

# Veritas™ Resiliency Platform 3.3.2 概述与规划指 南

# Veritas Resiliency Platform: Overview and Planning Guide

上次更新时间： 2019-02-14

文档版本： Document version: 3.3.2 Rev 0

## 法律声明

Copyright © 2019 Veritas Technologies LLC. © 2019 年 Veritas Technologies LLC 版权所有。 All rights reserved. 保留所有权利。

Veritas、Veritas 徽标、Veritas InfoScale 和 NetBackup 是 Veritas Technologies LLC 或其附属机构在美国和其他国家/地区的商标或注册商标。其他名称可能为其各自所有者的商标。

此产品可能包含需要 Veritas 将其归属权提供给第三方的第三方软件（以下称“第三程序”）。部分第三程序会根据开源或免费软件许可证提供。本软件随附的授权许可协议并未改变这些开源或免费软件许可证所规定的任何权利或义务。请参考本 Veritas 产品随附的第三方法律声明文档，获取位置如下：

<https://www.veritas.com/licensing/process>

本文档中介绍的产品根据限制其使用、复制、分发和反编译/逆向工程的许可证进行分发。未经 Veritas Technologies LLC 及其特许人（如果存在）事先书面授权，不得以任何方式任何形式复制本文档的任何部分。

本文档按“现状”提供，对于所有明示或暗示的条款、陈述和保证，包括任何适销性、针对特定用途的适用性或无侵害知识产权的暗示保证，均不提供任何担保，除非此类免责声明的范围在法律上视为无效。Veritas Technologies LLC 不对任何与性能或使用本文档相关的伴随或后果性损害负责。本文档所含信息如有更改，恕不另行通知。

根据 FAR 12.212 中的定义，本授权许可软件和文档被视为“商业计算机软件”，受 FAR Section 52.227-19 “Commercial Computer Software - Restricted Rights” (商业计算机软件 - 受限权利) 和 DFARS 227.7202 “Commercial Computer Software and Commercial Computer Software Documentation” (商业计算机软件和商业计算机软件文档) 中的适用规定，以及所有后续法规中规定的受限权利的制约，无论是由 Veritas 在本地交付还是以托管服务的形式交付，概莫能外。美国政府仅可根据本协议的条款对本授权许可软件和文档进行使用、修改、复制发行、执行、展示或公开。

Veritas Technologies LLC  
500 E Middlefield Road  
Mountain View, CA 94043

<http://www.veritas.com>

## 技术支持

技术支持将维护全球的支持中心。将根据您的支持协议以及当时最新的企业技术支持策略来提供所有支持服务。有关我们的支持服务以及如何联系技术支持的信息，请访问我们的网站：

<https://www.veritas.com/support>

可从以下 URL 管理 Veritas 帐户信息：

<https://my.veritas.com>

如果您对现有支持协议有疑问，请通过电子邮件联系您所在地区的支持协议管理团队，如下所示：

全球（日本除外）

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

日本

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## 文档

请确保您拥有最新版本的文档。每个文档的第 2 页将显示上次更新时间。每个指南的第 2 页上提供了文档版本信息。可在 Veritas 网站上获取最新文档：

<https://sort.veritas.com/documents>

## 文档反馈

您的反馈对我们很重要。建议改进意见，报告文档的错误或疏漏。包括您要报告的文本的文档标题、文档版本、章节标题和小节标题。将反馈发送至：

[vrpdocs@veritas.com](mailto:vrpdocs@veritas.com)

此外，还可以在 Veritas 社区网站上查看文档信息或提出问题：

<http://www.veritas.com/community/>

## Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) 是一个网站，提供了可用于自动化和简化某些耗时的管理任务的信息和工具。SORT 会根据具体产品帮助您准备安装和升级、识别数据中心的风险并提高操作效率。要了解 SORT 为您的产品提供了哪些服务和工具，请参见产品介绍：

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# 目录

<b>第 1 章</b>	<b>Resiliency Platform 概述</b> .....	<b>5</b>
	关于 Veritas Resiliency Platform .....	5
	关于 Resiliency Platform 功能和组件 .....	6
	关于 Resiliency Manager .....	8
	关于 Infrastructure Management Server (IMS) .....	8
	关于 Replication Gateway .....	10
	关于数据网关 .....	10
	关于 Resiliency Domain .....	11
	使用 Resiliency Platform 的恢复选项 .....	13
<b>第 2 章</b>	<b>规划环境以便使用 Resiliency Platform 进行灾难</b>	
	<b>恢复</b> .....	<b>14</b>
	关于 Veritas Resiliency Platform Data Mover .....	14
	Resiliency Platform Data Mover 的工作原理 .....	15
	Veritas Resiliency Platform Data Mover 如何处理虚拟机写入数据	
	.....	16
	Resiliency Platform Data Mover 的体系结构 .....	17
	关于 Resiliency Platform Data Mover 使用的同步 .....	19
	Resiliency Platform 部署中的复制 .....	21
	关于直接模式复制 .....	22
	关于对象存储模式复制 .....	22
	规划 Resiliency Domain 以提高效率和容错能力 .....	22
	开始使用 Resiliency Platform .....	24
	<b>索引</b> .....	<b>26</b>
	<b>术语表</b> .....	<b>27</b>

# Resiliency Platform 概述

本章节包括下列主题：

- [关于 Veritas Resiliency Platform](#)
- [关于 Resiliency Platform 功能和组件](#)
- [使用 Resiliency Platform 的恢复选项](#)

## 关于 Veritas Resiliency Platform

Veritas Resiliency Platform 提供统一的解决方案，可帮助您主动跨私有、公共和混合云维护业务运行时间。通过 Resiliency Platform，可以完成涉及数据中心中的虚拟机、应用程序和多层业务服务的所有弹性操作的自动化。通过插入到现有环境和基础架构中来保护当前技术投资。

对于数据复制，可以使用 Resiliency Platform Data Mover 或 Veritas Resiliency Platform 支持的任何第三方解决方案。有关支持的供应商和产品列表，请参见《Veritas Resiliency Platform 硬件和软件兼容性指南》。

Resiliency Platform Data Mover 是 Veritas Resiliency Platform 的单独许可功能。它可在地理位置分散的数据中心之间提供数据复制，从而促进有效的灾难恢复解决方案。Resiliency Platform Data Mover 可用于以下目的：

- 将 VMware 虚拟机恢复到 VMware 虚拟机
- 将 Linux 和 Windows 物理计算机恢复到 VMware 虚拟机
- 将 VMware 和 Hyper-V 虚拟机恢复到云数据中心
- 用于将 vCloud 虚拟机恢复到 vCloud 数据中心

Resiliency Platform 具有以下核心功能：

安全和遵从性

Veritas Resiliency Platform 为传输中的数据提供了增强的数据加密。

可预测性	客户可以预测性地满足关键业务恢复时间目标 (RTO) 和恢复点目标 (RPO)。
遵从性	客户可以通过审核报告和无中断的实时灾难恢复测试证明内外部业务连续性法规的遵从性。
自动化	客户可以实现所有弹性操作的完全自动化，包括恢复运行手册，以及启动和停止针对多层应用程序的恢复编排。这将降低人为错误造成的停机风险。
灵活性	客户可以灵活地保留其现有基础架构，可以利用 Resiliency Platform 所提供的灵活性按自己的条件进行创新，从而实现跨站点甚至云中的工作负载迁移。

请参见第 11 页的[“关于 Resiliency Domain”](#)。

## 关于 Resiliency Platform 功能和组件

下面简单介绍了 Veritas Resiliency Platform 的关键组件及其关系。负责部署和配置该产品的管理员需要详细了解这些信息。

Resiliency Manager	<p>在 Resiliency Domain 内提供弹性功能的组件。它由松散耦合服务、分布式数据存储库和管理控制台组成。Resiliency Manager 将作为虚拟设备进行部署。</p> <p>请参见第 8 页的<a href="#">“关于 Resiliency Manager”</a>。</p>
Infrastructure Management Server (IMS)	<p>发现、监控和管理数据中心内资产基础架构的组件。IMS 将有关资产基础架构的信息传输到 Resiliency Manager。IMS 将作为虚拟设备进行部署。</p> <p>要实现扩展，可以在同一数据中心内部署多个 IMS。</p> <p>请参见第 8 页的<a href="#">“关于 Infrastructure Management Server (IMS)”</a>。</p>
Replication Gateway	<p>Veritas Resiliency Platform Data Mover 的组件，作为虚拟设备部署在两个数据中心，用于在数据中心之间执行复制。</p> <p>如果计划使用任何第三方复制技术，则不需要部署 Replication Gateway。</p> <p>请参见第 10 页的<a href="#">“关于 Replication Gateway”</a>。</p>
数据网关	<p>Veritas Resiliency Platform 的组件，该组件在 AWS 数据中心内进行部署，以便使用对象存储启用复制。只有当您计划使用对象存储复制将数据中心资产恢复到 AWS 数据中心时，才需要部署此组件。</p> <p>请参见第 10 页的<a href="#">“关于数据网关”</a>。</p>

Resiliency Domain	<p>Resiliency Platform 部署的逻辑范围，包括两个数据中心内的 Resiliency Manager、IMS 和主机。</p> <p>它可以扩展到多个数据中心。</p> <p>请参见第 11 页的“关于 Resiliency Domain”。</p>
数据中心	<p>对于灾难恢复用例，Resiliency Domain 必须至少包含两个位于不同位置的数据中心（源数据中心和目标数据中心）。每个数据中心都拥有一个 Resiliency Manager 以及一个或多个 IMS。如果使用 Resiliency Platform Data Mover 进行复制，每个数据中心还必须至少拥有一个 Replication Gateway。</p>
资产基础架构	<p>一种数据中心资产，添加到 Resiliency Platform 后，便可由 IMS 发现并监控。</p> <p>资产基础架构可以包括虚拟机、物理计算机（Windows 或 Linux 服务器）、Hyper-V 和 VMware 的虚拟化服务器，以及 Enclosure（存储阵列）。一旦 IMS 发现了资产基础架构，控制台中将列出发现的虚拟机或应用程序以作为要管理或保护的资产。</p>
Resiliency Group	<p>Resiliency Platform 中的管理和控制单元。可以将相关资产组成一个 Resiliency Group，将其作为单个实体来管理和监控。</p>
Service Objective	<p>用于定义一组资产支持的操作和技术类型的模板。可以向每个 Resiliency Group 应用 Service Objective。</p> <p>标识服务特征的模板。这些可能是与可用性相关的特征（如局部冗余以及群集中的节点数）或 DR 特征（如远程恢复、恢复点目标 (RPO) SLA、演练支持等）。将一组资产添加到 Resiliency Group 时将应用 Service Objective。</p> <p>Resiliency Platform 将根据 Service Objective 定义来监控 Resiliency Group 并视情况提示风险。</p>
NetBackup Server	<p>允许使用 NetBackup 生成的备份映像将虚拟机还原到本地或远程数据中心的组件。</p> <p>仅当要使用 NetBackup 生成的备份映像还原虚拟机时，才需要添加此组件。</p>
Veritas InfoScale Operations Manager 管理服务器	<p>允许发现已在 Veritas InfoScale Operations Manager 中进行了配置的 InfoScale 应用程序的组件，也称为 Veritas InfoScale Operations Manager Server。可以在 Linux、Solaris、AIX 以及 Windows 平台上管理已在 Veritas InfoScale Operations Manager 中进行了配置的 InfoScale 应用程序。</p> <p>仅当要管理和恢复已在 Veritas InfoScale Operations Manager 中进行了配置的 InfoScale 应用程序时，才需要添加此组件。</p>

Virtual Business Service (VBS)

多层业务服务，其中每个 VBS 层托管一个或多个 Resiliency Group。通过 VBS，可以将多个服务分组成一个单元，以便执行虚拟化、自动化以及按照需要的顺序控制启动和停止操作。VBS 使用纵向分组机制来分组多个服务。可以对整个 VBS 执行灾难恢复操作。

## 关于 Resiliency Manager

Resiliency Manager 包含一组松散耦合服务、一个分布式数据存储库和一个管理 Web 控制台。Resiliency Manager 提供在 Resiliency Domain 中保护资产（如虚拟机）所需的服务。它还提供工作负载自动化服务。

首先，部署一个 Resiliency Manager，并创建 Resiliency Domain。然后，可以将多个 Resiliency Manager 添加到 Resiliency Domain，以提高本地访问的效率并实现容错。可以在同一数据中心或不同地理位置部署多个 Resiliency Manager。

Resiliency Manager 会从 Infrastructure Management Server (IMS) 中发现并管理与数据中心资产有关的信息，IMS 是另一个所需的 Resiliency Platform 组件。Resiliency Manager 将资产信息存储在其数据存储库中，并在其管理控制台中显示该信息。

属于同一域的多个 Resiliency Manager 会使用内置复制同步其数据库。每个 Resiliency Manager 都有其自己的 Web 控制台，但由于数据库已同步，所有控制台将显示相同数据。这样可以确保在任何一个 Resiliency Manager 不可用时数据的弹性和高可用性。可以从任何控制台执行操作，而结果将在 Resiliency Domain 的所有控制台中显示。

请参见第 11 页的“关于 Resiliency Domain”。

请参见第 8 页的“关于 Infrastructure Management Server (IMS)”。

## 关于 Infrastructure Management Server (IMS)

每个 Resiliency Manager 需要一个或多个 Infrastructure Management Server (IMS)。IMS 可发现和监控数据中心中的资产。使用 Web 控制台将资产基础架构添加到 Resiliency Platform，以便发现和监控 IMS。

资产基础架构可以包括主机、虚拟化服务器和 Enclosure（存储阵列）等对象。

IMS 会向 Resiliency Manager 发送资产相关信息，以便 Resiliency Manager 可以管理资产。从 Web 控制台启动的资产管理操作（例如启动或停止虚拟机）由 IMS 执行。

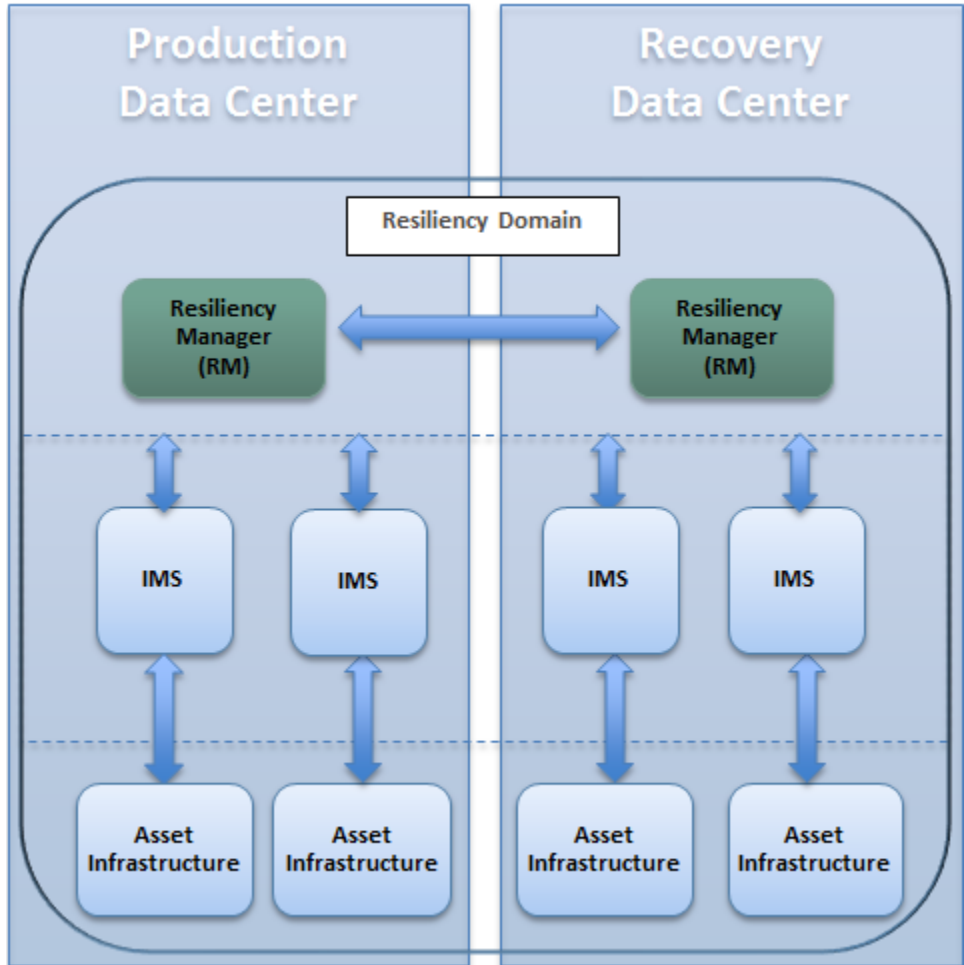
如果在不同地理位置有多个数据中心，可以为每个地理数据中心位置部署和配置单独的 IMS。

每个 IMS 一次只连接到一个 Resiliency Manager。如果出现 Resiliency Manager 故障，IMS 可以自动连接到同一域中的其他 Resiliency Manager。



此外，还可以在同一数据中心配置多个 Infrastructure Management Server。例如，为实现扩展，可以为单独的业务单元（如人力资源或财务）添加单独的 IMS。同一 Resiliency Manager 可以托管多个 IMS。

图 1-1 数据中心中的多个 Infrastructure Management Server



请参见第 11 页的“关于 Resiliency Domain”。

请参见第 8 页的“关于 Resiliency Manager”。

## 关于 Replication Gateway

如果计划将 Resiliency Platform Data Mover 用于环境中的数据复制，则需要在源和目标数据中心中部署和配置至少一个 Replication Gateway。

Veritas Resiliency Platform 的 Replication Gateway 组件是临时服务器，可在复制过程中汇总和批处理多个虚拟机的数据。Gateway 还会执行数据优化，如本地重复数据删除和压缩。源数据中心上的 Gateway 与目标数据中心上的 Gateway 始终配对。目标数据中心 Gateway 是临时服务器，可将数据应用到源数据中心存储。

每个 Replication Gateway 包括以下组件：

- I/O 接收器  
接收由应用程序主机以连续方式收集和发送的应用程序 I/O。
- 收发器  
定期通过 WAN 链接传输和接收数据。
- 填充器  
在云 Gateway 上接收数据后将其应用于存储。
- 调度程序  
在 Gateway 中管理作业和策略。
- 引擎  
维护复制状态并与所有其他组件进行协调。

## 关于数据网关

如果要选择对象存储复制模式以将资产迁移到 AWS，您需要在 AWS 环境中部署数据网关。

数据网关的作用类似于本地 Replication Gateway 和云 Replication Gateway 之间的通信通道。将从本地数据中心复制的数据压缩并以对象的形式存储在 S3 存储桶中。云 Replication Gateway 从 S3 存储桶中拉取该数据，将其解压缩，然后应用到目标磁盘。

可以使用单个数据网关在多个 Replication Gateway 之间复制数据。

要在 AWS 中部署数据网关，您需要下载 Veritas Resiliency Platform 随附的 zip 文件。

在 AWS 环境中部署数据网关时，可在 AWS 中创建一些资源。数据网关正在使用时不得删除这些资源，因为可能会影响产品的功能和特性。删除数据网关后，将自动删除这些资源。

## 关于 Resiliency Domain

Resiliency Domain 是 Veritas Resiliency Platform 部署的管理域。它表示部署的范围，可以分布在多个数据中心，并且可以包括多个 Resiliency Manager 和其他组件（如 IMS），以及要管理和保护的基础架构。在 Resiliency Domain 中，Resiliency Platform 可以保护资产，还可以协调资产工作负载任务的自动化。

Resiliency Domain 是部署环境中第一个 Resiliency Manager 并访问 Resiliency Manager 后从 Web 控制台创建的逻辑对象。

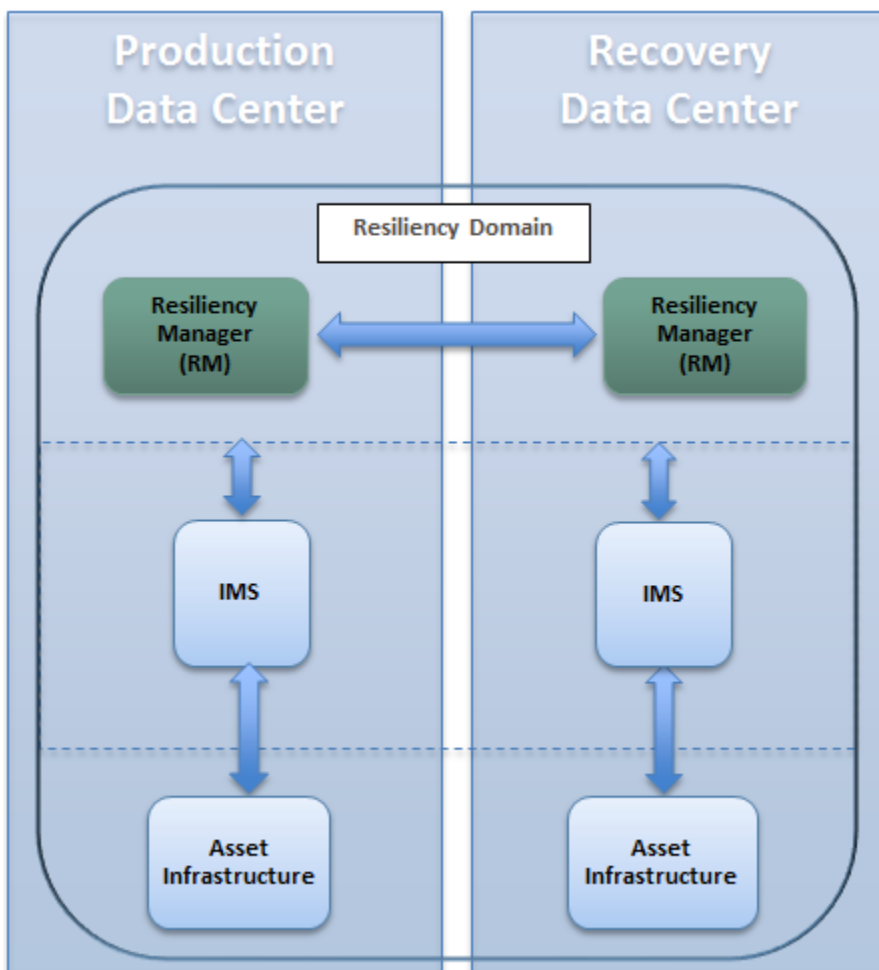
要进行灾难恢复，Resiliency Domain 必须包含至少两个数据中心，一个源数据中心和一个目标数据中心（可位于本地或云中）。

可以选择在单个数据中心实施 Resiliency Domain，以实现工作负载任务自动化。

资产基础架构包括将添加到 Resiliency Platform 用于 IMS 发现和监控的数据中心资产。资产基础架构可以包括虚拟和物理主机（Windows 或 Linux 服务器）以及 Hyper-V 和 VMware 虚拟化服务器。

根据所采用的复制技术，资产基础架构还可包括 Replication Gateway 或 Enclosure（存储阵列）。此图中不显示资产基础架构的复制详细信息。

图 1-2 Resiliency Domain 中的 Resiliency Platform 组件



请参见第 21 页的“Resiliency Platform 部署中的复制”。

请参见第 8 页的“关于 Resiliency Manager”。

请参见第 8 页的“关于 Infrastructure Management Server (IMS)”。

请参见第 22 页的“规划 Resiliency Domain 以提高效率和容错能力”。

## 使用 Resiliency Platform 的恢复选项

Resiliency Platform 可使用各种恢复选项。您可以使用任何受支持的第三方复制技术（NetBackup 或 Resiliency Platform Data Mover）复制并恢复数据中心上的数据。此外，也可以使用 Resiliency Platform 恢复 InfoScale 应用程序。

表 1-1

类别	恢复选项
使用第三方复制	恢复到本地数据中心： <ul style="list-style-type: none"><li>■ 将 VMware 虚拟机恢复到本地数据中心</li><li>■ 将 Hyper-V 虚拟机恢复到本地数据中心</li><li>■ 将应用程序恢复到本地数据中心</li></ul>
使用 NetBackup	恢复到本地和远程数据中心： <ul style="list-style-type: none"><li>■ 将 VMware 虚拟机恢复到本地和远程数据中心</li></ul>
使用 Resiliency Platform Data Mover	<ul style="list-style-type: none"><li>■ 恢复到本地数据中心：<ul style="list-style-type: none"><li>■ 使用 VAIO 将 VMware 虚拟机恢复到本地数据中心</li></ul></li><li>■ 恢复到 AWS 数据中心：<ul style="list-style-type: none"><li>■ 将 VMware 虚拟机恢复到 AWS 数据中心</li><li>■ 将 Hyper-V 虚拟机恢复到 AWS 数据中心</li></ul></li><li>■ 恢复到 vCloud 数据中心：<ul style="list-style-type: none"><li>■ 将 VMware 虚拟机恢复到 vCloud 数据中心</li><li>■ 将 Hyper-V 虚拟机恢复到 vCloud 数据中心</li><li>■ 将 VMware 虚拟机恢复到 vCloud 数据中心而不添加 vCenter 服务器</li><li>■ 将 Hyper-V 虚拟机恢复到 vCloud 数据中心而不添加 Hyper-V Server</li></ul></li><li>■ 恢复到 Azure 数据中心：<ul style="list-style-type: none"><li>■ 将 VMware 虚拟机恢复到 Azure 数据中心</li><li>■ 将 Hyper-V 虚拟机恢复到 Azure 数据中心</li></ul></li><li>■ 恢复到 OpenStack 数据中心：<ul style="list-style-type: none"><li>■ 将 VMware 虚拟机恢复到 OpenStack 数据中心</li><li>■ 将 Hyper-V 虚拟机恢复到 OpenStack 数据中心</li></ul></li></ul>
使用 Veritas InfoScale Management Server	恢复到本地数据中心： <ul style="list-style-type: none"><li>■ 将 InfoScale 应用程序恢复到本地数据中心</li></ul>

# 规划环境以便使用 Resiliency Platform 进行灾 难恢复

本章节包括下列主题：

- [关于 Veritas Resiliency Platform Data Mover](#)
- [Resiliency Platform 部署中的复制](#)
- [规划 Resiliency Domain 以提高效率和容错能力](#)
- [开始使用 Resiliency Platform](#)

## 关于 Veritas Resiliency Platform Data Mover

Veritas Resiliency Platform Data Mover 是 Veritas Resiliency Platform 的许可功能。

Resiliency Platform Data Mover 是一款复制解决方案，它使用由 VMware API I/O Filtering (VAIO) 框架所提供的 API 构建。该框架可供合作伙伴为客户创建自己的复制或缓存数据服务。Resiliency Platform Data Mover 解决方案已通过 VMware 认证。有关 VMware API I/O Filtering 框架的详细信息，请参考 VMware 文档。

Veritas Resiliency Platform Data Mover 仅允许复制 VMware 虚拟机。Veritas Resiliency Platform Data Mover 可在地理位置分散的数据中心之间提供数据复制，从而促进有效的灾难恢复解决方案。

Veritas Resiliency Platform Data Mover 包括以下功能：

- 复制虚拟机，包括通过 LAN 或 WAN 环境中的任何 IP 网络将其引导磁盘和数据磁盘从源数据中心复制到目标数据中心。

- 轻松恢复目标数据中心的虚拟机。
- 确保虚拟机的数据一致性。
- 在 Resiliency Group 级别恢复受 Data Mover 保护的虚拟机。
- 启用对目标数据中心恢复的无中断测试。

## Resiliency Platform Data Mover 的工作原理

Resiliency Platform 的 Veritas Resiliency Platform Data Mover 功能可将本地（源）数据中心的所有虚拟机复制到远程（目标）数据中心。该复制功能将提供完全一致的数据副本。如果源数据中心发生灾难，Resiliency Platform 可使用目标（远程）数据中心上的数据副本在远程数据中心上置备和启动虚拟机。

要使用 Resiliency Platform Data Mover 保护虚拟机，请将源数据中心的虚拟机分组到使用 Resiliency Platform Data Mover 提供灾难恢复保护的 Resiliency Group。Resiliency Group 是恢复单元，因此，需要一起恢复的虚拟机必须位于同一 Resiliency Group 中。

在配置过程中，Resiliency Platform 将虚拟机放在与虚拟机关联的多个 Veritas Replication Set 和复制单元中。每个 Veritas Replication Set 适用于单个虚拟机并包含连接到该虚拟机的所有磁盘（包括引导和数据磁盘）。每个组成磁盘称为复制单元。

当应用程序或虚拟机运行时，多个进程将以特定顺序对磁盘执行写入。例如，数据库会先将任何数据库更改发布到日志中，然后再向表空间执行写入。“写入顺序保真”这一术语是指，保持对所有组成磁盘（即复制单元）的写入都始终按顺序进行。

当复制处于活动状态时，Resiliency Platform Data Mover 将维持 Veritas Replication Set 的写入顺序保真。写入顺序保真可确保目标数据中心内的数据是一致的。即便目标数据中心的数据可能不是最新副本，Data Mover 也将确保此数据始终保持一致。

Resiliency Platform Data Mover 将按照写入数据的接收顺序跟踪源数据中心上的虚拟机的写入数据。它将以相同顺序在目标数据中心上应用写入数据，从而维持写入顺序保真。

复制包括对虚拟机的引导磁盘所做的任何更改。因此，如果源数据中心上发生灾难或者执行了计划的迁移，虚拟机可以在恢复数据中心上启动。Resiliency Platform 中的灾难恢复操作将置备恢复数据中心内的虚拟机，以便它们在操作期间联机。

### 关于复制可调参数

如果您使用 Resiliency Platform Data Mover 在数据中心之间复制数据，可以选择调整某些复制参数以优化复制操作的性能和可扩展性。

Resiliency Platform Data Mover 将数据从源数据中心的受保护虚拟机复制到目标数据中心的目標磁盤。Veritas Resiliency Platform 的 Replication Gateway 组件是一个临时服务器，可在复制期间聚合和批处理多个虚拟机中的数据。Veritas Resiliency Platform 的 Replication Gateway 组件上的分段存储包含以下两个部分：

- **预留存储：**Replication Gateway 将分段存储磁盤的特定部分分配给每个受保护的虚拟机。分段存储的此部分称为预留存储。
- **共享池：**分段存储的此部分在所有虚拟机之间共享。

## 可以调整的参数

以下是三个可调整的 Replication Gateway 参数（以优化恢复点目标 (RPO)、复制性能和可扩展性）：

- **更新集：**在将日期发送到目标 Replication Gateway 之前，源 Replication Gateway 会实施数据优化技术并创建数据集。在一段时间内收集的此数据集称为更新集。
- **复制频率：**设置为用于分隔和剪切更新集的时间段称为复制频率。在剪切更新集后，会调度更新集以传输到目标 Replication Gateway。
- **每个 Veritas Replication Set 的配额：**为预留存储中的每个虚拟机预留的空间称为每个 Veritas Replication Set 的配额。

表 2-1

可调参数类型	变更影响
每个 Veritas Replication Set 的配额 (Quota-per-CG)	扩展（受 Replication Gateway 保护的虚拟机数）
更新集大小 (Update-set-size)	性能（本地重复数据删除）、压缩、RPO
复制频率	在网关上配置的所有 Resiliency Group 的 RPO

以下公式用于链接上述复制可调参数：

预留存储 = 虚拟机数 \* 每个 Veritas Replication Set 的配额

更新集数量 = 每个 Veritas Replication Set 的配额/更新集大小。将始终在网关上预留用于此大量更新集的空间。

您可以使用 klish 菜单命令调整 Quota-per-CG、update-set-size 和 replication-frequency。

## Veritas Resiliency Platform Data Mover 如何处理虚拟机写入数据

Veritas Resiliency Platform Data Mover 将使用 ESXi 主机上运行的 vtstap 服务拦截和处理受保护的虚拟机写入数据。vtstap 服务将拦截指向存储的写入数据，同时直接从虚拟机存储处理读取数据。



vtstap 服务会记录写入 I/O 的位置，并对写入数据进行排序。写入数据将应用到虚拟机存储，然后，排序的写入数据会异步发送到源 Replication Gateway。在源 Replication Gateway 上累积的写入数据将定期发送到目标 Replication Gateway。目标 Replication Gateway 会按顺序向目标数据中心存储应用写入数据。这可确保源和目标数据中心上的数据一致。由于 Resiliency Platform Data Mover 使用异步复制，源和目标数据之间可能存在延迟，但始终保持一致。

Resiliency Platform Data Mover 通过按照列出的顺序执行以下步骤来处理传入的写入数据：

- 访客虚拟机中的操作系统向虚拟机存储发出写入数据。
- I/O Tap 模块 (vtstap) 记录 I/O 的位置。
- 将 IO 写入到虚拟机存储。
- vtstap 模块通过网络将 I/O 数据发送到源 Replication Gateway 中的 I/O 接收器。
- I/O 接收器聚合 I/O。
- 源 Replication Gateway 上的收发器将通过网络定期向目标 Replication Gateway 上的收发器发送 I/O。
- 然后，I/O 将发送到填充器，填充器将它们写入到目标数据中心存储。

## 复制精简磁盘

Resiliency Platform 支持通过在目标数据中心上置备相应的精简磁盘，以最佳方式保护具有精简磁盘的虚拟机。Resiliency Platform Data Mover 只会将使用的块从源数据中心上的磁盘复制到目标数据中心上的磁盘，从而保持磁盘的精简性质。除了精简磁盘，Resiliency Platform Data Mover 还会将使用的块从厚置备（延迟置零置备）磁盘复制到目标数据中心上的磁盘。

如果源数据中心上具有基于 NFS 的 Datastore，那么不管源数据中心上是何种磁盘类型，都将在目标数据中心上创建厚置备磁盘。这是必需操作，因为 NFS 层不使用精简配置。

当您从 3.1 或更早版本升级到 3.2 或更高版本时，如果源数据中心上具有精简磁盘并且已为 Resiliency Group 配置了灾难恢复 (DR)，您需要在升级后删除现有的 Resiliency Group。对 Resiliency Group 进行重新配置以利用精简置备功能。如果从 3.1 Update 1 进行升级，则无需执行此步骤。

## Resiliency Platform Data Mover 的体系结构

如果要将 VMware 虚拟机从一个本地数据中心恢复到另一个本地数据中心，则使用的复制技术为带 VMware vSphere APIs for I/O Filtering (VAIO) 框架的 Resiliency Platform Data Mover。该框架为经过 VMware 认证的复制提供 I/O 过滤器。该过滤器在 ESXi 服务器中运行，并拦截在访客操作系统和虚拟磁盘之间移动的 I/O 请求。有关 VMware API I/O Filtering 框架的详细信息，请参考 VMware 文档。

Resiliency Platform Data Mover 将在运行受保护虚拟机的 ESXi 主机上部署名为 **vtstap** 的用户空间模块。此模块使用 VMware VAIO API 来构建以拦截和复制来自虚拟机的 I/O。

在 Veritas Resiliency Platform Data Mover 过滤运行虚拟机的 ESXi 主机用户空间中的 I/O 后，I/O 将先通过源数据中心 Replication Gateway 中的以下路径，然后再复制到目标数据中心。

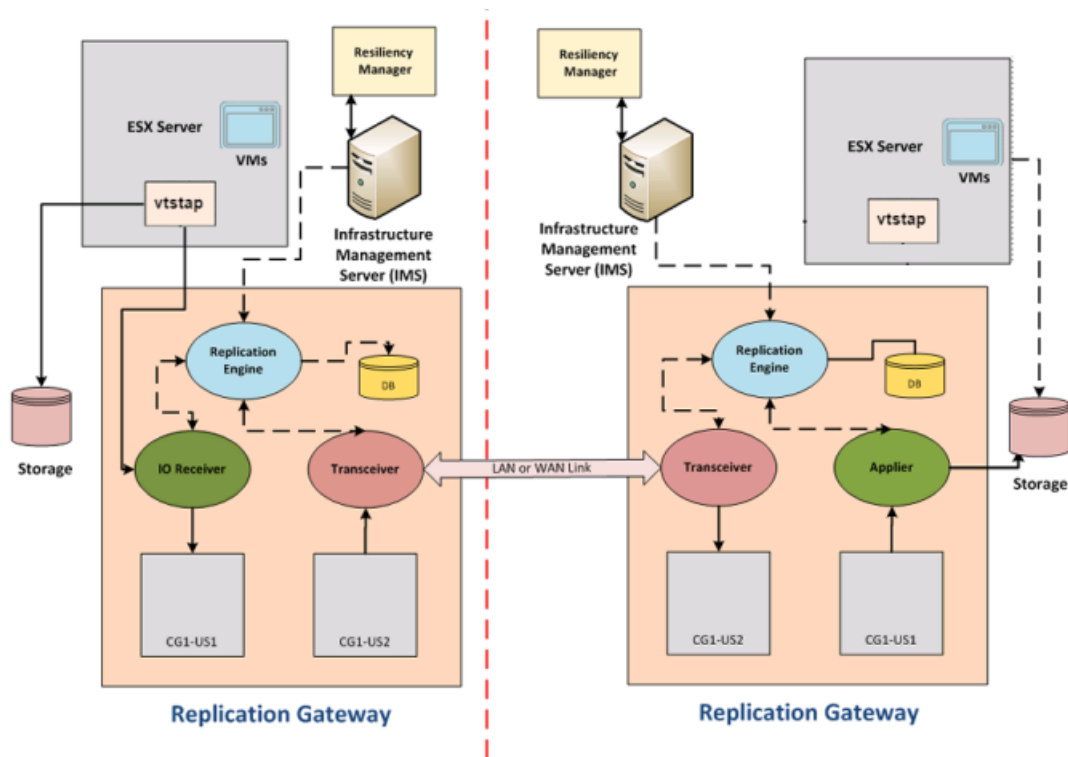
每个 Replication Gateway 包括四个在启用复制时运行的后台驻留程序：

- I/O 接收器  
持续接收由运行虚拟机的 ESXi 主机中的 **vtstap** 模块收集和发送的虚拟机 I/O。
- 收发器  
定期通过 WAN 链接传输和接收数据。
- 填充器  
在目标网关上收到数据之后将数据应用到存储。
- 调度程序  
管理和调度网关之间的数据传输。
- 引擎  
维护复制状态并与所有其他组件进行协调。

仅当运行灾难恢复操作（如接管）时，才会置备目标（恢复）数据中心上的虚拟机。之后，灾难恢复操作可使恢复数据中心内的虚拟机联机。如此可避免不必要的资源利用并计算其他数据中心内运行的工作负载。

要使用 Veritas Resiliency Platform Data Mover，源 Replication Gateway 和目标 Replication Gateway 将一起链接到 Replication Gateway 对。这将在源和目标数据中心之间建立复制通道。您可以选择对网关之间的通信进行加密，除非您使用专用 VPN 链接。

图 2-1 复制体系结构



## 关于 Resiliency Platform Data Mover 使用的同步

Veritas Resiliency Platform Data Mover 可使用两种类型的同步技术将数据从源数据中心复制到目标数据中心：

- 请参见第 19 页的“[关于数据完全同步](#)”。
- 请参见第 20 页的“[关于增量同步](#)”。

您无法在这两种类型的同步技术之间进行选择。在任何时候，所使用的同步技术均由 Resiliency Platform 根据要求在内部决定。

### 关于数据完全同步

Veritas Resiliency Platform 仅在以下情况下使用完全同步：

- 为 Resiliency Group 进行灾难恢复配置后：  
为 Resiliency Group 配置 Data Mover 时，启动复制。此时，目标数据中心上的存储必须与源数据中心的数据同步。这一同步整个数据集的过程是完全同步。

- 在接管操作后执行的重新同步操作期间：  
在接管之后，也需要进行完全同步。接管是源数据中心由于灾难而关闭时由用户发起的活动，需要在目标数据中心启动虚拟机才能提供业务连续性。在接管之后，虚拟机将在目标数据中心中运行。备份源数据中心并且其正常运行后，必须从目标数据中心执行重新同步操作，然后才能迁移回源数据中心。此重新同步操作将启动完全同步，将源数据中心上的数据与目标数据中心的数据进行同步。同步完成后，源数据中心将保持最新状态。然后，可以执行迁移操作。
- 从任何受保护的虚拟机添加或删除磁盘后：  
如果从任何受保护的虚拟机添加或删除磁盘，将引发风险。需要编辑 **Resiliency Group** 来解决此风险。在此编辑 **Resiliency Group** 操作期间，可以删除受影响的虚拟机。再次编辑 **Resiliency Group** 以重新添加虚拟机并更新配置。在编辑 **Resiliency Group** 操作完成后，启动完全同步。

完全同步所需的时间量取决于多个因素。这些因素包括复制磁盘的大小、LAN 和 WAN 环境的网络带宽以及在同步过程中发生的 I/O 量。完全同步完成后，复制将进入活动状态。在活动状态下，**Data Mover** 将维护写入顺序保真度。

如果复制状态是“正在同步”，可以在 **Resiliency Group** 详细信息页面上查看数据复制的状态。将在状态栏上使用完成百分比信息显示进度。同步数据所需的时间也会显示在此页面。

有时，在发生磁盘故障或基础架构故障后，需要手动调用完全同步以恢复复制。有关需要进行完全同步的情况的详细信息：

请参见第 19 页的[“关于 Resiliency Platform Data Mover 使用的同步”](#)。

## 关于增量同步

增量同步的目标是仅同步自上次同步（增量或完全同步）以来发生更改的数据。增量同步可节省在数据中心之间复制数据所使用的大量时间和资源。

除了在 **Veritas Resiliency Platform** 中执行完全同步的两种情况（在灾难恢复配置后和执行接管操作后），在所有其他时候，**Resiliency Platform** 在将数据从源数据中心复制到目标数据中心时使用增量同步。在 **Resiliency Platform** 中使用增量同步的这些实例包括：

- 如果在复制路径中有任何网络故障
- 如果 **Replication Gateway** 或受保护虚拟机发生系统重新启动
- 如果将正常运行或发生故障的 **Replication Gateway** 替换为另一个 **Replication Gateway**
- 如果执行迁移操作。在这种情况下，虚拟机将在目标站点上启动，然后复制方向发生更改。此时，**Resiliency Platform** 使用增量同步。

如果复制状态是“正在同步”，可以在 Resiliency Group 详细信息页面上查看数据复制的状态。将在状态栏上使用完成百分比信息显示进度。同步数据所需的时间也会显示在此页面。

请参见第 19 页的[“关于 Resiliency Platform Data Mover 使用的同步”](#)。

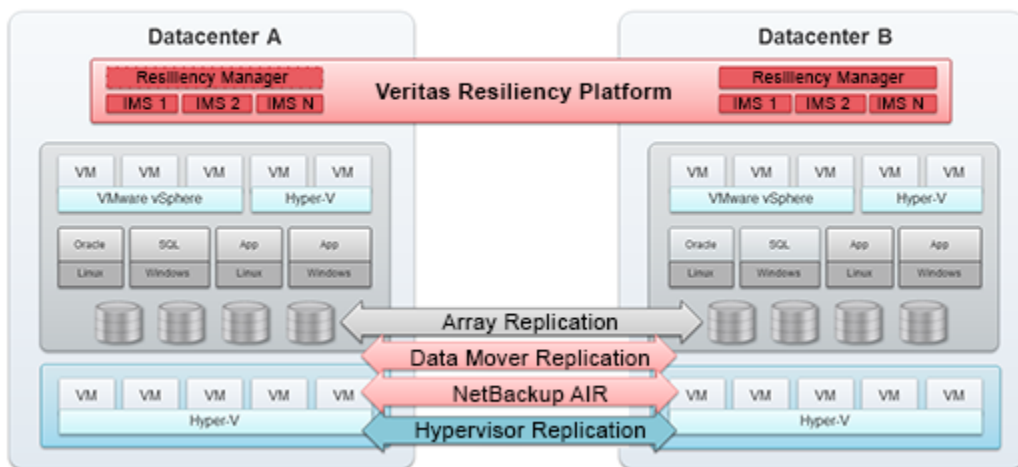
## Resiliency Platform 部署中的复制

Veritas Resiliency Platform 支持多种形式的复制，以便进行从源数据中心到目标数据中心的数据恢复。

- 使用支持的阵列进行基于阵列的复制（基于块的复制）
- 使用 Hyper-V Replica 进行基于 Hypervisor 的复制
- NetBackup 自动映像复制 (AIR)
- Resiliency Platform Data Mover（Resiliency Platform 的单独许可功能）

有关支持的复制硬件和软件的详细信息，请参考“硬件和软件兼容性列表”。

图 2-2 Resiliency Platform 部署中的复制



使用 Resiliency Platform Data Mover 将数据中心资产恢复到 AWS 时，可以选择两种复制模式：直接模式和对象存储模式。

## 关于直接模式复制

要使用 Veritas Resiliency Platform 将数据中心资产迁移到 Amazon Web Services (AWS)，可选择以下两种复制模式之一：直接模式和对象存储模式。

要使用 Veritas Resiliency Platform 迁移到 AWS 以外的数据中心，只能使用直接模式复制。

源数据中心的 Replication Gateway 始终与目标数据中心的 Replication Gateway 配对。在直接模式复制中，源数据中心的 Replication Gateway 直接与目标数据中心的 Replication Gateway 通信。源站点 Replication Gateway 充当临时服务器，它将在复制期间聚合和批处理多个虚拟机中的数据。目标数据中心 Gateway 是临时服务器，可将数据应用到恢复数据中心存储。

## 关于对象存储模式复制

如果要 将数据中心资产迁移到 AWS，可以选择在对象存储模式复制和直接模式复制之间进行选择。要启用对象存储模式复制，需要在 AWS 环境中部署数据网关。

请参见第 10 页的“[关于数据网关](#)”。

以下是在 Resiliency Platform 中使用对象存储模式复制的一些优点：

- 通过利用 AWS 服务实现可扩展性，根据用户需求自动扩展。
- 有助于实现 Replication Gateway 的弹性。由于数据不断进行复制，并且存储在 S3 存储桶中，因此目标数据中心上的 Replication Gateway 出现故障不会影响复制。

如果目标数据中心上的 Replication Gateway 出现故障，则在恢复或更换该网关后执行数据同步。如果源数据中心上的 Replication Gateway 在完成同步之前出现故障，则在使用直接复制模式时可能会丢失一些数据。但是，如果使用的是对象存储模式复制，则可从 S3 存储桶中拉取数据，因而不会丢失任何数据。

## 规划 Resiliency Domain 以提高效率和容错能力

在部署 Veritas Resiliency Platform 之前，应计划如何扩展部署以提高效率和容错能力。

尽管 Resiliency Domain 只需要一个 Resiliency Manager，您可以向域中添加多个 Resiliency Manager 实例。例如，可以按地理位置分布 Resiliency Manager 以提高本地访问的效率。为实现弹性部署，甚至可以在一个数据中心内有多个 Resiliency Manager。

如果 Resiliency Domain 中有多个 Resiliency Manager，建议两个 Resiliency Manager 之间的建议 WAN 延迟小于 30 毫秒。两个 Resiliency Manager 之间允许的最大 WAN 延迟为 50 毫秒。此延迟要求适用于位于一个数据中心或两个不同数据中心内的任意两个 Resiliency Manager。

对于生产环境中本地数据中心的灾难恢复，建议的最低部署为四个虚拟设备：源数据中心和目标数据中心内各一个 Resiliency Manager 和一个 Infrastructure Management Server (IMS)。在测试环境中，目标数据中心可以只有一个 Resiliency Manager。

对于云数据中心的灾难恢复，建议的最低部署为三个虚拟设备：源数据中心内一个 IMS，目标数据中心内一个 Resiliency Manager 和一个 IMS。

源数据中心和目标数据中心不需要 IMS 的一对一映射。例如，源数据中心可以有两个 IMS，目标数据中心可以有一个 IMS。可以将多个 Infrastructure Management Server (IMS) 添加到 Resiliency Domain。例如，如果要管理不同地理位置的多个数据中心，可以为每个地理数据中心位置配置单独的 IMS。此外，还可以在同一数据中心内配置多个 IMS。

如果计划使用 Resiliency Platform Data Mover 进行复制，则每个数据中心还需要至少一个额外的 Replication Gateway。Resiliency Platform 支持非对称配对的 Replication Gateway。此功能有助于根据数据传输速率和技术特定限制，在每一端仅部署所需数量的网关。源站点上的一个网关可以与目标站点上的多个网关配对，反之亦然。一个网关可以与对等站点上最多 16 个网关配对。

对于受网关对保护的每台虚拟机，源和目标网关都必须具有相当于 12 GB 的外部存储。例如，如果网关对支持 10 台虚拟机，则每个源和恢复（目标）网关都必须具有 120 GB 的外部存储。外部存储的最小大小必须是 50 GB。

表 2-2 参考主题

有关以下内容的详细信息...	请参考...
网络	<a href="#">关于 FIPS 支持</a> <a href="#">关于 NAT 支持</a> <a href="#">关于 IPv6 支持</a>
Resiliency Platform 复制设备的容量规划	<a href="#">VMware vSphere 环境</a> <a href="#">VMware vSphere 和 Azure 环境</a> <a href="#">VMware vSphere 和 AWS 环境</a>
数据中心需要的网络对象和网络对象映射	<a href="#">关于网络对象</a> <a href="#">在数据中心之间创建网络对</a>

请参见第 11 页的“[关于 Resiliency Domain](#)”。

请参见第 8 页的“[关于 Resiliency Manager](#)”。

请参见第 8 页的“[关于 Infrastructure Management Server \(IMS\)](#)”。

# 开始使用 Resiliency Platform

下表介绍了客户开始使用 Resiliency Platform 所涉及的各个步骤以及在执行每个步骤期间预期达到的效果：

表 2-3 开始使用 Resiliency Platform

步骤	说明
部署	<ul style="list-style-type: none"> <li>■ 部署 Resiliency Platform 虚拟设备并将其配置为 Resiliency Manager、Infrastructure Management Server (IMS) 或 Replication Gateway</li> <li>■ 通过快速入门向导定义 Resiliency Domain</li> <li>■ 将资产添加到 Resiliency Domain 以进行发现：                             <ul style="list-style-type: none"> <li>■ 虚拟机</li> <li>■ 应用程序</li> <li>■ 存储 Enclosure</li> </ul> </li> </ul>
发现	<ul style="list-style-type: none"> <li>■ Resiliency Platform 的深度发现能够标识以下内容：                             <ul style="list-style-type: none"> <li>■ 虚拟机</li> <li>■ 应用程序</li> <li>■ 存储 Enclosure</li> <li>■ 软件/硬件复制</li> <li>■ 虚拟网络 (vSwitch)</li> </ul> </li> </ul>
定义服务级别目标	<ul style="list-style-type: none"> <li>■ 基于预期恢复点目标 (RPO) 配置服务级别目标。由服务级别目标驱动的配置可启用以下功能：                             <ul style="list-style-type: none"> <li>■ 对资产进行基本监控</li> <li>■ 恢复资产</li> <li>■ 恢复多层业务服务 (VBS)</li> <li>■ 报告资产的运行状况</li> <li>■ 针对受保护资产的风险警报和通知</li> </ul> </li> </ul>



步骤	说明
管理	<ul style="list-style-type: none"> <li>■ 针对 Resiliency Group 和 VBS 的一键单击演练可验证灾难就绪性： <ul style="list-style-type: none"> <li>■ 自动演练</li> <li>■ 自动演练清理</li> <li>■ 对演练期间的工作负载进行网络隔离的选项</li> </ul> </li> <li>■ 针对 Resiliency Group 和 VBS 的一键单击恢复或迁移操作： <ul style="list-style-type: none"> <li>■ 根据服务级别目标进行自动恢复或迁移</li> <li>■ 使用预定义的网络自定义进行恢复</li> <li>■ 根据预定义的分组或顺序进行恢复</li> <li>■ 使用 Resiliency Plan 进行受控恢复</li> </ul> </li> <li>■ 针对 Resiliency Group 和 VBS 的一键单击撤离计划： <ul style="list-style-type: none"> <li>■ 为 VBS 定义优先级的选项</li> <li>■ 针对撤离计划的自动演练或清理演练</li> </ul> </li> </ul>

# 索引

## B

部署  
    复制 21

## D

Data Mover  
    处理应用程序写入数据 16  
    概述 14  
    关于 15  
Data Mover VAI0  
    体系结构 17

## F

复制  
    对象存储 22  
    可调参数 15  
    直接 22  
复制块跟踪磁盘  
    关于 16

## G

概述  
    IMS 8  
    Replication Gateway 10  
    Resiliency Domain 11  
    Resiliency Manager 8  
    数据网关 10

## S

数据复制  
    同步数据 19  
    完全同步 19  
数据网关 22

## T

同步数据  
    关于 19

## V

vtstap  
    关于 16

## W

完全同步  
    关于 19

# 术语表

Infrastructure Management Server (IMS)	用于发现、监控和管理数据中心内资产基础架构的 Veritas Resiliency Platform 组件。IMS 将有关资产基础架构的信息传输到 Resiliency Manager。
klish	命令行界面 SHell。在初始的引导配置后，在虚拟设备上提供命令行菜单以供您使用。
Replication Gateway	在源数据中心和目标数据中心之间执行数据复制的 Veritas Resiliency Platform 组件。
Resiliency Domain:	Resiliency Platform 部署的逻辑范围。它可以扩展到多个数据中心。
Resiliency Group	Veritas Resiliency Platform 中的管理和控制单元。相关的资产被分组到作为一个实体来管理和监视的 Resiliency Group 中。
Resiliency Manager	在 Resiliency Domain 内提供弹性功能的 Veritas Resiliency Platform 组件。它由松散耦合服务、分布式数据存储库和管理 Web 控制台组成。
Resiliency Plan	任务或操作，以及在预定义序列中执行的相关资产的集合。
Resiliency Plan 模板	定义任务或操作集合的执行顺序的模板。
Resiliency Platform Data Mover 复制主机	要使用 Resiliency Platform Data Mover 复制技术启用复制，需要添加资产并为复制做好准备。资产可以是物理计算机或虚拟机。
VAIO 框架	VMware 框架由用于 I/O Filtering 的 vSphere API 组成。此框架使得 Veritas Resiliency Platform 能够在 ESXi 服务器上运行过滤器并拦截任何从访客操作系统到虚拟磁盘的 I/O 请求。
Veritas Replication Set	属于 Resiliency Group 的虚拟机称为 Veritas Replication Set。连接到此虚拟机的所有磁盘（包括引导磁盘和数据磁盘）构成 Veritas Replication Set。在给定的 Replication Set 中所有磁盘之间维护写入顺序保真度。
Virtual Business Service (VBS)	多层 IT 服务，其中每个 VBS 层托管一个或多个 Resiliency Group。VBS 可以将多个服务分组成一个单元，以便执行虚拟化、自动化以及按照需要的顺序进行灾难恢复。
web 控制台	位于 Resiliency Manager 上的基于 web 的管理控制台，用于配置 Resiliency Domain 的设置并执行操作。
主机	在 Veritas Resiliency Platform 中，主机一词代表应用程序主机、Resiliency Platform Data Mover 主机、存储发现主机、VMware 发现主机和 Hyper-V 主机。
加载项	可以通过 Infrastructure Management Server (IMS) 安装在主机的专用附加软件包。

<b>层</b>	在 Virtual Business Service (VBS) 中，Resiliency Group 按层排列。层表示 Resiliency Group 之间的逻辑依赖性，并可确定 Resiliency Group 上操作执行的相对顺序。
<b>接管</b>	源数据中心由于灾难而关闭时由用户发起的活动，需要在目标数据中心还原资产才能提供业务连续性。
<b>数据中心</b>	一个包含由 Veritas Resiliency Platform 来管理的资产基础架构的位置。 对于此灾难恢复用例，Resiliency Domain 必须至少包含两个位于不同位置的数据中心（源数据中心和目标数据中心）。每个数据中心都拥有一个 Resiliency Manager 以及一个或多个 IMS。
<b>活动</b>	在 Resiliency Group 上执行的任务或操作。
<b>源数据中心</b>	通常情况下用于业务的数据中心。
<b>演练</b>	零停机时间测试，可模拟 Resiliency Group 的配置、应用程序数据、存储和故障转移行为。 演练会在灾难发生期间验证 Resiliency Group 故障转移到恢复数据中心的能力。
<b>目标数据中心</b>	出现灾难情景时使用的数据中心。
<b>虚拟设备</b>	包括操作系统环境以及与虚拟机一起部署的软件应用程序。 Veritas Resiliency Platform 虚拟设备将作为虚拟机进行部署，然后使用基本设置和角色进行配置（例如，Resiliency Manager）。
<b>角色</b>	有权访问一组预定义作业（操作）的用户角色。用于对 Veritas Resiliency Platformweb 控制台操作的用户和组分配权限。
<b>资产</b>	已被 Infrastructure Management Server (IMS) 发现的和可被分组为 Resiliency Group 的虚拟机、物理机、或应用程序。
<b>资产基础架构</b>	能够添加到用于 IMS 发现和监视的 Infrastructure Management Server (IMS) 数据中心资产。例如，虚拟化服务器、虚拟机、磁盘阵列和应用程序。
<b>迁移</b>	计划在源数据中心正常关闭资产，然后在目标数据中心启动资产的活动。在此过程中，复制可确保目标数据中心上提供的数据的一致性。