

# Site Recovery Manager 管理

Site Recovery Manager 5.8

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**威睿信息技术（中国）有  
限公司**  
北京办公室  
北京市  
朝阳区新源南路 8 号  
启皓北京东塔 8 层 801  
[www.vmware.com/cn](http://www.vmware.com/cn)

上海办公室  
上海市  
淮海中路 333 号  
瑞安大厦 804-809 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

广州办公室  
广州市  
天河路 385 号  
太古汇一座 3502 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

版权所有 © 2008-2017 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

# 目录

关于 VMware vCenter Site Recovery Manager 管理 7

更新的信息 8

## 1 Site Recovery Manager 特权、角色和权限 9

Site Recovery Manager 如何处理权限 10

Site Recovery Manager 和 vCenter Server 管理员角色 11

Site Recovery Manager 和 vSphere Replication 角色 11

管理共享恢复站点配置中的权限 11

分配 Site Recovery Manager 角色和权限 13

Site Recovery Manager 角色参考 15

## 2 复制虚拟机 19

将基于阵列的复制与 Site Recovery Manager 结合使用 19

配置基于阵列的复制 20

将 vSphere Replication 与 Site Recovery Manager 结合使用 24

复制虚拟机并启用多个时间点实例 25

将基于阵列的复制和 vSphere Replication 与 Site Recovery Manager 结合使用 26

## 3 正在创建和管理保护组 27

关于基于阵列的保护组和数据存储组 28

Site Recovery Manager 如何计算数据存储组 29

关于 vSphere Replication 保护组 30

创建保护组 30

通过文件夹对保护组进行组织 32

在保护组中添加或移除数据存储组或虚拟机 32

将清单映射应用于保护组中的所有成员 33

为保护组中的单个虚拟机配置清单映射 34

修改受保护虚拟机的设置 35

移除虚拟机的保护 36

保护组状态参考 37

虚拟机保护状态参考 38

## 4 创建、测试和运行恢复计划 39

测试恢复计划 40

测试网络和数据中心网络 40

通过运行恢复计划执行计划迁移或灾难恢复 41

使用强制恢复来运行恢复	41
测试恢复计划和运行恢复计划之间的差异	42
跨恢复站点上的多个主机执行虚拟机的测试恢复	43
创建、测试和运行恢复计划	43
创建恢复计划	44
通过文件夹对恢复计划进行组织	45
编辑恢复计划	45
测试恢复计划	46
测试恢复计划后清理	46
运行恢复计划	47
恢复虚拟机的时间点快照	48
取消测试或恢复	48
导出恢复计划步骤	49
查看和导出恢复计划历史记录	49
删除恢复计划	50
恢复计划状态参考	50
<b>5 配置恢复计划</b>	<b>53</b>
恢复计划步骤	54
创建自定义恢复步骤	54
自定义恢复步骤的类型	55
Site Recovery Manager 如何处理自定义恢复步骤故障	56
创建顶级消息提示或命令步骤	56
为单个虚拟机创建消息提示或命令步骤	57
写入命令步骤的准则	58
命令步骤的环境变量	59
运行恢复计划时挂起虚拟机	59
指定虚拟机的恢复优先级	60
配置虚拟机依赖关系	60
配置虚拟机启动和关机选项	61
<b>6 自定义虚拟机的 IP 属性</b>	<b>63</b>
手动自定义单个虚拟主机的 IP 属性	64
自定义多个虚拟机的 IP 属性	65
使用 DR IP Customizer 工具自定义多个虚拟机的 IP 属性	65
通过定义 IP 自定义规则自定义多台虚拟机的 IP 属性	78
<b>7 恢复后重新保护虚拟机</b>	<b>80</b>
Site Recovery Manager 如何使用基于阵列的复制重新保护虚拟机	81
Site Recovery Manager 如何利用 vSphere Replication 重新保护虚拟机	82
执行重新保护的前提条件	82

重新保护虚拟机 83

重新保护状态 83

## 8 通过执行故障恢复来还原恢复前的站点配置 85

执行故障恢复 86

## 9 Site Recovery Manager 与其他软件的互操作性 88

Site Recovery Manager 和 vCenter Server 88

Site Recovery Manager 如何在恢复期间与 DPM 和 DRS 交互 89

Site Recovery Manager 如何与 Storage DRS 或 Storage vMotion 交互 90

在使用 Storage DRS 或 Storage vMotion 的站点上将 Site Recovery Manager 用于基于阵列的复制 90

在使用 Storage DRS 或 Storage vMotion 的站点上将 Site Recovery Manager 与 vSphere Replication 结合使用 91

Site Recovery Manager 与 vSphere High Availability 进行交互的方式 91

Site Recovery Manager 和 vSphere PowerCLI 92

Site Recovery Manager 和 vCenter Orchestrator 92

适用于 Site Recovery Manager 的 vCenter Orchestrator 插件提供的自动化操作 92

保护 Microsoft 群集服务器和容错虚拟机 93

保护和恢复虚拟机的限制 95

## 10 高级 Site Recovery Manager 配置 98

重新配置 Site Recovery Manager 设置 98

更改 Site Recovery Manager 历史记录报告收集设置 98

更改本地站点设置 99

更改日志记录设置 100

更改恢复设置 102

更改远程站点设置 103

更改占位虚拟机创建超时时间 104

更改存储器设置 104

更改存储提供程序设置 105

更改 vSphere Replication 设置 107

修改设置以运行大型 Site Recovery Manager 环境 108

大型 Site Recovery Manager 环境的设置 109

修改长时间运行任务的设置 111

## 11 Site Recovery Manager 事件和警报 113

Site Recovery Manager 如何监控站点间的连接 113

配置 Site Recovery Manager 警报 114

Site Recovery Manager 事件参考 115

## 12 收集 Site Recovery Manager 日志文件 124

- 通过使用 Site Recovery Manager 界面收集 Site Recovery Manager 日志文件 124
- 手动收集 Site Recovery Manager 日志文件 125
- 更改 Site Recovery Manager Server 日志文件的大小和数目 125
- 配置 Site Recovery Manager 核心转储 127

### 13 Site Recovery Manager 故障排除 129

- Site Recovery Manager 运行标注时，会使命令行中的反斜线数量增加为原来的两倍 129
- 在恢复站点上同时打开多个虚拟机的电源会导致错误 130
- 向保护组添加虚拟机失败，并显示无法解析设备的错误 131
- 配置保护失败并显示占位虚拟机创建错误 131
- 快速删除和重新创建占位虚拟机失败 132
- 由于主机处于错误的状态，因此计划的迁移失败 132
- 恢复失败，在对某些虚拟机进行网络自定义期间出现超时错误 133
- 恢复失败，并显示主机和数据存储不可用错误 133
- 重新保护失败，并显示 vSphere Replication 超时错误 134
- 等待 VMware Tools 时恢复计划超时 134
- vSphere Replication 保护组同步失败 135
- 重新启动 vCenter Server 之后重新保护失败 135
- 重新扫描数据存储因存储设备未就绪失败 136

# 关于 VMware vCenter Site Recovery Manager 管理

VMware vCenter Site Recovery Manager (Site Recovery Manager) 是 VMware vCenter Server 的扩展，它提供了一个帮助您计划、测试和运行 vCenter Server 虚拟机恢复的业务连续性和灾难恢复解决方案。Site Recovery Manager 可以发现和管理复制的数据存储，并自动将清单从一个 vCenter Server 实例迁移到另一个实例。

## 目标读者

本书适用于熟悉 vSphere 及其复制技术（如基于主机的复制和复制的数据存储）的 Site Recovery Manager 管理员。此解决方案可满足要为其 vSphere 清单配置保护的管理人员的需求。它可能还适用于需要向受保护清单添加虚拟机或需要验证是否正确配置现有清单以与 Site Recovery Manager 配合使用的用户。

# 更新的信息

本《Site Recovery Manager 管理》随每一版本的产品更新或在必要时进行更新。

下表提供了《Site Recovery Manager 管理》的更新历史记录。

修订版本	描述
2020 年 8 月 5 日	在 VMware，我们重视包容性。为了向我们的客户、合作伙伴和内部社区贯彻这一原则，我们替换了内容中的一些术语。我们更新了本指南，移除了非包容性语言。
ZH_CN-001400-05	<ul style="list-style-type: none"><li>■ 在修改设置以运行大型 <a href="#">Site Recovery Manager</a> 环境中说明了 defaultMaxBootAndShutdownOpsPerCluster 和 defaultMaxBootAndShutdownOpsPerHost 的操作。</li><li>■ 在更改 <a href="#">Site Recovery Manager Server</a> 日志文件的大小和数目中更新了 <a href="#">Site Recovery Manager Server</a> 的最大日志大小。</li><li>■ 在以下主题中更新了有关 vSphere Replication 的同步超时期限信息<ul style="list-style-type: none"><li>■ <a href="#">更改 vSphere Replication 设置</a></li><li>■ <a href="#">大型 Site Recovery Manager 环境的设置</a></li><li>■ <a href="#">修改设置以运行大型 Site Recovery Manager 环境</a></li><li>■ <a href="#">重新保护失败，并显示 vSphere Replication 超时错误</a></li></ul></li><li>■ 在更改 <a href="#">vSphere Replication</a> 设置中更新了 <a href="#">allowOtherSolutionTagInRecovery</a> 设置的描述。</li></ul>
ZH_CN-001400-04	<ul style="list-style-type: none"><li>■ 在关于 <a href="#">vSphere Replication</a> 保护组中增加了针对 vSphere Replication 副本和 <a href="#">Site Recovery Manager</a> 占位虚拟机使用不同数据存储的建议。</li><li>■ 在重新保护虚拟机中增加了运行重新保护后检查恢复计划历史记录中是否存在错误的说明。</li></ul>
ZH_CN-001400-03	<ul style="list-style-type: none"><li>■ 更新了分配 <a href="#">Site Recovery Manager</a> 角色和权限，以便说明如何分配更细致的权限。</li><li>■ 增加了主题<a href="#">通过文件夹对保护组进行组织</a>和<a href="#">通过文件夹对恢复计划进行组织</a>。</li></ul>
ZH_CN-001400-02	<ul style="list-style-type: none"><li>■ 在安装存储复制适配器中更正了 myvmware.com 中的 SRA 下载路径，并阐明您可以从第三方站点下载经过认证的 SRA。</li><li>■ 纠正了报告恢复计划的 IP 地址映射、<a href="#">DR IP Customizer</a> 工具的语法和运行 <a href="#">DR IP Customizer</a> 自定义多个虚拟机的 IP 属性中 <a href="#">DR IP Reporter</a> 和 <a href="#">DR IP Customizer</a> 工具的语法。</li><li>■ 在重新配置 <a href="#">Site Recovery Manager</a> 设置中增加了升级期间或卸载并重新安装相同产品版本后不会保留高级设置的说明。</li><li>■ 增加了 <a href="#">配置 Site Recovery Manager 核心转储</a>。</li></ul>
ZH_CN-001400-01	<ul style="list-style-type: none"><li>■ 在 <a href="#">Site Recovery Manager</a> 角色参考中阐明了卸载 <a href="#">Site Recovery Manager</a> 时 <a href="#">Site Recovery Manager</a> 特权会出现的情况。</li><li>■ 在 <a href="#">Site Recovery Manager</a> 如何处理自定义恢复步骤故障中阐明了按虚拟机命令步骤失败时会出现的情况。</li><li>■ 在 <a href="#">恢复事件和存储和存储提供程序事件</a>中更正了事件名称。</li></ul>
ZH_CN-001400-00	初始版本。



# Site Recovery Manager 特权、角色和权限

# 1

Site Recovery Manager 通过为用户执行操作来提供灾难恢复。这些操作涉及管理对象（如恢复计划或保护组）和执行操作（如复制或关闭虚拟机电源）。Site Recovery Manager 使用角色和权限，以便仅具有适当角色和权限的用户才能执行操作。

Site Recovery Manager 向 vCenter Server 中添加多个角色，其中每个角色都包括用于完成 Site Recovery Manager 和 vCenter Server 任务的特权。可以为用户分配角色，以允许他们完成 Site Recovery Manager 中的任务。

## 特权

用于执行操作（如创建恢复计划或修改保护组）的权限。

## 角色

特权集合。默认角色提供特定用户（如管理保护组或执行恢复的用户）执行一组 Site Recovery Manager 任务所需的特权。一个用户在某个对象上最多只能有一个角色，但是，如果用户所属的多个组在该对象上均有角色，则这些角色可以组合。

## 权限

向某个特定用户或用户组授予的某个特定对象的角色。用户或用户组也称为主要用户。权限是角色、对象和主要用户的组合。例如，权限是用于修改特定保护组的特权。

有关 Site Recovery Manager 向 vCenter Server 添加的角色以及用户完成任务所需的特权的信息，请参见 [Site Recovery Manager 角色参考](#)。

### ■ [Site Recovery Manager 如何处理权限](#)

Site Recovery Manager 确定用户是否具有执行某项操作的权限，如配置保护或运行恢复计划中的各个步骤。此权限检查可确保对用户进行正确的身份验证，但不表示执行操作的安全性上下文。

### ■ [Site Recovery Manager 和 vCenter Server 管理员角色](#)

如果在安装 Site Recovery Manager 时，用户或用户组在 vCenter Server 实例上具有 vCenter Server 管理员角色，则该用户或用户组可获取所有 Site Recovery Manager 特权。

### ■ [Site Recovery Manager 和 vSphere Replication 角色](#)

安装 vSphere Replication 和 Site Recovery Manager 时，vCenter Server 管理员角色会继承所有 Site Recovery Manager 和 vSphere Replication 特权。

### ■ 管理共享恢复站点配置中的权限

可以将 Site Recovery Manager 配置为与共享恢复站点结合使用。共享恢复站点上的 vCenter Server 管理员必须对权限进行管理，以便每个用户都具有足够的特权来配置和使用 Site Recovery Manager，但任何用户都无权访问属于其他用户的资源。

### ■ 分配 Site Recovery Manager 角色和权限

在 Site Recovery Manager 的安装期间，具有 vCenter Server 管理员角色的用户被授予 Site Recovery Manager 的管理员角色。目前，只有 vCenter Server 管理员可以登录到 Site Recovery Manager，除非这些管理员明确为其他用户授予访问权限。

### ■ Site Recovery Manager 角色参考

Site Recovery Manager 包含一组角色。每个角色都包含一组特权，便于具有这些角色的用户完成不同操作。

## Site Recovery Manager 如何处理权限

Site Recovery Manager 确定用户是否具有执行某项操作的权限，如配置保护或运行恢复计划中的各个步骤。此权限检查可确保对用户进行正确的身份验证，但不表示执行操作的安全性上下文。

Site Recovery Manager 在用于连接站点的用户 ID 的安全性上下文中或在 Site Recovery Manager 服务运行的 ID（例如，本地系统 ID）上下文中执行各项操作。

在 Site Recovery Manager 确认用户对目标 vSphere 资源具有相应权限之后，Site Recovery Manager 可以通过使用 vSphere 管理员角色来代表用户执行操作。

对于在虚拟机上配置保护的操作，Site Recovery Manager 会在用户请求执行操作时验证用户权限。操作需要分两个阶段进行验证。

- 1 在配置过程中，Site Recovery Manager 会确认配置系统的用户是否具有在 vCenter Server 对象上完成配置所需的正确权限。例如，用户必须具备保护虚拟机和使用已恢复虚拟机要使用的辅助 vCenter Server 实例上的资源的权限。
- 2 执行配置的用户必须具备完成其正在配置的任务的正确权限。例如，用户必须具备运行恢复计划的权限。然后，Site Recovery Manager 将以 vCenter Server 管理员的身份代表用户完成任务。

因此，完成特定任务（如恢复）的用户不一定需要对 vSphere 资源执行操作的权限。该用户仅需要在 Site Recovery Manager 中运行恢复的权限。该角色将授权执行此操作，但此操作由充当管理员的 Site Recovery Manager 执行。在连接受保护站点和恢复站点时，Site Recovery Manager 可以使用所提供的管理员凭据来执行操作。

Site Recovery Manager 将使用与 vCenter Server 所用模型类似的模型为内部 Site Recovery Manager 对象维护权限数据库。Site Recovery Manager 甚至还可确认其在 vCenter Server 对象上的 Site Recovery Manager 特权。例如，Site Recovery Manager 可检查目标数据存储上的资源恢复使用权限，而不检查多个低级别权限（如分配空间）。Site Recovery Manager 还可确认远程 vCenter Server 实例上的权限。

要将 Site Recovery Manager 与 vSphere Replication 结合使用，必须为用户分配 vSphere Replication 角色及 Site Recovery Manager 角色。有关 vSphere Replication 角色的信息，请参见《vSphere Replication 管理》。

## Site Recovery Manager 和 vCenter Server 管理员角色

如果在安装 Site Recovery Manager 时，用户或用户组在 vCenter Server 实例上具有 vCenter Server 管理员角色，则该用户或用户组可获取所有 Site Recovery Manager 特权。

如果在安装 Site Recovery Manager 后为用户或用户组分配了 vCenter Server 管理员角色，则必须手动为 Site Recovery Manager 对象上的这些用户分配 Site Recovery Manager 角色。

可以将 Site Recovery Manager 角色分配给没有 vCenter Server 管理员角色的用户或用户组。在这种情况下，这些用户有权执行 Site Recovery Manager 操作，但无权执行所有 vCenter Server 操作。

## Site Recovery Manager 和 vSphere Replication 角色

安装 vSphere Replication 和 Site Recovery Manager 时，vCenter Server 管理员角色会继承所有 Site Recovery Manager 和 vSphere Replication 特权。

如果手动将 Site Recovery Manager 角色分配给用户或用户组，或者如果将 Site Recovery Manager 角色分配给非 vCenter Server 管理员用户或用户组，这些用户将不会获取 vSphere Replication 特权。Site Recovery Manager 角色不包含 vSphere Replication 角色的特权。例如，Site Recovery Manager 恢复管理员角色包含运行恢复计划的特权，包括含有 vSphere Replication 保护组的恢复计划，但不包括配置虚拟机上的 vSphere Replication 的特权。如果将 Site Recovery Manager 角色和 vSphere Replication 角色分开，则可以在不同用户之间分配响应。例如，具有 VRM 管理员角色的一个用户负责配置虚拟机上的 vSphere Replication，具有 Site Recovery Manager 恢复管理员角色的另一个用户负责运行恢复。

在某些情况下，非 vCenter Server 管理员用户可能需要执行 Site Recovery Manager 和 vSphere Replication 操作的特权。要将 Site Recovery Manager 角色与 vSphere Replication 角色结合在一起分配给一个用户，可以将该用户添加到两个用户组中。

### 示例：将 Site Recovery Manager 和 vSphere Replication 角色分配给用户

创建两个用户组后，可以为一个用户授予 Site Recovery Manager 角色和 vSphere Replication 角色的特权，而不需要该用户成为 vCenter Server 管理员。

- 1 创建两个用户组。
- 2 将 Site Recovery Manager 角色分配给一个用户组，例如，Site Recovery Manager 管理员。
- 3 将 vSphere Replication 角色分配给另一个用户组，例如 VRM 管理员。
- 4 将该用户添加到两个用户组中。

该用户具有 Site Recovery Manager 管理员角色以及 VRM 管理员角色的全部特权。

## 管理共享恢复站点配置中的权限

可以将 Site Recovery Manager 配置为与共享恢复站点结合使用。共享恢复站点上的 vCenter Server 管理员必须对权限进行管理，以便每个用户都具有足够的特权来配置和使用 Site Recovery Manager，但任何用户都无权访问属于其他用户的资源。

在共享恢复站点环境中，用户是一对 Site Recovery Manager Server 实例的所有者。具有足够权限的用户必须能够访问共享恢复站点，才能为其各自的受保护站点创建、测试和运行恢复计划。共享恢复站点上的 vCenter Server 管理员必须为每个用户创建一个单独的用户组。任何用户的用户帐户都不能是 vCenter Server 管理员组的成员。共享恢复站点唯一支持的配置是，由一个组织管理所有受保护站点和恢复站点。

---

**小心** 某些 Site Recovery Manager 角色允许用户在 Site Recovery Manager Server 上运行命令，因此只应将这些角色分配给受信任的管理员级别的用户。有关在 Site Recovery Manager Server 上运行命令的 Site Recovery Manager 角色列表，请参见 [Site Recovery Manager 角色参考](#)。

---

在共享恢复站点上，多个客户将共享一个 vCenter Server 实例。在某些情况下，多个客户可以在恢复站点上共享一个 ESXi 主机。可以将受保护站点上的资源映射到共享恢复站点上的共享资源。如果不需要单独保留客户的所有虚拟机（例如，如果所有客户都属于同一个组织），您可能会共享恢复站点上的资源。

还可以在共享恢复站点上创建独立的资源，然后将受保护站点上的资源映射到其在共享恢复站点上的专用资源。如果必须将客户的所有虚拟机全部单独保存（例如，如果所有客户属于不同的组织），您可能会使用此配置。

## 共享用户资源的准则

在共享恢复站点上配置共享用户资源的权限时，请遵循以下准则：

- 所有用户都必须对共享恢复站点上的所有 vCenter Server 文件夹具有读取访问权限。
- 请勿授予用户重命名、移动或删除数据中心或主机的权限。
- 请勿授予用户在其专用文件夹和资源池以外的位置创建虚拟机的权限。
- 请勿允许用户为并非专供自己使用的对象更改角色或分配权限。
- 为防止不同组织的资源之间出现不必要的权限传播，请勿在共享恢复站点的根文件夹、数据中心和 vCenter Server 的主机上传播权限。

## 隔离用户资源的准则

在共享恢复站点上配置隔离用户资源的权限时，请遵循以下准则：

- 在 vCenter Server 清单中向每个用户分配一个单独的虚拟机文件夹。
  - 为此文件夹设置权限，以防止任何其他用户在此文件夹中放置其虚拟机。例如，为用户文件夹上的用户设置管理员角色并激活传播选项。如果多个用户保护的虚拟机具有相同的名称，则该配置将防止可能出现的重复名称错误。
  - 将用户的所有占位虚拟机都放置在此文件夹中，以便这些占位虚拟机继承其权限。
  - 请勿向其他用户分配对此文件夹的访问权限。
- 向每个用户分配专用的资源池、数据存储和网络，并使用为文件夹配置权限的方法来配置权限。

---

**小心** 在其中隔离用户资源的部署仍假定 vSphere 站点之间存在信任关系。虽然可以隔离用户资源，但是无法隔离用户本身。如果必须保持所有用户完全隔离，则这不是一个合适的部署。

---

## 在共享恢复站点配置中查看任务和事件

在 vSphere Client 的“近期任务”面板中，有权查看某个对象的用户可以查看其他用户在此对象上启动的任务。所有用户都可查看其他用户在共享资源上执行的全部任务。例如，所有用户都可查看在共享的主机、数据中心或 vCenter Server 根文件夹上运行的任务。

Site Recovery Manager Server 的所有实例在共享恢复站点上生成的事件都具有相同的权限。可通过某一 Site Recovery Manager Server 实例查看事件的所有用户都可以通过在共享恢复站点上运行的所有 Site Recovery Manager Server 实例查看事件。

## 分配 Site Recovery Manager 角色和权限

在 Site Recovery Manager 的安装期间，具有 vCenter Server 管理员角色的用户被授予 Site Recovery Manager 的管理员角色。目前，只有 vCenter Server 管理员可以登录到 Site Recovery Manager，除非这些管理员明确为其他用户授予访问权限。

要允许其他用户访问 Site Recovery Manager，vCenter Server 管理员必须在 vSphere Web Client 的 Site Recovery Manager 界面中为这些用户授予权限。您可为每个站点分配站点范围的权限。您必须在两个站点上都添加相应的权限。

Site Recovery Manager 需要 vCenter Server 对象以及 Site Recovery Manager 对象的权限。要配置远程 vCenter Server 安装的权限，请启动另一个 vSphere Web Client 实例。在连接受保护站点和恢复站点之后，可以从这两个站点上的同一个 vSphere Web Client 实例更改 Site Recovery Manager 权限。

Site Recovery Manager 为 vCenter Server 角色和权限增添了更多权限，能够更精细地控制 Site Recovery Manager 特定任务和操作。有关每个 Site Recovery Manager 角色所包含的权限的信息，请参见 [Site Recovery Manager 角色参考](#)。

您可以通过为用户分配特定 Site Recovery Manager 对象（包括各个阵列管理器、保护组和恢复计划）的权限，为用户分配更细致的权限。您还可以通过为保护组和恢复计划文件夹以及站点的所有阵列管理器分配权限，允许用户访问保护组、恢复计划和阵列管理器的特定组。

### 步骤

- 1 在 vSphere Web Client 中，选择要为其分配权限的对象。

选项	描述
分配站点范围权限	单击 <b>站点恢复 &gt; 站点</b> ，然后选择一个站点。
为单个保护组分配权限	单击 <b>站点恢复</b> ，展开 <b>清单</b> ，单击 <b>保护组</b> ，然后选择一个保护组。
为保护组文件夹分配权限	单击 <b>站点恢复</b> ，展开 <b>清单树</b> ，单击 <b>保护组</b> ，然后选择一个保护组文件夹。您可以为根文件夹或子文件夹分配权限。
为单个恢复计划分配权限	单击 <b>站点恢复</b> ，展开 <b>清单</b> ，单击 <b>恢复计划</b> ，然后选择一个恢复计划。
为恢复计划文件夹分配权限	单击 <b>站点恢复</b> ，展开 <b>清单树</b> ，单击 <b>恢复计划</b> ，然后选择一个恢复计划文件夹。您可以为根文件夹或子文件夹分配权限。
为单个阵列管理器分配权限	单击 <b>站点恢复 &gt; 基于阵列的复制</b> ，然后选择一个阵列管理器。
为站点的所有阵列管理器分配权限	单击 <b>站点恢复</b> ，展开 <b>清单树</b> ，单击 <b>基于阵列的复制</b> ，然后选择一个站点文件夹。

- 2 在**管理**选项卡上，单击**权限**，然后单击**添加权限**图标。
- 3 为角色标识用户或组。
  - a 单击“用户和组”列中的**添加**。
  - b 从**域**下拉菜单中，选择包含用户或组的域。
  - c 在**搜索**文本框中输入用户或用户组名称，或者从**用户/组**列表选择一个名称。
  - d 单击**添加**，然后单击**确定**。
- 4 从**分配的角色**下拉菜单中选择一个角色，分配给在**步骤 3**中选择的用户或用户组。

**分配的角色**下拉菜单中包含 vCenter Server 及其插件允许分配的所有角色。Site Recovery Manager 为 vCenter Server 添加了若干个角色。

选项	操作
允许用户或用户组执行所有 Site Recovery Manager 配置和管理操作。	分配 <b>SRM 管理员</b> 角色。
允许用户或用户组管理和修改保护组以及配置虚拟机的保护。	分配 <b>SRM 保护组管理员</b> 角色。
允许用户或用户组执行恢复和测试恢复。	分配 <b>SRM 恢复管理员</b> 角色。
允许用户或用户组创建、修改和测试恢复计划。	分配 <b>SRM 恢复计划管理员</b> 角色。
允许用户或用户组测试恢复计划。	分配 <b>SRM 恢复测试管理员</b> 角色。

选择某个角色后，层次结构列表中会显示该角色包含的特权。单击层次结构列表中的某种特权可查看其描述。您无法修改每个角色包含的特权列表。

- 5 选择**传播到子项**可将所选角色应用于此角色可能会影响到的清单对象的所有子对象。
 

例如，如果某个角色包含修改文件夹特权，选择此选项可将此特权扩展到文件夹中的所有虚拟机。您可能会取消选择此选项以创建更加复杂的权限层次结构。例如，取消选择此选项可替换从层次结构树中的某个节点的根目录传播的权限，但不会替换该节点的子对象的权限。
- 6 单击**确定**将角色及其关联的特权分配给用户或用户组。
- 7 重复**步骤 2**到**步骤 6**，将角色和权限分配给其他 Site Recovery Manager 站点上的用户或用户组。

## 结果

为用户或用户组分配了指定的 Site Recovery Manager 角色。此用户或用户组具有执行该角色在您配置的 Site Recovery Manager 站点的对象上所定义的操作的特权。

## 示例：合并 Site Recovery Manager 角色

只能将一个角色分配给一个用户或用户组。如果非 vCenter Server 管理员用户需要一个以上的 Site Recovery Manager 角色的权限，可以创建多个用户组。例如，某个用户可能需要具有管理恢复计划和运行恢复计划的特权。

- 1 创建两个用户组。

- 2 将 **SRM 恢复计划管理员** 角色分配给一个组
- 3 将 **SRM 恢复管理员** 角色分配给其他组。
- 4 将该用户添加到两个用户组中。

如果成为既包含 **SRM 恢复计划管理员** 角色又包含 **SRM 恢复管理员** 角色的组的成员，用户可以管理恢复计划并运行恢复。

## Site Recovery Manager 角色参考

Site Recovery Manager 包含一组角色。每个角色都包含一组特权，便于具有这些角色的用户完成不同操作。

角色的特权和操作可以重叠。例如，Site Recovery Manager 管理员角色和 Site Recovery Manager 保护组管理员角色具有保护组的**创建**特权。使用该特权，用户可以完成用来管理保护组的一组任务中的一部分。

为两个站点上 Site Recovery Manager 对象的用户一致地分配角色，以使受保护对象和恢复对象的权限相同。

所有用户在这两个站点上至少要有 vCenter Server 的根文件夹和 Site Recovery Manager 的根节点的**系统.读取**权限。

---

**注** 如果卸载 Site Recovery Manager Server，Site Recovery Manager 会移除默认 Site Recovery Manager 角色，但会保留 Site Recovery Manager 特权。卸载 Site Recovery Manager 之后，仍可在其他角色上查看和分配 Site Recovery Manager 特权。这是标准的 vCenter Server 行为。从 vCenter Server 取消注册扩展时，不会移除特权。

---



表 1-1. Site Recovery Manager 角色

角色	此角色允许执行的操作	此角色包含的特权	此角色可以访问的 vCenter Server 清单中的 对象
Site Recovery Manager 管理员	<p>Site Recovery Manager 管理员授予执行所有 Site Recovery Manager 配置和管理操作的权限。</p> <ul style="list-style-type: none"> <li>■ 配置高级设置。</li> <li>■ 配置连接。</li> <li>■ 配置清单首选项。</li> <li>■ 配置占位数据存储。</li> <li>■ 配置阵列管理器。</li> <li>■ 管理保护组。</li> <li>■ 管理恢复计划。</li> <li>■ 执行重新保护操作。</li> <li>■ 配置虚拟机的保护。</li> <li>■ 编辑保护组。</li> <li>■ 移除保护组。</li> </ul> <p>具有此角色的用户无法运行恢复。只有具备 Site Recovery Manager 恢复管理员角色的用户可以执行恢复。</p>	<p>Site Recovery Manager.高级设置.修改 Site Recovery Manager.阵列管理器.配置 Site Recovery Manager.DiagnosticsExport.诊断.导出 Site Recovery Manager.清单首选项.修改 Site Recovery Manager.占位数据存储.配置 Site Recovery Manager.诊断 导出 Site Recovery Manager.保护组.分配给计划 Site Recovery Manager.保护组.创建 Site Recovery Manager.保护组.修改 Site Recovery Manager.保护组.移除 Site Recovery Manager.保护组.从计划移除 Site Recovery Manager.恢复历史记录.查看 删除的计划 Site Recovery Manager.恢复计划.配置 Site Recovery Manager.恢复计划.创建 Site Recovery Manager.恢复计划.修改 Site Recovery Manager.恢复计划.移除 Site Recovery Manager.恢复计划.重新保护 Site Recovery Manager.恢复计划.测试 Site Recovery Manager.远程站点.修改 数据存储.复制.保护 数据存储.复制.取消保护.停止 资源.恢复使用 虚拟机.SRM 保护.保护 虚拟机.SRM 保护.停止</p>	<ul style="list-style-type: none"> <li>■ 虚拟机</li> <li>■ 数据存储</li> <li>■ vCenter Server 文件夹</li> <li>■ 资源池</li> <li>■ Site Recovery Manager 服务实例</li> <li>■ 网络</li> <li>■ Site Recovery Manager 文件夹</li> <li>■ 保护组</li> <li>■ 恢复计划</li> <li>■ 阵列管理器</li> </ul>
Site Recovery Manager 保护组管理员	<p>Site Recovery Manager 保护组管理员角色允许用户管理保护组。</p> <ul style="list-style-type: none"> <li>■ 创建保护组。</li> <li>■ 修改保护组。</li> <li>■ 将虚拟机添加到保护组。</li> <li>■ 删除保护组。</li> <li>■ 配置虚拟机的保护。</li> <li>■ 删除虚拟机的保护。</li> </ul> <p>具有此角色的用户无法执行/测试恢复或创建/修改恢复计划。</p>	<p>Site Recovery Manager.保护组.创建 Site Recovery Manager.保护组.修改 Site Recovery Manager.保护组.移除 数据存储.复制.保护 数据存储.复制.取消保护.停止 资源.恢复使用 虚拟机.SRM 保护.保护 虚拟机.SRM 保护.停止</p>	<ul style="list-style-type: none"> <li>■ Site Recovery Manager 文件夹</li> <li>■ 保护组</li> </ul>



表 1-1. Site Recovery Manager 角色（续）

角色	此角色允许执行的操作	此角色包含的特权	此角色可以访问的 vCenter Server 清单中的 对象
Site Recovery Manager 恢复管理员	<p>Site Recovery Manager 恢复管理员角色允许用户执行恢复和重新保护操作。</p> <ul style="list-style-type: none"> <li>■ 从恢复计划中删除保护组。</li> <li>■ 测试恢复计划。</li> <li>■ 运行恢复计划。</li> <li>■ 运行重新保护操作。</li> <li>■ 在虚拟机上配置自定义命令步骤。</li> <li>■ 查看删除的恢复计划。</li> <li>■ 编辑虚拟机恢复属性。</li> </ul> <p>具有此角色的用户无法配置虚拟机的保护或创建/修改恢复计划。</p>	<p>Site Recovery Manager.保护组.从计划移除</p> <p>Site Recovery Manager.恢复计划.修改</p> <p>Site Recovery Manager.恢复计划.测试</p> <p>Site Recovery Manager.恢复计划.恢复</p> <p>Site Recovery Manager.恢复计划.重新保护</p> <p>Site Recovery Manager.恢复计划.配置.配置命令</p> <p>Site Recovery Manager.恢复历史记录.查看删除的计划</p>	<ul style="list-style-type: none"> <li>■ 保护组</li> <li>■ 恢复计划</li> <li>■ Site Recovery Manager 服务实例</li> </ul>

表 1-1. Site Recovery Manager 角色（续）

角色	此角色允许执行的操作	此角色包含的特权	此角色可以访问的 vCenter Server 清单中的 对象
Site Recovery Manager 恢复计划管理员	<p>Site Recovery Manager 恢复计划管理员角色允许用户创建和测试恢复计划。</p> <ul style="list-style-type: none"> <li>■ 将保护组添加到恢复计划。</li> <li>■ 从恢复计划中删除保护组。</li> <li>■ 在虚拟机上配置自定义命令步骤。</li> <li>■ 创建恢复计划。</li> <li>■ 测试恢复计划。</li> <li>■ 取消恢复计划测试。</li> <li>■ 编辑虚拟机恢复属性。</li> </ul> <p>具有此角色的用户无法配置虚拟机的保护或执行恢复/重新保护操作。</p>	<p>Site Recovery Manager.保护组.分配给计划</p> <p>Site Recovery Manager.保护组.从计划移除</p> <p>Site Recovery Manager.恢复计划.配置命令</p> <p>Site Recovery Manager.恢复计划.创建</p> <p>Site Recovery Manager.恢复计划.修改</p> <p>Site Recovery Manager.恢复计划.移除</p> <p>Site Recovery Manager.恢复计划.测试资源.恢复使用</p>	<ul style="list-style-type: none"> <li>■ 保护组</li> <li>■ 恢复计划</li> <li>■ vCenter Server 文件夹</li> <li>■ 数据存储</li> <li>■ 资源池</li> <li>■ 网络</li> </ul>
Site Recovery Manager 测试管理员	<p>Site Recovery Manager 测试管理员角色仅允许用户测试恢复计划。</p> <ul style="list-style-type: none"> <li>■ 测试恢复计划。</li> <li>■ 取消恢复计划测试。</li> <li>■ 编辑虚拟机恢复属性。</li> </ul> <p>具有此角色的用户无法配置虚拟机的保护、创建保护组/恢复计划或执行恢复/重新保护操作。</p>	<p>Site Recovery Manager.恢复计划.修改</p> <p>Site Recovery Manager.恢复计划.测试</p>	<p>恢复计划</p>

# 复制虚拟机

# 2

创建保护组之前，您必须在要保护的虚拟机上配置复制。

您可以通过使用基于阵列的复制、vSphere Replication 或两者的组合复制虚拟机。

本章讨论了以下主题：

- 将基于阵列的复制与 Site Recovery Manager 结合使用
- 将 vSphere Replication 与 Site Recovery Manager 结合使用
- 将基于阵列的复制和 vSphere Replication 与 Site Recovery Manager 结合使用

## 将基于阵列的复制与 Site Recovery Manager 结合使用

使用基于阵列的复制时，受保护站点中的一个或多个存储阵列会将数据复制到恢复站点中的对等阵列。通过存储复制适配器 (SRA)，您可以将 Site Recovery Manager 与各种阵列集成。

要将基于阵列的复制与 Site Recovery Manager 配合使用，必须先配置复制，然后才能将 Site Recovery Manager 配置为使用该复制。

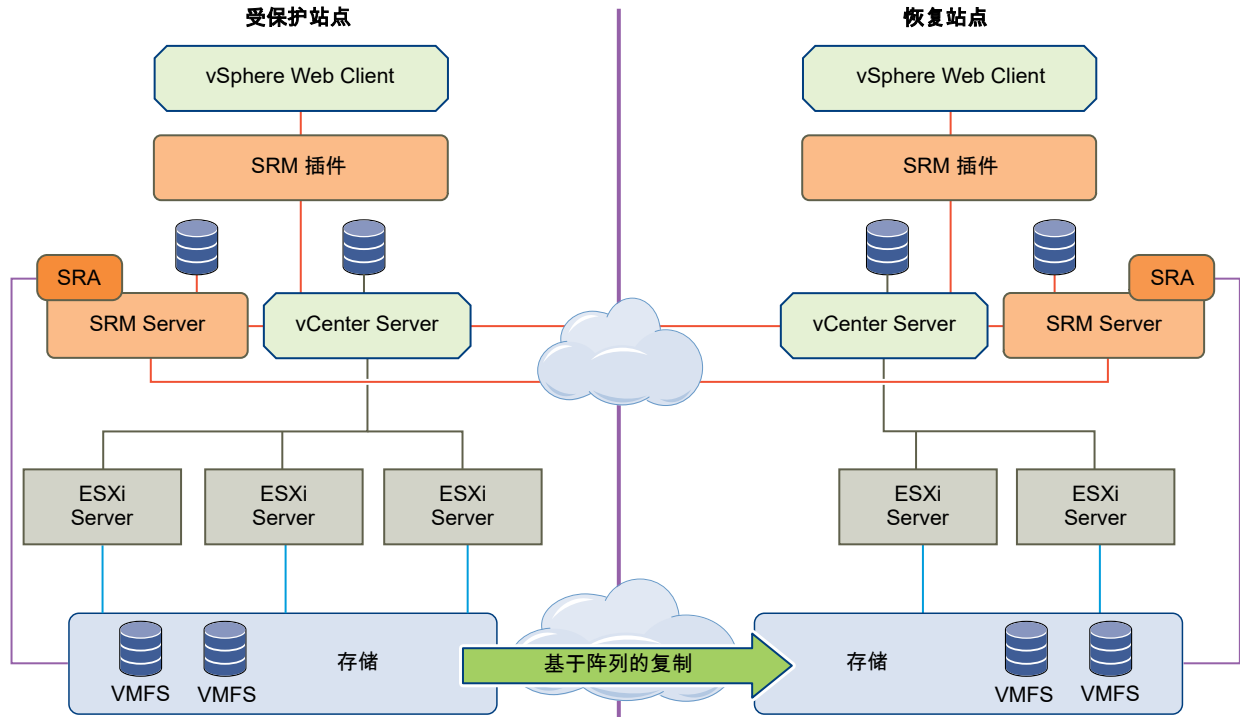
如果您的存储阵列支持一致性组，Site Recovery Manager 将与 vSphere Storage DRS 和 vSphere Storage vMotion 兼容。您可以使用 Storage DRS 和 Storage vMotion 在 Site Recovery Manager 所保护的一致性组内移动虚拟机。如果存储阵列不支持一致性组，则无法将 Storage DRS 和 Storage vMotion 与 Site Recovery Manager 结合使用。

可以保护包含使用 VMware vSphere Flash Read Cache 存储的磁盘的虚拟机。由于可能未针对 Flash Read Cache 配置虚拟机恢复，Site Recovery Manager 会在恢复站点上启动虚拟机时禁用磁盘上的 Flash Read Cache。Site Recovery Manager 将预留设置为零。在配置为使用 vSphere Flash Read Cache 的虚拟机上执行恢复之前，请通过 vSphere Web Client 记录虚拟机的缓存预留信息。恢复后，可以将虚拟机迁移到具有 Flash Read Cache 存储的主机，并手动还原虚拟机上的原始 Flash Read Cache 设置。

## 存储复制适配器

存储复制适配器不属于 Site Recovery Manager 版本的一部分。您的阵列供应商可对其进行开发和支持。您必须在 Site Recovery Manager Server 主机上安装一个特定于每个与 Site Recovery Manager 配合使用的阵列的 SRA。Site Recovery Manager 支持使用多个 SRA。

图 2-1. Site Recovery Manager 架构与基于阵列的复制



## 配置基于阵列的复制

要保护使用基于阵列的复制所复制的虚拟机，必须在每个站点配置存储复制适配器 (SRA)。

### 安装存储复制适配器

如果使用的是基于阵列的复制，则必须安装特定于与 Site Recovery Manager 配合使用的每个存储阵列的存储复制适配器 (SRA)。SRA 是阵列供应商提供的程序，可使 Site Recovery Manager 支持特定类型的阵列。

您必须在受保护站点和恢复站点的 Site Recovery Manager Server 主机上安装相应的 SRA。如果使用多种类型的存储阵列，必须针对两个 Site Recovery Manager Server 主机上的每种阵列类型安装 SRA。

**注** 您可以配置 Site Recovery Manager 以使用多种类型的存储阵列，但不能将一个虚拟机的虚拟机磁盘存储在不同供应商的多个阵列上。必须将一个虚拟机的所有磁盘存储在同一阵列上。

存储复制适配器随其安装说明一起提供。您必须安装与特定 Site Recovery Manager 版本对应的 SRA 版本。在两个站点上安装相同版本的 SRA。请勿混用 SRA 版本。

如果使用的是 vSphere Replication，则不需要 SRA。

### 前提条件

- 通过查阅适用于 Site Recovery Manager 的《VMware 兼容性指南》，针对您的存储类型检查 SRA 的可用性，网址为：<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra>。

- 可以下载 SRA，方法是转至 <https://my.vmware.com/web/vmware/downloads>，选择 **VMware vCenter Site Recovery Manager > 下载产品**，然后选择**驱动程序和工具 > 存储复制适配器 > 转至下载**。
- 如果从其他供应商站点获取 SRA，请通过检查适用于 Site Recovery Manager 的《VMware 兼容性指南》确认该 SRA 是否已通过您所使用的 Site Recovery Manager 版本认证，网址为：<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra>。
- 请阅读随 SRA 提供的文档。SRA 并非支持存储阵列支持的所有功能。SRA 提供的文档会详细介绍 SRA 支持和需要的功能。例如，HP 和 EMC 具有详细的物理要求，必须满足这些要求，SRA 才能按预期执行。
- 在安装 SRA 之前安装 Site Recovery Manager Server。
- SRA 可能需要安装供应商提供的其他组件。您可能需要在 Site Recovery Manager Server 主机上安装其中某些组件。其他组件可能只需要由 Site Recovery Manager Server 通过网络进行访问。有关这类要求的最新信息，请查看所安装的 SRA 的发行说明和自述文件。
- 启用存储阵列的创建复制设备快照副本的功能。请参见 SRA 文档。

#### 步骤

- 1 在每个 Site Recovery Manager Server 主机上安装 SRA。

安装程序会将 SRA 安装在 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra 中。

- 2 在 vSphere Web Client 中，转到**站点恢复 > 站点**，然后选择一个站点。
- 3 在**监控**选项卡中，单击 **SRA**，然后单击**重新扫描 SRA** 按钮。

此操作将刷新 SRA 信息，以使 Site Recovery Manager 能够发现 SRA。

### 配置阵列管理器

配对受保护站点和恢复站点之后，可配置其各自的阵列管理器，以便 Site Recovery Manager 可发现复制的设备、计算数据存储组并启动存储操作。

连接这些站点之后，通常仅需要配置阵列管理器一次。除非阵列管理器连接信息或凭据发生更改，或者要使用不同的阵列集，否则无需重新配置阵列管理器。

#### 前提条件

- 按照 Site Recovery Manager 的安装和配置的连接受保护站点和恢复站点中所述连接相应站点。
- 如**安装存储复制适配器**中所述，在两个站点上均安装 SRA。

#### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 基于阵列的复制**。
- 2 在**对象**选项卡中，单击该图标以添加阵列管理器。
- 3 从以下两个选项中选择：
  - 添加一对阵列管理器

- 添加一个阵列管理器。

- 4 为阵列管理器选择一个站点或一对站点，然后单击**下一步**。
- 5 从 **SRA 类型** 下拉菜单中，选择想要 Site Recovery Manager 使用的阵列管理器类型。

如果未显示任何管理器类型，请重新扫描 SRA 或检查是否已在 Site Recovery Manager Server 主机上安装 SRA。

- 6 在**显示名称**文本框中键入阵列的名称。

请使用描述性名称，以便您轻松识别与此阵列管理器关联的存储。

- 7 为所选 SRA 类型提供所需信息。

有关如何在这些文本框中填写信息的详细信息，请参见 SRA 供应商提供的文档。尽管文本框因 SRA 不同而异，但存在一些通用文本框，包括 IP 地址、协议信息、阵列名称和 IP 地址之间的映射关系以及用户名和密码。

- 8 单击**下一步**。

- 9 如果您选择添加一对阵列管理器，请配置阵列对，然后单击**下一步**。

如果已在对等站点上创建阵列管理器，也可以在单选项模式下配置阵列对。

- 10 从列表中选择阵列对。

- 11 查看配置，然后单击**完成**。

- 12 如有需要，请重复步骤以配置恢复站点的阵列管理器。

## 重新扫描阵列以检测配置更改

默认情况下，Site Recovery Manager 每 24 小时重新扫描一次阵列，以查看阵列中的设备配置是否有更改。但是，可随时强制执行阵列重新扫描。

通过更改“高级设置”中的 `storage.minDsGroupComputationInterval` 选项，可以重新配置 Site Recovery Manager 执行定期阵列扫描的频率。请参见[更改存储设置](#)。

如果对阵列管理器进行配置，Site Recovery Manager 会根据其发现的一组复制存储设备计算数据存储组。如果在任一站点更改阵列的配置以添加或移除设备，Site Recovery Manager 必须重新扫描阵列并重新计算数据存储组。

### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 基于阵列的复制**。
- 2 选择阵列。
- 3 在**管理**选项卡中，选择**阵列对**。

**阵列对**选项卡会提供有关阵列中所有存储设备的信息，包括本地设备名称、配对设备、复制方向、设备所属的保护组、数据存储的本地或远程状态以及每个 SRA 设备的一致性组 ID。

- 4 右键单击阵列对并选择**发现设备**以重新扫描阵列并重新计算数据存储组。

## 编辑阵列管理器

使用“编辑阵列管理器”向导修改阵列管理器的名称或其他设置，例如 IP 地址或用户名和密码。

有关如何填写适配器字段的详细信息，请参见 SRA 供应商提供的文档。尽管各 SRA 的字段会有所不同，但某些公共字段还是一致的，如 IP 地址、协议信息、阵列名称和 IP 地址之间的映射关系以及用户名和密码。

### 步骤

1 在 vSphere Web Client 中，单击**站点恢复 > 基于阵列的复制**。

2 右键单击一个阵列并选择**编辑阵列管理器**。

3 在**显示名称**字段中修改阵列的名称。

请使用描述性名称，以便您轻松识别与此阵列管理器关联的存储。您不能修改阵列管理器类型。

4 修改适配器信息。

这些字段由 SRA 创建。

5 启用阵列对，然后单击**下一步**。

6 单击**完成**完成阵列管理器的修改。

## 为交换文件指定非复制数据存储

每个虚拟机都需要一个交换文件。默认情况下，vCenter Server 会在与其他虚拟机文件相同的数据存储中创建交换文件。要阻止 Site Recovery Manager 复制交换文件，可以将虚拟机配置为在非复制数据存储中创建这些交换文件。

正常情况下，应将交换文件和其他虚拟机文件保存在同一数据存储中。但是，您可能需要阻止复制交换文件，以避免过度占用网络带宽。一些存储供应商也建议不要复制交换文件。所以，请仅在必要时才阻止复制交换文件。

---

**注** 如果对交换文件使用的是非复制数据存储，则必须为受保护站点和恢复站点上的所有受保护主机和群集创建非复制数据存储。非复制数据存储必须对群集中的所有主机可见，否则 vMotion 将无法工作。

---

### 步骤

1 在 vSphere Web Client 中，选择一台主机，然后选择**管理 > 设置**。

2 在**虚拟机**下，单击**交换文件位置**然后单击**编辑**。

3 选择**使用特定数据存储**。

4 选择一个非复制数据存储以包含交换文件，然后单击**确定**。

5 关闭再打开该主机上所有虚拟机的电源。

重置客户机操作系统是不够的。对交换文件的位置所做的更改在您关闭再打开虚拟机的电源后生效。

6 浏览为交换文件选择的数据存储，并确认虚拟机具有 VSWP 文件。

## 将 vSphere Replication 与 Site Recovery Manager 结合使用

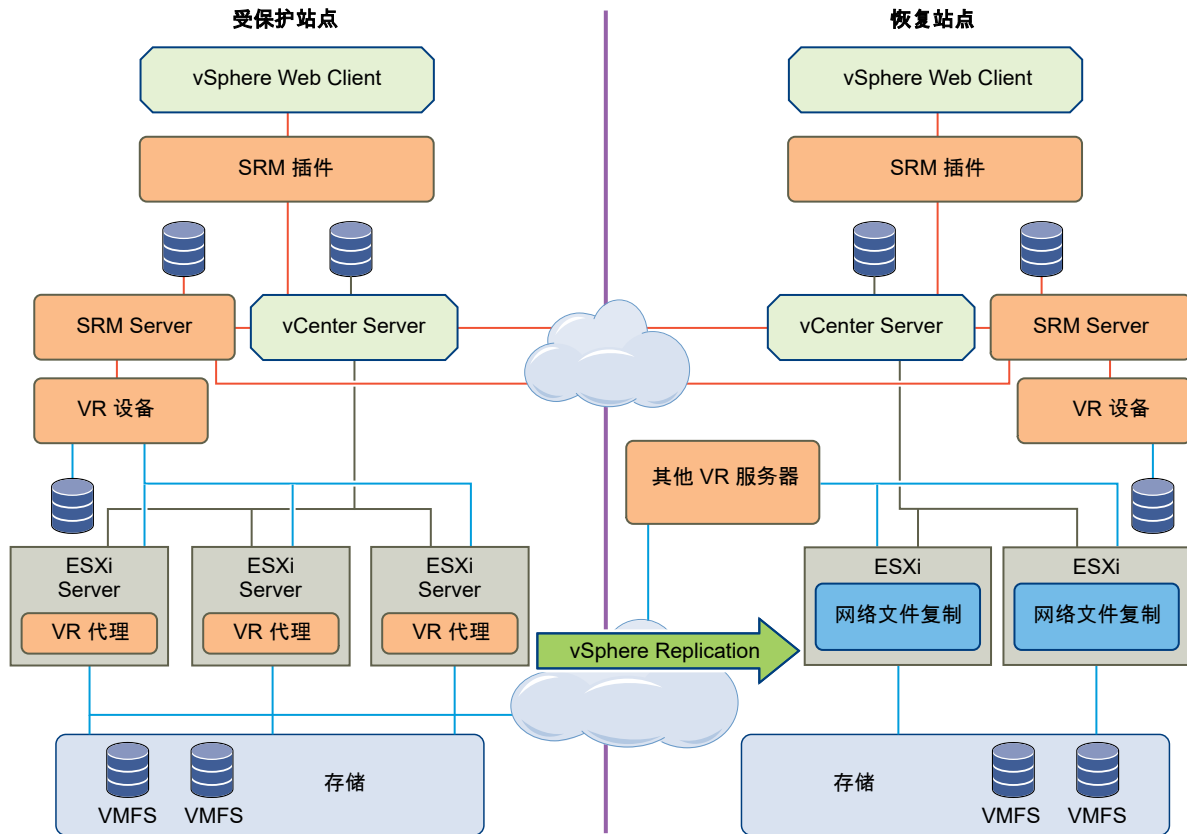
Site Recovery Manager 可使用 vSphere Replication 将数据复制到恢复站点中的服务器。

先前版本的 Site Recovery Manager 包括 vSphere Replication 设备。在先前的版本中，可在 Site Recovery Manager 界面中配置 vSphere Replication。在此版本中，您可以在虚拟机上部署 vSphere Replication 设备并配置 vSphere Replication，而不需要使用 Site Recovery Manager。有关部署和配置 vSphere Replication 的信息，请参见 vSphere Replication 文档，网址为 <https://www.vmware.com/support/pubs/vsphere-replication-pubs.html>。

vSphere Replication 不要求使用存储阵列。vSphere Replication 存储复制源和目标可以是任意存储设备，包括但不限于存储阵列。

可以配置 vSphere Replication 以在恢复站点中定期创建和保留受保护虚拟机的快照。生成虚拟机的多个时间点 (PIT) 快照后，您可在恢复站点中保留虚拟机的多个副本。每个快照反映了在某一特定时间点虚拟机的状态。使用 vSphere Replication 执行恢复时，您可以选择要恢复的快照。

图 2-2. 将 Site Recovery Manager 架构与 vSphere Replication 结合使用



## 将 vSphere Replication 和 Site Recovery Manager 与 vSphere Storage vMotion 和 vSphere Storage DRS 结合使用

vSphere Replication 在受保护站点上与 vSphere Storage vMotion 和 vSphere Storage DRS 兼容。可以使用 Storage vMotion 和 Storage DRS 移动受 vSphere Replication 保护的虚拟机的磁盘文件，而不会对复制产生任何影响。



## 将 vSphere Replication 和 VMware Virtual SAN 存储与 Site Recovery Manager 结合使用

可以将 VMware Virtual SAN 存储与 vSphere Replication 和 Site Recovery Manager 结合使用。

### 复制虚拟机并启用多个时间点实例

您可以恢复特定时间点 (PIT) (如上次已知的一致状态) 的虚拟机。

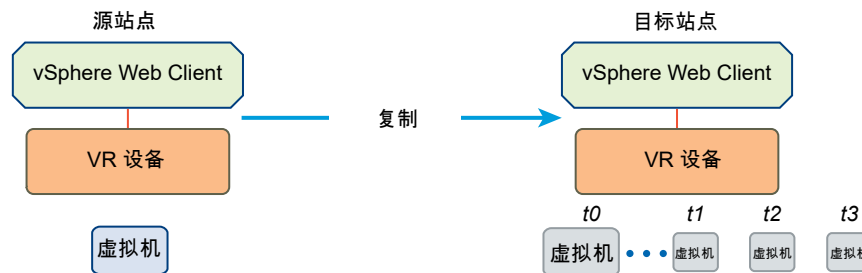
在虚拟机上配置 vSphere Replication 时，您可以在恢复设置中启用保留多个时间点 (PIT) 实例。vSphere Replication 基于您指定的保留策略在目标站点上保留虚拟机的多个快照实例。vSphere Replication 最多支持 24 个快照实例。恢复虚拟机后，您可以将其恢复到特定快照。

复制过程中，vSphere Replication 会将虚拟机的各个方面均复制到目标站点，包括任何潜在的病毒和损坏的应用程序。如果虚拟机遭受病毒攻击或被损坏，而您已将 vSphere Replication 配置为保留 PIT 快照，则可以恢复虚拟机，然后将其恢复到未损坏状态下的虚拟机快照。

例如，您可以使用 PIT 实例恢复数据库的上一个已知的正常状态。

**注** vSphere Replication 不会复制虚拟机快照。

图 2-3. 恢复某个时间点 (PIT) 的虚拟机



在恢复期间，Site Recovery Manager 仅恢复最新的 PIT 快照。要恢复较旧的快照，您必须在 Site Recovery Manager 界面的高级设置中启用 **vrReplication > preserveMpitImagesAsSnapshots** 选项。请参见[更改 vSphere Replication 设置](#)。

要从较旧的 PIT 快照中恢复虚拟机，您必须在恢复之后将虚拟机手动恢复到该快照。请参见[恢复虚拟机的时间点快照](#)。

如果您对已经配置了 IP 自定义的虚拟机恢复 PIT 快照，Site Recovery Manager 仅会将自定义应用到最新的 PIT 快照。如果您对已经配置了 IP 自定义的虚拟机恢复较旧的快照，必须手动配置 IP 设置。

## 将基于阵列的复制和 vSphere Replication 与 Site Recovery Manager 结合使用

可以在您的 Site Recovery Manager 部署中结合使用基于阵列的复制和 vSphere Replication。

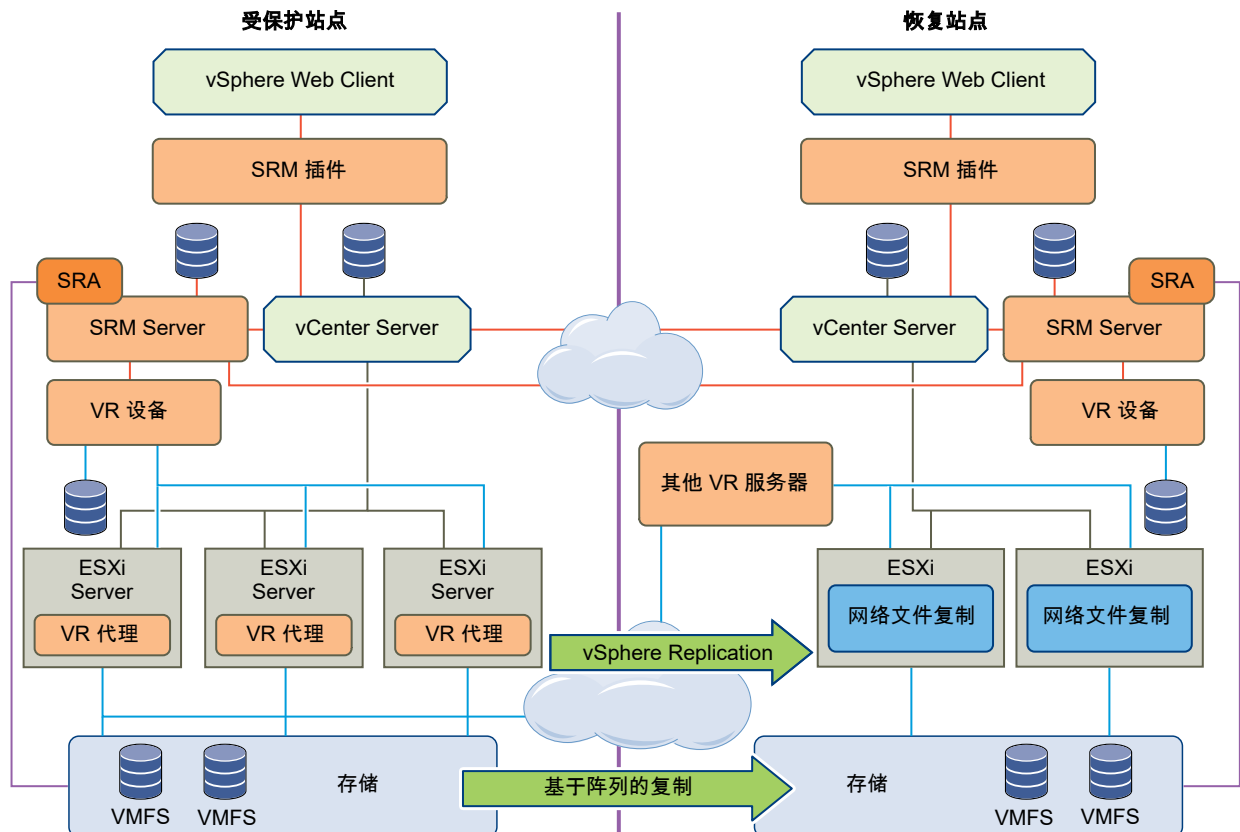
要创建使用基于阵列的复制和 vSphere Replication 的混合 Site Recovery Manager 部署，必须为这两种类型的复制配置受保护站点和恢复站点。

- 设置并连接存储阵列，然后在这两个站点上安装适用的存储复制适配器 (SRA)。
- 在这两个站点上部署 vSphere Replication 设备，然后在这些设备之间配置连接。
- 根据需要使用基于阵列的复制或 vSphere Replication 配置要复制的虚拟机。

**注** 请勿尝试在使用基于阵列的复制复制的数据存储上驻留的虚拟机上配置 vSphere Replication。

为通过基于阵列的复制配置的虚拟机创建基于阵列的保护组，为通过 vSphere Replication 配置的虚拟机创建 vSphere Replication 保护组，可以为虚拟机创建基于阵列的保护组。不能在保护组中混合复制类型。可以混合在同一个恢复计划中包含的基于阵列的保护组与 vSphere Replication 保护组。

图 2-4. 将 Site Recovery Manager 架构与基于阵列的复制和 vSphere Replication 结合使用



# 正在创建和管理保护组

## 3

配置复制解决方案后，可创建保护组。保护组是指 Site Recovery Manager 同时保护的一组虚拟机。

可以在恢复计划中包含一个或多个保护组。恢复计划可指定 Site Recovery Manager 如何恢复该计划所包含的保护组中的虚拟机。

根据您使用基于阵列的复制还是使用 vSphere Replication，可通过不同方式配置虚拟机并创建保护组。您不能创建既包含已配置基于阵列复制的虚拟机又包含已配置 vSphere Replication 的虚拟机的保护组。可以在同一个恢复计划中包含基于阵列的保护组和 vSphere Replication 保护组的组合。

在虚拟机上配置复制后，必须将每个虚拟机分配给恢复站点上的现有资源池、文件夹和网络。可以通过选择清单映射来指定这些分配的站点范围默认值。如果不指定清单映射，请为保护组中的每个虚拟机单独配置映射。

创建保护组后，Site Recovery Manager 将在恢复站点上创建占位虚拟机，并对组中的每个虚拟机应用清单映射。如果 Site Recovery Manager 无法将某一虚拟机映射到恢复站点上的文件夹、网络或资源池，则 Site Recovery Manager 会将该虚拟机置于“映射丢失”状态，并且不会为其创建占位虚拟机。

Site Recovery Manager 无法保护未在上面配置复制的虚拟机，也无法保护在上面错误地配置了复制的虚拟机。对于基于阵列的复制，即使虚拟机位于受保护数据存储中也是如此。

- [关于基于阵列的保护组和数据存储组](#)

为基于阵列的复制创建保护组时，请指定阵列信息，而 Site Recovery Manager 会将虚拟机组计算至数据存储组中。数据存储组包含受保护的虚拟机的所有文件。

- [关于 vSphere Replication 保护组](#)

您可以包括为 vSphere Replication 保护组中的 vSphere Replication 配置的虚拟机。

- [创建保护组](#)

可以通过创建保护组来启用 Site Recovery Manager 以保护虚拟机的安全。

- [通过文件夹对保护组进行组织](#)

您可以创建用于对保护组进行组织的文件夹。

- [在保护组中添加或移除数据存储组或虚拟机](#)

可以添加或移除基于阵列的保护组中的数据存储组，或添加或移除 vSphere Replication 保护组中的虚拟机。还可以更改保护组的名称和描述。

- [将清单映射应用于保护组中的所有成员](#)

如果保护组的状态为“未配置”，则可以使用现有站点范围的清单映射一次性为所有未配置的虚拟机配置保护。

- [为保护组中的单个虚拟机配置清单映射](#)

可以分别为保护组中的虚拟机配置映射。此功能可允许您针对不同的虚拟机使用恢复站点上的不同资源。

- [修改受保护虚拟机的设置](#)

您可以编辑保护组中虚拟机的设置。编辑虚拟机的设置以添加或更改存储设备（如硬盘或 DVD 驱动器）可能会影响该虚拟机的保护。

- [移除虚拟机的保护](#)

您可以暂时移除已复制虚拟机的保护，而不将其从保护组中移除。

- [保护组状态参考](#)

可以监控保护组的状态并确定在每个状态下所允许的操作。

- [虚拟机保护状态参考](#)

可以监控保护组中虚拟机的状态并确定在每个状态下允许的操作。

## 关于基于阵列的保护组和数据存储组

为基于阵列的复制创建保护组时，请指定阵列信息，而 Site Recovery Manager 会将虚拟机组计算至数据存储组中。数据存储组包含受保护的虚拟机的所有文件。

通过将虚拟机置于属于某个数据存储组（Site Recovery Manager 将其与保护组相关联）的数据存储中，可以将这些虚拟机添加到基于阵列的保护组。Site Recovery Manager 在检测到受保护虚拟机发生更改后会重新计算数据存储组。例如，如果将其他 LUN 上的硬盘添加到受保护虚拟机，则 Site Recovery Manager 会将该 LUN 添加到该保护组的数据存储组。必须重新配置保护才能保护该新 LUN。在配置阵列对或刷新设备列表时，Site Recovery Manager 将计算一致性组。

您还可以通过使用 Storage vMotion 将虚拟机的文件移动到数据存储组内的某一数据存储来将这些虚拟机添加到该保护组中。可通过将虚拟机的文件移动到其他数据存储来从基于阵列的保护组中移除虚拟机。

如果您的存储阵列支持一致性组，Site Recovery Manager 将与 vSphere Storage DRS 和 vSphere Storage vMotion 兼容。您可以使用 Storage DRS 和 Storage vMotion 在 Site Recovery Manager 所保护的一致性组内移动虚拟机。如果存储阵列不支持一致性组，则无法将 Storage DRS 和 Storage vMotion 与 Site Recovery Manager 结合使用。

- [Site Recovery Manager 如何计算数据存储组](#)

Site Recovery Manager 将根据在数据存储组中的数据存储上存放文件的虚拟机组以及存储这些数据存储的设备来确定该数据存储组的构成。

## Site Recovery Manager 如何计算数据存储组

Site Recovery Manager 将根据在数据存储组中的数据存储上存放文件的虚拟机组以及存储这些数据存储的设备来确定该数据存储组的构成。

使用基于阵列的复制时，每个存储阵列均支持一组复制的数据存储。在使用光纤通道和 iSCSI 等连接协议的存储区域网络 (SAN) 阵列中，这些数据存储称为逻辑存储单元 (LUN)，并由一个或多个物理数据存储组组成。在网络文件系统 (NFS) 阵列上，已复制的数据存储通常称为卷。在每对复制的存储设备中，其中一个数据存储为复制源，另一数据存储为复制目标。根据阵列的复制软件所控制的计划安排，写入源数据存储的数据将复制到目标数据存储上。当配置 Site Recovery Manager 以使用存储复制适配器 (SRA) 时，复制源位于受保护站点，复制目标则位于恢复站点。

数据存储为虚拟机文件提供存储空间。通过隐藏物理存储设备的详细信息，数据存储可简化存储容量分配，并提供一个统一的模式来满足虚拟机的存储需求。由于任何数据存储均可跨多个设备，因此 Site Recovery Manager 必须确保先复制所有支持该数据存储的设备，然后才可以保护使用该数据存储的虚拟机。Site Recovery Manager 还必须确保已复制所有包含受保护虚拟机文件的数据存储。在恢复或测试期间，Site Recovery Manager 必须同时处理所有这类数据存储。

为了实现这一目标，Site Recovery Manager 需将数据存储聚合成数据存储组，以适应跨多个数据存储的虚拟机的要求。Site Recovery Manager 会定期检查并确保数据存储组包含所有必需的数据存储，以便为相应的虚拟机提供保护。必要时，Site Recovery Manager 会重新计算数据存储组。例如，在向虚拟机添加新设备，而这些设备存储在先前不属于数据存储组的数据存储中时，可能会发生这种情况。

数据存储组由最小数据存储集组成，该数据存储集是确保以下情况所必需的：当任一虚拟机文件存储在此组的数据存储上时，所有虚拟机文件都存储在属于同一组的数据存储上。例如，如果一个虚拟机在两个不同数据存储中都具有磁盘，则 Site Recovery Manager 会将这两个数据存储合并为一个数据存储组。Site Recovery Manager 会根据设置的标准将设备合并到数据存储组中。

- 两个不同的数据存储包含属于同一虚拟机的文件。
- 属于两个虚拟机的数据存储在一个 SAN 阵列上共享一个裸磁盘映射 (RDM) 设备（如 Microsoft 群集服务器 (MSCS) 群集）。
- 两个数据存储跨多个与同一设备的不同分区对应的数据区。
- 一个数据存储跨与两个不同设备的分区对应的两个数据区。两个数据区必须位于同一个一致性组中，SRA 必须在设备发现阶段报告阵列中的一致性组信息。否则，即使 SRA 报告已复制构成此数据存储的数据区，也无法基于此数据存储创建保护组。
- 多个数据存储属于一个一致性组。一致性组是一组已复制的数据存储，其目标数据存储集的每个状态在某一特定时间都是作为源数据存储集的状态存在的。在非正式情况下，将同时复制数据存储；这样，当使用这些数据存储进行恢复时，访问目标的软件就不会将数据视为处于该软件未准备好进行处理的状态。

### 对跨多个 LUN 或数据区的 VMFS 数据存储上的虚拟机进行保护

由于只有部分存储阵列支持一致性组，因此，并不是所有 SRA 都会报告存储阵列中的一致性组信息。如果在执行数据存储发现命令后 SRA 报告阵列中的一致性组信息，则构成多数据区 VMFS 数据存储的 LUN 必须位于同一个存储阵列一致性组中。如果该阵列不支持一致性组，并且 SRA 未报告任何一致性组信息，则 Site Recovery Manager 无法保护多数据区的数据存储中的虚拟机。

## 关于 vSphere Replication 保护组

您可以包括为 vSphere Replication 保护组中的 vSphere Replication 配置的虚拟机。

创建或编辑 vSphere Replication 保护组时，可以选择 vCenter Server 清单中为 vSphere Replication 配置的虚拟机。

在虚拟机上配置 vSphere Replication 时，可在远程站点上的数据存储中选择一个目标位置。在保护组包括配置有 vSphere Replication 的虚拟机时，Site Recovery Manager 会创建一个占位虚拟机用于恢复。vSphere Replication 的复制目标和 Site Recovery Manager 创建的占位虚拟机可以位于恢复站点上的同一个数据存储中，因为它们会创建在不同的数据存储文件夹中。当复制目标和占位虚拟机位于同一数据存储中时，Site Recovery Manager 会使用复制目标名称加上后缀 (1) 来表示占位虚拟机名称。为避免混淆，最佳做法是对 vSphere Replication 复制目标和 Site Recovery Manager 占位虚拟机使用不同的数据存储。Site Recovery Manager 将清单映射应用于恢复站点上的占位虚拟机。

vSphere Replication 根据您在虚拟机上配置 vSphere Replication 时设定的恢复点目标同步复制目标虚拟机的磁盘文件。通过 Site Recovery Manager 执行恢复时，Site Recovery Manager 打开复制目标虚拟机的电源，并在恢复站点上的占位虚拟机的位置向 vCenter Server 注册该复制目标虚拟机。

使用 vSphere Replication 保护组时，Site Recovery Manager 依赖于 vSphere Replication，但是 vSphere Replication 不依赖于 Site Recovery Manager。您可以独立于 Site Recovery Manager 使用 vSphere Replication。例如，您可以使用 vSphere Replication 复制 vCenter Server 清单中的所有虚拟机，但只在保护组中包含部分虚拟机。您对 vSphere Replication 配置所做的更改会影响 Site Recovery Manager 对您在保护组中包括的虚拟机的保护。

- Site Recovery Manager 监控 vSphere Replication 保护组中虚拟机的 vSphere Replication 状态。如果保护组中虚拟机的复制未正常进行，Site Recovery Manager 无法恢复虚拟机。
- 如果在虚拟机上取消配置 vSphere Replication，Site Recovery Manager 将会继续在您包括该虚拟机的保护组中包括该虚拟机。Site Recovery Manager 无法恢复该虚拟机，直到您重新配置复制。如果在虚拟机上取消配置 vSphere Replication，您可以手动将其从保护组中删除。
- 如果您在驻留于 Site Recovery Manager 已通过基于阵列的复制进行保护的数据存储的虚拟机上配置了 vSphere Replication，则当尝试在 vSphere Replication 保护组中包括该虚拟机时，Site Recovery Manager 会报告一个错误。

如果从保护组中删除配置有 vSphere Replication 的虚拟机，vSphere Replication 会继续将虚拟机复制到恢复站点。如果运行相关联的恢复计划，虚拟机不会随保护组中的其余虚拟机恢复。

## 创建保护组

可以通过创建保护组来启用 Site Recovery Manager 以保护虚拟机的安全。

可以通过文件夹来对保护组进行组织。vSphere Web Client 中的不同视图显示了各保护组的名称，但不显示文件夹名称。如果不同的文件夹包含两个同名的保护组，则在 vSphere Web Client 的某些视图中可能很难将其区分开。因此，请确保保护组名称在所有文件夹中是唯一的。由于在某些环境中，并非所有用户都对所有文件夹拥有查看特权，因此，为确保保护组名称的唯一性，请不要使用文件夹来对保护组进行组织。

创建保护组时，请等待以确保操作按预期完成。确保 Site Recovery Manager 可创建保护组，并且在该组中可成功保护虚拟机。

### 前提条件

验证您是否已执行以下任务之一：

- 已将虚拟机包含在为其配置了基于阵列的复制的数据存储中
- 已在虚拟机上配置 vSphere Replication
- 已执行上述两项任务的组合

### 步骤

- 1 在 vSphere Web Client 中，单击 **站点恢复 > 保护组**。
- 2 在 **对象** 选项卡上，单击相应图标以创建保护组。
- 3 在“名称和位置”页面中，输入保护组的名称，选择一对站点或一个文件夹，然后单击 **下一步**。
- 4 在“保护组类型”页面上，选择受保护的站点，选择复制类型，然后单击 **下一步**。

选项	操作
基于阵列的复制组	选择 <b>基于阵列的复制 (ABR)</b> ，然后选择一个阵列对。
vSphere Replication 保护组	选择 <b>vSphere Replication</b> 。

- 5 选择要添加到保护组的数据存储组或虚拟机。

选项	操作
基于阵列的保护组	选择数据存储组，然后单击 <b>下一步</b> 。
vSphere Replication 保护组	从列表中选择虚拟机，然后单击 <b>下一步</b> 。

创建 vSphere Replication 保护组时，列表中仅显示您为 vSphere Replication 配置的虚拟机以及已不在保护组中的虚拟机。

- 6 （可选）输入该保护组的描述，然后单击 **下一步**。
- 7 查看设置，然后单击 **完成**。

您可以在 **保护组** 下的 **对象** 选项卡监视保护组的创建进度。

- 如果 Site Recovery Manager 成功将清单映射应用到受保护的虚拟机，保护组的状态将为“良好”。
- 如果您未配置清单映射，或者如果 Site Recovery Manager 无法应用这些映射，保护组的状态将为“未配置”。

## 后续步骤

如果保护组的状态为“未配置”，请将清单映射应用到虚拟机：

- 要应用站点范围的清单映射或检查已设置的清单映射是否有效，请参见 [Site Recovery Manager 的安装和配置中的选择清单映射](#)。要将这些映射应用到所有虚拟机，请参见 [将清单映射应用于保护组中的所有成员](#)。
- 要将清单映射分别应用到保护组中的每个虚拟机，请参见 [为保护组中的单个虚拟机配置清单映射](#)。

## 通过文件夹对保护组进行组织

您可以创建用于对保护组进行组织的文件夹。

如果您拥有很多保护组，将保护组组织到文件夹中非常有用。您可以通过将保护组放置到文件夹中并为不同用户或组分配不同的文件夹权限，从而限制对保护组的访问权限。有关如何为文件夹分配权限的信息，请参见 [分配 Site Recovery Manager 角色和权限](#)。

### 步骤

- 1 在 vSphere Web Client 的主页视图中，单击**站点恢复**。
- 2 展开**清单树**，然后单击**保护组**。
- 3 选择**相关对象**选项卡，然后单击**文件夹**。
- 4 单击**创建文件夹**图标，输入要创建的文件夹的名称，然后单击**确定**。
- 5 将新的或现有保护组添加到文件夹。

选项	描述
创建新保护组	右键单击文件夹，然后选择 <b>创建保护组</b> 。
添加现有保护组	将保护组从清单树拖放到文件夹中。

- 6 （可选）要重命名或删除某一文件夹，请右键单击该文件夹，然后选择**重命名文件夹**或**删除文件夹**。  
只有文件夹为空，您才能删除它。

## 在保护组中添加或移除数据存储组或虚拟机

可以添加或移除基于阵列的保护组中的数据存储组，或添加或移除 vSphere Replication 保护组中的虚拟机。还可以更改保护组的名称和描述。

### 前提条件

已创建保护组。

### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 保护组**。
- 2 右键单击保护组，然后选择**编辑保护组**。



### 3 （可选）更改保护组的名称，然后单击下一步。

无法更改位置设置。

### 4 单击下一步。

无法更改“受保护站点”或“复制类型”设置。对于基于阵列的保护组，无法更改阵列对。

### 5 修改保护组包含的数据存储组或虚拟机。

- 对于基于阵列的保护组，选中或取消选中要在保护组中添加或移除的数据存储组，然后单击下一步。
- 对于 vSphere Replication 保护组，选中或取消选中要在保护组中添加或移除的虚拟机，然后单击下一步。

### 6 （可选）输入该保护组的描述，然后单击下一步。

### 7 查看设置，然后单击下一步以应用设置。

Site Recovery Manager 更新保护组时，无法恢复或取消这些更改。

### 8 单击完成关闭向导。

#### 结果

- 如果已配置站点范围的清单映射，则 Site Recovery Manager 会将这些映射应用于已添加到保护组的虚拟机。如果成功，虚拟机的状态为“良好”。

---

**注** 将数据存储或虚拟机添加到保护组时，清单映射仅应用于新虚拟机。例如，如果更改清单映射，然后将数据存储添加到处于“良好”状态的保护组，则 Site Recovery Manager 会将新映射应用于位于新数据存储中新的受保护虚拟机。之前的受保护虚拟机将继续使用旧映射。

---

- 如果尚未配置站点范围的清单映射，则保护组的状态为“未配置”，新虚拟机的状态为“映射丢失”。

#### 后续步骤

如果保护组的状态为“未配置”，且新虚拟机的状态为“映射丢失”，则会将清单映射应用于虚拟机：

- 要应用站点范围的清单映射或检查已设置的清单映射是否有效，请参见 Site Recovery Manager 的安装和配置中的[选择清单映射](#)。要将这些映射应用于所有虚拟机，请参见[将清单映射应用于保护组中的所有成员](#)。
- 要将清单映射分别应用于保护组中的每个虚拟机，请参见[为保护组中的单个虚拟机配置清单映射](#)。

## 将清单映射应用于保护组中的所有成员

如果保护组的状态为“未配置”，则可以使用现有站点范围的清单映射一次性为所有未配置的虚拟机配置保护。

在创建保护组或向现有保护组添加虚拟机时，Site Recovery Manager 会将站点范围的清单映射应用于虚拟机。如果在创建保护组或向其添加虚拟机后更改站点范围的清单映射，虚拟机将继续使用原始清单映射恢复。要应用新的清单映射，必须在该保护组中的虚拟机上重新配置保护。

保护组的状态为“未配置”的原因有多种：

- 在创建保护组之前，未配置站点范围的清单映射。
- 在创建保护组之前，未配置占位数据存储映射。
- 在创建保护组之后，向其添加了虚拟机。
- 虚拟机失去其保护，可能是因为您在将其添加到保护组后对其进行了重新配置。例如，添加或移除了虚拟磁盘或设备。

#### 前提条件

- 配置或重新配置站点范围的清单映射。要选择清单映射，请参见 [Site Recovery Manager 的安装和配置中的选择清单映射](#)。
- 配置或重新配置占位数据存储映射。要配置占位数据存储，请参见 [Site Recovery Manager 的安装和配置中的配置占位数据存储](#)。

#### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 保护组**。
- 2 选择保护组，并在**相关对象**选项卡上单击**虚拟机**选项卡。
- 3 单击**全部配置**图标。

如果要激活**全部配置**按钮，则保护组中至少有一个虚拟机必须处于“未配置”状态。

- 4 单击**是**，以确认要向所有未配置的虚拟机应用清单映射。
  - 如果 Site Recovery Manager 成功向这些虚拟机应用了清单映射，则该保护组的状态为“良好”。
  - 如果 Site Recovery Manager 无法应用某些或所有清单映射，则虚拟机的状态为“未配置”或“映射丢失”。
  - 如果 Site Recovery Manager 应用了清单映射，但无法为虚拟机创建占位，则虚拟机的状态为“占位虚拟机创建错误”。
- 5 （可选）如果虚拟机的状态为“未配置”或“映射丢失”，请检查清单映射并再次单击**全部配置**。
- 6 （可选）如果虚拟机的状态为“占位虚拟机创建错误”，请检查占位数据存储映射并尝试重新创建占位虚拟机。
  - 要为单个虚拟机重新创建占位，请右键单击虚拟机，然后选择**重新创建占位**。
  - 要为多个虚拟机重新创建占位，请右键单击保护组，然后选择**还原占位虚拟机**。

## 为保护组中的单个虚拟机配置清单映射

可以分别为保护组中的虚拟机配置映射。此功能可允许您针对不同的虚拟机使用恢复站点上的不同资源。即使已配置站点范围的清单映射，也可以配置单个清单映射。如果已配置站点范围的清单映射，可以移除单个虚拟机的保护，并配置文件夹和资源映射以覆盖站点范围的映射。在不移除保护的情况下，也可以更改单个虚拟机的网络映射。

无法指定单个虚拟机的占位数据存储。必须将受保护的站点上的数据存储映射到站点级别的恢复站点上的占位数据存储。要配置占位数据存储，请参见 Site Recovery Manager 的安装和配置中的[配置占位数据存储](#)。

### 前提条件

已创建保护组。

### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 保护组**。
- 2 选择包含要配置的虚拟机的保护组。
- 3 在**相关对象**选项卡中，单击**虚拟机**选项卡。
- 4 右键单击该虚拟机，然后选择**配置保护**。
- 5 通过展开其状态为“未配置”的资源并选择恢复站点上的资源，配置清单映射。  
仅可更改文件夹、资源池和网络映射。
- 6 （可选）要将这些映射应用于站点上的所有受保护虚拟机，请选中每个资源的**另存为清单映射**复选框。  
如果未选中该复选框，则映射将仅应用于此虚拟机。
- 7 单击**确定**。
  - 如果 Site Recovery Manager 成功将清单映射应用于该虚拟机，则虚拟机的状态为“良好”。
  - 如果 Site Recovery Manager 无法应用某些或所有清单映射，则虚拟机的状态为“未配置”或“映射丢失”。
  - 如果 Site Recovery Manager 已应用清单映射，但无法创建占位虚拟机，则虚拟机的状态为“占位虚拟机创建错误”。
- 8 （可选）如果虚拟机的状态为“未配置”或“映射丢失”，请再次选择**配置保护**并检查清单映射。
- 9 （可选）如果虚拟机的状态为“占位虚拟机创建错误”，请检查站点级别的占位数据存储映射，右键单击该虚拟机，然后选择**重新创建占位**。

## 修改受保护虚拟机的设置

您可以编辑保护组中虚拟机的设置。编辑虚拟机的设置以添加或更改存储设备（如硬盘或 DVD 驱动器）可能会影响该虚拟机的保护。

如果使用基于阵列的复制，则在虚拟机上添加或更改设备会对保护产生影响，具体取决于您创建新设备的方式。

- 如果新设备位于不属于保护组的复制数据存储中，则包含虚拟机的保护组将进入“未配置”状态。重新配置保护组，以将包含新设备的数据存储添加到该保护组。
- 如果新设备位于受其他保护组保护的复制数据存储中，则虚拟机的保护无效。
- 如果新设备位于未复制的数据存储中，则必须复制数据存储或移除设备的保护。

- 如果使用 Storage vMotion 将虚拟机移至未复制的数据存储中，或移至 Site Recovery Manager 没有存储复制适配器 (SRA) 的阵列上的复制数据存储中，则虚拟机的保护无效。但是可以使用 Storage vMotion 将虚拟机移至属于其他保护组的数据存储中。

如果将设备添加到通过使用 vSphere Replication 保护的虚拟机中，则必须在该虚拟机上重新配置 vSphere Replication，以便为新设备选择复制选项。有关重新配置 vSphere Replication 设置的信息，请参见位于 <https://www.vmware.com/support/pubs/vsphere-replication-pubs.html> 上的 vSphere Replication 文档。

修改虚拟机后，必须为状态为“未配置”、“设备未找到”、“无法解析设备”或“映射丢失”的任何虚拟机重新配置保护。请参见[将清单映射应用于保护组中的所有成员和为保护组中的单个虚拟机配置清单映射](#)。

## 在受保护的虚拟机上禁用复制

必须为基于阵列的复制或 vSphere Replication 配置保护组中的所有虚拟机。如果在属于保护组的虚拟机上禁用复制，Site Recovery Manager 将无法恢复该虚拟机，且该保护组的状态为“未配置”。

- 如果移除属于基于阵列的复制保护组的虚拟机的保护，则必须将该虚拟机的文件移至不受保护的数据存储中。如果将不受保护的虚拟机的文件保留在 Site Recovery Manager 已在数据存储组中包括的数据存储中，则整个数据存储组的恢复将失败。
- 如果在保护组中已包括的虚拟机上禁用 vSphere Replication，则该虚拟机的恢复将失败，但组中所有正确配置的虚拟机的恢复将成功。您必须编辑保护组以移除该虚拟机。请参见[在保护组中添加或移除数据存储组或虚拟机](#)。

## 移除虚拟机的保护

您可以暂时移除已复制虚拟机的保护，而不将其从保护组中移除。

移除保护将删除恢复站点上的占位虚拟机。如果您移除了虚拟机的保护，相应虚拟机和保护组的状态将设置为“未配置”。可以成功运行包含保护组的恢复计划，但 Site Recovery Manager 不会恢复处于“未配置”状态的虚拟机。

您可能会因为各种不同的原因移除虚拟机的保护，如下所述：

- 您使用 vSphere Replication，但希望重新配置受保护的虚拟机。您可以在重新配置虚拟机时移除保护，以便正在进行的 Site Recovery Manager 测试或实际恢复不受更改影响。例如，在您先将设备添加到虚拟机并运行恢复，然后在新设备上配置 vSphere Replication 的情况下，如果未移除虚拟机的保护，恢复将显示错误。
- 您使用基于阵列的复制，并且某个用户移至您不希望保护的虚拟机。如果您移除了该虚拟机的保护，保护组仍显示“未配置”状态，但测试恢复和实际恢复继续成功执行。
- 您使用基于阵列的复制，并且虚拟机具有存储在未复制数据存储中的设备。可以移除虚拟机的保护，以便在您重定位设备文件时能够对组中的所有其他虚拟机成功执行恢复。
- 在基于阵列的复制中，虚拟机的 Site Recovery Manager 保护与该虚拟机的 Site Recovery Manager 存储管理之间存在差别。如果您移除了虚拟机中的保护，Site Recovery Manager 将不再恢复该虚拟机，但会继续监控和管理虚拟机文件的存储。

## 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 保护组**。
- 2 选择一个保护组，然后选择**相关对象 > 虚拟机**。
- 3 右键单击某个虚拟机并选择**移除保护**。
- 4 单击**是**确认移除虚拟机的保护。

## 保护组状态参考

可以监控保护组的状态并确定在每个状态下所允许的操作。

**表 3-1. 保护组状态**

状况	描述
正在加载	加载界面时短暂显示，直至显示保护组的状态。
确定	组空闲。所有虚拟机均处于“良好”状态。可以编辑组。
未配置	组空闲。某些虚拟机可能未处于“良好”状态。可以编辑组。
正在测试	组在运行测试的计划中使用。无法编辑组。
测试已完成	组在运行测试的计划中使用。无法编辑组。成功清理后组返回“良好”或“未配置”状态。
清理	组在测试后正在清理的计划中使用。无法编辑组。成功清理后组返回“良好”或“未配置”状态。如果清理失败，组转为“正在测试”状态。
正在恢复	组在正在运行恢复的计划中使用。无法编辑组。如果恢复成功，组转为“已恢复”状态。如果恢复失败，组状态改为“部分已恢复”。
部分已恢复	组在完成了恢复但部分虚拟机恢复失败的计划中。可以移除虚拟机，但无法配置或还原它们。
已恢复	组在已成功完成恢复的计划中。可以移除虚拟机，但无法配置或还原它们。
正在重新保护	组在运行重新保护的计划中使用。无法编辑组。重新保护成功后，组返回“良好”或“未配置”状态。如果重新保护失败，组转为“部分已重新保护”状态。
部分已重新保护	组在未能执行重新保护的计划中。可以移除虚拟机，但无法配置或还原它们。
正在配置保护	正在组中的虚拟机上执行保护操作。
正在移除保护	正从组中的虚拟机上移除保护。
正在还原占位	正在组中的虚拟机上创建占位。
操作正在进行中	正在组中执行至少一个“配置保护”和一个“移除保护”操作的组合。

## 虚拟机保护状态参考

可以监控保护组中虚拟机的状态并确定在每个状态下允许的操作。

**表 3-2. 虚拟机保护状态**

状况	描述
占位虚拟机未找到	已删除占位虚拟机。“还原占位符”图标已启用。
未找到原始受保护虚拟机	在故障切换之后和重新保护之前已删除原始生产虚拟机。“还原占位符”图标已启用。
由虚拟机使用的数据存储 <i>名称</i> 已从组中丢失	虚拟机需要的数据存储不在保护组中。编辑保护组以包含该数据存储。
由虚拟机使用的数据存储 <i>名称</i> 在其他组中受保护	虚拟机需要的数据存储在其他保护组中。从其他保护组中移除该数据存储，并编辑当前保护组以包含该数据存储。不能将一个数据存储包含在两个保护组中。
设备未找到: <i>设备名称</i>	已将未复制的磁盘或设备添加到受保护的虚拟机。必须编辑虚拟机的复制，在保护中包含或移除设备。
映射丢失: 文件夹 <i>名称</i> ; 网络 <i>名称</i> ; 资源池 <i>名称</i>	此虚拟机尚未配置文件夹、资源池或网络映射。修复站点的清单映射或手动配置虚拟机。
占位虚拟机创建错误: <i>服务器的错误字符串</i>	占位虚拟机创建过程中出错。
确定	存在受保护的虚拟机，并且提供程序和占位状态均已清除。
无效: <i>错误</i>	由于主数据存储未复制或虚拟机已删除，虚拟机无效。服务器的错误字符串包含详细信息。手动移除虚拟机的保护。
未配置	在创建保护组之后已添加新虚拟机。使用“全部配置”来配置虚拟机的保护。
错误: <i>错误</i>	错误可能为以下之一： <ul style="list-style-type: none"> <li>■ 恢复站点资源池、文件夹或网络不在同一数据中心。</li> <li>■ 未找到占位数据存储。</li> <li>■ 创建占位时出现任何 vCenter Server 错误，如连接或权限问题。</li> </ul>
正在配置保护	虚拟机操作。
正在移除保护	虚拟机操作。
正在还原占位	虚拟机操作。
正在加载	在界面正在加载直到出现虚拟机状态之前短暂出现。
映射冲突	Site Recovery Manager Server 报告清单冲突。虚拟机的资源池和文件夹位于不同的数据中心。
复制错误	vSphere Replication 报告有关虚拟机的错误。
复制警告	vSphere Replication 告有关虚拟机的警告。

# 创建、测试和运行恢复计划

# 4

在受保护站点和恢复站点配置 **Site Recovery Manager** 后，可以创建、测试和运行恢复计划。

恢复计划类似于自动操作手册。它控制恢复过程的每一个步骤，包括 **Site Recovery Manager** 开启和关闭虚拟机电源的顺序、恢复后的虚拟机所使用的网络地址等。恢复计划可以灵活配置，并且可以自定义。

一个恢复计划可包含一个或多个保护组。也可在多个恢复计划中包含同一个保护组。例如，可以创建一个恢复计划来处理将服务从受保护站点按计划迁移到恢复站点的操作，并创建另一恢复计划来处理电源故障或自然灾害等非计划事件。在本例中，如果让这些不同的恢复计划引用一个保护组，就可以确定如何执行恢复。要创建保护组，请参见[创建保护组](#)。

一次只能运行一个恢复计划来恢复某一特定保护组。如果同时测试或运行指定同一保护组的多个恢复计划，则只有一个恢复计划能够在此保护组上运行。指定同一保护组的其他正在运行的恢复计划将为此保护组及其包含的虚拟机报告警告。该警告可指示虚拟机已恢复，但不会报告其他恢复计划所涉及的其他保护组。

## ■ 测试恢复计划

创建或修改恢复计划时，请在尝试将此恢复计划用于计划的迁移或灾难恢复前，对其进行测试。

## ■ 通过运行恢复计划执行计划迁移或灾难恢复

您可以在计划的情况下运行恢复计划，以便将虚拟机从受保护站点迁移到恢复站点。当受保护站点遭遇可能会导致数据丢失的意外事件时，您也可以在非计划的情况下运行恢复计划。

## ■ 测试恢复计划和运行恢复计划之间的差异

虽然测试恢复计划对受保护站点或恢复站点都没有长久的影响，但运行恢复计划对这两个站点都有明显的影响。

## ■ 跨恢复站点上的多个主机执行虚拟机的测试恢复

可以创建恢复计划，用于恢复已隔离的测试网络中跨多个恢复站点主机的虚拟机。

## ■ 创建、测试和运行恢复计划

执行多组任务来创建、测试和运行恢复计划。

## ■ 导出恢复计划步骤

您可采用多种格式导出恢复计划的步骤以供日后参考，或者保留计划的打印件备份。

## ■ 查看和导出恢复计划历史记录

您可以查看和导出有关每次运行恢复计划、测试恢复计划或测试清理的报告。



## ■ 删除恢复计划

如果不需要恢复计划，您可以将其删除。

## ■ 恢复计划状态参考

可以监控恢复计划的状态并确定在每个状态下允许的操作。恢复计划的状态由计划中保护组的状态来决定。

# 测试恢复计划

创建或修改恢复计划时，请在尝试将此恢复计划用于计划的迁移或灾难恢复前，对其进行测试。

通过测试恢复计划，可确保将受该计划保护的虚拟机正确恢复到恢复站点。如果不测试恢复计划，则实际灾难恢复情况可能无法恢复所有虚拟机，从而导致数据丢失。

尽管 Site Recovery Manager 为避免中断受保护站点和恢复站点上正在进行的操作而做出若干让步，但测试恢复计划几乎可以演练恢复计划的每一个环节。恢复计划在测试时会挂起本地虚拟机，在实际恢复时也是如此。除此之外，运行测试恢复不会中断任何站点中的复制或正在进行的活动。

如果使用 vSphere Replication，则当您测试恢复计划时，受保护站点上的虚拟机仍能与恢复站点上的副本虚拟机磁盘文件进行同步。vSphere Replication 服务器会在恢复站点上的虚拟机磁盘文件中创建重做日志，以便同步能够继续正常进行。运行测试后执行清理时，vSphere Replication 服务器会从恢复站点上的磁盘删除重做日志，并且日志中累积的更改会永久性地写入虚拟机磁盘。

如果使用基于阵列的复制，则当您测试恢复计划时，受保护站点上的虚拟机仍能复制到恢复站点上的副本虚拟机磁盘文件中。测试恢复期间，阵列会创建托管恢复站点上虚拟机磁盘文件的卷的快照。测试正在进行时，阵列复制会继续正常进行。运行测试后执行清理时，阵列会删除测试恢复工作流程中先前创建的快照。

可以根据需要运行测试恢复。可以随时取消恢复计划测试。

运行故障切换或其他测试之前，必须成功运行清理操作。请参见[测试恢复计划后清理](#)。

测试恢复计划的权限不包括运行恢复计划的权限。运行恢复计划的权限不包括测试恢复计划的权限。必须单独分配每个权限。请参见[分配 Site Recovery Manager 角色和权限](#)。

# 测试网络和数据中心网络

测试恢复计划时，Site Recovery Manager 可创建用于连接已恢复虚拟机的测试网络。通过创建测试网络，可以运行测试而不中断生产环境中的虚拟机。

测试网络由其自身的虚拟交换机管理，且在大多数情况下，恢复的虚拟机可以使用此网络，而无需更改 IP 地址、网关等网络属性。如果在创建恢复计划时配置测试网络设置，您可以通过选择**自动**来使用该测试网络。测试网络无法跨主机运行。必须为恢复计划在恢复期间使用的每个网络都配置测试网络。

对于所有必须互相交互的虚拟机，您必须将这些虚拟机恢复到同一测试网络。例如，如果 Web 服务器访问数据库上的信息，则这些 Web 服务器和数据库虚拟机应一起恢复到同一网络。



数据中心网络是一种通常支持恢复站点上的现有虚拟机的网络。可以选择数据中心网络用作测试网络。要使用此网络，恢复的虚拟机必须符合其网络地址可用性规则。这些虚拟机必须使用网络交换机可以提供并进行路由的网络地址，且必须使用正确的网关和 DNS 主机等。使用 DHCP 的已恢复虚拟机无需进行其他自定义即可连接到此网络。其他虚拟机需要进行 IP 自定义并执行采用该自定义的其他恢复计划步骤。

## 通过运行恢复计划执行计划迁移或灾难恢复

您可以在计划的情况下运行恢复计划，以便将虚拟机从受保护站点迁移到恢复站点。当受保护站点遭遇可能会导致数据丢失的意外事件时，您也可以在非计划的情况下运行恢复计划。

在计划迁移过程中，Site Recovery Manager 会将恢复站点上的虚拟机数据与受保护站点上的虚拟机同步。Site Recovery Manager 会尝试正常关闭受保护的虚拟机并执行最终同步以防止数据丢失，然后再打开恢复站点上的虚拟机的电源。如果在计划的迁移期间出现错误，则计划会停止，以便您解决这些错误并重新运行计划。恢复完成之后便可重新保护虚拟机。

在灾难恢复过程中，Site Recovery Manager 首先尝试执行存储同步。如果同步成功，Site Recovery Manager 会根据您在配置复制技术时设置的恢复点目标 (RPO)，使用已同步存储的状态将恢复站点上的虚拟机恢复到最近的可用状态。当运行恢复计划以执行灾难恢复时，Site Recovery Manager 会尝试关闭受保护站点上的虚拟机。如果 Site Recovery Manager 无法关闭虚拟机，Site Recovery Manager 仍会启动恢复站点上的副本。如果受保护站点在执行灾难恢复后恢复联机，恢复计划将进入不一致状态（生产虚拟机在两个站点上运行，又称为裂脑情况）。Site Recovery Manager 会检测此状态并允许您再次运行该计划，以关闭受保护站点上的虚拟机的电源。恢复计划之后会恢复一致状态，并且您可以运行重新保护。

如果 Site Recovery Manager 检测到受保护站点上的数据存储处于全部路径异常 (APD) 状态，并且正在阻止虚拟机关闭，则 Site Recovery Manager 将等待一段时间，然后再次尝试关闭虚拟机。APD 通常是暂时状态，因此等待处于 APD 状态的数据存储恢复联机后，Site Recovery Manager 即可在该数据存储上正常关闭受保护虚拟机。

Site Recovery Manager 使用 VMware Tools 检测信号发现虚拟机在恢复站点上运行的时间。通过此方法，Site Recovery Manager 可以确保所有虚拟机均在恢复站点上运行。因此，VMware 建议您在受保护的虚拟机上安装 VMware Tools。如果在受保护的虚拟机上未安装或无法安装 VMware Tools，则必须将 Site Recovery Manager 配置为不等待 VMware Tools 在已恢复的虚拟机中启动，并且跳过客户机操作系统关闭步骤。请参见[更改恢复设置](#)。

Site Recovery Manager 完成最终复制后，Site Recovery Manager 会在两个站点中进行更改，这些更改需要大量时间和精力才能撤消。由于需要花费大量时间和精力，因此您必须单独分配测试恢复计划的特权和运行恢复计划的特权。

## 使用强制恢复来运行恢复

如果受保护站点处于脱机状态，并且 Site Recovery Manager 无法及时执行其通常任务从而使 RTO 增加到不可接受的程度，则可以使用强制恢复选项运行恢复。强制恢复将启动恢复站点上的虚拟机，但不会在受保护站点上执行任何操作。

---

**小心** 只有在恢复时间目标 (RTO) 因缺少与保护站点的连接受到严重影响的情况下，才使用强制恢复。

---

强制恢复用于以下情况：基础架构在受保护站点出现故障，从而导致受保护虚拟机难以管理且无法关闭、关闭电源或取消注册。在这种情况下，系统状况将长时间无法更改。要解决这种情况，您可以强制执行恢复。强制执行恢复将无法完成关闭受保护站点上虚拟机的过程。因此，将会发生裂脑的情况，但恢复可能会更快地完成。

如果在受保护站点存储阵列处于脱机状态或不可用时使用基于阵列的复制运行灾难恢复，可能会影响受保护存储阵列与恢复存储阵列之间的镜像。运行强制恢复后，必须先检查是否正确设置了受保护阵列和恢复阵列之间的镜像，然后才能执行其他复制操作。如果镜像设置错误，则必须使用存储阵列软件来修复镜像。

使用 vSphere Replication 运行灾难恢复时，Site Recovery Manager 为重新保护准备 vSphere Replication 存储，您无需像使用基于阵列的复制那样对镜像进行验证。

如果在受保护站点存储仍然可用的情况下启用强制恢复，则在顺序开始之前，保护站点上的任何未完成更改都不会复制到恢复站点。复制更改的操作将根据存储阵列的恢复点目标 (RPO) 时间段进行。如果在保护站点上添加新的虚拟机或模板，并且恢复在存储 RPO 时间段结束之前启动，则新的虚拟机或模板就会丢失，不会出现在复制的数据存储中。为避免丢失新的虚拟机或模板，请等到 RPO 时间段结束后，再运行强制恢复的恢复计划。

要在运行灾难恢复时选择强制恢复，必须在 Site Recovery Manager 恢复服务器上的“高级设置”中启用 `recovery.forceRecovery` 选项。在“运行恢复计划”向导中，仅在灾难恢复模式下选择强制恢复选项。该选项不可用于计划的迁移。

完成强制恢复并验证存储阵列的镜像后，便可以解决需要强制恢复的问题。解决基础问题后，重新运行恢复计划中的计划迁移，解决出现的所有问题，并重新运行计划直至其成功完成。重新运行恢复计划不会影响恢复站点上的已恢复虚拟机。

## 测试恢复计划和运行恢复计划之间的差异

虽然测试恢复计划对受保护站点或恢复站点都没有长久的影响，但运行恢复计划对这两个站点都有明显的影响。

测试和运行恢复计划时，您需要不同的特权。

表 4-1. 如何区分测试恢复计划和运行恢复计划

差异点	测试恢复计划	运行恢复计划
所需特权	需要 Site Recovery Manager.恢复计划.测试权限。	需要 Site Recovery Manager.恢复计划.恢复权限。
对受保护站点上虚拟机的影响	无	Site Recovery Manager 按相反的优先级顺序关闭虚拟机电源，并还原在受保护站点上挂起的任何虚拟机。
对恢复站点上虚拟机的影响	如果恢复计划需要，Site Recovery Manager 会挂起本地虚拟机。清理测试后，Site Recovery Manager 重新启动挂起的虚拟机。	如果恢复计划需要，Site Recovery Manager 会挂起本地虚拟机。

表 4-1. 如何区分测试恢复计划和运行恢复计划（续）

差异点	测试恢复计划	运行恢复计划
对复制的影响	Site Recovery Manager 在恢复站点创建复制存储的临时快照。对于基于阵列的复制，Site Recovery Manager 重新扫描阵列以发现它们。	在计划的迁移过程中，Site Recovery Manager 同步复制的数据存储，接着停止复制，然后使恢复站点的目标设备可写。在灾难恢复期间，Site Recovery Manager 尝试执行相同的步骤，但如果未成功，Site Recovery Manager 会忽略受保护站点的错误。
网络	如果明确指定测试网络，Site Recovery Manager 会将已恢复的虚拟机连接到测试网络。如果虚拟机网络分配方式为 <b>自动</b> ，Site Recovery Manager 会将虚拟机分配给未连接任何物理网络的临时网络。	Site Recovery Manager 将恢复后的虚拟机连接到用户指定的数据中心网络。
恢复计划中断	可以随时取消测试。	可以随时取消恢复。

## 跨恢复站点上的多个主机执行虚拟机的测试恢复

可以创建恢复计划，用于恢复已隔离的测试网络中跨多个恢复站点主机的虚拟机。

通过 Site Recovery Manager，可以为 vSwitch 提供 DVS 支持并实现跨主机恢复。如果接受配置为“自动”的默认测试网络，则会在恢复计划测试期间将跨主机恢复的虚拟机置于其各自的测试网络中。每个测试交换机均在主机之间隔离。因此，在测试恢复完成后，会隔离同一恢复计划中的虚拟机。要允许虚拟机之间进行通信，请建立并选择 DVS 交换机或 VLAN。通过一个隔离的 VLAN 将所有主机相互连接而不是连接到生产网络，这样可更真实地测试恢复。要实现恢复主机之间的连接并与生产网络隔离，请遵循以下建议：

- 创建连接到已隔离的专用 VLAN 的 DVS 交换机。此类 VLAN 允许连接主机和虚拟机，并同时与生产虚拟机相隔离。使用明确指明 DVS 用于测试的命名约定，然后在恢复计划编辑器中的恢复计划测试网络列中选择此 DVS。
- 在物理网络上创建测试 VLAN，这不会提供返回受保护站点的路由。将测试 VLAN 中继到恢复站点 vSphere 群集，并创建测试 VLAN ID 的虚拟交换机。使用明确的命名约定将这些交换机标识为用于测试。在恢复计划编辑器中，从测试恢复网络列中选择这些交换机。

## 创建、测试和运行恢复计划

执行多组任务来创建、测试和运行恢复计划。

### 步骤

#### 1 创建恢复计划

创建恢复计划，以建立 Site Recovery Manager 恢复虚拟机的方式。

#### 2 通过文件夹对恢复计划进行组织

您可以创建用于对恢复计划进行组织的文件夹。

### 3 编辑恢复计划

可以编辑恢复计划以更改创建此恢复计划时指定的属性。可从受保护站点或恢复站点编辑恢复计划。

### 4 测试恢复计划

测试恢复计划时，Site Recovery Manager 会在测试网络上以及恢复站点中已复制数据的临时快照上运行虚拟机的恢复计划。Site Recovery Manager 不会中断受保护站点上的操作。

### 5 测试恢复计划后清理

测试恢复计划后，可以通过运行清理操作使恢复计划返回到就绪状态。必须先完成清理操作，然后才能运行故障切换或其他测试。

### 6 运行恢复计划

运行恢复计划时，Site Recovery Manager 会将恢复计划中的所有虚拟机迁移至恢复站点。Site Recovery Manager 尝试关闭受保护站点中的相应虚拟机。

### 7 恢复虚拟机的时间点快照

通过 vSphere Replication，您可以保留虚拟机的时间点快照。可以将 Site Recovery Manager 配置为在您运行恢复计划时恢复虚拟机的多个时间点 (PIT) 快照。

### 8 取消测试或恢复

您可以在状态为“测试正在进行中”或“正在进行故障切换”时取消恢复计划测试。

## 创建恢复计划

创建恢复计划，以建立 Site Recovery Manager 恢复虚拟机的方式。

#### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**。
- 2 在**相关对象 > 恢复计划**选项卡上，单击用于创建恢复计划的图标。
- 3 输入计划的名称，选择一个位置，然后单击**下一步**。
- 4 选择恢复站点，然后单击**下一步**。
- 5 为要恢复的计划选择一个或多个保护组，然后单击**下一步**。
- 6 为其配置的恢复网络是由数据中心和恢复网络标识的所选恢复网络的虚拟机选择测试网络。测试网络仅可来自同一数据中心，且默认值为“自动”。

选项	操作
数据中心	选择虚拟机要恢复到的数据中心。
恢复网络	选择要用于计划的迁移和灾难恢复的网络。
测试网络	选择要用于恢复计划测试的测试网络。

- 7 单击 **下一步**。
- 8 （可选）为恢复计划添加描述，然后单击**下一步**。
- 9 查看摘要信息，然后单击**完成**创建恢复计划。

## 通过文件夹对恢复计划进行组织

您可以创建用于对恢复计划进行组织的文件夹。

如果您拥有很多恢复计划，将恢复计划组织到文件夹中非常有用。您可以通过将恢复计划放置到文件夹中并为不同用户或组分配不同的文件夹权限，从而限制对恢复计划的访问权限。有关如何为文件夹分配权限的信息，请参见[分配 Site Recovery Manager 角色和权限](#)。

### 步骤

- 1 在 vSphere Web Client 的主页视图中，单击**站点恢复**。
- 2 展开**清单树**，然后单击**恢复计划**。
- 3 选择**相关对象**选项卡，然后单击**文件夹**。
- 4 单击**创建文件夹**图标，输入要创建的文件夹的名称，然后单击**确定**。
- 5 将新的或现有恢复计划添加到文件夹。

选项	描述
创建新恢复计划	右键单击文件夹，然后选择 <b>创建恢复计划</b> 。
添加现有恢复计划	将恢复计划从清单树拖放到文件夹中。

- 6 （可选）要重命名或删除某一文件夹，请右键单击该文件夹，然后选择**重命名文件夹**或**删除文件夹**。  
只有文件夹为空，您才能删除它。

## 编辑恢复计划

可以编辑恢复计划以更改创建此恢复计划时指定的属性。可从受保护站点或恢复站点编辑恢复计划。

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**。
- 2 右键单击恢复计划，然后选择**编辑计划**。还可以从“恢复步骤”选项卡中编辑计划。
- 3 （可选）在**恢复计划名称**文本框中更改计划的名称，然后单击**下一步**。
- 4 在“恢复站点”页面上，单击**下一步**。  
您不能更改恢复站点。
- 5 （可选）选择或取消选择一个或多个保护组以将其添加到计划或从计划中移除，然后单击**下一步**。
- 6 （可选）更改恢复站点测试网络设置。
  - a 选择配置的网络设置，然后单击**移除**。
  - b 为任何恢复网络选择一个新的测试网络。
- 7 单击 **下一步**。
- 8 （可选）为计划输入或修改描述，然后单击**下一步**。

- 9 查看摘要信息，然后单击**完成**将指定更改应用于该恢复计划。

在“近期任务”视图中可以监控计划的更新。

## 测试恢复计划

测试恢复计划时，Site Recovery Manager 会在测试网络上以及恢复站点中已复制数据的临时快照上运行虚拟机的恢复计划。Site Recovery Manager 不会中断受保护站点上的操作。

测试恢复计划会运行计划中的所有步骤，其中关闭受保护站点中虚拟机电源以及强制恢复站点中的设备对复制数据的控制除外。如果计划要求暂停恢复站点上的本地虚拟机，则 Site Recovery Manager 会在测试期间挂起这些虚拟机。运行恢复计划测试不会对任一站点上的生产环境进行其他任何更改。

测试恢复计划将会在恢复计划中虚拟机的所有磁盘文件的恢复站点创建一个快照。创建快照将增加存储器上的 I/O 滞后时间。在测试恢复计划时，如果您发现响应时间较长，并且您使用的是 VMware Virtual SAN 存储，请使用 Virtual SAN 界面中的监控工具监控 I/O 滞后时间。

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 右键单击计划，然后选择**测试**。还可以从“恢复步骤”选项卡运行测试。
- 3 （可选）选择**将最近的更改复制到恢复站点**。

选择此选项可确保恢复站点具有受保护虚拟机的最新副本，但同步可能需要更多的时间。

- 4 单击**下一步**。
- 5 检查测试信息，然后单击**完成**。
- 6 单击**恢复步骤**选项卡监控测试进度并响应消息。

**恢复步骤**选项卡将显示各个步骤的进度。“近期任务”中的“测试”任务将跟踪整体进度。

---

**注** Site Recovery Manager 按预定顺序运行恢复步骤，但不等待所有保护组的“准备存储”步骤完成即继续执行后续步骤。

---

### 后续步骤

在恢复计划测试完成后执行清理操作，将恢复计划恢复到测试前的原始状态。

## 测试恢复计划后清理

测试恢复计划后，可以通过运行清理操作使恢复计划返回到就绪状态。必须先完成清理操作，然后才能运行故障切换或其他测试。

Site Recovery Manager 在测试后将执行多个清理操作。

- 关闭已恢复虚拟机的电源。
- 使用占位虚拟机替换已恢复的虚拟机，并保留其标识和配置信息。
- 清理已恢复的虚拟机在测试期间使用的已复制存储快照。



## 前提条件

确认您已测试恢复计划。

## 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 右键单击恢复计划，然后选择**清理**。还可以从“恢复步骤”选项卡运行清理。
- 3 检查清理信息，然后单击**下一步**。
- 4 单击**完成**。
- 5 清理完成后，如果报告错误，请选中**强制清理**选项再次运行清理。

**强制清理**选项会强制移除虚拟机、忽略任何错误，并使计划返回到就绪状态。如有必要，可选中**强制清理**选项运行清理数次，直到清理成功为止。

## 运行恢复计划

运行恢复计划时，Site Recovery Manager 会将恢复计划中的所有虚拟机迁移至恢复站点。Site Recovery Manager 尝试关闭受保护站点中的相应虚拟机。

**小心** 恢复计划会大量更改受保护站点和恢复站点的配置，并会停止复制。请不要运行任何未经测试的恢复计划。撤消这些更改可能需要大量时间和精力，并且会导致延长服务停机时间。

## 前提条件

要使用强制恢复，您必须先启用此功能。如 [更改恢复设置](#) 中所述，通过启用 **recovery.forceRecovery** 设置来启用强制恢复。

## 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 右键单击恢复计划，然后选择**运行**。
- 3 检查确认提示中的信息，然后选择**我知道该过程将永久改变虚拟机及受保护数据中心和恢复数据中心的基架构**。
- 4 选择要运行的恢复类型。

选项	描述
计划的迁移	两个站点都在运行时，请将虚拟机恢复到恢复站点。如果计划的迁移期间受保护站点上出现错误，计划的迁移操作将失败。
灾难恢复	如果受保护站点出现问题，请将虚拟机恢复到恢复站点。如果灾难恢复期间受保护站点上出现错误，灾难恢复将继续执行而不会失败。

- 5 （可选）选中**强制恢复 - 仅限于恢复站点操作**复选框。  
如果已启用强制恢复功能并已选择**灾难恢复**，则此选项可用。
- 6 单击**下一步**。

- 7 查看恢复信息，然后单击**完成**。
- 8 单击**监控**选项卡，并单击**恢复步骤**。

**恢复步骤**选项卡将显示各个步骤的进度。“近期任务”区域报告整个计划的进度。

## 恢复虚拟机的时间点快照

通过 vSphere Replication，您可以保留虚拟机的时间点快照。可以将 Site Recovery Manager 配置为在您运行恢复计划时恢复虚拟机的多个时间点 (PIT) 快照。

可以在虚拟机上配置 vSphere Replication 时配置 PIT 快照的保留。有关 PIT 快照的详细信息，请参见[复制虚拟机并启用多个时间点实例](#)。

要启用 PIT 快照，请使用 vSphere Web Client 中的 vSphere Replication 界面配置虚拟机的复制。

在恢复期间，Site Recovery Manager 仅恢复最新的 PIT 快照。要恢复较旧的快照，您必须在 Site Recovery Manager 界面的“高级设置”中启用 `vrReplication > preserveMpitImagesAsSnapshots` 选项。如果您对已经配置了 IP 自定义的虚拟机恢复 PIT 快照，Site Recovery Manager 仅会将自定义应用到最新的 PIT 快照。如果您恢复已经配置了 IP 自定义的虚拟机并恢复到较旧的 PIT 快照，必须手动配置 IP 设置。

时间点恢复对基于阵列的复制不可用。

### 步骤

- 1 通过设置 **vrReplication > preserveMpitImagesAsSnapshots** 选项，将 Site Recovery Manager 配置为保留较旧的 PIT 快照。
- 2 使用 vSphere Replication 界面通过选择用于保留多个 PIT 快照的选项配置虚拟机的复制。
- 3 在 Site Recovery Manager 界面中，将虚拟机添加到 vSphere Replication 保护组中。
- 4 将 vSphere Replication 保护组包含到恢复计划中。
- 5 运行恢复计划。

恢复计划完成后，虚拟机将恢复到恢复站点，其中包含您配置的多个 PIT 快照。

- 6 在**虚拟机和模板**视图中，右键单击已恢复的虚拟机，然后依次选择**快照 > 快照管理器**。
- 7 选择此虚拟机的其中一个 PIT 快照，然后单击**转到**。  
已恢复的虚拟机将恢复到所选的 PIT 快照。
- 8 （可选）如果您已为虚拟机配置 IP 自定义，且如果您选择了较旧的 PIT 快照，而不是最新的快照，请在已恢复的虚拟机上手动配置 IP 设置。

## 取消测试或恢复

您可以在状态为“测试正在进行中”或“正在进行故障切换”时取消恢复计划测试。

取消测试或恢复时，Site Recovery Manager 并不会开始任何过程，而是使用某些规则来停止正在进行的过程。取消故障切换需要您重新运行故障切换。

- 在取消操作完成之前，无法停止的过程（如打开电源或等待检测信号）将运行到完成。



- 如果取消，则清理操作将撤消添加或移除存储设备过程。

取消测试或恢复所需的时间取决于当前正在进行的过程的类型和数量。

#### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 右键单击恢复计划，然后选择**取消**。还可以在“恢复步骤”选项卡中取消计划。

#### 后续步骤

在取消测试后运行清理。

## 导出恢复计划步骤

您可采用多种格式导出恢复计划的步骤以供日后参考，或者保留计划的打印件备份。

正在执行测试恢复或实际恢复时，无法导出恢复计划步骤。

#### 前提条件

确认您具有恢复计划。

#### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**监控**选项卡中，单击**恢复步骤**。
- 3 单击**导出恢复计划步骤**图标。

您可将恢复计划步骤另存为 HTML、XML、CSV 或者 MS Excel 或 Word 文档。

- 4 单击**生成报告**。
- 5 单击**下载报告**并关闭窗口。

## 查看和导出恢复计划历史记录

您可以查看和导出有关每次运行恢复计划、测试恢复计划或测试清理的报告。

恢复计划历史记录可提供有关每次运行、测试或清理恢复计划的信息。历史记录包含有关整个计划和计划中每个步骤的结果及开始时间和结束时间的信息。可以随时导出历史记录，但历史记录始终都只包含已完成操作的条目。如果操作正在执行中，则历史记录在该操作完成后才会显示。

SRM 会保留已删除恢复计划的历史记录。可以从**站点恢复 > 站点**导出现有计划和已删除计划的历史记录报告。选择一个站点并单击**恢复计划历史记录**选项卡。

#### 前提条件

您已运行或测试某一恢复计划，或者已在测试完成之后执行清理。

## 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**监控**选项卡上，单击**历史记录**。
- 3 （可选）单击“导出”图标以导出特定时段、恢复计划运行、测试或清理操作的恢复计划历史记录。

您可将恢复计划历史记录另存为 HTML、XML、CSV 或者 MS Excel 或 Word 文档。

## 删除恢复计划

如果不需要恢复计划，您可以将其删除。

恢复计划必须是一致的状态，然后您才能删除它。

## 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 （可选）在**监控**选项卡上，单击**恢复计划历史记录**，然后单击**导出历史记录报告**以下载该计划的历史记录。

您可以在**恢复计划历史记录**中查看已删除计划的历史记录。

- 3 右键单击要删除的恢复计划，然后选择**删除恢复计划**。

## 恢复计划状态参考

可以监控恢复计划的状态并确定在每个状态下允许的操作。恢复计划的状态由计划中保护组的状态来决定。

表 4-2. 恢复状态

状况	描述
就绪	恢复步骤已清除。
测试正在进行中	取消测试会将计划移至“取消正在进行中”状态。
测试已完成	测试已完成，存在或没有错误。
测试已中断	测试正在运行时服务器出现故障。
清理正在进行中	成功清理后，计划状态转为“就绪”。 如果清理未完成，则状态会转为“清理未完成”。 如果设置了“强制清理”选项，则在出现错误后状态转为“就绪”。 如果在清理过程中出现故障，则状态会转为“清理未完成”。
清理未完成	清理过程中出错。 可以再次运行清理。 如果在此状态下运行清理，则清理向导提供可忽略错误的选项。
清理已中断	Site Recovery Manager 在清理过程中失败。 无法更改恢复选项。

表 4-2. 恢复状态 （续）

状况	描述
恢复正在进行中	如果取消恢复，则状态会转为“取消正在进行中”。
灾难恢复已完成	<p>在受保护站点上进行恢复的过程中，虚拟机关机遇到错误，可能是因为未在裂脑之前连接站点。</p> <p>系统提示裂脑警告并在站点重新连接时再次运行恢复。</p> <p>站点连接后，状态会转为“所需恢复 (裂脑)”</p>
恢复已启动	<p>对等站点上已启动恢复，但如果站点未连接，则确切状态未知。</p> <p>登录到恢复站点或重新连接站点以获取当前状态。</p>
所需恢复 (裂脑)	<p>在恢复过程中站点断开连接。重新连接站点时检测到裂脑情况。</p> <p>系统提示您再次运行恢复以同步站点。</p>
恢复已完成	<p>虚拟机均已恢复，但存在错误。再次运行恢复不会修复这些错误。</p> <p>在解决裂脑恢复后，计划转为此状态。</p> <p>可以查看上次恢复运行的恢复步骤。</p>
恢复未完成	<p>取消的恢复或数据存储错误。再次运行恢复。</p> <p>需要解决这些错误并重新运行恢复，或移除出现错误的虚拟机的保护。计划检测到通过两种方式之一解决了错误，并将状态更新为“恢复已完成”。</p>
部分恢复	某些（但并非所有）保护组通过重叠计划恢复。
恢复已中断	恢复过程中出现故障导致恢复暂停。单击 <b>恢复</b> 继续。无法更改恢复选项。
取消正在进行中	<p>取消测试会导致“测试已完成”，并取消上次结果。</p> <p>取消恢复会导致“恢复未完成”，并取消上次结果。</p>
重新保护正在进行中	如果在此状态下服务器出现故障，则会转为“重新保护已中断”。
部分重新保护	<p>已重新保护重叠计划。</p> <p>已重新保护的组会转为“就绪”状态，但是只有在其他组处于“已恢复”状态下，该状态才有效。</p>
重新保护未完成	重新保护未完成存储操作。必须连接站点才能在新运行中成功重新保护。
重新保护已中断	如果在重新保护过程中 Site Recovery Manager Server 失败，则再次运行重新保护以继续并正确清理状态。
在测试过程中等待用户输入	测试已暂停。关闭该提示以恢复测试。
在恢复过程中等待用户输入	恢复已暂停。关闭该提示以继续进行恢复。
保护组正在使用中	<p>计划包含正在由其他计划用于测试的组。在其他计划已完成组中的测试操作但尚未运行清理时，也会出现此状态。</p> <p>等待其他计划完成测试、清理或编辑计划以移除这些组。</p>

表 4-2. 恢复状态（续）

状况	描述
方向错误	<p>组处于混合状态下，这是一种无效状态。某些组在两个方向均已就绪：一个站点受保护，而一个站点在特定组中已恢复。移除某些保护组。</p> <p>对于出现的此错误，重叠计划已运行并已经重新保护计划中的所有组。</p>
计划不同步	<p>此状态可能在不同情况下出现：</p> <ul style="list-style-type: none"> <li>■ 在成功测试恢复和清理操作之间。当计划处于此状态时，无法编辑计划。运行清理可将计划返回至“就绪”状态。如果计划仍处于“计划不同步”状态，请编辑该计划。</li> <li>■ 在常规操作过程中，可以编辑计划。</li> </ul> <p>打开计划进行编辑会导致 Site Recovery Manager 在保护和恢复 Site Recovery Manager 服务器之间强制同步与计划有关的 Site Recovery Manager 内部数据，这会清除“计划不同步”状态。</p>
无保护组	<p>计划不包含任何保护组，因而计划无法运行。</p> <p>可以通过 API 或删除保护组来创建空计划。</p>
内部错误	<p>计划中存在未知状态的保护组，或发生了其他一些意外错误。</p> <p>无法运行计划，但可以删除计划。</p>

# 配置恢复计划

# 5

您可以配置恢复计划以在 **Site Recovery Manager Server** 或虚拟机上运行命令、显示计划运行时需要响应的消息、恢复期间挂起非重要的虚拟机、配置虚拟机之间的依赖关系、自定义虚拟机网络设置，以及更改受保护虚拟机的恢复优先级。

简单的恢复计划（仅指定已恢复的虚拟机要连接的测试网络以及虚拟机等待打开电源和进行自定义的超时值）可以提供一种有效的方式来测试 **Site Recovery Manager** 配置。大多数恢复计划需要先进行配置，然后才能在生产中使用。例如，受保护站点上用于紧急情况的恢复计划可能不同于服务从一个站点计划迁移到另一站点的恢复计划。

---

**注** 恢复计划将始终反映其恢复的保护组的当前状况。如果保护组中的任何成员显示除“正常”之外的状态，则必须先解决问题，然后才能对恢复计划进行更改。

---

## ■ 恢复计划步骤

恢复计划运行的一系列步骤必须按给定工作流（例如计划的迁移或重新保护）的特定顺序执行。无法更改这些步骤的顺序或目的，但可以插入自己的显示消息和运行命令的步骤。

## ■ 创建自定义恢复步骤

您可以创建自定义恢复步骤，以便在恢复过程中运行命令或向用户显示消息。

## ■ 运行恢复计划时挂起虚拟机

**Site Recovery Manager** 可在恢复和测试恢复期间挂起恢复站点上的虚拟机。

## ■ 指定虚拟机的恢复优先级

默认情况下，**Site Recovery Manager** 将新的恢复计划中的所有虚拟机的恢复优先级设置为 3。您可以提升或降低虚拟机的恢复优先级。恢复优先级指定虚拟机的关机和开机顺序。

## ■ 配置虚拟机依赖关系

如果某台虚拟机依赖于同一保护组中其他虚拟机上运行的服务，则可以在这些虚拟机之间配置依赖关系。通过配置依赖关系，可以确保虚拟机在恢复站点上按正确的顺序启动。只有虚拟机具有相同优先级时，依赖关系才有效。

## ■ 配置虚拟机启动和关机选项

您可以配置恢复期间虚拟机在恢复站点上如何启动和关机。

## 恢复计划步骤

恢复计划运行的一系列步骤必须按给定工作流（例如计划的迁移或重新保护）的特定顺序执行。无法更改这些步骤的顺序或目的，但可以插入自己的显示消息和运行命令的步骤。

Site Recovery Manager 会通过不同的方式运行不同的恢复计划步骤。

- 一些步骤在所有恢复过程中运行。
- 一些步骤仅在测试恢复过程中运行。
- 有些步骤在测试恢复过程中总是跳过。

在自定义恢复计划时，了解恢复步骤的内容、顺序及运行环境非常重要。

## 恢复顺序

运行恢复计划时，首先会关闭受保护站点中虚拟机的电源。Site Recovery Manager 会根据您设置的优先级关闭虚拟机的电源，高优先级的虚拟机最后关闭电源。Site Recovery Manager 会在测试恢复计划时省略此步骤。

Site Recovery Manager 会根据您设置的优先级，在恢复站点上打开虚拟机组的电源。在启动某个优先级组之前，下一个更高优先级组中的所有虚拟机必须恢复或恢复失败。如果在同一优先级组的虚拟机之间存在依赖关系，Site Recovery Manager 会首先打开其他虚拟机所依赖的虚拟机的电源。如果 Site Recovery Manager 可以满足虚拟机依赖关系，Site Recovery Manager 会尝试并行打开 vCenter Server 支持的最大数量的虚拟机的电源。

## 恢复计划超时与暂停

运行恢复计划的步骤时可能会出现多种超时情况。超时会导致计划在指定的时间间隔内暂停，为完成步骤留出时间。

消息步骤在得到用户确认之前会强制暂停计划。在向恢复计划添加消息步骤前，请确保其确有必要。在测试或运行包含消息步骤的恢复计划之前，请确保用户可以监控计划进度并根据需要对消息做出响应。

## 创建自定义恢复步骤

您可以创建自定义恢复步骤，以便在恢复过程中运行命令或向用户显示消息。

Site Recovery Manager 可以在 Site Recovery Manager Server 上或属于恢复计划的虚拟机中运行自定义步骤。您无法在要挂起的虚拟机上运行自定义步骤。

在重新保护过程中，Site Recovery Manager 将在恢复计划中保留所有自定义恢复步骤。如果在重新保护之后执行恢复或测试，则会在新的恢复站点（即原始受保护站点）上运行自定义恢复步骤。

重新保护之后，您通常无需修改而直接使用自定义恢复步骤来显示消息。如果某些自定义恢复步骤所运行的命令包含特定于站点的信息（如网络配置），则可能需要在重新保护之后修改这些步骤。

- **自定义恢复步骤的类型**

可以创建将包含在恢复计划中的不同类型的自定义恢复步骤。

## ■ Site Recovery Manager 如何处理自定义恢复步骤故障

Site Recovery Manager 将根据恢复步骤的类型以不同的方式处理自定义恢复步骤故障。

## ■ 创建顶级消息提示或命令步骤

您可以在恢复计划的任意位置添加顶级恢复步骤。顶级命令步骤是在恢复期间您在 Site Recovery Manager Server 上运行的命令或脚本。您也可以添加在恢复期间显示用户必须确认的消息提示的步骤。

## ■ 为单个虚拟机创建消息提示或命令步骤

您可以创建自定义恢复步骤以在 Site Recovery Manager 打开虚拟机电源之前或之后提示用户或提示 Site Recovery Manager 对虚拟机执行任务。

## ■ 写入命令步骤的准则

添加到恢复计划中的自定义恢复步骤的所有批处理文件或命令都必须满足某些要求。

## ■ 命令步骤的环境变量

Site Recovery Manager 可提供在自定义恢复步骤的命令中可以使用的环境变量。

# 自定义恢复步骤的类型

可以创建将包含在恢复计划中的不同类型的自定义恢复步骤。

自定义恢复步骤可以是命令恢复步骤，也可以是消息提示步骤。

## 命令恢复步骤

命令恢复步骤包含顶级命令或每虚拟机命令。

### 顶级命令

在 Site Recovery Manager Server 上运行。例如，您可以使用这些命令打开物理设备的电源或重定向网络流量。

### 每虚拟机命令

在恢复过程中，Site Recovery Manager 会将每虚拟机命令与新恢复的虚拟机相关联。打开虚拟机电源后，可以使用这些命令完成配置任务。您可在打开虚拟机电源之前或之后运行这些命令。配置为在打开虚拟机电源后运行的命令可以在 Site Recovery Manager Server 上运行，也可以在新恢复的虚拟机中运行。在新恢复的虚拟机上运行的命令将在该虚拟机上的 VMware Tools 所使用的用户帐户上下文中运行。您可能需要更改 VMware Tools 在已恢复的虚拟机上使用的用户帐户，具体取决于所写入的命令的功能。

## 消息提示恢复步骤

恢复过程中会在 Site Recovery Manager 用户界面中显示消息。可以使用此消息暂停恢复并向运行恢复计划的用户提供信息。例如，该消息可指导用户执行手动恢复任务或验证步骤。用户直接响应提示时可采取的唯一操作是关闭消息，这允许恢复继续进行。

## Site Recovery Manager 如何处理自定义恢复步骤故障

Site Recovery Manager 将根据恢复步骤的类型以不同的方式处理自定义恢复步骤故障。

Site Recovery Manager 将尝试完成所有自定义恢复步骤，但某些命令恢复步骤可能无法完成。

### 命令恢复步骤

默认情况下，Site Recovery Manager 等待命令恢复步骤完成的时间为 5 分钟。可以配置每个命令的超时时间。如果命令在此超时期限内完成，则会运行恢复计划中的下一个恢复步骤。Site Recovery Manager 将根据命令类型来处理自定义命令的故障。

命令类型	描述
顶级命令	如果恢复步骤失败，则 Site Recovery Manager 将记录失败情况并在 <b>恢复步骤</b> 选项卡上显示警告。后续的自定义恢复步骤将继续运行。
每虚拟机命令	将在虚拟机电源打开之前或之后以批处理模式运行。如果某一命令失败，则该批处理中剩余的每虚拟机命令不再运行。例如，如果添加五个命令以在打开电源前运行，并添加五个命令以在打开电源后运行，假定在打开电源前的批处理中第三个命令失败，则在打开电源前运行的其余两个命令将不再运行。Site Recovery Manager 不会打开虚拟机电源，因而无法运行任何打开电源后的命令。

### 消息提示恢复步骤

发布消息提示的自定义恢复步骤不能失败。在用户关闭提示之前，恢复计划将暂停执行。

## 创建顶级消息提示或命令步骤

您可以在恢复计划的任意位置添加顶级恢复步骤。顶级命令步骤是在恢复期间您在 Site Recovery Manager Server 上运行的命令或脚本。您也可以添加在恢复期间显示用户必须确认的消息提示的步骤。

#### 前提条件

- 您具有一个恢复计划，可向其添加自定义步骤。
- 有关写入命令以添加到命令步骤的信息，请参见 [写入命令步骤的准则](#)和 [命令步骤的环境变量](#)。

#### 步骤

- 1 在 vSphere Web Client 中，选择 **站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在 **监控** 选项卡上，单击 **恢复步骤**。
- 3 使用 **查看** 下拉菜单，选择添加步骤要运行的恢复计划的类型。

选项	描述
测试步骤	添加测试恢复计划时运行的步骤。
恢复步骤	添加执行计划的迁移或灾难恢复时运行的步骤

您不能在清理或重新保护操作中添加步骤。

- 4 右键单击某个步骤，您可在该步骤之前或之后添加自定义步骤，然后选择 **添加步骤**。
- 5 选择对 **SRM Server** 的 **命令**或**提示**。



- 6 在**名称**文本框中，输入步骤名称。  
步骤名称将显示在**恢复步骤**视图中的步骤列表中。
- 7 在**内容**文本框中，输入使步骤运行的命令。
  - 如果选择**对 SRM Server 的命令**，则输入要运行的命令或脚本。
  - 如果选择**提示**，则输入要在恢复计划运行期间显示的消息文本。
- 8 （可选）修改 Site Recovery Manager Server 上运行的命令的**超时**设置。  
如果创建提示步骤，则此选项不可用。
- 9 选择在步骤顺序中插入新步骤的位置。
  - 在所选步骤之前
  - 在所选步骤之后
- 10 单击**确定**即可向恢复计划中添加步骤。

## 为单个虚拟机创建消息提示或命令步骤

您可以创建自定义恢复步骤以在 Site Recovery Manager 打开虚拟机电源之前或之后提示用户或提示 Site Recovery Manager 对虚拟机执行任务。

Site Recovery Manager 将命令步骤与受保护虚拟机或已恢复虚拟机关联的方式和自定义信息相同。如果多个恢复计划包含同一个虚拟机，那么 Site Recovery Manager 会将命令和提示包含到所有这些恢复计划中。

### 前提条件

- 您具有一个恢复计划，可向其添加自定义步骤。
- 有关写入命令以添加到命令步骤的信息，请参见[写入命令步骤的准则](#)和[命令步骤的环境变量](#)。

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**相关对象**选项卡上，单击**虚拟机**。
- 3 右键单击虚拟机，然后单击**配置恢复**。
- 4 在**恢复属性**选项卡上，单击**打开电源前步骤**或**打开电源后步骤**。
- 5 单击加号图标以添加步骤。

## 6 选择要创建的步骤类型。

选项	描述
提示	提示用户执行某个任务或提供必须确认的信息，然后计划才能继续到下一步。此选项可用于打开电源前步骤和打开电源后步骤。
对 SRM 服务器的命令	在 Site Recovery Manager Server 上运行命令。此选项可用于打开电源前步骤和打开电源后步骤。
对恢复的虚拟机的命令	在已恢复的虚拟机上运行命令。此选项仅可用于打开电源后步骤。

## 7 在名称文本框中，输入步骤名称。

步骤名称将显示在**恢复步骤**视图中的步骤列表中。

## 8 在内容文本框中，输入使步骤运行的命令。

- 如果您选择了对 **SRM Server 的命令**或对**恢复的虚拟机的命令**，请输入要运行的命令或脚本。
- 如果选择**提示**，则输入要在恢复计划运行期间显示的消息文本。

## 9 （可选）修改 Site Recovery Manager Server 上运行的命令的**超时**设置。

如果创建提示步骤，则此选项不可用。

## 10 单击**确定**即可向恢复计划中添加步骤。

## 11 单击**确定**以重新配置虚拟机，以便在虚拟机打开电源之前或之后运行命令。

## 写入命令步骤的准则

添加到恢复计划中的自定义恢复步骤的所有批处理文件或命令都必须满足某些要求。

创建命令步骤以添加到恢复计划时，请确保考虑了运行此命令所必需的环境。命令步骤中的错误会影响恢复计划的完整性。先在恢复站点的 Site Recovery Manager Server 上测试该命令，然后再将其添加到计划中。

- 必须使用 Windows Command Shell 在本地主机上的完整路径将其启动。例如，要运行位于 `c:\alarmscript.bat` 中的脚本，请使用以下命令行：

```
c:\windows\system32\cmd.exe /c c:\alarmscript.bat
```

- 必须在恢复站点中的 Site Recovery Manager Server 上安装批处理文件和命令。
- 批处理文件和命令必须在 300 秒内完成。否则，恢复计划会终止并显示错误。要更改此限制，请参见[更改恢复设置](#)。
- 生成输出（其中包含 ASCII 值大于 127 的字符）的批处理文件或命令必须使用 UTF-8 编码。Site Recovery Manager 在日志文件和恢复历史记录中仅记录脚本输出中的最后 4KB 内容。生成更多输出的脚本应将输出重定向到文件，而不是将输出发送至要记录的标准输出。

## 命令步骤的环境变量

Site Recovery Manager 可提供在自定义恢复步骤的命令中可以使用的环境变量。

命令步骤使用 LocalSystem 帐户的标识在恢复站点的 Site Recovery Manager Server 主机上运行。命令步骤运行时，Site Recovery Manager 将提供可供其使用的环境变量。

表 5-1. 可用于所有命令步骤的环境变量

名称	值	示例
<i>VMware_RecoveryName</i>	正在运行的恢复计划的名称。	计划 A
<i>VMware_RecoveryMode</i>	恢复模式。	测试或恢复
<i>VMware_VC_Host</i>	恢复站点中 vCenter Server 的主机名。	vc_hostname.example.com
<i>VMware_VC_Port</i>	用于访问 vCenter Server 的网络端口。	443

Site Recovery Manager 使附加环境变量可用于在 Site Recovery Manager Server 或已恢复虚拟机上运行的每个虚拟机命令步骤。

表 5-2. 可用于每个虚拟机命令步骤的环境变量

名称	值	示例
<i>VMware_VM_Uuid</i>	vCenter 唯一标识此虚拟机时使用的 UUID。	4212145a-eeae-a02c-e525-ebba70b0d4f3
<i>VMware_VM_Name</i>	在受保护站点中设置的此虚拟机的名称。	我的新虚拟机
<i>VMware_VM_Ref</i>	虚拟机的受管对象 ID。	vm-1199
<i>VMware_VM_Guest Name</i>	VIM API 定义的客户端操作系统的名称。	otherGuest
<i>VMware_VM_GuestIP</i>	虚拟机的 IP 地址（如果已知）。	192.168.0.103
<i>VMware_VM_Path</i>	此虚拟机的 VMDK 的路径。	[datastore-123] jquser-vm2/jquser-vm2.vmdk

## 运行恢复计划时挂起虚拟机

Site Recovery Manager 可在恢复和测试恢复期间挂起恢复站点上的虚拟机。

在双活数据中心环境中，在恢复站点上运行非关键工作负载时，在恢复站点上挂起虚拟机非常有用。通过在恢复站点上挂起托管非关键工作负载的任何虚拟机，Site Recovery Manager 可为恢复的虚拟机释放容量。Site Recovery Manager 将恢复故障切换操作期间（故障切换反向运行时）挂起的虚拟机。

您只能添加要在恢复站点上挂起的虚拟机。

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**监控**选项卡中，单击**恢复步骤**。

- 3 右键单击**挂起恢复站点中的非关键虚拟机**并选择**添加非关键虚拟机**。
- 4 选择恢复站点上要在恢复期间挂起的虚拟机。
- 5 单击**确定**。

#### 结果

Site Recovery Manager 会在恢复计划运行时在恢复站点上挂起这些虚拟机。

## 指定虚拟机的恢复优先级

默认情况下，Site Recovery Manager 将新的恢复计划中的所有虚拟机的恢复优先级设置为 3。您可以提升或降低虚拟机的恢复优先级。恢复优先级指定虚拟机的关机 and 开机顺序。

如果更改虚拟机的优先级，Site Recovery Manager 会将新的优先级应用于包含此虚拟机的所有恢复计划。

Site Recovery Manager 会根据您设置的优先级，在恢复站点上启动虚拟机。Site Recovery Manager 首先启动优先级为 1 的虚拟机，然后启动优先级为 2 的虚拟机，以此类推。Site Recovery Manager 使用 VMware Tools 检测信号发现虚拟机在恢复站点上运行的时间。通过此方法，Site Recovery Manager 可确保在启动下一个优先级的虚拟机之前给定优先级的所有虚拟机均在运行。因此，必须在受保护的虚拟机上安装 VMware Tools。

#### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**相关对象**选项卡上，单击**虚拟机**。
- 3 右键单击虚拟机并选择**所有优先级操作**。
- 4 为该虚拟机选择新的优先级。  
最高优先级为 1。最低优先级为 5。
- 5 单击**是**确认更改优先级。

## 配置虚拟机依赖关系

如果某台虚拟机依赖于同一保护组中其他虚拟机上运行的服务，则可以在这些虚拟机之间配置依赖关系。通过配置依赖关系，可以确保虚拟机在恢复站点上按正确的顺序启动。只有虚拟机具有相同优先级时，依赖关系才有效。

恢复计划运行时，Site Recovery Manager 会先启动其他虚拟机依赖的虚拟机，然后再启动具有依赖关系的虚拟机。如果 Site Recovery Manager 无法启动其他虚拟机依赖的虚拟机，恢复计划会继续运行但会显示警告。只能在位于相同恢复优先级组的虚拟机之间配置依赖关系。如果您将虚拟机配置为依赖于较低优先级组中的虚拟机，则 Site Recovery Manager 会替代此依赖关系并先启动较高优先级组中的虚拟机。

如果您从恢复计划中移除了包含所依赖虚拟机的保护组，则具有依赖关系的虚拟机的依赖关系中，保护组的状态将设置为不在此计划中 (Not in this Plan)。如果配置的虚拟机与其依赖的虚拟机的优先级不相同，则所依赖的虚拟机的状态将设置为“较低优先级”或“较高优先级”。

### 前提条件

- 验证具有依赖关系的虚拟机及其依赖的虚拟机是否在同一恢复计划中。
- 验证具有依赖关系的虚拟机及其依赖的虚拟机是否在同一恢复优先级组中。

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**相关对象**选项卡上，单击**虚拟机**。
- 3 右键单击依赖于一台或多台其他虚拟机的虚拟机，然后选择**配置恢复**。
- 4 展开**虚拟机依赖关系**。
- 5 验证此虚拟机依赖的虚拟机是否已启动，并验证依赖关系的状态是否为“良好”。
- 6 （可选）要移除依赖关系，请从此虚拟机依赖的虚拟机的列表中选择一台虚拟机，然后单击**移除**。
- 7 单击**确定**。

## 配置虚拟机启动和关机选项

您可以配置恢复期间虚拟机在恢复站点上如何启动和关机。

您可以配置是否先关闭虚拟机的客户机操作系统，然后再在受保护站点上关闭虚拟机电源。您可以配置是否在恢复站点上打开虚拟机电源。您也可以在打开虚拟机电源之后再配置延迟，以便允许 **VMware Tools** 或其他应用程序先在已恢复的虚拟机上启动，然后再继续恢复计划。

### 前提条件

您已创建一个恢复计划。

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**相关对象**选项卡上，单击**虚拟机**。
- 3 右键单击虚拟机，然后选择**配置恢复**。
- 4 展开**关机操作**，然后选择此虚拟机的关机方法。

选项	描述
关闭客户机操作系统后再关闭电源	正常关闭虚拟机后再关闭电源。您可以为关机操作设置一个超时期限。将超时期限设为 0 相当于关闭电源选项。此选项需要 <b>VMware Tools</b> 在虚拟机上运行。
关闭电源	关闭虚拟机电源，但不关闭客户机操作系统。

- 5 展开**启动操作**并选择是否在恢复后打开虚拟机电源。

选项	描述
打开电源	在恢复站点上打开虚拟机电源。
不打开电源	恢复虚拟机，但不打开电源。

- 6 （可选）选中或取消选中**等待 VMware Tools** 复选框。

此选项仅在**步骤 5**中选择了**打开电源**时可用。

如果您选择**等待 VMware Tools**，则 Site Recovery Manager 会等待 VMware Tools 在打开虚拟机电源后启动，然后再继续恢复计划到下一步。您可以设置启动 VMware Tools 的超时期限。

- 7 （可选）选中或取消选中**在运行打开电源后步骤并启动从属虚拟机之前的额外延迟**复选框，并指定额外延迟的时间。

此选项仅在**步骤 5**中选择了**打开电源**时可用。

例如，您可以指定一个打开虚拟机电源之后的额外延迟，以允许其他虚拟机所依赖的应用程序启动。

# 自定义虚拟机的 IP 属性

## 6

可为受保护站点和恢复站点自定义虚拟机的 IP 设置。当已恢复虚拟机在目标站点上启动时，虚拟机的自定义 IP 属性将替代默认的 IP 设置。

如果不自定义虚拟机的 IP 属性，则 Site Recovery Manager 在从保护站点到恢复站点的恢复或测试过程中将使用恢复站点的 IP 设置。重新保护后，Site Recovery Manager 在从原始恢复站点到原始保护站点的恢复或测试过程中将使用保护站点的 IP 设置。

Site Recovery Manager 支持不同类型的 IP 自定义。

- 使用 IPv4 和 IPv6 地址。
- 为每个站点配置不同的 IP 自定义。
- 使用 DHCP、静态 IPv4 或静态 IPv6 地址。
- 自定义 Windows 和 Linux 虚拟机的地址。
- 为每个虚拟机自定义多个网卡。

有关 Site Recovery Manager 支持其 IP 自定义的客户机操作系统的列表，请参见 vCenter Site Recovery Manager 5.8 的兼容性列表，网址为 <https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html>。

可以将自定义设置与受保护虚拟机相关联。因此，如果同一受保护虚拟机属于多个恢复计划，则所有恢复计划都将使用自定义设置的单一副本。可以在配置虚拟机的恢复属性过程中配置 IP 自定义。

如果不在恢复站点上自定义网卡，则该网卡继续使用受保护站点的 IP 设置，反之亦然，且 Site Recovery Manager 不会在恢复过程中将 IP 自定义应用于虚拟机。

可以将 IP 自定义应用于单个或多个虚拟机。

如果在虚拟机上配置 IP 自定义，则 Site Recovery Manager 会向这些虚拟机添加恢复步骤。

### 客户机操作系统启动

对于配置 IP 自定义的所有虚拟机，客户机启动过程将同时启动。

### 自定义 IP

Site Recovery Manager 会将 IP 自定义推送到虚拟机。

### 客户机操作系统关闭

Site Recovery Manager 会关闭并重新引导虚拟机，以确保更改生效，并确保客户机操作系统服务在虚拟机重新启动时会应用这些更改。

IP 自定义过程完成后，虚拟机将根据设置的优先级组和任何依赖关系打开电源。在为每个虚拟机执行“等待 VMTTools”过程之前，会立即开始打开电源过程。

---

**注** 要自定义虚拟机的 IP 属性，必须在虚拟机上安装 VMware Tools 或 VMware 操作系统特定软件包 (OSP)。请参见 <http://www.vmware.com/download/packages.html>。

---

- **手动自定义单个虚拟主机的 IP 属性**

可以手动为受保护站点和恢复站点的各个虚拟机自定义 IP 设置。

- **自定义多个虚拟机的 IP 属性**

您可以通过使用 DR IP Customizer 工具并定义子网级别 IP 映射规则，来自定义受保护站点和恢复站点上多个虚拟机的 IP 属性。

## 手动自定义单个虚拟主机的 IP 属性

可以手动为受保护站点和恢复站点的各个虚拟机自定义 IP 设置。

---

**注** 手动定义 IP 自定义内容的虚拟机在恢复期间不受 IP 映射规则评估的控制。手动指定的 IP 配置优先于 IP 映射规则。

---

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**，然后选择一个恢复计划。
- 2 在**相关对象**选项卡上，单击**虚拟机**。
- 3 右键单击虚拟机，然后单击**配置恢复**。
- 4 单击 **IP 自定义**选项卡，然后选择**手动 IP 自定义**。
- 5 选择要修改 IP 设置的网卡。
- 6 单击**配置保护**或**配置恢复**，具体视要配置受保护站点上的 IP 设置还是恢复站点上的 IP 设置而定。
- 7 单击**常规**选项卡以配置设置。
  - a 选择要使用的寻址类型。

可用选项包括 DHCP、静态 IPv4 或静态 IPv6。
  - b 对于静态地址，输入 IP 地址、子网信息和网关服务器地址。

或者，如果虚拟机已打开电源并已安装 VMware Tools，则可以单击**检索**以导入在虚拟机上配置的当前设置。



## 8 单击 **DNS** 选项卡以配置 DNS 设置。

### a 选择查找 DNS 服务器的方式。

可使用 DHCP 查找 DNS 服务器，或者可指定主 DNS 服务器和备用 DNS 服务器。

### b 输入 DNS 后缀，然后单击**添加**，或者选择现有 DNS 后缀，然后单击**移除**、**上移**或**下移**。

## 9 单击 **WINS** 选项卡输入主 WINS 地址和辅助 WINS 地址。

仅当为 Windows 虚拟机配置 DHCP 或 IPv4 地址时，**WINS** 选项卡才可用。

## 10 重复步骤 6 到步骤 9 以配置恢复站点或受保护站点设置（如果需要）。

例如，如果配置了受保护站点的 IP 设置，则可能希望配置恢复站点的设置。

## 11 根据需要对其他网卡重复配置过程。

# 自定义多个虚拟机的 IP 属性

您可以通过使用 DR IP Customizer 工具并定义子网级别 IP 映射规则，来自定义受保护站点和恢复站点上多个虚拟机的 IP 属性。

在先前版本的 Site Recovery Manager 中，您已通过使用 DR IP Customizer 工具定义了多个虚拟机的 IP 属性。除了 DR IP Customizer 之外，还可以在 Site Recovery Manager 5.8 中通过定义子网级别 IP 自定义规则来自定义多个虚拟机的 IP 属性。

可以将子网级别 IP 自定义规则与 DR IP Customizer 组合在一起使用。

- 通过 DR IP Customizer，可快速地使用 CSV 文件为多个虚拟机定义明确的 IP 自定义设置。
- 可以通过使用 vSphere Web Client 为虚拟机应用子网级别 IP 自定义规则。

使用 DR IP Customizer 配置的虚拟机不受子网级别 IP 自定义规则的限制。可以通过使用 DR IP Customizer 或 IP 子网规则实现相同的 IP 自定义结果。在 Site Recovery Manager 5.8 中，DR IP Customizer 可以更好地控制各个虚拟机的 IP 配置，如自定义静态 IPv6。在从使用了 DR IP Customizer 的早期版本的 Site Recovery Manager 进行升级时，此控制是非常有用的。

## 使用 DR IP Customizer 工具自定义多个虚拟机的 IP 属性

通过 DR IP Customizer 工具，可为受保护站点和恢复站点上的多个受保护虚拟机定义明确的 IP 自定义设置。

除了定义子网 IP 映射规则外，还可以使用 DR IP Customizer 工具在虚拟机于恢复站点上启动时将自定义网络设置应用到这些虚拟机。您可以在逗号分隔值 (CSV) 文件中为 DR IP Customizer 工具提供自定义 IP 设置。

无需手动创建 CSV 文件，可以使用 DR IP Customizer 工具导出包含受保护虚拟机的网络配置相关信息的 CSV 文件。可以通过自定义该文件中的值将该文件用作要在恢复站点上应用的 CSV 文件的模板。

- 1 运行 DR IP Customizer 以生成包含受保护虚拟机的网络信息的 CSV 文件。
- 2 修改生成的 CSV 文件中与恢复站点相关的网络信息。

- 3 再次运行 DR IP Customizer 以应用 CSV，其中包含虚拟机在恢复站点上启动时所应用的经过修改的网络配置。

可以在受保护站点或恢复站点上运行 DR IP Customizer 工具。受保护虚拟机的虚拟机 ID 在每个站点都不同，因此无论您在运行 DR IP Customizer 工具生成 CSV 文件时使用哪一个站点，再次运行 DR IP Customizer 应用设置时，都必须使用同一个站点。

可以自定义受保护站点和恢复站点的 IP 设置，使 Site Recovery Manager 能够在重新保护操作期间使用正确的配置。

有关 Site Recovery Manager 支持其 IP 自定义的客户机操作系统的列表，请参见 vCenter Site Recovery Manager 5.8 的兼容性列表，网址为 <https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html>。

#### ■ 报告恢复计划的 IP 地址映射

IP 地址映射报告程序可生成 XML 文档，描述受保护虚拟机及其占位虚拟机的 IP 属性（按站点和恢复计划进行分组）。此信息可帮助您了解恢复计划的网络要求。

#### ■ DR IP Customizer 工具的语法

DR IP Customizer 工具包含一些选项，可用来收集有关 Site Recovery Manager 保护的虚拟机的网络信息。也可以使用这些选项为在恢复站点上启动的虚拟机应用自定义设置。

#### ■ DR IP Customizer CSV 文件的结构

DR IP Customizer 逗号分隔值 (CSV) 文件由标题行（定义文件中每一列的含义）和对应于恢复计划中每个占位虚拟机的一个或多个行组成。

#### ■ 修改 DR IP Customizer CSV 文件

您可以修改 DR IP Customizer 逗号分隔值 (CSV) 文件，以便当虚拟机在恢复站点上启动时，对这些虚拟机应用自定义网络设置。

#### ■ 运行 DR IP Customizer 自定义多个虚拟机的 IP 属性

可以使用 DR IP Customizer 工具为 Site Recovery Manager 所保护的多个虚拟机自定义 IP 属性。

## 报告恢复计划的 IP 地址映射

IP 地址映射报告程序可生成 XML 文档，描述受保护虚拟机及其占位虚拟机的 IP 属性（按站点和恢复计划进行分组）。此信息可帮助您了解恢复计划的网络要求。

由于 IP 地址映射报告程序必须连接到两个站点，因此可在任一站点上运行命令。命令运行时，会提示您输入每个站点的 vCenter 登录凭据。

### 步骤

- 1 在受保护站点或恢复站点的 Site Recovery Manager Server 主机上打开 Command Shell。
- 2 更改为 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin 目录。

3 如下例所示，运行 `dr-ip-reporter.exe` 命令。

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
```

要将网络列表限制为仅包含特定恢复计划所需的网络，请按以下示例所示，在命令行中包含 `-plan` 选项。

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
--plan recovery_plan_name
```

---

**注** 此命令通常会要求您验证每个站点上证书所表示的指纹。可以通过包含 `-i` 选项来取消验证请求。

---

## DR IP Customizer 工具的语法

DR IP Customizer 工具包含一些选项，可用来收集有关 Site Recovery Manager 保护的虚拟机的网络信息。也可以使用这些选项为在恢复站点上启动的虚拟机应用自定义设置。

---

**注** 该版本的 Site Recovery Manager 允许定义子网级别的 IP 映射规则，以自定义虚拟机上的 IP 设置，以及使用 DR IP Customizer 池。可以将子网级别的 IP 映射规则与 DR IP Customizer 结合使用。有关如何将子网级别 IP 映射规则与 DR IP Customizer 一起使用的信息，请参见[自定义多个虚拟机的 IP 属性](#)。

---

您可以在 Site Recovery Manager Server 主机上的 `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` 中找到可执行文件 `dr-ip-customizer.exe`。运行 `dr-ip-customizer.exe` 时，可根据要生成还是要应用逗号分隔值文件 (CSV) 来指定不同的选项。

```
dr-ip-customizer.exe
--cfg SRM 服务器配置 XML
--cmd apply/drop/generate
[--csv 现有 CSV 文件的名称]
[--out 要生成的新 CSV 文件的名称]
[--vc vCenter Server 地址]
[--ignore-thumbprint]
[--extra-dns-columns]
[--verbose]
```

可以在受保护站点或恢复站点上运行 DR IP Customizer 工具。受保护虚拟机的虚拟机 ID 在每个站点都不同，因此无论您在运行 DR IP Customizer 工具生成 CSV 文件时使用哪一个站点，再次运行 DR IP Customizer 应用设置时，都必须使用同一个站点。

DR IP Customizer 工具所提供的选项中有些是必选项，其他则为可选项。

表 6-1. DR IP Customizer 选项

选项	描述	必选
-h [ --help ]	显示有关 dr-ip-customizer.exe 的使用情况信息。	否
--cfg arg	Site Recovery Manager Server 的 XML 配置文件 vmware-dr.xml 文件的路径。	是
--cmd arg	<p>您可以指定不同的命令以便在不同的模式中运行 DR IP Customizer。</p> <ul style="list-style-type: none"> <li>■ apply 命令将现有 CSV 文件中的网络自定义设置应用到 Site Recovery Manager Server 实例上的恢复计划。</li> <li>■ generate 命令为 Site Recovery Manager 针对 vCenter Server 实例所保护的所有虚拟机生成一个基本 CSV 文件。</li> <li>■ drop 命令从输入 CSV 文件所指定的虚拟机中删除恢复设置。</li> </ul> <p>对于 apply 和 drop 命令，始终提供生成 CSV 文件所使用的同一个 vCenter Server 实例。</p>	是
--csv arg	用作输入的 CSV 文件的路径。	是，当运行 apply 和 drop 命令时。
-o [ --out ] arg	generate 命令创建的新 CSV 输出文件的名称。如果提供现有 CSV 文件的名称，则 generate 命令将覆盖其当前内容。	是，当运行 generate 命令时。
--vc arg	vCenter Server 地址。每个站点的受保护虚拟机的虚拟机 ID 都不同。当您生成 CSV 文件并应用该文件时，应使用同一个 vCenter Server 实例。	是
-i [ --ignore-thumbprint ]	忽略 vCenter Server 指纹确认提示。	否
-e [ --extra-dns-columns ]	弃用。	否
-v [ --verbose ]	启用详细输出。可在任何 --verbose 命令行中包含 dr-ip-customizer.exe 选项以记录额外的诊断消息。	否

## DR IP Customizer CSV 文件的结构

DR IP Customizer 逗号分隔值 (CSV) 文件由标题行（定义文件中每一列的含义）和对应于恢复计划中每个占位虚拟机的一个或多个行组成。

**注** 该版本的 Site Recovery Manager 允许定义子网级别的 IP 映射规则，以自定义虚拟机上的 IP 设置，以及使用 DR IP Customizer 池。可以将子网级别的 IP 映射规则与 DR IP Customizer 结合使用。有关如何能将子网级别 IP 映射规则与 DR IP Customizer 一起使用的信息，请参见[自定义多个虚拟机的 IP 属性](#)。

同时为这两个站点配置 IP 设置是一项可选操作。可以只为受保护站点提供设置，或者只为恢复站点提供设置，也可以为这两个站点都提供设置。可以通过完全不同的方式将每个站点配置为使用一组不同的网络适配器。

CSV 文件中有些字段在每一行中都是必填字段。其他字段在不需要自定义设置时可以保留空白。

**表 6-2. DR IP Customizer CSV 文件的列**

列	描述	自定义规则
虚拟机 ID	DR IP Customizer 从多个行中收集信息以应用于单个虚拟机时所使用的唯一标识符。此 ID 是 DR IP Customizer 的内部 ID，与 vCenter Server 使用的虚拟机 ID 不同。	不可自定义。不能为空。
虚拟机名称	显示在 vCenter Server 清单中的人工可读的虚拟机名称。	不可自定义。不能为空。
vCenter Server	受保护站点或恢复站点上的 vCenter Server 实例的地址。您可以在 vCenter Server 列中设置每个站点上虚拟机的 IP 设置。	不可自定义。不能为空。 该列可以同时包含两个 vCenter Server 实例。每个 vCenter Server 实例都要有与之对应的行。您可以配置一组 IP 设置在一个站点上使用，配置另一组 IP 设置在其他站点上使用。您也可以在这两个站点上都提供 IP 设置来执行重新保护操作。
适配器 ID	要自定义的适配器的 ID。适配器 ID 0 设置虚拟机的所有适配器上的全局设置。适配器 ID 1、2、3 等等的设置值用来配置虚拟机上特定网卡的设置。	可自定义。不能留空。 在适配器 ID 为 0 的行中，可修改的字段只有“DNS 服务器”和“DNS 后缀”。如果已指定这些值，则此 VM ID 所使用的的所有其他适配器都将继承这些值。 CSV 文件可在多行中包含多个 DNS 服务器。例如，如果需要两台全局 DNS 主机，可以加上两个适配器 ID 为 0 的行。 <ul style="list-style-type: none"> <li>■ 一行包含所有虚拟机信息和一台 DNS 主机。</li> <li>■ 另一行只包含第二台 DNS 主机。</li> </ul> 要为特定适配器另外添加一台 DNS 服务器，请在相应的适配器行中加入 DNS 服务器。例如，将 DNS 服务器添加到适配器 ID 1。

表 6-2. DR IP Customizer CSV 文件的列（续）

列	描述	自定义规则
DNS 域	此适配器的 DNS 域。	可自定义。可以留空。 如果输入值，其格式必须为 <b>example.company.com</b> 。
网络 BIOS	选择是否激活此适配器上的 NetBIOS。	可自定义。可以留空。 如果未留空，该列必须包含以下字符串之一：disableNetBIOS、enableNetBIOS 或 enableNetBIOSViaDhcp。
主要 WINS	DR IP Customizer 会验证 WINS 设置是否仅应用于 Windows 虚拟机，但不验证 NetBIOS 设置。	可自定义。可以留空。
辅助 WINS	DR IP Customizer 会验证 WINS 设置是否仅应用于 Windows 虚拟机，但不验证 NetBIOS 设置。	可自定义。可以留空。
IP 地址	此虚拟机的 IPv4 地址。	可自定义。不能为空。 虚拟机可以有多个虚拟网络适配器。您可以为每个虚拟网络适配器配置一个静态 IPv4 地址或一个静态 IPv6 地址。例如，如果设置静态 IPv4 地址，则必须将 IPv6 地址设置为 DHCP。
子网掩码	此虚拟机的子网掩码。	可自定义。可以留空。
网关	此虚拟机的一个或多个 IPv4 网关。	可自定义。可以留空。
IPv6 地址	此虚拟机的 IPv6 地址。	可自定义。如果不使用 IPv6，则可以留空。 虚拟机可以有多个虚拟网络适配器。您可以为每个虚拟网络适配器配置一个静态 IPv4 地址或一个静态 IPv6 地址。例如，如果设置静态 IPv6 地址，则必须将 IPv4 地址设置为 DHCP。 如果在 Windows Server 2003 上运行 Site Recovery Manager Server，并且为虚拟机自定义 IPv6 地址，则必须在 Site Recovery Manager Server 实例上启用 IPv6。Site Recovery Manager 在自定义期间执行 IP 地址验证，如果自定义 IPv6 地址，则要在 Site Recovery Manager Server 上启用 IPv6。 Windows Server 的新版本默认启用 IPv6。
IPv6 子网前缀长度	要使用的 Ipv6 子网前缀长度。	可自定义。可以留空。
IPv6 网关	此适配器的一个或多个 IPv4 网关。	可自定义。可以留空。

表 6-2. DR IP Customizer CSV 文件的列（续）

列	描述	自定义规则
DNS 服务器	一个或多个 DNS 服务器的地址。	可自定义。可以留空。 如果在适配器 ID 为 0 的行中输入此设置，则该设置将被视为全局设置。在 Windows 虚拟机上，如果在适配器 ID 不为 0 的行中设置了该设置，则该设置将应用于每个适配器。 在 Linux 虚拟机上，该设置始终是所有适配器的全局设置。 该列可以包含每个网卡的一个或多个 IPv4 或 IPv6 DNS 服务器。
DNS 后缀	DNS 服务器的一个或多个后缀。	可自定义。可以留空。 这些设置是 Windows 和 Linux 虚拟机上的所有适配器的全局设置。

## 修改 DR IP Customizer CSV 文件

您可以修改 DR IP Customizer 逗号分隔值 (CSV) 文件，以便当虚拟机在恢复站点上启动时，对这些虚拟机应用自定义网络设置。

**注** 该版本的 Site Recovery Manager 允许定义子网级别的 IP 映射规则，以自定义虚拟机上的 IP 设置，以及使用 DR IP Customizer 池。可以将子网级别的 IP 映射规则与 DR IP Customizer 结合使用。有关如何将子网级别 IP 映射规则与 DR IP Customizer 一起使用的信息，请参见[自定义多个虚拟机的 IP 属性](#)。

在 CSV 文件中表示虚拟机网络配置的一个难题在于虚拟机配置包含分层信息。例如，单个虚拟机可能包含多个适配器，且每个适配器的元素（如网关）可能具有多个列表。CSV 格式并不提供分层表示的机制。因此，CSV 文件中 DR IP Customizer 生成的每一行都可能会提供特定虚拟机的部分或全部相关信息。

对于具有简单网络配置的虚拟机，所有信息可以只包含在一行中。对于更为复杂的虚拟机，则可能需要占用多行。具有多个网卡或多个网关的虚拟机需要占用多行。CSV 文件中的每一行都包含标识信息，用于描述该信息将应用到哪个虚拟机和适配器。信息整合在一起后，可应用到相应虚拟机。

修改 DR IP Customizer CSV 文件时请遵循以下准则。

- 如果不需要某个设置，则忽略其值。
- 每个适配器均使用可能的最少行数。
- 在任何字段中都不要使用逗号。
- 根据需要指定适配器 ID 设置。DR IP Customizer 将您在 ID 为 0 的适配器上所指定的设置应用于所有网卡。要将设置应用于单个网卡，请在适配器 ID 1、2、...、 $n$  字段中指定相应值。
- 要为某一列指定多个值，请为此适配器再创建一行，并在这一行的该行中填写值。为确保附加行与指定虚拟机相关联，应复制“虚拟机 ID”、“虚拟机名称”、vCenter Server 和“适配器 ID”列的值。
- 要为每个受保护站点和恢复站点上的某个网络适配器指定一个 IP 地址，或指定多个 DNS 服务器地址，应为每个地址新增一行。将“虚拟机 ID”、“虚拟机名称”和“适配器 ID”值复制到每一行。

## DR IP Customizer CSV 文件示例

通过 `--cmd generate` 命令运行 `dr-ip-customizer.exe`，获取一个包含 vCenter Server 上受保护虚拟机的网络信息的 CSV 文件。编辑该 CSV 文件，对受保护虚拟机的 IP 设置进行自定义。

**注** 该版本的 Site Recovery Manager 允许定义子网级别的 IP 映射规则，以自定义虚拟机上的 IP 设置，以及使用 DR IP Customizer 池。可以将子网级别的 IP 映射规则与 DR IP Customizer 结合使用。有关如何将子网级别 IP 映射规则与 DR IP Customizer 一起使用的信息，请参见[自定义多个虚拟机的 IP 属性](#)。

### 示例：生成的 DR IP Customizer CSV 文件

对于只有两个受保护虚拟机的简单安装，生成的 CSV 文件可能只包含虚拟机 ID、虚拟机名称、两个站点上 vCenter Server 实例的名称以及一个适配器。

```
VM ID,VM Name,vCenter Server,Adapter ID,DNS Domain,Net BIOS,
Primary WINS,Secondary WINS,IP Address,Subnet Mask,Gateway(s),
IPv6 Address,IPv6 Subnet Prefix length,IPv6 Gateway(s),
DNS Server(s),DNS Suffix(es)
protected-vm-10301,vm-3-win,vcenter-server-site-B,0,,,,,,,,,
protected-vm-10301,vm-3-win,vcenter-server-site-A,0,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-A,0,,,,,,,,,
```

以上生成的 CSV 文件显示了两个虚拟机：vm-3-win 和 vm-1-linux。它们位于受保护站点和恢复站点（即 vcenter-server-site-B 和 vcenter-server-site-A）上。DR IP Customizer 为每个虚拟机和每个站点生成一个适配器 ID 为 0 的条目。如果您知道每个虚拟机上的网卡数量，则可另外添加一些行来自定义每个网卡。

### 示例：设置静态 IPv4 地址

可以对生成的 CSV 文件进行修改，将使用静态 IPv4 地址的两个网络适配器分配给受保护站点和恢复站点上的其中一个虚拟机 vm-3-win。

为了方便阅读，下表中的示例 CSV 文件已将空列省略。“DNS 域”、“NetBIOS”、“IPv6 地址”、“IPv6 子网前缀长度”和“IPv6 网关”列也已全部省略。

表 6-3. 在修改的 CSV 文件中设置静态 IPv4 地址

虚拟机 ID	虚拟机名称	vCenter Server	适配器 ID	主要 WINS	次要 WINS	IP 地址	子网掩码	网关	DNS 服务器	DNS 后缀
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com



表 6-3. 在修改的 CSV 文件中设置静态 IPv4 地址（续）

虚拟机 ID	虚拟机名称	vCenter Server	适配器 ID	主要 WINS	次要 WINS	IP 地址	子网掩码	网关	DNS 服务器	DNS 后缀
protected-vm-103-01		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	1.1.1.1	
protected-vm-103-01		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-103-01	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-103-01	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-103-01		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
protected-vm-103-01		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

以上 CSV 文件中的信息将不同的静态 IPv4 设置应用到受保护站点和恢复站点上的 vm-3-win。

- 在 vcenter-server-site-B 站点上：
  - 为该虚拟机的所有网卡设置 DNS 后缀 example.com 和 eng.example.com。
  - 添加一个网卡（适配器 ID 1），其主要 WINS 服务器和辅助 WINS 服务器分别为 2.2.3.4 和 2.2.3.5，静态 IPv4 地址为 192.168.1.21，DNS 服务器为 1.1.1.1。
  - 添加一个网卡（适配器 ID 2），其主要 WINS 服务器和辅助 WINS 服务器分别为 2.2.3.4 和 2.2.3.5，静态 IPv4 地址为 192.168.1.22，DNS 服务器为 1.1.1.2。
- 在 vcenter-server-site-A 站点上：
  - 为该虚拟机的所有网卡设置 DNS 后缀 example.com 和 eng.example.com。
  - 为该虚拟机的所有网卡设置 DNS 服务器 1.1.0.1 和 1.1.0.2。
  - 添加一个静态 IPv4 地址为 192.168.0.21 的网卡（适配器 ID 1）。
  - 添加一个网卡（适配器 ID 2），其主要 WINS 服务器和辅助 WINS 服务器分别为 1.2.3.4 和 1.2.3.5，静态 IPv4 地址为 192.168.0.22。

**示例：设置静态 IPv4 地址和 DHCP IPv4 地址**

可以对生成的 CSV 文件进行修改，将多个网卡分配给其中一个虚拟机 **vm-3-win**，该虚拟机结合使用静态 IPv4 地址和 DHCP IPv4 地址。这些设置在受保护站点和恢复站点上可以不同。

为了方便阅读，下表中的示例 CSV 文件已将空列省略。“DNS 域”、“NetBIOS”、“IPv6 地址”、“IPv6 子网前缀长度”和“IPv6 网关”列也已全部省略。

**表 6-4. 在修改的 CSV 文件中设置静态 IPv4 地址和 DHCP IPv4 地址**

虚拟机 ID	虚拟机名称	vCenter Server	适配器 ID	主要 WINS	次要 WINS	IP 地址	子网掩码	网关	DNS 服务器	DNS 后缀
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp				
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

以上 CSV 文件中的信息将不同的静态和动态 IPv4 设置应用到受保护站点和恢复站点上的 **vm-3-win**。

- 在 **vcenter-server-site-B** 站点上：
  - 为该虚拟机的所有网卡设置 DNS 后缀 **example.com** 和 **eng.example.com**。

- 添加一个网卡（适配器 ID 1），其主要 WINS 服务器和辅助 WINS 服务器分别为 2.2.3.4 和 2.2.3.5，静态 DNS 服务器为 1.1.1.1，并且使用 DHCP 来获取 IP 地址。
- 添加一个网卡（适配器 ID 2），其主要 WINS 服务器和辅助 WINS 服务器分别为 2.2.3.4 和 2.2.3.5，静态 IPv4 地址为 192.168.1.22，DNS 服务器为 1.1.1.2。
- 在 vcenter-server-site-A 站点上：
  - 为该虚拟机的所有网卡将 DNS 后缀设置为 example.com 和 eng.example.com。
  - 为该虚拟机的所有网卡设置 DNS 服务器 1.1.0.1 和 1.1.0.2。
  - 添加一个网卡（适配器 ID 1），该网卡使用 DHCP 来获取 IPv4 地址和全局分配的 DNS 服务器信息。
  - 添加一个网卡（适配器 ID 2），其主要 WINS 服务器和辅助 WINS 服务器分别为 1.2.3.4 和 1.2.3.5，静态 IPv4 地址为 192.168.0.22。

#### 示例：设置静态 IPv4 和 IPv6 地址以及 DHCP IPv4 和 IPv6 地址

可以对生成的 CSV 文件进行修改，将多个网卡分配给其中一个虚拟机 vm-3-win。网卡可以将静态 IPv4 和 IPv6 地址以及 DHCP IPv4 和 IPv6 地址结合使用。这些设置在受保护站点和恢复站点上可以不同。

为了方便阅读，下表中的示例 CSV 文件已将空列省略。“DNS 域”和“NetBIOS”列已省略。

表 6-5. 在修改的 CSV 文件中设置静态 IPv4 和 IPv6 地址以及 DHCP IPv4 和 IPv6 地址

虚拟机 ID	虚拟机名称	vCenter Server	适配器 ID	主要 WINS	次要 WINS	IP 地址	子网掩码	网关	IPv6 地址	IPv6 子网前缀长度	IPv6 网关	DNS 服务器	DNS 后缀
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	dhcp			1.1.1.1	

表 6-5. 在修改的 CSV 文件中设置静态 IPv4 和 IPv6 地址以及 DHCP IPv4 和 IPv6 地址（续）

虚拟机 ID	虚拟机名称	vCenter Server	适配器 ID	主要 WINS	次要 WINS	IP 地址	子网掩码	网关	IPv6 地址	IPv6 子网前缀长度	IPv6 网关	DNS 服务器	DNS 后缀
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	dhcp			::ffff:192.168.1.22	32	::ffff:192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	
protected-vm-10301		vcenter-server-site-A	1									::ffff:192.168.0.251	
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.0	192.168.0.1				1.1.1.1	

以上 CSV 文件中的信息将不同的 IP 设置应用到受保护站点和恢复站点上的 vm-3-win。

■ 在 vcenter-server-site-B 站点上：

- 为该虚拟机的所有网卡设置 DNS 后缀 example.com 和 eng.example.com。
- 添加一个网卡（适配器 ID 1），其主要 WINS 服务器和辅助 WINS 服务器分别为 2.2.3.4 和 2.2.3.5，静态 IPv4 地址为 192.168.1.21，DNS 服务器为 1.1.1.1，并且使用 DHCP 来获取 IPv6 地址。

- 添加一个网卡（适配器 ID 2），其主要 WINS 服务器和辅助 WINS 服务器分别为 2.2.3.4 和 2.2.3.5，静态 IPv6 地址为 ::ffff:192.168.1.22，DNS 服务器为 1.1.1.2，并且使用 DHCP 来获取 IPv4 地址。
- 在 vcenter-server-site-A 站点上：
  - 为该虚拟机的所有网卡将 DNS 后缀设置为 example.com 和 eng.example.com。
  - 添加一个网卡（适配器 ID 1），该网卡使用 DHCP 获取 IPv4 地址并设置静态 IPv6 地址 ::ffff:192.168.1.22。适配器 ID 1 使用静态 IPv6 DNS 服务器 ::ffff:192.168.0.250 和 ::ffff:192.168.0.251。
  - 添加一个网卡（适配器 ID 2），其主要 WINS 服务器和辅助 WINS 服务器分别为 1.2.3.4 和 1.2.3.5，静态 IPv4 地址为 192.168.0.22，DNS 服务器为 1.1.1.1。通过将 IPv6 列留空，适配器 ID 2 使用 DHCP 获取 IPv6 地址。

## 运行 DR IP Customizer 自定义多个虚拟机的 IP 属性

可以使用 DR IP Customizer 工具为 Site Recovery Manager 所保护的多个虚拟机自定义 IP 属性。

**注** 该版本的 Site Recovery Manager 允许定义子网级别的 IP 映射规则，以自定义虚拟机上的 IP 设置，以及使用 DR IP Customizer 池。可以将子网级别的 IP 映射规则与 DR IP Customizer 结合使用。有关如何将子网级别 IP 映射规则与 DR IP Customizer 一起使用的信息，请参见[自定义多个虚拟机的 IP 属性](#)。

### 前提条件

在对环境中的 vCenter Server 实例具有访问权限的计算机上使用 DR IP Customizer 工具。

### 步骤

- 1 在 Site Recovery Manager Server 主机上打开 Command Shell。
- 2 将目录更改为 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin。
- 3 运行 dr-ip-customizer.exe 命令生成包含受保护虚拟机相关信息的逗号分隔值 (CSV) 文件。

```
dr-ip-customizer.exe
--cfg ..\config\vmware-dr.xml
--cmd generate
--out "path_to_CSV_file.csv"
--vc vcenter_server_address
```

本示例中的 dr-ip-customizer.exe 将指向 Site Recovery Manager Server 的 vmware-dr.xml 文件，并为位于 *vcenter\_server\_address* 的 vCenter Server 实例生成 *path\_to\_CSV\_file.csv* 文件。

- 4 （可选）验证 vCenter Server 指纹并输入 **y** 确认您信任此 vCenter Server 实例。

如果指定 --ignore-thumbprint 选项，则不会提示您检查指纹。

## 5 输入 vCenter Server 实例的登录凭据。

可能会再次提示您确认信任此 vCenter Server 实例。

## 6 编辑所生成的 CSV 文件，自定义恢复计划中虚拟机的 IP 属性。

您可以使用电子表格应用程序编辑 CSV 文件。以新名称保存经过修改的 CSV 文件。

## 7 运行 dr-ip-customizer.exe 应用经过修改的 CSV 文件中的自定义 IP 属性。

可以在受保护站点或恢复站点上运行 DR IP Customizer 工具。受保护虚拟机的虚拟机 ID 在每个站点都不同，因此无论您在运行 DR IP Customizer 工具生成 CSV 文件时使用哪一个站点，再次运行 DR IP Customizer 应用设置时，都必须使用同一个站点。

```
dr-ip-customizer.exe
--cfg ..\config\vmware-dr.xml
--cmd apply
--csv "path_to_CSV_file.csv"
--vc vcenter_server_address
```

本示例中的 dr-ip-customizer.exe 将指向 Site Recovery Manager Server 的 vmware-dr.xml 文件，并把 path\_to\_CSV\_file.csv 文件中的自定义设置应用于位于 vcenter\_server\_address 的 vCenter Server 实例。

## 结果

指定的自定义内容会在恢复期间应用到 CSV 文件中列出的所有虚拟机。编辑这些虚拟机的恢复计划属性时，无需为这些虚拟机手动配置 IP 设置。

## 通过定义 IP 自定义规则自定义多台虚拟机的 IP 属性

您可以为受保护站点和恢复站点上选定的已配置虚拟网络映射指定单个子网级别的 IP 映射规则。

子网级别映射并不需要定义精确的适配器级别 IP 映射。相反，您只需定义一个 IP 自定义规则，Site Recovery Manager 会应用到相关适配器。IP 自定义规则用于测试和恢复工作流。不能在不同的网络映射之间重用 IP 自定义规则。

---

**重要事项** IP 子网映射规则仅支持 IPv4。Site Recovery Manager 不支持基于规则的 IPv6 自定义。Site Recovery Manager 并不评估配置为使用手动 IP 自定义的虚拟机的 IP 映射规则。

---

IP 自定义规则应用于从受保护站点 IPv4 子网故障切换至恢复站点 IPv4 子网的虚拟机，例如从 10.17.23.0/24 到 10.18.22.0/24。IP 自定义规则规定了在恢复期间 Site Recovery Manager 将评估已恢复虚拟机 NIC 的现有 IP 配置，并为 10.18.22.0/24 子网重新配置 10.17.23.0/24 子网上找到的静态 NIC。

如果规则匹配，则 Site Recovery Manager 通过保留原始 IPv4 地址的主机位并将其置于目标子网，以从旧地址派生新的静态 IPv4 地址。例如，如果原始受保护站点地址是 10.17.23.55/24，则新地址是 10.18.22.55/24。

如果默认网关文本框为空，则 Site Recovery Manager 通过保留原始 IPv4 地址的主机位并将其置于目标子网，以从原始参数派生新的网关参数。例如，如果原始受保护站点网关是 10.17.23.1，则新网关是 10.18.22.1。如果指定了明确的网关参数，则 Site Recovery Manager 将检查 IPv4 地址语法是否正确并完全应用该参数。

Site Recovery Manager 将应用指定的 DNS 和其他参数。启用 DHCP 的 NIC 不受自定义规则约束，因为其网络配置在恢复期间保持不变。

#### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 在**管理**选项卡上，选择**网络映射**。
- 3 选择要定义自定义规则的网络映射。
- 4 要定义规则，请单击**添加 IP 自定义规则**。
- 5 输入规则的名称。
- 6 指定映射到受保护站点和恢复站点的子网 IP 范围。
- 7 指定恢复站点网络的网络设置。
- 8 单击**确定**保存更改。

### 将 IP 自定义规则应用到虚拟机

您可以将 IP 自定义规则应用到受保护虚拟机的恢复设置。

应用 IP 自定义规则时，应为每个网络映射指定单个子网 IP 映射。

如果将高级设置选项 `recovery.useIpMapperAutomatically` 设置为 **True** 且为虚拟网络配置了 IP 映射规则，则 Site Recovery Manager 会在恢复期间评估子网 IP 映射规则以自定义虚拟机。如果将此选项设置为 **False**，则 Site Recovery Manager 不会在恢复期间评估 IP 映射规则。您可以使用 **IP 自定义**选项，替代此选项对每台虚拟机的影响。

`recovery.useIpMapperAutomatically` 默认选项是 **True**。如果将其设置为 **Auto**，则 Site Recovery Manager 将使用 IP 自定义规则自定义虚拟机。

#### 前提条件

有关 Site Recovery Manager 支持其 IP 自定义的客户机操作系统的列表，请参见 vCenter Site Recovery Manager 5.8 的兼容性列表，网址为 <https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html>。

#### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**。
- 2 在**相关对象**选项卡上，单击**虚拟机**。
- 3 右键单击虚拟机，然后单击**配置恢复**。
- 4 单击 **IP 自定义**。
- 5 从 IP 自定义模式列表中，选择**使用 IP 自定义规则 (如果适用)**，然后单击**确定**。

# 恢复后重新保护虚拟机

# 7

执行恢复后，恢复站点将成为新的受保护站点，但不受保护。如果原始受保护站点处于运行状态，则可以通过将原始受保护站点用作新的恢复站点来保护新的受保护站点，从而反转保护方向。

通过重新创建所有保护组和恢复计划来反向手动重新建立保护很耗时且容易出错。**Site Recovery Manager** 会提供重新保护功能，这是一种自动实现反向保护的方式。

**Site Recovery Manager** 执行恢复后，受保护虚拟机将在恢复站点上启动。由于之前的受保护站点可能已脱机，因此这些虚拟机不受保护。当受保护站点恢复联机后，通过运行重新保护，可以反转复制方向，以保护恢复站点上已恢复的虚拟机，使其重新返回到原始受保护站点上。

重新保护将使用在执行恢复之前建立的保护信息反转保护方向。仅当恢复完成且未出现任何错误之后才能启动重新保护过程。如果恢复已完成，但出现错误，则必须修复所有错误并重新运行恢复，重复此过程，直到不出现任何错误。

重新保护操作完成后，可以执行测试，以确认受保护站点和恢复站点的新配置有效。

您可针对包含为基于阵列的复制和 vSphere Replication 配置的虚拟机的保护组执行重新保护。

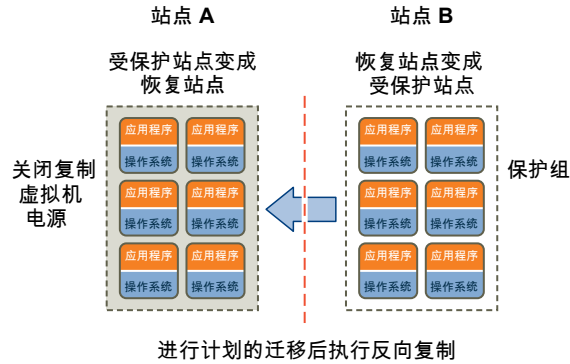
## 示例： 执行重新保护操作

站点 A 是受保护站点，站点 B 是恢复站点。如果站点 A 脱机，请运行恢复计划中的灾难恢复 workflow，以使虚拟机在站点 B 上联机。恢复后，来自站点 A 的受保护虚拟机将在站点 B 上启动，但不受保护。

当站点 A 恢复联机时，请通过执行计划的迁移来完成恢复，因为站点 A 虚拟机和数据存储需要先关闭电源并卸载，然后才能进行反向保护。随后，请启动重新保护操作，以保护站点 B 上的已恢复虚拟机。此时，站点 B 将成为受保护站点，而站点 A 则成为恢复站点。**Site Recovery Manager** 将从站点 B 到站点 A 执行反向复制。



图 7-1. Site Recovery Manager 重新保护过程



#### ■ Site Recovery Manager 如何使用基于阵列的复制重新保护虚拟机

在使用基于阵列的复制执行重新保护的过程中，Site Recovery Manager 先反转保护的方向，然后强制将存储从新的受保护站点同步到新的恢复站点。

#### ■ Site Recovery Manager 如何利用 vSphere Replication 重新保护虚拟机

在利用 vSphere Replication 的重新保护过程中，Site Recovery Manager 先反转保护的方向，然后强制将存储从新的受保护站点同步到新的恢复站点。

#### ■ 执行重新保护的前提条件

仅当满足特定的前提条件时才能执行重新保护。

#### ■ 重新保护虚拟机

重新保护将使 Site Recovery Manager 保护组和恢复计划的重新配置反向生效。执行重新保护操作后，可以使用计划的迁移工作流将虚拟机恢复为原始站点。

#### ■ 重新保护状态

重新保护过程会经历几个状态，您可以在 vSphere Client 的 Site Recovery Manager 插件的恢复计划中查看这些状态。

## Site Recovery Manager 如何使用基于阵列的复制重新保护虚拟机

在使用基于阵列的复制执行重新保护的过程中，Site Recovery Manager 先反转保护的方向，然后强制将存储从新的受保护站点同步到新的恢复站点。

启动重新保护过程时，Site Recovery Manager 指示基础存储阵列进行反向复制。反向复制后，Site Recovery Manager 会在新的恢复站点（即执行重新保护之前的原始受保护站点）创建占位虚拟机。

在新的受保护站点创建占位虚拟机时，Site Recovery Manager 会利用原始受保护虚拟机的位置来确定创建占位虚拟机的位置。Site Recovery Manager 使用原始受保护虚拟机的标识来创建占位虚拟机。如果原始受保护虚拟机不再可用，则 Site Recovery Manager 会利用从原始恢复站点到原始受保护站点的清单映射来确定占位虚拟机的资源池和文件夹。运行重新保护过程之前必须先在这两个站点上配置清单映射，否则该过程可能会失败。

使用基于阵列的复制重新保护虚拟机时，Site Recovery Manager 会将占位虚拟机的文件放置在原始受保护站点的占位数据存储中，而不是存放原始受保护虚拟机的数据存储中。

强制将数据从新的保护站点同步到新的恢复站点，可确保恢复站点具有在保护站点上运行的受保护虚拟机的当前副本。强制执行此同步可确保在完成重新保护过程后能立即进行恢复。

要了解 Site Recovery Manager 如何使用 vSphere Replication 重新保护虚拟机，请参见 [Site Recovery Manager 如何利用 vSphere Replication 重新保护虚拟机](#)。

## Site Recovery Manager 如何利用 vSphere Replication 重新保护虚拟机

在利用 vSphere Replication 的重新保护过程中，Site Recovery Manager 先反转保护的方向，然后强制将存储从新的受保护站点同步到新的恢复站点。

利用 vSphere Replication 执行重新保护时，Site Recovery Manager 在同步期间使用原始的 VMDK 文件作为初始副本。恢复过程中出现的完全同步主要执行校验和，只通过网络传输少量数据。

强制将数据从新的保护站点同步到新的恢复站点，可确保恢复站点具有在保护站点上运行的受保护虚拟机的当前副本。强制执行此同步可确保在完成重新保护过程后能立即进行恢复。

## 执行重新保护的前提条件

仅当满足特定的前提条件时才能执行重新保护。

您可针对包含为基于阵列的复制和 vSphere Replication 配置的虚拟机的保护组执行重新保护。

必须先满足以下前提条件，然后才能运行重新保护。

- 1 运行计划的迁移，并确保成功完成恢复计划的所有步骤。如果在恢复期间出现错误，请解决产生这些错误的问题，然后重新运行恢复。在重新运行恢复时，先前已成功完成的操作将被跳过。例如，已成功恢复的虚拟机将不会重新进行恢复，并且会无中断地继续运行。
- 2 原始受保护站点必须可用。vCenter Server 实例、ESXi Server、Site Recovery Manager Server 实例和相应的数据库必须都是可恢复的。
- 3 如果已执行灾难恢复操作，则当两个站点再次运行时必须执行计划的迁移。如果在尝试计划的迁移期间出错，则必须更正错误并重新运行计划的迁移，直到成功为止。

在某些情况下，重新保护不可用。

- 无法顺利完成恢复计划。要使重新保护可用，必须成功完成恢复计划的所有步骤。
- 无法还原原始站点，例如，物理灾难破坏了原始站点。要解除受保护站点和恢复站点之间的配对，并重新创建配对，这两个站点必须都可用。如果无法还原原始的受保护站点，则必须在受保护站点和恢复站点上重新安装 Site Recovery Manager。

## 重新保护虚拟机

重新保护将使 Site Recovery Manager 保护组和恢复计划的重新配置反向生效。执行重新保护操作后，可以使用计划的迁移 workflows 将虚拟机恢复为原始站点。

### 前提条件

请参见[执行重新保护的前提条件](#)。

### 步骤

- 1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**。
- 2 右键单击恢复计划，然后选择**重新保护**。
- 3 选中用于确认您了解重新保护操作不可逆的复选框。
- 4 （可选）选中**强制清理**复选框以忽略对恢复站点执行清理操作期间出现的错误，然后单击**下一步**。  
只有在执行了初始重新保护操作并且出现错误后，**强制清理**选项才可用。
- 5 查看重新保护信息，然后单击**完成**。
- 6 选择恢复计划并单击**监控 > 恢复步骤**选项卡，以监控重新保护操作的进度。
- 7 重新保护操作完成后，选择恢复计划，单击**监控 > 历史记录**，然后单击**导出选定历史记录项的报告按钮**。

即使重新保护操作期间出错，恢复计划仍可恢复到就绪状态。检查重新保护操作的历史记录报告，确保没有出错。如果在重新保护期间出错，请尝试修复错误并运行测试恢复，确保错误已修复。如果您未修复在重新保护期间发生的错误，随后又在未修复的情况下尝试运行计划的迁移或灾难恢复，有些虚拟机可能无法恢复。

### 结果

Site Recovery Manager 会互换恢复站点和受保护站点。Site Recovery Manager 会在新恢复站点从新的受保护站点创建虚拟机的占位副本。

## 重新保护状态

重新保护过程会经历几个状态，您可以在 vSphere Client 的 Site Recovery Manager 插件的恢复计划中查看这些状态。

如果重新保护失败，或部分成功，您可以执行补救措施以完成重新保护。

表 7-1. 重新保护状态

状况	描述	补救措施
重新保护正在进行中	Site Recovery Manager 正在运行重新保护。	无
部分重新保护	如果多个恢复计划共享同一保护组，并且在一些计划中的某些组（而不是其他的组）中成功进行重新保护，将出现部分重新保护。	在部分重新保护的计划中重新运行重新保护。
重新保护未完成	由于重新保护期间出现故障而出现此状况。例如，如果同步存储失败或创建占位虚拟机失败，均可能出现此状况。	<ul style="list-style-type: none"> <li>■ 如果重新保护操作无法同步存储，请确保站点处于连接状态，检查 vSphere Client 的重新保护进度，然后重新启动重新保护任务。如果重新保护仍未完成，请使用<b>强制清理</b>选项运行重新保护任务。</li> <li>■ 如果 Site Recovery Manager 创建占位虚拟机失败，则仍可进行恢复。在 vSphere Client 中查看重新保护的步骤，解决任何存在的问题，然后重新启动重新保护任务。</li> </ul>
重新保护已中断	如果一个 Site Recovery Manager 服务器在重新保护过程中意外停止，会导致重新保护中断。	确保两个 Site Recovery Manager 服务器均在运行并再次启动重新保护任务。

# 通过执行故障恢复来还原恢复前的站点配置

## 8

恢复后，要还原受保护站点和恢复站点的原始配置，您可以执行一系列称为故障恢复的可选步骤。

计划迁移或灾难恢复完成后，之前的恢复站点成为受保护站点。恢复完成后，新的受保护站点没有可恢复到的恢复站点。如果您运行重新保护，新的受保护站点由原始保护站点进行保护（与原始保护方向反向）。有关重新保护的信息，请参见第 7 章 [恢复后重新保护虚拟机](#)。

要在恢复前将受保护站点和恢复站点的配置还原到其初始配置，请执行故障恢复。

要执行故障恢复，请运行一系列重新保护以及计划的迁移操作。

- 1 执行重新保护。恢复站点将成为受保护站点。之前的受保护站点将成为恢复站点。
- 2 执行已计划的迁移，以关闭受保护站点上的虚拟机和启动恢复站点上的虚拟机。为避免中断虚拟机的可用性，您可能要在开始计划的迁移之前运行测试。如果测试中发现错误，则可在执行计划的迁移之前解决这些错误。
- 3 再次执行重新保护，以便在恢复之前将受保护站点和恢复站点恢复为其原始配置。

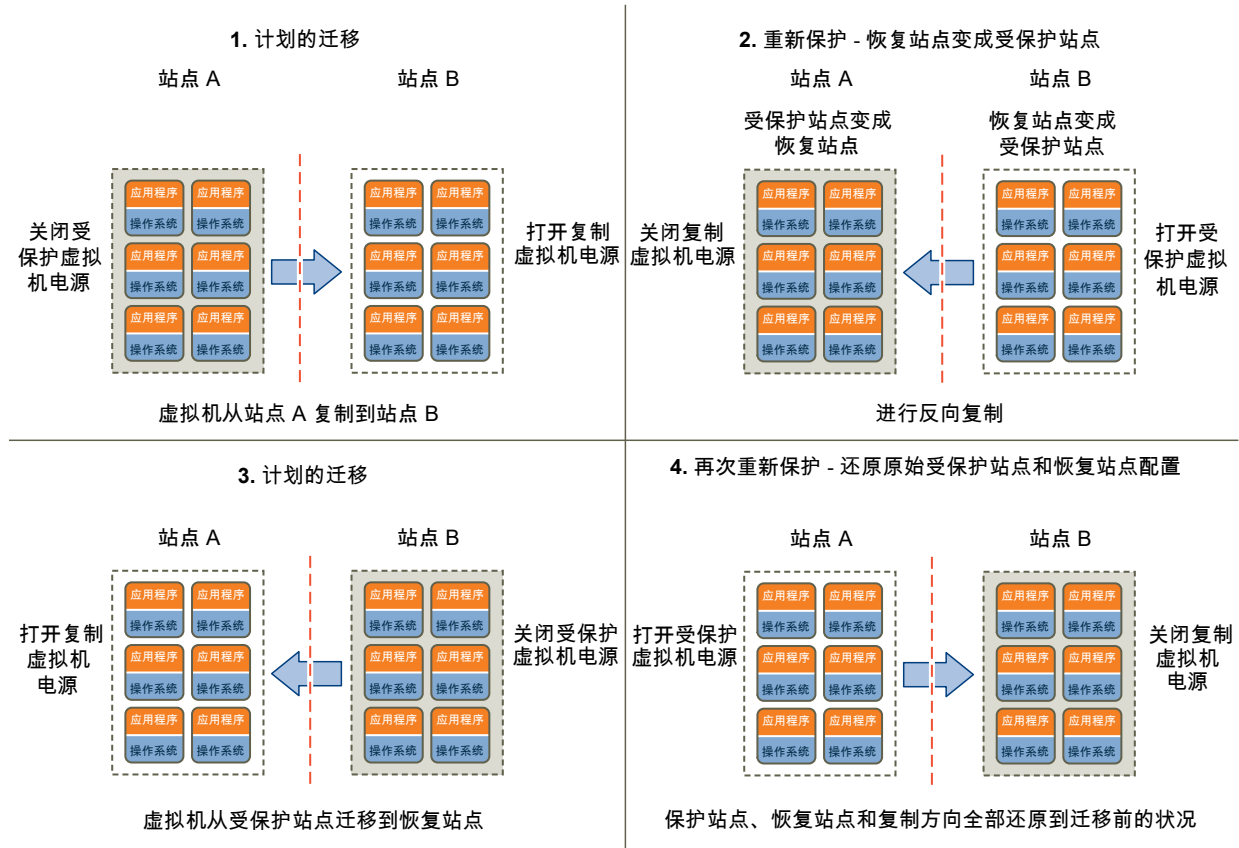
在事故发生后，当您将原始受保护站点恢复为在线状态后，当您准备好将服务还原到原始受保护站点时，请配置并运行故障恢复。

## 示例： 执行故障恢复操作

站点 A 是受保护站点，站点 B 是恢复站点。执行恢复后，会将虚拟机从站点 A 迁移到站点 B。要将站点 A 还原为受保护站点，可执行故障恢复。

- 1 虚拟机将执行从站点 A 到站点 B 的复制。
- 2 执行重新保护。站点 B（之前的恢复站点）将成为受保护站点。Site Recovery Manager 使用保护信息来建立对站点 B 的保护。站点 A 则成为恢复站点。
- 3 执行已计划的迁移，以便将站点 B 上受保护的虚拟机恢复到站点 A。
- 4 再次执行重新保护。站点 A 将成为受保护站点，站点 B 将成为恢复站点。

图 8-1. Site Recovery Manager 故障恢复过程



本章讨论了以下主题：

## ■ 执行故障恢复

# 执行故障恢复

Site Recovery Manager 执行恢复后，可执行故障恢复以还原受保护站点和恢复站点的原始配置。

为帮助理解，恢复之前的原始受保护站点为站点 A。原始恢复站点为站点 B。从站点 A 到站点 B 执行恢复后，已恢复虚拟机将在站点 B 上运行但不受任何保护。

## 前提条件

请确认满足以下条件。

- 您已执行恢复，且该恢复属于计划迁移或灾难恢复的一部分。
- 原始受保护站点（站点 A）正在运行。
- 如果已执行灾难恢复，则当原始受保护站点（站点 A）中的主机和数据存储再次运行时必须执行计划的迁移恢复。
- 自恢复后尚未运行重新保护。

## 步骤

1 在 vSphere Web Client 中，选择**站点恢复 > 恢复计划**。

2 右键单击恢复计划，然后选择**重新保护**。

3 选中用于确认您了解重新保护操作不可逆的复选框，然后单击**下一步**。

4 确定是否启用**强制清理**并单击**下一步**。

仅当您运行过一次重新保护并出现错误时，此选项才可用。启用该选项将强制移除虚拟机、忽略错误，并使恢复计划返回到就绪状态。

5 查看重新保护信息，然后单击**完成**。

6 在**监控**选项卡中，单击**恢复步骤**以监控重新保护操作，直至操作完成。

7 （可选）如果需要，请重新运行重新保护直到该操作顺利完成。

在重新保护操作结束时，Site Recovery Manager 会执行反向复制，使原始恢复站点（站点 B）变为现在的受保护站点。

8 （可选）测试完成后，右键单击恢复计划，然后选择**清理**以清理恢复计划。

9 右键单击恢复计划并选择**恢复**以在计划的迁移中运行恢复计划。

10 在**监控**选项卡中，单击**恢复步骤**以监控计划的迁移，直至迁移完成。

计划的迁移会关闭新的受保护站点（站点 B）中的虚拟机，并启动新的恢复站点（站点 A）中的虚拟机。如果需要，请重新运行计划的迁移直到该操作顺利完成。

当计划的迁移完成时，虚拟机将在原始受保护站点（站点 A）上运行但不受任何保护。原始恢复站点（站点 B）中的虚拟机将关闭电源。

11 右键单击恢复计划并选择**重新保护**，然后按照向导说明再次执行重新保护操作。

再次运行重新保护将按恢复之前的原始方向重新建立保护。

## 结果

您已成功将受保护站点和恢复站点还原为其在恢复之前的原始配置。此时受保护站点为站点 A，恢复站点为站点 B。

# Site Recovery Manager 与其他软件的互操作性

## 9

Site Recovery Manager Server 作为站点上 vCenter Server 的扩展运行。Site Recovery Manager 与其他 VMware 解决方案和第三方软件兼容。

可以在采用 Site Recovery Manager 进行保护的部署方案下运行其他 VMware 解决方案，例如 vCenter Update Manager、vCenter Server Heartbeat、VMware Fault Tolerance、vSphere Storage vMotion、vSphere Storage DRS 和 vCenter CapacityIQ。在将其他 VMware 解决方案连接到 Site Recovery Manager Server 所连接的 vCenter Server 实例之前，请仔细考虑。将其他 VMware 解决方案连接到与 Site Recovery Manager 相同的 vCenter Server 实例，可能会在升级 Site Recovery Manager 或 vSphere 时出现问题。请参见《VMware 产品互操作性列表》，检查这些解决方案的版本与您的 Site Recovery Manager 版本的兼容性和互操作性。

本章讨论了以下主题：

- Site Recovery Manager 和 vCenter Server
- Site Recovery Manager 如何在恢复期间与 DPM 和 DRS 交互
- Site Recovery Manager 如何与 Storage DRS 或 Storage vMotion 交互
- Site Recovery Manager 与 vSphere High Availability 进行交互的方式
- Site Recovery Manager 和 vSphere PowerCLI
- Site Recovery Manager 和 vCenter Orchestrator
- 保护 Microsoft 群集服务器和容错虚拟机
- 保护和恢复虚拟机的限制

## Site Recovery Manager 和 vCenter Server

Site Recovery Manager 利用存储管理、身份验证、授权和客户机自定义等 vCenter Server 服务。Site Recovery Manager 还使用一组标准的 vSphere 管理工具来管理这些服务。

由于 Site Recovery Manager Server 依靠 vCenter Server 提供某些服务，因此必须先站点上安装并配置 vCenter Server，然后才能安装 Site Recovery Manager。

可以将 Site Recovery Manager 和 vSphere Replication 与 vCenter Server Appliance 或标准 vCenter Server 安装结合使用。可以在一个站点上安装 vCenter Server Appliance，在另一个站点上进行标准 vCenter Server 安装。



## 对 vCenter Server 清单的更改如何影响 Site Recovery Manager

由于 Site Recovery Manager 保护组适用于一部分 vCenter Server 清单，因此，由 vCenter Server 管理员和用户对受保护清单所做的更改会影响 Site Recovery Manager 保护和恢复的完整性。Site Recovery Manager 依赖于受保护站点和恢复站点上 vCenter Server 清单中的特定对象（如虚拟机、文件夹、资源池和网络）的可用性。删除由恢复计划所引用的资源（如文件夹或网络）会使计划失效。在 vCenter Server 清单中重命名或重新定位对象不会影响 Site Recovery Manager，但如果操作导致在测试或恢复期间无法访问资源则除外。

Site Recovery Manager 允许在受保护站点中无中断地进行某些特定更改。

- 删除受保护的虚拟机。
- 删除存在清单映射的对象。

Site Recovery Manager 允许在恢复站点中无中断地进行某些特定更改。

- 将占位虚拟机移至其他文件夹或资源池。
- 删除存在清单映射的对象。

## Site Recovery Manager 和 vCenter Server 数据库

如果要更新由 Site Recovery Manager 扩展的 vCenter Server 安装，则在更新期间不要重新初始化 vCenter Server 数据库。Site Recovery Manager 将有关所有 vCenter Server 对象的标识信息存储在 Site Recovery Manager 数据库中。如果重新初始化 vCenter Server 数据库，则 Site Recovery Manager 已存储的标识数据将无法再与新的 vCenter Server 实例中的标识信息匹配，因此将找不到对象。

## Site Recovery Manager 如何在恢复期间与 DPM 和 DRS 交互

Distributed Power Management (DPM) 和 Distributed Resource Scheduler (DRS) 不是必需的，但 Site Recovery Manager 可以支持这两个服务，并且如果启用它们，则在使用 Site Recovery Manager 时会获得一定的优势。

DPM 是一项 VMware 功能，用于管理 ESX 主机的电源消耗情况。DRS 是一项 VMware 功能，用于管理 ESX 主机的虚拟机分配情况。

Site Recovery Manager 会临时禁用恢复站点上群集的 DPM，并确保当恢复或测试恢复开始时，群集中的所有主机均打开电源。这将在恢复虚拟机时留出足够的主机容量。恢复或测试结束后，Site Recovery Manager 将恢复站点上群集的 DPM 设置还原为其原始值。

对于计划的迁移和重新保护操作，Site Recovery Manager 同样会禁用受保护站点上受影响群集的 DPM，并确保群集中的所有主机均打开电源。这将使 Site Recovery Manager 可以完成主机级别的操作，例如卸载数据存储或在重新保护操作后清理存储。计划的迁移或重新保护操作结束后，Site Recovery Manager 将受保护站点上群集的 DPM 设置还原为其原始值。

群集中的主机将保持运行状态，以便 DPM 可以根据需要关闭这些主机的电源。Site Recovery Manager 将在可用 ESX 主机上按循环次序注册虚拟机，以便尝试尽可能平均地分布潜在的负载。Site Recovery Manager 会在打开恢复站点上的已恢复虚拟机的电源之前始终使用 DRS 放置以智能方式平衡多台主机间的负载，即使群集中已禁用 DRS 亦是如此。

如果已启用 DRS，并且 DRS 处于全自动模式，则 DRS 可能会移动其他虚拟机，以便在 Site Recovery Manager 打开已恢复虚拟机的电源期间进一步平衡群集中的负载。在 Site Recovery Manager 打开已恢复虚拟机的电源后，DRS 将继续平衡群集中所有虚拟机的负载。

## Site Recovery Manager 如何与 Storage DRS 或 Storage vMotion 交互

如果遵循特定准则，则在保护为 Storage DRS 或 Storage vMotion 配置的站点上的虚拟机时可以使用 Site Recovery Manager。

Storage DRS 或 Storage vMotion 的行为取决于是将 Site Recovery Manager 与基于阵列的复制还是与 vSphere Replication 结合使用。

### 在使用 Storage DRS 或 Storage vMotion 的站点上将 Site Recovery Manager 用于基于阵列的复制

如果您使用基于阵列的复制保护使用 Storage DRS 或 Storage vMotion 的站点上的虚拟机，则必须遵循以下准则。

- 如果您的存储阵列支持一致性组，Site Recovery Manager 将与 vSphere Storage DRS 和 vSphere Storage vMotion 兼容。您可以使用 Storage DRS 和 Storage vMotion 在 Site Recovery Manager 所保护的一致性组内移动虚拟机。如果存储阵列不支持一致性组，则无法将 Storage DRS 和 Storage vMotion 与 Site Recovery Manager 结合使用。
- 如果您在保护站点上启用了 Storage DRS，则数据存储群集中必须包含一个一致性组，且只能包含一个。请勿在群集中包含不属于该一致性组的任何数据存储。将多个一致性组置于同一个群集中可能会导致虚拟机在恢复过程中丢失。如果在恢复站点上启用了 Storage DRS，则还会在该恢复站点上应用此准则。
- 不使用 Storage DRS 或 Storage vMotion 定期移动虚拟机。请勿接受定期手动移动虚拟机的建议。可以偶尔移动虚拟机，但移动虚拟机次数过多可能会导致出现问题。移动虚拟机需要阵列通过网络复制虚拟机，此操作既需要时间又占用带宽。Storage DRS 或 Storage vMotion 移动虚拟机时，您可能在恢复过程中遇到以下问题：
  - 如果 Storage DRS 或 Storage vMotion 将虚拟机移至同一个保护组内的不同一致性组，则在将虚拟机的新位置传播到恢复站点的 Site Recovery Manager 与将更改复制到恢复站点的阵列之间存在一个很短的时间段。此外，阵列将源和目标一致性组复制到恢复站点上的一致性状态也需要一段时间。阵列将所有更改传播到恢复站点过程中，对此虚拟机执行灾难恢复可能会失败。
  - 如果 Storage DRS 或 Storage vMotion 将虚拟机移至不同的保护组，Site Recovery Manager 将生成针对此虚拟机的保护错误。您必须在旧保护组中取消配置虚拟机的保护，然后在新保护组中配置虚拟机的保护。在新保护组中配置保护之前，此虚拟机计划的迁移或灾难恢复会失败。

- 将磁盘添加到受保护的虚拟机导致出现的问题与移动整个虚拟机出现的问题相同。Site Recovery Manager 不会阻止您执行此操作，但如果虚拟机包含未复制的磁盘，并且未使磁盘脱离保护，则在移动之后，打开虚拟机电源将失败。
- 将受保护的磁盘移至其他一致性组导致出现的问题与移动整个虚拟机出现的问题相同。如果您将磁盘移至同一保护组中的其他一致性组，或者将其移至其他保护组，则会出现这些问题。Site Recovery Manager 并不会阻止您执行此操作，但如果磁盘已移至不同的一致性组，则在移动后打开虚拟机电源将失败。

## 在使用 Storage DRS 或 Storage vMotion 的站点上将 Site Recovery Manager 与 vSphere Replication 结合使用

如果您使用 vSphere Replication 保护使用 Storage DRS 或 Storage vMotion 的站点上的虚拟机，则必须遵循以下准则。

- vSphere Replication 在受保护站点上与 vSphere Storage vMotion 和 vSphere Storage DRS 兼容。可以使用 Storage vMotion 和 Storage DRS 移动受 vSphere Replication 保护的虚拟机的磁盘文件，而不会对复制产生任何影响。
- vSphere Replication 与 Storage vMotion 兼容，在磁盘或虚拟机的主目录移动时保存磁盘或虚拟机的状态。磁盘或虚拟机的复制在移动后继续正常执行。
- 仅当您将 Storage DRS 规则设置得非常激进，或者大量虚拟机在同一时间执行完全同步，完全同步才会导致 Storage DRS 触发 Storage vMotion。Storage DRS 的默认 I/O 滞后时间阈值为 15 毫秒。默认情况下，Storage DRS 每隔 8 小时执行一次负载平衡操作。Storage DRS 还会等收集到足够的与 I/O 负载有关的统计数据后再生成 Storage vMotion 建议。因此，如果完全同步持续的时间非常长，并且如果在该时间段内，完全同步生成的额外 I/O 导致滞后时间超过 I/O 滞后时间阈值，完全同步将仅影响 Storage DRS 建议。

## Site Recovery Manager 与 vSphere High Availability 进行交互的方式

您可以使用 Site Recovery Manager 来保护已启用 vSphere High Availability (HA) 的虚拟机。

HA 可以在同一站点内的新主机上重新启动发生故障的主机中的虚拟机，以此保护虚拟机免受 ESXi 主机故障的影响。Site Recovery Manager 通过在恢复站点重新启动虚拟机来保护虚拟机免受全站点故障的影响。HA 和 Site Recovery Manager 的主要区别在于 HA 在各虚拟机上运行，并自动重新启动虚拟机。Site Recovery Manager 在恢复计划级别运行并需要用户手动启动恢复。

要将虚拟机的 HA 设置传输到恢复站点，则必须在配置虚拟机保护后与执行恢复之前的这段时间内在占位虚拟机上设置 HA 设置。

您可以通过使用基于阵列的复制或 vSphere Replication 来复制 HA 虚拟机。如果 HA 在受保护站点的另一台主机上重新启动受保护的虚拟机，vSphere Replication 将在虚拟机重新启动后执行完全同步。

Site Recovery Manager 不需要 HA 作为保护虚拟机的必备条件。同样，HA 也不需要 Site Recovery Manager。

## Site Recovery Manager 和 vSphere PowerCLI

VMware vSphere PowerCLI 提供了 Windows PowerShell 接口以用于通过命令行访问 Site Recovery Manager 任务。

vSphere PowerCLI 公开了 Site Recovery Manager API。您可以使用 vSphere PowerCLI 管理 Site Recovery Manager 或创建脚本以实现 Site Recovery Manager 任务自动化。

有关如何使用 vSphere PowerCLI 管理 Site Recovery Manager 的信息，请参见 vSphere PowerCLI 文档，网址为 <https://www.vmware.com/support/developer/PowerCLI/>。

## Site Recovery Manager 和 vCenter Orchestrator

适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件允许您自动化某些 Site Recovery Manager 操作，方式为将这些操作包含在 vCenter Orchestrator 工作流中。

适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件包含运行 Site Recovery Manager 操作的操作和工作流。如果您是 vCenter Orchestrator 管理员，则可以创建包含来自 Site Recovery Manager 插件的操作和工作流的工作流。通过将 Site Recovery Manager 操作和工作流包含在 vCenter Orchestrator 工作流中，可以将 Site Recovery Manager 操作与其他 vCenter Orchestrator 插件提供的自动化操作合并。

例如，可以为 vCenter Server 创建使用 vCenter Orchestrator 插件的操作和工作流的工作流，以创建和配置虚拟机，并向 vCenter Server 注册这些虚拟机。在同一工作流中，可以使用来自 Site Recovery Manager 插件的操作和工作流来创建保护组，并在虚拟机一创建便立即对其进行保护。还可以使用 Site Recovery Manager 操作和工作流来配置受保护虚拟机的某些恢复设置。将 vCenter Server 和 Site Recovery Manager 操作和工作流合并在一个 vCenter Orchestrator 工作流中，以便允许您自动化创建和保护虚拟机的过程。

可以在共享恢复站点配置中使用适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件，在该配置中将多个 Site Recovery Manager 实例连接到了单个 vCenter Server 实例。还可以在已连接到同一 vCenter Single Sign-On 服务器的多个 vCenter Server 实例上将适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件与多个 Site Recovery Manager 实例配合使用。

有关使用 vCenter Orchestrator 创建工作流的信息，请参见 [vCenter Orchestrator 文档](#)。

有关如何使用适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件的信息，请参见 [vCenter Orchestrator 插件文档](#)。

### 适用于 Site Recovery Manager 的 vCenter Orchestrator 插件提供的自动化操作

通过适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件，您可以实现 Site Recovery Manager 基础架构创建过程的自动化，以向保护组中添加虚拟机以及配置虚拟机的恢复设置。

通过适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件，您可以通过将虚拟机添加到基于阵列的复制或 vSphere Replication 保护组来保护虚拟机的安全。该插件不会将在虚拟机上配置 vSphere Replication 的过程自动化。您必须手动在虚拟机上配置 vSphere Replication。

由于运行恢复会对受保护站点和恢复站点产生明显影响，因此，您不能使用适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件自动执行测试恢复、计划迁移或灾难恢复。恢复非常敏感，无法实现自动化，始终需要人工干预。

适用于 vCenter Site Recovery Manager 的 vCenter Orchestrator 插件包括 vCenter Orchestrator 操作、工作流、用于在某些事件发生时触发操作的策略模板以及用于对工作流显示 Site Recovery Manager API 的选定元素的脚本对象。

- 该插件提供创建 Site Recovery Manager 基础架构时执行的操作和工作流：
  - 创建基于阵列的保护组和 vSphere Replication 保护组
  - 在匹配对象之间创建清单映射
  - 将保护组添加到现有恢复计划
- 该插件提供保护虚拟机时执行的操作和工作流：
  - 使用现有基于阵列的保护组保护虚拟机
  - 使用现有 vSphere Replication 保护组保护虚拟机
- 该插件提供在虚拟机上配置恢复设置时执行的操作和工作流：
  - 设置恢复优先级
  - 创建每虚拟机恢复步骤
  - 设置已恢复虚拟机的最终电源状态
- 该插件提供从 Site Recovery Manager Server 获取信息时执行的操作和工作流：
  - 列出受保护的数据存储
  - 列出保护组和恢复计划
  - 按数据存储查找基于阵列的保护组
  - 获取未分配的复制数据存储和恢复计划状态

## 保护 Microsoft 群集服务器和容错虚拟机

可以使用 Site Recovery Manager 在一定限制内保护 Microsoft 群集服务器 (MSCS) 和容错虚拟机。

要使用 Site Recovery Manager 保护 MSCS 和容错虚拟机，您可能需要更改环境。

### 保护 MSCS 和容错虚拟机的一般限制

保护 MSCS 和容错虚拟机应遵循以下限制。

- 只能使用基于阵列的复制保护 MSCS 虚拟机。不支持使用 vSphere Replication 保护 MSCS 虚拟机。
- 重新保护 MSCS 或容错虚拟机需要 VMware High Availability (HA) 和 VMware Distributed Resource Scheduler (DRS)。如果要在重新保护期间在主要和辅助站点之间移动 MSCS 或容错虚拟机，则必须启用 HA 和 DRS，并根据需要设置关联性和反关联性规则。请参见 [MSCS 虚拟机保护的 DRS 要求](#)。

- vSphere 不支持 MSCS 虚拟机的 vSphere vMotion。

## MSCS 虚拟机保护的 ESXi 主机要求

要保护 MSCS 或容错虚拟机，运行虚拟机的 ESXi 主机必须满足某些条件。

- 必须在两台单独的 ESXi Server 实例上运行容错虚拟机及其卷影。
- 可以在下列可能的配置中运行由 MSCS 虚拟机组成的群集。

### 机箱内群集

群集中的 MSCS 虚拟机在一台 ESXi Server 上运行。在一个 ESXi Server 上，您最多可拥有五个 MSCS 节点。

### 跨机箱的群集

最多可将 MSCS 群集分散在五个 ESXi Server 实例中。您只能保护一个 ESXi Server 实例上任意 MSCS 群集的一个虚拟机节点。可以在 ESXi 主机上运行多个 MSCS 节点虚拟机，前提是这些虚拟机不在同一个 MSCS 群集中。此配置需要使用光纤通道 SAN 上的共享存储器作为仲裁磁盘。

## MSCS 虚拟机保护的 DRS 要求

要在包含 MSCS 虚拟机的站点上使用 DRS，必须配置 DRS 规则，以允许 Site Recovery Manager 保护虚拟机。如果占位虚拟机位于跨机箱的群集 MSCS 部署中或机箱内群集 MSCS 部署中，则遵循该准则可保护运行 DRS 的站点上的 MSCS 虚拟机。

- 由于 vSphere 不支持将 vSphere vMotion 用于 MSCS 虚拟机，则必须设置 VM to Host DRS 规则，以便 DRS 不对 MSCS 节点执行 vMotion。为受保护站点上的虚拟机和恢复站点上的卷影虚拟机设置 VM to Host 规则。
- 请先设置受保护站点上虚拟机的 DRS 规则，再配置客户机操作系统中的 MSCS。在部署、配置或打开虚拟机电源之后立即设置 DRS 规则。
- 创建 MSCS 节点的保护组之后，一旦占位虚拟机显示在恢复站点上，则立即在恢复站点的虚拟机上设置 DRS 规则。
- 恢复之后，在受保护站点上设置的 DRS 规则不会传输到恢复站点。因此，必须在恢复站点的占位虚拟机上设置 DRS 规则。
- 在恢复站点上设置 DRS 规则之前请勿运行测试恢复或实际恢复。

如果在受保护站点或恢复站点上不遵循准则，则 vSphere vMotion 可能会将 MSCS 虚拟机移至 Site Recovery Manager 不支持的配置。

- 在受保护站点或恢复站点上的机箱内群集部署中，vSphere vMotion 可能会将 MSCS 虚拟机移至不同的 ESXi 主机。
- 在受保护站点或恢复站点上的机箱内群集部署中，vSphere vMotion 可能会将某些或全部 MSCS 虚拟机移至单个 ESXi 主机。

## 保护和恢复虚拟机的限制

使用 Site Recovery Manager 保护和恢复虚拟机受到限制。

### 保护和恢复已挂起的虚拟机

当挂起虚拟机时，vSphere 会创建并保存其内存状态。该虚拟机恢复运行后，vSphere 将还原已保存的内存状态，以使虚拟机能够继续运行，而不会对其所运行的应用程序和客户机操作系统造成任何干扰。

### 保护和恢复包含快照的虚拟机

基于阵列的复制支持保护和恢复包含快照的虚拟机，但具有一些限制。

您可以通过设置 VMX 文件中的 `workingDir` 参数来指定用于存储快照增量文件的自定义位置。Site Recovery Manager 不支持使用 `workingDir` 参数。

如果您运行的 ESX 或 ESXi Server 版本早于版本 4.1，则也具有一些限制。

- 如果虚拟机具有多个 VMDK 磁盘文件，则所有磁盘文件都必须与 VMX 文件本身位于相同的文件夹中。
- 如果虚拟机已附加到裸磁盘映射 (RDM) 磁盘设备，则必须将该映射文件存储在与 VMX 文件本身相同的文件夹中。只有当您采用虚拟兼容性模式创建 RDM 映射时，RDM 快照才可用。

如果您正在运行的 ESX 或 ESXi Server 版本为 4.1 或更高，则这些限制不适用。

vSphere Replication 支持保护包含快照虚拟机，但您只能恢复最新的快照。vSphere Replication 会清除已恢复虚拟机中的快照信息。因此，恢复后快照将不再可用，除非您将 vSphere Replication 配置为保留多个时间点快照。有关结合使用多个时间点快照和 vSphere Replication 恢复旧快照的信息，请参见[复制虚拟机并启用多个时间点实例](#)。

### 使用内存状况快照保护和恢复虚拟机

使用内存状况快照保护虚拟机时，位于保护和恢复站点上的 ESXi 主机必须具有兼容的 CPU，如 VMware 知识库文章《[Intel 处理器的 vMotion CPU 兼容性要求](#)》和《[AMD 处理器的 vMotion CPU 兼容性要求](#)》中所定义。主机也必须启用相同的 BIOS 功能。如果服务器的 BIOS 配置不匹配，则即使其他配置均相同，服务器仍会出现兼容性错误消息。要检查的两个最常见的功能为 Non-Execute Memory Protection (NX/XD) 和 Virtualization Technology (VT/AMD-V)。

### 保护和恢复链接克隆虚拟机

vSphere Replication 不支持保护和恢复以链接克隆的形式存在的虚拟机。

如果快照树中的所有节点都已复制，则基于阵列的复制可支持保护和恢复以链接克隆的形式存在的虚拟机。

### 使用预留、关联性规则或限制保护和恢复虚拟机

当 Site Recovery Manager 将虚拟机恢复到恢复站点时，不会保留虚拟机上的任何预留、关联性规则或限制。由于恢复站点对受保护站点可能具有不同的资源要求，所以 Site Recovery Manager 不会保留恢复站点上的预留、关联性规则和限制。

您可以在恢复站点的资源池中配置预留和限制并相应地设置资源池映射，从而为已恢复的虚拟机设置预留、关联性规则和限制。或者，您也可以在恢复站点的占位虚拟机上手动设置预留、关联性规则或限制。

## 保护和恢复附加到 RDM 磁盘设备的虚拟机

根据您使用的是基于阵列的复制还是 vSphere Replication，保护和恢复附加到裸磁盘映射 (RDM) 磁盘设备的虚拟机将受到不同的支持。

- 基于阵列的复制支持物理兼容模式和虚拟兼容模式下的 RDM 设备。如果您结合使用 Site Recovery Manager 和基于阵列的复制，则可以保护和恢复使用物理兼容模式或虚拟兼容模式下的 RDM 的虚拟机。
- 对于源设备和目标设备，vSphere Replication 仅支持虚拟模式下的 RDM 设备。如果您使用 vSphere Replication，则无法保护和恢复使用物理兼容模式的 RDM 的虚拟机。
- 如果您同时使用基于阵列的复制和 vSphere Replication，则只能通过使用基于阵列的复制来保护和恢复使用物理兼容模式的 RDM 的虚拟机。您可以通过使用基于阵列的复制或者 vSphere Replication 保护和恢复使用虚拟兼容模式的 RDM 的虚拟机。

## 在使用 SIOC 的数据存储上执行虚拟机的计划迁移

在先前版本的 Site Recovery Manager 中，在运行计划的迁移之前，必须在恢复计划中包含的数据存储上禁用 Storage I/O Control (SIOC)。此版本的 Site Recovery Manager 完全支持 SIOC，因此，在运行计划的迁移之前不必禁用 SIOC。

## 使用 SIOC 的数据存储上的虚拟机的灾难恢复和重新保护

在先前版本的 Site Recovery Manager 中，如果在启用 SIOC 的情况下运行灾难恢复，此恢复将成功但会出现错误。恢复完成后，必须在受保护站点上手动禁用 SIOC 并再次运行计划的迁移恢复。在成功运行计划的迁移之前，无法运行重新保护。此版本的 Site Recovery Manager 完全支持 SIOC，因此，在不禁用 SIOC 的情况下恢复将成功并且不会出现错误，而且灾难恢复之后您可以运行计划的迁移和重新保护。

## 使用多个阵列中的组件保护和恢复虚拟机

Site Recovery Manager 中基于阵列的复制取决于阵列对的概念。Site Recovery Manager 会将其恢复的多个数据存储组定义为多个单元。因此，有关如何使用基于阵列的复制来存储受保护虚拟机的组件存在某些限制。

- Site Recovery Manager 不支持存储位于受保护站点的多个阵列中但要被复制到恢复站点的单个阵列中的虚拟机组件。
- 如果虚拟机组件跨两个阵列，则 Site Recovery Manager 不支持存储位于受保护站点的多个阵列中但要被复制到恢复站点的多个阵列中的虚拟机组件。

如果将虚拟机组件从多个阵列复制到恢复站点上的单个阵列或跨多个阵列，则受保护站点上数据存储的 UUID 的 VMX 配置会与恢复站点上的配置不匹配。



虚拟机 VMX 文件的位置决定了虚拟机所属的阵列对。一台虚拟机不能同时属于两个阵列对，所以如果某台虚拟机具有多个磁盘，并且如果这些磁盘中的一个磁盘位于此虚拟机所属的阵列对以外的阵列中，则 Site Recovery Manager 无法保护整个虚拟机。Site Recovery Manager 会将与虚拟机位于不同阵列对中的磁盘作为未复制的设备处理。

因此，所有虚拟磁盘、交换文件、RDM 设备以及 LUN 上的虚拟机工作目录存储到同一个阵列中可使 Site Recovery Manager 保护所有的虚拟机组件。

## Active Directory 域控制器的保护和恢复

不要使用 Site Recovery Manager 保护 Active Directory 域控制器。Active Directory 提供自带的复制技术和还原模式。请使用 Active Directory 复制技术和还原模式技术处理灾难恢复情形。

## 将 Site Recovery Manager 用于接入控制群集

可以使用群集上的接入控制保留恢复站点上的资源。但是，使用接入控制会在运行恢复计划时阻止 Site Recovery Manager 打开虚拟机电源，从而影响灾难恢复。如果打开虚拟机电源会违反相关的接入控制限制，则接入控制会阻止打开虚拟机电源。

在恢复过程中可以向恢复计划添加命令步骤，以运行禁用接入控制的 PowerCLI 脚本。有关创建命令步骤的信息，请参见[创建自定义恢复步骤](#)。

- 1 在运行 PowerCLI 脚本的恢复计划中创建打开电源前命令步骤，以禁用接入控制。

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$false
```

- 2 在恢复计划中创建打开电源后命令步骤，以便在打开虚拟机电源之后重新启用接入控制。

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$true
```

如果在恢复过程中禁用接入控制，则在执行紧随测试恢复的清理之后必须手动重新启用接入控制。禁用接入控制可能会影响 High Availability 重新启动恢复站点上虚拟机的功能。请勿长时间禁用接入控制。

# 高级 Site Recovery Manager 配置

# 10

Site Recovery Manager 的默认配置会启用一些简单的恢复方案。高级用户可以将 Site Recovery Manager 自定义为支持范围更广的站点恢复要求。

本章讨论了以下主题：

- 重新配置 Site Recovery Manager 设置
- 修改设置以运行大型 Site Recovery Manager 环境
- 修改长时间运行任务的设置

## 重新配置 Site Recovery Manager 设置

使用**高级设置**，您可以查看或更改 Site Recovery Manager 服务的多个自定义设置。“高级设置”为具有足够特权的用户提供了一种方式，以更改影响多种 Site Recovery Manager 功能的操作的默认值。

---

**重要事项** 在升级过程中，Site Recovery Manager 不会保留您在上一安装中配置的任何高级设置。这是设计问题。由于默认值发生了更改或性能方面有所改进，新版本可能不需要或不兼容您在上一版本的 Site Recovery Manager 中设置的高级设置。同样，如果卸载并重新安装相同版本的 Site Recovery Manager，将重用上一安装中的数据库，但不会保留高级设置。

---

## 更改 Site Recovery Manager 历史记录报告收集设置

Site Recovery Manager 历史记录报告可帮助在故障前后对 Site Recovery Manager Server 的行为进行诊断。可以更改要导出的历史记录报告的数量。

如果将站点 A 作为受保护站点，将站点 B 作为恢复站点来运行故障切换、测试、清理和重新保护操作，则可以在收集站点 B（恢复站点）的支持包时导出这些操作的历史记录报告。最新历史记录直接从 Site Recovery Manager 数据库提取。

执行重新保护后，站点 A 是新的恢复站点，站点 B 是受保护站点。运行故障切换、测试、清理和重新保护操作时，可以在为站点 A（恢复站点）收集支持包时导出历史记录报告。

### 前提条件

- 验证是否有管理员凭据。
- Site Recovery Manager 必须连接到可以使用有效的数据库凭据进行访问的 Site Recovery Manager 数据库。

**步骤**

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 在**管理**选项卡上，单击**高级设置**。
- 3 选择**导出历史记录**，然后单击**编辑**。
- 4 根据需要更改 **exportHistory.numReports** 的值。  
可以输入的值范围为 0 到 50。默认值为 5。
- 5 要选择不导出报告，可将该值改为零 (0)。
- 6 单击**确定**保存更改。

## 更改本地站点设置

Site Recovery Manager 会监控 Site Recovery Manager Server 主机上的资源消耗，并在达到资源阈值时发出警报。您可更改 Site Recovery Manager 发出警报的阈值和方式。

**步骤**

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 在**管理**选项卡上，单击**高级设置**。
- 3 单击**本地站点状态**。
- 4 单击**编辑**以更改设置。

选项	操作
更改 Site Recovery Manager 检查本地站点 CPU 使用情况、磁盘空间和可用内存的时间间隔。默认值为 60 秒。	在 <b>localSiteStatus.checkInterval</b> 文本框中输入新值。
更改本地站点的名称。	在 <b>localSiteStatus.displayName</b> 文本框中输入新值。
更改 Site Recovery Manager 在前后两次发出有关本地站点上 CPU 使用情况、磁盘空间和可用内存的警报之间等待的超时值。默认值为 600 秒。	在 <b>localSiteStatus.eventFrequency</b> 文本框中输入新值。
更改导致 Site Recovery Manager 发出 CPU 使用量过高事件的 CPU 使用量百分比。默认值为 70。	在 <b>localSiteStatus.maxCpuUsage</b> 文本框中输入新值。
更改导致 Site Recovery Manager 发出磁盘空间过低事件的可用磁盘空间百分比。默认值为 100。	在 <b>localSiteStatus.minDiskSpace</b> 文本框中输入新值。
更改导致 Site Recovery Manager 发出内存过低事件的可用内存量。默认值为 32 MB。	在 <b>localSiteStatus.minMemory</b> 文本框中输入新值。

- 5 单击**确定**保存更改。

## 更改日志记录设置

您可以更改 Site Recovery Manager 提供给 Site Recovery Manager Server 组件的日志记录级别。

Site Recovery Manager Server 可执行日志轮换。重新启动 Site Recovery Manager Server 或日志文件变大时，Site Recovery Manager Server 会新建日志文件并将后续日志消息写入新的日志文件。Site Recovery Manager Server 新建日志文件时，该服务器会压缩旧的日志文件以节省空间。

您可以降低某些 Site Recovery Manager Server 组件的日志记录级别，因为日志文件变大的速度过快。也可以增加某些组件的日志记录级别以帮助诊断问题。所有 Site Recovery Manager Server 组件的可用日志记录级别列表均相同。

### 无

关闭日志记录。

### 安静

记录最小日志条目。

### 应急

仅记录应急日志条目。在出现完全失败时显示应急消息。

### 错误

记录应急和错误日志条目。在出现可能会或可能不会导致失败的问题时显示错误消息。

### 警告

记录应急、错误和警告日志条目。因出现可能属于预期操作过程一部分的不良行为而显示警告消息。

### 信息

记录应急、错误、警告和信息日志条目。信息消息提供有关正常操作的信息。

### 详细

记录应急、错误、警告、信息和详细日志条目。详细消息提供较信息消息更加详细的信息。

### 琐事

记录应急、错误、警告、信息、详细和琐事日志条目。琐事消息提供所有可用信息。该级别的日志记录对于调试非常有用，但产生的数据过多，可能会影响性能。

---

**注** 仅当 VMware 支持部门要求时才设置此日志记录级别以帮助解决问题。

---

### 步骤

- 1 在 vSphere Web Client 中，单击 **站点恢复 > 站点**，然后选择一个站点。
- 2 在 **管理** 选项卡上，单击 **高级设置**。
- 3 单击 **日志管理器**。

#### 4 单击**编辑**以修改日志记录设置。

默认情况下，除非日志记录级别的描述中另有申明，否则所有的组件都将记录详细级别日志。

选项	描述
设置在 <b>logManager</b> 中没有相应条目的所有组件的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.Default</b> 下拉菜单中选择一个日志记录级别。
设置外部 API 模块的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.ExternalAPI</b> 下拉菜单中选择一个日志记录级别。
设置 <b>vSphere Replication</b> 的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.HbrProvider</b> 下拉菜单中选择一个日志记录级别。
设置 <b>IP Customizer</b> 工具的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.IPCustomizer</b> 下拉菜单中选择一个日志记录级别。
设置清单映射的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.InventoryMapper</b> 下拉菜单中选择一个日志记录级别。
设置许可问题的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.Licensing</b> 下拉菜单中选择一个日志记录级别。
设置持久性问题的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.Persistence</b> 下拉菜单中选择一个日志记录级别。
设置恢复操作的日志记录级别。默认值为 <b>trivia</b> 。	从 <b>logManager.Recovery</b> 下拉菜单中选择一个日志记录级别。默认情况下，恢复日志记录设置为 <b>琐事</b> 。
设置恢复配置操作的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.RecoveryConfig</b> 下拉菜单中选择一个日志记录级别。
设置基于阵列的复制操作的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.Replication</b> 下拉菜单中选择一个日志记录级别。
设置 <b>Site Recovery Manager Server</b> 和 <b>vCenter Server</b> 之间授权问题的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.ServerAuthorization</b> 下拉菜单中选择一个日志记录级别。
设置会话管理的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.SessionManager</b> 下拉菜单中选择一个日志记录级别。
设置 <b>SOAP Web 服务适配器</b> 的日志记录级别。默认值为 <b>info</b> 。	从 <b>logManager.SoapAdapter</b> 下拉菜单中选择一个日志记录级别。由于 SOAP 适配器生成的流量级别，将日志记录级别设置为 <b>琐事</b> 可能会影响性能。默认情况下，SOAP 适配器日志记录设置为 <b>信息</b> 。
设置存储问题的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.Storage</b> 下拉菜单中选择一个日志记录级别。
设置基于阵列的存储提供程序提供的消息的日志记录级别。默认值为 <b>verbose</b> 。	从 <b>logManager.StorageProvider</b> 下拉菜单中选择一个日志记录级别。

#### 5 单击**确定**保存更改。

新的日志记录级别在单击**确定**后将立即应用。无需重新启动 **Site Recovery Manager** 服务。如果重新启动 **Site Recovery Manager Server**，日志记录仍保留设置为所选择的级别。

## 更改恢复设置

您可调整测试或运行恢复计划时发生超时的默认值。如果由于超时而未能完成任务，可调整默认值。

执行恢复计划步骤时，可能会发生几种类型的超时。这些超时会导致计划暂停指定的时间间隔，为完成步骤留出时间。

Site Recovery Manager 会在您在某一虚拟机上配置保护时将一些高级设置应用到此虚拟机：

- `recovery.defaultPriority`
- `recovery.powerOnTimeout`
- `recovery.powerOnDelay`
- `recovery.customizationTimeout`
- `recovery.skipGuestShutdown`
- `recovery.powerOffTimeout`

Site Recovery Manager 在每个 Site Recovery Manager 站点上保留一份虚拟机恢复设置的副本。如果保护站点和恢复站点上的恢复高级设置不同，则 Site Recovery Manager 将虚拟机的恢复设置初始化为每个站点上的不同值。届时，当 Site Recovery Manager 将虚拟机从 A 站点恢复到 B 站点时，将应用 B 站点的本地恢复设置。当从 B 站点恢复到 A 站点时，Site Recovery Manager 将应用 A 站点的本地恢复设置。这种情况将一直存在，除非从恢复计划的“虚拟机”选项卡明确地编辑和保存单台虚拟机的恢复设置。两个 Site Recovery Manager 站点上受影响虚拟机的恢复设置将同步并变为一致。

### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 在**管理**选项卡上，单击**高级设置**。
- 3 单击**恢复**。
- 4 单击**编辑**以修改恢复站点设置。

选项	操作
更改 IP 自定义超时。默认值为 600 秒。	在 <code>recovery.customizationTimeout</code> 文本框中输入一个新的值。
更改恢复虚拟机的默认优先级。默认值为 3。	在 <code>recovery.defaultPriority</code> 文本框中输入一个新的值。
启用或禁用强制恢复。默认值为 <code>false</code> 。	选中或取消选中 <code>recovery.forceRecovery</code> 复选框。如果缺少与受保护站点的连接会严重影响 RTO，请激活强制恢复。该设置仅消除了运行恢复计划时选择强制恢复的限制。要实际启用强制恢复，请在运行计划时选择它。
更改打开群集中主机电源的超时时间。默认值为 1200 秒。	在 <code>recovery.hostPowerOnTimeout</code> 文本框中输入一个新的值。
更改关闭客户机操作系统电源的超时时间。默认值为 300 秒。	在 <code>recovery.powerOffTimeout</code> 文本框中输入一个新的值。新的超时值将应用到受保护站点中虚拟机的关闭电源任务。
更改打开虚拟机电源后启动从属任务前的延迟时间。默认值为 0。	在 <code>recovery.powerOnDelay</code> 文本框中输入一个新的值。新值将应用到恢复站点中虚拟机的打开电源任务。

选项	操作
更改打开虚拟机电源时等待 VMware Tools 的超时时间。默认值为 300 秒。	在 <code>recovery.powerOnTimeout</code> 文本框中输入一个新的值。新的打开电源值将应用到恢复站点中虚拟机的打开电源任务。如果受保护的虚拟机未安装 VMware Tools，请将此值设置为 0。
启用或禁用跳过关闭客户机操作系统。默认值为 <code>false</code> 。	选中或取消选中 <code>recovery.skipGuestShutdown</code> 复选框。选择该选项时， <code>recovery.powerOffTimeout</code> 不起作用。如果虚拟机中未安装 VMware Tools，启用该选项以自动禁用 <code>recovery.powerOffTimeout</code> ，跳过客户机直接关闭虚拟机电源来关闭 SRM（没有关机超时）。
启用或禁用恢复期间自动执行虚拟机 IP 自定义。默认值为 <code>true</code> 。	选中或取消选中 <code>recovery.useIpMapperAutomatically</code> 复选框。如果选中该选项且为虚拟网络配置了 IP 映射规则，则 Site Recovery Manager 会在恢复期间评估这些规则以自定义虚拟机。如果取消选中该选项，恢复期间不会评估 IP 映射规则。在虚拟机恢复设置 IP 自定义模式下，您可以针对每个虚拟机覆盖该选项。

## 5 单击**确定**保存更改。

### 结果

如果在配置了虚拟机保护之后更改任何高级设置，则新的设置将不会应用到此虚拟机。对这些高级设置所做的修改只能应用到在更改设置之后才受保护的虚拟机。这是由设计决定的，因为如果 Site Recovery Manager 将更改后的高级设置应用到已配置了保护的虚拟机，则可能会导致这些虚拟机的保护出现不需要的更改。

### 后续步骤

要将对这些高级设置所做的更改应用到先前已受保护的虚拟机，必须单独重新配置这些虚拟机。例如，如果重新配置 `defaultPriority` 设置，可以手动重新配置先前已受保护的虚拟机的优先级，以匹配新的 `defaultPriority` 设置。

- 1 在 vSphere Web Client 中，单击**站点恢复 > 保护组**，然后选择虚拟机所属的保护组。
- 2 在**相关对象**选项卡上，单击**虚拟机**。
- 3 选择虚拟机并单击**移除保护**。  
虚拟机状态将更改为“未配置”。
- 4 单击**全部配置**以重新配置保护组中的所有虚拟机，或选择一台虚拟机并单击**配置保护**以仅重新配置该虚拟机。

Site Recovery Manager 将较新的高级设置应用于虚拟机。

## 更改远程站点设置

您可修改受保护站点中的 Site Recovery Manager Server 用于确定远程站点中的 Site Recovery Manager Server 是否可用的默认值。

Site Recovery Manager 会监控受保护站点与恢复站点之间的连接，并在连接断开时发出警报。您可更改导致 Site Recovery Manager 发出连接事件的条件，也可更改 Site Recovery Manager 发出警报的方式。



**步骤**

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 在**管理**选项卡上，单击**高级设置**。
- 3 单击**远程站点状态**。
- 4 单击**编辑**以修改设置。

选项	操作
更改发出站点故障事件之前 Ping 失败的次数。默认值为 5。	在 <code>remoteSiteStatus.panicDelay</code> 文本框中输入一个新的值。
更改声明检查失败前要尝试的远程站点状态检查 (Ping) 次数。默认值为 2。	在 <code>remoteSiteStatus.pingFailedDelay</code> 文本框中输入一个新的值。
更改 Site Recovery Manager 检查远程站点中的 Site Recovery Manager Server 是否可用的时间间隔。默认值为 300 秒。	在 <code>remoteSiteStatus.pingInterval</code> 文本框中输入一个新的值。如果您指定的 <code>remoteSiteStatus.pingInterval</code> 值小于为 <code>connections.drPingInterval</code> 配置的值，Site Recovery Manager 会重置配置的值。您可以编辑 <code>vmware-dr.xml</code> 文件中的 <code>connections.drPingInterval</code> 值。如果为 <code>remoteSiteStatus.pingInterval</code> 指定的值超出范围，则会显示以下错误消息： <code>remoteSiteStatus.pingInterval</code> 的设置超出允许的范围。

- 5 单击**确定**保存更改。

## 更改占位虚拟机创建超时时间

可以调整复制设置以修改 Site Recovery Manager 等待完成创建占位虚拟机的时间。

**步骤**

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 在**管理**选项卡上，单击**高级设置**。
- 3 单击**复制**。
- 4 单击**编辑**以更改 `replication.placeholderVmCreationTimeout` 设置，从而修改在创建占位虚拟机时要等待的秒数。  
默认值为 300。
- 5 单击**确定**保存更改。

## 更改存储器设置

可以调整存储设置以修改 Site Recovery Manager 和 vCenter Server 与存储复制适配器 (SRA) 通信的方式。

**步骤**

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 在**管理**选项卡上，单击**高级设置**。



- 3 单击 **[存储器]**。
- 4 单击 **编辑** 以修改存储设置。

选项	操作
更改执行 SRA 命令的超时时间（秒）。默认值为 300 秒。	在 <code>storage.commandTimeout</code> 文本框中输入一个新的值。
更改最大并发 SRA 操作数。默认值为 5。	在 <code>storage.maxConcurrentCommandCnt</code> 文本框中输入一个新的值。
更改前后两次数据存储组计算之间的最短时间量（秒）。默认值为 0。	在 <code>storage.minDsGroupComputationInterval</code> 文本框中输入一个新的值。
更改在持续数据同步操作中前后两次状态更新之间的时间间隔。默认值为 30 秒。	在 <code>storage.querySyncStatusPollingInterval</code> 文本框中输入一个新的值。
更改前后两次存储阵列发现检查之间的时间间隔。默认值为 86400 秒（24 小时）。	在 <code>storage.storagePingInterval</code> 文本框中输入一个新的值。
更改数据同步操作完成允许的最大时间量。默认值为 86400 秒（24 小时）。	在 <code>storage.syncTimeout</code> 文本框中输入一个新的值。

- 5 单击 **确定** 保存更改。

## 更改存储提供程序设置

对于基于阵列的复制，SAN 提供程序是 Site Recovery Manager 与存储复制适配器 (SRA) 之间的接口。某些 SRA 需要您更改默认 SAN 提供程序的值。您可以更改 Site Recovery Manager SAN 提供程序的默认超时值和其他行为。

可以更改设置以便对数据存储名称、主机重新扫描计数和超时（秒）进行重新签名和修复。有关这些值的详细信息，请参见阵列供应商提供的 SRA 文档。

### 步骤

- 1 在 vSphere Web Client 中，单击 **站点恢复 > 站点**，然后选择一个站点。
- 2 在 **管理** 选项卡上，单击 **高级设置**。
- 3 单击 **存储提供程序**。
- 4 单击 **编辑** 以修改存储提供程序设置。

选项	操作
使 Site Recovery Manager 尝试分离并重新连接具有重复卷的 LUN。默认值为 true。	选中 <code>storageProvider.autoDetachLUNsWithDuplicateVolume</code> 复选框。
测试和恢复期间在 ESXi 主机上设置 <code>LVM.EnableResignature</code> 标记。默认值为 0。	在 <code>storageProvider.autoResignatureMode</code> 文本框中，输入 0 禁用，输入 1 启用，输入 2 忽略该标记。默认设置为 0。如果您将此标记设置为 1，Site Recovery Manager 可对所有已知 VMFS 快照卷（包括 Site Recovery Manager 不管理的卷）进行重新签名。如果您保持将此标记设置为 0，Site Recovery Manager 只对其管理的 VMFS 快照卷进行重新签名。

选项	操作
更改等待批量附加 LUN 操作在每个 ESXi 主机上完成的超时（秒）。默认值为 3600 秒。	在 <code>storageProvider.batchAttachTimeoutSec</code> 文本框中输入值。
更改等待批量分离 LUN 操作在每个 ESXi 主机上完成的超时（秒）。默认值为 3600 秒。	在 <code>storageProvider.batchDetachTimeoutSec</code> 文本框中输入值。
更改 Site Recovery Manager 等待挂载 VMFS 卷的时间间隔。默认值为 3600 秒。	在 <code>storageProvider.batchMountTimeoutSec</code> 文本框中输入一个新的值。如果您遇到 Site Recovery Manager 检查需要很长时间才能挂载的 VMFS 卷导致的超时，请更改此值。此设置在 Site Recovery Manager 5.5.1 及更高版本中提供。
更改 Site Recovery Manager 等待卸载 VMFS 卷的时间间隔。默认值为 3600 秒。	在 <code>storageProvider.batchUnmountTimeoutSec</code> 文本框中输入一个新的值。如果您遇到 Site Recovery Manager 检查需要很长时间才能卸载的 VMFS 卷导致的超时，请更改此值。此设置在 Site Recovery Manager 5.5.1 及更高版本中提供。
成功完成恢复后，强制移除已恢复的数据存储名称上的 <code>snap-xx</code> 前缀。默认值为 <code>false</code> 。	选中 <code>storageProvider.fixRecoveredDatastoreNames</code> 复选框。
在测试和恢复期间延迟主机扫描。默认值为 0。	<p>SRA 可以在恢复站点上升级的存储设备对 ESXi 主机可用之前向 Site Recovery Manager 发送响应。Site Recovery Manager 接收来自 SRA 的响应时，将重新扫描存储设备。如果存储设备尚未完全可用，ESXi Server 将不检测这些设备，Site Recovery Manager 在执行重新扫描时将不查找已复制的设备。此时将不创建数据存储，并且找不到已恢复的虚拟机。</p> <p>要延迟启动存储重新扫描，直至它们在 ESXi 主机上可用，可在 <code>storageProvider.hostRescanDelaySec</code> 文本框中输入新的值。</p> <p>仅当遇到数据存储不可用问题时才能更改此值。</p>
在测试和恢复期间重复主机扫描。默认值为 1。	在 <code>storageProvider.hostRescanRepeatCnt</code> 文本框中输入一个新的值。某些存储阵列需要进行多次重新扫描，例如，发现已故障切换的 LUN 的快照。在先前的版本中，您可能已使用 <code>storageProvider.hostRescanRepeatCnt</code> 参数在恢复中引入延迟。请改为使用 <code>storageProvider.hostRescanDelaySec</code> 参数。
更改 Site Recovery Manager 等待每次 HBA 重新扫描完成的时间间隔。默认值为 300 秒。	在 <code>storageProvider.hostRescanTimeoutSec</code> 文本框中输入一个新的值。
设置 Site Recovery Manager 尝试对 VMFS 卷进行重新签名的次数。默认值为 1。	在 <code>storageProvider.resignatureFailureRetryCount</code> 文本框中输入一个新的值。
设置对 VMFS 卷进行重新签名的超时时间。默认值为 900 秒。	在 <code>storageProvider.resignatureTimeoutSec</code> 文本框中输入一个新的值。如果您更改 <code>storageProvider.hostRescanTimeoutSec</code> 设置，请将 <code>storageProvider.resignatureTimeoutSec</code> 设置增大到用于 <code>storageProvider.hostRescanTimeoutSec</code> 的相同超时。
确定 Site Recovery Manager 在执行完 Storage vMotion 后不应视为潜在候选 VMX 文件的 VMX 文件路径。默认值为 <code>.snapshot</code> ，	<p>某些阵列会创建 <code>storageProvider.storageVmotionVmxSearch</code> 搜索算法应忽略的 VMX 文件路径。在 <code>storageProvider.storageVmotionVmxFilePathsToSkip</code> 文本框中输入逗号分隔的字符串列表，以标识要在 Storage vMotion 之后忽略的 VMX 文件路径。Site Recovery Manager 在执行 Storage vMotion 后不会将包含一个或多个此类字符串的 VMX 文件路径视为潜在候选 VMX 文件。</p>

选项	操作
在已恢复的数据存储中搜索 VMX 文件，以确定在测试或恢复之前或期间已由 Storage vMotion 移动的虚拟机。默认值为 true。	默认情况下，该选项处于选中状态。取消选中 <code>storageProvider.storageVmotionVmxSearch</code> 复选框可禁用此选项。
为批量卸载数据存储操作设置超时（秒）。默认值为 3600 秒。	在 <code>storageProvider.batchUnmountTimeoutSec</code> 文本框中输入值。
设置批量卸载 VMFS/NFS 卷的重试次数。默认值为 3。	在 <code>storageProvider.datastoreUnmountRetryCnt</code> 文本框中输入新的值。
设置等待 Virtual Center 报告新发现的数据存储的超时（秒）。默认值为 30 秒。	在 <code>storageProvider.waitForRecoveredDatastoreTimeoutSec</code> 文本框中输入新的值。
设置等待新发现的数据存储变为可访问的超时（秒）。默认值为 60 秒。	在 <code>storageProvider.waitForAccessibleDatastoreTimeoutSec</code> 文本框中输入新的值。
设置 Site Recovery Manager 等待 VMFS 卷变为挂载的时间间隔（秒）。默认值为 30 秒。	在 <code>storageProvider.waitForVmfsVolumesMountedStateTimeoutSec</code> 文本框中输入新的值。

- 5 单击 **确定** 保存更改。

## 更改 vSphere Replication 设置

可以调整全局设置以更改 Site Recovery Manager 如何与 vSphere Replication 交互。

### 步骤

- 1 在 vSphere Web Client 中，单击 **站点恢复 > 站点**，然后选择一个站点。
- 2 在 **管理** 选项卡上，单击 **高级设置**。
- 3 单击 **vSphere Replication**。
- 4 单击 **编辑** 以修改 vSphere Replication 设置。

选项	描述
允许 Site Recovery Manager 恢复由其他解决方案管理的虚拟机。默认值为 false。	vSphere Replication 允许解决方案管理虚拟机的复制。默认情况下，Site Recovery Manager 只恢复其管理的虚拟机。要允许 Site Recovery Manager 恢复由其他解决方案管理复制的虚拟机，请选中 <b>allowOtherSolutionTagInRecovery</b> 复选框。
恢复期间保留多个较早的时间点 (PIT) 快照。默认值为 true。	如果将 vSphere Replication 配置为创建受保护虚拟机的 PIT 快照，则执行恢复时，Site Recovery Manager 仅恢复最新快照。要在恢复期间恢复较早的 PIT 快照，请选择 <b>preserveMpitImagesAsSnapshots</b> 复选框。
更改重新保护操作期间反向复制的超时期限。默认值为 3600。	在 <code>reverseReplicationTimeout</code> 文本框中输入一个新的值。重新保护操作期间，如果您在 vSphere Replication 反向复制时遇到超时错误，请更改此值。

选项	描述
更改 vSphere Replication 同步操作的超时期限。默认值为 7200。	在 <code>synchronizationTimeout</code> 文本框中输入一个新的值。输入的值必须是要设置的超时时间的一半。默认值为 7200，对应于工作同步超时期限 14400 秒。如果您在 vSphere Replication 同步恢复站点上的虚拟机时遇到超时错误，请更改此值。
更改复制的默认 RPO 设置。默认值为 240。	在 <code>vrReplication.timeDefault</code> 文本框中输入一个新的值。默认值为 240 分钟（4 小时）。配置复制时将选择此值，但您可以在为单个虚拟机或一组虚拟机配置复制时在配置复制向导中指定其他 RPO。

- 单击 **确定** 保存更改。

## 修改设置以运行大型 Site Recovery Manager 环境

如果使用 Site Recovery Manager 测试或恢复大量虚拟机，您可能需要修改默认 Site Recovery Manager 设置以实现环境中的最佳恢复时间或避免超时。

在大型环境中，Site Recovery Manager 可能会同时打开或关闭大量虚拟机的电源。同时打开或关闭大量虚拟机的电源会造成虚拟基础架构的负载过高，这可能会导致超时。您可以通过限制 Site Recovery Manager 并发执行打开或关闭电源操作的次数，或通过增加超时期限来修改某些 Site Recovery Manager 设置以避免超时。

对打开或关闭电源操作设置的限制取决于您的基础架构可以处理的打开或关闭电源并发操作的次数。

可以修改 vSphere Web Client 或 Site Recovery Manager 客户端插件中 **高级设置** 菜单的某些选项。要修改其他设置，可以编辑 Site Recovery Manager Server 上的 `vmware-dr.xml` 配置文件。当存在某个选项时，请始终通过客户端菜单修改设置。如果修改设置，必须在受保护站点和恢复站点的 Site Recovery Manager Server 和 vCenter Server 实例上进行同样的修改。

有关可以更改的设置的描述，请参见 [大型 Site Recovery Manager 环境的设置](#)。

### 步骤

- 在 vSphere Web Client 中选择一个群集。
- 在 **管理** 选项卡上，选择 **设置 > vSphere DRS**。
- 单击 **[编辑]**。
- 在 **高级选项** 中，设置 `srmMaxBootShutdownOps` 设置。

选项	描述
选项文本框	输入 <code>srmMaxBootShutdownOps</code> 。
值文本框	输入引导和关机操作的最大次数，例如 32。如果将值设置为 32，则一旦第一批 32 个中的一个完成，下一个客户机将立即启动引导或关闭，即虚拟机 1 到 32 同时启动，然后虚拟机 33 在第一批某个完成后立即启动，虚拟机 34 在第一批的第二个完成后启动，以此类推。

- 单击 **确定** 保存更改。
- 登录 Site Recovery Manager Server 主机。

- 7 在文本编辑器中打开 vmware-dr.xml 文件。

您将在 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config 文件夹中找到 vmware-dr.xml 文件。

- 8 在 vmware-dr.xml 文件中更改 defaultMaxBootAndShutdownOpsPerCluster 和 defaultMaxBootAndShutdownOpsPerHost 设置：

```
<config>
...
  <defaultMaxBootAndShutdownOpsPerCluster>24</defaultMaxBootAndShutdownOpsPerCluster>
  <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
...
</config>
```

如果 vmware-dr.xml 文件中尚不存在这些元素，则可以将其添加到 <config> 部分的任意位置。如果将 <defaultMaxBootAndShutdownOpsPerCluster> 值设置为 **24**，则一旦第一批 24 个中的一个完成，下一个客户机将立即启动引导或关闭，即虚拟机 1 到 24 同时启动，然后虚拟机 25 在第一批某个完成后立即启动，虚拟机 26 在第一批的第二个完成后启动，以此类推。

- 9 重新启动 Site Recovery Manager Server 以应用新的设置。
- 10 在 vSphere Web Client 中，单击 **站点恢复 > 站点**，然后选择一个站点。
- 11 选择 **高级设置 > vSphere Replication**，并增大 vrReplication.synchronizationTimeout 设置。  
默认值为 7200，对应于工作同步超时期限 14400 秒。
- 12 选择 **高级设置 > 存储**，并增大 storage.commandTimeout 设置。  
默认值为 300 秒。
- 13 单击 **确定** 保存更改。

## 大型 Site Recovery Manager 环境的设置

要保护大量虚拟机，可以修改默认 Site Recovery Manager 设置，以便能够在您的环境中实现最佳恢复时间或避免超时。

可以修改 vSphere Web Client 或 Site Recovery Manager 客户端插件中 **高级设置** 菜单的某些选项。要修改其他设置，可以编辑 Site Recovery Manager Server 上的 vmware-dr.xml 配置文件。当存在某个选项时，请始终通过客户端菜单修改设置。如果修改设置，必须在受保护站点和恢复站点的 Site Recovery Manager Server 和 vCenter Server 实例上进行同样的修改。

要修改设置，请参见 [修改设置以运行大型 Site Recovery Manager 环境](#)。

表 10-1. 用于修改同时执行电源打开或电源关闭操作次数的设置

选项	描述
<b>srmMaxBootShutdownOps</b>	指定任何给定群集的最大并发打开电源操作数。客户机关机（但不是强制关闭电源）受该值限制。在主站点关闭（计划的故障切换）以及 IP 自定义工作流过程中会发生客户机关机情况。通过右键单击群集并选择 <b>设置</b> ，为 vSphere Web Client 中的每个群集修改此选项。单击 <b>vSphere DRS</b> ，然后单击 <b>编辑 &gt; 高级选项</b> 。键入选项以替代可在 <code>vmware-dr.xml</code> 文件中设置的 <b>defaultMaxBootAndShutdownOpsPerCluster</b> 值。可以在 <code>vmware-dr.xml</code> 文件中设置全局值 <b>defaultMaxBootAndShutdownOpsPerCluster</b> ，然后为 vSphere Web Client 中的单个群集设置不同的 <b>srmMaxBootShutdownOps</b> 值。默认情况下，限制处于关闭状态。
<b>defaultMaxBootAndShutdownOpsPerCluster</b>	指定受 Site Recovery Manager 保护的所有群集的最大并发打开电源操作数。客户机关机（但不是强制关闭电源）受该值限制。在主站点关闭（计划的故障切换）以及 IP 自定义工作流过程中会发生客户机关机情况。可在 <code>vmware-dr.xml</code> 文件中修改此设置。可在 vSphere Web Client 中设置的 <b>srmMaxBootShutdownOps</b> 值将替代 <b>defaultMaxBootAndShutdownOpsPerCluster</b> 值。可以在 <code>vmware-dr.xml</code> 文件中设置全局值 <b>defaultMaxBootAndShutdownOpsPerCluster</b> ，然后为 vSphere Web Client 中的单个群集设置不同的 <b>srmMaxBootShutdownOps</b> 值。默认情况下，限制处于关闭状态。
<b>defaultMaxBootAndShutdownOpsPerHost</b>	指定任何独立主机的最大并发打开电源操作数。只能在 <code>vmware-dr.xml</code> 文件中设置该选项。默认情况下，限制处于关闭状态。

表 10-2. 用于修改超时期限的设置

选项	描述
<b>vrReplication.synchronizationTimeout</b>	Site Recovery Manager 会在测试或故障切换期间强制执行超时以完成对由 vSphere Replication 复制的虚拟机的联机或脱机同步。如果同步未在指定的超时时间内完成（例如，由于网络太慢或虚拟机较大），Site Recovery Manager 将在测试或故障切换期间报告故障。在 vSphere Web Client 中修改此选项。在 <b>站点恢复</b> 中，选择一个站点。在 <b>管理</b> 选项卡上，选择 <b>高级设置 &gt; vSphere Replication</b> 。默认值为 7200，对应于工作同步超时期限 14400 秒。
<b>storage.commandTimeout</b>	在与 ABR 相关的工作流中运行 SRA 命令的超时时间。在某些情况下（例如显示 LUN 和快照时），一些阵列响应的时间比默认时间长。在 vSphere Web Client 中修改此选项。在 <b>站点恢复</b> 中，选择一个站点。在 <b>管理</b> 选项卡上，选择 <b>高级设置 &gt; 存储</b> 。默认值为 300 秒。

## 修改长时间运行任务的设置

如果运行需要较长时间才能完成的任务，那么可能远程站点上的默认超时期限已过，任务却尚未完成。您可以配置额外的超时，以允许完成长时间运行的任务。

长时间运行的任务可能是测试恢复，也可能是大型虚拟机的清理。如果虚拟机包含大型磁盘，那么执行测试恢复或完整恢复可能需要很长一段时间。默认超时期限会监控站点之间的连接，因此，如果完成某个任务所需的时间比默认超时期限要长，并且在运行时不向其他站点发送通知，那么将导致超时。在此情况下，您可以在 `vmware-dr.xml` 配置文件中添加一个设置，以便 Site Recovery Manager 在长时间运行的任务完成之前不会超时。

通过向 `vmware-dr.xml` 添加 `<RemoteManager><TaskDefaultTimeout>` 设置，可以配置额外超时期限以便任务得以在远程站点上完成。您也可以配置一个 `<TaskProgressDefaultTimeout>` 设置，以便在某个任务定期报告其进度的情况下，能够延长 Site Recovery Manager 提供给该任务的时间。

如果您配置 `<TaskDefaultTimeout>` 期限，则默认超时不会导致任务失败，即使任务完成时间比 `<DefaultTimeout>` 设置定义的期限要长也不例外。只要 Site Recovery Manager 继续收到来自远程站点的任务进度通知，那么测试恢复、大型虚拟机清理等长时间运行的任务将不会超时。

用于开始任务的初始调用受到 `<DefaultTimeout>` 设置的限制。长时间运行的任务开始后，其受到 `<TaskDefaultTimeout>` 设置的限制。如果某个任务在 `<TaskDefaultTimeout>` 过期时仍未完成，那么进度监视器会检查该任务是否发送了任何进度通知。如果该任务已发送了通知，那么进度监视器会应用 `<TaskProgressDefaultTimeout>` 设置，以允许为该任务提供更多的完成时间。当 `<TaskProgressDefaultTimeout>` 过期时，进度监视器会再次检查进度通知。如果该任务已发送了进度通知，进度监视器仍然会给予该任务更多的时间。如此循序往复，直到任务完成或停止发送进度通知为止。

### 步骤

1 登录 Site Recovery Manager Server 主机。

2 在文本编辑器中打开 `vmware-dr.xml` 文件。

您将在 `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` 文件夹中找到 `vmware-dr.xml` 文件。

3 找到 `vmware-dr.xml` 文件中的 `<RemoteManager>` 元素。

在远程站点上开始所有任务的默认超时为 900 秒，或 15 分钟。

```
<RemoteManager>
<DefaultTimeout>900</DefaultTimeout>
</RemoteManager>
```



- 4 在 <RemoteManager> 标记内添加一个 <TaskDefaultTimeout> 元素。

将 <TaskDefaultTimeout> 期限设置为大于 <DefaultTimeout> 期限的秒数。

<TaskDefaultTimeout> 没有最大值限制。

```
<RemoteManager>
<DefaultTimeout>900</DefaultTimeout>
<TaskDefaultTimeout>2700</TaskDefaultTimeout>
</RemoteManager>
```

- 5 在 <RemoteManager> 标记内添加一个 <TaskProgressDefaultTimeout> 元素。

<TaskProgressDefaultTimeout> 必须至少为 <TaskDefaultTimeout> 期限的 1/100。如果您设置的期限小于 <TaskDefaultTimeout> 期限的 1/100，那么 Site Recovery Manager 会静默调整该超时。

```
<RemoteManager>
<DefaultTimeout>900</DefaultTimeout>
<TaskDefaultTimeout>2700</TaskDefaultTimeout>
<TaskProgressDefaultTimeout>27</TaskProgressDefaultTimeout>
</RemoteManager>
```

- 6 保存并关闭 vmware-dr.xml 文件。
- 7 重新启动 Site Recovery Manager Server 服务以应用新的设置。



# Site Recovery Manager 事件和警报

# 11

Site Recovery Manager 支持事件日志记录。每个事件均包含在事件发生时 Site Recovery Manager 可触发的相应警报。这样就提供了一种方法，用于跟踪系统的健康状况，并在潜在问题影响 Site Recovery Manager 提供的保护之前解决这些问题。

本章讨论了以下主题：

- [Site Recovery Manager 如何监控站点间的连接](#)
- [配置 Site Recovery Manager 警报](#)

## Site Recovery Manager 如何监控站点间的连接

Site Recovery Manager 会监控受保护站点与恢复站点之间的连接，并在远程站点停止响应时记录事件。

当 Site Recovery Manager 在两个配对的 Site Recovery Manager Server 实例之间建立连接时，发起连接的 Site Recovery Manager Server 会发送 `RemoteSiteUpEvent`。

如果 Site Recovery Manager 检测到受监控的连接断开，则会通过向远程站点发送 ping 请求来启动定期连接检查。Site Recovery Manager 监控连接检查并记录事件。

- Site Recovery Manager 定期发送 ping。您可以通过设置 `remoteSiteStatus.pingInterval` 值来配置此时间间隔。默认为 300 秒。
- 连接监视器将跳过一些失败的 Ping 操作。您可以通过设置 `remoteSiteStatus.pingFailedDelay` 值来配置该失败的次数。默认值为 2。
- 当跳过的失败 ping 的数量超出 `remoteSiteStatus.pingFailedDelay` 设置的值时，Site Recovery Manager 会发送一个 `RemoteSitePingFailedEvent` 事件。
- 如果跳过的失败 ping 的数量超出更高的限制，Site Recovery Manager 将为每个失败的 ping 都发送一个 `RemoteSiteDownEvent` 事件，并停止发送 `RemoteSitePingFailedEvent` 事件。您可以通过设置 `remoteSiteStatus.panicDelay` 来配置 Ping 失败次数的上限。默认值为 5。
- Site Recovery Manager 继续发送 `RemoteSiteDownEvent` 事件，直至连接重新建立。
- 与远程站点 Site Recovery Manager Server 重新建立连接后，Site Recovery Manager 将发送 `RemoteSiteUpEvent` 事件。

## 配置 Site Recovery Manager 警报

Site Recovery Manager 会将警报添加到 vCenter Server 所支持的警报中。可以配置 Site Recovery Manager 警报以发送电子邮件通知、发送 SNMP 陷阱或在 vCenter Server 主机上运行脚本。

在 vSphere Web Client 中，**管理**下的**警报定义**选项卡列出了所有 Site Recovery Manager 警报。您可以编辑每个警报的设置，以指定在某一事件触发警报时 Site Recovery Manager 要采取的操作。默认情况下，在配置警报前所有 Site Recovery Manager 警报均不会起作用。

**注** 在具有多个 vCenter Server 的环境中，Site Recovery Manager 显示 Site Recovery Manager 服务器中已注册为扩展的所有事件，即使选择特定 vCenter Server 的事件也是如此。

### 前提条件

要使警报发送电子邮件通知，请在 **vCenter Server 设置**菜单中配置**邮件**设置。请参见《ESXi 和 vCenter Server 文档》。

### 步骤

- 1 在 vSphere Web Client 中，单击 vCenter Server
- 2 在**管理**选项卡中，单击**警报定义**选项卡以显示 vCenter Server 警报的列表。
- 3 单击**添加**以添加新的警报。
- 4 在**常规**页面上，输入警报名称、描述，并从下拉列表中选择要监控的对象。
- 5 选择该对象上发生的特定事件。
- 6 选中**启用此警报**复选框以启用该警报的操作，然后单击**下一步**。
- 7 在**触发器**页面上，单击**添加**以添加事件触发器。
- 8 从下拉列表中选择事件及其相应的状态。

如果在列表中看到重复的事件，则每个事件代表一个 Site Recovery Manager 实例，并会为注册所使用的扩展触发警报。例如，在具有多个 Site Recovery Manager 实例的情况下，可将 `RecoveryPlanCreated (SRM 1)` 和 `RecoveryPlanCreated (SRM 2)` 用于这两个扩展上的同一事件。

- 9 要添加触发警报的条件，请单击**添加**，然后从下拉列表选择一个参数、运算符以及从警告到严重条件的转换。
- 10 单击**下一步**。
- 11 在**操作**页面上，从下拉列表选择一个操作，在配置列中输入相关信息、运行操作的时间以及要重复操作的分钟数，然后单击**完成**。

### 后续步骤

要编辑警报定义，请右键单击警报，然后选择**编辑**。

## Site Recovery Manager 事件参考

Site Recovery Manager 监控不同类型的事件。

### 站点状态事件

站点状态事件提供有关受保护站点和恢复站点的状态以及两者之间连接的信息。

表 11-1. 站点状态事件

事件	描述	原因
UnknownStatusEvent	未知状态	无法获取 Site Recovery Manager Server 状态
RemoteSiteDownEvent	远程站点关闭	Site Recovery Manager Server 已断开与远程 Site Recovery Manager Server 的连接。
RemoteSitePingFailedEvent	远程站点 Ping 失败	远程站点出现故障或网络连接存在问题。
RemoteSiteCreatedEvent	远程站点已创建	本地站点已与远程站点成功配对。
RemoteSiteUpEvent	远程站点正常	Site Recovery Manager Server 重新建立与远程 Site Recovery Manager Server 的连接。
RemoteSiteDeletedEvent	远程站点已删除	远程 Site Recovery Manager 站点已删除。
HbrGroupVmAssociatedEvent	vSphere Replication 复制的虚拟机已添加到保护组中	vSphere Replication 复制的虚拟机已添加到保护组中。
HbrGroupVmDisassociatedEvent	vSphere Replication 复制的虚拟机已从保护组中移除	vSphere Replication 复制的虚拟机已从保护组中移除。
LocalHmsConnectionDownEvent	本地 vSphere Replication Server 关闭	重新尝试连接 vSphere Replication 失败。
LocalHmsConnectionUpEvent	与本地 vSphere Replication Server 之间的连接已还原	与 vSphere Replication 的连接成功。
LocalHmsPingFailedEvent	本地 vSphere Replication Server 未响应	无法建立与本地 vSphere Replication Server 的连接
LocalQsConnectionDownEvent	本地 Inventory Service 已关闭	无法连接到本地 Inventory Service 服务器。可通过在 vmware-dr.xml 配置文件中添加 <code>&lt;connections&gt;&lt;qsPanicDelay&gt;integer&lt;/qsPanicDelay&gt;&lt;/connections&gt;</code> ，指定要在 Site Recovery Manager 引发 LocalQsConnectionDownEvent 之前跳过的内部 ping 的数目。

表 11-1. 站点状态事件（续）

事件	描述	原因
LocalQsConnectionUpEvent	与本地 Inventory Service 之间的连接已还原	与本地清单服务器之间的连接成功。可通过在 vmware-dr.xml 配置文件中添加 <code>&lt;connections&gt;&lt;qsPingInterval&gt;number of seconds&lt;/qsPingInterval&gt;&lt;/connections&gt;</code> ，指定从 Site Recovery Manager 到 Inventory Service 的 ping 操作之间的时间间隔。
LocalQsPingFailedEvent	本地 Inventory Service 未响应	尝试连接本地 Inventory Service 失败。可通过在 vmware-dr.xml 配置文件中添加 <code>&lt;connections&gt;&lt;qsPingFailedDelay&gt;integer&lt;/qsPingFailedDelay&gt;&lt;/connections&gt;</code> ，指定要在 Site Recovery Manager 引发 LocalQsPingFailedEvent 之前跳过的内部 ping 的数目。
LowDiskSpaceEvent	磁盘空间低	本地站点上的可用磁盘空间较低。
LowMemoryEvent	内存低	本地站点上的可用内存较低。

## 保护组事件

保护组事件提供有关与保护组相关的操作和状态的信息。

这些事件有三种类别：

- 保护组复制信息事件
- 保护组复制警告事件
- 保护组复制错误事件

表 11-2. 保护组复制信息事件

事件	描述	原因
CreatedEvent	已创建保护组。	创建保护组的提交阶段完成之后，发布到两个 vCenter Server 上。
RemovedEvent	已移除保护组。	移除保护组的提交阶段完成之后，发布到两个 vCenter Server 上。
ReconfiguredEvent	已重新配置保护组。	重新配置保护组的提交阶段完成之后，发布到两个 vCenter Server 上。
ProtectedVmCreatedEvent	已为组中的虚拟机配置保护。	保护虚拟机的提交阶段完成之后，发布到两个 vCenter Server 上。
ProtectedVmRemovedEvent	不再为组中的虚拟机配置保护。	取消保护虚拟机的提交阶段完成之后，发布到两个 vCenter Server 上。
ProtectedVmReconfiguredProtectionSettingsEvent	已为虚拟机重新配置保护设置。	重新配置虚拟机保护设置的提交阶段完成之后，发布到两个 vCenter Server 上。

表 11-2. 保护组复制信息事件（续）

事件	描述	原因
ProtectedVmReconfiguredRecoveryLocationSettingsEvent	已为虚拟机重新配置恢复位置设置。	重新配置受保护虚拟机的恢复位置设置成功后才发布在受保护站点的 vCenter Server 上。
PlaceholderVmCreatedEvent	占位虚拟机是在 vCenter Server 清单中创建的。	由于保护、修复操作而创建占位虚拟机时发布在恢复站点 vCenter Server 上。
PlaceholderVmCreatedFromOldProductionVmEvent	占位虚拟机是在 vCenter Server 清单中使用原有受保护虚拟机的标识创建的。	由于在重新保护操作期间或之后将原有受保护虚拟机与占位虚拟机交换而创建占位虚拟机时发布在恢复站点 vCenter Server 上。

表 11-3. 保护组复制警告事件

事件	描述	原因
VmFullyProtectedEvent	组中的虚拟机：未解析设备已全部解析。	受保护虚拟机先前未解析的设备已全部解析。
VmNotFullyProtectedEvent	组中的虚拟机：需要为一个或多个设备配置保护。	仅在将恢复位置设置更新为非空 unresolvedDevices 集的设备处理时发布在受保护站点 vCenter Server 上。受保护虚拟机发生更改或在重新保护虚拟机期间会触发此事件。
PlaceholderVmUnexpectedlyDeletedEvent	组中的虚拟机：占位虚拟机已从 vCenter Server 清单中删除。	当 Site Recovery Manager 检测到从 vCenter Server 清单中意外删除或移除占位虚拟机时，发布在恢复站点 vCenter Server 上。

表 11-4. 保护组复制错误事件

事件	描述	原因
ProductionVmDeletedEvent	组中的虚拟机：受保护虚拟机已从虚拟机 vCenter Server 清单中移除。	当受保护虚拟机从 vCenter Server 清单中删除或移除时发布。
ProductionVmInvalidEvent	组中的虚拟机：无法解析要复制的受保护虚拟机的文件位置。	当复制提供程序无法找到受保护虚拟机文件以进行复制时发布。

## 恢复事件

恢复事件提供与 Site Recovery Manager 恢复过程相关联的操作和状态的相关信息。

表 11-5. 恢复事件

事件	描述	原因
RecoveryVmBegin	恢复计划已开始恢复指定虚拟机。	成功创建恢复虚拟机后发出指示。如果在获知虚拟机 ID 之前出现了一些错误，则不会触发此事件。
RecoveryVmEnd	恢复计划已完成虚拟机恢复。	在完成上一打开电源后脚本之后，或者在虚拟机出现恢复停止错误之后发出指示。

表 11-5. 恢复事件（续）

事件	描述	原因
PlanCreated	恢复计划 <i>hostname</i> 已创建。	创建新计划时发出指示。其发送到托管计划的各个 vCenter Server 实例中。
PlanDestroy	恢复计划已破坏。	从站点删除计划后发出指示。请注意，请求删除站点中的计划时，如果等待在另一站点上删除此计划，则可能会有明显的延迟。新计划将发送到托管计划的每个 vCenter Server 实例。
PlanEdit	恢复计划已更改。	编辑现有计划后发出指示。
PlanExecTestBegin	恢复计划已开始进行测试。	启动恢复测试后在恢复站点上发出指示。
PlanExecTestEnd	恢复计划已完成测试。	完成恢复测试后在恢复站点上发出指示。
PlanExecCleanupBegin	恢复计划已开始测试清理。	启动测试清理后在恢复站点上发出指示。
PlanExecCleanupEnd	恢复计划已完成测试清理。	完成测试清理后在恢复站点上发出指示。
PlanExecBegin	恢复计划已开始恢复。	启动恢复后在恢复站点上发出指示。
PlanExecEnd	恢复计划已完成恢复。	完成恢复后在恢复站点上发出指示。
PlanExecReprotectBegin	恢复计划已开始重新保护操作。	启动重新保护后在恢复站点上发出指示。
PlanExecReprotectEnd	恢复计划已完成重新保护操作。	完成重新保护后在恢复站点上发出指示。
PlanPromptDisplay	恢复计划正在显示提示并等待用户输入。	出现提示步骤时在恢复站点上发出指示。此事件关键字是提示的唯一标识符。
PlanPromptResponse	恢复计划已收到其提示的回答。	结束提示步骤时在恢复站点上发出指示。
PlanServerCommandBegin	恢复计划已开始在 Site Recovery Manager Server 计算机上运行命令。	当 Site Recovery Manager 已开始在 Site Recovery Manager Server 计算机上运行 callout 命令时在恢复站点上发出指示。
PlanServerCommandEnd	恢复计划已在 Site Recovery Manager Server 计算机上完成命令的执行。	当 Site Recovery Manager 在 Site Recovery Manager Server 计算机上完成了 callout 命令的运行时在恢复站点上发出指示。
PlanVmCommandBegin	恢复计划已开始在恢复的虚拟机上运行命令。	当 Site Recovery Manager 开始在恢复的虚拟机上运行 callout 命令时在恢复站点上发出指示。
PlanVmCommandEnd	恢复计划已在恢复的虚拟机上完成命令的执行。	当 Site Recovery Manager 已在恢复的虚拟机上完成 callout 命令的运行时在恢复站点上发出指示。

## 存储和存储提供程序事件

存储和存储提供程序事件提供有关与存储或存储提供程序相关的操作和状态的信息。

**表 11-6. SRA 事件**

事件	描述	原因
StorageAdaptLoadEvent	已加载指定的 SRA。	Site Recovery Manager 可在启动时或用户启动的 SRA 重新加载过程中检测到新的 SRA。
StorageAdaptReloadFailEvent	无法从指定路径加载 SRA。	Site Recovery Manager 无法在启动时或用户启动的 SRA 重新加载过程中重新加载先前已知的 SRA。
StorageAdaptChangeEvent	已加载新版本的指定 SRA。	Site Recovery Manager 检测到先前已知的 SRA 已升级。

**表 11-7. 阵列管理器事件**

事件	描述	原因
SAManagerAddedEvent	已使用指定的 SRA 创建指定的阵列管理器。	用户已添加阵列管理器。
SAManagerRemovedEvent	已删除指定的阵列管理器。	用户已移除阵列管理器。
SAManagerReconfigEvent	已重新配置指定的阵列管理器。	用户已编辑阵列管理器属性。
SAManagerPingOkEvent	已成功对指定的阵列管理器执行 Ping。	Site Recovery Manager Server 已成功 Ping 阵列管理器。
SAManagerPingFailEvent	无法 Ping 指定的阵列管理器。	Ping 阵列管理器过程中出错。

**表 11-8. 阵列对事件**

事件	描述	原因
SAPairDiscoveredEvent	已使用阵列管理器找到已复制的阵列对。	用户已创建可找到已复制阵列对的阵列管理器。
SAPairEnabledEvent	已使用阵列管理器启用已复制的阵列对。	用户已启用阵列对。
SAPairDisabledEvent	已使用阵列管理器禁用已复制的阵列对。	用户已禁用阵列对。
SAPairPingOkEvent	已成功对复制的阵列对执行 Ping。	Site Recovery Manager Server 已成功 Ping 阵列对。
SAPairPingFailEvent	无法 Ping 复制的阵列对。	Ping 阵列对过程中出错。

**表 11-9. 数据存储事件**

事件	描述	原因
StorageDsDiscoveredEvent	已找到复制的数据存储。	Site Recovery Manager Server 已找到复制的数据存储。
StorageDsLostEvent	指定的数据存储不再进行复制。	用户已关闭对支持数据存储的存储设备的复制。

表 11-9. 数据存储事件（续）

事件	描述	原因
StorageRdmDiscoveredEvent	已找到附加到指定虚拟机的复制的 RDM。	Site Recovery Manager Server 已找到复制的 RDM。将 RDM 磁盘添加到受保护的虚拟机时会发生该事件。
StorageRdmLostEvent	附加到指定虚拟机的 RDM 不再进行复制。	用户已关闭对支持 RDM 的 LUN 的复制。

表 11-10. 保护事件

事件	描述	原因
SPDsProtEvent	已保护指定保护组中的数据存储。	用户已将数据存储包含在新保护组或现有保护组中。
SPDsUnprotEvent	已取消保护指定的数据存储。	用户已从保护组移除数据存储或已删除包含此数据存储的保护组。当从保护组移除数据存储或移除保护组来取消保护该数据存储时会发生该事件。
SPVmDiscoveredEvent	已找到复制的虚拟机。	用户已在复制的数据存储上创建虚拟机。
SPVmLostEvent	指定的虚拟机不再进行复制	用户已将虚拟机迁移出复制的数据存储。
SPDsProtMissingEvent	复制的数据存储需要包含在指定的保护组中，但却包含在备用保护组中。	如果您的数据存储需要合并，并且仍未受到保护，则会发生该事件。发生冲突事件时，数据存储已受到保护。
SPDsProtConflictEvent	复制的数据存储需要包含在指定的保护组中。	如果您的数据存储需要合并，并且仍未受到保护，则会发生该事件。发生冲突事件时，数据存储已受到保护。
SPDsReplicationLostEvent	包含在指定保护组中的数据存储不再进行复制。	用户已关闭对支持数据存储的设备的复制。
SPGroupProtRestoredEvent	已恢复对指定保护组的保护。	保护组先前（非空）的问题已清除。
SPVmDsProtMissingEvent	由虚拟机使用的数据存储需要包含在指定的保护组中。	如果您将某个数据存储添加到已受保护组保护的虚拟机，但该数据存储不在此保护组中，您需要将其添加到保护组中。
SPVmDsProtConflictEvent	由指定虚拟机使用的数据存储需要添加到指定的保护组中，但当前正由备用保护组使用。	如果您将某个数据存储添加到已受保护组保护的虚拟机，但该数据存储不在此保护组中，您需要将其添加到保护组中。
SPVmDsReplicationLostEvent	由指定虚拟机使用且包含在指定保护组中的数据存储不再进行复制。	请参见说明。
SPVmProtRestoredEvent	已恢复对指定保护组中指定虚拟机的保护。	受保护虚拟机先前（非空）的问题已清除。清除与无保护虚拟机相关的问题后，将不会发布此事件
SPCgSpansProtGroupsEvent	指定的一致性组可以跨越指定的保护组。	如果两个受保护的数据存储位于不同的保护组中，则稍后将它们合并到阵列上的同一个一致性组中时会发生该事件。
SPCgDsMissingProtEvent	指定的一致性组的数据存储需要包含在指定的保护组中。	请参见说明。



表 11-10. 保护事件（续）

事件	描述	原因
SPDspansConsistGroupsEvent	数据存储跨不同一致性组中的设备。	如果多个 LUN 上具有相同的数据存储，但这些 LUN 不属于同一个一致性组，则会发生该事件。
SPNfsDsUrlConflictEvent	从指定卷挂载的 NFS 数据存储具有从远程主机挂载的不同 URL。远程路径具有指定的 URL，而从其他主机挂载的数据存储具有指定的 URL。	同一 NFS 卷是使用两个不同数据存储中相同的 NFS 服务器的不同 IP 地址挂载的。

## 许可事件

许可事件提供有关 Site Recovery Manager 许可状态更改的信息。

表 11-11. 许可事件

事件	描述	原因
LicenseExpiringEvent	指定站点的 Site Recovery Manager 许可证在指定天数后过期。	每隔 24 小时，即会检查一次即将过期的非评估许可证的剩余天数。此事件将与结果一起发布。
EvaluationLicenseExpiringEvent	指定站点的 Site Recovery Manager 评估许可证在指定天数后过期。	每隔 24 小时，即会检查一次评估许可证的剩余天数。此事件将与结果一起发布。
LicenseExpiredEvent	指定站点的 Site Recovery Manager 许可证已过期。	每隔 30 分钟，已过期的（非评估）许可证将发布一次此事件。
EvaluationLicenseExpiredEvent	指定站点的 Site Recovery Manager 评估许可证已过期。	每隔 30 分钟，评估许可证将发布一次此事件。
UnlicensedFeatureEvent	指定站点的 Site Recovery Manager 许可证分配数量已超出指定的许可证数量。	每隔 24 小时，基于虚拟机是否受保护判定，若许可证总数超出许可证容量，则发布一次此事件。
LicenseUsageChangedEvent	指定站点的 Site Recovery Manager 许可证正在使用总许可证数量中的指定数量。	每隔 24 小时，基于虚拟机是否受保护判定，若许可证总数未超出许可证容量，则发布一次此事件。

## 权限事件

权限事件提供有关 Site Recovery Manager 权限更改的信息。

表 11-12. 权限事件

事件	描述	原因
PermissionsAddedEvent	为 Site Recovery Manager 上的实体创建的权限。	已使用指定角色创建实体的权限。 IsPropagate 标记指定权限是否在实体层次结构中向下传播。
PermissionsDeletedEvent	Site Recovery Manager 上实体的权限规则已删除。	实体的权限已删除。
PermissionsUpdatedEvent	Site Recovery Manager 上的实体的权限已更改。	指定的实体的权限已修改。

## SNMP 陷阱

Site Recovery Manager 将 SNMP 陷阱发送到 vCenter Server 中定义的团体目标。可以使用 vSphere Web Client 对其进行配置。输入 localhost 或 127.0.0.1 作为 SNMP 陷阱的目标主机后，Site Recovery Manager 会使用 Site Recovery Manager 安装程序配置的 vSphere 服务器的 IP 地址或主机名。

Site Recovery Manager 5.x 的 SNMP 陷阱向后兼容 Site Recovery Manager 4.0 及更高版本。

**表 11-13. SNMP 陷阱**

事件	描述	原因
RecoveryPlanExecuteTestBeginTrap	恢复计划开始测试时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况。
RecoveryPlanExecuteTestEndTrap	恢复计划结束测试后，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、结果状态。
RecoveryPlanExecuteCleanupBeginTrap	恢复计划开始测试清理时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况。
RecoveryPlanExecuteCleanupEndTrap	恢复计划结束测试清理后，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、结果状态。
RecoveryPlanExecuteBeginTrap	恢复计划开始恢复时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况。
RecoveryPlanExecuteEndTrap	恢复计划结束恢复后，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、结果状态。
RecoveryPlanExecuteReprotectBeginTrap	Site Recovery Manager 开始针对恢复计划的重新保护工作流时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况。
RecoveryPlanExecuteReprotectEndTrap	Site Recovery Manager 完成针对恢复计划的重新保护工作流后，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、结果状态。
RecoveryVmBeginTrap	恢复计划开始恢复虚拟机时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、虚拟机名称、虚拟机 UUID。
RecoveryVmEndTrap	恢复计划完成恢复虚拟机后，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、虚拟机名称、虚拟机 UUID、结果状态。
RecoveryPlanServerCommandBeginTrap	恢复计划在 Site Recovery Manager Server 计算机上开始执行命令标注时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、命令名称。
RecoveryPlanServerCommandEndTrap	恢复计划在 Site Recovery Manager Server 计算机上完成执行命令标注后，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、命令名称、结果状态。
RecoveryPlanVmCommandBeginTrap	恢复计划在已恢复虚拟机上开始执行命令标注时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、命令名称、虚拟机名称、虚拟机 UUID。

表 11-13. SNMP 陷阱（续）

事件	描述	原因
RecoveryPlanVmCommandEndTrap	恢复计划在已恢复虚拟机上完成执行命令标注后，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、命令名称、虚拟机名称、虚拟机 UUID、结果状态。
RecoveryPlanPromptDisplayTrap	恢复计划在继续之前要求用户输入时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况、提示字符串。
RecoveryPlanPromptResponseTrap	恢复计划在继续之前不再要求用户输入信息时，会发送此陷阱。	Site Recovery Manager 站点名称、恢复计划名称、恢复类型、执行状况。

# 收集 Site Recovery Manager 日志文件

# 12

要帮助确定导致 Site Recovery Manager 日常运行期间所遇到的任何问题的原因，可能需要收集 Site Recovery Manager 日志文件以进行检查或发送到 VMware 支持部门。

Site Recovery Manager 会创建多个日志文件，这些日志文件中的信息可以帮助 VMware 支持部门诊断问题。可以使用 Site Recovery Manager 日志收集器简化日志文件收集。

Site Recovery Manager Server 和客户端使用不同的日志文件。

Site Recovery Manager Server 日志文件包含有关服务器配置的信息以及与服务器操作相关的消息。Site Recovery Manager Server 日志包还包含系统信息以及最新恢复计划执行的历史记录报告。

Site Recovery Manager 客户端日志文件包含有关客户端配置的信息以及与客户端插件操作相关的消息。Site Recovery Manager 包还包含安装程序日志文件以及日志目录的存储复制适配器 (SRA) 子目录的内容。

来自 Site Recovery Manager 系统中的 vCenter Server 实例和 ESXi Server 实例的日志文件可能还包含用于诊断 Site Recovery Manager 问题的有用信息。

Site Recovery Manager 日志文件会收集或检索文件，并将这些文件压缩成压缩文件，并放置在您所选择的位置中。

Site Recovery Manager 操作期间遇到的错误将显示在错误对话框中或显示在**近期任务**窗口中。大多数错误还会在 Site Recovery Manager 日志文件中生成条目。检查恢复站点和受保护站点的近期任务和日志文件。

## 通过使用 Site Recovery Manager 界面收集 Site Recovery Manager 日志文件

可将 Site Recovery Manager 的日志下载到用户指定的位置。

使用此信息了解并解决问题。为达到最佳效果，请收集每个站点中的日志。

### 步骤

- 1 在 vSphere Web Client 中，单击**站点恢复 > 站点**，然后选择一个站点。
- 2 从**操作**菜单中，选择**导出 SRM 日志**。还可右键单击站点，然后选择**导出 SRM 日志**。
- 3 在**导出 SRM 日志**向导中，单击**生成日志**并等待操作完成。
- 4 单击**下载日志**下载日志。

## 手动收集 Site Recovery Manager 日志文件

可以下载手动生成的日志包中的 Site Recovery Manager Server 日志文件。如果您无法访问 vSphere Client，该操作会非常有用。

以下过程生成的日志包与您使用 vSphere Client 生成的日志相同。

### 步骤

- ◆ 从**开始**菜单启动 Site Recovery Manager Server 日志文件的收集：
  - a 登录 Site Recovery Manager Server 主机。
  - b 选择**开始 > 程序 > VMware > VMware Site Recovery Manager > 生成 VMware vCenter Site Recovery Manager 日志包**。
- ◆ 从 Windows 命令行启动 Site Recovery Manager Server 日志文件的收集：
  - a 在 Site Recovery Manager Server 主机上启动 Windows Command Shell。
  - b 将目录更改为 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin。
  - c 运行下列命令。

```
cscript srm-support.wsf
```

### 结果

各个日志文件均收集在名为 srm-support-MM-DD-YYYY-HH-MM.zip 的文件中，其中 MM-DD-YYYY-HH-MM 表示创建日志文件的月、日、年、小时和分钟。默认情况下日志包保存在桌面上。

## 更改 Site Recovery Manager Server 日志文件的大小和数目

可更改 Site Recovery Manager Server 日志文件的大小、数目和位置。

可修改 Site Recovery Manager Server 上 vmware-dr.xml 配置文件中的 Site Recovery Manager 日志设置。

### 步骤

- 1 登录 Site Recovery Manager Server 主机。
- 2 在文本编辑器中打开 vmware-dr.xml 文件。  
 您将在 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config 文件夹中找到 vmware-dr.xml 文件。
- 3 查找 vmware-dr.xml 文件中的 <log> 部分。

#### 4 设置要保留的日志的最大大小（以字节为单位）。

通过向 <log> 部分中添加 <maxFileSize> 部分可设置最大日志大小。默认值为 **5242880** 字节。

```
<log>

    <maxFileSize>5242880</maxFileSize>

</log>
```

#### 5 设置要保留的日志文件的最大数量。

通过向 <log> 部分中添加 <maxFileNum> 部分可设置日志的最大数量。默认值为 **10** 个日志文件。

```
<log>

    <maxFileNum>50</maxFileNum>

</log>
```

#### 6 更改要在 Site Recovery Manager Server 上存储日志的位置。

通过修改 <log> 部分中的 <directory> 部分可更改日志位置。

```
<log>

    <directory>C:\ProgramData\VMware\VMware vCenter Site Recovery
    Manager\Logs</directory>

</log>
```

#### 7 更改日志文件的默认前缀。

通过修改 <log> 部分中的 <name> 部分可更改默认前缀。

```
<log>

    <name>vmware-dr</name>

</log>
```

#### 8 更改日志记录级别。

通过修改 <log> 部分中的 <level> 部分可更改日志记录级别。可能的日志记录级别包括错误、警告、信息、琐事和详细。

```
<log>

    <level>verbose</level>

</log>
```

## 9 （可选）为 Site Recovery Manager Server 组件设置日志记录级别。

可通过修改相应的 `<level>` 部分为组件设置特定的日志记录级别。可能的日志记录级别包括错误、警告、信息、琐事和详细。例如，可将恢复的日志记录级别设置为“琐事”。

```
<level id="Recovery">
  <logName>Recovery</logName>
  <logLevel>trivia</logLevel>
</level>
```

## 10 （可选）为存储复制适配器设置日志记录级别。

设置 Site Recovery Manager 日志记录级别并不会为 SRA 设置日志记录级别。通过向 `vmware-dr.xml` 中添加 `<level id="SraCommand">` 部分设置 SRA 日志记录级别，可更改 SRA 日志记录级别。可能的日志记录级别包括错误、警告、信息、琐事和详细。

```
<level id="SraCommand">
  <logName>SraCommand</logName>
  <logLevel>trivia</logLevel>
</level>
```

## 11 重新启动 Site Recovery Manager Server 服务以使更改生效。

# 配置 Site Recovery Manager 核心转储

可配置 Site Recovery Manager 核心转储设置以更改核心转储文件的位置并进行压缩。

可修改 Site Recovery Manager Server 上 `vmware-dr.xml` 配置文件中的 Site Recovery Manager 核心转储设置。

Site Recovery Manager Server `rundll32.exe` 子进程监视主 Site Recovery Manager Server 进程的紧急退出情况，然后负责生成核心转储。

### 步骤

#### 1 登录 Site Recovery Manager Server 主机。

#### 2 在文本编辑器中打开 `vmware-dr.xml` 文件。

您将在 `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` 文件夹中找到 `vmware-dr.xml` 文件。

#### 3 更改要在 Site Recovery Manager Server 上存储核心转储的位置。

可通过修改 `<coreDump>` 部分更改核心转储的位置。

```
<coreDump>C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles</coreDump>
```

默认路径为 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles，除非此位置不存在或不可写。在这种情况下，Site Recovery Manager Server 将使用 C:\ProgramData\VMware。

#### 4 使用核心转储系统参数限制创建或压缩的转储文件的数量。

```
<debug>
  <dumpCoreCompression>true,false</dumpCoreCompression>
  <dumpFullCore>true,false</dumpFullCore>
</debug>
```

选项	描述
<b>dumpCoreCompression</b>	如果不指定，默认值为 <b>false</b> 。Site Recovery Manager Server 在创建核心转储文件时不压缩之前的核心转储文件。如果指定 <b>true</b> ，Site Recovery Manager Server 会在生成新核心转储时压缩所有旧核心转储。
<b>dumpFullCore</b>	如果不指定，默认值为 <b>false</b> 。Site Recovery Manager Server 生成大小为几 MB 的核心转储文件，并在出现问题时提供支持帮助。如果将此值设置为 <b>true</b> ，Site Recovery Manager Server 会生成完整核心转储文件，文件大小可能为几个 GB，具体取决于执行核心转储时的工作负载。发生问题时，此较大文件可以为技术支持提供更多帮助。如果磁盘空间允许，请将此值设置为 <b>true</b> 。

#### 5 要修改核心转储文件的最大数量，请向 <debug> 部分添加以下行。

```
<maxCoreDumpFiles>max_files</maxCoreDumpFiles>
```

如果不指定，默认值为 **4**。此值指定核心转储目录中保留的核心转储文件的最大数量。Site Recovery Manager Server 创建核心转储时，Site Recovery Manager Server 会在必要时删除旧文件以避免超过最大值和占用过多的磁盘空间，尤其是在将 **dumpFullCore** 设置为 **true** 时。



# Site Recovery Manager 故障排除

# 13

如果在创建保护组和恢复计划、恢复或客户机自定义时遇到问题，可以对问题进行故障排除。

搜索问题原因时，还要查看位于 <http://kb.vmware.com/> 的 VMware 知识库。

## Site Recovery Manager 运行标注时，会使命令行中的反斜线数量增加为原来的两倍

如果标注命令行中有反斜线，Site Recovery Manager 会使所有反斜线数量增加为原来的两倍。

### 问题

命令行系统解释程序仅将文件路径中的双反斜线视为单反斜线。如果标注命令在参数中而不是在文件路径中需要反斜线，且该命令无法将双反斜线转换为单反斜线，则标注命令可能会失败，并发出错误消息。

例如，可以向 workflow 添加标注步骤并输入以下文本作为命令：

```
c:\Windows\system32\cmd.exe /C "C:\myscript.cmd" a/b/c \d\e\f \\g\\h c:\myscript.log
```

作为标注步骤的结果，Site Recovery Manager 将运行以下命令：

```
c:\Windows\system32\cmd.exe /C "C:\myscript.cmd" a/b/c \\d\\e\\f \\g\\h c:\myscript.log
```

如果 `myscript.cmd` 未将双反斜线更改为单反斜线，且参数 `\d\e\f` 和 `\\g\\h` 将区分反斜线的个数，则 `myscript.cmd` 会失败。

### 解决方案

- 1 另外创建一个命令行批处理文件，以包含命令和全部所需的参数。标注步骤无需任何参数即可运行此另外创建的批处理文件。例如，解决方案如下所示：
  - a 在文本编辑器（如记事本）中，创建文件 `c:\SRM_callout.cmd`，该文件包含以下内容：  
**`C:\myscript.cmd a/b/c \d\e\f \\g\\h c:\myscript.log`**
  - b 在恢复计划标注步骤中，输入要运行的命令：  
**`c:\Windows\system32\cmd.exe /C c:\SRM_callout.cmd`**

2 向使用单反斜线替换双反斜线的原始脚本文件中添加代码。

a 在脚本文件 `c:\myscript.cmd` 的开头添加类似于以下示例的代码。

```
@echo off
set arg2=%2
set arg3=%3
set fixed_arg2=%arg2:\\=%
set fixed_arg3=%arg3:\\=%
```

如果在脚本中使用 `shift` 命令，则所有与反斜线相关的参数都以这种方式处理。

b 如果在脚本中不使用 `shift` 命令，请进行以下更改：

将 `%2` 替换为 `%fixed_arg2%`。

将 `%3` 替换为 `%fixed_arg3%`。

c 请勿更改标注步骤命令。

## 在恢复站点上同时打开多个虚拟机的电源会导致错误

当多个虚拟机同时执行引导操作时，可能会在基于阵列的恢复和 vSphere Replication 恢复期间出现错误。

### 问题

当在恢复站点上同时打开多个虚拟机的电源时，您可能会在恢复历史记录报告中看到以下错误：

- 'echo 命令“Starting IP customization on Windows ...” > > %VMware\_GuestOp\_OutputFile%。
- 无法完成自定义，可能是由于脚本编制运行时错误或脚本参数无效。
- 向客户机虚拟机上载文件时出错。
- 600 秒后等待 VMware Tools 超时。

### 原因

默认情况下，Site Recovery Manager 不会限制可同时执行的电源打开操作次数。如果在恢复站点上打开虚拟机电源时遇到错误，您可以修改 `vmware-dr.xml` 文件，以便对同时打开电源的虚拟机数量设置限制。

如果遇到上述错误，请根据独立主机或群集所在环境的容量，限制恢复站点上电源打开操作的次数。

### 解决方案

- 1 在恢复服务器上，转到 `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config`。
- 2 在文本编辑器中打开 `vmware-dr.xml` 文件。

- 更新 `defaultMaxBootAndShutdownOpsPerCluster` 和 `defaultMaxBootAndShutdownOpsPerHost` 值以限制恢复站点上电源打开操作的次数。

以下示例显示了如何将电源打开操作次数限制为每个群集最多 32 次，每个独立主机最多 4 次。

```
<config>
<defaultMaxBootAndShutdownOpsPerCluster>32</defaultMaxBootAndShutdownOpsPerCluster>
<defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
</config>
```

- 重新启动 Site Recovery Manager Server 服务。

## 向保护组添加虚拟机失败，并显示无法解析设备的错误

如果未配置相应的清单映射，则向保护组添加虚拟机将失败，并显示错误。

### 问题

向保护组添加虚拟机时，您将看到以下错误消息：由于设备未解析，无法保护虚拟机 “*virtual machine name*” (Unable to protect VM '*virtual machine name*' due to unresolved devices)。

### 原因

您尚未配置将受保护站点上的虚拟机设备映射到恢复站点上对应设备的清单映射。

### 解决方案

如 Site Recovery Manager 的安装和配置中所述，配置清单映射。

## 配置保护失败并显示占位虚拟机创建错误

在多个虚拟机上配置保护时，配置失败并显示占位虚拟机创建错误。

### 问题

在大量虚拟机上同时配置保护时失败，并显示占位虚拟机创建超时错误或占位虚拟机创建命名错误：

- 占位虚拟机创建错误：操作已超时：300 秒 (Placeholder VM creation error:Operation timed out:300 seconds)
- 占位虚拟机创建错误：名称 “*placeholder\_name*” 已存在 (Placeholder VM creation error:The name '*placeholder\_name*' already exists)

使用不同的方式配置保护时会出现此问题：

- 创建的保护组包含一个或多个其中含有大量虚拟机的数据存储。
- 针对大量虚拟机，使用 Site Recovery Manager 界面中的**保护组 > 虚拟机 > 全部还原**选项。
- 使用 Site Recovery Manager API 手动保护大量虚拟机。

## 原因

恢复站点上的基础架构无法处理并发创建占位虚拟机的卷。

## 解决方案

增加默认为 300 秒的 `replication.placeholderVmCreationTimeout` 设置。请参见[更改占位虚拟机创建超时时间](#)。

更改此设置后，无需重新启动 Site Recovery Manager Server。Site Recovery Manager 会在您下次在虚拟机上配置保护时应用此设置。

# 快速删除和重新创建占位虚拟机失败

如果从某个数据存储删除所有占位虚拟机，卸载该数据存储，然后重新挂载数据存储，则重新创建占位虚拟机可能会失败。

## 问题

卸载数据存储后立即重新创建占位虚拟机可能会失败并出现错误 `NoCompatibleHostFound`。

## 原因

ESXi 主机和数据存储之间的关联每 10 分钟更新一次。如果您在卸载并重新挂载数据存储后但在下一次更新之前重新创建占位虚拟机，则无法找到主机。

## 解决方案

请在卸载并重新挂载数据存储后至少等待 10 分钟，然后重新创建占位虚拟机。

# 由于主机处于错误的状态，因此计划的迁移失败

如果在计划的迁移期间将恢复站点上的 ESXi 主机置于维护模式，则计划的迁移将失败。

## 问题

计划的迁移失败，并显示错误 `错误 - 在主机的当前状况下不允许执行此操作 (Error - The operation is not allowed in the current state of the host)`。

## 原因

当恢复站点上的 ESXi 主机处于维护模式时，Site Recovery Manager 无法打开恢复站点上虚拟机的电源。

## 解决方案

使恢复站点上的 ESXi 主机退出维护模式，然后重新运行计划的迁移。

## 恢复失败，在对某些虚拟机进行网络自定义期间出现超时错误

恢复期间，某些虚拟机没有恢复，并在网络自定义期间显示超时错误。

### 问题

恢复期间，某些虚拟机在默认的 120 秒超时时间段内没有恢复。

### 原因

该问题可能由以下原因之一产生。

- 正在恢复的虚拟机上未安装 VMware Tools 软件包。
- 尝试同时恢复多台虚拟机时恢复站点上群集的资源利用率较高。在这种情况下，您可以增加特定超时设置以允许任务有更多时间能够完成。请参见[更改恢复设置](#)。

### 解决方案

- 1 请验证正在恢复的虚拟机上是否已安装 VMware Tools。
- 2 检查恢复站点上的可用容量。

如果恢复站点的资源利用率较高，为客户机自定义增加超时时间段可以解决该问题。

- a 在 vSphere Web Client 中，单击**站点恢复 > 站点**，选择一个站点然后单击**管理 > 高级设置**。
- b 选择**恢复**，然后单击**编辑**。
- c 增加 `recovery.customizationTimeout` 参数，默认值为 600 秒。
- d 增加 `recovery.powerOnTimeout` 参数，默认值为 300 秒。

- 3 重新运行恢复。

## 恢复失败，并显示主机和数据存储不可用错误

如果您在 vCenter Server 清单中发生更改之后立即运行恢复或测试，恢复或测试恢复将失败，并显示与主机硬件和数据存储不可用有关的错误消息。

### 问题

恢复或测试恢复失败，并显示错误消息：已打开电源且不处于维护模式的主机 (具有硬件版本 “7” 和数据存储 “ds\_id”) 不可用... (No host with hardware version '7' and datastore 'ds\_id' which are powered on and not in maintenance mode are available...)

### 原因

Site Recovery Manager Server 会保留主机清单状况的缓存。有时，当清单最近发生更改（例如，主机无法访问、断开连接或与某些数据存储失去连接）时，Site Recovery Manager Server 可能需要长达 15 分钟才能更新其缓存。如果 Site Recovery Manager Server 缓存中的主机清单状况不正确，则恢复或测试恢复可能会失败。

## 解决方案

如果您对主机清单进行了更改，请先等待 15 分钟，再运行恢复。如果您再次收到错误消息，请等待 15 分钟后重新运行恢复。

## 重新保护失败，并显示 vSphere Replication 超时错误

对包含 vSphere Replication 保护组的恢复计划运行重新保护时，该操作将超时并显示错误。

### 问题

无法对包含 vSphere Replication 保护组的恢复计划执行重新保护操作，并显示错误操作超时：7200 秒，VR 同步失败，因为 VRM 组 <不可用>。操作超时：7200 秒 (Operation timed out: 7200 seconds VR synchronization failed for VRM group <Unavailable>. Operation timed out: 7200 seconds)。

### 原因

运行重新保护时，Site Recovery Manager 将对 vSphere Replication 保护组执行联机同步，这可能导致操作超时。默认超时值为 2 小时，对应于工作同步超时值 4 小时。

### 解决方案

增加“高级设置”中的 synchronizationTimeout 超时值。请参见[更改 vSphere Replication 设置](#)。

## 等待 VMware Tools 时恢复计划超时

等待 VMware Tools 启动过程中运行恢复计划失败，并出现超时错误。

### 问题

在执行恢复计划的关闭虚拟机步骤或等待 VMware Tools 步骤时，恢复操作失败。

### 原因

Site Recovery Manager 使用 VMware Tools 检测信号发现已恢复虚拟机在恢复站点上运行的时间。恢复操作需要您在受保护虚拟机上安装 VMware Tools。如果您未在受保护虚拟机上安装 VMware Tools，或者如果您未将 Site Recovery Manager 配置为不等到 VMware Tools 启动后再启动，恢复将失败。

### 解决方案

在受保护虚拟机上安装 VMware Tools。如果在受保护的虚拟机上未安装或无法安装 VMware Tools，则必须将 Site Recovery Manager 配置为不等待 VMware Tools 在已恢复的虚拟机中启动，并且跳过客户机操作系统关闭步骤。请参见[更改恢复设置](#)。

## vSphere Replication 保护组同步失败

在测试恢复、计划迁移和重新保护包含 vSphere Replication 保护组的恢复计划期间，虚拟机同步步骤失败并出现错误。

### 问题

vSphere Replication 保护组中的虚拟机同步失败，并出现错误消息错误 - VR 同步失败，因为 VRM 组 <不可用>。对象已被删除，或者未完全创建。

### 原因

保护组中的一个或多个虚拟机上 I/O 流量过多会导致同步完成之前超时。这可能是因为流量过大的原因。例如，将日志记录级别设置为“琐事”模式就可能生成过大的 I/O 流量。

### 解决方案

1 登录 Site Recovery Manager Server 主机。

2 在文本编辑器中打开 vmware-dr.xml 文件。

您将在 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config 文件夹中找到 vmware-dr.xml 文件。

3 向 vmware-dr.xml 文件中添加一个 <topology><drTaskCleanupTime> 元素。

您可以将 <topology> 元素添加到 <Config> 标记中的任何顶级位置。将 <drTaskCleanupTime> 的值至少设置为 300 秒。如果您将日志记录级别设置为“琐事”，请将 <drTaskCleanupTime> 设置为 1000 秒。

```
<topology>
<drTaskCleanupTime>1000</drTaskCleanupTime>
</topology>
```

4 保存并关闭 vmware-dr.xml 文件。

5 重新启动 Site Recovery Manager Server 服务以应用新的设置。

## 重新启动 vCenter Server 之后重新保护失败

重新启动 vCenter Server 之后，如果使用 vSphere Replication，则重新保护操作有时会失败。

### 问题

重新启动 vCenter Server 之后，如果使用 vSphere Replication，则重新保护操作将失败，并显示错误：

错误 - 无法撤销复制

虚拟机“virtual\_machine”。会话未进行身份验证 (Error - Unable to reverse replication for the virtual machine 'virtual\_machine'. The session is not authenticated)。

## 原因

在 vCenter Server 重新启动后，它无法刷新 Site Recovery Manager 用于与 vSphere Replication 进行通信的某些会话，并导致重新保护失败。

## 解决方案

在这两个站点上重新启动 Site Recovery Manager 服务。

# 重新扫描数据存储因存储设备未就绪失败

启动测试恢复或恢复时，某些 SRA 在恢复站点上提升的存储设备对 ESXi 主机可用之前向 Site Recovery Manager 发送响应。Site Recovery Manager 将重新扫描存储设备，但重新扫描失败。

## 问题

如果存储设备尚未完全可用，ESXi Server 将不检测这些设备，Site Recovery Manager 在执行重新扫描时将不查找已复制的设备。这会导致出现多种问题。

- 此时将不创建数据存储，并且找不到已恢复的虚拟机。
- ESXi 主机将对 vCenter Server 检测信号无响应，并断开与 vCenter Server 的连接。如果发生这种情况，vCenter Server 将向 Site Recovery Manager 发送一条错误，测试恢复或实际恢复失败。
- ESXi 主机可用，但重新扫描和磁盘重新签名将超出 Site Recovery Manager 或 vCenter Server 的超时时间，导致出现 Site Recovery Manager 错误。

## 原因

Site Recovery Manager 启动重新扫描时存储设备未就绪。

## 解决方案

要延迟启动存储重新扫描直至存储设备在 ESXi 主机上可用，请将 `storageProvider.hostRescanDelaySec` 设置增加到 20 到 180 秒之间的值。请参见[更改存储提供程序设置](#)。

---

**注** 在 Site Recovery Manager 5.1 及早期版本中，您可能已使用 `storageProvider.hostRescanRepeatCnt` 参数在恢复中引入延迟。请改为使用 `storageProvider.hostRescanDelaySec` 参数。

---