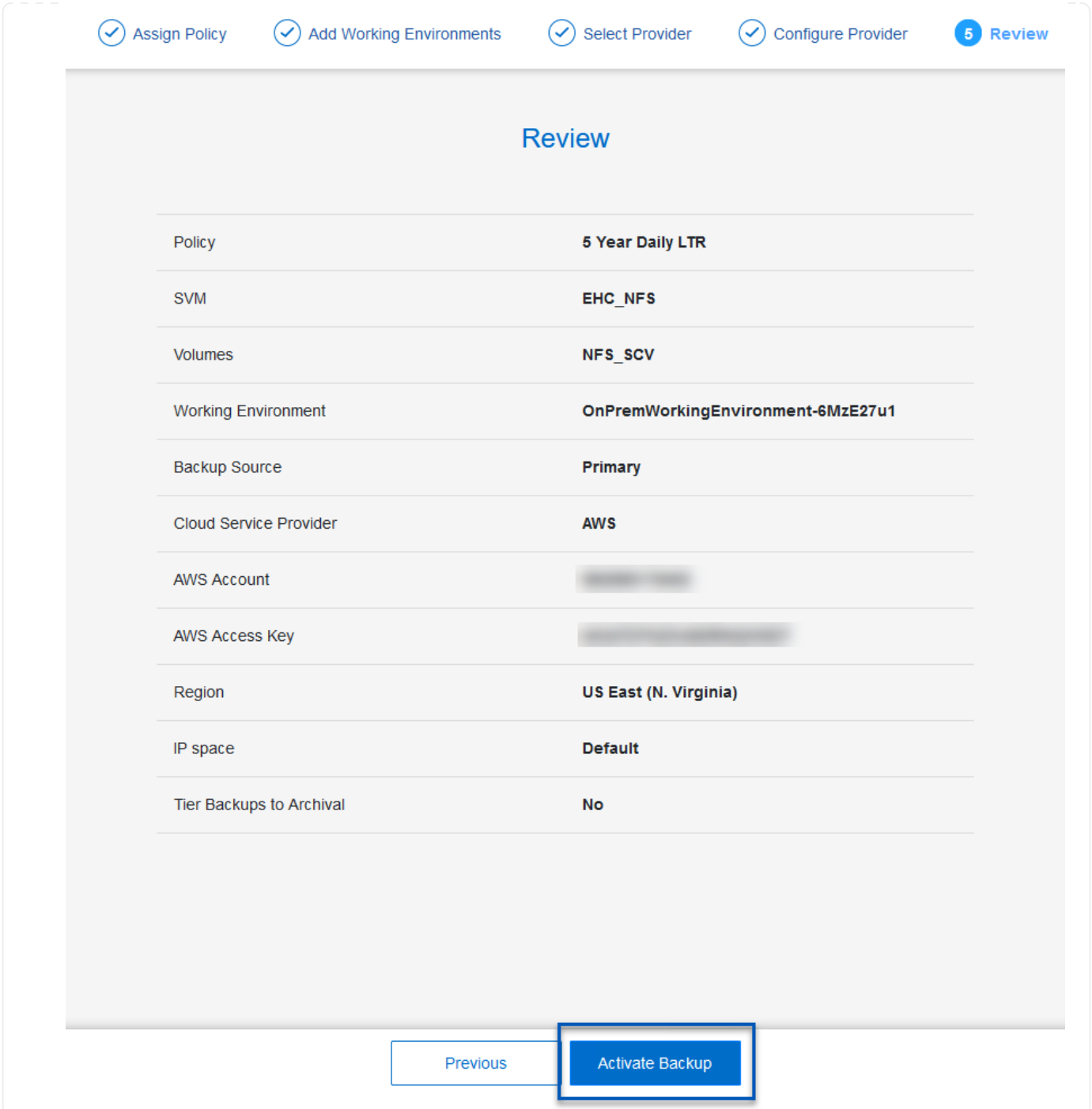
4. 在*选择提供商*页面上单击AWS、然后单击*下一步*按钮继续。



5. 填写AWS的提供商专用凭据信息、包括要使用的AWS访问密钥和机密密钥、区域和归档层。此外、请为内部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*Activate Backup*按钮以启动数据存储库的数据保护。



此时、数据传输可能不会立即开始。BlueXP备份和恢复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。

在数据丢失的情况下还原虚拟机

确保数据安全只是全面数据保护的一个方面。在发生数据丢失或勒索软件攻击时、能够从任何位置快速还原数据同样至关重要。此功能对于保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、二级存储和对象存储位置的保留计划进行自定义控制。此策略可以灵活地根据特定需求定制数据保护方法。

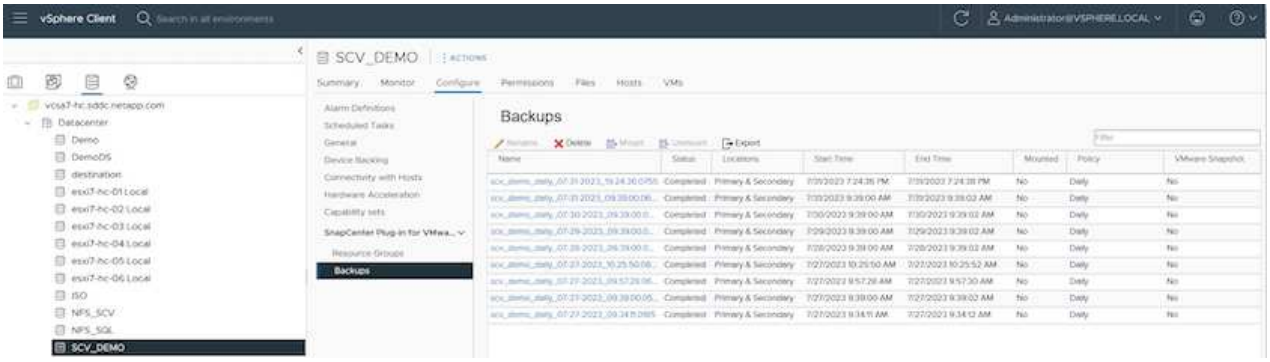
本节简要介绍了从适用于VMware vSphere的SnapCenter插件和适用于虚拟机的BlueXP备份和恢复执行数据还原的过程。

从适用于**VMware vSphere**的**SnapCenter**插件还原虚拟机

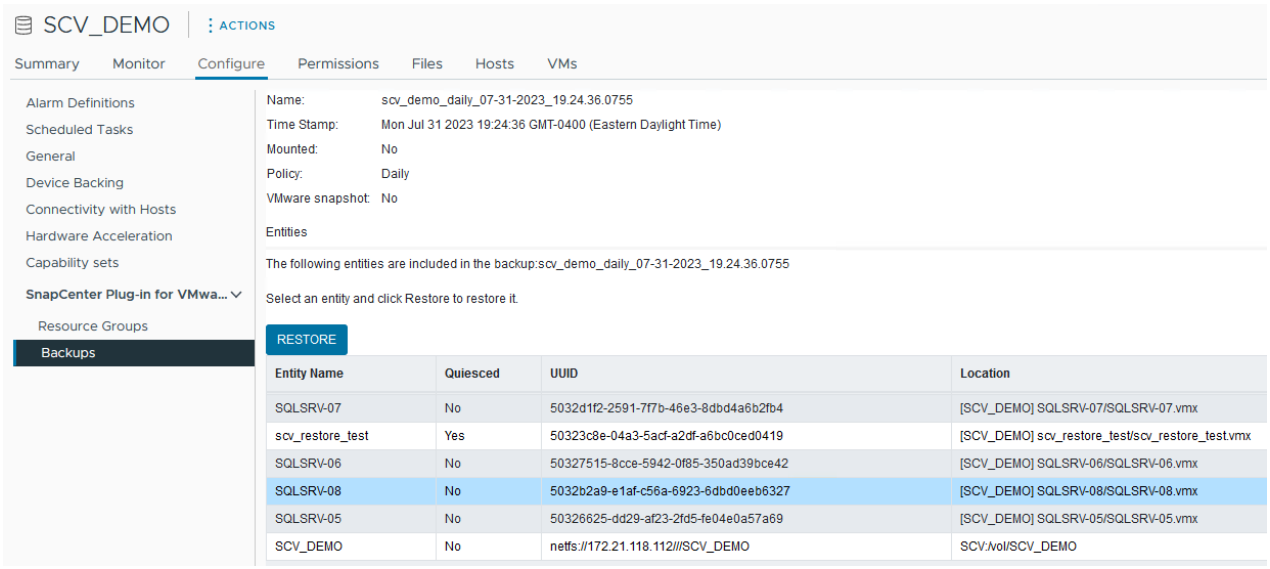
对于此解决方案虚拟机、已还原到原始位置和备用位置。本解决方案不会涵盖选择控制阀数据恢复能力的所有方面。有关选择控制阀所能提供的所有深度信息，参见 "从备份还原 VM" 在产品文档中。

要从主存储或二级存储还原虚拟机、请完成以下步骤。

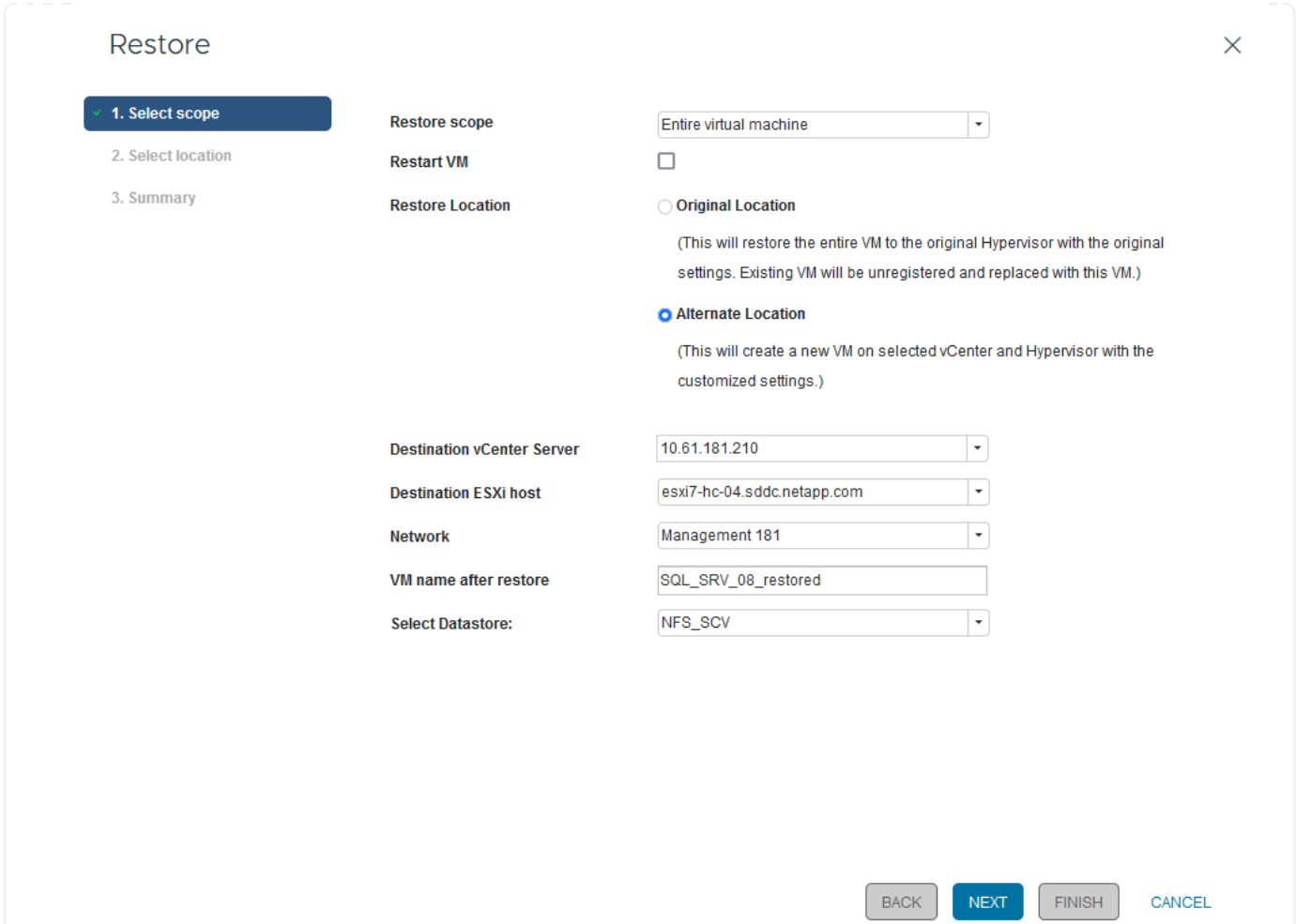
1. 从vCenter Client导航到*清单>存储*、然后单击包含要还原的虚拟机的数据存储库。
2. 从*配置*选项卡单击*备份*以访问可用备份列表。



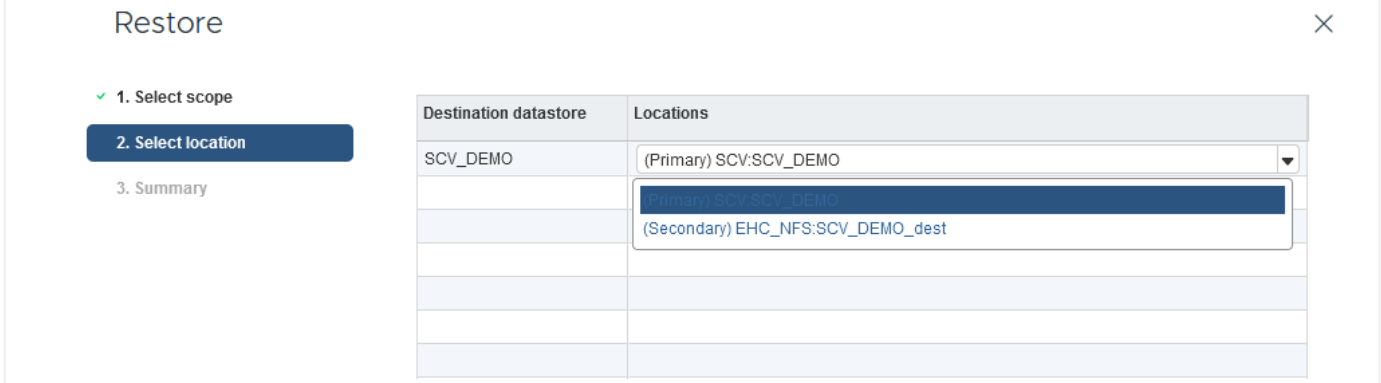
3. 单击备份以访问VM列表、然后选择要还原的VM。单击*Restore*。



4. 在还原向导中、选择还原整个虚拟机或特定VMDK。选择此选项可安装到原始位置或备用位置、并在还原后提供虚拟机名称和目标数据存储库。单击 * 下一步 * 。



5. 选择从主存储位置或二级存储位置进行备份。



6. 最后、查看备份作业的摘要、然后单击完成开始还原过程。

从虚拟机的**BlueXP**备份和恢复还原虚拟机

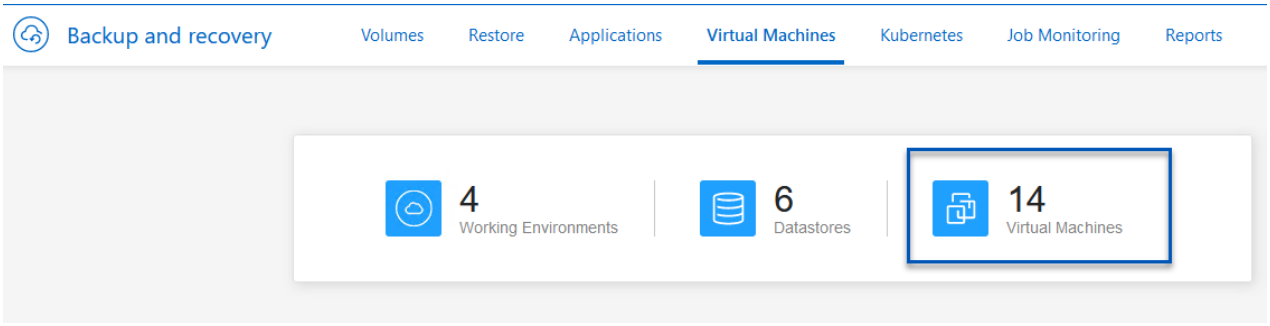
通过对虚拟机进行BlueXP备份和恢复、可以将虚拟机还原到其原始位置。还原功能可通过BlueXP Web控制台访问。

有关详细信息、请参见 "从云中还原虚拟机数据"。

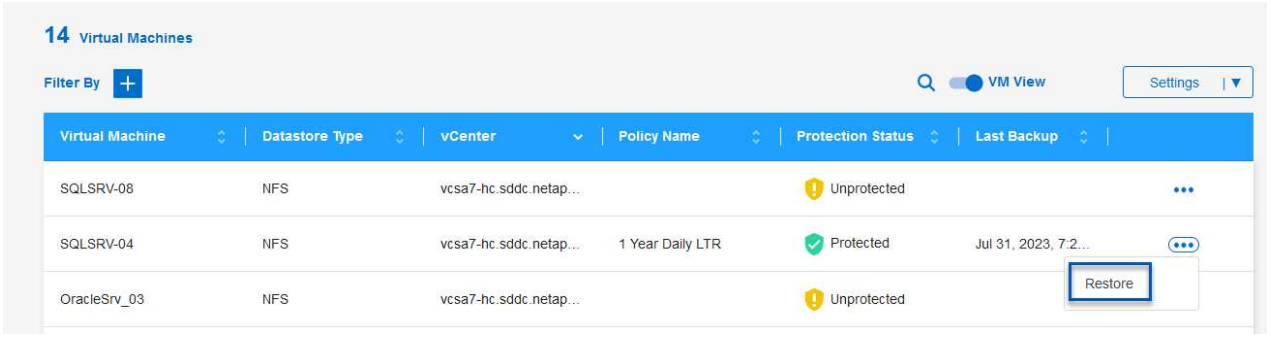
从BlueXP备份和恢复还原虚拟机

要从BlueXP备份和恢复还原虚拟机、请完成以下步骤。

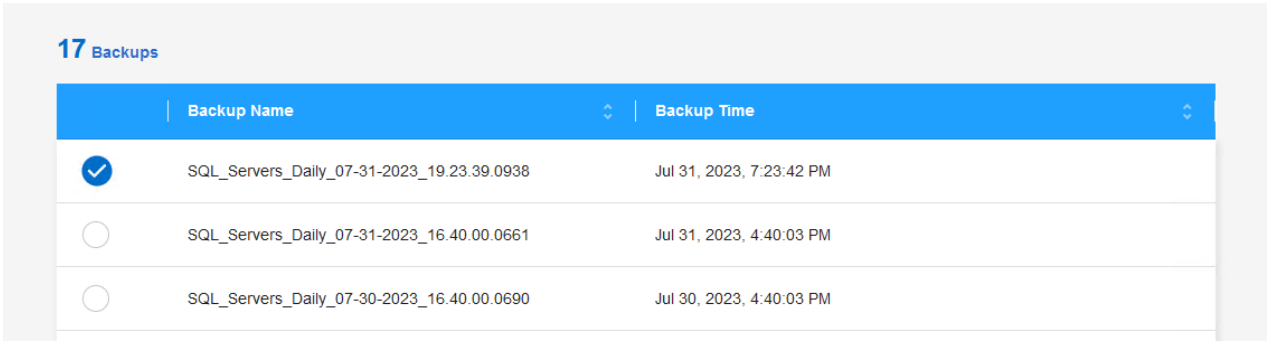
1. 导航到*保护>备份和恢复>虚拟机*，然后单击虚拟机以查看可还原的虚拟机列表。



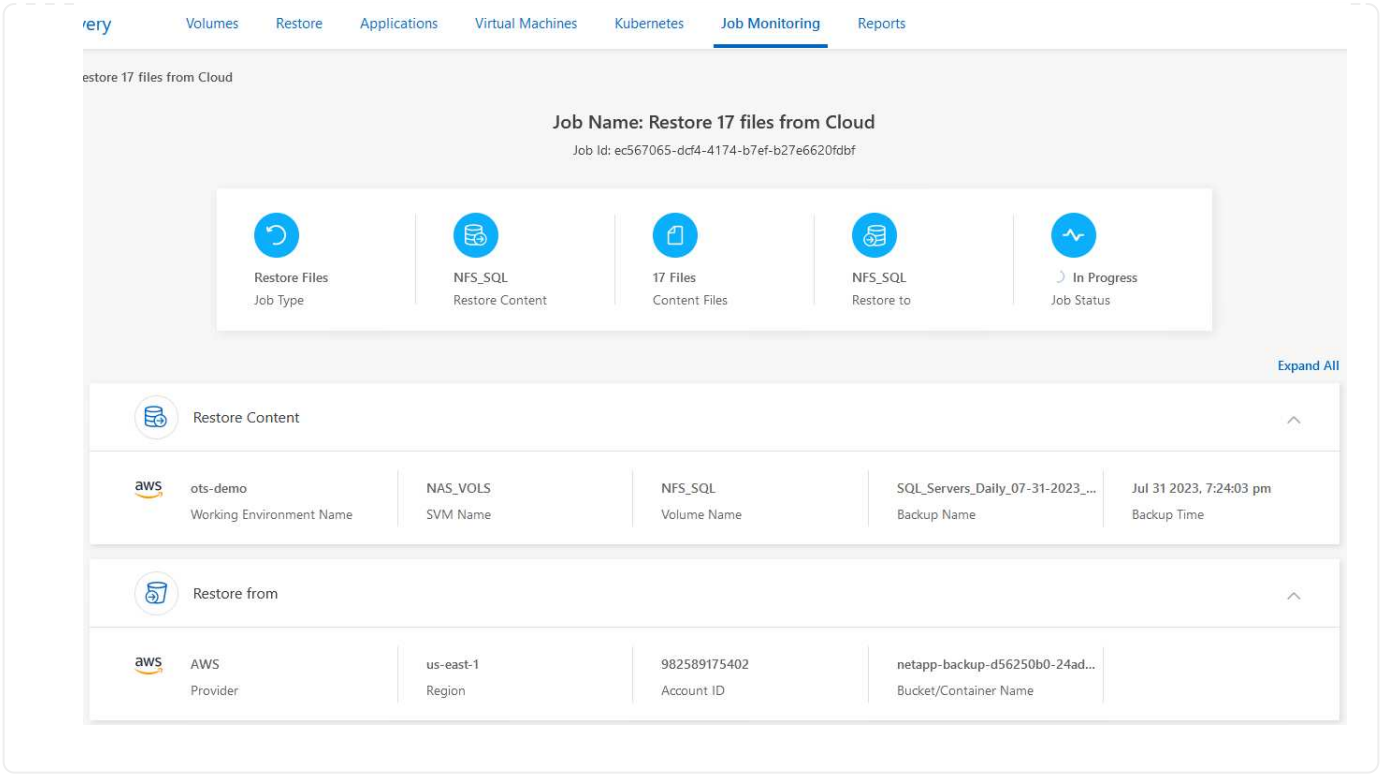
2. 访问要还原的虚拟机的设置下拉菜单、然后选择



3. 选择要从中进行还原的备份，然后单击*Next*。



4. 查看备份作业的摘要，然后单击*Restore*以启动恢复过程。
5. 通过*作业监控*选项卡监控恢复作业的进度。



结论

通过适用于VMware vSphere的SnapCenter插件和适用于虚拟机的BlueXP备份和恢复实施3-2-1备份策略后、可提供强大、可靠且经济高效的解决方案来实现数据保护。此策略不仅可以确保数据冗余和可访问性、还可以灵活地从任何位置以及内部ONTAP存储系统和基于云的对象存储还原数据。

本文档中提供的用例重点介绍经验证的数据保护技术、这些技术重点介绍了NetApp、VMware和领先云提供商之间的集成。适用于VMware vSphere的SnapCenter插件可与VMware vSphere无缝集成、从而可以高效地集中管理数据保护操作。这种集成简化了虚拟机的备份和恢复流程、从而可以在VMware生态系统中轻松地计划、监控和灵活地执行还原操作。适用于虚拟机的BlueXP备份和恢复通过将虚拟机数据安全地通过空中映射备份到基于云的对象存储、提供3-2-1中的一(1)个备份。直观的界面和逻辑工作流为关键数据的长期归档提供了一个安全平台。

追加信息

要详细了解此解决方案 中提供的技术、请参阅以下追加信息。

- "适用于 VMware vSphere 的 SnapCenter 插件文档"
- "BlueXP文档"

VMware Sovereign Cloud

适用于主权云的**VMware**资源

NetApp和VMware Sovereign Cloud

VMware Sovereign Cloud概述

对于许多处理和维护高度敏感数据的实体(如国家和州政府)以及监管严格的行业(如金融和医疗保健)来说、主权概念正逐渐成为云计算的必要组成部分。各国政府还希望扩大数字经济能力、减少对跨国公司云服务的依赖。

VMware Sovereign Cloud计划

VMware将主权云定义为：

- 保护和释放关键数据(例如国家数据、公司数据和个人数据)对私营和公共部门组织的价值
- 为数字经济提供全国性能力
- 利用经过审核的安全控制保护数据安全
- 确保遵守数据隐私法律
- 通过为数据驻留和数据主权提供完全的司法管辖控制、提高数据控制能力

与值得信赖的VMware Sovereign云服务提供商合作

为了确保成功、企业必须与他们信任的合作伙伴合作、这些合作伙伴必须能够托管真正的自主主权云平台。VMware Sover参加VMware云计划的云提供商致力于设计和运营基于现代软件定义架构的云解决方案、这些架构体现了VMware Sover要 云框架中概述的关键原则和最佳实践。

- 数据主权和管辖控制–所有数据均为驻留数据、并受收集数据的国家/地区的专属控制和权威约束。在管辖范围内全面管理业务
- 数据访问和完整性—云基础架构具有故障恢复能力、可在辖区内至少两个数据中心位置使用、并提供安全和专用连接选项。
- 数据安全与合规性–信息安全管理系统控制措施根据行业认可的全球(或区域)标准进行认证并定期审核。
- 数据独立性和移动性—支持现代应用程序架构、防止受制于供应商云、实现应用程序可移植性和独立性

有关VMware的详细信息、请访问：

- "VMware Sovereign Cloud概述"
- "什么是VMware Sover꾍 좨 云？ "
- "隆重介绍全新VMware Sovereign Cloud计划"
- "VMware Sovereign Cloud技术白皮书"

采用VMware Sovereign Cloud的Netpp：用例

NetApp通过集成多种NetApp技术、为VMware Sovereign Cloud概念提供支持。

使用以下链接详细了解NetApp技术与VMware Sovereover Cloud的集成：

- "NetApp StorageGRID作为对象存储扩展"

NetApp StorageGRID作为对象存储扩展

NetApp已与VMware合作、将NetApp StorageGRID集成到VMware Cloud Director中、以支持VMware Sovereign云。此VMware Cloud Director插件支持服务提供商使用StorageGRID作为其对象存储产品(无论使用情形如何)、并允许通过服务提供商用来管理其产品目录中其他部分的相同VMware多租户解决方案(VMware Cloud Director)进行StorageGRID管理。

提供VMware主权云的合作伙伴可以选择NetApp StorageGRID来帮助他们管理和维护包含非结构化数据的云环境。它在为Amazon S3 API等行业标准API提供本机支持方面实现了通用兼容性、有助于确保在各种云环境之间实现顺畅的互操作性、而自动化生命周期管理等独特创新有助于确保更经济高效地保护、存储和长期保留客户的非结构化数据。

NetApp的Sovereign Cloud与Cloud Director集成为客户提供以下优势：

- 确保敏感数据(包括元数据)仍受主权控制、同时防止可能违反数据隐私法律的外国当局访问。
- 提高安全性和合规性、保护应用程序和数据免受快速演变的攻击向量的影响、同时保持与可信本地系统的持续合规性。基础架构、内置框架和本地专家。
- 打造适应未来需求的基础架构、快速应对不断变化的数据隐私法规、安全威胁和地缘政治。
- 能够通过安全的数据共享和分析释放数据的价值、从而在不违反隐私法律的情况下推动创新。数据完整性受到保护、可确保获得准确的洞察力。

有关StorageGRID集成的详细信息、请查看以下内容：

- "NetApp公告"

采用**Red Hat OpenShift**容器工作负载的**NetApp**混合云

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

概述

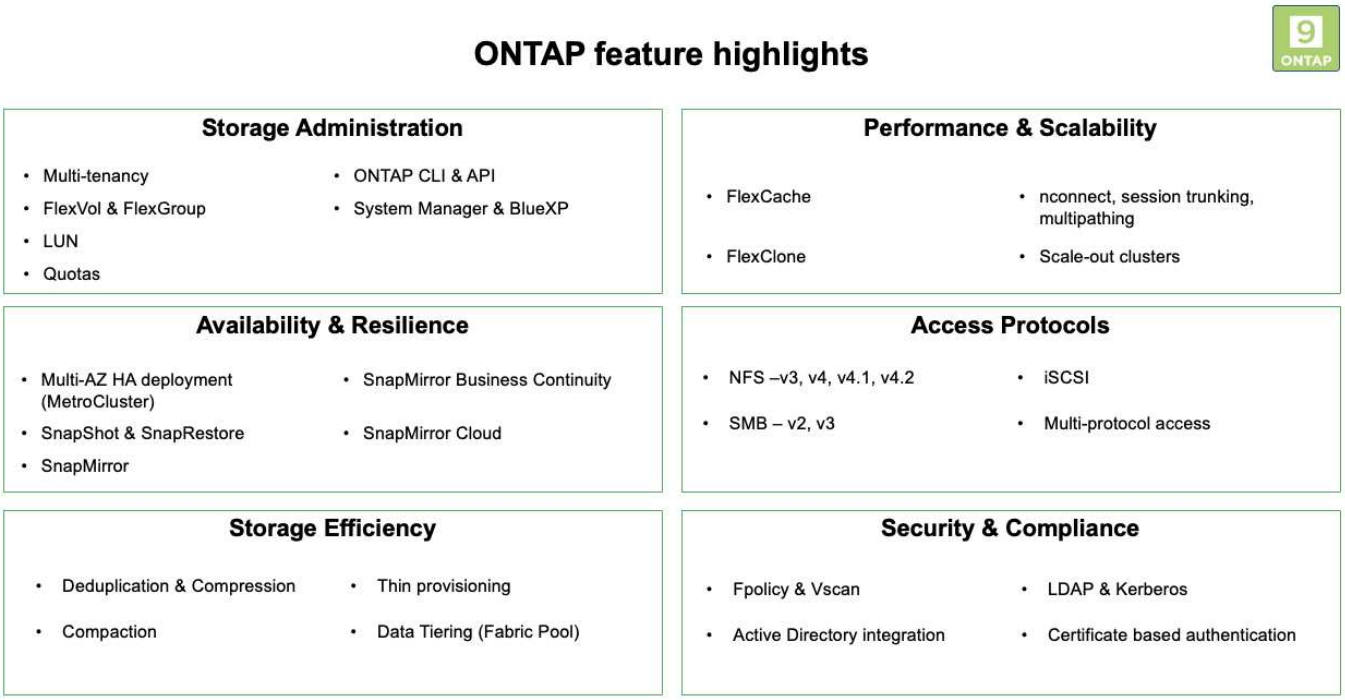
NetApp发现、越来越多的客户正在利用围绕Kubnetes构建的容器和流程编排平台来打造现代化的传统企业级应用程序以及构建新应用程序。Red Hat OpenShift容器平台就是我们看到许多客户采用的一个示例。

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

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

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

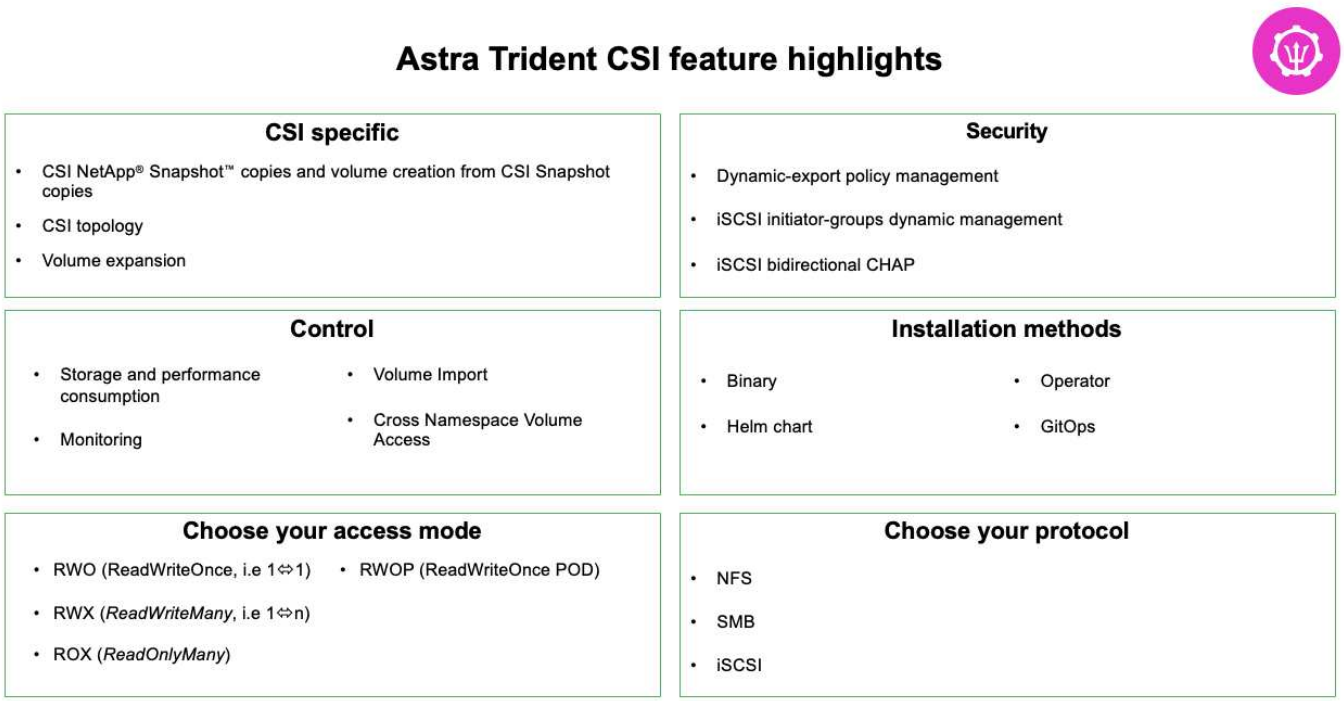
- Cloud Volumes Service for Google Cloud (CVS)、Azure NetApp Files (ANF)、Amazon FSx for NetApp ONTAP 可在超云中提供完全托管的存储



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

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

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



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

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

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

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

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

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

采用Red Hat OpenShift的NetApp混合多云：

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

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

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

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

- 内部部署
- 云
  - 自行管理的OpenShift集群和自行管理的NetApp存储
  - 提供商管理的OpenShift集群和提供商管理的NetApp存储

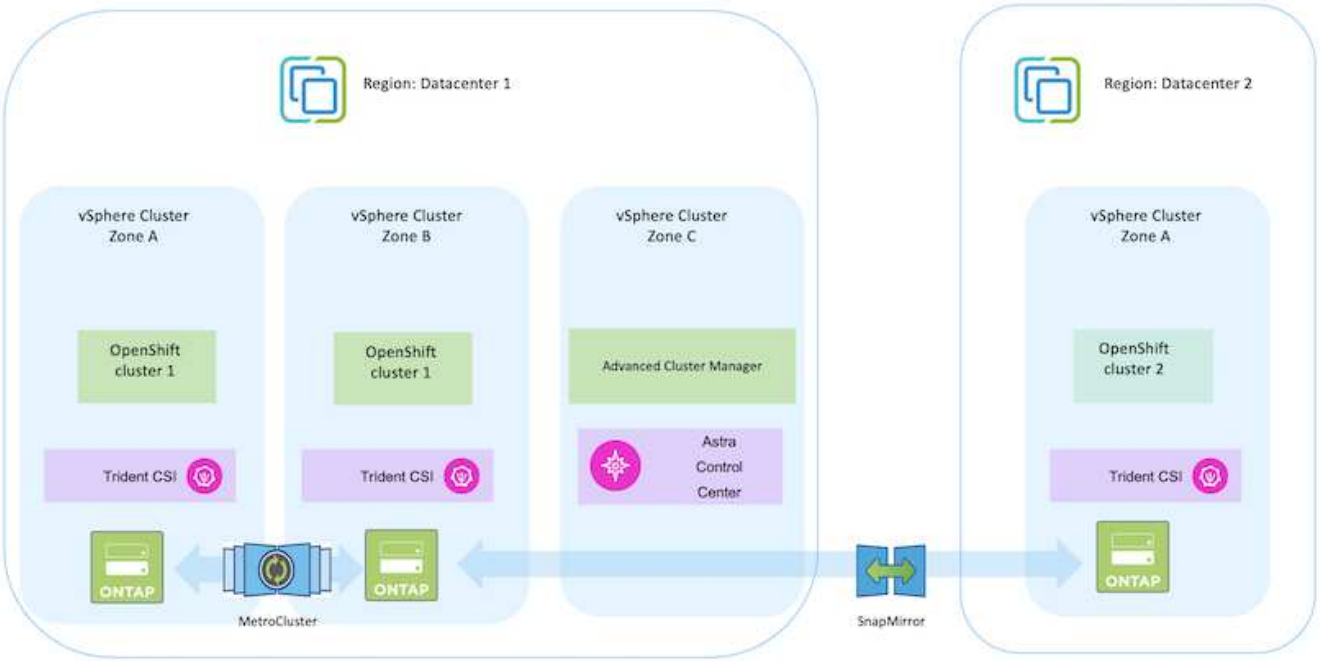
我们将在未来构建更多的解决方案和用例。

方案**1**：使用**ACC**在内部环境中保护和迁移数据

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

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

场景 **1**

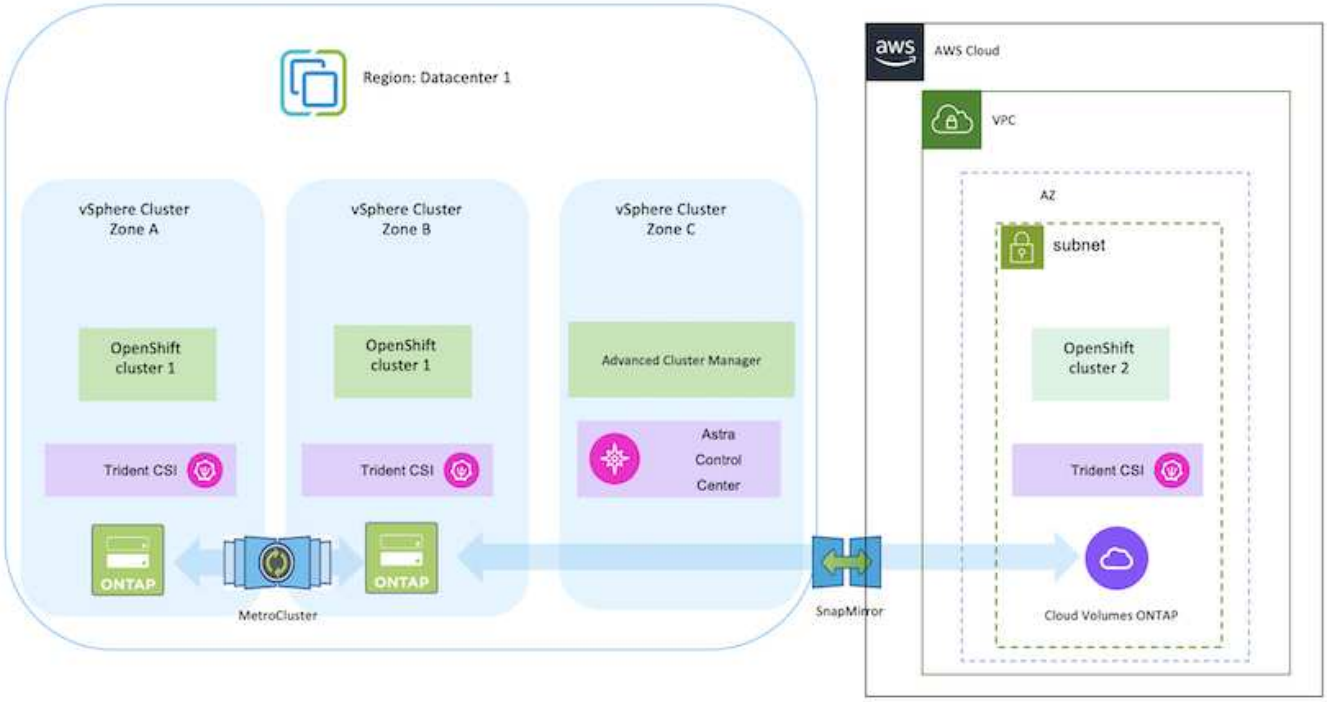


方案**2**：使用**ACC**保护数据并将其从内部环境迁移到**AWS**环境

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

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

场景 **2**

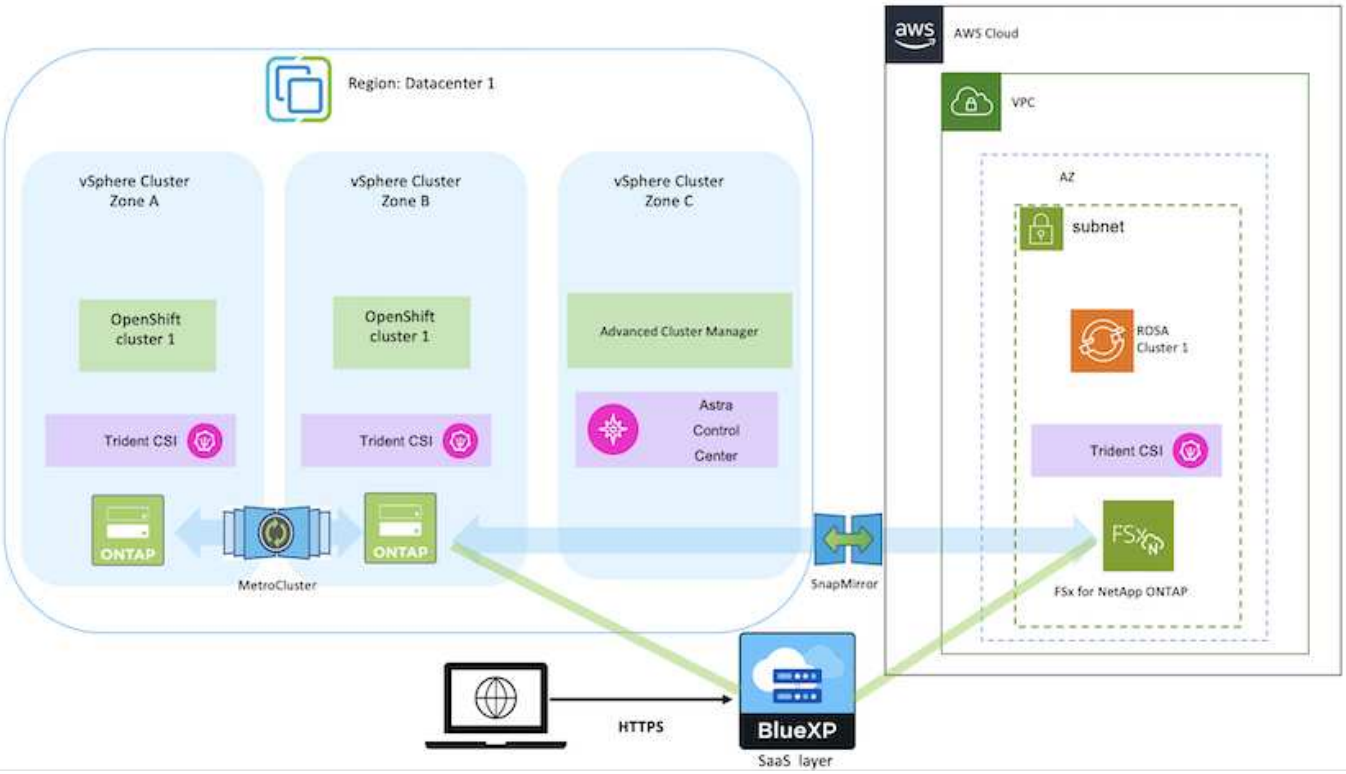


方案**3**：数据保护以及从内部环境迁移到**AWS**环境

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

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

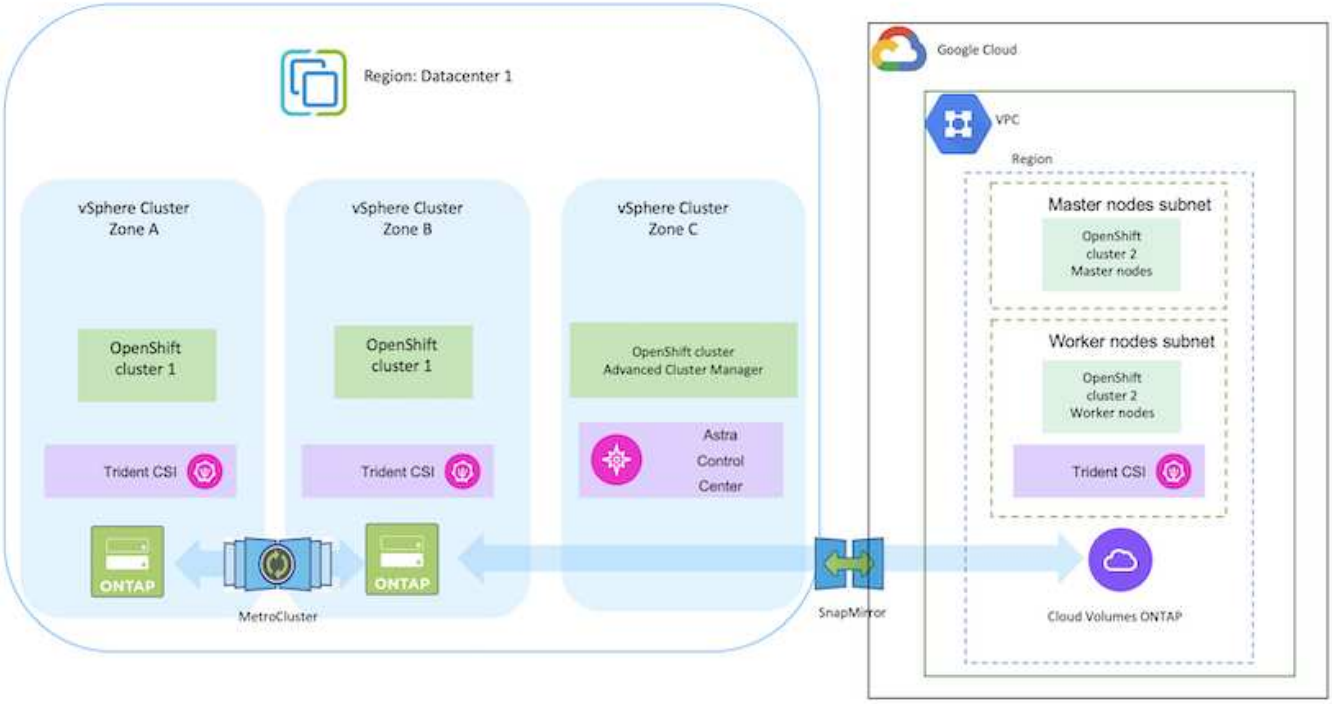
方案**3.**



方案**4**：使用**ACC**保护数据并将数据从内部环境迁移到**GCP**环境

内部：自行管理的**OpenShift**集群和自行管理的存储
Google Cloud：自行管理的**OpenShift**集群和自行管理的存储

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

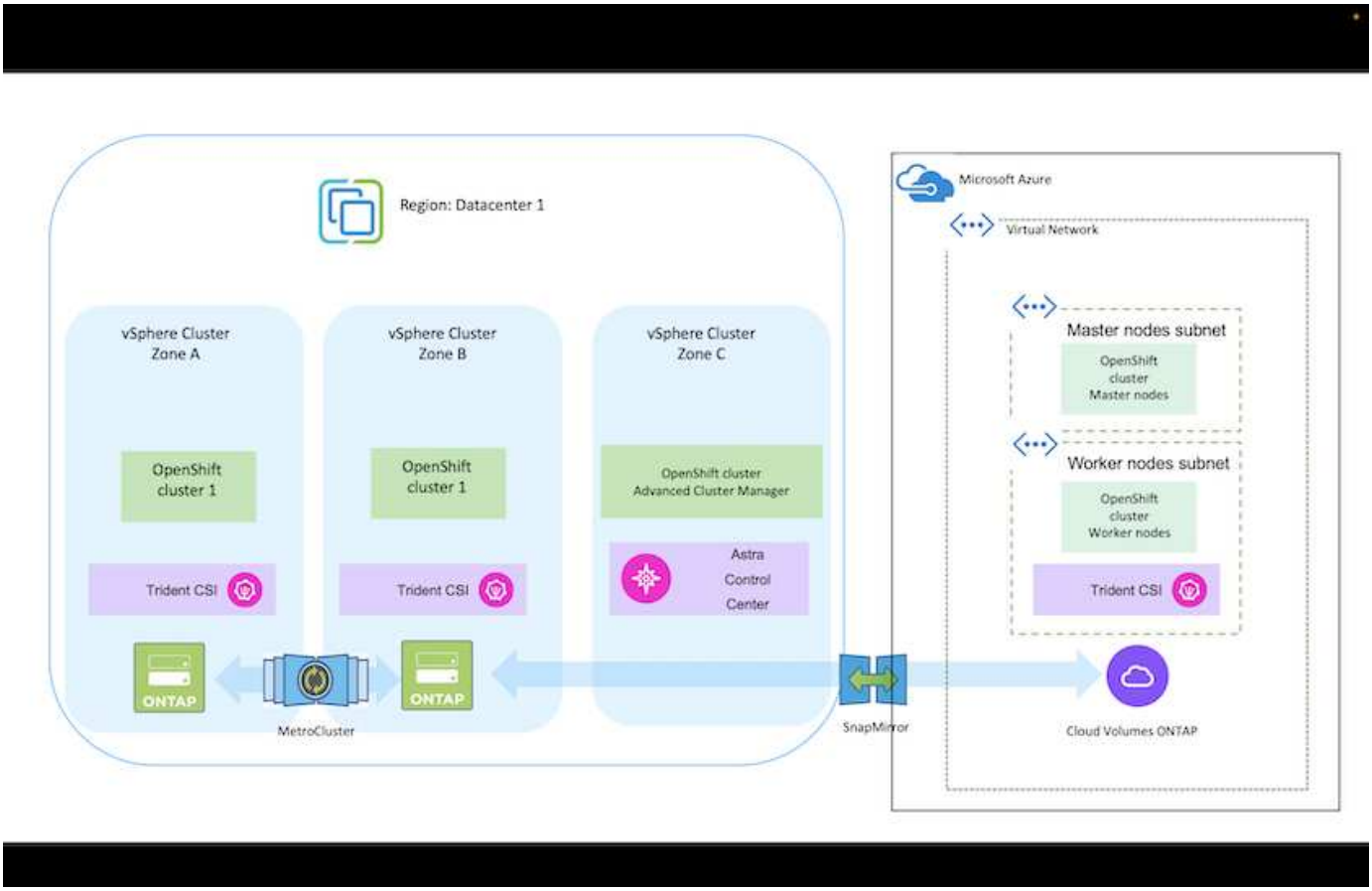


有关在MetroCluster 配置中使用ONTAP 时的注意事项、请参见 "此处"。

方案**5**：使用**ACC**保护数据并将其从内部环境迁移到**Azure**环境

内部：自行管理的**OpenShift**集群和自行管理的存储
Azure云：自行管理的**OpenShift**集群和自行管理的存储

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



有关在MetroCluster 配置中使用ONTAP 时的注意事项、请参见 "此处"。

解决方案 验证中使用的各种组件的版本

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

解决方案的方案1、2和3已使用下表所示的版本进行了验证：

* 组件 *	* 版本 *
VMware	vSphere Client 8.0.0.10200 VMware ESXi、8.0.0、20842819
集线器集群	OpenShift 4.11.34
源集群和目标集群	OpenShift 4.12.9、在内部和AWS中
NetApp Asta三端	TRIdent服务器和客户端23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
*NetApp ONTAP *	ONTAP 9.12.1
*AWS FSx for NetApp ONTAP *	单可用性(AZ)

已使用下表所示的版本对解决方案的方案4进行了验证：

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

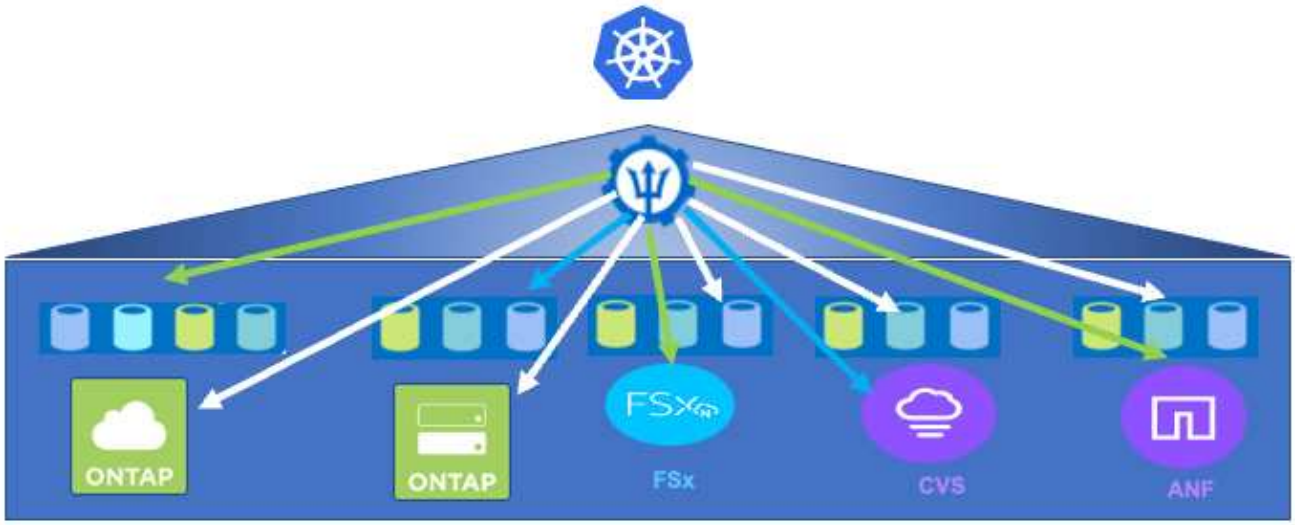
已使用下表所示的版本对解决方案的方案5进行了验证：

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

支持**NetApp**存储与**Red Hat Open Shift**容器的集成

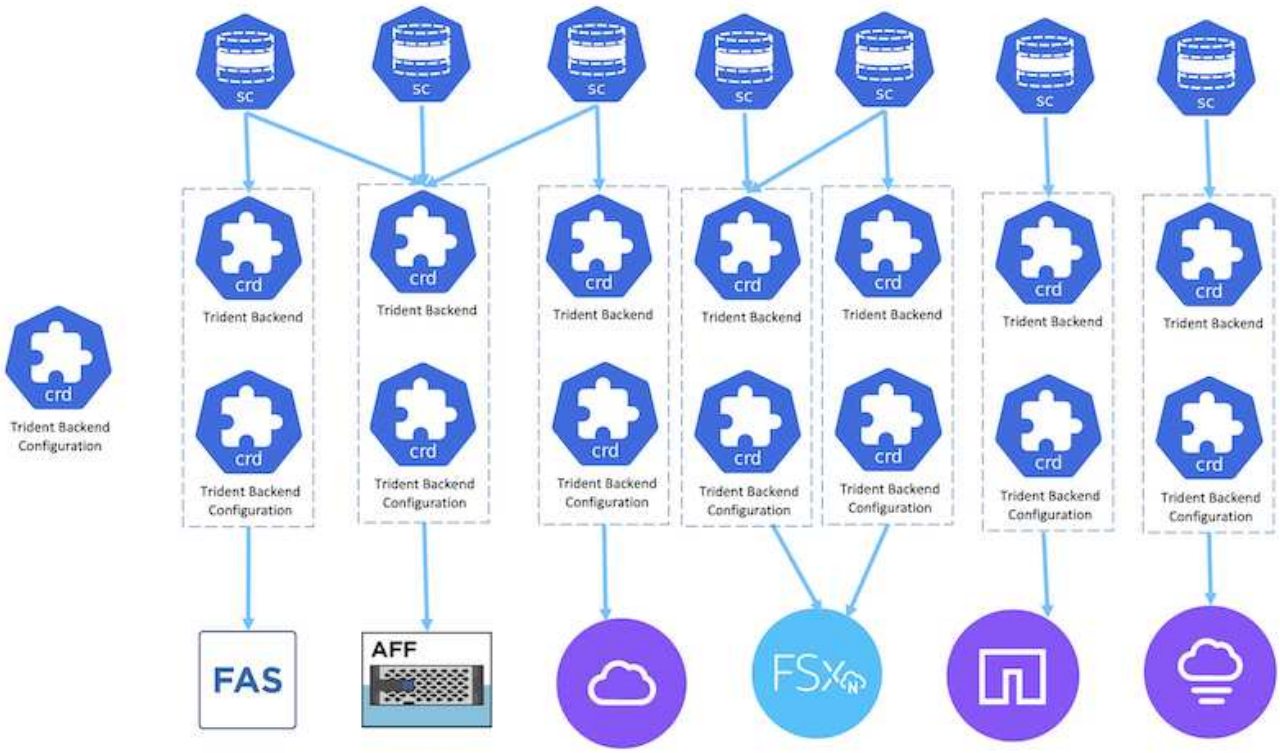
无论Red Hat Open Shift容器是在VMware上运行还是在超大型机中运行、NetApp A作用力三端均可用作其支持的各种后端NetApp存储的CSI配置程序。

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

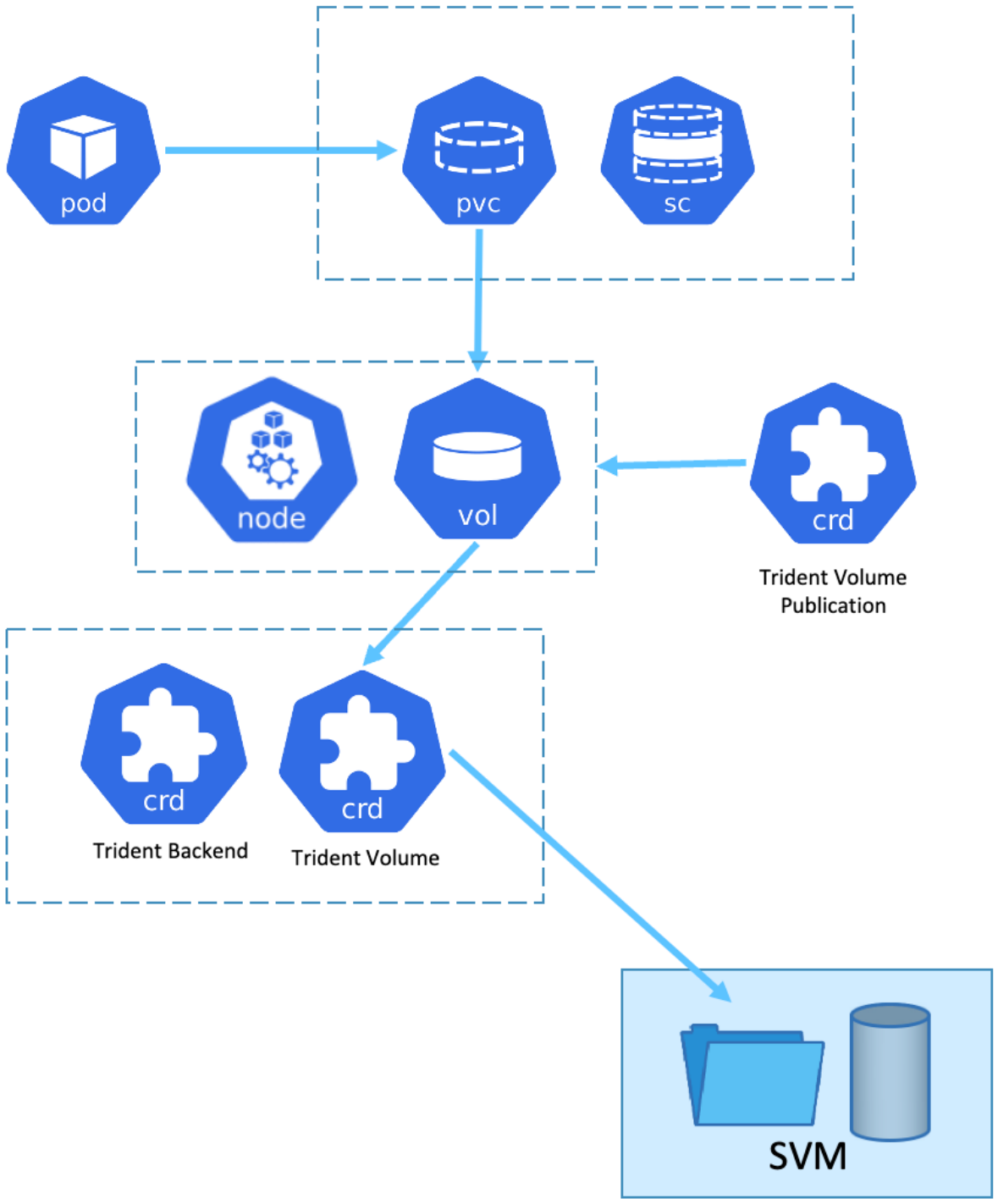


ONTAP Storage Virtual Machine (SVM)可提供安全多租户。一个OpenShift集群可以连接到一个或多个SVM、甚至可以连接到多个ONTAP 集群。存储类会根据参数或标签筛选后端存储。存储管理员可定义使用三级联后端配置连接到存储系统所需的参数。成功建立连接后、它将创建三项技术后端并填充存储类可以筛选的信息。

存储器和后端之间的关系如下所示。



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



容器存储接口(CSI)选项

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

VMware CSI支持

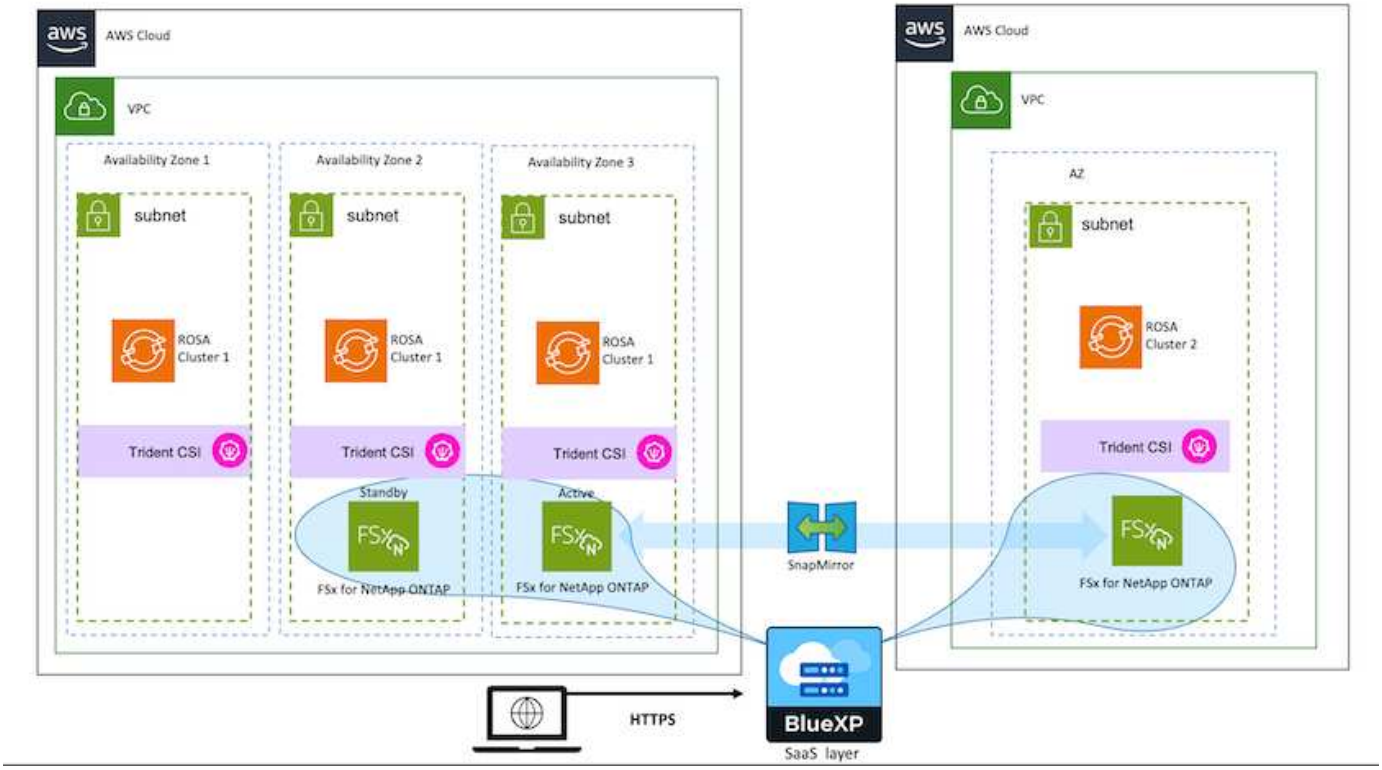
- 基于核心块的数据存储库(FC、FCoE、iSCSI、NVMeoF)
- 基于核心文件的数据存储库(NFS v3、v4)
- vVol数据存储库(块和文件)

通过以下驱动程序、可以支持**ONTAP**

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

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

在AWS中、FSx for NetApp ONTAP (FSxN)可以部署在单个可用性区域(AZ)或多个可用性区域(AZ)中。对于需要高可用性的生产工作负载、与单个AZ相比、多可用性可提供分区级容错、并具有更好的NVMe读取缓存。有关详细信息、请查看 "AWS性能准则"。
为了节省灾难恢复站点的成本、可以使用一个AZ FSx ONTAP。



有关FSx ONTAP 支持的SVM数量、请参见 "管理FSx ONTAP Storage Virtual Machine"

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

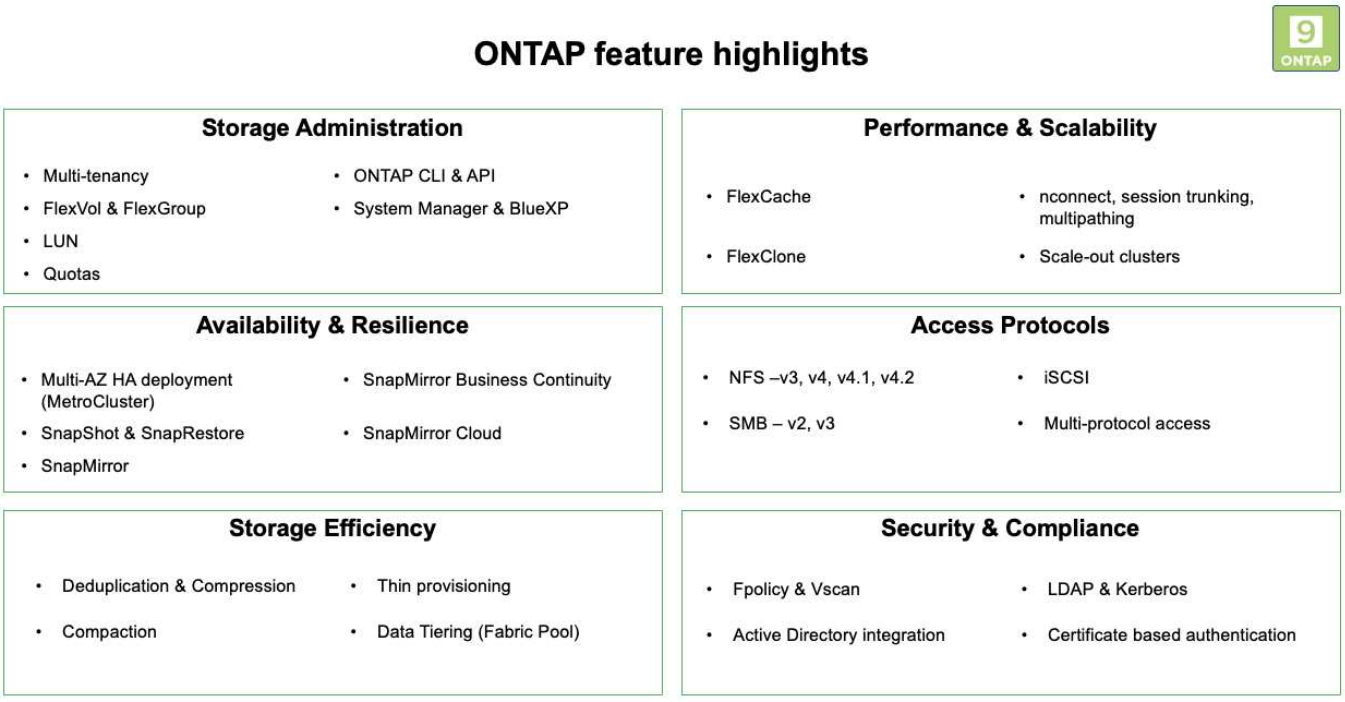
概述

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

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

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

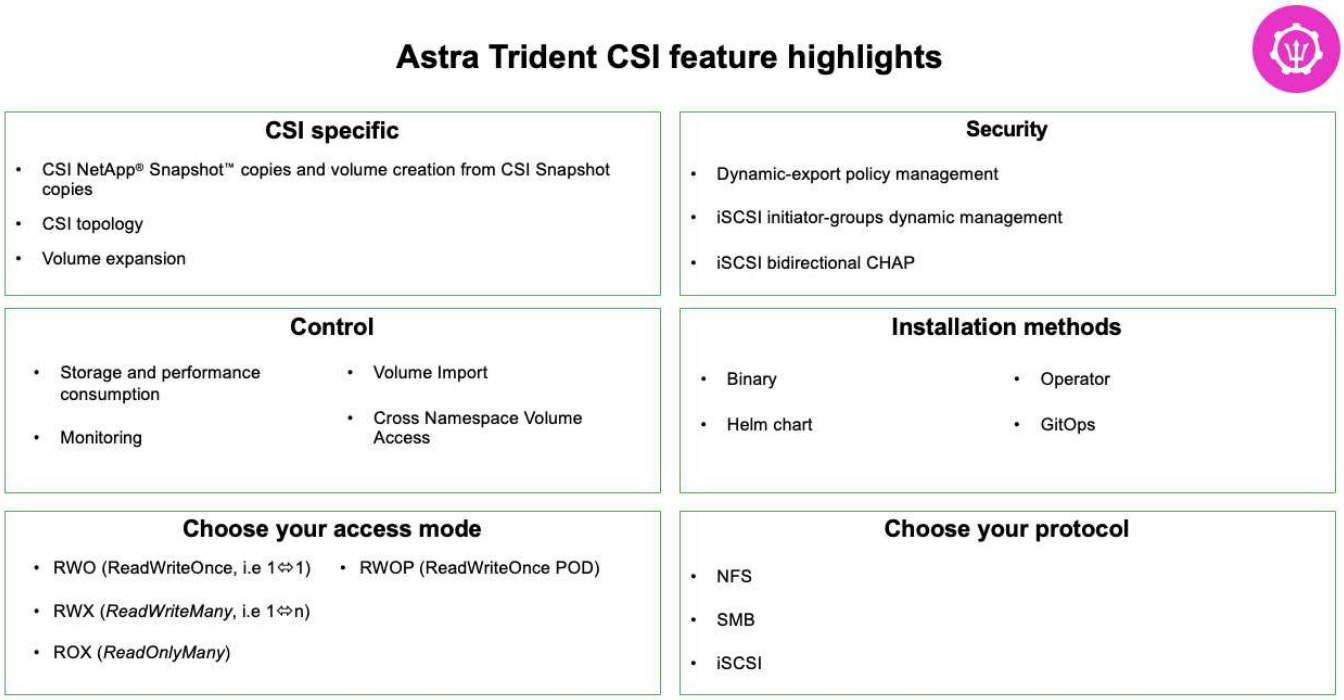
- 内部环境中的自行管理存储：
  - NetApp光纤连接存储(FAS)、NetApp全闪存FAS 阵列(AFF)、NetApp全SAN阵列(ASA)和ONTAP Select
- 内部部署中由提供商管理的存储：
  - NetApp Keystone 提供存储即服务(STaaS)
- 云中的自行管理存储：
  - NetApp Cloud Volumes ONTAP (CVO)可在超大容量云中提供自行管理的存储
- 云中由提供商管理的存储：
  - Cloud Volumes Service for Google Cloud (CVS)、Azure NetApp Files (ANF)、Amazon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



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

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

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



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

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

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

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

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

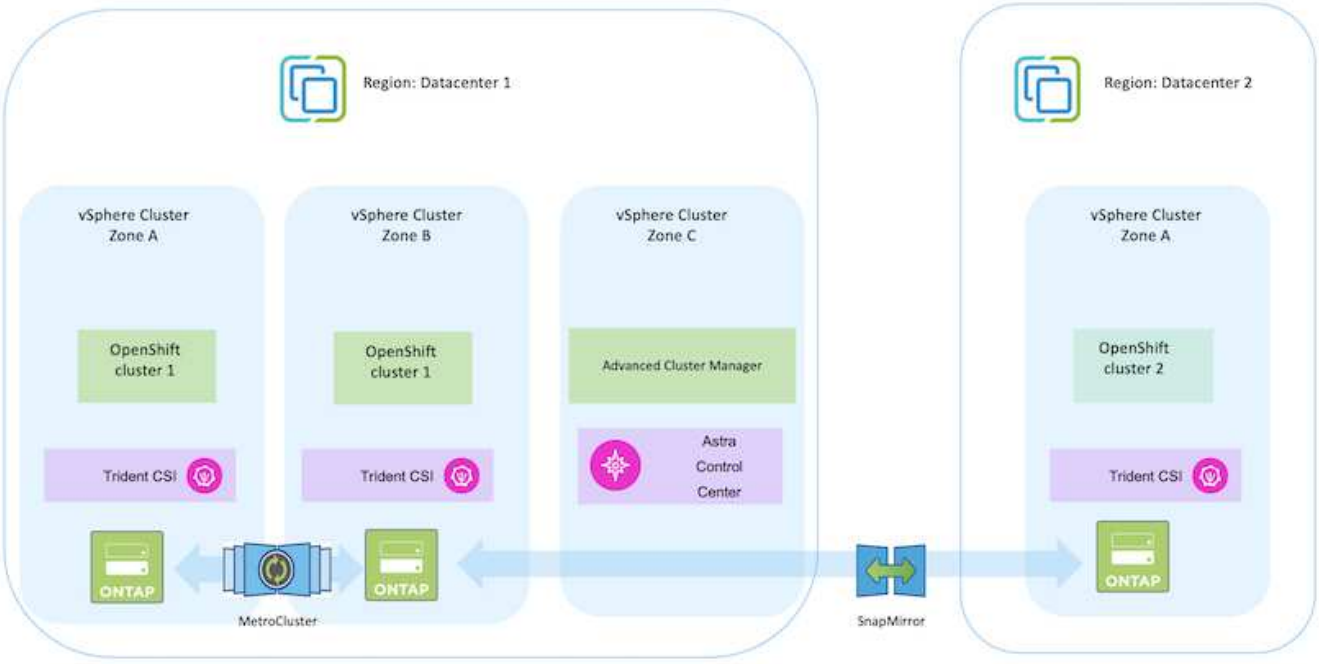
如果客户需要在私有数据中心的基础架构上运行现代化容器化应用程序、他们可以做到这一点。他们应规划和部署Red Hat OpenShift容器平台(OCP)、以便为部署容器工作负载打造一个成功的生产就绪环境。其OCP集群可以部署在VMware或裸机上。

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

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

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

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

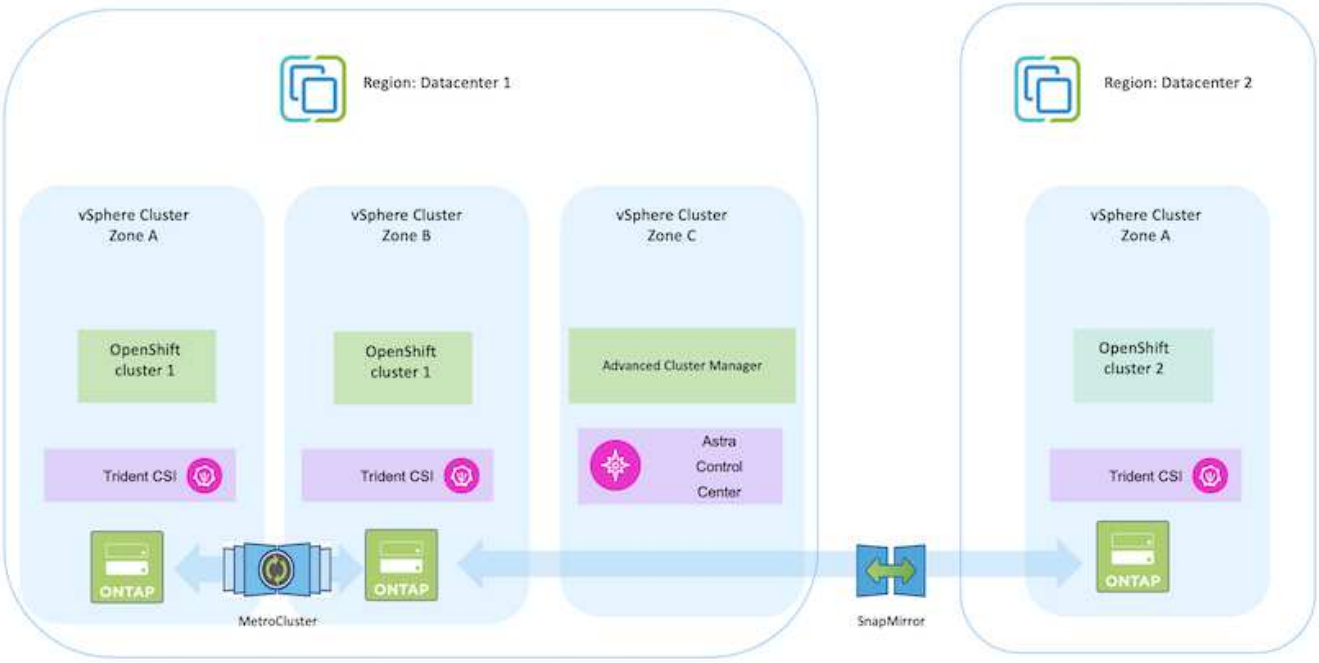


在**VMware**上部署和配置**Red Hat OpenShift**容器平台

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

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

下图展示了在数据中心内VMware上部署的集群。



设置过程可细分为以下步骤：

部署和配置**CentOS VM**

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

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

请参见的说明 "辅助部署" 部署OCP集群的方法。

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

在集线器集群上安装高级集群管理

可使用集线器集群上的高级集群管理操作员进行安装。请参阅说明 "此处"。

在集线器集群上安装内部**Red Hat Quay**注册表。

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

安装两个额外的**OCP**集群(源和目标)

- 可以使用集线器集群上的ACM部署其他集群。
- 请参阅说明 "此处"。

配置**NetApp ONTAP** 存储

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

在**OCP**集群上安装**NetApp Trident**

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

安装**NetApp Asta Control Center**

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

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

在源集群上部署应用程序

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

将源集群和目标集群添加到**Astra**控制中心。

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

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

使用**Astra**保护数据

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

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

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

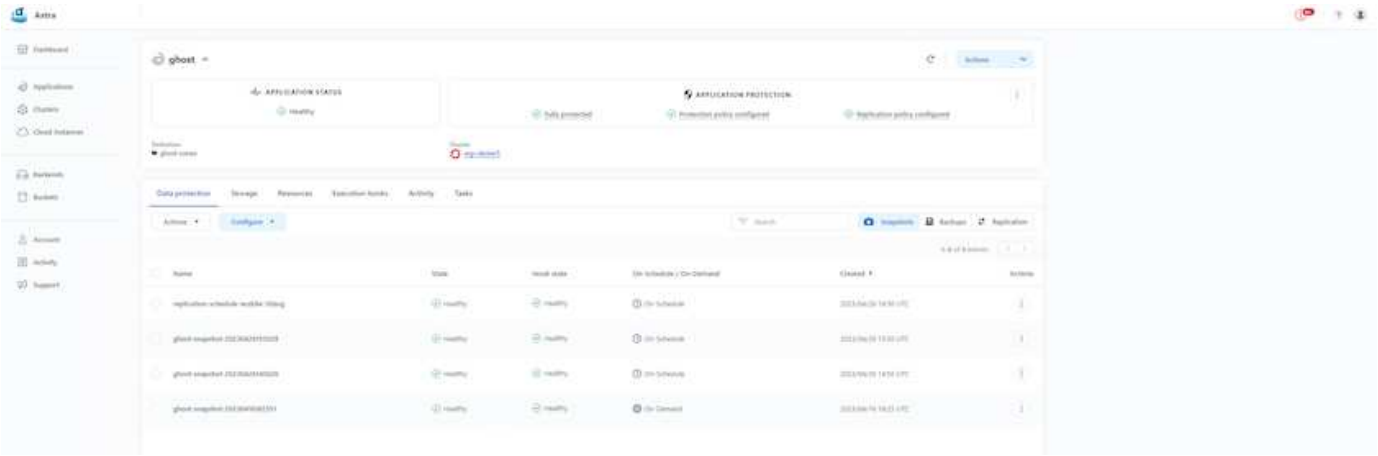
ONTAP 中的数据保护可通过临时或策略控制的方式实现-快照-备份和恢复

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

使用**ACC**创建**Snapshot**

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

使用**ACC**配置**Snapshot**

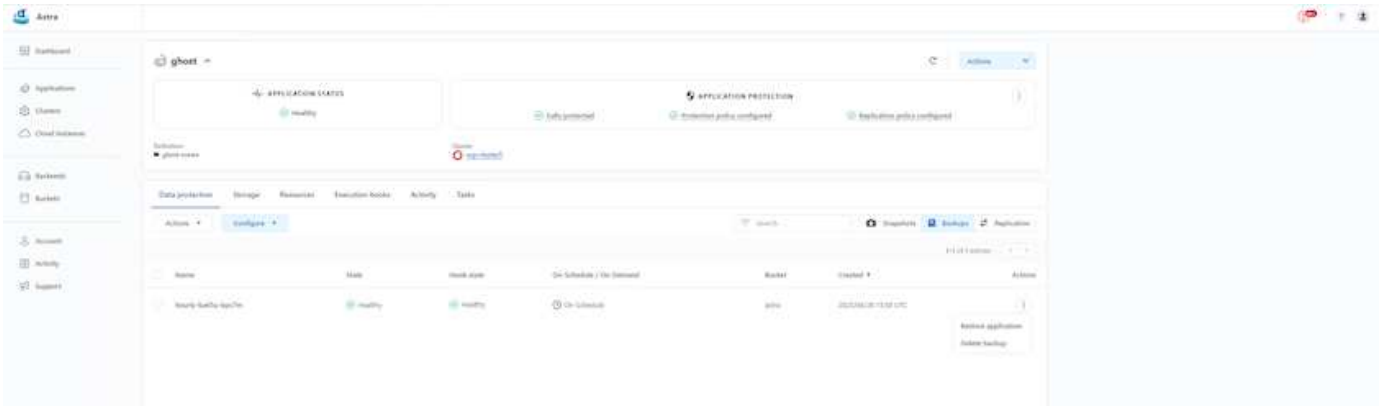


使用**ACC**进行备份和恢复

备份基于Snapshot。ACC可以使用CSI创建Snapshot副本、并使用时间点Snapshot副本执行备份。备份存储在外部对象存储中(任何兼容S3、包括位于不同位置的ONTAP S3)。可以为计划的备份和要保留的备份版本数配置保护策略。最小RPO为1小时。

使用**ACC**从备份还原应用程序

ACC从存储备份的S3存储分段还原应用程序。



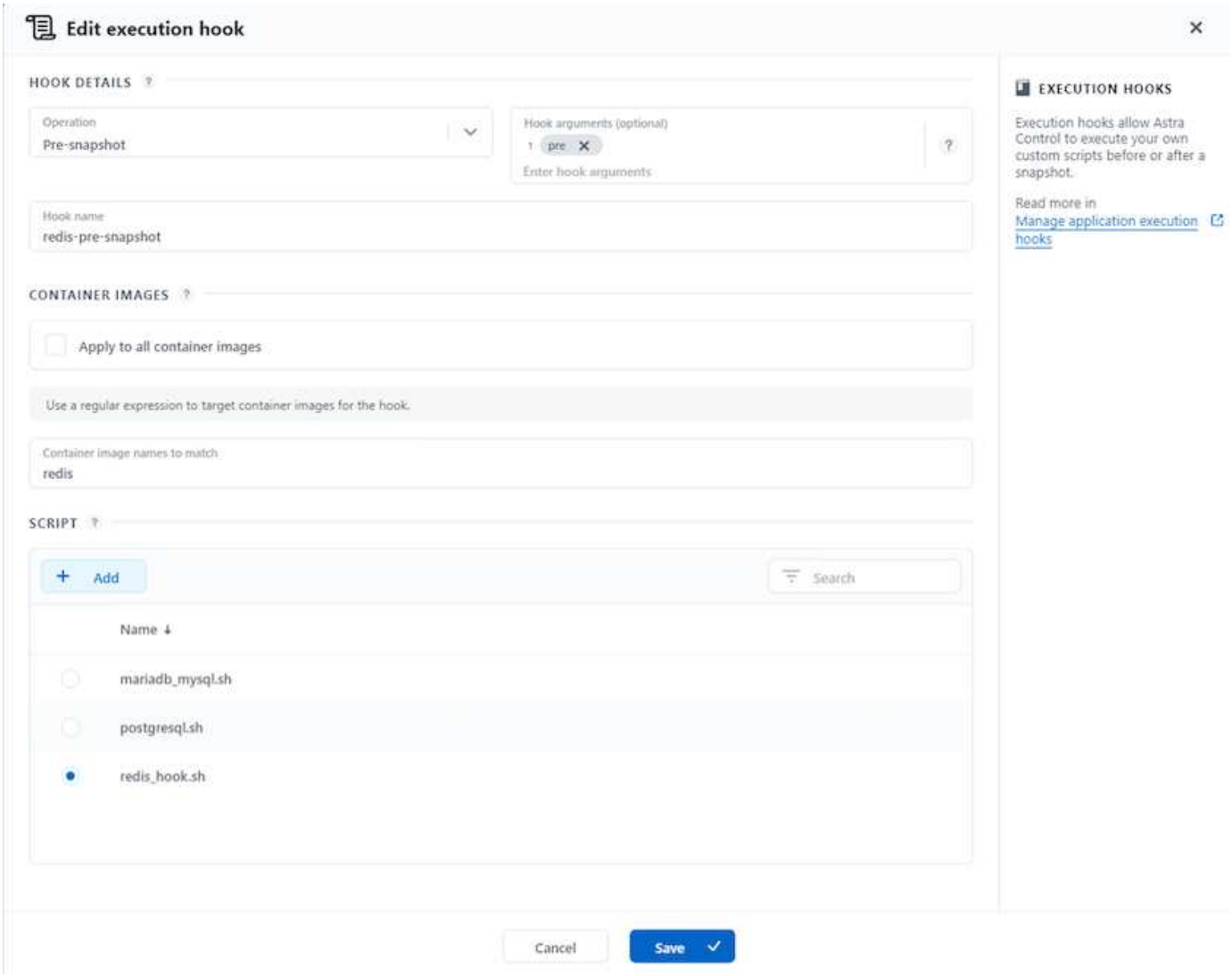
特定于应用程序的执行挂钩

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

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

"NetApp Verda GitHub项目" 为常见的云原生应用程序提供执行挂钩、使保护应用程序变得简单、强大且易于编排。如果您有足够的信息来支持存储库中没有的应用程序、请随时为该项目做出贡献。

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



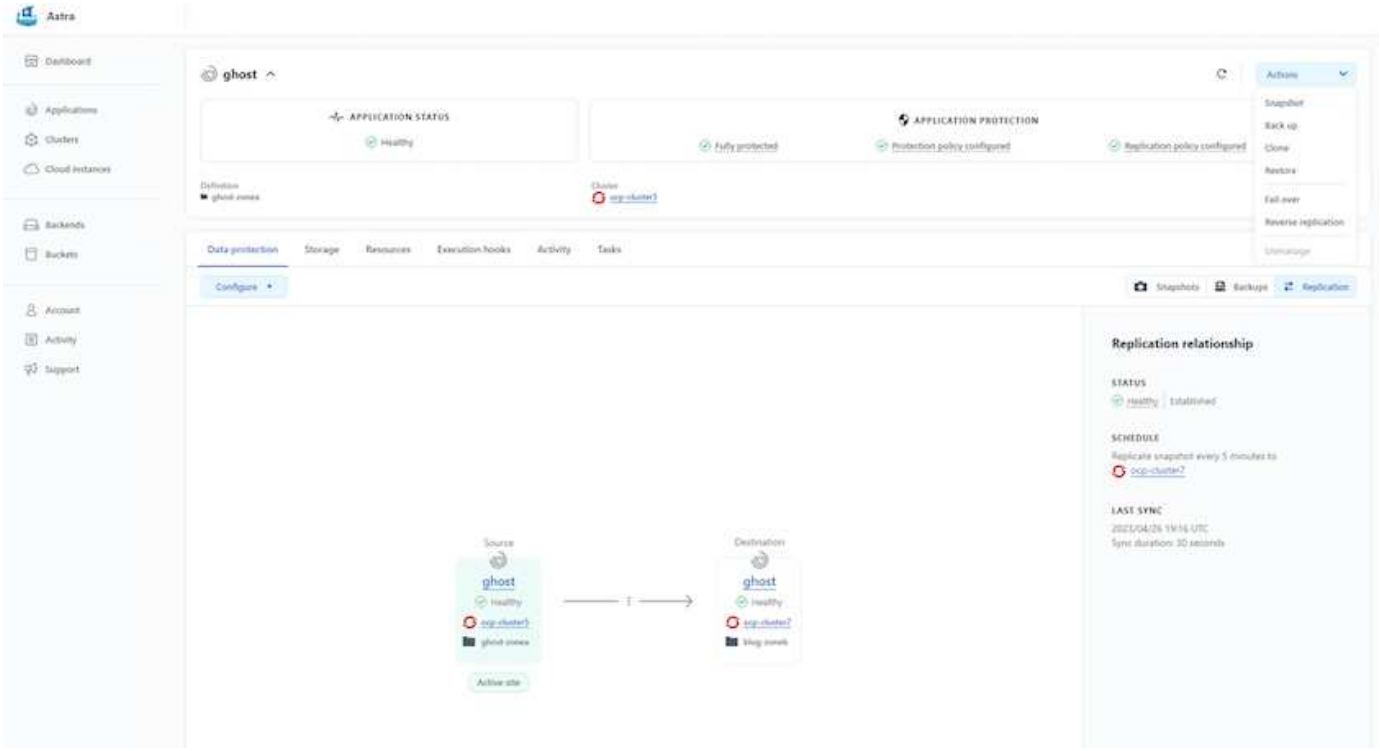
使用**ACC**复制

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

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

请参见 "此处" 有关SnapMirror设置说明、请参见。

采用**ACC**的**SnapMirror**



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

演示视频：

"使用Asta Control Center进行灾难恢复的演示视频"

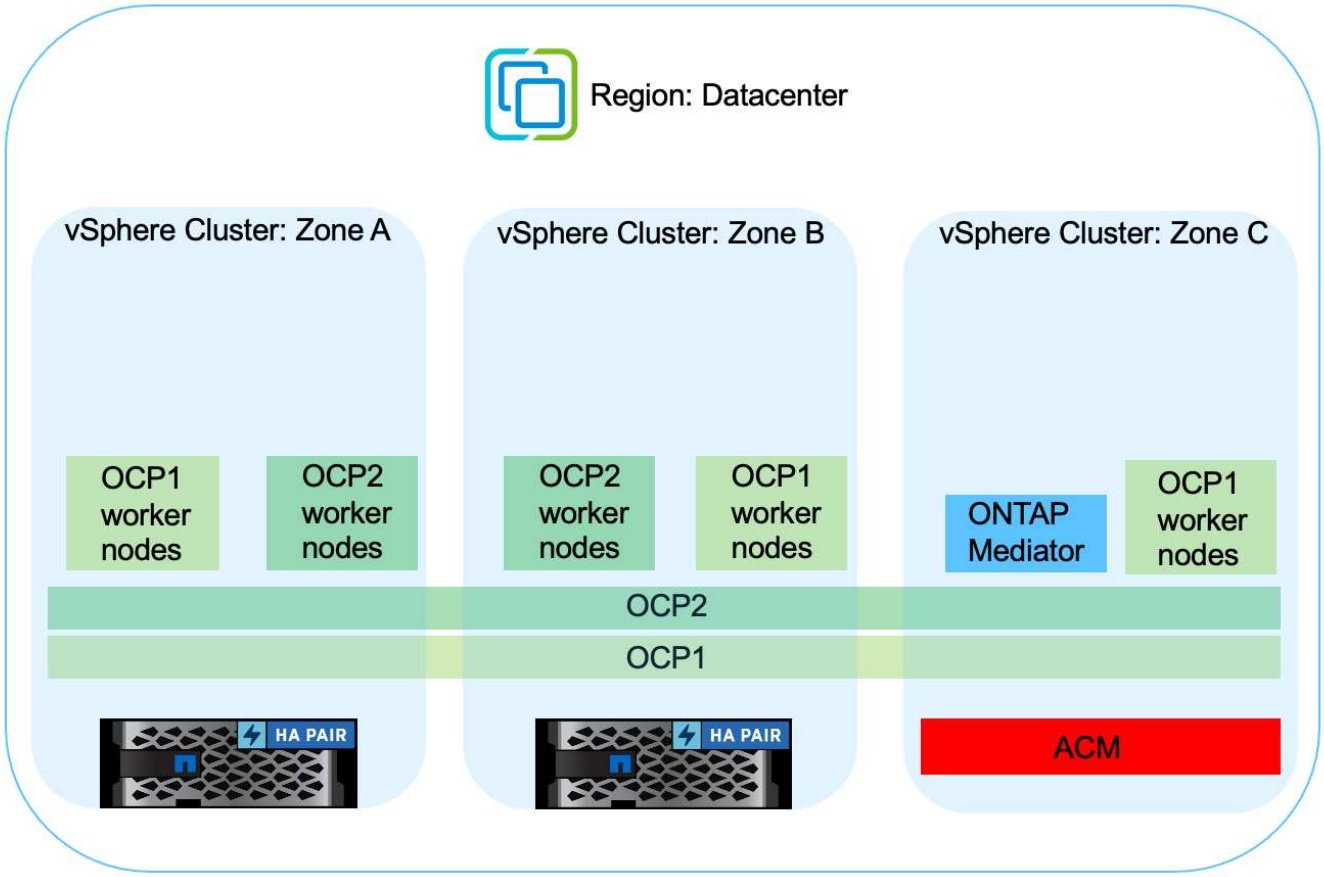
使用Astra Control Center保护数据

借助**MetroCluster** 实现业务连续性

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

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

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



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

有关Astra Control Center数据保护功能的详细信息、请参见 "此处"

使用**Astra Control Center**迁移数据

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

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

在不同的**Kubbernetes**环境之间迁移数据

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

要将应用程序从一个集群迁移到另一个集群、您可以使用ACC的以下功能之一：

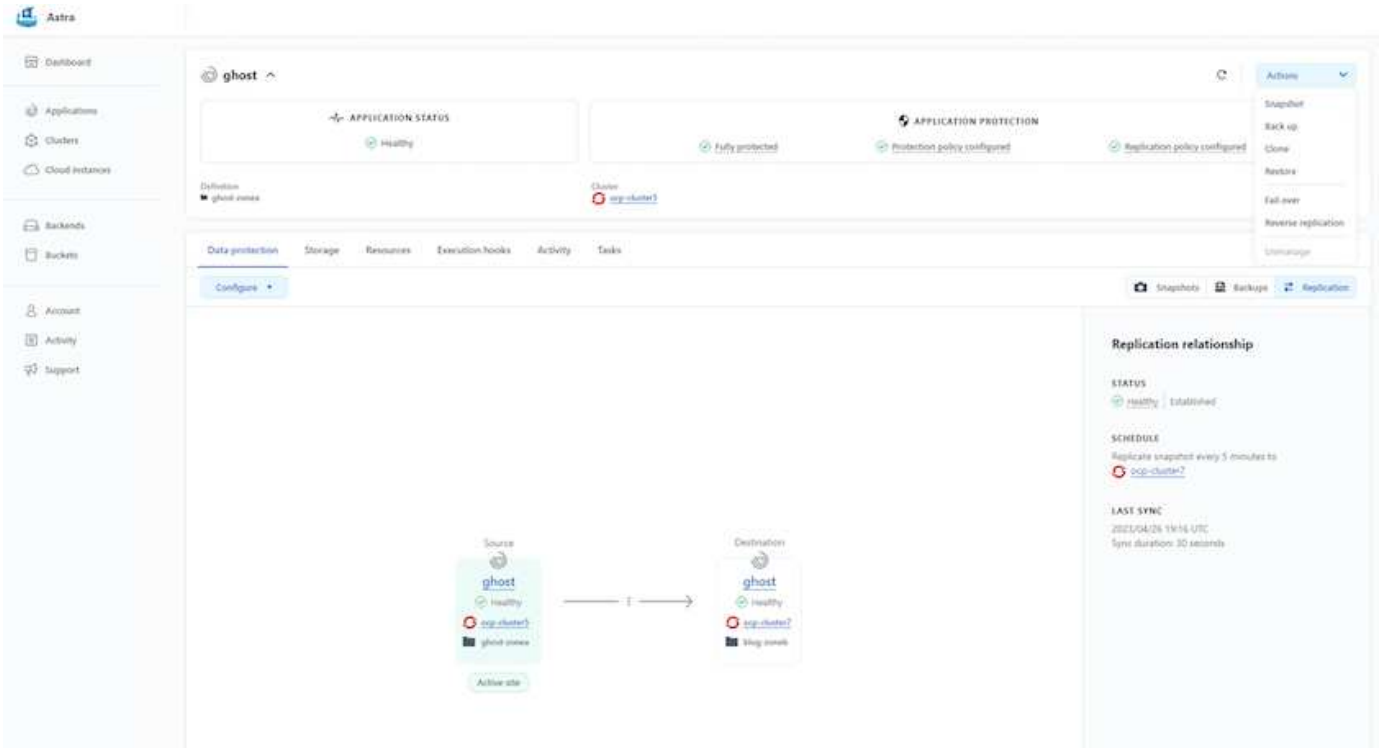
- 复制
- 备份和恢复
- 克隆

请参见 "数据保护部分" 用于复制、备份和恢复选项。

请参见 "此处" 有关克隆的更多详细信息。

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

使用**ACC**执行数据复制



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

概述

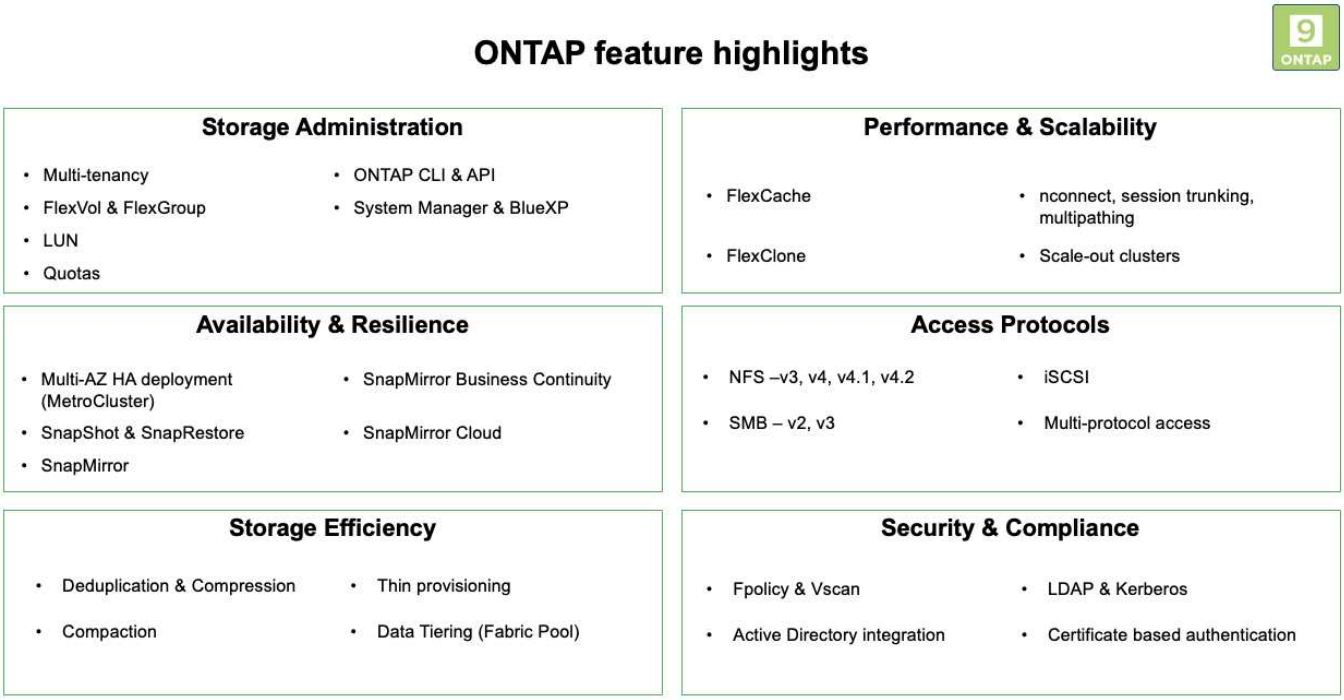
NetApp发现、越来越多的客户正在利用围绕Kubnetes构建的容器和流程编排平台来打造现代化的传统企业级应用程序以及构建新应用程序。Red Hat OpenShift容器平台就是我们看到许多客户采用的一个示例。

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

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

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

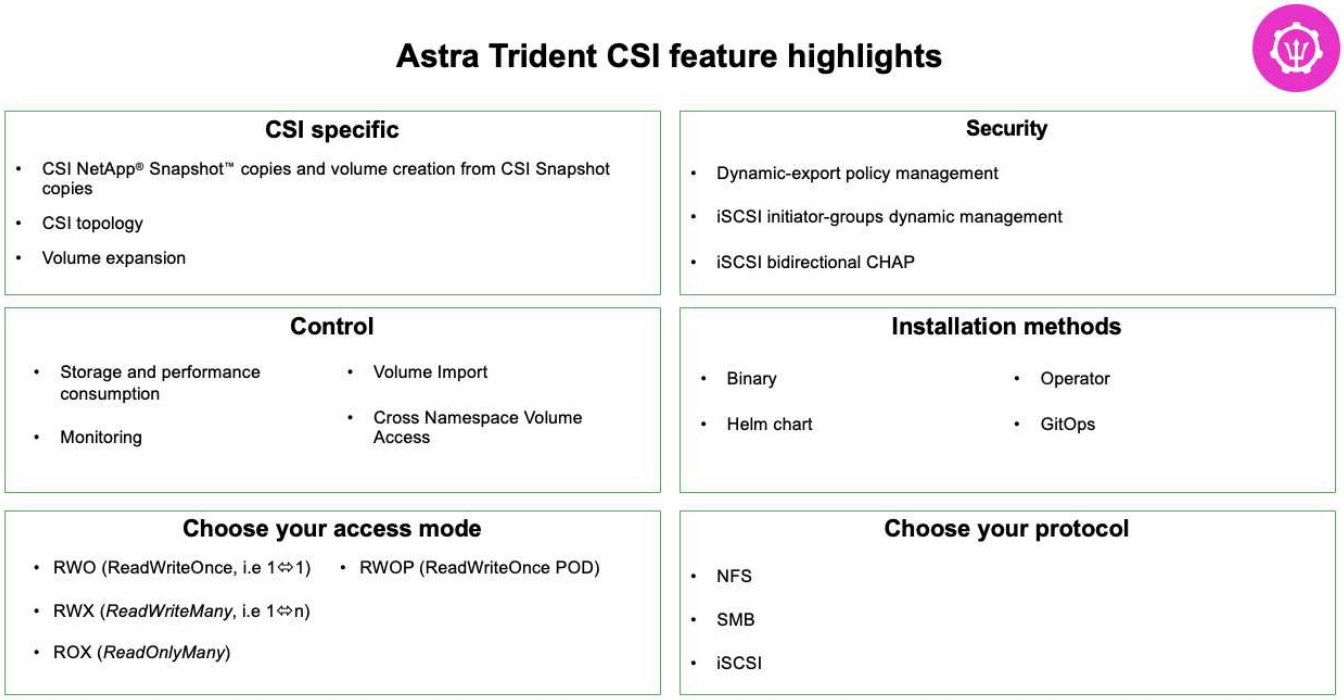
- 云中由提供商管理的存储：
  - Cloud Volumes Service for Google Cloud (CVS)、Azure NetApp Files (ANF)、Amazon FSx for NetApp ONTAP 可在超云中提供完全托管的存储



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

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

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



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

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

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

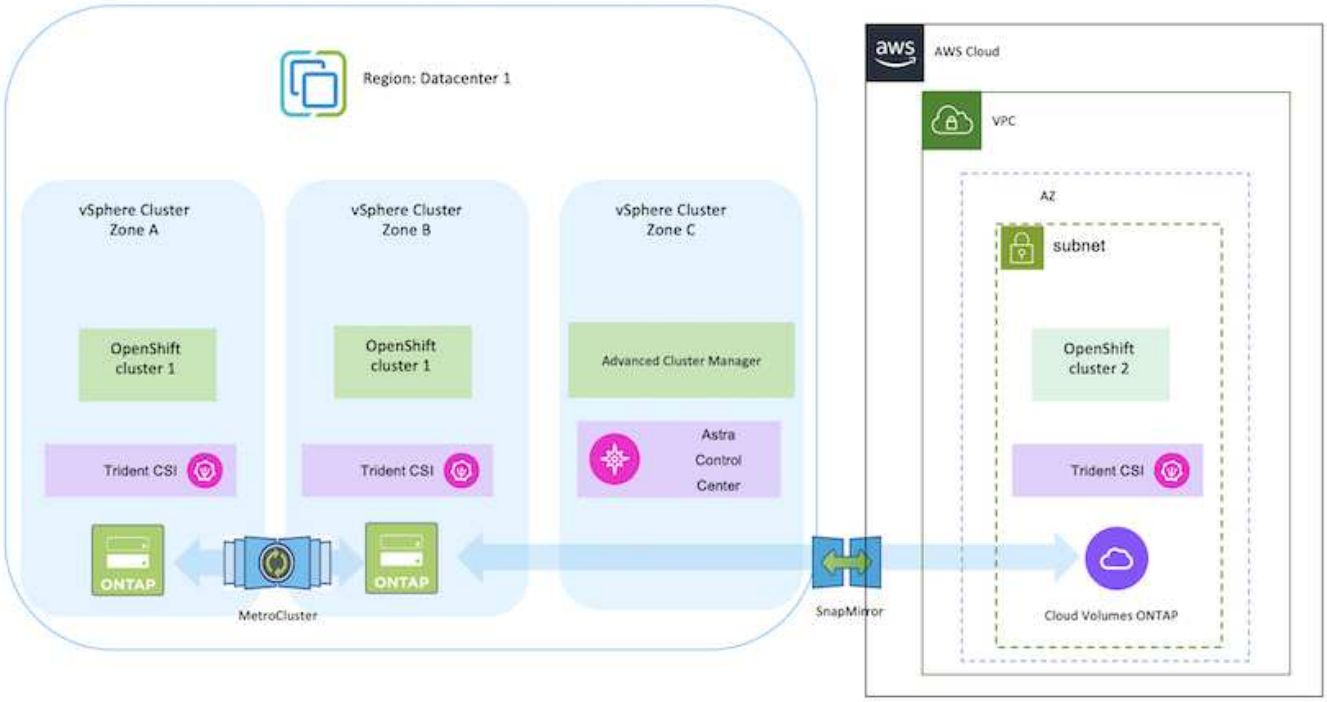
本参考文档使用NetApp Asta Control Center验证了在RedHat OpenShift容器平台上部署的基于容器的应用程序的迁移和保护。此外、解决方案 还提供了有关部署和使用Red Hat高级集群管理(ACM)来管理容器平台的详细信息。本文档还重点介绍了使用Asta Trident CSI配置程序将NetApp存储与Red Hat OpenShift容器平台集成的详细信息。Astra Control Center部署在集线器集群上、用于管理容器应用程序及其永久性存储生命周期。最后、它还提供了一个解决方案 、用于在AWS (ROSA)中使用Amazon FSx for NetApp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

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

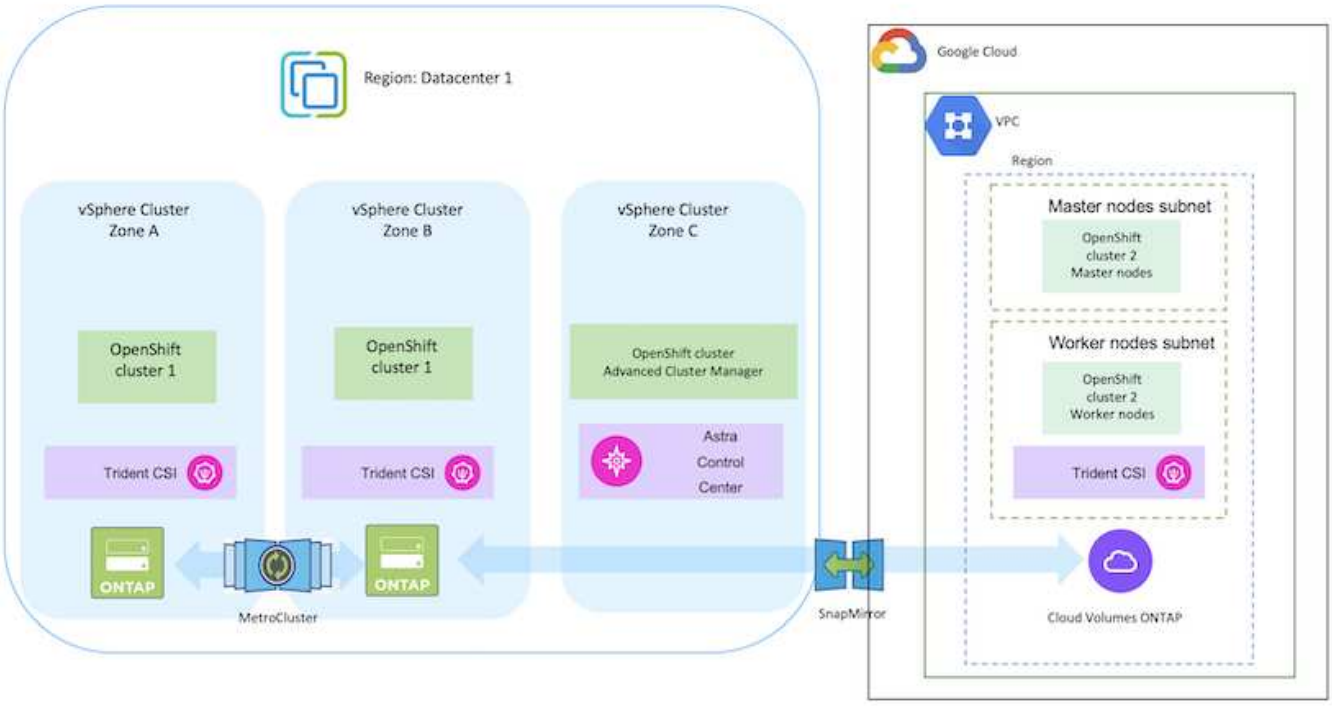
当客户准备将部分选定工作负载或所有工作负载从其数据中心迁移到云时、他们可能正处于现代化之旅的一个阶段。出于各种原因、他们可能会选择在云中使用自行管理的OpenShift容器和自行管理的NetApp存储。他们应在云中规划和部署Red Hat OpenShift容器平台(OCP)、以便打造一个成功的生产就绪环境、从而从数据中心迁移容器工作负载。他们的OCP集群可以部署在数据中心的VMware或裸机上、也可以部署在云环境中的AWS、Azure或Google Cloud上。

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

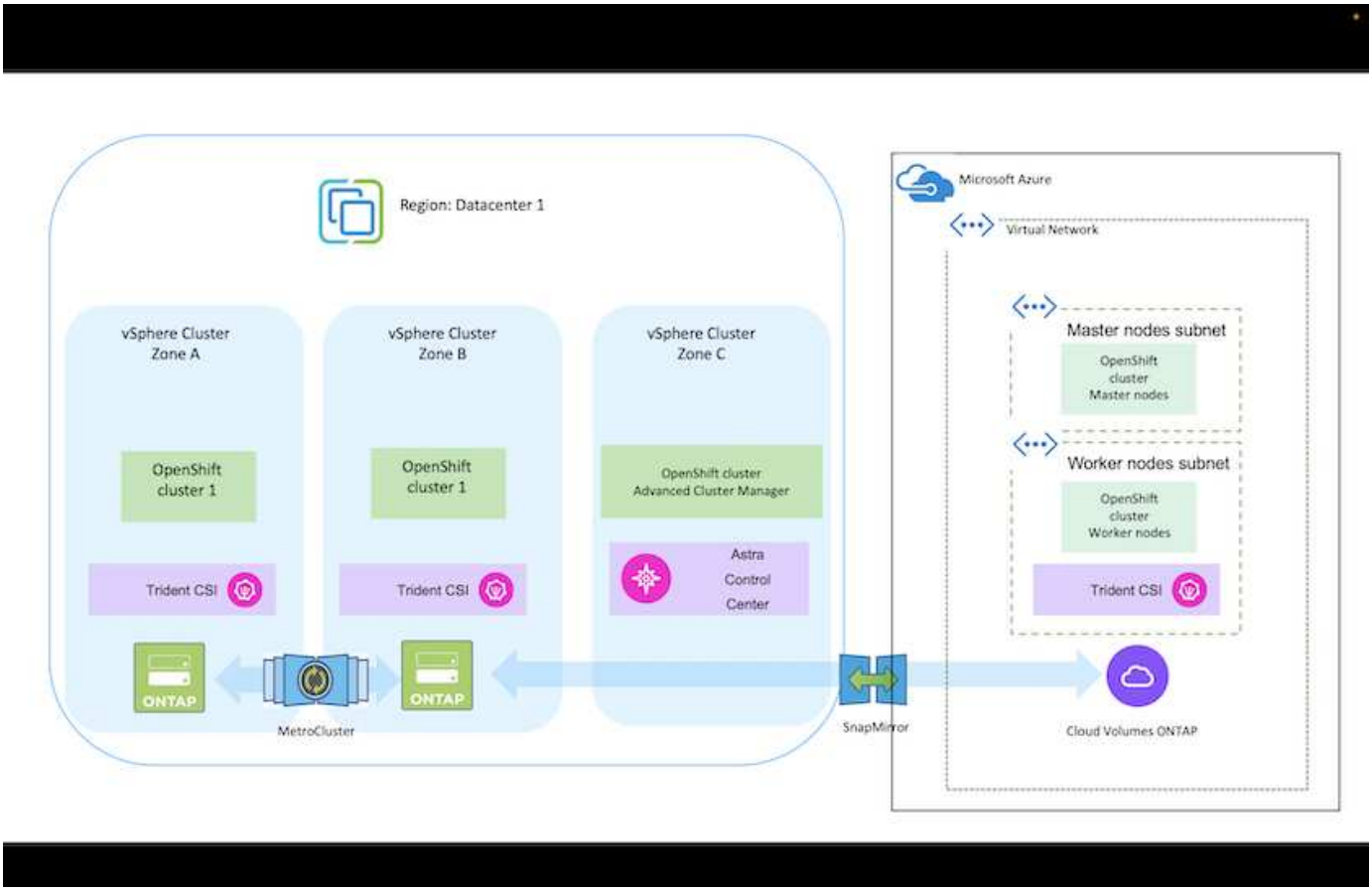
内部部署和AWS



内部部署和Google Cloud



内部部署和Azure Cloud

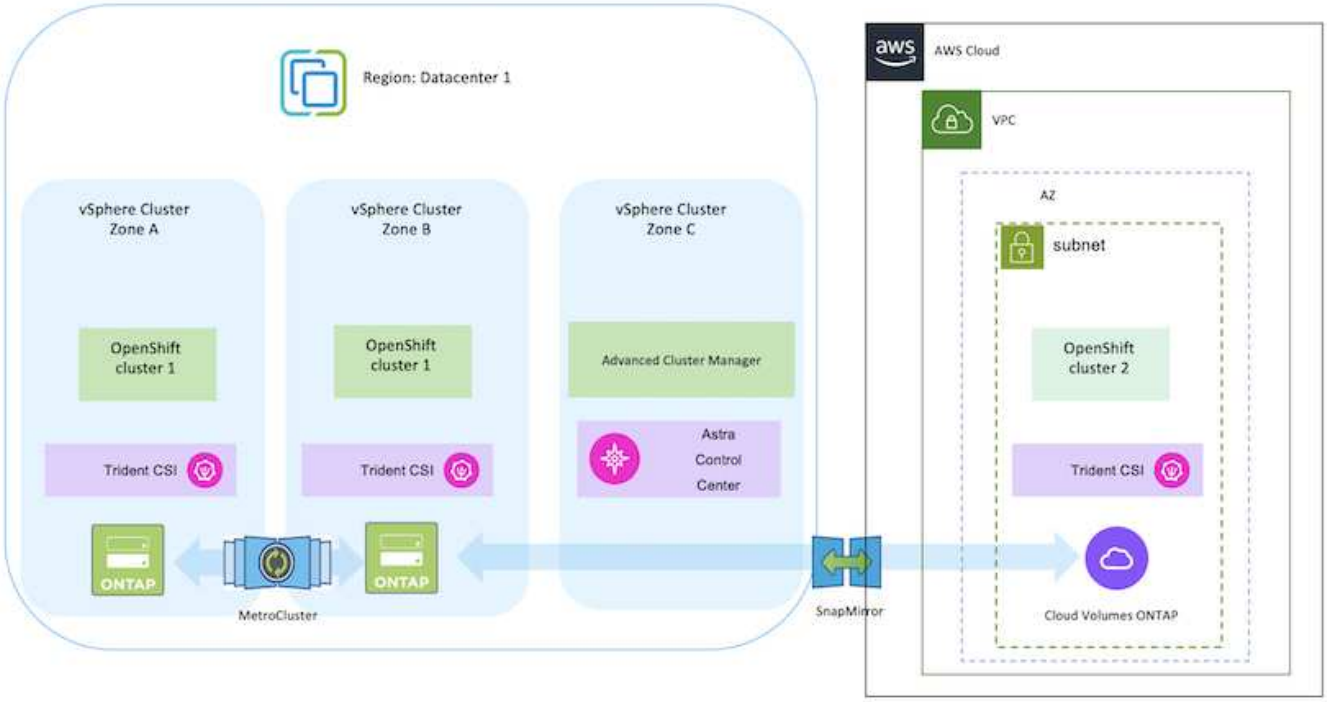


在**AWS**上部署和配置**Red Hat OpenShift**容器平台

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

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

下图展示了在AWS上部署并使用VPN连接到数据中心的集群。



设置过程可细分为以下步骤：

通过高级集群管理在**AWS**上安装**OCP**集群。

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

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

您也可以从OpenShift混合云控制台在AWS中创建集群。请参见 "此处" 有关说明，请参见。

使用ACM创建集群时、您可以在表单视图中填写详细信息后编辑YAML文件、从而自定义安装。创建集群后、您可以通过ssh登录到集群节点、以便进行故障排除或其他手动配置。使用您在安装期间提供的ssh密钥和username core进行登录。

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

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

该连接器也可以安装在云环境中。请参见 "此处" 适用于追加信息 。

在**OCP**集群中安装**Asta Trident**

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

将**AWS**上的**OCP**集群添加到**Asta Control Center**。

将AWS中的OCP集群添加到Astra Control Center。

对多区域架构使用三元数据的**CSI**拓扑功能

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

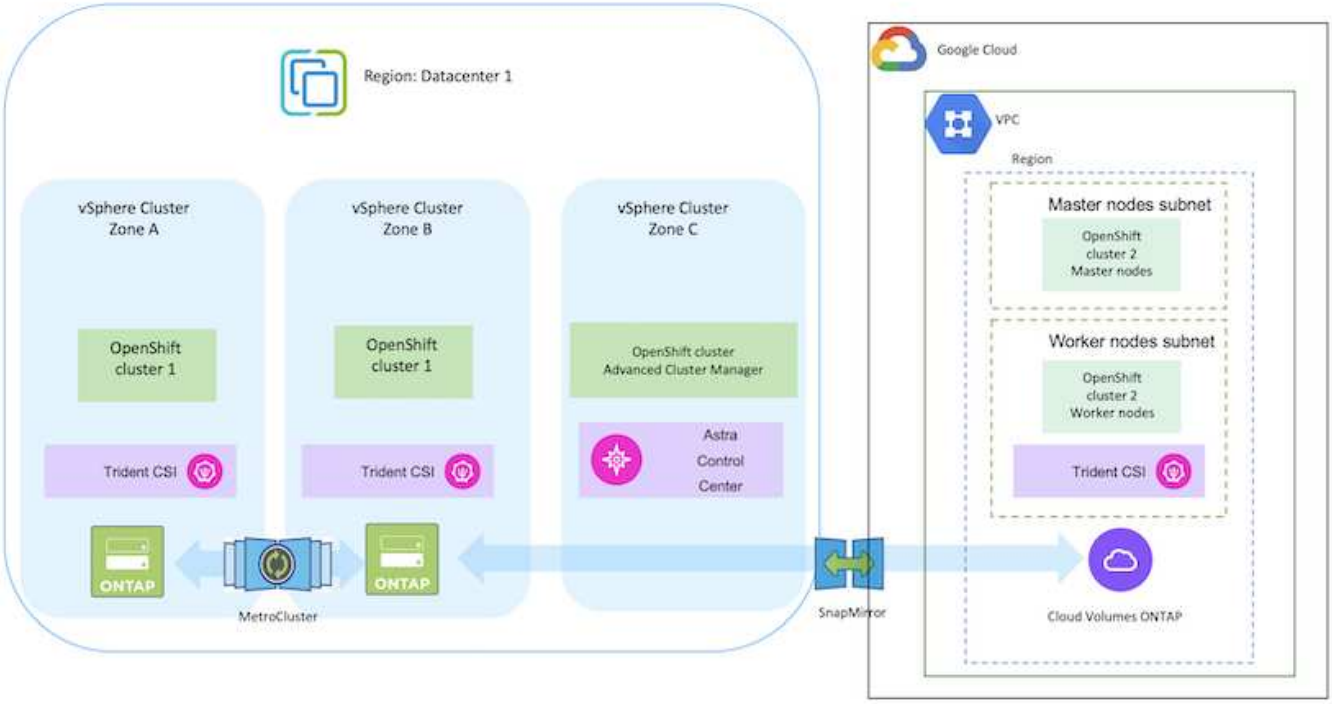
Kubarnetes支持两种卷绑定模式：-将***VolumeBindingMode***_设置为_***Immediate***(默认)时、Asta Trident会在没有任何拓扑感知功能的情况下创建卷。创建永久性卷时，不会依赖于请求的 Pod 的计划要求。-当***VolumeBindingMode***_设置为_***WaitForFirstConsumer***时，为PVC创建和绑定永久性卷的操作会延迟，直到计划和创建使用PVC的Pod为止。这样，卷就会根据拓扑要求强制实施的计划限制来创建。Astra三叉设计存储后端可以根据可用性区域选择性地配置卷(拓扑感知型后端)。对于使用此后端的 StorageClasses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

在**GCP**上部署和配置**Red Hat OpenShift**容器平台

在**GCP**上部署和配置**Red Hat OpenShift**容器平台

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

下图显示了部署在GCP上并使用VPN连接到数据中心的集群。



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

设置过程可细分为以下步骤：

使用命令行界面在**GCP**上安装**OCP**集群。

- 确保您已满足上述所有前提条件 "此处"。
- 对于内部和GCP之间的VPN连接、我们会创建并配置一个pfSense VM。有关说明，请参见 "此处"。
  - 只有在Google Cloud Platform中创建VPN网关后、才能在pfSense中配置远程网关地址。
  - 只有在OpenShift集群安装程序运行并为集群创建基础架构组件之后、才能配置阶段2的远程网络IP地址。
  - 只有在安装程序为集群创建基础架构组件后、才能在Google Cloud中配置VPN。
- 现在、在GCP上安装OpenShift集群。
  - 获取安装程序和拉取密钥、然后按照文档中提供的步骤部署集群 "此处"。
  - 此安装将在Google Cloud Platform中创建VPC网络。它还会在云DNS中创建一个私有区域并添加A记录。
    - 使用VPC网络的CIDR块地址配置pfSense并建立VPN连接。确保防火墙设置正确。
    - 使用Google Cloud DNS的A记录中的IP地址在内部环境的DNS中添加A记录。
  - 集群安装完成、并将提供一个kubeconfigfile文件以及用户名和密码以登录到集群的控制台。

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

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

在**GCP**的**OCP**集群中安装**Asta Trdent**

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

将**GCP**上的**OCP**集群添加到**Asta Control Center**。

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

对多区域架构使用三元数据的**CSI**拓扑功能

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

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

演示视频

在Google Cloud Platform上安装OpenShift集群

将OpenShift集群导入Astra Control Center

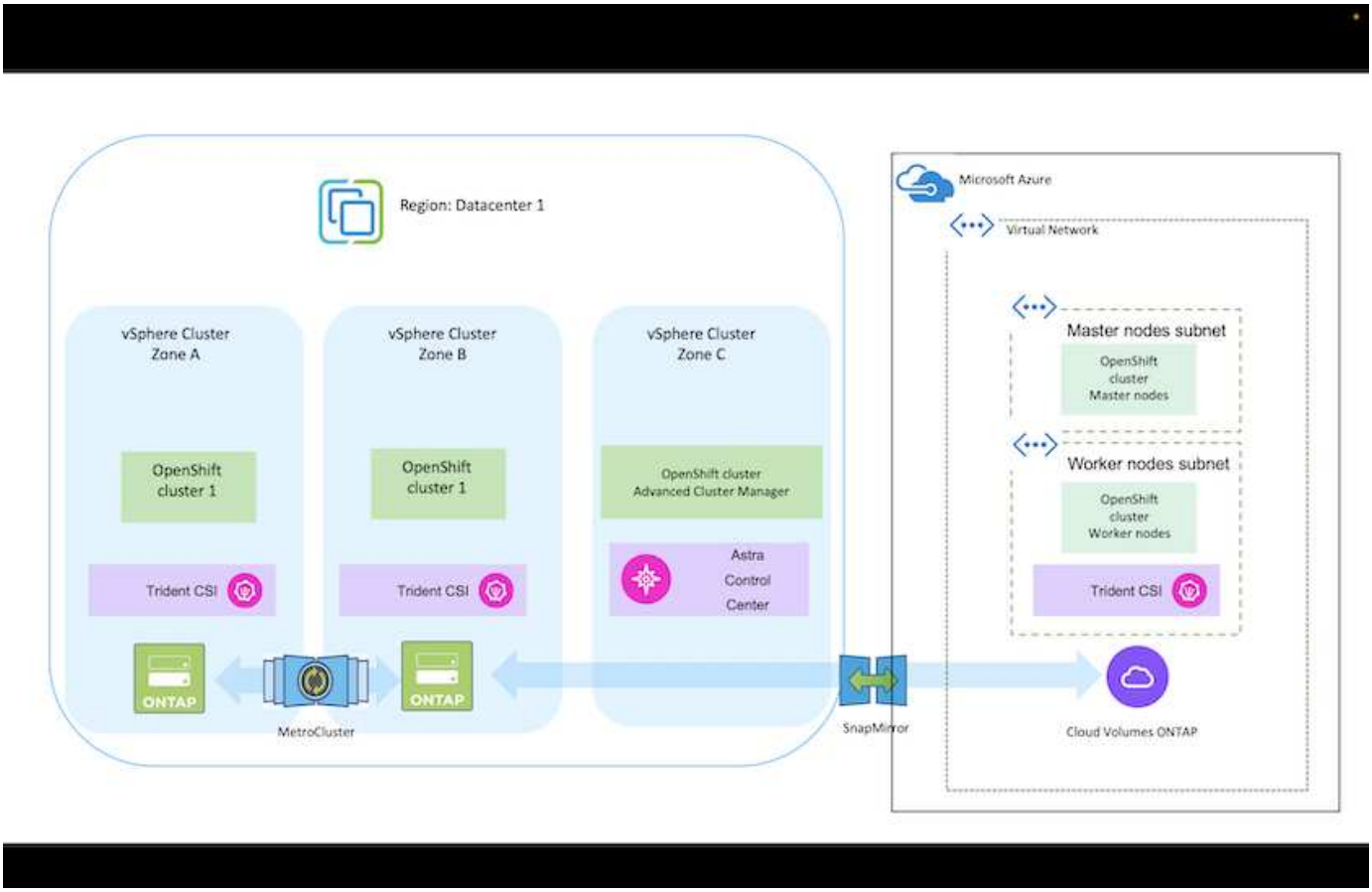
在**Azure**上部署和配置**Red Hat OpenShift**容器平台

在**Azure**上部署和配置**Red Hat OpenShift**容器平台

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

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

下图显示了部署在Azure上并使用VPN连接到数据中心的集群。



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

设置过程可细分为以下步骤：

使用命令行界面在**Azure**上安装**OCP**集群。

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

下面提供了一个示例install-config.yaml文件。

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
metadata:
  creationTimestamp: null
```

```
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

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

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

在**Azure**的**OCP**集群中安装**A**作用 力控制配置程序

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

将**Azure**上的**OCP**集群添加到**Asta**控制中心。

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

对多区域架构使用三元数据的**CSI**拓扑功能

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

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

演示视频

使用Asta Control对应用程序进行故障转移和故障恢复

使用**Astra Control Center**保护数据

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

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

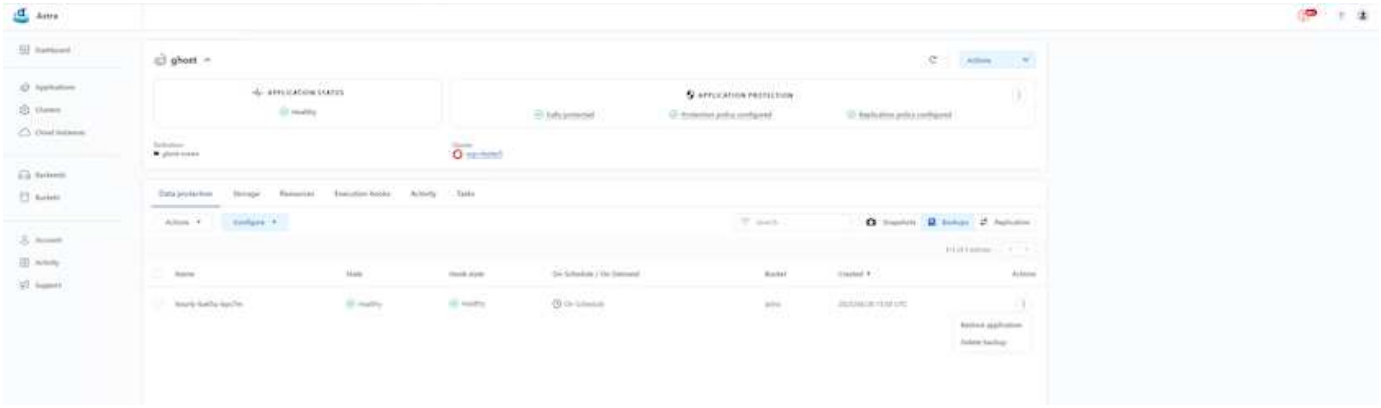
数据保护的要求各不相同、从还原到时间点副本、到自动故障转移到其他故障域、无需任何人为干预。许多客户选择ONTAP 作为其Kubernetes应用程序的首选存储平台、因为它具有丰富的功能、例如多租户、多协议、高性能和高容量产品、适用于多站点位置的复制和缓存、以及安全性和灵活性。

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

使用**ACC**进行备份和恢复

应用程序所有者可以查看和更新ACC发现的应用程序。ACC可以使用CSI创建Snapshot副本、并使用时间点Snapshot副本执行备份。备份目标可以是云环境中的对象存储。可以为计划的备份和要保留的备份版本数配置保护策略。最小RPO为1小时。

使用**ACC**从备份还原应用程序

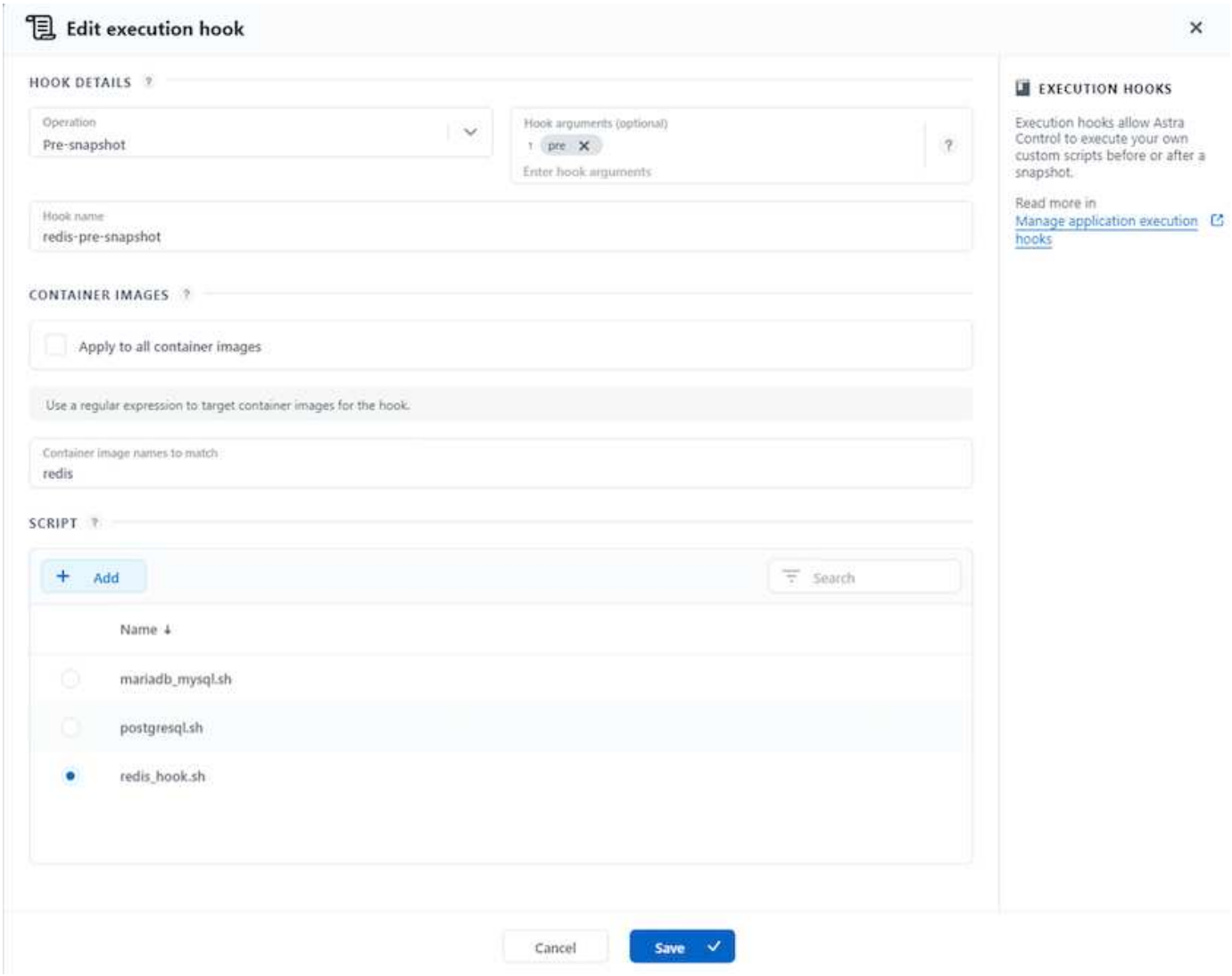


特定于应用程序的执行挂钩

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

NetApp的 "开源项目Verda" 为常见的云原生应用程序提供执行挂钩、使保护应用程序变得简单、强大且易于编排。如果您有足够的信息来支持存储库中没有的应用程序、请随时为该项目做出贡献。

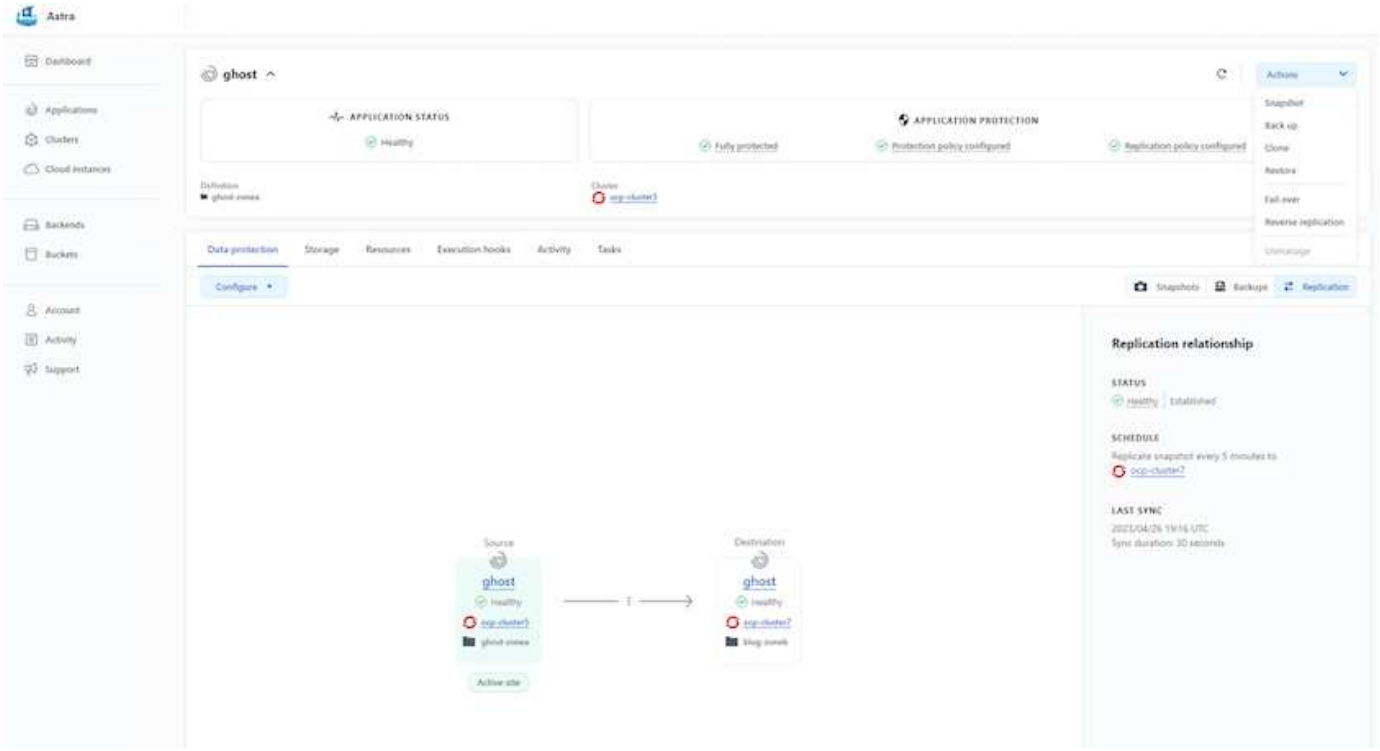
为**Redis**应用程序创建**Snapshot**前创建副本的示例执行挂钩。



使用**ACC**复制

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

采用**ACC**的**SnapMirror**



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

演示视频：

"使用Asta Control Center进行灾难恢复的演示视频"

使用Astra Control Center保护数据

有关Astra Control Center数据保护功能的详细信息、请参见 "此处"

使用**ACC**进行灾难恢复(使用复制进行故障转移和故障恢复)

使用Asta Control对应用程序进行故障转移和故障恢复

使用**Astra Control Center**迁移数据

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

数据迁移

要将应用程序从一个环境迁移到另一个环境、您可以使用ACC的以下功能之一：

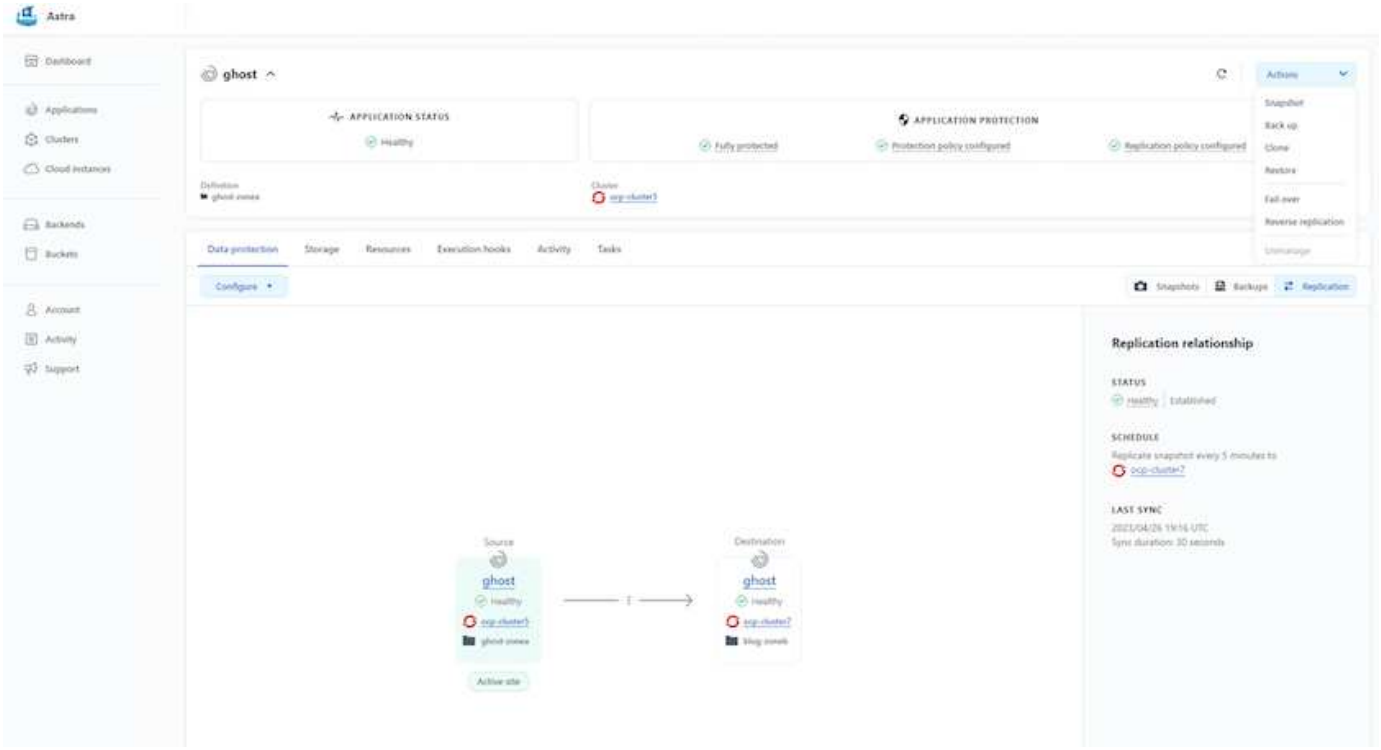
- 复制
- 备份和恢复
- 克隆

请参见 "数据保护部分" 用于复制、备份和恢复选项。

请参见 "此处" 有关克隆的更多详细信息。

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

使用**ACC**执行数据复制



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

概述

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

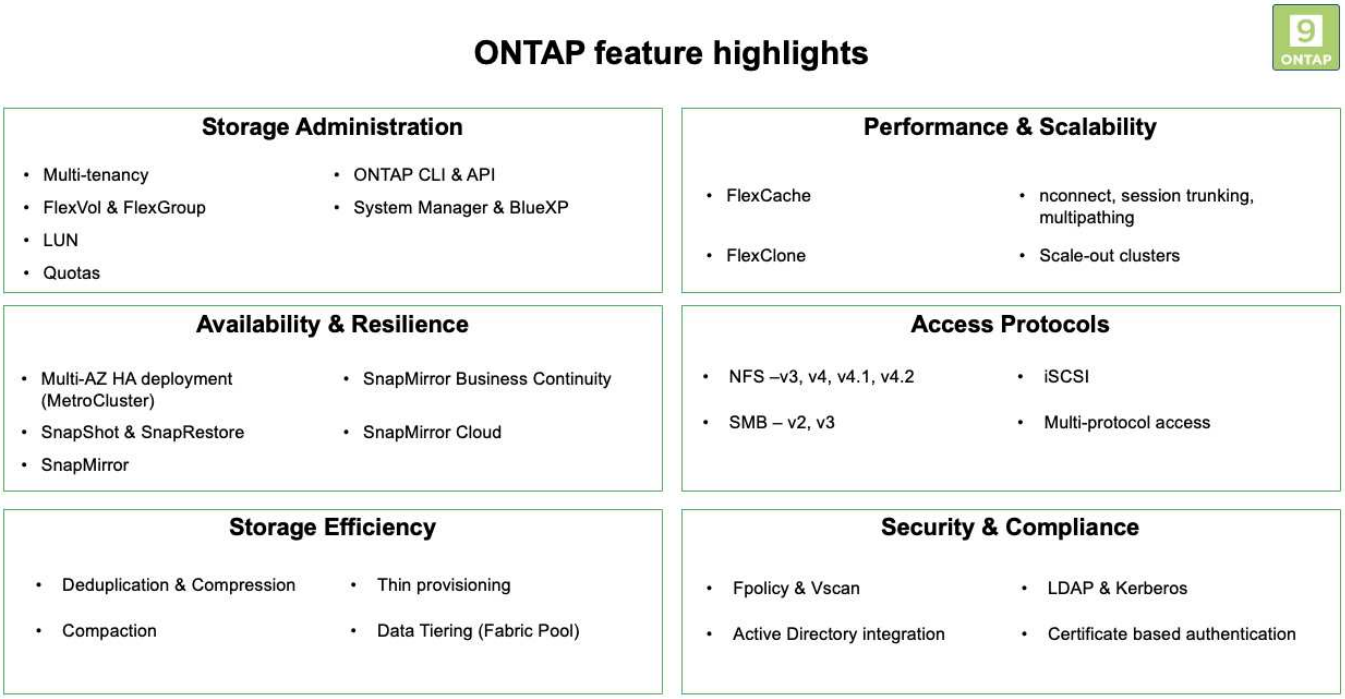
随着越来越多的客户开始在企业中采用容器、NetApp已做好充分准备、可以满足有状态应用程序的持久存储需求以及数据保护、数据安全和数据迁移等传统数据管理需求。但是、可以使用不同的策略、工具和方法来满足这些需求。

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

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

- NetApp Cloud Volumes ONTAP (CVO)可在超大容量云中提供自行管理的存储

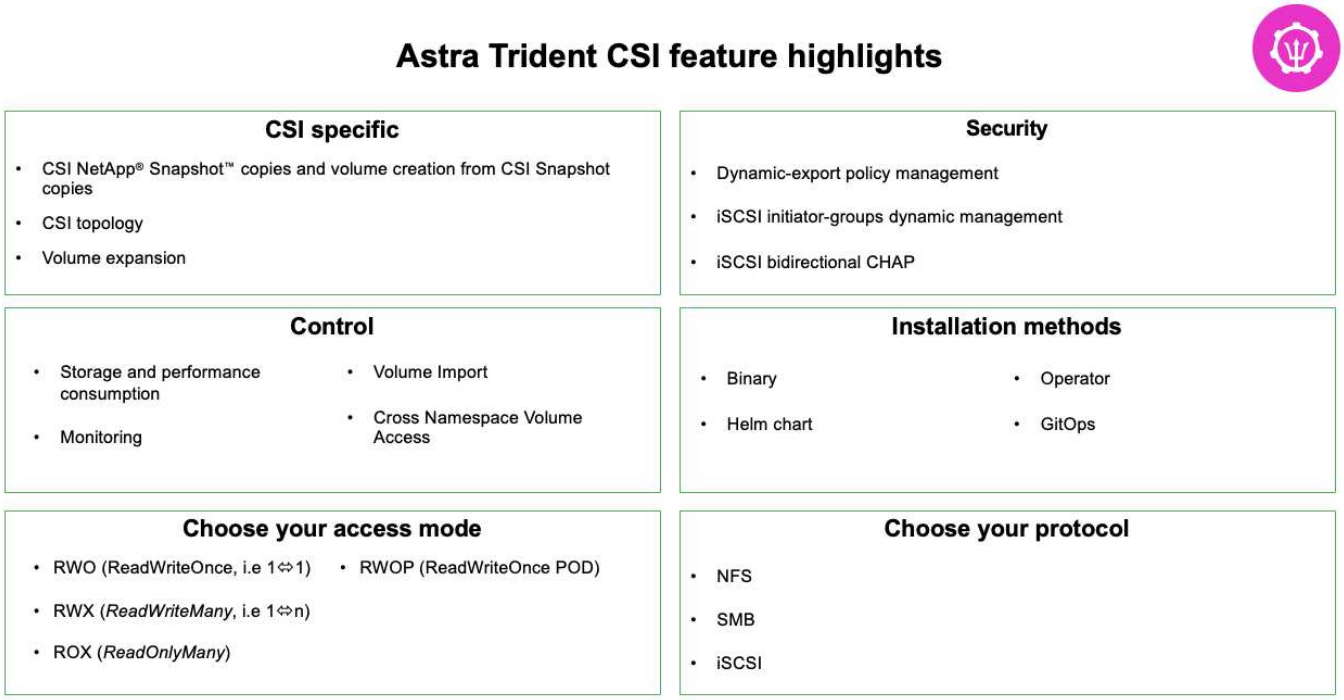
- 云中由提供商管理的存储：
  - Cloud Volumes Service for Google Cloud (CVS)、Azure NetApp Files (ANF)、Amazon FSx for NetApp ONTAP 可在超云中提供完全托管的存储



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

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

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



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

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

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

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

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

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

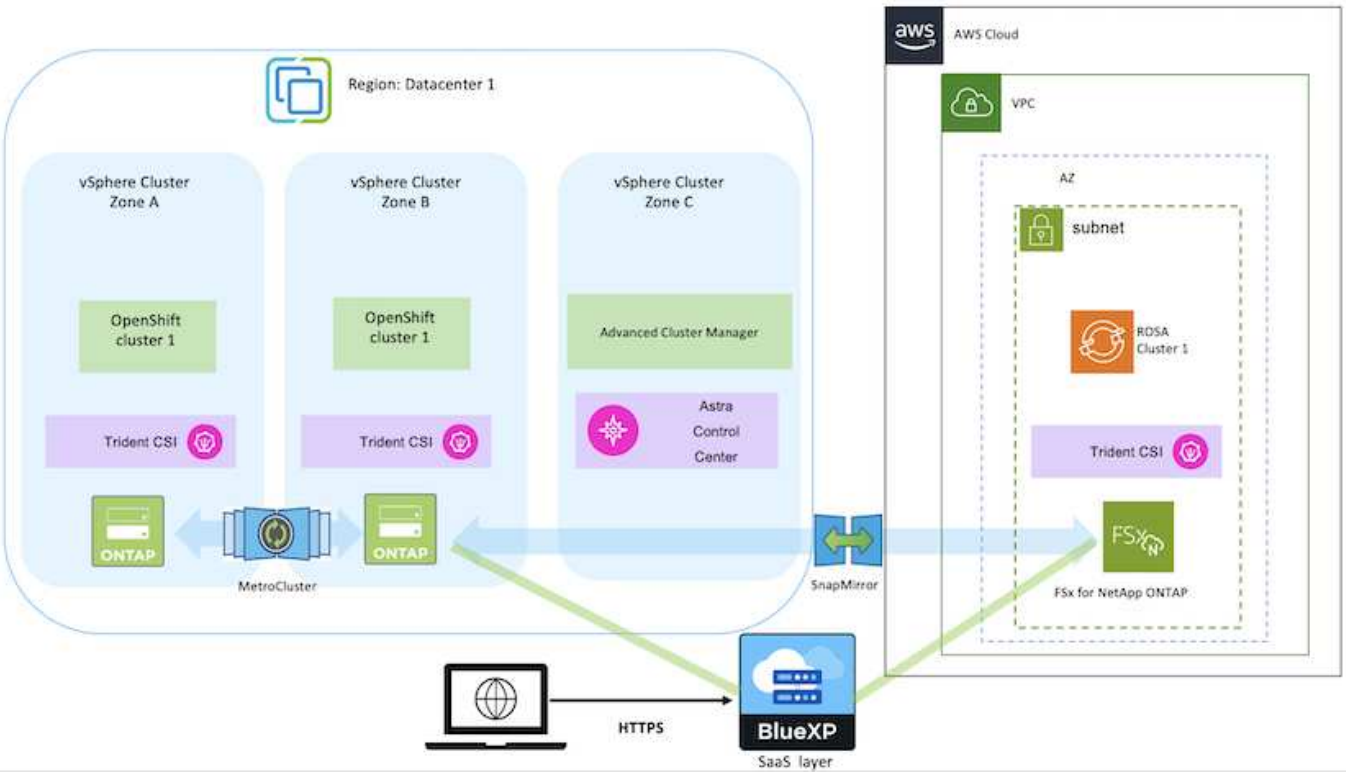
客户可能"生于云"、也可能正处于现代化之旅的某一时刻、准备将部分选定工作负载或所有工作负载从数据中心迁移到云。他们可以选择在云中使用提供商管理的OpenShift容器和提供商管理的NetApp存储来运行工作负载。他们应该在云中规划和部署托管Red Hat OpenShift容器集群(ROSA)、以便为其容器工作负载提供一个成功的生产就绪环境。在AWS云中、他们还可以部署FSx for NetApp ONTAP 来满足存储需求。

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

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

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

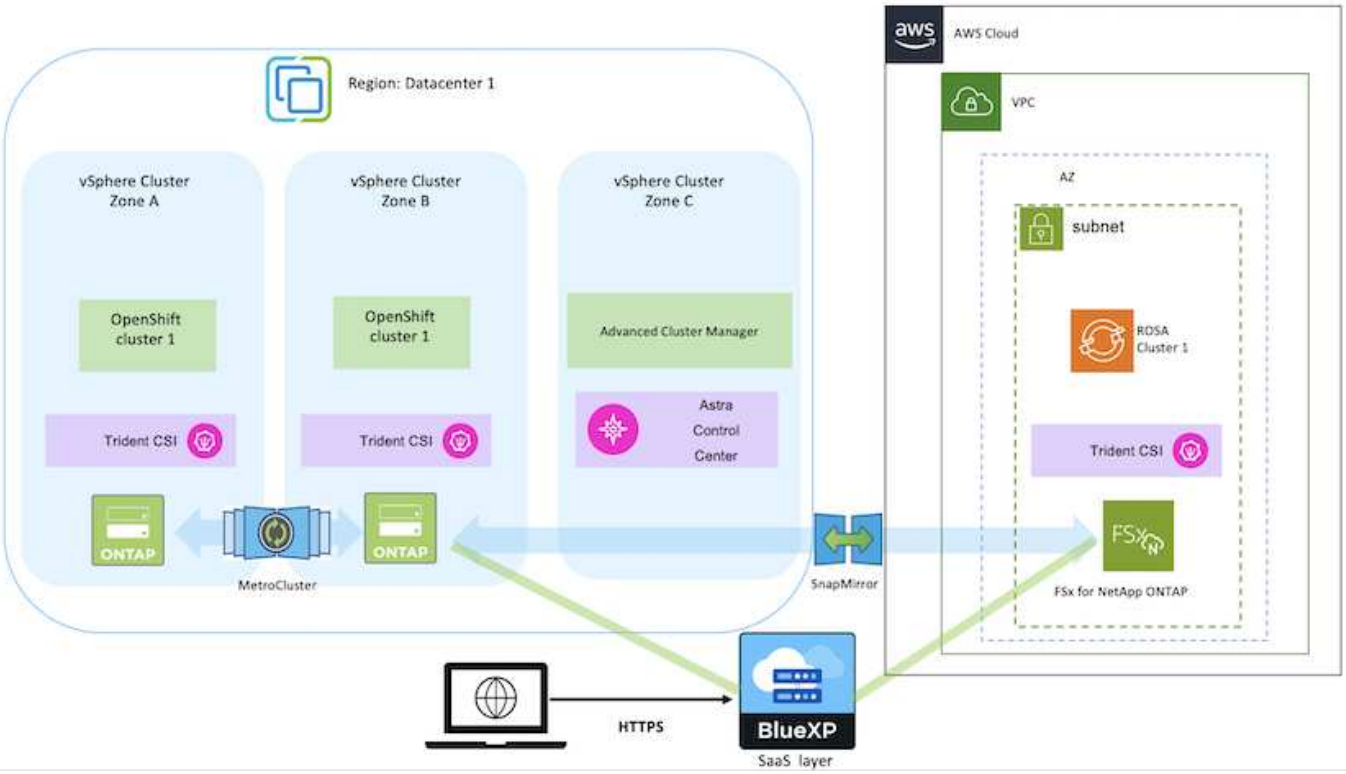
适用于**OpenShift**容器工作负载的数据保护和迁移解决方案



在**AWS**上部署和配置托管**Red Hat OpenShift**容器平台

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

下图展示了在AWS上部署并使用FSxN作为后端存储的ROSA集群。



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

设置过程可细分为以下步骤：

安装**ROSA**集群

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

安装**FSxN**

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

在**ROSA**集群上安装**TRIDent (**使用**Helm**图表)

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

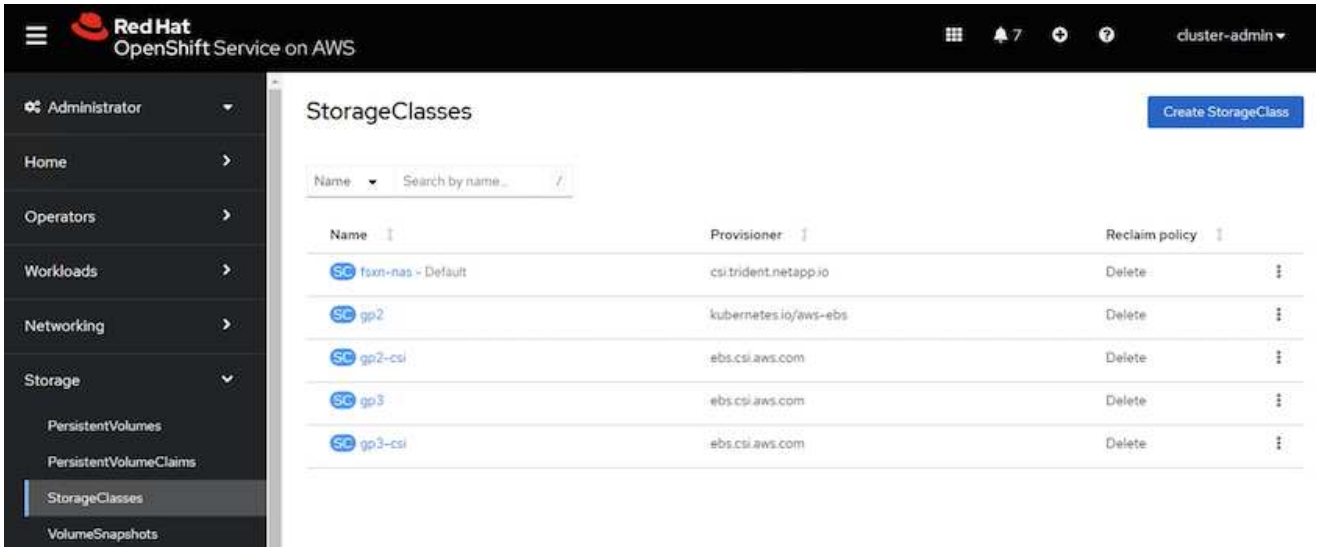
将FSxN与适用于ROSA集群的Asta Trident集成

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

```yaml
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**TRIDIent**创建后端和存储类(适用于**FSxN)**

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



使用**OpenShift GitOps**部署应用程序**(Argo CD)**

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

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

Helm参数：globL.storageClass：fsxn-nas

数据保护

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

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

本节详细介绍了使用ACS的以下数据保护选项：

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

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

备份/从备份中还原

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

FSx NetApp ONTAP for Red Hat OpenShift Service on AWS

快照/从快照还原

以下视频显示了如何创建ROSA应用程序的快照以及之后如何从快照中还原。

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

博客

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

创建快照并从中还原的分步详细信息

前提条件设置

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

后续步骤

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

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

1.创建管理员用户并登录到群集

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

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

此命令将提供如下输出。使用登录到集群 `oc login` 命令。

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

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

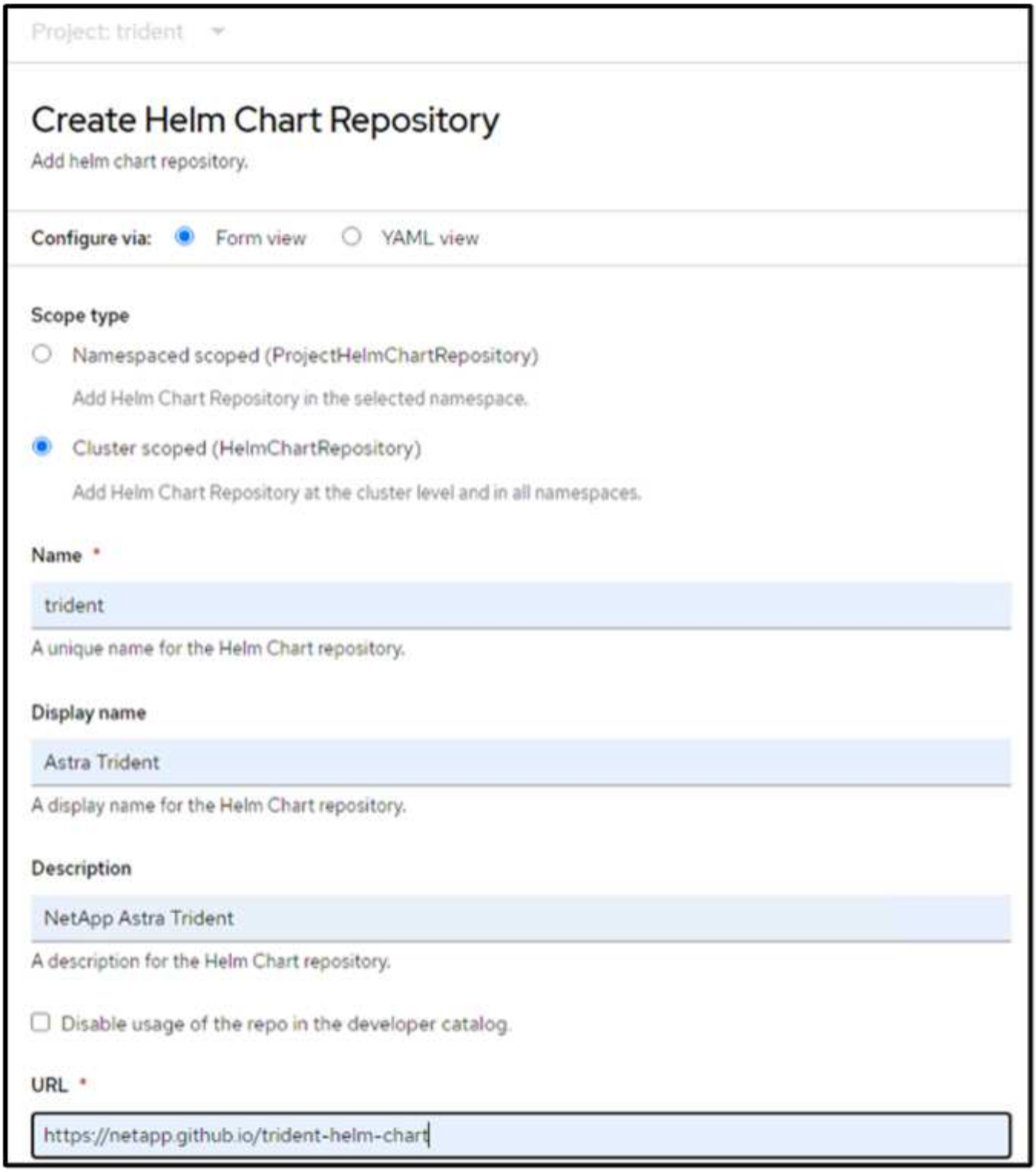
2.为群集创建**kubeconfig***文件

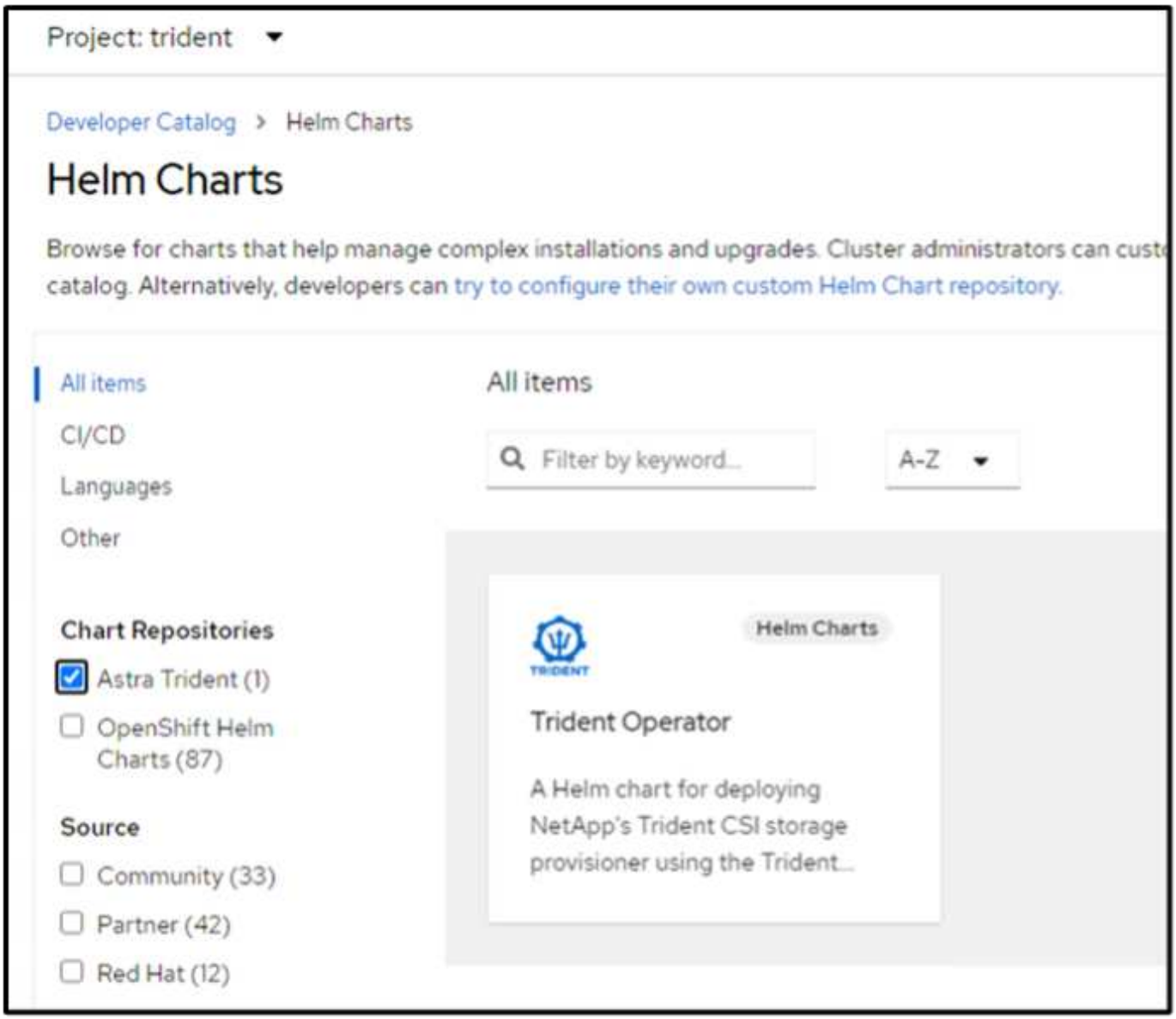
按照步骤进行操作 "此处" 为ROSA集群创建kubeconfig.稍后在将集群添加到ACS中时、将使用此kubeconfig.文件。

3.在群集上安装**Asta Trdent**

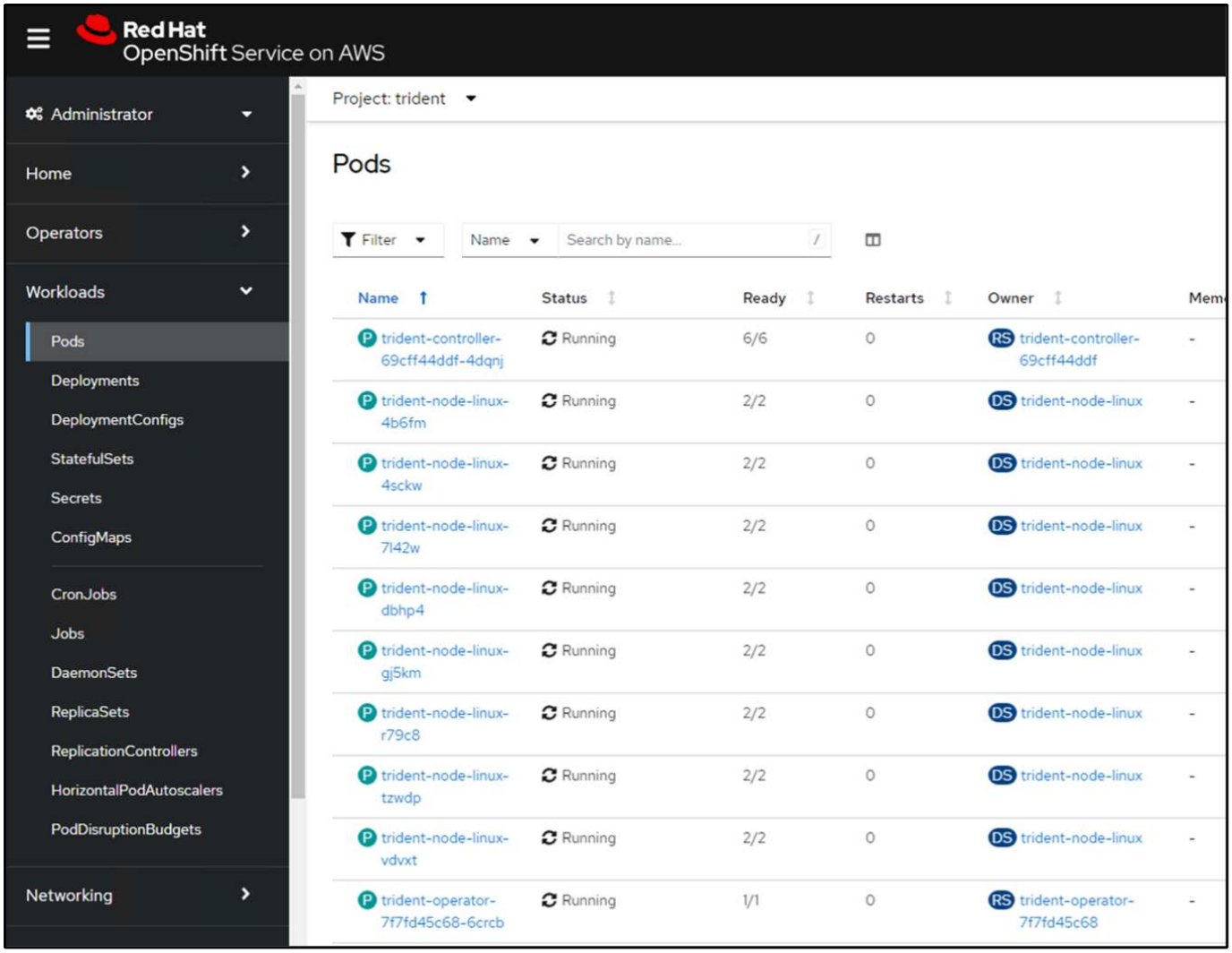
在ROSA集群上安装Asta Trident (最新版本)。要执行此操作、您可以按照给定的任一过程进行操作 "此处"。要从集群控制台使用Helm安装Trident、请先创建一个名为Trident的项目。

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


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



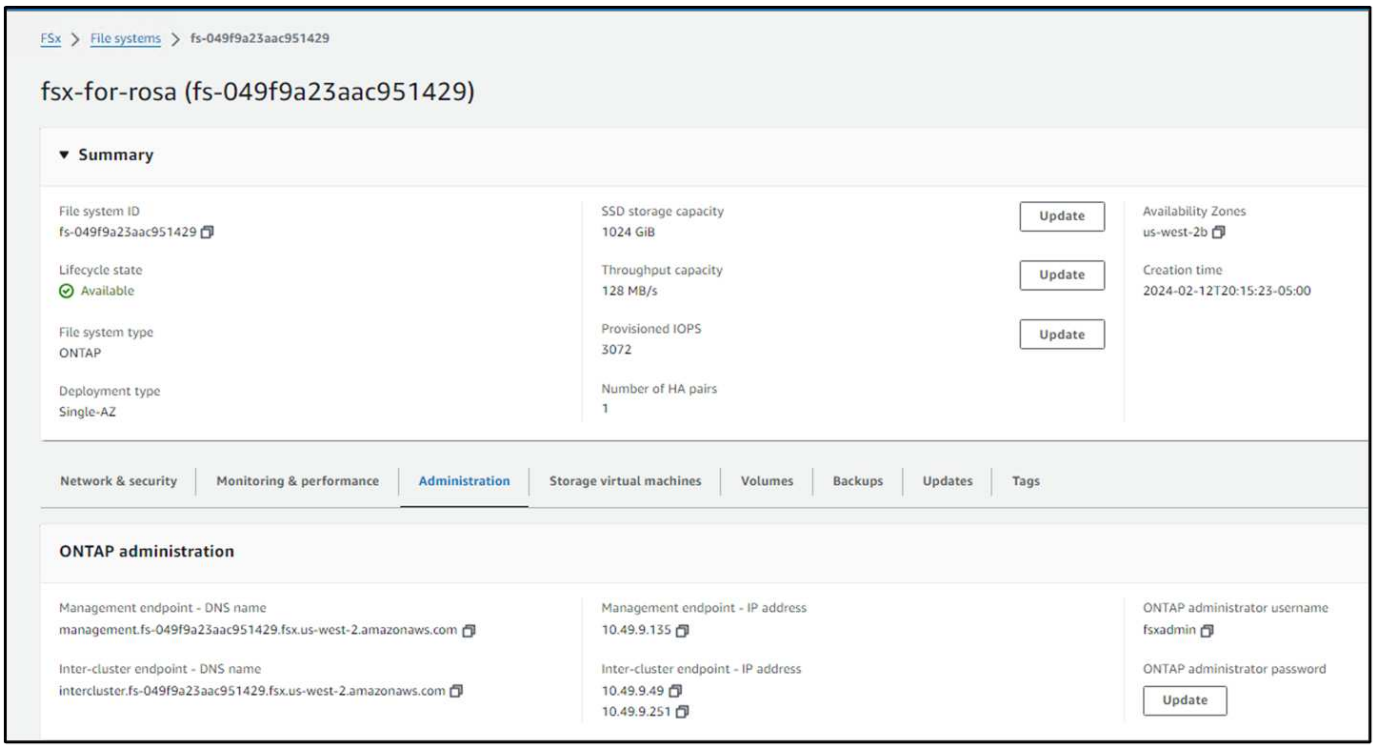
返回控制台上的"Administrator view"(管理员视图)、然后在三级工程中选择Pod、以验证所有三级工程模块是否正在运行。



4.使用三端**CSI**配置程序创建后端、存储类和快照类配置

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

您可以使用命令行创建对象、也可以从混合云控制台使用YAML文件创建对象。



Trident后端配置

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

存储类

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

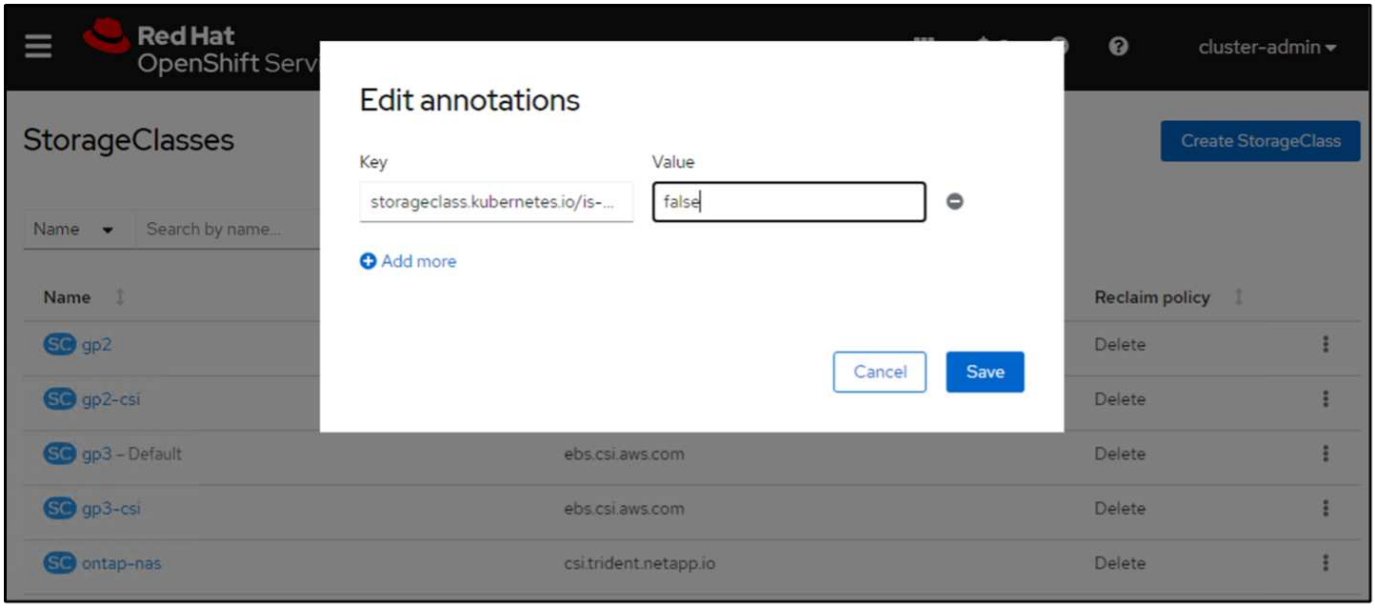
快照类

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

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

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

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



5.在群集上部署**PostgreSQL**应用程序

您可以从命令行部署此应用程序、如下所示：

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

如果您看不到应用程序Pod正在运行、则可能是由于安全上下文约束而导致错误。

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/postgresql      ClusterIP   172.30.245.50   <none>        5432/TCP   12m
service/postgresql-hl   ClusterIP   None            <none>        5432/TCP   12m

NAME                          READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                  MESSAGE
12m39s      Normal    WaitForFirstConsumer   persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate       statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate           statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

编辑以修复此错误 `runAsUser` 和 `fsGroup` 中的字段 `statefuleset.apps/postgresql` 具有的输出中的_id的对象 `oc get project` 命令、如下所示。

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

PostgreSQL应用程序应正在运行、并使用Amazon FSx支持的永久性卷作为NetApp ONTAP存储。

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

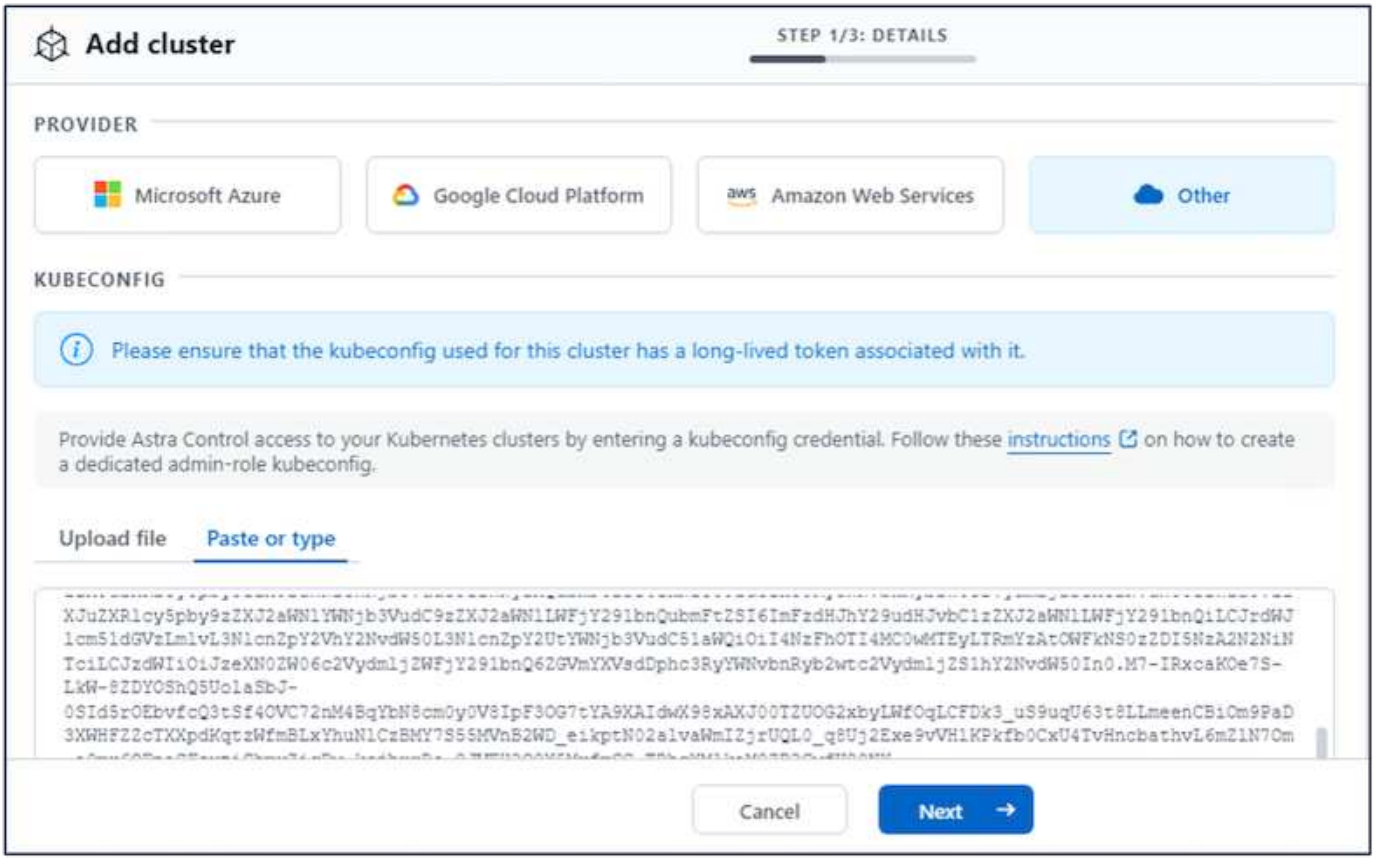
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6.创建数据库并添加记录

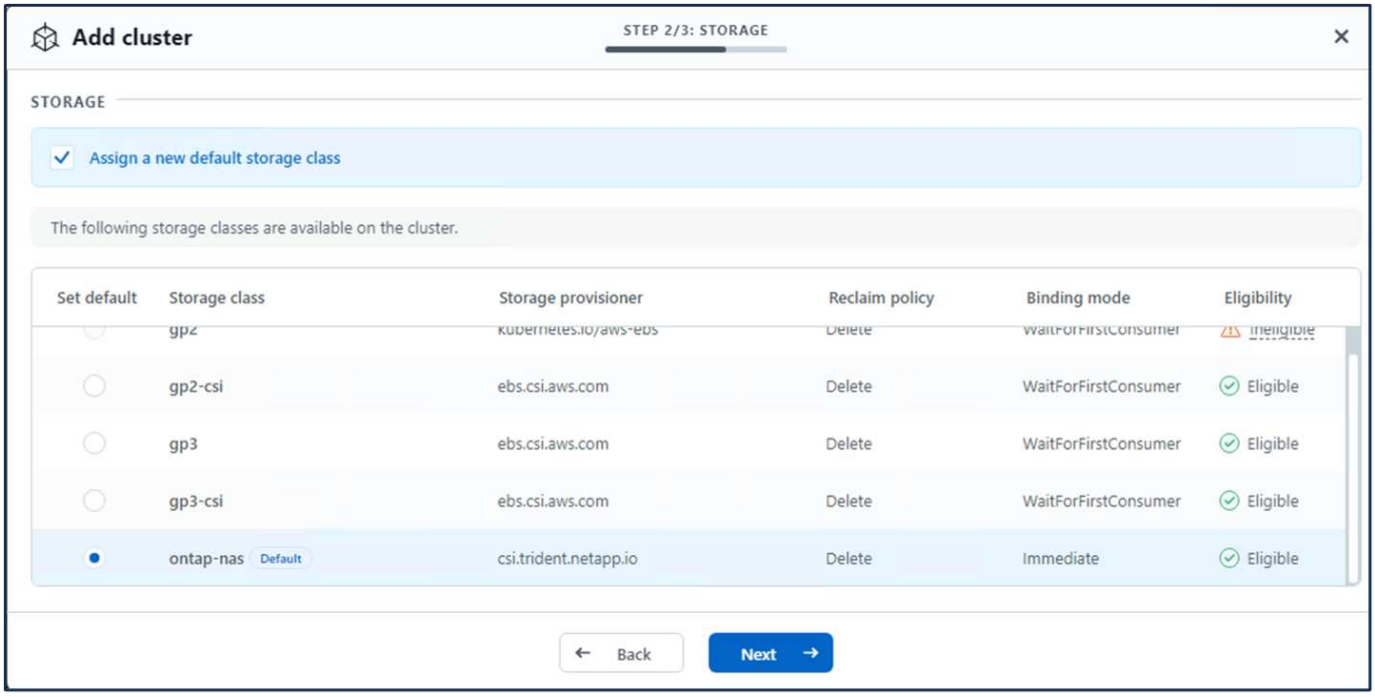
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7.将集群添加到**ACs**中

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

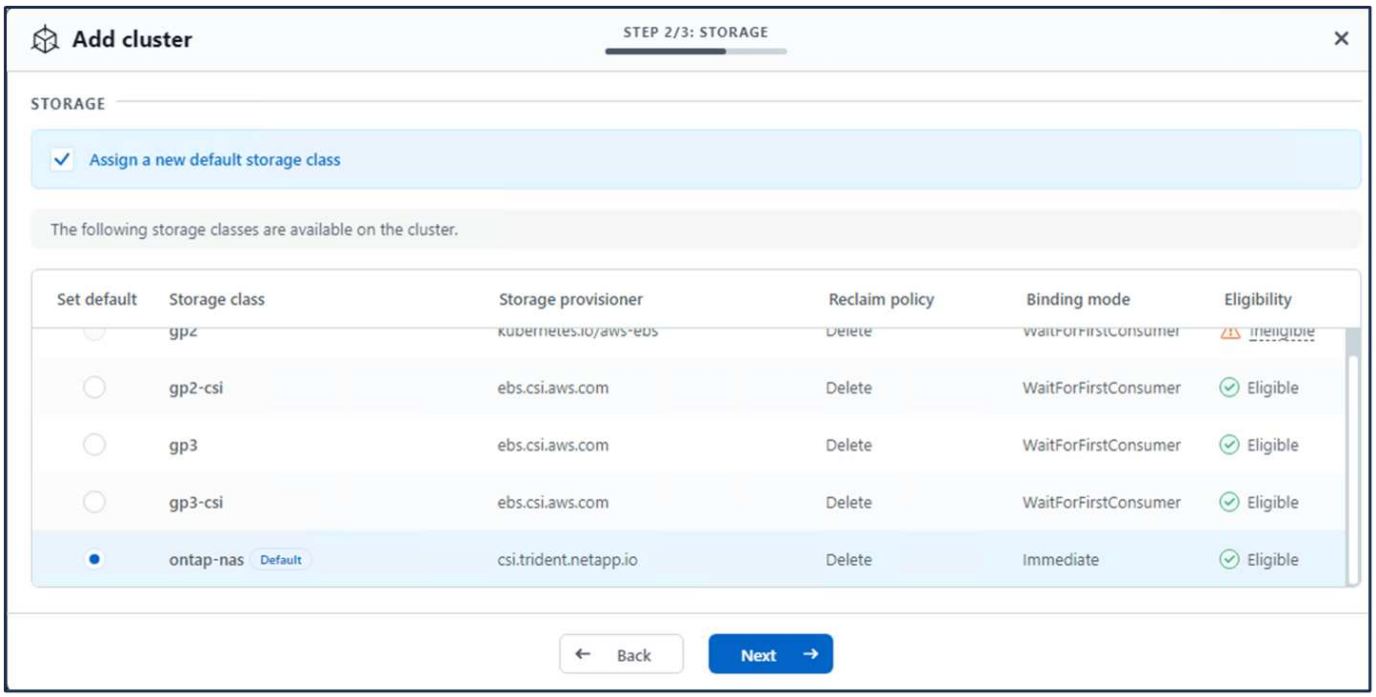


单击*Next*并选择ONTAP－NAS作为ACS的默认存储类。单击*Next*(下一步*)，查看详细信息，然后单击*Add*(添加)群集。



8.在**ACs**中定义应用程序

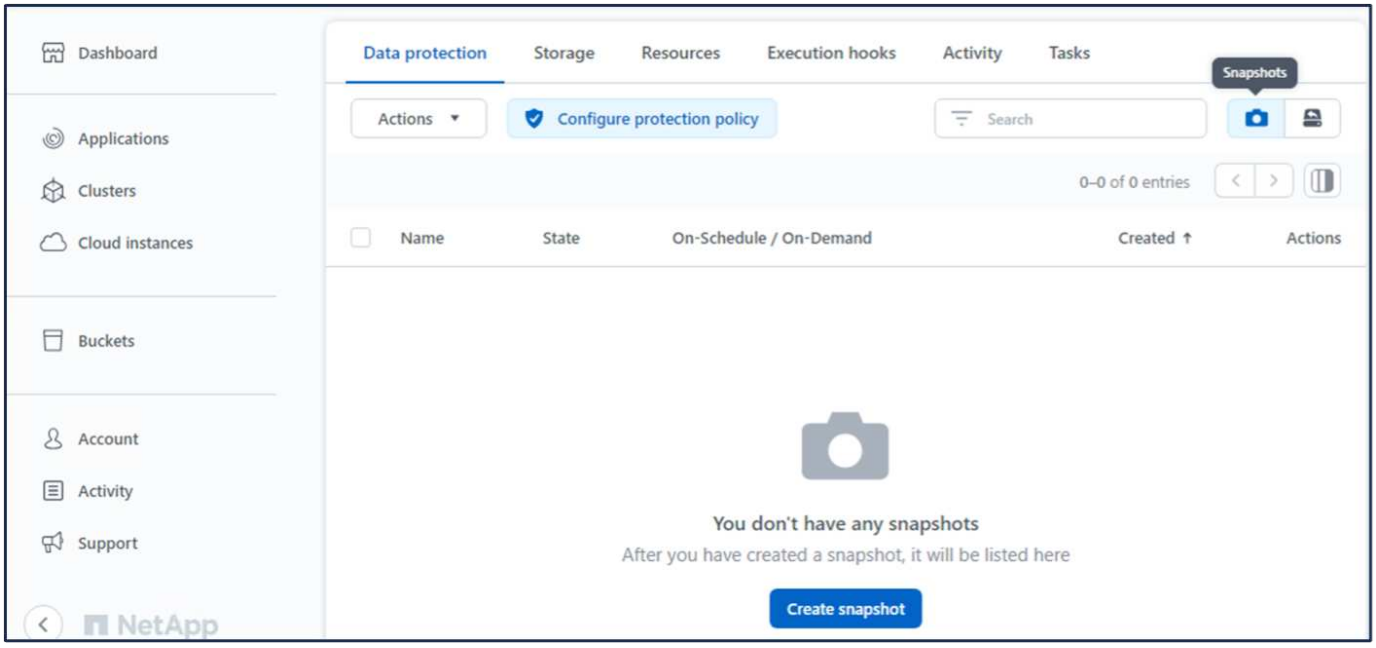
在ACS中定义PostgreSQL应用程序。在登录页面中，选择*Applications*、**Define***并填写相应的详细信息。单击“*下一步”几次，查看详细信息，然后单击“定义”。应用程序将添加到ACS。

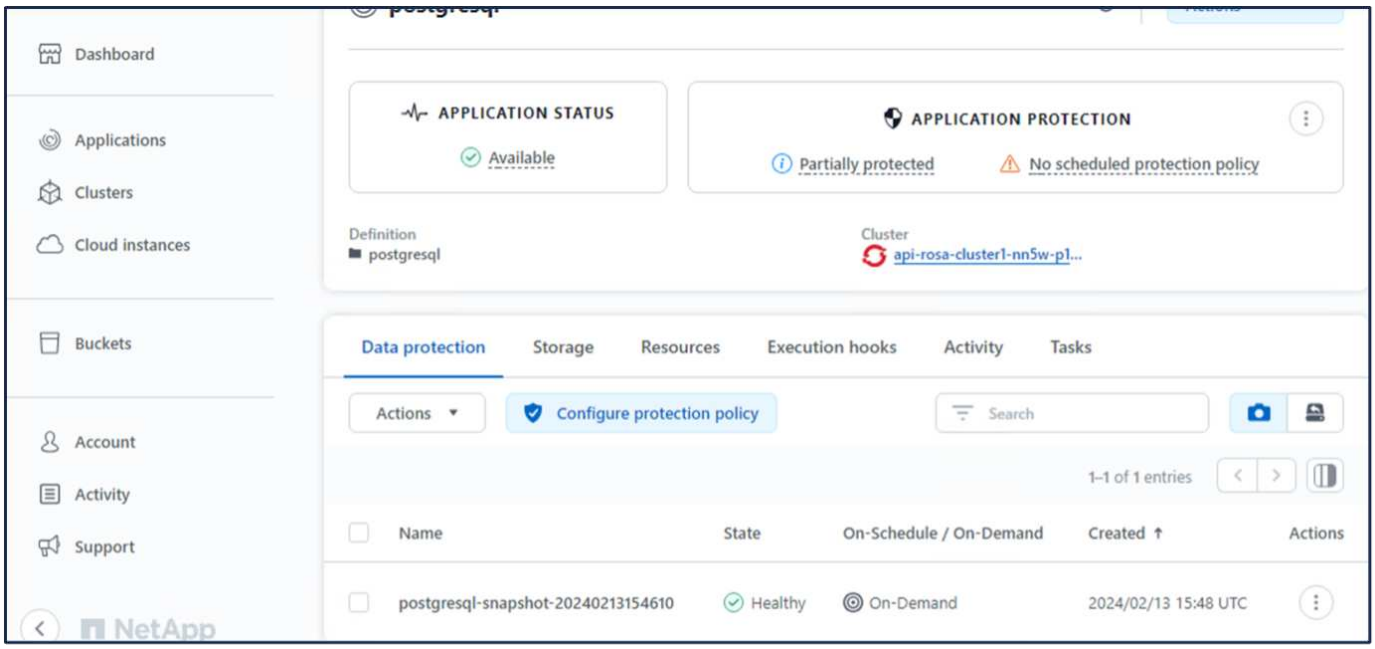


9.使用**ACs**创建快照

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

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





10.删除**PostgreSQL**应用程序中的数据库

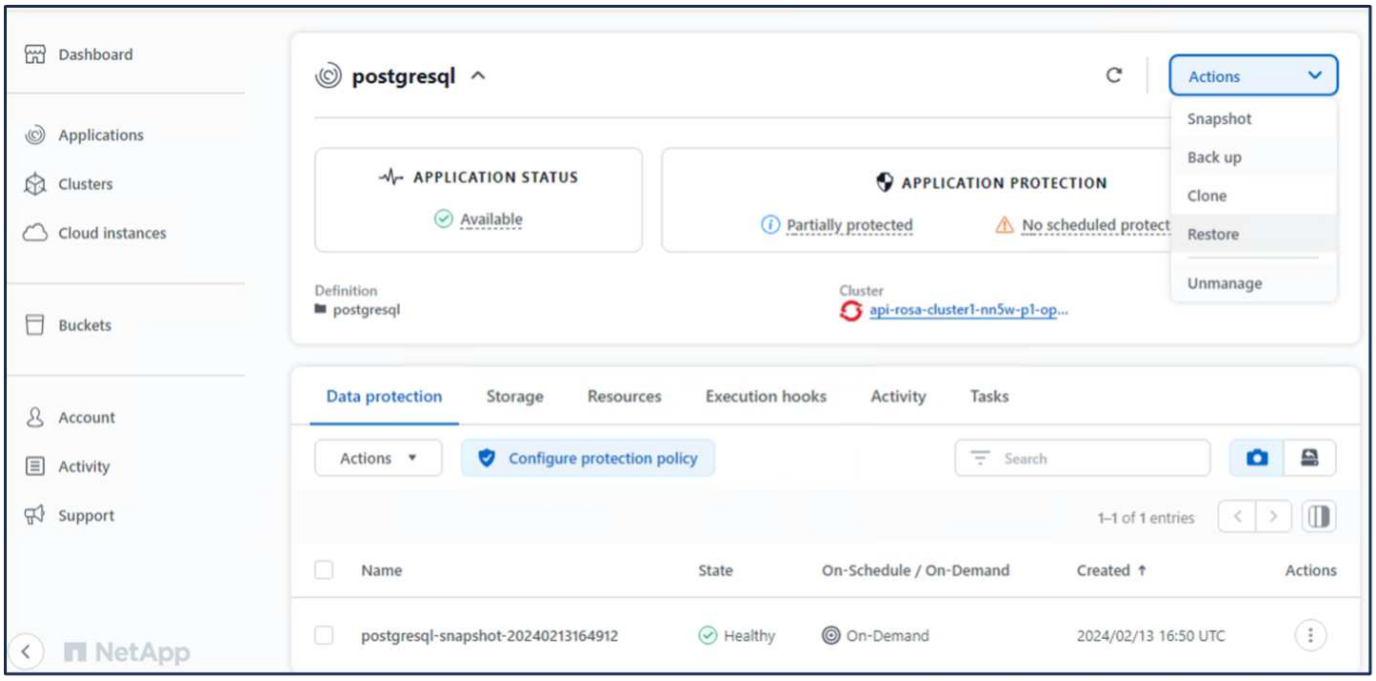
重新登录到PostgreSQL、列出可用数据库、删除先前创建的数据库并重新列出、以确保数据库已被删除。

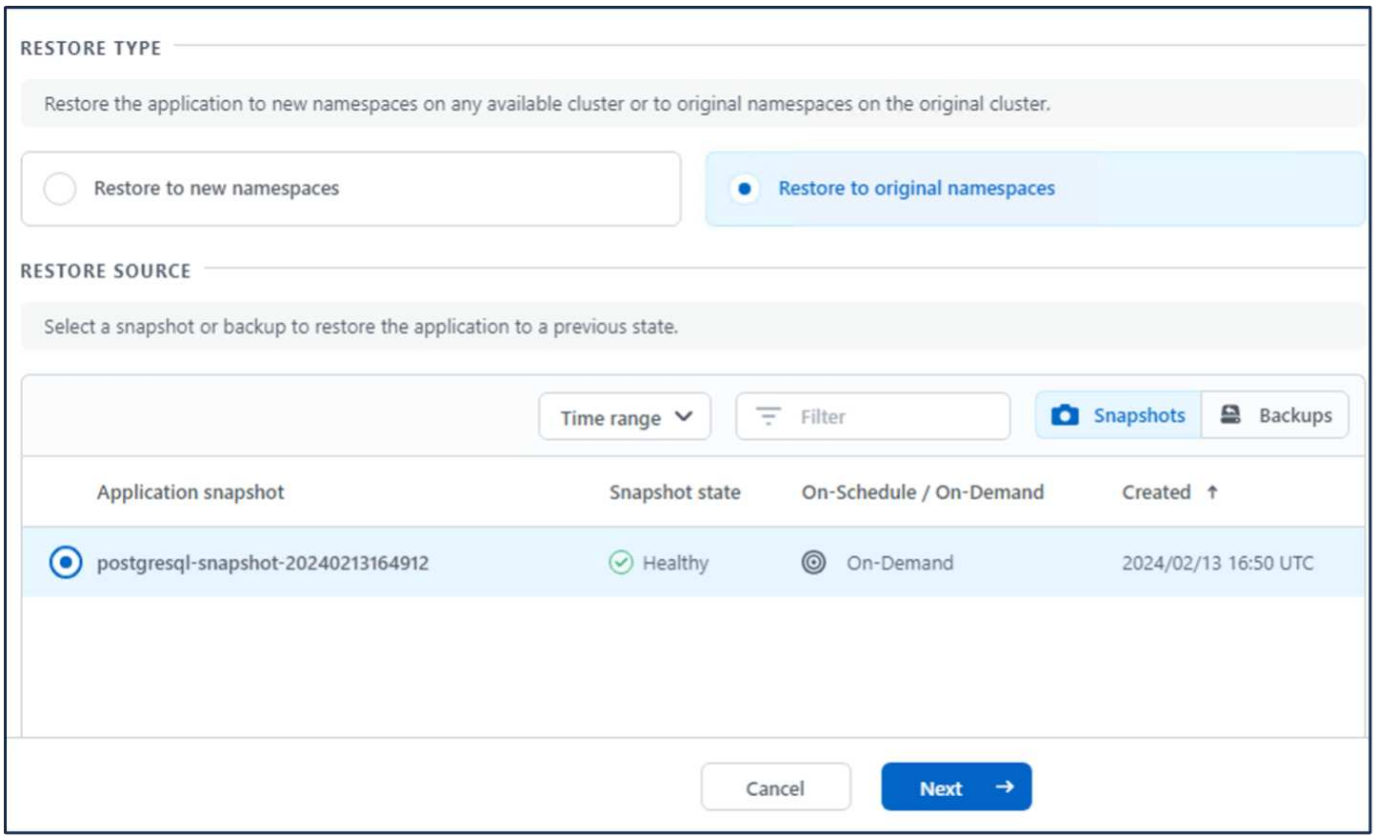
```
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
-
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
-
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

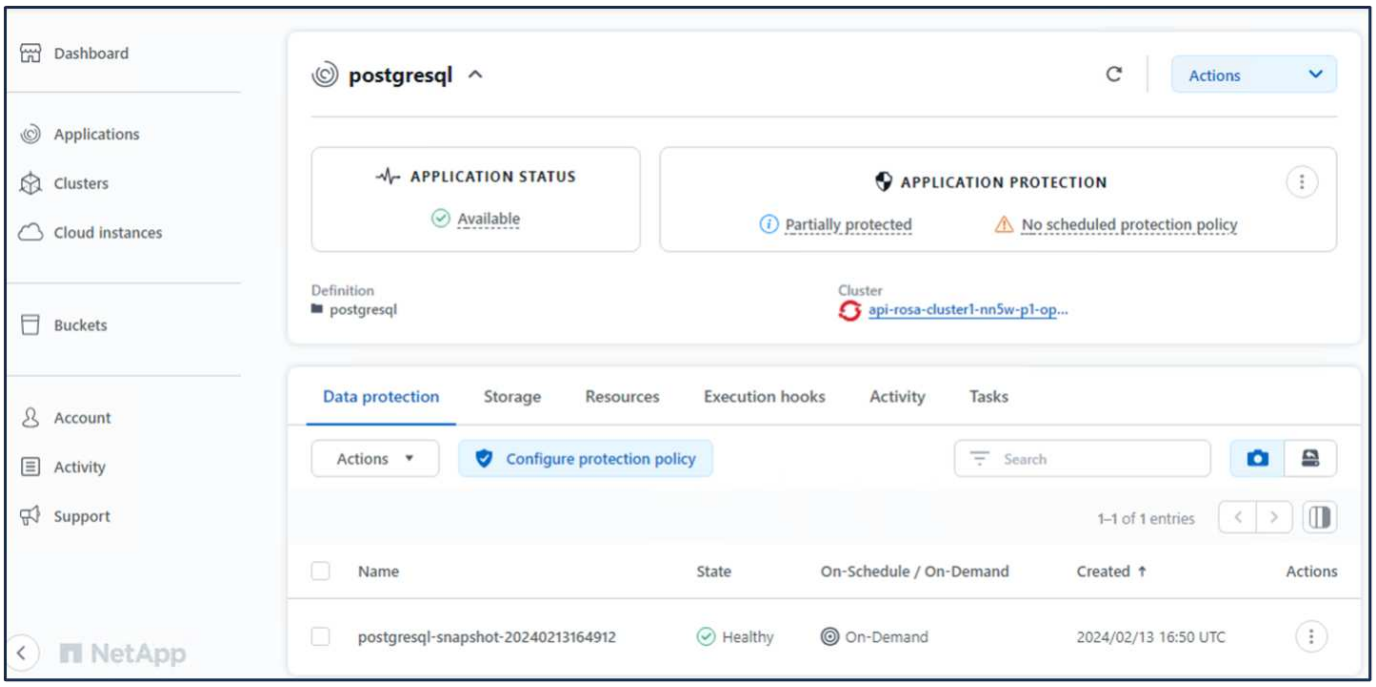
11.使用**ACs**从快照恢复

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

击*Restore*。从快照还原后、应用程序状态将从还原变为可用。







12.验证您的应用程序是否已从快照中恢复

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

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```


数据迁移

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

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

使用**Helm**将**FSxN**与**TRIdent**集成图表

Rosa集群与Amazon FSx for ONTAP集成

容器应用程序的迁移涉及：

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

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

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

对ROSA集群上的应用程序进行故障转移和故障恢复

适用于**OpenShift**容器工作负载的数据保护和迁移解决方案