使用 CVO 和 AVS（来宾连接存储）进行灾难恢复

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

目录

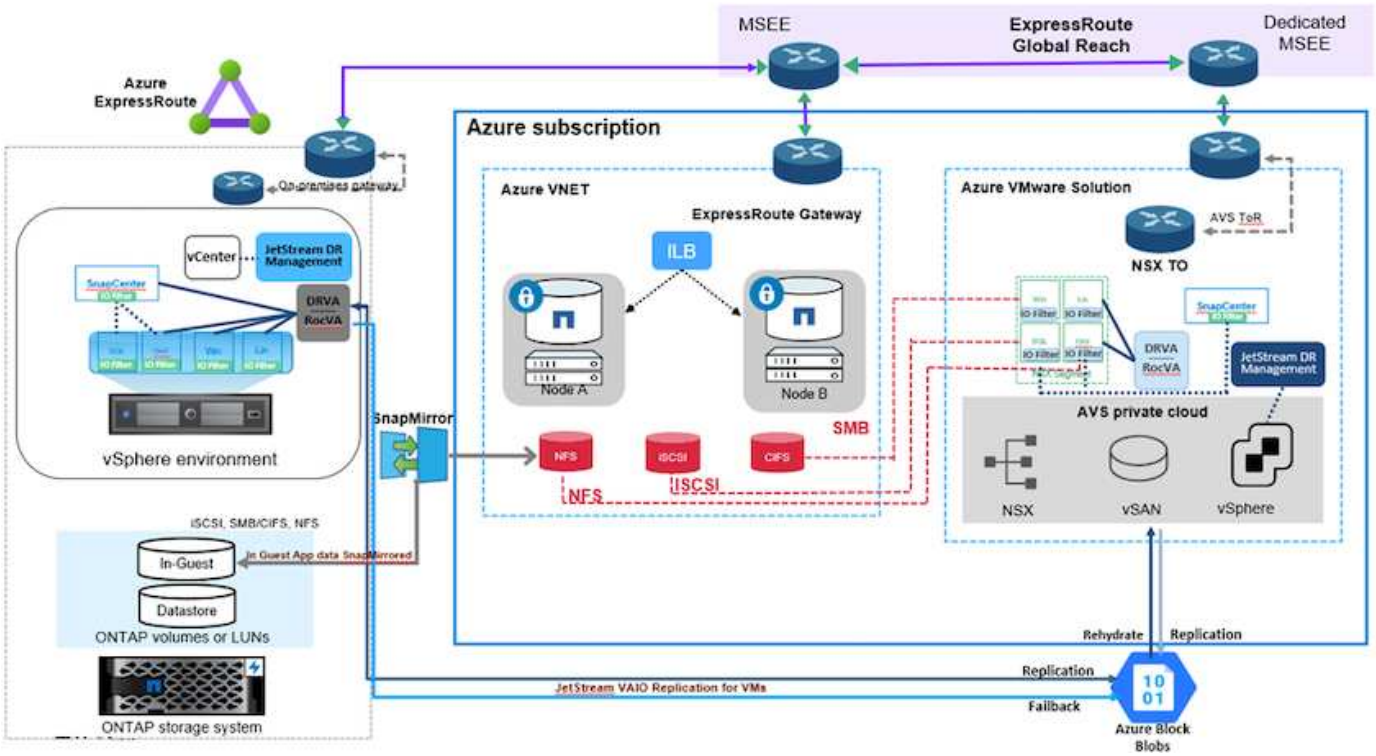
使用 CVO 和 AVS（来宾连接存储）进行灾难恢复

云端灾难恢复是一种具有弹性且经济高效的方法，可以保护工作负载免受站点中断和勒索软件等数据损坏事件的影响。借助NetApp SnapMirror，使用来宾连接存储的本地 VMware 工作负载可以复制到在 Azure 中运行的NetApp Cloud Volumes ONTAP 。

概述

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
```

本文档提供了使用NetApp SnapMirror、JetStream 和 Azure VMware 解决方案 (AVS) 设置和执行灾难恢复的分步方法。



假设

本文档重点介绍应用程序数据的客户机内存储（也称为客户机连接），我们假设本地环境使用SnapCenter进行应用程序一致性备份。

本文档适用于任何第三方备份或恢复解决方案。根据环境中使用的解决方案，遵循最佳实践来创建符合组织 SLA 的备份策略。

对于本地环境和 Azure 虚拟网络之间的连接，请使用快速路由全球覆盖或带有 VPN 网关的虚拟 WAN。应根据内部部署 vLAN 设计创建段。

将本地数据中心连接到 Azure 有多种选择，因此我们无法在本文档中概述特定的工作流程。请参阅 Azure 文档，了解适当的本地到 Azure 连接方法。

部署灾难恢复解决方案

解决方案部署概述

1. 确保使用SnapCenter备份应用程序数据并满足必要的 RPO 要求。
2. 使用适当的订阅和虚拟网络中的云管理器为Cloud Volumes ONTAP配置正确的实例大小。
   a. 为相关应用程序卷配置SnapMirror 。
   b. 更新SnapCenter中的备份策略以在计划的作业之后触发SnapMirror更新。
3. 在本地数据中心安装 JetStream DR 软件并启动对虚拟机的保护。
4. 在 Azure VMware 解决方案私有云中安装 JetStream DR 软件。
5. 在灾难事件期间，使用 Cloud Manager 中断SnapMirror关系并触发虚拟机到Azure NetApp Files或指定 AVS DR 站点中的 vSAN 数据存储的故障转移。
   a. 重新连接应用程序虚拟机的 ISCSI LUN 和 NFS 挂载。
6. 主站点恢复后，通过反向重新同步SnapMirror调用故障回复到受保护站点。

部署详情

在 **Azure** 上配置 **CVO** 并将卷复制到 **CVO**

第一步是在 Azure 上配置Cloud Volumes ONTAP （"链路") 并以所需的频率和快照保留将所需的卷复制到Cloud Volumes ONTAP 。

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB
✓	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB
✓	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB

配置 **AVS** 主机和 **CVO** 数据访问

部署 SDDC 时需要考虑的两个重要因素是 Azure VMware 解决方案中 SDDC 群集的大小以及保持 SDDC 服务的时间。灾难恢复解决方案的这两个关键考虑因素有助于降低总体运营成本。 SDDC 最小可以只有三台主机，最大可以达到全面部署的多主机集群。

部署 AVS 集群的决定主要基于 RPO/RTO 要求。借助 Azure VMware 解决方案，可以及时配置 SDDC，为测试或实际灾难事件做好准备。当您不处理灾难时，及时部署的 SDDC 可以节省 ESXi 主机成本。然而，这种部署形式会在配置 SDDC 时影响 RTO 几个小时。

最常见的部署选项是让 SDDC 以始终开启、指示灯亮起的操作模式运行。此选项占用空间较小，仅需三个始终可用的主机，同时还通过为模拟活动和合规性检查提供运行基线来加快恢复操作，从而避免生产站点和 DR 站点之间出现操作偏差的风险。当需要处理实际 DR 事件时，指示灯集群可以快速扩展到所需的级别。

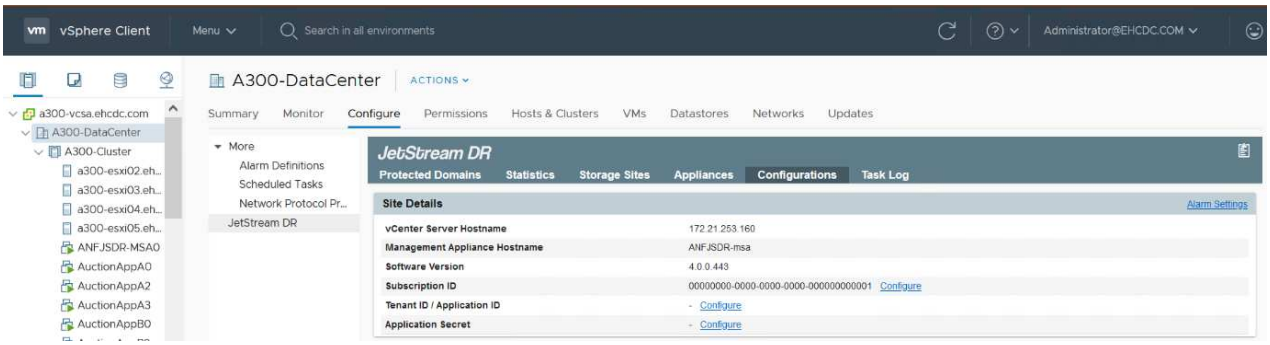
要配置 AVS SDDC（按需模式或指示灯模式），请参阅"在 Azure 上部署和配置虚拟化环境"。作为先决条件，请验证在建立连接后，驻留在 AVS 主机上的客户虚拟机是否能够使用来自Cloud Volumes ONTAP的数据。

正确配置Cloud Volumes ONTAP和 AVS 后，开始配置 Jetstream，通过使用 VAIO 机制并利用SnapMirror将应用程序卷复制到Cloud Volumes ONTAP，自动将本地工作负载恢复到 AVS（具有应用程序 VMDK 的虚拟机和具有客户机内存储的虚拟机）。

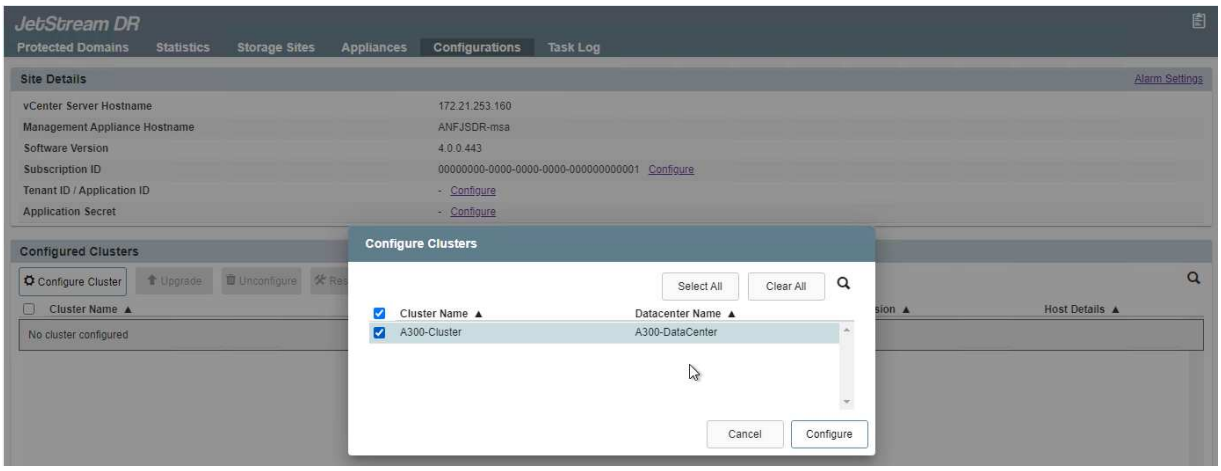
在本地数据中心安装 **JetStream DR**

JetStream DR 软件由三个主要组件组成：JetStream DR 管理服务器虚拟设备 (MSA)、DR 虚拟设备 (DRVA) 和主机组件（I/O 过滤包）。 MSA 用于在计算集群上安装和配置主机组件，然后管理 JetStream DR 软件。安装过程如下：

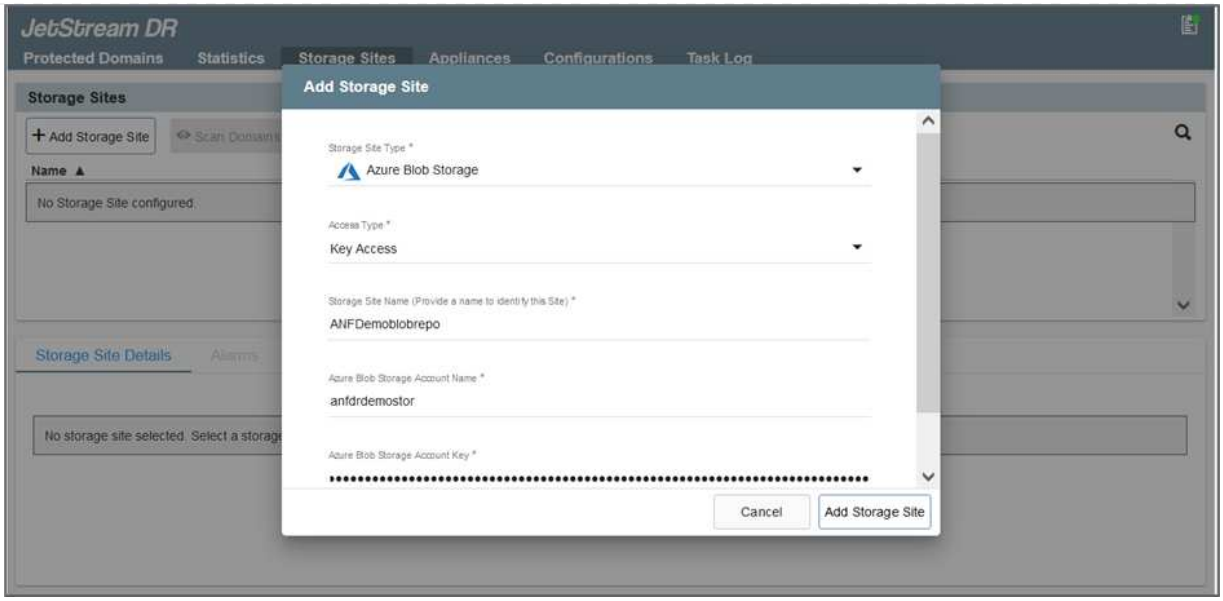
1. 检查先决条件。
2. 运行容量规划工具获取资源和配置建议。
3. 将 JetStream DR MSA 部署到指定集群中的每个 vSphere 主机。
4. 在浏览器中使用其 DNS 名称启动 MSA。
5. 向 MSA 注册 vCenter 服务器。
6. 部署 JetStream DR MSA 并注册 vCenter Server 后，使用 vSphere Web Client 导航到 JetStream DR 插件。这可以通过导航到数据中心 > 配置 > JetStream DR 来完成。



7. 从 JetStream DR 界面完成以下任务：
   a. 使用 I/O 筛选器包配置集群。

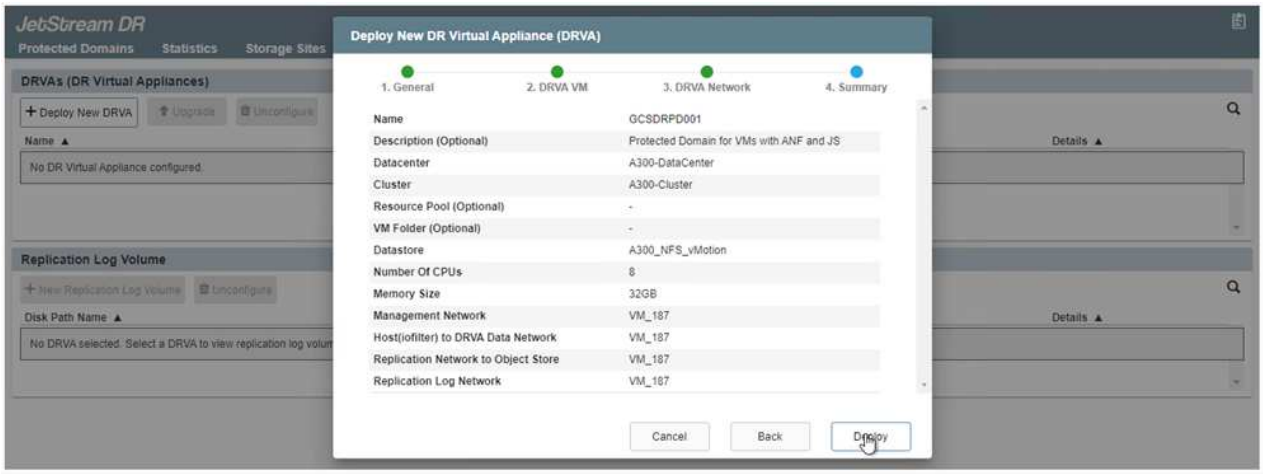


   b. 添加位于恢复站点的 Azure Blob 存储。

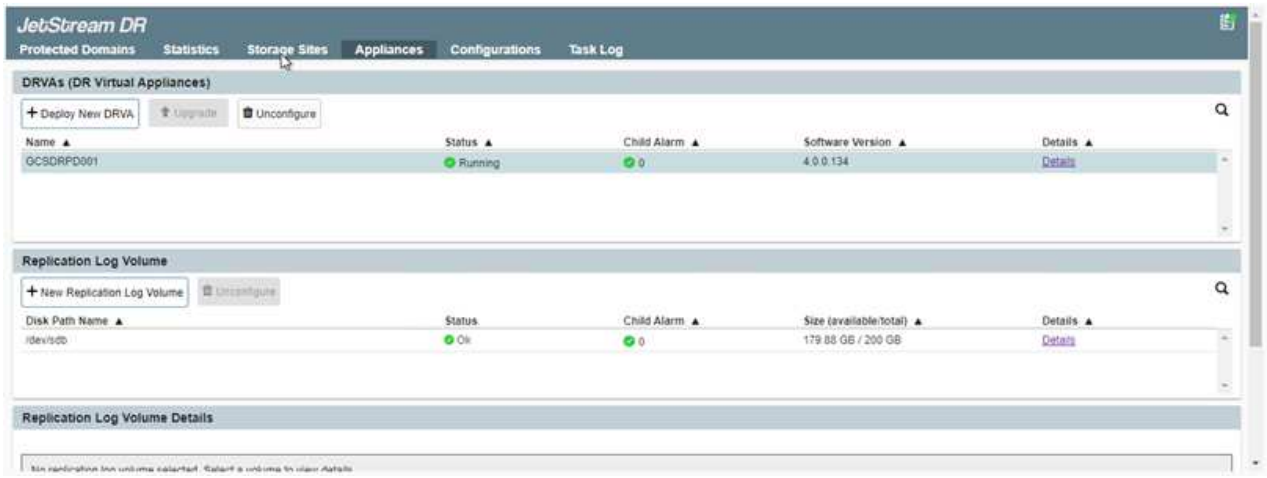


8. 从设备选项卡部署所需数量的 DR 虚拟设备 (DRVA)。

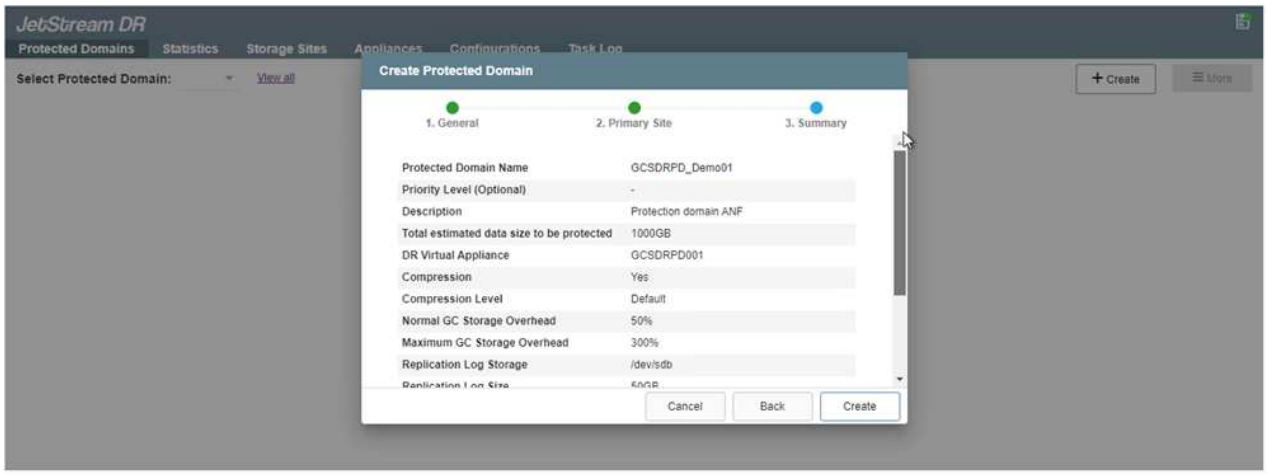
   使用容量规划工具来估计所需的 DRVA 数量。

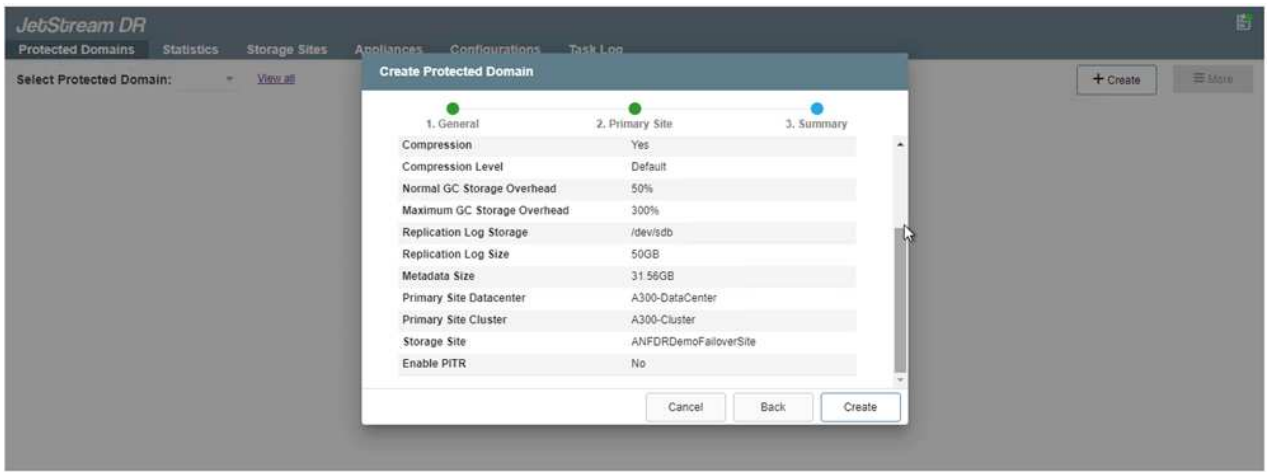


9. 使用来自可用数据存储或独立共享 iSCSI 存储池的 VMDK 为每个 DRVA 创建复制日志卷。



10. 在“受保护的域”选项卡中，使用有关 Azure Blob 存储站点、DRVA 实例和复制日志的信息创建所需数量的受保护域。受保护域定义集群内的特定虚拟机或一组应用程序虚拟机，这些虚拟机受到一起保护，并分配了故障转移/故障回复操作的优先级顺序。

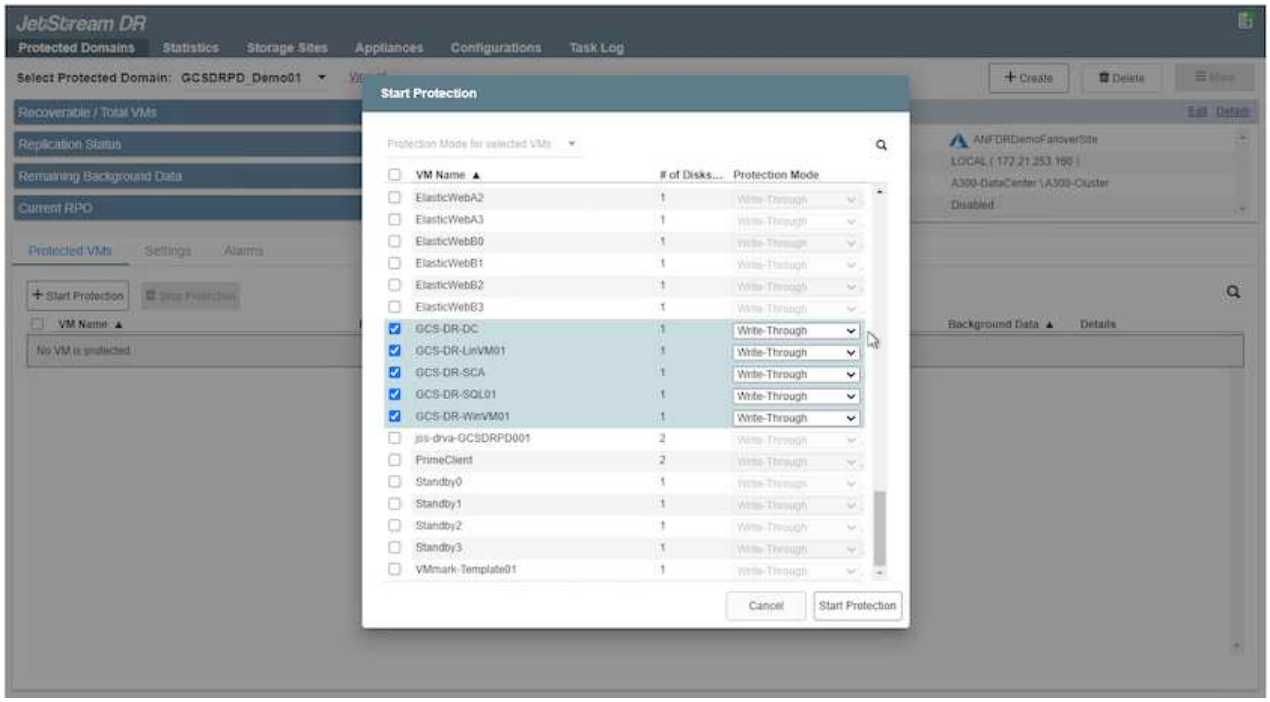




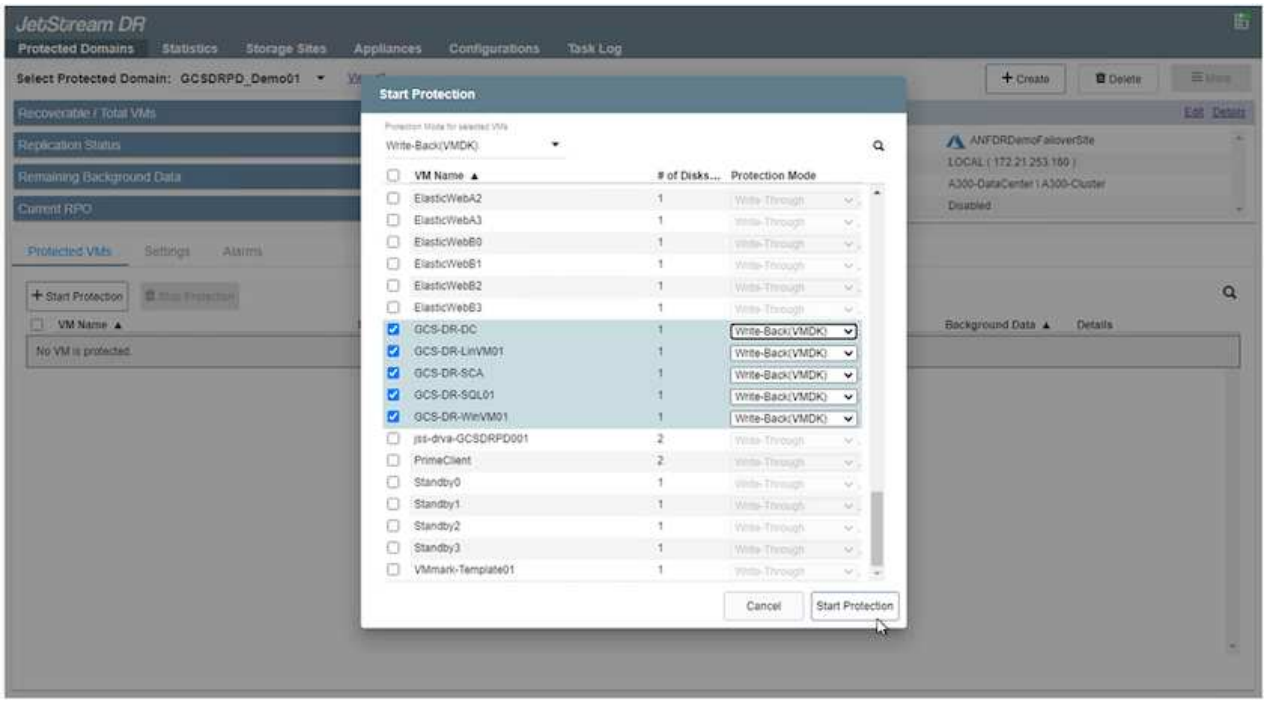
11. 选择要保护的虚拟机，并根据依赖关系将虚拟机分组到应用程序组中。应用程序定义允许您将虚拟机集分组为逻辑组，其中包含其启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

确保受保护域内的所有虚拟机使用相同的保护模式。

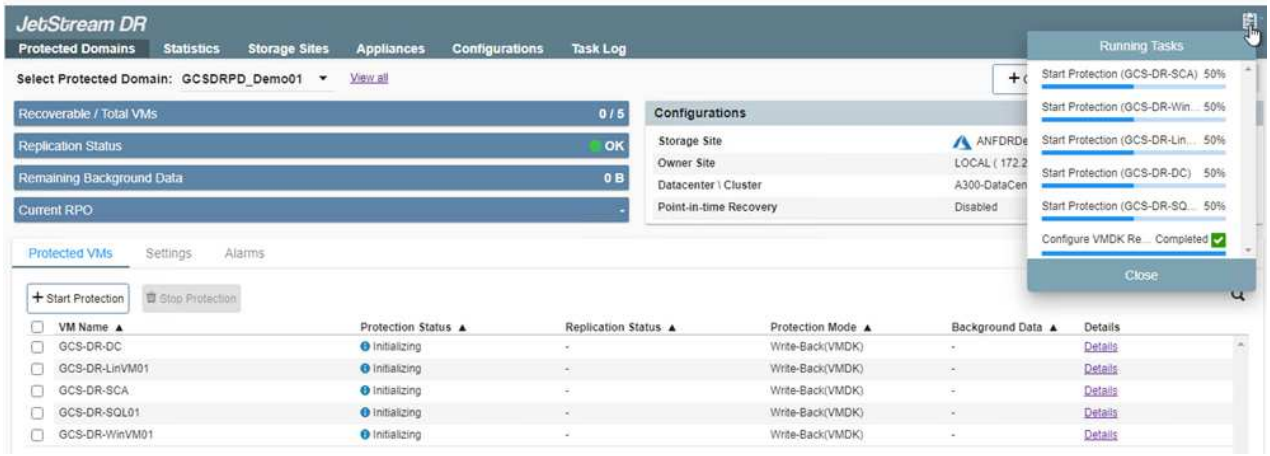
回写（VMDK）模式提供更高的性能。



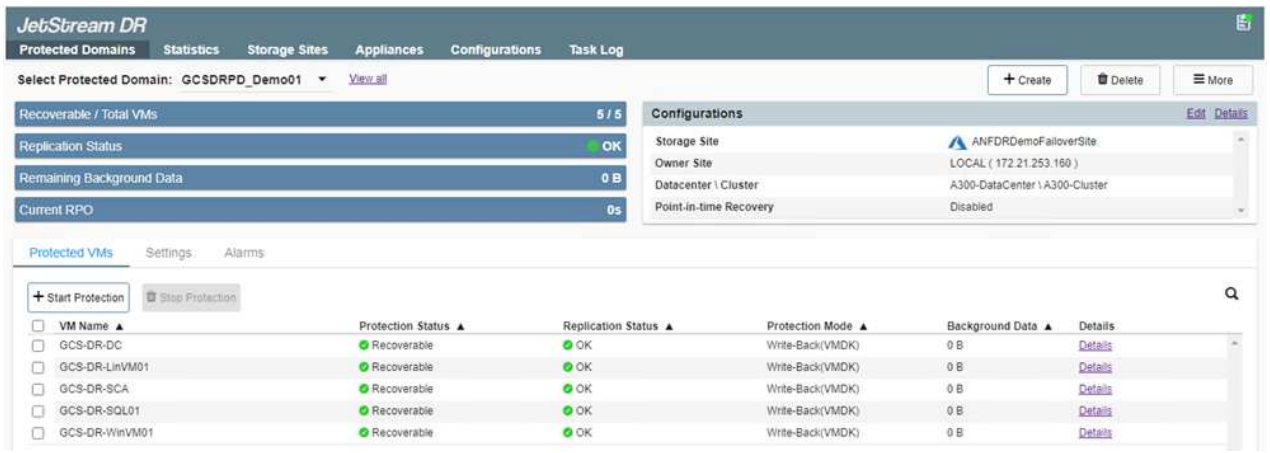
12. 确保复制日志卷放置在高性能存储上。



13. 完成后，单击“开始保护”以保护受保护的域。这将开始将选定虚拟机的数据复制到指定的 Blob 存储。



14. 复制完成后，虚拟机保护状态标记为可恢复。

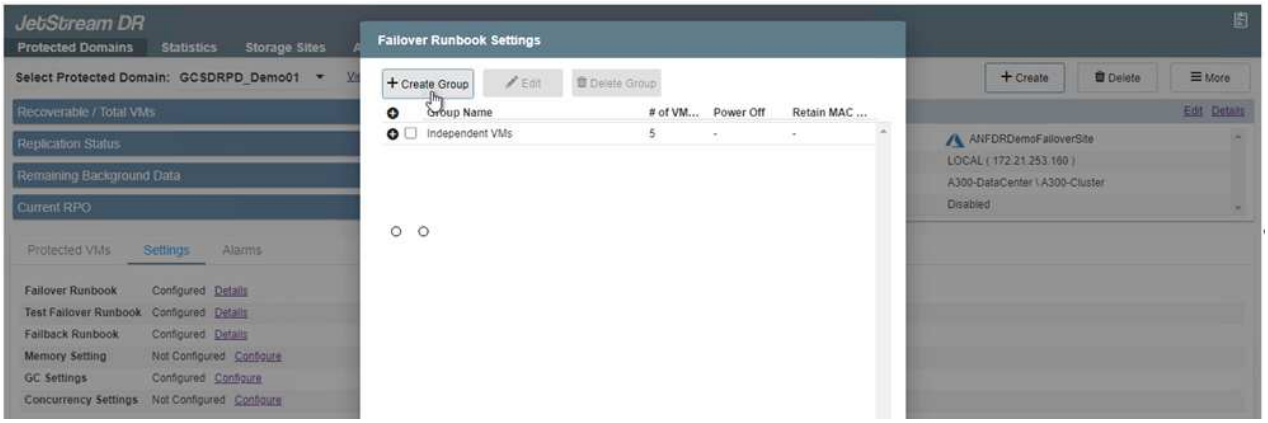


> 可以配置故障转移运行手册来对虚拟机进行分组（称为恢复组）、设置启动顺序以及修改 CPU/内存设置以及 IP 配置。

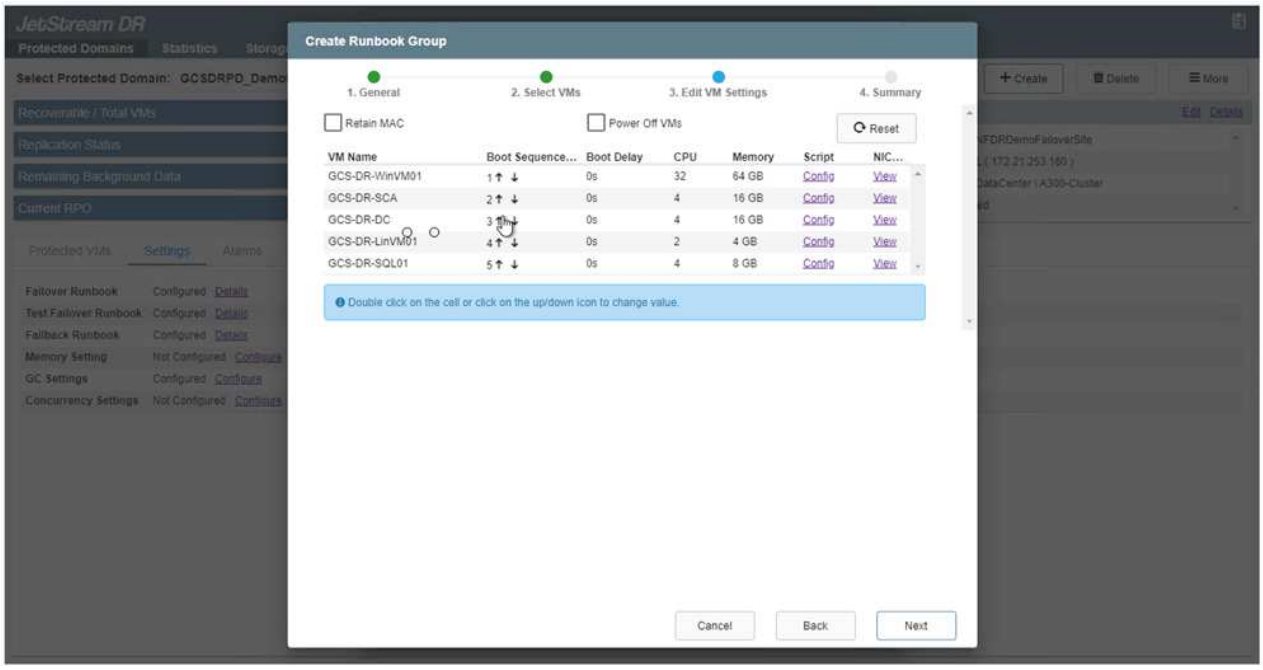
15. 单击“设置”，然后单击“运行手册配置”链接来配置运行手册组。

16. 单击“创建组”按钮开始创建新的运行手册组。

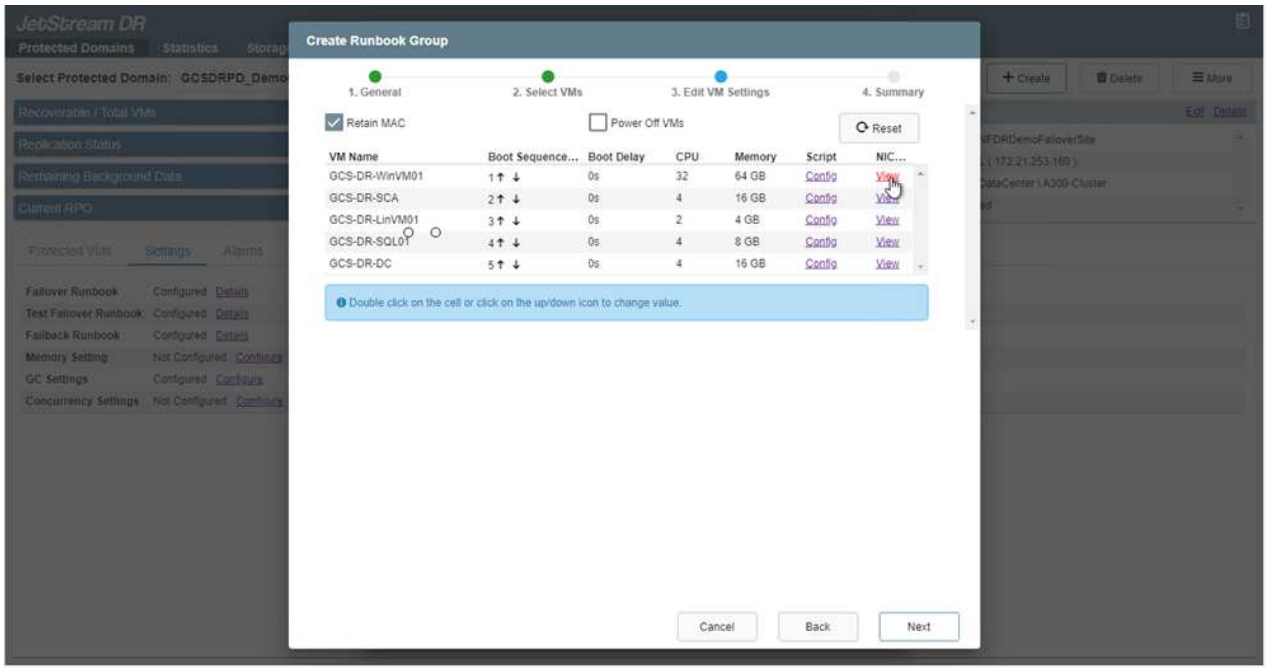
> 如果需要，在屏幕的下部，应用自定义前脚本和后脚本，以便在运行手册组操作之前和之后自动运行。确保 Runbook 脚本驻留在管理服务器上。



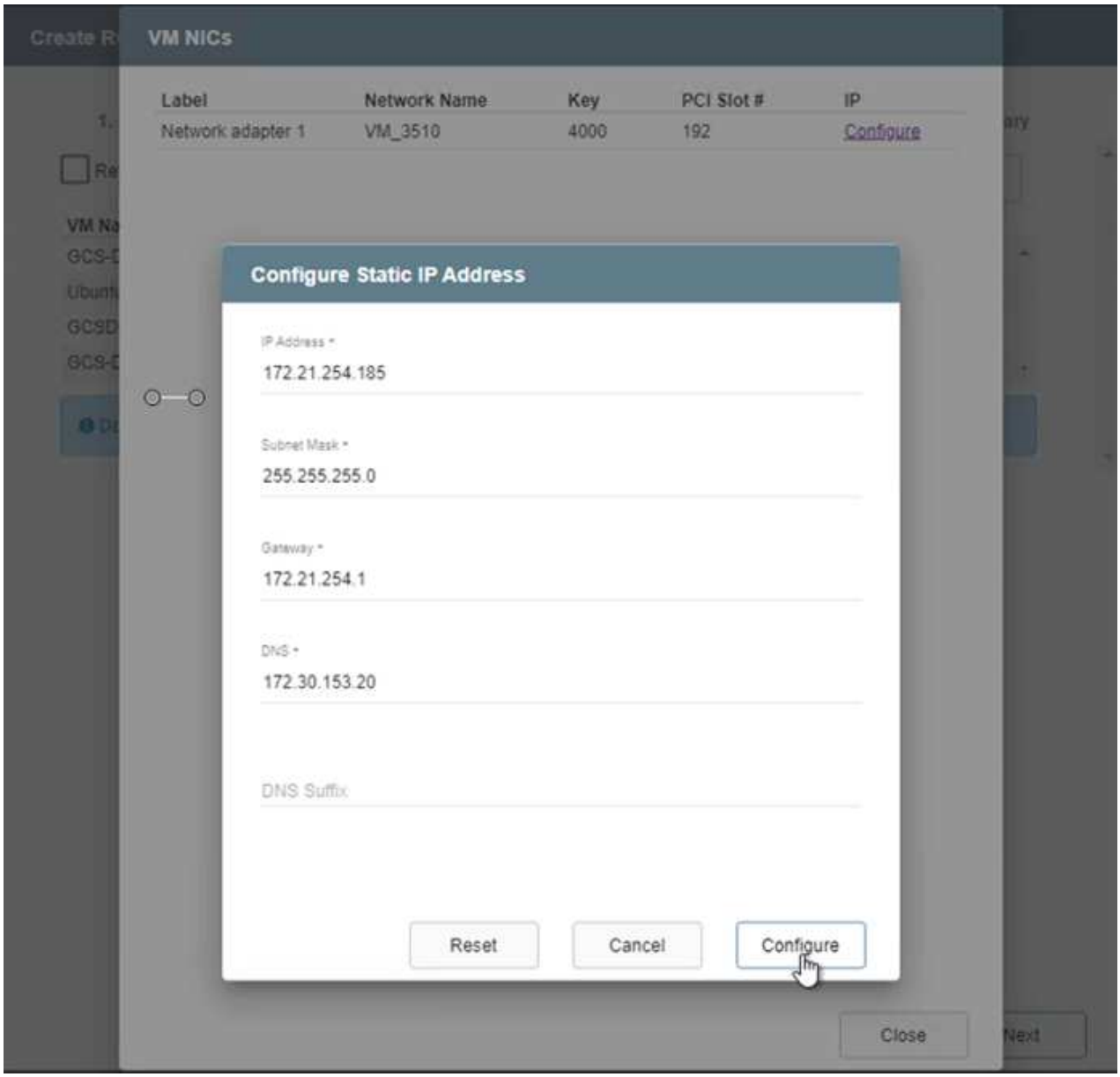
17. 根据需要编辑 VM 设置。指定恢复虚拟机的参数，包括启动顺序、启动延迟（以秒为单位）、CPU 数量以及要分配的内存量。单击向上或向下箭头更改虚拟机的启动顺序。还提供了保留 MAC 的选项。

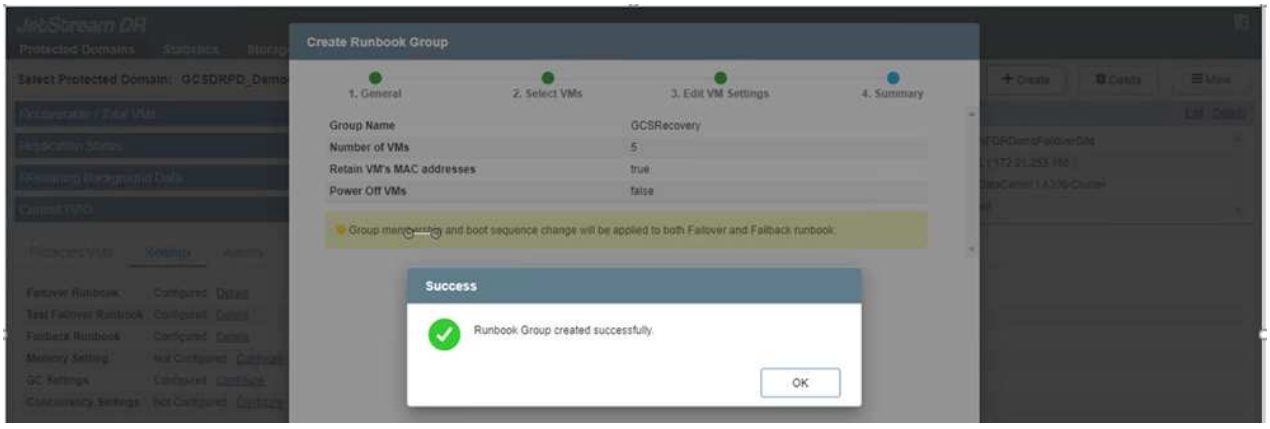


18. 可以为组中的各个虚拟机手动配置静态 IP 地址。单击虚拟机的 NIC 视图链接以手动配置其 IP 地址设置。



19. 单击配置按钮保存各个虚拟机的 NIC 设置。





故障转移和故障回复运行手册的状态现在均列为“已配置”。故障转移和故障回复运行手册组是使用相同的初始虚拟机组和设置成对创建的。如果需要，可以通过单击其各自的“详细信息”链接并进行更改来单独定制任何运行手册组的设置。

在私有云中为 **AVS** 安装 **JetStream DR**

恢复站点 (AVS) 的最佳实践是提前创建一个三节点的试点灯集群。这允许预先配置恢复站点基础设施，包括以下内容：

- 目标网络段、防火墙、DHCP 和 DNS 等服务等
- 为 AVS 安装 JetStream DR
- 将 ANF 卷配置为数据存储等

JetStream DR 支持关键任务域的接近零 RTO 模式。对于这些域，应该预先安装目标存储。在这种情况下，ANF 是推荐的存储类型。

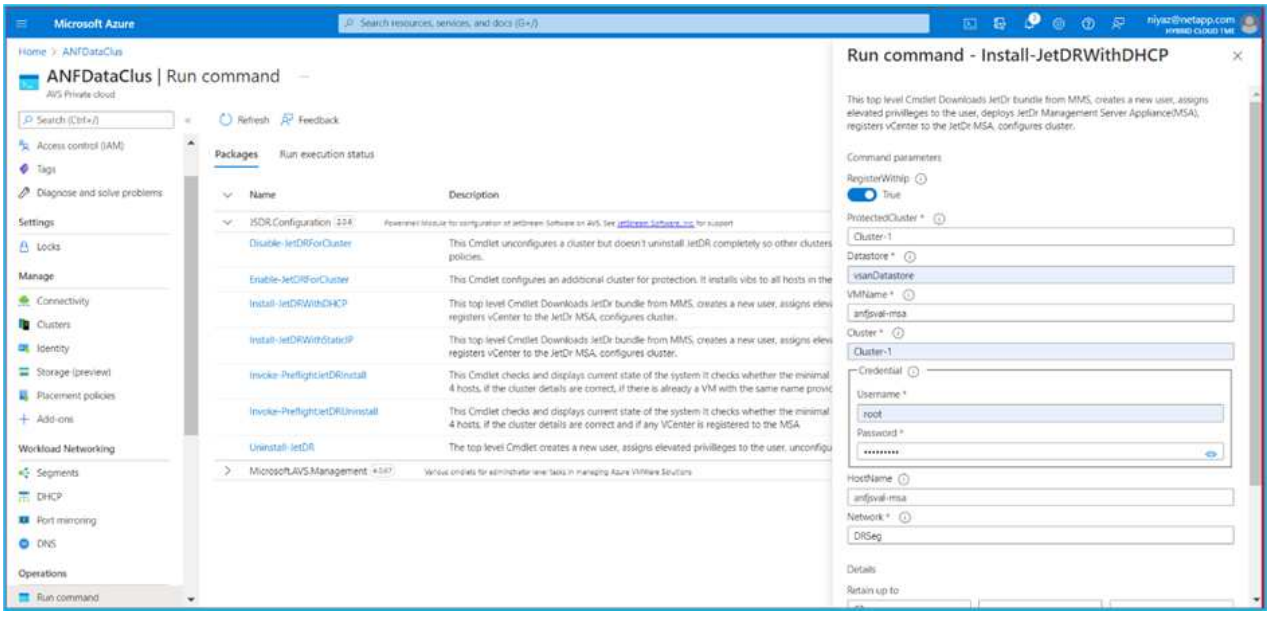
> 应在 AVS 集群上配置包括段创建在内的网络配置以满足本地要求。

> 根据 SLA 和 RTO 要求，您可以使用连续故障转移或常规（标准）故障转移模式。对于接近于零的 RTO，您应该在恢复站点开始持续补水。

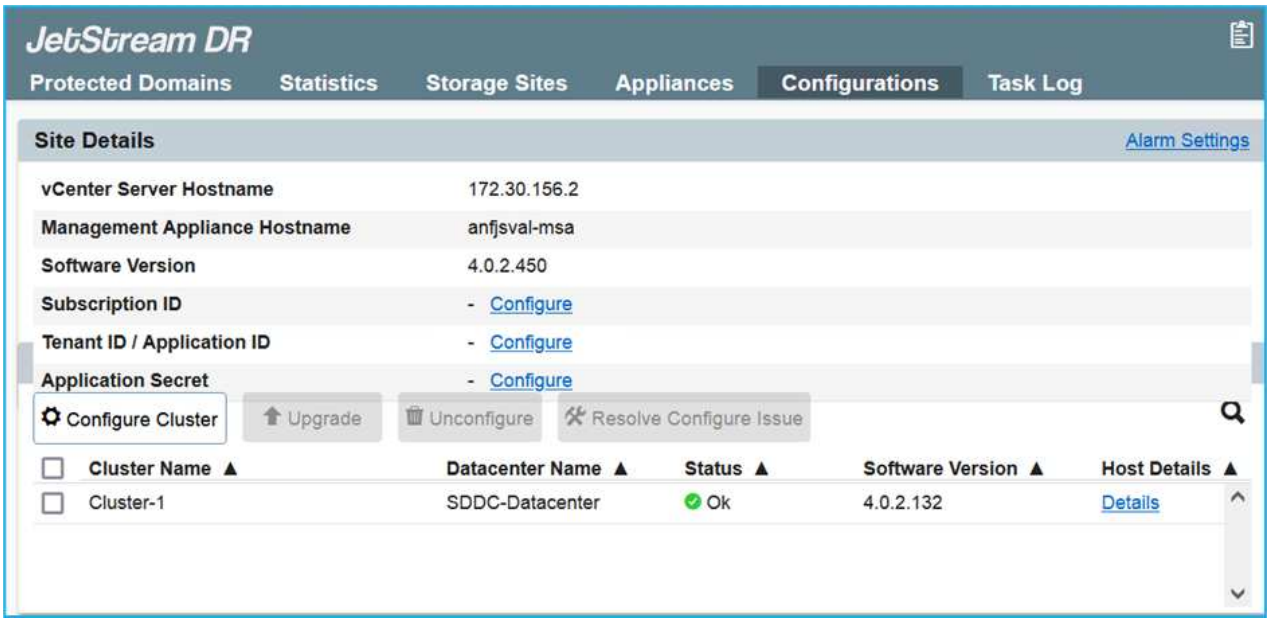
1. 要在 Azure VMware 解决方案私有云上安装 JetStream DR for AVS，请使用运行命令。从 Azure 门户转到 Azure VMware 解决方案，选择私有云，然后选择运行命令> 包> JSDR.Configuration。

   > Azure VMware 解决方案的默认 CloudAdmin 用户没有足够的权限来为 AVS 安装 JetStream DR。 Azure VMware 解决方案通过调用 JetStream DR 的 Azure VMware 解决方案运行命令，实现了 JetStream DR 的简化和自动化安装。

   以下屏幕截图显示了使用基于 DHCP 的 IP 地址的安装。

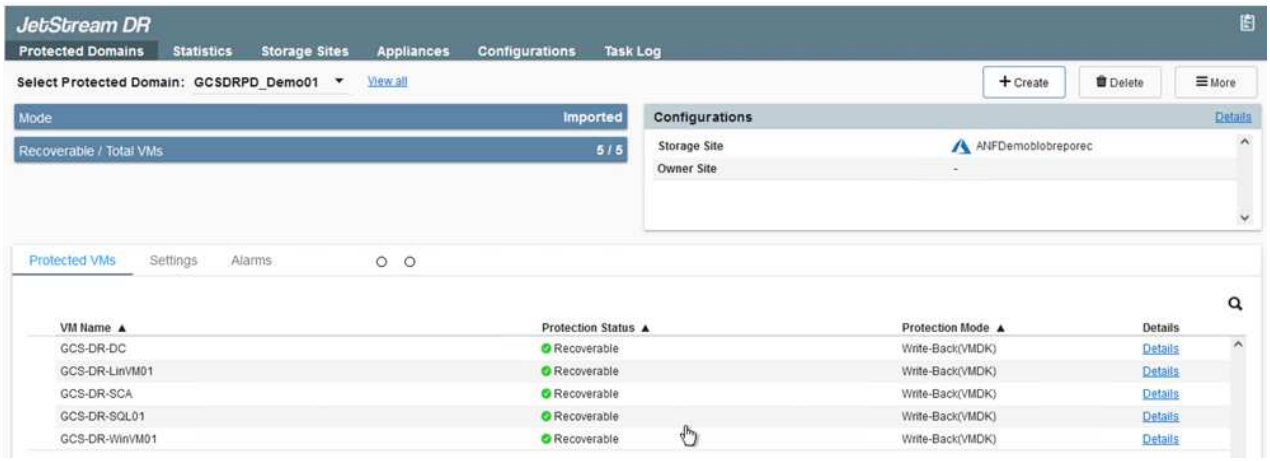


2. JetStream DR for AVS 安装完成后，刷新浏览器。要访问 JetStream DR UI，请转到 SDDC 数据中心 > 配置 > JetStream DR。



3. 从 JetStream DR 界面完成以下任务：
   a. 添加用于保护本地集群的 Azure Blob 存储帐户作为存储站点，然后运行扫描域选项。
   b. 在出现的弹出对话框窗口中，选择要导入的受保护域，然后单击其导入链接。

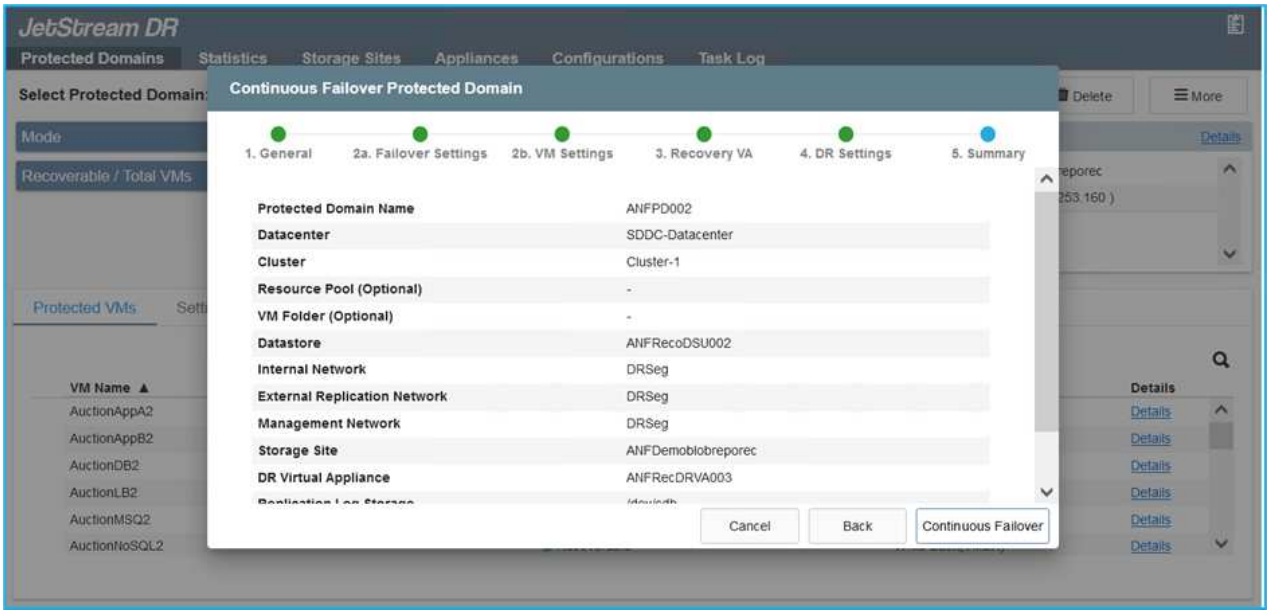
4. 该域名已导入以进行恢复。转到“受保护的域”选项卡并验证是否已选择目标域，或者从“选择受保护的域”菜单中选择所需的域。显示受保护域中可恢复的虚拟机列表。



5. 导入受保护域后，部署 DRVA 设备。

> 这些步骤也可以使用 CPT 创建的计划自动执行。

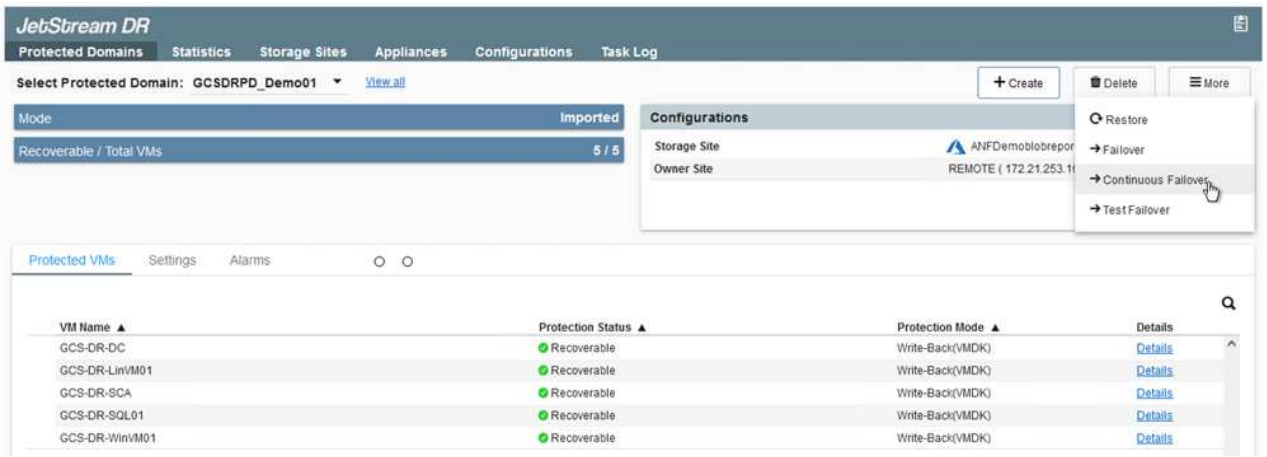
6. 使用可用的 vSAN 或 ANF 数据存储创建复制日志卷。
7. 导入受保护的域并配置恢复 VA 以使用 ANF 数据存储进行 VM 放置。



确保所选网段上启用了 DHCP，并且有足够的可用 IP。在域名恢复期间，暂时使用动态 IP。每个恢复的虚拟机（包括持续补水）都需要一个单独的动态 IP。恢复完成后，IP 被释放并可重复使用。

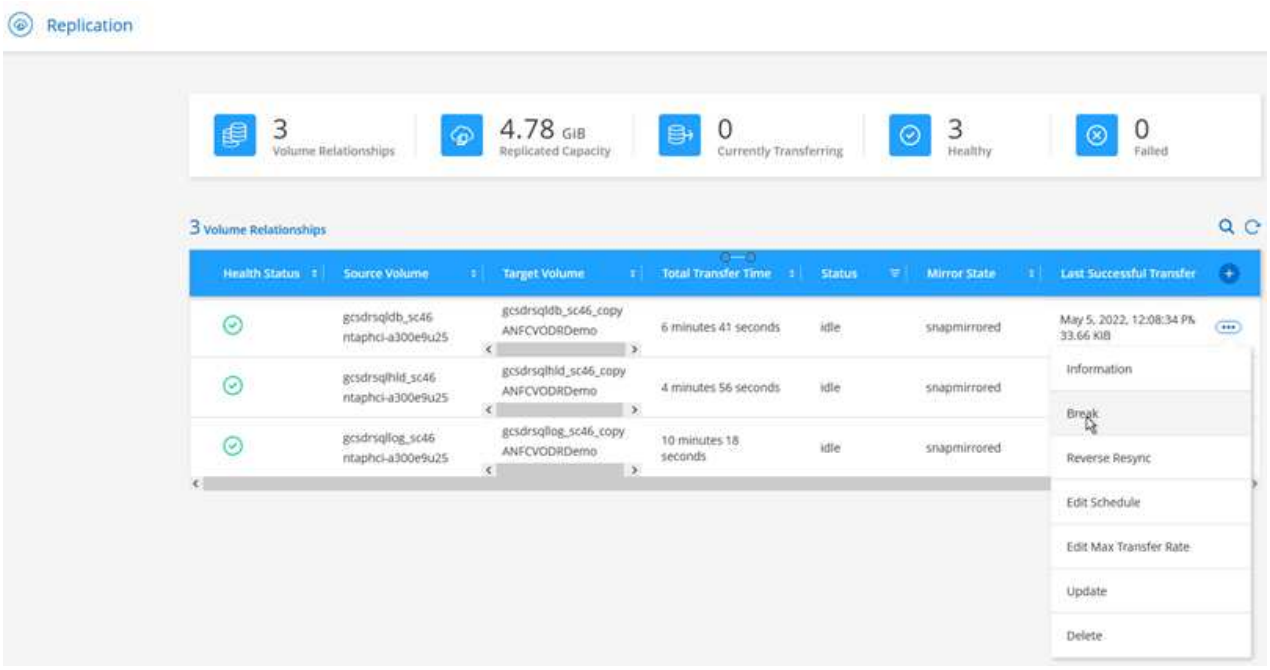
8. 选择适当的故障转移选项（连续故障转移或故障转移）。在这个例子中，选择了持续补水（持续故障转移）。

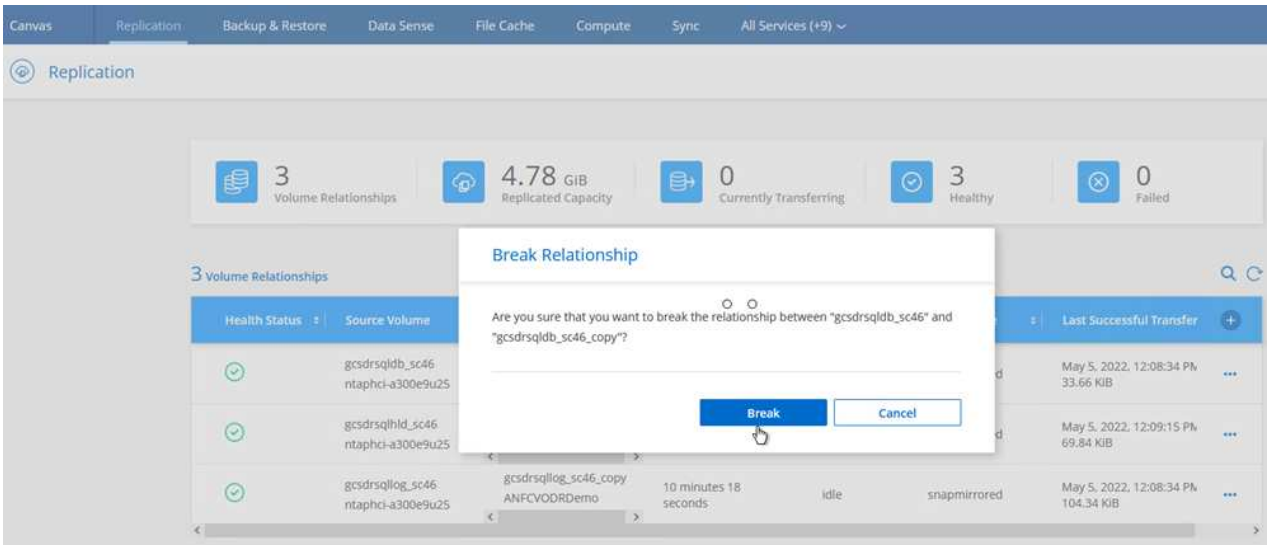
尽管连续故障转移和故障转移模式在执行配置时有所不同，但两种故障转移模式都使用相同的步骤进行配置。故障转移步骤是一起配置和执行的，以应对灾难事件。可以随时配置连续故障转移，然后允许其在正常系统运行期间在后台运行。灾难事件发生后，完成持续故障转移，立即将受保护虚拟机的所有权转移到恢复站点（接近零 RTO）。



持续故障转移过程开始，并且可以从 UI 监控其进度。单击“当前步骤”部分中的蓝色图标将打开一个弹出窗口，其中显示故障转移过程当前步骤的详细信息。

1. 当本地环境的受保护集群发生灾难（部分或全部故障）后，您可以在中断各个应用程序卷的SnapMirror关系后，使用 Jetstream 触发虚拟机的故障转移。

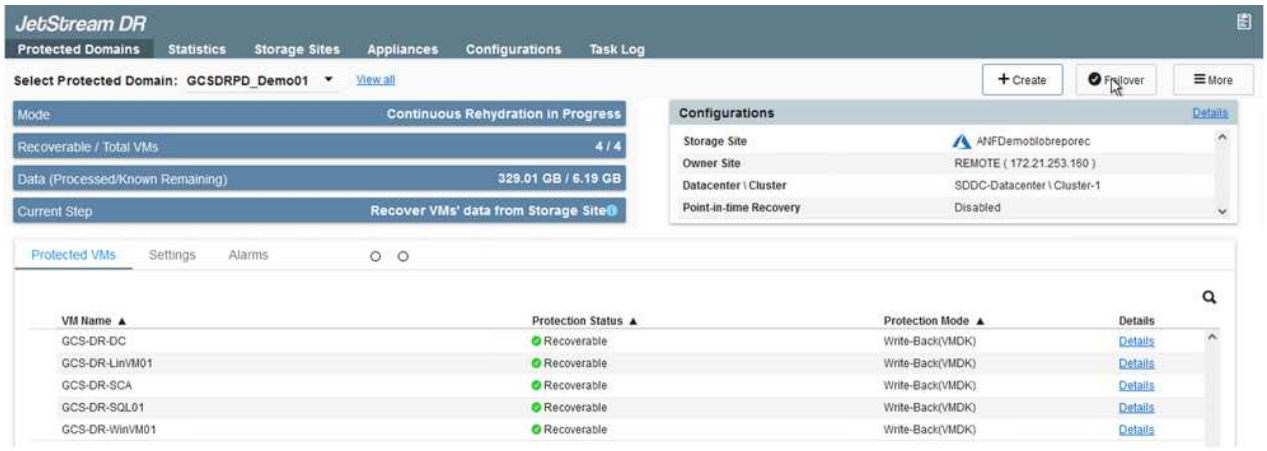


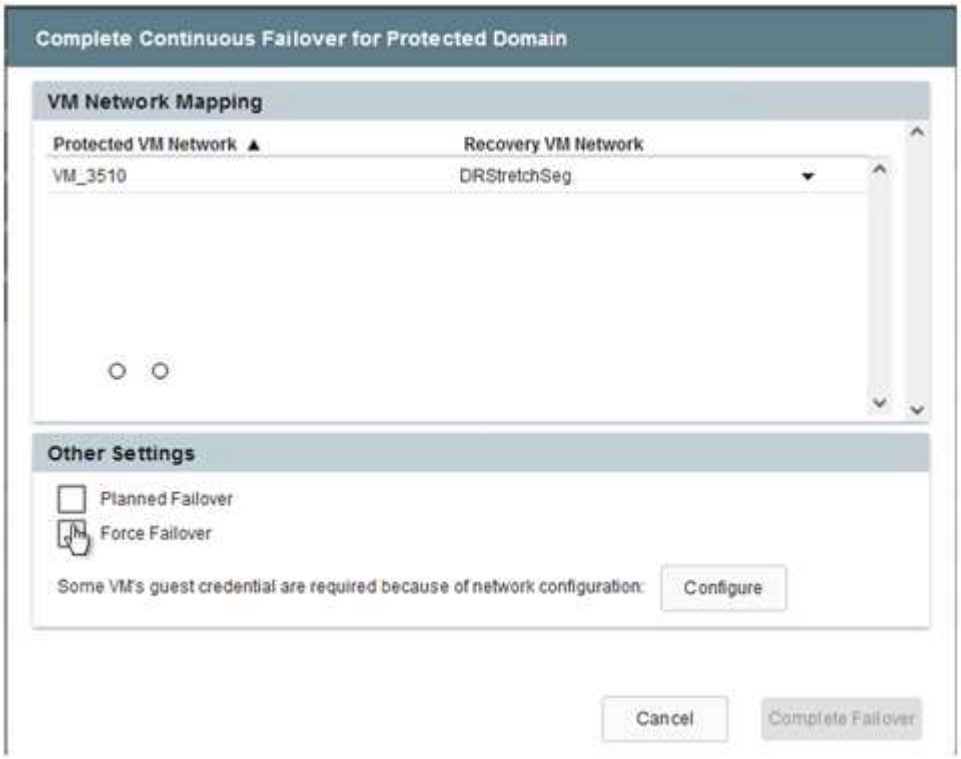


此步骤可以轻松实现自动化，以促进恢复过程。

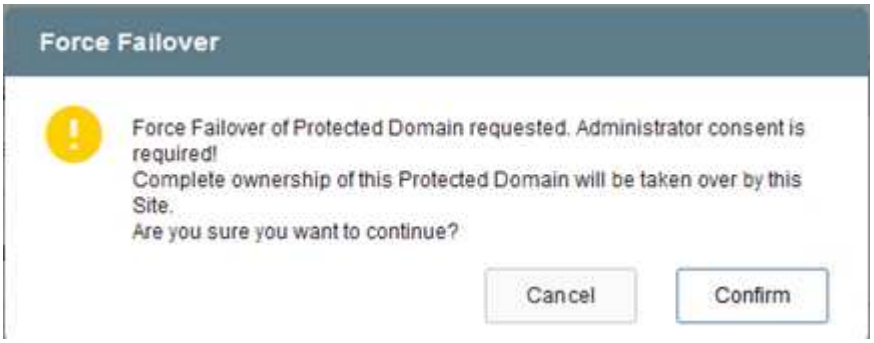
2. 访问 AVS SDDC（目标端）上的 Jetstream UI 并触发故障转移选项以完成故障转移。任务栏显示故障转移活动的进度。

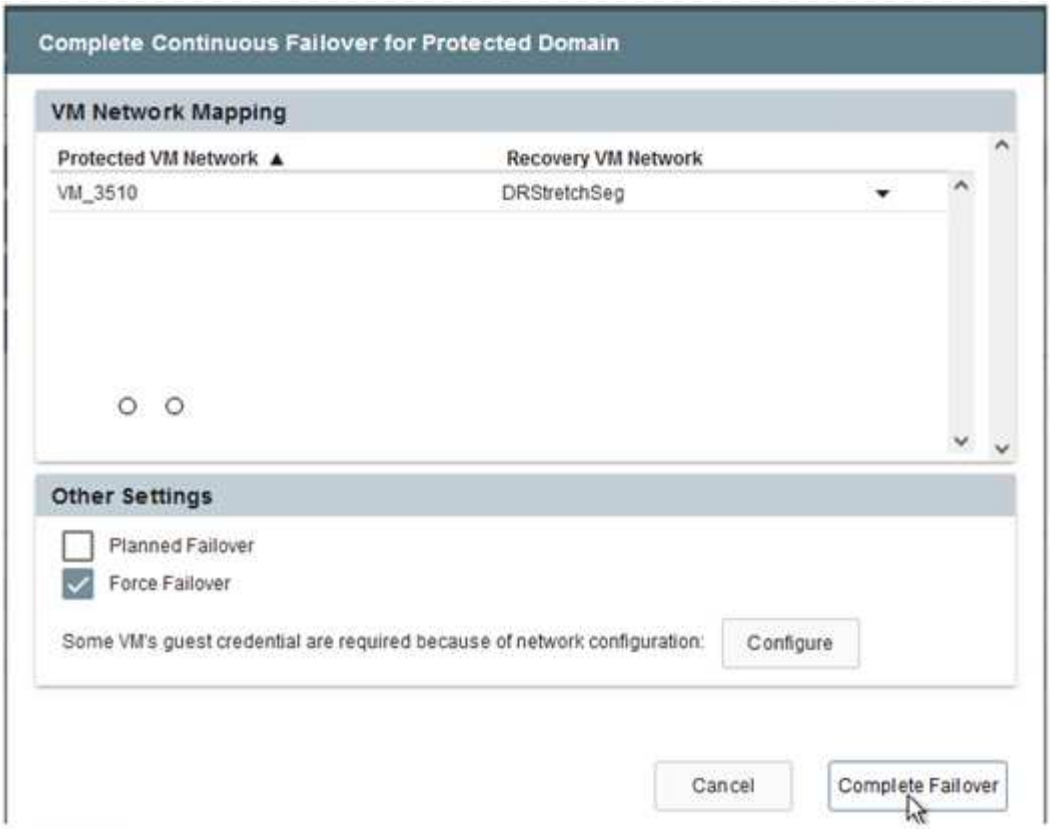
   在完成故障转移时出现的对话窗口中，可以将故障转移任务指定为计划的或假定为强制的。





强制故障转移假定主站点不再可访问，并且受保护域的所有权应由恢复站点直接承担。





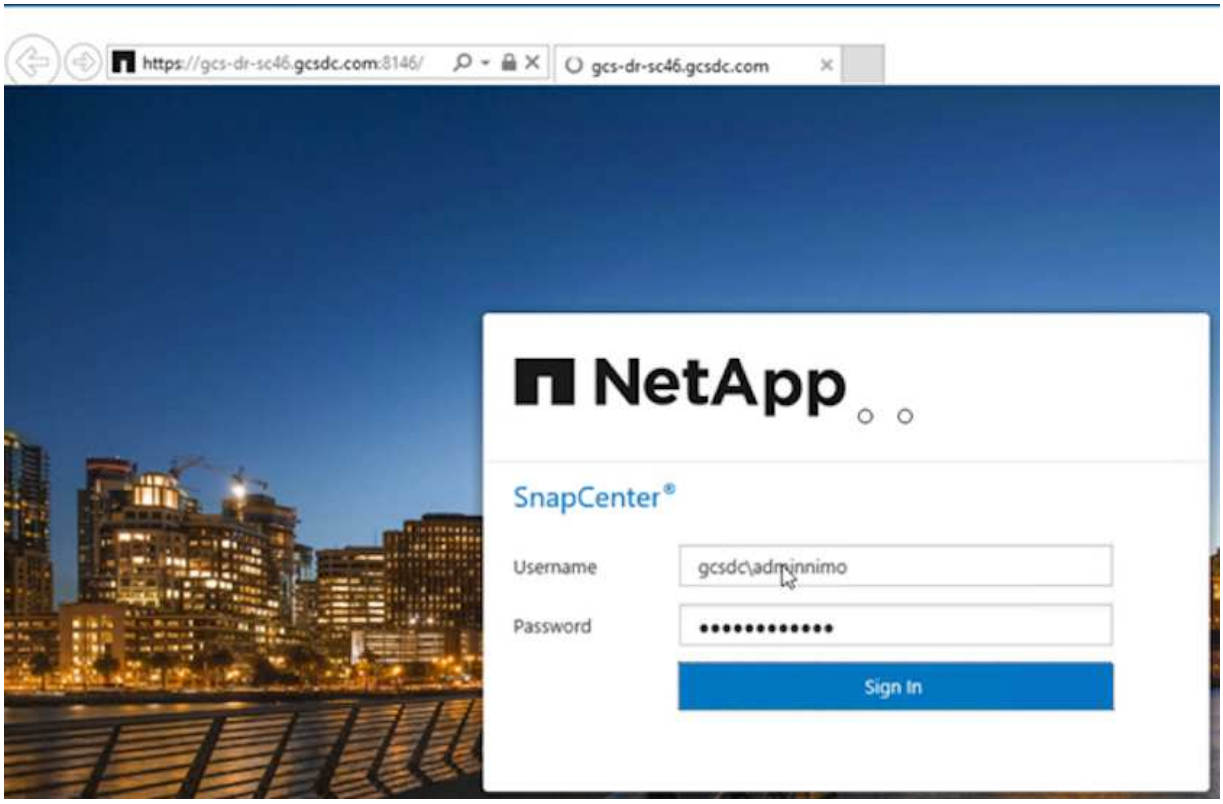
3. 连续故障转移完成后，会出现一条消息确认任务完成。任务完成后，访问恢复的虚拟机以配置 ISCSI 或 NFS 会话。

故障转移模式变为“故障转移中正在运行”，虚拟机状态变为“可恢复”。受保护域的所有虚拟机现在都在恢复站点上运行，并且处于故障转移运行手册设置指定的状态。

为了验证故障转移配置和基础设施，JetStream DR 可以在测试模式下运行（测试故障转移选项），以观察虚拟机及其数据从对象存储到测试恢复环境的恢复情况。当在测试模式下执行故障转移过程时，其操作类似于实际的故障转移过程。

4. 虚拟机恢复后，使用存储灾难恢复进行来宾存储。为了演示此过程，本例中使用了 SQL 服务器。
5. 登录 AVS SDDC 上恢复的SnapCenter VM 并启用 DR 模式。

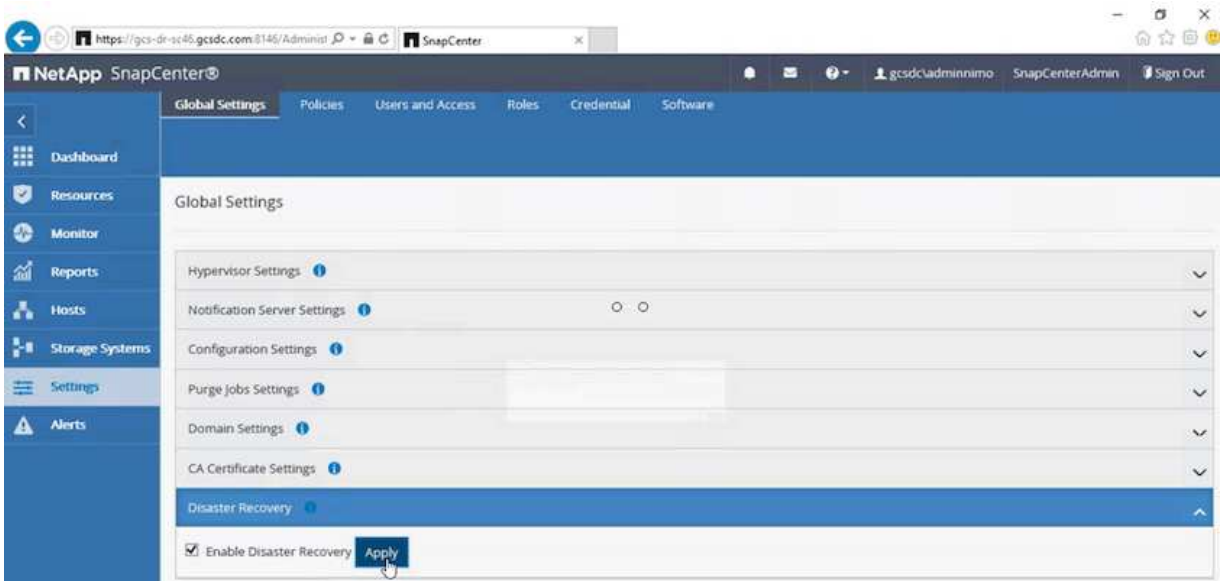
a. 使用浏览器访问SnapCenter UI。



b. 在设置页面中，导航到设置> 全局设置> 灾难恢复。

c. 选择启用灾难恢复。

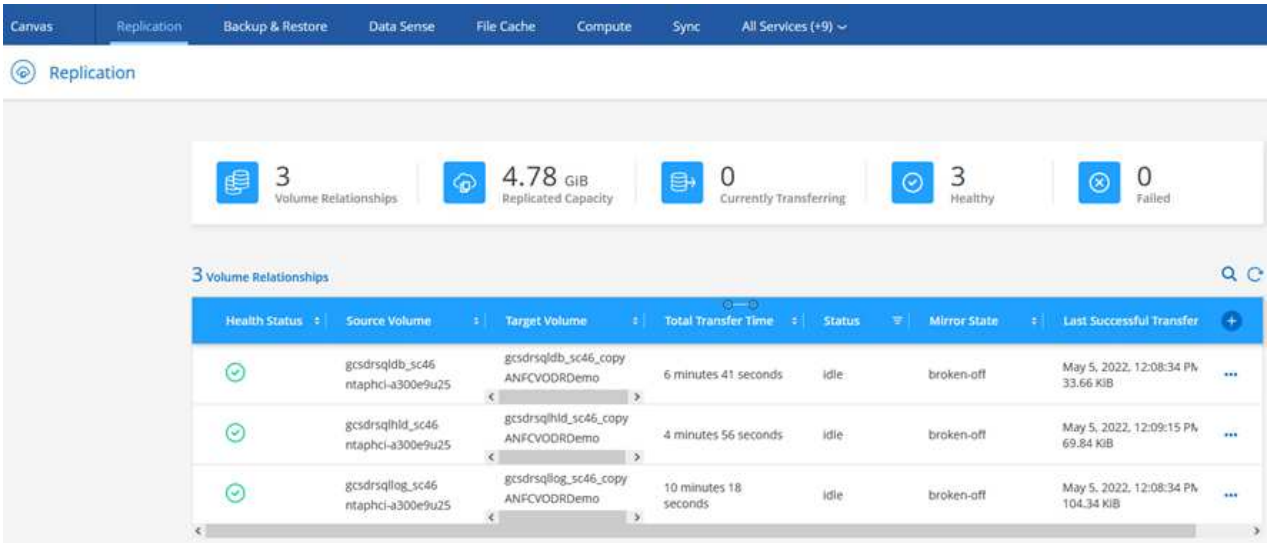
d. 单击“应用”。



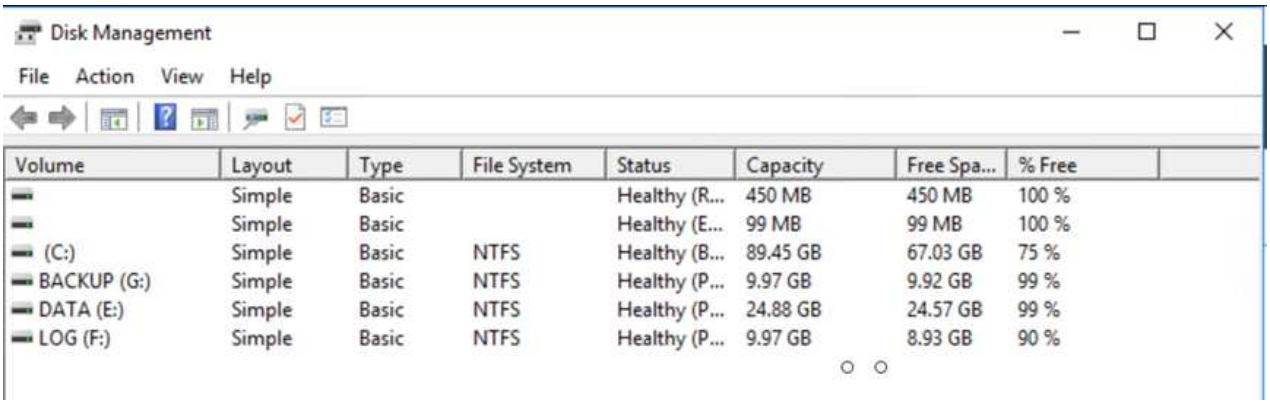
e. 单击“监视”>“作业”来验证 DR 作业是否已启用。

应使用NetApp SnapCenter 4.6 或更高版本进行存储灾难恢复。对于以前的版本，应使用应用程序一致性快照（使用SnapMirror复制），并且应执行手动恢复，以防必须在灾难恢复站点恢复以前的备份。

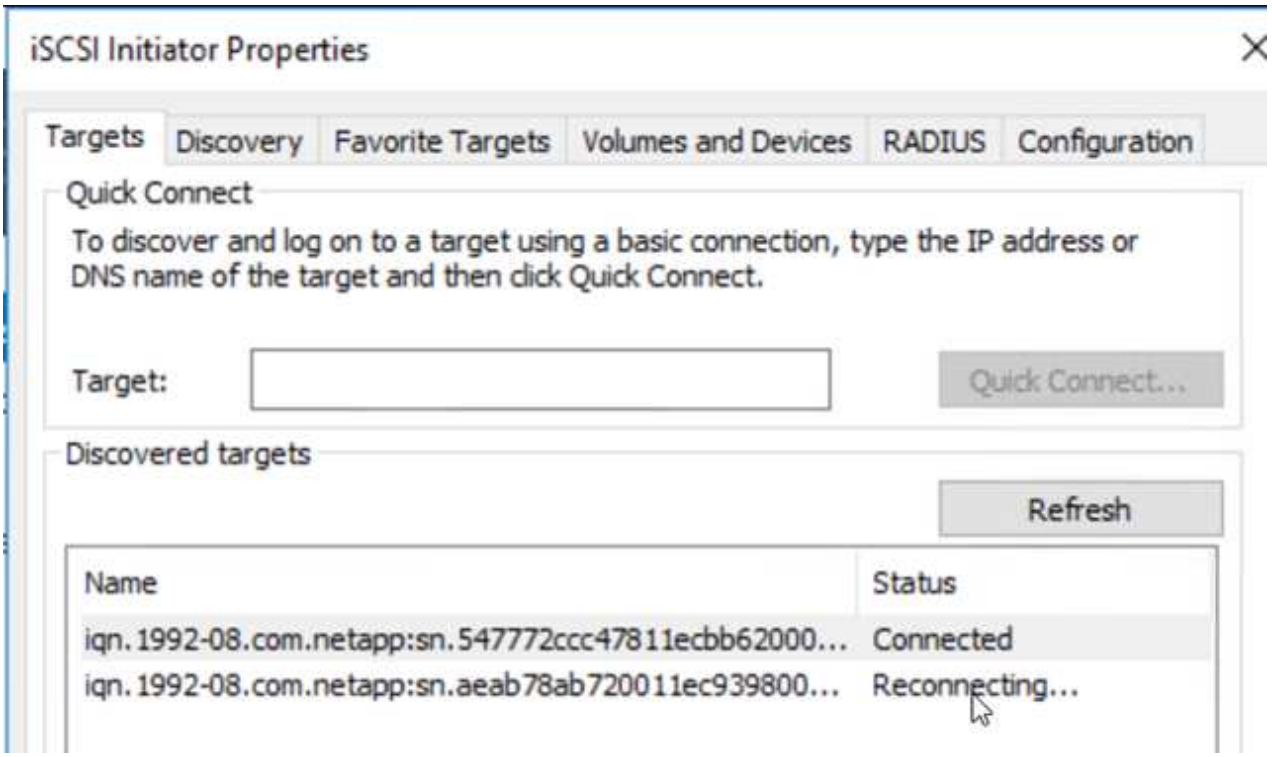
6. 确保SnapMirror关系已中断。



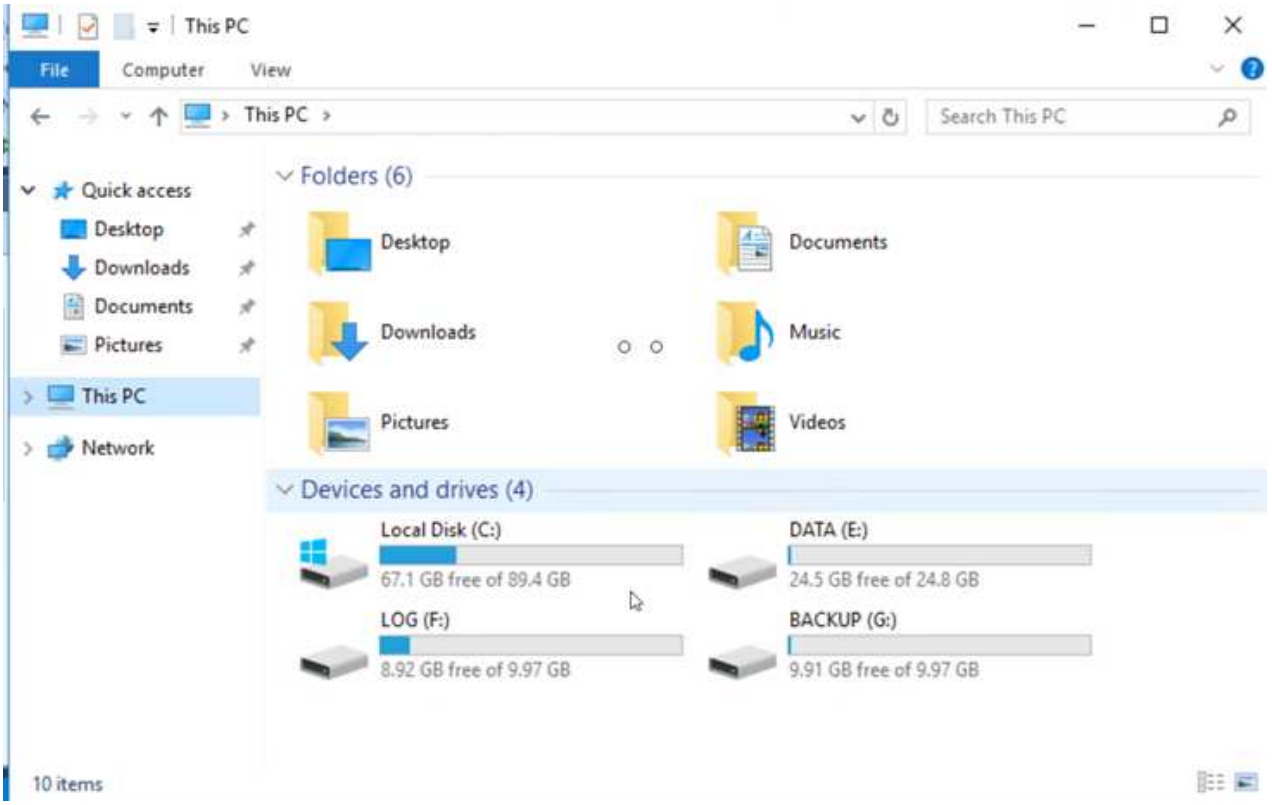
7. 将Cloud Volumes ONTAP中的 LUN 连接到具有相同驱动器号的恢复的 SQL 客户虚拟机。



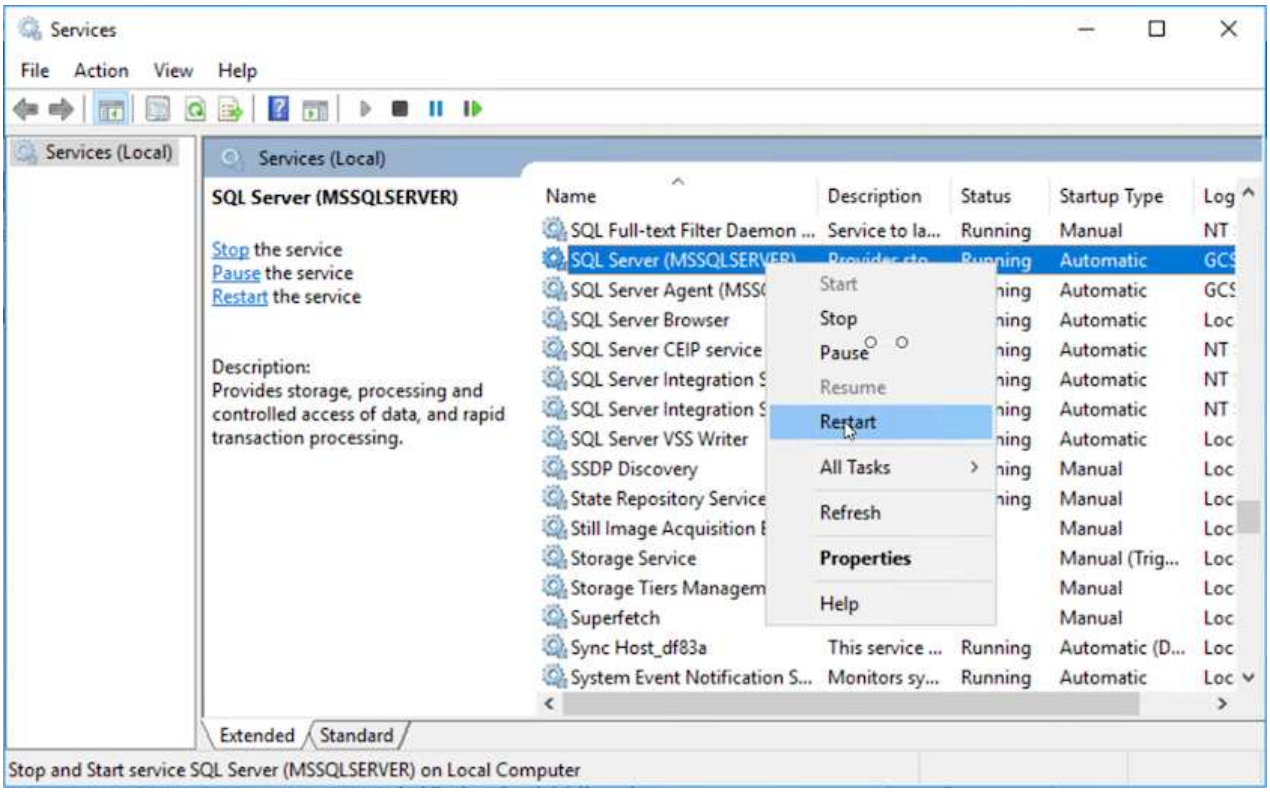
8. 打开 iSCSI 启动器，清除之前断开的会话，并为复制的Cloud Volumes ONTAP卷添加新目标以及多路径。



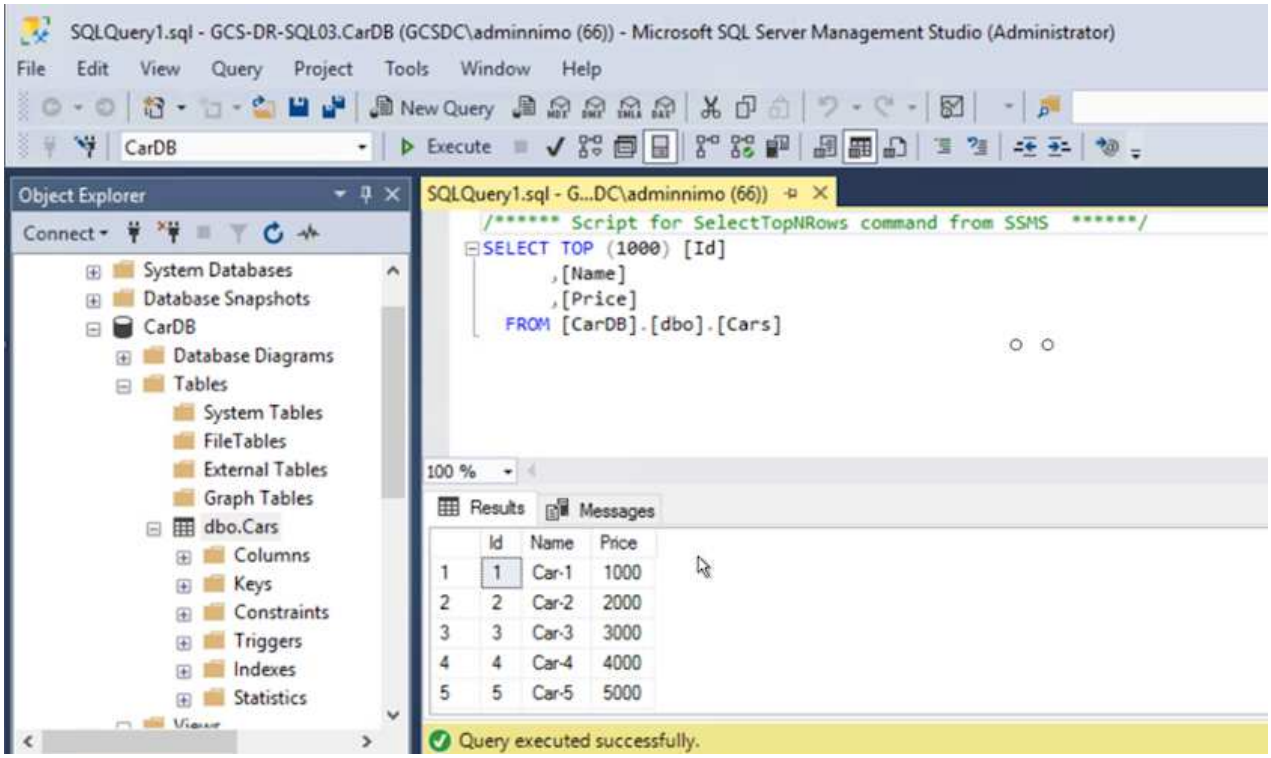
9. 确保所有磁盘都使用 DR 之前使用的相同驱动器号进行连接。



10. 重新启动 MSSQL 服务器服务。



11. 确保 SQL 资源已恢复在线。



对于 NFS，使用 mount 命令附加卷并更新 `/etc/fstab`条目。

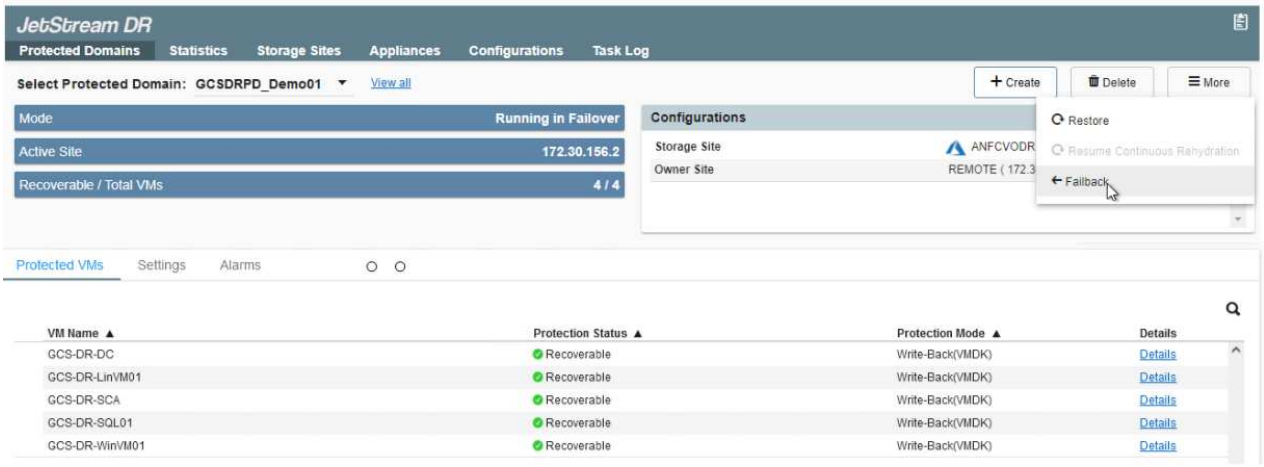
此时，操作可以运行并且业务可以继续正常进行。

在 NSX-T 端，可以创建单独的专用第 1 层网关来模拟故障转移场景。这可确保所有工作负载可以相互通信，但不会有任何流量可以路由进出环境，从而可以执行任何分类、遏制或强化任务而不会有交叉污染的风险。此操作超出了本文档的范围，但可以轻松实现模拟隔离。

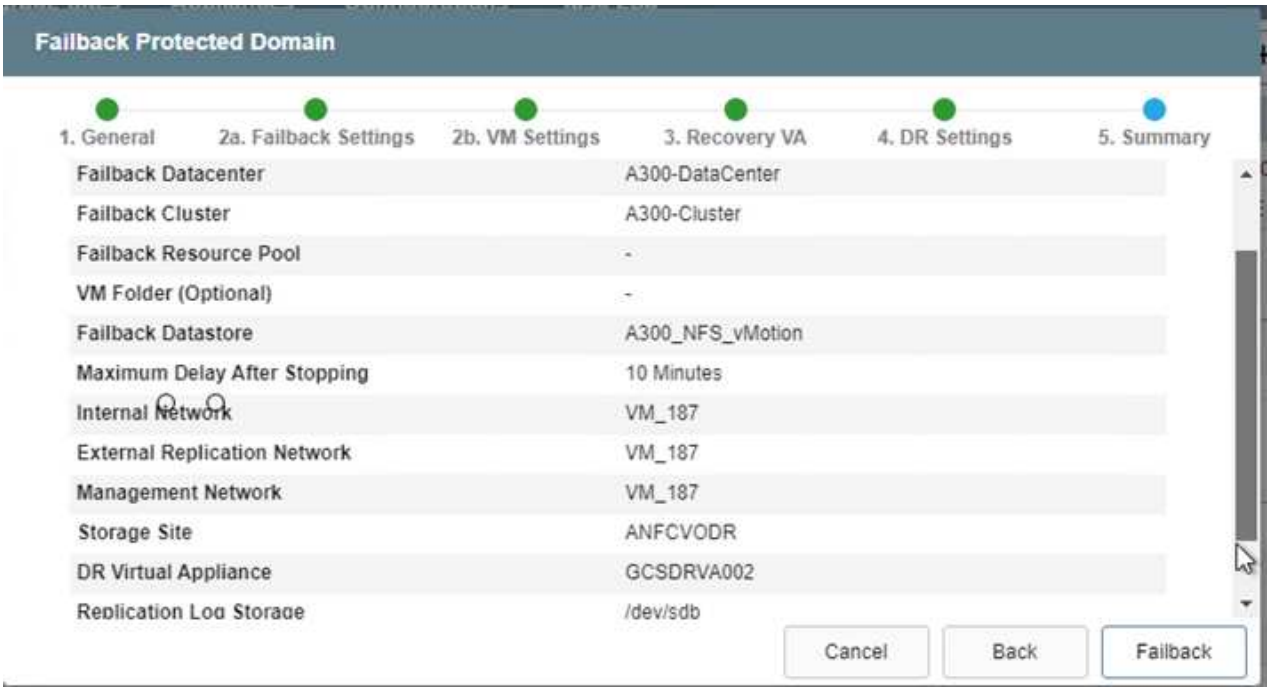
主站点重新启动并运行后，您可以执行故障恢复。 VM 保护由 Jetstream 恢复，并且必须逆转SnapMirror关系。

1. 恢复本地环境。根据灾难事件的类型，可能需要恢复和/或验证受保护集群的配置。如有必要，可能需要重新安装 JetStream DR 软件。
2. 访问恢复的本地环境，转到 Jetstream DR UI，然后选择适当的受保护域。受保护站点准备好故障恢复后，在 UI 中选择故障恢复选项。

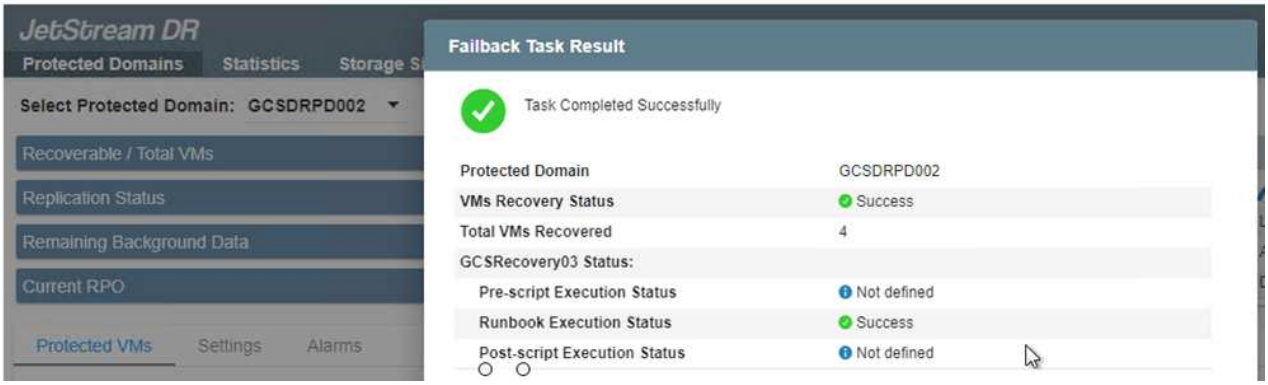
CPT 生成的故障恢复计划还可用于启动虚拟机及其数据从对象存储返回到原始 VMware 环境。



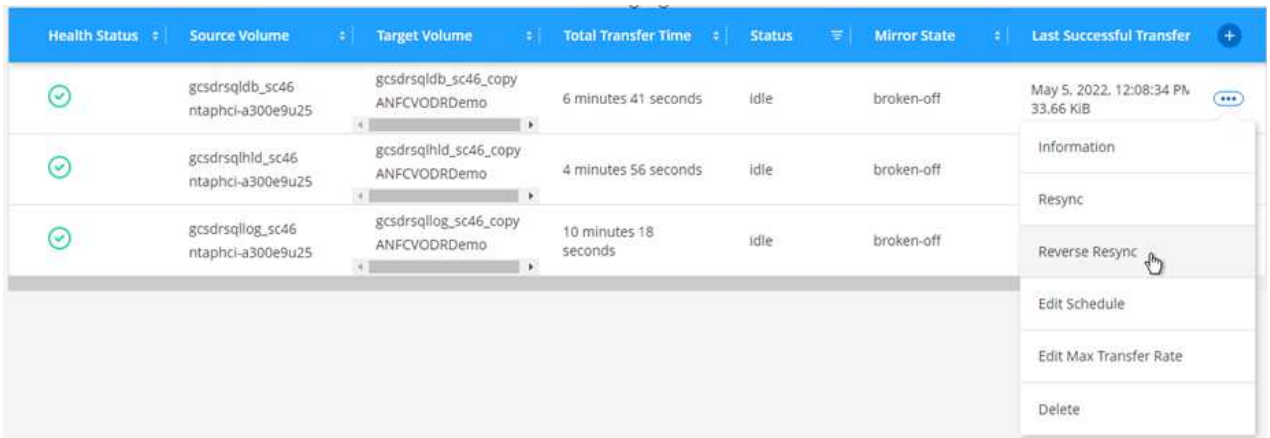
指定在恢复站点中暂停虚拟机并在受保护站点中重新启动虚拟机后的最大延迟。完成此过程所需的时间包括停止故障转移虚拟机后完成复制的时间、清理恢复站点所需的时间以及在受保护站点中重新创建虚拟机所需的时间。 NetApp建议 10 分钟。

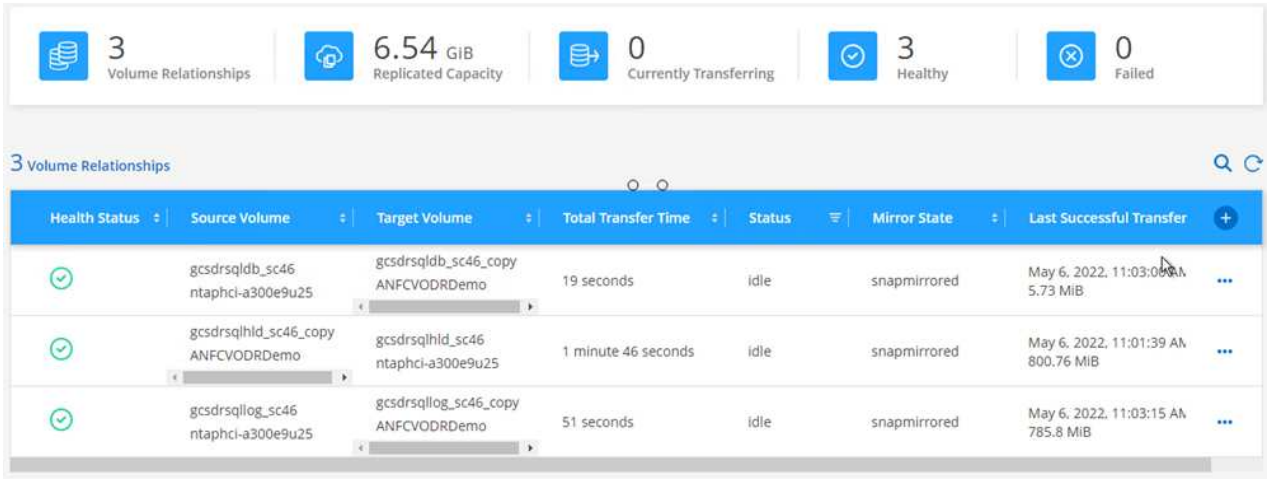


3. 完成故障恢复过程，然后确认恢复虚拟机保护和数据一致性。

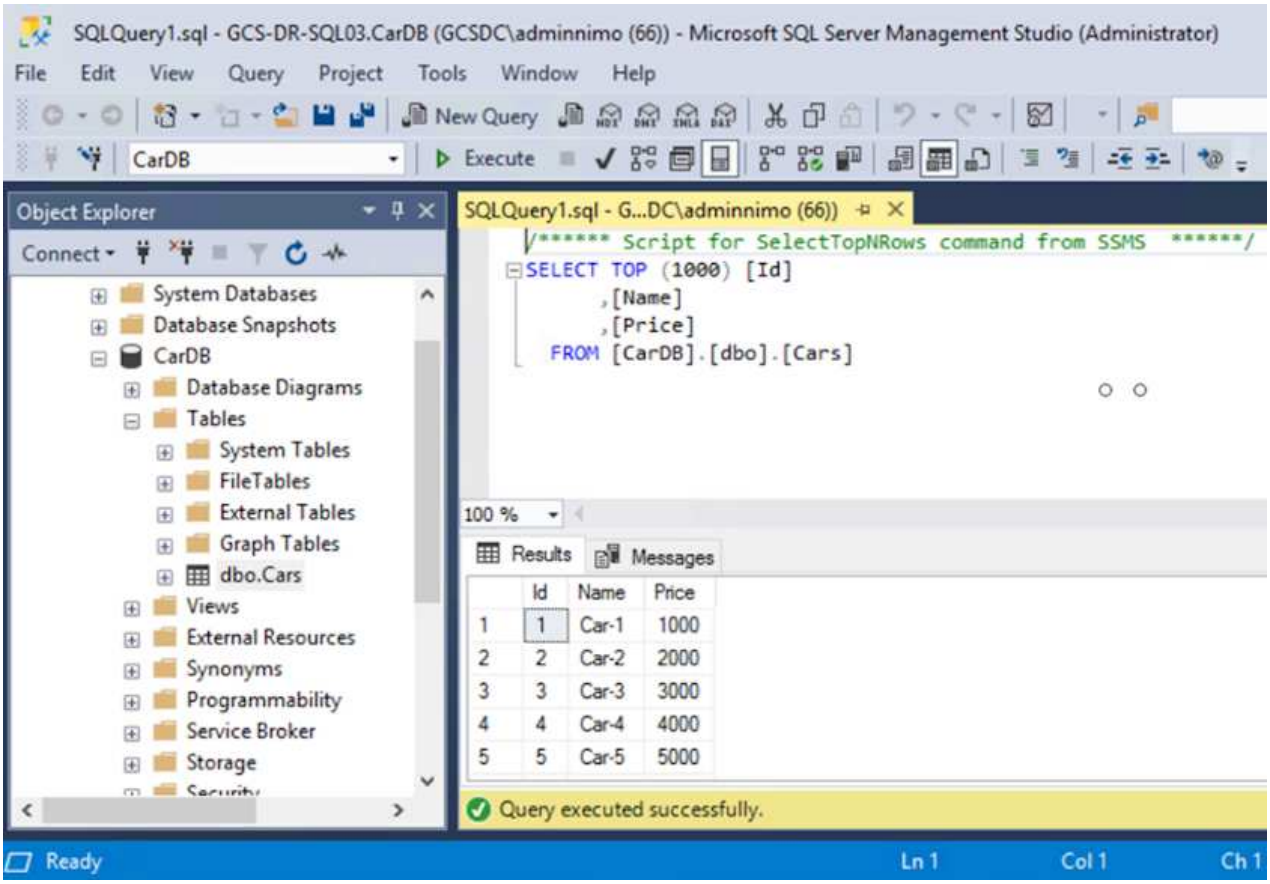


4. 虚拟机恢复后，断开辅助存储与主机的连接并连接到主存储。





5. 重新启动 MSSQL 服务器服务。
6. 验证 SQL 资源是否已恢复联机。



要故障恢复到主存储，请通过执行反向重新同步操作确保关系方向与故障转移之前保持相同。

为了在反向重新同步操作后保留主存储和辅助存储的角色，请再次执行反向重新同步操作。

此过程适用于其他应用程序，如 Oracle、类似的数据库类型以及任何其他使用来宾连接存储的应用程序。

与往常一样，在将关键工作负载转移到生产环境之前，请先测试恢复所涉及的步骤。

此解决方案的优势

- 使用SnapMirror的高效且有弹性的复制。
- 通过ONTAP快照保留恢复到任何可用的时间点。
- 从存储、计算、网络和应用程序验证步骤，恢复数百到数千台虚拟机所需的所有步骤均可实现完全自动化。
- SnapCenter使用不会改变复制卷的克隆机制。
  - 这避免了卷和快照数据损坏的风险。
  - 避免 DR 测试工作流程期间的复制中断。
  - 利用 DR 数据进行 DR 以外的工作流程，例如开发/测试、安全测试、补丁和升级测试以及补救测试。
- CPU 和 RAM 优化可以通过恢复到较小的计算集群来帮助降低云成本。