



# Data Protector

软件版本：10.00

## 管理员指南

文档发行日期：2017 年 6 月  
软件发行日期：2017 年 6 月

## 法律声明

### 担保

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

本文所含信息如有更改，恕不另行通知。

### 受限权利说明

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

### 版权通知

© 版权所有 2017 Micro Focus or one of its affiliates

### 商标通知

Adobe™ 是 Adobe Systems Incorporated 的商标。

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

UNIX® 是 The Open Group 的注册商标。

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

## 文档更新

该文档的标题页面包含如下标识信息：

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

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

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

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

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

## 支持

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

该网站提供有关软件所提供的产品、服务和支持的联系信息和详细信息。

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

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

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

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

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

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

# 内容

- 第 1 章： 简介 ..... 1
  - 关于 Data Protector ..... 1
    - Data Protector 的主要功能 ..... 1
  - Data Protector 体系结构 ..... 1
    - Cell Manager ..... 1
    - 安装服务器 ..... 2
    - 客户机系统 ..... 2
      - 要备份的系统 ..... 2
      - 带备份设备的系统 ..... 2
  - 设置 Data Protector 的任务概述 ..... 2
    - 步骤 ..... 2
  - Data Protector 操作 ..... 4
    - 备份会话 ..... 4
    - 还原会话 ..... 4
    - pre-exec 和 post-exec 命令 ..... 4
    - 对象复制、对象合并和对象验证会话 ..... 4
  - 用户界面 ..... 4
    - 图形用户界面 ..... 4
    - 命令行界面 ..... 5
  - 自定义 GUI 中的语言设置 ..... 5
    - 先决条件 ..... 5
    - 限制 ..... 5
    - 步骤 ..... 5
  - 启动 Data Protector GUI ..... 6
  - 使用 Microsoft 管理控制台 (MMC) ..... 6
    - 步骤 ..... 6
  - 从 Data Protector GUI 启动 Storage Optimizer ..... 6
- 第 2 章： 配置任务 ..... 7
  - 系统安全性 ..... 7
    - 为安全通信配置证书 ..... 7
    - 从 GUI 连接到任何 Cell Manager/Jumpstation UI ..... 8
  - 用户安全性 ..... 9
    - 用户权限 ..... 9
      - “启动备份规范”用户权限 ..... 9
      - 隐藏备份规范的内容 ..... 9
      - 主机信任 ..... 10
    - 用户组 ..... 10
    - 用户限制 ..... 10

用户验证 .....	10
严格主机名检查 .....	10
限制 .....	11
要求 .....	11
主机名解析 .....	11
安全日志 .....	11
客户机安全性事件 .....	12
Cell Manager 安全事件 .....	12
配置主机信任 .....	12
步骤 .....	12
加密 .....	12
关于数据加密 .....	12
启用 AES 256 位加密 .....	13
先决条件 .....	13
限制 .....	13
在文件系统备份规范中启用加密 .....	13
步骤 .....	13
在磁盘映像备份规范中启用加密 .....	14
步骤 .....	14
在内部数据库备份规范中启用加密 .....	14
步骤 .....	14
在应用程序集备份规范中启用加密 .....	14
限制 .....	14
步骤 .....	14
导出和导入含有加密备份的介质 .....	15
没有 CMMDB 的 Cell Manager 环境或 MoM 环境 .....	15
步骤 .....	15
有 CMMDB 的 MoM 环境 .....	15
步骤 .....	15
启用基于驱动器的加密 .....	16
先决条件 .....	16
限制 .....	16
建议 .....	16
在驱动器配置中启用基于驱动器的加密 .....	16
步骤 .....	16
在备份规范中启用基于驱动器的加密 .....	16
步骤 .....	16
为自动介质操作启用基于驱动器的加密 .....	17
步骤 .....	17
用户验证和 LDAP 简介 .....	17
初始化并配置 LDAP 登录模块 .....	18
初始化 LDAP 登录模块 .....	18
配置 LDAP 登录模块 .....	20
向 LDAP 用户或组授予 Data Protector 权限 .....	22
将 LDAP 用户添加至 Data Protector 用户组 .....	22
将 LDAP 组添加至 Data Protector 用户组 .....	22

使用 LDAP 凭据登录 .....	23
检查 LDAP 配置 .....	23
防火墙支持 .....	23
关于防火墙支持 .....	23
Data Protector 中的通信 .....	24
配置机制 .....	25
Data Protector 9.09 及更高版本中的端口使用情况 .....	26
限制 .....	27
DMZ 中的磁盘代理、介质代理和应用程序代理 .....	27
配置图 .....	28
打开的端口 .....	28
限制 .....	29
 第 3 章： 用户和用户组 .....	31
关于用户管理 .....	31
用户 .....	31
UNIX .....	31
Windows .....	31
预定义用户 .....	31
用户组 .....	32
预定义用户组 .....	32
可用的用户权限 .....	33
向用户提供 Web 服务访问权限 .....	33
使用 Data Protector GUI .....	34
使用 CLI .....	34
配置用户 .....	34
添加用户 .....	34
先决条件 .....	34
步骤 .....	34
显示用户 .....	35
先决条件 .....	35
步骤 .....	35
更改用户属性 .....	35
先决条件 .....	35
步骤 .....	35
将用户移动到另一个用户组 .....	36
先决条件 .....	36
步骤 .....	36
删除用户 .....	36
先决条件 .....	36
步骤 .....	36
配置用户组 .....	37
添加用户组 .....	37

先决条件 .....	37
步骤 .....	37
显示用户组 .....	37
先决条件 .....	37
步骤 .....	37
更改用户权限 .....	38
先决条件 .....	38
步骤 .....	38
删除用户组 .....	38
先决条件 .....	38
步骤 .....	38
 第 4 章： 内部数据库 .....	 39
关于 IDB .....	39
IDB 的用途是什么？ .....	39
IDB 大小和增大注意事项 .....	39
定期备份 IDB .....	39
IDB 体系结构 .....	39
IDB 的各个部分 .....	40
介质管理数据库 (MMDB) .....	40
MMDB 记录 .....	40
MMDB 大小和增大 .....	41
MMDB 位置 .....	41
编目数据库 (CDB) .....	41
CDB 记录 .....	41
CDB(对象和位置)大小和增大 .....	41
CDB 位置 .....	41
详细编目二进制文件 (DCBF) .....	41
DCBF 信息 .....	41
DCBF 大小和增大 .....	42
DCBF 位置 .....	42
会话消息二进制文件 (SMBF) .....	42
SMBF 记录 .....	42
SMBF 大小和增大 .....	42
SMBF 位置 .....	43
加密密钥库和编目文件 .....	43
密钥库位置 .....	43
编目文件位置 .....	43
IDB 操作 .....	43
备份 .....	44
IDB 备份和归档日志文件 .....	44
恢复 .....	44
对象副本和对象合并 .....	44
对象验证 .....	44
导出介质 .....	45

删除详细编目 .....	45
配置内部数据库 .....	45
IDB 配置 .....	45
为 IDB 分配磁盘空间 .....	45
先决条件 .....	46
需要多少磁盘空间? .....	46
提前规划哪些内容? .....	46
IDB 目录的位置 .....	46
限制 .....	46
建议 IDB 目录所在的位置 .....	47
稳定性注意事项 .....	48
IDB 备份配置 .....	48
准备和运行 IDB 备份规范的提示 .....	48
维护内部数据库 .....	49
关于 IDB 维护 .....	49
内部数据库的增大及性能 .....	50
关于 IDB 增大和性能 .....	50
IDB 增大关键因素 .....	50
IDB 性能关键因素 .....	50
IDB 增大和性能关键参数 .....	51
日志记录级别对 IDB 的影响 .....	51
编目保护对 IDB 的影响 .....	51
IDB 大小估计 .....	52
DC 目录维护 .....	52
检查 IDB 大小 .....	53
步骤 .....	53
减小 IDB 增大 .....	53
降低日志记录级别 .....	53
步骤 .....	53
降低编目保护 .....	54
步骤 .....	54
减小 IDB 当前大小 .....	54
更改对会话的编目保护 .....	54
步骤 .....	55
更改对于对象的编目保护 .....	55
步骤 .....	55
扩展 IDB 大小 .....	55
重新配置 DC 目录以获得更大容量 .....	55
步骤 .....	55
IDB 一致性检查 .....	55
将 IDB 移至不同的 Cell Manager .....	56
步骤 .....	56
步骤 .....	57
自定义 Data Protector 全局选项 .....	58
先决条件 .....	58
使用 GUI 设置全局选项 .....	58



步骤 .....	58
通过编辑全局文件自定义选项 .....	59
步骤 .....	59
配置 IDB 报告 .....	59
IDB 报告 .....	59
配置 IDB 通知 .....	59
IDB 通知 .....	59
还原 IDB .....	60
还原 IDB .....	60
先决条件 .....	60
限制 .....	60
步骤 .....	60
从加密备份准备 IDB 还原 .....	61
步骤 .....	61
关于 IDB 恢复 .....	61
完整恢复(自上次 IDB 备份以来还原和更新 IDB) .....	62
IDB 恢复方法的概述 .....	62
最方便的完整恢复 .....	62
省略(删除)损坏的 IDB 部分 .....	62
更多恢复方法 .....	63
IDB 损坏级别 .....	63
确认 IDB 损坏的级别 .....	64
步骤 .....	64
执行指导下的自动恢复(还原 IDB 和重放存档的日志文件) .....	64
先决条件 .....	64
步骤 .....	65
处理 IDB DCBF 部分中的 Minor 损坏 .....	65
在 DC 二进制文件丢失的情况下进行恢复 .....	65
步骤 .....	65
在 DC 二进制文件损坏的情况下进行恢复 .....	66
步骤 .....	66
使用 IDB 恢复文件和更改的设备还原 IDB .....	66
先决条件 .....	66
步骤 .....	67
在无 IDB 恢复文件的情况下还原 IDB .....	67
先决条件 .....	67
步骤 .....	68
从特定的 IDB 会话中还原 IDB .....	69
先决条件 .....	69
步骤 .....	69
在其他 Cell Manager 主机上还原 IDB 数据库。 .....	70
通过导入介质更新 IDB .....	71
步骤 .....	71

第 5 章： Manager-of-Managers 环境 .....	73
-------------------------------------	----

关于 MoM 环境 .....	73
关于 CMMDB .....	73
如何共享介质 .....	73
如何初始化介质 .....	73
MoM 环境配置过程 .....	74
先决条件 .....	74
MoM 环境配置过程 .....	74
设置 MoM Manager .....	74
步骤 .....	74
向单元添加 MoM 管理员 .....	75
先决条件 .....	75
步骤 .....	75
导入单元 .....	75
先决条件 .....	75
步骤 .....	75
在 MoM 中重新启动 Data Protector 服务 .....	75
停止 Data Protector 服务 .....	75
非群集环境中的 Cell Manager .....	75
Serviceguard 上的 Cell Manager .....	76
Symantec Veritas Cluster Server 上的 Cell Manager .....	76
Microsoft 群集服务器上的 Cell Manager .....	76
启动 Data Protector 服务 .....	76
非群集环境中的 Cell Manager .....	76
Serviceguard 上的 Cell Manager .....	76
Symantec Veritas Cluster Server 上的 Cell Manager .....	76
Microsoft 群集服务器上的 Cell Manager .....	76
配置 CMMDB .....	76
注意事项 .....	77
先决条件 .....	77
在客户机单元上配置 CMMDB .....	77
步骤 .....	77
在 MoM Manager 上配置 CMMDB .....	78
步骤 .....	78
关于集中式许可 .....	78
设置集中式许可 .....	78
先决条件 .....	78
步骤 .....	78
停用集中式许可 .....	79
步骤 .....	79
关于 MoM 环境管理 .....	80
导出单元 .....	80
步骤 .....	80
在单元之间移动客户机系统 .....	81
步骤 .....	81
停用集中式许可 .....	81
先决条件 .....	81

步骤 .....	81
配置 <b>Data Protector</b> 用户 .....	81
步骤 .....	82
将用户添加到其他单元 .....	82
步骤 .....	82
从单元删除用户 .....	82
步骤 .....	82
管理特定单元的设备 and 介质 .....	82
步骤 .....	83
管理特定单元的内部数据库 .....	83
步骤 .....	83
 第 6 章： 群集 .....	 84
关于群集 .....	84
关于 <b>Data Protector Microsoft</b> 群集服务器集成 .....	84
许可和 <b>MSCS</b> .....	84
配置 .....	84
如何管理群集感知备份 .....	84
<b>Data Protector</b> 的故障转移 .....	85
<b>Data Protector</b> 之外应用程序的故障转移 .....	85
关于 <b>Microsoft</b> 群集服务器的灾难恢复 .....	85
可能出现的场景 .....	86
关于 <b>Data Protector Serviceguard</b> 集成 .....	86
许可和 <b>Serviceguard</b> .....	86
配置 .....	86
关于 <b>Data Protector HACMP</b> 群集集成 .....	86
节点 .....	88
共享外部磁盘接口 .....	88
网络 .....	88
客户机 .....	88
任务 .....	88
 第 7 章： 主页上下文 .....	 89
仪表板 .....	89
遥测 .....	91
遥测的工作原理？ .....	91
计划程序 .....	92
从早期版本迁移计划 .....	93
计划选项 .....	94
节假日期间的计划排除 .....	94
使用预定义计划 .....	95
处理计划冲突 .....	95
在不同时区进行计划 .....	95
划分计划优先级 .....	95

限制 .....	96
计划程序用户界面 .....	96
计划程序任务 .....	98
创建计划 .....	98
编辑现有计划 .....	101
查看计划 .....	103
禁用和启用计划 .....	105
步骤 .....	105
在节假日禁用和启用计划 .....	105
步骤 .....	105
在特定日期和时间设置计划 .....	106
步骤 .....	106
定期设置计划 .....	106
使用预定义备份日程安排 .....	106
步骤 .....	106
配置重复计划 .....	107
步骤 .....	107
计划提示 .....	108
 第 8 章： 设备 .....	 109
关于备份设备 .....	109
什么是备份设备？ .....	109
关于配置备份设备 .....	109
备份设备的类型 .....	109
独立 .....	110
备份到磁盘设备 .....	110
SCSI 库 .....	110
堆栈器 .....	111
箱盒设备 .....	111
介质库 .....	112
独立文件设备 .....	112
文件库设备 .....	112
外部控制 .....	112
ADIC/GRAU DAS 库 .....	112
StorageTek ACS 库 .....	113
关于 StoreOnce 软件重复数据删除组件 .....	115
安装 .....	115
先决条件 .....	115
防火墙配置 .....	115
安装过程 .....	115
StoreOnce 软件重复数据删除的其他步骤 .....	115
远程安装 Data Protector StoreOnce 软件重复数据删除组件 .....	115
本地安装 Data Protector StoreOnce 软件重复数据删除组件 .....	116
设置 StoreOnce 软件服务/后台程序 .....	116
安装的目录结构 .....	116

故障排除 .....	117
磁盘空间不足警告 .....	117
system.db 文件的备份 .....	117
关于 StoreOnce 存储区和 DD Boost 重复数据删除设备 .....	120
多接口支持 .....	120
源端重复数据删除 .....	121
添加 B2D 设备 .....	122
备份 .....	122
还原 .....	124
源端重复数据删除注意事项 .....	125
基于光纤通道的 Catalyst 的 StoreOnce Catalyst 客户机配置 .....	125
Windows 客户机 .....	125
Linux 客户机 .....	126
AIX 客户机 .....	126
HP-UX 客户机 .....	126
Solaris 客户机 .....	127
与 B2D 设备相关的 omnirc 选项 .....	127
关于云 (Helion) 设备 .....	129
先决条件 .....	129
限制 .....	130
建议 .....	130
准备云 (Helion) 设备 .....	130
关于云 (Azure) 设备 .....	131
先决条件 .....	131
限制 .....	132
建议 .....	132
准备云 (Azure) 设备 .....	132
设备性能优化 .....	133
块大小 .....	133
确定最佳的块大小 .....	133
限制 .....	134
更改块大小 .....	134
设备性能 .....	134
支持新设备 .....	134
准备备份设备 .....	135
先决条件 .....	135
步骤 .....	135
在 SAN 环境中 .....	136
步骤 .....	136
文件设备 .....	136
步骤 .....	136
箱盒 .....	136
步骤 .....	136
SCSI 库、介质库、外部控制 .....	137

步骤 .....	137
Windows 机械手驱动程序 .....	137
步骤 .....	137
在 Windows 系统中创建 SCSI 地址 .....	137
磁光设备 .....	137
磁带设备 .....	137
无本机磁带驱动程序的 Windows .....	138
使用本机磁带驱动程序的 Windows .....	138
步骤 .....	138
在 UNIX 系统中查找设备文件名 .....	138
查找 HP-UX 中的设备文件名 .....	138
先决条件 .....	138
步骤 .....	138
查找 Solaris 中的设备文件名 .....	139
步骤 .....	139
在 UNIX 系统中创建设备文件 .....	139
在 HP-UX 系统中创建设备文件 .....	139
先决条件 .....	139
步骤 .....	139
在 Solaris 系统中创建设备文件 .....	140
先决条件 .....	140
步骤 .....	140
自动检测设备文件名和 SCSI 地址 .....	141
对于现有的 Data Protector 设备定义 .....	141
步骤 .....	141
创建 Data Protector 设备定义时 .....	141
步骤 .....	141
自动检测库的设备文件名和 SCSI 地址 .....	141
对于已配置的库 .....	141
步骤 .....	141
配置库时 .....	142
步骤 .....	142
关于配置备份设备 .....	142
关于库管理控制台 .....	142
什么是库管理控制台? .....	142
Data Protector 中对库管理控制台的支持 .....	142
限制 .....	143
自动配置备份设备 .....	143
先决条件 .....	143
设备自动配置 .....	143
步骤 .....	143
SAN 环境中的设备自动配置 .....	144
限制 .....	144
步骤 .....	144
配置独立设备 .....	145
步骤 .....	145

配置备份到磁盘设备 .....	145
多接口支持 .....	146
步骤 .....	146
配置备份到磁盘设备 - StoreOnce .....	146
步骤 .....	147
为存储刷新缓存 .....	148
使用 Data Protector GUI 刷新缓存 .....	149
使用 Data Protector CLI 刷新缓存 .....	149
配置备份到磁盘设备 - StoreOnce 软件 .....	149
配置重复数据删除存储的根目录 .....	149
创建存储 .....	151
配置备份到磁盘设备 - 数据域提升 .....	151
先决条件 .....	151
限制 .....	152
步骤 .....	152
在 AIX 系统上配置数据域提升 .....	153
步骤 .....	153
配置备份到磁盘设备 - 智能缓存 .....	153
配置智能缓存 .....	153
先决条件 .....	153
限制 .....	154
步骤 .....	155
配置云 (Helion) 设备 .....	155
获取 HPE 公共云项目名称 .....	155
步骤 .....	155
获取身份验证服务 URL .....	156
步骤 .....	156
创建访问密钥 .....	156
步骤 .....	156
配置备份到磁盘设备 - 云 (Helion) .....	157
步骤 .....	157
配置备份到磁盘设备 - 云 (Azure) .....	158
步骤 .....	158
配置文件库设备 .....	158
先决条件 .....	158
限制 .....	158
步骤 .....	159
关于配置设备的多个路径 .....	159
为何使用多条路径 .....	160
路径选择 .....	160
向后兼容 .....	161
限制 .....	161
设置设备和介质的高级选项 .....	161
步骤 .....	161
配置 VTL 设备 .....	162
步骤 .....	162

配置堆栈器设备 .....	162
步骤 .....	162
堆栈器设备介质管理 .....	163
配置介质库设备(光盘库) .....	163
配置介质库设备 .....	163
步骤 .....	163
配置介质库设备中的驱动器 .....	164
步骤 .....	164
配置 SCSI 库或箱盒设备 .....	164
配置 SCSI 库机械手 .....	164
步骤 .....	164
配置库中的驱动器 .....	165
步骤 .....	165
配置 SAN 环境中的设备 .....	166
注意事项 .....	166
配置方法 .....	166
使用 GUI 自动配置设备 .....	166
限制 .....	166
使用 CLI 自动配置设备(sanconf 命令) .....	167
设备锁定 .....	167
限制 .....	168
建议 .....	168
在 UNIX 系统中手动配置 .....	168
阶段 .....	168
手动配置 SAN 环境中的设备 .....	168
先决条件 .....	169
配置阶段 .....	169
配置 SAN 环境中的库 .....	169
步骤 .....	169
配置库中的驱动器 .....	170
步骤 .....	170
配置 SAN 环境中的 libtab 文件 .....	171
步骤 .....	171
配置 ADIC/GRAU DAS 库设备 .....	171
配置阶段 .....	172
连接库驱动器 .....	172
步骤 .....	172
准备安装介质代理 .....	172
步骤 .....	172
安装介质代理 .....	173
先决条件 .....	173
步骤 .....	174
配置 ADIC/GRAU DAS 库设备 .....	174
步骤 .....	175
配置 ADIC/GRAU DAS 库设备中的驱动器 .....	175
步骤 .....	175



配置 StorageTek ACS 库设备 .....	176
配置阶段 .....	176
连接库驱动器 .....	176
步骤 .....	176
安装介质代理 .....	176
先决条件 .....	177
步骤 .....	177
配置 StorageTek ACS 库设备 .....	178
步骤 .....	178
配置 StorageTek ACS 库设备中的驱动器 .....	179
步骤 .....	179
关于使用备份设备 .....	179
设备和介质的高级选项 .....	179
高级选项 - 设置 .....	180
选项 .....	180
高级选项 - 大小 .....	180
高级选项 - 其他 .....	180
装载请求 .....	180
设备锁名称 .....	180
有多种驱动器类型的库 .....	180
相同的密度设置 .....	180
每个驱动器类型都有不同的介质池 .....	181
自由池支持 .....	181
关于扫描 .....	181
何时使用扫描 .....	181
限制 .....	182
驱动器清洗 .....	182
限制 .....	182
自动清洗的条件 .....	183
计划的介质弹出 .....	183
设备锁定 .....	183
禁用备份设备 .....	184
手动禁用备份设备 .....	184
步骤 .....	184
自动禁用备份设备 .....	184
重命名备份设备 .....	185
步骤 .....	185
删除备份设备 .....	185
步骤 .....	185
响应装载请求 .....	185
先决条件 .....	185
步骤 .....	186
关于存储区域网络 (SAN) .....	186
什么是 SAN? .....	186
FC-AL 和 LIP .....	186
SAN 环境中的设备锁定 .....	187

锁定 <b>Data Protector</b> 专用的设备 .....	187
锁定由多个应用程序使用的设备 .....	187
间接和直接库访问 .....	188
间接库访问 .....	188
直接库访问 .....	188
配置 <b>SAN</b> 环境中的设备 .....	188
注意事项 .....	189
配置方法 .....	189
使用 <b>GUI</b> 自动配置设备 .....	189
限制 .....	189
使用 <b>CLI</b> 自动配置设备 ( <b>sanconf</b> 命令) .....	189
设备锁定 .....	190
限制 .....	190
建议 .....	190
在 <b>UNIX</b> 系统中手动配置 .....	191
阶段 .....	191
关于备份到磁盘 .....	191
什么是基于磁盘的备份设备? .....	191
如何配置基于磁盘的设备? .....	191
关于备份到磁盘设备 .....	191
关于重复数据删除 .....	192
何时使用重复数据删除功能 .....	193
重复数据删除功能的优点 .....	193
重复数据删除技术 .....	193
<b>StoreOnce</b> 软件重复数据删除 .....	193
<b>StoreOnce</b> 备份系统设备 .....	193
重复数据删除设置 .....	193
源端重复数据删除 .....	194
服务器端重复数据删除 .....	194
目标端重复数据删除 .....	194
关于文件库设备 .....	194
如何维护基于磁盘的设备? .....	195
文件仓库 .....	195
创建文件仓库 .....	195
文件仓库名称 .....	195
文件仓库大小 .....	195
文件仓库空间消耗 .....	196
磁盘已满处理 .....	196
每个磁盘的设备数 .....	196
设置文件库设备属性 .....	196
属性初始设置 .....	196
步骤 .....	196
更改设备属性 .....	196
步骤 .....	196
删除文件库设备 .....	197
删除阶段 .....	197

检查数据保护 .....	197
步骤 .....	197
回收文件仓库 .....	197
步骤 .....	197
删除导出的文件仓库图标 .....	197
步骤 .....	198
删除文件库设备 .....	198
步骤 .....	198
关于介质库设备 .....	198
介质库物理设备 .....	198
介质库文件设备 .....	198
建议对于 <b>Windows</b> 和 <b>UNIX</b> 采用的插槽大小 .....	199
如何维护文件介质库设备？ .....	199
配置文件介质库设备 .....	199
配置文件介质库设备 .....	199
先决条件 .....	199
步骤 .....	199
配置文件介质库设备中的驱动器 .....	200
步骤 .....	200
回收文件介质库插槽 .....	200
步骤 .....	200
关于独立设备 .....	201
独立物理设备 .....	201
独立文件设备 .....	201
配置独立文件设备 .....	201
先决条件 .....	202
步骤 .....	202
 第 9 章： 介质 .....	203
关于介质管理 .....	203
自定义设备和介质视图 .....	203
关于介质池 .....	203
自由池 .....	203
默认介质池 .....	204
自由池特征 .....	204
自由池属性 .....	204
何时使用自由池？ .....	204
介质质量计算 .....	204
自由池限制 .....	204
介质池属性 .....	205
介质池属性 - 常规 .....	205
介质池属性 - 分配 .....	205
分配 .....	205
介质池属性 - 状况 .....	205
介质状态因素 .....	205

介质池属性 - 使用 .....	206
介质池质量 .....	206
设备错误和介质质量 .....	206
创建介质池 .....	206
步骤 .....	206
修改介质池 .....	207
步骤 .....	207
删除介质池 .....	207
步骤 .....	208
介质生命周期 .....	208
准备备份用介质 .....	208
使用备份用介质 .....	208
将介质保管到安全位置 .....	208
报废介质 .....	209
介质类型 .....	209
支持的介质类型 .....	209
介质质量 .....	209
设备错误和介质质量 .....	209
如何为备份选择介质 .....	209
介质分配策略 .....	210
预分配介质 .....	210
介质状态 .....	210
介质使用 .....	210
限制 .....	210
介质选择因素 .....	211
使用不同的介质格式类型 .....	211
限制 .....	211
WORM 介质 .....	211
如何将 WORM 介质用于 Data Protector .....	212
所支持的 WORM 介质 .....	212
关于格式化介质 .....	212
用填充块进行格式化 .....	212
何时格式化介质 .....	212
介质标签 .....	213
识别介质格式 .....	213
Data Protector 介质格式类别 .....	213
格式化介质 .....	214
步骤 .....	214
格式化箱盒中的所有介质 .....	214
先决条件 .....	214
步骤 .....	214
格式化箱盒中的单个介质 .....	215
先决条件 .....	215
步骤 .....	215
格式化带库设备中的介质 .....	215
步骤 .....	215

关于导入介质 .....	216
注意事项 .....	216
何时导入介质? .....	216
导入介质 .....	216
步骤 .....	216
导入箱盒中的所有介质 .....	217
先决条件 .....	217
步骤 .....	217
导入箱盒中的单个介质 .....	217
先决条件 .....	217
步骤 .....	217
导入带库设备中的介质 .....	218
步骤 .....	218
导出和导入含有加密备份的介质 .....	218
没有 CMMDB 的 Cell Manager 环境或 MoM 环境 .....	218
步骤 .....	218
有 CMMDB 的 MoM 环境 .....	219
步骤 .....	219
关于介质复制 .....	219
先决条件 .....	219
限制 .....	219
何时复制介质 .....	220
复制介质的结果 .....	220
从副本还原 .....	220
复制介质 .....	220
在独立设备中复制介质 .....	220
步骤 .....	220
在带库设备中复制介质 .....	221
自动介质复制 .....	221
限制 .....	221
自动介质复制 .....	221
自动介质复制的类型 .....	222
备份后介质复制 .....	222
计划的介质复制 .....	222
配置备份后介质复制 .....	222
限制 .....	222
步骤 .....	223
配置计划的介质复制 .....	223
限制 .....	223
步骤 .....	223
扫描设备 .....	224
步骤 .....	224
扫描带库设备中的介质 .....	224
步骤 .....	224
扫描带库设备中的驱动器 .....	224
步骤 .....	224

激活条码读取器支持 .....	225
步骤 .....	225
扫描带库设备的条码 .....	225
先决条件 .....	225
步骤 .....	225
搜索和选择介质 .....	226
在介质池中搜索和选择介质 .....	226
步骤 .....	226
在库设备中搜索和选择介质 .....	226
步骤 .....	226
使用“介质列表”报告搜索介质 .....	226
步骤 .....	226
备份用介质的预分配列表 .....	226
预先分配备份用介质 .....	227
步骤 .....	227
回收介质 .....	227
步骤 .....	228
从介质导入目录 .....	228
步骤 .....	228
验证介质 .....	228
在独立设备中验证介质 .....	229
步骤 .....	229
在带库设备中验证介质 .....	229
步骤 .....	229
移动介质 .....	229
步骤 .....	229
导出介质 .....	230
步骤 .....	230
将目录介质数据复制到 MCF 文件中 .....	230
限制 .....	230
建议 .....	231
步骤 .....	231
从 MCF 文件导入目录介质数据 .....	231
先决条件 .....	231
限制 .....	231
步骤 .....	232
修改介质说明 .....	232
步骤 .....	232
修改介质位置 .....	232
步骤 .....	232
创建位置列表 .....	233
步骤 .....	233
设置介质位置优先级 .....	233
步骤 .....	233
保管介质 .....	234
先决条件 .....	234

步骤 .....	234
擦除介质 .....	234
步骤 .....	234
检测写保护介质 .....	234
关于装载请求 .....	235
关于带库特有的介质管理 .....	235
其他应用程序使用带库介质 .....	235
关于用于 ADIC/GRAU DAS 或 STK ACS 库的 Data Protector 查询操作 .....	236
添加插槽 .....	236
步骤 .....	236
删除插槽 .....	237
步骤 .....	237
放入介质 .....	237
步骤 .....	237
弹出介质 .....	237
批量弹出介质 .....	238
预定义介质弹出 .....	238
步骤 .....	238
擦除带库设备中的介质 .....	238
步骤 .....	238
手动添加 Volser .....	239
步骤 .....	239
查询 ADIC/GRAU DAS 和 StorageTek ACSLM 主机 .....	239
限制 .....	239
步骤 .....	239
 第 10 章： 备份 .....	 240
关于备份 .....	240
设置备份视图 .....	240
步骤 .....	240
备份类型 .....	240
完整备份 .....	241
增量备份 .....	241
增量备份的类型 .....	241
高级备份解决方案 .....	241
完整备份和增量备份 .....	241
传统增量备份 .....	242
传统增量备份的工作方式 .....	242
检测更改 .....	242
增强型增量备份 .....	243
为什么使用增强型增量备份 .....	243
对磁盘空间消耗的影响 .....	243
限制 .....	244
使用更改日志提供程序的增量备份 .....	244
先决条件 .....	244

性能损失和磁盘空间消耗 .....	245
注意事项 .....	245
限制 .....	246
合成备份 .....	246
如何执行合成备份 .....	246
虚拟完整备份 .....	246
标准备份过程 .....	246
先决条件 .....	247
文件系统备份 .....	247
创建备份规范 .....	247
限制 .....	247
步骤 .....	248
修改备份规范 .....	249
步骤 .....	249
预览和启动备份 .....	249
限制 .....	249
步骤 .....	249
中止备份 .....	250
步骤 .....	250
重新启动失败的备份 .....	250
先决条件 .....	250
注意事项 .....	250
限制 .....	250
步骤 .....	251
复制备份规范 .....	251
步骤 .....	251
删除备份规范 .....	251
步骤 .....	251
高级备份任务 .....	252
先决条件 .....	252
什么是高级备份任务? .....	252
选择网络共享磁盘进行备份 .....	252
先决条件 .....	253
Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012 .....	253
要求 .....	253
限制 .....	253
步骤 .....	253
仅选择特定文件(匹配)进行备份 .....	254
步骤 .....	255
使文件跳过备份 .....	255
步骤 .....	255
选择启动备份的快捷方式位置 .....	255
限制 .....	255
步骤 .....	256
使用多个磁带客户机进行备份 .....	256



步骤 .....	256
处理重复进行的小规模备份 .....	257
磁盘映像备份 .....	257
何时使用磁盘映像备份? .....	257
如何指定磁盘映像的某个部分? .....	258
在 UNIX 系统中 .....	258
在 Windows 系统中 .....	258
从何处查找磁盘映像的某个部分? .....	258
在 UNIX 系统中 .....	258
在 Windows 系统中 .....	258
执行磁盘发现的客户机备份 .....	259
何时使用磁盘发现 .....	260
备份规范 .....	260
Web 服务器备份 .....	260
启用网络唤醒支持 .....	260
步骤 .....	261
关于备份模板 .....	261
创建新备份模板 .....	262
步骤 .....	262
修改备份模板 .....	262
步骤 .....	263
复制备份模板 .....	263
步骤 .....	263
删除备份模板 .....	263
步骤 .....	263
将备份模板应用于备份规范 .....	263
步骤 .....	264
关于备份选项 .....	264
可用的备份选项 .....	265
备份规范选项 .....	265
文件系统选项 .....	265
磁盘映像选项 .....	265
设备选项 .....	265
计划选项 .....	266
最常用的选项 .....	266
交互式备份 .....	266
使用已保存的备份规范进行备份 .....	266
计划的备份 .....	266
到期的编目保护 .....	267
编目保护和备份 .....	267
编目保护和还原 .....	267
日志记录级别和备份速度 .....	267
日志记录级别和浏览还原 .....	268
日志记录级别和还原速度 .....	268
谁是备份会话的所有者? .....	269
为什么更改备份所有者? .....	269

谁可以还原私有对象？ .....	269
备份规范选项 .....	269
常规备份规范选项 .....	270
群集备份规范选项 .....	270
会话自动重新启动 .....	270
中止会话和中止 ID 参数 .....	270
EMC Symmetrix 备份规范选项 .....	270
客户机系统 .....	270
镜像类型 .....	271
EMC Symmetrix 拆分 pre-exec 和 post-exec .....	271
EMC Symmetrix 选项 .....	271
P9000 XP 磁盘阵列系列 备份规范选项 .....	271
客户机系统 .....	271
镜像类型 .....	271
复本管理选项 .....	271
在会话开始时 .....	271
在会话结束时 .....	272
应用程序系统选项 .....	272
备份系统选项 .....	272
P6000 EVA 磁盘阵列系列 备份规范选项 .....	272
客户机系统 .....	272
复制模式 .....	272
故障转移情况下的复本处理 .....	272
快照管理选项 .....	272
镜像克隆准备/同步 .....	273
复本管理选项 .....	273
应用程序系统选项 .....	273
备份系统选项 .....	273
文件系统选项 .....	273
文件系统选项 .....	273
其他文件系统选项 .....	274
WinFS 文件系统选项 .....	274
磁盘映像选项 .....	275
设备选项 .....	275
设备属性 - 常规 .....	275
计划选项 .....	276
会话选项 .....	276
分割镜像/快照备份 .....	276
设置备份选项 .....	276
步骤 .....	277
指定数据保护 .....	277
指定备份规范级别的数据保护 .....	277
步骤 .....	277
指定单独备份对象的数据保护 .....	277
步骤 .....	278
指定计划备份的数据保护 .....	278

使用 CLI 指定数据保护 .....	278
步骤 .....	278
更改特定对象的选项 .....	278
步骤 .....	278
更改备份设备选项 .....	279
步骤 .....	279
设置计划备份选项 .....	280
关于 pre-exec 和 post-exec 命令 .....	280
什么是 pre-exec 和 post-exec 命令? .....	280
配置备份的 pre-exec 和 post-exec 命令 .....	280
备份规范 .....	280
备份对象 .....	280
pre-exec 和 post-exec 命令如何运行? .....	281
备份规范的 pre-exec 和 post-exec 命令 .....	281
pre-exec 和 post-exec 特征 .....	281
命令的启动和位置以确保安全性 .....	281
Windows 系统 .....	281
UNIX 系统 .....	282
环境变量 .....	282
SMEXIT 值 .....	282
pre-exec 和 post-exec 命令的注意事项 .....	282
指定备份规范的 pre-exec 和 post-exec 命令 .....	283
特定备份对象的 pre-exec 和 post-exec 命令 .....	284
命令的启动和位置 .....	284
环境变量 .....	284
pre-exec 和 post-exec 命令的注意事项 .....	285
安全注意事项 .....	285
指定备份对象的 pre-exec 和 post-exec 命令 .....	286
指定所有对象的 pre-exec 和 post-exec 命令 .....	286
指定单独对象的 pre-exec 和 post-exec 命令 .....	286
指定集成的 pre-exec 和 post-exec 命令 .....	286
关于备份计划 .....	287
运行连续备份 .....	287
步骤 .....	287
关于备份规范组 .....	287
备份规范组的示例 .....	288
查看备份规范组 .....	288
步骤 .....	288
创建备份规范组 .....	288
步骤 .....	288
将备份规范保存到组中 .....	289
步骤 .....	289
在各个组之间移动备份规范或模板 .....	289
步骤 .....	289
删除备份规范组 .....	289
步骤 .....	290

关于 Windows 系统备份 .....	290
限制 .....	290
备份什么? .....	290
Windows Server 2012 .....	290
Windows 特有信息 .....	290
不备份什么? .....	291
Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012: .....	291
Windows Server 2012 .....	291
其他 Windows 系统 .....	291
NTFS 3.1 文件系统功能 .....	291
重分析点 .....	292
稀疏文件 .....	292
备份系统磁盘时发出警告 .....	292
配置备份 (Windows) .....	293
限制 .....	293
Windows 配置对象 .....	293
Active Directory .....	294
DFS .....	294
DHCP 和 WINS .....	294
配置文件 .....	294
可移动存储管理器数据库 .....	295
终端服务数据库 .....	295
Windows 服务 .....	295
系统状态数据备份 .....	295
远程存储服务 .....	296
远程存储服务: .....	296
远程存储数据库: .....	296
可移动存储管理器数据库 .....	296
系统文件保护 .....	296
关于 UNIX 系统备份 .....	296
限制 .....	297
备份什么? .....	297
应当从 UNIX 文件系统备份中排除什么? .....	297
NFS 备份 .....	297
何时使用 NFS 备份? .....	297
限制 .....	298
先决条件 .....	298
限制 .....	298
备份什么? .....	299
关于 Novell Open Enterprise Server (OES) 备份 .....	299
先决条件 .....	299
限制 .....	300
备份和还原压缩文件 .....	300
备份什么? .....	300
配置 Novell OES .....	300

使用 HPLOGIN 实用程序保存用户名和密码 .....	300
步骤 .....	300
以双模式加载 Target Service Agent for File Systems (tsafs) .....	300
步骤 .....	300
加载 Target Service Agent for Novell Directory Services (tsands) .....	301
步骤 .....	301
加载 GroupWise Target Service Agent for File Systems (tsafsgw) .....	301
步骤 .....	301
关于备份性能 .....	302
基础架构 .....	302
对象镜像和备份性能 .....	302
设备之外的高性能硬件 .....	303
硬件并行性 .....	303
并发 .....	303
对性能的影响 .....	303
多个数据流 .....	303
设备流式传送 .....	304
如何配置设备流式传送 .....	304
块大小 .....	304
段大小 .....	305
磁盘代理缓冲区的数量 .....	305
软件压缩 .....	305
硬件压缩 .....	306
磁盘映像与文件系统备份 .....	306
将对象分散到多个介质上 .....	307
文件系统扫描 .....	307
其他性能提示 .....	307
 第 11 章：对象合并 .....	 309
关于对象合并 .....	309
对象合并的类型 .....	309
备份后对象合并 .....	309
计划的对象合并 .....	309
如何合并对象 .....	309
设备的选择 .....	309
对象合并选项 .....	309
介质集的选择 .....	310
合并对象的所有权 .....	310
标准对象合并任务 .....	310
先决条件 .....	310
限制 .....	310
以交互方式合并对象 .....	311
步骤 .....	311
配置备份后对象合并 .....	312

- 步骤 ..... 312
- 计划对象合并 ..... 312
  - 步骤 ..... 312
- 复制对象合并规范 ..... 313
  - 步骤 ..... 313
- 第 12 章： 复制 ..... 314**
  - 关于复制备份数据 ..... 314
    - 关于对象复制 ..... 315
      - 什么是对象复制？ ..... 315
      - 自动对象复制 ..... 315
        - 备份后对象复制 ..... 316
        - 计划的对象复制 ..... 316
    - 如何复制对象 ..... 316
      - 设备的选择 ..... 316
      - 对象副本选项 ..... 316
      - 选择从中进行复制的介质集 ..... 317
      - 对象副本完成状态 ..... 317
        - 复制对象 ..... 317
        - 源对象 ..... 317
      - 对象副本所有权 ..... 317
    - 标准对象复制任务 ..... 317
      - 先决条件 ..... 317
      - 限制 ..... 318
    - 以交互方式复制对象 ..... 318
      - 步骤 ..... 318
    - 配置备份后对象复制 ..... 319
      - 步骤 ..... 320
    - 安排对象复制 ..... 320
      - 步骤 ..... 320
    - 重新启动失败的对象复制会话 ..... 321
      - 先决条件 ..... 321
      - 限制 ..... 321
      - 步骤 ..... 321
    - 复制对象复制规范 ..... 321
      - 步骤 ..... 322
    - 高级对象复制任务 ..... 322
    - 释放介质 ..... 322
      - 步骤 ..... 322
    - 取消介质的多路复用 ..... 323
      - 限制 ..... 323
      - 步骤 ..... 323
    - 合并还原链 ..... 324
      - 限制 ..... 324
      - 步骤 ..... 324

迁移到其他介质类型 .....	325
步骤 .....	325
关于磁盘暂存 .....	326
什么是磁盘分段？ .....	326
为什么要实施磁盘分段 .....	326
磁盘分段和重复进行的小型备份 .....	326
对象操作会话故障排除 .....	326
对象副本问题 .....	326
复制的对象比预期的少 .....	326
未复制所选库中的全部对象 .....	327
发出了装载其他介质的请求 .....	327
当创建对象副本时，保护结束时间会延长 .....	327
复制包含多个对象的会话时会话停止响应 .....	328
数据域提升设备上的复制会话无法在重试期间响应中止操作 .....	328
对象整合问题 .....	328
许多时间点的对象整合打开太多的文件 .....	328
第二次尝试对象合并至 B2D 设备失败 .....	329
关于复制 .....	329
自动复制 .....	330
备份后复制 .....	330
安排的复制 .....	330
限制 .....	330
注意事项 .....	330
如何启用复制 .....	331
自动复制同步 .....	331
先决条件 .....	331
注意事项 .....	331
限制 .....	331
导入外部 Cell Manager .....	332
执行对象复制会话 .....	332
关于对象镜像 .....	333
对象镜像的优点 .....	333
限制 .....	333
如何使用对象镜像 .....	333
复制介质 .....	334
在独立设备中复制介质 .....	334
步骤 .....	334
在带库设备中复制介质 .....	334
 第 13 章：对象验证 .....	 336
关于对象验证 .....	336
数据验证 .....	336
传递到主机 .....	336
对象验证会话的类型 .....	336
备份后对象验证 .....	336

计划的对象验证 .....	336
如何验证对象 .....	336
备份对象的选择 .....	337
自动操作 .....	337
交互式操作 .....	337
源设备的选择 .....	337
目标主机的选择 .....	337
安排 .....	337
标准对象验证任务 .....	337
先决条件 .....	338
限制 .....	338
以交互方式验证对象 .....	338
步骤 .....	338
配置备份后对象验证 .....	339
步骤 .....	339
配置计划对象验证 .....	340
步骤 .....	340
自定义对象验证环境 .....	341
 第 14 章： 还原 .....	 342
关于还原 .....	342
标准还原过程 .....	342
先决条件 .....	342
选择要还原的数据 .....	342
先决条件 .....	342
从备份对象列表选择数据 .....	343
步骤 .....	343
从备份会话列表选择数据 .....	343
限制 .....	343
步骤 .....	343
选择特定备份版本 .....	343
单独选择每个文件或目录的备份版本 .....	344
步骤 .....	344
同时选择几个文件或目录的备份版本 .....	344
步骤 .....	344
处理文件冲突 .....	344
步骤 .....	345
选择要从中还原的设备 .....	345
步骤 .....	345
查找还原所需的介质 .....	345
限制 .....	346
步骤 .....	346
预览和启动还原 .....	346



先决条件 .....	346
限制 .....	346
步骤 .....	347
中止还原 .....	347
步骤 .....	347
还原位置选项 .....	347
选择还原位置 .....	347
步骤 .....	347
指定个别文件和目录的还原位置 .....	348
还原到 .....	348
步骤 .....	348
还原为 .....	348
步骤 .....	348
关于恢复失败的会话 .....	349
文件系统备份会话 .....	349
限制 .....	350
文件系统还原会话 .....	350
此项功能的工作方式 .....	350
注意事项 .....	350
限制 .....	351
Data Protector Oracle Server 集成备份和还原会话 .....	351
恢复失败的会话 .....	351
先决条件 .....	351
步骤 .....	351
高级还原任务 .....	352
先决条件 .....	352
高级恢复任务 .....	352
跳过用于还原的文件 .....	352
步骤 .....	352
仅选择特定文件(匹配)用于还原 .....	353
步骤 .....	353
选择打开的文件用于还原 .....	353
步骤 .....	353
在还原期间拒绝访问文件 .....	354
步骤 .....	354
搜索要还原的文件 .....	354
步骤 .....	354
选择用于还原的 Windows 共享磁盘 .....	355
先决条件 .....	355
步骤 .....	355
并行还原对象 .....	355
先决条件 .....	356
限制 .....	356
步骤 .....	356
磁盘映像还原 .....	356
先决条件 .....	356

保管中的介质还原 .....	356
<b>Web 服务器还原 .....</b>	<b>357</b>
还原而不浏览 .....	357
还原整个对象和提取所需部分 .....	357
先决条件 .....	357
步骤 .....	357
使用仅还原模式匹配还原部分备份对象 .....	358
先决条件 .....	358
步骤 .....	358
手动还原文件或目录 .....	358
先决条件 .....	359
步骤 .....	359
还原选项 .....	359
常规还原选项 .....	359
pre-exec 和 post-exec 命令 .....	361
设备选择 .....	361
处理文件冲突 .....	361
Active Directory 特有选项 .....	362
复制模式 .....	362
设置还原选项 .....	362
步骤 .....	362
关于 Windows 系统还原 .....	362
NTFS 3.1 文件系统功能 .....	363
还原备份为共享磁盘的对象 .....	363
Windows 文件系统还原限制 .....	363
配置还原 .....	364
限制 .....	365
Windows 配置对象 .....	365
Active Directory .....	365
DFS .....	366
配置文件 .....	366
注册表 .....	367
可移动存储管理器数据库 .....	367
服务器配置对象 .....	367
SysVol .....	367
Windows TCP/IP 服务 .....	367
系统状态数据还原 .....	368
远程存储服务 .....	368
系统文件保护 .....	369
关于 UNIX 系统还原 .....	369
UNIX 系统特有信息 .....	369
关于 HP OpenVMS 系统还原 .....	369
限制 .....	369
文件系统信息还原 .....	370

第 15 章： 监控、报告、通知和 Data Protector 事件日志 .....	371
---	-----

关于监视 .....	371
查看当前正在运行的会话 .....	371
先决条件 .....	371
步骤 .....	371
查看完成的会话 .....	372
先决条件 .....	372
步骤 .....	372
中止正在运行的会话 .....	372
先决条件 .....	372
步骤 .....	372
关于报告 .....	373
功能 .....	373
报告格式 .....	373
报告类型 .....	374
配置报告 .....	374
单元信息 .....	374
客户机备份 .....	374
不是为 <b>Data Protector</b> 配置的客户机 .....	375
所配置的不由 <b>Data Protector</b> 使用的客户机 .....	375
所配置的不由 <b>Data Protector</b> 使用的设备 .....	375
许可 .....	376
查找计划 .....	376
IDB 报告 .....	376
IDB 大小 .....	376
池和介质报告 .....	377
介质的扩展列表 .....	377
介质列表 .....	377
池列表 .....	377
介质统计信息 .....	378
会话规范报告 .....	378
平均备份对象大小 .....	378
未针对备份配置的文件系统 .....	378
对象的最新备份 .....	379
没有备份的对象 .....	379
会话规范信息 .....	380
会话规范计划 .....	380
备份规范中的树 .....	380
时间范围中的会话报告 .....	381
客户机统计信息 .....	381
设备流 .....	381
已使用介质的扩展报告 .....	381
会话列表 .....	382
对象副本 .....	382
已使用介质的报告 .....	382
会话错误 .....	382
会话流 .....	383

会话统计信息 .....	383
单个会话报告 .....	383
会话设备 .....	384
会话介质 .....	384
会话对象副本 .....	384
会话对象 .....	384
每个客户机会话 .....	385
单个会话 .....	385
报告发送方法 .....	385
广播消息发送方法 .....	386
电子邮件发送方法 .....	386
在 Windows 系统中 .....	386
在 UNIX 系统中 .....	386
电子邮件 (SMTP) 发送方法 .....	386
在 Windows 系统中 .....	387
在 UNIX 系统中 .....	387
外部发送方法 .....	387
记录到文件发送方法 .....	387
SNMP 发送方法 .....	387
在 Windows 系统中 .....	387
在 UNIX 系统中 .....	387
使用 Data Protector GUI 配置报告组 .....	388
先决条件 .....	388
配置阶段 .....	388
配置报告组 .....	388
步骤 .....	388
向报告组添加报告 .....	389
步骤 .....	389
使用 Data Protector GUI 运行报告组 .....	389
先决条件 .....	389
步骤 .....	389
使用 Data Protector GUI 逐个运行报告 .....	389
先决条件 .....	389
步骤 .....	390
使用 Data Protector CLI 运行报告和报告组 .....	390
先决条件 .....	390
步骤 .....	390
创建新的邮件配置文件 .....	390
步骤 .....	390
配置 Windows SNMP 陷阱 .....	391
步骤 .....	391
关于通知 .....	392
通知类型 - 触发通知的事件 .....	392
警报 .....	392
证书已过期 .....	393
Csa 启动会话失败 .....	393

设备错误 .....	393
会话结束 .....	393
文件库磁盘使用 .....	394
运行状况检查失败 .....	394
需要执行 IDB 备份 .....	394
IDB 已损坏 .....	394
IDB 限制 .....	395
需要重新组织 IDB .....	395
IDB 空间不足 .....	395
许可证警告 .....	396
许可证将到期 .....	396
邮件插槽已满 .....	396
装载请求 .....	396
空闲介质不足 .....	397
会话错误 .....	397
会话开始 .....	397
会话太多 .....	397
意外事件 .....	398
检查 UNIX 介质代理 .....	398
用户检查失败 .....	398
通知发送方法 .....	399
广播消息发送方法 .....	399
电子邮件发送方法 .....	399
在 Windows 系统上 .....	399
在 UNIX 系统上 .....	399
电子邮件 (SMTP) 发送方法 .....	399
外部发送方法 .....	400
记录到文件发送方法 .....	400
Data Protector 事件日志发送方法 .....	400
SNMP 发送方法 .....	400
在 Windows 系统上 .....	400
在 UNIX 系统上 .....	400
使用报告组发送方法 .....	400
配置通知 .....	401
先决条件 .....	401
步骤 .....	401
关于 Data Protector 事件日志 .....	401
进程触发事件 .....	402
用户触发事件 .....	402
访问事件日志查看器 .....	402
先决条件 .....	402
步骤 .....	402
删除事件日志查看器内容 .....	402
先决条件 .....	402
步骤 .....	402
关于审计 .....	403

- 生成审计报告 ..... 403
  - 步骤 ..... 403
- 检查 Data Protector 是否正常工作 ..... 403
  - Data Protector 执行的检查 ..... 403
    - 维护任务 ..... 403
    - 检查 ..... 404
  - 应执行哪些检查？ ..... 404
  - 如何自动执行检查 ..... 406
- Data Protector 文档 ..... 407
  - 文档映射图 ..... 407
  - 缩写 ..... 407
  - 集成 ..... 409
- 发送文档反馈 ..... 412

# 第 1 章：简介

## 关于 Data Protector

Data Protector 是一款为快速增长的业务数据提供可靠的数据保护和高度可访问性的备份解决方案。Data Protector 具有专门为整个企业和分布式环境特别定制的综合备份和还原功能。

## Data Protector 的主要功能

- 可扩展和高度灵活的体系结构
- 支持混合环境
- 方便的集中管理
- 高性能备份
- 轻松还原
- 数据和控制通信安全性
- 支持高可用性
- 自动或无人看管操作
- 监视、报告和通知
- 服务管理
- 与联机数据库应用程序集成
- 与其他产品集成

## Data Protector 体系结构

Data Protector 可用于从多个站点上的一个系统到数千个系统的各种环境。基本管理单元是 Data Protector 单元。

Data Protector 单元是由 Cell Manager 系统、一个或多个安装服务器、客户机系统和设备组成的网络环境。

Cell Manager 和 Installation Server 可位于相同的系统上(这是默认选项)，或位于不同的系统上。

## Cell Manager

Cell Manager 是从中心点控制 Data Protector 单元的主要系统，其中安装了含有 IDB 的 Data Protector 核心软件。Cell Manager 运行多种 Session Manager，后者控制备份和还原会话，并将会话信息写入 IDB。IDB 跟踪备份文件以及 Data Protector 单元的配置。

## 安装服务器

Installation Server 是存储 Data Protector 软件存储库的计算机。对 UNIX 和 Windows 环境至少各需要一个 Installation Server，以便可以通过网络执行远程安装，以及将软件组件分发给单元中的客户机系统。

## 客户机系统

在 Cell Manager 系统上安装 Data Protector 软件之后，可以在单元中的每个系统上安装 Data Protector 组件。这些系统将成为 Data Protector 客户机。客户机的作用取决于已在此系统上安装的 Data Protector 软件。

## 要备份的系统

要备份的客户机系统必须装有 Data Protector 磁带客户机(DA 也称为备份代理)。磁盘代理会从系统上的磁盘中读取数据或将数据写入磁盘，并将数据发送到介质代理或从介质代理接收数据。磁带客户机还安装在 Cell Manager 上，从而可以备份 Cell Manager 上的数据、Data Protector 配置和 IDB。

## 带备份设备的系统

连接了备份设备的客户机系统必须装有 Data Protector 介质代理 (MA)。介质代理从设备中的介质读取数据或向其写入数据，并将数据发送到磁带客户机或从其接收数据。备份设备不仅可以与 Cell Manager 相连，还可以与任何系统相连。具有备份设备的客户机系统也称为驱动器服务器。具有多个备份设备的客户机系统称为多驱动器服务器。

## 设置 Data Protector 的任务概述

尽管配置 Data Protector 很容易，但某些高级计划将帮助您配置环境和优化备份。本节概述了设置备份环境的各种全局任务。

根据环境的大小和复杂程度，可能不必完成以下所有步骤。

## 步骤

1. 分析网络和组织结构。确定需要备份的系统。有关信息，请参见《*Data Protector 概念指南*》。
2. 检查是否有任何特殊的应用程序和数据库要备份，如 Microsoft Exchange Server、Microsoft SQL Server、Oracle Server、SAP R/3 等等。Data Protector 提供与这些产品的特定集成功能。  
有关如何配置集成，请参见 *Data Protector 集成指南*。
3. 确定 Data Protector 单元的配置，如：



- 要作为 **Cell Manager** 的系统
  - 要从中安装用户界面的系统
  - 本地备份与网络备份
  - 控制备份设备和库的系统
  - 连接、LAN 和/或 SAN 的类型
4. 根据设置购买所需的 **Data Protector** 许可证。这样即可获得安装所需的密码。  
或者，您也可以使用即开即用密码运行 **Data Protector**。但是，这种密码仅在安装之日起 60 天内有效。请参见《**Data Protector 安装指南**》。
5. 考虑安全方面：
- 分析安全注意事项。请参见《**Data Protector 安装指南**》。
  - 考虑需要配置的用户组。
  - 通过将数据以加密格式写入介质增强安全性。
6. 确定如何构建备份：
- 希望有哪些介质池以及如何使用它们？
  - 将使用哪些设备，以及如何使用？
  - 每个备份需要多少个副本？
  - 需要多少个备份规范以及应如何将其分组？
  - 如果计划备份到磁盘，请考虑高级备份策略，如合成备份和磁盘分段。
7. 安装 **Data Protector Cell Manager** 和安装服务器。然后使用 **Data Protector GUI** 将 **Data Protector** 代理分发到其他系统。有关信息，请参见《**Data Protector 安装指南**》。
8. 配置备份设备。
9. 配置介质池并准备介质。
10. 配置备份规范，包括 IDB 备份。
11. 配置报告(如果需要)。
12. 为灾难恢复做准备。有关灾难恢复的详细信息，请参见 **Data Protector 灾难恢复指南**。
13. 熟悉以下任务：
- 处理失败的备份
  - 执行还原
  - 复制已备份数据和保管介质
  - 测试灾难恢复
  - 维护 IDB

## Data Protector 操作

备份和还原任务在会话中完成。可以同时运行多个会话。最大会话数受单元中的 **Cell Manager** 配置(处理器速度、主内存大小、磁盘空间)等资源限制。

### 备份会话

备份会话是从客户机系统将数据备份到介质的过程。备份会话始终在 **Cell Manager** 系统上运行。备份会话基于备份规范，并且由操作员以交互形式启动或由 **Data Protector** 计划程序以无人看管形式启动。

### 还原会话

还原会话是将以前备份中的数据还原到磁盘的过程。还原会话采用交互形式，并由操作员使用 **Data Protector** 用户界面启动。

### pre-exec 和 post-exec 命令

通过 **pre-exec** 命令，可以在备份或还原会话之前执行某些操作。通过 **post-exec** 命令，可以在备份或还原会话之后执行某些操作。

可以为备份规范设置 **pre-exec** 和 **post-exec** 命令，并且可以在 **Cell Manager** 系统上执行，或者可以指定这些命令作为备份对象选项，并在运行各个磁盘代理的客户机系统上执行。

**pre-exec** 和 **post-exec** 脚本命令可编写为可执行文件或批处理文件(在 **Windows** 系统中)或 **shell** 脚本(在 **UNIX** 系统中)。**Data Protector** 不提供这些命令，必须(例如由备份操作员)单独编写。

### 对象复制、对象合并和对象验证会话

对象复制会话基于对象复制规范。对象合并会话基于对象合并规范。可以用交互形式启动或自动启动这两个会话。

对象验证会话基于对象验证规范。它检查由备份、对象复制或对象合并会话创建的对象的数据完整性，并检查能否将这些对象传送到所需位置。可以用交互形式启动或自动启动这些会话。

## 用户界面

**Data Protector** 提供图形用户界面 (GUI) 和命令行界面 (CLI)。

### 图形用户界面

对于 **Windows** 系统提供图形用户界面。

通过 **Data Protector** 的图形用户界面，从一个系统即可管理全部备份环境。甚至可以从一个系统管理多个备份环境。**Data Protector** 体系结构使您可以灵活地安装和使用 **Data Protector** 用户界面。不必从 **Cell Manager** 系统中使用用户界面，可以将其安装在桌面系统上。

为了方便操作，GUI 可安装在各种系统上，以使多个管理员可以通过其本地安装的控制台访问 **Data Protector**。从客户机系统将用户添加到 **Cell Manager** 上相应的 **Data Protector** 用户组，然后才能在该系统上开始使用 **Data Protector** GUI。

需要进行特定的安装和配置，才能在文件名和会话消息中显示国际字符。

**Data Protector 10.00** GUI 的先前版本与 **Data Protector 10.00** **Cell Manager** 不兼容。

## 命令行界面

除了图形用户界面以外，在 **Windows** 和 **UNIX** 系统上还提供命令行界面。命令行界面 (CLI) 遵照命令和选项的标准 **UNIX** 格式，并提供完整的 **Data Protector** 功能。可以在脚本中使用这些命令以加快处理通常执行的任务。

**omniintro** 手册页列出了所有受支持的 **Data Protector** 命令，以及命令在 **UNIX** 和 **Windows** 平台上的差异。有关详细信息，请参见《**Data Protector** 命令行界面参考》。

## 自定义 GUI 中的语言设置

在异构环境(一个单元中的不同操作系统有不同的区域设置)中处理文件名是一个重大难题。如果用某些区域设置备份文件名，然后用不同的区域设置查看或还原文件名，则需要进行特定的设置才能正确显示此类文件名。

## 先决条件

以下先决条件适用于 GUI 系统：

- 针对在 **Data Protector** GUI 系统中选择的编码字符集安装相应的字体。例如，要在运行于欧洲语言系统的 GUI 中查看日语字符，请安装日语字体。

## 限制

- **Windows** 和 **UNIX** 操作系统中字符编码转换的实现之间有少许不同。如果运行 **Data Protector** GUI 的平台与配置客户机时的平台不同，则无法正确映射某些字符。但是，只有少量字符可能显示不正确，而这不会影响备份或还原。

## 步骤

1. 在上下文列表中，单击**备份、监视、还原、报告或内部数据库**。
2. 在“视图”菜单中，单击**编码**。
3. 选择创建备份文件的系统所使用的字符编码。

## 启动 Data Protector GUI

要在 Windows 系统中启动 Data Protector GUI，请转到：

**开始 > 程序 > Data Protector > Data Protector Manager**

或者，运行命令 `manager`。

要指定要连接到的 Cell Manager，请运行：

```
manager -server Cell_Manager_name。
```

通过此命令的上下文特有选项，可以启动一个或多个 Data Protector 上下文。要启动 Data Protector“备份”和“还原”上下文，请运行：

```
manager -backup -restore
```

有关这些命令的详细信息，请参见 omnigui 手册页或《Data Protector 命令行界面参考》。

## 使用 Microsoft 管理控制台 (MMC)

在 Windows 系统中，可以使用 Microsoft 管理控制台访问 Data Protector 主页，也可以启动 Data Protector GUI。

Data Protector 管理单元 OB2\_Snap 实现了 Data Protector 与 MMC 的初步集成。要使用此管理单元，请执行以下操作：

### 步骤

1. 在 Data Protector 程序组中，选择 **Data Protector MMC 管理单元**。
2. 在控制台根下，选择 **Data Protector** 以显示可用的选项。

## 从 Data Protector GUI 启动 Storage Optimizer

可通过执行以下步骤，从 Data Protector GUI 启动 Storage Optimizer：

1. 在 Data Protector 全局文件中启用变量 StorageOptServer。  
其格式应如下所示：StorageOptServer = <server name>。此步骤是强制性的。
2. 在“备份”环境中，导航到**操作 > Storage Optimizer**。Storage Optimizer 即会在一个新的 Web 浏览器窗口中打开。

# 第 2 章：配置任务

## 系统安全性

在 **Data Protector 10.00** 中，所有通信默认基于 **TLS 1.2**。要在客户机和 **Cell Manager** 之间配置信任，必须在安装之前满足特定的先决条件。在 **Data Protector 10.00** 版本之前，用户可以选择通过启用加密控制通信 (**ECC**)，保护 **Cell Manager** 和客户机之间的通信。预先已启用 **10.00 ECC** 的 **DA** 和 **MA** 客户机可以继续与 **Data Protector 10.00** 搭配使用。

在 **10.00** 中，所有命令和脚本执行均通过 **Cell Manager** 路由。集中化命令执行可确保控制和数据都通过安全的 **TLS** 通道发送，从而保证数据完整性。此外，**Data Protector** 客户机现在只侦听并接受来自受信任且经验证 **Cell Manager** 的指令和脚本命令执行，这样可显著降低安全漏洞的风险。

有关安全性的详细信息，请参见《**Data Protector 安装指南**》。

## 为安全通信配置证书

在安装过程中，通过指纹验证，基于 **OpenSSL** 的自签名证书用于安全通信，以建立信任。如果您需要使用自定义证书，可以在安装 **Data Protector** 后，将 **Data Protector** 安装过程中生成的 **OpenSSL** 证书替换为自定义证书。以下步骤用于生成自定义证书、重新生成证书和重新分发证书。

### 自定义证书生成

用户可以生成自定义证书，并将文件复制到以下路径：

#### **Windows:**

私钥：<DP\_HOME>\config\sscertificates\localhost\_key.pem

自签名证书：<DP\_HOME>\config\sscertificates\localhost\_cert.pem

#### **Unix:**

私钥：/etc/opt/omni/config/sscertificates/localhost\_key.pem

自签名证书：/etc/opt/omni/config/sscertificates/localhost\_cert.pem

### 在 **Data Protector** 中重新生成证书

请运行以下命令以在 **Data Protector** 中重新生成证书：

```
omnicc -secure_comm -regenerate_cert
```

### 重新分发证书

证书的重新分发必须在使用自定义证书时或将要重新生成证书时完成。

### **Cell Manager** 证书重新分发

1. 通过运行以下命令，在所有安装服务器服务器(所有 **Windows** 和 **Unix**)中重新配置 **Cell Manager** 证书：

```
omnicc -secure_comm -reconfigure_peer <CM hostname>
```

2. 要重新分发和重新配置，必须在 CM 上运行以下命令：

```
omnicc -secure_comm -reconfigure_peer_all <input_file_path>
```

<input\_file\_path> 参数为可选。该文件应该具备属于该单元的所有客户机的凭据。

文件的格式为：

```
-host "linux_client_hostname" -user "<username>" -pass "password"
```

```
-host "windows_client_hostname" -user "<Domain>\<username>" -pass "<password>"
```

这里，每行对应一个客户机，如上所示，必须提及用户名和密码。

如果未指定 <input\_file\_path>，尝试重新分发和配置 Cell Manager 证书时，omnicc 会提示客户机凭据。

**注意：**

对于 Windows 客户机，Domain 名称必须带有前缀。

### 客户机证书重新分发

如果重新生成客户机证书，则必须重新分发至 Cell Manager。运行以下命令：

```
omnicc -secure_comm -reconfigure_peer <client_host_name>
```

### 报告

“报告”上下文中的“通知”部分添加了 **WarnCertificateExpiry** 通知。

借此，用户可为即将过期的证书生成通知。

默认情况下，为即将在 7 天后过期的证书生成通知。通过更改全局变量

**WarnCertificateExpiryBefore** 的值，可生成更早的通知。

## 从 GUI 连接到任何 Cell Manager/Jumpstation UI

如果使用已安装单元控制台组件的主机来连接多个 Cell Manager，安装 CC 组件的主机应受到其试图连接的 Cell Manager 的保护，并且所有 CM 都应使用 GUI 主机进行保护。

例如：

#### 案例 1：

如果主机 X 用于连接 Cell Manager 主机 CM1、主机 CM2 和主机 CM3(都为 10.0 或更高版本)，在主机 X 中运行以下命令：

```
Omnicc -secure_comm -configure_peer <hostCM1>
```

```
Omnicc -secure_comm -configure_peer <hostCM2>
```

```
Omnicc -secure_comm -configure_peer <hostCM3>
```

在上诉提及的所有 Cell Manager 中运行以下命令：

```
Omnicc -secure_comm -configure_peer <hostX>
```

#### 案例 2：

如果主机 X 为 10.00 之前的版本，而主机 CM1、主机 CM2 和主机 CM3 为 10.0 或更高版本，在三个 Cell Manager 中运行以下命令：

```
Omnicc -secure_comm -configure_for_gui <hostX>
```

### 案例 3:

如果 CM 的主机为 10.0 之前的版本，而主机 X 为 10.0 或更高版本，在主机 X 中执行以下命令：

```
Omnicc -secure_comm -configure_for_gui <hostCM1>
```

```
Omnicc -secure_comm -configure_for_gui <hostCM2>
```

```
Omnicc -secure_comm -configure_for_gui <hostCM3>
```

### 案例 4:

如果主机 CM1 为 10.0 之前的版本，主机 CM2 和主机 CM3 和主机 X 为 10.0 或更高版本。在主机 X 中运行以下命令：

```
Omnicc -secure_comm -configure_for_gui <hostCM1>
```

```
Omnicc -secure_comm -configure_peer <hostCM2>
```

```
Omnicc -secure_comm -configure_peer <hostCM3>
```

在主机 CM2 和主机 CM3 中运行以下命令

```
Omnicc -secure_comm -configure_peer <hostX>
```

## 用户安全性

Data Protector 用户是 Data Protector 的一个安全关键层。必须谨慎规划和测试用户的配置。

## 用户权限

某些用户权限很强大，因此象征着安全问题。例如，用户配置和客户机配置用户权限使用户可以更改安全设置。

**还原到其他客户机**用户权限也非常强大，尤其在与**作为 root 备份**或**作为 root 还原**用户权限结合时。

甚至不太强大的用户权限也有内在的风险与自身相关。可以配置 Data Protector 以限制某些用户权限，从而降低这些风险。

## “启动备份规范”用户权限

用户可使用 omnib 与 -datalist 选项从命令行中启动备份规范的备份会话。

通过结合**启动备份规范**和**启动备份**用户权限，用户可在 GUI 中查看配置的备份规范并能够启动备份规范或交互式备份的备份会话。

并不总是希望允许用户执行交互式备份。要仅允许具有**保存备份规范**用户权限的用户进行交互式备份，请将 StrictSecurityFlags 全局选项设置为 0x0200。

## 隐藏备份规范的内容

在高安全环境中，可能会将所保存备份规范的内容视为敏感甚至保密信息。

可以将 **Data Protector** 配置为对所有用户隐藏备份规范的内容，除具有**保存备份规范**用户权限的用户之外。为此，请将 **StrictSecurityFlags** 全局选项设置为 **0x0400**。

## 主机信任

主机信任功能仅需在有限数量的客户机内将数据从一个客户机还原到另一个客户机，从而减少了将**还原到其他客户机**用户权限授予用户的需要。可以定义一组主机，彼此信任对方的数据。

主机信任通常在以下情况下使用：

- 用于群集中的客户机(节点和虚拟服务器)。
- 如果客户机的主机名更改且旧备份对象的数据需要还原。
- 如果由于 **DNS** 问题导致客户机主机名与备份对象不匹配。
- 如果用户拥有多个客户机且需要将数据从一个客户机还原到另一个客户机。

## 用户组

**Data Protector** 默认情况下只有少数几个预定义的用户组。建议在 **Data Protector** 环境中为每种类型的用户定义特定的组，以将分配给他们的权限设置最小化。

## 用户限制

除定义特定用户组以外，还可以进一步限制用户操作，以仅对单元的特定系统执行操作。可通过在 **Cell Manager** 上配置 **user\_restrictions** 文件，强制执行此限制。这些限制仅适用于 **Data Protector** 用户组的成员，对管理员和操作员则不适用。

## 用户验证

用户配置与用户验证相关联。增强的验证如果没有详细的用户配置也没有价值，反之亦然 - 即使最详细的用户配置如果没有增强的验证也没有意义。

**Data Protector** 用户列表中不应存在“弱”用户规范，这一点很重要。请注意，用户规范的客户机部分是强部分(尤其在有增强的验证的情况下)，而无法可靠地验证用户和组部分。

具有强大用户权限的用户应配置给特定的客户机，他们将用于 **Data Protector** 管理。如果使用了多个客户机，则应为每个客户机添加一个入口，而不是将这种用户指定为 **user**、**group**、<Any>。不应允许不受信任的用户登录任何此类系统。

## 严格主机名检查

默认情况下，**Cell Manager** 使用相对简单的方法验证用户。它使用已启动用户界面或应用程序代理的客户机已知的主机名。此方法比较容易配置，并在将安全视为“建议”(即预计不会出现恶意攻击)的环境中可提供合理的安全级别。

而另一方面，严格主机名检查设置提供了增强的用户验证。这种验证使用由 **Cell Manager** 根据从连接中获得的 **IP** 地址进行反向 **DNS** 查询所解析的主机名。要启用严格主机名检查，请将 **StrictSecurityFlags** 全局选项设置为 **0x0001**。



## 限制

- 基于 IP 的用户验证的强度仅相当于网络中的防欺骗保护。安全性设计人员必须确定现有网络提供的防欺骗安全性级别是否足以满足特定的安全性要求。通过用防火墙、路由器、VPN 等将网络分段可以实现防欺骗保护。
- 特定客户机内用户间的分离不如客户机间的分离强大。在高安全环境中，不应在相同客户机中混合存在常规用户和高权限用户。
- 用户规范中使用的主机无法配置为使用 DHCP，除非将这些主机绑定到固定 IP，并在 DNS 中进行相应配置。

请了解这些限制，以便正确地评估通过此设置所能达到的安全程度。

## 要求

增强的验证不会自动对某些内部连接授予访问权限。因此，使用此验证后，必须为以下程序添加新用户：

- **Windows** 客户机中的任何应用程序代理 (OB2BAR)。必须为每个装有应用程序代理的客户机添加用户 SYSTEM、NT AUTHORITY、*client*。请注意，如果将某客户机上的 Inet 配置为使用特定帐户，则必须已配置该帐户。

## 主机名解析

在以下情况下，Data Protector 用于验证的主机名可能在默认用户验证与严格主机名检查间有所区别：

- 反向 DNS 查询将返回其他主机名。这可能是有意所为，或表明客户机或反向 DNS 表配置错误。
- 客户机是多宿主的(有多个网络适配器和/或多个 IP 地址)。此注意事项是否适用于特定的多宿主客户机，取决于该客户机在网络中的角色及在 DNS 中对其的配置方式。
- 客户机是群集。

通过此设置启用的检查的性质可能要求重新配置 Data Protector 用户。必须检查 Data Protector 用户的现有规范，以查看这些用户是否可能受到以上任何原因的影响。根据不同情况，可能需要更改现有规范或添加新规范，以解释可能作为连接来源的所有 IP。

请注意，如果启用严格主机名检查时必须修改用户规范，则在恢复为默认用户验证时还必须重新配置用户。因此，建议确定要使用的用户验证，并一直使用该方法。

可靠的反向 DNS 查询的先决条件是安全性的 DNS 服务器。您必须防止对所有未授权人员的物理访问和登录。

通过使用 IP 进行验证(而非使用主机名)，可解决某些潜在的与 DNS 相关的验证问题，但维护起来比较困难。

## 安全日志

如果在访问 Data Protector 功能或客户机时遇到问题，可以使用日志文件中的相关信息确定问题。例如，记录的事件可帮助您确定配置错误的用户或客户机。

## 客户机安全性事件

客户机安全事件记录到单元中每个客户机的默认 **Data Protector** 日志文件目录中的 `inet.log` 文件。

检查客户机上 **Data Protector** 最近的活动很有用。

## Cell Manager 安全事件

**Cell Manager** 安全事件记录在默认 **Data Protector** 服务器日志文件目录中的 `security.log` 文件中。

出现第一个安全事件时即创建 `security.log` 文件。

## 配置主机信任

可以定义一组主机，彼此信任对方的数据。

### 步骤

1. 在 **Windows Cell Manager** 上，创建 `Data_Protector_program_data\Config\Server\cell\host_trusts` 文件。  
在 **UNIX Cell Manager** 上，创建 `/etc/opt/omni/server/cell/host_trusts` 文件。
2. 在文件中，列出受信任主机。

例如：

```
GROUP="cluster.domain.com"
{
  cluster.domain.com
  node1.domain.com
  node2.domain.com
}
GROUP="DFG"
{
  computer.domain.com
  anothercomputer.domain.com
}
```

3. 保存文件。

## 加密

### 关于数据加密

通过 **Data Protector** 可以对备份数据进行加密，以使其与其他数据相比受到保护。提供以下两种数据加密技术：基于软件的和基于驱动器的加密。

Data Protector 软件加密简称 **AES 256 位加密**，以对于加密和解密使用相同密钥的高级加密标准 (AES) 加密算法为基础。对数据进行加密，然后再通过网络传输这些数据并将其写入介质。

Data Protector 基于驱动器的加密使用驱动器的加密功能。具体实现和加密强度取决于驱动器的固件。Data Protector 仅启用该功能并管理加密密钥。

打开加密之后，不需要任何其他配置。但是，对于 **AES 256 位加密**，Data Protector 通过命令行界面 (CLI) 提供加密密钥的高级手动管理(如到期、重新激活、导出、导入和删除密钥)。

使用 Data Protector GUI 或 CLI，可以确定对哪些备份对象加密或哪个备份介质含有加密对象，并可以获取这些对象的加密详细信息。

## 启用 **AES 256 位加密**

创建新备份规范或修改已配置的备份规范时，可以启用基于软件的 **AES 256 位加密**。

### 先决条件

- 必须有活动的加密密钥，然后才能执行加密的 IDB 备份。有关详细信息，请参见 *omnikeytool* 手册页或《*Data Protector 命令行界面参考*》。

### 限制

- **AES 256 位加密** 不对元数据(如文件名和文件大小)进行加密。
- 加密不适用于 ZDB 到磁盘备份和 ZDB 到磁盘 + 磁带备份的磁盘部分。
- 使用 **AES 256 位加密** 备份的对象无法合并。

## 在文件系统备份规范中启用加密

### 步骤

1. 在上下文列表中，单击 **备份**。
2. 在范围窗格中，展开 **备份规范**，然后展开 **文件系统**。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“选项”属性页中，单击“文件系统选项”的 **高级** 按钮。
5. 在“文件系统选项”窗口中，单击 **其他** 选项卡。在 **数据安全性** 下拉列表中，选择 **AES 256 位** 选项。
6. 单击 **确定**，然后单击 **应用** 以保存更改。

#### 提示：

要仅加密所选的备份对象，请转到 **备份对象摘要** 选项卡，然后在对象的属性中选择 **AES 256 位** 选项。

## 在磁盘映像备份规范中启用加密

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“备份对象摘要”页中，单击**属性**按钮。
5. 在“对象属性”窗口中，单击**其他**选项卡。在**数据安全性**下拉列表中，选择 **AES 256 位** 选项。
6. 单击**确定**，然后单击**应用**以保存更改。

## 在内部数据库备份规范中启用加密

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**内部数据库**。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“选项”页中的“常见应用程序选项”下，单击**高级**。
5. 在“公共应用程序选项”窗口中，单击**其他**选项卡。从**数据安全性**下拉列表中，选择 **AES 256 位** 选项。
6. 单击**确定**，然后单击**应用**以保存更改。

## 在应用程序集成备份规范中启用加密

### 限制

- 有关支持 AES 256 位加密的应用程序集成的最新列表，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新支持矩阵。
- 不能组合使用 Microsoft SQL Server 集成的**快速直接模式**和 **AES 256 位** 选项。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如 **MS SQL Server**)。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“选项”属性页中，单击“公共应用程序选项”的**高级**按钮。
5. 在“公共应用程序选项”窗口中，单击**其他**选项卡。在**数据安全性**下拉列表中，选择 **AES 256 位** 选项。
6. 单击**确定**，然后单击**应用**以保存更改。

## 导出和导入含有加密备份的介质

要将加密备份中的数据恢复到不同 **Data Protector** 单元中的客户机，需要将介质和加密密钥导入到目标 **Cell Manager**，如以下各节所述。

### 注意：

**Data Protector** 还通过命令行界面 (CLI) 提供加密密钥的高级手动管理(如使密钥过期、重新激活、导出、导入和删除密钥)。有关详细信息，请参见 **omnikeytool** 手册页或《**Data Protector** 命令行界面参考》。

## 没有 CMMDB 的 Cell Manager 环境或 MoM 环境

在不使用本地 MMDDB 的 **Cell Manager** 环境中或 **MoM** 环境中，执行以下步骤可导出和导入含有加密备份的介质：

### 步骤

1. 在原始 **Cell Manager** 上，从 **IDB** 导出介质。此操作还会将相关的加密密钥从密钥库导出到默认导出加密密钥目录下的 *mediumID.csv* 文件中。
2. 将 *mediumID.csv* 文件传输到目标 **Cell Manager**，并将其放置到默认导入加密密钥目录中。
3. 将导出的介质插入目标 **Cell Manager** 将使用的驱动器中。
4. 在目标 **Cell Manager** 上导入该介质。此操作还可从 *mediumID.csv* 文件中导入密钥。

### 注意：

如果密钥文件不存在，则仍可导入介质，但目录导入将因缺少解密密钥而中止。

## 有 CMMDB 的 MoM 环境

在使用 **CMMDB** 的 **MoM** 环境中，所有介质信息都存储在 **MoM Manager** 上，但这些介质使用的加密密钥 ID 以及 **CDB** 存储在每个各自 **Cell Manager** 上的本地密钥库中。请注意，所有介质管理操作都需要在 **MoM Cell Manager** 上完成。

要在 **CMMDB** 位于 **MoM Manager** 上的情况下导出和导入含有加密备份的介质，请执行以下步骤：

### 步骤

1. 从 **CMMDB** 导出介质。密钥 ID 将导出到默认导出加密密钥目录下的 *mediumID.csv* 文件中。
2. 将 *mediumID.csv* 文件传输到目标 **Cell Manager**，并将其放置到默认导入加密密钥目录中。
3. 从 **MoM Manager** 中，从带库弹出介质。
4. 将介质从原始介质池移至目标介质池，后者与目标单元中的某个驱动器关联。此操作还可导入目录。
5. 将导出的介质插入目标 **Cell Manager** 将使用的驱动器中。
6. 在目标 **Cell Manager** 上导入该介质。此操作还可从 *mediumID.csv* 文件中导入密钥。

## 启用基于驱动器的加密

有关支持基于驱动器的加密的最新设备列表，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新支持矩阵。

可以在以下过程中启用基于驱动器的加密：

- 配置驱动器或修改已配置的某个时。
- 配置备份、对象副本或对对象合并规范或修改已配置的某个时。
- 配置自动介质操作或修改已配置的某个时。

### 先决条件

- 必须有活动的加密密钥，然后才能执行加密的 IDB 备份。有关详细信息，请参见 [omnikeytool](#) 手册页或《*Data Protector* 命令行界面参考》。

### 限制

- 无法对 NDMP 服务器控制的设备或具有外部加密控制的库(例如 SKM 控制下的 ESL 库)中的驱动器使用基于驱动器的加密。

### 建议

- 为优化性能，使用的块大小应至少为 256 KB。

#### 注意：

当备份到同时包含加密和未加密备份的介质时，可能会看到 **Drive-based decryption enabled** 消息。这意味着介质上的最后一个备份是加密备份，并且已自动将其解密，以便在添加新备份之前 **Data Protector** 可以检查该备份。

## 在驱动器配置中启用基于驱动器的加密

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，依次展开 **设备**、所需的设备及其驱动器。
3. 右键单击所需的驱动器，然后单击 **属性**。
4. 在“设置”属性页中，单击 **高级** 按钮。
5. 在“高级选项”窗口的 **设置** 选项卡中，选择 **基于驱动器的加密** 选项，然后单击 **确定**。
6. 单击 **应用** 保存更改。

## 在备份规范中启用基于驱动器的加密

### 步骤

1. 在上下文列表中，单击 **备份**。
2. 在范围窗格中，展开 **备份规范**，然后展开备份规范的相应类型(例如 **文件系统**)。此时将显示所保存的全部备份规范。
3. 单击相应的备份规范。

4. 在“目标”页中，右键单击选择用于备份的设备，然后单击**属性**。
5. 在“设备属性”窗口中，选择**基于驱动器的加密**选项，然后单击**确定**。
6. 单击**应用**保存更改。

**提示：**

要修改对象复制或对象合并规范，请在**对象操作**上下文中打开该规范，然后执行步骤 4 到 6。

## 为自动介质操作启用基于驱动器的加密

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**自动操作**。此时将显示所有已配置的自动操作。
3. 单击要为其启用基于驱动器的加密的介质操作。
4. 在“选项”页中，选择**基于驱动器的加密**选项，然后单击**应用**。

**注意：**

**基于驱动器的加密**选项适用于自动介质操作中涉及的所有设备。

## 用户验证和 LDAP 简介

应在企业用户管理基础设施中结合将 **Data Protector** 作为企业系统进行认证和授权的功能。此连接允许向企业用户目录中配置的用户和组授予访问 **Data Protector** 服务的权限。

将在安全连接上执行用户身份验证，并将轻型目录访问协议 (LDAP) 用作基础技术。因此，用户可以使用其企业凭据访问 **Data Protector** 服务而无需单独保存密码。此外，可以在企业目录中将管理员或操作员保留为组，从而符合已建立的授权和审批流程。

使用 **Java** 验证和授权服务 (JAAS) 登录模块在 **Data Protector** 嵌入式应用程序服务器 (WildFly) 的安全域中配置 LDAP 集成。可选的 LDAP 登录模块可提供 LDAP 身份验证和授权服务，可将这些服务通过必需的 **Data Protector** 登录模块映射到 **Data Protector** 权限。如果未配置 LDAP 集成，**Data Protector** 将按照以前版本中的流程运行。

**Data Protector** 使用登录模块堆栈中的登录模块验证用户。如果用户使用 **Data Protector** GUI 连接 **Cell Manager**，则以下登录模块将执行用户验证：

1. **LDAP 登录模块**：针对现有 LDAP 服务器验证用户凭据，如用户名和密码。请参见[初始化并配置 LDAP 登录模块](#)。
2. **Data Protector 登录模块**：针对 **Data Protector** 用户列表和 Web 访问密码验证用户凭据。请参见[授予 LDAP 用户或组 Data Protector 权限](#)。
3. 执行 LDAP 初始化和配置所需的所有步骤后，还可以检查配置。请参见[检查 LDAP 配置](#)。

**注意：** 当在 **Data Protector** 中配置了用户或客户机以允许其使用典型方式访问 CLI 时，**Data Protector** GUI 不使用 LDAP 功能。

## 初始化并配置 LDAP 登录模块

LDAP 登录模块位于 WildFly 应用程序服务器(随 Data Protector 一起安装)的安全域中。必须在首次使用 LDAP 安全功能前初始化并配置 LDAP 登录模块。

1. 初始化 LDAP 登录模块。
2. 配置 LDAP 登录模块。

## 初始化 LDAP 登录模块

要初始化 LDAP 登录模块，请使用 jboss-cli 实用程序(也随 Data Protector 一起安装)

1. jboss-cli 实用程序位于： %Data\_Protector\_home%/AppServer/bin。请执行以下命令：
  - Windows: jboss-cli.bat --file=ldapinit.cli
  - UNIX: jboss-cli.sh --file=ldapinit.cli

此命令将在 WildFly 配置中创建一个 LDAP 登录模块，并将使用默认值来填充这一新的登录模块。standalone.xml 配置文件中的命令行生成的默认值为：

```
<security-domain name="hdpd-domain">
  <authentication>
    <login-module code="LdapExtended" flag="optional">
      <module-option name="java.naming.factory.initial"
        value="com.sun.jndi.ldap.LdapCtxFactory"/>
      <module-option name="java.naming.security.authentication" value="simple"/>
      <module-option name="roleFilter" value="(member={1})"/>
      <module-option name="roleAttributeID" value="memberOf"/>
      <module-option name="roleNameAttributeID" value="distinguishedName"/>
      <module-option name="roleAttributeIsDN" value="true"/>
      <module-option name="searchScope" value="SUBTREE_SCOPE"/>
      <module-option name="allowEmptyPasswords" value="true"/>
      <module-option name="password-stacking" value="useFirstPass"/>
    </login-module>
    <login-module code="com.hp.im.dp.cell.auth.DpLoginModule" flag="required">
      <module-option name="password-stacking" value="useFirstPass"/>
    </login-module>
  </authentication>
</security-domain>
```



**注意：**

如果 Cell Manager 安装在 UNIX 环境中并使用 LDAP 身份验证，则 standalone.xml 配置文件中通过命令行生成的默认值将会更改。更改如下：

```
<login-module code="LdapExtended" flag="optional">
  <module-option name="java.naming.factory.initial"
    value="com.sun.jndi.ldap.LdapCtxFactory"/>
  <module-option name="java.naming.security.authentication" value="simple"/>
  <module-option name="roleFilter" value="(member={1})"/>
  <module-option name="roleAttributeID" value="memberOf"/>
  <module-option name="roleNameAttributeID" value="distinguishedName"/>
  <module-option name="roleAttributeIsDN" value="true"/>
  <module-option name="searchScope" value="SUBTREE_SCOPE"/>
  <module-option name="allowEmptyPasswords" value="false"/>
  <module-option name="password-stacking" value="useFirstPass"/>
  <module-option name="java.naming.provider.url" value="ldap://<IP_of_
    Active_Directory_host>"/>
  <module-option name="baseCtxDN" value="OU=_Benutzer,DC=godyo,DC=int"/>
  <module-option name="rolesCtxDN" value="OU=_Gruppen,DC=godyo,DC=int"/>
  <module-option name="bindDN" value="CN=backup-service,OU=_Service_
    Accounts,DC=godyo,DC=int"/>
  <module-option name="bindCredential" value="password"/>
  <module-option name="baseFilter" value="(userPrincipalName={0})"/>
</login-module>
```

主要是配置参数 baseCtxDN 和 rolesCtxDN。组织单位 (OU) 参数用于对 UNIX Cell Manager 进行身份验证。

2. 要从远程客户机访问 Cell Manager 上的 WildFly 管理控制台，请启用对 WildFly 管理控制台的远程访问。为此，请使用文本编辑器，在 standalone.xml 文件的接口部分中将管理接口的绑定地址从 127.0.0.1 更改为 0.0.0.0:

```
<interfaces>
  <interface name="management">
    <inet-address value="{jboss.bind.address.management:0.0.0.0}"/>
  </interface>
  <interface name="public">
    <inet-address value="0.0.0.0"/>
  </interface>
```

```
<interface name="unsecure">  
  
<inet-address value="{jboss.bind.address.unsecure:127.0.0.1}"/>  
  
</interface>  
  
</interfaces>
```

3. 重新启动 Data Protector 服务：

```
omnisv stop  
  
omnisv start
```

## 配置 LDAP 登录模块

要配置 LDAP 登录模块，请使用 WildFly 应用程序的 Web 管理控制台，该控制台随 Data Protector 一起安装。请执行以下操作：

1. 要访问 WildFly 管理控制台，请创建一个 WildFly 用户。要创建 WildFly 用户，请运行 `add-user` 实用程序：
  - Windows: `add-user.bat`，所在位置： `%Data_Protector_home%/AppServer/bin`
  - UNIX: `add-user.sh`，所在位置： `/opt/omni/AppServer/bin`
2. 为以下参数提供输入内容：
  - **要添加的用户类型**：选择“管理用户”。
  - **领域**：将此字段留空，因为实用程序将选择默认值 `ManagementRealm`。
  - **用户名**：添加一个用户名。
  - **密码**：添加一个密码。
  - **组**：无。
3. 要访问 WildFly 管理控制台，请使用浏览器打开 URL: `<http://cell-manager-name:9990/console>`
4. 在“身份验证”屏幕中，指定由 `add-user` 实用程序创建的用户名和密码。
5. 单击**登录**。WildFly 应用程序服务器的管理控制台随即显示。
6. 在 WildFly 管理控制台中，选择**配置文件**选项卡。
7. 在**配置文件**选项卡中，展开**安全**节点，然后单击**安全域**。
8. 在已注册的安全域的列表中，对 `hdp-dp-domain` 单击**视图**。为安全域 `hdp-dp-domain` 定义了以下登录模块：
  - `LdapExtended`
  - `Com.hp.im.dp.cell.auth.DpLoginModule`
9. 选择 **LdapExtended** 模块。
10. 在“详细信息”部分中，单击**模块选项**选项卡。**模块选项**选项卡中列出了所有预定义的模块选项。

11. 要自定义和使用 LDAP 登录模块，需要添加其他模块选项。单击**添加**并为每个模块选项指定**名称**和**值**。有关详细信息，请参见下表：

模块选项	名称	值	说明
提供程序 URL	java.naming.provider.url	使用以下格式指定 LDAP 服务器的 URL： ldap://<server>:<port>	标准属性名称
基本上下文判别名称 (DN)	baseCtxDN	指定含有用户的 LDAP 位置的 DN。	从中启动用户搜索操作的上下文的固定 DN
Base 过滤器	baseFilter	按照以下格式在 LDAP 设置中指定与用户登录名匹配的属性： (<user-login-name-attribute>={0})。其中，<user-login-name-attribute>需要由相应的 LDAP 属性名称替换。	用于定位要进行身份验证的用户的上下文的搜索过滤器
角色上下文 DN	rolesCtxDN	指定含有用户组的 LDAP 位置的 DN。	要搜索用户组的上下文的固定 DN
绑定 DN	bindDN	指定由登录模块用于执行初始 LDAP 绑定的 LDAP 用户 DN。必须拥有所需权限以搜索用户和组的 LDAP 位置，来获取用户及其组。这些位置在 baseCtxDN 和 rolesCtxDN 模块选项中进行定义。	用于为用户和角色查询绑定 LDAP 服务器的 DN。这是一个对 baseCtxDN 和 rolesCtxDN 值具有读取/搜索权限的 DN。
绑定凭据	bindCredential	为在 BindDN 模块选项中提供的 LDAP 用户指定密码。	bindDN 的密码。

有关其他模块选项的更多信息，请访问以下 URL：

- <https://community.jboss.org/wiki/LdapExtLoginModule>
  - [http://technet.microsoft.com/en-us/library/cc773354\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc773354(v=ws.10).aspx)
12. 在重新加载 WildFly 应用程序服务器配置后更改将生效。要重新加载配置，请使用 jboss-cli 实用程序，该实用程序位于 %Data\_Protector\_home%/AppServer/bin 中。
13. 请执行以下命令：

- Windows: `jboss-cli.bat -c :reload`
- UNIX: `jboss-cli.sh -c :reload`

**注意：**在 MoM 环境中配置 LDAP 登录模块时，请确保在每个 Cell Manager 上执行上述步骤。MoM 环境中的每个 Cell Manager 需具有相同的 LDAP 登录模块配置。

## 向 LDAP 用户或组授予 Data Protector 权限

LDAP 用户仅在被授予 Data Protector 权限后才能连接到 Cell Manager。配置 LDAP 登录模块后，可以为 LDAP 用户授予所需的 Data Protector 权限。

要授予 Data Protector 权限，请执行以下步骤：

1. 启动 Data Protector GUI 并向 LDAP 用户或组授予 Data Protector 权限。
  - 向 Data Protector 用户组添加 LDAP 用户。
  - 向 Data Protector 用户组添加 LDAP 组。
2. 使用 LDAP 凭据登录。

## 将 LDAP 用户添加至 Data Protector 用户组

要将 LDAP 用户添加至 Data Protector 用户组，请执行以下步骤：

1. 在“上下文列表”中，单击用户。
2. 在“范围窗格”中，展开用户，然后右键单击要向其添加 LDAP 用户的用户组。
3. 单击添加/删除用户打开向导。
4. 在“添加/删除用户”对话框的手动选项卡中，提供以下详细信息：
  - 类型：选择 LDAP。
  - 名称：以 LDAP 用户主体名称格式指定 LDAP 用户。
  - 实体：输入 LDAP 用户。
  - 说明：这是可选字段。
5. 单击完成退出向导。

## 将 LDAP 组添加至 Data Protector 用户组

要将 LDAP 组添加至 Data Protector 用户组，请执行以下步骤：

1. 在“上下文列表”中，单击用户。
2. 在“范围窗格”中，展开用户，然后右键单击要向其添加 LDAP 组的用户组。
3. 单击添加/删除用户打开向导。
4. 在“添加/删除用户”对话框的手动选项卡中，提供以下详细信息：

- **类型：**选择 LDAP。
- **名称：**以判别名称 (DN) 格式指定 LDAP 组名称。
- **实体：**输入 LDAP 组。
- **说明：**这是可选字段。

5. 单击**完成**退出向导。

**注意：**将自动授予 LDAP 用户与其所属 LDAP 组相同级别的权限。

## 使用 LDAP 凭据登录

要使用 LDAP 凭据登录，请执行以下步骤：

1. 启动 Data Protector GUI 并连接至 Cell Manager。
2. 在 LDAP 身份验证屏幕上提供 LDAP 凭据以访问 Data Protector。LDAP 用户可以属于任何可用的 Data Protector 用户组。

## 检查 LDAP 配置

以下过程讲解如何检查是否为特定 LDAP 用户或组正确设置了用户权限，方法是从 Web 浏览器中查询 Data Protector 登录提供程序服务 getDpAc1。

要获取指定用户的 Data Protector 访问控制列表 (ACL)，请执行以下步骤：

1. 使用浏览器连接 Data Protector 登录提供程序 Web 服务。
2. 浏览器可能会提示您接受服务器证书。单击**接受**确认请求。
3. 将显示一个对话框，提示您提供登录凭据。提供已使用 Data Protector 配置的有效 LDAP 用户名和密码。
4. 浏览器将返回以下访问控制列表 (ACL)： `https://<server>:7116/dp-loginprovider/restws/dp-ac1`
5. 使用 ACL 检查所分配的权限是否与为对应 Data Protector 用户组指定的 Data Protector 用户权限相匹配。

## 防火墙支持

### 关于防火墙支持

可以在 Data Protector 进程跨越防火墙进行通信的环境中配置 Data Protector。从 Data Protector 9.09 和 10.00 开始，防火墙中必须打开的端口数量减少。这一变化仅在升级单元后出现，在此之前，旧客户机仍然以旧模式运行，使用与之前 Data Protector 版本相同的开放端口。

无需为 Data Protector 进程的侦听端口设置 OB2PORTRANGE 和 OB2PORTRANGESPEC 变量。仍然可为 Data Protector 设置这些变量，以用于主机中的进程间通信。以下示例解释了使用情况：

#### 示例 1:

Data Protector 9.09 MA 和早期版本的数据保护器 9.09 DA

MA 打开与所有地址绑定的端口。在 netstat 输出中，这显示为 MA 在侦听 0.0.0.0:1234。

- 这里，“1234”是一个例子，实际端口取决于使用 OB2PORTRANGE 变量和数据保护器配置设置的动态端口范围。
- “0.0.0.0”表示“所有地址”，对于 IPv6，相当于 [::]。这表示客户机可以通过任何路由连接。

来自相同主机的其他进程无法打开端口 1234。DA 直接连接至 MA 主机 1234。在防火墙中，您必须打开端口 1234。

#### 示例 2:

Data Protector 9.09 MA 和数据保护器 9.09 DA:

- 由于 MA 不知道连接的 DA 是 Data Protector 版本 9.09 还是更早版本，因此 MA 仍然会打开端口 0.0.0.0:1234。
- 与示例 1 相比，如果您确定将只连接 Data Protector 9.09 客户机时，则不需要在防火墙中打开端口 1234。这取决于您升级主机的顺序。

#### 示例 3:

MA 主机上已启用 Data Protector 9.09 MA、Data Protector 9.09 DA 和数据保护器防火墙

- MA 打开仅与环回接口绑定的端口。在 netstat 输出中，这显示为 MA 在侦听端口 127.0.0.1:1234，或者对于 IPv6，显示为 [::1]:1234。
- 旧 DA 将无法连接，因为无论是 Windows 还是其他一些防火墙，均无法从远程主机访问端口 1234。

#### 注意：

防火墙不阻止进程打开端口，仅连接至来自远程主机的这些端口。

有关 Data Protector 10.00 中端口使用情况的详细信息，请参阅 [Data Protector 9.09 及更高版本中的端口使用情况表](#)。

## Data Protector 中的通信

Data Protector 进程使用 TCP/IP 连接进行通信。Data Protector 需要以下端口：

- 每个 Data Protector 系统上的 Inet 端口(默认为 5555/5565)。

#### 注意：

Windows inet 为多线程。

- Cell Manager 系统上的 IDB 服务端口(默认为 7112)。
- Cell Manager 系统上的应用程序服务器端口(默认为 7116)。
- StoreOnceSoftware.exe 二进制文件的规则必须保留在入站防火墙例外中。由于 StoreOnceSoftware.exe 不支持(基于第三方代码的)单个端口传递，但的确会打开入站端口并接受这些端口上的通信。

在防火墙中，这些端口必须打开(可从远程主机访问)。

此外，Data Protector 会打开许多动态端口。在防火墙中，升级 Data Protector 单元之前，这些端口必须保持打开状态。单元升级到 Data Protector 10.00 或更高版本之后，这些端口在进程 (IPC) 中使用，从防火墙的角度而言，不需要打开。

若要配置动态端口的范围，需要进行以下更改：

- 限制在升级整个单元之前仍然需要在防火墙中打开的端口。
- 防止 Data Protector 打开第三方应用程序可能需要的端口。
- Data Protector 可与可能需要打开自有端口的非 Data Protector 软件通信。

**注意：**

在安装期间，需要为 Inet 打开以下端口：

- 全新 Data Protector 安装 - 5565
- 升级 Data Protector 安装 - 5555

## 配置机制

可以使用两个 omnirc 选项配置端口分配行为：

- OB2PORTRANGE

该选项设置所有 Data Protector 进程从中打开动态端口的端口范围。

- OB2PORTRANGESPEC

在 Data Protector 10.00 和 9.09 之前，端口范围有两个用途：

- 安全性：限制 Data Protector 打开的端口，因此端口用户需要在防火墙中打开。
- 与其他软件的冲突：非 Data Protector 软件可能需要端口 1000-2000 用于特定用途，因此通过使用 OB2PORTRANGE 阻止 Data Protector 使用该范围。这对 OB2PORTRANGE 有效。

**注意：**

- 默认情况下，动态端口由操作系统分配。
- 这些选项不影响 Inet 的固定端口 (5555/5565)、IDB 服务端口 (7112) 和应用程序服务器端口 (7116)。
- 端口范围选项限制 Data Protector 端口使用。它们不能阻止非 Data Protector 应用程序分配来自该范围的端口。

参与通信的代理升级后，防火墙中打开的端口数量会减少。在此之前，Data Protector 使用旧方法进行通信。旧版磁盘代理与新介质代理搭配使用，反之亦然。在升级所有单元主机之前，用户应该使端口保持打开状态。

在 inetd 支持 -p <proc\_limit> 选项的平台上，如果可能，避免使用该选项，否则建议使用大于 2200 的 proc\_limit 值。

启用实际防火墙之前，建议测试 Data Protector 与已启用 Data Protector 防火墙的环境。

要在整个单元中启用 Data Protector 防火墙，请运行以下命令：

```
omnicc -firewall -all -enable_dp
```

要在部分单元中启用 Data Protector 防火墙，请指定单个主机，而非 -all。

例如，要测试磁盘代理是否可以通过防火墙与介质代理通信，请运行以下命令以关闭防火墙：

```
omnicc -firewall -host MAhost DAhost -enable_dp
```

与 `-enable_dp` 选项一起，在 Windows 防火墙中使用 `-enable_os` 选项禁用 Data Protector 规则。

使用这些选项进行测试后，用户可以继续关闭第三方防火墙(例如，路由器)。

## Data Protector 9.09 及更高版本中的端口使用情况

下表提供有关不同 Data Protector 9.09 及更高版本组件的端口要求的信息：

Data Protector 主机	端口要求	应用程序主机上的 Data Protector 的端口要求	应用程序的第三方要求
作为安装目标	Linux/Unix: <ul style="list-style-type: none"><li>• REXEC<sup>1</sup>(不安全): 512</li><li>• RSH(不安全): 514</li><li>• SSH: 22</li></ul> Windows: SMB 服务: 445	无	无
作为 Cell Manager	<ul style="list-style-type: none"><li>• Inet:5555/5565</li><li>• hpdpass: 7116</li><li>• IDB 服务: 7112</li></ul>	无	无
作为 Data Protector 磁盘代理	Inet:5555/5565	无	无
作为 Data Protector 集成代理 <sup>4</sup>	Inet:5555/5565	无	无
作为 Data Protector 介质代理或 NDMP 介质代理	Inet:5555/5565	无	Store Once 重复数据删除系统 <sup>2</sup> <ul style="list-style-type: none"><li>• 命令端口: 9387</li><li>• 数据端口: 9388</li></ul> NDMP 服务器 <sup>2</sup> <ul style="list-style-type: none"><li>• 服务器: 10000</li></ul>



			<b>DDBoost<sup>3</sup></b> <ul style="list-style-type: none"><li>• NFS: 2049</li><li>• 管理的文件复制: 2051</li><li>• NFS 端口映射器: 111</li></ul>
--	--	--	---

<sup>1</sup> 只需要其中一个 REXEC/RSH/SSHD 端口，具体取决于安装方法。

<sup>2</sup> 有关可以打开的其他第三方端口的准确信息，请参考第三方软件文档。

<sup>3</sup> 有关 DDBoost 端口的详细信息，请参考《适用于 OpenStorage 的 EMC® Data Domain® Boost 管理指南》。

<sup>4</sup> 在 Windows Hyper-V 服务器上，对于 Hyper-v 备份和还原，以下端口需要打开

- **WMI 实例: 135(启动)**
- **Windows 远程管理 (HTTPS): 5986**

<sup>5</sup> 在 Windows Hyper-V 服务器上，对于 Hyper-v 备份和还原，以下端口需要打开

编写防火墙配置规则时，第一列中的进程必须能够在第二列中定义的端口上接受来自第三列中列出的进程的新 TCP 连接(设置了 SYN 位)。

此外，第一列中列出的进程必须能够在现有的 TCP 连接(未设置 SYN 位)上答复第三列中的进程。

例如，介质代理系统中的 Inet 进程必须能够在端口 5555/5565 上接受来自 Cell Manager 的新 TCP 连接。介质代理必须能够使用现有的 TCP 连接答复 Cell Manager。介质代理不必能够打开 TCP 连接。

## 限制

- 该功能在 OpenVMS 和 SCO 主机上不可用。如果介质代理(或打开端口的任何 Data Protector 组件)在这些系统上运行，用户仍然需要在防火墙中打开这些端口。

## DMZ 中的磁盘代理、介质代理和应用程序代理

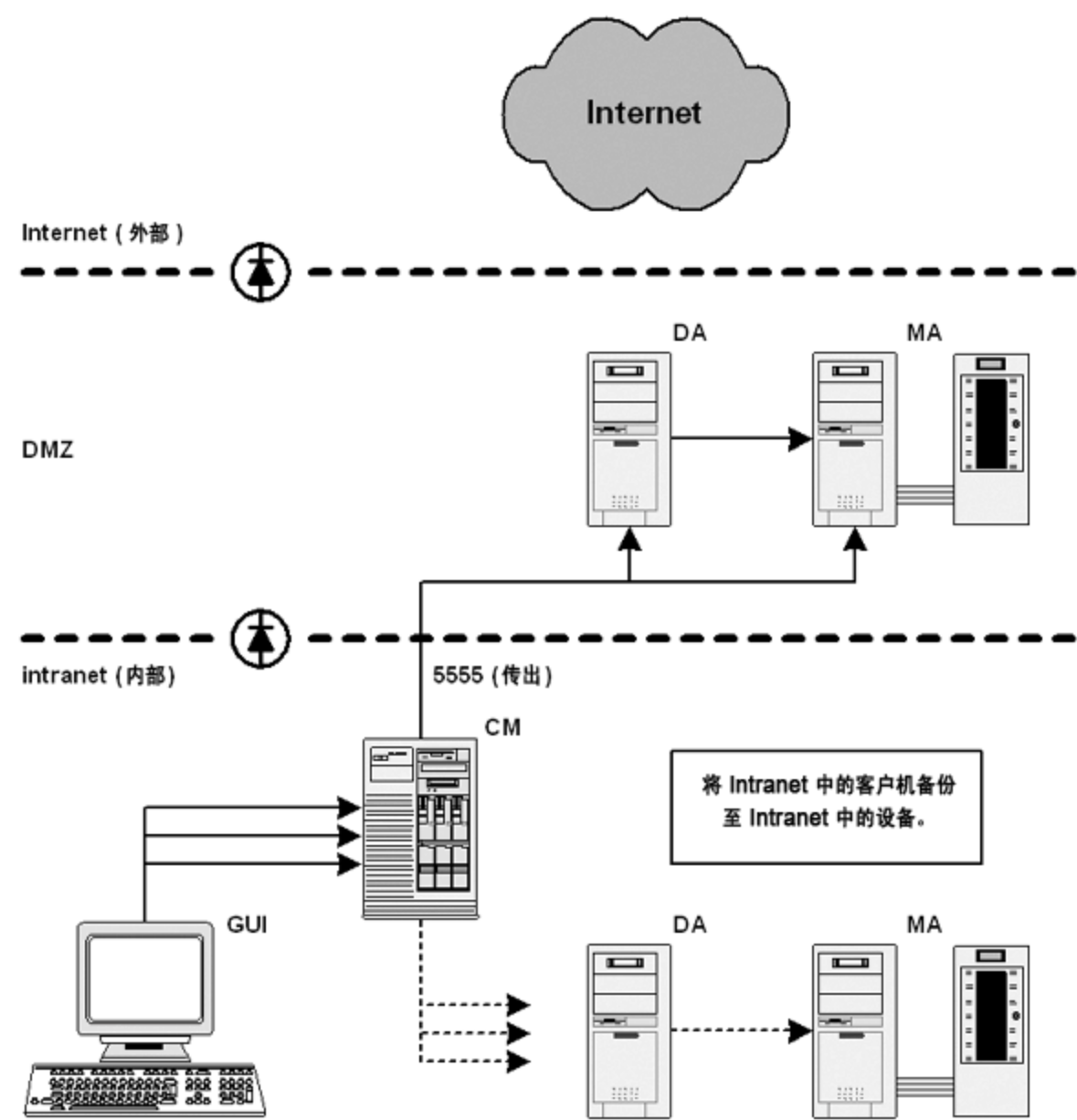
可以配置备份环境，以使 Cell Manager 和 GUI 在内部网中，并使某些磁盘代理、应用程序代理和介质代理在 DMZ 中。

配置图

打开的端口

限制

## 配置图



## 打开的端口

Data Protector 打开以下端口进行配置：

1. 磁盘代理和介质代理需要在端口 5555/5565 上接受来自会话管理器的连接：
  - 允许 CM 系统连接到 DA 系统中的端口 5555/5565
  - 允许 CM 系统连接到 MA 系统中的端口 5555/5565

2. 启用**重新连接已断开的连接**时，MA 和 DA 连接到会话管理器：
  - 允许 MA 和 DA 系统连接到 CM 系统中的端口 5555/5565
3. 应用程序代理需要连接至会话管理器和 CRS：
  - 允许应用程序服务器系统连接到 CM 系统中的端口 5555/5565

**注意：**

第 2 点和第 3 点允许从 DMZ 连接到内部网，这是一个潜在的安全风险。

## 限制

- 此单元可以备份 DMZ 中的客户机以及 Intranet 中的客户机。但是，必须将每组客户机都备份到在位于防火墙同端的客户机上配置的设备。  
如果防火墙不限制从 Intranet 到 DMZ 的连接，则可以将 Intranet 中的客户机备份到在 DMZ 中客户机上配置的设备。但是，建议不要这样做，因为以此方式备份的数据更容易受到攻击。
- 如果 DMZ 中的设备具有在不同客户机上配置的机械手，则此客户机也必须在 DMZ 中。



# 第 3 章：用户和用户组

## 关于用户管理

Data Protector 用户管理功能提供了一个安全层，可以防止未经授权的人员访问系统和数据。

安全基于与用户相关的安全概念。希望使用 Data Protector 的用户须配置为 Data Protector 用户。具有丰富用户权限的用户组使您能够灵活地将安全要求映射到 Data Protector 用户配置中。

默认情况下，除备份所有者以外，备份的数据对其他用户隐藏。其他用户甚至看不到已经备份数据。如果愿意，可以通过适当的用户权限使数据对其他用户可见。

## 用户

要使用 Data Protector，您必须是 Data Protector 授权用户。因此，您需要一个 Data Protector 帐户，并限制对 Data Protector 和备份数据的未授权访问。在小型环境中，一个人足以胜任备份任务。Data Protector 管理员创建此帐户指定用户登录名、用户可以从其中登录的系统，以及 Data Protector 用户组成员身份。每当用户启动 Data Protector 用户界面或执行特定任务时，都会对该信息进行检查。

每个用户仅属于一个用户组。这可以定义用户的用户权限。

您可以配置 UNIX 和 Windows 用户：

## UNIX

用户由登录名、UNIX 用户组和从中登录的系统定义。可以使用通配符。

## Windows

用户由登录名、Windows 域或工作组以及从中登录的系统定义。可以使用通配符。

## 预定义用户

在初始安装之后，除了 admin 组以外，所有默认用户组均为空组。Data Protector 将以下用户添加到 admin 组：

Cell Manager	用户帐户	标注
UNIX Cell Manager	Cell Manager 上的 root 用户 (root、any group、Cell Manager host)。	不应修改此用户帐户。CRS 后台程序和 Cell Manager 上的其他进程的正确操作需要此帐户。  最初仅允许此用户管理单元。要从任何其他客户机管理单元，请添加新用户。

Windows Cell Manager	在 <b>Data Protector</b> 安装期间指定的 <b>CRS</b> 服务帐户(限于 <b>Cell Manager</b> 主机)。	<b>CRS</b> 服务帐户应当保留不变，除非修改 <b>CRS</b> 服务的登录参数。 <b>CRS</b> 后台程序和 <b>Cell Manager</b> 上的其他进程的正确操作需要此帐户。
	安装 <b>Cell Manager</b> 的用户(初始单元管理员)。	此用户配置为初始单元管理员，并且可以从任何客户机管理该单元。建议在 <b>Data Protector</b> 安装完成之后修改此用户帐户。指定将从中管理单元的客户机，而不是允许从任何主机访问。如果要使用另一帐户，则添加此帐户，然后删除初始单元管理员，或仅从 <b>Cell Manager</b> 允许它。
	<b>Cell Manager</b> 上的本地系统帐户 (SYSTEM、NT AUTHORITY、 <i>Cell Manager host</i> )。	在 <b>CRS</b> 服务配置为使用本地系统帐户登录时提供此帐户。

建议在环境中为每种类型的用户定义特定的组，以将分配给他们的权限设置最小化。

有关 java 用户的详细信息，请参见《*Data Protector 安装指南*》。

**重要：**  
Admin 组的功能非常强大。**Data Protector** admin 用户组的成员在整个单元中有系统管理员功能。有关安全的详细信息，请参见《*Data Protector 安装指南*》。

## 用户组

用户组是具有相同权限的用户的集合。通过按照访问需要对用户分组，管理员可以简化用户配置。即，管理员可以将需要相同特定权限的用户放到同一组中。例如，用户可能需要监视单元中的会话、配置备份或还原文件的权限。

**Data Protector** 提供了默认用户组。可以使用提供的这些组、修改它们或者创建新组。

## 预定义用户组

为了简化配置，**Data Protector** 提供了三个具有以下用户权限的预定义用户组：

用户权限	管理员	操作员	用户
客户机配置	✓		
用户配置	✓		
设备配置	✓		
介质配置	✓	✓	

报告和通知	✓		
启动备份	✓	✓	
启动备份规范	✓	✓	
保存备份规范	✓		
作为 root 备份	✓		
切换会话所有权	✓	✓	
监控	✓	✓	
中止	✓	✓	
装载请求	✓	✓	
开始恢复	✓	✓	✓
还原到其他客户机	✓		
从其他用户还原	✓	✓	
作为 root 还原	✓		
查看私有对象	✓	✓	

在初始安装之后，除了 **admin** 用户组以外，所有预定义的组均为空组。

**重要：**

**Admin** 功能非常强大！**Data Protector admin** 用户组的成员在整个单元中有系统管理员权限。

在 **Cell Manager** 上设置的用户权限可确定 **Data Protector Cell Manager GUI** 或从中连接到 **Cell Manager** 的计算机的 **GUI** 上下文的可用性。例如，如果仅设置了“开始还原”用户权限，则在安装用户界面组件时仅有“还原”上下文可用。

## 可用的用户权限

**Data Protector** 提供了一组丰富的用户权限来实现高级安全功能。有关用户权限的更多详细信息，请参见 **Data Protector** 帮助。

## 向用户提供 **Web** 服务访问权限

**Data Protector** 使用 **Web** 服务进行内部通信和管理。某些 **Data Protector** 模块(如 **GUI**)默认配置为访问这些 **Web** 服务。但是，对于某些模块(如高级 **GRE Web** 插件和 **REST API**)，必须显式地向用户提供 **Web** 服务访问权限。

可以使用 **Data Protector GUI** 或使用 **CLI** 来提供 **Web** 服务访问权限。

**注意：**  
无法为 Data Protector 用户类的成员启用 WebAccess。

## 使用 Data Protector GUI

完成以下步骤：

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**，然后选择要向其提供 Web 服务访问权限的用户。
3. 在 Data Protector“用户”对话框“属性”部分的“常规”选项卡中，启用 **WebAccess** 复选框。  
“身份验证”窗口随即打开。
4. 在“密码”文本框中输入密码，然后单击**确定**。
5. 单击**应用**。

## 使用 CLI

根据要创建新用户还是更新现有用户的属性，运行以下命令之一：

- 创建具有 Web 服务访问权限的新用户：  
`omniusers -add -type {U | W} -name <UserName> -webaccess enable -passwd <Password>`
- 更新现有用户：  
`omniusers -webaccess enable -name UserName -passwd Password -group GroupOrDomainName -client ClientName`

有关 omniusers 命令的详细信息，请参见《Data Protector 命令行界面参考指南》。

## 配置用户

### 添加用户

可将用户添加到现有的用户组中，从而对 Data Protector 配置用户。

### 先决条件

需要有用户配置权限才能添加用户。

### 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击要向其添加用户的用户组。
4. 单击**添加/删除用户**打开向导。
5. 在“添加/删除用户”对话框中，输入特定用户属性。在输入**名称**和**组/域**或者 **UNIX 组**



时，确保输入与网络上现有用户相关的信息。

6. 单击 **>>** 将此用户添加到用户列表。

**提示：**

还可以通过在用户列表中选择用户并单击 **<<** 来删除用户。

7. 单击**完成**退出向导。

用户即被添加到用户组，并具有此分配给此组的用户权限。

## 显示用户

使用此过程可以查看特定用户属性。

## 先决条件

您是 **Data Protector** 用户。

## 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，双击要显示的用户。

特定用户属性即显示在结果区域中。

## 更改用户属性

在为 **Data Protector** 配置用户时，可以修改指定的用户属性。但通过将用户分配到另一个组会修改用户组，并因此修改用户权限。

## 先决条件

需要具有用户配置权限才能更改用户属性。

## 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，右键单击要修改的用户。
5. 单击**属性**。
6. 输入要更改的属性。在修改**名称**和**组/域**或者 **UNIX 组**时，确保输入的信息与网络上的现有用户相关。
7. 单击**应用**。

## 将用户移动到另一个用户组

要更改单个用户的用户权限，请将该用户移动到不同用户组。

### 先决条件

需要有用户配置权限才能移动用户。

### 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，右键单击要移动的用户。
5. 单击**移动**。
6. 在“目标组”列表中选择适当的用户组，并单击**确定**。

该用户即从原始用户组中删除，并添加到新用户组。新用户组的权限将分配给该用户。

## 删除用户

通过从配置用户的用户组删除用户，可以将该用户删除。

### 先决条件

需要有用户配置权限才能删除用户。

### 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 单击用户所属的用户组。
4. 在结果区域中，右键单击要删除的用户并单击**删除**。
5. 确认操作。

用户即从用户组删除中，不能再用于 **Data Protector**。

**提示：**  
还可以在“添加/删除用户”对话框中删除用户。

## 配置用户组

### 添加用户组

默认 **Data Protector** 用户组通常就足够了。可以定义自己的用户组，从而根据需要在 **Data Protector** 环境中控制权限的分配。但是，在添加新组之前，通过更改现有组，检查是否可以满足要求。

### 先决条件

必须具备**用户配置**权限。

### 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，右键单击**用户**。
3. 单击**添加用户组**以打开向导。
4. 输入新组的名称和说明。
5. 单击**下一步 (Next)**。
6. 设置新组的特定用户权限。
7. 单击**完成**退出向导。

新的空用户组即被添加到 **Data Protector**。

### 显示用户组

使用此过程可以查看特定用户组属性。

### 先决条件

您是 **Data Protector** 用户。

### 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击用户组。
4. 单击**属性**。

用户组的属性即显示在结果区域中。

## 更改用户权限

可以更改分配到任何用户组(admin 用户组除外)的用户权限，以便该组可以更好地满足您的要求。一个用户组必须至少分配一个用户权限。还可以修改组中每个用户的属性，例如用户所属的域，用户的真实姓名，以及用户所在的用户组。如果选择其中没有任何用户的组，则结果区域将显示该组的属性。如果选择其中有用户的组，则结果区域将列出该组中的用户。通过要在要修改其属性的用户上单击，还可以修改用户组中每个用户的属性。

### 先决条件

- 用户组可能不是 admin 用户组。
- 您必须具有 User configuration 权限。

### 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击要修改的用户组。
4. 单击**属性**，然后单击**用户权限**选项卡。
5. 根据需要更改权限。要将所有用户权限分配到用户组，请单击**全选**。若须更改大量用户权限，请单击**取消全选**从用户组删除所有权限，然后将至少一个用户权限分配到组。
6. 单击**应用**。

指定的用户权限即分配到用户组和属于此组的所有用户。

## 删除用户组

可以删除不再需要的用户组(admin 组除外)。

### 先决条件

- 用户组可能不是 admin 用户组。
- 您必须具有 User configuration 权限。

### 步骤

1. 在“上下文列表”中，单击**用户**。
2. 在“范围窗格”中，展开**用户**。
3. 右键单击要删除的用户组。
4. 单击**删除**。

用户组及其所有用户即从 Data Protector 中删除。

# 第 4 章：内部数据库

## 关于 IDB

内部数据库 (IDB) 是嵌入在位于 **Cell Manager** 上的 **Data Protector** 中的一个数据库，其中保存有关备份哪些数据、数据所在的介质、备份、恢复、对象复制、对象合并、对象验证和介质管理会话的结果以及配置哪些设备和库的信息。

## IDB 的用途是什么？

IDB 中存储的信息可实现以下目的：

- 快速方便地还原  
可以浏览要还原的文件和目录。可以快速找到还原所需的介质，并因加快还原的速度。
- 备份管理  
可以验证备份会话的结果。
- 介质管理  
可以在备份、对象复制和对象合并会话期间分配介质、跟踪介质管理操作和介质属性、介质组集中到不同的介质池中，并且跟踪磁带库中的介质位置。
- 加密/解密管理：利用 IDB 中存储的信息，**Data Protector** 可以为加密的备份或复制会话分配加密密钥，并可提供恢复加密的备份对象所需的解密密钥。

## IDB 大小和增大注意事项

IDB 可以增大到很大的程度，并且会对备份性能和 **Cell Manager** 系统造成显著影响。**Data Protector** 管理员必须了解 IDB 并决定在 IDB 中保存哪些信息以及保存多长时间。使恢复时间和功能与 IDB 的大小和增长保持平衡是管理员的任务。**Data Protector** 提供两个关键参数，日志记录级别和编目保护，帮助您平衡您的需求。

## 定期备份 IDB

Micro Focus 强烈建议定期备份 IDB。有关详细信息，请参见 [IDB 备份配置](#)。

## IDB 体系结构

内部数据库 (IDB) 由以下几部分组成：

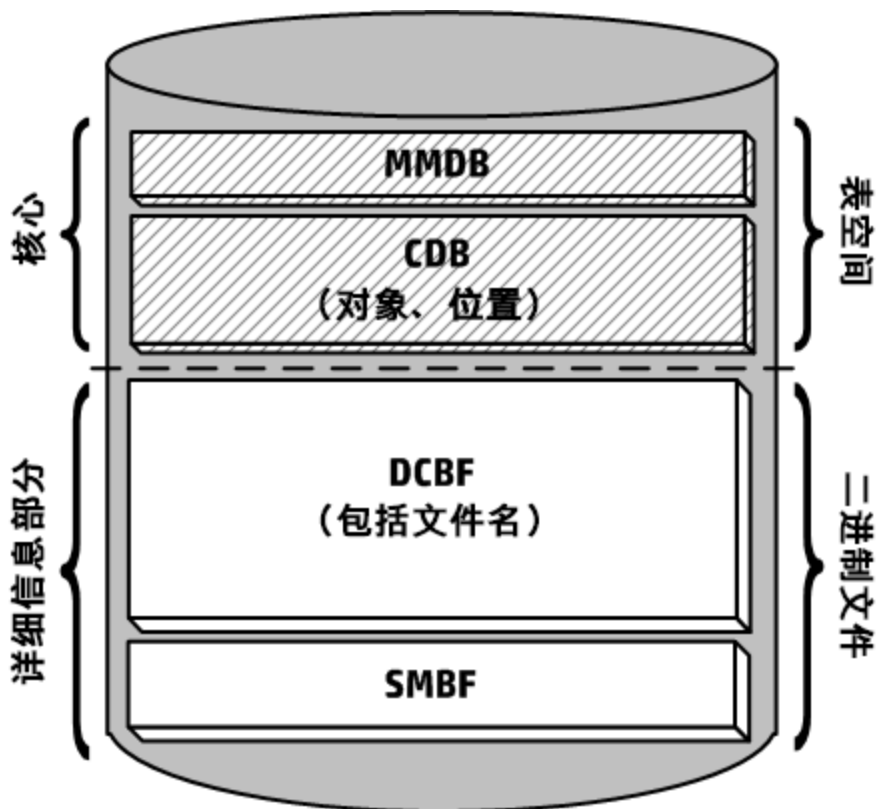
- 介质管理数据库 (MMDB)
- 编目数据库 (CDB)
- 详细编目二进制文件 (DCBF)

- 会话消息二进制文件 (SMBF)
- 加密密钥库和编目文件

IDB 的每个部分都存储了某些特定的 Data Protector 信息(记录)，以不同方式影响 IDB 大小和增大，位于 Cell Manager 上一个单独的目录中。

## IDB 的各个部分

### 数据库架构



MMDB 和 CDB 部分使用由表空间构成的嵌入式数据库来实现。此数据库由 hdp-idb、hdp-idb-cp 和 hdp-as 进程控制。CDB(对象和位置)和 MMDB 是 IDB 的核心部分。

IDB 的 DCBF 和 SMBF 部分由二进制文件构成。更新直接进行(无事务)。

在管理器的管理器 (MoM) 环境中，MMDB 可以移至中心系统，以创建中心介质管理数据库 (CMMDB)。

## 介质管理数据库 (MMDB)

### MMDB 记录

介质管理数据库存储有关以下各项的信息：

- 配置的设备、库、库驱动器和插槽
- Data Protector 介质
- 配置的介质池和介质盒

## MMDB 大小和增大

MMDB 的大小不会变得非常大。MMDB 中最大的部分通常由有关 Data Protector 介质的信息占用。

## MMDB 位置

MMDB 位于以下目录中：

**Windows 系统：** `Data_Protector_program_data\server\db80\idb`

**UNIX 系统：** `/var/opt/omni/server/db80/idb`

## 编目数据库 (CDB)

### CDB 记录

编目数据库存储有关以下各项的信息：

- 备份、还原、对象复制、对象合并、对象验证和介质管理会话。这是发送到 Data Protector“监视”窗口的信息的副本。
- 备份的对象、对象版本和对象副本。如果是加密的对象版本，则还会存储密钥标识符 (KeyID-StoreID)。
- 所备份的对象在介质上的位置。对于每个备份对象，Data Protector 都会存储有关其备份所用介质和数据段的信息。对于对象副本和对象镜像也是如此。

## CDB(对象和位置)大小和增大

CDB 记录占用 IDB 中很小的一部分空间。

## CDB 位置

CDB 位于以下目录中：

**Windows 系统：** `Data_Protector_program_data\server\db80\idb`

**UNIX 系统：** `/var/opt/omni/server/db80/idb`

## 详细编目二进制文件 (DCBF)

### DCBF 信息

“详细编目二进制文件”部分存储有关以下内容的信息：

- 备份文件(文件名)的路径名以及客户机系统名称。两次备份之间创建的文件的文件名添加到 DCBF 中。
- 文件元数据。这是有关备份文件版本、其文件大小、修改时间，属性/保护以及备份副本在备份介质上的位置的信息。

将为每个 Data Protector 备份介质创建一个 DC(Detail Catalog)二进制文件。介质被覆盖时，将删除旧的二进制文件并创建一个新的。

## DCBF 大小和增大

在文件系统备份一般都使用全部记录 (Log all) 选项的环境中，DCBF 占 IDB 的最大部分。日志记录级别和编目保护可用于指定 IDB 中实际存储的信息和存储时长。

默认情况下，为 DC 二进制文件配置五个 DC 目录。如果备份介质或 DC 二进制文件的数量变得极大或者您遇到磁盘空间问题，可以创建多个目录，从而扩展 IDB 的大小。

DCBF 中最大且增长最快的部分是文件名部分。

文件名部分的增长与备份环境的增长和动态变化以及备份次数成正比。

在 IDB 中文件或目录大约占用 100 字节。

## DCBF 位置

默认情况下，DCBF 位于以下目录中编号从 dcbf0 到 dcbf4 的子目录中：

**Windows 系统：** *Data\_Protector\_program\_data\server\db80\dcbf*

**UNIX 系统：** */var/opt/omni/server/db80/dcbf*

考虑 Cell Manager 上的磁盘空间，并重新定位 DC 目录(如有必要)。可以创建更多个 DC 目录，并将其定位到不同的磁盘。

## 会话消息二进制文件 (SMBF)

### SMBF 记录

会话消息二进制文件部分存储备份、还原、对象复制、对象合并、对象验证和介质管理会话期间生成的会话消息。对于每个会话会创建一个二进制文件。文件按年份和月份进行分组。

## SMBF 大小和增大

SMBF 大小取决于以下因素：

- 执行的会话数。
- 会话中的消息数。一个会话消息大约占用 200 字节。通过更改报告级别选项，可更改在执行备份、还原和介质管理操作时显示的消息量。这会影响存储在 IDB 中的消息量。



## SMBF 位置

SMBF 位于以下目录中：

**Windows 系统：** *Data\_Protector\_program\_data\server\db80\msg*

**UNIX 系统：** */var/opt/omni/server/db80/msg*

可以通过编辑 `SessionMessageDir` 全局选项重新定位目录。

## 加密密钥库和编目文件

所有在加密备份期间创建的密钥，无论是手动还是自动创建，都存储在密钥库中。密钥也可用于对象复制、对象验证和还原会话。如果是硬件加密，密钥也可用于对象合并会话。

对于软件加密，密钥标识符(每个密钥标识符由 **KeyID** 和 **StoreID** 构成)会映射到加密的对象版本中。该映射存储在编目数据库中。介质中不同的对象可以有不同的(软件)加密密钥。

对于硬件加密，密钥标识符会映射到介质 ID，这些映射存储在编目文件中。该文件包含将加密介质导出到其他单元所需的信息。

## 密钥库位置

密钥库位于以下目录中：

**Windows 系统：** *Data\_Protector\_program\_data\server\db80\keystore*

**UNIX 系统：** */var/opt/omni/server/db80/keystore*

## 编目文件位置

编目文件位于以下目录中：

**Windows 系统：** *Data\_Protector\_program\_data\server\db80\keystore\catalog*

**UNIX 系统：** */var/opt/omni/server/db80/keystore/catalog*

## IDB 操作

了解以下 Data Protector 操作期间 IDB 的行为：

- 备份
- 恢复
- 对象副本和对象合并
- 对象验证
- 导出介质
- 删除详细编目

## 备份

备份会话启动时，将在 **IDB** 中创建会话记录。此外，对于会话中的每个对象还会创建一个对象版本记录。这两种记录都存储在 **CDB** 部分中，并具有多种属性。备份会话管理器在备份期间会更新介质。所有介质记录都存储在 **MMDB** 部分中，并根据相关策略为备份分配这些记录。

在磁带上写入数据段(在它之后写入目录段)后，对于作为此数据段一部分的每个对象版本在 **CDB** 中都存储一个介质位置记录。此外，还会在详细编目 (**DC**) 二进制文件中存储该编目。每个 **Data Protector** 介质都将保留一个 **DC** 二进制文件。**DC** 二进制文件的名称为 *MediumID\_TimeStamp.dat*。向同一介质追加备份时不更改此名称。如果在备份期间覆盖了该介质，则将删除旧的 **DC** 二进制文件，然后创建新的 **DC** 二进制文件。

备份期间生成的所有会话消息都存储在会话消息二进制文件(**SMBF** 部分)中。

## IDB 备份和归档日志文件

根据内部数据库备份规范的配置，**IDB** 备份过程可以删除旧的归档日志文件并开始创建 **IDB** 恢复所必需的新归档日志文件。

## 恢复

配置恢复时，**Data Protector** 在 **CDB** 和 **DCBF** 部分中执行一组查询，以使用户能够浏览所备份数据的虚拟文件系统。这些浏览查询分为两步完成。第一步是选择特定对象(文件系统或逻辑驱动器)。如果此对象存储了许多备份版本，则此操作需要一些时间，因为 **Data Protector** 将扫描 **DCBF** 以生成查找缓存供以后浏览。第二步是浏览目录。

选择特定的文件版本后，**Data Protector** 确定所需的介质，并定位所选文件使用的介质位置记录。这些介质则由介质代理读取，并将数据发送到用于恢复所选文件的磁带客户机。

## 对象副本和对象合并

在对象副本或对象合并会话期间，将运行与备份和还原会话期间相同的进程。大体上是，像还原数据一样从源介质读取数据，然后像备份数据一样将数据写入目标介质。对象复制或对象合并会话对 **IDB** 操作的影响与备份和恢复相同。有关详细信息，请参见前面的各节。

## 对象验证

对象验证会话期间，运行与还原会话期间相同的数据库进程。大体上是，像还原数据一样从源介质读取数据，然后将数据发送到执行验证的主机的磁带客户机。对象验证会话对 **IDB** 操作的效果与还原会话相同。有关详细信息，请参见上面的“还原”一节。

验证会话期间生成的所有会话消息都存储在会话消息二进制文件中。

## 导出介质

导出介质后将删除以下各项：

- 从 CDB 部分中删除该介质中的所有介质位置记录。
- 从 CDB 部分中删除目前在任何其他介质上都没有位置的所有对象。
- 删除过时会话(其介质已被覆盖或导出)。同时还会删除这些会话的会话消息。
- 从 MMDB 部分中删除介质记录，并从 DCBF 部分中删除该介质的 DC 二进制文件。

## 删除详细编目

删除特定介质的详细编目时，同时还会删除其 DC 二进制文件。删除该介质上所有对象版本的编目保护也能达到相同结果(DC 二进制文件的下一次每日维护时将删除该二进制文件)。所有其他记录仍然保留在 CDB 和 MMDB 部分中，并可以从此类介质中运行恢复(但无法浏览)。

## 配置内部数据库

### IDB 配置

内部数据库配置有助于管理以下各项：

- IDB 和可用磁盘空间的大小
- IDB 目录的位置
- IDB 自身的备份，在 IDB 损坏或发生灾难时需要此备份
- IDB 报告和通知的配置

需要提前准备，以便能够及时在任何时间点恢复 IDB。IDB 还原将还原 IDB 中存储的信息，并且必须进行此还原才能在 Cell Manager 受到灾难打击时还原备份的数据。IDB 恢复的准备由以下各项组成：

- 检查稳定性注意事项
- 重新定位 IDB 目录
- 配置 IDB 备份
- 定期备份 IDB

配置 IDB 后，维护的工作量即降到最低，主要是对通知和报告采取的行动。

## 为 IDB 分配磁盘空间

内部数据库最终会在 Cell Manager 占用相当大量的磁盘空间。需要提前规划，并考虑分配 IDB 在未来需要的磁盘空间。

## 先决条件

- 需要了解影响 IDB 增大的关键因素，如文件数、文件动态、环境增大等等。
- 需要根据环境要求和可用磁盘空间设置日志记录级别和编目保护策略。
- 需要估计未来的 IDB 大小(未来 IDB 所需的磁盘空间)。

## 需要多少磁盘空间？

根据定义和操作备份中使用的许多配置方面和策略，容纳 IDB 的磁盘空间将显著不同。

以下环境简化场景中，3 个月后 IDB 大约需要 900 MB 磁盘空间，并且以后很少会增大：

- 要备份 100 个系统(每个系统 10,000 个文件；没有邮件服务器)
- 数据卷合计 350 GB
- 文件系统备份的典型动态为每月有 3% 的新文件
- 每周进行一次完整备份和四次增量备份
- 日志记录级别设置为全部记录(可方便地浏览文件名，然后再恢复)。这是最繁重的日志记录选项。
- 完整备份的编目保护设置为三个月，增量备份为两周。

**注意：**

IDB 中如果采用大型配置或较长的编目保护期，则 IDB 需要 20 GB 以上的容量。

## 提前规划哪些内容？

通常 IDB 在开始阶段增大速度很快(直到到达目录保留期为止)。在这之后，IDB 的增大主要由每月新文件占很大比例的系统的动态以及环境(要备份的新系统)的增大决定。

了解不同的 IDB 增大函数很重要：

- IDB 部分(包含文件名和文件元数据)的大小与备份数、单元中的已备份文件数以及编目保护的持续时间成正比。
- 预测归档日志文件占用的存储空间并非易事。影响大小的重要因素是 IDB 备份之间所备份的新文件名数和整体备份活动(如果预定备份是主要操作，则为周)。

## IDB 目录的位置

内部数据库位于 Cell Manager 上。您可能希望重新定位某些 IDB 目录，并遵照建议以优化稳定性。

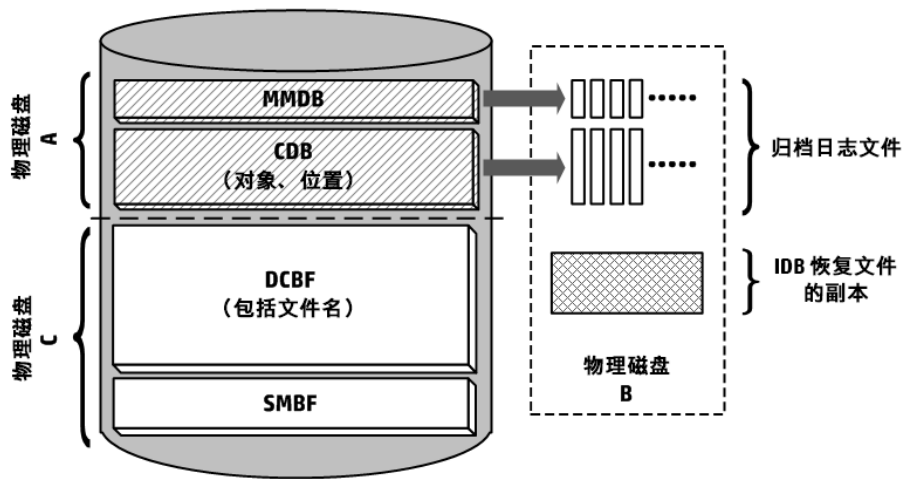
## 限制

- IDB 文件只能位于本地连接磁盘(未使用 NFS 装载或映射为网络共享文件夹)上的卷中。
- 如果在群集中安装 IDB，则必须将其安装在群集组(Microsoft 服务器群集)或群集包(Serviceguard)中的卷上。

- 如果 IDB 安装在群集中，则必须将其安装在群集组 (Microsoft 服务器群集)、群集包 (Serviceguard) 或群集服务组 (Symantec Veritas Cluster Server) 中的卷上。

## 建议 IDB 目录所在的位置

IDB 部分	Windows 系统中的位置	UNIX 系统中的位置	能否重新定位
表空间 (CDB、 MMDB)	<i>Data_Protector_ program_ data\server\db80\idb</i>  <i>Data_Protector_ program_ data\server\db80\jce</i>  <i>Data_Protector_ program_ data\server\db80\pg</i>	<i>/var/opt/omni/server/db80/idb</i>  <i>/var/opt/omni/server/db80/jce</i>  <i>/var/opt/omni/server/db80/pg</i>	目录路径固定，但可以装载不同的卷。
二进制文件 (DCBF、 SMBF)	<i>Data_Protector_ program_ data\server\db80\dcbf</i>  <i>Data_Protector_ program_ data\server\db80\msg</i>  <i>Data_Protector_ program_ data\server\db80\meta</i>	<i>/var/opt/omni/server/db80/dcbf</i>  <i>/var/opt/omni/server/db80/msg</i>  <i>/var/opt/omni/server/db80/meta</i>	可以修改目录路径。此外，可以装载单独的卷。
归档日志文件	<i>Data_Protector_ program_ data \server\db80\pg\pg_ xlog_archive</i>	<i>/var/opt/omni/server/db80/pg/pg_ xlog_archive</i>	目录路径固定，但可以装载不同的卷。
IDB 恢复文件	<i>Data_Protector_ program_data \server\db80\logfiles \rlog</i>	<i>/var/opt/omni/server/db80/logfiles/rlog</i>	可以在所需位置放置文件的副本。



## 稳定性注意事项

- IDB 的核心部分、CDB(对象，位置)和 MMDB 对于 Data Protector 的运行至关重要。
- 无需 IDB 的 DCBF 和 SMBF 部分即可执行 Data Protector 的基本操作(如备份和还原)。但是，如果没有这些部分，则还原就不太方便(不能浏览文件)，并且会丢失会话消息。
- 如果 IDB 恢复文件和归档日志文件丢失，则不会影响正常操作，但 IDB 还原会困难得多，并且无法重放自上次 IDB 备份以来生成的 IDB 数据。而是需要重新导入使用过的介质。

## IDB 备份配置

管理 Data Protector 单元的关键部分是配置 IDB 备份本身。在进行灾难准备时，可以执行的最重要任务是定期执行 IDB 备份。在 Cell Manager 发生灾难时，脱机恢复 IDB 对于恢复其他备份数据至关重要。

要创建 IDB 备份规范，请在备份上下文的“范围窗格”中选择**内部数据库**，然后按照标准的备份过程操作。有关详细信息，请参见[创建备份规范](#)。

## 准备和运行 IDB 备份规范的提示

配置 IDB 备份时，请考虑以下各项：

- 排定每天至少执行一次 IDB 备份。这样可确保始终有 IDB 的当前备份。安排它在 Cell Manager 上活动较少的时候运行。

### 警告：

始终应在对 IDB 配置进行任何修改后备份内部数据库，例如，在更改“内部数据库服务”和“应用程序服务器”用户帐户的密码后。未执行此操作可能会导致无法成功执行联机 IDB 恢复或脱机 IDB 恢复。

- IDB 备份的设备和介质选择，将对灾难之后执行 IDB 恢复的难易程度或可能性产生巨大的影响。

- 使用可以通过自动配置进行配置的设备能够大大简化设备配置。
- 如果使用文件介质库设备，请确保介质库位于包含 IDB 的驱动器以外的其他磁盘驱动器上。
- 如果可能，请使用本地连接到 Cell Manager 的设备。
- 不要使用文件库，因为无法将文件库介质导入到文件库。
- StoreOnce 软件 (SOS) 介质的导入可能十分复杂，因此如果已经记录并测试 SOS 介质导入，请仅使用 SOS 设备进行 IDB 备份。在专用备份设备中的单独备份介质上，使用单独的介质池执行 IDB 备份。
- 确保了解哪些介质用于 IDB 备份。可以配置会话介质报告以收到有关用于备份的介质的通知。这样可大大简化最终的还原。
- 设置数据和编码保护，以便拥有足够的 IDB 备份副本，满足业务需求。
- 除非绝对必要，请勿禁用自动 IDB 一致性检查。控制一致性检查的检查内部数据库备份选项默认情况下处于选中状态。
- 要提高数据的机密性，可以将加密与 IDB 备份配合使用。IDB 备份包括密钥库。

**注意：**

必须有活动的加密密钥，然后才能启动加密的 IDB 备份，因为备份 IDB 期间无法创建新密钥。  
在加密 IDB 备份期间，加密密钥将自动导出到默认 Data Protector 导出加密密钥目录下的 IDBClientName-keys.csv 文件中。  
必须格外注意备份之后的密钥。发生灾难时，需要密钥进行恢复。运行加密 IDB 备份之后，将使用的相应密钥复制到一个非常安全的位置。

- IDB 备份的设备和介质选择，将对灾难之后执行 IDB 恢复的难易程度或可能性产生巨大的影响。StoreOnce 软件 (SOS) 介质的导入可能十分复杂，因此如果已经记录并测试 SOS 介质导入，请仅使用 SOS 设备进行 IDB 备份。在专用备份设备中的单独备份介质上，使用单独的介质池执行 IDB 备份。

**注意：**不支持 IDB 备份到在灾难恢复之后导入的 StoreOnce Software (SOS) 介质。

- 强烈建议记录并测试 DP IDB 恢复过程。

## 维护内部数据库

### 关于 IDB 维护

如果已配置内部数据库通知和报告，则会通知您是否需要执行维护任务。应执行何种维护任务取决于当前 IDB 情况。

情况	可能会通知您，方法是 <sup>1</sup>	执行以下操作
IDB 空间用尽	"IDB 空间不足"通知	扩展 IDB 大小

		减小 IDB 增大 减小 IDB 当前大小
要检查 IDB 大小	“IDB 大小”报告	检查 IDB 大小
IDB 运行不正常 - 可能已损坏	“IDB 损坏”通知	检查 IDB 一致性

<sup>1</sup> 只有在配置了通知和报告的情况下，您才能收到它们。

**注意：**

Micro Focus 建议定期检查 Data Protector 事件日志，并检查是否有最终的 IDB 事件。管理员可能会考虑设置由电子邮件发送的通知，以便对传入的通知做出快速反应。

## 内部数据库的增大及性能

### 关于 IDB 增大和性能

要配置和维护内部数据库，必须了解影响 IDB 增大和性能的关键因素和参数。

此处给出的数据适用于文件系统备份，并阐明最坏的情况(最大或增大最快的 IDB)。如果执行磁盘映像，应用程序集成或 NDMP 备份，则 IDB 中只会存储少量数据。

### IDB 增大关键因素

IDB 增大取决于环境和 Data Protector 设置，这些设置定义希望 Data Protector 保留多少历史记录和详细信息以便可以浏览和搜索文件。

关键因素	对 IDB 增大的影响
有关环境的文件和大小的详细信息	Data Protector 可以跟踪文件的每个版本。这意味着在每次备份期间，都将向每个备份文件的 DCBF 部分中存储一个文件名记录(大约 100 字节)。
(完整)备份的频率	备份越频繁，在 IDB 中存储的信息就越多。如果文件系统不常发生变化，则只有 DCBF 部分会增长。
对象副本数	创建的对象副本和对象镜像越多，IDB 中存储的信息就越多。IDB 中存储的对象副本和对象镜像的信息均与备份对象相同。

### IDB 性能关键因素

关键因素	备份期间对 IDB 负载和性能的影响
并行驱动器数	同时运行的(磁带)驱动器数影响 IDB 上的负载。例如，如果在 10 个备份会话中同时运行 10 个驱动器，或在 5 个会话中同时运行 10 个驱动器，则数据库上的负载几乎相同。每个新驱动器意味着必须在数据库中存储另一个目录源。



文件平均大小	如果备份小文件，则可以更快地生成目录，并且 IDB 的负载因此也更高。
IDB 磁盘性能	备份期间 Data Protector 的主要活动是读写磁盘。因此，用于 IDB 的 Cell Manager 上磁盘(子系统)的速度会影响性能。

## IDB 增大和性能关键参数

关键参数	对 IDB 增大的影响	对 IDB 性能的影响
日志记录级别	定义向 IDB 中写入有关文件和目录的数据量以及所需的存储空间。	浏览数据进行还原的便利程度的影响。
编目保护	定义有关所备份数据的信息(如文件名和文件版本)在 IDB 中保留多久。  如果编目保护到期，不会立即从 IDB 中删除数据。而是将在整个介质上数据的所有编目保护都到期的那一天删除这些数据。	无。

根据为编目保护所设置的时间段(相对较短的一段时间，时间段与数据保护相同)以及有效的日志记录级别，实际 IDB 增长会有所不同。在编目保护到期之前，IDB 的主要增大将持续。在那之后，增大就降低到最小程度，并由备份环境的增大决定。

## 日志记录级别对 IDB 的影响

不同的日志记录级别设置影响内部数据库增长、浏览文件系统进行恢复的便利程度，在极少的情况下还会影响备份性能。

下方提供的数据适用于文件系统备份。如果执行磁盘映像，联机数据库或 NDMP 备份，则 IDB 中只会存储少量数据。

无日志 (No Log)	仅存储对象信息，通常每个文件系统对象 2 kB。
记录目录 (Log Directories)	与不记录任何内容相同，额外存储每个备份的目录占用 30 字节。
日志文件	与记录目录相同，额外存储每个备份的文件占用 12 字节。
全部记录 (Log All)	与记录文件相同，额外存储每个备份的文件占用 18 字节。

## 编目保护对 IDB 的影响

内部数据库的最大部分与编目保护期和所选的日志记录级别成正比。编目保护期内执行的备份越多，IDB 中积累的数据就越多。换句话说，它是存储每个文件所需的数据乘以编目保护期内备份的文件数得到的。

目录保护到期后，并不会立即从 IDB 中删除信息。Data Protector 每天自动删除一次这些信息。由于 IDB 中的信息是按介质排列的，因此只有在介质上所有对象的编目保护都到期时，才会删除这些信息。如果这样，特定 DC 二进制文件占用的整个空间将变为空闲。

应设置编目保护，以使其至少包括上一次完整备份。例如，可以将完整备份的编目保护设为 8 周，将增量备份的编目保护设为 1 周。

## IDB 大小估计

如果主要执行文件系统备份，则内部数据库在某些条件下可能会增长到相当可观的大小(几 TB)。如果执行磁盘映像或联机数据库备份，则 IDB 很可能不会超过几 GB。

## DC 目录维护

IDB 允许在存储 IDB 详细编目二进制文件 (DCBF) 部分的位置注册多个目录。这样可以将 DC 二进制文件分发到更多磁盘或卷上。默认情况下，有五个目录，其名称分别为从 dcbf0 到 dcbf4。

每个 DCBF 目录都有多个配置参数：

- 分配顺序
- 路径
- 最大大小
- 最大文件数
- 空间不足

有关配置参数的详细信息，请参见 Data Protector 帮助。

需要创建新的二进制文件时，Data Protector 就会执行“DCBF 分配过程”：

1. 从所有可能的 DC 目录的列表中，Data Protector 清除所有停用或消失的目录。请注意，在缺少 DC 目录的情况下，将生成 IDBCorrupted 事件。

不考虑所有已满的 DC 目录。如果至少以下一个条件属实，则 DC 目录即为已满：

Maximum size - Current size < Low space

Free disk space < Low space

Maximum files <= Current files

2. 一组用户可选择的算法(DCDirAllocation 全局选项)选择实际 DC 目录：

- Fill in sequence

Data Protector 按照配置的顺序在第一个不完整 DC 目录中创建新的 DC 二进制文件。

- Balance size

Data Protector 选择包含(与总大小的有效限制成正比)最少的 DCBF 数据的 DC 目录。选择以下值的最小者：

$(\text{Maximum size} - \text{Current size} - \text{Low space}) / (\text{Maximum size} - \text{Low space})$

- Balance number

**Data Protector** 选择包含(与文件数的有效限制成正比)最少的 DC 二进制文件的 DC 目录。选择以下值的最小者：

Current files / Maximum files

请参见影响 DCBF 行为的 DCDirAllocation 和 MaxDCDirs 全局选项。

## 检查 IDB 大小

可以使用 **Data Protector GUI** 检查内部数据库各个部分的当前大小。

此外，如果已配置，则“IDB 大小报告”以及“IDB 空间不足”通知会告知您 IDB 大小。

### 步骤

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**使用情况**项。将显示以下 IDB 项目：编目数据库、介质管理数据库、详细编目二进制文件、会话消息二进制文件及无服务器集成二进制文件。  
“无服务器集成二进制文件”项与安装的 **Data Protector** 版本中不再支持的功能相关。
3. 通过查看 IDB 各个部分及其记录的属性，检查 IDB 的大小：
  - 右键单击 IDB 项目，例如**编目数据库**，然后单击**属性**以查看 IDB 部分的磁盘使用情况。磁盘使用情况显示 IDB 的特定部分当前占用了多少磁盘空间。单击**记录统计信息**选项卡，以查看 IDB 特定部分中所有记录的统计信息。
  - 要检查 DC 目录的磁盘使用情况，请展开**详细编目二进制文件**，双击 DC 目录，然后单击**磁盘使用情况**选项卡。

## 减小 IDB 增大

通过降低备份、对象复制和对象合并规范的日志记录级别和编目保护设置，可以减小内部数据库的增大。这些操作不影响 IDB 的当前大小，但影响其未来的增大。

降低日志记录级别会使还原时浏览起来不太方便。

减少编目保护的效果是某些还原(即已超过编目保护的那些备份的还原)中无法浏览。

以下过程介绍如何在备份规范中更改这些设置。

### 降低日志记录级别

通过降低备份规范的日志记录级别，减少存储在 IDB 上的数据(文件/目录)的数量(**全部记录 -> 日志文件 -> 日志目录 -> 无日志**)。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型(例如**文件系统**)。此时将显示所保存的全部备份规范。

3. 双击要更改其日志记录级别的备份规范，然后单击**选项**选项卡。
4. 在“选项”属性页中，单击相应的高级按钮(在**文件系统选项**下)。
5. 单击**其他**选项卡，并在**日志记录**下，更改日志记录级别。
6. 单击**确定 (OK)**应用更改。

## 降低编目保护

通过降低编目保护，只能降低对 IDB 中还原浏览信息的保护。仍将在介质上存储信息。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 双击要更改其编目保护的备份规范，然后单击**选项**选项卡。
4. 在“选项”属性页中，单击相应的高级按钮(在**文件系统选项**下)。
5. 单击**选项**选项卡，并在**编目保护**下，更改编目保护。
6. 单击**确定 (OK)**应用更改。

## 减小 IDB 当前大小

通过将编目保护设置更改为完整的备份、对象复制或对象合并会话(会话中所有对象)，或更改为仅特定对象，降低内部数据库当前大小。

减少编目保护的效果是某些还原(即已超过编目保护的那些备份的还原)中无法浏览。

此操作不影响将来的 IDB 增大。

更改将在以下情况下生效：

- 如果从介质上的所有对象中删除了编目保护。
- 每天在 **Data Protector** 从 IDB 中自动删除过时数据时(默认情况下为中午)进行。可以使用 **DailyMaintenanceTime** 全局选项指定时间。请使用二十四小时制表示法。

可以通过运行 **omnidbutil -purge -dcbf** 命令立即启动清除。有关从 IDB 中删除其他过时项目的信息，请参见 **omnidbutil** 手册页或 **Data Protector** 命令行界面参考。

通过更改编目保护，只能更改对 IDB 中还原浏览信息的保护。仍将在介质上存储信息。因此，如果导出介质，再将其导回，则 **Data Protector** 将从介质重新读取有关编目保护的信息。

## 更改对会话的编目保护

更改对备份会话的保护可更改对会话中所备份所有对象的保护。

## 步骤

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**会话**项。
3. 右键单击要更改其保护的会话，然后单击**更改编目保护**。
4. 指定会话的新编目保护，然后单击**完成**应用更改。

## 更改对于对象的编目保护

更改对特定对象的保护可更改对此对象的保护，无论是在哪个会话中备份该对象。

## 步骤

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**对象**项。
3. 右键单击要更改其保护的對象，然后单击**更改编目保护**。
4. 指定对象的新编目保护，然后单击**完成**应用更改。

## 扩展 IDB 大小

由于 IDB 的详细信息部分(备份对象的名称、版本和元数据)需要更多可用磁盘空间存储，因此您可能需要通过创建新的 DC 目录或重新配置现有目录以获得更大容量来扩展内部数据库。

## 重新配置 DC 目录以获得更大容量

可以通过修改分配序列、最大大小、最大文件数或空间不足选项重新配置现有 DC 目录。请注意，选定 DC 目录中的文件数和当前总大小可能会限制调整范围。

## 步骤

1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中，展开**使用情况**，然后展开**详细编目二进制文件**。
3. 右键单击选定 DC 目录的路径，然后单击**属性**。
4. 在结果区域中，根据需要修改可用选项。
5. 单击**完成**以应用更改。

## IDB 一致性检查

内部数据库的内容必须在逻辑上正确，换句话说各个 IDB 部分必须一致且有序。可以手动对 IDB 的特定部分和整个 IDB 执行一致性检查。

Data Protector 默认情况下在备份 IDB 之前检查 IDB 的一致性(快速检查)。这样做对在 Cell Manager 遇到灾难时恢复 IDB 和备份的数据极其重要。

IDB 检查类型	检查的内容	命令
IDB 的快速检查	核心(MMDB 和 CDB)、文件名以及简单检查 DCBF 部分。	omnidbcheck -quick
DCBF 部分的简单检查	DC 二进制文件是否存在及其大小。	omnidbcheck -bf
DCBF 部分的完整检查	介质位置的一致性和 DC 二进制文件。	omnidbcheck -dc
检查 SMBF 部分	是否存在会话消息二进制文件。	omnidbcheck -smbf
介质一致性检查	介质的一致性。还会在介质一致性失败时列出不一致的介质名称。	omnidbcheck -media_consistency
架构一致性检查	IDB 架构的一致性。还会在 Data Protector 安装期间检测架构中自最初创建以来的所有更改。	omnidbcheck -schema_consistency
数据库一致性检查	数据库的一致性。还会在数据库一致性失败时列出错误。	omnidbcheck -database_consistency
IDB 的扩展检查	执行除 SMBF 检查之外的所有检查。	omnidbcheck -extended

## 将 IDB 移至不同的 Cell Manager

可以将内部数据库移至运行于相同操作系统上的不同 Cell Manager。

在第一个场景中，即从 Data Protector 客户机上的备份设备执行 IDB 恢复，请进行如下操作：

### 步骤

1. 在 Data Protector 客户机 *client.company.com* 上准备备份设备 *PreparedDevice*。
2. 使用备份设备 *PreparedDevice* 运行 IDB 备份。
3. 在主机 *cmb.company.com* 上准备新的 Data Protector Cell Manager 全新安装。
4. 从主机 *cma.company.com* 上的 Cell Manager 导出客户机 *client.company.com*。
5. 将客户机 *client.company.com* 导入主机 *cmb.company.com* 上的新 Cell Manager。
6. 将备份设备 *PreparedDevice* 导入新的 Cell Manager。
7. 从 *PreparedDevice* 备份设备运行 IDB 恢复。
8. 停止 Data Protector 服务。

9. 对于位于 standalone.xml 配置文件中的所有密码(keystore-password、truststore-password、ssl password 和 ca-certificate-password)，使用来自 webservice.properties 配置文件的 KeystorePassword。

这些配置文件可从以下位置获取：

**Windows:**

- ProgramData\OmniBack\Config\client\components\webservice.properties
- ProgramData\OmniBack\Config\server\AppServer\standalone.xml

**UNIX:**

- /etc/opt/omni/client/components/webservice.properties
- /etc/opt/omni/server/AppServer/standalone.xml

10. 启动 Data Protector 服务。
11. 将客户机从原始 Cell Manager 导入新的 Cell Manager。

**重要：**

每个客户机以前必须从原始 Cell Manager 导出过。

12. 重新将 GUI 连接到新的 Cell Manager。

在第二个场景，从原始 Cell Manager 上的备份设备执行 IDB 还原，请执行如下操作：

## 步骤

1. 在原始 Cell Manager 上准备备份设备 *PreparedDevice*。
2. 使用备份设备 *PreparedDevice* 运行 IDB 备份。
3. 在主机 *cmb.company.com* 上准备新的 Data Protector Cell Manager 全新安装。
4. 从原始 Cell Manager 导出备份设备 *PreparedDevice*。
5. 将备份设备 *PreparedDevice* 导入主机 *cmb.company.com* 上的新 Cell Manager。
6. 从 *PreparedDevice* 备份设备运行 IDB 恢复。
7. 停止 Data Protector 服务。
8. 对于位于 standalone.xml 配置文件中的所有密码(keystore-password、truststore-password、ssl password 和 ca-certificate-password)，使用来自 webservice.properties 配置文件的 KeystorePassword。

这些配置文件可从以下位置获取：

**Windows:**

- ProgramData\OmniBack\Config\client\components\webservice.properties
- ProgramData\OmniBack\Config\server\AppServer\standalone.xml

**UNIX:**

- /etc/opt/omni/client/components/webservice.properties
- /etc/opt/omni/server/AppServer/standalone.xml

9. 启动 Data Protector 服务。
10. 将客户机从原始 Cell Manager 导入新的 Cell Manager。

**重要：**  
每个客户机以前必须从原始 Cell Manager 导出过。

11. 重新将 GUI 连接到新的 Cell Manager。

## 自定义 Data Protector 全局选项

在 Data Protector 全局选项文件中，可以修改全局选项的值或添加新的全局选项。

### 先决条件

- 您的用户帐户必须是 Data Protector Admin 用户组的成员。

## 使用 GUI 设置全局选项


### 步骤


要使用 GUI 设置全局选项，请执行以下操作：


1. 在上下文列表中，单击**内部数据库**。
2. 在范围窗格中的**内部数据库**下，单击**全局选项**。

结果区域中将显示 **Data Protector 全局选项**表，该表包含六列：

- 组 - 代表选项所属的上下文部分。
- 使用中 - 指示选项的状态。所选选项处于活动状态，而空复选框指示在全局选项文件中注释掉的不活动选项。
- 名称
- 来源 - 表示从中加载选项的文件。
- 值 - 表示选项的当前设置值。
- 说明 - 告知您如何使用选项。

3. 要修改选项，请在结果窗格内的“值”列中单击要更改的值，再单击“编辑”按钮  并输入一个新值。单击**保存**保存该选项。

要添加选项，请单击“添加”图标 ，在对话框中填写选项参数，然后单击**添加**。

4. 在结果窗格顶部，单击“保存”按钮 。

还可以在保存前修改多行。

要更改该表的外观，请使用表标题中的过滤器。



如果在保存过程中有任何内容出错，则会在全局选项文件夹中创建名为 `global.old` 的原始全局选项文件副本。

## 通过编辑全局文件自定义选项

除了使用 GUI 外，还可在文本编辑器中编辑 `global` 文件，以设置 **Data Protector** 全局选项。

### 警告：

**Micro Focus** 建议使用 GUI 设置全局选项，因为它可确保在保存时验证更改，并减小由于超出范围或无效设置、意外删除或是录入和拼写错误而导致问题的概率。

## 步骤

1. 打开任何文本编辑器
2. 在文本编辑器中，打开 `global` 文件，该文件位于默认 **Data Protector** 服务器配置目录的 `options` 子目录中。
3. 要激活选项，请删除其名称前的 `#` 标记并将其设置为所需值。
4. 以 Unicode 格式保存文件。

## 配置 IDB 报告

通过配置内部数据库报告，可以在需要执行某些 IDB 维护任务(如扩展 IDB 大小和减小 IDB 增大)时告知您。

### IDB 报告

报告	告知您...
内部数据库大小报告	... IDB 特定部分的大小。

## 配置 IDB 通知

通过配置内部数据库通知，可以在需要执行某些 IDB 维护任务(如扩展 IDB 大小、检查 IDB 一致性等等)时告知您。

### IDB 通知

通知	告知您...
IDB 空间不足	... IDB 空间用尽。
IDB 限制	... 如果任何 <b>MMDB</b> 或 <b>CDB</b> 部分达到其限制。
需要执行 IDB 备份	... 如果 IDB 备份不够频繁或者连续增量 IDB 备份太多。

## 还原 IDB

可以从标准 IDB 备份过程中创建的备份映像还原内部数据库 (IDB)。如果 IDB 损坏，则无法使用此还原过程，而是需要执行一种 IDB 恢复方法。

要还原内部数据库，请执行以下操作：

- 还原 IDB

从加密的 IDB 备份进行还原时，还需要执行额外的步骤，然后才能进行实际还原：

- 从加密备份准备 IDB 还原

## 还原 IDB

在联机还原内部数据库期间，基本 IDB 部分 (CDB、MMDB、SMBF) 仅能还原到与原始 IDB 不同的位置，而 Cell Manager 配置数据和 IDB 的详细编目二进制文件 (DCBF) 部分可以还原到原始位置或其他位置。

## 先决条件

- 根据内部数据库备份映像的大小，确保 Cell Manager 上有足够的空闲磁盘空间可用。

## 限制

SG 群集设置不支持通过选项“使用已还原的数据库作为新的内部数据库”将已还原的 IDB 用作新的 IDB。可以在会话报告中设置 omnirc 变量 OB2SGENABLED，它提供将已还原的 IDB 用作新 IDB 的步骤。设置 omnirc 变量时，会话报告中会出现以下消息：

[警告] 来自：OB2BAR\_POSTGRES\_BAR@<主机名> "DPIDB" 时间：<日期时间>

[175:316]不支持在群集环境中自动替换内部数据库。

单击消息中的错误编号，了解将已还原的 IDB 用作新 IDB 所需要遵循的步骤的详细信息。

## 步骤

1. 在“上下文列表”中，单击**还原**。
2. 在范围窗格中，展开**还原对象**，然后展开**内部数据库**。
3. 展开从中备份 IDB 的 Cell Manager 并单击**内部数据库**。
4. 在“内部数据库属性”页上，要还原内部数据库的基本部分，请将**还原内部数据库**选项保持选中状态。IDB 的基本部分是编目数据库 (CDB)、介质管理数据库 (MMDB) 和会话消息二进制文件 (SMBF)。指定要在还原期间用于内部数据库服务的临时端口，以及 IDB 的基本部分应还原到的位置。

此外，决定是否使用存档的日志文件执行内部数据库恢复，以及是否应将还原的 IDB 作为单元的新内部数据库投入使用。

5. 选择**还原目录二进制文件**以还原 IDB 的 DCBF 部分，并选择其还原位置：
6. 指定是否 Data Protector 应将 IDB 还原到特定时间点，其中该时间不为上一次创建 IDB

备份映像的时间。在这种情况下，内部数据库的基本部分将还原到上一轮的备份状态，然后再恢复到指定时间。

7. 在**配置文件**属性页上，进行有关 **Cell Manager** 配置数据还原的选择。如果选择该数据进行还原，还应指定其备份对象的版本、恢复位置并指定 **Data Protector** 如何处理仍存在于原始位置的配置文件。
8. 在**选项**属性页上，指定还原会话的可选 **pre-exec** 和 **post-exec** 命令。
9. 在**设备**属性页上，进行有关会话中使用哪些设备的选择。
10. 在**介质**属性页上，检查将用于还原 IDB 的备份介质。(可选)调整 **Data Protector** 在会话期间将考虑使用的优先级。
11. 从“操作”菜单，选择**启动还原**，或在结果窗格中，单击**还原**。
12. 单击**完成 (Finish)**。

**重要：**

在时间点 IDB 还原会话后，将特定文件从 `auditing_IDBRestoreSessionID_NNNNNNNNNN` 目录复制到原始的 `auditing` 目录。这将使审计信息与还原的 IDB 的状态一致。应复制以下审计日志：

`YYYY_MM_DD.med`

`YYYY_MM_DD.obj`

`YYYY_MM_DD.ses`

以上文件名中，`YYYY`、`MM` 和 `DD` 字符串对应于“内部数据库”属性页上**还原至**选项指定的日期。

**注意：**

还原后，您可能希望检查 IDB 一致性。

## 从加密备份准备 IDB 还原

在加密 IDB 备份期间，加密密钥将自动导出到默认 **Data Protector** 导出加密密钥目录下的 `IDB-ClientName-keys.csv` 文件中。

还原 IDB 之前，进行如下操作：

### 步骤

1. 将 `IDB-ClientName-keys.csv` 文件传输到将执行 IDB 还原的 **Cell Manager**。
2. 通过运行以下命令导入密钥：

```
omnikeytool -import CSVFile
```

**Cell Manager** 将使用联机 KMS 中的密钥对包含 IDB 备份的介质上的数据进行解密。

## 关于 IDB 恢复

如果所有或某些 IDB 文件不可用或损坏，则需要恢复内部数据库。

IDB 问题分为三种级别，每种级别都有各自的修复方法：

- 解决由操作系统配置问题(如未装载文件系统、名称服务问题等等)导致的 IDB 问题。
- 忽略或删除 IDB 中有问题的非核心部分(二进制文件)。如果确认的 IDB 损坏级别为 **minor** (损坏不在 IDB 的核心部分)，则可以执行此操作。
- 执行由 IDB 还原和自上次 IDB 备份以来更新 IDB 组成的完整恢复。如果确认的 IDB 损坏级别为 **critical**(损坏在核心部分)，则必须采取此操作。

## 完整恢复(自上次 IDB 备份以来还原和更新 IDB)

完整恢复由两个阶段组成：

1. IDB 还原，此阶段使 IDB 恢复上一个(可用)一致状态。
2. 将 IDB 从上一个一致状态更新到上次 IDB 仍正常运行的时刻。

根据在发生问题之前为 IDB 恢复所做准备的充足程度(IDB 恢复文件、IDB 备份映像、原始备份设备和归档日志文件的可用性)，恢复过程可能不同。如果上述各项都可用，则可以使用一种非常方便的 IDB 恢复方法，在指导下进行自动恢复。

## IDB 恢复方法的概述

可使用多种恢复方法恢复内部数据库。根据所确认的损坏级别，您的要求以及 IDB 恢复文件、原始备份设备和归档日志文件的可用性，恢复过程会有所不同。

## 最方便的完整恢复

此恢复方法指导您完成还原 IDB 和重放归档日志文件的过程。如果归档日志文件不可用，则通过导入自上一次 IDB 备份以来的所有介质，仍可以更新 IDB。

损坏级别	问题类型	当前情况	恢复过程
Critical	缺少完整的 IDB，或损坏了核心部分。	IDB 恢复文件和用于 IDB 备份的原始设备可用。	执行 <a href="#">指导下的自动恢复(恢复 IDB 和重放归档日志文件)</a> (如果可能)。否则，按照“更多恢复方法”下给出的某种方法进行操作。

## 省略(删除)损坏的 IDB 部分

如果确认的损坏级别为 **minor**(损坏不在核心部分)，则可以考虑省略(删除)IDB 的丢失或损坏部分，或改为执行完整 IDB 恢复。

损坏级别	问题类型	恢复过程
Minor	DC 二进制文件丢失或损坏。	<a href="#">处理 IDB DCBF 部分中的 Minor 损坏</a>

## 更多恢复方法

以下这些恢复过程可适应多种特定的情况。它们假定要恢复完整 IDB，但因某些原因无法执行指导下的自动恢复方法。恢复由还原 IDB 和更新 IDB 组成。

还原

当前情况	注解	恢复过程(还原 IDB)
IDB 恢复文件可用，但已更改了用于 IDB 备份的原始设备。	此方法本质上与指导下的自动恢复方法相同，但接受的指导较少、更复杂和花费时间更多。	使用 IDB 恢复文件和更改的设备还原 IDB
IDB 恢复文件不可用。	此方法本质上与指导下的自动恢复方法相同，但接受的指导较少、更复杂和花费时间更多。	在无 IDB 恢复文件的情况下还原 IDB
要从特定 IDB 备份(不是最新的那个)恢复 IDB。	此方法并不提供 IDB 的最新状态作为结果。	从特定的 IDB 会话中还原 IDB

自上一次 IDB 备份以来更新 IDB

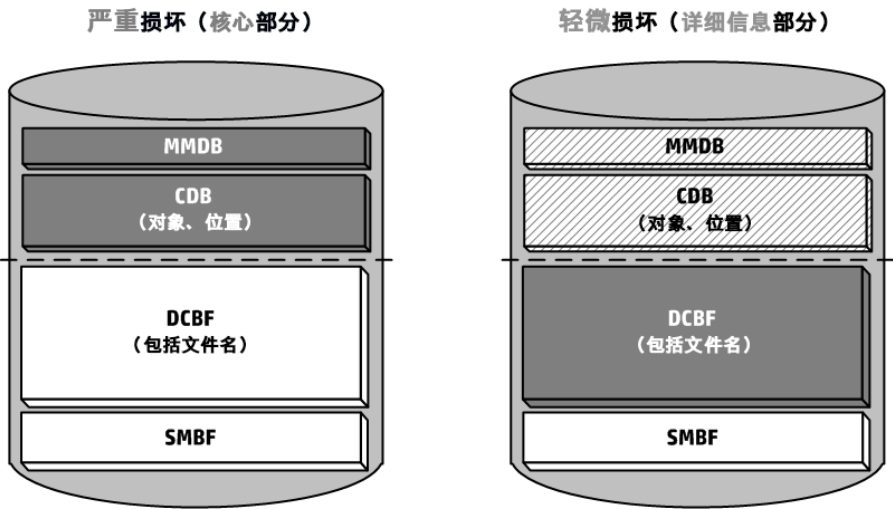
当前情况	恢复过程(更新 IDB)
归档日志文件不可用。	通过导入介质更新 IDB

## IDB 损坏级别

内部数据库损坏分为两个级别：严重和轻微。级别取决于 IDB 中发生损坏的部分。

可以使用 IDB 一致性检查确定 IDB 的哪个部分损坏。

根据损坏的级别，IDB 恢复过程有所不同。



## 确认 IDB 损坏的级别

确认损坏的级别，以便选择相应的内部数据库恢复方法。

### 步骤

1. 使用 `omnidbcheck -extended` 命令确认损坏的级别。

**注意：**

扩展检查可能会花费相当长的一段时间。可以改为运行 `omnidbcheck` 命令的某些部分。例如，运行 `omnidbcheck -connection` 以确认 IDB 的连接是否正常工作。

确认损坏的级别之后，执行相应的恢复过程。

## 执行指导下的自动恢复(还原 IDB 和重放存档的日志文件)

指导下的自动恢复是最方便的内部数据库恢复方法。如果 IDB 恢复文件和用于 IDB 备份的原始设备以及 IDB 备份介质都可用，则可以执行该方法。

该方法指导您还原 IDB 并重放上一次 IDB 备份以来的归档日志文件。如果存档日志文件不可用，仍可以通过导入介质更新上一次 IDB 备份的 IDB。

事务重放将更新 IDB 的核心部分。不更新二进制文件，并因此将丢失对二进制文件的更改。直到 IDB 损坏为止，以下各项才对从上一次 IDB 备份中运行的备份可用：

- 会话消息
- 浏览文件版本(可还原完整对象)。在备份使用的介质上执行导入目录以恢复更改。

### 先决条件

- 根据内部数据库备份映像的大小，确保 Cell Manager 上有足够的空闲磁盘空间可用。
- 确保 Cell Manager 上的总 RAM 是《Data Protector 产品声明、软件说明和参考中》Data Protector Cell Manager 安装要求中所述的两倍。如果 Cell Manager 是 UNIX 系统，请确保其核心参数 `shmmax` 设置为同一部分中所述的所需值的两倍。
- 在与 IDB 备份时相同的目录(在 Windows 系统中，必须分配相同驱动器号)上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 IDB 恢复到不同磁盘/卷布局的过程进行操作。可以使用 `omniofflr` 命令的 `-preview` 选项查看要将文件还原到的位置。
- 在 Cell Manager 和连接设备(首选用于 IDB 备份的设备)的系统上安装 Data Protector。
- 如果在 Serviceguard 上安装 IDB，则在执行指导下的自动恢复之前，必须在活动节点上运行以下命令：
  1. `cmhaltpkg PackageName`，其中 `PackageName` 是 Data Protector 群集包的名称。此命令可停止 Data Protector 包，并卸载 Data Protector 共享卷组。
  2. `vgchange -a e /dev/vg_name`，其中 `vg_name` 是 Data Protector 共享卷组的名称。此命令将激活 Data Protector 共享卷组。要列出系统上的卷组，请运行 `ll /dev/*/group`。

3. `mount /dev/vg_name/lv_name/MountPoint`, 其中 *MountPoint* 是 Data Protector 共享卷组的装载点名称。此命令将装载 Data Protector 共享卷组。

指导下的自动恢复完成后, 运行活动节点上的 `cmrunpkg PackageName` 命令以启动 Data Protector 包。

- 如果在 Symantec Veritas Cluster Server 上安装 IDB, 请使活动节点上的 Data Protector 应用程序资源脱机, 然后再执行指导下的自动恢复。

指导下的自动恢复完成后, 使活动节点上的 Data Protector 应用程序资源联机以启动 Data Protector 服务。

- 如果在 Microsoft 群集服务器上安装 IDB, 则使用群集管理器实用程序使 OOBVS\_HPDP\_AS, OOBVS\_HPDP\_IDB, 和 OOBVS\_HPDP\_IDB\_CP 群集组脱机, 并停止活动节点上的 Inet 服务, 然后再执行指导下的自动恢复。指导下的自动恢复完成后, 使用群集管理器实用程序联机使 OOBVS\_HPDP\_AS, OOBVS\_HPDP\_IDB, OOBVS\_HPDP\_IDB\_CP, 和 OOBVS\_MCRC 群集组联机, 然后重新启动 Inet 服务。

## 步骤

1. 运行 `omniofflr -idb -autorecover` 命令。

此命令读取 IDB 恢复文件, 如果将 IDB 备份记录到文件, 则它将停止服务, 并就地启动 IDB 的还原。将使用 IDB 恢复文件中的数据自动生成所有选项。

还原完成后, `omniofflr` 检查是否有归档日志文件可供重放。如果存档日志文件可用, 则将要求您确认日志的重放。如果取消此步骤或存档日志文件不可用, 则输出将告知您如何通过以下操作从上一次 IDB 备份以来更新 IDB:

- 导入介质
- 查找存档日志文件并在稍后重放

重放日志文件或导入介质以更新 IDB 后, 就应该成功恢复了完整 IDB。

## 处理 IDB DCBF 部分中的 Minor 损坏

如果检测严重程度为轻微的内部数据库损坏, 则它意味着某些 DC 二进制文件丢失或损坏。如果是这种情况, 则不需要进行完整 IDB 恢复。可以通过从介质导入目录, 方便地重新创建二进制文件。根据损坏类型选择恢复过程:

## 在 DC 二进制文件丢失的情况下进行恢复

组织 DC 二进制文件, 以使对于每个介质都有一个二进制文件。如果某些 DC 二进制文件丢失, 则某些介质的介质位置将指向不存在的文件。当浏览相关的文件系统时, 就会显示错误消息。

## 步骤

1. 从 `omnidbcheck -bf` 输出中, 找出丢失的二进制文件的介质 ID。运行 `omnimm -media_info medium-id` 命令以获取介质的其他属性, 如介质标签和介质池。

2. 运行 `omnidbutil -fixmpos` 命令以在介质位置 (mpos) 和二进制文件之间建立一致性。
3. 从介质导入编目，以重新创建二进制文件。

## 在 DC 二进制文件损坏的情况下进行恢复

如果 DC 二进制文件损坏，可以删除 DC 二进制文件并通过导入具有正确日志记录级别的介质来重新创建它们。删除文件所产生的唯一影响是某些介质位置将指向不存在的二进制文件，因此在浏览相关的文件系统时将显示错误消息。

### 步骤

1. 从 `omnidbcheck -dc` 输出中，找出损坏的 DC 二进制文件的介质 ID。运行 `omnimm -media_info medium-id` 命令以获取介质的其他属性，如介质标签和介质池。
2. 找出受影响介质的 DC 二进制文件。DC 二进制文件的名称为：*MediumID\_TimeStamp.dat* (在 MediumID 中，冒号“:”替换为下划线“\_”)。
3. 删除损坏的 DC 二进制文件。
4. 运行 `omnidbutil -fixmpos` 命令以在介质位置 (mpos) 和二进制文件之间建立一致性。
5. 从介质导入编目，以重新创建二进制文件。

## 使用 IDB 恢复文件和更改的设备还原 IDB

如果 IDB 恢复文件可用，但用于 IDB 备份的原始设备与用于恢复的不同，或者介质位于不同插槽中，则使用此过程可以恢复内部数据库。

### 先决条件

- 在与 IDB 备份时相同的目录 (在 Windows 系统中，必须分配相同驱动器号) 上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 IDB 恢复到不同磁盘/卷布局的过程进行操作。可以使用 `omniofflr` 命令的 `-preview` 选项查看要将文件恢复到的位置。
- 如果可能，则将 `media.log` 文件从以前的安装移至安全位置。此文件将向您提供从上一次 IDB 备份以来有关所用介质的信息。如果归档日志文件不可用，则这对更新 IDB 很有用。
- 在 Cell Manager 和连接设备 (首选用于 IDB 备份的设备) 的系统上安装 Data Protector。
- 如果在 Serviceguard 上安装 IDB，则在执行指导下的自动恢复之前，必须在活动节点上运行以下命令：
  1. `cmhaltpkg PackageName`，其中 `PackageName` 是 Data Protector 群集包的名称。此命令可停止 Data Protector 包，并卸载 Data Protector 共享卷组。
  2. `vgchange -a e /dev/vg_name`，其中 `vg_name` 是 Data Protector 共享卷组的名称。此命令将激活 Data Protector 共享卷组。要列出系统上的卷组，请运行 `ll /dev/*/group`。
  3. `mount /dev/vg_name/Lv_name/MountPoint`，其中 `MountPoint` 是 Data Protector 共享卷组的装载点名称。此命令将装载 Data Protector 共享卷组。

指导下的自动恢复完成后，运行活动节点上的 `cmrunpkg PackageName` 命令以启动 Data Protector 包。

- 如果在 Symantec Veritas Cluster Server 上安装 IDB，请使活动节点上的 Data Protector 应用



程序资源脱机，然后再执行指导下的自动恢复。

指导下的自动恢复完成后，使活动节点上的 **Data Protector** 应用程序资源联机以启动 **Data Protector** 服务。

- 如果在 **Microsoft** 群集服务器上安装 **IDB**，则使用群集管理器实用程序使 **OBVS\_HPDP\_AS**，**OBVS\_HPDP\_IDB**，和 **OBVS\_HPDP\_IDB\_CP** 群集组脱机，并停止活动节点上的 **Inet** 服务，然后再执行指导下的自动恢复。指导下的自动恢复完成后，使用群集管理器实用程序联机使 **OBVS\_HPDP\_AS**，**OBVS\_HPDP\_IDB**，**OBVS\_HPDP\_IDB\_CP**，和 **OBVS\_MCRS** 群集组联机，然后重新启动 **Inet** 服务。

## 步骤

1. 运行以下命令，创建含有还原作业选项的文本文件：

```
omniofflr -idb -autorecover -save C:\TEMP\restjob.txt -skiprestore -logview
```

指定的 **-logview** 命令在会话 **ID** 旁列出第一个归档日志文件。请记住要还原的会话的第一个存档日志文件，因为您需要它才能在还原之后更新 **IDB**。例如，在输出 **2013/02/09-2 AAAAAAH** 中，要记住第一个归档日志文件 **AAAAAAH** 才能恢复 **2013/02/09-2 session**。

所创建的 **restjob.txt** 文件包含有关(在执行 **IDB** 备份时)介质最初所在的原始设备和插槽的信息。

2. 修改 **restjob.txt** 文件，指定介质当前所在的当前设备或插槽。

3. 使用 **omniofflr -idb -read C:\TEMP\restjob.txt** 命令运行恢复。

此命令指导您完成以下过程：还原 **IDB** 和重放从上一次 **IDB** 备份以来的存档日志文件。如果归档日志文件不可用，则通过导入自上一次 **IDB** 备份以来所使用的所有介质，仍可以更新 **IDB**。

## 在无 **IDB** 恢复文件的情况下还原 **IDB**

如果 **IDB** 恢复文件不可用，则使用此过程恢复内部数据库。

### 先决条件

- 在与 **IDB** 备份时相同的目录(在 **Windows** 系统中，必须分配相同驱动器号)上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 **IDB** 恢复到不同磁盘/卷布局的过程进行操作。可以使用 **omniofflr** 命令的 **-preview** 选项查看要将文件恢复到的位置。
- 如果可能，则将 **media.log** 文件从以前的安装移至安全位置。此文件将向您提供从上一次 **IDB** 备份以来有关所用介质的信息。如果归档日志文件不可用，则这对更新 **IDB** 很有用。
- 在 **Cell Manager** 和连接设备(首选用于 **IDB** 备份的设备)的系统上安装 **Data Protector**。
- 如果在 **Serviceguard** 上安装 **IDB**，则在执行指导下的自动恢复之前，必须在活动节点上运行以下命令：
  1. **cmhaltpkg PackageName**，其中 **PackageName** 是 **Data Protector** 群集包的名称。此命令可停止 **Data Protector** 包，并卸载 **Data Protector** 共享卷组。
  2. **vgchange -a e /dev/vg\_name**，其中 **vg\_name** 是 **Data Protector** 共享卷组的名称。此命

令将激活 Data Protector 共享卷组。要列出系统上的卷组，请运行 `ll /dev/*/group`。

3. `mount /dev/vg_name/lv_name/MountPoint`，其中 *MountPoint* 是 Data Protector 共享卷组的装载点名称。此命令将装载 Data Protector 共享卷组。

指导下的自动恢复完成后，运行活动节点上的 `cmrunpkg PackageName` 命令以启动 Data Protector 包。

- 如果在 Symantec Veritas Cluster Server 上安装 IDB，请使活动节点上的 Data Protector 应用程序资源脱机，然后再执行指导下的自动恢复。

指导下的自动恢复完成后，使活动节点上的 Data Protector 应用程序资源联机以启动 Data Protector 服务。

- 如果在 Microsoft 群集服务器上安装 IDB，则使用群集管理器实用程序使 OBVS\_HPDP\_AS, OBVS\_HPDP\_IDB, 和 OBVS\_HPDP\_IDB\_CP 群集组脱机，并停止活动节点上的 Inet 服务，然后再执行指导下的自动恢复。指导下的自动恢复完成后，使用群集管理器实用程序联机使 OBVS\_HPDP\_AS, OBVS\_HPDP\_IDB, OBVS\_HPDP\_IDB\_CP, 和 OBVS\_MCRS 群集组联机，然后重新启动 Inet 服务。

## 步骤

1. 使用 Data Protector GUI 配置设备。
2. 查找含有最新 IDB 备份的介质。
3. 将该介质插入设备中，然后使用以下命令显示介质的内容：

```
omnimlist -dev device_name
```

对于 IDB 还原，需要介质 ID 和磁带客户机 ID 用于要还原的备份会话。

4. 使用以下命令显示有关设备配置的信息：

```
omnidownload -dev device_name
```

对于 IDB 还原，需要以下信息：

- Mahost(介质代理主机)
- 策略(号)：可使用以下转换来获得策略号：1 表示独立设备、3 表示堆栈器设备、5 表示介质库设备、6 表示外部控制设备、8 表示 GRAU DAS 带库、9 表示 StorageTek ACS 带库以及 10 表示 SCSI 带库。
- 介质类型(号)：介质类型号定义为 `scsitab` 文件中的介质类。有关位置，请参见[对新设备的支持](#)主题。
- SCSI 地址
- 机械手 SCSI 地址(仅当使用交换器库设备时)

5. 使用所得到的信息运行 `omniofflr` 命令：

```
omniofflr -idb -policy PolicyNumber -type MediaTypeNumber [-ioctl  
RoboticsSCSIAddress] -dev SCSIAddress -mahost MAClientName -maid MediumID -daid  
DiskAgentID
```

例如，可以使用以下命令从介质 ID 为 0100007f:3a486bd7:0410:0001 且磁带客户机 ID 为 977824764 的备份会话恢复 IDB，其中使用类型为 DLT、连接到系统 `company.dot.com` 且 SCSI 地址为 `scsi0:1:2:0` 的独立设备执行：

```
omniofflr -idb -policy 1 -type 10 -dev scsi0:1:2:0 -mahost company.dot.com -  
maid 0100007f:3a486bd7:0410:0001 -daid 977824764
```

此命令指导您完成以下过程：恢复 IDB 和重放从上一次 IDB 备份以来的归档日志文件。如果日志文件不可用，仍可以通过导入从上一次 IDB 备份以来的所有介质更新 IDB。

## 从特定的 IDB 会话中还原 IDB

如果 IDB 恢复文件可用，则使用此过程可从最新备份以外的备份恢复内部数据库。

### 先决条件

- 在与 IDB 备份时相同的目录(在 Windows 系统中，必须分配相同驱动器号)上装载与灾难之前相同大小的磁盘。如果无法确保这一点，则按照将 IDB 恢复到不同磁盘/卷布局的过程进行操作。可以使用 `omniofflr` 命令的 `-preview` 选项查看要将文件恢复到的位置。
- 如果可能，则将 `media.log` 文件从以前的安装存储到安全位置。此文件将向您提供从上一次 IDB 备份以来有关所用介质的信息。如果归档日志文件不可用，则这对更新 IDB 很有用。
- 在 Cell Manager 和连接设备(首选用于 IDB 备份的设备)的系统上安装 Data Protector。
- 如果在 Serviceguard 上安装 IDB，则在执行指导下的自动恢复之前，必须在活动节点上运行以下命令：
  - `cmhaltpkg PackageName`，其中 `PackageName` 是 Data Protector 群集包的名称。此命令可停止 Data Protector 包，并卸载 Data Protector 共享卷组。
  - `vgchange -a e /dev/vg_name`，其中 `vg_name` 是 Data Protector 共享卷组的名称。此命令将激活 Data Protector 共享卷组。要列出系统上的卷组，请运行 `ll /dev/*/group`。
  - `mount /dev/vg_name/Lv_name/MountPoint`，其中 `MountPoint` 是 Data Protector 共享卷组的装载点名称。此命令将装载 Data Protector 共享卷组。

指导下的自动恢复完成后，运行活动节点上的 `cmrunpkg PackageName` 命令以启动 Data Protector 包。

- 如果在 Symantec Veritas Cluster Server 上安装 IDB，请使活动节点上的 Data Protector 应用程序资源脱机，然后再执行指导下的自动恢复。

指导下的自动恢复完成后，使活动节点上的 Data Protector 应用程序资源联机以启动 Data Protector 服务。

- 如果在 Microsoft 群集服务器上安装 IDB，则使用群集管理器实用程序使 OBVS\_HPDP\_AS, OBVS\_HPDP\_IDB, 和 OBVS\_HPDP\_IDB\_CP 群集组脱机，并停止活动节点上的 Inet 服务，然后再执行指导下的自动恢复。指导下的自动恢复完成后，使用群集管理器实用程序使 OBVS\_HPDP\_AS, OBVS\_HPDP\_IDB, OBVS\_HPDP\_IDB\_CP, 和 OBVS\_MCRS 群集组联机，然后重新启动 Inet 服务并运行 `omnidbutil -fixmpos` 命令。

### 步骤

- 使用以下命令检查所有备份：

```
omniofflr -idb -autorecover -logview -skiprestore
```
- 通过运行以下命令，选择要从中还原的备份会话并执行 IDB 还原：

```
omniofflr -idb -autorecover -session SessionID
```

此命令指导您完成以下过程：恢复 IDB 和重放从上一次 IDB 备份以来的归档日志文件。如果归档日志文件不可用，则通过导入自上一次 IDB 备份以来所使用的所有介质，仍可以更新 IDB。

## 在其他 Cell Manager 主机上还原 IDB 数据库。

使用以下步骤在不同的 Cell Manager 主机上恢复 IDB 数据库。

1. 在新 Cell Manager 主机上安装 Data Protector，然后导入包含旧 Cell Manager 主机的 IDB 备份的设备。
2. 仅将配置文件还原到新位置。例如，`/tmp/idb/config`。
3. 创建原始文件 `/etc/opt/omni/server/cell/cell_info` 的副本。
4. 将完整的 IDB 数据库还原到新位置。例如，`/tmp/idb/newidb`。
  - 要还原数据库文件，请选择选项 **StartDatabaseServer** 和 **UseRestoredDatabaseAsNewDatabase**。
  - 要将编目二进制文件作为目标，请选择“还原到原始位置”。
  - 要将配置文件作为目标，请选择**还原到原始位置**并将冲突解决选择为**覆盖**。
5. 无错误完成还原后，创建以下原始文件的副本(作为预防措施):
  - `/etc/opt/omni/server/AppServer/standalone.xml`
  - `/etc/opt/omni/server/idb/idb.config`
  - `/etc/opt/omni/server/idb/ulist`
6. 通过运行以下命令停止 Data Protector 服务：`/opt/omni/sbin/omnisv stop`
7. 覆盖以下文件：`/etc/opt/omni/server/cell/cell_info`，在步骤 3 中已创建了该文件的副本。
8. 在首选的编辑器中打开文件 `/etc/opt/omni/server/AppServer/standalone.xml`，然后找到 `keystore-password` 和 `truststore-password` 并记下来。它们通常是相同的。
9. 在首选的编辑器中打开文件 `/etc/opt/omni/client/components/webservice.properties`，用在 `standalone.xml` 文件中找到的值替换 `keystore-password` 和 `truststore-password`，然后保存更改并关闭文件。  
在群集环境中，必须编辑群集的所有节点上的 `webservice.properties` 文件。
10. 通过运行以下命令重新生成证书：`/opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -server_id <hostname> -user_id hpd -store_password <your keystore password>`
11. 确保以下文件不包含旧 Cell Manager 的主机名：
  - `/etc/opt/omni/client/components/dp-jobexecutionengine-backup/webservice.properties` `/etc/opt/omni/client/components/dp-jobexecutionengine-consolidation/webservice.properties`

- /etc/opt/omni/client/components/dp-jobexecutionengine-copy\webservice.properties
  - /etc/opt/omni/client/components/dp-jobexecutionengine-verification\webservice.properties
  - /etc/opt/omni/client/components/dp-loginprovider\webservice.properties
  - /etc/opt/omni/client/components/dp-Scheduler-gui\webservice.properties
  - /etc/opt/omni/client/components/dp-webservice-server\webservice.properties
  - /etc/opt/omni/client/components/jce-dispatcher\webservice.properties
  - /etc/opt/omni/client/components/jce-serviceregistry\webservice.properties
  - /etc/opt/omni/client/components/webservice.properties
12. 将以下变量添加到 `omnirc` 文件 - `/opt/omni/.omnirc: OB2_CERT_VERIFYHOST=0` 中。如果 `omnirc` 文件不存在，则创建一个空文本文件并将其重命名为 `.omnirc` 或将 `.omnirc.TMPL` 重命名为 `.omnirc`
  13. 通过运行以下命令启动 **Data Protector** 服务： `/opt/omni/sbin/omnisv start`
  14. 运行以下命令更改某些 **Data Protector** 文件的所有权： `/opt/omni/sbin/omnidbutil -change_cell_name <old_cm_hostname>`
  15. 运行以下命令清除正在运行的会话： `/opt/omni/sbin/omnidbutil -clear`
  16. 在 Windows GUI 客户机中，删除具有旧证书的文件夹。启动 **Data Protector** 服务后，**Data Protector** GUI 将从 **Cell Manager** 导入新证书。可以在以下路径中找到旧证书：  
`C:\Users\<USERNAME>\AppData\Local\Hewlett-Packard\Data Protector\ca\<NEW_CM_HOSTNAME>`
  17. 执行以下附加的非强制性步骤：
    - a. 运行以下命令以确认 IDB 使用的是来自新位置的文件(表空间文件和预写日志位于新位置，而 DCBF 位于原始文件夹)： `/opt/omni/sbin/omnidbutil -show_db_files`
    - b. 更新包含旧 **Cell Manager** 的主机名的文件(通常在用户列表、`barlist` 和配置文件中)。可通过运行以下命令找到它们： `grep -rnw /etc/opt/omni -e <OLD_CM_HOSTNAME>`
    - c. 重新配置设备以使用新 **Cell Manager**。

## 通过导入介质更新 IDB

如果归档日志文件不可用，请通过导入上一次 IDB 备份使用的所有介质更新内部数据库。IDB 还原结束后即执行此操作。

### 步骤

1. 启动 **Data Protector** 进程和服务。
2. 递增会话计数器。初始化和还原 IDB 后，计数器被设置为 0。因此，任何新会话的会话 ID 都与那一天已启动的会话相同。

以下命令将会话计数器设置为 200，对于大多数情况下此数值已足够：

```
omnidbutil -set_session_counter 200
```

如有必要，现在立即开始备份。

3. 导出和导入含有上一个 IDB 备份的介质。这样将产生有关上一个 IDB 备份的一致信息。
4. 导入(如果已在 IDB 中，则导出)上一个 IDB 备份和 IDB 恢复时使用的介质。有关使用的介质的列表，请参见默认 **Data Protector** 服务器日志文件位置中的 `media.log` 文件。
5. 运行 `omnidbcheck` 命令。

此时应成功恢复完整 IDB。

**注意：**

如果要将包含 **CMMDB** 或远程 **MMDB** 的 IDB 恢复到不同的磁盘布局，则需要在更新 IDB 之后运行 `omnidbutil -cdbsync` 命令。

# 第 5 章：Manager-of-Managers 环境

## 关于 MoM 环境

Data Protector 管理器的管理器概念使管理员可以管理大型环境，也称为企业备份环境，其中多个 Data Protector 单元都集中来自单个点。

这种方式可以处理备份环境的几乎无限制增长：可以添加新单元，也可以将现有单元拆分为若干单元。

请注意，每个 MoM 客户机和 MoM Manager 都需要运行 Data Protector 的相同版本。

Manager-of-Managers 提供以下功能：

- 集中管理所有任务  
通过 Data Protector 可从一处配置、管理和控制企业备份环境。其中包括配置备份、还原、介质管理、监视和报告整个备份环境的状态。
- Centralized Media Management Database (CMMDB)  
(可选)环境中的所有单元都可以共享常用的中心数据库，以管理企业中的设备和介质。通过 CMMDB，可以在 MoM 环境中的若干单元之间共享高端设备和介质。这样使一个单元(使用 CMMDB)的所有设备都可由使用 CMMDB 的其他单元访问。
- 集中式许可证管理  
通过 Data Protector 可以配置整个 MoM 环境的集中式许可。所有 Data Protector 许可证都安装和保留在 MoM Manager 上。根据需要将许可证分发给特定的单元。

## 关于 CMMDB

在具有高端备份设备的大型多单元环境中，可能希望在几个单元之间共享设备和介质。通过对所有单元设置一个集中 MMDB 并对每个单元保留一个单独的 CDB，可以实现此目的。这样可以在保证多单元结构的安全功能的同时共享介质和设备。

## 如何共享介质

使用 CMMDB 时，介质只能归在这些介质上执行第一次备份的 Data Protector 单元拥有。介质所有者显示在介质视图中。当介质受到保护时，只能在介质上追加来自该单元的备份。每个其上数据受到保护的介质都具有相应信息，其中显示哪个单元当前拥有这些数据。保护到期后，介质即再次对其他单元可用。

## 如何初始化介质

如果磁带已由一个单元初始化，则只要磁带上没有任何受保护的数据，则任何其他单元都可以使用该磁带。如果库中加载了磁带但尚未将其初始化，则任何单元都可将其初始化(假定采用宽松策略，并且没有其他磁带可用)。介质分配规则以同样方式适用于共享磁带，但只有拥有可追加介质的单元才能追加这些介质。

**重要：**

请考虑以下几点：

- 集中式 MMDB 对许可有重大影响。MMDB 从本地变为远程之后，应立即从客户机单元中删除与从 MoM 管理器取得(验证)的库和设备关联的所有许可证。
- 企业环境中的单元必须能够访问 CMMDB 才能运行备份。例如，如果该单元与 MoM 单元之间发生网络故障，则会发生此情况。在 MoM 单元与其他 Data Protector 单元之间需要采用可靠的网络连接。

## MoM 环境配置过程

### 先决条件

- 必须为 MoM 管理器选择一个系统。所选择的系统必须是高度可靠的装有软件的 Data Protector Cell Manager。
- 在 MoM 单元上和每个预期的 MoM 客户机单元上安装必要的许可证。

### MoM 环境配置过程

MoM 环境配置过程由几个阶段组成。需要：

1. 设置 MoM Manager。
2. 将 Data Protector 单元导入 MoM 环境中。
3. 在 MoM 环境中每个单元上的 admin 用户组中创建将充当 MoM 管理员的 Data Protector 用户。
4. 重新启动 Data Protector 服务。

(可选)还可以配置集中式介质管理数据库，配置集中式许可，并分发 MoM 配置。

## 设置 MoM Manager

要设置企业环境，请将某个 Cell Manager 配置为 MoM Manager。

### 步骤

1. 在“上下文列表”中，单击**客户机**。
2. 在“操作”菜单中，单击将 **CM 配置为 Data Protector 管理器的管理器服务器**。
3. 重新启动 Data Protector 服务。
4. 通过在 Data Protector 程序组中选择 **Data Protector 管理器的管理器**来启动 MoM 用户界面。

此外，也可以从 `Data_Protector_home\bin` 目录运行 mom。有关 mom 命令的详细信息，请参见 omnigui 手册页或 *Data Protector 命令行界面* 参考。



## 向单元添加 **MoM** 管理员

**MoM** 管理员可以在企业环境中的所有单元中执行管理任务。

### 先决条件

需要在 **MoM** 环境中每个 **Cell Manager** 上的 **admin** 用户组中都有一个特定的用户。例如，可能有一个称为 **MoM\_Admin** 的用户。此用户将是 **MoM** 管理员。

### 步骤

1. 使用 **Data Protector Manager**，以 **admin** 用户组成员的身份(必须具有置 **User configuration** 用户权限)连接到 **MoM** 环境中的每个 **Cell Manager**。
2. 向 **Data Protector admin** 用户组中添加将成为 **MoM** 管理员的用户。

## 导入单元

将单元导入 **MoM** 环境中，即可用 **MoM** 管理器集中管理该单元。

群集客户机用其虚拟服务器名称向 **MoM** 管理器标识自身。如果在 **MoM** 环境中导入群集，则只需使用其虚拟服务器名称。

### 先决条件

- 活动用户必须是要导入的单元的 **Cell Manager** 上 **Admin** 用户组的成员。

### 步骤

1. 在 **Data Protector** 管理器的管理器中，在“上下文列表”中单击 **客户机**。
2. 右键单击 **企业客户机**，然后单击 **导入 Cell Manager**。
3. 选择要导入的 **Cell Manager**，然后单击 **完成**。

## 在 **MoM** 中重新启动 **Data Protector** 服务

配置 **MoM** 环境之后，将通知您重新启动 **Data Protector** 服务。

如果使用 **Windows Service Control Manager** 在 **Cell Manager** 上停止和启动服务，则系统将仅保留数据库日志的当前和以前的副本。使用 **omnisv** 命令将保存所有以前的数据库日志。

### 停止 **Data Protector** 服务

#### 非群集环境中的 **Cell Manager**

运行以下命令：**omnisv -stop**。

## Serviceguard 上的 Cell Manager

运行以下命令：`cmhaltpkg PackageName`，其中 *PackageName* 是 Data Protector 群集包的名称。

此命令可停止 Data Protector 包，并卸载 Data Protector 共享卷组。

## Symantec Veritas Cluster Server 上的 Cell Manager

使 Data Protector 应用程序资源脱机。

## Microsoft 群集服务器上的 Cell Manager

使 OBVS\_HPDP\_AS, OBVS\_HPDP\_IDB, 和 OBVS\_HPDP\_IDB\_CP 群集组脱机(在活动节点上使用 Cluster Administrator 实用程序)。

## 启动 Data Protector 服务

### 非群集环境中的 Cell Manager

运行以下命令：`omnisv -start`

## Serviceguard 上的 Cell Manager

使用 `cmrunpkg -n NodeName PackageName` 命令重新启动 Data Protector 包。

## Symantec Veritas Cluster Server 上的 Cell Manager

使 Data Protector 应用程序资源联机。

## Microsoft 群集服务器上的 Cell Manager

使用 Cluster Administrator 实用程序使 OBVS\_HPDP\_AS, OBVS\_HPDP\_IDB, OBVS\_HPDP\_IDB\_CP, and OBVS\_MCRS 群集组联机。

## 配置 CMMDB

如果想拥有中心介质管理，则要设置 CMMDB。如果不设置 CMMDB，则每个单元将拥有自己的 IDB。

配置期间，有一个本地介质管理数据库将合并到 CMMDB 中(如果选择这样做)。可以决定每个单元将使用 CMMDB 还是其自身的本地 MMDB。

### 重要：

配置了 CMMDB 并开始使用它之后，即无法将其拆分回相应的本地 MMDB 中。不应尝试恢复 MMDB 的旧状态，而要从头创建新 MMDB。

## 注意事项

如果要配置新单元(并且尚未配置设备和介质)，则不需要合并数据库。只需要将单元与已配置了设备和介质的 CMMDB 合并。

## 先决条件

- 检查是否所有单元中的 Data Protector Cell Manager 都已安装了相同版本的 Data Protector，并且其正在运行。
- 确认在要添加到 CMMDB 的任何单元上没有运行备份、还原或介质管理会话。

## 在客户机单元上配置 CMMDB

### 步骤

1. 以 admin 用户组成员的身份登录客户机单元的 Cell Manager。
2. 创建包含 MMDB 服务器的名称(完全限定)的文件。在 Windows 系统中，以 Unicode 格式保存文件：

**Windows 系统：** `Data_Protector_program_data\Config\server\cell\mmdb_server`

**UNIX 系统：** `/etc/opt/omni/server/cell/mmdb_server`

3. 启用 MoM Manager 以建立单元连接，方法是修改 `pg_hba.conf` 文件，该文件位于内部数据库位置的 `pg` 目录中。

在文本编辑器中打开该文件，并添加以下行：

```
host hdpidb hdpidb_app MoM_Server_IP_Address/32 trust
```

添加到下行之后

```
# IPv4 local connections:
```

```
host all all 127.0.0.1/32 md5
```

保存文件。

#### 注意：

如果 MoM 客户机上的 Cell Manager 是群集环境的一部分，您需要在 MoM 客户机的 Cell Manager 上的 `pg_hba.conf` 文件中指定所有群集节点的 IP 地址(每个节点一个行项目)或群集的子网。

在文本编辑器中打开该文件，并添加以下行：

```
host hdpidb hdpidb_app Cluster_Subnet trust
```

添加到下行之后

```
# IPv4 local connections:
```

```
host all all 127.0.0.1/32 md5
```

保存文件。

4. 重新启动 Data Protector 服务。

5. 通过运行以下命令更新配置文件：

```
omnicc -update_mom_server
```

对于要将其 MMDB 合并到 CMMDB 的所有客户机单元重复这些步骤。

## 在 MoM Manager 上配置 CMMDB

### 步骤

1. 登录到 Manager-of-Managers，并且出于安全原因将 idb 表空间目录复制到临时位置。

idb 是位于内部数据库位置的子目录。

2. 运行以下命令，将本地 MMDB 合并到 CMMDB 中：

```
omnidbutil -mergemmdb MoM_Client_Cell_Manager_Hostname
```

确保 IDB 服务 (hpd-idb) 端口 7112 在执行命令期间在 MoM Manager 和客户机 Cell Manager 上均打开。在合并完成后可关闭端口。

3. 运行以下命令，同步本地 CDB：

```
omnidbutil -cdbsync MoM_Client_Cell_Manager_Hostname
```

4. 编辑介质池和设备的重复名称。如果两个单元上都存在默认池，则对于默认池始终会发生这种重复现象。重复名称在其名称后面追加“\_N”，其中 N 表示一个数字。在这种情况下，手动更改使用这些设备的备份规范以使用新设备名称。

对于要将其 MMDB 合并到 CMMDB 的所有客户机单元重复这些步骤。

## 关于集中式许可

集中式许可意味着在 MoM 管理器上配置所有许可证，并且可以根据需要将这些许可证分配给特定单元。集中式许可简化了许可证管理。MoM 管理员对 MoM 环境中的所有单元执行许可管理，其中包括分发和移动许可证。

设置集中式许可为可选操作。作为替代，也可以在每个 Cell Manager 上安装单独的许可证。这些许可证仅限安装它们的单元使用，并且所有许可管理任务都必须在本机执行。

## 设置集中式许可

设置集中式许可可简化企业环境中的许可证管理。

### 先决条件

如果要将现有 Data Protector 单元合并到 MoM 环境中，则向 *Password Delivery Center* 发出请求，以将许可证从现有 Cell Managers 移至新 MoM 管理器。

### 步骤

1. 登录 MoM Manager，然后创建 licdistrib.dat 文件：

**Windows 系统：** *Data\_Protector\_program\_data\Config\server\cell\licdistrib.dat*

**UNIX 系统：** `/etc/opt/omni/server/cell/licdistrib.dat`

2. 登录到 MoM 环境中的每个 Cell Manager，然后创建含有 MoM Manager 名称的 `lic_server` 文件：

**Windows 系统：** `Data_Protector_program_data\Config\server\cell\lic_server`

**UNIX 系统：** `/etc/opt/omni/server/cell/lic_server`

3. 在做出更改的每个 Cell Manager 上停止并重新启动 Data Protector 服务。
4. 在 Data Protector 管理器的管理器中，在“上下文列表”中单击 **客户机**。
5. 在范围窗格中，右键单击要更改的许可信息所在的 Cell Manager，然后单击 **配置许可** 以打开向导。此时将显示对所选 Cell Manager 可用的许可证的类型和数量。

**注意：**

用虚拟主机名标识群集客户机。

6. 单击 **远程** 选项，将许可从本地更改为远程。此时“已用”列更改为“已分配”。
7. 修改许可证配置。修改过程中只有“已分配”列可用。
  - 要释放(丢弃)许可证类型，因此增加可用许可证的数量，请在“已分配”列中减去其相应的数字。
  - 要分配许可证类型，请在“已分配”列中增加其相应的数字。
8. 单击 **完成** 应用配置。
9. 对于要为其设置集中式许可的所有 Cell Manager 重复上述步骤。
10. 使用 `omnisv -stop` 和 `omnisv -start` 命令停止并重新启动 Data Protector 进程。

如果在 Serviceguard 上配置 Cell Manager，则先运行 `cmhaltpkg PackageName` 命令以停止 Data Protector 包，再运行 `cmrunpkg -n NodeName PackageName` 命令以将其启动，其中 `PackageName` 是 Data Protector 群集包的名称。

如果在 Symantec Veritas Cluster Server 上配置 Cell Manager，则先使 Data Protector 应用程序资源脱机，然后再使 Data Protector 应用程序资源联机。

在做出更改的每个 Cell Manager 上，停止并重新启动 Data Protector 服务之后，更改即生效。

**注意：**

Data Protector 每小时用 MoM Manager 检查一次许可证配置。当通信出现问题或 MoM Manager 不可用，将该许可状态保持 72 小时。如果此后 72 小时内未解决问题，则使用本地许可证。

## 停用集中式许可

可以停用集中式许可并将其转换为本地许可。

### 步骤

1. 在 Data Protector 管理器的管理器中，在“上下文列表”中单击 **客户机**。
2. 在范围窗格中，右键单击要停用其集中式许可的 Cell Manager，然后单击 **配置许可** 以

打开向导。此时将显示对所选 **Cell Manager** 可用的许可证的类型和数量。

**注意：**  
用虚拟主机名标识群集客户机。

3. 单击**本地**选项，将许可从远程更改为本地。
4. 单击**完成**应用配置。
5. 对于要停用其集中式许可的所有 **Cell Manager** 重复上述步骤。
6. 登录 **MoM Manager** 并装载位于默认的 **Data Protector** 服务器配置目录的 **cell** 目录。
7. 例如，将 **licdistrib.dat** 文件重命名为 **licdistrib.old**。

在使用 **omnisv -stop** 和 **omnisv -start** 命令停止并重新启动 **Data Protector** 服务后，所做的更改将在做过更改的 **MoM Manager** 和每个 **Cell Manager** 上生效。

如果在 **Serviceguard** 上配置 **Cell Manager**，则先运行 **cmhaltpkg PackageName** 命令以停止 **Data Protector** 包，再运行 **cmrunpkg -n NodeName PackageName** 命令以将其启动，其中 **PackageName** 是 **Data Protector** 群集包的名称。

如果在 **Symantec Veritas Cluster Server** 上配置 **Cell Manager**，则先使 **Data Protector** 应用程序资源脱机，然后再使 **Data Protector** 应用程序资源联机。

## 关于 MoM 环境管理

通过 **MoM** 管理器可以从一处配置、管理和控制企业备份环境。

在 **MoM** 用户界面中，可以导入和导出单元，在各单元之间移动客户机，以及将 **MoM** 配置分发到环境中的其他单元。

用本地管理员的相同方式在 **MoM Manager** 上执行其他任务。按照标准过程配置备份和还原、管理特定单元的设备 and 介质、配置 **Data Protector** 用户和用户组、添加客户机、监视正在运行的会话和备份环境的状态以及配置报告和通知。

**注意：**  
只能从相应的 **Cell Manager** 而非 **MoM Manager** 配置连接到单独单元中客户机的设备。只能从 **MoM Manager** 配置直接连接到 **Cell Manager** 的设备。

## 导出单元

导出单元将从 **MoM** 环境中删除该单元。

群集客户机用其虚拟服务器名称向 **MoM** 管理器标识自身。如果在 **MoM** 环境中导出群集，则只需使用其虚拟服务器名称。

## 步骤

1. 在 **Data Protector** 管理器的管理器中，在“上下文列表”中单击**客户机**。
2. 在范围窗格中，右键单击要导出的 **Cell Manager**，然后单击**导出 Cell Manager**。
3. 确认选择。

## 在单元之间移动客户机系统

通过 **Data Protector** 可以在单元之间移动系统。在此过程中，**Data Protector** 执行以下操作：

- 检查是否在任何备份规范中配置了要移动的客户机，并从初始 **Cell Manager** 上配置的备份规范中删除属于此客户机的所有备份客户机，同时其他客户机的备份对象保留原样。因此，**Data Protector** 确保将客户机移至另一个单元之后，备份规范中没有剩余的孤立备份对象。
- 检查系统上是否配置了任何设备，并且指导您完成将设备移至另一个系统的步骤。
- 检查此系统上的设备中是否有已使用的介质，并且指导您完成移动介质的步骤。

### 步骤

1. 在 **Data Protector** 管理器的管理器中，在“上下文列表”中单击**客户机**。
2. 展开要移至另一个单元的客户机系统所在的 **Cell Manager**。
3. 右键单击该客户机系统，然后单击**将客户机系统移至其他单元**以打开向导。
4. 选择目标 **Cell Manager**。
5. 单击**完成**移动客户机。

## 停用集中式许可

**Data Protector** 允许您在 **MoM** 环境中的所有 **Cell Manager** 上创建常用用户类规范、**Holidays** 文件设置、全局选项设置和保管。

### 先决条件

在 **MoM Manager** 上创建所需的用户类规范、**Holidays** 文件设置和全局选项设置。

### 步骤

1. 在 **Data Protector** 管理器的管理器中，在“上下文列表”中单击**客户机**。
2. 右键单击**企业客户机**，然后单击**分发配置**。
3. 在“分发配置”对话框中，选择配置类型以及要向其分发所选配置的 **Cell Manager**。
4. 单击**完成**分发配置。

## 配置 **Data Protector** 用户

可将用户或用户组添加到 **MoM** 环境，就像对单个 **Cell Manager** 那样。此过程用新用户更新所有 **Cell Manager**。

## 步骤

1. 在 Data Protector 管理器的管理器中，在“上下文列表”中单击**用户**。
2. 选择要向其添加用户的 **Cell Manager**。
3. 在“编辑”菜单中，如果要添加新用户，则单击**添加**，然后选择**用户**；如果要添加新用户组，则选择**用户组**。
4. 输入所需的信息，然后单击**完成**。

## 将用户添加到其他单元

可以将现有用户添加到 MoM 环境中的其他单元。该用户将自动添加到目标 **Cell Manager** 上与其在源 **Cell Manager** 上所处相同的用户组。

### 注意：

如果目标 **Cell Manager** 上不存在用户在源 **Cell Manager** 上所在的组，则无法将该用户添加到目标单元。

## 步骤

1. 在 Data Protector 管理器的管理器中，在“上下文列表”中单击**用户**。
2. 在范围窗格中，展开 **Cell Manager**，然后展开该用户所在的组。
3. 右键单击该用户，然后单击**向其他单元添加用户**以打开向导。
4. 选择目标 **Cell Manager**。
5. 单击**完成**退出向导。

## 从单元删除用户

可以从 MoM 环境的单元中删除用户。

## 步骤

1. 在 Data Protector 管理器的管理器中，在“上下文列表”中单击**用户**。
2. 在范围窗格中，展开 **Cell Manager**，然后展开该用户所在的组。
3. 右键单击该用户，然后单击**从单元中删除用户**以打开向导。
4. 选择要从中删除用户的 **Cell Manager**。
5. 单击**完成**退出向导。

## 管理特定单元的设备 and 介质

可以配置企业环境中任何单元的设备 and 介质。



## 步骤

1. 在 Data Protector 管理器的管理器中，在“上下文列表”中单击**客户机**。
2. 选择要管理的介质或设备所在的单元。
3. 在工具菜单中，单击**设备和介质管理**。  
此时将打开 Data Protector Manager，并显示“设备和介质”上下文。
4. 像本地管理员那样配置设备和介质。

### 注意：

只能从相应的 Cell Manager 而非 MoM Manager 配置连接到单独单元中客户机的设备。只能从 MoM Manager 配置直接连接到 Cell Manager 的设备。

## 管理特定单元的内部数据库

可以管理企业环境中任何单元的 IDB。

## 步骤

1. 在 Data Protector 管理器的管理器中，在“上下文列表”中单击**客户机**。
2. 选择要管理的 Cell Manager。
3. 在工具菜单中，单击**数据库管理**。在“内部数据库”上下文中，像本地管理员那样执行数据库管理任务。

# 第 6 章：群集

## 关于群集

有关群集概念、架构和群集环境中的 **Data Protector** 的详细信息，请参见 *Data Protector 概念指南*。

有关在群集环境中安装 **Data Protector** 的详细信息，请参见 *Data Protector 安装指南*。

## 关于 **Data Protector Microsoft** 群集服务器集成

有关群集概念、架构和群集环境中的 **Data Protector** 的详细信息，请参见 *Data Protector 概念指南*。

有关在群集环境中安装 **Data Protector** 的详细信息，请参见 *Data Protector 安装指南*。

作为其高可用性的一部分，**Data Protector** 可与 **Microsoft** 群集服务器 (MSCS) 相集成，从而使您可以备份完整群集(本地和共享磁盘)以及群集环境中运行的应用程序。有关支持的操作系统版本、群集支持级别以及支持的配置的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

假定您熟悉 MSCS。如果不熟悉，请参见 MSCS 联机文档获得详细信息。

## 许可和 MSCS

购买 **Data Protector Cell Manager** 的许可证时，请注意，许可证将与虚拟服务器绑定，并且无论 MSCS 群集中的哪个系统运行 **Data Protector Cell Manager**，这个许可证都会起作用。

## 配置

有两种方式可以配置集成：

- **Data Protector Cell Manager** 可安装在 MSCS 上。这样可提高 **Data Protector Cell Manager** 的可用性，在故障转移时 **Data Protector** 服务可从一个群集节点自动迁移到另一个，并因此自动重新启动失败的备份会话。
- **Data Protector** 群集感知客户机可以安装在 MSCS 中，因此支持文件系统备份和群集感知应用程序的备份。

要备份群集感知应用程序，请在配置备份规范时使用其虚拟服务器名称。

### 注意：

群集服务组件(例如数据库管理器)可保持中央群集数据库前后一致，该数据库存储有关节点、资源或组的状态更改的信息。群集数据库必须存储在群集的共享磁盘卷上。

## 如何管理群集感知备份

在 **Data Protector** 群集 **Cell Manager** 中，备份会话是群集感知会话。可以设置相应的选项，定义在发生 **Data Protector** 或其他群集感知应用程序的故障转移时的备份行为。

## Data Protector 的故障转移

如果在备份期间发生群集感知 **Data Protector** 的故障转移，则所有运行和挂起的备份会话都将失败。在 **Data Protector GUI** 中和备份规范中，可以设置三个选项之一，这些选项定义在 **Data Protector** 故障转移时自动重新启动备份会话。

## Data Protector 之外应用程序的故障转移

由于群集感知 **Data Protector** 是群集环境中的存储应用程序，因此它需要了解群集中可能正在运行的其他应用程序。如果这些应用程序正在 **Data Protector** 以外的节点上运行，并且如果某些应用程序故障转移到正在运行 **Data Protector** 的节点，则这样将导致此节点上的负载很高。因此，以前仅管理过备份操作的节点现在还必须处理关键的应用程序请求。通过 **Data Protector**，可定义这种情况下应发生什么，以便保护关键应用程序数据，并再次进行负载均衡。

可以：

- 中止所有正在运行的备份会话  
如果备份的重要性低于应用程序，则 **Data Protector** 可以自动中止所有正在运行的会话，以便在应用程序的故障转移之后均衡负载。  
要设置此选项，需要创建含 **omniclus** 命令的相应脚本。
- 临时禁用备份活动  
如果备份的重要性低于应用程序，则 **Data Protector** 还可以自动将 **Cell Manager** 禁用一段时间，以便在应用程序的故障转移之后均衡负载。所有正在运行的会话继续运行，但直到再次启用 **Cell Manager** 时才能启动新的备份。  
要设置此选项，需要创建含 **omniclus** 命令的相应脚本。
- 根据已用会话时间中止正在运行的会话  
要在应用程序的故障转移之后均衡负载，可以根据备份会话已运行的时间中止这些会话。如果某个正在运行的特定备份会话刚刚结束，则 **Data Protector** 可以继续该会话。如果备份会话刚刚启动，并且如果该会话不重要，则 **Data Protector** 可以中止该会话。  
要设置这些选项之一，需要创建含有 **omniclus** 命令的相应脚本，并在 **Data Protector GUI** 中设置群集备份选项。
- 根据逻辑 ID 中止正在运行的会话  
如果某个正在运行的特定备份会话比应用程序更重要，则 **Data Protector** 可以继续此会话。要在故障转移之后均衡负载，可以通过使用一个重要会话的中止 ID，中止除了该会话以外的所有备份会话。  
要设置此选项，需要创建含有 **omniclus** 命令的相应脚本，并在 **Data Protector GUI** 中设置群集备份选项。

## 关于 Microsoft 群集服务器的灾难恢复

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

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

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

## 可能出现的场景

MSCS 的灾难恢复有两种可能出现的场景：

- 非活动节点上发生的灾难
- 群集中的所有节点都经历了灾难

## 关于 Data Protector Serviceguard 集成

有关群集概念、架构和群集环境中的 Data Protector 的详细信息，请参见 *Data Protector 概念指南*。

有关在群集环境中安装 Data Protector 的详细信息，请参见 *Data Protector 安装指南*。

作为其高可用性的一部分，Data Protector 可与用于 HP-UX 和 Linux 系统的 Serviceguard (SG) 相集成，从而使您可以备份完整群集(本地和共享磁盘)以及群集环境中运行的应用程序。有关支持的操作系统版本、支持的配置和群集支持级别的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。

假定您熟悉 Serviceguard。如果不熟悉，请参见《管理 Serviceguard》手册以获取详细信息。

## 许可和 Serviceguard

购买 Data Protector Cell Manager 的许可证时，请注意，许可证将与虚拟服务器绑定，并且无论 SG 群集中的哪个物理节点运行 Data Protector 群集包，只要该包在其中一个节点上运行，该许可证就会起作用。

## 配置

有两种方式可以配置集成：

- Data Protector Cell Manager 可安装在 SG 中。这样在故障转移时 Data Protector 服务可从一个群集节点自动迁移到另一个，并因此自动重新启动失败的备份会话。  
处于非活动状态的群集节点同样可作为安装服务器使用。
- Data Protector 群集感知客户机可以安装在 SG 中，因此支持文件系统备份和群集感知应用程序的备份。

## 关于 Data Protector HACMP 群集集成

有关群集概念、架构和群集环境中的 Data Protector 的详细信息，请参见 *Data Protector 概念指南*。

有关在群集环境中安装 Data Protector 的详细信息，请参见 *Data Protector 安装指南*。

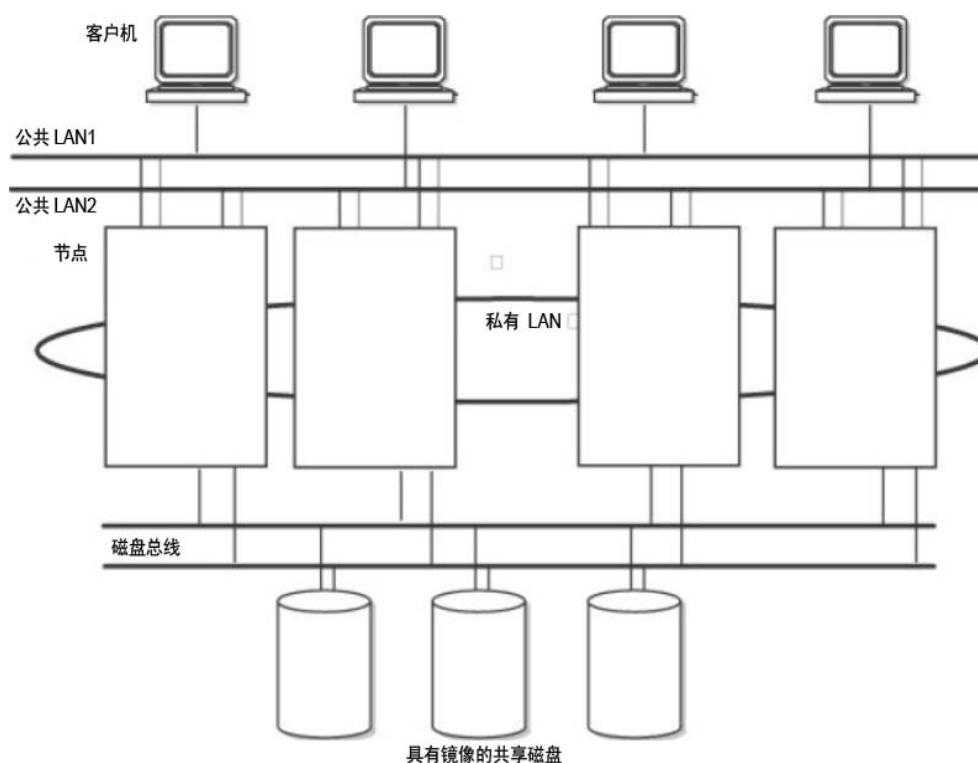
HACMP 软件是 IBM 关于建立基于 UNIX 的任务关键计算环境的解决方案，它基于高可用性 (HA) 和群集多处理 (CMP) 技术。它确保具备应用程序等关键资源可供处理。

创建 HACMP 群集的主要原因是为任务关键应用程序提供一个高度可用的环境。例如，HACMP 群集可以运行一个数据库服务器程序，为客户机应用程序提供服务。客户机向服务器程序发送查询，后者通过访问存储在共享外部磁盘上的数据库响应其请求。

要确保 HACMP 群集中这些应用程序的可用性，请由 HACMP 控制这些应用程序。HACMP 确保即使群集中有组件发生故障，应用程序对客户机进程也保持可用。如果有组件发生故障，则 HACMP 将应用程序(连同确保可访问应用程序的资源一起)移至群集中的另一个节点。

通过虚拟服务器名称(虚拟环境域名)访问整个群集，该名称代表网络上的整个 HACMP 群集。

### 典型的 HACMP 群集设置



如图所示，HACMP 群集由以下物理组件组成：

- 节点
- 共享外部磁盘接口
- 网络
- 网络接口
- 客户机

## 节点

节点组成了 HACMP 群集的核心。每个节点都由一个唯一名称标识，并包含一个用于运行 AIX 操作系统、HACMP 软件和应用程序软件的处理器。节点可能拥有一组资源磁盘、卷组、文件系统、网络、网络地址和应用程序。

## 共享外部磁盘接口

每个节点都可以访问一个或多个共享外部磁盘设备(以物理方式连接到多个节点的磁盘)。共享磁盘存储任务关键数据，通常进行镜像或配置 RAID 以形成数据冗余。注意，HACMP 群集中的节点使用内部磁盘存储操作系统和应用程序二进制文件，但不共享这些磁盘。

## 网络

HACMP 软件作为 AIX 操作系统的一个独立分层组件，旨在配合任何基于 TCP/IP 的网络一起工作。节点使用网络可：

- 允许客户机访问群集节点、
- 使群集节点可以交换波动信号消息、
- 序列化对数据的访问(在并发访问环境中)。

HACMP 软件定义两种类型的通信网络，具体取决于这些网络所使用的通信接口基于 TCP/IP 子系统(基于 TCP/IP)还是基于非 TCP/IP 子系统(基于设备)。

## 客户机

客户机是可以通过 LAN 访问群集中节点的处理机。每个客户机都运行一个“前端”，即客户机应用程序，

以查询群集节点上运行的服务器应用程序。

## 任务

如何安装和配置 Data Protector IBM HACMP 群集集成

# 第 7 章：主页上下文

借助 Data Protector 10.00，GUI 中引入了新的管理上下文，为访问**仪表板**、**遥测 UI** 和基于 Web 的**计划程序**提供了统一方式。

## 仪表板

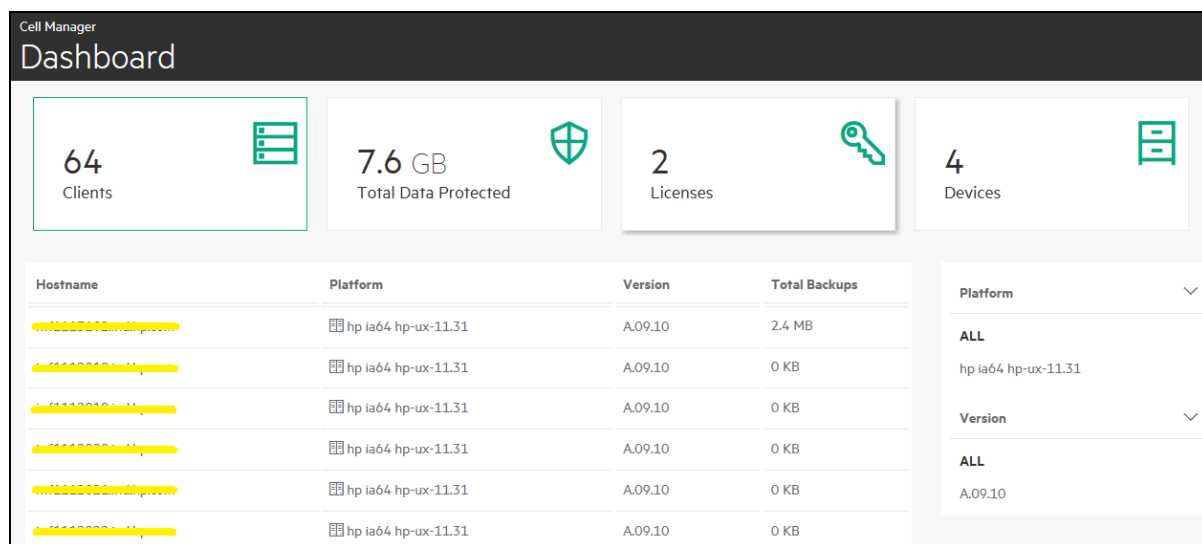
仪表板页面为用户提供 **Cell Manager** 实例的总体概述，其中包括受保护的总数据、可用的客户机数、存储设备和所安装的许可证。

### 如何访问仪表板页面？

要访问仪表板页面，请单击 GUI 中的**主页**上下文菜单，然后单击左侧窗格中的“仪表板”。

仪表板页面分成 4 个不同的类别：

- 客户机
- 受保护的总数据
- 许可证
- 设备



## 客户机

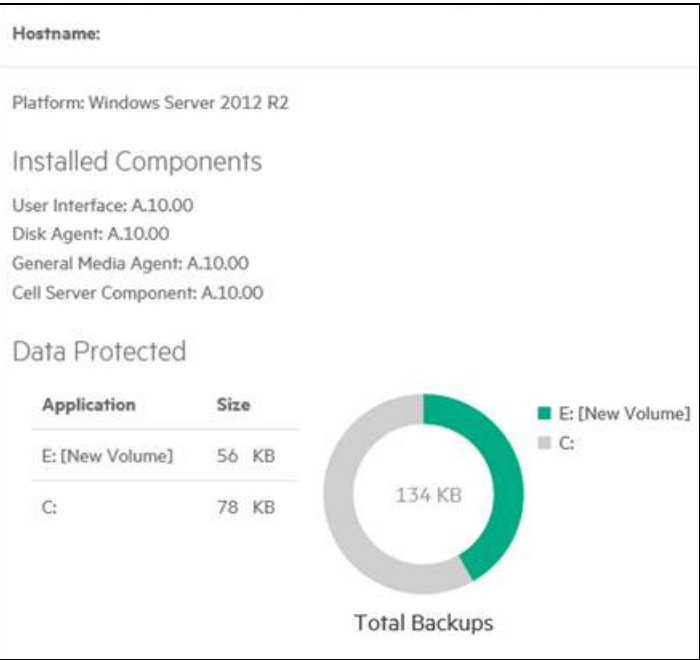
“客户机”列出了当前配置的客户机，以及主机名、操作系统、版本和总备份大小。

- **主机名**：此列包含所有可用主机的主机名。主机名可以根据用户的喜好按升序或降序排列。当用户单击该行时，会出现**其他客户机详细信息**对话框，其中包含有关已安装组件和应用程序备份的信息。备份以图表形式显示，图表中显示不同的应用程序备份。
- **平台**：此列包含由客户机使用的所有操作系统。页面的右侧有一些额外的过滤器，这些过滤器用来显示具有特定操作系统的客户机。

- **版本：**此列包含 **Cell Manager** 版本号或客户机版本号。页面的右侧有一些额外的过滤器，这些过滤器用来显示具有特定版本的客户机。
- **总备份大小：**此列包含在每个客户机上备份的总数据大小。

受保护的总数据

在 **Cell Manager** 上保护的总数据数据以图表形式显示，其中包含为相应数据类型(文件系统)备份的数据量。



许可证

在每个系统上安装的许可证数量。这会按如下方式进一步分类：

- **在线许可证：**在线许可证是可允许您在一段时间内获取许可证的许可机制。
- **容量许可证：**容量许可证是可允许您基于所备份的数据量获取许可证的许可机制。

设备

列出 **Cell Manager** 上的所有存储设备。

这会按如下方式进一步分类：

- **主机名：**此列包含设备或介质服务器的主机名。这可以根据用户的喜好按升序或降序排列。
- **带库名称：**此列包含存储设备的所有带库名称。
- **设备：**此列包含存储设备的设备类型。在该页面的右侧，有一个可供用户基于特定设备类型对列进行过滤的选项。
- **类型：**此列包含存储设备的设备类型。
- **池名称：**此列包含存储设备的所有介质池。
- **使用情况：**用来备份数据的设备的容量。



## 遥测

Data Protector 遥测客户机服务通过应用程序服务器从 Data Protector Cell Manager 收集数据，并将遥测数据上传到 Data Protector 支持供进一步分析。

### 如何访问遥测页面？

要访问遥测页面，请单击 GUI 中主页上下文菜单，然后单击左窗格中的“遥测”。

遥测客户机服务是部署在单元控制台 (CC) 客户机上的 Windows 和 Linux 服务。服务页面会显示 Data Protector 遥测客户机服务，用户可以从其中启动或停止该服务。

Data Protector 收集以下高层次遥测信息：

- 组件信息 - Data Protector 组件及其版本。它还收集有关主机 OS 版本的信息。
- 设备或介质服务器 - 与 Cell Manager 中的客户机关联的详细信息，其中包括附加设备使用大小数据的主机名详细信息、设备的名称、库名称、设备类型以及将介质放置到的池的名称。
- 设备使用大小 - 设备的使用大小。
- 基于容量的许可 (CBL) - 利用 CBL 收集有关容量的信息。有关详细信息，请参见《Data Protector 安装指南》。
- 传统许可证类别 - 它收集有关每个主机安装的许可证及可用许可证的信息。
- 客户机使用情况 - 此信息是为每个客户机收集的。此类信息包括：主机名、应用程序名称和备份数据的总大小。
- 存储使用情况 - 在设备上备份的总数据。

### 先决条件

- 部署在 CC 上的遥测客户机服务必须配置代理才能与客户支持后端服务器进行通信。
- 配置遥测时，应提供客户名称和代理信息。

#### 注意：

会收集与客户相关的内部信息，但会屏蔽主机信息。

在收集遥测数据期间，Cell Manager 的性能不会受到影响。

### 限制：

- 遥测客户机服务仅在 Windows x64 和 Linux x64 操作系统上受支持。

## 遥测的工作原理？

在遥测注册过程中，信息存储在 IDB 中。已安装 DP GUI 组件的任何 Windows 主机都是合适的遥测客户机。根据已配置的上传频率，Cell Console (CC) 客户机检查 IDB 设置，从 Cell Manager 获取遥测数据，并将数据上传到后端服务器。

如果收集过程中服务脱机，则不执行上传遥测。当服务联机时，客户机才可上传遥测数据。

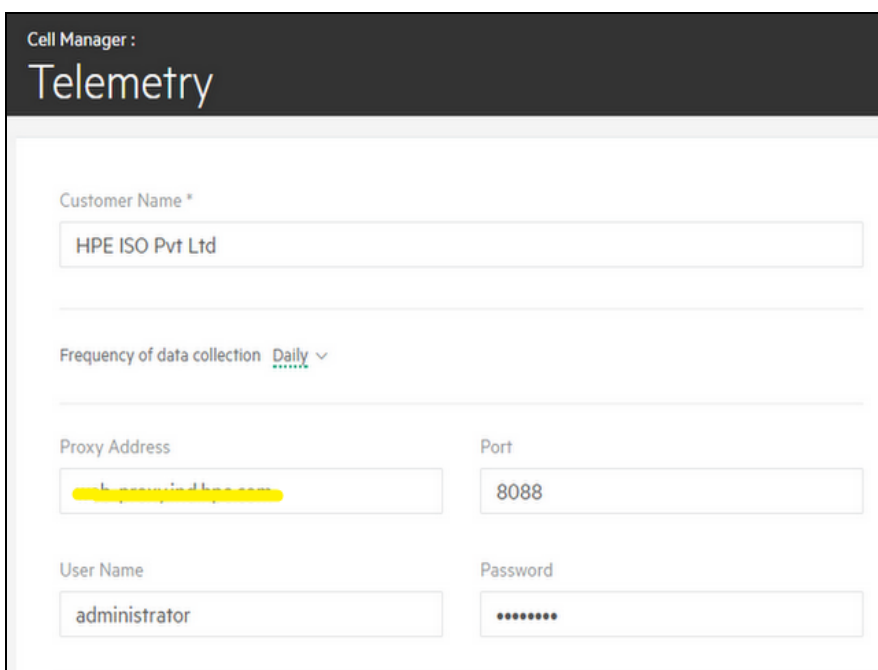
在单元中，如果有多个遥测客户机，则只有一个客户机按照上传频率执行后端上传。使用上传状态和时间更新 IDB。

在遥测客户机中，如果访问外部网络需要代理，则您需要指定代理参数。如果可以直接连接，则可以忽略此操作。

### 遥测页面

客户可以从“遥测”页面订阅或取消订阅遥测更新。要订阅遥测更新，请输入以下字段：

- **客户名称：**客户的名称。
- **数据收集频率：**用户可以选择数据的收集频率，即“每天”、“每周”、“每月”和“每季度”。
- **代理 [可选]：**已配置代理服务器的地址。
- **端口 [可选]：**代理服务器的端口。
- **用户名 [可选]：**连接到代理服务器的用户名。
- **密码 [可选]：**给定用户名的密码。

The screenshot shows a web interface titled "Cell Manager : Telemetry". It contains a form with the following fields: "Customer Name \*" with the value "HPE ISO Pvt Ltd"; "Frequency of data collection" with a dropdown menu set to "Daily"; "Proxy Address" with a value that is partially obscured by a yellow highlight; "Port" with the value "8088"; "User Name" with the value "administrator"; and "Password" with a masked value represented by dots.

在输入上面的字段并选择数据收集频率之后，接受条款和条件并单击**订阅**。

## 计划程序

### 重要：

借助 **Data Protector 10.00**，基本计划程序和高级计划程序已过时，被基于 **Web** 的新计划程序所替代。在升级过程中，现有的所有计划将自动迁移至新的计划程序。

**Data Protector 10.00** 引入了基于 **Web** 的新计划程序，该计划程序具有细化的用户界面、简单且易于使用的 **Web** 控件，便于轻松管理计划。您现在可以使用单个计划程序向导设置计划优先级、数据保护、重复模式和修复冲突。

使用计划程序定期自动执行各种操作，如备份、介质复制、对象合并和复制。借助无人看管的后台操作执行，无论何时运行操作，都无需手动重复计划。

**如何访问计划程序页面？**

要访问计划程序页面，请单击 GUI 中的**主页**上下文菜单，然后单击左窗格中的**计划程序**。

## 从早期版本迁移计划

升级到 **Data Protector 10.00** 后，所有现有的计划将自动迁移到基于 **Web** 的新计划程序。无需手动干预。

在升级到 **Data Protector 10.00** 期间，所有现有的计划文件都会附加 **.migrate** 后缀。

例如，在 **10.00** 之前的 **Data Protector** 版本中，如果您具有名称为 **WeeklyBackup** 的备份规范计划，则文件名将在升级过程中被修改为 **WeeklyBackup.migrate**。如果迁移失败，则不会重命名文件。

如果计划未正确迁移，则可能会要求您将这些 **.migrate** 文件提供给软件支持以进行故障排除。

已迁移的计划文件可从以下位置获取：

规范类型	计划路径
备份计划	Windows: <i>Data Protector_program_data\OmniBack\Config\Server\amoschedules</i> Unix: <i>/var/opt/omni/server/amoschedules</i>
集成计划	Windows: <i>Data Protector_program_data\OmniBack\Config\Server\Barschedules</i> Unix: <i>/var/opt/omni/server/Barschedules</i>
复制操作计划	Windows: <i>Data Protector_program_data\OmniBack\Config\Server\copylists\scheduled\schedules</i> Unix: <i>/var/opt/omni/server/copylists/scheduled/schedules</i>
合并操作计划	Windows: <i>Data Protector_program_data\OmniBack\Config\Server\consolidationlists\scheduled\schedules</i> Unix: <i>/var/opt/omni/server/consolidationlists/scheduled/schedules</i>
验证操作计划	Windows: <i>Data Protector_program_data\OmniBack\Config\Server\verificationlists\scheduled\schedules</i> Unix: <i>/var/opt/omni/server/verificationlists/scheduled/schedules</i>
报告组计划	Windows: <i>Data Protector_program_data\OmniBack\Config\Server\rptschedules</i> Unix: <i>/var/opt/omni/server/rptschedules</i>

如果在升级过程中计划迁移失败，您可以手动运行以下命令，以便将现有计划成功迁移到新的计划程序：

```
omnidbutil -migrate_schedules
```

**注意：**

- 以前版本的 **Data Protector** 中添加的计划没有与其关联的名称属性。因此，迁移后，迁移的计划的名称显示为 ...。您可以编辑这些计划并向计划提供名称。
- 在升级过程中，在早期版本的 **Data Protector** 中配置的分钟/小时/年计划将不迁移至 **Data Protector 10.00**。

## 计划选项

根据规范类型，您可以设置以下计划选项：

- 备份类型：备份类型，完整或增量。
- 网络负载：会话的网络负载。将此选项设置为**中**或**低**可减少运行 **Data Protector** 时网络上的负载。这样可防止数据传输阻止其他用户使用网络，但会增加会话完成所需的时间。
- 数据保护：所备份数据的保护期，以防备份被覆盖。
- 重复模式：计划必须运行的频率。
- 估计持续时间：估计会话的持续时间，可确定计划在日程视图中的显示方式。

在 **ZDB 到磁盘 + 磁带** 或 **ZDB 到磁盘** (如果启用了即时恢复) 的情况下，可以指定**分割镜像/快照备份**选项。

可以用不同的选项值多次计划每个备份规范。在一个备份规范内，可以同时计划“**ZDB 到磁盘**”和“**ZDB 到磁盘 + 磁带**”会话，并为每次单独或定期计划的备份指定不同的数据保护期。

此外，新计划程序包括以下功能：

## 节假日期间的计划排除

可以通过编辑默认 **Data Protector** 服务器配置目录下的 **Holidays** 文件来设置不同的假日。

默认情况下，**Data Protector** 在节假日运行备份。如果要更改默认行为，请考虑以下示例。如果将日期 1 月 1 日注册为节假日，则 **Data Protector** 不会在该日期进行备份。如果已计划在 1 月 1 日进行一次完整备份，1 月 2 日进行一次增量备份，则 **Data Protector** 将跳过在 1 月 1 日运行完整备份，但将运行 1 月 2 日计划的增量备份。增量备份将以最后一次完整备份为基础。

在 **Holidays** 文件中编辑或添加新条目时，请考虑以下因素：

- 每行中的第一个数字表示一年中连续的天数。**Data Protector** 忽略此值，但必须将此值设置为 0 到 366 之间。可以将其设置为 0 以表示该数字与其后的日期不对应。
- 将日期指定为 **Mmmd**，其中 **Mmm** 是月份的三字母缩写，而 **d** 是月中某天的数字形式 (例如 Jan 1)。注意，无论您的区域设置为何，都必须以英文指定月份。
- 节假日的说明为可选，并且 **Data Protector** 当前不使用该说明。

无论文件顶部指定的年份是多少，文件中指定的节假日都始终按原样使用，并且如果节假日不是在每年的相同日期发生，就必须手动进行编辑。如果不想使用计划程序的**假日**选项，则可以删除 **Holidays** 文件中的条目或将其注释掉，以防无意中用过期的或没有为您所在国家/地区或公司专门要求而自定义的 **Holidays** 文件时造成混淆。

## 使用预定义计划

**Data Protector** 计划程序配备一组预定义计划，有助于简化计划配置。以后也可以修改这些计划。

## 处理计划冲突

计划定期备份时，可能会发生所选备份开始时间已被同一备份规范中的另一个计划备份占用的情况。在此情况下，**Data Protector** 计划向导向您展示存在计划冲突。您可以重新定义重复模式，或者允许计划程序在仍有时间段空闲的日期设置计划。根据时间空档可用性，设置以下值作为计划状态：

- 活动：计划没有冲突，将在计划的时间运行。
- 重叠：计划处于冲突状态，但当可以运行计划时，在选定日期有可用的时间空档。
- 非活动：计划处于冲突状态，当可以运行计划时，在选定日期没有可用的时间空档。
- 禁用：用户已明确禁用计划。

## 在不同时区进行计划

所有计划都会显示在 **Cell Manager** 系统的时区的日历中。如果为备份或对象操作会话指定了 **Cell Manager** 的时区之外的其他时区，则会话将在指定的时间和时区运行。

## 划分计划优先级

您可以使用计划向导，为每个计划设置优先级。如果多个正在运行的会话同时请求访问特定设备，则优先级将确定会话的排队顺序。可以为每个计划设置优先级。

- 您可指定某一计划会话能够暂停其他会话(如果其优先级低于所选会话)。

### 注意：

**CMMDB** 环境中不支持“计划优先级”和“暂停优先级较低的作业”选项。

- 文件系统、VMware 和 Oracle Server 集成会话能够暂停会话并从会话停止处恢复会话。对于其他集成，会话在暂停后将重新启动。
- 备份会话到磁盘 (B2D) 设备因其优先级的缘故，不受暂停限制。
- 对于包含各种备份设备(如文件库和 B2D)的备份会话，暂停功能仅适用于非 B2D 设备。
- 计划程序可维护内部作业队列以管理优先级。如果多个作业将同一文件库共享为目标设备，计划程序一次只分配一个作业，并且只在前一个作业完成且释放设备后才分配下一个作业。优先级最高的作业将最先分配。如果多个作业的优先级相同，则计划时间最早的作业将最先分配。如果它们的优先级和计划时间都相同，则随机从中选取一个进行分配。

### 计划和优先级示例

下面是计划程序如何基于优先级和暂停处理备份会话的示例。

有三个会话要计划，其中：

- Job1 优先级为 2000，且启用了**暂停优先级较低的作业**选项。
  - Job2 优先级为 4000。
  - Job3 优先级为 3000，且启用了**暂停优先级较低的作业**选项。
    1. Job2 当前正在运行。
    2. 同时计划 Job1 和 Job3。Job1 会话启用了暂停其他会话的选项。因此，Job2 会话将暂停，以支持 Job1。
    3. 一旦 Job1 会话完成，Job3 会话便运行。
- 暂停的 Job2 会话将保持暂停，直到它能够按照计划和优先级运行。如果有其他优先级更高的会话，此对话可能永远没有机会运行。

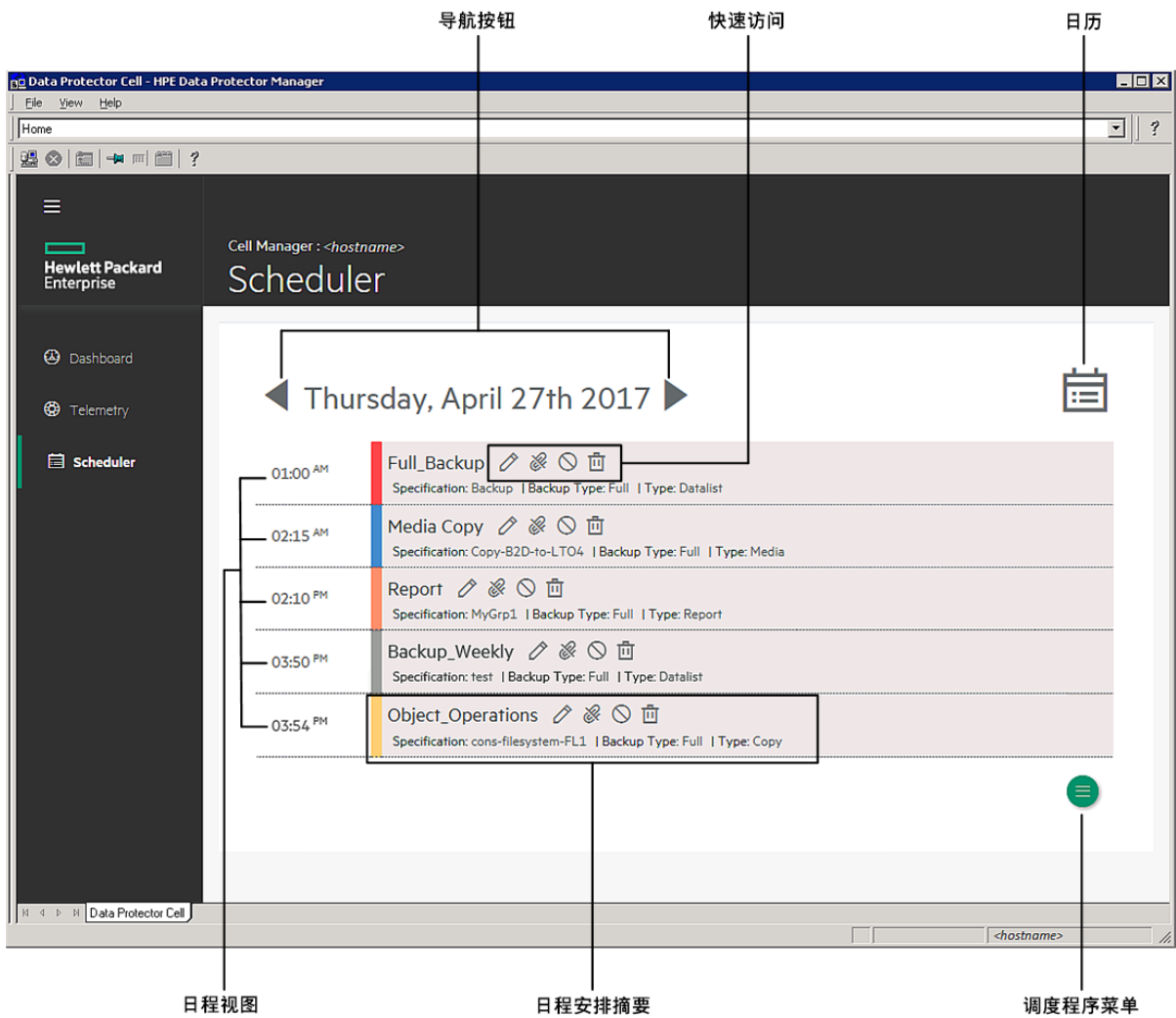
## 限制

对于 Data Protector 计划程序，存在以下限制：

- 浏览器限制：要使“计划程序”页面正常工作，计算机必须安装 Microsoft Internet Explorer 11。

## 计划程序用户界面

下图显示此页出现的计划程序 UI 和各种控件。



下表对所有控件进行了说明：

控制	说明
导航按钮	通过上一步和下一步导航按钮，您可以向后和向前移动日期，并查看选定日期的日程。
快速访问	<p>一系列图标，可用于每个计划，为常用的计划程序操作提供快捷方式。</p> <div></div> <ul style="list-style-type: none"><li>• 编辑：打开计划向导，可让您修改该计划可用的所有设置。</li><li>• 禁用实例：针对选定日期，禁用当前实例。如果是重复计划，则仅禁用选定的实例。禁用实例时，计划从该日的日程中删除。</li><li>• 禁用系列：禁用该计划的所有实例。如果您禁用计划，</li></ul>

	计划将呈灰色显示。禁用某个计划不会影响任何当前正在运行的计划。 <ul style="list-style-type: none"><li>删除：删除计划。</li></ul>
日历	显示日历。您可以在日历中选择日期，显示该日的日程。
日程视图	列出所选日期的所有计划，包括禁用的计划。
计划摘要	提供计划的摘要。例如，您可以查看为其创建计划的规范名称、必须执行的备份类型(完整/增量)和计划类型。每个计划旁边的颜色编码表示 <b>类型</b> ： <ul style="list-style-type: none"><li>红色表示该计划为备份操作创建。</li><li>蓝色表示该计划为介质操作创建。</li><li>橙色表示该计划为报告生成创建。</li><li>黄色表示该计划为复制操作创建。</li><li>灰色表示该计划已禁用。</li></ul>
计划程序菜单	计划程序菜单为您提供创建新计划的选项。

## 计划程序任务

您可以使用计划程序执行以下任务。



- 创建计划
- 编辑现有计划
- 查看计划
- 禁用和启用计划
- 在节假日禁用和启用计划
- 在特定日期和时间设置计划
- 定期设置计划

**已弃用：**  
您不能在基于 **Web** 的新计划程序中重置计划。重置计划选项用于在规范中清除当年的所有计划设置。

## 创建计划

完成以下步骤，以创建计划。

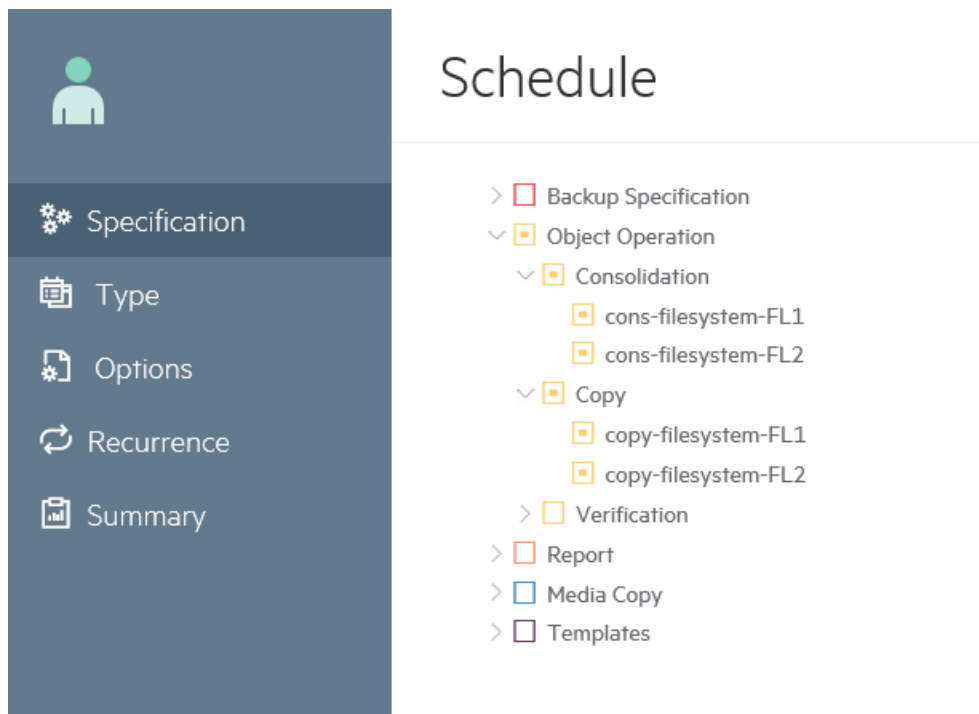
此过程中的步骤显示如何为备份规范创建计划。计划向导中为您提供的选项基于您选择的规范类型。

- 在上下文菜单中，单击**主页**，然后在左窗格中单击**计划程序**。“计划程序”页面随即打开。
- 在“计划程序”页面的右下角，单击计划程序菜单图标，然后单击添加图标以打开计划程序向导。“规范”页面随即打开。



3. 选择要为其创建计划的规范类型。

例如，下图显示扩展的对象操作树，其中列出了您可以为其创建计划的操作：合并、复制和验证。



如果您想要为现有模板添加计划，单击**模板**。

然后，您可以将该模板应用于备份上下文中的规范。应用模板后，将为该规范激活模板中的所有计划。

注意，您不能使用该向导计划模板。

单击**下一步 (Next)**。“类型”页面随即打开。

4. 单击计划类型。

- 单击**自定义**，创建您自己的计划。
- 单击**预定义**，使用其中一个可用的预定义计划与 **Data Protector**。选择下列选项之一：
  - 每日密集备份：**Data Protector**在午夜执行完整备份，并在每天 12:00(中午)和 18:00(下午 6 点)执行两次额外增量备份。
  - 每日完整备份：**Data Protector**在每天 21:00(晚上 9 点)执行完整备份。
  - 每周完整备份：**Data Protector**在每星期五执行完整备份，并在星期一至星期五的 21:00(晚上 9 点)执行增量 1 备份。
  - 两周完整备份：**Data Protector**在每隔一周的星期五执行完整备份。在这些备份之间，**Data Protector**会在每个星期一至星期五的 21:00(晚上 9 点)执行增量 1 备份。
  - 每月完整备份：**Data Protector**在每月的第一天执行完整备份，每周执行增量 1 备份，每隔一天执行一次增量备份。

单击**下一步 (Next)**。“选项”页面随即打开。

5. 在 **计划名称** 文本框中，为您的计划输入名称。
6. 选择 **备份类型**，完整或增量。有关不同备份选项类型的详细信息，请参见 [备份类型](#)。
7. 选择 **保护级别**。保护级别决定有关备份数据的信息在 IDB 中保留多久。如果无编目保护，仍可还原数据，但不能在 **Data Protector GUI** 中浏览这些数据。从以下选项中选择一项。
  - 无：不提供任何保护。
  - 默认值：在数据受保护的时期保护有关 IDB 中备份数据的信息。
  - 直至：直到指定的日期才能覆盖 IDB 中的信息。对信息的保护在所选日期当天的中午停止。
  - 天数：在指定的天数内不能覆盖 IDB 中的信息。
  - 周数：在指定的周数内不能覆盖 IDB 中的信息。
  - 永久：IDB 中的信息永久可用。
8. 移动滑块设置优先级，或者如果优先级数字必须超过滑块值，在 **优先级** 文本框中输入数字。如果多个会话同时尝试访问同一个设备，则可以考虑优先级。这种情况下，此选项可决定会话排列的顺序。

如果高优先级会话开始排队时低优先级会话正在运行，则允许当前运行的会话结束。如果多个优先级相同的会话请求访问同一个设备，则这些会话中的任意一个均有可能首先获得访问权。
9. 指定 **网络负载**。将此选项设置为中或低可减少运行 **Data Protector** 时网络上的负载。这样可防止数据传输阻止其他用户使用网络，但会增加会话完成所需的时间。
10. 如果计划的会话必须能够在繁忙设备中暂停其他低优先级的会话，则打开 **暂停优先级较低的作业** 选项。如果多个会话同时尝试访问同一个设备，则可以考虑此选项。在这种情况下，该选项可以指定已选定会话可以在其完成前，暂停其他会话。已暂停会话将在此会话完成后完成。

**注意：**

此功能仅可用于文件系统、VMware 和 Oracle Server 集成会话。备份会话到磁盘 (B2D) 设备因其优先级的缘故，不受暂停限制。对于包含各种备份设备(如文件库和 B2D)的备份会话，暂停功能仅适用于非 B2D 设备。

11. 默认情况下，计划已启用。关闭 **计划已启用** 选项，以禁用计划。
12. 如果您希望在节假日运行操作，打开 **节假日运行** 选项。要将不同的日子指定为节假日，请编辑 **Holidays** 文件。

单击 **下一步 (Next)**。“重复”页面随即打开。
13. 在“重复模式”中，指定备份的执行频率。从以下选项中选择模式和频率：
  - **一次**：计划在特定日期仅运行一次。您可以选择起始日期、时区和必须运行计划的时间。
  - **每天**：计划定期在指定时间运行。您可以使用“每 <value> 天”字段，指定计划频率。例如，如果重复值为 4，表示每 4 天运行一次计划。

您可以选择起始日期、时区和必须运行计划的时间。

- **每周：**计划每周在指定日期运行。您可以使用“每 <value> 周”字段，指定计划频率。例如，如果重复值为 **2**，表示每 **2** 周在选定某天运行计划。  
您可以选择起始日期、时区和必须运行计划的时间。
- **每月：**计划每月在当月的指定日期运行。您可以使用“每 <value> 月”字段，指定计划频率。例如，如果重复值为 **2**，表示每 **2** 个月在选定某天运行计划。  
您可以选择起始日期、时区和必须运行计划的时间。

14. 从以下选项中选择**重复结束**：

- 无结束日期：如果备份无限期重复，则选择该项。
- 结束日期：如果计划必须在指定日期结束，则选择该项。结束日期与开始日期出现在同一时区。

如果您选择**一次**，**重复结束**选项不可用。

15. 指定**估计持续时间**。该值确定计划在计划视图中的显示顺序。

单击**下一步 (Next)**。“摘要”页面随即打开。

16. 查看所有计划选项。如果存在计划冲突，**发现冲突**选项显示为**是**，您无法完成计划创建任务，直到执行以下某个操作：

- 重新定义计划重复模式。单击“上一步”，返回**重复**页面。
- 打开**填补时间空档**选项。仅当选定日期有可用的时间空档时，该选项才可用。如果没有时间空档，您必须重新定义计划重复模式。

单击**完成**创建计划。

## 编辑现有计划


完成以下步骤，以编辑现有计划。

**注意：**

如果修改计划的以下任何选项，则将删除该计划，并使用新值创建新计划。该新计划移动至队列末尾，并根据时间空档可用性，应用状态。

- 开始日期
- 结束日期
- 时区
- 重复模式
- 每 **n** 值
- 估计持续时间
- 节假日

此过程中的步骤显示如何为备份规范编辑计划。计划向导中为您提供的选项基于您选择的规范类型。

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 右键单击合适的备份规范，然后单击**编辑计划**。“计划程序”页面随即打开。备份规范的所有可用计划均列在右窗格中。
4. 在“计划程序”页面，针对要更改其配置的计划，单击**编辑**图标 。计划向导的“选项”页面随即打开。
5. 在**计划名称**文本框中，更新计划的名称。

**重要：**

对于从 10.00 之前的 Data Protector 版本迁移的计划，计划名称显示为 ...。

6. 选择**备份类型**，完整或增量。有关不同备份选项类型的详细信息，请参见**备份类型**。
7. 选择**保护级别**。保护级别决定有关备份数据的信息在 IDB 中保留多久。如果无编目保护，仍可还原数据，但不能在 Data Protector GUI 中浏览这些数据。从以下选项中选择一项。
  - 无：不提供任何保护。
  - 默认值：在数据受保护的时期保护有关 IDB 中备份数据的信息。
  - 直到：直到指定的日期才能覆盖 IDB 中的信息。对信息的保护在所选日期当天的中午停止。
  - 天数：在指定的天数内不能覆盖 IDB 中的信息。
  - 周数：在指定的周数内不能覆盖 IDB 中的信息。
  - 永久：IDB 中的信息永久可用。
8. 移动滑块设置优先级，或者如果优先级数字必须超过滑块值，在**优先级**文本框中输入数字。如果多个会话同时尝试访问同一个设备，则可以考虑优先级。这种情况下，此选项可决定会话排列的顺序。

如果高优先级会话开始排队时低优先级会话正在运行，则允许当前运行的会话结束。如果多个优先级相同的会话请求访问同一个设备，则这些会话中的任意一个均有可能首先获得访问权。
9. 指定**网络负载**。将此选项设置为中或低可减少运行 Data Protector 时网络上的负载。这样可防止数据传输阻止其他用户使用网络，但会增加会话完成所需的时间。
10. 如果计划的会话必须能够在繁忙设备中暂停其他低优先级的会话，则打开**暂停优先级较低的作业**选项。如果多个会话同时尝试访问同一个设备，则可以考虑此选项。在这种情况下，该选项可以指定已选定会话可以在其完成前，暂停其他会话。已暂停会话将在此会话完成后完成。

**注意：**

此功能可用于文件系统、VMware 和 Oracle Server 集成会话。备份会话到磁盘 (B2D) 设备因其优先级的缘故，不受暂停限制。对于包含各种备份设备(如文件库和 B2D)的备份会话，暂停功能仅适用于非 B2D 设备。

11. 默认情况下，计划已打开。要禁用计划，请关闭**计划已启用**选项。


12. 如果您希望在节假日运行操作，打开**节假日运行**选项。默认情况下，Data Protector 在节假日也运行计划的操作。要将不同的日子指定为节假日，请编辑 **Holidays** 文件。  
单击**下一步 (Next)**。“重复”页面随即打开。
13. 在“重复模式”中，指定备份的执行频率。从以下选项中选择模式和频率：
  - **一次**：计划在特定日期仅运行一次。您可以选择起始日期、时区和必须运行计划的时间。
  - **每天**：计划定期在指定时间运行。您可以使用“每 <value> 天”字段，指定计划频率。例如，如果重复值为 **4**，表示每 4 天运行一次计划。  
您可以选择起始日期、时区和必须运行计划的时间。
  - **每周**：计划每周在指定日期运行。您可以使用“每 <value> 周”字段，指定计划频率。例如，如果重复值为 **2**，表示每 2 周在选定某天运行计划。  
您可以选择起始日期、时区和必须运行计划的时间。
  - **每月**：计划每月在当月的指定日期运行。您可以使用“每 <value> 月”字段，指定计划频率。例如，如果重复值为 **2**，表示每 2 个月在选定某天运行计划。  
您可以选择起始日期、时区和必须运行计划的时间。
14. 从以下选项中选择**重复结束**：
  - **无结束日期**：如果备份无限期重复，则选择该项。
  - **结束日期**：如果计划必须在指定日期结束，则选择该项。结束日期与开始日期出现在同一时区。

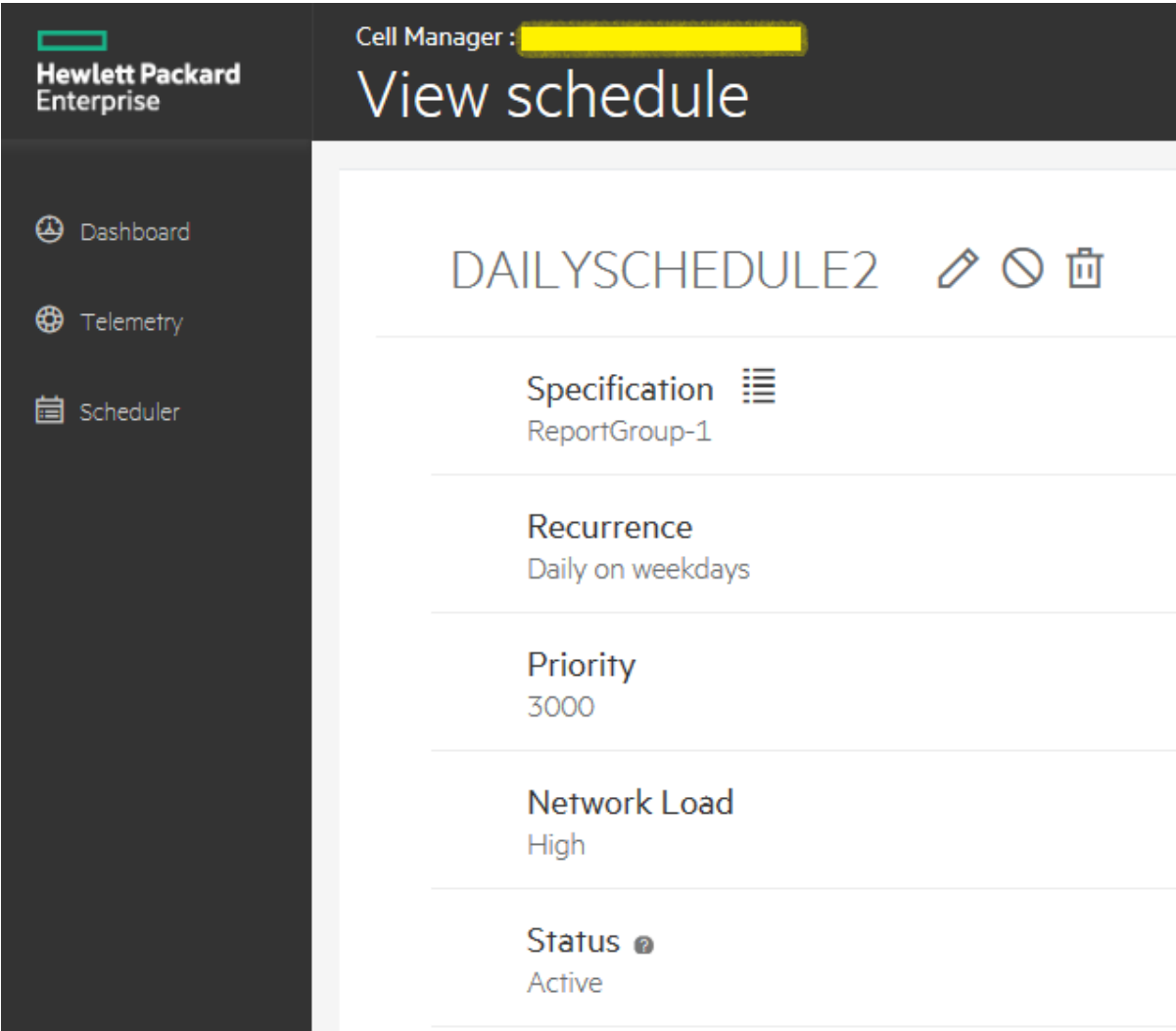
如果您选择**一次**，**重复结束**选项不可用。
15. 指定**估计持续时间**。该值确定计划在计划视图中的显示顺序。  
单击**下一步 (Next)**。“摘要”页面随即打开。
16. 查看所有计划选项。如果存在计划冲突，**发现冲突**选项显示为**是**，您无法完成计划创建任务，直到执行以下某个操作：
  - 重新定义计划重复模式。单击“上一步”，返回**重复**页面。
  - 打开**填补时间空档**选项。仅当选定日期有可用的时间空档时，该选项才可用。如果没有时间空档，您必须重新定义计划重复模式。

单击**完成**保存计划。

## 查看计划

要查看特定计划的详细信息，请单击日程视图中的计划名称。

要查看该规范的所有计划，请单击“查看计划”页面中的  图标。该规范的所有计划均显示在右窗格中。



“查看计划”页面显示以下有关计划的详细信息：

- 规范：为其创建计划的规范类型。
- 重复：为计划设置的重复模式。
- 优先级：计划优先级确定计划的运行顺序。
- 网络负载：运行 **Data Protector** 时，为网络上的负载设置的当前值。
- 状态：状态参数根据时间空档可用性显示以下值：
  - 活动：计划没有冲突，将在计划的时间运行。
  - 重叠：计划处于冲突状态，但当可以运行计划时，在选定日期有可用的时间空档。
  - 非活动：计划处于冲突状态，当可以运行计划时，在选定日期没有可用的时间空档。
  - 禁用：用户已明确禁用计划。

## 禁用和启用计划

默认情况下，计划会在添加时启用，但是可以禁用它，从而使计划设置保持不变以供将来使用。

禁用备份计划不会影响当前正在运行的备份会话。

此过程中的步骤显示如何禁用和启用备份规范的计划。计划向导中为您提供的选项基于您选择的规范类型。

### 步骤

1. 在上下文列表中，选择**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 右键单击合适的备份规范，然后单击**编辑计划**。“查看计划”页面随即打开。在右窗格可看到备份规范的所有可用计划。
4. 单击要编辑的计划，然后单击“查看计划”页面中的**编辑**计划图标。计划向导随即打开。
5. 在“选项”页中，**关闭启用计划**滑块，以禁用计划，然后单击**下一步**。**打开**滑块以启用计划。“重复”页面随即打开。
6. 验证重复模式，然后单击**下一步**。“摘要”页面随即打开。
7. 检查计划选项并单击**完成**。

## 在节假日禁用和启用计划

默认情况下，**Data Protector**在节假日运行计划。通过选择**节假日**选项，可以更改此行为。直到取消选中此选项后才会执行节假日备份。

此过程中的步骤显示如何在节假日启用和禁用备份规范的计划。计划向导中为您提供的选项基于您选择的规范类型。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 右键单击要禁用或启用其节假日备份计划的备份规范，然后单击**编辑计划**。“计划程序”页面随即打开。在右窗格可看到备份规范的所有可用计划。
4. 单击要编辑的计划，然后单击“查看计划”页面中的**编辑**计划图标。计划向导随即打开。
5. 在“选项”页中，**关闭节假日运行**滑块，以阻止在节假日执行操作。如果要在节假日执行操作，则**打开**滑块。
6. 单击**下一步**。“重复”页面随即打开。
7. 验证重复模式，然后单击**下一步**。“摘要”页面随即打开。
8. 检查计划选项并单击**完成**。

## 在特定日期和时间设置计划

可以计划会话在特定日期的特定时间自动启动。

此过程中的步骤显示如何在特定日期和时间设置备份规范的计划。计划向导中为您提供的选项基于您选择的规范类型。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 右键单击合适的备份规范，然后单击**编辑计划**。“计划”页面随即打开。备份规范的所有可用计划均列在右窗格中。
4. 单击要编辑的计划，然后单击**编辑计划**图标。计划向导随即打开。
5. 在“选项”页面查看设置，然后单击**下一步**。“重复”页面随即打开。
6. 在“重复模式”中，选择**一次**，然后指定起始日期、时区和必须开始备份的时间。您也可以指定备份持续时间，然后单击**下一步**。
7. 在“摘要”页面查看计划选项，然后单击**完成**。

如果对备份计划的时间已被计划备份占用，则新计划的备份将优先于上一个备份。

## 定期设置计划

定期计划是指按一定时间间隔运行的计划。例如，可能配置了定期备份，以便在周日 **3:00** 进行完整备份，然后每隔两天重复一次。下一次完整备份将在下周二 **3:00** 进行。定期备份简化了对于经常安排的备份的配置。

创建新的规范类型时通过按照向导操作，可以设置定期备份，或者可以修改现有规范的计划，如以下过程中所述：

这些过程中的步骤显示如何定期计划备份规范。计划向导中为您提供的选项基于您选择的规范类型。

## 使用预定义备份日程安排

使用预定义备份日程安排可简化对文件系统备份规范的配置。以后也可以修改日程安排。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开**文件系统**。此时将显示所保存的全部备份规范。
3. 右键单击合适的备份规范，然后单击**编辑计划**。计划向导随即打开。
4. 在“类型”页面，选择**预定义**，然后从预定义的计划列表中选择合适的计划，选择下列选项之一：



- **每日密集备份：**Data Protector 在午夜执行完整备份，并在每天 12:00(中午)和 18:00(下午 6 点)执行两次额外增量备份。
- **每日完整备份：**Data Protector 在每天 21:00(晚上 9 点)执行完整备份。
- **每周完整备份：**Data Protector 在每星期五执行完整备份，并在星期一至星期五的 21:00(晚上 9 点)执行增量 1 备份。
- **两周完整备份：**Data Protector 在每隔一周的星期五执行完整备份。在这些备份之间，Data Protector 会在每个星期一至星期五的 21:00(晚上 9 点)执行增量 1 备份。
- **每月完整备份：**Data Protector 在每月的第一天执行完整备份，每周执行增量 1 备份，每隔一天执行一次增量备份。

单击**下一步**。“选项”页面随即打开。

5. 在“选项”页面指定选项，然后单击**下一步**。“重复”页面随即打开。
6. 在“重复”页面指定选项，然后单击**下一步**。“摘要”页面随即打开。
7. 检查计划选项并单击**完成**。

## 配置重复计划

您可以创建计划，以使其在特定时间和日期开始，并按照定义的模式重复。例如，可以安排在接下来半年内每周五的 21 点进行一次完整备份。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 右键单击合适的备份规范，然后单击**编辑计划**。计划向导随即打开。
4. 在“类型”页面，选择**自定义**，然后单击**下一步**。“选项”页面随即打开。
5. 在“计划名称”文本框中，输入新计划的名称。选择备份类型(完整或增量；对于特定集成还有某些其他地方备份类型)，备份保护、优先级和网络负载。单击**下一步**。“重复”页面随即打开。
6. 在“重复模式”中，从以下选项中选择模式和频率：
  - **每天：**计划定期在指定时间运行。您可以使用“每 <value> 天”字段，指定计划频率。例如，如果重复值为 4，表示每 4 天运行一次计划。
  - **每周：**计划每周在指定日期运行。您可以使用“每 <value> 周”字段，指定计划频率。例如，如果重复值为 2，表示每 2 周在选定星期数运行计划。
  - **每月：**计划每月在当月的指定日期运行。您可以使用“每 <value> 月”字段，指定计划频率。例如，如果重复值为 2，表示每 2 个月在选定某天运行计划。

7. 从以下选项中指定重复的范围，然后单击**下一步**。
  - 开始：计划的初始日期。指定日期、时区和必须开始计划的时间。
  - 重复结束：最后一个计划必须运行的日期。如果计划必须无限期运行，选择**无结束日期**。

**注意：**

如果将循环设置为 2 次或更多次(例如每隔 2 周的周六)，但不设置启动日期，则由于 **Data Protector** 日程安排算法，可能无法在符合您的选择的第一个日期安排第一次备份(例如将在第二个周六安排第一次备份)。

8. 在“摘要”页面查看计划选项，然后单击**完成**。
9. 在 **ZDB 到磁盘 + 磁带**或 **ZDB 到磁盘**(启用了即时恢复)的情况下，指定分割镜像/快照备份选项。  
单击**确定**。

如果日程安排有冲突，则 **Data Protector** 将通知您，以使您可以修改日程安排。

## 计划提示

创建计划时，使用以下提示：

- 启动计划时，**Data Protector** 尝试分配所有需要的资源，如许可证、设备和 IDB 的访问权限。如果所需的某个资源不可用，则将会话排入队列，同时 **Data Protector** 每分钟都尝试为排队的会话获得所需资源，直到达到超时时间为止。通过更改 **SmWaitForDevice** 全局选项，可以修改超时。  
**Data Protector** 获得资源后，即启动排队的会话。排队的会话启动时可能不遵循其显示顺序。
- 为防止 **Cell Manager** 过载，默认情况下将以保守方式限制单元中的并发会话数。如果同时计划的会话数超过了有效限制，并且有效限制低于最大可配置限制，则超过的会话将排入队列。可以使用 **MaxBSessions** 全局选项修改此限制。  
另一方面，同时调用的、超过最大可配置限制的会话将不会启动，相关错误将记录到 **Data Protector** 事件日志中。
- 为了简化安排，**Data Protector** 为组客户机提供了备份规范。一个备份规范中配置的所有客户机将同时在一个备份会话中进行备份。
- 请确保有足够的介质和设备能够顺畅地运行无人看管备份。
- 应用备份模板时，模板的计划设置优先于备份规范的计划设置。应用模板之后，仍可修改备份规范并设置不同的计划。
- 计划程序粒度通过重复模式设置，至少为 1 分钟或更多。
- 备份和复制会话是资源密集型进程(尤其是在介质代理服务服务器上)，启动后需要为它们分配内存。因此，需要确保不同时启动多个备份和复制会话。例如，如果您需要在下午 6 点左右启动 9 个备份规范，则必须在下午 5:45 启动前 3 个备份，在下午 6:00 启动接下来的 3 个备份，并在下午 6:15 启动最后 3 个备份。不应将所有 9 个备份规范均计划在下午 6:00 启动。

# 第 8 章：设备

## 关于备份设备

**Data Protector** 定义具有 **Data Protector** 使用情况属性的物理设备，并为其建立模型。多个 **Data Protector** 设备定义可以引用同一个物理设备。通过此设备概念，可方便灵活地配置设备，并在备份规范中使用这些设备。

## 什么是备份设备？

一种物理设备，被配置为与可从存储介质读取数据和向其写入数据的 **Data Protector** 配合使用。例如，此设备可以是独立的 **DDS/DAT** 驱动器或库。

有关 **Data Protector** 支持的设备的列表，请参见 **Data Protector** 设备支持矩阵。可使用 **scsitab** 文件配置不受支持的设备。

某些备份设备(如磁带驱动器)受特定 **Data Protector** 许可证管辖。有关详细信息，请参见《*Data Protector 安装指南*》。

## 关于配置备份设备

完成准备部分之后，可以配置备份设备，使其与 **Data Protector** 配合使用。

建议让 **Data Protector** 自动配置备份设备。**Data Protector** 可以自动配置最常用的备份设备(包括库)。虽然仍需要为备份会话准备介质，但 **Data Protector** 可确定设备的名称、策略、介质类型、介质策略和设备文件或 **SCSI** 地址，并且还可配置驱动器和插槽。

也可以手动配置备份设备。配置备份设备的方式取决于设备类型。

可以使用未在 **Data Protector** 产品声明、软件说明和参考中列为受支持的设备。将使用 **scsitab** 文件配置不支持的设备。

**注意：**外部控制是控制 **Data Protector** 未知的库的一种方法。如果 **Data Protector** 不支持某个特定设备，则用户可以编写相应的脚本/程序，以运行机械手控制，将介质从特定插槽加载到指定的驱动器中。通过引用特殊脚本，可以将库配置为外部控制。

## 备份设备的类型

**Data Protector** 支持以下可配置的设备类型(取决于已安装的组件)：

- 独立
- 备份到磁盘设备
- **SCSI** 库
- 堆栈器
- 箱盒设备

- 介质库
- 独立文件设备
- 文件库设备
- 外部控制
- ADIC/GRAU DAS 库
- StorageTek ACS 库

## 独立

独立设备是包含一个驱动器的简单设备，该驱动器一次从一个介质读取或写入一个介质(如 DDS 或 DLT)。这些设备用于小规模备份。介质充满后，操作员必须手动将其替换为新介质，备份才能继续。因此，独立设备不适合大规模的无人看管备份。

## 备份到磁盘设备

备份到磁盘 (B2D) 设备是基于磁盘的存储设备，与 Data Protector 介质库或文件库设备相比，可提供附加功能，如通过多个主机(网关)进行访问，或重复数据删除(具体取决于设备类型)。

## SCSI 库

SCSI 库设备是大型备份设备，也称为自动加载器。这些设备由设备存储库中的大量介质磁带盒组成，并且可以有多个驱动器，一次处理多个介质。大多数库设备在驱动器变脏时还可以自动清洗驱动器。

典型的库设备中，每个驱动器和库的一个机械手机构(可将介质从插槽移至驱动器，然后将其移回)有一个对应的 SCSI ID(Windows 系统)或设备文件(UNIX 系统)。(例如，一个由四个驱动器组成的库拥有五个 SCSI ID，四个用于驱动器，一个用于机械手装置)。

介质存储在设备存储库的插槽中。Data Protector 向每个插槽分配一个数字，从一开始。管理库时，要使用其数字引用插槽。

驱动器索引标识驱动器在库中的机械位置。索引编号与机械手控制紧密相关。库机械手只了解驱动器索引编号，而没有有关驱动器 SCSI 地址的信息。驱动器索引是一个顺序整数(从 1 开始)，必须与驱动器的 SCSI 地址相结合。SCSI 库、Commandview TL 的许多 Web 界面或 SCSI 库的控制面板将从“0”开始对驱动器编号。驱动器“0”在 Data Protector 设备配置中无效，第一个驱动器必须始终为“1”。

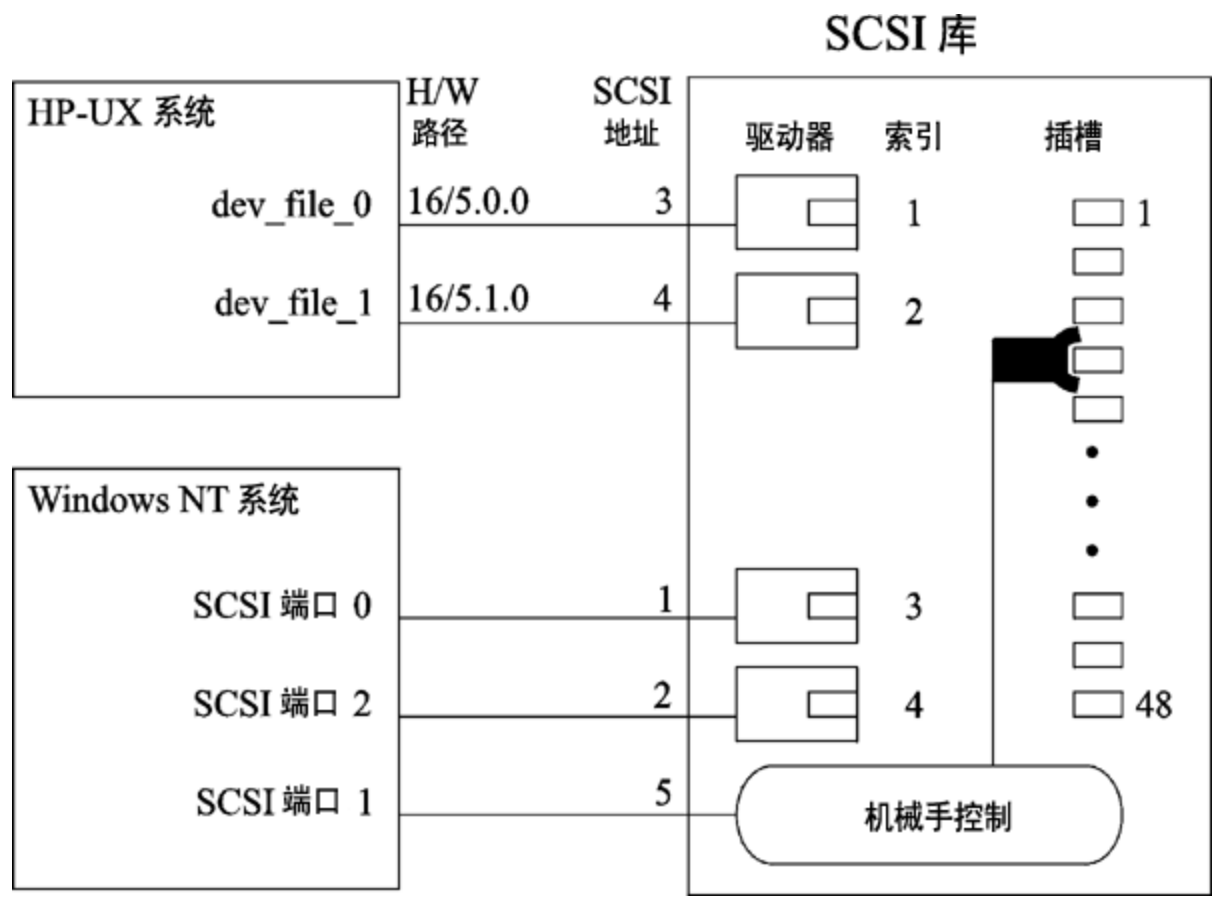
例如，对于四个驱动器的库，驱动器索引为 1、2、3 和 4。如果库中只有一个驱动器，则驱动器索引为 1。

驱动器索引必须与相应的 SCSI 地址匹配。这意味着需要配置各对内容：

SCSI address\_A 对应于索引 1，SCSI address\_B 对应于索引 2，以此类推。

配置箱盒设备时，还要指定此类型的设备。

**驱动器索引到 SCSI 地址的映射**



## 堆栈器

堆栈器是一个单独的设备，通常其中只有一个驱动器。它顺序而非随机加载介质，因此建议使用宽松介质分配策略。堆栈器从“堆栈”(其存储库)中提取介质，并将介质插入其驱动器中。这种交换始终仅限于弹出已在驱动器中的介质以及插入来自堆栈的下一个介质。自动完成加载，但必须手动加载第一个介质。磁带已满后将弹出，并自动加载下一个磁带。堆栈器箱盒中的所有磁带用完后，必须手动卸载箱盒，然后插入下一个箱盒。仍然必须将第一个磁带手动加载到驱动器中。

如果没有介质，则不会中止备份或还原会话，而是将发出一个装载请求。如果在一个超时周期内不更改堆栈器箱盒，则将不会中止整个会话。

## 箱盒设备

箱盒设备将许多介质组成一个单位，称为箱盒。通过箱盒，可以比使用许多单独的介质更方便地处理大量数据。箱盒中每个介质上的操作都由 **Data Protector** 完全控制。可以将 **XP DAT 24x6** 配置为箱盒设备。

## 介质库

介质库是一种库设备。它可以包含光盘或文件介质。如果设备用于容纳文件介质，则将其称为文件介质库设备。在初始配置期间定义设备将容纳的介质类型。

如果要在 **UNIX** 上运行光盘介质库，则需要为每个交换器插槽或盘面配置一个 **UNIX** 设备文件。

## 独立文件设备

独立文件设备是指定目录中的一个文件，您向该文件备份数据而非写入磁带。

## 文件库设备

文件库设备由一组目录组成，您向这组目录备份数据而非写入磁带。

## 外部控制

外部控制是控制 **Data Protector** 未知的库的一种方法。如果 **Data Protector** 不支持某个特定设备，则用户可以编写相应的脚本/程序，以运行机械手控制，将介质从特定插槽加载到指定的驱动器中。通过引用特殊脚本，可以将库配置为外部控制。

## ADIC/GRAU DAS 库

**ADIC/GRAU DAS** 库是一种大型的库 (silo)。它用于备份数据量极大，且存储数据所需的介质数量也很大的复杂环境中。它可以处理成百上千个磁带。通常，**ADIC/GRAU DAS** 库可以容纳多种类型的备份驱动器和数千个介质插槽，所有这些都由内部机械手装置提供服务，并通过特殊的库控制单元进行控制。可以将库中的一组专用介质分配给应用程序，以便可以在 **Data Protector** 与其他应用程序之间共享该库。

可以从 **Data Protector** 用户界面执行所有介质操作。对于采用可识别格式的介质，**Data Protector** 将该格式显示为如 **tar** 等介质类型。对于采用无法识别格式的介质，介质类型为 **foreign**。

介质管理数据库跟踪所有 **Data Protector** 和非 **Data Protector** 介质，无论驻留(介质在设备的存储库中)还是非驻留(介质在设备的存储库以外)，同时提供成熟的覆盖保护。**Data Protector** 不会覆盖采用可识别格式的含数据介质。但是，无法保证使用相同介质的某些其他应用程序不会覆盖磁带上的 **Data Protector** 数据。建议 **Data Protector** 所使用的介质不要由任何其他应用程序使用，反之亦然。

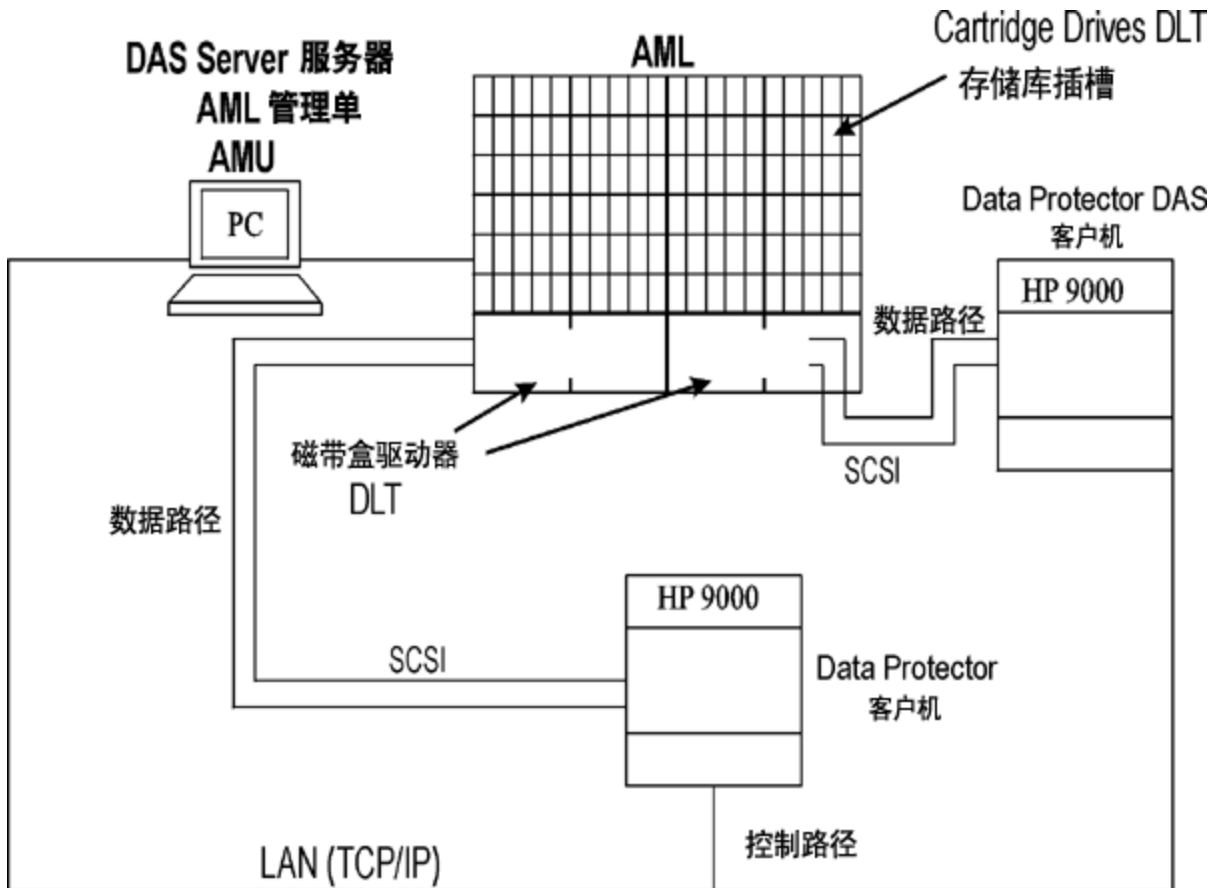
介质的实际位置由 **DAS** 服务器维护，该服务器使用其 **volser** 跟踪该位置。在存储库中到处移动介质时，并非每次都向该介质分配相同的物理插槽。因此，处理介质时不能依赖于插槽号，而是要依赖于条形码 (**volser**)。

使用驱动器所设置的次数之后，**ADIC/GRAU DAS** 库可以自动清洗其驱动器。但是，建议不要这么做，因为驱动器清洗将中断当时正在运行的会话，从而导致该会话失败。如果要使用库的清洗功能，则必须确保在没有 **Data Protector** 会话运行时执行驱动器清洗。

**重要：**

必须为每种介质类型创建一个逻辑 Data Protector 库。虽然 ADIC/GRAU 或 STK ACS 系统可以存储许多在物理上不同类型的介质，但 Data Protector 只能识别仅含其中一种介质类型的库。

**Data Protector 与 ADIC/GRAU DAS 库系统的集成**



## StorageTek ACS 库

StorageTek Automated Cartridge System (ACS) 库是一种机械手库 (silo)。它用于备份数据量极大，且存储数据所需的介质数量也很大的复杂环境中。它可以处理数百个磁带。可以将设备中的一组专用介质分配给应用程序，以便可以在 Data Protector 与其他应用程序之间共享该库。

通常，此类设备有多种类型的备份驱动器和数千个介质插槽，所有这些都由内部机械手机构提供服务，并且通过 ACS Library Server (ACSL) 软件进行控制。由 Data Protector 发起的与介质和与设备相关的操作通过用户界面传递到 ACSLS，后者随后直接控制机械手，并执行介质的移动和加载。

正确安装和配置库后，通过 Data Protector 可在备份和还原会话期间轻松地处理介质。可以从 Data Protector 用户界面执行所有介质操作。对于采用可识别格式的介质，Data Protector 将该格式显示为如 tar 等介质类型。对于采用无法识别格式的介质，介质类型为 foreign。

介质管理数据库跟踪所有 Data Protector 和非 Data Protector 介质，无论驻留(介质在设备的存储库中)还是非驻留(介质在设备的存储库以外)，同时提供成熟的覆盖保护。Data Protector 不会覆盖采用可识别格式的含数据介质。但是，无法保证使用相同介质的某些其他应用程序不会覆盖磁带上的 Data Protector 数据。建议 Data Protector 所使用的介质不要由任何其他应用程序使用，反之亦然。

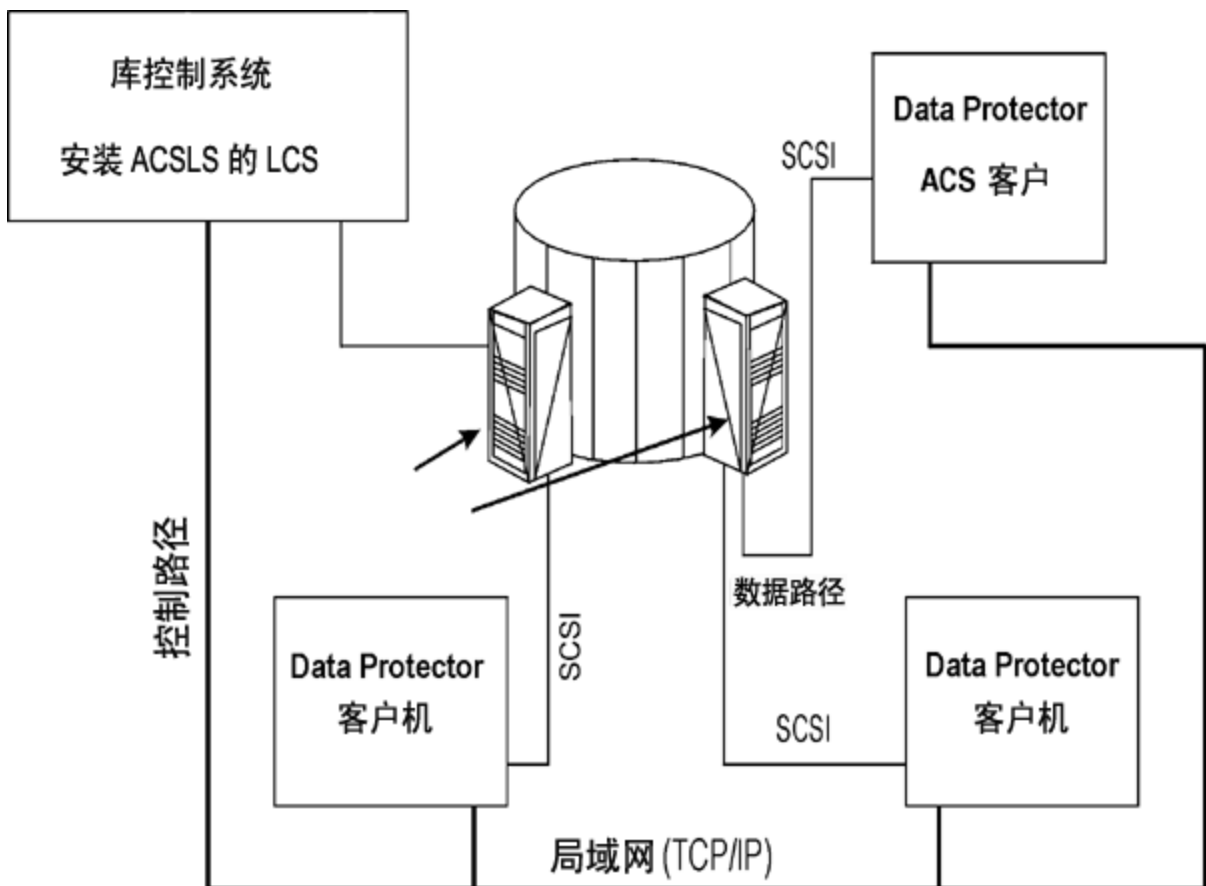
介质的实际位置由 ACS 服务器维护，该服务器使用其 volser 跟踪该位置。在存储库中到处移动介质时，并非每次都向该介质分配相同的物理插槽。因此，处理介质时不能依赖于插槽号，而是要依赖于条形码 (volser)。

使用驱动器所设置的次数之后，StorageTek ACS 库可以自动清洗其驱动器。但是，建议不要这么做，因为库驱动器清洗将中断当时正在运行的会话，从而导致该会话失败。如果要使用库的清洗功能，则必须确保在没有 Data Protector 会话运行时执行驱动器清洗。

**重要：**

必须为每种介质类型创建一个逻辑 Data Protector 库。虽然 ADIC/GRAU 或 STK ACS 系统可以存储许多在物理上不同类型的介质，但 Data Protector 只能识别仅含其中一种介质类型的库。

**Data Protector 与 StorageTek ACS 库的集成**





# 关于 **StoreOnce** 软件重复数据删除组件 安装

本节概述了安装 **StoreOnce** 软件重复数据删除组件时的主要安装任务和特定要求。

## 先决条件

确保已在支持的系统上安装 **Data Protector 10.00 Cell Manager**、用户界面客户机和安装服务器。

有关详细信息，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新 **Data Protector** 支持矩阵。有关如何在各种架构中安装 **Data Protector** 的信息，请参见《**Data Protector** 安装和许可指南》。

## 防火墙配置

确保已为传入的连接打开以下端口：

- 9387/tcp – 命令端口 (针对 **StoreOnce** 软件系统和 **StoreOnce** 备份系统)。
- 9388/tcp – 数据端口 (针对 **StoreOnce** 软件系统和 **StoreOnce** 备份系统)。

必须在防火墙中打开端口 **9387** 和 **9388**，将目标设备与任何网关分开。(Windows 系统：端口在安装过程中打开，UNIX 系统：端口必须手动打开。)有关 **Data Protector** 端口的详细信息，请参见《**Data Protector** 帮助》的索引：“端口范围”。

## 安装过程

在所有将成为网关的系统上安装 **Data Protector** 介质代理或 **NDMP** 介质代理组件，其中包括将启用源端重复数据删除的客户机。

有关说明，请参见《**Data Protector** 安装指南》。有关受支持操作系统版本的详细列表，请参见最新的支持矩阵，地址为：<https://softwaresupport.softwaregrp.com/>。

## **StoreOnce** 软件重复数据删除的其他步骤

在将托管 **StoreOnce** 存储区的系统上安装 **Data Protector StoreOnce** 软件重复数据删除组件。  
**StoreOnce** 软件重复数据删除组件可以本地安装或远程安装。

### 远程安装 **Data Protector StoreOnce** 软件重复数据删除组件

1. 通过 **Data Protector** 用户界面组件连接到任何客户机。
2. 打开 **Data Protector** GUI，在“上下文”列表中，选择“客户机”。
3. 将 **Data Protector StoreOnce** 软件重复数据删除组件添加到备份客户机：

- 如果备份客户机不是 **Data Protector** 单元的一部分，则使用 **Data Protector** 添加客户机功能。
- 如果备份客户机已经是 **Data Protector** 单元的一部分，则使用 **Data Protector** 添加组件功能。

成功安装后，**StoreOnce** 软件重复数据删除组件列在安装的组件列表中。  
在可以使用 **StoreOnce** 软件重复数据删除之前，必须配置存储的根目录。

## 本地安装 **Data Protector StoreOnce** 软件重复数据删除组件

**Windows 系统：**  
在本地安装 **Data Protector** 的过程中，在“组件”列表中选择 the **StoreOnce Software Deduplication** 组件。

**Linux 系统：**  
运行 `omnisetup.sh -installStoreOnceSoftware`。

## 设置 **StoreOnce** 软件服务/后台程序

**Windows 系统：**  
成功安装后，**StoreOnce** 软件可执行文件作为服务启动(请参见任务管理器中的“服务”选项卡)。服务名称是 **Data Protector StoreOnceSoftware**，描述是 **StoreOnce Software Deduplication**，启动类型是自动。

**Linux 系统：**  
要安装 **StoreOnce** 软件后台程序，以使其在系统重新启动后自动启动，请将文件 **StoreOnceSoftwared** 复制到 `/etc/init.d` 目录并将其包含在启动脚本中。也可以使用命令手动启动或停止后台程序：

```
/opt/omni/sbin/StoreOnceSoftwared start
```

和

```
/opt/omni/sbin/StoreOnceSoftwared stop
```

从系统中删除 **StoreOnce** 软件重复数据删除组件可自动停止进程，并从 `/etc/init.d/` 目录中删除文件 **StoreOnceSoftwared**。

## 安装的目录结构

**Windows 系统：**  
安装组件包括以下文件：

文件名(F)	文件位置
StoreOnceSoftware.exe	Data_Protector_home\bin
system.db	Data_Protector_program_data\Config\client\StoreOnceSoftware

**Linux 系统：**  
成功安装后，**StoreOnce** 软件作为后台进程(后台程序)启动。重新启动后，可以自动启动。  
安装组件包括以下文件：

文件名(F)	文件位置
StoreOnceSoftware	/opt/omni/lbin
StoreOnceSoftwared	/etc/init.d/ /opt/omni/lbin
system.db	/etc/opt/omni/client/StoreOnceSoftware

## 故障排除

本节提供使用 **Data Protector StoreOnce** 软件集成时的日志和事件报告、警告、诊断及问题解决信息。有关一般 **Data Protector** 故障排除信息，请参见《**Data Protector** 故障排除指南》。

## 磁盘空间不足警告

为避免存储区所在的磁盘空间不足，当达到预定义阈值时，将写入警告消息(Windows 系统上的事件日志或 Linux 系统上的 **Syslog**)。阈值的默认值是存储区容量的 10%。默认值可以使用 **omnirc** 选项进行修改。在对存储执行任何进一步读取/写入操作之前，或者如果 **StoreOnce** 软件实用程序重新启动，警告消息每天发出一次。在会话开始和结束时，警告还显示在备份会话消息中。磁盘空间不足警告消息是：

You are running out of disk space on Deduplication Store root directory: [path].  
The threshold x% is reached. Please free space or add more disks. [warning].

## system.db 文件的备份

**system.db** 数据库文件包含根目录信息及有关存储区的信息。该文件位于 *DataProtector\_Program\_Data\OmniBack\Config\client\StoreOnceSoftware* 下。如果该文件被删除或丢失，则无法访问存储区和已备份的数据。为避免出现此情况，每次更改数据库时，将 **system.db** 文件的备份复制到 *.\Store\_Root\StoreOnceLibrary\system.db.bak*。通过将备份文件复制到原始位置，重命名并重新启动 **StoreOnce** 软件实用程序，可还原 **system.db** 文件。

确保根目录下的文件受到保护(RAID 或备份)。

下方列出了 **StoreOnce** 软件实用程序报告的常见问题和错误。错误通常与操作环境和重复数据删除存储区的目录结构相关。

**StoreOnce** 软件实用程序未能找到存储区的根目录。

问题
Accessing the system.db file: The system.db file is inaccessible (for example, permission denied, or disk full).
操作
更改权限，释放磁盘空间，或使数据库可访问。对于重复数据删除存储区的根目录，

数据库文件 (**system.db**) 包含空值或无值。

**StoreOnce** 软件实用程序未能启动。

**问题**

访问 **system.db** 文件：存储区根目录中的 **system.db** 文件丢失。

**操作**

还原或重新创建 **system.db** 文件。请参见上一问题。

在存储区的启动过程中，记录了错误。无法访问存储区。

**问题**

启动存储区：无法访问存储目录。

**操作**

使存储区的目录可访问，检查权限并验证根目录是否存在。

已成功启动存储区，但没有找到项目。

**问题**

启动存储区：存储区目录丢失。

**操作**

还原根目录和根目录下的存储区。

记录了错误。无法访问存储区。

**问题**

启动存储区：存储区较脏，无法恢复。

**操作**

还原根目录和根目录下的存储区。

停止存储区时报告错误。

**问题**

停止存储区：项目打开(例如，备份或还原会话正在运行)。

**操作**

在停止 **StoreOnce** 软件实用程序之前，检查所有操作是否均已完成。

关闭过程中报告了错误。恢复可能发生在下一次启动时。

问题
停止存储区：无法停止内务管理实用程序。
操作
检查所有操作是否均已完成，然后停止 <b>StoreOnce</b> 软件实用程序。恢复可能发生在下一次启动时。

当可用磁盘空间不足时，将记录警告消息。

问题
由于磁盘空间和内存不足， <b>StoreOnce</b> 软件服务/后台程序在 Windows 事件日志或 Linux syslog 中记录了警告和错误消息。  当系统达到剩余可用虚拟内存的 <b>25%</b> 时，记录了警告消息，当只剩下剩余可用虚拟内存的 <b>20%</b> 时，记录了错误消息，服务/后台程序开始拒绝读取和写入操作。
操作
释放系统资源。释放磁盘空间或内存后，服务/后台程序将停止拒绝操作。

**Data Protector** 显示警告“存储区不存在”，并且备份会话失败。

问题
使用 <b>StoreOnce</b> 备份系统设备执行备份会话时， <b>Data Protector</b> 显示类似以下的警告，并且会话异常结束：  [Warning] From: BSM@computer.company.com "CS2BackupTmp" Time: 6/18/2012 1:34:08 PM Got error: " Store does not exist. " when contacting " DeviceName" B2D device!  如果 <b>B2D</b> 设备上已删除此存储或已修改此存储的访问权限，则可能会出现此问题。
操作
<ul style="list-style-type: none"><li>• 检查存储区是否存在，或是否已修改此存储区的任何权限。</li><li>• 如果已正确设置存储区，则检查 <b>Data Protector</b> 中的设备设置。右键单击设备，选择“属性”，并在“设备 - 存储和网关”页面检查“客户机 ID”。</li></ul>

**B2D** 设备的状态更新按指定时间间隔执行。

问题
已超出备份大小软配额或存储区大小软配额，但 <b>Data Protector</b> 没有报告任何警告。
操作
无。下一个备份会话将正确报告警告。

# 关于 StoreOnce 存储区和 DD Boost 重复数据删除设备

Data Protector 支持 HPE (StoreOnce) 和 EMC (DD Boost) 的重复数据删除产品。Catalyst 是指在前一个产品中管理重复数据删除的软件，在以下材料中互换使用。有关详细信息，请参见 *Data Protector* 概念指南。

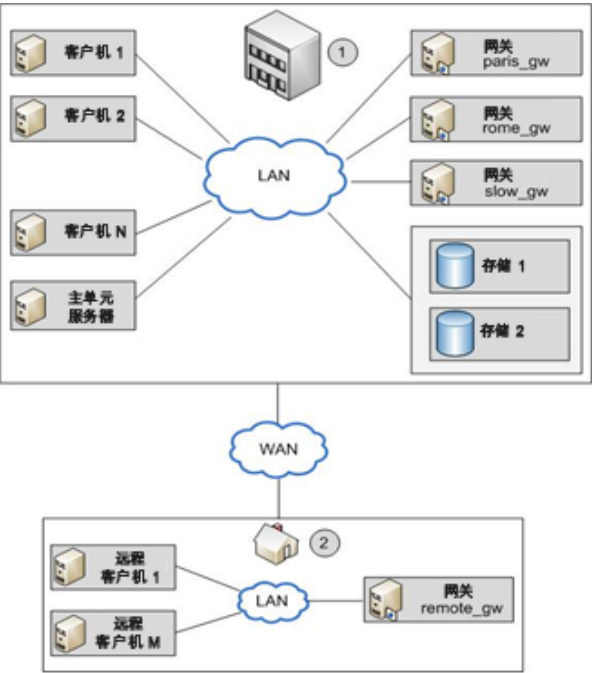
本节包含示例环境和配置过程。

## 多接口支持

Data Protector 提供多接口支持，IP 和 FC 连接可导致相同的 Catalyst 或 Boost 存储区。Data Protector 支持与同一 Catalyst/DDBoost 存储区建立 IP 以及光纤通道连接，而无需配置单独的存储区。可同时通过这两种接口访问存储。例如，有时本地客户机可通过光纤通道访问单个 Catalyst/DDBoost 存储以执行较快的备份，而远程客户机可通过 WAN 访问同一存储以执行较慢的备份。

### 使用 B2D 设备的配置示例

下图提供中央办公室/远程办公室配置的典型使用模型。



项目	说明
1	中央办公室。该 LAN 位于中央办公室。通过 WAN 连接到远程办公室的 LAN。
2	远程办公室。该 LAN 位于远程办公室。

Data Protector Cell Manager 安装在主机 *master* 的中央办公室中。中央办公室有多个客户机：*client1* 到 *clientN* (非网关客户机)、*paris\_gw*, *rome\_gw* 和 *slow\_gw* (网关客户机)。此外，在中央办公室配置了两个对象存储区 (Store1 和 Store2)。

远程办公室包括客户机 *remote1* 至 *remoteM* 和 *remote\_gw*。远程办公室的所有客户机属于与中央办公室的客户机相同的 Data Protector 单元。远程办公室通过较慢的 WAN 网络连接至中央办公室。

**注意：**

网关只是安装有介质代理组件的客户机。将它们视为网关客户机。客户机若要成为网关，则必须是 64 位系统。

配置 B2D 设备时，您必须指定某些参数，如存储区的名称和位置、网关、网络路径。在上述示例中，您想要使用存储区 Store1 (通过 StoreOnce 软件重复数据删除访问)，以用于在您的环境中备份客户机。为此，您可将 B2D 设备配置为将 Store1 用作存储库。您还决定，客户机 *paris\_gw*、*rome\_gw* 和 *slow\_gw* 将用作中央办公室的其他 Data Protector 客户机的网关。此外，请注意以下事项：

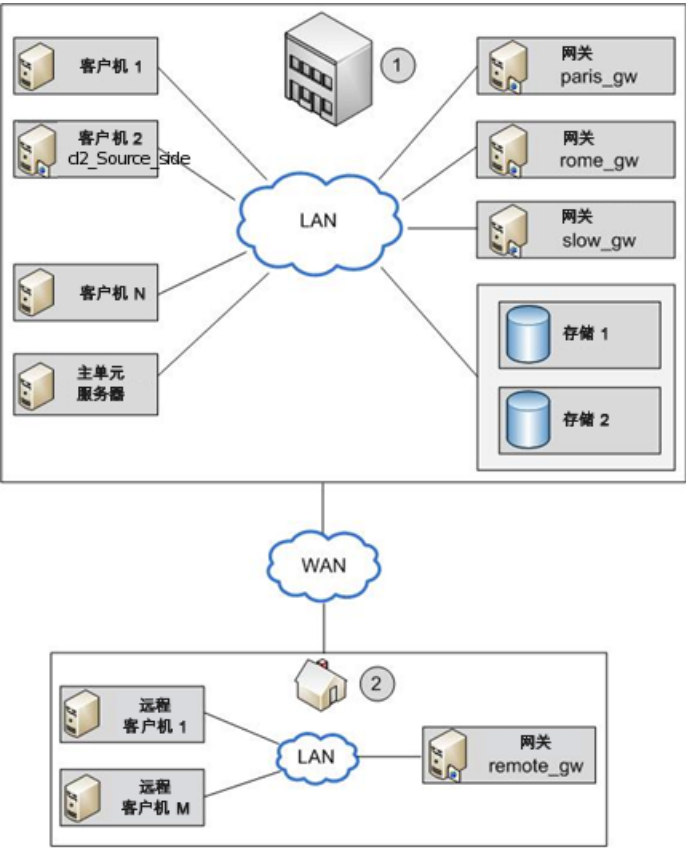
- 并发可指定多个并行写入到设备的磁盘代理。多个磁盘代理并行读取数据 (从磁盘)，为介质代理提供连续的数据流。借助 StoreOnce 软件重复数据删除，每个介质代理的磁盘代理并发设置为 1 (这样可以改善重复数据删除比率)。
- Data Protector 支持备份到未加密存储区和已加密存储区。可在创建存储区时启用加密功能。注意，存储区一经创建，就不能将其从已加密状态更改为未加密状态，反之亦然。
- 每个设备只能配置一个存储区。
- 存储区由包含重复数据删除系统和存储名称相关信息的网络路径 (UNC) 表示。(注意：在 B2D 设备的环境中，重复数据删除系统是指重复数据删除存储区所在的宿主计算机的名称。)

## 源端重复数据删除

如果各个客户机的备份数据量有限，则上述场景适用。然而，为减少网络流量，您可以配置源端网关。

例如，在我们的场景中，*client2* 系统上有许多重复的数据，但系统负载属于中度。为减少网络负载，您可以启用 B2D 设备的源端重复数据删除。如果您在 *client2* 的备份规范中也启用了源端重复数据删除，则将在 *client2* 上自动创建源端网关，介质代理将仅通过网络发送删除重复的数据。

同样，如果您为其他客户机启用源端重复数据删除，也将这些客户机上自动创建源端网关。



## 添加 B2D 设备

添加 B2D 设备的步骤与添加设备类型的步骤类似。有关详细信息，请参见《Data Protector 在线帮助》和《Data Protector 管理员指南》。

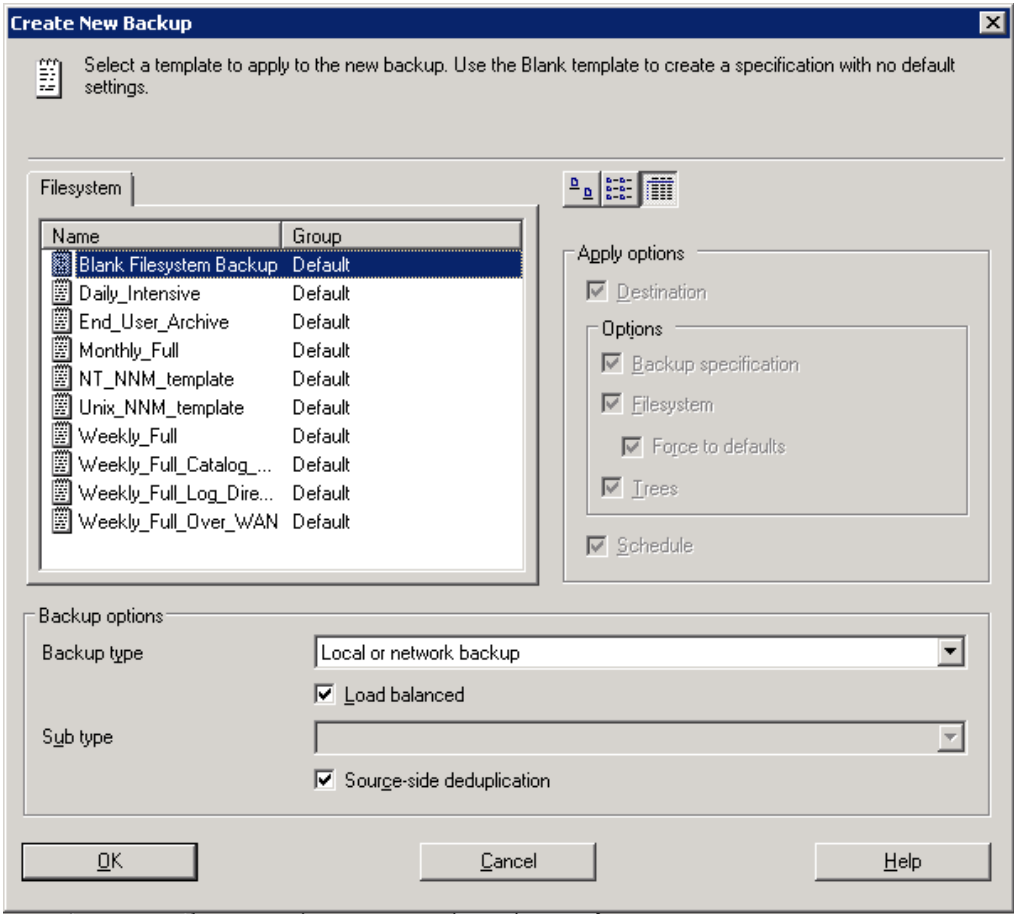
## 备份

在备份规范中指定 B2D 设备可告知 Data Protector 执行重复数据删除类型备份。重复数据删除进程在后台运行，删除重复的数据写入到 StoreOnce 软件系统或 StoreOnce 备份系统。

您执行与传统备份相同的重复数据删除类型备份：

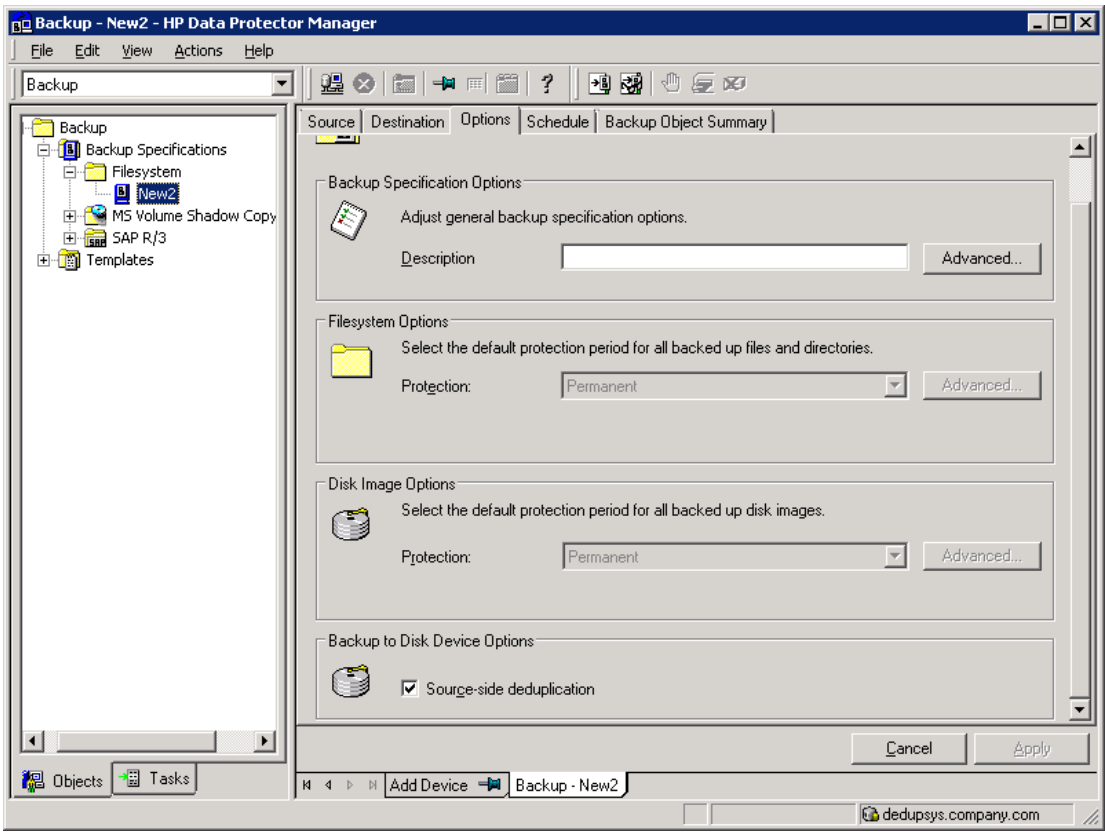
1. 添加新的 B2D 设备(在此例中，通过指定 StoreOnce 软件重复数据删除或 StoreOnce 备份系统)。
2. 创建以该设备为目标的备份规范。请参见《Data Protector 帮助》的索引：“创建, 备份规范”。或者，要启用源端重复数据删除，请在创建备份规范时选择源端重复数据删除选项。





在“源”页面选择备份对象时，Data Protector 将用阴影表示所有未配置源端网关的客户机。通过在“显示”下拉列表中选择**源端重复数据删除**，您可以过滤客户机列表。

或者，选择备份规范，打开“选项”窗格，并选择**源端重复数据删除**。



3. 在“目标”页面，选择将用于备份的网关。单击**属性**以查看和修改网关选项。注意，通过指定选项**每个网关的并行流的最大数量**，将覆盖在设备配置过程中设置的值。

**注意：**  
选择源端重复数据删除时，您只能备份支持源端网关的客户机中的对象，而且只能选择带有源端网关的设备。如果取消选择该选项，Data Protector 将自动选择 B2D 设备的所有网关，而非源端网关，并显示警告消息。

**重要：**  
如果您在现有备份规范中启用源端重复数据删除，则取消选中且不备份无法执行源端重复数据删除的客户机。

## 还原

使用与传统还原操作相同的方法还原备份的数据。虽然与传统还原进程相比，从重复数据删除存储区中检索数据的后台进程明显不同，但不执行任何特殊任务。检索进程的主要操作包括，将待还原数据加载到内存，从索引表读取参考信息，并使用该信息再水合备份数据。请参见《Data Protector 帮助》的索引：“还原”。

## 源端重复数据删除注意事项

如果执行备份时已启用源端重复数据删除且在不支持源端网关的客户机上执行还原，则 will 使用普通网关。

## 基于光纤通道的 Catalyst 的 StoreOnce Catalyst 客户机配置

### 注意：

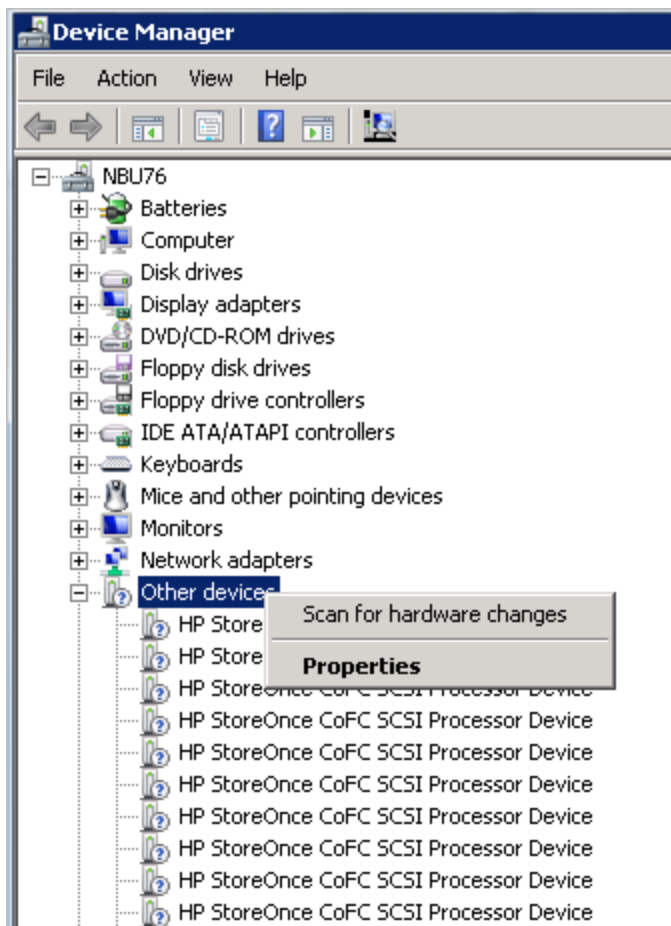
以下信息不是权威信息。有关最新且最详细的信息，请参阅 StoreOnce 文档。

## Windows 客户机

通过光纤通道备份运行 Catalyst 需要管理员权限。

基于光纤通道的 StoreOnce Catalyst 表示**处理器**的一种设备类型。对设备进行分区或更改每个启动器端口的设备数量后，请执行以下操作：

1. 转到 **Windows 设备管理器**，右键单击**其他设备**。
2. 选择**扫描硬件更改**，以检测新设备。



## Linux 客户机

基于光纤通道的 **StoreOnce Catalyst** 表示处理器的一种设备类型。在 **Linux** 上，设备文件在 **/dev/sg\*** 中创建。默认情况下，只有根用户才能访问 **/dev/sg\*** 设备。对于非根用户，使用 **Linux udev** 规则提供备份用户权限，以访问设备文件。

要创建 **udev** 规则，请执行以下操作：

- a. 在每个备份服务器的以下位置，创建 **udev** 文件：

```
/etc/udev/rules.d/70-cofc.rules
```

- b. 在文件中添加以下规则：

```
KERNEL=="sg[0-9]*", ATTRS{vendor}=="HP*", ATTRS{model}=="StoreOnce CoFC*",  
ATTRS{rev}=="CAT1", GROUP="###CORRECT_USER_GROUP###"
```

其中，**###CORRECT\_USER\_GROUP###** 替换为 **Linux** 用户组，将执行备份和还原。例如，**dba/oracle**。

- c. 扫描设备文件更改，以更新权限。

**lsscsi --generic** 命令可用于确定哪个 **/dev/sg\*** 设备文件属于基于光纤通道的 **Catalyst**。

## AIX 客户机

在 **StoreOnce** 软件 3.14 版本之前，只能通过请求使用 **AIX** 上基于光纤通道的 **StoreOnce Catalyst**。

### 注意：

在 **StoreOnce** 版本低于 3.14 的 **AIX 6.1** 或 **7.1** 上，如果您需要基于光纤通道的 **Catalyst**，请联系 **StoreOnce** 支持。

基于光纤通道的 **StoreOnce Catalyst** 代表 **AIX** 上的顺序的一种设备类型。这些设备文件在 **/dev/rmt\*** 位置创建。对设备进行分区或更改每个启动器端口的设备数量后，请执行以下操作：

- a. 执行 **storeonce-cofc-passthrough-install.sh** 脚本。

### 注意：

该安装脚本是 **StoreOnce** 软件套件的一部分，不是 **Data Protector** 的一部分。

- b. 作为根用户执行 **cfgmgr** 命令，以扫描设备文件中的更改。
- c. 默认情况下，只有根用户才能访问 **/dev/rmt\*** 设备文件。作为根用户运行备份需要其他权限。

## HP-UX 客户机

基于光纤通道的 **StoreOnce Catalyst** 表示处理器的一种设备类型。在 **HP-UX** 上，设备文件在 **/dev/pt/ptX** 位置创建。

对设备进行分区或更改每个启动器端口的设备数量后，请执行以下操作：

- a. 扫描设备文件更改。
- b. 作为根用户执行 **ioscan -fnC /dev/pt** 命令。

默认情况下，只有根用户才能访问 `/dev/pt/ptX` 设备。对于非根用户，使用 `chmod o+rwX /dev/pt/pt*` 命令提供备份用户权限，以访问设备文件。

- c. 要获得 `/dev/pt/ptX` 设备文件的权限，请使用基于光纤通道的 Catalyst 命令：  

```
/usr/sbin/scsimgr -p get_attr all_lun -a device_file -a dev_type -a pid |  
grep StoreOnce
```
- d. 在相应设备上使用 `chmod o+rwX` 命令。

## Solaris 客户机

基于光纤通道的 StoreOnce Catalyst 表示处理器的一种设备类型。在 Solaris 上，设备文件在 `/dev/scsi/processor/*` 位置创建。对设备进行分区或更改每个启动器端口的设备数量后，请执行以下操作：

- a. 扫描设备文件更改。
- b. 如果您是根用户，请执行以下命令：
  - `add_drv -vi scsiclass,03 sgen`
  - `update_drv -vai scsiclass,03 sgen`

默认情况下，只有根用户才能访问 `/dev/scsi/processor/*` 设备。对于非根用户，使用 `chmod -R o+rwX /dev/scsi/processor/*` 命令提供备份用户权限，以访问设备文件。
- c. 要获得 `/dev/scsi/processor/*` 设备文件的权限，请使用基于光纤通道的 Catalyst 命令：  

```
for i in /dev/scsi/processor/*; do echo $i; ls $i; luxadm inq $i | egrep  
"Vendor|Product"; echo; done
```
- d. 在相应设备上使用 `chmod -R o+rwX` 命令。

## 与 B2D 设备相关的 omnirc 选项

Omnirc 文件通过其他选项增强。使用该文件设置端口号和磁盘空间阈值警告等参数。

`OB2_STOREONCESOFTWARE_COMMAND_PORT=PortNumber`

该选项更改用于介质代理和 StoreOnce 软件实用程序之间的命令通信的端口。

例如： `OB2_STOREONCESOFTWARE_COMMAND_PORT=12345`

默认值： 9387

`OB2_STOREONCESOFTWARE_DATA_PORT=PortNumber`

该选项更改用于介质代理和 StoreOnce 软件实用程序之间的数据通信的端口。

例如： `OB2_STOREONCESOFTWARE_DATA_PORT=12346`

默认值： 9388

`OB2_STOREONCESOFTWARE_SESSION_IDLE_TIMEOUT=s`

**StoreOnce** 软件后台程序定期检查空闲连接并终止这些连接。该选项指定闲置秒数，之后，连接被视为空闲。

默认值：300(范围：最小：10)

**OB2\_STOREONCESOFTWARE\_DISK\_SPACE\_THRESHOLD=%**

该选项将设置可用磁盘空间的阈值。

默认值：10%(范围：1% - 95%)

**OB2\_STOREONCESOFTWARE\_MINIMUM\_DISK\_SPACE=n**

该选项控制 **StoreOnce** 软件需要保留的最小磁盘空间(以 MB 为单位)。如果达到该最小值，向任何存储写入数据的操作将失败。默认值：1000(最小：500)

**OB2\_STOREONCESOFTWARE\_SSL\_ENABLE=0|1**

默认值：1

该选项启用或禁用客户机与 **StoreOnce** 软件后台程序之间的安全控制通信。注意，即使 **StoreOnce** 软件后台程序运行的客户机使用安全控制通信，但如果您将该选项设置为 0，也将不使用。

启用安全通信后，手动重新启动 **StoreOnce** 软件后台程序。

**OB2\_STOREONCESOFTWARE\_DISABLE\_IPV6\_LISTEN=0|1**

默认值：0

默认情况下，**StoreOnce** 软件后台程序侦听双堆栈套接字(相同端口上的 IPv6 和 IPv4)。如果设置为 1，IPv6 被禁用。该选项适用于 RPC 和 lpcServer 侦听端口。

**OB2D2D\_COMMAND\_PORT=PortNumber**

该选项更改用于介质代理和 **StoreOnce** 备份系统之间的命令通信的端口。

例如：OB2D2D\_COMMAND\_PORT =12345

默认值：9387

**OB2D2D\_DATA\_PORT=PortNumber**

该选项更改用于介质代理和 **StoreOnce** 备份系统实用程序之间的数据通信的端口。

例如：OB2D2D\_DATA\_PORT=12346

默认值：9388

**OB2D2D\_NUM\_OF\_LBWTHREADS=ThreadNum**

定义在介质代理客户机上执行重复数据删除时用于重复数据删除计算的线程数量。如果您具备更强大的网关，您可以将该数字增加至 8 个线程。必须在每个网关上单独设置该选项。

默认值：4

`OB2D2D_BANDWIDTH_BUFF_SIZE=Size`

设置在介质代理客户机上执行重复数据删除时的缓冲区大小。当介质代理通过 LAN 与 D2D 设备通信时，默认设置合适。当 WAN 网络用于通信时，更合适的值是 20 MB。必须在每个网关上单独设置该选项。

默认值：10 MB

## 关于云 (Helion) 设备

云 (Helion) 设备是通过云 (Helion) 凭据配置的设备，支持 HPE 公共云。介质代理已得到增强，可在数据传输至云 (Helion) 设备时充当云网关。其行为类似于备份到磁盘 (B2D) 设备。

## 先决条件

### HPE 公共云中的先决条件：

- 您必须具有 HPE 公共云帐户和凭据。有关详细信息，请参见 <https://horizon.hpcloud.com>。
- 必须订阅 HPE 公共云中的对象存储。
- 对于 HPE 公共云中的项目，必须记录项目名称。
- 地理区域的身份验证服务 URL 最接近数据中心。
- 如果您决定使用访问密钥(而不用户名和密码凭据)进行身份验证，请在 HPE 公共云中创建访问密钥。

### Data Protector 中的先决条件：

- 确保已在支持的系统上安装 Data Protector 的最新 Cell Manager、用户界面客户机和安装服务器，以及最新的 9.04 常规补丁版本包。  
有关详细信息，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新 Data Protector 支持矩阵。有关如何在各种架构中安装 Data Protector 的信息，请参见 *Data Protector 安装指南*。
- 在将成为云网关的 Windows 和 Linux 系统上安装 Data Protector 介质代理或 NDMP 介质代理组件，其中包括将启用云 Helion 设备的客户机。有关说明，请参见 *Data Protector 安装指南*。  
有关受支持操作系统版本的详细列表，请参见最新支持矩阵，地址为：<https://softwaresupport.softwaregrp.com/>。

## 限制

- 云 (Helion) 设备对象复制已经过测试，受以下各项的支持：
  - 源设备：文件库设备和 StoreOnce 设备。
  - VMware 备份规范
- 在对象存储中选择或创建容器时，需遵循以下限制：
  - 只能为每个设备分配一个容器。
  - 不同的设备无法使用相同的容器。
  - 将容器分配给设备之后，不能进行更改。
- 配置云 (Helion) 设备时，请确保其块大小等于或大于内部源设备。  
如果要在内部设备与云 (Helion) 设备之间来回执行对象复制，则这两个设备上的块大小必须匹配。可以在网关属性中设置块大小。

## 建议

建议对云 (Helion) 设备执行以下操作：

- 备份 VMware 规范时，请使用数据源的本地云网关，因为这将减少对象复制操作期间的网络负载。
- 尽可能将访问密钥用作身份验证模式。它可进一步限制对云 (Helion) 设备的整体访问，并提高所生成系统的安全性。
- 将大数据集复制到 HPE 云时，请分解至多个备份规范中。  
这样可以并行运行许多复制会话，从而提高整体带宽利用率并更高效地将数据复制到 HPE 云。
- 建议不要在云 (Helion) 设备上合并，因为这需要大量带宽以及关联的 HPE 云成本。

## 准备云 (Helion) 设备

要将对象复制操作配置到云 (Helion) 设备，必须执行以下任务。

1. 配置备份规范，将数据备份到本地备份设备。有关详细信息，请参见[创建备份规范](#)。
2. 在 HPE 公共云中，获取进行身份验证所需的用户帐户凭据或访问密钥、对象存储的订阅、身份验证服务 URL 以及其他 HPE 公共云先决条件。这些将用于配置云 (Helion) 设备。
3. 在 Data Protector 中，配置云 (Helion) 设备。有关详细信息，请参见[配置云设备](#)。
4. 分别使用本地备份设备和云 (Helion) 作为源设备和目标备份设备，配置对象复制会话。

创建“复制到云 (Helion) 设备”对象操作之后，本地备份设备中存储的数据可复制到 HPE 公共云。默认情况下，会对发送到云 (Helion) 设备的数据进行压缩和加密。

5. 要从云 (Helion) 设备还原数据，您可以：



- 创建从云 (Helion) 设备到本地备份设备的对象复制，并从本地备份设备还原到客户机。
- 回收并导出本地介质，然后直接从云 (Helion) 设备还原到客户机。
- 通过指定要用于还原的云 (Helion) 设备，直接从云 (Helion) 设备中还原，即使存在本地版本也如此。
- 将介质位置优先级设置为云 (Helion) 介质，而非本地介质。请参见 [设置介质位置优先级](#)。

## 关于云 (Azure) 设备

新的云设备用于实现备份和从 Data Protector 到 Microsoft Azure 对象存储的对象复制。云 (Azure) 设备使用 Azure 凭据进行配置，并将数据发送到云。

### 先决条件

#### 云 (Azure) 设备门户的先决条件：

- 您必须拥有 Microsoft Azure 帐户。有关详细信息，请参见 [Microsoft Azure 门户](#)。
- 您必须拥有 Microsoft Azure 在创建 Microsoft Azure 存储帐户时生成的两个存储访问密钥。为帐户生成了两个访问密钥。创建相关的 Data Protector 设备时，在提供凭据的过程中需要这些密钥。
- 必须准确设置系统时间，以确保网关主机和 Microsoft Azure 之间正确同步。

#### Data Protector 中的先决条件：

- 确保已在支持的系统上安装 Data Protector 的 Cell Manager、用户界面客户机和安装服务器，以及最新的常规补丁版本包。  
有关如何在各种架构中安装 Data Protector 的详细信息，请参见《Data Protector 安装指南》。
- 在将成为云 (Azure) 网关的 Windows 和 Linux 系统上安装 Data Protector 介质代理或 NDMP 介质代理组件，其中包括将启用云 (Azure) 设备的客户机。有关说明，请参见《Data Protector 安装指南》。

有关受支持操作系统版本的详细列表，请参见最新支持矩阵，地址为：<https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=>。

#### 注意：

- 如果介质代理系统需要配置代理服务器才可连接到 Web，则需要在 omnirc 文件中设置 omnirc 变量 OB2\_CLOUD\_DEVICE\_PROXY=<proxy\_server:port\_number>。
- 介质代理具有内置重试机制，可处理不同错误情况。因此，用户操作有时可能需要一段时间才能完成。在正常情况下，不会观察到此类问题。

## 限制

以下是云 (Azure) 设备的限制：

- 云 (Azure) 设备对象复制受以下各项的支持：
  - 源设备：文件库设备和 StoreOnce 设备。
  - 文件系统备份规范
- 在云 (Azure) 设备中选择或创建容器时，需遵循以下限制：
  - 只能为每个设备分配一个容器。
  - 多个设备无法使用相同的容器。
  - 将容器分配给设备之后，不能进行更改。

### 云 (Azure) 设备 blob 大小限制

Data Protector 介质作为数据和元数据的一个或多个 blob，上传到云 (Azure) 设备。云 (Azure) 的 blob 大小限制为 195 GB，而 Data Protector 介质的大小没有上限。然而，为遵守该限制，一个 Data Protector 介质可跨多个 blob，每个 blob 的大小上限为 75 GB。每个 blob 存储的确切数据量是数据可压缩程度的函数。

## 建议

以下是配置云 (Azure) 设备的建议：

- 备份文件系统规范时，请使用数据源的本地云 (Azure) 设备网关，因为这将减少对象复制操作期间的网络负载。
- 由于在默认情况下，到云 (Azure) 的对象复制作业经过加密，因此在为复制操作生成数据的初始备份规范中，应关闭加密。如果加密开启，数据会加密两次，消耗额外的 CPU 资源，对象复制数据变得不可压缩。因此，传输到云 (Azure) 的数据量增加，延长了复制时间。
- 将数据复制到云 (Azure) 设备时，请将大数据集分解成多个备份规范，以便能够并行启用多个复制会话。从而增加整体带宽。
- 建议不要在云 (Azure) 设备上合并，因为这需要大量带宽以及关联成本。

## 准备云 (Azure) 设备

要将对象复制操作配置到云 (Azure) 设备，必须执行以下任务。

1. 配置备份规范，将数据备份到本地备份设备。有关详细信息，请参见[创建备份规范 \(第 247 页\)](#)。
2. 登录 [Microsoft Azure](#) 门户，并获取使用 Microsoft Azure 存储帐户所需的访问密钥。
3. 在 Data Protector 中配置云 (Azure) 设备。有关详细信息，请参见[配置备份到磁盘设备 - 云 \(Azure\) \(第 158 页\)](#)。

4. 分别使用本地备份设备和云 (Azure) 设备作为源设备和目标备份设备，配置对象复制会话。

创建“复制到云 (Azure) 设备”对象操作之后，本地备份设备中存储的数据可复制到云 (Azure) 设备。默认情况下，会对发送到云 (Azure) 的数据进行压缩和加密。

5. 从云 (Azure) 设备还原数据。要还原数据，您可以：
  - 创建从云 (Azure) 设备到本地备份设备的对象复制，并从本地备份设备还原到客户机。
  - 回收并导出本地介质，然后直接从云 (Azure) 设备还原到客户机。
  - 通过指定要用于还原的云 (Azure) 设备，直接从云 (Azure) 中还原，即使存在本地版本也如此。
  - 将介质位置优先级设置为云 (Azure) 介质，而非本地介质。请参见[设置介质位置优先级 \(第 233 页\)](#)。

## 设备性能优化

### 块大小

每个逻辑设备都可配置为以特定大小(块大小)的单位处理数据。不同设备有不同的默认块大小，这些大小可以使用(成功完成所有会话)，但可能不是最佳选择。通过调整块大小，可以增强 **Data Protector** 会话的性能。

最佳的块大小值取决于所处环境：

- 硬件(设备、网桥、交换机等等)
- 固件
- 软件(操作系统、驱动程序、防火墙等等)

要获得最佳结果，请首先通过安装最新的驱动程序和固件优化环境、优化网络等等。

### 确定最佳的块大小

要确定最佳的块大小，请通过用不同的块大小值运行常规的 **Data Protector** 任务(备份、还原、复制等等)执行不同的测试，并度量性能。

**注意：**

更改设备块大小后，就无法再用此设备(用旧的块大小)还原旧的备份。

因此，请将旧的逻辑设备和介质池保留原样，以便能够从旧介质还原数据，并创建各种块大小值的新逻辑设备和介质池用于测试目的。或者，了解如何在执行还原时更改块大小。还原对话框将提示您块大小。

## 限制

- 灾难恢复：要能够执行脱机 EADR/OBDR 恢复(增强型自动灾难恢复，一键式灾难恢复)，请使用默认的块大小备份数据。
- 库：如果在同一库中使用类似技术的若干驱动器类型，则这些驱动器的块大小必须相同。
- SCSI 适配器：检查设备所连接的主机 SCSI 适配器是否支持所选的块大小。
- 对象复制功能：目标设备的块大小必须等于或大于源设备。
- 对象合并功能：目标设备的块大小必须等于或大于源设备。
- 镜像：设备的块大小在镜像链中不得递减。用于写入镜像 1 的设备的块大小必须等于或大于用于备份的设备；用于写入镜像 2 的设备的块大小必须等于或大于用于写入镜像 1 的设备，以此类推。

有关其他限制，请参见《*Data Protector 产品声明、软件说明和参考*》。

## 更改块大小

可以在特定设备的“高级选项”对话框的“大小”选项卡中设置块大小。有关详细信息，请参见 [设置设备和介质的高级选项](#)。

## 设备性能

由于设备向磁带写入数据(或从中读取数据)时可保持的速度不同，设备类型和型号会影响性能。

数据传输率还取决于是否使用硬件压缩。可以达到的压缩率取决于要备份的数据的性质。在大多数情况下，使用带硬件压缩的高速设备能提高性能。但是，仅在设备流畅无阻时才使用此类高速设备。

在备份会话的开始和结束时，备份设备需要些时间以执行回绕介质和装载或卸载介质等操作。

库提供了自动化的优势：必须在备份时加载新的或可重用的介质，并且必须在还原时快速访问介质，但由于库访问是自动化的，因此该过程更快。

基于磁盘的设备使用起来比传统设备快。使用基于磁盘的设备时不需要装载和卸载介质，并且访问基于磁盘的设备中的数据时速度更快，因此减少了备份和还原所需的时间长度。

## 支持新设备

要使用未在 *Data Protector 产品声明、软件说明和参考* 中列为受支持的设备，请使用 `scsitab` 文件。

scsitab 文件是一种机器可读的 Data Protector 支持矩阵，并包括有关所有受支持设备的信息。Data Protector 介质代理使用 scsitab 文件确定是否支持给定设备或库。该文件还提供有关设备及其特定参数的信息。

**重要：**

不支持修改 scsitab 文件。

要使用未在 *Data Protector* 产品声明、软件说明和参考中列为受支持的设备，请从 Data Protector 网站(位于 <https://software.microfocus.com/zh-cn/products/data-protector-backup-recovery-software/overview>)下载 scsitab 文件的最新软件包。

下载 scsitab 软件包之后，请按照软件包附带的安装过程进行操作。

scsitab 文件位于设备所连接的系统中的以下位置：

**Windows 系统：** *Data\_Protector\_home\scsitab*

**HP-UX、Solaris 和 Linux 系统：** */opt/omni/scsitab*

**其他 UNIX 系统：** */usr/omni/scsitab*

如果在配置设备时仍收到相同的错误，请与客户支持人员联系，获取何时将支持该设备的信息。

## 准备备份设备

准备备份设备包括将设备连接到系统或在 SAN 环境中连接到 SAN 和了解要使用哪些(正常工作的)关联的设备文件(SCSI 地址)。

## 先决条件

介质代理(常规介质代理或 NDMP 介质代理)必须安装在每个连接了备份设备的系统中或在 SAN 环境中安装在控制 SAN 上备份设备的系统中。

## 步骤

1. 将备份设备连接到计算机系统或在 SAN 环境中连接到 SAN。
2. 继续准备：

**Windows 系统：**

为连接到 Windows 系统的设备指定 [SCSI 地址语法](#)。

**UNIX 系统：**

为连接到 UNIX 系统的设备[查找或创建设备文件名](#)。

3. 如果有若干设备要使用同一个介质，则必须确保写入密度和块大小设置完全相同。
4. 引导系统以使系统识别出该设备。
5. 对于某些备份设备，必须执行额外的步骤。

准备备份设备之后，配置该设备与 Data Protector 配合使用。准备要与备份配合使用的介质。

- 在 SAN 环境中
- 文件设备
- 箱盒
- SCSI 库、介质库、外部控制
- Windows 机械手驱动程序

## 在 SAN 环境中

### 步骤

1. 核实需要访问共享库的所有系统中存在的机械手设备文件名都相同。如果要使用间接库访问功能，则忽略此步骤。

#### HP-UX 和 Solaris 系统：

如有必要，通过硬链接或软链接达到设备文件标识的要求。

#### Windows 系统：

使用 libtab 文本文件覆盖默认的 SCSI 设备标识，然后将机械手控制设备重新分配给另一个主机上定义的逻辑驱动器。

应在介质代理客户机上的 *Data\_Protector\_home* 目录中创建 libtab 文件，使其成为采用以下语法的文本文件(允许在逻辑驱动器名称中使用空格)：

```
hostnamecontrol_device_filedevice_name
```

例如

```
computer.company.com scsi2:0:4:0 DLT_1
```

## 文件设备

对要用作设备的文件禁用 Windows 压缩选项。可以使用 Windows 资源管理器执行此操作：

### 步骤

1. 右键单击文件，单击**属性**，然后清除**属性**下的**压缩**选项。

## 箱盒

### 步骤

1. 创建一个支持箱盒的介质池，然后再配置箱盒设备。该设备必须支持箱盒(例如 12000e)。

## SCSI 库、介质库、外部控制

### 步骤

1. 决定库中的哪些插槽要用于 Data Protector。配置库时，将需要指定这些插槽。

## Windows 机械手驱动程序

在 Windows 系统中，将为启用的磁带库自动加载机械手驱动程序。要在 Windows 系统中将库机械手与 Data Protector 配合使用，请禁用相应的 Windows 驱动程序。

### 步骤

1. 在控制面板中，双击**管理工具**。
2. 双击**计算机管理**，然后单击**设备管理器**。
3. 展开**介质更换器**。
4. 右键单击介质更换器并选择**禁用**。
5. 重新启动系统以应用更改。机械手现在准备好，可以用 Data Protector 进行配置。

## 在 Windows 系统中创建 SCSI 地址

SCSI 地址语法取决于连接到 Windows 系统的物理设备(磁光或磁带)的类型。设备必须已连接到系统(并已通电)，然后再启动系统。

**提示：**  
可以使用 Data Protector 自动检测 SCSI 地址。

### 磁光设备

如果系统连接了磁光设备，则 SCSI 地址语法为 N:B:T:P:L(N 为可移动驱动器的装载点、B 为总线编号、T 为 SCSI 目标 ID、P 为路径、L 为 LUN)。

在**控制面板**中打开 **SCSI 适配器**，然后双击目标设备的名称。再单击**设置**以打开设备属性页。此时将显示所有必要的信息。

### 磁带设备

如果系统连接了磁带设备，则 SCSI 地址语法取决于是否加载了本机磁带驱动程序。地址语法还取决于系统。有关创建目标 SCSI 地址的说明，请参见以下各部分：

[无本机磁带驱动程序的 Windows](#)

[使用本机磁带驱动程序的 Windows](#)

## 无本机磁带驱动程序的 Windows

如果未加载本机磁带驱动程序，则 SCSI 地址语法为 P:B:T:L(P 为 SCSI 端口、B 为总线编号、T 为 SCSI 目标 ID、L 为 LUN)。查找所连接磁带驱动器的属性可收集这些信息。

在**控制面板**中打开 **SCSI 适配器**，然后双击目标设备的名称。再单击**设置**以打开设备属性页。此时将显示所有必要的信息。

## 使用本机磁带驱动程序的 Windows

如果加载了本机磁带驱动程序，则 SCSI 地址语法为 `tapeN`(N 为驱动器实例编号)。只能使用驱动器的实例编号创建磁带驱动器文件，例如，如果 N 等于 0，则为 `tape0`。

### 步骤

1. 在 Windows“控制面板”中，双击**管理工具**。
2. 在“管理工具”窗口中，双击**计算机管理**。展开**可移动存储**，然后展开**物理位置**。
3. 右键单击磁带驱动器并选择**属性**。

如果加载了本机磁带驱动程序，则设备文件名会显示在“常规”属性页中。否则，可在“设备信息”属性页中找到相关信息。

## 在 UNIX 系统中查找设备文件名

需要了解设备文件名以便配置连接到 UNIX 系统的设备。

设备文件的创建过程取决于特定的 UNIX 操作系统供应商。对于 HP-UX 和 Solaris 平台上的设备，请参见以下各节。对于其他 UNIX 平台上的设备，请查询各自供应商的信息。

## 查找 HP-UX 中的设备文件名

### 先决条件

使用 `/usr/sbin/ioscan -f` 命令检查是否正确连接了设备。

### 步骤

1. 在 HP-UX 系统中启动 **System Administration Manager (SAM)** 应用程序。
2. 单击**外围设备**，然后单击**磁带驱动器**。
3. 单击目标设备。
4. 在“操作”菜单中，单击**显示设备文件**。此时将显示设备文件名。使用其中语法为 `*BEST` 的文件名。对于非重绕设备，使用其中语法为 `'BESTn'` 的文件名。

如果不显示任何设备文件名，则需要创建这些文件名。



## 查找 Solaris 中的设备文件名

### 步骤

1. 按 **Stop** 和 **A** 停止客户机系统。
2. 在 ok 提示符下，使用 `probe-scsi-all` 命令检查是否正确连接了设备。  
这样可提供有关所连接 SCSI 设备的信息，这些信息应包括所连接备份设备的设备 ID 字符串。
3. 在 ok 提示符下，输入 `go` 返回正常运行。
4. 列出 `/drv/rmt` 的内容，如果使用多驱动器库，则还要列出 `/drv` 目录：
  - `/drv/rmt` 目录应包含备份设备的驱动器的设备文件名。
  - 如果使用多驱动器库设备，则 `/drv` 目录应包含机械手的设备文件名。

如果不显示任何设备文件名，则需要创建这些文件名。

有关设备文件的更多信息，请参见《*Data Protector 安装指南*》。

## 在 UNIX 系统中创建设备文件

如果在系统初始化(引导过程)期间没有创建对应于特定备份设备的设备文件，则必须手动创建这些设备文件。管理库控制设备(库机械手)所需的设备文件就是这种情况。

设备文件的创建过程取决于特定的 UNIX 操作系统供应商。对于 HP-UX 和 Solaris 平台上的设备，请参见以下各节。对于其他 UNIX 平台上的设备，请查询各自供应商的信息。

## 在 HP-UX 系统中创建设备文件

### 先决条件

- 使用 `/usr/sbin/ioscan -f` 命令检查是否正确连接了设备。

### 步骤

1. 在 HP-UX 系统中启动 **System Administration Manager (SAM)** 应用程序。
2. 单击**外围设备**，然后单击**磁带驱动器**。
3. 单击目标设备。
4. 在“操作”菜单中，单击**创建设备文件**，然后单击**创建默认设备文件**。

## 在 Solaris 系统中创建设备文件

### 先决条件

- 首先必须更新客户机的设备和驱动程序配置文件，如果使用库设备则安装另一个驱动程序，并在客户机上创建新的设备文件，然后才能在 Solaris 客户机上使用新的备份设备。

### 步骤

1. 按 **Stop** 和 **A** 停止客户机系统。
2. 在 ok 提示符下，运行 `probe-scsi-all` 命令，以检查客户机系统上的可用 SCSI 地址，然后为要连接的设备选择一个地址(适用于单驱动器设备)。在多驱动器设备的情况下，将需要为每个驱动器选择一个 SCSI 地址，还要为机械手机构选择一个。
3. 在 ok 提示符下，输入 `go` 返回正常运行。
4. 关闭客户机系统，并将其断电。
5. 在备份设备上设置所选的 SCSI 地址。
6. 如有必要，在将 SCSI 设备连接到相关客户机系统时，关闭系统，并将其断电。
7. 将备份设备连接到客户机系统
8. 首先给备份设备通电，然后再给客户机系统通电(如果之前断电)。
9. 按 **Stop** 和 **A** 再次停止系统。
10. 在 ok 提示符下，运行 `probe-scsi-all` 命令。  
这样可提供有关所连接 SCSI 设备的信息，包括新连接的备份设备的正确设备 ID 字符串。
11. 在 ok 提示符下，输入 `go` 返回正常运行。
12. 编辑配置文件 `st.conf`，并为驱动器添加所需的设备信息和 SCSI 地址。  
有关如何执行此操作的更多信息，请参见《*Data Protector 安装指南*》。
13. 如果要将多驱动器设备与库机械手机构相连，则还要执行以下步骤。有关详细信息，请参见《*Data Protector 安装指南*》。
  - a. 将 `sst` 驱动程序复制到客户机上，然后安装它。
  - b. 将配置文件 `sst.conf`(Solaris 8 或 9)或 `sgen.conf` (Solaris 10) 复制到相关客户机系统上并编辑该文件，为机械手装置添加一个条目。
  - c. 编辑 `/etc/devlink.tab` 文件，并添加机械手机构设备文件的条目。
14. 根据需要更新驱动程序和配置文件后，为客户机系统创建新的设备文件：
  - a. 从 `/drv/mnt/` 目录中删除所有现有的设备文件。
  - b. 运行命令 `shutdown -i0 -g0` 关闭系统。
  - c. 运行命令 `boot -rv` 重新启动系统。
  - d. 重新引导完毕后，列出 `/dev` 目录的内容以检查所创建的设备文件。机械手机构的设备文件应位于 `/dev` 目录中，而驱动器的设备文件应位于 `/dev/rmt` 目录中。

## 自动检测设备文件名和 **SCSI** 地址

可以自动检测连接到 Windows、HP-UX 或 Solaris 平台的大多数设备的设备文件名(SCSI 地址)。

### 对于现有的 **Data Protector** 设备定义

#### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中，右键单击设备，然后单击 **属性**。
4. 单击 **驱动器** 选项卡。
5. 使用下拉列表可自动检测设备的 **SCSI** 地址(设备文件名)。

### 创建 **Data Protector** 设备定义时

#### 步骤

1. 按照配置设备的过程操作。
2. 在向导中，当提示指定设备文件名(SCSI 地址)时，使用下拉列表选择可用设备。

## 自动检测库的设备文件名和 **SCSI** 地址

可以自动检测连接到 Windows、HP-UX 或 Solaris 平台的库机械手的设备文件名(SCSI 地址)。

### 对于已配置的库

#### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中，右键单击库，然后单击 **属性**。
4. 单击 **控制** 选项卡。
5. 在库的机械手 **SCSI** 地址区域中，使用下拉列表选择库机械手的可用文件名(SCSI 地址)。

## 配置库时

### 步骤

1. 按照用于配置库机械手的过程操作。
2. 在向导中，当提示指定 **SCSI 地址**(文件名)时，使用下拉列表选择库机械手的可用文件名(**SCSI 地址**)。

## 关于配置备份设备

完成准备部分之后，可以配置备份设备，使其与 **Data Protector** 配合使用。

建议让 **Data Protector** 自动配置备份设备。**Data Protector** 可以自动配置最常用的备份设备(包括库)。虽然仍需要为备份会话准备介质，但 **Data Protector** 可确定设备的名称、策略、介质类型、介质策略和设备文件或 **SCSI 地址**，并且还可配置驱动器和插槽。

也可以手动配置备份设备。配置备份设备的方式取决于设备类型。

可以使用未在 **Data Protector** 产品声明、软件说明和参考中列为受支持的设备。将使用 **scsitab** 文件配置不支持的设备。

## 关于库管理控制台

### 什么是库管理控制台？

当前许多磁带库都集成了管理控制台，使您可以在远程执行库的配置、管理和监视任务。库管理控制台是库的 **Web** 界面，该界面就像普通网页一样显示在 **Web** 浏览器中。磁带库配备此类 **Web** 控制台后，即可从任何远程系统执行各种任务。例如，可以设置库配置参数、将磁带加载到库驱动器中以及检查库的当前状态。可远程执行的任务范围取决于管理控制台的实施，它独立于 **Data Protector**。

每个库管理控制台都有自己的 **URL**(**Web 地址**)，这是管理控制台界面的入口点。在 **Web** 浏览器的地址栏中键入此 **URL** 即可访问控制台界面。

## Data Protector 中对库管理控制台的支持

库配置包含表示库管理控制台 **URL** 的参数。可以在库配置或重新配置过程中指定 **管理控制台 URL**。

通过扩展 **Data Protector** GUI 功能，简化了对管理控制台界面的访问。可调用 **Web** 浏览器，然后从 **Data Protector** GUI 中加载控制台界面。根据操作系统，将使用系统默认 **Web** 浏览器(在 **Windows** 系统中)或 **Data Protector** 配置中指定的 **Web** 浏览器(在 **UNIX** 系统中)。

#### 重要：

使用库管理控制台之前，请考虑某些可通过控制台执行的操作可能会妨碍介质管理操作和/或备份和还原会话

## 限制

不支持输入空格和双引号作为管理控制台 URL 的一部分；而应输入安全的 URL 代码。下表中显示了不受支持的字符及其安全 URL 代码等效字符。

字符	安全 URL 代码
空格	%20
双引号 (")	%22

## 自动配置备份设备

将备份设备连接到要配置的系统并且存在正常工作的设备文件(SCSI 地址)之后，可以配置该备份设备与 Data Protector 配合使用。自动配置表示 Data Protector 将为您创建设备定义。

Data Protector 可以检测和自动配置连接到 SAN 中一个或几个系统的最常用备份设备。以后可以修改自动配置的设备的属性，以使其适合您的特定需要。

以下操作系统中可以进行自动配置：

- Windows
- HP-UX
- Solaris
- Linux

### 注意：

如果在可移动存储服务运行时自动配置库，则将无法正确组合驱动器和机械手(更换器)。

## 先决条件

要自动配置的每个客户机系统必须装有介质代理。

## 设备自动配置

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**自动配置设备**以打开向导。
3. 选择含有要配置的设备的客户机系统，然后单击**下一步**。
4. 选择系统上要配置的备份设备。单击**下一步**。
5. 要启用对已更改 SCSI 地址的自动发现，请选择**自动发现已更改的 SCSI 地址**，然后单击**完成**。对于箱盒设备，在自动配置后将介质池更改为支持箱盒的一个池。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。

## SAN 环境中的设备自动配置

Data Protector 提供 SAN 环境中的设备自动配置，此环境中不同客户机使用一个库中的磁带驱动器。Data Protector 自动配置功能可在多个客户机系统上自动配置设备和库。

Data Protector 确定设备的名称、锁名称、策略、介质类型、介质策略和设备文件或 SCSI 地址，并配置驱动器和插槽。

### 注意：

将新主机引入 SAN 环境中时，将不自动更新所配置的库和设备。

- 如果要在新主机上使用现有的库，请删除此库，并在新主机上配置一个同名的新库。
- 如果要将设备添加到现有库，或者可以删除该库，然后在新主机上自动配置一个同名的新库以及新驱动器，或者可以手动将驱动器添加到库中。

## 限制

自动配置无法用于配置 SAN 环境中的以下设备：

- 混合介质库
- DAS 或 ACSLS 库
- NDMP 设备

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **设备**，然后单击 **自动配置设备** 以打开向导。
3. 选择要配置的客户机系统。在 Microsoft 群集服务器环境中，选择虚拟服务器。  
单击 **下一步**。
4. 选择系统上要配置的设备或库。
5. 配置库时，选择控制主机，即库对多个客户机可见时将控制库机械手的客户机。如果可看到库的系统之间有 **Cell Manager**，则默认情况下选择它。可以在以下两个视图之间切换：
  - **按设备分组**  
显示所有设备和库的列表。展开库或设备，然后选择要从中配置库或设备的客户机系统。
  - **按主机分组**  
显示连接了设备的客户机的列表。展开要从中配置设备或库的客户机。
6. (可选)要启用多路径设备，请选择 **自动配置多路径设备**。单击 **下一步**。
7. 要启用对已更改 SCSI 地址的自动发现，请选择 **自动发现已更改的 SCSI 地址**。
8. 单击 **完成 (Finish)**。此时将显示所配置设备的列表。

可以扫描设备以验证配置。

## 配置独立设备

将备份设备连接到系统并且存在正常工作的设备文件(SCSI 地址)之后，可以配置该备份设备与 Data Protector 配合使用。

建议让 Data Protector 自动配置备份设备。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明(可选)。
5. (可选)选择**多路径设备**。
6. 如果未选择**多路径设备**选项，则从“客户机”下拉列表中选择客户机(备份系统)的名称。
7. 在“设备类型”列表中，选择**独立设备**设备类型，然后单击**下一步**。
8. 输入物理设备的 **SCSI 地址**(Windows 系统)或设备文件名(UNIX 系统)，然后单击**添加**。

对于多路径设备，从下拉列表中选择客户机，然后输入该设备的设备文件名。单击**添加**，将路径添加到所配置路径的列表中。

#### 提示：

可以输入多个地址以创建设备链。

向设备链添加设备的顺序决定了 Data Protector 使用这些设备的顺序。

当设备链中的所有介质都装满后，Data Protector 将发出装载请求。将第一个设备中的介质替换为新介质，格式化新介质，然后确认装载请求。Data Protector 可以立即使用已识别且不受保护的介质。还可以使用空白介质。

9. 如果要启用对已更改 SCSI 地址的自动发现，则选择**自动发现已更改的 SCSI 地址**。单击**下一步**。
10. 在“介质类型”列表中，对要配置的设备选择介质类型。
11. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。
12. 单击**完成**退出向导。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。如果正确配置了设备，则 Data Protector 将可以在插槽中加载、读取和卸载介质。

## 配置备份到磁盘设备

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 Data Protector 对设备进行使用配置。可用的备份到磁盘设备：StoreOnce 备份系统、StoreOnce 软件、云 (Helion)、云 (Azure)、数据域提升和智能缓存。

## 多接口支持

Data Protector 提供多接口支持。Data Protector 支持与同一 Catalyst/DDBoost 存储建立 IP 以及光纤通道连接，而无需配置单独的存储。可同时通过这两种接口访问存储。

例如，有时本地客户机可通过光纤通道访问单个 Catalyst/DDBoost 存储以执行较快的备份，而远程客户机可通过 WAN 访问同一存储以执行较慢的备份。

在 Solaris 环境中或 FC 配置为重复数据删除目标的标识符时，此功能不可用。此选项仅适用于 StoreOnce 备份系统和 DD Boost。

有关此功能的工作方式的更多详细信息，请参见《Data Protector 管理员指南》和 Data Protector 命令行界面参考。

### 重要：

添加 StoreOnce 或 DDBoost 设备时，强烈建议使用 IP 地址或主机名，以利用多接口功能。

## 步骤

要添加 B2D 设备(定位到现有存储)，请按以下步骤操作：

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **设备**，然后单击 **添加设备** 以打开向导。
3. 指定设备名称及其说明(可选)。
4. 选择 **备份到磁盘** 设备类型，然后选择 **接口类型**：**StoreOnce 备份系统**、**数据域提升**、**StoreOnce 软件**、**云(Helion)**、**云(Azure)** 或 **智能缓存**。
5. 配置设备的步骤因所选的接口类型而异。
  - [配置 StoreOnce](#)
  - [配置 StoreOnce 软件](#)
  - [配置数据域提升](#)
  - [配置智能缓存](#)
  - [配置云 \(Helion\) 设备](#)
  - [配置云 \(Azure\) 设备](#)

添加 B2D 设备的步骤与添加设备类型的步骤类似。另外，对于 StoreOnce 软件重复数据删除设备，必须首先配置根目录，然后再创建存储(请参见 [配置备份到磁盘设备 - StoreOnce 软件](#))。

## 配置备份到磁盘设备 - StoreOnce

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 Data Protector 对设备进行使用配置。



如果要配置 StoreOnce 软件重复数据删除设备，则需要执行一些其他步骤。请参见[配置备份到磁盘设备 - StoreOnce 软件](#)。

**注意：**

Data Protector 最多支持八个成员的联合存储。可以在 StoreOnce 中更改存储中的成员数。要反映此更改，可以使用 Data Protector GUI 或 CLI 手动刷新 Data Protector 缓存。有关详细信息，请参见[刷新存储的缓存](#)。所有联合成员均必须联机，联合存储才能发挥作用。

## 步骤

要添加 StoreOnce 备份系统或 StoreOnce 软件 B2D 设备(定位到现有存储)，请按以下步骤操作：

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 指定设备名称及其说明(可选)。
4. 选择**备份到磁盘**设备类型，然后选择接口类型：**StoreOnce 备份系统**或**StoreOnce 软件**。
5. (可选)在**管理控制台 URL**文本框中输入设备管理控制台的有效 URL。单击**下一步**。
6. 对于 StoreOnce 备份系统设备，请输入**客户机 ID**和密码(可选)以访问存储。您可以在密码中使用以下字符：[a-z][A-Z][0-9][\_+(){}:#\$\*;=?@[^~]?
7. 在**重复数据删除系统**框中，输入重复数据删除系统的 IP 地址、主机名、完全限定域名 (FQDN)或光纤通道 (FC) 地址(重复数据删除存储所在的宿主计算机)。  
或单击**选择服务集**，查询并检索重复数据删除系统的地址。

**注意：**

对于 StoreOnce 软件接口，支持 IPv4 或 IPv6 地址，或 FQDN。但是，对于 StoreOnce 备份系统接口，如果使用最新的 StoreOnce Catalyst 版本，则支持 IPv4 或 IPv6 地址、FQDN 或 FC 全局标识符。

如果使用 FC 连接到 StoreOnce 备份系统，请指定设备的 FC 地址。确保使用的介质代理或网关已连接到 FC 设备，且与 StoreOnce 备份系统设备位于同一区域。

8. 单击**选择/创建存储**按钮，选择现有的联合或非联合存储，或者创建非联合存储。从列表中选择存储名称。  
要创建加密存储，请选择**已加密存储**选项。单击**确定**。

**注意：**只能在创建存储区时启用加密功能。存储一经创建，就无法将其从已加密状态转换成未加密状态，反之亦然。StoreOnce 软件重复数据删除设备不支持存储加密。

不能使用 Data Protector GUI 创建联合存储。需要使用 StoreOnce 管理控制台创建它们。

9. (可选)选择**源端重复数据删除**以启用源端重复数据删除。此时将打开“源端重复数据删除属性”窗口。查看属性并在需要时进行修改。默认情况下，源端网关将命名为 DeviceName\_Source\_side。注意，只能为每个设备创建一个源端网关。如果在备份规范中启用了源端重复数据删除，则在备份的系统上此(虚拟)网关将被自动扩展。

**注意：**

对于联合存储，所有写入操作均在低带宽模式中执行(服务器端重复数据删除)。即使网关配置为目标端重复数据删除(高带宽模式)，它也会自动切换到低带宽模式。

10. 选择一个网关，然后单击**添加**以显示“属性”对话框。根据需要更改任意网关属性，然后单击**确定**添加网关。如果使用 FC 连接到 StoreOnce 备份系统，请确保使用的介质代理或网关已连接到 FC 设备，且与 StoreOnce 备份系统设备位于同一区域。

**注意：**

连接到 Data Protector 网关的联合成员必须是联合存储的成员。如果使用 StoreOnce 缩小了联合成员，请使用[刷新存储的缓存](#)中提到的步骤，将 Data Protector 网关调整为连接到不同的联合成员。

要查看网关属性，请选择所需的网关然后单击**属性**。要设置其他网关选项，请单击**设置**选项卡，再单击**高级**打开“高级”属性窗口。

在“高级属性”窗口中，要限制每个网关上的流数，请选择**每个网关的并行流的最大数量**。可以指定最多 100 个流。如果未选择此选项，则不限制流数。注意，还可以在创建备份规范时设置此选项。在这种情况下，B2D 设备创建过程中指定的值将被覆盖。

要限制网关所使用的网络带宽，请选择**限制网关网络带宽(Kbps)**并输入以每秒千位(kbps)为单位的限制。

要启用服务器端重复数据删除，请选择**服务器端重复数据删除**。

如果已配置 IP 地址或 FQDN 作为重复数据删除目标，则使用 **FC** 和 **回退至 IP** 选项可用，并且它们默认处于选中状态。

11. 要验证连接，请单击**检查**。
12. 单击**下一步**进入“设置”窗口，在此窗口中可以指定以下选项：
  - 每个 每个存储的连接数
  - 备份大小软配额 (GB)
  - 存储大小软配额 (GB)
  - **Catalyst 项目大小阈值 (GB)**：为 StoreOnce Software Deduplication 和 StoreOnce 备份系统设备定义 Catalyst 项目的阈值大小。如果当前的催化剂项目超过此大小，您将无法再向其中附加更多对象。默认情况下，催化剂项目的大小是无限制的。
  - **每个 Catalyst 项目一个对象**：选中后，对于 StoreOnce Software Deduplication 和 StoreOnce 备份系统设备，为每个 Catalyst 项目启用一个对象。
13. 单击**下一步**以显示“摘要”窗口，其中包括已配置 B2D 存储的详细信息。此外，对于联合存储，它还包括所有联合成员及其状态(联机或脱机)的列表。
14. 检查设置并单击**完成**。新配置的 B2D 设备将显示在范围窗格中。

## 为存储刷新缓存

使用 StoreOnce 3.12，可以在联合存储中添加或删除联合成员。要反映此更改，可以使用 Data Protector GUI 或 CLI 手动刷新 Data Protector 缓存。

## 使用 Data Protector GUI 刷新缓存

1. 在上下文列表中，单击 **设备和介质**。
2. 在“范围窗格”中，展开 **设备**。
3. 右键单击所需的 StoreOnce 设备，然后单击 **属性**。
4. 单击 **存储和网关** 选项卡，然后单击 **选择/创建存储**。如有必要，更改目录路径，使其包括当前活动的联合成员的地址。
5. 选择与此 StoreOnce 设备关联的同一存储，然后单击 **确定**。
6. 单击 **应用**。

## 使用 Data Protector CLI 刷新缓存

1. 请执行以下命令：  

```
omnidownload -library <DPDeviceName> -file <DPDeviceOutputFile>
```
2. 编辑 DPDeviceOutputFile。  
如果设备未联合，请删除以下行：  

```
B2DTEAMEDSTORE 1
B2DTEAMEDMEMBERS
"<teamed.device.one>"
"<teamed.device.two>"
...
```

  
如果设备已联合，请在替换适当的成组设备 IP 地址后，将这些行添加到 DPDeviceOutputFile。如有必要，更改目录路径，使其包括当前活动的联合成员的地址。

**注意：**地址和格式应该与 StoreOnce 成组策略文件中的地址和格式完全匹配。  
例如，如果成组策略文件包括 IPv6 地址，则必须也在此文件中添加相同地址。

3. 使用以下命令保存修改后的文件：  

```
omniupload -modify_library <DPDeviceName> -file <DPDeviceOutputFile>
```

有关这些命令的详细信息，请参见 *Data Protector* 命令行界面参考。

## 配置备份到磁盘设备 - StoreOnce 软件

如果您正在配置 StoreOnce Software Deduplication 设备，需要额外的步骤。

- [配置重复数据删除存储的根目录](#)
- [创建存储](#)

### 配置重复数据删除存储的根目录

本节描述了如何配置存储的根目录。此操作必须在安装软件后、创建第一个重复数据删除存储前完成。

如果存储共享相同的根目录，一个 **StoreOnce Software Deduplication** 系统可以托管多个重复数据删除存储。每个存储的操作独立于其他存储，即，重复数据删除仅发生在一个存储内，每个存储有其自己的索引表。虽然所有存储在相同进程下运行，但可以单独启动/停止(这并不表示以物理方式启动/停止存储，请参见《重复数据删除白皮书 — 附录

**A: StoreOnceSoftware 实用程序**》，了解详细信息)。如果操作停止(脱机)，则不能在存储上完成。

不能以物理方式分隔共享相同根目录的存储。该设计确保在所有磁盘上统一加载，并提供更好的性能。

安装成功后，**StoreOnceSoftware 实用程序**以正在运行但等待配置存储根目录的模式启动。在配置根目录之前，无法添加 **B2D** 设备，无法创建存储。

可通过以下方式配置存储根目录：

- **GUI**：遵循添加设备的步骤，出现提示时，指定根目录(请参见下文，了解详细信息)。
- **CLI**：使用命令 **StoreOnceSoftware -configure\_store\_root**(请参见《重复数据删除白皮书 — 附录 **A: StoreOnceSoftware 实用程序**》，了解详细信息)。

**注意：**根目录必须已经存在(于服务器上)，您必须具备写入权限，然后才能配置。这是因为 (**GUI**) 配置过程要求您指定其位置。

使用 **GUI** 配置根目录的过程与创建存储类似，但包括一些额外步骤。配置好根目录后，不再需要这些额外步骤。要配置根目录(同时创建存储)，请按如下方式继续操作：

1. 按照添加设备的过程操作：
  - a. 在“设备和介质”上下文中，右键单击 **设备 > 添加设备**。
  - b. 指定设备名称，添加说明，选择设备类型 **备份到磁盘**，然后选择接口 **StoreOnce Software Deduplication**。
  - c. (可选)在**管理控制台 URL** 文本框中输入设备管理控制台的有效 URL。
  - d. 单击**下一步**以显示可指定存储和网关列表的屏幕。
  - e. 对于 **StoreOnce** 备份系统设备，请输入**客户机 ID**和**密码**(可选)以访问存储。
2. 在“重复数据删除系统”框中，输入重复数据删除存储所在的宿主计算机的主机名、IP 地址或完全限定域名 (FQDN)。
3. 选择一个网关，单击**添加**以显示属性对话框，然后单击**确定**以添加该网关。
4. 单击**检查**。“根目录未配置”消息随即显示。
5. 在对话框中，指定根目录路径(例如，**C:\Volumes\StoreOnceRoot**)，所有存储都将驻留在该路径下，然后单击**确定**。(注意：无法浏览到有效的根目录)。
6. 如果根目录存在，对话框关闭，设备配置继续。**StoreOnceSoftware 实用程序**在指定的根目录中创建子目录(存储)。如果根目录不存在，将显示错误消息。
7. 继续执行**添加设备**的过程。

配置根目录和创建存储时，注意以下几点：

- 不要使用安装操作系统 (OS) 的相同磁盘。
- 使用专用(独有)存储磁盘。
- 在每个卷上，**Data Protector**支持最多 **32** 个存储。

**注意：**在 **Windows** 系统上，要改进性能，请将以下选项应用于将放置存储根的 **NTFS** 卷：

使用以下命令，在卷上禁用短(类似于 **DOS**)文件名的创建：**fsutil behavior set**

#### Disable8dot3 Volume 1

使用以下命令，增加 NTFS 内部日志文件大小：Chkdsk Volume /L:131072

## 创建存储

创建存储之前，确保存储的根目录已配置，并且物理存储磁盘(LUN 设备)已格式化且已装载到 **StoreOnce Software Deduplication** 系统。LUN 设备可位于本地磁盘或磁盘阵列(SCSI 或光纤通道接口)或相同 LAN 的 NAS 设备(iSCSI 接口)。使用 iSCSI 接口时，可靠的网络连接必须提供不超过 2 毫秒的延迟和至少 1 GB/秒的吞吐量。

可通过以下方式创建存储：

- **GUI**：遵循添加设备的步骤，出现提示时，指定存储的名称(请参见下文，了解详细信息)。
- **CLI**：使用命令 **StoreOnceSoftware --create\_store**(请参见《重复数据删除白皮书 — 附录 A: StoreOnceSoftware 实用程序》，了解详细信息)。

创建存储的过程与添加设备类似，但包括一些额外步骤。要创建存储，请执行以下操作：

1. 按照添加设备的过程操作：
  - a. 在“设备和介质”上下文中，右键单击 **设备 > 添加设备**。
  - b. 指定设备名称，添加说明，选择设备类型 **备份到磁盘**，然后选择接口 **StoreOnce Software Deduplication**。
  - c. 单击 **下一步** 以显示可指定存储和网关列表的屏幕。
2. 选择重复数据删除系统，并为存储指定名称。存储名称的最大长度为 80 个字符(仅字母数字字符)。
  - a. 选择一个网关，单击 **添加** 以显示属性对话框，然后单击 **确定** 以添加该网关。
  - b. 单击 **检查** 验证连接。如果存储不存在，则会创建。(注意：单击 **下一步** 也将验证连接。)
  - c. 继续执行 **添加设备** 的过程。

如果您指定的存储名称不正确，将无法通过 **GUI** 更改。再次运行该过程，并以正确名称创建存储。使用 **CLI** 删除名称错误的存储(假设数据未写入)。

## 配置备份到磁盘设备 - 数据域提升

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 **Data Protector** 对设备进行使用配置。

### 先决条件

- 要支持在数据域设备之间进行复制，必须在数据域设备上启用虚拟合成。
  - 使用 **ssh** 连接到数据域设备，并运行以下命令：

```
ddboost option set virtual-synthetics enabled
```
- 要支持复制，必须在具有相同管理角色的源设备和目标设备上配置同一数据域提升用户。有关详细信息，请参见您的数据域文档。

## 限制

- 执行交互复制时，只能选择一个会话进行复制。
- 如果修改加密强度的默认值，则不支持 **Data Protector** 操作。

**注意：**提到数据域提升设备时，使用“存储单元”一词，而非“存储”。

## 步骤

要添加 **DDBoost B2D** 设备(以现有存储为目标)，执行以下操作：

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **设备**，然后单击 **添加设备** 以打开向导。
3. 指定设备名称及其说明(可选)。
4. 选择 **备份到磁盘** 设备类型，然后选择 **接口类型：数据域提升**。
5. (可选)在 **管理控制台 URL** 文本框中输入设备管理控制台的有效 URL。单击 **下一步**。
6. 输入 **用户名** 和 **密码**。您可以在密码中使用以下字符：[a-z][A-Z][0-9][\_+(){}:#\$\*=?@[]^~]?
7. 输入存储单元名称(假设存储单元已经存在)。
8. 在 **重复数据删除系统** 文本框中，输入重复数据删除系统的主机名、IP 地址或 FC 地址(重复数据删除存储单元所在的宿主计算机)。

**注意：**建议您使用 IP 地址或 FQDN 以利用多接口功能。要了解此功能的相关内容，请参见 [多接口支持](#)。

9. (可选)选择 **源端重复数据删除** 以启用源端重复数据删除。此时将打开“源端重复数据删除属性”窗口。查看属性并在需要时进行修改。默认情况下，源端网关将命名为 **DeviceName\_Source\_side**。注意，只能为每个设备创建一个源端网关。如果在备份规范中启用了源端重复数据删除，则在备份的系统上此(虚拟)网关将被自动扩展。
10. 选择一个网关，然后单击 **添加** 以显示“属性”对话框。根据需要更改任意网关属性，然后单击 **确定** 添加网关。

要查看网关属性，请选择所需的网关然后单击 **属性**。要设置其他网关选项，请单击 **设置** 选项卡，再单击 **高级** 打开“高级”属性窗口。

要限制每个网关上的流数，请选择 **每个网关的并行流的最大数量**。可以指定最多 100 个流。如果未选择此选项，则不限制流数。注意，还可以在创建备份规范时设置此选项。在这种情况下，**B2D** 设备创建过程中指定的值将被覆盖。

要限制网关所使用的网络带宽，请选择 **限制网关网络带宽(Kbps)** 并输入以每秒千位(kbps)为单位的限制。

如果已配置 IP 地址或 FQDN 作为重复数据删除目标，则使用 **FC** 和 **回退至 IP** 选项可用，并且它们默认处于选中状态。

要启用服务器端重复数据删除，请选择 **服务器端重复数据删除**。

11. 要验证连接，请单击 **检查**。
12. 单击 **下一步** 进入“设置”窗口，在此窗口中可以指定以下选项：



- **每个存储单元的连接数的最大数量：**定义限制物理连接的最大读写流的中值。
- **备份大小软配额 (GB)：**输入备份大小软配额(以 GB 为单位)
- **存储大小软配额 (GB)：**如果已创建存储单元，或者如果已手动为整个数据域操作系统 (DD OS) 启用配额并在创建存储单元时指定配额，则支持该设置。
- **存储介质项大小阈值 (GB)：**定义数据域提升设备的存储项的阈值大小。如果当前的存储项超过此大小，您将无法再向其中附加更多对象。默认情况下，存储项的大小是无限制的。
- **每个存储介质项的一个对象：**选中后，对于数据域提升设备，每个存储项启用一个对象。

13. 单击**下一步**以显示“摘要”窗口，其中包括已配置 B2D 存储单元的详细信息。

14. 检查设置并单击**完成**。新配置的 B2D 设备将显示在范围窗格中。

## 在 AIX 系统上配置数据域提升

要在 AIX 系统上配置通过光纤通道 (FC) 协议的数据域提升，您必须安装 AIX DDdfc 设备驱动程序。驱动程序文件名为 DDdfc.1.0.0.x.bff，其中 x 是版本号。

### 步骤

1. 作为 root 用户，登录 AIX 客户机。
2. 输入 # smitty install 命令。
3. 选择**安装和更新软件**。
4. 选择**安装软件**。
5. 输入路径 /usr/omni/drv 以安装 DDdfc.1.0.0.x.bff 文件，其中 x 是版本号。
6. 按 **F4**，选择想要安装的 DDdfc.1.0.0.x 版本。
7. 按 **Tab**，将“仅预览？”行的值 切换至“否”。
8. 按 **Enter**，接受信息并安装驱动程序。

## 配置备份到磁盘设备 - 智能缓存

在使用备份到磁盘 (B2D) 设备执行备份之前，需要使用 Data Protector 对设备进行使用配置。

### 配置智能缓存

#### 先决条件

- 必须具有要在其中创建智能缓存设备的介质代理主机的用户凭据。在非分步恢复期间，VMware 插件使用这些凭据访问网络共享。

**注意：**在单个介质代理主机中，只能使用一个操作系统用户凭据创建智能缓存设备。如果多个用户同时同一介质代理主机上创建智能缓存设备，则 VMware

**Granular Recovery** 请求可能会遇到“访问被拒绝”错误。

- 对于 Linux 操作系统，必须在智能缓存客户机上安装和运行 Samba 服务器，这是因为 Data Protector 在恢复期间使用 Samba 服务器创建共享。要验证 Samba 服务器是否正在运行，请执行以下命令：`ps -ef | grep smbd`。Samba 服务器的默认安全模式为用户级。如果更改了默认模式，则必须使用以下命令将其更新为用户级：`[global] security = user`。
- 确保 Samba 共享具有读写权限。如果已在 Linux 系统中部署增强安全机制的 Linux (SELinux) 内核安全模块，请执行 `# setsebool -P samba_export_all_rw on` 命令来启用对 Samba 共享的读写权限。
- 在 Samba 服务器中，必须使用以下命令将介质代理主机的用户添加到 Samba 密码数据库：`smbpasswd -a <user>`。可以使用以下命令验证用户是否已添加到密码数据库：`pdbedit -w -L`。
- 必须定期清理 Samba 配置文件 (`smb.conf`)。这可确保以前的 Samba 共享配置信息被删除。
- 如果智能缓存存储是 Windows ReFS 文件系统、CIFS 或 NFS 共享，则必须在同一主机上部署 VMware 非分步恢复代理和介质代理模块。
- 如果智能缓存存储是本地固定磁盘或 SAN 存储 LUN，则 VMware 非分步恢复代理主机和介质代理模块可能不同。
- 必须将整个文件系统专用于一个智能缓存设备。此文件系统不应由其他应用程序使用，也不应由其他智能缓存/备份到磁盘设备共享。
- 仅可将单个介质池与一个智能缓存设备相关联。

## 限制

- 智能缓存仅在 Windows x64 和 Linux x64 平台上可用。
- 对于位于网络共享上的 Windows 智能缓存设备，仅 Windows Server 2008 和更高版本的系统支持非分步 GRE。
- 智能缓存仅可用作 VMware 备份的目标。
- 在 Linux 操作系统上，如果已安装 NDMP 介质代理，则不支持备份到智能缓存。
- 不支持已编码或 AES 256 位已加密的 VMware 备份到智能缓存设备。
- 不支持源到智能缓存设备的已编码或 AES 256 位已加密的对象复制。但是，支持在具有硬件加密的磁带设备中进行对象复制。
- 每个智能缓存设备仅支持一个装载点。
- 如果空间不足，则备份到智能缓存设备可能失败。确保智能缓存设备中具有多余的磁盘空间。
- 智能缓存设备不支持导出和导入介质。
- 如果在 Resilient File System (ReFS) 卷或网络共享 (CIFS/NFS) 上创建智能缓存设备，请在同一主机上安装装载代理组件(用于恢复)，否则非分步恢复将失败。
- 在 StoreOnce 4500 上，智能缓存设备配置不支持 CIFS。



## 步骤

1. 在磁盘上的所需位置中为智能缓存设备创建目录，例如，c:\SmartCache。  
可以在本地或网络驱动器(或 Linux 系统中由 NFS 装载的文件系统)上创建智能缓存设备。要指定网络驱动器，请使用以下格式：\\hostname\share\_name。  
“浏览驱动器”对话框中没有显示主机名以及共享名称和网络驱动器。必须输入 UNC 名称的路径。
2. 在 **Windows** 操作系统中，要获取访问包含智能缓存设备的共享磁盘的权限，请在介质代理上更改 **Data Protector Inet** 帐户。可以通过提供本地客户机系统和远程共享磁盘的访问权限来执行此操作。此外，确保它是特定用户帐户，而非系统帐户。设置 **Inet** 帐户后，配置和使用共享磁盘上的智能缓存设备。
3. 在 **Data Protector** 的上下文列表中，单击**设备和介质**。
4. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
5. 指定设备名称及其说明(可选)。
6. 选择**备份到磁盘**设备类型，然后选择**智能缓存**接口类型。
7. 在“客户机”下拉列表中，选择设备所在的系统。单击**下一步**。
8. 输入用户的用户名和密码，此用户需要访问在非分步恢复期间创建的共享。
9. 指定智能缓存设备的目录。单击**添加**。
10. 要更改目录的默认属性，请选择该目录，然后单击**属性**。
11. 单击**下一步**以显示“摘要”窗口。检查设置并单击**完成**。新配置的 B2D 设备将显示在范围窗格中。

## 配置云 (Helion) 设备

配置云 **Helion** 设备，以准备将对象复制到云对象存储中。

在准备过程中，必须完成以下步骤：

- 获取 **HPE 公共云项目名称**
- 获取身份验证服务 **URL**
- 创建访问密钥

接下来，可以将“云 (Helion)”设备配置为“备份到磁盘”设备，请参见 **Data Protector**。

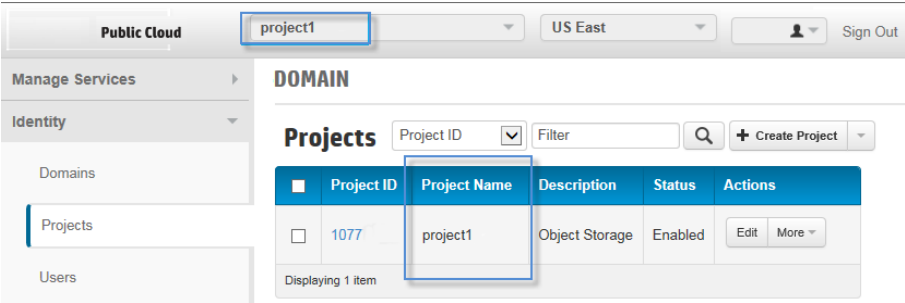
配置备份到磁盘设备 - 云 (Helion)

## 获取 HPE 公共云项目名称

### 步骤

1. 使用 **HPE 公有云凭据**登录到 **HPE 公有云控制台** (<https://horizon.hpcloud.com>)。
2. 从“项目”列表中选择适当的项目。
3. 记录项目名称，供将来在 **Data Protector GUI** 中使用。该名称将在设备创建期间在“租户/项目”字段中指定。

HPE 公共云中的项目



获取身份验证服务 URL

步骤

1. 从“用户”菜单中，选择**角色和 API 端点**。此时将打开“用户角色和 API 端点”页面。
  2. 单击**服务 API 端点**选项卡。此时将显示服务 API 端点的列表。
  3. 对于最接近数据中心的地理区域，请记录服务类型**标识**的服务 API 端点 URL。
- 稍后，在 Data Protector GUI 中创建云 (Helion) 设备期间，它将在“身份验证服务”字段中指定。

如果您决定使用访问密钥进行身份验证，请记录以 **/v3/** 后缀结尾的身份验证服务 URL。

例如：

<https://region-b.geo-1.identity.hpcloudsvc.com:35357/v3/>

HPE 公有云中的服务 API 端点

Current Roles

Service API Endpoints

Service API Endpoints

Service Name	URL(s)	Region	Service Type
Identity	Public URL: <a href="https://region-a.geo-1.identity.hpcloudsvc.com:35357/v2.0/">https://region-a.geo-1.identity.hpcloudsvc.com:35357/v2.0/</a>	US West	identity
Identity	Public URL: <a href="https://region-a.geo-1.identity.hpcloudsvc.com:35357/v3/">https://region-a.geo-1.identity.hpcloudsvc.com:35357/v3/</a>	US West	identity
Identity	Public URL: <a href="https://region-b.geo-1.identity.hpcloudsvc.com:35357/v2.0/">https://region-b.geo-1.identity.hpcloudsvc.com:35357/v2.0/</a>	US East	identity
Identity	Public URL: <a href="https://region-b.geo-1.identity.hpcloudsvc.com:35357/v3/">https://region-b.geo-1.identity.hpcloudsvc.com:35357/v3/</a>	US East	identity

创建访问密钥

步骤

1. 从“用户”菜单中，选择**管理访问密钥**。此时将打开“管理访问密钥”页。
2. 要创建新密钥，请指定新密钥的**开始日期**和**结束日期**，然后单击**创建密钥**。系统将创建新密钥。

在 HPE 公有云中创建访问密钥

Manage Keys for:

Keys

Show Secret Keys

ID	Valid From	Valid To	Created On	Status	Actions
AAA123P09BOZ123	2013-07-01T15:30:07.000Z	2023-06-29T15:30:07.000Z	2013-07-01T15:30:07.273Z	active	Deactivate More ▾
B08DK123SDFAZ45	2014-03-25T00:00:00.000Z	2024-03-24T00:00:00.000Z	2014-03-25T15:51:36.465Z	active	Deactivate More ▾

Displaying 2 items

Create new key

Start Date \*

2014-04-02

End Date \*

2024-04-01

Create Key

3. 单击**显示密钥**，显示新密钥的 ID 和密钥。

HPE 公有云中的密钥

Manage Keys for:

Keys

ID	Valid From	Valid To	Created On	Secret Key	Status	Actions
ABC1DEF242CCCC	2013-07-01T15:30:07.000Z	2023-06-29T15:30:07.000Z	2013-07-01T15:30:07.273Z	1e43z2ABC09C1DWfQasb30odL42ABC09C1D	active	Deactivate
1432ABC09CDW04	2014-03-25T00:00:00.000Z	2024-03-24T00:00:00.000Z	2014-03-25T15:51:36.465Z	A1bC1D6Fdh2ABC09C1D242CmiC1C9dpaz2C	active	Deactivate

Displaying 2 items

4. 复制密钥 ID 和密钥信息以供将来使用。它们将在 Data Protector GUI 中创建“云 (Helion)”设备期间指定。

配置备份到磁盘设备 - 云 (Helion)

在 Data Protector 中，配置“备份到磁盘”设备并将接口类型设置为“云 (Helion)”设备。

步骤

- 在上下文列表中，单击**设备和介质**。
- 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
- 指定设备名称及其说明(可选)。
- 选择**备份到磁盘**设备类型，然后选择接口类型：**云 (Helion)**。单击**下一步**。
- 指定**身份验证服务 URL**。这是**获取身份验证服务 URL**中的服务 API 端点 URL。
- 在**身份验证模式**列表中，选择身份验证的模式。
  - 要使用用户名和密码身份验证，请选择**用户名和密码**并输入 HPE 公有云凭据。
  - 要使用访问密钥进行身份验证，请选择**访问密钥**并输入**访问密钥 ID**和**密钥**。这些是在**创建访问密钥**中创建的密钥。

**注意：**  
要使用访问密钥进行身份验证，则身份验证服务 URL 必须包含 **/v3/** 后缀。  
例如：  
`https://region-b.geo-1.identity.hpcloudsvc.com:35357/v3/`

- 指定**租户/项目**。这是**获取项目名称**中的项目名称。
- 单击**选择/创建容器**，从现有容器的列表中选择容器或创建新容器。
- 指定数据源的本地网关。

- a. 选择一个网关，然后单击**添加**以显示“属性”对话框。根据需要更改任意网关属性，然后单击**确定**添加网关。
10. 单击**下一步**以显示“摘要”窗口。检查设置并单击**完成**。新配置的设备将显示在“范围窗格”中。

## 配置备份到磁盘设备 - 云 (Azure)

在 Data Protector 中，配置“备份到磁盘”设备，将**接口类型**设为：“云 (Azure)”。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在**设备名称**字段指定设备名称，可选填**说明**字段。
4. 选择**备份到磁盘**设备类型，然后选择**接口类型**：“云 (Azure)”。单击**下一步 (Next)**。  
默认情况下会输入**管理控制台 URL**。
5. 在字段中输入**存储帐户名**、**密钥**和**密钥 2**的信息。单击**添加**添加网关以向云 (Azure) 发送数据。此时将显示“选择容器”窗口。
6. 选择现有的容器或创建新的容器以加载数据。可以通过默认值添加网关。  
对象复制的块大小存在限制。如果将对象从本地设备复制到云，并复制回同一设备以备恢复，则本地设备和云设备的块大小必须匹配。
7. 单击**检查**验证网关是否已连接到云 (Azure)。如果连接成功，则“状态”显示为**正常**。设备已创建且可供使用。

## 配置文件库设备

请注意，文件库设备所在的磁盘必须在介质代理的本地。否则，设备性能可能会降低。

### 先决条件

- 文件库设备所在的磁盘必须在文件库设备所在的文件系统中可见。
- 文件库设备所在的磁盘上必须存在其中要创建文件库设备的内容的目录。
- 如果要在 Windows 系统上创建文件库设备，需为要用作文件库设备的文件禁用 Windows 压缩选项。

### 限制

- 文件库设备可以包括一个或多个目录。但只有一个目录可以位于文件系统上。
- 可用于配置文件库类型设备的目录的路径名长度不能超过 46 个字符。

## 步骤

1. 在希望文件库设备所在的磁盘上为该设备创建一个目录，例如：`c:\FileLibrary`。  
可以在本地或网络驱动器(或 UNIX 系统中由 NFS 装载的文件系统)上创建文件库设备。可以用 `\\hostname\share_name` 形式指定网络驱动器，也可以将其映射到驱动器盘符 (`S:\datastore\My_FileLibrary`)。

“浏览驱动器”对话框中输入路径的地方没有显示主机名以及共享名和网络驱动器。需要自行输入 UNC 名称或网络驱动器的路径。

在 **Windows** 操作系统上，要获得正确的权限以访问文件库设备所在的共享磁盘，请更改介质代理上的 **Data Protector Inet** 帐户(通过向其授予访问本地客户机系统和远程共享磁盘的权限)。此外，确保它是特定用户帐户，而非系统帐户。设置 **Inet** 帐户后，即可配置和使用共享磁盘上的文件库设备。

### 重要：

不要从磁盘删除为文件库创建的目录。如果删除了该目录，则将丢失文件库设备中的任何数据。

2. 在 **Data Protector Manager**“上下文列表”中，单击 **设备和介质**。
3. 在“范围窗格”中，右键单击 **设备**，然后单击 **添加设备** 以打开向导。
4. 在“设备名称”文本框中，键入文件库设备的名称。
5. 在“说明”文本框中，键入库的说明(可选)。
6. 在“设备类型”下拉列表中，选择 **文件库**。
7. 在“客户机”下拉列表中，选择设备所在的系统。单击 **下一步**。
8. 指定希望库所在的目录或一组目录。单击 **添加**。
9. 要更改目录的默认属性，请选择该目录，然后单击 **属性**。
10. 输入文件库设备的写入程序数量。默认为所添加的目录的数量。如果所添加的写入器多于设备中的目录数，则可能将提高设备性能。这一点取决于硬件配置。需要在环境中测试这一点。单击 **下一步**。
11. 文件库设备的“介质类型”为“文件”。要在此文件库中启用虚拟完整备份，请选择 **使用分布式文件介质格式**。单击 **下一步**。
12. 查看文件库设备配置的摘要。单击 **完成** 退出向导。

此时所配置设备的列表中将显示该设备的名称。设备名称还显示在向其分配该设备的介质池中。

直到第一次使用该设备，该设备中才会显示文件仓库。

第一次使用该设备之后，可以扫描该设备以验证配置。

默认情况下，由文件库使用的介质池的介质使用策略为不可追加。建议使用此策略，因为这样可使您从文件库中受益，如自动重用过期的介质。此外，要使用文件库执行对象复制或对象合并，必须采用不可追加的介质使用策略。

## 关于配置设备的多个路径

**SAN** 环境中的设备通常连接到若干客户机，因此可以通过若干路径访问该设备，这些路径包括客户机名称和 **SCSI** 地址(UNIX 系统中的设备文件)。**Data Protector** 可以使用这些路径

中的任意一种。您可以将所有物理设备路径配置为单个逻辑设备——多路径设备。

例如，连接到 **client1** 的磁带设备配置为 `/dev/rs1` 和 `/dev/rs2`，在 **client2** 上配置为 `/dev/r1s1`，在 **client3** 上配置为 `scsi1:0:1:1`。因此，可以通过四条不同的路径访问该设备：`client1:/dev/rs1`、`client1:/dev/rs2`、`client2:/dev/r1s1` 和 `client3:scsi1:0:1:1`。因此，多路径设备包含指向此磁带设备的所有四个路径。

## 为何使用多条路径

如果使用以前版本的 **Data Protector**，只能从一个客户机访问设备。为解决此问题，必须为使用锁名称的物理设备配置多个逻辑设备。因此，如果使用锁名称来配置从不同系统对单个物理设备的访问，就不得不在每个系统上配置所有设备。例如，如果有 10 台客户机与单个设备连接，则必须用相同的锁名称配置 10 台设备。而使用当前版本的 **Data Protector** 简化了这一配置过程，您可以为所有路径配置单个多路径设备。

多路径设备可提高系统的复原能力。**Data Protector** 将尝试使用所定义的第一个路径。如果某台客户机上的所有路径都不可访问，**Data Protector** 会尝试使用下一台客户机上的路径。只有当所有列出的路径都不可用时，才会中止会话。

## 路径选择

备份会话期间，按设备配置期间定义的顺序选择设备路径，但如果在备份规范中选择了首选客户机则例外。在这种情况下，首先使用首选客户机上的路径。

还原会话期间，按以下顺序选择路径：

1. 还原对象的目标客户机上的路径，如果所有对象都还原到同一目标客户机
2. 过去用于备份的路径
3. 其他可用路径

对于配置了多个路径的设备，首选本地路径。如果没有本地路径可用，则以预定义顺序使用任何可用路径。

如果启用了直接库访问功能，则无论配置了什么顺序，都会首先使用本地路径(目标客户机上的路径)进行库控制。

**Data Protector** 备份会话管理器 (BSM) 在多路径 SAN 环境中尽可能使用本地设备。您可通过使用 LANfree 全局选项调整此行为。

LANfree 全局选项有两个可能的值：

- 0—是默认值。对于低于 8.11 的早期 **Data Protector** 版本，无需进行任何更改。
- 1—适用于具有以下特点的多路径环境：**Data Protector** 选择生成对象的主机，而不是从多路径列表中选择首选主机或第一个主机。

下文介绍 LANfree 全局选项设置为 1 时多路径设备分配的实际改进。

- **Data Protector** 优先为已配置主机路径的设备选择生成数据的该主机。
- **Data Protector** 在生成数据的主机上为已配置主机路径的设备启动新介质代理 (MA)。即使已通过可用的并发插槽为目标设备启动远程 MA，也会执行此操作。

在以下情况下，**Data Protector** 可能还无法对设备使用本地路径：

- 如果用户已指定负载均衡(MIN 或 MAX 参数)，则 BSM 可选择并锁定任何不属于生成数据主机本地的设备。
- 如果控制多路径设备的 MA 在一个主机上执行，而对象来自具有设备路径的其他主机，则 Data Protector 不会将 MA 迁移到本地主机，但会通过 LAN 将数据传送到已启动的 MA。已达到负载均衡的 MAX 值时，便会发生这种情况。
- 设置 IgnoreObjectLocalityForDeviceSelection 全局选项之后，将禁用 LANfree 设置。默认情况下，未设置 IgnoreObjectLocalityForDeviceSelection。

在以下情况下，用户可能需要添加额外的设备路径，才能实现无 LAN 备份：

- 当备份客户机具有多个网络接口和主机名时。在这种情况下，根据 DNS 配置，Data Protector 备份可能会经过多个接口。然后，建议为每个接口添加本地路径。
- 当对属于 Windows 群集资源的 Windows 文件服务器执行文件系统备份时。在此类设置中，每个 Windows 群集资源均应有自己的主机名，应为这些主机名创建单独的设备路径条目。

## 向后兼容

在升级过程中，不用重新配置使用以前版本的 Data Protector 配置过的设备，无需任何更改就可像在先前版本的 Data Protector 中那样使用这些设备。为了利用新增的多路径功能，请将设备重新配置为多路径设备。

## 限制

以下限制适用：

- NDMP 设备和介质库不支持多路径。
- 多路径设备不支持设备链。

## 设置设备和介质的高级选项

配置新设备时或更改设备属性时，可以设置设备和介质的高级选项。是否有这些选项取决于设备类型。

配置备份时也可以设置其中某些选项。一般而言，备份规范中设置的设备选项优先于为设备设置的选项。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在“范围窗格”中，展开**设备**。
3. 右键单击要更改其选项的设备(库设备情况下为驱动器)，然后单击**属性**。
4. 单击**设置**选项卡，然后单击**高级**按钮，打开“高级选项”页：**设置**、**大小**和**其他**。
5. 指定所需的选项，然后单击**确定**应用更改。

## 配置 VTL 设备

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**环境**，然后右键单击**设备**，并单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入 VTL 的名称。
4. 在“说明”文本框中，输入说明(可选)。
5. (可选)选择**多路径设备**。
6. 在“设备类型”列表中，选择 **SCSI 库**。然后，在“接口类型”列表中自动选择 **SCSI**。
7. 如果未选择**多路径设备**选项，则在“客户机”列表中选择客户机的名称。
8. (可选)在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。单击**下一步**。
9. 指定有关库 SCSI 地址和驱动器处理的所需信息，然后单击**下一步**。
10. 指定要与 Data Protector 配合使用的插槽，然后单击**下一步**。
11. 选择将与设备配合使用的介质类型。
12. 单击**完成**退出向导。

**注意：**如果在 RedHat Linux (RHEL) 7.1 系统上使用 VTL 设备，则必须手动加载通用 SCSI 驱动程序。可以通过执行命令 `modprobe -vs sg` 完成此操作。还建议将此命令添加到 RHEL init scripts 或 cron job 以确保在系统启动时启动此命令。

## 配置堆栈器设备

将备份设备连接到系统并且存在正常工作的设备文件(SCSI 地址)之后，可以配置该备份设备与 Data Protector 配合使用。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明(可选)。
5. (可选)选择**多路径设备**。
6. 如果未选择**多路径设备**选项，则选择客户机的名称。
7. 单击**下一步**。
8. 在“设备类型”列表中，选择**堆栈器**设备类型，然后单击**下一步**。
9. 在“数据设备”文本框中，输入物理设备的 SCSI 地址(Windows 系统)，输入设备文件名(UNIX 系统)，或使用下拉箭头自动检测驱动器地址或文件名。  
对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。



10. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
11. 单击**下一步**。
12. 在“介质类型”下拉列表中，对要配置的设备选择介质类型。
13. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。
14. 单击**完成**退出向导。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。如果正确配置了设备，则 **Data Protector** 将可以在插槽中加载、读取和卸载介质。

## 堆栈器设备介质管理

配置堆栈器设备之后，请考虑管理此类设备中的介质有一些具体问题。例如，对于堆栈器设备中的每个介质，必须单独运行扫描、验证或格式化操作。应正确加载介质才能运行 **Data Protector** 会话。

## 配置介质库设备(光盘库)

将备份设备连接到系统并且存在正常工作的设备文件(SCSI 地址)之后，可以配置该备份设备与 **Data Protector** 配合使用。

### 配置介质库设备

#### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明(可选)。
5. 在“设备类型”列表中，选择**介质库**设备类型。
6. 在“客户机”列表中，选择客户机的名称。
7. (可选)在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
8. 单击**下一步**。
9. 为介质库指定一组文件/磁盘。使用短划线一次输入多个文件或磁盘(例如 /tmp/FILE 1-3)，然后单击**添加**。对于磁光盘介质库，磁盘名称必须以 A/a 或 B/b 结尾。单击**下一步**。
10. 在“介质类型”列表中，对要配置的设备选择介质类型。
11. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

## 配置介质库设备中的驱动器

### 步骤

1. 在“设备名称”文本框中，输入设备的名称。
2. 在“说明”文本框中，输入说明(可选)。
3. 指定所选介质类型的介质池。可以从“介质池”列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。单击**下一步**。
4. (可选)选择**设备可用于还原和/或设备可用作进行对象复制的源设备**，并指定**设备标记**。
5. 单击**完成**退出向导。

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。

## 配置 SCSI 库或箱盒设备

将备份设备连接到系统并且存在正常工作的设备文件(SCSI 地址)之后，可以配置该备份设备与 **Data Protector** 配合使用。

除了配置箱盒设备时必须指定设置了**箱盒支持**选项的介质池外，库和箱盒设备的配置过程相同。

建议让 **Data Protector** 自动配置备份设备。

## 配置 SCSI 库机械手

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明(可选)。
5. (可选)选择**多路径设备**。
6. 在“设备类型”列表中，选择 **SCSI 库** 设备类型。
7. 在“接口类型”列表中，选择 **SCSI** 接口类型。
8. 如果未选择**多路径设备**选项，则在“客户机”列表中选择客户机的名称。
9. (可选)在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
10. 单击**下一步**。
11. 输入库机械手的 SCSI 地址，或使用下拉箭头自动检测驱动器地址或文件名  
对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。
12. 在**繁忙驱动器处理**列表中，选择在驱动器繁忙时 **Data Protector** 应采取的操作。

13. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
14. (可选)选择**SCSI 保留/释放(机械手控制)**。单击**下一步**。
15. 指定设备的插槽。使用短划线输入插槽范围，然后单击**添加**。例如，输入 1-3，然后单击**添加**可同时添加插槽 1、2 和 3。请勿使用字母或以零开头。单击**下一步**。
16. 在“介质类型”下拉列表中，对要配置的设备选择介质类型。
17. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

## 配置库中的驱动器

### 步骤

1. 在“设备名称”文本框中，输入设备的名称。
2. 在“说明”文本框中，输入说明(可选)。
3. (可选)选择**多路径设备**。
4. 如果未选择**多路径设备**选项，则在“客户机”列表中选择客户机的名称。

**提示：**

可以配置库，以使每个驱动器从运行 **Data Protector** 介质代理的不同系统接收数据。这样可以提高高端环境中的性能。从“客户机”下拉列表中，选择要与每个驱动器配合使用的客户机系统。

单击**下一步**。

5. 在“数据驱动器”文本框中，输入数据驱动器的 **SCSI 地址**或文件名。  
对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。
6. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
7. 在“驱动器索引”文本框中，输入库中驱动器的索引。单击**下一步**。
8. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。建议使用默认的介质池。

**注意：**

不必将所有驱动器都配置为用于 **Data Protector**。可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。

指定箱盒设备的介质池时，请选择设置了**箱盒支持**选项的池。

单击**下一步**。

9. (可选)选择**设备可用于还原和/或设备可用作进行对象复制的源设备**，并指定**设备标记**。
10. 单击**完成**退出向导。

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。如果正确配置了设备，则 **Data Protector** 将可以在插槽中加载、读取和卸载介质。

## 配置 SAN 环境中的设备

SAN 环境的规模可以从一个客户机使用一个库到若干客户机使用若干库不等。客户机可以采用不同的操作系统。从 **Data Protector** 的角度看，配置 SAN 环境的目标是：

- 在要共享库机械手的每个主机上，为每个主机创建一个库机械手。如果只有一个主机控制机械手，则仅为默认的机械手控制主机创建库定义。
- 在要参与共享库中同一(磁带)驱动器的每个主机上：
  - 为要使用的每个设备都创建设备定义。
  - 如果另一个主机也将使用(物理)设备(共享设备)，则使用锁名称。
  - (可选)如果要使用直接访问，则选择此功能。如果使用此功能，请确保在该主机上设置了 **libtab** 文件。

## 注意事项

- **Microsoft 群集服务器**：确保两个群集节点上的驱动器硬件路径相同：配置设备后，即执行故障转移核实这一点。

## 配置方法

有三种配置方法，具体采用哪一种取决于参与 SAN 配置的平台：

## 使用 GUI 自动配置设备

可以使用 **Data Protector** 自动配置功能在 SAN 环境中的多个主机上自动配置设备和库。以下操作系统中提供自动配置功能：

- Windows
- HP-UX
- Solaris
- Linux
- AIX

## 限制

自动配置无法用于配置 SAN 环境中的以下设备：

- 混合介质库
- DAS 或 ACSLS 库
- NDMP 设备

**Data Protector** 可发现连接到环境的备份设备。对于库设备，**Data Protector** 确定插槽数、介质类型和属于库的驱动器。然后，**Data Protector** 设置逻辑名称、锁名称、介质类型、设备的设备文件或 **SCSI** 地址以及驱动器和插槽，从而配置设备。

**注意：**

将新主机引入 SAN 环境中时，将不自动更新所配置的库和设备。

- 要在新主机上使用现有的库，请删除此库，并在新主机上配置一个同名的新库。
- 要将设备添加到现有的库，或者删除该库，然后在新主机上自动配置一个同名的新库以及新驱动器，或者手动将驱动器添加到库中。

## 使用 CLI 自动配置设备(sanconf 命令)

可以使用 sanconf 命令配置 SAN 环境中的设备和库。sanconf 命令是一个实用程序，使用它可以更轻松地配置单个 Data Protector 单元的 SAN 环境中以及具有集中式介质管理数据库 (CMMDB) 的 MoM 环境中的库。它通过从多个客户机收集有关驱动器的信息并将这些驱动器配置为一个库，可自动配置 SAN 环境中的库。在 MoM 环境中，sanconf 还可以配置使用 CMMDB 的任何 Data Protector 单元中的任何库(如果运行 sanconf 的单元使用 CMMDB)。以下操作系统中提供 sanconf：

- Windows
- HP-UX
- Solaris

sanconf 可以检测和配置连接到在以下操作系统中运行的客户机的受支持设备：

- Windows
- HP-UX
- Solaris
- Linux
- AIX

使用此命令，可以：

- 扫描指定的 Data Protector，同时收集有关连接到 SAN 环境中客户机的驱动器和机械手的 SCSI 地址的信息。
- 使用在扫描 Data Protector 客户机期间收集的信息，配置或修改给定客户机的库或驱动器的设置。
- 从库中删除所有或指定客户机上的驱动器。

## 设备锁定

sanconf 命令自动为配置的驱动器创建锁名称。锁名称由驱动器供应商 ID 字符串、产品 ID 字符串和产品序列号组成。

例如，供应商 ID 为“HP”、产品 ID 为“DLT8000”和序列号为“A1B2C3D4E5”的 DLT8000 驱动器的锁名称将为 HP:DLT8000:A1B2C3D4E5。

还可以手动添加锁名称。锁名称对于每个逻辑设备都是唯一的。

不得更改由 sanconf 命令创建的锁名称。手动创建并且表示已由 sanconf 配置的物理驱动器的所有其他逻辑驱动器也必须使用由 sanconf 创建的锁名称。

## 限制

- 有关通过 `sanconf` 支持的库的完整列表，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新支持矩阵。
- `sanconf` 不提供以下功能：
  - 将备用驱动器放入驱动器插槽中。
  - 混合驱动器类型；例如，DLT、9840 和 LTO 驱动器的组合。
  - 配置当前不可用的客户机。只有在使用包括通过扫描客户机收集的信息的配置文件执行库的配置时，才能配置此类客户机。

## 建议

对于系统中的特定设备仅配置一个驱动程序。

有关如何使用 `sanconf` 命令的信息，请参见 `sanconf` 手册页或 `Data Protector` 命令行界面参考。

## 在 UNIX 系统中手动配置

手动配置 SAN 环境中连接到 UNIX 系统的共享设备时，必须：

- 为要使用的每个设备都创建设备定义。
- 使用锁名称。
- (可选)如果要使用直接访问，则选择此功能。如果这样做，则必须确保正确配置了该主机上的 `libtab` 文件。

## 阶段

1. 手动配置设备
2. 手动配置 `libtab` 文件

## 手动配置 SAN 环境中的设备

以下过程表示若干系统使用驱动器和库机械手、若干应用程序(不只是 `Data Protector`)使用驱动器以及所有系统都发送机械手控制命令(直接库访问)。以下任务还提供用于不同环境的替代步骤。

要控制机械手，可以使用 SAN 中的任意客户机。首先需要在充当默认机械手控制系统的客户机上配置库机械手控制。无论哪个客户机请求介质移动，都将使用此客户机管理介质移动。这样做是为了放置多个主机同时请求介质移动时机械手出现冲突。只有在主机故障并启用了直接访问时，由请求介质移动的本地主机执行机械手控制。

## 先决条件

必须在需要与共享库通信的每个客户机上安装 **Data Protector** 介质代理(常规介质代理或 NDMP 介质代理)。

## 配置阶段

配置 SAN 环境中的库

配置库中的驱动器

## 配置 SAN 环境中的库

### 注意：

如果希望由群集管理机械手控制，则需要确保：

- 每个群集节点上都存在机械手控制。
- 库机械手配置中使用了虚拟群集名称。
- 使用 `mksf` 命令或使用 `libtab` 文件安装了常用的机械手和设备文件名。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **设备**，然后单击 **添加设备** 以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. (可选)在“说明”文本框中，输入说明。
5. (可选)选择 **多路径设备**。
6. 在“设备类型”下拉列表中，选择 **SCSI 库** 设备类型。
7. 在“接口类型”下拉列表中，选择 **SCSI** 接口类型。
8. 如果未选择 **多路径设备**，则从“客户机”下拉列表中选择客户机的名称。
9. (可选)在 **管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
10. 单击 **下一步**。
11. 输入库机械手的 **SCSI** 地址，或使用下拉箭头自动检测驱动器地址或文件名。  
对于多路径设备，还要从“客户机”下拉列表中选择客户机名称。单击 **添加**，将路径添加到所配置路径的列表中。
12. 在 **繁忙驱动器处理** 列表中，选择 **弹出介质**。
13. 如果要启用对已更改 **SCSI** 地址的自动发现，则选择 **自动发现已更改的 SCSI 地址**。  
单击 **下一步**。
14. 指定设备的插槽。使用短划线一次输入多个插槽，然后单击 **添加**。例如，输入 **1-3**，然后单击 **添加** 可同时添加插槽 **1**、**2** 和 **3**。单击 **下一步**。
15. 在“介质类型”下拉列表中，对要配置的设备选择介质类型。
16. 单击 **完成** 退出此向导。此时将提示您配置库驱动器。单击 **是**，然后将显示驱动器配置向导。按照向导操作，如下方的任务中所述。

## 配置库中的驱动器

在从中要使用每个驱动器的每个客户机上配置这些驱动器。

### 步骤

1. 在“设备名称”文本框中，输入驱动器的名称。  
建议使用以下命名约定：
  - LibraryLogicalName\_DriveIndex\_Hostname，例如 SAN\_LIB\_2\_hotdog(对于非多路径设备)
  - LibraryLogicalName\_DriveIndex，例如 SAN\_LIB\_2(对于多路径设备)
2. (可选)在“说明”文本框中，输入说明。
3. (可选)选择**多路径设备**。
4. 如果未选择**多路径设备**，则从“客户机”下拉列表中选择客户机的名称。
5. 单击**下一步**。
6. 在“数据驱动器”文本框中，输入数据驱动器的 **SCSI** 地址或文件名  
对于多路径设备，还要从“客户机”下拉列表中选择客户机名称。单击**添加**，将路径添加到所配置路径的列表中。
7. 在“驱动器索引”文本框中，输入库中驱动器的索引。
8. 如果要启用对已更改 **SCSI** 地址的自动发现，则选择**自动发现已更改的 SCSI 地址**。  
单击**下一步**。
9. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。  
可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。
10. 单击**高级**按钮。在**设置**选项卡中，选择**使用直接库访问**选项。  
如果只希望由一个系统发送用于启动 **Data Protector** 的机械手控制命令，则不要选择**使用直接库访问**选项。用 **Data Protector** 配置库/驱动器时选择的客户机系统将控制库机械手。
11. 对于多路径驱动器不必执行此步骤。单击**下一步**。
  - 如果 **Data Protector** 是唯一一个访问驱动器的应用程序，则单击**其他**选项卡，选择**使用锁名称**选项，然后输入名称。记住该名称，因为在另一个客户机上配置相同驱动器时将需要该名称。建议使用以下命名约定：  
LibraryLogicalName\_DriveIndex，例如 SAN\_LIB\_D2
  - 如果 **Data Protector** 不是唯一一个访问驱动器的应用程序，则选择**使用锁名称**选项，并确保操作规则要求同时只能从一个应用程序中独占访问所有设备。
  - 如果只有一个系统使用该驱动器，则不要选择**使用锁名称**选项。
12. (可选)选择**设备可用于还原和/或设备可用作进行对象复制的源设备**，并指定**设备标记**。
13. 单击**完成**退出向导。



驱动器由若干系统和若干应用程序(不仅由 **Data Protector**)使用。使用设备锁定(定义“锁名称”)，并确保操作规则要求同时只能从一个应用程序中独占访问所有设备

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。

## 配置 SAN 环境中的 libtab 文件

libtab 文件的用途是映射库机械手控制访问权限，以便也可以在“直接访问请求系统”上工作，因为此处的本地控制路径可能与默认库机械手控制系统上使用的路径不同。

在每个需要“直接访问”库机械手，并且与配置为默认库机械手控制系统的系统不同的 Windows 和 UNIX 客户机上都需要一个 libtab 文件。

### 步骤

1. 在每个请求直接访问的系统上的以下目录中以纯文本格式创建 libtab 文件：

**Windows 系统：** *Data\_Protector\_home\libtab*

**HP-UX 和 Solaris 系统：** */opt/omni/.libtab*

**其他 UNIX 系统：** */usr/omni/.libtab*

2. 在 libtab 文件中提供以下信息：

*FullyQualifiedHostname DeviceFile | SCSIPath DeviceName*

- *FullyQualifiedHostname* 是请求直接访问控制库机械手的客户机的名称。如果客户机是群集的一部分，则应使用节点名称。
- *DeviceFile | SCSIPath* 是此客户机上库机械手驱动程序的控制路径。
- *DeviceName* 是在此客户机上使用的设备定义的名称。

对于请求直接访问的每个设备都需要有一行。

如果系统是群集的一部分，则 *FullyQualifiedHostname* 必须是虚拟服务器名称，并且 *DeviceFile | SCSIPath* 必须指向群集节点(物理系统)。

## 配置 ADIC/GRAU DAS 库设备

Data Protector 提供一个专用的 ADIC/GRAU 库策略，用于将 ADIC/GRAU 库配置为 Data Protector 备份设备。

装有介质代理软件并通过 DAS 服务器访问库机械手的每个系统都称为 DAS 客户机。

以下内容可能会提供其他信息：

- ADIC/GRAU 功能需要持有特定的 Data Protector 许可证。有关详细信息，请参见《*Data Protector 安装指南*》。
- 由于此库管理由不同应用程序使用的介质，因此必须配置希望将哪些介质和驱动器与 Data Protector 配合使用，以及要跟踪哪些介质。
- Data Protector 自行保持独立的介质分配策略，并且不使用暂存池。

## 配置阶段

1. 连接库驱动器
2. 准备安装介质代理
3. 安装介质代理
4. 配置 ADIC/GRAU DAS 库设备
5. 配置 ADIC/GRAU DAS 库设备中的驱动器

## 连接库驱动器

### 步骤

1. 将库驱动器和机械手物理连接到要安装介质代理软件的系统。  
有关如何将备份设备物理连接到 UNIX 和 Windows 系统的信息，请参见《Data Protector 安装指南》。
2. 配置 ADIC/GRAU 库。请参见 ADIC/GRAU 库随附的文档获取相关说明。  
有关受支持 ADIC/GRAU 库的详细信息，请访问  
<https://softwaresupport.softwaregrp.com/>。

## 准备安装介质代理

### 步骤

1. 如果 DAS 服务器基于 OS/2，则在配置 Data Protector ADIC/GRAU 备份设备之前，请创建或者更新 DAS 服务器计算机上的 C:\DAS\ETC\CONFIG 文件。  
在此文件中，必须定义所有 DAS 客户机的列表。对于 Data Protector，这意味着必须定义每个装有介质代理的 Data Protector 客户机。  
每个 DAS 客户机都用唯一的客户机名称(无空格)进行标识，例如 OMNIBACK\_C1。在此示例中，C:\DAS\ETC\CONFIG 文件的内容应类似于此：

```
client client_name = OMNIBACK_C1,  
# hostname = AMU,"client1"  
ip_address = 19.18.17.15,  
requests = complete,  
options = (avc,dismount),  
volumes = ((ALL)),  
drives = ((ALL)),  
inserts = ((ALL)),  
ejects = ((ALL)),  
scratchPools = ((ALL))
```

必须在每个 Data Protector 介质代理客户机上将这些名称配置为 omnirc 选项 DAS\_CLIENT。omnirc 文件是 *Data\_Protector\_home* 目录 (Windows 系统) 中的文件 omnirc，或文件 .omnirc (UNIX 系统)。例如，在 IP 地址为 19.18.17.15 的系统上，omnirc 文件中相应的行为 DAS\_CLIENT=OMNIBACK\_C1。

2. 了解如何静态或动态配置了 ADIC/GRAU 库插槽分配策略。有关如何检查所用分配策略的类型的信息，请参见 AMU Reference Manual。

静态策略对于每个 volser 具有专用的插槽，而动态分配策略则随机分配插槽。根据已设置的策略相应地配置 Data Protector。

如果已配置了静态分配策略，则将以下 omnirc 选项添加到控制库机械手的系统中：

```
OB2_ACIEJECTTOTAL = 0
```

请注意，这适用于 HP-UX 和 Windows。

有关配置 ADIC/GRAU 库的进一步问题，请与 ADIC/GRAU 支持人员联系或查阅 ADIC/GRAU 文档。

## 安装介质代理

可以在将物理连接到 ADIC/GRAU 库中备份驱动器的系统中和在将通过 DAS 服务器访问库机械手的系统中安装常规介质代理或 NDMP 介质代理。

### 注意：

需要特殊的许可证，具体取决于含介质的存储库的大小或 ADIC/GRAU 库中使用的驱动器数和插槽数。有关详细信息，请参见《Data Protector 安装指南》。

## 先决条件

- ADIC/GRAU 库必须经过配置并正在运行。有关如何配置 ADIC/GRAU 库，请参见 ADIC/GRAU 库随附的文档。
- DAS 服务器必须正常运行，并且必须正确配置 DAS 客户机。
  - 需要用 DAS 软件控制 ADIC/GRAU 库。该软件由一个 DAS 服务器和多个 DAS 客户机构成。有关 DAS 软件的详细信息，请参见 ADIC/GRAU 库随附的文档。
- 安装介质代理之前，请获取以下信息：
  - DAS 服务器的主机名。

- 含有驱动器相应 DAS 名称的可用驱动器列表。

如果已定义 ADIC/GRAU 系统的 DAS 客户机，则运行以下命令以获取此列表：

```
dasadmin listd2 [client] 或
```

```
dasadmin listd [client]，其中，[client] 是要显示所保留驱动器的 DAS 客户机。
```

dasadmin 命令位于 OS/2 主机上的 C:\DAS\BIN 目录中，即装有 DAS 客户机的目录中：

**Windows 系统：** %SystemRoot%\system32

**UNIX 系统：** /usr/local/aci/bin

- 含有相应格式规范的可用插入/弹出区域的列表。

可以在 OS/2 主机上 AMS (AML 管理软件) 的图形配置中获得此列表：

在“管理”菜单中，单击**配置**以启动配置。双击 **I/O** 打开 **EIF-Configuration** 窗口，然后单击**逻辑范围**。在文本框中，将会列出可用的“插入/弹出区域”。

请注意，一个 **Data Protector** 库设备只能处理一种介质类型。记住哪种介质类型属于每个指定的“插入/弹出区域”非常重要，因为稍后将需要该数据来为 **Data Protector** 库配置“插入/弹出区域”。

- **Windows 系统：** Windows 系统：驱动器的 SCSI 地址列表，例如 `scsi4:0:1:0`。
- **UNIX 系统：** 驱动器的 UNIX 设备文件的列表。

在系统上运行 `ioscan -fn` 系统命令以显示所需的信息。

## 步骤

1. 使用 **Data Protector** 图形用户界面和安装服务器，将介质代理组件分发到客户机。
2. 为客户机界面安装 **ADIC/GRAU** 库。

### Windows 系统：

- 将 `aci.dll`、`winrpc32.dll` 和 `ezrpc32.dll` 库复制到 `Data_Protector_home\bin` 目录。(这三个库是随 **ADIC/GRAU** 库提供的 **DAS** 客户机软件的一部分。在安装介质上或 **AMU-PC** 上的 `C:\DAS\AMU\` 目录中可以找到它们。)
- 将这三个库也复制到 `%SystemRoot%\system32` 目录。
- 将 `Portinst` 和 `Portmapper` 服务复制到 **DAS** 客户机上。(这些必需文件是随 **ADIC/GRAU** 库提供的 **DAS** 客户机软件的一部分。在安装介质上可以找到它们。)
- 在“控制面板”中，转至**管理工具、服务**，然后启动 `portinst` 来安装 `portmapper`。
- 重新启动 **DAS** 客户机以启动 `portmapper` 服务。
- 在“控制面板”中，转到**管理工具、服务**，检查 `portmapper` 和 `rpc` 服务是否正在运行。

### HP-UX、Linux 和 AIX 系统：

将共享库 `libaci.sl`(**HP-UX** 系统)、`libaci.so`(**Linux** 系统)或 `libaci.o`(**AIX** 系统)复制到目录 `/opt/omni/lib`(**HP-UX** 和 **Linux** 系统)或 `/usr/omni/lib`(**AIX** 系统)。您必须具有访问该目录的权限。确保共享库已为每个人(**root**、组和其他人)读取并执行了权限。  
(`libaci.sl` 和 `libaci.o` 共享库是随 **ADIC/GRAU** 库提供的 **DAS** 客户机软件的一部分。在安装介质上可以找到它们。)

3. 正确安装 **DAS** 软件之后，执行 `devbra -dev` 命令，检查库驱动器是否正确连接到系统。此命令位于默认的 **Data Protector** 管理命令目录中。

此时将显示包含相应设备文件/SCSI 地址的库驱动器的列表。

## 配置 **ADIC/GRAU DAS** 库设备

当 **ADIC/GRAU** 库物理连接到系统并且装有介质代理后，可以从 **Data Protector GUI** 中配置 **ADIC/GRAU** 库设备。然后，**DAS** 客户机将在特定的介质管理操作(查询、放入、弹出)期间访问 **ADIC/GRAU** 机械手。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**。
3. 在“设备名称”文本框中，键入设备的名称。
4. 在“说明”文本框中，(可选)键入说明。
5. (可选)选择**多路径设备**。
6. 在“设备类型”列表中，选择 **GRAU DAS 库**。
7. 如果未选择**多路径设备**选项，则选择将访问 ADIC/GRAU 机械手的介质代理客户机的名称。
8. (可选)在**管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
9. 单击**下一步 (Next)**。
10. 在“DAS 服务器”文本框中，键入 DAS 服务器的主机名。  
对于多路径设备，还要选择客户机名称，然后单击**添加**，将路径添加到所配置路径的列表中。
11. 在**繁忙驱动器处理**列表中，选择在驱动器繁忙时 Data Protector 应采取的操作，然后单击**下一步**。
12. 指定库的导入和导出区域，然后单击**添加**。单击**下一步 (Next)**。
13. 在“介质类型”列表中，为设备选择相应的介质类型。
14. 单击**完成**退出向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

## 配置 ADIC/GRAU DAS 库设备中的驱动器

### 步骤

1. 在“设备名称”文本框中，键入驱动器的名称。
2. 在“说明”文本框中，(可选)键入说明。
3. (可选)选择**多路径设备**。
4. 如果未选择**多路径设备**选项，则选择将访问 ADIC/GRAU 机械手的介质代理客户机的名称。
5. 单击**下一步 (Next)**。
6. 在“数据驱动器”文本框中，指定设备的 SCSI 地址。  
对于多路径设备，还要选择将访问 ADIC/GRAU 机械手的介质代理客户机的名称，然后单击**添加**，将路径添加到所配置路径的列表中。
7. 选择**自动发现已更改的 SCSI 地址**可启用对已更改 SCSI 地址的自动发现。
8. 在“驱动器名称”文本框中，指定在安装介质代理期间获取的 ADIC/GRAU 驱动器名称。单击**下一步 (Next)**。
9. 选择驱动器的**默认介质池**。
10. 单击**高级**以设置驱动器的高级选项，例如**并发**。单击**确定**。单击**下一步 (Next)**。

11. (可选)选择设备可用于还原和/或设备可用作进行对象复制的源设备，并指定设备标记。
12. 单击**完成**退出向导。

## 配置 StorageTek ACS 库设备

Data Protector 提供一个专用的 StorageTek ACS 库策略，用于将 StorageTek ACS 库配置为 Data Protector 备份设备。

装有介质代理软件并通过 ACSLS 访问库机械手的每个系统都称为 ACS 客户机。

以下内容可能会提供其他信息：

- STK 功能需要持有特定的 Data Protector 许可证。有关详细信息，请参见《Data Protector 安装指南》。
- 由于此库管理由不同应用程序使用的介质，因此必须配置希望将哪些介质和驱动器与 Data Protector 配合使用，以及要跟踪哪些介质。
- Data Protector 自行保持独立的介质分配策略，并且不使用暂存池。

## 配置阶段

1. [连接库驱动器](#)
2. [安装介质代理](#)
3. [配置 StorageTek ACS 库设备](#)
4. [配置 StorageTek ACS 库设备中的驱动器](#)

## 连接库驱动器

### 步骤

1. 将库驱动器和机械手物理连接到要安装介质代理软件的系统。  
有关如何将备份设备物理连接到 UNIX 和 Windows 系统的信息，请参见《Data Protector 安装指南》。
2. 配置 StorageTek ACS 库。请参见 STK ACS 库随附的文档获取相关说明。  
有关受支持 StorageTek 库的详细信息，请参见 <https://softwaresupport.softwaregrp.com/>。

## 安装介质代理

可以在将物理连接到 StorageTek 库中备份驱动器的系统中和在将通过 ACSLS 访问库机械手的系统中，安装常规介质代理或 NDMP 介质代理。

### 注意：

需要特殊的许可证，具体取决于含介质的存储库的大小或 StorageTek 库中使用的驱动器数和插槽数。有关详细信息，请参见《Data Protector 安装指南》。

## 先决条件

- StorageTek 库必须经过配置并正在运行。有关如何配置 StorageTek 库，请参见 StorageTek 库随附的文档。
- 必须获取以下信息，然后再开始安装介质代理软件：
  - 运行 ACSLS 的主机的 *hostname*。
  - 要用于 Data Protector 的 ACS 驱动器 ID 的列表。登录正在运行 ACSLS 的主机，并执行以下命令以显示该列表：  

```
rlogin "ACSLS hostname" -l acssa
```

输入终端类型并等待命令提示符。在 ACSSA 提示符处，输入以下命令：  

```
ACSSA> query drive all
```

ACS 驱动器的格式规范必须为以下格式：  

```
ACS DRIVE: ID:##,##,## - (ACS num, LSM num, PANEL, DRIVE)
```
  - 请确保将用于 Data Protector 的驱动器处于 **online** 状态。如果某个驱动器不处于 **online** 状态，则在 ACSLS 主机上使用以下命令更改状态：  

```
vary drive drive_id online
```
  - 可用的 ACS CAP ID 和 ACS CAP 格式规范的列表。登录正在运行 ACSLS 的主机，并执行以下命令以显示该列表：  

```
rlogin "ACSLS hostname" -l acssa
```

输入终端类型并等待命令提示符。在 ACSSA 提示符处，输入以下命令：  

```
ACSSA> query cap all
```

ACS CAP 的格式规范必须为以下格式：  

```
ACS CAP: ID:##,##,## (ACS num, LSM num, CAP num)
```
  - 确保将用于 Data Protector 的 CAP 处于 **online** 状态，并处于 **manual** 工作模式。如果 CAP 不处于 **online** 状态，则使用以下命令更改状态：  

```
vary cap cap_id online
```

如果 CAP 未处于 **manual** 操作模式，则使用以下命令更改模式：  

```
set cap manual cap_id
```
  - **Windows 系统：**Windows 系统：驱动器的 SCSI 地址列表，例如 `scsi4:0:1:0`。
  - **UNIX 系统：**驱动器的 UNIX 设备文件的列表。  
在系统上运行 `ioscan -fn` 系统命令以显示所需的信息。

## 步骤

1. 使用 Data Protector GUI 和适用于 Windows 的安装服务器将介质代理组件分发到客户机。
2. 在可访问库中机械手的所有库主机(介质代理客户机)上启动 ACS ssi 后台程序。

### Windows 系统：

安装 LibAttach 服务。有关详细信息，请参见 ACS 文档。请确保在 LibAttach 服务配置期间输入相应的 ACSLS 主机名。成功配置之后，将自动启动 LibAttach 服务，并且在每次系统重新启动之后也会自动启动该服务。

#### 注意：

安装 LibAttach 服务之后，检查 libattach\bin 目录是否已自动添加到系统路径。如果未添加，则手动添加它。

有关该服务的详细信息，请参见 StorageTek 库随附的文档。

### HP-UX 和 Solaris 系统：

请执行以下命令：

```
/opt/omni/acs/ssi.sh start ACS_LS_hostname
```

### AIX 系统：

请执行以下命令：

```
/usr/omni/acs/ssi.sh start ACS_LS_hostname
```

3. 从默认的 Data Protector 管理命令目录中执行 devbra -dev 命令，以检查库驱动器是否正确连接到您的介质代理客户机。

此时将显示包含相应设备文件/SCSI 地址的库驱动器的列表。

## 配置 StorageTek ACS 库设备

当 StorageTek 库物理连接到系统并且装有介质代理后，可以从 Data Protector GUI 中配置 StorageTek 库设备。然后，ACS 客户机将在特定的介质管理操作(查询、放入、弹出)期间访问 StorageTek 机械手。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **设备**，然后单击 **添加设备**。
3. 在“设备名称”文本框中，键入设备的名称。
4. 在“说明”文本框中，(可选)键入说明。
5. (可选)选择 **多路径设备**。
6. 在“设备类型”列表中，选择 **StorageTek ACS 库**。
7. 如果未选择 **多路径设备** 选项，则选择将访问 StorageTek 机械手的介质代理客户机。
8. (可选)在 **管理控制台 URL** 文本框中输入库管理控制台的有效 URL。
9. 单击 **下一步 (Next)**。
10. 在“ACSLM 主机名”文本框中，键入 ACS 服务器的主机名。  
对于多路径设备，还要选择客户机名称，然后将路径添加到所配置路径的列表中。
11. 在 **繁忙驱动器处理** 列表中，选择在驱动器繁忙时 Data Protector 应采取的操作，然后单击 **下一步**。
12. 指定库的 **CAPs**，然后单击 **添加**。单击 **下一步 (Next)**。
13. 在“介质类型”列表中，为设备选择相应的介质类型。



14. 单击**完成**退出向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

## 配置 StorageTek ACS 库设备中的驱动器

### 步骤

1. 在“设备名称”文本框中，键入驱动器的名称。
2. 在“说明”文本框中，(可选)键入说明。
3. (可选)选择**多路径设备**。
4. 如果未选择**多路径设备**选项，则选择将访问 StorageTek 机械手的介质代理客户机。
5. 单击**下一步 (Next)**。
6. 在“数据驱动器”文本框中，指定设备的 SCSI 地址。  
对于多路径设备，还要选择将访问 StorageTek 机械手的介质代理客户机，然后单击**添加**，将路径添加到所配置路径的列表中。
7. 在“驱动器索引”文本框中，指定在安装介质代理期间获取的 StorageTek 驱动器索引。  
驱动器索引为由逗号分隔的四个数字的组合。单击**下一步 (Next)**。
8. 选择驱动器的**默认介质池**。
9. 单击**高级**以设置驱动器的高级选项，例如**并发**。单击**确定**。单击**下一步 (Next)**。
10. (可选)选择**设备可用于还原和/或设备可用作进行对象复制的源设备**，并指定**设备标记**。
11. 单击**完成**退出向导。

## 关于使用备份设备

使用备份设备适用于多种任务，如扫描设备以确认设备中的介质、通过指定虚拟锁名称锁定设备、执行计划的介质弹出、自动或手动清洗不洁驱动器、重命名备份设备以及响应装载请求以确认设备中有所需的介质。

Data Protector 还为设备和介质提供一组对设备和介质管理有益的高级选项，具体有哪些选项取决于设备类型。

此外，在同一库中可以使用多种驱动器类型，但必须了解所用介质的特性。

当某个设备因某种原因无法运行时，可以禁止使用该设备进行备份，并自动使用设备列表中另一个可用的设备。如果不想再使用某个设备，可以从 Data Protector 配置中将其删除。

## 设备和介质的高级选项

Data Protector 为设备和介质提供一组高级选项。是否有这些选项取决于设备类型。例如，用于配置库的选项比独立设备的选项多。

配置新设备时或更改设备属性时，可以设置这些选项。一般而言，这些选项适用于各自设备。还可以优化所列出的一组选项以适合特定的备份规范。一般而言，这些选项优先于为设备设置的选项。配置或更改备份规范时，可以访问这些选项。

有关高级选项的详细信息，请参见 **Data Protector** 帮助。

## 高级选项 - 设置

并发

### 选项

- **CRC 检查**
- **检测不洁驱动器**
- **基于驱动器的加密**
- **会话后弹出介质**
- **重新扫描**
- **使用直接库访问(特定于 SAN 的选项)**

## 高级选项 - 大小

- **块大小(KB)**
- **磁盘代理缓冲区**
- **段大小(MB)(S)**

## 高级选项 - 其他

### 装载请求

- **延迟(分钟)(D)**
- **脚本**

### 设备锁名称

- **使用锁名称**

## 有多种驱动器类型的库

在同一个库中可以使用多种相似技术的驱动器类型，如 **DLT 4000/7000/8000(DDS 系列中也是如此)**。如果要在任意驱动器中使用介质，但无法确保所有介质上都采用常用格式，则这可能会产生问题。例如，还原时 **DLT-4000** 无法读取用 **DLT-8000(最高密度)**写入的磁带。压缩和非压缩介质也无法互换使用。

通过设置相同的密度或为每个驱动器类型创建不同的介质池可以避免这些种类的问题。

## 相同的密度设置

此方法在所有介质上都使用一种常用格式，这种格式允许在任意驱动器中互换地使用所有介质。对于 **Windows** 系统中使用的设备，需要查看有关如何使用特定的写入密度的驱动

器文档。在 UNIX 系统上，创建设备文件名时或通过选择相关的设备文件名并在设备定义中使用这些设备文件名，可以设置驱动器的密度。必须将密度设置为相同的值。例如，在 DLT 4000 和 DLT 7000 的情况下，应设置 DLT 4000 密度。还必须确保所使用设备的块大小设置相同。必须在格式化介质时在设备定义中使用此设置。当所有介质的密度设置都相等时，还可以根据需要使用自由池。在还原期间，可以在任意驱动器中使用任意介质。

## 每个驱动器类型都有不同的介质池

此方法明确地将一组驱动器使用的介质与另一组驱动器使用的介质相隔离，从而可以更好地优化驱动器和介质的使用情况。可以对不同组的驱动器配置不同的介质池。这样可以对不同的驱动器类型使用不同的密度设置。例如，创建一个 DLT-4k-pool 和一个 DLT-8k-pool。必须在格式化介质时在设备定义中使用此设置。例如，必须由 DLT-8000 以最高密度设置格式化 DLT-8000-highest-density 的池中的介质。

### 自由池支持

不能用一个自由池“跨越”上述池。这样无法在设备中正确识别“其他”池中的介质，而是会将其视为陌生介质。在用不兼容的方式写入相同介质类型 (DLT) 时，自由池的概念仅适用于每种驱动器类型一个池(如 DLT-8k-pool)。还原期间，必须了解来自某个池的介质只能与相关设备配合使用。

## 关于扫描

扫描将检查插入驱动器中的介质的格式，显示设备存储库的内容，并更新 IDB 中的这些信息。

- 在独立设备中，扫描驱动器中的介质。
- 在带库设备中，扫描所选插槽中的介质。
- 在支持条码的带库设备中，扫描使用条码的介质。
- 在文件库设备中，更新 IDB 中有关文件仓库的相应信息。
- 对于 ADIC/GRAU DAS 或 STK ACS 库，Data Protector 将查询 ADIC/GRAU DAS 或 STK ACSLM Server，然后根据从服务器返回的信息同步 IDB 中的相应信息。

## 何时使用扫描

要更新有关设备中介质的 Data Protector 信息时即可扫描设备。如果手动更改介质的位置，则必须扫描设备。手动更改位置(插槽、驱动器)将使 IDB 中的信息产生不一致的现象，因为 Data Protector 无法获知手动更改。扫描将 MMDB 与所选位置(例如库中的插槽)实际存在的介质进行同步。

确保单元中所有介质的条码标签都唯一。如果在扫描期间检测到已有的条码，则以逻辑方式移动 IDB 中已有的介质。

如果已将一个文件仓库移至另一个位置，则在文件库设备中执行扫描。

## 限制

如果在存储库中对 ADIC/GRAU 库配置了多于 3970 个 volser，则无法成功完成 volser 扫描。解决此问题的方法是配置多个逻辑 ADIC/GRAU 库，以便将大型存储库中的插槽隔离为多个较小的存储库。

### 重要：

对于 ADIC/GRAU DAS 和 STK ACSL 库，当为同一个物理库配置了多个逻辑库时，建议不要查询 DAS 或 STK ACSL Server。请手动添加 volser。但是，对于 ADIC/GRAU DAS 库，当不使用 Data Protector 而使用 ADIC/GRAU DAS 实用程序配置逻辑库时，可以安全地在此类库上进行 Data Protector 查询操作。

## 驱动器清洗

Data Protector 提供了多种清洗不洁驱动器的方法：

- 库内置的清洗机构

某些磁带库具有一种功能，可在驱动器请求清洗磁头时自动清洗驱动器。库检测到不洁驱动器时，将自动加载清洗磁带，并且不向 Data Protector 通知此操作。这将中断任何活动的会话，从而导致其失败。由于这种由特定硬件管理的清洗过程与 Data Protector 不兼容，因此建议不要采用此过程。请改用由 Data Protector 管理的自动驱动器清洗。

- 由 Data Protector 管理的自动驱动器清洗

Data Protector 可使用清洗磁带自动清洗大多数设备。对于 SCSI 库和箱盒设备，可以定义在哪些插槽中放置磁头清洁磁带。不洁驱动器发送清洗请求，然后 Data Protector 使用清洗磁带清洗该驱动器。此方法可防止因驱动器不洁而使会话失败(前提是有合适的介质可用于备份)。支持条码的库和不支持条码的库都支持自动驱动器清洗。

- 手动清洗

如果未配置自动驱动器清洗，则需要手动清洗不洁驱动器。如果 Data Protector 检测到不洁驱动器，则会话监视器窗口中会显示清洗请求。然后您必须手动将清洗磁带插入驱动器中。

使用一种特殊的磁带清洗卡盒(含有略带摩擦性的磁带)清洗磁头。加载后，驱动器即识别这种特殊的磁带卡盒，然后开始清洗磁头。

## 限制

- Data Protector 不支持用诊断供应商的特殊 SCSI 命令通过在一个特殊的清洗磁带存放插槽中存放的清洗磁带执行驱动器清洗。无法使用普通的 SCSI 命令访问这些特殊的清洗磁带存放插槽，因此这些插槽无法用于由 Data Protector 管理的自动驱动器清洗。请配置标准插槽以存放清洗磁带。
- 磁头清洁磁带的检测和使用取决于运行介质代理的系统平台。有关更多信息，请参见《Data Protector 产品声明、软件说明和参考》。
- 如果配置由 Data Protector 管理的自动驱动器清洗，则不应使用另一种设备管理应用程序，因为这可能会导致意外的结果。这是因为读取 cleanme 请求时会清除此请求，具体取决于特定设备类型和供应商。

- 不支持用共享的清洗磁带自动清洗逻辑库的驱动器。需要为每个逻辑库都配置其特定的清洗磁带。

## 自动清洗的条件

- 在不支持条码的库中，**Data Protector** 设备定义中已配置了清洗磁带插槽，并且该插槽中含有清洗磁带卡盒。清洗磁带库插槽必须与其他库插槽一同进行配置。
- 在支持条码的库中，必须激活条码支持才能启用自动驱动器清洗。磁头清洁磁带的条形码标签以 CLN 作为其前缀，**Data Protector** 通过此标签可自动识别磁头清洁磁带条码。
- 所配置的驱动器启用了检测不洁驱动器选项。

**Data Protector** 收到驱动器需要清洗的通知时，将自动加载清洗磁带，清洗驱动器，然后恢复会话。所有清洁活动将记录在 **Data Protector** 服务器日志文件目录中的 `cleaning.log` 文件中。

## 计划的介质弹出

**Data Protector** 可以使用报告功能配合一个脚本执行计划的介质弹出。

必须在 **Cell Manager** 上创建程序或脚本才能执行弹出，并且还必须在 **Cell Manager** 上安装任何适用的解释程序。

可以设置和计划报告组，以使其创建报告，并将该报告作为输入发送给脚本。此类报告组应包括仅列出要弹出的介质的报告(例如，可以使用“介质报告”列表)。启动报告组(作为日程计划或“结束会话”等通知的结果)后，**Data Protector** 将启动脚本，并使用报告结果作为输入。脚本通过使用 **Data Protector omnimm CLI** 命令，分析报告并执行所指定介质的弹出。

默认情况下，如果需要从邮件插槽中取出介质，以使弹出操作可以继续(例如，如果要弹出的介质多于库中的空邮件插槽)，则将在事件日志查看器中通知您。如果在默认时间过后没有从邮件槽中取出介质，并且仍有介质要弹出，则 **omnimm** 命令将中止该操作。可以在 **omnirc** 文件中更改默认的时间跨度。

## 设备锁定

通过将设备配置为不同的设备名称，即可多次为同一物理设备配置不同特征。因此，可以将一个物理设备配置为多个 **Data Protector** 备份设备，并且一个设备即可用于多个备份会话。内部锁定逻辑设备可防止两个 **Data Protector** 会话同时访问相同的物理设备。例如，如果一个备份会话正在使用某个特定设备，则所有其他备份/还原会话必须等待此设备空闲，然后再开始使用此设备。开始备份或还原会话时，**Data Protector** 将锁定用于该会话的设备、驱动器和插槽。

执行介质操作(如初始化、扫描、验证、复制或导入)的介质会话也会锁定设备。在此期间，没有其他操作可以锁定和使用该设备。如果介质会话无法获取锁定，则操作失败，必须以后重试操作。

备份或还原会话发出装载请求时将释放锁定，从而使您只能执行介质管理操作。仍将保留设备，以使任何其他备份或还原会话都不能使用设备。此外，首次介质操作期间不允许在同一驱动器上进行其他介质管理操作。确认装载请求后，备份或还原会话将再次锁定设备，并继续会话。

由于内部锁定在逻辑设备上而非物理设备上进行，因此如果在一个备份规范中指定一个设备名称，而在另一个备份规范中对同一物理设备指定另一个设备名称，则会发生冲突。根据备份计划，**Data Protector** 可能会尝试同时在若干备份会话中使用同一物理设备，这样可能会导致冲突。在其他操作(如备份和还原、备份和扫描等等)中使用两个设备名称时也可能发生此情况。要防止 **Data Protector** 可能尝试同时在若干备份会话中使用相同物理设备时发生冲突，请在设备配置中指定虚拟锁名称。然后，**Data Protector** 使用此锁名称检查设备是否可用，从而防止冲突。对于同一物理设备，必须在所有备份设备配置中使用相同的锁名称。

**注意：**

“设备流”报告中有关物理设备的信息取自当前配置的设备，并且可能与实际使用该设备时的相应信息不同(例如，最近更改了设备逻辑名称，但内部数据库中的某些会话仍然包含以前的设备名称)。

“设备流”报告始终显示当前信息 - 含当前逻辑设备名称的当前物理表示形式。

## 禁用备份设备

### 手动禁用备份设备

如果禁用某个备份设备，则所有后续备份都跳过该设备。如果已选择负载均衡，则改用备份规范的设备列表中定义的下一个可用设备。还会禁用与已禁用设备使用相同锁名称的所有设备。

这样您可以避免备份因设备受损或处于维护模式而失败，同时使其他设备可用于(和配置为)备份。

设备受损或处于维护模式时禁用备份设备很有用。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。此时将在结果区域中显示所配置设备的列表。
3. 右键单击要禁用的设备，然后单击 **属性**。
4. 单击 **设置** 选项卡，然后选择 **禁用设备** 选项。
5. 单击 **应用**。

此时即禁用设备。要允许设备进行备份，请取消选中 **禁用设备** 选项。

### 自动禁用备份设备

可以配置 **Data Protector** 以自动禁用已发生一定数量未知错误的设备。该阈值可以通过将 `SmDeviceErrorThreshold` 全局选项设置为 `SmDeviceErrorThreshold=MaxNumberOfUnknownErrors` 来确定。

要在对设备做出安排后允许该设备进行备份，请右键单击该设备，然后单击 **启用设备**。

## 重命名备份设备

重命名备份设备时，该设备不再以其旧名称用于备份或还原。

**重要：**

请确保从使用该设备的所有备份规范中删除了该设备的旧名称。否则，Data Protector 将尝试备份到不存在的设备或从该设备还原，并因此会话将失败。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。此时将在结果区域中显示所配置设备的列表。
3. 右键单击设备的名称，然后单击 **属性**。
4. 在“常规”属性页中，修改“设备名称”文本框中的名称。
5. 单击 **应用**。

此时所配置设备的列表中将以新名称显示该设备。

## 删除备份设备

从 Data Protector 配置中删除备份设备时，该设备就不再用于备份或还原。

**重要：**

请确保从使用该设备的所有备份规范中删除了该设备的旧名称。否则，Data Protector 将尝试备份到不存在的设备或从该设备还原，并因此会话将失败。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。此时将在结果区域中显示所配置设备的列表。
3. 右键单击要删除的设备，然后单击 **删除**。确认操作。

此时即从所配置设备的列表中删除了该设备。

**提示：**

如果不再将某个备份设备与 Data Protector 配合使用，则可能要从系统中删除介质代理软件组件。可使用“客户机”上下文完成此操作。

## 响应装载请求

对装载请求作出响应可确认所需的介质位于设备中。必须了解如何选择介质进行备份。

### 先决条件

您必须已经添加到 Admin 用户组中，或者获得了“监视”用户权限。

## 步骤

1. 在上下文列表中，选择**监视**。
2. 将所需的介质插入设备中。如果有库设备，则不必使用由装载请求所请求的插槽。
3. 在结果区域中，双击含有装载请求状态的会话以显示有关会话的详细信息。
4. 选择具有装载请求状态的设备。
5. 在**操作**菜单中，选择**确认装载请求**，或右键单击含有装载请求状态的设备，然后选择**确认装载请求**。

此时会话和设备的状态变为“正在运行”。

## 关于存储区域网络 (SAN)

### 什么是 SAN？

存储区域网络 (SAN) 是专用于数据存储的网络，以高速光纤通道技术为基础。通过 SAN 可进行从应用程序服务器到某个单独网络的卸载存储操作。Data Protector 支持此技术，使多个主机可以共享通过 SAN 连接的存储设备，从而形成多系统对多设备的连接。通过多次定义同一物理设备达到此目的，例如，在需要访问该设备的每个系统上都定义一次。

在 SAN 环境中使用 Data Protector 时，必须考虑以下几点：

- 每个系统都可以有其(伪)本地设备，但通常都在若干系统之间共享设备。这一点适用于单独的驱动器以及库中的机械手。
- 必须小心谨慎，以防多个系统同时写入相同设备。需要在所有系统之间同步对设备的访问。使用锁定机制实现这一点。
- SAN 技术对于管理多个系统中的库机械手是一种极好的方式。只要发送到机械手的请求在所涉及的全部系统之间同步，这种方式就能直接管理机械手。

### FC-AL 和 LIP

在光纤通道仲裁环路 (FC-AL) 中使用磁带设备可能会导致一些有可能中止备份会话的异常现象。出现此问题是因为只要连接/断开新 FC 链路以及只要重新引导连接到 FC-AL 的系统，FC-AL 就会执行环路初始化协议 (LIP)。FC-AL 的这种重新初始化将使正在运行的备份中止。应重新启动此类被终止的作业。

FC-AL 环路上发生 LIP 时，任何具有活动 I/O 进程的实用程序都会出现 I/O 错误。对于尝试使用共享磁带的备份实用程序，I/O 错误会导致当前备份会话失败：

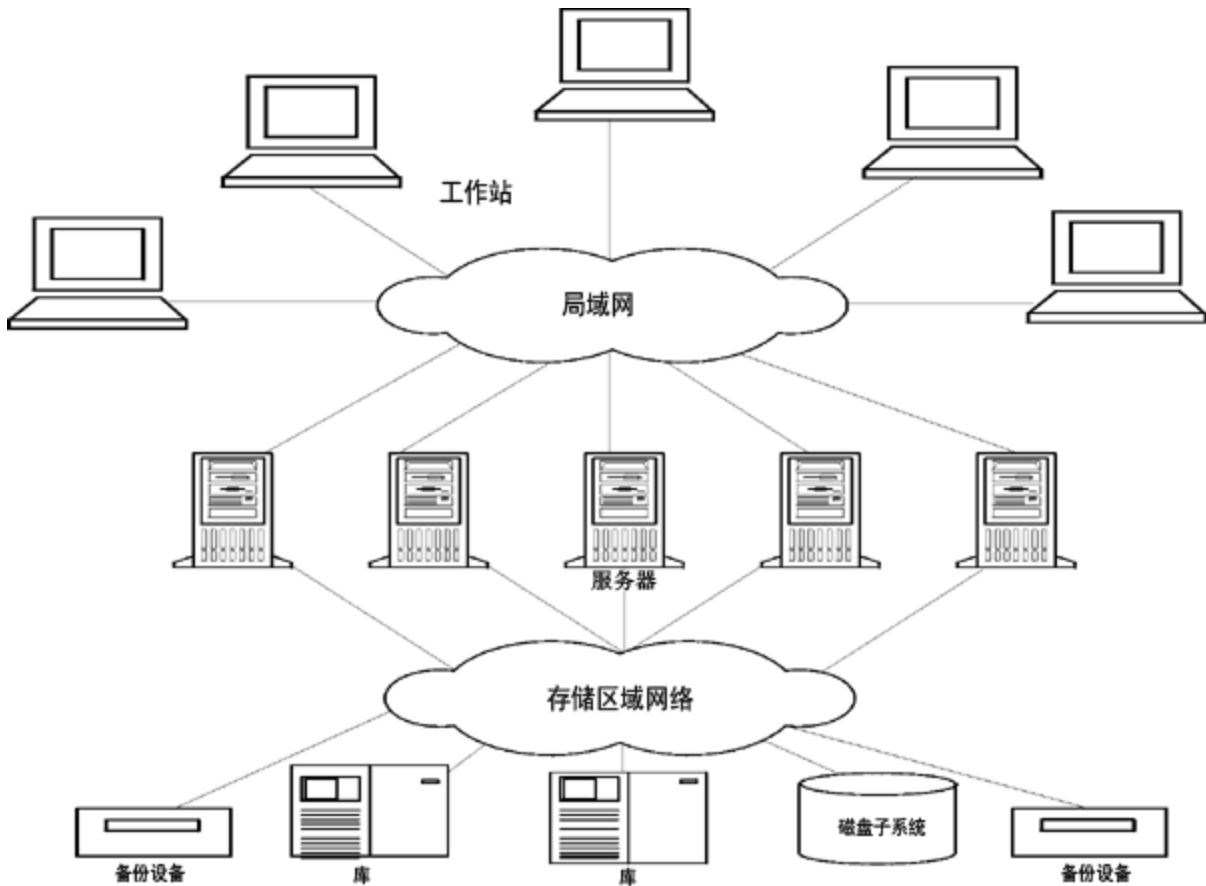
- 倒回和卸载磁带
- 备份会话中止

建议采取以下措施：

- 备份会话正在运行时，不要添加新设备或从仲裁环路取下设备。
- 备份会话正在运行时，不要接触 FC 组件。静电会导致 LIP。
- 不要使用 Windows 中的 discovery 或 HP-UX 系统中的 ioscan，因为这些命令也会导致 LIP。



### SAN 中多系统对多设备的连接示例



## SAN 环境中的设备锁定

Data Protector 支持 SAN 概念，使多个系统能够共享 SAN 环境中的备份设备。相同设备可由多个应用程序共享。该设备还可由 Data Protector 环境中的多个系统共享。锁定的用途是确保一次只有一个系统与在若干系统之间共享的设备进行通信。

### 锁定 Data Protector 专用的设备

如果只有 Data Protector 这一个应用程序使用驱动器，但需要从若干系统中使用这个驱动器，则可以使用设备锁定机制。

如果 Data Protector 是若干系统中唯一一个使用机械手控制的应用程序，则 Data Protector 从内部处理这种情况，假定库控制位于与需要控制它的所有系统相同的单元中。在这种情况下，由 Data Protector 内部控制管理对设备访问的所有同步。

### 锁定由多个应用程序使用的设备

如果多个系统正在使用 Data Protector 访问同一物理设备，则必须使用设备锁定机制。

如果 **Data Protector** 和至少一个其他应用程序要从几个系统中使用相同设备，则每个应用程序都必须使用相同(常规)的设备锁定机制。此机制必须在若干应用程序中都正常发挥作用。**Data Protector** 当前不支持此模式。如果必须这样，则操作规则必须保证一次只从一个应用程序中独占访问所有设备。

## 间接和直接库访问

配置具有 **SCSI** 库设备或 **silo** 库 (**ADIC/GRAU** 和 **StorageTek**)的 **Data Protector** 时，有以下两种方式可供客户机系统访问库机械手：

### 间接库访问

间接库访问时，只有一个系统(默认机械手控制系统)发送从 **Data Protector** 发起的机械手控制命令。任何其他请求机械手功能的系统将请求转发到机械手控制系统，此系统随后将实际命令发送到机械手。在 **Data Protector** 中为所有来自 **Data Protector** 的请求透明完成此操作。

### 直接库访问

直接库访问时，每个系统都直接向库机械手发送控制命令。因此，每个系统都不依赖于任何其他系统即可发挥作用。

由于直接库访问时有多个系统向同一个库发送命令，因此必须协调此通信的顺序。

在 **Data Protector** 中，每个库定义都与控制库机械手的主机关联(默认情况下)。如果另一个主机请求移动某个介质，则 **Data Protector** 将首先访问库定义中指定的系统以执行介质移动。如果该系统不可用，并且设置了 **libtab** 文件，则可以从本地主机直接访问库机械手。所有这些都在 **Data Protector** 中透明完成。

如果为多路径设备启用了直接库访问功能，则无论配置了什么顺序，都会首先使用本地路径(目标客户机上的路径)进行库控制。对多路径设备忽略 **libtab** 文件。

## 配置 SAN 环境中的设备

**SAN** 环境的规模可以从一个客户机使用一个库到若干客户机使用若干库不等。客户机可以采用不同的操作系统。从 **Data Protector** 的角度看，配置 **SAN** 环境的目标是：

- 在要共享库机械手的每个主机上，为每个主机创建一个库机械手。如果只有一个主机控制机械手，则仅为默认的机械手控制主机创建库定义。
- 在要参与共享库中同一(磁带)驱动器的每个主机上：
  - 为要使用的每个设备都创建设备定义。
  - 如果另一个主机也将使用(物理)设备(共享设备)，则使用锁名称。
  - (可选)如果要使用直接访问，则选择此功能。如果使用此功能，请确保在该主机上设置了 **libtab** 文件。

## 注意事项

- **Microsoft 群集服务器**：确保两个群集节点上的驱动器硬件路径相同：配置设备后，即执行故障转移核实这一点。

## 配置方法

有三种配置方法，具体采用哪一种取决于参与 SAN 配置的平台：

## 使用 GUI 自动配置设备

可以使用 **Data Protector** 自动配置功能在 SAN 环境中的多个主机上自动配置设备和库。以下操作系统中提供自动配置功能：

- Windows
- HP-UX
- Solaris
- Linux
- AIX

## 限制

自动配置无法用于配置 SAN 环境中的以下设备：

- 混合介质库
- DAS 或 ACSLS 库
- NDMP 设备

**Data Protector** 可发现连接到环境的备份设备。对于库设备，**Data Protector** 确定插槽数、介质类型和属于库的驱动器。然后，**Data Protector** 设置逻辑名称、锁名称、介质类型、设备的设备文件或 SCSI 地址以及驱动器和插槽，从而配置设备。

### 注意：

将新主机引入 SAN 环境中时，将不自动更新所配置的库和设备。

- 要在新主机上使用现有的库，请删除此库，并在新主机上配置一个同名的新库。
- 要将设备添加到现有的库，或者删除该库，然后在新主机上自动配置一个同名的新库以及新驱动器，或者手动将驱动器添加到库中。

## 使用 CLI 自动配置设备(sanconf 命令)

可以使用 **sanconf** 命令配置 SAN 环境中的设备和库。**sanconf** 命令是一个实用程序，使用它可以更轻松地配置单个 **Data Protector** 单元的 SAN 环境中以及具有集中式介质管理数据库 (CMMDB) 的 MoM 环境中的库。它通过从多个客户机收集有关驱动器的信息并将这些驱动器配置为一个库，可自动配置 SAN 环境中的库。在 MoM 环境中，**sanconf** 还可以配置使用 CMMDB 的任何 **Data Protector** 单元中的任何库(如果运行 **sanconf** 的单元使用 CMMDB)。以下操作系统中提供 **sanconf**：

- Windows
- HP-UX
- Solaris

sanconf 可以检测和配置连接到在以下操作系统中运行的客户机的受支持设备：

- Windows
- HP-UX
- Solaris
- Linux
- AIX

使用此命令，可以：

- 扫描指定的 **Data Protector**，同时收集有关连接到 **SAN** 环境中客户机的驱动器和机械手的 **SCSI** 地址的信息。
- 使用在扫描 **Data Protector** 客户机期间收集的信息，配置或修改给定客户机的库或驱动器的设置。
- 从库中删除所有或指定客户机上的驱动器。

## 设备锁定

sanconf 命令自动为配置的驱动器创建锁名称。锁名称由驱动器供应商 ID 字符串、产品 ID 字符串和产品序列号组成。

例如，供应商 ID 为“HP”、产品 ID 为“DLT8000”和序列号为“A1B2C3D4E5”的 DLT8000 驱动器的锁名称将为 HP:DLT8000:A1B2C3D4E5。

还可以手动添加锁名称。锁名称对于每个逻辑设备都是唯一的。

不得更改由 sanconf 命令创建的锁名称。手动创建并且表示已由 sanconf 配置的物理驱动器的所有其他逻辑驱动器也必须使用由 sanconf 创建的锁名称。

## 限制

- 有关通过 sanconf 支持的库的完整列表，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新支持矩阵。
- sanconf 不提供以下功能：
  - 将备用驱动器放入驱动器插槽中。
  - 混合驱动器类型；例如，DLT、9840 和 LTO 驱动器的组合。
  - 配置当前不可用的客户机。只有在使用包括通过扫描客户机收集的信息的配置文件执行库的配置时，才能配置此类客户机。

## 建议

对于系统中的特定设备仅配置一个驱动程序。

有关如何使用 `sanconf` 命令的信息，请参见 `sanconf` 手册页或 **Data Protector** 命令行界面参考。

## 在 UNIX 系统中手动配置

手动配置 SAN 环境中连接到 UNIX 系统的共享设备时，必须：

- 为要使用的每个设备都创建设备定义。
- 使用锁名称。
- (可选)如果要使用直接访问，则选择此功能。如果这样做，则必须确保正确配置了该主机上的 `libtab` 文件。

## 阶段

1. 手动配置设备
2. 手动配置 `libtab` 文件

## 关于备份到磁盘

**Data Protector** 备份到磁盘可将数据保存到磁盘而非磁带。**Data Protector** 写入位于一个或多个磁盘上的目录。将数据写入位于磁盘上目录中的文件。

磁盘备份比备份到磁盘速度快，因为无须执行任何机械过程(如加载磁带)即可进行备份。此外，磁盘存储正在变得日益廉价。

许多处理业务关键数据的应用程序都需要在完成每个事务后即备份该事务。基于磁盘的备份意味着可以在整个工作日不断写入磁盘。

## 什么是基于磁盘的备份设备？

概念上，基于磁盘的备份设备类似于磁带驱动器或磁带堆栈。此类设备有一个或多个目录，等同于磁带驱动器中的存储库。正在进行备份时，基于磁盘的备份设备将数据写入文件仓库，如同这些仓库将文件写入磁带一样。由于基于磁盘的备份设备将数据写入位于磁盘上的文件，因此这些设备也称为“文件设备”。

## 如何配置基于磁盘的设备？

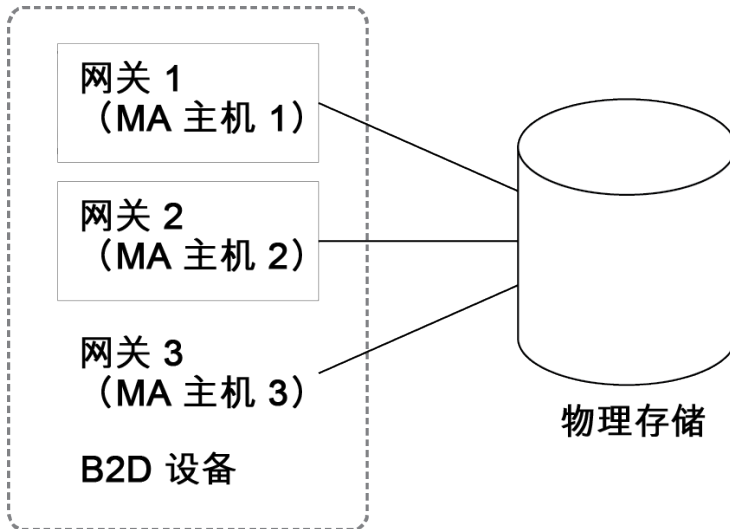
使用 **Data Protector** GUI 配置基于磁盘的备份设备。这些设备使用所有 **Data Protector** 介质管理以及备份和还原设施。

## 关于备份到磁盘设备

备份到磁盘 (B2D) 设备是将数据备份到物理磁盘存储的设备。B2D 设备支持多主机配置。这表示可以通过多个主机(称为网关)访问单个物理存储。每个网关都表示一个安装有介质代理组件的 **Data Protector** 客户机。物理存储还可以分区为表示特定存储部分的各个存储区(这类似于对硬盘进行分区)。物理存储上的每个存储区只能通过一个 B2D 设备进行访问。但是，多个 B2D 设备可以访问相同物理存储上的不同存储区。

尽管类似于其他基于库的设备，但是 **B2D** 设备的行为方式不同，因为网关可实现更大灵活性。与库驱动器不同，每个网关都表示一个主机，在该主机上可以同时启动多个介质代理(采用单个或多个会话)。

#### **B2D 设备(逻辑视图)**



可以在特定网关上启动的介质代理数由以下各项定义：

- 网关限制。每个 **B2D** 网关都受限于最大数量的并行流。
- 存储区上的连接限制。配置 **B2D** 设备时，在 **GUI** 中指定此限制。如果该值保留为未选中状态，则 **Data Protector** 使用可用的最大值。
- 物理存储单元的物理连接限制。此值从物理存储区检索得到。
- 根据当前操作，每个 **Session Manager** 会尝试针对以下输入参数平衡网关上的介质代理数：
  - 要备份的对象数
  - 对象位置
  - 物理连接限制。

**B2D** 设备使用特殊数据格式进行快速读/写访问，这与传统 **Data Protector** 磁带格式不兼容。该数据格式会在您选择 **B2D** 设备时自动设置。

## 关于重复数据删除

重复数据删除是一种数据压缩技术，通过不备份重复数据来减小备份数据的大小。重复数据删除过程将数据流分割为可管理的数据区块(或块)。这些数据区块的内容随后会相互进行比较。如果发现相同区块，则会将它们替换为指向唯一区块的指针。换句话说，如果发现 **20** 个相同区块，则只保留(并备份)一个唯一区块，其他 **19** 个区块都会替换为指针。备份数据会写入基于磁盘的目标设备(称为重复数据删除存储)。进行还原操作时，唯一区块会进行复制并插入指针所指示的正确位置。对于重复数据删除类型的还原操作，还原过程有时称为备份数据的“再水合”。

## 何时使用重复数据删除功能

通常，在备份可能包含同一个 1 MB 图形文件附件的 100 个实例的电子邮件系统时，会使用重复数据删除。如果该系统是使用传统备份技术备份的，则该附件的所有 100 个实例都会进行备份。这需要大约 100 MB 的存储空间。但是，借助重复数据删除，实际上只存储该附件的一个实例。所有其他实例都引用到存储的唯一副本。在此示例中，重复数据删除率大约为 100:1。虽然此示例称为文件级别重复数据删除，但是可用于演示使用备份到磁盘设备和重复数据删除的优点。

## 重复数据删除功能的优点

通常，重复数据删除可提高备份服务的整体速度并降低总存储成本。重复数据删除可显著减少所需磁盘存储空间量。因为重复数据删除是基于磁盘的系统，所以还原服务级别要高得多，会减少磁带(或其他介质)处理错误。

## 重复数据删除技术

市场上提供了多种重复数据删除技术。这些技术通常分为基于硬件的解决方案和基于软件的解决方案。这些解决方案可以进一步细分，例如分为文件级别(单实例化)或块级别重复数据删除。

Data Protector 以下重复数据删除后端：

### StoreOnce 软件重复数据删除

Data Protector 的 StoreOnce 软件重复数据删除提供基于软件的块级别重复数据删除解决方案。

使用 StoreOnce 软件重复数据删除时，请注意以下事项：

- 重复数据删除仅备份到基于磁盘的设备。它不能用于可移动介质，如磁带驱动器或库。
- 因为 Data Protector 使用仅限软件的方法进行重复数据删除(即，使用 StoreOnce 软件重复数据删除时)，所以除了标准硬盘，无需特定硬件来存储备份数据。
- StoreOnce 软件重复数据删除使用基于哈希的分块技术，将数据流分割为可调大小的数据区块。
- 在重复数据删除过程中，重复数据会删除，仅存储数据的一个副本，以及指向唯一副本的引用链接。重复数据删除能够减少所需存储容量，因为仅存储唯一数据。
- 在备份规范中指定备份到磁盘目标设备可告知 Data Protector 执行重复数据删除类型备份。

### StoreOnce 备份系统设备

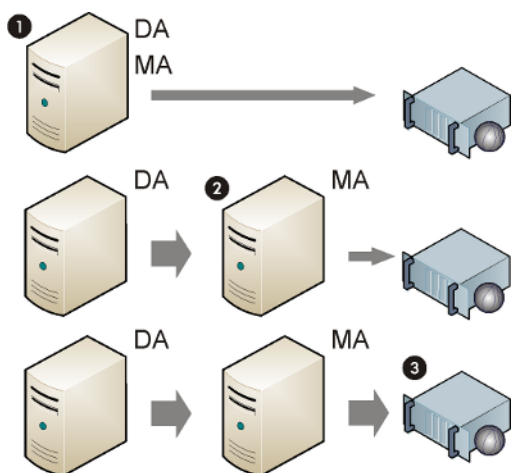
StoreOnce 备份系统设备是支持重复数据删除的磁盘到磁盘 (D2D) 备份设备。

## 重复数据删除设置

Data Protector 支持各种重复数据删除设置：

- 源端重复数据删除 (1)—数据在源端(备份的系统)进行重复数据删除。
- 服务器端重复数据删除 (2)—数据在介质代理系统(网关)上进行重复数据删除。
- 目标端重复数据删除 (3)—数据在目标设备(StoreOnce 备份系统或 StoreOnce 软件系统)上进行重复数据删除。

### 重复数据删除设置



### 源端重复数据删除

对于源端重复数据删除 (1)，介质代理会与 磁盘代理一起安装在进行备份的客户机上，因而客户机成为网关(源端网关)。重复数据删除由介质代理在客户机自身上执行，因此只有删除了重复数据的数据才会发送到目标设备，从而可减少总体网络流量。并发流的数量受限于负载均衡设置。在介质代理完成本地对象备份之后，新的介质代理会在下一个客户机系统上启动。请注意，备份的系统必须支持重复数据删除。

### 服务器端重复数据删除

对于服务器端重复数据删除，重复数据删除由介质代理在单独的介质代理客户机(网关)上执行。这样可减少备份的系统和目标设备上的负载，但是不会减少磁盘代理与介质代理之间的网络流量。

请注意，介质代理客户机必须支持重复数据删除。服务器端重复数据删除使您可以从本地不支持重复数据删除的客户机进行重复数据删除。

### 目标端重复数据删除

重复数据删除过程在目标设备上进行。它从安装在客户机(网关)上的介质代理接收要备份的数据。目标端重复数据删除不会减少介质代理与重复数据删除系统之间的网络流量。

## 关于文件库设备

文件库设备是位于由您定义的内部或外部硬盘驱动器上某个目录中的一种设备。文件库设备由一组目录组成。向该设备进行备份时，将自动在这些目录中创建文件。文件库目录中包含的文件称为文件仓库。



**Data Protector** 设置的文件库设备没有最大容量。设备大小的唯一限制由目录所在文件系统的最大大小决定。例如，**Linux** 中运行的文件库设备的最大大小将是可以在文件系统中保存的最大大小。

首次配置文件库设备时，要指定该设备中每个文件仓库的容量。使用设备期间随时都可以使用文件库属性重置文件仓库的调整大小属性。

文件库设备可以位于本地或外置硬盘驱动器上，只要 **Data Protector** 了解其路径即可。配置文件库设备时要指定路径。

## 如何维护基于磁盘的设备？

如果所使用的所有基于磁盘的设备都已装满，则在继续用该设备进行备份之前，将需要执行以下操作之一：

- 开始将数据移至磁带，以释放文件设备或一个或多个文件插槽。
- 循环回收文件仓库。
- 向文件设备添加新文件仓库。

## 文件仓库

文件仓库是包含从备份到文件库设备的数据的那些文件。

## 创建文件仓库

使用文件库设备启动第一个备份时，**Data Protector** 在设备中自动创建文件仓库。**Data Protector** 为使用该设备进行的每个数据备份会话创建一个文件仓库。如果要备份的数据量大于默认最大文件仓库大小，则 **Data Protector** 将为一个备份会话创建多个文件仓库。

## 文件仓库名称

每个文件仓库的名称都是由系统自动生成的一个唯一标识符。

**Data Protector** 还向文件仓库添加一个介质标识符。这样将文件仓库标识为介质池中的介质。添加到介质的标识符有助于在执行还原时标识特定的备份会话。查看文件仓库属性时，可以看到该标识符。

请注意，如果已回收文件仓库，则尽管文件仓库图标在 **GUI** 中仍可见，但文件仓库名称可能从 **GUI** 中消失。

## 文件仓库大小

最初创建文件库设备时定义文件仓库的大小。在此过程中，要指定该设备的所有大小属性，包括文件仓库的最大大小。文件仓库的大小属性尽管仅输入一次，但适用于全局的每个文件仓库。如果在一个会话中要备份的数据大小大于最初指定的文件仓库大小，则 **Data Protector** 自动创建更多文件仓库，直到为文件库设备分配的磁盘空间用尽为止。

默认文件仓库大小为 **5 GB**。可以增加此值(最多 **2 TB**)，但性能可能会降低一些。

## 文件仓库空间消耗

**Data Protector** 自动创建文件仓库，直到对于设备没有磁盘空间可用为止。最初设置设备时，在设备属性中定义必须为文件库设备保持可用的空间量。

## 磁盘已满处理

如果对文件库设备可用的总磁盘空间低于用户指定的水平，则发出通知。

## 每个磁盘的设备数

文件库设备可以包括一个或多个目录。但只有一个目录可以位于文件系统上。

在文件仓库位于多个磁盘上的情况下，建议不要将来自两个不同文件库设备的文件仓库放置在一个磁盘上。这是由于如果属性不同，可能会在 **Data Protector** 中产生冲突(例如，如果在一个文件库设备上将文件仓库的剩余磁盘空间指定为 **20 MB**，而在其他文件库设备上指定为 **10 MB**)。

## 设置文件库设备属性

可以在文件库设备初始配置期间设置文件库设备属性，也可以在设备运转之后更改这些属性。

## 属性初始设置

### 步骤

1. 在文件库设备配置期间，选择文件库设备目录，然后单击**属性**。
2. 指定设备的大小属性。单击**确定**。
3. 单击**下一步**，并继续配置文件库设备。

## 更改设备属性

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，然后单击要更改的文件库设备的名称。
3. 右键单击文件库设备名称，然后单击**属性**。
4. 单击**存储库**选项卡。在列表中选择文件库路径。
5. 单击**属性**。指定设备的所有大小属性，单击**确定**。

更改设备属性之后，**Data Protector** 将“属性”对话框中指定的属性应用于文件库设备中创建的每个文件仓库。后续设备属性更改之前创建的任何文件仓库的属性将不受影响。

## 删除文件库设备

文件库设备不得包含任何受保护数据，然后才能删除该设备。这意味着必须更改文件库中包含的每个文件仓库的数据保护级别，然后才能删除该设备。

### 删除阶段

1. 检查数据保护
2. 回收文件仓库
3. 删除导出的文件仓库图标
4. 删除文件库设备

### 检查数据保护

#### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，选择要删除的文件库设备的名称，并打开该文件库中的“目录”文件夹。
3. 在结果区域中找到“保护”列。检查哪些文件仓库的保护级别为永久。

### 回收文件仓库

通过回收和删除文件仓库或整个文件库设备，可释放磁盘空间。

可以循环回收单独的文件仓库或文件库中的所有文件仓库。这意味着可以在下一次备份中恢复和使用由回收项占据的磁盘空间。通过删除不受保护的文件仓库和创建新文件仓库可达到此目的。

#### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开文件库设备的文件仓库。
3. 在结果区域中，通过单击单独的仓库，选择要循环回收的文件仓库。
4. 右键单击所选的仓库，然后单击 **导出**。  
导出文件仓库将可从 IDB 删除有关该文件仓库的信息。Data Protector 不再识别存在文件仓库。但仍保留仓库信息，如果需要恢复文件仓库，则以后还可以导入这些信息。
5. 右键单击所选仓库，然后单击 **回收**。
6. 对文件库中数据保护级别为“完整”的每个文件仓库重复此操作。

将文件仓库标为回收后，由 Data Protector 为其自动生成的名称即消失，而只有文件仓库图标在 Data Protector GUI 中可见。可以删除导出的文件仓库图标。

### 删除导出的文件仓库图标

导出文件仓库后，其名称即消失，而只有仓库图标在 Data Protector Manager 中可见。

## 步骤

1. 在结果区域中，选择要删除的图标。
2. 右键单击所选图标，然后单击**删除**。
3. 对每个要删除的导出文件仓库图标重复此操作。

这样将从 GUI 删除图标，但不会从 IDB 中物理删除该文件。

## 删除文件库设备

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，选择要删除的文件库设备的名称。
3. 右键单击该文件库设备，然后单击**删除**。

现在将从 IDB 中删除该文件库设备。

## 关于介质库设备

### 介质库物理设备

介质库是一种库设备。它可以包含光盘或文件介质。如果设备用于容纳文件介质，则将其称为文件介质库设备。在初始配置期间定义设备将容纳的介质类型。如果要在 UNIX 上运行光盘介质库，则需要为每个交换器插槽或盘面配置一个 UNIX 设备文件。

### 介质库文件设备

文件介质库设备在逻辑上等同于磁带堆栈。它包含多个插槽，初始设备配置期间用户定义其大小。手动配置此设备。使用文件介质库时，可更改该属性。如果用于包含文件介质，则该设备写入磁盘而非磁带。文件介质库设备以文件的形式保存数据；每个此类文件都等同于磁带设备中的一个插槽。

此设备的最大建议数据存储容量仅由正在运行文件介质库的操作系统在文件系统中所能存储的数据量限制。文件介质库设备中每个插槽的最大容量为 2 TB。但是，通常建议将插槽大小对于 Windows 保持在 100 MB 到 50 GB 之间(在 Windows 系统上)，对于 UNIX 保持在 100 MB 到 2 TB 之间(在 UNIX 系统上)。例如，如果有 1 TB 数据要备份，则可以采用以下设备配置：

**Windows 系统：**1 个文件介质库设备，其中具有 100 个文件插槽，每个插槽 10 GB

**UNIX 系统：**1 个文件介质库设备，其中具有 250 个文件插槽，每个插槽 4 GB

要提高介质库文件设备的性能，建议每个磁盘仅有一个设备，并且每个设备仅有一个驱动器。还应避免 Data Protector 正在备份/还原时其他应用程序从磁盘传输大量数据或将大量数据传输到磁盘。

## 建议对于 Windows 和 UNIX 采用的插槽大小

可用磁盘空间	插槽数	插槽大小
1 TB	100	10
5 TB	250	20
10 TB	250	40

## 如何维护文件介质库设备？

如果所使用的所有文件介质库设备都已装满，则在继续用该设备进行备份之前，将需要执行以下操作之一：

- 开始将数据移至磁带，以释放文件设备或一个或多个文件插槽。
- 循环回收介质库插槽。
- 向文件设备添加新的介质库插槽。

## 配置文件介质库设备

建议将所创建的设备置于 IDB 所在磁盘以外的磁盘上。这样可确保有足够的磁盘空间供数据库使用。将设备数据库和 IDB 放置在不同的磁盘上还能提高性能。

## 配置文件介质库设备

**重要：**

请考虑以下几点：

- 请勿使用现有设备的名称配置这些设备，因为现有设备将被覆盖。
- 请勿使用相同的设备名称用于配置多个设备，因为每次访问设备时都会覆盖设备名称。

## 先决条件

- 在 Windows 系统中，必须对要用作设备的文件禁用 Windows 压缩选项。
- 必须已在磁盘上创建设备所在的目录，然后再创建设备。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，右键单击**设备**，然后单击**添加设备**以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明(可选)。
5. 在“设备类型”列表中，选择**介质库**设备类型。

6. 在“客户机”列表中，选择客户机的名称。
7. 在“管理控制台 URL”文本框中，输入库管理控制台的有效 URL 地址(可选)。
8. 单击**下一步**。
9. 为介质库指定一组文件/磁盘。使用短划线一次输入多个文件或磁盘(例如 /tmp/FILE 1-3)，然后单击**添加**。对于磁光盘介质库，磁盘名称必须以 A/a 或 B/b 结尾。单击**下一步**。
10. 在“介质类型”列表中，对要配置的设备选择**文件**。
11. 单击**完成**退出此向导。此时将提示您配置库驱动器。单击**是**，然后将显示驱动器配置向导。

## 配置文件介质库设备中的驱动器

### 步骤

1. 在“设备名称”文本框中，输入设备的名称。
2. 在“说明”文本框中，输入说明(可选)。
3. 指定所选介质类型的介质池。可以从“介质池”列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。可以对所有驱动器配置一个介质池，也可以对每个驱动器都配置一个独立的介质池。单击**下一步**。
4. (可选)选择**设备可用于还原和/或设备可用作进行对象复制的源设备**，并指定**设备标记**。
5. 单击**完成**退出向导。

此时所配置驱动器的列表中将显示该驱动器的名称。可以扫描驱动器以验证配置。

## 回收文件介质库插槽

对文件介质库中的每个文件插槽都设置了数据保护，因此通过将其保护设置为**无**可以循环回收单个插槽。因此，拥有多个小型插槽可以提高灵活性，并使数据保护和空间保留管理更高效。回收文件介质库设备中的插槽将去除其数据保护，这样即可重新使用插槽进行备份。后续的备份会话中将覆盖插槽中的数据。

#### **重要：**

如果使用此方法，则介质上的现有数据将被覆盖并丢失。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开文件介质库设备插槽。
3. 在结果区域中，选择要循环回收的插槽。
4. 右键单击所选插槽，然后单击**回收**。

## 关于独立设备

### 独立物理设备

独立设备是包含一个驱动器的简单设备，该驱动器一次从一个介质读取或写入一个介质 (如 DDS 或 DLT)。这些设备用于小规模备份。介质充满后，操作员必须手动将其替换为新介质，备份才能继续。因此，独立设备不适合大规模的无人看管备份。

### 独立文件设备

独立文件设备是指定目录中的一个文件，您向该文件备份数据而非写入磁带。此设备以文件的形式保存数据；每个此类文件都等同于磁带设备中的一个插槽。独立文件设备适用于较小的备份。

文件设备的最大容量为 2 TB。但是，通常建议将独立文件设备大小对于 Windows 系统保持在 100 MB 到 50 GB 之间，对于 UNIX 系统保持在 100 MB 到 2 TB 之间。Data Protector 从不测量文件系统上的可用空间量；对于文件大小限制，它采用默认或指定容量。对于文件设备不能使用压缩文件。可以通过设置 FileMediumCapacity 全局选项来更改默认文件大小。

独立文件设备的默认最大大小为 100 MB。如果想备份更大的独立文件设备，则可以通过设置 FileMediumCapacity 全局选项来更改默认文件大小。有关设置全局选项的详细信息，请参见[自定义 Data Protector 全局选项](#)或[通过编辑全局文件自定义全局选项](#)。

例如，为 20GB (20Gb = 20000 MB) 的最大容量设置如下 FileMediumCapacity 全局选项：

```
# FileMediumCapacity=MaxSizeInMBytes  
  
FileMediumCapacity=20000
```

首次格式化介质时指定文件设备的容量。重新格式化介质时，可以指定新大小；但是，将使用最初指定的大小。只能通过从系统中删除文件才能更改文件设备的容量。

指定的大小应至少比文件系统中的最大可用空间小 1 MB。文件设备达到其大小限制时，Data Protector 将发出装载请求。

要提高独立文件设备的性能，建议每个磁盘仅有一个设备，并且每个设备仅有一个驱动器。还应避免 Data Protector 正在备份/还原时其他应用程序从磁盘传输大量数据或将大量数据传输到磁盘。

文件可以位于本地或外置硬盘驱动器上，只要 Data Protector 了解其路径即可。配置文件设备时要指定路径。

### 配置独立文件设备

建议将所创建的设备置于 IDB 所在磁盘以外的磁盘上。这样可确保有足够的磁盘空间供数据库使用。将设备数据库和 IDB 放置在不同的磁盘上还能提高性能。

**重要：**  
请考虑以下几点：

- 请勿使用现有设备的名称配置这些设备，因为现有设备将被覆盖。
- 请勿使用相同的设备名称用于配置多个设备，因为每次访问设备时都会覆盖设备名称。

## 先决条件

- 在 **Windows** 系统中，必须对要用作设备的文件禁用 **Windows** 压缩选项。
- 必须已在磁盘上创建设备所在的目录，然后再创建设备。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **设备**，然后单击 **添加设备** 以打开向导。
3. 在“设备名称”文本框中，输入设备的名称。
4. 在“说明”文本框中，输入说明(可选)。
5. 在“客户机”列表中，选择客户机的名称。
6. 在“设备类型”列表中，选择 **独立设备** 设备类型，然后单击 **下一步**。
7. 在文本框中，输入文件设备的路径名和文件名，例如 `c:\My_Backup\file_device.bin`。
8. 单击 **添加**，然后单击 **下一步**。
9. 在“介质类型”列表中，选择 **文件** 介质类型。
10. 指定所选介质类型的介质池。可以从“介质池”下拉列表中选择现有的池，或输入新池名称。在这种情况下，将自动创建池。
11. 单击 **完成** 退出向导。

此时所配置设备的列表中将显示该设备的名称。可以扫描设备以验证配置。

此时已将设备指定为 **Data Protector**，但磁盘上尚未实际存在该设备。必须格式化该设备，然后才能将其用于备份。



# 第 9 章：介质

## 关于介质管理

Data Protector 提供强大的介质管理功能，通过此功能可以更简单高效地管理大量介质。系统使用 IDB 存储有关备份、恢复和介质管理事件的信息。

Data Protector 介质管理的高级功能为：

- 保护免遭意外覆盖。
- 介质池使您可以考虑大型介质集，而不必担心每个单独的介质。
- 可以在不以物理方式访问介质的情况下将所有与介质相关的目录数据从一个 Data Protector Cell Manager 传输到另一个。
- 自由池功能使您可以避免备份因缺少(空闲)介质而失败。
- 跟踪所有介质、每个介质的状态，以及在多个 Data Protector 单元之间共享这些信息：数据保护到期时间、备份用介质的可用性以及备份到每个介质的内容的编目。
- 可以明确定义对特定备份要使用哪些介质和哪些设备。
- 自动识别 Data Protector 介质和其他常用磁带格式。
- 识别和支持大型库中的条码设备以及支持条码的 silo 设备。
- 可以在多个 Data Protector 单元之间共享集中式介质信息。
- 支持介质保管，也称为归档或场外存储。
- 在介质上交交互或自动创建其他数据副本。
- 详细的筛选和分页设置。

## 自定义设备和介质视图

通过配置 MediaView、MagazineView、SCSIView、ExternalView、JukeboxView、ACSView 和 DASView 全局选项，可以自定义“设备和介质”上下文的默认视图。通过指定对应的令牌字符串，自定义将在库或介质管理上下文中显示的属性。有关详细信息，请参见[自定义 Data Protector 全局选项](#)。

## 关于介质池

介质池表示用于备份一组同类介质。可以定期备份用一个介质池、存档备份用一个、每个部门用一个等等。每个介质池定义介质使用情况、分配策略和介质状态因素。

## 自由池

自由池是当池中所有介质都在使用时可用的同类介质的辅助源。配备自由池有助于避免备份因缺少空闲介质而失败。

受保护介质属于某个特定的池(例如属于 **SAP** 池)，而空闲介质可以自动移至其他几个池所使用的自由池。这个公用空闲池用于向使用这个自由池的所有池分配空闲介质。可以对每个介质池决定是否要将其与某个自由池相联系。

## 默认介质池

默认介质池是 **Data Protector** 作为设备定义的一部分提供的池。如果在备份规范中没有指定任何介质池，则使用此池。

## 自由池特征

自由池是可以配置为允许跨介质池共享空闲介质的介质池，这些池可以减少因装载请求而导致的操作员干预。自由池的使用为可选。

对于自由池的一些特征，应在使用之前多加考虑。

## 自由池属性

自由池：

- 如果将空闲池与介质池相联系，或如果空闲池不为空，则无法删除该空闲池
- 与常规池不同的是它无法用于分配，因为它不能容纳受保护的介质。因此，分配策略选项(严格/宽松、可追加/不可追加)不可用。
- 仅包含空闲的 **Data Protector** 介质(无未知或空白介质)。

## 何时使用自由池？

在以下两种场合下，介质在常规池和自由池之间移动：

- 如果常规池中沒有空闲介质，**Data Protector** 将从自由池中分配介质。这样将使介质自动移至常规池。
- 介质上的所有数据都到期(并且介质位于常规池中)时，可将介质自动移至自由池。

## 介质质量计算

“链接”池之间以相同方式计算介质质量。仅对自由池可配置介质状态因素，并且所有使用自由池的池都将继承这些因素。不使用自由池的池有拥有其自己单独的计算基础。

## 自由池限制

- 无法将受保护的介质移至自由池。
- 无法在介质上使用某些操作(如导入、复制和循环回收)，因为可以在受保护的介质上进行这些操作。
- 选择了箱盒支持选项的池无法使用自由池。
- 使用空闲池时，可能会遇到池中出现暂时不一致的情况(1 天)(例如常规池中有一个不受保护的介质等待解除对空闲池的分配)。

- 如果自由池中有包含不同数据格式类型的介质，则 **Data Protector** 自动重新格式化所分配的介质(如有必要)。例如，可以将 **NDMP** 介质重新格式化为正常介质。

## 介质池属性

配置介质池时，指定介质池属性。某些属性可以接下来修改。

有关介质池属性的详细信息，请参见 **Data Protector** 帮助。

### 介质池属性 - 常规

- 说明
- 池名称
- 介质类型

### 介质池属性 - 分配

#### 分配

介质分配策略定义介质池中访问介质的顺序，以使介质均匀地磨损。包括：

- 严格
- 宽松
- 首先分配未格式化的介质
- 使用自由池
- 将自由介质移至自由池
- 箱盒支持

### 介质池属性 - 状况

#### 介质状态因素

介质状态因素定义介质的状态，因此确定介质能够可靠地用于备份的时间长度。例如，备份到旧或磨损的介质更容易产生读/写错误。根据这些因素，**Data Protector** 将介质的状况从良好改为中等或差。对整个介质池而非每个介质设置状况因素。

**重要：**

要使 **Data Protector** 准确计算介质的状况，请在向介质池添加介质时使用新介质。

**注意：**

如果池使用自由池选项，则从空闲池继承介质状态因素。

可以选择的两个介质状态因素包括：

- 最大覆盖数
- 有效期(月)

## 介质池属性 - 使用

介质使用策略控制如何将新备份添加到已使用的介质中。 包括：

- 可追加
- 不可追加
- 仅对于增量可追加

## 介质池质量

池中质量最低的介质决定介质池的质量。 例如，只要池中有一个介质为差，就会将整个介质池标为差。

介质的质量影响如何为备份选择介质，因为它影响能否写入介质和读取该介质所含数据。 先选择状况良好的介质，然后再选择状况中等的介质。 不选择状况差的介质进行备份。

介质状态取决于以下某个介质状态因素：

- 良好
- 中等
- 差

在介质池属性的“状况”属性页中，可以更改用于计算介质状况的介质状态因素。 新的介质状态因素将用于计算介质池中所有介质的状况。

## 设备错误和介质质量

如果备份期间设备发生故障，则将此设备中用于备份的介质标为差。 如果问题是因介质错误所致，这样可以防止未来再出错。

如果此错误是因不洁驱动器，请清洗驱动器，然后验证介质以重置其状况。

建议调查池中是否出现被标为差的介质。 可以使用“验证”获取有关每个介质的状况的详细信息。 建议不要只是循环回收介质。

## 创建介质池

Data Protector 提供默认介质池，但您可以根据自身需要创建自己的介质池。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，右键单击**池**，然后单击**添加介质池**以打开向导。
3. 在“池名称”文本框中键入介质池的名称，在“说明”文本框中键入说明(可选)，并在“介质类型”下拉列表中选择将用于备份设备的介质类型。单击**下一步 (Next)**。
4. 设置以下选项：

- 更改“介质使用策略”和“介质分配策略”的默认值(可选)。
- 要使用自由池，请首先选择**使用自由池**选项，然后从下拉列表中选择自由池。
- 要禁用向自由池自动解除分配空闲介质，请选择**将空闲介质移动到自由池**选项。
- 如果要配置支持箱盒的设备的介质池，则选择**箱盒支持**选项。此选项不能与介质池一起使用。

单击**下一步 (Next)**。

5. 更改“介质状态因素”对话框中的设置(可选)。
6. 单击**完成**以创建介质池，然后退出向导。

**提示：**

可以修改已配置的介质池。但是，无法修改其介质类型。

## 修改介质池

可以修改介质池属性以更好地符合您的需要：可以更改介质池的名称、其说明、介质使用策略和介质分配策略或介质状态因素。无法更改介质类型。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。此时将在结果区域中显示所配置介质池的列表。
3. 右键单击要修改的介质池的名称，然后单击**属性**。
4. 在“常规”属性页中，可以在“池名称”文本框中更改介质池的名称，或在“说明”文本框中更改说明。
5. 单击**分配**选项卡，以更改“介质使用策略”和“介质分配策略”的设置、(取消)选择自由池的使用、启用或禁用**将空闲介质移动到自由池**选项或者选择**箱盒支持**选项。
6. 单击**状况**选项卡，以更改“介质状态因素”对话框中的设置或将介质状况因素设置为默认。
7. 单击**应用**确认。

## 删除介质池

通过从 **Data Protector** 配置删除介质池，停止使用此介质池进行备份。无法删除用作备份设备的默认池的介质池。在这种情况下，更改所有设备的介质池或删除设备。

如果尝试删除非空介质池，则将提示您先导出或移动池中的所有介质。

**重要：**

如果删除备份规范中使用的介质池，则将从该规范中删除介质池。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。此时将在结果区域中显示所配置介质池的列表。
3. 右键单击要删除的介质池，然后单击 **删除**。确认操作。

所配置介质池的列表中不再显示该介质池。

## 介质生命周期

介质生命周期以介质的使用开始，在达到最大使用标准时结束。它通常由以下部分组成：

### 准备备份用介质

这一阶段包括格式化/初始化介质和将其分配给介质池，具体方法是格式化(未使用的介质和使用过的非 **Data Protector** 介质)或导入(使用过的 **Data Protector** 介质)。处理已使用过的介质时，请考虑使用回收/取消保护和导出功能。

### 使用备份用介质

这一阶段包括如何为备份选择介质、检查哪些介质状态因素(例如覆盖数)、如何将新备份追加到介质和数据保护何时到期。

### 将介质保管到安全位置

保管介质包括为安全存储准备介质和实际存储。要准备保管，需要设置相应的数据保护和编目保护策略，以创建保管位置的列表、以指定和修改介质位置、以弹出介质以及在某些情况下扫描设备。

**Data Protector** 支持各种级别的保管：

- 数据保护和编目保护策略。
- 轻松选择和弹出带库中的介质。
- 介质位置通知您存储介质的物理位置。
- 通过报告显示指定时间范围内用于备份的介质。
- 通过报告显示备份期间哪些备份规范使用了指定的介质。
- 通过报告显示存储在特定位置、其数据保护期在特定时间到期的介质。
- 显示还原所需介质的列表及其物理存储位置。
- 根据特定标准(如写入介质的时间或保护已到期的介质)才介质视图中筛选介质。

建议制作备份数据的副本用于保管，并在站点上保留原始介质以便可以进行还原。**Data Protector** 允许以交互方式创建或自动创建介质上数据的其他副本。

## 报废介质

介质到期(超过其最大使用标准)后，即将其标为差，并且不再被 **Data Protector** 使用。

## 介质类型

介质类型就是介质的物理种类，如 DDS 或 DLT。对于 **Data Protector**，在配置设备时选择相应的介质类型，而 **Data Protector** 将估算特定介质池的介质上的可用空间。

## 支持的介质类型

有关受支持的介质类型的详细信息，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新支持矩阵。

## 介质质量

介质的质量影响如何为备份选择介质，因为它影响能否写入介质和读取该介质所含数据。先选择状况良好的介质，然后再选择状况中等的介质。不选择状况差的介质进行备份。

介质状态取决于以下某个介质状态因素：

- 良好
- 中等
- 差

可以查看介质的“信息”属性页以获取有关介质质量(状况)的信息。

在介质池属性的“选项”属性页中，可以更改用于计算介质状况的介质状态因素。新的介质状态因素将用于计算介质池中所有介质的状况。

介质质量有助于确定何时必须更换介质。

## 设备错误和介质质量

如果备份期间设备发生故障，则将此设备中用于备份的介质标为差。如果问题是因介质错误所致，这样可以防止未来再出错。

如果此错误是因不洁驱动器，请清洗驱动器，然后验证介质以重置其状况。

建议调查是否有介质被标为差。可以使用“验证”获取有关每个介质的状况的详细信息。建议不要只是循环回收介质。

## 如何为备份选择介质

**Data Protector** 介质管理自动选择最适合备份的介质。介质选择的基本标准如下：

- 不选择状况差的介质进行备份。
- 只有在没有状况良好的介质可用时才使用状况中等的介质。
- 如果有，则首先使用状况良好的介质。

- 始终从指定的池选择介质。当池不包含不受保护的介质时，**Data Protector** 将访问自由池(如果已配置)。

此外，介质选择基于以下因素：

## 介质分配策略

可以使用介质分配策略影响如何为备份选择介质。可以指定宽松策略(任何合适的介质都可用于备份)，或严格策略(特定介质必须以预定义顺序可用)。

## 预分配介质

可以指定介质池中的介质将用于备份的顺序。此顺序称为预分配列表。

## 介质状态

介质状态也会影响为备份选择的介质。例如，状况良好的介质在状况中等的介质之前用于备份。状况差的介质不用于备份。

只有在标为中等的介质上没有受保护的介质时才会使用这些介质。否则，将发出装载请求，索要空闲介质。

## 介质使用

介质使用策略控制如何将新备份添加到已使用的介质中，并影响为备份选择哪些介质。

## 限制

在 **Travan** 设备中使用的介质上不能追加备份。

可追加的介质必须处于良好状况，包含某些当前受保护的對象并且不得已满。如果有多个设备用于负载均衡，则可追加的概念按设备适用，即每个设备都使用可追加的介质作为会话中的第一个介质。在相同介质上追加数据的备份会话不一定与相同的备份规范有关。

### 注意：

如果使用追加功能，并且备份需要多个介质，则只有所使用的第一个介质可以包含来自以前会话的备份数据。随后，**Data Protector** 将仅使用空的或不受保护的介质。

可能的策略有：可追加、不可追加或只可追加增量。

可以在介质上为某个客户机创建还原链。这些介质将仅包含一个完整备份以及与同一客户机相关的增量备份：

- 对于每个具有**仅对于增量可追加**介质使用策略的客户机配置一个池。
- 将一个不同的池与备份规范中的每个客户机相关，或为每个客户机创建一个单独的备份规范。

请注意，偶尔将创建仅包含增量备份的介质。



## 介质选择因素

分配策略	首先分配未格式化的介质	Data Protector 选择顺序
宽松	关闭	<ol style="list-style-type: none"><li>1. 预分配列表(如果指定)</li><li>2. 可追加的(如使用策略中所设置)</li><li>3. 不受保护的 Data Protector 介质</li><li>4. 未格式化的介质</li><li>5. 中等介质</li></ol>
宽松	打开	<ol style="list-style-type: none"><li>1. 预分配列表(如果指定)</li><li>2. 可追加的(如使用策略中所设置)</li><li>3. 未格式化的介质</li><li>4. 不受保护的 Data Protector 介质</li><li>5. 中等介质</li></ol>
严格	不适用	<ol style="list-style-type: none"><li>1. 预分配列表(如果指定)</li><li>2. 可追加的(如使用策略中所设置)</li><li>3. 不受保护的 Data Protector 介质</li><li>4. 中等介质</li></ol>

## 使用不同的介质格式类型

Data Protector 可识别两种不同的格式类型和使用这些类型向介质写入数据：

- Data Protector(适用于 Data Protector 直接控制下的备份设备)
- NDMP(适用于连接到 NDMP 服务器的备份设备)

两种格式类型使用两种不同的 Data Protector 介质代理组件(常规介质代理或 NDMP 介质代理)与备份设备进行通信。

## 限制

- 由一种格式类型写入的介质在使用不同格式类型的备份设备中将被识别为空白或外部介质。
- 不能在相同介质上使用不同格式类型备份对象。
- 不能在同一系统上安装两个不同的 Data Protector 介质代理组件。
- 强烈建议对不同的介质格式类型使用不同的介质池。

## WORM 介质

WORM(写入一次，读取多次)是一种数据存储技术，通过它可以将信息一次性写入介质，并防止驱动器擦除数据。WORM 介质有意设计为不可重写，因为它们旨在存储不希望意

外擦除的数据。

## 如何将 **WORM** 介质用于 **Data Protector**

仅 **Windows** 平台中支持检测 **WORM** 磁带。在其他平台中，**Data Protector** 会将磁带识别为可重写，并将它按照任何其他磁带的方式加以处理。尝试覆盖 **WORM** 介质上的数据时，将显示以下错误消息：

```
Cannot write to device ([19] The media is write protected.)
```

```
Tape Alert [ 9]: You are trying to write to a write-protected cartridge.
```

要防止出现这种情况，请执行以下操作：

- 将 **WORM** 介质的备份保护设置为“永久”。
- 将 **WORM** 介质和可重写的介质保存在不同的介质池中。

## 所支持的 **WORM** 介质

对于所支持的 **WORM** 介质支持进行所有 **Data Protector** 介质操作。有关受支持 **WORM** 磁带驱动器和介质的最新列表，请参见最新的支持矩阵，网址为：<https://softwaresupport.softwaregrp.com/>。

## 关于格式化介质

通过在 **IDB** 中保存有关介质的信息(介质 **ID**、说明和位置)，并通过在介质(介质头)上写入这些信息，格式化(初始化)介质使其做好准备，供 **Data Protector** 使用。格式化介质时，还会指定其所属的介质池。

## 用填充块进行格式化

可以扩展介质头的大小，并用不可压缩的数据(填充块)将其填满。创建介质副本时这会很有用。填充块不复制到目标介质。这样可确保目标介质不会在源介质之前到达磁带末尾。

如果使用对象副本功能复制备份数据，则不需要填充磁带。

默认情况下禁用磁带填充。要启用它，请在备份设备所连接的系统上的 **omnirc** 文件中设置 **OB2BLKPadding\_n** 选项。

## 何时格式化介质

首先需要格式化介质，然后再用其进行备份。但是，当对于介质池使用宽松介质分配策略时，不需要用单独的一步格式化介质。如果将全局选项 **InitOnLoosePolicy** 设置为 **1**(默认值为 **0**)，则 **Data Protector** 在选择新介质进行备份时即自动格式化这些介质。

首先必须格式化非 **Data Protector** 介质，然后再备份。

直到取消保护时才格式化具有受保护数据的 **Data Protector** 介质，此后可覆盖旧数据。

## 介质标签

格式化时，Data Protector 用唯一介质标签和介质 ID 标记每个介质。两者都存储在 IDB 中，并使 Data Protector 可以管理介质。介质标签是用户定义的说明和介质条形码的组合 (如果为库选择了在初始化时将条形码用作介质标签选项)。条码显示为介质说明的前缀。例如，[CW8279]Default DLT\_1 是一个介质标签，Default DLT\_1 为说明，CW8279 为条码。(可选)在初始化介质期间，可以将条码作为介质标签写入磁带上的介质头。

格式化介质后，即无法更改介质自身上写入的介质标签和位置，除非再次将其格式化(这会导致覆盖数据)。修改介质属性仅更改 IDB 中的此信息。

尽管可以更改标签并排除条码数字，但建议不要这么做。在这种情况下，应手动跟踪分配给介质的实际条码和介质标签。

## 识别介质格式

如果介质已由某些其他应用程序使用，则 Data Protector 可识别介质上通用格式的数据。但是，建议不要依赖 Data Protector 来识别其他介质类型，因为能否识别取决于您所使用的平台。

要确保不覆盖任何 Data Protector 介质，必须选择严格分配策略。

Data Protector 按照所识别的格式做出不同的行动，如下表所示。

### Data Protector 介质格式类别

介质格式	备份行为	可能进行的操作
未知或新(空白)	宽松策略：用于备份 严格策略：不用于备份	格式化介质
写入时压缩的介质，当前以无压缩方式使用	宽松策略：用于备份 严格策略：不用于备份	格式化介质
写入时不压缩的介质，当前以压缩方式使用	宽松策略：用于备份 严格策略：不用于备份	格式化介质
外部 Data Protector(另一个单元中)	不用于备份	导入或强制格式化介质
tar、cpio、OmniBack I、ANSI label	不用于备份(无法保证)	强制格式化介质
Data Protector 不受保护的介质	用于备份	导出介质
Data Protector 受保护的介质	追加备份	回收(取消保护)介质

**注意：**  
如果尝试用不支持硬件压缩的设备读取使用硬件压缩写入的介质，Data Protector 无法识别介质和读取数据。因此，将该介质视为未知或新。

## 格式化介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 **Data Protector** 介质，此后可覆盖旧数据。

### 注意：

直到向文件库设备进行首次备份后，才能将其格式化。这是因为此前设备不包含任何文件仓库，并且无法手动创建文件仓库。备份期间创建的文件仓库等同于介质。根据文件库设备的介质池介质分配策略，将自动删除新格式化的介质。

### 重要：

使用**强制操作**选项可用 **Data Protector** 可识别的其他格式(tar、OmniBack I 等等)将介质格式化，或重新格式化 **Data Protector** 介质。

直到取消保护后，才会格式化含有受保护数据的 **Data Protector** 介质。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，右键单击要向其添加介质的介质池，然后单击**格式化**以打开向导。
4. 选择目标介质所在的设备，然后单击**下一步**。
5. 指定新介质的**介质说明**和**位置**(可选)，然后单击**下一步**。
6. 指定会话的其他选项：可以选择**在操作完成之后弹出介质**选项，或使用**强制操作**选项。还可以**指定介质大小**，或使**默认**选项保持选中状态。
7. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 **Data Protector**。

## 格式化箱盒中的所有介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 **Data Protector** 介质，此后可覆盖旧数据。

## 先决条件

要在一步中格式化箱盒中的所有介质，请使用选择了**箱盒支持**选项的设备。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击所需的介质池。
4. 右键单击**箱盒**项，然后单击**格式化箱盒**以打开向导。
5. 选择库中要用其执行操作的驱动器，然后单击**下一步**。

6. 指定新介质的说明和位置(可选)，然后单击**下一步**。
7. 指定会话的其他选项：可以使用**强制操作**选项并选择**指定介质大小**选项，或使**默认**选项保持选中状态。
8. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 **Data Protector**。

## 格式化箱盒中的单个介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 **Data Protector** 介质，此后可覆盖旧数据。

### 先决条件

要格式化箱盒中的介质，请使用选择了**箱盒支持**选项的设备。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，右键单击要向其添加介质的介质池，然后单击**格式化**以打开向导。
4. 选择目标介质所在的设备以及要在其上执行操作的介质所在的插槽，然后单击**下一步**。
5. 指定新介质的说明和位置(可选)，然后单击**下一步**。
6. 指定会话的其他选项：可以使用**强制操作**选项并选择**指定介质大小**选项，或使**默认**选项保持选中状态。
7. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 **Data Protector**。

## 格式化带库设备中的介质

首先必须格式化介质，然后再将其用于备份。直到取消保护时才格式化具有受保护数据的 **Data Protector** 介质，此后可覆盖旧数据。

如果使用库设备，则可以使用 **Ctrl** 键选择多个插槽，并在一步中格式化多个介质。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开“设备”，展开库设备，然后单击**插槽**。
3. 在结果区域中，右键单击要格式化的介质所在的插槽，然后单击**格式化**以打开向导。
4. 选择库中要用其执行操作的驱动器，然后单击**下一步**。
5. 选择要向其添加格式化的介质的介质池，然后单击**下一步**。
6. 指定新介质的**介质说明**和位置(可选)，然后单击**下一步**。
7. 指定会话的其他选项：可以使用**强制操作**选项并选择**指定介质大小**选项，或使**默认**选

项保持选中状态。

8. 单击**完成**以开始格式化，然后退出向导。

格式化完成后，将介质格式设置为 **Data Protector**。

## 关于导入介质

介质导入是在不丢失介质上数据的前提下将单元之外的 **Data Protector** 介质添加到介质池中的行为。此前必须已导出该介质，即该介质来自另一个 **Data Protector** 单元。

导入介质时，将有关介质上备份数据的信息读入 **IDB** 中，以使您以后可以浏览它进行还原。

## 注意事项

- 在介质导入期间，不重新构造对象或介质大小等属性信息，因此所导入对象的大小显示为 **0 kB**。
- 根据所使用的备份设备和介质，导入可能会花费相当长的一段时间。
- 无法将介质导入自由池中。
- 如果尝试导入已删除的副本，并且原始介质不在 **IDB** 中，则首先需要使用强制操作选项导入原始介质，或使用作为原始副本导入选项导入副本。
- 在将数据保护已过期的 **WORM** 介质导入 **Data Protector** 单元时，请确保使用选项**保护**(默认情况下此值被设置为“永久”)指定新的数据保护值。这允许将 **Data Protector** 附加到 **WORM** 介质。

## 何时导入介质？

通常在 **Data Protector** 单元之间移动介质时使用导入功能。在这种情况下，不更新有关介质上空间的信息。

应在一个备份会话中导入所使用的全部介质。如果在备份会话中仅添加部分介质，则无法还原跨越到其他介质的数据。

涉及文件库设备时，只能导入以前属于该文件库设备并且以前已导出的文件仓库。如果要从位于目标主机之外主机上的文件库导入介质，则只能将其导入介质库设备。

## 导入介质

要向介质池添加已由 **Data Protector** 使用的介质，以使您以后可以浏览可供恢复的数据时，可导入介质。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，单击**设备**。
3. 在结果区域中，右键单击要向其导入介质的设备，然后单击**导入**以打开向导。
4. 选择要向其添加所导入介质的介质池，然后单击**下一步**。

5. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项(可选)。

6. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 **Data Protector**。

## 导入箱盒中的所有介质

要向介质池添加已由 **Data Protector** 使用的介质，以使您以后可以浏览可供恢复的数据时，可导入介质。

### 先决条件

要在一步中导入箱盒中的所有介质，请使用选择了**箱盒支持**选项的设备。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击箱盒中的介质所在的介质池。此时将显示“介质”和“箱盒”项。
4. 右键单击**箱盒**项，然后单击**导入箱盒**以打开向导。
5. 选择库中要用其执行操作的驱动器，然后单击**下一步**。
6. 指定新介质的说明(可选)，或保留已设置的**自动生成**选项，然后单击**下一步**。
7. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项(可选)。
8. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 **Data Protector**。

## 导入箱盒中的单个介质

要向介质池添加介质，以使您以后可以浏览可供恢复的数据时，可导入已由 **Data Protector** 使用的介质。

### 先决条件

要导入箱盒中的介质，请使用选择了**箱盒支持**选项的设备。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**池**。
3. 在结果区域中，双击箱盒中的介质所在的介质池。此时将显示“介质”和“箱盒”项。
4. 右键单击**介质**项，然后单击**导入**以打开向导。
5. 选择目标介质所在的库的驱动器和插槽，然后单击**下一步**。

6. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项(可选)。

7. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 **Data Protector**。

## 导入带库设备中的介质

要向介质池添加已由 **Data Protector** 使用的介质，以使您以后可以浏览可供恢复的数据时，可导入介质。

如果使用库设备，则可以使用 **Ctrl** 键选择多个插槽，并在一步中格式化多个介质。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，展开库设备，然后单击**插槽**。
3. 在结果区域中，选择要导入的介质所在的插槽。
4. 右键单击所选插槽，然后单击**导入**以打开向导。
5. 选择交换器从中将加载要导入的介质的库的驱动器，然后单击**下一步**。
6. 选择要向其添加导入的介质的介质池，然后单击**下一步**。
7. 选择**作为原始副本导入**选项，并决定符合需要的**日志记录**选项(可选)。
8. 单击**完成**以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，将介质类型设置为 **Data Protector**。

## 导出和导入含有加密备份的介质

要将加密备份中的数据恢复到不同 **Data Protector** 单元中的客户机，需要将介质和加密密钥导入到目标 **Cell Manager**，如以下各节所述。

### 注意：

**Data Protector** 还通过命令行界面 (CLI) 提供加密密钥的高级手动管理(如使密钥过期、重新激活、导出、导入和删除密钥)。有关详细信息，请参见 **omnikeytool** 手册页或《**Data Protector** 命令行界面参考》。

## 没有 CMMDB 的 Cell Manager 环境或 MoM 环境

在不使用本地 MMDb 的 **Cell Manager** 环境中或 MoM 环境中，执行以下步骤可导出和导入含有加密备份的介质：

### 步骤

1. 在原始 **Cell Manager** 上，从 IDB 导出介质。此操作还会将相关的加密密钥从密钥库导出到默认导出加密密钥目录下的 **mediumID.csv** 文件中。
2. 将 **mediumID.csv** 文件传输到目标 **Cell Manager**，并将其放置到默认导入加密密钥目录中。



3. 将导出的介质插入目标 **Cell Manager** 将使用的驱动器中。
4. 在目标 **Cell Manager** 上导入该介质。此操作还可从 *mediumID.csv* 文件中导入密钥。

**注意：**

如果密钥文件不存在，则仍可导入介质，但目录导入将因缺少解密密钥而中止。

## 有 CMMDB 的 MoM 环境

在使用 CMMDB 的 MoM 环境中，所有介质信息都存储在 MoM Manager 上，但这些介质使用的加密密钥 ID 以及 CDB 存储在每个各自 **Cell Manager** 上的本地密钥库中。请注意，所有介质管理操作都需要在 MoM **Cell Manager** 上完成。

要在 CMMDB 位于 MoM Manager 上的情况下导出和导入含有加密备份的介质，请执行以下步骤：

### 步骤

1. 从 CMMDB 导出介质。密钥 ID 将导出到默认导出加密密钥目录下的 *mediumID.csv* 文件中。
2. 将 *mediumID.csv* 文件传输到目标 **Cell Manager**，并将其放置到默认导入加密密钥目录中。
3. 从 MoM Manager 中，从带库弹出介质。
4. 将介质从原始介质池移至目标介质池，后者与目标单元中的某个驱动器关联。此操作还可导入目录。
5. 将导出的介质插入目标 **Cell Manager** 将使用的驱动器中。
6. 在目标 **Cell Manager** 上导入该介质。此操作还可从 *mediumID.csv* 文件中导入密钥。

## 关于介质复制

**Data Protector** 介质复制功能使您能够在执行备份后复制介质。介质复制是创建包含备份的介质的精确副本的过程。可以将副本或原始介质移至一个安全位置用于归档或保管，并在站点上保留其他介质集用于恢复。

### 先决条件

需要两个设备，一个用于源介质，一个用于目标介质。还可以在具有多个驱动器的库设备中复制介质。在这种情况下，使用一个驱动器用于源介质，另一个用于目标介质。

- 源介质和目标介质必须属于同一介质类型。
- 如果目标介质是具有数据保护的 **Data Protector** 介质，则首先必须回收介质，然后再将其格式化。

### 限制

- 可以对介质(源介质)制作多个副本(目标介质)，但不能对介质副本制作副本。
- 只能复制位于 **Data Protector** 中的介质(设备中的介质)。
- 由于介质复制旨在对通常移至不同位置的介质制作准确副本，因此文件库不支持此功

能。要在文件库中制作数据的副本，请使用对象副本功能。

- 介质复制操作对自由池中的介质不可用。
- 受 NDMP 服务器控制的 NAS 设备的设备并发限制为 1。
- NDMP-Celerra 备份会话不支持介质复制。

## 何时复制介质

只要备份会话完成，即可复制介质。但是，需要考虑将用于复制介质的设备的可用性。建议等待所有使用特定设备的备份完成，然后再使用这些设备进行介质复制。

## 复制介质的结果

复制介质的结果是两个完全相同的介质集 — 原始介质集和副本。其中任何一个都可用于还原。

复制源介质之后，**Data Protector** 将其标记为不可追加，以防止追加新备份。(这可能导致原始数据与其副本不同。)副本也标记为不可追加。

## 从副本还原

默认情况下，**Data Protector** 从原始介质集还原数据。但是，如果原始介质集不可用，但副本可用，则可使用副本进行还原。

如果还原期间设备中既没有原始介质集也没有副本，则 **Data Protector** 会发出一个装载请求，其中显示原始介质集和副本都是还原所需的介质。可以使用其中任意一个。

如果使用独立设备执行还原，则可以选择从副本而非从原始介质集还原。为此，请在将用于还原的设备中插入副本，或选择含有副本的设备。但是，如果使用库设备执行还原，并且原始介质集位于库中，则 **Data Protector** 将使用它进行还原。

### 注意：

复制介质时，有可能目标介质在源介质之前达到磁带末尾。如果以流式传送模式写入源介质，并且在繁忙的系统上或通过负载繁重的网络制作副本(这两种情况会产生空白空间，磁带在此处停止并再次启动)，则会发生这种情况。通过在格式化介质时启用磁带填充，可以阻止这种情况发生。

## 复制介质

可以复制介质用于归档或保管。需要单独启动每个介质的复制，因为在一个介质复制会话中只能复制一个介质。

## 在独立设备中复制介质

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **设备**，右键单击含有要复制的介质的设备，然后单击 **复制**。
3. 选择目标介质所在的设备(库的驱动器和插槽)，然后单击 **下一步**。

4. 选择要向其添加介质副本的介质池，然后单击**下一步**。
5. 指定介质副本的说明和位置(可选)，然后单击**下一步**。
6. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

**提示：**

如果目标介质具有 Data Protector 可识别的其他格式(tar 和 OmniBack I 等等)或如果这些介质是不受保护的 Data Protector 介质，则使用**强制操作**选项。

7. 单击**完成**以开始复制，然后退出向导。
- “会话信息”消息显示介质复制操作的状态。

## 在带库设备中复制介质

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中的**介质**下，展开**池**，然后展开含有要复制的介质的介质池。右键单击介质，然后单击**复制**以打开向导。
3. 为要复制的介质选择驱动器，然后单击**下一步**。如果带库只有一个驱动器，则跳过此步骤。
4. 选择目标介质所在的设备(库的驱动器和插槽)，然后单击**下一步**。
5. 选择要向其添加介质副本的介质池，然后单击**下一步**。
6. 指定介质副本的说明和位置(可选)，然后单击**下一步**。
7. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

**提示：**

如果目标介质具有 Data Protector 可识别的其他格式(tar 和 OmniBack I 等等)或如果这些介质是不受保护的 Data Protector 介质，则使用**强制操作**选项。

8. 单击**完成**以开始复制，然后退出向导。
- “会话信息”消息显示介质复制操作的状态。

## 自动介质复制

自动介质复制是为包含备份的介质创建副本的自动化过程。与手动启动的介质复制相比，要外注意一些额外限制：

### 限制

- 无法使用独立设备进行自动介质复制；而只能使用库设备。  
无法使用磁盘备份 (B2D) 设备进行自动介质复制。
- NDMP-Celerra 备份会话不支持自动介质复制。

## 自动介质复制

首先，创建自动介质复制规范。自动介质复制会话开始时，Data Protector 会根据自动介质复制规范中指定的参数生成介质列表，作为源介质。对于每个源介质，都会选择要将数

据复制到的目标介质。目标介质从源介质所在的同一介质池、自由池或库内的空白介质中选择。

对于每个源介质，**Data Protector** 都会从您在自动介质复制规范中指定的设备中选择一对设备。自动介质复制功能提供其自己的负载均衡。**Data Protector** 通过利用尽可能多的设备和选择本地设备(如果其可用)，尝试充分利用可用的设备。

会话开始的时候锁定设备。那时不可用的设备就不能用于会话中，因为会话开始后即无法锁定设备。请注意，对于每种介质类型必须至少有一对设备可用，整个会话才能成功完成。如果无法锁定会话必需的最少设备数，则会话将失败。

源介质定义目标介质的目标池。这意味着复制的介质将属于与原始介质相同的池。

副本的默认保护期与原始保护期相同。创建或修改自动介质复制规范时，可以设置不同的保护期。

自动介质复制功能不处理装载请求或清除请求。如果收到装载请求，则中止相关的介质对，但会话将继续。自动介质复制会话完成之后，可以手动复制未复制的介质。

如果发生介质错误，则该自动介质复制会话中将避免使用出错的设备。但是，如果没有其他设备可用，则将重新使用该介质。

## 自动介质复制的类型

自动介质复制分为两种类型：备份后介质复制和计划的介质复制。

### 备份后介质复制

备份后介质复制发生在完成备份会话之后。它复制该特定会话中使用的介质。

### 计划的介质复制

计划的介质复制发生在用户定义的某个时间。不同备份规范中使用的介质可以在单个会话中复制。创建自动介质复制规范来定义要复制的介质。

## 配置备份后介质复制

备份后介质复制是在备份会话结束之后为特定备份会话中所使用的介质创建副本的一个过程。

#### 注意：

如果中止备份会话，则即使只有一部分对象成功完成，也会启动备份后介质复制会话。

## 限制

- 只能使用带库设备。
- 源介质和目标介质必须属于同一类型。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **自动操作**，然后单击 **添加备份后介质选项** 以打开向导。
3. 在“备份规范”下拉列表中，选择要复制其介质的备份规范。在“介质操作类型”下拉列表中，选择 **介质复制**，然后单击 **下一步**。
4. 选择将使用的源设备和目标设备。对于每种介质类型，至少必须有一对设备(一个源设备和一个目标设备)。单击 **下一步 (Next)**。
5. 指定副本数、操作之后是否自动弹出介质以及目标介质的位置和保护。单击 **完成** 退出向导。

## 配置计划的介质复制

计划的介质复制是在计划时间为特定备份会话中使用的介质创建副本的一个过程。可以在一个会话中计划多个复制操作。如果有足够的设备可用，将同时复制这些介质。否则，将按顺序复制这些介质。

## 限制

- 只能使用库设备。
- 源介质和目标介质必须属于同一类型。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，右键单击 **自动操作**，然后单击 **添加计划的介质操作** 以打开向导。
3. 在“介质操作名称”文本框中，键入操作的名称。在“介质操作类型”下拉列表中，选择 **介质复制**，然后单击 **下一步**。
4. 选择将使用的源设备和目标设备。对于每种介质类型，至少必须有一对设备(一个源设备和一个目标设备)。单击 **下一步**。
5. 指定要从中搜索备份会话的时间范围。单击 **下一步**。
6. 指定要复制的备份的备份规范。单击 **下一步**。
7. 指定源介质的所需状况和保护。单击 **下一步**。
8. 指定副本数、操作之后是否自动弹出介质以及目标介质的位置和保护。单击 **完成** 退出向导。或者，您可以使用计划程序计划介质复制。

有关如何在 **Data Protector** 中创建和编辑计划的更多信息，请参见 [计划程序 \(第 92 页\)](#)。

### 重要：

借助 **Data Protector 10.00**，基本计划程序和高级计划程序已过时，被基于 Web 的新计划程序所替代。可以配置无人看管备份，具体方法是排定备份会话使其在特定的时间执行。升级 **Data Protector** 时，所有现有的 **Data Protector** 计划会自动迁移至新的计划程序。

## 扫描设备

扫描设备可更新有关设备中介质的 **Data Protector** 信息，或在手动更改介质位置之后更新该信息。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。
3. 在结果区域中，右键单击要扫描的设备，然后单击 **扫描**。

此时“会话信息”消息将显示扫描操作的状态。

## 扫描带库设备中的介质

扫描库的所选插槽中的介质可更新有关设备中介质的 **Data Protector** 信息。

根据所选插槽的数量，扫描可能需要花费一些时间。**Data Protector** 必须将每个插槽中的介质加载到驱动器中，然后读取介质头。

可以使用 **Ctrl** 键选择多个插槽，并在一步中扫描多个介质。但是，只能使用一个驱动器。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。
3. 在结果区域中，双击库设备，然后双击 **插槽**。
4. 在结果区域中，选择含有要扫描的介质的插槽。
5. 右键单击所选插槽，然后单击 **扫描** 以打开向导。
6. 选择交换器将从中加载要扫描的介质的带库的驱动器。
7. 单击 **完成** 以开始扫描，然后退出向导。

此时“会话信息”消息将显示扫描操作的状态。

#### 提示：

如果启用了条形码读取器支持选项，则可以使用 **条形码扫描** 选项快速扫描 **SCSI** 库。

## 扫描带库设备中的驱动器

扫描库设备的驱动器可更新有关驱动器中介质的 **Data Protector** 信息。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。

3. 在结果区域中，双击要扫描其驱动器的库设备，然后双击目标**驱动器**图标。
4. 右键单击要扫描的驱动器，然后单击**扫描**。

此时“会话信息”消息将显示扫描操作的状态。

## 激活条码读取器支持

如果 SCSI 库设备使用含条形码的介质，则 Data Protector 可以使用条形码提供以下条形码支持：

- 识别前缀为 CLN 的磁带。
- 按介质的条码引用介质。Data Protector 显示介质条形码作为介质说明的前缀。
- 使用介质条码快速扫描库存储库的插槽中的介质。

### 提示：

如果在库属性中选择**在初始化时将条形码用作介质标签**选项，则默认情况下在初始化介质期间将启用**介质说明**选项中的**使用条形码**选项。如果未选择此选项，则默认选项为“自动生成”。Data Protector 自动格式化介质时将使用默认选项。

### 注意：

单元中的所有条码都必须唯一，而不考虑介质类型或有多个库这一事实。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开“设备”，右键单击目标库设备，然后选择**属性**。此时将打开带库设备的“属性”页。
3. 单击**控制**选项卡，然后选择**条码读取器支持**选项。
4. 要在每次用此库初始化介质时将条形码写入到磁带上的介质头中，请选择**在初始化时将条形码用作介质标签**选项。
5. 单击**应用**确认。

## 扫描带库设备的条码

使用**条形码扫描**选项可快速扫描 SCSI 库。这比扫描无条码功能的存储库快得多。

## 先决条件

需要启用**条形码读取器支持**选项。

## 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开“设备”，右键单击目标库设备，然后单击**条码扫描**。

此时“会话信息”消息将显示条码扫描操作的状态。

## 搜索和选择介质

可以搜索和选择介质池中或库设备中的介质。还可以使用“介质列表”报告列出介质。使用此功能可以定位和选择特定介质，而不浏览介质的整个列表。

介质选择对保管用途特别有用，如将上周写入的所有介质移至保管库。

### 在介质池中搜索和选择介质

#### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。
3. 在结果区域中，右键单击介质池，然后单击 **选择介质**。此时将显示“选择介质”对话框。
4. 根据介质说明、介质位置、会话、时间范围、保护搜索和选择介质，或使用“组合选择”选项。

### 在库设备中搜索和选择介质

#### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。
3. 在结果区域中，双击库设备，右键单击 **插槽**，然后单击 **选择介质**。此时将显示“选择介质”对话框。
4. 根据介质说明、介质位置、会话、时间范围、保护搜索和选择介质，或使用“组合选择”选项。

### 使用“介质列表”报告搜索介质

#### 步骤

1. 在上下文列表中，单击 **报告**，然后单击 **任务** 选项卡。
2. 在范围窗格中，展开 **池和介质**，然后单击 **介质列表** 以打开向导。
3. 按照向导操作，指定搜索的标准。单击 **完成** 以显示搜索的结果。

## 备份用介质的预分配列表

可以指定介质池中的介质将用于备份的顺序。此顺序称为预分配列表。配置备份时，指定预分配列表。预分配列表的用途是控制哪些介质将用于备份会话。必须在每次备份之前将预分配列表与可用介质相匹配。

还可以在使用对象副本或对象合并功能时预分配介质。

根据介质池的分配策略，**Data Protector** 以两种不同方式行动：



- 如果将预分配列表与**严格**介质分配策略结合使用，则 **Data Protector** 预计将以该顺序提供备份设备中的介质。如果介质不可用，则 **Data Protector** 将发出装载请求。如果在 **SCSI** 交换器中加载预分配列表中提及的介质，则 **Data Protector** 将自动处理介质顺序。
- 如果将预分配列表与**宽松**介质分配策略结合使用，则首先使用预分配列表中的介质。如果介质不可用，则使用带库中的任何适用介质。

## 预先分配备份用介质

以下内容可能会提供其他信息：

- 还可以在使用对象副本或对象合并功能时预分配介质。
- 默认情况下，文件库介质池的介质使用策略为不可追加。由于此策略对文件库有益，因此建议不要更改它而使用文件库设备介质的预先分配列表。

要在所保存的备份规范中预先分配介质，请按照以下这些步骤进行操作：

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如“文件系统”)。此时将显示所保存的全部备份规范。
3. 双击相应的备份规范，然后单击**目标**选项卡。
4. 在“目标”页中，右键单击选择用于备份的设备，然后单击**属性**。
5. 在“设备属性”对话框中，从“介质池”下拉列表中选择所需的介质池。
6. 在“prealloc 列表”下，单击**添加**。  
此时将显示所选介质池中介质的列表。
7. 选择某个介质，然后单击**添加**。
8. 对所需的所有介质重复步骤 6 和 7。完成后，单击**确定**，返回“目标”属性页。
9. 如果有多个设备用于备份，则重复步骤 4 到 8。
10. 单击**应用**保存更改。

## 回收介质

要取消对介质上所有已备份数据的数据保护，以使 **Data Protector** 可以在后续备份期间覆盖介质时，可循环回收(取消保护)介质。回收并不真正更改介质上的数据；它只是告知 **Data Protector** 此数据不再受保护。

### 重要：

请考虑以下几点：

- 回收可取消对介质上所有对象的保护。这还包括位于其他介质上的相同对象和会话中的数据。
- 回收操作对自由池中的介质不可用。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。此时将在结果区域中显示所配置介质池的列表。
3. 双击含有要循环回收的介质的介质池。
4. 右键单击目标介质名称，然后单击 **回收**。还可以使用 **Ctrl** 或 **Shift** 键同时选择多个介质。

操作完成后，将介质的保护设置为“无”。

## 从介质导入目录

从介质导入目录可将文件名和文件版本等详细信息写入 IDB 中，从而使您能够浏览可供还原的文件和目录。

如果特定对象的编目保护已到期，并且不能再浏览其文件和目录，则还可以使用“导入编目”。如果 IDB 中已存在有关所指定介质的详细信息，则将不复制这些数据。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。
3. 在结果区域中，双击要从中导入目录的介质所在的介质池。
4. 右键单击该介质，然后单击 **导入编目**。
5. 如果有更多驱动器，则选择要向其导入介质的库驱动器，然后单击 **下一步**。
6. 选择符合需要的 **日志记录** 选项。
7. 单击 **完成** 以开始导入，然后退出向导。

此时“会话信息”消息将显示导入操作的状态。导入完成后，可以浏览可供还原的文件和目录。

## 验证介质

验证介质可检查介质上的数据格式是否有效，并在 IDB 中更新有关介质的信息。只能验证驻留的 **Data Protector** 介质。根据所使用的备份设备和介质，验证可能会花费相当长的一段时间。

可以验证介质副本，然后再将其保管起来。如果备份期间报告了错误，也可以验证介质以检查备份是否可用。

验证介质时，**Data Protector** 执行以下操作：

- 检查具有有关介质信息(介质标识、说明和位置)的 **Data Protector** 头。
- 读取介质上的所有块，并验证块格式。
- 如果备份期间使用了 **CRC 检查** 选项，则重新计算 **CRC**，并将它与介质上存储的对应值进行比较。在这种情况下，备份数据本身在每个块中一致。此检查级别的可靠性很高。

如果未使用“CRC 检查”选项而通过了验证操作，则这意味着已读取了介质上的所有数据。介质未导致读错误，因此磁带的硬件状态至少可接受。可以将此检查级别视为部分判断标准。

## 在独立设备中验证介质

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **设备**，右键单击含有要验证的介质的设备，然后单击 **验证**。
3. 在结果区域中，可以选择在**操作完成之后弹出介质**选项。单击**完成**验证介质。

对于独立文件设备跳过此步骤。

此时“会话信息”消息将显示验证的状态。

## 在带库设备中验证介质

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中的 **设备** 下，展开库设备，然后展开 **插槽**。右键单击含有要验证的介质的插槽，然后单击 **验证**。
3. 在结果区域中，选择用于执行验证的库驱动器，然后单击 **完成**。

此时“会话信息”消息将显示验证的状态。

## 移动介质

如果要重新组织备份并重新安排每个池的用途，则可以将介质从一个介质池移至相同类型的另一个介质池。要使用作为另一个介质池默认设备的设备中的介质时，此操作也很有用。

#### 注意：

无法将介质移至空闲介质池。使用自由池时，在两个实例中移动介质(行为取决于所选的空闲池选项)：

- 选择(分配)用于备份的介质时，将这些介质从自由池移至常规池。
- 介质保护到期后，将介质从常规池移至自由池。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。
3. 在结果区域中，双击要从中移动介质的介质池。此时将显示各自池中介质的列表。
4. 右键单击要移动的介质，然后单击 **移动到池** 以打开向导。还可以使用 **Ctrl** 或 **Shift** 键同时选择多个介质。

5. 选择要向其移动介质的介质池。
6. 单击 **完成** 以移动介质，然后退出向导。

**提示：**

要将介质移至另一个单元，请从一个单元导出介质，然后将其导入另一个单元。

## 导出介质

要将介质移至另一个 **Data Protector** 单元时，导出该介质。导出将从 **IDB** 中删除有关介质及其内容的信息。**Data Protector** 将不再认为此介质存在。介质上的数据保持不变。

**注意：**

建议不要手动导出依赖日常维护来清理存储的备份到磁盘 (B2D) 设备上的介质，因为手动导出所有介质至关重要。允许通过日常维护来清理存储。

如果导出原始介质并仍有副本，则其中一个副本变为原本。

**重要：**

导出介质之前必须通过回收介质取消其保护。

应导出同一备份会话的所有介质。如果会话中的数据跨越多个介质，而您仅导出一个介质，则可能无法还原数据。**Data Protector** 仍知道介质上存在数据，但某些介质不再可用。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。
3. 在结果区域中，双击含有要导出的介质的介质池，右键单击介质名称，然后单击 **导出**。
4. 确认操作。

池中介质的列表中不再显示所导出的介质。

## 将目录介质数据复制到 MCF 文件中

将与介质相关的编目数据复制到文件可将文件名和文件版本等详细信息写入介质容器格式 (MCF) 文件中，这些文件位于 **Cell Manager** 上的目录 `Data_Protector_program_data\Config\Server\export\mcf` (Windows 系统) 或 `/var/opt/omni/server/export/mcf` (UNIX 系统) 中。然后将这些文件导入另一个其中与介质相关的目录数据可供浏览的 **Data Protector Cell Manager** 中。

## 限制

- 只能选择 **Data Protector** 介质。
- 由于 **Data Protector** 文件库的性质，无法从一个库导出介质再将其导入另一个库，因此应避免对此类介质执行 **将编目复制到文件** 和 **从文件导入编目**。

## 建议

- 由于每个介质可能有大量目录数据，因此建议在一个单独的分区或装载点上存储文件。
- 通过将全局选项中的 `EnableMCFCompression` 设置为 1，可以减小文件的大小。默认情况下禁用压缩。

以下内容可能会提供其他信息：

- 不从原始 **Cell Manager** 删除与介质相关的目录数据。
- 此操作为每个介质创建一个 **MCF** 文件。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后展开 **池**。
3. 展开要复制其目录的介质所在的介质池。
4. 右键单击介质，然后单击 **将目录复制到文件**。
5. 指定 **MCF** 文件的输出目录，此文件将包含与介质相关的目录数据。
6. 单击 **完成** 以开始复制，然后退出向导。

所导出的 **MCF** 文件可以传输到目标 **Cell Manager**。

### 提示：

通过展开 **设备**，右键单击所选设备的插槽，然后执行步骤 5 和 6，可以达到相同的结果。

## 从 **MCF** 文件导入目录介质数据

从原始 **Cell Manager** 中的介质容器格式 (**MCF**) 文件导入与介质相关的目录数据副本，使您可以浏览目标 **Cell Manager** 上的文件。

## 先决条件

- 确保要导入的 **MCF** 文件已从原始 **Cell Manager** 转移而来，并在当前的 **Cell Manager** 上可访问。

## 限制

- 从文件导入介质之后，需要有物理介质的操作(例如还原、介质复制)无法使用该介质。要使介质完全可供 **Data Protector** 操作使用，必须以物理方式可访问该介质，并且通过使用 **Data Protector** 介质扫描可扫描到该介质，否则将发出装载请求。

以下内容可能会提供其他信息：

- 从 **MCF** 文件导入大量介质编目时，请确保导入的所有介质都是恢复链一部分。
- 可以在一个会话中从多种介质池导入不同类型的介质。
- **Data Protector** GUI 仅显示和允许选择扩展名为 `mcf` 的文件。目录树中隐藏其他文件。但是，可以通过命令行界面(command-line interface, CLI)选择这些文件。有关详细信息，请参见 *omnim* 手册页或《**Data Protector** 命令行界面参考》。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，右键单击 **池**，然后单击 **从 MCF 文件导入编目** 以打开向导。
3. 指定要导入的 **MCF** 文件。
4. 指定会话的其他选项：默认情况下，选择 **如有可能，导入到原始池** 选项。可以选择“新池的前缀”或 **作为原始副本导入** 选项。
5. 单击 **完成** 以开始导入，然后退出向导。

## 修改介质说明

介质说明有助于标识介质。说明写入介质上，并存储在 **IDB** 中。格式化新介质时可添加介质说明。如果在备份期间自动格式化介质，则可能要将自动创建的说明更改为更符合您需要的某些内容。

修改介质说明后，**Data Protector** 修改 **IDB** 中而非介质本身上的说明。如果导出介质然后再导入介质，则 **IDB** 中的说明将替换为介质中的说明。

还会更改介质标签的说明部分，但条码部分仍保持相同。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。
3. 在结果区域中，双击含有要更改的介质说明的介质池。此时将显示介质池中介质的列表。
4. 右键单击含有要更改的说明的介质，然后单击 **属性** 以打开该介质的“常规”属性页。
5. 在“说明”文本框中，键入介质的新说明。
6. 单击 **应用** 确认。

## 修改介质位置

介质位于设备之外时，指定介质位置有助于查找介质。位置信息存储在 **IDB** 中。初始化介质时应输入位置，而将介质移至不同位置(保管)，例如场外存储(“Shelf 4-Box 3”)时应修改位置。

位置从不写入介质头。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，展开 **介质**，然后单击 **池**。
3. 在结果区域中，双击含有要更改的介质位置的介质池。此时将显示介质池中介质的列表。
4. 右键单击含有要更改的指定位置的介质，然后单击 **更改位置** 以打开向导。

5. 指定介质的新位置。
6. 单击**完成**退出向导。

## 创建位置列表

可以创建常用预定义保管位置的列表。在不同介质管理任务(例如格式化介质时)中为特定介质选择位置时，即出现此预定义保管位置列表。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在“编辑”菜单中，单击**位置**。
3. 输入所需的位置，然后单击**添加**按钮。重复此步骤，输入多个位置。
4. 单击**完成**。

## 设置介质位置优先级

如果要恢复、复制、合并或验证的对象版本存在于多个介质集上，则任何介质集都可用于操作。默认情况下，**Data Protector** 自动选择最合适的介质集。通过指定介质位置的优先级可以影响介质集的选择。

如果设置了介质位置优先级，则如果多个介质集同样符合介质集选择算法的条件，则 **Data Protector** 将使用优先级最高(优先级 1 为最高，优先级 **None** 为最低)的介质集。

可以在还原、对象副本、对象合并或对象验证会话级别取代介质位置优先级。

以下内容可能会提供其他信息：

- 默认情况下，仅当两个或更多介质集的评级相同时，才会考虑介质位置优先级。为使介质位置优先级优先于其他选择因素，请将全局选项 **UserSpecifiedMediaPriorityHasHigherImportance** 设置为 1。
- 为使介质位置优先级生效，必须指定每个介质的位置。可以对单独或多个介质进行此操作。
- 介质位置优先级不考虑使用介质复制功能获取的副本。仅当原始介质(用作源进行复制的介质)不存在或不能用时，才使用此类副本。

### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**介质**，然后单击**位置**。
3. 在结果区域中，双击某个位置以显示其属性。
4. 在**位置优先级**下拉列表中，选择一个可用数字，其中 1 表示最高优先级。
5. 单击**应用**确认选择。

## 保管介质

建议制作备份数据的副本用于保管，并在站点上保留原始介质以便可以进行还原。Data Protector 允许以交互方式创建或自动创建介质上数据的其他副本。

### 先决条件

- 配置备份规范时，需要具备所需的数据保护和编目保护策略集。
- 需要在 Data Protector 中配置保管库。使用指示将从中保留介质的物理位置的名称。

### 步骤

1. 在 Data Protector Manager 中，更改要存储的介质的位置。
2. 从设备弹出介质，然后将介质存储在保管库中。

## 擦除介质

此功能仅对磁光盘可用。使用此功能在备份会话之前擦除磁光盘，并因此可加快备份速度。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。
3. 在结果区域中，双击含有要擦除的介质的磁光设备。
4. 右键单击该介质，然后单击 **擦除** 以打开向导。
5. 选择 **在操作完成之后弹出介质** 选项(可选)。
6. 单击 **完成** 擦除介质，然后退出向导。

此时“会话信息”消息将显示擦除操作的状态。

## 检测写保护介质

通过将写入保护开关设置为打开，Data Protector 可以检测和处理通过机械方式保护的介质。

以下操作可以检测和处理写保护介质：

- 只读操作，如列表、扫描和验证。只读操作可检测写保护介质，并在没有任何警告的情况下进行操作。
- 写操作，如初始化、擦除和备份。写操作可检测写保护介质，并会中止会话，或跳过写保护介质。备份会话将写保护介质视为不可用介质，并按照介质分配策略行动。如果分配策略为严格，则发出装载请求。如果分配策略为宽松，则跳过该介质。

对写入保护介质的检测和对该介质的写入保护状态的所有更改都将被记录到 media.log 文件中。



**注意：**  
建议不要将写保护介质用于 Data Protector。

## 关于装载请求

装载请求是让您向设备中插入介质的一种屏幕提示。通过提供所需介质答复装载请求后，会话即可继续。

Data Protector 在以下情况下会发出装载请求：

- 指定的介质不可用。如果预分配列表用于备份，或恢复所需的介质缺少介质，则会发生此情况。
- 没有合适的介质可用。如果池内当前位于库中的介质不合适，如果独立设备中的介质不合适，或如果设备为空，则会发生此情况。
- 邮件插槽打开。在这种情况下，必须关闭邮件插槽。

Data Protector 将自动选择最适于备份的介质。必须了解为备份选择介质的方式。

## 关于带库特有的介质管理

Data Protector 为复杂设备(如库)提供某些特定的介质管理任务，以简化对大量介质的管理。

某些任务(例如选择、复制、回收或移动介质以及修改介质位置)遵循标准过程。其他任务(如添加或删除插槽以及放入、弹出、验证、格式化、导入、扫描或擦除介质)可能取决于所使用的设备类型。

在支持条码的库中，Data Protector 可以根据条码生成介质说明，并在初始化期间将其写入磁带上的介质头。

## 其他应用程序使用带库介质

库中(尤其是在 ADIC/GRAU 和 StorageTek 等非常庞大的库中)的介质可以由许多应用程序使用，而不仅由 Data Protector 使用，因此必须了解哪些应用程序使用哪些介质以防覆盖介质。

理想情况下，专门将库与 Data Protector 配合使用，并允许 Data Protector 管理完整库。但是，如果有多个应用程序使用库，则应小心谨慎地向 Data Protector 和其他应用程序分配不重叠的介质子集。Data Protector 自身保持独立的介质分配策略。这表示如果已将某个特定的介质分配给 Data Protector(添加到 Data Protector 介质池)，则在其生存期期间或直到从 Data Protector 介质池将其删除为止，该介质都受到 Data Protector 的控制。

**重要：**  
对于每种类型的介质，都必须在 Data Protector 中配置一个库。虽然 ADIC/GRAU 或 StorageTek 系统可以存储许多在物理上不同类型的介质，但 Data Protector 只能识别仅含其中一种介质类型的库。因此，必须在系统中为每种介质类型都创建一个 Data Protector 库。

以下内容可能会有所帮助：

- 对于 ADIC/GRAU DAS 和 StorageTek 库，使用 Data Protector 命令处理介质。如果使用 ADIC/GRAU DAS 或 StorageTek ACS 命令手动处理介质，则 Data Protector 将无法跟踪介质上位置或信息的更改。
- 用 Data Protector 管理整个库。这样将进行集中式管理，其中可以跟踪库中的 Data Protector 和非 Data Protector 介质。
- 为每种介质类型至少创建一个介质池，例如一个池用于 4mm 介质类型，一个池用于 3480 介质类型。根据您所处的环境，可能要创建更多介质池，例如每个部门一个介质池。
- 确保 Data Protector 和其他应用程序不使用相同介质集。

## 关于用于 ADIC/GRAU DAS 或 STK ACS 库的 Data Protector 查询操作

启动 Data Protector 查询操作后，将查询 DAS 或 ACS Library Server 上配置的所有介质，即使在 Data Protector 中将介质配置为属于多个逻辑 ADIC/GRAU DAS 或 STK ACS 库(相同物理库的)时也是如此。此外，Data Protector 查询操作还查询在 DAS 或 ACS Library Server 上配置用于 Data Protector 以外应用程序的介质。因此，在 Data Protector 中启动查询操作之后，属于其他逻辑 ADIC/GRAU DAS 或 STK ACS 库的介质(启动查询操作的之外)将被移至启动该查询操作的逻辑 ADIC/GRAU DAS 或 STK ACS 库中。

因此，对于 ADIC/GRAU DAS 或 STK ACS 库，建议不要使用 Data Protector 查询操作。建议使用 Data Protector 添加 volser 操作手动添加 volser，而非使用 Data Protector 查询操作同步 IDB。

### 注意：

当不使用 Data Protector，而是使用 ADIC/GRAU DAS 实用程序配置逻辑库时，本节中的信息不适用于 ADIC/GRAU DAS 库的情况。如果使用 ADIC/GRAU DAS 实用程序配置多个逻辑库，则可以在此类库上安全地使用 Data Protector 查询操作。

## 添加插槽

Data Protector 全面支持处理库所用的介质池中的插槽和介质。添加插槽将为存储设备的介质配置一个位置。

在某些库中，配置库后将自动检测和添加插槽。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。
3. 在结果区域中，右键单击库的名称，然后单击 **属性**。
4. 单击 **存储库** 选项卡，指定要用于 Data Protector 的插槽，然后单击 **添加** 将插槽添加到列表中。使用短划线可一次输入多个插槽，例如 5-12。

请确保使用带库所支持的格式。例如，向 SCSI 带库添加插槽时，请勿使用字母或以零开头。

5. 单击 **应用** 确认。

## 删除插槽

Data Protector 全面支持处理库所用的介质池中的插槽和介质。删除插槽将阻止 Data Protector 使用和访问存储库中的插槽。并将从 IDB 中删除有关插槽的信息。

仅支持对任何设备上的空插槽删除介质插槽。

此操作不会影响 GRAU DAS 库中的 volser，而只会从 IDB 中删除特定介质。因此，Data Protector 不知道存在这些介质，并且不使用这些介质。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。
3. 在结果区域中，右键单击库的名称，然后单击 **属性**。
4. 单击 **存储库** 选项卡，选择要删除的插槽，然后单击 **删除**。
5. 单击 **应用** 确认。

此时插槽列表中不再显示该插槽。

## 放入介质

放入介质意味着将其以物理方式放入库存储库中，并自动将所添加的介质注册为库的成员。

可以选择要使用的插槽。放入介质不会影响其所属的介质池。

建议使用 Data Protector GUI 放入介质。如果使用设备的控制机构手动放入介质，则 IDB 中的信息将不再一致，并且必须扫描设备以更新此信息。

**提示：**  
可以在一个操作中将多个介质放入设备中。

## 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中双击带库的名称。
4. 双击 **插槽**，以便在结果区域中显示插槽的列表。
5. 右键单击要从中放入介质的插槽(或多个插槽)，然后单击 **放入** 以启动会话。

此时将提示您根据需要将其他介质插入设备。

## 弹出介质

弹出介质意味着将其以物理方式从存储库插槽转移到带库设备中的插入/弹出区域(也称为邮件插槽)。

建议使用 **Data Protector Manager** 弹出介质。 如果使用设备的控制机构手动弹出介质，则 IDB 中的信息将不再一致。 要更新此信息，请扫描设备。

当介质因邮件插槽已满而无法弹出时，**Data Protector** 将重试该操作，直到邮件插槽变为空闲或直到预定义的时间限制到期为止。 此重试期间，其他会话可访问机械手。

执行弹出期间，其他会话无法使用所指定的任何介质。

## 批量弹出介质

通过单一操作可从库中弹出多个介质。 介质已满时，**Data Protector** 会指示您从邮件插槽取出介质，为选择要弹出的其他介质腾出空间。

## 预定义介质弹出

对于某些操作(如自动介质复制)，可以在会话完成之后指定是否将自动弹出介质。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。 此时将在结果区域中显示所配置设备的列表。
3. 在结果区域中双击带库的名称。
4. 双击**插槽**项，以便在结果区域中显示插槽的列表。
5. 右键单击要弹出的插槽(或多个插槽)，然后单击**弹出**以打开向导。
6. 指定介质的新位置(可选)。
7. 单击**完成**弹出介质，然后退出向导。

此时“会话信息”消息将显示弹出操作的状态。

## 擦除带库设备中的介质

擦除介质仅对磁光盘可用。 只能在备份会话之前擦除磁光盘介质。 这样可加快备份速度。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，单击 **设备**。
3. 在结果区域中，双击含有要擦除的介质的磁光设备。 此时将显示“插槽”和“驱动器”项。
4. 双击**插槽**。
5. 右键单击含有擦除的介质的插槽，然后单击**擦除**以打开向导。
6. 在交换器将从中加载要擦除的介质的库中选择驱动器。
7. 单击**完成**擦除介质，然后退出向导。

此时“会话信息”消息将显示擦除操作的状态。

## 手动添加 Volser

对于 ADIC/GRAU DAS 或 STK ACS 库，可以手动将 volser 添加到 Data Protector 中所配置的库，而非对库进行查询。对于 ADIC/GRAU DAS 或 STK ACS 库，当为同一个物理库配置了多个逻辑库后，建议采用此方法将 volser 添加到在 Data Protector 中所配置的库。但是，对于 ADIC/GRAU DAS 库，在不使用 Data Protector 而使用 ADIC/GRAU DAS 实用程序配置逻辑库时，可以安全地在此类库上使用 Data Protector 查询操作代替手动添加 volser。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在范围窗格中，浏览要向其添加 volser 的库，然后将其展开。
3. 右键单击 **插槽**，然后从弹出菜单中选择 **添加 Volser**。
4. 在“前缀”文本框中，输入 volser 的前缀。通常由三个字母组成。  
在“从”文本框中，指定要添加到库的 volser 范围的起始数字。  
在“到”文本框中，指定要添加到库的 volser 范围的结束数字。
5. 单击“完成”，将 volser 添加到 IDB。

## 查询 ADIC/GRAU DAS 和 StorageTek ACSLM 主机

要从服务器获取有关 ADIC/GRAU 或 StorageTek 库中存储库的信息，可以查询 DAS 或 ACSLM 主机(服务器)。查询用服务器的介质数据库的内容做出响应，然后将 IDB 中的信息与存储库中的实际信息进行同步。

如果已使用 GRAU DAS 或 StorageTek ACS 命令管理介质，则此操作非常有用，因为前者会导致与 IDB 的不一致 — Data Protector 不知道库存储库中介质的最新状态。

### 限制

如果在存储库中对 ADIC/GRAU 库配置了多于 3970 个 volser，则无法成功完成 volser 扫描。解决此问题的方法是配置多个逻辑 ADIC/GRAU 库，以便将大型存储库中的插槽隔离为多个较小的存储库。

#### 重要：

对于 ADIC/GRAU DAS 和 STK ACS 库，当为同一个物理库配置了多个逻辑库时，建议不要查询 DAS 或 STK ACSLM Server。请手动添加 volser。但是，对于 ADIC/GRAU DAS 库，当不使用 Data Protector 而使用 ADIC/GRAU DAS 实用程序配置逻辑库时，可以安全地在此类库上进行 Data Protector 查询操作。

### 步骤

1. 在上下文列表中，单击 **设备和介质**。
2. 在已配置设备的列表中，右键单击要查询的库，然后单击 **查询**。

此操作将查询 DAS 或 ACSLM 主机中的信息。

# 第 10 章：备份

## 关于备份

备份是在备份介质上创建系统数据副本的过程。此副本将存储和保留起来，供以后原始数据在发生损坏时使用。

备份会话以备份规范为基础，而且能够以交互方式启动。在备份会话期间，**Data Protector** 读取备份对象，通过网络传输其数据，然后将其写入设备中的介质。

### 重要：

请确保备份的数据前后一致。例如，可能会在备份之前关闭应用程序，或将其置于“备份”模式以避免备份期间数据发生更改。如果所备份的数据前后不一致，则在还原和尝试使用数据时可能会遇到意外的结果。

**Data Protector** 备份的高级功能包括：

- 自动平衡设备的使用情况(负载均衡)
- 备份共享磁盘
- 安排无人看管备份
- 同时进行完全备份和增量备份以节省时间和介质
- 允许以多种不同的方式组织备份
- 使用对象镜像功能同时备份到多个位置

**Data Protector** 帮助中提供的过程假定您使用根据可供备份或模板使用的数据类型所设置的默认备份视图(按类型)。

有关如何备份 **Oracle**、**SAP R/3**、**Microsoft Exchange Server**、**Microsoft SQL Server**、**Informix Server**、**IBM DB2 UDB** 或 **Sybase** 等数据库应用程序的信息，请参见 ***Data Protector** 集成指南*。

## 设置备份视图

可以根据需要设置备份视图。默认备份视图是**按类型**。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，选择一个可用视图。

根据已选的视图显示“备份”上下文。

## 备份类型

**Data Protector** 提供两种基本的文件系统备份类型：完整备份和增量备份。这些备份类型适用于整个备份规范，并仅适用于文件系统对象。

要组合使用完整和增量备份，请确保备份对象拥有完全相同的：

- 客户机名称
- 驱动器/装载点
- 说明
- 所有者(适用于私有对象)

如果执行交互式备份，则会提示您选择备份类型。安排备份时，在计划向导中指定备份类型。例如，可以创建一个日程安排，对相同的备份规范在周六执行完整备份，在所有工作日执行 **Incr1** 备份。

## 完整备份

完整备份始终备份所选的全部对象，即使从上一次备份以来没有更改也是如此。对象的第一个备份始终是完整备份。如果备份时不存在具有相同所有权的受保护完整备份(适用于专用对象)，则任何后续备份都将以完整备份的形式执行。

## 增量备份

增量备份备份自上次仍受保护的(完整或增量)备份以来的更改。必须存在对象的完整备份(客户机名称、装载点、说明和所有者完全相同)，然后才能对该对象进行增量备份。

## 增量备份的类型

**Data Protector** 提供不同类型的增量备份。

- 增量  
简单的增量备份基于仍受保护的上次备份，后者可以是完整备份或增量备份。
- 增量 1-9  
分级增量备份取决于低一级别仍受保护的上一次备份。例如，**1** 级增量备份保存自上次完整备份以来的所有更改，而 **5** 级增量备份保存自上次 **4** 级增量备份以来的所有更改。**Incr1-9** 备份永不引用现有的 **Incr** 备份。
- 差异  
在 **Incr1** 备份的某些应用程序集成中使用的术语。差异备份将保存从上次完整备份以来所做的所有更改。

## 高级备份解决方案

**Data Protector** 还提供高级备份解决方案，如增强型增量备份和合成备份。

## 完整备份和增量备份

提高备份性能的基本方法是减少所备份数据的量。规划完整备份和增量备份时，应充分利用时间和资源。通常不需要在同一天对所有系统都执行完整备份。

请考虑以下有关备份类型的内容：

	完整备份	增量备份
资源	需要比增量备份更多的时间，并且需要更多介质空间。	仅备份自上次备份以来发生的更改，这样需要的时间和介质空间较少。
设备处理	如果使用只有一个驱动器的独立设备，则在备份不适合单个介质时需要手动更换介质。	但备份不大可能需要额外的介质。
还原	可实现简单且快速的还原。	由于所需的介质较多，因此还原需要较长时间。
对 IDB 的影响	占据 IDB 中的更多空间。	占用 IDB 中的空间较少。

**注意：**  
必须设置适当的数据保护以确保所有需要的完整备份和增量备份可供还原。如果数据保护设置得不正确，则可能会覆盖某些介质，这会导致还原链中断。

## 传统增量备份

### 传统增量备份的工作方式

在运行备份对象的增量备份之前，**Data Protector** 将备份对象中的树与此对象的有效还原链中的树进行比较。如果树不匹配(例如，选中了备份对象中上次备份时尚不存在的其他目录进行备份，或者存在备份对象相同、树不同的多个备份规范)，将自动执行完整备份。这可确保备份中包括全部所选文件。

### 检测更改

对于传统的增量备份，确定某文件自上次备份以来有没有更改的主要标准是该文件的修改时间。但是，有一些情况下此标准无效。例如，如果将某个文件重命名、移至新位置或改变了其部分属性，其修改日期不会更改。因此，在增量备份中并不总是备份该文件。而是在下次完整备份中备份此类文件。

增量备份中是否备份名称、位置或属性发生更改的文件，还取决于备份规范中以下选项的设置。首选设置可改善对更改的检测。

**Windows 系统：** 不使用归档属性

默认情况下，不选择此选项(使用存档属性)。这是首选设置。

**UNIX 系统：** 不保留访问时间属性

默认情况下，不选择此选项(保留访问时间属性)已首选此选项。

您可以使用 **Windows NTFS** 更改日志提供程序执行传统增量备份。在此情况下，将使用 **Windows** 更改日记生成自上次完整备份以来已修改的文件的列表，而不执行文件树遍历。使用更改日志提供程序可提高增量备份的总体性能，方式与其提高增强型增量备份性能的方式相同。如果由于某种原因而无法使用更改日志提供程序，则会执行常规的传统增量备份。



要可靠地检测和备份重命名和移动过以及属性发生更改的文件，请使用增强型增量备份。

## 增强型增量备份

对于传统的增量备份，确定某文件自上次备份以来有没有更改的主要标准是该文件的修改时间。但是，有一些情况下此标准无效。例如，如果将某个文件重命名、移至新位置或改变了其部分属性，其修改日期不会更改。因此，在增量备份中并不总是备份该文件。而是在下次完整备份中备份此类文件。

增强型增量备份能可靠检测和备份重命名过的、移动过的和属性更改过的文件。

能否检测到某些更改(如权限或 ACL 的更改)还取决于备份规范中以下选项的设置。首选设置可使增强型增量备份最大程度地检测到更改。

- **Windows 系统：**不使用归档属性

默认情况下，不选择此选项(使用存档属性)。这是首选设置。

- **UNIX 系统：**不保留访问时间属性

默认情况下，不选择此选项(保留访问时间属性)该选项在被选中时为首选设置。

部分选择备份的树变更时，使用增强型增量备份就无需对整个备份对象进行完整备份。例如，如果自上次备份以来选择了其他目录进行备份，则将执行该目录(树)的完整备份，而对剩余部分进行增量备份。

此外，还可以使用 **Windows NTFS** 更改日志提供程序，执行增强型增量备份。在此情况下，将使用 **Windows** 更改日记生成自上次完整备份以来已修改的文件的列表，而不执行文件树遍历。使用更改日志提供程序可提高增量备份的总体性能，尤其是在文件众多但其中仅有一小部分文件发生变化的环境中。

## 为什么使用增强型增量备份

使用增强型增量备份是为了：

- 确保对名称、位置或属性发生更改的文件进行增量备份。
- 在仅所选的某些树发生更改时消除不需要的完整备份。
- 实现后续的对象合并(合成备份)。

## 对磁盘空间消耗的影响

增强型增量备份在所备份的每个客户机上使用一个小数据库。会对每个文件系统装载点都创建数据库。增强型增量备份存储库位于以下目录中：

- **Windows 系统：** `Data_Protector_home\enhincrd\MountPointDir`

通过将任何“.”(冒号)和“\”(反斜杠)字符替换为“\_”(下划线)字符，并删除结尾的“.”或“\”，可从装载点获取装载点目录 (MountPointDir)。

- **HP-UX 和 Linux 系统：** `/var/opt/omni/enhincrd`

对客户机上磁盘空间的影响通常小于选择进行备份的文件大小的 1%。确保定期清除增强型增量备份数据库。可以通过设置 `OB2_ENHINC_DELETE_INTERVAL` 和 `OB2_ENHINC_DELETE_THRESHOLD` omnic 选项来执行此操作。

### 磁盘代理并发

多个磁盘代理可能会同时访问增强型增量备份数据库。要避免可能出现的备份问题，请通过设置以下 `omnirc` 选项来配置磁盘代理行为：

- `OB2_ENHINC_LOCK_TIMEOUT`
- `OB2_ENHINC_SQLITE_MAX_ROWS`
- `OB2_ENHINC_MAX_MEMORY_LIMIT`

## 限制

- 仅目录级别支持增强型增量备份。如果逐个选择文件进行备份，则将不使用增强型增量模式。
- 使用增强型增量模式时，硬链接检测被禁用。

## 使用更改日志提供程序的增量备份

传统的增强型增量备份通过执行文件树遍历生成要备份的文件的列表。这个过程可能会占用相当长的时间，尤其是目录结构很大且包含大量文件的情况。**Windows NTFS 更改日志提供程序**(基于 **Windows 更改日记**)解决此问题的方式为向更改日记查询发生更改的文件的列表，而非执行文件树遍历。更改日记能够可靠地检测并记录对 **NTFS** 卷上文件和目录所做的全部更改，因此 **Data Protector** 可使用它作为一种跟踪机制，以生成自上次完整备份以来已修改的文件的列表。这对于具有大型文件系统但在两次备份之间仅有少量文件发生更改的环境大有裨益。在这种情况下，可以用短得多的时间完成确定哪些文件发生更改的过程。

每个 **NTFS** 卷都有自己的更改日记数据库。对文件或目录做出一次更改，就会向日记追加一条记录。记录中标明了更改的文件名、时间和类型。请注意，日记中并不保留发生更改的实际数据。如果日记文件变得过大，则系统会清除日记开头处最旧的记录。如果已从更改日记中清除了备份所需的数据，则 **Data Protector** 将执行完整备份，并发出无法使用更改日记的警告。

在使用更改日志提供程序的增量备份中是否备份某个文件，取决于在备份规范中是否设置了如有可能，请使用本机文件系统更改日志提供程序选项。如果指定了此选项，则 **Data Protector** 尝试使用“更改日记”。如果“更改日记”处于不活动状态，则 **Data Protector** 会发出一个警告。如果在增强型增量备份过程中发生这种情况，则改为执行完整备份。如果在传统增量备份过程中发生这种情况，则改为执行常规增量备份。自动设置不保留访问时间属性和不使用归档属性选项，并且不能禁用这两个选项。

## 先决条件

- 使用 `omnicjutil -query` 命令确保在所需的卷上激活更改日记。如果更改日记不活动，请通过运行 `omnicjutil - start` 启动更改日记。有关 `omnicjutil` 命令的详细信息，请参见位于该 `Mount_point/DOCS/C/MAN` 目录的安装包中的 **Data Protector** 命令行界面参考。
- 确保至少存在一个完整备份(在备份规范中选择了**使用本机文件系统更改日志提供程序(如果有)**选项)，然后再使用更改日志提供程序启动增强型增量备份。

## 性能损失和磁盘空间消耗

要达到更改日志提供程序的最佳性能，请在启动备份(备份类型为 **Incr**)时使用增量备份。也支持 **Incr1-9**，但性能可能会降低一些。

打开后，更改日记会消耗一些 **CPU** 时间和磁盘空间。所消耗的磁盘空间限制为 **4 GB**。可以设置更改日记的最大大小，以及当日记达到其最大大小时对其要截断的大小。有关详细信息，请参见 *Data Protector* 命令行界面参考。

要优化更改日志提供程序的性能，可以使用 **OB2\_CLP\_MAX\_ENTRIES omnirc** 选项指定更改日志提供程序在内存中可容纳的条目数。有关详细信息，请参见《*Data Protector 故障排除指南*》。

在以下情况下，**Data Protector** 执行完整备份，并忽略在备份规范中设置更改日志提供程序选项：

- 如果在客户机系统上更改日记不活动。
- 如果已从更改日记清除了所需的数据。
- 如果更改日记 ID 与原先不同(这意味着另一个应用程序已删除然后又重新创建了更改日记)。

默认情况下，首次执行更改日志提供程序时，它不会创建增强型增量存储库。这意味着更改日志提供程序首次发生错误时将执行完整备份，而此过程将创建增强型增量存储库。可以通过 **OB2\_CLP\_CREATE\_EI\_REPOSITORY omnirc** 选项更改此行为。有关详细信息，请参见《*Data Protector 故障排除指南*》。

## 注意事项

- **Data Protector** 对更改日记没有独占访问权限。这意味着，通过激活或取消激活更改日记，其他应用程序也会影响 **Data Protector**。如果在给定卷上禁用更改日记，则不会向日记中记录任何文件和目录更改。默认情况下，**NTFS** 卷禁用了其更改日记，因此必须使用 **cjutil** 或 **omnicjutil** 命令显式将其激活。同时，任何其他应用程序都可以随时激活或禁用卷的日记。有关更改日记的详细信息，请参见 **Windows** 文档。

请注意，在 **Windows Vista**、**Windows 7**、**Windows 8**、**Windows Server 2008** 和 **Windows Server 2012** 中，默认情况下更改日记处于活动状态。

- 在文件系统中只有少量更改的环境下，使用更改日志提供程序大有裨益。如果要备份包含许多更改(例如，含有创建并在创建不久后删除的许多临时文件)的文件系统，则对树进行普通遍历更快。
- **Windows** 更改日记 **API** 不提供有关属性的详细信息。所有属性更改都组合在一起。使用 **API** 时，无法确定更改日记中的条目是由要清除的存档属性还是上次访问时间中的更改所引起。

更改日志提供程序不清除存档属性。备份文件之后，**Data Protector** 的正常行为是清除存档属性。因此，使用更改日志提供程序时，将自动选中**不使用存档属性**选项。

备份文件之后，**Data Protector** 的正常行为是重置上次访问时间(因为备份过程总是会更改上次访问时间)。更改日志提供程序不会将其重置，因此将自动选中**不保留访问时间属性**选项。

自动选择这两个选项的原因是为了避免多次备份相同文件的情况。如果清除了存档属性或重置了上次访问时间，则在更改日记中显示一个条目，并在下次会话中备份文件，即使尚未更改文件也是如此。

- 需要使用 `cjutil - query` 命令不时地监控 NextUsn 数字，并在 NextUsn 接近 MaxUsn 数字时重新启动更改日记。
- 如果已更改了备份规范，则完整地备份所有新树。这意味着对所有新树执行普通树遍历，而对旧树使用更改日志提供程序。
- 如果重命名备份空间下的目录，则将对该目录执行普通树遍历。

## 限制

- 仅支持对 Windows NTFS 进行备份。

## 合成备份

合成备份是一种高级备份解决方案，无需运行定期的完整备份。在初始完整备份之后，只需要运行增量备份，然后与完整备份合并为一个新的合成完整备份。此过程可以无限重复，不再需要运行完整备份。在还原速度方面，此类备份与传统的完整备份相当。

Data Protector 用一种名为对象合并的操作执行合成备份。

## 如何执行合成备份

合成备份过程由以下步骤组成：

1. 在用于完整备份和增量备份的备份规范中，启用**增强型增量备份**选项。
2. 执行完整备份。
3. 配置后续的增量备份，使其写入一个文件库或 B2D 设备(智能缓存除外)
4. 当存在至少一个增量备份时，执行对象合并。执行对象合并的频率取决于备份策略。

## 虚拟完整备份

虚拟完整备份是一种更高效的合成备份类型。此解决方案用指针合并数据，而非复制数据。因此，合并所用时间更短，并且避免了对数据不必要的复制。

该过程与常规合成备份基本相同，但有以下额外要求：

- 所有备份(完整备份、增量备份和所产生的虚拟完整备份)均必须写入一个文件库。
- 文件库必须使用分布式文件介质格式。

### 注意：

通过虚拟完整备份，可以减少空间消耗，因为对象共享相同的数据块。但是，如果数据块损坏，可能会影响多个对象。为提高可靠性，请将文件库放置在 RAID 磁盘上。

## 标准备份过程

标准备份过程由以下几个部分组成：

- 选择要备份的数据。
- 选择要将这些数据备份到的位置。
- 选择要额外创建多少备份副本(镜像)。
- 开始或安排备份会话。

与此同时，创建备份规范。通过设置各种选项(使用默认值或将其设置为满足特定需要)定义如何备份的详细信息。

要更改这些预定义的设置，请指定：

- 目标备份规范中所有对象的备份选项，如 **pre-exec** 和数据保护
- 希望执行备份的日期和时间

## 先决条件

- 需要在要备份的每个系统上都安装磁盘代理，除非使用 **NFS**(在 **UNIX** 系统中)或执行网络共享备份(在 **Windows** 系统中)备份这些系统。
- 至少需要在 **Data Protector** 单元中配置一个备份设备。
- 需要将介质做好备份的准备。
- 需要具有执行备份的相应用户权限。

## 文件系统备份

对于每个文件系统，可以限制对特定的几个目录树进行备份。对于每个目录树，可以：

- 排除任何子树或文件
- 备份符合特定通配符模式的文件
- 跳过符合特定通配符模式的文件

例如，软件应用程序永久使用某些文件。应从文件系统备份中排除这些文件，并应以特殊方式备份这些文件。

## 创建备份规范

备份规范定义要备份的客户机、磁盘、目录和文件；要使用的磁带设备或驱动器；其他备份副本(镜像)的数量；备份选项；以及时间安排信息(希望何时执行备份)。备份规范可以像将一个磁盘备份到独立 **DDS** 驱动器一样简单，也可以像指定将 **40** 台大型服务器备份到含有 **8** 个驱动器的磁带库一样复杂。

## 限制

- **Data Protector GUI** 可显示的备份规范数量是有限的。可显示的备份规范数量取决于备份规范的参数大小(名称、组、所有权信息以及备份规范是否为负载均衡的信息)。此大小不应超过 **80 KB**。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击要备份的项目类型(例如**文件系统**)，然后单击**添加备份**。
4. 在**创建新备份**对话框中，选择一个可用的模板以及备份类型，然后根据需要指定其他选项。单击**确定**打开向导。
5. 在零宕机时间备份的情况下，此时将显示“配置”页。配置集成，然后单击**下一步**。
6. 在集成备份的情况下，选择客户机和应用程序数据库。单击**下一步 (Next)**。
7. 在“源”属性页中，展开包含要备份的对象的系统，然后选择要备份的内容。

### 重要：

在 UNIX 系统中，如果要执行即时恢复，请选择要备份的卷组中的所有文件系统。否则，将无法使用 **Data Protector GUI** 进行即时恢复，或者(如果使用 **Data Protector CLI** 执行即时恢复)会损坏数据。

单击**下一步 (Next)**。

8. 在“目标”属性页中，选择将用于备份的设备。

还可以指定是否要在备份会话期间额外创建备份的其他副本(镜像)。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。无法使用 ZDB 到磁盘或 NDMP 来镜像备份的对象。

### 提示：

如果备份经过负载均衡，则通过右键单击所选的设备并单击**给设备排序**，可以设置 **Data Protector** 使用设备将采用的顺序。

单击**下一步 (Next)**。

9. 在“选项”属性页中，可以设置备份选项。可用的备份选项取决于所备份的数据类型。例如，磁盘映像备份并不具有文件系统备份所具有的所有备份选项。单击**下一步 (Next)**。
10. 在“备份摘要”页中，检查备份规范的摘要。建议首先保存备份规范，然后再开始预览。预览不可用于 **Data Protector** 内部数据库备份、特定 **Data Protector** 应用程序集成的备份会话以及零宕机时间备份 (ZDB)。单击**下一步 (Next)**。
11. 在备份向导的结尾处，可以保存、保存并计划、开始或预览所配置的备份。此时会发生以下情况：
  - 如果保存所配置的备份，则它以新备份规范的形式出现在范围窗格的备份上下文中。随后可以预览或不修改即开始所保存的备份，或者可以修改该备份，然后再预览或开始该备份。
  - 如果保存并计划所配置的备份，请首先保存备份规范，然后打开“调度程序”页面，在其中可以指定必须运行此保存的备份规范的日期和时间。
  - 如果开始或预览所配置的备份，则“会话信息”消息将显示备份的状态。

### 提示：

通过复制现有规范，然后修改某个副本，可以创建多个备份规范。

## 修改备份规范

可以修改已配置和保存的备份规范。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 单击要修改的备份规范。
4. 在“源”属性页以及其他属性页(“目标”、“选项”和“日程”)中修改备份规范，然后单击**应用**。

修改备份后，即可在**操作**菜单中预览或开始该备份。

#### 注意：

预览不可用于 **Data Protector** 内部数据库备份、特定 **Data Protector** 应用程序集成的备份会话以及零宕机时间备份 (ZDB)。

#### 提示：

修改备份规范、执行备份然后选择对象进行还原时，仅选择上一个版本中备份的文件和目录进行还原。要更改备份版本，请右键单击对象，然后单击**选择版本**。

## 预览和启动备份

可以预览备份以验证您的选择。预览不从选择进行备份的磁盘中读取数据，也不将数据写入为备份配置的设备中的介质。但是，预览将检查通过所使用的基础架构进行的通信，并确定数据大小和目标处是否有介质。

向 **Data Protector** 提供所有备份的信息之后，可以启动现有的(已配置和保存)备份。

### 限制

- 预览不可用于 **Data Protector** 内部数据库备份以及特定 **Data Protector** 应用程序集成的备份会话。
- 预览不可用于零宕机时间备份 (ZDB)。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 选择要启动或预览的备份规范。
4. 在**操作**菜单中，如果要预览备份，则单击**预览备份**，或单击**启动备份**以启动该备份。
5. 在“预览或启动备份”对话框中，选择备份类型(完整或增量；对于特定集成还有某些其

他备份类型)和网络负载。

在 ZDB 到磁盘 + 磁带或 ZDB 到磁盘(启用了即时恢复)的情况下，指定分割镜像/快照备份选项。

6. 单击**确定**预览或启动备份。

此时“会话信息”消息将显示备份的状态。

**提示：**

配置新备份时，可以在备份向导的结尾处启动交互式备份或交互式预览。

## 中止备份

中止备份会话可终止备份会话。仅对中止会话之前备份的数据将存在备份副本。

### 步骤

1. 在“操作”菜单中，单击**中止**，以中止备份会话。

如果在中止备份会话时该会话仍在确定您选择进行备份的磁盘大小，则不会立即中止该会话。确定大小后即中止备份。

**提示：**

可以中止 Data Protector 监视器上下文中一个或多个当前正在运行的会话。

## 重新启动失败的备份

在备份会话期间，某些系统因其关闭、有某些临时网络连接性问题等等而不可用。这些情况导致无法备份某些系统或只能备份一部分，换句话说，某些对象失败。解决了妨碍的问题后，可以重新启动出现问题的会话。此操作只会重新启动失败的对象。

### 先决条件

- 您必须位于 Data Protector Admin 用户组中，或者获得了 Data Protector 监视用户权限。

### 注意事项

- 对于失败的文件系统和 Oracle Server 集成备份会话，您还可以使用恢复会话功能从会话失败的点开始继续备份。

### 限制

- 无法重新启动以交互方式运行(意味着它们是基于未保存的备份规范)的失败会话。
- 无法同时重新启动多个会话。

**重要：**

重新启动失败的备份会话之前不要更改备份规范。否则将无法重新启动所有对象。



## 步骤

1. 如果您使用的是普通 **Cell Manager**，在上下文列表中单击**内部数据库**。  
如果您使用的是管理器的管理器，在上下文列表中选择**客户机**，然后展开**企业客户机**。选择会话出现问题的 **Cell Manager**。从“工具”菜单中选择**数据库管理**，从而打开一个新 **Data Protector GUI** 窗口，并显示“内部数据库”上下文。
2. 在范围窗格中，展开**内部数据库**，然后单击**会话**。  
此时将在结果区域中显示会话的列表。每个会话的状态显示在“状态”列中。
3. 右键单击失败、中止或完成但发生过失败或出现错误的会话，然后选择**重新启动失败的对象**以备份失败的对象。
4. 单击**是**确认。

## 复制备份规范

可以复制已配置和保存的备份规范。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 在结果区域中，右键单击要复制的备份规范，然后单击**复制为**。此时将打开“将备份复制为”对话框。
4. 在“名称”文本框中，输入所复制的备份规范的名称。(可选)从“组”下拉列表中，选择所复制的备份规范所属的备份规范组。
5. 单击**确定**。

此时将在范围窗格中和结果区域中的新名称下显示所复制的备份规范。

## 删除备份规范

可以删除已配置和保存的备份规范。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 右键单击要删除的备份规范，然后单击**删除**。确认选择。

此时即从范围窗格的备份上下文中删除备份规范。

## 高级备份任务

可以用多种方式控制备份。Data Protector 提供一组适用于 Windows 和 UNIX 系统的高级备份任务。

### 先决条件

- 需要在要备份的每个系统上都安装磁盘代理，除非使用 NFS(在 UNIX 系统中)或执行网络共享备份(在 Windows 系统中)备份这些系统。
- 至少需要在单元中配置一个备份设备。
- 需要将介质做好备份的准备。
- 需要具有执行备份的相应用户权限。
- 在进行之前必须考虑标准备份过程。

### 什么是高级备份任务？

高级备份任务包括指定默认情况下不使用的某些选项或采取某些不遵循标准备份过程的操作。

- 选择网络共享磁盘进行备份
- 仅选择特定文件(匹配)进行备份
- 使文件跳过备份
- 选择启动备份的快捷方式位置
- 使用多个磁盘代理进行备份
- 执行磁盘发现的客户机备份
- 磁盘映像备份
- Web 服务器备份

## 选择网络共享磁盘进行备份

可以备份 Windows 共享磁盘上的数据。必须使用常规 Data Protector 磁带客户机才能通过共享磁盘备份其他远程系统。

使用共享磁盘方法进行备份是对无法以其他方式备份的系统进行备份的一种解决方法。建议不要将此方法作为主要备份方法。

在以下条件下，备份位于网络中共享的 Windows 系统上的文件系统：

- 如果系统不是 Data Protector 单元的一部分，并且未安装 Data Protector 磁带客户机。
- 如果要备份不由 Data Protector 直接支持的平台，如 Windows for Workgroups、Windows 3.1 系统或 Windows NT。

**提示：**

为了减少网络负载，磁带客户机客户应也是介质代理客户。否则，数据将在网络上传输两次。

## 先决条件

必须更改磁带客户机上的 **Data Protector Inet** 帐户，以便获得正确的权限以访问要备份的共享磁盘。此帐户必须具有同时访问本地客户机系统和远程共享磁盘的权限。对于早于 **Windows Vista** 和 **Windows Server 2008** 系统的 **Windows** 版本，帐户必须是特定用户帐户，而不能是本地系统帐户。

设置 **Inet** 服务的用户帐户后，即可备份共享磁盘，如同其位于本地系统上一样。

## Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012

必须添加一个对要备份的共享磁盘具有访问权限的用户帐户。此帐户必须是本地系统帐户。

必须满足这一先决条件，然后才能更改磁带客户机上的 **Data Protector Inet** 帐户。在将运行磁带客户机的 **Data Protector** 客户机上运行以下命令：

```
omniinetpasswd -add User@Domain [Password]
```

## 要求

- 必须使用备份向导映射共享驱动器。
- 使用 **Windows GUI**，因为 **UNIX GUI** 中不支持浏览 **Windows** 系统。

## 限制

- 备份共享磁盘并不备份所有文件属性。只能备份共享主机上可见的内容。可以还原数据，但可能会缺少某些文件/目录属性。
- 不支持使用 **VSS** 功能备份在网络共享卷上存储其数据的写入程序。此外，**Windows Server 2012** 也不支持在启用了磁带客户机和使用卷影副本选项的情况下备份网络共享或远程网络文件夹。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击要备份的项目类型(例如**文件系统**)，然后单击**添加备份**。
4. 在**创建新备份**对话框中，选择一个可用的模板，然后单击**确定**打开向导。
5. 在“源”属性页中，从下拉列表中选择**网络共享备份**(当 **GUI** 在 **Windows** 系统中运行时可用)。
6. 单击**映射网络共享**以打开**浏览网络共享**窗口。
7. 在“客户机系统”下拉列表中，选择具有将用于备份的磁带客户机的客户机系统。
8. 在“共享目录”框中，选择或指定共享磁盘，然后单击**确定**。如果要选择更多磁盘，请使用**应用**。

9. 在“源”属性页中，选择或指定要备份的共享文件系统。单击**下一步 (Next)**。
10. 在“目标”属性页中，选择将用于备份的设备。  
还可以指定是否要在备份会话期间额外创建备份的其他副本(镜像)。通过单击**添加镜像**和**删除镜像**按钮，指定所需的镜像数。分别为备份和每个镜像选择单独的设备。无法使用 ZDB 到磁盘或 NDMP 备份功能镜像对象备份。

**提示：**

如果备份经过负载均衡，则通过右键单击所选的设备并单击**给设备排序**，可以设置 Data Protector 使用设备将采用的顺序。

单击**下一步 (Next)**。

11. 在“选项”属性页中，可以设置备份选项。可用的备份选项取决于所备份的数据类型。例如，磁盘映像备份并不具有文件系统备份所具有的所有备份选项。  
在 Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012 中，执行额外的步骤：
  - a. 在“备份规范选项”下，单击**高级**按钮。
  - b. 在“备份选项”对话框中的“所有权”下，输入对将备份的共享磁盘具有访问权限的用户帐户的相关信息。
  - c. 单击**确定**。
12. 单击**下一步 (Next)**。
13. 在“备份摘要”页中，检查备份规范的摘要。建议首先保存备份规范，然后再开始预览。单击**下一步 (Next)**。
14. 在备份向导的结尾处，可以保存、保存并计划、开始或预览所配置的备份。此时会发生以下情况：
  - 如果保存所配置的备份，则它以新备份规范的形式出现在范围窗格的备份上下文中。随后可以预览或不修改即开始所保存的备份，或者可以修改该备份，然后再预览或开始该备份。
  - 如果保存并计划所配置的备份，请首先保存备份规范，然后打开“调度程序”页面，在其中可以指定必须运行此保存的备份规范的日期和时间。
  - 如果开始或预览所配置的备份，则“会话信息”消息将显示备份的状态。

对于所备份的每个磁盘都启动一个磁带客户机。如果同时启动过多备份，则这样可能会降低备份性能。

## 仅选择特定文件(匹配)进行备份

通过使用通配符，可以备份符合特定标准的文件。

**注意：**

Data Protector NDMP 服务器集成不支持此功能。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 选择具有目标对象的备份规范。
4. 单击**备份对象摘要**选项卡。
5. 在“备份对象摘要”页中，右键单击某个备份对象，然后单击**属性**。
6. 单击**树/筛选器**选项卡，然后单击**筛选器**按钮。
7. 在“仅”文本框中，输入要用于仅备份特定文件的标准，然后单击**添加**按钮。  
如果要使用更多标准，则重复此步骤。
8. 单击**确定**。

## 使文件跳过备份

通过使用通配符，可以使符合特定标准的文件跳过备份。

**注意：**  
Data Protector NDMP 服务器集成不支持使文件跳过备份。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 选择具有目标对象的备份规范。
4. 单击**备份对象摘要**选项卡。
5. 在“备份摘要”页中，右键单击某个备份对象，然后单击**属性**。
6. 单击**树/筛选器**选项卡，然后单击**筛选器**按钮。
7. 在“跳过”文本框中，输入要用于跳过某些文件(如 \*.tmp)的标准，然后单击**添加**按钮。  
如果要使用更多标准，则重复此步骤。
8. 单击**确定**。

## 选择启动备份的快捷方式位置

可以在磁盘上创建所选备份规范的快捷方式，以后可以使用该快捷方式运行备份，而无需使用 Data Protector GUI。双击它可打开命令提示符，然后针对所选备份规范运行 omnib 命令。

## 限制

- 在 Windows 系统上仅支持用于启动备份的快捷方式。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。
3. 右键单击“所选备份规范”，然后单击**选择快捷键的位置**。此时将显示“另存为”对话框。
4. 输入名称并选择快捷键的位置，然后单击**保存**。

用于启动所选备份的快捷方式将出现在磁盘上所选位置。

## 使用多个磁带客户机进行备份

备份大型对象时，可使用多个磁带客户机加快备份的速度。

以下内容可能会提供其他信息：

- 在备份规范中，必须手动定义将使用新的磁带客户机备份哪些目录/文件。应小心操作以避免相同数据发生重叠。
- 如果多个磁带客户机同时访问同一磁盘，则从磁盘检索数据的性能将下降。使用磁盘阵列时，这一点可能有所不同。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击要备份的项目类型(例如**文件系统**)，然后单击**添加备份**。
4. 在“创建新备份”对话框中，选择一个可用的模板，然后单击**确定**打开向导。
5. 在“源”属性页中，如果要使用磁带客户机备份目录/文件，则请勿选择位于同一逻辑磁盘或装载点上的目录/文件。但是，可以选择用一个磁带客户机备份目录/文件。单击**下一步 (Next)**。
6. 在“目标”属性页中，选择将用于备份的设备。单击**下一步 (Next)**。  
还可以指定是否要在备份会话期间额外创建备份的其他副本(镜像)。通过单击**添加镜像**和**删除镜像**，指定要创建的镜像数和将做此用途的设备。用于创建对象镜像的设备不得与用于备份的设备相同。**ZDB** 到磁盘和 **NDMP** 备份不支持对象镜像。
7. 在“选项”属性页中，根据需要指定其他选项，然后单击**下一步**。
8. 在“备份摘要”页中，单击**手动添加**。
9. 在“选择备份对象”对话框中，选择要备份的对象类型(例如 **Windows 文件系统**)。单击**下一步 (Next)**。
10. 在“常规选择”对话框中，选择要备份的客户机系统和装载点。还必须输入说明。单击**下一步 (Next)**。
11. 在“树/筛选器选择”对话框中，指定要备份或从备份中排除的目录/文件。将使用一个磁带客户机备份此处选择的内容。单击**下一步 (Next)**。
12. 在“常规”、“高级”和“Windows 特有对象选项”对话框中，根据需要指定其他选项，然后单击**下一步**，并在最后一个对话框中单击**完成**。

13. 对于要使用另一个磁带客户机备份的装载点上的目录/文件重复第 9-13 步。
14. 在“备份摘要”页中，查看备份规范的摘要，然后单击下一步。
15. 在备份向导的结尾处，可以保存、保存并计划、开始或预览所配置的备份。

## 处理重复进行的小规模备份

需要对大量小型对象执行重复进行的备份时，需要运行大量备份会话。在每个备份会话期间，驱动器中将加载然后卸载介质。这样的备份不仅缓慢，还会造成介质质量变差。要更节省地使用介质并节省时间，建议创建一个文件库设备，然后使用它向磁盘而非磁带执行重复进行的小规模备份。然后可以使用对象副本功能将数据从磁盘移至磁带介质。

使用这种方法后，备份将执行得更快，而介质将使用得更节省，因为在对象复制会话中对于介质只会加载和卸载一次。

要对大量小型对象执行频繁备份，请执行以下任务：

1. 配置一个文件库设备。将每个写入程序的块大小设置为第二阶段中将使用的设备的块大小。
2. 为所有小型对象创建一个备份规范。在备份的第一步中使用所创建的文件设备。
3. 执行或计划备份。
4. 使用对象副本功能将所备份的数据移至磁带。

## 磁盘映像备份

可以在 UNIX 和 Windows 平台上执行磁盘映像备份。

磁盘的磁盘映像备份是一种高速备份，其中 Data Protector 备份磁盘、磁盘分区或逻辑卷，但不跟踪这些数据源上存储的文件和目录结构。Data Protector 存储字符级别的磁盘映像结构。

可以对磁盘的特定部分或整个磁盘执行磁盘映像备份。

### 注意：

在 Windows 系统中，使用 VSS 写入程序执行磁盘映像备份。这可确保卷在备份过程中保持未锁定状态，可以由其他应用程序访问。这在备份系统卷时尤其重要。默认情况下会启用磁盘映像的 VSS 备份。要自定义 VSS 磁盘映像备份，请使用以下 omnirc 选项：OB2\_VSS\_RAW\_BACKUP、OB2\_VSS\_RAW\_BACKUP\_ALLOW\_FALLBACK 和 OB2\_VSS\_SNAPSHOT\_TIMEOUT。

## 何时使用磁盘映像备份？

- 当小文件众多而又需要高速备份时。
- 为灾难恢复或在重要软件更新之前需要对磁盘进行完整备份时。在 Windows 系统中，可以在准备到 EADR 和 OBDR 时使用磁盘映像备份。
- 无法进行磁盘对磁盘的直接连接以及要将文件系统复制到另一个磁盘时。后者必须与原始磁盘相同。

## 如何指定磁盘映像的某个部分？

### 在 UNIX 系统中

- 要指定磁盘映像分区，请使用以下格式： `/dev/rdisk/Filename`，例如：  
`/dev/rdisk/c2t0do`
- 要指定原始逻辑卷的某个部分，请使用以下格式： `/dev/vgNumber/r1volNumber`，例如：  
`/dev/vg01/r1vol1`

### 在 Windows 系统中

可以用两种方式指定磁盘映像的某个部分：第一种方式选择特定卷，第二种方式选择整个磁盘。在零宕机时间备份的情况下，请使用第二种方式：

- `\\.\DriveLetter`，例如： `\\.\E:`

**注意：**

当为卷名称指定了驱动器号时，卷在备份过程中不会锁定。未装载或作为 NTFS 文件夹装载的卷无法用于磁盘映像备份。

- `\\.\PHYSICALDRIVE#`，其中 `#` 是要备份的磁盘的当前编号。例如： `\\.\PHYSICALDRIVE3`

## 从何处查找磁盘映像的某个部分？

### 在 UNIX 系统中

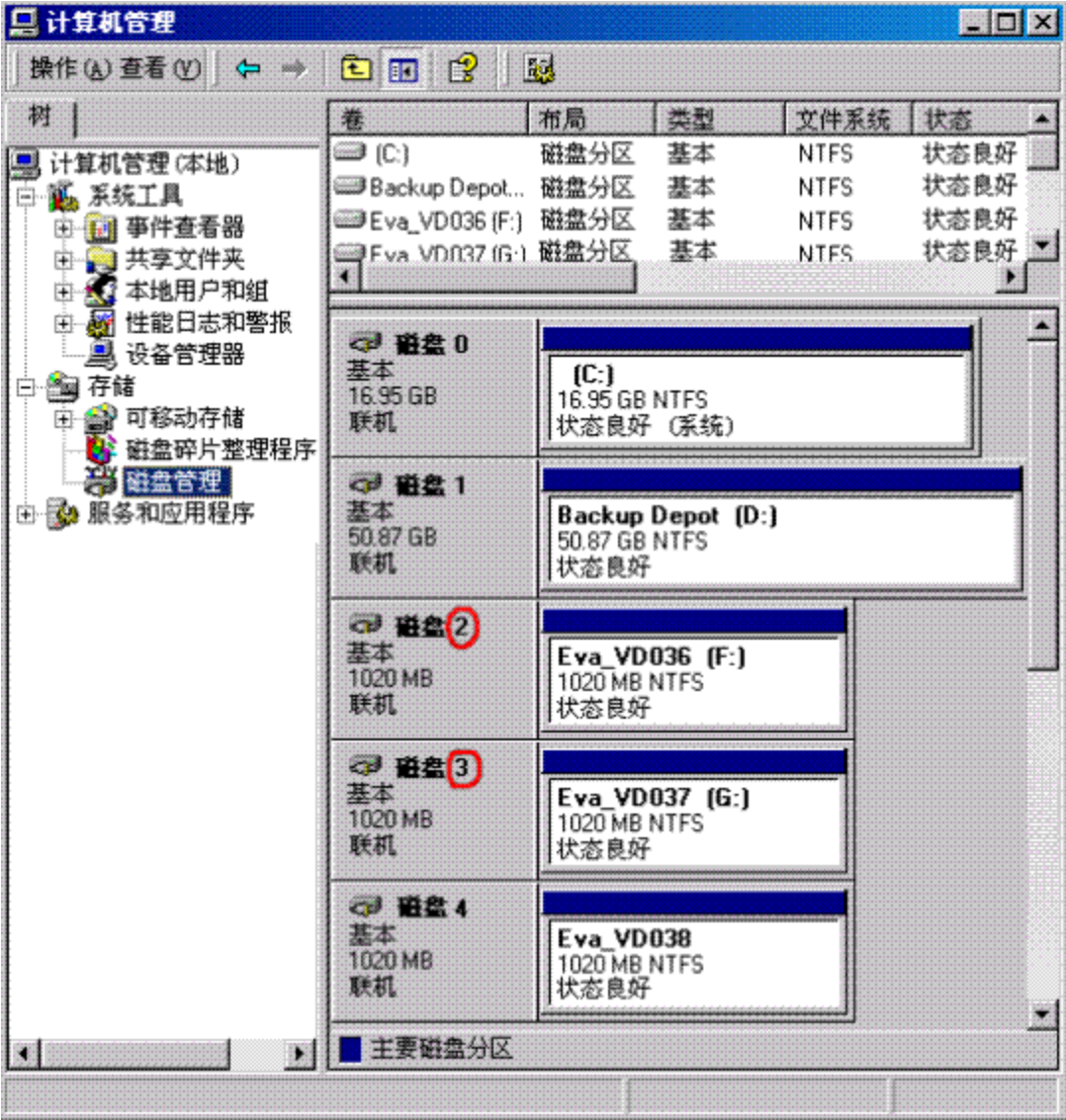
通常在 `/dev/rdisk` 目录中列出各个磁盘映像分区。可在 `/dev/vgNumber` 中找到原始逻辑卷。在 HP-UX 系统中，可在 `/dev/vgNumber` 中找到原始逻辑卷。原始逻辑卷的第一个字母是 `r`，如 `/dev/vg01/r1vol2`。

### 在 Windows 系统中

可通过从控制面板中单击 **管理工具**，然后依次单击 **计算机管理**、**存储**、**磁盘管理** 找到磁盘的当前编号(以及驱动器号)。

**Windows 系统中表示磁盘的数字(物理驱动器编号)**





**注意：**  
在 Windows 系统中，如果重新启动系统，表示磁盘的数字可能会发生变化。

## 执行磁盘发现的客户机备份

对于执行磁盘发现的客户机备份，要指定客户机作为数据源。如果随后装载另一个磁盘，则备份中将加入该磁盘。在文件系统备份中必须指定备份规范中尚未指定的任何新加磁盘或新装载的文件系统，相比之下，如果使用磁盘发现，则不必这样做。

Data Protector 在备份时与客户机联系，并查找与该系统连接的磁盘上的所有文件系统。然后将每个检测到的文件系统(还包括 Windows 系统中的 CONFIGURATION)作为常规文件系统进行备份。此时将生成每个文件系统对象的说明，并将文件系统装载点追加到客户机备份的说明中。

使用磁盘发现进行备份时，Data Protector 仅备份真实磁盘。因此，在 UNIX 系统中，Data Protector 不发现 NFS、CD 装载的文件系统和可移动装载点。此外，在 Windows 系统中，Data Protector 也不发现 CD 和具有可移动介质的驱动器。

## 何时使用磁盘发现

此备份类型在配置快速变化的动态环境中尤为有用。建议在以下条件下采用：

- 如果所备份的工作站具有频繁装载或卸除的较小磁盘。
- 如果希望在不考虑装载了多少个文件系统的情况下将装载点后的数据备份到一个目录中。例如，/home/data，其中 /home/data/disk1 和 /home/data/newdisk/disk2 可以频繁装载或卸除且彼此独立。
- 如果备份整个系统为灾难恢复做准备。

## 备份规范

创建将定义磁盘发现备份的备份规范时，单击客户机系统名称旁而非系统磁盘(卷)旁的复选框。选择客户机系统后，即可在“备份对象摘要”属性页中检查所配置的备份类型。在 Type 标签下，应看到 Client System。

## Web 服务器备份

要备份 Web 服务器，请使用标准备份过程以备份文件、目录和客户机。此外，还需要考虑以下各项：

- 执行客户机备份时，Data Protector 备份整个 Web 服务器，但不备份其他客户机/服务器上存储的数据。要备份其他客户机/服务器上的数据，还需要选择这些数据进行备份。
- 执行文件系统备份时，需要了解 Web 服务器及其各自客户机的所有文件和目录的位置。始终包括 Web 配置文件和根目录。
- Data Protector 以静态状态备份所有文件。如果备份期间文件发生更改，则不备份更改。

如果 Web 服务器上含有 Oracle 或 Informix Server 等数据库，则要使用该数据库特有的备份过程。

## 启用网络唤醒支持

如果您的 Windows 系统支持网络唤醒，则可以使用 Data Protector 网络唤醒支持。

当 Backup Session Manager 未能连接到配置为使用网络唤醒支持的客户机时，它会根据网络唤醒协议发送唤醒请求，并重试连接到该客户机。这样可以完全利用桌面系统的节能功能，否则节能功能将妨碍备份过程。

可以为配备了与网络唤醒兼容的 LAN 接口(如 NightDIRECTOR 序列)的计算机启用网络唤醒支持。BIOS 设置中有网络唤醒(Wake ONLAN, WOL)选项。

在 Windows 客户机上安装磁盘代理并将其添加到单元时，将自动发现客户机的 MAC 地址。也可以手动更改 MAC 地址。

## 步骤

1. 在“上下文列表 (Context List)”中，单击**客户机 (Clients)**。
2. 在范围窗格中，浏览所需的客户机，右键单击该客户机，然后单击**属性**。
3. 单击**高级**选项卡。
4. 选择启用 **Magic Packet** 选项。如果需要，则更改 **MAC** 地址。
5. 单击**应用**。

## 关于备份模板

**Data Protector** 备份模板可帮助您简化对(许多)备份规范和相关选项的处理。模板对于备份规范有一组明确指定的选项，可使用这些选项作为创建和修改备份规范的基础。

模板的用途是以用法相同的不同对象(设备选项或/和文件系统选项等特定区域的常见选项设置)配置多个备份规范。

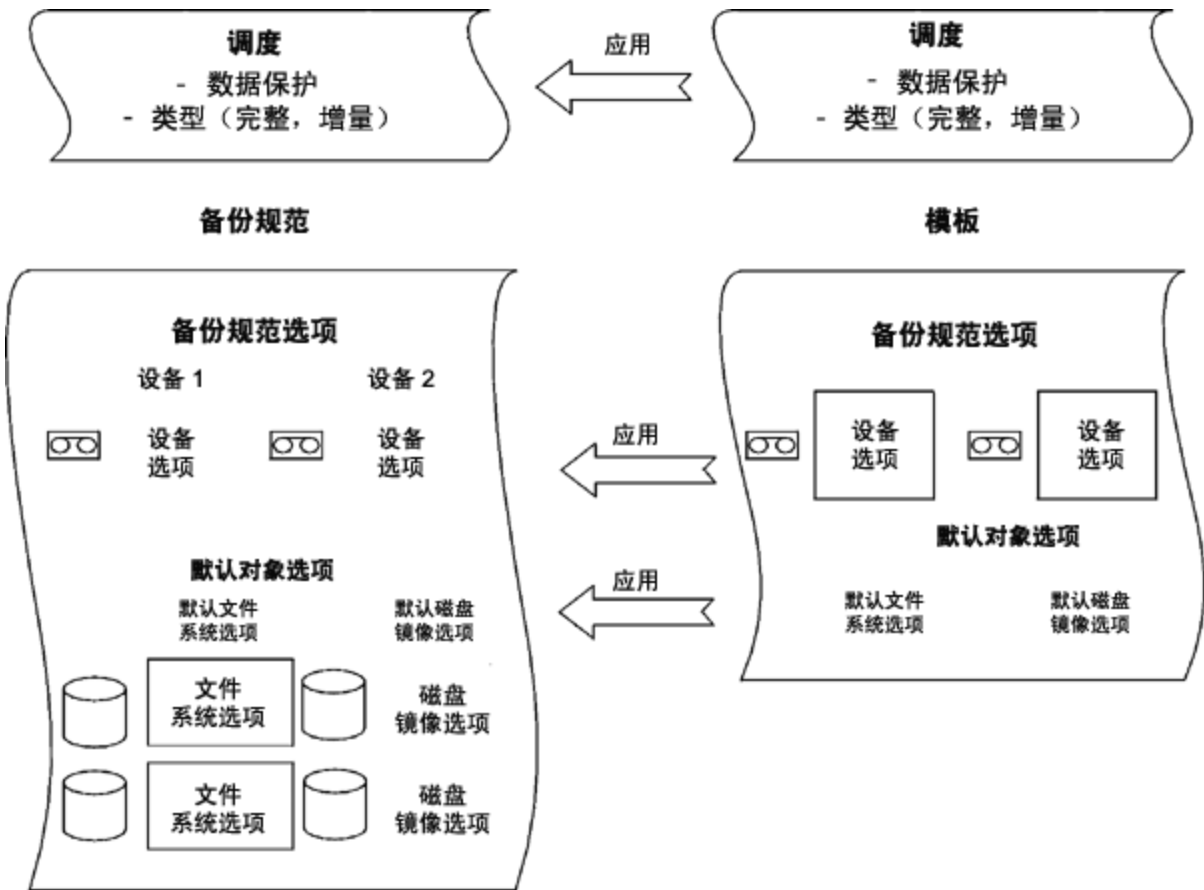
**Data Protector** 为不同类型的数据(文件系统、**Exchange** 等等)提供默认模板，不必指定对象、设备、选项和日程。在空白备份模板(如空白文件系统备份、空白 **Informix** 备份等等)中，未选择任何对象或设备。备份规范选项和对象选项的默认值为 **Data Protector**，并且没有任何备份计划。

模板的创建和修改方式类似于备份，但备份模板中不选择对象等元素。随后可以向现有备份规范应用模板，或者可以在创建新备份时使用该模板。如果随后更改模板，则要使更改生效，必须再次应用该模板。

### 提示：

将光标移至模板上方时将显示一个弹出窗口，其中含有模板的说明。

### 备份选项方案



## 创建新备份模板

可以为具有特殊需要的环境创建包含特殊设置的新备份模板。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**模板**。
3. 右键单击要创建的模板类型(例如**文件系统**)，然后单击**添加模板**打开向导。
4. 按照向导操作，确定要使用的备份设备、要设置的备份选项以及计划。

创建新备份规范时或将模板应用于一个或多个备份规范时，有新模板可用。

## 修改备份模板

可以修改备份模板。如果希望备份规范根据模板更改，则必须重新应用它，因为备份规范不会自动更新。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**模板**，然后展开要修改的模板类型(例如**文件系统**)。此时将显示该类型的所有已保存模板。
3. 右键单击要修改的模板，然后单击**属性**。
4. 在模板的属性页中，修改已选的模板，然后单击**应用**。

修改备份模板之后，可以将其应用于备份规范，或将其用于创建新备份规范。

## 复制备份模板

可以复制备份模板。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开**模板**，然后展开备份模板的相应类型(例如**文件系统**)。此时将显示所保存的全部备份模板。
3. 在结果区域中，右键单击要复制的模板，然后单击**复制为**。此时将打开“将备份复制为”对话框。
4. 在“名称”文本框中，输入所复制的模板的名称。(可选)从“组”下拉列表中，为所复制的模板选择一个不同的组。
5. 单击**确定**。

此时将在范围窗格中和结果区域中显示所复制的备份模板。

## 删除备份模板

可以删除备份模板。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在“范围窗格”中，展开**模板**，然后展开备份模板的相应类型(例如**文件系统**)。此时将显示所保存的全部备份模板。
3. 右键单击要删除的模板，然后单击**删除**。确认选择。

此时即删除备份模板。

## 将备份模板应用于备份规范

可以将模板应用于一个或若干备份会话。在这种情况下，可以选择应该应用哪些选项组。

**注意：**

如果将备份模板应用于现有的备份规范，并选择文件系统选项和/或计划选项，则模板中的保护设置将替换备份规范各个相应部分中以前的数据保护设置。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**。
3. 右键单击某个保存的备份规范，然后单击**应用模板**。
4. 在**应用模板**对话框中，选择要应用于备份规范的模板。

**提示：**

可以取消选择模板中的某些选项(**树**、**备份选项**、**设备**等等)，这样就不会将其应用于所选的备份规范。

**注意：**

要将模板应用于集成备份规范，不应在结果区域中打开要应用的备份规范。如果首先单击备份规范将其打开，然后尝试将模板应用于此备份规范，则**应用模板**选项将不可用。

5. 单击**确定**将模板应用于备份规范。

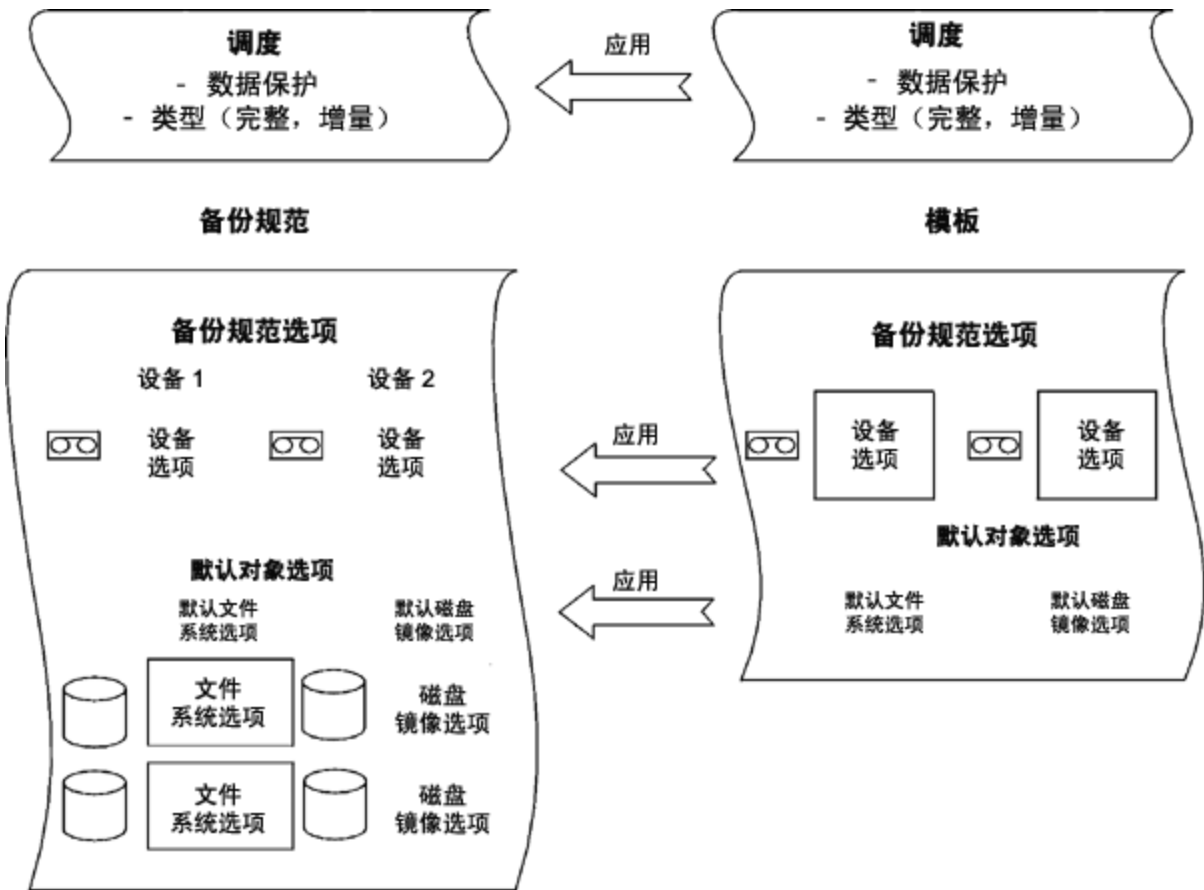
应用模板选项后，仍可修改备份规范和更改任何设置。

## 关于备份选项

Data Protector 提供一组全面的备份选项，通过这些选项可以对备份进行微调。所有这些选项都有适合大多数情况的默认值(选择或不选择)。

是否具有备份选项取决于要备份的数据类型。例如，磁盘映像备份并不具有文件系统备份所具有的所有备份选项。特定备份类型的上下文相关帮助中介绍了 **Exchange**、**SQL** 等的选项属性页中公共和特定的应用程序选项。

### 备份选项方案



## 可用的备份选项

备份数据时有下面的一组选项可用：

### 备份规范选项

这些选项适用于整个备份规范，无论备份对象的类型是什么。

### 文件系统选项

这些选项适用于文件系统备份的每个对象。还可以更改特定对象的选项。特定的对象设置优先于默认设置。

### 磁盘映像选项

这些选项适用于磁盘映像备份的每个对象。还可以更改特定对象的选项。特定的对象设置优先于默认设置。

### 设备选项

这些选项定义备份设备的行为。如果未设置设备选项，则从设备定义中读取相应的值。

## 计划选项

对于每次单独的或定期的计划备份，都可以指定备份类型(完整或增量；对于特定集成还有某些其他备份类型)、网络负载和数据保护。对于 ZDB，可以选择 ZDB 到磁盘 + 磁带或 ZDB 到磁盘(如果启用了即时恢复)。

在计划向导中指定的数据保护优先于备份规范中任何其他地方的保护设置。

## 最常用的选项

以下列出了根据特定备份策略经常要修改的选项。

- 数据保护
- 编目保护
- 日志记录
- 负载均衡
- 所有权

数据保护：在介质上将数据保留多长时间

配置保护策略对于数据安全和成功管理环境至关重要。必须根据公司的数据保护策略指定在介质上将备份数据保留多长时间。例如，可能决定数据在三周后到期，然后可以用后续备份覆盖这些数据。

可以在不同的位置指定数据保护。此选项有不同的组合，具体取决于正在运行交互式备份、启动已保存的备份规范还是安排备份。默认值为永久。

## 交互式备份

配置交互式备份时，可以更改整个备份的默认数据保护。此外，还可以为各个备份对象指定不同的数据保护期。在备份对象级别上指定的保护优先于默认的保护设置。

## 使用已保存的备份规范进行备份

使用 GUI 启动已保存的备份时将应用数据保护，如针对交互式备份所述。

使用 CLI 启动已保存的备份时，也可以指定数据保护。这将优先于备份规范中的所有数据保护设置。

## 计划的备份

可以为每个单独或定期计划的备份指定不同的保护期。计划向导中指定的数据保护优先于备份规范中的所有其他数据保护设置。如果保持默认保护，则将应用数据保护，如针对交互式备份所述。

编目保护：在 IDB 上将数据保留多长时间

可以单独设置编目保护和数据保护。当数据保护结束并且重写介质时，无论编目保护设置是什么，都将删除对象的目录。



编目保护与日志记录级别一起，对 IDB 的增大、浏览数据进行还原的方便程度以及备份性能有着重要影响。请定义适合您所在环境的编目保护策略，这一点很重要。如果将日志记录级别设置为无日志，则编目保护无效。

如果编目保护为永久，则只有在导出或删除介质时才会删除 IDB 中的信息。在这种情况下，IDB 的大小线性增长，直到数据保护期限到期为止，即使单元中的文件数没有发生变化时也是如此。

默认值为**与数据保护相同**。这意味着只要有介质可供还原，就可以浏览并选择文件或目录。

由于操作系统限制，可以设置的最后保护日期为 2038 年 1 月 18 日。

## 到期的编目保护

目录保护到期后，并不会立即从 IDB 中删除信息。Data Protector 每天自动删除一次这些信息。由于 IDB 中的信息是按介质排列的，因此只有在介质上所有对象的编目保护都到期时，才会删除这些信息。

当编目保护到期时，仍能进行还原，但必须手动指定文件名。

## 编目保护和备份

编目保护设置对备份性能没有任何影响。

## 编目保护和还原

编目保护到期时，会像使用无日志(No Log)选项备份数据那样还原数据。

日志记录：更改有关 IDB 中存储的数据的详细信息

Data Protector 日志记录级别决定在备份期间写入 IDB 的关于文件和目录的详细信息量。有如下四个日志记录级别：

- 全部记录
- 记录文件
- 记录目录
- 不记录任何内容

Micro Focus 建议在同一个单元中使用不同的日志记录级别。一个单元通常由每日生成大量文件的邮件(或类似)服务器、将所有信息存储在少量文件中的数据库服务器以及一些用户工作站组成。由于这些系统的动态变化截然不同，找到一种适合所有系统的设置非常困难。Micro Focus 建议使用以下日志记录级别设置创建多种备份规范：

- 对于电子邮件服务器，使用日志目录选项。
- 对于数据库服务器，使用无日志选项，因为浏览各个文件对此情况无意义。
- 对于工作站，使用日志文件选项，以使您可以搜索并还原不同版本的文件。
- 通过全部记录选项，可以查看修改时间和 ACL 等文件属性。

## 日志记录级别和备份速度

无论所选的日志记录级别是什么，备份速度都大致一样。

## 日志记录级别和浏览还原

信息存储详细程度的变化会影响还原期间使用 **Data ProtectorGUI** 浏览文件的信息量。如果设置了**无日志**选项，则无法浏览数据；如果设置了**日志目录**选项，则可以浏览目录；如果设置了**日志文件**选项，则可以浏览完整数据，但不会显示文件属性(大小、创建日期和修改日期等)。

如果知道要还原的文件的名称，则无论生效的日志记录级别是什么，都始终可以手动指定它们而不是通过浏览来寻找它们。

## 日志记录级别和还原速度

以**全部记录 (Log All)**、**记录目录 (Log Directories)**或**记录文件 (Log Files)**日志记录级别运行的对应备份会话对还原速度的影响大致相同。

如果备份会话使用**无日志**日志记录级别运行，则还原速度可能在还原单个文件时降低。在这种情况下，**Data Protector**必须从对象的开头起读取所有数据，然后再查找要还原的文件。

在进行完整系统还原的情况下，无论如何都要读取整个备份对象，因此日志记录级别的影响不大。

负载均衡：使备份设备的使用情况保持均衡

要将大量对象备份到许多可用设备，并希望 **Data Protector** 使所有设备始终处于繁忙状态时，可使用负载均衡选项。应使用负载均衡最大限度地降低不可用的设备对备份的影响。

要备份少量对象时、在简单设备(如 **DDS**)上备份对象时、要手动选择对象将备份到的设备时或要了解将在哪些介质对象上备份时，请清除负载均衡选项。

将对象分配到在负载均衡备份规范中指定的设备列表中的某个可用设备。启动第一个设备，并使用其并发定义所选择的对象数。启动下一个设备并选择对象，直到列表中再也没有对象或已运行了最大数量的设备为止。

如果某个设备变为不可用，则在失败时仅中止备份到该设备的对象。实际备份的是失败时间之前备份到设备的所有对象。如果在备份规范中指定了任何其他设备，并且尚未使用最大数量的设备，则将启动新设备。设备在遇到以下情况时可能会变为不可用：

- 在备份期间失败
- 在备份期间停止
- 正由另一个会话使用
- 完全无法启动

根据以下标准访问要备份的对象：

- 位于连接到备份设备的客户机上的对象具有更高的优先级。
- 通过选择对象，使每个客户机的磁盘代理数尽可能保持较低水平。
- 对象大小在向设备分配对象方面不起作用。

应用模板中的设备选项时应考虑以下规则：

- 如果模板中未选择负载均衡选项，则设备不与备份规范一起使用。
- 如果同时在模板和备份规范中选择了负载均衡选项，则应用设备选项。
- 如果仅在模板中选择了负载均衡选项，则只有在备份规范没有设备时才会应用设备选项。

所有权：谁可以还原

## 谁是备份会话的所有者？

每个备份会话和在会话中备份的所有数据都会指定有一个所有者。所有者可以是启动交互式备份的用户、运行 **CRS** 进程时使用的帐户，或在备份规范选项中指定为所有者的用户。

如果用户未修改某个现有备份规范即启动它，则不会将备份会话视为交互式会话。

如果用户启动了经过修改的备份规范，则除非以下情况属实，否则该用户即为所有者：

- 用户具有切换会话所有权用户权限。
- 备份规范(其中指定用户名、组名或域名以及系统名称)中明确定义了备份会话所有者。

如果在 **UNIX Cell Manager** 上计划了备份，则除非以上情况属实，否则会话所有者为 `root:sys`。

如果在 **Windows Cell Manager** 上计划了备份，则除非以上情况属实，否则会话所有者为安装期间指定的用户。

## 为什么更改备份所有者？

如果管理员配置并安排了备份规范，并且允许操作员运行该备份规范，但操作员无法修改或保存该备份规范，则可能要更改备份所有者。如果对所有对象都设置了私有备份选项，则操作员将无法还原任何内容，但仍可管理备份和重新启动失败的会话。

如果更改了备份配置但未保存，则将备份视为交互式备份，并且不更改所有者。如果以交互方式启动增量备份，并且您不是完整备份的所有者，则将进行另一次完整备份而非增量备份。

## 谁可以还原私有对象？

除非将对象标为公共，否则只有以下用户可以还原该对象：

- **Admin** 和 **Operator** 用户组的成员。
- 具有“启动还原”用户权限的备份会话所有者。可能需要其他用户权限，如“还原到另一个客户机”。
- 具有查看私有对象用户权限的用户。

也可以将查看和还原私有对象的权限授予 **admin** 或 **operator** 以外的组。

## 备份规范选项

这些选项适用于整个备份规范，无论备份对象的类型是什么。

基本选项是**负载均衡**默认情况下，在“创建新备份”对话框中启用此选项。如果这里禁用了此选项，则以后可以在备份规范的“目标”属性页的“备份”选项卡中选择此选项。

有关备份规范的详细信息，请参见 **Data Protector** 帮助。

## 常规备份规范选项

- 说明
- 在客户机上
- Post-exec
- Pre-exec
- 重新连接已断开的连接
- 所有权

## 群集备份规范选项

### 会话自动重新启动

如果在备份期间发生了群集感知 **Data Protector** 的故障转移，则所有正在运行和挂起的备份会话将失败。以下选项定义了 **Data Protector** 在故障转移之后的行为：

- 故障转移时不重新启动备份
- 重新启动所有对象的备份
- 重新启动失败对象的备份

### 中止会话和中止 ID 参数

当 **Data Protector** 之外的某些群集感知应用程序在 **Data Protector** 之外的节点上运行，并且故障转移到该节点(即运行 **Data Protector** 的节点)时，可以控制此系统上的负载。以下选项配合 **omniclus** 命令可定义 **Data Protector** 在故障转移之后的行为。

- 不检查已用的会话时间
- 小于此时间则中止
- 大于此时间则中止
- 不检查中止 ID
- 检查中止 ID

## EMC Symmetrix 备份规范选项

### 客户机系统

- 应用程序系统
- 备份系统

## 镜像类型

- TimeFinder
- Symmetrix Remote Data Facility
- 组合 [SRDF + TimeFinder]

## EMC Symmetrix 拆分 pre-exec 和 post-exec

- 拆分 pre-exec
- 拆分 post-exec

## EMC Symmetrix 选项

- 运行 Symmetrix 环境发现
- 在备份之前重新建立链接
- 在备份完成之后重新建立链接

## P9000 XP 磁盘阵列系列 备份规范选项

## 客户机系统

只有在保存了备份规范之后才能修改这组选项。

- 应用程序系统
- 备份系统

## 镜像类型

- Business Copy P9000 XP
- Continuous Access P9000 XP
- ( Continuous Access P9000 XP + Business Copy P9000 XP) 组合
- MU 编号

## 复本管理选项

- 在备份完成之后保留复本
- 跟踪即时恢复的复本

## 在会话开始时

- 如果尚未同步，则同步磁盘
- 如果镜像磁盘尚未同步，则中止会话

## 在会话结束时

- 为备份 (重新同步) 准备下一镜像磁盘

## 应用程序系统选项

- 卸载应用程序系统上的文件系统
- 使应用程序命令行停止/静默
- 重新启动应用程序命令行

## 备份系统选项

- 使用与应用程序系统上相同的装载点
- 备份系统上安装路径的根目录
- 将目录添加到装载路径
- 在目标装载点自动卸除文件系统
- 让备份系统处于启用状态
- 以读取/写入模式启用备份系统

## **P6000 EVA** 磁盘阵列系列 备份规范选项

## 客户机系统

- 应用程序系统
- 备份系统

## 复制模式

- Business Copy P6000 EVA
- Continuous Access P6000 EVA + Business Copy P6000 EVA

## 故障转移情况下的复本处理

- 按照复制的方向
- 保持复本位置

## 快照管理选项

- 快照源
- 快照类型
- 冗余级别
- 未完全创建快照式克隆则最多推迟磁带备份 n 分钟

## 镜像克隆准备/同步

- 在会话开始时
- 在会话结束时

## 复本管理选项

- 在备份完成之后保留复本
- 轮换的复本数量
- 跟踪即时恢复的复本

## 应用程序系统选项

- 在复本生成之前卸除应用程序系统上的文件系统
- 使应用程序命令行停止/静默
- 重新启动应用程序命令行

## 备份系统选项

- 使用与应用程序系统上相同的装载点
- 备份系统上安装路径的根目录
- 将目录添加到装载路径
- 在目标装载点自动卸除文件系统
- 让备份系统处于启用状态
- 以读取/写入模式启用备份系统

## 文件系统选项

这些选项适用于文件系统备份的每个对象。

基本选项为保护。

有多组**高级**文件系统选项：

- 文件系统选项
- 其他文件系统选项
- WinFS 文件系统选项

有关文件系统选项的详细信息，请参见《Data Protector 帮助》。

## 文件系统选项

- 编目保护
- Post-exec

- Pre-exec
- 公共
- 报告级别

## 其他文件系统选项

- 备份文件的大小
- 将 POSIX 硬链接备份为文件
- 将 POSIX 硬链接备份为文件
- 将完整 DR 映像复制到磁盘
- **数据安全性**
  - 无
  - AES 256 位
  - 编码
- 显示统计信息
- 不保留访问时间属性
- 增强型增量备份
- 使用本机文件系统更改日志提供程序(如果有)
- 在备份期间锁定文件
- 日志记录

**Data Protector** 日志记录级别定义了备份期间写入内部数据库的关于备份文件和目录的详细信息量。有如下四个日志记录级别：

- 全部记录
  - 记录文件
  - 记录目录
  - 不记录任何内容
- 软件压缩

## WinFS 文件系统选项

- 异步读取(A)
- 备份目录的共享信息
- 检测 NTFS 硬链接
- 不使用归档属性
- 打开文件



- 重试次数
- 超时
- 将打开的锁定文件报告为
- **MS Volume Shadow Copy 选项**
  - 使用卷影复制
  - 允许回退

## 磁盘映像选项

这些选项适用于选择进行备份的所有磁盘映像对象。

基本选项为保护。

有关磁盘映像选项的详细信息，请参见 **Data Protector** 帮助。

可以设置以下**高级**磁盘映像选项：

- 编目保护
- **数据安全性**
  - 无
  - AES 256 位
  - 编码
- 显示统计信息
- Post-exec
- Pre-exec
- 公共
- 报告级别
- 软件压缩

## 设备选项

对特定备份规范中当前所选的备份设备可以设置这些选项。 这些选项是在配置备份设备或更改其属性时所设置的一部分选项。 所列选项对某个特定备份规范有效。 这些选项优先于在“设备和介质”上下文中设置的选项(这些选项一般适用于各自的设备)。

有关设备选项的详细信息，请参见 **Data Protector** 帮助。

## 设备属性 - 常规

- CRC 检查
- 并发

- 基于驱动器的加密
- 介质池
- prealloc 列表
- 重新扫描

## 计划选项

安排备份时，可以设置其他选项。对于每次计划备份，都可以指定备份类型(完整或增量；特定集成还有某些其他备份类型)、数据保护、优先级、网络负载、重复模式和估计持续时间。对于 ZDB，可以选择 ZDB 到磁盘 + 磁带或 ZDB 到磁盘(如果启用了即时恢复)。

在计划程序中指定的数据保护优先于备份规范中任何其他地方的保护设置。

有关如何使用计划向导在 Data Protector 中创建和编辑计划的更多信息，请参见 [计划程序\(第 92 页\)](#)。

## 会话选项

- 备份类型
  - 完整
  - 增量
- 备份保护
- 优先级
- 网络负载
- 重复模式
- 估计持续时间

## 分割镜像/快照备份

(此选项在 ZDB 提供，但仅限“ZDB 到磁盘 + 磁带”或“ZDB 到磁盘”的情况下(启用了即时恢复))。

## 设置备份选项

创建新的备份规范时，可以设置备份选项。在这种情况下，遵循向导进入“选项”属性页。还可以为已配置和保存的备份规范设置备份选项。

### 注意：

可以在两个级别设置对象选项(文件系统和磁盘映像选项)。首先，可以为所有文件系统和为备份规范中的所有磁盘映像对象单独设置默认对象选项。然后，可以为特定对象设置这些选项。这些设置将优先于默认值。例如，要压缩除 CPU 较慢的某个客户机以外所有客户机中的数据，请在设置文件系统选项时启用**压缩**选项。然后，选择该慢速客户机，并对此客户机清除**压缩**选项。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 双击要设置其备份选项的备份规范，然后单击**选项**选项卡。
4. 在“选项”页中，根据需要设置选项。单击某个**高级**按钮以设置高级选项(按照要设置的选项的类型)。

除了备份规范选项外，还可以设置例如文件系统选项、磁盘映像选项等等，具体取决于配置其备份规范的数据类型。

5. 查找所需的选项，然后选择或取消选择该选项，或输入所需的信息。
6. 单击**确定**，然后单击**应用**以保存更改。

## 指定数据保护

运行交互式备份、启动保存的备份规范或排定备份时，可以指定数据保护。默认值为永久。

### 注意：

由于操作系统限制，可以设置的最后保护日期为 2038 年 1 月 18 日。

## 指定备份规范级别的数据保护

创建新的备份规范时，或修改现有的备份规范时，可以指定数据保护。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 双击要设置其备份选项的备份规范，然后单击**选项**选项卡。
4. 如果要备份文件系统，则在“文件系统选项”下指定保护选项。对于集成，单击“公共应用程序选项”下的**高级**，并在“选项”选项卡中指定**保护**选项。
5. 单击**确定**，然后单击**应用**以保存更改。

## 指定单独备份对象的数据保护

对文件系统和磁盘映像对象可以指定不同的保护期。

创建新的备份规范时，或修改现有的备份规范时，可以指定单独对象的数据保护。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 双击要设置其备份选项的备份规范，然后单击**备份对象摘要**选项卡。
4. 右键单击对象，然后单击**属性**。
5. 单击**选项**选项卡并指定保护选项。
6. 单击**确定**，然后单击**应用**以保存更改。

## 指定计划备份的数据保护

可以为每个单独或定期计划的备份指定不同的保护期。计划向导中指定的数据保护优先于备份规范中的所有其他数据保护设置。

计划备份时，可以指定计划备份的数据保护。

## 使用 CLI 指定数据保护

使用 CLI 运行备份时，也可以指定数据保护。这将优先于备份规范中的所有数据保护设置。

## 步骤

1. 请输入以下命令：  
`omnib -datalist Name -protect ProtectionPeriod`

其中 *Name* 是备份规范的名称。

例如，要运行受到两周保护的备份，请输入：

```
omnib -datalist MyBackup -protect weeks 2
```

有关详细信息，请参见 omnib 手册页或《*Data Protector 命令行界面参考*》。

## 更改特定对象的选项

可以将选项应用于特定对象，或手动更改默认选项。

可以在创建新备份规范的同时应用这些选项。在这种情况下，遵循向导进入“备份对象摘要”页。

还可以为已配置和保存的备份规范应用选项。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型(例如**文件系统**)。此时将显

示所保存的全部备份规范。

3. 双击要为其应用特定对象的选项的备份规范，然后单击**备份对象摘要**选项卡。
4. 在“备份对象摘要”页中，可以更改对象属性、对象顺序或镜像选项。

更改对象属性：

- a. 右键单击对象，然后单击**属性**。
- b. 在“对象属性”对话框中，更改特定对象的选项。根据所选的对象，将显示以下选项卡中的一部分：**常规**、**选项**、**其他**、**树/过滤器**、**WinFS 选项**、**选项和数据库**。单击相应的选项卡修改选项。
- c. 单击**确定**应用更改。

要更改对象的顺序：

- a. 右键单击某个对象，然后单击**上移**或**下移**。重复该过程，直到获得所需的顺序为止。
- b. 单击**应用**。

更改镜像选项：

- a. 选择某个对象，然后单击**更改镜像**。
- b. 要更改镜像的设备，请确保选择镜像，突出显示该镜像，并从**设备**下拉列表选择一个设备。还可以取消选择所选备份对象的镜像。

## 更改备份设备选项

在创建新的备份规范的同时，可以设置备份设备选项和这些设备的顺序。在这种情况下，遵循向导进入“目标”属性页。

还可以为已配置和保存的备份规范设置备份设备选项。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 双击要更改其设备选项的备份规范，然后单击**目标**选项卡。
4. 在“目标”属性页中，可以更改设备选项。
  - 要更改已经过负载均衡的备份的设备，请取消选择设备，然后选择其他设备。
  - 要更改未经过负载均衡的备份的设备，请选择要使用的所有设备。然后单击**备份对象摘要**选项卡，选择所需的对象，然后单击**更改设备**。
  - 要更改镜像对象的设备，请选择要用于特定镜像的所有设备。然后单击**备份对象摘要**选项卡，选择所需的对象，然后单击**更改镜像**。
  - 要更改设备的顺序(如果备份经过负载均衡)，请右键单击任何所选设备，然后单击**将设备排序**。
  - 要设置其他设备属性，请右键单击任何所选设备，然后单击**属性**。

5. 指定所需的选项，然后单击**确定**。
6. 单击**应用**。

## 设置计划备份选项

安排备份时，可以设置其他选项。这些选项仅对所计划的备份有效，而对以交互方式启动的备份无效。在计划向导中指定的数据保护优先于备份规范中任何其他地方的保护设置。

为所计划的备份创建新备份规范时，可以设置计划备份选项。在备份向导中选择**保存并计划**选项，以计划备份。

在安排已配置和保存的备份规范中的备份时，也可以设置计划备份选项。有关如何在 Data Protector 中创建和编辑计划的更多信息，请参见 [计划程序 \(第 92 页\)](#)。

## 关于 pre-exec 和 post-exec 命令

### 什么是 pre-exec 和 post-exec 命令？

pre-exec 和 post-exec 命令用于在备份或还原之前和/或之后执行额外的操作。此类操作包括检查要备份的文件数、停止某些事务处理或在备份之前关闭应用程序，随后将其重新启动。Data Protector 不提供 pre-exec 和 post-exec 命令。必须自行编写脚本以执行所需的操作。这些脚本在 Windows 系统中可编写为可执行文件或批处理文件，在 UNIX 系统中可编写为 shell 脚本。批处理文件中运行的所有命令返回的退出代码都必须以 0 表示成功，以大于 0 表示失败。

对于某些备份对象(属于 Client System 类型)有一种特殊的行为(主机备份)。即使仅指定 pre-exec 和 post-exec 命令一次，对于每个文件系统(或逻辑驱动器)也会启动每种命令一次。

### 配置备份的 pre-exec 和 post-exec 命令

可以在如下两个级别上配置 pre-exec 和 post-exec 命令：

#### 备份规范

备份会话启动之前将执行 pre-exec 命令。备份会话停止后将执行 post-exec 命令。指定这些命令作为整个备份规范的备份选项。默认情况下，在 Cell Manager 上执行备份会话的 pre-exec 和 post-exec 命令，但可以选择另一个系统。

#### 备份对象

备份对象之前启动备份对象的 pre-exec 命令。备份对象之后执行备份对象的 post-exec 命令。将这些命令指定为对象的备份选项。在正运行备份对象的磁带客户机的系统上执行对象的 pre-exec 和 post-exec 命令。

## pre-exec 和 post-exec 命令如何运行？

1. 整个备份规范的 **pre-exec** 命令启动并执行完毕。
2. 对于备份规范中的每个对象：
  - a. **pre-exec** 命令启动并执行完毕。
  - b. 备份对象。
  - c. (备份规范中每个对象的) **post-exec** 命令启动并执行完毕。
3. 整个备份规范的 **post-exec** 命令启动并执行完毕。

## 备份规范的 pre-exec 和 post-exec 命令

**pre-exec** 和 **post-exec** 命令在 Windows 系统中可编写为可执行文件或批处理文件；在 UNIX 系统中可编写为 **shell** 脚本。批处理文件中运行的所有命令返回的退出代码都必须以 0 表示成功，以大于 0 表示失败。

## pre-exec 和 post-exec 特征

- 命令的启动和位置以确保安全性
- 环境变量
- **SMEXIT** 值
- **pre-exec** 和 **post-exec** 命令的注意事项

## 命令的启动和位置以确保安全性

分别在备份会话前后启动备份会话的 **pre-exec** 和 **post-exec** 命令。默认情况下在 **Cell Manager** 上执行这些命令，但可以选择其他系统。

## Windows 系统

在 **Cell Manager** 上执行时，**pre-exec** 和 **post-exec** 脚本由 **Data Protector CRS** 启动；而在远程执行时，以 **Data Protector Inet** 服务帐户(默认情况下为本地系统帐户)执行这些脚本。

**Cell Manager** 及其他系统上的脚本必须位于 **Data\_Protector\_home\bin** 目录中，用户必须仅指定文件名或相对路径名。

对于 **pre-exec** 和 **post-exec** 命令，仅支持 **.bat**、**.exe** 和 **.cmd** 扩展名。要运行扩展名不受支持的(例如 **.vbs**)脚本，请创建用于启动该脚本的批处理文件。然后配置 **Data Protector**，将批处理文件作为 **pre-exec** 或 **post-exec** 命令运行，该批处理文件随后启动扩展名不受支持的脚本。

如果使用引号 (") 指定路径名，则不要使用反斜杠和引号的组合 (\")。如果需要在路径名末尾使用尾随的反斜杠，则要使用双反斜杠 (\\)。

**注意：**  
禁止直接使用 **perl.exe**。

## UNIX 系统

Pre-exec 和 post-exec 脚本由备份会话所有者启动，除非备份会话所有者具有 Backup as root 权限；那么，将以 root 启动这些命令。

在 Cell Manager 或远程 UNIX 客户机上，备份规范的 exec 命令必须位于如下位置：

**HP-UX、Solaris 和 Linux 系统：** /opt/omni/sbin

**其他 UNIX 系统：** /usr/omni/bin

对于位于 /opt/omni/sbin 或 /usr/omni/bin 目录中的命令，可仅指定文件名，否则要指定完整的路径名。

## 环境变量

以下环境变量由 Data Protector 设置，并且只能在 Cell Manager 上备份规范的 pre-exec 和 post-exec 脚本中使用，如果在任何其他系统上执行命令，则不能使用这些环境变量。

有关环境变量的详细信息，请参见 Data Protector 帮助。

- DATALIST
- MODE
- OWNER
- PREVIEW
- RESTARTED
- SESSIONID
- SESSIONKEY
- SMEXIT

## SMEXIT 值

值	说明
0	成功备份了所有文件。
10	成功完成了所有代理，但并未备份所有文件。
11	一个或多个代理失败，或有数据库错误。
12	无任何代理完成了操作；Data Protector 中止了会话。
13	用户中止了会话。

## pre-exec 和 post-exec 命令的注意事项

- 在 Windows 系统上，必须指定完整的文件名，其中包括扩展名(例如 .exe 或 .bat)。
- 指定脚本名称时，如果因路径中有空格而需要使用单引号 (UNIX 系统中)或双引号 (Windows 系统中)，则永远不要使用两者的组合。或者使用单引号，或者使用双引号。



例如，"S'ilvousplat.bat" 错误，而允许使用 S'ilvousplat.bat。

- 成功完成后，pre-exec 或 post-exec 命令的退出值必须为零。
- 如果 pre-exec 命令失败(返回的值小于 0)，则将备份会话的状态设置为 Failed，并中止会话。不再执行 post-exec 命令。
- 如果 post-exec 命令失败(返回的值小于 0)，则将备份会话状态设置为 Completed with errors。
- 如果 post-exec 命令返回小于 0 的值和 omnib 命令 11，则将备份状态设置为 Completed with failures。
- 除非中止会话并且未执行或未设置 pre-exec 命令，否则始终执行 post-exec 命令。如果设置了 OB2FORCEPOSTEXEC omnirc 选项，则始终执行 post-exec 命令。
- 默认情况下，在预览备份期间不执行 pre-exec 和 post-exec 命令。此行为由全局选项文件中的 ExecScriptOnPreview 选项定义。
- 处理 pre-exec 和 post-exec 命令的方式与处理命令提示符下输入的命令相同。但是，不允许使用特殊字符 ?、\*、"、|、< 和 >。
- pre-exec 和 post-exec 命令的执行是使用管道机制实现的。pre-exec 或 post-exec 函数中启动的所有过程都必须结束，然后处理才能继续。
- 运行 pre-exec 或 post-exec 命令时，无法中止备份会话。
- pre-exec 和 post-exec 命令运行于后台模式。因此，不要使用任何需要用户交互的命令。
- 提供超时。默认情况下，pre-exec 和 post-exec 脚本必须至少每隔 15 分钟发送一些输出，否则将中止脚本。通过修改 ScriptOutputTimeout 全局选项可以更改此时间间隔。
- pre-exec 和 post-exec 命令的任何输出都写入 IDB，并显示在 Data Protector GUI 中。
- 在 UNIX 系统中，pre- 或 post-exec 脚本可能会停止响应，因为它在启动新进程之前未关闭所有文件描述符。如果新进程在后台运行并且不退出，例如数据库服务器进程 (dbstart)，则脚本将停止响应。

可以使用 detach 命令。detach.c 文件中提供 detach 命令的源，但不支持该源。例如：  
/opt/omni/bin/utilns/detach pre\_script [arguments...]

- 通过将 SmDisableScript 全局选项设置为 1，可以在 Cell Manager 上禁止执行会话 pre-exec 和 post-exec 命令。
- 通过在 omnirc 文件中添加行 OB2REXECOFF=1，可以在任何客户机上禁止执行远程会话 pre-exec 和 post-exec 命令。
- 通过指定允许哪些 Cell Manager 访问客户机，可以保护客户机。只有受到允许的 Cell Manager 能够在客户机上执行 pre-exec 和 post-exec 命令。
- 在 UNIX 系统上，由命令写入 stdout 的文本将发送到会话管理器，并写入数据库。stderr 将重定向到 /dev/null。可以将其重定向到 stdout，以获取记录到数据库的错误消息。

## 指定备份规范的 pre-exec 和 post-exec 命令

要指定所保存的备份规范的 pre-exec 和 post-exec 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。

- 3. 双击要为其指定 **pre-exec** 和 **post-exec** 命令的备份规范，然后单击**选项**选项卡。
- 4. 在“备份规范选项”下，单击**高级**。
- 5. 在“备份选项”对话框的“常规”选项卡中，在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
- 6. 单击**确定**，然后单击**应用**以保存更改。

## 特定备份对象的 **pre-exec** 和 **post-exec** 命令

**pre-exec** 和 **post-exec** 命令在 Windows 系统中可编写为可执行文件或批处理文件；在 UNIX 系统中可编写为 **shell** 脚本。批处理文件中运行的所有命令返回的退出代码都必须以 0 表示成功，以大于 0 表示失败。

### 命令的启动和位置

分别在备份对象前后执行对象的 **pre-exec** 和 **post-exec** 命令。可以为备份规范中的所有对象或逐个为每个对象指定这些命令。备份集成(例如 Oracle)时，将数据库视为一个对象，因此在数据库备份前后执行这些命令。在运行磁盘代理的系统上执行这些命令。

<b>Windows 系统：</b>	<p>以 Data Protector Inet Service 帐户(默认情况下为本地系统帐户)启动备份对象的 <b>pre-exec</b> 和 <b>post-exec</b> 脚本。</p> <p>备份对象的 <b>exec</b> 脚本可位于运行 Disk Agent 的系统上的任何目录中。但是，对于客户机备份，它们必须位于 <i>Data_Protector_home\bin</i> 中。如果脚本位于 <i>Data_Protector_home\bin</i> 中，则仅指定文件名，否则必须指定完整路径名。</p> <p>对于 <b>pre-exec</b> 和 <b>post-exec</b> 命令，仅支持 <b>.bat</b>、<b>.exe</b> 和 <b>.cmd</b> 扩展名。要运行扩展名不受支持的(例如 <b>.vbs</b>)脚本，请创建用于启动该脚本的批处理文件。然后配置 Data Protector，将批处理文件作为 <b>pre-exec</b> 或 <b>post-exec</b> 命令运行，该批处理文件随后启动扩展名不受支持的脚本。</p> <p>如果使用引号 (") 指定路径名，则不要使用反斜杠和引号的组合 (\")。如果需要在路径名末尾使用尾随的反斜杠，则要使用双反斜杠 (\\)。</p>
<b>UNIX 系统：</b>	<p><b>Pre-exec</b> 和 <b>post-exec</b> 脚本由备份会话所有者启动，除非备份会话所有者具有 Backup as root 权限；否则将以 root 身份启动这些命令。</p> <p>备份对象的 <b>exec</b> 命令可位于运行磁盘代理的系统上的任何目录中。但是，对于客户机备份，这些命令必须位于默认的管理命令目录中。如果这些命令位于默认的管理命令目录中，则仅需指定文件名，否则必须指定完整的路径名。</p>

### 环境变量

对于 **post-exec** 命令 Data Protector 设置了 BDACC 环境变量。

## pre-exec 和 post-exec 命令的注意事项

- 如果执行客户机系统(主机)备份，则在特定系统的第一次文件系统备份之前启动 **pre-exec** 脚本，同时在备份之后启动 **post-exec** 脚本。在这种情况下无法导出 BDACC，因为该变量与单个文件系统对象而非整个客户机系统(主机)相关。
- 在 Windows 系统上，必须指定完整的文件名，其中包括扩展名(例如 .exe 或 .bat)。
- 指定脚本名称时，如果因路径中有空格而需要使用单引号(UNIX 系统中)或双引号(Windows 系统中)，则永远不要使用两者的组合。或者使用单引号，或者使用双引号。例如，"S'ilvousplat.bat" 错误，而允许使用 S'ilvousplat.bat。
- 成功完成后，**pre-exec** 或 **post-exec** 命令的退出值必须为零。
- 如果 **pre-exec** 命令失败(返回非零值)，则中止此对象的备份。随后将对象的状态设置为 Aborted，并且磁盘代理停止处理，但执行 **post-exec** 命令(除非 **post-exec** 命令与 BDACC 环境变量相关)。不存在任何对象的备份。
- 如果 **post-exec** 命令失败(返回非零值)，则将对象的状态设置为 Aborted。存在对象的备份，并且可以还原数据。
- 如果客户机上没有可执行脚本或如果脚本的路径错误，则 Data Protector 显示脚本失败和会话中止的错误消息。
- 默认情况下，在预览备份期间不执行 **pre-exec** 和 **post-exec** 命令。该行为由 ExecScriptOnPreview 全局选项定义。
- 处理 **pre-exec** 和 **post-exec** 命令的方式与处理命令提示符下输入的命令相同。但是，不允许使用特殊字符 ?、\*、"、|、< 和 >。
- 运行 **pre-exec** 或 **post-exec** 命令时，无法中止备份会话。
- **pre-exec** 和 **post-exec** 进程运行于后台模式。因此，不要在 **pre-exec** 和 **post-exec** 命令中使用需要用户交互的命令。
- 提供超时。默认情况下，**pre-exec** 和 **post-exec** 脚本必须至少每隔 15 分钟发送一些输出，否则将中止脚本。通过修改 ScriptOutputTimeout 全局选项可以更改此时间间隔。
- **pre-exec** 和 **post-exec** 命令的任何输出都写入 IDB，并显示在 Data Protector 图形用户界面中。
- 在 UNIX 系统中，**pre-** 或 **post-exec** 脚本可能会停止响应，因为它在启动新进程之前未关闭所有文件描述符。如果新进程在后台运行并且不退出，例如数据库服务器进程(dbstart)，则脚本将停止响应。  
可以使用 detach 命令。detach.c 文件中提供 detach 命令的源，但不支持该源。例如：  
/opt/omni/bin/utilns/detach pre\_script [arguments...]
- 默认情况下，**pre-exec** 和 **post-exec** 命令应至少每隔 120 分钟向磁盘代理发送一次输出，否则将中止对象的备份。通过修改 SmDaIdleTimeout 全局选项可以更改此时间间隔。
- 在 UNIX 系统上，由命令写入 stdout 的文本将发送到会话管理器，并写入数据库。stderr 将重定向到 /dev/null。可以将其重定向到 stdout，以获取记录到数据库的错误消息。

## 安全注意事项

**pre-exec** 和 **post-exec** 命令可能有危险，因为如果未经授权的人员使用这些命令，可能会产生大量攻击。如果不使用这些命令，建议将其禁用。此外，如果要使用 **pre-exec** 和 **post-**

**exec** 脚本，请将其放在安全位置，以防未经授权的人员修改这些脚本。

通过将 **StrictSecurityFlag** 全局选项设置为 **0x0100**，仅允许具有作为 **root** 备份或作为 **root** 还原权限的用户运行 **pre-post-exec** 命令。

通过在特定客户机上的 **omnirc** 文件中添加 **OB20EXECCOFF=1** 这一行，可以对任何备份对象禁用 **pre-exec** 和 **post-exec** 脚本。要在所有客户机上都禁止执行远程会话 **pre-exec** 和 **post-exec** 命令，请向特定客户机上的 **omnirc** 文件中添加 **OB2REXECOFF=1**。

通过指定允许哪些 **Cell Manager** 访问客户机，可以保护客户机。只有受到允许的 **Cell Manager** 能够在客户机上执行 **pre-exec** 和 **post-exec** 命令。

## 指定备份对象的 **pre-exec** 和 **post-exec** 命令

### 指定所有对象的 **pre-exec** 和 **post-exec** 命令

要指定所保存的备份规范中所有对象的 **pre-exec** 和 **post-exec** 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 双击要为其指定 **pre-exec** 和 **post-exec** 命令的备份规范，然后单击**选项**选项卡。
4. 在“文件系统选项”(磁盘映像备份的已保存备份规范中的“**Disk Image 选项**”)下，单击**高级**。
5. 在“文件系统选项”(磁盘映像备份的“**Disk Image 选项**”)对话框的“选项”选项卡中，在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
6. 单击**确定**，然后单击**应用**以保存更改。

### 指定单独对象的 **pre-exec** 和 **post-exec** 命令

要仅指定所保存的备份规范中单独对象的 **pre-exec** 和 **post-exec** 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如**文件系统**)。此时将显示所保存的全部备份规范。
3. 双击要为其指定 **pre-exec** 和 **post-exec** 命令的备份规范，然后单击**备份对象摘要**选项卡。
4. 右键单击对象，然后单击**属性**。
5. 在“对象属性”对话框中，单击**选项**选项卡。
6. 在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
7. 单击**确定**，然后单击**应用**以保存更改。

### 指定集成的 **pre-exec** 和 **post-exec** 命令

备份集成(例如 **Oracle**)时，将数据库视为一个对象，因此在数据库备份前后执行这些命令。这些命令在应用程序客户机上执行。

要指定所保存的备份规范中集合的 **pre-exec** 和 **post-exec** 命令，请执行以下步骤：

1. 在上下文列表中，单击**备份**。
2. 在范围窗格中，展开**备份规范**，然后展开备份规范的相应类型(例如 **Oracle Server**)。此时将显示所保存的全部备份规范。
3. 双击要为其指定 **pre-exec** 和 **post-exec** 命令的备份规范，然后单击**选项**选项卡。
4. 在“应用程序特有选项”下，单击**高级**。
5. 在“应用程序特有选项”对话框中，在 **Pre-exec** 和/或 **Post-exec** 文本框中填写文件名或路径名。
6. 单击**确定**，然后单击**应用**以保存更改。

## 关于备份计划

### 重要：

借助 **Data Protector 10.00**，基本计划程序和高级计划程序已过时，被基于 **Web** 的新计划程序所替代。升级 **Data Protector** 时，所有现有的 **Data Protector** 计划会自动迁移至新的计划程序。

可以配置无人看管备份，具体方法是排定备份会话使其在特定的时间执行。计划可按照每天、每周或每月的间隔进行设置。此外，您也可以指定计划选项，如优先级、网络负载和数据保护。

有关如何在 **Data Protector** 中创建和编辑计划的更多信息，请参见 [计划程序 \(第 92 页\)](#)。

## 运行连续备份

一个备份完成之后可以启动另一个备份。例如，文件系统备份完成之后可以启动 **Oracle** 数据库的备份。

在第一个备份规范中使用 **post-exec** 命令启动连续备份。

### 步骤

1. 计划第一个备份。
2. 单击**选项**选项卡，然后在**备份规范选项**下单击**高级**。
3. 在 **Post-exec** 文本框中，输入含有希望在完成第一个备份后要启动的备份规范的名称的 **omnib** 命令(例如 `omnib -datalist name_of_the_backup_specification`)，然后单击**确定**。

### 提示：

还可以自行指定检查第一个备份的状态的脚本。

## 关于备份规范组

通过 **Data Protector** 可以将备份规范划分为不同的组。例如，如果管理大量备份规范，并且希望按常见特征将其分组，这一点会很有用。

将备份规范划分为有意义的组可便于查找和维护单独的备份规范。这样还可以将模板中的公共选项设置应用于整个组。例如，如果要将设备列表更改为组中的所有备份规范，则可以有选择地应用模板的设备设置。

**提示：**  
可以将模板中的公共选项设置(例如用于设备的)应用于一组备份规范。选择组中的所有备份规范(单击组名，然后按 **Ctrl+A**)，右键单击目标组，然后单击**应用模板**。

**注意：**  
**Data Protector GUI** 所能显示的备份规范数有限。可显示的备份规范数量取决于备份规范的参数大小(名称、组、所有权信息以及备份规范是否为负载均衡的信息)。此大小不应超过 **80 KB**。

## 备份规范组的示例

大型企业的备份规范可能会以如下方式组织：

User_files	此组包含对 10 个部门中每个部门的所有用户每周执行一次完整备份的备份规范。
SERVERS_DR	此组包含供公司服务器为灾难恢复做准备的备份规范。每次安装新服务器时，都会创建新的备份规范，并将其添加到此组。
END_USER_ARCHIVE	此组用于保存按最终用户请求生成的备份规范。例如，要释放磁盘空间的最终用户必须首先将其硬盘存档。

## 查看备份规范组

**Data Protector** 帮助中的过程假定您使用默认的备份视图(按类型)。可以更改视图，以便查看按组排列的备份规范。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，选择**分组依据**。

## 创建备份规范组

可以使用各种标准创建不同的备份规范组。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。此时将在范围窗格中的“备份规范”下显示可用备份组的列表。

3. 右键单击**备份规范**项，然后单击**添加组**。此时将出现“添加新组”对话框。
  4. 在“名称”文本框中，输入新组的名称，然后单击**确定**。
- 此时新备份规范组将显示在“备份规范”项下。现在可以将备份规范添加到相应的组中。

## 将备份规范保存到组中

可以将新的备份规范保存到一个特定的组中。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。此时将在范围窗格中的“备份规范”下显示可用备份组的列表。
3. 展开**备份规范**，右键单击要向其添加备份规范的组，然后单击**添加备份**以打开备份向导。
4. 遵循向导创建新的备份规范。在向导的最后一页(“保存”、“启动”或“预览”页)中，单击**另存为**。此时将显示“将备份另存为”对话框。
5. 在“名称”文本框中，输入备份规范的名称。
6. 在“组”下拉列表中，选择要向其保存备份规范的组，然后单击**确定**以保存规范，然后退出向导。默认情况下，显示的备份组是被右键单击以启动向导的那个备份组。

此时将在所选组下显示保存的备份规范。

## 在各个组之间移动备份规范或模板

可以将备份规范或模板从一个备份组移至另一个备份组。

### 步骤

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。此时将在范围窗格中的“备份规范”和“模板”下显示可用备份组的列表。
3. 展开**备份规范或模板**以及具有要移动的备份规范或模板的组。
4. 右键单击要移动的备份规范或模板，然后单击**更改组**。此时将显示“更改组”对话框。  
如果显示备份规范属性，则禁用**更改组**选项。
5. 在“名称”下拉列表中，选择要将备份规范或模板移至的组，然后单击**确定**。

此时备份规范或模板将显示在其新组下。

## 删除备份规范组

可以删除不再需要的备份规范组。

## 步骤

1. 在上下文列表中，单击**备份**。
2. 在“视图”菜单中，单击**按组**。
3. 展开**备份规范**项和**模板**项。此时将显示可用备份组的列表。
4. 展开要删除的组。

**重要：**

无法删除包含备份规范和模板的组。必须首先从组中删除或移动备份规范和模板。

5. 右键单击目标组，然后单击**删除组**。

此时已删除目标备份规范组。

## 关于 Windows 系统备份

备份过程与标准备份过程相同，但有一些方面是 Windows 所特有的。

### 限制

要运行 VSS 文件系统备份，系统中必须至少有一个 NTFS 文件系统。

### 备份什么？

磁盘驱动器上的文件系统备份涉及读取目录结构，所选磁盘驱动器上的文件内容，以及有关文件和目录的 Windows 特有信息。

### Windows Server 2012

- 压缩文件以压缩格式备份和还原
- 加密文件以加密格式备份和还原

### Windows 特有信息

- 完整 Unicode 文件名
- FAT16、FAT32、VFAT 和 NTFS 属性

备份文件后，即清除其存档属性。通过设置备份规范的高级文件系统备份选项中的不使用归档属性选项，可以更改此行为。

- NTFS 备用数据流
- NTFS 安全数据
- 目录共享信息

如果通过网络共享目录，则默认情况下将备份共享信息。还原期间，默认情况下将还原共享信息，还原后将在网络上共享该目录。通过清除**备份目录的共享信息**选项，可以更改此行为。



## 不备份什么？

在备份规范中，可以指定备份要排除或跳过的文件的列表(专用排除列表)。除了专用排除列表以外，默认情况下 Data Protector 将排除以下内容：

### Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012：

- Windows 客户机或 Cell Manager(仅限 Windows Server 2008)备份的 Windows 客户机备份中的默认 Data Protector 日志文件目录。
- Windows 客户机或 Cell Manager(仅限 Windows Server 2008)备份的 Windows 客户机备份中的默认 Data Protector 临时文件目录。
- Windows Cell Manager(仅限 Windows Server 2008)备份中的内部数据库目录。
- 注册表项 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup 中指定的文件。

### Windows Server 2012

- 使用复原文件系统 (ReFS) 格式化的卷

### 其他 Windows 系统

- Windows 客户机备份中的默认 Data Protector 日志文件目录。
- Windows 客户机备份中的默认 Data Protector 临时文件目录。
- 注册表项 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup 中指定的文件。

例如，即使您在备份规范中选择了内部数据库目录，系统也会从 Cell Manager 备份中排除该目录。这是因为必须以一种特殊的方式备份 IDB 才能确保数据一致性。

所有 Data Protector 主机都将证书和私钥文件保留在以下位置：

- <programdata>/Omniback/Config/sscertificates (在 Windows 中)
- /etc/opt/omni/config/sscertificates/ (在 Linux 中)

在文件系统备份期间，如果这些文件包含在上述位置中，则会备份除私钥以外的其他所有文件。

## NTFS 3.1 文件系统功能

- NTFS 3.1 文件系统支持重分析点  
卷装入点、单实例存储 (SIS) 和目录联接都基于重解析点这个概念。这些重解析点被选择为任何其他文件系统对象。
- NTFS 3.1 文件系统支持符号链接，此概念随 Windows Vista 和 Windows Server 2008 操作系统引入。

**Data Protector** 以处理 **NTFS** 重分析点的方式处理符号链接。

- **NTFS 3.1** 文件系统支持稀疏文件，这是减少磁盘空间分配量的一种高效方式。  
以稀疏方式备份这些文件可节省磁带空间。备份稀疏文件后，只能向 **NTFS 3.1** 文件系统以稀疏方式还原这些文件。
- 某些 **NTFS 3.1** 特有的功能由保留自身数据记录的系统服务控制。将这些数据结构作为 **CONFIGURATION** 的一部分进行备份。
- **NTFS 3.1** 文件系统支持与其他备用数据流一起由 **Data Protector** 备份的对象 ID。
- 加密的文件  
对于由 **Microsoft** 加密的 **NTFS 3.1** 文件均采用加密方式进行备份和还原，但只有在将这些文件解密后才能正确查看其内容。

## 重分析点

重解析点是附加了一种唯一标记(称为重分析点 ID)的普通文件系统对象。**NTFS 3.1** 目录或文件可以包含重分析点，此点通常通过定向到另一位置中的数据来模仿内容。

默认情况下，**Data Protector** 在遇到重分析点时，不遵循重分析点 ID。这也称为备份原始重分析点。这种情况影响配置备份的方式：

- 如果使用磁盘传递配置备份，则将对所有数据备份一次。
- 如果备份包含重分析点的文件系统或驱动器，则必须确保对重分析点所指的数据进行了备份。例如，不遵循 **Windows** 目录连接重分析点，因此必须单独备份联接。但 **SIS** 重分析点例外。

单实例存储 (**SIS**) 服务定期检查磁盘上的文件。如果服务检测到多个相同的文件，则会将这些文件替换为重分析点，并将数据存储在与常用的存储库中，从而减少磁盘空间的使用。

通过重分析点，可以按逻辑卷的形式装载磁盘驱动器。**Data Protector** 将装载的卷视为普通驱动器，因此这些卷可见，并作为可选择进行备份的对象。

## 稀疏文件

稀疏文件包含许多组零数据 - 例如，远远多于压缩文件。在备份时，**Data Protector** 自动跳过零的部分，以便仅为非零部分分配备份设备上的介质空间。

**UNIX** 和 **Windows** 稀疏文件不兼容。

## 备份系统磁盘时发出警告

系统磁盘上的某些文件始终繁忙，因此任何应用程序(包括磁盘代理)都无法将其打开。这些文件的内容只能作为 **CONFIGURATION** 的一部分进行备份。

文件系统备份访问这些文件时(如备份整个系统磁盘时)，**Data Protector** 未能打开这些文件，并报告警告或错误。

虽然从文件系统备份的角度看此行为正确，但它会产生可管理性问题。由于始终报告大量警告，因此可能遗漏了另一个文件的失败。

从文件系统备份中排除通过 **CONFIGURATION** 备份进行备份的文件可避免出现警告。

**注意：**

备份不活动的系统磁盘(例如在双引导情况下)时，以前列出的文件不是当前活动 **CONFIGURATION** 的一部分。可以在文件系统备份中备份这些文件，因此不应排除这些文件。

## 配置备份 (Windows)

对于 Windows 操作系统维护的特殊数据结构，不将其视为文件系统备份的一部分。通过 **Data Protector**，可以备份一种特殊的数据结构，称为 **CONFIGURATION**。

要执行配置备份，请在创建文件系统备份规范时，选择对象 **CONFIGURATION** 或只选择其某些部分。如果在备份向导中选择 **CONFIGURATION**，则始终备份事件日志、配置文件和用户磁盘配额。

在 Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012 上，使用 Microsoft 卷影复制服务执行配置备份。

## 限制

- 一次只能在系统中运行一个 **CONFIGURATION** 备份。
- 应成对备份 **Active Directory** 服务和 **SysVol**。

## Windows 配置对象

- **Active Directory** 服务
- 证书服务器
- **COM+** 类注册数据库 (**ComPlusDatabase**)
- **DFS**
- **DHCP**
- **DNS** 服务器
- **EISA** 实用程序分区
- 事件日志
- 文件复制服务
- **Internet Information Server (IIS)**
- 用户配置文件 (**Documents and Settings**)
- **Windows** 注册表
- 可移动存储管理器数据库
- **SystemRecoveryData**
- **SysVol**
- 终端服务数据库
- 用户磁盘配额 (**QuotaInformation**)
- **WINS** 服务器

**CONFIGURATION** 在各种 Windows 系统中有所不同。

对于某些对象，必须考虑一些特殊的要点。以下各节中列出了这些要点。

## Active Directory

备份 Active Directory 服务时，也同时备份 File Replication Service 和分布式文件系统 (Distributed File System, DFS)。有关复制文件和分发文件的所有配置信息都存储在 Active Directory 中。

## DFS

Data Protector 将 Windows 分布式文件系统 (Distributed File System, DFS) 备份为以下某项的一部分：

- Windows 注册表(如果以独立模式配置 DFS)
- Windows Active Directory(如果以域模式配置 DFS)

## DHCP 和 WINS

Data Protector 备份 DHCP 和/或 WINS 数据库时，将停止相应的服务，然后在备份数据库之后重新启动该服务。建议在工作时间之外计划对运行 DHCP 和/或 WINS 服务的服务器进行 CONFIGURATION 备份。

DHCP 和 WINS 服务还自行提供其数据库的内部备份副本。如果环境不能接受偶尔关闭这些服务，则可以从 Data Protector 备份中排除这些服务，并通过文件系统备份来备份数据库的内部备份副本。有关内部备份副本的位置以及如何确保足够频繁地制作这些副本的详细信息，请参见 Microsoft MSDN 文档。

## 配置文件

如果选择整个系统进行备份，则将备份两次“配置文件”(一次作为文件系统备份的一部分，一次作为 CONFIGURATION 的一部分)。要避免出现这种情况，请从文件系统备份中排除配置文件数据。用户配置文件数据位于 c:\Documents and Settings 目录中：

这些目录包含系统中配置的所有用户配置文件，并且由 Data Protector 进行备份。如果为多个用户配置系统，则每个定义的用户都有一个单独的用户配置文件。例如，All Users 和 Default User 配置文件包含所有已定义用户常用的配置文件组件和分配给新创建用户的配置文件组件。

Data Protector 从以下注册表项读取配置文件的位置：

HKEY\_USERS\DEFAULT\Software\Microsoft\Windows\

CurrentVersion\Explorer\Shell Folders

(有关常用配置文件组件的信息所在的位置)

HKEY\_USERS\DEFAULT\Software\Microsoft\Windows\

CurrentVersion\Explorer\User Shell Folders

## 可移动存储管理器数据库

在 Windows Vista 和 Windows Server 2008 操作系统中，要启用可移动存储管理器数据库配置对象的备份，请确保在将备份的系统中安装可移动存储管理器。

## 终端服务数据库

在 Windows Vista 和 Windows Server 2008 操作系统中，要启用终端服务数据库配置对象的备份，请确保在将备份的系统中安装终端服务授权服务。

## Windows 服务

备份 Windows 服务意味着备份由相应服务使用的数据结构。有一个特定的数据库将导出(转储)到随后备份的文件中。如果在备份向导中选择 **CONFIGURATION**，则将始终备份 Windows 服务。

Windows 服务必须正常运行，以使 **Data Protector** 可以检测出该服务，并在备份向导中提供它作为一个可选项。如果在备份时服务未运行，则相应的备份对象将失败。

要备份某个服务，请在 **CONFIGURATION** 下选择相应的文件夹。例如，如果使用 **Active Directory** 发布证书吊销列表 (CRLs)，则将 **Active Directory** 服务连同证书服务器一起备份。

## 系统状态数据备份

Windows 系统状态由与 Windows 系统各个方面相关的若干元素组成。这些元素在其各自的 Windows 备份对象下形成各自的结构。

Windows 系统状态不是可选择的备份项。通过 **Data Protector**，可以备份单独的对象，如注册表或 COM+ 类注册数据库。建议备份整个 **CONFIGURATION** 树。在 Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012 系统上，需要用启用了 **使用卷影复制** 选项的文件系统备份功能备份特定卷或整个客户机系统。

系统状态包括以下内容：

- 引导文件：Ntldr.exe、Ntdetect.com 和 boot.ini
- Registry 和 COM+ Class Registration Database (ComPlusDatabase)
- System File Protection 服务(保存在 System Volume Information 目录中)

如果安装和配置该服务，则 Windows Server 系统的系统状态数据还包括：

- ActiveDirectoryService
- CertificateServer
- Cluster Service information
- IIS Metadirectory
- RemoteStorageService
- RemovableStorageManagementDatabase
- SystemFileProtection

- SYSVOL directory
- TerminalServiceDatabase

在 Windows Vista、Windows 7、Windows 8、Windows Server 2008 和 Windows Server 2012 系统中，系统状态数据还包括属于可安装的其他服务器角色或服务的数据。

## 远程存储服务

远程存储服务用于自动将不常访问的文件从本地移至远程存储。打开此类文件时，将自动检索远程文件。尽管 RSS 数据库是系统状态数据的一部分，但要手动备份这些数据库。

### 远程存储服务：

- 远程存储引擎： *%SystemRoot%\system32\RsEng.exe*  
协调用于存储不常用数据的服务和管理工具
- 远程存储文件： *%SystemRoot%\system32\RsFsa.exe*  
管理在远程存储文件上的操作
- 远程存储通知： *%SystemRoot%\system32\RsNotify.exe*  
向客户机通知有关检索的数据

### 远程存储数据库：

远程存储数据库位于以下目录中： *%SystemRoot%\system32\RemoteStorage*

- RSS 引擎数据库： *%SystemRoot%\system32\RemoteStorage\EngDb*
- RSS 引擎备份数据库： *%SystemRoot%\system32\RemoteStorage\EngDb.bak*
- RSS 文件数据库： *%SystemRoot%\system32\RemoteStorage\FsaDb*
- RSS 跟踪数据库： *%SystemRoot%\system32\RemoteStorage\Trace*

## 可移动存储管理器数据库

可以备份可移动存储数据库，但此服务不用于 Data Protector 介质管理。由 Data Protector 配置设备之前，必须禁用与机械手介质更换器配合使用的本机机械手驱动程序。

## 系统文件保护

重新启动计算机之后，系统文件保护服务扫描并验证所有受保护系统文件的版本。如果系统文件保护服务发现受保护文件被覆盖，则该服务将检索文件的正确版本，然后替换错误的文件。通过 Data Protector，可以备份并还原受保护文件，以使其不被覆盖。在标准文件系统备份过程中可以使用移动繁忙文件选项备份受保护文件。

## 关于 UNIX 系统备份

要在 UNIX 系统中执行备份，请使用标准备份过程。在备份使用 NFS 的磁盘时，对于 VxFS 快照备份，或对于 UNIX 磁盘映像备份，需要执行某些额外的步骤。

## 限制

- 备份由 **NFS** 装载的文件系统时，并不保留所有文件属性。
- 可以备份的最大文件大小取决于操作系统和文件系统的限制。

有关受支持平台和已知限制的完整列表，请参见《**Data Protector** 产品声明、软件说明和参考》。

## 备份什么？

- **Data Protector** 备份目录结构、常规文件和特殊文件。特殊文件分为字符设备文件、块设备文件、UNIX 域套接字、FIFO 文件、HP-UX 网络特殊文件和 XENIX 特殊命名文件。
- 不遵循符号链接，将其备份为符号链接。
- 不遵循装入点，将其备份为普通空目录。
- 如果有多个硬链接引用同一个文件，则只备份该文件一次。通过设置**将 POSIX 硬链接备份为文件**选项可以更改此行为。
- 基本 **ACL**(文件权限属性)和时间属性与所有受支持的 **UNIX** 平台上的文件一并进行备份。但是，在某些平台上对扩展 **ACL** 的支持有限。有关详细信息，请参见“**Data Protector** 平台和集成支持矩阵”，网址为 <https://softwaresupport.softwaregrp.com/>。读取文件之前保存上次访问每个文件的时间，然后在备份文件之后返回该原始值。通过设置**不保留访问时间属性**选项可以更改此行为。

## 应当从 **UNIX** 文件系统备份中排除什么？

- 内部数据库目录，它们需要通过特殊方式进行备份(在线)。
- 临时目录

## NFS 备份

**NFS**(网络文件系统)是一种分布式文件系统协议，利用该协议，计算机可以通过网络访问文件，就像在其本地磁盘上一样。通过 **NFS** 可以备份从本地可访问的远程 **UNIX** 系统中的文件系统。

## 何时使用 **NFS** 备份？

- 当系统不是 **Data Protector** 单元的一部分或未安装磁盘代理时。
- 要备份 **Data Protector** 不支持的系统平台时。

当配置常规文件系统备份时，建议从备份中排除由 **NFS** 装载的文件系统。这样可以避免出现警告消息，而如果还要备份磁盘实际所在的系统，则可以避免对相同磁盘进行重复备份。

## 限制

- 可以备份 HP-UX、Solaris 和 Linux 客户机上由 NFS 装载的卷。不能备份软链接、字符和设备文件。有关受支持平台的详细信息，请参见 <https://softwaresupport.softwaregrp.com/> 上的最新支持矩阵。
- 不保留 ACL(访问控制列表)属性。NFS 不支持对远程文件采用 ACL。单独的手动条目可指定各种系统调用、库调用和命令的行为。通过网络传输具有可选条目的文件或操纵远程文件时，可以无提示地删除可选条目。

HP OpenVMS 文件系统的备份过程与标准文件系统备份过程相同，但有一些方面是 OpenVMS 所特有的。

## 先决条件

- 要备份 OpenVMS 系统上的数据，请在 OpenVMS 系统上安装 OpenVMS 磁带客户机。
- 要将连接到 OpenVMS 系统的备份设备与 Data Protector 一起使用，请在 OpenVMS 系统上安装 General 介质代理。

## 限制

- 任何输入到 GUI 中或传递到 CLI 的文件规范都必须采用 UNIX 样式语法  
`/disk/directory1/directory2/filename.ext.n`  
字符串应当以斜线开头，后跟磁盘、目录和文件名，其间以斜线分隔。  
请勿在磁盘名称后加冒号。  
版本号前应使用句号而非分号。  
OpenVMS 文件的文件规范不区分大小写，但位于 ODS-5 磁盘上的文件除外。例如，OpenVMS 文件规范  
`$1$DGA100:[bUSERS.DOE]LOGIN.COM';1`  
必须按以下形式指定：  
`/$1$DGA100/USERS/DOE/LOGIN.COM.1`
- 没有隐式版本号。必须始终指定版本号。仅备份选定的备份文件版本。如果要包括文件的所有版本，请在 GUI 窗口中进行选择，或者使用 CLI 在 **仅有 (-only)** 选项下包括文件规范，其中包括版本号通配符，如下所示：  
`/DKA1/dir1/filename.txt.*`
- 要成功备份带写入保护的卷影磁盘，请在备份规范中启用 **不保留访问时间属性** 选项。
- 如果备份期间启用了 **不保留访问时间属性 (Do not preserve access time attributes)** 选项，则上次访问日期将更新为 ODS-5 磁盘上的当前日期和时间。在 ODS-2 磁盘上，此选项无效，因而所有日期保持不变。
- 在 OpenVMS 上不提供磁盘映像备份功能。没有与“BACKUP/PHYSICAL”等效的功能。
- OpenVMS 上不提供将 **POSIX 硬链接** 作为文件进行备份 (`-hlink`)、软件压缩 (`-compress`) 和 **编码** (`-encode`) 选项。



对于具有多个目录条目的文件，仅使用主路径名备份一次。将次路径条目另存为软链接。还原期间，还会还原这些额外的路径条目。

没有与 BACKUP/IMAGE 等效的功能。要制作 OpenVMS 可引导系统磁盘的还原副本，必须使用 OpenVMS WRITEBOOT 实用程序向还原磁盘上写入引导块。

- 无论启用还是禁用了**在备份期间锁定文件 (-lock)**选项，始终都会锁定要备份的文件。如果启用了 -lock 选项，则不会备份任何打开(用于写入)的文件。如果禁用了 -lock 选项，将备份任何打开的文件。
- **pre-exec** 和 **post-exec** 命令过程的默认设备和目录是 /omni\$root/bin。要在任何其他地方放置命令过程，文件规范所包含的设备和目录路径必须采用 UNIX 样式格式。例如：  
/SYS\$MANAGER/DP\_SAVE1.COM
- 对**跳过 (-skip)**或**仅有 (-only)**过滤器指定通配符时，使用“\*”代表多个字符，使用“?”代表单个字符。
- Data Protector 文件库在 OpenVMS ODS-2 磁盘上不受支持。
- 在 OpenVMS 系统上，Data Protector 不支持卷和卷集上的磁盘配额。

要对启用磁盘配额的卷上的数据执行备份，请配置 **pre-exec** 脚本，以便在开始备份之前在涉及的卷上禁用磁盘配额，并配置 **post-exec** 脚本，以便在完成备份之后启用磁盘配额。

## 备份什么？

目录结构和文件与以下文件系统信息一并进行备份：

- 文件和目录属性
- ACL(访问控制列表)

只能从装入的 FILES-11 ODS-2 或 ODS-5 卷备份文件。

## 关于 Novell Open Enterprise Server (OES) 备份

Novell OES 的备份过程与标准备份过程相同，但有一些方面是 Novell OES 所特有的。

### 先决条件

- 必须在 Novell OES 系统上安装 Data Protector 磁盘代理。
- 必须以双模式加载 Target Service Agent for File Systems (tsafs)。
- 对于 NDS/eDirectory 备份，必须加载 Target Service Agent for Novell Directory Services (tsands)。
- 对于 GroupWise 备份，必须加载 GroupWise Target Service Agent for File Systems (tsafsgw)。
- 必须选择用于登录 Novell OES 备份服务的用户帐户，并保存到 HPLOGIN.NLM 文件。可以使用任何用户帐户，但用于备份的文件和目录将仅限于用户帐户的那些文件和目录。
- 必须在 Novell OES 系统上安装 Storage Management Services (SMS)。

## 限制

- 不支持软件数据压缩。即使在选择了备份选项软件压缩时，也不会影响备份的数据。

## 备份和还原压缩文件

Novell OES 提供文件压缩功能。默认情况下，Data Protector 以其压缩格式备份压缩文件，随后以其压缩格式还原压缩文件。只能将此类文件还原到具有压缩卷的 Novell OES。

## 备份什么？

- 本机 Linux 卷
- Novell GroupWise 数据

备份每个文件之后，将清除文件的存档标志，并设置存档日期/时间。

## 配置 Novell OES

### 使用 HPLOGIN 实用程序保存用户名和密码

HPLOGIN 实用程序位于目录 /opt/omni/sbin 中。运行此实用程序，将正确的用户凭据(用户名和密码)保存到文件 /root/OMNI\$CFG.DAT 中。

#### 步骤

1. 将当前工作目录更改为 /opt/omni/sbin。
2. 运行 HPLOGIN 实用程序：

```
./hplogin
```

### 以双模式加载 Target Service Agent for File Systems (tsafs)

#### 步骤

1. 在目标系统上配置 TSA。默认情况下以 Linux 模式加载 TSA。将其更改为双模式：
  - a. 将当前工作目录更改为 /opt/novell/sms/bin。
  - b. 检查是否已加载 tsafs：

```
./smsconfig -t
```
  - c. 如果已加载，则将其卸载：

```
./smsconfig -u tsafs
```
  - d. 以双模式加载 TSA：

```
./smsconfig -l tsafs --tsaMode=Dual
```
2. Open Enterprise Server Linux 上 tsafs 配置文件的完整路径名为 /etc/opt/novell/sms/tsafs.conf。加载 TSA 后，它读取其默认配置的配置文件。每

次加载 TSA 时，都要将此文件配置为在双模式下自动加载 tsafs。

3. 编辑文件 `/etc/opt/novell/sms/tsafs.conf`，将 `tsamode` 从 `Linux` 改为 `dual`，然后保存文件：

```
tsamode=Dual
```

## 加载 Target Service Agent for Novell Directory Services (tsands)

可以手动加载 `tsands` 代理或将它配置为在 Novell OES 启动过程中自动加载。

### 步骤

- 要手动加载该代理，请执行以下操作：
  1. 打开终端窗口。
  2. 将当前目录更改为 `/opt/novell/sms/bin`。
  3. 运行以下命令以检查该代理是否已加载：

```
./smsconfig -t
```
  4. 如果该代理未加载，请加载它：

```
./smsconfig -l tsands
```
- 要配置该代理的自动加载，请执行以下操作：
  1. 将以下行添加到配置文件 `/etc/opt/novell/sms/smdrd.conf` 中：

```
autoload: tsands
```

## 加载 GroupWise Target Service Agent for File Systems (tsafsgw)

可以手动加载 `tsafsgw` 代理或将它配置为在 Novell OES 启动过程中自动加载。

### 步骤

- 要手动加载该代理，请执行以下操作：
  1. 打开终端窗口。
  2. 将当前目录更改为 `/opt/novell/sms/bin`。
  3. 运行以下命令以检查该代理是否已加载：

```
./smsconfig -t
```
  4. 如果该代理未加载，请通过提供合适参数来加载它：

```
./smsconfig -l tsafsgw --home DomainDirectory --home PostOfficeDirectory
```
- 要配置该代理的自动加载，请执行以下操作：
  1. 将以下行添加到配置文件 `/etc/opt/novell/sms/smdrd.conf` 中(将参数占位符替换为实际值)：

```
autoload: tsafsgw --home DomainDirectory --home PostOfficeDirectory
```

## 关于备份性能

配置备份时，应考虑备份性能因素。由于可变因素和排列组合众多，因此无法给出满足所有用户要求并且经济上负担得起的明确建议。但是，尝试提高备份或还原的性能时，应考虑以下几点：

### 基础架构

基础结构对备份和还原的性能有着巨大影响。最重要的因素是要有多条并行性的数据路径和使用高速设备。

- 网络与本地备份和还原

通过网络发送数据会引入额外的开销，因为网络也成为性能考虑因素的一部分。对于以下情况，**Data Protector** 处理数据流的方式有所不同：

- 网络数据流：磁盘到内存到网络到内存到设备
- 本地数据流：磁盘到内存到设备

要最大程度地提高性能，建议对大容量数据流使用本地备份配置。

- 所使用的设备、计算机系统本身以及硬件的并行使用也对性能有明显的影响。

要努力使备份或还原性能达到最大限度，可以：

- 设置适当的并发以实现设备流式传送
- 优化段和块大小
- 调整磁盘代理缓冲区的数量
- 使用软件或硬件压缩
- 使用基于磁盘的备份设备 — 文件库
- 计划完整备份和增量备份
- 使用合成备份和磁盘分段等高级备份策略
- 优化备份对象向介质的分布
- 禁用文件系统扫描

### 对象镜像和备份性能

对象镜像对备份性能有影响。在 **Cell Manager** 和介质代理客户机上，写入镜像的影响与备份额外对象的影响相同。在这些系统中，备份性能的降低将取决于镜像数。在磁盘代理上，镜像对性能无影响，因为备份对象只读取一次。

备份性能还取决于设备块大小和设备连接等因素。如果备份和对象镜像所用设备的块大小不同，则将在会话期间将镜像数据重新打包，此过程会占用额外的时间和资源。如果通过网络传输数据，则将增加网络负载并消耗更多时间。

## 设备之外的高性能硬件

计算机系统自身读取磁盘和写入设备的速度对性能有着直接影响。备份期间，通过读取磁盘、处理软件压缩(解压缩)等操作加载系统。

除了 I/O 性能和网络类型之外，磁盘读取数据速率和可用 CPU 也是系统自身的重要性能标准。

## 硬件并行性

可以将并行使用多个数据路径作为提高性能的一种非常高效的方法。其中包括网络基础架构。并行性技术在以下情况中大有助益：

- 如果有若干系统在本地备份，即磁盘和相关设备连接到相同的系统。
- 如果通过网络备份若干系统。在这种情况下，网络流量的路由需要经过优化，以使数据路径不发生重叠现象，否则会降低性能。
- 如果有若干对象(磁盘)备份到一个或若干(磁带)设备。
- 如果可以使用特定系统之间的若干专用网络链路。例如，**system\_A** 有 6 个要备份的对象(磁盘)，而 **system\_B** 有 3 个快速磁带设备。解决方案是在 **system\_A** 与 **system\_B** 之间放置 3 条专用于备份的网络链路。
- 如果使用了若干设备，并启用了**负载均衡**选项。

## 并发

为每个介质代理启动的磁盘代理数量称为磁盘代理(备份)并发，使用设备的高级选项或在配置备份时可以修改此项。备份规范中设置的并发优先于设备定义中设置的并发。

Data Protector 提供的默认磁盘代理数足以满足大多数情况。例如，在标准 DDS 设备上，两个磁盘代理可以发送设备流式传送所需的足够数据。对于带有多个驱动器、每个驱动器受一个介质代理控制的库设备，可以单独设置每个驱动器的并发数目。

## 对性能的影响

如果设置正确，则备份并发可提高备份性能。例如，如果您的库设备有四个驱动器，每个驱动器受一个介质代理控制，每个介质代理从两个磁盘代理并发地接收数据，来自八个磁盘的数据同时进行备份。

## 多个数据流

同时可以将磁盘的多个部分备份到多个设备。此方法可提高备份速度，对于将容量很大且速度很快的磁盘备份到相对较慢的设备时很有用。多个磁盘代理从磁盘并行读取数据，并将数据发送到多个介质代理。

请注意，如果通过多个磁盘代理备份一个装载点，数据将包含在多个对象中。要还原整个装载点，必须在一个备份规范中定义装载点的所有部分，然后还原整个会话。

## 设备流式传送

要最大限度地提高设备的性能，必须使其进行流式传送。如果设备可以向介质输送足够的数据，使数据保持不断前移，则设备就是在进行流式传送。否则，必须让磁带停止转动，设备等待更多数据，然后将磁带倒回一些，继续写入磁带等等诸如此类。也就是说，如果向磁带写入的数据速率小于或等于计算机系统可以向设备提供的数据速率，则设备就是在进行流式传送。设备流式传送还取决于其他因素，如网络负载和一次操作中写入备份设备的数据的块大小。在以网络为中心的备份基础架构中，设备流式传送值得关注。对于本地备份(其中磁盘和设备都连接到相同的系统)，如果磁盘足够快，则并发为 1 即可满足需要。

## 如何配置设备流式传送

要使设备可以进行流式传送，必须向设备发送足够数量的数据。**Data Protector** 会为将数据写入设备的每个介质代理启动多个磁盘代理。

## 块大小

段并不作为完整单位，而是分为更小的子单位，称为块。设备硬件按设备类型特有的块大小处理其接收的数据。

**Data Protector** 对于不同的设备类型使用相应的默认设备块大小。块大小适用于 **Data Protector** 创建的所有设备，并适用于不同平台上运行的介质代理。

增加块大小可提高性能。配置新设备时或使用设备的高级选项更改设备属性时，可以调整发送到设备的块。还原时可适应块大小。

### 警告：

为受特定操作系统上所运行的 **Data Protector Media Agent** 控制的设备增加块大小之前，请确保所需块大小不会超过该操作系统支持的默认最大块大小。如果超过限制，则 **Data Protector** 无法从这类设备还原数据。有关是否可以调整最大支持块大小以及如何调整的信息，请参见操作系统文档。

应在格式化磁带之前更改块大小。介质头上写入了设备块大小，以使 **Data Protector** 了解要使用的大小。如果设备的块大小与介质的块大小不同，就会发生错误。

但是，在更改设备的块大小之前，需要检查所使用的主机适配器支持的块大小。老式 SCSI 卡(如 Adaptec 2940)的最小块大小通常为 56 KB。用于较新 SCSI 卡的最小块大小为 64 KB。

通过修改 Windows 介质代理客户机的注册表，可以增加其上的最大块大小。该过程取决于主机总线适配器类型：SCSI、光纤通道或 iSCSI。有关详细信息，请参见链接的示例主题。

更改特定主机总线适配器的块大小之前，请参见供应商文档，或与供应商技术支持人员联系。

## 段大小

介质可划分为数据段、目录段和头段。头信息存储在头段中，大小与块大小相同。数据存储在数据段的数据块中。每个数据段的信息存储在相应的编目段中。这些信息先存储在介质代理内存中，然后写入介质的编目段和 IDB。

段大小(以 MB 为单位度量)是数据段的最大大小。如果要备份大量小型文件，可以通过编目段的最大大小限制实际段大小。段大小可以由用户针对每个设备进行配置，并且在还原期间和导入介质期间会影响性能。配置新设备时或使用设备的高级选项更改设备属性时，可以调整段大小。

最佳段大小取决于设备中使用的介质类型和要备份的数据类型。每盘磁带的平均段数为 50。通过将磁带的本机容量除以 50，可以算出默认段大小。对于所有介质类型，最大编目大小都限制为一个固定数字 (12 MB)。

达到第一个限制后，Data Protector 即完成一个段。备份大量小文件时，将更快地达到介质目录限制，而这会使段大小更小。

## 磁盘代理缓冲区的数量

Data Protector 介质代理和磁盘代理使用内存缓冲器保存等待传输的数据。该内存分为许多个缓冲区(每个磁盘代理对应一个缓冲区，具体取决于设备并发数)。每个缓冲区由 8 磁盘代理缓冲区组成(大小与配置的设备块大小相同)。

配置新设备时或使用设备的高级选项更改设备属性时可以更改此值，但很少有这种必要。更改此设置有两个根本原因：

- 内存不足：介质代理所需的共享内存可以按如下方法计算：

$DAConcurrency * NumberOfBuffers * BlockSize$

例如，将缓冲器的数量从 8 个改为 4 个即可减少 50% 的内存消耗，但也会产生性能问题。

- 流式传送

如果可用网络带宽在备份期间变化很大，则介质代理要有足够的数据可供写入，设备才能保持流式传送模式，这一点很重要。在这种情况下，应增加缓冲器的数量。

## 软件压缩

从磁盘读取数据时，由客户机 CPU 执行软件压缩。这样可减少通过网络发送的数据，但需要客户机提供大量 CPU 资源。

默认情况下，软件压缩处于禁用状态。通常，只有在为了提高性能时才应使用硬件压缩。只应在通过慢速网络对许多系统进行备份时使用软件压缩，这种情况下在通过网络发送数据之前即可压缩这些数据。

如果使用了软件压缩，就会禁用硬件压缩，因为试图压缩数据两次实际上会使数据膨胀。

# 硬件压缩

大多数新型备份设备都提供了内置的硬件压缩功能，在设备配置过程中创建设备文件或 SCSI 地址时可启用该功能。

硬件压缩由一个设备完成，该设备从介质代理客户机收到原始数据，然后以压缩模式将这些数据写入磁带。硬件压缩可以提高磁带驱动器接收数据时的速度，因为写入磁带的数  
据较少。

请考虑以下有关硬件压缩的内容：

- 请小心使用硬件压缩，因为以压缩模式写入的介质不能使用处于非压缩模式的设备读取，反之亦然。
- 请勿同时使用软件和硬件压缩，因为双重压缩会降低性能，并且不会产生更好的压缩结果。
- Ultrium LTO 驱动器使用自动硬件压缩，无法禁用。建议在用 Data Protector 配置 Ultrium LTO 驱动器时使软件压缩选项保持禁用。
- 用不支持硬件压缩的设备读取使用硬件压缩写入的介质时，Data Protector 无法识别介质和读取数据。而是将此类介质视为未知介质或新介质。

配置设备时，如果从下拉列表中选择 SCSI 地址，则 Data Protector 将自动确定设备能否使用硬件压缩。

在 UNIX 系统中，可通过选择硬件压缩设备文件启用硬件压缩。

在 Windows 系统上，如果检测不成功而由您手动输入 SCSI 地址，应在设备/驱动器 SCSI 地址的末尾添加 C，例如：scsi:0:3:0C(如果加载了磁带驱动程序，则为 tape2:0:1:0C)。如果设备支持硬件压缩，则将使用硬件压缩，否则将忽略 C 选项。

要在 Windows 系统上禁用硬件压缩，请在设备/驱动器 SCSI 地址末尾添加 N，例如：scsi:0:3:0N

对于多路径设备，要单独为每个路径设置此选项。

# 磁盘映像与文件系统备份

在磁盘映像备份与文件系统备份之间进行选择时，应考虑其优点和缺点。在大多数情况下，建议采用文件系统备份。

	文件系统备份	磁盘映像备份
备份一致性	文件可以在备份过程中锁定，并以一致的状态进行备份。会保留文件和目录的结构。	文件在备份过程中不会锁定，并以时间点状态进行备份。无法浏览文件和目录的结构。
备份大小	备份数据占用的空间与文件和文件夹数据在备份时的累积大小相同。	备份数据在备份介质上占用的空间与原始备份卷的大小相同。
备份和还原速度	当备份磁盘未满且文件数较少时，备份和还原速度较快。	当备份磁盘已满且存在大量小文件时，备份和还原速度较快。



还原可用性	更容易在还原的文件中导航，因为保留了文件和目录的结构。	会还原整个磁盘或磁盘分区，无法浏览文件和目录的结构。
-------	-----------------------------	----------------------------

**注意：**  
在 Windows 系统中，可以使用 VSS 写入程序执行磁盘映像和文件系统备份。这可确保卷在备份过程中保持未锁定状态，可以由其他应用程序访问。这在备份系统卷时非常重要。

## 将对象分散到多个介质上

可以相应地配置备份，以使备份数据在几个不同配置中的介质上结束。例如，可以配置一个备份，其中一个对象到一个介质，或若干对象到若干介质，并且每个介质都包含每个对象中的数据。

某些条件下，某种分散方式在备份性能方面可能具有优势，但它可能不是最佳的还原配置。应相应地定义备份策略，以使您优化备份的设置(因为经常进行备份)，并同时具有可接受的还原介质情况。

## 文件系统扫描

Data Protector 备份文件之前，将对选择进行备份的树执行一次扫描。这会影响性能。由于 Windows 系统中的快速文件系统扫描和 UNIX 系统中的文件系统扫描功能所产生的影响可忽略不计，因此建议不要仅为提高性能而更改默认设置。

根据要备份的系统，文件系统扫描有所不同：

系统	文件系统扫描功能	如何禁用该扫描功能？
Windows	快速文件系统扫描(始终选择)	可以通过将 OB2NOTREEWALK 选项设置为 1 来禁用文件系统扫描。
	检测 NTFS 硬链接(默认：未选中)	选择检测 NTFS 硬链接选项会使性能显著降低。只有存在 NTFS 硬链接时才应选择它。
UNIX	检测硬链接并计算大小(默认：已选中)	选择将 POSIX 硬链接备份为文件选项会使文件系统扫描不活动。

## 其他性能提示

遵照表中列出的提示，可以提高备份或还原的性能。

什么可提高性能？	如何提高性能？
修补程序	确保已安装与网络性能有关的所有修补程序。

设备的位置	尽可能使用本地设备。
LAN 卡	<p>可以在总线上将 <b>FDDI</b> 卡上移，以使其获得更高的优先级。使用 <b>ftp</b> 在介质代理与磁盘代理系统之间传输大型文件，以查看传输速度与 <b>Data Protector</b> 性能相比如何。</p> <p>请注意，以半双工配置的网卡会降低性能。</p>
高速设备	如果怀疑到磁带设备的持续数据流速度太慢，或设备未正确处理该数据流，可以在介质代理客户机上模拟高速设备。
设备配置	可以调整发送到设备的块以提高性能。
<b>CRC</b> 检查选项	可以禁用 <b>CRC</b> 检查选项。如果启用，则此选项会因 <b>CRC</b> 计算(由介质代理客户机执行)而影响性能。
日志记录和报告级别	<p>如果更新 <b>IDB</b> 所用时间过长，可以通过将日志记录设置为无日志而将其禁用。</p> <p>通过将报告级别设置为“严重”可以过滤消息。</p>
<b>Data Protector</b> 应用程序客户机	如果应用程序客户机( <b>Oracle</b> 、 <b>SAP R/3</b> )的还原会话耗时过长，则您可以减小 <b>SmWaitforNewClient</b> 的值。将其值设置为小于默认值 ( <b>5 分钟</b> )的值。

# 第 11 章：对象合并

## 关于对象合并

使用 **Data Protector** 对象合并功能可以将备份对象的还原链合并为此对象的全新合并版本。使用此功能后，即不再需要运行完整备份。而是可以无限地运行增量备份，并根据需要合并还原链。

对象合并会话期间，**Data Protector** 从源介质读取备份数据，合并数据，然后合并后的版本写入目标介质。对象合并会话可以得到指定对象版本的合成完整备份。

## 对象合并的类型

可以用交互方式启动对象合并会话，也可以指定自动启动会话。**Data Protector** 可提供两种自动对象合并：备份后对象合并和计划的对象合并。

### 备份后对象合并

自动对象合并规范中指定的备份会话完成后进行的对象合并即为备份后对象合并。它合并根据在该特定备份会话中备份的自动对象合并规范所选的对象。

### 计划的对象合并

计划的对象合并发生在用户定义的某个时间。可以在一个计划的对象合并会话中合并不同备份会话期间备份的对象。

## 如何合并对象

首先，创建对象合并规范。在规范中，选择要合并的对象版本、要使用的介质和设备以及会话选项。

## 设备的选择

需要分别使用单独的设备读取完整备份、读取增量备份以及写入合成完整备份。目标设备的块大小可以大于源设备。但是，为避免影响性能，建议这些设备的块大小相同，并且连接到相同系统。

会话中不能使用该会话开始时没有的设备。如果发生介质错误，则该会话中将避免使用出错的设备。

## 对象合并选项

可以在对象合并规范中启用源对象过滤并指定数据保护、编目保护和日志记录级别。其中大部分选项的等效选项也用于备份。

## 介质集的选择

如果将参与合并的对象版本有副本位于不同的介质集上，则这些介质集中的任何一个都可以用作源。默认情况下，**Data Protector** 自动选择最合适的介质集。通过指定介质位置的优先级可以影响介质集的选择。

介质选择的总体过程与还原相同。以交互方式合并对象时，可以手动选择要使用的介质集。配置自动对象合并时无法选择介质，因为通常稍后执行对象的备份。

## 合并对象的所有权

合并备份对象的所有者为原始备份对象的所有者，而非调用对象合并会话的 **Data Protector** 用户。

## 标准对象合并任务

下面是对象合并功能的先决条件和限制：

### 先决条件

- 在启用增强型增量备份选项的情况下执行将合并的所有备份。
- 将合并的所有增量备份都位于一个文件库或 **B2D** 设备中。
- 还原链完成，表示组成它的所有对象版本的状态都为 **Completed** 或 **Completed/Errors**，并且持有这些对象版本的所有介质都可用。
- 配置了必要的备份设备，并已准备好介质。
- 需要在将参与对象合并会话的每个系统上安装介质代理。
- 需要有适当的用户权限用于启动对象合并会话。对于备份也适用相同的用户权限。
- 要执行虚拟完整备份，所有备份(完整、增量和虚拟完整)都必须位于使用分布式文件介质格式的一个文件库中。

### 限制

- 目标设备的块大小必须等于或大于源设备。
- 同一介质不能在同一对象合并会话中同时用作源介质和目标介质。
- 读取源介质时，该介质不可用于还原。
- 使用 **AES 256** 位加密备份的对象合并不能使用。

除智能缓存外，所有 **B2D** 设备均支持对象合并。

#### 注意：

每当更改备份规范中软件压缩或编码选项的设置时，都必须执行一次完整备份，作为后续对象合并的基础。

## 以交互方式合并对象

根据需要，可以选择用于从“对象”或“会话”起始点开始的交互式合并的对象。不能保存交互式对象合并规范，只能启动对象合并会话。

### 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并**，然后展开**交互**。
3. 单击**对象或会话**打开向导。
  - 单击**对象**以列出对象。
  - 单击**会话**以列出从中向介质写入对象的会话。
4. 选择希望合并的对象的时间点。无法选择完整备份，因为就此类备份本身而言无法合并。

选择时间点将选择整个还原链。如果对于同一时间点存在若干还原链，则选择所有链，但实际仅使用一个链。以蓝色标记您的选择，以黑色标记组成还原链的其他增量，以灰色(阴影)标记相应的完整备份。蓝色复选标记指示将进行合并的时间点。

可以为合并选择多个时间点，并且还原链可以重叠。如果选择的时间点已有黑色复选标记，则该复选标记将变为蓝色。

要清除所选的还原链，请单击蓝色复选标记。此时将清除整个还原链，除非某些对象版本是另一个还原链的一部分，这种情况下这些对象版本仍保持选中状态，并有黑色复选标记。

单击**下一步**。
5. 指定将读取增量备份和完整备份的设备。

通过选择特定文件库或 B2D 设备(智能缓存除外)作为读取进行增量备份的设备，限制向这些库或设备进行对象合并。将仅合并位于指定设备中的对象。

默认情况下，读取完整备份的设备是在所选备份规范中用于备份的那些设备。如果需要，可以在此处更改这些设备。单击**下一步**。
6. 选择对象合并操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击**下一步**。
7. 根据需要指定选项。单击**下一步**。
8. 此时将显示包含所选对象的介质的列表。

可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

单击**下一步**。
9. 查看将参与操作的对象版本。如果使用备用还原链，可能发生实际并不使用列出的所有对象版本的情况。单击**下一步**。
10. 查看所选时间点的摘要。要更改特定时间点的选项，请在列表中选择该时间点，然后单击**属性**。
11. 单击**完成**退出向导。

## 配置备份后对象合并

自动对象合并规范中备份规范的名称所指定的备份会话完成后进行的对象合并即为备份后对象合并。它合并在该特定备份会话中备份的符合指定标准的对象。

### 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并**，然后展开**自动**。
3. 右键单击**备份后**，然后单击**添加**以打开向导。
4. 选择包含要合并的对象的备份规范。单击**下一步**。
5. 指定用于对象合并操作的对象筛选器。单击**下一步**。
6. 指定将读取增量备份和完整备份的设备。

通过选择特定文件库或 B2D 设备(智能缓存除外)作为读取进行增量备份的设备，限制向这些库或设备进行对象合并。将仅合并位于指定设备中的对象。

默认情况下，读取完整备份的设备是在所选备份规范中用于备份的那些设备。如果需要，可以在此处更改这些设备。单击**下一步**。

7. 选择对象合并操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击**下一步**。
8. 根据需要指定选项。单击**下一步**。
9. 单击**另存为...**，输入规范名称，然后单击**确定**以保存备份后对象合并规范。

## 计划对象合并

计划对象合并发生在用户定义的某个时间。它合并符合指定标准的对象。可以在一个预定对象合并会话中合并不同备份会话期间备份的对象。

当有许多可选择的还原链时，Data Protector 合并包含时间点最新的对象版本的那个还原链。例如，备份会话：完整、增量 1、增量 2、增量 2、增量 2 生成三个恢复链，但 Data Protector 仅合并一个由完整、增量 1、和最新 增量 2 组成的链。

### 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并**，然后展开**自动**。
3. 右键单击**预定**，然后单击**添加**以打开向导。
4. 选择包含要合并的对象的备份规范。单击**下一步 (Next)**。
5. 为对象合并操作指定时间筛选器。将仅合并指定时间范围内备份的对象。单击**下一步 (Next)**。
6. 指定用于对象合并操作的对象筛选器。单击**下一步 (Next)**。

7. 指定将读取增量备份和完整备份的设备。

通过选择特定文件库或 B2D 设备(智能缓存除外)作为读取进行增量备份的设备，限制向这些库或设备进行对象合并。将仅合并位于指定设备中的对象。

默认情况下，读取完整备份的设备是在所选备份规范中用于备份的那些设备。如果需要，可以在此处更改这些设备。单击**下一步 (Next)**。

8. 选择对象合并操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击**下一步 (Next)**。
9. 根据需要指定选项。单击**下一步 (Next)**。
10. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存计划对象合并规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。

有关如何使用调度程序在 Data Protector 中创建和编辑计划，请参见 [计划程序 \(第 92 页\)](#)。

**重要：**

在 Data Protector 10.00 中，基本调度程序和高级调度程序均已废弃，并且替换为基于 Web 的新调度程序。可以配置无人看管备份，具体方法是排定备份会话使其在特定的时间执行。

在升级 Data Protector 的过程中，所有现有的 Data Protector 计划都会自动迁移到新的调度程序。

## 复制对象合并规范

可以复制已配置和保存的对象合并规范。

### 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**合并、自动**，然后展开**备份后**。此时将显示所保存的全部备份规范。
3. 在结果区域中，右键单击要复制的对象合并规范，然后单击**复制为**。此时将显示“复制为”对话框。
4. 在“名称”文本框中，键入所复制的对象合并规范的名称。
5. 单击**确定**。

所复制的对象合并规范显示在范围窗格的“对象操作”上下文中以及结果区域中的新名称下。

# 第 12 章：复制

## 关于复制备份数据

复制已备份数据有一些好处。可以复制数据以提高其安全性和可用性，或为了操作原因而这样做。

Data Protector 可提供以下方法来复制已备份数据：对象副本、对象镜像、介质复制和备份到磁盘 (B2D) 设备上的复制。

	对象复制	复制	对象镜像	介质复制
复制什么	一个或若干备份会话、对象复制会话或对象合并会话中对象版本的任意组合	来自备份会话、对象复制会话或对象合并会话的对象集	备份会话中的一组对象	整个介质
复制的时间	完成备份后的任何时间	完成备份后的任何时间	备份期间	完成备份后的任何时间
源和目标介质的介质类型	可以不同	仅能将数据复制到相同类型的 B2D 设备	可以不同	必须相同
源和目标介质的尺寸大小	可以不同	目标设备必须具备足够的空间用于删除了重复数据后的数据	可以不同	必须相同
是否可追加目标介质	是	否	是	否 <sup>1</sup>
操作的结果	包含所选对象版本的介质	存储在目标 B2D 设备上的完全相同的副本	包含所选对象版本的介质	与源介质相同的介质

<sup>1</sup> 只能使用未格式化的介质、空介质，或保护到期的介质作为目标介质。完成该操作后，源介质和目标介质都变为不可附加。

还可以组合使用复制方法。例如，可以创建对象镜像结果数据的对象副本或介质副本。或者，可以复制包含对象副本的整个介质。



## 关于对象复制

### 什么是对象复制？

**Data Protector** 对象复制功能使您能将所选对象版本复制到特定介质集。可以从一个或多个备份会话、对象复制会话或对象合并会话中选择对象版本。在对象复制会话中，**Data Protector** 会从源介质读取备份的数据，传输数据，并将其写入目标介质。

对象复制会话可以得到包含指定对象版本副本的介质集。

以下是对象副本功能的特征：

- 会话开始  
可以用交互形式启动或自动启动对象副本会话。
- 介质的选择  
作为源介质，可以使用包含备份的原始介质集、包含对象副本的介质集或者作为介质副本的介质集。  
但是，启动对象复制会话之后即无法选择介质集。如有装载请求，需要提供由 **Data Protector** 请求的特定介质，或其完全相同的副本(使用介质复制功能创建)。
- 介质类型  
可以将对象复制到不同类型的介质。此外，目标设备的块大小可以等于或大于源设备的块大小。
- 介质策略  
可以向已包含备份或对象副本的介质追加数据。
- 保护策略  
可以对源对象和对象副本单独设置保护周期。

可以用交互形式启动对象复制会话，或指定自动启动会话。

### 自动对象复制

在自动对象副本规范中，可以指定一个或多个标准用于选择将复制的对象版本：

- 备份规范 - 仅复制使用特定备份规范备份的对象版本。
- 对象副本规范 - 仅复制使用特定对象副本规范复制的对象版本。
- 对象合并规范 - 仅复制使用特定对象合并规范合并的对象版本。
- 数据保护 - 仅复制受保护的版本。
- 现有副本数 - 仅复制不超过指定成功复制数的对象版本。
- 库 - 仅复制位于指定库中介质上的对象版本。
- 时间范围(仅在计划的对象副本规范中) - 仅复制指定时间段内备份的对象版本。

**Data Protector** 可提供两种自动对象复制：备份后对象复制和计划的对象复制。

## 备份后对象复制

备份后对象复制以及(备份后对象复制的子集)复制后和合并后对象复制，发生在自动对象副本规范中指定的会话完成之后。它们复制根据该特定会话中写入的自动对象复制规范选择的对象。

## 计划的对象复制

计划的对象复制发生在用户定义的某个时间。在一个计划的对象副本会话中可以复制不同会话中的对象。

## 如何复制对象

首先，创建对象复制规范。在规范中，选择要复制的对象、要使用的介质和设备、会话选项以及当同一对象位于多个介质集上时影响 **Data Protector** 如何选择介质集的介质位置优先级。

## 设备的选择

您需要将要使用的设备与源介质和目标介质分开。目标设备的块大小可以大于源设备。但是，为避免影响性能，建议目标设备和源设备具有相同的块大小，且连接到同一系统或 **SAN** 环境。

默认情况下对于对象复制要进行负载均衡。**Data Protector** 通过使用尽可能多的设备，最优地利用可用的设备。

如果不指定要用于对象副本规范中的源设备，则 **Data Protector** 将使用默认设备。默认情况下，将使用用于写入对象的设备作为源设备。如果需要，可以更改源设备。如果不按对象选择目标设备，则 **Data Protector** 将自动从您在对象复制规范中选择的那些设备中选择最合适的设备。

会话开始的时候锁定设备。那时不可用的设备就不能用于会话中，因为会话开始后即无法锁定设备。如果发生介质错误，则该复制会话中将避免使用出错的设备。

## 对象副本选项

可以在对象复制规范中启用源对象过滤并为对象副本指定数据保护、编目保护和日志记录级别。其中大部分选项的等效选项也用于备份。

根据策略，备份的对象及其副本可以指定相同或不同的选项值。例如，可以对一个备份对象指定**无日志**值以提高备份性能，然后在后续的对象复制会话中对相同的对象指定**全部记录**值。

要创建与所备份对象完全相同的副本，请为对象副本指定相同的日志记录级别。请考虑这一点：日志记录级别高于“无日志”的每次对象复制都对 **IDB** 大小有影响。

## 选择从中进行复制的介质集

如果要复制的对象版本存在于多个介质集(用 **Data Protector** 数据复制方法之一创建的)上，则任何介质集都可用作复制源。默认情况下，**Data Protector** 会自动选择要使用的介质集。通过指定介质位置的优先级可以影响介质集的选择。

介质选择的总体过程与还原相同。以交互方式复制对象时，可以在起始点为“对象”或“会话”时手动选择要从中进行复制的介质集。配置自动对象复制时无法选择介质，因为通常稍后执行对象的备份。

## 对象副本完成状态

### 复制对象

如果 **IDB** 中记录了状态为 **Completed** 或 **Completed/Errors** 的对象所在的所有介质，则可以复制这些对象。如果复制操作成功，则所复制对象的状态与相应所备份对象的状态相同。

如果已中止对象复制会话，或如果该会话因其他原因失败，则此类会话所得的对象副本处于 **Failed** 状态。无法再次复制状态为 **Failed** 的对象副本；其数据和编目保护设置为 **None**。

### 源对象

如果对象副本会话失败，则所复制的源对象保持不变。

如果对象复制会话完成但有错，则成功复制的源对象将其数据和编目保护设置为源对象选项中指定的值。

如果中止对象复制会话，则 **all** 源对象的数据和编目保护都保持不变。在这种情况下，如果要更改任何所复制对象的保护，则必须在 **IDB** 中手动进行。

## 对象副本所有权

复制备份对象的所有者为原始备份对象的所有者，而非调用对象复制会话的 **Data Protector** 用户。

## 标准对象复制任务

下方是对象复制功能的先决条件和限制：

### 先决条件

- 需要在将参与对象复制会话的每个系统上安装介质代理。
- 需要至少在 **Data Protector** 单元中配置两个备份设备。
- 需要为对象复制会话准备好介质。
- 需要有适当的用户权限用于执行对象复制会话。

## 限制

- 无法复制使用 ZDB 到磁盘或 NDMP 备份功能备份的对象。
- 无法在一个对象复制会话中创建一个对象版本的多个副本。
- 目标设备的块大小必须等于或大于源设备。
- 同一介质不能在同一对象复制会话中同时用作源介质和目标介质。
- 对象复制期间，用作源的介质不可用于还原。
- 无法取消 SAP MaxDB、DB2 UDB 或 SQL 集成对象的多路复用。
- 无法复制在向导最后一页中以交互方式运行的会话过程中备份、复制或合并的对象。
- 无法从同一个对象复制规范中同时启动两个或更多个对象复制会话。

### 重要：

请考虑以下几点：

- Data Protector SAP MaxDB、DB2 UDB 和 Microsoft SQL Server 集成具有相互依赖的数据流。因此，对象复制操作必须在介质上保留对象的布局才能进行还原。要确保这一点，请选择这些集成中备份 ID 相同的所有对象进行复制。否则，无法从此副本进行还原。
- 复制 SAP MaxDB、DB2 UDB 或 Microsoft SQL Server 集成对象所需的最少设备数与用于备份的设备数相等。用于备份和复制这些对象的设备的并发必须相同。
- 如果从 ZDB 到磁盘 + 磁带会话复制对象时选择了成功复制之后更改数据和编目保护选项，则请注意，在指定时期之后可以覆盖源对象。覆盖介质之后，将不能再使用 GUI 从此备份进行即时恢复。
- 如果中止对象复制会话，则所有源对象的数据和编目保护都保持不变。在这种情况下，如果要更改任何所复制对象的保护，则必须在 IDB 中手动进行。

## 以交互方式复制对象

备份对象后，可以将其复制到新的介质集中。

根据需要，可以选择用于从“介质”、“对象”或“会话”起始点开始的交互式复制的对象。不能保存交互式对象副本规范，只能启动对象复制会话。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**介质**、**对象**或**会话**以打开向导。
  - 单击**介质**可列出介质池和介质。
  - 单击**对象**以列出备份数据的类型，如“文件系统”、“数据库”等等。
  - 单击**会话**以列出从中向介质写入对象的会话。
4. 选择要复制的对象。

如果在之前的步骤中选择了会话，则可以右键单击集成对象并单击**选择备份集**，以选择具有相同备份 ID 的所有集成对象。

**注意：**

自 Data Protector 10.00 起，对于 Vmware 备份，将虚拟机磁盘视为并行运行的对象。虚拟机的磁盘对象会列在**介质**列表中，但它们处于禁用状态，表明虚拟机磁盘已备份到介质。将在虚拟机对象上执行复制或验证操作，并将其所有关联的磁盘对象视为内部对象。

自 Data Protector 10.00 起，对于 Vmware 集成，只有在**介质**列表中选择虚拟机对象后，才会启动**下一步**选项。

单击**下一步**。

5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。选择原始设备，然后单击**更改**。新设备的名称出现在“设备状态”下。新设备将仅用于此会话。

有关设备的详细信息，请右键单击该设备，并单击**信息**。

指定对象复制期间所选设备不可用(例如如果被禁用或已在使用中)时 Data Protector 应做些什么。选择自动设备选择或原始设备选择。

单击**下一步**。

6. 选择用于对象复制操作的目标设备。

可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 Data Protector 将从此列表中选择最合适的设备。

单击**下一步**。

7. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击**下一步**。

或者，要启用两个 B2D 设备之间的复制而不启用复制，请选择使用复制。选择“使用复制”后，“复制到外部单元”即启用。

8. 此时将显示包含所选对象的介质的列表。

如果起始点是“对象”或“会话”，则还会列出介质位置优先级。可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

单击**下一步**。

9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

可以指定源对象选项、目标对象选项和目标设备。如果使用了“对象”或“会话”起始点，则当存在多个副本时，可以手动选择将使用对象版本的哪个副本。

10. 单击**完成**启动复制会话。

## 配置备份后对象复制

备份后对象复制在自动对象复制规范中的备份、对象复制或对象合并规范的名称所指定的备份会话、对象复制会话或对象合并会话完成之后发生。它复制该特定会话中符合指定标准的对象。

如果备份会话失败，则备份后对象复制会话不会启动。如果备份会话已中止，但包含完成的对象，则默认情况下备份后对象复制会话将复制完成的对象。要禁用已中止会话的复制，请将全局选项 CopyStartPostBackupOnAbortedSession 设置为 0。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**自动**。
3. 右键单击**备份后**，然后单击**添加**以打开向导。
4. 选择包含要复制的对象的备份、对象副本或对象合并规范。单击**下一步 (Next)**。
5. 指定用于对象复制操作的对象筛选器。将仅复制符合指定标准的对象。单击**下一步 (Next)**。
6. 指定用于对象复制操作的带库筛选器。将仅复制位于指定库中介质上的对象。单击**下一步 (Next)**。
7. 在所选备份规范中用于备份的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击**下一步 (Next)**。
8. 选择用于对象复制操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击**下一步 (Next)**。
9. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击**下一步 (Next)**。  
或者，要启用两个 B2D 设备之间的复制而不启用复制，请选择使用复制。
10. 单击**另存为...**，输入规范名称，然后单击**确定**以保存备份后对象复制规范。

## 安排对象复制

计划对象复制发生在用户定义的某个时间。可在一个排定对象复制会话中复制来自不同备份会话、对象复制会话或对象合并会话的对象。

### 提示：

也可以使用基于 Web 的调度程序的高级设置来计划对象复制会话。要访问调度程序，请在上下文列表中单击**主页**，然后单击左侧窗格中的**调度程序**。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**自动**。
3. 右键单击**预定**，然后单击**添加**以打开向导。
4. 选择包含要复制的对象的备份、对象副本或对象合并规范。  
还可以按备份组查看备份规范。这样，如果向某个备份组添加备份规范或从该组删除备份规范，则对象复制功能自动确认更改，而您无须手动修改对象副本规范。  
请注意，如果从组视图更改为任何其他视图，则显示一条警告消息，提醒更改视图将删除当前所选的全部内容。如果继续，将清除以前所选的全部内容。  
单击**下一步 (Next)**。
5. 指定用于对象复制操作的对象筛选器。将仅复制符合指定标准的对象。单击**下一步 (Next)**。
6. 指定用于对象复制操作的带库筛选器。将仅复制位于指定库中介质上的对象。单击**下一步 (Next)**。

7. 在所选备份规范中用于备份的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击**下一步 (Next)**。
8. 选择用于对象复制操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击**下一步 (Next)**。
9. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击**下一步 (Next)**。  
或者，要启用两个 B2D 设备之间的复制而不启用复制，请选择使用复制。
10. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存计划对象复制规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。  
有关如何使用调度程序在 Data Protector 中创建和编辑计划，请参见 [计划程序 \(第 92 页\)](#)。

## 重新启动失败的对象复制会话

由于网络连接问题或系统不可用，对象复制会话期间可能会发生某些对象失败的情况。解决了妨碍的问题后，可以重新启动出现问题的会话。此操作只会重新启动失败的对象。

### 先决条件

- 您必须位于 Data Protector Admin 用户组中，或者获得了 Data Protector 监视用户权限。

### 限制

- 无法重新启动以交互方式运行(意味着它们是基于未保存的对象副本规范)的失败会话。
- 无法同时重新启动多个会话。

#### 重要：

重新启动失败的对象复制会话之前，请勿更改对象复制规范。否则将无法重新启动所有对象。

### 步骤

1. 如果您使用的是普通 Cell Manager，在上下文列表中单击**内部数据库**。  
如果您使用的是管理器的管理器，在“上下文列表”中选择**客户机**，然后展开**企业客户机**。选择会话出现问题的 Cell Manager。从“工具”菜单中选择**数据库管理**，从而打开一个新 Data Protector GUI 窗口，并显示“内部数据库”上下文。
2. 在范围窗格中，展开**内部数据库**，然后单击**会话**。  
此时将在结果区域中显示会话的列表。每个会话的状态显示在“状态”列中。
3. 右键单击失败、中止或完成但发生过失败或出现错误的会话，然后选择**重新启动失败的对象**以复制失败的对象。
4. 单击**是**确认。

## 复制对象复制规范

可以复制已配置和保存的对象复制规范。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**、**自动**和**备份后**。此时将显示所保存的全部对象复制规范。
3. 在结果区域中，右键单击要复制的对象复制规范，然后单击**复制为**。此时将显示“复制为”对话框。
4. 在“名称”文本框中，键入所复制的对象复制副本的名称。
5. 单击**确定**。

所复制的对象副本规范显示在范围窗格的“对象操作”上下文中以及结果区域中的新名称下。

## 高级对象复制任务

为了以下多种用途，创建已备份数据的其他副本：

- 保管  
您可以制作已备份、已复制或已合并对象的副本，并将其保存在多个位置。
- 释放介质  
要只保存介质上受保护对象的版本，您可以复制此类对象版本，然后释放介质以便覆盖。
- 取消复用介质  
您可以复制对象以消除数据的交叉存取。
- 合并还原链  
您可以复制还原到一个介质集所需的所有对象版本。
- 迁移到其他介质类型  
您可以将备份复制到不同类型的介质。
- 支持高级备份概念  
您可以使用磁盘分段等备份概念。

## 释放介质

介质可以包含保护期各异的备份对象。可能会发生受保护对象仅占用少量介质空间的情况。但是，直到所有对象的保护都到期后，才能重用此类介质。

要使介质的使用合理化，可以使用对象复制功能释放仅包含某些受保护对象的介质。将受保护的复制对象复制到新的介质集中，并且可以重用该介质。也可以从失败的对象释放介质。在对象复制会话中不复制这些对象。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。



3. 单击**介质**打开向导。
4. 在“对象”页中，选择选项仅启用受保护对象的选择。展开介质池，然后选择要释放的介质。单击**下一步 (Next)**。
5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击**下一步 (Next)**。
6. 选择用于对象复制操作的目标设备。  
可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 **Data Protector** 将从此列表中选择最合适的设备。  
单击**下一步 (Next)**。
7. 在“选项”页中的“源对象”选项下，选择成功复制之后更改数据和编目保护，以便在复制这些对象之后删除源对象的保护。选择在成功完成复制之后回收失败的源对象的数据和编目保护，以删除失败的源对象的保护(不会复制这些对象)。根据需要指定其他选项。单击**下一步 (Next)**。
8. 此时将显示包含所选对象的介质的列表。单击**下一步 (Next)**。
9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。可以指定源对象选项、目标对象选项和目标设备。
10. 单击**完成**启动复制会话。

## 取消介质的多路复用

多路复用的介质包含多个对象的交错数据。此类介质可能由于多个并行设备的备份会话而产生。复用介质会削弱备份的隐私安全，而且需要更多时间才能还原。

使用对象复制功能，可以取消介质的多路复用。来自多路复用介质的对象将复制到若干介质。

## 限制

**Data Protector** 仅读取源介质一次。要能取消介质上所有对象的多路复用，操作所需的最小目标设备数与用于写入对象的设备并发相同。如果可用设备较少，则目标介质上仍对某些对象进行多路复用。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。
3. 单击**会话**打开向导。
4. 展开所需的会话，然后选择要复制的对象。单击**下一步**。
5. 如果不希望取消多路复用操作占用为定期备份而配置的设备，并且如果要在取消多路复用操作期间仅使用一个设备读取数据，则执行此步骤。  
将源设备映射到单个设备。

### 重要：

如果使用一个独立文件设备作为源设备，则跳过此步骤。如果使用文件介质库设备或文件库设备作为源设备，请确保将源设备映射到相同文件介质库中或相

同文件库中的设备。

右键单击每个设备，然后单击**更改设备**。选择新设备，然后单击**确定**。

6. 单击**下一步**。

7. 选择用于对象复制操作的目标设备。所需的设备数取决于写入对象时使用的设备并发。

右键单击每个所选的驱动器，然后单击**属性**。将**并发**选项设置为 1。单击**确定**。

可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 **Data Protector** 将从此列表中选择最合适的设备。

单击**下一步**。

8. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击**下一步**。

9. 此时将显示包含所选对象的介质的列表。

可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

单击**下一步**。

10. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

可以指定源对象选项、目标对象选项和目标设备。如果存在多个副本，则还可以手动选择将使用对象版本的哪个副本。

11. 单击**完成**启动复制会话。

## 合并还原链

使用对象复制功能，可以将对象版本的还原链复制到新的介质集。从这种介质集可以更快更方便地还原，因为不需要加载多个介质和寻找所需的对象版本。

### 注意：

**Data Protector** 还提供一个更强大的功能，称为对象合并。使用对象复制可以将还原链的所有备份复制为一个序列的同时，对象合并将备份合并为一个新的对象版本，合成完整备份。

## 限制

对于集成对象无法选择还原链。

## 步骤

1. 在上下文列表中，单击**对象操作**。

2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。

3. 单击**对象**打开向导。

4. 在“对象”页中，展开某种数据类型，然后展开客户机及其逻辑磁盘或装载点以显示对象版本。右键单击要复制的对象，然后单击**选择还原链**。单击**下一步**。

5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击**下一步**。

6. 选择用于对象复制操作的目标设备。

可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 **Data Protector** 将从此列表中选择最合适的设备。

单击**下一步**。

7. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击**下一步**。

8. 此时将显示包含所选对象的介质的列表。

可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

单击**下一步**。

9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

可以指定源对象选项、目标对象选项和目标设备。如果存在多个副本，则还可以手动选择将使用对象版本的哪个副本。

10. 单击**完成**启动复制会话。

## 迁移到其他介质类型

可以使用对象复制功能将备份数据迁移至块大小相同或更大的另一种介质类型。

### 步骤

1. 在上下文列表中，单击**对象操作**。

2. 在“范围窗格”中，依次展开**复制**、**对象复制**和**交互**。

3. 单击**介质**打开向导。

4. 选择要复制的对象，然后单击**下一步**。

5. 用于写入所选对象的设备默认情况下在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击**下一步**。

6. 选择用于对象复制操作的目标设备。

可以从此处指定的设备列表中指定“摘要”页中每个对象的设备。如果未指定每个对象的设备，则 **Data Protector** 将从此列表中选择最合适的设备。

单击**下一步**。

7. 根据需要指定源对象选项、目标对象选项和目标介质选项。单击**下一步**。

8. 此时将显示包含所选对象的介质的列表。单击**下一步**。

9. 查看所选对象的摘要。要更改特定对象的选项，请在列表中选择该对象，然后单击**属性**。

可以指定源对象选项、目标对象选项和目标设备。

10. 单击**完成**启动复制会话。

## 关于磁盘暂存

### 什么是磁盘分段？

磁盘分段的概念基于在若干阶段中备份数据。备份阶段由两部分组成：将数据备份到一种类型的介质，然后将数据复制到另一种类型的介质。通常可能以如下方式使用该功能

1. 数据备份到高性能和高可访问性、但容量有限的介质(例如系统磁盘)。此类备份通常在可能最需要快速还原的那段时间内保持可访问的状态。
2. 一段时间之后，使用对象复制功能将数据移至较低性能和较低可访问性、但容量很大的介质进行存储。

可以使用专为此用途配置的计划对象副本规范以此方式执行磁盘分段。

如下方法有可能作为一种替代方法：

1. 创建一个备份规范，将数据备份到高性能介质，该介质中将保护设置为需要还原功能的整个时期。
2. 创建自动备份后复制规范，将备份数据复制到较低性能的介质，并将原始备份的保留期重置为需要快速还原功能的关键时期。默认情况下，在原始备份规范中指定的保护期内保留辅助副本。

使用此方法后，关键时期内进行这两次复制都更加安全。

### 为什么要实施磁盘分段

使用磁盘分段概念会带来以下优点：

- 可提高备份和还原的性能。
- 可减少存储备份数据的成本。
- 可提高对于还原的数据可用性和可访问性。

### 磁盘分段和重复进行的小型备份

磁盘分段也消除了将大量小对象频繁备份到磁带的必要。由于要频繁装载和卸载介质，此类备份很不方便。使用磁盘分段可以降低备份时间和避免介质质量下降。

## 对象操作会话故障排除

### 对象副本问题

#### 复制的对象比预期的少

问题
使用备份后或计划的对象副本，匹配所选过滤器的对象数比实际复制的对象数多。 将显示以下消息：

Too many objects match specified filters.
<b>操作</b>
<ul style="list-style-type: none"><li>• 减少对象版本选择的条件。</li><li>• 通过设置全局选项 <code>CopyAutomatedMaxObjects</code>，增加在会话中复制的最大对象数量。</li></ul>

## 未复制所选库中的全部对象

<b>问题</b>
使用备份后或计划的对象副本，不复制在所选库中的介质上驻留的某些对象。如果对象在所选库中没有完整的介质集，则会发生此情况。
<b>操作</b>
将缺少的介质插入所选库中，或者选择有这些对象的完整介质集的库。

## 发出了装载其他介质的请求

<b>问题</b>
在交互式对象复制会话中，从介质开始点选择了特定介质。但发出了装载其他介质的请求。如果在介质上驻留的对象跨另一个介质，则会发生此情况。
<b>操作</b>
将所需介质插入设备中，并确认装载请求。

## 当创建对象副本时，保护结束时间会延长

<b>问题</b>
<p>当创建对象副本时，不从原始对象继承保护结束时间。而是复制保护时间长度，但将开始时间设置为对象副本创建时间而不是对象创建时间。这导致保护时间比原始保护时间长。原始备份和对象复制会话之间经过的时间越长，保护结束时间之间的差别就越大。</p> <p>例如，如果对象在 9 月 5 日创建，保护设置为 14 天，则保护将在 9 月 19 日过期。如果在 9 月 10 日启动对象复制会话，则对象副本保护将在 9 月 24 日过期。</p> <p>在某些情况下，不希望出现这种行为，必须保留保护结束时间。</p>
<b>操作</b>
将全局选项 <code>CopyDataProtectionEndtimeEqualToBackup</code> 设置为 1，可确保对象副本保护结束时间等于备份对象保护结束时间。默认情况下，该选项设置为 0。增加允许文件的最大数。

## 复制包含多个对象的会话时会话停止响应

问题
<p>将会话复制到另一个设备上时，会话停止响应。会话输出提供以下信息：</p> <pre>[Normal] From: BMA@company.com "d2d1_1_gw1 [GW 26177:1:15198446278003495809]" Time: 3/21/2013 9:13:06 AM  COMPLETED Media Agent "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"</pre> <p>已知此问题会在包含 HP-UX 介质代理的双 IP 堆栈网络配置中发生。</p>
操作
<p>配置 IP 堆栈网络时，在介质代理客户机上的 <code>/etc/hosts</code> 文件中为 IPv6 localhost 地址添加一个单独的条目。</p> <p>例如，在 <code>hosts</code> 文件中有如下条目：</p> <pre>::1 localhost loopback</pre> <p>要解决此问题，请为 IPv6 地址添加以下行：</p> <pre>::1 ipv6-localhost ipv6-loopback</pre>

## 数据域提升设备上的复制会话无法在重试期间响应中止操作

问题
<p>将会话从一个数据域提升备份设备复制到另一个备份设备时或者当设备的可用流不足时，复制会话将无法在重试期间响应中止操作。</p>
操作
<p>当 <code>omnirc DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT</code> 设置为不受支持的 0 时将出现问题。</p> <p>此变量定义当数据域提升设备没有足够的流时，复制会话在开始另一重试操作前要等待的时间。如果间隔太长或设置为 0，则会话无法响应中止操作。</p> <p><code>DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT</code> 的默认值为 60 秒。</p> <p>有关 <code>DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT</code> 的完整说明，请参见 <code>omnirc</code> 文件。</p>

## 对象整合问题

### 许多时间点的对象整合打开太多的文件

问题
<p>如果启动具有许多时间点的对象合并操作，则 <b>Data Protector</b> 要读取所需的全部介质才能完成操作。这将同时打开所有文件。当 <b>Data Protector</b> 打开的文件超过操作系统允许的</p>

文件数时，会显示与以下类似的消息：

```
|Major| From: RMA@computer.company.com "AFL1_ConsolidateConc2_bs128" Time: time  
/omni/temp/Cons_Media/AFL1/
```

```
0a1109ab54417fab351d15500c6.fd
```

```
Cannot open device ([24] Too many open files)
```

#### 操作

增加允许文件的最大数。

##### HP-UX 系统：

1. 使用系统管理管理器 (SAM) 设置打开文件的最大数：
  - a. 选择**核心配置 > 可配置参数**，然后选择**操作 > 修改可配置参数**。
  - b. 在**公式/值**字段中输入新的 **maxfiles\_lim** 和 **maxfiles** 值。
2. 在应用新值之后，重新启动计算机。

##### Solaris 系统：

1. 通过编辑 `/etc/system` 文件设置打开文件的最大数量。添加以下行：

```
set rlim_fd_cur=value  
set rlim_fd_max=value
```
2. 在应用新值之后，重新启动计算机。

## 第二次尝试对象合并至 **B2D** 设备失败

#### 问题

如果第一次对象合并后执行增量备份，并随后执行第二次对象合并，则操作将会失败。

#### 操作

要确保第二次合并成功，请在第一次对象合并后执行完整备份。然后再执行增量备份，稍后可能会合并。

## 关于复制

通过 **Data Protector** 复制功能，可以在两个具有复制功能的备份到磁盘 (**B2D**) 设备之间复制对象，而无需通过介质代理传输数据。可以选择备份会话、对象复制会话或对象合并会话。在复制会话期间，**Data Protector** 会从正在复制的会话中读取对象，然后启动从源 **B2D** 设备到目标设备的复制。

复制会话的结果为来自指定会话的所有对象的副本。

以下内容定义复制功能：

- 会话的启动  
可以用交互形式启动或自动启动复制会话。

- 目标设备的选择  
可以筛选具有复制功能的设备并选择适当的设备。
- 保护策略  
可以对源对象和对象副本单独设置保护周期。  
可以用交互方式启动复制会话，也可以指定自动启动会话。

## 自动复制

在自动复制规范中，可以指定一个或多个标准用于选择将复制的对象版本：

- 备份规范 - 仅复制使用特定备份规范备份的对象版本。
- 对象副本规范 - 仅复制使用特定对象副本规范复制的对象版本。
- 对象合并规范 - 仅复制使用特定对象合并规范合并的对象版本。
- 数据保护 - 仅复制受保护的版本。
- 现有副本数 - 仅复制不超过指定成功复制数的对象版本。
- 库 - 仅复制位于指定库中介质上的对象版本。
- 时间范围(仅在预定对象副本规范中) - 仅复制指定时间段内备份的对象版本。

**Data Protector** 可提供两种自动复制：备份后复制和排定复制。

## 备份后复制

备份后复制以及(备份后复制的子集)复制后和合并后复制，发生在自动对象副本规范中指定的会话完成之后。它们复制根据写入该特定会话的自动复制规范选择的对象。

## 安排的复制

安排的复制在用户定义的时间发生。可在单个计划的复制会话中复制来自不同会话的对象。

## 限制

- 仅可为复制选择备份、对象副本、对象合并或对象复制会话。不支持选择单个对象。
- 不支持源或目标设备上不同的块大小。
- 配置交互会话时，一次仅可选择一个会话。

## 注意事项

- 由于复制基于会话，所以可能会覆盖单个对象的设置。例如，如果会话中已包含一个对象的多个副本，**Data Protector** 将忽略选项 **仅包括副本数小于指定值的对象**，并复制会话中的所有对象，其中包括此对象，即使这样会导致对象的副本数超出此选项所允许的数量。
- 默认情况下，**Data Protector** 将选择原始对象版本(如果找到同一对象的多个副本)作为源设备。在某些情况下，原始版本可能会因为其属于不同的介质类型而无法复制。  
通过选择能够复制的库或特定库，选择正确的源设备。



## 如何启用复制

可以在创建对象副本规范时启用从一个 B2D 设备到另一个 B2D 设备的复制：

1. 请确保源和目标设备能够复制。使用**能够复制**过滤器过滤设备，或明确选择特定的 B2D 设备。
2. 设置复制操作选项时，请选择**使用复制**。

有关详细过程，请参见标准对象复制任务。

## 自动复制同步

通过 Data Protector 复制功能，可以在两个具有复制功能的备份到磁盘 (B2D) 设备之间复制对象，而无需通过介质代理传输数据。自动复制同步功能是正常复制的扩展，借助它可以在由不同 Cell Manager 管理的两个重复数据删除设备之间复制备份元数据。通过此功能，可以在两个重复数据删除设备之间轻松交换备份数据及其他元数据。

## 先决条件

确保源 Cell Manager 上的 Data Protector 用户 (CRS 在其帐户下运行) 有权访问目标 Cell Manager。

## 注意事项

对于集成备份，不要从部分失败的备份会话 (即已完成但有错误的备份会话) 执行自动复制同步过程。复制将会成功，但是从复制的会话恢复可能会失败。

## 限制

- 考虑对正常复制功能应用的所有限制。
- 目标 Cell Manager 的版本应与源 Cell Manager 的版本相同或更高。
- 源 Cell Manager 和外部 Cell Manager (目标 Cell Manager) 中为复制选择的设备必须指向相同的物理设备和数据存储。
- 一次可复制的最大介质数取决于目标设备上的可用空闲连接数。例如，如果目标设备具有 100 个空闲连接，建议同时复制不超过 100 个介质。此外，如果要使用目标设备执行其他操作，可同时复制的介质数必须少于可用的空闲连接数。  
对于 StoreOnce 和数据域提升设备，分别检查可用的数据连接和复制流。有关支持的流的详细信息，请参见各自的设备手册。
- 不支持使用旧版 GUI 的自动复制同步列表。您可能会看到以下错误消息：“Error parsing Copy Specification file. The file may be corrupted or invalid”。此消息表明旧版的 Data Protector GUI 不支持新列表。
- 自动复制同步过程不支持**仅包括副本数小于指定值的对象**选项。

自动复制同步包含两个步骤：

1. [导入外部 Cell Manager](#)
2. [执行对象复制会话](#)

## 导入外部 Cell Manager

触发自动复制同步的第一步是将外部 Cell Manager 导入源 Cell Manager。要导入外部 Cell Manager:

1. 在“上下文列表”中，单击**客户机**。
2. 在“范围窗格”中，右键单击**客户机**并单击**导入客户机**。
3. 键入客户机的名称或浏览网络以选择要导入的客户机(仅在 Windows GUI 上)。如果导入的是管理重复数据删除设备的 Cell Manager，请选择 **Data Protector 外部单元服务器**。

**注意：**如果执行的是自动复制同步过程，需要以上步骤。

4. 单击**完成 (Finish)** 以导入客户机。

所导入客户机的名称将显示在结果区域中。

**注意：**只能在导入的 Cell Manager 上执行自动复制同步操作。您将无法使用该 Cell Manager 执行其他任何操作。

## 执行对象复制会话

将外部 Cell Manager 导入源 Cell Manager 后，可以执行对象复制会话，将备份数据和其他元数据复制到外部 Cell Manager 中。根据要求，您可以执行调度的、备份后或交互式对象复制。

要执行对象复制会话：

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，导航至**复制 > 对象复制 > 自动**。
3. 右键单击**预定**，然后单击**添加**以打开向导。您也可以执行交互式或备份后对象复制会话。
4. 选择包含要复制的对象的备份、对象副本或对象合并规范。单击**下一步 (Next)**。
5. 指定用于对象复制操作的对象筛选器。将仅复制符合指定标准的对象。单击**下一步 (Next)**。
6. 指定用于对象复制操作的带库筛选器。将仅复制位于指定库中介质上的对象。单击**下一步 (Next)**。
7. 默认情况下，在选定备份规范中用于备份的设备在对象复制操作中用作源设备。如果需要，可以在此处更改源设备。单击**下一步 (Next)**。
8. 选择用于对象复制操作的目标设备。Data Protector 将从此处指定的设备中选择最合适的设备。单击**下一步 (Next)**。

选中**显示能够复制**复选框，以仅选择具有备份到磁盘(重复数据删除)设备的设备。只有在备份到磁盘设备上才可以进行复制。

9. 根据需要指定源对象选项、目标对象选项和目标介质选项。

选择**使用复制**以启用两个 B2D 设备之间的复制而不是复本的复制。

选择**复制到外部单元**以启用将对象复制到之前导入的外部单元服务器(此 Cell Manager 包含第二个重复数据删除设备)。

单击**下一步 (Next)**。

10. 从下拉菜单中选择之前导入的外部单元服务器。这样将列出链接到备份到磁盘存储的设备。

从目标 **Cell Manager** 创建且具有相同存储名称的所有设备都会显示在此处。因此，确保选择具有正确存储名称的设备来执行复制。

选择所需的设备或网关，然后单击**下一步**。

11. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存计划对象复制规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。

有关如何使用调度程序在 **Data Protector** 中创建和编辑计划，请参见 [计划程序 \(第 92 页\)](#)。

运行调度的对象复制会话以完成自动复制同步过程。

## 关于对象镜像

通过 **Data Protector** 的对象镜像功能，可以在备份会话期间将同一数据同时写入多个介质集。您可以将全部或部分备份对象镜像到一个或多个其他介质集。

使用对象镜像的成功执行备份会话的结果是得到一个包含已备份对象的介质集以及包含镜像对象的其他介质集。这些介质集上的镜像对象被视为对象副本。

## 对象镜像的优点

使用对象镜像功能可以达到以下目的：

- 由于存在多个副本，它可提高已备份数据的可用性。
- 它使得多地点保管介质变得更加容易，因为已备份数据可以镜像到远程站点。
- 由于相同数据写入到若干介质上，因此它提高了备份的容错能力。一个介质上的介质故障不会影响创建其他镜像。

## 限制

- 无法使用 **ZDB** 到磁盘或 **NDMP** 备份功能镜像对象备份。
- 无法在一个会话中将一个对象多次镜像到相同设备。
- 设备的块大小在镜像链中不得递减。这意味着：
  - 用于写入镜像 1 的设备的块大小必须等于或大于用于备份的设备。
  - 用于写入镜像 2 的设备的块大小必须等于或大于用于写入镜像 1 的设备，以此类推。

## 如何使用对象镜像

配置备份规范时即可指定对象镜像。在备份规范中，选择要镜像的对象，然后指定镜像数。要能够指定超过 5 个镜像，请提高 **MaxNumberOfMirrors** 全局选项的值。

分别为备份和每个镜像指定单独的设备。具有对象镜像的备份会话开始后，Data Protector 从备份规范中指定的那些设备中选择设备。为避免影响性能，建议设备采用相同的块大小，并且都连接到相同系统或 SAN 环境。镜像 SAP MaxDB、DB2 UDB 或 Microsoft SQL Server 集成对象所需的最少设备数与用于备份的设备数相等。

默认情况下对于对象镜像进行负载均衡。Data Protector 通过使用尽可能多的设备，最优地利用可用的设备。从命令行执行对象镜像操作时，负载均衡不可用。

## 复制介质

可以复制介质用于归档或保管。需要单独启动每个介质的复制，因为在一个介质复制会话中只能复制一个介质。

### 在独立设备中复制介质

#### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中，展开**设备**，右键单击含有要复制的介质的设备，然后单击**复制**。
3. 选择目标介质所在的设备(库的驱动器和插槽)，然后单击**下一步**。
4. 选择要向其添加介质副本的介质池，然后单击**下一步**。
5. 指定介质副本的说明和位置(可选)，然后单击**下一步**。
6. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

#### 提示：

如果目标介质具有 Data Protector 可识别的其他格式(tar 和 OmniBack I 等等)或如果这些介质是不受保护的 Data Protector 介质，则使用**强制操作**选项。

7. 单击**完成**以开始复制，然后退出向导。  
“会话信息”消息显示介质复制操作的状态。

### 在带库设备中复制介质

#### 步骤

1. 在上下文列表中，单击**设备和介质**。
2. 在范围窗格中的**介质**下，展开**池**，然后展开含有要复制的介质的介质池。右键单击介质，然后单击**复制**以打开向导。
3. 为要复制的介质选择驱动器，然后单击**下一步**。如果带库只有一个驱动器，则跳过此步骤。
4. 选择目标介质所在的设备(库的驱动器和插槽)，然后单击**下一步**。
5. 选择要向其添加介质副本的介质池，然后单击**下一步**。
6. 指定介质副本的说明和位置(可选)，然后单击**下一步**。
7. 指定会话的其他选项：可以选择**强制操作**选项，指定介质大小和介质保护。

**提示：**

如果目标介质具有 Data Protector 可识别的其他格式(tar 和 OmniBack I 等等)或如果这些介质是不受保护的 Data Protector 介质，则使用**强制操作**选项。

8. 单击**完成**以开始复制，然后退出向导。  
“会话信息”消息显示介质复制操作的状态。

# 第 13 章：对象验证

## 关于对象验证

通过 **Data Protector** 对象验证功能，可以对备份对象进行验证。使用此功能，不必再单独以交互方式验证完整的备份介质。现在可以在计划的会话中或在操作后会话中以交互方式验证单个或多个介质上的单个或多个对象。

所验证的对象可以是原始备份对象、对象副本和合并对象。

## 数据验证

在对象验证会话期间，**Data Protector** 以验证介质时使用的类似方式验证各个备份对象的数据。

## 传递到主机

默认情况下，对其执行数据验证过程的目标主机是原始备份源主机。这样可验证 **Data Protector** 能否将备份数据从介质代理主机传递到该主机。此外，可以指定不同的目标主机，或可以在介质代理主机上执行验证，从而避免涉及任何网络。

## 对象验证会话的类型

可以用交互方式启动对象验证会话，也可以指定自动启动会话。**Data Protector** 可提供两种自动对象验证：备份后对象验证和计划的对象验证。

## 备份后对象验证

完成备份、对象复制或合并会话之后立即执行备份后对象验证，并验证这些会话期间创建的对象。在备份后对象验证规范中指定要验证的对象。这样将指定备份、对象复制和/或合并规范以定义所创建的对象，并提供用于筛选对象的标准。一个备份后对象验证规范中可以包括多个备份、对象复制和/或合并规范。

## 计划的对象验证

计划的对象验证在 **Data Protector** 计划程序中指定的时间执行，并验证指定时期内创建的备份、复制或合并对象版本。在计划的对象验证规范中指定要验证的对象和对象版本创建的有效期。这样将指定备份、对象复制和/或合并规范以定义所创建的对象，并提供用于筛选对象的标准。一个计划的对象验证规范中可以包括多个备份、对象复制和/或合并规范。

## 如何验证对象

首先，启动交互式会话，或创建对象验证规范。选择要验证的备份对象、源设备、介质和验证目标主机。

## 备份对象的选择

### 自动操作

对于自动对象验证规范，可以通过选择备份、对象复制或合并规范，然后按照保护、副本数、可用库或时间范围(仅计划)进行筛选，从而选择要验证的对象。在此情况下，无法选择单个对象版本进行验证：**Data Protector** 将验证与过滤条件匹配的所有对象版本。

### 交互式操作

对于交互式会话，可以从介质、会话或 **IDB** 中的对象选择向导列表中选择单独的对象。在这种情况下，可以选择所需对象版本的单独副本进行验证。

## 源设备的选择

默认情况下，**Data Protector** 执行自动设备选择。此外，可以强制选择原始设备，或选择新设备。

## 目标主机的选择

默认情况下，**Data Protector** 在源主机(即原始备份的源对象所在的主机)上执行验证过程，从而验证对象数据及其传递。还可以指定备用远程主机或介质代理主机，从而仅验证对象数据。请注意，所选目标主机必须装有 **Data Protector** 磁盘代理。

## 安排

使用 **Data Protector** 计划程序，以用于备份的相同方式对计划的验证操作执行计划。

有关如何使用计划程序在 **Data Protector** 中创建和编辑计划的更多信息，请参见 [计划程序\(第 92 页\)](#)。

### 重要：

借助 **Data Protector 10.00**，基本计划程序和高级计划程序已过时，被基于 **Web** 的新计划程序所替代。可以配置无人看管备份，具体方法是排定备份会话使其在特定的时间执行。升级 **Data Protector** 时，所有现有的 **Data Protector** 计划会自动迁移至新的计划程序。

## 标准对象验证任务

下面是对对象验证功能的先决条件和限制：

## 先决条件

- 需要在将充当对象验证会话中的源主机的每个系统上安装介质代理。
- 需要在将充当对象验证会话中的目标主机的每个系统上安装磁盘代理。
- 对象验证处理中涉及的所有磁盘代理都必须为 **A.06.11** 或更高版本。
- 应配置必要的设备，并准备好介质。
- 您需要在源主机和目标主机上有适当的用户权限才能运行对象验证会话：它们是“启动还原”和“从其他用户还原”用户权限。
- 如果目标主机是 **UNIX** 主机，则必须有“作为 **root** 还原”权限。

## 限制

- 读取源介质时，该介质不可用于还原。
- 应用程序集成对象的对象验证包括验证对象数据传递到目标主机以及这些数据从 **Data Protector** 格式的角度来看保持一致。未执行任何应用程序集成特有的检查。
- 对于使用 **ZDB** 到磁盘备份的对象或 **ZDB** 到磁盘 + 磁带的磁盘部分不能使用对象验证。

## 以交互方式验证对象

根据需要，可以选择用于从“介质”、“对象”或“会话”起始点开始的交互式验证的对象。不能保存交互式对象验证规范，只能启动对象验证会话。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**验证**，然后展开**对象验证**。
3. 展开**交互**。
4. 单击**介质**、**对象**或**会话**以打开向导。
  - 单击**介质**可列出已将对象写入的可用介质。
  - 单击**对象**可列出已写入可用介质的对象。
  - 单击**会话**可列出从中已将对象写入可用介质的会话。
5. 选择要验证的对象。

### 注意：

自 **Data Protector 10.00** 起，对于 **Vmware** 备份，将虚拟机磁盘视为并行运行的对象。虚拟机的磁盘对象会列在**介质**列表中，但它们处于禁用状态，表明虚拟机磁盘已备份到介质。将在虚拟机对象上执行复制或验证操作，并将其所有关联的磁盘对象视为内部对象。



自 Data Protector 10.00 起，对于 Vmware 集成，只有在介质列表中选择虚拟机对象后，才会启用下一步选项。

单击**下一步 (Next)**。

6. 选择将从中读取对象的源设备。默认情况下，选择自动选择设备。  
还可以强制选择原始设备，或者可通过单击**原始设备**再选择**更改设备**用其他驱动器代替。

单击**下一步 (Next)**。

7. 选择对象验证操作的目标主机。此主机必须装有所需版本级别的 Data Protector 磁带客户机。

默认情况下，选择原始备份源主机。还可以选择介质代理主机(其中装有所选的源设备)或从单元中选择装有所需版本级别的磁带客户机的任意主机。单击**下一步 (Next)**。

8. 此时将显示包含所选对象的介质的列表。可以更改介质位置的优先级，以影响同一对象位于多个介质集上时介质的选择。

单击**下一步 (Next)**。

9. 此时将显示选择进行验证的对象版本的摘要。
  - 要显示特定对象版本的详细信息，请在列表中选择该版本，然后单击**属性**。  
如果存在对象版本的多个副本，则默认情况下 Data Protector 选择一个最适合进行验证的副本。可以在属性中手动选择要验证哪个副本。  
单击**确定**。

- 要从列表中删除对象版本，请在列表中选择该版本，然后单击**删除**。

10. 单击**完成**以关闭向导并启动验证。

## 配置备份后对象验证

备份后对象验证配置为在备份会话、对象复制会话或对象合并会话完成之后进行。

在自动对象验证规范中选择相关的备份、对象副本和/或合并规范的名称。运行使用这些所选规范中任意一种的会话时，在该会话完成之后，Data Protector 使用在对象验证规范中指定的标准，验证在会话期间产生的对象。

## 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**验证**，然后展开**对象验证**。
3. 展开**自动**，右键单击**备份后**，然后选择**添加**以打开向导。
4. 选择要紧跟在对象验证规范后的备份规范。单击**下一步 (Next)**。
5. 选择要紧跟在对象验证规范后的对象副本规范。单击**下一步 (Next)**。
6. 选择要紧跟在对象验证规范后的合并规范。单击**下一步 (Next)**。
7. 如果需要，请指定用于对象验证操作的对象筛选器。将仅验证符合指定标准的对象。  
单击**下一步 (Next)**。

8. 如果需要，请指定用于对象验证操作的带库筛选器。将仅验证指定库中介质上包含的对象。单击**下一步 (Next)**。
9. 选择将从中读取对象的源设备。默认情况下，Data Protector 使用自动设备选择。  
此外，可以强制选择原始设备。这表示如果设备不可用，则 Data Protector 将等待到它可用为止。还可以通过右键单击**原始设备**并选择**更改设备**，用另一个驱动器代替原始设备，例如接下来由新设备替换原始设备。  
单击**下一步 (Next)**。
10. 选择对象验证操作的目标主机。此主机必须装有 Data Protector 磁带客户机。  
可以选择：
  - 生成了原始备份对象的主机(默认选择)。这还将验证网络路径中的 Data Protector 组件。
  - 介质代理主机，即含有源设备的主机，但不涉及任何网络。
  - 备用远程主机，验证该主机的网络路径中的 Data Protector 组件。单击**下一步 (Next)**。
11. 单击**另存为...**，输入规范名称，然后单击**确定**以保存验证规范。

## 配置计划对象验证

计划对象验证发生在用户定义的某个时间。可在一个排定对象验证会话中验证由不同备份会话、对象复制会话或对象合并会话生成的对象。

### 步骤

1. 在上下文列表中，单击**对象操作**。
2. 在范围窗格中，展开**验证**，然后展开**对象验证**。
3. 展开**自动**，右键单击**预定**，然后选择**添加**以打开向导。
4. 选择定义要为其安排验证的输出对象的备份规范。单击**下一步 (Next)**。
5. 选择定义要为其安排验证的输出对象的对象副本规范。单击**下一步 (Next)**。
6. 选择定义要为其安排验证的输出对象的合并规范。单击**下一步 (Next)**。
7. 如果需要，请指定用于对象验证操作的对象筛选器。  
这使您可以根据保护、副本数或创建时间筛选可用对象。将验证符合筛选器标准的所有对象版本。  
单击**下一步 (Next)**。
8. 如果需要，请指定用于对象验证操作的带库筛选器。将仅验证指定库中介质上包含的对象。单击**下一步 (Next)**。
9. 选择将从中读取对象的源设备。默认情况下，Data Protector 使用自动设备选择。  
此外，可以强制选择原始设备。这表示如果设备不可用，则 Data Protector 将等待到它可用为止。还可以通过右键单击**原始设备**并选择**更改设备**，用另一个驱动器代替原始设备，例如接下来由新设备替换原始设备。

单击**下一步 (Next)**。

10. 选择对象验证操作的目标主机。此主机必须装有 **Data Protector** 磁带客户机。

可以选择：

- 生成了原始备份对象的主机(默认选择)。这还将验证网络路径中的 **Data Protector** 组件。
- 介质代理主机，即含有源设备的主机，但不涉及任何网络。
- 备用远程主机，验证该主机的网络路径中的 **Data Protector** 组件。

单击**下一步 (Next)**。

11. 单击**保存并计划 (Save and Schedule)...**。输入规范名称，然后单击**确定**以保存验证规范。保存规范后，将会打开“计划”向导。按照向导中的步骤执行操作，以计划规范。

有关如何使用调度程序在 **Data Protector** 中创建和编辑计划，请参见 [计划程序 \(第 92 页\)](#)。

## 自定义对象验证环境

通过修改在没有对象供验证会话进行验证时所生成的消息级别和会话状态，可以自定义对象验证环境。要实现此目的，请修改 **SessionStatusWhenNoObjectToVerify** 全局选项。

# 第 14 章：还原

## 关于还原

还原是将原始数据从备份副本重新创建到磁盘的过程。此过程由数据准备及实际还原和一些可能的还原后操作组成，执行还原后操作是为了使该数据做好使用准备。

有关恢复概念的详细信息，请参见 *Data Protector 概念指南* 和 *Data Protector 集成指南*。

根据平台的不同，指定这些功能和可用选项的方式可能有所不同。

有关如何通过应用程序集成恢复到应用程序(如 Oracle、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server、Informix Server、IBM DB2 UDB 或 Sybase)的信息，请参见 *Data Protector 集成指南*。

## 标准还原过程

标准还原过程由几个阶段组成。

1. 选择要恢复的数据。
2. 查找必需介质。
3. 启动恢复会话。

其他设置根据备份过程预定义，但可以修改。

## 先决条件

要执行恢复，您必须有合适的用户权限。这些权限根据用户组定义。

## 选择要还原的数据

可以通过以下两种可能的方式浏览要恢复的数据：从备份对象列表或从会话列表。不同之处在于还原目录和文件的显示范围不同：

- **还原对象**使用的备份对象列表按单元中的客户机系统分类并按不同数据类型分类(比如文件系统，磁盘映像，内部数据库，等等)。可以浏览所有目录、文件和版本，这些版本已备份并仍然可用于还原。
- **还原会话**使用的文件系统会话列表具有在这些会话中备份的所有对象。可以选择查看自去年、上一个月或上一周以来的会话。可以浏览在此会话中备份的所有对象(如在备份规范中命名的所有客户机的任何驱动器)，以及此恢复链的所有版本。默认情况下，还原所选目录或文件的整个还原链，但也可以仅从单个会话还原数据。

## 先决条件

要浏览对象并选择目录或特定文件，必须已经使用目录、文件名或全部记录日志记录级别完成了相应的备份。

## 从备份对象列表选择数据

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象(UNIX 系统上的装载点，Windows 系统上的驱动器)。
4. 在“源”属性页中，展开该对象，然后选择要还原的目录或文件。

默认情况下，当选择整个目录时，仅选择最后一个备份会话的目录和/或文件用于还原。尚未在相同备份会话中备份的相同树结构中的目录和文件将被覆盖。如果要从任何其他备份会话中还原数据，请右键单击所选目录，并单击**还原版本**。在“备份版本”下拉列表中，选择要从中还原的备份版本。

#### 提示：

如果重复上述步骤并在多个对象(装载点或驱动器)下选择数据，则可以执行并行恢复。

## 从备份会话列表选择数据

### 限制

- 无法从特定备份会话执行联机数据库集成的恢复。
- 无法使用“恢复会话”模式从复制会话执行恢复。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开**恢复会话**以显示客户机，然后显示在特定客户机上备份的对象。单击某个对象可以打开该对象的属性页。
3. 在**源**页中，选择要还原的目录和文件。

默认情况下，将恢复整个恢复链(已选择**显示完整链**)。要从此会话中仅恢复数据，请选择**仅显示此会话**。

4. 指定还原目标，并设置还原选项。
5. 单击**恢复**以启动恢复会话。

#### 提示：

要执行并行恢复，请在启动恢复之前，对其他对象重复步骤 2 至 4。

## 选择特定备份版本

在选择要还原的数据之后，可以选择其备份版本。

## 单独选择每个文件或目录的备份版本

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，文件系统)。
3. 展开具有要恢复的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，选择要还原的对象。默认情况下，将为还原选择最新备份版本。
5. 右键单击该对象，并单击**还原版本**。
6. 在“备份版本”下拉列表中，选择要还原的备份版本。单击“...”，如果需要关于备份版本的详细信息。当使用记录属性的日志记录级别执行备份时，“...”按钮才可用。
7. 单击**确定**。

在选择用于还原的版本之后，在“源”属性页中只有此版本的文件和目录显示为可以还原。其他文件和目录显示为灰色，无法还原。

## 同时选择几个文件或目录的备份版本

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，文件系统)。
3. 展开具有要恢复的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，选择要还原的多个对象。默认情况下，将为还原选择最新备份版本。
5. 单击**还原摘要**选项卡，选择所有对象，右键单击所选对象，然后单击**按日期选择版本**。
6. 单击**按日期和时间选择版本**选项，并从弹出菜单中选择天。
7. 通过在**按日期和时间选择版本**下拉列表中显示的时间上单击，可以输入时间。
8. 在**备份时间上的差异**下，如果没有备份版本对应于任何所选对象的日期和时间选择，则进行任何必要的调整。
9. 在**如果选择的日期和时间与选择的条件不匹配**下，如果没有备份版本对应于任何所选对象的日期和时间选择以及**备份时间中的差异**更正，则进行任何必要的调整。
10. 单击**确定**。

在已经指定还原条件之后，与选择对应的备份版本将显示在“源”属性页中每个要还原对象的旁边。

## 处理文件冲突

您可以选择解决磁盘上当前文件版本与备份版本之间冲突的方法。

## 步骤

1. 在上下文列表中，单击**还原**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要恢复的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，选择要还原的磁盘、目录或文件。
5. 单击**目标**选项卡，然后在“文件冲突处理”下，选择可用选项之一：
  - 保持最新
  - 不覆盖
  - 覆盖

## 选择要从中还原的设备

默认情况下，**Data Protector** 使用在备份期间使用的相同设备还原选择的数据。但是，可以为还原选择备用设备。

## 步骤

1. 在上下文列表中，单击**还原**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要恢复的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，展开该对象，然后选择要还原的内容。
5. 单击**设备**选项卡以打开“设备”属性页。

这里列出在备份期间使用的设备。

要使用备用设备恢复数据，请选择原始设备，并单击**更改**。在“选择新设备”对话框中，选择备用设备，并单击**确定**。新设备的名称出现在“设备状态”下。新设备将仅用于此会话。

有关设备的详细信息，请右键单击该设备，并单击**信息**。

指定当选择的设备在还原期间不可用(例如，如果已被禁用或在使用中)时，**Data Protector** 应如何操作。选择**自动设备选择**或**原始设备选择**。

## 查找还原所需的介质

在选择要还原的数据之后，需要获取包含数据的介质列表。如果使用独立设备，或者库外保存介质，必须选择该选项。

如果要恢复的对象版本存在于多个介质集上，通过设置介质位置优先级或手动选择要使用的介质集，可以影响将用于恢复的介质集的选择。

如果使用合成备份，则对于一个对象的同一时间点，通常有多个恢复链。默认情况下，**Data Protector** 会选择最方便的还原链以及所选还原链内最合适的介质。

**注意：**

使用介质副本功能获取的副本不列为必要介质。仅当原始介质(用作复制源的介质)不可用或不能用时，才使用介质副本。

## 限制

- 对于某些集成，不能在“还原”上下文中设置介质位置优先级。GUI 对于这些集成不显示“介质”选项卡。
- 还原集成对象时，无法手动选择介质集。

## 步骤

1. 在上下文列表中，单击**还原**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要恢复的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，展开该对象，然后选择要还原的内容。
5. 单击**介质**选项卡以打开“介质”属性页。其中将列出所需的介质。有关介质的详细信息，请右键单击相应介质，并单击**信息**。

如果要还原的对象版本存在于多个介质集上，将列出包含对象版本的所有介质。介质集的选择取决于 **Data Protector** 内部介质集选择算法和介质位置优先级设置。

- 要覆盖介质位置优先级设置，请选择一个位置，并单击**更改优先级**。为该位置选择一个不同优先级，并单击**确定**。
  - 要手动选择要从中还原的介质集，请单击**副本**选项卡。在“副本”属性页中，选择希望的对象版本，并单击**属性**。选择**手动选择源副本**选项，从下拉列表选择希望的副本，并单击**确定**。
6. 如有必要，将介质插入设备。

**提示：**

还可以通过在“启动恢复会话”对话框中单击**所需介质**，列出恢复所需的介质，其中包括含有所选对象的对象副本的介质。启动还原时将出现此对话框。

## 预览和启动还原

### 先决条件

- 确保在设备中提供或加载了所需的介质。

### 限制

- 对于 **Data Protector** 内部数据库还原和 **Data Protector** 应用程序集成的还原会话，预览不可用。



## 步骤

1. 在还原属性页中选择要还原的内容并指定选项，包括选择要使用的设备。
2. 检查还原需要哪些介质。
3. 在**操作**菜单中，如果希望预览，请单击**预览恢复**，如果要实际启动恢复过程，请单击**启动恢复**。还可以单击**属性**页上的**预览**或**恢复**按钮。
4. 在“启动会话”向导中，检查您的选择，并指定**报告级别**、**网络负载**和**启用可恢复的恢复**选项。

还原监视器可显示还原的进度。

## 中止还原

中止还原会话将停止还原。在中止会话之前处理的数据将还原到指定位置。

## 步骤

1. 要中止恢复会话，请在**操作**菜单中单击**中止**。

**提示：**  
可以从 **Data Protector** 监视器中止恢复会话。

## 还原位置选项

默认情况下，**Data Protector** 将数据还原到从中备份它的同一客户机和目录。通过指定要将数据还原到的位置，可以在“目标”属性页中更改这些默认设置：

- 使用合适的用户权限，可以恢复到另一客户机系统
- 可以还原到另一个目录

可以按每个对象设置常规还原位置。

另外，**Data Protector** 还提供了**恢复为/恢复至**选项，可以为个别文件和目录指定与相同备份对象不同的位置。

## 选择还原位置

在选择要还原的数据之后，可以选择要将数据还原到的位置。可以将数据还原到另一个客户机系统，并更改目录路径。这适用于要还原的整个对象。

## 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在范围窗格中的“还原对象”下，展开合适的数据类型。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，选择要还原的对象。
5. 单击**目标**选项卡，然后在**目标客户机**下拉列表中，选择要在新客户机上还原的客户机

系统。默认情况下，Data Protector 使用原始目录结构进行恢复：如果数据是从系统 A 上的 C:\temp 目录备份的，则将该数据恢复到系统 B 上的 C:\temp 目录。

6. 通过选择**恢复到新位置**选项，然后输入或浏览新标记目录，可以更改恢复的目录路径。在备份时，目录路径附加到新标记目录：如果数据是从 C:\sound\songs 目录备份的，并且输入 \users\bing 作为新路径，则将该数据恢复到 C:\users\bing\sound\songs 目录。

## 指定个别文件和目录的还原位置

可以在每个对象中指定任何目录或文件的单个还原路径。在**还原为/到**选项下指定的单个位置将覆盖在“目标”属性页中指定的位置。

此功能可用于最初选择的树节点(目录)和在层次结构上不依赖于任何已选择的树节点上的树节点。选定树节点由蓝色复选标记表示，依赖的树节点由黑色复选标记表示。

### 还原到

“还原到”将路径从备份附加到此处选择的新位置。新位置必须是现有目录。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在范围窗格中的“还原对象”下，展开合适的数据类型。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，选择要还原的对象。
5. 右键单击特定的文件或目录，然后单击**恢复为/恢复至**。
6. 在“目标”选项卡下的“恢复”下拉列表中，选择**至**。
7. 作为 Windows 系统上的选项，可以在“驱动器”文本框中选择要将数据还原到的另一个驱动器。如果要还原到另一个客户机系统，则单击**浏览**。
8. 在“位置”文本框中，输入文件或目录的新路径。将原始路径添加到新路径：如果 colors.mp3 文件是从 C:\sound\songs 目录备份的，并且输入 \users\bing 作为新路径，则该文件将恢复到 C:\users\bing\sound\songs 目录。
9. 单击**确定**。

### 还原为

**还原为**使用在这里选择的新位置替换备份路径。目标路径可以是新目录或现有目录。在还原文件和目录时，可以对其重命名。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在范围窗格中的“还原对象”下，展开合适的数据类型。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，选择要还原的对象。

5. 右键单击特定的文件或目录，然后单击**恢复为/恢复至**。
6. 在“目标”选项卡下的“恢复”下拉列表中，选择**为**。
7. 作为 Windows 系统上的选项，可以在“驱动器”文本框中选择要将数据还原到的另一个驱动器。如果要还原到另一个客户机系统，则单击**浏览**。
8. 在“位置”文本框中，输入文件或目录的新路径。例如，如果 colors.mp3 文件是从 C:\sound\songs 目录备份的，并且输入 \users\bing\colors.mp 作为新路径，则该文件将恢复到 C:\users\bing 目录。

**警告：**

在以下情况下，应注意启用**覆盖**选项时有删除数据的风险：

- 指定用已经存在的名称还原
- 输入现有路径而不指定文件或目录名。

例如，如果在“位置”文本框中输入一个新路径 \users\bing 来恢复文件 colors.mp，但没有输入该文件的名称，则 colors.mp 文件将恢复为 bing。以前的 bing 目录将被删除，并替换为恢复的文件。

9. 单击**确定**。

## 关于恢复失败的会话

因以下任何原因失败的备份和还原会话都可以使用 **Data Protector** 还原会话功能进行还原：

- 网络连接性问题
- 致命的磁盘代理问题
- 致命的介质代理问题
- **Session Manager** 严重问题
- 介质严重问题(例如磁带撕裂)
- 从 GUI 调用的“中止”命令

但是，首先必须解决阻碍的问题。

还原失败的会话时，**Data Protector** 会继续进行备份或还原，正好从失败的会话停止之处开始。恢复的会话从原始会话中继承所有选项。

并非所有的会话类型都可以恢复。**Data Protector** 可以恢复下列会话：

- 文件系统备份会话
- 文件系统还原会话
- **Data Protector Oracle Server** 集成备份会话
- **Data Protector Oracle Server** 集成还原会话

## 文件系统备份会话

文件系统备份会话的恢复会话功能基于写入内部数据库的检查点文件信息。备份会话失败时，系统会在内部数据库中将上次备份的文件标记为检查点。因此，备份会话可以在会话恢复后从失败点继续执行。失败点的文件在开始时备份，而剩余的数据将作为增量备份追加到原始备份会话中。恢复的会话自动继承原始会话的选项。

如果从文件系统中删除了标记为检查点的文件，则恢复功能仍然可以确定哪些数据尚未备份。可以多次恢复失败的备份会话，直至其成功完成。

在图形用户界面中，可以使用失败的会话的上下文菜单恢复会话。在命令行界面中，可以使用 `omnib -resume` 选项恢复会话。

## 限制

- 不支持对灾难恢复进行恢复。
- 不支持对包含 **NDMP** 介质数据格式对象的会话进行恢复。
- 使用以下备份客户机系统备份的对象不可恢复：**Solaris 9**、**SCO OpenServer** 和 **OpenVMS**。

## 文件系统还原会话

文件系统还原会话的还原会话功能基于还原会话期间创建的检查点，并包含有关会话中使用了哪些还原选项和已成功还原了哪些文件的信息。还原新文件后，即可更新对应的检查点文件。

默认情况下，在 **Cell Manager** 和目标客户机上均创建检查点文件(但仅在 **Cell Manager** 上创建包含有关还原选项信息的检查点文件)。

在 **Cell Manager** 上的以下位置创建检查点文件：

**Windows 系统：** `\config\server\sessions\checkpoint`

**UNIX 系统：** `/var/opt/omni/server/sessions/checkpoint`

在客户机上，系统将在默认 **Data Protector** 临时文件目录下的 **Checkpoint** 子目录中创建检查点文件。

## 此项功能的工作方式

还原失败的还原会话时，**Data Protector** 从检查点文件读取信息，然后从失败的还原会话停止之处继续还原。实际上，当恢复还原会话时，其检查点文件即移至所恢复还原会话的检查点文件目录，其中不断更新这些检查点文件。因此，对于失败的还原会话只能恢复一次。如果尝试再次恢复失败的会话，则操作将失败，因为那里已不再有相应的检查点文件。

## 注意事项

- 在群集环境中，请确保在共享磁盘上创建检查点文件，这样两个群集节点即均可访问这些文件。要更改检查点文件的位置，请使用 `OB2CHECKPOINTDIR omnirc` 选项。必须在两个群集节点上都设置该选项，并且该变量必须指向相同目录。
- 启动还原会话之前，通过清除 **启用可恢复还原** 选项，可禁止创建检查点文件(可在还原向导末尾的“启动还原会话”对话框中找到该选项)。但是，如果此类还原会话失败，即无法恢复，因为将缺少检查点文件。由于 **Data Protector** 在此类会话的末尾删除了检查点文件，因此也无法恢复成功完成的会话。
- 还原会话之后，如果该会话未成功完成，则还可以恢复该会话。这是因为所恢复的还原会话继承了原始会话的检查点文件。因此，它继承了原始会话中使用的所有还原选项，包括 **启用可恢复还原** 选项。
- 从 **IDB** 删除还原会话后(默认情况下 30 天后删除会话)，还会清除其检查点文件。使用

omnidbinit 命令初始化 IDB 时，也会清除检查点文件。

- 如果在一个失败的会话中使用**没有覆盖**选项还原一个或多个对象，则必须将 omnirc 选项 OB2NOOVERWRITE\_TRAVERSEDIOBJ 设置为 1，然后再还原该会话。

## 限制

- 如果还原会话因目标客户机崩溃而失败，则还原会话功能可能无法正确工作。它完全依赖于客户机崩溃时是否成功地将检查点文件从内存保存到磁盘中。
- 如果还原会话正好在还原硬链接文件时失败，则还原会话功能可能无法还原其余的硬链接文件。这是由于在备份期间，Data Protector 对硬链接文件仅备份一次。对于与其硬链接的其他文件，它仅备份对文件的引用。因此，还原硬链接文件是相互联系的，因此必须将文件一起还原。请注意，如果还原会话在开始还原硬链接文件之前或在已成功还原这些文件之后失败，则不会发生此问题。
- 假定要还原已在以下会话中备份的树：完整、增量和增量。如果还原会话因在某个备份会话中创建的树备份对象不可用而失败(例如上次 Incr 备份会话中使用的备份介质已损坏)，则必须提供该备份对象的副本。如果此类对象复制不存在，则无法还原失败的还原会话，即使存在缺少的备份对象的合成完整备份也是如此。

## Data Protector Oracle Server 集成备份和还原会话

有关 Data Protector Oracle Server 集成备份和还原会话的还原会话功能，请参见《Data Protector 集成指南》。

## 恢复失败的会话

可以使用 Data Protector 恢复会话功能恢复失败的备份和恢复会话(例如由于某些网络连接性问题)。恢复失败的会话时，Data Protector 会继续进行备份或还原，正好从失败的会话停止之处开始。

## 先决条件

- 您必须位于 Data Protector Admin 用户组中，或者获得了 Data Protector 监视用户权限。

## 步骤

1. 如果您使用的是普通 Cell Manager，在上下文列表中单击**内部数据库**。  
如果您使用的是管理器的管理器，在上下文列表中选择**客户机**，然后展开**企业客户机**。选择会话出现问题的 Cell Manager。从“工具”菜单中选择**数据库管理**，从而打开一个新 Data Protector GUI 窗口，并显示“内部数据库”上下文。
2. 在范围窗格中，展开**内部数据库**，然后单击**会话**。  
此时将在结果区域中显示会话的列表。每个会话的状态显示在“状态”列中。
3. 右键单击失败的会话并选择**恢复会话**。

## 高级还原任务

可以通过许多方式控制还原。Data Protector 为 Windows 和 UNIX 系统提供了一组高级恢复任务。

### 先决条件

- 要执行恢复，您需要有合适的用户权限。这些权限根据用户组定义。
- 在继续之前必须考虑标准还原过程。

### 高级恢复任务

高级还原任务包括指定很少使用的选项，或采取一些不遵循标准还原过程的操作。要还原数据，仍须执行大多数标准还原步骤。

遵循标准还原过程的方式取决于要执行的高级任务。例如，不进行浏览也可还原数据。在这种情况下，需要用其他方式指定所需文件，但仍可以在其他步骤中遵循标准还原过程。

- 跳过用于还原的文件
- 仅选择特定文件(匹配)用于还原
- 选择打开的文件用于还原
- 在还原期间拒绝访问文件
- 搜索要还原的文件
- 选择用于还原的 Windows 共享磁盘
- 并行还原对象
- 磁盘映像还原
- 保管中的介质还原
- Web 服务器还原
- 还原而不浏览

### 跳过用于还原的文件

Data Protector 允许跳过已备份但不想还原的文件。通过使用通配符，您可以跳过匹配特定模式的文件。

**注意：**  
Data Protector 服务器集成不支持跳过还原的文件。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开合适的数据类型(例如，**文件系统**)。

3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象(UNIX 系统上的装载点，Windows 系统上的驱动器)。
4. 在“源”属性页中，选择要还原的目录。
5. 右键单击该目录，然后单击**属性**。
6. 单击**跳过**选项卡。
7. 在文本框中，输入用于匹配跳过文件的文件名或条件(例如，\*.mp3)，然后单击**添加**。  
在此示例中，不会恢复 mp3 文件。要使用更多条件，请重复此步骤。
8. 单击**确定**。

## 仅选择特定文件(匹配)用于还原

Data Protector 仅允许从匹配特定模式的备份还原这些文件。通过使用通配符，可以指定要使用的模式。

**注意：**  
Data Protector NDMP 服务器集成不支持此功能。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开合适的数据类型(例如，文件系统)。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象(UNIX 系统上的装载点，Windows 系统上的驱动器)。
4. 在“源”属性页中，选择要还原的目录。
5. 右键单击该目录，然后单击**属性**。
6. 单击**仅恢复**选项卡。
7. 在文本框中，输入文件名或输入匹配要恢复文件的条件，例如，\*.mp3，然后单击**添加**。这将仅恢复 mp3 文件。要添加更多条件，请重复此步骤。
8. 单击**确定**。

## 选择打开的文件用于还原

默认情况下，Data Protector 不还原正在由某些其他应用程序使用的文件(打开文件)。可以依照下列步骤还原打开的文件。

### 步骤

1. 在上下文列表中，单击**还原**。
2. 在“范围窗格”中，展开合适的数据类型(例如，文件系统)。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象(UNIX 系统上的装载点，Windows 系统上的驱动器)。
4. 在“源”属性页中，展开该对象，然后选择要还原的内容。
5. 单击**选项**选项卡，然后选择**移动繁忙文件**选项。

## 在还原期间拒绝访问文件

默认情况下，Data Protector 在还原期间不锁定文件。您可以更改此默认行为。

### 步骤

1. 在上下文列表中，单击**还原**。
2. 在“范围窗格”中，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象(UNIX 系统上的装载点，Windows 系统上的驱动器)。
4. 在“源”属性页中，展开该对象，然后选择要还原的内容。
5. 单击**选项**选项卡，然后选择在**恢复期间锁定文件**选项。

## 搜索要还原的文件

如果不知道要恢复的文件的完整路径，则可以在 IDB 中搜索该文件，但前提是在备份时已将日志记录级别设置为记录文件或全部记录。如果至少知道文件名的一部分，则可以使用**通过查询恢复**任务搜索文件和目录。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 单击“范围窗格”底部的**任务**导航选项卡。范围窗格中将列出预定义的还原任务。
3. 单击**通过查询恢复**以打开该向导。
4. 指定文件名的一部分，并使用通配符。

例如，键入 \*.exe 可以搜索具有此扩展名的所有备份文件。

指定非 SCII 字符时，确保 Data Protector GUI 中的当前编码与创建文件时使用的编码匹配。否则，Data Protector 将找不到文件。

在具有 UNIX Cell Manager 的环境中，如果您希望查找包含通配符 ? 的多字节字符，则该通配符将生成所需的结果。您需要指定多个通配符 ?。例如，如果当前编码中的多字节字符使用 3 个字节表示，则将 ??? 添加到字符串中。

如果目录可用，则仅将基本名称与模式进行比较。如果目录不可用，则将完整路径名称与模式进行比较。

5. (可选)指定其他参数。单击**下一步 (Next)**。
6. (可选)指定希望的时间段和修改时间。单击**下一步 (Next)**。

Data Protector 将列出与指定条件匹配的所有文件和目录。

7. 从与选择条件匹配的文件列表中，选择要还原的文件。要指定其他选项，请单击相应的选项卡。要指定**报告级别**、**网络负载**和**启用可恢复的恢复**选项，请单击**下一步**。要启动恢复，请单击**完成**。



## 选择用于还原的 Windows 共享磁盘

Data Protector 允许还原到共享磁盘，即使最初未从共享磁盘备份数据。

将 UNIX 或 Windows 文件系统还原到 Windows 共享磁盘的原因：

- 如果系统不是 Data Protector 单元的一部分，并且未安装 Data Protector 磁带客户机。
- 如果要还原到的平台不被 Data Protector 直接支持，例如 Windows 工作组或 Windows 3.1 系统。
- 如果希望使数据从几个系统提供。

在将数据还原到不同于其从中备份的文件系统类型时(例如，从 UNIX 系统到 Windows 系统)，特定于文件系统的属性可能会丢失。

## 先决条件

必须在磁带客户机上更改 Data Protector Inet 帐户，才能有正确权限访问要还原的共享磁盘。此帐户必须具有同时访问本地客户机系统和远程共享磁盘的权限。该帐户必须是特定用户帐户，而不是系统帐户。

## 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中，展开合适的数据类型。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象。
4. 在“源”属性页中，展开该对象，然后选择要还原的内容。
5. 单击**目标**选项卡。
6. 在**目标客户机**下拉列表中，选择用于恢复的磁带客户机的 Windows 客户机系统。

### 提示：

如果手动输入网络路径，则可以避免必须执行其余步骤，方法是，在**恢复到新位置**文本框中指定远程磁盘的 UNC 共享名称(\\COMPUTER\_NAME\SHARE\_NAME，例如 \\TUZLA\TEMP)。

如果在 UNIX 系统上使用 GUI，则必须这样做，因为系统不可能确认 Windows 共享驱动器的存在或浏览该驱动器。因此，您必须自己确认该驱动器可用并已正确指定，否则还原可能失败。

7. 选择**恢复到新位置**选项，然后单击**浏览**以显示**浏览驱动器**对话框。
8. 展开**Microsoft Windows 网络**，并选择要向其恢复数据的共享磁盘。
9. 单击**确定**。

## 并行还原对象

并行恢复允许从多个对象到多个磁盘或文件系统并发恢复数据，同时仅读取一次介质，因此可以提高恢复的速度。

## 先决条件

在备份时，必须使用 2 个或更多的并发数将来自不同对象的数据发送到同一设备。

## 限制

无法并行还原相同对象。例如，如果在**恢复对象**下为同一恢复选择了一个对象，然后在**恢复会话**下选择了包含相同对象的会话，该对象仅会恢复一次并将显示警告。

## 步骤

1. 像单个还原那样选择数据。还可以指定还原目标、选项等等。
2. 在范围窗格中返回到“还原”上下文，并对要还原的其他对象下的数据重复步骤 1。
3. 在**操作菜单**中，单击**开始还原**。将通知您选择了多个对象。
4. 选择**所有所选对象(并行恢复)**选项，并单击**下一步**。
5. 在“启动会话”向导中检查您的选择。单击**下一步 (Next)**。
6. 指定**报告级别**、**网络负载**和**启用可恢复的恢复**选项，并单击**完成**以启动对象的并行恢复。

## 磁盘映像还原

磁盘映像恢复是相应磁盘映像备份的快速恢复。Data Protector 可恢复磁盘的完整映像，逐扇区恢复而不是仅恢复选择的文件或目录。

要还原 UNIX 或 Windows 磁盘映像，请在“还原”上下文下展开**磁盘映像**对象，然后使用标准还原过程。

## 先决条件

- 要恢复的备份必须是磁盘映像类型。
- 在 UNIX 系统上，需要使用 **pre-exec** 和 **post-exec** 命令在恢复磁盘映像之前卸除磁盘并在恢复之后重新装载磁盘(例如，**pre-exec: umount /dev/rdisk/disk1**, **post-exec: mount /dev/rdisk/disk1 /mount\_dir**)。
- 如果要将磁盘映像还原到备份它的磁盘之外的磁盘，则新磁盘必须具有相同大小或者更大。

## 保管中的介质还原

从保管库中的介质还原与从任何其他介质还原非常类似。不过，根据数据和编目保护策略的定义方式，可能需要执行一些附加步骤：

- 如果有库，则输入介质并扫描它。
- 如果介质的编目保护仍然有效，则使用 Data Protector 用户界面选择要恢复的数据。

- 如果介质的编目保护已经过期，则 **Data Protector** 没有关于备份的数据的详细信息。通过手动指定要恢复的文件或目录恢复数据。

**提示：**

要在编目保护过期之后从介质重新读取有关文件和目录的详细信息，请导出介质然后再导入，并指定要读取的详细编目数据。在此之后，便可以在 **Data Protector** 用户界面中浏览文件和目录。

## Web 服务器还原

要还原 **Web** 服务器，请使用标准还原过程以还原文件、目录和客户机。此外，还需要考虑以下各项：

- 所有数据都应还原到原始位置。
- 应始终包括配置文件和根目录。
- 在还原期间，应关闭 **Web** 服务器，但是操作系统必须正常运行。在还原之后重新启动 **Web** 服务器。

如果 **Web** 服务器上含有 **Oracle** 或 **Informix Server** 等数据库，则要使用该数据库特有的还原过程。

## 还原而不浏览

当数据的编目保护已过期，或者使用不记录任何内容或记录目录选项执行了备份时，可以手动为恢复指定文件或目录。

如果不知道文件或目录名称，则可以还原整个对象，然后提取所需部分，也可以使用**仅还原**功能仅还原与特定模式匹配的文件，然后从中提取需要的部分。

## 还原整个对象和提取所需部分

在不能浏览要还原的文件或目录时，可以还原整个对象，然后仅提取需要的部分。

### 先决条件

要还原整个对象，需要一个与整个对象一样大的临时存储区。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要还原的数据的客户机系统，然后单击要还原的对象。
4. 单击**目标**选项卡。选择一个足够存储整个对象的临时目录。
5. 在其他还原属性页中指定选项，包括选择要使用的设备。
6. 在**操作**菜单中，如果希望预览，请单击**预览恢复**，如果要实际启动恢复过程，请单击**启动恢复**。
7. 在“启动会话”向导中，检查您的选择，并指定**报告级别**、**网络负载**和**启用可恢复的恢**

**复**选项。还原监视器可显示还原的进度。

8. 完成还原时，可以从还原的对象提取需要的数据部分，并且将它们复制到希望的位置。注意，此操作在 **Data Protector** 以外执行。

## 使用仅还原模式匹配还原部分备份对象

在不能浏览要还原的文件或目录时，可以使用模式匹配命中目录(或文件或更高级别的目录)，模式匹配可以避免还原最不需要的对象部分。通过使用通配符，可以指定要使用的模式。

**注意：**  
**Data Protector NDMP** 服务器集成不支持此功能。

### 先决条件

- 需要使用相当特定的模式定义，此功能才有效。
- 需要一个临时存储区域用于还原的部分。其大小取决于还原的对象部分的大小，这与使用的匹配模式的精度有关。

### 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要还原的数据的客户机系统，然后单击要还原的对象。
4. 在“源”属性页中，右键单击要从中还原的对象，然后单击**属性**。
5. 单击**仅恢复**选项卡，并在文本框中指定匹配要恢复的文件的模式(例如，“\*order\*40\*.ppt”)，然后单击**添加**。应添加若干这样的模式，以便尽可能准确地指定要还原文件的类型。
6. 单击**确定**。
7. 单击**目标**选项卡。选择足够大的临时目录，以便能够存储备份对象的各部分。
8. 在其他还原属性页中指定选项，包括选择要使用的设备。
9. 在**操作**菜单中，如果希望预览，请单击**预览恢复**，如果要实际启动恢复过程，请单击**启动恢复**。
10. 在“启动会话”向导中，检查您的选择，并指定报告级别、网络负载和启用可恢复的恢复选项。还原监视器可显示还原的进度。如果选择了“警告”报告级别，则 **Data Protector** 将发出警告消息，因为文件和目录的列表不在 IDB 编目中。这不影响还原。
11. 完成还原时，可以从还原的对象提取需要的数据部分，并将它们复制到希望的位置。注意，此操作在 **Data Protector** 以外执行。

## 手动还原文件或目录

在不能浏览要还原的文件或目录时，可以手动指定文件或目录。当数据的编目保护过期时，或使用**不记录任何内容**选项完成备份时会发生这种情况。

## 先决条件

要手动添加文件或目录，需要知道文件或目录的确切路径和名称。文件和路径名称区分大小写。

## 步骤

1. 在“上下文列表”中，单击**恢复**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要还原的数据的客户机系统，右键单击具有要手动还原的文件或目录的对象，然后单击**属性**。
4. 单击**还原摘要**选项卡，然后在文本框中输入路径的缺失部分和要还原的文件或目录的名称。
5. 单击**添加**以确认。将出现“版本”窗口。
6. 从“版本”下拉列表中，选择要还原的备份版本，然后单击**确定**。将显示对象名称和版本。
7. 在其他还原属性页中指定选项，包括选择要使用的设备。
8. 在**操作**菜单中，如果希望预览，请单击**预览恢复**，如果要实际启动恢复过程，请单击**启动恢复**。
9. 在“启动会话”向导中，检查您的选择，并指定**报告级别**、**网络负载**和**启用可恢复的恢复**选项。

还原监视器可显示还原的进度。如果选择了“警告”报告级别，则 **Data Protector** 将发出警告消息，因为文件和目录的列表不在 IDB 编目中。这不影响还原。

## 还原选项

**Data Protector** 提供一组全面的还原选项，可以使用这些选项对还原进行微调。所有这些选项具有在大多数情况下合适的默认值。

以下选项列表按每对象设置。还原选项根据要还原的数据类型提供。

有关还原选项的详细信息，请参见 **Data Protector** 帮助。

## 常规还原选项

- **显示完整链**。在还原链中显示所有文件和目录。默认情况下，选择此选项，并且还原整个还原链。
- **仅显示此会话**。仅显示此会话中备份的文件和目录。这使您可以从增量备份会话还原文件和目录，而非还原整个还原链。默认情况下，禁用此选项。
- **目标客户机**。默认情况下，还原到从中备份数据的同一客户机系统。可以从下拉列表中选择单元中的另一个系统。磁盘代理在所选客户机系统上启动，并在那里还原数据。

需要有**还原到其他客户机**用户权限才能还原到其他客户机系统。

- **忽略已删除的文件**。为了使此选项正常工作，**Cell Manager** 上的时间和数据所还原到的

系统上的时间必须同步。

如果选择了此选项，**Data Protector**将重新创建备份目录树在上次增量备份会话时的状态，同时保留在上次增量备份会话之后创建或修改的文件。在完整备份(定义还原链的初始会话)和所选增量备份之间删除的文件将被还原，并会在稍后的后续增量还原期间还原文件夹时被删除。

如果未选择此选项，则 **Data Protector** 还将还原完整备份映像中所包含的文件，以及在完整备份(定义还原链的初始会话)和所选增量备份之间被删除的文件。

当在启用了此选项的情况下使用**还原为**或**还原至**功能时，请谨慎选择还原位置，以防止意外删除现有文件。

默认：未选择。

- **移动繁忙文件。** 如果应用程序正在使用磁盘上的某个文件，当还原要替换此文件时，即与此选项相关。此选项仅适用于因应用程序或其他进程使用而被操作系统锁定的文件。此选项与**保持最新**或**覆盖**选项一起使用。

默认情况下，禁用此选项。

在 **UNIX** 系统中，**Data Protector**将繁忙文件从 **filename** 移至 **#filename**(在文件名前面添加井号)。应用程序将继续使用繁忙文件，直到其关闭该文件为止。随后，将使用还原的文件。

在 **Linux** 系统中，不支持此选项。

在 **Windows** 系统中，该文件还原为 **filename.001.**。所有应用程序都继续使用旧文件。重新引导系统后，旧文件将替换为还原的文件。

- **列出已还原的数据。** 在还原对象时，监视器窗口中将显示文件和目录的名称。默认情况下，禁用此选项。
- **显示统计信息。** 报告所备份或还原的每个对象的统计信息(如大小和性能)。可以在监视器窗口中查看这些信息。默认情况下，禁用此选项。
- **省略不需要的对象版本。** 如果选择目录进行还原，并且以日志记录级别**全部记录**或**记录文件**执行备份，则此选项适用。

如果已选择此选项，则 **Data Protector**在 **IDB** 中检查还原链中的每个备份是否有任何文件要还原。将跳过其中没有对象版本要还原的备份。请注意，此检查可能需要一些时间。

如果不选择此选项，则读取还原链中的每个备份，即使从上一次备份以来没有任何更改也是如此。

要还原空目录，请取消选中此选项。

默认：选择。

- **还原稀疏文件。** 以其原始压缩形式还原稀疏文件。这很重要，因为稀疏文件可以消耗其他磁盘空间，除非以其原始形式还原它们。默认情况下，禁用此选项。  
此选项仅应用于 **UNIX** 稀疏文件。**Windows** 稀疏文件始终还原为稀疏。
- **在还原期间锁定文件。** 在还原期间拒绝访问文件。默认情况下，禁用此选项。
- **还原时间属性。** 保留每个所还原文件的时间属性值。禁用此选项时，**Data Protector**将所还原对象的时间属性设置为当前日期和时间。默认情况下，启用此选项。
- **还原保护属性。** 保留每个所还原文件的原始保护属性。如果禁用此选项，则 **Data Protector**应用当前还原会话的保护属性。默认情况下，启用此选项。

在 **Windows** 系统上，此选项仅应用于文件属性。始终还原安全信息，即使禁用此选项时也如此。

- **还原目录的共享信息。** 指定将还原目录的共享信息。默认情况下，选择此选项。  
还原备份目录时网络上共享的目录时，如果选择此选项，则在还原之后，还将共享目录(前提是创建备份时选择了**备份目录的共享信息**选项)。

## pre-exec 和 post-exec 命令

- **Pre-exec。** 可以输入一个要在启动每个对象的还原之前执行的命令(或脚本)。此命令(或脚本)必须返回成功，Data Protector 才能进行还原。  
在运行磁盘代理的客户机系统上执行 pre-exec 命令(或脚本)。在 Windows 系统上，脚本必须位于 `Data_Protector_home\bin` 目录或其子目录中。在 Unix 系统上，脚本必须位于 `/opt/omni/libin` 目录或其子目录中。  
请注意，Windows 系统中仅支持扩展名为 `.bat`、`.exe` 和 `.cmd` 的 pre-exec 脚本。要运行具有不受支持扩展名(例如 `.vbs`)的 pre-exec 脚本，请创建批处理文件(`.bat`)以启动该脚本。然后配置 Data Protector，将批处理文件作为 pre-exec 命令运行，该批处理文件随后启动扩展名不受支持的脚本。
- **Post-exec。** 可以输入一个要在完成每个对象的还原之后执行的命令(或脚本)。在运行磁盘代理的客户机系统上执行 post-exec 命令(或脚本)。

## 设备选择

- **自动选择设备。** 当没有原始设备可供还原或对象副本使用时适用。选择此选项可使 Data Protector 能够自动将不可用的设备替换为针对还原或对象副本选择的、并且设备标记与原始设备相同的其他设备。如果没有足够的设备可供替换原始设备，则启动还原或对象副本时设备将少于备份期间使用的设备。  
默认情况下，Data Protector 首先尝试使用原始设备。如果未选择原始设备用于还原或对象副本，则考虑全局选项。要优先使用备用设备或干脆不用原始设备，请修改全局选项 `AutomaticDeviceSelectionOrder`。  
对于 Data Protector SAP MaxDB、DB2 UDB、Microsoft SQL Server 和 Microsoft SharePoint Server 2007/2010/2013 集成，请确保可用设备数等于或大于备份期间所用的设备数。  
默认：选择。
- **原始设备选择。** 当目前没有原始设备可供还原或对象副本使用时适用。选择此选项可指示 Data Protector 等待所选设备变为可用。  
这是 Data Protector SAP MaxDB、IBM DB2 UDB、Microsoft SQL Server 和 Microsoft SharePoint Server 2007/2010/2013 集成的首选选项。  
默认：未选择。

## 处理文件冲突

- **保留最新文件。** 如果选择了此选项，则保持文件的版本最新。如果磁盘上的文件比备份的版本新，则不还原文件。如果磁盘上的文件比备份的版本旧，则用备份中的较新版本覆盖该文件。默认情况下，启用此选项。
- **没有覆盖。** 如果选择了此选项，则保留磁盘上存在的文件。这意味着它们不会被备份中这些文件的其他版本覆盖。仅从备份还原当前不存在的文件。默认情况下，禁用此选项。
- **覆盖。** 如果选择了此选项，则将磁盘上的现有文件将替换为备份中的文件。默认情况下，禁用此选项。

## Active Directory 特有选项

### 复制模式

- **权威。** 这是 Windows Server 特有的一个选项，用于处理 Active Directory 还原。还原之后不更新 Active Directory 数据库，并且还原的数据将覆盖目标中的现有数据。只有在还原会话完成之后通过从命令提示符下运行 `ntdsutil.exe` 才能执行权威还原。
- **非权威。** 在使用标准复制技术还原之后更新 Active Directory 数据库。非权威复制模式是默认选项。
- **主。** “主”复制模式可使 NT 目录服务联机，并用于还原 FileRepllicationService 以及 Active Directory 服务。复制共享的所有复制合作伙伴丢失时，必须使用此选项。对于证书服务器和 Active Directory 服务器，主与权威作用相同。

### 设置还原选项

在选择要还原的数据之后，可以设置还原选项。还原选项具有在大多数情况下合适的默认值。这些选项根据要还原的数据类型提供。例如，对文件系统还原提供所有还原选项，但对磁盘映像还原不提供。

### 步骤

1. 在上下文列表中，单击**还原**。
2. 在“范围窗格”中的“恢复对象”下，展开合适的数据类型(例如，**文件系统**)。
3. 展开具有要还原的数据的客户机系统，然后单击具有该数据的对象(UNIX 系统上的装载点，Windows 系统上的驱动器)。
4. 在“源”属性页中，选择要还原的数据。
5. 单击**选项**选项卡以打开“选项”属性页。通过单击选项旁边的框可以选中或取消选中相应的选项。

## 关于 Windows 系统还原

在还原 Windows 文件系统时，Data Protector 将还原文件和目录中的数据，以及有关文件和目录的特定于 Windows 的信息。

还原以下特定于 Windows 的信息：

- 完整 Unicode 文件名
- FAT16、FAT32、VFAT  
NTFS 属性
- 多组备用数据流。
- 共享信息



如果在备份期间目录在网络上共享，则在备份介质上存储共享信息。默认情况下，还原之后目录将在网络上共享，除非已经存在具有相同共享名称的共享目录。要防止恢复正在恢复的目录的共享信息，请取消选中恢复目录的共享信息选项。

“文件冲突处理”选项也适用于目录共享信息的还原。例如，如果为恢复使用了没有覆盖恢复选项，将保留磁盘上存在的目录的目录共享信息。

- NTFS 备用数据流
- NTFS 安全数据

### NTFS 3.1 文件系统功能

- NTFS 3.1 文件系统支持重新分析点  
卷装入点、单实例存储 (SIS) 和目录联接都基于重解析点这个概念。这些重解析点被选为任何其他文件系统对象。
- NTFS 3.1 文件系统支持符号链接，此概念随 Windows Vista 和 Windows Server 2008 操作系统引入。

Data Protector 以处理 NTFS 重新分析点的方式处理符号链接。

- NTFS 3.1 文件系统支持稀疏文件，这是减少磁盘空间分配量的一种高效方式。  
以稀疏方式备份这些文件可节省磁带空间。备份稀疏文件后，只能向 NTFS 3.1 文件系统以稀疏方式还原这些文件。
- 某些 NTFS 3.1 特有的功能由保留自身数据记录的系统服务控制。将这些数据结构作为 CONFIGURATION 的一部分进行备份。
- 加密的文件  
对于由 Microsoft 加密的 NTFS 3.1 文件均采用加密方式进行备份和还原，但只有在将这些文件解密后才能正确查看其内容。
- 压缩文件以压缩格式备份和还原。

在还原到与执行备份时不同的文件系统类型时，请考虑文件系统还原限制。

### 还原备份为共享磁盘的对象

备份为共享磁盘的对象与用于备份它们的磁带客户机关联。如果环境没有改变，则可以像本地 Windows 文件系统一样还原共享磁盘。默认情况下，使用备份共享磁盘时所用的同一磁带客户机将数据还原到原始位置。

### Windows 文件系统还原限制

可以将数据还原到与执行备份时不同的文件系统类型。

开始	结束				
	FAT32	FAT16	CDFS	UDF	NTFS

					3.1 <sup>1</sup>
FAT32	FC	FC	不适用	不适用	FC
FAT16	FC	FC	不适用	不适用	FC
CDFS	FC	FC	不适用	不适用	FC
UDF	FC	FC	不适用	不适用	FC
NTFS 3.1 <sup>2</sup>	*	*	不适用	不适用	FC

图例	
FC	完全兼容。保留整个文件属性。
*	不还原重解析点、稀疏文件和加密的文件。还原的文件不带安全信息和备用数据流。

该表显示了 NTFS 3.1.x 文件系统对象只能足以还原到 NTFS 3.1 文件系统。还原到不同文件系统版本时，将丢失特定于文件系统的属性和备用数据流。

- Windows 重解析点(如目录连接或卷装载点)只能还原到 NTFS 3.1 文件系统。UNIX 重解析点无法还原到 NTFS 3.1 文件系统。
- 还原包含 SIS 重解析点的 NTFS 3.1 文件系统时，可能发生磁盘已满的情况。如果将原始文件还原到可能占用更多可用空间的多个目标文件，则会发生此情况。
- 只能以稀疏方式向 NTFS 3.1 文件系统还原稀疏文件。
- 用户磁盘配额无法使用 Data Protector 还原。
- 如果用户尝试将稀疏文件还原到非 NTFS 3.1 文件系统，则 Data Protector 将发出警告。还原到除 NTFS 3.1 以外的文件系统的稀疏文件不包括零部分。
- Microsoft 加密的 NTFS 3.1 文件只能还原到 NTFS 3.1 文件系统，因为其他文件系统驱动程序无法解密它们。

## 配置还原

要恢复 Windows CONFIGURATION，请选择 CONFIGURATION 对象或它的某些部分，并遵循标准恢复过程进行恢复。

CONFIGURATION 由影响系统操作的数据结构组成。因此，必须为此类还原准备系统。先决条件取决于 CONFIGURATION 项目的内容和 Windows 操作系统版本。

<sup>1</sup> 它在 Windows XP、Windows Vista、Windows 7、Windows 8、Windows Server 2003、Windows Server 2008 和 Windows Server 2012 上使用。  
<sup>2</sup> 它在 Windows XP、Windows Vista、Windows 7、Windows 8、Windows Server 2003、Windows Server 2008 和 Windows Server 2012 上使用。

## 限制

- 应成对还原 Active Directory 服务和 SysVol。
- 用户磁盘配额无法使用 Data Protector 还原。备份的信息可以使用 Microsoft 实用工具手动还原。
- 尽管 Data Protector 允许您恢复单个配置对象，但**建议不要**这样做。强烈建议您将完整配置恢复作为**灾难恢复**过程的一部分执行。

## Windows 配置对象

有关配置对象的更多详细信息，请参见 Data Protector 帮助。

- Active Directory 服务
- 证书服务器
- COM+ 类注册数据库 (ComPlusDatabase)
- DFS
- DHCP
- DNS 服务器
- 事件日志
- 文件复制服务
- Internet Information Server (IIS)
- 用户配置文件 (Documents and Settings)
- Windows 注册表
- Removable Storage Management Database
- SystemRecoveryData
- SysVol
- 终端服务数据库
- 用户磁盘配额 (QuotaInformation)
- WINS 服务器

在完成整个 CONFIGURATION 对象的还原之后重新启动系统，以便让还原的数据生效。

某些对象有一些特殊注意事项和任务。

## Active Directory

要还原 Active Directory 服务，必须使用目录服务还原模式启动选项重新启动系统。在目录服务还原模式下启动系统时，无法使用域用户帐户。必须配置 Data Protector Inet 和 crs 服务(用于 Cell Manager)才能使用本地系统帐户登录，然后重新启动服务。还原 Active Directory 时，还会还原文件复制服务 (FRS) 和分布式文件系统(Distributed File System, DFS)。

可以通过以下三种复制模式之一还原 Active Directory(Windows 特有选项):

- 非权威
- 权威
- 主

**注意：**

要执行**权威**恢复，还需要在完成恢复会话之后运行 `ntdsutil.exe`。例如，要执行典型权威恢复，请在命令提示符下输入 `ntdsutil`，然后输入 `authoritative restore`，然后恢复数据库。重新启动服务器，并等待复制发生。

**提示：**

还可以创建 `post-exec` 命令来执行 Active Directory 权威恢复所需的其他操作。例如，要执行整个目录的权威还原，请使用以下行：

```
ntdsutil "popups off" "authoritative restore" "restore database" quit quit
```

## DFS

Data Protector 将 Windows 分布式文件系统(Distributed File System, DFS)还原为以下某项的一部分：

- Windows 注册表(如果以独立模式配置 DFS)
- Windows Active Directory(如果以域模式配置 DFS)

## 配置文件

- 如果各个用户以交互方式或作为服务登录，则无法成功还原用户配置文件。如果用户在恢复时登录，则 **Data Protector** 将无法恢复包含用户的注册表配置单元的文件 `NTUSER.DAT`。

必须注销系统，并停止在要还原其配置文件的用户帐户下运行的所有服务。可以从其他系统或者作为不同用户在还原目标系统上登录来启动还原会话。

- 要一次性还原所有用户配置文件，则必须停止未在本地系统帐户下运行的任何服务，并从系统中注销。然后在另一个客户机上使用 **Data Protector GUI** 远程启动还原会话。
- 只有在系统上已经定义了用户配置文件的位置时，才可以还原用户配置文件。只要系统的配置文件中存在现有用户配置文件或删除的配置文件的个别文件，就可以还原它们。如果从控制面板中删除了用户配置文件，或者出于某种其他原因，系统上不再有用户配置文件，则还原将失败，并显示以下错误：

[84:208] Configuration object not recognized by the system => not restored.

要还原此类用户配置文件，必须作为该用户登录并首先重新创建该配置文件。系统为用户的配置文件分配一个目录，并创建一个默认配置文件。要保持还原的文件不被合并，可以在运行还原会话之前删除最近创建的配置文件中的文件。然后注销，并作为其他用户或使用其他系统进行登录来启动还原会话。系统可能为用户分配不同的名称。在此情况下，可以使用**还原为**选项，将文件恢复到最近分配的位置。

- 在还原用户配置文件时，始终会覆盖文件，不管还原规范中的“文件冲突处理”选项如何。而且，**忽略已删除的文件**选项不可用。在磁盘上存在但在备份时不显示的文件还原之后将保留在用户配置文件中。
- 还可以使用**恢复为**选项恢复用户配置文件。可以指定文件的临时位置，然后将希望的文件手动复制到用户的配置文件目录。也可以通过用户的配置文件目录直接恢复，这

可能需要使用**移动繁忙文件**选项，使用此选项可以恢复用户配置文件，即使登录用户正在使用该文件也可以恢复。不过，请注意，在此情况下，正在使用的文件只有在重新启动系统之后才会被替换。

## 注册表

如果选择整个 Windows Registry 进行恢复，则在恢复期间不会恢复某些注册表项，并会以特殊方式对待这些项。这是因为这些项由操作系统使用。可以在以下注册表项下找到它们：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\KeysNotToRestore

## 可移动存储管理器数据库

RSM 服务必须在连接可移动存储设备(CD-ROM 除外)的所有系统上运行。

## 服务器配置对象

目标系统必须安装并运行各自的服务器。对于除证书服务器以外的所有服务器，将联机还原数据。

证书服务器的数据以脱机方式还原。在启动还原之前，停止证书服务器的服务。可以仅使用权威模式恢复证书服务器。

## SysVol

可以通过以下三种模式之一执行 SysVol 目录的还原：

- 非权威  
如果域中至少有一个域控制器可用并且正常运行，则文件将还原到其原始位置。还原的数据不传播到其他域控制器。
- 权威  
如果从本地域控制器删除了关键 SysVol 数据并且将删除传播到了其他域控制器，则执行权威还原。
- 主  
如果域中的所有域控制器丢失并且要从备份重建域控制器，则会通知 FRS 还原主文件，并将文件还原到其原始位置。

## Windows TCP/IP 服务

在运行 Microsoft TCP/IP 协议并配置为 WINS 服务器、DHCP 服务器或 DNS 服务器的 Windows 系统上，可以还原管理网络通信的服务。

要恢复 Windows TCP/IP 服务，请展开 CONFIGURATION 项目，并选择 WINS、DHCP 或 DNSServerDatabase。

在还原之前会自动停止所有这些服务。

在完成还原时，重新启动系统。

## 系统状态数据还原

如果使用 **Active Directory**(此目录始终是系统状态的一部分)，必须在目录服务还原模式下启动系统。

从 **Data Protector** 角度看，系统状态由一些特定文件系统对象和 **CONFIGURATION** 对象组成。在 **Windows Vista**、**Windows 7**、**Windows 8**、**Windows Server 2008** 和 **Windows Server 2012** 中，系统状态还包括属于可安装的其他服务器角色或服务的数据。与在备份向导中选择对象相反，用于还原的不同对象在单独的还原向导中选择。

在“源”属性页中，选择：

- 属于 **CONFIGURATION** 的系统状态对象：
  - **ActiveDirectoryService**
  - **CertificateServer**
  - **Cluster Service information**
  - **IIS Metadirectory**
  - **RemoteStorageService**
  - **RemovableStorageManagementDatabase**
  - **SystemFileProtection**
  - **SYSVOL directory**
  - **TerminalServiceDatabase**
- **SystemVolumeInformation** (包括系统文件保护服务)
- 启动文件(它们位于系统驱动器上)
- 数据属于特定服务器角色或服务驻留的卷甚至整个客户机系统(对于 **Windows Vista**、**Windows 7**、**Windows 8**、**Windows Server 2008** 和 **Windows Server 2012**)

在完成还原时，重新启动系统。

## 远程存储服务

远程存储服务 (**RSS**) 用于自动将不常访问的文件从本地移至远程存储。打开此类文件时，将自动检索远程文件。

尽管 **RSS** 数据库是系统状态数据的一部分，但要手动还原这些数据库。必须脱机还原 **RSS** 数据库。可以提供 **pre-exec** 和 **post-exec** 脚本来停止和重新启动该服务，或在还原前后分别手动停止并重新启动该服务。

选择以下还原目录：

`%SystemRoot%\system32\RemoteStorage`

`%SystemRoot%\system32\NtmsData`

## 系统文件保护

重新启动计算机之后，系统文件保护服务扫描并验证所有受保护系统文件的版本。如果系统文件保护服务发现受保护文件被覆盖，则该服务将检索文件的正确版本，然后替换错误的文件。通过 **Data Protector**，可以备份并恢复受保护文件，以使其不被覆盖。

## 关于 UNIX 系统还原

在将文件从执行备份的位置还原到原始位置时，**Data Protector** 将还原文件，并包括文件属性。

系统特有数据，如 UNIX 系统上的 ACL(访问控制列表)仅还原到从中进行备份的相同文件系统类型和操作系统。

## UNIX 系统特有信息

在恢复 VxFS 数据时，使用恢复为选项，并将其恢复到所需的位置。

## 关于 HP OpenVMS 系统还原

使用标准还原过程可以还原 HP OpenVMS 文件系统。

## 限制

- 对于在任何其他操作系统平台上保存的文件和目录，并非可以还原所有文件属性，在此情况下也不会还原 ACL。
- 在还原期间创建但尚未包括在存储中的目录将获取在目录中还原的第一个文件的属性，除非使用 `-no_protection` 选项禁用。
- 任何输入到 GUI 中或传递到 CLI 的文件规范都必须采用 UNIX 样式语法

`/disk/directory1/directory2/filename.ext.n`

字符串应当以斜线开头，后跟磁盘、目录和文件名，其间以斜线分隔。

请勿在磁盘名称后加冒号。

版本号前应使用句号而非分号。

OpenVMS 文件的文件规范不区分大小写。例如，OpenVMS 文件规范

`$1$DGA100:[USERS.DOE]LOGIN.COM';1`

必须按以下形式指定：

`/$1$DGA100/Users/Doe/Login.Com.1`

- 没有隐式版本号。必须始终指定版本号。仅还原被选择进行还原的文件版本。如果要包括文件的所有版本，请在 GUI 窗口中进行选择，或者使用 CLI 在 **仅有 (-only)** 选项下包括文件规范，其中包括版本号通配符，如下所示：

`/DKA1/dir1/filename.txt.*`

- 如果还原到原始位置以外的位置，则仅更改磁盘设备和启动目录。原始目录路径被添加到目标路径，形成新的还原位置。

- 如果在还原期间禁用了**还原时间属性** (-notouch)选项，则将用 ODS-5 磁盘上的当前日期和时间更新上次访问日期。在 ODS-2 磁盘上，原始日期会保留在文件中。
- 另存为软链接的文件将使用等效的 DCL SET FILE/ENTER 命令还原。在此情况下不会还原任何数据。输入的软链接指向保存此文件时的主路径/文件名。如果主路径/文件名不存在或未还原，则软链接的创建将失败。

要制作 OpenVMS 可引导系统磁盘的还原副本，必须在还原磁盘之后使用 OpenVMS WRITEBOOT 实用程序写入引导块。

- 在 OpenVMS 上不能使用**移动繁忙文件** (-move)和**还原稀疏文件** (-sparse)选项。
- 从 OpenVMS 系统上的 ODS-5 磁盘备份的具有扩展文件系统名(即大小写字母、Unicode 字符等)的文件可能无法还原到 ODS-2 磁盘。
- 无论启用还是禁用了**在还原期间锁定文件** (-lock)选项，始终会锁定要还原的文件。
- pre-exec 和 post-exec 命令过程的默认设备和目录是 /omni\$root/bin。要在任何其他地方放置命令过程，文件规范所包含的设备和目录路径必须采用 UNIX 样式格式。例如：  
/SYS\$MANAGER/DP\_SAVE1.COM
- 如果禁用了**还原保护属性** (-no\_protection)选项，则使用默认的所有者、保护和 ACL 创建文件。
- 为**跳过** (-skip)或**仅有** (-only)过滤器指定通配符时，使用“\*”代表多个字符，使用“?”代表单个字符。
- 在 OpenVMS 系统上，Data Protector 不支持卷和卷集上的磁盘配额。

要对启用磁盘配额的卷上的数据执行还原，请配置 post-exec 脚本，以便在开始还原之前在涉及的卷上禁用磁盘配额，并配置 pre-exec 脚本，以便在完成还原之后启用磁盘配额。

## 文件系统信息还原

目录结构和文件与以下文件系统信息一并进行还原：

- 文件和目录属性
- ACL(访问控制列表)，如果可用(参见“限制”)
- 辅助文件条目

在 OpenVMS 文件系统备份期间，具有多个目录条目的文件将使用主路径名称备份一次。辅助路径条目保存为软链接。

例如，OpenVMS 系统磁盘上系统特定根具有另存为软链接的 SYSCOMMON.DIR;1 路径。此路径的数据将保存在 [VMS\$COMMON...] 下。

在文件系统还原期间，将还原这些额外的路径条目。

只能将文件还原到已装载的 FILES-11、ODS-2 或 ODS-5 卷。



# 第 15 章：监控、报告、通知和 Data Protector 事件日志

## 关于监视

通过 **Data Protector** 监视，可以管理正在运行的会话以及答复装载请求。可以查看会话的状态、其类型、所有者和会话 ID；会话的开始时间以及相应备份规范的名称。

运行交互式备份、还原、对象复制、对象合并、对象验证或介质管理会话时将打开一个监视窗口，其中显示对象、备份设备和会话期间生成的消息。即使关闭用户界面，会话也仍在继续。

通过在配置备份规范期间或启动还原会话期间更改**报告级别**选项，可以更改在备份或还原会话期间报告消息的级别。

可以使用管理器的管理器功能同时监视多个单元。

## 查看当前正在运行的会话

可以在“监视”上下文中查看当前正在运行的会话。

### 注意：

**pre-exec** 脚本执行完毕之后，在“监视”上下文中显示当前正在运行的会话。

到达刷新闻隔(默认情况下 5 秒)后，即自动用新会话更新当前正在运行的会话的列表。要更改默认刷新闻隔，请在“文件”菜单中单击**首选项**，然后单击“监视”选项卡。可以为 **Cell Manager** 和 **MoM** 指定刷新闻隔(以秒计)。

## 先决条件

您必须已经添加到 **Admin** 用户组中，或者获得了“监视”用户权限。

## 步骤

1. 在上下文列表中，单击**监视**。  
在结果区域中显示当前会话的状态。

### 提示：

通过单击相应的列标题，可以对会话进行排序(按 **status**、**type**、**owner** 等等)。对于 **VMware** 集成，还可以按 **VM name** 和 **item name** 对会话进行排序。这里，**VM name** 指 **vCenter** 中虚拟机的名称，**item name** 指与虚拟机相关的磁盘对象或配置的名称。

2. 双击要查看的正在运行的会话。

### 提示：

要从“监视”上下文的结果区域中删除所有完成或中止的会话，请在范围窗格中单击**当前会话**，然后从“操作”菜单中选择**清除会话**。要从当前会话列表中删除特定的完成或中止的会话，请右键单击该会话，然后选择**从列表中删除**。如果重新启动 **Data Protector GUI**，

将从“监视”上下文的的结果区域中自动删除所有完成或中止的会话。

## 查看完成的会话

可以在“内部数据库”上下文中查看完成或中止的会话。

### 先决条件

您必须已经添加到 **Admin** 用户组中，或者获得了“监视”用户权限。

### 步骤

1. 在上下文列表中，单击**内部数据库**。  
如果正在运行 **Manager-of-Managers**，则在上下文列表中选择**监视**，然后选择您所选的 **Cell Manager**。从“工具”菜单中选择**数据库管理**，从而打开一个选择新 **Data Protector** GUI，并显示“内部数据库”上下文。
2. 在范围窗格中，展开**会话**以显示 IDB 中存储的所有会话。此时会话将按日期排序。每个会话都由会话 ID 标识，此标识由 YY/MM/DD 格式的日期和唯一编号组成。
3. 右键单击会话，然后选择**属性**，以查看有关特定会话的详细信息。
4. 单击**常规**、**消息**或**介质**选项卡，以分别显示有关会话、会话消息的常规信息或有关此会话所用介质的信息。

## 中止正在运行的会话

如果要停止备份、还原或介质管理操作，则中止会话。仅对中止会话之前备份或还原的数据存在备份副本或还原的数据。

### 先决条件

您必须已加入 **admin** 用户组中，或者获授了“监控”用户权限。

### 步骤

1. 在上下文列表中，单击**监视**。此时将在结果区域中显示当前会话的进度和状态。  
如果正在运行管理器的管理器，展开范围窗格中的**企业监控器**，然后选择要监视的 **Cell Manager**。此时将在结果区域中显示当前会话的进度和状态。
2. 单击列标题可对会话进行排序。
3. 右键单击会话，然后选择**中止**。

如果在中止备份会话时该会话仍在确定您选择进行备份的磁盘大小，则不会立即中止该会话。确定大小(树遍历)后即中止备份。

#### 提示：

如果以交互方式启动了备份、恢复或介质管理会话，则还可以分别在 **Data Protector**“备份”、“恢复”或“设备和介质”上下文中中止相应的会话。

## 关于报告

Data Protector 报告提供有关备份环境的各种信息。例如，可以检查上一次备份、对象复制、对象合并或对象验证的状态，检查网络中的哪些系统没有针对备份进行过配置，检查介质池中介质的使用量，检查设备的状态等等。

可以使用 Data Protector GUI 或任何支持 Java 的 Web 浏览器配置报告和报告组。通过报告组可以方便地管理报告，计划报告组中的报告，以及定义将报告划分到报告组中所采用的标准。

通过参数可以自定义报告。通过某些参数可实现多种选择。如果在配置报告时未指定任何可选的输入参数(可选选择)，则设置默认值，对于对象为 *all*，对于时间范围为 *no time limit*。要配置报告或报告组，需要提供：

- 报告的名称
- 报告的类型
- 发送方法
- 接收方
- 格式

所有其他输入参数(选择)取决于报告的类型。

### 注意：

默认情况下启用 VADP Reporting 功能。要禁用它，请将 `EnableDPAforVM` 全局变量设置为 0。

## 功能

- 可以在报告组中收集各种报告(可按通知计划、交互式启动或触发)。
- 可使用以下各项启动报告：Data Protector GUI、Data Protector CLI、Data Protector 计划程序、通知事件或包括用于启动报告的 Data Protector CLI 命令的 `post-exec` 脚本。
- 使用管理器的管理器 (MoM) 功能时，多单元配置也可使用报告。
- 以多种格式提供报告的输出，并且(可选)还可以显示输入参数(选择)。

## 报告格式

可以生成多种格式的 Data Protector 报告。

如果单独启动每个报告，则在 Data Protector Manager 中显示报告，并且不必选择报告格式。

如果将报告集中到报告组中，则必须指定每个报告的格式和收件人。

可以从以下报告格式中进行选择：

- **ASCII** - 以纯文本生成报告。
- **HTML** - 以 HTML 格式生成报告。此格式对使用 Web 浏览器进行查看很有用。例如，通过单击链接和查看 Intranet 上的报告，可以检查系统是否已经过备份。

- **Short** - 以纯文本生成报告，仅以摘要形式显示最重要的信息。对于广播消息建议采用此格式。
- **Tab** - 以制表符分隔字段的形式生成报告。如果计划将报告导入其他应用程序或脚本中做进一步分析(如 **Microsoft Excel**)，则此格式很有用。

报告的实际输出因所选格式而异。仅 **Tab** 格式显示所有报告的所有字段，而其他格式有时可能仅显示所选字段。

## 报告类型

根据有关要检索的备份环境的信息，可以生成各种类型的报告：

### 配置报告

配置报告提供 **Data Protector** 单元的配置、不用于备份的设备、未针对备份配置的系统等的相关信息。

### 单元信息

说明：	<p>列出与 <b>Data Protector</b> 单元相关的信息(客户机数、备份规范、介质管理服务器、许可服务器)。</p> <p><b>Data Protector 8.14</b> 中引入的 <b>VADP</b> 功能可提供虚拟机的增强型报告。<b>VMware</b> 虚拟机表示为 <b>Data Protector</b> 客户机，它们称为 <b>VADP</b> 客户机。<b>VADP</b> 客户机显示有关虚拟机来宾操作系统的信息。如果 <b>VM</b> 工具已安装并且正在运行，且 <b>VM</b> 已开启，输出的主机信息部分显示操作系统、<b>IP</b> 地址或主机名等信息。</p> <p>如果已在虚拟机配置，<b>VM</b> 主机名必须显示 <b>DNS</b> 名称。</p> <p>如果 <b>VM</b> 没有 <b>DNS</b> 名称且 <b>IPv4</b> 可用，<b>VM</b> 主机名必须显示 <b>IP</b> 地址。</p> <p>如果 <b>DNS</b> 名称或 <b>IP</b> 地址不可用(或者)如果 <b>VM</b> 只有 <b>IPv6</b> 地址，<b>VM</b> 主机名必须显示 <b>VM</b> 名称。</p>
必要选择：	无
可选选择：	无
支持的格式：	所有格式
<b>omnirpt</b> 选项：	<b>cell_info</b>

### 客户机备份

说明：	<p>列出有关指定客户机的信息，如：未配置的文件系统、所有对象、包含有效备份的所有对象及其备份次数和平均大小。</p> <p>注意，客户机备份报告不包括有关应用程序集成备份对象和备份</p>
-----	---

	规范的信息。
必要选择：	主机名
可选选择：	无
支持的格式：	所有格式
<i>omnirpt</i> 选项：	host

## 不是为 **Data Protector** 配置的客户机

### 注意：

根据网络状况，生成此报告可能需要一些时间。无法中止此类型的报告。

说明：	列出所选域中并非当前单元一部分的客户机。
必要选择：	网络范围
可选选择：	无
支持的格式：	所有格式
<i>omnirpt</i> 选项：	hosts_not_conf

## 所配置的不由 **Data Protector** 使用的客户机

说明：	列出不用于备份且未配置任何设备的所有已配置客户机。
必要选择：	无
可选选择：	无
支持的格式：	所有格式
<i>omnirpt</i> 选项：	hosts_unused

## 所配置的不由 **Data Protector** 使用的设备

Description:	列出完全不用于备份、对象副本或对象合并的已配置目标设备。
必要选择：	无
可选选择：	无
支持的格式：	所有格式
<i>omnirpt</i> 选项：	dev_unused

## 许可

说明：	列出所有许可证和可用许可证数。
必要选择：	无
可选选择：	无
支持的格式：	所有格式
<i>omnirpt</i> 选项：	licensing

## 查找计划

说明：	列出安排在指定天数后启动的所有备份、对象副本、对象合并或验证规范，最多提前一年。
必要选择：	天数
可选选择：	无
支持的格式：	所有格式
<i>omnirpt</i> 选项：	lookup_sch

## IDB 报告

IDB 报告提供 IDB 大小的相关信息。

### IDB 大小

说明：	提供一个表，其中包含介质管理数据库、编目数据库、归档日志文件、数据文件、详细编目二进制文件目录的统计信息、SMBF (msg 目录)和 IDB 磁盘空间不足的相关信息。
必要选择：	无
可选选择：	无
支持的格式：	所有格式
<i>omnirpt</i> 选项：	db_size

#### 重要：

此报告中的**已使用**列显示每个 IDB 部分已用项目所占的百分比。此数字的计算方法是当前的项目数除以特定 IDB 部分的最大项目数(以百分比为单位)。如果项目数没有限制，则此数字永远是 0%。

若要了解 IDB 的特定部分是否空间不足，可以另外配置 IDB 空间不足通知。

## 池和介质报告

池和介质报告提供有关介质池和所用介质的信息。

### 介质的扩展列表

说明:	列出所有符合指定搜索标准的介质。对于每个介质，其中提供介质 ID、介质标签、介质位置、介质状态、介质保护、已用空间和总空间 (MB)、上次访问介质的时间、介质池和介质类型、已使用介质进行备份的会话规范、对象复制或对象合并以及会话类型和子类型的相关信息。
必要选择:	无
可选选择:	会话规范、备份规范组、说明、位置、池名称、介质类型(DDS、DLT 等等)、状况、到期、时间范围、库设备
支持的格式:	所有格式
omnirpt 选项:	media_list_extended

### 介质列表

说明:	列出所有符合指定搜索标准的介质。对于每个介质，其中提供介质 ID、介质标签、介质位置、介质状态、介质保护、已用空间和总空间 (MB)、上次访问介质的时间、介质池和介质类型的相关信息。
必要选择:	无
可选选择:	说明、位置、池名称、介质类型(DDS、DLT 等等)、状况、到期、时间范围、库设备
支持的格式:	所有格式
omnirpt 选项:	media_list

### 池列表

说明:	列出所有符合指定搜索标准的池。对于每个池，其中提供池名称、说明、介质类型、介质总数、包含受保护数据的已满介质和可追加的介质数量、包含不受保护数据的空闲介质数、差、中等和良好介质数的相关信息。
必要选择:	无
可选选择:	池名称、位置、介质类型(DDS、DLT 等等)、库设备、时间范围

支持的格式：	所有格式
omnirpt 选项：	pool_list

## 介质统计信息

说明：	报告有关符合搜索标准的介质的统计信息。其中提供以下信息：介质数；暂存介质数；受保护、良好、中等和差介质数；可追加介质数；介质上的总空间、已用空间和可用空间。
必要选择：	无
可选选择：	说明、位置、池名称、介质类型(DDS、DLT 等等)、状况、状态、过期、时间范围、库设备
支持的格式：	所有格式
omnirpt 选项：	media_statistics

## 会话规范报告

会话规范报告提供有关备份、对象复制、对象合并或对象验证的信息，如所备份对象的平均大小、会话的日程、未针对备份配置的文件系统等。

### 平均备份对象大小

说明：	<p>显示指定备份规范中对象的平均大小。它显示对象的完整和增量备份的大小。</p> <p>Data Protector 8.14 中引入的 VADP 功能可提供虚拟机的增强型报告。VMware 虚拟机表示为 Data Protector 客户机，它们称为 VADP 客户机。VADP 客户机的新对象名称格式如下：</p> <p>&lt;hostname&gt;:/&lt;vCenter&gt;/&lt;path&gt;/&lt;vmname&gt; [&lt;UUID&gt;]</p> <p>此处，&lt;hostname&gt; 是来宾虚拟机的 DNS。如果 DNS 名称未知，则使用 IP 地址或 VM 名称。</p>
必要选择：	无
可选选择：	备份规范、备份规范组、天数(从启动报告开始倒着计算)
支持的格式：	所有格式
omnirpt 选项：	obj_avesize

### 未针对备份配置的文件系统

说明：	列出任何所选备份规范中均未配置的所有磁盘(文件系统)。
-----	-----------------------------



必要选择：	无
可选选择：	备份规范、备份规范组
支持的格式：	所有格式
omnirpt 选项：	fs_not_conf

## 对象的最新备份

说明：	<p>列出 IDB 中的所有对象。对于每个对象，显示上一次完整备份和上一次增量备份时间、上一次完整对象副本和上一次增量对象复制时间以及上一次对象合并时间。</p> <p>Data Protector 8.14 中引入的 VADP 功能可提供虚拟机的增强型报告。VMware 虚拟机表示为 Data Protector 客户机，它们称为 VADP 客户机。VADP 客户机的新对象名称格式如下：</p> <p>&lt;hostname&gt;:/&lt;vCenter&gt;/&lt;path&gt;/&lt;vmname&gt; [&lt;UUID&gt;]</p> <p>此处，&lt;hostname&gt; 是来宾虚拟机的 DNS 名称。如果 DNS 名称未知，则使用 IP 地址或 VM 名称。</p> <p>可以使用备份规范筛选器和/或对象创建时间筛选器缩小所列出的对象的范围(请参见 Optional Selections)。但是，请考虑以下特殊情况：</p> <ul style="list-style-type: none"> <li>总是列出不符合对象创建时间筛选器中条件的 Filesystem 类型的对象(文件系统对象)。但是，在这种情况下，将其对象创建时间字段保留为空。</li> <li>如果从备份规范清除某些文件系统对象，则这些文件系统对象将不包括在报告中，即使这些对象存在于 IDB 中也是如此。</li> </ul> <p>上面的注意事项不适用于 Bar 类型的对象(集成对象)。</p>
必要选择：	无
可选选择：	备份规范、备份规范组、天数(从启动报告开始倒着计算)
支持的格式：	所有格式
omnirpt 选项：	obj_lastbackup

## 没有备份的对象

说明：	列出作为备份规范一部分但没有有效备份(成功完成的备份，保护尚未到期)的所有对象。集成的备份规范无此报告。
必要选择：	无
可选选择：	备份规范、备份规范组、天数(从启动报告开始倒着计算)

支持的格式：	所有格式
<b>omnirpt</b> 选项：	obj_nobackup

## 会话规范信息

说明：	显示有关所有选定备份、对象复制、对象合并和对象验证规范的信息，例如类型(如 IDB、MSESE、E2010)、会话类型、会话规范名称、组、所有者以及 pre-exec 和 post-exec 命令。
必要选择：	无
可选选择：	会话规范、备份规范组
支持的格式：	所有格式
<b>omnirpt</b> 选项：	dl_info

## 会话规范计划

说明：	列出每个指定的备份、对象副本、对象合并和对象验证规范的下次开始时间，最多提前一年。
必要选择：	无
可选选择：	会话规范、备份规范组
支持的格式：	所有格式
<b>omnirpt</b> 选项：	dl_sched

## 备份规范中的树

说明：	<p>列出指定备份规范中的所有树。还显示驱动器的名称和树的名称。</p> <p><b>Data Protector 8.14</b> 中引入的 VADP 功能可提供虚拟机的增强型报告。<b>VMware</b> 虚拟机表示为 <b>Data Protector</b> 客户机，它们称为 <b>VADP</b> 客户机。报告显示 <b>VMware</b> 对象的所有 VM 名称。</p>
必要选择：	无
可选选择：	备份规范、备份规范组
支持的格式：	所有格式
<b>omnirpt</b> 选项：	dl_trees

## 时间范围中的会话报告

时间范围报告中的会话提供有关在指定时间段运行的备份、对象副本、对象合并或对象验证会话的信息。

### 客户机统计信息

说明：	列出客户机及其备份状态统计信息。仅列出符合搜索标准的客户机。  <b>Data Protector 8.14</b> 中引入的 <b>VADP</b> 功能可提供虚拟机的增强型报告。 <b>VMware</b> 虚拟机表示为 <b>Data Protector</b> 客户机，它们称为 <b>VADP</b> 客户机，其中 <b>VM</b> 名称是客户机名称。
必要选择：	时间范围
可选选择：	备份规范、备份规范组、主机名
支持的格式：	所有格式
<b>omnirpt</b> 选项：	<b>host_statistics</b>

### 设备流

说明：	以图形方式呈现每个设备的使用情况。显示符合搜索标准的备份、对象副本和对象合并会话的流程图。如果将 <b>RptShowPhysicalDeviceInDeviceFlowReport</b> 全局选项设置为 <b>1</b> ，则相同的物理设备将集中在一起(显示为其锁名称或序列号)。如果没有指定的锁名称或序列号，则显示逻辑名称。
必要选择：	时间范围
可选选择：	会话规范、备份规范组
支持的格式：	<b>HTML</b>
<b>omnirpt</b> 选项：	<b>device_flow</b>

### 已使用介质的扩展报告

说明：	提供有关在特定时间范围内由备份、对象副本和对象合并会话使用的目标介质以及会话类型和子类型的扩展信息。
必要选择：	时间范围
可选选择：	会话规范、备份规范组
支持的格式：	所有格式

<b>omnirpt 选项：</b>	<b>used_media_extended</b>
--------------------	----------------------------

## 会话列表

<b>说明：</b>	列出指定时间范围内的所有会话及其统计信息。
<b>必要选择：</b>	时间范围
<b>可选选择：</b>	会话规范、备份规范组
<b>支持的格式：</b>	所有格式
<b>omnirpt 选项：</b>	<b>list_sessions</b>

## 对象副本

<b>说明：</b>	<p>显示指定时间范围内对象版本的有效副本数。副本数包括原始对象版本。</p> <p>VMware 虚拟机表示为 Data Protector 客户机，它们称为 VADP 客户机。VADP 客户机的新对象名称格式如下：</p> <p>&lt;hostname&gt;:/&lt;vCenter&gt;/&lt;path&gt;/&lt;vmname&gt; [&lt;UUID&gt;]</p> <p>此处，&lt;hostname&gt;是来宾虚拟机的 DNS 名称。如果 DNS 名称未知，则使用 IP 地址或 VM 名称。</p>
<b>必要选择：</b>	时间范围
<b>可选选择：</b>	会话规范、备份规范组、副本数
<b>支持的格式：</b>	所有格式
<b>omnirpt 选项：</b>	<b>obj_copies</b>

## 已使用介质的报告

<b>说明：</b>	列出在指定时间范围的备份、对象副本和对对象合并会话期间使用的目标介质及其统计信息。
<b>必要选择：</b>	时间范围
<b>可选选择：</b>	会话规范、备份规范组
<b>支持的格式：</b>	所有格式
<b>omnirpt 选项：</b>	<b>used_media</b>

## 会话错误

--	--

<b>说明：</b>	显示备份、对象副本、对象合并或对象验证会话期间发生的错误消息的列表。将消息按客户机分组。
<b>必要选择：</b>	时间范围
<b>可选选择：</b>	会话规范、备份规范组、主机名、消息级别
<b>支持的格式：</b>	所有格式
<b>omnirpt 选项：</b>	session_errors

## 会话流

<b>说明：</b>	<p>以图形方式呈现指定时间范围内每个会话的持续时间。显示符合搜索标准的备份、对象副本、对象合并和对象验证会话的流程图。</p> <p>图表中的颜色表示会话的以下总体状态：</p> <ul style="list-style-type: none"><li>• 红色：会话失败或中止。</li><li>• 绿色：会话成功完成，或完成但有错。</li><li>• 黄色：会话完成，但有失败的情况。</li><li>• 蓝色：会话正在排队，或发了出装载请求。</li></ul>
<b>必要选择：</b>	时间范围
<b>可选选择：</b>	会话规范、备份规范组
<b>支持的格式：</b>	HTML
<b>omnirpt 选项：</b>	session_flow

## 会话统计信息

<b>说明：</b>	显示所选时间范围内的备份、对象副本或对象合并状态统计信息。
<b>必要选择：</b>	时间范围
<b>可选选择：</b>	会话规范、备份规范组
<b>支持的格式：</b>	所有格式
<b>omnirpt 选项：</b>	session_statistics

## 单个会话报告

单会话报告提供有关特定会话的详细信息。

## 会话设备

说明：	提供有关所选会话中使用的所有目标设备的信息。
必要选择：	会话 ID
可选选择：	无
支持的格式：	所有格式
omnipt 选项：	session_devices

## 会话介质

说明：	提供有关所选会话中使用的所有目标介质的信息。
必要选择：	会话 ID
可选选择：	无
支持的格式：	所有格式
omnipt 选项：	session_media

## 会话对象副本

说明：	<p>显示所选的备份、对象副本或对象合并会话中的有效副本数。</p> <p>Data Protector 8.14 中引入的 VADP 功能可提供虚拟机的增强型报告。VMware 虚拟机表示为 Data Protector 客户机，它们称为 VADP 客户机。VADP 客户机的新对象名称格式如下：</p> <p>&lt;hostname&gt;:/&lt;vCenter&gt;/&lt;path&gt;/&lt;vmname&gt; [&lt;UUID&gt;]</p> <p>此处，&lt;hostname&gt; 是来宾虚拟机的 DNS 名称。如果 DNS 名称未知，则使用 IP 地址或 VM 名称。</p>
必要选择：	会话 ID
可选选择：	无
支持的格式：	所有格式
omnipt 选项：	session_objcopies

## 会话对象

说明：	列出作为所选会话一部分的所有备份、对象副本或对象合并对象及其统计信息。
-----	-------------------------------------

	<b>Data Protector 8.14</b> 中引入的 <b>VADP</b> 功能可提供虚拟机的增强型报告。 <b>VMware</b> 虚拟机表示为 <b>Data Protector</b> 客户机，它们称为 <b>VADP</b> 客户机。会话对象报告显示 <b>VM</b> 名称和 <b>VM</b> 路径。
必要选择：	会话 ID
可选选择：	无
支持的格式：	所有格式
<b>omnirpt</b> 选项：	<b>session_objects</b>

## 每个客户机会话

说明：	<p>提供有关作为所选备份会话一部分的每个客户机的信息。通过使用<b>生成多个报告</b>选项，可以将此报告拆分为若干更小的报告，其中每个报告对应一个客户机。</p> <p><b>VMware</b> 虚拟机表示为 <b>Data Protector</b> 客户机，它们称为 <b>VADP</b> 客户机。<b>VADP</b> 客户机的新对象名称格式如下：</p> <p>&lt;hostname&gt;:/&lt;vCenter&gt;/&lt;path&gt;/&lt;vmname&gt; [&lt;UUID&gt;]</p> <p>此处，&lt;hostname&gt; 是来宾虚拟机的 DNS 名称。如果 DNS 名称未知，则使用 IP 地址或 VM 名称。</p>
必要选择：	会话 ID
可选选择：	消息级别
支持的格式：	所有格式
<b>omnirpt</b> 选项：	<b>session_hosts</b>

## 单个会话

说明：	显示有关单个 <b>Data Protector</b> 备份、对象复制或对象合并会话的所有相关信息。
必要选择：	会话 ID
可选选择：	消息级别
支持的格式：	所有格式
<b>omnirpt</b> 选项：	<b>single_session</b>

## 报告发送方法

配置或启动报告或报告组时，可以在多种发送方法之间进行选择。

## 广播消息发送方法

通过广播消息发送方法，可以将具有报告输出的广播消息发送到指定系统。

只有通过指定应向其发送广播消息的系统才能只将广播消息发送到 **Windows** 系统。广播消息限制在 1000 字符以下，因此首选 **short** 格式。

## 电子邮件发送方法

可以将包含报告输出的电子邮件发送到指定的收件人。请确保提供收件人的完整电子邮件地址。

### 重要：

由于 **Microsoft Outlook** 的安全功能，使用电子邮件发送方法可能会导致 **CRS** 服务停止响应。有关解决方案的详细信息，请参见《*Data Protector 产品声明、软件说明和参考*》。或者，使用电子邮件 (**SMTP**) 作为电子邮件发送方法。

### 注意：

如果在 **Data Protector Cell Manager** 上安装了 **Microsoft Exchange Server 2007**，则电子邮件报告发送方法不起作用。请改用电子邮件 (**SMTP**) 发送方法。

## 在 Windows 系统中

要从 **Windows** 系统发送电子邮件报告，需要具有邮件配置文件。您可以使用现有的邮件配置文件，也可以创建一个名为 **OmniBack** 的新配置文件。

要使用现有的邮件配置文件，请将以下行添加到 **Data Protector omnirc** 文件：

```
OB2_MAPIPROFILE=existing_MAPI_profile_name
```

**HTML** 电子邮件报告在 **Windows** 中的显示取决于电子邮件客户机设置。许多电子邮件客户机以纯 **ASCII** 文本显示报告。要确保以 **HTML** 方式正确地显示报告，请在 **Web** 浏览器中打开报告。

## 在 UNIX 系统中

必须配置并在 **UNIX** 系统中运行电子邮件子系统；无需其他配置。

由于操作系统的限制，因此如果在使用不同区域设置的系统之间传递本地化的电子邮件报告，则其中的国际字符在 **UNIX** 系统中可能显示错误。

## 电子邮件 (SMTP) 发送方法

可以使用 **SMTP** 协议将包含报告输出的电子邮件发送到指定的收件人。请确保提供收件人的完整电子邮件地址。

建议采用这种电子邮件发送方法。

默认情况下，将用于发送报告的 **SMTP** 服务器的地址设置为 **Cell Manager** 的 IP 地址。要更改地址，请编辑 **SMTPServer** 全局选项。必须从 **Cell Manager** 系统可访问 **SMTP** 服务器，但 **SMTP** 服务器不需要是 **Data Protector** 单元的一部分。



## 在 Windows 系统中

有关如何将现有 Microsoft Exchange Server 配置为支持 SMTP，请参见 Microsoft Exchange Server 文档。

HTML 电子邮件报告在 Windows 中的显示取决于电子邮件客户机设置。许多电子邮件客户机以纯 ASCII 文本显示报告。要确保正确地显示报告，请在 Web 浏览器中打开报告。

## 在 UNIX 系统中

由于操作系统的限制，因此如果在使用不同区域设置的系统之间传递本地化的电子邮件报告，则其中的国际字符在 UNIX 中可能显示错误。

## 外部发送方法

通过外部脚本发送方法，可在自己的脚本中处理报告的输出。脚本以标准输入 (STDIN) 的形式接收输出。建议脚本处理采用 **tab** 格式。

位于 Cell Manager 系统上的脚本必须位于 /opt/omni/sbin(HP-UX 系统)或 Data\_Protector\_home\bin(Windows 系统)目录中。仅提供脚本的名称，而非整个路径。

请注意，在 Windows 系统上，支持的外部脚本扩展名只有 .bat、.exe 和 .cmd。要运行扩展名不受支持(例如 .vbs)的脚本，请创建批处理文件以启动该脚本。然后配置 Data Protector 以外部脚本的形式运行批处理文件，它随后启动扩展名不受支持的脚本。

还可以使用此发送方法执行指定介质的预定弹出。

## 记录到文件发送方法

通过记录到文件发送方法，可发布含有报告输出的文件。

文件将发布到 Cell Manager 系统。必须指定要向其发布报告的文件的名称。如果存在该文件，将覆盖它。

## SNMP 发送方法

通过 SNMP 陷阱发送方法，可以采用 SNMP 陷阱的形式发送报告。该 SNMP 陷阱可由应用程序使用各种 SNMP 陷阱进一步处理。

### 注意：

SNMP 发送方法仅适用于不超过所配置 SNMP 陷阱的最大大小的报告。否则，报告将分段。

## 在 Windows 系统中

SNMP 陷阱将发送到在 Windows SNMP 陷阱配置中配置的系统。需要配置 Windows SNMP 陷阱才能在 Cell Manager 上使用 SNMP 发送方法。

## 在 UNIX 系统中

在 UNIX Cell Manager 上，将 SNMP 陷阱发送到报告中配置的系统。

## 使用 Data Protector GUI 配置报告组

可以单独地(以交互方式)运行 Data Protector 报告，也可以将这些报告集中到报告组中，然后启动报告组。可以向已配置的报告组添加单独的报告。“装载请求报告”和“设备错误报告”只能用于报告组中，而不能作为交互报告。

使用 Data Protector GUI，报告组使您可以：

- 立即(以交互方式)启动所有报告。
- 计划组在指定时间启动报告。
- 由通知触发时组时启动组。

要在报告的输出中显示输入参数(选择)，请在报告向导中选择**在报告中显示选择标准**选项。此选项对没有必需或可选输入参数(选择)的报告不可用。报告的输出仅显示更改了默认值的必需参数和可选参数。

### 先决条件

- 您必须已加入 admin 用户组或向您授予了报告和通知用户权限。
- 不应删除以其帐户身份运行 CRS 服务的 Data Protector 用户。安装时默认情况下将配置此用户。在 Windows Cell Manager 上，这是以其帐户身份执行安装的用户。在 UNIX Cell Manager 上，这是 Cell Manager 的 root 用户。

### 配置阶段

#### 配置报告组

##### 步骤

1. 在上下文列表中，选择**报告**。
2. 右键单击**报告**，然后单击**添加报告组**以打开向导。
3. 命名报告组，然后单击**下一步**。
4. 单击**完成**以添加报告组，然后退出此向导。或者，您现在可以执行以下任务：
  - 计划报告组：右键单击报告组，然后单击**编辑计划**。“计划程序”页面随即打开。有关如何使用计划程序在 Data Protector 中创建和编辑计划的更多信息，请参见 [计划程序 \(第 92 页\)](#)。
  - 向报告组添加报告：右键单击报告组，然后单击**添加报告**。按照添加报告向导的操作添加报告。

**提示：**

要由通知触发报告组，请配置报告组，然后将通知配置为使用“使用报告组”发送方法。

## 向报告组添加报告

### 步骤

1. 在“报告”上下文中，展开**报告**，右键单击报告组，然后单击**添加报告**以打开添加报告向导。如果在报告组配置过程之后立即配置报告，则跳过此步骤。
2. 在结果区域中，从列表中选择一种报告类型。
3. 在“名称”文本框中，键入报告的名称并在“类型”下拉列表中选择报告。单击**下一步**。
4. 可用的向导选项取决于所选的报告。例如，对“IDB 大小”报告可用的所有向导选项对“介质列表”报告不可用。单击**下一步**所需次数，到达向导的最后一页。
5. 在“发送方法”下拉列表中，选择报告发送方法，然后在“电子邮件地址”文本框中输入报告的收件人。在“格式”下拉列表中，选择报告的格式。单击**添加**将收件人添加到配置的收件人组中。

对所有收件人重复此步骤。

6. 单击**完成**向报告组添加报告，然后退出此向导。

对要添加到报告组的所有报告重复此过程。

## 使用 Data Protector GUI 运行报告组

可以一起运行报告组中的所有报告。

### 先决条件

- 您必须已经添加到 **Admin** 用户组中，或者获得了报告和通知用户权限。
- 不应删除以其帐户身份运行 **CRS** 服务的 **Data Protector** 用户。安装时默认情况下将配置此用户。在 **Windows Cell Manager** 上，这是以其帐户身份执行安装的用户。在 **UNIX Cell Manager** 上，这是 **Cell Manager** 的 **root** 用户。

### 步骤

1. 在上下文列表中，选择**报告**。
2. 在范围窗格中，浏览并右键单击要启动的报告组，然后单击**启动**。
3. 单击**是**确认。

## 使用 Data Protector GUI 逐个运行报告

可以单独地以交互方式运行报告，也可以将这些报告集中到报告组中，然后一起运行报告组中的所有报告。

“装载请求报告”和“设备错误报告”只能用于报告组中，而不能作为交互报告。

### 先决条件

- 您必须位于 **Admin** 用户组中，或具有“报告和通知”用户权限。
- 不应删除以其帐户身份运行 **CRS** 服务的 **Data Protector** 用户。安装时默认情况下将配置

此用户。在 Windows Cell Manager 上，这是以其帐户身份执行安装的用户。在 UNIX Cell Manager 上，这是 Cell Manager 的 root 用户。

## 步骤

1. 在上下文列表中，选择**报告**。
2. 单击范围窗格下的**任务**选项卡。
3. 在范围窗格中，浏览所需的报告类型，然后选择某个报告以打开向导。
4. 可用的向导选项取决于所选的报告。例如，对“IDB 大小”报告可用的所有向导选项对“介质列表”报告不可用。单击**下一步**所需次数，到达向导的最后一页。
5. 在报告向导的结尾，单击**完成**以显示报告的输出。

## 使用 Data Protector CLI 运行报告和报告组

可以使用命令行界面 (CLI) 生成 Data Protector 报告。通过 CLI 可以在要使用的其他脚本中包括 Data Protector 报告。可以生成单独的报告、启动报告组、定义报告格式和发送方法。

## 先决条件

- 您必须已经添加到 Admin 用户组中，或者获得了报告和通知用户权限。
- 不应删除以其帐户身份运行 CRS 服务的 Data Protector 用户。安装时默认情况下将配置此用户。在 Windows Cell Manager 上，这是以其帐户身份执行安装的用户。在 UNIX Cell Manager 上，这是 Cell Manager 的 root 用户。

## 步骤

1. 使用 omnirpt 命令生成报告。有关命令的详细说明，请参见 omnirpt 手册页或 *Data Protector 命令行界面* 参考。

## 创建新的邮件配置文件

要从 Windows 系统发送电子邮件报告或通知，需要具有邮件配置文件。要创建名为 OmniBack 的新邮件配置文件，请在装有 Microsoft Outlook 2002 的 Windows 系统上使用下面的过程。

### 重要：

由于 Microsoft Outlook 的安全功能，使用电子邮件发送方法可能会导致 CRS 服务停止响应。有关解决方案的详细信息，请参见《Data Protector 产品声明、软件说明和参考》。或者，使用 e-mail (SMTP) 发送方法。

## 步骤

1. 在 Windows 控制面板中，双击**邮件**图标。
2. 在“邮件设置 - Outlook”对话框中，单击**显示配置文件**。
3. 在“邮件”对话框中，单击**添加**。
4. 在“新建配置文件”对话框中，在“配置文件名称”文本框中键入 OmniBack，然后单击**确定**。

以启动电子邮件帐户向导。

5. 选择**添加新的电子邮件帐户**，然后单击**下一步**。
6. 在“服务器类型”页中，选择 **Microsoft Exchange Server**，然后单击**下一步**。
7. 在“Exchange Server 设置”页中，键入本地 Microsoft Exchange Server 系统的名称、用户名，然后单击**下一步**。
8. 单击**完成**结束向导。

## 配置 Windows SNMP 陷阱

在 Windows Cell Manager 上，将 SNMP 陷阱发送到 Windows SNMP 陷阱配置中配置的系统。在 Windows 系统中，要使用 SNMP 发送方法发送通知或报告，需要配置 Windows SNMP 陷阱。

在 UNIX Cell Manager 上，将 SNMP 陷阱发送到通知或报告中配置的系统；无需其他配置。

### 步骤

1. 从目录 `Data_Protector_home\bin` 调用 `omnisnmp` 命令。  
它将在系统注册表中的  
`CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents` 下创建相应的 Data Protector 条目。
2. **Windows XP、Windows Server 2003:**
  - a. 在控制面板中，选择**网络连接**。
  - b. 在“高级”菜单中，选择**可选网络组件**以启动向导。
  - c. 选择**管理和监视工具**，然后单击**下一步**。
  - d. 按照向导的操作安装管理和监视工具。

#### **Windows 7、Windows 8:**

- a. 在控制面板中，选择**程序和功能**。
- b. 选择**开启或关闭 Windows 功能**。
- c. 选择**简单网络管理协议(SNMP)**，然后单击**确定**。

#### **Windows Server 2008、Windows Server 2012:**

- a. 在“开始”菜单中，右键单击**计算机**，然后选择**管理**。
  - b. 选择**功能**，然后单击**添加功能**。
  - c. 在“功能”树形结构中，选择 **SNMP 服务**，然后选择 **SNMP 服务**。
  - d. 单击**下一步**，然后单击**安装**。
3. 打开**控制面板、管理工具、服务**。
  4. 右键单击 **SNMP Service**，并选择**属性**。
    - a. 选择**陷阱**选项卡。在“社区名称”文本框中输入 `public`，并在“陷阱目标”文本框中输入应用程序管理服务器的主机名。
    - b. 选择**安全**选项卡。在“接受团体名称”下，选择 `public` 团体，单击**编辑**，然后将“团体权利”设置为 `READ CREATE`。

如果选择在从这些主机接受 SNMP 包下且身份验证失败，则使用 IP 地址而非“陷阱目标”文本框中的主机名。

- c. 确认您的更改。
5. 调用 omnismnp。

## 关于通知

通过 Data Protector，可在发生特定事件时从 Cell Manager 发送通知。例如，备份、对象复制、对象合并或对象验证会话完成后，可以发送含有会话状态的电子邮件。

可以设置通知，以使其触发报告。

可以使用 Data Protector GUI 或任何支持 Java 的 Web 浏览器配置通知。

通过设置输入参数可自定义通知。通过某些输入参数可实现多种选择。所有其他输入参数取决于通知的类型。根据发送方法，接收方可以是以下任意一项：

- 系统
- 电子邮件地址
- SNMP 陷阱
- 脚本
- 文件
- 所配置的报告组
- Data Protector 事件日志

默认情况下对通知配置默认值，并且将通知发送到 Data Protector 事件日志。要使用某些其他发送方法和/或其他输入参数值发送其他通知，必须更改配置值。

要访问 Data Protector 通知功能，您必须已加入 admin 用户组或被授予了报告和通知用户权限。

## 通知类型 - 触发通知的事件

通知分为两种主要类型。

- 事件发生时触发的通知
- 由 Data Protector 检查和维护机制计划和启动的通知

### 警报

事件/通知名称：	警报
由什么触发通知：	Data Protector 内部严重情况，例如自动介质复制升级、升级核心部分结束、升级详细信息部分结束、清除结束、会话中止、UCP 期间磁带代理升级等。
默认消息级别：	警告
所显示的消息：	警报: <i>Alarm_message</i>

## 证书已过期

事件/通知名称：	ExpiredCertificates
由什么触发通知：	Cell Manager 证书目录中存储的证书已过期或尚未生效。Cell Manager 证书目录存储用于安全控制通信的所有客户机证书。
默认消息级别：	警告
所显示的消息：	证书 <i>certificate_name</i> 已过期或尚未生效。

## Csa 启动会话失败

事件/通知名称：	CsaStartSessionFailed
由什么触发通知：	备份会话完成，但出现错误消息： Could not start a new backup session.
默认消息级别：	重大
所显示的消息：	数据列表 <i>datalist_name</i> 的 CsaStartSession 失败。

## 设备错误

事件/通知名称：	DeviceError
由什么触发通知：	设备 <b>设备</b> 上的错误(默认为 <Any>)。
默认消息级别：	严重
所显示的消息：	设备 <i>Device</i> 上发生错误。

## 会话结束

事件/通知名称：	EndofSession
由什么触发通知：	会话规范 <b>会话规范</b> 中指定的以消息 <b>会话状态</b> (默认为 Completed with errors)结束的备份、复制、合并或对象验证会话(默认为 <Any>)。
默认消息级别：	警告
所显示的消息：	会话规范 <i>backup_specification</i> , 备份规范组 <i>group</i> 的备份会话 <i>session_ID</i> 已完成，总体状态为 <i>session_overall_status</i> ; <i>session_type</i> 会话规范 <i>session_spec</i> 的会话 <i>session_ID</i> 已完成，总体状态为 <i>session_status</i> 。

## 文件库磁盘使用

事件/通知名称：	FileLibraryDiskUsage
由什么触发通知：	文件库 <b>文件库的名称</b> (默认为： A11)。
默认消息级别：	警告
所显示的消息：	<i>File Library Path</i> 目录中的 <i>File Library Device</i> 磁盘空间低。

## 运行状况检查失败

事件/通知名称：	HealthCheckFailed
由什么触发通知：	<p>由 <code>omnihealthcheck</code> 命令返回的非零值。 如果以下情况属实，则该命令返回零：</p> <ul style="list-style-type: none"><li>• Data Protector 服务(CRS、MMD、hdp-idb、hdp-idb-cp、hdp-as、KMS、omnitrig 和 omniinet)均为活动状态。</li><li>• Data Protector 介质管理数据库 (MMDB) 是一致的。</li><li>• 至少存在一个 IDB 的备份。</li></ul> <p>有关该命令的详细信息，请参见 <code>omnihealthcheck</code> 手册页或《<i>Data Protector 命令行界面参考</i>》。 默认情况下，Data Protector 每天启动一次运行状况检查(运行 <code>omnihealthcheck</code> 命令)。</p>
默认消息级别：	严重
所显示的消息：	运行状况检查消息： <i>healthcheck_command</i> 失败。

## 需要执行 IDB 备份

事件/通知名称：	IDBBackupNeeded
由什么触发通知：	连续增量 IDB 备份太多或完整 IDB 备份不够频繁。
默认消息级别：	警告
所显示的消息：	有 <i>n</i> 个连续增量 IDB 备份。 Data Protector 内部数据库的最后备份在 <i>MM/DD/YY hh:mm:ss</i> 上完成。

## IDB 已损坏

事件/通知名称：	IDBCorrupted
由什么触发通知：	IDB 的一部分损坏。



默认消息级别：	严重
所显示的消息：	<p>已检测到 Data Protector 内部数据库的 <i>IDB_part</i> 部分中发生损坏 (<i>error_message</i>)。</p> <p>错误消息的值为：</p> <ul style="list-style-type: none"> <li>• Verification of datafile(s) failed.</li> <li>• KeyStore is corrupted.</li> <li>• Media and Media in position tables are not consistent.</li> <li>• Database is not in consistent state.</li> <li>• Database schema is not consistent.</li> </ul>

## IDB 限制

事件/通知名称：	IDBLimits
由什么触发通知：	达到任何 MMDB 或 CDB 部分的限制。
默认消息级别：	重大
所显示的消息：	Data Protector 内部数据库的 <i>IDB_part</i> 部分已达到其限制。

## 需要重新组织 IDB

事件/通知名称：	IDBReorganizationNeeded
由什么触发通知：	由于存在碎片或浪费的空间，需要重新组织一个或多个 IDB 实体。
默认消息级别：	警告
所显示的消息：	<p>检测到表格 <i>name_of_table</i> 过大。</p> <p>检测到列 <i>uuid</i> 中存在表 <i>name_of_table</i> 的碎片。检测到索引 <i>name_of_index</i> 的碎片。</p>

## IDB 空间不足

事件/通知名称：	IDBSpaceLow
由什么触发通知：	<p>以下事件之一：</p> <ul style="list-style-type: none"> <li>• 最大可用磁盘大小低于 <b>IDB 磁盘可用阈值 [MB]</b>(默认值：300 MB)的值。</li> <li>• 所有 DC 目录的最大大小与当前大小之差低于 <b>DCBF 大小限制阈值 [MB]</b>(默认为：500 MB)的值。</li> </ul>

	<ul style="list-style-type: none"> <li>最大可用磁盘大小低于 <b>WAL 磁盘可用阈值 [MB]</b>(默认值： 300 MB)的值。</li> </ul> <p>默认情况下， Data Protector 每天检查一次“IDB 空间不足”条件。</p>
默认消息级别：	重大
所显示的消息：	Data Protector 内部数据库空间用尽。

## 许可证警告

事件/通知名称：	LicenseWarning
由什么触发通知：	对于购买许可证的需要。
默认消息级别：	警告
所显示的消息：	<i>n</i> 需要为类别 <i>name of the license</i> 购买许可证。 运行 <code>omnicc -check_licenses -detail</code> ，了解更多信息。

## 许可证将到期

事件/通知名称：	LicenseWillExpire
由什么触发通知：	Data Protector 许可证的即将到期日期。 许可证将在 <b>许可证有效期剩余天数</b> 中指定的天数后到期(此字段的默认值为： 10)。
默认消息级别：	警告
所显示的消息：	第一个许可证将在 <i>License expires in days</i> 天后过期。

## 邮件插槽已满

事件/通知名称：	MailSlotsFull
由什么触发通知：	设备 <b>设备</b> 的完整邮箱插槽(默认为： <Any>)。
默认消息级别：	警告
所显示的消息：	库 <i>Device</i> 的所有邮件插槽已用完。 立即将其删除。

## 装载请求

事件/通知名称：	MountRequest
由什么触发通知：	设备 <b>设备</b> 的装载请求(默认为： <Any>)。

默认消息级别：	警告
所显示的消息：	设备上的装载请求 <i>Device</i> 。

## 空闲介质不足

事件/通知名称：	NotEnoughFreeMedia
由什么触发通知：	介质池中缺少可用介质。 请注意，如果介质池配置为使用自由池，则还会考虑自由池中的可用介质的数量。
默认消息级别：	警告
所显示的消息：	介质池 <i>Media Pool</i> 仅包含 <i>number_of_media</i> 可用介质。

## 会话错误

事件/通知名称：	SessionError
由什么触发通知：	“监视器”窗口中显示含有级别为单个消息级别(默认为：Major)的消息的备份、复制、合并或对象验证会话。
默认消息级别：	重大
所显示的消息：	会话规范 <i>backup_specification</i> 、备份规范组 <i>group</i> 的备份会话 <i>session_ID</i> 有误： <i>number_of_errors</i> 。  <i>session_type</i> 会话规范 <i>session_spec</i> 的会话 <i>session_ID</i> 有误： <i>number_of_errors</i> 。

## 会话开始

事件/通知名称：	StartofSession
由什么触发通知：	会话规范 <b>会话规范</b> 中指定的备份、复制、合并或对象验证会话的开始(默认为： <Any>)。
默认消息级别：	Normal
所显示的消息：	对会话规范 <i>backup_specification</i> 备份规范组 <i>group</i> 启动了备份会话 <i>session_ID</i> 。  <i>session_type</i> 对会话规范 <i>session_spec</i> 启动了会话 <i>session_ID</i> 。

## 会话太多

事件/通知名称：	TooManySessions
----------	-----------------

由什么触发通知：	已同时运行 1000 个会话时启动会话。
默认消息级别：	警告
所显示的消息：	由于达到同时运行会话的最大数目，无法启动会话。

## 意外事件

事件/通知名称：	UnexpectedEvents
由什么触发通知：	上次进行检查以来 Data Protector 事件日志中新事件的数量异常大。数量超过 <b>事件数</b> (默认值为：20)。 默认情况下，Data Protector 每天检查一次此条件。
默认消息级别：	警告
所显示的消息：	Data Protector 事件日志在最后一天增加了 <i>number_of events_in_Last_day</i> 个意外事件。

## 检查 UNIX 介质代理

事件/通知名称：	UnixMediaAgentWarning
由什么触发通知：	mrgcfg -check_ma 命令在客户机设备使用重绕设备文件而不是非重绕设备文件时触发此通知。
默认消息级别：	警告
所显示的消息：	介质代理、客户机可能已使用重绕设备文件而不是非重绕设备文件对设备进行了配置。这样可能会导致 SAN 环境中出现问题。

## 用户检查失败

事件/通知名称：	UserCheckFailed
由什么触发通知：	由用户创建的为 <b>命令路径</b> 的脚本/命令返回的非零值，该脚本/命令位于默认的 Data Protector 管理命令目录中。 默认情况下，Data Protector 每天启动一次用户检查(运行脚本)(默认为：None)。
默认消息级别：	重大
所显示的消息：	用户检查失败，返回退出代码 <i>error_code:error_description</i> 。

## 通知发送方法

配置通知时，可以在多种发送方法之间进行选择。默认情况下，将所有通知都配置为发送到 **Data Protector** 事件日志。要使用另一种发送方法发送通知，还必须配置其他通知。可用的通知发送方法包括：

### 广播消息发送方法

通过广播消息发送方法，可以在发生指定事件之后将具有通知输出的广播消息发送到指定系统。

只有通过指定目标系统的方式才能将广播消息发送到 **Windows** 系统。广播消息限制在 1000 字符以下，因此首选 **short** 格式。

### 电子邮件发送方法

可以将包含通知输出的电子邮件发送到指定的收件人。请确保提供收件人的完整电子邮件地址。

**重要：**

由于 **Microsoft Outlook** 的安全功能，使用电子邮件发送方法可能会导致 **CRS** 服务停止响应。有关解决方案的详细信息，请参见《**Data Protector** 产品声明、软件说明和参考》。因此，建议采用 **SMTP** 方法发送电子邮件通知。

**注意：**

如果在 **Data Protector Cell Manager** 上安装了 **Microsoft Exchange Server 2007**，则电子邮件通知发送方法不起作用。请改用电子邮件 (**SMTP**) 发送方法。

### 在 **Windows** 系统上

要从 **Windows** 系统发送电子邮件通知，需要具有邮件配置文件。您可以使用现有的邮件配置文件，也可以创建一个名为 **OmniBack** 的新配置文件。

要使用现有的邮件配置文件，请将以下行添加到 **Data Protector omnirc** 文件：

```
OB2_MAPIPROFILE=existing_MAPI_profile_name
```

### 在 **UNIX** 系统上

必须配置并在 **UNIX** 系统中运行电子邮件子系统。

由于操作系统的限制，因此如果在使用不同区域设置的系统之间传递本地化的电子邮件通知，则其中的国际字符在 **UNIX** 系统中可能显示错误。

### 电子邮件 (**SMTP**) 发送方法

可以将包含通知输出的电子邮件发送到指定的收件人。请确保提供收件人的完整电子邮件地址。

建议采用这种电子邮件发送方法。

默认情况下，将用于发送通知的 SMTP 服务器的地址设置为 Cell Manager 的 IP 地址。要更改地址，请编辑 SMTPServer 全局选项。必须从 Cell Manager 系统可访问 SMTP 服务器，但 SMTP 服务器不需要是 Data Protector 单元的一部分。

## 外部发送方法

通过外部脚本发送方法，可在自己的脚本中处理通知的输出。脚本以标准输入 (STDIN) 的形式接收输出。建议脚本处理采用 *tab* 格式。

位于 Cell Manager 系统上的脚本必须位于默认的 Data Protector 管理命令目录中。仅提供脚本的名称，而非路径。

请注意，在 Windows 系统上，支持的外部脚本扩展名只有 .bat、.exe 和 .cmd。要运行扩展名不受支持(例如 .vbs)的脚本，请创建批处理文件以启动该脚本。然后配置 Data Protector 以外部脚本的形式运行批处理文件，它随后启动扩展名不受支持的脚本。

还可以使用此发送方法执行指定介质的计划弹出。

## 记录到文件发送方法

通过记录到文件发送方法，可在发生指定事件时发布含有通知输出的文件。

文件将发布到 Cell Manager 系统。必须指定要向其发布通知的文件的名称。如果存在该文件，将覆盖它。

## Data Protector 事件日志发送方法

默认情况下，所有通知都发送到 Data Protector 事件日志。仅 admin 用户组中的 Data Protector 用户以及获授“报告和通知”用户权限的 Data Protector 用户可访问 Data Protector 事件日志。可以查看或删除 Data Protector 事件日志中的所有事件。

## SNMP 发送方法

通过 SNMP 发送方法，可在发生指定事件时发送含有通知输出的 SNMP 陷阱。该 SNMP 陷阱可由应用程序使用各种 SNMP 陷阱进一步处理。

### 在 Windows 系统上

在 Windows Cell Manager 上，将 SNMP 陷阱发送到 Windows SNMP 陷阱配置中配置的系统。需要配置 Windows SNMP 陷阱才能在 Windows 系统中使用 SNMP 发送方法。

### 在 UNIX 系统上

在 UNIX Cell Manager 上，将 SNMP 陷阱发送到通知中配置的系统。

## 使用报告组发送方法

通过使用报告组发送方法，可在发生指定事件时运行报告组。

## 配置通知

要配置通知，需要提供通知的名称、通知的类型、消息级别、发送方法和收件人。所有其他输入参数取决于通知的类型。

## 先决条件

您必须已加入 `admin` 用户组或向您授予了报告和通知用户权限。

## 步骤

1. 在上下文列表中，选择**报告**。
2. 右键单击**通知**，然后单击**添加通知**以打开向导。
3. 向导选项取决于您所选的通知。例如，对“**IDB 空间不足**”通知可用的所有选项对“**IDB 限值**”通知不可用。单击**下一步**所需次数，到达向导的最后一页。
4. 单击**完成**退出向导。

发生指定事件时将使用指定的发送方法发送相应的通知。

### 提示：

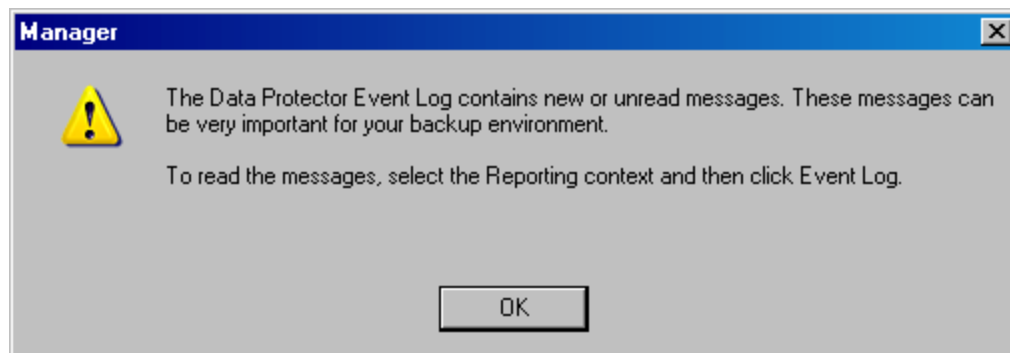
要由通知触发报告组，请配置报告组，然后将通知配置为使用“使用报告组”发送方法。

## 关于 Data Protector 事件日志

Data Protector 事件日志表示一种集中式事件管理机制，可处理 Data Protector 操作期间发生的特定事件。Data Protector 事件日志记录机制记录两类事件：进程触发和用户触发。事件记录在 Cell Manager 上的默认 Data Protector 日志文件目录下的 `Ob2EventLog.txt` 文件中。

使用事件日志查看器查看 Data Protector 事件日志有助于排除各种可能出现的问题。

用户启动 Data Protector 图形用户界面后，如果在 Data Protector 事件日志中有此用户尚未查看的新通知，则会显示以下消息：



Data Protector GUI 随之自动切换到“报告”上下文。

以下内容可能会提供其他信息：

- 您必须是 **admin** 用户组的成员或者向您授予了报告和通知用户权限。
- **Data Protector** 事件日志不自动刷新。若要查看新消息，请按 **F5** 手动刷新事件日志。

## 进程触发事件

事件由通知功能记录。

## 用户触发事件

用户执行特定 **GUI** 操作或一组 **GUI** 操作时会记录事件。这组操作包括备份修改、对象副本、合并规范、对用户和用户组的操作、设备创建和修改、介质相关配置以及远程安装操作。

默认情况下，对于用户触发的事件禁用日志记录。要启用它，必须将全局选项 **EventLogAudit** 设置为 **1**。

在 **MoM** 环境中，如果全局选项设置为 **1**，则仅会在本地 **Cell Manager** 系统上记录事件。

## 访问事件日志查看器

通过访问 **Data Protector** 事件日志查看器，可以浏览所记录的事件。

## 先决条件

您必须是 **admin** 用户组的成员或者向您授予了报告和通知用户权限。

## 步骤

1. 在上下文列表中，选择 **报告**。
2. 在范围窗格中，展开 **报告**。
3. 选择 **事件日志** 以显示它。

## 删除事件日志查看器内容

### 注意：

删除事件日志查看器内容不会删除 **Ob2EventLog.txt** 文件的内容。

## 先决条件

您必须是 **Admin** 用户组的成员，或者获得了“报告和通知”用户权限。

## 步骤

1. 在上下文列表中，选择 **报告**。
2. 在范围窗格中，展开 **报告**。
3. 右键单击 **事件日志**，然后选择 **清空事件日志** 以删除事件日志查看器中的所有条目。



## 关于审计

Data Protector 提供备份会话审计功能，此功能存储有关整个 Data Protector 单元在用户定义的期限内执行的所有备份任务的不可篡改和不可重写的信息。可根据需要以完整和可打印方式检索审计信息用于审计或管理。

通过修改全局选项 `AuditLogEnable` 和 `AuditLogRetention`，可以启用审计信息日志记录并设置审计日志文件的保留期。

## 生成审计报告

要生成审计报告，请按照下面的步骤进行操作。

**注意：**  
在 MoM 环境中，必须对每个 Cell Manager 单独执行审计报告。

## 步骤

1. 在上下文列表中，单击 **内部数据库**。
2. 在范围窗格中，单击 **审计** 项以打开“审计”页。
3. 从“搜索间隔”下拉列表中，选择其中的一个值(例如 Last week)。
4. 单击 **更新** 按钮，显示所选期间执行的所有备份会话的列表。
5. 从会话列表中选择某个特定会话，在“审计”属性页的中间和底部显示有关所使用介质和对象的详细信息。

## 检查 Data Protector 是否正常工作

### Data Protector 执行的检查

Data Protector 提供其自身的检查和维护机制，用以执行日常维护任务和检查。日常维护执行一系列命令，从 Data Protector 内部数据库的许多部分中清除过时的数据。

默认情况下，日常维护在每天中午进行。它不清除 IDB 的所有部分，仅清除无需独占访问 IDB 就可以完成的部分。

## 维护任务

默认情况下，Data Protector 每天中午 12:00 执行以下任务：

- 通过执行如下 `omnidbutil -purge` 命令，删除过时的 DC 二进制文件、会话和相关消息：

- -dcbf
- -sessions
- -messages

日常维护 -sessions 选项取决于 KeepObsoleteSessions 全局选项的设置，而 messages 选项取决于 KeepMessages 全局选项的设置。

- 在设置了使用自由池和将自由介质移动到自由池选项的介质池中查找任何空闲(未保护)介质，并通过执行 omnidbutil -free\_pool\_update 命令取消向自由池分配自由介质。
- 检查对介质的保护并删除介质和对应的介质位置。如果介质从 IDB 导出，则 IDB 不再识别位置，因此，Data Protector 无法为此类介质释放存储。必须手动从存储中删除该介质，且介质位置也应从设备上下文中手动删除。

有关详细信息，请参见 omnidbutil 手册页或《Data Protector 命令行界面参考》。

## 检查

默认情况下，Data Protector 每天中午 12:30 开始检查以下通知：

- IDB 空间不足
- IDB 限制
- 需要执行 IDB 备份
- 空闲介质不足
- 运行状况检查失败
- 用户检查失败(如果已配置)
- 意外事件
- 许可证警告
- 许可证将到期

默认情况下，Data Protector 在每个星期一中午 12:30 开始检查以下通知：

- 需要重新组织 IDB

默认情况下，将任何触发的通知发送到 Data Protector 事件日志。

### 提示：

可以更改维护任务和检查的默认计划值。分别使用 DailyMaintenanceTime 和 DailyCheckTime 全局选项以及二十四小时制表示法。

## 应执行哪些检查？

除了 Data Protector 默认情况下执行的检查以外，还建议您执行一些常规检查。这样可确保 Data Protector 正常运行和防患于未然。

### 提示：

通过开发脚本和使用“用户检查失败”通知，可以自动执行这些检查。

一些检查(例如，`omnihealthcheck` 和 `omnitrig -run_checks` 命令)已经作为 Data Protector 检查和维护机制的一部分执行。

有关使用的命令的详细信息，请参见各自的手册页或者《Data Protector 命令行界面参考》。

执行什么检查？	检查什么和如何检查？
检查 Data Protector Cell Manager	<p>如果此命令的退出代码是 0(表示成功)，则表示成功完成以下检查。0 以外的退出值表示检查失败。</p> <ol style="list-style-type: none"> <li>运行 <code>omnihealthcheck</code> 命令以检查： <ul style="list-style-type: none"> <li>Data Protector 服务 (CRS、MMD、<code>hpd-idb</code>、<code>hpd-idb-cp</code>、<code>hpd-as</code>、<code>omnitrig</code>、KMS 和 <code>Inet</code>)处于活动状态</li> <li>Data Protector 介质管理数据库是一致的</li> <li>是否至少存在 IDB 的一个备份映像</li> </ul> <p>仅当所有三项检查成功完成时(每个检查的退出代码都是 0)，该命令的退出代码才是 0(表示成功)。</p> </li> <li>运行 <code>omnidbcheck -quick</code> 命令检查 IDB。</li> </ol>
检查是否正确配置了备份	<ol style="list-style-type: none"> <li>对重要备份规范运行备份预览。成功完成的预览证明： <ul style="list-style-type: none"> <li>备份规范中的所有客户机都可以从 Cell Manager 访问。</li> <li>可以访问所有文件。</li> <li>确定要备份的数据量。</li> <li>正确配置了所有备份设备。</li> </ul> <p>请注意，某些集成和 ZDB 不支持预览。</p> </li> <li>运行 <code>omnirpt -report dl_sched</code> 命令以检查计划的备份规范是否符合备份策略。该命令列出所有备份规范及其计划。</li> </ol>
验证 Data Protector 安装	使用 Data Protector GUI、客户机上下文验证安装，检查 Data Protector 软件组件在 Cell Manager 或客户机系统是否已启动并正在运行。
检查 Data Protector 日志文件	<p>检查以下 Data Protector 日志文件，并确定可能的問題：</p> <ul style="list-style-type: none"> <li><code>event.log</code></li> <li><code>debug.log</code></li> <li><code>purge.log</code></li> </ul>
运行通知检查	<p>默认情况下，Data Protector 对以下通知每天启动一次检查。任何触发的通知都发送到 Data Protector 事件日志。</p> <p>还可以运行 <code>omnitrig -run_checks</code> 命令以启动对通知的检查：</p> <ul style="list-style-type: none"> <li>IDB 空间不足</li> </ul>

	<ul style="list-style-type: none"><li>• 空闲介质不足</li><li>• 意外事件</li><li>• 运行状况检查失败</li><li>• IDB 限制</li><li>• 需要执行 IDB 备份</li><li>• 需要重新组织 IDB</li><li>• 许可证将到期</li><li>• 许可证警告</li><li>• 用户检查失败(如果已配置)</li></ul>
检查其他系统资源	检查以下操作系统日志文件，并确定可能的问题：  <b>Windows 系统：</b> Windows 事件查看器及其安全、系统和应用程序日志  <b>UNIX 系统：</b> /var/adm/syslog/syslog.log
检查 IDB 恢复文件	检查 IDB 恢复文件 obrindex.dat，确保定期创建了成功恢复 Cell Manager 系统所需的 IDB 和配置文件。

## 如何自动执行检查

通过使用脚本和配置“用户检查失败”通知可以自动执行检查。

“用户检查失败”通知执行在此通知中指定为输入参数的命令或脚本，如果脚本中任何已执行命令的返回值不是 0，将触发通知。将通过所选的发送方法通知您。

命令/脚本必须位于应用程序系统上默认的 Data Protector 管理命令目录中。

配置的“用户检查失败”通知每天在 Data Protector 日常检查过程中启动，并在触发时发送到 Data Protector 事件日志。

# Data Protector 文档

## 注意：

软件支持网站(网址为：<https://softwaresupport.softwaregrp.com/>)中可用的文档集包含最新更新和更正。

您可从以下位置访问 Data Protector 文档集：

- Data Protector 安装目录。  
**Windows 系统：** `Data_Protector_home\docs`  
**UNIX 系统：** `/opt/omni/doc/C`
- Data Protector GUI 的帮助菜单。
- 支持网站(网址为：<https://softwaresupport.softwaregrp.com/>)

## 文档映射图

下表显示了可以从何处查找不同类型的信息。带灰色阴影的方框代表首选查找位置。

											集成指南				ZDB 指南		GRE 指南			
	Admin	帮助	入门	概念	安装	故障排除	DR	CLI	PA	集成 VSS	MSFT	Oracle/SAP	IBM	Sybase/NDMP	虚拟环境	ZDB 管理	ZDB IG	Exchange	SharePoint	VMware
管理任务	X	X																		
备份		X	X	X						X	X	X	X	X	X	X	X			
CLI								X												
概念、技术		X		X						X	X	X	X	X	X	X	X	X	X	X
灾难恢复				X			X													
安装、升级			X		X				X											
即时恢复				X	X											X	X			
许可					X				X											
限制		X			X	X			X	X	X	X	X	X	X		X			
新功能		X							X											
计划策略		X		X																
过程、任务	X	X			X	X	X			X	X	X	X	X	X	X	X	X	X	X
建议				X					X											
要求					X				X	X	X	X	X	X	X					
还原	X	X	X	X						X	X	X	X	X	X	X	X	X	X	X
支持的配置				X																
故障排除		X			X	X				X	X	X	X	X	X	X	X	X	X	X

## 缩写

以下对文档映射图中的缩写进行了说明。文档项标题前面均带有单词“Data Protector”。

缩写	文档项	
管理员	管理员指南	本指南介绍 <b>Data Protector</b> 中的管理任务。
CLI	命令行界面参考	本指南描述了 <b>Data Protector</b> 命令行界面、命令选项和它们的用途，并提供一些基本命令行示例。
概念	概念指南	本指南介绍 <b>Data Protector</b> 概念、零宕机时间备份 (ZDB) 概念，并提供有关 <b>Data Protector</b> 工作原理的背景信息。它应与面向任务的帮助配合使用。
DR	灾难恢复指南	本指南介绍如何规划、准备、测试和执行灾难恢复。
入门	入门指南	本指南包含使用 <b>Data Protector</b> 的入门信息。本指南列出安装先决条件，提供有关为执行备份和还原而安装和配置基本备份环境和过程的说明，还列出了可供了解进一步信息的资源。
GRE 指南	适用于 Microsoft SharePoint Server、Exchange 和 VMware 的 Granular Recovery Extension 用户指南	<p>本指南介绍如何配置和使用适用于以下组件的 <b>Data Protector Granular Recovery Extension</b>:</p> <ul style="list-style-type: none"> <li>• Microsoft SharePoint Server</li> <li>• Exchange Server</li> <li>• VMware vSphere</li> </ul>
帮助	帮助	
安装	安装指南	本指南介绍如何针对您所用环境的操作系统和体系结构来安装 <b>Data Protector</b> 软件。本指南还详细介绍了如何升级 <b>Data Protector</b> ，以及如何获取适用于您所用环境的正确许可证。
集成指南	集成指南	<p>本指南介绍 <b>Data Protector</b> 与以下应用程序的集成:</p> <ul style="list-style-type: none"> <li>• <b>MSFT</b>: Microsoft SQL Server、Microsoft SharePoint Server 和 Microsoft Exchange Server。</li> </ul>

缩写	文档项	
		<ul style="list-style-type: none"> <li>• <b>IBM:</b> Informix Server、IBM DB2 UDB 和 Lotus Notes/Domino Server。</li> <li>• <b>Oracle/SAP:</b> Oracle Server、MySQL、SAP R3、SAP MaxDB 和 SAP HANA Appliance。</li> <li>• <b>Sybase/NDMP:</b> Sybase 和 Network Data Management Protocol Server、</li> <li>• <b>虚拟环境:</b> 与 VMware vSphere、VMware vCloud Director、Microsoft Hyper-V 和 Citrix XenServer 进行虚拟环境集成。</li> </ul>
集成 VSS	Microsoft Volume Shadow Copy Service 的集成指南	本指南介绍 Data Protector 与 Microsoft 卷影复制服务 (VSS) 的集成。
PA	产品声明、软件说明和参考	本指南介绍最新版本的新功能。此外，它还提供有关安装要求、必需补丁、限制以及已知问题和变通方法的信息。
故障排除	故障诊断指南	本指南介绍如何对在使用 Data Protector 时遇到的问题进行故障诊断。
ZDB 管理	ZDB 管理员指南	本指南介绍如何配置和使用 Data Protector 与磁盘阵列的集成。适用于备份管理员或操作员。它涵盖了零宕机时间备份、即时恢复以及文件系统和磁盘映像的还原。
ZDB IG	ZDB 集成指南	本指南介绍如何配置和使用 Data Protector 来执行零宕机时间备份、即时恢复，以及 Oracle Server、SAP R/3、Microsoft Exchange Server、Microsoft SQL Server 数据库和适用于 VMware 的虚拟环境的标准还原。

## 集成

### 软件应用程序集成

软件应用程序	指南
IBM DB2 UDB	集成指南
Informix Server	集成指南
Lotus Notes/Domino Server	集成指南
Microsoft Exchange Server	集成指南、ZDB IG、GRE 指南
Microsoft Hyper-V	集成指南
Microsoft SharePoint Server	集成指南、ZDB IG、GRE 指南
Microsoft SQL Server	集成指南、ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	集成 VSS
Network Data Management Protocol (NDMP) Server	集成指南
Oracle Server	集成指南、ZDB IG
MySQL Server	集成指南
SAP HANA Appliance	集成指南
SAP MaxDB	集成指南
SAP R/3	集成指南、ZDB IG
Sybase Server	集成指南
VMware vCloud Director	集成指南
VMware vSphere	集成指南、ZDB IG、GRE 指南

### 磁盘阵列系统集成

查看以下指南了解与以下系列的磁盘阵列系统的集成有关的详细信息：

磁盘阵列系列	指南
EMC Symmetrix	所有 ZDB
P4000 SAN 解决方案	概念、ZDB 管理、集成指南



磁盘阵列系列	指南
P6000 EVA 磁盘阵列系列	所有 ZDB、集成指南
P9000 XP 磁盘阵列系列	所有 ZDB、集成指南
3PAR StoreServ Storage	概念、ZDB 管理、集成指南
NetApp Storage	概念、ZDB 管理、ZDB IG
EMC VNX	概念、ZDB 管理、ZDB IG
EMC VMAX	概念、ZDB 管理、ZDB IG

# 发送文档反馈

如果对此文档有任何评论，可以通过电子邮件[联系文档团队](#)。如果该系统配置了电子邮件客户机，请单击上面的链接，此时会打开一个电子邮件窗口，其主题行中将显示以下信息：

## 有关管理员指南 (Data Protector 10.00) 的反馈

将反馈添加到电子邮件中并单击**发送**。

如果无可用的电子邮件客户机，请将以上信息复制到 Web 邮件客户机中的新邮件，并将反馈发送至 [docs.feedback@microfocus.com](mailto:docs.feedback@microfocus.com)。

期待您的反馈！