



# 将NetApp Disaster Recovery与Amazon EVS 结合使用

## NetApp Disaster Recovery

NetApp

February 04, 2026

# 目录

将NetApp Disaster Recovery与 Amazon EVS 结合使用 . . . . .	1
使用 Amazon Elastic VMware Service 和Amazon FSx for NetApp ONTAP实现NetApp Disaster Recovery . . . . .	1
使用 Amazon EVS 和 Amazon FS for NetApp ONTAP 的NetApp Disaster Recovery解决方案概述 . . . . .	1
安装用于NetApp Disaster Recovery的NetApp Console代理 . . . . .	2
安装 . . . . .	2
为 Amazon EVS 配置NetApp Disaster Recovery . . . . .	3
为 Amazon EVS 配置NetApp Disaster Recovery概述 . . . . .	3
Amazon EVS 与NetApp Disaster Recovery的先决条件 . . . . .	3
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 . . . . .	4
将NetApp Disaster Recovery服务添加到您的 Amazon EVS NetApp Console帐户 . . . . .	5
在NetApp Disaster Recovery中为 Amazon EVS 添加站点 . . . . .	6
在NetApp Disaster Recovery中添加本地和 Amazon EVS vCenter 集群 . . . . .	7
为 Amazon EVS 创建复制计划 . . . . .	8
在NetApp Disaster Recovery概述中创建复制计划 . . . . .	8
创建复制计划：步骤 1 - 在NetApp Disaster Recovery中选择 vCenter . . . . .	8
创建复制计划：步骤 2 - 在NetApp Disaster Recovery中选择虚拟机资源 . . . . .	9
创建复制计划：步骤 3 - 在NetApp Disaster Recovery中映射资源 . . . . .	9
创建复制计划：步骤 4 - 验证NetApp Disaster Recovery中的设置 . . . . .	13
验证NetApp Disaster Recovery中一切正常 . . . . .	13
使用NetApp Disaster Recovery执行复制计划操作 . . . . .	13
故障转移 . . . . .	14
测试故障转移 . . . . .	14
运行合规性检查 . . . . .	15
刷新资源 . . . . .	15
迁移 . . . . .	15
立即拍摄快照 . . . . .	16
禁用或启用复制计划 . . . . .	16
清理旧快照 . . . . .	16
协调快照 . . . . .	16
删除复制计划 . . . . .	16
编辑时间表 . . . . .	17

# 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、网络和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存储托管数据存储备份到 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[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

源	目标	端口	详细信息
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”。

[添加系统]

2. 在添加系统页面中，选择\*On-Premises\*卡。

[添加系统映像]

3. 在 On-Premises ONTAP卡上选择 发现。

[添加系统映像]

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”。

[添加系统映像]

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”。

[添加系统映像]

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

[添加系统映像]

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

[添加系统映像]

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”。

[添加系统映像]

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

- 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%
```

- 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

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

[站点选项]

3. 从站点选项中，选择\*添加\*。

[在站点选项中添加选项]

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”。

[创建站点对话框]

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。

[站点选项]

2. 从站点选项中，选择\*添加\*。

[在站点页面上添加选项]

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”。

[添加对话框]

## 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”。

[添加 vCenter 选项]

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”。

[添加 vCenter 对话框]

## 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\*。

[复制计划屏幕]

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”。

[创建复制计划，选择 vCenter]

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。

[复制计划，应用程序页面]

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 ([25.25]) 要求您提供地图信息。
- 标有复选图标 ([25.25]) 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。

[[创建复制计划，资源映射页面](#)]

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 (▼)。

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。

[[创建复制计划、计算资源](#)]

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。

[[创建复制计划、网络资源](#)]

## 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。

[创建复制计划、网络资源]

### 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。

[创建复制计划、虚拟机资源]

### 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。

[创建复制计划、启动顺序]

## 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。

[创建复制计划、自定义客户操作系统操作]

## 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

[创建复制计划、数据存储映射]

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[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[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[操作菜单的水平点]。
2. 选择\*故障转移\*。

[故障转移菜单选项]

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”。

[故障转移对话框]

## 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[操作菜单的水平点]。
2. 从菜单中选择\*测试故障转移\*。

[测试故障转移菜单选项]

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\*。

[测试故障转移对话框]

## 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[NetApp Disaster Recovery服务中的操作菜单图标]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：

[运行合规性检查菜单选项]

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。

[刷新资源菜单选项] | *evs-rp-menu-refresh-resources.png*

## 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[NetApp Disaster Recovery服务中的操作菜单图标]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”：

[迁移菜单选项] | *evs-rp-menu-migrate.png*

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[NetApp Disaster Recovery服务中的操作菜单图标]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\*：

[立即拍摄快照菜单选项] | *evs-rp-menu-take-snapshot-now.png*

## 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。

[禁用/启用菜单选项] | *evs-rp-menu-disable-enable.png*

## 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[NetApp Disaster Recovery服务中的操作菜单图标]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\*。

[清理旧快照菜单选项] | *evs-rp-menu-cleanup-old-snapshots.png*

## 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[NetApp Disaster Recovery服务中的操作菜单图标]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\*。

[协调快照菜单选项] | *evs-rp-menu-reconcile-snapshots.png*

## 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[NetApp Disaster Recovery服务中的操作菜单图标]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”。

[删除菜单选项] | *evs-rp-menu-delete.png*

## 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[NetApp Disaster Recovery服务中的操作菜单图标]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\*。

[编辑时间表菜单选项] | *evs-rp-menu-edit-schedules.png*

## 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：

[合规性检查时间表] | *evs-rp-edit-compliance-check-schedule.png*

## 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[NetApp Disaster Recovery服务中的操作菜单图标]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\*。

[编辑计划测试故障转移] | *evs-rp-edit-schedule-test-failover.png*

## 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。