



NetApp Disaster Recovery文档

NetApp Disaster Recovery

NetApp
February 04, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/data-services-disaster-recovery/index.html> on February 04, 2026. Always check docs.netapp.com for the latest.

目录

- NetApp Disaster Recovery文档 1
- 发行说明 2
 - NetApp Disaster Recovery的新功能 2
 - 2026年1月12日 2
 - 2025年12月9日 3
 - 2025年12月1日 3
 - 2025年11月10日 3
 - 2025年10月6日 4
 - 2025年8月4日 4
 - 2025年7月14日 5
 - 2025年6月30日 6
 - 2025年6月23日 6
 - 2025年6月9日 6
 - 2025年5月13日 6
 - 2025年4月16日 8
 - 2025年3月10日 8
 - 2025年2月19日 9
 - 2024年10月30日 9
 - 2024年9月20日 11
 - 2024年8月2日 11
 - 2024年7月17日 11
 - 2024年7月5日 12
 - 2024年5月15日 13
 - 2024年3月5日 13
 - 2024年2月1日 14
 - 2024年1月11日 15
 - 2023年10月20日 15
 - 2023年9月27日 15
 - 2023年8月1日 16
 - 2023年5月18日 17
 - NetApp Disaster Recovery的局限性 17
 - 等待故障回复完成后再运行发现 17
 - NetApp Console可能无法发现Amazon FSx for NetApp ONTAP 17
 - Google Cloud NetApp Volumes的局限性 18
- 开始使用 19
 - 了解NetApp Disaster Recovery 19
 - NetApp Console 20
 - 使用NetApp Disaster Recoveryfor VMware 的优势 20
 - NetApp Disaster Recoveryfor VMware 的功能 21

成本	21
许可	22
30天免费试用	22
NetApp Disaster Recovery的工作原理	22
支持的保护目标和数据存储类型	24
可能对您有帮助的NetApp Disaster Recovery术语	24
NetApp Disaster Recovery前提条件	25
软件版本	25
Google Cloud 的先决条件和注意事项	25
ONTAP存储前提条件	26
VMware vCenter 集群先决条件	26
NetApp Console前提条件	27
工作负载先决条件	28
更多信息	28
NetApp Disaster Recovery快速入门	28
为NetApp Disaster Recovery设置基础架构	29
采用 VMware Cloud 和Amazon FSx for NetApp ONTAP 的混合云	29
私有云	31
访问NetApp Disaster Recovery	32
设置NetApp Disaster Recovery许可	33
使用 30 天免费试用版进行尝试	34
试用期结束后，通过其中一个市场进行订阅	35
试用结束后，通过NetApp购买 BYOL 许可证	36
许可证到期时更新	37
结束免费试用	37
使用NetApp Disaster Recovery	39
使用NetApp Disaster Recovery概述	39
在仪表板上查看NetApp Disaster Recovery计划的运行状况	39
将 vCenter 添加到NetApp Disaster Recovery中的站点	40
为 vCenter 站点添加子网映射	43
编辑 vCenter 服务器站点并自定义发现计划	45
手动刷新发现	47
在NetApp Disaster Recovery中创建资源组以组织虚拟机	48
在NetApp Disaster Recovery中创建复制计划	51
创建计划	52
编辑计划以测试合规性并确保故障转移测试有效	64
使用NetApp Disaster Recovery将应用程序复制到另一个站点	65
使用NetApp Disaster Recovery将应用程序迁移到另一个站点	66
使用NetApp Disaster Recovery将应用程序故障转移到远程站点	66
测试故障转移过程	67
故障转移测试后清理测试环境	68

将源站点故障转移到灾难恢复站点	68
使用NetApp Disaster Recovery将应用程序故障恢复到原始源	69
关于故障恢复	70
开始之前	70
步骤	70
使用NetApp Disaster Recovery管理站点、资源组、复制计划、数据存储库和虚拟机信息	70
管理 vCenter 站点	71
管理资源组	71
管理复制计划	72
查看数据存储信息	74
查看虚拟机信息	74
监控NetApp Disaster Recovery作业	75
查看职位	75
取消作业	75
创建NetApp Disaster Recovery报告	75
参考	77
用于 NetApp Disaster Recovery 的必需 vCenter 权限	77
使用NetApp Disaster Recovery时切换控制台代理	79
开始之前	79
步骤	79
更多信息	80
将NetApp Disaster Recovery与 Amazon EVS 结合使用	80
使用 Amazon Elastic VMware Service 和Amazon FSx for NetApp ONTAP实现NetApp Disaster Recovery	80
使用 Amazon EVS 和 Amazon FS for NetApp ONTAP 的NetApp Disaster Recovery解决方案概述	81
安装用于NetApp Disaster Recovery的NetApp Console代理	82
为 Amazon EVS 配置NetApp Disaster Recovery	83
为 Amazon EVS 创建复制计划	95
使用NetApp Disaster Recovery执行复制计划操作	108
NetApp Disaster Recovery常见问题解答	121
知识和支持	122
注册以获得支持	122
支持注册概述	122
注册NetApp Console以获取NetApp支持	122
关联 NSS 凭据以获得Cloud Volumes ONTAP支持	124
获取帮助	125
获取云提供商文件服务的支持	125
使用自助选项	125
向NetApp支持创建案例	126
管理您的支持案例	127
法律声明	129

版权	129
商标	129
专利	129
隐私政策	129
开源	129

NetApp Disaster Recovery文档

发行说明

NetApp Disaster Recovery的新功能

了解NetApp Disaster Recovery的新特性。

2026年1月12日

版本 4.2.9

支持本地环境中的多个控制台代理

如果您在本地使用灾难恢复，现在可以为每个 vCenter 实例部署控制台代理，从而提高恢复能力。

例如，如果您有两个站点（站点 A 和 B），则站点 A 可以将控制台代理 A 连接到 vCenter 1、ONTAP部署 1 和ONTAP部署 2。站点 B 可以将控制台代理 B 连接到 vCenter 2 和ONTAP部署 3 和 4。

有关灾难恢复中的控制台代理的信息，请参阅 ["创建控制台代理"](#)。

使用基于数据存储的保护机制，在故障转移后为复制计划添加虚拟机

当故障转移被触发时，任何使用基于数据存储的保护的复制计划都会包含已添加到数据存储中的虚拟机，前提是这些虚拟机已被发现。故障转移完成前，您必须提供新增虚拟机的映射详细信息。

有关详细信息，请参阅 ["故障转移应用程序"](#)。

新邮件通知

灾难恢复功能现在会针对以下事件发送电子邮件通知：

- 接近容量使用极限
- 报告生成完成
- 工作失败
- 许可证到期或违规

Swagger 改进

现在您可以从灾难恢复中访问 Swagger 文档。在灾难恢复中，选择设置，然后选择**API** 文档以链接到 Swagger，或者在浏览器的隐身/隐私模式下访问此 URL：["https://snapcenter.cloudmanager.cloud.netapp.com/api/api-doc/draas"](https://snapcenter.cloudmanager.cloud.netapp.com/api/api-doc/draas)。

改进的用户界面

灾难恢复功能现在提供更完善的警告和错误解决方法。此版本修复了导致已取消的作业无法在用户界面中显示的错误。已取消的职位现在可以查看了。当同一个目标网络映射到多个不同的源网络时，还会发出新的警告。

保留复制计划中默认添加的 **VM** 文件夹结构

创建复制时，新的默认设置是保留 VM 文件夹结构。如果恢复目标没有原始文件夹层次结构，灾难恢复程序会创建它。您可以取消选择此选项以忽略原始文件夹层次结构。

有关详细信息，请参阅 ["创建复制计划"](#)。

2025年12月9日

版本 4.2.8P1

文件夹层级结构保留

默认情况下，灾难恢复会在故障转移时保留虚拟机清单层次结构（文件夹结构）。如果恢复目标中没有所需的文件夹，灾难恢复功能会创建该文件夹。

现在您可以通过指定新的父 VM 文件夹或取消选中“保留原始文件夹层次结构”选项来覆盖此设置。

有关详细信息，请参阅 ["创建复制计划"](#)。

简化控制台代理更新

灾难恢复现在支持在工作环境中使用多个控制台代理的简化流程。要在控制台代理之间切换，您必须编辑 vCenter 配置，重新发现凭据，并刷新复制计划以使用新的控制台代理。

有关详细信息，请参阅 ["切换控制台代理"](#)。

2025年12月1日

版本 4.2.8

支持使用 **Google Cloud NetApp Volumes** 的 **Google Cloud VMware Engine**。

NetApp Disaster Recovery 现在支持使用 Google Cloud NetApp Volumes 的 Google Cloud VMware Engine 进行迁移、故障转移、故障恢复和测试操作。这种集成实现了本地环境和 Google Cloud 之间的无缝灾难恢复工作流程。

请务必仔细阅读。["前提条件"](#)和["限制"](#)适用于谷歌云。

2025年11月10日

版本 4.2.7

级联故障转移支持

现在您可以在 ONTAP 中配置级联关系，并使用该复制关系的任何分支进行灾难恢复。

注册期间降低 **VMware** 硬件支持级别

灾难恢复功能现在支持在注册过程中将 VMware 硬件降级到早期版本的 vSphere。当源 ESX 主机运行的版本比灾难恢复站点的版本更新时，这非常有用。

有关详细信息，请参阅 ["在NetApp Disaster Recovery中创建复制计划"](#)。

优雅关机

灾难恢复现在会优雅地关闭虚拟机，而不是直接断电。如果某个虚拟机关机时间超过十分钟，灾难恢复功能会将其关闭。

备份前脚本支持

现在您可以将自定义脚本注入到故障转移工作流程中，以便在创建备份之前运行。备份前脚本允许您在复制快照之前控制虚拟机的状态，并为虚拟机的转换做好准备。例如，您可以注入一个脚本来卸载 NFS 挂载点，然后在故障转移后使用另一个脚本重新挂载该挂载点。

有关详细信息，请参阅 ["在NetApp Disaster Recovery中创建复制计划"](#)。

2025年10月6日

版本 4.2.6

BlueXP disaster recovery现已更名为NetApp Disaster Recovery

BlueXP disaster recovery已重命名为NetApp Disaster Recovery。

BlueXP现在是NetApp Console

NetApp Console建立在增强和重组的BlueXP基础之上，可在企业级内部和云环境中集中管理NetApp存储和NetApp Data Services，提供实时洞察、更快的工作流程和简化的管理，并且高度安全且合规。

有关具体变更内容，请参阅..... ["NetApp Console发行说明"](#)。

其他更新

- Amazon Elastic VMware Service (EVS) 与Amazon FSx for NetApp ONTAP的支持已公开预览。随着此版本的发布，它现已普遍可用。有关详细信息，请参阅["使用 Amazon Elastic VMware Service 和Amazon FSx for NetApp ONTAP实现NetApp Disaster Recovery"](#)。
- 存储发现改进，包括减少本地部署的发现时间
- 身份和访问管理 (IAM) 支持，包括基于角色的访问控制 (RBAC) 和增强的用户权限
- 对 Azure VMware 解决方案和Cloud Volumes ONTAP 的私人预览支持。有了此支持，您现在可以使用Cloud Volumes ONTAP存储配置从本地到 Azure VMware 解决方案的灾难恢复保护。

2025年8月4日

版本 4.2.5P2

NetApp Disaster Recovery更新

此版本包括以下更新：

- 改进了 VMFS 支持，以处理来自多个存储虚拟机的相同 LUN。

- 改进了测试拆卸清理以处理已被卸载或删除的数据存储。
- 改进了子网映射，以便现在可以验证输入的网关是否包含在提供的网络中。
- 解决了虚拟机名称包含“.com”时可能导致复制计划失败的问题。
- 在创建复制计划的过程中，删除了阻止目标卷与源卷相同的限制。
- 在 Azure 市场中添加了对NetApp智能服务的即用即付 (PAYGO) 订阅支持，并在免费试用对话框中添加了 Azure 市场的链接。

详情请见 ["NetApp Disaster Recovery许可"](#)和 ["设置NetApp Disaster Recovery许可"](#)。

2025年7月14日

版本 4.2.5

NetApp Disaster Recovery中的用户角色

NetApp Disaster Recovery现在采用角色来管理每个用户对特定功能和操作的访问权限。

该服务使用特定于NetApp Disaster Recovery的以下角色。

- 灾难恢复管理员：在NetApp Disaster Recovery中执行任何操作。
- 灾难恢复故障转移管理员：在NetApp Disaster Recovery中执行故障转移和迁移操作。
- 灾难恢复应用程序管理员：创建和修改复制计划并启动测试故障转移。
- 灾难恢复查看器：查看NetApp Disaster Recovery中的信息，但不能执行任何操作。

如果您单击NetApp Disaster Recovery服务并首次对其进行配置，则必须具有 **SnapCenterAdmin** 权限或具有 **Organization Admin** 角色。

有关详细信息，请参阅["NetApp Disaster Recovery中的用户角色和权限"](#)。

["了解所有服务的访问角色"](#)。

NetApp Disaster Recovery中的其他更新

- 增强网络发现
- 可扩展性改进：
 - 过滤所需的元数据而不是所有细节
 - 发现改进，以更快地检索和更新虚拟机资源
 - 数据检索和数据更新的内存优化和性能优化
 - vCenter SDK 客户端创建和池管理改进
- 下次计划或手动发现时的陈旧数据管理：
 - 当在 vCenter 中删除虚拟机时， NetApp Disaster Recovery现在会自动将其从复制计划中删除。
 - 当 vCenter 中删除数据存储区或网络时， NetApp Disaster Recovery现在会将其从复制计划和资源组中删除。

- 当在 vCenter 中删除集群、主机或数据中心时，NetApp Disaster Recovery 现在会将其从复制计划和资源组中删除。
- 您现在可以在浏览器的隐身模式下访问 Swagger 文档。您可以从 NetApp Disaster Recovery 中的“设置”选项 > “API 文档”中访问它，也可以在浏览器的隐身模式下直接通过以下 URL 访问它：["Swagger 文档"](#)。
- 在某些情况下，故障回复操作完成后，iGroup 会被遗留下来。如果 iGroup 已过时，则此更新会将其删除。
- 如果在复制计划中使用了 NFS FQDN，NetApp Disaster Recovery 现在会将其解析为 IP 地址。如果灾难恢复站点中无法解析 FQDN，则此更新很有用。
- UI 对齐改进
- 成功发现后，记录捕获 vCenter 大小详细信息的日志改进

2025年6月30日

版本 4.2.4P2

发现改进

此更新改进了发现过程，从而减少了发现所需的时间。

2025年6月23日

版本 4.2.4P1

子网映射改进

此更新通过新的搜索功能增强了“添加和编辑子网映射”对话框。现在您可以通过输入搜索词快速找到特定子网，从而更轻松地管理子网映射。

2025年6月9日

版本 4.2.4

Windows 本地管理员密码解决方案 (LAPS) 支持

Windows 本地管理员密码解决方案 (Windows LAPS) 是 Windows 的一项功能，可自动管理和备份 Active Directory 上本地管理员帐户的密码。

您现在可以通过提供域控制器详细信息来选择子网映射选项并检查 LAPS 选项。使用此选项，您不需要为每个虚拟机提供密码。

有关详细信息，请参阅 ["创建复制计划"](#)。

2025年5月13日

版本 4.2.3

子网映射

在此版本中，您可以使用子网映射以新的方式管理故障转移时的 IP 地址，这使您能够为每个 vCenter 添加子

网。当您这样做时，您需要为每个虚拟网络定义 IPv4 CIDR、默认网关和 DNS。

故障转移时，NetApp Disaster Recovery通过查看为映射的虚拟网络提供的 CIDR 来确定每个 vNIC 的适当 IP 地址，并使用它来派生新的 IP 地址。

例如：

- 网络A = 10.1.1.0/24
- 网络B = 192.168.1.0/24

VM1 有一个连接到 NetworkA 的 vNIC (10.1.1.50)。在复制计划设置中，NetworkA 映射到 NetworkB。

故障转移时，NetApp Disaster Recovery会替换原始 IP 地址 (10.1.1) 的网络部分，并保留原始 IP 地址 (10.1.1.50) 的主机地址 (.50)。对于 VM1，NetApp Disaster Recovery查看 NetworkB 的 CIDR 设置，并使用 NetworkB 网络部分 192.168.1，同时保留主机部分 (.50) 来为 VM1 创建新的 IP 地址。新的IP变为 192.168.1.50。

总之，主机地址保持不变，而网络地址则被站点子网映射中配置的地址替换。这使您能够更轻松的管理故障转移时的 IP 地址重新分配，特别是当您需要管理数百个网络和数千个虚拟机时。

有关如何在站点中包含子网映射的详细信息，请参阅 ["添加 vCenter 服务器站点"](#)。

跳过保护

您现在可以跳过保护，以便服务在复制计划故障转移后不会自动创建反向保护关系。如果您希望在NetApp Disaster Recovery中将恢复的站点恢复在线之前对其执行其他操作，这将非常有用。

当您启动故障转移时，如果原始源站点处于在线状态，则默认情况下服务会自动为复制计划中的每个卷创建反向保护关系。这意味着该服务创建从目标站点到源站点的SnapMirror关系。当您启动故障恢复时，该服务还会自动逆转SnapMirror关系。

启动故障转移时，您现在可以选择“跳过保护”选项。这样，服务就不会自动逆转SnapMirror关系。相反，它可将写卷留在复制计划的两侧。

原始源站点恢复在线后，您可以通过从复制计划操作菜单中选择*保护资源*来建立反向保护。这会尝试为计划中的每个卷创建反向复制关系。您可以重复运行此作业，直到恢复保护。当保护恢复后，您可以按照通常的方式启动故障恢复。

有关跳过保护的详细信息，请参阅 ["将应用程序故障转移到远程站点"](#)。

复制计划中的**SnapMirror**计划更新

NetApp Disaster Recovery现在支持使用外部快照管理解决方案，例如本机ONTAP SnapMirror策略调度程序或与ONTAP 的第三方集成。如果复制计划中的每个数据存储库（卷）都已具有在其他地方管理的SnapMirror关系，则可以将这些快照用作NetApp Disaster Recovery中的恢复点。

要进行配置，请在复制计划 > 资源映射部分中，在配置数据存储映射时选中 使用平台管理的备份和保留计划 复选框。

选择该选项后，NetApp Disaster Recovery不会配置备份计划。但是，您仍然需要配置保留计划，因为仍可能需要拍摄快照以进行测试、故障转移和故障回复操作。

配置完成后，服务不会定期拍摄任何快照，而是依赖外部实体来拍摄和更新这些快照。

有关在复制计划中使用外部快照解决方案的详细信息，请参阅：["创建复制计划"](#)。

2025年4月16日

版本 4.2.2

虚拟机的计划发现

NetApp Disaster Recovery每 24 小时执行一次发现。通过此版本，您现在可以自定义发现计划以满足您的需求并在需要时减少对性能的影响。例如，如果您有大量虚拟机，则可以将发现计划设置为每 48 小时运行一次。如果您拥有的虚拟机数量较少，则可以将发现计划设置为每 12 小时运行一次。

如果您不想安排发现，您可以禁用计划发现选项并随时手动刷新发现。

有关详细信息，请参阅["添加 vCenter 服务器站点"](#)。

资源组数据存储支持

以前，您只能通过虚拟机创建资源组。在此版本中，您可以按数据存储创建资源组。当您创建复制计划并为该计划创建资源组时，数据存储区中的所有虚拟机都将被列出。如果您有大量虚拟机并希望按数据存储对它们进行分组，这将非常有用。

您可以通过以下方式创建具有数据存储区的资源组：

- 当您使用数据存储区添加资源组时，您可以看到数据存储区的列表。您可以选择一个或多个数据存储来创建资源组。
- 当您创建复制计划并在计划内创建资源组时，您可以在数据存储区中看到虚拟机。

有关详细信息，请参阅["创建复制计划"](#)。

免费试用或许可证到期通知

此版本提供免费试用将在 60 天后到期的通知，以确保您有时间获得许可证。此版本还在许可证到期当天提供通知。

服务更新通知

在此版本中，顶部会出现一个横幅，表明服务正在升级并且服务处于维护模式。服务升级时横幅出现，升级完成后横幅消失。虽然您可以在升级过程中继续在 UI 中工作，但您无法提交新作业。更新完成后，计划作业将运行，服务将返回生产模式。

2025年3月10日

版本 4.2.1

智能代理支持

NetApp Console代理支持智能代理。智能代理是一种将您的内部部署系统连接到NetApp Disaster Recovery的轻量级、安全且高效的方法。它在您的系统和NetApp Disaster Recovery之间提供安全连接，而无需 VPN 或直接互联网访问。这种优化的代理实现可卸载本地网络内的 API 流量。

配置代理后，NetApp Disaster Recovery会尝试直接与 VMware 或ONTAP通信，如果直接通信失败，则使用配置的代理。

NetApp Disaster Recovery代理实施需要使用 HTTPS 协议在控制台代理与任何 vCenter Server 和ONTAP阵列之间进行端口 443 通信。控制台代理内的NetApp Disaster Recovery代理在执行任何操作时直接与 VMware vSphere、VC 或ONTAP通信。

有关NetApp Disaster Recovery智能代理的更多信息，请参阅 ["为NetApp Disaster Recovery设置基础架构"](#)。

有关NetApp Console中常规代理设置的更多信息，请参阅 ["配置控制台代理以使用代理服务器"](#)。

随时结束免费试用

您可以随时停止免费试用，也可以等到试用期结束。

看 ["结束免费试用"](#)。

2025年2月19日

4.2 版

ASA r2 支持 VMFS 存储上的虚拟机和数据存储

此版本的NetApp Disaster Recovery为 VMFS 存储上的虚拟机和数据存储区提供ASA r2 支持。在ASA r2 系统上，ONTAP软件支持基本的 SAN 功能，同时删除 SAN 环境中不支持的功能。

此版本支持ASA r2 的以下功能：

- 主存储的一致性组配置（仅限平面一致性组，即只有一个级别，没有层次结构）
- 备份（一致性组）操作，包括SnapMirror自动化

NetApp Disaster Recovery中对ASA r2 的支持使用ONTAP 9.16.1。

虽然数据存储库可以挂载在ONTAP卷或ASA r2 存储单元上，NetApp Disaster Recovery中的资源组不能同时包含来自ONTAP的数据存储库和来自ASA r2 的数据存储库。您可以从ONTAP中选择一个数据存储区，也可以从资源组中的ASA r2 中选择一个数据存储区。

2024年10月30日

报告

您现在可以生成和下载报告来帮助您分析您的景观。预先设计的报告总结了故障转移和故障回复，显示了所有站点上的复制详细信息，并显示了过去七天的作业详细信息。

参考 ["创建灾难恢复报告"](#)。

30天免费试用

您现在可以注册NetApp Disaster Recovery30 天免费试用版。此前，免费试用期为 90 天。

参考 ["设置许可"](#)。

禁用和启用复制计划

先前的版本包括对故障转移测试计划结构的更新，这是支持每日和每周计划所必需的。此更新要求您禁用并重新启用所有现有的复制计划，以便您能够使用新的每日和每周故障转移测试计划。这是一次性要求。

方法如下：

1. 从菜单中选择*复制计划*。
2. 选择一个计划并选择操作图标以显示下拉菜单。
3. 选择*禁用*。
4. 几分钟后，选择*启用*。

文件夹映射

当您创建复制计划并映射计算资源时，您现在可以映射文件夹，以便在您为数据中心、集群和主机指定的文件夹中恢复虚拟机。

有关详细信息，请参阅 ["创建复制计划"](#)。

可用于故障转移、故障回复和测试故障转移的虚拟机详细信息

当发生故障并且您正在启动故障转移、执行故障回复或测试故障转移时，您现在可以查看虚拟机的详细信息并确定哪些虚拟机未重新启动。

参考 ["将应用程序故障转移到远程站点"](#)。

具有有序启动顺序的 VM 启动延迟

创建复制计划时，您现在可以为计划中的每个 VM 设置启动延迟。这使您可以设置虚拟机的启动顺序，以确保所有优先级为一的虚拟机都在后续优先级虚拟机启动之前运行。

有关详细信息，请参阅 ["创建复制计划"](#)。

虚拟机操作系统信息

创建复制计划时，您现在可以看到计划中每个虚拟机的操作系统。这有助于决定如何将虚拟机分组到资源组中。

有关详细信息，请参阅 ["创建复制计划"](#)。

VM 名称别名

创建复制计划时，您现在可以在灾难恢复站点上为虚拟机名称添加前缀和后缀。这使您能够为计划中的虚拟机使用更具描述性的名称。

有关详细信息，请参阅 ["创建复制计划"](#)。

清理旧快照

您可以删除超出指定保留数量的不再需要的快照。当您降低快照保留计数时，快照可能会随着时间的推移而累积，现在您可以删除它们以释放空间。您可以随时根据需要或在删除复制计划时执行此操作。

有关详细信息，请参阅 ["管理站点、资源组、复制计划、数据存储和虚拟机信息"](#)。

协调快照

您现在可以协调源和目标之间不同步的快照。如果在NetApp Disaster Recovery之外的目标上删除快照，则可能会发生这种情况。该服务每 24 小时自动删除源上的快照。但是，您可以根据需要执行此操作。此功能使您能够确保快照在所有站点上都是一致的。

有关详细信息，请参阅 ["管理复制计划"](#)。

2024年9月20日

支持本地到本地 **VMware VMFS** 数据存储区

此版本支持安装在 VMware vSphere 虚拟机文件系统 (VMFS) 数据存储上的虚拟机，用于受 iSCSI 和 FC 保护的本地存储。此前，该服务提供了支持 iSCSI 和 FC 的 VMFS 数据存储的_技术预览_。

以下是有关 iSCSI 和 FC 协议的一些其他注意事项：

- FC 支持针对客户端前端协议，而不是针对复制。
- NetApp Disaster Recovery仅支持每个ONTAP卷一个 LUN。该卷不应具有多个 LUN。
- 对于任何复制计划，目标ONTAP卷都应使用与托管受保护虚拟机的源ONTAP卷相同的协议。例如，如果源使用 FC 协议，则目标也应该使用 FC。

2024年8月2日

支持 **FC** 的本地到本地 **VMware VMFS** 数据存储区

此版本包括对安装在 VMware vSphere 虚拟机文件系统 (VMFS) 数据存储上的虚拟机的支持的_技术预览_，用于对本地存储进行 FC 保护。此前，该服务提供了支持 iSCSI VMFS 数据存储的技术预览。



NetApp不会向您收取任何预览的工作负载容量的费用。

取消作业

在此版本中，您现在可以在作业监视器 UI 中取消作业。

参考 ["监控作业"](#)。

2024年7月17日

故障转移测试计划

此版本包括对故障转移测试计划结构的更新，这是支持每日和每周计划所必需的。此更新要求您禁用并重新启用所有现有的复制计划，以便您能够使用新的每日和每周故障转移测试计划。这是一次性要求。

方法如下：

1. 从菜单中选择*复制计划*。

2. 选择一个计划并选择操作图标以显示下拉菜单。
3. 选择*禁用*。
4. 几分钟后，选择*启用*。

复制计划更新

此版本包括复制计划数据的更新，解决了“未找到快照”的问题。这要求您将所有复制计划中的保留计数更改为 1 并启动按需快照。此过程会创建一个新的备份并删除所有旧备份。

方法如下：

1. 从菜单中选择*复制计划*。
2. 选择复制计划，选择*故障转移映射*选项卡，然后选择*编辑*铅笔图标。
3. 选择“数据存储”箭头将其展开。
4. 请注意复制计划中的保留计数的值。完成这些步骤后，您需要恢复此原始值。
5. 将计数减少到 1。
6. 启动按需快照。为此，在复制计划页面上，选择该计划，选择操作图标，然后选择“立即创建快照”。
7. 快照作业成功完成后，将复制计划中的计数增加回您在第一步中记下的原始值。
8. 对所有现有的复制计划重复这些步骤。

2024年7月5日

此NetApp Disaster Recovery版本包括以下更新：

支持AFF A 系列

此版本支持NetApp AFF A 系列硬件平台。

支持本地到本地 VMware VMFS 数据存储区

此版本包括对安装在受本地存储保护的 VMware vSphere 虚拟机文件系统 (VMFS) 数据存储上的虚拟机的支持的技术预览。在此版本中，技术预览版支持将本地 VMware 工作负载灾难恢复到具有 VMFS 数据存储的本地 VMware 环境。



NetApp不会向您收取任何预览的工作负载容量的费用。

复制计划更新

您可以通过在“应用程序”页面上按数据存储过滤虚拟机以及在“资源映射”页面上选择更多目标详细信息来更轻松地添加复制计划。参考 [“创建复制计划”](#)。

编辑复制计划

在此版本中，故障转移映射页面得到了增强，更加清晰。

参考 [“管理计划”](#)。

编辑虚拟机

在此版本中，计划中编辑虚拟机的过程包含一些小的 UI 改进。

参考 ["管理虚拟机"](#)。

故障转移更新

在启动故障转移之前，您现在可以确定虚拟机的状态以及它们是已打开还是已关闭。故障转移过程现在使您能够立即拍摄快照或选择快照。

参考 ["将应用程序故障转移到远程站点"](#)。

故障转移测试计划

您现在可以编辑故障转移测试并为故障转移测试设置每日、每周和每月的计划。

参考 ["管理计划"](#)。

先决条件信息的更新

NetApp Disaster Recovery前提条件信息已更新。

参考 ["NetApp Disaster Recovery前提条件"](#)。

2024年5月15日

此NetApp Disaster Recovery版本包括以下更新：

将 **VMware** 工作负载从本地复制到本地

现在，此功能已作为一项通用功能发布。以前，它是一个功能有限的技术预览版。

许可更新

借助NetApp Disaster Recovery，您可以注册 90 天免费试用版、通过 Amazon Marketplace 购买即用即付 (PAYGO) 订阅或自带许可证 (BYOL)，后者是您从NetApp销售代表或NetApp支持站点 (NSS) 获得的NetApp许可证文件 (NLF)。

有关设置NetApp Disaster Recovery许可的详细信息，请参阅["设置许可"](#)。

["了解有关NetApp Disaster Recovery的更多信息"](#)。

2024年3月5日

这是NetApp Disaster Recovery的通用版本，其中包括以下更新。

许可更新

使用NetApp Disaster Recovery，您可以注册 90 天免费试用或自带许可证 (BYOL)，即您从NetApp销售代表处获得的NetApp许可证文件 (NLF)。您可以使用许可证序列号在NetApp Console订阅中激活 BYOL。NetApp

Disaster Recovery费用基于数据存储区的配置容量。

有关设置NetApp Disaster Recovery许可的详细信息，请参阅 ["设置许可"](#)。

有关管理*所有* NetApp Console数据服务的许可证的详细信息，请参阅： ["管理所有NetApp Console数据服务的许可证"](#)。

编辑时间表

在此版本中，您现在可以设置计划来测试合规性和故障转移测试，以确保它们在您需要时能够正常工作。

有关详细信息，请参阅 ["创建复制计划"](#)。

2024年2月1日

此NetApp Disaster Recovery预览版包括以下更新：

网络增强

在此版本中，您现在可以调整 VM CPU 和 RAM 值的大小。您现在还可以为 VM 选择网络 DHCP 或静态 IP 地址。

- DHCP：如果选择此选项，则需要为 VM 提供凭据。
- 静态IP：您可以选择与源VM相同或不同的信息。如果您选择与来源相同，则无需输入凭据。另一方面，如果您选择使用来自源的不同信息，您可以提供凭据、IP 地址、子网掩码、DNS 和网关信息。

有关详细信息，请参阅 ["创建复制计划"](#)。

自定义脚本

现在可以将其作为故障转移后流程包括在内。使用自定义脚本，您可以让NetApp Disaster Recovery在故障转移过程后运行您的脚本。例如，您可以使用自定义脚本在故障转移完成后恢复所有数据库事务。

有关详细信息，请参阅 ["故障转移到远程站点"](#)。

SnapMirror 关系

您现在可以在制定复制计划时创建SnapMirror关系。以前，您必须在NetApp Disaster Recovery之外创建关系。

有关详细信息，请参阅 ["创建复制计划"](#)。

一致性组

创建复制计划时，您可以包含来自不同卷和不同 SVM 的 VM。 NetApp Disaster Recovery通过包含所有卷来创建一致性组快照并更新所有辅助位置。

有关详细信息，请参阅 ["创建复制计划"](#)。

VM 开机延迟选项

创建复制计划时，您可以将虚拟机添加到资源组。使用资源组，您可以在每个虚拟机上设置延迟，以便它们按照

延迟的顺序启动。

有关详细信息，请参阅 ["创建复制计划"](#)。

应用程序一致的 **Snapshot** 副本

您可以指定创建应用程序一致的 Snapshot 副本。该服务将使应用程序静止，然后拍摄快照以获得应用程序的一致状态。

有关详细信息，请参阅 ["创建复制计划"](#)。

2024年1月11日

NetApp Disaster Recovery的预览版本包括以下更新：

更快速地查看仪表板

通过此版本，您可以更快地从仪表板访问其他页面上的信息。

["了解NetApp Disaster Recovery"](#)。

2023年10月20日

NetApp Disaster Recovery的预览版本包括以下更新。

保护本地基于 **NFS** 的 **VMware** 工作负载

现在，借助NetApp Disaster Recovery，您可以保护本地基于 NFS 的 VMware 工作负载，使其免受公共云之外的另一个本地基于 NFS 的 VMware 环境的灾难影响。NetApp Disaster Recovery负责协调灾难恢复计划的完成。



对于此预览版产品，NetApp保留在正式发布之前修改产品详细信息、内容和时间表的权利。

["了解有关NetApp Disaster Recovery的更多信息"](#)。

2023年9月27日

NetApp Disaster Recovery的预览版本包括以下更新：

仪表板更新

现在您可以在仪表盘上选择选项，从而更轻松地快速查看信息。此外，仪表板现在显示故障转移和迁移的状态。

参考 ["在仪表板上查看灾难恢复计划的运行状况"](#)。

复制计划更新

- **RPO**：您现在可以在复制计划的数据存储部分输入恢复点目标 (RPO) 和保留计数。这表示必须存在且不早于设定时间的数据量。例如，如果将其设置为 5 分钟，则在发生灾难时系统可能会丢失最多 5 分钟的数据，而不会影响关键业务需求。

参考 ["创建复制计划"](#)。

- 网络增强功能：当您在复制计划的虚拟机部分中映射源位置和目标位置之间的网络时，NetApp Disaster Recovery现在提供两个选项：DHCP 或静态 IP。以前，仅支持 DHCP。对于静态 IP，您可以配置子网、网关和 DNS 服务器。此外，您现在可以输入虚拟机的凭据。

参考 ["创建复制计划"](#)。

- 编辑时间表：您现在可以更新复制计划时间表。

参考 ["管理资源"](#)。

- * SnapMirror自动化*：在此版本中创建复制计划时，您可以在以下配置之一中定义源卷和目标卷之间的SnapMirror关系：
 - 1 至 1
 - 扇出架构中的一对多
 - 多对一作为一致性组
 - 多对多

参考 ["创建复制计划"](#)。

2023年8月1日

NetApp Disaster Recovery预览

NetApp Disaster Recovery预览版是一种基于云的灾难恢复服务，可自动执行灾难恢复工作流程。最初，借助NetApp Disaster Recovery预览版，您可以使用Amazon FSx for ONTAP将运行NetApp存储的本地基于 NFS 的 VMware 工作负载保护到 AWS 上的 VMware Cloud (VMC)。



对于此预览版产品，NetApp保留在正式发布之前修改产品详细信息、内容和时间表的权利。

["了解有关NetApp Disaster Recovery的更多信息"](#)。

此版本包括以下更新：

资源组更新启动顺序

创建灾难恢复或复制计划时，您可以将虚拟机添加到功能资源组中。资源组使您能够将一组依赖的虚拟机放入满足您要求的逻辑组中。例如，组可以包含恢复时可以执行的启动顺序。在此版本中，每个资源组可以包含一个或多个虚拟机。虚拟机将根据您在计划中包含的顺序启动。参考 ["选择要复制的应用程序并分配资源组"](#)。

复制验证

创建灾难恢复或复制计划后，在向导中确定重复，并启动到灾难恢复站点的复制，NetApp Disaster Recovery每 30 分钟验证一次复制是否确实按照计划进行。您可以在作业监视器页面中监视进度。参考 ["将应用程序复制到另一个站点"](#)。

复制计划显示恢复点目标（RPO）传输时间表

创建灾难恢复或复制计划时，您需要选择虚拟机。在此版本中，您现在可以查看与数据存储区或虚拟机关联的每个卷关联的SnapMirror。您还可以查看与SnapMirror计划关联的 RPO 传输计划。RPO 可帮助您确定备份计划是否足以在灾难后恢复。参考 ["创建复制计划"](#)。

作业监视器更新

作业监视器页面现在包含刷新选项，以便您可以获得最新的操作状态。参考 ["监控灾难恢复作业"](#)。

2023年5月18日

这是NetApp Disaster Recovery的初始版本。

基于云的灾难恢复服务

NetApp Disaster Recovery是一种基于云的灾难恢复服务，可自动执行灾难恢复工作流程。最初，借助NetApp Disaster Recovery预览版，您可以使用Amazon FSx for ONTAP将运行NetApp存储的本地基于 NFS 的 VMware 工作负载保护到 AWS 上的 VMware Cloud (VMC)。

["了解有关NetApp Disaster Recovery的更多信息"](#)。

NetApp Disaster Recovery的局限性

已知限制标识了此版本服务不支持或无法与其正确互操作的平台、设备或功能。

等待故障回复完成后再运行发现

故障转移完成后，请勿在源 vCenter 上手动启动发现。等待故障恢复完成，然后在源 vCenter 上启动发现。

NetApp Console可能无法发现Amazon FSx for NetApp ONTAP

有时，NetApp Console无法发现Amazon FSx for NetApp ONTAP集群。这可能是由于 FSx 凭证不正确。

解决方法：在NetApp Console中添加Amazon FSx for NetApp ONTAP集群，并定期刷新集群以显示任何更改。

如果需要从NetApp Disaster Recovery中删除ONTAP FSx 集群，请完成以下步骤：

1. 在NetApp Console代理中，使用云提供商的连接选项，连接到控制台代理运行的 Linux VM，使用 ``docker restart occm`` 命令。

参考 ["管理现有的控制台代理"](#)。

1. 在NetApp Console系统页面中，再次添加Amazon FSx for ONTAP系统并提供 FSx 凭证。

参考 ["创建Amazon FSx for NetApp ONTAP文件系统"](#)。

- 2.

从NetApp Disaster Recovery中，选择“站点”，在 vCenter 行上选择“操作”选项 ，然后从“操作”菜单中选择“刷新”以刷新NetApp Disaster Recovery中的 FSx 发现。

这将重新发现数据存储、其虚拟机及其目标关系。

Google Cloud NetApp Volumes的局限性

- 运行故障转移测试后，至少需要等待 52 小时才能删除克隆卷。您必须手动删除该卷。52 小时后，您可以再次测试故障转移。
- 如果挂载操作的任何部分失败，故障转移将不会成功，作业将超时。Google 最多需要三天时间来调查该问题，在此期间，vCenter 上所有与数据存储相关的操作都会被阻止。

开始使用

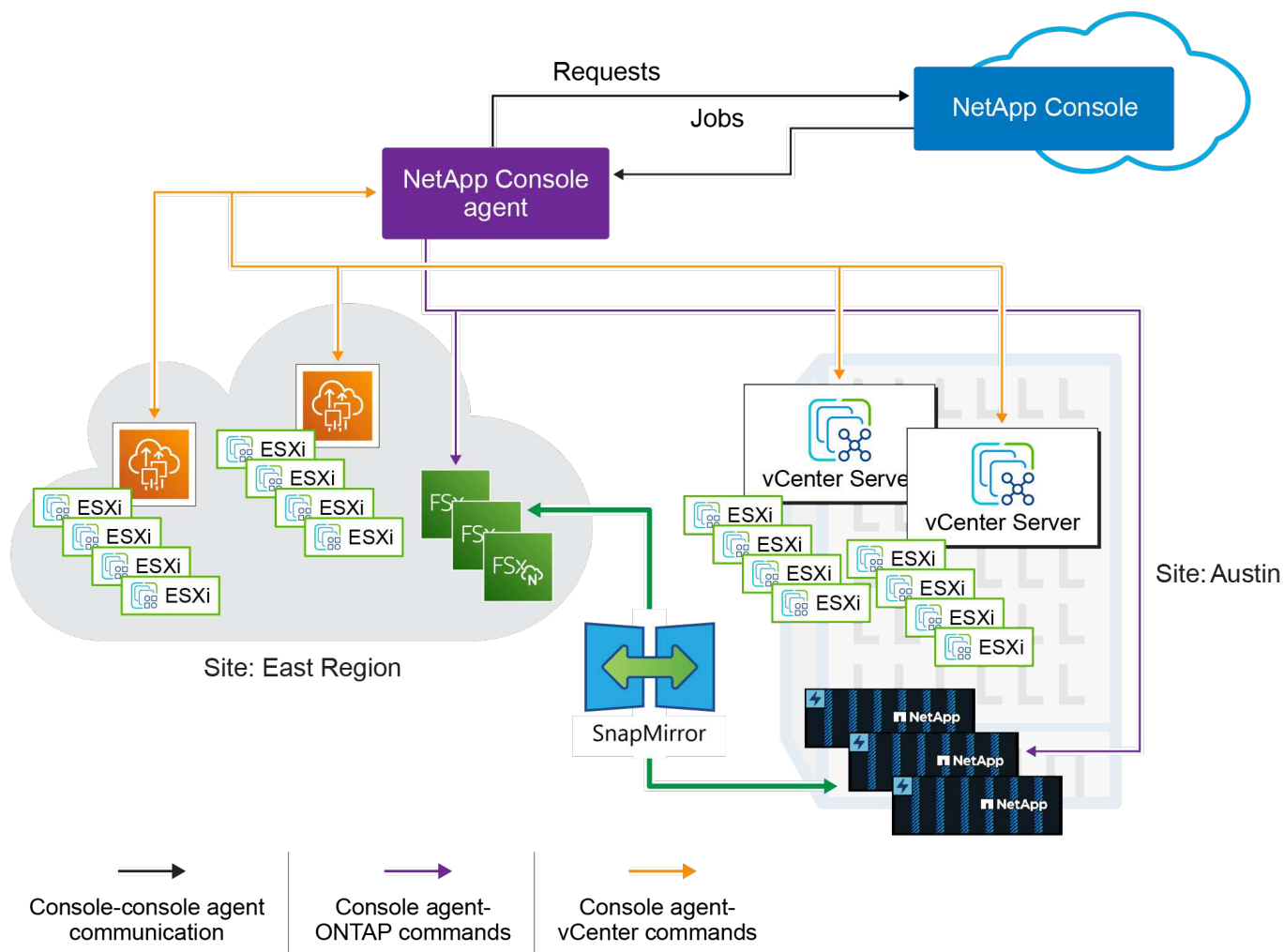
了解NetApp Disaster Recovery

云端灾难恢复是一种具有弹性且经济高效的方式，可以保护工作负载免受站点中断和数据损坏事件的影响。借助NetApp Disaster Recovery for VMware，您可以将运行ONTAP存储的本地 VMware VM 或数据存储库工作负载复制到使用NetApp云存储的公共云中的 VMware 软件定义数据中心，或复制到另一个以ONTAP存储为灾难恢复站点的本地 VMware 环境。您还可以使用灾难恢复将虚拟机工作负载从一个站点迁移到另一个站点。

NetApp Disaster Recovery是一种基于云的灾难恢复服务，可自动执行灾难恢复工作流程。借助NetApp Disaster Recovery，您可以将内部基于 NFS 的工作负载和 VMware vSphere 虚拟机文件系统 (VMFS) 数据存储（用于运行NetApp存储的 iSCSI 和 FC）保护到以下其中一项：

- Amazon Elastic VMware Service (EVS) 和Amazon FSx for NetApp ONTAP有关详细信息，请参阅["使用 Amazon Elastic VMware Service 和Amazon FSx for NetApp ONTAP实现NetApp Disaster Recovery"](#)。
- AWS 上的 VMware Cloud (VMC) 以及适用Amazon FSx for NetApp ONTAP
- 带有NetApp Cloud Volumes ONTAP (iSCSI) 的 Azure VMware 解决方案 (AVS)（私人预览版）
- Google Cloud VMware Engine (GCVE) 与Google Cloud NetApp Volumes
- 另一个具有ONTAP存储的本地 NFS 和/或基于 VMFS (iSCSI/FC) 的 VMware 环境

NetApp Disaster Recovery使用ONTAP SnapMirror技术与集成本机 VMware 业务流程来保护 VMware VM 及其相关的磁盘操作系统映像，同时保留ONTAP的所有存储效率优势。灾难恢复使用这些技术作为到灾难恢复站点的复制传输。这使得主站点和辅助站点能够实现业界最佳的存储效率（压缩和重复数据删除）。



NetApp Console

可通过NetApp Console访问NetApp Disaster Recovery。

NetApp Console提供企业级跨本地和云环境的NetApp存储和数据服务的集中管理。需要控制台才能访问和使用NetApp数据服务。作为管理界面，它使您能够从一个界面管理许多存储资源。控制台管理员可以控制企业内所有系统的存储和服务的访问。

您不需要许可证或订阅即可开始使用NetApp Console，并且只有当您需要在云中部署控制台代理以确保与存储系统或NetApp数据服务的连接时才需要付费。但是，一些可从控制台访问的NetApp数据服务是需要许可或基于订阅的。

详细了解 ["NetApp Console"](#)。

使用NetApp Disaster Recoveryfor VMware 的优势

NetApp Disaster Recovery具有以下优势：

- 通过多个时间点恢复操作简化 vCenter 发现和应用程序恢复的用户体验。
- 通过降低运营成本来降低总体拥有成本，并能够以最少的资源创建和调整灾难恢复计划。
- 通过虚拟故障转移测试持续做好灾难恢复准备，不会中断运营。您可以定期测试 DR 故障转移计划，而不会

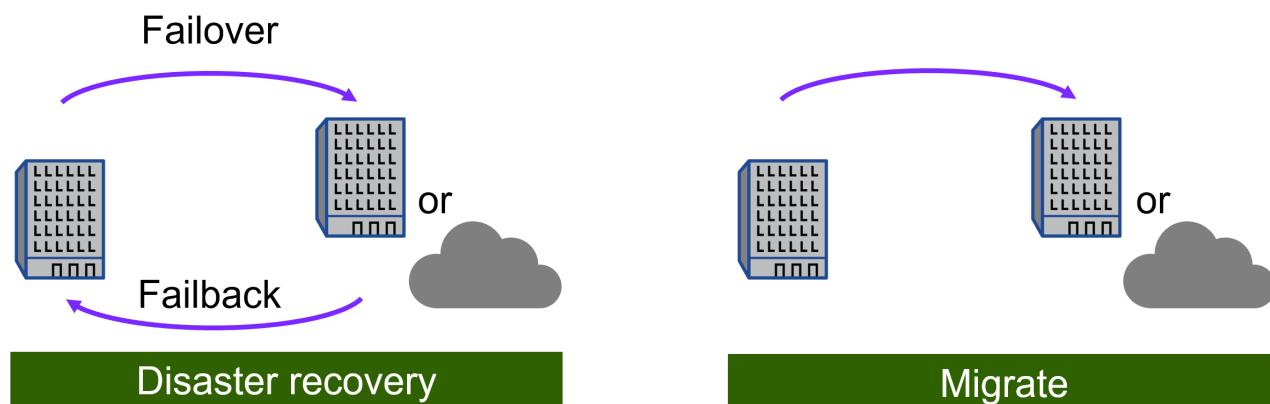
影响生产工作负载。

- 通过 IT 环境的动态变化和在灾难恢复计划中解决该问题的能力来更快地实现价值。
- 能够通过ONTAP和 VMware 的后端编排同时管理存储层和虚拟层，而无需部署和维护虚拟服务器设备 (VSA)。
- VMware 的 DR 解决方案可能会占用大量资源。许多 DR 解决方案使用 VSA 在 VMware 虚拟层复制虚拟机，这会消耗更多的计算资源并损失ONTAP宝贵的存储效率。由于灾难恢复使用ONTAP SnapMirror技术，它可以使用我们的永久增量复制模型将数据从生产数据存储复制到 DR 站点，并具有ONTAP的所有本机数据压缩和重复数据删除效率。

NetApp Disaster Recovery for VMware 的功能

NetApp Disaster Recovery让您充分利用多种NetApp技术来实现以下目标：

- 使用SnapMirror复制将本地生产站点上的 VMware 应用程序复制到云端或本地的灾难恢复远程站点。
- 将 VMware 工作负载从原始站点迁移到另一个站点。
- 进行故障转移测试。当您执行此操作时，该服务会创建临时虚拟机。灾难恢复从选定的快照创建一个新的FlexClone卷，并且由FlexClone卷支持的临时数据存储区映射到 ESXi 主机。此过程不会消耗本地ONTAP存储或 AWS 中 FSx for NetApp ONTAP存储的额外物理容量。原始源卷不会被修改，即使在灾难恢复期间，副本作业也可以继续。
- 如果发生灾难，请根据需要将主站点故障转移到灾难恢复站点，该站点可以是带有Amazon FSx for NetApp ONTAP 的AWS 上的 VMware Cloud，也可以是带有ONTAP的本地 VMware 环境。
- 灾难解决后，根据需要从灾难恢复站点故障回复到主站点。
- 将虚拟机或数据存储分组到逻辑资源组中，以实现高效管理。



vSphere 服务器的配置是在 vSphere Server 中的NetApp Disaster Recovery之外完成的。

成本

NetApp不会向您收取NetApp Disaster Recovery试用版的费用。

NetApp Disaster Recovery可以通过NetApp许可证或通过 Amazon Web Services 的年度订阅计划使用。



一些版本包括技术预览。NetApp不会向您收取任何预览的工作负载容量的费用。看["NetApp Disaster Recovery的新功能"](#)了解有关最新技术预览的信息。

许可

您可以使用以下许可证类型：

- 注册即可获得 30 天免费试用。
- 通过 Amazon Web Services (AWS) Marketplace 或 Microsoft Azure Marketplace 购买即用即付 (PAYGO) 订阅。此许可证使您能够购买固定保护容量许可证，而无需任何长期承诺。
- 自带许可证 (BYOL)，即您从NetApp销售代表处获得的NetApp许可证文件 (NLF)。您可以使用许可证序列号在NetApp Console中激活 BYOL。

所有NetApp数据服务的许可证均通过NetApp Console中的订阅进行管理。设置 BYOL 后，您可以在控制台中看到该服务的有效许可证。

该服务根据受保护的ONTAP卷上托管的数据量进行许可。该服务通过将受保护的虚拟机映射到其 vCenter 数据存储区来确定应考虑哪些卷用于许可目的。每个数据存储库都托管在ONTAP卷或 LUN 上。ONTAP报告的该卷或 LUN 的已用容量用于确定许可。

受保护的卷可以托管许多虚拟机。有些可能不属于NetApp Disaster Recovery资源组。无论如何，该卷或 LUN 上所有虚拟机消耗的存储都将用于满足许可证最大容量要求。



当至少有一个虚拟机具有复制计划时，NetApp Disaster Recovery费用基于源站点上数据存储区的已用容量。故障转移数据存储区的容量不包含在容量限额内。对于 BYOL，如果数据超出允许的容量，服务中的操作将受到限制，直到您获得额外的容量许可证或在NetApp Console中升级许可证。

有关设置NetApp Disaster Recovery许可的详细信息，请参阅["设置NetApp Disaster Recovery许可"](#)。

30天免费试用

您可以通过 30 天免费试用版来试用NetApp Disaster Recovery。

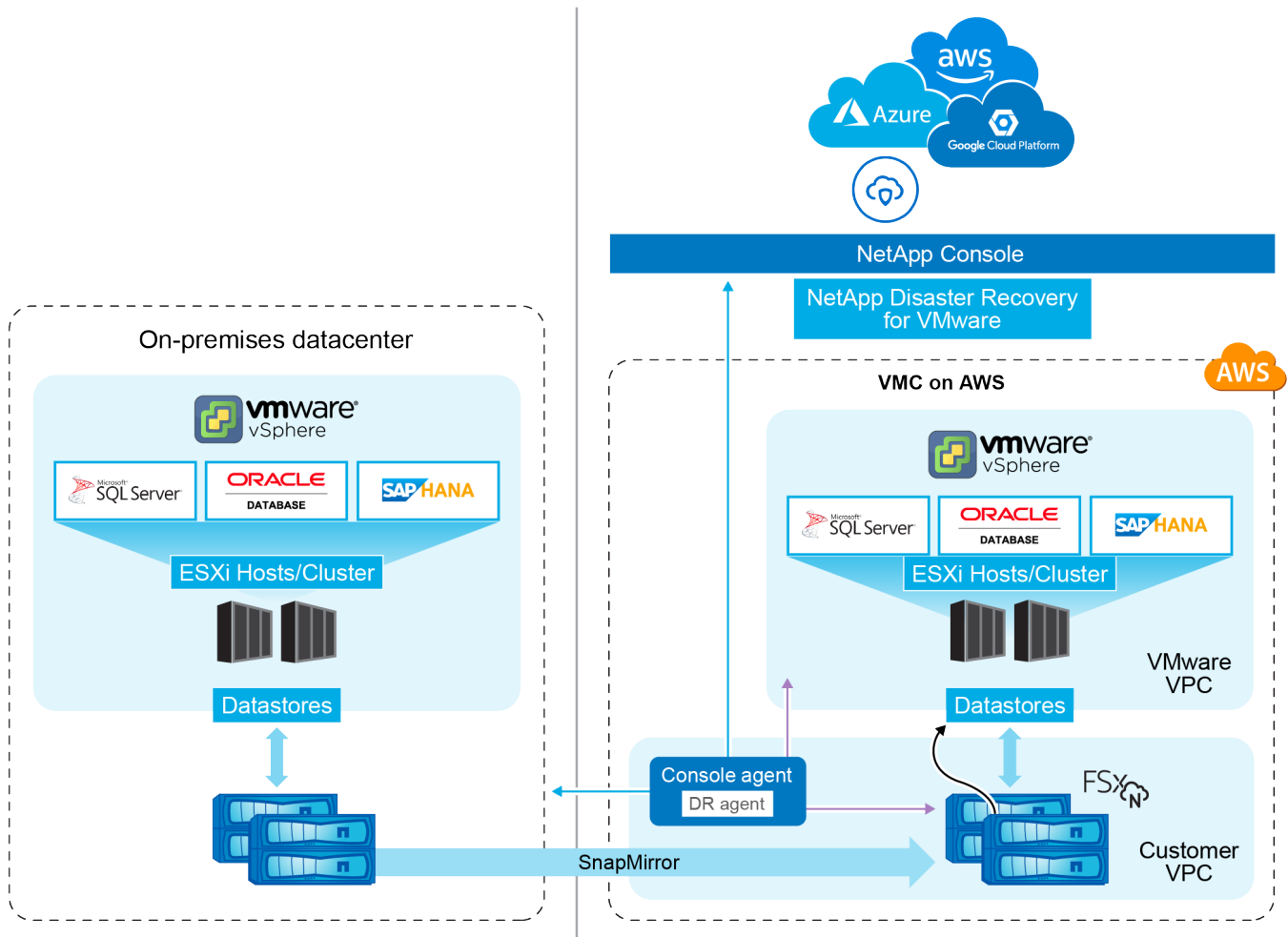
要在 30 天试用期结束后继续使用，您需要从云提供商处获得即用即付 (PAYGO) 订阅或从NetApp购买 BYOL 许可证。

您可以随时购买许可证，并且在 30 天试用期结束之前不会向您收费。

NetApp Disaster Recovery的工作原理

NetApp Disaster Recovery是托管在NetApp Console软件即服务 (SaaS) 环境中的服务。灾难恢复可以将本地站点复制到Amazon FSx for ONTAP或其他本地站点的工作负载恢复。此服务可自动执行从SnapMirror级别的恢复，包括将虚拟机注册到 VMware Cloud on AWS，以及直接在 VMware 网络虚拟化和安全平台 NSX-T 上进行网络映射。所有虚拟机云环境均包含此功能。

NetApp Disaster Recovery使用ONTAP SnapMirror技术，该技术可提供高效的复制并保留ONTAP永久增量快照的效率。SnapMirror复制可确保应用程序一致的快照副本始终保持同步，并且数据在故障转移后可立即使用。



当发生灾难时，此服务可帮助您通过中断SnapMirror关系并使目标站点处于活动状态来恢复其他本地 VMware 环境或 VMC 中的虚拟机。

- 该服务还允许您将虚拟机故障恢复到原始源位置。
- 您可以在不中断原始虚拟机的情况下测试灾难恢复故障转移过程。该测试通过创建卷的FlexClone将虚拟机恢复到隔离网络。
- 对于故障转移或测试故障转移过程，您可以选择最新（默认）或选定的快照来恢复虚拟机。

灾难恢复的组成部分

灾难恢复使用以下组件为 VMware 工作负载提供灾难恢复：

- *** NetApp Console***：用于管理灾难恢复计划的用户界面。您可以使用NetApp Console在本地和云环境中创建和管理复制计划、资源组和故障转移操作。
- **控制台代理**：在您的云托管网络或本地 VMware 环境中运行的轻量级软件组件。它与NetApp Console通信并管理本地环境和灾难恢复站点之间的数据复制。控制台代理安装在 VMware 环境中的虚拟机上。
- *** ONTAP存储集群***：ONTAP存储集群是托管 VMware 工作负载的主要存储系统。ONTAP存储集群为您的灾难恢复计划提供底层存储基础架构。灾难恢复使用ONTAP存储 API 来管理ONTAP存储集群（例如本地阵列）和基于云的解决方案（例如Amazon FSx for NetApp ONTAP）。
- **vCenter 服务器**：VMware vCenter 是您的 VMware 环境的管理服务器。它管理 ESXi 主机及其相关的数据存储。控制台代理与 VMware vCenter 通信，以管理本地环境和灾难恢复站点之间的数据复制。这包括

将ONTAP LUN 和卷注册为数据存储、重新配置虚拟机以及启动和停止虚拟机。

灾难恢复保护工作流程

当复制计划分配给资源组时，灾难恢复会对资源组和计划中的所有组件执行发现检查，以确保该计划可以激活。

如果此检查成功，灾难恢复将执行以下初始化步骤：

1. 对于目标资源组中的每个虚拟机，确定托管 VMware 数据存储。
2. 对于找到的每个 VMware 数据存储库，识别托管ONTAP FlexVol volume或 LUN。
3. 对于找到的每个ONTAP卷和 LUN，确定源卷和目标站点中的目标卷之间是否存在现有的SnapMirror关系。
 - a. 如果没有预先存在的SnapMirror关系，请创建任何新的目标卷，并在每个未受保护的源卷之间创建新的SnapMirror关系。
 - b. 如果存在预先存在的SnapMirror关系，请使用该关系执行所有复制操作。

灾难恢复创建并初始化所有关系后，在每次计划备份时，该服务都会执行以下数据保护步骤：

1. 对于每个标记为“应用程序一致”的虚拟机，使用 VMtools 将支持的应用程序置于备份状态。
2. 为托管受保护的 VMware 数据存储的所有ONTAP卷创建新快照。
3. 执行SnapMirror更新操作以将这些快照复制到目标ONTAP集群。
4. 确定保留的快照数量是否超过了复制计划中定义的最大快照保留量，并从源卷和目标卷中删除任何多余的快照。

支持的保护目标和数据存储类型

支持的数据存储类型 NetApp Disaster Recovery支持以下数据存储类型：

- 托管在ONTAP集群上的ONTAP FlexVol卷上的 NFS 数据存储库。
- 使用 iSCSI 或 FC 协议的 VMware vSphere 虚拟机文件系统 (VMFS) 数据存储

支持的保护目标

- AWS 上的 VMware Cloud (VMC) 以及适用Amazon FSx for NetApp ONTAP
- 另一个本地、基于 NFS 的 VMware 环境，具有ONTAP存储或本地 FC/iSCSI VMSF
- Amazon Elastic VMware 服务
- 带有NetApp Cloud Volumes ONTAP (iSCSI) 的 Azure VMware 解决方案 (AVS) (私人预览版)
- Google Cloud VMware Engine (GCVE) 与Google Cloud NetApp Volumes

可能对您有帮助的NetApp Disaster Recovery术语

了解一些与灾难恢复相关的术语可能会对您有所帮助。

- 数据存储：VMware vCenter 数据容器，它使用文件系统来保存 VMDK 文件。典型的数据存储类型是 NFS、VMFS、vSAN 或 vVol。灾难恢复支持 NFS 和 VMFS 数据存储。每个 VMware 数据存储库都托管在单个ONTAP卷或 LUN 上。灾难恢复支持位于ONTAP集群上的FlexVol卷上托管的 NFS 和 VMFS 数据存储库。

- 复制计划：一组关于备份频率以及如何处理故障转移事件的规则。计划被分配给一个或多个资源组。
- 恢复点目标 (RPO)：发生灾难时可接受的最大数据丢失量。RPO 在复制计划的数据复制频率或复制计划中定义。
- 恢复时间目标 (RTO)：从灾难中恢复可接受的最长时间。RTO 在复制计划中定义，是故障转移到 DR 站点并重新启动所有虚拟机所需的时间。
- 资源组：一个逻辑容器，使您能够将多个虚拟机作为一个单元进行管理。一个虚拟机一次只能属于一个资源组。您可以为想要保护的每个应用程序或工作负载创建一个资源组。
- 站点：通常与托管一个或多个 vCenter 集群和ONTAP存储的物理数据中心或云位置相关联的逻辑容器。

NetApp Disaster Recovery前提条件

在使用NetApp Disaster Recovery之前，请确保您的环境满足ONTAP存储、VMware vCenter 集群和NetApp Console的要求。

软件版本

组件	最低版本
Amazon FSx for NetApp ONTAP	最新可用版本
使用Google Cloud NetApp Volumes 的Google Cloud VMware Engine	最新可用版本
ONTAP 软件	ONTAP 9.10.0 或更高版本
适用于 AWS 的 VMware Cloud	最新可用版本
VMware 本地 vCenter	7.0u3 或更高版本

Google Cloud 的先决条件和注意事项

使用 Google Google Cloud NetApp Volumes VMware Engine 上进行灾难恢复时，请确保配置正确的权限并遵守以下注意事项。

- 请联系 Google SRE 团队，将以下服务添加到允许列表中：
 - 同步 API，用于将快照从本地存储传输到Google Cloud NetApp Volumes。
 - Google 与 VMware 引擎合作的项目，用于创建、挂载和卸载数据存储。
- 你必须[提交请求，将您的卷添加到混合复制允许列表中](#)。
- 注意["Google Cloud NetApp Volumes配额和限制"](#)。
- 一个复制计划只能添加一个卷或数据存储。
- 复习["限制"](#)。

故障转移注意事项

- 仅使用最新快照支持故障转移。如果需要，可以在故障转移期间创建新快照（即必须禁用选择性快照选项）。
- 故障转移后无法创建新的快照。
- 故障转移后无法保留和协调快照。

故障恢复考虑因素

- 只有在启用选择性快照选项的情况下才能进行故障恢复。您无法通过创建新快照来执行故障恢复。
- 如果删除本地存储和Google Cloud NetApp Volumes存储集群之间的集群对等连接，则必须手动从本地集群中清除集群和存储 VM 对等连接条目。有关详细信息，请参阅 ["删除虚拟服务器对等关系"](#)。

Google Cloud 权限

应为 Google Cloud 中的服务主体分配以下角色或等效权限：

- ["计算管理员角色"](#)
- ["NetApp Console的 Google Cloud 权限"](#)
- ["Google Cloud NetApp Volumes管理员"](#)
- ["VMware Engine 服务管理员"](#)

NetApp Console权限

NetApp Console用户必须具有以下角色：

- ["Google Cloud NetApp Volumes管理员"](#)
- ["SnapCenter管理员"](#)
- ["灾难恢复故障转移管理员"](#)

ONTAP存储前提条件

这些先决条件适用于ONTAP或 Amazon FSx for NetApp ONTAP实例。

- 源集群和目标集群必须具有对等关系。
- 承载灾难恢复卷的 SVM 必须存在于目标集群上。
- 源 SVM 和目标 SVM 必须具有对等关系。
- 如果使用Amazon FSx for NetApp ONTAP进行部署，则适用以下先决条件：
 - 您的 VPC 中必须存在用于托管 VMware DR 数据存储区的Amazon FSx for NetApp ONTAP实例。首先，请参阅["Amazon FSx for ONTAP文档"](#)。

VMware vCenter 集群先决条件

这些先决条件适用于本地 vCenter 集群和 VMware Cloud for AWS 软件定义数据中心 (SDDC)。

- 审查["vCenter 权限"](#)NetApp Disaster Recovery所必需的。
- 您希望NetApp Disaster Recovery管理的所有 VMware 集群都使用ONTAP卷来托管您想要保护的任何虚拟

机。

- NetApp Disaster Recovery要管理的所有 VMware 数据存储库都必须使用以下协议之一：
 - NFS
 - 使用 iSCSI 或 FC 协议的 VMFS
- VMware vSphere 版本 7.0 Update 3 (7.0v3) 或更高版本
- 如果您使用的是 VMware Cloud SDDC，则这些先决条件适用。
 - 在 VMware Cloud Console 中，使用管理员和 NSX Cloud 管理员的服务角色。还可以使用组织所有者作为组织角色。参考 ["将 VMware Cloud Foundations 与 AWS FSx for NetApp ONTAP文档结合使用"](#)。
 - 将 VMware Cloud SDDC 与Amazon FSx for NetApp ONTAP实例链接。参考 ["VMware Cloud on AWS 与Amazon FSx for NetApp ONTAP集成部署信息"](#)。

NetApp Console前提条件

开始使用NetApp Console

如果你还没有这样做的话，["注册NetApp Console并创建组织"](#)。

收集ONTAP和 VMware 的凭证

- 必须将Amazon FSx for ONTAP和 AWS 凭证添加到管理NetApp Disaster Recovery的NetApp Console项目中的系统中。
- NetApp Disaster Recovery需要 vCenter 凭据。在NetApp Disaster Recovery中添加站点时，您需要输入 vCenter 凭据。

有关所需 vCenter 权限的列表，请参阅["NetApp Disaster Recovery所需的 vCenter 权限"](#)。有关如何添加站点的说明，请参阅["添加站点"](#)。

创建NetApp Console代理

控制台代理是一个软件组件，它使控制台能够与您的ONTAP存储和 VMware vCenter 集群进行通信。它是灾难恢复正常运行所必需的。代理程序驻留在您的私有网络（本地数据中心或云 VPC）中，并与您的ONTAP存储实例以及任何其他服务器和应用程序组件进行通信。对于灾难恢复，这是对您管理的 vCenter 集群的访问。

必须在NetApp Console中设置控制台代理。当您使用该代理时，它将包含适合灾难恢复服务的功能。

- NetApp Disaster Recovery仅适用于标准模式代理部署。看 ["在标准模式下开始使用NetApp Console"](#)。
- 确保源和目标 vCenter 集群都使用相同的 Console 代理。
- 所需的控制台代理类型：
 - 本地到本地灾难恢复：在灾难恢复站点中安装本地 Console 代理。使用此方法，主站点的故障不会阻止服务在 DR 站点重新启动虚拟资源。请参阅 ["在本地安装并设置控制台代理"](#)。

灾难恢复还支持使用多个本地配置的控制台代理。在这种情况下，控制台代理会将操作定向到 vCenter 和ONTAP阵列集群，源和目标各自拥有自己的控制台代理。建议使用多个控制台代理，以减少延迟并缩短控制台代理或站点发生故障时的恢复时间。

- 本地到 **AWS**：在您的 AWS VPC 中安装 AWS 的控制台代理。参考 ["AWS 中的控制台代理安装选项"](#)。



对于本地到本地，请使用本地控制台代理。对于本地到 AWS，使用 AWS 控制台代理，它可以访问源本地 vCenter 和目标本地 vCenter。

- 已安装的控制台代理必须能够访问灾难恢复将要管理的任何 VMware vCenter 集群实例和由这些 vCenter 集群管理的 ESXi 主机。
- 所有由 NetApp Disaster Recovery 管理的 ONTAP 阵列都必须添加到 NetApp Console 项目内用于管理 NetApp Disaster Recovery 的任何系统中。

看 ["发现本地 ONTAP 集群"](#)。

- 有关为 NetApp Disaster Recovery 设置智能代理的信息，请参阅["为 NetApp Disaster Recovery 设置基础架构"](#)。

工作负载先决条件

为了确保应用程序一致性流程成功，请满足以下先决条件：

- 确保 VMware 工具（或 Open VM 工具）正在要保护的虚拟机上运行。
- 对于运行 Microsoft SQL Server、Oracle 数据库或两者的 Windows 虚拟机，必须启用数据库的 VSS 写入器。
- 在 Linux 操作系统上运行的 Oracle 数据库必须为 Oracle 数据库 SYSDBA 角色启用操作系统用户身份验证。

更多信息

- [所需 vCenter 权限](#)
- [Amazon EVS 与 NetApp Disaster Recovery 的先决条件](#)

NetApp Disaster Recovery 快速入门

以下是开始使用 NetApp Disaster Recovery 所需步骤的概述。每个步骤中的链接都会将您带到提供更多详细信息的页面。

1

审查先决条件

["确保您的系统满足这些要求"](#)。

2

设置 NetApp Disaster Recovery

- ["设置服务的基础结构"](#)。
- ["设置许可"](#)。

3

下一步是什么？

设置服务后，您可以执行以下操作。

- "将您的 vCenter 站点添加到NetApp Disaster Recovery"。
- "创建第一个资源组"。
- "创建您的第一个复制计划"。
- "将应用程序复制到另一个站点"。
- "将应用程序故障转移到远程站点"。
- "将应用程序故障恢复到原始源站点"。
- "管理站点、资源组和复制计划"。
- "监控灾难恢复操作"。

为NetApp Disaster Recovery设置基础架构

要使用NetApp Disaster Recovery，请执行几个步骤在 Amazon Web Services (AWS) 和NetApp Console中对其进行设置。



审查["前提条件"](#)以确保您的系统已准备就绪。

您可以在以下基础架构中使用NetApp Disaster Recovery：

- 混合云 DR 将本地 VMware 和ONTAP数据中心复制到基于 VMware Cloud on AWS 和Amazon FSx for NetApp ONTAP 的AWS DR 基础架构。
- 私有云 DR 将本地 VMware 和ONTAP vCenter 复制到另一个本地 VMware 和ONTAP vCenter。

采用 VMware Cloud 和Amazon FSx for NetApp ONTAP 的混合云

此方法包括使用 NFS 协议托管在ONTAP FlexVol卷上的数据存储在本地生产 vCenter 基础架构。DR 站点由一个或多个 VMware Cloud SDDC 实例组成，这些实例使用由一个或多个 FSx for ONTAP实例通过 NFS 协议提供的FlexVol卷上托管的数据存储。

生产站点和 DR 站点通过与 AWS 兼容的安全连接进行连接。常见的连接类型是安全 VPN（私有或 AWS 提供）、AWS Direct Connect 或其他批准的互连方法。

对于涉及 AWS 云基础设施的灾难恢复，您必须使用 AWS 的控制台代理。该代理应安装在与 FSx for ONTAP实例相同的 VPC 中。如果在其他 VPC 中部署了额外的 FSx for ONTAP实例，则托管代理的 VPC 必须能够访问其他 VPC。

AWS 可用区

AWS 支持在给定区域内的一个或多个可用区 (AZ) 中部署解决方案。灾难恢复使用两种 AWS 托管服务：
： VMware Cloud for AWS 和 AWS FSx for NetApp ONTAP。

- **VMware Cloud for AWS：**支持在单可用区或双可用区延伸集群 SDDC 环境中部署。灾难恢复仅支持针对 Amazon VMware Cloud for AWS 的单可用区 SDDC 部署。
- **AWS FSx for NetApp ONTAP：**当以双可用区配置部署时，每个卷都由单个 FSx 系统拥有。每个卷由单个 FSx 系统拥有。该卷的数据被镜像到第二个 FSx 系统。FSx for ONTAP系统可以部署在单可用区或双可用区部署中。灾难恢复支持单可用区和多可用区 FSx for ONTAP部署。

最佳实践：对于 AWS DR 站点配置，NetApp 建议对 VMware Cloud 和 AWS FSx for ONTAP 实例使用单可用区部署。由于 AWS 用于 DR，因此引入多个 AZ 没有任何优势。多可用区可能会增加成本和复杂性。

本地到 AWS

AWS 提供了以下方法将私有数据中心连接到 AWS 云。每种解决方案都有其优点和成本考虑。

- **AWS Direct Connect**：这是位于与您的私有数据中心相同的地理区域并由 AWS 合作伙伴提供的 AWS 云互连。此解决方案在您的本地数据中心和 AWS 云之间提供安全的私有连接，而无需公共互联网连接。这是 AWS 提供的最直接、最有效的连接方式。
- **AWS 互联网网关**：这提供了 AWS 云资源和外部计算资源之间的公共连接。这种类型的连接通常用于向外部客户提供服务，例如不需要安全性的 HTTP/HTTPS 服务。没有服务质量控制、安全性或连接性保证。因此，不建议使用此连接方法将生产数据中心连接到云。
- **AWS Site-Site VPN**：此虚拟专用网络连接可用于与公共互联网服务提供商一起提供安全的访问连接。VPN 对往返于 AWS 云的所有数据进行加密和解密。VPN 可以基于软件，也可以基于硬件。对于企业应用程序，公共互联网服务提供商 (ISP) 应提供服务质量保证，以确保为 DR 复制提供足够的带宽和延迟。

最佳实践：对于 AWS DR 站点配置，NetApp 建议使用 AWS Direct Connect。该解决方案为企业应用程序提供最高的性能和安全性。如果不可用，则应使用高性能公共 ISP 连接以及 VPN。确保 ISP 提供商业 QoS 服务级别以确保足够的网络性能。

VPC 到 VPC 互连

AWS 提供以下类型的 VPC 到 VPC 互连。每种解决方案都有其优点和成本考虑。

- **VPC Peering**：这是两个 VPC 之间的私有连接。这是 AWS 提供的最直接、最有效的连接方式。VPC 对等连接可用于连接相同或不同 AWS 区域中的 VPC。
- **AWS 互联网网关**：这通常用于提供 AWS VPC 资源与非 AWS 资源和端点之间的连接。所有流量都遵循“发夹”路径，其中发往另一个 VPC 的 VPC 流量通过互联网网关退出 AWS 基础设施，并通过相同或不同的网关返回 AWS 基础设施。这不是适合企业 VMware 解决方案的 VPC 连接类型。
- **AWS Transit Gateway**：这是一种基于集中式路由器的连接类型，使每个 VPC 能够连接到单个中央网关，该网关充当所有 VPC 到 VPC 流量的中央枢纽。这也可以连接到您的 VPN 解决方案，以使本地数据中心资源能够访问 AWS VPC 托管的资源。这种类型的连接通常需要额外的成本来实现。

最佳实践：对于涉及 VMware Cloud 和单个 FSx for ONTAP VPC 的 DR 解决方案，NetApp 建议您使用 VPC 对等连接。如果部署了多个 FSx for ONTAP VPC，我们建议使用 AWS Transit Gateway 来减少多个 VPC 对等连接的管理开销。

使用 AWS 为本地到云端的保护做好准备

要使用 AWS 设置 NetApp Disaster Recovery 以实现本地到云的保护，您需要设置以下内容：

- 为 NetApp ONTAP 设置 AWS FSx
- 设置 VMware Cloud on AWS SDDC

为 NetApp ONTAP 设置 AWS FSx

- 创建 Amazon FSx for NetApp ONTAP 文件系统。
 - 为 ONTAP 配置 FSx。Amazon FSx for NetApp ONTAP 是一项完全托管的服务，它基于 NetApp ONTAP 文件系统构建，提供高度可靠、可扩展、高性能且功能丰富的文件存储。

- 按照以下步骤操作 ["技术报告 4938：使用 VMware Cloud on AWS 将 Amazon FSx ONTAP 挂载为 NFS 数据存储"](#)和 ["Amazon FSx for NetApp ONTAP 快速入门"](#)为 ONTAP 配置和部署 FSx。

- 将 Amazon FSx for ONTAP 添加到系统，并为 FSx for ONTAP 添加 AWS 凭证。
- 在 AWS FSx for ONTAP 实例中创建或验证您的目标 ONTAP SVM。
- 在 NetApp Console 中配置源本地 ONTAP 集群和 FSx for ONTAP 实例之间的复制。

参考 ["如何设置 FSx for ONTAP 系统"](#)了解详细步骤。

设置 VMware Cloud on AWS SDDC

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

要在 AWS 上配置 VMware Cloud 环境，请按照 ["在 AWS 上部署和配置虚拟化环境"](#)。指示灯集群还可用于灾难恢复目的。

私有云

您可以使用 NetApp Disaster Recovery 来保护托管在一个或多个 vCenter 集群上的 VMware VM，方法是将 VM 数据存储复制到同一私有数据中心或远程私有或共置数据中心的另一个 vCenter 集群。

对于本地到本地的情况，请在其中一个物理站点安装控制台代理。

灾难恢复支持使用以太网和 TCP/IP 进行站点到站点的复制。确保有足够的带宽来支持生产站点虚拟机上的数据变化率，以便所有更改都可以在恢复点目标 (RPO) 时间范围内复制到 DR 站点。

为本地到本地保护做好准备

在设置 NetApp Disaster Recovery 以进行本地到本地保护之前，请确保满足以下要求：

- ONTAP 存储
 - 确保您拥有 ONTAP 凭据。
 - 创建或验证您的灾难恢复站点。
 - 创建或验证您的目标 ONTAP SVM。
 - 确保您的源 ONTAP SVM 和目标 ONTAP SVM 对等。
- vCenter 集群
 - 确保要保护的虚拟机托管在 NFS 数据存储区（使用 ONTAP NFS 卷）或 VMFS 数据存储区（使用 NetApp iSCSI LUN）上。
 - 审查 ["vCenter 权限"](#) NetApp Disaster Recovery 所必需的。
 - 创建灾难恢复用户帐户（不是默认的 vCenter 管理员帐户）并将 vCenter 权限分配给该帐户。

智能代理支持

NetApp Console 代理支持智能代理。智能代理是一种将您的内部环境连接到 NetApp Console 的轻量级、安全且

高效的方法。它在您的系统和控制台服务之间提供安全连接，而无需 VPN 或直接互联网访问。这种优化的代理实现可卸载本地网络内的 API 流量。

配置代理后，NetApp Disaster Recovery会尝试直接与 VMware 或ONTAP通信，如果直接通信失败，则使用配置的代理。

NetApp Disaster Recovery代理实施需要使用 HTTPS 协议在控制台代理与任何 vCenter Server 和ONTAP阵列之间进行端口 443 通信。控制台代理内的NetApp Disaster Recovery代理在执行任何操作时直接与 VMware vSphere、VC 或ONTAP通信。

有关NetApp Console中常规代理设置的更多信息，请参阅 ["配置控制台代理以使用代理服务器"](#)。

访问NetApp Disaster Recovery

您可以使用NetApp Console登录NetApp Disaster Recovery服务。

要登录，您可以使用您的NetApp支持站点凭证，也可以使用您的电子邮件和密码注册NetApp云登录。 ["了解有关登录的更多信息"](#)。

特定任务需要特定的用户角色。 ["了解NetApp Disaster Recovery中的用户角色和权限"](#)

。 <https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html>["了解所有服务的NetApp Console访问角色"^]。

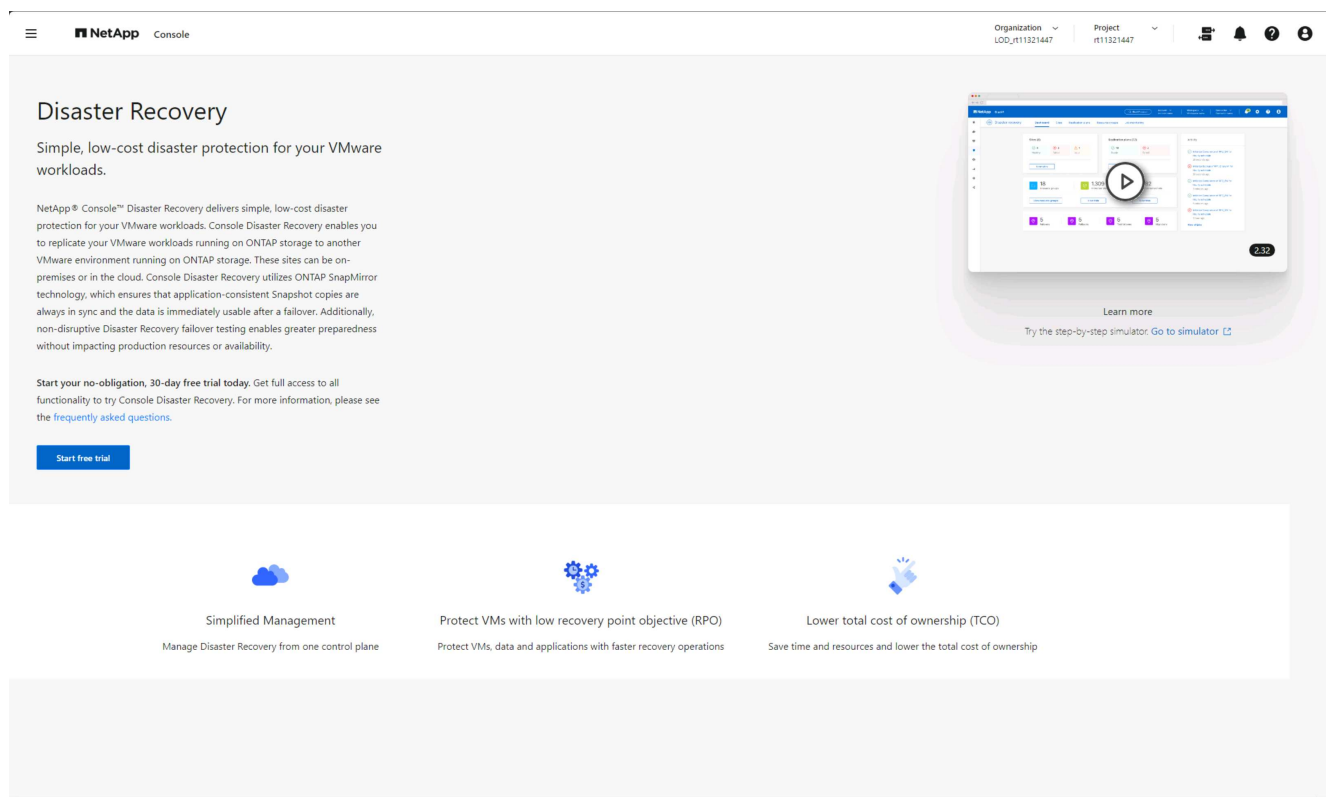
步骤

1. 打开 Web 浏览器并转到 ["NetApp Console"](#)。

出现NetApp Console登录页面。

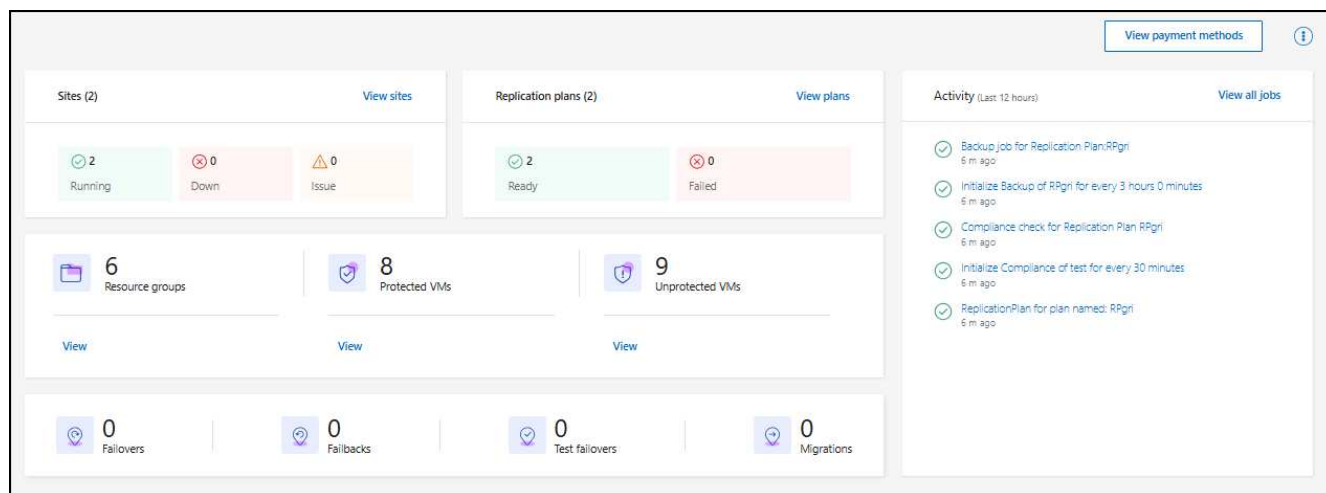
2. 登录到NetApp Console。
3. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。

如果这是您第一次登录此服务，则会出现登录页面，您可以注册免费试用。



否则，将出现NetApp Disaster Recovery仪表板。

- 如果您尚未添加NetApp Console代理，则需要添加一个。要添加代理，请参阅 ["了解控制台代理"](#)。
- 如果您是具有现有代理的NetApp Console用户，当您选择“灾难恢复”时，会出现一条有关注册的消息。
- 如果您已经在使用该服务，当您选择“灾难恢复”时，就会出现仪表板。



设置NetApp Disaster Recovery许可

使用NetApp Disaster Recovery，您可以使用不同的许可计划，包括免费试用、按需付费订阅或自带许可证。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员或灾难恢复应用程序管理员角

色。

"了解NetApp Disaster Recovery中的用户角色和权限"。https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html["了解所有服务的访问角色"^]。

许可选项 您可以使用以下许可选项：

- 注册即可获得 30 天免费试用。
- 购买 Amazon Web Services (AWS) Marketplace 或 Microsoft Azure Marketplace 的即用即付 (PAYGO) 订阅。
- 自带许可证 (BYOL)，即您从NetApp销售代表处获得的NetApp许可证文件 (NLF)。您可以使用许可证序列号在NetApp Console中激活 BYOL。



当至少有一个虚拟机具有复制计划时，NetApp Disaster Recovery费用基于源站点上数据存储区的已用容量。故障转移数据存储区的容量不包含在容量限额内。对于 BYOL，如果数据超出允许的容量，服务中的操作将受到限制，直到您获得额外的容量许可证或在NetApp Console中升级许可证。

"了解有关订阅的更多信息"。

免费试用结束或许可证到期后，您仍然可以在服务中执行以下操作：

- 查看任何资源，例如工作负载或复制计划。
- 删除任何资源，例如工作负载或复制计划。
- 运行在试用期间或许可证下创建的所有计划操作。

使用 30 天免费试用版进行尝试

您可以通过 30 天免费试用版来试用NetApp Disaster Recovery。



试用期间不实施任何容量限制。

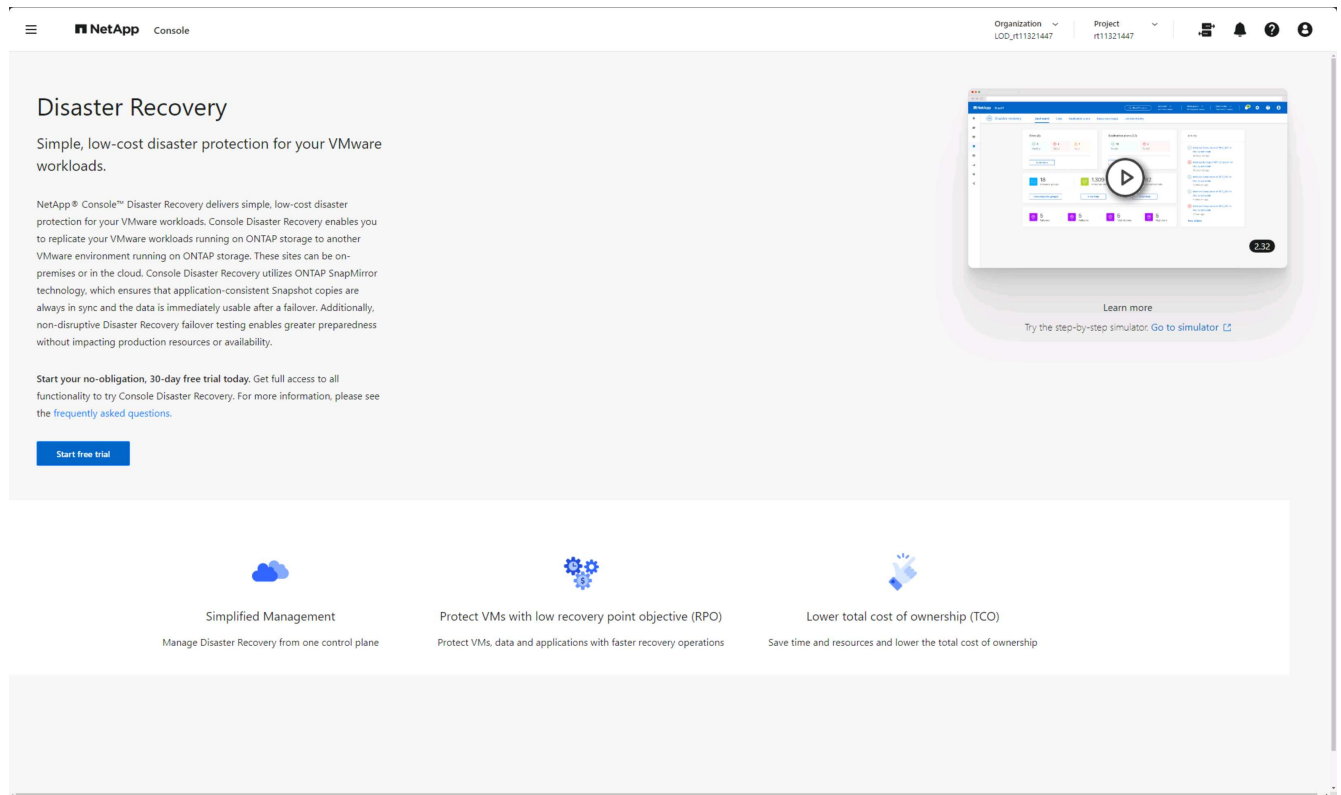
试用期结束后，若要继续，您需要购买 BYOL 许可证或 PAYGO AWS 订阅。您可以随时获得许可证，并且在试用期结束之前不会向您收费。

在试用期间，您可以使用全部功能。

步骤

1. 登录 "NetApp Console"。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。

如果这是您第一次登录此服务，则会出现登录页面。



3. 如果您尚未为其他服务添加控制台代理，请添加一个。

要添加控制台代理，请参阅 ["了解控制台代理"](#)。

4. 设置代理后，在NetApp Disaster Recovery登录页面中，添加代理的按钮将更改为开始免费试用的按钮。选择*开始免费试用*。

5. 首先添加 vCenter。

有关详细信息，请参阅["添加 vCenter 站点"](#)。

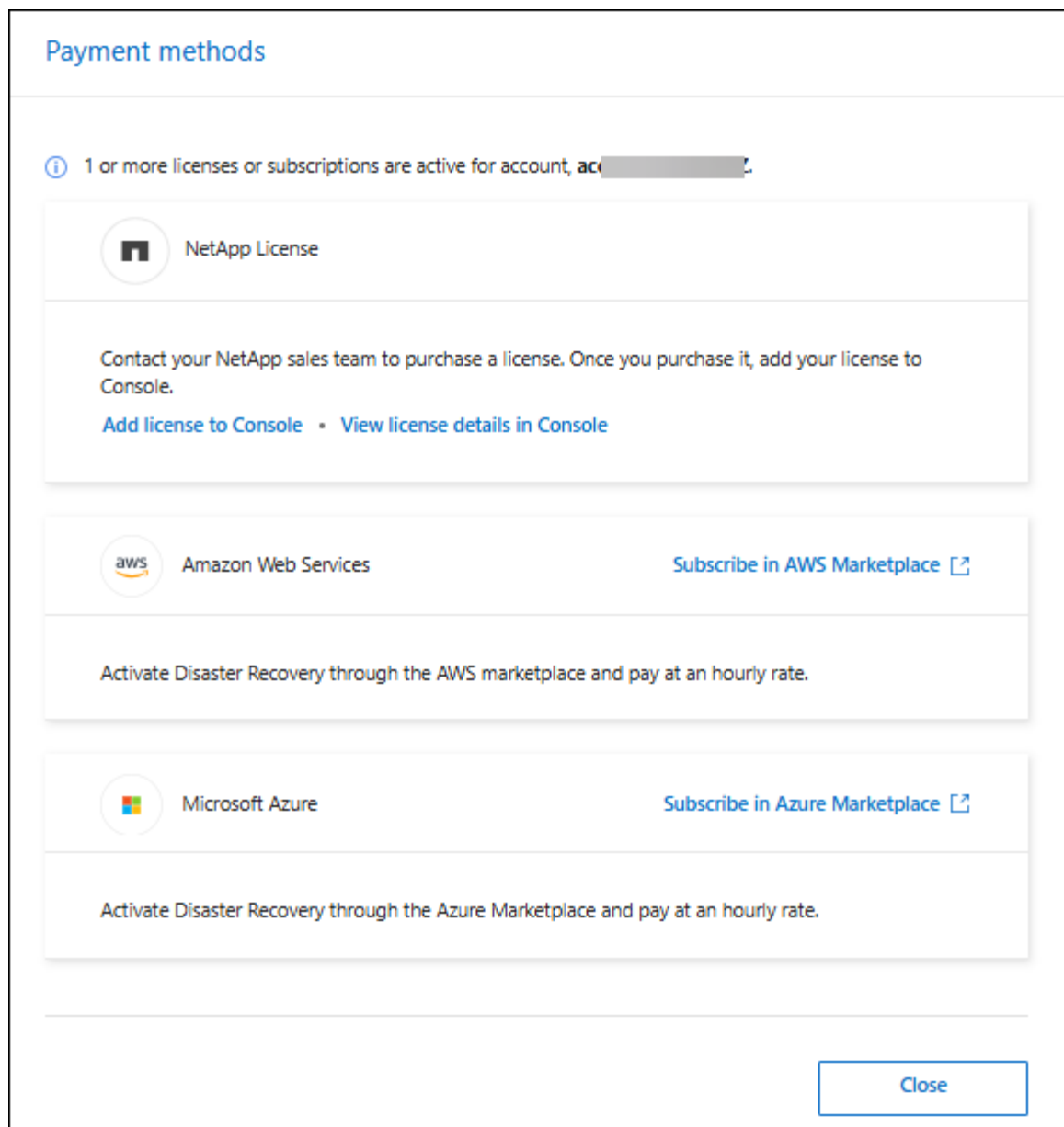
试用期结束后，通过其中一个市场进行订阅

免费试用结束后，您可以从NetApp购买许可证，也可以通过 AWS Marketplace 或 Microsoft Azure Marketplace 订阅。此过程提供了如何在其中一个市场中直接订阅的高级概述。

步骤

1. 在NetApp Disaster Recovery中，您会看到一条消息，提示免费试用即将到期。在消息中，选择*订阅或购买许可证*。

或者，从中选择*查看付款方式*。



2. 选择*在 AWS Marketplace 中订阅*或*在 Azure Marketplace 中订阅*。
3. 使用 AWS Marketplace 或 Microsoft Azure Marketplace 订阅 * NetApp Disaster Recovery*。
4. 当您返回到NetApp Disaster Recovery时，会出现一条消息表明您已订阅。

您可以在NetApp Console订阅页面查看订阅详细信息。["详细了解如何使用NetApp Console管理订阅"](#)。

试用结束后，通过NetApp购买 BYOL 许可证

试用结束后，您可以通过NetApp销售代表购买许可证。

如果您自带许可证 (BYOL)，则设置包括购买许可证、获取NetApp许可证文件 (NLF) 以及将许可证添加到NetApp Console。

将许可证添加到**NetApp Console*** 从NetApp销售代表处购买NetApp Disaster Recovery许可证后，您可以在控制台中管理该许可证。

"了解如何使用NetApp Console添加许可证"。

许可证到期时更新

如果您的许可期限即将到期，或者您的许可容量已达到限制，您将在NetApp Disaster RecoveryUI 中收到通知。您可以在 NetApp Disaster Recovery许可证到期之前进行更新，这样您访问扫描数据的能力就不会中断。



此消息也会出现在NetApp Console和 "通知"。

"了解如何使用NetApp Console更新许可证"。

结束免费试用

您可以随时停止免费试用，也可以等到试用期结束。

步骤

1. 在NetApp Disaster Recovery中，选择 免费试用 - 查看详细信息。
2. 在下拉详细信息中，选择*结束免费试用*。

End free trial

Are you sure that you want to end your free trial on your account ██████████ito1? We will delete your data 60 days after you end your trial. If you subscribe or purchase a license within 60 days, we will retain your data. You may also delete your data immediately when you end your trial.

This action is not reversible.

☐ Delete data immediately after ending my free trial

Comments

Type "end trial" to end your free trial.

End

Cancel

3. 如果您想删除所有数据，请选中*结束免费试用后立即删除数据*。

这将删除所有计划、复制计划、资源组、vCenter 和站点。审计数据、操作日志和作业历史记录将保留直至产品生命周期结束。



如果您结束免费试用，未请求删除数据，并且未购买许可证或订阅，则NetApp Disaster Recovery在免费试用结束后 60 天删除您的所有数据。

4. 在文本框中输入“结束试用”。
5. 选择*结束*。

使用NetApp Disaster Recovery

使用NetApp Disaster Recovery概述

使用NetApp Disaster Recovery，您可以实现以下目标：

- "查看灾难恢复计划的健康状况"。
- "添加 vCenter 站点"。
- "创建资源组以将虚拟机组织在一起"
- "制定灾难恢复计划"。
- "复制 VMware 应用程序"使用SnapMirror复制将主站点上的数据迁移到云中的灾难恢复远程站点。
- "迁移 VMware 应用程序"从您的主站点到另一个站点。
- "测试故障转移"而不会破坏原始虚拟机。
- 一旦发生灾害，"故障转移您的主站点"使用 FSx for NetApp ONTAP迁移到 AWS 上的 VMware Cloud。
- 灾难解除后，"故障恢复"从灾难恢复站点到主站点。
- "监控灾难恢复操作"在作业监控页面上。

在仪表板上查看NetApp Disaster Recovery计划的运行状况

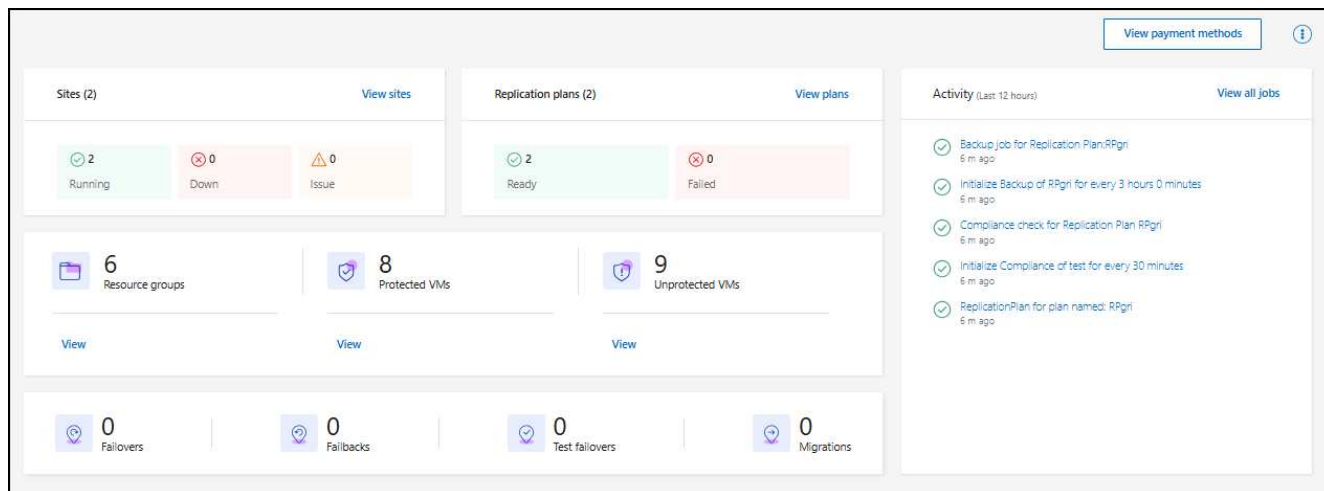
使用NetApp Disaster Recovery仪表板，您可以确定灾难恢复站点和复制计划的健康状况。您可以快速确定哪些站点和计划是健康的、断开的或降级的。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复应用程序管理员或灾难恢复查看器角色。

"了解NetApp Disaster Recovery中的用户角色和权限"。<https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html>["了解所有服务的NetApp Console访问角色"^]。

步骤

1. 登录 "NetApp Console"。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从NetApp Disaster Recovery菜单中，选择 仪表板。



4. 查看仪表板上的以下信息：

- 站点：查看站点的健康状况。站点可以具有以下状态之一：

- 正在运行：vCenter 已连接、健康且正在运行。
- 关闭：vCenter 无法访问或存在连接问题。
- 问题：vCenter 无法访问或存在连接问题。

要查看站点详细信息，请选择“查看全部”查看状态或选择“查看站点”查看全部。

- 复制计划：查看计划的健康状况。计划可以具有以下状态之一：

- 准备好
- 失败的

要查看复制计划的详细信息，请选择“查看全部”查看状态或选择“查看复制计划”查看全部。

- 资源组：查看资源组的健康状况。资源组可以具有以下状态之一：
- 受保护的虚拟机：虚拟机是资源组的一部分。
- 未受保护的虚拟机：虚拟机不属于资源组的一部分。

要查看详细信息，请选择每个下方的“查看”链接。

- 故障转移、测试故障转移和迁移的次数。例如，如果您创建了两个计划并迁移到目标，则迁移计数显示为“2”。

5. 查看活动窗格中的所有操作。要查看作业监视器上的所有操作，请选择“查看所有作业”。

将 vCenter 添加到NetApp Disaster Recovery中的站点

在创建灾难恢复计划之前，您需要在NetApp Console中将主 vCenter 服务器添加到站点，并将目标 vCenter 灾难恢复站点添加到站点。



确保源 vCenter 和目标 vCenter 使用相同的NetApp Console代理。

添加 vCenter 后，NetApp Disaster Recovery会对 vCenter 环境进行深度发现，包括 vCenter 集群、ESXi 主机、数据存储库、存储占用空间、虚拟机详细信息、SnapMirror副本和虚拟机网络。

所需的**NetApp Console**角色 组织管理员、文件夹或项目经理或灾难恢复管理员。

"了解NetApp Disaster Recovery中的用户角色和权限"。 <https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html>了解所有服务的NetApp Console访问角色"]。

关于此任务

如果您在以前的版本中添加了 vCenter 并想要自定义发现计划，则必须编辑 vCenter 服务器站点并设置计划。



NetApp Disaster Recovery每 24 小时执行一次发现。设置站点后，您可以稍后编辑 vCenter 以自定义满足您需求的发现计划。例如，如果您有大量虚拟机，则可以将发现计划设置为每 23 小时 59 分钟运行一次。如果您拥有的虚拟机数量较少，则可以将发现计划设置为每 12 小时运行一次。最小间隔为 30 分钟，最大间隔为 24 小时。

您应该首先执行一些手动发现以获取有关您的环境的最新信息。之后，您可以设置计划以自动运行。

如果您有早期版本的 vCenter 并想要更改发现运行的时间，请编辑 vCenter 服务器站点并设置计划。

新添加或删除的虚拟机将在下一次计划的发现中或在立即手动发现期间被识别。

仅当复制计划处于以下状态之一时，虚拟机才可以受到保护：

- 已就绪
- 故障回复已提交
- 测试故障转移已提交

站点中的 **vCenter** 集群 每个站点包含一个或多个 vCenter。这些 vCenter 使用一个或多个ONTAP存储集群来托管 NFS 或 VMFS 数据存储库。

vCenter 群集只能驻留在一个站点中。您需要以下信息才能将 vCenter 群集添加到站点：

- vCenter 管理 IP 地址或 FQDN
- 具有执行操作所需权限的 vCenter 帐户的凭据。看"[所需的 vCenter 权限](#)"了解更多信息。
- 对于云托管的 VMware 站点，所需的云访问密钥
- 用于访问 vCenter 的安全证书。



该服务支持自签名安全证书或来自中央证书颁发机构 (CA) 的证书。

步骤

1. 登录 "[NetApp Console](#)"。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。

如果您是第一次使用NetApp灾难恢复，则需要添加 vCenter 信息。如果您已经添加了 vCenter 信息，您将看到仪表板。



根据您添加的站点类型，会出现不同的字段。

3. 如果一些 vCenter 站点已经存在并且您想要添加更多，请从菜单中选择“站点”，然后选择“添加”。
4. 在“站点”页面中，选择站点，然后选择“添加 vCenter”。
5. 来源：选择*发现 vCenter 服务器*以输入有关源 vCenter 站点的信息。



要添加更多 vCenter 站点，请选择“站点”，然后选择“添加”。

Add vCenter server

Enter connection details for the vCenter server that is accessible from the Console Agent.

Site	Console Agent
sit .gri2	DRaaSTest
vCenter IP address	Port
	443
vCenter user name	vCenter password
admin	

☒ Use self-signed certificates ⓘ

ⓘ By default, vCenter discovery will run automatically once every 24 hours. This can be edited later. Discovery can also be triggered manually at any time.

- 选择站点，然后选择NetApp Console代理，并提供 vCenter 凭据。
- 仅限本地站点： 要接受源 vCenter 的自签名证书，请选中该复选框。



自签名证书不如其他证书安全。如果您的 vCenter *未*配置证书颁发机构 (CA) 证书，则应选中此框；否则，与 vCenter 的连接将不起作用。

6. 选择“添加”。

接下来添加目标 vCenter。

7. 为目标 vCenter 重新添加站点。

8. 再次选择*添加 vCenter*并添加目标 vCenter 信息。

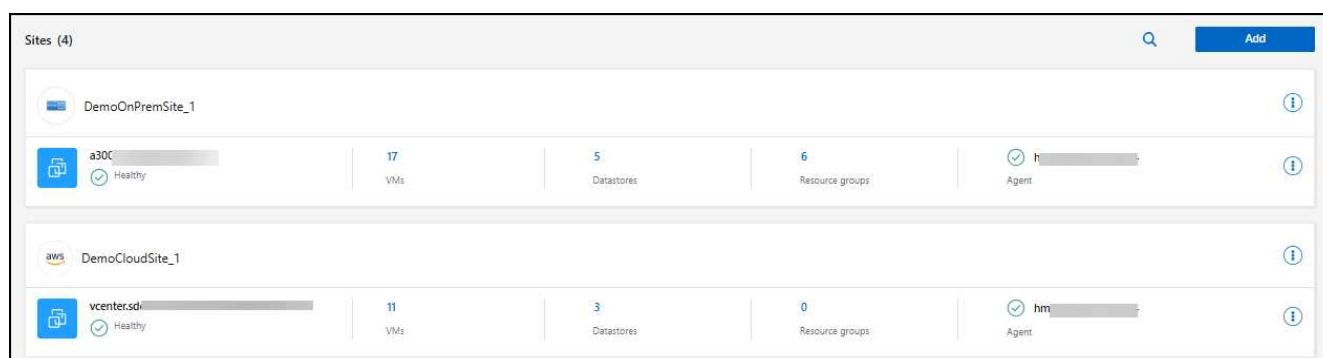
9. 目标：

a. 选择目标站点和位置。如果目标是云，请选择*AWS*。

- （仅适用于云站点）**API 令牌**：输入 API 令牌以授权您的组织访问服务。通过提供特定的组织和服务角色来创建 API 令牌。
- （仅适用于云站点）**长组织 ID**：输入组织的唯一 ID。您可以通过单击 NetApp Console 的“帐户”部分中的用户名来识别此 ID。

b. 选择“添加”。

源 vCenter 和目标 vCenter 出现在站点列表中。



10. 要查看操作进度，请从菜单中选择*作业监控*。

为 vCenter 站点添加子网映射

您可以使用子网映射来管理故障转移操作中的 IP 地址，这使您能够为每个 vCenter 添加子网。当您这样做时，您需要为每个虚拟网络定义 IPv4 CIDR、默认网关和 DNS。

故障转移时，NetApp Disaster Recovery 使用映射网络的 CIDR 为每个 vNIC 分配一个新的 IP 地址。

例如：

- 网络A = 10.1.1.0/24
- 网络B = 192.168.1.0/24

VM1 有一个连接到 NetworkA 的 vNIC（10.1.1.50）。在复制计划设置中，NetworkA 映射到 NetworkB。

故障转移时，NetApp Disaster Recovery 会替换原始 IP 地址 (10.1.1) 的网络部分，并保留原始 IP 地址 (10.1.1.50) 的主机地址 (.50)。对于 VM1，NetApp Disaster Recovery 查看 NetworkB 的 CIDR 设置，并使用 NetworkB 网络部分 192.168.1，同时保留主机部分 (.50) 来为 VM1 创建新的 IP 地址。新的 IP 变为 192.168.1.50。

总之，主机地址保持不变，而网络地址则被站点子网映射中配置的地址替换。这使您能够更轻松地管理故障转移时的 IP 地址重新分配，特别是当您管理数百个网络和数千个虚拟机时。

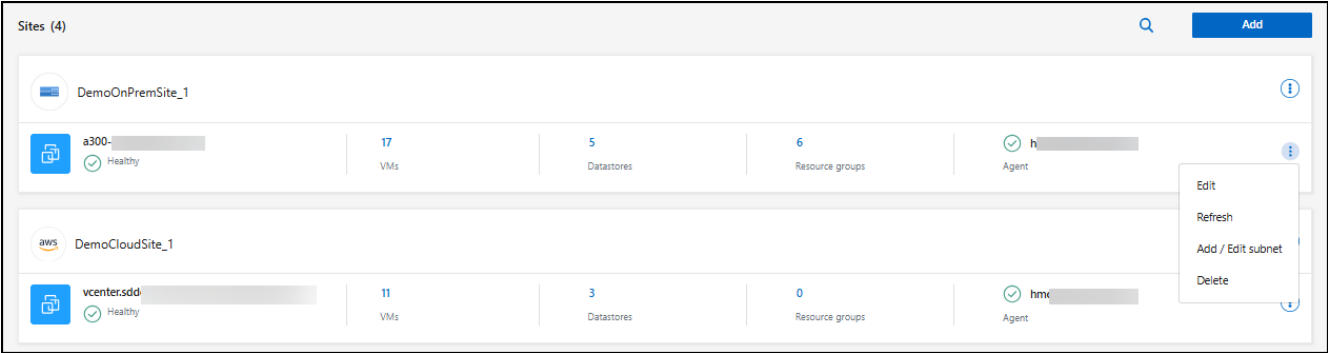
使用子网映射是一个可选的两步过程：

- 首先，为每个 vCenter 站点添加子网映射。

- 其次，在复制计划中，在虚拟机选项卡和目标 IP 字段中指明您想要使用子网映射。

步骤

1. 从NetApp Disaster Recovery菜单中，选择 站点。
2. 从行动  右侧图标，选择*添加子网*。



出现配置子网页面：

Configure subnet

Network Name	Datacenter Name	Subnet	Gateway	DNS
mgmt_1_esxi98	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
mgmt_1_esx92	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
VM Network	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
mgmt_1_esxi94	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
Mgmt_1_esx91	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS

1 - 5 of 12 << < 1 > >>

Add subnet mappingCancel

3. 在配置子网页面中，输入以下信息：
 - a. 子网：输入子网的 IPv4 CIDR，最大为 /32。



CIDR 表示法是一种指定 IP 地址及其网络掩码的方法。/24 表示网络掩码。该数字由 IP 地址和“/”后面的数字组成，该数字表示 IP 地址中有多少位表示网络。例如 192.168.0.50/24，IP 地址为 192.168.0.50，网络地址总位数为 24 位。192.168.0.50 255.255.255.0 变成 192.168.0.0/24。

- b. 网关：输入子网的默认网关。
- c. DNS：输入子网的 DNS。

4. 选择*添加子网映射*。

为复制计划选择子网映射

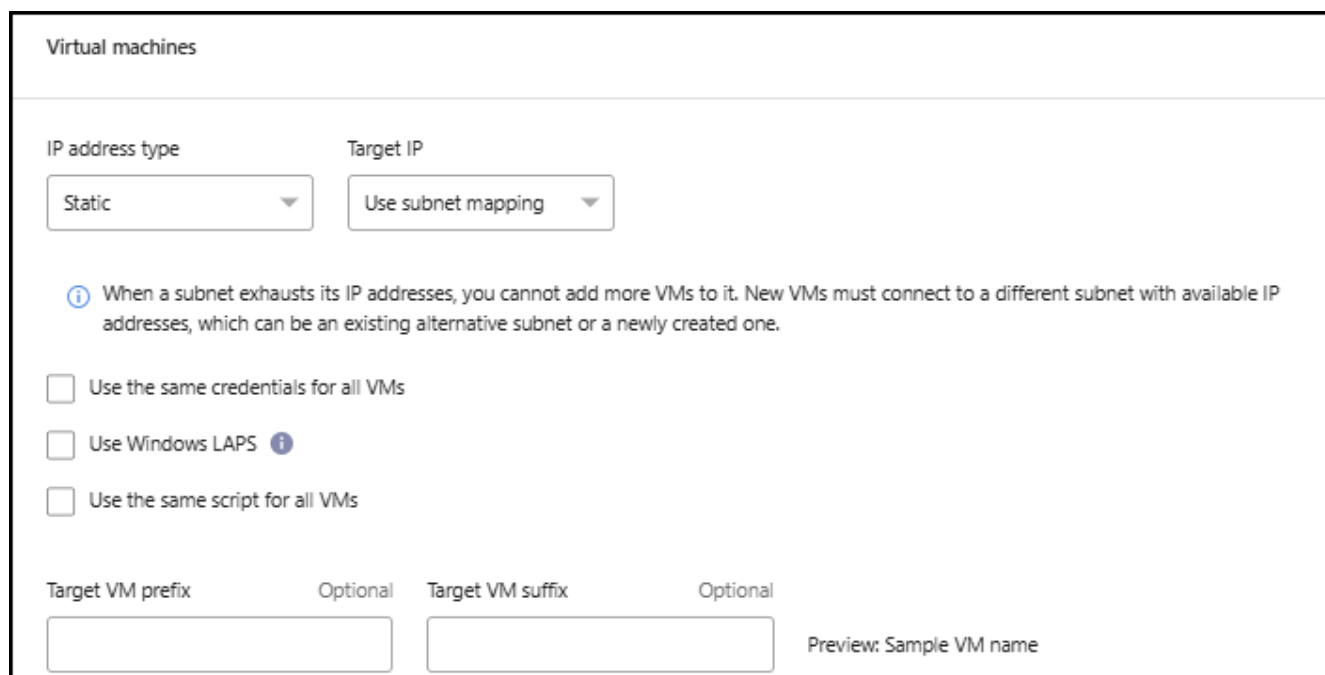
创建复制计划时，您可以选择复制计划的子网映射。

使用子网映射是一个可选的两步过程：

- 首先，为每个 vCenter 站点添加子网映射。
- 其次，在复制计划中，表明您想要使用子网映射。

步骤

1. 从NetApp Disaster Recovery菜单中，选择 复制计划。
2. 选择*添加*以添加复制计划。
3. 通过添加 vCenter 服务器、选择资源组或应用程序并完成映射，以通常的方式填写字段。
4. 在复制计划 > 资源映射页面中，选择 虚拟机 部分。



Virtual machines

IP address type: Static (dropdown)

Target IP: Use subnet mapping (dropdown)

When a subnet exhausts its IP addresses, you cannot add more VMs to it. New VMs must connect to a different subnet with available IP addresses, which can be an existing alternative subnet or a newly created one.

☐ Use the same credentials for all VMs

☐ Use Windows LAPS *i*

☐ Use the same script for all VMs

Target VM prefix: Optional

Target VM suffix: Optional

Preview: Sample VM name

5. 在*目标 IP* 字段中，从下拉列表中选择*使用子网映射*。



如果有两个虚拟机（例如，一个是 Linux，另一个是 Windows），则只需要 Windows 的凭据。

6. 继续创建复制计划。

编辑 vCenter 服务器站点并自定义发现计划

您可以编辑 vCenter 服务器站点来自定义发现计划。例如，如果您有大量虚拟机，则可以将发现计划设置为每 23 小时 59 分钟运行一次。如果您拥有的虚拟机数量较少，则可以将发现计划设置为每 12 小时运行一次。

如果您有早期版本的 vCenter 并想要更改发现运行的时间，请编辑 vCenter 服务器站点并设置计划。

如果您不想安排发现，您可以禁用计划发现选项并随时手动刷新发现。

步骤

1. 从NetApp Disaster Recovery菜单中，选择 站点。
2. 选择您要编辑的站点。
3. 选择操作  右侧的图标并选择*编辑*。
4. 在编辑 vCenter 服务器页面中，根据需要编辑字段。
5. 要自定义发现计划，请选中“启用计划发现”框并选择所需的日期和时间间隔。

Edit vCenter server

Enter connection details for the vCenter server that is accessible from the BlueXP Connector.

Site

Source

BlueXP Connector

SecLab_Connector_4

vCenter IP address

172.26.212.218

port

443

vCenter user name

vCenter password

☒ Use self-signed certificates

☒ Enable scheduled discovery

Start discovery from

2025-04-02

12

:

00

AM

Run discovery once every

23

Hour(s)

59

Minute(s)

Save

Cancel

6. 选择*保存*。

手动刷新发现

您可以随时手动刷新发现。如果您添加或删除了虚拟机并想要更新NetApp Disaster Recovery中的信息，这将非常有用。

步骤

1. 从NetApp Disaster Recovery菜单中，选择 站点。
2. 选择您想要刷新的站点。

3.

选择操作  右侧的图标并选择*刷新*。

在NetApp Disaster Recovery中创建资源组以组织虚拟机

添加 vCenter 站点后，您可以创建资源组，以虚拟机或数据存储区作为单个单元来保护虚拟机。资源组使您能够将一组依赖的虚拟机组织成满足您要求的逻辑组。例如，您可以将与一个应用程序关联的虚拟机分组，也可以将具有相似层的应用程序分组。再举一个例子，组可以包含可以在恢复时运行的延迟启动命令。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员或灾难恢复应用程序管理员角色。

"[了解NetApp Disaster Recovery中的用户角色和权限](https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html)"。https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html["了解所有服务的NetApp Console访问角色"^]。

关于此任务

您可以对虚拟机本身或数据存储中的虚拟机进行分组。

您可以使用以下方法创建资源组：

- 从资源组选项
- 当您创建灾难恢复或_复制计划_时。如果源 vCenter 集群托管了大量虚拟机，则在创建复制计划时创建资源组可能会更轻松。有关在创建复制计划时创建资源组的说明，请参阅"[创建复制计划](#)"。



每个资源组可以包含一个或多个虚拟机或数据存储区。虚拟机将根据您在复制计划中包含它们的顺序启动。您可以通过在资源组列表中上下拖动虚拟机或数据存储来更改顺序。

关于资源组

资源组允许您将虚拟机或数据存储组合为一个单元。

例如，销售点应用程序可能会使用多个虚拟机来存储数据库、业务逻辑和店面。您可以使用一个资源组管理所有这些虚拟机。设置资源组以应用虚拟机启动顺序、网络连接和应用程序所需的所有虚拟机的恢复的复制计划规则。

它是如何工作的？

NetApp Disaster Recovery通过复制资源组中托管虚拟机的底层ONTAP卷和 LUN 来保护虚拟机。为此，系统向 vCenter 查询资源组中托管虚拟机的每个数据存储的名称。然后， NetApp Disaster Recovery会识别托管该数据存储的源ONTAP卷或 LUN。所有保护均使用SnapMirror复制在ONTAP卷级别执行。

如果资源组中的虚拟机托管在不同的数据存储上， NetApp Disaster Recovery将使用以下方法之一来创建ONTAP卷或 LUN 的数据一致快照。

FlexVol卷的相对位置	快照副本流程
多个数据存储 - 同一 SVM 中的FlexVol卷	• ONTAP一致性组已创建 • 拍摄的一致性组快照 • 执行卷范围的SnapMirror复制
多个数据存储 - 多个 SVM 中的FlexVol卷	• ONTAP API: <code>cg_start</code>。使所有卷静止以便可以拍摄快照，并启动所有资源组卷的卷范围快照。 • ONTAP API: <code>cg_end</code>。恢复所有卷上的 I/O，并在拍摄快照后启用卷范围的SnapMirror复制。

创建资源组时，请考虑以下问题：

- 在将数据存储区添加到资源组之前，请先启动虚拟机的手动发现或计划发现。这可确保虚拟机被发现并列在资源组中。如果您不启动手动发现，虚拟机可能不会列在资源组中。
- 确保数据存储区中至少有一个虚拟机。如果数据存储区中没有虚拟机，灾难恢复将无法发现该数据存储区。
- 单个数据存储区不应托管受多个复制计划保护的虚拟机。
- 不要在同一数据存储上托管受保护和不受保护的虚拟机。如果受保护的虚拟机和不受保护的虚拟机托管在同一数据存储上，则可能会出现以下问题：
 - 由于NetApp Disaster Recovery使用SnapMirror并且系统复制整个ONTAP卷，因此该卷的已用容量用于许可考虑。在这种情况下，受保护和不受保护的虚拟机所消耗的卷空间都将包含在此计算中。
 - 如果资源组及其关联的数据存储库需要故障转移到灾难恢复站点，则任何未受保护的虚拟机（不属于资源组但托管在ONTAP卷上的虚拟机）将在故障转移过程中不再存在于源站点上，从而导致源站点上未受保护的虚拟机发生故障。此外，NetApp Disaster Recovery不会在故障转移 vCenter 站点启动那些未受保护的虚拟机。
- 要保护虚拟机，必须将其包含在资源组中。

最佳实践：在部署NetApp Disaster Recovery之前组织您的虚拟机，以最大限度地减少“数据存储蔓延”。将需要保护的虚拟机放置在数据存储的子集上，将不需要保护的虚拟机放置在不同的数据存储子集上。确保任何给定数据存储上的虚拟机不受不同的复制计划的保护。

步骤

1. 登录 ["NetApp Console"](#)。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从NetApp Disaster Recovery菜单中，选择 资源组。
4. 选择“添加”。
5. 输入资源组的名称。
6. 选择虚拟机所在的源 vCenter 集群。
7. 根据您的搜索方式选择*虚拟机*或*数据存储*。
8. 选择“添加资源组”选项卡。系统列出所选 vCenter 集群中的所有数据存储区或虚拟机。如果您选择了“数据存储”，系统将列出所选 vCenter 群集中的所有数据存储。如果您选择了“虚拟机”，系统将列出所选 vCenter 集群中的所有虚拟机。

9. 在添加资源组页面的左侧，选择要保护的虚拟机。

Add resource group

Name

DemoRG

vCenter

☒ Virtual machines

☐ Datastores

Select virtual machines

Q Search all datastores

☒ VMFS_Centos_vm1_ds4

☒ VMFS_Centos_vm1_ds5

☒ VMFS_RHEL_vm2_ds1

☐ VMFS_RHEL_vm2_ds2

☐ VMFS_RHEL_vm2_ds3

☐ VMFS_RHEL_vm2_ds4

☐ VMFS_RHEL_vm2_ds5

Selected VMs (3)

VMFS_Centos_vm1_ds4

×

VMFS_Centos_vm1_ds5

×

VMFS_RHEL_vm2_ds1

×

Add

Cancel

Add resource group

Name: vCenter:

☐ Virtual machines ☒ Datastores

Select datastores

Search datastores

- ☐ DS4_auto_vmfs_6d7
- ☐ DS2_auto_vmfs_6d7
- ☐ DS1_surya_nfs_scale
- ☒ DS4_auto_nfs_450
- ☒ DS3_auto_nfs_450
- ☐ DS1_auto_nfs_450
- ☐ DS2_auto_nfs_450

Selected datastores (2)

- DS4_auto_nfs_450 X
- DS3_auto_nfs_450 X

10. 或者，通过将每个虚拟机在列表中向上或向下拖动来更改右侧虚拟机的顺序。虚拟机将根据您包含它们的顺序启动。
11. 选择“添加”。

在NetApp Disaster Recovery中创建复制计划

添加 vCenter 站点后，就可以创建灾难恢复或复制计划了。复制计划管理 VMware 基础架构的数据保护。选择源和目标 vCenter，挑选资源组，并对应用程序的恢复和启动方式进行分组。例如，您可以对与一个应用程序关联的虚拟机 (VM) 进行分组，也可以对具有相似层的应用程序进行分组。此类计划有时被称为_蓝图_。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员或灾难恢复应用程序管理员角色。

["了解NetApp Disaster Recovery中的用户角色和权限"](https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html)。https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html["了解所有服务的NetApp Console访问角色"^]。

关于此任务

您可以创建复制计划并编辑合规性和测试计划。运行虚拟机的测试故障转移而不影响生产工作负载。

您可以保护多个数据存储上的多个虚拟机。 NetApp Disaster Recovery为托管受保护 VM 数据存储的所有 ONTAP 卷创建 ONTAP 一致性组。

仅当复制计划处于以下状态之一时，虚拟机才可以受到保护：

- 已就绪
- 故障回复已提交
- 测试故障转移已提交

复制计划快照

灾难恢复在源集群和目标集群上维护相同数量的快照。默认情况下，该服务每 24 小时执行一次快照协调过程，以确保源集群和目标集群上的快照数量相同。

以下情况可能会导致源集群和目标集群之间的快照数量不同：

- 某些情况可能会导致灾难恢复之外的ONTAP操作在卷中添加或删除快照：
 - 如果源站点上缺少快照，则目标站点上的相应快照可能会被删除，具体取决于关系的默认SnapMirror策略。
 - 如果目标站点上缺少快照，则服务可能会在下一个计划的快照协调过程中删除源站点上的相应快照，具体取决于关系的默认SnapMirror策略。
- 复制计划的快照保留计数的减少可能导致服务删除源站点和目标站点上最旧的快照以满足新减少的保留数量。

在这些情况下，灾难恢复会在下一次一致性检查时从源和目标集群中删除较旧的快照。或者，管理员可以通过选择“操作”立即执行快照清理 ●●●复制计划上的图标并选择*清理快照*。

该服务每 24 小时执行一次快照对称性检查。

开始之前

- 在创建SnapMirror关系之前，请在灾难恢复之外设置集群和 SVM 对等关系。
- 使用 Google Cloud，您只能向复制计划添加一个卷或数据存储。



在部署NetApp Disaster Recovery之前整理您的虚拟机，以最大限度地减少“数据存储蔓延”。将需要保护的虚拟机放置在数据存储的子集上，将不需要保护的虚拟机放置在不同的数据存储子集上。使用基于数据存储的保护来确保任何给定数据存储上的虚拟机都受到保护。

创建计划

向导将引导您完成以下步骤：

- 选择 vCenter 服务器。
- 选择要复制的虚拟机或数据存储区并分配资源组。
- 映射资源如何从源环境映射到目标。
- 设置计划运行的频率、运行客户托管脚本、设置启动顺序并选择恢复点目标。
- 审查计划。

制定计划时，您应该遵循以下准则：

- 对计划中的所有虚拟机使用相同的凭据。
- 对计划中的所有虚拟机使用相同的脚本。
- 对计划中的所有虚拟机使用相同的子网、DNS 和网关。

选择 vCenter 服务器

首先，选择源 vCenter，然后选择目标 vCenter。

步骤

1. 登录 "NetApp Console"。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从NetApp Disaster Recovery菜单中，选择 复制计划，然后选择 添加。或者，如果您刚开始使用该服务，请从仪表板中选择*添加复制计划*。

The screenshot shows the 'Add replication plan' wizard in the NetApp Console. The title bar at the top indicates the current step is '1 vCenter servers', with other steps being '2 Applications', '3 Resource mapping', and '4 Review'. The breadcrumb trail shows 'Replication plan > Add plan'. The main heading is 'vCenter servers' with the instruction 'Provide the plan name and select the source and target vCenter servers.' Below this, there is a text input field for 'Replication plan name' containing 'RPgr4'. A blue information icon and text prompt the user to 'Select a source vCenter where your data exists, to replicate to the selected target vCenter.' A diagram illustrates the replication process: two server icons on the left labeled 'Source vCenter' with a dropdown menu showing 'a3C', an arrow labeled 'Replicate' in the middle, and a cloud icon on the right labeled 'Target vCenter' with a dropdown menu showing 'vcenter.sdd'. At the bottom, there are 'Cancel' and 'Next' buttons.

4. 为复制计划创建一个名称。
5. 从源和目标 vCenter 列表中选择源 vCenter 和目标 vCenter。
6. 选择“下一步”。

选择要复制的应用程序并分配资源组

下一步是将所需的虚拟机或数据存储分组到功能资源组中。资源组使您能够使用公共快照保护一组虚拟机或数据存储区。

当您在复制计划中选择应用程序时，您可以看到计划中每个虚拟机或数据存储区的操作系统。这有助于决定如何将虚拟机或数据存储分组到资源组中。



每个资源组可以包含一个或多个虚拟机或数据存储区。

创建资源组时，请考虑以下问题：

- 在将数据存储区添加到资源组之前，请先启动虚拟机的手动发现或计划发现。这可确保虚拟机被发现并列在资源组中。如果您不触发手动发现，虚拟机可能不会列在资源组中。
- 确保数据存储区中至少有一个虚拟机。如果数据存储中没有虚拟机，则不会发现该数据存储。
- 单个数据存储区不应托管受多个复制计划保护的虚拟机。
- 不要在同一数据存储上托管受保护和不受保护的虚拟机。如果受保护的虚拟机和不受保护的虚拟机托管在同一数据存储上，则可能会出现以下问题：
 - 由于NetApp Disaster Recovery使用SnapMirror并且系统复制整个ONTAP卷，因此该卷的已用容量用于许可考虑。在这种情况下，受保护和不受保护的虚拟机所消耗的卷空间都将包含在此计算中。
 - 如果资源组及其关联的数据存储库需要故障转移到灾难恢复站点，则任何未受保护的虚拟机（不属于资源组但托管在ONTAP卷上的虚拟机）将在故障转移过程中不再存在于源站点上，从而导致源站点上未受保护的虚拟机发生故障。此外，NetApp Disaster Recovery不会在故障转移 vCenter 站点启动那些未受保护的虚拟机。
- 要保护虚拟机，必须将其包含在资源组中。



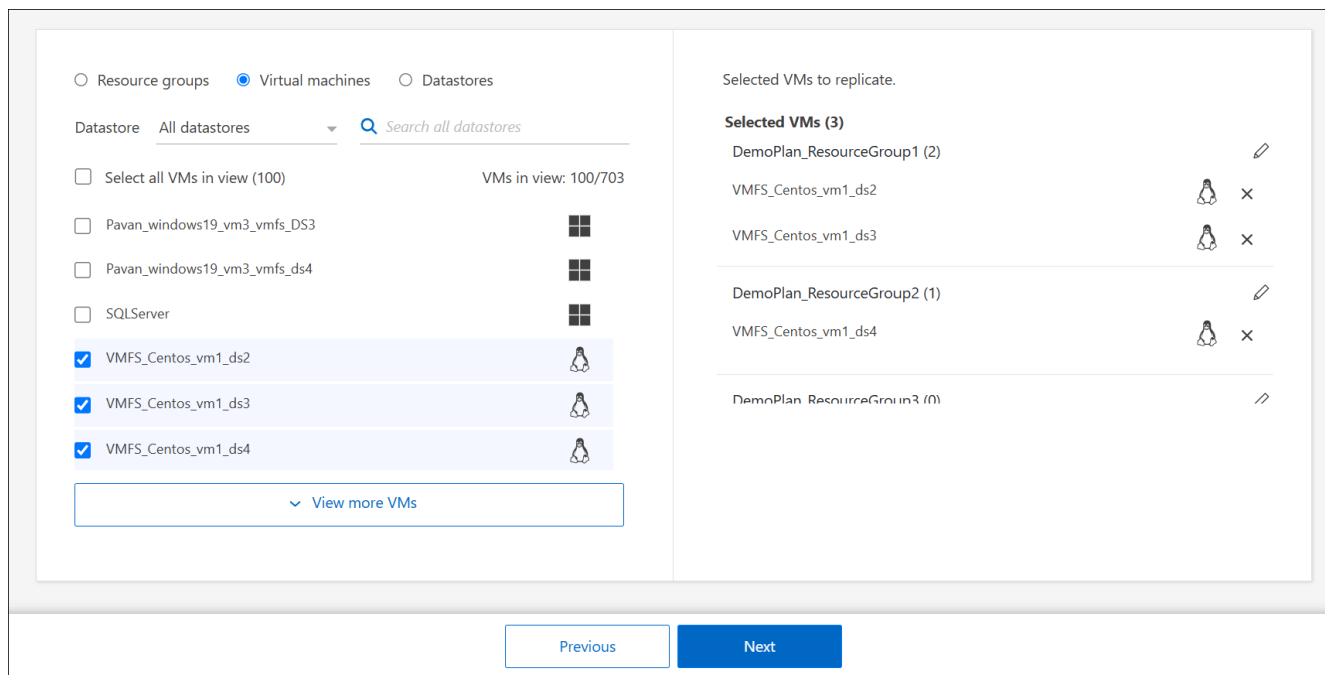
为故障转移测试创建一套单独的专用映射，以防止 VMS 使用相同的 IP 地址连接到生产网络。

步骤

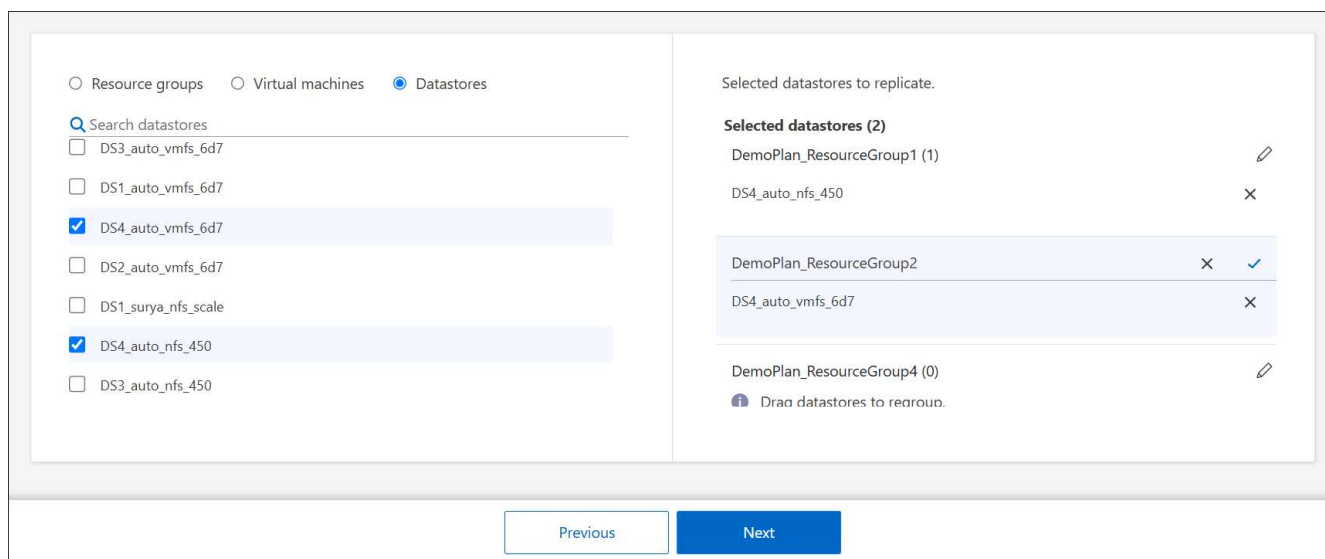
1. 选择“虚拟机”或“数据存储”。
2. 可选择按名称搜索特定的虚拟机或数据存储。
3. 在“应用程序”页面的左侧，选择要保护并分配到所选组的虚拟机或数据存储区。

源 vCenter 必须位于本地 vCenter 上。目标 vCenter 可以是同一站点或远程站点中的第二个本地 vCenter，也可以是基于云的软件定义数据中心 (SDDC)，例如 VMware Cloud on AWS。这两个 vCenter 都应该已经添加到您的灾难恢复工作环境中。

所选资源将自动添加到组 1，并启动新的组 2。每次向最后一个组添加资源时，都会添加另一个组。



或者，对于数据存储：



4. 或者，执行以下任一操作：

- 要更改群组名称，请点击群组*编辑*  图标。
- 要从组中删除资源，请选择资源旁边的 **X**。
- 要将资源移动到不同的组，请将其拖放到新组中。



要将数据存储移动到不同的资源组，请取消选择不需要的数据存储并提交复制计划。然后，创建或编辑其他复制计划并重新选择数据存储。

5. 选择“下一步”。

将源资源映射到目标

在资源映射步骤中，指定源环境中的资源应如何映射到目标。创建复制计划时，您可以为计划中的每个虚拟机设置启动延迟和顺序。这使您可以设置虚拟机的启动顺序。

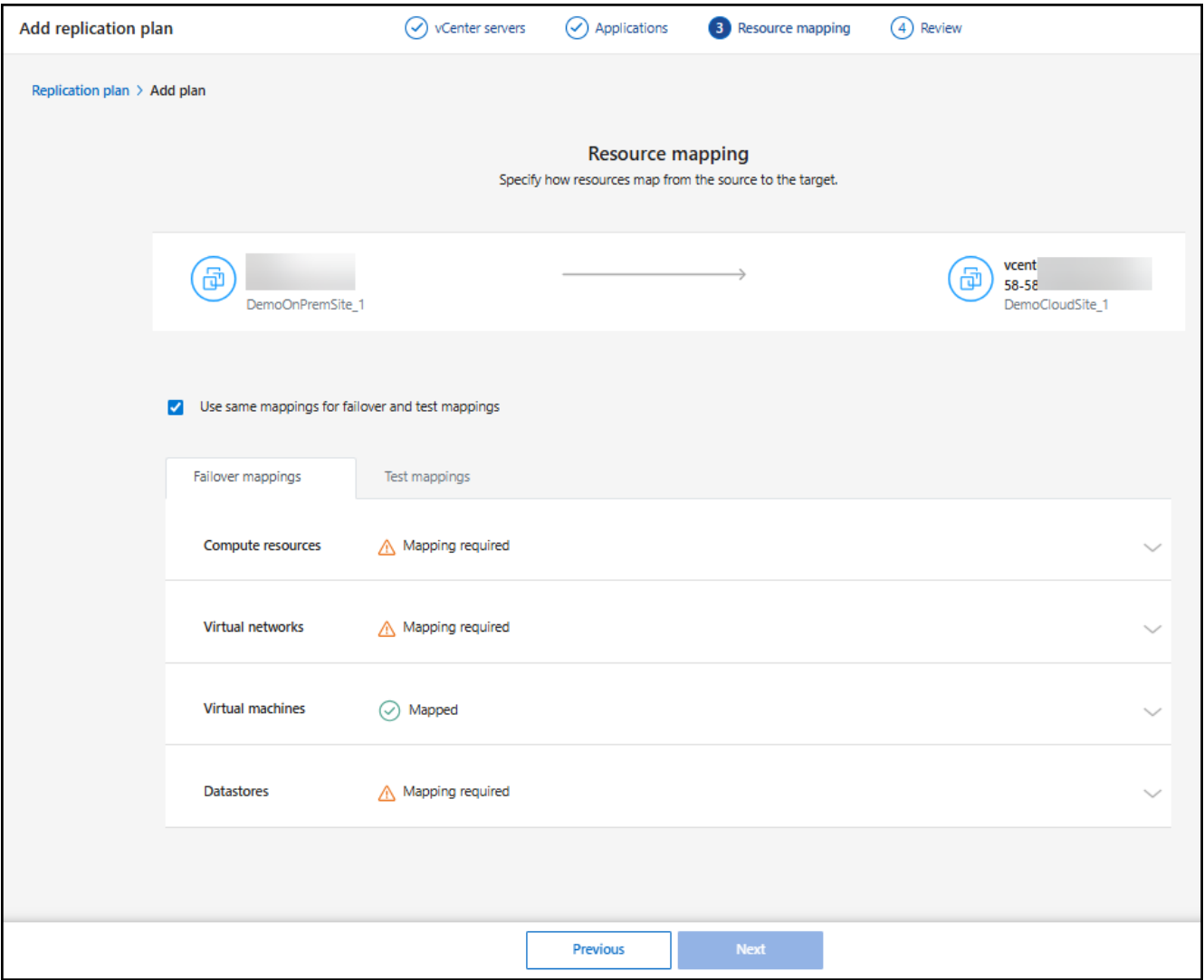
如果您计划将测试故障转移作为 DR 计划的一部分执行，则应提供一组测试故障转移映射，以确保故障转移测试期间启动的虚拟机不会干扰生产虚拟机。您可以通过为测试虚拟机提供不同的 IP 地址，或者将测试虚拟机的虚拟 NIC 映射到与生产隔离但具有相同 IP 配置的不同网络（称为_气泡_或_测试网络_）来实现此目的。

开始之前

如果要在服务中创建SnapMirror关系，则集群及其 SVM 对等关系应该已在NetApp Disaster Recovery之外设置。

步骤

- 1. 在“资源映射”页面中，选中该复选框，以便对故障转移和测试操作使用相同的映射。



- 2. 在故障转移映射选项卡中，选择每个资源右侧的向下箭头并映射每个部分中的资源：
 - 计算资源
 - 虚拟网络

- 虚拟机
- 数据存储库

地图资源 > 计算资源部分

计算资源部分定义了故障转移后虚拟机的恢复位置。将源 vCenter 数据中心和集群映射到目标数据中心和集群。

或者，可以在特定的 vCenter ESXi 主机上重新启动虚拟机。如果启用了 VMWare DRS，您可以根据需要自动将 VM 移动到备用主机以满足 DR 配置的策略。

或者，您可以将此复制计划中的所有虚拟机放入 vCenter 的唯一文件夹中。这提供了一种在 vCenter 内快速组织故障转移虚拟机的简便方法。

选择“计算资源”旁边的向下箭头。

- 源数据中心和目标数据中心
- 目标集群
- 目标主机（可选）：选择集群后，您可以设置此信息。



如果 vCenter 配置了分布式资源调度程序 (DRS) 来管理集群中的多个主机，则您无需选择主机。如果您选择一个主机，NetApp Disaster Recovery 会将所有虚拟机放置在选定的主机上。* 目标 VM 文件夹（可选）：创建一个新的根文件夹来存储选定的 VM。

地图资源 > 虚拟网络部分

虚拟机使用连接到虚拟网络的虚拟网卡。在故障转移过程中，该服务将这些虚拟网卡连接到目标 VMware 环境中定义的虚拟网络。对于资源组中虚拟机使用的每个源虚拟网络，该服务都需要一个目标虚拟网络分配。



您可以将多个源虚拟网络分配给同一个目标虚拟网络。但这可能会造成 IP 网络配置冲突。您可以将多个源网络映射到单个目标网络，以确保所有源网络具有相同的配置。

在故障转移映射选项卡中，选择“虚拟网络”旁边的向下箭头。选择源虚拟局域网和目标虚拟局域网。

选择映射到适当虚拟 LAN 的网络。虚拟 LAN 应该已经配置好了，因此请选择适当的虚拟 LAN 来映射 VM。

地图资源 > 虚拟机部分

您可以通过设置以下任意选项来配置受复制计划保护的资源组中的每个虚拟机，以适应目标 vCenter 虚拟环境：

- 虚拟 CPU 的数量
- 虚拟 DRAM 的数量
- IP 地址配置
- 作为故障转移过程的一部分，能够执行客户操作系统 shell 脚本
- 能够使用唯一的前缀和后缀更改故障转移虚拟机名称
- 能够在虚拟机故障转移期间设置重启顺序

在“故障转移映射”选项卡中，选择“虚拟机”旁边的向下箭头。

虚拟机的默认设置是映射的。默认映射使用与虚拟机在生产环境中相同的设置（相同的 IP 地址、子网掩码和网关）。

如果您对默认设置进行任何更改，则必须将目标 IP 字段更改为“与源不同”。



如果将设置更改为“与源不同”，则需要提供 VM 客户操作系统凭据。

根据您的选择，此部分可能会显示不同的字段。

您可以增加或减少分配给每个故障转移 VM 的虚拟 CPU 数量。但是，每个虚拟机至少需要一个虚拟 CPU。您可以更改分配给每个虚拟机的虚拟 CPU 和虚拟 DRAM 的数量。您可能想要更改默认虚拟 CPU 和虚拟 DRAM 设置的最常见原因是目标 vCenter 集群节点没有源 vCenter 集群那么多的可用资源。

网络设置 灾难恢复支持针对 VM 网络的大量配置选项。如果目标站点的虚拟网络使用与源站点上的生产虚拟网络不同的 TCP/IP 设置，则可能需要更改这些设置。

在最基本（和默认）级别，设置只是对目标站点上的每个 VM 使用与源站点上相同的 TCP/IP 网络设置。这要求您在源和目标虚拟网络上配置相同的 TCP/IP 设置。

该服务支持虚拟机的静态或动态主机配置协议 (DHCP) IP 配置的网络设置。DHCP 提供了一种基于标准的方法来动态配置主机网络端口的 TCP/IP 设置。DHCP 必须至少提供一个 TCP/IP 地址，还可以提供一个默认网关地址（用于路由到外部互联网连接）、一个子网掩码和一个 DNS 服务器地址。DHCP 通常用于最终用户计算设备，例如员工台式机、笔记本电脑和移动电话连接，同时也可用于任何网络计算设备，例如服务器。

- ***使用相同的子网掩码、DNS 和网关设置*选项：**由于这些设置对于连接到相同虚拟网络的所有虚拟机通常都是相同的，因此您可能会发现配置一次这些设置并让灾难恢复使用复制计划保护的资源组中所有虚拟机的设置会更容易。如果某些虚拟机使用不同的设置，则需要取消选中此框并为每个虚拟机提供这些设置。
- **IP 地址类型：**重新配置虚拟机配置以匹配目标虚拟网络要求。NetApp Disaster Recovery 提供两个选项：
 - **DHCP 或静态 IP。**对于静态 IP，配置子网掩码、网关和 DNS 服务器。此外，输入虚拟机的凭据。
 - **DHCP：**如果您希望虚拟机从 DHCP 服务器获取网络配置信息，请选择此设置。如果您选择此选项，则只需提供 VM 的凭据。
 - **静态 IP：**如果您想手动指定 IP 配置信息，请选择此设置。您可以选择以下之一：与源相同、与源不同或子网映射。如果您选择与来源相同，则无需输入凭据。另一方面，如果您选择使用来自源的不同信息，则可以提供凭据、VM 的 IP 地址、子网掩码、DNS 和网关信息。VM 客户操作系统凭据应提供给全局级别或每个 VM 级别。

当将大型环境恢复到较小的目标集群或进行灾难恢复测试而无需配置一对一的物理 VMware 基础架构时，这会非常有用。

Virtual machines

IP address type

Static

Target IP

Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

☐ Downgrade VM hardware version and register ⓘ

☒ Retain original folder hierarchy ⓘ

Target VM prefix

Optional

Target VM suffix

Optional

Preview: Sample VM name

- 脚本：您可以将自定义的访客操作系统托管脚本（.sh、.bat 或 .ps1 格式）作为后处理程序包含在内。借助自定义脚本，灾难恢复可以在故障转移、故障恢复和迁移过程之后运行您的脚本。例如，您可以使用自定义脚本在故障转移完成后恢复所有数据库事务。该服务可以在运行 Microsoft Windows 或任何受支持的 Linux 变体的虚拟机中运行脚本，并支持命令行参数。您可以将脚本分配给单个虚拟机，也可以分配给复制计划中的所有虚拟机。

要使用 VM 客户操作系统启用脚本执行，必须满足以下条件：

- 必须在虚拟机上安装 VMware Tools。
- 必须提供适当的用户凭据以及足够的来宾操作系统权限才能运行该脚本。
- （可选）包括脚本的超时值（以秒为单位）。

运行 **Microsoft Windows** 的虚拟机：可以运行 Windows 批处理 (.bat) 或 PowerShell (ps1) 脚本。Windows 脚本可以使用命令行参数。格式化每个参数 ``arg_name$value`` 格式，其中 ``arg_name`` 是参数的名称，``$value`` 是参数的值，每个值用分号分隔 ``argument$value`` 一对。

运行 **Linux** 的虚拟机：可以运行虚拟机使用的 Linux 版本支持的任何 shell 脚本 (.sh)。Linux 脚本可以使用命令行参数。在以分号分隔的值列表中提供参数。不支持命名参数。将每个参数添加到 `Arg[x]` 参数列表并使用指针引用每个值 ``Arg[x]` 数组，例如，``value1;value2;value3``。

- 降级虚拟机硬件版本并注册：如果目标 ESX 主机版本早于源版本，请选择此项，以便在注册期间匹配。
- 保留原始文件夹层次结构：默认情况下，灾难恢复会在故障转移时保留虚拟机清单层次结构（文件夹结构）。如果恢复目标_不_具有原始文件夹层次结构，则灾难恢复功能会创建它。

取消选中此框可忽略原始文件夹层次结构。

- 目标 **VM** 前缀和后缀：在虚拟机详细信息下，您可以选择为每个故障转移的 VM 名称添加前缀和后缀。这有助于区分故障转移的虚拟机和在同一 vCenter 集群上运行的生产虚拟机。例如，您可以向虚拟机名称添加前缀“DR-”和后缀“-failover”。有些人会添加第二个生产 vCenter，以便在发生灾难时临时在不同站点托管虚拟机。添加前缀或后缀可以帮助您快速识别故障转移的虚拟机。您还可以在自定义脚本中使用前缀或后缀。

供域控制器详细信息。

如果您不使用 Windows LAPS，则该 VM 是 Windows VM，并且 VM 行上的凭据选项已启用。您可以提供虚拟机的凭据。

Disaster recovery

Add replication plan

✓ vCenter servers

✓ Applications

3 Resource mapping

4 Recurrence

5 Review

DHCP

☐ Use the same credentials for all VMs

☐ Use the same scripts for all VMs

Source VM

Operating system

CPUs

RAM (GB)

Boot order

Boot delay (mins)

Create application-consistent replicas

Scripts

Credentials

Resource group 1

SQL_PRD_1

Linux

4

16

1

0

☒

None

Required

Resource group 2

SQL_PRD_2

Linux

4

32

2

0

☒

file.py, +2

Required

SQL_PRD_3

Linux

8

64

3

0

☒

sql_dr_prod.py

Provided

SQL_PRD_4

Linux

8

64

4

0

☒

sql_dr_prod.py

Provided

SQL_PRD_5

Linux

8

64

5

0

☒

sql_dr_prod.py

Provided

SQL_PRD_6

Linux

8

64

6

0

☒

sql_dr_prod.py

Provided

Datastores

Mapped

Previous

Next

创建应用程序一致的副本

许多虚拟机托管数据库服务器，例如 Oracle 或 Microsoft SQL Server。这些数据库服务器需要应用程序一致的快照，以确保在拍摄快照时数据库处于一致状态。

应用程序一致性快照可确保在拍摄快照时数据库处于一致状态。这很重要，因为它可以确保数据库在故障转移或故障回复操作后能够恢复到一致状态。

数据库服务器管理的数据可能与托管数据库服务器的虚拟机托管在同一个数据存储上，也可能托管在不同的数据存储上。下表显示了灾难恢复中应用程序一致性快照支持的配置：

数据位置	支持	笔记
与虚拟机位于同一 vCenter 数据存储区内	是	由于数据库服务器和数据库都位于同一个数据存储区中，因此在故障转移时服务器和数据都将同步。
与虚拟机位于不同的 vCenter 数据存储区内	否	灾难恢复无法识别数据库服务器的数据何时位于不同的 vCenter 数据存储上。该服务无法复制数据，但可以复制数据库服务器虚拟机。 虽然数据库数据无法复制，但该服务可确保数据库服务器执行所有必要步骤，以确保数据库在 VM 备份时处于静止状态。

数据位置	支持	笔记
在外部数据源中	否	如果数据驻留在客户机安装的 LUN 或 NFS 共享上，灾难恢复无法复制数据，但可以复制数据库服务器 VM。 虽然数据库数据无法复制，但该服务可确保数据库服务器执行所有必要步骤，以确保数据库在 VM 备份时处于静止状态。

在计划备份期间，灾难恢复会使数据库服务器处于静止状态，然后对托管数据库服务器的虚拟机进行快照。这可确保在拍摄快照时数据库处于一致状态。

- 对于 Windows VM，该服务使用 Microsoft 卷影复制服务 (VSS) 与任一数据库服务器协调。
- 对于 Linux VM，该服务使用一组脚本将 Oracle 服务器置于备份模式。

要启用虚拟机及其托管数据存储的应用程序一致性副本，请选中每个虚拟机的“创建应用程序一致性副本”*旁边的框，并提供具有适当权限的来宾登录凭据。

地图资源 > 数据存储部分

VMware 数据存储库托管在ONTAP FlexVol卷或使用 VMware VMFS 的ONTAP iSCSI 或 FC LUN 上。使用数据存储部分定义目标ONTAP集群、存储虚拟机 (SVM) 以及卷或 LUN，以将磁盘上的数据复制到目标。

选择“数据存储”旁边的向下箭头。根据虚拟机的选择，自动选择数据存储映射。

根据您的选择，此部分可能会启用或禁用。

Datastores

☒ Use platform managed backups and retention schedules ⓘ

Start running retention from

2025-05-13

12

:

00

AM

ⓘ

Run retention once every

03

Hour(s)

00

Minute(s)

Retention count for all datastores ⓘ

30

Source datastore

DS_Testing_Staging (Temp_3510_N1:DR_Vol_Staging)

Target datastore

DS_Testing_Staging (test:DR_Vol_Staging_dest)

Preferred NFS LIF

Select preferred NFS LIF

Export policy

Select export policy

- 使用平台管理的备份和保留计划：如果您使用外部快照管理解决方案，请选中此框。 NetApp Disaster Recovery支持使用外部快照管理解决方案，例如本机ONTAP SnapMirror策略调度程序或第三方集成。如果复制计划中的每个数据存储库（卷）都已具有在其他地方管理的SnapMirror关系，则可以将这些快照用作NetApp Disaster Recovery中的恢复点。

选择此选项后， NetApp Disaster Recovery不会配置备份计划。但是，您仍然需要配置保留计划，因为仍可

能需要拍摄快照以进行测试、故障转移和故障回复操作。

配置完成后，服务不会定期拍摄任何快照，而是依赖外部实体来拍摄和更新这些快照。

- 开始时间：输入您希望备份和保留开始运行的日期和时间。
- 运行间隔：输入以小时和分钟为单位的时间间隔。例如，如果您输入 1 小时，则服务将每小时拍摄一次快照。
- 保留计数：输入您想要保留的快照数量。



保留的快照数量以及每个快照之间的数据变化率决定了源和目标上消耗的存储空间量。保留的快照越多，消耗的存储空间就越多。

- 源和目标数据存储：如果存在多个（扇出） SnapMirror关系，您可以选择要使用的目标。如果卷已建立SnapMirror关系，则会显示相应的源数据存储库和目标数据存储库。如果卷没有SnapMirror关系，您现在可以通过选择目标集群、选择目标 SVM 并提供卷名称来创建一个。该服务将创建卷和SnapMirror关系。



如果要在服务中创建SnapMirror关系，则集群及其 SVM 对等关系应该已在NetApp Disaster Recovery之外设置。

- 如果虚拟机来自同一卷和同一 SVM，则该服务将执行标准ONTAP快照并更新辅助目标。
 - 如果虚拟机来自不同的卷和相同的 SVM，则该服务将通过包含所有卷来创建一致性组快照并更新辅助目标。
 - 如果虚拟机来自不同的卷和不同的 SVM，则该服务通过包含相同或不同集群中的所有卷来执行一致性组启动阶段和提交阶段快照，并更新辅助目标。
 - 在故障转移期间，您可以选择任何快照。如果您选择最新的快照，该服务将按需创建备份、更新目标并使用该快照进行故障转移。
- 首选 **NFS LIF** 和 导出策略：通常，让服务选择首选 NFS LIF 和导出策略。如果要使用特定的 NFS LIF 或导出策略，请选择每个字段旁边的向下箭头并选择相应的选项。

您可以选择在故障转移事件后为卷使用特定的数据接口 (LIF)。如果目标 SVM 有多个 LIF，这对于数据流量平衡很有用。

为了进一步控制 NAS 数据访问安全性，该服务可以为不同的数据存储卷分配特定的 NAS 导出策略。导出策略定义访问数据存储卷的 NFS 客户端的访问控制规则。如果您未指定导出策略，则服务将使用 SVM 的默认导出策略。



建议您创建一个专门的导出策略，将卷访问权限限制为_仅_将托管受保护虚拟机的源 vCenter ESXi 主机和目标 vCenter ESXi 主机。这样可以确保外部实体无法访问 NFS 导出内容。

添加测试故障转移映射

步骤

1. 要为测试环境设置不同的映射，请取消选中该框并选择“测试映射”选项卡。
2. 像以前一样浏览每个选项卡，但这次针对测试环境。

在测试映射选项卡上，虚拟机和数据存储映射被禁用。



您可以稍后测试整个计划。现在，您正在为测试环境设置映射。

审查复制计划

最后，花几分钟时间检查一下复制计划。



您可以稍后禁用或删除复制计划。

步骤

1. 查看每个选项卡中的信息：计划详细信息、故障转移映射和虚拟机。
2. 选择*添加计划*。

该计划已添加到计划列表中。

编辑计划以测试合规性并确保故障转移测试有效

您可能需要设置计划来测试合规性和故障转移测试，以确保它们在需要时能够正常工作。

- 合规时间影响：创建复制计划时，服务默认创建合规计划。默认合规时间为 30 分钟。要更改此时间，您可以编辑复制计划中的时间表。
- 测试故障转移影响：您可以根据需要或按计划测试故障转移过程。这使您可以测试虚拟机到复制计划中指定的目标的故障转移。

测试故障转移会创建FlexClone卷、挂载数据存储库并在该数据存储库上移动工作负载。测试故障转移操作不会影响生产工作负载、测试站点上使用的SnapMirror关系以及必须继续正常运行的受保护工作负载。

根据计划，故障转移测试运行并确保工作负载移动到复制计划指定的目标。

步骤

1. 从NetApp Disaster Recovery菜单中，选择 复制计划。

Replication plans (3)							Q	Create report	Add
Name	Compliance status	Plan status	Protected site	Resource groups	Failover site				
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1	...			
RPgri	Healthy	Ready	DemoOnPremSite_1	rggri1	DemoCloudSite_1	...			
rpgr3	Healthy	Ready	site-onprem-gri2	rpgr3_ResourceGroup1	DemoOnPremSite_1	...			

2. 选择*操作* ... 图标并选择*编辑时间表*。
3. 输入您希望NetApp Disaster Recovery检查测试合规性的频率（分钟）。
4. 要检查您的故障转移测试是否正常，请检查*按月度计划运行故障转移*。
 - a. 选择您希望运行这些测试的日期和时间。
 - b. 输入您希望测试开始的日期（yyyy-mm-dd 格式）。

Edit schedules: RP_DRAAS

Compliance checks and test failovers run on a recurring basis. Enter how often these actions should occur.

Compliance check

Frequency (min) ⓘ

30

Test failover

☒ Run test failovers on a schedule ⓘ

☒ Use on-demand snapshot for scheduled test failover

Repeat

Daily ▼

Hour : Minute AM/PM Start date ⓘ

12 : 00 AM 2025-05-13 📅

☒ Automatically cleanup 10 minutes after test failover ⓘ

Save **Cancel**

5. 使用按需快照进行计划测试故障转移：要在启动自动测试故障转移之前拍摄新快照，请选中此框。
6. 要在故障转移测试完成后清理测试环境，请选中*测试故障转移后自动清理*并输入在清理开始前等待的分钟数。



此过程将从测试位置取消注册临时虚拟机、删除已创建的FlexClone卷并卸载临时数据存储区。

7. 选择*保存*。

使用NetApp Disaster Recovery将应用程序复制到另一个站点

使用NetApp Disaster Recovery，您可以使用SnapMirror复制将源站点上的 VMware 应用程序复制到云中的灾难恢复远程站点。



创建灾难恢复计划、在向导中确定重复并启动到灾难恢复站点的复制后，NetApp Disaster Recovery每 30 分钟验证一次复制是否确实按照计划进行。您可以在作业监视器页面中监视进度。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员或灾难恢复故障转移管理员角色。

["了解NetApp Disaster Recovery中的用户角色和权限"](https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html)。https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html["了解所有服务的NetApp Console访问角色"^]。

开始之前

在启动复制之前，您应该创建复制计划并选择复制应用程序。然后，“操作”菜单中会出现“复制”选项。

步骤

1. 登录 **"NetApp Console"**。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从菜单中选择*复制计划*。
4. 选择复制计划。
5. 在右侧，选择“操作”选项 ... 并选择*复制*。

使用NetApp Disaster Recovery将应用程序迁移到另一个站点

使用NetApp Disaster Recovery，您可以将源站点上的 VMware 应用程序迁移到另一个站点。



创建复制计划、在向导中确定重复并启动迁移后，NetApp Disaster Recovery每 30 分钟会验证一次迁移是否确实按照计划进行。您可以在作业监视器页面中监视进度。

开始之前

在启动迁移之前，您应该创建一个复制计划并选择迁移应用程序。然后，“操作”菜单中会出现“迁移”选项。

步骤

1. 登录 **"NetApp Console"**。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从菜单中选择*复制计划*。
4. 选择复制计划。
5. 在右侧，选择“操作”选项 ... 并选择*迁移*。

使用NetApp Disaster Recovery将应用程序故障转移到远程站点

如果发生灾难，请将您的主要本地 VMware 站点故障转移到另一个本地 VMware 站点或 AWS 上的 VMware Cloud。您可以测试故障转移过程以确保在需要时能够成功。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员或灾难恢复故障转移管理员角色。

["了解NetApp Disaster Recovery中的用户角色和权限"](https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html)。https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html["了解所有服务的NetApp Console访问角色"^]。

关于此任务

在故障转移期间，灾难恢复默认使用最新的SnapMirror快照副本，但您可以从某个时间点快照中选择特定的快照（根据SnapMirror的保留策略）。如果最新副本遭到破坏（例如在勒索软件攻击期间），请使用时间点选项。

此过程会有所不同，具体取决于生产站点是否健康以及您是否由于关键基础设施故障以外的原因执行到灾难恢复站点的故障转移：

- 发生严重生产站点故障，导致无法访问源 vCenter 或ONTAP集群： NetApp Disaster Recovery允许您选择任何可用的快照进行恢复。
- 生产环境健康：您可以“立即拍摄快照”或选择之前创建的快照。

此过程会中断复制关系，将 vCenter 源虚拟机置于脱机状态，将卷注册为灾难恢复 vCenter 中的数据存储区，使用计划中的故障转移规则重新启动受保护的虚拟机，并在目标站点上启用读/写功能。

测试故障转移过程

在开始故障转移之前，您可以测试该过程。测试不会使虚拟机脱机。

在故障转移测试期间，灾难恢复功能会临时创建虚拟机。灾难恢复将支持FlexClone卷的临时数据存储映射到 ESXi 主机。

此过程不会占用本地ONTAP存储或 AWS 中NetApp ONTAP存储的 FSx 的额外物理容量。原始源卷不会被修改，即使在灾难恢复期间，副本作业也可以继续进行。

完成测试后，您应该使用*清理测试*选项重置虚拟机。虽然建议这样做，但这不是必需的。

测试故障转移操作不会影响生产工作负载、测试站点上使用的SnapMirror关系以及必须继续正常运行的受保护工作负载。

对于测试故障转移，灾难恢复执行以下操作：

- 对目标集群和SnapMirror关系执行预检查。
- 从选定的快照为目标站点ONTAP集群上的每个受保护的ONTAP卷创建一个新的FlexClone卷。
- 如果任何数据存储都是 VMFS，则创建一个 iGroup 并将其映射到每个 LUN。
- 将目标虚拟机在 vCenter 中注册为新的数据存储区。
- 根据资源组页面中捕获的启动顺序启动目标虚拟机。
- 取消停顿虚拟机中任何被标记为“应用程序一致”的受支持的数据库应用程序。
- 如果源 vCenter 和ONTAP集群仍处于活动状态，请创建反向SnapMirror关系，以将故障转移状态下的任何更改复制回原始源站点。

步骤

1. 登录 "NetApp Console"。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从NetApp Disaster Recovery菜单中，选择 复制计划。
4. 选择复制计划。

5. 在右侧，选择“操作”选项  并选择“测试故障转移”。
6. 在测试故障转移页面中，输入“测试故障转移”并选择“测试故障转移”。
7. 测试完成后，清理测试环境。

故障转移测试后清理测试环境

故障转移测试完成后，您应该清理测试环境。此过程将从测试位置、FlexClone 和临时数据存储区中删除临时虚拟机。

步骤

1. 从 NetApp Disaster Recovery 菜单中，选择 复制计划。
2. 选择复制计划。
3. 在右侧，选择“操作”选项  然后“清理故障转移测试”。
4. 在“测试故障转移”页面中，输入“清理故障转移”，然后选择“清理故障转移测试”。

将源站点故障转移到灾难恢复站点

如果发生灾难，您可以根据需要将主要本地 VMware 站点故障转移到另一个本地 VMware 站点或使用 FSx for NetApp ONTAP 的 AWS 上的 VMware Cloud。

故障转移过程涉及以下操作：

- 灾难恢复对目标集群和 SnapMirror 关系执行预检查。
- 如果您选择了最新的快照，则会执行 SnapMirror 更新以复制最新的更改。
- 源虚拟机已关闭。
- SnapMirror 关系已中断，目标卷变为读/写。
- 根据快照的选择，活动文件系统将恢复到指定的快照（最新或选定）。
- 根据复制计划中捕获的信息创建数据存储并将其安装到 VMware 或 VMC 集群或主机。如果任何数据存储都是 VMFS，则创建一个 iGroup 并将其映射到每个 LUN。
- 目标虚拟机在 vCenter 中注册为新的数据存储区。
- 目标虚拟机根据资源组页面中捕获的启动顺序启动。
- 如果源 vCenter 仍处于活动状态，请关闭所有正在进行故障转移的源端虚拟机。
- 取消暂停虚拟机中任何被标记为“应用程序一致”的受支持的数据库应用程序。
- 如果源 vCenter 和 ONTAP 集群仍处于活动状态，请创建反向 SnapMirror 关系，以便在故障转移状态下将任何更改复制回原始源站点。 SnapMirror 关系从目标虚拟机到源虚拟机是相反的。



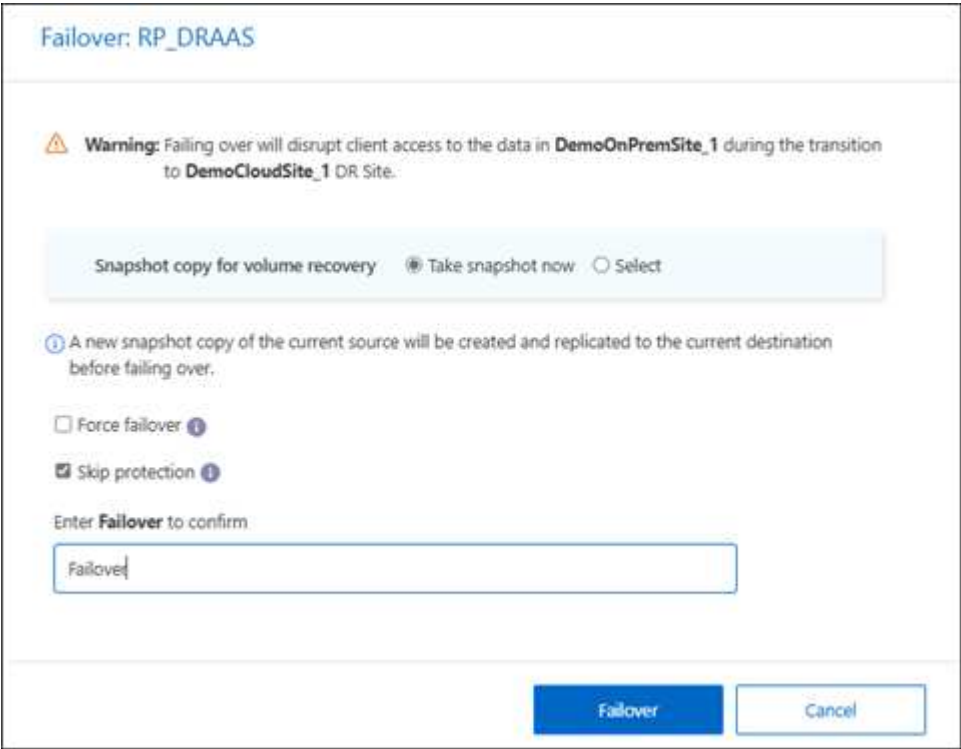
对于基于数据存储的复制计划，如果您已添加并发现了任何虚拟机，但未提供映射详细信息，则这些虚拟机将包含在故障转移中。故障转移失败后，作业中会发出通知。您必须提供映射详细信息才能成功完成故障转移。



故障转移启动后，您可以在灾难恢复站点的 vCenter 中看到恢复的虚拟机（虚拟机、网络和数据存储）。默认情况下，虚拟机会恢复到 Workload 文件夹。

步骤

1. 从NetApp Disaster Recovery菜单中，选择 复制计划。
2. 选择复制计划。
3. 在右侧，选择“操作”选项 ●●● 并选择*故障转移*。



4. 在故障转移页面中，您可以立即创建一个新的快照，或者选择一个现有的快照作为数据存储的恢复基础。默认为最新版本。

在发生故障转移之前，将拍摄当前源的快照并将其复制到当前目标。

5. 或者，如果您希望在检测到通常会阻止故障转移发生的错误时仍进行故障转移，请选择“强制故障转移”。
6. 或者，如果您希望服务在复制计划故障转移后不自动创建反向SnapMirror保护关系，请选择“跳过保护”。如果您希望在NetApp Disaster Recovery中将恢复的站点恢复在线之前对其执行其他操作，这将非常有用。



您可以通过从复制计划操作菜单中选择*保护资源*来建立反向保护。这会尝试为计划中的每个卷创建反向复制关系。您可以重复运行此作业，直到恢复保护。当保护恢复后，您可以按照通常的方式启动故障恢复。

7. 在框中输入“故障转移”。
8. 选择*故障转移*。
9. 要检查进度，请在菜单中选择*作业监控*。

使用NetApp Disaster Recovery将应用程序故障恢复到原始源

灾难解决后，从灾难恢复站点故障回复到源站点以恢复正常运行。您可以选择要恢复的快照。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员或灾难恢复故障转移管理员角色。

"[了解NetApp Disaster Recovery中的用户角色和权限](https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html)"。https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html]"了解所有服务的NetApp Console访问角色"]。

关于故障恢复

在故障恢复过程中，NetApp Disaster Recovery会将所有更改复制（重新同步）回原始源虚拟机，然后再反转复制方向。这个过程始于一段已经完成失败转移至目标的关系，并包括以下步骤：

- 对恢复的站点执行合规性检查。
- 刷新已确定位于恢复站点中的每个 vCenter 群集的 vCenter 信息。
- 在目标站点上，关闭并取消注册虚拟机，然后卸载卷。
- 打破原始源上的SnapMirror关系以使其可读/写。
- 重新同步SnapMirror关系以逆转复制。
- 启动并注册源虚拟机，并在源上挂载卷。

开始之前

如果您使用的是基于数据存储的保护，则已添加到数据存储中的虚拟机可能会在故障转移过程中添加到数据存储中。如果发生这种情况，请确保在启动故障恢复之前提供这些虚拟机的附加映射信息。要编辑资源映射，请参阅"[管理复制计划](#)"。

步骤

1. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
2. 从NetApp Disaster Recovery菜单中，选择 复制计划。
3. 选择复制计划。
4. 在右侧，选择“操作”选项  并选择*故障恢复*。
5. 输入复制计划名称以启动故障恢复。
6. 选择要从中恢复的数据存储的快照。默认是最新的。
7. 要监控作业进度，请在灾难恢复菜单中选择“作业监控”。

使用NetApp Disaster Recovery管理站点、资源组、复制计划、数据存储库和虚拟机信息

NetApp Disaster Recovery提供所有资源的概览和更详细的视角：

- 站点
- 资源组
- 复制计划
- 数据存储库

- 虚拟机

任务需要不同的NetApp Console角色。有关详细信息，请参阅每个任务中的“所需的NetApp Console角色”部分。

"了解NetApp Disaster Recovery中的用户角色和权限"。 <https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html>["了解所有服务的NetApp Console访问角色"]。

管理 vCenter 站点

您可以编辑 vCenter 站点名称和站点类型（本地或 AWS）。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员或灾难恢复管理员角色。

步骤

1. 从菜单中选择*站点*。
2. 选择“操作”选项  在 vCenter 名称右侧，选择“编辑”。
3. 编辑 vCenter 站点名称和位置。

管理资源组

您可以按虚拟机或数据存储创建资源组。它们可以在创建复制计划时添加，也可以在创建复制计划之后添加。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员或灾难恢复应用程序管理员角色。

您可以通过以下方式按数据存储创建资源组：

- 当您使用数据存储区添加资源组时，您可以看到数据存储区的列表。您可以选择一个或多个数据存储来创建资源组。
- 当您创建复制计划并在计划内创建资源组时，您可以在数据存储区中看到虚拟机。

您可以使用资源组执行以下操作：

- 更改资源组名称。
- 将虚拟机添加到资源组。
- 从资源组中删除虚拟机。
- 删除资源组。

有关创建资源组的详细信息，请参阅["创建资源组以将 VM 组织在一起"](#)。

步骤

1. 从菜单中选择*资源组*。
2. 要添加资源组，请选择“添加组”。
3. 您可以通过选择“操作”选项来修改或删除资源组。 。

管理复制计划

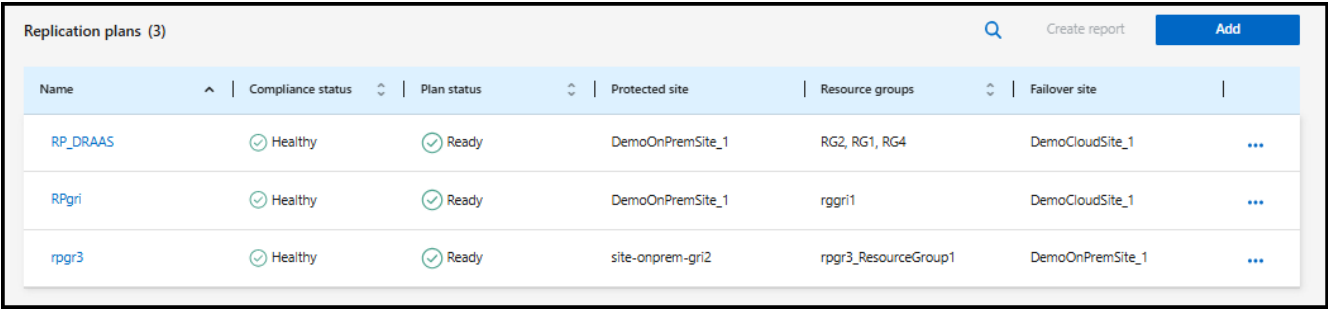
您可以禁用、启用和删除复制计划。您可以更改时间表。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员或灾难恢复应用程序管理员角色。

- 如果您想暂时暂停复制计划，您可以禁用它，然后启用它。
- 如果您不再需要该计划，您可以将其删除。

步骤

1. 从菜单中选择*复制计划*。



Replication plans (3)						Q	Create report	Add
Name	Compliance status	Plan status	Protected site	Resource groups	Failover site			
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1	...		
RPgri	Healthy	Ready	DemoOnPremSite_1	rggri1	DemoCloudSite_1	...		
rpgr3	Healthy	Ready	site-onprem-gri2	rpgr3_ResourceGroup1	DemoOnPremSite_1	...		

2. 要查看计划详情，请选择“操作”选项 并选择*查看计划详情*。
3. 执行以下操作之一：
 - 要编辑计划详情（更改重复），请选择“计划详情”选项卡，然后选择右侧的“编辑”图标。
 - 要编辑资源映射，请选择“故障转移映射”选项卡并选择“编辑”图标。
 - 要添加或编辑虚拟机，请选择“虚拟机”选项卡，然后选择“添加虚拟机”选项或“编辑”图标。
4. 通过选择左侧面包屑中的“复制计划”返回计划列表。
5. 要使用该计划执行操作，请从复制计划列表中选择“操作”选项 在计划右侧，选择任意选项，例如*编辑计划*、测试故障转移、故障转移、故障回复、迁移、立即拍摄快照、清理旧快照、禁用、启用*或*删除*。
6. 要设置或更改测试故障转移计划或设置合规性频率检查，请选择“操作”选项 在计划右侧，选择“编辑时间表”。
 - a. 在“编辑计划”页面中，输入您希望故障转移合规性检查发生的频率（分钟）。
 - b. 检查*按计划运行测试故障转移*。
 - c. 在重复选项中，选择每日、每周或每月的计划。
 - d. 选择*保存*。

按需协调快照

灾难恢复功能每 24 小时自动删除源上的快照。如果发现源和目标之间的快照不同步，则需要解决快照之间的差异，以确保站点之间的一致性。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员或灾难恢复应用程序管理员角色。

步骤

- 1. 从菜单中选择*复制计划*。

Replication plans (3) Q Create report Add

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site	
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1	...
RPgri	Healthy	Ready	DemoOnPremSite_1	rggri1	DemoCloudSite_1	...
rpgr3	Healthy	Ready	site-onprem-gri2	rpgr3_ResourceGroup1	DemoOnPremSite_1	...

- 2. 从复制计划列表中，选择“操作”选项 然后*协调快照*。
- 3. 审查对帐信息。
- 4. 选择*协调*。

删除复制计划

如果删除复制计划，您还可以删除该计划创建的主快照和辅助快照。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员或灾难恢复应用程序管理员角色。

步骤

- 1. 从菜单中选择*复制计划*。
- 2. 选择“操作”选项 在计划右侧，选择“删除”。
- 3. 选择要删除主快照、辅助快照，还是仅删除计划创建的元数据。
- 4. 输入“删除”以确认删除。
- 5. 选择*删除*。

更改故障转移计划的保留计数

更改保留计数可以增加或减少保存的数据存储数量。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员或灾难恢复应用程序管理员角色。

步骤

- 1. 从菜单中选择*复制计划*。
- 2. 选择复制计划，然后选择“故障转移映射”选项卡。选择“编辑”铅笔图标。
- 3. 选择“数据存储”行中的向下箭头将其展开。

1 The selected virtual machines are from different volumes. Once the plan is created, Disaster Recovery will create a consistency group snapshot of the source that spans multiple volumes.

☐ Use platform managed backups and retention schedules

Start taking backups and running retention from 2025-10-22 12 : 00 AM

Take backups and run retention once every 03 Hour(s) 00 Minute(s)

Retention count for all datastores

30

Source datastore

BizAppDatastore (Temp_3510_N1:DR_Prod_Source)

DS_SFO (Temp_3510_N1:DR_SFO)

DS_Testing_Staging (Temp_3510_N1:DR_Vol_Staging)

BizAppDatastore (Temp_3510_N1:DR_Prod_Source)

Target datastore

testDR_Prod_dest

Preferred NFS LIF Select preferred NFS LIF Export policy Select export policy

System SVM Destination volume name

Select a System Select an SVM DR_SFO_dest

Preferred NFS LIF Export policy

Select preferred NFS LIF Select export policy

DS_Testing_Staging (testDR_Vol_Staging_dest) Transfer schedule(RPO) : hourly, asyn

Preferred NFS LIF Export policy

Select preferred NFS LIF Select export policy

testDR_Prod_dest

Preferred NFS LIF Export policy

Select preferred NFS LIF Select export policy

Cancel Save

4. 更改所有数据存储的保留计数值。

5. 选择复制计划后，选择“操作”菜单，然后选择“清理旧快照”以删除目标上的旧快照以匹配新的保留计数。

查看数据存储信息

您可以查看有关源和目标上存在多少个数据存储区的信息。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员、灾难恢复应用程序管理员或灾难恢复查看器角色。

步骤

1. 从菜单中选择*仪表板*。
2. 在站点行中选择 vCenter。
3. 选择*数据存储*。
4. 查看数据存储信息。

查看虚拟机信息

您可以查看源和目标上存在多少个虚拟机以及 CPU、内存和可用容量的信息。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员、灾难恢复应用程序管理员或灾难恢复查看器角色。

步骤

1. 从菜单中选择*仪表板*。
2. 在站点行中选择 vCenter。
3. 选择“虚拟机”。

4. 查看虚拟机信息。

监控NetApp Disaster Recovery作业

您可以监控所有NetApp Disaster Recovery作业并确定其进度。

查看职位

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复应用程序管理员或灾难恢复查看器角色。

"了解NetApp Disaster Recovery中的用户角色和权限"。 <https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html>["了解所有服务的NetApp Console访问角色"^]。

步骤

1. 登录 "NetApp Console"。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从菜单中选择*作业监控*。
4. 探索与操作相关的所有作业并查看其时间戳和状态。
5. 要查看特定作业的详细信息，请选择该行。
6. 要刷新信息，请选择*刷新*。

取消作业

如果某项工作正在进行中或处于排队状态，而您不想让它继续，则可以取消它。如果作业停留在同一状态，您可能想要取消它，并且想要释放队列中的下一个操作。您可能想在作业超时之前取消它。

所需的**NetApp Console**角色 组织管理员、文件夹或项目管理员、灾难恢复管理员、灾难恢复故障转移管理员或灾难恢复应用程序管理员角色。

"了解NetApp Disaster Recovery中的用户角色和权限"。 <https://docs.netapp.com/us-en/console-setup-admin/reference-iam-predefined-roles.html>["了解所有服务的NetApp Console访问角色"^]。

步骤

1. 从NetApp Console左侧导航栏中，选择 保护 > 灾难恢复。
2. 从菜单中选择*作业监控*。
3. 在“作业监视器”页面中，记下要取消的作业的 ID。

该作业必须处于“进行中”或“排队”状态。

4. 在“操作”列中，选择“取消作业”。

创建NetApp Disaster Recovery报告

查看NetApp Disaster Recovery报告可以帮助您分析灾难恢复准备情况。预先设计的报告

包括过去七天帐户内所有站点的测试故障转移摘要、复制计划详细信息和作业详细信息。

您可以下载 PDF、HTML 或 JSON 格式的报告。

下载链接有效期为六小时。

步骤

1. 登录 ["NetApp Console"](#)。
2. 从NetApp Console左侧导航中，选择 保护 > 灾难恢复。
3. 从NetApp Console左侧导航栏中，选择 复制计划。
4. 选择*创建报告*。
5. 选择文件格式类型和过去 7 天内的时间段。
6. 选择“创建”。



该报告可能需要几分钟才能显示。

7. 要下载报告，请选择*下载报告*并在管理员的下载文件夹中选择它。

参考

用于 NetApp Disaster Recovery 的必需 vCenter 权限

要使 NetApp Disaster Recovery 执行其服务，vCenter 帐户必须具有最低的 vCenter 权限集。这些权限包括注册和注销数据存储区、启动和停止虚拟机 (VM) 以及重新配置 VM。

下表列出了 Disaster Recovery 与 vCenter 集群接口所需的所有权限。

类型	权限名称 (vSphere 客户端)	权限名称 (API)	描述
数据存储库	Datastore.Config	配置数据存储库	允许配置数据存储库。
	Datastore.Delete	删除数据存储库	允许删除数据存储库。
	Datastore.Rename	重命名数据存储库	允许重命名数据存储库。
文件夹	文件夹.创建	创建文件夹	允许创建新文件夹。
	文件夹.删除	删除文件夹	允许删除文件夹。需要对象及其父级上的权限。
	文件夹重命名	重命名文件夹	允许修改文件夹名称。
网络	网络分配	分配网络	允许将网络分配给 VM。
	Network.Config	配置	允许配置网络。
虚拟机配置	VirtualMachine.Config.AdvancedConfig	高级配置	允许在虚拟机的配置文件中添加或修改高级参数。
	VirtualMachine.Config.Settings	更改设置	允许更改常规 VM 设置。
	VirtualMachine.Config.CPUCount	更改 CPU 计数	允许更改虚拟 CPU 数量。
	VirtualMachine.Config.Memory	更改内存	允许更改分配给 VM 的内存量。
	VirtualMachine.Config.Resource	更改资源	允许更改资源池中 VM 节点的资源配置。
	VirtualMachine.Config.Rename	重命名	允许重命名 VM 或修改其注释。
	VirtualMachine.Config.EditDevice	修改设备设置	允许更改现有设备的属性。
	VirtualMachine.Config.ReloadFromPath	从路径重新加载	允许在保留标识的同时更改 VM 配置路径。
	VirtualMachine.Config.ResetGuestInfo	重置访客信息	允许编辑 VM 的来宾操作系统信息。

类型	权限名称 (vSphere 客户端)	权限名称 (API)	描述
虚拟机来宾	VirtualMachine.GuestOperations.ModifyAliases	来宾操作别名修改	允许修改 VM 的别名。
	VirtualMachine.GuestOperations.QueryAliases	来宾操作别名查询	允许查询 VM 的别名。
	VirtualMachine.GuestOperations.Modify	子系统操作修改	允许修改操作，包括将文件传输至 VM。
	VirtualMachine.GuestOperations.Execute	访客操作程序执行	允许在 VM 内运行应用程序。
	VirtualMachine.GuestOperations.Query	来宾操作查询	允许查询客户机操作系统。操作包括列出文件。
虚拟机交互	VirtualMachine.Interact.AnswerQuestion	回答问题	允许解决虚拟机状态转换或运行时错误期间的问题。
	VirtualMachine.Interact.PowerOff	关闭	允许关闭已通电的 VM。
	VirtualMachine.Interact.PowerOn	启动	允许打开或恢复 VM。
	VirtualMachine.交互.ToolsInstall	VMware Tools 安装	允许装载/卸载 VMware Tools 安装程序。
	VirtualMachine.清单.CreateFromExisting	基于现有清单创建	允许从模板克隆或部署 VM。
	VirtualMachine.清单.创建	新建	允许创建 VM 并分配资源。
	VirtualMachine.清单.注册	注册	允许将现有 VM 添加到库存。
	VirtualMachine.Inventory.Delete	删除	允许删除虚拟机及其文件。需要对象及其父级上的权限。
	VirtualMachine.Inventory.Unregister	注销	允许注销虚拟机。此权限需要对象及其父级上的权限。
虚拟机配置	VirtualMachine.配置.克隆	克隆虚拟机	允许克隆 VM 并分配资源。
	VirtualMachine.配置.自定义	自定义来宾	允许自定义 VM 的来宾操作系统。
	VirtualMachine.配置.ModifyCustSpecs	修改自定义规范	允许创建、修改或删除自定义规范。
	VirtualMachine 配置 ReadCustSpecs	读取自定义规范	允许读取虚拟机的自定义规范。
虚拟机服务配置	VirtualMachine.Namespace.Query	查询服务配置	允许检索 VM 服务列表。
	VirtualMachine.命名空间.ReadContent	读取服务配置	允许检索现有 VM 服务配置。

类型	权限名称 (vSphere 客户端)	权限名称 (API)	描述
虚拟机快照	VirtualMachine 状态。CreateSnapshot	创建 Snapshot	允许从 VM 的当前状态创建快照。
	VirtualMachine 状态。RemoveSnapshot	删除快照	允许删除快照。
	VirtualMachine 状态。RenameSnapshot	重命名 snapshot	允许重命名快照或更新其描述。
	VirtualMachine.State.RevertToSnapshot	还原为快照	允许将虚拟机恢复到给定快照的状态。

使用NetApp Disaster Recovery时切换控制台代理

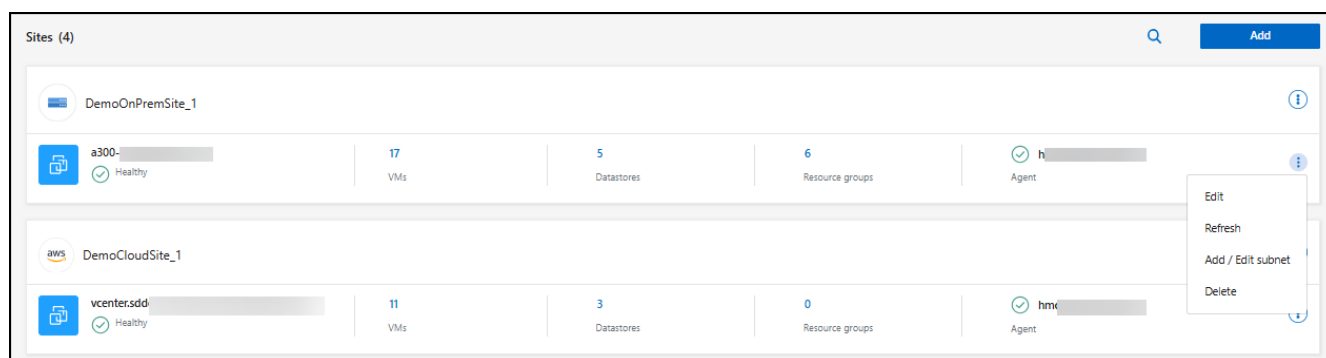
NetApp Console支持在单个工作环境中使用多个控制台代理。使用多个控制台代理有助于在对另一个控制台代理进行维护或控制台代理发生故障时保持对资源的访问。由于每个控制台代理都有一个唯一的标识符，因此不正确地切换控制台代理可能会影响工作环境中资源的可用性。

开始之前

- 您必须有[为您的工作环境至少添加了两个控制台代理](#)。
- 两个控制台代理必须包含相同的ONTAP集群。

步骤

1. 在灾难恢复中，选择站点。
2. 您必须更改源 vCenter 和目标 vCenter 的控制台代理。确定要修改的 vCenter。选择 vCenter 的操作菜单，然后选择编辑。



3. 从下拉菜单中选择要使用的控制台代理，然后重新输入您的 vCenter 用户名和密码。选择保存。

Enter connection details for the vCenter server that is accessible from the Console Agent.

Site	Console Agent
DemoOnPremSite_1	hmcdrasconnector4
vCenter IP address	ShivaOnPremConnDemo hmcdrasconnector4 DRaaSTest
a300-vcsa06.ehcdc.com	
vCenter user name	vCenter password
☒ Use self-signed certificates ⓘ	
☐ Enable scheduled discovery	

Save

Cancel

4. 对要修改的每个其他 vCenter 重复步骤 2 和 3。
5. 在您修改过的 vCenter 中，刷新 vCenter 以发现新的控制台代理。对每个已修改的 vCenter 重复此步骤。
6. 在灾难恢复中，导航至复制计划。
7. 确定要用于恢复工作流的复制计划。选择操作菜单 `...` 然后刷新资源。您可以在“作业监控”中监控作业状态。

更多信息

- ["了解控制台代理"](#)

将NetApp Disaster Recovery与 Amazon EVS 结合使用

使用 Amazon Elastic VMware Service 和Amazon FSx for NetApp ONTAP实现NetApp Disaster Recovery

客户越来越依赖虚拟化基础架构来处理生产计算工作负载，例如基于 VMware vSphere 的工作负载。由于这些虚拟机 (VM) 对业务变得越来越重要，客户需要保护这些 VM 免受与物理计算资源相同类型的灾难的影响。目前提供的灾难恢复 (DR) 解决方案复杂、昂贵且

资源密集。NetApp是用于虚拟化基础架构的最大存储提供商，它有既得利益确保其客户的虚拟机受到保护，就像我们保护任何类型的ONTAP存储托管数据一样。为了实现这一目标，NetApp创建了NetApp Disaster Recovery服务。

任何 DR 解决方案面临的主要挑战之一是管理购买、配置和维护额外计算、网络 and 存储资源的增量成本，以提供 DR 复制和恢复基础设施。保护关键内部虚拟资源的一个流行选择是使用云托管虚拟资源作为 DR 复制和恢复基础设施。亚马逊就是此类解决方案的一个例子，它可以提供与NetApp ONTAP托管 VM 基础架构兼容的经济高效的资源。

亚马逊推出了 Amazon Elastic VMware Service (Amazon EVS)，可在您的虚拟私有云 (VPC) 内支持 VMware Cloud Foundation。Amazon EVS 提供 AWS 的弹性和性能以及熟悉的 VMware 软件和工具，使 Amazon EVS vCenters 能够作为本地虚拟化基础设施的扩展进行集成。

虽然 Amazon EVS 附带了存储资源，但对于存储工作负载繁重的组织来说，使用本机存储可能会降低其效率。在这些情况下，将 Amazon EVS 与 Amazon FSx for NetApp ONTAP 存储 (Amazon FSxN) 结合使用可以提供更灵活的存储解决方案。此外，当您在本地使用 NetApp ONTAP 存储解决方案来托管您的 VMware 基础架构时，使用带有 FSx for ONTAP 的 Amazon EVS 意味着您可以在本地和云托管基础架构之间获得一流的数据互操作性和保护功能。

有关 Amazon FSx for NetApp ONTAP 的信息，请参阅 ["Amazon FSx for NetApp ONTAP 入门"](#)。

使用 **Amazon EVS** 和 **Amazon FS for NetApp ONTAP** 的 **NetApp Disaster Recovery** 解决方案概述

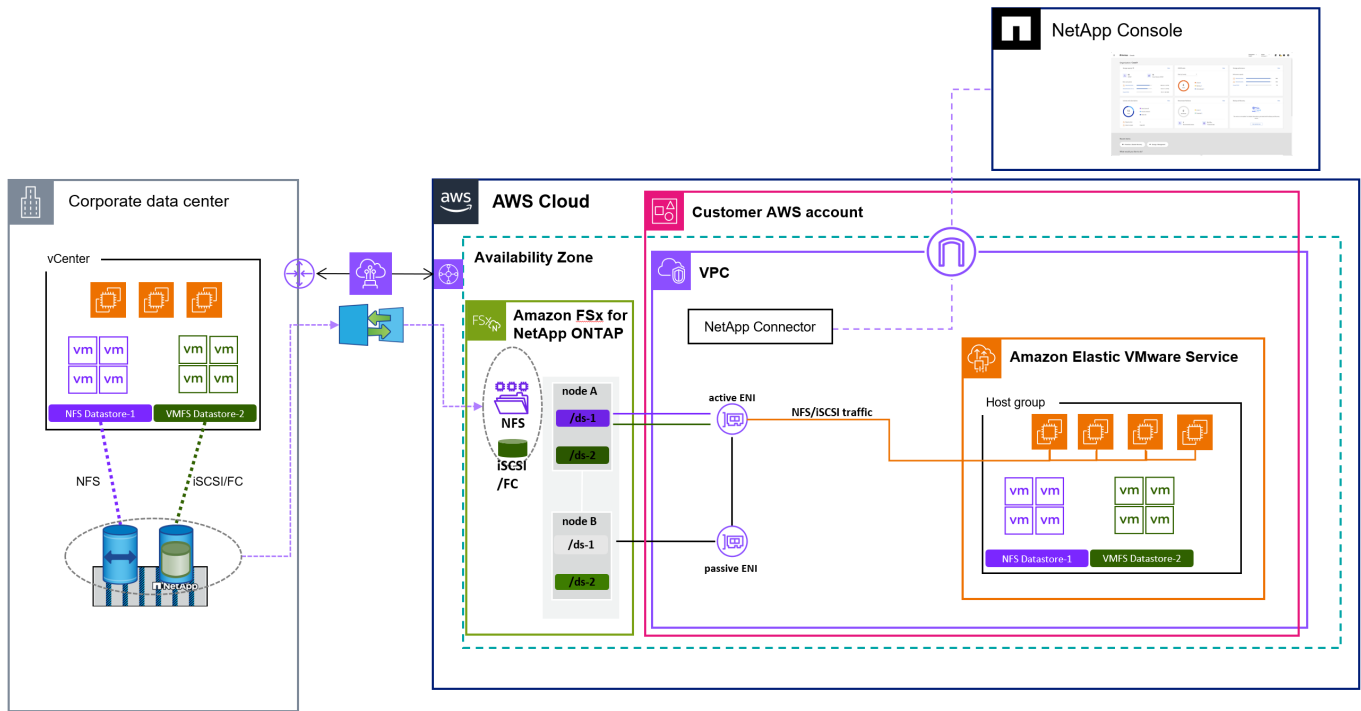
NetApp Disaster Recovery 是托管在 NetApp Console 软件即服务环境中的增值服务，它依赖于核心 NetApp Console 架构。控制台内用于 VMware 保护的 DR 服务由几个主要组件组成。

有关 NetApp Disaster Recovery 解决方案的完整概述，请参阅 ["了解 NetApp Disaster Recovery"](#)。

如果您想要将本地 VMware 托管的虚拟机保护到 Amazon AWS，请使用该服务通过 Amazon FSx for NetApp ONTAP 存储托管数据存储在 Amazon EVS。

下图显示了该服务如何使用 Amazon EVS 保护您的虚拟机。

使用 Amazon EVS 和 FSx for ONTAP 进行 NetApp Disaster Recovery 概述



1. Amazon EVS 部署在您的帐户中的单个可用区 (AZ) 配置中以及您的虚拟私有云 (VPC) 内。
2. FSx for ONTAP文件系统与 Amazon EVS 部署在同一 AZ 中。文件系统通过弹性网络接口 (ENI)、VPC 对等连接或 AmazonTransit 网关直接连接到 Amazon EVS。
3. NetApp Console代理已安装在您的 VPC 中。NetApp Console代理托管多个数据管理服务（称为代理），包括管理本地物理数据中心和 Amazon AWS 托管资源上的 VMware 基础架构的 DR 的NetApp Disaster Recovery代理。
4. NetApp Disaster Recovery代理与NetApp Console云托管服务安全通信以接收任务并将这些任务分发到适当的内部部署和 AWS 托管的 vCenter 和ONTAP存储实例。
5. 您可以使用NetApp Console云托管 UI 控制台创建复制计划，指示应保护的虚拟机、应保护这些虚拟机的频率，以及在从内部站点发生故障转移时重新启动这些虚拟机所需执行的程序。
6. 复制计划确定哪些 vCenter 数据存储库托管受保护的虚拟机以及托管这些数据存储库的ONTAP卷。如果 FSx for ONTAP集群上尚不存在卷， NetApp Disaster Recovery会自动创建它们。
7. 为每个已识别的源ONTAP卷与每个目标 FSx for ONTAP托管ONTAP卷创建SnapMirror关系，并根据复制计划中用户提供的 RPO 创建复制计划。
8. 如果主站点发生故障，管理员会在NetApp Console内启动手动故障转移过程，并选择备份作为还原点。
9. NetApp Disaster Recovery代理激活 FSx for ONTAP托管的数据保护卷。
10. 该代理向 Amazon EVS vCenter 注册每个已激活的 FSx for ONTAP卷，向 Amazon EVS vCenter 注册每个受保护的虚拟机，并根据复制计划中包含的预定义规则启动每个虚拟机。

安装用于NetApp Disaster Recovery的NetApp Console代理

NetApp Console 代理使您能够将 NetApp Console 部署连接到基础架构，以便在 AWS、Azure、Google Cloud 或本地环境中安全地编排解决方案。Console 代理执行 NetApp Console 需要执行的操作，以管理您的数据基础架构。Console 代理会不断轮询 NetApp Disaster Recovery 软件作为服务层，以了解需要采取的任何操作。

对于 NetApp Disaster Recovery，执行的操作使用每个相应服务的本机 API 来协调 VMware vCenter 群集和 ONTAP 存储实例，以便为在本地位置运行的生产虚拟机提供保护。虽然可以在任何网络位置安装 Console 代理，但建议您在灾难恢复站点中安装 Console 代理以进行 NetApp Disaster Recovery。在 DR 站点中安装可确保在主站点发生故障时，NetApp 控制台 UI 保持与 Console 代理的连接，并可以在该 DR 站点中协调恢复过程。

安装

- 要使用 Disaster Recovery，请在标准模式下安装 Console 代理。要了解有关 Console 代理安装类型的更多信息，请访问 ["了解 NetApp Console 部署模式"](#)。

Console 代理的具体安装步骤取决于您的部署类型。有关详细信息，请参见 ["了解控制台代理"](#)。



使用 Amazon AWS 安装 Console 代理的最简单方法是使用 AWS Marketplace。有关使用 AWS Marketplace 安装 Console 代理的详细信息，请参阅 ["从 AWS Marketplace 创建 Console 代理"](#)。

为 Amazon EVS 配置 NetApp Disaster Recovery

为 Amazon EVS 配置 NetApp Disaster Recovery 概述

安装 NetApp Console 代理后，您需要将参与灾难恢复过程的所有 ONTAP 存储和 VMware vCenter 资源与 NetApp Disaster Recovery。

- ["Amazon EVS 与 NetApp Disaster Recovery 的先决条件"](#)
- ["将 ONTAP 存储阵列添加到 NetApp Disaster Recovery"](#)
- ["为 Amazon EVS 启用 NetApp Disaster Recovery"](#)
- ["将 vCenter 站点添加到 NetApp Disaster Recovery"](#)
- ["将 vCenter 集群添加到 NetApp Disaster Recovery"](#)

Amazon EVS 与 NetApp Disaster Recovery 的先决条件

确保您查看并满足使用 NetApp Disaster Recovery 配置 Amazon EVS 的要求。

前提条件

- 请查看 ["灾难恢复的一般先决条件"](#)。
- 创建一个 vCenter 用户帐户，该帐户具有 NetApp Disaster Recovery 所需的特定 VMware 权限，以执行必要的操作。



建议您不要使用默认的“administrator@vsphere.com”管理员账户。相反，您应在所有将参与灾难恢复流程的 vCenter 集群上创建一个专用于 NetApp Disaster Recovery 的用户账户。有关所需具体权限列表，请参见 ["NetApp Disaster Recovery 所需的 vCenter 权限"](#)。

- 确保将承载受 Disaster Recovery 保护的虚拟机的所有 vCenter 数据存储区都位于 NetApp ONTAP 存储资源上。

在使用 Amazon FSx for NetApp ONTAP 时，Disaster Recovery 支持 NFS 和基于 iSCSI（而非 FC）的 VMFS。虽然 Disaster Recovery 支持 FC，但 Amazon FSx for NetApp ONTAP 不支持。

- 确保您的 Amazon EVS vCenter 已连接到 Amazon FSx for NetApp ONTAP 存储集群。
- 确保在所有受保护的虚拟机上安装 VMware 工具。
- 确保使用 Amazon 批准的连接方法将您的本地网络连接到 AWS VPC 网络。建议您使用 AWS Direct Connect、AWS Private Link 或 AWS Site-to-Site VPN。
- 检查并确保符合具有 Disaster Recovery 功能的 EVS 的连接和端口要求：

源	目标	端口	详细信息
Amazon FSxN	本地 ONTAP	TCP 11104、11105 、ICMP	SnapMirror
本地 ONTAP	Amazon FSxN	TCP 11104、11105 、ICMP	SnapMirror
NetApp Console 代理	本地 ONTAP	TCP 443，仅 ICMP	API 调用
NetApp Console 代理	Amazon FSxN	TCP 441，仅 ICMP	API 调用
NetApp Console 代理	vCenter（本地、EVS ）、ESXi 主机（本 地、EVS）	443	API 调用、脚本执行

使用**NetApp Disaster Recovery**功能将本地阵列添加到适用于 **Amazon EVS** 的**NetApp Console**系统

在使用**NetApp Disaster Recovery**之前，您必须将内部部署和云托管存储实例添加到**NetApp Console**系统。

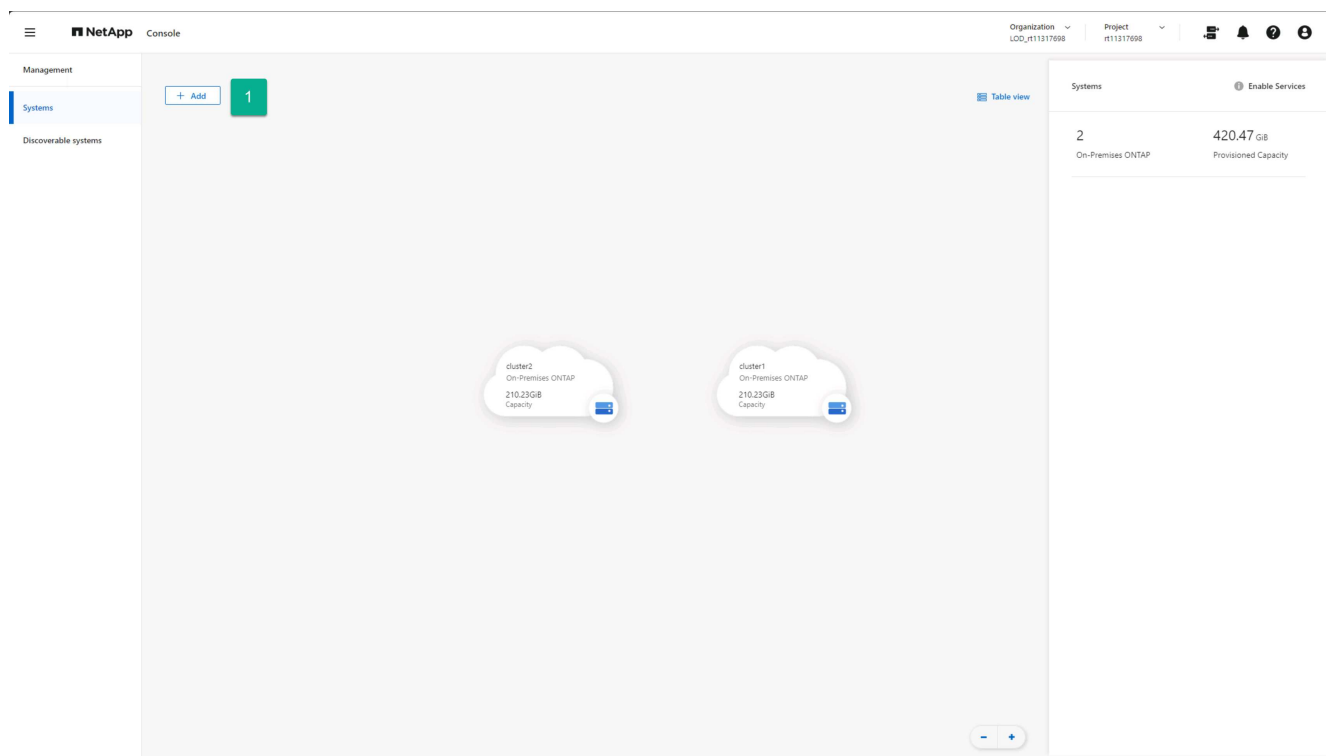
您需要执行以下操作：

- 将内部部署阵列添加到您的**NetApp Console**系统。
- 将Amazon FSx for NetApp ONTAP（FSx for ONTAP）实例添加到您的**NetApp Console**系统。

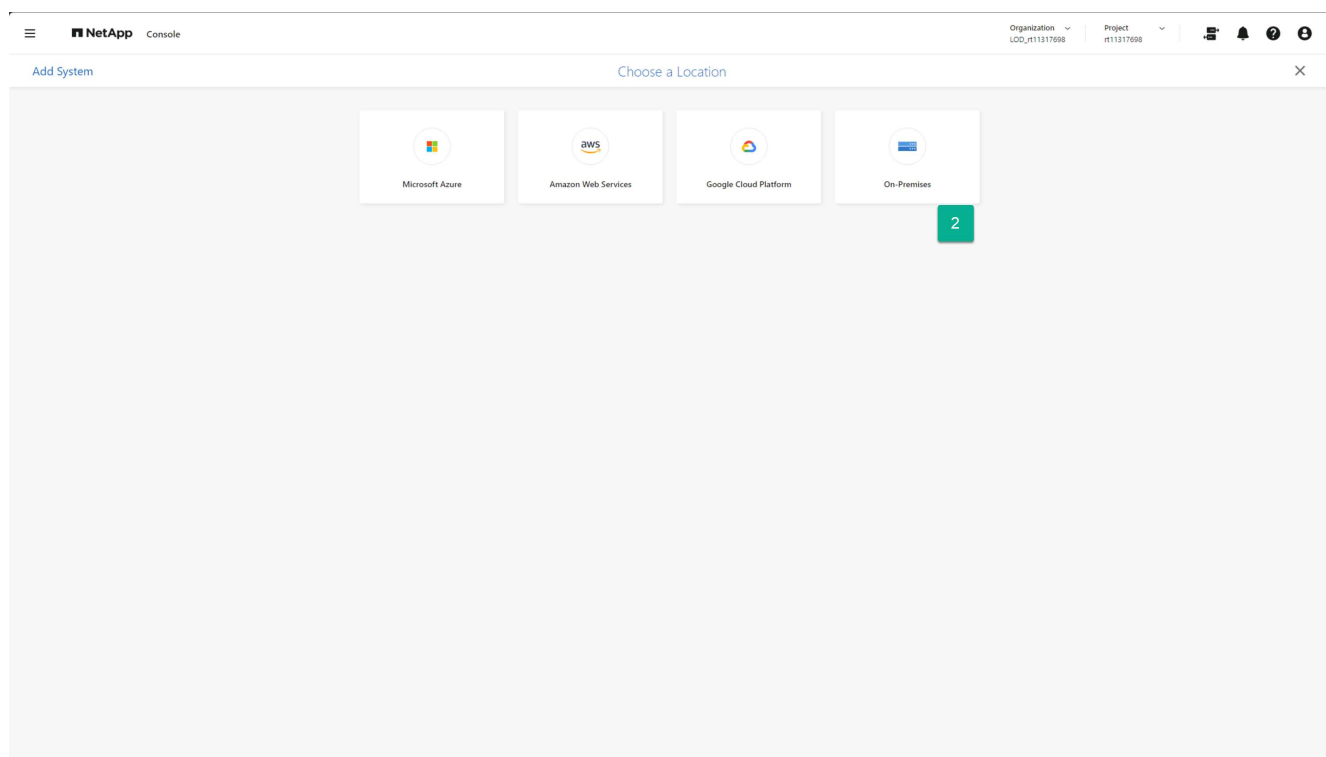
将本地存储阵列添加到**NetApp Console**系统

将本地ONTAP存储资源添加到您的**NetApp Console**系统。

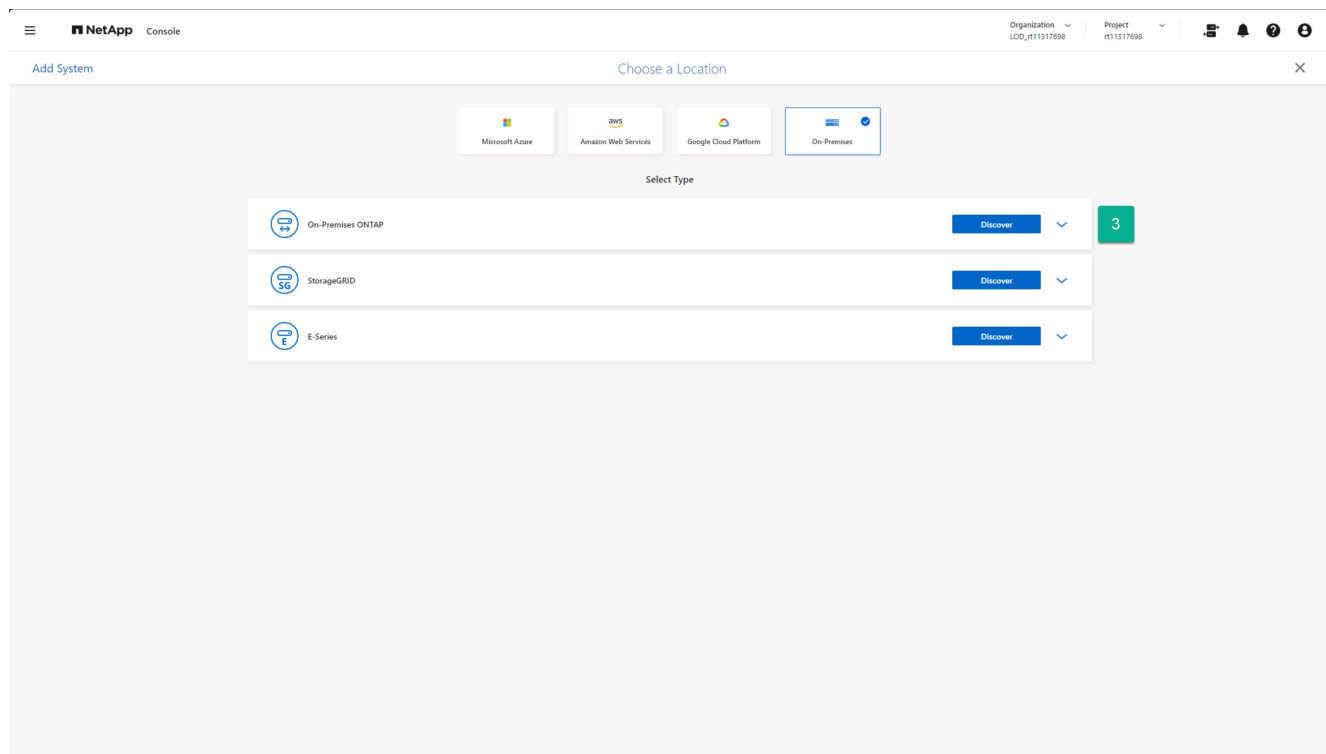
1. 在**NetApp Console**系统页面中，选择“添加系统”。



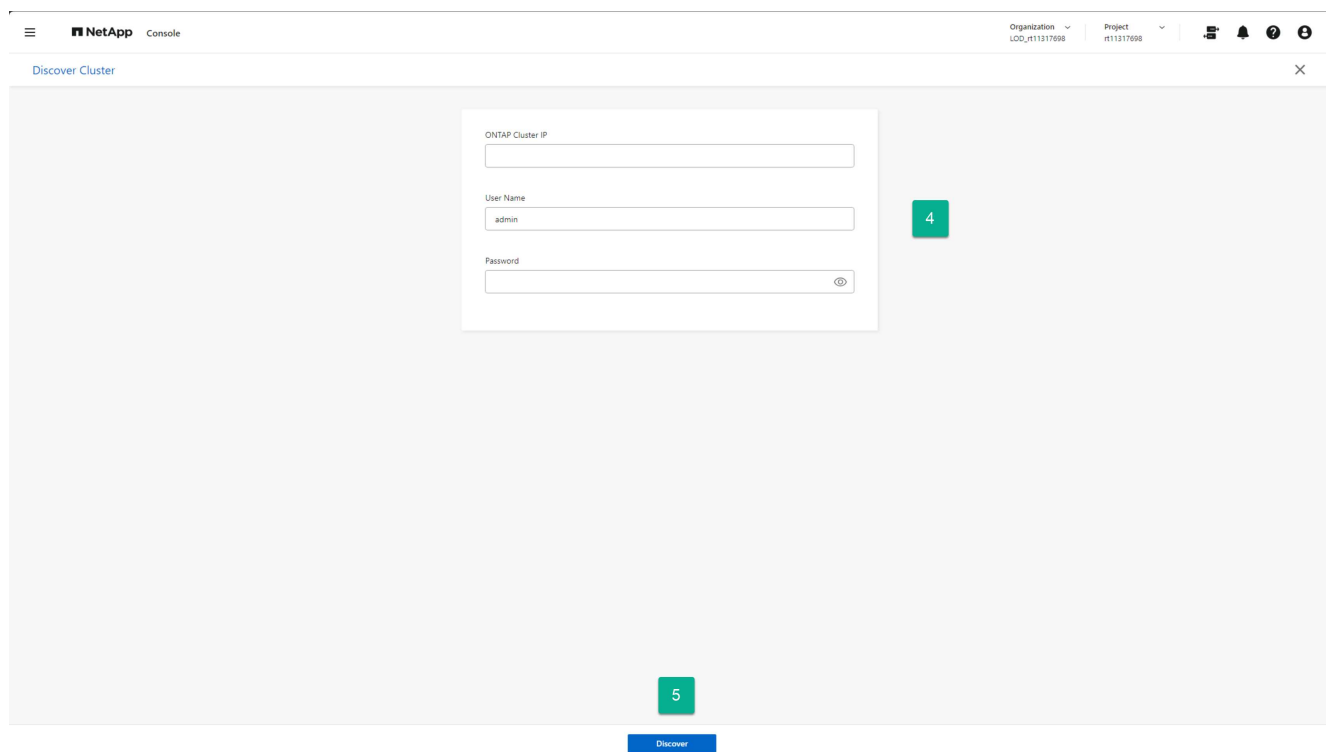
2. 在添加系统页面中，选择*On-Premises*卡。



3. 在 On-Premises ONTAP卡上选择 发现。



4. 在发现集群页面上，输入以下信息：
 - a. ONTAP阵列集群管理端口的 IP 地址
 - b. 管理员用户名
 - c. 管理员密码
5. 选择页面底部的“发现”。

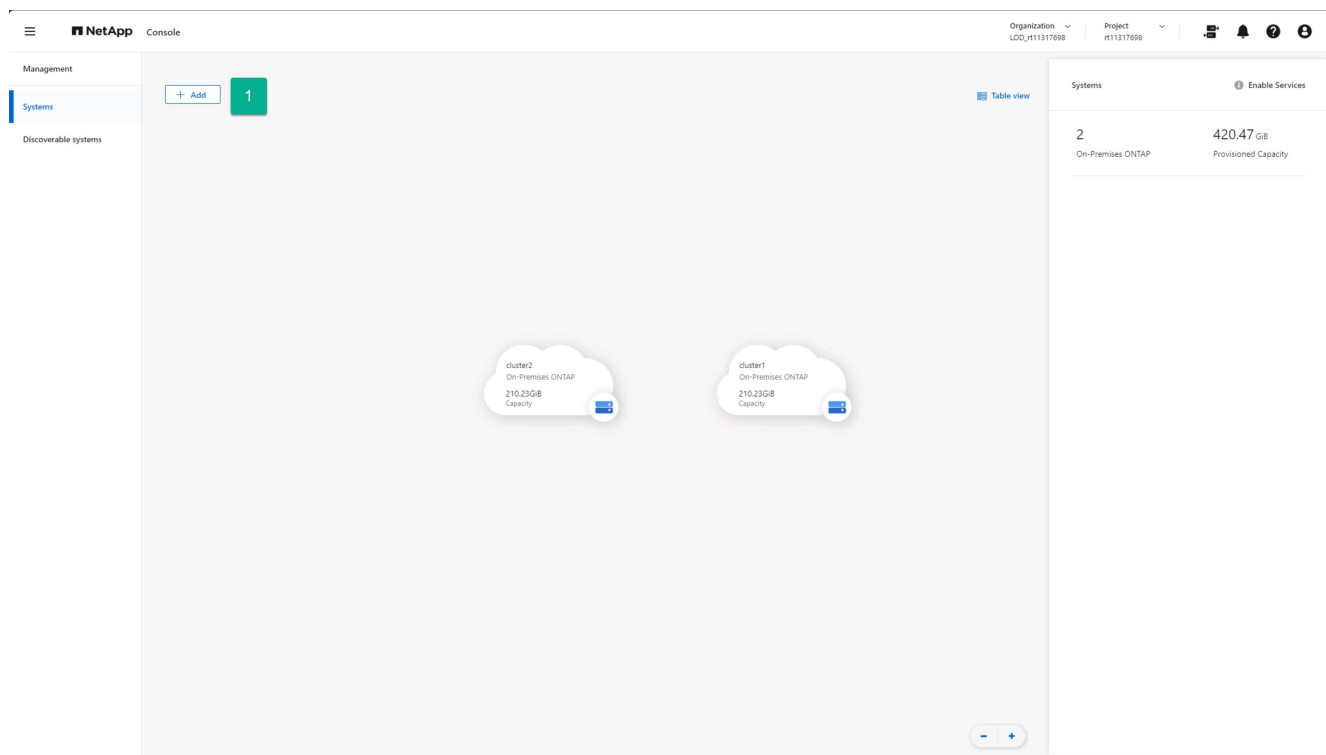


6. 对将托管 vCenter 数据存储区的每个ONTAP阵列重复步骤 1-5。

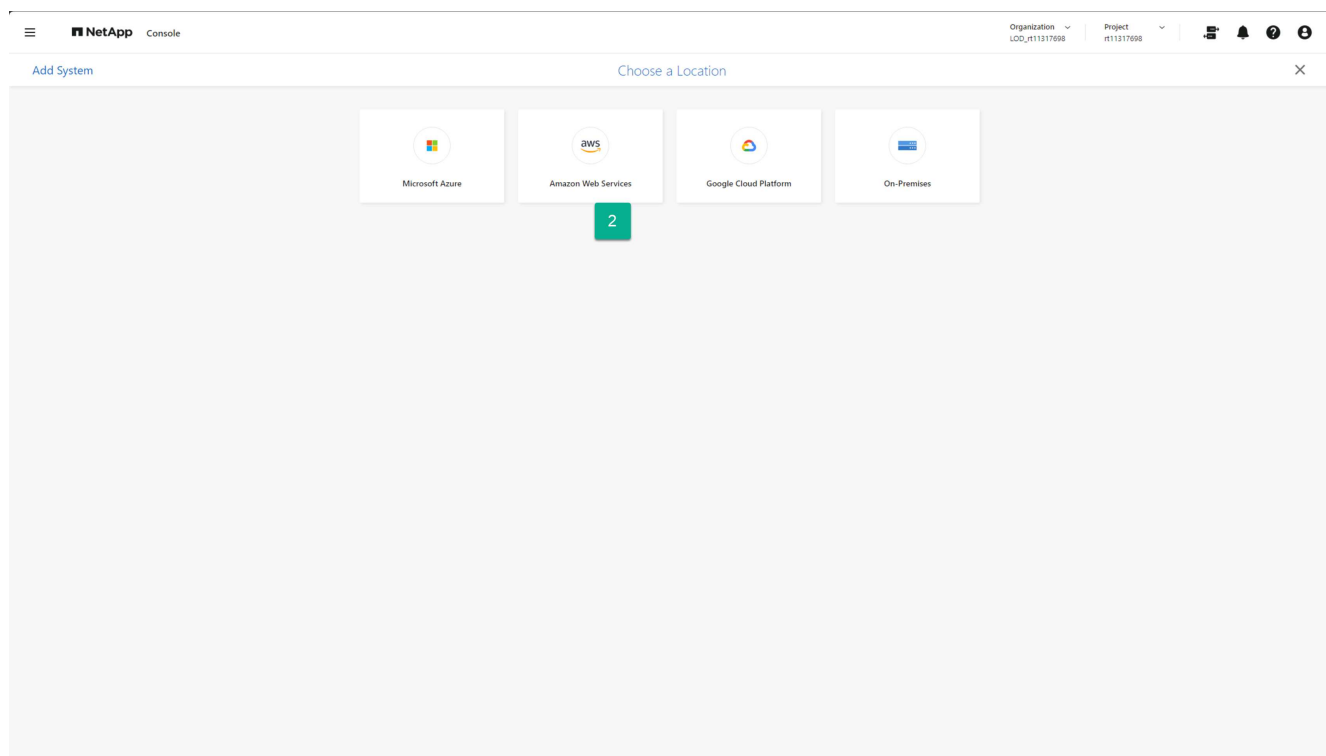
将**Amazon FSx for NetApp ONTAP**存储实例添加到**NetApp Console**系统

接下来，将Amazon FSx for NetApp ONTAP存储资源添加到您的NetApp Console系统。

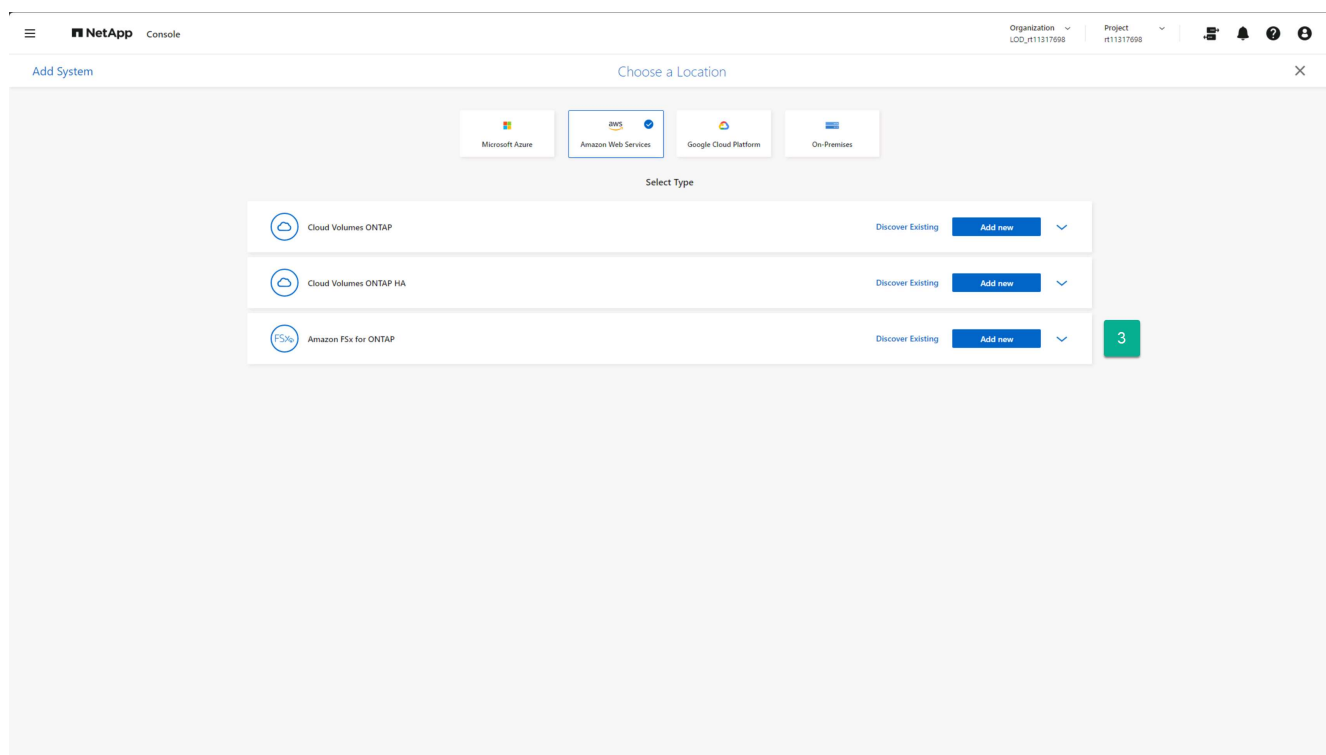
1. 在NetApp Console系统页面中，选择“添加系统”。



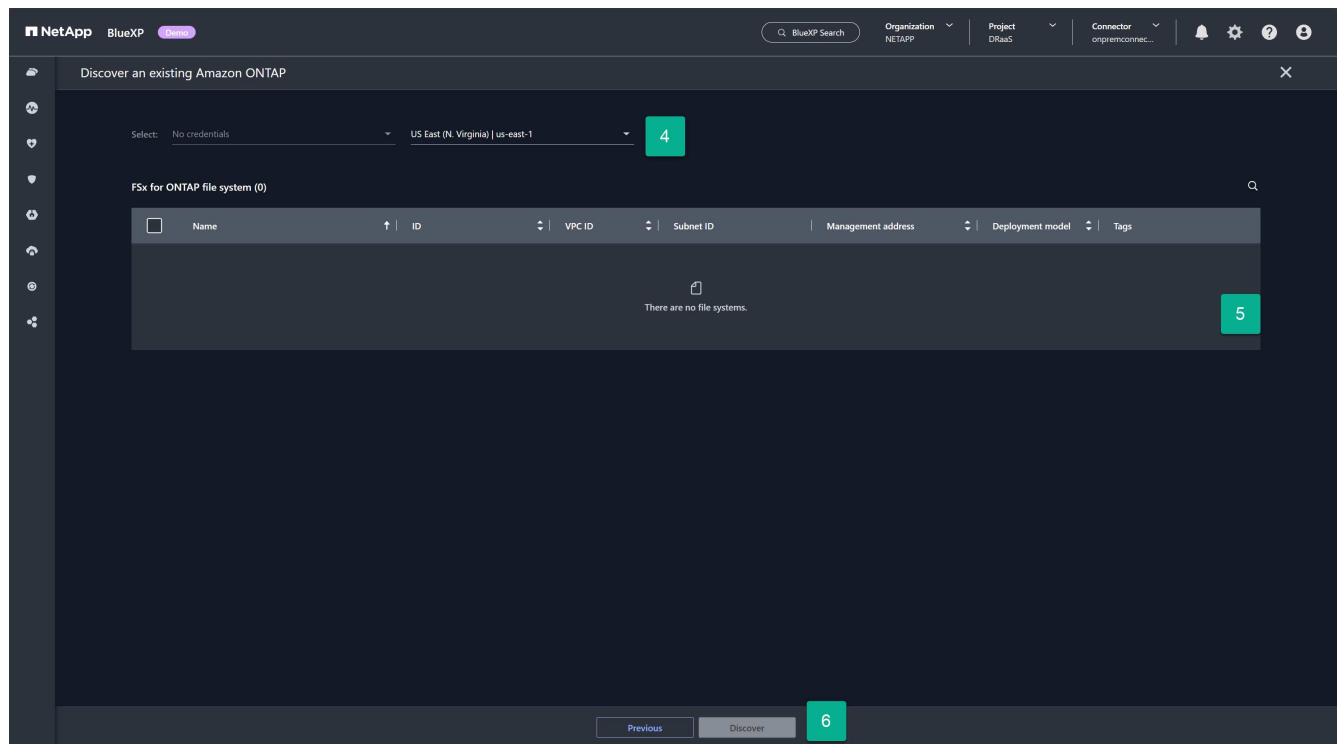
2. 从添加系统页面中，选择*Amazon Web Services*卡。



3. 选择Amazon FSx for ONTAP卡上的 **Discover Existing** 链接。



4. 选择托管 FSx for ONTAP实例的凭证和 AWS 区域。
5. 选择一个或多个要添加的 FSx for ONTAP文件系统。
6. 选择页面底部的“发现”。



7. 对于将托管 vCenter 数据存储区的每个 FSx for ONTAP实例重复步骤 1-6。

将**NetApp Disaster Recovery**服务添加到您的 **Amazon EVS NetApp Console**帐户

NetApp Disaster Recovery是一种许可产品，必须先购买才能使用。有多种类型的许可证，并且您可以通过多种方式购买许可证。许可证授权您在特定时间段内保护特定数量的数据。

有关NetApp Disaster Recovery许可证的更多信息，请参阅["设置NetApp Disaster Recovery许可"](#)。

许可证类型

有两种主要的许可证类型：

- NetApp提供["30天试用许可证"](#)您可以使用它来评估使用ONTAP和 VMware 资源的NetApp Disaster Recovery。此许可证提供 30 天的使用期限，不受限制地使用受保护的容量。
- 如果您希望在 30 天试用期之后获得 DR 保护，请购买生产许可证。您可以通过任何 NetApp 云合作伙伴的市场购买此许可证，但对于本指南，我们建议您使用 Amazon AWS Marketplace 购买NetApp Disaster Recovery的市场许可证。要了解有关通过 Amazon Marketplace 购买许可证的更多信息，请参阅["通过 AWS Marketplace 订阅"](#)。

确定灾难恢复容量需求

在购买许可证之前，您应该了解需要保护多少ONTAP存储容量。使用NetApp ONTAP存储的优势之一是NetApp存储数据的效率很高。ONTAP卷中存储的所有数据（例如托管虚拟机的 VMware 数据存储区）都是以高效的方式存储的数据。ONTAP在将数据写入物理存储时默认采用三种存储效率：压缩、重复数据删除和压缩。最终结果是存储效率在 1.5:1 到 4:1 之间，具体取决于所存储的数据类型。事实上，NetApp提供了 ["存储效率保证"](#)对于某些工作负载。

这对您有利，因为在应用所有ONTAP存储效率之后，NetApp Disaster Recovery会计算许可容量。例如，假设

您在 vCenter 中配置了一个 100 TB (TiB) NFS 数据存储区来托管您想要使用该服务保护的 100 台虚拟机。此外，假设当数据写入ONTAP卷时，自动应用的存储效率技术会导致这些虚拟机仅消耗 33TiB（3：1 的存储效率）。NetApp Disaster Recovery仅需要获得 33TiB 的许可，而不是 100TiB。与其他 DR 解决方案相比，这对于您的 DR 解决方案的总体拥有成本来说是一个非常大的好处。

步骤

1. 要确定托管要保护的 VMware 数据存储库的每个卷上消耗的数据量，请通过对每个卷运行ONTAP CLI 命令来确定磁盘容量消耗：`volume show-space -volume < volume name > -vserver < SVM name >`。

例如：

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                Used      Used%
-----
User Data                             163.4MB    3%
Filesystem Metadata                   172KB     0%
Inodes                               2.93MB    0%
Snapshot Reserve                     292.9MB    5%
Total Metadata                       185KB     0%
Total Used                           459.4MB    8%
Total Physical Used                  166.4MB    3%
```

2. 注意每个卷的“总物理使用量”值。这是NetApp Disaster Recovery需要保护的数据量，也是您将用来确定需要许可多少容量的值。

在NetApp Disaster Recovery中为 Amazon EVS 添加站点

在保护虚拟机基础架构之前，请确定哪些 VMware vCenter 群集托管着要保护的虚拟机以及这些 vCenter 位于何处。第一步是创建一个站点来代表源数据中心和目标数据中心。站点是故障域或恢复域。

您需要创建以下内容：

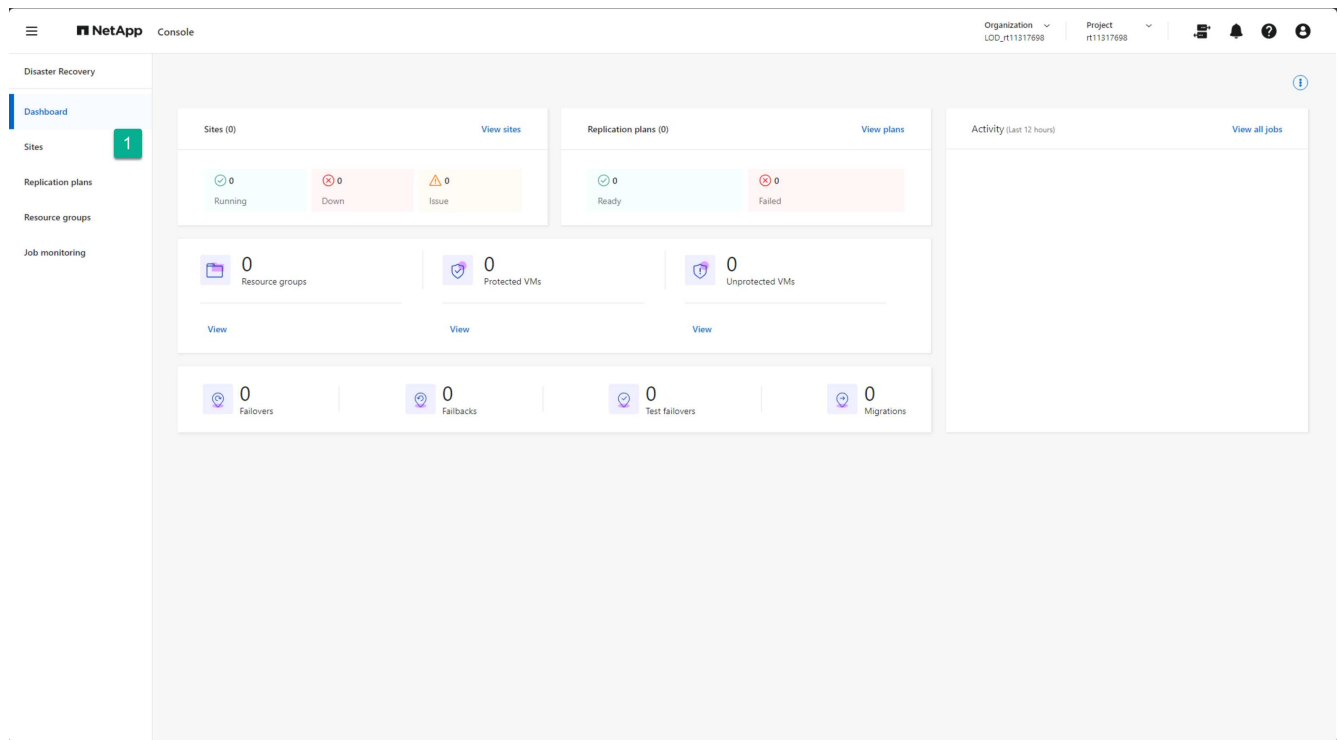
- 代表生产 vCenter 集群所在的每个生产数据中心的站点
- Amazon FSx for NetApp ONTAP站点

创建本地站点

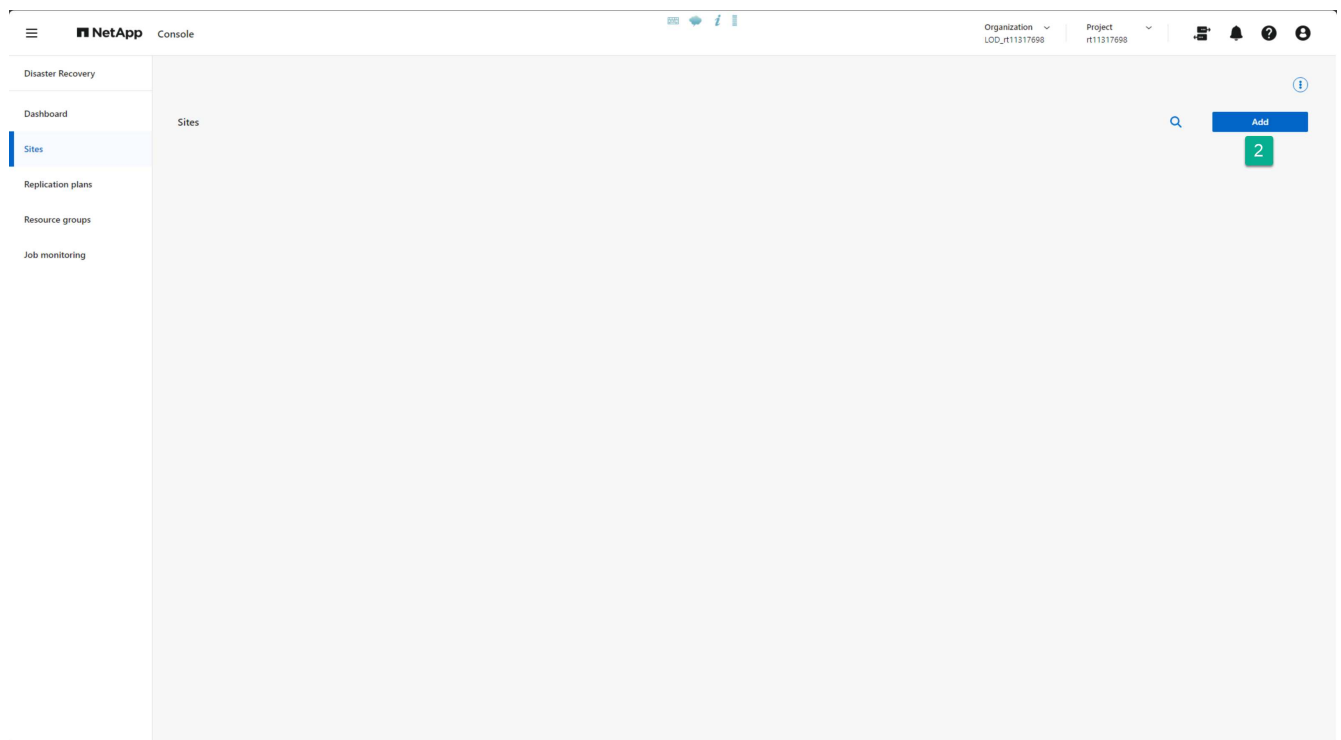
创建生产 vCenter 站点。

步骤

1. 从NetApp Console左侧导航栏中，选择 保护 > 灾难恢复。
2. 从NetApp Disaster Recovery中的任何页面中，选择“站点”选项。



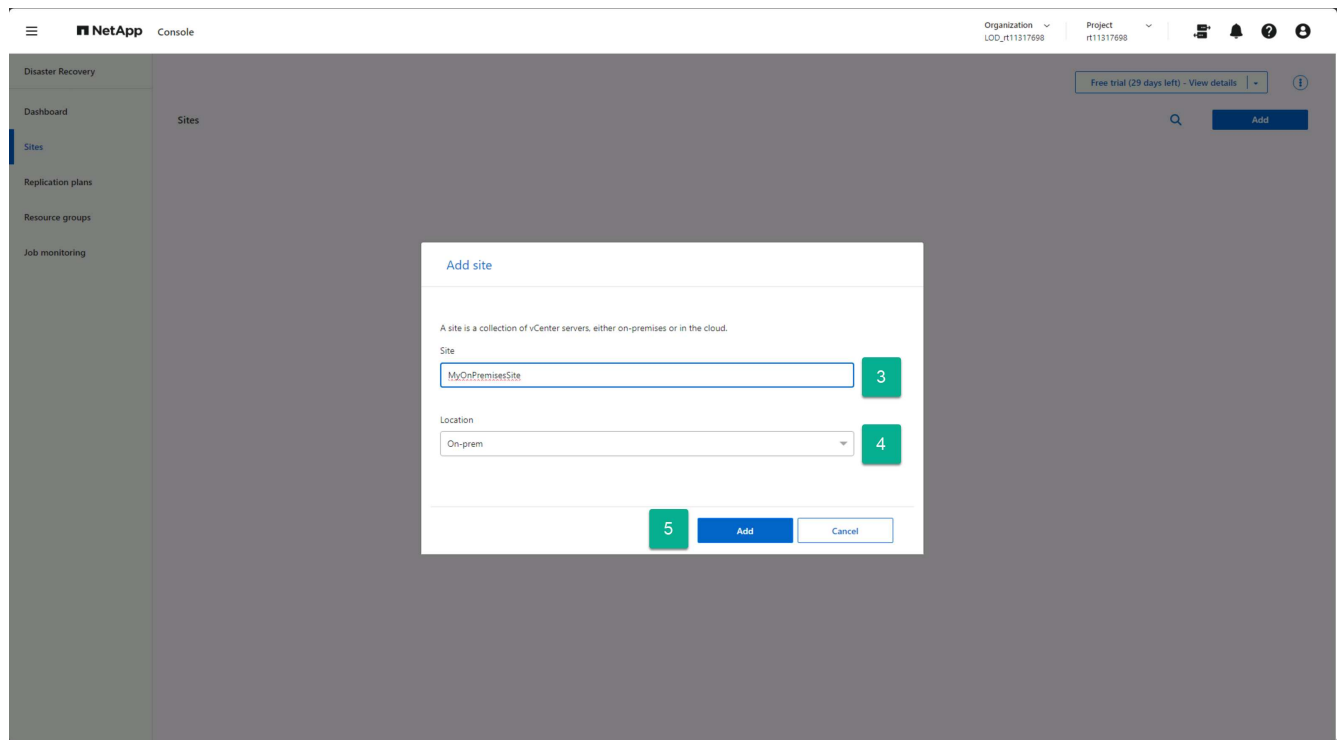
3. 从站点选项中，选择*添加*。



4. 在添加站点对话框中，提供站点名称。

5. 选择“On-prem”作为位置。

6. 选择“添加”。

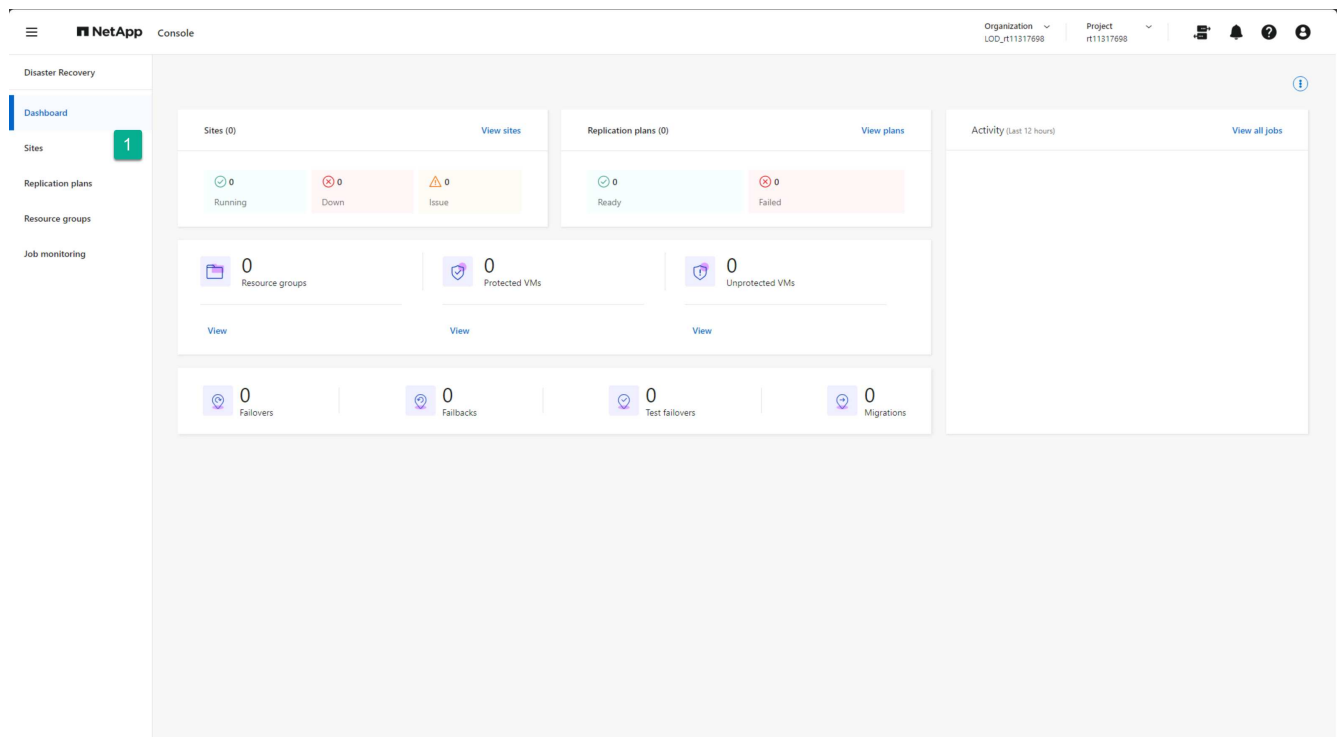


如果您有其他生产 vCenter 站点，则可以使用相同的步骤添加它们。

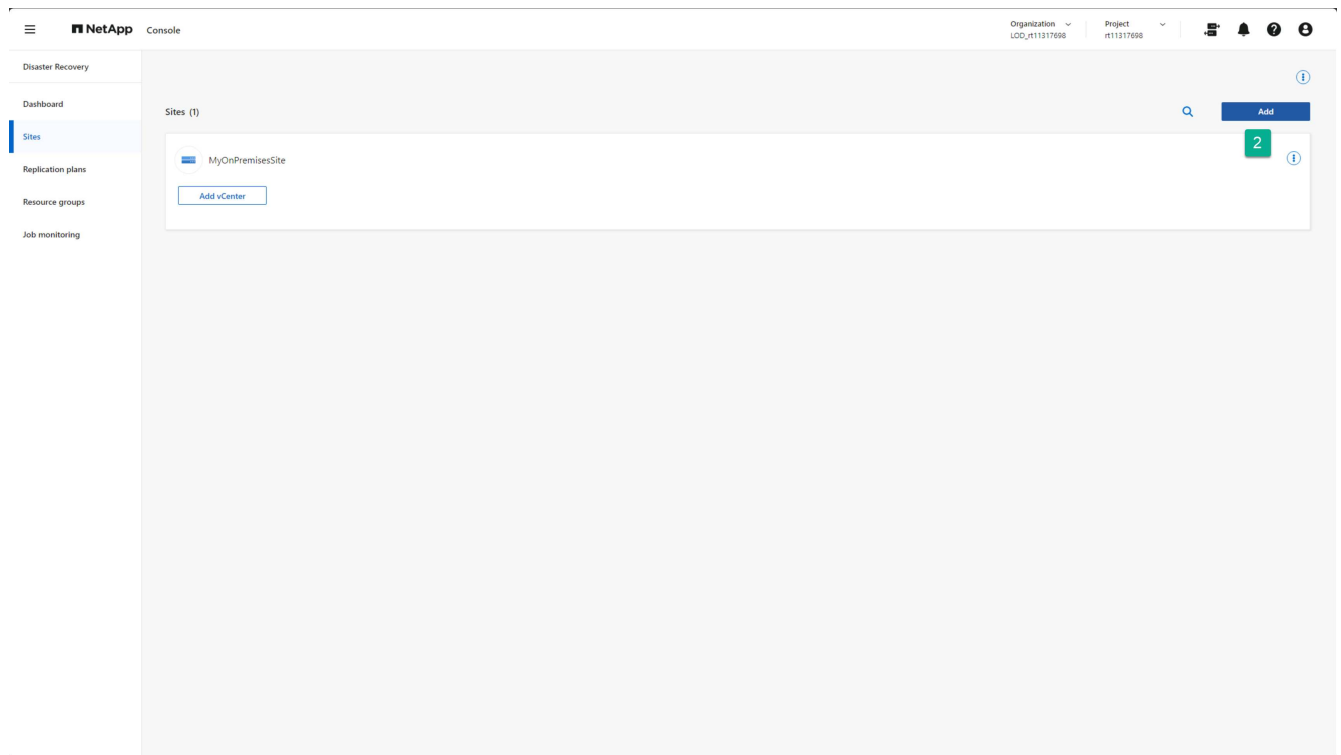
创建亚马逊云站点

使用Amazon FSx for NetApp ONTAP存储为 Amazon EVS 创建 DR 站点。

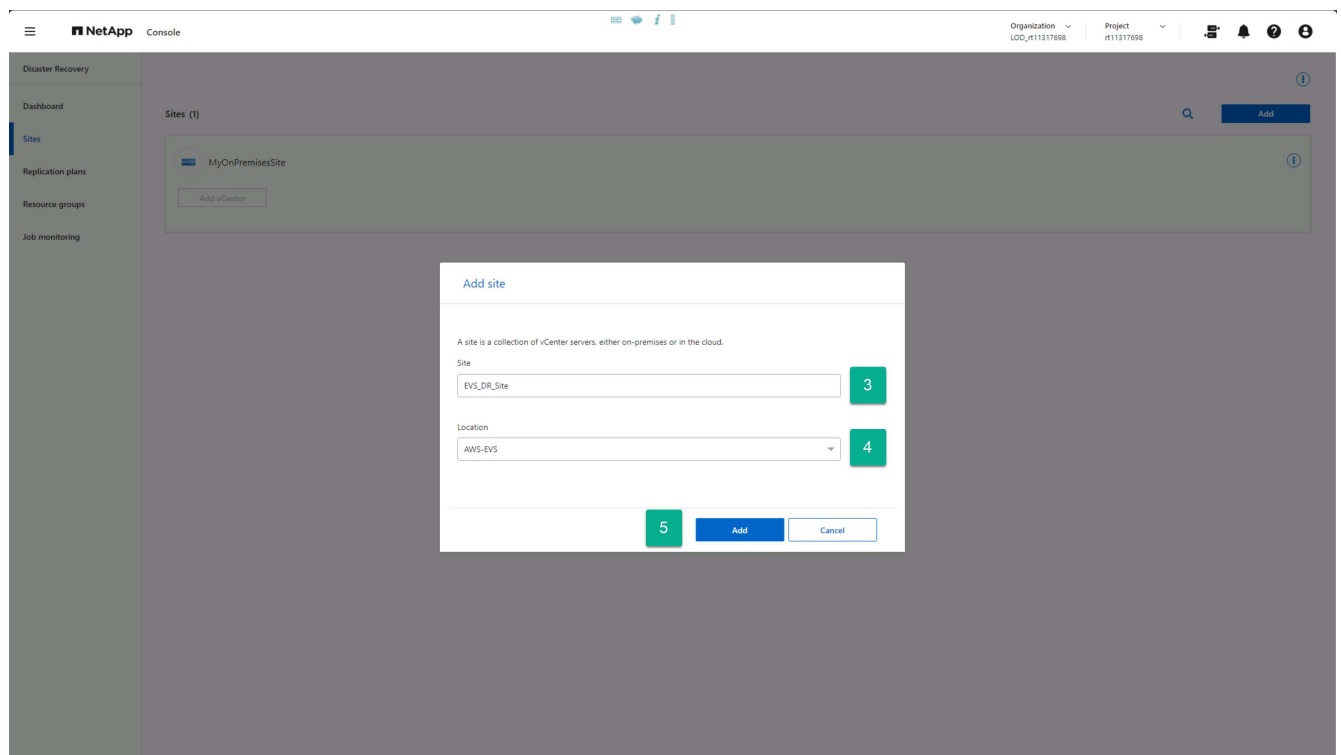
1. 从NetApp Disaster Recovery中的任何页面中，选择“站点”选项。



2. 从站点选项中，选择*添加*。



3. 在添加站点对话框中，提供站点名称。
4. 选择“AWS-EVS”作为位置。
5. 选择“添加”。



结果

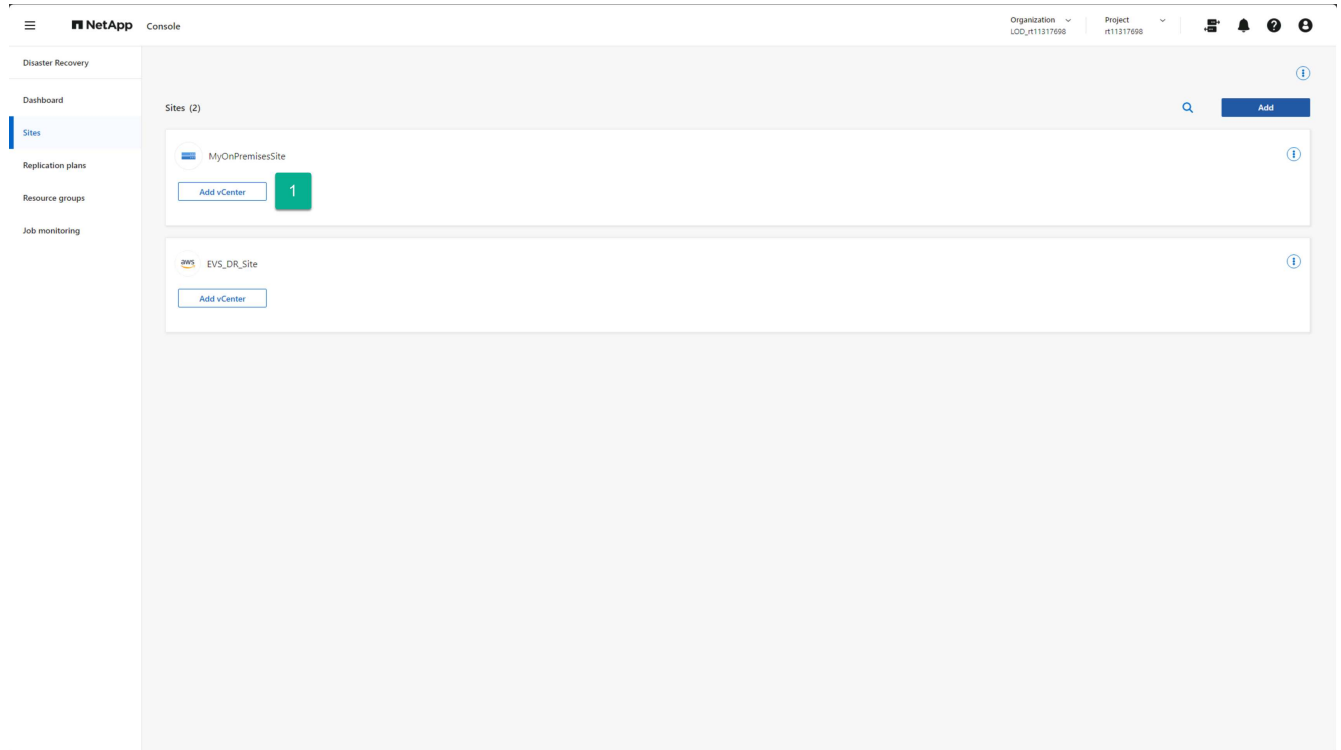
现在您已经创建了一个生产（源）站点和一个 DR（目标）站点。

在NetApp Disaster Recovery中添加本地和 Amazon EVS vCenter 集群

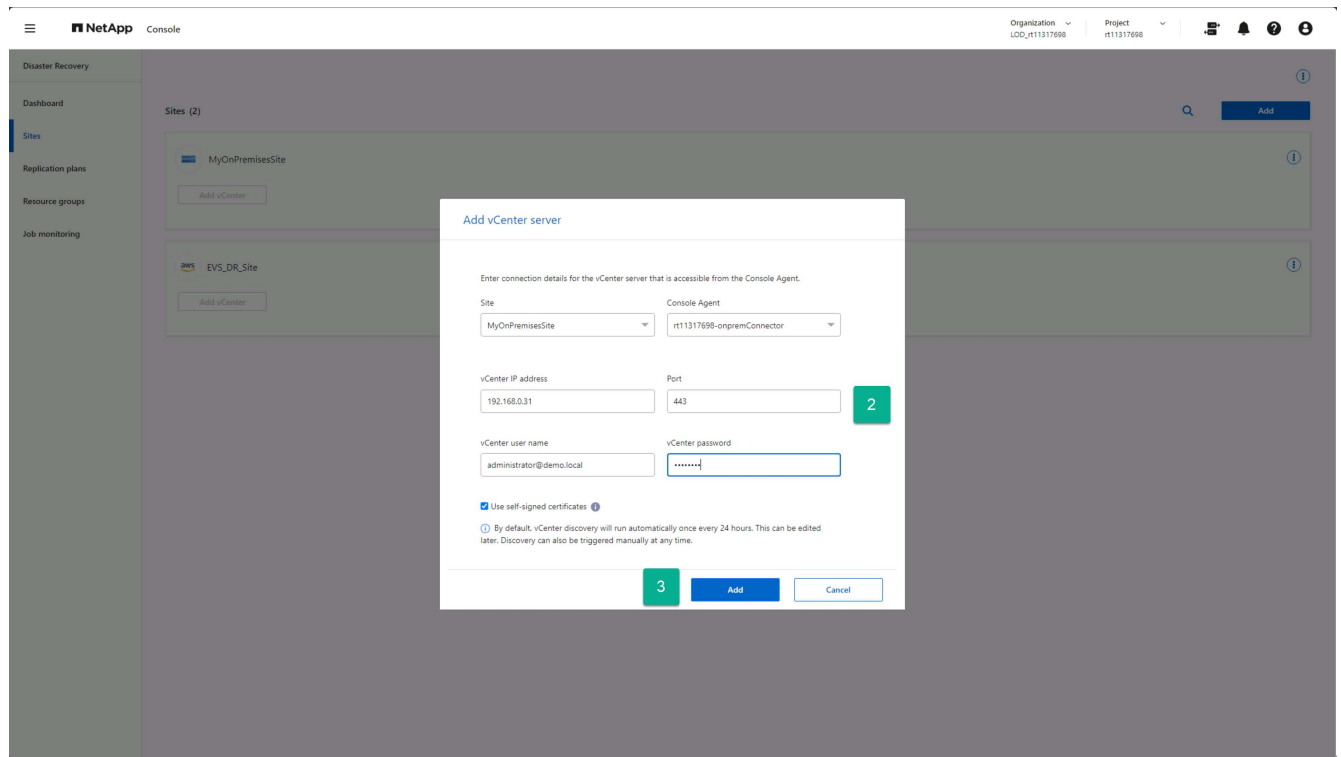
创建站点后，您现在可以将 vCenter 集群添加到NetApp Disaster Recovery中的每个站点。当我们创建每个站点时，我们都会指出每种站点的类型。这会告诉NetApp Disaster Recovery每种站点类型中托管的 vCenter 需要什么类型的访问。Amazon EVS 的优势之一是 Amazon EVS vCenter 和本地 vCenter 之间没有真正的区别。两者都需要相同的连接和身份验证信息。

向每个站点添加 vCenter 的步骤

1. 从“站点”选项中，选择所需站点的“添加 vCenter”。



2. 在添加 vCenter 服务器对话框中，选择或提供以下信息：
 - a. 托管在您的 AWS VPC 内的NetApp Console代理。
 - b. 要添加的 vCenter 的 IP 地址或 FQDN。
 - c. 如果不同，请将端口值更改为 vCenter 集群管理器使用的 TCP 端口。
 - d. 先前创建的帐户的 vCenter 用户名， NetApp Disaster Recovery将使用该用户名来管理 vCenter。
 - e. 所提供用户名的 vCenter 密码。
 - f. 如果您的公司使用外部证书颁发机构 (CA) 或 vCenter Endpoint 证书存储来访问您的 vCenter，请取消选中 使用自签名证书 复选框。否则，请保留此框的选中状态。
3. 选择“添加”。



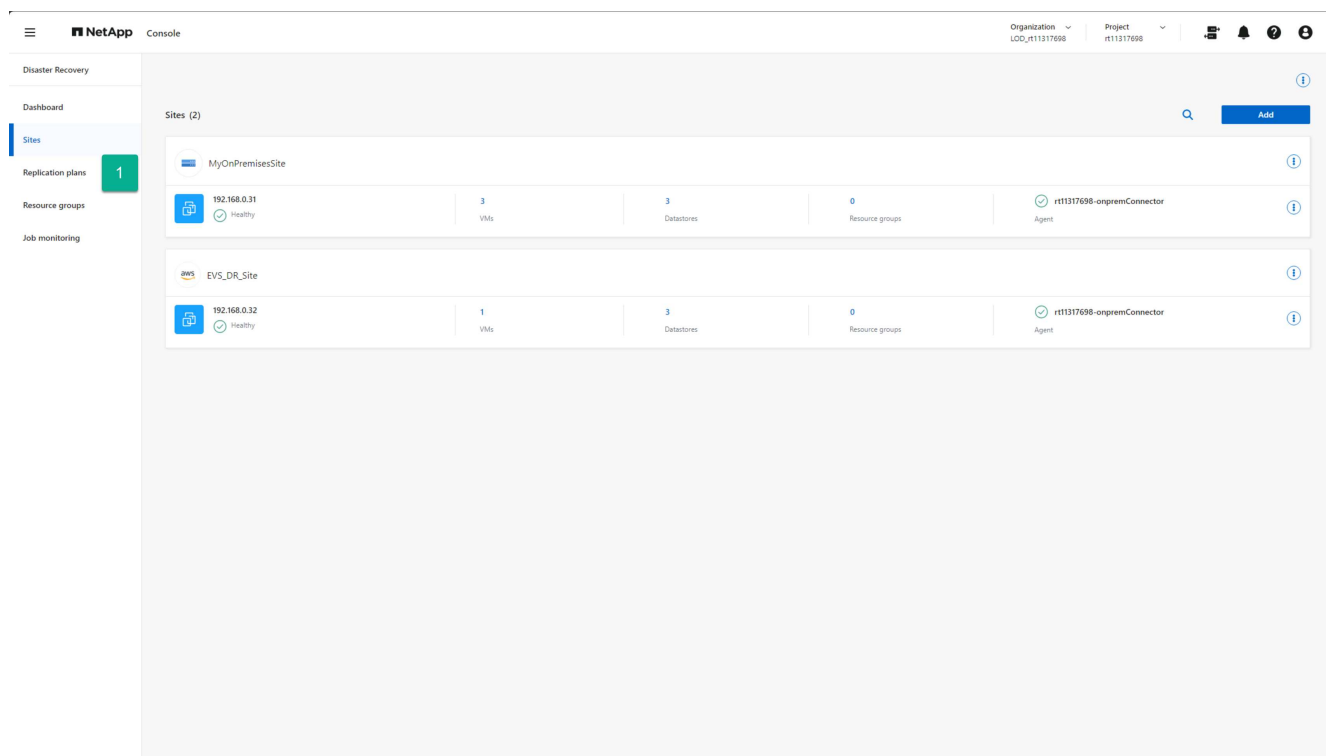
为 Amazon EVS 创建复制计划

在NetApp Disaster Recovery概述中创建复制计划

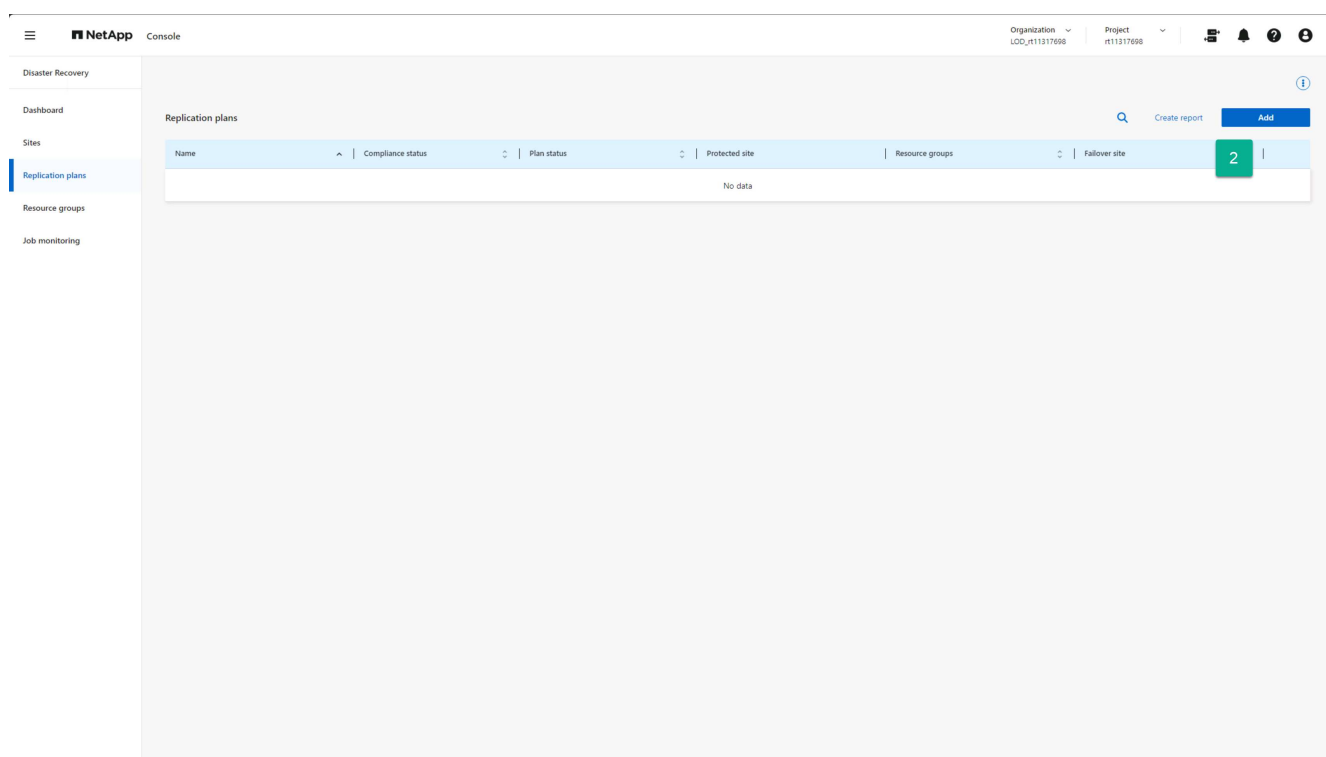
在本地站点上有要保护的 vCenter 并且您有一个配置为使用Amazon FSx for NetApp ONTAP 的Amazon EVS 站点（可将其用作 DR 目标）后，您可以创建复制计划 (RP) 来保护本地站点内 vCenter 集群上托管的任何虚拟机集。

要开始复制计划创建过程：

1. 从任何NetApp Disaster Recovery屏幕中，选择“复制计划”选项。



2. 在复制计划页面中，选择*添加*。



这将打开创建复制计划向导。

继续"创建复制计划向导步骤 1"。

创建复制计划：步骤 1 - 在NetApp Disaster Recovery中选择 vCenter

首先，使用NetApp Disaster Recovery，提供复制计划名称并选择复制的源和目标 vCenter。

1. 为复制计划输入一个唯一的名称。

复制计划名称仅允许使用字母数字字符和下划线 (_)。

2. 选择源 vCenter 集群。
3. 选择目标 vCenter 集群。
4. 选择“下一步”。

NetApp Console

Disaster Recovery

Add replication plan

1 vCenter servers 2 Applications 3 Resource mapping 4 Review

Replication plan > Add plan

Dashboard

Sites

Replication plans

Resource groups

Job monitoring

vCenter servers

Provide the plan name and select the source and target vCenter servers.

Replication plan name

EVS_DR_Plan 1

Select a source vCenter where your data exists, to replicate to the selected target vCenter.

Source vCenter

192.168.0.31 2

Target vCenter

192.168.0.32 3

Replicate

4

Cancel Next

继续["创建复制计划向导步骤 2"](#)。

创建复制计划：步骤 2 - 在NetApp Disaster Recovery中选择虚拟机资源

选择要使用NetApp Disaster Recovery保护的虚拟机。

有多种方法可以选择要保护的虚拟机：

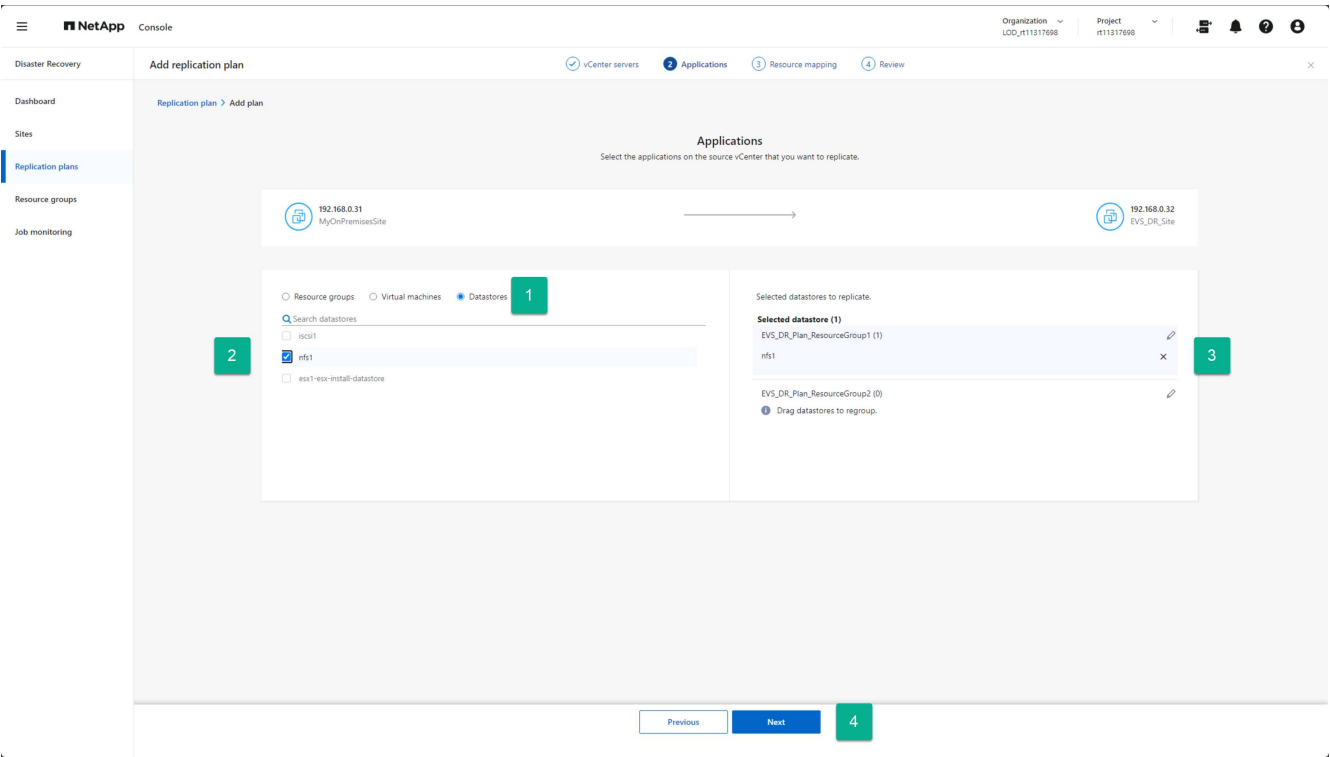
- 选择单个虚拟机：单击“虚拟机”按钮，您可以选择要保护的单个虚拟机。当您选择每个虚拟机时，服务会将其添加到位于屏幕右侧的默认资源组中。
- 选择先前创建的资源组：您可以使用NetApp Disaster Recovery菜单中的资源组选项预先创建自定义资源组。这不是必需的，因为您可以使用其他两种方法来创建资源组作为复制计划过程的一部分。有关详细信息，请参阅["创建复制计划"](#)。
- 选择整个 vCenter 数据存储：如果您有大量虚拟机需要使用此复制计划保护，则选择单个虚拟机可能效率不

高。由于NetApp Disaster Recovery使用基于卷的SnapMirror复制来保护虚拟机，因此驻留在数据存储区上的所有虚拟机都将作为卷的一部分进行复制。大多数情况下，您应该使用NetApp Disaster Recovery保护并重新启动数据存储区上的所有虚拟机。使用此选项可以告诉服务将选定数据存储上托管的任何虚拟机添加到受保护虚拟机列表中。

对于本指导说明，我们选择整个 vCenter 数据存储。

访问此页面的步骤

1. 从“复制计划”页面继续到“应用程序”部分。
2. 查看打开的“应用程序”页面中的信息。



选择数据存储区的步骤：

1. 选择*数据存储*。
2. 选中您想要保护的每个数据存储旁边的复选框。
3. （可选）通过选择资源组名称旁边的铅笔图标，将资源组重命名为合适的名称。
4. 选择“下一步”。

继续["创建复制计划向导步骤3"](#)。

创建复制计划：步骤 3 - 在NetApp Disaster Recovery中映射资源

在您获得要使用NetApp Disaster Recovery保护的虚拟机列表后，请提供故障转移期间要使用的故障转移映射和虚拟机配置信息。

您需要映射四种主要类型的信息：

- 计算资源

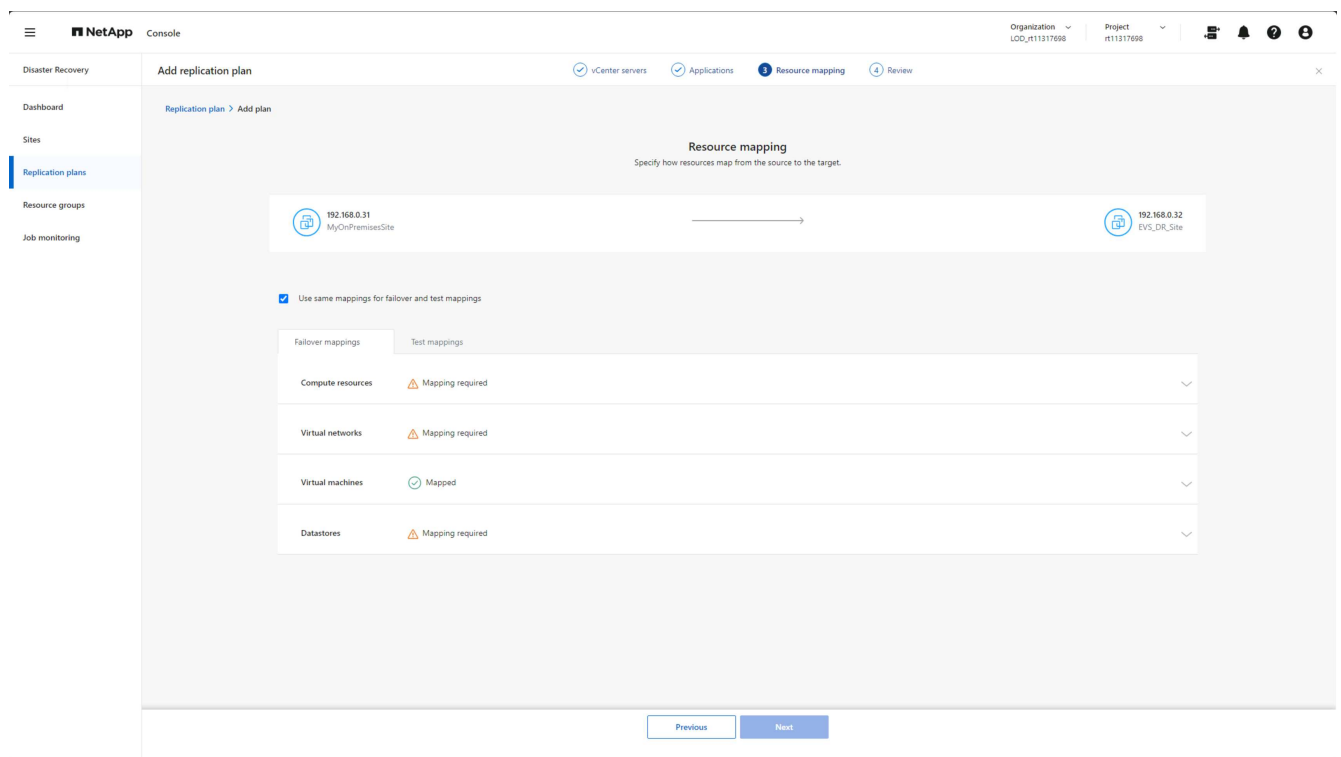
- 虚拟网络
- 虚拟机重新配置
- 数据存储映射

每个虚拟机都需要前三种类型的信息。每个托管要保护的虚拟机的数据存储都需要进行数据存储映射。

- 带有警告图标 () 要求您提供地图信息。
- 标有复选图标 () 已被映射或具有默认映射。检查它们以确保当前配置满足您的要求。

访问此页面的步骤

1. 从“复制计划”页面继续到“资源映射”部分。
2. 查看打开的“资源映射”页面上的信息。



3. 要打开所需的每个映射类别，请选择该部分旁边的向下箭头 (v)。

计算资源映射

由于一个站点可以托管多个虚拟数据中心和多个 vCenter 集群，因此您需要确定在发生故障转移时在哪个 vCenter 集群上恢复虚拟机。

映射计算资源的步骤

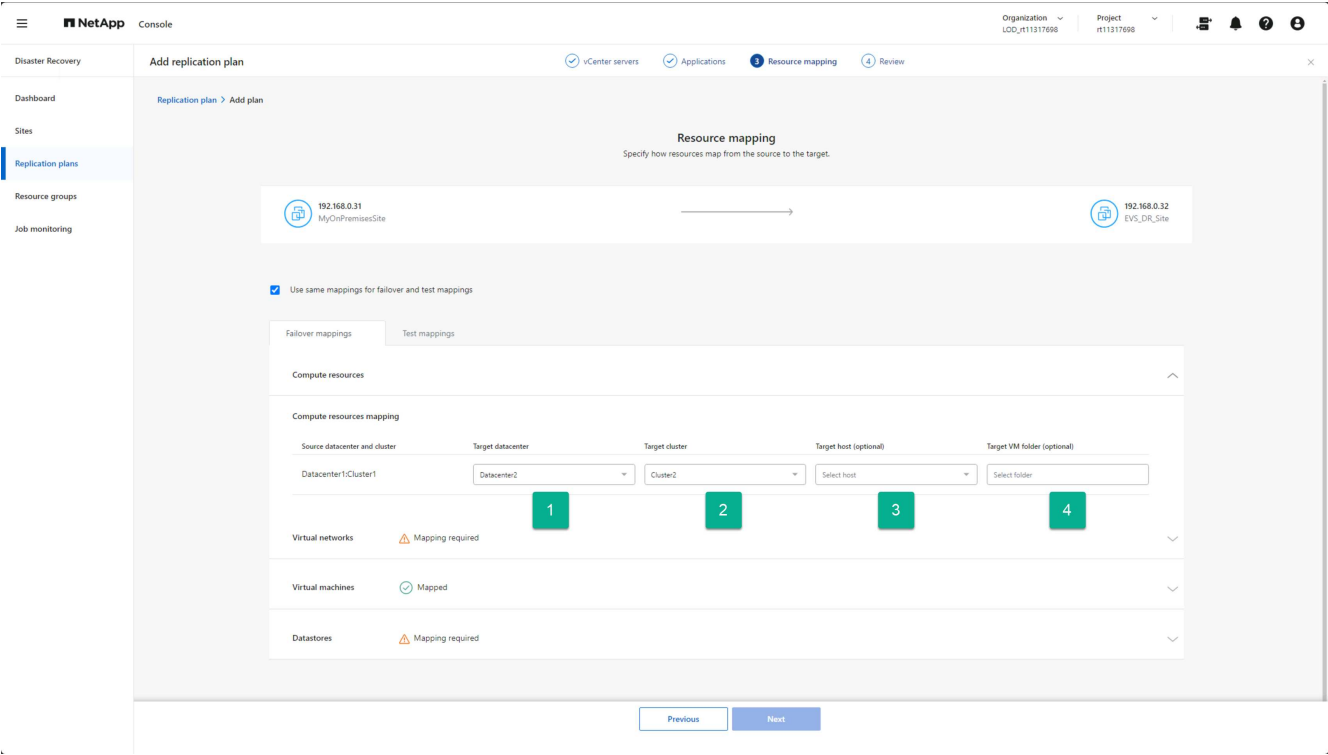
1. 从位于 DR 站点的数据中心列表中选择虚拟数据中心。
2. 从所选虚拟数据中心内的集群列表中选择用于托管数据存储区和虚拟机的集群。

3. （可选）选择目标集群中的目标主机。

此步骤不是必需的，因为NetApp Disaster Recovery会选择在 vCenter 中添加到集群的第一个主机。此时，虚拟机要么继续在该 ESXi 主机上运行，要么 VMware DRS 根据配置的 DRS 规则根据需要将虚拟机移动到不同的 ESXi 主机。

4. （可选）提供用于放置 VM 注册的顶级 vCenter 文件夹的名称。

这是为了满足您的组织需求，并不是必需的。

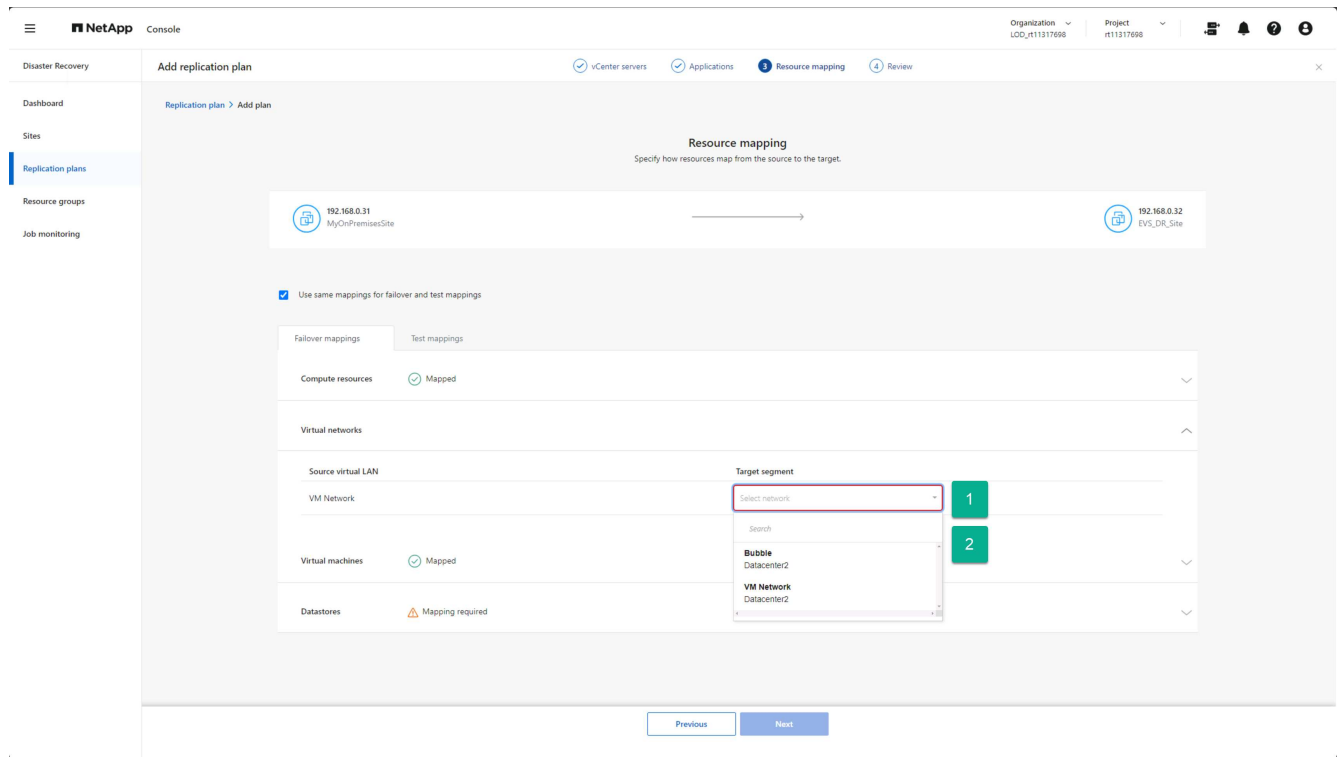


映射虚拟网络资源

每个虚拟机可以有一个或多个虚拟网卡连接到 vCenter 网络基础架构内的虚拟网络。为了确保每个虚拟机在 DR 站点重新启动时都能正确连接到所需的网络，请确定哪些 DR 站点虚拟网络可连接这些虚拟机。通过将本地站点中的每个虚拟网络映射到 DR 站点上的关联网络来实现此目的。

选择每个源虚拟网络要映射到哪个目标虚拟网络

- 1. 从下拉列表中选择目标段。
- 2. 对列出的每个源虚拟网络重复上一步。



定义故障转移期间虚拟机重新配置的选项

每个虚拟机可能都需要修改才能在 DR vCenter 站点中正常工作。虚拟机部分使您能够提供必要的更改。

默认情况下，NetApp Disaster Recovery 对每个虚拟机使用与源本地站点相同的设置。这假设虚拟机将使用相同的 IP 地址、虚拟 CPU 和虚拟 DRAM 配置。

网络重新配置

支持的 IP 地址类型为静态和 DHCP。对于静态 IP 地址，您有以下目标 IP 设置：

- 与源相同：顾名思义，该服务在目标虚拟机上使用的 IP 地址与源站点虚拟机上使用的 IP 地址相同。这要求您为上一步中映射的虚拟网络配置相同的子网设置。
- 与源不同：该服务为每个 VM 提供了一组 IP 地址字段，这些字段必须针对目标虚拟网络上使用的适当子网进行配置，您在上一节中已映射该子网。对于每个虚拟机，您必须提供 IP 地址、子网掩码、DNS 和默认网关值。或者，对所有虚拟机使用相同的子网掩码、DNS 和网关设置，以简化所有虚拟机连接到同一子网时的过程。
- 子网映射：此选项根据目标虚拟网络的 CIDR 配置重新配置每个 VM 的 IP 地址。要使用此功能，请确保每个 vCenter 的虚拟网络在服务内都有定义的 CIDR 设置，如“站点”页面中的 vCenter 信息中所更改的那样。

配置子网后，子网映射对源和目标 VM 配置使用相同的 IP 地址单元组件，但根据提供的 CIDR 信息替换 IP 地址的子网组件。此功能还要求源虚拟网络和目标虚拟网络具有相同的 IP 地址类别（/xx CIDR 的组成部分）。这可确保目标站点有足够的 IP 地址来托管所有受保护的虚拟机。

对于此 EVS 设置，我们假设源和目标 IP 配置相同，不需要任何额外的重新配置。

更改网络设置重新配置

1. 选择故障转移虚拟机使用的 IP 寻址类型。

2. (可选) 通过提供可选的前缀和后缀值为重新启动的虚拟机提供虚拟机重命名方案。

1

2

Source VM	Operating system	CPUs	RAM	Boot order	Boot delay (mins between 0 and 10)	Create application consistent replicas	Scripts	Credentials
Linux1	Linux	1	2 GiB	1	0	☐	None	Not required
Linux4	Linux	1	2 GiB	3	5	☐	None	Not required
Linux3	Linux	1	2 GiB	2	5	☐	None	Not required

VM 计算资源重新配置

重新配置虚拟机计算资源有多种选择。NetApp Disaster Recovery 支持更改虚拟 CPU 的数量、虚拟 DRAM 的数量和 VM 名称。

指定任何 VM 配置更改

1. (可选) 修改每个虚拟机应使用的虚拟 CPU 数量。如果您的 DR vCenter 集群主机没有源 vCenter 集群那么多的 CPU 核心，则可能需要这样做。
2. (可选) 修改每个虚拟机应使用的虚拟 DRAM 数量。如果您的 DR vCenter 集群主机没有源 vCenter 集群主机那么多的物理 DRAM，则可能需要这样做。

NetApp Console

Disaster Recovery | Add replication plan

Organization: LCO_r11317698 | Project: r11317698

Steps: vCenter servers | Applications | **Resource mapping** | Review

Falover mappings | Test mappings

Compute resources: ☒ Mapped

Virtual networks: ☒ Mapped

Virtual machines

IP address type: Static | Target IP: Same as source

☐ Use the same credentials for all VMs
☐ Use the same script for all VMs

Target VM prefix: | Optional | Target VM suffix: | Optional | Preview: Sample VM name

Source VM	Operating system	CPUs	RAM	Boot order	Boot delay(mins between 0 and 10)	Create application consistent replicas	Scripts	Credentials
Linux1	Linux	1	2 GiB	1	0	☐	None 🔗	Not required
Linux4	Linux	1	2 GiB	3	5	☐	None 🔗	Not required
Linux3	Linux	1	2 GiB	2	5	☐	None 🔗	Not required

1 2

1 - 3 of 3 << < 1 > >>

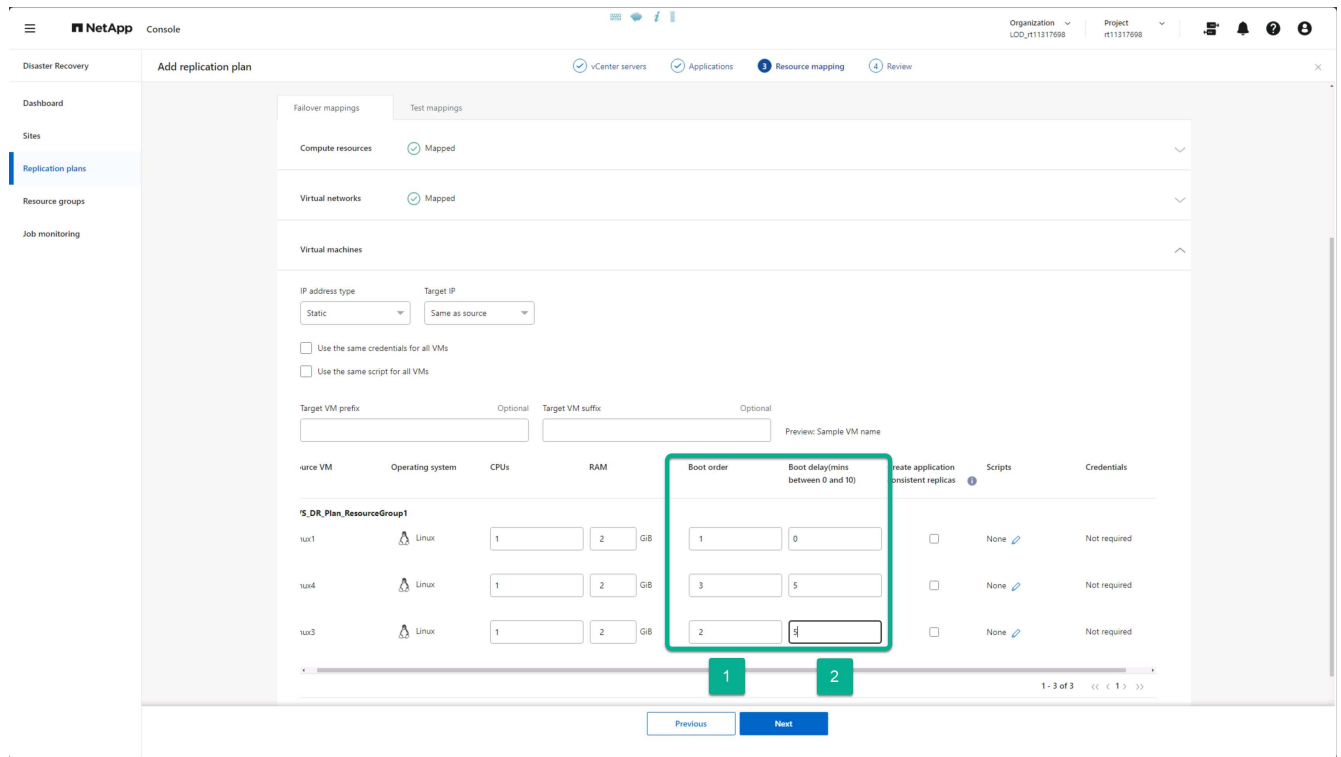
Previous Next

启动顺序

NetApp Disaster Recovery支持根据启动顺序字段有序重启虚拟机。启动顺序字段指示每个资源组中的虚拟机如何启动。启动顺序字段中具有相同值的虚拟机将并行启动。

修改启动顺序设置

1. （可选）修改您希望重新启动虚拟机的顺序。该字段可采用任意数值。 NetApp Disaster Recovery尝试并行重新启动具有相同数值的虚拟机。
2. （可选）提供每次 VM 重启之间的延迟。该时间是在该虚拟机重启完成后、具有下一个更高启动顺序号的虚拟机之前注入的。这个数字以分钟为单位。



自定义客户操作系统操作

NetApp Disaster Recovery支持为每个虚拟机执行一些客户操作系统操作：

- NetApp Disaster Recovery可以为运行 Oracle 数据库和 Microsoft SQL Server 数据库的虚拟机进行应用程序一致的备份。
- NetApp Disaster Recovery可以执行适合每个虚拟机的客户操作系统的自定义脚本。执行此类脚本需要客户操作系统可接受的用户凭证，并且该凭证具有足够的权限来执行脚本中列出的操作。

修改每个虚拟机的自定义客户操作系统操作

1. （可选）如果虚拟机托管 Oracle 或 SQL Server 数据库，请选中“创建应用程序一致副本”复选框。
2. （可选）要在启动过程中在客户操作系统中采取自定义操作，请为任何虚拟机上传脚本。要在所有虚拟机中运行单个脚本，请使用突出显示的复选框并填写字段。
3. 某些配置更改需要具有足够权限的用户凭据才能执行操作。在下列情况下提供凭证：
 - 客户操作系统将在虚拟机内执行脚本。
 - 需要执行应用程序一致的快照。

The screenshot shows the 'Add replication plan' wizard in the NetApp Console, specifically the 'Resource mapping' step. The left sidebar contains navigation links: Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main area is divided into 'Failover mappings' and 'Test mappings' tabs. Under 'Failover mappings', there are sections for 'Compute resources' (Mapped), 'Virtual networks' (Mapped), and 'Virtual machines'. The 'Virtual machines' section includes fields for 'IP address type' (Static), 'Target IP' (Same as source), and checkboxes for 'Use the same credentials for all VMs' and 'Use the same script for all VMs'. Below these are fields for 'Target VM prefix' and 'Target VM suffix', both marked as 'Optional'. A 'Preview: Sample VM name' field is also present. A table lists VMs with columns: source VM, Operating system, CPUs, RAM, Boot order, Boot delay (mins between 0 and 10), Create application consistent replicas, Scripts, and Credentials. The table shows three VMs: vux1, vux4, and vux3, all running Linux. VM1 has a script 'VM-boot-script.ps1' provided, while vux4 and vux3 have 'None' for scripts and 'Not required' for credentials. At the bottom, there are 'Previous' and 'Next' buttons, and a progress indicator showing steps 1, 2, and 3, with step 3 being the current step.

地图数据存储

创建复制计划的最后一步是确定ONTAP应如何保护数据存储库。这些设置定义了复制计划恢复点目标 (RPO)、应维护多少个备份以及在何处复制每个 vCenter 数据存储区的托管ONTAP卷。

默认情况下， NetApp Disaster Recovery管理其自己的快照复制计划；但是，您可以选择指定使用现有的SnapMirror复制策略计划来保护数据存储区。

此外，您还可以选择自定义要使用的数据 LIF（逻辑接口）和导出策略。如果您不提供这些设置， NetApp Disaster Recovery将使用与相应协议（NFS、iSCSI 或 FC）关联的所有数据 LIF，并使用 NFS 卷的默认导出策略。

配置数据存储（卷）映射

1. （可选）决定是否要使用现有的ONTAP SnapMirror复制计划或让NetApp Disaster Recovery管理虚拟机的保护（默认）。
2. 提供服务开始备份的起点。
3. 指定服务进行备份并将其复制到 DR 目标Amazon FSx for NetApp ONTAP集群的频率。
4. 指定应保留多少个历史备份。该服务在源和目标存储集群上维护相同数量的备份。
5. （可选）为每个卷选择一个默认逻辑接口（数据 LIF）。如果未选择任何内容，则会配置目标 SVM 中支持卷访问协议的所有数据 LIF。
6. （可选）为任何 NFS 卷选择导出策略。如果未选择，则使用默认导出策略

继续"创建复制计划向导步骤4"。

创建复制计划：步骤 4 - 验证NetApp Disaster Recovery中的设置

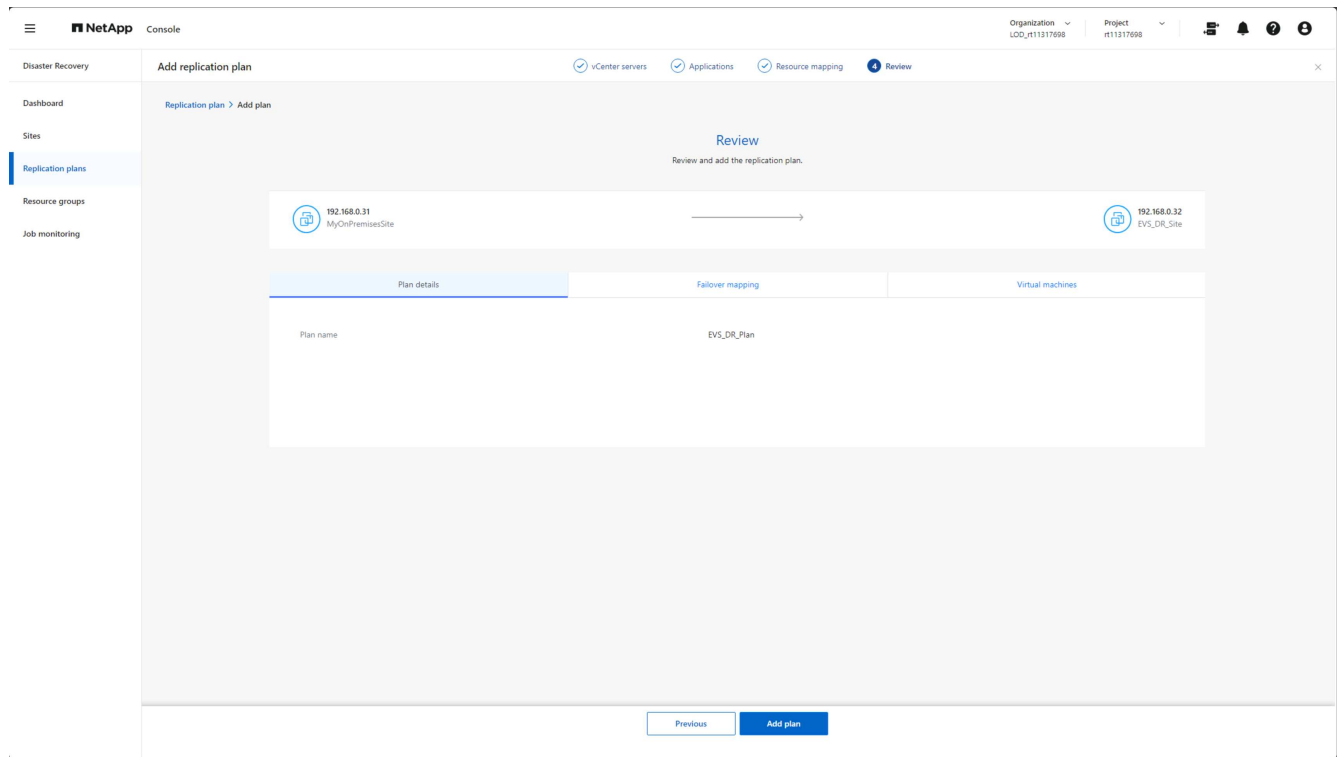
在NetApp Disaster Recovery中添加复制计划信息后，请验证您输入的信息是否正确。

步骤

1. 在激活复制计划之前，选择“保存”来检查您的设置。

您可以选择每个选项卡来查看设置，并通过选择铅笔图标在任何选项卡上进行更改。

复制计划设置审查



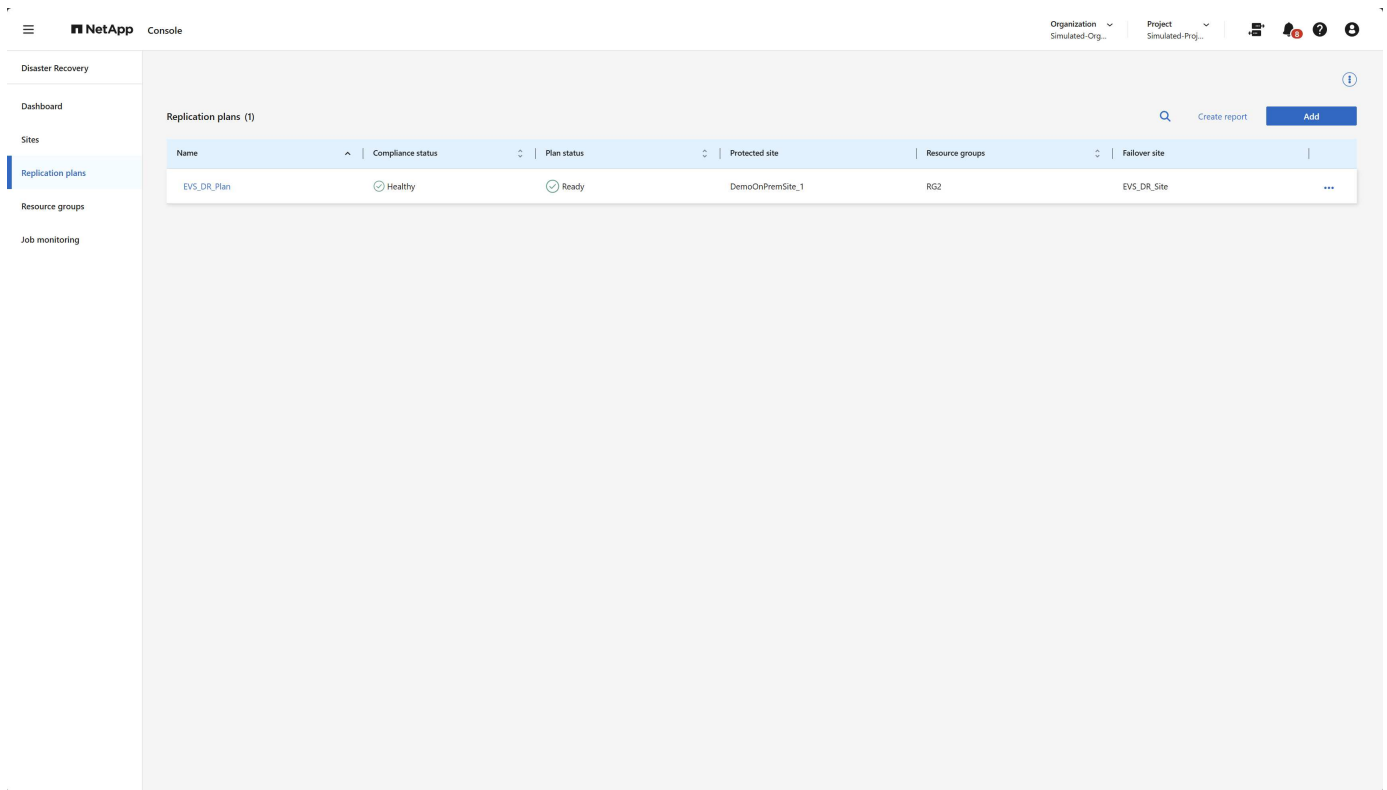
2. 当您确认所有设置正确无误后，选择屏幕底部的*添加计划*。

继续["验证复制计划"](#)。

验证**NetApp Disaster Recovery**中一切正常

在NetApp Disaster Recovery中添加复制计划后，您将返回到“复制计划”页面，您可以在其中查看复制计划及其状态。您应该验证复制计划是否处于*健康*状态。如果不是，您应该检查复制计划的状态并在继续之前纠正任何问题。

图：复制计划页面



NetApp Disaster Recovery执行一系列测试，以验证所有组件（ONTAP集群、vCenter 集群和虚拟机）是否可访问且处于正确状态，以便服务保护虚拟机。这被称为合规性检查，并且会定期进行。

在复制计划页面中，您可以看到以下信息：

- 上次合规性检查的状态
- 复制计划的复制状态
- 受保护（源）站点的名称
- 复制计划保护的资源组列表
- 故障转移（目标）站点的名称

使用NetApp Disaster Recovery执行复制计划操作

使用NetApp Disaster Recovery与 Amazon EVS 和Amazon FSx for NetApp ONTAP执行以下操作：故障转移、测试故障转移、刷新资源、迁移、立即拍摄快照、禁用/启用复制计划、清理旧快照、协调快照、删除复制计划和编辑计划。

故障转移

您可能需要执行的主要操作是您希望永远不会发生的操作：在生产本地站点发生灾难性故障时故障转移到 DR（目标）数据中心。

故障转移是一个手动启动的过程。

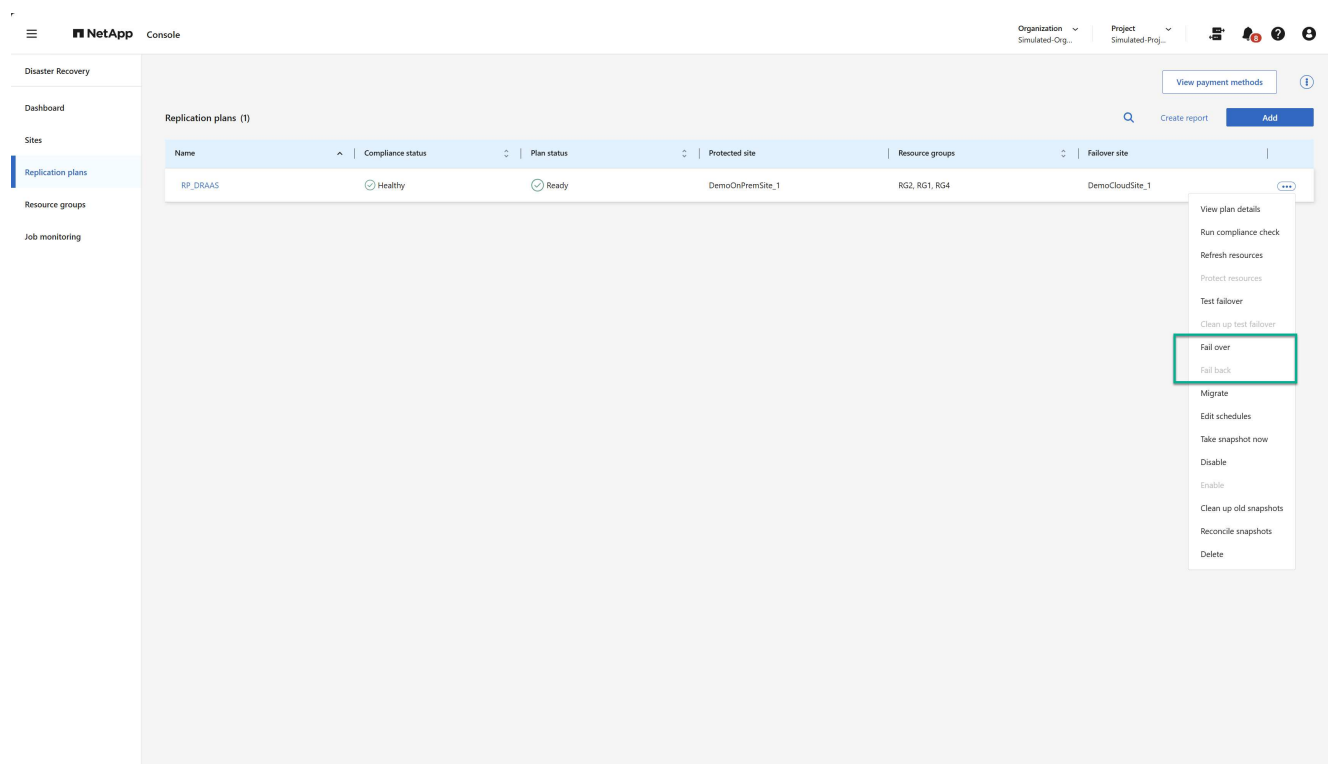
访问故障转移操作的步骤

1. 从NetApp Console左侧导航栏中，选择 保护 > 灾难恢复。

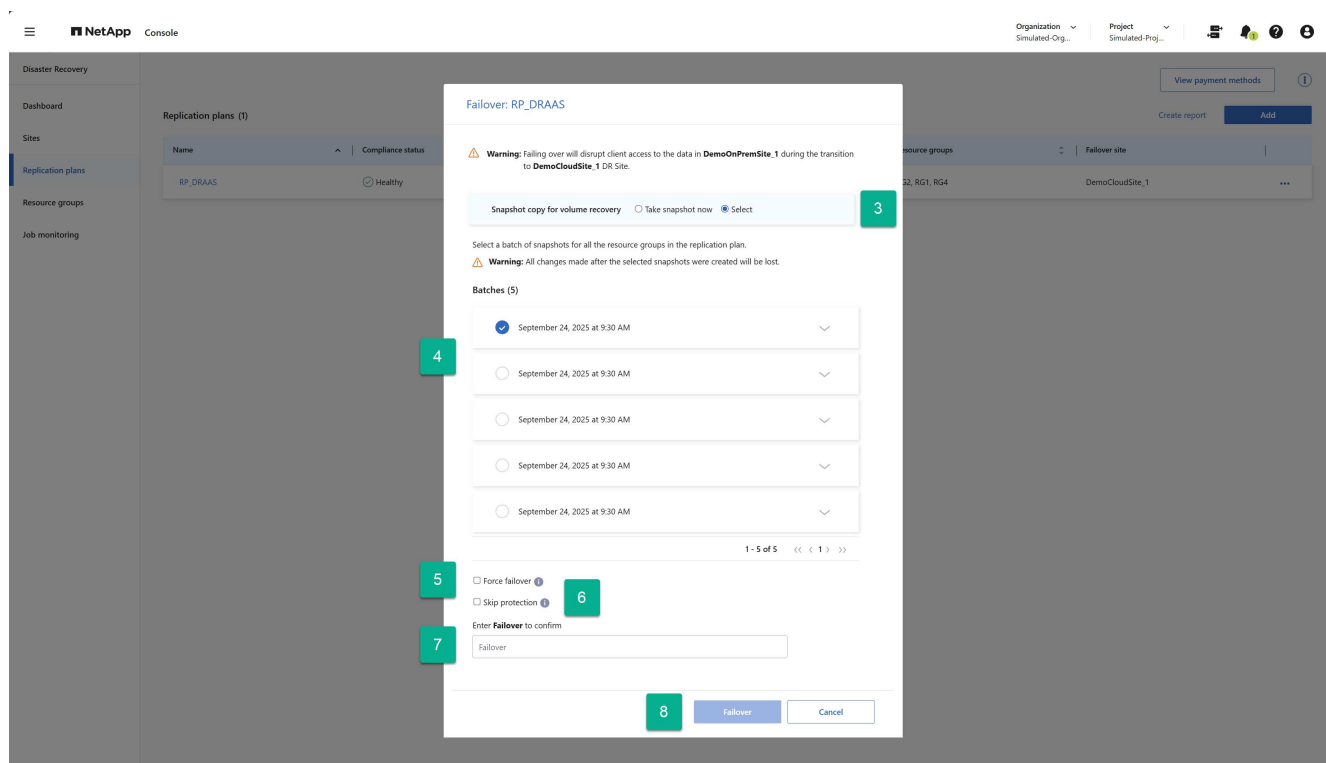
2. 从NetApp Disaster Recovery菜单中，选择 复制计划。

执行故障转移的步骤

1. 在复制计划页面中，选择复制计划的操作选项 。
2. 选择*故障转移*。



3. 如果无法访问生产（受保护）站点，请选择之前创建的快照作为恢复映像。为此，请选择*选择*。
4. 选择要用于恢复的备份。
5. （可选）选择是否希望NetApp Disaster Recovery强制执行故障转移过程，而不管复制计划的状态如何。这只能作为最后的手段。
6. （可选）选择是否希望NetApp Disaster Recovery在生产站点恢复后自动创建反向保护关系。
7. 输入单词“Failover”以确认您是否要继续。
8. 选择“故障转移”。



测试故障转移

测试故障转移与故障转移类似，但有两个区别。

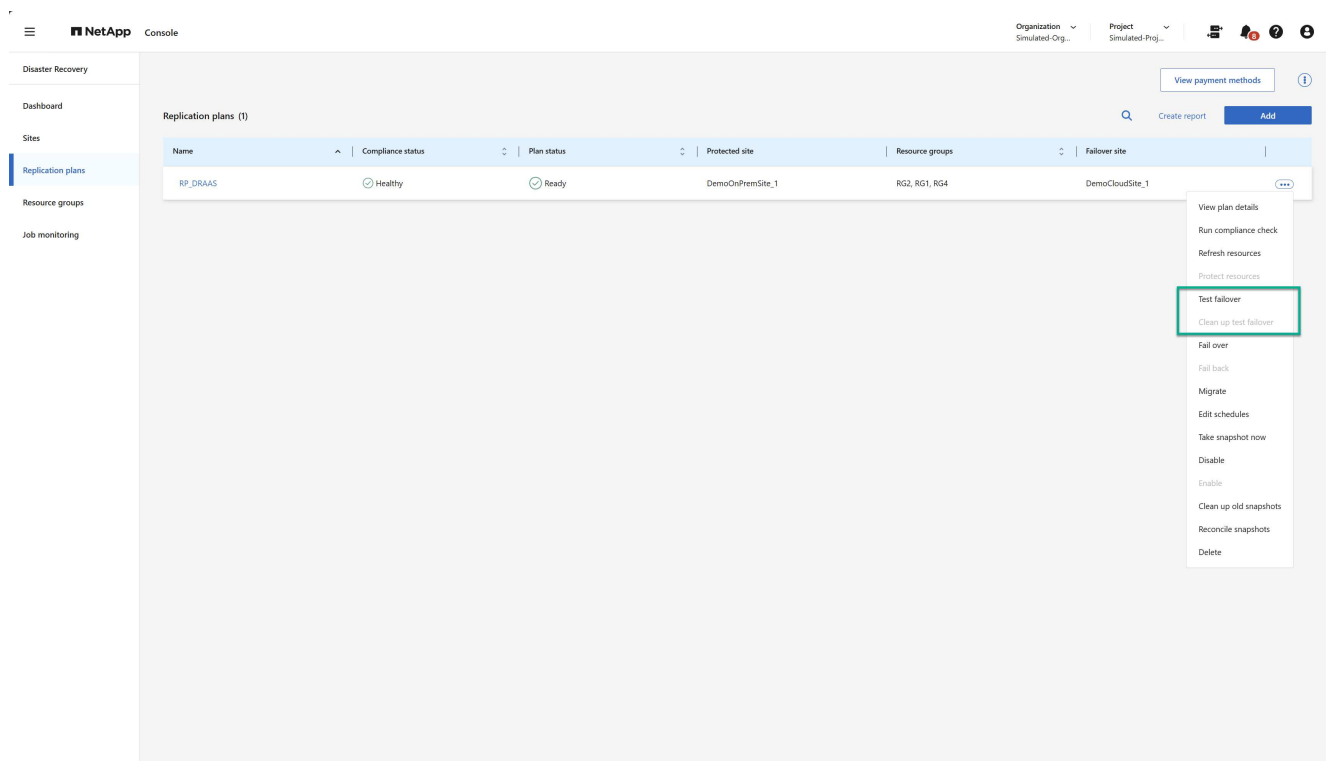
- 生产站点仍然处于活动状态，所有虚拟机仍在按预期运行。
- NetApp Disaster Recovery对生产虚拟机的保护仍在继续。

这是通过在目标站点使用本机ONTAP FlexClone卷来实现的。要了解有关测试故障转移的更多信息，请参阅["将应用程序故障转移到远程站点 | NetApp文档"](#)。

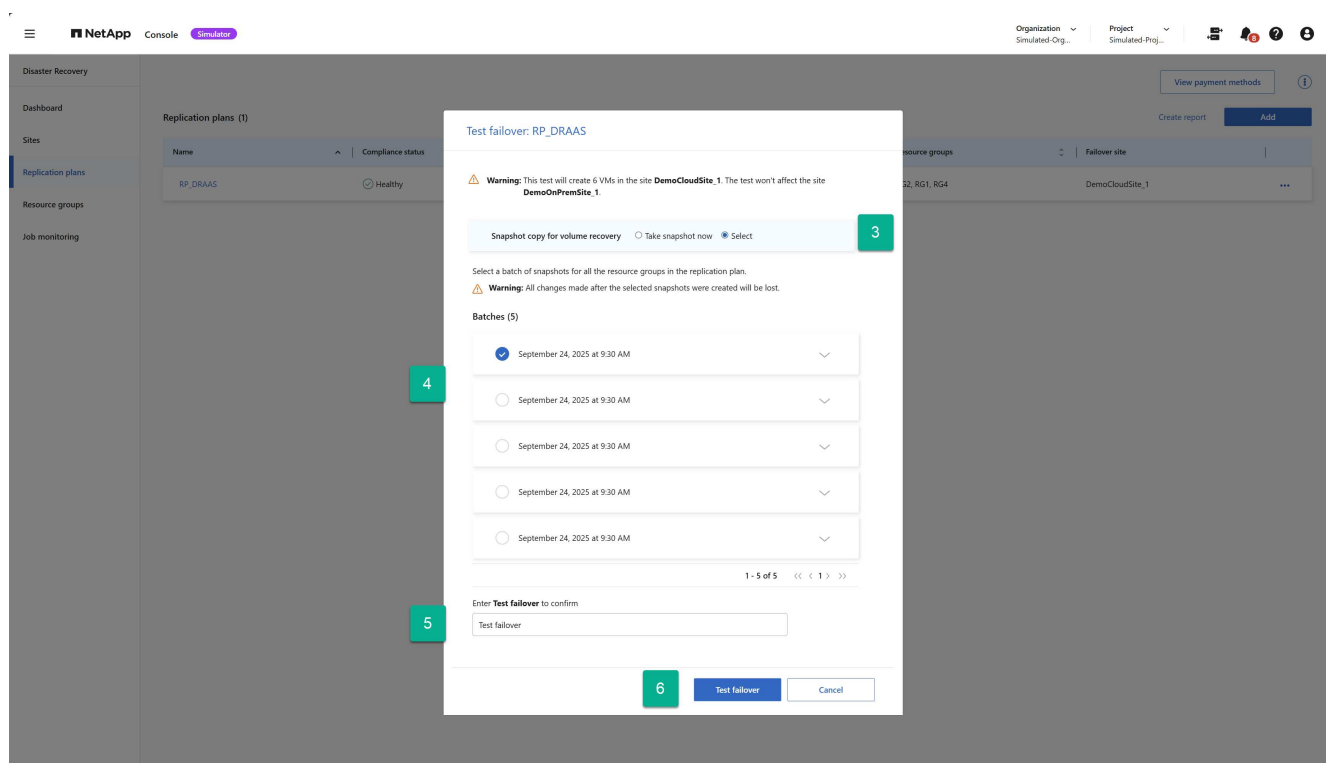
执行测试故障转移的步骤与执行实际故障转移的步骤相同，只是您使用复制计划的上下文菜单上的测试故障转移操作。

步骤

1. 选择复制计划的操作选项 .
2. 从菜单中选择*测试故障转移*。



3. 决定是否要获取生产环境的最新状态（立即拍摄快照）或使用先前创建的复制计划备份（选择）
4. 如果您选择了之前创建的备份，则选择要用于恢复的备份。
5. 输入“测试故障转移”一词来验证您是否要继续。
6. 选择*测试故障转移*。

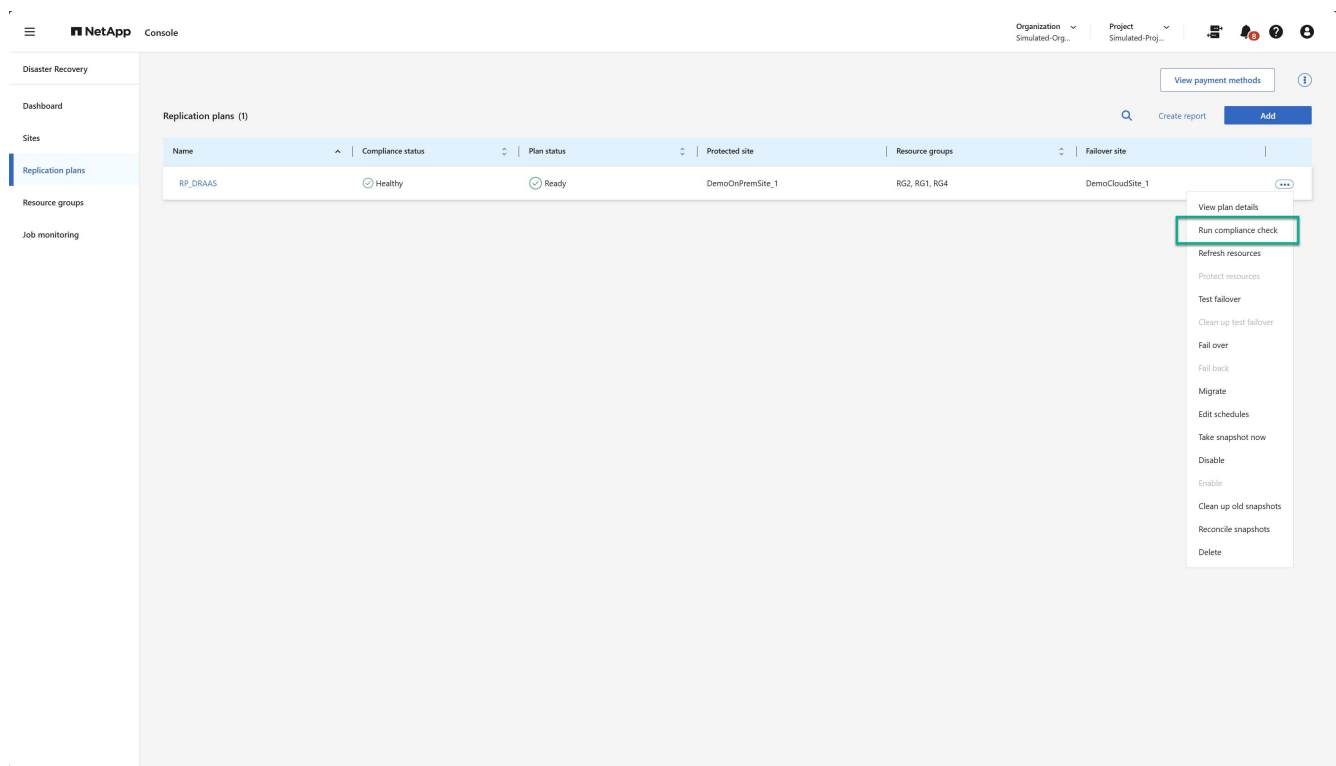


运行合规性检查

默认情况下，合规性检查每三小时运行一次。您可能随时想要手动运行合规性检查。

步骤

1. 选择“操作”选项  复制计划旁边。
2. 从复制计划的操作菜单中选择*运行合规性检查*选项：



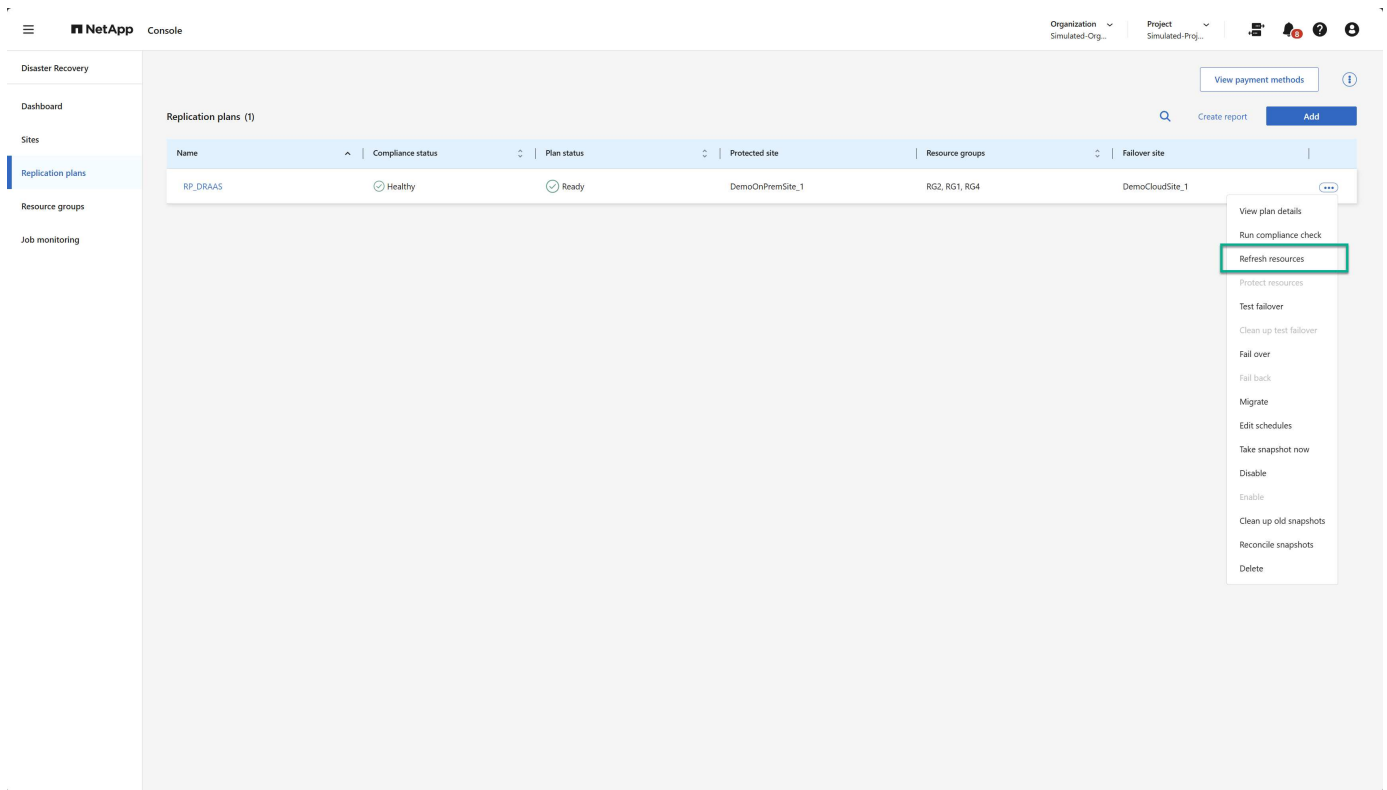
3. 要更改NetApp Disaster Recovery自动运行合规性检查的频率，请从复制计划的操作菜单中选择“编辑计划”选项。

刷新资源

每次对虚拟基础架构进行更改（例如添加或删除虚拟机、添加或删除数据存储区或在数据存储区之间移动虚拟机）时，都需要在NetApp Disaster Recovery服务中对受影响的 vCenter 集群执行刷新。该服务默认每 24 小时自动执行一次此操作，但手动刷新可确保最新的虚拟基础设施信息可用并考虑到 DR 保护。

有两种情况需要刷新：

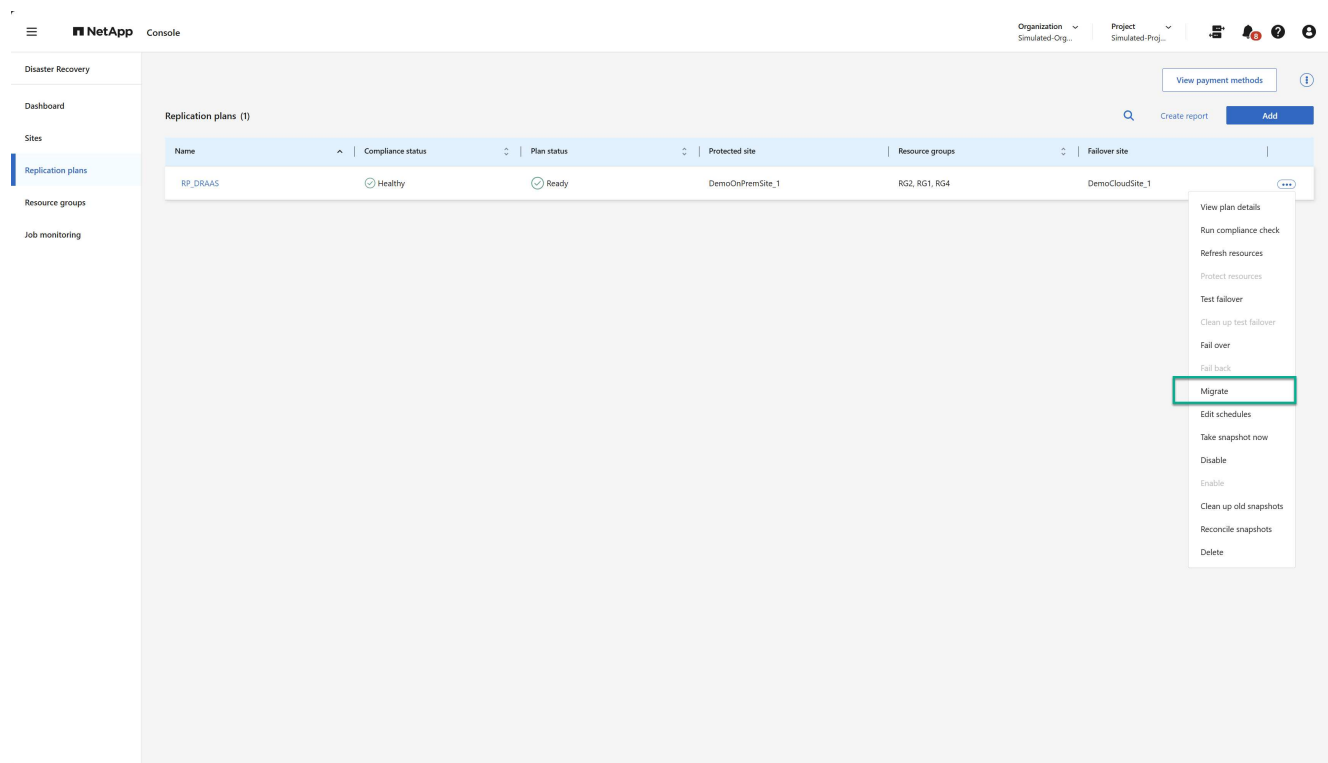
- vCenter 刷新：每当在 vCenter 群集中添加、删除或移出虚拟机时，执行 vCenter 刷新：
- 复制计划刷新：每当虚拟机在同一源 vCenter 集群中的数据存储之间移动时，执行复制计划刷新。



迁移

虽然NetApp Disaster Recovery主要用于灾难恢复用例，但它也可以将一组虚拟机从源站点一次性移动到目标站点。这可能是为了协调迁移到云项目，也可能是为了避免灾难——例如恶劣天气、政治冲突或其他潜在的暂时灾难性事件。

1. 选择“操作”选项 ●●●复制计划旁边。
2. 要将复制计划中的虚拟机移动到目标 Amazon EVS 集群，请从复制计划的操作菜单中选择“迁移”：

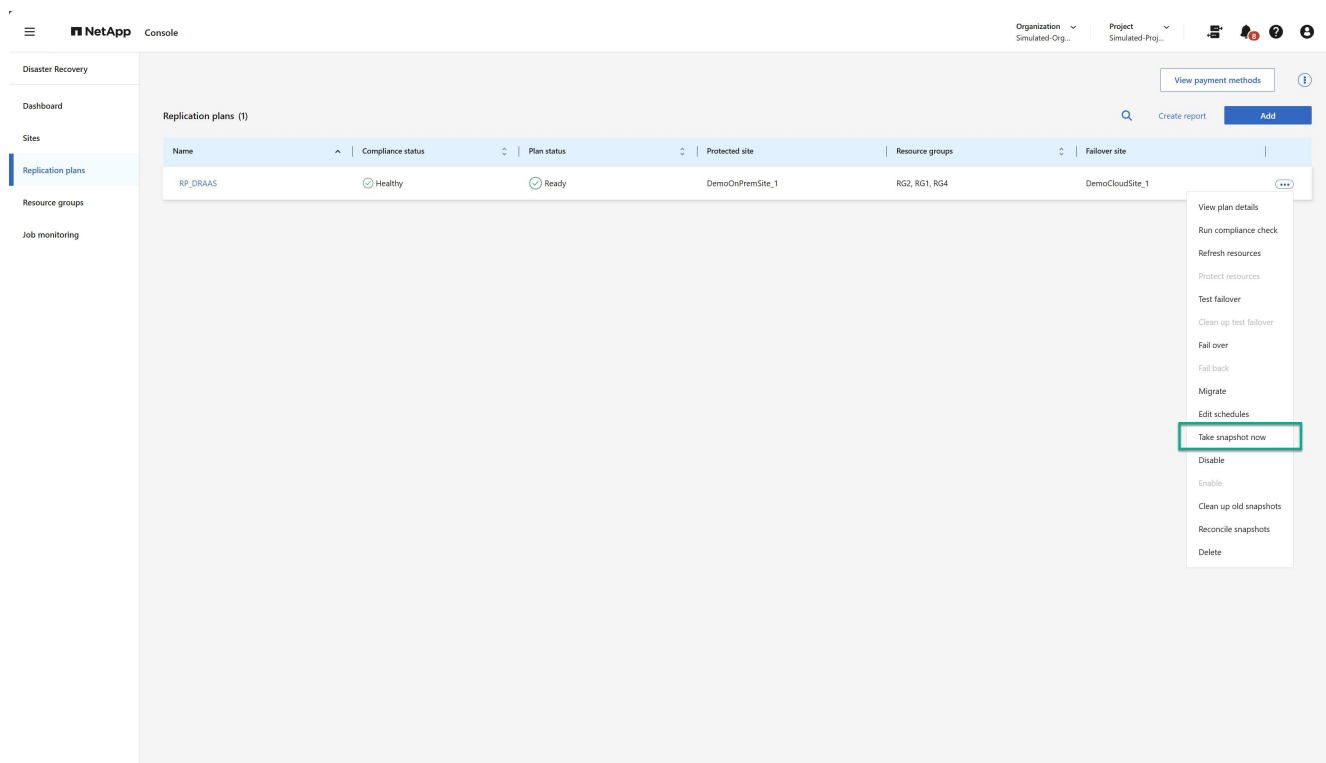


3. 在“迁移”对话框中输入信息。

立即拍摄快照

您可以随时立即拍摄复制计划的快照。此快照包含在复制计划的快照保留计数设置的NetApp Disaster Recovery考虑因素中。

1. 选择“操作”选项 ●●●复制计划旁边。
2. 要立即拍摄复制计划资源的快照，请在复制计划的操作菜单上选择*立即拍摄快照*：

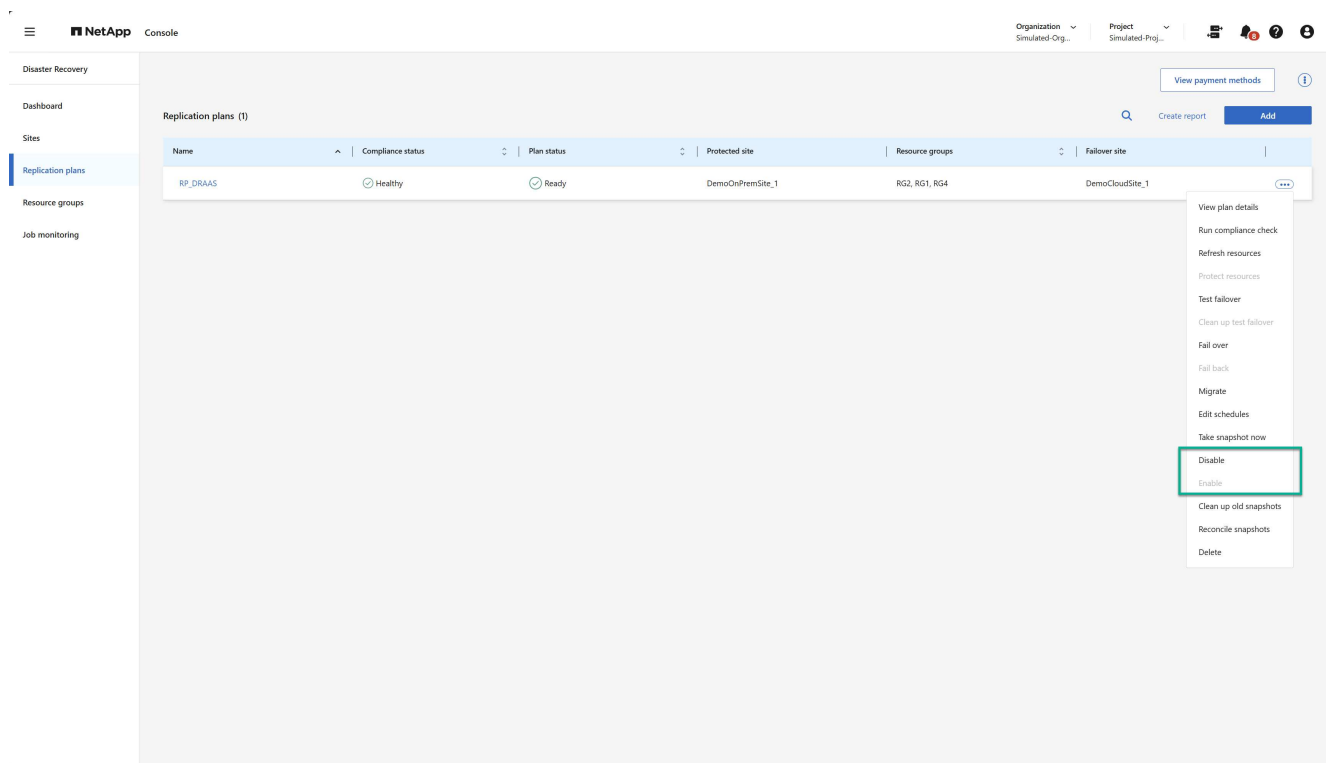


禁用或启用复制计划

您可能需要暂时停止复制计划来执行一些可能影响复制过程的操作或维护。该服务提供了停止和启动复制的方法。

1. 要暂时停止复制，请在复制计划的操作菜单上选择*禁用*。
2. 要重新启动复制，请在复制计划的操作菜单上选择*启用*。

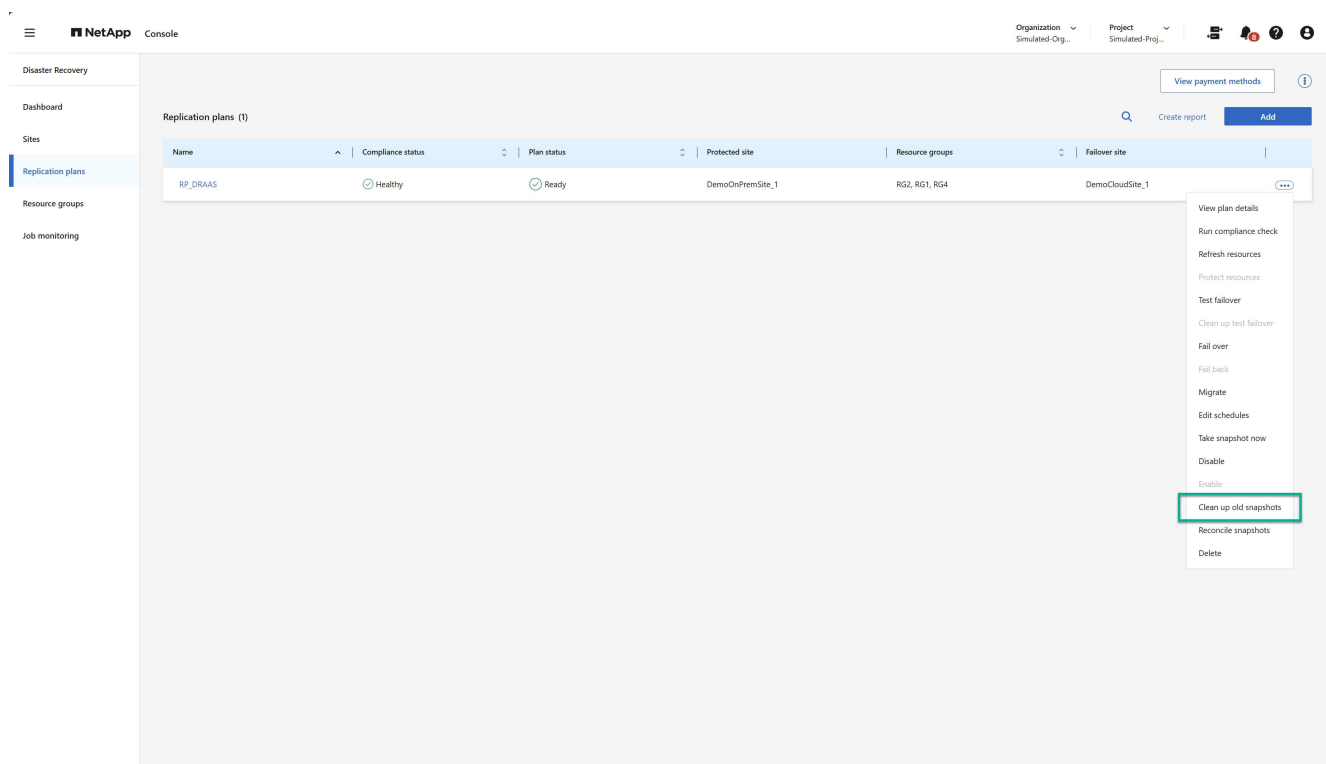
当复制计划处于活动状态时，“启用”命令将显示为灰色。当复制计划被禁用时，“禁用”命令将变灰。



清理旧快照

您可能想要清理保留在源站点和目标站点上的旧快照。如果复制计划的快照保留计数发生改变，就会发生这种情况。

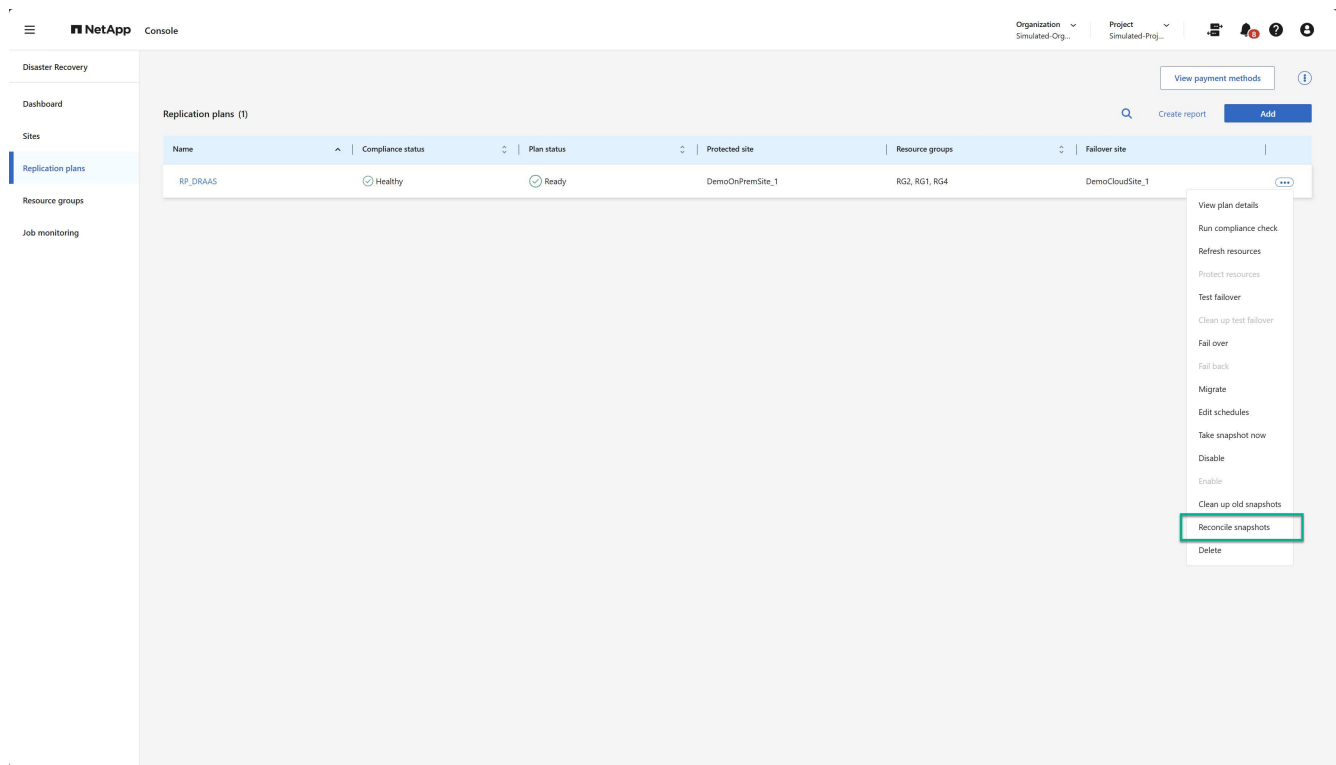
1. 选择“操作”选项 ... 复制计划旁边。
2. 要手动删除这些旧快照，请从复制计划的操作菜单中选择*清理旧快照*。



协调快照

由于该服务协调ONTAP卷快照，因此ONTAP存储管理员可以在服务不知情的情况下使用ONTAP系统管理器、ONTAP CLI 或ONTAP REST API 直接删除快照。该服务每 24 小时自动删除源上不在目标集群上的任何快照。但是，您可以根据需要执行此操作。此功能使您能够确保快照在所有站点上都是一致的。

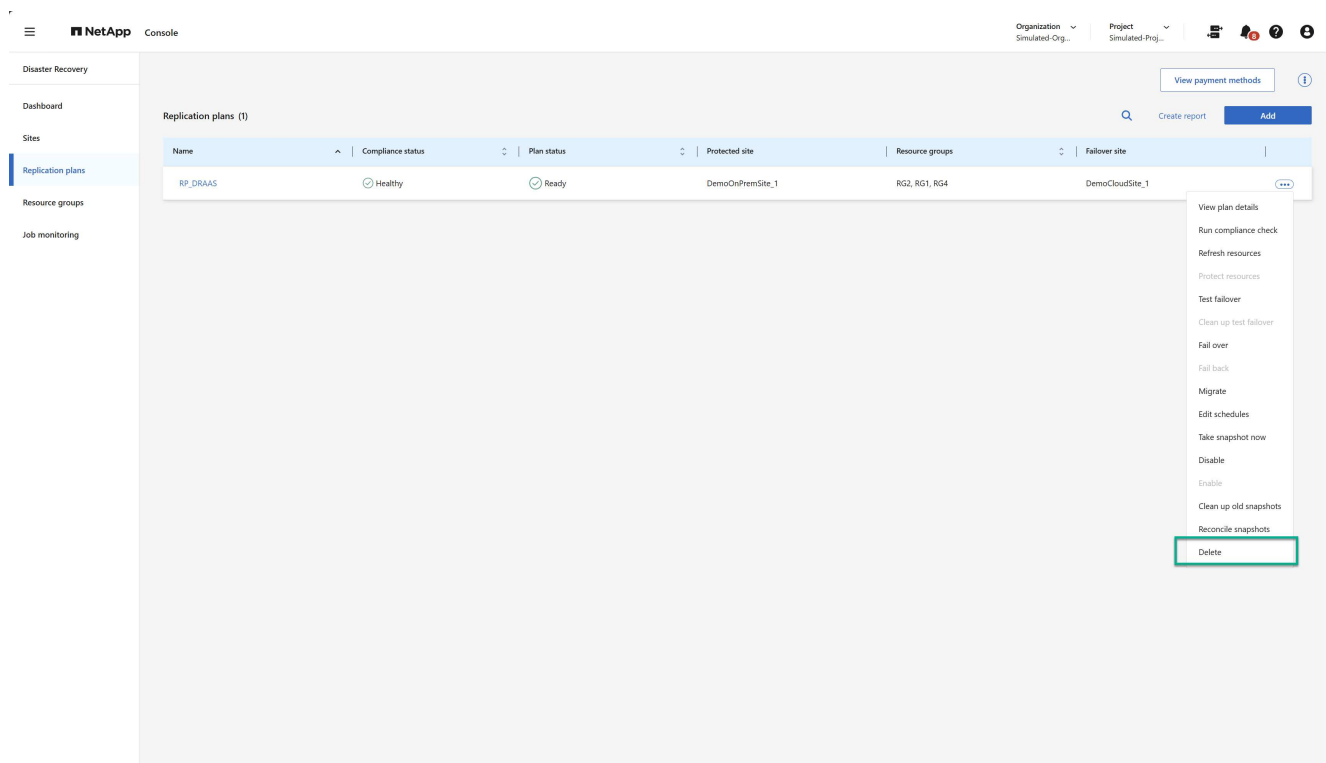
1. 选择“操作”选项  复制计划旁边。
2. 要从源集群中删除目标集群上不存在的快照，请从复制计划的操作菜单中选择*协调快照*。



删除复制计划

如果不再需要复制计划，您可以将其删除。

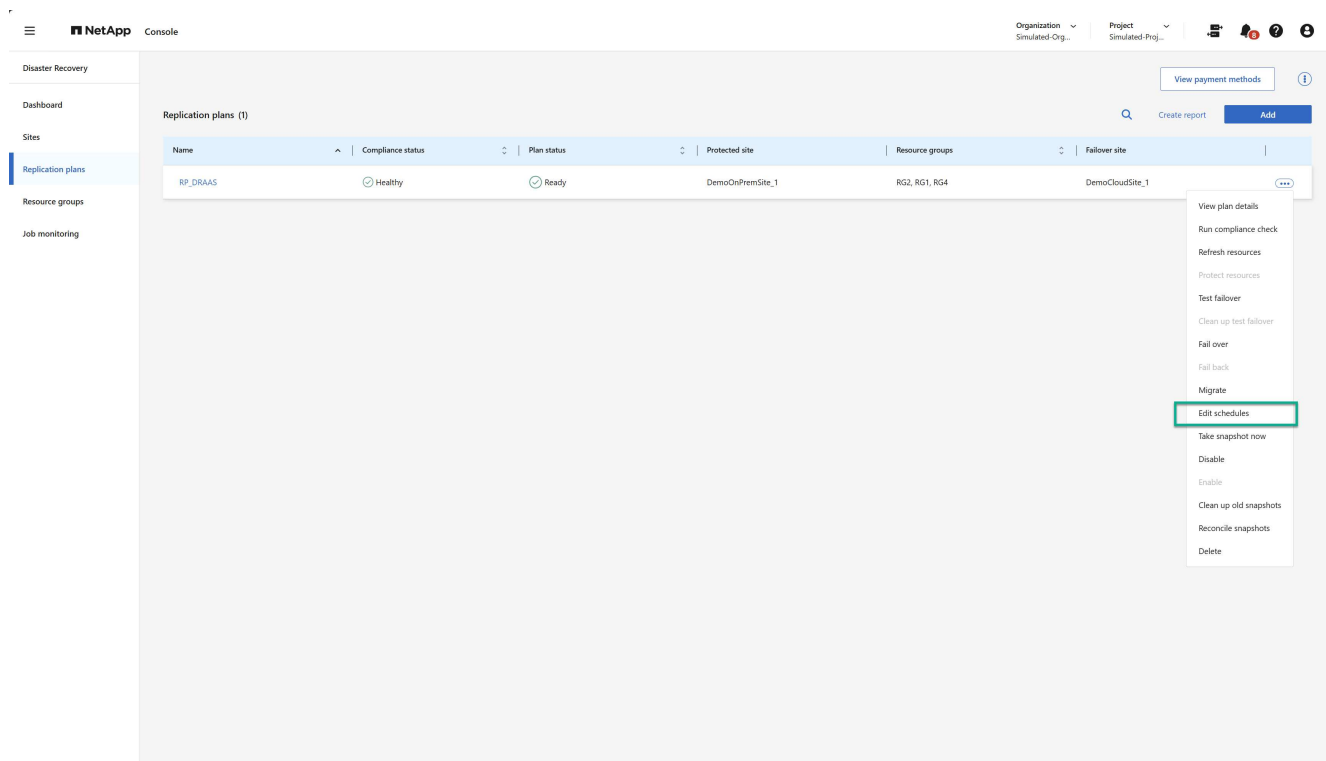
1. 选择“操作”选项  复制计划旁边。
2. 要删除复制计划，请从复制计划的上下文菜单中选择“删除”。



编辑时间表

两项操作会定期自动执行：测试故障转移和合规性检查。

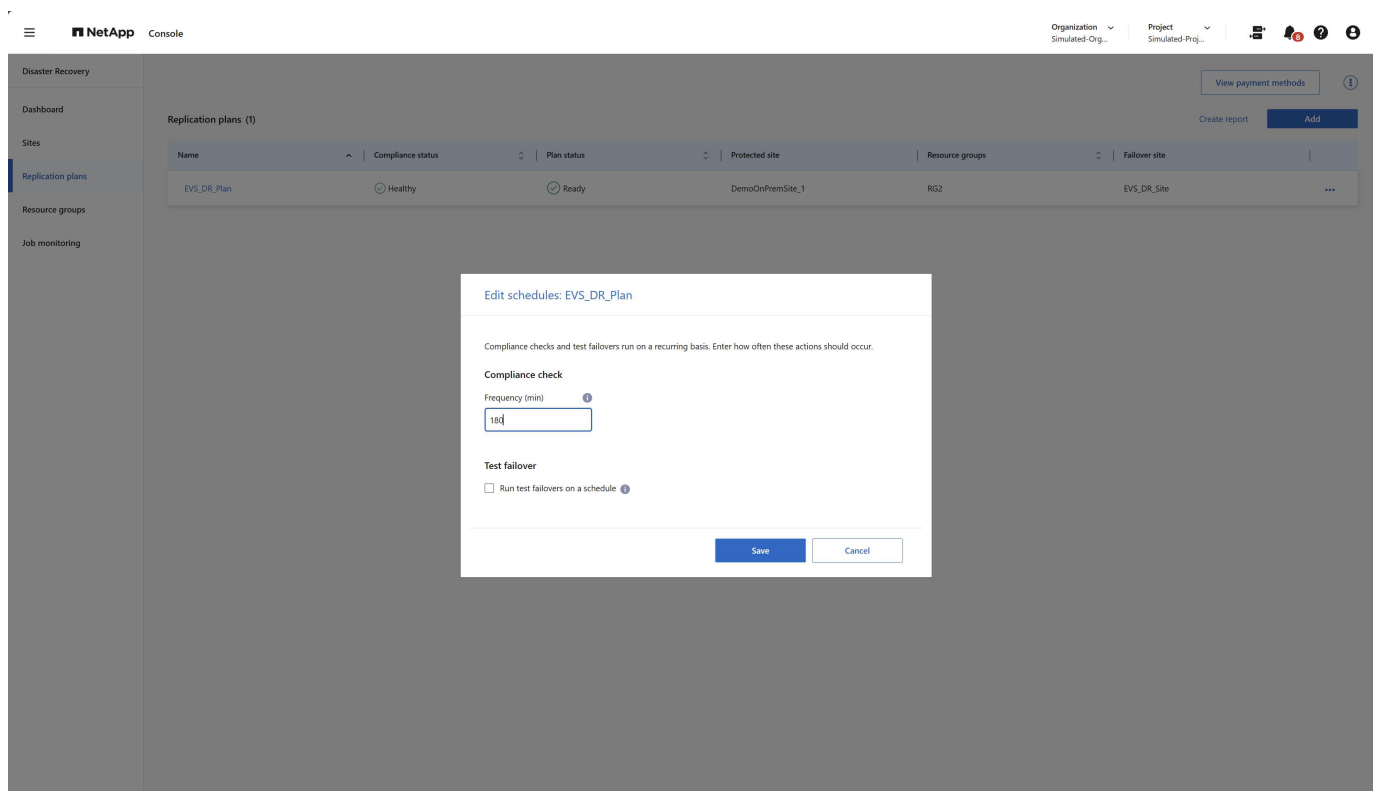
1. 选择“操作”选项  复制计划旁边。
2. 要更改这两个操作中的任一个的计划，请选择复制计划的*编辑计划*。



更改合规性检查间隔

默认情况下，每三小时执行一次合规性检查。您可以将其更改为 30 分钟到 24 小时之间的任意间隔。

要更改此间隔，请更改“编辑计划”对话框中的“频率”字段：



安排自动测试故障转移

默认情况下，测试故障转移是手动执行的。您可以安排自动测试故障转移，这有助于确保您的复制计划按预期执行。要了解有关测试故障转移过程的更多信息，请参阅[“测试故障转移过程”](#)。

安排测试故障转移的步骤

1. 选择“操作”选项 ●●●复制计划旁边。
2. 选择*运行故障转移*。
3. 选中*按计划运行测试故障转移*复选框。
4. （可选）检查*使用按需快照进行计划测试故障转移*。
5. 在重复下拉菜单中选择间隔类型。
6. 选择何时执行测试故障转移
 - a. 每周：选择星期几
 - b. 每月：选择月份中的日期
7. 选择运行测试故障转移的时间
8. 选择开始日期。
9. 决定是否希望服务自动清理测试环境，以及在清理过程开始之前希望测试环境运行多长时间。
10. 选择*保存*。

NetApp

Console

Simulator

Organization

Project

Disaster Recovery

Dashboard

Sites

Replication plans

Resource groups

Job monitoring

Replication plans (1)

Name	Compliance status
EVS_DR_Plan	Healthy

Resource groups

Fallover site

62	EVS_DR_Site	...
----	-------------	-----

View payment methods

Create report

Add

Edit schedules: EVS_DR_Plan

Compliance checks and test failovers run on a recurring basis. Enter how often these actions should occur.

Compliance check

Frequency (min)

180

Test failover

Run test failovers on a schedule

Use on-demand snapshot for scheduled test failover

Repeat

Weekly

Day of the week

Saturday

Hour

Minute

AM/PM

Start date

01

:

00

AM

2025-09-23

Automatically cleanup

10

minutes after test failover

Save

Cancel

3

4

5

6

7

8

9

10

120

NetApp Disaster Recovery常见问题解答

如果您只是想快速找到问题的答案，此常见问题解答可以为您提供帮助。

- NetApp Disaster RecoveryURL 是什么？ *对于 URL，在浏览器中输入： ["https://console.netapp.com/"](https://console.netapp.com/)访问NetApp控制台。

*您需要许可证才能使用NetApp Disaster Recovery吗？ *需要NetApp Disaster Recovery许可证才能获得完全访问权限。但是，您可以通过免费试用版进行尝试。

有关设置NetApp Disaster Recovery许可的详细信息，请参阅["设置NetApp Disaster Recovery许可"](#)。

如何访问**NetApp Disaster Recovery**？ NetApp Disaster Recovery不需要任何启用。灾难恢复选项会自动出现在NetApp Console左侧导航栏中。

知识和支持

注册以获得支持

需要进行支持注册才能获得针对NetApp Console及其存储解决方案和数据服务的技术支持。还需要支持注册才能启用Cloud Volumes ONTAP系统的关键工作流程。

注册支持并不能使NetApp获得云提供商文件服务的支持。有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品文档中的“获取帮助”。

- ["适用于ONTAP 的Amazon FSx"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

支持注册概述

激活支持权利的注册方式有两种：

- 注册您的NetApp Console帐户序列号（您的 20 位 960xxxxxxxx 序列号位于控制台中的“支持资源”页面上）。
- 在您的云提供商市场中注册与订阅相关的Cloud Volumes ONTAP序列号（这些是 20 位 909201xxxxxxxx 序列号）。

这些序列号通常称为_PAYGO 序列号_，由NetApp Console在Cloud Volumes ONTAP部署时生成。

注册两种类型的序列号可以实现开立支持票和自动生成案例等功能。通过将NetApp支持站点 (NSS) 帐户添加到控制台即可完成注册，如下所述。

注册NetApp Console以获取NetApp支持

要注册支持并激活支持权利，您的NetApp Console帐户中的一名用户必须将NetApp支持站点帐户与其控制台登录名关联。如何注册NetApp支持取决于您是否已经拥有NetApp支持站点 (NSS) 帐户。

拥有 **NSS** 帐户的现有客户

如果您是拥有 NSS 帐户的NetApp客户，则只需通过控制台注册即可获得支持。

步骤

1. 选择“管理”>“凭证”。
2. 选择*用户凭证*。
3. 选择*添加 NSS 凭据*并按照NetApp支持站点 (NSS) 身份验证提示进行操作。
4. 要确认注册过程是否成功，请选择“帮助”图标，然后选择“支持”。

*资源*页面应显示您的控制台帐户已注册以获得支持。

请注意，如果其他控制台用户尚未将NetApp支持站点帐户与其登录名关联，他们将看不到相同的支持注册状态。但是，这并不意味着您的帐户没有注册支持。只要组织中的一名用户遵循了这些步骤，您的帐户就已注册。

现有客户但没有 NSS 帐户

如果您是现有的NetApp客户，拥有现有许可证和序列号但没有 NSS 帐户，则需要创建一个 NSS 帐户并将其与您的控制台登录关联。

步骤

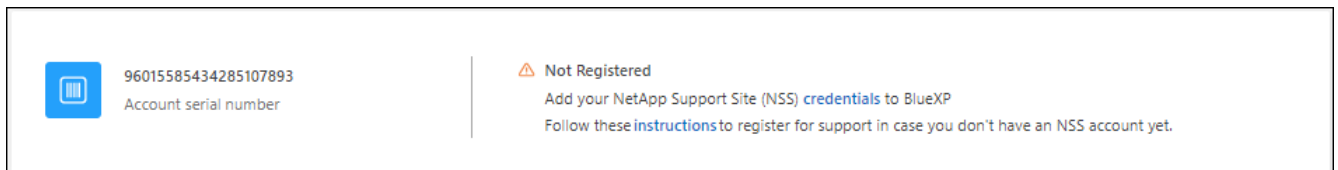
1. 通过完成以下操作创建NetApp支持站点帐户 "[NetApp支持站点用户注册表](#)"
 - a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
 - b. 请务必复制上面用于序列号字段的控制台帐户序列号（960xxxx）。这将加快账户处理速度。
2. 完成以下步骤，将您的新 NSS 帐户与您的控制台登录名关联[拥有 NSS 帐户的现有客户](#)。

NetApp全新产品

如果您是NetApp新用户并且没有 NSS 帐户，请按照以下步骤操作。

步骤

1. 在控制台的右上角，选择“帮助”图标，然后选择“支持”。
2. 从支持注册页面找到您的帐户 ID 序列号。



3. 导航至 "[NetApp 的支持注册网站](#)"并选择*我不是注册的NetApp客户*。
4. 填写必填字段（带有红色星号的字段）。
5. 在*产品线*字段中，选择*云管理器*，然后选择适用的计费提供商。
6. 从上面的步骤 2 复制您的帐户序列号，完成安全检查，然后确认您已阅读 NetApp 的全球数据隐私政策。

一封电子邮件会立即发送到提供的邮箱以完成此安全交易。如果几分钟内没有收到验证电子邮件，请务必检查您的垃圾邮件文件夹。

7. 从电子邮件中确认操作。

确认向NetApp提交您的请求并建议您创建NetApp支持站点帐户。

8. 通过完成以下操作创建NetApp支持站点帐户 "[NetApp支持站点用户注册表](#)"
 - a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
 - b. 请务必复制上面用于序列号字段的帐户序列号（960xxxx）。这将加快处理速度。

完成后

NetApp应该在此过程中与您联系。这是针对新用户的一次性入职培训。

拥有NetApp支持站点帐户后，请按照以下步骤将该帐户与您的控制台登录关联[拥有 NSS 帐户的现有客户](#)。

关联 NSS 凭据以获得Cloud Volumes ONTAP支持

需要将NetApp支持站点凭据与您的控制台帐户关联，才能为Cloud Volumes ONTAP启用以下关键工作流程：

- 注册即用即付Cloud Volumes ONTAP系统以获得支持

需要提供您的 NSS 帐户才能激活对您的系统的支持并获得对NetApp技术支持资源的访问权限。

- 自带许可证 (BYOL) 时部署Cloud Volumes ONTAP

需要提供您的 NSS 帐户，以便控制台可以上传您的许可证密钥并启用您购买的期限的订阅。这包括期限续订的自动更新。

- 将Cloud Volumes ONTAP软件升级到最新版本

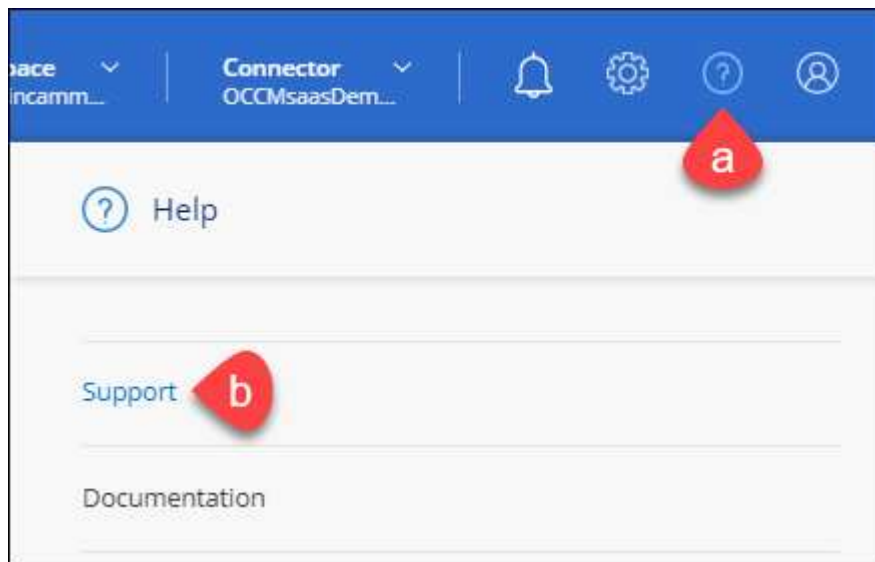
将 NSS 凭据与您的NetApp Console帐户关联与将 NSS 帐户与控制台用户登录关联不同。

这些 NSS 凭证与您的特定控制台帐户 ID 相关联。属于控制台组织的用户可以从*支持 > NSS 管理*访问这些凭据。

- 如果您有客户级帐户，则可以添加一个或多个 NSS 帐户。
- 如果您有合作伙伴或经销商帐户，则可以添加一个或多个 NSS 帐户，但不能与客户级帐户一起添加。

步骤

1. 在控制台的右上角，选择“帮助”图标，然后选择“支持”。



2. 选择*NSS 管理 > 添加 NSS 帐户*。
3. 当出现提示时，选择“继续”以重定向到 Microsoft 登录页面。

NetApp使用 Microsoft Entra ID 作为特定于支持和许可的身份验证服务的身份提供者。

4. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码以执行身份验证过程。

这些操作使控制台能够使用您的 NSS 帐户进行许可证下载、软件升级验证和未来支持注册等操作。

请注意以下事项：

- NSS 帐户必须是客户级帐户（不是访客或临时帐户）。您可以拥有多个客户级 NSS 帐户。
- 如果该帐户是合作伙伴级别帐户，则只能有一个 NSS 帐户。如果您尝试添加客户级 NSS 帐户并且合作伙伴级帐户已存在，您将收到以下错误消息：

“此帐户不允许使用 NSS 客户类型，因为已经存在不同类型的 NSS 用户。”

如果您已有客户级 NSS 帐户并尝试添加合作伙伴级帐户，情况也是如此。

- 成功登录后，NetApp将存储 NSS 用户名。

这是系统生成的映射到您的电子邮件的 ID。在*NSS 管理*页面上，您可以显示来自 [...](#) 菜单。

- 如果您需要刷新登录凭证令牌，还有一个*更新凭证*选项 [...](#) 菜单。

使用此选项会提示您再次登录。请注意，这些帐户的令牌将在 90 天后过期。我们将发布通知来提醒您此事。

获取帮助

NetApp以多种方式NetApp Console及其云服务提供支持。全天候提供广泛的免费自助支持选项，例如知识库 (KB) 文章和社区论坛。您的支持注册包含通过网络工单获取的远程技术支持。

获取云提供商文件服务的支持

有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品的文档。

- ["适用于ONTAP 的Amazon FSx"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

要获得特定于NetApp及其存储解决方案和数据服务的技术支持，请使用下面描述的支持选项。

使用自助选项

这些选项每周 7 天、每天 24 小时免费提供：

- 文档

您当前正在查看的NetApp Console文档。

- ["知识库"](#)

搜索NetApp知识库以查找有助于解决问题的文章。

- ["社区"](#)

加入NetApp Console社区，关注正在进行的讨论或创建新的讨论。

向NetApp支持创建案例

除了上述自助支持选项之外，您还可以在激活支持后与NetApp支持专家合作解决任何问题。

开始之前

- 要使用“创建案例”功能，您必须首先将您的NetApp支持站点凭据与您的控制台登录关联。 ["了解如何管理与控制台登录相关的凭据"](#)。
- 如果您要为具有序列号的ONTAP系统打开案例，那么您的 NSS 帐户必须与该系统的序列号相关联。

步骤

1. 在NetApp Console中，选择“帮助”>“支持”。
2. 在“资源”页面上，选择“技术支持”下的可用选项之一：
 - a. 如果您想通过电话与某人交谈，请选择“致电我们”。您将被引导至 netapp.com 上的一个页面，其中列出了您可以拨打的电话号码。
 - b. 选择“创建案例”向NetApp支持专家开具一张票：
 - 服务：选择与问题相关的服务。例如，* NetApp Console* 特定于控制台内的工作流或功能的技术支持问题。
 - 系统：如果适用于存储，请选择* Cloud Volumes ONTAP* 或 **On-Prem**，然后选择相关的工作环境。

系统列表位于控制台组织范围内，并且您在顶部横幅中选择了控制台代理。

- 案例优先级：选择案例的优先级，可以是低、中、高或严重。

要了解有关这些优先事项的更多详细信息，请将鼠标悬停在字段名称旁边的信息图标上。

- 问题描述：提供问题的详细描述，包括任何适用的错误消息或您执行的故障排除步骤。
- 其他电子邮件地址：如果您想让其他人知道此问题，请输入其他电子邮件地址。
- 附件（可选）：一次最多上传五个附件。

每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

ntapitdemo 

NetApp Support Site Account

Service

Select ▼

Working Enviroment

Select ▼

Case Priority 

Low - General guidance ▼

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional) 

Type here

Attachment (Optional)

No files selected

 Upload 

完成后

将会出现一个弹出窗口，其中显示您的支持案例编号。NetApp支持专家将审查您的案例并尽快回复您。

要查看支持案例的历史记录，您可以选择*设置>时间线*并查找名为“创建支持案例”的操作。最右边的按钮可让您展开操作以查看详细信息。

尝试创建案例时，您可能会遇到以下错误消息：

“您无权针对所选服务创建案例”

此错误可能意味着 NSS 帐户及其关联的记录公司与NetApp Console帐户序列号的记录公司不同（即。960xxxx）或工作环境序列号。您可以使用以下选项之一寻求帮助：

- 提交非技术案例 <https://mysupport.netapp.com/site/help>

管理您的支持案例

您可以直接从控制台查看和管理活动和已解决的支持案例。您可以管理与您的 NSS 帐户和公司相关的案例。

请注意以下事项：

- 页面顶部的案例管理仪表板提供两种视图：
 - 左侧视图显示了您提供的用户 NSS 帐户在过去 3 个月内打开的案件总数。
 - 右侧的视图根据您的用户 NSS 帐户显示了过去 3 个月内贵公司级别开设的案件总数。表中的结果反映了与您选择的视图相关的案例。
 - 您可以添加或删除感兴趣的列，并且可以过滤优先级和状态等列的内容。其他列仅提供排序功能。
- 请查看以下步骤以了解更多详细信息。
- 在每个案件级别，我们提供更新案件记录或关闭尚未关闭或待关闭状态的案件的功能。

步骤

1. 在 NetApp Console 中，选择“帮助”>“支持”。
2. 选择*案例管理*，如果出现提示，请将您的 NSS 帐户添加到控制台。

案例管理*页面显示与您的控制台用户帐户关联的 **NSS** 帐户相关的未结案例。这与出现在 ***NSS** 管理 页面顶部的 NSS 帐户相同。

3. （可选）修改表中显示的信息：
 - 在“组织的案例”下，选择“查看”以查看与您的公司相关的所有案例。
 - 通过选择精确的日期范围或选择不同的时间范围来修改日期范围。
 - 过滤列的内容。
 - 通过选择  然后选择您想要显示的列。
4. 通过选择管理现有案例  并选择其中一个可用选项：
 - 查看案例：查看有关特定案例的完整详细信息。
 - 更新案例说明：提供有关您的问题的更多详细信息，或选择*上传文件*以附加最多五个文件。

每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

- 结案：提供有关结案原因的详细信息，然后选择*结案*。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商标

NETAPP、NETAPP 徽标和NetApp商标页面上列出的标志是NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

专利

NetApp拥有的专利的最新列表可以在以下位置找到：

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

隐私政策

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

开源

通知文件提供有关NetApp软件中使用的第三方版权和许可的信息。

["NetApp Disaster Recovery通知"](#)

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。