MICRO FOCUS

Data Protector

软件版本：10.00

灾难恢复指南

文档发行日期：2017 年 6 月
软件发行日期：2017 年 6 月

法律声明

担保

Micro Focus or one of its affiliates 产品和服务随附的明示担保声明中说明了对此类产品和服务的全部担保。 本文所述的任何内容均不构成额外担保。Micro Focus 对本文中的技术或编辑错误或遗漏概不负责。

本文所含信息如有更改，恕不另行通知。

受限权利说明

机密计算机软件。 占有、使用或复制本文档需要 Micro Focus 提供有效许可证。根据 FAR 12.211 和 12.212 的规定，商业计算机软件、计算机软件文档和商业项目的技术数据依据供应商的标准商业许可授权给美国政府使用。

版权通知

商标通知

Adobe™ 是 Adobe Systems Incorporated 的商标。

Microsoft® 和 Windows® 是 Microsoft Corporation 在美国的注册商标。

UNIX® 是 The Open Group 的注册商标。

本产品包含版权归 © 1995-2002 Jean-loup Gailly and Mark Adler 所有的“zlib”通用压缩库界面。

文档更新

该文档的标题页面包含如下标识信息：

- 软件版本号，表示软件版本。
- 文档发行日期，会在文档每次更新时进行更改。
- 软件发行日期，表示该软件版本的发行日期。

要查看最近的软件更新，请转到 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=。

要验证是否在使用最新版本的文档，请转到 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

该站点要求注册 Passport 并登录。要注册 Passport ID，请转到 https://cf.passport.softwaregrp.com/hppcf/login.do。

如果您订阅了相应的产品支持服务，您还将收到该产品的更新或新版本。 请联系您的销售代表了解详细信息。

支持

请访问软件在线支持网站，网址为 https://softwaresupport.softwaregrp.com/。

该网站提供有关软件所提供的产品、服务和支持的联系信息和详细信息。

软件在线支持为客户提供自助解决的能力。 通过它，可以快捷高效地访问管理业务所必需的交互式技术支持工具。 作为一名重要的支持客户，您可通过使用支持网站获得以下益处：

- 搜索您所感兴趣的知识文档
- 提交并追踪支持案例和增强请求
- 下载软件修补程序
- 访问产品文档
- 管理支持合同
- 查找客户支持合同

- 查看关于可用服务的信息
- 与其他软件客户一起探讨
- 研究软件培训并注册

大多数支持区域要求注册为 Passport 用户并登录。许多地方还要求阅读支持合同。

要注册 Passport ID，请转到 https://cf.passport.softwaregrp.com/hppcf/login.do。

有关访问级别的详细信息，请转到 https://softwaresupport.softwaregrp.com/。

内容

第 1 章： 简介

Data Protector 灾难恢复概览

本章综述灾难恢复过程、解释灾难恢复指南中用到的基本术语并概括介绍灾难恢复方法。

计算机灾难指的是任何使计算机系统无法引导的事件，无论是因为人为错误、硬件故障还是自然灾害。 在这些情况中，计算机的引导分区或系统分区很有可能不可用，并且需要先恢复环境，然后才能开始正常的还原操作。 灾难恢复包括对引导分区进行重新分区和/或重新格式化，并用定义环境的所有配置信息恢复操作系统。 *必须*完成此步骤，才能恢复其他用户数据。

有关灾难恢复的详细信息，请参见《*Data Protector 灾难恢复指南*》。

原始系统是指在系统发生计算机灾难之前由 Data Protector 备份的系统配置。

目标系统是指计算机灾难发生后的系统。 目标系统通常处于不可引导状态，Data Protector 灾难恢复的目标是将该系统还原为原始系统配置。 受影响系统与目标系统的区别在于目标系统已更换了所有故障硬件。

引导磁盘/分区/卷是指包含引导过程的初始步骤所需的文件的磁盘/分区/卷，而**系统磁盘/分区/卷**是指包含操作系统文件的磁盘/分区/卷。

> **注意：**
> Microsoft 将引导分区定义为包含操作系统文件的分区，而将系统分区定义为包含引导过程的初始步骤所需的文件的分区。

托管系统是用于磁盘传递灾难恢复的工作 Data Protector 客户机，其中安装了磁盘代理。

辅助磁盘是可引导磁盘，具有带网络连接且装有 Data Protector 磁盘代理的最小操作系统。 它可以随身携带，用于在 UNIX 客户机磁盘传递灾难恢复的第一阶段引导目标系统。

灾难恢复操作系统 (DR OS) 是用于运行灾难恢复过程的操作系统环境。 它为 Data Protector 提供了一个基本的运行时环境(磁盘、网络、磁带和文件系统访问)。 必须首先安装并配置此操作系统，Data Protector 灾难恢复才能得以执行。

DR OS 可以是临时或活动的。 **临时 DR OS** 专门用作还原其他某些操作系统与目标操作系统配置数据的主机环境。 在目标系统还原为原始系统配置之后，它会被删除。 **活动 DR OS** 不仅托管 Data Protector 灾难恢复过程，还可以作为所还原系统的一部分，因为它可将自身的配置数据替换为原始配置数据。

关键卷是引导系统和 Data Protector 卷所需的卷。 不考虑操作系统，这些卷包括：

- 引导卷
- 系统卷
- 包含 Data Protector 可执行文件的卷
- IDB 所在的卷(对于 Cell Manager)

> **注意：**
> 如果 IDB 位于多个卷上，则 IDB 所在的所有卷都会被视为关键卷。

除了上述的关键卷以外，CONFIGURATION 也是 Windows 和 Linux 系统的关键卷集的一部分。 在 Windows 系统中，服务备份为 CONFIGURATION 备份的一部分。

在 Windows 系统中，CONFIGURATION 对象中包括的某些项可位于系统、引导、Data Protector 或 IDB 卷以外的卷上。 在这种情况下，这些卷也是关键卷集的一部分：

- 用户配置文件卷
- Windows Server 系统上的证书服务器数据库卷
- Windows Server 的域控制器上的 Active Directory 服务卷
- Microsoft 群集服务器上的仲裁卷

在 Linux 系统上，CONFIGURATION 对象仅包含与自动灾难恢复方法相关的数据，例如卷、装载点、网络设置等类似项目。

可访问 Cell Manager 时执行**联机恢复**。 在这种情况下，大多数 Data Protector 功能都可用 (Cell Manager 可运行会话，还原会话会记录到 IDB 中，您可以使用 GUI 监控还原进度等等)。

在 Cell Manager 不可访问时，执行**脱机恢复**(例如，由于网络故障，Cell Manager 遭受灾难，联机恢复失败等等)。 只有独立设备、SCSI 库、文件库和备份到磁盘 (B2D) 设备可用于脱机恢复。 只能对 Cell Manager 执行脱机恢复。

如果在 SRD 文件中指定的所有介质代理系统均可访问，则会执行**远程恢复**。 如果其中任意系统发生故障，则灾难恢复过程会故障切换到本地模式。 这意味着会在目标系统上搜索本地连接的设备。 如果只找到一个设备，则会自动使用该设备。 否则，Data Protector 会提示您选择设备，该设备将用于进行还原。 注意，脱机 OBDR 始终在本地执行。

灾难是一种严重情况，但以下因素可能使情况更加恶化：

- 系统必须尽快、尽可能高效地恢复联机状态。
- 灾难恢复不是常见事件，并且管理员可能不熟悉所需的步骤。
- 执行恢复的现有人员可能只具有系统方面的基础知识。

灾难恢复不是经过定义、简单易用的解决方案。 而是一个复杂的过程，涉及到执行的大量计划和准备工作。 必须完整地定义一个分步过程，才能为从灾难情况中迅速恢复做好准备。

灾难恢复阶段过程

无论采用什么恢复方法，灾难恢复的过程都可分为四个连续的阶段：

1. 阶段 0
2. 阶段 1
3. 阶段 2
4. 阶段 3

1. **阶段 0**(准备)是成功实施灾难恢复的先决条件。 必须在灾难发生前完成规划和准备。
2. 在**阶段 1** 中，安装并配置 DR OS，此过程通常包括对引导分区进行重新分区和重新格式化，这是因为系统的引导或系统分区并非一直可用而环境需要在常规还原操作再次继续之前得到恢复。
3. 在阶段 2 中，使用 Data Protector 定义环境所用的所有配置信息还原操作系统(还原成原样)。
4. 只有在完成在此步骤后，才能还原应用程序和用户的数据(**阶段 3**)。

需要按照经完善定义的分步过程执行以确保快速且高效的还原。

灾难恢复方法

本节综述灾难恢复方法。有关不同操作系统上支持的灾难恢复方法的列表，请参见最新的支持矩阵，网址为：https://softwaresupport.softwaregrp.com/。

> **注意：**
> 每种灾难恢复方法都有一些限制，在实现之前应考虑这些限制。

灾难恢复方法概述 (第 13 页)概述了 Data Protector 灾难恢复方法。

灾难恢复方法概述

阶段 0	阶段 1	阶段 2	阶段 3
手动灾难恢复			
整个系统的文件系统完整备份，内部数据库备份(仅限 Cell Manager)。更新 SRD 文件(仅限 Windows 系统)在原始系统上收集信息以启用 DR OS 的安装和配置。	通过网络支持安装 DR OS。 对磁盘进行重新分区，然后重新建立原始存储结构。	执行 `drstart` 命令以自动恢复关键卷。要执行高级恢复任务，还需要执行其他步骤。	使用标准 Data Protector 还原过程还原用户和应用程序数据。
请参见辅助手动灾难恢复 (AMDR) (第 21 页)或手动灾难恢复 (MDR) (第 78 页)。			
磁盘传递灾难恢复 (DDDR)(仅限 UNIX 系统)			
整个系统的文件系统完整备份和内部数据库备份(仅限 Cell Manager)生成辅助磁盘。	将辅助磁盘连接到目标系统。 对更换磁盘进行重新分区，然后重新建立原始存储结构。	将原始系统的引导磁盘还原到更换磁盘，删除辅助引导磁盘。 重新启动系统。 要执行高级恢复任务，还需要执行其他步骤。	使用标准 Data Protector 还原过程还原用户和应用程序数据。
请参见磁盘传递灾难恢复 (DDDR) (第 85 页)。			
增强型自动灾难恢复 (EADR)			
整个系统的文件系统完整备份，内部数据库备份(仅限 Cell Manager)。准备和更新 SRD 文件。准备 DR OS 映像。	从灾难恢复 CD、USB 闪存驱动器或网络引导系统并选择恢复范围。	自动还原关键卷。要执行高级恢复任务，还需要执行其他步骤。	使用标准 Data Protector 还原过程还原用户和应用程序数据。

请参见增强型自动灾难恢复 (EADR) (第 33 页)或增强型自动灾难恢复 (EADR) (第 90 页)。			
一键式灾难恢复 (OBDR)			
使用 OBDR 向导完整备份整个系统的文件系统。准备和更新 SRD 文件。	从 OBDR 磁带引导目标系统并选择恢复范围。	自动还原关键卷。	使用标准 Data Protector 还原过程还原用户和应用程序数据。
请参见一键式灾难恢复 (OBDR) (第 49 页)或一键式灾难恢复 (OBDR) (第 99 页)。			

必须先完成以下阶段，然后才能进入下一个阶段：

- *阶段 0*：

  必须执行客户机完整备份和 IDB 备份(仅在 Cell Manager 上)，并且管理员必须从原始系统收集足够的信息以启用 DR OS 的安装和配置。应该为 UNIX 系统的磁盘传递灾难恢复创建辅助引导磁盘。
- *阶段 1*：

  必须安装和配置 DR OS 并重新建立原始存储结构(所有卷已做好还原准备)。在 UNIX 上用于磁盘传递灾难恢复的更换磁盘必须可引导。
- *阶段 2*：

  还原关键卷。要执行高级恢复任务，还需要执行其他步骤。请参见“高级恢复任务”一节。
- *阶段 3*：

  检查应用程序数据是否正确还原(例如，数据库是否一致)。

手动灾难恢复方法

这是基本灾难恢复方法，该方法涉及将目标系统恢复为原始系统配置。

首先，必须安装和配置 DR OS。然后使用 Data Protector 还原数据(包括操作系统文件)，用还原后的操作系统文件替换操作系统文件。

对于手动恢复，重要的是要收集有关存储结构的信息(如分区信息、磁盘镜像和条带)，这些信息不保留在平面文件中。

磁盘传递灾难恢复

磁盘传递灾难恢复 (DDDR) 方法在 UNIX 客户机上受支持。有关受支持操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

此方法无需其他客户机，而需要装有最小化的操作系统、网络组件和 Data Protector 磁盘代理的可引导辅助磁盘(可以随身携带)。需要在灾难之前收集足够的信息才能正确地对磁盘进行格式化和分区。

此方法可以简单快速地恢复客户机。

> **提示：**
> 此方法对热交换硬盘驱动器尤其有用，因为可以在电源仍接通且系统正在运行的同

时断开硬盘驱动器与系统的连接，然后连接新驱动器。

请参见磁盘传递灾难恢复 (DDDR) (第 85 页)。

增强型自动灾难恢复 (EADR)

Data Protector 提供了针对 Windows 和 Linux Data Protector 客户机以及 Cell Manager 的增强型灾难恢复过程(只需极少的用户干预)。

备份时，EADR 过程将自动收集所有相关的环境数据。在配置备份期间，对于单元中的每个已备份客户机，临时安装和配置 DR OS 所需的数据打包到单个大型 **DR 映像(恢复集)**文件中，该文件存储在备份磁带(以及 Cell Manager(可选))上。

除了此映像文件外，Cell Manager 还将存储阶段 1 启动信息(存储在 P1S 文件中)，该启动信息是对磁盘进行正确的格式化和分区所必需的。如果发生灾难，可以使用 EADR 向导从备份介质还原 DR OS 映像(如果在完整备份期间尚未在 Cell Manager 上保存该映像)。可以将其转换为**灾难恢复 CD ISO 映像**、将其保存在可引导 USB 驱动器上，或创建可引导网络映像。然后可以使用任何 CD 刻录工具将 CD ISO 映像刻录到 CD。

在从 CD 、USB 驱动器或网络启动目标系统时，Data Protector 将自动安装和配置 DR OS、对磁盘进行格式化和分区，最后用 Data Protector 将原始系统恢复到备份时的状态。

恢复的卷包括：

- 引导卷
- 系统卷
- 包含 Data Protector 安装和配置的卷

使用标准 Data Protector 还原过程可恢复任何剩余的卷。

一键式灾难恢复 (OBDR)

一键式灾难恢复 (OBDR) 是针对 Windows 和 Linux Data Protector 客户机的自动 Data Protector 灾难恢复方法，只需极少的用户干预。 它以使用 OBDR 设备和将映像文件复制到磁带上的概念为基础。 有关受支持操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

OBDR 备份期间，临时 DR OS 安装和配置所需的数据打包在一个大型 OBDR 映像文件中，并存储在备份磁带上。 灾难发生时，OBDR 设备用于直接从含有灾难恢复信息的 OBDR 映像文件所在的磁带引导目标系统。 然后，Data Protector 安装和配置 DR OS，对磁盘进行格式化和分区，最后用 Data Protector 将原始操作系统还原到备份时的状态。

自动恢复的卷包括：

- 引导卷
- 系统卷
- 包含 Data Protector 安装和配置的卷

使用标准 Data Protector 还原过程可恢复剩余的卷。

重要：
每次更改硬件、软件或配置之后都需要在客户机上本地准备好一个新的 OBDR 引导

磁带。 这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

Micro Focus 建议限制对备份介质、DR 映像、SRD 文件和灾难恢复 CD 以及存储 DR OS 数据的 USB 驱动器的访问

Data Protector 集成和灾难恢复

灾难恢复是一个极其复杂的过程，涉及到来自多家供应商的产品。 因此，能否成功实施灾难恢复取决于涉及的所有供应商。 此处提供的信息仅供参考。

请查看数据库/应用程序供应商关于如何为灾难恢复做准备的说明。

以下是有关如何恢复应用程序的常规过程：

1. 执行灾难恢复。
2. 安装、配置和初始化数据库/应用程序，以便可将 Data Protector 介质上的数据加载回系统。 请查看数据库/应用程序供应商文档，了解准备数据库所需的详细过程和步骤。
3. 确保数据库/应用程序服务器已安装所需的 Data Protector 客户机软件，并且已针对数据库/应用程序进行配置。 按照相应的《*Data Protector 集成指南*》中的步骤进行操作。
4. 启动还原。 完成恢复后，按照数据库/应用程序供应商提供的说明执行使数据库重新联机所需的任何额外步骤。

第 2 章： 如何为灾难恢复做准备

请仔细按照下方的说明为灾难恢复做准备，以确保快速高效地进行还原。 准备过程与灾难恢复方法无关，其中包括开发详细的灾难恢复计划、执行一致和相关的备份以及更新 Windows 中的 SRD 文件。

本章节包含灾难恢复中适用于所有灾难恢复方法的常规准备过程。 对每个特定的灾难恢复方法都需要进行额外的准备。 有关其他准备步骤，请参见对应主题。

请记住，使 Cell Manager 做好灾难恢复的准备至关重要，这一点需要多加注意。

> **重要：**
> 请在灾难发生之前准备灾难恢复。

规划

制定一个详细的灾难恢复计划对灾难恢复的成功有着重要影响。 要在具有多个不同的系统的大型环境中部署灾难恢复，请执行以下操作：

1. **计划**

   计划必须由 IT 管理部门进行准备，并且应包括以下步骤：

   - 将应首先恢复的最重要系统列一个清单。 关键系统是网络正常运行所需的系统(DNS 服务器、域控制器、网关等等)、Cell Manager 和介质代理客户机。 应在所有其他系统之前恢复这些系统。
   - 选择适用于系统的灾难恢复方法。 根据这些方法，考虑每个系统需要哪些准备步骤。
   - 确定一种在恢复时获取必要信息(如存储 IDB 的介质、更新后 SRD 文件所在的位置以及 Cell Manager 备份介质的位置和标签)的方法。 定义软件库的位置以便执行新的安装。
   - 创建详细的分步核对清单，指导您完成整个过程。
   - 创建并执行测试计划，以确认恢复将真正起作用。

2. **恢复准备**

   在运行备份之前执行以下准备步骤，以保证备份期间的环境一致性：

   所有系统：

   - 执行定期和一致的备份。
   - 需要了解卷组和分区的概念。 在 UNIX 系统中，应了解有关存储环境结构的信息所在的位置。

   UNIX 系统：

   - 创建 pre-exec 脚本，用来收集存储结构和执行其他特定的客户机准备。
   - 创建工具，如具有最小操作系统、网络资源和已安装 Data Protector 磁盘代理的辅助磁

盘。

Windows 系统：

- 确保具有有效的 CONFIGURATION 备份供您处理。
- 更新 SRD 文件，并将其存储在安全位置。 出于安全考虑，应限制对 SRD 文件的访问。

3. **执行恢复过程**

   按照已测试过的过程和清单恢复受影响系统。

> **警告：**
> 不要更改为灾难恢复准备的系统上的默认 Inet 侦听端口。 反之，如果此类系统受到灾难打击，灾难恢复进程可能会失败。

一致和相关的备份

如果发生灾难，目标系统应恢复原始系统配置。 此外，系统的操作和运行应该如同执行上一次有效备份之前那样。

> **注意：**
> 在 UNIX 系统中，系统引导完毕后，某些后台程序或进程就会因为各种原因而处于活动状态(运行级别 2)。 此类进程甚至可能会将数据读入内存，并在其运行时将“dirty flag”写入某些文件。 在标准操作阶段(标准运行级别 4)执行的备份对此类应用程序产生的重新启动不太可能没有错误。 为了按照示例操作，如果在这样的伪恢复之后启动许可证服务器，它将发现从文件读取的数据不一致，并且将拒绝像预期那样运行服务。
>
> 在 Windows 系统中，当系统正常运行时无法替换许多系统文件，因为系统将其锁定。 例如，无法还原当前正在使用的用户配置文件。 必须更改登录帐户，或者必须停止相关服务。

根据备份运行时系统中活动的内容，可能会违反应用程序的数据一致性，从而导致恢复后重新启动和执行出现问题。

创建一致和相关的备份

- 理想情况下，要在相关分区设置为脱机时执行备份，但通常无法满足这种条件。
- 备份期间检查系统中的活动。 仅与操作系统相关的进程和联机备份的数据库服务可以在备份执行期间保持活动状态。
- 确保将系统活动降到最低限度。 例如，仅核心操作系统、基本网络和备份应处于活动状态。 不应运行任何底层应用程序服务。 使用适当的 pre-exec 脚本可实现这一点。

灾难恢复使用 btrfs 子卷和通过文件系统 root 备份的卷中的数据(跨文件系统边界)，以创建灾难恢复 ISO 映像并执行恢复和还原。 这表示所有系统、配置文件和相关用户数据必须包括在 / (root) 文件系统对象的备份中。 所有单独备份的数据(使用 OB2_SHOW_BTRFS_MOUNTS 的数据)只能用于常规磁盘代理文件系统还原操作，不可用于恢复过程。 这仅适用于 Linux 操作系统。

> **注意：**
> Data Protector 包括手动创建的 btrfs 快照中的数据。

一致和相关的备份中应包括的内容取决于您计划使用的灾难恢复方法和系统特有的情况(例如 Microsoft 群集服务器的灾难恢复)。 请参见有关准备特定灾难恢复方法的主题。

加密备份

如果备份经过加密，则必须确保安全地存储加密密钥，并在启动灾难恢复时这些密钥可用。 如果无法访问适当的加密密钥，灾难恢复过程就会中止。 各种灾难恢复方法都有额外的要求。

加密密钥集中存储在 Cell Manager 上；因此灾难恢复客户机必须连接到 Cell Manager 才能获得加密密钥。 有关加密概念的详细信息，请参见 Data Protector 帮助索引：“加密”。

可能会有以下两种灾难恢复的场景：

- 恢复从中可与 Cell Manager 建立连接的客户机。 对于此类场景不需要进行与加密相关的其他准备，因为 Data Protector 会自动获取加密密钥。
- Cell Manager 的灾难恢复或独立客户机恢复，其中无法与 Cell Manager 建立连接。

  提示输入时，必须提供可移动介质(例如磁盘)上的加密密钥。

  这些密钥不是灾难恢复 OS 映像的一部分，而是导出到密钥文件 (DR-*ClientName*-*keys*.csv)。 必须将密钥手动存储到单独的可移动介质，如磁盘或 USB 闪存驱动器。 确保始终具有每个备份的密钥的相应副本，以便为灾难恢复做好准备。 如果加密密钥不可用，则无法执行灾难恢复。

更新和编辑系统恢复数据

系统恢复数据 (SRD) 是一个使用 Unicode (UTF-16) 格式的文本文件，其中包含配置目标系统所需的信息。 在 Windows 客户机上执行 CONFIGURATION 备份时将生成 SRD 文件，随后该文件将被存储在 Cell Manager 上的以下目录中：

Windows 系统： *Data_Protector_program_data*\Config\Server\DR\SRD

UNIX 系统： /etc/opt/omni/server/dr/srd。

> **重要：**
> 如果 IDB 不可用，则有关对象和介质的信息将仅存储在 SRD 文件中。

Cell Manager 上的 SRD 文件名与生成该文件的计算机的主机名相同，例如 computer.company.com)。

CONFIGURATION 备份之后，SRD 文件仅包含安装 DR OS 所需的系统信息。 要执行灾难恢复，必须向 SRD 添加有关备份对象和相应介质的其他信息。 只能在 Windows 或 Linux 客户机上更新 SRD。 经过更新的 SRD 文件的名称为 recovery.srd。

可以使用以下三种不同的方法更新 SRD 文件：

- 更新 SRD 文件向导(仅在 Windows 系统中提供)
- omnisrdupdate 作为独立设备实用程序的命令
- omnisrdupdate 作为备份会话 post-exec 脚本的命令

> **重要：**
> 当您为 Cell Manager 更新 SRD 文件时，请指定一个比文件系统备份会话更新的 IDB 备份会话，以便可以在恢复后浏览文件系统备份会话和数据。

有关如何更新 SRD 文件的详细过程，请参见更新 SRD 文件(Windows 客户机)(第 26 页)。

第 3 章： Windows 系统中的灾难恢复

辅助手动灾难恢复 (AMDR)

在恢复时，Windows 需要安装灾难恢复操作系统 (DR OS)。恢复原始操作系统的过程通过 omnidr 命令自动执行。

决定进行灾难恢复之前，Windows 系统将进一步尝试恢复系统。通过以“安全”模式或从恢复软磁盘引导系统并尝试解决问题，可以实现这一点。

概述

确保已执行准备一章中提及的所有常规准备步骤。Windows 系统的常规辅助手动灾难恢复过程如下：

1. **阶段 1**
   a. 更换故障硬件。
   b. 重新安装操作系统(创建并格式化必需的卷)。
   c. 重新安装 Service Pack。
   d. 手动对磁盘进行重新分区，然后使用原始驱动器号分配重新建立存储结构。

   > **提示：**
   > 您可以将手动灾难恢复的阶段 1 与自动部署工具结合使用。

2. **阶段 2**
   a. 执行将安装 DR OS 并将启动关键卷还原的 Data Protector drstart 命令。
   b. drstart 命令完成后，必须重新启动系统。
   c. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤。有关详细信息，请参见“高级任务”(第 72 页)。
3. **阶段 3**
   a. 使用 Data Protector 标准还原过程还原用户和应用程序数据。

要求

- 这些分区的大小必须等于或大于故障磁盘上分区的大小。这样存储在崩溃磁盘上的信息可还原到一个新磁盘。此外，新卷的文件系统类型(FAT、NTFS)和压缩属性必须匹配。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置(扇区重新映射)。
- 所有硬件都必须相同。
- 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复：
  `omnicc -secure_comm -configure_for_dr <hostname_of_client being_recovered>`
- 联机恢复客户机之后，在 Cell Manager 上运行以下命令：
  `omnicc -secure_comm -configure_peer <client_host_name> -overwrite`

步骤

1. 为辅助手动灾难恢复做的准备(Windows 系统)(第 22 页).
2. 手动安装和配置 Windows 系统 (第 28 页).
3. 手动还原系统数据(Windows 系统)(第 31 页).
4. 还原供应商特有的分区(Windows 系统)(第 32 页).
5. 还原用户数据。

为辅助手动灾难恢复做的准备(Windows 系统)

要做好准备而使灾难恢复成功，请遵照与灾难恢复常规准备过程相关的说明，然后再执行本主题中列出的步骤。 提前准备，以便快速高效地执行灾难恢复。 应特别注意 Cell Manager 的灾难恢复准备。

> **重要：**
> 请在灾难发生之前准备灾难恢复。

常规准备

完成本节中列出的步骤前，还请参见规划 (第 17 页)以了解适用于所有灾难恢复方法的常规准备过程。 要快速高效地从灾难中恢复，请考虑以下步骤并相应地准备环境：

1. 需要 Windows 可引导安装 CD-ROM 以使系统可以从 CD-ROM 启动。 如果没有可引导 CD-ROM 驱动器，则还可以使用 Windows 磁盘。
2. 请确保具有适用于要恢复的系统的驱动程序。 可能需要在 Windows 安装过程中安装某些驱动程序，如 HBA 和 SCSI 驱动程序。
3. 要恢复受影响的系统，在灾难之前需要有关系统的以下信息：
   - 如果在灾难之前未使用 DHCP，则需要 TCP/IP 属性(IP 地址、默认网关、子网掩码、DNS 顺序 (IPv4)、子网前缀长度以及首选和备用 DNS 服务器 (IPv6))
   - 客户机属性(主机名、域)
4. 确保以下情况属实：
   - 您应当具备有效的客户机完整备份映像(包括有效的 CONFIGURATION 备份数据)。请参见《Data Protector 帮助》的索引：“备份, Windows 特定”和“备份, 配置”。
   - 应具有要用于恢复的 SRD 文件，并用有关备份会话中对象的信息更新该文件。
   - 为了恢复 Cell Manager，您应当具备有效的“内部数据库”备份映像，它是在客户机备份映像之后创建的。 有关如何配置和执行 IDB 备份的详细信息，请参见《Data Protector 帮助》的索引：“IDB, 配置”。
   - 在使用 Microsoft 群集服务器的情况下，一致的备份还包括(在相同的备份会话中)

- 所有节点
- 管理虚拟服务器(由管理员定义)
- 如果将 Data Protector 配置为群集感知应用程序，则还包括 Cell Manager 虚拟服务器和 IDB。

有关详细信息，请参见关于 Microsoft 群集服务器的灾难恢复 (第 61 页)。

- 具有引导分区的磁盘需要一定的可用磁盘空间以安装 Data Protector 灾难恢复 (15 MB) 和 DR OS。 此外，还需要还原原始系统所需的空闲磁盘空间。

5. 将 drsetup 映像(“drsetup 软盘”)复制到 U 盘驱动器或软盘上。 软盘数目取决于平台以及 Windows 操作系统的版本。 这些映像位于：
   - 32 位 Windows 系统：

     Windows Vista 和更高版本： *Data_Protector_program_data*\Depot\DRSetupX86

     Windows XP、Windows Server 2003： *Data_Protector_home*\Depot\DRSetupX86

     Data Protector 安装介质： \i386\tools\DRSetupX86

   - AMD64/Intel EM64T 平台上的 64 位 Windows 系统：

     Windows Vista 和更高版本： *Data_Protector_program_data*\Depot\DRSetupX64

     Windows XP、Windows Server 2003： *Data_Protector_home*\Depot\DRSetupX64

     Data Protector 安装介质： \i386\tools\DRSetupX64

   - Itanium 平台上的 64 位 Windows 系统：

     Windows Vista 和更高版本： *Data_Protector_program_data*\Depot\DRSetupIA64

     Windows XP、Windows Server 2003： *Data_Protector_home*\Depot\DRSetupIA64

     Data Protector 安装介质： \i386\tools\DRSetupIA64

   发生灾难时，将受影响系统的已更新 SRD 文件保存到第一张软磁盘(磁盘 1)上。 每个站点的所有 Windows 系统仅需要一组软磁盘，但始终必须将受影响客户机的已更新 SRD 文件复制到第一张软磁盘上。 如果找到多个 SRD 文件，Data Protector 将要求您选择适当的版本。
6. 要按照灾难之前的样子重新创建各个磁盘分区，请记录每个分区的以下信息(恢复过程中将需要这些信息)：
   - 分区的长度和顺序
   - 分配给分区的驱动器号
   - 分区的文件系统类型

   此信息存储在 SRD 文件中。 SRD 文件的 diskinfo 部分中的 -type 选项显示特定卷的卷文件系统类型：

   如何从 SRD 文件中确定文件系统类型

类型编号	文件系统
1	Fat12

类型编号	文件系统
4 和 6	Fat32
5 和 15	扩展分区
7	NTFS
11 和 12	Fat32
18	EISA
66	LDM 分区

下一页上的表是灾难恢复准备工作的示例。请注意表中的数据属于特定系统且无法用于任何其他系统。有关可在准备辅助手动灾难恢复时使用的空模板，请参见Windows 灾难恢复准备表的示例 (第 123 页)。

使用 CLI 更新恢复磁盘

Data Protector 不提供用于自动创建恢复映像(软盘)的命令。但是，您可以通过执行 omnisrdupdate 命令手动更新恢复集中第一个软盘的内容。将恢复集中的第一个软盘插入软盘驱动器并将位置指定为 a:\，例如：

Data Protector 客户机系统：

```
omnisrdupdate -session 10/04/2011-1 -host clientsys.company.com -location a:\ -asr
```

Data Protector Cell Manager：

```
omnisrdupdate -session 10/04/2011-1 10/04/2011-2 -host cmsys.company.com -location
a:\ -asr
```

要手动创建恢复软盘，您还需要将 DRDiskNumber.cab 文件从 Data_Protector_program_data\Depot\DRSetup\DiskDiskNumber 文件夹复制到相应的恢复软盘。

Cell Manager 的额外准备

成功对 Cell Manager 进行灾难恢复还需要额外的准备：

- 对 Cell Manager 执行灾难恢复之前，在用于灾难恢复的介质主机上运行以下命令：

  ```
  omnicc -secure_comm -configure_for_dr <cell_manager_hostname>
  ```
- 恢复完成之后，在介质主机上运行以下命令：

  ```
  omnicc -secure_comm -configure_peer <cell_manager_hostname>
  ```
- 定期备份 IDB。

限制

- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。

Windows 灾难恢复准备表的示例

客户机属性	计算机名称	ANAPURNA
	主机名	anapurna.company.com
驱动程序		tatpi.sys、aic78xx.sys
Windows Service Pack		Windows Vista
IPv4 的 TCP/IP 属性	IP 地址	10.17.2.61
	默认网关	10.17.250.250
	子网掩码	255.255.0.0
	DNS 顺序	10.17.3.108、10.17.100.100
IPv6 的 TCP/IP 属性	IP 地址	td10:1234:5678:abba::6:1600
	子网前缀长度	64
	默认网关	td10:1234:5678:abba::6:1603
	首选 DNS 服务器	td10:1234:5678:abba::6:1603
	备用 DNS 服务器	td10:1234:5678:abba::6:1604
介质标签/条码数字		“anapurna - 灾难恢复”/ [000577]
分区信息和顺序	第一个磁盘标签	
	第一个分区长度	31 MB
	第一个驱动器号	
	第一个文件系统	EISA
	第二个磁盘标签	BOOT
	第二个分区长度	1419 MB
	第二个驱动器号	C:
	第二个文件系统	NTFS/HPFS
	第三个磁盘标签	
	第三个分区长度	
	第三个驱动器号	
	第三个文件系统	

更新 SRD 文件(Windows 客户机)

CONFIGURATION 备份之后，SRD 文件仅包含安装 DR OS 所需的系统信息。 该文件位于 Cell Manager 上：

Windows 系统： *Data_Protector_program_data*\Config\Server\DR\SRD

UNIX 系统： /etc/opt/omni/server/dr/srd

要执行灾难恢复，必须向 SRD 添加有关备份对象和相应介质的其他信息。 只能在 Windows 客户机上更新 SRD。 Cell Manager 上的 SRD 文件名与生成该文件的计算机的主机名相同 - 例如 computer.company.com。 经过更新的 SRD 文件的名称为 recovery.srd。

SRD 文件中存储的有关备份设备或介质的信息可能在执行灾难恢复时过期。 在这种情况下，执行灾难恢复之前，要编辑 SRD 文件以将错误信息替换为相关信息。

> **重要：**
> 在安全位置(而非在 Cell Manager 上)存储 Cell Manager 的 SRD 文件。 建议限制对 SRD 文件的访问。

在 Windows 系统上使用 Data Protector 灾难恢复向导更新 SRD 文件

步骤

1. 在 Data Protector 上下文列表中，单击**还原**。
2. 在范围窗格中，单击**任务**，然后单击**灾难恢复**以打开灾难恢复向导。
3. 在“主机”下拉列表中，选择要为其更新 SRD 文件的系统。
4. 在“灾难恢复方法”列表中，选择 **SRD 文件更新**。 单击**下一步**。

   Data Protector 首先在 Cell Manager 中搜索 SRD 文件。 如果未找到，则 Data Protector 从上一个备份中还原该文件。
5. 选择还原逻辑卷和系统配置所需的对象和版本。 为每个对象单击**下一步**。
6. 指定 SRD 文件的目标。 单击**完成 (Finish)**。

使用 omnisrdupdate 命令更新 SRD 文件

可以将 omnisrdupdate 用作独立命令。

要更新 SRD 文件，请修改现有的备份规范，或用指定的 post-exec 脚本创建新的备份规范。

步骤

1. 在 Data Protector 上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。 此时将显示所保存的全部备份规范。

3. 单击要修改的备份规范。
4. 在“选项”属性页中的“备份规范选项”下，单击**高级**。
5. 在“备份选项”窗口的 post-exec 文本框中键入 omnisrdupdate。
6. 在“客户机上”下拉列表中，选择将从中执行此 post-exec 脚本的客户机，然后单击**确定**。
7. 单击**应用**保存更改，然后退出向导。

使用 post-exec 脚本更新 SRD 文件

另一种更新 SRD 的方法是将 omnisrdupdate 命令用作备份 post-exec 脚本。 为此，请修改现有的备份规范或创建新的备份规范。 执行以下步骤修改备份规范，以便在备份会话停止时，SRD 文件使用有关已备份对象的信息进行了更新：

1. 在备份上下文中，展开**备份规范**项，然后展开**文件系统**。
2. 选择要修改的备份规范(它必须包含所有在 SRD 文件中标记为关键的备份对象，否则更新将失败。 建议执行磁盘发现的客户机备份并在“结果区域”中单击**选项**。
3. 单击“备份规范选项”下的**高级**按钮。
4. 在 post-exec 文本框中键入 omnisrdupdate。
5. 在“客户机上”下拉列表中，选择将从中执行此 post-exec 脚本的客户机，然后单击**确定**确认。 它应该是源页上标记为要备份的客户机。

将 omnisrdupdate 命令作为 post-exec 实用程序执行时，会话 ID 将被自动获取，无需指定。

可以通过与独立实用程序相同的方式 (-location *Path*, -host *ClientName*) 指定其他所有选项。

> **重要：**
> 由于 IDB 是在单独的会话中备份的，因此无法在 post-exec 脚本中使用 omnisrdupdate 更新 Cell Manager 的 SRD。

编辑 SRD 文件的示例

如果 SRD 文件中的信息不再是最新的(例如更改了备份设备)，请修改更新的 SRD 文件 (recovery.srd)，然后再执行灾难恢复的阶段 2，以更新错误的信息并因此使恢复取得成功。

可以使用 devbra -dev 命令显示某些设备配置信息。

更改 MA 客户机

使用连接到客户机 old_mahost.company.com 的备份设备执行备份以用于灾难恢复。 灾难恢复时，相同的备份设备连接到具有相同 SCSI 地址的客户机 new_mahost.company.com。 要执行灾难恢复，请将经过更新的 SRD 文件中的 -mahost old_mahost.company.com 字符串替换为 -mahost new_mahost.company.com，然后再执行灾难恢复阶段 2。

如果备份设备在新 MA 客户机上的 SCSI 地址不同，则在经过更新的 SRD 文件中还要相应地修改 -devaddr 选项的值。

编辑文件之后，以 Unicode (UTF-16) 格式将其保存到原始位置。

更改备份设备

要使用备份设备之外的另一个设备执行灾难恢复，请在经过更新的 SRD 文件中修改以下选项值：

-dev、-devaddr、-devtype、-devpolicy、-devioctl 和 -physloc

其中：

-dev	指定要用于备份的备份设备或驱动器(库)的逻辑名称，
-devaddr	指定该设备的 SCSI 地址，
-devtype	指定 Data Protector 设备类型，
-devpolicy	指定设备策略，此策略可以定义为 1(独立设备)、3(堆栈器)、5(介质库)、6(外部控制)、8(Grau DAS 交换器库)、9(STK Silo 介质库)或 10 (SCSI-II 库)，
-devioctl	指定机械手 SCSI 地址。
-physloc	指定库插槽
-storname	指定逻辑库名称

例如，使用设备名称为 Ultrium_dagnja、连接到 MA 主机 dagnja(Windows 系统)的 Ultrium 独立设备执行了一次备份用于灾难恢复。 但是，对于灾难恢复，您喜欢使用逻辑库名称为 Autoldr_kerala、具有连接到 MA 客户机 kerala(Linux 系统)的驱动器 Ultrium_kerala 的 Ultrium 机械手库。

首先，在 kerala 上运行 devbra -dev 命令，以显示已配置设备及其配置信息的列表。 将需要此信息以替换经过更新的 SRD 文件中的以下选项值：

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13 -devpolicy 1 -mahost
dagnja.company.com
```

以及如下：

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13 -devpolicy 10 -devioctl
/dev/sg1 -physloc " 2 -1" -storname "AutoLdr_kerala" -mahost kerala.company.com.
```

编辑文件之后，以 Unicode (UTF-16) 格式将其保存到原始位置。

手动安装和配置 **Windows** 系统

灾难发生之后，应首先安装和配置操作系统。 安装操作系统之后，可以进行系统数据恢复。

步骤

阶段 1

1. 如果需要，请从 CD-ROM 安装 Windows 系统，然后安装其他驱动程序。 必须将 Windows 操作系统安装在灾难之前所安装的相同分区上。 请勿在安装系统期间安装 Internet Information Server (IIS)。

   重要：
   如果已使用无人看管安装程序安装了 Windows 操作系统，则现在请使用相同的脚本重新安装 Windows，以确保将 *%SystemRoot%* 和 *%SystemDrive%*\Documents and Settings 文件夹安装到相同位置。

2. 显示“Windows Partition Setup”屏幕时，请执行以下操作：
   - 如果灾难之前系统上存在 EISA 实用程序分区 (EUP)，则使用 SRD 文件中存储的 EUP 信息创建(如果因灾难而不存在)和格式化“虚拟”FAT 分区。 EUP 稍后将恢复到由“虚拟”分区占用的空间。 “虚拟”分区之后立即创建和格式化临时引导分区。
   - 如果灾难之前系统上不存在 EUP，则创建(如果因灾难而不存在引导分区)和格式化引导分区(如果灾难之前磁盘上存在该分区)。

     Windows 安装程序提示输入 Windows 安装目录时，在引导分区上指定一个与原始 Windows 安装所在目录相同的新目录。

     注意：
     安装期间，不要将系统添加到其以前所在的 Windows 域，而是要添加到工作组。 如果要还原主域控制器 (PDC)，则确保目标还原系统不位于受影响 PDC 曾控制的域中。

3. 安装 TCP/IP 协议。 如果灾难发生之前未使用 DHCP，请通过提供以下信息将 TCP/IP 协议配置为灾难前的状态：受影响客户机的主机名、其 IP 地址、默认网关、子网掩码和 DNS 服务器。 可以从 SRD 文件获取此信息。 确保标有**此计算机的主 DNS 后缀**的字段中包含您的域名。

   注意：
   默认情况下，在 Windows 安装期间 Windows 将安装动态主机配置协议 (DHCP)。

4. 在 Windows Administrators 组中创建新的临时灾难恢复帐户(例如 DRAdmin)，然后将其添加到 Cell Manager 上的 Data Protector Admin 组。 请参见《*Data Protector 帮助*》的索引：“添加 Data Protector 用户”。

   灾难之前系统中不得存在该用户帐户。 此过程中稍后将删除该临时 Windows 用户帐户。

5. 使用新创建的帐户注销和登录系统。
6. 创建和格式化所有未格式化的分区(如果使用“虚拟”EISA 实用程序分区，则包括该分区)，如同灾难之前磁盘上存在这些分区那样。 使用供应商特有的过程创建实用程序分区。 必须将“虚拟”EISA 实用程序分区格式化为 FAT 文件系统。 按灾难之前的方式向这些分区分配驱动器号。

阶段 2

1. 如果 SRD 文件中的信息并非最新(例如因为灾难之后更改了备份设备)，并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
2. 从 *Data_Protector_home*\Depot\drsetup\disk1 (Cell Manager) 或 \i386\tools\drsetup\disk1(Data Protector 安装介质)目录中运行 drstart。

   如果已准备 drsetup 软盘，则也可以从第一个软盘上运行 drstart。
3. drstart 首先扫描当前工作目录、软盘驱动器和 CD-ROM 驱动器，以确定灾难恢复设置文件(dr1.cab 和 omnicab.ini)的位置。 如果找到了所需的文件，则 drstart 实用程序将在 *%SystemRoot%*\system32\OB2DR 目录中安装灾难恢复文件。 如果未找到这些文件，则应浏览查找它们或在 DR Installation Source 文本框中输入其路径。
4. 如果发现 SRD 文件 (recovery.srd) 与 dr1.cab 和 omnicab.ini 在同一目录中，drstart 会将 recovery.srd 复制到 *%SystemRoot%*\system32\OB2DR\bin 目录，并且 omnidr 实用程序将自动启动。 否则，您可以在 SRD Path 文本框中输入 SRD 文件 (recovery.srd) 的位置或浏览查找该文件。 单击**下一步**。

   如果在软盘上找到了多个 SRD 文件，Data Protector 将要求您选择一个适当的 SRD 文件版本。

   omnidr 成功完成之后，正常引导系统需要的所有关键对象都会还原。
5. 从 Cell Manager 上的 Data Protector Admin 组中删除临时 Data Protector 用户帐户(在阶段 1 添加)，除非灾难恢复之前 Cell Manager 上就存在该帐户。
6. 重新启动系统，登录并验证还原的应用程序正在运行。

阶段 3

6. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤(如恢复 MSCS 或 IIS、编辑 kb.cfg 和 SRD 文件)。 有关详细信息，请参见还原 Data Protector Cell Manager 详情 (第 65 页)和“高级恢复任务”一节。
7. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

第一次登录之后将删除临时 DR OS，但以下情况除外：

- 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。
- 您手动执行带有 -no_reset 或 -debug 选项的 omnidr 命令。
- 灾难恢复失败。

还原 Data Protector Cell Manager 详情

执行 Windows 系统的常规手动灾难恢复过程之后，使用 Data Protector 执行额外步骤以还原 Cell Manager。

要使 IDB 恢复保持一致，请还原有关灾难恢复期间未还原的备份对象的信息。 为此，请通过导入含有用于灾难恢复的 Cell Manager 完整客户机备份的介质来更新 IDB。

手动还原系统数据(Windows 系统)

安装和配置操作系统(阶段 1)之后，可以使用 Data Protector 恢复 Data Protector 客户机或 Cell Manager。 Cell Manager 和 Internet Information Server (IIS) 的灾难恢复还要求执行其他步骤。

还原 Windows 系统

步骤

阶段 2

1. 如果 SRD 文件中的信息并非最新(例如因为灾难之后更改了备份设备)，并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
2. 从 *Data_Protector_home*\Depot\drsetup\disk1 (Cell Manager) 或 \i386\tools\drsetup\disk1(Data Protector 安装介质)目录中运行 drstart。

   如果已准备 drsetup 软盘，则也可以从第一个软盘上运行 drstart。
3. drstart 首先扫描当前工作目录、软盘驱动器和 CD-ROM 驱动器，以确定灾难恢复设置文件(dr1.cab 和 omnicab.ini)的位置。 如果找到了所需的文件，则 drstart 实用程序将在 *%SystemRoot%*\system32\OB2DR 目录中安装灾难恢复文件。 如果未找到这些文件，则应浏览查找它们或在 DR Installation Source 文本框中输入其路径。
4. 如果发现 SRD 文件 (recovery.srd) 与 dr1.cab 和 omnicab.ini 在同一目录中，drstart 会将 recovery.srd 复制到 *%SystemRoot%*\system32\OB2DR\bin 目录，并且 omnidr 实用程序将自动启动。 否则，您可以在 SRD Path 文本框中输入 SRD 文件 (recovery.srd) 的位置或浏览查找该文件。 单击**下一步**。

   如果在软盘上找到了多个 SRD 文件，Data Protector 将要求您选择一个适当的 SRD 文件版本。

   omnidr 成功完成之后，正常引导系统需要的所有关键对象都会还原。
5. 从 Cell Manager 上的 Data Protector Admin 组中删除临时 Data Protector 用户帐户(在阶段 1 添加)，除非灾难恢复之前 Cell Manager 上就存在该帐户。
6. 重新启动系统，登录并验证还原的应用程序正在运行。

阶段 3

6. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤(如恢复 MSCS 或 IIS、编辑 kb.cfg 和 SRD 文件)。 有关详细信息，请参见还原 Data Protector Cell Manager 详情 (第 65 页)和“高级恢复任务”一节。
7. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

第一次登录之后将删除临时 DR OS，但以下情况除外：

- 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。
- 您手动执行带有 -no_reset 或 -debug 选项的 omnidr 命令。
- 灾难恢复失败。

还原 Data Protector Cell Manager 详情

执行 Windows 系统的常规手动灾难恢复过程之后，使用 Data Protector 执行额外步骤以还原 Cell Manager。

要使 IDB 恢复保持一致，请还原有关灾难恢复期间未还原的备份对象的信息。 为此，请通过导入含有用于灾难恢复的 Cell Manager 完整客户机备份的介质来更新 IDB。

还原供应商特有的分区(Windows 系统)

如果需要，可以用恢复供应商特有的分区 (VSP) 结束常规手动灾难恢复过程。

免责声明

恢复 VSP 可能是一个复杂过程，需要 Windows 操作系统的高级技术和知识。 此处提供的信息仅为方便您使用。 使用这些信息应由*您自担风险*。 如果恢复 VSP 之后更改了分区顺序，则将需要修改 `boot.ini` 文件。 `boot.ini` 文件有误将导致系统不可引导。

为灾难恢复所做的准备

此信息仅适用于辅助手动灾难恢复 (AMDR)，因为增强型自动灾难恢复 (EADR) 和一键式灾难恢复 (OBDR) 将自动恢复 VSP，因此建议使用后两种方法恢复 VSP。

执行 AMDR 时，必须手动重新创建以前的存储结构(包括 VSP)。

ASR 将自动重新创建以前的存储结构，并在用于 VSP 的磁盘上保留未分配的空间。 然后必须使用供应商特有的工具和过程在未分配的磁盘空间上重新创建 VSP。

要允许通过 Data Protector 访问 VSP，必须使用 Data Protector `omnipm` 实用程序在 Windows 中映射 VSP。

步骤

1. 运行 *`Data_Protector_home`*`\bin\utilns\omnipm`启动 Data Protector Partition Mapper。
2. 在 Partition Mapper 窗口中的“类型”列下，选择以供应商特有 ID 标识的分区。
3. 单击**映射**，将驱动器盘符分配给所选分区。 在对话框窗口中，指定驱动器盘符，然后单击**确定**。
4. 使用标准 Data Protector 恢复过程，将备份数据恢复到所映射的 EISA 实用程序分区上。
5. 对步骤 3 中映射的分区取消映射。

警告：
恢复期间请勿覆盖 VSP 根中的操作系统文件(通常为 `*.sys` 文件)，因为这会导致系统不可引导。 因此建议将这些文件添加到排除列表中。

还原 Eisa 实用程序分区

步骤

1. 如果未保留 Eisa 实用程序分区 (EUP)，则必须手动创建该分区。 注意，EUP 应位于系统 BIOS 所识别的第一个磁盘上。 由于 Disk Manager 无法创建 EUP，因此创建一个普通的 FAT16 分区，并向其分配一个驱动器号。
2. 使用 Data Protector 还原其内容。 对于 Eisa 实用程序分区配置对象，选择**恢复为**选项。 所分配的驱动器号必须是创建 EUP 期间分配的驱动器号，并且要还原到的目录必须为根目录 (\)。
3. 重新安排根目录条目(如有必要)。
   a. 运行 omnipm，选择 EUP，然后单击**根...**。 此时将显示 EUP 的根目录。
   b. 将根目录的条目重新排序到其原始位置。 使用拖放或右键单击条目以显示选项菜单。
4. 将 FAT16 分区更改为真正的 EUP。
   a. 选择 EUP，然后单击**取消映射**。 此时即删除驱动器号。
   b. 单击**类型**。 此时将显示一个对话框窗口。 选择 **Eisa 实用程序分区**。

增强型自动灾难恢复 (EADR)

增强型自动灾难恢复用于恢复普通 Data Protector Cell Manager 和客户机，以及属于 Microsoft 群集服务器 (MSCS) 一部分的 Data Protector Cell Manager 和客户机。

本节将介绍在遇到灾难恢复情况后需要执行的步骤/任务。

概述

确保已执行准备一章中提及的所有常规准备步骤。 对 Windows 客户机使用增强型自动灾难恢复方法的常规步骤包括：

1. **阶段 1**
   a. 更换故障硬件。
   b. 从灾难恢复 CD、USB 驱动器或通过网络启动目标系统并选择恢复的范围。 这是完全无人看管的恢复。

   > **重要：**
   > Windows Server 2003：如果您要恢复域控制器，在启动灾难恢复向导之前，标准的 Windows 登录对话框将提示您输入用户名 (Administrator) 和“目录服务还原模式”管理员帐户的密码。

2. **阶段 2**
   a. 根据您所选的恢复范围，系统将自动还原所选的卷。 关键卷(引导分区和操作系统)始终会被还原。

3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

> **重要：**
> 提前为任何必须首先还原的关键系统(尤其是 DNS 服务器、Cell Manager、介质代理客户机、文件服务器等等)准备好灾难恢复 CD、可引导 USB 驱动器或带恢复集的可引导网络映像。
>
> 提前为 Cell Manager 恢复准备好包含加密密钥的可移动介质。

以下各节将介绍与 Windows 客户机的 EADR 相关的限制、准备和恢复。 有关详细信息，另请参见“高级恢复任务”一节。

先决条件

在选择此灾难恢复方法前，请考虑以下要求和限制：

- 需要用新硬盘更换受影响的磁盘。 新磁盘的大小必须等于或大于受影响的磁盘。 如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 为了对 Cell Manager 进行灾难恢复，您应当具备有效的“内部数据库”备份映像，它应当比文件系统备份映像新。
- 目标系统的硬件配置必须与原始系统相同。 其中包括 SCSI BIOS 设置(扇区重新映射)。
- 确保已启用自动装载功能。 自动装载功能可确保所有卷(没有装载点)都处于联机状态。 如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。 因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

  如果需要禁用自动装载功能，则确保已装载系统保留分区。
- **Windows Server 2003：** 如果受影响的系统是域控制器，则需要“目录服务还原模式”管理员帐户的密码。
- 在 Windows XP 和 Windows Server 2003 系统上，引导分区(在其上安装了 DR OS)必须大于 200 MB，否则灾难恢复将失败。 如果没有这些磁盘空间，则灾难恢复将失败。 如果已在原始分区上应用了压缩驱动器，则必须有 400 MB 可用。
- 在 Windows Vista 及更高版本中，至少有一个卷必须为 NTFS 卷。
- 在 Windows Server 2003 系统上，引导所需的所有驱动程序都必须安装在 *%SystemRoot%* 文件夹下。
- 对于远程还原，在引导 DR OS 映像时，网络必须可用。

为增强的自动灾难恢复做的准备(Windows 和 Linux)

要做好准备而使灾难恢复成功，请遵照与所有灾难恢复方法的常规准备过程相关的说明，然后再执行本主题中列出的步骤。 必须提前准备，以便快速高效地执行灾难恢复。 应特别注意 Cell Manager 的灾难恢复准备。

> **重要：**
> 请在灾难发生之前准备灾难恢复。

先决条件

在选择此灾难恢复方法前，请考虑以下要求和限制：

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。 有关详细信息，请参见《*Data Protector 安装指南*》。
- 在 Windows Vista 及更高版本中，至少有一个卷必须为 NTFS 卷。
- 用于灾难恢复的所有必要数据的备份可能需要大量可用空间。 通常 500 MB 便足够，最高可能需要 1 GB，具体取决于操作系统。
- 在 DR OS 映像创建期间，安装 Data Protector 所在的分区必须至少具有 500 MB 的临时可用空间。 此空间是创建临时映像所必需的。
- 确保已启用自动装载功能。 自动装载功能可确保所有卷(没有装载点)都处于联机状态。 如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。 因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

  如果需要禁用自动装载功能，则确保已装载系统保留分区。
- 在 Windows Server 2003 系统上，引导所需的所有驱动程序都必须安装在 *%SystemRoot%* 文件夹下。
- 确保已启用自动装载功能。 自动装载功能可确保所有卷(没有装载点)都处于联机状态。 如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。 因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

  如果需要禁用自动装载功能，则确保已装载系统保留分区。
- 在群集环境中，如果每个群集节点上的总线地址枚举相同，则可以成功备份群集节点。 这表示需要：
  - 群集节点主板硬件相同
  - 两个节点上的 OS 版本(Service Pack 和更新)相同
  - 总线控制器的数量和类型相同
  - 必须在相同的 PCI 主板插槽中插入总线控制器。
- 在备份时应当激活操作系统。 否则，当激活期到期时，灾难恢复会失败。
- 要创建 Windows Vista 和更高版本的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包 (ADK)：

  Windows Vista 和 Windows Server 2008：

  适用于 Windows Vista SP1 和 Windows Server 2008 的自动安装工具包 (AIK)

  Windows 7 和 Windows Server 2008 R2：
  - 适用于 Windows 7 的 Windows 自动安装工具包 (AIK)
  - 适用于 Windows 7 SP1 的 Windows 自动安装工具包 (AIK) 补充(可选，适用于 Microsoft Windows 7 SP1 和 Windows Server 2008 R2 SP1)

  Windows 8 和 Windows Server 2012：
  - Windows 8 和 Windows Server 2012 的评估和部署工具包 (ADK 1.0)

Data Protector 将检查 WAIK/ADK 版本，如果没有适当的版本可用，将中止映像创建。

Windows 8.1 和 Windows Server 2012 R2：

- Windows 8.1 和 Windows Server 2012 R2 的评估和部署工具包 (ADK 1.1)

- 对于从可引导 USB 设备进行的灾难恢复，请确保：
  - USB 存储设备的大小应至少为 1 GB
  - 目标系统支持从 USB 设备引导。 较旧的系统可能需要更新 BIOS，否则可能完全无法从 USB 存储设备启动。
- 要为 Windows Vista 和更高版本的 Windows 系统创建可引导网络映像，必须满足以下条件：
  - 在目标系统上，已启用网络适配器以通过 PXE 协议进行通信。 此系统的 BIOS 应与 PXE 协议兼容。
  - 已经在 Windows Server 2008 和更高版本的 Windows 系统上安装并配置 Windows 部署服务 (WDS) 服务器。 WDS 服务器必须为 Active Directory 域的成员或 Active Directory 域的域控制器。
  - 具有活动范围的 DNS 服务器和 DHCP 服务器正在网络中运行。
- 要备份位于 Windows Vista 和更高版本上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。
- 在为 RedHat 7 客户机创建恢复 ISO 映像的过程中，恢复介质创建主机必须安装 **squashfs 工具**，才能成功创建恢复 ISO 映像。

限制

- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。 可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- 可以在 Windows 7、Windows 8、Windows Server 2008 R2 系统(在所有受支持平台上)、Windows Server 2008 系统(在 Itanium 平台上)以及 Windows Server 2012 和更高版本上创建可引导 USB 驱动器。
- 在 Windows XP 和 Windows Server 2003 上，不支持恢复 SAN 引导配置。
- 仅可在 Windows Vista 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows XP 和 Windows Server 2003 上，无法通过网络引导目标系统。
- 在 Windows XP 和 Windows Server 2003 上，可使用控制台界面而不是 Data Protector 灾难恢复 GUI。
- 在 Windows Vista 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- 请勿选择属于检查点重新启动备份会话的备份对象版本。
- 选择对象复制作为恢复源时，需遵守以下规则：
  - 只能选择完整备份对象的副本用于恢复。
  - 仅在从卷的列表中创建卷恢复集时才能选择对象副本。 不支持会话。

- 不支持介质副本。

- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。
- DRM 还原监控器监控 VRDA 进程写入磁盘的总字节数。 写入磁盘的总字节数并不总是与 Data Protector 会话管理器中显示的数量匹配。

  > **注意：**
  > 仅在 Windows Vista 及更高版本上实施新的恢复会话监控器。

- 在脱机还原期间，稀疏文件将还原为其完整大小。 这可能会导致目标卷空间不足。
- AUTODR 不支持恢复多个设备上的 btrfs(多种 btrfs raid 配置)，因为它们不受 SLES 11.3 支持。
- SLES 11.3 上当前的 btrfs 工具不会在新创建的 btrfs 文件系统上设置 UUID。 因此，在恢复期间，AUTODR 无法像备份时那样在 btrfs 文件系统上设置相同的 UUID。

  如果按 UUID 而不是设备名称装载 btrfs 文件系统，您需要在还原后手动编辑 `/etc/fstab` 文件。 需要执行此操作来反映恢复后 btrfs 设备的新的也是正确的 UUID。 这同样适用于 GRUB 配置，因此避免用于 root 设备的 UUID，并按名称更换设备。

  在系统恢复后，btrfs 的 UUID 将与备份期间的不同。 如果从在系统上次恢复之前创建的备份再执行一次恢复，AUTODR 将尝试识别正常的 btrfs 文件系统并跳过重新创建它们。
- AUTODR 只能将备份中的 btrfs 设备配置映射到按 UUID 恢复的现有系统中的 btrfs 设备。 它会跳过恢复错误的设备或重新创建的设备。

  要避免这种情况，应仅从在系统上次恢复后创建的备份恢复 btrfs 文件系统或在系统恢复之前手动销毁现有 btrfs 文件系统。 这同样适用于用户在上次备份后手动重新创建的 btrfs 文件系统。

  > **注意：**
  > Data Protector 将在开始恢复过程之前警告用户这种情况。

- btrfs 快照可以备份，但是只能还原为普通子卷。 在这种情况下，不会在快照与创建快照所在的子卷之间共享任何数据。 父对象与其快照之间的整体写时复制 (COW) 关系会丢失。 因此，在某些情况下，无法还原完整的数据集，因为快照中的数据重复，在还原期间底层设备上空间不足。
- 只有装载的 btrfs 子卷中的数据受保护。 考虑一下，可从 OS 文件系统接口和装载的父子卷访问子子卷。 在这种情况下，子卷不受保护，因为磁盘代理 (DA) 将其检测为不同的文件系统并跳过它们，原因是它们没有专用的装载点。
- 使用 `/etc/fstab` 文件中的 `subvolid`(请参阅 *btrfs 文档*)装载选项装载的子卷可能会在恢复的系统中跳过装载或装载到错误的装载点，因为恢复后子卷的 `subvolid` 不需要与备份期间的相同。 尽管会重新创建所有子卷，但是 Data Protector 会跳过在此类子卷中还原数据或者可能会在错误的子卷中还原数据。

  > **注意：**
  > 使用 `fstab` 中的 `subvol` 选项而不是 `subvolid`。

磁盘和分区配置

- 驻留在 Windows 群集中的共享动态磁盘不支持 EADR。
- 如果系统保留卷驻留在动态磁盘上，在 Data Protector GUI 中，卷不由黄色图标指示，而是指示为绿色图标。

- 通过动态磁盘执行灾难恢复时，在启动 EADR 之前需要清除所有磁盘。
- EADR 会话之后，将重新创建所有卷，但只有恢复范围内的卷能够还原。
- 新磁盘的大小必须等于或大于崩溃的磁盘。 如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12(包括 EISA)和 0xFE 的供应商特有分区。
- 在 Windows XP 和 Windows Server 2003 系统上，不能在 Data Protector 安装于 FAT/FAT32 分区上的系统中创建灾难恢复 ISO 映像。 单元中至少需要有一个在 NTFS 卷上安装 Data Protector 的客户机，才能创建灾难恢复映像
- 恢复使用 HPE Intelligent Provisioning 工具(1.4 和 1.5 版本)部署的操作系统可能会由于错误的 MBR 分区信息而失败。
- 稀疏文件被还原为其完整大小。 这可能会导致目标卷空间用尽。
- 不支持物理磁盘不完全属于存储池的存储空间配置。

常规准备

1. 执行完整的客户机系统备份。 建议备份整个客户机，如若不然，您至少需要选择以下关键卷和对象：
   - 引导和系统卷
   - Data Protector 安装卷
   - CONFIGURATION 对象所在的卷
   - Active Directory 数据库卷(如果使用 Active Directory 控制器)
   - 仲裁卷(如果是 Microsoft 群集服务器)

   有关 *Data Protector Cell Manager 系统*，请参见Cell Manager 的额外准备 (第 40 页)。

   请参见 *Data Protector 帮助*索引：“备份, Windows 特有”和“备份, 配置”

   在客户机完整备份期间，恢复集和 P1S 文件存储在备份介质和 Cell Manager(恢复集可选)上。

   注意事项：

   ***Windows Vista 和更高版本*：**

   - 请确保同时备份存在的系统卷。
   - 可以通过使用 VSS 写入程序的磁盘映像备份来备份逻辑卷。 VSS 磁盘映像备份可确保卷在备份过程中保持未锁定状态，并可由其他应用程序访问。 必须使用常规文件系统备份来备份 IDB 和 CONFIGURATION 对象以及未装载的卷或作为 NTFS 文件夹装载的卷。

   ***Windows Server 2012 (R2)*：**

- 使用磁盘映像备份在以下情况下备份卷：
  - 已删除重复数据的卷

    在文件系统还原期间，将卷再次合成，并且在恢复期间您可运行目标卷上的空间。 磁盘映像还原会保持卷的大小。
  - 使用复原文件系统 (ReFS) 的卷

Microsoft 群集服务器：

- 一致的备份包括(在相同的备份会话)中：
  - 所有节点
  - 管理虚拟服务器(由管理员定义)
  - 如果将 Data Protector 配置为群集感知应用程序，则包括 Cell Manager 虚拟服务器和 IDB。

  以上各项应包含在相同的备份会话中。

  有关详细信息，请参见关于 Microsoft 群集服务器的灾难恢复 (第 61 页)。

- *群集共享卷：*执行客户机系统完整备份前，请先使用 Data Protector 虚拟环境备份虚拟硬盘 (VHD) 文件和 CSV 配置数据。 请参见《*Data Protector 集成指南*》。

  必须卸载虚拟硬盘 (VHD) 以确保一致性。

- 执行备份之后，在 MSCS 中合并所有节点的 P1S 文件，以使每个节点的 P1S 文件都包含关于共享群集卷配置的信息。

  如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。 如果要恢复 Cell Manager 或如果无法与 Cell Manager 建立连接，则需要该密钥。

Windows Server 2008 和更高版本的 Windows Server 上的 Active Directory：

- 如果您的 Windows Server 是 Active Directory 大小超过 512 MB 的域控制器，则需要修改客户机备份的备份规范：在源页中，展开 `CONFIGURATION` 对象，并清除 `ActiveDirectoryService` 和 `SYSVOL` 项的复选框。

  > **注意：**
  > 将仍作为系统卷 (`C:/`) 备份的一部分备份 Active Directory 和 SYSVOL。 默认情况下，它们分别位于 `C:/Windows/NTDS` 和 `C:/Windows/SYSVOL`。

2. 在执行客户机的灾难恢复之前，在 Cell Manager 上运行以下命令，以进行联机恢复，并在介质主机上运行，以进行脱机恢复。
   ```
   omnicc -secure_comm -configure_for_dr <hostname_of_client being_recovered>
   ```
3. 联机恢复客户机之后，在 Cell Manager 上运行以下命令：
   ```
   omnicc -secure_comm -configure_peer <client_host_name> -overwrite
   ```
4. 灾难发生之后，使用 EADR 向导将 DR 映像转换为灾难恢复 CD ISO 映像。
   Windows Vista 及更高版本：或者，使用 DR OS 映像代替灾难恢复 CD 来创建可引导网络映像或可引导 USB 驱动器。
5. 使用支持 ISO9660 格式的任何 CD 录制工具在 CD 上录制灾难恢复 CD ISO 映像。 此灾难恢复 CD 随后可用于引导目标系统并自动还原关键卷。
6. 执行灾难恢复测试计划。

7. 在 Windows 系统上，如果在启动后某些服务或驱动程序无法运行，则可能需要手动编辑 kb.cfg 文件。

Cell Manager 的额外准备

成功对 Cell Manager 进行灾难恢复还需要额外的准备。

- 对 Cell Manager 执行灾难恢复之前，在用于灾难恢复的介质主机上运行以下命令：
  `omnicc -secure_comm -configure_for_dr <cell_manager_hostname>`
- 恢复完成之后，在介质主机上运行以下命令：
  `omnicc -secure_comm -configure_peer <cell_manager_hostname>`
- 定期备份 IDB。 IDB 会话不应早于文件系统会话。
- 在安全位置(而非在 Cell Manager 上)存储 Cell Manager 的 SRD 文件。
- 提前为 Cell Manager 准备灾难恢复操作系统映像。

将恢复集保存到 Cell Manager

在进行完整客户机备份期间，恢复集打包在单个大型文件中，并存储在备份介质上和(可选)Cell Manager 上。 如果计划在 Cell Manager 上录制灾难恢复 CD，则将恢复集文件保存到 Cell Manager 会很有用，这是因为从硬盘获取恢复集比从备份介质还原要快得多。

如果在备份期间将恢复集保存到 Cell Manager，则系统会将其保存到默认的 Data Protector P1S 文件位置。

要更改默认位置，请指定一个新的全局选项 `EADRImagePath = valid_path`(例如 `EADRImagePath = /home/images` 或 `EADRImagePath = C:\temp`)。

请参见《Data Protector 帮助》的索引："全局选项, 修改"。

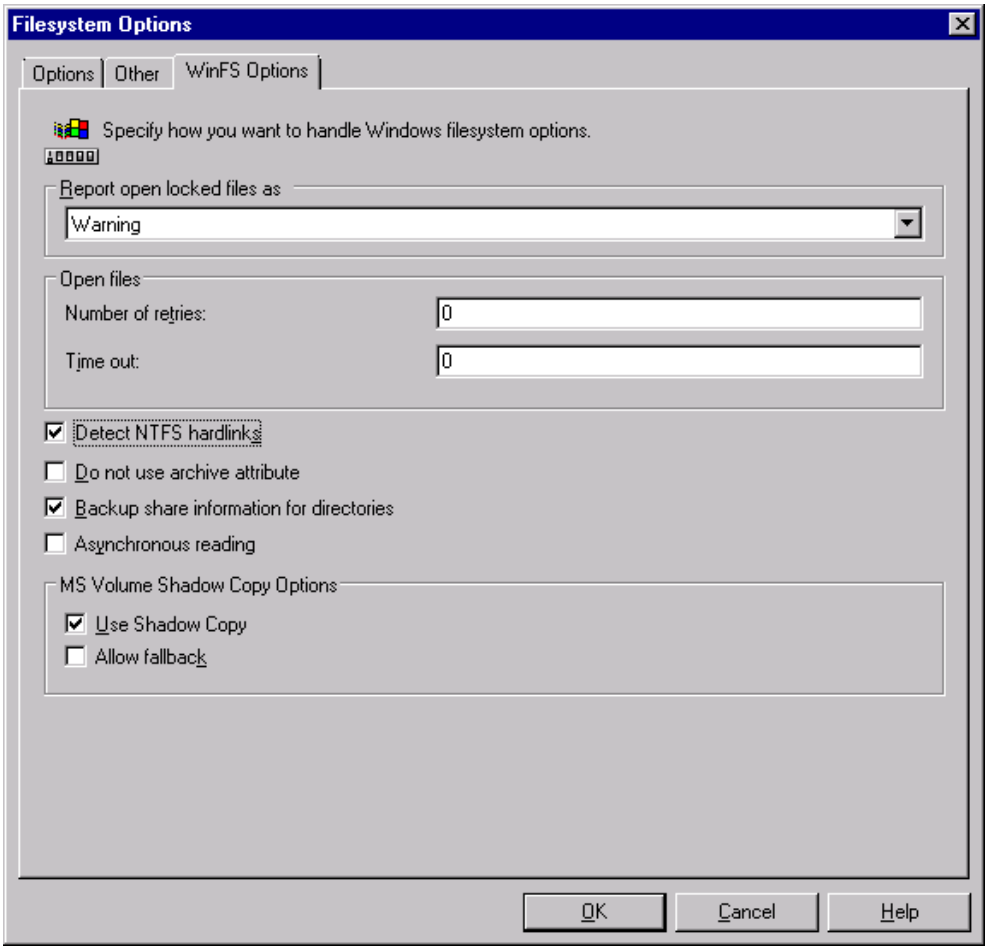
> **提示：**
> 如果在目标目录中没有足够的可用磁盘空间，则可以创建装载点(Windows 系统)或另一个卷的链接(UNIX 系统)。

将备份规范中所有客户机的恢复集文件保存到 Cell Manager

步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范(创建该备份规范 - 如果尚未执行此操作)。 有关详细信息，请参见《Data Protector 帮助》的索引："创建, 备份规范"。
4. 在"结果区域"中，单击**选项**。
5. 在**文件系统选项**下，单击**高级**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. **Windows Vista 及更高版本**：在 **WinFS 选项**页中，选择**检测 NTFS 硬链接**，选中**使用卷影复制**选项并清除**允许回退**。 请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

“WinFS 选项”选项卡



将备份规范中特定客户机的恢复集保存到 Cell Manager

要仅为备份规范中的特定客户机复制恢复集文件，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范(创建该备份规范 - 如果尚未执行此操作)。 有关详细信息，请参见《Data Protector 帮助》的索引：“创建, 备份规范”。
4. 在"结果区域"中，单击**备份对象摘要**。
5. 选择要将其恢复集文件存储在 Cell Manager 上的客户机，并单击**属性**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。
7. **Windows Vista 及更高版本：**在 **WinFS 选项**页中，选中**检测 NTFS 硬链接**和**使用卷影复制**选项并清除**允许回退**。 请注意，如果手动添加对象或更新现有备份规范，则不会自动选中**检测 NTFS 硬链接**选项。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。 对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。 在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 *Data_Protector_program_data*\Config\Server\export\keys\DR-*ClientName*-keys.csv(Windows 系统)或 /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv(UNIX 系统)，其中 *ClientName* 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

准备 DR OS 映像

灾难发生之前，应准备一个要录制在灾难恢复 CD 上或保存到可引导 USB 驱动器的 DR OS 映像，它随后可用于增强的自动灾难恢复。 或者，也可以准备可引导的网络映像。

请注意，必须在将准备 DR OS 映像的系统上安装 Data Protector 自动灾难恢复组件。

每次硬件、软件或配置更改之后都必须根据新的恢复集准备好一个新的灾难恢复 OS 映像。

为必须首先恢复的任何关键系统提前准备 DR OS 映像，尤其是网络正常工作所需的系统(DNS 服务器、域控制器、网关等)、Cell Manager、介质代理客户机和文件服务器等。

建议对含有 OS 映像的备份介质和灾难恢复 CD 或 USB 驱动器的访问权限进行限制。

步骤

1. 在 Data Protector 上下文列表中，单击**恢复**。
2. 在“范围窗格”中，单击**任务**，然后单击**灾难恢复**以启动灾难恢复向导。
3. 在结果区域中，从**要恢复的主机**下拉列表中选择要为其准备 DR OS 映像的客户机，然后单击**验证**以验证该客户机。

   > **注意：**
   > 经过验证的客户机将添加到**要恢复的主机**下拉列表中。

4. 在**恢复介质创建主机**下拉列表中，选择要在其上准备 DR OS 映像的客户机。 默认设置下，该客户机与为其准备 DR OS 映像的客户机一样。 您在其上准备 DR OS 映像的客户机必须安装有相同 OS 类型(Windows、Linux)，并且必须已安装“磁带客户机”。
5. 使**增强的自动灾难恢复**保持选中状态，并选择要从备份会话还是从卷列表构建卷恢复集。 默认情况下，选择**备份会话**。

   单击**下一步 (Next)**。
6. 具体取决于所选的恢复集构建方法：
   - 如果选择了备份会话，则应选择主机备份会话；如果是 Cell Manager，则选择 IDB 会话。
   - 如果选择了“卷”列表，则应为每个关键对象选择相应的对象版本。

单击**下一步 (Next)**。

7. 选择恢复集文件的位置。 默认情况下，**从备份还原恢复集文件**处于选中状态。

   如果在备份期间已在 Cell Manager 上保存了恢复集文件，则应选择**指向恢复集文件的路径**并指定其位置。 单击**下一步 (Next)**。

8. 选择映像格式。 可用的选项如下：
   - **创建可引导 ISO 映像**：DR ISO 映像(默认情况下为 `recovery.iso`)
   - **创建可引导 USB 驱动器**：可引导 USB 驱动器上的 DR OS 映像
   - **创建可引导网络映像**：可用于网络引导的 DR OS 映像(默认情况下为 `recovery.wim`)
9. 如果创建的是可引导 ISO 映像或可引导网络映像，请选择要将创建的映像放置到的目标目录。

   如果要创建可引导的 USB 驱动器，请选择要在其中放置所创建的映像的目标 USB 驱动器或磁盘编号。

   > **重要：**
   > 在创建可引导的 USB 驱动器时，该驱动器上存储的所有数据将丢失。

10. 也可选择设置密码来防止对 DR OS 映像进行未授权的使用。 锁图标指示是否设置了密码。

    单击**密码**打开“密码保护映像”对话框并输入密码。 要删除密码，清除字段内容即可。

11. **Windows Vista 和更高版本：**

    查看并修改(如果需要)插入 DR OS 映像中的驱动程序的列表。

    可以使用此选项将缺少的驱动程序添加到 DR OS 中。 通过单击**添加**或**删除**，手动添加或删除驱动程序。 要重新加载原始驱动程序，请单击**重新加载**。 恢复集的 `%Drivers%` 部分中的驱动程序将自动插入 DR OS 映像中。

    > **重要：**
    > 在备份过程中收集且存储在恢复集的 `%Drivers%` 目录中的驱动程序可能并不总是适合在 DR OS 中使用。 在某些情况下，可能需要插入 Windows 预安装环境 (WinPE) 所特有的驱动程序才能确保恢复期间硬件能正常工作。

12. 单击**完成**以退出向导并创建 DR OS 映像。
13. 如果要创建可引导的 CD 或 DVD，可使用支持 ISO9660 格式的刻录工具，将 ISO 映像刻录在 CD 或 DVD 上。

使用增强型自动灾难恢复恢复 Windows 系统

只有完成了所有准备步骤后，才能成功执行 Windows 系统的增强型自动灾难恢复。如果要恢复 Cell Manager，将先从内部数据库的备份映像将该内部数据库还原，然后从卷和 CONFIGURATION 对象的备份映像将卷和 CONFIGURATION 对象还原。有关受支持操作系统的详细信息，请参见《Data Protector 产品声明、软件说明和参考》。

步骤

阶段 1

1. 除非要执行脱机灾难恢复，否则根据目标系统的操作系统，要向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的 Data Protector 帐户：

   Windows Vista 和更高版本：

   - 类型：Windows
   - 名称:SYSTEM
   - 组/域：NT AUTHORITY
   - 客户机：正在恢复的系统的临时主机名

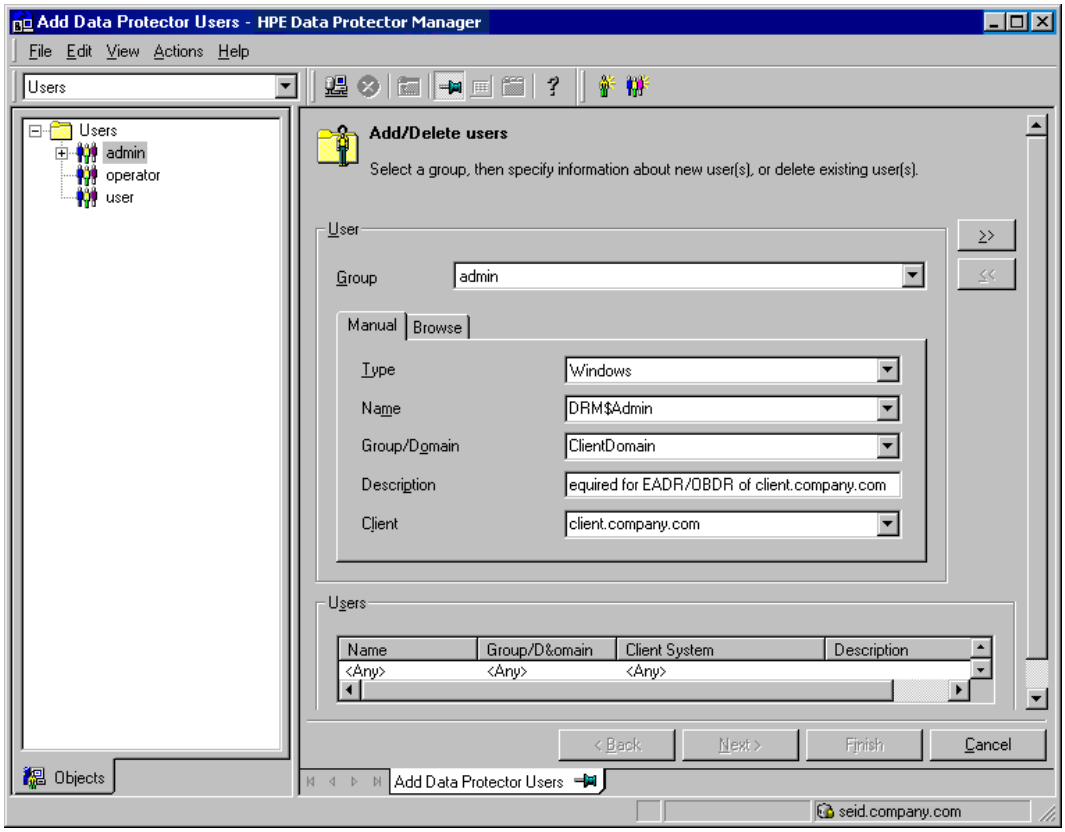
     Windows 预安装环境 (WinPE) 向系统分配了临时主机名。通过在 WinPE 的命令提示符窗口中运行 hostname 命令，可以检索该主机名。

   Windows XP、Windows Server 2003：

   - 类型：Windows
   - 名称:DRM$Admin
   - 组/域：目标系统的主机名
   - 客户机：目标系统的完全限定域名 (FQDN)

   有关添加用户的详细信息，请参见 Data Protector 帮助索引：“添加 Data Protector 用户”。

   添加用户帐户



2. 从原始系统的灾难恢复 CD、可引导 USB 驱动器或可引导网络映像引导客户机系统。如果要从灾难恢复 CD 启动目标系统，请确保没有外部 USB 磁盘(包括 USB 密钥)连接到系统，然后再开始恢复过程。

> **注意：**
> 如果在恢复期间屏幕缩短，可用以下凭据登录：
>
> 用户： `DRM$ADMIN`
>
> 密码： `Dr8$ad81n$pa55wD`

3. **Windows Server 2003：** 如果要恢复域控制器，请在出现“欢迎使用 Windows”对话框时，按 **Ctrl+Alt+Delete** 键，输入“目录服务还原模式”管理员帐户的密码，然后单击**确定**。
4. 选择恢复范围和恢复选项。下面的步骤将随操作系统的不同而不同：

   Windows Vista 和更高版本：

   a. 灾难恢复 GUI(安装程序向导)出现，并显示原始系统信息。单击**下一步 (Next)**。

   > **提示：**
   > 当显示进度条时，系统会提供一些键盘选项。可以通过将鼠标悬停在进度条上来检查可用的选项及其说明信息。

   b. 在“恢复范围”页面上，选择恢复的范围：

   - `Default Recovery`：恢复关键卷(系统磁盘、引导磁盘和 Data Protector 安装卷)。对所有其他磁盘进行分区和格式化，并使其保持空白，为阶段 3 做好准备。
   - `Minimal Recovery`：仅恢复系统磁盘和引导磁盘。

- Full Recovery：恢复“还原集”中的所有卷，而不是仅恢复关键卷。
- Full with Shared Volumes：对 Microsoft 群集服务器 (MSCS) 可用。如果 MSCS 中的所有节点都受到灾难的打击，并且要执行第一个节点的 EADR，则应使用此选项。它将恢复“还原集”中的所有卷，其中包括备份时由备份节点锁定的群集共享卷。如果至少一个节点活动并且正在运行 MSCS 服务，则将不还原共享卷，因为节点将锁定这些共享卷。在这种情况下，应使用 Default Recovery。

c. (可选)要修改恢复设置，请单击**设置**以打开“恢复设置”页面。

系统提供了以下其他一些恢复选项，其中一些选项需在灾难恢复未结束或需执行其他步骤时使用：

- Use original network settings：如果需要还原原始网络配置(例如，由于缺少 DHCP 服务器)，可选择此选项。默认设置下未选中该选项，并且 DR OS 恢复环境会使用 DHCP 网络配置。
- Restore BCD：如果选择此选项，则 Data Protector 在灾难还原会话期间还会提前还原引导配置数据 (BCD) 存储，然后在 Data Protector 还原会话中再还原该存储。默认情况下选择此选项。
- Restore DAT：如果选中，Data Protector 灾难恢复模块还将还原 Microsoft VSS 写入程序的数据。默认设置下，DR 模块会跳过 VSS 写入程序数据的还原。如果在非 VSS 备份期间， Data Protector 无法备份关键写入程序，您可使用该选项。要在 DR 模块还原之前还原数据，可选择 Pre。要在 Data Protector 之后还原数据，可选择 Post。
- Initialize Disks Manually：使用此选项可以手动映射原始系统磁盘和当前系统磁盘，并对它们进行初始化以使其与原始配置匹配。默认情况下，不选择此选项。

  如果选择了此选项，在恢复过程启动时将显示新的磁盘映射和初始化页面。灾难恢复模块将提供初始磁盘映射并显示初始映射尝试的结果。使用提供的选项更改磁盘映射。映射完成后，卷得到初始化并且系统将重新启动。
- Restore Storage Spaces：默认情况下，将还原存储空间。在恢复时，如果存储配置允许，您可以取消选项该选项并将虚拟磁盘直接还原为物理磁盘。请注意，如果要将存储空间还原为不同的硬件或 USB 磁盘，则需要手动对磁盘进行初始化。
- Enable Dissimilar Hardware Restore：如果启用，Data Protector将在恢复过程中扫描系统中缺少的驱动程序。可通过从下拉列表中选择下列方法之一来启用该选项：
  - Unattend默认此模式使用预定义的配置文件自动将操作系统配置到不同的硬件平台中。对于不同的硬件，这是主要的恢复模式。请在第一个实例中使用。
  - Generic：如果无人参与模式失败(可能是因为所还原的操作系统的配置不正确)，可选择此项。它将调整所还原的操作系统注册表及其驱动程序和服务，以适应不同的硬件。
- Remove Devices：在启用了 Dissimilar Hardware 选项时可用。如果选中，Data Protector将从还原的操作系统的注册表中删除原始设备。
- Connect iSCSI Devices：如果原始计算机正在使用 iSCSI，则会启用该选项。通过选择该选项，Data Protector 可在备份时自动还原基本 iSCSI 配置。如果未选中，将跳过 iSCSI 配置。

您也可使用本机 Microsoft iSCSI 配置向导来管理更为复杂的 iSCSI 配置。如果 DR GUI 检测到某些 iSCSI 功能(例如安全选项)需要手动配置，则会提供选项来运行 Microsoft iSCSI 配置向导。

- Map Cluster Disks Manually：在 Windows Server 2008 及更高版本上可用。如果选择此选项，您可以手动映射群集卷。如果不选择此选项，将自动映射卷。在执行自动映射后，建议检查所有卷是否已正确映射。
- Remove Boot Descriptor：在 Intel Itanium 系统中可用。删除由灾难恢复过程留下的所有引导描述符。
- Manual disk selection：在 Intel Itanium 系统中可用。如果磁盘设置显著变化，则灾难恢复模块可能找不到引导磁盘。使用此选项可选择正确的引导磁盘。

要将选项重置为默认设置，请单击**重置默认设置**。

单击**保存 >** 以保存更改。

d. 单击**完成**启动恢复。恢复过程开始，并且您可以监视进度。

如果已使用 BitLocker 驱动器加密对卷进行了加密，则系统将提示您解锁已加密的驱动器。

> **提示：**
> 在灾难恢复 GUI 中，可以单击**任务**执行以下操作：
> - 运行命令提示符、任务管理器或磁盘管理器
> - 访问 Map Network Drives 和 Load Drivers 工具
> - 查看特定于灾难恢复过程的日志文件
> - 启用或禁用 DRM 配置文件，以及在文本编辑器中查看和编辑该文件
> - 编辑 WinPE 恢复环境的 hosts 文件
> - 访问“帮助”和查看 GUI 图标图例

Windows XP 和 Windows Server 2003 系统：

a. 显示以下消息时按 **F12**：To start recovery of the machine *Hostname* press F12。

b. 在引导过程开始时将显示范围选择菜单。选择恢复的范围，然后按 **Enter**。有 5 种不同的恢复范围：

- Reboot：不执行灾难恢复，但重新启动系统。
- Default Recovery：恢复关键卷(系统磁盘、引导磁盘和 Data Protector 卷)。对所有其他磁盘进行分区和格式化，并使其保持空白，为阶段 3 做好准备。
- Minimal Recovery：仅恢复系统磁盘和引导磁盘。
- Full Recovery：恢复“还原集”中的所有卷，而不是仅恢复关键卷。
- Full with Shared Volumes：对 Microsoft 群集服务器 (MSCS) 可用。如果 MSCS 中的所有节点都受到灾难的打击，并且要执行第一个节点的 EADR，则应使用此选项。它将恢复“还原集”中的所有卷，其中包括备份时由备份节点锁定的群集共享卷。如果至少一个节点活动并且正在运行 MSCS 服务，则将不还原共享卷，因为节点将锁定这些共享卷。在这种情况下，应使用 Default Recovery。

系统提供了以下其他一些恢复选项，其中一些选项需在灾难恢复未结束或需执行其他步骤时使用：

- Remove Boot Descriptor：在 Intel Itanium 系统中可用。删除由灾难恢复过程留下的所有引导描述符。

- Manual disk selection：在 Intel Itanium 系统中可用。如果磁盘设置显著变化，则灾难恢复模块可能找不到引导磁盘。使用此选项可选择正确的引导磁盘。

阶段 2

4. 选择了恢复的范围之后，Data Protector 开始设置 DR OS。可以监视进度，而在安装 DR OS 后将重新启动系统。在 Windows Vista 和更高的版本中，不会执行系统重启。

   提示 To start recovery of the machine *Hostname* press F12 时等待 10 秒，以便从硬盘而非从 CD 引导。

   在 Windows XP 和 Windows Server 2003 上，如果 DR OS 无法正常引导或无法访问网络，则可能需要编辑 kb.cfg 文件。

   此时将显示灾难恢复向导。要修改灾难恢复选项，请按任意键在倒数期间停止向导，然后修改选项。

   可用的选项如下：

   - Debugs...：启用调试。请参见调试灾难恢复会话 (第 107 页)。
   - Omit deleted files：将不还原在连续增量备份期间删除的文件。这可能会减慢恢复速度。
   - Install only：此选项仅向目标系统安装临时操作系统，并因此结束灾难恢复的阶段 1。将不自动启动灾难恢复阶段 2。例如，如果要编辑 SRD 文件，可以使用此选项。

   此外，可以使用相应的按钮启动注册表编辑器、命令行或任务管理器。

   单击**完成**继续进行灾难恢复。
5. 如果 DR OS 映像受密码保护，请提供密码并继续恢复。
6. 如果灾难恢复备份经过加密，并且您要恢复 Cell Manager 或无法访问 Cell Manager 的客户机，则将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库 (DR-*ClientName*-keys.csv)(例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器)，并输入密钥库文件的完整路径。密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。现在将继续进行灾难恢复，不会再有其他中断现象。
7. 如果 SRD 文件中的信息并非最新(例如因为灾难之后更改了备份设备)，并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
8. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。第一次登录之后将删除临时 DR OS，但以下情况除外：
   - Minimal Recovery 处于选定状态。
   - 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。

- 您手动执行带有 omnidr 或 -no_reset 选项的 -debug 命令。
- 灾难恢复失败。

在 Windows Vista 和更高的版本中，永远不会保留临时的 DR OS。

注意，Data Protector 将首先尝试执行联机恢复。如果联机恢复因任何原因而失败(例如，Cell Manager 或网络服务不可用，防火墙正在阻止访问 Cell Manager)Data Protector 将尝试执行远程脱机恢复。甚至如果远程脱机还原失败(例如，因为介质代理主机仅接受来自 Cell Manager 的请求)，则 Data Protector 也将执行本地脱机还原。

9. 删除步骤 1 中从 Cell Manager 上 Data Protector Admin 用户组创建的客户机的本地 Administrator 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。
10. 如果要恢复 Cell Manager，则要使 IDB 一致。

阶段 3

10. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

> **注意：**
> Data Protector 在恢复之后不会还原卷压缩标志。备份时压缩的所有文件将还原为压缩形式，但如果还希望以压缩形式创建任何新文件，则必须手动设置卷压缩。

11. 如果要执行 Microsoft 群集服务器中所有节点的灾难恢复，则需要其他步骤。

一键式灾难恢复 (OBDR)

一键式灾难恢复 (OBDR) 是针对 Windows Data Protector 客户机的自动 Data Protector 恢复方法，只需极少的用户干预。有关受支持操作系统的详细信息，请参见最新的支持矩阵，网址为：https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

备份时，OBDR 将自动收集所有相关的环境数据。备份期间，临时安装和配置 DR OS 所需的数据打包在单个大型 OBDR 映像文件中，并存储在备份磁带上。灾难发生时，OBDR 设备(能够模拟 CD-ROM 的备份设备)用于直接从含有灾难恢复信息的 OBDR 映像文件所在的磁带引导目标系统。

启动 DR OS 映像后，Data Protector 将自动对磁盘进行格式化和分区，最后用 Data Protector 将原始操作系统还原到备份时的状态。

> **重要：**
> 每次硬件、软件或配置更改之后都要执行新的备份。这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

恢复的卷包括：

- 引导分区
- 系统分区
- 用于存储 Data Protector 安装数据的分区

使用标准 Data Protector 恢复过程可恢复任何剩余的分区。

概述

确保已执行准备一章中提及的所有常规准备步骤。对 Windows 客户机使用一键式灾难恢复方法的常规步骤如下：

1. **阶段 1**

   从恢复磁带引导并选择恢复范围。
2. **阶段 2**

   根据您所选的恢复范围，系统将自动还原所选的卷。

   关键卷(引导分区和操作系统)始终会被还原。
3. **阶段 3**

   使用标准 Data Protector 还原过程还原剩余的所有分区。

> **重要：**
> Micro Focus 建议限制对 OBDR 引导介质的访问。

以下各节将介绍有关在 Windows 系统上执行一键式灾难恢复的要求、限制、准备和恢复。另请参见“高级恢复任务”一节。

要求

- 必须在要允许使用此方法进行恢复的系统上安装 Data Protector 自动灾难恢复组件。有关详细信息，请参见《*Data Protector 安装指南*》。
- 客户机系统必须支持从将用于 OBDR 的磁带设备引导。

  有关支持的系统、设备和介质的详细信息，请参见磁带硬件兼容性表和最新的支持矩阵，网址为：https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。
- 目标系统的硬件配置必须与原始系统相同。其中包括 SCSI BIOS 设置(扇区重新映射)。
- 新磁盘的大小必须等于或大于受影响的磁盘。如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- Windows XP 和 Windows Server 2003：备份时引导分区上另外需要 200 MB 的可用磁盘空间。如果没有这些磁盘空间，则灾难恢复将失败。如果已在原始分区上应用了压缩驱动器，则必须有 400 MB 可用。
- 在 OBDR 备份期间，安装 Data Protector 所在的分区必须至少具有 500 MB 的临时可用空间。此空间是创建临时映像所必需的。
- Windows Server 2003：引导所需的所有驱动程序都必须安装在 *%SystemRoot%* 文件夹下。
- 必须为支持 OBDR 的设备创建具有不可追加介质使用策略和宽松介质分配策略的介质池。只有此池中的介质可用于灾难恢复。
- Windows XP 和 Windows Server 2003：在备份时应激活操作系统。否则，当激活期到期时，灾难恢复会失败。
- 要创建 Windows Vista 和更高版本的 DR OS 映像，必须在将创建映像的系统上安装相应版本的 Windows 自动安装工具包 (WAIK) 或评估和部署工具包：

Windows Vista 和 Windows Server 2008：

适用于 Windows Vista SP1 和 Windows Server 2008 的自动安装工具包 (AIK)

Windows 7 和 Windows Server 2008 R2：

- 适用于 Windows 7 的 Windows 自动安装工具包 (AIK)
- 适用于 Windows 7 SP1 的 Windows 自动安装工具包 (AIK) 补充(可选，适用于 Microsoft Windows 7 SP1 和 Windows Server 2008 R2 SP1)

Windows 8 和 Windows Server 2012：

- Windows 8 和 Windows Server 2012 的评估和部署工具包 (ADK 1.0)

Windows 8.1 和 Windows Server 2012 R2：

- Windows 8.1 和 Windows Server 2012 R2 的评估和部署工具包 (ADK 1.1)

- 要备份位于 Windows Vista、Windows 7 或 Windows Server 2008 系统上的 IIS 配置对象，请安装 IIS 6 Metabase Compatibility 包。

限制

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。
- 不支持不使用 Microsoft 引导加载程序的多引导系统。
- 在 Windows XP 和 Windows Server 2003 上，不支持恢复 SAN 引导配置。
- 仅可在 Windows Vista 及更高版本上将逻辑卷的 VSS 磁盘映像备份用于灾难恢复。
- 在 Windows XP 和 Windows Server 2003 上，可使用控制台界面而不是 Data Protector 灾难恢复 GUI。
- 在 Windows XP 和 Windows Server 2003 上，不支持使用“网络组合”适配器进行配置恢复。
- 在 Windows Vista 及更高版本上，仅可将原来加密的文件夹还原为未加密状态。
- Internet Information Server 数据库、终端服务数据库和证书服务器数据库在阶段 2 不会自动还原。 可以使用标准 Data Protector 还原过程在目标系统上还原这些数据库。
- DRM 还原监控器监控 VRDA 进程写入磁盘的总字节数。 写入磁盘的总字节数并不总是与 Data Protector 会话管理器中显示的数量匹配。

> **注意：**
> 仅在 Windows Vista 及更高版本上实施新的恢复会话监控器。

- 在脱机还原期间，稀疏文件将还原为其完整大小。 这可能会导致目标卷空间不足。

磁盘和分区配置

- 不支持动态磁盘(包括从 Windows NT 升级而来的镜像集)。
- 新磁盘的大小必须等于或大于崩溃的磁盘。 如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- OBDR 仅支持类型为 0x12(包括 EISA)和 0xFE 的供应商特有分区。
- 在 NTFS 卷上安装了 Data Protector 的系统支持 OBDR。
- 在 Intel Itanium 系统上，仅本地 SCSI 磁盘支持引导磁盘的恢复。

为一键式灾难恢复做的准备(Windows 和 Unix)

要做好准备而使灾难恢复成功，请遵照与灾难恢复常规准备过程相关的说明，然后再执行本主题中列出的步骤。 提前准备，以便快速高效地执行灾难恢复。

> **重要：**
> 请在灾难发生之前准备灾难恢复。

准备步骤

完成灾难恢复的常规准备之后，执行以下特定步骤以准备 OBDR。

1. 为 DDS 或 LTO 介质创建一个采用**不可追加**介质使用策略和**宽松**介质分配策略的介质池(因为备份介质在 OBDR 备份期间进行格式化)。 此外，将此介质池指定为 OBDR 设备的默认介质池。 请参见《*Data Protector 帮助*》的索引："创建介质池"。 只有此类池中的介质可用于 OBDR。
2. 在要允许使用 OBDR 进行恢复的系统上本地执行 OBDR 备份。

   注意事项

   Windows Vista 及更高版本：请确保备份存在的系统卷(例如引导卷)。

   Windows Server 2012 (R2)：使用磁盘映像备份在以下情况下备份卷：

   - 重复卷

     在文件系统还原期间，将把卷再次合成，并且在恢复期间您可运行目标卷上的空间。 磁盘映像还原会保持卷的大小。

   - 使用复原文件系统 (ReFS) 的卷

   Microsoft 群集服务器：一致的备份包括(在相同的备份会话中)：

   - 所有节点
   - 管理虚拟服务器(由管理员定义)
   - 如果将 Data Protector 配置为群集感知应用程序，则为客户机系统的虚拟服务器。

   要使用 OBDR 方法在 MSCS 上自动还原所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点，以使共享磁盘卷在 OBDR 备份期间不会由另一个节点锁定。 也就是说无法收集足够的信息为备份期间由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

   群集共享卷：执行客户机系统完整备份前，请先使用 Data Protector 虚拟环境备份虚拟硬盘驱动器 (VHD) 文件和 CSV 配置数据。 请参见《*Data Protector 集成指南*》。 必须在单独的设备上执行备份，因为只有在不可追加介质上才可以执行 OBDR 备份。

   必须卸载虚拟硬盘 (VHD) 以确保一致性。

   如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。 如果无法建立和 Cell Manager 之间的连接，您将需要密钥。
3. 对客户机执行灾难恢复之前，请在 Cell Manager 和介质主机上运行以下命令，分别进行联机恢复和脱机恢复：

```
omnicc -secure_comm -configure_for_dr <hostname_of_client being_recovered>
```

4. 联机恢复客户机之后，在 Cell Manager 上运行以下命令：
   ```
   omnicc -secure_comm -configure_peer <client_host_name> -overwrite
   ```
5. 执行灾难恢复测试计划。
6. 在 Windows 系统上，如果在系统启动后某些服务或驱动程序无法运行，则可能需要手动编辑 `kb.cfg` 文件。

创建一键式灾难恢复的备份规范

必须创建一键式灾难恢复 (OBDR) 备份规范，才能准备好 OBDR 引导磁带。

先决条件

- 添加 OBDR 设备前，为 DDS 或 LTO 介质创建一个采用不可追加介质使用策略和宽松介质分配策略的介质池。必须选择所创建的该介质池作为 OBDR 设备的默认介质池。
- 此设备必须在本地连接到要允许使用 OBDR 进行恢复的系统。
- 在要允许使用 OBDR 方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复和用户界面组件。
- 必须在要允许使用 OBDR 进行恢复的系统上本地创建备份规范。

> **提示：**
> 为了能够使用 OBDR 方法自动还原 MS 群集中的所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点。实际上无法收集足够的信息为由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

限制

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。

此备份规范属一键式灾难恢复方法所独有。默认情况下，会将必需卷备份为文件系统。但是，在 Windows Vista 和更高版本中，您可以选择通过 VSS 写入程序将逻辑卷备份为磁盘映像。这可确保卷在备份过程中保持未锁定状态，可以由其他应用程序访问。要将逻辑卷备份为磁盘映像，必须修改为 OBDR 创建的备份规范。

创建 OBDR 的备份规范

修改 OBDR 备份规范以使用磁盘映像备份

创建 **OBDR** 的备份规范

步骤

1. 在 Data Protector 上下文列表中，单击**备份**。
2. 在范围窗格中，单击**任务**，然后单击**一键式灾难恢复向导**。
3. 在“结果区域”中，从下拉列表中选择要为其执行 OBDR 备份(在客户机上本地)的客户机，然后单击**下一步**。
4. 此时已选择需要备份的关键卷。单击**下一步 (Next)**。

> **重要：**
> 重要卷由系统自动选择，并无法取消选择。选择要保留的任何其他分区，因为在恢复过程中 Data Protector 将从系统中删除所有分区。

5. 选择要用于备份的本地设备或驱动器。只能选择一个设备或驱动器。单击**下一步 (Next)**。
6. **Windows Vista 或更高版本：**

   查看并修改(如果需要)插入 DR OS 映像中的驱动程序的列表。

   可以使用此选项将缺少的驱动程序添加到 DR ISO 映像中。通过单击**添加**或**删除**，手动添加或删除驱动程序。要重新加载原始驱动程序，请单击**重新加载**。恢复集的 %Drivers% 部分中的驱动程序将自动插入 DR OS 映像中。

   (可选)选择备份选项。

   > **重要：**
   > 在备份过程中收集且存储在恢复集的 %Drivers% 目录中的驱动程序可能并不总是适合在 DR OS 中使用。在某些情况下，可能需要添加 Windows 预安装环境 (WinPE) 所特有的驱动程序才能确保恢复期间硬件能正常工作。

   Linux：选择备份选项。有关可用选项的更多详细信息，请参见《*Data Protector 帮助*》的索引："备份选项"。

   单击**下一步 (Next)**。
7. (可选)安排备份。单击**下一步 (Next)**。
8. 在"备份摘要"页中，查看备份规范设置，然后单击**下一步**。

   无法更改以前选择的备份设备或备份规范相互之间的先后顺序。仅可删除 OBDR 非必需备份对象，并且只能查看常规对象属性。也可以更改备份对象说明。
9. 将经过修改的备份规范保存为 OBDR 备份规范，以使其成为原始的一键式灾难恢复格式。也可以选择使用**保存并计划**选项来计划备份。
10. a. 单击"启动备份"以交互方式运行备份。此时将显示"启动备份"对话框。单击"确定"开始备份。

    如果备份为加密备份，则 omnisrdupdate 实用程序将自动导出加密 ID，此操作作为 post-exec 命令执行。

系统的可引导映像文件(包含安装和配置临时 DR OS 所需的所有信息)将写在磁带的开头，以使其可引导。

> **重要：重要说明：**每次硬件、软件或配置更改之后执行新的备份并准备好可引导的备份介质。这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

修改 OBDR 备份规范以使用磁盘映像备份

步骤

1. 在范围窗格中，单击已创建的 OBDR 备份规范。当系统询问您是否要将其视为 OBDR 备份规范或视为普通的备份规范，单击**否**。

> **注意：**
> 当将一个 OBDR 备份规范保存为普通备份规范之后，该备份规范仍然可以用于 OBDR。

2. 在“备份对象摘要”页面中，选择要将其备份为磁盘映像的逻辑卷，然后单击**删除**。

> **注意：**
> 只能备份逻辑卷。应使用文件系统备份来对配置对象、未装载或装载为 NTFS 文件夹的卷执行备份。

3. 单击**手动添加**以打开向导。
4. 在“选择备份对象”页中，单击**磁盘映像对象**选项，然后单击**下一步**。
5. 在“常规选择”页中，选择要用磁盘映像进行备份的客户机，并提供相应的描述信息。单击**下一步 (Next)**。

> **注意：**
> 对于每个磁盘映像对象，描述信息必须是唯一的。使用一个描述性名称，例如 `[Disk Image C] for C: volume`。

6. 在“常规对象选项”属性页中，将数据保护设置为**无**。单击**下一步 (Next)**。

> **注意：**
> 当将数据保护功能设置为**无**时，磁带内容可由更新的 OBDR 备份覆盖。

7. 在“高级对象选项”属性页中，可以指定磁盘映像对象的高级备份选项。单击**下一步 (Next)**。
8. 在“磁盘映像对象选项”属性页中，指定磁盘映像中要备份的部分。使用以下格式：

   `\\.\DriveLetter:`，例如：`\\.\E:`

> **注意：**
> 当卷的名称被指定为驱动器号时，不会在备份过程中锁定该卷。未装载或作为 NTFS 文件夹装载的卷无法用于磁盘映像备份。

9. 单击**完成**退出向导。
10. 在“备份对象摘要”页中，检查备份规范的摘要。指定为磁盘映像的逻辑卷应属于“磁盘映像”类型。单击**应用**。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。 对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。 在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 *Data_Protector_program_data*\Config\Server\export\keys\DR-*ClientName*-keys.csv(Windows 系统)或 /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv(UNIX 系统)，其中 *ClientName* 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

使用一键式灾难恢复恢复 Windows 系统

只有完成了所有准备步骤后，才能成功执行 Windows 系统的一键式灾难恢复 (OBDR)。

有关 OBDR 所支持的操作系统的详细信息，请参见《Data Protector 产品声明、软件说明和参考》。

先决条件

- 需要用新硬盘更换受影响的磁盘。
- 应有一个可引导 OBDR 备份介质，其中含有要恢复的客户机的所有关键对象。必须在客户机上本地执行 OBDR 备份。
- 需要一个在本地连接到目标系统的 OBDR 设备。

步骤

阶段 1

1. 除非要执行脱机灾难恢复，否则根据目标系统的操作系统，要向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的帐户：

   Windows Vista 和更高版本：

   - 类型：Windows
   - 名称:SYSTEM
   - 组/域：NT AUTHORITY
   - 客户机：正在恢复的系统的临时主机名

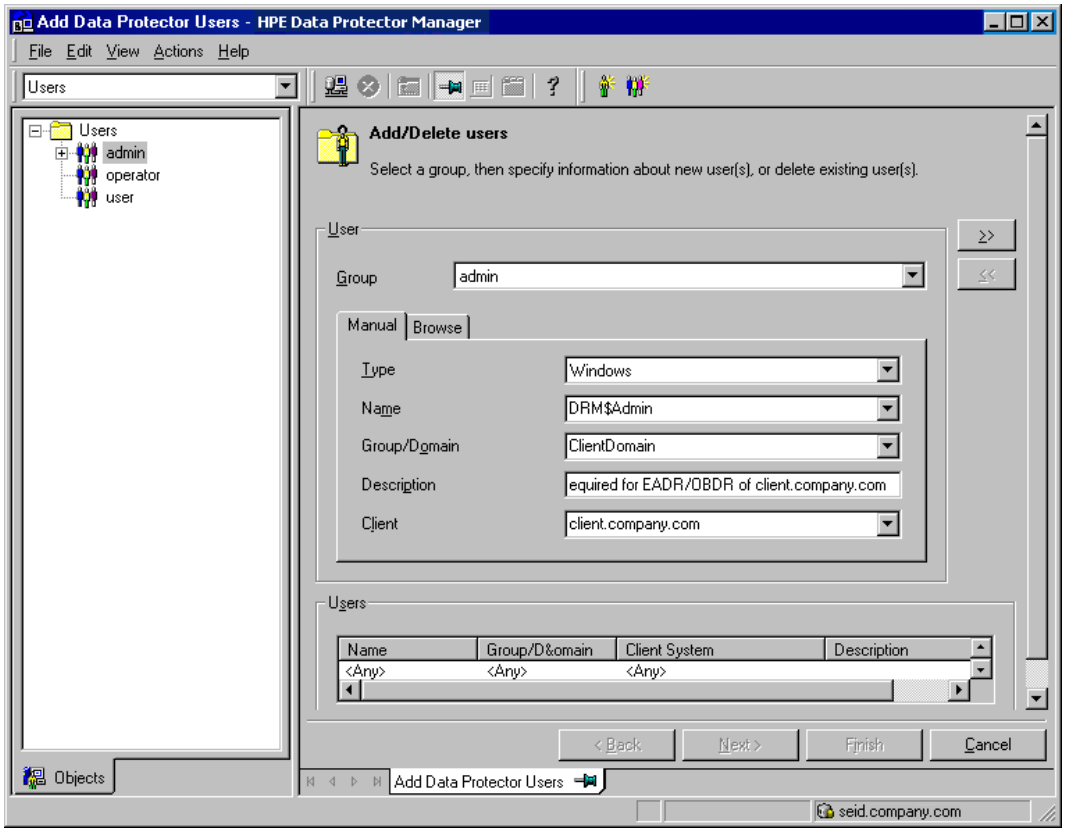
     Windows 预安装环境 (WinPE) 向系统分配了临时主机名。通过在 WinPE 的命令提示符窗口中运行 hostname 命令，可以检索该主机名。

   Windows XP、Windows Server 2003：

   - 类型：Windows
   - 名称:DRM$Admin
   - 组/域：目标系统的主机名
   - 客户机：目标系统的完全限定域名 (FQDN)

   有关添加用户的详细信息，请参见 Data Protector 帮助索引：“添加 Data Protector 用户”。

   添加用户帐户



2. 将包含映像文件和备份数据的磁带插入 OBDR 设备中。
3. 关闭目标系统，并关闭磁带设备的电源。在启动恢复过程之前，确保没有外置 USB 磁盘(包括 USB 闪存)连接到系统。
4. 打开目标系统的电源，并在其初始化时，按磁带设备上的**弹出**按钮，并打开该设备的电源。有关详细信息，请参见设备文档。
5. 选择恢复范围和恢复选项。下面的步骤将随操作系统的不同而不同：

   Windows Vista 和更高版本：

   a. 灾难恢复 GUI(安装程序向导)出现，并显示原始系统信息。单击**下一步 (Next)**。

   > **提示：**
   > 当显示进度条时，系统会提供一些键盘选项。可以通过将鼠标悬停在进度条上来检查可用的选项及其说明信息。

   b. 在“恢复范围”页面上，选择恢复的范围：

   - `Default Recovery`：恢复关键卷(系统磁盘、引导磁盘和 Data Protector 安装卷)。对所有其他磁盘进行分区和格式化，并使其保持空白，为阶段 3 做好准备。
   - `Minimal Recovery`：仅恢复系统磁盘和引导磁盘。
   - `Full Recovery`：恢复“还原集”中的所有卷，而不是仅恢复关键卷。
   - `Full with Shared Volumes`：对 Microsoft 群集服务器 (MSCS) 可用。如果 MSCS 中的所有节点都受到灾难的打击，并且要执行第一个节点的 EADR，则应使用此选项。它将恢复“还原集”中的所有卷，其中包括备份时由备份节点锁定的群集共享卷。如果至少一个节点活动并且正在运行 MSCS 服务，则将不还原共享卷，因为节点将锁定这些共享卷。在这种情况下，应使用 `Default Recovery`。

c. (可选)要修改恢复设置，请单击**设置**以打开“恢复设置”页面。

系统提供了以下其他一些恢复选项，其中一些选项需在灾难恢复未结束或需执行其他步骤时使用：

- Use original network settings：如果需要还原原始网络配置(例如，由于缺少 DHCP 服务器)，可选择此选项。默认设置下未选中该选项，并且 DR OS 恢复环境会使用 DHCP 网络配置。
- Restore BCD：如果选择此选项，则 Data Protector 在灾难还原会话期间还会提前还原引导配置数据 (BCD) 存储，然后在 Data Protector 还原会话中再还原该存储。默认情况下选择此选项。
- Restore DAT：如果选中，Data Protector 灾难恢复模块还将还原 Microsoft VSS 写入程序的数据。默认设置下，DR 模块会跳过 VSS 写入程序数据的还原。如果在非 VSS 备份期间， Data Protector 无法备份关键写入程序，您可使用该选项。要在 DR 模块还原之前还原数据，可选择 Pre。要在 Data Protector 之后还原数据，可选择 Post。
- Initialize Disks Manually：使用此选项可以手动映射原始系统磁盘和当前系统磁盘，并对它们进行初始化以使其与原始配置匹配。默认情况下，不选择此选项。

  如果选择了此选项，在恢复过程启动时将显示新的磁盘映射和初始化页面。灾难恢复模块将提供初始磁盘映射并显示初始映射尝试的结果。使用提供的选项更改磁盘映射。映射完成后，卷得到初始化并且系统将重新启动。
- Restore Storage Spaces：默认情况下，将还原存储空间。在恢复时，如果存储配置允许，您可以取消选项该选项并将虚拟磁盘直接还原为物理磁盘。请注意，如果要将存储空间还原为不同的硬件或 USB 磁盘，则需要手动对磁盘进行初始化。
- Enable Dissimilar Hardware Restore：如果启用，Data Protector将在恢复过程中扫描系统中缺少的驱动程序。可通过从下拉列表中选择下列方法之一来启用该选项：
  - Unattend默认此模式使用预定义的配置文件自动将操作系统配置到不同的硬件平台中。对于不同的硬件，这是主要的恢复模式。请在第一个实例中使用。
  - Generic：如果无人参与模式失败(可能是因为所还原的操作系统的配置不正确)，可选择此项。它将调整所还原的操作系统注册表及其驱动程序和服务，以适应不同的硬件。
- Remove Devices：在启用了 Dissimilar Hardware 选项时可用。如果选中，Data Protector将从还原的操作系统的注册表中删除原始设备。
- Connect iSCSI Devices：如果原始计算机正在使用 iSCSI，则会启用该选项。通过选择该选项，Data Protector 可在备份时自动还原基本 iSCSI 配置。如果未选中，将跳过 iSCSI 配置。

  您也可使用本机 Microsoft iSCSI 配置向导来管理更为复杂的 iSCSI 配置。如果 DR GUI 检测到某些 iSCSI 功能(例如安全选项)需要手动配置，则会提供选项来运行 Microsoft iSCSI 配置向导。
- Map Cluster Disks Manually：在 Windows Server 2008 及更高版本上可用。如果选择此选项，您可以手动映射群集卷。如果不选择此选项，将自动映射卷。在执行自动映射后，建议检查所有卷是否已正确映射。
- Remove Boot Descriptor：在 Intel Itanium 系统中可用。删除由灾难恢复过程留

下的所有引导描述符。

- Manual disk selection：在 Intel Itanium 系统中可用。如果磁盘设置显著变化，则灾难恢复模块可能找不到引导磁盘。使用此选项可选择正确的引导磁盘。

要将选项重置为默认设置，请单击**重置默认设置**。

单击**保存 >** 以保存更改。

d. 恢复过程开始，并且您可以监视进度。

如果已使用 BitLocker 驱动器加密对卷进行了加密，则系统将提示您解锁已加密的驱动器。

> **提示：**
> 在灾难恢复 GUI 中，可以单击**任务**执行以下操作：
> - 运行命令提示符、任务管理器或磁盘管理器
> - 访问 Map Network Drives 和 Load Drivers 工具
> - 查看特定于灾难恢复过程的日志文件
> - 启用或禁用 DRM 配置文件，以及在文本编辑器中查看和编辑该文件
> - 编辑 WinPE 恢复环境的 hosts 文件
> - 访问“帮助”和查看 GUI 图标图例

Windows XP、Windows Server 2003：

a. 显示以下消息时按 **F12**：To start recovery of the machine HOSTNAME press F12。

b. 在引导过程开始时将显示范围选择菜单。选择恢复的范围，然后按 **Enter**。有 5 种不同的恢复范围：

- Reboot：不执行灾难恢复，但重新启动系统。
- Default Recovery：恢复关键卷(系统磁盘、引导磁盘和 OBInstall 卷)。对所有其他磁盘进行分区和格式化，并使其保持空白，为阶段 3 做好准备。
- Minimal Recovery：仅恢复系统磁盘和引导磁盘。
- Full Recovery：恢复“还原集”中的所有卷，而不是仅恢复关键卷。
- Full with Shared Volumes：对 Microsoft 群集服务器 (MSCS) 可用。如果 MSCS 中的所有节点都受到灾难的打击，并且要执行第一个节点的 OBDR，则应使用此选项。它将恢复“还原集”中的所有卷，其中包括备份时由备份节点锁定的群集共享卷。如果至少一个节点活动并且正在运行 MSCS 服务，则将不还原共享卷，因为节点将锁定这些共享卷。在这种情况下，应使用 Default Recovery。

系统提供了以下其他一些恢复选项，其中一些选项需在灾难恢复未结束或需执行其他步骤时使用：

- Remove Boot Descriptor：在 Intel Itanium 系统中可用。删除由灾难恢复过程留下的所有引导描述符。
- Manual disk selection：在 Intel Itanium 系统中可用。如果磁盘设置显著变化，则灾难恢复模块可能找不到引导磁盘。使用此选项可选择正确的引导磁盘。

阶段 2

6. 选择了恢复的范围之后，Data Protector 开始直接将 DR OS 安装到硬盘。可以监视进度，而在安装 DR OS 后将重新启动系统。如果 DR OS 无法正常引导或无法访问网

络，则可能需要编辑 kb.cfg 文件。在 Windows Vista 和更高版本中，不安装 DR OS，并且不执行系统重新启动。

7. 如果灾难恢复备份已加密，并且要恢复其 Cell Manager 无法访问的客户机，将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库 (DR-*ClientName*-keys.csv)(例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器)，并输入密钥库文件的完整路径。密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。现在将继续进行灾难恢复，不会再有其他中断现象。

8. 如果 SRD 文件中的信息并非最新(例如因为灾难之后更改了备份设备)，并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
9. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。第一次登录之后将删除临时 DR OS，但以下情况除外：
   - `Minimal Recovery` 处于选定状态。
   - 灾难恢复向导在备份介质上找到 DR 安装和 SRD 文件之后的 10 秒暂停期间中断了灾难恢复向导，并且选择了**调试**选项。
   - 您手动执行带有 `omnidr` 或 `-no_reset` 选项的 `-debug` 命令。
   - 灾难恢复失败。

   注意，Data Protector 将首先尝试执行联机还原。如果联机还原因任何原因而失败(如 Cell Manager 或网络服务不可用，或防火墙正在阻止访问 Cell Manager)，则 Data Protector 将尝试执行远程脱机恢复。如果远程脱机还原失败(如因为介质代理主机仅接受来自 Cell Manager 的请求)，则 Data Protector 将执行本地脱机还原。
10. 从 Cell Manager 上的 Data Protector `admin` 用户组中删除在第 1 步创建的客户机的本地 Administrator 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。

阶段 3

12. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

    > **注意：**
    > Data Protector 在恢复之后不会还原卷压缩标志。备份时压缩的所有文件将还原为压缩形式，但如果还希望压缩任何新文件，则必须手动设置卷压缩。

13. 如果要执行 Microsoft 群集服务器中所有节点的灾难恢复，则需要其他步骤。

高级任务

Microsoft 群集服务器的灾难恢复

关于 Microsoft 群集服务器的灾难恢复

可以使用除了磁盘查递灾难恢复之外的任何灾难恢复方法恢复 Microsoft 群集服务器 (MSCS)。 有关特定灾难恢复方法的所有详情、限制和要求也适用于 MSCS 的灾难恢复。 选择适于群集的灾难恢复方法，并将其包括在灾难恢复计划中。 请考虑每个灾难恢复方法的限制和要求，然后再做决定。 从测试计划中执行测试。

有关受支持操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

必须符合灾难恢复的所有先决条件(例如一致和最新的备份、经过更新的 SRD 文件、更换了故障硬件等等)才能恢复 MSCS。

可能出现的场景

MSCS 的灾难恢复有两种可能出现的场景：

- 非活动节点上发生的灾难
- 群集中的所有节点都经历了灾难

为 Microsoft 群集服务器灾难恢复所做准备的详情

必须符合灾难恢复的所有先决条件(如一致和最新的备份映像、经过更新的 SRD 文件、更换了故障硬件等等)才能恢复 Microsoft 群集服务器 (MSCS)。 有关特定灾难恢复方法的所有详情、限制和要求还适用于 MSCS 的灾难恢复。

MSCS 的一致备份映像包括：

- 所有节点
- 虚拟服务器
- 如果将 Data Protector 配置为群集感知应用程序，则 Cell Manager 应包括在备份规范中

EADR 详情

实际上无法收集足够的信息为备份期间由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。 需要此信息才能还原所有共享群集卷。 要在群集中所有节点的 P1S 文件中都包括有关共享群集卷的信息，请执行以下操作之一：

- 执行客户机完整备份之后，合并群集中所有节点的 P1S 文件中有关共享群集卷的信息，以使每个节点的 P1S 文件都包含有关共享群集卷配置的信息。
- 将所有共享群集卷临时移至将备份的节点上。 此方式可收集有关所有共享群集卷的所有必要信息，但只有该节点可以作为主节点。

OBDR 详情

要更快还原，请使用 omnisrdupdate 命令作为 post-exec 命令，在 OBDR 备份之后更新 SRD 文件。 执行 OBDR 时在软盘驱动器中插入具有经过更新的 SRD 文件的磁盘，以向 Data Protector 告知备份对象在磁带上的位置。 还原 MSCS 数据库将更快，因为 Data Protector 不会在磁带中搜索 MSCS 数据库的位置。

为了能够自动还原 MSCS 中的所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点。 无法收集足够的信息为备份期间由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

恢复 Microsoft 群集服务器

Microsoft 群集服务器 (MSCS) 的灾难恢复有两种可能的场景：

至少有一个节点正常运行

群集中的所有节点都经历了灾难

至少有一个节点正常运行

这是 MSCS 灾难恢复的基本场景。 除了灾难恢复的其他先决条件以外，还必须满足以下先决条件。

先决条件

- 至少有一个群集节点正常运行(活动节点)。
- 此节点上正在运行群集服务。
- 所有物理磁盘资源都必须联机(即，由群集拥有)。
- 具有所有正常的群集功能(群集管理组联机)。
- Cell Manager 处于联机状态。

在这种情况下，群集节点的灾难恢复与 Data Protector 客户机的灾难恢复步骤相同。 应遵照将用于还原受影响的非活动节点的特定灾难恢复方法的说明。

仅还原本地磁盘，因为灾难之后将所有共享磁盘都移至正常运行的节点并锁定。

恢复辅助节点之后，该节点将在引导后加入群集。

恢复所有节点并且这些节点加入群集之后，可以还原 MSCS 数据库以确保其一致性。 MSCS 数据库是 Windows 系统中 CONFIGURATION 对象的一部分。

群集中的所有节点都经历了灾难

在这种情况下，MSCS 中的所有节点都不可用，并且未运行群集服务。

除了灾难恢复的其他先决条件以外，还必须满足以下先决条件。

先决条件

- 主节点必须对仲裁磁盘具有写访问权限(不得锁定仲裁磁盘)。
- 恢复 Cell Manager 时，主节点必须对所有 IDB 卷都具有访问权限。

在这种情况下，必须首先还原含有仲裁磁盘的主节点。 如果已在群集中安装了 Cell Manager，则还必须还原 IDB。 (可选)可以还原 MSCS 数据库。 还原主节点之后，可以还原所有剩余的节点。

对于 AMDR，MSCS 服务使用写入每个硬盘的 MBR 中的硬盘签名识别物理磁盘。 如果已更换共享群集磁盘，则这意味着在灾难恢复的阶段 1 期间更改了磁盘签名。 因此，MSCS 服务无法将更换的磁盘识别为有效的群集资源，并且依赖于这些资源的群集组将失败。 要防止出现这种情况，请在更换了共享群集磁盘的情况下还原原始硬盘签名。

步骤

1. 执行主节点(包括仲裁磁盘)的灾难恢复。

   辅助手动灾难恢复 (AMDR)：

   `drstart -full_clus` 命令将自动还原仲裁磁盘上的所有用户和应用程序数据。

   增强型自动灾难恢复 (EADR)、一键式灾难恢复 (OBDR)：

   当系统要求您选择恢复的范围时，请选择**完整(含共享卷)**以还原仲裁磁盘。
2. 重新启动系统。
3. 还原 MSCS 数据库，此数据库是 Windows 系统中 CONFIGURATION 对象的一部分。 MSCS 服务必须正在运行才能还原 MSCS 数据库，因此无法在灾难恢复的阶段 2 期间自动还原该数据库。 但是，可以在阶段 2 结束时使用标准 Data Protector 还原过程手动还原群集数据库。
4. **除一键式灾难恢复 (OBDR) 之外的方法：**

   如果要恢复 Cell Manager，则要使 IDB 一致。
5. 还原仲裁和 IDB 卷。 如果所有其他卷未损坏，则这些卷将保留原样并由所恢复的主节点占用。 如果这些卷已损坏，则必须执行以下步骤：
   a. 禁用群集服务和群集磁盘驱动程序(MSDN Q176970 中所述的步骤)。
   b. 重新启动系统。
   c. 重建以前的存储结构。
   d. 启用群集磁盘驱动程序和群集服务。
   e. 重新启动系统，并还原用户和应用程序数据。
6. 还原剩余的节点。

合并 Microsoft 群集服务器的 P1S 文件

执行备份之后，增强型自动灾难恢复 (EADR) 还需要另一个步骤才能还原活动节点。 必须合并 Microsoft 群集服务器 (MSCS) 中所有节点的 P1S 文件中有关共享群集卷的信息，以使每个节点的 P1S 文件都包含有关共享群集卷配置的信息。 需要这些信息才能还原所有共享群集卷。 通过将所有共享群集卷临时移至将备份的节点，可以避免在备份之后合并 P1S 文件。 在这种情况下，可以收集有关所有共享群集卷的所有必要信息。 这意味着只有该节点可以作为主节点。

Windows

要合并所有节点的 P1S 文件，请从 *Data_Protector_home*\bin\drim\bin 目录中执行 merge.exe 命令：

merge *p1sA_path ... p1sX_path*

其中 p1sA 是第一个节点的 P1S 文件的完整路径，p1sX 是 MSCS 中上一个节点的 P1S 文件的完整路径。

经过更新的 P1S 文件的文件名结尾追加了 .merged(例如，computer.company.com.merged)。将合并的 P1S 文件重命名为其原始名称(删除 .merged 扩展名)。

例如，要合并具有 2 个节点的 MSCS 中的 P1S 文件，请键入：

merge *Data_Protector_program_data*\Config\server\dr\p1s\node1.company.com *Data_Protector_program_data*\Config\server\dr\p1s\node2.company.com.

合并后的文件将为 node1.company.com.merged 和 node2.company.com.merged。

UNIX

merge.exe 命令仅适用于装有 Data Protector 自动灾难恢复组件的 Windows 系统。 在 UNIX Cell Manager 上，执行以下步骤。

步骤

1. 将 P1S 文件复制到装有自动灾难恢复组件的 Windows 客户机上。
2. 合并这些文件。
3. 将合并后的 P1S 文件重命名为其原始名称。
4. 将合并后的 P1S 文件复制回 UNIX Cell Manager。

在 Windows 系统中还原原始硬盘签名

Microsoft 群集服务器 (MSCS) 服务使用写入每个硬盘的 MBR 中的硬盘签名识别物理磁盘。如果已更换共享群集磁盘，则这意味着在灾难恢复的阶段 1 期间更改了磁盘签名。 因此，群集服务无法将更换的磁盘识别为有效的群集资源，并且依赖于这些资源的群集组将失败。 这一点仅适用于活动节点的还原(即，如果群集中的所有节点都遇到灾难)，因为只要有至少一个节点正常运行，并占有资源的所有权，共享群集资源即可使用。 此问题不适用于 EADR 和 OBDR 关键磁盘，因为将自动恢复所有 EADR 和 OBDR 关键磁盘的原始磁盘签名。 如果更换了任何其他磁盘，则还必须还原其硬盘签名。

最关键的共享磁盘是群集仲裁资源。 如果已将其更换，则必须还原原始磁盘签名，否则将无法启动群集服务。 阶段 2 期间，MSCS 数据库将还原到系统卷上的 \TEMP\ClusterDatabase 目录中。 重新引导系统之后，群集服务将不运行，因为在阶段 1 中更改了硬盘签名而无法识别仲裁资源。

在 Windows 中还原原始硬盘签名

在 Windows 系统中，可以通过运行 clubar实用程序(位于 *Data_Protector_home*\bin\utilns 中)来解决此问题。该实用程序将还原原来的硬盘签名。 clubar 成功完成之后，将自动启

动群集服务。

例如，要从 C:\temp\ClusterDatabase 还原 MSCS 数据库，请在命令提示符下键入：

```
clubar r C:\temp\ClusterDatabase force q:.
```

有关 clubar 的用法和语法的详细信息，请参见 *Data_Protector_home*\bin\utilns 中的 clubar.txt 文件。

如果 Cell Manager 上的 Data Protector 共享磁盘与仲裁磁盘不同，则还必须还原该共享磁盘。 要还原 Data Protector 共享磁盘和任何其他应用程序磁盘的签名，应使用 Windows 资源工具包中包括的 dumpcfg 实用程序。 有关使用 dumpcfg 的详细信息，请运行 dumpcfg /? 或参见 Windows 资源工具包文档。 有关 Windows 系统中硬盘签名问题的详细信息，请参见 MSDN 文章 Q280425。

获取原始硬盘签名

可以从 SRD 文件获取原始硬盘签名。 签名是 SRD 文件中跟随在 -volume 关键字之后的数字。

仲裁磁盘的签名仅存储在活动节点的 SRD 文件中(备份时)，因为它使仲裁磁盘处于锁定状态，并因此阻止其他节点访问仲裁磁盘。 因此建议始终备份整个群集，因为需要群集中所有节点的 SRD 文件，只有所有 SRD 文件集中在一起所包括的信息才足以在阶段 1 中配置共享磁盘卷的磁盘。 请注意，将 SRD 文件中存储的硬盘签名表示为十进制数，而 dumpcfg 需要十六进制值。

SRD 文件中硬盘签名的示例

可以从 SRD 文件获取原始硬盘签名。 签名是 SRD 文件中跟随在 -volume 关键字之后的数字。 以下是 SRD 文件中硬盘签名的示例：

```
-volume 5666415943 -number 0 -letter C -offslow 32256 -offshigh 0 -lenlow 320430592
-lenhigh 2 -fttype 4 -ftgroup 0 -ftmember 0

-volume 3927615943 -number 0 -letter Q -offslow 320495104 -offshigh 2 -lenlow
1339236864 -lenhigh 0 -fttype 4 -ftgroup 0 -ftmember 0
```

跟随在 -volume 关键字后的数字就是硬盘的签名。 在这种情况下，SRD 文件存储有关本地硬盘(使用驱动器号盘符 C)和仲裁磁盘(使用驱动器盘符 Q)的信息。

还原 Data Protector Cell Manager 详情

本节将介绍还原 Windows Cell Manager 时应该执行的特定方法的其他步骤。

使 IDB 一致(所有恢复方法)

仅在执行常规灾难恢复过程后才应使用本节所述的过程。

要使 IDB 一致，请导入含有上一个备份的介质，以便将有关备份对象的信息导入 IDB。 为此，请执行以下步骤：

1. 使用 Data Protector GUI，回收包含仍有待还原的卷的备份的介质，以便能够将该介质导入 IDB。 有关回收介质的详细信息，请参见《Data Protector 帮助》的索引："回收介

质”。

有时，因为 Data Protector 锁定介质而导致无法回收。 在这种情况下，请停止 Data Protector 进程，然后通过执行以下命令删除 \tmp 目录：

a. `omnisv -stop`
b. `del Data_Protector_program_data\tmp\*.*`
c. `omnisv -start`

2. 使用 Data Protector GUI，导出包含仍有待还原的卷的备份的介质。 有关导出介质的详细信息，请参见《Data Protector 帮助》的索引：“导出, 介质”。
3. 使用 Data Protector GUI，导入包含仍有待还原的分区的备份的介质。 有关导入介质的详细信息，请参见《Data Protector 帮助》的索引：“导入, 介质”。

增强的自动灾难恢复细节

如果使用增强的自动灾难恢复方法恢复 Windows Cell Manager，则需要在阶段 0 中执行两个额外的步骤：

- 应提前准备包含 Cell Manager 的 DR OS 映像或可引导网络映像的灾难恢复 CD 或 USB 驱动器。

  重要：
  每次硬件、软件或配置更改之后执行新的备份并准备新的 DR OS 映像。 这一点也适用于任何网络更改，如 IP 地址或 DNS 服务器的更改。

- 作为灾难恢复准备策略的一部分，除了 Cell Manager 之外，还应将 Cell Manager 经过更新的 SRD 文件保存在多个安全的位置，因为当 IDB 不可用时，SRD 文件是唯一一个存储对象和介质相关信息的 Data Protector 文件。 如果 SRD 文件仅保存在 Cell Manager 上，则当 Cell Manager 发生故障时将无法访问该文件。 请参见“准备”(第 27 页)。
- 如果备份已加密，则必须在灾难发生之前，将加密密钥保存到可移动介质。 如果加密密钥仅保存在 Cell Manager 上，则当 Cell Manager 发生故障时将无法访问该加密密钥。 没有加密密钥便无法执行灾难恢复。 请参见“准备”(第 27 页)。

重要：
Micro Focus 建议限制对备份介质、恢复集文件、SRD 文件、包含加密密钥的可移动介质、灾难恢复 CD 以及存储 DR OS 数据的 USB 驱动器的访问。

还原 Internet Information Server 详情

灾难恢复不支持 Internet Information Server (IIS)。 要恢复 IIS，必须满足以下要求(除了辅助手动灾难恢复所需的要求以外)：

要求

- 不要在全新安装系统期间安装 IIS。

执行以下步骤(除了辅助手动灾难恢复所需的步骤以外)：

步骤

1. 如果正在运行 IIS 管理服务，则停止或卸载该服务。
2. 运行 drstart 命令。

IIS 数据库以纯文本文件(文件名为 DisasterRecovery)形式还原到默认 IIS 位置 (*%SystemRoot%*\system32\inetsrv)。

成功引导之后，使用标准 Data Protector 还原过程或“IIS 备份/还原”管理单元还原 IIS 数据库。注意，这可能需要使用相当长的时间。

编辑 kb.cfg 文件

kb.cfg 文件位于 *Data_Protector_home*\bin\drim\config 目录中，用于存储 *%SystemRoot%* 目录中的驱动程序文件的位置信息。此文件的用途是提供一种灵活的方法，使 Data Protector 可以在 DR OS 中包括驱动程序(和其他需要的文件)，以使系统采用与引导相关的特定硬件或应用程序配置。默认的 kb.cfg 文件已包含行业标准硬件配置所需的所有文件。

例如，某些驱动程序的功能分散到多个单独的文件中，驱动程序需要所有这些文件才能正常工作。有时，如果未在 kb.cfg 文件中逐个列出所有驱动程序文件，则 Data Protector 无法识别这些驱动程序文件。在这种情况下，DR OS 中将不包括这些驱动程序文件。使用 kb.cfg 文件的默认版本创建和执行测试计划。如果 DR OS 无法正常不引导或无法访问网络，则可能需要修改此文件。

如果要备份这些驱动程序，则以适当的格式将相关文件的信息添加到 kb.cfg 文件中，如 kb.cfg 文件开始处的说明中所述。编辑文件的最简单方式是复制和粘贴现有行，并将其替换为相关信息。

注意，路径分隔符是“/”(正斜杠)。忽略空格，但引号中的路径名除外，因此相关条目可分散在多行中。还可以添加以“#”(磅)符号开始的注释行。

编辑 kb.cfg 文件完毕之后，将其保存到原始位置。然后，执行另一个客户机完整备份，将添加的文件包含在恢复集中。

> **重要：**
> 由于系统硬件和应用程序的配置任务繁重，因此无法为所有可能的配置提供“即用型”解决方案。因此可以修改此文件以包括驱动程序或其他文件，风险自担。
>
> 对此文件的任何修改都由您自己承担风险，这些修改本身不受 Micro Focus 支持。

> **警告：**
> 建议创建并执行测试计划，以确保编辑 kb.cfg 文件之后灾难恢复可正常运行。

编辑 SRD 文件

有关经过更新的 SRD 文件 (recovery.srd) 中存储的有关备份设备或介质的信息可能在执行灾难恢复时过期。如果要执行联机恢复，那么这不会产生问题，因为必要的信息存储在 Cell Manager 上的 IDB 中。但是，如果要执行脱机恢复，则无法访问 IDB 中存储的信息。

例如，灾难不仅打击 Cell Manager，而且还会打击与之相连的备份设备。如果灾难之后将该备份设备更换为不同的备份设备，则 SRD 文件中存储的信息将不正确，从而恢复将失

败。在这种情况下，先编辑经过更新的 SRD 文件，然后再执行灾难恢复的阶段 2，以更新错误信息，并因此使恢复得以成功。

要编辑 SRD 文件，请在文本编辑器中将其打开(有关 SRD 文件的位置，请参见下方特定方法的详情)，然后更新已更改的信息。

> **提示：**
> 可以使用 `devbra -dev` 命令显示设备配置信息。

例如，如果目标系统的客户机名称已更改，则替换 `-host` 选项的值。还可以编辑有关以下内容的信息：

- Cell Manager 客户机名称 (`-cm`)，
- 介质代理客户机 (`-mahost`)，
- 设备名称 (`-dev`)，
- 设备类型 (`-type`)，
- 地址 (`-devaddr`)，
- 策略 (`-devpolicy`)，
- 机械手 SCSI 地址 (`-devioctl`)
- 库插槽 (`-physloc`) 等。

编辑文件之后，以 Unicode (UTF-16) 格式将其保存到原始位置。

对于某些灾难恢复方法和操作系统而言，灾难恢复中对经编辑的 SRD 文件的使用方式将有所不同。下方介绍了特定灾难恢复方法的具体信息。

> **重要：**
> 出于安全原因，应限制对 SRD 文件的访问。

AMDR

EADR/OBDR

AMDR

如果 SRD 文件中的信息过时，则在执行定期 AMDR 恢复过程之前，执行以下步骤。

步骤

1. 在文本编辑器中打开 `recovery.srd` 文件(位于第一个 `drsetup/ASR` 软盘上)，并做出必要的更改。
2. 以 Unicode (UTF-16) 格式将文件保存到其原始位置。

EADR/OBDR

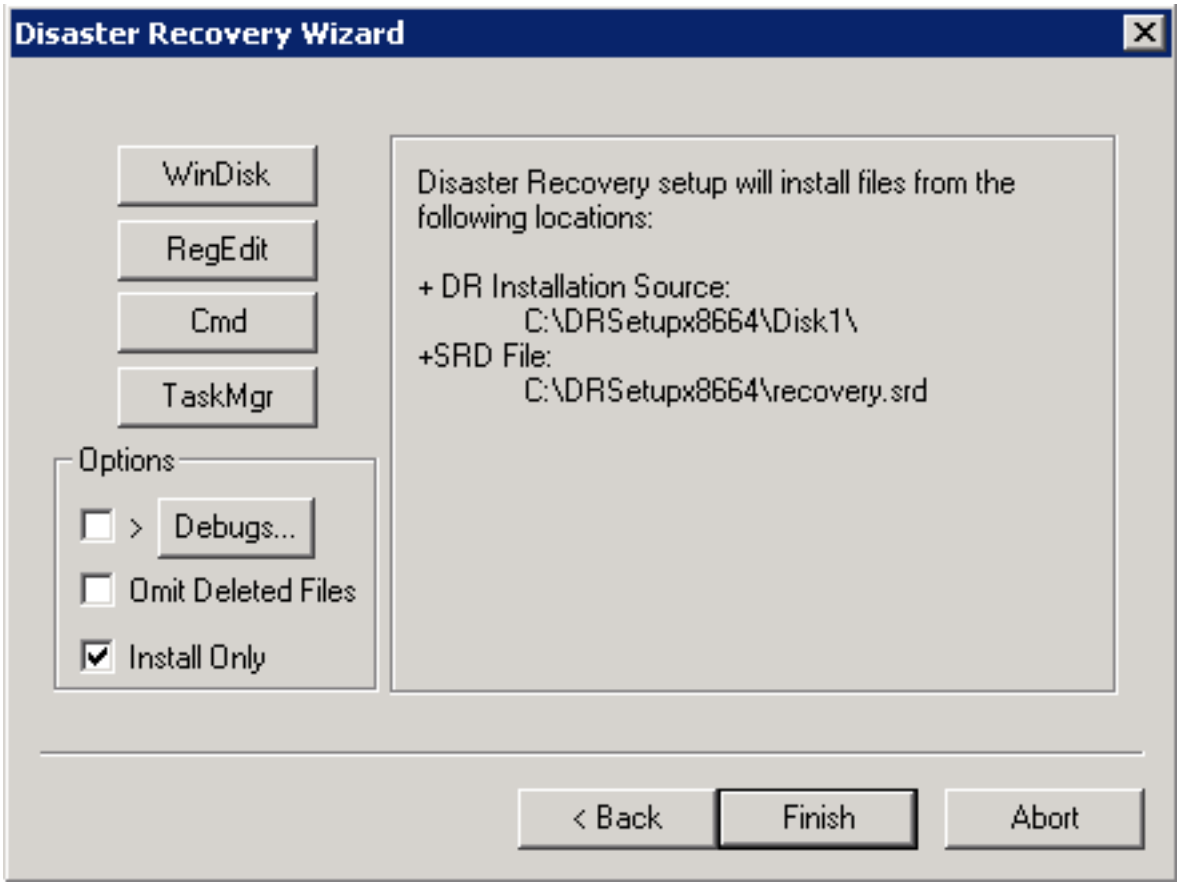
如果 SRD 文件中的信息过时，则在继续定期 EADR/OBDR 过程之前，执行以下其他步骤。

步骤

Windows 系统

1. 显示“灾难恢复向导”时，按任意键在倒数期间停止向导，选择**仅安装**选项，然后单击 Finish。此选项仅向目标系统安装临时操作系统，并因此结束灾难恢复的阶段 1。如果选择**仅安装**选项，则将不自动启动灾难恢复阶段 2。

   灾难恢复向导中的“仅安装”选项



2. 选择**忽略已删除的文件**选项。该选项可在还原时间删除连续增量备份期间删除的文件。如果指定，在进行增量备份时，omnidr 二进制文件会将同一选项转发给 Data Protector还原工具(omnir 和 omniofflr)。该选项对还原完整备份对象版本无效。但是，选择该选项可以大大延长还原的时间。
3. 运行 **Windows 任务管理器**(按 **Ctrl+Alt+Del**，然后选择**任务管理器**)。
4. 在 Windows 任务管理器中，单击**文件**，然后单击**新建任务(运行...)**。
5. 从“运行”对话框中运行以下命令：`notepad C:\DRSYS\System32\OB2DR\bin\recovery.srd` 然后按 **Enter**。此时将在记事本中打开 SRD 文件。
6. 编辑 SRD 文件。
7. 编辑 SRD 文件并将其保存到原始位置之后，从下列位置中运行以下命令 `C:\DRSYS\System32\OB2DR\bin`

```
omnidr -drimini C:\$DRIM$.OB2\OBRecovery.ini
```

8. 在定期 EADR/OBDR 恢复过程中继续下一个步骤。

Linux 系统

1. 显示“灾难恢复向导”时，按 **q** 键在倒数期间停止向导，然后选择**仅安装**选项。此选项仅会在目标系统中安装最低版本的 Data Protector。如果选择“仅安装”选项，则将不自动启动灾难恢复阶段 2。
2. 切换到另一个 shell。

   编辑 SRD 文件 `/opt/omni/bin/recovery.srd`。有关详细信息，请参见《*Data Protector 灾难恢复指南*》。
3. 在编辑并保存 SRD 文件后，执行：

   ```
   omnidr -srd recovery.srd -drimini /opt/omni/bin/drim/drecovery.ini
   ```
4. 在恢复过程完成后，返回之前的 shell 并执行普通 EADR/OBDR 恢复过程中的下一步。

编辑 SRD 文件的示例

如果 SRD 文件中的信息不再是最新的(例如更改了备份设备)，请修改更新的 SRD 文件 (`recovery.srd`)，然后再执行灾难恢复的阶段 2，以更新错误的信息并因此使恢复取得成功。

可以使用 `devbra -dev` 命令显示某些设备配置信息。

更改 MA 客户机

使用连接到客户机 `old_mahost.company.com` 的备份设备执行备份以用于灾难恢复。灾难恢复时，相同的备份设备连接到具有相同 SCSI 地址的客户机 `new_mahost.company.com`。要执行灾难恢复，请将经过更新的 SRD 文件中的 `-mahost old_mahost.company.com` 字符串替换为 `-mahost new_mahost.company.com`，然后再执行灾难恢复阶段 2。

如果备份设备在新 MA 客户机上的 SCSI 地址不同，则在经过更新的 SRD 文件中还要相应地修改 `-devaddr` 选项的值。

编辑文件之后，以 Unicode (UTF-16) 格式将其保存到原始位置。

更改备份设备

要使用备份设备之外的另一个设备执行灾难恢复，请在经过更新的 SRD 文件中修改以下选项值：

`-dev`、`-devaddr`、`-devtype`、`-devpolicy`、`-devioctl` 和 `-physloc`

其中：

`-dev`	指定要用于备份的备份设备或驱动器(库)的逻辑名称，
`-devaddr`	指定该设备的 SCSI 地址，
`-devtype`	指定 Data Protector 设备类型，

-devpolicy	指定设备策略，此策略可以定义为 1(独立设备)、3(堆栈器)、5(介质库)、6(外部控制)、8(Grau DAS 交换器库)、9(STK Silo 介质库)或 10 (SCSI-II 库)，
-devioctl	指定机械手 SCSI 地址。
-physloc	指定库插槽
-storname	指定逻辑库名称

例如，使用设备名称为 Ultrium_dagnja、连接到 MA 主机 dagnja(Windows 系统)的 Ultrium 独立设备执行了一次备份用于灾难恢复。 但是，对于灾难恢复，您喜欢使用逻辑库名称为 Autoldr_kerala、具有连接到 MA 客户机 kerala(Linux 系统)的驱动器 Ultrium_kerala 的 Ultrium 机械手库。

首先，在 kerala 上运行 devbra -dev 命令，以显示已配置设备及其配置信息的列表。 将需要此信息以替换经过更新的 SRD 文件中的以下选项值：

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13 -devpolicy 1 -mahost
dagnja.company.com
```

以及如下：

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13 -devpolicy 10 -devioctl
/dev/sg1 -physloc " 2 -1" -storname "AutoLdr_kerala" -mahost kerala.company.com.
```

编辑文件之后，以 Unicode (UTF-16) 格式将其保存到原始位置。

Windows BitLocker 驱动器加密

在 Windows Vista 及更高版本上的灾难恢复过程中，可以解锁使用 BitLocker Drive Encryption 加密的卷。

限制

如果不解除对特定卷的锁定或如果该卷损坏，则无法解除锁定，并且因此必须格式化，灾难恢复之后对该卷不再加密。 在这种环境下，需要再次对该卷进行加密。

请注意，还原系统卷时始终保持不加密状态。

步骤

1. 当灾难恢复模块检测到加密卷时，系统会提示您解锁它。
   单击**是**启动 Unlocker 向导。 请注意，如果单击**否**，加密的卷将保持锁定状态。
2. 在“选择锁定卷”页中，将列出检测到的加密卷。 选择要解锁的卷，然后单击**下一步**。
3. 在“解锁卷”页(每个选定卷一页)中，系统会要求您指定解锁方法。 可用的解锁方法如下：
   - *密码(在 Windows 7 及更高版本上可用)*
     在加密卷时所使用的字符串。

- 通行密码

  在加密卷时使用的长于通常密码的字符串。

- 恢复密钥

  在每个加密卷上创建的特殊隐藏密钥。恢复密钥具有 BEK 扩展名，保存在恢复密钥文本文件中。您可以单击**浏览**以找到恢复密钥文件。

在文本框中键入所请求的信息，然后单击**下一步**。

4. 检查卷是否已成功解锁，然后单击**完成**。

> **注意：**
> 如果解锁过程失败，可以查看错误信息，然后重试或跳过解锁过程。

恢复到不同的硬件

> **注意：**
> 恢复到不同的硬件是对增强的自动灾难恢复的扩展。您需参考该信息和此处的信息。

发生硬件故障或类似灾难后，您可能需要将备份还原到部分或所有硬件不同于原始硬件的系统中(**不同硬件**)。

不同硬件还原将在标准 EADR 和 OBDR 步骤中增加以下步骤：

1. 在备份时，灾难恢复模块还会收集网络配置信息和硬件信息。
2. 该模块支持将关键设备驱动程序插入 DR OS 映像，以便在还原期间使用它们。如果缺少部分驱动程序，您还可以在还原时手动插入它们。
3. 在还原期间，使用网络和硬件信息为还原的 OS 配置和映射网络，并检测是否缺少关键硬件。

当可能需要对不同硬件进行还原时

- **硬件故障**

  当部分关键引导硬件(例如存储控制器、处理器或主板)发生故障并必须使用不同硬件替换时，需要执行不同硬件还原。

- **灾难**

  在发生以下绝对硬件灾难时需要执行不同硬件还原：

  ◦ 无法找到匹配的硬件(由于预算有限、故障硬件老化或其他原因)。

  ◦ 无法承受宕机时间带来的损失；系统必须立即投入正常运行。

  在这些情况下，采用不同硬件还原可能意味着更低的预算成本，因为不需要对原始系统进行精确克隆。

- **迁移**

  在以下情况下需要执行不同硬件还原：

- 当无法选择是否重新安装和重新配置 OS 时，需迁移到其他硬件(例如更快或更新的硬件)。
- 从物理系统迁移至虚拟环境或反之。

  从灾难恢复模块的角度而言，虚拟环境相当于另一个硬件平台，也需要为其提供关键驱动程序，以还原在某个其他虚拟或物理平台上所做的系统备份。以下列出的限制和要求也适用于虚拟环境。

概述

对不同硬件还原的阶段采用标准灾难恢复阶段，*但具有以下区别*：

- **阶段 0**：收集有关网络配置和硬件的其他信息。
- **阶段 1**：将机器置于灾难恢复可执行文件能够访问磁盘、文件系统、网络和 WIN32 API 的状态。检查关键还原设备。如果缺少任何驱动程序，您会收到提供它们的提示。
- **阶段 2**，尽管还原 OS 是相同的，但之后需执行一个额外的子阶段：
  - **阶段 2a**：通过插入关键的驱动程序、更新注册表和映射网络，还原的操作系统已准备就绪并且适应硬件。
- **阶段 3** 完全相同，在该阶段还原阶段 2 没有还原的数据。

要求

- 至少必须为目标计算机提供所有关键的引导驱动程序(包括网络驱动程序)。这些驱动程序可在映像创建时直接添加到映像中(推荐)或在还原时加载(在阶段 1 期间)。此外，如果要尝试本地还原，还必须具有本地安装的备份设备(例如磁带设备)的驱动程序。

  有关详细信息，请参见驱动程序 (第 74 页)。
- 对还原的 OS 进行自动网络配置还原时，需具有网络驱动程序。
- 还原系统必须至少具有与备份系统原来相同的磁盘数量(容量相同或更高)。
- 硬件制造商的目标硬件(服务器或工作站)应支持原始 OS 。
- 建议在执行不同硬件还原前，目标硬件的系统固件应是最新的。
- 如果您需要在备份期间禁用不同的硬件支持，在您想要备份的系统上编辑文件 驱动程序 (第 74 页) 并将 `enable_disshw` 选项设置为 `0`。
- 系统必须至少包含一个 NTFS 卷，作为备份阶段 VSS 目的的存储点。

限制

如果采用**使用卷影副本**选项(默认情况下受支持的平台中此选项处于选中状态)执行还原，则灾难恢复模块仅支持不同硬件还原。

- 仅以下操作系统上的 EADR 和 OBDR 可提供不同硬件支持：
  - Windows Vista
  - Windows 7
  - Windows Server 2008

- Windows Server 2008 R2
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

有关详细信息，请参见 https://softwaresupport.softwaregrp.com/ 上的最新支持矩阵。

- 支持以下跨平台还原组合：

从	至
64 位 (x64) 操作系统	64 位 (x64) 硬件架构
32 位操作系统	32 位或 64 位 (x64) 硬件架构

升级后的操作系统只有使用“常规”恢复选项方可支持不同硬件还原(请参见 恢复过程 (第 75 页))。

- 不支持网卡组合配置。如果需要对网卡进行组合，必须在 OS 还原后重新配置网卡。灾难恢复模块只能还原物理网卡配置。
- 灾难恢复模块只能插入提供 INF 文件的驱动程序。在阶段 1 或阶段 2a 期间，不支持自身具有安装步骤的驱动程序(例如显卡驱动程序)且无法插入此类驱动程序。但是，对于关键的引导驱动程序，制造商通常会提供 INF 文件。
- 目标硬件的磁盘应始终连接相同类型的主机适配器总线(例如 SCSI 或 SAS)，否则还原可能失败。
- 使用“无人看管”模式还原域控制器时，必须手动登录才可完成 sysprep 清理。清理完成后，OS 将自动重新启动，系统就可以使用了。

建议

尝试执行不同硬件还原前，目标硬件的系统固件应是最新的。

驱动程序

> **注意：**
> DR OS 映像包括由关键的常规程序组成的大型数据库，尤其是存储控制器。如果无法找到要插入的原始驱动程序，很有可能 DR OS 映像中已经存在常规驱动程序。

为确保在不同硬件上进行还原，必须具有新系统还原和引导所需的关键驱动程序。您将需要提供以下驱动程序：

- 目标系统的所有存储控制器的驱动程序。此驱动程序将支持在还原/引导时检测底层存储。
- 支持对现有驱动程序存储位置的网络还原和访问的网卡驱动程序，以及尝试本地还原时本地连接的备份设备的驱动程序(例如磁带驱动器)。

原始硬件的驱动程序可能包含在准备阶段(阶段 0)备份期间的 DR OS 映像中，而且您可以在创建映像期间添加新硬件的驱动程序。您还可选择在还原过程中手动添加它们。

尽管灾难恢复模块在还原过程中只搜索关键的引导驱动程序，您仍可以在 DR OS 映像中添加额外的非关键引导驱动程序，然后使用“加载驱动程序”任务菜单选项在还原过程中插入它们。

完成操作系统引导后，应安装其他缺少的硬件驱动程序。

准备

> **注意：**
> 完成对系统的所有硬件配置更改后，需执行此准备操作。

EADR (请参见 EADR 准备) 和 OBDR(请参见 OBDR 准备)的准备相同，其更改如下：

- 灾难恢复模块还会收集网络配置信息和硬件信息。
- 应具备关键设备驱动程序(例如存储、网络或磁带驱动程序)，以便灾难恢复模块可在创建映像时将驱动程序插入 DR OS 映像。请参见驱动程序 (第 74 页)。

恢复过程

如果在 Data Protector 灾难恢复 GUI 的“恢复选项”页上启用了对不同硬件的还原功能，系统将在恢复过程中扫描缺少的驱动程序。如果缺少任何关键的驱动程序(如存储、磁带、网络驱动程序或磁盘控制器)，系统会提示您加载所缺少的驱动程序。

步骤

1. 在灾难恢复过程中，当系统提示您加载缺少的驱动程序时，单击**是**启动“不同硬件”向导。如果单击**否**，驱动程序注入过程将被跳过。
2. 在“选择设备”页中，选择要加载驱动程序的设备。单击**下一步**。
3. 在“驱动程序搜索位置”页上，指定要在所运行的系统上用于保存驱动程序的位置。浏览到设备驱动程序，或在“驱动程序路径”文本框中键入位置，然后单击**添加路径**将指定的路径添加到列表。可以使用**搜索树深度**选项将搜索调整为您的特定系统范围。

   > **注意：**
   > 可以从搜索列表中删除指定的位置，方法是右键单击该位置，然后选择**删除**。

   将在指定的位置搜索缺少的驱动程序。单击**下一步**。
4. 在指定位置搜索缺少的驱动程序后，可能得到以下结果：
   - 找到设备驱动程序：在“驱动程序路径”文本框中指定了对应驱动程序信息文件(`*.inf`)的完整路径。验证该驱动程序是否正确，然后单击**下一步**加载它。
   - 找不到设备驱动程序：“驱动程序路径”文本框为空。执行以下某个操作：

     如果要搜索其他驱动程序，请单击**浏览**。在“浏览文件”对话框中，选择设备驱动程序的路径，然后单击**下一步**。

     如果不需要将驱动程序加载到该设备，可以将“驱动程序路径”文本框留空，并单击**下一步**进入下一个页面，或者单击**跳过**退出向导。

> **注意：**
> 如果指定了与设备不对应的驱动程序，此驱动程序将显示为无效，并且无法加载。 如果驱动程序不正确，可以更改它或跳过加载过程。

5. 在“驱动程序安装进度”页中，可以查看是否已成功加载设备驱动程序。 如果报告了任何错误，可以单击**重试**以重新尝试加载驱动程序。 单击**完成 (Finish)**。

还原和准备 OS

还原 OS 的过程与标准的 EADR(从步骤 5 开始)和 OBDR(从步骤 6 开始)过程相同。 之后，恢复过程将准备已还原的 OS 并使其适应不同的硬件来为应用程序和文件还原准备 OS。 这包括插入引导关键型驱动程序、更新已还原的 OS 的注册表和映射网络。

由于所有引导关键型驱动程序都应存在(在阶段 0 期间加载到正在运行的 DR OS 映像中或在 OS 还原期间手动添加)，因此插入操作将自动发生。 但是可能需要您的干预才能纠正网络映射。

纠正网络映射

在还原不同的硬件之后，灾难恢复模块将检查所恢复的系统上的网络适配器是否与原始系统上的网络适配器不同。 灾难恢复模块无法始终将原始系统的网络配置映射到其自身上的目标系统的网络配置。 例如，当目标系统有一张网卡而原始系统有两张或更多网卡，或者向目标系统添加其他网络适配器时会发生这种情况。 当检测到此类差异或无法自动确定正确的网络映射时，您可以选择将原始网络适配器映射到在目标系统上发现的网络适配器。

> **注意：**
> 网络映射仅在有可用的网络适配器的情况下发生。 无法映射没有驱动程序的网络适配器。 因此，您应在还原过程开始之前加载网卡驱动程序。

步骤

1. 在“网络适配器映射”页中，在原始网络适配器下拉列表中选择原始系统的网络适配器。 在当前网络适配器下拉列表中，选择目标系统上的一个可用网络适配器。 单击**添加映射**。 您创建的映射即被添加到列表中。

   > **注意：**
   > 可以从列表中删除映射，方法是右键单击映射然后选择**删除**。

2. 在映射所有需要的网络适配器之后，单击**完成**。

OS 成功还原后

不同的硬件还原将重置 OS 激活。 OS 成功还原后，您应：

- 重新激活 OS。
- 检查并重新安装(如果需要)缺少的系统驱动程序。

还原用户和应用程序数据

此阶段与用于 EADR 的过程相同。 请参见增强型自动灾难恢复 (EADR) (第 33 页)。

注意：
OS 启动后，第三方应用程序服务和驱动程序可能无法加载。 可能需要重新安装、重新配置这些应用程序或者在不需要这些应用程序时将其从当前系统中删除。

将物理系统恢复为虚拟机 (P2V)

Data Protector 支持恢复到为原始操作系统提供支持的虚拟环境，例如 VMware vSphere、Microsoft Hyper-V 或 Citrix XenServer。

先决条件

目标虚拟机必须满足以下要求：

- 来宾操作系统必须与原始操作系统的类型相同(Windows 或 Linux)。
- 虚拟机的磁盘数量必须大于或等于原始系统的磁盘数量。
- 磁盘的大小必须大于或等于其原始对应版本的大小。
- 磁盘顺序必须与原始系统中的磁盘顺序相同。
- 分配给虚拟机的内存量可能会对恢复过程产生影响，因此建议至少为虚拟机分配 1 GB 的内存。
- 虚拟视频卡内存大小必须满足原始系统的基于原始系统的显示分辨率的要求。 如果可能，请使用自动设置。
- 添加与原始计算机上数量相同的网络适配器。 适配器必须连接到原始适配器所连接到的网络。

步骤

使用 DR OS 映像引导虚拟机并按照标准灾难恢复过程恢复到不同的硬件。

将虚拟机恢复为物理系统 (V2P)

使用标准灾难恢复过程恢复到不同的硬件，执行虚拟机到物理系统的灾难恢复。

第 4 章： UNIX 系统中的灾难恢复

手动灾难恢复 (MDR)

手动灾难恢复是一种基础的恢复方法。此方法涉及以初始安装的相同方式重新安装系统从而恢复系统。Data Protector 用于还原所有文件，其中包括操作系统。

HP-UX 客户机的 MDR 基于 Ignite-UX 产品；这个应用程序主要是为 HP-UX 系统的安装和配置任务而开发的，它(除了是一个强大的系统管理界面)提供系统准备和从灾难恢复系统的功能。

Ignite-UX 侧重于目标客户机的灾难恢复的同时，必须使用 Data Protector 还原用户和应用程序数据，以便完成灾难恢复的阶段 3。

> **注意：**
> 本节未涵盖 Ignite-UX 的完整功能。有关详细信息，请参见《Ignite-UX 管理指南》。

概述

Ignite-UX 提供 2 种不同的方法用于针对灾难准备系统和从灾难恢复系统：

- 使用自定义安装介质 (Golden Image)
- 使用系统恢复工具(make_tape_recovery、make_net_recovery)

使用自定义安装介质最适于 IT 环境中具有大量基本相同的硬件配置和 OS 版本，使用系统恢复工具则支持创建恢复存档(针对各个系统对这些存档进行了自定义)。

使用这两种方法都可以创建 DDS 磁带或 CD 等可引导安装介质。使用这些介质，系统管理员能够直接从故障客户机的系统控制台中执行本地灾难恢复。

此外，这两种方法还都可以通过向故障客户机分配合适的 Golden Image 或以前创建的“恢复存档”，用于运行基于网络的客户机恢复。在这种情况下，客户机直接从 Ignite 服务器引导，并且从所分配的仓库(必须位于网络上的 NFS 共享中)中运行安装。

在受支持的位置使用 Ignite-UX GUI。

为手动灾难恢复做的准备 (HP-UX Cell Manager)

要做好准备而使灾难恢复成功，应遵照与常规准备过程相关的说明以及特定方法要求。必须提前准备，以便快速高效地执行灾难恢复。

为 Cell Manager 的手动灾难恢复所做的准备包括：

- 收集备份规范的信息
- 准备备份规范(使用 pre-exec 脚本)
- 执行备份
- 定期执行内部数据库备份会话

在 Cell Manager 上执行灾难恢复之前，必须进行所有这些准备步骤。

一次性准备

应在灾难恢复计划中记录这些文件的位置，以便在发生灾难时可以找到这些信息。 此外，应考虑版本管理(每个备份有一组“辅助信息”)。

如果要备份的系统有在底层活动的应用程序进程，则应建立 minimal activity(经过修改的 init 1 run-level)状态，以便准备 Cell Manager 进行一致的备份。

HP-UX 系统

- 从 /sbin/rc1.d to /sbin/rc0.d 移动某些终止链接，并补充对引导部分的更改。 终止链接包括移至运行级别 1 就会被暂停的基本服务，而备份需要这些服务。
- 确保在系统上配置了 rpcd(在 /etc/rc.config.d/dce 文件中配置 RPCD=1 选项)。

这样将准备系统，以使其进入最低限度活动的状态，该状态特征如下：

- Init-1 (FS_mounted, hostname_set, date_set, syncer_running)
- 运行进程：network、inetd、rpcd、 swagentd

备份系统

准备好备份规范之后，应执行备份过程。 定期重复此过程，或至少在每次系统配置有更大更改之后，尤其是在物理或逻辑卷结构方面发生任何更改之后重复此过程。 请特别注意 IDB 和文件系统备份：

- 定期备份 IDB(最好在单独的备份规范中，并计划在 Cell Manager 自身的备份之后)。
- 在连接到 Cell Manager 系统的某个特定设备上运行 IDB 和文件系统备份，以使您了解设备中的介质包含 IDB 的最新备份版本。

手动安装和配置 HP-UX 系统 (Cell Manager)

灾难发生之后，应首先安装和配置操作系统(阶段 1)。 然后可以恢复 Cell Manager。

步骤

阶段 1

1. 替换受影响的磁盘。
2. 从操作系统安装介质引导系统。
3. 重新安装操作系统。 安装期间，使用在准备阶段收集的数据(使用 pre-exec 脚本)重新创建和配置物理和逻辑存储/卷结构、文件系统、装载点、网络设置等等。

手动还原系统数据 (HP-UX Cell Manager)

安装和配置操作系统(阶段 1)之后，可以使用 Data Protector 恢复 Cell Manager。

先决条件

- 您需要一个介质，其中包含 Cell Manager 系统根卷的最新备份映像，以及 IDB 的更新的最新备份映像。
- 需要连接到 Cell Manager 系统的设备。

步骤

阶段 2

1. 在 Cell Manager 上重新安装 Data Protector 软件。
2. 从 IDB 和 `/etc/opt/omni` 目录各自的最新备份映像将它们还原至临时目录。 这样可简化从备份介质中还原所有其他文件。 删除 `/etc/opt/omni/` 目录，并将其替换为临时目录中的 `/etc/opt/omni` 目录。 这样将重新创建以前的配置。
3. 使用 `omnisv -start` 命令启动 Data Protector 进程。

阶段 3

4. 启动 Data Protector GUI，并从备份映像还原所需文件。
5. 重新启动系统。

现在应成功恢复了 Cell Manager。

为手动灾难恢复做的准备(HP-UX 客户机)

Ignite-UX 提供 2 种不同的方法用于针对灾难准备系统和从灾难恢复系统：

使用自定义安装介质 (Golden Image)

使用系统恢复工具(make_tape_recovery、make_net_recovery)

使用自定义安装介质 (Golden Image)

大型 IT 环境通常由大量基于相同硬件和软件的系统组成。 如果使用已安装系统的完整快照安装其他系统，则可以显著缩短新系统用于安装 OS、应用程序和所需修补程序的时间。 Ignite-UX 含有一项功能，通过该功能可以修改网络或文件系统设置等参数，以及将 Data Protector 等软件添加到映像(用 Ignite-UX 命令 `make_config`)，然后再将此类 Golden Image 分配给另一个系统。 因此，此功能可用于从灾难恢复系统。

使用自定义安装介质的常规步骤包括：

1. **阶段 0**
   a. 创建客户机系统的 Golden Image。
2. **阶段 1** 和 **2**
   a. 用替换磁盘替换故障磁盘。
   b. 从 Ignite-UX 服务器引导 HP-UX 客户机然后配置网络。

c. 从 Ignite-UX 服务器安装 Golden Image。

3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

创建 Golden Image

1. 将 /opt/ignite/data/scripts/make_sys_image 文件从 Ignite-UX 服务器复制到客户机系统上的一个临时目录中。
2. 在客户机节点上运行以下命令，以便在另一个系统上创建客户机的压缩映像： make_sys_image -d *directory of the archive* -n *name of the archive*.gz -s *IP address of the target system*

   此命令将在系统中用 --d 和 -s 选项定义的指定目录中创建以 gzip 格式压缩的文件仓库。 确保 HP-UX 客户机已授予了对目标系统的无密码访问权限(.rhosts 文件的一个条目中有目标系统上的客户机系统的名称)，否则命令将失败。
3. 向目标系统上的 /etc/exports 目录添加目标目录，然后在目标服务器上导出该目录 (exportfs -av)。
4. 在配置 Ignite-UX 服务器上，将归档模板文件 core.cfg 复制到 archive_*name*.cfg： cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/*OS_Release*/archive_*name*.cfg.

   示例： cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg
5. 在复制的配置文件中检查和更改以下参数：
   - 在 sw_source 节中：

     load_order = 0

     source_format = archive

     source_type="NET"

     # change_media=FALSE

     post_load_script = "/opt/ignite/data/scripts/os_arch_post_l"

     post_config_script = "/opt/ignite/data/scripts/os_arch_post_c"

     nfs_source = "*IP Target System*:*Full Path*
   - 在匹配的 OS archive 节中：

     archive_path = "*archive_name*.gz
6. 通过对映像文件运行命令 archive_impact 确定“impacts”条目，并且复制配置文件的相同“OS archive”节中的输出： /opt/ignite/lbin/archive_impact -t -g *archive_name*.gz。

   示例： /opt/ignite/lbin/archive_impact -t -g /image/archive_HPUX11_31_DP70_CL.gz

   impacts = "/" 506Kb

   impacts = "/.root" 32Kb

   impacts = "/dev" 12Kb

   impacts = "/etc" 26275Kb

```
impacts = "/opt" 827022Kb
impacts = "/sbin" 35124Kb
impacts = "/stand" 1116Kb
impacts = "/tcadm" 1Kb
impacts = "/usr" 729579Kb
impacts = "/var" 254639Kb
```

7. 要使 Ignite-UX 了解新创建的仓库，请将具有以下布局的 cfg 条目添加到 /var/opt/ignite/INDEX 文件中：

   ```
   cfg "This_configuration_name" {
   description "Description of this configuration"
   "/opt/ignite/data/OS/config"
   "/var/opt/ignite/data/OS/ archive_name.cfg"
   }
   ```

   示例：

   ```
   cfg "HPUX11_31_DP70_Client" {
   description "HPUX 11.i OS incl Patches and DP70 Client"
   "/opt/ignite/data/Rel_B.11.31/config"
   "/var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg"
   }
   ```

8. 确保保留一个或多个 IP 地址，用于引导 /etc/opt/ignite/instl_boottab 文件中配置的客户机。 IP 地址的数字等于同时引导的客户机的数量。

上述过程完成之后，将拥有 HP-UX 客户机的 Golden Image(含有特定的硬件和软件配置)，它可用于恢复相似布局的任何客户机。

需要重复这些步骤，为所有硬件和软件配置不同的系统创建 Golden Image。

通过 Ignite-UX，可以根据所创建的 Golden Image 创建可引导磁带或 CD。 有关详细信息，请参见《Ignite-UX 管理指南》。

恢复 HP-UX 客户机

有 3 种不同的方法可使用手动灾难恢复 (MDR) 恢复 HP-UX 客户机：

使用 Golden Image 进行恢复

从可引导备份磁带进行恢复

从网络进行恢复

使用 Golden Image 进行恢复

通过应用 Golden Image(位于网络上的 NFS 共享上)可恢复 HP-UX 客户机。

在客户机上

步骤

1. 更换故障硬件。
2. 从 Ignite-UX 服务器引导 HP-UX 客户机： `boot lan.IP-address Ignite-UX server install.`
3. 显示“欢迎使用 Ignite-UX”屏幕时，选择**安装 HP-UX**。
4. 从“GUI 选项”屏幕中选择 **Ignite-UX 服务器上运行的远程图形界面**。
5. 对“网络配置”对话框作出回应。
6. 系统现在已为远程 Ignite-UX 服务器控制的安装做好准备。

在 Ignite-UX 服务器上

步骤

1. 在 Ignite-UX GUI 中右键单击客户机图标，然后选择**安装客户机 - 新安装**。
2. 选择要安装的 Golden Image，检查设置(网络、文件系统、时区...)，然后单击**开始**。
3. 通过右键单击客户机图标并选择**客户机状态**，可以检查安装进度。
4. 安装结束之后，使用标准 Data Protector 还原过程还原其他用户和应用程序数据。

从可引导备份磁带进行恢复

使用 make_tape_recovery 命令创建可引导备份磁带。

步骤

1. 更换故障硬件。
2. 确保将磁带设备在本地连接到受影响的 HP-UX 客户机，并插入含有要还原的存档的介质。
3. 从准备的恢复磁带引导。 为此，请在 boot admin 菜单中键入 `SEARCH`，获得所有可用的引导设备的列表。 确定哪一个是磁带驱动器，然后键入 boot 命令： `boot hardware path` 或 `boot Pnumber`。
4. 此时将自动启动恢复过程。
5. 恢复成功完成之后，使用标准 Data Protector 还原过程还原其他用户和应用程序数据。

从网络进行恢复

可以从位于 Ignite-UX 服务器上的恢复归档文件通过网络引导目标系统。 按照有关如何使用 Golden Image 执行恢复的说明进行操作，并确保为安装选择了所需的存档。

使用系统恢复工具(make_tape_recovery、make_net_recovery)

使用与 Ignite-UX 捆绑的系统恢复工具，可从磁盘故障中快速轻松地恢复。 系统恢复工具的恢复存档仅包括必要的 HP-UX 目录。 但是，还可以在归档中加入其他文件和目录(例如其他卷组或 Data Protector 文件和目录)以加快恢复过程。

make_tape_recovery 可创建针对系统自定义的可引导恢复(安装)磁带，并支持无人看管的灾难恢复，具体方法是将备份设备直接连接到目标系统，并从可引导恢复磁带启动目标系统。 在创建归档和恢复客户机期间，备份设备必须本地连接到客户机。

make_net_recovery 可通过网络在 Ignite-UX 服务器或其他任何指定的系统上创建恢复归档。 从由 Ignite-UX make_boot_tape 命令创建的可引导磁带启动或系统直接从 Ignite-UX 服务器引导之后，可以跨越子网恢复目标系统。 直接从 Ignite-UX 服务器启动的过程可以借助 Ignite-UX bootsys 命令自动化，也可以在引导控制台上以交互方式指定启动过程。

使用系统恢复工具的常规步骤包括：

1. **阶段 0**
   a. 在 Ignite-UX 服务器上使用 Ignite-UX GUI 创建 HP-UX 客户机的恢复存档。
2. **阶段 1** 和 **2**
   a. 用替换磁盘替换故障磁盘。
   b. 对于本地还原，从准备的恢复磁带引导。
   c. 进行本地还原时，恢复过程将自动启动。
      对于网络还原，从 Ignite-UX 客户机引导并配置网络和 UI。
      进行网络还原时，从 Ignite-UX 服务器安装 Golden Image。
3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

先决条件

必须在客户机上安装 Ignite-UX 文件集，以使 Ignite-UX 服务器能够与客户机通信，然后才能针对灾难准备系统。

确保 Ignite-UX 服务器上和客户机上的 Ignite-UX 文件集的修订版相同。 使所有内容保持一致的最简单方式是从 Ignite-UX 服务器上生成的仓库中安装 Ignite-UX。 通过在 Ignite-UX 服务器上运行以下命令，可以构造此仓库：pkg_rec_depot -f。 此命令可在 /var/opt/ignite/depots/recovery_cmds 下创建 Ignite-UX 仓库，该目录可以在客户机上由 swinstall 指定为用于安装 Ignite-UX 软件的源目录。

在客户机节点上安装 Ignite-UX 之后，可以使用 make_net_recovery 或 make_tape_recovery 在 Ignite-UX 服务器上使用 GUI 创建恢复归档。

使用 **make_tape_recovery** 创建存档

1. 确保将备份设备连接到 HP-UX 客户机。
2. 通过执行以下命令，启动 Ignite-UX GUI：/opt/ignite/bin/ignite &。
3. 右键单击客户机图标，然后选择 Create Tape Recovery Archive。

4. 如果有多个设备连接到 HP-UX 客户机，则选择一个磁带设备。
5. 选择要加入存档中的卷组。
6. 现在将开始磁带创建过程。 通过右键单击客户机图标并选择 Client Status，检查 Ignite-UX 服务器上的状态和日志文件。

> **注意：**
> Ignite-UX 建议使用 90m DDS1 备份磁带，以确保磁带适用于任何 DDS 驱动器。

使用 make_net_recovery 创建存档

使用 make_net_recovery 创建恢复归档的过程与使用 make_tape_recovery 几乎相同。 此命令的优点是不需要在本地连接备份设备，因为默认情况下恢复存档存储在 Ignite-UX 服务器上。

1. 通过执行以下命令，启动 Ignite-UX GUI： /opt/ignite/bin/ignite &
2. 右键单击客户机图标，然后选择 Create Network Recovery Archive。
3. 选择目标系统和目录。 确保有足够的空间可存储压缩后的存档。
4. 选择要加入存档中的卷组。
5. 现在将开始存档创建过程。 通过右键单击图标并选择 Client Status，检查 Ignite-UX 服务器上的状态和日志文件。

> **注意：**
> 使用 Ignite-UX 可以根据压缩的存档文件创建可引导的存档磁带。 请参见《Ignite-UX Administration Guide》中的“Create a Bootable Archive Tape via the Network”一章。

磁盘传递灾难恢复 (DDDR)

磁盘传递灾难恢复有两种可能的方法。 可以使用正常运行的 Data Protector 客户机系统，并在连接到此客户机时创建新磁盘。 此外，可以使用辅助磁盘，而不使用其他正常运行的客户机。 需要在灾难之前收集足够的数据才能正确地对磁盘进行格式化和分区。

概述

使用装有最小化操作系统(其上配置有网络并安装了 Data Protector 代理)的辅助磁盘(可以随身携带)执行 UNIX 客户机的磁盘传递。

确保已执行准备一章中提及的所有常规准备步骤。 对 UNIX 客户机使用辅助磁盘的常规步骤包括：

1. **阶段 1**
   a. 用替换磁盘替换故障磁盘，将辅助磁盘连接到目标系统，然后使用辅助磁盘上安装的最小化操作系统重新启动系统。
   b. 手动对这些磁盘进行重新分区，重新建立存储结构并使替换磁盘可引导。
2. **阶段 2**

a. 使用标准 Data Protector 还原过程将原始系统的引导磁盘还原到替换磁盘(使用**恢复至**选项)。
b. 关闭系统并删除辅助磁盘。 如果您使用的是热插拔硬盘驱动器，则无需关闭系统。
c. 重新启动系统。

3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

限制

- 应在与目标系统相同硬件级别的系统上准备辅助磁盘。
- 群集环境恢复可能与标准过程有所不同。 根据群集环境的配置，可能需要对环境执行额外的步骤和修改。
- 不支持 RAID。

为 UNIX 客户机的磁盘传递灾难恢复做的准备

要做好准备而使灾难恢复成功，应遵照与常规准备过程相关的说明以及特定方法要求。 必须提前准备，以便快速高效地执行灾难恢复。 有关受支持操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

为磁盘传递灾难恢复做的准备包括：

- 收集备份规范的信息
- 准备辅助磁盘
- 准备备份规范(使用 pre-exec 脚本)
- 执行备份

在客户机系统上执行灾难恢复之前，必须进行所有这些准备过程。

一次性准备

如果在 pre-exec 命令过程中收集信息，则应在灾难恢复计划中记录这些文件的位置，以便在发生灾难时可以找到这些信息。 此外，应考虑版本管理(每个备份有一组“辅助信息”)。

还应在每个客户机系统上建立 minimal activity(经过修改的 init 1 run-level)状态，以便准备其进行一致的备份，并因此避免恢复之后出现问题。 有关详细信息，请参见操作系统文档。

HP-UX 示例

- 从 /sbin/rc1.d to /sbin/rc0.d 移动某些终止链接，并补充对引导部分的更改。 终止链接包括移至运行级别 1 就会被暂停的基本服务，而备份需要这些服务。
- 确保在系统上配置了 rpcd(在 /etc/rc.config.d/dce 文件中配置 RPCD=1 选项)。

这样将准备系统，以使其进入最低限度活动的状态，该状态特征如下：

- Init-1 (FS_mounted, hostname_set, date_set, syncer_running)
- 网络必须正在运行
- 运行进程：network、inetd、rpcd、 swagentd

Solaris 示例

- 从 /etc/rc1.d to /etc/rc0.d 移动某些终止链接，并补充对引导部分的更改。 终止链接包括移至运行级别 1 就会被暂停的基本服务，而备份需要这些服务。
- 确保在系统中配置了 rpcbind。

这样将准备系统，以使其进入最低限度活动的状态，该状态特征如下：

- Init-1
- 网络必须正在运行
- 运行的进程： network, inetd, rpcbind

AIX

无需任何操作，因为用于准备辅助磁盘的 alt_disk_install 命令可确保一致的磁盘映像，而不必进入最低限度系统活动的状态。

准备辅助磁盘

如果要使用辅助磁盘，则需要首先准备它。 每个单元和平台仅需要一个可引导辅助磁盘。 该磁盘必须包含操作系统和网络配置，且必须可引导。

备份系统

准备好备份规范之后，应执行备份过程。 定期重复此过程，或至少在每次系统配置有更大更改之后，尤其是在物理或逻辑卷结构方面发生任何更改之后重复此过程。

为 UNIX 客户机的灾难恢复创建备份规范

要为 UNIX 客户机的灾难恢复配置备份规范，请修改现有规范，或用指定的 pre-exec 和 post-exec 脚本创建新规范。 有关受支持操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

步骤

1. 提供将执行以下操作的 pre-exec 脚本：
   - 收集有关环境的所有必要信息，并将其存储在稳妥之处以备灾难恢复时使用。 这些信息包括：
     - 系统的物理和逻辑存储结构
     - 当前逻辑卷结构(例如 HP-UX 系统中，使用 vgcfgbackup 和 vgdisplay -v)
     - 群集配置数据、磁盘镜像和条带化

- 文件系统和装载点概述(例如 HP-UX 系统中，使用 bdf 或 /etc/fstab 的副本)
- 系统分页空间信息(例如 HP-UX 系统中，swapinfo 命令的输出)
- I/O 结构概述(例如 HP-UX 系统中，使用 HP-UX 系统中的 ioscan -fun 和 ioscan -fkn)
- 客户机网络设置

也可以将数据的紧急副本放入备份本身内。 如果是这样，则请在实际恢复之前提取信息。

- 从系统中注销所有用户。
- 关闭所有应用程序，除非单独备份应用程序数据(例如使用联机数据库备份)。
- (可选)限制通过网络访问系统，以便在备份运行时无人可登录系统(例如 HP-UX 系统中，覆盖 inetd.sec 并使用 inetd -c))。
- 如果需要，进入最低限度系统活动的状态(例如 HP-UX 系统中，使用 sbin/init 1；wait 60；检查是否达到 run-level 1)。 注意，这是经过修改的“init 1”状态。

2. 提供将系统还原到标准运行级别、重新启动应用程序等等的 post-exec 脚本。
3. 在 Data Protector Cell Manager 上使用 pre-exec 和 post-exec 脚本为客户机配置备份规范。其中应包括所有磁盘。
4. 执行此备份过程并定期重复执行该过程，或者至少在每次发生重大系统配置更改时，尤其是逻辑卷结构发生任何更改(例如，在 HP-UX 上使用 LVM)时执行此过程。

使用 DDDR 安装和配置 UNIX 客户机

灾难发生之后，应首先为故障客户机安装和配置新磁盘(阶段 1)。

先决条件

- 需要用新硬盘更换受影响的磁盘。
- 应在与目标系统相同硬件级别的系统上准备辅助磁盘。
- 辅助磁盘应包含相关的 UNIX 操作系统和 Data Protector 代理。
- 应有要恢复的客户机的有效完整备份。

步骤

1. 将故障磁盘替换为类似大小的新磁盘。
2. 将辅助磁盘(包含所需的操作系统和 Data Protector 客户机)连接到系统，并将其作为引导设备。
3. 从辅助操作系统引导。
4. 如果适用，则重新构造逻辑卷结构(例如，在 HP-UX 系统中使用 LVM)。 对非根卷组使用备份数据(例如使用 HP-UX 系统中的 vgcfgrestore 或 SAM)。
5. 此外，创建要在修复的磁盘上还原的根卷组(例如使用 HP-UX 系统中的 vgimport)。 它

在还原过程中不像是根卷组，因为正在运行辅助磁盘中的操作系统。

6. 使用相关的 UNIX 命令使新磁盘可引导。
7. 在备份期间，根据辅助存储设备上保存的数据重新构造任何其他存储结构，如镜像、条带化、Serviceguard 等等。
8. 创建文件系统，并根据备份中数据的需要装载这些文件系统。 使用相似但并非原始的装载点名称(例如 /etc_restore 对于 /etc 等等)。
9. 删除要还原的装载点中的任何文件；这些装载点必须为空。
10. 开始还原系统数据。

使用 DDDR 还原系统数据(UNIX 客户机)

可以将系统还原为上次成功执行备份时的状态。 首先应安装和配置 UNIX 客户机(阶段 1)。有关受支持操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

先决条件

- 应安装并配置相关的操作系统。
- 应安装 Data Protector。
- 应有要恢复的客户机的有效完整备份。
- 还原所需的介质应可用。

步骤

阶段 2

1. 启动 Data Protector 用户界面，然后打开到 Data Protector Cell Manager 的连接。
2. 将包含辅助磁盘的系统导入单元。
3. 选择要从中还原的备份版本。
4. 使用选项**还原为** *new_mountpoint* 将所有必需的装载点还原到系统，包括(未来的)根卷。

   备份中的根卷还原为“已修复磁盘”上的根卷。 任何内容都不还原到辅助磁盘上当前运行的辅助操作系统。
5. 关闭并重新启动刚还原的系统。
6. 断开辅助磁盘与系统的连接。
7. 从新的(或已修复的)磁盘重新启动系统。

阶段 3

8. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

增强型自动灾难恢复 (EADR)

Data Protector 提供了针对 Linux Data Protector Cell Manager 和客户机的增强型灾难恢复过程。有关支持的操作系统的详细信息，请参见最新的支持矩阵，网址为：https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

备份时，EADR 将自动收集所有相关的环境数据。在整个客户机系统的完整备份期间，对于单元中的每个已备份客户机，临时安装和配置 DR OS 所需的数据打包在单个大型恢复集文件中并存储在备份磁带上(以及可选存储在 Cell Manager 上)。

除此映像文件以外，对磁盘进行正确分区和格式化所需的阶段 1 启动文件(P1S 文件)存储在备份介质和 Cell Manager 上。灾难发生时，增强型自动灾难恢复向导用于从备份介质还原恢复集(如果其在完整备份期间未保存在 Cell Manager 上)并将其转换为灾难恢复 CD ISO 映像。可以使用任何 CD 刻录工具将 CD ISO 映像录制到 CD 上并用于引导目标系统。

启动 DR OS 映像后，Data Protector 将自动对磁盘进行格式化和分区，最后用 Data Protector 将原始系统恢复到备份时的状态。

> **重要：**
> Micro Focus 建议限制对备份介质、恢复集文件、SRD 文件和灾难恢复 CD 的访问。

概述

确保已执行准备一章中提及的所有常规准备步骤。对 Linux 客户机使用增强型自动灾难恢复方法的常规步骤包括：

1. **阶段 1**
   a. 更换故障硬件。
   b. 从灾难恢复 CD 或 USB 闪存驱动器引导目标系统并选择恢复的范围。这是完全无人看管的恢复。
2. **阶段 2**
   a. 根据您所选的恢复范围，系统将自动还原所选的卷。关键卷(引导卷、根卷以及包含 Data Protector 安装和配置的卷)始终会被还原。
3. **阶段 3**
   a. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

> **重要：**
> 提前为任何必须首先还原的关键卷(尤其是 DNS 服务器、Cell Manager、介质代理客户机、文件服务器等等)准备好 DR OS 映像。

提前为 Cell Manager 恢复准备好包含加密密钥的可移动介质。

以下各节将介绍与 Linux 客户机的 EADR 相关的限制、准备步骤和恢复过程。

要求

- 在要允许使用此方法进行恢复的系统上和从中将准备 DR OS 映像的系统上必须安装 Data Protector 自动灾难恢复组件。 有关详细信息，请参见《*Data Protector 安装指南*》。
- 目标系统的硬件配置必须与原始系统相同。 其中包括 SCSI BIOS 设置(扇区重新映射)。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 备份时引导分区上还需要另外 200 MB 的可用磁盘空间。 如果没有这些磁盘空间，则灾难恢复将失败。
- 在 EADR 准备期间，安装 Data Protector 所在的卷必须至少具有 800 MB 的临时可用空间。 此空间是创建临时映像所必需的。
- 系统的 BIOS 必须支持可引导 CD 扩展(如 El-Torito 标准所定义)，并且必须支持通过 INT13h 功能 XXh 使用 LBA 寻址对硬盘驱动器进行读/写访问。 可以在系统的用户手册中或通过在引导之前检查系统设置而检查 BIOS 选项。

限制

- 增强型自动灾难恢复 (EADR) 和一键式灾难恢复 (OBDR) 仅在 Linux 系统上可用。
- 必须在 Linux 系统上创建 Linux 系统的 DR ISO 映像。 不可以在其他系统(Windows 系统、HP-UX 系统、Solaris 系统)上创建 DR ISO 映像。 该限制不适用于更新 SRD 文件或其他任务。
- 如果某个装载点名为 `CONFIGURATION` 且包含目录 `SystemRecoveryData`，则不会备份目录 `SystemRecoveryData` 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。 在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID， 从而导致灾难恢复失败。
- 不支持自定义内核安装或配置，仅支持随分发提供的原始内核。
- 在 SELINUX 强制模式启用的情况下还原 Linux 客户机时，系统必须在恢复后对所有系统文件进行重新标记，此过程可能需要一段时间才能完成，具体取决于系统配置。 如果使用宽容模式，系统日志将包含大量 SELINUX 警告消息。
- 在选择了 CONFIGRATION/SYSTEMRECOVERYDATA 对象的情况下创建备份规范时，默认情况下会从备份中排除文件夹 `/opt/omni/bin/drim/log` 和 `/opt/omni/bin/drim/tmp`。
- 不支持使用恢复的对象备份进行恢复，因为不能保证此类备份的一致性。
- 需要在恢复之前手动连接不在 MiniOS 引导时自动连接的 Fusion IO 磁盘。 将旧的 Fusion IO 磁盘替换为新磁盘或发生内部 Fusion IO 磁盘错误时，需要执行此操作。 在 MiniOS 中连接之前，需要使用特定工具对这些磁盘进行格式化。 要手动格式化 Fusion IO 磁盘并将其连接到系统，恢复开始之前需要在 MiniOS 中显示的 Linux shell 中运行以下命令：
  - `fio-status` – 列出所有 Fusion IO 磁盘的状态。
  - `fio-format [path]` – 执行 Fusion IO 磁盘的低级格式化。
  - `fio-attach [path]` – 将 Fusion IO 磁盘连接到系统。
- 在脱机还原期间，稀疏文件将还原为其完整大小。 这可能会导致目标卷空间不足。
- AUTODR 不支持恢复多个设备上的 btrfs(多种 btrfs raid 配置)，因为它们不受 SLES 11.3 支

持。

- SLES 11.3 上当前的 btrfs 工具不会在新创建的 btrfs 文件系统上设置 UUID。 因此，在恢复期间，AUTODR 无法像备份时那样在 btrfs 文件系统上设置相同的 UUID。

  如果按 UUID 而不是设备名称装载 btrfs 文件系统，您需要在还原后手动编辑 `/etc/fstab` 文件。 需要执行此操作来反映恢复后 btrfs 设备的新的也是正确的 UUID。 这同样适用于 GRUB 配置，因此请避免 UUID。

  在系统恢复后，btrfs 的 UUID 将与备份期间的不同。 如果从在系统上次恢复之前创建的备份再执行一次恢复，AUTODR 将尝试识别正常的 btrfs 文件系统并跳过重新创建它们。
- AUTODR 只能将备份中的 btrfs 设备配置映射到按 UUID 恢复的现有系统中的 btrfs 设备。 它会跳过恢复错误的设备或重新创建的设备。

  要避免这种情况，应仅从在系统上次恢复后创建的备份恢复 btrfs 文件系统或在系统恢复之前手动销毁现有 btrfs 文件系统。 这同样适用于用户在上次备份后手动重新创建的 btrfs 文件系统。

  > **注意：**
  > Data Protector 将在开始恢复过程之前警告用户这种情况。

- btrfs 快照可以备份，但是只能还原为普通子卷。 在这种情况下，不会在快照与创建快照所在的子卷之间共享任何数据。 父对象与其快照之间的整体写时复制 (COW) 关系会丢失。 因此，在某些情况下，无法还原完整的数据集，因为快照中的数据重复，在还原期间底层设备上空间不足。
- 只有装载的 btrfs 子卷中的数据受保护。 考虑一下，可从 OS 文件系统接口和装载的父子卷访问子子卷。 在这种情况下，子卷不受保护，因为磁盘代理 (DA) 将其检测为不同的文件系统并跳过它们，原因是它们没有专用的装载点。
- 使用 `/etc/fstab` 文件中的 `subvolid`(请参阅 *btrfs 文档*)装载选项装载的子卷可能会在恢复的系统中跳过装载或装载到错误的装载点，因为恢复后子卷的 `subvolid` 不需要与备份期间的相同。 尽管会重新创建所有子卷，但是 Data Protector 会跳过在此类子卷中还原数据或者可能会在错误的子卷中还原数据。

  > **注意：**
  > 使用 `fstab` 中的 `subvol` 选项而不是 `subvolid`。

- 不支持使用基于以太网的光纤通道 (FCoE) LUN 和基于以太网的光纤通道 (FCoE) SAN 引导对系统执行 EADR。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。 如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- EADR 仅支持类型为 0x12(包括 EISA)和 0xFE 的供应商特有分区。

为增强型自动灾难恢复做的准备

要做好准备而使灾难恢复成功，请遵照与所有灾难恢复方法的常规准备过程相关的说明，然后再执行本主题中列出的步骤。 必须提前准备，以便快速高效地执行灾难恢复。 应特别注意 Cell Manager 的灾难恢复准备。

重要：
请在灾难发生之前准备灾难恢复。

常规准备

1. 执行完整的客户机系统备份。 建议备份整个客户机，如若不然，您至少需要选择以下关键卷和对象：
   - 引导和系统卷
   - Data Protector 安装卷
   - CONFIGURATION 对象所在的卷

   对于 *Data Protector Cell Manager 系统*，请参见Cell Manager 的额外准备 (第 93 页)。
   请参见《*Data Protector 帮助*》的索引：“备份, UNIX 特定”和“备份, 配置”。
   在进行完整客户机备份期间，恢复集和 P1S 文件存储在备份介质上和(可选)Cell Manager 上。
2. 灾难发生之后，使用 EADR 向导将 DR 映像转换为灾难恢复 CD ISO 映像。
3. 使用支持 ISO9660 格式的任何 CD 录制工具在 CD 上录制灾难恢复 CD ISO 映像。 此灾难恢复 CD 随后可用于引导目标系统并自动还原关键卷。
4. 执行灾难恢复测试计划。

Cell Manager 的额外准备

成功对 Cell Manager 进行灾难恢复还需要额外的准备。

- 定期备份 IDB。 IDB 会话不应早于文件系统会话。
- 在安全位置(而非在 Cell Manager 上)存储 Cell Manager 的 SRD 文件。
- 提前为 Cell Manager 准备灾难恢复操作系统映像。

将恢复集保存到 Cell Manager

在进行完整客户机备份期间，恢复集打包在单个大型文件中，并存储在备份介质上和(可选)Cell Manager 上。 如果计划在 Cell Manager 上录制灾难恢复 CD，则将恢复集文件保存到 Cell Manager 会很有用，这是因为从硬盘获取恢复集文件比从备份介质还原要快得多。

如果在备份期间将恢复集保存到 Cell Manager，则系统会将其保存到默认的 Data Protector P1S 文件位置。

要更改默认位置，请指定一个新的全局选项 `EADRImagePath = valid_path`(例如 `EADRImagePath = /home/images` 或 `EADRImagePath = C:\temp`)。

请参见《Data Protector 帮助》的索引：“全局选项, 修改”。

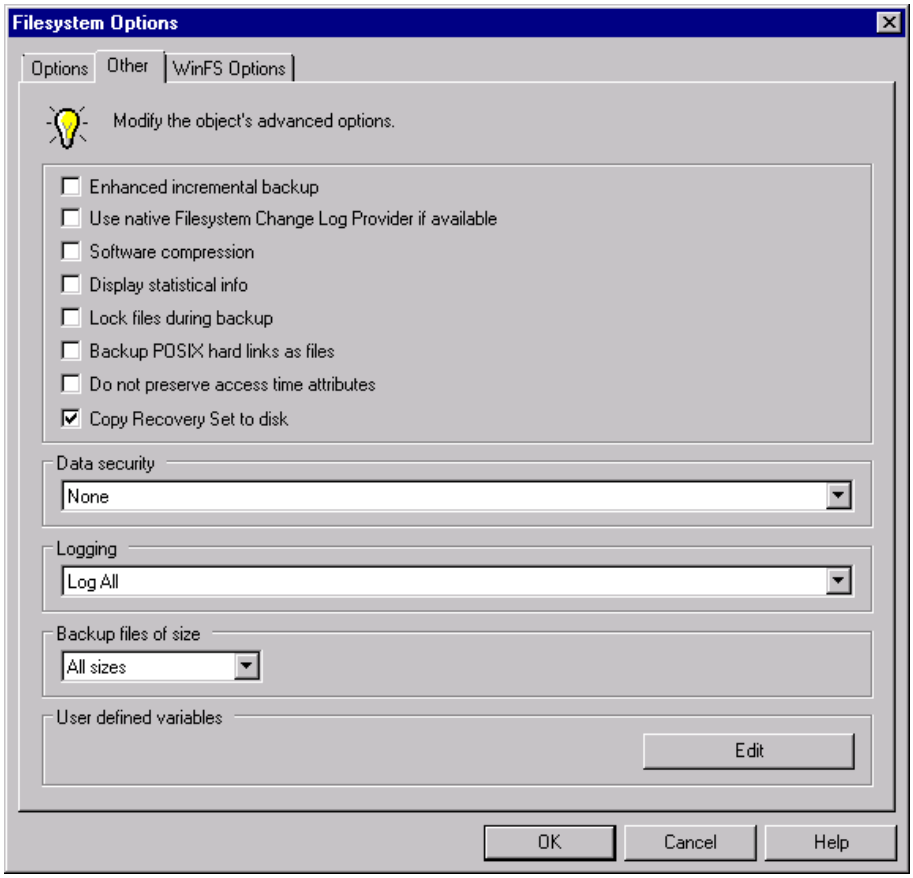
提示：
如果在目标目录中没有足够的可用磁盘空间，则可以创建装载点(Windows 系统)或另一个卷的链接(UNIX 系统)。

将备份规范中所有客户机的恢复集保存到 Cell Manager

步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范(创建该备份规范 - 如果尚未执行此操作)。 有关详细信息，请参见《Data Protector 帮助》的索引：“创建, 备份规范”。
4. 在"结果区域"中，单击**选项**。
5. 在**文件系统选项**下，单击**高级**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。

“其他选项”选项卡



将备份规范中特定客户机的恢复集保存到 Cell Manager

要仅为备份规范中的特定客户机复制恢复集文件，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。
3. 选择将用于完整客户机备份的备份规范(创建该备份规范 - 如果尚未执行此操作)。 有

关详细信息，请参见《Data Protector 帮助》的索引：“创建, 备份规范”。

4. 在"结果区域"中，单击**备份对象摘要**。
5. 选择要将其恢复集文件存储在 Cell Manager 上的客户机，并单击**属性**。
6. 在**其他**页中，选择**将恢复集复制到磁盘**。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。 对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。 在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 *Data_Protector_program_data*\Config\Server\export\keys\DR-*ClientName*-keys.csv(Windows 系统)或 /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv(UNIX 系统)，其中 *ClientName* 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

准备 DR OS 映像

灾难发生之前，应准备一个要录制在灾难恢复 CD 上或保存到可引导 USB 驱动器的 DR OS 映像，它随后可用于增强的自动灾难恢复。 或者，也可以准备可引导的网络映像。

请注意，必须在将准备 DR OS 映像的系统上安装 Data Protector 自动灾难恢复组件。

每次硬件、软件或配置更改之后都必须准备好一个新的灾难恢复 OS 映像。

为必须首先恢复的任何关键系统提前准备 DR OS 映像，尤其是网络正常工作所需的系统(DNS 服务器、域控制器、网关等)、Cell Manager、介质代理客户机和文件服务器等。

建议对含有 OS 映像的备份介质和灾难恢复 CD 或 USB 驱动器的访问权限进行限制。

步骤

1. 在 Data Protector 上下文列表中，单击**恢复**。
2. 在“范围窗格”中，单击**任务**，然后单击**灾难恢复**以启动灾难恢复向导。
3. 在结果区域中，从**要恢复的主机**下拉列表中选择要为其准备 DR OS 映像的客户机，然后单击**验证**以验证该客户机。

   > **注意：**
   > 经过验证的客户机将添加到**要恢复的主机**下拉列表中。

4. 在**恢复介质创建主机**下拉列表中，选择要在其上准备 DR OS 映像的客户机。 默认设置下，该客户机与为其准备 DR OS 映像的客户机一样。 您在其上准备 DR OS 映像的客户机必须安装有相同 OS 类型(Windows、Linux)，并且必须已安装“磁带客户机”。
5. 使**增强的自动灾难恢复**保持选中状态，并选择要从备份会话还是从卷列表构建卷恢复集。 默认情况下，选择**备份会话**。

   单击**下一步 (Next)**。
6. 具体取决于所选的恢复集构建方法：

- 如果选择了备份会话，则应选择主机备份会话；如果是 Cell Manager，则选择 IDB 会话。
- 如果选择了“卷”列表，则应为每个关键对象选择相应的对象版本。

单击**下一步 (Next)**。

7. 选择恢复集文件的位置。 默认情况下，**从备份还原恢复集文件**处于选中状态。
   如果在备份期间已在 Cell Manager 上保存了恢复集文件，则应选择**指向恢复集文件的路径**并指定其位置。 单击**下一步 (Next)**。
8. 选择映像格式。 可用的选项如下：
   - **创建可引导 ISO 映像**： DR ISO 映像(默认情况下为 `recovery.iso`)
   - **创建可引导 USB 驱动器**： 可引导 USB 驱动器上的 DR OS 映像
   - **创建可引导网络映像**： 可用于网络引导的 DR OS 映像(默认情况下为 `recovery.wim`)
9. 如果创建的是可引导 ISO 映像或可引导网络映像，请选择要将创建的映像放置到的目标目录。
   如果要创建可引导的 USB 驱动器，请选择要在其中放置所创建的映像的目标 USB 驱动器或磁盘编号。

   > **重要：**
   > 在创建可引导的 USB 驱动器时，该驱动器上存储的所有数据将丢失。

10. 也可选择设置密码来防止对 DR OS 映像进行未授权的使用。 锁图标指示是否设置了密码。
    单击**密码**打开“密码保护映像”对话框并输入密码。 要删除密码，清除字段内容即可。
11. 单击**完成**以退出向导并创建 DR OS 映像。
12. 如果要创建可引导的 CD 或 DVD，可使用支持 ISO9660 格式的刻录工具，将 ISO 映像刻录在 CD 或 DVD 上。

使用 EADR 恢复 Linux 系统

只有在完成所有准备步骤后，才能成功执行 Linux 系统的增强型自动灾难恢复。 如果要恢复 Cell Manager，将先从内部数据库的备份映像将该内部数据库还原，然后从卷和 CONFIGURATION 对象的备份映像将卷和 CONFIGURATION 对象还原。 有关受支持操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

先决条件

- 需要用新硬盘更换受影响的磁盘。
- 您应当具有要恢复的整个系统的有效完整文件系统备份(客户机备份)。
- 为了对 Cell Manager 进行灾难恢复，您应当具备有效的“内部数据库”备份映像，它应当比文件系统备份映像新。
- 需要灾难恢复 CD。

步骤

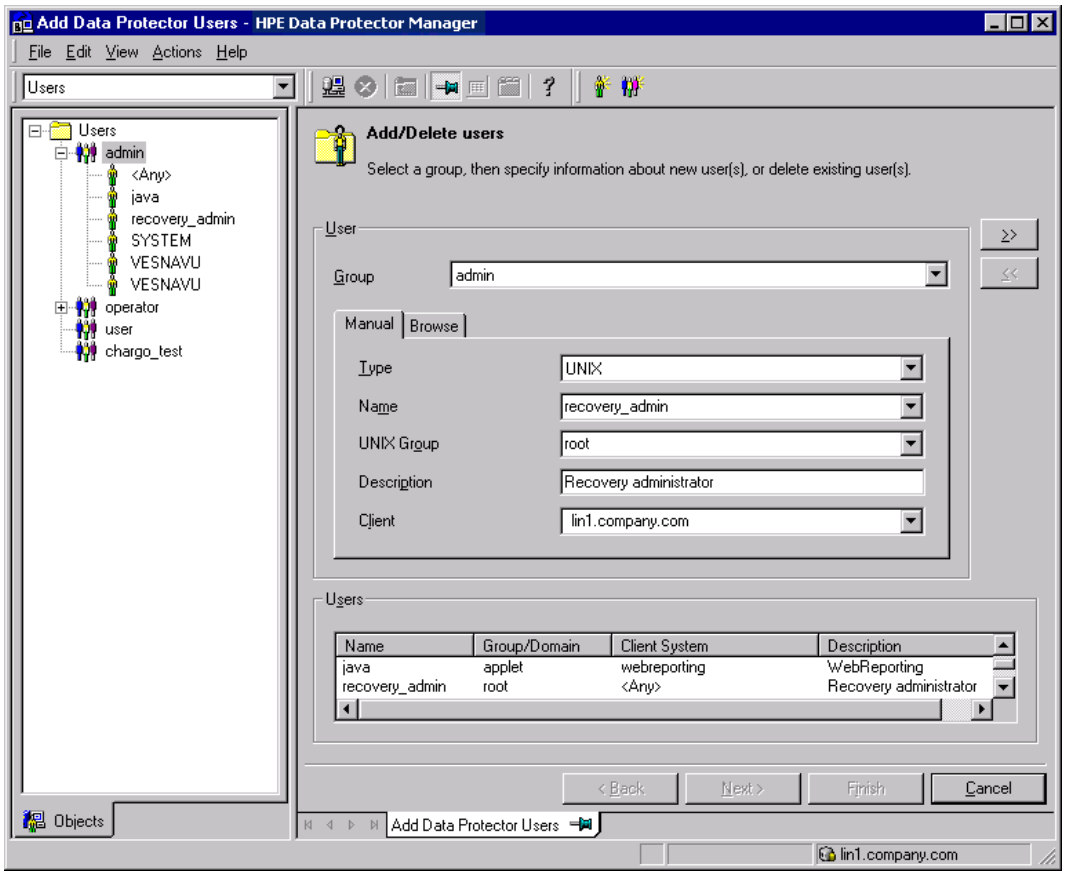
阶段 1

1. 除非要执行脱机灾难恢复，否则向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的 Data Protector admin 帐户：
   - 启动还原
   - 还原到其他客户机
   - 作为 root 还原

   > **注意：**
   > 灾难恢复过程只能由 root 用户执行。

   有关添加用户的详细信息，请参见《Data Protector 帮助》的索引：“添加 Data Protector 用户”。

   添加用户帐户



2. 从原始系统的灾难恢复 CD 引导客户机系统。
3. 显示以下消息时按 **Enter**：按 Enter 从恢复 CD 引导。
4. 首先将 DR OS 加载到内存中，然后显示范围菜单。 选择恢复范围。 有四种不同的恢

复范围和两个其他选项：

- Reboot：不执行灾难恢复，但重新启动计算机。
- Default Recovery：恢复 /boot 和 /(根)卷，以及 Data Protector 安装及配置文件所在的所有卷(/opt、/etc 和 /var)。 所有其他磁盘均未进行分区和格式化，可在阶段 3 中使用。
- Minimal Recovery：仅恢复 /boot 和 /(根)卷。
- Full Recovery：恢复所有卷，而不仅仅是关键卷。
- Full with Shared Volumes：恢复所有卷，包括在备份时锁定的共享卷。
- Run shell：运行 Linux shell。 可以将其用于高级配置或恢复任务。

> **注意：**
> 无论选择的恢复范围如何(默认、最低限度或完全恢复)，通过灾难恢复可恢复所有 BTRFS 卷和子卷。

阶段 2

5. 此时将显示灾难恢复向导。 要修改灾难恢复选项，请按任意键在倒数期间停止向导，然后修改选项。 要继续执行灾难恢复，选择**继续进行还原**。

   > **注意：**请确保 Cell Manager 和介质(备份)主机可访问。 否则，可能需要修改 NIC 和 MAC 地址。 有关详细信息，请参见 Cell Manager 和 RMA 主机未响应。

6. 如果灾难恢复备份经过加密，并且您要恢复 Cell Manager 或无法访问 Cell Manager 的客户机，则将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库 (DR-*ClientName*-keys.csv)(例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器)，并输入密钥库文件的完整路径。 密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。 现在将继续进行灾难恢复，不会再有其他中断现象。

7. 如果 SRD 文件中的信息并非最新(例如，因为灾难之后更改了备份设备)，并且要执行脱机恢复，则应在继续此过程之前编辑 SRD 文件。
8. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。

   请注意，Data Protector 将首先尝试执行联机还原。 如果联机还原因任何原因而失败(如 Cell Manager 或网络服务不可用，或防火墙正在阻止访问 Cell Manager)，则 Data Protector 将尝试执行远程脱机恢复。 甚至如果远程脱机还原失败(例如，因为介质代理主机仅接受来自 Cell Manager 的请求)，则 Data Protector 也将执行本地脱机还原。

9. 从 Cell Manager 上的 Data Protector admin 用户组中删除在第 1 步创建的客户机的本地 Data Protector 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。
10. 如果要恢复 Cell Manager，则要使 IDB 一致。

阶段 3

11. 使用标准 Data Protector 还原过程还原用户和应用程序数据。
12. 如果要执行群集中所有节点的灾难恢复，则需要其他步骤。

一键式灾难恢复 (OBDR)

一键式灾难恢复 (OBDR) 是针对 Linux Data Protector 客户机的自动 Data Protector 恢复方法，只需极少的用户干预。 有关支持的操作系统的详细信息，请参见最新的支持矩阵，网址为：https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

备份时，OBDR 将自动收集所有相关的环境数据。 备份期间，临时安装和配置 DR OS 所需的数据打包在单个大型 OBDR 映像文件(恢复集)中，并存储在备份磁带上。 灾难发生时，OBDR 设备(能够模拟 CD-ROM 的备份设备)用于直接从含有灾难恢复信息的 OBDR 映像文件所在的磁带引导目标系统。

然后，Data Protector 运行并配置灾难恢复操作系统 (DR OS)，对磁盘进行分区和格式化，最后使用 Data Protector 将原始操作系统还原到备份时的状态。

> **重要：**
> 每次硬件、软件或配置更改之后都要执行新的备份。 这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

OBDR 过程根据所选的恢复范围恢复卷。

使用标准 Data Protector 还原过程可恢复任何剩余的卷。

概述

确保已执行准备一章中提及的所有常规准备步骤。 对 Windows 客户机使用一键式灾难恢复方法的常规步骤包括：

1. **阶段 1**
   从恢复磁带引导并选择恢复范围。
2. **阶段 2**
   根据您所选的恢复范围，系统将自动还原所选的卷。
   关键卷(引导分区和操作系统)始终会被还原。
3. **阶段 3**
   使用标准 Data Protector 还原过程还原剩余的所有分区。

> **重要：**
> Micro Focus 建议限制对 OBDR 引导介质的访问。

以下各节将介绍有关在 Windows 系统上执行一键式灾难恢复的要求、限制、准备和恢复。

要求

- 在要允许使用此方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复组件。 此外，必须在将准备 DR OS 映像的系统上安装自动灾难恢复组件。 有关详细信息，请参见《*Data Protector 安装指南*》。
- 客户机系统必须支持从将用于 OBDR 的磁带设备引导。

  有关支持的系统、设备和介质的详细信息，请参见磁带硬件兼容性表和最新的支持矩阵，网址为：https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。
- 目标系统的硬件配置必须与原始系统相同。 其中包括 SCSI BIOS 设置(扇区重新映射)。
- 替换磁盘必须连接到相同总线上的相同主机总线适配器。
- 装有 Data Protector 的卷应至少有 800 MB 的可用空间。 此空间是创建临时映像所必需的。
- 必须为支持 OBDR 的设备创建具有不可追加介质使用策略和宽松介质分配策略的介质池。 只有此池中的介质可用于灾难恢复。
- 在 SAN 引导配置中，确保目标系统上的以下项目与原始系统上的一致。
  - 本地 HBA 的 BIOS 参数
  - SAN 磁盘 LUN 数目
- 在多路径 SAN 磁盘配置中，目标系统磁盘的 LUN 和 WWID 必须与原始系统上的一致。

限制

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。
- 一次只能在相同的 OBDR 设备上为一个所选的客户机或 Cell Manager 运行一键式灾难恢复备份会话。 必须在连接到本地的支持 OBDR 的单个设备上实现这一点。
- 不支持 USB 磁带存储设备。
- 如果某个装载点名为 `CONFIGURATION` 且包含目录 `SystemRecoveryData`，则不会备份目录 `SystemRecoveryData` 中的数据。
- 请勿使用磁盘 ID 装载磁盘，因为磁盘 ID 是唯一的，且取决于磁盘序列号。 在灾难恢复情况下，可能会替换磁盘，新的磁盘将具有新的 ID， 从而导致灾难恢复失败。
- 在 SELINUX 强制模式启用的情况下还原 Linux 客户机时，系统必须在恢复后对所有系统文件进行重新标记，此过程可能需要一段时间才能完成，具体取决于系统配置。 如果使用宽容模式，系统日志将包含大量 SELINUX 警告消息。
- 在选择了 CONFIGRATION/SYSTEMRECOVERYDATA 对象的情况下创建备份规范时，默认情况下会从备份中排除文件夹 `/opt/omni/bin/drim/log` 和 `/opt/omni/bin/drim/tmp`。
- 需要在恢复之前手动连接不在 MiniOS 引导时自动连接的 Fusion IO 磁盘。 将旧的 Fusion IO 磁盘替换为新磁盘或发生内部 Fusion IO 磁盘错误时，需要执行此操作。 在 MiniOS 中连接之前，需要使用特定工具对这些磁盘进行格式化。 要手动格式化 Fusion IO 磁盘并将其连接到系统，恢复开始之前需要在 MiniOS 中显示的 Linux shell 中运行以下命令：

- `fio-status` – 列出所有 Fusion IO 磁盘的状态。
- `fio-format [path]` – 执行 Fusion IO 磁盘的低级格式化。
- `fio-attach [path]` – 将 Fusion IO 磁盘连接到系统。

- 在脱机还原期间，稀疏文件将还原为其完整大小。 这可能会导致目标卷空间不足。

磁盘和分区配置

- 新磁盘的大小必须等于或大于崩溃的磁盘。 如果它大于原始磁盘，则多出的容量将保持为未分配的状态。
- OBDR 仅支持类型为 0x12(包括 EISA)和 0xFE 的供应商特有分区。

为一键式灾难恢复做的准备

要做好准备而使灾难恢复成功，请遵照与灾难恢复常规准备过程相关的说明，然后再执行本主题中列出的步骤。 提前准备，以便快速高效地执行灾难恢复。

> **重要：**
> 请在灾难发生之前准备灾难恢复。

准备步骤

完成灾难恢复的常规准备之后，执行以下特定步骤以准备 OBDR。

1. 为 DDS 或 LTO 介质创建一个采用**不可追加**介质使用策略和**宽松**介质分配策略的介质池(因为备份介质在 OBDR 备份期间进行格式化)。 此外，将此介质池指定为 OBDR 设备的默认介质池。 请参见《*Data Protector 帮助*》的索引：“创建介质池”。 只有此类池中的介质可用于 OBDR。
2. 在要允许使用 OBDR 进行恢复的系统上本地执行 OBDR 备份。

   如果对客户机完整备份进行加密，则要将加密密钥存储在可移动介质上，以使其可供灾难恢复使用。 如果无法建立和 Cell Manager 之间的连接，您将需要密钥。
3. 执行灾难恢复测试计划。

创建一键式灾难恢复的备份规范

必须创建一键式灾难恢复 (OBDR) 备份规范，才能准备好 OBDR 引导磁带。

先决条件

- 添加 OBDR 设备前，为 DDS 或 LTO 介质创建一个采用不可追加介质使用策略和宽松介质分配策略的介质池。 必须选择所创建的该介质池作为 OBDR 设备的默认介质池。
- 此设备必须在本地连接到要允许使用 OBDR 进行恢复的系统。
- 在要允许使用 OBDR 方法进行恢复的系统上必须安装 Data Protector 自动灾难恢复和用户界面组件。
- 必须在要允许使用 OBDR 进行恢复的系统上本地创建备份规范。

提示：
为了能够使用 OBDR 方法自动还原 MS 群集中的所有共享磁盘卷，请将所有卷临时移至正在为其准备 OBDR 引导磁带的节点。 实际上无法收集足够的信息为由另一个节点锁定的共享磁盘卷配置处于阶段 1 的磁盘。

限制

- 一键式灾难恢复 (OBDR) 不适用于 Data Protector Cell Manager。

创建 **OBDR** 的备份规范

步骤

1. 在 Data Protector 上下文列表中，单击**备份**。
2. 在范围窗格中，单击**任务**，然后单击**一键式灾难恢复向导**。
3. 在“结果区域”中，从下拉列表中选择要为其执行 OBDR 备份(在客户机上本地)的客户机，然后单击**下一步**。
4. 此时已选择需要备份的关键卷。 单击**下一步**。

   重要：
   重要卷由系统自动选择，并无法取消选择。 选择要保留的任何其他分区，因为在恢复过程中 Data Protector 将从系统中删除所有分区。
5. 选择要用于备份的本地设备或驱动器。 只能选择一个设备或驱动器。 单击**下一步**。
6. 选择备份选项。 有关可用选项的更多详细信息，请参见《*Data Protector 帮助*》的索引：“备份选项”。
7. 单击“下一步”转到“计划程序”页面，此页面可用于计划备份。 请参见《*Data Protector 帮助*》的索引：“计划特定日期和时间的备份”。
8. 在“备份摘要”页中，查看备份规范设置，然后单击**下一步**。

   注意：
   无法更改以前选择的备份设备或备份规范相互之间的先后顺序。 仅可删除 OBDR 非必需备份对象，并且只能查看常规对象属性。

   也可以更改备份对象说明。
9. 在备份向导的最后一个页面上，您可以保存备份规范、保存并计划备份、启动交互式备份或预览备份。

   Micro Focus 建议保存备份规范以便可在随后计划或修改该规范。

   保存备份规范后，可以对其进行编辑。 右键单击备份规范并选择“属性”。 建议您将修改后的备份规范视为标准 Data Protector 备份规范或 OBDR 备份规范。 将其另存为 OBDR 备份规范以确保不会覆盖其中的 OBDR 特有选项。 如果将其另存为标准备份规范，则可能无法将其用于 OBDR 目的。
10. 单击“启动备份”以交互方式运行备份。 此时将显示“启动备份”对话框。 单击“确定”开始备份。

    如果备份为加密备份，则 omnisrdupdate 实用程序将自动导出加密 ID，此操作作为 post-exec 命令执行。

系统的可引导映像文件(包含安装和配置临时 DR OS 所需的所有信息)将写在磁带的开头，以使其可引导。

> **重要：**
> 每次硬件、软件或配置更改之后执行新的备份并准备好可引导的备份介质。 这一点也适用于任何网络配置更改，如 IP 地址或 DNS 服务器的更改。

准备加密密钥

对于 Cell Manager 恢复或脱机客户机恢复，必须通过在可移动介质上存储加密密钥，确保灾难恢复期间有加密密钥可用。 对于 Cell Manager 恢复，请在灾难发生之前提前准备可移动介质。

加密密钥不是 DR OS 映像文件的一部分。 在创建灾难恢复映像期间，密钥将自动导出到 Cell Manager 的文件 *Data_Protector_program_data*\Config\Server\export\keys\DR-*ClientName*-keys.csv(Windows 系统)或 /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv(UNIX 系统)，其中 *ClientName* 是正在创建映像的客户机的名称。

确保对于为灾难恢复准备的每个备份都有正确的加密密钥。

使用 OBDR 恢复 Linux 系统

只有在完成所有准备步骤后，才能成功执行 Linux 系统的一键式灾难恢复 (OBDR)。

有关 OBDR 所支持的操作系统的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

先决条件

- 需要用新硬盘更换受影响的磁盘。
- 应有一个可引导 OBDR 备份介质，其中含有要恢复的客户机的所有关键对象。 必须在客户机上本地执行 OBDR 备份。
- 需要一个在本地连接到目标系统的 OBDR 设备。

步骤

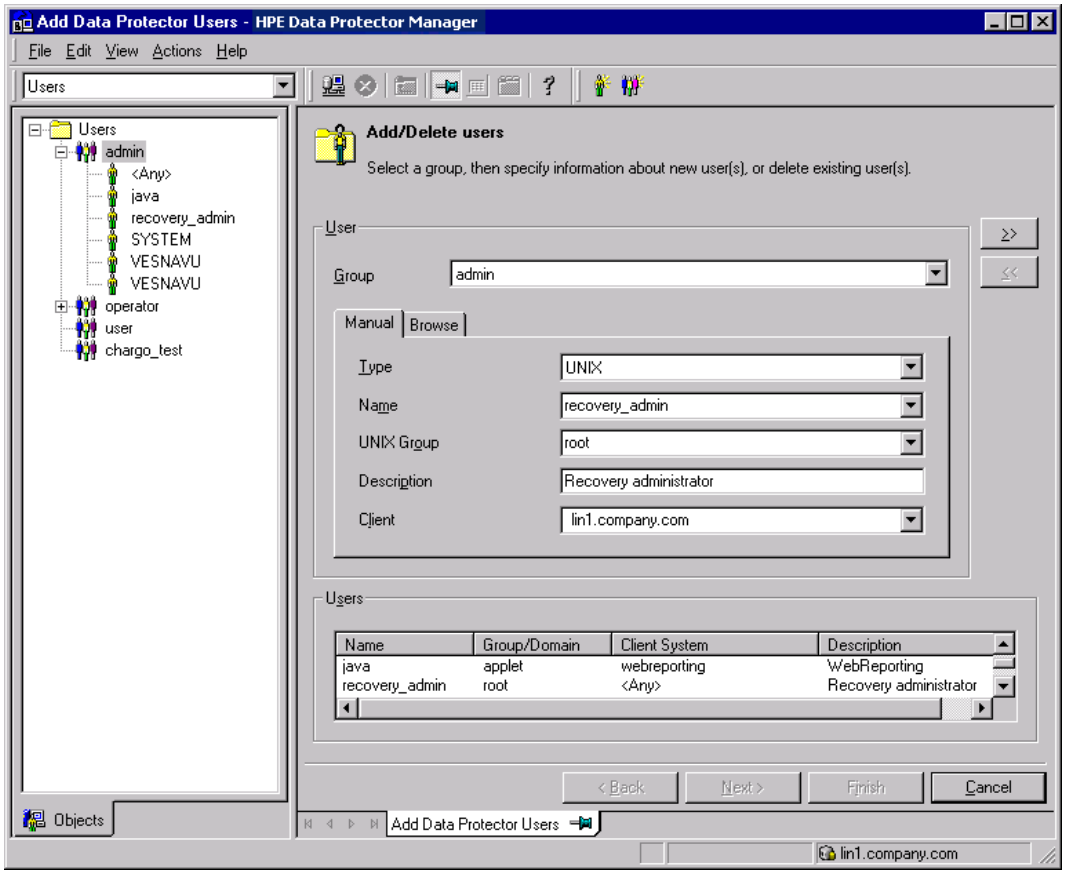
阶段 1

1. 除非要执行脱机灾难恢复，否则根据目标系统的操作系统，要向 Cell Manager 上的 Data Protector admin 用户组添加具有以下属性的 Data Protector admin 帐户：
   - 启动还原
   - 还原到其他客户机
   - 作为 root 还原

> **注意：**
> 灾难恢复过程只能由 root 用户执行。

有关添加用户的详细信息，请参见《Data Protector 帮助》的索引：“添加 Data Protector 用户”。

添加用户帐户



2. 将包含映像文件和备份数据的磁带插入 OBDR 设备中。
3. 关闭目标系统，并关闭磁带设备的电源。
4. 打开目标系统的电源，并在其初始化时，按磁带设备上的“弹出”按钮，并打开该设备的电源。 有关详细信息，请参见设备文档。
5. 首先将 DR OS 加载到内存中，然后显示范围菜单。 选择恢复范围。 有四种不同的恢复范围和两个其他选项：
   - `Reboot`：不执行灾难恢复，但重新启动计算机。
   - `Default Recovery`：恢复 `/boot` 和 `/`(根)卷，以及 Data Protector 安装及配置所在的所有卷(`/opt`、`/etc` 和 `/var`)。 所有其他磁盘均未进行分区和格式化，可在阶段 3 中使用。
   - `Minimal Recovery`：仅恢复 `/boot` 和 `/`(根)卷。
   - `Full Recovery`：恢复所有卷，而不仅仅是关键卷。

- `Full with Shared Volumes`：恢复所有卷，包括在备份时锁定的共享卷。
- `Run shell`：运行 Linux shell。 可以将其用于高级配置或恢复任务。

阶段 2

6. 此时将显示灾难恢复向导。 要修改灾难恢复选项，请按任意键在倒数期间停止向导，然后修改选项。 选择“继续进行还原”以继续执行灾难恢复操作。
7. 如果灾难恢复备份已加密，并且要恢复其 Cell Manager 无法访问的客户机，将显示以下提示：

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   按 **y**。

   确保客户机上存在密钥库 (`DR-ClientName-keys.csv`)(例如，通过插入 CD-ROM、软盘或 USB 闪存驱动器)，并输入密钥库文件的完整路径。 密钥库文件将复制到在 DR OS 中的默认位置，并由磁盘代理使用。 现在将继续进行灾难恢复，不会再有其他中断现象。
8. 如果 SRD 文件中的信息并非最新(例如因为灾难之后更改了备份设备)，并且要执行脱机恢复，则在继续此过程之前请编辑 SRD 文件。
9. 然后，Data Protector 将在所选的恢复范围内重建以前的存储结构，并还原所有关键卷。

   注意，Data Protector 将首先尝试执行联机还原。 如果联机还原因任何原因而失败(如 Cell Manager 或网络服务不可用，或防火墙正在阻止访问 Cell Manager)，则 Data Protector 将尝试执行远程脱机恢复。 如果远程脱机还原失败(如因为介质代理主机仅接受来自 Cell Manager 的请求)，则 Data Protector 将执行本地脱机还原。
10. 从 Cell Manager 上的 Data Protector `admin` 用户组中删除在第 1 步创建的客户机的本地 Data Protector 帐户，除非灾难恢复之前 Cell Manager 上就存在该帐户。

阶段 3

11. 如果要恢复 Cell Manager 或执行高级恢复任务，还需要执行其他步骤(例如编辑 SRD 文件)。
12. 使用标准 Data Protector 还原过程还原用户和应用程序数据。

第 5 章： 灾难恢复故障排除

本章包含执行灾难恢复时可能遇到的问题的说明。您可先从关于特定灾难恢复方法入手，然后了解常规灾难恢复问题。有关从何处查找错误消息的信息，请参见灾难恢复故障排除 (第 106 页)。

有关 Data Protector 常规故障排除的信息，请参见*Data Protector 故障排除指南*。

开始之前

- 确保已安装最新的正式 Data Protector 修补程序。有关如何验证的详细信息，请参见《Data Protector 帮助》的索引："修补程序"。
- 有关常规 Data Protector 限制以及已知问题和解决方法，请参见*Data Protector 产品声明、软件说明和参考*。
- 有关受支持设备、平台的最新列表及其他信息，请参见 https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=。

自动灾难恢复故障排除

AUTODR.log 文件

自动灾难恢复包括两种灾难恢复方法：EADR 和 OBDR。与这些方法相关的消息记录在 AUTODR.log 文件中，该文件位于默认的 Data Protector 临时文件目录中。如果发生错误，应该检查该文件。

AUTODR.log 记录了许多不同的消息，主要用于开发和支持。其中只有一部分与您相关并指示发生了错误。通常在日志文件的末尾记录这些错误消息，并在后面追加 traceback。

AUTODR.log 文件中有四个消息级别(请注意，它们并非与 Data Protector GUI 中备份会话末尾报告的消息的相同报告级别相对应)：

- Critical error：错误很严重，以致于对象的备份无法继续并将中止。
- Error：有错误，但是否为关键错误取决于不同因素。

  例如，AUTODR.log 报告一个错误：DR OS 中尚未包括某些驱动程序。缺少驱动程序可能是经过恢复的系统在恢复之后无法使用的原因。这种情况还可能会导致引导操作系统之后某些非关键服务不运行。错误的严重性取决于未备份哪个驱动程序。
- Warning 和 Info：这些不是错误消息，通常并不表示有什么错误。

AUTODR.log 文件中所述的两个最常见的消息为：

- unsupported location：Data Protector 声明 *%SystemRoot%* 目录下没有 DR OS 中应包括的服务或驱动程序所需的某个文件。

  防病毒和远程控制软件(例如 pcAnywhere)通常使用此类驱动程序。此消息很重要，因为它可能表示服务/驱动程序需要缺少的文件，因此在引导之后无法正常运行。灾难恢复的成功取决于哪个服务或驱动程序受到了影响。对于此问题可能的解决方案是将缺少的文件复制到

%SystemRoot% 目录中，并在 Windows 注册表中更改其路径。 请注意，错误地编辑 Windows 注册表可能对系统造成严重损坏。

调试灾难恢复会话

在灾难恢复会话期间，调试设置和调试日志位置取决于灾难恢复阶段：

- 在 DR OS 准备期间，调试日志会自动保存到 `X:\$DRM$\log`(Windows Vista 及更高版本)、`c:\$DRM$\log`(Windows XP、Windows Server 2003)或 `/opt/omni/bin/drim/log/Phase1.log` (Linux 系统)。
- 在数据还原步骤期间，必须在灾难恢复向导中手动选择调试选项以启用调试。

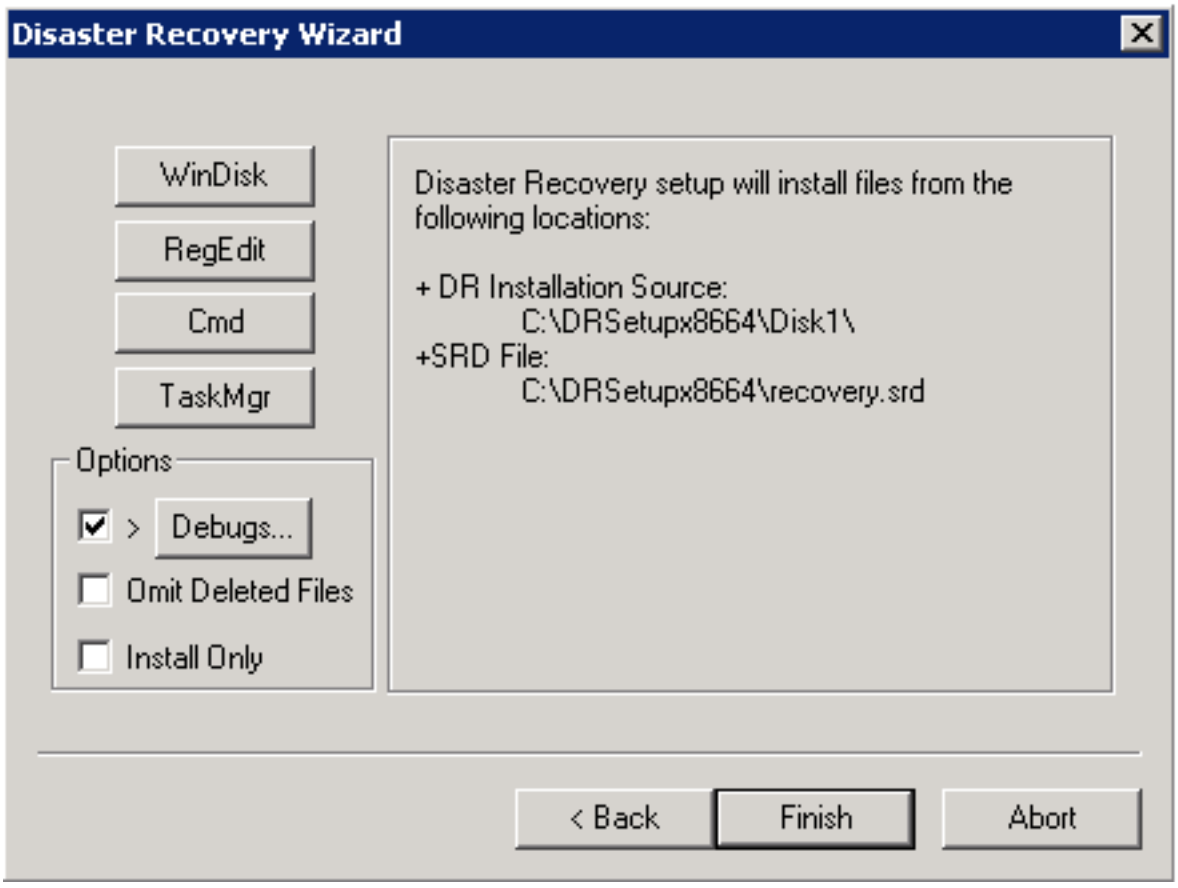
Windows

要创建调试日志：

1. 在灾难恢复向导中，按任意键在倒数期间停止向导。

   选中“调试”按钮左侧的复选框。

   在灾难恢复会话期间启用调试

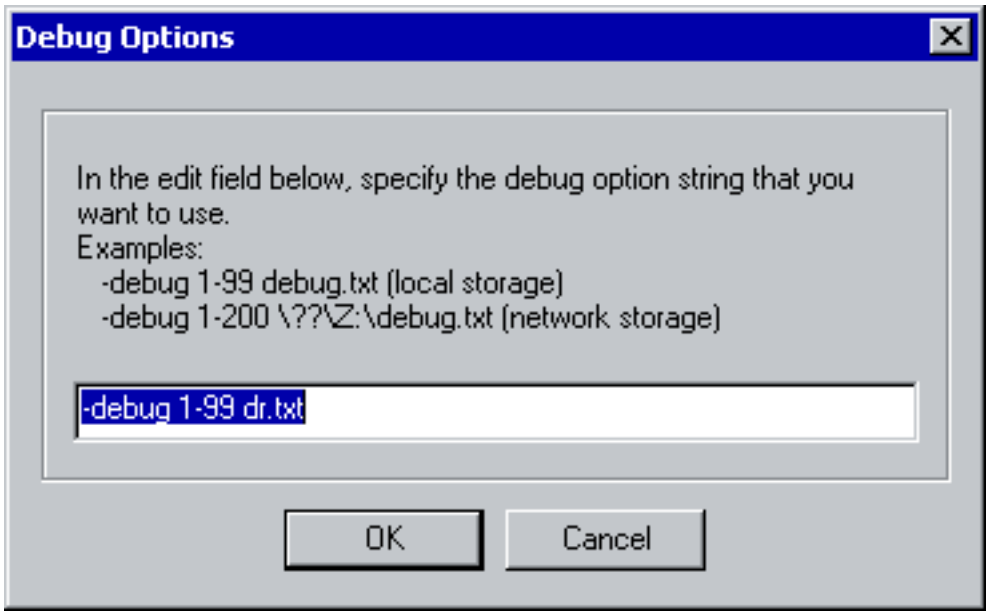


2. 要指定调试选项(如保存调试的位置)，请单击**调试...**。 默认情况下，调试信息保存到 *%SystemRoot%*\system32\OB2DR\tmp 目录中。

> **注意：**
> 在 Windows Vista 及更高版本中，目录 *%SystemRoot%*\system32\OB2DR\tmp 位于 RAM 磁盘上。 RAM 磁盘的大小通常限制为小于 64 MB。 RAM 磁盘用量达到限制后，Data Protector 的行为可能会变得无法预测。 因此，如果预计灾难恢复会话将产生大量调试，则必须更改调试将保存到的位置。

此时将显示“调试选项”窗口。

更改调试日志的位置



3. 输入保存调试日志的位置。 驱动器前面必须带有 \\?，例如 \\?\Z:\debug.txt。 如果选择在网络共享上保存调试，则使用 net use 命令装载向其写入调试日志的共享。 例如， `net use X: "\\client\debug_output_folder /user:username password".`

Linux 系统

要创建调试日志：

1. 在灾难恢复向导中，选择**使用调试**。
2. 在调试选项屏幕上，选择使用默认选项或选择对默认选项进行修改。

```
Select one of following options:
1) Use Default Debug Option "-debug 1-200 dr.txt"
2) Specify Different Debug Option
3) Disable Debug option
Command [1-3]:
```

> **注意：**
> 在 Linux 系统上，保存调试日志的目录位于 RAM 磁盘上。 RAM 磁盘大小通常是有限的。 RAM 磁盘用量达到限制后，Data Protector 的行为可能会变得无法预测。 因此，如果预计灾难恢复会话将产生大量调试，则应当更改调试将保存到

> 的位置。 若要更改位置，请选择**指定其他调试选项**。

3. 将出现一个新屏幕，您可以在该屏幕上输入调试参数。

   Examples:

   -debug 1-200 debug.txt (local storage)

   -debug 1-200 //servername/sharename/debug.txt (windows share)

   -debug 1-200 servername:/sharename/debug.txt (nfs share)

   Specify the debug option string that you want to use:

   可以选择将调试文件保存到 Windows 共享磁盘或 NFS 共享文件夹。

在灾难恢复期间设置 omnirc 选项

有关 omnirc 选项的常规信息，请参见《*Data Protector 故障排除指南*》。

如果需要在 Windows 或 Linux 系统中的灾难恢复期间设置 omnirc 选项，则执行以下步骤：

Windows 系统

1. 显示灾难恢复向导时，按任意键在倒数期间停止向导。
2. 单击 **Cmd** 启动命令提示符。
3. 运行以下命令：

   echo variable > *%SystemRoot%*\system32\OB2DR\omnirc

   其中，variable 是 omnirc 选项，与应在 omnirc 文件中写入的完全一样。

   例如：

   echo OB2RECONNECT_RETRY=1000 > *%SystemRoot%*\system32\OB2DR\omnirc

   此命令在灾难恢复操作系统中创建一个将 OB2RECONNECT_RETRY 选项设置为 1000 秒的 omnirc 文件。
4. 关闭命令提示符，然后在灾难恢复向导中单击**下一步**以继续灾难恢复。

Linux 系统

1. 在灾难恢复向导中，通过按 **Alt F3**，切换到另一个控制台。
2. 在控制台中，运行以下命令：

   echo *variable* > /opt/omni/.omnirc

   其中，*variable* 是 omnirc 选项，与应在 .omnirc 文件中写入的完全一样。

   示例：

   echo OB2RECONNECT_RETRY=1000 > /opt/omni/.omnirc

   此命令在灾难恢复操作系统中创建一个将 OB2RECONNECT_RETRY 选项设置为 1000 秒的 .omnirc 文件。
3. 键入 **exit** 退出 shell，并在灾难恢复向导中继续进行灾难恢复。

Windows 上的 drm.cfg 文件

Data Protector 灾难恢复配置经过精心设置，以适用于大量系统配置。 但是，在某些情况下，这些设置可能不是最合适的，或者可能要修改某些设置才能排除系统中的问题。

drm.cfg 文件包含可以修改并影响灾难恢复过程的几个参数，及其影响的说明。 此文件对 EADR 和 OBDR 可用。

要更改参数：

1. 将模板文件 drm.cfg.tmpl 复制为 drm.cfg。 安装或升级期间将在 *Data_Protector_home*\bin\drim\config 中创建模板，并将所有参数设置为默认值。
2. 编辑 drm.cfg 文件。 为参数设置所需的值。 按照文件中的说明进行操作。

禁止自动收集 EADR 或 OBDR

运行客户机完整备份时，CONFIGURATION 备份可能会在收集某种备份方法所需的数据时失败，即使此方法不用于灾难恢复也是如此，因为 Data Protector 默认情况下收集所有自动灾难恢复方法的数据。 例如，如果引导磁盘为 LDM 磁盘，则 Data Protector 收集 EADR 的数据时可能会发生这种情况。

禁用对灾难恢复方法数据已失败的自动收集。 这样将允许 Data Protector 收集其他方法所需的数据。

将 OB2_TURNOFF_COLLECTING 选项设置为以下值之一：

值	说明
0	默认设置，打开对所有自动方法(EADR、OBDR)的数据收集。
1	关闭对 EADR/OBDR 数据的收集
2	仍收集 EADR/OBDR 数据。
3	关闭对所有方法的收集。

常见问题(所有方法)

执行灾难恢复时，可能会发生以下问题：

无法从介质副本或对象副本执行灾难恢复

问题
无法从介质副本或对象副本执行灾难恢复。 默认情况下，Data Protector 使用原始介质集执行灾难恢复。 因此，灾难恢复向导中不显示副本对象版本。

操作

- 对象复制：从 IDB 导出原始介质集中的所有介质，然后重新生成 SRD 文件。 然后，Data Protector 在灾难恢复向导中向您提供原始介质集的第一个可用复本。
- 介质复制：在 SRD 文件中，将原始介质的介质 ID 替换为介质复本的介质 ID。 然后，Data Protector 在灾难恢复向导中向您提供原始介质集的第一个可用复本。

在灾难恢复完成后，您将无法登录

问题

灾难恢复结束之后登录系统时出现问题。

可能会收到以下消息：

```
The system cannot log you on to this domain, because the system's computer account in its primary domain is missing or the password on that account is incorrect.
```

此类消息可能由以下某个原因导致：

- 收集灾难恢复的所有信息之后，重新安装了 Windows，并将其添加到问题域中。
- 收集灾难恢复的所有信息之后，从冲突域删除了系统，随后将其添加到同一域或其他某个域中。

在类似这种情况下，Windows 将生成新的系统安全信息，这些信息与灾难恢复期间还原的信息不兼容。

操作

1. 以管理员身份从本地登录系统。
2. 在控制面板中，单击**网络**，然后使用**标识**选项卡从系统的当前域将系统移至一个临时工作组。
3. 将系统重新插入以前从中移出该系统的域中。 需要域管理员密码。 单击**确定**。
4. 重新启动系统。

要更新此新状态，请重复灾难恢复的所有必要的准备步骤。

由于网络设置不当，灾难恢复失败

问题

由于 Data Protector 恢复一个具有不当网络配置的客户机，导致灾难恢复会话失败。

用于配置客户机网络的默认设置取决于客户机的操作系统：

Windows XP、Windows Server 2003：

在 SRD 文件中指定的原始网络配置(备份时的网络配置)。

Windows Vista 和更高版本：

由 DHCP 设置定义的网络配置。
操作
要切换到非默认的网络配置： 1. 启动灾难恢复会话。 2. 如果 Data Protector 显示： **Windows XP、Windows Server 2003：** 在下面的 10 秒钟内按 F8 将网络切换到 DHCP... **Windows Vista 和更高版本：** 在下面的 10 秒钟内按 F8 切换到备份时的网络设置... 按 **F8**。

对 BTRFS 型文件系统的支持有限

问题
对 BTRFS 型文件系统的支持有限。 如果装载的 btrfs 子卷具有子子卷，则备份期间将跳过子子卷中的数据。 子子卷将作为空文件夹来备份。
操作
1. 将每个子卷装载为新的装载点。 2. 在备份规范中配置新的装载点。

灾难恢复期间显示错误消息

问题
在灾难恢复期间，显示以下错误消息： `Failed to perform post-DR operations`
操作

要完成灾难恢复进程，请手动运行 omnicc 命令。
• 对于联机恢复：在 Cell Manager 上运行以下命令：
`omnicc -secure_comm –configure_peer <hostname_of_client_being_recovered> -overwrite`
• 对于脱机恢复：在介质代理上运行以下命令：
`omnicc -secure_comm -remove_peer <hostname_of_client_being_recovered>`

辅助手动灾难恢复故障排除

执行辅助手动灾难恢复时，可能会发生以下问题：

“Cannot copy file”

问题
Drstart 报告：“Can not copy *filename*."
报告此错误是因为 *drstart* 实用程序无法复制指定的文件。 其中一个原因可能是系统锁定了该文件。 例如，如果 *drstart* 无法复制 *omniinet.exe*，则可能是因为已在运行 Inet 服务。 这不是正常情况，并且不应在全新安装之后发生。
操作
此时将显示一个对话框，询问您是否要继续复制其余文件。 如果单击**是**，则 drstart 将跳过锁定的文件，继续复制其他文件。 如果系统锁定了文件，则这样做即可解决问题，由于灾难恢复所需的进程已在运行，因此不需要复制该文件。 还可以通过单击**中止**关闭 drstart 实用程序。

增强型自动灾难恢复和一键式灾难恢复故障排除

在使用增强型自动灾难恢复或一键式灾难恢复方法期间您可能会遇到以下问题：

连接到系统的 D2D 网关恢复时，Linux 上的 EADR 联机还原失败

带有已分离 SAN-LVM 卷的 RHEL EADR 不起作用 (第 121 页)

未能收集自动 DR 信息

问题
使用 EADR 或 OBDR 时，可能会收到以下错误：“Automatic DR information could not be collected. Aborting the collecting of system recovery data”。
操作

可能导致此错误的原因存储在位于默认 Data Protector 临时文件目录的 autodr.log 文件中：
1. 检查是否正确配置了所有存储设备。 如果设备管理器将设备报告为“未知设备”，则必须安装正确的设备驱动程序，然后才能执行 EADR/OBDR。 如果有配置错误的存储设备连接到系统，则 autodr.log 中会显示类似条目：
`DRIM_WIN_ERROR 13 SetupDiGetDeviceRegistryProperty`
2. 必须有足够的注册表空间可用。 建议将最大注册表大小至少设置为当前注册表大小的两倍。 如果没有足够的注册表空间可用，则 autodr.log 中会显示类似条目：
`ERROR registry 'Exception while saving registry' .... WindowsError: [Errno 1450] Insufficient system resources exist to complete the requested service.`

3. 确保已启用自动装载功能。 自动装载功能可确保所有卷(没有装载点)都处于联机状态。 如果禁用了自动装载，没有驱动器盘符的所有卷在引导过程中都处于脱机状态。 因此，系统保留分区将无权访问驱动器盘符，这可能会导致灾难恢复过程失败。

   如果需要禁用自动装载功能，则确保已装载系统保留分区。

如果仍然存在问题，请卸载 Data Protector 自动灾难恢复组件(以便至少可以进行手动灾难恢复)，然后与技术支持人员联系。

检测到某些非关键错误

问题
使用 EADR 或 OBDR 时，可能会收到以下错误：“Some non-critical errors were detected during the collecting of Automatic DR data. Review the Automatic DR log file.
操作
执行自动灾难恢复模块期间检测到非关键错误意味着备份很可能仍用于灾难恢复目的。 可能导致非严重错误的原因存储在位于默认 Data Protector 临时文件目录的 autodr.log 中。 例如： *%SystemRoot%* 文件夹以外的服务或驱动程序(例如病毒扫描程序)。 Autodr.log 会包含类似的错误消息： `ERROR safeboot 'unsupported location' 'intercheck support 06' 2 u'\\??\\D:\\Program Files\\Sophos SWEEP for NT\\icntst06.sys'.` 可以忽略此错误消息，因为它不影响灾难恢复的成功。

从带有计划网关的 StoreOnce/DDBoost 设备创建设备时，还原会话失败

问题

从带有计划网关的 StoreOnce/DD Boost 设备配置设备，并且配置同一客户端用于灾难恢复时，还原会话将会结束，并在 Cell Manager 上显示以下警告消息：
`[Major] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM`
`[61:3003] Lost connection to B2D gateway named "DeviceName" on host <hostname>`
`Ipc subsystem reports: "unknown"`
`[Warning] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM`
`Device <DeviceName> is disabled and will not be used.`
此错误是由于丢失与客户机 B2D 网关的连接而发生的。

操作
忽略还原会话结束时显示的警告消息。 增强自动灾难恢复将会成功，您可以在客户机恢复控制台上查看结果。

还原期间网络不可用

问题
有多种原因可以导致此问题，例如网络电缆或开关损坏。 网络故障另一个可能的原因是 DNS 服务器(备份时配置)在还原期间脱机。 由于 DR OS 的配置与备份同时进行，因此网络将不可用。
操作
1. 请确保不是开关、电缆等问题。 2. 如果 DNS 服务器(备份时配置)在还原期间脱机，则可以： • 执行脱机恢复，并且在恢复之后更改 DNS 设置。 • 开始阶段 2 之前编辑注册表。 在这种情况下，必须在阶段 2 之前重新启动系统，更改才能生效。 阶段 2 结束之后，必须更正设置，然后才能开始阶段 3。 **警告：** 错误地编辑注册表可能会导致灾难恢复失败。

连接到系统的 D2D 网关恢复时， Linux 上的 EADR 联机还原失败

问题
将 D2D 设备用于 EADR 联机还原时，RMA 失败并显示以下错误消息： `[61:1005] Got unexpected close from RMA on clientsystem.domain.org if the gateway is configured on the same EADR system`
操作
删除分配给正在恢复的 DR 系统的网关并添加一个新网关。 有关如何重新配置网关的详细信息，请参见《*HPE 重复数据删除指南*》。

因缺少网络驱动程序而无法使用网络

问题
在 Windows Vista 或 Windows Server 2008 系统中，灾难恢复期间网络不可用，因为 DR OS 不支持网卡。

操作
将缺少的驱动程序插入到 DR OS 映像中。

当 Cell Manager 和客户机位于不同的域时， EADR 和 OBDR 联机恢复失败

问题
这可能是由于错误的网络配置导致。
操作
1. 在 Cell Manager 和客户机系统上更新 host 文件。 这些文件必须包含 Cell Manager 和客户机的主机名及其 IP 地址。 2. 检查 Cell Manager 和客户机之间的 ping 请求是否返回正确的值。 如果发生问题，请联系您的网络管理员。 3. 使用 omnicheck -dns 命令检查 Cell Manager 和客户机之间的 DNS 解析是否正确。 有关更多详细信息，请参见 omnicheck 手册页或《*Data Protector 命令行界面参考*》。 如果发生问题，请联系您的网络管理员。

自动登录不起作用

问题
有时自动登录不起作用。
操作
使用密码为空的管理员帐户手动登录。

EADR 期间计算机停止响应

问题
灾难恢复 CD 有问题可能会导致这种情况。
操作
• 检查 CD 是否可读。 • 请勿重复使用 CD-RW 过多次数。

无法为 Microsoft 群集服务器的 EADR 创建 CD ISO 映像

问题
必须备份仲裁磁盘，以便能够创建 CD ISO 映像。
操作
备份仲裁磁盘。

在 Microsoft 群集服务器客户机上创建 CD ISO 映像的操作失败

问题
在 Microsoft 群集服务器环境中，不能在群集客户机上创建 ISO 映像。 文件系统还原将按预期执行。 出现问题的原因是 Data Protector 尝试使用群集 IP 地址(是虚拟地址)而不是域名(解析为物理客户机的 IP 地址)。
操作
更改网络服务的连接顺序，使得Local Area Connection位于顶部。

介质创建主机上安装了防病毒软件时，创建 ISO 映像失败

问题
使用 WAIK/ADK 创建 ISO 映像并且在介质创建主机上安装防病毒软件后，创建 ISO 映像失败并显示以下错误消息： 在 GUI 中： ISO 映像创建失败。 请检查位于 Data Protector 临时目录中的 autodr 日志。 在 autodr.log 文件中： “添加包 (Add-Package)”操作失败并显示“访问被拒绝 (Access Denied) (5)”错误。
操作
临时禁用介质创建主机上的防病毒代理，直至完成 ISO 映像创建过程。

加密功能基于驱动器时，使用 omniiso 创建 ISO 映像失败

问题

在备份规范中禁用**基于驱动器的加密**后，从备份会话创建 ISO 映像失败，并显示以下错误消息：

[Major] From: omniiso@computer.company.com "omniiso" Time: <DateTime>

Error updating SRD file objects [error: -1]. Aborting.

以下情况会出现错误消息：

- 如果任何后续备份在备份规范中启用了**基于驱动器的加密**。
- 如果目标驱动器与创建 iso 映像并获取发往不同介质的后续备份的会话中的目标驱动器相同。

由于没有为第一个介质创建密钥库，因此会出现该问题。 当驱动器被后续备份标记为已加密时， omniiso 尝试为第一个介质导出加密密钥，并失败。

操作

- 将未加密的备份移到其他已禁用基于驱动器的加密的驱动器，并重新运行 omniiso。
- 避免在启用/禁用**“基于驱动器的加密”**的情况下运行到同一目标驱动器的备份。

阶段 1 期间不重新装载卷

问题

在某些系统中(取决于磁盘控制器及其配置)，灾难恢复的阶段 1 期间无法正确重新装载与不同卷上的装载点关联的卷(未分配驱动器号)。 如果重新创建或重新格式化包含装载点的卷(例如含有 DR OS 的系统卷)，导致操作系统以“安全模式”引导，以及检测不到原始装载点的目标卷上存在的文件系统。 因此，灾难恢复模块无法识别此卷，并且在 drecovery.ini 文件中将其报告为 MISSING。 此类卷的内容保留原样，即使无法识别该卷也是如此。

操作

- 装载含有驱动器号的卷，并用 chkdsk /v /f 命令验证该卷，或等待至系统完全还原为止，然后重新创建原始装载点。
- 手动将系统直接重新启动至 MiniOS(不从恢复 CD 启动)。 以前卸载的卷将自动装载到驱动器号。

灾难恢复失败或中止之后保留引导描述符

问题

在 Intel Itanium 系统中，失败或中止的灾难恢复会话之后，可能在 EFI 环境中保留引导描述符(名为 DRM Temporary OS)。 重新开始灾难恢复过程时，这可能会导致多余的行为。
操作
从范围选择菜单中使用**删除引导描述符**选项删除引导描述符。 删除引导描述符之后，可以通过选择范围继续灾难恢复。

在 Intel Itanium 系统中选择了错误或非引导的磁盘

问题
在 Intel Itanium 系统中，选择了错误的引导磁盘(或根本就是非引导磁盘)。
操作
1. 从范围选择菜单中选择**手动选择磁盘**。 此时将显示一个新菜单，其中列出所有可用的磁盘。 2. 确定正确的引导磁盘。 按 **o** 查看有关原始磁盘的信息，按 **d** 查看有关所选磁盘的详细信息。 3. 使用光标键从列表中选择磁盘，然后按 **b**。 通过按 **c**，可以删除某个选择。 如果引导磁盘与系统磁盘不同(默认情况下这两个磁盘相同)，则还必须选择系统磁盘。 选择**返回**。 4. 选择恢复的范围，然后将继续灾难恢复。

灾难恢复失败，并显示消息“空间不足”

问题

对 Windows Server 2008 R2 域控制器执行的灾难恢复失败，并显示类似如下所示的错误消息：
`[Major] From: VRDA@computer.company.com "Dev1" [/CONFIGURATION]" Time:`
`07.12.2012 15:33:58 X:\windows\System32\OB2DR\tmp\config\`
`ActiveDirectoryService\D$\ Windows\NTDS\ntds.dit Cannot write:`
`([112] There is not enough space on the disk. ) => not restored.`

操作
1. 修改客户机备份的备份规范：在源页面中，展开 CONFIGURATION 对象，并清除 ActiveDirectoryService 和 SYSVOL 项目的复选框。 **注意：** Active Directory 和 SYSVOL 将仍作为系统卷 (C:/) 备份的一部分进行备份。 默认情况下，它们分别位于 C:/Windows/NTDS 和 C:/Windows/SYSVOL 中。

2. 重复灾难恢复过程。

Windows 8.1 客户机灾难恢复失败，并显示“无法写入: ([13] 数据无效。) => 未还原。” 消息

问题
对 Windows Server 8.1 客户机执行的灾难恢复失败，并显示类似如下所示的错误： [Major] From: VRDA@computer.company.com "hostname" [mountpoint]" Time: <timestamp> <filename> Cannot write: ([13] The data is invalid.) => not restored.
操作
通过从灾难恢复 CD 引导客户机系统，对 Windows 8.1 客户机的分区进行格式化并继续执行灾难恢复。

恢复映像创建失败，报告 Windows 群集中缺少卷

问题
在某些情况下，DR 恢复映像创建向导由于系统上不存在的卷而失败，Disk Witness Quorum 配置随即验证群集数据库未损坏(群集文件夹在仲裁磁盘上存在)并且事件日志与仲裁相关。
操作
要解决此问题，请重新创建仲裁并再次执行配置备份。

在客户机备份期间显示小错误或警告消息

问题
在客户机备份期间，可能报告以下小错误： Cannot perform stat(): ([2] No such file or directory) File is shorter than it was when it was opened 这类警告和错误消息可能由于临时 Data Protector 目录中被修改的文件而导致。 例如，如果同时备份 /CONFIGURATION 装载点和 /(根)装载点，就可能发生该情况。
操作
从备份规范中排除 /opt/omni/bin/drim/tmp 和 /opt/omni/bin/drim/log 目录。

在使用 8.10 或更高版本创建的备份规范中，系统将自动排除这些文件。

Cell Manager 和 RMA 主机不响应

问题

在 RHEL 操作系统中对 Linux 虚拟机执行灾难恢复失败，并显示以下错误消息：
`Cell Manager is not responding. Attempting offline restore.`
`RMA host is not responding.`
出现此类错误的原因可能是因为用于灾难恢复的虚拟机的 NIC 和 MAC 地址将与原始虚拟机的不同。 该虚拟机将没有 IP 地址，并且联机恢复失败。

操作
执行以下步骤： • 按 **Alt+F2** 打开另一个命令 shell。 • 导航到 `/etc/sysconfig/network`。 • 修改接口文件以匹配当前接口和 MAC 地址。 • 重新启动网络服务。 • 如果需要，编辑用于网络连接的主机文件。 • 确保客户机可连接到 Cell Manager 和介质(备份)主机。 • 按 **Alt+F1** 返回到主命令 shell 窗口，然后选择恢复选项。

使用 D2D 和 DDBoost 设备时， EADR 脱机还原失败

问题
如果您正在使用已配置用户名和密码的磁盘到磁盘设备，则脱机 EADR 将会失败。
操作
临时删除用户名和密码以执行还原。

带有已分离 SAN-LVM 卷的 RHEL EADR 不起作用

问题
在 Linux 系统上，在 EADR 恢复之后，如果您使用的是**默认恢复**或**最小恢复**方法，则可能无法启动已恢复系统。 启动过程中，将显示以下错误消息： **尝试打开 <volume_name> 时， super-block 中的幻数不正确**
操作

EADR 恢复后，在启动恢复的系统之前，您应该进入 OS 维护、根密码、装载 -o 重新装载， rw /(在读取/写入模式下重新装载“/”装载点)，并编辑 /etc/fstab。

如果选择默认恢复选项，则您必须添加注释，或从 fstab 中删除所有装载点，/boot、/、/opt、/etc 和 /var 除外。

如果选择最小恢复选项，则必须添加注释，或从 fstab 中删除所有装载点，/boot、/ 除外。

Internet Information Server 的灾难恢复故障排除

Internet Information Server (IIS) 的灾难恢复出现问题通常是未运行服务或未安装服务造成的。

依赖于 IIS 的服务不自动启动

问题
恢复 IIS 之后任何依赖于 IIS 的服务(例如 SMTP、NNTP)都不自动启动。
操作

1. 手动启动这些服务。
2. 如果此操作失败，则停止 IIS 管理服务，并使用**覆盖**选项还原 *%SystemRoot%*\system32\inetsrv\MetaBase.bin 文件。

   > **注意：**
   > *%SystemRoot%*\system32\inetsrv 目录是 IIS 服务的默认位置。 如果已将服务安装到另一个位置，则使用此位置作为还原 MetaBase.bin 文件的目标。

3. 启动 IIS 管理服务和所有相关服务。

附录 A： 准备任务示例

在 HP-UX 11.x 中移动终止链接的示例

```
# The system will go from "run-level" 4 to "run-level 1"

# retaining the (rpcd), inetd, networking, swagentd services up. The state is called
"minimum activity" for backup purposes (need networking).

# IMPORTANT: ensure the links are present in /sbin/rc1.d before

# moving and they do have this exact name. You have to rename them for the rc0.d
directory. Put them BELOW the lowest (original "/sbin/rc0.d/Kxx") "K...-link" in rc0.d

# Move K430dce K500inetd K660net K900swagentd into ../rc0.d BELOW the lowest kill
link!!!

echo "may need to be modified for this system"

exit 1

#

cd /sbin/rc1.d

mv K430dce ../rc0.d/K109dce

mv K500inetd ../rc0.d/K110inetd

mv K660net ../rc0.d/K116net

mv K900swagentd ../rc0.d/K120swagentd
```

Windows 灾难恢复准备表的示例

客户机属性	计算机名称	ANAPURNA
	主机名	anapurna.company.com
驱动程序		tatpi.sys、aic78xx.sys
Windows Service Pack		Windows Vista
IPv4 的 TCP/IP 属性	IP 地址	10.17.2.61
	默认网关	10.17.250.250
	子网掩码	255.255.0.0
	DNS 顺序	10.17.3.108、10.17.100.100

IPv6 的 TCP/IP 属性	IP 地址	td10:1234:5678:abba::6:1600
	子网前缀长度	64
	默认网关	td10:1234:5678:abba::6:1603
	首选 DNS 服务器	td10:1234:5678:abba::6:1603
	备用 DNS 服务器	td10:1234:5678:abba::6:1604
介质标签/条码数字		“anapurna - 灾难恢复”/[000577]
分区信息和顺序	第一个磁盘标签	
	第一个分区长度	31 MB
	第一个驱动器号	
	第一个文件系统	EISA
	第二个磁盘标签	BOOT
	第二个分区长度	1419 MB
	第二个驱动器号	C:
	第二个文件系统	NTFS/HPFS
	第三个磁盘标签	
	第三个分区长度	
	第三个驱动器号	
	第三个文件系统	

发送文档反馈

如果对此文档有任何评论，可以通过电子邮件联系文档团队。如果该系统配置了电子邮件客户机，请单击上面的链接，此时会打开一个电子邮件窗口，其主题行中将显示以下信息：

有关灾难恢复指南 (Data Protector 10.00) 的反馈

将反馈添加到电子邮件中并单击**发送**。

如果无可用的电子邮件客户机，请将以上信息复制到 Web 邮件客户机中的新邮件，并将反馈发送至 docs.feedback@microfocus.com 。

期待您的反馈！