Site Recovery Manager 管理

Site Recovery Manager 8.2

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

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

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

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

关于 VMware Site Recovery Manager 管理 8

更新信息 9

1 Site Recovery Manager 特权、角色和权限 10

Site Recovery Manager 如何处理权限 11

Site Recovery Manager 和 vCenter Server 管理员角色 12

Site Recovery Manager 和 vSphere Replication 角色 12

管理共享恢复站点配置中的权限 12

分配 Site Recovery Manager 角色和权限 14

Site Recovery Manager 角色参考 16

2 复制虚拟机 20

将基于阵列的复制与 Site Recovery Manager 结合使用 20

配置基于阵列的复制 21

将 vSphere Replication 与 Site Recovery Manager 结合使用 27

复制虚拟机并启用多个时间点实例 28

将基于阵列的复制和 vSphere Replication 与 Site Recovery Manager 结合使用 28

3 配置映射 30

适用于基于阵列的复制保护组和 vSphere Replication 保护组的清单映射 31

存储策略保护组的清单映射 31

配置临时占位映射 33

用户在配置临时占位映射后获得虚拟机访问权限 34

配置清单映射 35

关于存储策略映射 36

选择存储策略映射 37

4 关于占位虚拟机 38

恢复过程对占位虚拟机的影响 39

选择占位数据存储 40

5 创建和管理保护组 41

关于基于阵列的复制保护组和数据存储组 42

Site Recovery Manager 如何计算数据存储组 42

vSphere Replication 保护组 43

关于存储策略保护组 44

存储策略保护组的必备条件 45
存储策略保护组的限制 46
存储策略保护组和非受保护虚拟机 48
保护加密的虚拟机 48
保护组状态概述 49
虚拟机保护状态概述 50
创建保护组 51
创建 vSphere Replication 保护组 52
创建存储策略保护组 53
创建基于阵列的复制保护组 54
通过文件夹对保护组进行组织 55
在保护组中添加和移除数据存储组或虚拟机 55
将清单映射应用于基于阵列的保护组或 vSphere Replication 保护组的所有成员 56
为基于阵列的保护组或 vSphere Replication 保护组中的单个虚拟机配置清单映射 57
修改基于阵列的保护组或 vSphere Replication 保护组中虚拟机的设置 58
移除虚拟机的保护 59
移除虚拟机的保护 59

6 创建、测试和运行恢复计划 61
测试恢复计划 62
测试网络和数据中心网络 62
通过运行恢复计划执行计划内迁移或灾难恢复 63
使用强制恢复来运行恢复 64
测试恢复计划和运行恢复计划之间的差异 65
跨恢复站点上的多个主机执行虚拟机的测试恢复 66
创建、测试和运行恢复计划 66
创建恢复计划 67
通过文件夹对恢复计划进行组织 67
编辑恢复计划 68
测试恢复计划 68
测试恢复计划后清理 69
运行恢复计划 69
恢复虚拟机的时间点快照 71
取消测试或恢复 71
禁用存储策略保护组中虚拟机的恢复 72
禁用存储策略保护组中一致性组的恢复 72
导出恢复计划步骤 73
查看和导出恢复计划历史记录报告 73
删除恢复计划 74
恢复计划状态概述 75

7 配置恢复计划 78
恢复计划步骤 78
创建自定义恢复步骤 79
自定义恢复步骤的类型 80
Site Recovery Manager 如何处理自定义恢复步骤故障 81
写入命令步骤的准则 81
命令步骤的环境变量 82
创建顶级消息提示或命令步骤 84
为单个虚拟机创建消息提示或命令步骤 85
运行恢复计划时挂起虚拟机 86
指定虚拟机的恢复优先级 86
配置虚拟机依赖关系 87
对计划的迁移启用 vSphere vMotion 88
配置虚拟机启动和关机选项 89
保护和恢复虚拟机的限制 90

8 自定义虚拟机的 IP 属性 92
手动自定义单个虚拟机的 IP 属性 93
将 IP 自定义规则应用到虚拟机 94
自定义多个虚拟机的 IP 属性 95
使用 DR IP Customizer 工具自定义多个虚拟机的 IP 属性 95
通过定义 IP 自定义规则自定义多台虚拟机的 IP 属性 113

9 恢复后重新保护虚拟机 114
Site Recovery Manager 如何使用基于阵列的复制重新保护虚拟机 116
Site Recovery Manager 如何利用 vSphere Replication 重新保护虚拟机 116
Site Recovery Manager 如何使用存储策略保护来重新保护虚拟机 116
执行重新保护的前提条件 117
重新保护虚拟机 118
重新保护状态概述 118

10 通过执行故障恢复来还原恢复前的站点配置 120
执行故障恢复 121

11 Site Recovery Manager 与其他软件的互操作性 123
Site Recovery Manager 和 vCenter Server 124
让 Site Recovery Manager 与 VMware vSAN 存储和 vSphere Replication 协同工作 125
Site Recovery Manager 如何在恢复期间与 DPM 和 DRS 交互 125
Site Recovery Manager 如何与 Storage DRS 或 Storage vMotion 交互 126
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 126

在使用 Storage DRS 或 Storage vMotion 的站点上将 Site Recovery Manager 与 vSphere Replication 结合使用 127
Site Recovery Manager 与 vSphere High Availability 进行交互的方式 128
Site Recovery Manager 如何与延伸存储交互 128
将 Site Recovery Manager 与 NSX Data Center for vSphere 结合使用 130
Site Recovery Manager 和 vSphere PowerCLI 130
Site Recovery Manager 和虚拟机加密 130
Site Recovery Manager 和 vRealize Orchestrator 131
保护 Microsoft 群集服务器和容错虚拟机 131
结合使用 Site Recovery Manager 与 SIOC 数据存储 133
将 Site Recovery Manager 与接入控制群集结合使用 133
Site Recovery Manager 和附加到 RDM 磁盘设备的虚拟机 134
Site Recovery Manager 和 Active Directory 域控制器 134

12 高级 Site Recovery Manager 配置 135
重新配置 Site Recovery Manager 设置 135
更改连接设置 135
更改 Site Recovery Manager 历史记录报告收集设置 136
更改本地站点设置 137
更改日志记录设置 137
更改恢复设置 140
更改远程管理器设置 143
更改远程站点设置 144
更改复制设置 144
更改 SSO 设置 145
更改存储器设置 145
更改 ABR 存储策略设置 147
更改存储提供程序设置 147
更改 vSphere Replication 设置 149
更改遥测设置 150
修改设置以运行大型 Site Recovery Manager 环境 151
大型 Site Recovery Manager 环境的设置 152

13 Site Recovery Manager 事件和警报 155
Site Recovery Manager 如何监控站点间的连接 155
创建 Site Recovery Manager 警报 155
Site Recovery Manager 事件参考 156

14 收集 Site Recovery Manager 日志文件 165
通过使用 Site Recovery Manager 界面收集 Site Recovery Manager 日志文件 165
手动收集 Site Recovery Manager 日志文件 166

更改 Site Recovery Manager Server 日志文件的大小和数目 166
配置 Site Recovery Manager 核心转储 168

15 Site Recovery Manager 故障排除 170
在恢复站点上同时打开多个虚拟机的电源会导致错误 170
向保护组添加虚拟机失败，并显示无法解析设备的错误 171
配置保护失败并显示占位虚拟机创建错误 171
快速删除和重新创建占位虚拟机失败 172
由于主机处于错误的状态，因此计划的迁移失败 172
计划的迁移由于存储策略保护组同步不成功而失败 173
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 173
恢复失败，并显示主机和数据存储不可用错误 174
重新保护失败，并显示 vSphere Replication 超时错误 175
等待 VMware Tools 时恢复计划超时 175
vSphere Replication 保护组同步失败 176
重新扫描数据存储因存储设备未就绪失败 177
计划的迁移期间恢复在执行到 36% 时停止 177
恢复失败，并显示有关非复制配置文件的错误 178
恢复因用户权限受限而失败 178
恢复因不支持结合使用 VMware Tools 与 ESXi 而失败 179

关于 VMware Site Recovery Manager 管理

VMware Site Recovery Manager 是 VMware vCenter Server 的扩展，提供了业务连续性和灾难恢复解决方案，可帮助您计划、测试和运行 vCenter Server 虚拟机恢复。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。

目标受众

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。

更新信息

本《Site Recovery Manager 8.2 管理指南》随产品的每个版本一起更新或在必要时进行更新。

下表列出了《Site Recovery Manager 8.2 管理指南》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。
2019 年 8 月 14 日	■ 添加了的新主题 Site Recovery Manager 和虚拟机加密。 ■ 更新了主题“DR IP Customizer 工具的语法”中的信息。 ■ 更新了主题“运行 DR IP Customizer 自定义多个虚拟机的 IP 属性”中的信息。
2019 年 5 月 09 日	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，以使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

  可以在 Site Recovery Manager 上配置权限以使用共享恢复站点。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 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 管理员才能登录到 Site Recovery Manager，除非这些管理员将访问权限明确授予其他用户。

- 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。Site Recovery Manager 可以使用您在连接受保护站点和恢复站点时提供的用户凭据来执行操作。

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

可以在 Site Recovery Manager 上配置权限以使用共享恢复站点。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。
- 为防止不必要的权限在不同组织的资源之间传播，请勿在共享恢复站点上的 vCenter Server 的根文件夹、数据中心和主机上传播权限。

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，所有用户都可以查看在共享的主机、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 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 管理员才能登录到 Site Recovery Manager，除非这些管理员将访问权限明确授予其他用户。

要允许其他用户访问 Site Recovery Manager，vCenter Server 管理员必须在 Site Recovery Manager 用户界面中授予这些用户相应的权限。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 对象和 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。连接受保护站点和恢复站点后，可以在这两个站点上的同一 Site Recovery Manager 用户界面中更改 Site Recovery Manager 权限。

Site Recovery Manager 扩充了 vCenter Server 角色和权限，为其添加了可对 Site Recovery Manager 特定任务和操作进行精细控制的权限。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。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**权限**，选择一个站点，然后单击**添加**。

a 从**域**下拉菜单中，选择包含用户或组的域。

b 从**用户/组**列表中搜索特定的用户/组，然后选择该用户/组。

默认情况下，vCenter Single Sign-On 最多返回 5000 行，分为两部分显示。一部分显示用户，另一部分显示解决方案用户和组。可以从 vCenter Server 高级设置中更改该设置。

c 从**角色**下拉菜单中选择要分配给用户或用户组的角色。

角色下拉菜单中包含 vCenter Server 及其插件提供的所有角色。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 **SRM 管理员**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 **SRM 保护组管理员**角色。
允许用户或用户组执行恢复和测试恢复。	分配 **SRM 恢复管理员**角色。
允许用户或用户组创建、修改和测试恢复计划。	分配 **SRM 恢复计划管理员**角色。
允许用户或用户组测试恢复计划。	分配 **SRM 恢复测试管理员**角色。

4 选择**传播到子项**，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。

5 单击**添加**将角色及其关联的特权分配给用户或用户组。

6 重复步骤 3 到步骤 5，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

您已将给定的 Site Recovery Manager 角色分配给用户或用户组。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。如果不属于 vCenter Server 管理员的用户需要具有多个 Site Recovery Manager 角色的特权，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	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。 ■ 配置高级设置。 ■ 配置连接。 ■ 配置清单首选项。 ■ 配置占位数据存储。 ■ 配置阵列管理器。 ■ 管理保护组。 ■ 管理恢复计划。 ■ 运行恢复计划。 ■ 执行重新保护操作。 ■ 配置虚拟机的保护。 ■ 编辑保护组。 ■ 移除保护组。 ■ 查看存储策略对象。 Site Recovery Manager 管理员用户无法编辑继承的权限。要限制特定用户的访问权限或将访问权限授予用户，Site Recovery Manager 管理员必须添加新角色。	**Site Recovery Manager.高级设置.修改** **Site Recovery Manager.阵列管理器.配置** **Site Recovery Manager.诊断.导出** **Site Recovery Manager.内部.内部访问** **Site Recovery Manager.清单首选项.修改** **Site Recovery Manager.占位数据存储.配置** **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.删除历史记录** **Site Recovery Manager.恢复历史记录.查看删除的计划** **Site Recovery Manager.恢复计划.配置命令** **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.恢复** **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** **Site Recovery Manager.配置文件驱动的存储.配置文件驱动的存储视图**	■ 虚拟机 ■ 数据存储 ■ vCenter Server 文件夹 ■ 资源池 ■ Site Recovery Manager 服务实例 ■ 网络 ■ Site Recovery Manager 文件夹 ■ 保护组 ■ 恢复计划 ■ 阵列管理器
Site Recovery Manager 保护组管理员	Site Recovery Manager 保护组管理员角色允许用户管理保护组。 ■ 创建保护组。 ■ 修改保护组。 ■ 将虚拟机添加到保护组。 ■ 删除保护组。 ■ 配置虚拟机的保护。 ■ 删除虚拟机的保护。 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。	**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**	■ Site Recovery Manager 文件夹 ■ 保护组

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	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。 ■ 从恢复计划中删除保护组。 ■ 测试恢复计划。 ■ 运行恢复计划。 ■ 运行重新保护操作。 ■ 在虚拟机上配置自定义命令步骤。 ■ 查看删除的恢复计划。 ■ 编辑虚拟机恢复属性。 具有此角色的用户无法配置虚拟机保护，也无法创建或移除恢复计划。	**Site Recovery Manager.保护组.从计划移除** **Site Recovery Manager.恢复计划.修改** **Site Recovery Manager.恢复计划.测试** **Site Recovery Manager.恢复计划.恢复** **Site Recovery Manager.恢复计划.重新保护** **Site Recovery Manager.恢复计划.配置命令** **Site Recovery Manager.恢复历史记录.查看删除的计划**	■ 保护组 ■ 恢复计划 ■ Site Recovery Manager 服务实例
Site Recovery Manager 恢复计划管理员	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。 ■ 将保护组添加到恢复计划。 ■ 从恢复计划中删除保护组。 ■ 在虚拟机上配置自定义命令步骤。 ■ 创建恢复计划。 ■ 测试恢复计划。 ■ 取消恢复计划测试。 ■ 编辑虚拟机恢复属性。 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。	**Site Recovery Manager.保护组.分配给计划** **Site Recovery Manager.保护组.从计划移除** **Site Recovery Manager.恢复计划.配置命令** **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.测试** **资源.恢复使用**	■ 保护组 ■ 恢复计划 ■ vCenter Server 文件夹 ■ 数据存储 ■ 资源池 ■ 网络

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 测试管理员	Site Recovery Manager 测试管理员角色仅允许用户测试恢复计划。 ■ 测试恢复计划。 ■ 取消恢复计划测试。 ■ 编辑虚拟机恢复属性。 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。	**Site Recovery Manager.恢复计划.修改** **Site Recovery Manager.恢复计划.测试**	■ 恢复计划
Site Recovery Manager 远程用户	Site Recovery Manager 远程用户角色授予用户进行跨站点 Site Recovery Manager 操作所需的一组最低特权。	**数据存储.浏览数据存储** **数据存储.低级别文件操作** **数据存储.更新虚拟机文件** **数据存储.更新虚拟机元数据** **主机.vSphere Replication.管理复制** **虚拟机.快照管理.移除快照** **虚拟机.vSphere Replication.配置复制** **虚拟机.vSphere Replication.管理复制** **虚拟机.vSphere Replication.监控复制**	■ 虚拟机 ■ 数据存储

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文件。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。

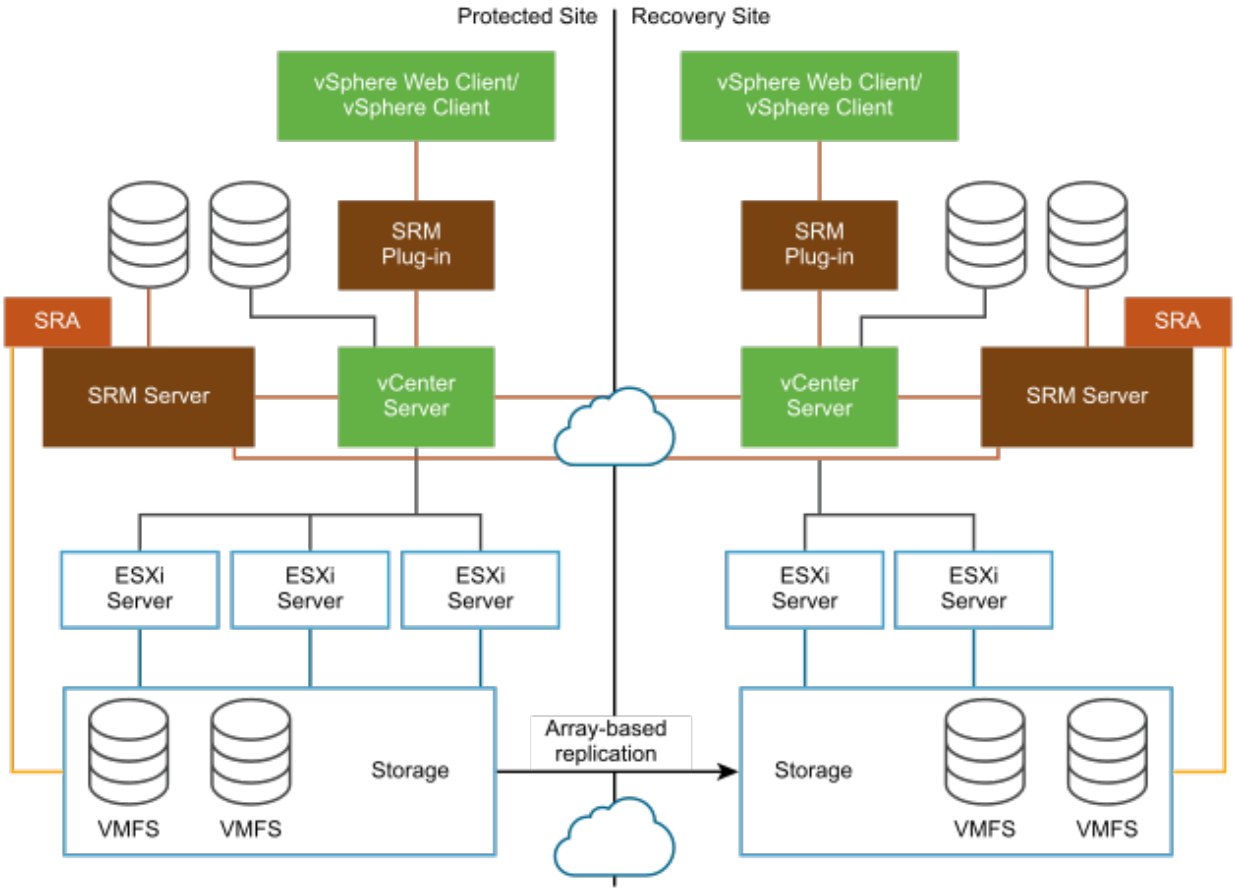
可以保护包含使用 VMware vSphere Flash Read Cache 存储的磁盘的虚拟机。由于可能未针对 Flash Read Cache 配置虚拟机恢复，Site Recovery Manager 会在恢复站点上启动虚拟机时禁用磁盘上的 Flash Read Cache。Site Recovery Manager 将预留设置为零。在配置为使用 vSphere Flash Read Cache 的虚拟机上执行恢复之前，请通过 vSphere Web Client 记录虚拟机的缓存预留信息。恢复后，可以将虚拟机迁移到具有 Flash Read Cache 存储的主机，并手动还原虚拟机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

如果要使用存储策略保护组来保护虚拟机，则必须使用基于阵列的复制来复制这些虚拟机。

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进行复制的虚拟机（包括使用存储策略保护组保护的虚拟机），您必须在每个站点上配置存储复制适配器 (SRA)。

安装存储复制适配器

如果您使用基于阵列的复制保护虚拟机或结合使用基于阵列的复制和存储策略保护来保护虚拟机，则必须针对用于 Site Recovery Manager 的每个存储阵列安装特定的存储复制适配器 (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 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 Client 中，单击 **Site Recovery > 打开 Site Recovery**，选择站点对，然后单击**查看详细信息**。
3. 在**站点对**选项卡中，转到**配置 > 基于阵列的复制 > 存储复制适配器**，然后单击**重新扫描适配器**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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在“站点对”选项卡上，单击**配置 > 基于阵列的复制 > 阵列对**。

4 单击**添加**按钮以添加阵列管理器。

5 选择要让 Site Recovery Manager 使用的存储复制适配器，然后单击**下一步**。

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 输入本地阵列管理器的名称，提供所选 SRA 类型的必要信息，然后单击**下一步**。

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。

有关如何在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。

7 （可选） 如果不希望创建阵列对，请选中**请勿立即创建远程阵列管理器**复选框，然后单击**完成**。

8 输入远程阵列管理器的名称，提供所选 SRA 类型的必要信息，然后单击**下一步**。

9 在**阵列对**页面上，选择要启用的阵列对，然后单击**下一步**。

10 查看配置，然后单击**完成**。

将存储复制适配器添加到 Site Recovery Manager Appliance

如果计划对基于阵列的复制使用 Site Recovery Manager，则必须将存储复制适配器 (SRA) 添加到 Site Recovery Manager Server。SRA 文件以 `.tar.gz` 存档的形式分发。

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。

前提条件

- 下载 SRA。转至 https://my.vmware.com/web/vmware/downloads，选择 **VMware 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，请确认已针对您使用的 Site Recovery Manager 版本对其进行认证。请参见 Site Recovery Manager 的《VMware 兼容性指南》，网址为 http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra。
- 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 以管理员身份登录到 Site Recovery Manager Appliance 管理界面。

2 在 Site Recovery Manager Appliance 管理界面中，单击**存储复制适配器**，然后单击**新建适配器**。

3 单击**上载**，导航到保存 SRA 文件的目录，然后选择该文件。

4 完成后，单击**关闭**。

Site Recovery Manager Appliance 管理界面中将显示“存储复制适配器”卡视图。

5 登录到 vSphere Client 或 vSphere Web Client。

6 单击 **Site Recovery > 打开 Site Recovery**，选择站点对，然后单击**查看详细信息**。

7 在**站点对**选项卡中，转到**配置 > 基于阵列的复制 > 存储复制适配器**，然后单击**重新扫描适配器**按钮。

下载并上载存储复制适配器的配置存档

如果将 Site Recovery Manager Appliance 与基于阵列的复制配合使用，并且需要替换存储复制适配器 (SRA)，则可以下载此 SRA 的配置存档，然后将配置导入替换项 SRA。

前提条件

要下载 SRA 配置文件并将其导入另一个 SRA，必须使用从同一供应商获取的 SRA。

步骤

1 以管理员身份登录到 Site Recovery Manager Appliance 管理界面。

2 单击**存储复制适配器**选项卡。

3 选择相应的“存储复制适配器”卡视图，然后单击下拉菜单 (⋮)。

选项	描述
下载配置存档	下载所选 SRA 的配置存档。
上载配置存档	导入所选 SRA 的配置。 a 导航到保存 SRA 配置存档文件的目录，然后选择该文件。配置文件以 `.tar.gz` 存档的形式分发。 b 单击**打开**。

删除存储复制适配器

可以使用 Site Recovery Manager Appliance 管理界面从 Site Recovery Manager Server 中删除存储复制适配器 (SRA)。

注 如果删除 SRA，则当前正在运行的涉及此适配器所控制存储阵列的任何操作都会中断，包括但不限于恢复、测试、清理、重新保护操作。

步骤

1 以管理员身份登录到 Site Recovery Manager Appliance 管理界面。

2 在 Site Recovery Manager Appliance 管理界面中，单击**存储复制适配器**。

3 选择相应的“存储复制适配器”卡视图，然后从下拉菜单 (⋮) 中单击**删除**。

4 确认您已了解删除适配器的后果并单击**删除**。

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。

通过配置阵列管理器，Site Recovery Manager 可根据它发现的一组复制的存储设备来计算数据存储组。如果更改任一站点上的阵列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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在“站点对”选项卡上，单击**配置 > 基于阵列的复制 > 阵列对**。

4 选择一个阵列对，然后单击**阵列管理器对 > 发现阵列对**以重新扫描阵列，或单击**发现设备**以重新计算存储设备和一致性组。

选择阵列对时，**阵列对**选项卡会提供有关阵列中所有存储设备的详细信息，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。

编辑阵列管理器

使用“编辑本地阵列管理器”向导或“编辑远程阵列管理器”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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在“站点对”选项卡上，单击**配置 > 基于阵列的复制 > 阵列对**。

4 选择一个阵列对，单击**阵列管理器对**，然后单击**编辑本地阵列管理器**或**编辑远程阵列管理器**。

5 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。

6 修改适配器信息。

这些字段由 SRA 创建。

7 单击**保存**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，请仅在绝对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。群集中的所有主机都必须能够访问该非复制数据存储，否则 vMotion 将无法运行。

步骤

1. 在 vSphere Client 中，选择**主机和群集**，选择一个主机，然后单击**配置**。
2. 在**虚拟机**下，选择**交换文件位置**，然后单击**编辑**。
3. 选择**使用特定数据存储**，然后选择一个非复制数据存储。
4. 单击**确定**。
5. 关闭该主机上所有虚拟机的电源后再打开。

   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。

灾难恢复期间隔离延伸存储的设备

在延伸存储的灾难恢复中，故障切换命令必须隔离恢复站点中的设备。

启动灾难恢复时，如果受保护站点中的某些主机仍处于运行状态并继续运行虚拟机，由于文件已锁定，Site Recovery Manager 将无法打开恢复站点中相应虚拟机的电源。如果存储阵列隔离了恢复站点中的设备，恢复站点中的 ESX 主机可以断开必需锁定并打开虚拟机的电源。

Site Recovery Manager 必须在故障切换 SRA 命令中为受保护站点中尚未取消激活的延伸设备使用 `isolation="true"`。

如果恢复站点的同一设备上存在正在运行的虚拟机，并且恢复站点 ESXi 挂载了受保护站点的存储，则在隔离期间存在写入失败的风险。建议在受保护站点上运行延伸存储上的所有虚拟机。

适用于延伸存储的隔离实施详细信息因阵列供应商而异。某些阵列供应商在运行隔离的故障切换 SRA 命令后，可能会导致受保护站点中的设备无法访问。某些阵列供应商可能会针对特定设备断开源站点和目标站点之间的通信。

将 vSphere Replication 与 Site Recovery Manager 结合使用

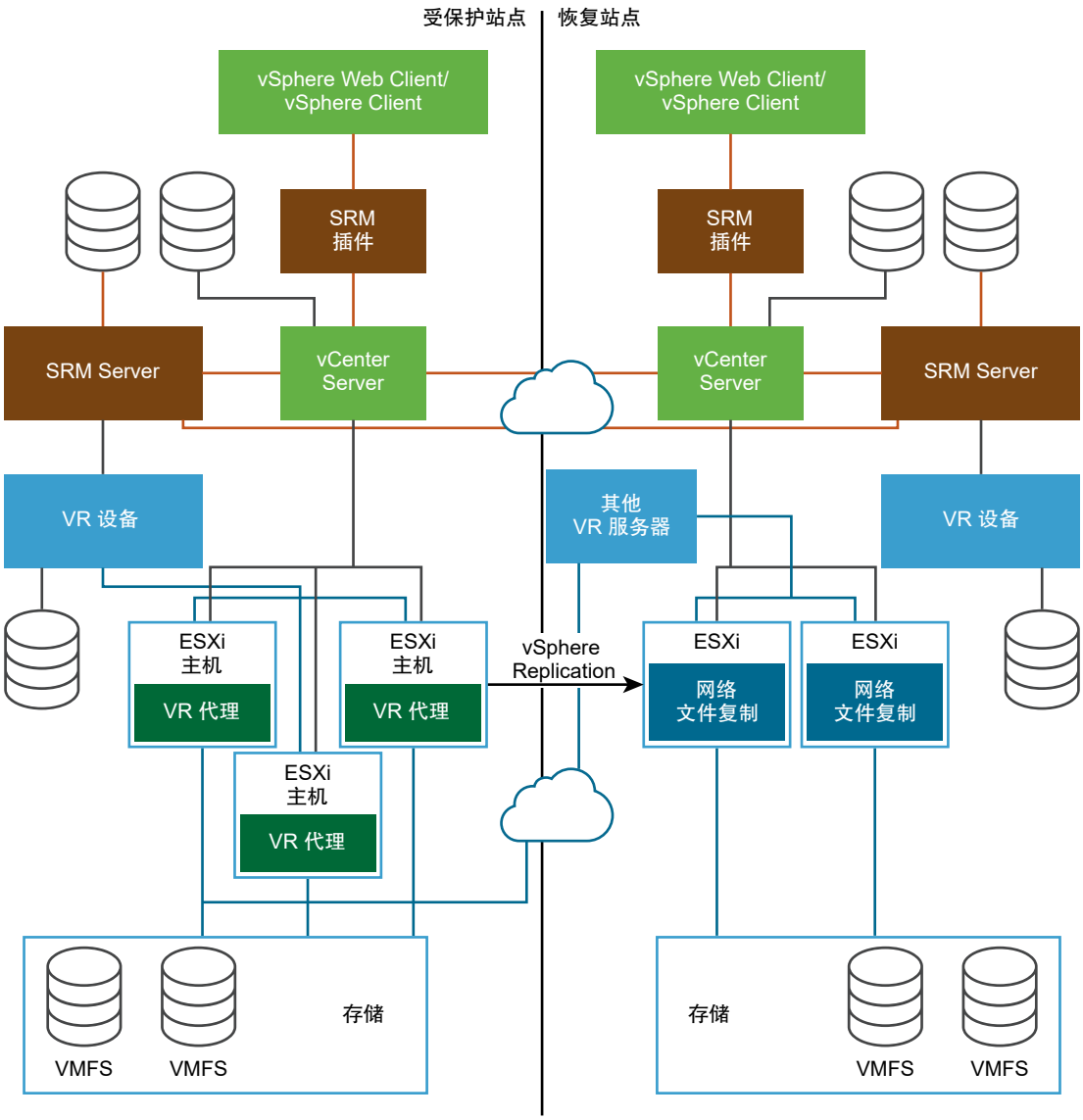
Site Recovery Manager 可使用 vSphere Replication 将数据复制到恢复站点中的服务器。

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



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。

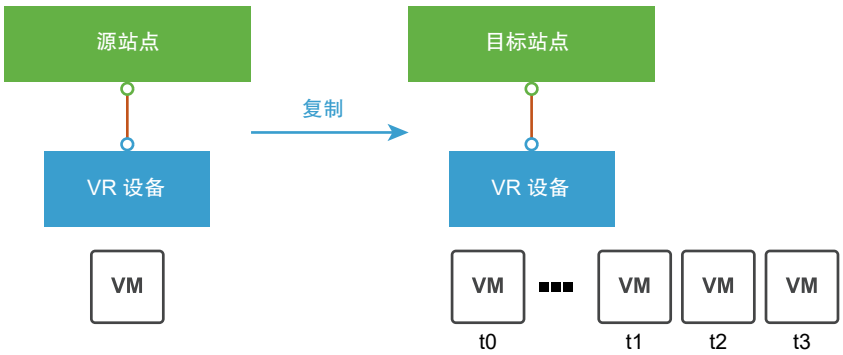
配置虚拟机的复制时，可以在“配置复制”向导的恢复设置中启用多个时间点 (MPIT) 实例。vSphere Replication 根据您指定的保留策略在目标站点上保留虚拟机的多个快照实例。vSphere Replication 最多支持 24 个快照实例。恢复虚拟机后，您可以将其恢复到特定快照。

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。

还可以使用 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



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。

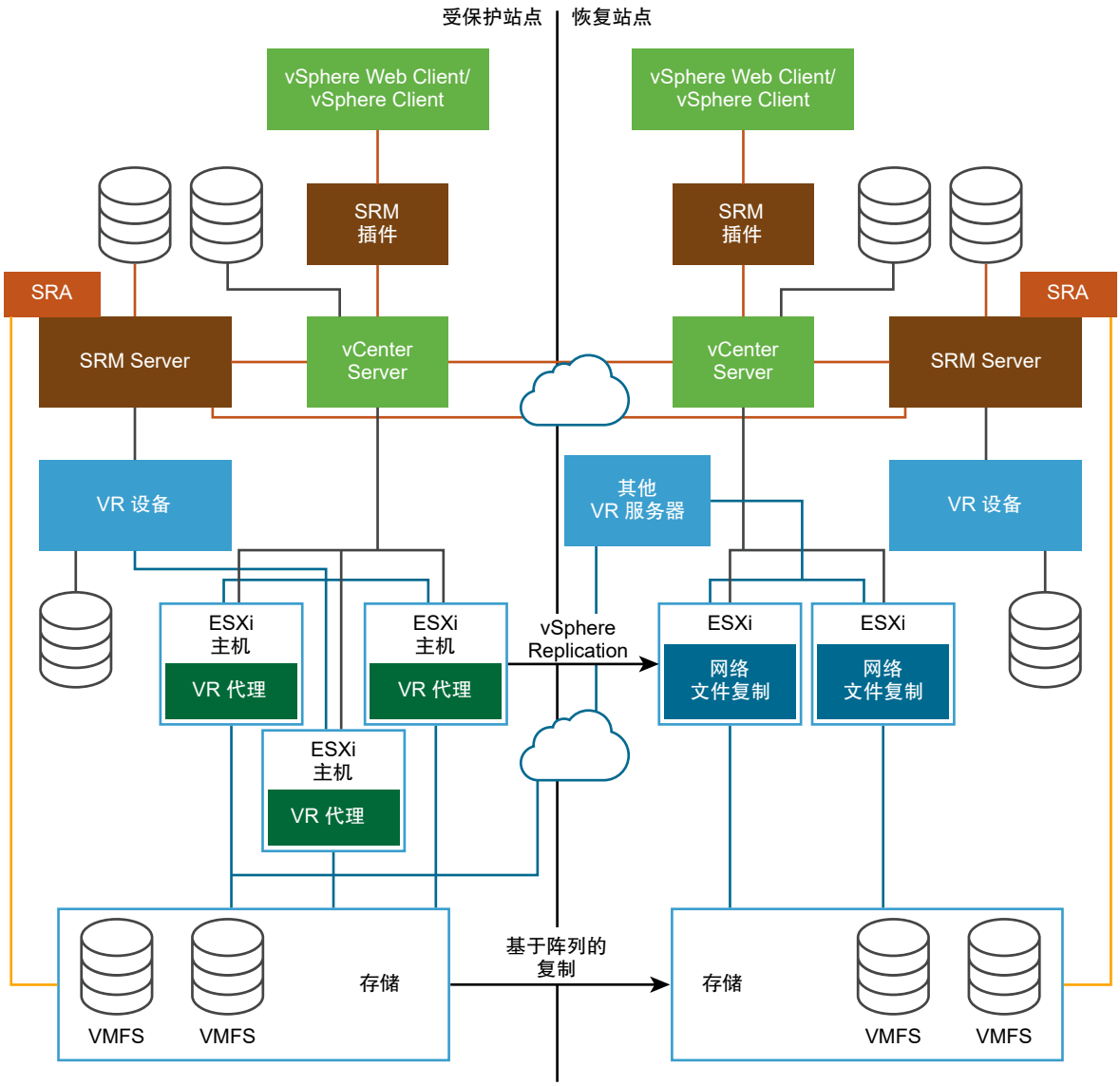
要创建使用基于阵列的复制和 vSphere Replication 的混合 Site Recovery Manager 部署，必须为这两种类型的复制配置受保护站点和恢复站点。

- 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



配置映射

3

通过映射，您可以指定 Site Recovery Manager 如何将受保护站点上的虚拟机资源映射到恢复站点上的资源。

您可以配置站点范围的映射，将受保护站点上 vCenter Server 清单中的对象映射到恢复站点上 vCenter Server 清单中的相应对象。

- 网络，包括指定其他网络以用于恢复计划测试的选项
- 数据中心或虚拟机文件夹
- 计算资源，包括资源池、独立主机、vApp 或群集

在恢复过程中，当虚拟机在恢复站点上启动时，这些虚拟机会使用您在映射中指定的恢复站点上的资源。要启用双向保护和重新保护，您可以配置反向映射，以便将恢复站点上的对象映射回其在受保护站点上的对应对象。您也可以反向配置其他映射，以便某个站点上的已恢复虚拟机针对该站点上的受保护虚拟机使用其他资源。

根据您使用的是基于阵列的保护组和 vSphere Replication 保护组，还是存储策略保护组，Site Recovery Manager 应用清单映射的方式有所不同。有关 Site Recovery Manager 如何将清单映射应用于不同类型保护组之间差别的信息，请参见适用于基于阵列的复制保护组和 vSphere Replication 保护组的清单映射和存储策略保护组的清单映射 。

如果使用的是存储策略保护组，除了映射清单对象之外，还要将受保护站点上的存储策略映射到恢复站点上的存储策略。

本章讨论了以下主题：

- 适用于基于阵列的复制保护组和 vSphere Replication 保护组的清单映射
- 存储策略保护组的清单映射
- 配置清单映射
- 关于存储策略映射
- 选择存储策略映射

适用于基于阵列的复制保护组和 vSphere Replication 保护组的清单映射

对于基于阵列的保护和 vSphere Replication 保护，Site Recovery Manager 会在您创建保护组时将清单映射应用于组中的所有虚拟机。

创建基于阵列的保护组或 vSphere Replication 保护组时，Site Recovery Manager 将创建占位虚拟机。Site Recovery Manager 从站点范围的清单映射中为占位虚拟机派生资源分配。

如果配置站点范围的清单映射，无论何时都可以将清单映射重新应用于保护组（例如将新的虚拟机添加到现有保护组时）。

如果更改某个站点的站点范围的清单映射，此更改不会影响现有保护组中 Site Recovery Manager 已保护的虚拟机。如果在虚拟机上重新配置保护，Site Recovery Manager 只会将新映射应用到之前受保的护虚拟机。

除非虚拟机具有有效清单映射，否则 Site Recovery Manager 无法保护虚拟机。但是，对于基于阵列的复制保护组和 vSphere Replication 保护组，不会强制要求配置站点范围的清单映射。如果创建了基于阵列的复制保护组或 vSphere Replication 保护组而未定义站点范围的清单映射，则可以单独配置组中的每个虚拟机。可以通过在保护组中配置虚拟机保护来替代站点范围的清单映射。也可以在创建保护组后创建站点范围的清单映射，然后将这些站点范围的映射应用到该保护组。

- 有关配置站点范围的清单映射的信息，请参见配置清单映射。
- 有关在虚拟机上单独配置映射的信息，请参见为基于阵列的保护组或 vSphere Replication 保护组中的单个虚拟机配置清单映射。
- 有关将站点范围的清单映射应用到现有保护组的信息，请参见将清单映射应用于基于阵列的保护组或 vSphere Replication 保护组的所有成员。

由于占位虚拟机不支持网卡，因此您无法更改占位虚拟机的网络配置。您仅可在清单映射中更改占位虚拟机的网络。如果不存在网络的映射，则可以在配置单个虚拟机的保护时指定一个网络。对占位虚拟机的更改会替代在配置虚拟机的保护时建立的设置。在测试和恢复过程中，Site Recovery Manager 会在恢复站点保留这些更改。

存储策略保护组的清单映射

对于存储策略保护，Site Recovery Manager 会在您运行包含存储策略保护组的恢复计划时，将清单映射应用到虚拟机。

使用基于阵列的保护组和 vSphere Replication 保护组时，Site Recovery Manager 会在您配置虚拟机保护时应用清单映射。使用存储策略保护组时，由于存储策略保护是动态的，因此 Site Recovery Manager 只会在您运行恢复计划时应用清单映射。运行恢复计划时会根据清单映射确定虚拟机放置位置，因此 Site Recovery Manager 不会在恢复站点上创建占位虚拟机。

由于 Site Recovery Manager 在运行恢复计划时会针对存储策略保护组应用清单映射，因此无法在存储策略保护组中的虚拟机上单独配置映射。运行存储策略保护的恢复时，Site Recovery Manager 始终使用站点范围的清单映射。如果缺少清单映射，包含存储策略保护组的恢复计划的测试恢复、计划迁移和灾难恢复将失败。可以将 Site Recovery Manager 配置为定期轮询存储策略保护组中的虚拟机以查找缺少的映射，并在缺少任何可能导致存储策略保护组恢复失败的映射时报告警告。有关如何配置定期轮询以查找缺少的映射的信息，请参见更改复制设置。

注 如果在缺少网络映射但其他映射都存在的情况下运行测试恢复，Site Recovery Manager 会使用自动生成的测试网络，测试将成功但显示警告。如果测试恢复成功但显示缺少网络映射的警告，请配置网络映射并再次运行测试。计划迁移和灾难恢复不使用测试网络，如果缺少网络映射，计划迁移和灾难恢复将失败。

如果恢复计划因缺少映射而失败且受保护站点可用，请配置缺少的映射并再次运行计划。有关如何配置站点范围的清单映射的信息，请参见配置清单映射。

资源清单映射和存储策略保护组

鉴于虚拟机保护的动态性，存储策略保护组在如何设置资源清单映射方面具有特定的要求和限制。

- Site Recovery Manager 要求保护站点上已挂载受存储策略保护组保护的数据存储的所有顶级计算资源（群集或非受管主机）具有现有资源清单映射。
- Site Recovery Manager 根据顶级计算资源映射确定已恢复数据存储的所需可见性，且不考虑资源池的资源映射。
  - 如果资源池的父顶级计算资源不存在资源映射，则 Site Recovery Manager 无法应用该资源池的现有映射。
  - 如果保护站点资源池的某现有映射映射到与其父项不同的恢复计算资源层次结构，则不会向映射的计算资源显示该资源池下的虚拟机的存储。

为确保存储策略保护组恢复成功，必须在创建资源映射时遵循以下规则。

- 为已挂载受存储策略保护组保护的数据存储的所有受保护的顶级计算资源（群集或非受管主机）创建资源映射。
- 如果必须为资源池创建其他映射，请将其映射到其父顶级受保护计算资源所映射到的同一顶级恢复计算资源下的一个目标。例如，如果受保护主机或群集 P 映射到恢复主机或群集 R，或者 R 下的恢复资源池，则 P 下的所有受保护资源池也必须映射到 R 或 R 下的恢复资源池。

存储策略保护的临时占位映射

运行恢复计划时，Site Recovery Manager 会针对存储策略保护应用清单映射。如果运行包含存储策略保护组的恢复计划且尚未配置清单映射，或映射的对象丢失，则测试恢复、计划迁移和灾难恢复将失败。

通常只有受保护站点和恢复站点同时可用时，才能配置清单映射。如果包含存储策略保护组的恢复计划因缺少映射而失败且受保护站点不可用，则您无法以正常方式配置缺少的映射。为了解决此问题，当恢复计划因缺少映射而失败且受保护站点不可用时，Site Recovery Manager 会创建临时占位映射。临时占位映射允许您配置缺少的映射，以便在受保护站点脱机时可以成功运行恢复。临时占位映射是不完整的映射，可标识受保护站点上包含恢复计划中的虚拟机的清单对象。临时占位映射在恢复站点上不包含目标对象。恢复因缺少映射而失败且受保护站点不可用时，Site Recovery Manager 会创建临时占位映射，您可以完成临时占位映射并成功重新运行恢复。

有关如何配置临时占位映射的信息，请参见配置临时占位映射。

配置临时占位映射

如果包含存储策略保护组的恢复计划因缺少映射而失败且受保护站点不可用，Site Recovery Manager 会创建临时占位映射。您需要完成这些临时占位映射，恢复才能够成功。

由于在运行恢复计划时 Site Recovery Manager 将清单映射应用到存储策略保护组中的虚拟机，因此存储策略保护组需要站点范围的清单映射。如果缺少站点范围的清单映射，包含存储策略保护组的恢复计划的恢复测试、计划迁移和灾难恢复将失败。

如果包含存储策略保护组的恢复计划因缺少映射而失败且受保护站点可用，则以常规方式配置缺少的映射，然后再次运行恢复。有关如何配置站点范围的清单映射的信息，请参见配置清单映射。

如果包含存储策略保护组的恢复计划因缺少映射而失败且受保护站点不可用，您将无法正常配置缺少的映射。要使恢复成功，必须完成因缺少映射而导致恢复计划失败时 Site Recovery Manager 创建的临时占位映射。

前提条件

- 受保护站点不可用。
- 在包含存储策略保护组的恢复计划中运行了灾难恢复。
- 恢复因缺少清单映射而失败。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 单击**恢复计划**选项卡，然后选择失败的恢复计划。
4. 选择**恢复步骤**，然后展开处于错误状态的步骤。
5. 将指针悬停在错误消息上方以查看完整消息。

   如果缺少清单映射，您会看到有关缺少映射的错误。

   例如，如果缺少资源映射，您会看到：无法获取与占位虚拟机关联的主机。资源映射中缺少资源池 *address* 的映射 (Cannot fetch hosts associated with placeholder VMs. Mapping for resourcePool address missing in resource mappings)。

6 选择**站点对**选项卡，然后检查恢复站点的远程 SRM 连接。

您会看到一条消息，通知您受保护站点脱机，Site Recovery Manager 已创建临时占位映射。

7 选择下列选项卡：**网络映射**、**文件夹映射**、**资源映射**以及**存储策略映射**选项卡。

缺少映射时，Site Recovery Manager 已在受保护站点上选择某个资源。恢复站点上的相应资源会显示：映射丢失 (Mapping is missing)。

8 选择临时占位映射，然后单击图标以编辑该映射。

9 在恢复站点上选择一个资源（Site Recovery Manager 在受保护站点上选择的资源将映射到该资源），然后单击**确定**。

10 单击**恢复计划**选项卡，选择失败的恢复计划，然后再次运行恢复计划。

如果已配置所有缺少的映射，恢复将成功。如果仍缺少映射，恢复将失败。

11 如果恢复再次失败，重复步骤步骤 4 至步骤 10，直到恢复成功。

后续步骤

当受保护站点再次可用时，以常规方式配置站点范围的清单映射，然后再次运行恢复，以便 Site Recovery Manager 能够完成受保护站点上的恢复步骤。

注 Site Recovery Manager 不会保留临时占位映射。如果重新启动恢复站点上的 Site Recovery Manager Server，您配置的临时占位映射将丢失。在运行必须配置临时占位映射的恢复后，始终配置正常的清单映射。

用户在配置临时占位映射后获得虚拟机访问权限

在受保护站点不可用时完成临时占位映射的用户可能会意外获得虚拟机访问权限。

问题

灾难恢复期间受保护站点不可用，Site Recovery Manager 创建了临时占位映射。运行恢复计划的用户完成临时占位映射并重新运行计划。恢复后，用户获得了恢复站点上虚拟机的访问权限，而其在受保护站点上并无此访问权限。

- 用户在受保护站点不可用时运行灾难恢复。
- 用户无权访问受保护站点上的所有清单对象。
- Site Recovery Manager 检测到缺少映射，进而创建临时占位映射，其中包含受保护站点上用户无权访问的对象。
- 用户配置从受保护站点上的对象到恢复站点上用户可访问的对象的目标映射。
- 恢复后，由于已恢复虚拟机使用恢复站点上用户有权访问的资源，因此用户现在可以访问原本在受保护站点上无法访问的虚拟机。

原因

如果受保护站点不可用，Site Recovery Manager 必须使用受保护站点上的清单对象创建临时占位映射，才能对这些清单对象执行权限检查。

解决方案

验证有权运行恢复计划的用户是否也有权访问两个站点上的所有对象。

配置清单映射

清单映射提供了恢复站点的清单中的默认对象，以便在您运行恢复时供已恢复虚拟机使用。

对于基于阵列的保护和 vSphere Replication 保护，如果您在创建保护组之前配置站点范围的清单映射，则在创建保护组时无需在每个虚拟机上单独配置保护。创建基于阵列的复制保护组或 vSphere Replication 保护组时，Site Recovery Manager 会将站点范围的映射应用到该保护组中的所有虚拟机。

使用存储策略保护时，Site Recovery Manager 会在运行恢复计划时应用清单映射。您无法在存储策略保护组中的虚拟机上单独配置保护。因此，如果使用存储策略保护，您必须配置站点范围的清单映射。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在**站点对**选项卡上，展开**配置**，然后选择要配置的资源类型。

选项	操作
网络映射	将保护站点上的网络映射至恢复站点上的网络。
文件夹映射	将保护站点上的数据中心或虚拟机文件夹映射到恢复站点上的数据中心或虚拟机文件夹。
资源映射	将受保护站点上的资源池、独立主机、vApp 或群集映射至恢复站点上的资源池、独立主机、vApp 或群集。您可以将一个站点上任意类型的资源映射到另一个站点上任意类型的资源。 **注** 您无法将属于群集的单个主机映射到其他资源对象。

4 单击**新建**以创建新映射。

5 选择自动创建映射还是手动创建映射，然后单击**下一步**。

该步骤仅适用于网络映射和文件夹映射。自动映射仅适用于网络和文件夹映射。必须手动配置资源映射。

选项	描述
自动	Site Recovery Manager 自动将受保护站点上的网络和文件夹映射到恢复站点上具有相同名称的网络和文件夹。
手动	将受保护站点上的特定网络和文件夹映射到恢复站点上的特定网络、文件夹和资源。

6 在受保护站点上选择要映射到恢复站点项目的项目。

- 如果选择了自动映射，则展开左侧清单项，选择本地站点上的某个父节点（例如数据中心或文件夹），然后展开右侧清单项，选择远程站点上的某个父节点。

- 如果选择了手动映射，则展开左侧清单项，选择本地站点上的某个特定对象，然后展开右侧清单项，选择要将此对象映射到的远程站点上的对象。

如果选择手动映射，您可以将本地站点上的多个项目映射到远程站点上的单个项目。您在远程站点上一次只能选择一个项目。

注 仅存储策略保护组支持 NSX 通用线路自动映射。如果您使用的是虚拟机保护组，则必须明确配置通用线路两端之间的网络映射，以确保虚拟机在同一通用线路上恢复。请参见将 Site Recovery Manager 与 NSX Data Center for vSphere 结合使用。

7 单击**添加映射**。

这些映射会显示在页面底部。如果选择了自动映射，Site Recovery Manager 会自动将您在受保护站点上所选的节点下的所有项目映射到在恢复站点上所选的节点下具有相同名称的项目。

8 单击**下一步**。

9 （可选） 如果要配置网络映射，请在**选择测试网络**页面中单击“测试网络”列的网络，并使用下拉菜单选择测试恢复计划时要使用的网络。

您可以配置 Site Recovery Manager 以在测试恢复计划时在恢复站点上创建隔离的网络。创建隔离的测试网络可以使测试继续进行，而无需在恢复站点的生产网络上增加额外流量。

- 选择**隔离的网络 (自动创建)** 可自动在恢复站点上创建隔离的网络以用于测试。此为默认选项。
- 在恢复站点上选择一个现有网络用于测试。

10 （可选） 在**准备反向映射**页面上，选择与映射对应的复选框。

选中该选项可以创建从远程站点上的项目到本地站点上的项目的相应映射。您需要反向映射来建立双向保护并运行重新保护操作。如果两个或多个映射在远程站点上有相同目标，则无法选择该选项。

11 单击**完成**以创建映射。

12 重复步骤 3 至步骤 11 以建立其余资源类型的映射。

关于存储策略映射

您可以保护与存储策略关联的虚拟机，方法是将虚拟机包含在存储策略保护组中。

根据您在 vCenter Server 中定义的规则和标记，存储策略会将虚拟机放置在 vCenter Server 清单以及数据存储中。存储策略可移动清单中的虚拟机，也可以移至其他数据存储，以适应 vCenter Server 环境中的更改。

如果将受保护站点上的存储策略映射至恢复站点上的存储策略，则运行恢复计划时， Site Recovery Manager 会根据恢复站点上所映射的存储策略，将已恢复虚拟机放置在恢复站点的 vCenter Server 清单以及数据存储中。

选择存储策略映射

如果将受保护站点上的存储策略映射至恢复站点上的存储策略，则运行恢复计划时，Site Recovery Manager 会根据恢复站点上所映射的存储策略，将已恢复虚拟机放置在恢复站点的 vCenter Server 清单以及数据存储中。

前提条件

您同时在受保护站点和恢复站点上创建了存储策略。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在**站点对**选项卡上，单击**配置 > 存储策略映射**。

4 选择一个站点，然后单击**新建**以创建映射。

5 选择自动创建映射还是手动创建映射，然后单击**下一步**。

选项	描述
为具有匹配名称的存储策略自动准备映射	Site Recovery Manager 自动将受保护站点上的存储策略映射到恢复站点上具有相同名称的存储策略。
手动准备映射	将受保护站点上的特定存储策略映射到恢复站点上的特定存储策略。

6 选择受保护站点上的存储策略以映射到恢复站点上的存储策略。

- 如果选择自动映射，Site Recovery Manager 会在受保护站点上选择与恢复站点上的存储策略具有相同名称的任何存储策略。
- 如果选择手动映射，请在受保护站点上选择一个特定存储策略，然后在恢复站点上选择要将该存储策略映射到的存储策略。

如果选择手动映射，您可以将本地站点上的多个存储策略映射到远程站点上的单个存储策略。您在远程站点上一次只能选择一个项目。

7 单击**添加映射**。

这些映射会显示在页面底部。

8 单击**下一步**。

9 （可选） 在**反向映射**页面上，选中与映射对应的复选框，然后单击**下一步**。

选中该选项可以创建从远程站点的存储策略到本地站点的存储策略的相应映射。您需要反向映射来建立双向保护并运行重新保护操作。如果两个或多个映射在远程站点上有相同目标，则无法选择该选项。

10 单击**完成**以创建映射。

关于占位虚拟机

4

创建包含数据存储组的基于阵列的复制保护组或包含各个虚拟机的 vSphere Replication 保护组时，Site Recovery Manager 会在恢复站点为保护组中的每个虚拟机创建占位虚拟机。

占位虚拟机是虚拟机文件的子集。Site Recovery Manager 使用该文件子集来向恢复站点上的 vCenter Server 注册虚拟机。

占位虚拟机的文件非常小，并不代表受保护虚拟机的完整副本。占位虚拟机未连接任何磁盘。占位虚拟机会在恢复站点上预留计算资源，并在 vCenter Server 清单中提供运行恢复时受保护虚拟机进行恢复的位置。

恢复站点清单中的占位虚拟机为 vCenter Server 管理员提供了虚拟机受 Site Recovery Manager 保护的可视化指示。占位虚拟机还向 vCenter Server 管理员指示在 Site Recovery Manager 运行测试或运行恢复计划时虚拟机可以打开电源并开始消耗本地资源。

在通过测试或运行恢复计划来恢复受保护虚拟机时，Site Recovery Manager 会使用已恢复的虚拟机替换占位虚拟机并根据恢复计划的设置打开其电源。恢复计划测试完成后，Site Recovery Manager 会在清理过程中还原占位虚拟机并关闭已恢复虚拟机的电源。

注 Site Recovery Manager 不会为存储策略保护组创建占位虚拟机。有关在使用存储策略保护组时 Site Recovery Manager 如何在恢复站点上放置虚拟机的信息，请参见存储策略保护组的清单映射 和关于存储策略映射。

关于占位虚拟机模板

保护受保护站点上的模板时，Site Recovery Manager 会通过在计算资源的默认资源池中创建虚拟机并将该虚拟机标记为模板来创建占位模板。Site Recovery Manager 从恢复站点上数据中心中的可用计算资源集（受保护站点上虚拟机的文件夹映射到该资源集）中选择计算资源。所选计算资源中的所有主机必须至少对一个占位数据存储具有访问权限。计算资源中至少有一个主机必须支持受保护虚拟机模板的硬件版本。

关于占位数据存储

如果使用基于阵列的复制保护数据存储组，或者使用 vSphere Replication 保护各个虚拟机，您必须在恢复站点上确定 Site Recovery Manager 可用于存储占位虚拟机文件的数据存储。

注 Site Recovery Manager 不会为存储策略保护组创建占位虚拟机。如果仅使用存储策略保护组，则无需确定占位数据存储。

占位虚拟机文件非常小，因此占位数据存储无需容纳全部虚拟机。

要启用计划的迁移和重新保护，必须在两个站点中选择占位数据存储。

本章讨论了以下主题：

- 恢复过程对占位虚拟机的影响
- 选择占位数据存储

恢复过程对占位虚拟机的影响

创建基于阵列的保护组和 vSphere Replication 保护组时，Site Recovery Manager 会在恢复站点上创建占位虚拟机。运行包含这些保护组的恢复计划时，Site Recovery Manager 会使用实际虚拟机替换占位虚拟机。

注 Site Recovery Manager 不会为存储策略保护组创建占位虚拟机。此示例适用于基于阵列的保护组和 vSphere Replication 保护组，不适用于存储策略保护组。有关使用存储策略保护组时 Site Recovery Manager 如何恢复虚拟机的信息，请参见关于存储策略保护组。

此示例说明运行包含基于阵列的保护组和 vSphere Replication 保护组的恢复计划时，Site Recovery Manager 使用实际虚拟机替换恢复站点上的占位虚拟机的过程。

1 根据所使用的复制类型，不使用 Site Recovery Manager 将虚拟机复制到恢复站点。
   - 对于基于数据存储的复制，存储阵列将复制包含虚拟机文件的数据存储，作为目标存储阵列中的原始存储。
   - vSphere Replication 将复制单个虚拟机，方法是在配置为 vSphere Replication 目标的数据存储中生成虚拟机的副本。这些虚拟机副本未打开电源。
2 在恢复站点上指定一个数据存储，供 Site Recovery Manager 用于存储占位虚拟机文件。
3 通过向保护组添加数据存储组或单个虚拟机，在虚拟机上配置 Site Recovery Manager 保护时，Site Recovery Manager 会在恢复站点上的占位数据存储中为该虚拟机创建占位虚拟机。
4 运行恢复计划时，Site Recovery Manager 会关闭受保护站点上的虚拟机，并根据所使用的复制类型激活恢复站点上的虚拟机。
   - 对于基于数据存储的复制，Site Recovery Manager 将显示恢复站点上包含已复制的虚拟机的原始存储，作为 vCenter Server 数据存储。Site Recovery Manager 会向占位数据存储所注册的 ESXi 主机或群集注册已恢复的数据存储。
   - vSphere Replication 将打开恢复站点上虚拟机副本的电源。

5 Site Recovery Manager 向 vCenter Server 发送请求，要求将占位虚拟机的身份与恢复站点上所显示的已复制的虚拟机进行交换。

选择占位数据存储

如果使用基于阵列的保护组或 vSphere Replication 保护组，您必须在恢复站点上指定一个占位数据存储，以供 Site Recovery Manager 用于存储占位虚拟机。

必须在一对站点中的两个站点上均配置占位数据存储，才能建立双向保护并执行重新保护。

注 Site Recovery Manager 不会为存储策略保护组创建占位虚拟机。如果仅使用存储策略保护组，则无需选择占位数据存储。

前提条件

- 确认已连接并配对受保护站点和恢复站点。
- 占位数据存储必须满足特定标准。
  - 对于群集，占位数据存储必须对群集中的所有主机可见。
  - 您不能选择使用基于阵列的复制进行复制的任何数据存储作为占位数据存储。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在**站点对**选项卡上，选择**配置 > 占位数据存储**。

4 选择一个站点，然后单击**新建**以配置占位数据存储。

5 选择一个数据存储，将其指定为本地站点上占位虚拟机的位置，然后单击**确定**。

将显示先前配置的数据存储，但您无法选择它们。如果数据存储已复制但 Site Recovery Manager 没有用于该数据存储的阵列管理器，则可能不会提供用来选择已复制数据存储的选项。不要选择 Site Recovery Manager 不进行管理的已复制数据存储。

重要事项 如果使用 vSphere Replication，则可选择已用作目标数据存储进行复制的占位数据存储。如果使用同一数据存储，Site Recovery Manager 会使用复制目标的名称并添加后缀 (1) 来创建占位虚拟机。有关 vSphere Replication 保护组的信息，请参见 vSphere Replication 保护组。选择同一数据存储可能会在区分复制目标和占位虚拟机时造成混淆。为避免混淆，最佳做法是使用不同的数据存储。

确保占位数据存储与 vSphere Replication 复制目标数据存储位于不同的 Storage DRS 群集中。

注 在使用 vSphere Replication 配置或重新配置虚拟机复制时，请不要将占位虚拟机文件夹设置为虚拟机的复制文件夹。

6 选择一对站点中的另一个站点。

7 重复步骤 3 到步骤 5 以配置另一个站点上的占位数据存储。

创建和管理保护组

5

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 或存储策略保护，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的复制的虚拟机又包含已配置 vSphere Replication 或存储策略保护的虚拟机的保护组。同一个恢复计划中可以同时包含基于阵列的复制保护组和 vSphere Replication 保护组。同一个恢复计划中不能同时包含存储策略保护组和基于阵列的复制保护组以及 vSphere Replication 保护组。

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。对于基于阵列的复制保护组和 vSphere Replication 保护组，如果未指定清单映射，则请分别为保护组中的每个虚拟机配置映射。您不能分别为存储策略保护组中的虚拟机配置映射，因此，如果您使用的是存储策略保护组，则必须配置站点范围的清单映射。

创建基于阵列的复制保护组或 vSphere Replication 保护组后，Site Recovery Manager 将在恢复站点上创建占位虚拟机，并将清单映射应用到组中的每个虚拟机。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。对于存储策略保护组，Site Recovery Manager 会在您运行恢复计划时应用清单映射。Site Recovery Manager 不会为存储策略保护组创建占位虚拟机。

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。

本章讨论了以下主题：

- 关于基于阵列的复制保护组和数据存储组
- vSphere Replication 保护组
- 关于存储策略保护组
- 保护加密的虚拟机
- 保护组状态概述
- 虚拟机保护状态概述
- 创建保护组
- 通过文件夹对保护组进行组织

- 在保护组中添加和移除数据存储组或虚拟机
- 将清单映射应用于基于阵列的保护组或 vSphere Replication 保护组的所有成员
- 为基于阵列的保护组或 vSphere Replication 保护组中的单个虚拟机配置清单映射
- 修改基于阵列的保护组或 vSphere Replication 保护组中虚拟机的设置
- 移除虚拟机的保护

关于基于阵列的复制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复制保护组。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复制保护组中移除虚拟机。

您可以通过基于阵列的复制保护组保护和恢复加密的虚拟机。使用基于阵列的复制保护和恢复加密虚拟机需要 VMware vSphere 6.7 及更高版本。

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文件。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。

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。

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。

注 在使用 vSphere Replication 配置或重新配置虚拟机复制时，请不要将占位虚拟机文件夹设置为虚拟机的复制文件夹。

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。

关于存储策略保护组

存储策略保护组可对与存储策略关联的虚拟机启用自动保护。

可使用基于阵列的复制将数据存储从受保护站点复制到恢复站点。如果对数据存储进行标记，然后创建映射到该标记的存储策略，数据存储会自动与该存储策略进行关联。包含该存储策略的存储策略保护组将自动保护数据存储中已正确标记的所有虚拟机。如果解除虚拟机与存储策略的关联，或将该虚拟机从数据存储中移除， Site Recovery Manager 将自动取消其保护。

创建存储策略保护组时， Site Recovery Manager 会执行以下操作：

- 在本地 Site Recovery Manager Server 实例上创建代表存储策略保护组的受管对象。

- 将您选择的存储策略与存储策略保护组关联。 Site Recovery Manager 会保护包含在存储策略保护组中的所有合规存储策略。
- 本地存储策略保护组会积极保护本地 vCenter Server 实例上相应的 vSphere 实体，并确定所包含的存储策略的合规性。根据 vSphere 清单的最新已知状态，新创建的存储策略保护组的初始保护包括保护与保护组中存储策略关联的所有虚拟机。

  注 初始保护不包括相关一致性组的任何存储同步。您必须根据常规调度来复制存储，而不是通过 vSphere 及 Site Recovery Manager。

- 启动 vSphere 清单监控可检测初始保护后添加至该清单中的所有 vSphere 实体。如果 Site Recovery Manager 无法保护任何 vSphere 实体，存储策略保护组的创建不会失败，但会在保护组属性中显示错误。
- 在恢复站点的 Site Recovery Manager Server 实例上创建代表存储策略保护组的对等受管对象。即使底层存储尚未准备恢复，该对象在创建后也可立即进行恢复。

创建存储策略保护组后，可能需要同步底层存储以确保受保护 vSphere 实体可恢复。创建保护组后，尽快使用复制最近更改的选项来运行测试恢复。

存储策略保护组的必备条件

创建存储策略保护组时，必须首先创建存储策略并确保环境满足某些必备条件。

前提条件

- 创建数据存储标记，并将其分配给数据存储以与存储策略关联：
  - 如果环境不使用增强型链接模式，请在受保护站点和恢复站点上创建标记类别和标记，并将其分配给受保护站点上要保护的数据存储。
  - 如果环境使用增强型链接模式，请仅在受保护站点上创建标记类别和标记。标记将复制到增强型链接模式环境中的其他 vCenter Server 实例。
- 在两个站点上的 vCenter Server 中创建虚拟机存储策略，其中包括分配给要保护的数据存储的标记。在两个站点上创建虚拟机策略，即使环境使用增强型链接模式也是如此。每个站点上的存储策略可以使用不同名称。
- 将要保护的虚拟机与受保护站点上的相应存储策略相关联。必须将虚拟机的所有磁盘与同一存储策略相关联。
- 使用阵列供应商提供的复制技术配置从受保护站点到恢复站点的基于阵列的数据存储复制。
- 在 Site Recovery Manager 中配置清单映射。存储策略保护组在应用清单映射方面具有特定行为，在如何设置资源清单映射方面具有特定要求。例如，如果使用存储策略保护组但未配置映射，则计划迁移或灾难恢复将失败，而 Site Recovery Manager 会使用临时占位映射成功完成操作。
- Site Recovery Manager Server 启动时，Site Recovery Manager 将在 vCenter Server 中查询基于存储策略的管理和标记管理器服务以查找与存储策略关联的虚拟机。启动或重新启动 Site Recovery Manager Server 时，这些服务和 vCenter Server 必须正在运行。如果未在运行，Site Recovery Manager Server 将不会启动。

有关如何创建存储策略的信息，请参见 VMware vSphere ESXi 和 vCenter Server 6.7 文档中的虚拟机存储策略。

有关如何创建清单映射的信息，请参见配置清单映射。

有关存储策略保护组和清单映射的信息，请参见存储策略保护组的清单映射 。

有关存储策略保护组的已知限制的信息，请参见存储策略保护组的限制。

存储策略保护组的限制

存储策略保护组存在一些限制。

保护虚拟机模板

符合受保护的存储策略的数据存储不应包含虚拟机模板。

保护具有 RDM 磁盘的虚拟机

符合受保护的存储策略的数据存储不应包含具有 RDM 磁盘的虚拟机。

保护虚拟机和许可限制

- 由于许可限制最初未保护的虚拟机将不受保护，即使修改一致性组和虚拟机以满足许可限制后也是如此。
- 由于许可限制最初未保护的虚拟机将不受保护，即使安装了适用于大量虚拟机的许可证后也是如此。

增强型链接模式环境中的重复标记

在增强型链接模式环境中，如果 vCenter Server 实例间出现临时网络分区，则可能会在其中一个站点上创建一个标记，并在另一站点上创建一个同名的标记。您可能会使用第一个标记来标记其中一个站点上的一组数据存储，并使用第二个相同的标记来标记另一站点上的另一组数据存储。由于 Site Recovery Manager 根据名称而非 ID 来查找标记，因此，移除网络分区后，两个站点上的数据存储显示为标记了相同的标记。如果删除其中一个重复的标记，则 Site Recovery Manager 可能会从具有该标记的数据存储中的一致性组中移除保护。这些一致性组中的虚拟机将失去保护，虚拟机的恢复设置也将被删除。

要避免发生这种情况，请先解决标记冲突，然后再创建存储策略保护组并配置虚拟机恢复设置。如果您在创建存储策略保护组后遇到这种情况，请暂时关闭受保护站点并解决标记冲突。

更改恢复和重新保护之间的阵列状态

在运行恢复计划之后且运行重新保护之前，如果您更改阵列设备的状态，例如，为了修复反向复制问题，您启动对存储设备的重新扫描，则 Site Recovery Manager 会意外停止。如果发生这种情况，必须重新创建相应的保护组和恢复计划。

将非复制数据存储与存储策略关联

可以将非复制数据存储与包含在存储策略保护组中的存储策略相关联。但是，Site Recovery Manager 不会保护驻留在非复制数据存储上的虚拟机，即使该数据存储与包含在存储策略保护组中的存储策略关联也是如此。如果运行包含该保护组的恢复计划，则非复制数据存储上具有文件的任何虚拟机都将在保护组中显示有错误，因此不会恢复。

数据存储跨多个一致性组

请勿将数据存储配置为跨多个一致性组。Site Recovery Manager 无法保护此类使用多个一致性组的数据存储或虚拟机，并且操作会失败。

- 如果没有一致性组支持的其他数据存储属于存储策略，则保护组可能会跳过该一致性组。
- 保护组可能不会报告与数据存储相关的问题。
- 使用跨一致性组的数据存储的虚拟机将处于不受保护的状态，即使虚拟机使用正确的存储策略也是如此。
- 跨多个一致性组的数据存储将显示为非复制数据存储，并且不受存储策略保护组保护。Site Recovery Manager 将保护组迁移到恢复站点时，这些数据存储可能会消失。

同时在基于阵列的复制保护组和存储策略保护组中保护相同的一致性组

如果标记某个复制数据存储并将其与某个存储策略关联，则可以将该存储策略及其关联的一致性组包含在存储策略保护组中。还可以将包含标记数据存储的数据存储组包含在基于阵列的复制保护组中。因此，一致性组最终会同时包含在基于阵列的复制保护组和存储策略保护组中。

存储策略保护组和基于阵列的复制保护组同时尝试保护同一个一致性组时，基于阵列的复制保护组将获取一致性组及其所包含的虚拟机的所有权。存储策略保护组将一致性组和虚拟机标记为错误状态。在这种情况下，必须从其中一个保护组中移除一致性组。

- 要将一致性组保留在基于阵列的复制保护组中，请解除受影响虚拟机与存储策略的关联。同时解除一致性组与存储策略的关联。此操作会从存储策略保护组中移除一致性组和虚拟机。
- 要将一致性组保留在存储策略保护组中，请编辑基于阵列的复制保护组以移除数据存储和虚拟机。这将自动解决存储策略保护组中的错误。

在恢复期间和恢复之后更改一致性组和虚拟机的保护状态

通过对数据存储进行标记和取消标记或将虚拟机与存储策略关联和取消关联，可以更改存储策略保护组中包含的一致性组和虚拟机的保护状态。如果在更改虚拟机和一致性组的保护状态时，没有计划的迁移或灾难恢复在运行，Site Recovery Manager 将会更新 SPPG 中虚拟机和一致性组的保护状态。

如果在更改虚拟机和一致性组的保护状态时，有使用存储策略保护组的计划迁移或灾难恢复在运行，Site Recovery Manager 用户界面可能会显示对保护站点的更改，但恢复工作流无法正常更新，恢复会失败。

为了确保成功完成恢复过程，在运行 SPPG 的计划迁移或灾难恢复期间，不得更改 SPPG 中虚拟机和一致性组的保护状态。更确切地说，从包含 SPPG 的恢复计划首次进入“正在进行恢复”状态到该计划到达“恢复完成”状态的这段时间内，不支持更 改保护状态。

如果运行的恢复计划包含存储策略保护组，那么无论运行是否成功，都无法向该保护组添加一致性组或虚拟机。不要向处于“已恢复”或“部分已恢复”状态的存储策略保护组添加新的一致性组或虚拟机。可向以下现有存储策略保护组添加新的一致性组或虚拟机：从未包含在恢复计划运行中或仅包含在测试恢复中的存储策略保护组。

运行包含存储策略保护组的恢复计划后，必须在新的存储策略保护组中包含所有新的一致性组或虚拟机。从恢复的存储策略保护组中移除新的一致性组或虚拟机，然后将这些一致性组或虚拟机添加到新的存储策略保护组中。Site Recovery Manager 仅支持对单个保护组中的对象进行保护。

资源清单映射的要求

存储策略保护组在如何设置资源清单映射方面具有特定的要求和限制。有关详细信息，请参见存储策略保护组的清单映射 。

存储策略保护组和非受保护虚拟机

您的环境、存储策略的实施以及数据存储和要保护的虚拟机的配置必须满足存储策略保护组的必备条件。如果不满足必备条件，Site Recovery Manager 可能无法保护存储策略保护组中的所有虚拟机。

有关必须满足的存储策略保护的必备条件，请参见存储策略保护组的必备条件。

例如，未与存储策略关联的虚拟机可以和与存储策略关联的虚拟机一起驻留在标记数据存储中。如果存储策略保护组中包含了该存储策略，由于这些虚拟机未与该存储策略关联，因此 Site Recovery Manager 不会保护这些虚拟机。

除了虚拟机未与正确的存储策略关联以外，非受保护虚拟机会由于其他原因显示在存储策略保护组中。有关非受保护虚拟机可显示在存储策略保护组中的其他情况的说明，请参见存储策略保护组的限制。

如果存储策略保护组包含非受保护虚拟机，这些虚拟机将显示在存储策略保护组的**相关对象 > 虚拟机**视图中。保护组显示为错误状态。

Site Recovery Manager 处理非受保护虚拟机的方式取决于您运行的恢复的类型。

注 您只能尝试保护从未运行恢复的存储策略保护组中的非受保护虚拟机。如果已在包含非受保护虚拟机的存储策略保护组中运行恢复，无论运行是否成功，您必须从存储策略保护组中移除这些虚拟机。

- 如果在包含非受保护虚拟机的存储策略保护组中运行测试恢复，该操作将失败并显示错误。如果测试恢复由于非复制虚拟机而失败，请在尝试保护或移除非受保护虚拟机之前运行清理，然后再次运行测试。运行清理后，如果从未在该保护组上运行恢复，请尝试修复受影响虚拟机的保护，例如，通过将虚拟机与正确的存储策略关联，或将虚拟机文件从非复制数据存储移动到复制的数据存储。
- 如果在包含非受保护虚拟机的存储策略保护组中运行计划迁移，该操作将失败，恢复计划会显示“恢复未完成”状态。在计划迁移的停用步骤中，受保护站点上的非受保护虚拟机可防止 Site Recovery Manager 将存储设为只读，否则虚拟机可能无法访问其数据。如果保护组处于“恢复未完成”状态，您必须将非受保护虚拟机从受保护数据存储中移除，并解除虚拟机与存储策略的关联。
- 如果在包含非受保护虚拟机的存储策略保护组中运行灾难恢复，操作将成功，但 Site Recovery Manager 不会恢复非受保护虚拟机。当受保护站点恢复联机，您尝试运行计划迁移以完成恢复时，如果受保护站点中仍存在非受保护虚拟机，计划迁移将失败。如果保护组处于“恢复未完成”状态，您必须将非受保护虚拟机从受保护数据存储中移除，并解除虚拟机与存储策略的关联。

保护加密的虚拟机

可以使用基于阵列的复制保护组、vSphere Replication 保护组或存储策略保护组 (SPPG) 来保护和恢复加密的虚拟机。

创建存储策略后，必须使用以下步骤编辑存储策略的规则集。

前提条件

- 如果要使用 SPPG，请完成存储策略保护组的必备条件中的必备条件。
- 确保恢复站点和受保护站点使用一个公用的密钥管理服务器 (Key Management Server, KMS)，或者两个站点的密钥管理服务器集群都使用通用加密密钥。有关如何设置密钥管理服务器集群的信息，请参见《VMware vSphere ESXi 和 vCenter Server 6.7》文档。

步骤

1. 在**虚拟机存储策略**向导的**规则集**页面上，选择**在存储策略中使用规则集**，并确保为“存储类型”选择基于“标记”的替换选项。
2. 单击**<添加规则>**，然后单击**类别中的标记**。
3. 在<选择类别>中，单击您的类别。
4. 确保为“类别中的标记”选择“以任一…标记”。
5. 单击**添加标记…**，然后选择您的标记。

后续步骤

1. 创建存储策略映射，确保恢复站点上的存储策略与受保护站点上的策略相同。有关如何创建存储策略映射的信息，请参见选择存储策略映射。
2. 创建基于阵列的复制保护组、vSphere Replication 保护组或存储策略保护组。有关创建基于阵列的复制保护组的信息，请参见创建基于阵列的复制保护组。有关创建 vSphere Replication 保护组的信息，请参见创建 vSphere Replication 保护组。有关创建存储策略保护组的信息，请参见创建存储策略保护组。

保护组状态概述

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 5-1. 保护组状态

状态	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。
良好	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，组恢复为良好或未配置状态。

表 5-1. 保护组状态 （续）

状态	描述
正在清理	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，组恢复为良好或未配置状态。 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，组恢复为良好或未配置状态。 如果重新保护失败，组将处于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。

虚拟机保护状态概述

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 5-2. 虚拟机保护状态

状态	描述
未找到占位虚拟机	已删除占位虚拟机。 **还原占位**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**图标已启用。
虚拟机使用的数据存储 *名称* 在组中丢失	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。

表 5-2. 虚拟机保护状态 （续）

状态	描述
虚拟机使用的数据存储 *名称*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： *设备名称*	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，以便在保护中包含或移除设备。
缺少映射： 文件夹 *名称*；网络 *名称*；资源池 *名称*	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： *服务器返回的错误字符串*	占位虚拟机创建过程中出错。
良好	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： *错误*	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： *错误*	错误可能为以下之一： ■ 恢复站点资源池、文件夹或网络不在同一数据中心。 ■ 未找到占位数据存储。 ■ 创建占位时出现任何 vCenter Server 错误，如连接或权限问题。
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。

创建保护组

可以创建保护组，以便 Site Recovery Manager 保护虚拟机。

创建保护组时，请等待操作按预期完成。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。

可以将保护组组织到文件夹中。

注 保护组的名称必须不同于所选文件夹的名称。

创建 vSphere Replication 保护组

创建 vSphere Replication 保护组以保护配置了 vSphere Replication 的虚拟机。

前提条件

确认您已在虚拟机上配置 vSphere Replication。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**保护组**选项卡，然后单击**新建**以创建保护组。

4 在**名称和方向**页面上，输入保护组的名称和描述，选择一个方向，然后单击**下一步**。

5 在**保护组类型**窗格中，选择**单个虚拟机 (vSphere Replication)**，然后单击**下一步**。

6 从列表中选择要添加到保护组的虚拟机，然后单击**下一步**。

只有已为 vSphere Replication 配置但尚未列入保护组中的虚拟机才会显示在列表中。

7 在**恢复计划**页面上，可以选择将保护组添加到恢复计划。

选项	描述
添加到现有恢复计划	将保护组添加到现有恢复计划。
添加到新恢复计划	将保护组添加到新恢复计划。 如果选择此选项，必须输入恢复计划名称。
不立即添加到恢复计划	如果不希望将保护组添加到恢复计划，请选择此选项。

8 查看设置，然后单击**完成**。

结果

您可以在**保护组**选项卡上监控保护组的创建进度。

- 如果 Site Recovery Manager 成功将清单映射应用到受保护的虚拟机，保护组的保护状态将为良好。
- 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，保护组的保护状态将为未配置。

后续步骤

如果保护组的保护状态为“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，请参见配置清单映射。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基于阵列的保护组或 vSphere Replication 保护组的所有成员。

- 要将清单映射分别应用于保护组中的每个虚拟机，请参见为基于阵列的保护组或 vSphere Replication 保护组中的单个虚拟机配置清单映射。

创建存储策略保护组

创建存储策略保护组以保护与存储策略相关联的虚拟机。

前提条件

确认您满足存储策略保护组的必备条件中的要求并已查看存储策略保护组的限制。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 单击**保护组**选项卡，然后单击**新建**以创建保护组。
4. 在**名称和方向**页面上，输入保护组的名称和描述，选择一个方向，然后单击**下一步**。
5. 在**保护组类型**页面上，选择**存储策略 (基于阵列的复制)**，然后单击**下一步**。
6. 选择要添加到保护组的存储策略，然后单击**下一步**。
7. 在**恢复计划**页面上，可以选择将保护组添加到恢复计划。

选项	描述
添加到现有恢复计划	将保护组添加到现有恢复计划。
添加到新恢复计划	将保护组添加到新恢复计划。 如果选择此选项，必须输入恢复计划名称。
不立即添加到恢复计划	如果不希望将保护组添加到恢复计划，请选择此选项。

8. 查看设置，然后单击**完成**。

   您可以在**保护组**选项卡上监控保护组的创建进度。

   - 如果 Site Recovery Manager 可以成功保护与存储策略相关联的所有虚拟机，则保护组的保护状态为良好。
   - 如果 Site Recovery Manager 无法保护与存储策略相关联的所有虚拟机，则保护组的保护状态为未配置。

后续步骤

如果保护组的保护状态为未配置，请验证您是否满足存储策略保护组的必备条件中的必备条件，查看存储策略保护组的限制，相应修改存储策略实施，并尝试重新创建保护组。

创建基于阵列的复制保护组

创建基于阵列的复制保护组以保护配置了基于阵列的复制的虚拟机。

前提条件

确认已将虚拟机包含在配置了基于阵列的复制的数据存储中。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**保护组**选项卡，然后单击**新建**以创建保护组。

4 在**名称和方向**页面上，输入保护组的名称和描述，选择一个方向，然后单击**下一步**。

5 在**保护组类型**窗格中，选择**数据存储组 (基于阵列的复制)**，选择一个阵列对，然后单击**下一步**。

6 选择要添加到保护组的数据存储组，然后单击**下一步**。

选择数据存储组时，组中包含的虚拟机将显示在**虚拟机**表中。

7 在**恢复计划**页面上，可以选择将保护组添加到恢复计划。

选项	描述
添加到现有恢复计划	将保护组添加到现有恢复计划。
添加到新恢复计划	将保护组添加到新恢复计划。 如果选择此选项，必须输入恢复计划名称。
不立即添加到恢复计划	如果不希望将保护组添加到恢复计划，请选择此选项。

8 查看设置，然后单击**完成**。

您可以在**保护组**选项卡上监控保护组的创建进度。

- 如果 Site Recovery Manager 成功将清单映射应用到受保护的虚拟机，保护组的保护状态将为良好。
- 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，保护组的保护状态将为未配置。

后续步骤

如果保护组的保护状态为“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，请参见配置清单映射。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基于阵列的保护组或 vSphere Replication 保护组的所有成员。
- 要将清单映射分别应用于保护组中的每个虚拟机，请参见为基于阵列的保护组或 vSphere Replication 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 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

2 单击**保护组**选项卡，然后在左侧窗格中右键单击**保护组**，并单击**新建文件夹**。

3 输入新文件夹的名称，然后单击**添加**。

4 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**新建保护组**。
添加现有保护组	右键单击清单树中的一个保护组，然后选择**移动**。选择目标文件夹，然后单击**移动**。

在保护组中添加和移除数据存储组或虚拟机

可以在基于阵列的复制保护组中添加和移除数据存储组，或在 vSphere Replication 保护组中添加和移除虚拟机。还可以更改基于阵列的复制保护组或 vSphere Replication 保护组的名称和描述。

注 初始创建存储策略保护组后，您无法对其进行编辑。通过修改受保护数据存储中虚拟机的存储策略关联，可向现有存储策略保护组添加虚拟机或从中移除虚拟机。仅当从未在存储策略保护组中运行恢复时，才能在该保护组中添加或移除虚拟机。有关详细信息，请参见存储策略保护组的限制。

前提条件

您已创建基于阵列的复制保护组或 vSphere Replication 保护组。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**保护组**选项卡，右键单击一个保护组，然后单击**编辑**。

4 （可选） 更改保护组的名称或描述，然后单击**下一步**。

5 单击**下一步**。

6 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**。

7 查看设置，然后单击**下一步**以应用更改。

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**。

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 会将新映射应用于新数据存储中的新受保护虚拟机。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，新虚拟机的状态为缺少映射。

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缺少映射，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，请参见配置清单映射。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基于阵列的保护组或 vSphere Replication 保护组的所有成员。
- 要将清单映射分别应用于保护组中的每个虚拟机，请参见为基于阵列的保护组或 vSphere Replication 保护组中的单个虚拟机配置清单映射。

将清单映射应用于基于阵列的保护组或 vSphere Replication 保护组的所有成员

如果基于阵列的保护组或 vSphere Replication 保护组的保护状态为未配置，您可以使用现有站点范围的清单映射为所有未配置的虚拟机配置保护。

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，请参见配置清单映射。
- 配置或重新配置占位数据存储映射。要配置占位数据存储，请参见选择占位数据存储。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**保护组**选项卡，单击一个保护组，然后在右侧窗格中单击**虚拟机**选项卡。

4 单击**配置所有虚拟机**按钮。

保护组中至少有一个虚拟机必须处于“未配置”状态，**配置所有虚拟机**按钮才会处于活动状态。

5 单击**是**，以确认要向所有未配置的虚拟机应用清单映射。

6 监控虚拟机的状态。如果 Site Recovery Manager 无法应用部分或全部清单映射，或者如果无法为虚拟机创建占位，则可以执行补救操作。

状态	操作
确定	不需要任何操作
未配置或缺少映射	检查清单映射，然后再次单击**配置所有虚拟机**
占位虚拟机创建错误	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**。

为基于阵列的保护组或 vSphere Replication 保护组中的单个虚拟机配置清单映射

可以分别为基于阵列的保护组或 vSphere Replication 保护组中的虚拟机配置映射。这样，可以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，也可以在基于阵列的保护组或 vSphere Replication 保护组中的虚拟机上配置各个清单映射。在这种情况下，可以移除单个虚拟机的保护，并配置文件夹和资源映射以替代站点范围的映射。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，请参见选择占位数据存储。

前提条件

已创建基于阵列的保护组或 vSphere Replication 保护组。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**保护组**选项卡，然后单击包含待配置虚拟机的保护组。

4 在右侧窗格中，单击**虚拟机**选项卡。

5 右键单击该虚拟机，然后单击**配置保护**。

6 通过展开资源，选中**替代站点映射**复选框，然后选择恢复站点上的资源，配置清单映射。单击**确定**。

仅可更改文件夹、资源池和网络映射。

7 监控虚拟机的状态。如果 Site Recovery Manager 无法应用部分或全部清单映射，或者如果无法为虚拟机创建占位，则可以执行补救操作。

状态	操作
确定	不需要任何操作
未配置或缺少映射	再次单击**配置保护**并检查清单映射。
占位虚拟机创建错误	在站点级别检查占位数据存储映射，右键单击虚拟机，然后单击**重新创建占位**。

修改基于阵列的保护组或 vSphere Replication 保护组中虚拟机的设置

修改受保护虚拟机的设置并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。

注 您不能修改存储策略保护组中保护的虚拟机的设置。

如果使用基于阵列的复制，则在受保护的虚拟机上添加或更改设备会对保护产生影响，具体取决于新设备的创建方式。

- 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。您可以使用 Storage vMotion 将虚拟机移至其他保护组中的数据存储中。

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://docs.vmware.com/cn/vSphere-Replication/index.html 上的 vSphere Replication 文档。

修改基于阵列的保护组和 vSphere Replication 保护组中的虚拟机后，必须为状态为未配置、设备未找到、未解析的设备或缺少映射的任何虚拟机重新配置保护。请参见将清单映射应用于基于阵列的保护组或 vSphere Replication 保护组的所有成员和为基于阵列的保护组或 vSphere Replication 保护组中的单个虚拟机配置清单映射。

移除虚拟机的保护

您可能会出于各种不同的原因而要移除虚拟机的保护。移除虚拟机的保护会对保护组造成不同的影响。

移除保护将删除恢复站点上的占位虚拟机。如果您移除基于阵列的复制保护组或 vSphere Replication 保护组中的虚拟机的保护，虚拟机和保护组的状态将设置为**未配置**。针对受保护虚拟机成功运行了包含保护组的恢复计划，但 Site Recovery Manager 不会恢复处于**未配置**状态的虚拟机或保护组。如果运行计划内迁移，计划会进入**恢复未完成**状态。

注 您无法临时移除存储策略保护组中的虚拟机的保护。

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。如果您移除基于阵列的复制保护组中的虚拟机的保护，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。

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 并且要将受保护虚拟机从保护组中排除。
- 您使用基于阵列的复制，但某个用户将您不想保护的虚拟机移至已复制的数据存储。如果您移除虚拟机的保护，保护组将显示**未配置**状态。整个组的测试恢复和计划迁移将失败。灾难恢复会成功，但是仅针对组中的受保护虚拟机，将跳过受保护站点上的某些操作。恢复计划进入 `Recovery required` 状态。在这种情况下，请将虚拟机移出受保护数据存储。
- 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，以便在您重新放置设备文件时能够对组中的所有其他虚拟机成功执行灾难恢复。

根据您使用基于阵列的复制还是 vSphere Replication，移除虚拟机的保护会对保护组产生不同的影响。

- 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。如果将非受保护虚拟机的文件保留在 Site Recovery Manager 包含在数据存储组中的数据存储中，则整个数据存储组的测试恢复和计划迁移将失败。灾难恢复会成功，但是仅针对数据存储组中的受保护虚拟机，您必须移动未受保护的虚拟机，才能运行计划内迁移以完成恢复。
- 如果禁用保护组中的虚拟机上的 vSphere Replication，则该虚拟机的恢复将失败，但保护组中所有正确配置的虚拟机的恢复将成功。您必须移除虚拟机的保护并将虚拟机移出保护组，方法是编辑保护组或者单击**移除虚拟机**。请参见在保护组中添加和移除数据存储组或虚拟机。

移除虚拟机的保护

您可以临时移除基于阵列的复制保护组或 vSphere Replication 保护组中已复制虚拟机的保护，而不将其从保护组中移除。

注 您无法临时移除存储策略保护组中的虚拟机的保护。

步骤

1. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
2. 单击**保护组**选项卡，选择一个保护组，然后在右侧窗格中单击**虚拟机**选项卡。
3. 右键单击某个虚拟机并单击**移除保护**。

4 单击**是**确认移除虚拟机的保护。

创建、测试和运行恢复计划

6

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，您可以创建一个恢复计划来处理整个组织中从受保护站点到恢复站点的计划服务迁移，也可以为各个部门创建不同的恢复计划。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。

一次只能运行一个恢复计划来恢复某一特定保护组。如果其他恢复计划共享了某个保护组，则测试或运行包含该保护组的恢复计划时，其他恢复计划会将该保护组的状态更改为保护组正在使用中，且您无法运行它们。

- 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内迁移或灾难恢复

  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。如果受保护站点发生可能会导致数据丢失的意外事件，还可以在未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

  可以通过创建、测试和运行恢复计划自定义 Site Recovery Manager 在恢复过程中的操作。
- 禁用存储策略保护组中虚拟机的恢复

  您可以禁用存储策略保护组中的虚拟机的恢复，而不将其从保护组中移除。
- 禁用存储策略保护组中一致性组的恢复

  您可以禁用存储策略保护组中的一致性组的恢复，而不将其从保护组中移除。
- 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报告
  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，可将其删除。
- 恢复计划状态概述
  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。恢复计划中保护组的状态确定了计划的状态。

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中删除重做日志，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，阵列会移除测试恢复工作流中先前创建的快照。

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。

隔离的测试网络由自己的虚拟交换机管理，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。隔离的测试网络不会跨主机运行。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必须一起恢复到同一网络。

数据中心网络是恢复站点的现有网络。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。如果 DHCP 配置正确，使用 DHCP 的已恢复虚拟机可以连接到该网络而无需其他自定义。其他虚拟机可能需要进行 IP 自定义并执行其他恢复计划步骤来应用该自定义。

通过运行恢复计划执行计划内迁移或灾难恢复

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。如果受保护站点发生可能会导致数据丢失的意外事件，还可以在未计划的情况下运行恢复计划。

注　通过运行恢复计划执行计划迁移和灾难恢复时，Site Recovery Manager 会在这两个站点上进行更改，而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。

计划的迁移

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。

灾难恢复

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 仍会打开恢复站点上的副本的电源。

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 会检测此状态且您可以再次运行该计划，以关闭受保护站点上的虚拟机的电源。之后，恢复计划会恢复一致状态，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。

使用 VMware Tools

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。VMware Tools 还可用于正常关闭受保护虚拟机的客户机操作系统。因此，最好在受保护虚拟机上安装 VMware Tools。如果在受保护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。

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 无法及时执行其任务，这会将 RTO 增加到一个不可接受的级别。在这种情况下，可以使用强制恢复选项运行恢复计划。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。

何时使用强制恢复

可在以下情况下使用强制恢复：基础架构在受保护站点失败，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。

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。

通过 vSphere Replication 进行强制恢复

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。

通过基于阵列的复制进行强制恢复

如果在受保护站点的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。

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。

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。

启用强制恢复

要在运行灾难恢复时选择强制恢复，必须在恢复站点的 Site Recovery Manager 服务器上的“高级设置”中启用 `recovery.forceRecovery` 选项。有关详细信息，请参见更改恢复设置。

在**运行恢复计划**向导中，只能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。

在强制恢复后运行计划内迁移

在运行强制恢复后运行计划的迁移时，如果基础数据存储是只读的或不可用，则受保护站点上的虚拟机可能无法关闭。在这种情况下，登录受保护站点上的 vCenter Server 并手动关闭虚拟机的电源。关闭虚拟机的电源后，再次运行计划的迁移。

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 6-1. 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。
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为**隔离的网络 (自动创建)** 且没有站点级别映射，Site Recovery Manager 会将虚拟机分配给未连接到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。如果您接受配置为**使用站点级别映射**的默认测试网络，则没有站点级别映射时，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

可以通过创建、测试和运行恢复计划自定义 Site Recovery Manager 在恢复过程中的操作。

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

要控制不同用户或组对恢复计划的访问，可以通过文件夹对恢复计划进行组织。

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，可以将 Site Recovery Manager 配置为在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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，然后单击**新建**以创建恢复计划。

4 输入计划的名称、描述和方向，选择一个文件夹，然后单击**下一步**。

注 恢复计划的名称必须不同于所选文件夹的名称。

5 从菜单中选择组类型。

选项	操作
单个虚拟机或数据存储组的保护组	选择此选项以创建一个包含基于阵列的复制和 vSphere Replication 保护组的恢复计划。
存储策略保护组	选择此选项以创建一个包含存储策略保护组的恢复计划。 如果使用延伸存储，则选择此选项。

6 为要恢复的计划选择一个或多个保护组，然后单击**下一步**。

7 从**测试网络**下拉菜单中选择要在测试恢复过程中使用的网络，然后单击**下一步**。

如果没有站点级别映射，默认选项**使用站点级别映射**会创建隔离测试网络。

8 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

要控制不同用户或组对恢复计划的访问，可以通过文件夹对恢复计划进行组织。

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 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

2 单击**恢复计划**选项卡，然后在左侧窗格中右键单击**恢复计划**，并单击**新建文件夹**。

3 输入要创建的文件夹的名称，然后单击**添加**。

4 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**新建恢复计划**。
添加现有恢复计划	右键单击清单树中的恢复计划，然后单击**移动**。选择目标文件夹，然后单击**移动**。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，右键单击一个恢复计划，然后单击**编辑**。

4 （可选） 更改计划的名称或描述，然后单击**下一步**。

您无法更改恢复计划的方向和位置。

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） 从下拉菜单中，在恢复站点上选择不同的测试网络，然后单击**下一步**。

7 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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，右键单击一个恢复计划，然后单击**测试**。

您也可以通过在恢复计划的**恢复步骤**视图中单击**测试**图标来运行测试。

4 （可选） 选择**将最近的更改复制到恢复站点**。

选中此复选框可确保恢复站点具有受保护虚拟机的最新副本，但意味着同步可能需要更多的时间。

5 单击**下一步**。

6 检查测试信息，然后单击**完成**。

7 单击“恢复计划”选项卡中的**恢复步骤**选项卡以监控测试进度并对消息进行响应。

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。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，右键单击一个恢复计划，然后选择**清理**。

您也可以通过在恢复计划的**恢复步骤**视图中单击**清理**图标来运行测试。

4 检查清理信息，然后单击**下一步**。

5 单击**完成**。

6 （可选） 如果清理完成但出现错误，则选中**强制清理**复选框以在清理操作过程中忽略错误，然后重新运行清理。如有必要，可多次运行清理，直至完成时无任何错误。

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。
- 确保您已配置完整的清单映射。如果您仅配置了临时占位符清单映射并使用**启用符合条件虚拟机的 vMotion** 选项运行计划的迁移，计划的迁移将失败，即使两个站点均在运行也是如此。
- 要使用**启用符合条件虚拟机的 vMotion** 选项进行计划迁移，请在虚拟机上启用 vMotion。有关在虚拟机上启用 vMotion 的说明，请参见对计划的迁移启用 vSphere vMotion。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 单击**恢复计划**选项卡，右键单击一个恢复计划，然后单击**运行**。
4. 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础架构**。
5. 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。如果您的阵列支持延伸的存储，请选中**启用符合条件虚拟机的 vMotion** 复选框。
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。

6. （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。
7. 单击**下一步**。
8. 查看恢复信息，然后单击**完成**。
9. 要监控各个步骤的进度，请单击恢复计划，然后单击**恢复步骤**选项卡。

结果

近期任务面板会报告整个计划的进度。

恢复虚拟机的时间点快照

通过 vSphere Replication，可以将 Site Recovery Manager 配置为在运行恢复计划时恢复虚拟机的多个时间点 (PIT) 快照。

前提条件

1 通过将**高级设置**中的 **vrReplication.preserveMpitImagesAsSnapshots** 选项的值设置为 `true`，将 Site Recovery Manager 配置为保留较旧的 PIT 快照。有关详细信息，请参见更改 vSphere Replication 设置和复制虚拟机并启用多个时间点实例。

2 使用 vSphere Replication 配置虚拟机的复制。

3 将虚拟机添加到 vSphere Replication 保护组并在恢复计划中包含该保护组。

步骤

1 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。

2 在**虚拟机和模板**视图中，右键单击已恢复的虚拟机，然后选择**快照 > 管理快照**。

3 选择此虚拟机的其中一个 PIT 快照，然后单击**恢复到**。

已恢复的虚拟机将恢复到所选的 PIT 快照。

4 （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，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。
- 清理操作将撤消添加或移除存储设备的过程。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 选择**恢复计划**选项卡，右键单击一个恢复计划，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。

禁用存储策略保护组中虚拟机的恢复

您可以禁用存储策略保护组中的虚拟机的恢复，而不将其从保护组中移除。

如果运行的恢复计划无法正确完成，则可以禁用导致错误的虚拟机的恢复。您必须对每个虚拟机分别重复此过程。

前提条件

要使用“禁用恢复”功能，存储策略保护组必须处于“部分已恢复”状态。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**保护组**选项卡，单击存储策略保护组，然后单击**虚拟机**选项卡。

4 选择虚拟机，然后单击**禁用恢复**按钮。

5 单击**是**确认。

结果

下次运行恢复计划时，将跳过虚拟机恢复。

后续步骤

再次运行恢复计划。

禁用存储策略保护组中一致性组的恢复

您可以禁用存储策略保护组中的一致性组的恢复，而不将其从保护组中移除。

如果运行 SPPG 恢复计划时一致性组导致错误，则可以禁用一致性组恢复。您必须对每个一致性组分别重复此过程。

前提条件

要使用“禁用恢复”功能，存储策略保护组必须处于“部分已恢复”状态，并且必须满足以下条件之一：

- 恢复站点上不显示一致性组。
- 恢复站点上显示一致性组，但为空。
- 恢复站点上显示一致性组，但组中的所有虚拟机都存在错误。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 选择**保护组**选项卡，单击存储策略保护组，然后选择**一致性组**选项卡。

4 选择一致性组，然后单击**禁用恢复**按钮。

5 单击**是**确认。

结果

下次运行恢复计划时，将跳过一致性组恢复。

后续步骤

再次运行恢复计划。请参见运行恢复计划。

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。

前提条件

确认没有正在进行的测试恢复或实际恢复。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，然后单击一个恢复计划。

4 （必选） 单击**恢复步骤**选项卡，然后从**查看**下拉菜单中选择恢复步骤模式。

选项	描述
测试步骤	导出测试恢复步骤。
恢复步骤	导出恢复步骤。
清理步骤	导出清理步骤。
重新保护步骤	导出重新保护步骤。

注 根据恢复计划状态，选择恢复步骤模式的选项可能不可用。

5 单击**导出步骤**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。

6 单击**下载**并关闭窗口。

此外，还可以在新选项卡中打开恢复计划步骤报告

查看和导出恢复计划历史记录报告

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。

恢复计划历史记录报告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报告，但历史记录报告始终都只包含已完成操作的条目。如果操作正在执行中，则历史记录报告在该操作完成后才会显示。

Site Recovery Manager 会保留已删除恢复计划的历史记录。可以导出现有计划和已删除计划的历史记录报告。

要导出现有计划的历史记录报告，请执行以下步骤。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 在**站点对**选项卡上，单击**恢复计划历史记录**。
4. （可选） 要导出特定时间段内的整个恢复计划历史记录列表，请单击**全部导出**。
5. （可选） 从恢复计划历史记录列表中选择一项，然后单击**导出报告**以查看特定时间段的恢复计划历史记录、恢复计划运行、测试、清理或重新保护操作。
6. 选择所生成文件的格式，然后单击**下载**或**在新选项卡中打开**。

   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，可将其删除。

前提条件

确认恢复计划处于一致状态。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 单击**恢复计划**选项卡，右键单击要删除的恢复计划，然后单击**删除**。

恢复计划状态概述

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。恢复计划中保护组的状态确定了计划的状态。

表 6-2. 恢复状态

状态	描述
就绪	恢复步骤已清除。 对于存储策略保护组，恢复计划处于此状态时，恢复步骤不显示虚拟机和一致性组。 您可以在**虚拟机**选项卡中验证恢复计划中的受保护虚拟机。
测试正在进行中	取消测试会使计划处于正在取消状态。
测试已完成	测试已完成，存在或没有错误。如果测试期间出现故障，计划将进入“测试已中断”状态。
测试已中断	测试正在运行时服务器出现故障。
正在清理	成功清理后，计划状态变成就绪。 如果清理未完成，则状态为清理未完成。 如果设置了**强制清理**选项，则在出现错误后状态变成就绪。 如果在清理过程中出现故障，则状态将为清理未完成。
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。
正在恢复	如果取消恢复，则状态变成正在取消。
灾难恢复已完成	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。 系统提示裂脑警告并在站点重新连接时再次运行恢复。 站点连接后，状态变成需要恢复 （裂脑）。
恢复已启动	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。 登录到恢复站点或重新连接站点以获取当前状态。
需要恢复 （裂脑）	在恢复过程中站点断开连接。站点重新连接时检测到裂脑情况。 系统提示您再次运行恢复以同步站点。 对于存储策略保护组，恢复计划处于此状态时，恢复步骤不显示虚拟机和一致性组。 您可以在**虚拟机**选项卡中验证恢复计划中的受保护虚拟机。
恢复已完成	如果出错，虚拟机将全部恢复，但存在错误。再次运行恢复不会修复这些错误。 在解决裂脑恢复后，计划转为此状态。 可以查看上次恢复运行的恢复步骤。 对于存储策略保护组，恢复计划处于此状态时，恢复步骤不显示虚拟机和一致性组。 您可以在**虚拟机**选项卡中验证恢复计划中的受保护虚拟机。 在恢复过程中站点断开连接。连接状态是触发此状态的唯一属性。

表 6-2. 恢复状态 （续）

状态	描述
恢复未完成	已取消恢复或数据存储错误。再次运行恢复。 必须解决错误并重新运行恢复，或移除对出现错误的虚拟机的保护。计划检测到通过这两种方式之一解决了错误，并会将状态更新为恢复已完成。
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**运行**继续。无法更改恢复选项。
正在取消	取消测试会导致**测试已完成**状态，并取消上次结果。 取消恢复会导致**恢复未完成**状态，并取消上次结果。 如果在早期取消操作，则可能导致进入**就绪**状态。
正在重新保护	如果在此状态下服务器出现故障，则会变成**重新保护已中断**状态。
部分重新保护	已重新保护重叠计划。 已重新保护的组变成**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。
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。 重新保护完成了存储操作，但未完成创建卷影虚拟机的操作。即使运行虚拟机的站点已断开连接，您也可以再次运行重新保护，然后再立即进行恢复。
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。
正在等待用户输入	测试已暂停。关闭该提示以恢复测试。 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	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。 等待其他计划完成测试、清理或编辑计划以移除这些组。
方向错误	组处于混合状态下，这是一种无效状态。计划包含相反方向就绪的不同组。选择一个方向作为正确方向，并移除相反方向的保护组。 对于出现的此错误，重叠计划已运行且已重新保护计划中的一部分组。
正在删除	等待删除对等计划时，计划进入此短暂的状态。删除另一计划时计划自动完成。

表 6-2. 恢复状态 （续）

状态	描述
计划不同步	此状态可能在不同情况下出现： ■ 在成功测试恢复和清理操作之间。如果您无法编辑处于此状态的计划，请运行清理以将此计划恢复为就绪状态。要允许清理，可能需要在另一个站点的 VMware Site Recovery 用户界面中打开该计划。如果计划仍处于计划不同步状态，请编辑该计划。 ■ 在常规操作过程中，可以编辑计划。 打开计划进行编辑后，保存更改会导致 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。
无保护组	计划不包含任何保护组，因而计划无法运行。 可以编辑包括恢复站点的计划。 可以通过 API 或 UI 或通过删除保护组来创建空计划。
内部错误	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。 无法运行计划，但可以删除计划。

配置恢复计划

7

您可以配置恢复计划以在 Site Recovery Manager Server 或虚拟机上运行命令、显示计划在 Site Recovery Manager Server 上或客户机操作系统中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。

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。

恢复计划正在运行时，其状况反映了恢复计划运行的状况，而不是所包含的保护组的状况。

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。
- 有些步骤仅针对延伸存储运行。

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，Site Recovery Manager 将执行以下操作：

1 Site Recovery Manager 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 在测试恢复计划时跳过此步骤。

2 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。

恢复过程中，将忽略不同优先级组中虚拟机之间的依赖关系。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。

针对延伸存储的恢复步骤

恢复计划向导提供了一个选项：使用 vSphere vMotion 对受保护站点中驻留在延伸存储上的所有受保护且已打开电源的虚拟机执行故障切换。选中此选项后，恢复过程中将在关闭受保护站点虚拟机电源前执行其他两个步骤。

- **为虚拟机迁移准备存储**。Site Recovery Manager 将每个一致性组的首选项更改为恢复站点。
- **迁移虚拟机**。如果未打开生产虚拟机的电源，则该步骤将失败。如果已打开生产虚拟机的电源，则 Site Recovery Manager 将启动 vSphere vMotion 以将虚拟机迁移到恢复站点。

小心 如果符合迁移条件的虚拟机的优先级低于不符合条件的虚拟机或者依赖不符合条件的虚拟机，则不会迁移这些虚拟机。

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。

添加自定义恢复步骤后，将在测试工作流和运行工作流之间共享这些步骤。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。

但是，如果某些自定义步骤运行包含站点特定的信息（如网络配置）的命令，则可能需要在重新保护之后修改这些步骤。

可以在恢复计划步骤中配置命令和提示，表示某个特定操作已完成。您无法在“配置测试网络”步骤前添加命令或提示。

您无法向以下与存储策略保护组相关的顶级步骤添加命令或提示：

- 完成存储一致性组测试恢复

- 完成虚拟机测试恢复
- 完成保护组测试恢复
- 完成保护组实时迁移
- 完成受保护站点上的保护组操作
- 完成存储一致性组恢复
- 完成虚拟机恢复
- 完成保护组恢复

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

顶级命令在 Site Recovery Manager Server 上运行。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，可以使用这些命令执行配置任务。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。您可能需要更改已恢复虚拟机上的 VMware Tools 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。

命令和提示的执行步骤

对于存储策略保护组，如果在第一优先级虚拟机之前添加命令或提示，则 Site Recovery Manager 会在所有虚拟机完成**应用虚拟机策略**步骤之后运行此命令或提示。

对于基于阵列的复制保护组和 vSphere Replication 保护组，在**创建可写存储快照**和第一个非空虚拟机优先级组之间添加的第一个命令或提示（或自定义步骤）将与**创建可写存储快照**步骤同时启动，以解决重新启动故障情形。

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**恢复步骤**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。恢复计划会暂停，直到关闭提示。

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、脚本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。

适用于 Windows 的 Site Recovery Manager

- 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 4 KB 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。

Site Recovery Manager Appliance

- 必须将脚本复制到**管理员**用户的主目录 `/home/admin` 中。

- 必须更改脚本的访问权限，**srm** 用户才可运行该脚本。例如，对于 bash 脚本，请使用以下命令行：

```
chmod 755 Myscript.sh
```

- 运行脚本时，必须使用本地主机上的完整路径。例如，要运行 bash 脚本，请使用以下命令：

```
/bin/sh /home/admin/Myscript.sh
```

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。

Site Recovery Manager Server 上的命令步骤以 Site Recovery Manager 服务帐户的身份运行。在默认配置中，已恢复虚拟机上的命令步骤以 VMware Tools 服务帐户的身份运行。可以更改与 **recovery.autoDeployGuestAlias** 设置兼容的虚拟机的默认配置。有关 **recovery.autoDeployGuestAlias** 设置的信息，请参见更改恢复设置。

Site Recovery Manager 仅在命令步骤的持续期间设置环境变量。完成此命令后，Site Recovery Manager Server 和已恢复虚拟机的客户机操作系统中都不会存在特定的环境变量。

表 7-1. 可用于所有命令步骤的环境变量

名称	值	示例
VMware_RecoveryName	正在运行的恢复计划的名称。	计划 A
VMware_RecoveryMode	恢复模式。	测试或恢复
VMware_VC_Host	恢复站点中 vCenter Server 的主机名。	vc_hostname.example.com
VMware_VC_Port	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 7-2. 可用于每个虚拟机命令步骤的环境变量

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

表 7-3. 在已恢复虚拟机上运行每个虚拟机命令步骤时可用的环境变量

名称	值与描述	示例
VMware_GuestOp_OutputFile	该值为命令输出文件的路径。 如果命令可以创建文件，Site Recovery Manager 会下载该文件的内容，并将其作为结果添加到恢复计划历史记录和服务器日志。 Site Recovery Manager 会将命令输出文件的最后 4 KB 添加到恢复计划历史记录和服务器日志。如果脚本生成的输出大于 4 KB，则该输出必须记录在自定义位置。 命令完成后，Site Recovery Manager 将删除命令输出文件。	`C:\Windows\TEMP\vmware0\srmStdOut.log`

示例： 可在 Site Recovery Manager 上运行的命令

对于适用于 Windows 的 Site Recovery Manager，可以创建包含以下内容的 `myServerScript.bat` 文件。

```
@echo off
echo %DATE% %TIME% : Recovery Plan %VMware_RecoveryName% ran in %VMware_RecoveryMode% mode"
:: some more custom actions
```

要运行 `myServerScript.bat` 文件，请使用以下命令内容。

```
C:\Windows\System32\cmd.exe /c C:\myScripts\myServerScript.bat > %VMware_GuestOp_OutputFile%
2>&1
```

对于 Site Recovery Manager Appliance，可以创建包含以下内容的 `myServerScript.sh` 脚本。

```
clear
echo "$(date "+%Y-%m-%d %H:%M:%S") : Recovery Plan $VMware_RecoveryName ran in
$VMware_RecoveryMode mode"
# some more custom actions
```

注 在脚本中编写命令时，请勿使用竖线 (|) 和单引号 (') 符号。

要运行 `myServerScript.sh` 文件，请使用以下命令内容。

```
/bin/sh /home/admin/myServerScript.sh
```

示例： 在已恢复虚拟机上运行的命令内容

对于 Windows 客户机操作系统，可以创建包含以下内容的 `myGuestScript.bat` 文件。

```
@echo off
echo %DATE% %TIME% : VM %VMware_VM_Name% recovered by RP %VMware_RecoveryName% ran in
%VMware_RecoveryMode% mode
echo %DATE% %TIME% : Configured with the following FQDN: %VMware_VM_GuestName% and IP:
%VMware_VM_GuestIp%
:: some more custom actions
```

要运行 myGuestScript.bat，请使用以下命令内容。

```
C:\Windows\System32\cmd.exe /c C:\myScripts\myGuestScript.bat > %VMware_GuestOp_OutputFile%
2>&1
```

对于 Linux 或 UNIX 客户机操作系统，可以创建包含以下内容的 myGuestScript.sh 文件。

```
echo $(date) : VM $VMware_VM_Name recovered by $VMware_RecoveryName ran
echo $(date) : Configured with the following FQDN: $VMware_VM_GuestName and IP:
$VMware_VM_GuestIp
# some more custom actions
```

要运行 myGuestScript.sh 文件，请使用以下命令内容。

```
/bin/sh myGuestScript.sh &>$VMware_GuestOp_OutputFile
```

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。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 在**恢复计划**选项卡上，选择一个恢复计划，然后单击**恢复步骤**。
4. 使用**查看**下拉菜单选择要添加的步骤类型。

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	添加执行计划内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。

5. 选择添加该步骤的位置。
   - 要将步骤添加在某步骤的前面，请右键单击该步骤并选择**在以下内容之前添加步骤:**。
   - 要将步骤添加在最后一步的后面，请右键单击最后一步并选择**在以下内容之后添加步骤:**。
6. 选择**对 SRM Server 的命令**或**提示**。
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，输入命令、脚本或消息提示。

- 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。

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**添加**以将步骤添加到恢复计划。

后续步骤

您可以右键单击新创建的步骤并选择编辑、删除或在该步骤前后添加步骤的选项。

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。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在**恢复计划**选项卡上，选择一个恢复计划，然后单击**恢复步骤**。

4 右键单击虚拟机，然后单击**配置恢复**。

5 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**。

6 单击加号图标以添加步骤。

7 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。

8 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。

9 在**内容**文本框中，输入命令、脚本或消息提示。

- 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。

10 （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。

11 要将步骤添加到恢复计划，请单击**添加**。

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

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以及在恢复站点上运行非关键工作负载的情况下，挂起恢复站点上的虚拟机非常有用。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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，单击一个恢复计划，然后单击**恢复步骤**。

4 右键单击**挂起恢复站点上的非关键虚拟机**，然后单击**添加或移除非关键虚拟机**。

5 选择恢复站点上要在恢复期间挂起的虚拟机。

6 单击**保存**。

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。恢复优先级确定了虚拟机的关机和打开电源顺序。

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。

小心　如果符合延伸存储迁移条件的虚拟机的优先级低于不符合延伸存储迁移条件的虚拟机，则不会迁移符合条件的虚拟机。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 单击**恢复计划**选项卡，单击一个恢复计划，然后单击**虚拟机**。
4. 右键单击虚拟机并单击**优先级组**。
5. 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。
6. 要确认优先级更改，请单击**是**。

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。

小心　如果符合延伸存储迁移条件的虚拟机所依赖的虚拟机不符合延伸存储迁移条件，将不迁移这些虚拟机。

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。如果将虚拟机配置为依赖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包含所依赖虚拟机的保护组，则在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。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

确认具有依赖关系的虚拟机及其依赖的虚拟机位于同一恢复计划和同一恢复优先级组中。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，单击一个恢复计划，然后单击**虚拟机**。

4 右键单击依赖一台或多台其他虚拟机的虚拟机，然后单击**配置恢复**。

5 展开**虚拟机依赖关系**。

6 从下拉菜单中选择**查看全部**。

7 从选定恢复计划的所有虚拟机列表中选择一个或多个虚拟机。

所选虚拟机将添加到依赖关系列表中。

8 验证**虚拟机依赖关系**列表中的虚拟机是否已打开电源，以及依赖关系状态是否为**良好**。

9 （可选） 要移除依赖关系，从下拉菜单中选择**查看虚拟机依赖关系**，从此虚拟机依赖的虚拟机列表中选择一个虚拟机，然后单击**移除**。

10 单击**确定**。

对计划的迁移启用 vSphere vMotion

虚拟机的 vSphere vMotion 迁移仅适用于计划的迁移。可以在**恢复属性**对话框中启用或禁用 vSphere vMotion。

前提条件

- 在执行 vSphere vMotion 迁移之前，请确认虚拟机属于存储策略保护组，位于延伸存储上且已打开电源。
- 确保您已配置完整的清单映射。如果您仅配置了临时占位符清单映射并使用**启用符合条件虚拟机的 vMotion** 选项运行计划的迁移，计划的迁移将失败，即使两个站点均在运行也是如此。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，单击一个恢复计划，然后单击**虚拟机**选项卡。

4 右键单击虚拟机，然后单击**配置恢复**。

选择**对计划的迁移使用 vMotion (虚拟机应该打开电源)**。

5 单击**确定**。

结果

计划迁移期间不会重新启动。将忽略配置的关机或启动操作或者在打开电源之前配置的步骤。将运行打开电源后配置的步骤。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，单击一个恢复计划，然后单击**虚拟机**。

4 右键单击虚拟机，然后单击**配置恢复**。

5 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。此选项需要在虚拟机上运行 VMware Tools。 **注** 当超过超时时间时，虚拟机将关闭电源。如果虚拟机的操作系统在超过超时时间后仍未完成关闭任务，可能会导致数据丢失。对于需要较长时间才能正常关闭的大型虚拟机，设置较长的关闭电源超时。
关闭电源	关闭虚拟机电源，但不关闭客户机操作系统。

6 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。

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

此选项仅在步骤 6 中选择了**打开电源**时可用。

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

8 （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 6 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。

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 将还原保存的内存状态，以便虚拟机可继续运行，而不会对其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。

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。仅当受保护虚拟机上启用了**预留所有客户机内存 (全部锁定)** 设置时例外。

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。

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，有关如何存储使用基于阵列的复制保护的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。一个虚拟机不能同时属于两个阵列对，所以如果某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。

自定义虚拟机的 IP 属性

8

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。

> **注** 每个网卡只配置一个 IP 地址。

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 Site Recovery Manager 8.2 兼容性列表，网址为 https://docs.vmware.com/cn/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.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。

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。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 单击**恢复计划**选项卡，单击一个恢复计划，然后单击**虚拟机**。

4 右键单击虚拟机，然后单击**配置恢复**。

5 单击 **IP 自定义**选项卡，然后从下拉菜单中选择**手动 IP 自定义**。

6 选择要修改 IP 设置的网卡。

7 针对受保护站点或恢复站点单击**配置**，具体取决于要配置的 IP 设置集。

8 要配置 IPv4 设置，请单击 **IPv4** 选项卡。

   - 选择 DHCP，或者针对静态地址，输入 IP 地址、子网信息和网关服务器地址。
   - 如果虚拟机已打开电源且已安装 VMware Tools，则可以单击**检索**以导入在虚拟机上配置的当前设置。

9 要配置 IPv6 设置，请单击 **IPv6** 选项卡。

   - 选择 DHCP，或者针对静态地址，输入 IP 地址、子网信息和网关服务器地址。
   - 如果虚拟机已打开电源且已安装 VMware Tools，则可以单击**检索**以导入在虚拟机上配置的当前设置。

10 要配置 DNS 设置，请单击 **DNS** 选项卡。

- **表 8-1. DNS 设置**

设置	选项
DNS 服务器	选择查找 DNS 服务器的方式： ■ 使用 DHCP 自动获取 DNS 地址。 ■ 指定首选和备用 DNS 服务器。
DNS 后缀	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**。

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

11 （必选） 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。

12 重复步骤 7 到步骤 10 以配置恢复站点或受保护站点设置（如有必要）。

13 根据需要对其他网卡重复配置过程。

结果

恢复期间应用恢复站点设置。故障恢复期间应用受保护站点设置。

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。

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 并为虚拟网络配置 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 Site Recovery Manager 8.2 兼容性列表，网址为 https://docs.vmware.com/cn/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.html。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 选择**恢复计划**选项卡，单击一个恢复计划，然后选择**虚拟机**。

4 右键单击虚拟机，然后单击**配置恢复**。

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**。

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。

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 在受保护的虚拟机上再次运行 DR IP Customizer 以应用 CSV，其中包含虚拟机在恢复站点上启动时要应用的经修改的网络配置。

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 Site Recovery Manager 8.2 兼容性列表，网址为 https://docs.vmware.com/cn/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.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，会提示您提供每个站点的 vCenter Server 登录凭据。

步骤

1 登录到受保护站点或恢复站点中的 Site Recovery Manager Server 主机，然后打开命令提示符。

2 将工作目录更改为：

   - 对于 Windows：`C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`。
   - 对于 Linux：`/opt/vmware/srm/bin/`。

3 运行 `dr-ip-reporter` 命令。

   - 如果某个 Platform Services Controller 具有单个 vCenter Server 实例，请运行以下命令：
     - 对于 Windows：

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

- 对于 Linux：

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out path_to_report_file.xml
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

该示例将 `dr-ip-reporter` 指向 Site Recovery Manager Server 的 `vmware-dr.xml` 文件，并针对位于 https://*Platform_Services_Controller_address* 的与 Platform Services Controller 相关的 vCenter Server 实例生成报告文件。

- 如果 Platform Services Controller 包括多个 vCenter Server 实例，则必须在 `--vcid` 参数中指定 vCenter Server ID。
  - 对于 Windows：

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

  - 对于 Linux：

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

该示例将 `dr-ip-reporter` 指向 Site Recovery Manager Server 的 `vmware-dr.xml` 文件，并为 ID 为 *vCenter_Server_ID* 的 vCenter Server 实例生成报告文件。

注 vCenter Server ID 与 vCenter Server 名称不同。

- 要将网络列表限制为仅包含特定恢复计划所需的网络，请在命令行中包含 `--plan` 选项：
  - 对于 Windows：

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--plan recovery_plan_name
```

  - 对于 Linux：

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--plan recovery_plan_name
```

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 通过 Site Recovery Manager，可以定义子网级别的 IP 映射规则，以使用 DR IP Customizer 工具自定义虚拟机上的 IP 设置。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。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则会在 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`。
- 如果使用的是 Site Recovery Manager Virtual Appliance，则 `dr-ip-customizer` 位于设备上的 `/opt/vmware/srm/bin/` 目录中。

运行 `dr-ip-customizer.exe` 或 `dr-ip-customizer` 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 Server 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 ]
--uri https://host[:port]/lookupservice/sdk
--vcid  UUID
[--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 8-2. DR IP Customizer 选项

选项	描述	必选
`-h [ --help ]`	显示有关 `dr-ip-customizer.exe` 或 `dr-ip-customizer` 的使用情况信息。	不支持
`--cfg arg`	应用程序 XML 配置文件 `vmware-dr.xml` 的路径。	是

表 8-2. DR IP Customizer 选项 （续）

选项	描述	必选
`--cmd arg`	您可以指定不同的命令以便在不同的模式中运行 DR IP Customizer。 ■ `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。 ■ `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。 ■ `drop` 命令从输入 CSV 文件所指定的虚拟机中删除恢复设置。 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。	是
`--csv arg`	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。
`--uri arg`	Platform Service Controller 上的 Lookup Service URL，形式为：`https://host[:port]/lookupservice/sdk` 。如果端口不是 443，请指定端口。Site Recovery Manager 实例将此地址与主站点的基础架构节点关联。 对于 `apply` 和 `drop` 命令，使用生成 CSV 文件所使用的同一个 vCenter Server 实例。	是
`--vcid arg`	主站点 vCenter Server 实例 UUID。	可选，除非主站点基础架构包含多个 vCenter Server 实例。
`-i [ --ignore-thumbprint ]`	忽略 vCenter Server 指纹确认提示。	不支持
`-e [ --extra-dns-columns ]`	如果输入 CSV 文件包含额外的 DNS 信息列，则必须指定此选项。	不支持
`-v [ --verbose ]`	启用详细输出。可在任何 `dr-ip-customizer.exe` 或 `dr-ip-customizer` 命令行中包含 `--verbose` 选项以记录额外的诊断消息。	不支持

未指定 `--vcid` 值时，该工具便会将 UUID 输出到 Lookup Service，如以下示例所示：

- 对于 Windows：

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\config\vmware-dr.xml" -i --cmd generate -o "c:\tmp\output.csv" --uri
https://service.company.com:443/lookupservice/sdk --vcid ?
```

- 对于 Linux：

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml" -i --cmd
generate -o "/home/admin/output.csv" --uri
https://service.company.com:443/lookupservice/sdk --vcid ?
```

生成的错误消息包括 vCenter Server 实例 UUID，后跟每个注册到 Lookup Service 的 vCenter Server 的 vCenter Server DNS 主机名。

错误：找不到 VC 实例。请使用以下已知的 VC 实例之一：e07c907e-cd41-4fe7-b38a-f4c0e677a18c vc.company.com (ERROR: Failed to locate VC instance. Use one of the following known VC instances: e07c907e-cd41-4fe7-b38a-f4c0e677a18c vc.company.com)

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 通过 Site Recovery Manager，可以定义子网级别的 IP 映射规则，以使用 DR IP Customizer 工具自定义虚拟机上的 IP 设置。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。

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 8-3. 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。该标识符与 vCenter Server 使用的虚拟机 ID（如果存在）相同，否则为 BIOS ID。	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。

表 8-3. DR IP Customizer CSV 文件的列 （续）

列	描述	自定义规则
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。 ■ 一行包含所有虚拟机信息和一台 DNS 主机。 ■ 另一行只包含第二台 DNS 主机。 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。
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 **`example.company.com`**。
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。
次要 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。
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。如果该字段未设置为特定静态地址，则必须将其设置为 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。

表 8-3. DR IP Customizer CSV 文件的列 （续）

列	描述	自定义规则
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。 虚拟机可以具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 IPv6 地址。如果该字段未设置为特定静态地址，则必须将其设置为 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 IPv6 网关。	可自定义。可以留空。
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 通过 Site Recovery Manager，可以定义子网级别的 IP 映射规则，以使用 DR IP Customizer 工具自定义虚拟机上的 IP 设置。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。

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，并在这一列的该行中填写值。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` 或 `dr-ip-customizer`，获取包含 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 通过 Site Recovery Manager，可以定义子网级别的 IP 映射规则，以使用 DR IP Customizer 工具自定义虚拟机上的 IP 设置。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。

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)
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-B,0,,,,,,,,,,,
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-A,0,,,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,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 8-4. 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
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com

表 8-4. 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
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
103b9e8b-1f90-faca-8028-13820b8f236e		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 8-5. 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
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com

表 8-5. 在修改的 CSV 文件中设置静态 IPv4 地址和 DHCP 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
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			dhcp				
103b9e8b-1f90-faca-8028-13820b8f236e		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 8-6. 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
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0										example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0										eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e		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

表 8-6. 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
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0										eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1									::ffff:192.168.0.251	
103b9e8b-1f90-faca-8028-13820b8f236e		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				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 通过 Site Recovery Manager，可以定义子网级别的 IP 映射规则，以使用 DR IP Customizer 工具自定义虚拟机上的 IP 设置。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。

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。
- 如果使用的是适用于 Windows 的 Site Recovery Manager，用于运行 DR IP Customizer 工具的用户帐户至少需要具有 Site Recovery Manager 恢复计划管理员角色。
- 如果使用的是 Site Recovery Manager Virtual Appliance，则必须以管理员用户身份使用 SSH。

步骤

1 登录到 Site Recovery Manager Server 主机并打开命令 shell。

2 将工作目录更改为：
  - 对于 Windows：`C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`。
  - 对于 Linux：`/opt/vmware/srm/bin/`。

3 运行 `dr-ip-customizer` 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。
  - 如果 Platform Services Controller 具有单个 vCenter Server 实例

    对于 Windows，运行以下命令：

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\config\vmware-dr.xml"
--cmd generate --out "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

对于 Linux，运行以下命令：

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd generate --out "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

该示例将 `dr-ip-customizer` 指向 Site Recovery Manager Server 的 `vmware-dr.xml` 文件，并针对位于 https://*Platform_ Services_ Controller_ address* 的与 Platform Services Controller 相关的 vCenter Server 实例生成 CSV 文件。

- 如果某个 Platform Services Controller 具有多个 vCenter Server 实例，则必须在 `--vcid` 参数中指定 vCenter Server ID。如果不指定 `--vcid`，或提供的 ID 不正确，则工具会列出所有可用的 vCenter Server 实例。

  对于 Windows，运行以下命令：

  ```
  dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
  Manager\config\vmware-dr.xml"
  --cmd generate --out "C:\tmp\output.csv"
  --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
  --vcid vCenter_Server_ID
  ```

  对于 Linux，运行以下命令：

  ```
  /opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
  --cmd generate --out "/home/admin/output.csv"
  --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
  --vcid vCenter_Server_ID
  ```

  该示例将 `dr-ip-customizer` 指向 Site Recovery Manager Server 的 `vmware-dr.xml` 文件，并为 ID 为 *vCenter_ Server_ ID* 的 vCenter Server 实例生成 CSV 文件。

  注 vCenter Server ID 与 vCenter Server 名称不同。

4 （必选） 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` 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。

- 如果 Platform Services Controller 具有单个 vCenter Server 实例

对于 Windows，运行以下命令：

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\config\vmware-dr.xml"
--cmd apply --csv "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

对于 Linux，运行以下命令：

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd apply --csv "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

该示例将 `dr-ip-customizer` 指向 Site Recovery Manager Server 的 `vmware-dr.xml` 文件，并将 CSV 文件中的自定义内容应用到位于 https://*Platform_Services_Controller_address* 的与 Platform Services Controller 相关的 vCenter Server。

- 如果某个 Platform Services Controller 具有多个 vCenter Server 实例，则必须在 `--vcid` 参数中指定 vCenter Server ID。

  对于 Windows，运行以下命令：

  ```
  dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
  Manager\config\vmware-dr.xml"
  --cmd apply --csv "C:\tmp\output.csv"
  --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
  --vcid vCenter_Server_ID
  ```

  对于 Linux，运行以下命令：

  ```
  /opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
  --cmd apply --csv "/home/admin/output.csv"
  --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
  --vcid vCenter_Server_ID
  ```

  该示例将 `dr-ip-customizer` 指向 Site Recovery Manager Server 的 `vmware-dr.xml` 文件，并将 CSV 文件中的自定义内容应用到 ID 为 *vCenter_Server_ID* 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。
- 将 IP 子网映射规则应用到已启用 IPv6 的 Windows 虚拟机时，IPv6 设置（DHCP 或静态）在恢复后不受影响。对于 Linux 虚拟机，IPv6 设置将重置为 DHCP。
- 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为 10.17.23.1，则新网关为 10.18.22.1。如果指定明确的网关参数，Site Recovery Manager 会检查 IPv4 地址语法是否正确并严格应用该参数。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 在**站点对**选项卡上，单击**配置 > 网络映射**。
4. 选择要定义自定义规则的网络映射。
5. 要定义规则，请单击**添加 IP 自定义规则**。
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**添加**以保存更改。

恢复后重新保护虚拟机

9

执行恢复后，恢复站点将成为主站点，但是虚拟机尚未受到保护。如果原始受保护站点处于运行状态，则可以反转保护方向，将原始受保护站点用作新的恢复站点。

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，虚拟机将在恢复站点上启动。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。

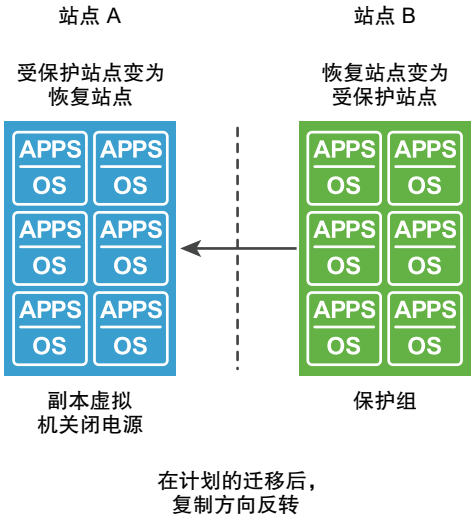
您可以针对包含基于阵列的复制保护组、vSphere Replication 保护组和存储策略保护组的恢复计划执行重新保护。

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工作流，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 9-1. 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。

- Site Recovery Manager 如何使用存储策略保护来重新保护虚拟机

  在使用存储策略保护进行重新保护的过程中，Site Recovery Manager 会反转保护方向，并保护之前的恢复站点上与相关存储策略关联的虚拟机。Site Recovery Manager 在新的受保护站点上重新建立 vSphere 实体保护和监控。

- 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。

- 重新保护状态概述

  重新保护过程可经历几个状态，您可以在 Site Recovery 用户界面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（即执行重新保护操作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。

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。

如果要在 vSphere Replication 保护的虚拟机上手动设置反向复制，请使用 Site Recovery 用户界面强制停止旧恢复站点（即新的受保护站点）上的入站复制组。如果您仅删除原始受保护站点上的虚拟机，重新保护将失败。

Site Recovery Manager 如何使用存储策略保护来重新保护虚拟机

在使用存储策略保护进行重新保护的过程中，Site Recovery Manager 会反转保护方向，并保护之前的恢复站点上与相关存储策略关联的虚拟机。Site Recovery Manager 在新的受保护站点上重新建立 vSphere 实体保护和监控。

存储策略保护组的反向复制与基于阵列的复制保护组的反向复制相同，因为它仅影响基础存储。当您在包含存储策略保护组的恢复计划中执行重新保护时，您的存储阵列提供的复制技术将对与保护组中所包含存储策略相关的所有一致性组进行反向复制。

如果存储阵列无法对保护组中的任何一致性组进行反向复制，恢复计划将进入“重新保护未完成”状态。在此状态下，您必须解决存储问题并再次运行重新保护。对存储策略保护组重新运行重新保护仅影响之前未成功完成的重新保护操作的一致性组的复制方向。

当存储阵列已反转复制方向时，Site Recovery Manager 将重新建立 vSphere 实体保护和监控。在重新保护期间重新建立 vSphere 实体保护和监控的条件没有在创建存储策略保护组时建立 vSphere 实体保护和监控的条件那么严格：

- Site Recovery Manager 检查新的受保护站点上的存储策略是否合规。如果新的受保护站点上的存储策略不合规，重新保护不会失败，但 Site Recovery Manager 无法保护与该存储策略相关的虚拟机。有关合规性的信息，请参见存储策略保护组的必备条件和存储策略保护组的限制。
- Site Recovery Manager 在新的受保护站点上重新启动 vSphere 实体监控。
- Site Recovery Manager 开始保护所有合规的虚拟机。这可能不是您最初运行恢复计划时恢复的相同虚拟机集，因为您或其他用户可能已将更多的虚拟机与新的受保护站点上的存储策略关联起来。如果 Site Recovery Manager 无法保护新的受保护站点上的虚拟机，重新保护也不会失败。
- 存储策略保护组已准备好从新的受保护站点恢复到新的恢复站点。

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。

您可以针对包含基于阵列的复制保护组、vSphere Replication 保护组和存储策略保护组的恢复计划执行重新保护。

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，请解决导致这些错误的问题，然后重新运行恢复。在重新运行恢复时，将跳过先前已成功完成的操作。例如，已成功恢复的虚拟机将不会重新进行恢复，将无中断地继续运行。
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均可恢复。
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。如果在尝试计划迁移期间出错，则必须更正错误并重新运行计划迁移，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，这两个站点必须均可用。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工作流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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 单击**恢复计划**选项卡，右键单击一个恢复计划，然后单击**重新保护**。
4. 选中用于确认您了解重新保护操作不可逆的复选框。
5. （可选） 要在恢复站点上执行清理操作期间忽略错误，请选中**强制清理**复选框，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。
6. 查看重新保护信息，然后单击**完成**。
7. 要监控重新保护操作的进度，请选择恢复计划，然后单击**恢复步骤**选项卡。
8. 重新保护操作完成后，选择恢复计划，单击**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。

重新保护状态概述

重新保护过程可经历几个状态，您可以在 Site Recovery 用户界面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 9-1. 重新保护状态

状态	描述	补救措施
正在重新保护	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且部分保护组已成功在其他计划中受到重新保护，则会出现此状况。	在部分重新保护的计划中重新运行重新保护。

表 9-1. 重新保护状态 （续）

状态	描述	补救措施
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，如果执行反向复制失败或创建占位虚拟机失败，则可能出现此状态。	■ 如果重新保护操作无法执行反向复制，请确保站点处于连接状态，在 Site Recovery UI 中查看重新保护进度，然后重新启动重新保护任务。如果重新保护仍然不成功，请使用**强制清理**选项运行重新保护任务。 ■ 如果 Site Recovery Manager 创建占位虚拟机失败，则仍可进行恢复。在 Site Recovery 用户界面中查看重新保护步骤，解决任何问题，然后重新运行重新保护。
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。
就绪	重新保护成功完成后会出现。	无。

通过执行故障恢复来还原恢复前的站点配置

10

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 9 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内迁移操作。

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 要关闭受保护站点上的虚拟机和启动恢复站点上的虚拟机，请执行计划的迁移。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。

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。

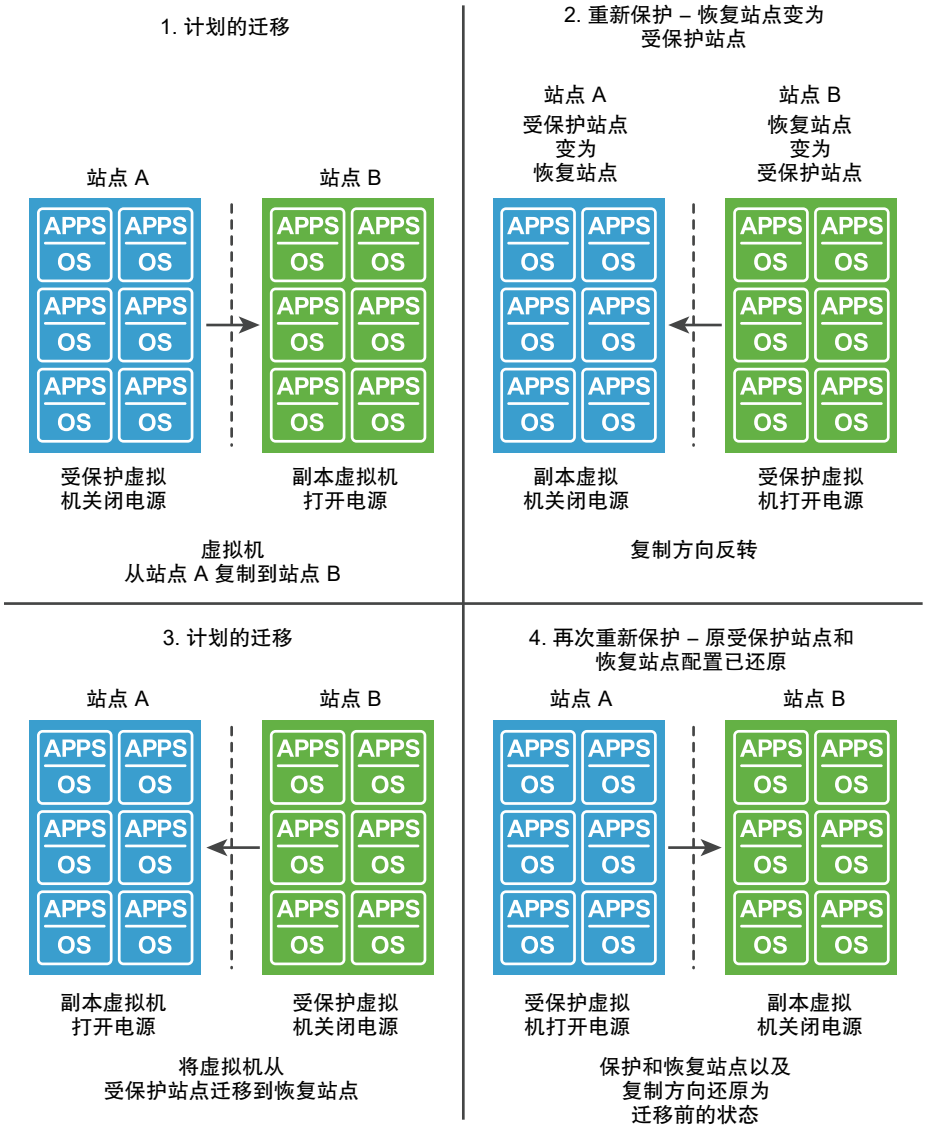
1 虚拟机将执行从站点 A 到站点 B 的复制。

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 要将站点 B 上的受保护虚拟机恢复到站点 A，请执行计划的迁移。

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 10-1. 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。

从站点 A 恢复到站点 B 后，已恢复的虚拟机将在站点 B 上运行，但不受保护。

前提条件

- 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。

- 自恢复后尚未运行重新保护。
- 如果已执行灾难恢复，则当原始受保护站点中的主机和数据存储再次运行时必须执行计划的迁移。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在**恢复计划**选项卡上，右键单击一个恢复计划，然后单击**重新保护**。

4 选中用于确认您了解重新保护操作不可逆的复选框。

5 确定是否启用**强制清理**并单击**下一步**。

仅当运行了一次重新保护并出现错误时，**强制清理**才可用。启用该选项将强制移除虚拟机、忽略错误，并使恢复计划恢复为就绪状态。

6 查看重新保护信息，然后单击**完成**。

7 选择恢复计划，并单击**恢复步骤**以监控重新保护操作直至完成。

8 （必选） 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。

9 要使恢复计划作为计划的迁移运行，请右键单击恢复计划，然后单击**恢复**。

10 选择恢复计划并单击**恢复步骤**以监控计划迁移直至完成。

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单击**重新保护**，然后按照向导说明再次执行重新保护操作。

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

11

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 和 vSphere Storage DRS。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
- 让 Site Recovery Manager 与 VMware vSAN 存储和 vSphere Replication 协同工作
- 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 如何与延伸存储交互
- 将 Site Recovery Manager 与 NSX Data Center for vSphere 结合使用
- Site Recovery Manager 和 vSphere PowerCLI
- Site Recovery Manager 和虚拟机加密
- Site Recovery Manager 和 vRealize Orchestrator
- 保护 Microsoft 群集服务器和容错虚拟机
- 结合使用 Site Recovery Manager 与 SIOC 数据存储
- 将 Site Recovery Manager 与接入控制群集结合使用
- Site Recovery Manager 和附加到 RDM 磁盘设备的虚拟机
- Site Recovery Manager 和 Active Directory 域控制器

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，因此必须先在站点上安装并配置 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。

对于基于阵列的复制和 vSphere Replication，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。

注 存储策略保护组处理更改的方式有所不同。请参见存储策略保护组的清单映射 。

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。

让 Site Recovery Manager 与 VMware vSAN 存储和 vSphere Replication 协同工作

您可以对 Site Recovery Manager 和 vSphere Replication 使用 VMware vSAN 存储。

Site Recovery Manager 支持对 vSphere Replication 使用 vSAN。无法对基于阵列的复制使用 vSAN 存储。

有关 vSphere Replication 和 vSAN 兼容版本的信息，请参见 VMware 产品互操作性列表，网址为 https://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

有关对 vSAN 使用 vSphere Replication 的信息，请参见《vSphere Replication 管理》中的将 vSphere Replication 与 VMware vSAN 存储结合使用。

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。

有关 Site Recovery Manager 如何处理 Storage DRS 的数据存储标记的信息，请参见 http://kb.vmware.com/kb/2108196。

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。

- Storage DRS 在计算放置位置建议以执行自动或手动迁移时考虑数据存储的保护和复制状态。Storage DRS 检查数据存储是否已复制以及是一致性组还是保护组的一部分，然后相应地对数据存储进行标记。有关 Site Recovery Manager 如何处理数据存储标记的详细信息，请参见 http://kb.vmware.com/kb/2108196。
- Site Recovery Manager 支持包含不同一致性组中的数据存储的 Storage DRS 群集。如果将虚拟机迁移至不是保护组一部分的数据存储，则需要将保护组重新配置为包含该数据存储。
- Site Recovery Manager 不受限制地在同一一致性组中的非复制数据存储之间以及复制数据存储之间支持 Storage vMotion。在这些情况下，Storage DRS 可以在处于自动模式的群集中执行自动 Storage vMotion，也可以针对处于手动模式的群集中的 Storage vMotion 发出建议。
- 对于复制数据存储与非复制数据存储之间的 Storage vMotion，或不同一致性组中复制数据存储之间的 Storage vMotion，需要考虑特殊的注意事项。在这些情况下，Storage DRS 不会自动启动或建议 Storage vMotion。手动启动的 Storage vMotion 会导致详述可能的影响的警告。
- 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，您可能会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的过程中，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。

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

如果使用 vSphere Replication 保护或恢复使用 Storage DRS 或 Storage vMotion 的站点上的虚拟机，请遵循以下准则。

- vSphere Replication 在受保护站点和恢复站点上均与 vSphere Storage DRS 兼容。在受保护站点上，您可以使用 Storage DRS 移动 vSphere Replication 保护的虚拟机的磁盘文件，这不会对正在进行的复制产生任何影响。在恢复站点上，您必须向 vCenter Single Sign-On 服务注册 vSphere Replication 设备，以便 Storage DRS 识别 Storage DRS 群集上的副本磁盘文件并生成迁移建议。您可以使用 Storage DRS 迁移副本磁盘文件，这不会对后续恢复产生任何影响。有关详细信息，请参见 vSphere Replication 文档中的“向 vCenter Single Sign-On 注册 vSphere Replication 设备”。
- vSphere Replication 在受保护站点上与 Storage vMotion 兼容。在受保护站点上，您可以使用 Storage vMotion 移动已复制的虚拟机的磁盘文件，这不会对正在进行的复制产生任何影响。
- Site Recovery Manager 成功地检测到更改并对虚拟机进行故障切换。
- Site Recovery Manager 在具有包含 vSphere Replication 副本磁盘的数据存储的恢复站点上支持 Storage DRS 群集。
- 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。
- 完全同步会导致 Storage DRS 生成迁移建议，或者如果 Storage DRS 在全自动模式下运行，则会直接触发 Storage vMotion。如果 DRS 规则非常严苛，或者如果大量虚拟机同时执行完全同步，则会出现这种情况。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。
- 在受保护虚拟机数据存储上通过手动模式使用 Storage DRS 时，故障切换后可能存在失效的建议。将故障切换虚拟机重新保护至原始站点后，如果应用这些失效的 Storage DRS 建议，Site Recovery Manager 占位虚拟机会损坏，从而导致应用了 Storage DRS 建议的虚拟机到原始站点的后续恢复失败。如果应用失效的更新，请取消注册占位虚拟机并使用 Site Recovery Manager 修复操作重新创建有效的占位虚拟机。要避免该问题，请在重新保护成功完成后为受影响的 Storage DRS 存储群集重新生成 Storage DRS 建议，以便从该站点中清除先前故障切换中的失效建议。

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 如何与延伸存储交互

延伸存储支持对基于阵列的复制可用。

Site Recovery Manager 支持受保护站点和恢复站点之间的主动/主动延伸存储，方法是使用 Cross vCenter Server vMotion 执行计划迁移，从而消除服务停机时间。灾难恢复和测试恢复将继续使用基于 LUN 的现有恢复功能。

重要事项 延伸存储仅在 vCenter Single Sign-On 增强型链接模式环境中受支持。如果站点不是增强型链接模式，使用 Cross vCenter Server vMotion 进行计划迁移将失败。在计划的迁移期间使用跨 vCenter Server 的 vMotion 时，需要延伸存储。

保护组

重要事项 延伸存储的保护组必须创建为存储策略保护组。您必须创建存储配置文件并使用其保护和恢复延伸存储设备。

- 具有延伸设备的保护组的首选方向必须为从受保护站点到恢复站点。首选方向必须与阵列为对应设备维护的站点首选项匹配。如果阵列支持站点首选项，则受保护站点必须具有站点首选项。
- 延伸和非延伸虚拟机与一致性组可以位于同一保护组和恢复计划中。
- 延伸虚拟机必须位于延伸数据存储上，且必须在受保护站点上打开电源。
- 您无法使用相同的延伸设备对在相反方向创建两个保护组。您可以将虚拟机放置在与受保护站点上的受保护设备对应的恢复站点上的延伸设备上，但是，如果恢复站点 ESXi 挂载了受保护站点的存储，则存在数据损坏风险。您无法保护这些虚拟机，但它们会在重新保护过程中自动受保护。

计划的迁移

- **运行恢复计划**向导提供了相应选项，可以使用 Cross vCenter Server vMotion 来执行计划的迁移。如果选择此选项，Cross vCenter Server vMotion 将用于受保护站点上延伸存储中所有受保护且已打开电源的虚拟机。如果未选择此选项，将对复制的 LUN 使用常规恢复工作流，包括延伸存储。
- 如果 Cross vCenter Server vMotion 由于任何原因失败，恢复计划将在“迁移虚拟机”步骤停止，且不会继续。如果您无法解决阻止 Site Recovery Manager 使用 Cross vCenter Server vMotion 的问题，请将 vSphere vMotion 选项关闭并重新运行恢复计划。迁移可以对复制的 LUN 使用常规恢复工作流。
- 在取消激活步骤中，延伸设备将在受保护站点上保持挂载状态，即使未使用 vMotion。 Site Recovery Manager 将忽略受保护站点上延伸设备中的非受保护副本虚拟机，且不会将其取消注册。

测试恢复

- 通过对复制的设备（包括延伸设备）使用常规测试恢复工作流来执行测试恢复。对延伸设备上的每个虚拟机执行 vMotion 兼容性检查。
- 如果阵列不支持为延伸设备创建读写快照， Site Recovery Manager 将不允许您对这些设备执行测试恢复。

跨 vCenter Server 的 vMotion

对于从 vSphere Distributed Switch 端口组到标准交换机网络的迁移，Cross vCenter Server vMotion 不受支持。在这种情况下，尝试使用 Cross vCenter Server vMotion 迁移虚拟机将导致这些错误消息。

- 在与保护组 <PG-name> 中虚拟机 <vm-name> 的 Cross vCenter Server vMotion 兼容的群集 <cluster-name> 中，找不到主机。
- 当前连接的网络接口 <network-adapter-name> 无法使用网络 <network-name>，因为基于源网络类型的 vMotion 不支持目标网络的类型。

Cross vCenter Server vMotion 在下列情况下将不起作用。

- 已对群集禁用 Distributed Resource Scheduler
- 虚拟机具有快照
- 虚拟机是链接克隆

《ESXi 和 vCenter Server 6.7》文档将讨论 vSphere 中跨 vCenter Server 的 vMotion 要求。

将 Site Recovery Manager 与 NSX Data Center for vSphere 结合使用

Site Recovery Manager 可以保护连接到受保护站点和恢复站点上的 NSX 网络的虚拟机，并且无需配置清单映射。

NSX Data Center for vSphere 支持通用逻辑交换机，它允许创建跨 vCenter Server 边界的第 2 层网络。将通用逻辑交换机与 NSX 一起使用时，连接到相同第 2 层网络的受保护站点和恢复站点都各有一个虚拟端口组。这意味着使用存储策略保护组和通用逻辑交换机时，您无需指定任何网络映射。Site Recovery Manager 会与 NSX Data Center for vSphere 一起将虚拟机自动映射到恢复站点上的正确网络。

您可以通过在延伸网络上手动配置网络映射来替代自动映射。支持增强型链接模式和非增强型链接模式拓扑。

限制

- 仅存储策略保护组和通用逻辑交换机支持 NSX 通用线路自动映射。
- VMware NSX-T™ Data Center 不支持存储策略保护组的网络自动映射。
- 对于虚拟机保护组，必须明确配置通用线路两端之间的网络映射，以确保虚拟机在同一通用线路上恢复。
- 仅完全恢复支持此功能。必须手动执行测试故障切换。

有关详细信息，请参见配置清单映射。

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 和虚拟机加密

您可以使用 Site Recovery Manager 通过基于阵列的保护组、存储策略保护组和 vSphere Replication 保护组来保护和恢复加密虚拟机。

加密不仅能保护虚拟机，还能保护虚拟机磁盘和其他文件。您可以在 vCenter Server 和密钥管理服务器 (Key Management Server, KMS) 之间设置可信连接。然后，vCenter Server 可以根据需要从 KMS 检索密钥。必须使用在受保护站点和恢复站点上以相同名称注册的 KMS 群集。有关详细信息，请参见《管理 VMware vSAN》指南中的“设置 KMS 群集”。

要对加密虚拟机执行客户机自定义，Site Recovery Manager 需要 ESXi 6.5 或更高版本。

有关虚拟机加密的详细信息，请参见《vSphere 安全性》文档中的虚拟机加密。

有关存储策略保护组和加密虚拟机的详细信息，请参见保护加密的虚拟机。

有关 vSphere Replication 和加密虚拟机的详细信息，请参见 vSphere Replication 管理文档中的复制加密虚拟机。

Site Recovery Manager 和 vRealize Orchestrator

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

适用于 Site Recovery Manager 的 vRealize Orchestrator Plug-in 包含运行 Site Recovery Manager 操作的操作和工作流。如果您是 vRealize 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 vRealize Orchestrator 工作流中，可以将 Site Recovery Manager 操作与其他 vRealize Orchestrator 插件提供的自动化操作合并。

例如，可以为 vCenter Server 创建使用 vRealize 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 vRealize 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 Site Recovery Manager 的 vRealize Orchestrator Plug-in，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 适用于 Site Recovery Manager 的 vRealize Orchestrator Plug-in 实例上将 Site Recovery Manager 与多个 vCenter Server 实例配合使用。

有关使用 vRealize Orchestrator 创建工作流的信息，请参见 vRealize Orchestrator 文档。

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。
- 保护和重新保护 MSCS 或容错虚拟机要求受保护站点和恢复站点上具有 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。
- 可以使用基于阵列的复制保护多个 vCPU 容错 (SMP-FT) 虚拟机。主要和辅助故障容错虚拟机磁盘文件必须驻留在复制的 LUN 上，且所有 LUN 必须属于同一个一致性组。

- 如果主要 SMP-FT 虚拟机的文件中有错误，则 Site Recovery Manager 仅尝试故障切换主要 SMP-FT 虚拟机，而会不尝试回退到辅助 SMP-FT 虚拟机。
- SMP-FT 虚拟机受到保护且其存储不满足复制要求时，Site Recovery Manager 不会生成警告。
- 一个 SMP-FT 虚拟机只能由一个保护组保护。
- Site Recovery Manager 不支持由 vSphere Replication 复制的 SMP-FT 虚拟机。
- Site Recovery Manager 不支持存储策略保护组中的 SMP-FT 虚拟机。SMP-FT 不支持存储配置文件。
- 执行重新保护时，Site Recovery Manager 不会保留原始受保护站点上的 SMP-FT 配置。
- 执行故障切换时，目标虚拟机作为非 FT 虚拟机打开电源。通过使用 Site Recovery Manager 之外的工具，可以在故障切换后将其配置为 SMP-FT 虚拟机。

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 虚拟机在单个 ESXi 主机上运行。在一个 ESXi 主机上，您最多可以拥有五个 MSCS 节点。

  跨机箱的群集

  最多可以将 MSCS 群集分散在五个 ESXi 主机实例中。您只能保护一个 ESXi 主机实例上任意 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。

- 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群集跨机箱部署中，vSphere vMotion 可能会将某些或全部 MSCS 虚拟机移至单个 ESXi 主机。

结合使用 Site Recovery Manager 与 SIOC 数据存储

Site Recovery Manager 完全支持 Storage I/O Control (SIOC)。

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。

将 Site Recovery Manager 与接入控制群集结合使用

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。

Site Recovery Manager 和附加到 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。

注 Site Recovery Manager 不支持保护附加到存储策略保护组中的 RDM 设备的虚拟机。

- 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。

Site Recovery Manager 和 Active Directory 域控制器

Site Recovery Manager 支持保护充当 Active Directory 域控制器的虚拟机，就像 Site Recovery Manager 支持的任何其他应用程序一样。

作为本机 Active Directory 复制技术和还原模式的替代方法，可以在灾难场景中使用 Site Recovery Manager 保护 Active Directory 基础架构。如果遇到任何问题，这些问题可能与特定网络配置和域控制器依赖关系相关。

高级 Site Recovery Manager 配置

12

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

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。

更改连接设置

Site Recovery Manager 与其他服务进行通信。

步骤

1. 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 在左侧窗格中，单击**配置 > 高级设置 > 连接**。

4 选择一个站点，然后单击**编辑**以更改设置。

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 **connections.hmsPanicDelay** 文本框中输入新值。
更改声明检查失败前要尝试的状态检查 (Ping) 次数。默认值为 2。	在 **connections.hmsPingFailedDelay** 文本框中输入新值。
更改等待从服务器更新的超时值。默认值为 900 秒。	在 **connections.waitForUpdatesTimeout** 文本框中输入新值。

5 要保存更改，请单击**确定**。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 导出历史记录**。

4 选择一个站点，然后单击**编辑**以更改设置。

5 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。

6 要选择不导出报告，可将该值改为零 (0)。

7 要保存更改，请单击**确定**。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 本地站点状态**。

4 选择一个站点，然后单击**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 **localSiteStatus.checkInterval** 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 **localSiteStatus.eventFrequency** 文本框中输入新值。
更改服务器时钟之间允许的最大时间差异。默认为 20 秒。	在 **localSiteStatus.maxClockSkew** 文本框中输入新值。如果检测到的服务器时钟的时间偏差超过 Site Recovery Manager Server 时钟设置的秒数，Site Recovery Manager 会引发事件。
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 **localSiteStatus.maxCpuUsage** 文本框中输入新值。
更改 Site Recovery Manager 证书过期（引发证书过期事件）之前的剩余天数。默认值为 30 天。	在 **localSiteStatus.minCertRemainingTime** 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 MB。	在 **localSiteStatus.minDiskSpace** 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 **localSiteStatus.minMemory** 文本框中输入新值。

5 要保存更改，请单击**确定**。

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。

none

关闭日志记录。

quiet

记录最小日志条目。

panic

仅记录应急日志条目。在出现完全失败时显示应急消息。

error

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。

warning

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。

info

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。

verbose

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。

trivia

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 日志管理器**。

4 选择一个站点，然后单击**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 logManager 中没有相应条目的所有组件的日志记录级别。默认值为 verbose。	从 **logManager.Default** 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 verbose。	从 **logManager.ExternalAPI** 下拉菜单中选择一个日志记录级别。
设置 vSphere Replication 的日志记录级别。默认值为 verbose。	从 **logManager.HbrProvider** 下拉菜单中选择一个日志记录级别。
设置 IP Customizer 工具的日志记录级别。默认值为 verbose。	从 **logManager.IPCustomizer** 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 verbose。	从 **logManager.InventoryMapper** 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 verbose。	从 **logManager.Licensing** 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 verbose。	从 **logManager.Persistence** 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 trivia。	从 **logManager.Recovery** 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**琐事**。
设置恢复配置操作的日志记录级别。默认值为 verbose。	从 **logManager.RecoveryConfig** 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 verbose。	从 **logManager.Replication** 下拉菜单中选择一个日志记录级别。
设置 Site Recovery Manager Server 和 vCenter Server 之间授权问题的日志记录级别。默认值为 verbose。	从 **logManager.ServerAuthorization** 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 verbose。	从 **logManager.SessionManager** 下拉菜单中选择一个日志记录级别。
设置 SOAP Web 服务适配器的日志记录级别。默认值为 info。	从 **logManager.SoapAdapter** 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**琐事**可能会影响性能。默认情况下，SOAP 适配器日志记录设置为**信息**。
设置存储问题的日志记录级别。默认值为 verbose。	从 **logManager.Storage** 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 verbose。	从 **logManager.StorageProvider** 下拉菜单中选择一个日志记录级别。

5 要保存更改，请单击**确定**。

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。

在执行恢复计划步骤期间，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.autoDeployGuestAlias`
- `recovery.defaultPriority`
- `recovery.powerOnTimeout`
- `recovery.powerOnDelay`
- `recovery.customizationShutdownTimeout`
- `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。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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。
2. 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。
3. 在左侧窗格中，单击**配置 > 高级设置 > 恢复**。

4 选择一个站点，然后单击**编辑**以修改恢复站点设置。

选项	操作
启用或禁用客户机用户映射的自动配置。此选项仅适用于使用兼容版本的 VMware Tools 的虚拟机。默认值为 true。 **有关兼容版本的 VMware Tools 的信息，请参见 Site Recovery Manager 8.2 兼容性列表。**	选择 **recovery.autoDeployGuestAlias** 的值，以启用或禁用客户机用户映射的自动配置。 如果该值为 true，则在恢复期间，Site Recovery Manager 会在所有虚拟机的客户机操作系统中创建客户机用户映射，并在恢复完成时移除这些映射。要使用此选项，必须安装兼容版本的 VMware Tools ，并且必须在要恢复的虚拟机上配置 IP 自定义或客户机标注操作。运行恢复过程之前，必须确保 ESXi 主机与恢复站点上的 vCenter Single Sign-On 服务器之间的时间同步。 如果该值为 false，必须手动将恢复站点上的本地 Site Recovery Manager 解决方案用户映射到受保护虚拟机上的客户机用户帐户。客户机操作系统用户必须有权在客户机操作系统中运行命令和访问文件。如果配置 IP 自定义或客户机标注操作，必须确保受保护虚拟机的客户机操作系统与恢复站点上的 vCenter Single Sign-On 服务器之间的时间同步。 如果 Site Recovery Manager 站点处于增强型链接模式，则可使用 vSphere Web Client 配置客户机用户映射。 有关如何配置客户机用户映射的信息，请参见《VMware vSphere ESXi 和 vCenter Server》文档中的“在客户机操作系统上配置用户映射”一章。 如果 Site Recovery Manager 站点不处于增强型链接模式，则必须使用 vSphere API 配置客户机用户映射并确保别名证书已映射。最佳做法是使用 vCenter Single Sign-On 服务器的签名证书。有关 vSphere API 的信息，请参见《VMware vSphere API 参考》文档。
更改 IP 自定义中虚拟机电源关闭超时时间。默认值为 300 秒。	在 **recovery.customizationShutdownTimeout** 文本框中输入新值。此值只是 IP 自定义工作流中使用的虚拟机电源关闭的最小超时时间（以秒为单位）。如果在虚拟机恢复设置中指定电源关闭超时时间，两者中的较大值优先。
更改 IP 自定义超时。默认值为 600 秒。	在 **recovery.customizationTimeout** 文本框中输入一个新的值。此值是在 Site Recovery Manager Server 中准备 IP 自定义脚本时使用的超时时间。无需更改此值。
更改恢复虚拟机的默认优先级。默认值为 3。	在 **recovery.defaultPriority** 文本框中输入一个新的值。
启用或禁用强制恢复。默认值为 false。	选中或取消选中 **recovery.forceRecovery** 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 **recovery.hostPowerOnTimeout** 文本框中输入一个新的值。
更改关闭虚拟机电源前等待客户机关机完成的默认超时值。默认值为 300 秒。	在 **recovery.powerOffTimeout** 文本框中输入一个新的值。该值定义将尝试关闭电源作为关闭虚拟机的最后办法之前客户机操作系统的超时时间。 **注** 超过超时时间后，虚拟机将关闭电源。如果虚拟机的操作系统在超过超时时间后仍未完成关闭任务，可能会导致数据丢失。对于需要较长时间才能正常关闭的大型虚拟机，请为其单独设置客户机操作系统关闭电源超时，如配置虚拟机启动和关机选项中所述。
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 **recovery.powerOnDelay** 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。
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 **recovery.powerOnTimeout** 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。如果受保护虚拟机未安装 VMware Tools，请将该值设置为 0，以便在打开这些虚拟机电源时跳过等待 VMware Tools，并避免 SRM 中出现超时错误。

选项	操作
启用或禁用跳过关闭客户机操作系统。默认值为 false。	选中或取消选中 **recovery.skipGuestShutdown** 复选框。 如果 skipGuestShutdown=true，Site Recovery Manager 不会尝试在保护站点虚拟机上关闭客户机操作系统，而会直接关闭虚拟机电源。在这种情况下，为 recovery.powerOffTimeout 设置的值与该设置均无效。如果虚拟机中未安装 VMware Tools，启用该设置可避免 Site Recovery Manager 中出现客户机操作系统关闭错误。 您也可以启用此选项，跳过客户机操作系统直接关闭虚拟机电源（没有关机超时）。请参见配置虚拟机启动和关机选项。
启用或禁用恢复期间自动执行虚拟机 IP 自定义。默认值为 true。	选中或取消选中 **recovery.useIpMapperAutomatically** 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 要保存更改，请单击**确定**。

后续步骤

要将更改应用到您之前已保护的虚拟机，必须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。您可以通过“恢复计划”或“保护组”应用更改。

请参见将恢复设置应用到恢复计划中的虚拟机和将恢复设置应用到保护组中的虚拟机。

将恢复设置应用到恢复计划中的虚拟机

如果更改受保护虚拟机的高级恢复设置，您必须重新配置虚拟机才能使设置生效。

应用单个设置或将恢复设置应用到单个虚拟机时，您可以在恢复计划中更有效地配置恢复设置。在某些情况下，您只能以此方式应用设置，例如，在灾难恢复或恢复未完成的情况下更改设置。

步骤

1 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

2 选择**恢复计划**选项卡，然后单击虚拟机所在的恢复计划。

3 在**虚拟机**选项卡上，右键单击虚拟机，然后单击**配置恢复**。

4 针对恢复属性设置执行所需更改。

5 单击**确定**。

后续步骤

要将恢复设置应用到保护组中的虚拟机，请参见将恢复设置应用到保护组中的虚拟机。

将恢复设置应用到保护组中的虚拟机

如果更改受保护虚拟机的高级恢复设置，您必须重新配置虚拟机才能使设置生效。

将恢复设置应用到多个虚拟机时，可使用“保护组”功能更方便地更新恢复设置，尽管此功能也可用于单个虚拟机。您可以选择保护组中的所有虚拟机一次性更新设置。

步骤

1 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

2 选择**保护组**选项卡，然后单击虚拟机所在的保护组。

3 在**虚拟机**选项卡上，右键单击虚拟机，然后单击**移除保护**。

虚拟机状态将更改为“未配置”。

4 单击**配置所有虚拟机**以重新配置保护组中的所有虚拟机，或选择一个虚拟机并单击**配置保护**仅重新配置该虚拟机。

后续步骤

要将恢复设置应用到恢复计划中的虚拟机，请参见将恢复设置应用到恢复计划中的虚拟机。

更改远程管理器设置

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。如果完成某个任务所需的时间比默认超时期限要长，并且在运行时不向另一个站点发送通知，则可能会发生超时。在这种情况下，您可以更改远程管理器设置，以便 Site Recovery Manager 不会在长时间运行任务完成之前超时。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 远程管理器**。

4 选择一个站点，然后单击**编辑**以修改远程管理器设置。

选项	操作
配置等待远程操作完成的最大时间。默认值为 900 秒。	在 **remoteManager.defaultTimeout** 文本框中输入一个新值。
将虚拟机标记为受 Site Recovery Manager 保护。默认值为 true。	选中 **remoteManager.enableCustomFields** 复选框。
设置等待请求在远程站点聚合的时间期限。默认值为 2000 毫秒。	在 **remoteManager.powerOnAggregationInterval** 文本框中输入一个新值。
配置等待已取消任务停止的最长时间。默认值为 300 秒。	在 **remoteManager.taskCancelDefaultTimeout** 文本框中输入一个新值。
配置等待任务在远程站点完成的额外超时期限。默认值为 900 秒。	在 **remoteManager.taskDefaultTimeout** 文本框中输入一个新值。
配置等待远程任务报告进度的秒数。如果在该时间段内收到进度更新，则允许该任务使用更多的时间完成。默认值为 180 秒。	在 **remoteManager.taskProgressDefaultTimeout** 文本框中输入一个新值。

选项	操作
配置出现故障时尝试打开虚拟机电源的次数。默认值为 5 次。	在 **remoteManager.vmPowerOnRetryCount** 文本框中输入一个新值。
配置出现故障时尝试关闭虚拟机客户机操作系统的次数。默认值为 5 次。	在 **remoteManager.vmGuestShutDownRetryCount** 文本框中输入一个新值。
配置出现故障时尝试重新配置虚拟机设置的次数。默认值为 5 次。	在 **remoteManager.vmReconfigureRetryCount** 文本框中输入一个新值。
配置等待 xVC-vMotion 超时的秒数。默认值为 3600 秒。	在 **remoteManager.xVcVMotionTimeout** 文本框中输入一个新值。

5 要保存更改，请单击**确定**。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 远程站点状态**。

4 选择一个站点，然后单击**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 **remoteSiteStatus.drPanicDelay** 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 **remoteSiteStatus.drPingFailedDelay** 文本框中输入一个新的值。

5 要保存更改，请单击**确定**。

更改复制设置

可以编辑复制设置以修改 Site Recovery Manager 等待完成创建占位虚拟机的时间。您可以修改存储策略保护组中的虚拟机的保护轮询时间间隔。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 复制**。

4 选择一个站点，然后单击**编辑**以更改设置。

选项	操作
在执行计划的迁移期间，在取消激活保护站点时跳过对非受保护副本虚拟机的检查。默认值为 false。	选中该文本框以启用值 **replication.disablePiggybackVmsCheckDuringDeactivate**。
更改创建占位虚拟机时等待的超时（以秒为单位）。默认值为 300 秒。	在 **replication.placeholderVmCreationTimeout** 文本框中输入一个新值。
定期轮询存储策略保护组中的虚拟机以查找缺少的映射，并在缺少任何可能导致存储策略保护组恢复失败的映射时报告警告。默认值为 false。	选中复选框以将 **replication.pollForMissingInventoryMappings** 值更改为 true。
更改在远程站点上启动联机同步之前等待一致性组信息复制到该站点的超时时间（以秒为单位）。默认为 900 秒。	在 **replication.protectionInfoSyncTimeout** 文本框中输入一个新值。
更改时间间隔（以秒为单位）以轮询存储策略保护组和缺少的清单映射。默认值为 120 秒。	在 **replication.protectionPollInterval** 文本框中输入一个新值。 注 在更新轮询时间间隔之前，请估算环境中的更改、更改频率和环境性能。

5 要保存更改，请单击**确定**。

更改 SSO 设置

可修改 Single Sign On 设置以便 Site Recovery Manager 续订 SSO 令牌。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > SSO**。

4 选择一个站点，单击**编辑**以更改 **sso.sts.tokenLifetime** 设置，从而指定在续订 SSO 令牌前可以使用的秒数。

默认值为 28800 秒（8 小时）。

5 要保存更改，请单击**确定**。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 存储**。

4 选择一个站点，然后单击**编辑**以修改存储设置。

选项	操作
更改在尝试将标记附加到已恢复的数据存储之前等待的时间（以秒为单位）。默认值为 30 秒。	在 **storage.attachTagsDelaySec** 文本框中输入一个新值。
更改运行 SRA 命令的超时时间（以秒为单位）。默认值为 300 秒。	在 **storage.commandTimeout** 文本框中输入一个新的值。
更改与数据存储监控相关的操作之间的超时（以秒为单位）。默认值为 30 秒。	在 **storage.datastoreMonitoringPollingInterval** 文本框中输入一个新值。
允许 Site Recovery Manager 创建 Storage DRS 兼容性要求的标记类别和已复制标记。默认值为 true。	选中 **storage.enableSdrsStandardTagCategoryCreation** 复选框。
允许 Site Recovery Manager 自动创建标记并将其附加到已复制或受保护的数据存储，以实现 Storage DRS 兼容性。默认值为 true。	选中 **storage.enableSdrsTagging** 复选框。如果清除该复选框，Site Recovery Manager 会删除所有标记和标记类别并破坏与 Storage DRS 的兼容性。
允许 Site Recovery Manager 修复已复制或受保护的数据存储上缺少的或不正确的标记，以实现 Storage DRS 兼容性。默认值为 true。	选中 **storage.enableSdrsTaggingRepair** 复选框。
更改最大并发 SRA 操作数。默认值为 5。	在 **storage.maxConcurrentCommandCnt** 文本框中输入一个新的值。
更改要记录的 SRA 命令控制台输出的最大长度（以字节为单位）。默认值为 1048576 字节 (1 MB)。	在 **storage.maxSraCommandOutputLength** 文本框中输入一个新值。 ■ 值为 0 表示无 SRA 输出日志。 ■ 值为 -1 表示对长度无限制。 ■ 如果输入 0 和 -1 之外的其他值，且不在 512 字节和 10 MB 之间的区间内，则值会自动设置为默认值 1 MB。
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 **storage.minDsGroupComputationInterval** 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 **storage.querySyncStatusPollingInterval** 文本框中输入一个新的值。
更改 Storage DRS 标记相关操作之间的时间间隔。默认值为 50 秒。	在 **storage.sdrsTaggingPollInterval** 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 **storage.storagePingInterval** 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 **storage.syncTimeout** 文本框中输入一个新的值。

5 要保存更改，请单击**确定**。

更改 ABR 存储策略设置

您可以修改“ABR 存储策略”设置来指定对符合虚拟机存储策略的数据存储执行自动发现的时间间隔（以秒为单位）。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > ABR 存储策略**。

4 选择一个站点并单击**编辑**。

5 根据需要更改 **storagePolicyAbrReplication.policyDatastorePollInterval** 的值。默认值为 20 秒。

6 要保存更改，请单击**确定**。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 存储提供程序**。

4 选择一个站点，然后单击**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 **storageProvider.autoDetachLUNsWithDuplicateVolume** 复选框。
测试和恢复期间在 ESXi 主机上设置 `LVM.EnableResignature` 标记。默认值为 0。	在 **storageProvider.autoResignatureMode** 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。如果将此标记设置为 1，Site Recovery Manager 会对所有已知 VMFS 快照卷（包括 Site Recovery Manager 不管理的任何卷）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。
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 **storageProvider.batchAttachTimeoutSec** 文本框中输入值。

选项	操作
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 **storageProvider.batchDetachTimeoutSec** 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 **storageProvider.batchMountTimeoutSec** 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 **storageProvider.batchUnmountTimeoutSec** 文本框中输入一个新的值。如果因 Site Recovery Manager 检查 VMFS 卷需要很长时间才能卸载而发生超时，请更改该值。此设置在 Site Recovery Manager 5.5.1 及更高版本中提供。
设置批量卸载 VMFS/NFS 卷的重试次数。默认为重试 3 次。	在 **storageProvider.datastoreUnmountRetryCount** 文本框中输入一个新的值。
更改 Site Recovery Manager 在尝试卸载数据存储之前等待的时间间隔。默认为 1 秒。	在 **storageProvider.datastoreUnmountRetryDelaySec** 文本框中输入一个新的值。
更改在测试和恢复期间收到 SRA 响应后获取 ESXi 主机上的数据存储之前等待的时间（以秒为单位）。此设置仅适用于没有 SCSI 设备的情况。默认值为 0。	在 **storageProvider.fetchDatastoreDelaySec** 文本框中输入一个新值。
成功完成恢复后，强制移除已恢复的数据存储名称中的 **snap-*xx*** 前缀。默认值为 false。	选中 **storageProvider.fixRecoveredDatastoreNames** 复选框。
更改在移除已恢复的数据存储名称中的 **snap-*xx*** 前缀之前 Site Recovery Manager 等待的时间。默认值为 0 秒。	在 **storageProvider.fixRecoveredDatastoreNamesDelaySec** 文本框中输入一个新的值。
在测试和恢复期间延迟主机扫描。默认值为 0 秒。	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。 要延迟启动存储重新扫描，直至它们在 ESXi 主机上可用，可在 **storageProvider.hostRescanDelaySec** 文本框中输入新的值。 仅当遇到数据存储不可用问题时才能更改此值。
在测试和恢复期间重复主机扫描。默认值为 1。	在 **storageProvider.hostRescanRepeatCnt** 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 **storageProvider.hostRescanRepeatCnt** 参数在恢复中引入延迟。请改为使用 **storageProvider.hostRescanDelaySec** 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 **storageProvider.hostRescanTimeoutSec** 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 **storageProvider.resignatureFailureRetryCount** 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 **storageProvider.resignatureTimeoutSec** 文本框中输入一个新的值。如果您更改 **storageProvider.hostRescanTimeoutSec** 设置，请将 **storageProvider.resignatureTimeoutSec** 设置增大到用于 **storageProvider.hostRescanTimeoutSec** 的相同超时。

选项	操作
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 .snapshot，	某些阵列会创建 `storageProvider.storageVmotionVmxSearch` 搜索算法应忽略的 VMX 文件路径。在 **storageProvider.storageVmotionVmxFilePathsToSkip** 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。
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 **storageProvider.storageVmotionVmxSearch** 复选框可禁用此选项。
设置本地延伸设备与相应的远程延伸设备匹配的超时（以秒为单位）。默认为 300 秒。	在 **storageProvider.stretchedDevicesMatchTimeout** 文本框中输入新的值。
设置每个主机的并行 xVC-vMotion 请求数。此限制适用于源主机和目标主机。默认值为 2。	在 **storageProvider.vmMigrationLimitPerHost** 文本框中输入一个新值。
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 **storageProvider.waitForAccessibleDatastoreTimeoutSec** 文本框中输入新的值。
允许 Site Recovery Manager 在恢复之后等待发现数据存储。	选中 **storageProvider.waitForDeviceRediscovery** 复选框。
允许 Site Recovery Manager 在故障切换之后等待发现数据存储。	选中 **storageProvider.waitForDeviceRediscoveryAfterPrepareFailover** 复选框。
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 **storageProvider.waitForRecoveredDatastoreTimeoutSec** 文本框中输入新的值。
设置 Site Recovery Manager 等待 VMFS 卷变为已挂载的时间间隔（秒）。默认值为 30 秒。	在 **storageProvider.waitForVmfsVolumesMountedStateTimeoutSec** 文本框中输入新的值。

5 要保存更改，请单击**确定**。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > vSphere Replication**。

4 选择一个站点，然后单击**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 **vrReplication.allowOtherSolutionTagInRecovery** 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，请选中 **vrReplication.preserveMpitImagesAsSnapshots** 复选框。
更改重新保护操作期间反向复制的超时期限	在 **vrReplication.reverseReplicationTimeout** 文本框中键入新值。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。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。
更改 vSphere Replication 同步操作的超时期限。默认值为 7200。	在 **vrReplication.synchronizationTimeout** 文本框中输入一个新值。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 **vrReplication.timeDefault** 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。

5 要保存更改，请单击**确定**。

更改遥测设置

您可以编辑 Site Recovery Manager 的遥测设置以指定发送遥测报告时要使用的代理主机。

步骤

1 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在左侧窗格中，单击**配置 > 高级设置 > 遥测**。

4 选择一个站点，然后单击**编辑**以更改设置。

选项	描述
指定发送遥测报告时使用的 HTTP 代理主机名。	在 **telemetry.proxyHost** 文本框中输入 HTTP 代理的名称。
指定发送遥测报告时使用的 HTTP 代理端口。	在 **telemetry.proxyPort** 框中输入端口号。
指定发送遥测报告时是否使用 SSL 连接到 HTTP 代理。默认值为 false。	移动滑块以将值 **telemetry.proxyUseSsl** 更改为 true。

5 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。

可以在 vSphere Web Client 或 Site Recovery Manager 客户端插件的**高级设置**菜单中修改某些选项。要修改其他设置，请编辑 Site Recovery Manager Server 或 Site Recovery Manager Virtual Appliance 上的 `vmware-dr.xml` 配置文件。可以时，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 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

1 在 vSphere Web Client 或 vSphere Client 中选择群集。

2 在**配置**选项卡上，选择**服务 > vSphere DRS**。

如果使用的是 vCenter Server 6.0 Update 3，在**管理**选项卡上，选择**服务 > vSphere DRS**

3 单击 **[编辑]**。

4 在**高级选项**中，设置 `srmMaxBootShutdownOps` 设置。

选项	描述
选项文本框	输入 `srmMaxBootShutdownOps`。
值文本框	输入最大并发启动和关机操作数。例如，如果将该值设置为 32，则表示虚拟机 1 到 32 同时启动或关闭，当第一批中的一个虚拟机完成时，虚拟机 33 便立即启动或关闭。当第一批中的第二个虚拟机完成时，虚拟机 34 启动，依此类推。

5 要保存更改，请单击**确定**。

6 登录 Site Recovery Manager Server 主机。

7 在文本编辑器中打开 `vmware-dr.xml` 文件。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则会在 Site Recovery Manager Server 主机上的 `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` 文件夹中找到 `vmware-dr.xml` 文件。
- 如果使用的是 Site Recovery Manager Virtual Appliance，则会在设备上的 `/opt/vmware/srm/conf/` 目录中找到 `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，则第一批 24 个客户机中的一个完成时，下一个客户机便立即启动或关闭。这表示，虚拟机 1 到 24 全部同时启动，当第一批中的一个虚拟机完成时，虚拟机 25 便立即启动。当第一批中的第二个虚拟机完成时，虚拟机 26 启动，依此类推。

9 要应用新设置，请重新启动 Site Recovery Manager Server。

10 在 vSphere Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

11 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

12 在左侧窗格中，单击**配置 > 高级设置 > vSphere Replication**，然后增加 vrReplication.synchronizationTimeout 和 vrReplication.reverseReplicationTimeout 设置。

默认值为 7200，对应于工作同步超时期限 14400 秒。

13 选择**高级设置 > 存储**，选择站点，然后增加 storage.commandTimeout 设置。

默认值为 300 秒。

14 要保存更改，请单击**确定**。

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。

可以在 vSphere Web Client 或 Site Recovery Manager 客户端插件的**高级设置**菜单中修改某些选项。要修改其他设置，请编辑 Site Recovery Manager Server 或 Site Recovery Manager Virtual Appliance 上的 vmware-dr.xml 配置文件。可以时，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 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 12-1. 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
srmMaxBootShutdownOps	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**设置**，为 vSphere Web Client 或 vSphere Client 中的每个群集修改此选项。单击 **vSphere DRS**，然后单击**编辑 > 高级选项**。键入选项以替代可在 `vmware-dr.xml` 文件中设置的 **defaultMaxBootAndShutdownOpsPerCluster** 值。可以在 `vmware-dr.xml` 文件中设置全局值 **defaultMaxBootAndShutdownOpsPerCluster**，然后为 vSphere Web Client 或 vSphere Client 中的各个群集设置不同的 **srmMaxBootShutdownOps** 值。默认情况下，限制处于关闭状态。
defaultMaxBootAndShutdownOpsPerCluster	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 `vmware-dr.xml` 文件中修改此设置。可在 vSphere Web Client 中设置的 **srmMaxBootShutdownOps** 值将替代 **defaultMaxBootAndShutdownOpsPerCluster** 值。可以在 `vmware-dr.xml` 文件中设置全局值 **defaultMaxBootAndShutdownOpsPerCluster**，然后为 vSphere Web Client 中的单个群集设置不同的 **srmMaxBootShutdownOps** 值。默认情况下，限制处于关闭状态。
defaultMaxBootAndShutdownOpsPerHost	指定任何独立主机的最大并发打开电源操作数。只能在 `vmware-dr.xml` 文件中设置该选项。默认情况下，限制处于关闭状态。

表 12-2. 用于修改超时期限的设置

选项	描述
vrReplication.synchronizationTimeout	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 Site Recovery 用户界面中修改此选项。在 Site Recovery“主页”选项卡上，选择站点对，然后单击**查看详细信息**。在左侧窗格中，选择**配置 > 高级设置 > vSphere Replication**。默认值为 7200，对应于工作同步超时期限 14400 秒。
vrReplication.reverseReplicationTimeout	重新保护操作期间反向复制的超时期限。在 Site Recovery 用户界面中修改此选项。在 Site Recovery“主页”选项卡上，选择站点对，然后单击**查看详细信息**。在左侧窗格中，选择**配置 > 高级设置 > vSphere Replication**。默认值为 7200，对应于工作同步超时期限 14400 秒。
storage.commandTimeout	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 Site Recovery 用户界面中修改此选项。在 Site Recovery“主页”选项卡上，选择站点对，然后单击**查看详细信息**。在左侧窗格中，选择**配置 > 高级设置 > 存储**。默认值为 300 秒。

Site Recovery Manager 事件和警报 13

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
- 创建 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 会发送一个 `RemoteSiteUpEvent` 事件。

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。

- 连接监视器将跳过一些失败的 Ping 操作。您可以通过设置 `remoteSiteStatus.drPingFailedDelay` 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.drPingFailedDelay` 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 发送一个 `RemoteSiteDownEvent` 事件，并停止发送 `RemoteSitePingFailedEvent` 事件。您可以通过设置 `remoteSiteStatus.drPanicDelay` 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，直至重新建立连接。
- 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。

创建 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。

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 Client 中，单击 vCenter Server。

2 在**配置**选项卡中，展开**更多**，然后单击**警报定义**以显示 vCenter Server 警报列表。

3 单击**添加**以添加新的警报。

4 在**名称**页面上，输入警报名称和描述，然后单击**下一步**。

5 在**目标**页面上，从下拉菜单中选择一个目标，然后单击**下一步**。

6 在**警报规则**页面上，从下拉菜单中选择一个事件，然后选择相应的状态。

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。

7 要添加触发警报的条件，请单击**添加参数**，从下拉菜单中选择一个参数，然后选择运算符以及从警告到严重条件的转换。

8 （可选） 选择发送电子邮件通知、SNMP 陷阱还是运行脚本。

9 单击**下一步**。

10 在**查看**页面上，选择是否启用警报，然后单击**创建**。

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 13-1. 站点状态事件

事件名称	事件类型	事件描述	类别
未知状态	`UnknownStatusEvent`	无法获取 Site Recovery Manager Server 状态	信息
远程站点关闭	`RemoteSiteDownEvent`	Site Recovery Manager Server 已断开与远程 Site Recovery Manager Server 的连接。	错误

表 13-1. 站点状态事件 （续）

事件名称	事件类型	事件描述	类别
远程站点 Ping 失败	RemoteSitePingFailedEvent	远程站点出现故障或网络连接存在问题。	警告
远程站点已创建	RemoteSiteCreatedEvent	本地站点已与远程站点成功配对。	信息
远程站点正常	RemoteSiteUpEvent	Site Recovery Manager Server 重新建立与远程 Site Recovery Manager Server 的连接。	信息
远程站点已删除	RemoteSiteDeletedEvent	远程 Site Recovery Manager 站点已删除。	信息
vSphere Replication 复制的虚拟机已添加到保护组中	HbrGroupVmAssociatedEvent	vSphere Replication 复制的虚拟机已添加到保护组中。	信息
vSphere Replication 复制的虚拟机已从保护组中移除	HbrGroupVmDisassociatedEvent	vSphere Replication 复制的虚拟机已从保护组中移除。	信息
本地 vSphere Replication Server 关闭	LocalHmsConnectionDownEvent	重新尝试连接 vSphere Replication 失败。	错误
与本地 vSphere Replication Server 之间的连接已还原	LocalHmsConnectionUpEvent	与 vSphere Replication 的连接成功。	信息
本地 vSphere Replication Server 未响应	LocalHmsPingFailedEvent	无法建立与本地 vSphere Replication Server 的连接	警告
磁盘空间低	LowDiskSpaceEvent	本地站点上的可用磁盘空间较低。	警告
内存低	LowMemoryEvent	本地站点上的可用内存较低。	警告
SRM Server 证书尚未生效	SrmCertificateNotValidEvent	指定 SRM Server 的 SSL/TLS 证书尚未生效。	错误
SRM Server 证书即将过期	SrmCertificateExpiringEvent	指定 SRM Server 的 SSL/TLS 证书将在指定的天数后过期。	信息
SRM Server 证书已过期	SrmCertificateExpiredEvent	指定 SRM Server 的 SSL/TLS 证书已过期。	错误

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。

表 13-2. 保护组复制事件

事件	描述	原因	类别
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。	信息
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。	信息
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。	信息

表 13-2. 保护组复制事件 （续）

事件	描述	原因	类别
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。	信息
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。	信息
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。	信息
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。	信息
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。	信息
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。	信息
VmFullyProtectedEvent	组中的虚拟机：未解析的设备已全部解析。	受保护虚拟机先前未解析的设备已全部解析。	警告
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。	警告
PlaceholderVmUnexpectedlyDeletedEvent	组中的虚拟机：已从 vCenter Server 清单中移除占位虚拟机。	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。	警告
ProductionVmDeletedEvent	组中的虚拟机：已从虚拟机 vCenter Server 清单中移除受保护的虚拟机。	当受保护虚拟机从 vCenter Server 清单中删除或移除时发布。	错误
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。	错误

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 13-3. 恢复事件

事件名称	事件类型	事件描述	类别
恢复计划已开始恢复指定虚拟机。	RecoveryVmBegin	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。	信息
恢复计划已完成虚拟机恢复。	RecoveryVmEnd	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。	信息
恢复计划 [data.Plan] 无法注册虚拟机 [data.Vm]。	RecoveryVmRegisterFailed	恢复的虚拟机向恢复站点 VC 注册失败后，在 SPPG 情况下发出指示。如果针对本地 VC 运行计划，则 [data.local] 将为 true。	信息

表 13-3. 恢复事件 （续）

事件名称	事件类型	事件描述	类别
恢复计划 *hostname* 已创建。	PlanCreated	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。	信息
恢复计划已破坏。	PlanDestroy	从站点删除计划后发出指示。请注意，在请求删除计划的站点上会有明显延迟，因为它会等待从另一站点上删除此计划。新计划将发送到托管计划的每个 vCenter Server 实例。	信息
恢复计划已更改。	PlanEdit	编辑现有计划后发出指示。	信息
恢复计划已开始进行测试。	PlanExecTestBegin	启动恢复测试后在恢复站点上发出指示。	信息
恢复计划已完成测试。	PlanExecTestEnd	完成恢复测试后在恢复站点上发出指示。	信息
恢复计划已开始测试清理。	PlanExecCleanupBegin	启动测试清理后在恢复站点上发出指示。	信息
恢复计划已完成测试清理。	PlanExecCleanupEnd	完成测试清理后在恢复站点上发出指示。	信息
恢复计划已开始恢复。	PlanExecBegin	启动恢复后在恢复站点上发出指示。	信息
恢复计划已完成恢复。	PlanExecEnd	完成恢复后在恢复站点上发出指示。	信息
恢复计划已开始重新保护操作。	PlanExecReprotectBegin	启动重新保护后在恢复站点上发出指示。	信息
恢复计划已完成重新保护操作。	PlanExecReprotectEnd	完成重新保护后在恢复站点上发出指示。	信息
恢复计划正在显示提示并等待用户输入。	PlanPromptDisplay	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。	信息
恢复计划已收到其提示的回答。	PlanPromptResponse	结束提示步骤时在恢复站点上发出指示。	信息
恢复计划已开始在 Site Recovery Manager Server 计算机上运行命令。	PlanServerCommandBegin	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。	信息
恢复计划已在 Site Recovery Manager Server 计算机上完成命令的执行。	PlanServerCommandEnd	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。	信息
恢复计划已开始在恢复的虚拟机上运行命令。	PlanVmCommandBegin	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。	信息
恢复计划已在恢复的虚拟机上完成命令的执行。	PlanVmCommandEnd	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。	信息

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 13-4. SRA 事件

事件	描述	原因	类别
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。	信息
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。	错误
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。	信息

表 13-5. 阵列管理器事件

事件	描述	原因	类别
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。	信息
SAManagerRemovedEvent	已删除指定的阵列管理器。	用户已移除阵列管理器。	信息
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。	信息
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。	信息
SAManagerPingFailEvent	无法 Ping 指定的阵列管理器。	Ping 阵列管理器过程中出错。	错误

表 13-6. 阵列对事件

事件	描述	原因	类别
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。	信息
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。	信息
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。	信息
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。	信息
SAPairPingFailEvent	无法 Ping 复制的阵列对。	Ping 阵列对过程中出错。	错误

表 13-7. 数据存储事件

事件	描述	原因	类别
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。	信息
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。	信息
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。	信息
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。	信息

表 13-8. 保护事件

事件	描述	原因	类别	事件目标
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。	信息	数据存储
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。	信息	数据存储
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。	信息	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。	信息	虚拟机
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。	警告	数据存储
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。	错误	数据存储
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。	错误	数据存储
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。	信息	保护组
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。	警告	数据存储
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。	错误	数据存储

表 13-8. 保护事件 （续）

事件	描述	原因	类别	事件目标
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。	错误	数据存储
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	信息	虚拟机
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。	错误	数据存储
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。	错误	数据存储
SPDsSpansConsistGroupsEvent	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。	错误	数据存储
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。	错误	数据存储

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 13-9. 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。

表 13-9. 许可事件 （续）

事件	描述	原因
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 13-10. 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。

表 13-11. 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。

表 13-11. SNMP 陷阱 （续）

事件	描述	原因
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。
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

14

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

2 在 **Site Recovery** 主页选项卡上，选择站点对，然后单击**查看详细信息**。

3 在**站点对**选项卡上，单击**摘要**，然后单击 Site Recovery Manager 框中的**名称**。

4 选择一个服务器，然后单击**导出日志**。

5 单击**下载**以下载日志。

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，手动收集日志文件会非常有用。

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

- 要收集 Site Recovery Manager 日志文件，请使用以下方法之一：

任务	操作
从 Site Recovery Manager Server Windows 主机使用命令提示符生成日志包	a 登录到 Site Recovery Manager Server 主机并打开命令提示符。 b 将工作目录更改为 `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`。 c 运行下列命令：`cscript srm-support.wsf` 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。
从 Site Recovery Manager Server Windows 主机使用开始菜单生成日志包	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 Site Recovery Manager Appliance 生成日志包	a 登录到 Site Recovery Manager Appliance 主机并打开命令提示符。 b 将工作目录更改为 `/opt/vmware/srm/bin/`。 c 运行下列命令： ■ 如果以管理员用户身份登录：`sudo ./srm-support-linux.sh`。 ■ 如果以 root 用户身份登录：`./srm-support-linux.sh`。

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。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则会在 Site Recovery Manager Server 主机上的 `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` 文件夹中找到 `vmware-dr.xml` 文件。

- 如果使用的是 Site Recovery Manager Virtual Appliance，则会在设备上的 `/opt/vmware/srm/conf/` 目录中找到 `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 10485760 字节。

```
<log>
   <maxFileSize>10485760</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 20 个日志文件。

```
<log>
   <maxFileNum>20</maxFileNum>
</log>
```

6 （可选） 通过修改 `<log>` 部分中的 `<directory>` 部分，更改 Site Recovery Manager Server 上用于存储日志文件的位置。

注 如果更改日志文件的位置，则必须确认您的 Site Recovery Manager 用户帐户具有写入新目录所需的权限。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则日志的默认路径为 `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs`。
- 如果使用的是 Site Recovery Manager Appliance，则日志文件的默认位置为 `/var/log/vmware/srm`。

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、详细和琐事。如果您将级别设置为“琐事”，您将看到对性能产生明显的负面影响。

```
<log>
   <level>info</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。例如，可将恢复组件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。

```
<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。

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。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则会在 Site Recovery Manager Server 主机上的 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config 文件夹中找到 vmware-dr.xml 文件。
- 如果使用的是 Site Recovery Manager Virtual Appliance，则会在设备上的 /opt/vmware/srm/conf/ 目录中找到 vmware-dr.xml 文件。

3 通过修改 vmware-dr.xml 文件的 <coreDump> 部分，更改 Site Recovery Manager Server 上用于存储核心转储的位置。

注 如果更改核心转储文件的位置，则必须确认您的 Site Recovery Manager 用户帐户具有写入新目录所需的权限。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则核心转储的默认路径为 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles，除非该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。
- 如果使用的是 Site Recovery Manager Appliance，核心转储的默认位置为 /var/log/vmware/srm/DumpFiles。

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>
```

参数	描述
dumpCoreCompression	如果不指定，默认值为 false。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 *true*，Site Recovery Manager Server 会在生成新核心转储时压缩所有旧核心转储。
dumpFullCore	如果不指定，默认值为 *false*。Site Recovery Manager Server 生成数 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 true，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 *true*。

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或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 15

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。

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，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% (The command 'echo "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 (Cannot complete customization, possibly due to a scripting runtime error or invalid script parameters)。
- 向客户机虚拟机上载文件时出错 (An error occurred when uploading files to the guest VM)。
- 等待 VMware Tools 600 秒后超时 (Timed out waiting for VMware Tools after 600 seconds)。

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 登录 Site Recovery Manager Server 主机。

2 在文本编辑器中打开 vmware-dr.xml 文件。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则会在 Site Recovery Manager Server 主机上的 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config 文件夹中找到 vmware-dr.xml 文件。
- 如果使用的是 Site Recovery Manager Virtual Appliance，则会在设备上的 /opt/vmware/srm/conf/ 目录中找到 vmware-dr.xml 文件。

3 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>
```

4 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

如果未映射虚拟机的设备，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

您尚未将受保护站点上的虚拟机设备映射到恢复站点上的相应设备。

解决方案

如修改基于阵列的保护组或 vSphere Replication 保护组中虚拟机的设置中所述配置虚拟机的保护设置。

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。请参见更改复制设置。

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。

计划的迁移由于存储策略保护组同步不成功而失败

当您尝试对包含存储策略保护组的恢复计划运行计划迁移时，由于未将更改同步到保护组，该恢复计划将失败。

问题

当您尝试对包含存储策略保护组的恢复计划运行计划迁移时，会看到以下错误消息：对等站点尚未将更改完全同步到保护组 (`The peer site has not finished synchronizing changes to protection group`)。

原因

当对包含存储策略保护组的恢复计划运行计划迁移时，在运行计划迁移之前， Site Recovery Manager 会检查受保护站点和恢复站点上的保护组是否已同步。

如果两个站点上的保护组已进行同步，将开始计划的迁移。如果两个站点上的保护组未同步，则会看到错误消息。

解决方案

1 关闭错误消息，然后再次单击**完成**。

2 （可选） 如果错误仍然存在，请取消计划的迁移，稍等片刻，然后再次尝试运行计划的迁移。

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 Client 或 vSphere Web Client 中，单击 **Site Recovery > 打开 Site Recovery**。

b 在 Site Recovery“主页”选项卡上，选择站点对，然后单击**查看详细信息**。

c 在左侧窗格中，单击**配置 > 高级设置 > 恢复**。

d 选择一个站点，然后单击**编辑**以修改恢复站点设置。

e 增加 `recovery.customizationTimeout` 参数，默认值为 600 秒。

f 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

在“高级设置”中增加 vrReplication.synchronizationTimeout 和 vrReplication.reverseReplicationTimeout 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。出现这种情况的原因可能在于通信量过大。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。

- 如果使用的是适用于 Windows 的 Site Recovery Manager，则会在 Site Recovery Manager Server 主机上的 C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config 文件夹中找到 vmware-dr.xml 文件。
- 如果使用的是 Site Recovery Manager Virtual Appliance，则会在设备上的 /opt/vmware/srm/conf/ 目录中找到 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。

计划的迁移期间恢复在执行到 36% 时停止

如果您在计划的迁移期间在受保护站点上停止了 Site Recovery Manager 服务，操作将在执行到 36% 时停止。

问题

在计划的迁移期间，如果您在受保护站点上停止了 Site Recovery Manager 服务，当工作流执行到步骤 15 **卸载受保护站点存储**时，可能不会正常退出，但会在执行到 36% 时停止。

解决方案

单击**取消**以取消工作流，然后重新运行工作流。

操作失败并显示有关非复制配置文件的错误

如果同时在两个方向运行多个恢复或重新保护操作，则操作将失败并显示有关非复制虚拟机配置文件的错误。

问题

如果同时运行多个包含基于阵列的复制保护组或存储策略保护组的恢复计划，其中部分操作从站点 A 到站点 B，部分操作从站点 B 到站点 A，则部分或所有计划将失败，并显示以下错误：`Cannot protect virtual machine 'virtual_machine_name' because its config file 'virtual_machine_config_file.vmx' is located on a non-replicated or non-protected datastore`。

原因

之所以发生此问题，是因为反向运行的恢复操作延迟了站点上的数据存储计算。

解决方案

等待部分操作完成并对失败的恢复计划重新运行该操作。或者，在同一方向同时运行所有计划的迁移。完成后，再反向运行计划的迁移。

恢复因用户权限受限而失败

如果 Site Recovery Manager 解决方案用户无权执行 IP 自定义或客户机操作系统标注操作，您可能会在恢复过程中收到错误。

问题

如果 Site Recovery Manager 解决方案用户对已恢复虚拟机的客户机操作系统没有相应的权限，您可能会在恢复过程中收到以下错误消息之一。

```
GuestPermissionDenied
```

```
CannotAccessFile
```

原因

如果 Site Recovery Manager 解决方案用户映射到的客户机操作系统用户在客户机操作系统中对文件没有访问权限或者无权运行命令，则会出现该问题。

解决方案

1. 如果使用 Site Recovery Manager 配置客户机用户映射，请确保运行 VMware Tools 服务的客户机操作系统用户对文件具有访问权限或者有权运行命令。

   有关如何启用或禁用客户机用户映射的自动配置的信息，请参见更改恢复设置。

2. （可选） 如果手动配置客户机用户映射，请将恢复站点上的本地 Site Recovery Manager 解决方案用户映射到具有相应权限的客户机操作系统用户。

3 重新运行恢复计划。

恢复因不支持结合使用 VMware Tools 与 ESXi 而失败

如果虚拟机上安装的 VMware Tools 版本和恢复站点上的 ESXi 主机版本与 Site Recovery Manager 不兼容，恢复过程可能会失败。

问题

您可能会在恢复过程中收到以下错误。

```
OperationNotSupportedByGuest
```

原因

如果使用不兼容的 VMware Tools 和 ESXi 版本，可能会出现该问题。有关 Site Recovery Manager、VMware Tools 与 ESXi 之间的兼容性信息，请参见 Site Recovery Manager 8.2 兼容性列表。

解决方案

- 确保 VMware Tools 和 ESXi 的版本与 Site Recovery Manager 兼容。