

**IBM Spectrum Protect for Virtual
Environments
V 8.1.7**

**Data Protection for VMware
安装指南**



**IBM Spectrum Protect for Virtual
Environments
V 8.1.7**

**Data Protection for VMware
安装指南**



注释：

在使用本资料及其支持的产品之前，请阅读第 113 页的『声明』中的信息。

目录

关于本出版物	v
本出版物的目标读者	v
出版物	v

V8.1.7 中的新增内容	vii
--------------------------------	------------

第 1 章 安装和升级 Data Protection for VMware 1

可安装组件	1
Data Protection for VMware vSphere GUI	2
IBM Spectrum Protect 恢复代理进程	5
IBM Spectrum Protect vSphere Client 插件	5
Data Protection for VMware 命令行界面	6
IBM Spectrum Protect 文件复原界面	7
数据移动设备功能部件	7
规划安装 Data Protection for VMware	9
安装路线图	9
安装方案	10
系统需求	10
安装 Data Protection for VMware 组件	19
获取 Data Protection for VMware 安装包	20
使用安装向导安装 Data Protection for VMware 组件	21
以静默方式安装 Data Protection for VMware 组件	24
安装 Data Protection for VMware 后进行“第一步”	26
升级 Data Protection for VMware	27
升级 Data Protection for VMware	28
在 Windows 64 位系统上以静默方式升级 Data Protection for VMware	29
在 Linux 系统上以静默方式升级 Data Protection for VMware	29
在 vCenter Server Linked Mode 环境中升级 Data Protection for VMware	30
卸载 Data Protection for VMware	31
在 Windows 上卸载 Data Protection for VMware	31
以静默方式为 Windows 卸载 Data Protection for VMware	33
在 Linux 系统上卸载 Data Protection for VMware	33
修改 Data Protection for VMware 的现有安装	36
在 Data Protection for VMware 的现有安装中修改程序包	36
在 Data Protection for VMware 的现有安装中修改功能部件	36

第 2 章 配置 Data Protection for VMware 39

使用向导配置新安装	39
使用笔记本编辑现有安装	40
为文件复原操作启用环境	40
在 Linux 上设置文件复原操作	42
修改文件复原操作的选项	43
文件复原选项	43
配置文件复原操作的日志活动	44
文件复原日志活动选项	45
配置数据移动设备节点以获取标记支持	46
配置环境以执行虚拟机即时完全复原操作	49
1. 配置 ESXi 主机上的 iSCSI 软件	50
2. 在数据移动设备上安装和配置应用程序	50
3. 设置恢复代理进程连接	51
4. 为 ESXi 主机和数据移动设备配置专用的 iSCSI 网络	51
配置 Data Protection for VMware 的安全设置	52
配置安全设置以将数据移动设备和 VMCLI 节点连接到 IBM Spectrum Protect 服务器	53
使用传输层安全性配置 Data Protection for VMware vSphere GUI 通信	57
VMware vCenter Server 用户特权需求	63
Data Protection for VMware vSphere GUI 用户角色	66
Data Protection for VMware GUI 注册密钥	68
配置 恢复代理程序 GUI	69
启用从 恢复代理程序到 IBM Spectrum Protect 服务器的安全通信	73
语言环境设置	76
日志文件活动	77
启动和运行 Data Protection for VMware 的服务	79

附录 A. 高级配置任务 81

在 vSphere 环境中设置 IBM Spectrum Protect 节点	82
使用 vSphere 插件 GUI 设置数据移动设备节点	83
在 vSphere 环境中手动设置数据移动设备节点	84
在 vSphere 环境中配置 Data Protection for VMware 命令行界面	88
vSphere 环境命令行界面配置核对表	90
磁带配置指南	93
在 Linux 系统上手动配置 iSCSI 设备	95
在 Windows 系统上手动配置 iSCSI 设备	97
在 Linux 系统上手动配置装配代理节点	99
在远程 Windows 系统上手动配置装配代理节点	101
在 Linux 系统上手动配置多个客户机接收器服务	103
修改 VMCLI 配置文件	105

附录 B. 迁移至持续增量式增量备份策略	107
附录 C. IBM Spectrum Protect 产品系列的辅助功能选项	111
声明	113
词汇表	117
索引	119

关于本出版物

IBM Spectrum Protect™ for Virtual Environments 提供从 Windows 和 Linux 访客机器上的完全 VM 备份中进行的无主机块级别增量备份、文件恢复以及即时复原。当您将 IBM Spectrum Protect for Virtual Environments 与 IBM Spectrum Protect 数据移动设备配合使用时，可以进行块级别增量备份。

本出版物的目标读者

本出版物的目标读者是希望安装和配置 IBM Spectrum Protect for Virtual Environments 的用户和管理员。

《IBM Spectrum Protect for Virtual Environments: Data Protection for VMware 用户指南》中记录了概述信息、用户任务、备份和复原场景、命令参考以及错误消息。

出版物

IBM Spectrum Protect 产品系列包括 IBM Spectrum Protect Plus、IBM Spectrum Protect for Virtual Environments、IBM Spectrum Protect for Databases 以及若干其他 IBM® 存储管理产品。

要查看 IBM 产品文档，请参阅 IBM Knowledge Center。

V8.1.7 中的新增内容

IBM Spectrum Protect for Virtual Environments V8.1.7 引入了新的功能和更新。

要获取本发行版以及先前的 V8 发行版中的新功能和更新的列表，请参阅 Data Protection for VMware 更新。

在本产品文档中，新增信息和更改的信息通过更改左侧的竖线 (|) 来指示。

第 1 章 安装和升级 Data Protection for VMware

IBM Spectrum Protect for Virtual Environments 的安装包含规划、安装和初始配置。

可安装组件

Data Protection for VMware 包含若干组件，您可以安装这些组件来保护您的虚拟环境。

根据操作系统环境，以下 Data Protection for VMware 功能部件可用于安装：

限制：每个安装包都为您提供一个用户许可文件 (EULA)。如果您不接受该文件，那么安装过程将结束。

表 1. 按操作系统列出的可用 Data Protection for VMware 功能部件

组件	Linux	Windows
IBM Spectrum Protect 恢复代理进程 此组件提供虚拟安装和即时复原功能。		√
恢复代理进程命令行界面 用于装配操作的命令行界面。		√
文档 文档包含自述文件和法律声明文件。	√	√
Data Protection for VMware 支持文件 该组件使 IBM Spectrum Protect 能够运行以下备份类型： <ul style="list-style-type: none">• 持续增量式增量备份• 持续增量式完全备份 应用程序保护需要此组件。如果卸载备份工作负载，那么此文件必须安装在 vStorage 备份服务器上。	√	√
Data Protection for VMware vSphere GUI 此组件是用于访问 VMware vCenter Server 上的 VM 数据的图形用户界面 (GUI)。此 GUI 的内容在以下视图中提供： <ul style="list-style-type: none">• Web 浏览器视图。可使用 GUI Web 服务器主机的 URL 在受支持的 Web 浏览器中访问此视图。例如： https://guihost.mycompany.com:9081/TsmVMwareUI/• VMware vSphere Web 客户机中的 IBM Spectrum Protect vSphere Client 插件 视图。该视图中的此面板专门设计为在 vSphere Web 客户机中集成，但是是从与其他视图相同的 GUI Web 服务器获取此视图的数据和命令。IBM Spectrum Protect vSphere Client 插件提供 Web 浏览器视图中可用功能的子集以及一些其他功能。此视图中不提供配置和高级报告功能。	√	√

表 1. 按操作系统列出的可用 *Data Protection for VMware* 功能部件 (续)

组件	Linux	Windows
文件复原 GUI 此组件是一个基于 Web 的 GUI，支持您从 VMware 虚拟机备份复原文件，而无需管理员帮助。安装 Data Protection for VMware GUI 时，将自动安装该 GUI。可通过配置向导启用该 GUI。	1	√
数据移动设备 IBM Spectrum Protect 数据移动设备可为 Data Protection for VMware 迁移数据。此功能称为数据移动设备。数据移动设备将数据从虚拟环境移动到 IBM Spectrum Protect 服务器。当您在服务器上安装数据移动设备时，该服务器可用作 vStorage 备份服务器。可以将数据移动设备与 Data Protection for VMware 安装在同一系统上，也可以安装在另一服务器上。	√	√

1. 尽管文件复原界面组件必须在 Windows 系统上安装并启用，但您可以使用此界面来在 Windows 和 Linux 访客虚拟机上复原文件。
2. 安装 Data Protection for VMware 时，会在安装中包含数据移动设备。典型安装意味着您无需执行额外的仅数据移动设备安装以在此机器上获取数据移动设备。

Data Protection for VMware 将备份工作负载从 VM 卸载到 vStorage 备份服务器。要完成此任务，必须在 vStorage 备份服务器上安装数据移动设备。

Data Protection for VMware vSphere GUI

Data Protection for VMware vSphere GUI (vSphere GUI) 组件是一个图形用户界面，用于访问 VMware vCenter Server 上的 VM 数据。

概述

Data Protection for VMware vSphere GUI 是用于完成以下任务的主要界面：

- 启动或调度备份，将 VM 备份到 IBM Spectrum Protect 服务器。
- 启动完全恢复，从 IBM Spectrum Protect 服务器恢复 VM。
- 发出有关任务进度、已完成的最新事件、备份状态和空间使用情况的报告。此消息可帮助您对备份处理中发生的错误进行故障诊断。

提示：随 vSphere GUI 一起安装的联机帮助中提供了有关如何使用该 GUI 完成任务的信息。在任何 GUI 窗口中单击[了解更多信息](#)可打开联机帮助以获取任务帮助。

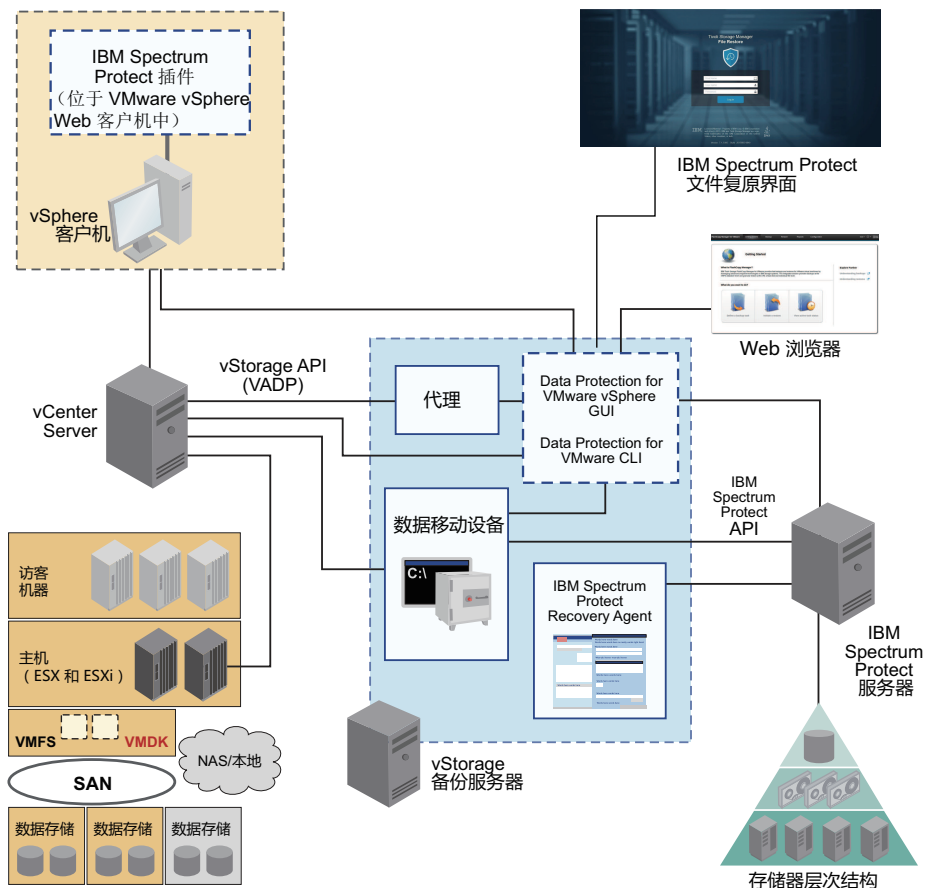


图 1. VMware vSphere 用户环境中的 Data Protection for VMware 系统组件

需求

Data Protection for VMware vSphere GUI 可以安装在满足操作系统先决条件的任何系统上。vSphere GUI 资源需求极低，因为它不处理 I/O 数据传输。

提示：将 vSphere GUI 安装在 vStorage 备份服务器上是最常见的配置。

vSphere GUI 必须通过网络连接到以下系统：

- vStorage 备份服务器
- IBM Spectrum Protect 服务器
- vCenter Server

此外，用于 Derby 数据库的端口（缺省为 1527）和用于 GUI Web 服务器的端口（缺省为 9081）必须可用。

配置

可以向单个 vCenter Server 注册多个 vSphere GUI。此方案可减少由单个 VMware vSphere GUI 管理的数据中心数（及其 VM 访客备份数）。这样，vCenter Server 就可以管理 vCenter Server 上定义的数据中心总数其中的一部分。

要更新受管数据中心，请转至配置 > 编辑配置。

向单个 vCenter Server 注册多个 vSphere GUI 时，请遵循以下准则：

- 每个数据中心只能由一个已安装的 vSphere GUI 管理。
- 每个已安装的 vSphere GUI 都需要有一个唯一的 VMCLI 节点名。
- 为每个已安装的 vSphere GUI 使用唯一的数据移动设备节点名可以简化节点管理。

访问 vSphere GUI

可以使用以下方法访问 vSphere GUI：

- 独立的 Web 浏览器 GUI。可通过指向 GUI Web 服务器的 URL 书签来访问此 GUI，例如：

```
https://hostname:port/TsmVMwareUI/
```

其中：

- *hostname* 是安装 Data Protection for VMware vSphere GUI 的系统的名称
- *port* 是可用于访问 vSphere GUI 的端口号。缺省端口号为 9080。对于安全端口，缺省值为 9081。
- vSphere Web Client 扩展（称为 Data Protection 扩展），它连接至 GUI Web 服务器以访问 IBM 存储中的虚拟机。内容是 Web 浏览器 GUI 中所提供内容的一部分。

安装期间，可以指定一种或多种访问方法。

Windows

缺省安装目录为 C:\IBM\SpectrumProtect\webserver。

Linux

缺省安装目录为 /opt/tivoli/tsm/tdpvmware/common/webserver。

IBM Spectrum Protect 恢复代理进程

使用恢复代理进程服务来从 IBM Spectrum Protect 服务器装配任何快照卷。

概述

您可以使用 iSCSI 协议从远程系统访问快照。

如果您需要在客户机系统上使用只读访问权以本地方式查看快照，请使用 Data Protection for VMware V8.1.4 或更低版本。

此外，恢复代理进程还提供即时复原功能和访客内应用程序的保护。当复原操作在后台继续进行时，即时复原使正在使用的卷保持可用。应用程序保护使访客虚拟机中安装的应用程序（例如 Microsoft Exchange Server 和 Microsoft SQL Server）可用于备份和复原保护。

恢复代理进程可以从远程系统完成以下任务：

- 收集有关可以复原的数据的信息，例如：
 - 已备份的 VM。
 - 已备份虚拟机的可用快照。
 - 特定快照中的可用分区。

有关命令、参数和返回码的详细信息，请参阅《IBM Spectrum Protect for Virtual Environments: Data Protection for VMware 用户指南》中的命令参考部分。

需求

Windows 在 Windows 系统上，恢复代理程序 GUI 和命令行界面在 Data Protection for VMware 的完整安装或数据移动设备的高级安装过程中进行安装。

访问恢复代理进程

Windows 可以从开始菜单访问恢复代理进程：开始 > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect 恢复代理进程**

IBM Spectrum Protect vSphere Client 插件

IBM Spectrum Protect vSphere Client 插件是提供 Data Protection for VMware vSphere GUI 的视图的 VMware vSphere Web 客户机扩展。

概述

IBM Spectrum Protect vSphere Client 插件提供 Data Protection for VMware vSphere GUI 的浏览器视图中可用的功能的子集以及一些其他功能。

需求

要安装 IBM Spectrum Protect vSphere Client 插件，必须在运行 IBM Spectrum Protect for Virtual Environments 配置向导时选中以下选项：

- 在配置向导的 **vCenter** 设置页面上，选中**更新注册**可向关联的 vCenter 注册插件。

- 输入 GUI 主机地址、vCenter 用户和密码。

注：缺省域基于本地域地址，并且无法以外部方式进行访问。如果需要外部访问权，请指定可由 DNS 解析的 GUI 主机地址或指定 IP 地址。

完成向导之后，将向 vCenter 注册该插件。

访问数据保护插件

您可以从 vSphere Web 客户机访问插件：

1. 使用 vCenter 凭证登录到 vSphere Web 客户机。数据保护插件位于主菜单 **IBM Spectrum Protect** 下。
2. 选择此菜单项将使您进入 IBM Spectrum Protect 扩展的主要区域。与 vCenter 库存中的特定项相关联的监视和配置部分还具有 IBM Spectrum Protect for Virtual Environments 功能。

Data Protection for VMware 命令行界面

Data Protection for VMware CLI 是随 Data Protection for VMware vSphere GUI 一起安装的全功能命令行界面。

概述

可以使用 Data Protection for VMware CLI 完成以下任务：

- 启动或调度备份，将 VM 备份到 IBM Spectrum Protect 服务器。
- 启动完全恢复，从 IBM Spectrum Protect 服务器恢复 VM、VM 文件或 VM 磁盘 (VMDK)。
- 查看有关备份数据库和环境的配置信息。

虽然 Data Protection for VMware vSphere GUI 是主任务界面，但 Data Protection for VMware CLI 提供了非常有用的辅助界面。

例如，Data Protection for VMware CLI 可用于实施与 Data Protection for VMware vSphere GUI 所实施机制不同的调度机制。此外，Data Protection for VMware CLI 在评估脚本自动化结果时也非常有用。

访问 Data Protection for VMware 命令行界面

可以从命令行访问 Data Protection for VMware CLI。

有关可用命令的详细信息，请参阅《*IBM Spectrum Protect for Virtual Environments: Data Protection for VMware* 用户指南》中的命令参考部分

IBM Spectrum Protect 文件复原界面

可以从 VMware 虚拟机备份复原单个文件。

概述

文件复原界面是基于 Web 的界面，可以在其中从 VM 备份复原单个文件。此界面的优势是文件、软件 and 平台所有者无需事先了解 IBM Spectrum Protect 备份和复原操作，就能够复原自己的文件。

当您选择相应选项以保护 vSphere 环境中的数据时，会安装文件复原界面功能部件。在 Data Protection for VMware 配置向导中，必须启用文件复原功能部件，该界面才可以使用。

访问 IBM Spectrum Protect 文件复原界面

要访问文件复原界面，请打开 Web 浏览器，并输入管理员提供的 URL。例如：

`https://hostname:9081/FileRestoreUI`

其中 *hostname* 是安装 Data Protection for VMware vSphere GUI 的系统的主机名。

数据移动设备功能部件

数据移动设备是 Data Protection for VMware 的软件组件，可用于在 IBM Spectrum Protect 服务器上往来移动数据。

概述

在典型 VMware 环境中，数据移动设备用于将虚拟机备份保存到数据中心节点。

安装 Data Protection for VMware 时，会在安装中包含数据移动设备。数据移动设备与 Data Protection for VMware vSphere GUI 和其他 Data Protection for VMware 组件安装在相同系统上。

您也可以将数据移动设备安装在独立于其他 Data Protection for VMware 组件的远程系统上，以在多个系统之间重新分发备份工作负载。

VMware 环境中不支持快照差分备份操作。无法运行位于主机（其中还安装了 Data Protection for VMware 数据移动设备）的 NetApp 文件程序上的文件系统快照差分备份操作。

设置数据移动设备

有关规划、安装和配置数据移动设备的信息，请复查以下列表：

操作	描述
确定保护 vSphere 环境所需的数据移动设备数量。	可能需要多个数据移动设备节点来保护 vSphere 环境。 要确定所需的数据移动设备节点数量，请参阅技术说明 2007197。本技术说明还包含有关使用虚拟或物理机器作为数据移动设备节点和数据移动设备所在位置的注意事项。

操作	描述
安装 Data Protection for VMware。	<p>要安装 Data Protection for VMware，请运行 Data Protection for VMware 安装程序并选择典型安装（针对 Windows 操作系统）或完整（针对 Linux 操作系统）。此安装选项将安装所有 Data Protection for VMware 组件，包括数据移动设备。</p> <p>有关如何运行 Data Protection for VMware 安装程序的信息，请参阅第 19 页的『安装 Data Protection for VMware 组件』。</p>
定义适用于环境的数据移动设备。	<p>当 Data Protection for VMware 安装向导完成时，Data Protection for VMware vSphere GUI 配置向导会打开并支持您设置与 IBM Spectrum Protect 服务器的通信。</p> <p>在配置向导的"数据移动设备节点"页面上，为本地数据移动设备和将在独立系统上安装的任何远程数据移动设备定义信息。</p> <p>如果在 Windows 操作系统上安装并在定义数据移动设备时选择创建服务，那么数据移动设备的配置信息将保存在以下位置中的选项文件中： C:\Program Files\Tivoli\TSM\baclient\</p> <p>此外，将配置数据移动设备所需的服务。</p> <p>如果在 Linux 操作系统上安装数据移动设备或者在 Windows 操作系统上安装数据移动设备，但配置期间未选择创建服务，那么必须完成第 83 页的『使用 vSphere 插件 GUI 设置数据移动设备节点』中的步骤以创建选项文件和配置所需的服务。</p>
根据需要在远程系统上安装和配置其他数据移动设备。	<p>要在远程系统上安装数据移动设备，请运行 Data Protection for VMware 安装程序并执行以下操作之一：</p> <p>在 Windows 操作系统上，选择配置向导中的高级安装 > 仅安装数据移动设备功能部件。</p> <p>在 Linux 操作系统上，从配置向导中的安装集列表中选择定制。确保选中 Data Protection for VMware 数据移动设备。缺省情况下，此选项处于已选择状态。</p> <p>安装完成时，要在远程系统上设置数据移动设备，请根据第 83 页的『使用 vSphere 插件 GUI 设置数据移动设备节点』中的指示信息进行操作。</p>

规划安装 Data Protection for VMware

通过将备份工作负载从基于 VMware ESXi 的主机卸载到 vStorage 备份服务器，Data Protection for VMware 消除了运行备份对 VM 的影响。

Data Protection for VMware 与集成的数据移动设备配合工作，以完成 VM 的持续增量式完全备份和持续增量式增量备份。数据移动设备节点将数据"移动"到 IBM Spectrum Protect 服务器进行存储，用于以后的 VM 映像级别复原。在磁盘卷级别和完全 VM 级别可以进行即时复原。

提示：数据移动设备是单独许可的组件，它包含自己的用户界面和文档。为充分完善全面的计划以使用 Data Protection for VMware 保护 VM，需要熟悉此产品及其文档。适用于 Windows 64 位的 Data Protection for VMware 包含数据移动设备功能部件。

安装路线图

下表标识成功的安装过程的完成步骤。

表 2. Data Protection for VMware 新客户或现有客户的安装任务

步骤	任务	从此处开始
1	检查系统需求。	确保将安装 Data Protection for VMware 的系统满足系统需求。
2	检查用户许可权需求。	通过使用必需的用户许可权级别，避免可能发生的安装错误或延迟。
3	检查必需通信端口的可用性。	通过在尝试安装 Data Protection for VMware 之前打开必需的通信端口，防止安装失败或延迟。
4	安装 Data Protection for VMware： <ul style="list-style-type: none">使用安装向导安装 Data Protection for VMware第 24 页的『以静默方式安装 Data Protection for VMware 组件』 升级 Data Protection for VMware： 升级 Data Protection for VMware	每个安装包都为您提供一个用户许可文件 (EULA)。如果您不接受该文件，那么安装将结束。
5	第 39 页的『使用向导配置新安装』 如果计划升级 Data Protection for VMware，那么根据所安装的组件，可能需要执行更多配置任务。请参阅《IBM Spectrum Protect for Virtual Environments: Data Protection for VMware 用户指南》中的配置主题，以获取更多详细信息。	使用配置向导进行初始配置。根据所安装的功能部件，如本节中所述，可能需要执行更多配置任务。

提示：为帮助规划特定 Data Protection for VMware 备份环境所需的代理主机数，IBM Spectrum Protect Wiki 上提供了以下出版物：

Step by Step Guide To vStorage Backup Server (Proxy) Sizing

此出版物在 IBM Spectrum Protect for Virtual Environments 产品部分中提供。

安装方案

安装 Data Protection for VMware 之前，请选择最适合您业务需求的方案。

可以使用 GUI 或以静默方式安装 Data Protection for VMware 和数据移动设备：

- 第 21 页的『使用安装向导安装 Data Protection for VMware 组件』
- 第 24 页的『以静默方式安装 Data Protection for VMware 组件』

有关按平台列出的可用功能部件和组件的列表，请参阅第 1 页的『可安装组件』。

表 3. 安装方案

方案编号	描述	必须完成的任务
1	对于要将 Data Protection for VMware 和数据移动设备安装在同一系统上的新安装，请使用此方案。	Windows 可以使用套件安装程序在 GUI 中或以静默方式进行安装。 Linux 可以使用 InstallAnywhere 在 GUI 中或以静默方式进行安装。
2	如果要在该系统上安装数据移动设备（安装代理）、恢复代理程序以及所需的支持软件包，请使用此方案。	Windows 可以使用“套件安装程序”完成高级安装。 Linux 数据移动设备功能部件现已随 Data Protection for VMware 一起安装。

系统需求

要实现 Data Protection for VMware 组件，系统必须满足相应的系统需求。

软件需求

软件和操作系统需求的详细信息可能随时间而更改。要了解最新的软件需求，请参阅技术说明 1505139。

硬件需求

硬件需求随以下项的变化而变化：

- 保护的服务器数
- 保护的卷数
- 数据集大小
- LAN 和 SAN 连接

注：恢复代理程序组件不支持在不依赖 LAN 的环境中进行操作。

下表描述安装 Data Protection for VMware 所需的硬件需求。

表 4. Data Protection for VMware 的硬件需求。

组件	最低需求	Preferred
系统	IntelPentium D 双核处理器或兼容产品	不适用

表 4. Data Protection for VMware 的硬件需求。(续)

组件	最低需求	Preferred
内存	4 GB RAM, 4 GB 虚拟地址空间	不适用
可用硬盘	4.4 GB	9.0 GB
网络	1 GbE	10 GbE

注：根据并行进程的数量，虚拟机备份可能需要占用大量内存。

可通过 `dsmc backup vm` 命令扩展内存需求，并且可通过以下公式来计算此需求：

$$\text{Required memory} = (\text{DiskSize} / \text{MBLKSize}) * \text{ReadBufferSize} * \text{VMMAXPARALLEL}$$

其中：

- **DiskSize** 是当前正在处理的访客磁盘的大小。
- **MBLKSize** 是巨型块的大小。该值针对小于 2 TB 的磁盘等于 128 MB，针对大于 2 TB 的磁盘等于 1 GB；
- **ReadBufferSize** 是用于适应 MBLK 信息的 IBM Spectrum Protect 内部缓冲区的大小。此缓冲区大小等于 256 KB；
- **VMMAXPARALLEL** 是单一备份操作进程任一时间可备份的虚拟机的最大数量。

例如，要备份 10 个访客（每个访客含 40 GB 磁盘），并在单一备份操作进程中使用 VMMAXPARALLEL 2 来运行，将需要：

- **DiskSize** = 40 GB = 41943040 KB；
- **MBLKSize** = 128 MB = 131072 KB；
- **ReadBufferSize** = 256 KB；
- **VMMAXPARALLEL** = 2。

$$\text{Required memory} = (41943040 / 131072) * 256\text{kB} * 2 = 163840\text{KB} = 160\text{MB}。$$

注：要在五次并行备份操作进程中使用“VMMAXPARALLEL 2”来备份同样数量的访客，将需要相比于上一个示例（最多）五倍的内存，即 800 MB。

限制：以下限制适用于备份操作中涉及的 VMware VMDK：

- 对于持续增量式增量备份方式，备份操作中涉及的每个单独的 VMDK 不能超过 8 TB。如果 VMDK 超过 8 TB，那么备份操作将失败。要将 VMDK 的大小增大至大于缺省值 2 TB，请使用 `vmxvirtualdisks` 选项指定最大大小。有关更多信息，请在 IBM Knowledge Center 上搜索 `vmxvirtualdisks`。
- 对于持续增量式完全备份方式，备份操作中涉及的每个单独的 VMDK 不能超过 2 TB。如果 VMDK 超过 2 TB，那么备份操作将失败。

为防止在使用任何一种备份方式期间失败，可以通过在数据移动设备选项文件中指定 `vmxvirtualdisks yes` 来跳过 VMDK 处理。有关更多信息，请参阅 `Vmskipvirtualdisks`。

文件复原先决条件

使用 IBM Spectrum Protect Data Protection for VMware 文件复原界面复原文件之前，请确保您的环境满足最低先决条件。

要启用文件复原功能，必须在 Windows 系统上安装 Data Protection for VMware。

VMware 虚拟机先决条件

以下先决条件适用于包含要复原的文件的 VMware 虚拟机：

- **Linux** **Windows** 虚拟机上必须安装 VMware Tools。
- **Linux** **Windows** 文件复原操作期间，虚拟机必须正在运行。
- **Windows** 数据移动设备系统与包含要复原的文件的虚拟机必须属于同一 Windows 域或位于与该虚拟机具有信任关系的域中。
- **Windows** 如果从 Windows 域中删除某个虚拟机并随后复原，那么该虚拟机必须重新加入域以确保域信任关系。在域信任关系复原之前，请勿尝试从虚拟机复原文件。
- **Windows** 如果用户未拥有要复原的文件，那么必须为该虚拟机的用户分配 Microsoft Windows 的 复原文件和目录特权。
- 有关使用 Data Protection for VMware 文件复原界面所需的 Microsoft Windows 域帐户先决条件的进一步信息，请参阅技术说明 1998066。
- **Linux** 虚拟机要求进行本地用户认证。通过 Windows 域、轻量级目录访问协议 (LDAP)、Kerberos 或其他网络认证方法无法进行认证。
- **Linux** 在 Red Hat Enterprise Linux 6 操作系统上，sshd 守护程序配置文件 (/etc/ssh/sshd_config) 中的 ChallengeResponseAuthentication 选项必须指定 YES 或被注释掉。例如，下列任一语句有效：

```
ChallengeResponseAuthentication yes
#ChallengeResponseAuthentication no
```

修改此选项后，请重新启动 sshd 守护程序。

数据移动设备先决条件

数据移动设备系统表示从一个系统"将数据移动"到另一个系统的特定数据移动设备。

- **Windows** 数据移动设备系统与包含要复原的文件的虚拟机必须属于同一个 Windows 域。

安装代理程序先决条件

安装代理系统代表通过 iSCSI 连接访问安装的虚拟机磁盘的 Linux 或 Windows 代理系统。此系统使装配的虚拟机磁盘上的文件系统能够作为复原点从文件复原界面访问。

Linux Linux 操作系统提供一个守护程序，用于在系统可以使用逻辑卷管理器 (LVM) 卷组时激活这些卷组。请在 Linux 安装代理系统上设置此守护程序，以便在系统可以使用 LVM 卷组时不激活这些卷组。有关如何设置此守护程序的详细信息，请参阅相应的 Linux 文档。

Linux **Windows** Windows 安装代理系统和 Linux 安装代理系统必须位于同一个子网中。

Microsoft Windows 域帐户先决条件

以下先决条件适用于 Windows 域帐户。第一个需求是建立对所有 VM 都具有本地管理权限的 Windows 域用户帐户：

- 要执行必要的任务以启用对虚拟机访客的文件恢复，您需要一个属于 Windows 域并且是安装代理系统上的本地管理员的用户帐户。具有此帐户的管理员在 Data Protection for VMware vSphere GUI 配置向导或笔记本中输入帐户凭证，以启用文件复原操作的环境。
- 要创建具有足够特权来使用文件复原界面的用户帐户，可以使用 Windows 组策略对象集中管理单个域用户，从而使其能够使用本地管理员凭证访问多台机器，并选择性地限制不需要的操作。

以下步骤说明如何能够创建此用户帐户。通过使用 Active Directory 用户和计算机 MMC 插入在域控制器上完成这些步骤：

1. 选择操作->新建->组，然后创建名为 **FR Admins** 的新安全组。组作用域应设置为 Global。
2. 创建用户名为 fradmin1 的新域用户帐户并将其添加到 **FR Admins** 安全组。您还可以向该组添加其他域用户帐户。
3. 要对 fradmin1 可以访问的计算机集合提供更多控制，请创建新组织单元
4. 从域对象中，选择新建->组织单元，将其命名为 FR Computers
5. 使用多台机器填充 FR Computers 组织单元。 .

从组策略 MMC 插入在域控制器上完成以下步骤：

1. 创建名为 FR Admin GPO 的新组策略对象，该对象会将 **FR Admins** 组中的管理员添加到与组策略对象应用到的组织单元关联的计算机的本地管理员组。
2. 在组策略对象中，将帐户添加到本地管理员组以及（可选）远程桌面用户。
3. 选择 FR Computers 组织单元并添加新创建的组策略对象。

注：组策略对象可能已与域本身关联，但在此情况下，fradmin1 将位于域中所有计算机的本地管理员组中。使用显式组织单元会提供额外控制。

4. 可选：使用组策略管理来限制本地计算机上不需要的操作，例如 Deny log on locally 和 Deny log on through Terminal Services。
5. 在 Data Protection for VMware vSphere GUI 配置向导或配置笔记本的"文件复原"页面上，更新设置以使用上述步骤中创建的 domain\fradmin1 帐户。
6. 重新启动安装代理客户机访问守护程序 (CAD) 服务。

设置具有合适特权的帐户后：

- **Windows** 在 Data Protection for VMware vSphere GUI 配置向导或配置笔记本中输入凭证，以启用文件复原操作的环境。
- **Windows** 文件所有者使用 Windows 域用户凭证来访问远程虚拟机（包含要复原的文件）。这些凭证在登录期间在文件复原界面中输入。域用户凭证验证文件所有者是否有权登录远程虚拟机以及是否有权将文件复原到远程虚拟机。这些凭证不需要任何特殊许可权。
- **Windows** 如果文件所有者使用的 Windows 域用户帐户被限制为访问特定计算机（而不是访问域中的所有计算机），请确保安装代理系统包含在此域用户帐户可访问的计算机的列表中。否则，文件所有者无法登录到文件复原界面。

磁带介质先决条件

不支持从磁带介质进行文件复原。首选方法是从磁盘存储器复原文件。

必需的安装许可权

开始安装之前，请确保您的用户标识包含必需的许可权级别。

关于此任务

表 5. 安装和配置 Data Protection for VMware 所需的用户许可权

系统	所需许可权
Windows	管理员
Linux	root 用户
vCenter Server	管理员特权 vCenter Server 角色需要以下特权：扩展 > 注册扩展、注销扩展、更新扩展。在 VMware vCenter Server 层次结构中，必须将此新角色应用于安装期间指定的用户标识的 vCenter 对象。
IBM Spectrum Protect 服务器 限制：必须启动服务器。	管理访问权 (系统或不受限制的策略域特权)

必需的通信端口

查看安装 Data Protection for VMware 时必须在防火墙中打开的通信端口的列表。

下表中标识的端口反映典型安装。典型安装包括在同一 Windows 系统上安装以下组件：

- Data Protection for VMware GUI 服务器
- vStorage 备份服务器（数据移动设备）
- Windows 装配代理
- IBM Spectrum Protect 文件复原界面

如果使用非典型安装，那么可能需要更多端口。

限制：Windows 装配代理 和 Linux 装配代理 必须位于同一子网中。

表 6. 必需的通信端口. 下表标识 Data Protection for VMware 访问的端口。

TCP 端口	发起方：出站（自主机）	目标：入站（至主机）
443	vStorage 备份服务器	vCenter Server（安全 HTTP）
443	Data Protection for VMware vSphere GUI 服务器	vCenter Server
443 仅当数据移动设备为 Linux 系统时，才需要此设置。	Windows 装配代理	vCenter Server
443	vStorage 备份服务器	平台服务控制器
443	Data Protection for VMware vSphere GUI 服务器	平台服务控制器
443	Windows 装配代理	平台服务控制器
902 443	vCenter Server	ESXi 主机
902 443	vStorage 备份服务器（代理）	ESXi 主机（所有受保护主机）
1500 (tcpport)	vStorage 备份服务器（代理）	IBM Spectrum Protect 服务器
1500 (tcpadminport)	Data Protection for VMware vSphere GUI 服务器 <ul style="list-style-type: none"> 1500 (tcpadminport) 是非 SSL 通信 对于 SSL 通信，tcpadminport 是支持与 IBM Spectrum Protect 服务器进行 SSL 通信的唯一端口。用于 SSL 协议的正确端口号通常是 IBM Spectrum Protect 服务器 dsmserv.opt 文件中的 ssltcpadminport 选项所指定的值。但是，如果 dsmserv.opt 文件中指定 adminonclient no，那么用于 SSL 协议的正确端口号是 ssltcpadminport 选项指定的值。ssltcpadminport 选项没有缺省值。因此，该值必须由用户指定。 	IBM Spectrum Protect 服务器
1527 内部 Derby 数据库		
1501 1581 (httpport)	IBM Spectrum Protect 服务器	vStorage 备份服务器 <ul style="list-style-type: none"> 数据移动设备调度程序 Web 客户机 客户机接收器守护程序

表 6. 必需的通信端口 (续). 下表标识 Data Protection for VMware 访问的端口。

TCP 端口	发起方：出站（自主机）	目标：入站（至主机）
1581 (httpport) 1582、1583 (webports)	Data Protection for VMware vSphere GUI 服务器	vStorage 备份服务器
9081 GUI Web 服务器 (HTTPS 协议)	vSphere 客户机	Data Protection for VMware vSphere GUI 服务器（用于通过 Web 浏览器访问 vCenter 的安全 HTTPS 端口）
22 恢复代理进程的 SSH 缺省端口	恢复代理进程	Data Protection for VMware Windows"装配"主机 • 用于 Linux 恢复代理进程的 SSH
3260	Linux Data Protection for VMware 文件复原	Data Protection for VMware Windows"装配"主机 • iSCSI
3260 恢复代理进程的 iSCSI 缺省端口	使用动态磁盘进行文件复原的 Windows 目标	Data Protection for VMware Windows"装配"主机 • iSCSI
5985	文件复原 GUI 操作	Windows 远程管理
135	Windows 装配代理	包含要使用 IBM Spectrum Protect 文件复原界面复原的文件的 VMware 虚拟机

VMware vCenter Server 用户特权需求

运行 Data Protection for VMware 操作需要某些 VMware vCenter Server 特权。

使用 Data Protection for VMware vSphere GUI 的 Web 浏览器视图来保护 VMware 数据中心时所需的 vCenter Server 特权

用于登录到 Data Protection for VMware vSphere GUI 的浏览器视图的 vCenter Server 用户标识

必须具有足够的 VMware 特权才能查看此 GUI 所管理的数据中心的内容。

例如，VMware vSphere 环境包含五个数据中心。用户"jenn"仅对其中的两个数据中心具有足够的特权。因此，在这些视图中，"jenn"只能看到其具备足够特权的上述两个数据中心。另外三个数据中心（用户"jenn"对其不具有特权）对"jenn"不可见。

VMware vCenter Server 将一组特权集合起来定义为角色。角色应用于特定用户或组的对象，用于创建特权。在 VMware vSphere Web Client 中，必须创建带有一组特权的角色。要为备份和复原操作创建 vCenter Server 角色，请使用 VMware vSphere Client 添加角色功能。

如果要使特权传播到 vCenter 内的所有数据中心，请指定 vCenter Server，然后选中传播至子代复选框。否则，如果将角色指定给所需数据中心，那么只有在传播至子代复选框选中的情况下，才能限制许可权。浏览器 GUI 的强制实施处于数据中心级别。

以下示例显示如何控制两个 VMware 用户组对数据中心的访问。首先，创建一个包含技术说明 7047438 中定义的所有权限的角色。此示例中的特权级别是由名称为 "TDPVMwareManage" 的角色来标识。组 1 要求访问数据中心 Primary1_DC 和 Primary2_DC 的管理虚拟机。组 2 要求访问数据中心 Secondary1_DC 和 Secondary2_DC 的管理虚拟机。

对于组 1，请为数据中心 Primary1_DC 和 Primary2_DC 分配 "TDPVMwareManage" 角色。对于组 2，请为数据中心 Secondary1_DC 和 Secondary2_DC 分配 "TDPVMwareManage" 角色。

每个 VMware 用户组中的用户可以使用 Data Protection for VMware GUI 仅在其各自数据中心中管理虚拟机。

提示：在创建角色时，请考虑向角色中添加您之后针对对象完成其他任务所需要的额外特权。

使用数据移动设备所需要的 vCenter Server 特权

安装在 vStorage 备份服务器（数据移动设备节点）上的 IBM Spectrum Protect 数据移动设备需要 VMCUser 和 VMCPw 选项。VMCUser 选项指定要备份、复原或查询的 vCenter 或 ESX 服务器的用户标识。分配给用户标识 (VMCUser) 的必需特权确保客户机可以在虚拟机和 VMware 环境中运行。此用户标识必须具有上述技术说明中所述的 VMware 权限。

要创建用于备份和复原操作的 vCenter Server 角色，请使用 VMware vSphere Client 的添加角色功能。在添加此用户标识 (VMCUser) 的特权时，必须选择传播至子代选项。此外，请考虑为此角色添加其他特权，以用于备份和复原之外的其他任务。对于 VMCUser 选项，强制实施处于顶级对象。

使用 Data Protection for VMware vSphere GUI 的 IBM Spectrum Protect vSphere Client 插件视图来保护 VMware 数据中心时所需的 vCenter Server 特权

IBM Spectrum Protect vSphere Client 插件需要一组特权，这组特权不同于登录到 GUI 所需的特权。

在安装期间，将为 IBM Spectrum Protect vSphere Client 插件创建以下定制特权：

- 数据中心 > IBM Data Protection
- 全局 > 配置 IBM Data Protection

将注册 IBM Spectrum Protect vSphere Client 插件所需的定制特权，以作为单独扩展。特权扩展关键字是 com.ibm.tsm.tdpvmware.IBMDDataProtection.privileges。

这些特权允许 VMware 管理员启用和禁用对 IBM Spectrum Protect vSphere Client 插件内容的访问权。只有对必需 VMware 对象具备这些定制特权的用户才能访问

IBM Spectrum Protect vSphere Client 插件 内容。 一个 IBM Spectrum Protect vSphere Client 插件 向每个 vCenter Server 注册并且由配置为支持 vCenter Server 的所有 GUI 主机共享。

从 VMware vSphere Web 客户机中, 您必须使用 IBM Spectrum Protect vSphere Client 插件为能够完成虚拟机数据保护功能的用户创建一个角色。 对于此角色, 除了 Web 客户机所需要的标准虚拟机管理员角色特权外, 还必须指定**数据中心 > IBM Data Protection** 特权。 对于每个数据中心, 请您希望授予其管理虚拟机权限的每个用户或用户组分配此角色。

vCenter 级别的用户需要**全局 > IBM Data Protection** 特权。 此特权允许用户管理、编辑或删除 vCenter Server 与 Data Protection for VMware vSphere GUI Web 服务器之间的连接。 请将此特权分配给熟悉 Data Protection for VMware vSphere GUI (用于保护其各自 vCenter Server) 的管理员。 可以在此扩展的"连接"页面中管理 IBM Spectrum Protect vSphere Client 插件连接。

以下示例显示了如何针对两个用户组来控制对数据中心的访问。 组 1 需要访问权才能管理数据中心 NewYork_DC 和 Boston_DC 的虚拟机。 组 2 需要访问权才能管理数据中心 LosAngeles_DC 和 SanFrancisco_DC 的虚拟机。

例如, 从 VMware vSphere 客户机中, 创建"IBMDDataProtectManage"角色, 分配标准虚拟机管理员角色特权以及**数据中心 > IBM Data Protection** 特权。

对于组 1, 请为数据中心 NewYork_DC 和 Boston_DC 分配"IBMDDataProtectManage"角色。 对于组 2, 请为数据中心 LosAngeles_DC 和 SanFrancisco_DC 分配"IBMDDataProtectManage"角色。

每个组中的用户可以在 vSphere Web 客户机中使用 IBM Spectrum Protect vSphere Client 插件 以仅在其各自数据中心中管理虚拟机。

与许可权不足相关的问题

当 Web 浏览器用户没有任何数据中心的足够许可权时, 会阻止对视图的访问。 而系统会发出错误消息 GVM2013E, 以告知用户由于许可权不足而无权访问任何受管数据中心。 还提供了其他新消息, 用于向用户告知因许可权不足而引发的问题。 要解决任何与许可权相关的问题, 请确保如上述各节中所述设置用户角色。 用户角色必须具有"必需特权 vCenter Server 用户标识和数据移动设备"表中标识的所有特权, 并且这些特权必须通过传播至子代复选框在数据中心级别应用。

当 IBM Spectrum Protect vSphere Client 插件用户没有某个数据库中心的足够许可权时, 该数据中心及其内容的数据保护功能将变得在此扩展中不可用。

当 IBM Spectrum Protect 用户标识 (由 VMCUser 选项指定) 包含的许可权不足以执行备份和复原操作时, 将显示以下消息:

ANS9365E VMware vStorage API 错误。
"执行此操作的许可权遭到拒绝。"

当 IBM Spectrum Protect 用户标识包含的许可权不足以查看机器时, 将显示以下消息:

备份 VM 命令已启动。 要处理的虚拟机总数: 1
ANS4155E VMware 服务器上找不到虚拟机"tango"。
ANS4148E 虚拟机"foxtrot"的完全 VM 备份失败, RC 4390

有关权限使用的进一步信息，请参阅 **Data Protection for VMware vSphere GUI** 和数据移动设备所需的 **vCenter Server** 权限上的注释。

要通过 VMware Virtual Center Server 检索日志信息以了解许可权问题，请完成以下步骤：

1. 在"vCenter Server 设置"中，选择日志记录选项，然后将 **vCenter** 日志记录设置为细微（细微）。
2. 重新生成该许可权错误。
3. 将 **vCenter** 日志记录重置为其先前值可防止记录过多的日志信息。
4. 在"系统日志"中，查找最新的 vCenter Server 日志 (vpxd-wxyz.log) 并搜索字符串 NoPermission。 例如：

```
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
Throw: vim.fault.NoPermission
```



此日志消息表明用户标识不包含创建快照的足够权限 (createSnapshot)。

安装 Data Protection for VMware 组件

可以安装与您的操作系统相应的 Data Protection for VMware 包中提供的所有组件或部分组件。

关于此任务

可以使用 Data Protection for VMware 安装程序安装以下组件：

- IBM Spectrum Protect 恢复代理进程
-  恢复代理进程命令行界面
-  文档（自述文件和法律声明文件）
- Data Protection for VMware 支持文件
- Data Protection for VMware vSphere GUI
- 数据移动设备功能部件，其中包含以下项：
 - 数据移动设备 GUI
 - 数据移动设备 Web 客户机
 - Client API (64 位) 运行时文件
 - 管理客户机命令行
 - VMware vStorage API 运行时文件

如果要安装数据移动设备（安装代理）、恢复代理程序以及所需的支持软件包，可以选择完全安装或使用"高级安装"选项。

提示：可以在 Data Protection for VMware 软件所在的系统上创建多个数据移动设备，也可以在远程系统上创建数据移动设备。此配置会增加可供 Data Protection for VMware 使用的资源。安装有数据移动设备的系统称为 vStorage 备份服务器。

获取 Data Protection for VMware 安装包

您可以从 IBM 下载站点（例如，IBM Passport Advantage®）获取 Data Protection for VMware 安装包。

Linux

开始之前

如果计划下载文件，请将最大文件大小的系统用户限制设置为无限制，以确保文件能够正确下载：

1. 要查询最大文件大小值，请发出以下命令：

```
ulimit -Hf
```
2. 如果未将最大文件大小的系统用户限制设置为无限制，请遵循与您操作系统相应的文档中的指示信息，将其更改为无限制。

过程

1. 从以下其中一个 Web 站点下载相应的程序包文件：
 - 对于首次安装或新发行版，请访问位于 <http://www.ibm.com/software/lotus/passportadvantage/> 的 Passport Advantage。Passport Advantage 是可以下载许可包文件的唯一站点。
 - 有关最新信息、更新和维护修订，请访问 IBM Spectrum Protect 支持站点：http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager。
2. 如果是从 IBM 下载站点下载的包，请完成以下步骤：
 - a. 将包文件下载到您选择的目录。该路径长度不得超过 40 个字符。确保将安装文件抽取到空目录。请勿抽取到包含先前抽取的文件或任何其他文件的目录中。
 - b.

Linux

 确保为该包设置了可执行文件许可权。如有必要，通过发出以下命令更改文件许可权：

```
chmod a+x package_name.bin
```
 - c.

Linux

 发出以下命令来抽取包：

```
./package_name.bin
```

其中 *package_name* 是下载的文件名称。
 - d.

Windows

 双击 *package_name* 来解压缩程序包，其中 *package_name* 是下载的文件名称。

使用安装向导安装 Data Protection for VMware 组件

可以使用安装向导来安装 Data Protection for VMware 组件。

关于此任务

Windows 您可以使用套件安装程序来安装 Data Protection for VMware 和数据移动设备。

Linux 您可以使用独立安装程序来安装 Data Protection for VMware 和数据移动设备。

在 Windows 系统上安装 Data Protection for VMware 组件

使用安装向导安装 Data Protection for VMware 组件和功能部件。

开始之前

安装 Data Protection for VMware 组件之前，请确保满足以下需求：

- 具有管理员访问特权的用户标识。
- 可通过网络连接到 VMware vCenter Server 6.x（或更高版本），并具有管理员访问特权。
- 到含管理员访问权（系统或不受限制的策略域 特权）的 IBM Spectrum Protect 服务器的网络连接。此服务器必须可用并正在运行。
- 确保您已复查以下需求：
 - 第 10 页的『系统需求』
 - 第 14 页的『必需的安装许可权』
 - 第 14 页的『必需的通信端口』

安装 Data Protection for VMware 之前，必须了解以下选项：

安装类型

典型安装

使用典型安装时，将安装所有 Data Protection for VMware 组件和功能部件。

高级安装

"高级安装"面板提供了安装单个数据移动设备的选项。此过程将在系统上安装数据移动设备（安装代理）、恢复代理程序以及所需的支持软件包。使用此安装选项可添加单个数据移动设备。此选项还可以安装应用程序保护代理程序，以支持单个数据库的恢复。安装后，可以使用 IBM Spectrum Protect GUI 通过 VMware vSphere 插件来配置数据移动设备和服务。

关于此任务

您可以使用套件安装程序来安装 Data Protection for VMware。套件安装程序的 spinstall.exe 文件位于安装包的根目录下。

有关可以安装的组件和功能部件的列表，请参阅第 1 页的『可安装组件』。

过程

要安装 Data Protection for VMware，请从您已选择安装的组件的 spinstall.exe 文件所在位置完成以下步骤：

1. 双击 spinstall.exe 文件。
2. 遵循向导指示信息以安装选定组件。

下一步做什么

要访问 Data Protection for VMware vSphere GUI，请参阅以下内容：

- 第 27 页的『访问 Data Protection for VMware vSphere GUI』

首次启动 GUI 时，配置向导将自动显示。

在 Linux 系统上安装 Data Protection for VMware

使用 InstallAnywhere 方式在 Linux 系统上安装 Data Protection for VMware。

开始之前

安装 Data Protection for VMware 之前，请确保满足以下需求：

- 确保用户标识具有必需的许可权级别，并确保必需的通信端口已打开，然后再继续操作。
- 安装过程创建用户 tdpvmware。您必须以用户 tdpvmware 身份并使用 root 用户标识发出所有 **vmcli** 命令。
- 以控制台方式安装时，需要 X Window Server。
- 确保您已复查以下需求：
 - 第 10 页的『系统需求』
 - 第 14 页的『必需的安装许可权』
 - 第 14 页的『必需的通信端口』

过程

要安装 Data Protection for VMware，请完成以下步骤：

1. 从安装文件夹下，将目录切换至 CD/Linux/DataProtectionForVMware。
2. 在命令行中输入以下命令：

```
./install-Linux.bin
```

结果

如果接收到任何警告或错误，请检查日志文件以获取更多信息。请参阅第 77 页的『日志文件活动』。

如果因失败而未能安装 Data Protection for VMware，请参阅第 33 页的『在 Linux 系统上卸载 Data Protection for VMware』中的"手动除去 Data Protection for VMware"过程。

在 Linux 上执行 Data Protection for VMware 的全新安装

如果 Linux 安装中断，通常您可以重新启动该安装。但是，如果安装未能重新启动，那么将需要进行全新安装。

关于此任务

启动全新安装之前，请确保已除去产品。请执行以下步骤以确保清洁的环境：

过程

1. 如果 Data Protection for VMware vSphere GUI 已安装，请完成以下任务：
 - a. 通过发出以下命令，停止 Data Protection for VMware 命令行界面：
`/etc/init.d/vmcli stop`
 - b. 通过发出以下命令，停止 Data Protection for VMware GUI Web 服务器：
`/etc/init.d/webserver stop`
 - c. 通过发出以下命令，除去 .rpm 包：
`rpm -e TIVsm-TDPVMwarePlugin`
2. 除去 Deployment Engine 产品条目：
 - a. 发出以下命令，以列出所有 Deployment Engine 条目：
`/usr/ibm/common/acs/bin/de_lsrootiu.sh`
 - b. 发出以下命令，以除去所有 Deployment Engine 条目：
`/usr/ibm/common/acs/bin/deleteRootIU.sh <UUID> <discriminant>`
 - c. 除去 /var/ibm/common 目录。
 - d. 除去 /usr/ibm/common 目录。
 - e. 如果存在 /tmp 目录，请通过除去 acu_de.log 文件将其清除。
 - f. 除去包含安装 Deployment Engine 的用户标识的 /tmp 目录。
 - g. 除去 /etc/inittab 系统文件中所有的 Deployment Engine 条目。这些条目通过 #Begin AC Solution Install block 和 #End AC Solution Install block 定界。除去这些定界符之间的所有文本和定界文本本身。
 - h. 除去 /etc/inittab 系统文件中所有的 Deployment Engine 条目。
3. 从已失败安装中除去所有 Data Protection for VMware 文件：
 - a. 除去 <USER_INSTALL_DIR> 中的文件，该目录是已失败安装尝试执行的路径。例如：`/opt/tivoli/tsm/TDPVMware/`
 - b. 除去任何桌面快捷方式。
4. 备份全局注册表文件 (/var/.com.zerog.registry.xml)。备份此文件后，除去引用 Data Protection for VMware 的所有标记。
5. 除去根目录下包含 TDPVMware 字符串的日志文件。例如：
`IA-TDPVMware-00.log` 或 `IA-TDPVMware_Uninstall-00.log`。
6. 除去运行 Data Protection for VMware 命令行界面的用户。
 - a. 发出以下命令：
`userdel -r tdpvmware`
 - b. 发出以下命令：
`groupdel tdpvmware`

提示：在某些版本的 Linux 中，当不存在其他关联的用户时，`userdel` 命令也将除去组。因此，忽略任何与命令相关的失败消息。

结果

完成这些步骤后，启动全新安装。

以静默方式安装 Data Protection for VMware 组件

可在后台安装 Data Protection for VMware。在此静默安装期间，不显示任何消息。

关于此任务

Windows 您可以使用套件安装程序来安装 Data Protection for VMware 和数据移动设备。

Linux 您可以使用独立安装程序来安装 Data Protection for VMware 和数据移动设备。

在 Windows 系统上以静默方式安装 Data Protection for VMware

使用套件安装程序以静默方式安装所有 Data Protection for VMware 组件和数据移动设备功能部件。

开始之前

安装 Data Protection for VMware 和数据移动设备功能部件之前，请确保您的系统满足以下章节中的需求：

- 第 10 页的『系统需求』
- 第 14 页的『必需的安装许可权』
- 第 14 页的『必需的通信端口』

关于此任务

限制：所有功能部件都将安装到其缺省位置。要找到组件的缺省安装目录，请参阅第 1 页的『可安装组件』中的子主题。

过程

要安装 Data Protection for VMware，请完成以下步骤：

1. 从命令提示符发出以下命令：

```
cd extract_folder\TSMVMWARE_WIN
```

2. 输入以下命令：

```
spinstall.exe /silent
```

首次安装卷时显示以下消息：

尚未注册虚拟卷驱动程序。现在，恢复代理进程可以注册此驱动程序。注册期间，可能会显示 Microsoft Windows 徽标警告。接受此警告以允许注册完成。
是否要现在注册虚拟卷驱动程序？

要继续，请输入是以注册虚拟卷驱动程序。

相关任务:

第 33 页的『以静默方式为 Windows 卸载 Data Protection for VMware』

在 Linux 系统上以静默方式安装 Data Protection for VMware

可以定制在 Linux 操作系统上以静默方式安装哪些 Data Protection for VMware 功能部件。

开始之前

安装 Data Protection for VMware 之前，请确保满足以下需求：

- 确保用户标识具有必需的许可权级别，并确保必需的通信端口已打开，然后再继续操作。
- 安装过程创建用户 tdpvmware。您必须以用户 tdpvmware 身份并使用 root 用户标识发出所有 **vmcli** 命令。
- 以控制台方式安装时，需要 X Window Server。
- 确保您已复查以下需求：
 - 第 10 页的『系统需求』
 - 第 14 页的『必需的安装许可权』
 - 第 14 页的『必需的通信端口』

关于此任务

Data Protection for VMware 提供以下适用于 Linux 操作系统的静默安装功能部件：

表 7. Data Protection for VMware 静默安装功能部件

功能部件	描述	缺省情况下是否已安装
Docs	自述文件	是
TDPVMwareDM	此功能部件的安装包括支持文件。 使 IBM Spectrum Protect 能够运行以下备份类型： <ul style="list-style-type: none"> • VM 定期增量备份 • VM 完全增量永久备份 • VM 增量永久增量备份 如果卸载备份工作负载，那么此文件必须安装在 vStorage 备份服务器上。	是
TDPVMwareGUI	Data Protection for VMware vSphere GUI。 注：还包含支持文件安装。	否

过程

要安装 Data Protection for VMware，请从安装包解压缩到的目录中完成以下步骤：

1. 打开 `path../Linux/DataProtectionForVMware/installer.properties` 文件，并对以下条目取消注释以接受许可证（其中 `path` 是安装文件夹）：

```
LICENSE_ACCEPTED=TRUE
```

2. 选择以下其中一种方法来安装 Data Protection for VMware 组件：

- 对于缺省安装，打开 CD/Linux/DataProtectionForVMware 文件夹，并输入以下命令：

```
./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
```

- 对于定制安装，完成以下步骤：

a. 使用相应值编辑 installer.properties 文件：

- 1) 指定 **INSTALL_MODE=Custom**。确保井号 (#) 已从此语句除去。
- 2) 使用 **CHOSEN_INSTALL_FEATURE_LIST** 选项指定要安装的功能部件。例如，如果使用以下值，那么将安装所有功能部件：

```
CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
```

b. 从 CD/Linux/DataProtectionForVMware 文件夹发出以下命令：

```
./install-Linux.bin -i silent -f installer.properties
```

安装 Data Protection for VMware 后进行"第一步"

安装 Data Protection for VMware 之后，准备进行配置。使用配置向导是配置 Data Protection for VMware 的首选方法。

配置工作表

使用此工作表来记录配置和管理 Data Protection for VMware 时所需的信息。此工作表旨在帮助您在配置之后记住您指定的值。

表 8. Data Protection for VMware 配置工作表

项	您使用的值	注释
IBM Spectrum Protect 服务器信息		
IBM Spectrum Protect 服务器地址		
IBM Spectrum Protect 服务器端口		
IBM Spectrum Protect 服务器管理员标识/密码		
IBM Spectrum Protect 服务器管理端口		
节点定义选项		
要向节点添加的前缀		
注册新节点时要使用的策略域		
vCenter 节点名/密码		
VMCLI 节点名/密码		
数据中心节点名/密码 切记：可以创建多个数据中心节点。		数据中心节点名包括指定前缀，后跟下划线字符，最后是数据中心名称。 例如：nodePrefix_datacenterName
vStorage 备份服务器上的数据移动设备节点名/密码 切记：可以创建多个数据移动设备节点。		数据移动设备节点包括数据中心节点名，后跟下划线字符，最后是 DM。 例如：datacenterNodename_DM
远程服务器上的数据移动设备节点名/密码 切记：可以创建不在 vStorage 备份服务器上的多个数据移动设备节点。		

表 8. Data Protection for VMware 配置工作表 (续)

项	您使用的值	注释
装配代理节点	Windows:	
装配代理节点在复原数据时使用。	Linux:	

访问 Data Protection for VMware vSphere GUI

使用 Data Protection for VMware vSphere GUI 来备份、复原和管理 VMware vCenter 环境中的虚拟机。

开始之前

安装期间，必须选择相应选项以保护 vSphere 环境中的数据，然后才能访问 Data Protection for VMware vSphere GUI。

过程

- 如果在安装期间选择了支持通过 **Web 浏览器访问 GUI** 选项，那么可以从浏览器访问 Data Protection for VMware vSphere GUI:
 1. 打开 Web 浏览器，并输入以下 URL:


```
https://hostname:port/TsmVMwareUI
```

 其中:
 - *hostname* 是安装 Data Protection for VMware vSphere GUI 的系统的名称
 - *port* 是可用于访问 vSphere GUI 的端口号。缺省端口号为 9080。对于安全端口，缺省值为 9081。
 2. 使用您的 vCenter 用户标识和密码登录。
- 如果在安装期间未选择支持通过 **Web 浏览器访问 GUI** 选项，那么通过完成以下步骤来启动 Data Protection for VMware vSphere GUI:
 1. 打开 VMware vSphere Client，然后使用 vCenter 用户标识和密码登录。
 2. 在 vSphere Client 的"解决方案和应用程序"面板中，单击 Data Protection for VMware vSphere GUI 图标。

升级 Data Protection for VMware

可以从先前版本的 Data Protection for VMware 升级该软件。

有关与较低版本的兼容性，请参阅技术说明 1993819。

从 V7.1.8 升级：如果升级过程中显示一条消息，询问您是否要覆盖现有 jextract 文件，请选择**全部覆盖**。

升级 Data Protection for VMware

此过程记录如何升级至 Data Protection for VMware V8.1.7。

开始之前

要点：此升级过程适用于未安装 IBM Spectrum Protect Snapshot for VMware 的系统。

您必须具有管理员特权才能升级 Data Protection for VMware。

对现有 Data Protection for VMware vSphere GUI 的更新通过以下方式处理：

- 参数文件在 Data Protection for VMware vSphere GUI 升级过程开始之前备份。
- 将使用相同的 Derby 数据库端口号和 WebSphere® Application Server 缺省基本端口号。
- **Linux** 概要文件 (vmcliprofile) 中的值用于 Data Protection for VMware 命令行界面。

限制：

- **Windows** 当 IBM Spectrum Protect for Virtual Environments 安装到非缺省位置时，升级过程会将 IBM Spectrum Protect for Virtual Environments V8.1.7 功能部件安装到缺省安装目录。无法升级到非缺省位置。请参阅第 1 页的『可安装组件』中的子主题，以了解每个功能部件的缺省安装目录。
- **Linux** **Windows** 升级过程不会安装新组件。

例如，如果先前版本仅安装有 恢复代理程序 GUI，那么升级过程不会安装 恢复代理程序命令行界面。 这种情况下，必须再次运行安装程序并选择安装缺少的组件。

- **Linux** Linux 版本上的 恢复代理程序必须与 Windows 代理上的 恢复代理程序具有相同的版本。 因此，如果升级 Linux 上的 恢复代理程序，那么还必须升级 Windows 代理上的 恢复代理程序版本。

过程

要升级 Data Protection for VMware，请完成以下步骤：

1. 停止正在运行的所有 Data Protection for VMware 组件和服务。
2. 卸载所有已装配的虚拟卷。 可以使用 恢复代理程序 GUI 或命令行界面 (`mount del` 命令) 来卸载卷。
3. 按第 21 页的『在 Windows 系统上安装 Data Protection for VMware 组件』中的指示信息操作。

注： **Linux** 如果安装了数据移动设备 V6.x，那么必须先将其卸载，然后再安装 V8.1.7。 遵循“卸载 IBM Spectrum Protect Linux x86_64 客户机”主题中的指示信息。

4. 下载代码包。
5. 从保存代码包的文件夹中启动升级过程：
 - a. **Windows** 运行 `spinstall.exe` 文件。

- Linux

在一台机器上只能安装一个 Data Protection for VMware vSphere GUI。因此，同一机器上不允许存在多个 Data Protection for VMware vSphere GUI。

在 Windows 64 位系统上以静默方式升级 Data Protection for VMware

您可以在受支持的 64 位操作系统上静默升级 Data Protection for VMware。

开始之前

当 Data Protection for VMware V6.X 安装到非缺省位置时，静默升级过程会将 Data Protection for VMware V8.1.7 功能部件安装到缺省安装目录。无法以静默方式升级到非缺省位置。请参阅第 1 页的『可安装组件』一节中的子主题，以了解每个功能部件的缺省安装目录。

过程

要升级 Data Protection for VMware，请完成以下步骤：

1. 停止正在运行的所有 Data Protection for VMware 组件。
2. 卸装所有已装配的虚拟卷。 可以使用 恢复代理程序 GUI 或命令行界面 (`mount del` 命令) 来卸装卷。
3. 卸装所有已装配的虚拟卷。 可以使用 恢复代理程序 GUI 或命令行界面 (`mount del` 命令) 来卸装卷。
4. 下载代码包。
5. 浏览至 Data Protection for VMware 的文件夹。
6. 从命令提示符窗口中, 输入以下命令: `spinstall.exe /silent GUI_MODE=vcenter DIRECT_START=1 VCENTER_HOSTNAME=<hostname> VCENTER_USERNAME=<username> VCENTER_PASSWORD=<pass> /debuglog <file path>`

在 Linux 系统上以静默方式升级 Data Protection for VMware

可以在受支持的 Linux 操作系统上以静默方式升级 Data Protection for VMware。

关于此任务

将以下 Data Protection for VMware 参数与静默安装功能部件配合使用：

表 9. *Data Protection for VMware* 静默安装升级参数

参数	描述	缺省值
VCENTER_HOSTNAME	vCenter Server 标准域名或 IP 地址。	无
VCENTER_USERNAME	vCenter 用户标识。 此用户标识必须是有权注册和注销扩展的 VMware 管理员。	无
VCENTER_PASSWORD	vCenter 密码。	无

表 9. Data Protection for VMware 静默安装升级参数 (续)

参数	描述	缺省值
DIRECT_START	要在 Web 浏览器中访问 Data Protection for VMware vSphere GUI，请指定 DIRECT_START=YES 。 可通过指向 GUI Web 服务器的 URL 书签来访问 Data Protection for VMware vSphere GUI。 如果不希望在 Web 浏览器中访问 Data Protection for VMware vSphere GUI，请指定 DIRECT_START=NO 。	YES 要点： 升级完成后，除非重新安装产品，否则无法更改 DIRECT_START 值。

过程

要升级 Data Protection for VMware，请完成以下步骤：

1. 确保没有任何活动的备份、复原或装配会话。
2. 确保所有现有 Data Protection for VMware vSphere GUI 或 恢复代理程序 GUI 都已关闭。
3. 下载代码包。
4. 从 Data Protection for VMware 文件夹，转至 Linux 文件夹。
5. 从命令提示符窗口中，输入带有首选参数的 `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` 命令。
例如： `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true -VCENTER_HOSTNAME=hostname -VCENTER_USERNAME=username -VCENTER_PASSWORD=password -DIRECT_START=yes -REGISTER_PLUGIN=yes`

在 vCenter Server Linked Mode 环境中升级 Data Protection for VMware

所有 Data Protection for VMware GUI 主机都必须及时更新，以使 Data Protection for VMware 组件能够支持当前 VMware Linked Mode 功能部件。

关于此任务

注：此信息特定于 VMware vCenter 上运行的 vSphere 应用程序 V6.0、V6.5 和 V6.7。

VMware vCenter Server Linked Mode 是一种工具，该工具提供管理区域的概述，以便服务器可以支持更多数量的虚拟机。 IBM Spectrum Protect Data Protection for VMware 插件与在链接方式下运行的 VMware 兼容。 请参阅 vCenter Enhanced Linked Mode 上的 VMware 文档，以获取有关此 VMware 功能部件的更多信息

当 vCenter 处于链接方式下时，通过 vSphere UI 可在单个视图中查看所有 vCenter。通过登录到链接在一起的任何 vCenter，同一 UI 可视。 因此，IBM Spectrum Protect Data Protection 插件显示在所有 vCenter 上，即使已在单个 vCenter 上对其进行安装和配置也如此。

虽然该插件对于每个 vCenter 都可视，但是该插件的功能仅可供具有关联的 IBM Spectrum Protect Data Protection for VMware GUI 主机的每个 vCenter 使用。

在升级 vCenter Server Linked Mode 环境时，请考虑以下问题：

- 在链接方式使用 vCenter 时，所升级的第一个 vCenter 将导致更新级别的插件对于所有链接的 vCenter 都可视。IBM Spectrum Protect Data Protection for VMware 插件已开发为与单个更低级别发行版的 GUI 主机兼容。例如，Data Protection for VMware V8.1.6 插件仍与 Data Protection for VMware V8.1.4 GUI 主机兼容。
- 虽然更低级别的 GUI 主机仍然适用于更新的插件，但是更新发行版中引入的功能将不起所用。必须及时更新所有 GUI 主机，以实现更新插件的完整功能。

示例

在升级到 V8.1.6 之前，vCenter1 和 vCenter2 处于链接方式下。它们各自具有 IBM Data Protection for VMware GUI 主机。vSphere 内的插件和 GUI 主机的版本为 V8.1.4。

vCenter1 现已升级到 V8.1.6。插件和 GUI host1 的版本现在为 V8.1.6。登录到 vSphere for vCenter2 的用户将会看到 V8.1.6 插件而不是 V8.1.4 插件。然后，用户可以浏览至 **IBM Spectrum Protect -> 配置 -> 连接**，并且看到 vCenter1 具有版本为 V8.1.6 的 GUI 主机，但是 vCenter2 GUI 主机的版本仍为 V8.1.4。

对于 vCenter2，Spectrum Protect 插件仍以与其在 V8.1.4 中的相同方式运作。区别在于，V8.1.6 的任何新功能部件都无法在 vCenter2 上使用，而只能在 vCenter1 上使用，直至完成对 vCenter2 的 GUI 主机的 V8.1.6 升级为止。

卸载 Data Protection for VMware

卸载 Data Protection for VMware 的过程与新安装和升级版本相同。

在 Windows 上卸载 Data Protection for VMware

从 Windows 系统上卸载 Data Protection for VMware 组件并除去文件和目录。

开始之前

为确保成功卸载，请使用以下指导信息：

- 如果其他 Data Protection for VMware Web GUI 主机使用 IBM Spectrum Protect vSphere Client 插件，请勿注销 Web Client 扩展。

关于此任务

卸载完成后，配置和属性文件位于 >C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config 目录中。

过程

1. 停止正在运行的所有 Data Protection for VMware 组件。
2. 卸装所有已装配的虚拟卷。
3. 使用数据移动设备 delete backup 命令删除所有现有的虚拟机备份。
4. 使用 dsmdutil remove 命令移除所有已安装的数据移动设备服务。

要获取服务列表，请转至 C:\Program Files\Tivoli\TSM\baclient\，并运行 dsmcutil list 命令。

使用以下类似命令移除服务，并将带引号的名称调整为列示的服务：

```
dsmcutil remove /name:"TSM Remote Client Agent"
dsmcutil remove /name:"TSM Client Acceptor"
```

5. 单击开始 > 控制面板 > 程序和功能 > 卸载程序。 卸载以下程序：

- IBM Spectrum Protect for Virtual Environments Data Protection for VMware 套件
- IBM Spectrum Protect for Virtual Environments Data Protection for VMware 许可证
- IBM Spectrum Protect JVM

6. 将以下 Data Protection for VMware 文件和目录（如果存在）从文件系统中移除。对于 IBM Spectrum Protect for Virtual Environments V8.1.6 及更高版本，请删除：

```
C:\IBM\SpectrumProtect
C:\Program Files\IBM\SpectrumProtect
C:\ProgramData\Tivoli\TSM
C:\ProgramData\config
C:\IBM\SpectrumProtect
C:\Program Files\IBM\SpectrumProtect
```

还可以移除：

```
C:\Program Files\Tivoli\TSM
```

如果不再需要剩下的日志文件和配置文件。 如果要保留这些文件，那么这些文件将位于 C:\Program Files\Tivoli\TSM\baclient。 对于 IBM Spectrum Protect for Virtual Environments V8.1.4 及先前版本，请删除：

```
C:\IBM\tivoli
C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
C:\Program Files\Common Files\Tivoli
C:\ProgramData\Tivoli\TSM
C:\ProgramData\config
```

还可以移除：

```
C:\Program Files\Tivoli\TSM
```

如果不再需要剩下的日志文件和配置文件。 如果要保留这些文件，那么这些文件将位于 C:\Program Files\Tivoli\TSM\baclient。

下一步做什么

请检查是否已从系统中除去所有组件。

以静默方式为 Windows 卸载 Data Protection for VMware

您可以在 Windows 操作系统上以静默方式卸载 Data Protection for VMware。

关于此任务

卸载完成后，配置和属性文件位于 >C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config 目录中。

过程

要卸载 Data Protection for VMware，请完成以下步骤：

1. 停止正在运行的所有 Data Protection for VMware 组件。
2. 卸载所有已装配的虚拟卷。可以使用 恢复代理程序 GUI 或命令行界面 (`mount del` 命令) 来卸载卷。
3. 在命令提示符窗口中，使用 `cd` 命令切换至以下其中一个文件夹：
 - 要定制卸载操作，请转至 X64 文件夹。
 - 要使用套件安装程序卸载 Data Protection for VMware，请转至 <extract folder>TSM4VE_WIN。
4. 在命令提示符窗口中，运行以下命令：
 - 对于定制卸载操作，请从以下命令中选择：
 - 输入此命令以卸载 Data Protection for VMware 并注销 Data Protection for VMware vSphere GUI：

```
spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
VCENTER_HOSTNAME=<vCenter 主机名或 IP>
VCENTER_USERNAME=<vCenter 用户名>
VCENTER_PASSWORD=<vCenter 密码>"
```
 - 要使用套件安装程序卸载所有功能部件，请输入以下命令：

```
spinstall.exe /silent /remove
```
5. 卸载完成后，重新启动系统。

在 Linux 系统上卸载 Data Protection for VMware

在受支持的 Linux 操作系统上卸载 Data Protection for VMware 以及移除文件和目录。

开始之前

为确保成功卸载，请使用以下指导信息：

- 移除 IBM Spectrum Protect Server 中的节点。必须先执行此操作才能卸载 Data Protection for VMware 产品：
 1. 通过 `/opt/tivoli/tsm/client/ba/bin/dsmadm` 运行 `dsmadm`。
 2. 可能需要使用 `del` 命令来删除节点的文件空间：`del file nodename *`
 3. 使用 `q` 命令查询节点：`q filespace nodename *`
 4. 使用 `rem` 命令移除节点：`rem node nodename`
- 停止为数据移动设备创建的 `dsmcad` 服务。使用 <http://www-01.ibm.com/support/docview.wss?uid=swg21358414> 技术说明中的指示信息
 1. 使用 `ps` 命令检查是否正在运行 `dsmcad` 服务：`ps -ef|grep dsmcad`

2. 使用 kill 命令暂停 dsmcad 服务：kill -9 dsmcad-processID
- 必须清除与创建“数据移动设备”服务相关的文件。转至安装目录，然后发出以下命令：

```
/opt/tivoli/tsm/client/ba/bin/dsmutilnx cleanupDmFiles 1
```

按 Enter 键选择节点名，然后按 Enter 删除。

可以在 dsm.sys 中查找节点名

- 当您从 VMware vSphere 5.5 环境卸载 IBM Spectrum Protect vSphere Client 插件时，将仅除去其关联的特权标签和描述。实际的特权仍保持已安装状态。此问题是已知的 VMware 限制。有关更多信息，请参阅以下 VMware 知识库文章：
<http://kb.vmware.com/kb/2004601>。
- 产品卸载后，Data Protection for VMware 支持文件不会除去。

关于此任务

在 Linux 系统上卸载 Data Protection for VMware 时，缺省情况下，卸载类型与原始安装类型的过程相同。要使用其他卸载过程，请指定正确的参数。例如，如果使用的是静默安装过程，那么可以通过指定 -i swing 参数来使用安装向导进行卸载。请以 root 用户身份运行卸载过程。必须获取 root 用户概要文件。如果使用 su 命令切换为 root 用户，请使用 su - 命令获取 root 用户概要文件。

卸载过程开始除去程序文件时，取消卸载过程不能使系统回复清洁状态。此情境可能会导致重新安装尝试失败。因此，请通过完成第 35 页的『从 Linux 系统手动除去 Data Protection for VMware』中描述的任务来清理系统。

要卸载 Data Protection for VMware，请完成以下步骤：

过程

1. 切换到卸载程序所在目录。以下路径是卸载程序的缺省位置：/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/
2. 根据安装类型，使用下列方法之一卸载 Data Protection for VMware：

注：必须在一行中输入此过程中的命令。以下示例为适应页格式而显示两行。

- 要使用安装向导卸载 Data Protection for VMware，请输入以下命令：

```
./Uninstall_Tivoli_Data_Protection_for_VMware -i swing
```

- 要使用控制台卸载 Data Protection for VMware，请输入以下命令：

```
./Uninstall_Tivoli_Data_Protection_for_VMware -i console
```

- 要以静默方式卸载 Data Protection for VMware，请输入以下命令：

```
./Uninstall_Tivoli_Data_Protection_for_VMware -i silent  
-f uninstall.properties
```

uninstall.properties 文件包含 vCenter 连接信息。需要此信息以卸载 Data Protection for VMware vSphere GUI。

从 Linux 系统手动除去 Data Protection for VMware

关于此任务

使用标准卸载过程无法卸载 Data Protection for VMware 时，必须如以下步骤中所述，手动从系统除去 Data Protection for VMware。请以 root 用户身份完成此过程。

过程

1. 如果已安装 Data Protection for VMware vSphere GUI，请使用此命令将其程序包从 Package Manager 数据库中除去：

```
rpm -e TIVsm-TDPVMwarePlugin
```

2. 使用此命令除去 IBM Spectrum Protect API：

```
rpm -e TIVsm-API64  
gskssl64.linux.x86_64.rpm  
skcrypt64.linux.x86_64  
TIVsm-TDPVMwarePlugin.x86_64.rpm  
TIVsm-DPAPI.x86_64.rpm
```

3. 除去 Deployment Engine 中的产品条目：

- a. 发出以下命令来查看所有条目的列表：

```
/usr/ibm/common/accsi/bin/de_lsrootiu.sh
```

- b. 发出以下命令来除去与 Data Protection for VMware 相关的已安装单元条目：

```
/usr/ibm/common/accsi/bin/deleteRootIU.sh <UUID> <discriminant>
```

确保已除去这些单元条目：

```
FBJRE  
TDPVMwareGUI  
JavaHelp  
TDPVMwareDM
```

卸载程序完成之后，将移除以下目录（如果存在）：

- /opt/tivoli/tsm/client
- /opt/tivoli/tsm/tdpvmware

移除用户 tdpvmware 以及关联的目录：

- userdel tdpvmware
- /home/tdpvmware
- /etc/adsm

4. 备份全局注册表文件 (/var/.com.zerog.registry.xml)。文件备份后，除去与 Data Protection for VMware 相关的所有标记。
5. 除去安装目录 (/opt/tivoli/tsm/tdpvmware) 中的所有文件。此外，除去桌面上的所有快捷方式。
6. 备份 /root 目录中文件名包含 TDPVMware 的日志文件。例如，IA-TDPVMware-00.log 或 IA-TDPVMware_Uninstall-00.log。在这些日志文件备份完成后，将其除去。如果安装过程再次失败，那么通过除去这些文件您就可以查看发出的所有错误。
7. 现在可以按第 22 页的『在 Linux 系统上安装 Data Protection for VMware』中所述再次安装本产品。

修改 Data Protection for VMware 的现有安装

本部分提供了在现有 Data Protection for VMware 安装中修改程序包和功能部件的指示信息。

通过使用 Suite Installer，可以更改系统上安装的底层程序包。要修改任何独立的程序包功能部件，可以使用 Windows 的**程序和功能**控制面板。

在 Data Protection for VMware 的现有安装中修改程序包

您可以使用套件安装程序来对 Data Protection for VMware 的现有安装中的程序包进行更改。

开始之前

在使用套件安装程序之前，请确保您具有源介质。 套件安装程序的 spinstall.exe 可执行文件位于安装包的根目录下。

关于此任务

使用套件安装程序来修改在 Data Protection for VMware 的现有安装中安装的程序包。您可以选择添加或删除：

- 数据移动设备
- Data Protection for VMware

请完成以下步骤：

过程

1. 双击 spinstall.exe 文件以运行套件安装程序包。
2. 使用**定制安装**面板上的程序包复选框来确定需要安装的程序包。
3. 选择此安装所需的程序包。

在 Data Protection for VMware 的现有安装中修改功能部件

您可以使用 Windows“程序和功能”控制面板来对 Data Protection for VMware 的现有安装中的功能部件进行更改。

开始之前

在修改安装包之前，请确保您具有源介质。

关于此任务

使用 Windows 来修改 Data Protection for VMware 的现有安装中可用的独立程序包功能部件。 您可以选择修改以下功能部件：

- 数据移动设备
- Data Protection for VMware

请完成以下步骤：

过程

1. 在 Windows 控制面板的**程序和功能**部分中，右键单击 IBM Spectrum Protect for Virtual Environments: Data Protection for VMware 应用程序。
2. 单击**修改**以更新当前安装的程序包功能部件。
3. 选择此安装所需的功能部件。

第 2 章 配置 Data Protection for VMware

本节提供有关配置 Data Protection for VMware 和启动相关服务的指示信息。

提示：安装 Data Protection for VMware 之后，IBM License Metric Tool 仅在连接到 IBM Spectrum Protect 服务器并用于数据操作时才对数据移动设备进行计数。随后，该数据移动设备将始终包含在许可证计算中。未连接到服务器并且未用于数据操作的数据移动设备将从许可证计算中排除。

使用向导配置新安装

使用配置向导来完成初始配置或较小的更改。

开始之前

安装有 Data Protection for VMware 的系统必须通过网络连接至以下服务器：

- vStorage 备份服务器
- IBM Spectrum Protect 服务器
- vCenter Server

关于此任务

要配置 Data Protection for VMware 环境，请完成以下步骤：

过程

1. 打开 Web 浏览器，并输入 GUI Web 服务器地址。 例如：
`https://guihost.mycompany.com:9081/TsmVMwareUI/`
2. 使用 vCenter 用户名和密码登录。
3. 在"入门"窗口中，转至"配置"窗口，然后单击**运行配置向导**。
4. 按照向导中每一页的指示信息操作，直到显示"摘要"窗口。 复查设置，然后单击**完成**以完成配置并退出向导。

提示：随 GUI 一起安装的联机帮助中提供了有关每个配置页面的信息。 在任何 GUI 窗口中单击**了解更多信息**可打开联机帮助以获取任务帮助。 请参阅"运行配置向导"主题。

5. 验证数据移动设备节点是否正确配置：
 - a. 单击**配置选项卡**以查看"配置状态"页面。
 - b. 在"配置状态"页面中，选择某个数据移动设备节点以在"状态详细信息"窗格中查看其状态信息。 节点显示警告或错误时，请单击该节点并使用"状态详细信息"窗格中的信息来解决该问题。 然后，选择该节点并单击**验证所选节点**以确定是否解决了该问题。 单击**刷新**以重新测试所有节点。

结果

捷径：成功完成此向导任务后，备份 VM 数据不需要任何其他配置任务。

使用笔记本编辑现有安装

使用"编辑配置"笔记本来编辑现有配置设置

开始之前

"编辑配置"笔记本为现有配置提供以下任务：

- 设置或更改 IBM Spectrum Protect 管理员标识。
- 重置密码并解锁 VMCLI 节点。
- （vSphere 环境）在 Data Protection for VMware vSphere GUI 域中添加或删除 VMware 数据中心。
- 添加或删除装配代理节点。 修改现有装配代理节点的密码。
- 添加或删除数据移动设备节点。 修改现有数据移动设备节点的密码。
- 启用文件复原。
- 启用数据移动设备节点的标记支持。

关于此任务

要编辑现有配置，请完成以下步骤：

过程

1. 打开 Web 浏览器，并输入 GUI Web 服务器地址。 例如：

`https://guihost.mycompany.com:9081/TsmVMwareUI/`

使用 vCenter 用户名和密码登录。

2. 在"入门"窗口中，转至"配置"窗口，然后单击**编辑配置**。
3. 转到与编辑任务相关的页面，按照指示信息操作。 必须先单击**确定**以保存更改，然后才能继续至另一个"配置设置"页面。否则，您的更改将不会生效。

要点：随 GUI 一起安装的联机帮助中提供了有关每个配置页面的信息。在任何 GUI 窗口中单击**了解更多信息**可打开联机帮助以获取任务帮助。 请参阅"编辑现有配置"主题。

结果

更新后的设置显示在"配置"窗口中。

为文件复原操作启用环境

Windows

在管理员启用文件复原功能后，文件所有者可以在没有帮助的情况下复原文件。

开始之前

如果您没有验证是否满足了所有先决条件，请复审《IBM Spectrum Protect for Virtual Environments: Data Protection for VMware 用户指南》中有关文件复原先决条件的主题。

关于此任务

在安装有 Data Protection for VMware vSphere GUI 的系统上完成以下步骤。

过程

1. 启动 Data Protection for VMware vSphere GUI，方法是打开 Web 浏览器并输入 GUI Web 服务器地址。例如：

```
https://<GUI web server  
address>:9081/TsmVMwareUI/
```

使用 vCenter 用户标识和密码登录。

2. 在"入门"窗口中，单击**配置**，然后从"任务"列表中选择以下其中一项任务：

- 如果要配置新环境，请完成以下步骤：

- a. 选择**运行客户机配置向导**。

- b. 按照向导中每一页的指示信息操作。使用以下指导信息来完成"文件复原"页面：

- 1) 选择**启用文件复原选项**。

- 2) 输入文件复原界面中显示的管理员联系信息。如果您不希望提供联系信息，请取消选中该复选框。

- 3) 如果环境包含 Windows 虚拟机备份，请输入 Windows 域用户凭证。否则，请清空该复选框，并且不输入任何凭证。

提示：文件复原操作使用 Windows 域用户凭证来访问远程虚拟机上的网络共享。如果环境包含 Windows 虚拟机的备份并且未输入凭证或输入了错误的凭证，那么操作将失败。因此，仅在没有 Windows 虚拟机备份的情况下清空此复选框。

- 4) 检查文件复原界面 URL 以验证是否可访问该界面。

切记：记录文件复原界面的 URL。访客虚拟机的所有者可以通过此 URL 访问文件复原界面。

- 5) 单击**确定**以保存您的更改。

- 如果要更新现有环境，请完成以下步骤：

- a. 选择**编辑 TSM 配置**。

- b. 在"文件复原"页面上，使用以下指导信息：

- 1) 选择**启用文件复原选项**。

- 2) 输入文件复原界面中显示的管理员联系信息。如果您不希望提供联系信息，请取消选中该复选框。

- 3) 如果环境包含 Windows 虚拟机备份，请输入 Windows 域用户凭证。否则，请清空该复选框，并且不输入任何凭证。

提示：文件复原操作使用 Windows 域用户凭证来访问远程虚拟机上的网络共享。如果环境包含 Windows 虚拟机的备份并且未输入凭证或输入了错误的凭证，那么操作将失败。因此，仅在没有 Windows 虚拟机备份的情况下清空此复选框。

- 4) 检查文件复原界面 URL 以验证是否可访问该界面。

切记：记录文件复原界面的 URL。访客虚拟机的所有者可以通过此 URL 访问文件复原界面。

- 5) 单击**确定**以保存您的更改。

结果

已为环境启用文件复原操作。文件所有者可以通过使用 URL 访问 IBM Spectrum Protect 文件复原界面来复原其文件。

在 Linux 上设置文件复原操作

Linux

当 Data Protection for VMware 安装在 Linux 系统上时，要启用文件复原功能，必须在 Windows 系统上设置另一个 Data Protection for VMware 环境。

关于此任务

在 Linux 环境中运行 Data Protection for VMware 时，必须在 Windows 系统上安装文件复原功能以启用文件复原功能。

过程

1. 设置一个用于文件复原功能的单独 Windows 服务器。
2. 在 Windows 系统上安装 Data Protection for VMware。在安装期间，请接受缺省值。
3. 在 Windows 系统上配置 Data Protection for VMware 时，请使用下列节点名：
 - a. 创建一个名为 VCENTER_FR 的 vCenter 节点。
 - b. 创建一个名为 VMCLI_FR 的 VMCLI 节点。
 - c. 复用 Linux 环境中的数据中心节点名。
例如：DATACENTER。
 - d. 请勿创建数据移动设备节点。在此方案中，文件复原功能不需要数据移动设备节点。
 - e. 创建一对新的安装代理节点，其中节点名分别为 REMOTE_FR_MP_WIN 和 REMOTE_FR_MP_LNX。
4. 在配置向导的"文件复原"页面上，选择启用文件复原选项。
5. 要访问文件复原界面，请打开 Web 浏览器并输入管理员所提供的 URL。例如：
`https://hostname:9081/FileRestoreUI`

其中，hostname 是安装了 Data Protection for VMware 的 Windows 系统的主机名。

结果

以下示例显示 IBM Spectrum Protect 服务器上的代理节点关系：

tsm: SERVER>q proxy

Target Node	Agent Node
VCENTER	VMCLI_DATACENTER
VCENTER_FR	VMCLI_FR_DATACENTER
DATACENTER	VMCLI_VMCLI_FR
	DATAMOVER1
	REMOTE_MP_WIN REMOTE_MP_LNX
	REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX

为了启用文件复原功能而创建的其他节点具有 _FR 后缀。

修改文件复原操作的选项

Windows

要允许管理员配置和控制文件复原操作的复原处理，请修改 frConfig.props 文件中的选项。

关于此任务

在安装有 Data Protection for VMware vSphere GUI 的系统上完成以下步骤。

过程

1. 转至 frConfig.props 文件所在的目录。例如，打开命令提示符，并发出以下命令：
`cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI`
2. 以管理员方式使用文本编辑器打开 frConfig.props 文件，并根据需要修改选项。使用『文件复原选项』中的信息来确定要修改的选项。
3. 保存更改，并关闭 frConfig.props 文件。

结果

修改的选项将应用于 IBM Spectrum Protect 文件复原界面。

文件复原选项

frConfig.props 选项控制文件复原操作的配置、支持和复原处理。

enable_contact_info=false | true

指定是否提供文件所有者可用于获取支持的管理员联系信息。

false

文件所有者不会接收到管理员联系信息。此值是缺省值。

true

文件所有者将接收到管理员联系信息。

如果指定 **enable_contact_info=true**，那么必须在 **contact_info** 选项中提供信息。

enable_filerestore=false | true

指定文件所有者是否可以使用 IBM Spectrum Protect 文件复原界面从虚拟机复原其文件。

false

文件所有者无法使用 IBM Spectrum Protect 文件复原界面复原其文件。此值是缺省值。

true

文件所有者可以使用 IBM Spectrum Protect 文件复原界面复原其文件。

maximum_mount_points=num_mount_points

指定用户帐户可用的并发恢复点最大数。最小值是 1 个恢复点。最大值是 256 个装配点。缺省值是 2 个装配点。

提示：要防止虚拟机被并发复原操作装配多次，请将此选项设置为较低的值。

mount_session_timeout_minutes=num_mins

指定会话取消之前复原和已装配恢复点可处于空闲状态的时间（以分钟为单位）。取消将卸载恢复点。最大值为 8 小时（480 分钟）。缺省值为 30 分钟。

提示：要防止意外取消会话，请增加分钟数。

restore_info_duration_hours=num_hrs

指定有关最近复原活动的信息在 IBM Spectrum Protect 文件复原界面中保留的时间（以小时为单位）。使用“复原活动”窗口可查看错误信息和最近完成的任务。此信息提供了找到最近复原的文件的一种方法。最大值为 14 天（336 小时）。缺省值为一星期（168 小时）。

contact_info=administrator information

提供文件所有者可用于获取支持的管理员联系信息。联系信息显示在 IBM Spectrum Protect 文件复原界面中的以下位置：

- “登录”窗口
- “帮助”菜单中的“关于”窗格
- 界面消息中的“支持信息”链接

可以使用 Data Protection for VMware vSphere GUI 配置向导或笔记本覆盖以下选项：

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

配置文件复原操作的日志活动

要允许管理员配置和控制文件复原操作的内容格式化方式和内容记录方式，请修改 FRLog.config 文件中的选项。

开始之前

FRLog.config 文件在首次访问 IBM Spectrum Protect 文件复原界面时生成。

关于此任务

在安装有 Data Protection for VMware vSphere GUI 的系统上完成以下步骤。

过程

1. 转至 FRLog.config 文件所在的目录。 打开命令提示符，并发出以下命令：

```
cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
```
2. 以管理员方式使用文本编辑器打开 FRLog.config 文件，并根据需要修改选项。 使用『文件复原日志活动选项』中的信息来确定要修改的选项。
3. 保存更改，并关闭 FRLog.config 文件。
4. 重新启动 GUI Web 服务器：
 - a. 单击开始 > 控制面板 > 管理工具 > 服务。
 - b. 右键单击 **Data Protection for VMware Web 服务器服务**，然后单击重新启动。

结果

设置将应用于文件复原操作的日志记录信息的内容和格式。

文件复原日志活动选项

FRLog.config 选项控制文件复原操作的日志记录信息的内容和格式。

以下选项将文件复原任务的信息记录在 fr_gui.log 文件中：

MAX_LOG_FILES=number

指定要保留的 fr_gui.log 文件最大数。 缺省值为 8。

MAX_LOG_FILE_SIZE=number

指定 fr_gui.log 文件的最大大小（以 KB 为单位）。 缺省值为 8192 KB。

以下选项将文件复原服务的信息记录在 fr_api.log 文件中。 这些服务是与文件复原活动相关的内部 API 服务：

API_MAX_LOG_FILES=number

指定要保留的 fr_api.log 文件最大数。 缺省值为 8。

API_MAX_LOG_FILE_SIZE=number

指定 fr_api.log 文件的最大大小（以 KB 为单位）。 缺省值为 8192 KB。

API_LOG_FILE_NAME=API_log_file_name

指定 API 日志文件的名称。 缺省值为 fr_api.log。

API_LOG_FILE_LOCATION=API_log_file_name

指定 API 日志文件的位置。 必须使用正斜杠 (/) 指定位置。 缺省位置为 C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs。

FR.API.LOG=ON | OFF

指定是否为文件复原服务启用日志记录。

- 要为文件复原服务启用日志记录，请指定 ON。 缺省值为 ON。
- 要为文件复原服务禁用日志记录，请指定 OFF。

要对在文件恢复操作期间可能遇到的问题进行故障诊断，请参阅文件恢复的跟踪选项。跟踪选项也在 `FRLog.config` 文件中指定。

配置数据移动设备节点以获取标记支持

在数据移动设备节点上启用标记支持时，管理员可以向 VMware vCenter 内的库存对象应用数据保护标记。

开始之前

请确保满足以下需求：

- VMware vCenter Server 必须是 V6.0 更新 1 或更高版本。
- 为了使 Data Protection for VMware vSphere GUI 能够在标记支持下正常运行，请确保在 GUI 安装期间满足以下需求：
 - 在同一台服务器上必须安装至少一个数据移动设备和 Data Protection for VMware vSphere GUI。必须配置此数据移动设备节点，以便保存 vCenter 服务器凭证。您可以通过运行配置向导保存数据移动设备节点密码或者在数据移动设备命令行上使用 `dsmc set password` 命令来保存凭证。

如果使用在虚拟机或物理机器上运行的其他数据移动设备作为附加数据移动设备，可以将其安装在其他服务器上。对于标记支持，所有这些数据移动设备都必须使用 `VMTAGDATAMOVER YES` 选项来进行配置。这些附加数据移动设备无需在相同服务器上安装 Data Protection for VMware vSphere GUI 即可使其作为基于标记的数据移动设备来正常工作。

- **Linux** 对于 Linux 数据移动设备，请确保在 `LD_LIBRARY_PATH` 环境变量中指定数据移动设备安装目录和 Java™ 共享库 `libjvm.so`。在数据移动设备上启用 `vmtagdatamover` 选项时，到 `libjvm.so` 的路径将用于标记支持。有关指示信息，请参阅在 vSphere 环境中设置数据移动设备节点。
- **Linux** 在 Linux 操作系统上，必须使用缺省用户名 (`tdpvmware`) 来安装 Data Protection for VMware vSphere GUI。
- 在 UNIX 和 Linux 客户机上，`TSM.PWD` 文件中的现有密码已迁移至同一位置的新密码库。对于 root 用户，密码库的缺省位置为 `/etc/adsm`。对于非 root 用户，密码库的位置由 `passworddir` 选项指定。

迁移后，将删除 `TSM.PWD` 文件。

注：有关使用标记所需权限的进一步信息，请参阅安装 Data Protection for VMware 组件

关于此任务

您可以使用数据保护标记在 VMware 库存对象中配置虚拟机的备份策略。这些数据保护标记在 IBM Spectrum Protect vSphere Client 插件中显示为可更改的设置。

过程

请使用以下某种方法：

选项	描述
使用 vSphere 插件 GUI 配置数据移动设备节点	<div><div><div>1. 从 vSphere 插件中，选择 IBM Spectrum Protect。</div><div>2. 在配置选项卡中，选择数据移动设备。</div><div>3. 在添加数据移动设备面板中，从下拉菜单选择数据中心。</div><div>4. 接受缺省值，或编辑数据移动设备名称、数据移动设备主机名、vCenter 用户和 vCenter 密码的设置。</div><div>5. 设置完成后，单击添加。</div></div><div>要获取更多详细信息，请参阅《Data Protection for VMware vSphere GUI 安装指南》中的"使用 vSphere 插件 GUI 设置数据移动设备节点"主题。</div></div>




选项	描述
要在 Windows 或 Linux 上通过使用 Data Protection for VMware vSphere GUI 为标记支持配置新数据移动设备	<ol style="list-style-type: none"> 1. 在安装 Data Protection for VMware vSphere GUI 的系统上，通过打开 Web 浏览器并输入 GUI Web 服务器地址来启动 GUI。例如： <code>https://<GUI web server address>:9081/TsmVMwareUI/</code> 2. 使用 vCenter 用户标识和密码登录。 3. 转至配置选项卡，并选择编辑 IBM Spectrum Protect 配置操作。 4. 转至"配置"配置页的"数据移动设备节点"页面。 5. 通过完成以下步骤来添加数据移动设备节点： <ol style="list-style-type: none"> a. 对于要为其设置标记支持的数据移动设备节点，请选择创建服务。缺省情况下，选中基于标记的节点，为标记支持启用数据移动设备节点 b. 要将基于标记的节点指定为缺省数据移动设备节点，请选中缺省数据移动设备。缺省数据移动设备节点会备份添加到数据中心内的任何容器的所有新的 VM，前提是此容器已处于保护集合中。缺省数据移动设备还会备份保护集合中未分配 Data Mover 标记的所有 VM。 提示：对于 Linux 系统，如果选择新的数据移动设备节点作为缺省标记节点，那么请从与该数据中心关联的任何其他数据移动设备选项文件中除去 vmtagdefaultdatamover 行。 c. 单击确定以保存您的更改。 这样会将 vmtagdatamover 和 vmtagdefaultdatamover（如果已设置）选项添加到数据移动设备选项文件 (dsm.opt) 中。
当数据移动设备节点与 Data Protection for VMware vSphere GUI 位于相同服务器上时，要为标记支持配置现有 Windows 数据移动设备节点	<ol style="list-style-type: none"> 1. 完成先前指示信息中的步骤 1 - 3，为标记支持配置新数据移动设备节点。 2. 在"数据移动设备节点"页面上，针对要为其启用标记支持的节点选择基于标记的节点。 3. 可选：要将基于标记的节点指定为缺省数据移动设备节点，请选中缺省数据移动设备。

选项	描述
要为标记支持配置现有 Linux 数据移动设备节点或者配置与 Data Protection for VMware vSphere GUI 位于不同服务器上的现有 Windows 数据移动设备节点	<ol style="list-style-type: none">1. 请将 vmtagdatamover yes 选项添加到数据移动设备选项文件（针对 Linux 为 dsm.sys，针对 Windows 为 dsm.opt）。2. 可选：要将基于标记的节点指定为缺省数据移动设备节点，请将 vmtagdefaultdatamover yes 或 vmtagdefaultdatamover dm_name 选项添加到数据移动设备选项文件中。 提示：对于 Linux 系统，如果选择新的数据移动设备节点作为缺省标记节点，那么请从与该数据中心关联的任何其他数据移动设备选项文件中除去 vmtagdefaultdatamover 行。

结果

对数据移动设备节点启用标记支持后，数据移动设备将在运行备份时查询 VMware 库存以获取标记信息。然后，数据移动设备将根据所设置的数据保护标记来备份虚拟机。如果未对数据移动设备节点配置标记支持，那么备份操作期间将会忽略所有数据保护标记。

相关信息:

-  Vmtagdatamover
-  Vmtagdefaultdatamover
-  配置备份策略

配置环境以执行虚拟机即时完全复原操作

为虚拟机即时完全复原和即时访问操作设置专用的 iSCSI 网络。

开始之前

使用相应的 VMware 文档（ESXi 或 vSphere）来确定配置 iSCSI 虚拟交换机和虚拟网络所要遵循的特定步骤。尽管提供了常规的准则，但有关如何添加虚拟网络和虚拟交换机的特定文档和说明已超出了产品文档的范围。本出版物发布时，VMware vSphere ESXi 和 vCenter 5.5 文档在 VMware ESXi 和 vCenter Server 5 文档处提供。"联网"主题包含有关添加以及配置虚拟交换机机和虚拟网络的信息。

要点：提供这些配置设置是为了帮助设置 VMware 环境以执行高效的虚拟机即时完全复原和即时访问操作。但是，由于这些设置适用于 VMware 配置任务和 VMware 用户界面，您必须参阅相应的 VMware 文档以获取详细的逐步指示信息。

关于此任务

此过程要求用于即时复原操作的每个 ESXi 主机上都具有一个 iSCSI 适配器。请使用相应的 VMware 文档来设置该适配器。本出版物发布时，以下过程在此 VMware vSphere 资源处提供。

- 要设置软件 iSCSI 适配器，请遵循 VMware“配置软件 iSCSI 适配器”过程中的指示信息。
- 要设置硬件 iSCSI 适配器，请遵循 VMware“设置独立的硬件 iSCSI 适配器”过程中的指示信息。

1. 配置 ESXi 主机上的 iSCSI 软件

过程

此任务将设置用于基本配置的 iSCSI 软件。

1. 登录到将用于即时复原操作的 ESXi 主机。
2. 遵循此 VMware 知识库文章中的指示信息，直至 iSCSI 适配器已启用：<http://kb.vmware.com/kb/1008083>
IBM Spectrum Protect 会自动发现 iscsi 目标服务器。
3. 验证 ESXi 主机上 iSCSI 适配器的 IP 地址是否为数据移动设备所使用的子网地址。
4. 验证 ESXi 主机上是否已启用 Storage vMotion 许可证。

下一步做什么

在 ESXi 主机上设置 iSCSI 软件之后，在数据移动设备系统上安装和配置应用程序。

2. 在数据移动设备上安装和配置应用程序

开始之前

如果恢复代理程序和 IBM Spectrum Protect 数据移动设备已安装并配置在数据移动设备系统上，请从步骤 3 开始执行。

过程

此任务将设置数据移动设备系统，该系统带有用于即时复原操作的应用程序和设置。

1. 在数据移动设备系统上安装恢复代理程序和 IBM Spectrum Protect 数据移动设备。
在安装 Data Protection for VMware 过程的步骤 4 中，选择安装完整的数据移动设备以用于访客内应用程序保护安装类型。
2. 配置数据移动设备。
遵循客户机文档中“配置数据移动设备”主题的指示信息。
3. 设置 iSCSI 服务器 IP 地址：
 - a. 转至 C:\Program Files\Tivoli\TSM\baclient\dsm.opt 文件，然后指定以下参数：
VMISCSIServeraddress=<公开 iSCSI 目标的数据移动设备系统上网卡的 IP 地址。>
如果数据移动设备系统具有多个网卡，请确保为 iSCSI 网络指定正确的网卡。

下一步做什么

设置数据移动设备系统之后，在恢复代理进程 CLI 与恢复代理进程 GUI 之间建立连接。

3. 设置恢复代理进程连接

开始之前

可以将恢复代理进程命令行界面 (CLI) 版本 7.1.x 视为恢复代理进程 GUI 的命令行 API。可以使用恢复代理进程 CLI 来与恢复代理进程 GUI 通信。

过程

此任务将在恢复代理进程 CLI 与恢复代理进程 GUI 之间建立连接。

1. 在数据移动设备系统上启动恢复代理进程 CLI。
在 **Windows** 开始菜单中，单击程序 > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect 恢复代理进程**。

2. 在命令提示符窗口中，输入以下命令：

```
RecoveryAgentShell.exe -c set_connection mount_computer  
<公开 iSCSI 目标的数据移动设备系统上网卡的 IP 地址。>
```

此命令将在恢复代理进程 CLI 与恢复代理进程 GUI 之间建立连接。

下一步做什么

建立连接之后，配置专用的 iSCSI 网络。

4. 为 ESXi 主机和数据移动设备配置专用的 iSCSI 网络

开始之前

请查看以下准则，然后再继续进行此任务。

- 为即时复原操作使用专用的 iSCSI 网络。
- 用于即时复原操作的每个 ESXi 主机都必须具有第二个可用的物理网卡。此第二网卡绑定到各自 ESXi 主机的软件 iSCSI 适配器。
- 虚拟机中运行的数据移动设备系统必须具有第二个可用的网卡。此第二网卡绑定到 ESXi 主机的软件 iSCSI 适配器。
- 用于即时复原操作的每个 ESXi 主机都必须具有辅助 VMware 数据存储。此临时数据存储包含操作期间创建的虚拟机的配置信息和数据。

过程

此任务将为 ESXi 主机和虚拟机中运行的数据移动设备设置专用的 iSCSI 网络。

1. 登录到将用于即时复原操作的 ESXi 主机。

2. 为 iSCSI 网络设置虚拟交换机。

以下步骤使用 *vSwitch1* 作为虚拟交换机。

- a. 为连接类型选择 **VMkernel** 网络适配器。
iSCSI 网络需要此连接类型。
- b. 为 **VMkernel** 网络访问选择创建 **vSphere** 标准交换机。
- c. 为 **VMkernel** 连接设置选择网络标签。

指定一个标签，表明 *vSwitch1* 和此网络用于您的 iSCSI 流量。

例如：*VMkernel iSCSI*。

- d. 在 **VMkernel1 IP 连接** 设置中指定 *vSwitch1* 的 IP 地址和子网掩码。
请勿更改子网掩码或 **VMkernel1** 缺省网关值。
 - e. 指定内核端口，以使 iSCSI 网络能够正常工作。
3. 为虚拟机网络设置虚拟交换机。
以下步骤使用 *vSwitch0* 作为虚拟交换机。
 - a. 为连接类型选择虚拟机。
 - b. 为 **VMkernel1** 网络访问选择创建 **vSphere** 标准交换机。
 - c. 转至端口组属性选项卡，然后选择网络标签。
指定与为 *vSwitch1* 虚拟机网络所指定标签相同的标签。
例如：*VMkernel iSCSI*。
 4. 将新创建的 iSCSI 适配器与 **VMkernel1** 网络适配器绑定。
遵循 VMware"将 iSCSI 适配器与 VMkernel 适配器绑定"过程中的指示信息。本出版物发布时，此过程在 VMware ESXi 和 vCenter Server 5 文档处提供。

提示：如果在扫描 iSCSI 设备时发生超时，请减少连接到 ESXi 主机的 iSCSI 设备数。然后，再次扫描 iSCSI 设备。
 5. 验证 iSCSI 适配器绑定属性是否正确。
 - a. 在 VMware vSphere Client 中，转至 **硬件 > 存储适配器**。
 - b. 右键单击 iSCSI 适配器，然后选择 **iSCSI 发起方属性**。确保存在以下绑定属性：

表 10. iSCSI 网络设置

虚拟机网络	iSCSI 网络
标准交换机: <i>vSwitch0</i>	标准交换机: <i>vSwitch1</i>
虚拟机端口组: VM 网络	VMkernel1 端口: <i>VMkernel iSCSI</i> 提示: <i>VMkernel iSCSI</i> 绑定到 VMkernel1 适配器: <i>vmk1</i> ，该适配器位于物理网络适配器: <i>vmnic1</i> 上。
物理适配器: <i>vmnic0</i>	VMkernel1 网络适配器: <i>vmk1</i>
	物理网络适配器: <i>vmnic1</i>
	虚拟网络适配器 IP 地址: 192.168.42.x (iSCSI 网络的子网)

结果

专用 iSCSI 网络已准备就绪，可用于完全 VM 即时复原和即时访问操作。

配置 Data Protection for VMware 的安全设置

Data Protection for VMware 数据移动设备、vmcli 命令行界面和 Data Protection for VMware vSphere GUI 组件需要配置以启用与 IBM Spectrum Protect 服务器的安全连接。

配置安全设置以将数据移动设备和 VMCLI 节点连接到 IBM Spectrum Protect 服务器

在连接到 IBM Spectrum Protect 服务器 V7.1.8 或者 V8.1.2 或更高版本时，有一些配置选项与数据移动设备和 VMCLI 节点的 Data Protection for VMware 安全设置相关。在大多数用例中建议接受这些选项的缺省值，这样可以透明方式配置这些组件以获取增强的安全性。

使用缺省安全设置进行配置（快速路径）

快速路径详细描述了一些会影响数据移动设备和 VMCLI 节点与服务器的连接安全性的配置选项以及接受缺省值时各种用例的行为。快速路径方案可使端点配置过程中的步骤降至最少。

此方案在节点首次连接时自动从服务器获取证书，并假定 IBM Spectrum Protect 服务器 **SESSIONSECURITY** 参数设置为 **TRANSITIONAL**，这是首次连接时的缺省值。在首先将 IBM Spectrum Protect 服务器升级到 V7.1.8 及更高 V7 级别或者 V8.1.2 及更高 V8 级别，然后将 Data Protection for VMware 升级到这些级别时，您可以遵循此方案，反之亦然。

警告： 如果针对 LDAP 认证配置了 IBM Spectrum Protect 服务器，那么不能使用此方案。如果使用 LDAP，那么可使用 `dsmcert` 实用程序手动导入必需的证书。有关更多信息，请参阅第 55 页的『在不使用自动证书分发的情况下进行配置』。

影响会话安全性的数据移动设备节点选项

以下 `dsmc` 选项指定数据移动设备节点的安全设置。有关这些选项的更多信息，请参阅客户机选项参考。

- **SSLREQUIRED。** 缺省值 `Default` 支持到 V7.1.8 或 V8.1.2 之前的服务器的现有会话安全连接，并自动配置 Data Protection for VMware 数据移动设备以使用 TLS 进行认证，从而安全地连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器。
- **SSLACCEPTCERTFROMSERV。** 缺省值 `Yes` 支持数据移动设备自动接受来自服务器的自签名公用证书，并自动配置数据移动设备以在数据移动设备连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器时使用此证书。
- **SSL。** 缺省值 `No` 指示在数据移动设备和 V7.1.8 或 V8.1.2 之前的服务器之间传输数据时，不使用加密。在数据移动设备连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器时，缺省值 `No` 指示不加密对象数据。在数据移动设备与服务器通信时，加密所有其他信息。值 `Yes` 指示在数据移动设备与服务器通信时使用 TLS 加密所有信息，包括对象数据。
- **SSLFIPSMODE。** 缺省值 `No` 指示不需要联邦信息处理标准 (FIPS) 认证的 TLS 库。

此外，仅在数据移动设备使用 TLS 连接来连至 V7.1.8 或 V8.1.2 之前的服务器时，以下选项才适用。在数据移动设备连接到更高版本的服务器时，将忽略这些选项。

- **SSLDISABLELEGACYTLS。** 值 `No` 指示数据移动设备不需要 TLS 1.2 用于 SSL 会话。其允许使用 TLS 1.1 和较低级别 SSL 协议的连接。在数据移动设备与 V7.1.7 或者 V8.1.1 或更低版本的 IBM Spectrum Protect 服务器通信时，`No` 为缺省值。
- **LANFREESL。** 缺省值 `No` 指示如果配置了不依赖 LAN 的数据传输，那么在与存储代理程序通信时数据移动设备不使用 TLS。

- REPLSSLPORT。 指定在数据移动设备与复制目标服务器通信时针对 TLS 启用的 TCP/IP 端口地址。

影响会话安全的 VMCLI 节点选项

以下参数指定 VMCLI 节点的安全设置。 有关这些选项的更多信息，请参阅概要文件参数。

- VE_TSM_SSL。 缺省值 NO 指示在数据移动设备和 V7.1.8 或 V8.1.2 之前的服务器之间传输数据时，不使用加密。 如果想要在连接到 V7.1.8 之前的服务器时使用 TLS 加密所有信息，请将该值设置为 YES。
- VE_TSM_SSLACCEPTCERTFROMSERV。 缺省值 YES 支持接口自动接受来自服务器的自签名公用证书，并自动配置接口以在数据移动设备连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器时使用此证书。
- VE_TSM_SSLREQUIRED。 缺省值 DEFAULT 支持到 V7.1.8 或 V8.1.2 之前的服务器的现有会话安全连接，并自动配置接口以使用 TLS 进行认证，从而安全地连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器。

缺省安全设置的用例

- 首先，服务器升级到 V7.1.8 或者 V8.1.2 或更高版本。 然后，升级 Data Protection for VMware。 现有数据移动设备和 VMCLI 节点不使用 SSL 通信：
 - 无需对数据移动设备和 VMCLI 节点的安全选项进行任何更改。
 - 在节点向服务器进行认证时，配置会自动更新为使用 TLS。
- 首先，服务器升级到 V7.1.8 或者 V8.1.2 或更高版本。 然后，升级 Data Protection for VMware。 现有数据移动设备和 VMCLI 节点使用 SSL 通信：
 - 无需对数据移动设备和 VMCLI 节点的安全选项进行任何更改。
 - 将继续使用利用现有服务器公用证书的 SSL 通信。
 - SSL 通信将自动增强为使用服务器所需的 TLS 级别。
- 首先，Data Protection for VMware 升级到 V7.1.8 或者 V8.1.2 或更高版本。 之后升级服务器。 现有数据移动设备和 VMCLI 节点不使用 SSL 通信：
 - 无需对数据移动设备和 VMCLI 节点的安全选项进行任何更改。
 - 对于级别低于 V7.1.8 或 V8.1.2 的服务器，将继续使用现有认证协议。
 - 将服务器更新到 V7.1.8 或者 V8.1.2 或更高版本后，当节点向服务器认证时，配置会自动更新为使用 TLS。
- 首先，Data Protection for VMware 升级到 V7.1.8 或者 V8.1.2 或更高版本。 之后升级服务器。 现有数据移动设备和 VMCLI 节点使用 SSL 通信：
 - 无需对数据移动设备和 VMCLI 节点的安全选项进行任何更改。
 - 对于级别低于 V7.1.8 或 V8.1.2 的服务器，将继续使用利用现有服务器公用证书的 SSL 通信。
 - 将服务器更新到 V7.1.8 或者 V8.1.2 或更高版本后，SSL 通信将自动增强为使用服务器所需要的 TLS 级别。
- 首先，Data Protection for VMware 升级到 V7.1.8 或者 V8.1.2 或更高版本。 然后，数据移动设备和 VMCLI 节点连接到多个服务器。 服务器在不同时间进行升级：
 - 无需对数据移动设备和 VMCLI 节点的安全选项进行任何更改。

- 数据移动设备和 VMCLI 节点将现有认证和会话安全协议用于版本低于 V7.1.8 或 V8.1.2 的服务器，并且在初始连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器时自动升级为使用 TLS 认证。按服务器管理会话安全。
- 新客户机安装，服务器为 V7.1.8 或者 V8.1.2 或更高版本：
 - 根据新安装配置 Data Protection for VMware。
 - 安全选项的缺省值将针对 TLS 加密的会话认证自动配置数据移动设备和 VMCLI 节点。
 - 如果需要加密客户机与服务器之间的所有数据传输，那么将 SSL 参数设置为值 Yes。
- 新客户机安装，服务器版本低于 V7.1.8 或 V8.1.2：
 - 根据新客户机安装配置客户机。
 - 如果不需要对所有数据传输使用 SSL 加密，那么接受客户机会话安全参数的缺省值。
 - 将使用非 SSL 认证协议，直至服务器升级到 V7.1.8 或者 V8.1.2 或更高版本。
 - 如果需要加密数据移动设备和服务器之间的所有数据传输，那么将 SSL 参数设置为值 Yes，然后继续手动配置 SSL。
 - 请参阅 Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer 以获取配置指示信息。
 - 将服务器更新到 V7.1.8 或者 V8.1.2 或更高版本后，SSL 通信将自动增强为使用服务器所需要的 TLS 级别。

在不使用自动证书分发的情况下进行配置

本方案详细描述了在不接受来自服务器的自动证书分发时影响数据移动设备和 VMCLI 节点安全的配置选项。例如，如果将服务器配置为使用 LDAP 认证或者需要认证中心 (CA) 签署证书，那么不接受来自服务器的自动证书分发。

影响会话安全的选项

安全设置选项与第 53 页的『使用缺省安全设置进行配置（快速路径）』中描述的选项相同，但唯一例外的是，您必须将 SSLACCEPTCERTFROMSERV 选项设置为 No 以确保在数据移动设备节点首次连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器时，节点不会自动接受来自服务器的自签名公用证书。

在不使用自动证书分发的情况下配置数据移动设备节点的用例

如果无法实现或不需要自动证书分发，那么使用 dsmcert 实用程序来导入证书。从 IBM Spectrum Protect 服务器或 CA 获取必需证书。CA 可来自于诸如 VeriSign 或 Thawte 等公司，或者是贵公司内部维护的内部 CA。

如果数据移动设备和 VMCLI 节点位于同一机器上，那么只需要一个证书。如果节点位于不同的机器上，那么每台机器都需要一个证书。

- 首先，将服务器升级到 V7.1.8 或 V8.1.2。然后，升级 Data Protection for VMware。现有数据移动设备节点不使用 SSL 通信：
 - 使用值 No 设置 SSLACCEPTCERTFROMSERV 选项。

- 从 IBM Spectrum Protect 服务器或 CA 获取必需证书，并使用 dsmcert 实用程序导入证书。请参阅 Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer 以获取配置指示信息。
- 首先，将服务器升级到 V7.1.8 或 V8.1.2。然后，升级 Data Protection for VMware。现有数据移动设备节点使用 SSL 通信：
 - 无需对数据移动设备节点的安全选项进行任何更改。如果节点已有助于 SSL 通信的服务器证书，那么 SSLACCEPTCERTFROMSERV 选项不适用。
 - 将继续使用利用现有服务器公用证书的 SSL 通信。
 - SSL 通信将自动增强为使用服务器所需的 TLS 级别。
- 首先，将 Data Protection for VMware 升级到 V7.1.8 或 V8.1.2。之后升级服务器。现有数据移动设备节点不使用 SSL 通信：
 - 使用值 No 设置 SSLACCEPTCERTFROMSERV 选项。
 - 对于级别低于 V7.1.8 或 V8.1.2 的服务器，将继续使用现有认证协议。
 - 在数据移动设备节点连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器之前：
 - 从 IBM Spectrum Protect 服务器或 CA 获取必需证书，并使用 dsmcert 实用程序导入证书。请参阅 Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer 以获取配置指示信息。
- 首先，将 Data Protection for VMware 升级到 V7.1.8 或 V8.1.2。之后升级服务器。现有数据移动设备节点使用 SSL 通信
 - 无需对数据移动设备节点的安全选项进行任何更改。如果节点已有助于 SSL 通信的服务器证书，那么 SSLACCEPTCERTFROMSERV 选项不适用。
 - 对于级别低于 V7.1.8 或 V8.1.2 的服务器，将继续使用利用现有服务器公用证书的 SSL 通信。
 - 将服务器更新到 V7.1.8 或者 V8.1.2 或更高版本后，SSL 通信将自动增强为使用服务器所需要的 TLS 级别。
- 首先，将 Data Protection for VMware 升级到 V7.1.8 或 V8.1.2。然后，数据移动设备节点连接到多个服务器。服务器在不同时间进行升级：
 - 使用值 No 设置 SSLACCEPTCERTFROMSERV 选项。
 - 对于级别低于 V7.1.8 或 V8.1.2 的服务器，将继续使用现有认证协议。
 - 在数据移动设备节点连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器之前，或者在任何服务器级别都需要 SSL 通信时：
 - 从 IBM Spectrum Protect 服务器或 CA 获取必需证书，并使用 dsmcert 实用程序导入证书。请参阅 Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer 以获取配置指示信息。
 - 数据移动设备节点将现有认证和会话安全协议用于版本低于 V7.1.8 或 V8.1.2 的服务器，并且在初始连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器时自动升级为使用 TLS 认证。按服务器管理会话安全。
- 新 Data Protection for VMware 安装，服务器为 V7.1.8 或者 V8.1.2 或更高版本：
 - 根据新安装配置 Data Protection for VMware。
 - 使用值 No 设置 SSLACCEPTCERTFROMSERV 选项。
 - 从 IBM Spectrum Protect 服务器或 CA 获取必需证书，并使用 dsmcert 实用程序导入证书。请参阅 Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer 以获取配置指示信息。

- 如果需要加密数据移动设备与服务器之间的所有数据传输，那么将 SSL 参数设置为值 Yes。
- 新 Data Protection for VMware 安装，服务器版本低于 V7.1.8 或 V8.1.2，需要 SSL 加密会话：
 - 根据新安装配置 Data Protection for VMware。
 - 将 SSL 参数设置为值 Yes。
 - 从 IBM Spectrum Protect 服务器或 CA 获取必需证书，并使用 dsmcert 实用程序导入证书。请参阅 Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer 以获取配置指示信息。
- 新 Data Protection for VMware 安装，服务器版本低于 V7.1.8 或 V8.1.2，不需要 SSL 加密会话：
 - 根据新安装配置 Data Protection for VMware。
 - 使用值 No 设置 SSLACCEPTCERTFROMSERV 选项。
 - 将使用非 SSL 认证协议，直至服务器升级到 V7.1.8 或者 V8.1.2 或更高版本。
 - 在数据移动设备节点连接到 V7.1.8 或者 V8.1.2 或更高版本的服务器之前：
 - 从 IBM Spectrum Protect 服务器或 CA 获取必需证书，并使用 dsmcert 实用程序导入证书。请参阅 Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer 以获取配置指示信息。

使用传输层安全性配置 Data Protection for VMware vSphere GUI 通信

Data Protection for VMware vSphere GUI 使用传输层安全性 (TLS) 协议提供与 Web 浏览器、VMware vCenter Server 和 (可选) IBM Spectrum Protect 服务器的安全通信。

关于此任务

对于与 Web 浏览器和 VMware VCenter Server 的通信，始终启用 TLS 协议。在安装 Data Protection for VMware 期间，将生成自签名 TLS 数字证书并用于连接。

也可以使用由认证中心 (CA) 签署的证书与 Web 浏览器进行通信。Data Protection for VMware 要使用来自 CA 的证书，请参阅使用第三方证书进行 Web 浏览器会话。

对于与 IBM Spectrum Protect 服务器的通信，是否使用 TLS 协议取决于服务器版本。

如果使用 IBM Spectrum Protect 服务器 V7.1.7 或 V8.1.1 或更早版本

使用 TLS 协议与服务器通信是可选操作。您可以手动启用 Data Protection for VMware vSphere GUI 以通过 TLS 协议与服务器通信，方法是根据第 58 页的『启用与 IBM Spectrum Protect 服务器的安全通信』中的描述，创建或更新信任库并导入证书

如果使用 IBM Spectrum Protect 服务器 V7.1.8 或 V8.1.2 或更高版本

必须使用 TLS 协议。在大多数情况下，首次使用第 53 页的『使用缺省安全设置进行配置 (快速路径)』中描述的缺省安全设置时，将自动创建信任库。但是，在某些情况下，可能需要手动创建信任库。

要点：当 Data Protection for VMware vSphere GUI 首次与服务器通信时，快速路径场景会自动获取证书，并假设 IBM Spectrum Protect 服务器

SESSIONSECURITY 参数设置为 **TRANSITIONAL**，这是首次连接时的缺省值。在 GUI 连接到服务器之后，**SESSIONSECURITY** 参数设置为 **STRICT**。由于 GUI 使用服务器管理员标识连接服务器，因此如果另一个实体已经使用该标识进行连接，那么在尝试连接服务器时，GUI 中会显示错误消息。要解决此问题，请将 **SESSIONSECURITY** 参数设置回 **TRANSITIONAL**。

启用与 IBM Spectrum Protect 服务器的安全通信

如果使用的是 IBM Spectrum Protect 服务器 V7.1.7 或更早版本或者 V8.1.2 或更早版本，使用 TLS 协议连接服务器是可选的，如果想要使用该协议支持 Data Protection for VMware vSphere GUI 与服务器通信，必须手动启用该通信。

开始之前

从服务器管理员处获取证书副本。

关于此任务

如果使用服务器 V7.1.8 或 V8.1.2 或更高版本，TLS 协议是必需的，并且在使用第 53 页的『使用缺省安全设置进行配置（快速路径）』所述的缺省安全设置首次使用时，会自动创建包含证书的信任库。但是，在某些情况下，可能需要手动创建信任库并按本主题所述配置 Data Protection for VMware vSphere GUI。

以下过程使用 Java™ 密钥和证书管理工具 **keytool**。

在 Linux 操作系统上，工具位于 /opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/ 目录中。

在 Microsoft Windows 操作系统上，该工具位于 C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre\bin 目录中。

在运行 **keytool** 命令时，您可能需要指定完整路径。

过程

1. 从命令行，将目录切换到信任库位置：

- 在 Linux 上：/opt/tivoli/tsm/tdpvmware/common/scripts/
- 在 Windows 上：C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\

2. 使用以下命令创建信任库并导入证书：

```
keytool -importcert -alias my-cert -file cert.pem -keystore  
tsm-ve-truststore.jks -storepass password
```

其中：

-alias my-cert
用于在信任库中标识证书的唯一别名。

-file cert.pem
文件包含服务器自签名证书或 CA 根证书。

-storepass password
密钥库密码。 确保记住此密码以供将来使用。

3. 启动 Data Protection for VMware vSphere GUI 并转至“配置”窗口。

- 如果您正在创建初始配置，单击任务 > 运行 IBM Spectrum Protect 配置向导，然后转至“服务器凭证”页面。
 - 如果您正在修改现有配置，单击任务 > 编辑 IBM Spectrum Protect 配置，然后转至“服务器凭证”页面。
4. 在 **IBM Spectrum Protect** 管理端口字段中输入端口号。这是允许使用 SSL 或 TLS 建立管理连接的服务器端口。
 5. 选择在管理端口上使用加密通信。
 6. 如果想要将此设置用于未来的 GUI 会话，请选择保存管理员标识、密码和端口设置。
 7. 单击**确定**以应用更改。

使用认证中心的证书

要使用由认证中心 (CA) 签署的证书，必须完成多个步骤。

关于此任务

以下过程使用名为 **keytool** 的标准密钥和界面管理工具。

在 Linux 操作系统上，其位于 /opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/ 目录中。

在 Microsoft Windows 操作系统上，其位于 C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre 目录中。

在从命令行运行 **keytool** 时，您可能需要指定完整路径。

过程

1. 获取密钥库访问权。
2. 创建证书签名请求 (CSR)。
3. 向认证中心发送证书签名请求以进行签名。
4. 在 Data Protection for VMware vSphere GUI 中接收签名的证书。

获取密钥库访问权：

证书存储在 Java 密钥库中。使用密码保护密钥库内容。要处理密钥库中的证书，您必须获取密钥库访问权。

关于此任务

在安装期间将自动生成缺省自签名证书和密钥库密码，因此您可能不知道初始密码。

完成以下步骤以将原始密钥库替换为新密钥库和新的自签名证书。将使用您选择的密码保护新密钥库。

如果您已知道密钥库密码，请跳过此过程。

过程

1. 停止 Data Protection for VMware vSphere GUI 服务。
2. 从命令行，将目录切换到密钥库位置。

- 在 Linux 上: /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/
- 在 Windows 上: C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\

3. 通过重命名密钥库文件 (key.jks) 或将其移至其他位置, 生成此文件的备份副本。
4. 通过发出以下命令创建新密钥库和新的自签名证书:

```
keytool -genkeypair -alias vekey -dname
CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
-sigalg SHA256withRSA -keysize 2048 -validity days -keystore
key.jks -storepass password -keypass password
```

其中:

-dname CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM

fqdn 是安装 Data Protection for VMware vSphere GUI 的计算机的 DNS 名称或标准域名。

-validity days

证书有效期。

-storepass password

密钥库密码。 确保记住此密码以供将来使用。

-keypass password

证书的专用密钥密码。 此密码必须匹配密钥库密码。

5. 使用 **securityUtility** 工具编码密钥库密码。 发出以下命令。

- 在 Linux 上: /opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode
- 在 Windows 上: C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode

在提示时输入密钥库密码, 然后保存输出 (例如, 将其复制到剪贴板)。

6. 在编辑器中打开 bootstrap.properties 文件, 并将 veProfile.keystore.pswd 属性设置为先前步骤中编码的值。 bootstrap.properties 文件位于以下位置:

- 在 Linux 上: /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/
- 在 Windows 上: C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\

7. 启动 Data Protection for VMware vSphere GUI 服务。

相关参考:

第 79 页的『启动和运行 Data Protection for VMware 的服务』

创建证书签名请求：

在获取密钥库访问后，必须创建证书签名请求 (CSR)。

过程

完成以下步骤以创建 CSR：

1. 从命令行，将目录切换到密钥库位置。

- 在 Linux 上： /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/
- 在 Windows 上： C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\

2. 发出以下命令创建新证书：

```
keytool -genkeypair -alias mykey -dname  
CN=fqdn,OU=unit,O=organization -keyalg RSA -sigalg SHA256withRSA  
-keysize 2048 -validity days -keystore key.jks -storepass  
password -keypass password
```

其中：

-alias mykey

mykey 是标识密钥库中的证书的唯一别名。在收到签名证书时将进行重命名。

-dname CN=fqdn,OU=unit,O=organization

fqdn 是安装 Data Protection for VMware vSphere GUI 的计算机的 DNS 名称或标准域名。

Unit 和 *organization* 是用户策略或认证中心需要的组织信息。

-validity days

证书有效期。

-storepass password

密钥库密码。如果您不知道或者忘记密钥库密码，请参阅第 59 页的『获取密钥库访问权』。

-keypass password

证书的专用密钥密码。此密码必须匹配密钥库密码。

3. 发出以下命令创建 CSR：

```
keytool -certreq -alias mykey -file certreq.pem -keystore key.jks
```

其中：

-alias mykey

来自先前步骤的证书别名。

-file certreq.pem

用于存储证书签名请求的文件。

将证书签名请求发送到认证中心：

在创建证书请求 (certreq.pem) 后，您必须将其发送到认证中心以进行签名。请遵循认证中心的特定指示信息。

接收签名证书：

在从认证中心 (CA) 获取签名证书后，必须在密钥库中接收证书。

过程

要接收签名证书，请完成以下步骤：

1. 从命令行，将目录切换到密钥库位置。
 - 在 Linux 上：/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/
 - 在 Windows 上：C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\
2. 将从 CA 收到的文件复制到此位置。这些文件包含 Data Protection for VMware vSphere GUI 的 CA 根证书、中间 CA 证书（如果有）和签名证书。
3. 停止 Data Protection for VMware vSphere GUI 服务。
4. 通过将密钥库文件 (key.jks) 复制到其他名称或位置，生成此文件的备份副本。
5. 使用以下命令导入中间 CA 证书（如果有）。在提示信任证书时，回答 *yes*。根据需要，针对多个中间 CA 重复此步骤。

```
keytool -importcert -alias ca-intermediate -file intermediate.pem  
-keystore key.jks -storepass password
```

其中：

-alias *ca-intermediate*

用于在密钥库中标识证书的唯一别名。每个中间证书必须具有一个唯一别名。

-file *intermediate.pem*

从 CA 获取的中间证书文件。

-storepass *password*

密钥库密码。

6. 通过发出以下命令，导入 CA 根证书。在提示信任此证书时，回答 *yes*。

```
keytool -importcert -alias ca-root -file root.pem -keystore  
key.jks -storepass password
```

其中：

-alias *ca-root*

用于在密钥库中标识证书的唯一别名。

-file *root.pem*

从 CA 获取的根证书文件。

-storepass *password*

密钥库密码。

7. 通过发出以下命令，导入签名证书：


```
keytool -importcert -alias mykey -file signedcert.pem -keystore  
key.jks -storepass password
```

其中：

-alias mykey

签名证书的别名。 此别名必须与生成证书签名请求 (CSR) 时使用的名称相同。

-file signedcert.pem

从 CA 收到的签名证书文件。

-storepass password

密钥库密码。

8. 删除包含 vekey 别名的现有证书：

```
keytool -delete -alias vekey -keystore key.jks -storepass password
```

其中，-storepass password 是密钥库的密码。

9. 将签名证书重命名为 vekey：

```
keytool -changealias -alias mykey -destalias vekey -keystore  
key.jks -storepass password
```

其中：

-alias mykey

签名证书的别名。

-storepass password

密钥库密码。

10. 启动 Data Protection for VMware vSphere GUI 服务。

相关参考：

第 79 页的『启动和运行 Data Protection for VMware 的服务』

VMware vCenter Server 用户特权需求

运行 Data Protection for VMware 操作需要某些 VMware vCenter Server 特权。

使用 Data Protection for VMware vSphere GUI 的 Web 浏览器视图来保护 VMware 数据中心时所需的 vCenter Server 特权

用于登录到 Data Protection for VMware vSphere GUI 的浏览器视图的 vCenter Server 用户标识

必须具有足够的 VMware 特权才能查看此 GUI 所管理的数据中心的内容。

例如，VMware vSphere 环境包含五个数据中心。 用户"jenn"仅对其中的两个数据中心具有足够的特权。 因此，在这些视图中，"jenn"只能看到其具备足够特权的上述两个数据中心。 另外三个数据中心（用户"jenn"对其不具有特权）对"jenn"不可见。

VMware vCenter Server 将一组特权集合起来定义为角色。 角色应用于特定用户或组的对象，用于创建特权。 在 VMware vSphere Web Client 中，必须创建带有一组特权的角色。 要为备份和复原操作创建 vCenter Server 角色，请使用 VMware vSphere Client 添加角色功能。

如果要使特权传播到 vCenter 内的所有数据中心，请指定 vCenter Server，然后选中传播至子代复选框。否则，如果将角色指定给所需数据中心，那么只有在传播至子代复选框选中的情况下，才能限制许可权。浏览器 GUI 的强制实施处于数据中心级别。

以下示例显示如何控制两个 VMware 用户组对数据中心的访问。首先，创建一个包含技术说明 7047438 中定义的所有权限的角色。此示例中的特权级别是由名称为 "TDPVMwareManage" 的角色来标识。组 1 要求访问数据中心 Primary1_DC 和 Primary2_DC 的管理虚拟机。组 2 要求访问数据中心 Secondary1_DC 和 Secondary2_DC 的管理虚拟机。

对于组 1，请为数据中心 Primary1_DC 和 Primary2_DC 分配 "TDPVMwareManage" 角色。对于组 2，请为数据中心 Secondary1_DC 和 Secondary2_DC 分配 "TDPVMwareManage" 角色。

每个 VMware 用户组中的用户可以使用 Data Protection for VMware GUI 仅在其各自数据中心中管理虚拟机。

提示：在创建角色时，请考虑向角色中添加您之后针对对象完成其他任务所需要的额外特权。

使用数据移动设备所需要的 vCenter Server 特权

安装在 vStorage 备份服务器（数据移动设备节点）上的 IBM Spectrum Protect 数据移动设备需要 VMCUser 和 VMCPw 选项。VMCUser 选项指定要备份、复原或查询的 vCenter 或 ESX 服务器的用户标识。分配给用户标识 (VMCUser) 的必需特权确保客户机可以在虚拟机和 VMware 环境中运行。此用户标识必须具有上述技术说明中所述的 VMware 权限。

要创建用于备份和复原操作的 vCenter Server 角色，请使用 VMware vSphere Client 的添加角色功能。在添加此用户标识 (VMCUser) 的特权时，必须选择传播至子代选项。此外，请考虑为此角色添加其他特权，以用于备份和复原之外的其他任务。对于 VMCUser 选项，强制实施处于顶级对象。

使用 Data Protection for VMware vSphere GUI 的 IBM Spectrum Protect vSphere Client 插件视图来保护 VMware 数据中心时所需的 vCenter Server 特权

IBM Spectrum Protect vSphere Client 插件需要一组特权，这组特权不同于登录到 GUI 所需的特权。

在安装期间，将为 IBM Spectrum Protect vSphere Client 插件创建以下定制特权：

- 数据中心 > IBM Data Protection
- 全局 > 配置 IBM Data Protection

将注册 IBM Spectrum Protect vSphere Client 插件所需的定制特权，以作为单独扩展。特权扩展关键字是 `com.ibm.tsm.tdpvmware.IBMDDataProtection.privileges`。

这些特权允许 VMware 管理员启用和禁用对 IBM Spectrum Protect vSphere Client 插件内容的访问权。只有对必需 VMware 对象具备这些定制特权的用户才能访问

IBM Spectrum Protect vSphere Client 插件 内容。 一个 IBM Spectrum Protect vSphere Client 插件 向每个 vCenter Server 注册并且由配置为支持 vCenter Server 的所有 GUI 主机共享。

从 VMware vSphere Web 客户机中, 您必须使用 IBM Spectrum Protect vSphere Client 插件为能够完成虚拟机数据保护功能的用户创建一个角色。 对于此角色, 除了 Web 客户机所需要的标准虚拟机管理员角色特权外, 还必须指定**数据中心 > IBM Data Protection** 特权。 对于每个数据中心, 请您希望授予其管理虚拟机权限的每个用户或用户组分配此角色。

vCenter 级别的用户需要**全局 > IBM Data Protection** 特权。 此特权允许用户管理、编辑或删除 vCenter Server 与 Data Protection for VMware vSphere GUI Web 服务器之间的连接。 请将此特权分配给熟悉 Data Protection for VMware vSphere GUI (用于保护其各自 vCenter Server) 的管理员。 可以在此扩展的"连接"页面中管理 IBM Spectrum Protect vSphere Client 插件连接。

以下示例显示了如何针对两个用户组来控制对数据中心的访问。 组 1 需要访问权才能管理数据中心 NewYork_DC 和 Boston_DC 的虚拟机。 组 2 需要访问权才能管理数据中心 LosAngeles_DC 和 SanFrancisco_DC 的虚拟机。

例如, 从 VMware vSphere 客户机中, 创建"IBMDDataProtectManage"角色, 分配标准虚拟机管理员角色特权以及**数据中心 > IBM Data Protection** 特权。

对于组 1, 请为数据中心 NewYork_DC 和 Boston_DC 分配"IBMDDataProtectManage"角色。 对于组 2, 请为数据中心 LosAngeles_DC 和 SanFrancisco_DC 分配"IBMDDataProtectManage"角色。

每个组中的用户可以在 vSphere Web 客户机中使用 IBM Spectrum Protect vSphere Client 插件 以仅在其各自数据中心中管理虚拟机。

与许可权不足相关的问题

当 Web 浏览器用户没有任何数据中心的足够许可权时, 会阻止对视图的访问。 而系统会发出错误消息 GVM2013E, 以告知用户由于许可权不足而无权访问任何受管数据中心。 还提供了其他新消息, 用于向用户告知因许可权不足而引发的问题。 要解决任何与许可权相关的问题, 请确保如上述各节中所述设置用户角色。 用户角色必须具有"必需特权 vCenter Server 用户标识和数据移动设备"表中标识的所有特权, 并且这些特权必须通过传播至子代复选框在数据中心级别应用。

当 IBM Spectrum Protect vSphere Client 插件用户没有某个数据库中心的足够许可权时, 该数据中心及其内容的数据保护功能将变得在此扩展中不可用。

当 IBM Spectrum Protect 用户标识 (由 VMCUser 选项指定) 包含的许可权不足以执行备份和复原操作时, 将显示以下消息:

```
ANS9365E VMware vStorage API 错误。  
"执行此操作的许可权遭到拒绝。"
```

当 IBM Spectrum Protect 用户标识包含的许可权不足以查看机器时, 将显示以下消息:

```
备份 VM 命令已启动。 要处理的虚拟机总数: 1  
ANS4155E VMware 服务器上找不到虚拟机"tango"。  
ANS4148E 虚拟机"foxtrot"的完全 VM 备份失败, RC 4390
```

有关权限使用的进一步信息，请参阅 **Data Protection for VMware vSphere GUI** 和数据移动设备所需的 **vCenter Server** 权限上的注释。

要通过 VMware Virtual Center Server 检索日志信息以了解许可权问题，请完成以下步骤：

1. 在"vCenter Server 设置"中，选择日志记录选项，然后将 **vCenter** 日志记录设置为细微（细微）。
2. 重新生成该许可权错误。
3. 将 **vCenter** 日志记录重置为其先前值可防止记录过多的日志信息。
4. 在"系统日志"中，查找最新的 vCenter Server 日志 (vpxd-wxyz.log) 并搜索字符串 NoPermission。例如：

```
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
Throw: vim.fault.NoPermission
```

此日志消息表明用户标识不包含创建快照的足够权限 (createSnapshot)。

Data Protection for VMware vSphere GUI 用户角色

Data Protection for VMware vSphere GUI 功能的可用性基于为 IBM Spectrum Protect 管理员标识分配的权限级别。

管理员标识必须与节点名匹配。在先前的产品发行版中，**REGISTER NODE** 命令会自动创建管理用户标识，此用户标识的名称与节点名匹配。从 IBM Spectrum Protect V8.1 开始，**REGISTER NODE** 命令不会自动创建与节点名匹配的管理用户标识。

注册新节点时，IBM Spectrum Protect 服务器管理员必须在 **REGISTER NODE** 服务器命令中指定 `userid` 参数：

```
REGISTER NODE node_name password userid=user_id
```

其中节点名与管理用户标识必须相同。例如：

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

缺省情况下，节点具有客户机所有者权限。

可通过 Data Protection for VMware vSphere GUI 运行的任务基于分配给该管理员标识的特权级别。

如果管理员标识没有不受限的策略域特权，那么您无法在 IBM Spectrum Protect 服务器上注册新的节点或设置其代理关系。如果未输入管理员标识，那么将创建宏脚本，以便能够在 IBM Spectrum Protect 服务器上运行。

配置 Data Protection for VMware vSphere GUI 时，会请求 IBM Spectrum Protect 管理员标识。此表根据分配给该标识的特权级别列出可用的功能：

- 值"是"表示用户角色可用的功能。
- 值"否"表示用户角色不可用的功能。

要查看您当前的 Data Protection for VMware vSphere GUI 角色，请将鼠标悬停在导航栏中您的用户标识上。

表 11. 基于 IBM Spectrum Protect 管理员标识特权需求的可用功能

	操作员	有报告特权的操作员	受限制管理员	管理员
摘要	运行立即备份与复原	操作员加报告	操作员加报告以及所列策略域的调度操作	所有角色，包括初始配置
IBM Spectrum Protect 管理员标识特权级别	无	以下某个特权级别： <ul style="list-style-type: none"> • 存储 • 操作员 • 分析人员 	策略（受限）或以下某个特权级别： <ul style="list-style-type: none"> • 存储 • 操作员 • 分析人员 	策略（不受限）或系统

"备份"选项卡

管理立即运行备份任务	是	是	是	是
管理已调度备份任务	否 ¹	否 ¹	是（在策略域内）	是
查看立即运行备份任务	是	是	是	是
查看已调度备份任务	否	是	是	是
删除已调度备份任务	否	否	是（在策略域内）	是

"复原"选项卡

运行复原任务	是	是	是	是
--------	---	---	---	---

"报告"选项卡

事件	否	是	是	是
最近任务	是	是	是	是
备份状态	否	是	是	是
应用程序保护	否	是	是	是
数据中心占用量	否	是	是	是

"配置"选项卡

节点注册 （"配置状态"-> 运行配置向导）	否	否	否 ²	是
更改 IBM Spectrum Protect 管理员标识凭证 （"配置状态"-> 编辑配置）	是	是	是	是

表 11. 基于 IBM Spectrum Protect 管理员标识特权需求的可用功能 (续)

	操作员	有报告特权的操 作员	受限制管理员	管理员
更改 VMCLI 节 点密码 (“配置状态”-> 编辑配置)	否	否	是	是
更改 GUI 域 (“配置状态”-> 编辑配置)	是 ³	是 ³	是 ³	是
更改数据移动设 备节点 (“配置状态”-> 编辑配置)	否	否	否 ²	是
更改装配代理节 点 (“配置状态”-> 编辑配置)	否	否	否 ²	是

1. 您不能注册节点，因为需要无限制的域策略。
2. 可以添加或除去 VMware 数据中心以及注册数据中心节点。

要查看 IBM Spectrum Protect 管理员标识权限级别和对应的 Data Protection for VMware vSphere GUI 角色：

1. 转到“配置”窗口。
2. 单击编辑配置。
3. “Spectrum Protect 服务器凭证”页面上将显示相关信息。

要点：

- 如果 IBM Spectrum Protect 管理员标识权限级别在 IBM Spectrum Protect 服务器上发生更改，那么必须重新启动 Data Protection for VMware vSphere GUI 以反映此更改。
- 更改“用户角色”时，必须单击**确定**保存更改，然后再转至其他“配置设置”页面或尝试其他配置更改。否则，“用户角色”更改不会生效。

Data Protection for VMware GUI 注册密钥

根据您在安装期间选择的选项，可以使用不同的方法访问 Data Protection for VMware GUI。将会为 Data Protection for VMware GUI 创建注册密钥。

短语“Data Protection for VMware GUI”适用于以下 GUI：

- Web 浏览器中访问的 Data Protection for VMware vSphere GUI
- vSphere Web Client GUI 中的 IBM Spectrum Protect vSphere Client 插件

IBM Spectrum Protect vSphere Client 插件注册密钥是 com.ibm.tsm.tdpmware.IBMDDataProtection。当您在安装期间选中**注册 vSphere Web Client 扩展**复选框时，会注册此密钥。将为每个 vCenter Serve 注册一个 IBM Spectrum Protect vSphere Client 插件实例。

对于 Web 浏览器中访问的 Data Protection for VMware vSphere GUI，不创建注册密钥。

要查看注册密钥，请登录到 VMware Managed Object Browser (MOB)。登录到 MOB 后，转至内容 → 扩展管理器以查看注册密钥。

配置 恢复代理程序 GUI

提供了关于如何设置 恢复代理程序 GUI 以进行装配、文件复原或即时复原操作的指示信息。

开始之前

在 恢复代理程序 GUI 中尝试某项操作前，必须先完成这些配置任务。

要点：随 恢复代理程序 GUI 一起安装的联机帮助中提供了有关如何使用该 GUI 完成任务的信息。在任何 GUI 窗口中单击**帮助**可打开联机帮助以获取任务帮助。

过程

1. 登录到要在其中复原文件的系统。 必须在系统上安装 恢复代理程序。
2. 在 恢复代理程序 GUI 中单击**选择 TSM Server**以连接到 IBM Spectrum Protect 服务器。 如果 恢复代理程序与 Data Protection for VMware vSphere GUI 安装在同一系统中，并且已使用 Data Protection for VMware vSphere GUI 配置向导成功地配置了应用程序，那么存在以下情况：
 - 数据移动设备节点和 IBM Spectrum Protect 服务器填充在 恢复代理程序"TSM 服务器"字段中。
 - 以下字段填充在"TSM 服务器信息"面板中：
 - 认证节点包含可用数据移动设备节点的列表。
 - 目标节点包含对所选数据移动设备节点可用的数据中心节点的列表。

如果用配置向导在本地仅指定了一个数据移动设备节点，那么 恢复代理程序会在启动时使用该节点进行认证。恢复代理程序会记住与 IBM Spectrum Protect 服务器连接的最后一个节点的名称。如果为此节点（连接的最后一个节点的名称）选择了**使用密码访问权生成**，那么 恢复代理程序在启动时会使用这些凭证来连接到 IBM Spectrum Protect 服务器。如果先前从未连接到 IBM Spectrum Protect 服务器，那么只会通过向导配置一个数据移动设备节点和一个数据中心节点，恢复代理程序在启动时会使用这些凭证连接到 IBM Spectrum Protect 服务器。

指定下列选项：

服务器地址

输入 IBM Spectrum Protect 的 IP 地址或主机名。

服务器端口

输入用于与服务器进行 TCP/IP 通信的端口号。 缺省端口号为 1500。

节点访问方法：

Asnodename

选择此选项以使用代理节点访问位于目标节点中的 VM 备份。 代理节点是授予"代理"权限以代表目标节点执行操作的节点。

IBM Spectrum Protect 管理员通常使用 `grant proxynode` 命令来创建两个现有节点之间的代理关系。

如果选择此选项，请完成以下步骤：

- a. 在目标节点字段中输入目标节点（VM 备份所在的节点）的名称。
- b. 在认证节点字段中输入代理节点的名称。
- c. 在密码字段中输入代理节点的密码。
- d. 单击**确定**以保存这些设置并退出 IBM Spectrum Protect 信息对话框。

使用此方法时，恢复代理程序用户只知道代理节点密码，而目标节点密码是受保护的。

Fromnode

选择此选项以使用只具有对目标节点中特定 VM 快照数据的访问权的节点。

通常使用 `set access` 命令从拥有 VM 备份的目标节点对此节点授予访问权：

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

例如，以下命令对名为 `myMountNode` 的节点授予权限来从名为 `myTestVM` 的 VM 复原文件：

```
set access backup -TYPE=VM myTestVM myMountNode
```

如果选择此选项，请完成以下步骤：

- a. 在目标节点字段中输入目标节点（VM 备份所在的节点）的名称。
- b. 在认证节点字段中输入已授予有限访问权的节点的名称。
- c. 在密码字段中输入已授予有限访问权的节点的密码。
- d. 单击**确定**以保存这些设置并退出 IBM Spectrum Protect 信息对话框。

使用此方法时，您可以看到已备份的 VM 的完整列表。但是，您只能复原已为该节点授予对其访问权的 VM 备份。此外，不保护快照数据在服务器上不到期。因此，在此方法中不支持即时复原。

直接 选择此选项以直接对目标节点（VM 备份所在的节点）进行认证。

如果选择此选项，请完成以下步骤：

- a. 在认证节点字段中输入目标节点（VM 备份所在的节点）的名称。
- b. 在密码字段中输入目标节点的密码。
- c. 单击**确定**以保存这些设置并退出 IBM Spectrum Protect 信息对话框。

使用密码访问权生成

如果选择了此选项而密码字段为空时，恢复代理程序将使用存储在注册表中的现有密码进行认证。如果未选择此选项，那么您必须手动输入密码。

要使用该选项，必须先手动设置应用该选项的节点的初始密码。首次与 IBM Spectrum Protect 节点连接时必须指定初始密码，方法是在**密码**字段中输入密码，然后选择使用**"密码访问生成"**复选框。

但是，将本地数据移动设备节点用作认证节点时，注册表中可能已存储了密码。因此，请选择使用**"密码访问生成"**复选框而不输入密码。

恢复代理程序会查询指定的服务器以获取受保护 VM 的列表，然后显示该列表。

3. 恢复设置以设置下列装配、备份和复原选项：

虚拟卷写高速缓存

在 Windows 备份代理主机上运行的恢复代理程序会保存在即时复原和装配期间创建的数据更改。这些更改将保存在写高速缓存中的虚拟卷上。缺省情况下，写高速缓存已启用并指定 C:\ProgramData\Tivoli\TSM\TDPVMware\mount\ 路径和最大高速缓存大小为选定文件夹可用空间的 90%。要防止系统卷被写满，请将写高速缓存改为非系统卷的卷上的路径。

临时文件的文件夹

指定保存数据更改的路径。写高速缓存必须位于本地驱动器上且不能设置为共享文件夹上的路径。如果写高速缓存被禁用或已满，那么尝试启动即时复原会话或安装会话将失败。

高速缓存大小

指定写高速缓存的大小。允许的最大高速缓存大小为选定文件夹可用空间大小的 90%。

限制：要防止复原处理中的任何中断，请在所有防病毒保护设置中排除写高速缓存路径。

数据访问

指定要访问的数据类型。如果正在使用脱机设备（例如磁带或虚拟磁带库），则必须指定适用的数据类型。

存储器类型

从下列存储设备中指定一个以从其装配快照：

磁盘/文件

快照是从磁盘或文件装配的。此设备是缺省的。

磁带 快照是从磁带存储池装配的。选择此选项后，就不可能装配多个快照或运行即时复原操作。

VTL 快照是从脱机虚拟磁带库装配的。支持在同一虚拟磁带库上同时装配会话。

注：当存储类型发生更改时，您必须重新启动服务以便更改生效。

禁用到期保护

在装配操作过程中，IBM Spectrum Protect 服务器上的快照处于锁定状态，以防止操作期间快照到期。因为会将其他快照添加到已装配的快照序列中，所以可能会发生到期情况。此选项指定了是否要在装配操作过程中禁用到期保护。

- 要防止快照到期，请勿选择此选项。IBM Spectrum Protect 服务器上的快照处于锁定状态，防止快照在装配操作期间到期。
- 要禁用到期保护，请选择此选项。缺省情况下，此选项处于已选择状态。IBM Spectrum Protect 服务器上的快照未处于锁定状态，不会防止快照在装配操作期间到期。因此，快照可能会在装配操作期间到期。到期可能会产生意外结果，并对装配点造成不利影响。例如，装配点可能无法使用，或者包含错误。但是，到期不会影响当前的活动副本。在操作过程中，活动副本不会到期。

如果快照位于目标复制服务器，那么无法锁定该快照，因为它处于只读模式。服务器尝试进行锁定会导致装配操作失败。为了避免锁定尝试并防止此类失败，请选择此选项来禁用到期保护。

向前读取大小（以 16 KB 块计）

指定在读请求发送到单个块后，从存储设备检索的额外数据块的数量。缺省值如下所示：

- 磁盘或文件：64
- 磁带：1024
- VTL：64

任何设备的最大值均为 1024。

向前读取高速缓存的大小（以块计）

指定储存额外数据块的高速缓存的大小。缺省值如下所示：

- 磁盘或文件：10000
- 磁带：75000
- VTL：10000

由于每个快照都有自己的高速缓存，请确保计划同时装配或复原的快照数量。累积高速缓存大小不能超过 75000 个块。

驱动程序超时（秒）

该值指定了在文件系统驱动程序中处理数据请求的时间。如果没有及时完成处理，那么将取消请求，并且错误将返回到文件系统驱动程序中。如果遇到超时，请考虑增大该值。例如，当网络速度慢、存储设备处于忙碌状态，或者正在处理多个装配或即时复原会话时，可能发生超时。缺省值如下所示：

- 磁盘或文件：60
- 磁带：180
- VTL：60

单击**确定**保存更改并退出设置。

4. 验证每个 IBM Spectrum Protect 服务器节点（使用 Asnodename 和 Fromnode 选项指定）是否允许删除备份。在操作过程中，恢复代理程序会创建未使用的临时对象。您可以使用 BACKDElete=Yes 服务器选项将这些对象移除，从而使这些对象不会在节点中累积。

- a. 登录 IBM Spectrum Protect 服务器并以命令行方式启动管理客户机会话：

```
dsmadm -id=admin -password=admin -dataonly=yes
```

- b. 输入以下命令：

```
Query Node <nodename> Format=Detailed
```

请确保每个节点的命令输出包含以下语句：

```
Backup Delete Allowed?: Yes
```

如果不包含此语句，那么请使用以下命令来更新每个节点：

```
UPDate Node <nodename> BACKDElete=Yes
```

对每个节点再次运行 Query Node 命令以验证每个节点是否允许删除备份。

5. 如果在 iSCSI 网络中使用恢复代理进程，并且“恢复代理进程”不使用数据移动设备，请转至 C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf 文件，并指定 [IMOUNT] 标记和 **Target IP** 参数：

```
[IMOUNT config]
Target IP=<IP address of the network card on the system
that exposes the iSCSI targets.>
```

例如：

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

添加或更改 Target IP 参数后，请重新启动恢复代理进程 GUI 或恢复代理进程 CLI。

启用从 恢复代理程序到 IBM Spectrum Protect 服务器的安全通信

如果将 IBM Spectrum Protect 服务器配置为使用安全套接字层 (SSL) 或传输层安全性 (TLS) 协议，那么启用 恢复代理程序 以通过使用协议与服务器进行通信。

开始之前

开始配置到服务器的安全通信之前，请考虑以下需求：

- 针对 SSL 启用的每台服务器都必须具有唯一的证书。证书可采用以下任一类型：
 - 由服务器自签名的证书。
 - 由第三方认证中心 (CA) 颁发的证书。CA 证书可来自诸如 Symantec 或 Thawte 等证书，或者也可以是贵公司内部维护的内部证书。
- 出于性能考虑，仅限将 SSL 或 TLS 用于需要确保安全性的会话。请考虑在服务器上添加其他处理器资源以应对增多的需求。
- 对于连接到使用 TLS V1.2 的服务器的客户机，证书签名算法必须是安全散列算法 1 (SHA-1) 或更高版本。如果使用自签名证书连接到使用 TSL V1.2 的服务器，那么必须使用 cert256.arm 证书。IBM Spectrum Protect 管理员可能需要在服务器上更改缺省证书。
- 要禁用安全性低于 TLS 1.2 的安全性协议，请将 **SSLDISABLELEGACYtls yes** 选项添加到 C:\windows\system32\fb.opt 或 C:\Windows\SysWOW64\fb.opt 文件中。TLS 1.2 或更高版本有助于防止恶意程序的攻击。

使用 IBM Spectrum Protect 服务器自签名证书启用安全通信

如果 IBM Spectrum Protect 服务器使用的是自签名证书，那么必须从服务器管理员处获取该证书的副本，并将 恢复代理程序配置为使用 SSL 或 TLS 协议与服务器进行通信。

关于此任务

每台服务器自行生成自己的证书。如果 V6.3 和更高版本的服务器使用 TLS 1.2 或更高版本，那么此服务器会生成名为 `cert256.arm` 的文件，如果此服务器使用更低版本的 SSL 或 TLS，那么会生成名为 `cert.arm` 的文件。低于 V6.3 的服务器版本会生成名为 `cert.arm` 的文件，与采用何种协议无关。必须选择在服务器上设置为缺省证书的证书。

证书文件存储在服务器工作站上的服务器实例目录中。例如，`C:\IBM\tivoli\tsm\server\bin\cert256.arm`。如果此证书文件不存在，那么使用设置的这些选项重新启动服务器时，会创建此证书文件。

过程

要使用自签名证书启用从恢复代理进程到服务器的 SSL 或 TLS 通信：

1. 将 GSKit 二进制路径和库路径附加到客户机上的 PATH 环境变量中。例如：

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;  
C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```

2. 如果是首次以客户机配置 SSL 或 TLS，必须创建客户机本地密钥数据库 `dsmcert.kdb`。从 `C:\Windows\SysWOW64` 目录中运行 `gsk8capicmd_64` 命令，如下示例中所示：

```
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
```

您提供的密码用于对密钥数据库进行加密。密码加密后自动存储在密码存储文件 (`dsmcert.sth`) 中。密码存储文件供客户机用于检索密钥数据库密码。

3. 获取服务器自签名证书。
4. 将此证书导入 `dsmcert.kdb` 数据库。必须将每台客户机的证书都导入 `dsmcert.kdb`。从 `C:\Windows\SysWOW64` 目录中运行 `gsk8capicmd_64` 命令，如下示例中所示：

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server server_name self-signed key"  
-file path_to_certificate -format ascii -trust enable
```

可将多个服务器证书添加到 `dsmcert.kdb` 数据库中，以便客户机能够连接到不同服务器。不同证书必须具有不同标签。请为标签使用有意义的名称。

要点： 对于服务器的灾难恢复，如果证书已丢失，那么服务器将自动生成一个新证书。然后，每台客户机都必须导入新证书。

5. 将服务器证书添加到 `dsmcert.kdb` 数据库后，请将 `ssl yes` 选项添加到 `C:\Windows\SysWOW64\fb.opt` 文件中，并更新 `tcpport` 选项的值。

要点：

通常，将在不同于非 SSL 和非 TLS 连接的端口上设置用于 SSL 和 TLS 连接的服务器。请勿为 `tcpport` 值指定非 SSL 或 TLS 端口号。如果 `tcpport` 的值不正确，那么恢复代理进程将无法连接到服务器。

无法通过针对 SSL 或 TLS 启用的恢复代理进程连接到非 SSL 或非 TLS 端口，也无法将 SSL 或 TLS 端口连接到未针对 SSL 或 TLS 启用的恢复代理进程。

- 请在以下恢复代理进程配置文件中设置正确的 SSL 或 TLS 端口。

- C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf
- C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf

使用第三方证书启用安全通信

如果 IBM Spectrum Protect 服务器使用第三方认证中心 (CA)，那么必须获取 CA 根证书。

关于此任务

如果此证书是由诸如 Symantec 或 Thawte 之类的 CA 发放的，那么此证书已准备就绪，可使用 SSL 或 TLS，并且您可跳过以下配置步骤。要获取预安装的 CA 根证书列表，请在 IBM Knowledge Center 上搜索**认证中心根证书**。

如果此证书并非是由预安装的根证书发放的或者属于贵公司内部维护的内部 CA 证书，那么必须将恢复代理程序配置为使用 SSL 或 TLS 协议来与服务器进行通信。

过程

要使用 CA 证书启用从恢复代理进程到服务器的 SSL 或 TLS 通信：

1. 将 GSKit 二进制路径和库路径附加到 PATH 环境变量中。例如：

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;  
C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```

2. 如果是首次为客户机上配置 SSL 或 TLS，必须创建客户机本地密钥数据库 dsmcert.kdb。对于客户机，请从 C:\Windows\SysWOW64 目录中运行 **gsk8capicmd_64** 命令，如以下示例中所示：

```
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
```

您提供的密码用于对密钥数据库进行加密。密码加密后自动存储在密码存储文件 (dsmcert.sth) 中。密码存储文件供客户机用于检索密钥数据库密码。

3. 获取 CA 证书。

4. 将此证书导入 dsmcert.kdb 数据库。必须将每台客户机的证书都导入 dsmcert.kdb。对于客户机，请从 C:\Windows\SysWOW64 目录中运行 **gsk8capicmd_64** 命令，如以下示例中所示：

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"  
-file path_to_CA_root_certificate -format ascii -trust enable
```

可将多个服务器证书添加到 dsmcert.kdb 数据库中，以便客户机能够连接到不同服务器。不同证书必须具有不同标签。请为标签使用有意义的名称。

要点： 对于服务器的灾难恢复，如果证书已丢失，那么服务器将自动生成一个新证书。每台客户机都必须导入新证书。

5. 将服务器证书添加到 dsmcert.kdb 数据库后，请将 **ssl yes** 选项添加到 C:\Windows\SysWOW64\fb.opt 文件中，并更新 **tcpport** 选项的值。

要点：

通常，将在不同于非 SSL 和非 TLS 连接的端口上设置用于 SSL 和 TLS 连接的服务器。请勿为 tcpport 值指定非 SSL 或 TLS 端口号。如果 tcpport 的值不正确，那么恢复代理进程将无法连接到服务器。

无法通过针对 SSL 或 TLS 启用的恢复代理进程连接到非 SSL 或非 TLS 端口，也无法将 SSL 或 TLS 端口连接到未针对 SSL 或 TLS 启用的恢复代理进程。

6. 请在以下恢复代理进程配置文件中设置正确的 SSL 或 TLS 端口。
 - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf
 - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf

语言环境设置

语言环境设置确定用于界面、消息和联机帮助的语言。

Data Protection for VMware GUI

短语"Data Protection for VMware GUI"适用于以下 GUI：

- 在 Web 浏览器中访问的 Data Protection for VMware vSphere GUI
- vSphere Web 客户机 GUI 中的 IBM Spectrum Protect vSphere Client 插件

如果运行 Data Protection for VMware GUI、VMware vSphere Client 和 IBM Spectrum Protect 服务器的处理器之间的语言环境设置不一致，那么 Data Protection for VMware GUI 不支持在包含不一致语言环境设置的环境中运行。

在运行 Data Protection for VMware GUI、VMware vSphere Client 和 IBM Spectrum Protect 服务器的系统之间指定相同的语言环境设置。

当通过"了解更多信息"链接首次访问 Data Protection for VMware GUI 帮助页面时，帮助将以运行 Data Protection for VMware GUI 的系统语言环境设置所指定的语言显示。首次访问帮助时，帮助不会以 VMware vSphere Client 的语言环境所指定的语言显示。在此情况下，Data Protection for VMware GUI 帮助页面显示之后，单击帮助中的至少两个链接，然后关闭帮助。下次通过"了解更多信息"链接启动帮助时，帮助将以 VMware vSphere Client 的语言环境设置所指定的语言显示。

IBM Spectrum Protect 文件复原界面

界面内容和消息提示语言由访问 IBM Spectrum Protect 文件复原界面的 Web 浏览器的语言设置确定。

对于记录到 fr_api.log 文件中的错误消息，IBM Spectrum Protect 文件复原界面将使用运行 Data Protection for VMware vSphere GUI 的系统语言环境设置所指定的语言。

日志文件活动

Data Protection for VMware 在安装、备份、装配和复原操作期间创建和修改若干日志文件。

Data Protection for VMware 日志文件是使用 .sf 文件扩展名的纯文本文件。

Windows

日志位于以下目录中：

%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware

这些目录针对每个 Data Protection for VMware 组件包含一个子目录。例如，恢复代理程序子目录为 \mount，而恢复代理程序命令行界面子目录为 \shell。

可以从 **Windows** > 开始菜单搜索日志文件，方法是选择控制面板 > 搜索并输入 *.log。

Linux

日志位于以下两个路径中：

<user.home>/tivoli/tsm/ve/mount/log

/opt/tivoli/tsm/TDPVMware/mount/engine/var

可以通过输入以下命令来搜索日志文件：

```
find /opt/tivoli/ -name "*.log"
```

要点：每次启动安装时，就会覆盖现有的日志文件。如果您遇到安装问题并且必须重新安装产品，请在再次尝试安装之前，从 %allusersprofile% 目录检索现有 TDPVMwareInstallation.log 文件。

注：当 Data Protection for VMware 服务正在运行时，若干日志文件将保持打开状态。因此，某些文件管理器不显示这些文件的当前状态，所以可能会报告文件大小为零。选择或打开一个此类文件会强制文件管理器更新该文件的详细信息。

恢复代理程序日志文件

恢复代理程序日志文件为 TDP_FOR_VMWARE_MOUNTnnn.sf。包含最新数据的日志文件存储在编号为 040 的日志文件 (TDP_FOR_VMWARE_MOUNT040.sf) 中。当日志文件达到最大大小限制时，会创建新日志文件。日志文件名相同，但日志文件编号减 1。具体而言，编号为 040 的日志文件中的数据会复制到编号为 039 的日志文件中。编号为 040 的日志文件包含最新的日志文件数据。当 040 再次达到最大文件大小时，039 文件内容会移至 038，同时 040 的信息会再次移至 039。

Data Protection for VMware GUI 日志文件

Data Protection for VMware vSphere GUI 将日志文件放置在以下目录中：

Windows

C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs

Linux

/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

收集日志文件时，请确保所有子目录都包含在压缩文件中。

Data Protection for VMware 命令行界面日志文件

Data Protection for VMware 命令行界面将日志文件放置在以下目录中：

Windows

C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\logs

Linux /opt/tivoli/tsm/tdpvmware/common/logs
收集日志文件时，请确保所有子目录都包含在压缩文件中。

IBM Spectrum Protect 文件复原界面日志文件

IBM Spectrum Protect 文件复原界面将错误消息记录在 fr_api.log、fr_gui.log 和 messages.log 文件中。这些文件位于以下缺省目录中：

Windows C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs

Linux /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

通过设置文件复原日志活动文件 (FRLog.config) 中的 API_LOG_FILE_NAME 和 API_LOG_FILE_LOCATION 选项，可以更改 fr_api.log 文件的名称和位置。

IBM Spectrum Protect 服务器也会记录文件复原操作。可以使用服务器管理命令行客户机来搜索这些消息。

- 要以命令行方式启动管理客户机会话，请在工作站上输入以下命令：

```
dsmadm -id=admin -password=admin -dataonly=yes
```

输入带有 **-ID** 和 **-PASSWORD** 选项的 **DSMADM** 命令（如上所示），就不会提示您输入用户标识和密码。

- 要搜索 SQL 摘要扩展表以查看有关文件复原操作的结果，请从管理命令行客户机发出 **select** 命令：

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
```

可以通过在 select 语句中包含一个或多个以下条件来缩小搜索范围：

```
- * ENTITY='DATA_MOVER_NODE_NAME'  
- * AS_ENTITY='DATA_CENTER_NODE_NAME'  
- * SUB_ENTITY='VM_HOST_NAME'  
- * START_TIME='yyyy-MM-dd HH:mm:ss'
```

例如：

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'  
and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'  
and START_TIME>'2017-03-11 17:30:00'
```

START_TIME 条件支持使用以下符号进行查询：等号 (=)、小于号 (<) 或大于号 (>)。

- 要搜索 SQL 活动日志表以查看有关文件复原操作的事件，请从管理命令行客户机发出 **select** 命令：

```
select * from ACTLOG
```

可以通过在 select 语句中包含一个或多个以下条件来缩小搜索范围：

```
- * NODENAME='DATA_CENTER_NODE_NAME'  
- * DATE_TIME='yyyy-MM-dd HH:mm:ss'
```

例如：

```
select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
```

使用大写字符指定 DATA_MOVER_NODE_NAME 和 DATA_CENTER_NODE_NAME。

DATE_TIME 条件支持使用以下符号进行查询：等号 (=)、小于号 (<) 或大于号 (>)。

启动和运行 Data Protection for VMware 的服务

缺省情况下，启动 Windows 操作系统时，将在本地系统帐户下启动 恢复代理程序。

在 Microsoft Windows 上运行 恢复代理程序 服务

从 Windows"开始"菜单启动 恢复代理程序后，该服务将自动停止。从"开始"菜单启动的 恢复代理程序完成后，服务将自动启动。此外，对于这些操作系统，该服务不提供 GUI。要使用 GUI，请转至 Windows"开始"菜单，然后选择**所有程序 > IBM Spectrum Protect > Data Protection for VMware > 恢复代理程序**。

Data Protection for VMware 命令行界面

可以通过完成以下任务来验证 Data Protection for VMware 命令行界面是否正在运行：

Windows 转至**开始 > 控制面板 > 管理工具 > 服务**，并验证 Data Protection for VMware 命令行界面的状态是否为已启动。

Linux 转至脚本目录 (/opt/tivoli/tsm/tdpvmware/common/scripts/) 并发出此命令：

```
./vmclid status
```

- 如果守护程序未在运行，请发出以下命令以手动启动守护程序：

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

以下 init 脚本也可用于停止和启动守护程序：

```
./vmclid stop  
./vmclid start
```

附录 A. 高级配置任务

必须使用可用的应用程序界面来手动配置和验证每个组件。

开始之前

请确保满足以下条件，然后再继续执行此任务：

- IBM Spectrum Protect 服务器必须可用才能注册节点。
- Data Protection for VMware vSphere GUI 安装在满足操作系统先决条件的系统上。
它必须通过网络连接至以下系统：
 - vStorage 备份服务器
 - IBM Spectrum Protect 服务器
 - vCenter Server

过程

1. 登录到 IBM Spectrum Protect 服务器，并完成第 82 页的『在 vSphere 环境中设置 IBM Spectrum Protect 节点』中所述的任务。
2. 登录到 vStorage 备份服务器，并完成第 83 页的『使用 vSphere 插件 GUI 设置数据移动设备节点』中所述的任务。
3. 登录到安装有 Data Protection for VMware vSphere GUI 的系统，并完成第 88 页的『在 vSphere 环境中配置 Data Protection for VMware 命令行界面』中所述的任务。
4. 在安装有 Data Protection for VMware vSphere GUI 的系统上，启动 vSphere Client 并登录到 vCenter。如果 vSphere 客户机已在运行，那么必须停止并重新启动该客户机。
5. 转至 vSphere 客户机中的主目录。单击“解决方案和应用程序”面板中的 Data Protection for VMware vSphere GUI 图标。

提示：如果未显示该图标，那么 Data Protection for VMware vSphere GUI 未注册或者已发生连接错误。

- a. 在 vSphere 客户机菜单中，转至 **插件 > 管理插件** 以启动插件管理器。
- b. 如果能够找到 Data Protection for VMware vSphere GUI 并且发生连接错误，请发出 ping 命令，验证与安装有 Data Protection for VMware vSphere GUI 的机器的连接。

结果

Data Protection for VMware vSphere GUI 已为备份或复原操作做好了准备。

在 vSphere 环境中设置 IBM Spectrum Protect 节点

此过程描述在 vSphere 环境中如何向 IBM Spectrum Protect 服务器手动注册节点以及为这些节点授予代理权限。

开始之前

要点：

关于此任务

此过程中的所有步骤均在 IBM Spectrum Protect 服务器上完成。

提示：也可以使用 Data Protection for VMware vSphere GUI 配置向导或“编辑配置”笔记本来完成此任务。启动 Data Protection for VMware vSphere GUI，方法是打开 Web 浏览器并转至 GUI Web 服务器。例如：

<https://guihost.mycompany.com:9081/TsmVMwareUI/>

使用 vCenter 用户名和密码登录。

- 对于初始配置，请转至配置 > 运行配置向导。
- 对于现有配置，请转至配置 > 编辑配置。

过程

1. 登录 IBM Spectrum Protect 服务器并以命令行方式启动管理客户机会话：

```
dsmadm -id=admin -password=admin -dataonly=yes
```
2. 发出 REGister Node 命令以向 IBM Spectrum Protect 服务器注册以下节点：
 - a. 表示 VMware vCenter 的节点（vCenter 节点）：

```
REGister Node MY_VCNode <password for MY_VCNode>
```
 - b. 在 IBM Spectrum Protect 与 Data Protection for VMware vSphere GUI 之间通信的节点（VMCLI 节点）：

```
REGister Node MY_VMCLINode <password for MY_VMCLINode>
```
 - c. 表示数据中心并用于存储 VM 数据的节点（数据中心节点）：

```
REGister Node MY_DCNode <password for MY_DCNode>
```
 - d. 从一个系统“将数据移动”到另一个系统的节点（数据移动设备节点）：

```
REGister Node MY_DMNode <password for MY_DMNode>
```
3. 发出 GRant PROXynode 命令，为这些节点定义代理关系：

警告： 向 IBM Spectrum Protect 服务器注册节点时，请勿使用 userid 参数。

切记： 目标节点拥有数据，而代理进程节点代表目标节点执行操作。向目标节点授予代理权限后，代理进程节点可以为目标节点执行备份和复原操作。

- a. 通过发出以下命令，向 vCenter 节点授予代理权限：

```
GRant PROXynode TArget=MY_VCNode AGent=MY_DCNode,MY_VMCLINode
```

此命令将向 MY_DCNode 和 MY_VMCLINode 授予代表 MY_VCNode 备份和复原 VM 的权限。
- b. 通过发出以下命令，向数据中心节点授予代理权限：

```
GRant PROXynode TArget=MY_DCNode AGent=MY_VMCLINode,MY_DMNode
```

此命令将向 MY_VMCLINODE 和 MY_DMNODE 授予代表 MY_DCNODE 备份和复原 VM 的权限。

- c. (可选) 向环境中的任何其他数据中心节点或数据移动设备节点授予代理权限。
- d. 通过发出 IBM Spectrum Protect 服务器 Query PROXynode 命令, 验证代理关系。 预期的命令输出如下所示: 期望的命令输出为:

Target Node	Agent Node
MY_VCNODE	MY_DCNODE MY_VMCLINODE
MY_DCNODE	MY_VMCLINODE MY_DMNODE

下一步做什么

成功设置 IBM Spectrum Protect 节点后, 下一项手动配置任务是如『使用 vSphere 插件 GUI 设置数据移动设备节点』中所述设置数据移动设备节点。

使用 vSphere 插件 GUI 设置数据移动设备节点

如果在 vSphere 环境中将备份工作负载卸载到 vStorage 备份服务器, 可以使用"数据移动设备"向导设置一系列数据移动设备节点来运行操作, 并将数据移至 IBM Spectrum Protect 服务器。

开始之前

设置数据移动设备节点需要配置更改、启动必需服务以及验证设置。

可以使用插件 GUI 执行这些任务, 这样能够简化并加速创建一系列数据移动设备节点。另外, 可以手动执行工作, 有关更多信息, 请参阅 第 84 页的『在 vSphere 环境中手动设置数据移动设备节点』。

在标准 Data Protection for VMware 环境中, 将为每个数据移动设备节点使用单独的 dsm.opt 文件 (Windows) 或 dsm.sys 文件节 (Linux)。如果 vStorage 备份服务器上的多个数据移动设备节点都用于重复数据删除, 并且这些节点都有权移动同一数据中心节点的数据, 那么每个 dsm.opt 文件或 dsm.sys 文件节对于 dedupcachepath 选项必须包含不同的值。

物理数据移动设备节点通常使用 SAN 备份和复原数据。如果将数据移动设备节点配置为直接访问存储卷, 请关闭自动盘符分配。如果未关闭盘符分配, 那么数据移动设备节点上的客户机可能会破坏虚拟盘的原始数据映射 (RDM)。如果虚拟盘的 RDM 已损坏, 那么备份将失败。

限制: Data Protection for VMware 不支持将 vStorage 备份服务器 (用作数据移动设备) 调度为备份其自身。请确保将 vStorage 备份服务器排除在其自己的调度以外。对于包含 vStorage 备份服务器的 VM, 请使用其他 vStorage 备份服务器来执行该 VM 的备份。

如果需要执行上述任意调整, 请参阅"在 vSphere 环境中手动设置数据移动设备节点"主题。

关于此任务

使用 vSphere 插件配置数据移动设备节点。

过程

1. 从 vSphere 插件中，选择 IBM Spectrum Protect。
2. 在配置选项卡中，选择**数据移动设备**。
3. 在添加数据移动设备面板中，从下拉菜单选择数据中心。
4. 根据需要编辑以下字段：
 - **数据移动设备名称**：即已使用基于节点前缀的建议名称填写的节点名、数据中心节点名、数据移动设备名称以及增量编号。
 - **数据移动设备主机名**
 - **vCenter 用户**，使用注册插件的用户名填写。
 - **vCenter 密码**设置完成后，单击**添加**。
5. 结果屏幕将显示：
 - 配置的数据移动设备名称。
 - 选项文件位置。 可以通过编辑该文件来配置数据移动设备。
 - 日志文件位置。
 - 已使用的缺省选项。
6. 现在可以使用 **IBM Spectrum Protect > 配置数据移动设备**选项卡来测试数据移动设备。 也可以验证安装是否成功，具体方法是选中该数据移动设备，然后单击**验证**，或者在下次添加某个数据移动设备时检查状态。
7. 可以使用 **IBM Spectrum Protect > 调度**选项卡添加要调度的数据移动设备。

在 vSphere 环境中手动设置数据移动设备节点

如果在 vSphere 环境中将备份工作负载卸载到 vStorage 备份服务器，那么可以手动设置数据移动设备节点以运行操作并将数据移至 IBM Spectrum Protect 服务器。

开始之前

物理数据移动设备节点通常使用 SAN 备份和复原数据。 如果将数据移动设备节点配置为直接访问存储卷，请关闭自动分配盘符。 如果未关闭盘符分配，那么数据移动设备节点上的客户机可能会破坏虚拟盘的原始数据映射 (RDM)。 如果虚拟盘的 RDM 已损坏，那么备份将失败。

必需服务：如以下步骤所述，数据移动设备需要客户机接收器服务、远程客户机代理程序服务和数据移动设备调度程序服务。 如果从数据中心移除了数据移动设备，请卸载并删除数据移动设备的这些服务。

要点：如果数据移动设备与 Data Protection for VMware vSphere GUI 安装在相同的 Windows 系统上，并且在数据移动设备配置期间选中了**创建服务**，那么无需执行以下步骤。

在标准 Data Protection for VMware 环境中，将为每个数据移动设备节点使用单独的 dsm.opt 文件 (Windows) 或 dsm.sys 文件节 (Linux)。如果 vStorage 备份服务器上的多个数据移动设备节点都用于重复数据删除，并且这些节点都有权移动同一数据中心节点的数据，那么每个 dsm.opt 文件或 dsm.sys 文件节对于 dedupcachepath 选项必须包含不同的值。要获取最佳结果，请为每个 dsm.opt 文件或 dsm.sys 文件节指定不同的 schedlogname 和 errorlogname 选项。步骤 2 中提供了最少所需的选项集。

物理数据移动设备节点通常使用 SAN 备份和复原数据。如果将数据移动设备节点配置为直接访问存储卷，请关闭自动盘符分配。如果未关闭盘符分配，那么数据移动设备节点上的客户机可能会破坏虚拟盘的原始数据映射 (RDM)。如果虚拟盘的 RDM 已损坏，那么备份将失败。

限制：Data Protection for VMware 不支持将 vStorage 备份服务器（用作数据移动设备）调度为备份其自身。请确保将 vStorage 备份服务器排除在其自己的调度以外。对于包含 vStorage 备份服务器的 VM，请使用其他 vStorage 备份服务器来执行该 VM 的备份。

关于此任务

提示：该过程中的所有步骤均在 vStorage 备份服务器上完成。

过程

1. **Linux** 确保目标机器上已安装 Java 软件。
2. **Linux** 设置相关的环境变量。
 - a. 确保已正确导出 JAVA_HOME 环境变量：
`export JAVA_HOME=<jre-or-jdk-install-dir>`
 - b. 确保已正确导出 PATH 环境变量：
`export PATH=$PATH:$JAVA_HOME/jre/bin`
 - c. 确保已正确导出 LD_LIBRARY_PATH 环境变量。选中或将其设置为客户机安装目录和 Java 共享库 libjvm.so：

对于 IBM Java：
`export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic`

对于 Oracle Java：
`export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server`
3. 在以下位置创建 dsm.opt 或 dsm.sys 选项文件：
 - **Windows:** C:\Program Files\Tivoli\TSM\baclient
 - **Linux:** /opt/tivoli/tsm/client/ba/bin
4. 将这些选项从数据移动设备的样本选项文件复制到 dsm.opt 或 dsm.sys 文件中。要查找数据移动设备的样本文件：
 - 打开 Web 浏览器，并输入 GUI Web 服务器地址。例如：
`https://guihost.mycompany.com:9081/TsmVMwareUI/`
 - 使用 vCenter 用户名和密码登录，并确保选中**配置方式**。
 - 在配置向导中，转至“数据移动设备节点”页面。
 - 找到所需的数据移动设备，然后单击**查看**。

- 将样本选项从 **Windows** 或 **Linux** 选项卡复制到选项文件中。

如果环境需要，可以更新这些选项。

要获取选项描述，请参阅选项参考。

对于即时访问、即时复原或安装（文件复原）操作，请确保将 VMISCSISERVERADDRESS 添加到数据移动设备选项文件。在即时操作中用于 iSCSI 数据传输的 vStorage Backup Server 上，指定网络卡的 iSCSI 服务器 IP 地址。与 ESX 主机上的 iSCSI 设备绑定的物理网络接口卡 (NIC) 必须与用于 iSCSI 传输的 vStorage Backup Server 上的 NIC 位于同一子网。

5. 发出以下命令来设置数据移动设备节点的 VMware vCenter 用户名和密码：

```
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
```

6. 通过完成以下任务设置客户机接收器服务和数据移动设备调度程序服务：

- **Windows** 此过程使用"IBM Spectrum Protect 客户机 GUI 配置"向导来设置客户机接收器服务和调度程序服务。缺省情况下，远程客户机代理进程服务也通过向导进行设置。如果将 IBM Spectrum Protect 客户端服务配置实用程序 (dsmcutil) 用于此服务，那么确保还安装了远程客户机代理进程服务。

通过转至实用程序 > 设置向导，从文件菜单启动"IBM Spectrum Protect 客户机配置"向导：

- 选择**帮助我配置 TSM Web 客户机**。按提示输入信息。
 - a. 在您希望服务何时启动？选项中，选择当 **Windows** 引导时自动启动。
 - b. 在您是否希望在此向导完成时启动服务？选项中，选择是。

操作成功完成后，返回到向导欢迎页面并继续执行步骤 b。

提示：如果在同一机器上配置多个数据移动设备节点，必须为每个客户机接收器实例指定不同的端口值。

- 选择**帮助我配置 TSM 客户机调度程序**。按提示输入信息。
 - a. 输入调度程序名称时，请确保选择**使用客户机接收器守护程序 (CAD) 管理调度程序**选项。
 - b. 在您希望服务何时启动？选项中，选择当 **Windows** 引导时自动启动。
 - c. 在您是否希望在此向导完成时启动服务？选项中，选择是。

- **Linux** 对于 **Linux** 上的数据移动设备，请完成以下步骤：

- a. 安装程序在 /etc/init.d 中针对客户机接收器 (dsmcad) 创建启动脚本。在 /etc/init.d/dsmcad file 中选中或设置相关的环境变量。
- b. 在 dsm.sys 文件中针对数据移动设备节点的一节中指定以下选项：

- 指定带有以下两个参数的 managedservices 选项：

```
managedservices schedule webclient
```

该设置用于指示客户机接收器来管理 Web 客户机和调度程序。

- （可选）如果希望将调度和错误信息定向到缺省文件以外的日志文件，那么请以用于存储日志信息的标准路径名和文件名来指定 schedlogname 和 errorlogname 选项。例如：

```
schedlogname /vmsched/dsmsched_dm.log
errorlogname /vmsched/dsmerror_dm.log
```


c. 启动客户机接收器服务：

客户机接收器必须先启动，然后才能管理调度程序任务或管理 Web 客户机。
作为 root 用户完成以下步骤：

- 1) 配置客户机接收器服务和数据移动设备调度程序服务以充当 vStorage 备份服务器。
- 2) 通过发出以下命令启动客户机接收器：

```
service dsmcad start
```

要使客户机接收器能够在系统重新启动后自动启动，请按如下 shell 提示符添加服务：

```
# chkconfig --add dsmcad
```

提示：如果要通过 Linux 命令行直接运行 **dsmc** 命令，那么还必须将步骤 2 中提到的同等环境变量应用于命令 Shell。

7. 使用 **-asnodename** 和 **-optfile** 命令行参数启动数据移动设备命令行会话：

```
dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
```

请确保初始登录后，不会提示您输入密码。

警告：为了避免 IBM Spectrum Protect 调度程序失败，请确保 dsm.opt 文件(Windows) 或 dsm.sys 文件节 (Linux) 中未设置 asnodename 选项。该调度程序向 IBM Spectrum Protect 服务器查询与 nodename（数据移动设备节点）而非 asnodename（数据中心节点）相关联的调度。如果在 dsm.opt 或 dsm.sys 中设置了 asnodename，那么会查询与 asnodename（而非 nodename）相关联的调度。从而导致调度操作失败。

完成以下任务：

a. 通过发出以下命令来验证与 IBM Spectrum Protect 服务器的连接：

```
dsmc query session
```

该命令显示关于会话的信息，包括当前节点名、建立会话的时间、服务器信息以及服务器连接信息。

b. 通过发出此命令来验证您能否备份 VM：

```
dsmc backup vm vm1
```

在步骤 5b 和 5d 中，vm1 是 VM 的名称。

c. 通过发出以下命令验证备份是否已成功完成：

```
dsmc query vm "*" 
```

d. 通过发出此命令来验证能否复原 VM：

```
dsmc restore vm vm1 -vmname=vm1-restore
```

8. 验证客户机接收器和代理程序是否设置正确：

a. 在 Web 浏览器中，输入 IBM Spectrum Protect vSphere Client 插件地址。
例如：

```
https://guihost.mycompany.com/vsphere-client/
```

b. 使用 vCenter 用户名和密码登录。

- c. 在 vSphere Web 客户机中，单击 **IBM Spectrum Protect > 配置 > 数据移动设备**。
- d. 确保在数据移动设备的状态列中显示已验证。 如果显示失败，那么请悬停于此状态上已查看失败消息。

提示：当安装 Data Protection for VMware vSphere GUI 的系统上的 IP 地址发生更改时，必须完成以下操作：

- a. 再次设置客户机接收器，以使 Data Protection for VMware vSphere GUI 变为启用状态，可进行操作。否则，插件管理器会将 Data Protection for VMware vSphere GUI 状态显示为已禁用。

在 vSphere 环境中配置 Data Protection for VMware 命令行界面

在安装有 Data Protection for VMware vSphere GUI 的系统上更新 Data Protection for VMware 命令行界面概要文件。

开始之前

此概要文件 (vmcliprofile) 位于安装有 Data Protection for VMware vSphere GUI 的系统上的以下目录中：

Linux /opt/tivoli/tsm/tdpvmware/common/scripts

Windows 64 位：C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts

关于此任务

此过程中的所有步骤都在安装有 Data Protection for VMware vSphere GUI 的系统上完成。

提示：也可以使用 Data Protection for VMware vSphere GUI 配置向导或配置笔记本来完成此任务。 转至 Data Protection for VMware vSphere GUI"配置"窗口，然后单击**运行配置向导或编辑配置**。

过程

1. 使用以下设置来更新此概要文件：

VE_TSMCLI_NODE_NAME

指定用于将 Data Protection for VMware 命令行界面连接至 IBM Spectrum Protect 服务器和代理进程节点 (MY_VMCLINODE) 的节点。

限制：与 IBM Spectrum Protect 服务器通信时，VMCLI 节点不支持 SSL 协议或 LDAP 认证。

VE_VCENTER_NODE_NAME

指定表示 vCenter 的虚拟节点 (MY_VCNODE)。

VE_DATACENTER_NAME

指定映射到数据中心的虚拟节点。 正确的语法如下所示：

datacenter_name::datacenter_node_name

- datacenter_name 值区分大小写。
- 确保为环境中的每个数据中心 (MY_DCNODE) 都设置此参数。
- Data Protection for VMware vSphere GUI不支持 vCenter 中存在多个同名的数据中心。

VE_TSM_SERVER_NAME

指定 IBM Spectrum Protect 服务器的主机名或 IP。

VE_TSM_SERVER_PORT

指定要用于 IBM Spectrum Protect 服务器的端口名。缺省值为 1500。

下面提供了包含这些设置的示例概要文件：

VE_TSMCLI_NODE_NAME	MY_VMCLINODE
VE_VCENTER_NODE_NAME	MY_VCNODE
VE_DATACENTER_NAME	MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME	tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT	1500

2. 在 pwd.txt 文件中设置 VMCLI 节点密码。

此密码用于将 Data Protection for VMware 命令行界面连接至 IBM Spectrum Protect 服务器和数据移动设备节点的节点。它由 VE_TSMCLI_NODE_NAME 概要文件参数指定。

a. 发出 echo 命令，以创建包含密码的文本文件：

Linux echo password1 > pwd.txt

Windows echo password1> pwd.txt

Windows 密码 (password1) 与大于号 (>) 之间不存在空格。

b. 发出以下 vmcli 命令，为 VMCLI 节点设置密码：

```
vmcli -f set_password -I pwd.txt
```

要点：

- **Linux** 您必须作为 tdpvmware 用户而不是 Root 用户来发出 vmcli -f set_password 命令。
- **Linux** **Windows** 如果计划生成应用程序保护报告，那么必须指定 **-type VMGuest** 参数以标识该密码将应用于 VM。例如：

```
vmcli -f set_password -type VMGuest -I password.txt
```

3. 验证 Data Protection for VMware 命令行界面是否正在运行：

Windows 单击开始 > 控制面板 > 管理工具 > 服务，并验证 Data Protection for VMware 命令行界面 的状态是否为已启动。

Linux 转至脚本目录 (/opt/tivoli/tsm/tdpvmware/common/scripts/) 并发出此命令：

```
./vmclid status
```

- 如果守护程序正在运行，请前进步骤 4。
- 如果守护程序未在运行，请发出以下命令以手动启动守护程序：

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

以下 init 脚本也可用于停止和启动守护程序：

```
./vmclid stop  
./vmclid start
```

4. 发出 vmcli 命令以验证 Data Protection for VMware 命令行界面是否可识别 IBM Spectrum Protect 节点配置：

```
vmcli -f inquire_config -t TSM
```

5. 验证节点以确保不会发生任何配置错误：
 - a. 单击 vSphere Client 的"解决方案和应用程序"窗口中的图标以启动 Data Protection for VMware vSphere GUI。
 - b. 转到"配置"窗口。
 - c. 选择表中的某个节点，然后单击验证所选节点。"状态详细信息"窗格中将显示状态信息。

下一步做什么

Linux

Windows

成功完成本节中所述的三项手动配置任务后：

1. 第 82 页的『在 vSphere 环境中设置 IBM Spectrum Protect 节点』
2. 第 83 页的『使用 vSphere 插件 GUI 设置数据移动设备节点』

备份 VM 数据不需要其他配置任务。

vSphere 环境命令行界面配置核对表

使用此过程在 vSphere 环境中仅通过命令行界面配置 Data Protection for VMware。

过程

在 IBM Spectrum Protect 服务器上完成步骤 1 和步骤 2。

1. 向 IBM Spectrum Protect 服务器注册以下节点：
 - a. 表示 VMware vCenter 的节点（vCenter 节点）：

```
REGister Node MY_VCNode <password for MY_VCNode>
```
 - b. 在 IBM Spectrum Protect 与 Data Protection for VMware vSphere GUI 之间通信的节点（VMCLI 节点）：

```
REGister Node MY_VMCLINode <password for MY_VMCLINode>
```
 - c. 表示数据中心并用于存储 VM 数据的节点（数据中心节点）：

```
REGister Node MY_DCNode <password for MY_DCNode>
```
 - d. 从一个系统"将数据移动"到另一个系统的节点（数据移动设备节点）：

```
REGister Node MY_DMNode <password for MY_DMNode>
```
2. 为以下节点定义代理关系：
 - a. 通过发出以下命令，向 vCenter 节点授予代理权限：

```
GRant PROXynode Target=MY_VCNode AGent=MY_DCNode,MY_VMCLINode
```

此命令将向 MY_DCNode 和 MY_VMCLINode 授予代表 MY_VCNode 备份和复原 VM 的权限。
 - b. 通过发出以下命令，向数据中心节点授予代理权限：

```
GRant PROXynode Target=MY_DCNode AGent=MY_VMCLINode,MY_DMNode
```

此命令将向 MY_VMCLINODE 和 MY_DMNODE 授予代表 MY_DCNODE 备份和复原 VM 的权限。

- c. (可选) 向环境中的任何其他数据中心节点或数据移动设备节点授予代理权限。
- d. 通过发出 IBM Spectrum Protect 服务器 Query PROXynode 命令, 验证代理关系。预期的命令输出如下所示:

Target Node	Agent Node
MY_VCNODE	MY_DCNODE MY_VMCLINODE
MY_DCNODE	MY_VMCLINODE MY_DMNODE

在 vStorage 备份服务器上完成步骤 3 到步骤 9。

3. 为以下数据移动设备选项设置相应的值:

- **Windows** 在 dsm.opt 选项文件中指定以下选项。
- **Linux** 在 dsm.sys 文件中与数据移动设备节点相应一节中指定以下选项。

NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPOINT
COMMMETHOD
HTTPPORT

注: 仅当使用多个客户机接收器服务 (CAD) 时, 才需要 HTTPPORT。例如, 如果存在两个数据移动设备节点 (以及两个 CAD 服务), 那么每个数据移动设备节点的选项文件必须指定不同的 HTTPPORT 值。

以下提供了包含这些选项的 dsm.dm.opt 文件示例:

```
NODename MY_DMNODE
PASSWORDAccess generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType Fullvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPOINT 1500
COMMMethod tcpip
HTTPPORT 1583
```

4. 通过发出以下命令来验证与 IBM Spectrum Protect 服务器的连接:
dsmc query session
5. 发出以下命令来设置数据移动设备节点的 VMware vCenter 用户名和密码:
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
6. 设置以下 IBM Spectrum Protect 服务:

- **Windows**
 - a. 安装调度程序服务:
dsmcutil install scheduler /name:"TSM Central Scheduler Service"
/node:MY_DMNODE /password:MY_DMNODEPWD /startnow:no /autostart:no

b. 安装 CAD:

```
dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE  
/password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt  
/cadschedname:"TSM Central Scheduler Service" /startnow:no  
/autostart:yes
```

c. 安装远程客户机代理进程服务:

```
dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE  
/password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt  
/partnername:"TSM CAD - MY_DMNODE" /startnow:no
```

- **Linux** 在 `dsm.sys` 文件与数据移动设备节点相应的节中指定 `managedservices` 选项:

确保指定 `schedule` 和 `webclient` 参数:

```
managedservices schedule webclient
```

该设置用于指示客户机接收器来管理 Web 客户机和调度程序。

- 7. **Linux** 要将客户机接收器服务和数据移动设备调度程序服务配置为充当 vStorage 备份服务器,请在 `/etc/init.d/dsmcad` 文件中设置以下环境变量:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```

- 8. **Linux** 启动客户机接收器服务: 安装程序将在 `/etc/init.d` 中为客户机接收器守护程序 (`dsmcad`) 创建启动脚本。客户机接收器守护程序必须先启动,然后才能管理调度程序任务或管理 Web 客户机。以 `root` 用户身份使用以下命令来启动守护程序:

```
service dsmcad start
```

要使客户机接收器守护程序能够在系统重新启动后自动启动,请按如下 shell 提示符添加服务:

```
# chkconfig --add dsmcad
```

- 9. 验证 IBM Spectrum Protect 服务是否正确设置:

a. 登录到远程系统。

b. 通过以下地址和端口使用 Web 浏览器连接到 HOST1 系统:

```
http://HOST1.xyz.yourcompany.com:1581
```

在安装有 Data Protection for VMware vSphere GUI 的系统上完成步骤 10。

- 10. 为 Data Protection for VMware 命令行界面概要文件 (`vmcliprofile`) 中的以下选项设置相应的值:

```
VE_TSMCLI_NODE_NAME  
VE_VCENTER_NODE_NAME  
VE_DATACENTER_NAME  
VE_TSM_SERVER_NAME  
VE_TSM_SERVER_PORT
```

以下提供了包含这些选项的概要文件示例:

```
VE_TSMCLI_NODE_NAME MY_VMCLINODE  
VE_VCENTER_NODE_NAME MY_VCNODE  
VE_DATACENTER_NAME MyDatacenter1::MY_DCNODE  
VE_TSM_SERVER_NAME tsmserver.mycompany.xyz.com  
VE_TSM_SERVER_PORT 1500
```

概要文件位于以下目录中：

Linux /opt/tivoli/tsm/tdpvmware/common/scripts

Windows 64 位：C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts

a. 为 VMCLI 节点设置密码：

1) 发出 echo 命令，以创建包含密码的文本文件：

Linux

```
echo password1 > pwd.txt
```

Windows

```
echo password1> pwd.txt
```

2) 发出以下 vmcli 命令，为 VMCLI 节点设置密码：

要点： **Linux**

必须以 tdpvmware 用户身份而非 root 用户身份发出此命令。

```
vmcli -f set_password -I pwd.txt
```

b. 验证 Data Protection for VMware 命令行界面是否正在运行：

Windows

从 Windows 命令提示符发出以下命令：

```
net start
```

Linux

发出以下命令：

```
./vmclid status
```

c. 发出 vmcli 命令以验证 Data Protection for VMware 命令行界面是否可识别 IBM Spectrum Protect 节点配置：

```
vmcli -f inquire_config -t TSM
```

磁带配置指南

在对磁带存储器尝试备份操作之前请复审这些准则。

准备备份到磁带

Linux

Windows

在尝试备份到磁带前，必须在 IBM Spectrum Protect 服务器上为磁带备份设置这些参数：

1. 定义管理类：

```
define mgmtclass <domain name> <policy set name> <mgmtclass name>
```

例如：

```
define mgmtclass tape tape DISK
```

2. 定义副本组：

```
define copygroup <domain name> <policy set name> <mgmtclass name>  
destination=<stgpool name>
```

例如：

```
define copygroup tape tape DISK destination=Diskpool
```

3. 激活策略集：

```
activate policyset <domain name> <policy set name>
```

例如：

```
activate policyset tape tape
```

配置向物理磁带的备份时，存在其他配置需求。必须总是保留磁盘上的 IBM Spectrum Protect 元数据（控制文件）和磁带上的实际 VM 备份。

- 使用 VMMC 选项以存储具有管理类而非缺省管理类的 VMware 备份（和 VMware 控制文件）。
- 使用 VMCTLMC 选项指定在 VMware 备份过程中专用于 VMware 控制文件的管理类。您指定的管理类将覆盖缺省管理类。也将覆盖由 VMMC 选项指定的管理类。VMCTLMC 管理类必须指定不能迁移到磁带的磁盘存储池。
- VMMC 选项总是用于控制 VM 备份上的保留时间。此选项可以应用到磁盘和磁带配置。VMCTLMC 不用于设置控制文件的保留时间。控制文件和数据文件是相同分组的组成部分，根据 VMMC 选项的保留时间策略同时到期。当选项都已设置完毕后，VMMC 将用于数据文件、VMCTLMC 将用于控制文件。

限制：如果复原操作使用不依赖 LAN 的配置中的存储代理进程，那么此类复原操作可能从副本存储池复原文件，即使数据可从主存储池获取。如果复原请求针对特定的文件，或者复原请求未使用无查询方法，并且文件的主副本存储在无法通过不依赖 LAN 的路径访问的存储池中，那么可能发生此情况。这还可能影响非复原情境，例如 Data Protection for VMware 备份操作。在 Data Protection for VMware 环境中，VM 控制文件的首选存储方法是磁盘，因此在增量备份过程中不需要使用装配来复原文件。这些 VM 控制文件不仅需要放置在磁盘上，还不应该备份到可通过不依赖 LAN 的路径访问的副本存储池。如果已备份到此类存储池，那么从 Data Protection for VMware 客户机进行不依赖 LAN 的增量备份时，将使用磁带装配来复原这些文件。

如果 IBM Spectrum Protect 服务器环境使用从磁盘到磁带的迁移，请在迁移前考虑以下指南：

- 将磁盘存储池 MIGDELAY 设为支持要满足的来自磁盘的大部分装配请求。普通用途模式表明最近几天内很有可能发生单个文件恢复。例如，通常为文件上次修改之后的 3 到 5 天。因此，可以考虑为这个短暂的时间保留磁盘上的数据，以优化恢复操作。

此外，如果将客户端删除重复与磁盘存储池配合使用，那么请设置用于管理完全 VM 备份的频率的 MIGDELAY 选项。至少对 VM 完成两次完全备份后再将数据从删除重复的存储池迁移到磁带。数据移动到磁带之后，就再也不会重复。例如，如果每周都运行完全备份，则需要考虑将 MIGDELAY 设置为至少为 10 天的值。此设置确保每次完全备份都可以从移动到磁带之前的原备份中识别和使用重复数据。

- 应该使用设备类文件存储池，而不能使用磁盘设备类存储池。设备类 MAXCAPACITY 参数指定的卷大小的一般值为 8 GB 到 16 GB。对于关联的存储池，考虑使用按照文件空间进行的并置。备份的每个 VM 都表示为 IBM Spec-

trum Protect 服务器上的一个独立文件空间。按文件空间进行并置将保存来自相同卷（磁盘文件）上的给定 VM 的多个增量备份的数据。迁移到磁带时，按文件空间并置会将来自给定 VM 的多个增量备份同时放到物理磁带上。

使用设置对话框以设置磁带方式值。

如果装配或即时复原操作同时需要备份操作正在使用的同一磁带存储器，备份操作会中断。

在 Linux 系统上手动配置 iSCSI 设备

Linux

此过程描述如何配置在 iSCSI 装配操作期间使用的 Linux 系统。此 VM 快照是从 IBM Spectrum Protect 服务器存储器装配的。

开始之前

在 iSCSI 装配期间，将在“恢复代理进程”系统上创建 iSCSI 目标。恢复代理进程系统上不需要 Microsoft iSCSI 发起程序。

提示：Open-iSCSI Initiator 随 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 提供。

请查看以下 iSCSI 需求，然后再继续进行此任务：

- 您可以从任意系统连接至 iSCSI 目标以创建包含备份数据的卷。您可以从其他系统装配该卷。
- iSCSI 启动程序在必须连接到 iSCSI 目标的任何系统上都是必需的。
- 在复原数据的系统上必须已安装 iSCSI 启动程序。
- 如果卷跨多个磁盘，那么您必须装配所有必需的磁盘。使用镜像卷时，只要装配镜像磁盘中的一个。装配一个磁盘可以避免耗时的同步操作。

关于此任务

完成以下步骤以配置在 iSCSI 装配操作期间使用的 Linux 系统：

过程

1. 在复原数据的系统上记录 iSCSI 启动程序的名称。iSCSI 启动程序名称位于 `/etc/iscsi/initiatorname.iscsi` 文件。如果 `InitiatorName=` 值为空，请使用以下命令创建发起方名称：

```
twauslbpoc01:~ # /sbin/iscsi-iname
```

以下是发起方名称示例：

```
iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

2. 将启动程序名称添加到 `/etc/iscsi/initiatorname.iscsi` 文件。

- a. 使用 **vi** 命令编辑 `/etc/iscsi/initiatorname.iscsi` 文件。例如：

```
twauslbpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
```

- b. 使用启动程序名称更新 **InitiatorName=** 参数。例如：

```
InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

3. 在安装有 恢复代理程序（或 iSCSI 目标）的系统上完成以下步骤：
 - a. 启动 恢复代理程序。完成"选择 IBM Spectrum Protect 服务器"和"选择快照"对话框，然后单击**安装**。
 - b. 在选择装配目标对话框中，选择装配 iSCSI 目标。
 - c. 创建目标名称。请确保该名称是唯一的，并且可以在运行 iSCSI 发起方的系统中识别该名称。例如：


```
iscsi-mount-tsm4ve
```
 - d. 输入在步骤 1 中记录的 iSCSI 发起方名称并单击**确定**。
 - e. 验证您刚装配的卷是否显示在 Mounted Volumes 字段中。
4. 找到并启动在步骤 1 中选择的发起方系统中的 iSCSI 发起方程序：
 - a. 发出以下命令以验证 iSCSI 服务是否正在运行：

Red Hat Enterprise Linux:

```
service iscsi status
```

SUSE Linux Enterprise Server:

```
service open-iscsi status
```

如果该服务未运行，请发出以下命令以启动该服务：

Red Hat Enterprise Linux:

```
service iscsi start
```

SUSE Linux Enterprise Server:

```
service open-iscsi start
```
 - b. 发出以下命令以连接到 iSCSI 目标：


```
iscsiadm -m discovery -t sendtargets -p <IP/hostname of  
恢复代理程序 system> --login
```
 - c. 发出以下命令以验证新的原始设备是否可用：


```
fdisk -l
```
5. 装配文件系统：

对于非 LVM 卷，发出以下命令。在此示例中，新设备为 /dev/sdb1：

```
mkdir /mountdir  
mount /dev/sdb1 /mountdir
```

对于 LVM 卷，对 Linux 访客完成以下任务：

 - a. 确保 vgimportclone 脚本在 Linux 系统上可用。基本（缺省）LVM 软件包中未提供此脚本。因此，您可能需要将 LVM 软件包更新到提供此脚本的级别。
 - b. 发出 **vgimportclone** 命令，包含新的基本卷组名 (VolGroupSnap01)。例如：


```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```
 - c. 发出 **lvchange** 命令以将逻辑卷标记为活动。例如：


```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```
 - d. 发出以下命令以装配该卷：


```
mkdir /mountdir  
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```
6. 在文件复原操作完成后，发出以下命令：

- 对于非 LVM 卷，请发出以下命令：
 - a. 卸装文件系统：


```
umount /dev/sdb1 /mountdir
```
 - b. 移除该卷。 如果该卷属于某个卷组的一部分，首先发出以下命令以从该卷组中除去该卷：


```
vgreduce <your_volume_group> /dev/sdb1
```

然后发出以下命令以除去该卷：

```
pvremove /dev/sdb1
```
 - c. 从单个目标注销：


```
iscsiadm --mode node --targetname <目标名称> --logout
```
 - d. 从所有目标注销：


```
iscsiadm --mode node --logout
```
- 对于 LVM 卷，对 Linux 访客完成以下任务：
 - a. 卸装文件系统：


```
umount /mountdir
```
 - b. 除去逻辑卷：


```
lvm lvremove LogVol00
```
 - c. 除去卷组：


```
lvm vgremove VolGroupSnap01
```
 - d. 从单个目标注销：


```
iscsiadm --mode node --targetname <目标名称> --logout
```
 - e. 从所有目标注销：


```
iscsiadm --mode node --logout
```

在 Windows 系统上手动配置 iSCSI 设备

Windows

此过程描述如何配置在 iSCSI 装配操作期间使用的 Windows 系统。 从 IBM Spectrum Protect 服务器存储器装配快照。

开始之前

请查看以下 iSCSI 需求，然后再继续进行此任务：

- 在 iSCSI 装配期间，将在 恢复代理程序系统上创建 iSCSI 目标。您可以从任意系统连接至 iSCSI 目标以创建包含备份数据的卷。 另外，还可以从其他系统装配该卷。
- iSCSI 启动程序在必须连接到 iSCSI 目标的任何系统上都是必需的。
- 请确保在复原数据的系统上已安装 iSCSI 启动程序。
- 恢复代理程序系统上不需要 Microsoft iSCSI 发起方。

请查看以下磁盘和卷需求，然后再继续执行此任务：

- 如果卷跨多个磁盘，那么您必须装配所有必需的磁盘。 使用镜像卷时，只要装配镜像磁盘中的一个。 装配一个磁盘可以避免耗时的同步操作。

- 如果多个动态磁盘用于备份系统中，那么这些磁盘将分配到同一个组中。因此，当您只装配一个磁盘时，Windows 磁盘管理器可能认为缺少某些磁盘而发出错误消息。请忽略此消息。仍然可以访问备份磁盘中的数据，除非某些数据在其他磁盘组中。可以通过装配所有动态磁盘来解决该问题。

关于此任务

完成以下步骤以配置在 iSCSI 装配操作期间使用的 Windows 系统：

过程

1. 在 恢复代理程序系统上，在 LAN 防火墙和 Windows 客户机防火墙中打开端口 3260。在复原数据的系统上记录 iSCSI 启动程序的名称。

iSCSI 发起方名称显示在控制面板的 iSCSI 发起方配置窗口中。例如：

```
iqn.1991-05.com.microsoft:hostname
```

2. 在安装了 恢复代理程序（或 iSCSI 目标）的系统中完成以下任务：
 - a. 启动 恢复代理程序 GUI。完成"选择 IBM Spectrum Protect 服务器"和"选择快照"对话框，然后单击**安装**。
 - b. 在"选择装配目标"对话框中，选择**装配 iSCSI 目标**。
 - c. 创建目标名称。请确保该名称是唯一的，并且可以在运行 iSCSI 发起方的系统中识别该名称。例如：


```
iscsi-mount-tsm4ve
```
 - d. 输入在步骤 1 中记录的 iSCSI 发起方名称并单击**确定**。
 - e. 验证您刚装配的卷是否显示在"装配的卷"字段中。
 - f. 如果在 iSCSI 网络中使用"恢复代理进程"，并且"恢复代理进程"不使用数据移动设备，请转至 C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf 文件，并指定 [IMOUNT] 标记和 **Target IP** 参数：

```
[IMOUNT config]
Target IP=<IP address of the network card on the system
that exposes the iSCSI targets.>
```

例如：

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

添加或更改 Target IP 参数后，请重新启动恢复代理进程 GUI 或恢复代理进程 CLI。

3. 找到并启动在步骤 1 中选择的发起方系统中的 iSCSI 发起方程序：
 - a. 连接到 iSCSI 目标：
 - 1) 在"目标"选项卡中，输入"目标："对话框中的步骤 2 中使用的 恢复代理程序（iSCSI 目标）的 TCP/IP 地址。单击**快速连接**。
 - 2) "快速连接"对话框将显示与步骤 2c 中指定的目标名称匹配的目标。如果它还未连接，请选择此目标并单击**连接**。

- b. 在启动程序系统上，转至控制面板 > 管理工具 > 计算机管理 > 存储 > 磁盘管理。
 - 1) 如果装配的 iSCSI 目标列示为 Type=Foreign，那么请右键单击外部磁盘并选择导入外部磁盘。选择"外部磁盘组"。单击确定。
 - 2) 下一个屏幕将显示"外部磁盘"的类型、条件和大小。单击确定并等待磁盘导入。
 - 3) 磁盘导入完成后，请按 **F5**（刷新）。装配的 iSCSI 快照可见并包含分配的盘符。如果未自动分配盘符，请右键单击所需的分区并选择更改盘符或路径。单击添加并选择盘符。
4. 打开 Windows 资源管理器（或其他实用程序）并浏览已装配的快照，以进行文件复原操作。
5. 复原文件之后，请完成以下任务：
 - a. 使用"iSCSI 启动程序属性"对话框断开每个 iSCSI 目标的连接。
 - b. 通过在 恢复代理程序 GUI 中选择步骤 2 中的卷并单击卸装来卸装该卷。

在 Linux 系统上手动配置装配代理节点

Linux

完成此任务以将装配代理节点添加到远程 Linux 系统。

开始之前

在标准 Data Protection for VMware vSphere GUI 环境中，针对每个装配代理节点使用一个独立的 dsm.sys 文件节。此过程中的所有步骤均使用备份服务器上安装的数据移动设备完成。

关于此任务

此任务通过更新数据移动设备选项并验证与 IBM Spectrum Protect 服务器的连接来设置装配代理节点。

过程

1. 在 dsm.sys 文件中针对 装配代理节点 的一节中指定以下选项。

NODENAME

指定先前定义的装配代理节点的名称。IBM Spectrum Protect 调度与此节点关联。

PASSWORDACCESS

指定 GENERATE 以使密码自动生成（而不是通过用户提示）。

MANAGEDSERVICES

指定此选项以指示客户机接收器管理 Web 客户机以及调度程序 (schedule webclient)。

TCPSERVERADDRESS

指定 IBM Spectrum Protect 服务器的 TCP/IP 地址。

TCPPORT

指定 IBM Spectrum Protect 服务器的 TCP/IP 端口地址。

COMMMETHOD

指定 IBM Spectrum Protect 服务器要使用的通信方法。对于装配代理节点，必须指定 TCP/IP 作为通信方法。如果指定其他方法，操作会失败。

HTTPPORT

该选项指定了 TCP/IP 端口，并且仅当使用所个客户机接收器服务 (CAD) 时才必须指定该选项。例如，如果存在两个装配代理节点（以及两个 CAD 服务），那么每个装配代理节点的选项文件必须指定不同的 HTTPPORT 值。

限制：请勿在 dsm.sys 文件中启用不依赖 LAN 选项 (ENABLELANFREE YES)。装配代理节点不支持此选项。

以下提供了包含这些设置的 dsm.sys 文件示例：

```
Servername      tsm_server1
NODename datacenter1_MP_LNX
PASSWORDAccess  generate
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.myco.com
TCPPort         1500
COMMMethod tcpip
HTTPPORT 1583
```

2. 发出此命令为装配代理节点设置 VMware vCenter 用户和密码：

```
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
```

3. 使用 -asnodename 和 -optfile 命令行参数启动数据移动设备命令行会话：

```
dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys
```

请确保初始登录后，不会提示您输入密码。

警告：为避免 IBM Spectrum Protect 调度程序失败，请确保 dsm.sys 文件节中未设置 asnodename 选项 (Linux)。该调度程序向 IBM Spectrum Protect 服务器查询与 nodename（装配代理节点）而非 asnodename（数据中心节点）相关联的调度。如果在 dsm.sys 中已设置 asnodename，那么将查询与 asnodename（而非 nodename）关联的调度。从而导致调度操作失败。

4. 通过发出以下命令来验证与 IBM Spectrum Protect 服务器的连接：

```
dsmc query session
```

该命令显示关于会话的信息，包括当前节点名、建立会话的时间、服务器信息以及服务器连接信息。

5. 通过完成以下任务来设置客户机接收器服务 (CAD) 和数据移动设备调度程序服务：

- 在 dsm.sys 文件中针对装配代理节点的一节中指定以下选项：

- 指定带有以下两个参数的 managedservices 选项：

```
managedservices schedule webclient
```

该设置用于指示客户机接收器来管理 Web 客户机和调度程序。

- 如果要将调度和错误信息定向至日志文件而非缺省文件，请指定 schedlogname 和 errorlogname 选项。每个选项都必须包含存储日志信息的标准路径和文件名。例如：

```
schedlogname /vmsched/dsmsched_mp_lnx.log
errorlogname /vmsched/dsmerror_mp_lnx.log
```

- 要将客户机接收器服务和数据移动设备调度程序服务配置为充当备份服务器，请在 /etc/init.d/dsmcad 文件中设置以下环境变量：

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```

- 启动客户机接收器服务：

安装程序将在 /etc/init.d 中为客户机接收器守护程序 (dsmcad) 创建启动脚本。客户机接收器守护程序必须先启动，然后才能管理调度程序任务或管理 Web 客户机。以 root 用户身份使用以下命令来启动守护程序：

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
service dsmcad start
```

要使客户机接收器守护程序能够在系统重新启动后自动启动，请按如下 shell 提示符添加服务：

```
# chkconfig --add dsmcad
```

6. 验证客户机接收器和代理进程是否设置正确：

- a. 登录到远程系统。
- b. 通过以下地址和端口使用 Web 浏览器连接到 HOST1 系统：

`http://HOST1.xyz.yourcompany.com:1581`

在远程 Windows 系统上手动配置装配代理节点

Windows

完成此任务以将装配代理节点添加到远程 Windows 系统。当您要添加第二个 Windows 装配代理节点添加到自己的环境中时，此任务是必需的。

开始之前

请确保已配置主要的 Windows 装配代理节点，然后再继续进行此任务。

关于此任务

在远程 Windows 装配代理系统上完成以下步骤：

过程

1. 在远程 Windows 装配代理系统上装配以下组件：

- 恢复代理程序
- IBM Spectrum Protect 数据移动设备

在 IBM Spectrum Protect for Virtual Environments 下载映像上访问这两个产品。在位于以下地址的 IBM Knowledge Center 中提供了分步安装指示信息：第 21 页的『在 Windows 系统上安装 Data Protection for VMware 组件』

2. 从创建的 Windows 装配代理节点检索样本选项文件内容，并将其添加到远程 Windows 装配代理系统上的选项文件：
 - a. 在 Windows 主装配代理系统上，转至 Data Protection for VMware vSphere GUI 中的“配置”窗口。
 - b. 单击“任务”列表中的编辑 **TSM** 配置。装入配置页可能需要一些时间。
 - c. 转至“装配代理节点对”页面。
 - d. 在表格的“主节点”列中，转至含暂挂位置的 Windows 装配代理节点，然后单击视图设置。
 - e. 复制显示在装配代理设置对话框中的样本 dsm.opt 文件内容。

- f. 将样本 dsm.opt 文件内容粘贴（或添加）到远程 Windows 装配代理系统上。使用将此选项文件的角色标识为远程装配代理节点的约定来命名此选项文件。例如：dsm.REMOTE1_MP_WIN.opt。

限制：请勿在选项文件中启用不依赖 LAN 选项 (ENABLELANFREE YES)。装配代理节点不支持此选项。

3. 发出此数据移动设备命令，为装配代理节点设置 VMware vCenter 用户和密码：

提示：要启动 dsmc 命令行，请打开 **Windows 开始菜单**，选择程序→ **IBM Spectrum Protect** → **备份客户机命令行**。

```
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
-optfile=dsm.REMOTE1_MP_WIN.opt
```

4. 通过发出以下命令来验证与 IBM Spectrum Protect 服务器的连接：

```
dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
```

该命令显示关于会话的信息，包括当前节点名、建立会话的时间、服务器信息以及服务器连接信息。

5. 通过完成以下步骤来设置客户机接收器服务 (CAD) 和数据移动设备调度程序服务：此步骤使用"IBM Spectrum Protect 客户机 GUI 配置"向导来设置 CAD 和调度程序服务。缺省情况下，还可通过该向导设置"远程客户机代理进程服务"。如果将 IBM Spectrum Protect 客户机服务配置实用程序 (dsmcutil) 用于此任务，请确保还要安装"远程客户机代理进程服务"。
通过转至**实用程序 > 设置向导**，从文件菜单启动"IBM Spectrum Protect 客户机配置"向导：

- a. 选择帮助我配置 TSM Web 客户机。按照提示输入信息。
- 1) 在您希望服务何时启动？选项中，选择当 Windows 引导时自动启动。
 - 2) 在您是否希望在此向导完成时启动服务？选项中，选择是。

操作成功完成后，返回到向导欢迎页面并继续执行步骤 b。

提示：如果在同一系统上配置多个装配代理节点，必须为每个客户机接收器实例指定不同的端口值。

- b. 选择帮助我配置 TSM 客户机调度程序。按照提示输入信息。
- 1) 输入调度程序名称时，请确保选择使用客户机接收器守护程序 (CAD) 管理调度程序选项。
 - 2) 在您希望服务何时启动？选项中，选择当 Windows 引导时自动启动。
 - 3) 在您是否希望在此向导完成时启动服务？选项中，选择是。
6. 验证客户机接收器和代理进程是否设置正确。通过以下地址和端口使用 Web 浏览器连接到 HOST1 系统：

<http://HOST1.xyz.yourcompany.com:1581>

在 Linux 系统上手动配置多个客户机接收器服务

在某些情况下，在一台 Linux 客户机主机上使用多个 dsmcad 服务可能会有益处。

关于此任务

本任务设置在系统启动时自动运行和启动的多个 dsmcad 实例：

过程

1. 在 dsm.sys 文件中创建两个唯一节点节（缺省情况下，此文件位于 /opt/tivoli/tsm/client/ba/bin/ 中）：

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
COMMethod      TCPip
TCPPort        1500
TCPServeraddress localhost
nodename        node1
errorlogname    /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
schedlogname    /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
manageservices  webclient sched
httpport        1581
passwordaccess  generate

SErvername node2
COMMethod      TCPip
TCPPort        1500
TCPServeraddress localhost
nodename        node2
errorlogname    /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
schedlogname    /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
manageservices  webclient sched
httpport        1582
passwordaccess  generate
```

提示：包含特定包含/排除选项来区分这些节点可能会有益处。否则，可能使用两个节点名备份相同数据。

2. 创建两个 dsm.opt 文件，分别用于两个节点（缺省情况下，这些文件位于 /opt/tivoli/tsm/client/ba/bin 中）：

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. 通过使用凭证登录为两个节点启用 passwordaccess generate：

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. 创建缺省 rc.dsmcad init 脚本的两份副本（缺省情况下，该脚本位于 /opt/tivoli/tsm/client/ba/bin 中）：

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. 编辑 rc.dsmcad-node1：

- a. 将 Red Hat Enterprise Linux 分发版的以下行：

```
daemon $DSMCAD_BIN
```

更改为以下行：

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

- b. 将 SUSE Linux Enterprise Server 分发版的以下行：

```
startproc $DSMCAD_BIN
```

更改为以下行：

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

6. 编辑 rc.dsmcad-node2：

- a. 将 Red Hat Enterprise Linux 分发版的以下行：

```
daemon $DSMCAD_BIN
```

更改为以下行：

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

- b. 将 SUSE Linux Enterprise Server 分发版的以下行：

```
startproc $DSMCAD_BIN
```

更改为以下行：

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

7. 在 /etc/init.d/ 中创建新链接以指向两个新的 rc.dsmcad init 脚本。这些链接使 Linux init 服务能够在系统启动时启动 dsmcad 服务：

```
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
# ls -la dsm*
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

8. 通过 chkconfig 注册两个新的 rc 脚本：

```
# chkconfig --add dsmcad-node1
# chkconfig --add dsmcad-node2
```

9. 通过 service dsmcad start 命令测试配置以确保脚本顺利装入和启动：

```
# service dsmcad-node1 start
Starting dsmcad-node1: [ OK ]
# service dsmcad-node2 start
Starting dsmcad-node2: [ OK ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

在此示例中，命令文本分两行防止以适应页面格式化。

10. 重新启动并确认两个 dsmcad 实例自动启动：

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

在此示例中，命令文本分两行防止以适应页面格式化。

修改 VMCLI 配置文件

VMCLI 配置文件 (vmcliConfiguration.xml) 包含 Data Protection for VMware vSphere GUI 的设置。

Data Protection for VMware 安装过程要求用户指定 vCenter Server IP 地址以及是否支持通过 Web 浏览器访问 GUI。但是，安装之后，安装者无法修改服务器 IP 地址和 GUI 访问方法。

要更新这些设置，可以手动编辑 VMCLI 配置文件 (vmcliConfiguration.xml)。安装期间会在以下位置创建此文件：

Windows 系统上：

C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI

Linux 系统上：

/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/

要修改是否支持通过 Web 浏览器访问 GUI，请在 **<enable_direct_start></enable_direct_start>** 参数中输入以下其中一个值：

- *yes* 可以通过 Web 浏览器直接访问 GUI。例如：

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* 无法通过 Web 浏览器直接访问 GUI。例如：

```
<enable_direct_start>no</enable_direct_start>
```

要将 GUI 用于 vSphere 保护，请在 **<mode></mode>** 参数中指定以下其中一个值：

- *vcenter* GUI 将用于 vSphere 保护。例如：

```
<mode>vcenter</mode>
```

要修改 vCenter Server IP 地址，请确保已设置 **<mode>vcenter</mode>**，然后在 **<vcenter_url></vcenter_url>** 参数中指定 IP 地址。例如：

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

vCenter Server IP 地址需要以 https:// 值开头。vCenter Server IP 地址需要以 /sdk 值结尾。

vmcliConfiguration.xml 文件示例

以下 vmcliConfiguration.xml 文件配置为用于 vSphere 保护，并支持通过 Web 浏览器访问 GUI:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
  <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
  <interruptDelay>900000</interruptDelay>
  <mode>vcenter</mode>
  <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
  <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

附录 B. 迁移至持续增量式增量备份策略

使用此过程来迁移现有备份调度、策略和数据移动设备节点，以供在增量永久备份策略中使用。

开始之前

可以使用 Data Protection for VMware V6.2 和 V6.3 中实现的持续增量式完全备份策略。如果要继续使用持续增量式完全备份策略，那么无需更改策略或调度。您必须确保如以下过程中所记录，仅将数据移动设备节点升级至版本 6.4（或更高版本）。但是，如果要使用持续增量式增量备份策略，除将数据移动设备节点更新至 V6.4（或更高版本）外，还必须为迁移至此持续增量式增量备份策略的数据移动设备节点更新调度和策略。

要将现有 Data Protection for VMware 调度迁移至持续增量式增量备份策略，必须完成此过程中记录的任务。

要点：

- 尽管某些任务是独立的，但是所有应用程序和组件最终都必须升级，这样才能从持续增量式增量备份策略获益。本出版物提供指导您完成每个任务的所有信息。
- 有多种方法可完成整个迁移过程。但是，本出版物中记录的方法被视为典型 Data Protection for VMware 环境的高效方法。
- 此过程中将迁移的调度是使用 Data Protection for VMware vSphere GUI 备份向导创建的调度。如果要迁移的调度是手动创建的，那么此过程中标识的调度更新也必须手动执行。

关于此任务

过程

1. 升级保护单个 vCenter 的所有 vStorage 备份服务器。确保此升级对于所有数据移动设备节点同时完成。
 - 此升级需要在 vStorage 备份服务器上安装 IBM Spectrum Protect 数据移动设备 V6.4（或更高版本）。
 - 作为一项独立任务，无需在完成步骤 1 之后立即完成步骤 2 或步骤 3。升级数据移动设备节点后，可以继续备份现有环境中的 VM。您可在更方便的时机完成步骤 2 和步骤 3。

提示：如果您的环境使用多个 vStorage 备份服务器，请考虑仅升级一个服务器。然后，确保该服务器成功运行，之后再升级其余的 vStorage 备份服务器。

2. 更新备份策略和备份调度以实现持续增量式增量备份：

通过在管理命令行客户机中发出命令 (dsmadm)，在 IBM Spectrum Protect 上完成以下备份策略任务：

 - a. 为持续增量式增量备份的相应域和策略集创建管理类。此示例将为域 domain1 和策略集 prodbackups 创建管理类 mgmt_ifincr28。管理类名用于描述可保留 28 个备份版本的持续增量式增量备份策略。

```
define mgmtclass domain1 prodbackups mgmt_ifincr28
description="Retain 28 backup versions"
```

- b. 创建持续增量式增量备份的备份副本组。此示例将为域 domain1、策略集 prodbackups 和管理类 mgmt_ifincr28 创建标准备份副本组：

```
define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
```

standard type=backup 条目是缺省值，无需指定。此示例中包含这些条目以便说明副本组名为 STANDARD，而副本组的类型为 backup（而非 archive）。

- c. 使用相应的版本、保留时间和到期设置更新备份副本组：

切记：在 Data Protection for VMware V6.2 和 V6.3 中，备份版本、保留时间和到期基于备份链粒度级别。此方法意味着即使同时采用持续增量式完全备份和持续增量式增量备份（作为 6.2 和 6.3 持续增量式完全备份策略的一部分），版本到期也只会将完全备份计算在内。在 Data Protection for VMware V6.4（或更高版本）中，备份版本、保留时间和到期基于单个备份粒度级别。此方法意味着版本到期会将持续增量式完全备份和持续增量式增量备份都计算在内。

verexists 参数指定要在服务器上保留的 VM 备份版本最大数。如果持续增量式增量备份操作导致超过该数字，那么服务器将使服务器存储中存在的最旧的备份版本到期。此示例指定 verexists=28。此值意味着服务器上最多将保留 28 个 VM 备份版本。

retextra 参数指定在 VM 备份版本变为不活动状态之后，该版本保留的最大天数。此示例指定 retextra=nolimit。此值意味着最大数目的不活动 VM 备份版本将无限期保留。但是，当指定 verexists 时，verexists 值将取代 nolimit 值。因此，在此示例中，服务器上最多将保留 28 个不活动 VM 备份版本。

根据此步骤中描述的设置，备份副本组将按如下所示更新：

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

在此示例中，现有 Data Protection for VMware V6.3 环境包含以下主机和调度：

- 一个 ESX 集群 (esxcluster)，其中包含两个 ESX 主机 (esxhost1 和 esxhost2)。
- bup_esxcluster_full 调度使用数据移动设备节点 dm1 对每个 ESX 主机运行每周一次的持续增量式完全备份。
- bup_esxcluster_incr 调度使用数据移动设备节点 dm2 对每个 ESX 主机运行每天一次的持续增量式增量备份。

在 Data Protection for VMware vSphere GUI 中完成以下备份调度任务：

- a. 单击 vSphere Client 的"解决方案和应用程序"窗口中的图标以启动 Data Protection for VMware vSphere GUI。
- b. 在"入门"窗口中，单击**备份**选项卡以打开"管理备份调度"窗口。
- c. 找到要更新的备份调度（用于持续增量式完全备份或持续增量式增量备份）。在此过程中，将使用持续增量式完全 bup_esxcluster_full 调度。
- d. 右键单击该调度，然后选择**属性**。
- e. 转至"调度"页面，然后从**备份策略**下拉列表中指定增量。
- f. 单击**确定**以保存更新。

- 当文件空间包含一个（或多个）持续增量式增量备份时，不支持持续增量式完全备份。

使用 verexists 参数进行版本控制的示例

在此调度迁移示例中，Data Protection for VMware V6.3 使用以下两个备份调度：

- `-mode=full`：调度为每周进行持续增量式完全备份（周日），要在服务器上保留的 VM 备份版本的最大数量为四 (`verexists=4`)。
- `-mode=incr`：调度为每个工作日进行持续增量式增量备份（周一至周六）。

对于 4 周长的时间段，生成的备份数为 28：

- 4 个持续增量式完全备份（每周 1 次完全备份乘以 4 周）
- 24 个持续增量式增量备份（6 个工作日增量备份乘以 4 周）

由于 Data Protection for VMware V6.3 仅计算完全备份，因此 `verexists=4` 值将保留所有 28 个备份。

要使用 Data Protection for VMware V6.4（或更高版本）和持续增量式增量备份策略提供相同级别的保护，请创建以下调度：

`-mode=iffull`：调度为每天进行 1 次持续增量式完全备份，`verexists` 参数设置为 28。

对于 4 周长的时间段，生成的备份数为 28：

- 1 个持续增量式完全备份（初始备份乘以 1 天）
- 27 个持续增量式增量备份（每天 1 次持续增量式备份乘以 27 天）

由于 Data Protection for VMware V6.4（或更高版本）将持续增量式完全备份和持续增量式增量备份都计算在内，因此 `verexists=28` 值将保留所有 28 个备份。

附录 C. IBM Spectrum Protect 产品系列的辅助功能选项

辅助功能选项帮助具有残疾（如行动不便或视力欠佳）的用户顺利使用信息技术内容。

概述

IBM Spectrum Protect 系列产品包括下列主要辅助功能选项：

- 仅键盘操作
- 使用屏幕朗读器的操作

IBM Spectrum Protect 系列产品使用最新 W3C 标准 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) 来确保符合 US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) 和 Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) 的要求。要充分利用的辅助功能选项功能部件，请使用最新版本的屏幕朗读器和受本产品支持的最新 Web 浏览器。

已对 IBM Knowledge Center 中的产品文档启用了辅助功能选项。在 IBM Knowledge Center 帮助的辅助功能选项部分 (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility) 中描述了 IBM Knowledge Center 的辅助功能选项功能部件。

键盘导航

本产品使用标准导航键。

界面信息

用户界面不含每秒闪烁 2 - 55 次的内容。

Web 用户界面依靠级联样式表来正确呈现内容并提供实用体验。该应用程序为视力欠佳用户提供了一种等效的方式来使用系统显示设置，其中包括高对比度方式。您可以使用设备或 Web 浏览器设置来控制字体大小。

Web 用户界面包含 WAI-ARIA 导航地标，您可以使用这些地标快速浏览到该应用程序中的功能区域。

供应商软件

IBM Spectrum Protect 产品系列包括 IBM 许可协议未覆盖的某些供应商软件。IBM 未对这些产品的辅助功能作任何说明。请联系供应商以获取有关其产品的辅助功能选项信息。

相关辅助功能选项信息

除建立标准 IBM 技术支持和支持 Web 站点外，IBM 还建立了 TTY 电话服务，供失聪或有听力障碍的客户访问销售与支持服务：

TTY 服务

800-IBM-3383 (800-426-3383)

(在北美地区)

有关 IBM 对辅助功能选项的承诺的更多信息，请参阅 IBM Accessibility (www.ibm.com/able)。

声明

本信息是为在美国国内供应的产品和服务而编写的。IBM 可能会以其他语言提供本资料。但是，您可能需要拥有该语言的产品或产品版本副本才能访问本资料。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您所在区域当前可获得的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或默示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US*

有关双字节 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供本出版物，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关不侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或默示的保证。因此本条款可能不适用于您。

本信息可能包含技术方面不够准确的地方或印刷错误。本信息将定期更改；这些更改将编入本信息的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及 (ii) 允许对已经交换的信息进行相互使用，请与下列地址联系：

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本文中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

此处讨论的性能数据是在特定的操作条件下获得并提供的。实际结果可能会有差异。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若现实生活中实际业务企业使用的名字和地址与此相似，纯属巧合。

版权许可证：

本信息包含源语言形式的样本应用程序，用以阐明在不同操作平台上的编程技术。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例尚未在所有条件下经过全面测试。因此，IBM 不能担保或默示这些程序的可靠性、可维护性或功能。这些实例程序“按现状”提供，不附有任何种类的保证。对于因使用样本程序所引起的任何损害，IBM 概不负责。

凡这些样本程序的每份拷贝或其任何部分或任何演绎作品，都必须包括如下版权声明：©（贵公司的名称）（年）。此部分代码是根据 IBM 公司的样本程序衍生出来的。© Copyright IBM Corp.（输入年份）。

商标

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp. 在世界多个司法管辖区的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 页面“版权和商标信息”(www.ibm.com/legal/copytrade.shtml) 提供了 IBM 商标的最新列表。

Adobe 是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标。

Linear Tape-Open、LTO 和 Ultrium 是 HP、IBM Corp 和 Quantum 在美国和其他国家或地区的商标。

Intel 和 Itanium 是 Intel Corporation 或其子公司在美国和其他国家或地区的商标或注册商标。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

Microsoft、Windows 和 Windows NT 是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

UNIX 是 The Open Group 在美国和/或其他国家或地区的注册商标。

VMware、VMware vCenter Server 或 VMware vSphere 是 VMware, Inc. 或其子公司在美国和/或其他管辖区域的注册商标或商标。

产品文档的条款和条件

根据下列条款和条件授予对这些出版物的使用许可权。

适用性

这些条款和条件是对 IBM Web 站点任何使用条款的补充。

个人用途

您可以为了个人使用而非商业性使用复制这些出版物，但前提是保留所有专有权声明。未经 IBM 明确许可，不能分发或展示这些出版物或其中任何部分，也不能制作其衍生产品。

商业用途

您仅可在贵公司内部复制、分发和显示这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得制作这些出版物的演绎作品，也不得在贵公司外部复制、分发或显示这些出版物或其部分出版物。

权利

除非本许可明确授权，否则对于这些出版物或其中包含的任何信息、数据、软件或其他知识产权，均不授予任何其他的许可、特许或权利，无论是明示还是默示。

只要 IBM 认为这些出版物的使用会损害其利益或者 IBM 判定未正确遵守上述指示信息，IBM 将有权撤销本文授予的许可权。

只有您完全遵循所有适用的法律和法规，包括所有的美国出口法律和法规，您才可以下载、出口或再出口该信息。

IBM 对这些出版物的内容不作任何保证。本出版物以"按现状"的基础提供，不附有任何形式的（无论是明示的，还是默示的）保证，包括但不限于默示的有关适销性、不侵权以及适用于某特定用途的保证。

隐私策略注意事项

IBM 软件产品（"软件产品"，包括软件即服务解决方案）可以使用 cookie 或其他技术来收集产品使用信息，以帮助改善最终用户体验，定制与最终用户的交互或用于其他目的。在许多情况下，"软件产品"不会收集任何个人可标识信息。我们的某些"软件产品"可帮助您收集个人可标识信息。如果此"软件产品"使用 cookie 来收集个人可标识信息，那么下面将提供关于此产品使用 cookie 的具体信息。

此"软件产品"不使用 cookie 或其他技术来收集个人可标识信息。

如果为此"软件产品"部署的配置使客户能够通过 cookie 和其他技术从最终用户那里收集个人可标识信息，那么您应该自行搜寻适用于此类数据收集的所有法律的法律建议，包括所有通知和同意需求。

有关将各种技术（包括 cookie）用于这些目的的更多信息，请参阅标题为"Cookie、Web 信标和其他技术"的部分中的 IBM 的隐私策略 (<http://www.ibm.com/privacy>) 和 IBM 的联机隐私声明 (<http://www.ibm.com/privacy/details>) 以及"IBM Software Products and Software-as-a-Service Privacy Statement"(<http://www.ibm.com/software/info/product-privacy>)。

词汇表

词汇表提供 IBM Spectrum Protect 系列产品的术语和定义。

请参阅 IBM Spectrum Protect 词汇表。

索引

[A]

安装

- 必需的通信端口 14
- 获取包 20
- 可安装组件 1
- 路线图 9
- 软件需求 10
- 系统需求 10
- 下载包 20
- 硬件需求 10
- 用户许可权 14
- 组件 19
- Data Protection for VMware 1
- Linux
 - 使用安装向导 22
- Windows
 - 使用安装向导 21

安装过程

- Linux
 - 静默 25
 - 全新 23
- Windows 64 位
 - 静默套件安装程序 24

安装向导

- Linux
 - 使用安装向导 22
- Windows
 - 使用安装向导 21

[B]

标记支持

- 启用 46

[C]

残疾 111

出版物 v

处理选项

- 使用 52, 53, 55

创建证书签名请求

- 第三方证书 61

磁带存储器

- 配置 93

[D]

第三方证书

- 创建证书签名请求 61

第三方证书 (续)

- 发送证书签名请求 62
- 接收签名证书 62
- 密钥库访问 59
- 配置 TLS 59

端口

- 安装 14

[F]

发送证书签名请求

- 第三方证书 62

服务 79

辅助功能选项 111

复原

- 配置日志记录 44
- 配置选项 43
- 文件 12, 43, 44, 45
- 先决条件 12
- 选项 43, 45

[G]

管理员特权

- Data Protection for VMware vSphere GUI 66

规划

- 必需的通信端口 14
- 概述 9
- 路线图 9
- 系统需求 10
- 许可权 14

[H]

恢复代理程序 GUI

- 配置 69
- 选项 69

恢复代理进程 5

[J]

键盘 111

接收签名证书

- 第三方证书 62

静默安装

- Linux 25
- Windows 64 位
 - 静默套件安装程序 24

静默升级

- Linux 29

静默升级 (续)

Windows 64 位 29

静默卸载

Linux

静默方式 33

Windows 64 位

静默方式 33

[K]

可安装组件 1

数据移动设备 7

文件复原 GUI 7

Data Protection for VMware 命令行界面 6

Data Protection for VMware vSphere GUI 2

IBM Spectrum Protect vSphere Client 插件 5

客户机接收器

配置 103

[M]

密钥库访问

第三方证书 59

[P]

配置

初始配置 39

磁带存储器 93

概述 39

高级任务 81

恢复代理程序 GUI 69

客户机接收器 103

启用标记支持 46

启用文件复原 41

数据移动设备节点

vSphere 环境 83, 84

文件复原

选项 43

现有配置 40

语言环境设置 76

装配代理节点

Linux 99

Windows 101

Data Protection for VMware 工作表 26

IBM Spectrum Protect 节点

vSphere 环境 82

iSCSI 装配 95, 97

SSL 57

TLS 通信 57

VMCLI

vSphere 环境 88

VMCLI 配置文件 105

vSphere 环境

命令行核对表 90

配置 (续)

Web 浏览器通信 57

配置笔记本 40

配置向导 39

配置 TLS

第三方证书 59

启用与服务器的安全通信 58, 73, 74, 75

认证中心 59

凭证

许可权 14

[Q]

启用与服务器的安全通信

配置 TLS 58, 73, 74, 75

迁移

调度 107

权限

许可权 14

[R]

日志记录

文件复原 44

软件需求 10

[S]

升级

从 V6.x

标准 28

概述 27

Linked Mode 30

Linux

静默 29

vCenter

Linked Mode 30

Windows 64 位

静默 29

数据移动设备 7

节点

在 vSphere 环境中配置 83, 84

[T]

通信端口

安装 14

[W]

文件复原

配置日志记录 44

配置选项 43

启用 41

文件复原 (续)
 先决条件 12
 选项 43, 45
 Linux 环境 42
文件复原 GUI 7

[X]

系统需求 10
卸载
 Linux
 典型 31
 静默方式 33
 Windows 64 位
 典型 31
 静默方式 33
修改
 概述 36
修改安装 36
许可权
 安装 14
 Data Protection for VMware vSphere GUI
 操作 66

[Y]

硬件需求 10
用户
 许可权 14
语言环境
 设置 76

[Z]

正在复原
 恢复代理进程 5
注册密钥 68
组件 1
 恢复代理进程 5
 可安装组件 19
 数据移动设备 7
 文件复原 GUI 7
 Data Protection for VMware 命令行界面 6
 Data Protection for VMware vSphere GUI 2
 IBM Spectrum Protect vSphere Client 插件 5

D

Data Protection for VMware
 规划 9
 可安装组件 1
 下载包 20
Data Protection for VMware 命令行界面 6
Data Protection for VMware V8.1.7 中的新增内容 vii
Data Protection for VMware vSphere GUI 2, 27

Data Protection for VMware vSphere GUI (续)
 许可权
 操作 66

G

GUI
 Data Protection for VMware vSphere GUI 27

I

IBM Knowledge Center v
IBM Spectrum Protect 节点
 配置
 vSphere 环境 82
IBM Spectrum Protect vSphere Client 插件 5
iSCSI 装配
 配置 95, 97

K

Knowledge Center v

L

Linux
 安装过程
 静默 25
 全新 23
 升级
 静默 29
 卸载
 典型 31
 静默方式 33

S

SSL
 配置 57, 58, 73, 74, 75

T

TLS 通信
 配置 57

V

VMCLI
 在 vSphere 环境中配置 88
VMCLI 配置文件
 修改 105
 vmcliConfiguration.xml 105
vSphere GUI 27

W

Windows 64 位

安装过程

静默套件安装程序 24

升级

静默 29

卸载

典型 31

静默方式 33



程序号: 5725-X00

Printed in China