保护AzAzure / AVS上的工作负载

NetApp Solutions

NetApp
April 12, 2024

目录

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。

解决方案 部署概述

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。

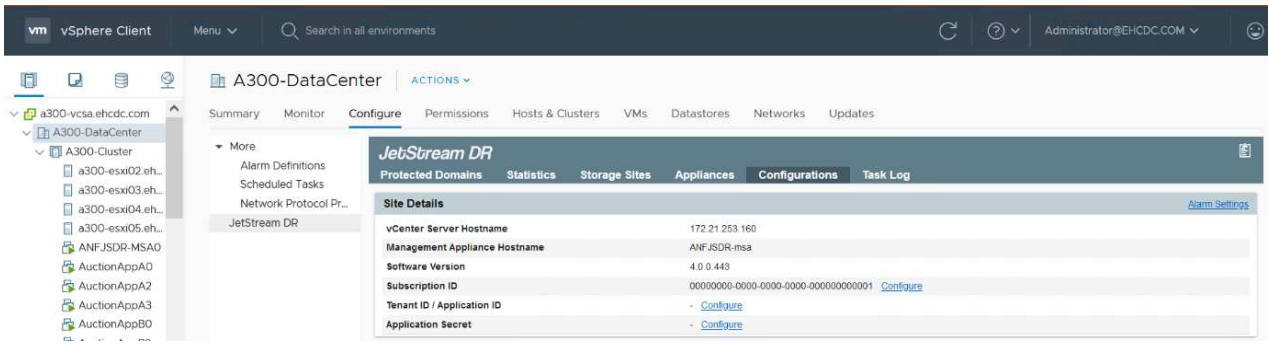
> 规定的域数量和内容取决于各种VM特征、例如平均IOPS、总容量、优先级(用于定义故障转移顺序)、RTO等。

在内部数据中心中安装Jetstream DR

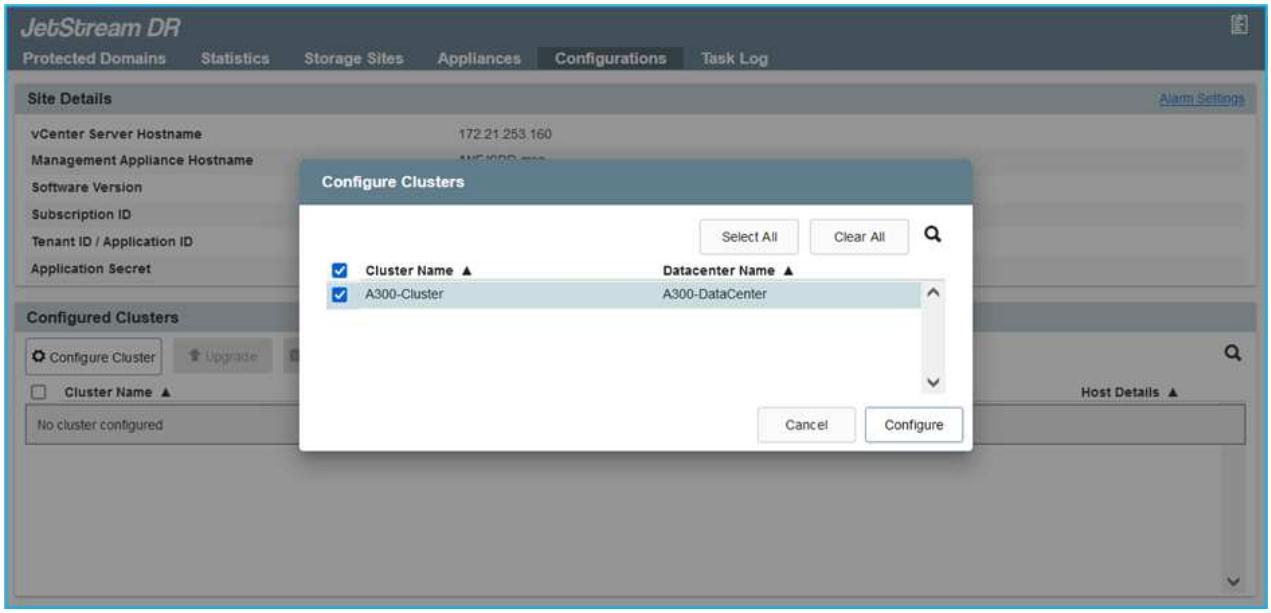
Jetstream灾难恢复软件由三个主要组件组成：Jetstream灾难恢复管理服务器虚拟设备(Virtual Appliance、MSA)、灾难恢复虚拟设备(DR Virtual Appliance、DRVA)和主机组件(I/O筛选器软件包)。MSA用于在计算集群上安装和配置主机组件、然后管理Jetstream DR软件。以下列表提供了安装过程的高级问题描述：

如何为内部环境安装**Jetstream DR**

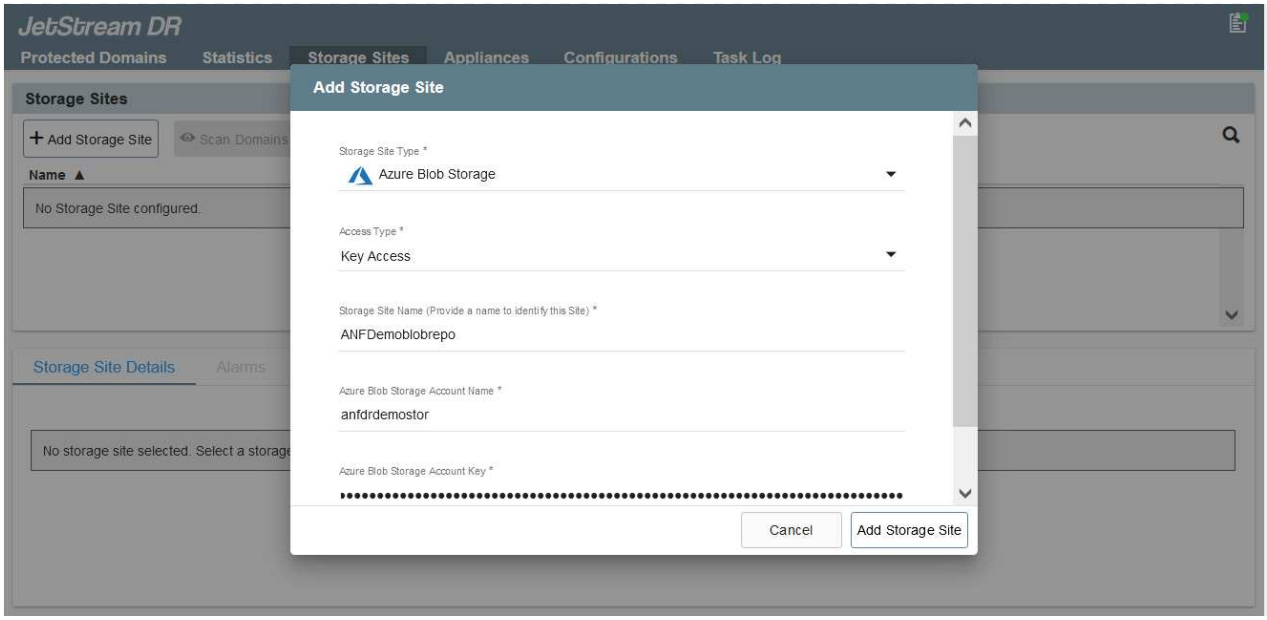
1. 检查前提条件。
2. 运行容量规划工具以获取资源和配置建议(可选、但建议用于概念验证试用)。
3. 将Jetstream DR MSA部署到指定集群中的vSphere主机。
4. 在浏览器中使用其DNS名称启动MSA。
5. 向MSA注册vCenter Server。要执行安装、请完成以下详细步骤：
6. 部署Jetstream DR MSA并注册vCenter Server后、请使用vSphere Web Client访问Jetstream DR插件。可通过导航到"数据中心">"配置">"Jetstream DR"来完成此操作。



7. 从Jetstream灾难恢复界面中、选择相应的集群。



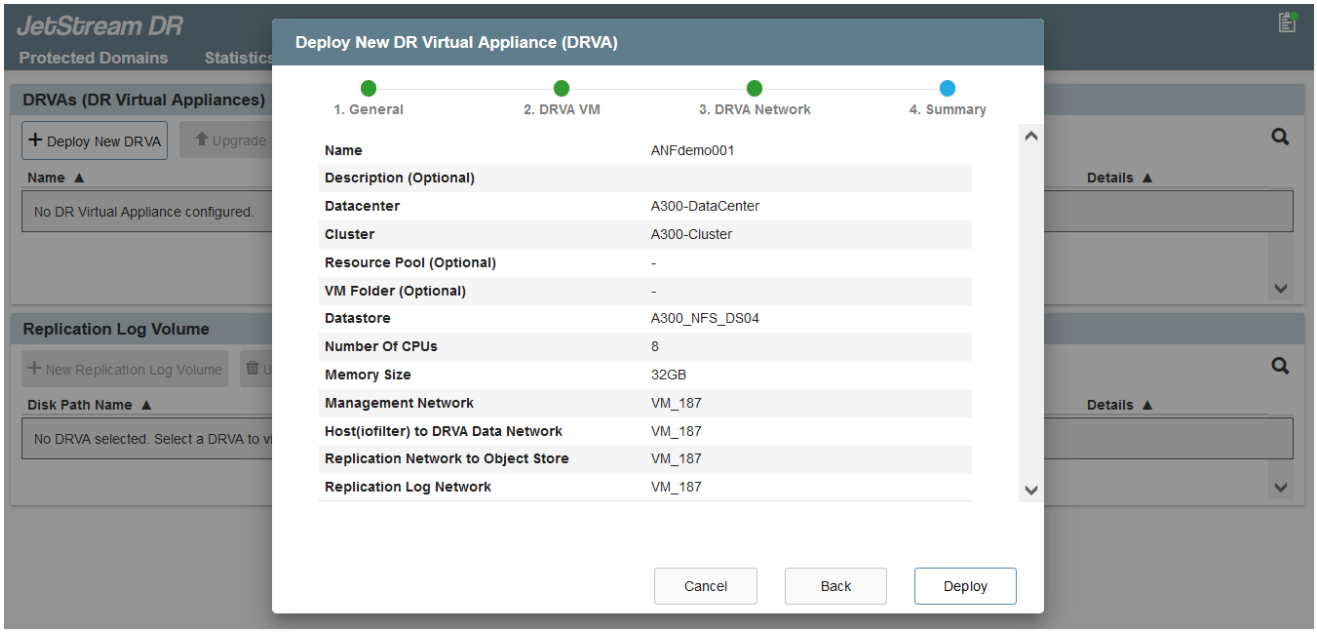
8. 使用I/O筛选器软件包配置集群。



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)。

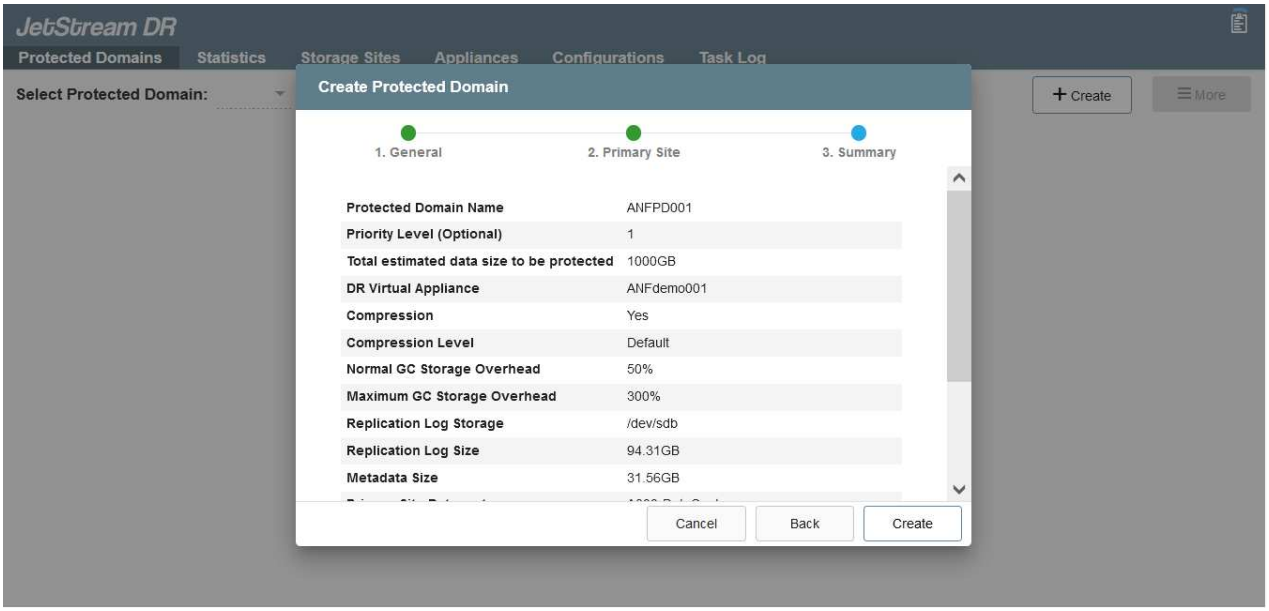
Jetstream DRVA是一个虚拟设备、可促进数据复制过程中的关键功能。受保护集群必须至少包含一个DRVA、通常每个主机配置一个DRVA。每个DRVA都可以管理多个受保护域。



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

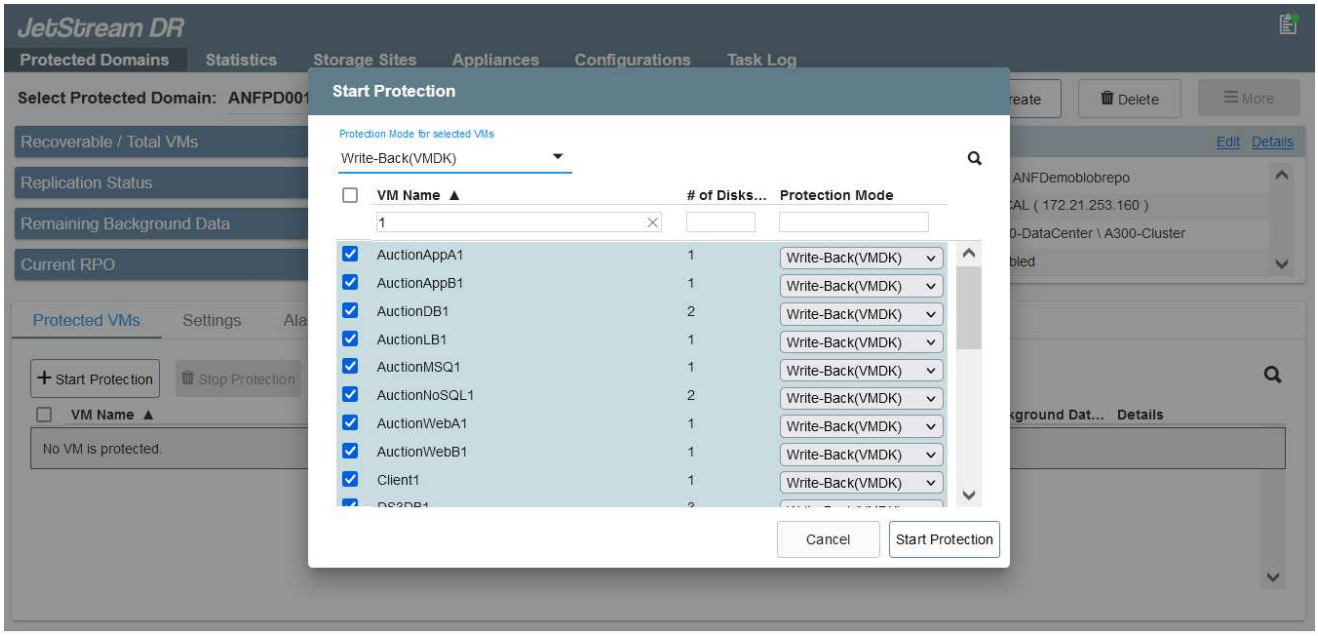
分配优先级顺序。



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。

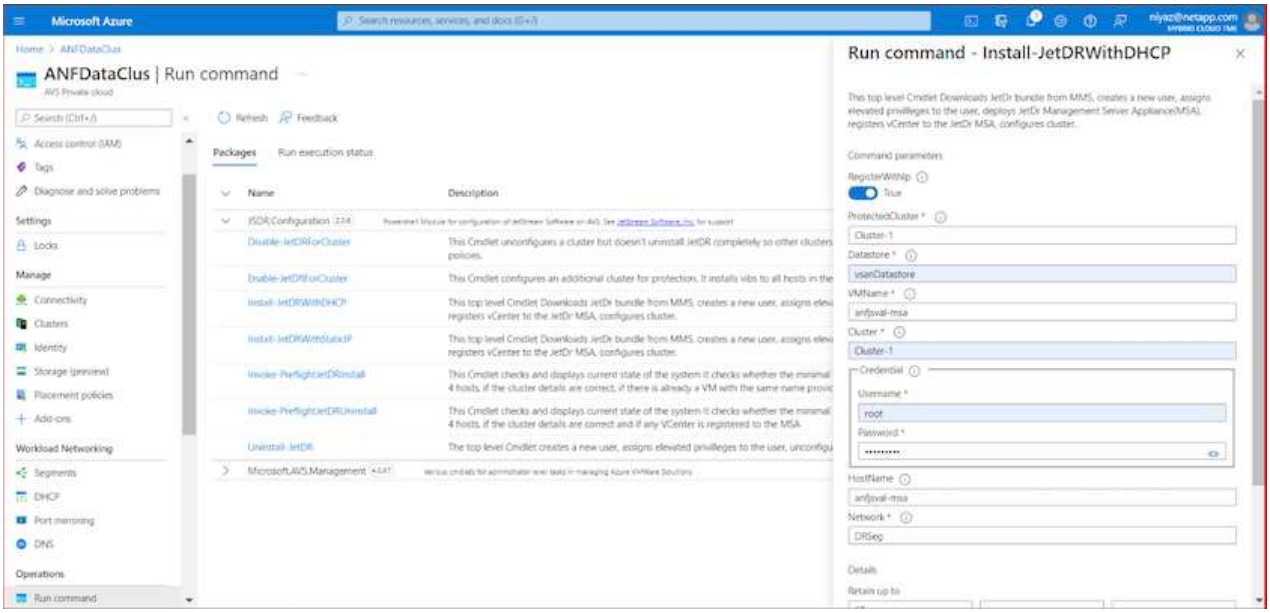
如何在私有云中安装**Jetstream DR for AVS**

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：

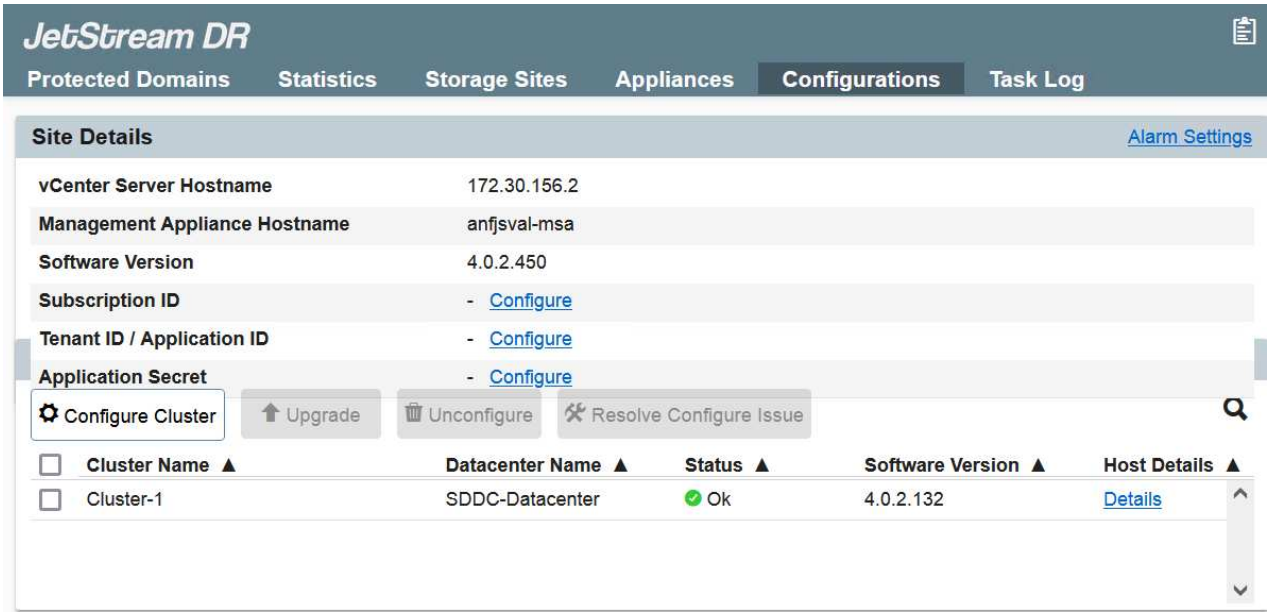
1. 从Azure门户中、转到Azure VMware解决方案 、选择私有云、然后选择运行命令>软件包> JSDR.Configuration。

> 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。

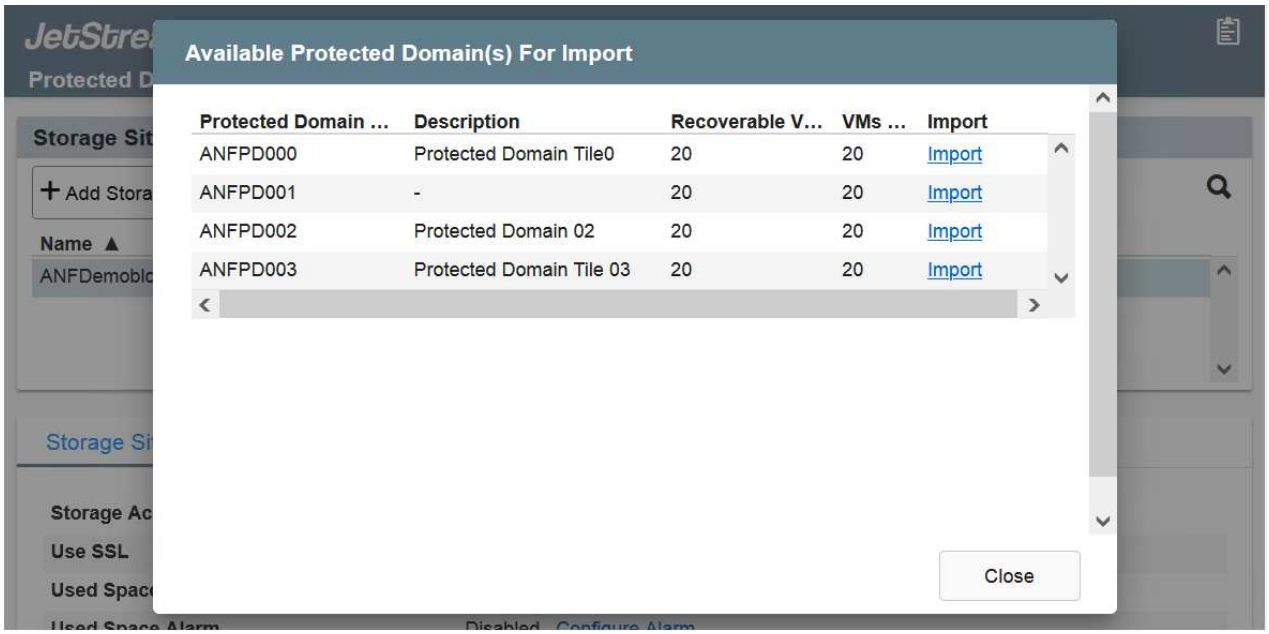
以下屏幕截图显示了使用基于DHCP的IP地址进行安装的情况。



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。



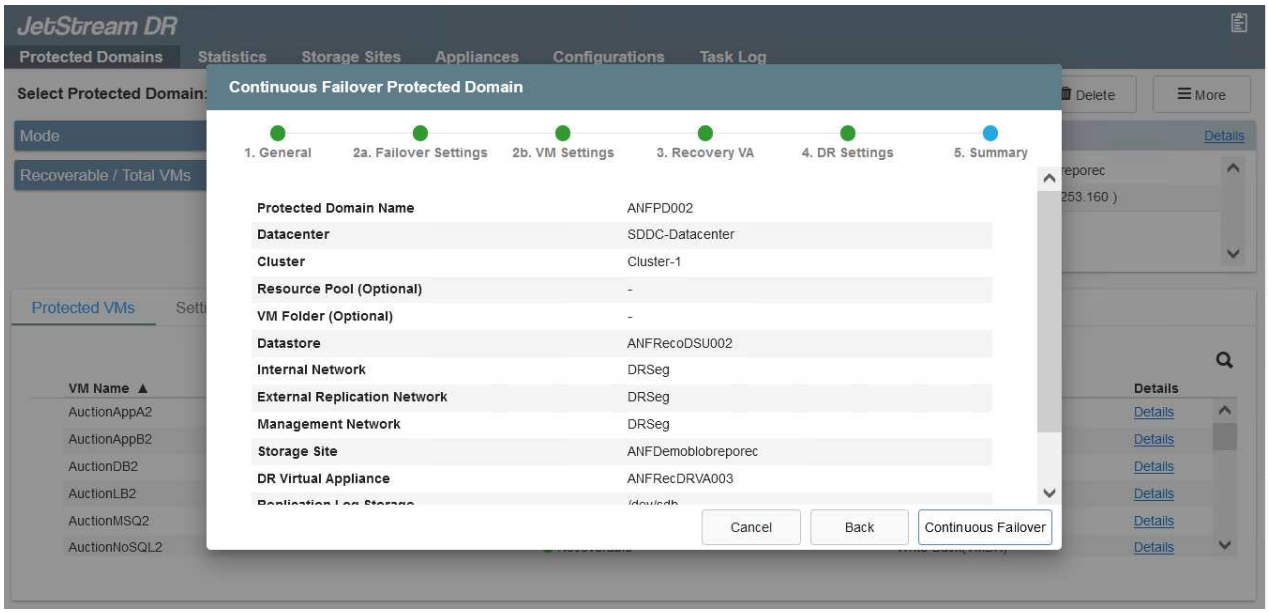
3. 从Jetstream DR界面中、添加用于将内部集群作为存储站点进行保护的Azure Blob Storage帐户、然后运行扫描域选项。



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。

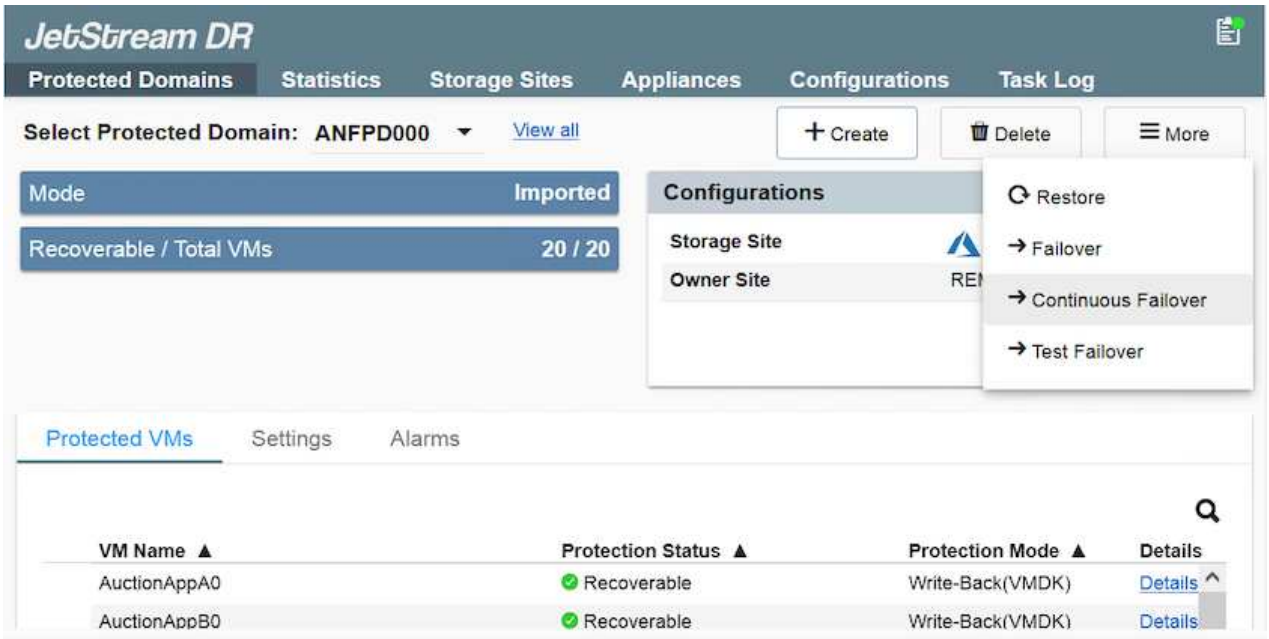
> 也可以使用CPT创建的计划自动执行这些步骤。

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)。



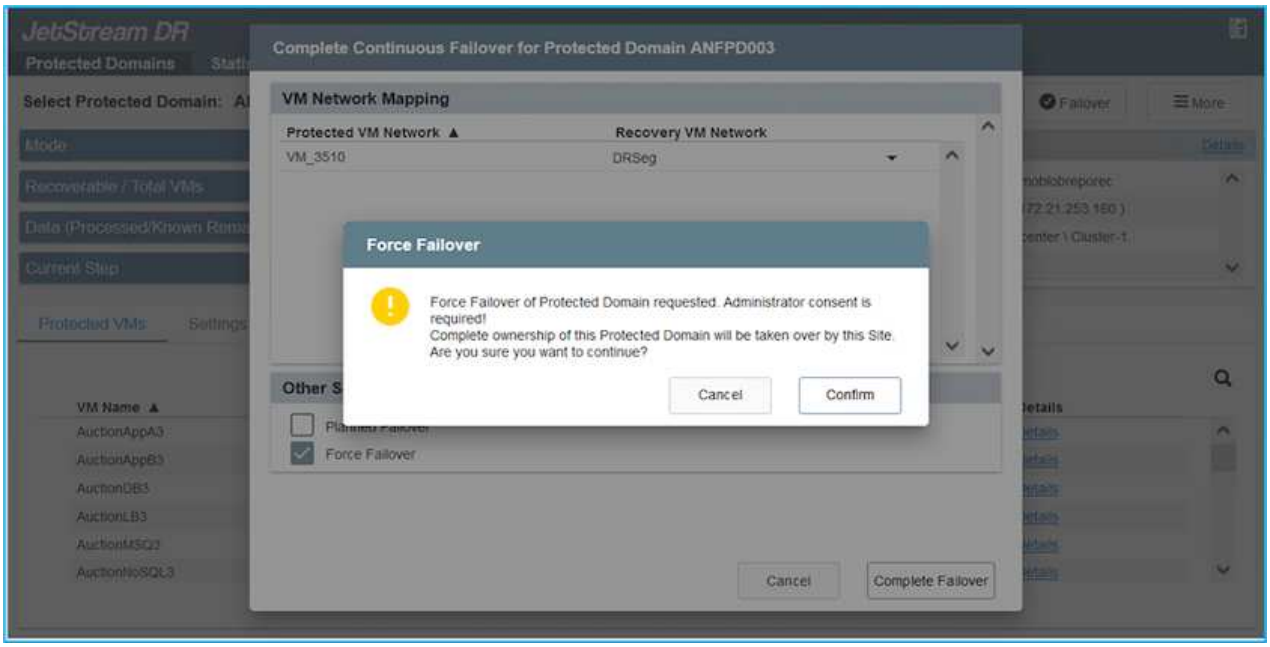
正在执行故障转移/故障恢复

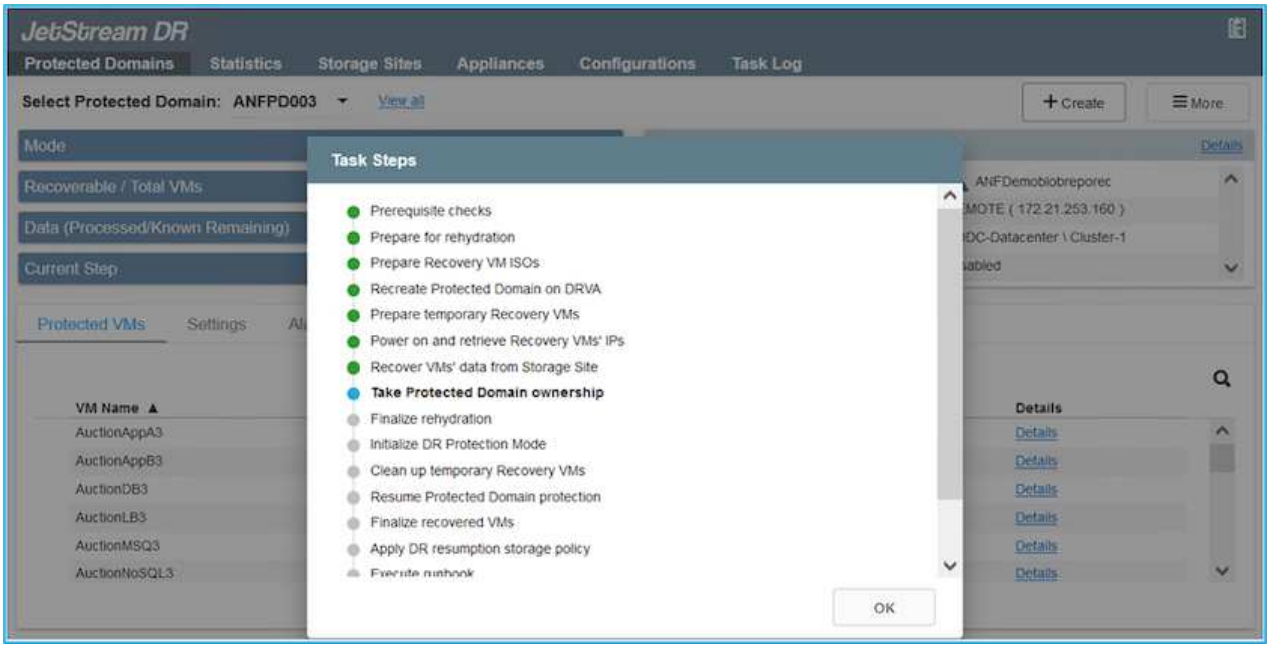
如何执行故障转移/故障恢复

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。

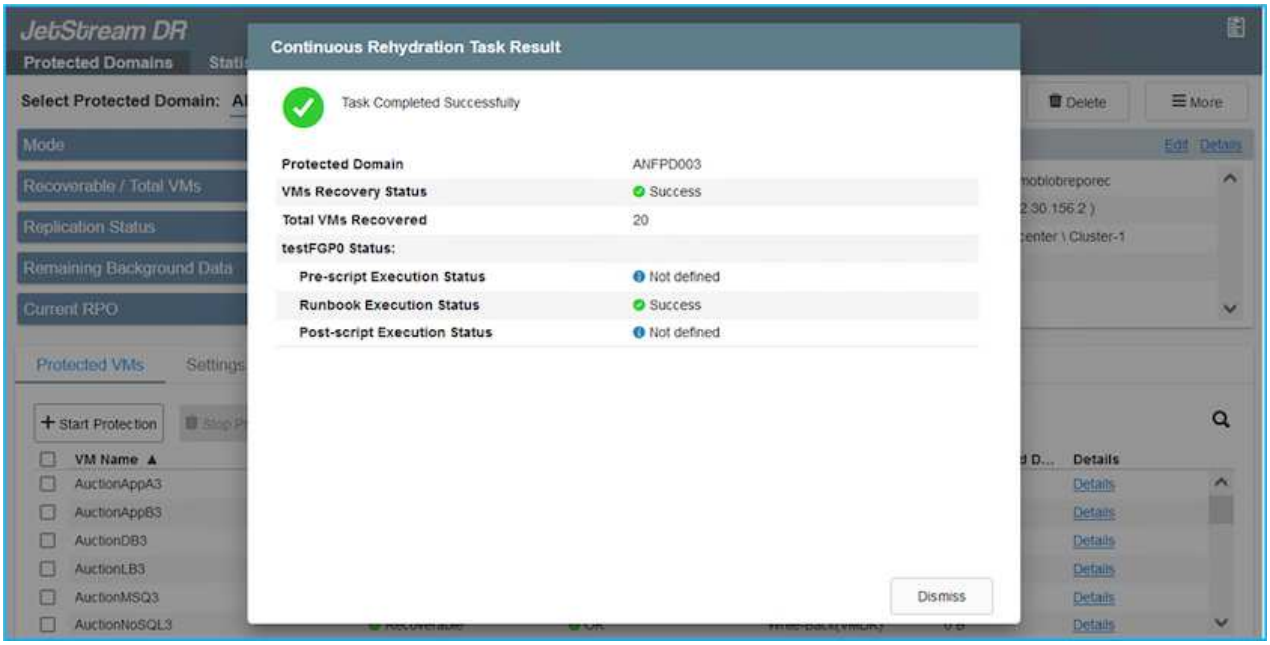
> 在AVS中启动受保护的VM后进行故障转移(针对持续或标准再融合)、保护将自动恢复、Jetstream DR将继续将其数据复制到Azure Blob Storage中的相应/原始容器中。





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。

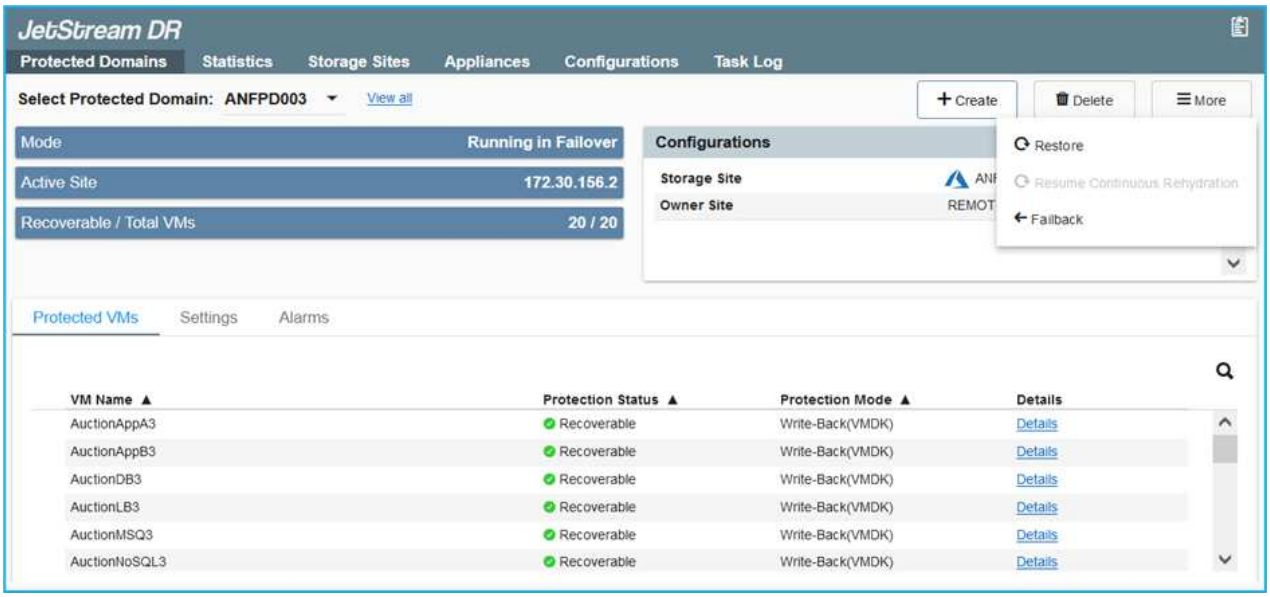


主站点启动并重新运行后、可以执行故障恢复。VM保护将恢复、应检查数据一致性。

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。



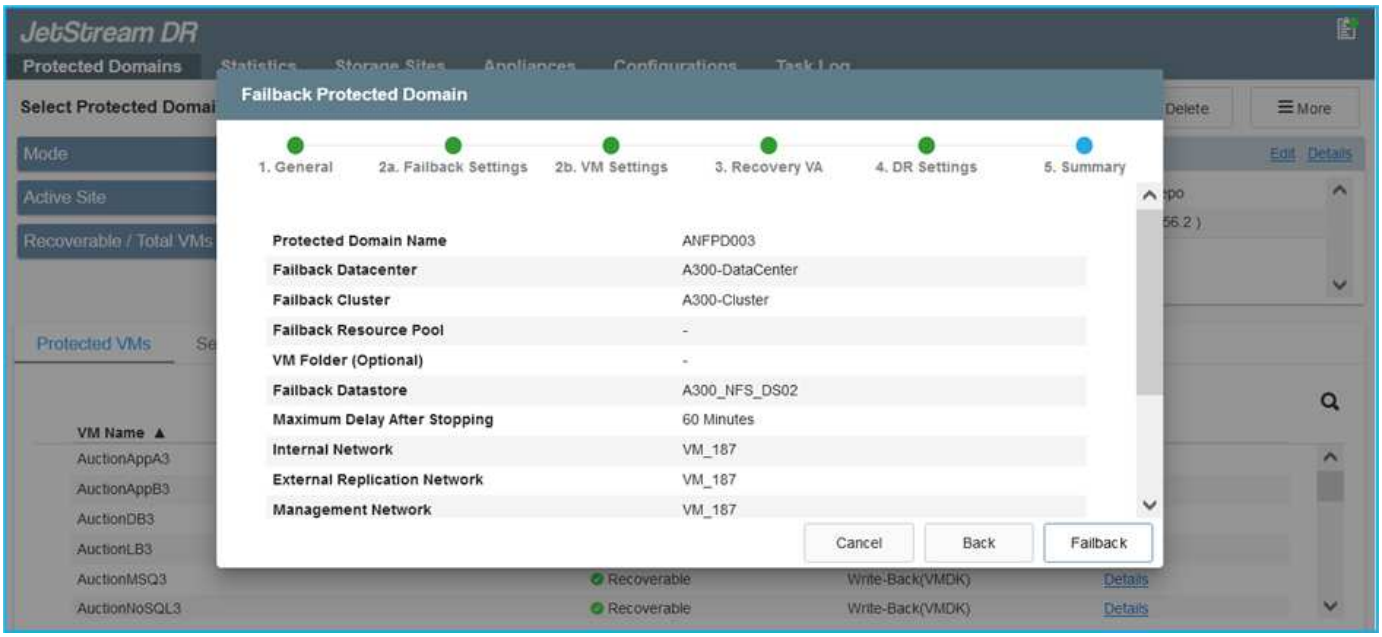
> CPT生成的故障恢复计划还可用于启动VM及其数据从对象存储返回到原始VMware环境的操作。

> 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。



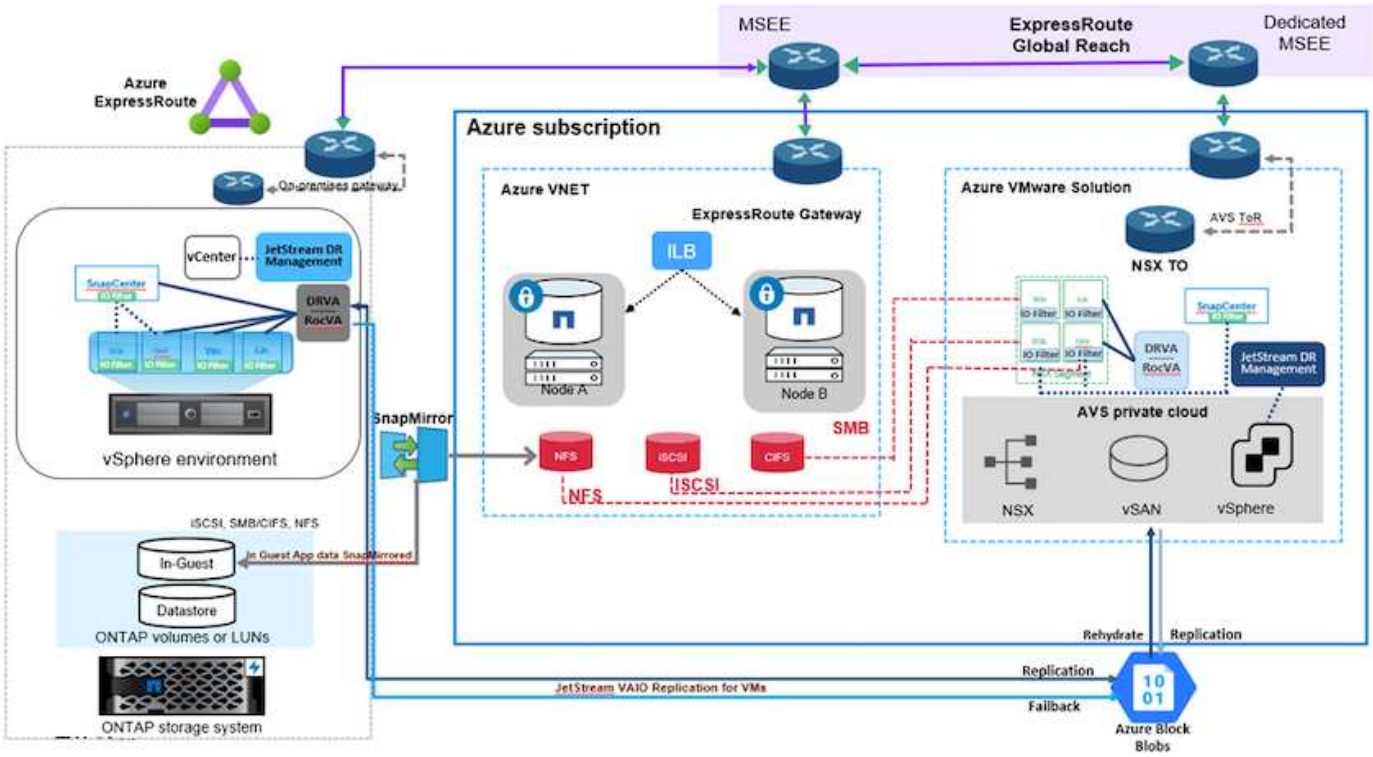
使用CVO和AVS进行灾难恢复(来宾连接存储)

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**

第一步是在Azure上配置Cloud Volumes ONTAP ("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。

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。

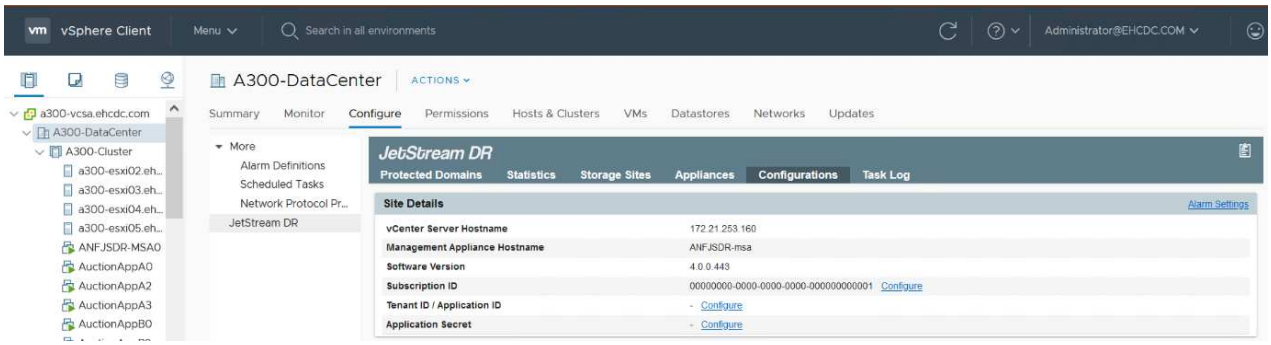
要配置AVS SDDC (无论是按需配置还是在指示灯模式下配置)、请参见 "在 Azure 上部署和配置虚拟化环境"。前提条件是、在建立连接后、验证AVS主机上的子虚拟机是否能够使用Cloud Volumes ONTAP 中的数据。

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)。

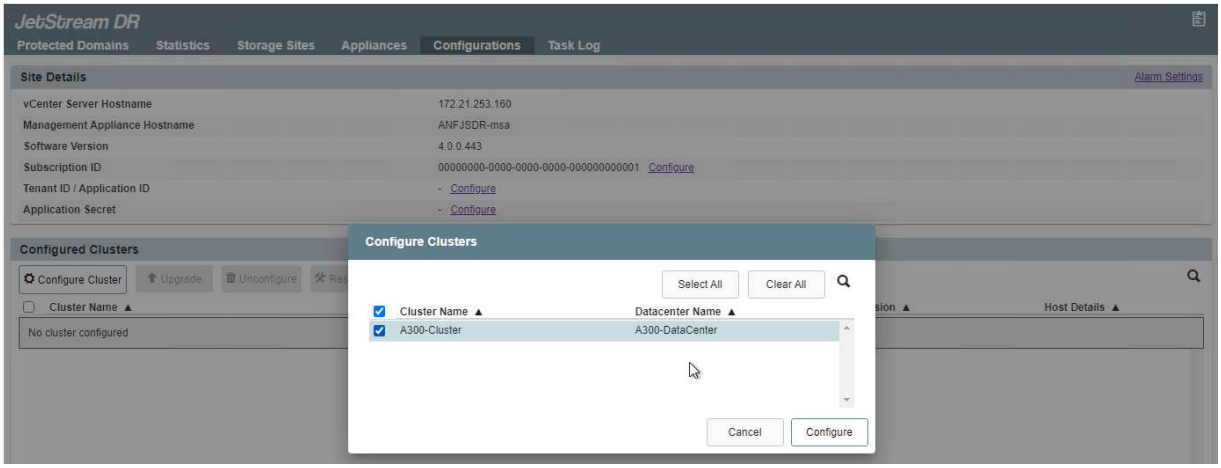
在内部数据中心中安装**Jetstream DR**

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。安装过程如下：

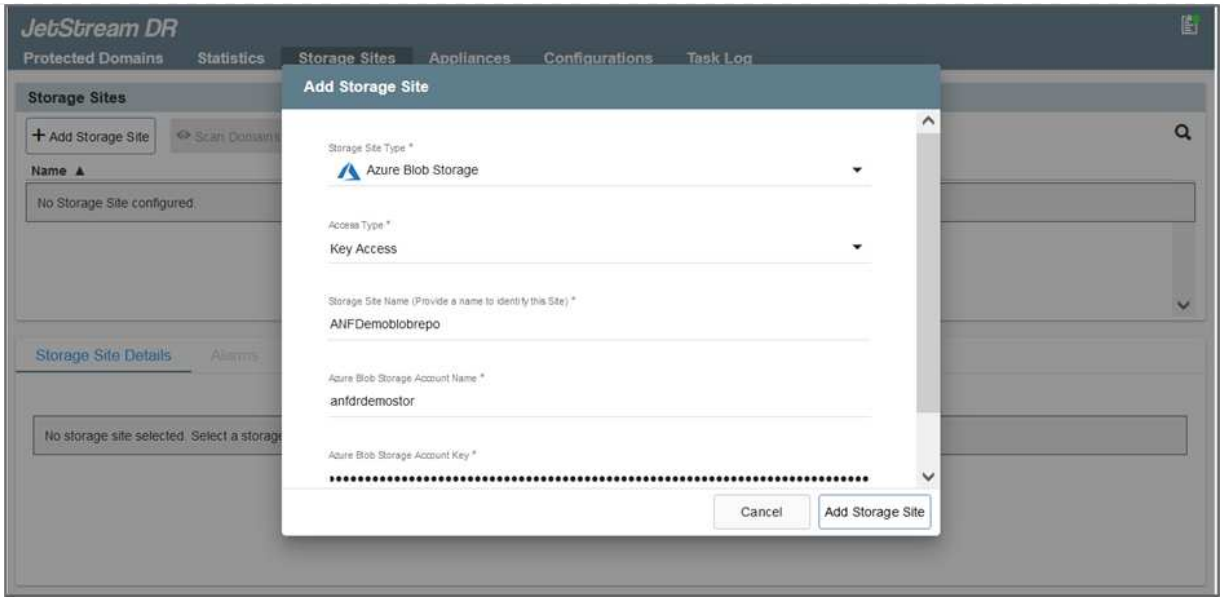
1. 检查前提条件。
2. 运行容量规划工具以获取资源和配置建议。
3. 将Jetstream DR MSA部署到指定集群中的每个vSphere主机。
4. 在浏览器中使用其DNS名称启动MSA。
5. 向MSA注册vCenter Server。
6. 部署Jetstream DR MSA并注册vCenter Server后、导航到vSphere Web Client中的Jetstream DR插件。可通过导航到"数据中心">"配置">"Jetstream DR"来完成此操作。



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。

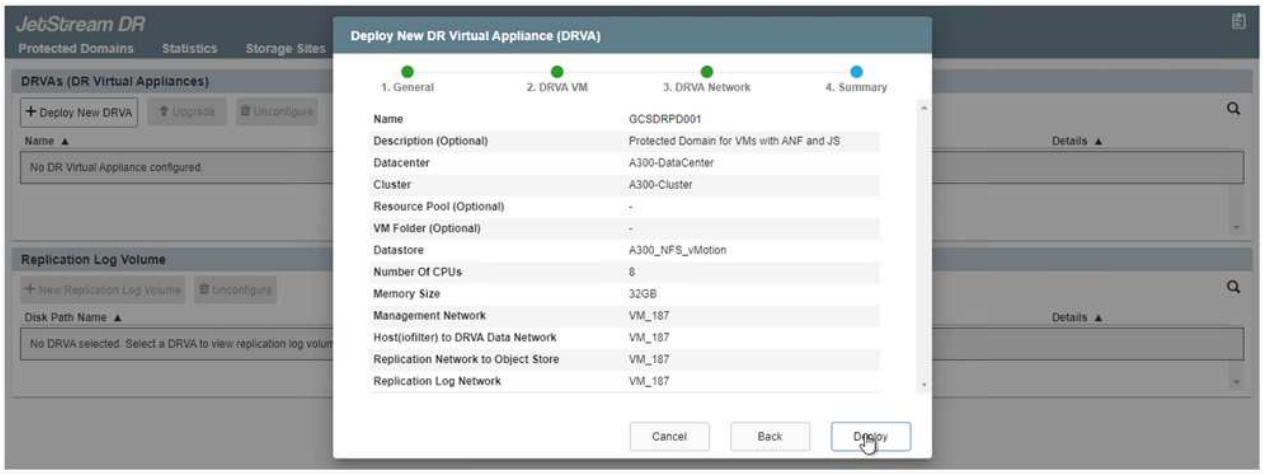


   b. 添加位于恢复站点的Azure Blob存储。

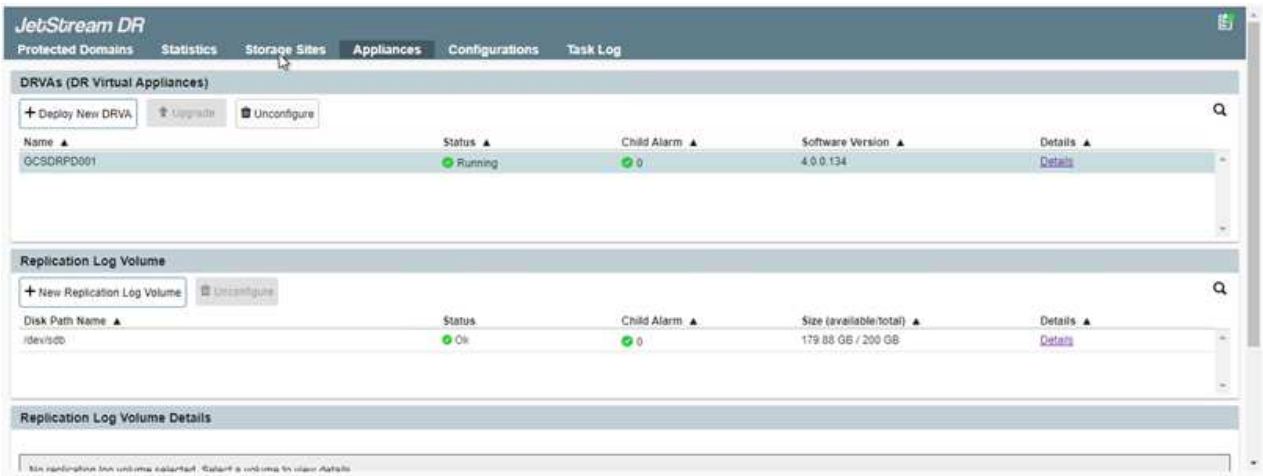


8. 从设备选项卡部署所需数量的灾难恢复虚拟设备(DR Virtual Appliances、DRVA)。

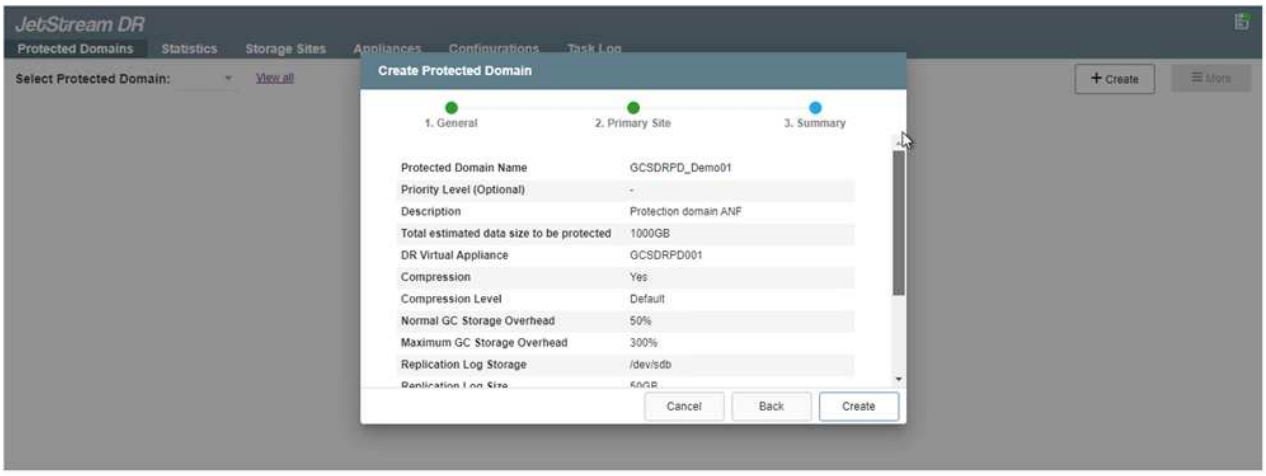
> ⓘ 使用容量规划工具估计所需的DRBA数量。

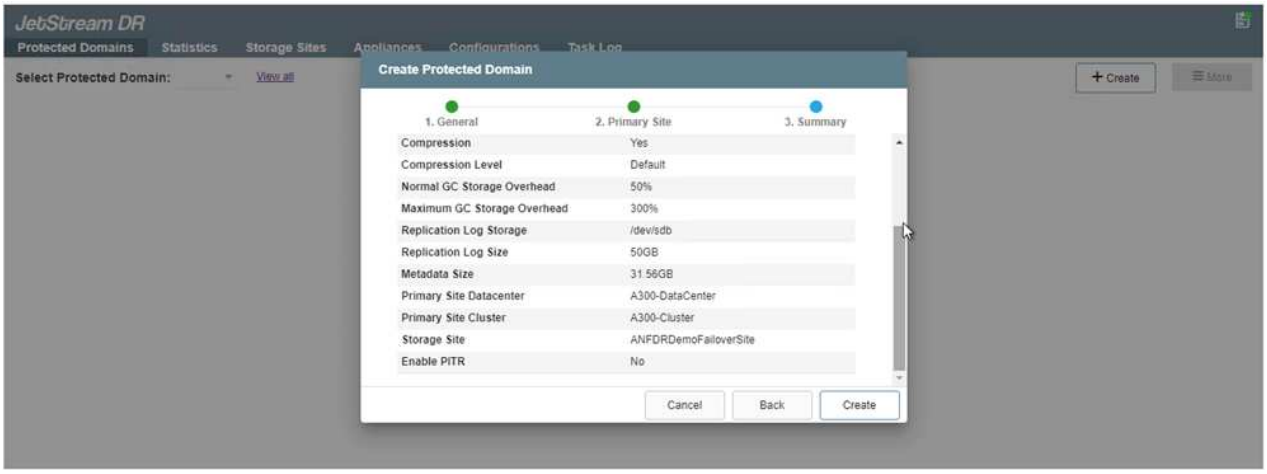


9. 使用可用数据存储库或独立的共享iSCSI存储池中的VMDK为每个DRVA创建复制日志卷。



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。

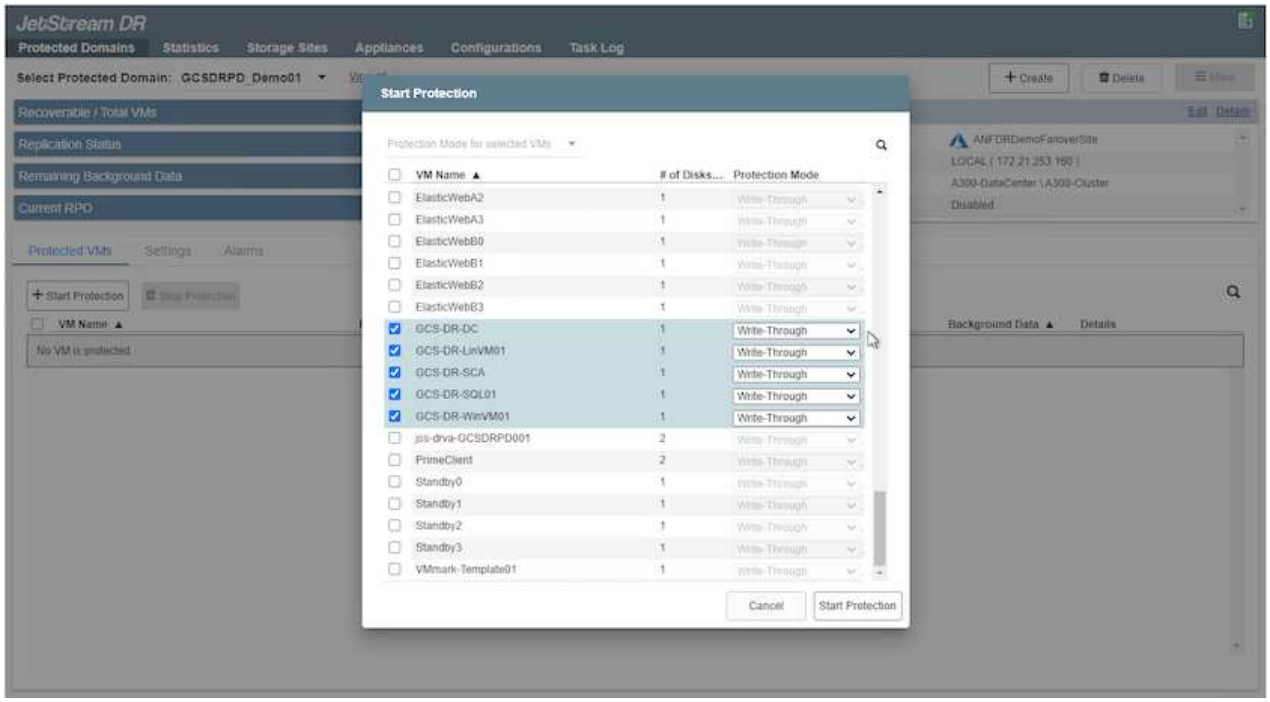




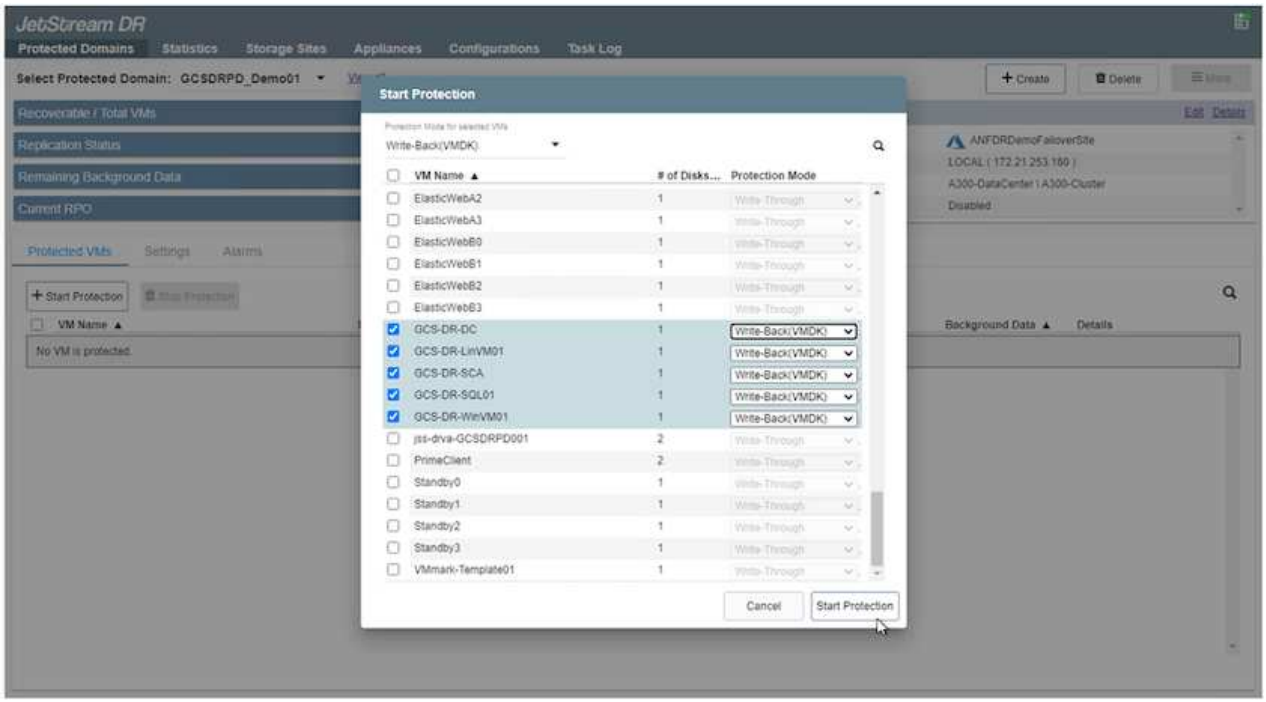
11. 选择要保护的VM、并根据依赖关系将这些VM分组到应用程序组中。通过应用程序定义、您可以将VM集分组到逻辑组中、这些逻辑组包含其启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

> ⓘ 确保对受保护域中的所有VM使用相同的保护模式。

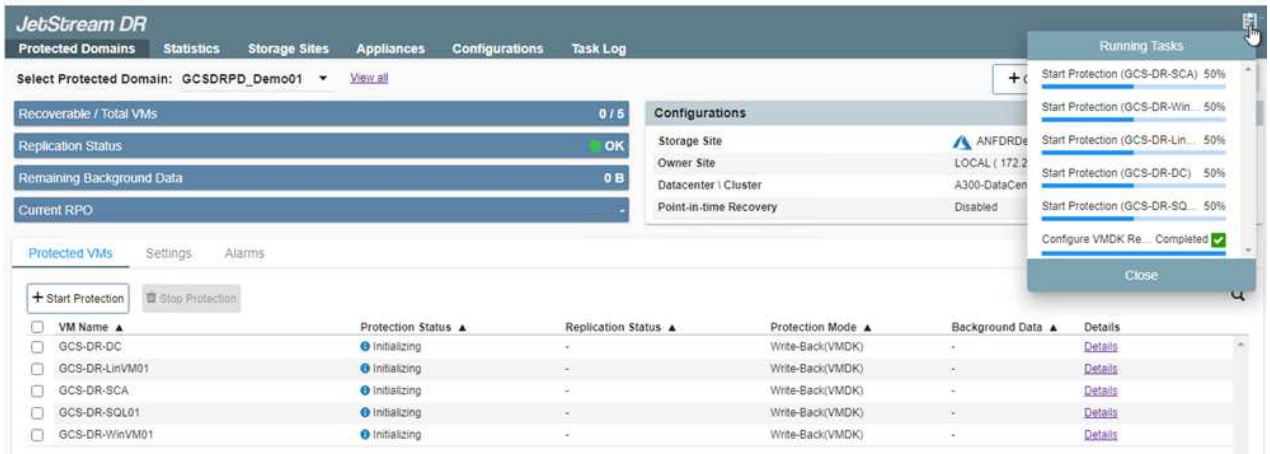
回写(VMDK)模式可提供更高的性能。



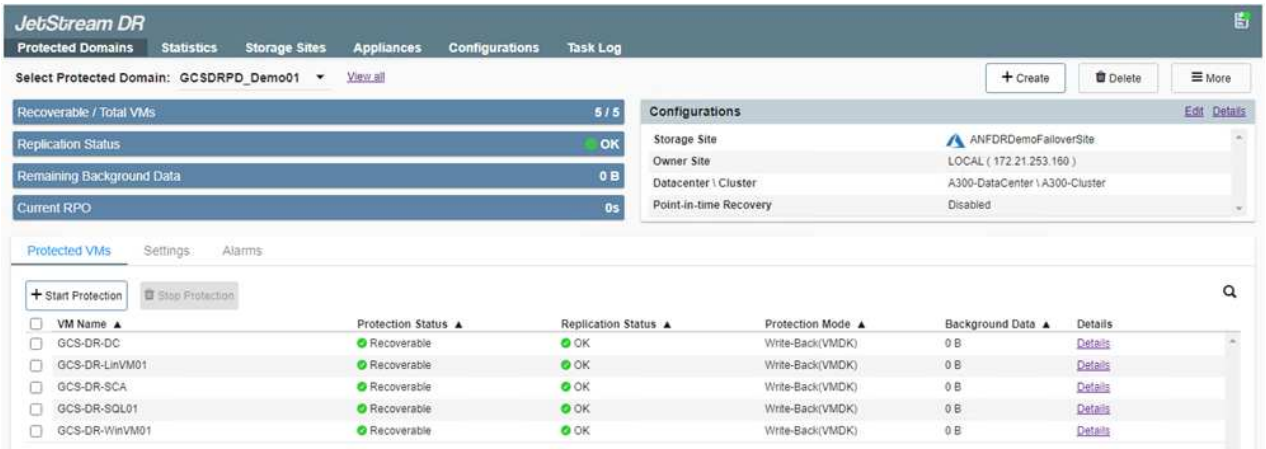
12. 确保将复制日志卷放置在高性能存储上。



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。

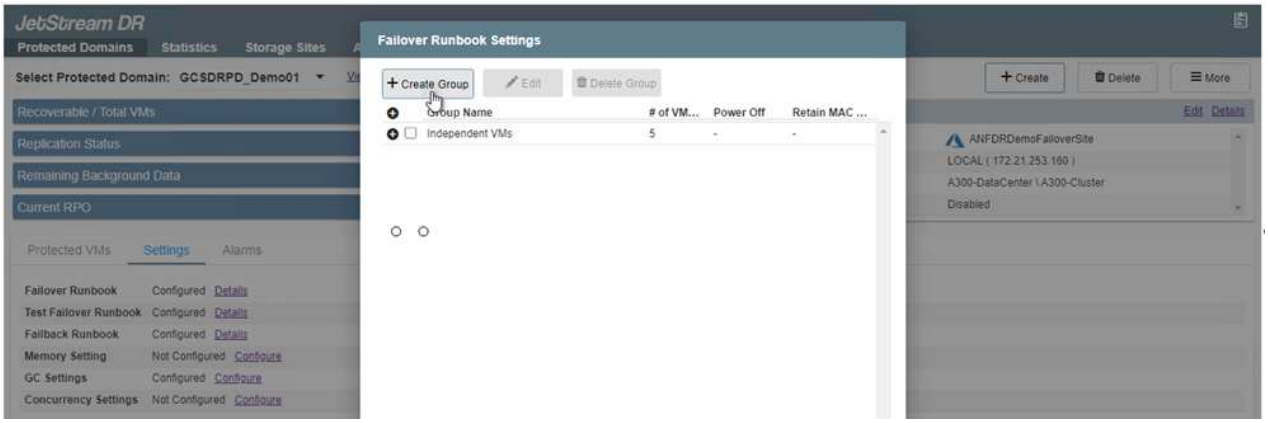


> 可以对故障转移运行手册进行配置、以便对VM (称为恢复组)进行分组、设置启动顺序以及修改CPU/内存设置以及IP配置。

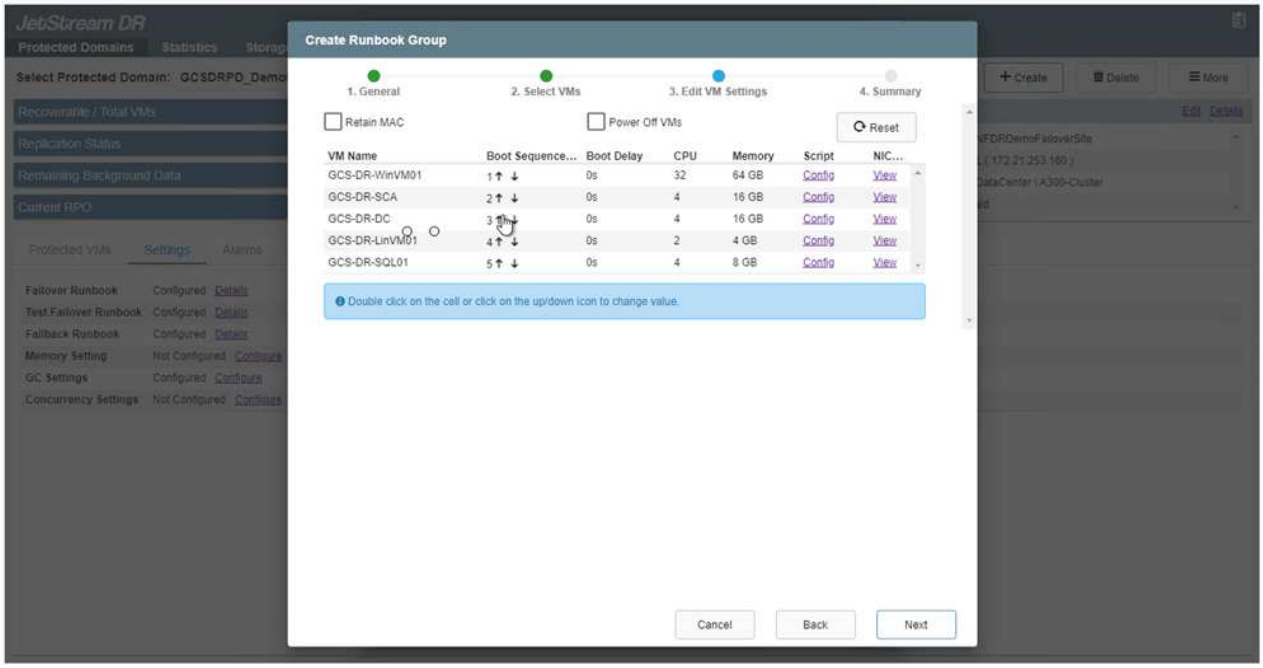
15. 单击设置、然后单击运行手册配置链接以配置运行手册组。

16. 单击创建组按钮开始创建新的运行手册组。

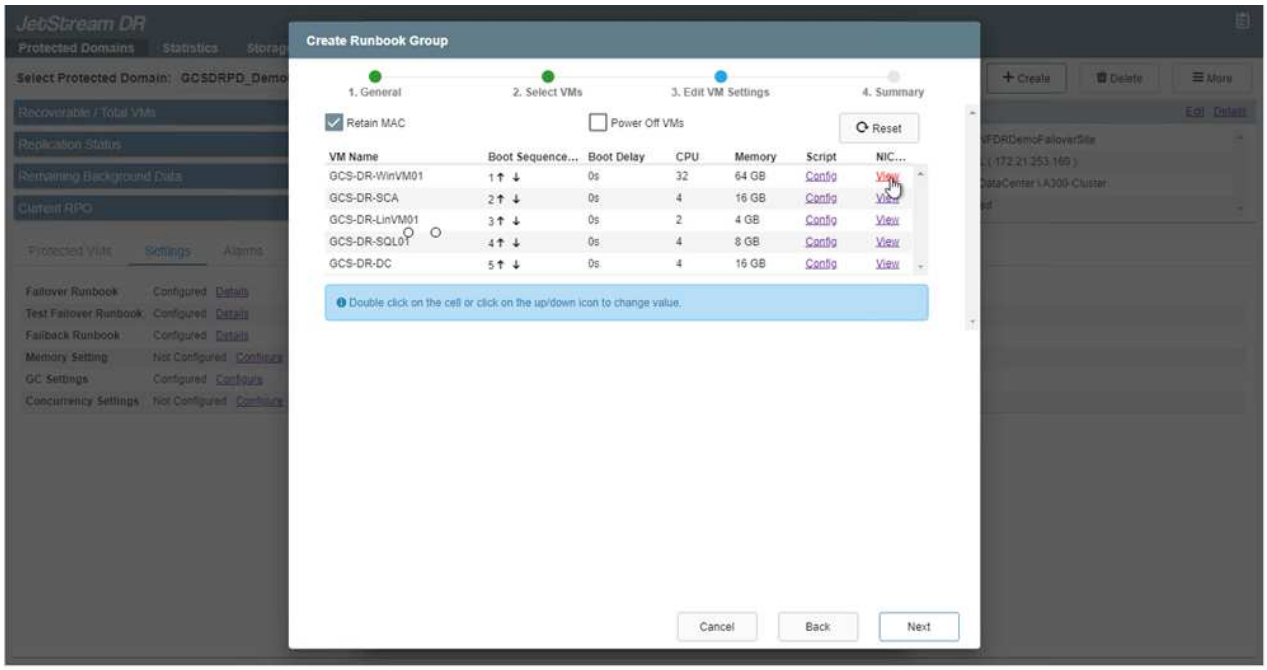
> 如果需要、请在屏幕下部应用自定义预脚本和后脚本、以便在运行手册组执行操作之前和之后自动运行。确保Runbook脚本驻留在管理服务器上。



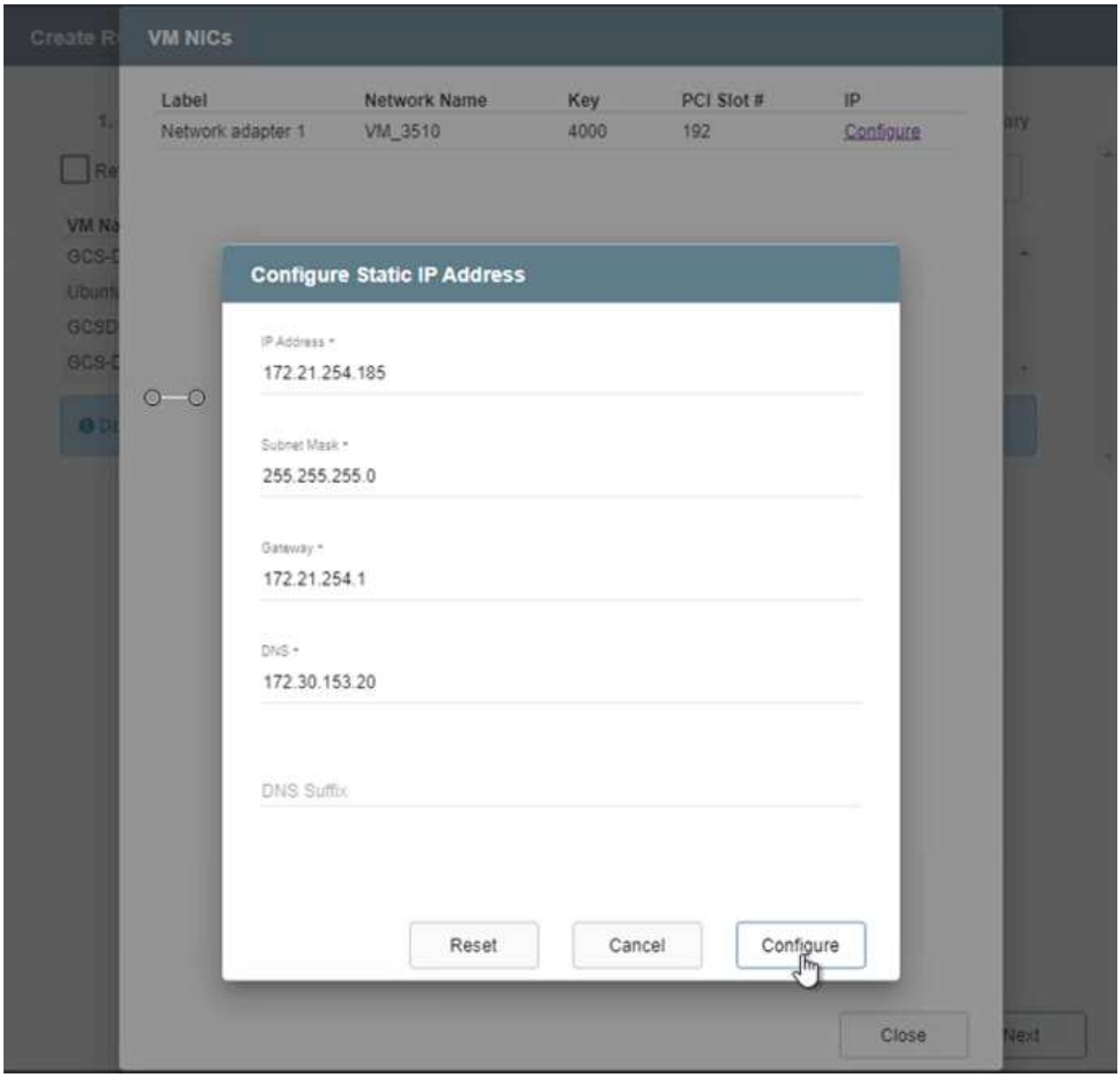
17. 根据需要编辑VM设置。指定用于恢复VM的参数、包括启动顺序、启动延迟(以秒为单位指定)、CPU数量以及要分配的内存量。单击向上或向下箭头更改VM的启动顺序。此外、还提供了用于保留MAC的选项。

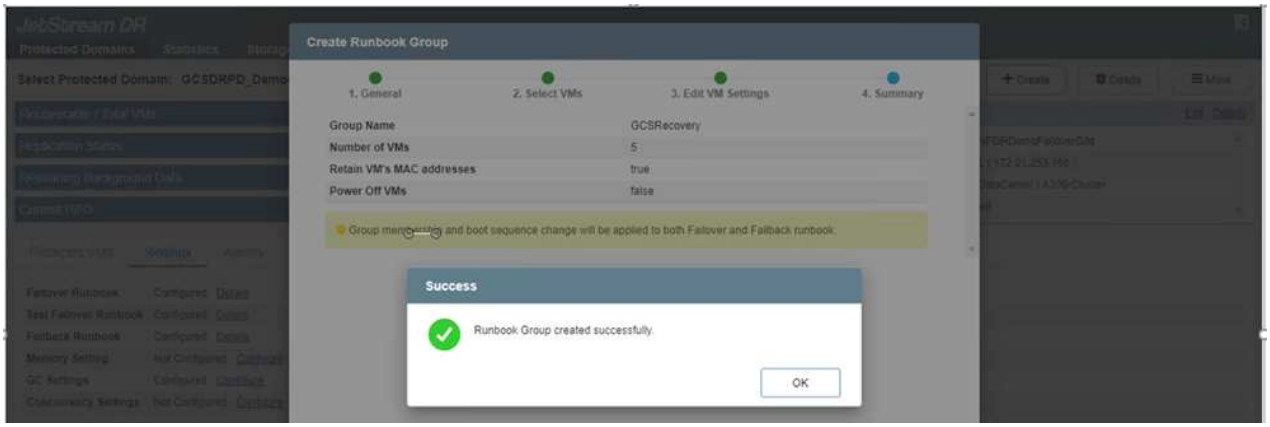


18. 可以为组中的各个VM手动配置静态IP地址。单击虚拟机的NIC视图链接以手动配置其IP地址设置。



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。

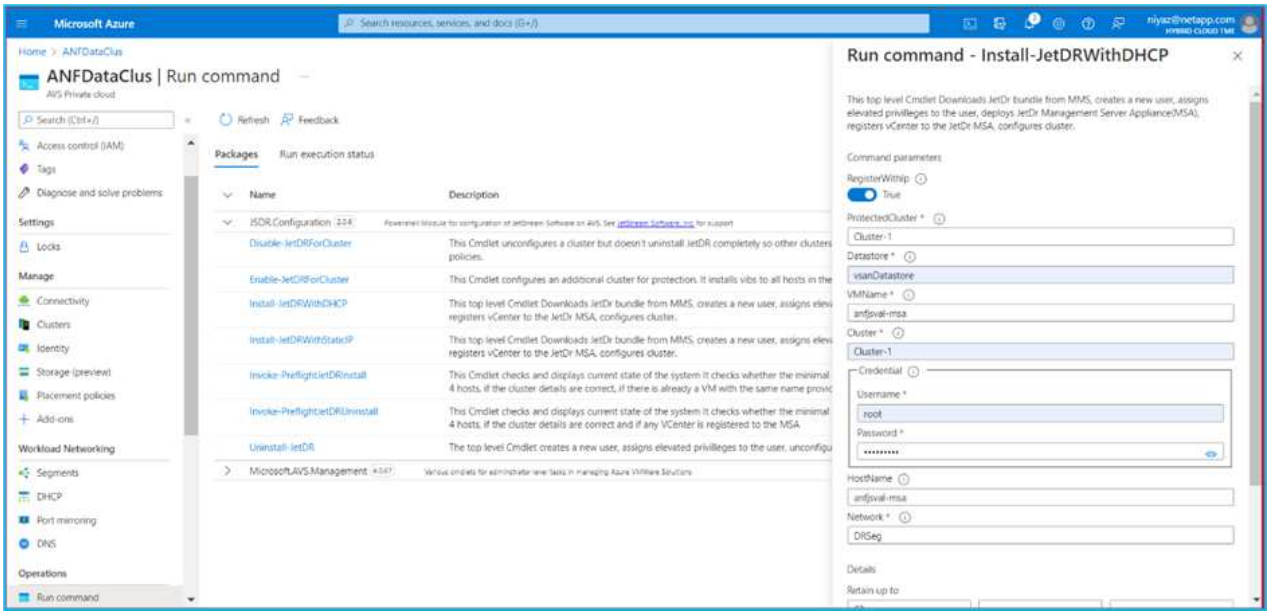
> 应在AVS集群上配置网络配置、包括创建网段、以满足内部部署要求。

> 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。

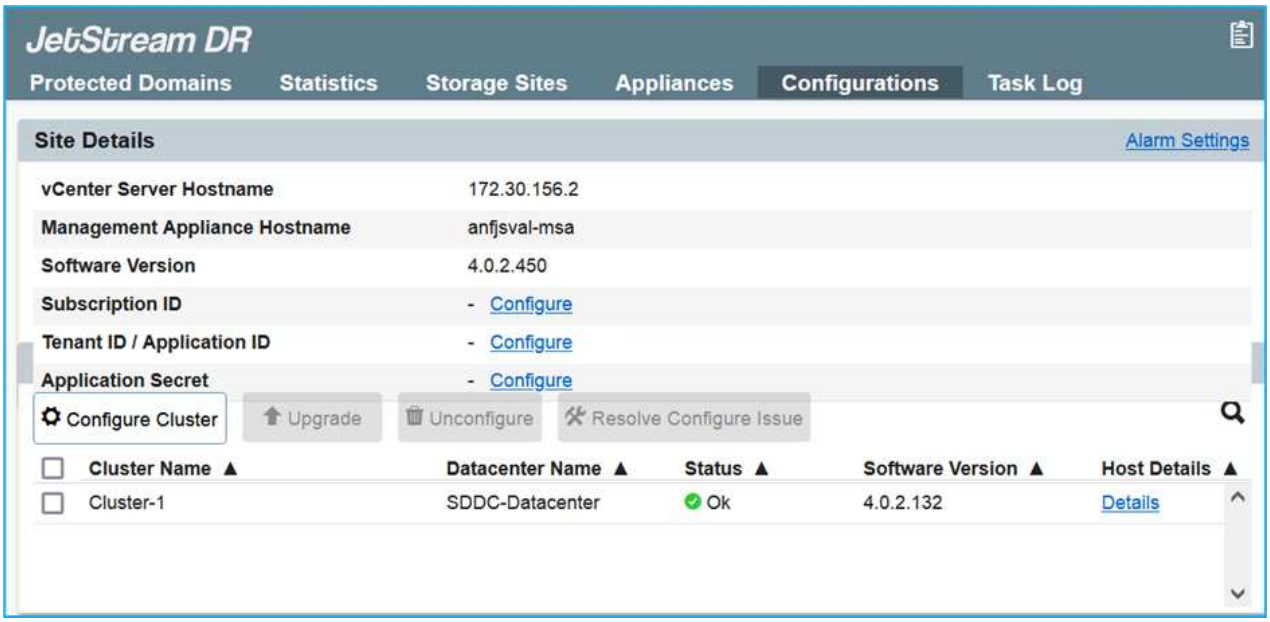
1. 要在Azure VMware解决方案 私有云上安装Jetstream DR for AVS、请使用Run命令。从Azure门户中、转到Azure VMware解决方案 、选择私有云、然后选择运行命令>软件包> JSDR.Configuration。

   > 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。

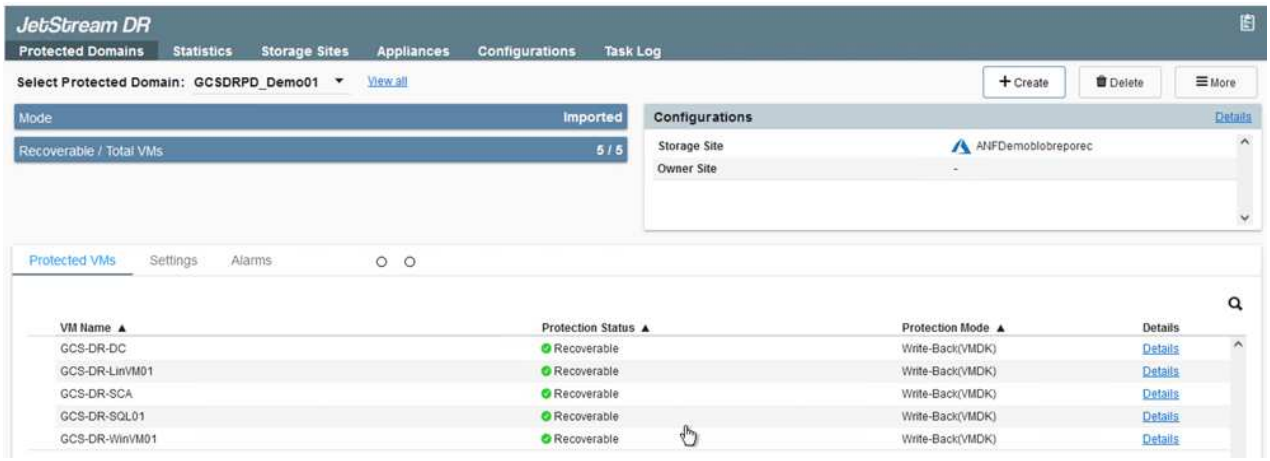


2. 完成适用于AVS的Jetstream DR安装后、刷新浏览器。要访问Jetstream DR UI、请转到SDDC Datacenter >配置> Jetstream DR。



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。

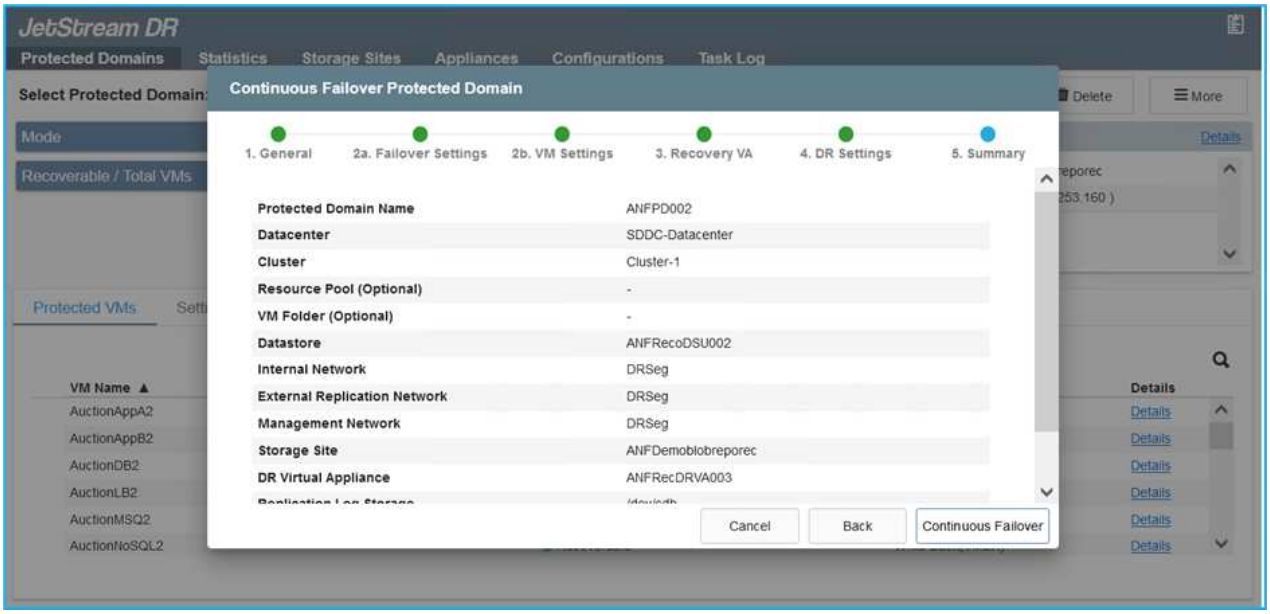
4. 已导入此域以进行恢复。转到"受保护域"选项卡并验证是否已选择目标域、或者从"选择受保护域"菜单中选择所需域。此时将显示受保护域中可恢复的VM列表。



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。

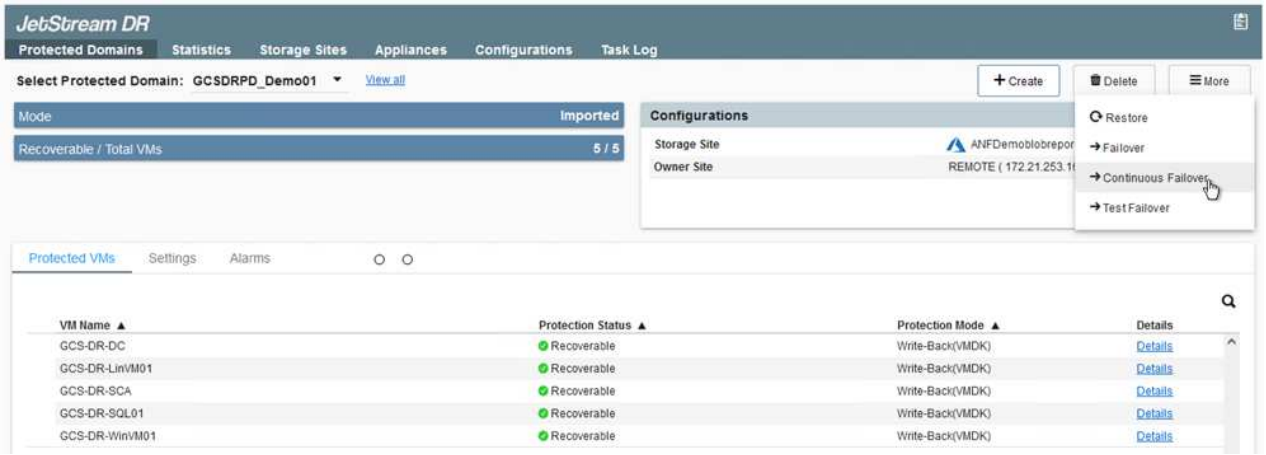
6. 使用可用的vSAN或ANF数据存储库创建复制日志卷。
7. 导入受保护域并配置恢复VA以使用ANF数据存储库放置VM。



> 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。

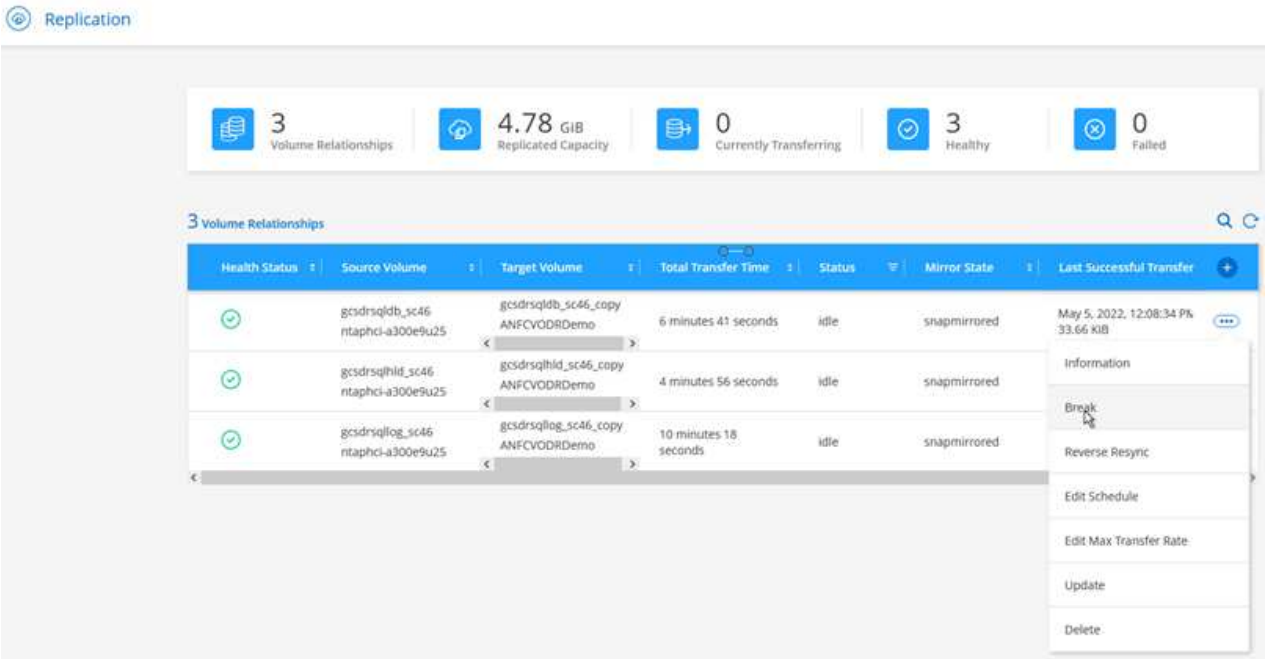
8. 选择相应的故障转移选项(持续故障转移或故障转移)。在此示例中、选择了持续再融合(持续故障转移)。

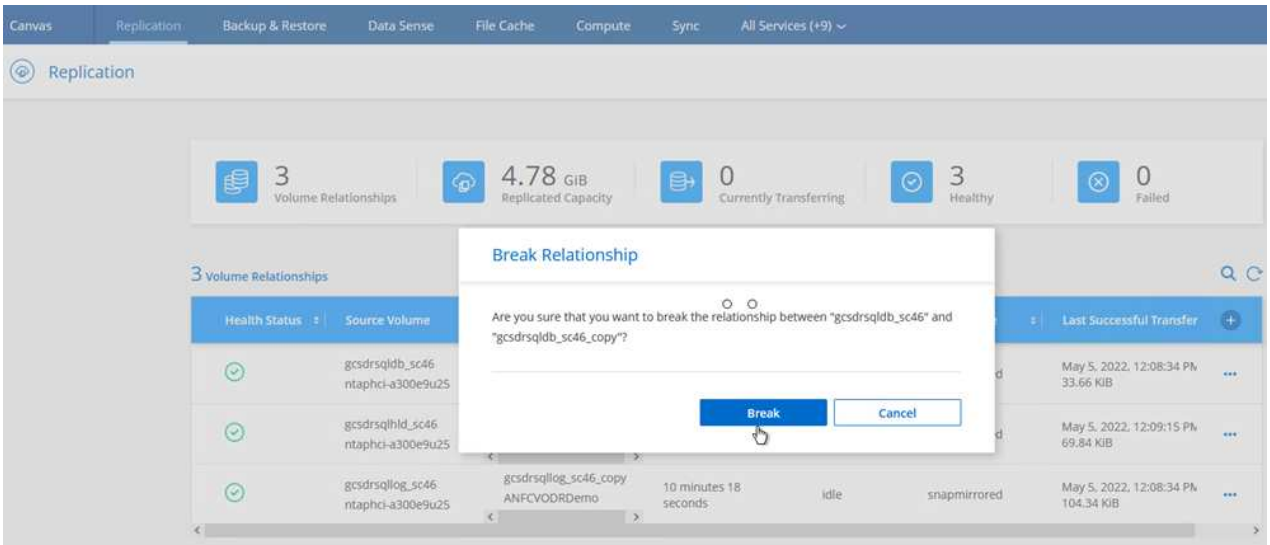
> 尽管执行配置时的持续故障转移和故障转移模式有所不同、但这两种故障转移模式都使用相同的步骤进行配置。在发生灾难事件时、可以同时配置和执行故障转移步骤。可以随时配置持续故障转移、然后允许在正常系统运行期间在后台运行。发生灾难事件后、将完成持续故障转移、以便立即将受保护VM的所有权转移到恢复站点(接近零的RTO)。



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。

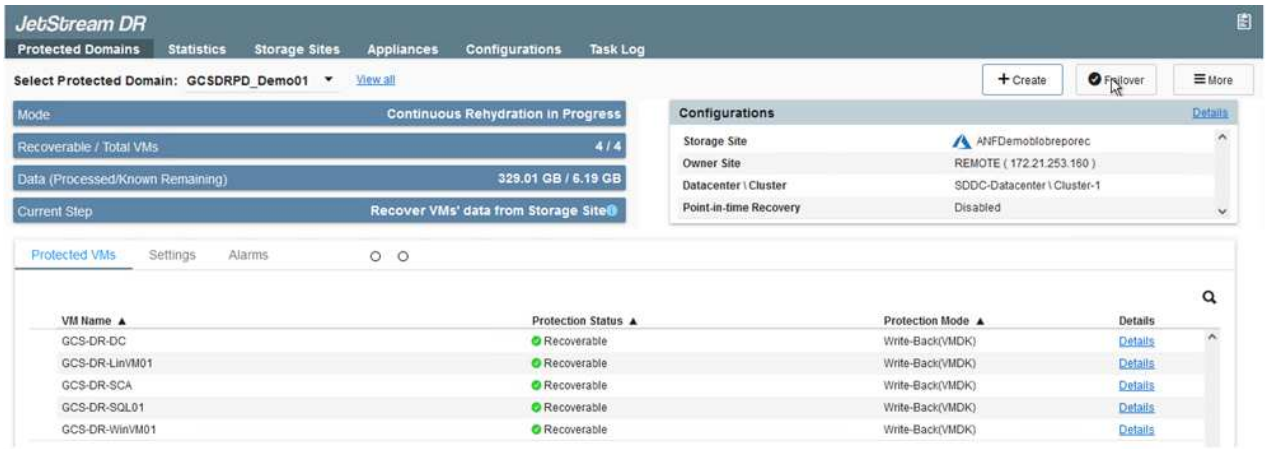


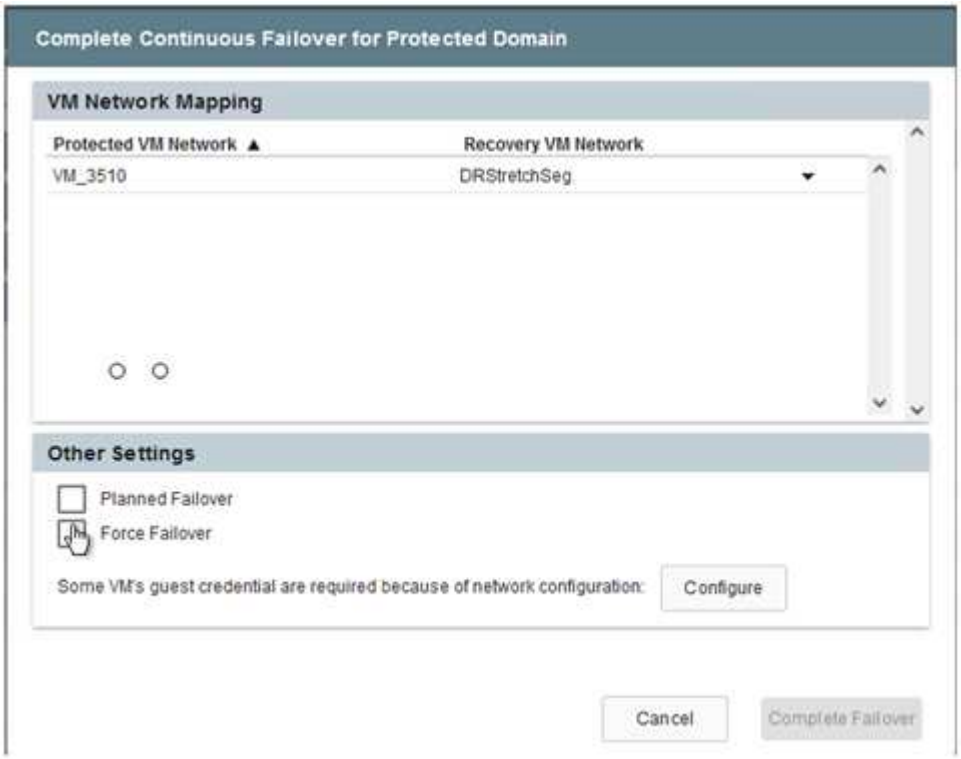


> 此步骤可以轻松地自动执行、以便于恢复过程。

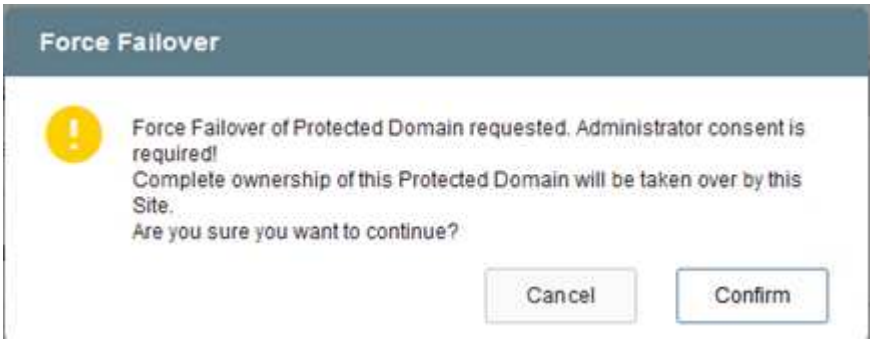
2. 在AVS SDDC (目标端)上访问Jetstream UI并触发故障转移选项以完成故障转移。任务栏将显示故障转移活动的进度。

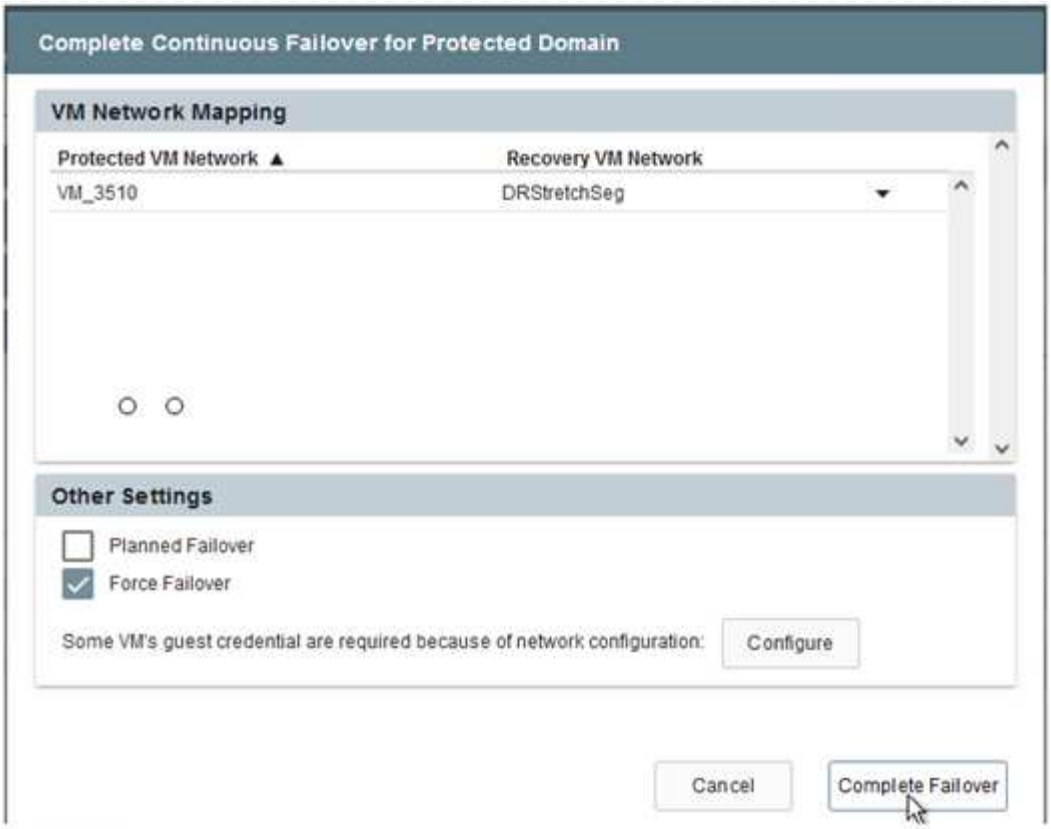
   在完成故障转移时显示的对话框窗口中、可以按计划或假定强制指定故障转移任务。





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。





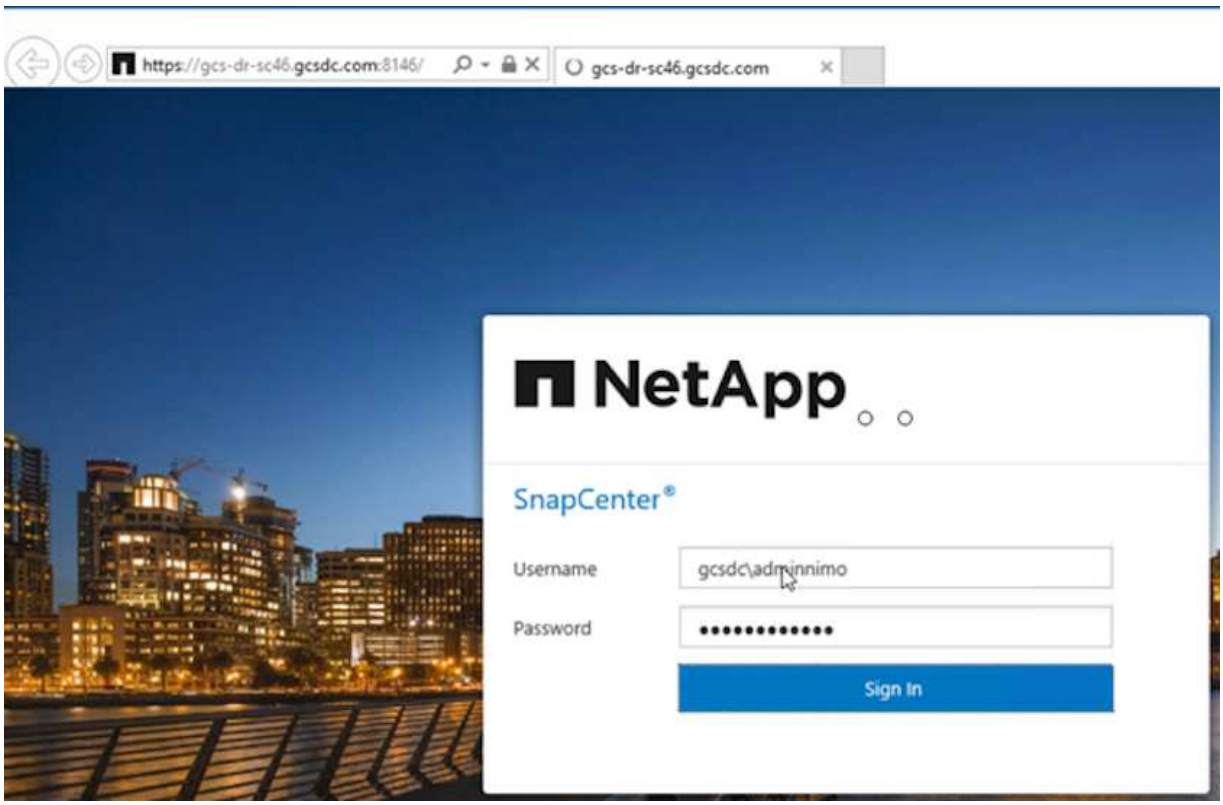
3. 持续故障转移完成后、将显示一条消息、确认任务完成。任务完成后、访问已恢复的VM以配置iSCSI或NFS会话。

> 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。

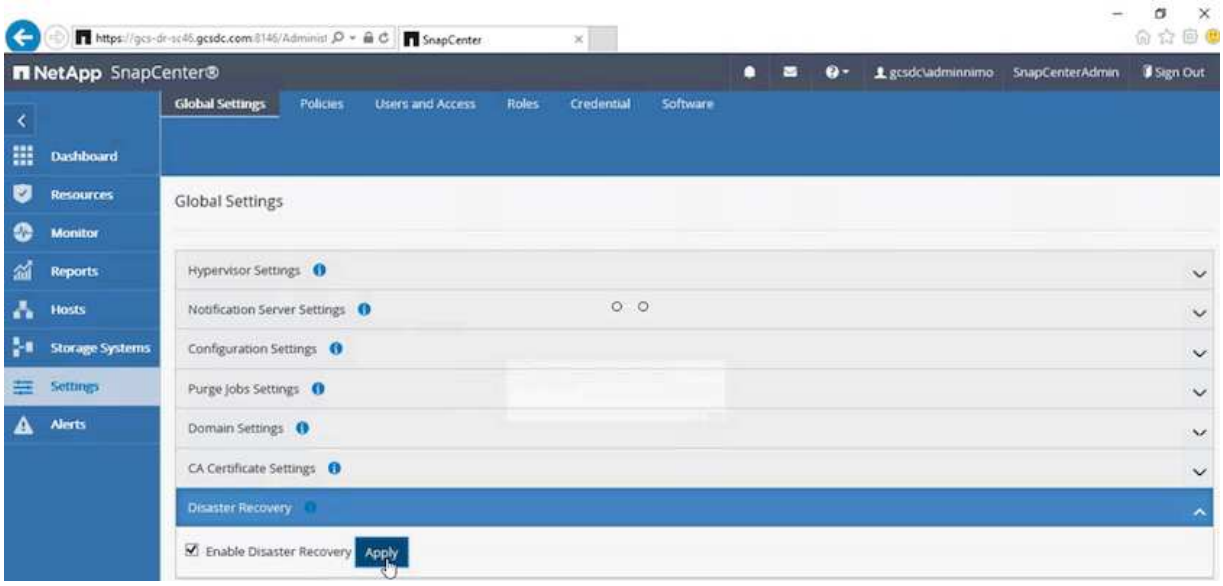
> 要验证故障转移配置和基础架构、可以在测试模式(测试故障转移选项)下运行Jetstream DR、以观察虚拟机及其数据从对象存储恢复到测试恢复环境的过程。在测试模式下执行故障转移操作步骤 时、其操作类似于实际的故障转移过程。

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。



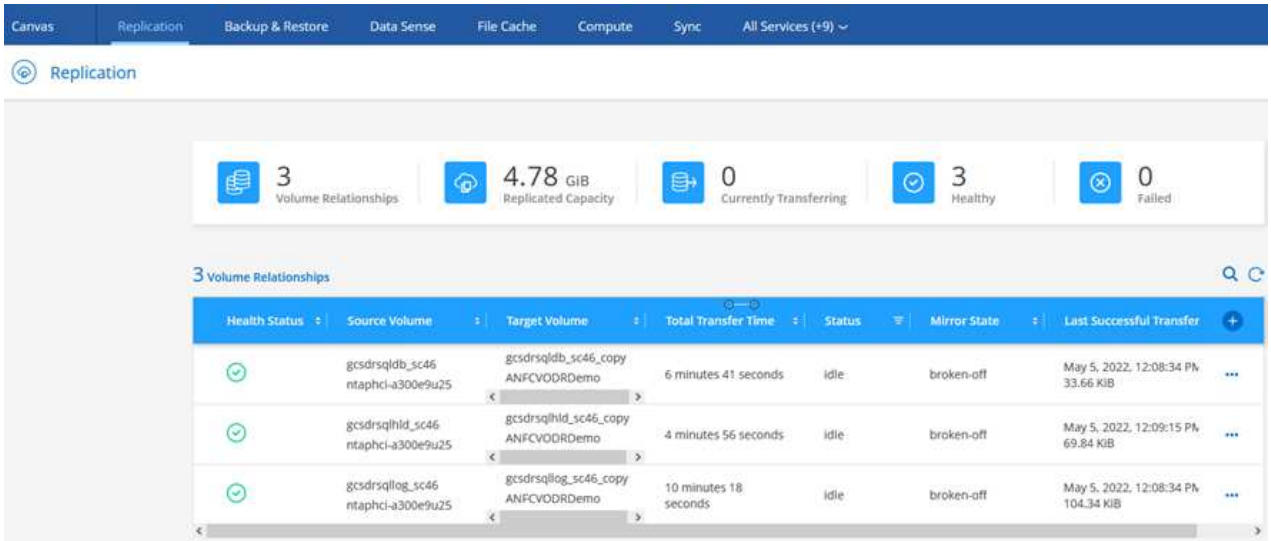
   b. 在设置页面中、导航到设置>全局设置>灾难恢复。
   c. 选择启用灾难恢复。
   d. 单击应用。



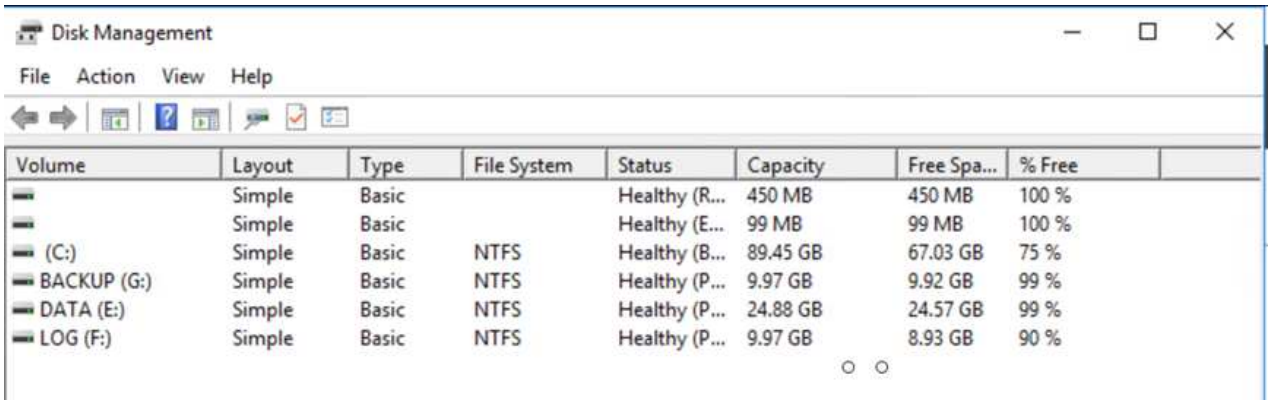
   e. 单击"监控">"作业"以验证是否已启用灾难恢复作业。

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。

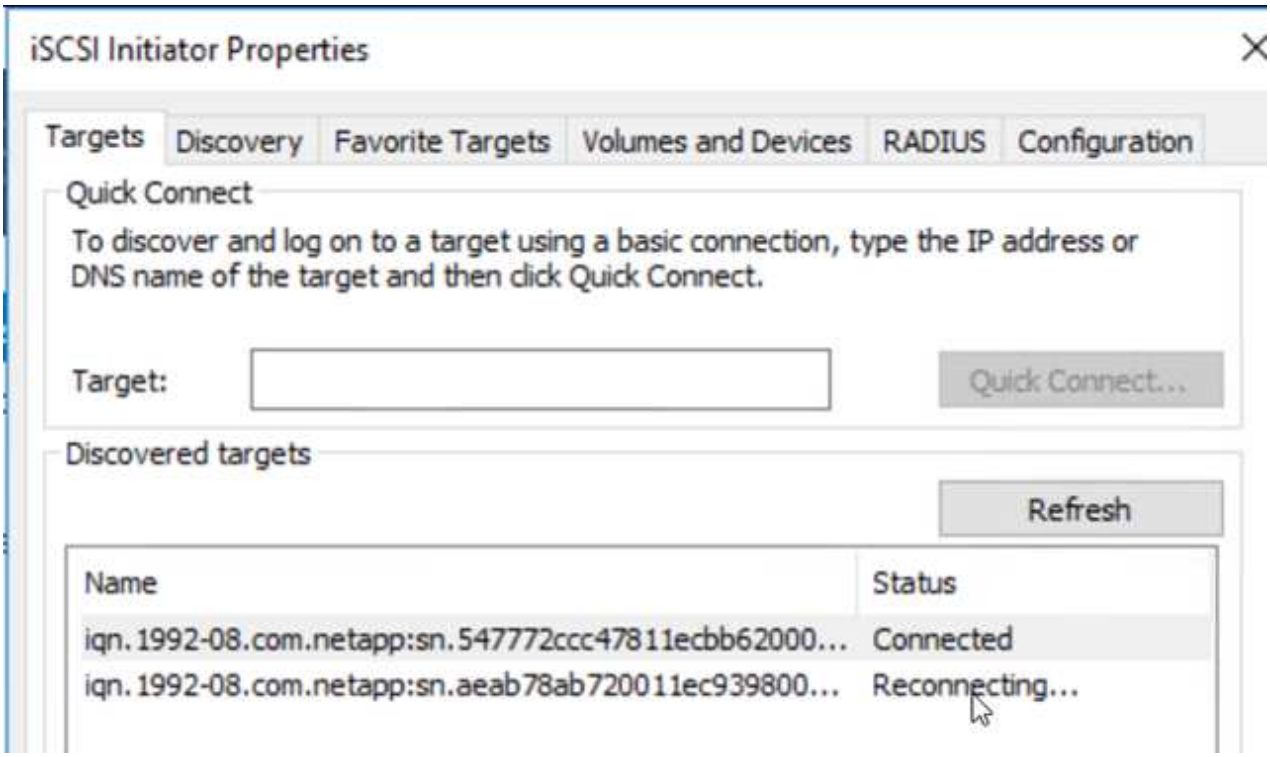
6. 确保SnapMirror关系已断开。



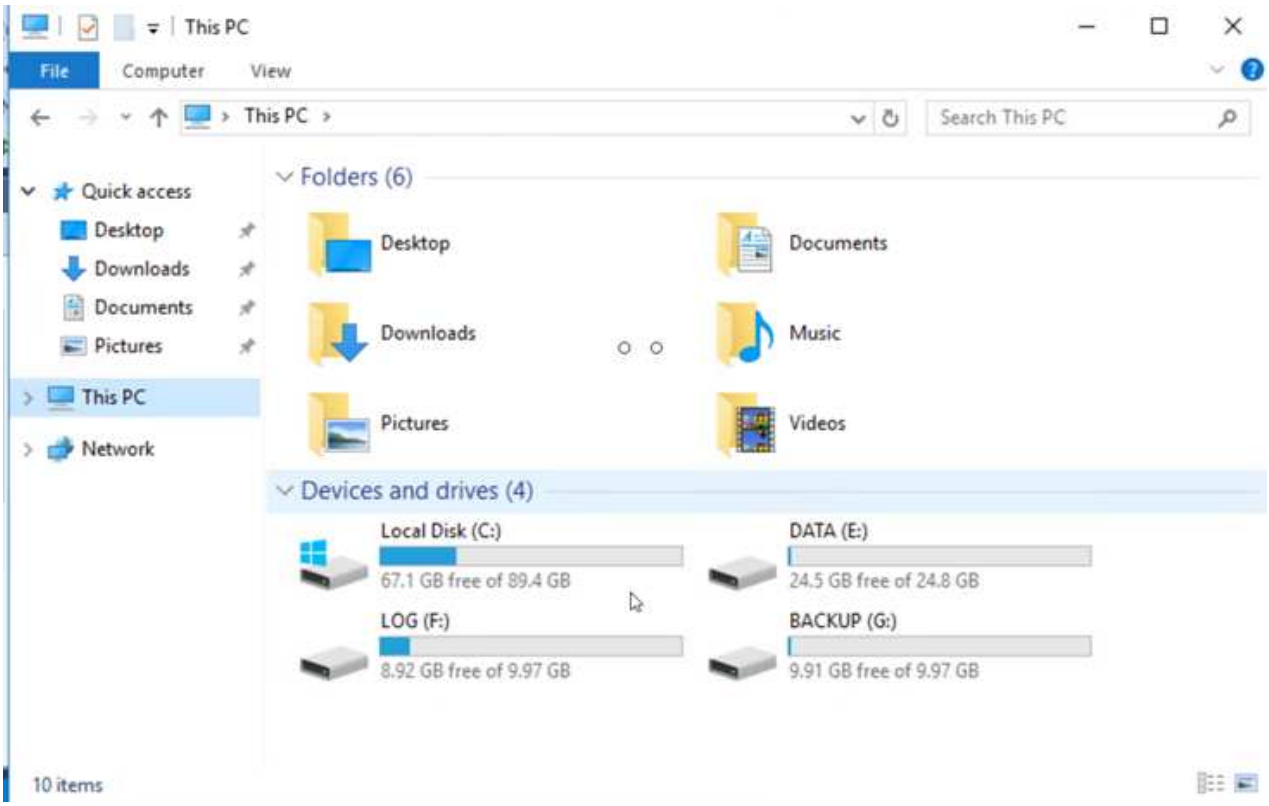
7. 使用相同的驱动器号将LUN从Cloud Volumes ONTAP 连接到已恢复的SQL子虚拟机。



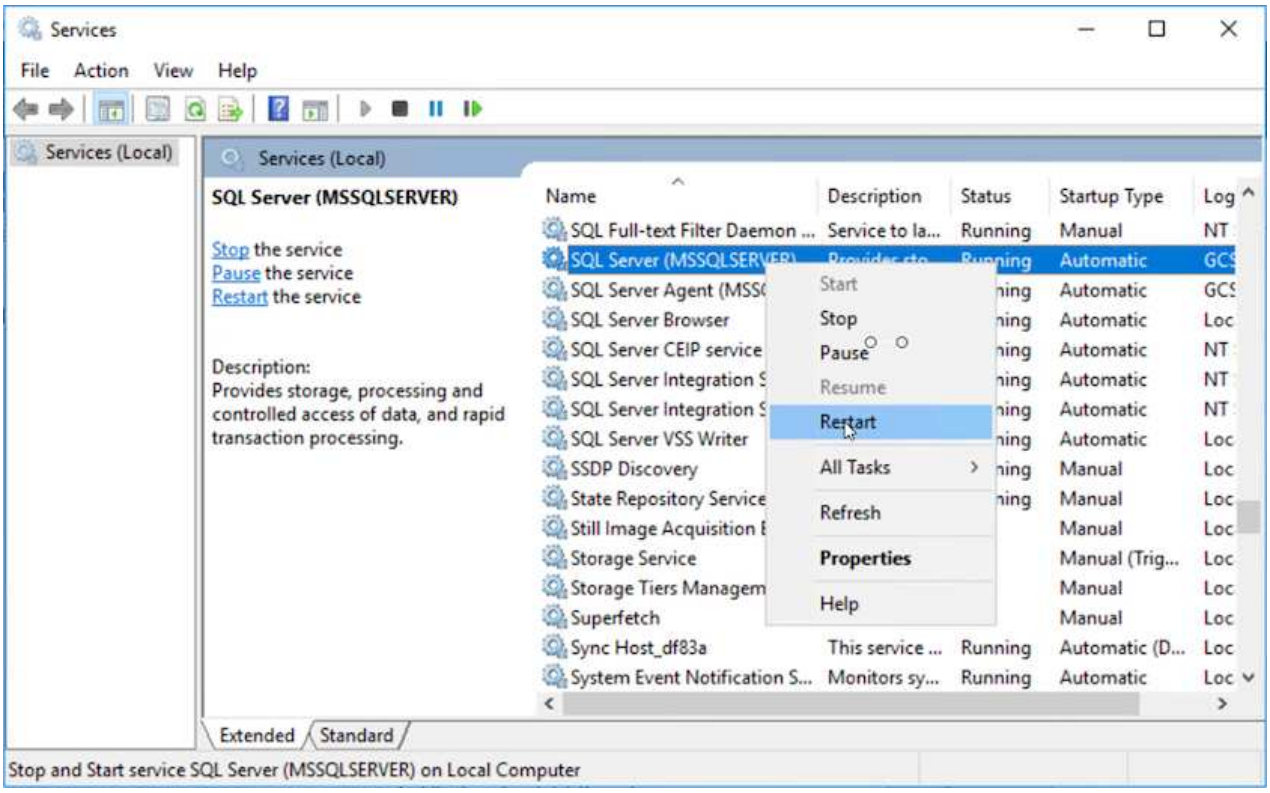
8. 打开iSCSI启动程序、清除先前已断开连接的会话、然后为复制的Cloud Volumes ONTAP 卷添加新目标以及多路径。



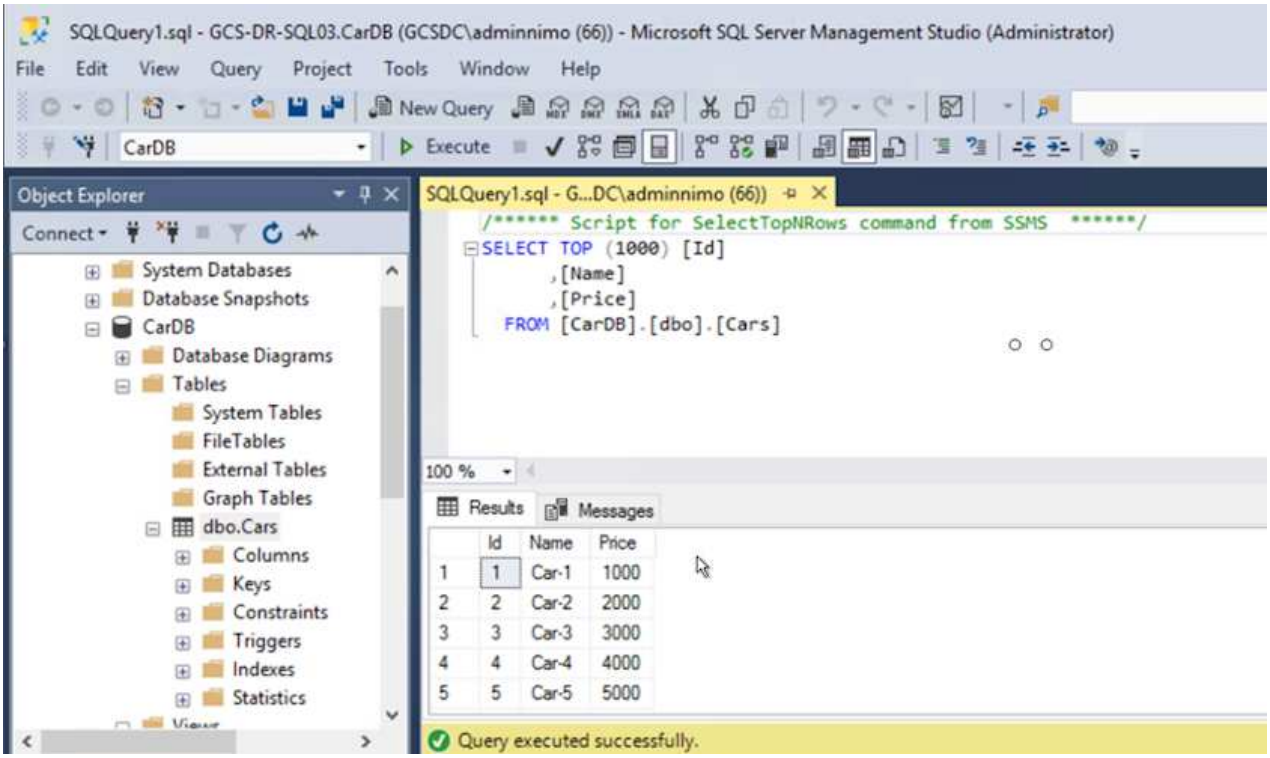
9. 确保使用DR之前使用的相同驱动器盘符连接所有磁盘。



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。

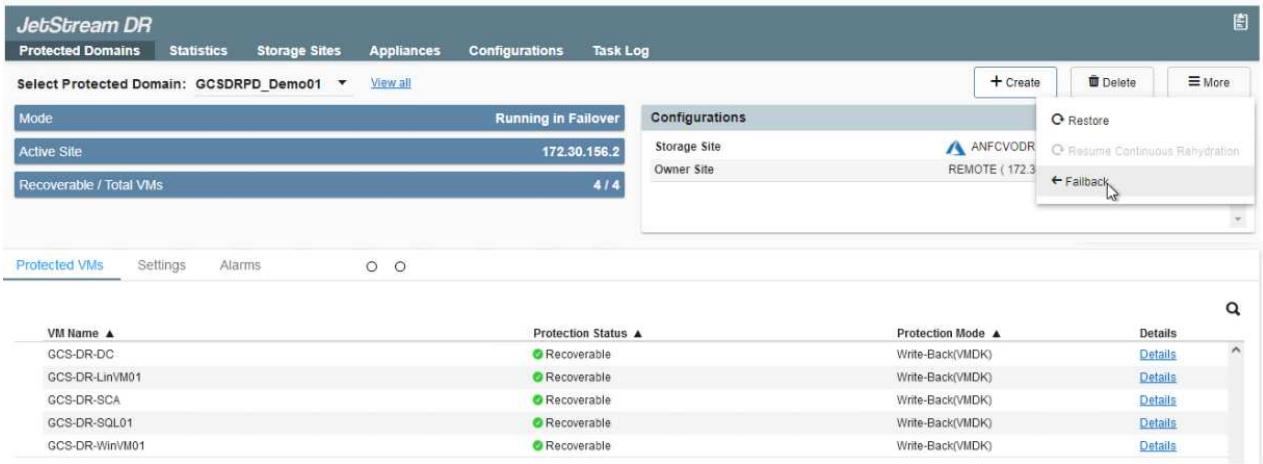
此时、可以正常运行运营并继续正常运营。

> 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。

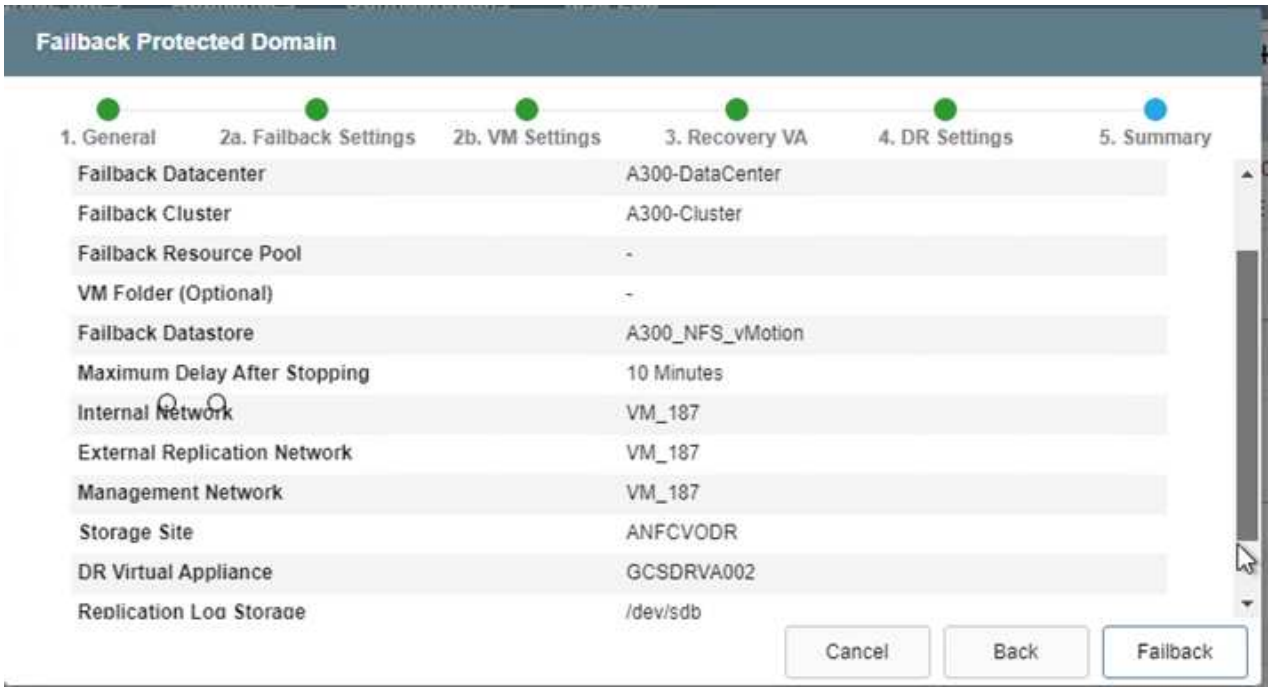
主站点启动并重新运行后、您可以执行故障恢复。Jetstream将恢复VM保护、并且必须反转SnapMirror关系。

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。

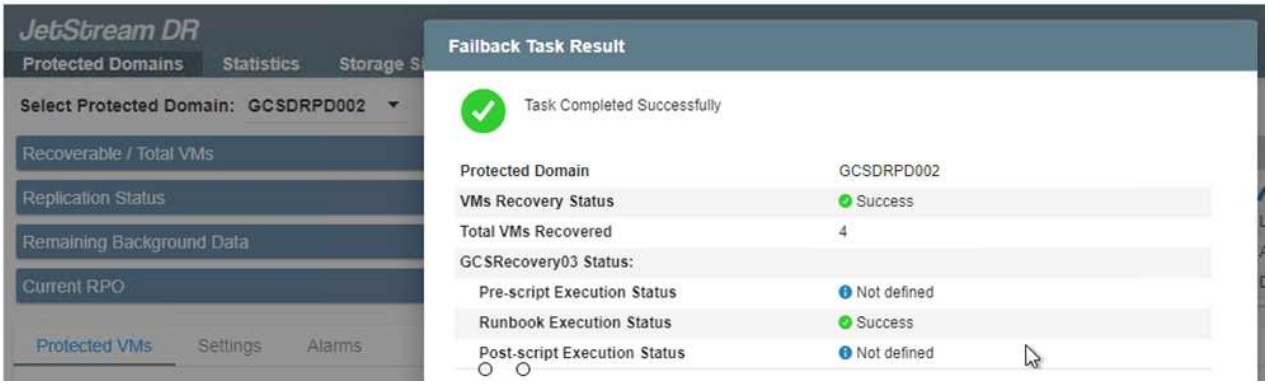
> CPT生成的故障恢复计划还可用于启动VM及其数据从对象存储返回到原始VMware环境的操作。



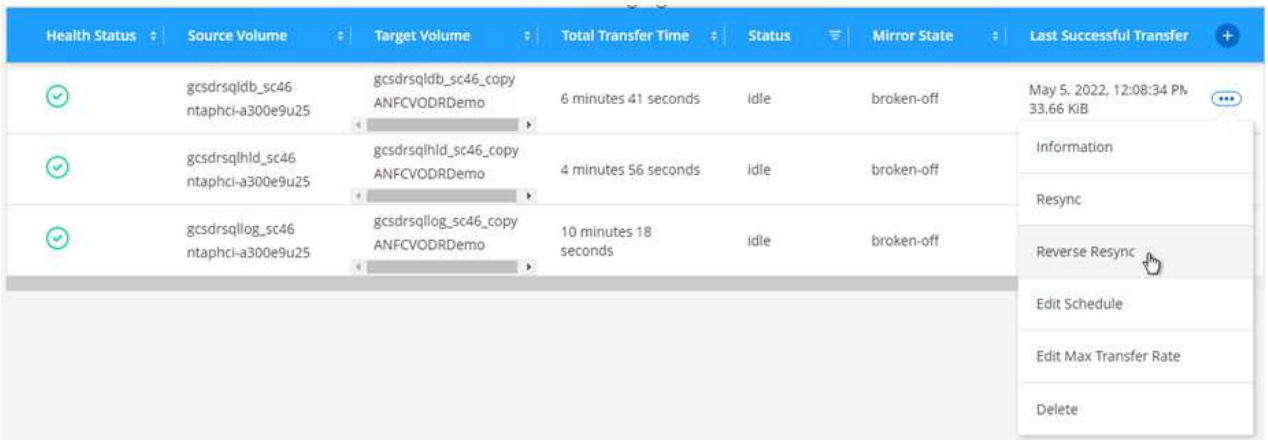
> 指定暂停恢复站点中的VM并在受保护站点中重新启动VM后的最大延迟。完成此过程所需的时间包括：停止故障转移VM后完成复制、清理恢复站点所需的时间以及在受保护站点中重新创建VM所需的时间。NetApp建议10分钟。

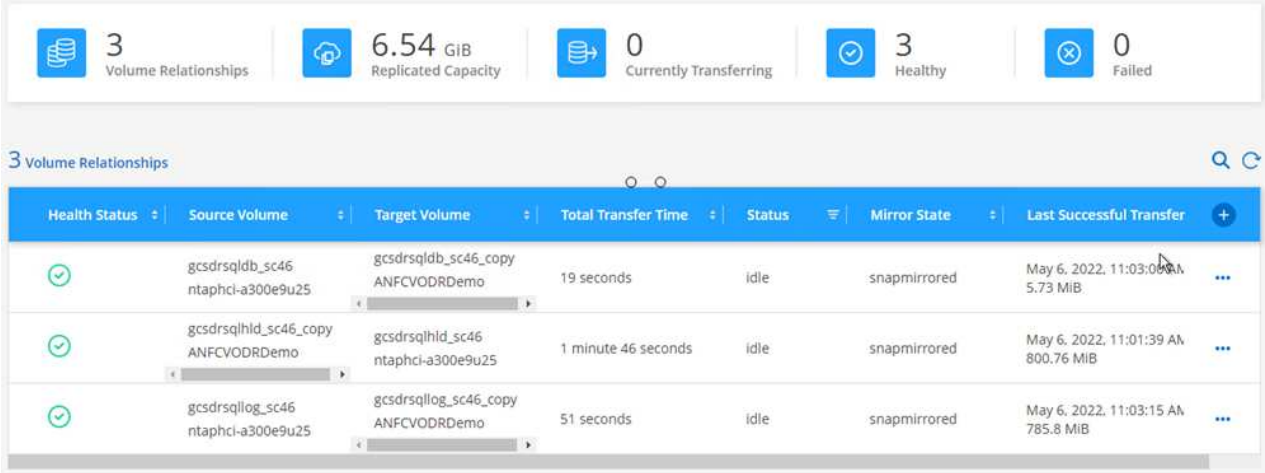


3. 完成故障恢复过程、然后确认虚拟机保护恢复和数据一致性。

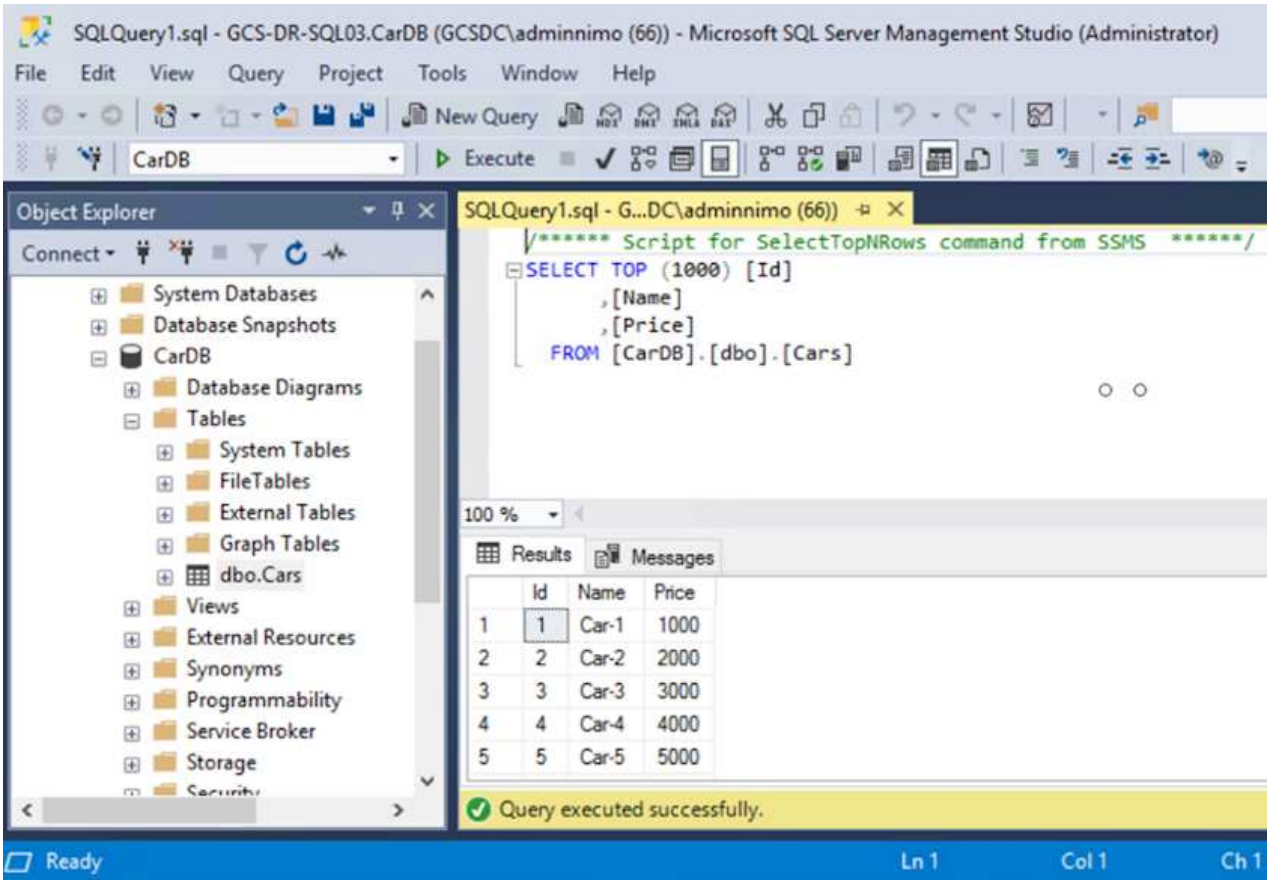


4. 恢复VM后、断开二级存储与主机的连接并连接到主存储。





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。

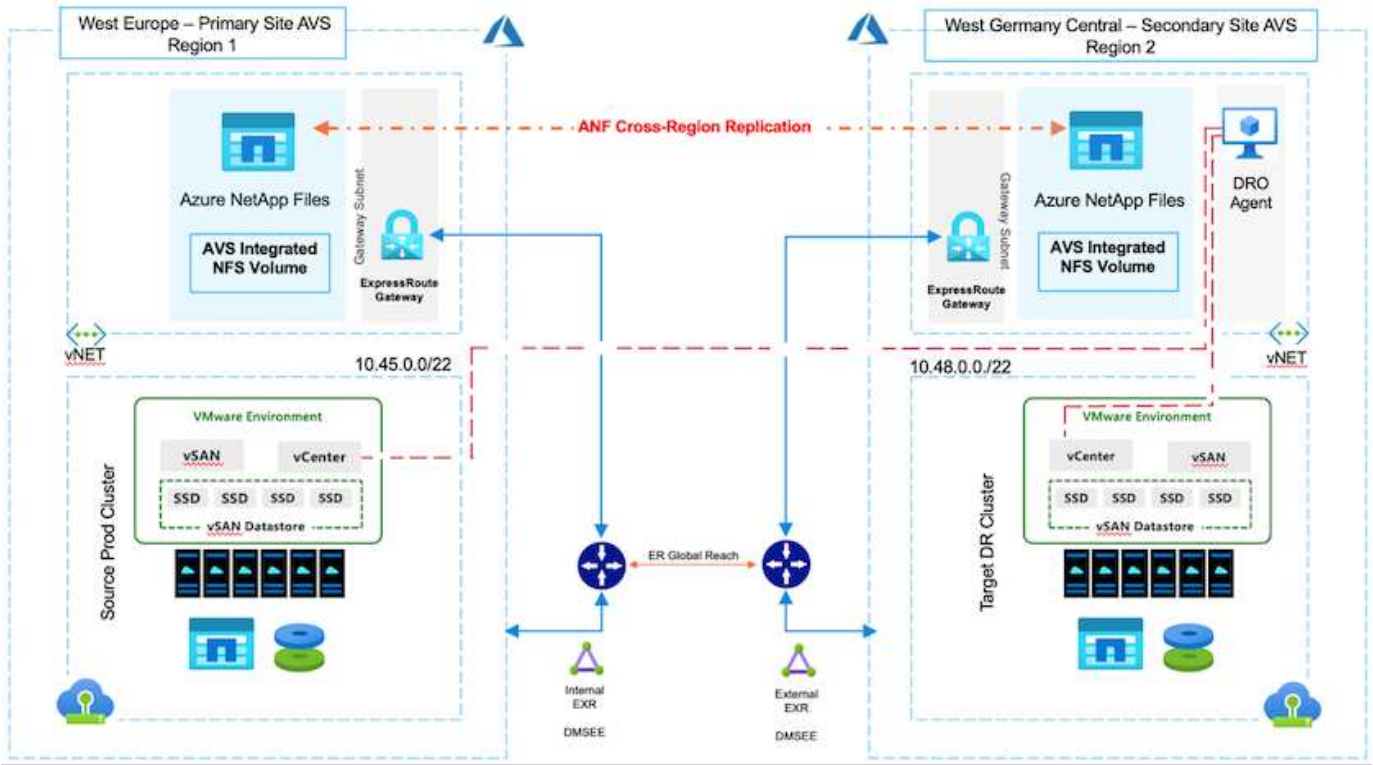
TR-4955：《使用Azure NetApp Files (ANF)和Azure VMware解决方案 (AVS)进行灾难恢复》

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。

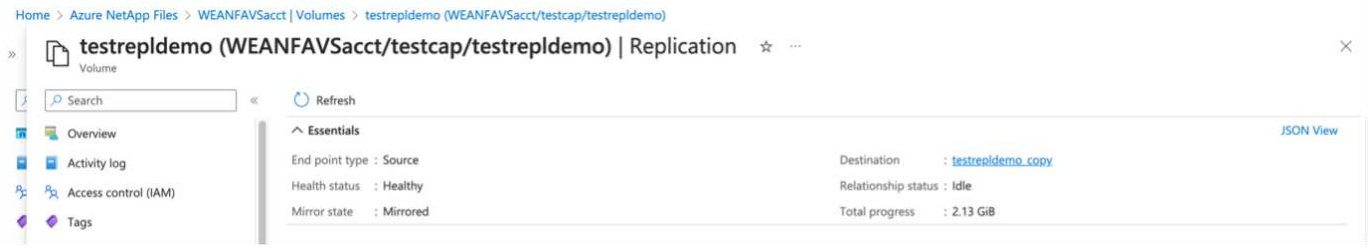
> 在初始版本中、DRO支持现有AVS SDDC集群。即将发布的版本将提供按需创建SDDC的功能。

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：

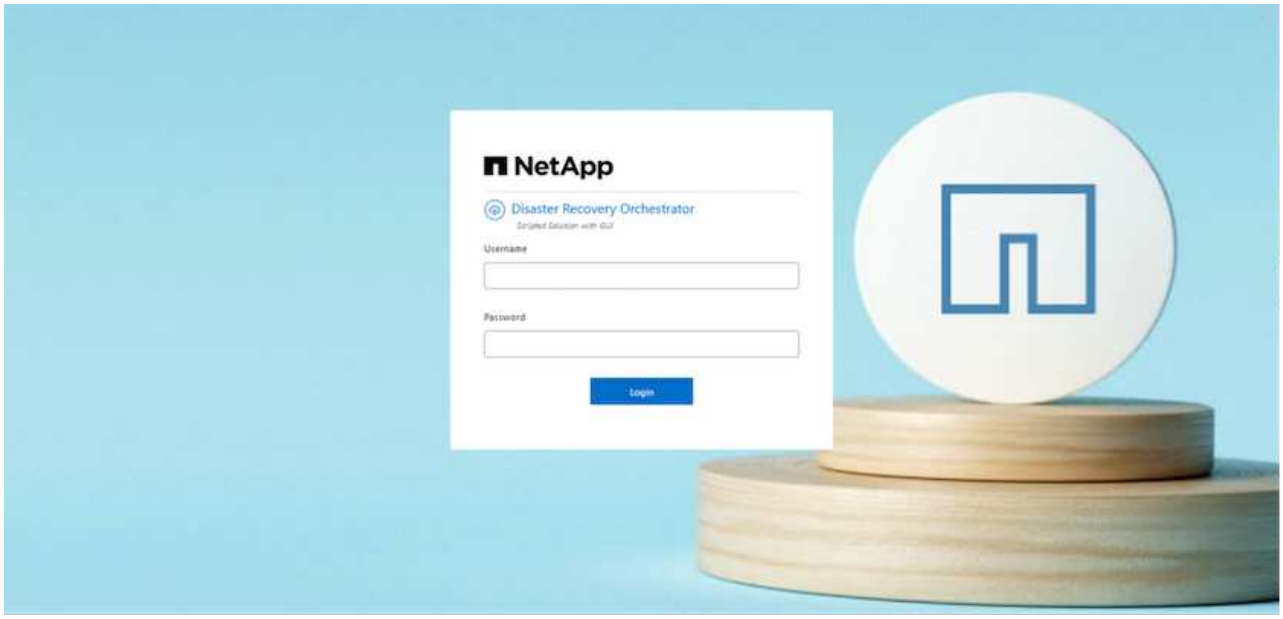
```
git clone https://github.com/NetApp/DRO-Azure.git
```

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。

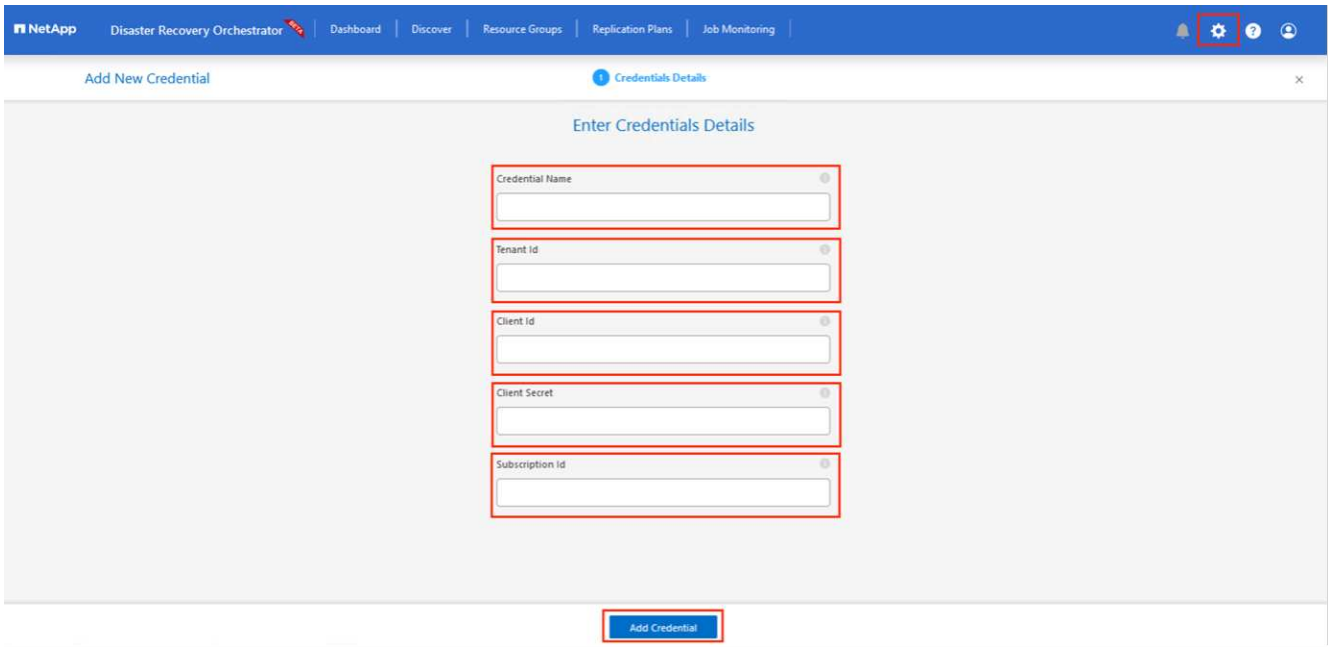
要执行此操作、请完成以下步骤：

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

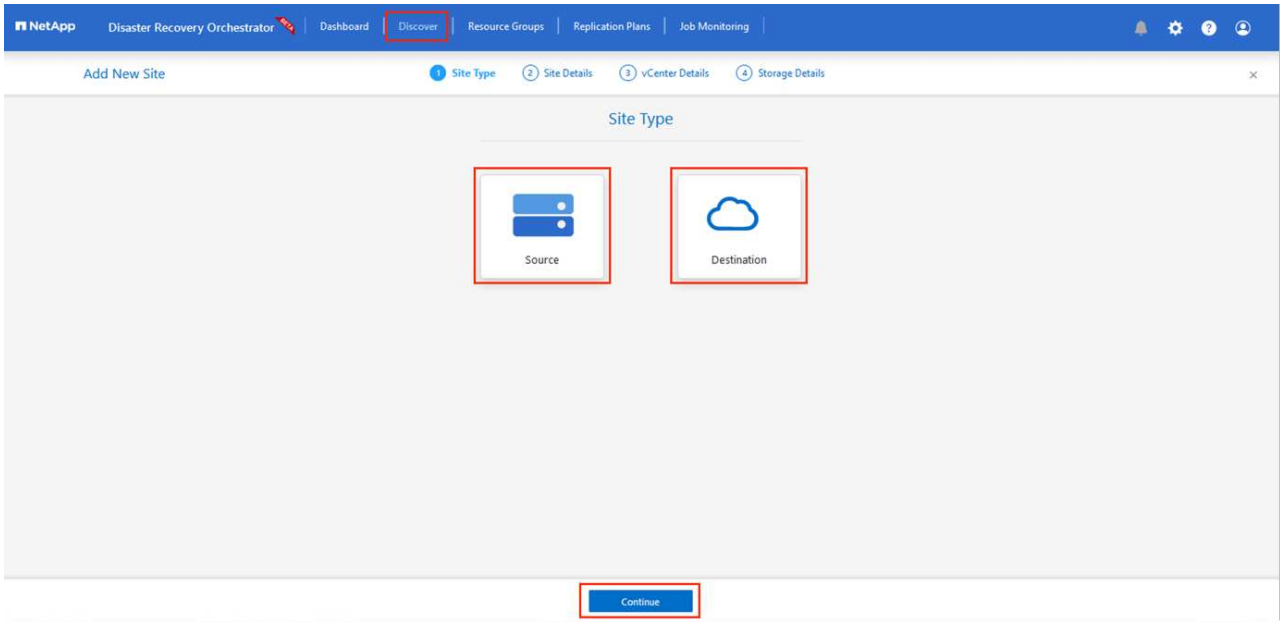
     创建AD应用程序时、您应已捕获此信息。

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：

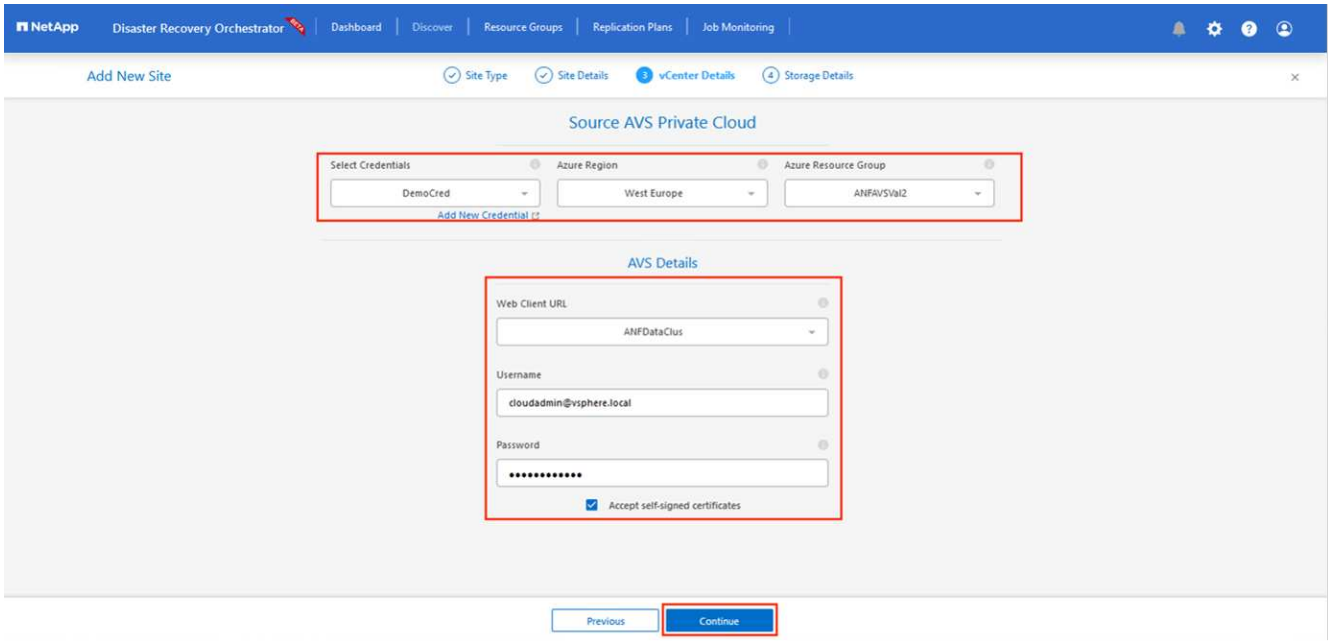
6. 转到*Discover (发现)*选项卡。
7. 单击*添加新站点*。
8. 添加以下主AVS站点(在控制台中指定为*Source*)。
   - SDDC vCenter
   - Azure NetApp Files 存储帐户
9. 添加以下二级AVS站点(在控制台中指定为*目标*)。
   - SDDC vCenter
   - Azure NetApp Files 存储帐户



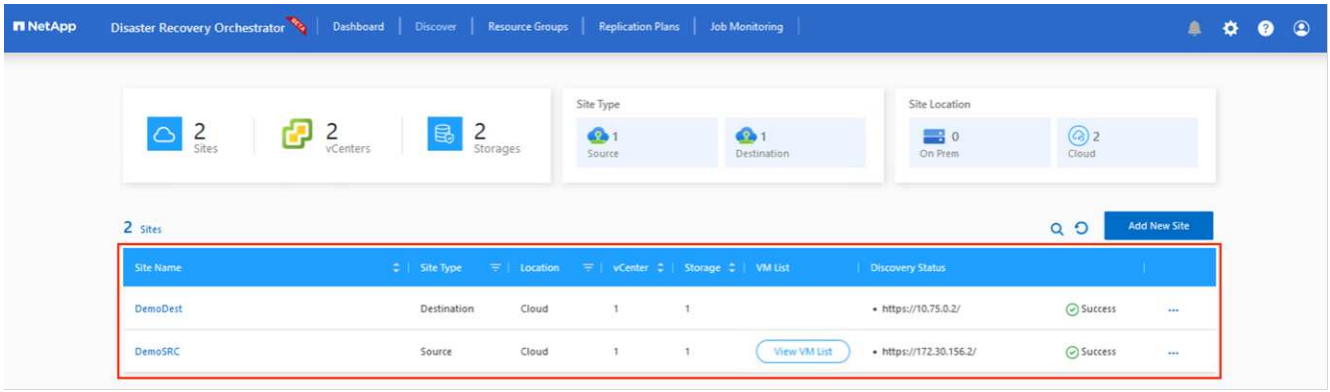
10. 通过单击*源*添加站点详细信息，输入友好的站点名称，然后选择连接器。然后单击 * 继续 * 。

> 为了便于演示、本文档将介绍如何添加源站点。

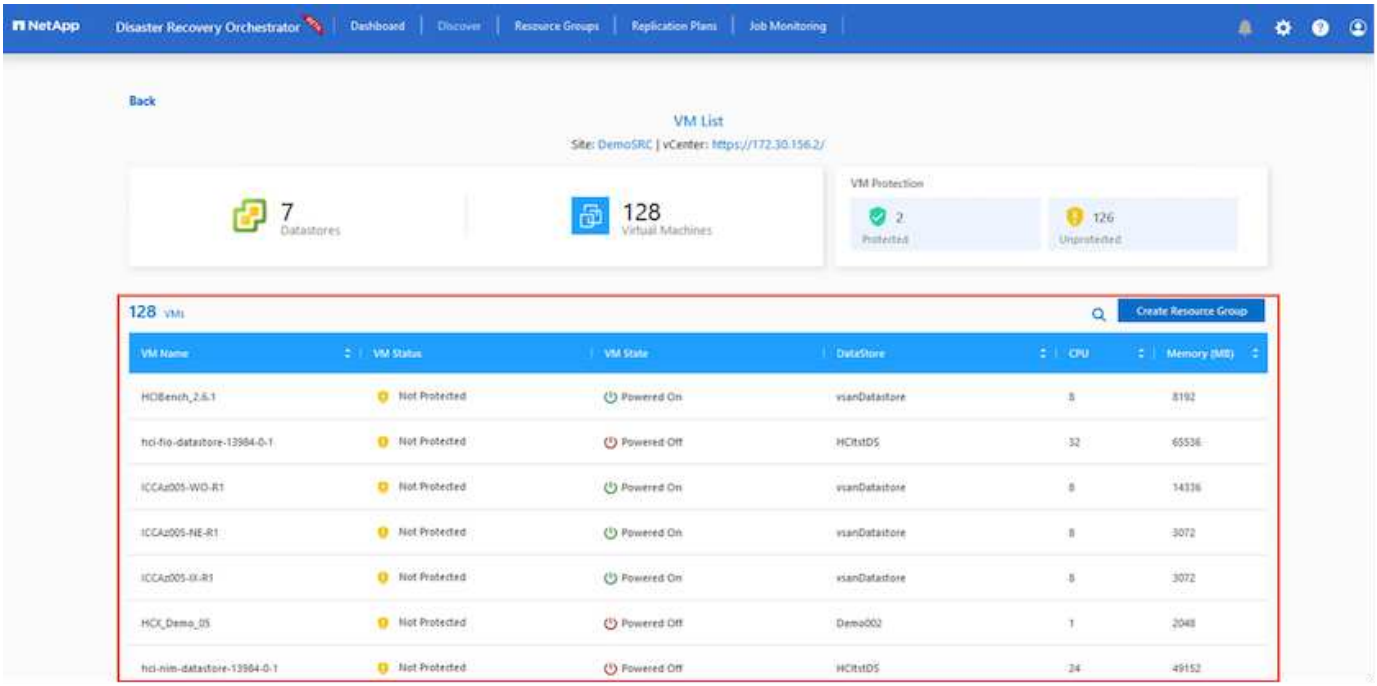
11. 更新vCenter详细信息。为此、请从主AVS SDDC的下拉列表中选择凭据、Azure区域和资源组。
12. DRO列出了该区域内的所有可用SDDC。从下拉列表中选择指定的私有云URL。
13. 输入 `cloudadmin@vsphere.local` 用户凭据。可从Azure门户访问此内容。请按照本中所述的步骤进行操作 "链接。"。完成后，单击*继续*。



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。



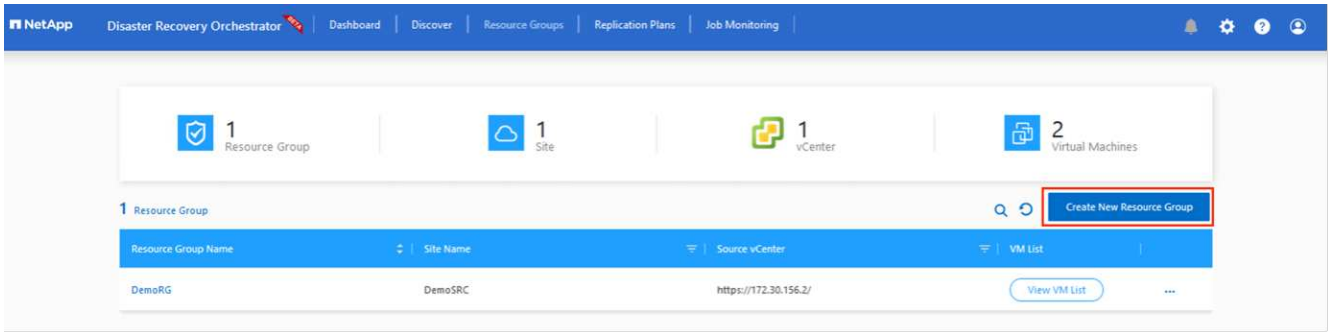
下一步是将所需的VM作为资源组分组到其功能组中。

资源分组

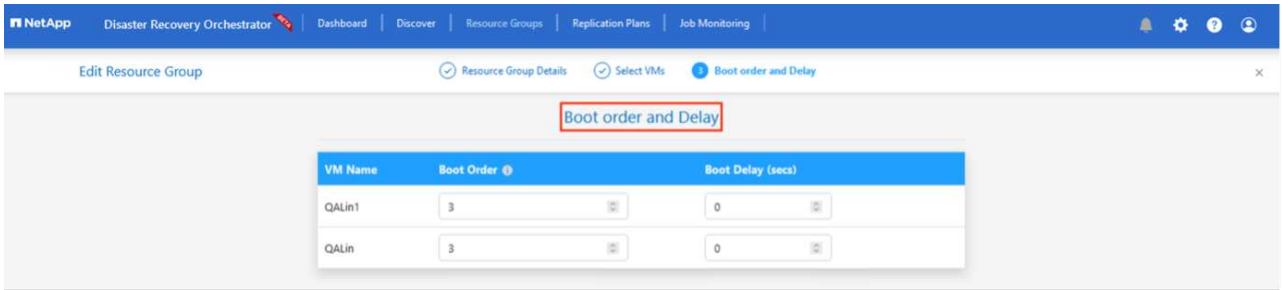
添加平台后、将要恢复的VM分组到资源组中。使用DRO资源组、您可以将一组依赖虚拟机分组到逻辑组中、这些逻辑组包含启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

要开始创建资源组，请单击*Create New Resource Group*菜单项。

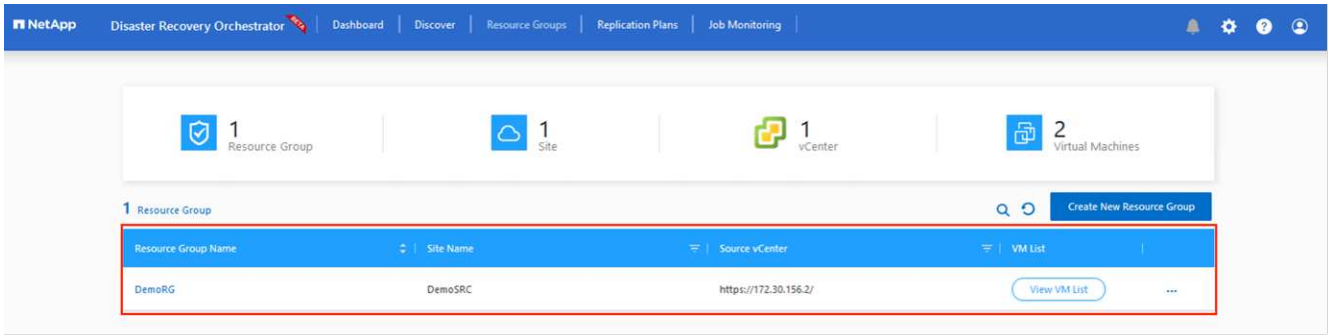
1. 访问*Resource Group*ps并单击*Create New Resource Group*。



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*。

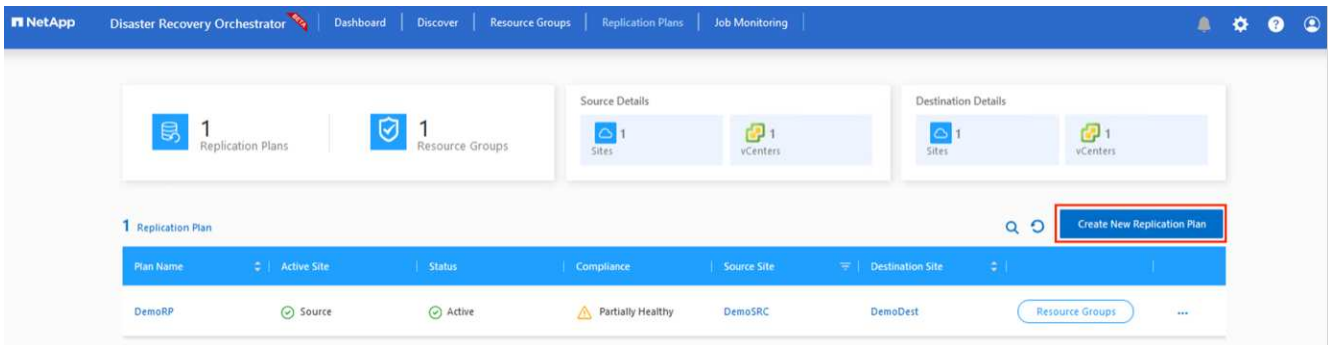


复制计划

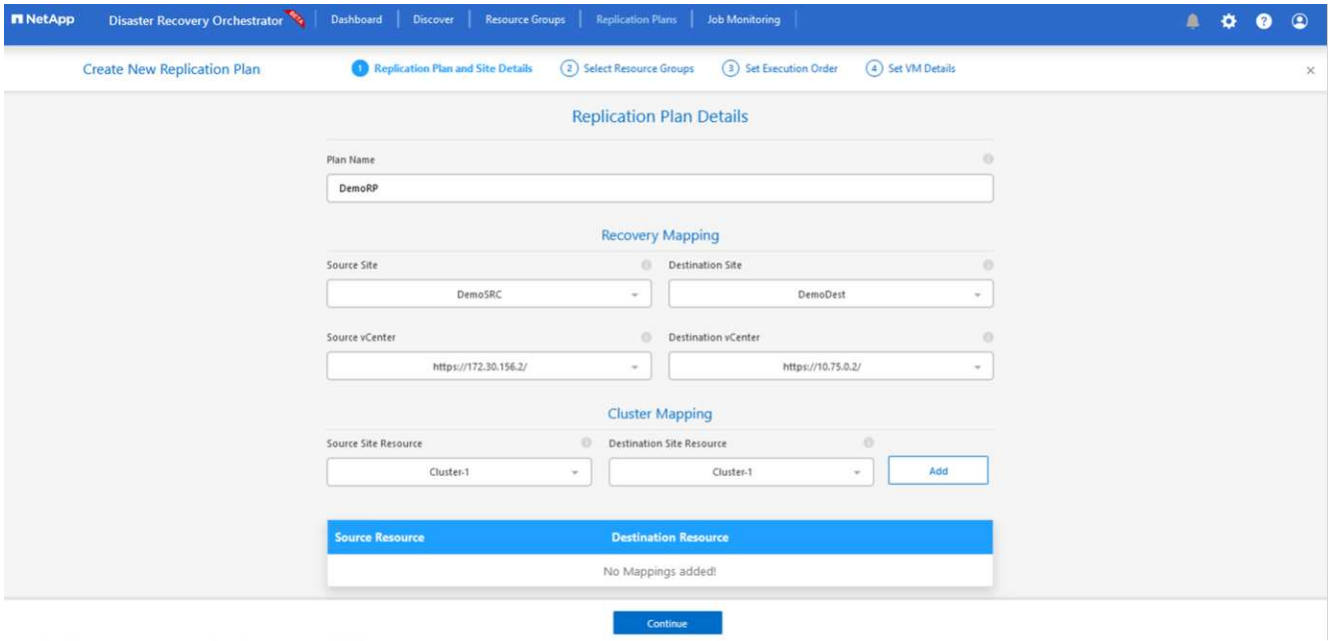
您必须制定在发生灾难时恢复应用程序的计划。从下拉列表中选择源和目标vCenter平台、选择要包含在此计划中的资源组、同时还包括应用程序应如何还原和启动的分组(例如、域控制器、第1层、第2层等)。计划通常也称为蓝图。要定义恢复计划，请导航到“复制计划”选项卡，然后单击*New Replication Plan*。

要开始创建复制计划、请完成以下步骤：

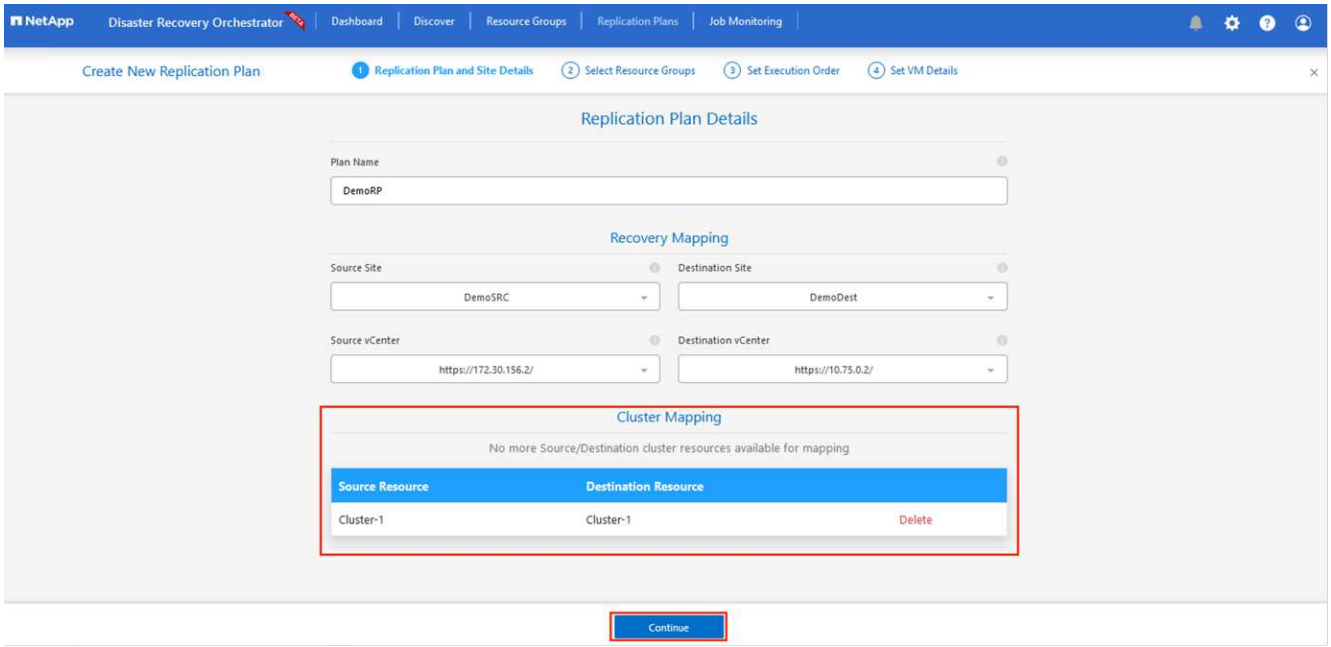
1. 导航到*复制计划*，然后单击*创建新复制计划*。



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。

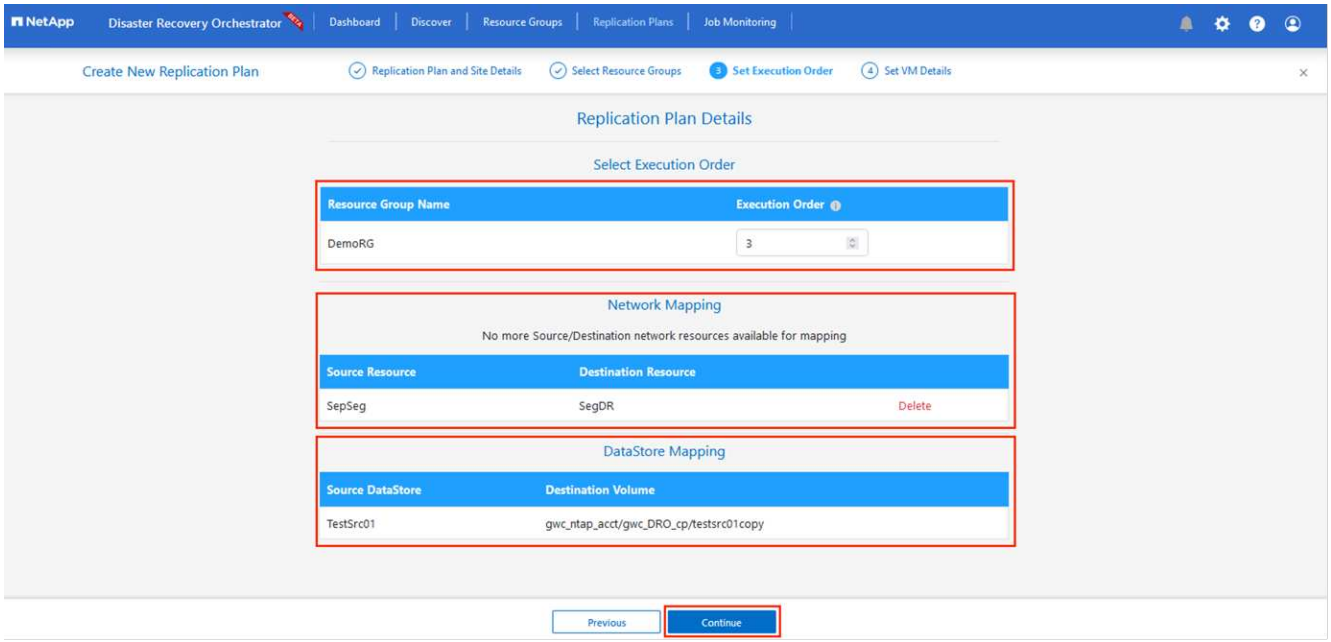


3. 恢复映射完成后，选择*Cluster Mapping*。



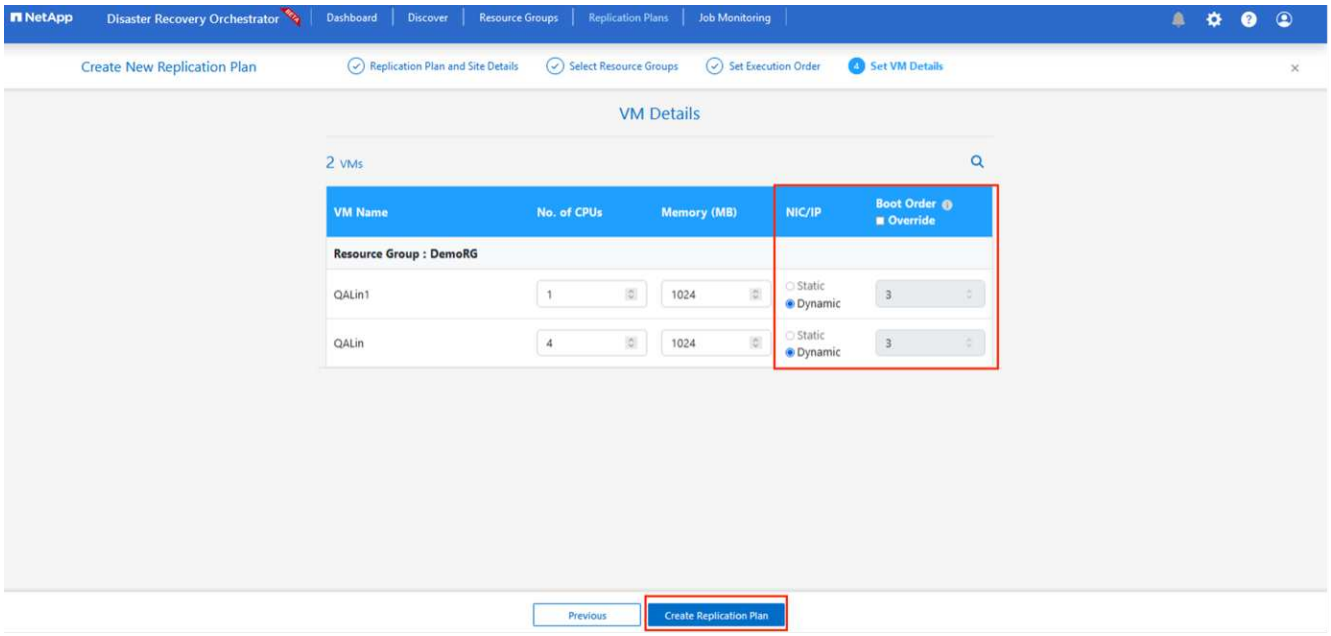
4. 选择*资源组详细信息*、然后单击*继续*。
5. 设置资源组的执行顺序。使用此选项可以选择存在多个资源组时的操作顺序。
6. 完成后、将网络映射设置为相应的网段。区块应已在二级AVS集群上配置、要将虚拟机映射到这些区块、请选择适当的区块。
7. 系统会根据所选虚拟机自动选择数据存储库映射。

> 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。

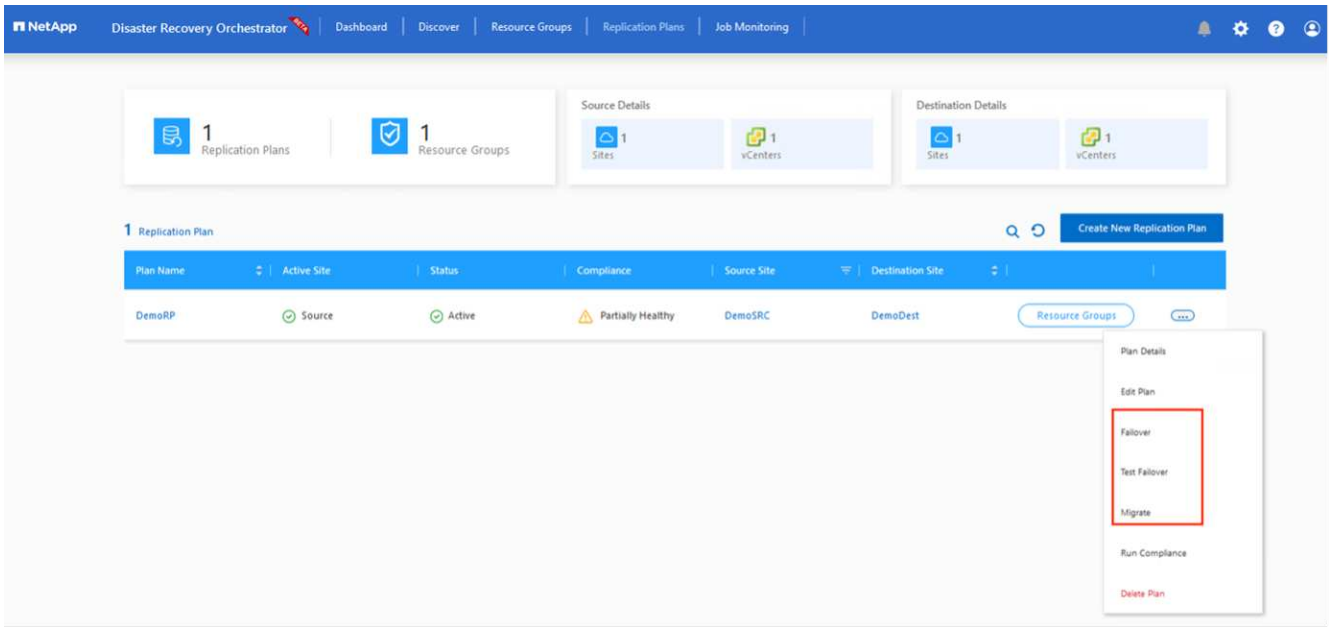


8. 在VM详细信息下、您可以选择调整VM CPU和RAM参数的大小。如果您要将大型环境恢复到较小的目标集群、或者在执行灾难恢复测试时无需配置一对一物理VMware基础架构、则此功能非常有用。此外、还可以修改资源组中所有选定VM的启动顺序和启动延迟(秒)。如果需要对您在资源组引导顺序选择期间选择的内容

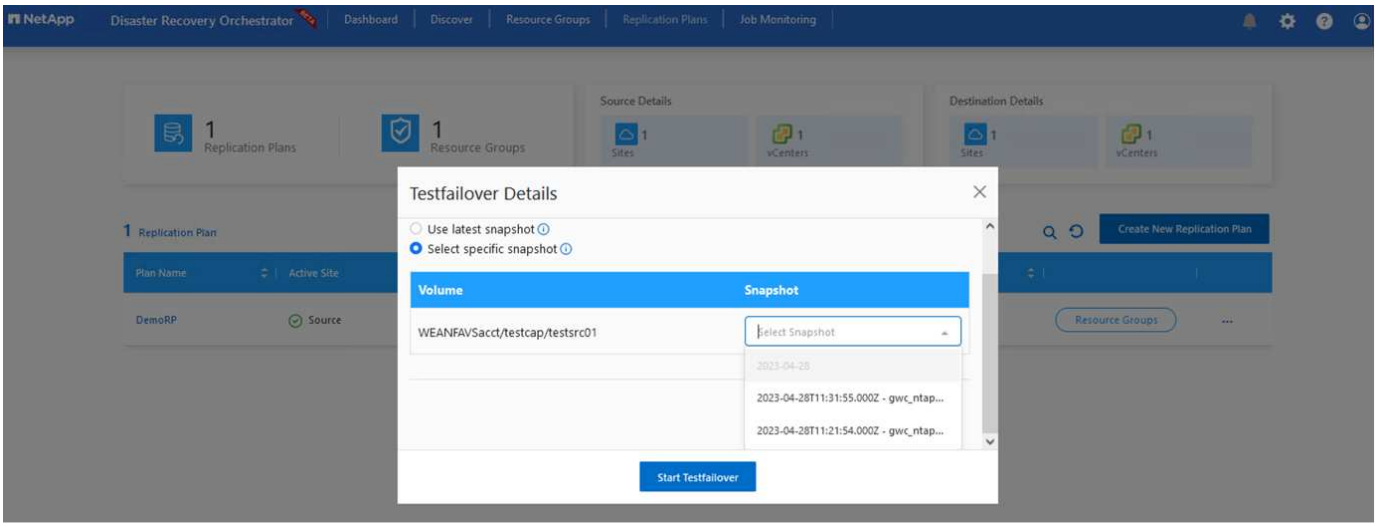
进行任何更改，则还可以使用一个附加选项来修改引导顺序。默认情况下、系统会使用在资源组选择期间选择的引导顺序、但在此阶段可以执行任何修改。



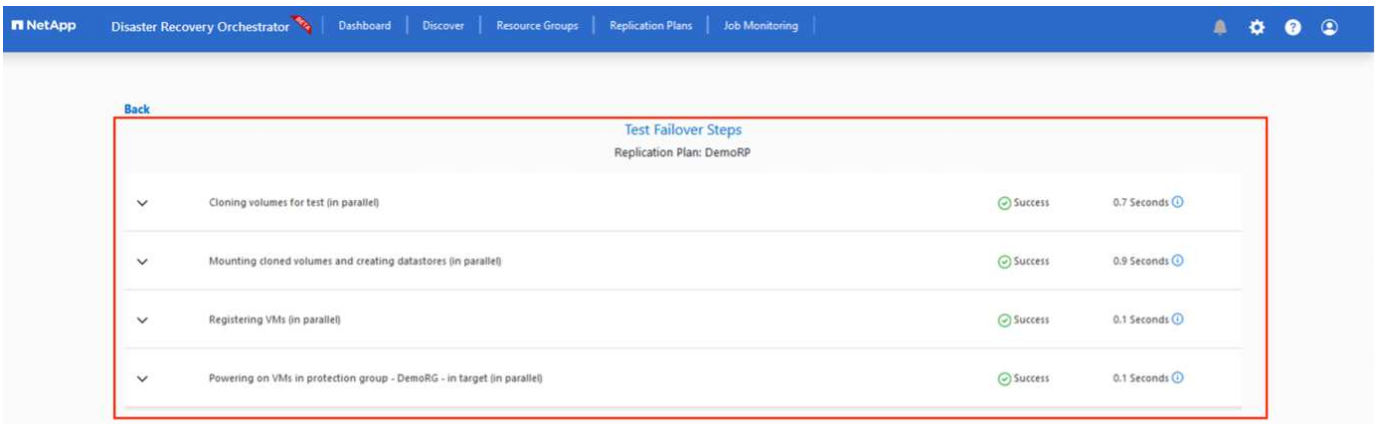
9. 单击*创建复制计划*。创建复制计划后，您可以根据需要执行故障转移、测试故障转移或迁移选项。



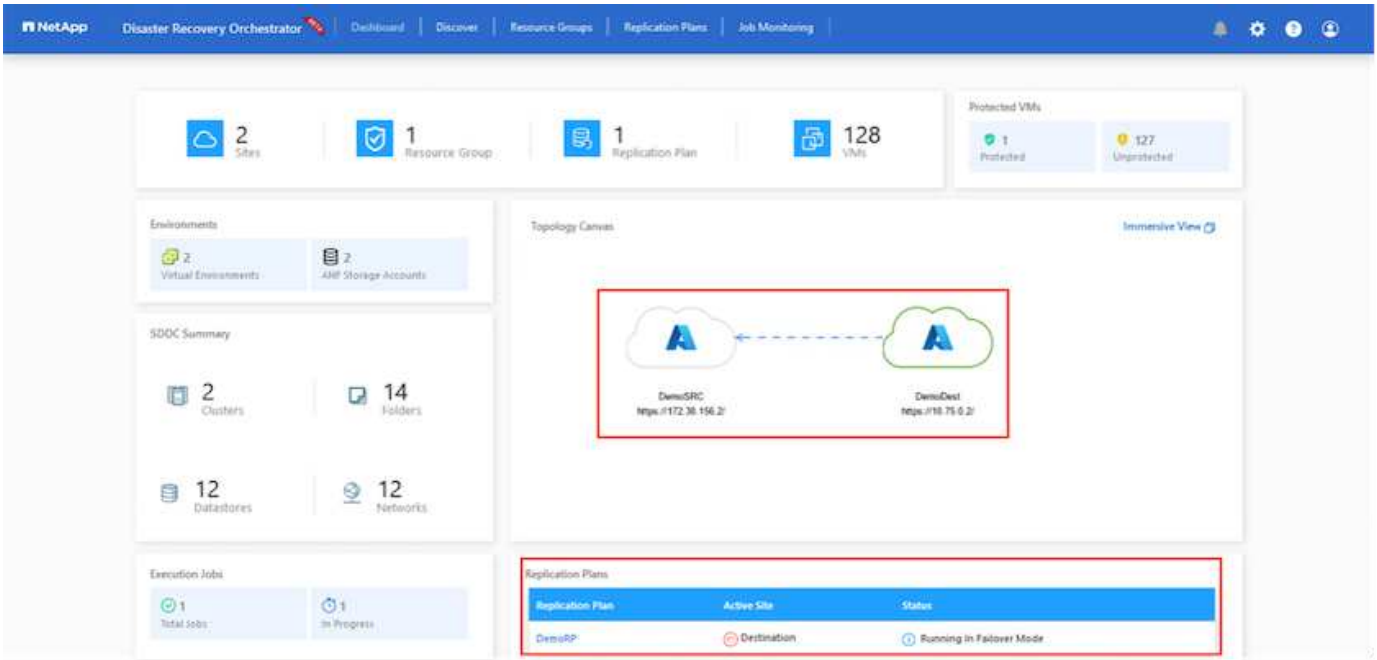
在故障转移和测试故障转移选项期间、将使用最新的快照、或者可以从时间点快照中选择特定快照。如果您正面临勒索软件等损坏事件、其中最新副本已被泄露或加密、则时间点选项非常有用。DRO显示所有可用的时间点。



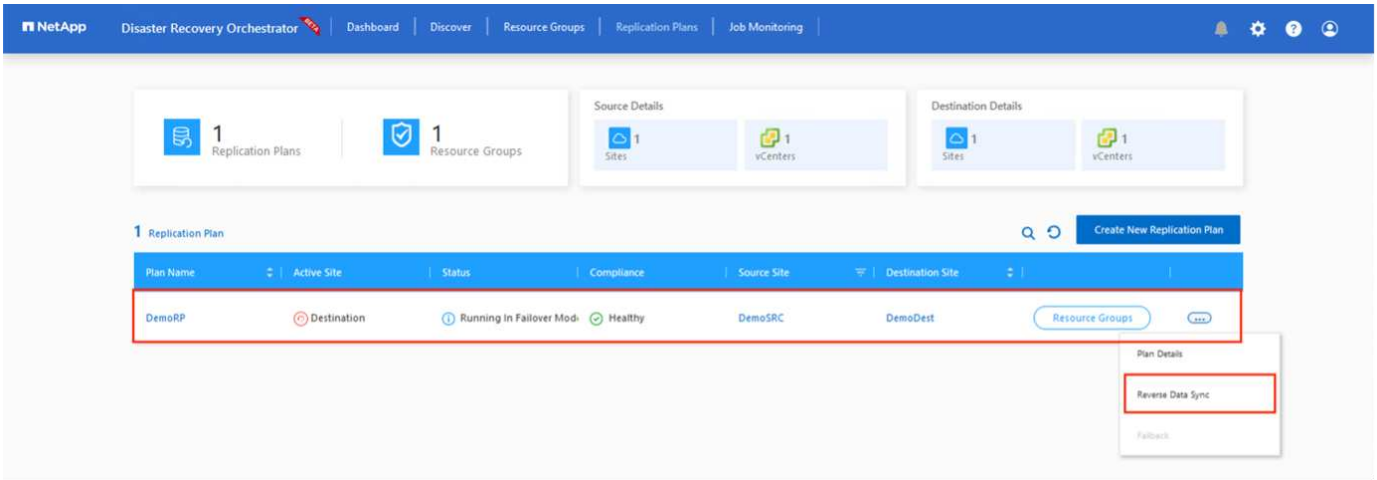
要使用复制计划中指定的配置触发故障转移或测试故障转移，可以单击*Failover或*Test Failover。您可以在任务菜单中监控复制计划。



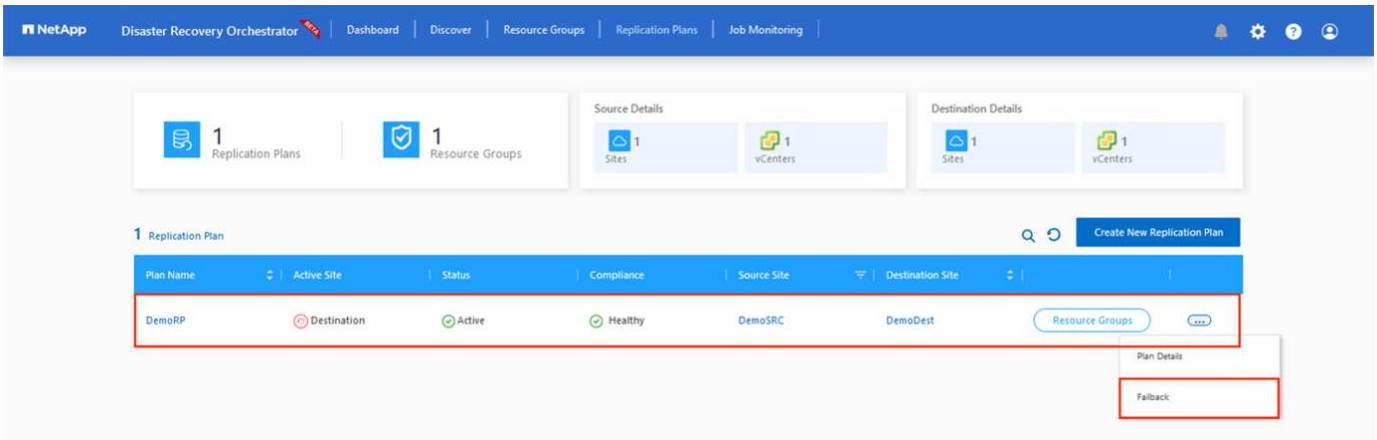
触发故障转移后、可以在二级站点AVS SDDC vCenter (VM、网络和数据存储库)中看到恢复的项目。默认情况下、VM会恢复到工作负载文件夹。

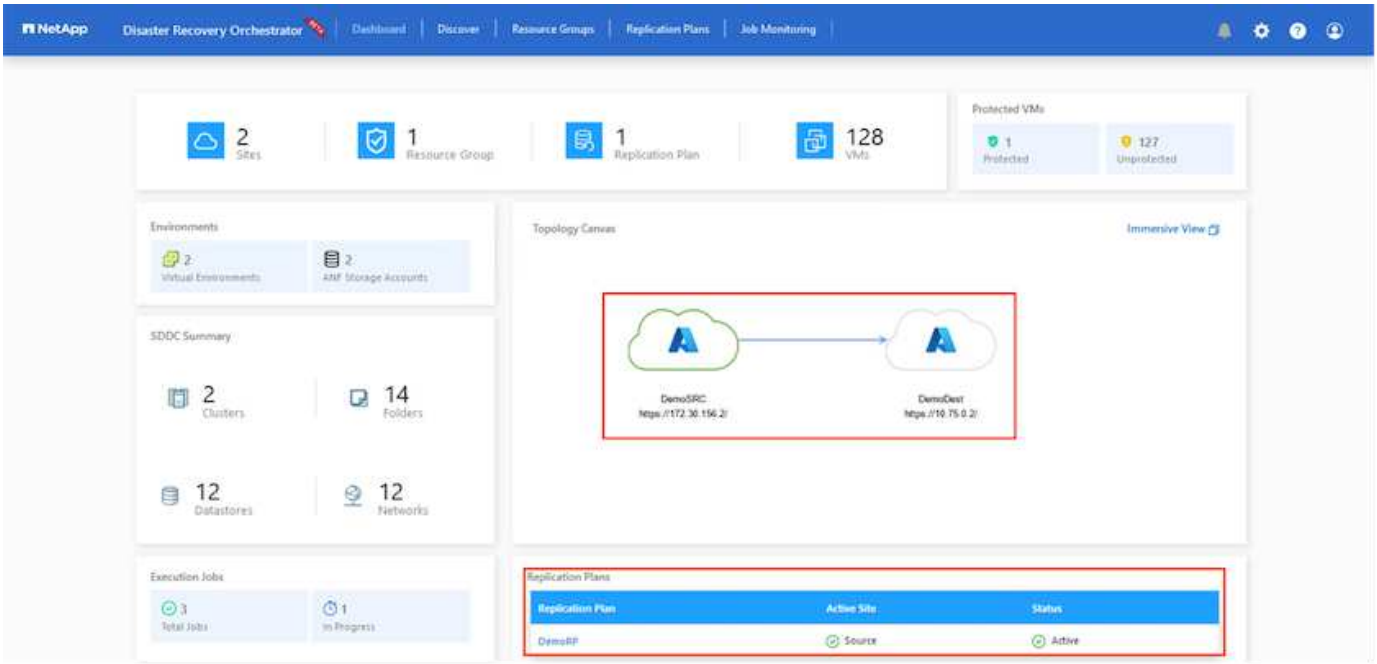


可以在复制计划级别触发故障恢复。如果发生测试故障转移、可使用拆卸选项回滚更改并删除新创建的卷。与故障转移相关的故障恢复过程分为两步。选择复制计划并选择*反向数据同步*。



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

  "https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html"

- 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