

DL 设备上的 Rapid Recovery 6.0

用户指南

注、小心和警告

 **注:** “注”表示可以帮助您更好地使用计算机的重要信息。

 **小心:** “小心”表示可能会损坏硬件或导致数据丢失，并说明如何避免此类问题。

 **警告:** “警告”表示可能会造成财产损失、人身伤害甚至死亡。

版权所有 © 2016 Dell Inc. 保留所有权利。 本产品受美国、国际版权和知识产权法律保护。Dell 和 Dell 徽标是 Dell Inc. 在美国和/或其他管辖区域的商标。所有此处提及的其他商标和名称可能是其各自所属公司的商标。

1 DL 设备简介.....	11
部署架构.....	11
Smart Agent.....	12
DL 设备 Core.....	13
快照流程.....	13
复制灾难恢复站点或服务提供商.....	13
恢复.....	13
产品功能	13
了解存储库.....	14
Rapid Recovery 中的重复数据消除.....	15
了解加密密钥.....	15
Rapid Recovery 中的复制.....	16
保留和存档.....	19
虚拟化和云.....	20
警报和事件管理.....	20
许可证门户.....	21
Web 控制台.....	21
服务管理 API.....	21
2 使用 DL 设备 Core.....	22
了解 Rapid Recovery Core Console.....	22
访问 Rapid Recovery Core Console.....	22
了解快速入门指南.....	22
导航 Rapid Recovery Core Console.....	24
查看“受保护机器”菜单.....	27
从导航菜单查看被复制的机器.....	31
查看“仅限恢复点”菜单.....	31
查看自定义群菜单.....	32
使用“错误”对话框.....	32
Core 设置.....	32
Rapid Recovery Core 设置.....	32
备份并还原 Core 设置.....	56
Core 级工具.....	57
配置 Core 的路线图	60
存储库.....	60
管理 DVM 存储库.....	60
管理安全性	70
应用加密或从受保护机器中移除加密.....	71
管理加密密钥.....	73
管理云帐户.....	79
关于云帐户.....	79

添加云帐户.....	79
编辑云帐户.....	81
配置云帐户设置.....	81
删除云帐户.....	81
存档.....	82
了解存档.....	82
创建存档.....	82
编辑计划存档.....	84
暂停或恢复计划存档.....	86
强制执行存档作业.....	86
检查存档.....	86
附加存档.....	87
导入存档.....	88
事件.....	90
Rapid Recovery 事件.....	90
使用任务、警报和日记查看事件.....	90
了解电子邮件通知.....	93
系统事件的通知组、SMTP 设置和通知模板.....	96
配置通知组.....	96
关于配置减少重复.....	98
配置事件保留.....	99
快速设备自行恢复.....	99
创建 RASR USB 闪存盘.....	100
执行 RASR.....	100
Local Mount Utility.....	101
关于 Local Mount Utility.....	101
在 Local Mount Utility 中处理 Rapid Recovery Core 机器.....	102
在 Local Mount Utility 中使用受保护机器.....	104
使用 Local Mount Utility 托盘菜单.....	107
3 管理您的设备.....	108
监测设备的状态.....	108
Windows 备份.....	108
备份状态.....	109
Windows 备份策略.....	110
配置存储.....	111
删除虚拟磁盘的空间分配.....	112
Recovery and Update Utility.....	112
升级设备.....	112
修复您的设备.....	113
4 保护工作站和服务.....	114
保护机器.....	114
关于用 Rapid Recovery 保护计算机.....	114
访问受保护机器诊断.....	166

管理机器.....	168
移除机器.....	168
取消机器上的操作.....	169
查看机器的许可证信息.....	169
VM 导出.....	169
关于使用 Rapid Recovery 导出至虚拟机.....	169
管理导出.....	180
管理老化数据.....	191
关于 Rapid Recovery 数据保留和存档.....	192
管理保留策略.....	192
复制.....	196
Rapid Recovery 中的复制.....	196
恢复点链和孤立恢复点.....	200
当复制开始时.....	201
确定您的播种需求和策略.....	201
复制数据传输的性能注意事项.....	203
复制到自管目标 Core.....	204
查看传入和传出复制.....	206
配置复制.....	208
复制到第三方目标 Core.....	208
添加机器至现有复制.....	212
在目标 Core 上使用种子驱动器.....	214
管理复制设置.....	215
移除复制.....	221
恢复已复制数据.....	222
5 恢复数据.....	223
管理恢复	223
快照和恢复点.....	223
管理快照和恢复点.....	223
查看受保护机器的恢复点页面.....	223
安装恢复点.....	225
卸载恢复点.....	226
使用 Linux 恢复点.....	227
强制创建快照.....	228
移除恢复点.....	229
删除孤立恢复点链.....	229
手动迁移恢复点到其他存储库.....	230
还原数据.....	230
关于使用 Rapid Recovery 还原数据.....	230
了解实时恢复.....	231
从恢复点还原数据.....	231
关于从恢复点还原卷.....	232
执行群集和群集节点还原.....	234
从连接的存档中还原.....	235

了解 Windows 机器执行 Bare Metal Restore.....	236
Windows 机器的裸机还原.....	236
了解 Windows 机器启动 CD 创建.....	240
针对 BMR 使用通用恢复控制台.....	242
对 Linux 机器执行 Bare Metal Restore.....	248
验证裸机还原.....	256
6 生成并查看报告.....	260
关于 Rapid Recovery 报告.....	260
从 Core Console 生成报告.....	261
从 Core Console 管理计划报告.....	263
使用“报告”菜单.....	267
使用“报告”工具栏.....	267
了解“作业”报告.....	269
了解作业摘要报告.....	269
了解失败报告.....	270
了解摘要报告.....	270
了解存储库报告.....	271
Central Management Console.....	272
了解 Rapid Recovery Central Management Console.....	272
配置 Rapid Recovery Central Management Console.....	273
了解 Central Management Console Core 报告.....	276
7 了解 Rapid Recovery Command Line Management 实用程序.....	278
命令.....	279
存档.....	280
CancelActiveJobs.....	281
CheckRepository.....	282
CreateArchiveRepository.....	283
CreateBootCD.....	284
CreateRepository.....	285
DeleteRepository.....	286
Dismount.....	287
DismountArchiveRepository.....	288
EditEsxServer.....	289
Force.....	290
ForceAttach.....	291
ForceChecksum.....	291
ForceLogTruncation.....	292
ForceMount.....	293
ForceReplication.....	294
ForceRollup.....	295
ForceVirtualStandby.....	296
帮助.....	296
List.....	297
安装.....	299

MountArchiveRepository.....	300
NewCloudAccount.....	301
OpenDvmRepository.....	302
Pause.....	303
Protect.....	304
ProtectCluster.....	305
ProtectEsxServer.....	306
RemoveAgent.....	307
RemoveArchiveRepository.....	308
RemovePoints.....	309
RemoveScheduledArchive.....	310
RemoveVirtualStandby.....	311
Replicate.....	312
复制.....	313
RestoreAgent.....	315
RestoreArchive.....	316
RestoreUrc.....	317
Resume.....	318
SeedDrive.....	319
StartExport.....	320
UpdateRepository.....	322
版本.....	324
VirtualStandby.....	324
本地化.....	327
附录 A: Core Console 参考.....	328
查看 Core Console 用户指南.....	328
按钮条.....	329
图标栏.....	330
左侧导航菜单.....	331
查看 Protected Machines（受保护机器）面板.....	333
查看受保护机器的事件.....	335
查看受保护机器的 More（更多）菜单.....	337
附录 B: 了解 Rapid Recovery PowerShell 模块.....	338
使用 PowerShell 的先决条件.....	339
powershell.exe.config.....	339
启动 PowerShell 并导入模块.....	339
使用命令和命令行工具.....	339
获得命令行工具帮助和示例.....	339
Rapid Recovery PowerShell 模块 cmdlet.....	340
Edit-EsxVirtualStandby.....	342
Edit-HyperVVirtualStandby.....	344
Edit-ScheduledArchive.....	345
Edit-VBVirtualStandby.....	347
Edit-VMVirtualStandby.....	348
Get-ActiveJobs.....	349

Get-Clusters.....	350
Get-CompletedJobs.....	351
Get-ExchangeMailStores.....	352
Get-Failed.....	353
Get-FailedJobs.....	354
Get-Mounts.....	355
Get-Passed.....	356
Get-ProtectedServers.....	357
Get-ProtectionGroups.....	357
Get-QueuedJobs.....	358
Get-RecoveryPoints.....	359
Get-ReplicatedServers.....	360
Get-Repositories.....	361
Get-ScheduledArchives.....	362
Get-SqlDatabases.....	363
Get-UnprotectedVolumes.....	363
Get-VirtualizedServers.....	364
Get-Volumes.....	365
New-Base.....	366
New-CloudAccount.....	367
New-EncryptionKey.....	368
New-EsxiVirtualStandby.....	369
New-HyperVVirtualStandby.....	370
New-Mount.....	372
Resume-Replication.....	373
New-Repository.....	374
New-ScheduledArchive.....	375
New-Snapshot.....	377
New-VBVirtualStandby.....	377
New-VMVirtualStandby.....	379
Push-Replication.....	380
Push-Rollup.....	381
Remove-Agent.....	382
Remove-Mount.....	383
Remove-Mounts.....	384
Remove-RecoveryPoints.....	384
Remove-Repository.....	385
Remove-ScheduledArchive.....	386
Remove-VirtualStandby.....	387
Resume-Replication.....	388
Resume-Snapshot.....	389
Resume-VirtualStandby.....	390
Resume-VMExport.....	391
Start-Archive.....	392
Start-AttachabilityChec.....	393

Start-ChecksumCheck.....	394
Start-EsxiExport.....	395
Start-HypervExport.....	396
Start-LogTruncation.....	397
Start-MountabilityCheck.....	398
Start-Protect.....	399
Start-ProtectCluster.....	400
Start-RepositoryCheck.....	401
Start-RestoreArchive.....	402
Start-ScheduledArchive.....	403
Start-VBExport.....	404
Start-VirtualStandby.....	406
Start-VMExport.....	406
Stop-ActiveJobs.....	408
Suspend-Replication.....	409
Suspend-RepositoryActivity.....	410
Suspend-ScheduledArchive.....	411
Suspend-Snapshot.....	412
Suspend-VirtualStandby.....	412
Suspend-VMExport.....	413
Update-Repository.....	414
本地化.....	415
限定符.....	415
附录 C: 使用脚本扩展 Rapid Recovery 作业.....	417
在 Rapid Recovery 中使用 PowerShell 脚本.....	417
PowerShell Scripting 的先决条件.....	417
powershell.exe.config.....	418
测试 PowerShell 脚本.....	418
本地化.....	418
限定符.....	418
PowerShell Scripting 的输入参数.....	419
AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents).....	419
AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer).....	419
BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs).....	420
ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks).....	421
DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange).....	421
ExportJobRequest (namespace Replay.Core.Contracts.Export).....	421
NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql).....	422
RollupJobRequest (namespace Replay.Core.Contracts.Rollup).....	422
TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer).....	422
TransferJobRequest (namespace Replay.Core.Contracts.Transfer).....	422
TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution).....	424
TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution).....	424
TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution).....	426
VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization).....	426

VolumeImageldsCollection (namespace Replay.Core.Contracts.RecoveryPoints).....	426
VolumeName (namespace Replay.Common.Contracts.Metadata.Storage).....	427
VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage).....	427
VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer).....	427
VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer).....	428
示例 PowerShell 脚本.....	428
PreTransferScript.ps1.....	428
PostTransferScript.ps1.....	429
PreExportScript.ps1.....	429
PostExportScript.ps1.....	430
PreNightlyJobScript.ps1.....	430
PostNightlyJobScript.ps1.....	432
使用 Rapid Recovery 中的 Bourne Shell 脚本.....	433
Bourne Shell Scripting 的先决条件.....	434
支持传输和后传输脚本参数.....	434
测试 Bourne Shell Scripting.....	434
Bourne Shell Scripting 的输入参数.....	434
TransferPrescriptParameters_VolumeNames.....	435
TransferPostscriptParameter.....	435
示例 Bourne Shell 脚本.....	436
PreTransferScript.sh.....	436
PostTransferScript.sh.....	436
PostExportScript.sh.....	437
附录 D: Rapid Recovery API.....	438
目标用户.....	438
使用 Rapid Recovery REST API.....	438
下载并查看 Core 和 Agent API.....	438
推荐的补充阅读.....	439
关于 Dell.....	440
联系 Dell.....	440
技术支持资源.....	440
词汇表.....	441

DL 设备简介

DL 设备加 Rapid Recovery 软件是一种备份、复制和恢复解决方案，可提供近乎零的恢复时间目标和恢复点目标。Rapid Recovery 提供数据保护、灾难恢复、数据迁移和数据管理。您具有执行裸机还原的灵活性（类似或不同的硬件）并且您可以将备份还原到物理机或虚拟机，无论来源是什么。通过 Rapid Recovery，您可以复制到一个或多个目标以增加冗余性和安全性。

通过在一个解决方案中结合使用备份、复制和恢复可提供最快、最可靠的备份，进而保护虚拟机 (VM)、物理机和云环境，为您的设备创立了统一数据保护新标准。您的设备内置有全局重复数据消除、压缩、加密和复制功能，能够处理多达数 PB 的数据，适用于所有私有云或公共云基础结构。只需几分钟就可以完成服务器应用程序和数据的恢复，能够满足数据保留和法规遵从性要求。

您的设备支持 VMware vSphere 和 Microsoft Hyper-V 私有云和公共云上的多虚拟机监控程序环境。

Rapid Recovery 可提供：

- **灵活性。**您可以执行到多个平台的通用恢复，包括从物理到虚拟、虚拟到物理、虚拟到虚拟和物理到物理的还原。
- **云集成。**您可以利用支持专有和开放平台的云存储供应商，存档和复制到云。
- **智能重复数据消除。**您可以通过存储数据一次并在之后对其进行引用来减少存储要求（每个存储库或加密域一次）。
- **即时恢复。**我们的实时恢复功能允许您首先访问重要数据，同时并行完成其余的还原操作。
- **文件级恢复。**您可以在内部、从远程位置或从云以文件级别恢复数据。
- **虚拟支持。**对虚拟化的增强支持包括针对 VMware® ESXi™ 5 和更高版本的无代理保护和自动查找，以及导出到 Microsoft® Hyper-V® 群集共享卷。

有关 Rapid Recovery 的更多信息，请参阅以下资源。

- Dell Rapid Recovery 产品支持网站 <https://support.software.dell.com/rapid-recovery/>。
- 说明文件网站 <https://support.software.dell.com/rapid-recovery/release-notes-guides/> 和 <http://www.dell.com/support/home/>。

主题：

- 部署架构
- 产品功能

部署架构

您的设备是一种可扩展的备份和恢复产品，可以灵活地部署在企业环境中，也可以作为一种服务由托管服务提供商交付。部署类型取决于客户的规模和要求。准备部署您的设备时，需要规划网络存储拓扑、核心硬件和灾难恢复基础结构以及安全性。

部署架构包括本地组件和远程组件。对于不需要使用灾难恢复站点或托管服务提供商进行非现场恢复的环境来说，远程组件可能不是必选组件。基本本地部署包括一台称为“Core”的备份服务器以及一台或多台受保护机器。通过复制在灾难恢复站点提供全面恢复功能，从而支持非现场组件。Core 使用基本映像和增量快照来编辑受保护机器的恢复点。

此外，您的设备具有应用程序感知功能，因为它能够检测 Microsoft Exchange 和 SQL 及其各自数据库和日志文件的存在状态，然后按照依赖关系自动将这些卷分组，从而实现全面保护和有效恢复。这有助于确保在执行恢复时不会遇到不完整的备份。备份通过应用程序感知型块级快照来执行。此外，您的设备还能够截断受保护的 Microsoft Exchange Server 和 SQL Server 的日志。

下图展示了简单的部署。在此图中，AppSure 代理软件安装在文件服务器、电子邮件服务器、数据库服务器或虚拟机等机器上，并且连接到单个 Core（包含中央存储库）并受其保护。许可证门户用于管理环境中的受保护机器和 Core 的许可证订阅、组 and 用户。许可证门户允许用户登录、激活帐户、下载软件以及按照环境中的许可证来部署受保护机器和 Core。

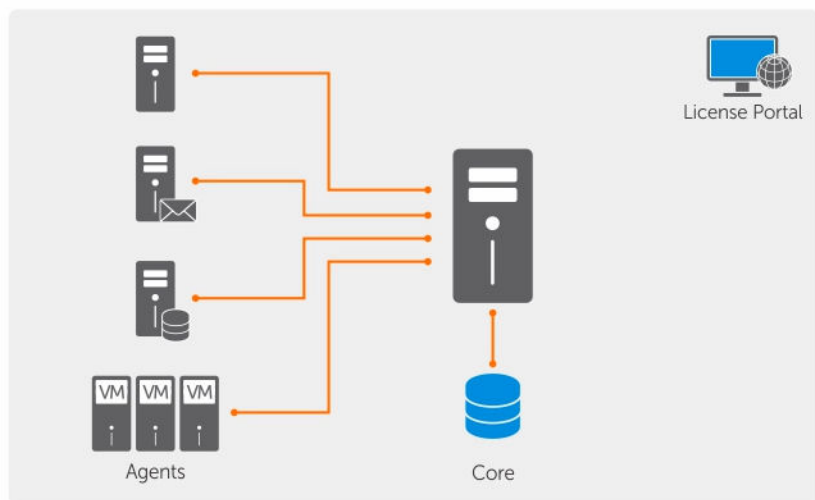


图 1: 基本部署架构

您也可以如下图所示部署多个 Core。中央控制台可管理多个 Core。

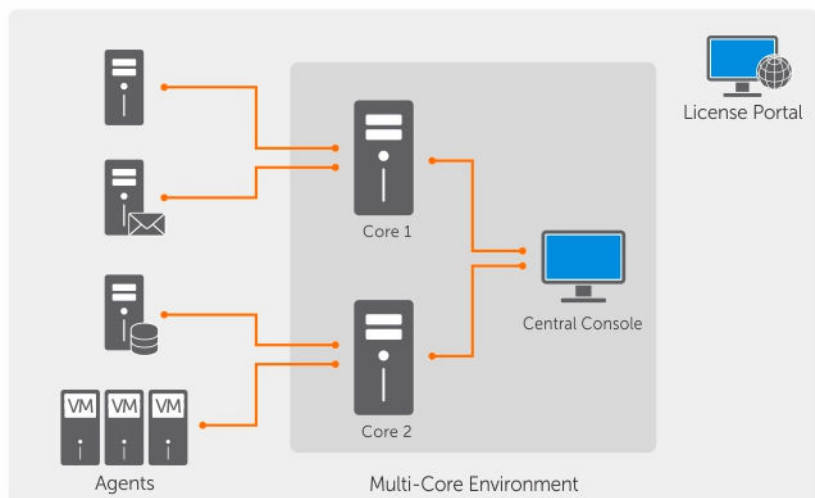


图 2: 多 Core 部署架构

Smart Agent

Smart Agent 跟踪磁盘卷上更改的块，然后在预定义的保护时间间隔拍摄更改块的映像。永久块级增量快照方法可防止将相同数据从受保护机器重复复制到 Core。Rapid Recovery Smart Agent 安装在 Rapid Recovery Core 保护的机器上。

Smart Agent 具有应用程序感知功能，它不仅能够检测所安装应用程序的类型，还能够检测数据的位置。它按照依赖关系（例如数据库）自动将数据卷分组，再将它们记录在一起，从而实现有效保护和快速恢复。配置 Rapid Recovery Agent 软件后，它会使用智能技术跟踪受保护磁盘卷上发生更改的块。快照准备就绪之后，系统会通过基于套接字的智能多线程连接迅速将其传输至 Core。为节约受保护机器上的 CPU 带宽和内存，Smart Agent 不会在源头对数据执行加密或重复数据消除操作，系统会将受保护机器与 Core 进行配对，以提供保护。

DL 设备 Core

Core 是部署架构的核心组件。Core 存储并管理所有机器备份并提供用于备份、恢复和保留、复制、存档和管理的 Core 服务。Core 是一台独立的网络可寻址的计算机，运行 64 位的 Microsoft Windows 操作系统。您的设备执行基于目标的内联压缩、加密以及接收自受保护机器的数据的重复数据消除。然后 Core 在存储库（例如存储区域网 (SAN) 或直接连接存储 (DAS)）中存储快照备份。

存储库还可以位于 Core 中的内部存储上。通过从 Web 浏览器访问以下 URL 来管理 Core: **https://CORENAME:8006/apprecovery/admin**。可通过 REST API 从内部访问所有 Core 服务。可从 Core 内部访问 Core 服务，也可以通过 Internet 从能够发送和接收 HTTP/HTTPS 请求和响应的任意应用程序直接进行访问。所有 API 操作均通过 SSL 执行，并使用 X.509 v3 证书互相进行身份验证。

Core 会与其他 Core 配对以进行复制。

快照流程

快照是从受保护机器传输至 Core 的基本映像。在生成数据的应用程序仍处于使用中时，快照会捕获并存储给定时间点的磁盘卷状态。在 Rapid Recovery 中，可强制创建快照、临时暂停快照并查看存储库中当前恢复点的列表，以及在需要时删除它们。恢复点用于还原受保护机器或安装到本地文件系统。通过 Rapid Recover 捕获的快照是在数据块级别完成的并且具有应用程序感知功能。也就是说，在创建快照前，所有开放性事务、滚动事务日志均已完成并且高速缓存已刷新到磁盘。

Rapid Recovery 使用低级别卷筛选驱动程序，后者先附加到已安装的卷上，然后跟踪下一个待处理快照的所有数据块级更改。Microsoft 卷影服务 (VSS) 有助于创建应用程序崩溃一致性快照。

复制灾难恢复站点或服务提供商

复制过程需要两个 Core 之间具有配对的“源-目标”关系。源 Core 复制受保护机器的恢复点，然后不断将其异步传输至远程灾难恢复站点上的目标 Core。非现场位置可以是公司所有的数据中心（自管 Core）或第三方托管服务提供商 (MSP) 的位置或云环境。复制到 MSP 时，可以使用允许提出连接请求、接收自动反馈通知的内置工作流。对于初始数据传输，可以使用外部介质执行数据播种，这对大型数据集或具有慢速链路的站点来说非常有用。

当发生严重中断时，设备支持在复制环境下执行故障转移和故障回复。发生全面中断时，次要站点中的目标 Core 可以从复制的受保护机器恢复实例，并立即开始对故障转移后的机器进行保护。主要站点还原后，已复制 Core 可以将已恢复实例的数据故障回复到主要站点上的受保护机器。

恢复

可以在本地站点或复制的远程站点执行恢复。在部署进入稳定状态并且具有本地保护和可选复制后，Core 允许您使用 Verified Recovery（验证恢复）、Universal Recovery（通用恢复）或 Live Recovery（实时恢复）执行恢复。

产品功能

您可以使用以下各项特性和功能管理关键数据的保护和恢复：

- Repository（存储库）
- Rapid Recovery 中的重复数据消除
- Encryption（加密）
- 复制
- 保留和存档
- 虚拟化和云
- 警报和事件管理

- [许可证门户](#)
- [Web 控制台](#)
- [服务管理 API](#)

了解存储库

存储库是一个集中位置，从受保护工作站和服务器捕获的备份快照数据会在其中进行存储和管理。数据以恢复点的形式保存到存储库中。

存储库可位于不同存储技术平台上，包括存储区域网络 (SAN)、直接连接存储 (DAS) 或网络连接存储 (NAS)。

① 注: 将 **Rapid Recovery Core** 的存储库存储在主要存储设备上。对于存储卷，速度是最关键的因素。由于性能局限性，不支持 **Data Domain** 等存档存储设备。同样，请勿将存储库存储在云层的 **NAS** 文件管理器上，因为这些设备在用作主要存储时性能上通常存在局限性。

DAS 提供最高的数据带宽和最快的访问速率并易于实现。为获得最佳结果，请使用 DAS 和独立磁盘 (RAID) 6 存储的冗余阵列。有关更多信息，请参阅 [Dell 知识库文章 118153](#) “存储库选项：直接连接的存储、存储区域网络或网络连接存储。”

任何存储库的存储位置应始终在您指定的子目录中（例如，**E:\Repository**），切勿在卷根目录中（例如，**E:**）。

Rapid Recovery 存储库格式使用重复数据消除卷管理器 (DVM)。DVM 存储库支持多个卷、单个 Core 上最多 255 个存储库以及数据区的使用。您仅可在安装 Windows 操作系统的机器上创建 DVM 存储库。当使用新的 Rapid Recovery 安装时，您可以使用此存储库类型。您可以在创建时指定 DVM 存储库的大小并可稍后添加数据区。

DVM 存储库功能和属性包括：

- 支持从 Rapid Recovery 6.x 存档和恢复点进行恢复
- 仅支持 Windows 操作系统上的存储位置。存储库卷可以位于本地（位于连接到 Core 服务器的存储上）或位于 Internet 文件系统 (CIFS) 共享位置中的存储位置上。
- 支持的存储类型包括存储区域网络 (SAN)、直接连接存储 (DAS) 或网络连接存储 (NAS)
- 需要 8GB RAM，最好是使用错误检查修正(ECC) 内存
- Core 机器上需要使用四核处理器（此长期存在的要求现在现在是强制的）
- 每个主机支持多个 DVM 存储库
- 无需附加服务：DVM 存储库使用本机 Core 服务来与 Core 通信和跟踪事件
- 每个 DVM 存储库最多支持 4096 个存储库数据区（也称为存储位置）
- 固定大小：DVM 存储库要求您指定卷上存储库的大小。指定的大小不能超过卷的大小。定义为存储位置的每个卷必须至少有 1GB 的可用空间。
- 存储库存储位置可以是简单磁盘或动态磁盘，但速度是最重要的因素
- 可以使用在 Core 控制台中创建和管理的标准加密密钥（基于 Core 的加密）
- 跨整个存储库（或者，如果使用加密密钥，则跨每个存储库内的加密域）进行重复数据消除
- 在 Core 设置中使用一个大小可调的专用 DVM 重复数据消除高速缓存和可配置的存储位置
- 优化写入数据，将存储库中的快照数据本地存储到 Core，通过 Core 处理所有数据
- 创建后无法重命名
- 此类型的新存储库可以使用 REST API、Rapid Recovery 命令行管理实用程序 (cmdutil.exe) 或 Windows PowerShell® cmdlet 进行创建

当您创建 DVM 存储库时，Rapid Recovery Core 在指定位置预分配数据和元数据所需的存储空间。最小 DVM 存储库大小为 1GB，出于实用目的，此大小通常太小，但用于测试除外。

因为 DVM 重复数据消除需要主高速缓存和耳机高速缓存，确保您保留的存储空间为重复数据消除高速缓存大小的两倍。例如，如果您在 Core 的 DVM 重复数据消除高速缓存设置中保留 1.5GB，则高速缓存卷上应保留 3GB。高速缓存默认安装路径在 C 驱动器上。有关更多信息，请参阅[了解清除重复项缓存大小和存储位置](#)。

您可以创建与单个 Core 关联多个独立存储库，最多为 255 个 DVM 存储库。存储库可以跨不同的存储技术平台。

通过添加新的文件数据区或规格，您可以进一步增加 DVM 存储库的大小。扩展存储库最多可包含 4096 个跨不同存储技术的数据区。

有关使用 DVM 存储库的更多信息，请参阅[管理 DVM 存储库](#)。

Rapid Recovery 中的重复数据消除

重复数据消除是一种数据压缩技术，可减少存储需求和网络负载。该过程涉及在磁盘上实际只存储一次唯一的数据块。在 Rapid Recovery 中，当任何唯一数据块在存储库内出现第二次时，将存储该数据的虚拟引用，而不是再次存储该数据。

重复数据消除在 Rapid Recovery Core 捕获的备份快照中进行。在单个存储库对备份信息执行重复数据消除操作。无法跨多个存储库执行重复数据消除操作。

Rapid Recovery 版本 6.0.2 为所有 DVM 存储库使用基于目标的重复数据消除。在此模式中，信息传输到 DVM 存储库（目标），然后从存储库执行重复数据消除。

大部分重复数据消除过程以内嵌的形式发生（在备份信息传输过程中）。

为获得最大效果，Rapid Recovery 现在还提供按后处理形式执行的重复数据消除。后处理有时也称为直通重复数据消除。使用此模式时，存储库中的数据会与 DVM 数据高速缓存中的引用进行比较。如果存储库中的数据块已被保存，则每个额外出现的该数据将被替换为该数据的指引或引用。

这种后处理可以节省存储库卷上的空间，尤其是在重复数据消除高速缓存已满，随后增加高速缓存以充分利用额外的重复数据消除功能时。执行存储库优化作业时，会发生此类型的重复数据消除。此功能是 DVM 存储库所独有，也称为重复数据块回收。

有关存储库优化作业的更多信息，请参阅[关于存储库优化作业](#)。有关执行此任务的更多信息，请参阅[优化 DVM 存储库](#)。

因此，Rapid Recovery 可以充分利用此处所述的所有类型的重复数据消除：基于目标的重复数据消除、内嵌重复数据消除和后处理重复数据消除。

有关 DVM 存储库的唯一数据块的引用存储位置的更多信息，请参阅[了解清除重复项缓存大小和存储位置](#)。

了解加密密钥

Rapid Recovery Core 可使用您通过 Core Console 定义和管理的加密密钥对任何存储库内的所有卷加密快照数据。

Rapid Recovery 并非加密整个存储库，而是允许您为单个 Rapid Recovery Core 上受保护的一个或多个机器指定加密密钥。每个活动的加密密钥都会创建一个加密域。在 Core 上可创建无限数量的加密密钥。

在多租户环境（在单个 Core 托管多个加密域时）中，每个加密域内的数据已经过分区和重复数据消除。因此，如果您希望在一组受保护机器之间最大限度地获得重复数据消除的好处，Dell 建议为多个受保护机器使用单个加密密钥。

您也可以使用三种方法之一在多个 Core 之间共享加密密钥。一种方法是通过一个 Rapid Recovery Core 将加密密钥导出为文件，然后将其导入到另一个 Core。第二种方法是归档通过加密密钥保护的数据，然后将该存档数据导入到另一个 Rapid Recovery Core。第三种方法是使用加密密钥从受保护机器复制恢复点，源 Core 中使用的加密密钥会在目标 Core 中显示为复制的加密密钥。

在所有情况下，一旦导入，Core 中出现的任何加密密钥的状态都为“已锁定”。要访问拥有锁定加密密钥的数据，您必须将其解除。有关导入、导出、锁定或解锁加密密钥的信息，请参阅主题[管理加密密钥](#)。

关键安全概念和注意事项包括：

- 在兼容 SHA-3 的密码块链 (CBC) 模式下，采用 256 位高级加密标准 (AES) 进行加密。

- 重复数据消除在加密域内进行操作，以便确保隐私。
- 进行加密时不会影响性能。
- 您可以将单一加密密钥应用到任意数量的受保护机器，但任何受保护机器都只能一次应用一个加密密钥。
- 您可以添加、移除、导入、导出、修改和删除 Rapid Recovery Core 上配置的加密密钥。

小心：只要您将加密密钥应用到受保护的机器，**Rapid Recovery** 都会拍摄一个新的快照。在您为受保护的机器断开加密密钥的关联后，也将触发新的快照。

Rapid Recovery Core 生成的加密密钥是包含四个参数的文本文件，如下表所述：

表. 1: 加密密钥的组件

组件	说明
名称	此值等同于当在 Rapid Recovery Core Console 中添加密钥时提供的密钥名。
键	此参数包含 107 个随机生成的英文字母、数字和数学运算符字符。
ID	密钥 ID 由 26 个随机生成的大写和小写英文字母组成。
注释	注释包含创建密钥时输入的密钥说明文本。

Rapid Recovery 中的复制

本节提供概念和过程方面的信息，以便帮助了解和配置 Rapid Recovery 中的复制功能。

复制是从 Rapid Recovery Core 复制恢复点并将其发送至另一个 Rapid Recovery Core 以满足灾难恢复目的的过程。此过程需要两个或多个 Core 之间配对的“源-目标”关系。

源 Core 复制所选受保护机器的恢复点，然后不断将快照数据异步传输至目标 Core。

除非您通过设置复制计划更改默认行为，否则 Core 会在完成每个备份快照、校验和检查、可附加性检查和每夜作业后立即启动复制作业。有关详情，请参阅[计划复制](#)。

为获得最佳的数据安全性，管理员通常在远程灾难恢复站点使用目标 Core。您可以将上述出站复制配置到公司自己的数据中心或远程灾难恢复站点（即“自管”目标 Core）。或将上述出站复制配置到托管服务提供商 (MSP) 提供的非现场备份和灾难恢复服务。复制到第三方 Core 时，可以使用允许提出连接请求和接收自动反馈通知的内置工作流。

复制按受保护的机器进行管理。可以将任何源 Core 上的受保护或复制机器（或全部机器）配置为复制到目标 Core。

可能的复制方案包括：

- **复制到本地位置。**目标 Core 位于本地数据中心或现场位置，并且将始终保持复制。在此配置下，丢失 Core 不会妨碍恢复。
- **复制到非现场位置。**目标 Core 位于非现场灾难恢复设施内，以备在发生丢失时进行恢复。
- **相互复制。**两个不同地点的数据中心各自包含一个 Core，都对机器进行保护并相互充当对方的非现场灾难恢复备份。在此方案下，各个 Core 会将受保护机器复制到位于另一数据中心的 Core。
- **托管和云复制。**Rapid Recovery MSP 合作伙伴在数据中心或公共云中维护多个目标 Core。在每个 Core 上，MSP 合作伙伴可让一个或多个客户从位于客户站点的源 Core 将恢复点复制到 MSP 的目标 Core，并收取费用。

① 注：在此方案下，客户仅有权访问自己的数据。

可能的复制配置包括：

- **点对点复制。**将一个或多个受保护机器从单个源 Core 复制到单个目标 Core。

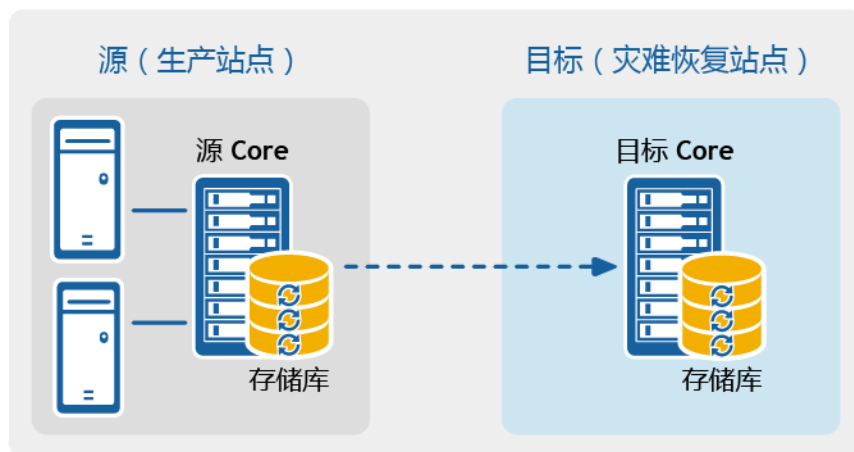


图 3: 点对点复制配置

- **多点到点复制。**将受保护机器从多个源 Core 复制到单个目标 Core。

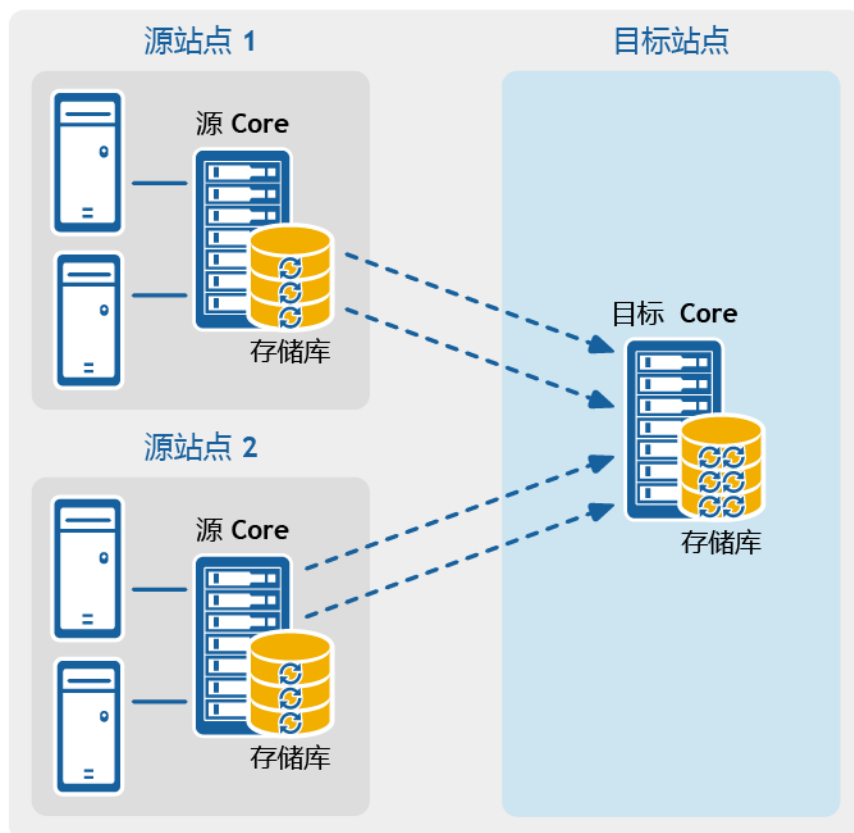


图 4: 多点到点复制配置

- **点到多点复制。**将一个或多个受保护机器从单个源 Core 复制到多个目标 Core。

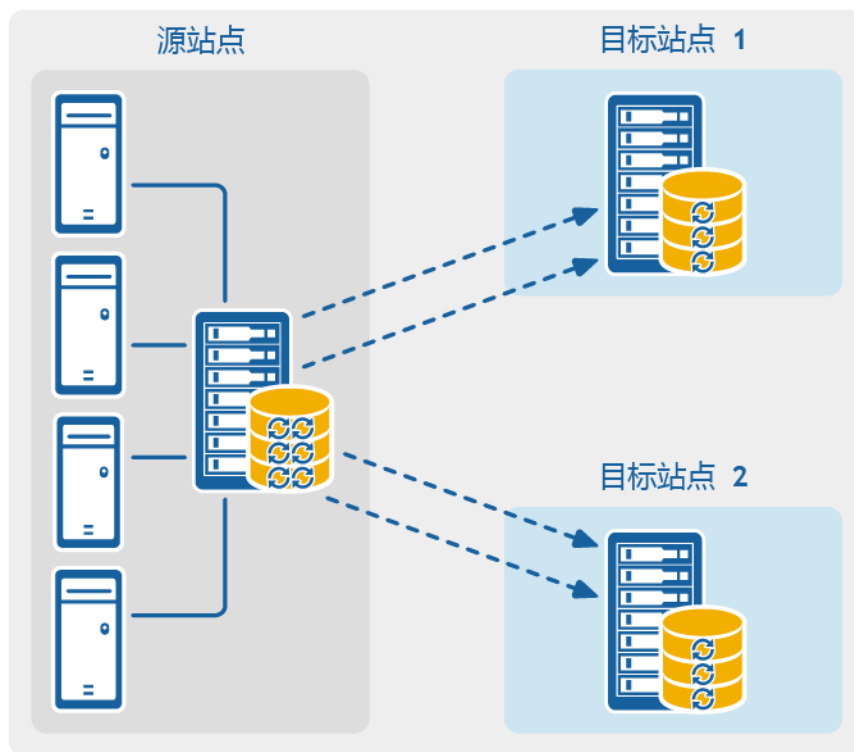


图 5: 点到多点复制配置

- **多跃点复制。** 将一个或多个受保护机器从一个目标 Core 复制到另一个目标 Core，从而在复制的 Core 上产生额外的故障转移或恢复选项。

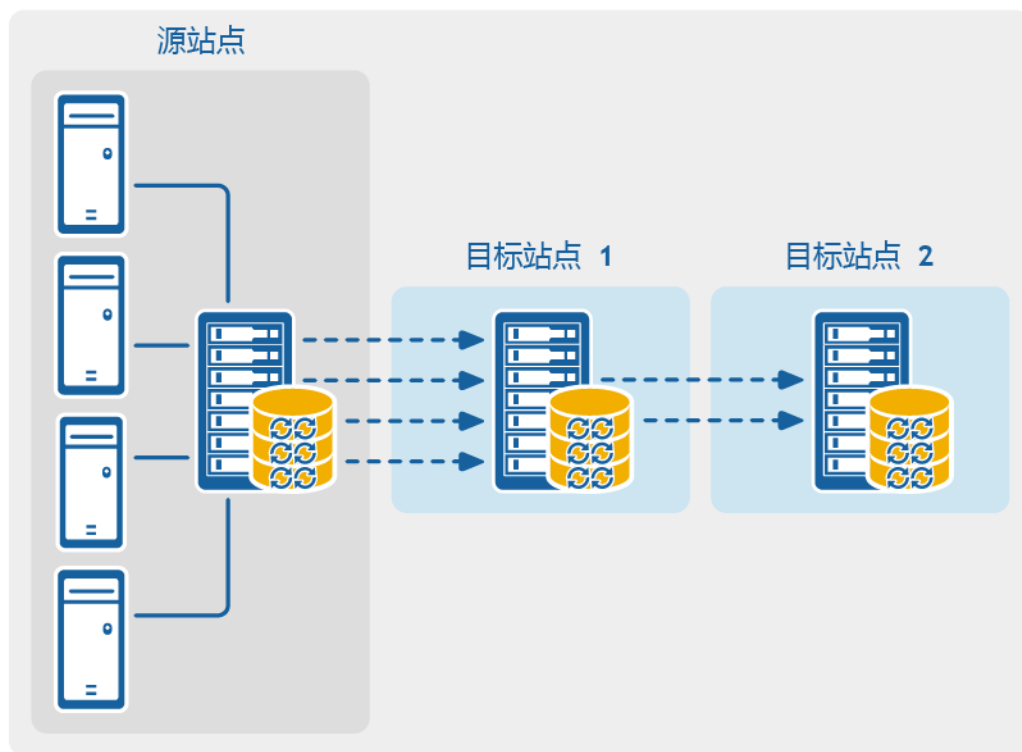


图 6: 多跃点复制配置

如果使用 Dell 数据保护备份设备（例如 DL1x00 或 DL4x00 系列），您复制到的目标 Core 必须配置一个有效的软件许可证。在购买时，这些硬件设备包括一个复制目标许可证。在您购买设备时收到的欢迎电子邮件消息中检查您的许可证密钥。如需帮助，请访问许可帮助网站 (<https://support.software.dell.com/licensing-assistance>) 或发送电子邮件至 license@software.dell.com。

保留和存档

在设备中，备份和保留策略十分灵活，因此易于配置。根据组织的需求定制保留策略的能力不仅有助于满足符合性要求，也不会对 RTO 造成影响。

将备份存储至短期（快速且昂贵）介质时，保留策略将限制其保留期限。有时，某些业务和技术要求延长这些备份的保留期限，但是使用快速存储的成本过高。因此，需要创建长期（速度慢、价格低）存储。企业通常使用长期存储来存档合规和非合规数据。存档功能支持延长合规和非合规数据的保留期限，也用于将复制数据播种到目标 Core。

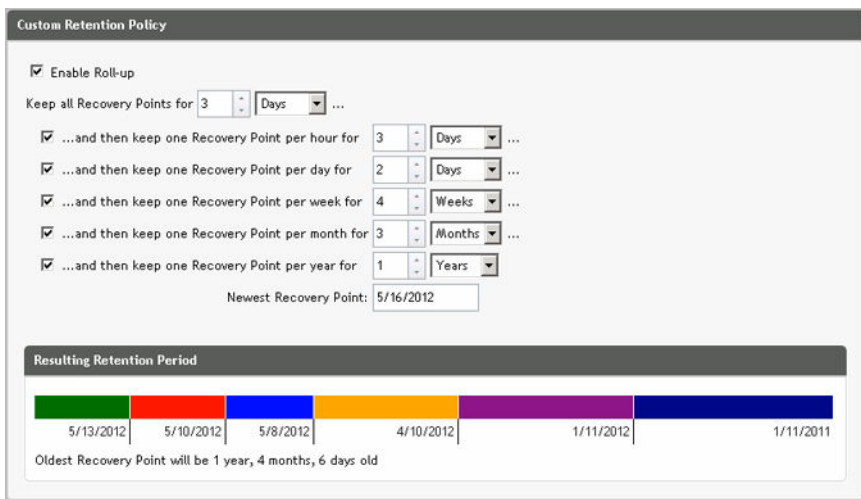


图 7: 自定义保留策略

在设备中，保留策略可以进行自定义，以指定备份恢复点应保留的时间长度。当恢复点的期龄接近保留截止期限终点并且恢复点的期龄最终超过这一期限时，系统将从保留池中移除这些恢复点。通常情况下，由于数据量和保留期限的增长十分迅速，此过程的效率低下而且最终会失败。设备将利用复杂的保留策略来管理大量数据的保留期限，同时利用高效的元数据操作来对老化数据执行前滚操作，从而解决大型数据的问题。

用户可以每隔几分钟执行一次备份。这些备份会在数天、数月或数年后过期，保留策略能够管理旧备份的老化和删除问题。简单的瀑布模型方法对老化过程进行了定义。瀑布中的层级按照分钟、小时、天、周、月和年进行定义。保留策略由每晚的前滚过程执行。

对于长期存档，设备可在任何可移动介质上创建源 Core 或目标 Core 的存档。存档经过内部优化，其中所有数据均执行过压缩、加密和重复数据消除。如果存档的总大小超过可移动介质上的可用空间，则可以根据介质上的可用空间跨越多台设备进行存档。存档还可以通过密码短语锁定。从存档进行恢复不需要新 Core，如果管理员拥有密码短语和加密密钥，所有 Core 均可以获取存档并恢复数据。

虚拟化和云

Core 可直接用于云，您可以利用云的计算能力进行恢复。

您的设备可以将所有受保护或已复制机器导出至虚拟机，如获得许可的 VMware 或 Hyper-V 版本。您可以执行一次性虚拟导出，也可以通过建立连续虚拟导出来建立一个虚拟待机虚拟机。如果采用连续导出，虚拟机会在每次快照后进行增量更新。增量更新非常迅速，同时提供待机克隆功能，只需单击一个按钮即可启动。支持的虚拟机导出类型为 VMware Workstation/Server 文件夹；直接导出至 vSphere 或 VMware ESX (i) 主机；导出至 Oracle VirtualBox；以及导出至 Windows Server 2008 (x64)、2008 R2、2012 (x64) 和 2012 R2（包括支持 Hyper-V 第 2 代虚拟机）中的 Microsoft Hyper-V Server

此外，您现在可以将存储库数据存档至使用 Microsoft Azure、Amazon S3、Rackspace Cloud Block Storage 的云或其他基于 OpenStack 的云服务。

警报和事件管理

除 HTTP REST API 之外，设备还包括丰富的事件日志记录和通知功能，并使用电子邮件、系统日志或 Windows 事件日志实现。电子邮件通知可以用来提醒用户或组各种事件的运行状况或状态，以应对警报。系统日志和 Windows 事件日志方法用于在多操作系统环境中将日志记录集中至存储库。在纯 Windows 环境中，仅使用 Windows 事件日志。

许可证门户

许可证门户提供了简单易用的工具来管理许可证权限。您可以下载、激活、查看和管理许可证密钥，并且可以创建公司配置文件来跟踪许可证资产。此外，通过此门户，服务提供商和转销商可以跟踪并管理他们的客户许可证。

Web 控制台

设备具有基于 Web 的全新中央控制台，能够从一个中心位置管理分散的 Core。具有多个分散 Core 的 MSP 和企业客户可以部署中央控制台来获取统一视图，以便进行集中管理。中央控制台能够在层级组织单位中组织各托管 Core。这些组织单位可以代表 MSP 的业务部门、地点或客户。中央控制台还可以跨越管理 Core 运行多种报告。

服务管理 API

设备随附服务管理 API，能够为所有通过 Central Management Console 获得的功能提供编程访问。服务管理 API 属于 REST API。所有 API 操作均通过 SSL 执行，并使用 X.509 v3 证书互相进行身份验证。用户可以从环境内访问管理服务，也可以通过 Internet 从能够发送 HTTPS 请求和接收 HTTPS 响应的任意应用程序直接进行访问。此方法能够促进与所有 Web 应用程序的轻松集成，例如关系管理方法 (RMM) 工具或计费系统。还包括面向 PowerShell 脚本编写的 SDK 客户端。

使用 DL 设备 Core

了解 Rapid Recovery Core Console

本章介绍了 Rapid Recovery Core Console 用户界面 (UI) 的不同元素。

访问 Rapid Recovery Core Console

要访问 Rapid Recovery Core Console，请完成以下步骤。

- 要访问 Rapid Recovery Core Console，请执行以下操作之一：
 - a 从本地登录到 Rapid Recovery Core 服务器，然后双击 Core Console 图标。
 - b 或者，在网页浏览器中键入以下 URL 之一：
 - <https://<yourCoreServerName>:8006/apprcovery/admin/> 或
 - <https://<yourCoreServerIPaddress>:8006/apprcovery/admin/>

注：由于 Rapid Recovery Core Console UI 取决于 JavaScript，因此您用来访问 Core Console 的网页浏览器必须启用 JavaScript。

如果已更改 Rapid Recovery 服务的默认端口，则应相应地更新上述 URL 中的端口。

了解快速入门指南

快速入门指南功能向您提供用于配置和使用 Rapid Recovery Core 的一系列指导性建议任务。

首次升级到或安装 Rapid Recovery Core 并导航至 Core Console 时，将自动显示“Quick Start Guide”（《快速入门指南》）。单击指南的欢迎页面上的**入门指南**可查看各种建议的配置任务。使用**跳过步骤**和**返回**选项可浏览指南。查看最后一项建议的任务后，单击**完成**以关闭指南。

可以随时从 Core Console 中的“帮助”菜单再次启动“快速启动指南”。您也可以在快速入门指南中选择隐藏**欢迎**页面。

除非您隐藏“Quick Start Guide”（《快速入门指南》），否则每次登录 Rapid Recovery Core Console 并访问**主页**页面时将重新显示该指南。有关更多信息，请参阅**隐藏快速入门指南**。

您无需执行指南建议的步骤。您可以只查看建议的任务，使用**跳过步骤**和**返回**选项导航有关任务。（可选）要在任何点上隐藏指南，请单击**退出指南**。

如果选择快速入门指南建议的任何配置任务请按照指南的任何步骤中的提示操作，且将显示相应向导或用户界面中的相关区域。本文介绍了完成指南建议的每项任务的过程，如下表所示。

注：并非所有用户都需要执行快速入门指南建议的所有配置任务。您必须根据特定需要了解要完成的任务。

快速入门指南阐述了以下配置任务：

表. 2: 快速入门指南配置任务

功能	简短说明	选择任务的结果，链接到过程
保护	保护单台机器、保护服务器群集或使用批量保护来保护多台机器	单击“保护”或从下拉菜单中选择保护机器以打开“保护机器向导”。有关完成“保护机器向导”的信息，请参阅保护机器。 从下拉菜单中选择保护群集以打开“连接到群集”对话框。有关保护群集的更多信息，请参阅保护群集。 从下拉菜单中选择批量保护将打开“保护多台机器向导”。有关完成“保护多台机器向导”的信息，请参阅关于保护多台计算机。
复制	设置从主（源）Core 到次要（目标）Core 的复制	单击 复制 以打开“复制”页面。提示您使用“复制向导”添加目标 Core。有关使用“复制向导”在自管 Core 上设置复制的信息，请参阅 复制到自管目标 Core 。有关复制的一般信息，请参阅 配置复制 。
虚拟导出	执行从受保护机器到虚拟机的一次性导出或建立连续导出	单击 导出 以执行从受保护机器到虚拟机的数据导出。您可执行一次性导出，或设置 Virtual Standby 进行连续导出到虚拟机。有关虚拟导出的信息，请参阅 关于使用 Rapid Recovery 导出至虚拟机 。
配置	允许您设置 Rapid Recovery Core 的其他配置	单击 更多 以查看可以配置或管理的其他功能。功能包括存档、装载、引导 CD、存储库、加密密钥、云帐户、文件搜索、保留策略、通知、报告、日志等等。
配置：加密	添加或导入可以用于一台或多台受保护机器的加密密钥	单击 加密密钥 ，通过添加或导入加密密钥管理受保护数据的安全性。可以将加密密钥应用到一台或多台受保护的机器。有关加密的信息，请参阅主题 了解加密密钥 。
配置：通知	设置事件、警告和警报的通知	单击 事件 将指定事件、警告和警报的通知组。要通过电子邮件发送通知，您还必须创建 SMTP 服务器设置。有关管理事件的更多信息，请参阅主题 事件 ，包括 配置通知组 和主题 配置电子邮件服务器 。
配置：保留	查看或更改 Core 的默认保留策略	单击 保留策略 以打开 Core 的“保留策略”页面。您可以在此定义汇总前恢复点保持的时间长短。有关保留策略的概念信息，请参阅主题 管理老化数据 。有关过程信息，请参阅 管理保留策略 。
还原	从 Core 上的恢复点还原数据	单击 还原 以打开“还原机器向导”。有关还原数据的信息，请参阅主题 关于从恢复点还原卷 。

隐藏快速入门指南

首次升级到或安装 Rapid Recovery Core 时，将自动显示“快速启动指南”。

从“帮助”下拉菜单中选择“快速启动指南”及每次访问 Core Console 上的“主页”页面时，也会显示该指南。

要隐藏“快速入门指南”，请使用以下过程。

- 在 Rapid Recovery Core Console 中，如果正在查看“快速启动指南”的**欢迎**页面，请执行以下操作：
 - 如果要隐藏“快速启动指南”的**欢迎**页面，请选择**不再显示**。

① 注：下次及每次打开“快速启动指南”时，此选项将隐藏欢迎页面，直到升级 **Rapid Recovery Core** 为止。
如果选择隐藏此页面，并希望以后访问高级选项，则选择向导中的**返回**查看此隐藏页面。

- 如果要隐藏此会话的“快速入门指南”，则单击**关闭**。
此时将关闭“快速入门指南”。下次访问 Core Console 上的“主页”页面时，将重新显示“快速启动指南”。

您还可以从“帮助”菜单中打开快速入门指南。

- 在“快速入门指南”的任意页面中单击**退出指南**。
此时将关闭“快速入门指南”。如果选择此选项，则仍可以从“帮助”菜单中打开“快速入门指南”。

导航 Rapid Recovery Core Console

当登录 Core Console 并单击**主页**  时，将显示**主页**页面。**主页**页面为您提供 Rapid Recovery Core 视图和两个选项。在主查看区域中，默认内容为新的 Core 仪表板，其中显示您的系统上的一组实时报告。默认仪表板报告包括最新传输作业状态、每个机器传输、存储库概览以及受保护机器、复制的机器和仅有恢复点机器的连接状态。或者，您可以切换到经典“摘要表”视图。在此视图中，页面标题显示 Rapid Recovery Core 的显示名称，并且您可以看到摘要表，其中显示受保护机器、存储库和最近的警报。有关更多信息，请分别参阅[了解“主页”页面（摘要表视图）](#)和[了解 Core 仪表板](#)。

在**主页**页面上（和 Core Console 中的每个页面上），左侧导航区域显示在 Core 上受保护的项目。您可以通过执行以下操作之一来导航到 UI 中的其他页面：

- 从左侧导航区域中的图标栏单击相应的图标。可从图标栏访问的选项包括“复制”、“Virtual Standby”、“事件”、“设置”和“更多”。
- 在图标栏上展开 （更多）菜单，然后选择目标
- 从按钮栏中单击一个按钮或菜单选项。按钮包括“保护”、“还原”、“存档”和“复制”。

当您从左侧导航区域选择一个项目时，Core Console 的焦点将变为显示有关该项目的摘要信息。例如，如果您单击受保护机器的名称，Core Console 将仅显示有关该机器的信息，而不是有关 Core 的信息。在本例中，受保护机器的显示名称显示为页面标题。子菜单会出现在右侧，可让您查看有关受保护机器的特定信息。菜单选项包括：“摘要”、“恢复点”、“事件”、“设置”、“报告”和“更多”。

要返回查看有关 Core 的信息，包括仪表板报告或多台受保护或复制机器的摘要视图，请单击 UI 左上角的主页  图标。在**主页**页面上，您可以单击页面右上角的红色链接来在仪表板视图和摘要页面视图之间切换。

您可以使用 Core Console 顶部的标题为您正在 Core 中查看的信息提供上下文。例如：

- 每当您看到 Core 的显示名称或 IP 地址用作页面标题时，即表明您正在查看有关 Core 的摘要信息。
- 如果标题为“仪表板”，即表明您正在查看 Core 仪表板。
- 如果您在页面顶部看到受保护机器的显示名称或 IP 地址或者“摘要”窗格，即表明您正在查看有关受 Core 保护或在 Core 中复制的单台机器的信息。
- 如果您看到标题“受保护机器”，即表明您正在查看有关 Rapid Recovery Core 中所有受保护机器的信息。
- 如果您看到标题“机器复制自...”，即表明您正在查看有关在 Rapid Recovery Core 中复制的所有机器的信息。
- 如果您看到页面标题“仅有恢复点”，即表明您正在查看有关此 Core 上所有仅有恢复点的机器的信息。

有关可从每个页面上获取的特性和功能的信息，请查看以下相应部分。

有关查看受保护机器的更多信息，请参阅[查看“受保护机器”菜单](#)。有关管理受保护机器的更多信息，请参阅[管理受保护机器](#)。

有关查看复制机器的更多信息，请参阅[查看传入和传出复制](#)。

有关查看仅有恢复点的机器的更多信息，请参阅[查看“仅限恢复点”菜单](#)

了解左侧导航区域

Core Console 的左侧导航区显示在用户界面的左侧。此导航区域中的内容可能会有所不同，具体取决于您的 Rapid Recovery Core 中保护的对象类型。

左侧导航区域始终包含以下内容：

- **图标栏**。用于在 Core Console 的主页面之间进行导航。
- **文本筛选器**。文本筛选器是一个文本字段，该字段可让您筛选在其下出现的各种菜单中显示的项目。单击文本筛选器右侧的箭头可展开和折叠其下出现的每个菜单。

在这些元素之后，左侧导航区域一般会显示菜单来帮助您导航，筛选和查看 Core 上受保护的物体。这包括受保护机器、被复制的机器等。

每个菜单均为上下文相关；也就是说，每个菜单仅在相关时才显示在 Core Console 中。例如，如果您保护至少一个机器，将显示“受保护机器”菜单，以此类推。

有关更多信息，请参阅[查看 Core Console 用户指南](#)中的左侧导航区域表。

查看 Rapid Recovery Core Console 主页页面

每次登录到 Rapid Recovery Core Console 或每次单击图标栏中的[主页](#)  图标时，均会显示[主页](#)。

Core Console 的[主页](#)页面提供一个新的[仪表板](#)视图和熟悉的[摘要表](#)视图。仪表板为默认视图。

您可以通过单击[主页](#)页面右上方的红色链接，在[主页](#)页面上的视图之间切换。

在“主页”页面和 Core Console 的其他各页面中，您可以通过利用左侧导航区域导航到您想要的功能。

有关更多信息，请参阅以下主题：

- [了解左侧导航区域](#)
- [了解 Core 仪表板](#)
- [了解“主页”页面（摘要表视图）](#)

了解“主页”页面（摘要表视图）

[主页](#)页面仅适用于 Core。在仪表板视图中，它显示实时图形报告。当切换到摘要表视图时，[主页](#)页面显示 Core 保护或复制的所有机器、与您的 Core 关联的存储库以及此 Core 上的机器警报。

[主页](#)页面上每个窗格的视图可展开或收缩。例如，如果单击“受保护机器”窗格右上角的  （收缩视图）图标，则受保护机器的视图将收缩，仅窗格的名称可见。要展开视图以再次查看所有受保护机器，请单击  （展开视图）图标。

下表介绍了当处于摘要表视图时[主页](#)页面上的各种元素。

表. 3: “主页”页面选项

UI 元素	说明
受保护机器	“受保护机器”窗格列出了此 Core 保护的机器。无论是否有任何机器已添加到您的 Core 中保护，此窗格都会显示。 此部分包括每台受保护机器的以下信息： • 机器类型。图标显示机器是物理机器、虚拟机还是受保护的群集。 • 状态。“状态”列中的彩色圆圈显示受保护机器可访问、已暂停还是脱机且不可访问。 • 显示名称。受保护机器的显示名称或 IP 地址。 • 存储库名称。存储该机器恢复点的存储库名称。 • 上次快照。Rapid Recovery 为该机器创建最近的恢复点快照的日期和时间。 • 恢复点。存储在存储库中的恢复点数量以及每个受保护机器的空间使用。 • 版本。该机器上安装的 Rapid Recovery Agent 软件版本。

如果您单击此窗格中显示的特定机器名称，此时将显示“摘要”页面，其中显示所选机器的摘要信息。有关可以在“摘要”页面上完成内容的更多信息，请参阅[查看受保护机器的摘要信息](#)。

复制机器

“复制机器”窗格列出此 Core 从另一个 Core 复制的任何机器。除非您的 Core 从另一个 Core 复制机器，否则不会出现此窗格。

此部分包括每台复制机器的以下信息：

- **机器类型。**图标显示机器是物理机器、虚拟机还是受保护的群集。
- **状态。**“状态”列中的彩色圆圈显示复制机器可访问、已暂停还是脱机且不可访问。
- **显示名称。**复制的机器的显示名称或 IP 地址。
- **复制名称。**您在此目标 Core 上复制的任何机器的源 Core 的显示名称。当设置复制时，您可以定义此名称。
- **存储库名称。**存储该机器恢复点的存储库名称。
- **最后复制的快照。**Rapid Recovery 创建原始受保护机器的最新副本的日期和时间。
- **恢复点。**存储在存储库中的恢复点数量以及每台复制机器的空间使用。
- **版本。**该机器上安装的 Rapid Recovery Agent 软件版本。

如果单击此窗格中显示的特定机器，将出现“摘要”页面，显示该复制机器的摘要信息。

仅有恢复点的机器

“仅有恢复点的机器”窗格列出当已保留恢复点时已从保护或复制范围中删除的任何机器。这些机器可用于文件级别的恢复，但无法用于裸机还原、恢复整个卷或添加快照数据。除非您有任何机器符合此定义，否则不显示此窗格。

该部分包括仅限恢复点机器的以下信息：

- **机器类型。**图标显示机器是物理机器、虚拟机还是受保护的群集。
- **状态。**“状态”列中的彩色圆圈显示仅有恢复点的机器可访问、已暂停还是脱机且不可访问。
- **显示名称。**保留其恢复点的机器的显示名称或 IP 地址。
- **存储库名称。**存储该机器的恢复点的存储库的名称。
- **恢复点。**存储在存储库中的恢复点数量以及每个仅有恢复点的机器的空间使用。

如果单击此窗格中显示的特定机器，将出现此仅有恢复点的机器的“摘要”页面。

DVM 存储库

不管是否创建了任何 DVM 存储库，对于 DL1000 都会显示此窗格。除非您的 Core 有一个或多个 DVM 存储库，否则此窗格不会出现。

它包括每个 DVM 存储库的以下信息：

- **类型。**一个图标描述存储库。
 - **状态。**“状态”列中的彩色圆圈显示存储库已安装并可接受恢复点传输、不可访问还是处于错误状态。
 - **存储库名称。**存储库的显示名称。
 - **空间使用。**存储库中使用的总空间量以及存储卷的大小或区域。
 - **受保护数据。**存储库的已用空间容量。
 - **机器。**存储库存储其恢复点的机器数量。
 - **恢复点。**存储在存储库中的恢复点数量。
 - **压缩率。**存储库压缩数据以节省空间的比率。
- 有关更多信息，请参阅[了解存储库](#)。

警报

本部分列出了 Core 的重要警报和它保护的每台机器。本部分包括以下信息：

- **图标。**图标栏表示警报性质。这些包括信息性消息、错误
- **日期。**Rapid Recovery 发出警报时显示的日期和时间。
- **消息。**介绍警报。

您也可以在“Core 事件”页面上查看这些详细信息。有关更多信息，请参阅[使用任务、警报和日记查看事件](#)。

了解 Core 仪表板

Core 仪表板显示一组与 Core 和受保护机器相关的数据的实时图形报告。此仪表板包括以下报告：

- **传输作业。**此报告显示在过去 24 小时内已完成的所有快照数据传输（包括基本映像和增量快照）。快照包括基本映像和增量快照。此仪表板报告以圆形图显示。
- **每台机器的传输作业。**此作业显示受保护机器在过去 24 小时内成功和失败的传输作业数。此仪表板报告以线形图显示。
- **存储库。**此报告显示与您的 Core 关联的存储库。它将显示存储库数目、每个存储库中受保护机器的数量、恢复点数量以及压缩或重复数据消除的百分比。此报告每分钟刷新一次。
- **机器连接。**此报告显示受保护和已复制到 Core 上的机器的连接状态。它还会显示[仅有恢复点的机器](#)上的数据连接。

通过单击报告标题中的向上或向下箭头，您可以折叠或展开仪表板上的任何报告视图。一些仪表板报告（计算机连接和存储库）的箭头旁边有一个加号，通过该加号，您可以分别添加另一个受保护机器或另一个存储库。

您也可以通过拖放移动仪表板上其他报告的位置，以按您使用最有效的方式对报告进行排序。

查看“受保护机器”菜单

在 Rapid Recovery 用户界面中，“受保护机器”菜单显示在左侧导航区域中。与导航区域中的所有菜单标签一样，此菜单的标签会以字母全部大写方式显示。默认情况下，此菜单完全展开，并显示受此 Core 保护的机器列表。如果已保护任何服务器群集，它们都将包括在此列表中。

通过单击此菜单左侧的箭头，您可以折叠或展开 Core 中的受保护机器和服务器群集视图。

“受保护机器”菜单包括右侧的一个下拉菜单，其中列出可在所有受保护机器上执行的功能。单击[受保护机器](#)右侧的箭头可查看菜单及执行以下任何操作：

- 强制创建所有机器的增量快照
- 强制创建所有机器的基本映像
- 暂停对所有机器的保护（如果保护处于活动状态）
- 恢复对所有机器的保护（如果保护处于暂停状态）
- 刷新所有受保护机器的元数据
- 在 Core 上从保护范围中移除所有机器

“受保护机器”菜单中列出的每台机器也包括一个下拉菜单，仅控制该机器的功能。在任何机器的下拉菜单中，您可以执行以下操作：

- 强制创建所选机器的增量快照
- 暂停对所选机器的保护（如果保护处于活动状态）
- 恢复保护（如果保护处于暂停状态）
- 刷新元数据
- 在 Core 上从保护范围中移除所选机器
- 导航至所选机器的“摘要”页面
- 导航至所选机器的“恢复点”页面
- 导航至所选机器的“事件”页面
- 导航至所选机器的“设置”页面
- 生成特定于该机器的报告
- 访问特定于所选机器的更多功能，包括系统信息、安装、保留策略、通知或机器特定日志

- 创建“受保护机器”列表中显示的自定义标签

如果在 Rapid Recovery Core 中管理服务器群集，则群集也会显示在左侧导航菜单中。在任何群集的下拉菜单中，您还可以执行以下操作：

- 导航至所选群集的**受保护节点**页面

如果单击“受保护机器”菜单左侧的箭头，则会收缩受保护机器和服务器群集列表，且不会列出任何机器。再次单击此箭头将重新展开机器列表。

单击“受保护机器”菜单中的任何机器名称将打开该机器的“摘要”页面。有关可以在“摘要”页面上完成内容的更多信息，请参阅[查看受保护机器的摘要信息](#)。

最后，直接单击**受保护机器**菜单会导致主要内容区域中显示**受保护机器**页面，并具有单个窗格显示此 Core 上的受保护机器。有关可以在“受保护机器”页面的**受保护机器**窗格中完成的内容的更多信息，请参阅[查看 Protected Machines（受保护机器）面板](#)。

① | 注：从受保护机器页面中，您可以单击图标栏中的主页图标从 **Core** 角度返回到某个视图。

查看受保护机器的摘要信息

当您在 Core Console 中单击受保护机器的名称时，将显示**摘要**页面。在此页面上，至少包含一个**摘要**窗格和**卷**窗格。如果将某台机器添加到复制，也会显示**复制**窗格。

如果有一个或多个受保护 Exchange Server，您还将看到 **Exchange Server 信息** 窗格，其包含有关受保护 Exchange Server 的信息。

如果有一个或多个受保护 SQL Server，您还将看到 **SQL Server 信息** 窗格，其包含有关受保护 SQL Server 的信息。

此页面顶部是您可以在受保护机器上执行的操作的菜单。在页面下面，至少显示一个“摘要”窗格和“卷”窗格。如果将某台机器添加到复制，也会显示“复制”窗格。

当在“摘要”页面和所有其他视图上显示受保护机器的信息时，页面顶部会显示一个菜单以及您可以执行的功能。此菜单显示在受保护机器的名称正下方。

相关链接

- [查看“摘要”窗格](#)
- [查看受保护计算机上的卷](#)
- [查看复制信息](#)
- [查看“Exchange Server 信息”窗格](#)
- [查看“SQL Server 信息”窗格](#)

查看“摘要”窗格

摘要窗格包含有关受保护计算机的摘要信息，其中包括主机名、最后一次快照的日期和时间、下一次计划快照的日期和时间、加密密钥信息和 Rapid Recovery Agent 软件的版本信息。还有指向详细的计算机“系统信息”页面的链接。

查看受保护计算机上的卷

对于任何受保护计算机，从“摘要”页面“卷”窗格中，您可以为列出的任何卷执行以下操作：

- 为选定的卷设置或修改保护计划。通常在第一次保护机器时，就会创建保护计划。有关修改保护计划的更多信息，请参阅[修改保护计划](#)。
- 强行执行基本映像或快照。快照通常根据保护计划发生。然而，在任何时候，您可以为所选卷强制基本映像或增量快照。有关更多信息，请参阅[强制创建快照](#)。

查看复制信息

复制窗格包含关于复制计算机的摘要信息，包括复制名称、复制状态、进度和可用空间。

查看“Exchange Server 信息”窗格

仅为属于 Exchange Server 的受保护机器显示 **Exchange Server 信息**窗格。

此窗格包含关于受保护 Exchange Server 的摘要信息，包括已安装的 Microsoft Exchange 版本、Exchange 的安装路径以及为 Exchange 邮箱数据定义的路径。

“邮件存储”网格显示了 Exchange 数据库 (EDB) 名称、EDB 文件的路径、日志文件的存储路径、日志前缀、系统路径、数据库可用性组 (DAG) 和邮件存储类型。

查看“SQL Server 信息”窗格

仅为属于 SQL Server 的受保护机器显示 **SQL Server 信息**窗格。

此窗格中包含有关受保护 SQL Server 的摘要信息。您可以展开数据库信息以查看数据库中的每个表的详细信息。您还可以查看数据库或表名称以及数据库路径。

查看计算机的恢复点

“恢复点”页面显示为受保护机器收集的恢复点列表，以及相关机器和存储库数据。在该页面中，您可以安装、导出和还原特定恢复点，以及删除恢复点。

该页面分为两个窗格：“恢复点摘要”和“恢复点”。“摘要”窗格不包含任何可操作链接。它只显示以下机器数据。

表. 4: “恢复点摘要”窗格数据

UI 元素	说明
恢复点总计	为此特殊受保护机器收集的恢复点的数量。
受保护数据合计	受保护机器上的数据量存储在该存储库中。
存储库	Rapid Recovery 在其中存储该受保护机器恢复点的存储库名称。
存储库状态	进度条显示存储库已使用总空间的百分比。已使用数据量和存储库总容量将显示进度条下方。

有关更多信息，请参阅[查看 Protected Machines（受保护机器）面板](#)。

查看受保护机器的事件

在**事件**页面上，您可以查看选定受保护机器上的已发生或正在进行的作业。页面顶部的按钮，可导航至三个类别活动中的作业列表：

- **任务。**为使操作成功，Rapid Recovery 必须执行的作业。
- **警报。**与任务或事件相关的包含错误和警告的通知。
- **日记。**所有受保护机器的任务和警报的组合。

下表包含**事件**页面上每个元素的介绍。

表. 5: “事件”页面元素

UI 元素	说明
搜索关键字	可在每一类中搜索指定项目。仅可用于任务。
发件人	为缩小结果范围，您可以输入开始搜索的日期。仅可用于任务。
收件人	为缩小结果范围，您可以输入停止搜索的日期。仅可用于任务。
状态图标	每个图标表示不同的作业状态。对于警报和任务，通过单击其中一个图标，您可按该状态筛选列表，本质上可生成报告。再次单击图标将移除筛选的状态。您可以通过多个状态进行筛选。状态包括： • 活动。正在进行的作业。 • 排队。一项作业开始前须等待另一作业完成。 • 正在等待。等待您批准或完成的作业，如种子驱动器。（有关种子驱动器的更多信息，请参阅复制。） • 完成。成功完成的作业。 • 失败。失败并未完成的作业。
服务图标	该按钮将服务作业添加到作业列表中。单击此图标时，每个状态图标上将显示一个较小的服务图标，可以让您筛选具有这些状态的服务作业（如果存在）。服务作业包括删除索引文件或移除机器保护。
导出类型下拉列表	下拉列表包含可以导出事件报告的格式。仅可用于任务。它包括以下格式： • PDF • HTML • CSV • XLS • XLSX
 （导出图标）	将事件报告导出到选择的格式。仅可用于任务。
页面选择	事件报告可以包括多个页面的多个作业。 事件 页面底部的数字和箭头可让您导航报告的其他页面。

事件页面显示表中的所有事件。下表列出了为每个项目显示的信息。

表. 6: “事件”摘要表的详细信息

UI 元素	说明
状态	显示任务、警报或日记项目的状态。可用于警报或日记项目，单击标题以按状态筛选结果。
名称	名称仅可用于任务。此文本字段列出了为这台受保护机器完成的作业类型。示例包括卷的传输、维护存储库、汇总、执行可安装性检查、执行校验和检查，等等。
开始时间	可用于任务、警报和日记项目。显示了作业或任务开始时的日期和时间。
结束时间	仅可用于任务。显示了任务完成时的日期和时间。
 作业详细信息	仅可用于任务。打开 监控活动任务 对话框，使得您可以查看特定作业或任务的详细信息。这些详细信息包括作业 ID、Core 传输数据的速率（如果相关）、作业完成经过时间、总工作量（以 GB 为单位）以及与作业关联的所有子任务。
Message（消息）	可用于警报和日记项目。此文本字段提供了警报或日记项目的描述性消息。

查看受保护机器的报告

使用  下拉菜单可为选定的受保护机器按需生成报告。

“作业”报告提供了有关所选机器的成功作业和失败作业状态的报告。可以在失败报告中进一步查看失败的作业。有关此报告类型的更多信息，请参阅[了解“作业”报告](#)。

“失败”报告提供了有关指定机器的失败和已取消 Core 作业的信息。有关此报告类型的更多信息，请参阅[了解失败报告](#)。

有关生成这些报告的更多信息，请参阅[按需生成 Core 报告](#)。

从导航菜单查看被复制的机器

如果您的 Core 从另一个 Rapid Recovery Core 复制机器，则源 Core 的显示名称将在 Core Console 的左侧导航区域中显示为可折叠菜单。与导航区域中的所有菜单标签一样，此复制机器菜单名称会以所有字母大写的形式显示在“受保护机器”菜单下方。默认情况下，复制的机器菜单将完全展开并列出来自该源 Core 的、在您的目标 Core 上复制的所有机器。

通过单击此菜单左侧的箭头，您可以折叠或展开来自该源 Core 的复制机器的视图。

每个复制的机器菜单都在右侧包含了一个下拉菜单，其中包括了可同时在来自该源 Core 的所有复制机器上执行的功能。单击复制的机器菜单右侧的箭头以查看您可以执行的功能的下拉式列表。其中包括以下操作：

- 暂停复制。如果复制目前处于活动状态，此操作会在您恢复之前停止复制。
- 恢复复制。如果复制已暂停，此操作将再次开始复制。
- 强制复制。按需复制，而非按计划时间复制。
- 移除复制。删除源 Core 和目标 Core 之间的复制关系。（可选）您可以删除此 Core 中存储的恢复点。有关详情，请参阅[移除复制](#)。

直接单击导航菜单中的源 Core 名称会导致从 **[源 Core 名称] 复制的机器** 页面显示在主要内容区域中。有关可以在该页面上实现的功能的详细信息，请参阅[查看传入和传出复制](#)。

相关链接

[暂停和恢复复制](#)

[强制复制](#)

[移除复制](#)

查看“仅限恢复点”菜单

如果满足以下其中一个条件，则“仅有恢复点”菜单会显示在左侧导航区域中：

- 如果您的 Rapid Recovery Core 保留来自以前受到保护的机器的一些恢复点
- 如果您删除了复制，但保留了恢复点。

与导航区域中的所有菜单标签一样，此菜单的标签全部以大写字母形式显示。

通过单击此菜单左侧的箭头，您可以折叠或展开仅限恢复点机器的视图。

菜单包括右侧的一个下拉菜单，其中列出可在所有仅限恢复点机器上同时执行的功能。在这种情况下，可执行的唯一功能是从 Core 移除恢复点。

 **小心:** 该操作将删除 **Rapid Recovery Core** 中所有仅有恢复点的机器，永久删除，防止从该 **Core** 中的这些恢复点还原信息。

查看自定义群菜单

只有您已定义一个或多个自定义组，“自定义组”菜单才会出现在左侧导航区。与导航区域中的所有菜单卷标一样，此菜单的卷标全部以大写字母形式显示。

通过单击其左侧的箭头，您可以折叠或展开此菜单中的项目。

“自定义组”菜单包括右侧的一个下拉菜单，其中列出可在该组中所有类似项目上同时执行的功能。

有关详情，请参阅[了解自定义组](#)。

使用“错误”对话框

Rapid RecoveryRapid Recovery Core Console 用户界面中出错时，例如尝试输入一个无效的参数，会出现一个“错误”对话框。对话框通常显示错误的原因，包括提供有关错误更多信息的链接和一个关闭按钮。您必须在继续前关闭“错误”对话框，但您可能想查看有关错误的更多信息。

在“错误”对话框中，选择以下选项：

用户界面错误引起的“错误”对话框显示无法在 Rapid Recovery“事件”选项卡中进行跟踪，因为它们只是验证或数据录入错误。然而，当您单击“搜索知识库”选择查找错误时，那么该错误提供的 URL 链接将记录到 CoreAppRecovery.log 文件中。您可以使用文本字符串“URL 生成的 KB 文章”搜索日志，以在浏览器中查看 URL 的每个错误。有关下载或查看 Core 错误日志的详细信息，请分别参阅主题[下载并查看 Core 日志文件](#)或[访问 Core 日志](#)。

Core 设置

本节介绍了如何从  “设置”图标管理和更改 Rapid Recovery Core 的设置。

Rapid Recovery Core 设置

Rapid Recovery Core 设置默认情况下已配置，用于为大多数用户提供最佳性能。这些设置会影响 Rapid Recovery Core 的性能，或是

在某些情况下影响 Rapid Recovery Core Console 中信息的显示。从图标栏中，单击  （设置）以访问 Core 设置。所有 Core 设置的列表显示在左侧。您可以从此列表单击任何设置的标题以跳转至右侧该设置的完全配置。或者，您也可以向下滚动浏览右侧的所有 Core 设置以查看所有配置选项。有关更多信息，请参阅 [Rapid Recovery Core 设置](#)。

您也可以访问 Core 工具，例如，查看系统信息摘要或下载 Core 日志文件。有关更多信息，请参阅 [Core 级工具](#)。

您可以配置的 Rapid Recovery Core 设置完整集在下表中有介绍。

表. 7: Rapid Recovery Core 可配置设置

配置设置	说明
备份和还原 Core 配置	Rapid Recovery 可让您将 Core 配置设置备份到 XML 文件。如果您有备份文件，您可以用以还原或迁移 Core 设置。

配置设置	说明
	有关备份和还原 Core 设置的更多信息，请参阅 备份并还原 Core 设置 。
常规	常规设置包括普遍用于 Rapid Recovery Core 的配置选项，包括显示选项以及用于 Web 服务器和 Rapid Recovery 服务的端口。 有关 Rapid Recovery Core 常规设置的更多信息，包括如何配置这些设置，请参阅配置 Core 常规设置。
更新	更新设置控制自动升级功能的各方面，检查更新的 Rapid Recovery 软件版本。 有关更新 Rapid Recovery Core 设置的更多信息，包括如何配置这些设置，请参阅配置更新设置。
每夜作业	每夜作业设置是 Core 每天都会执行的自动任务。您可以配置工作的开始时间和要执行的作业。Dell 建议计划正常营业时间外的作业，以在资源需求高的时候降低系统负载。 有关更多信息，请参阅了解每夜作业、配置 Core 的每夜作业和自定义受保护机器的每夜作业。
传输队列	如果因缺少资源而无法作业，传输队列设置控制传输操作尝试的次数。可用于确定传输数据的最大并发传输数和最大重试次数。 有关传输队列设置的更多信息，请参阅修改传输队列设置。
客户端超时	客户端超时设置可确定特定连接请求前的时长或超时前尝试读取和写入操作的时长。 有关客户端超时设置的更多信息，请参阅调整客户端超时设置。
DVM 清除重复项缓存	重复数据清除确保信息独特块只在存储库中存储一次，创建重复数据块的引用。引用存储在重复数据清除缓存中。如果使用加密密钥，则重复数据清除在每个加密域中都会发生。 DVM 重复数据清除缓存设置允许您配置大小并指定主要和次要高速缓存的位置，以及元数据高速缓存的位置。 有关清除重复项缓存的更多信息，请参阅了解清除重复项缓存大小和存储位置。有关调整设置的信息，请参阅配置 DVM 清除重复项缓存设置。
Replay 引擎	Replay 引擎设置控制有关 Replay 引擎通信通道的信息（比如 IP 地址和超时设置），以帮助调整特定于您网络需求的性能。 有关 Rapid Recovery 引擎设置的更多信息，请参阅配置 Replay 引擎设置。
部署	部署设置使您能够设置用于将 Rapid Recovery Agent 软件从 Core 部署到想要保护的机器的选项。 有关配置部署设置的更多信息，请参阅配置部署设置。
数据库连接	Rapid Recovery 将交易信息存储在 MongoDB 服务数据库中，该数据库默认本地安装在 Core 机器上。您可以配置这些设置以更改数据库中保留信息的时间长短，或更改连接池大小允许更多或更少的并发连接。 有关建立或修改用于服务数据库的数据库连接设置，请参阅配置数据库连接设置。
本地数据库	Rapid Recovery 在“事件”页面上显示有关 Core 任务、事件和警报的信息。Rapid Recovery 存储 MongoDB 服务数据库中的该交易信息，其本地安装在与 Rapid Recovery Core 相同的机器上。 您可以使用本地数据库设置，配置用于本地 Mongo 服务数据库的凭据信息（用户名和密码）。有关调整本地数据库设置的更多信息，请参阅修改本地数据库连接设置。
SMTP 服务器	配置用于 Core 的简单邮件传输协议 (SMTP) 服务器设置，您也可以通过电子邮件发送 Core 事件信息。 有关配置 SMTP 电子邮件服务器的更多信息，请参阅配置电子邮件服务器。 注: 要通过电子邮件发送事件信息，您还必须配置通知组设置。有关指定事件以接收电子邮件警报的更多信息，请参阅配置通知组。
云配置	使用“云配置”设置可以为受支持的云存储帐户指定配置设置。这些设置不会创建云帐户。然而，它们将现有云存储帐户与您的 Rapid Recovery Core 相关联以方便执行操作，如存档 Rapid Recovery 信息。

配置设置	说明
	有关管理 Rapid Recovery Core 中云存储帐户信息的更多信息，请参阅 管理云帐户 。
报告	报告设置包括单个配置参数，可用于选择在从 Rapid Recovery Core 生成报告时使用的字体。 有关更改端口设置的更多信息，请参阅 管理报告设置 。
可附加性	可附加性设置让您能够指定是否在受保护机器上执行 SQL 可附加性检查或者是否在 Core 上使用 SQL Server 实例。如果在 Core 上指定 SQL，您必须提供凭据信息。 有关如何管理 Core 的 SQL 可附加性设置的更多信息，请参阅 管理 Core SQL 可附加性设置 。
作业	每次启动复制等操作时，便会自动创建 Core 作业。您可以使用 Core 作业设置指定每个作业的设置。 您可以配置一次性执行的作业数量。为防止网络或其他通信错误阻止作业一次性成功，您可以使用尝试计数设置来设置应尝试作业的次数。 有关可用的 Core 作业，以及如何配置它们的更多信息，请参阅 Core 作业设置 。
许可	在 Core Console 中，Rapid Recovery 可用于更改与 Core 关联的许可证、限制每天快照数、查看许可证池信息以及联系许可证服务器。 有关从 Core 上管理许可证的更多信息，请参阅 管理许可证 。 有关管理许可证的更多信息，请参阅“Dell Data Protection Rapid Recovery 许可证门户 User Guide”（《Dell Data Protection Rapid Recovery 许可证门户用户指南》）。 ❗ 注: Dell Data Protection Rapid Recovery 许可证门户的发行周期不同于 Rapid Recovery 软件。有关最新的产品说明文件，请参阅 Dell 技术说明文件页面。
SNMP 配置	简单网络管理协议 (SNMP) 是 IP 网络上的一种用于管理设备的协议。您可以将 Rapid Recovery Core 配置为 SNMP 代理。然后 Core 可以报告警报、存储库状态和受保护机器等信息。 有关将 SNMP 与 Rapid Recovery 一起使用的更多信息，请参阅 了解 SNMP 设置 。
vSphere	vSphere Core 设置仅适用于虚拟机无代理保护用户。如果使用 vSphere 主机，这些设置包括应用到虚拟机的连接设置。 有关 VMware 或 ESXi 无代理保护的 vSphere 设置的更多信息，请参阅 配置 vSphere 设置 。
日志上载	当此选项设置为“是”时，Rapid Recovery Core 会持续将日志文件上载给 Dell 进行分析，以提高整体产品质量。此设置是可选的。

配置 Core 常规设置

Rapid Recovery Core 的常规设置包括 Core 显示名称、Web 服务器端口、服务端口和区域设置（Core Console 显示语言）。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**常规**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“常规”标题。
此时将显示常规 Core 设置。
- 3 单击您想要更改的常规设置。
您选择的设置将变为可编辑，采用文本字段或下拉菜单形式。
- 4 根据下表中的说明输入配置信息。

表. 8: 常规设置信息

文本框	说明
显示名称	输入 Core 新的显示名称。此名称将显示在 Rapid Recovery Core Console 中。最多可输入 64 个字符。
Web 服务器端口	输入 Web 服务器的端口号。默认端口号为 8006。
服务端口	输入 Rapid Recovery Core 服务的端口号。默认端口号为 8006。
区域设置	在“区域设置”下拉式列表中，选择您想要显示的语言。 您可以从英语、法语、德语、日语、韩语、葡萄牙语、简体中文和西班牙语中选择。

注: 如果更改语言，请确认信息，该信息表示在更新语言可在 Core Console 中显示之前必须重启 Rapid Recovery Core 服务。您可以从 Windows 任务管理器中重新启动此服务。

- 5 对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。

配置更新设置

Rapid Recovery 包括自动更新功能。安装 Rapid Recovery Core 时，您可以选择在新的更新可用时是否自动更新 Rapid Recovery Core 软件以及系统检查更新的频率。

Rapid Recovery 版本编号通常包括四部分信息，用小数点分隔：主要版本号、次要版本号、修订和内部版本号。例如，Rapid Recovery 的第一个更名版本是 6.0.1.609。下一版本是 6.0.2.142。

自动更新功能会比较版本号中的所有数字。如果启用自动更新，只有主要版本号与次要版本号一致时，Core 软件才会在没有干预的情况下更新。例如，从 Core 版本 6.0.1.609 到 6.0.2.142（均以 6.0 开头）会进行自动更新。在同一台机器上，Core 不会从 6.0.2.142 自动更新至 6.1.1.XXX，因为第一个小数点后的数字不相等。系统会改为（通过 Core Console 顶部的横幅）通知您，Core 软件有更新可用。通过此通知，您可以查看发行说明，并确定更新到最新 Core 版本是否适合您的需求。

注: 有关安装 Rapid Recovery Core 软件的信息，请参阅“Dell Data Protection | Rapid Recovery Installation and Upgrade Guide”（《Dell Data Protection | Rapid Recovery 安装和升级指南》）。

您可以随时查看和更改系统用于检查更新的设置。

小心: 使用复制时，配置系统以自动安装更新可能会导致源 Core 在目标 Core 之前升级，这可能会导致无法复制或无法设置 Core 之间的新复制。对于复制用户，Dell 建议管理员仅将自动升级应用于目标 Core，然后手动升级源 Core，最后升级受保护机器。

要配置更新设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**更新**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“更新”标题。
此时将显示更新 Core 设置。
- 3 单击您想要更改的设置。
您选择的设置将变为可编辑。
- 4 根据下表中的说明输入配置信息。

表. 9: 更新设置信息

文本框	说明
检查新的更新	选择 Rapid Recovery 检查并安装更新的频率。可以从以下选项中选择： • 从不 • 每天 • 每周 • 每月 如果您选择自动更新，在所选时间阈值过后，如果更新可用，它将在每夜作业已完成之后安装。
安装更新	要指定可用更新处理更新的方式，请选择以下选项之一： • 从不检查更新 • 更新时通知我，但不自动安装更新 • 自动安装更新
状态	状态指明是否有任何新更新可用。
上次检查	“上次检查”字段指明系统上次检查更新的日期和时间。 单击 立即检查 以立即验证是否有软件更新可用。无论您设置的频率如何，都会执行此检查。

5 对于每项设置，当对所做的更改满意时，请单击  以保存更改并退出编辑模式，或单击  退出编辑模式而不保存。

了解每夜作业

每夜作业是每天在正常办公时间之外的预定时间发生的自动化任务。这些作业是内存密集型的，并包括最适合在 Rapid Recovery Core 是不太活跃时执行的各种完整性检查和数据整合任务。

下表中介绍了所有每夜作业以及其适用的范围。每夜作业可在 Core 级别进行管理（这适用于 Core 上所有受保护机器）。这些也可应用于特定受保护机器的每夜作业会将范围列为“受保护机器”。

表. 10: 每夜作业信息

作业名称	范围	说明
 更改	不适用	此控件可打开 Nightly Jobs（每夜作业）对话框，您可在其中启用、禁用或更改每个每夜作业的设置。
Nightly jobs time（每夜作业时间）	全部	此设置代表每夜作业计划开始运行的时间。Dell 建议在活动较少的时间配置您的 Core 以运行每夜作业。 默认时间为 12:00 AM。
Rollup（前滚）	Core 或受保护机器	将保留策略应用于所备份数据，方法是结合使用或“汇总”策略中规定的计划上的恢复点。您可以在 Core 上自定义策略，这默认适用于所有受保护机器。默认情况下，汇总作业可对整个 Core 运行；或单击  定义要使用 Core 策略汇总哪些受保护机器。 有关使用受保护机器上不同于 Core 中设置的默认策略的保留策略，请参阅 自定义受保护机器的保留策略设置 。
Check attachability of SQL databases（检查 SQL 数据库的可附加性）	受保护机器	检查包含 SQL 数据库的恢复点的完整性。过程如下： • 为包含数据库的保护组安装最新的恢复点。 • 从 SQL Server 连接到数据库。 • 打开数据库。

作业名称	范围	说明
		- 关闭数据库。 - 卸载恢复点。 要启用此每夜检查，请指定一个 SQL Server 实例以便对受保护机器上的 SQL Server 数据库执行可附加性检查。 ① 注: 如果您没有保护您的 Core 中 SQL Server，则不显示此选项。
Download logs from protected machines (从受保护机器下载日志)	Core	受保护机器的日志会下载到 Core，以便可将其发送到日志记录服务器。
Consolidate VMware snapshots for protected virtual machines (整合受保护虚拟机的 VMware 快照)	Core 或受保护机器	在没有 Rapid Recovery Agent 软件的情况下，如果您使用本机 VMware API 来保护机器，则此每夜作业是相关的。 您应定期整合 VMware 快照。启用此每夜作业可允许您每日执行这些整合。此每夜作业包含一个参数，Maximum simultaneous consolidations (最大同步整合数)，它必须设置为一个介于 1 和 100 之间的数。
Check integrity of recovery points (检查恢复点的完整性)	Core 或受保护机器	检查每个受保护机器恢复点的完整性。默认情况下，未启用 Check integrity of recovery points 选项。 过程如下： - 安装每个保护组的最新恢复点。 - 枚举每个卷的文件和文件夹。 - 检查恢复点，以确保它们有效。 - 卸载恢复点。
Check checksum of Exchange databases (检查 Exchange 数据库的校验和)	受保护机器	检查包含 Exchange 数据库 (EDB) 文件的恢复点的完整性。 ① 注: 如果您没有保护您的 Core 中 Exchange Server，则不显示此选项。
Truncate SQL logs (simple recovery model only) (截断 SQL 日志 (仅适用于简单恢复模式))	受保护机器	维护 SQL Server 日志的大小，方法是截断数据库事务日志以匹配最后一个恢复点。 ① 注: 如果您没有保护您的 Core 中 SQL Server，则不显示此选项。
Truncate Exchange logs (截断 Exchange 日志)	受保护机器	维护 Exchange 日志的大小，方法是截断数据库事务日志以匹配最后一个恢复点。 ① 注: 如果您没有保护您的 Core 中 Exchange Server，则不显示此选项。
Log repository statistics (记录存储库统计信息)	Core	将存储库统计信息发送至日志记录服务器。

作业名称	范围	说明
Delete old events and jobs（删除旧的事件和作业）	Core	通过删除旧事件，维护事件数据库的规模。天数是可配置的，默认为 30 天。

配置 Core 的每夜作业

当 Rapid Recovery Core 上的每夜作业选项启用时，选定的作业每天将在为受 Core 保护的所有机器指定的时间执行一次。相反，如果禁用 Core 级别的每夜作业，则指定的每夜作业将不再为受 Core 保护的机器执行。

① 注: 如果按照[了解每夜作业](#)主题所述，每夜作业的范围包括受保护机器，您只能配置该每夜作业以分别应用于一台或更多特定受保护机器。有关将每夜作业设置应用到特定受保护机器的更多信息，请参阅[自定义受保护机器的每夜作业](#)。

因为每夜作业为内存密集型，Dell 建议配置 Core 以在不活跃的时候执行每夜作业。每夜作业默认的计划运行时间为上午 12 点。如果另有更合适的时间，请使用该过程更改“每夜作业时间”字段内的该设置。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从设置页面左侧的 Core 设置列表中，单击**每夜作业**。
 - 在设置页面右侧向下滚动，直至您可以看到“每夜作业”标题。此时将显示每夜作业 Core 设置。
- 3 要更改任何每夜作业或要更改每夜作业开始执行的时间，请单击  **更改**。此时将显示**每夜作业**对话框。
- 4 如果您想更改每夜作业的执行时间，请在**每夜作业时间**字段中输入新时间。
- 5 在第一列中，单击以选择您想要为 Core 设置的每个每夜作业选项。单击任何所选的选项以将其清除。
- 6 单击**确定**。
每夜作业将关闭，您的 Core 每夜作业设置将保存。

修改传输队列设置

传输队列设置是 Core 级设置，用于确定传输数据的最大并发传输数和最大重试次数。

要修改传输队列设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**传输队列**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“传输队列”标题。此时将显示传输队列 Core 设置。
- 3 单击您想要更改的设置。
您选择的设置将变为可编辑。
- 4 根据下表中的说明输入配置信息。

表. 11: 传输队列设置信息

文本框	说明
最大并发传输数	输入一个值以更新并发传输数量。

文本框	说明
	设置 1 至 60 之间的数字。数字越小，对网络和其他系统资源造成的负载也越小。随着所处理的代理数增加，对系统造成的负载也会增加。
Maximum Retries (最大重试次数)	输入一个值以设置在取消传输操作之前尝试的最大数量。 设置 1 至 60 之间的数字。

- 5 对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。

调整客户端超时设置

客户端超时设置控制在操作超时前尝试各种操作的时长。

① | 注: Dell 建议在环境中遇到问题前保持默认超时设置，建议您通过 Dell Support 代表更改设置。

要调整客户端超时设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击  (设置)，然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**客户端超时**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“客户端超时”标题。
此时将显示“客户端超时”核心设置。
- 3 单击您想要更改的设置。
您选择的设置将变为可编辑。
- 4 根据下表中的说明输入配置信息。
- 5

表. 12: 客户端超时设置信息

设置	说明
连接超时	通过超文本传输协议 (http) 发送数据时，控制 Core 和受保护机器之间的连接超时。 输入连接发生超时之前要等待的时间量。使用 HH:MM:SS 格式。
① 注: 默认设置为 0:05:00 或五分钟。	
读取/写入超时	通过 http 读取或写入流数据时，控制 Core 和受保护机器之间的连接超时。例如，为增量快照接收从受保护机器到 Core 更改的数据块。 输入读/写事件期间发生超时之前要等待的时间长度。使用 HH:MM:SS 格式。
① 注: 默认设置为 0:05:00 或五分钟。	
连接 UI 超时	控制通过 http 在图形用户界面和 Rapid Recovery Core 服务之间的连接超时。 输入连接 UI 发生超时之前要等待的时间长度。使用 HH:MM:SS 格式。
① 注: 默认设置为 0:05:00 或五分钟。	
读取/写入 UI 超时	控制通过 http 在图形用户界面和 Rapid Recovery Core 服务之间用于读取和写入数据流的连接超时。 输入读取或写入事件期间发生超时之前要等待的时间长度。使用 HH:MM:SS 格式。

 **注:** 默认设置为 **0:05:00** 或五分钟。

6 对于每项设置，当对所做的更改满意时，请单击  以保存更改并退出编辑模式，或单击  退出编辑模式而不保存。

了解清除重复项缓存大小和存储位置

全局重复数据消除可以减少 Core 备份数据所需的磁盘存储空间容量。每个存储库已重复数据清除，在磁盘上一次物理存储每个唯一的块，并且使用后续备份中块的虚拟引用或指针。为识别重复块，Rapid Recovery 为重复数据消除卷管理器 (DVM) 存储库提供了清除重复项缓存。高速缓存保留对唯一块的引用。

默认情况下，对于 DVM 存储库，此清除重复项缓存为 1.5 GB。此大小对于许多存储库是足够的。缓存超出时，数据将在存储库中进行重复数据清除。一旦冗余信息容量大到使清除重复项缓存变满，存储库不再为新添加数据进一步充分利用重复数据清除。清除重复项缓存填充根据备份数据类型变化（且每位用户都不同）前，数据量已经保存在存储库中。

您可以通过更改 Rapid Recovery Core 中的清除重复项缓存配置增加 DVM 清除重复项缓存的大小。有关如何增加高速缓存大小的更多信息，请参阅[配置 DVM 清除重复项缓存设置](#)。

当您增加 DVM 清除重复项缓存大小时，有两个因素需要考虑：磁盘空间和 RAM 使用情况。

磁盘空间。DVM 清除重复项缓存的两个副本存储在磁盘上：主要缓存和作为平行的副本的次要缓存。因此，如果对 DVM 存储库使用默认高速缓存大小 1.5 GB，则将使用您的系统中 3 GB 的磁盘存储。当增加高速缓存的大小，所使用的磁盘空间容量比例是高速缓存大小的两倍。为确保性能恰当并能够预防故障，Core 将动态更改这些高速缓存的优先级。两者都需要，唯一的区别是，指定的高速缓存作为主要高速缓存首先被保存。

RAM 使用情况。当 Rapid Recovery Core 启动时，它会将清除重复项缓存加载到 RAM 中。因此，高速缓存的大小影响您的系统的内存使用。Core 使用的总 RAM 量取决于许多因素。这些因素包括哪些操作正在运行、用户的数量、受保护机器的数量以及清除重复项缓存的大小。Core 执行的每项操作（传输、复制、汇总等）都会消耗更多的 RAM。操作完成后，内存消耗相应地减小。但是，管理员应该考虑高效操作最高的 RAM 负载要求。

Rapid Recovery Core 的默认设置将 DVM 存储库的主要高速缓存、次要高速缓存和元数据高速缓存放在 AppRecovery 目录中。此文件夹安装在 Core 机器上。

 **注:** 根据您的设置，AppRecovery 目录可能在 Rapid Recovery Core 上不可见。要查看此目录，您可能需要更改“文件夹选项”控制面板以显示隐藏文件、文件夹和驱动器。

假设 Rapid Recovery Core 安装在 C 驱动器上，这些位置通常如下：

表. 13: DVM 清除重复项缓存设置的默认存储位置

设置	默认存储位置
主要高速缓存位置	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
次要高速缓存位置	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
元数据高速缓存位置	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

您可以更改这些高速缓存的存储位置。例如，对于提高的故障容差，假如 Rapid Recovery Core 可以访问次要高速缓存（而不是主要高速缓存）的位置，则您可以更改此位置为不同的驱动器。

有关如何更改这些设置的存储位置的更多信息，请参阅主题[配置 DVM 清除重复项缓存设置](#)。

Dell 建议您单独规划重复数据消除存储。重复数据消除仅对单个存储库执行（而不跨多个存储库）。如果使用基于 Core 的加密，重复数据消除会进一步限制为受单个密钥保护的数据，因为出于安全目的，每个密钥用作一个加密域。

有关重复数据消除的更多信息，请参阅 [Rapid Recovery 中的重复数据消除](#)。

配置 DVM 清除重复项缓存设置

要配置 DVM 存储库的清除重复项缓存设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击 **DVM 清除重复项缓存**。只有当您的 Core 有一个或多个 DVM 存储库时，此设置才会显示。
 - 在“设置”页面右侧向下滚动，直至您可以看到“DVM 清除重复项缓存”标题。
此时将显示 DVM 清除重复项缓存 Core 设置。
- 3 如果您想要随时还原默认 DVM 清除重复项缓存设置，请执行以下操作：
 - a 在清除重复项缓存设置区域顶部，单击**还原默认值**。
此时将显示“还原默认值”对话框。
 - b 单击**是**确认还原。
- 4 单击您想要更改的设置。
您选择的设置将变为可编辑。
- 5 要更改个别清除重复项缓存设置，请根据下表中的说明输入配置信息。

表. 14: DVM 清除重复项缓存设置信息

设置	说明
 （还原默认值）	此控件将 DVM 高速缓存位置重设为系统默认位置，下面介绍了每个设置的系统默认位置。
主要高速缓存位置	如果想要更改 DVM 存储库的主要高速缓存的位置，则在“主要高速缓存位置”文本框中，输入可访问 Core 的存储位置路径。 默认位置为： C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache 由于主要高速缓存和次要高速缓存的大小相同，这两个缓存的共同存储所需的空间容量是分配给清除重复项缓存容量的两倍。例如，如果指定清除重复项缓存默认大小为 1.5 GB，请确保两个存储位置各自具有至少 1.5 GB。特别是，如果两个位置属于同一驱动器（例如，C 驱动器），则可用磁盘空间必须至少为 3.0GB。
次要高速缓存位置	如果想要更改 DVM 存储库的次要高速缓存的位置，则在“次要高速缓存位置”文本框中，输入可访问 Core 的存储位置路径。 默认位置为： C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
高速缓存元数据位置	如果想要更改 DVM 存储库的高速缓存元数据位置，则在“高速缓存元数据位置”文本框中，输入可访问 Core 的存储位置路径。 默认位置为： C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata
清除重复项缓存大小 (GB)	如果您想要更改 DVM 存储库的清除重复项缓存大小，请在“清除重复项缓存大小”文本框中输入新的容量（以 GB 为单位）。 默认位置为：

设置	说明
	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
	最小高速缓存大小设置为 1.5GB。此外，高速缓存大小不能超过已安装 RAM 的 50%。

6 对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。

配置 Replay 引擎设置

您可以配置有关 Replay 引擎的信息，这是 Rapid Recovery 的通信通道。这些设置可确定 Core 设置以提供有效通信。

一般来说，Dell 建议使用默认设置。在某些情况下，您可以直接通过 Dell Support 修改这些设置，以调整特定于网络需求的性能。

要配置 Replay 引擎设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击  （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击 **Replay 引擎**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“Replay 引擎”标题。此时将显示“Replay 引擎”核心设置。
- 3 单击您想要更改的设置。
您选择的设置将变为可编辑。
- 4 根据下表中的说明输入配置信息。

表. 15: Replay 引擎设置信息

文本框	说明
IP 地址	当为恢复点执行安装和还原以允许受保护机器和 Core 之间的反馈时，Core 使用此 IP 地址。Replay 引擎的 IP 地址将自动填充 Core 机器的 IP 地址。如果您手动输入服务器 IP 地址，则当受保护机器无法解析自动提供的 IP 地址时，将使用此值。 除非能够与 Core 通信的受保护机器遇到问题，否则您不需要手动设置此值。
首选端口	输入端口号或接受默认设置。默认端口号为 8007。 端口用于指定 Replay 引擎的通信通道。
使用中的端口	表示正用于 Replay 引擎配置的端口。
允许自动分配端口	单击以便允许自动分配 TCP 端口。
管理组	输入管理组的新名称。默认名称为 BUILTIN\Administrators。
最小异步 I/O 长度	输入一个值或选择默认设置。它描述了最小异步输入/输出长度。 默认设置为 65536。
读取超时	输入一个读取超时值或选择默认设置。默认设置为 00:05:00。
写入超时	输入一个写入超时值或选择默认设置。默认设置为 00:05:00。
接收缓冲区大小	输入一个入站缓冲区大小或接受默认设置。默认设置为 8192。
发送缓冲区大小	输入一个出站缓冲区大小或接受默认设置。默认设置为 8192。

文本框	说明
无延迟	建议取消选中此复选框，否则将会影响网络效率。如果确定需要修改此设置，请联系 Dell Support 获取执行此操作的指导。

- 5 对于每项设置，当对所做的更改满意时，请单击  以保存更改并退出编辑模式，或单击  退出编辑模式而不保存。

配置部署设置

Rapid Recovery 允许您将安装程序从 Rapid Recovery Core 下载到想要保护的机器上。

您可以将与 Rapid Recovery Agent 软件部署相关的设置从 Core 配置到要保护的机器上。

要配置部署设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**部署**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“部署”标题。
 此时将显示部署 Core 设置。
- 3 单击您想要更改的设置。
- 4 根据下表中的说明输入配置信息。

表. 16: 部署设置信息

文本框	说明
Agent 安装程序名称	默认文件名为 Agent-Web.exe。如果出于任何原因希望更改此文件名，您可以使用此设置指定 Core Web Installer 可执行文件的新名称。该文件将流式下载 Rapid Recovery Core 安装程序的最新版本，最新版本可直接在 Web 中运行，您可以根据需要暂停和恢复该过程。
Core 地址	输入 Core 服务器的地址。通常包括协议、Core 服务器和端口的名称，以及 Core 文件所在的目录。 例如，如果服务器为示例，则设置为 https://sample:8006/apprecovery/admin/Core
接收失败超时	超时前应尝试部署 Agent 软件的时间量。 默认设置为 00:25:00 或二十五分钟。如果您想要更改此设置，请输入您希望在读或写事件期间发生超时之前系统尝试部署 Agent 软件的时间长度。使用 HH:MM:SS 格式。
最大并行安装数	该设置控制用于 Core 的 Agent 软件部署的最大数量以进行一次性尝试。 默认设置为 100。

- 5 对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。

配置数据库连接设置

Rapid Recovery 在“事件”页面上显示有关 Core 任务、事件和警报的信息。Rapid Recovery 存储 MongoDB 服务数据库中的该交易信息，其默认本地安装在 Core 机器上。您可以配置这些设置以更改数据库中保留信息的时间长短，或更改连接池大小允许更多或更少的并发连接。

如果使用第二个 Rapid Recovery Core，您可以将第一个 Core 上的数据库连接设置配置到第二个 Core 机器点上。通过这种方式，两个 Core 上的事件数据将存储在第二 Core 上的 MongoDB 中。

或者，您可以在 Core 上将数据库连接设置配置到另一台单独安装有 MongoDB 的机器上，Rapid Recovery Core 可通过网络对 MongoDB 进行访问。Core 的事件交易数据稍后不会本地保存到服务数据库中。有关建立或修改用于服务数据库的数据库连接设置，请参阅[配置数据库连接设置](#)。

① | 注: 有关查看 **Rapid Recovery Core** 上事件信息的更多信息，请参阅[使用任务、警报和日记查看事件](#)。

客户可以选择在另一台机器上指定 MongoDB 服务数据库安装，该机器可在网络上访问 Rapid Recovery Core。如果 Rapid Recovery Core 服务数据库安装在非 Rapid Recovery Core 托管的机器上，您必须在这些设置中提供数据库凭据（用户名和密码）。

要修改 Rapid Recovery Core 使用的服务数据库的数据库连接设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击  （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**数据库连接**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“数据库连接”标题。
此时将显示数据库连接 Core 设置。
- 3 从“数据库连接”设置区域顶部，您可以执行以下操作：
 - 单击**测试连接**以验证设置。
当您更改任何数据库连接设置时，建议测试连接。
 - 单击**还原默认值**以还原所有默认数据库连接设置。
系统将提示您确认此操作，这将导致放弃任何自定义的数据库连接设置。
- 4 单击您想要更改的设置。
您选择的设置将变为可编辑。
- 5 根据下表中的说明输入配置信息。

表. 17: 数据库连接设置信息

文本框	说明
主机名	输入数据库连接的主机名。 ① 注: 如果 localhost 指定为主机的参数，则 MongoDB 将本地安装在托管 Core 的机器上。
端口	输入数据库连接的端口号。 ① 注: 默认设置为 27017 。
用户名	输入具有访问 MongoDB 服务数据库管理权限的用户名称。 ① 注: 如果主机名参数是 localhost ，则不需要填写该字段。
密码	输入与指定用户名关联的密码。 ① 注: 如果主机名参数是 localhost ，则不需要填写该字段。
保留期（天）	输入服务数据库中事件和作业历史的保留天数。
最大连接池大小	设置缓存以便动态重复使用的数据库连接的最大数量。 ① 注: 默认设置为 100 。
最小连接池大小	设置缓存以便动态重复使用的数据库连接的最小数量。 ① 注: 默认设置为 0 。

- 6 对于每项设置，当对所做的更改满意时，请单击  以保存更改并退出编辑模式，或单击  退出编辑模式而不保存。

修改本地数据库连接设置

您可以在“事件”页面上查看与 Rapid Recovery Core 相关的系统事件。Rapid Recovery Core 将交易信息存储在 MongoDB 服务数据库中。默认情况下，该数据库安装在本地 Core 机器上，并且数据库连接设置中的主机名默认为 localhost。在这种情况下，环回接口会跳过本地网络接口硬件，不需要数据库凭据。

（可选）要提高安全性，您可以明确指定 Rapid Recovery Core 使用的 MongoDB 数据库的数据库凭据（用户名和密码）。

注: 有关查看 **Rapid Recovery Core** 上事件信息的更多信息，请参阅[使用任务、警报和日记查看事件](#)。有关数据库连接设置的信息，请参阅[配置数据库连接设置](#)。

要修改本地数据库连接设置以指定数据库凭据，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击  （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**本地数据库设置**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“本地数据库设置”标题。此时将显示“本地数据库”核心设置。
- 3 单击您想要更改的设置。
您选择的设置将变为可编辑。
- 4 根据下表中的说明输入用于连接至服务数据库的正确凭据。

表. 18: 本地数据库设置信息

文本框	说明
用户名	输入具有访问 MongoDB 服务数据库管理权限的用户名称。
密码	输入与指定用户名关联的密码。

- 5 对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。

管理 SMTP 服务器设置

如果配置用于 Core 的简单邮件传输协议 (SMTP) 服务器设置，您可以通过电子邮件发送任务、事件和警报通知。

主题[配置电子邮件服务器](#)中介绍了有关配置 SMTP 电子邮件服务器的信息。

注: 要通过电子邮件发送事件信息，您还必须配置通知组设置。有关指定事件以接收电子邮件警报的更多信息，请参阅[配置通知组](#)。

管理云配置设置

在 Rapid Recovery 中，您可以将您拥有的云存储提供商存储帐户与您的 Rapid Recovery Core 相关联。这可让您在数据老化时将受保护机器中的信息存档。

Rapid Recovery 集成了 Amazon™ S3、Microsoft Azure 和使用 OpenStack 开源技术的托管云提供商。

有关管理 Rapid Recovery Core 中云存储帐户信息的更多信息，请参阅[管理云帐户](#)。

管理报告设置

您可以为 Rapid Recovery Core 或受保护机器生成报告。有关您可以生成的报告的信息，请参阅[生成并查看报告](#)。

要管理 Core 报告的报告设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击  （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**报告**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“报告”标题。此时将显示**报告** Core 设置。下表中介绍了报告设置。

选项	说明
恢复默认值	此选项将所有报告设置还原为默认设置。下表列出了每个设置的默认值。
字体	此选项控制用于报告的默认字体。默认值为 Trebuchet MS 字体。您可以将此字体更改为可用于您的系统的任何字体。
纸张大小	此选项控制打印报告的默认纸张大小。默认值为 A4。可以从以下纸张大小中选择： • Letter • Tabloid • Ledger • Legal • A3 • A4 • Executive • B4 • C3Envelope • C4Envelope
页面方向	此选项控制导出的报告的页面方向。默认方向为“纵向”。可以从以下布局选项中选择： • 纵向 • 横向
3	要更改报告的任何设置，请在相应的设置字段中单击。设置字段显示为可配置的下拉菜单。
4	单击下拉菜单，然后选择可用的值之一。 例如，在“字体”字段中，单击 Times New Roman 。
5	对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。 您选择的选项现在显示为所选报告参数的新设置。

管理 Core SQL 可附加性设置

SQL 可附加性设置作为 Rapid Recovery 每夜作业的一部分执行。为降低许可成本，Rapid Recovery 为您提供了两种执行可附加性检查的方法：使用 Rapid Recovery Core 机器上安装的获得许可的 SQL Server 实例，或者使用受保护机器上已安装的 SQL Server 实例。

第二种方法现在是默认设置。但是，如果在执行每夜作业期间已过度使用受保护机器，请考虑使用 Core 上的 SQL Server 实例执行检查。

总之，管理 Core SQL 可附加性设置的过程涉及以下任务：

- 安装用于包含数据库保护群组的最新恢复点。
 - 从 SQL Server 连接到数据库。
 - 打开数据库。
 - 关闭数据库。
 - 卸载恢复点。
- 为启用该每夜检查，请指定 SQL Server 实例用以在受保护机器上进行 SQL Server 数据库的可附加性检查。

① 注: 如果您不保护 Core 中的 SQL Server，则该选项将不会显示。

要配置 Core 以在执行每夜作业过程中执行 SQL 可附加性检查，请完成以下步骤。

① 注: 如果您选择默认选项以使用受保护机器上安装的 SQL Server 实例，则该 SQL Server 实例将管理所有受保护的 SQL 机器的 SQL 可附加性。如果您不想将此设置应用到所有受保护的 SQL 机器，请选择“使用 Core 上的 SQL Server”。要在 Core 上执行可附加性检查，您必须安装或使用 Core 机器上获得许可的 SQL Server 版本。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击  （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**可附加性**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“可附加性”标题。
- 3 要使用受保护的 SQL Server 机器上安装的 SQL Server 实例，请选择**使用受保护机器上的 SQL Server**。此为默认选项。
- 4 要使用 Rapid Recovery Core 上安装的 SQL Server 实例，请选择**使用 Core 上的 SQL Server**，然后根据下表中的说明输入身份验证信息。

表. 19: SQL Server 凭据信息

文本框	说明
SQL Server	从“SQL Server”下拉菜单中，从 Core 服务器中选择相应的 SQL Server 实例。
凭据类型	从以下选项中选择您的凭据的相应身份验证方法： • Windows • SQL
用户名	根据所选凭据类型指定用于在 Core 上访问 SQL Server 的用户名。
密码	根据所选凭据类型指定用于在 Core 上访问 SQL Server 的密码。

- 5 单击**测试连接**。

① 注: 如果输入错误凭据，将显示一条消息，指出凭据失败。纠正凭据信息，然后再次测试连接。
- 6 在对您所做的更改满意后，单击**应用**。

了解 Core 作业

Core 作业是 Rapid Recovery Core 执行以支持其操作的过程，包括备份到恢复点、复制数据、存档数据、将数据导出到虚拟机、维护存储库等。对于某些操作会自动启动 Core 作业，例如，按制定的计划复制或存档。您也可以从 Core Console 上的各种元素按需调用一些作业。

- 当查看或编辑 Core 作业设置时，每个 Core 作业都有两个参数：“最大并发作业数”和“尝试计数”。
 - “最大并发作业数”参数确定可以同时运行该类型的作业数。

- “尝试计数”参数确定如果网络或其他通信错误导致作业第一次无法成功则在放弃作业之前应尝试作业的次数。
- 在“Core 作业”表中，“设置”列指明列出的作业默认包括在 Core 作业中还是必须显式添加。

下表介绍了可用的主要 Core 作业及它们的功能。

表. 20: Core 作业

作业名称	说明	最大并发作业数	尝试计数	设置
检查快照中 SQL 数据库的可附加性	可让 Core 检查 SQL 数据库的一致性，并确保所有支持 MDF（数据）和 LDF（日志）文件都在备份快照中可用。过程： • 安装用于包含 SQL 数据库的保护组的最新恢复点。 • 安装数据库。如果从受保护的 SQL Server 执行可附加性，请使用 UNC 路径安装。 • 从 SQL Server 连接到数据库。 • 执行可附加性检查。 • 执行清理操作。 • 关闭数据库。 • 卸载数据库。 • 卸载恢复点。	1	0	Default（默认值）
检查 Exchange 数据库的校验和	检查包含 Exchange 数据库的恢复点的完整性。过程： • 安装用于包含 SQL 数据库的保护组的最新恢复点。 • 从 SQL Server 连接到数据库。 • 打开数据库。 • 关闭数据库。 • 卸载恢复点。	1	0	Default（默认值）
检查 Exchange 数据库可安装性	检查 Exchange 数据库是否可安装。	1	0	Default（默认值）
从远程源复制受保护机器数据	将受保护机器的恢复点的副本从源 Core 传输到目标 Core。此作业将在接收传入的已复制恢复点的目标 Core 上运行。	3	0	Default（默认值）
将受保护机器数据复制到远程目标	将受保护机器的恢复点的副本从源 Core（原始保存位置）传输到目标 Core。此作业在源 Core 上运行，控制传出复制。	1	3	Default（默认值）
汇总恢复点	通过按保留策略中定义的计划组合或“汇总”恢复点，来对所备份数据应用保留策略。	1	0	Default（默认值）
检查恢复点	检查恢复点的完整性。	1	0	添加
删除所有恢复点	删除受保护机器上的整套恢复点。	1	0	添加
删除恢复点链	删除受保护机器上完整的恢复点链。	1	0	添加

作业名称	说明	最大并发作业数	尝试计数	设置
删除恢复点范围	按恢复点标识符或日期范围删除受保护机器上的一组恢复点。	1	0	添加
部署 Agent 软件到机器	将 Rapid Recovery Agent 软件部署到指定的机器。	1	0	添加
下载 Exchange 库	将 Microsoft Exchange 库从受保护机器下载到 Core 机器，路径为 C:\ProgramData\AppRecovery\ExchangeLibraries。	1	0	添加
导出到存档	使用所选恢复点的存档在指定路径中创建备份。过程： - 安装恢复点。 - 将数据写入到备份。 - 卸载恢复点。	1	0	添加
导出到虚拟机	将数据从受保护机器的指定恢复点作为虚拟机复制到目标路径。过程： - 安装恢复点。 - 从目标路径中的恢复点数据创建虚拟机。 - 卸载恢复点。	1	0	添加
导入存档	从先前创建的 Core 存档上的指定备份导入恢复点。	1	0	添加
维护存储库	执行存储库检查。过程： - 检查存储库文件系统。 - 安装恢复点。 - 重新计算存储库的清除重复项缓存。 - 从存储库加载恢复点。	1	0	添加
安装恢复点快照	将恢复点安装到指定路径。	1	0	添加
保护 ESX® 虚拟机	将所有指定的虚拟机添加到无代理保护。 该作业是在使用“保护多台机器向导”将一个或多个虚拟机的无代理保护添加到 Core 之后立即执行的。 该作业设置每个指定虚拟机的 ID 号、将有关 Core 的信息写入到配置文件并从文件检索元数据。	1	0	添加
从恢复点还原	从恢复点还原到指定的目标机器。过程： - 安装恢复点。 - 将恢复点中的所有数据写入到指定机器。 - 卸载恢复点。	1	0	添加
上传日志	将日志上传到指定服务器。	1	0	添加

“设置”中包含一些 Core 作业。作业设置可让您指定 Core 可以运行的相同类型的并发作业数以及如果第一个作业尝试失败则应重试的次数。

有关这些设置的更多信息，请参阅 [Core 作业设置](#)。

有关将作业添加到 Core 设置的信息，请参阅 [将 Core 作业添加到设置](#)。

有关在“设置”列表中编辑作业的设置的信息，请参阅[编辑 Core 作业设置](#)。

Core 作业设置

当您从图标栏中选择 （设置）时，您可以访问某些 Core 作业的设置。“Core 设置”页面上的**作业**区域可让您确定列出的每种作业类型的两个设置：

- 1 Core 一次尝试这种类型的作业的最大数量。这必须设置为 1 到 50 之间的值。
- 2 如果网络或其他通信错误导致作业第一次无法成功则应尝试作业的次数。这必须设置为 0 到 10 之间的值。

许多作业都自动包括在 Core 中。这些作业在“设置”列中包括“默认”值（如主题[了解 Core 作业](#)中所示）。

如果您想要配置这些设置以控制这些功能的最大作业数或重试次数，您可以向设置添加一些其他作业。这些作业在“设置”列中包括“添加”值。有关如何将这些作业添加到“设置”表的信息，请参阅[将 Core 作业添加到设置](#)。

“设置”中不可用的 Core 作业不提供设置这两个参数的能力。

对于设置中列出的作业，您可以编辑现有设置。这可让您自定义两个参数、从作业设置列表中删除作业类型或还原默认设置。有关详细信息，请参阅主题[编辑 Core 作业设置](#)。

将 Core 作业添加到设置

Core 作业设置可让您针对每种作业类型定义 Core 一次尝试的最大作业数以及在第一次尝试失败后应重试该作业的次数。

每种 Core 作业类型都有以下两个参数的默认值，如 [Core 作业设置](#) 主题中所述。此列表还指明默认情况下 Core 设置中包括哪种作业类型。

将 Core 作业添加到设置使您能够更改您添加的作业类型的这些参数。

要将作业添加到 Core 设置，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击**作业**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“作业”标题。此时将显示“作业”核心设置。
- 3 在“Core 设置”页面上，单击  **添加**。此时将显示“作业设置”对话框。
- 4 在**作业设置**对话框中，从**作业**字段中选择您想要添加到 Core 设置的作业的名称。这些作业将在 [Core 作业设置](#) 主题中进行介绍。
- 5 要设置 Core 一次性尝试的最大作业数量，请在**最大并发作业数**文本框中输入一个介于 1 至 50 的新值。
- 6 要设置 Core 在放弃作业前进行的尝试次数，请在**尝试计数**文本框中输入一个介于 0 至 10 的新值。
- 7 单击**保存**。
“作业设置”对话框关闭，应用新作业设置。

编辑 Core 作业设置

Core 作业设置可让您针对每种作业类型定义 Core 一次尝试的最大作业数以及在第一次尝试失败后应重试该作业的次数。

每种 Core 作业类型都有以下两个参数的默认值，如[了解 Core 作业](#)主题中所述。此列表还指明默认情况下 Core 设置中包括哪种作业类型。当编辑 Core 作业设置时，您可以完成以下操作：

- 您可以自定义每个 Core 作业类型的设置。
- 您可以从 Core 设置列表中删除作业类型。如果设置中默认包括该作业类型，则此功能不可用。

① **注：**从 Core 设置中删除作业只会从此列表中删除作业类型。要在将来再次编辑该作业类型的 Core 设置，您可以按照主题[将 Core 作业添加到设置](#)中所述将其添加到列表。

- 您可以将任何作业类型的设置还原为默认设置。

① **注：**尽管默认情况下，您只能对 Core 设置中包含的作业类型使用此功能，但是，您可以通过将其他作业类型从列表中删除并重新添加它们来将它们设置为默认值。

要编辑作业设置，请完成以下过程中的步骤。

1 导航至 Rapid Recovery Core Console。

2 在图标栏上，单击 （设置），然后执行以下操作之一：

- 从“设置”页面左侧的 Core 设置列表中，单击**作业**。
- 在“设置”页面右侧向下滚动，直至您可以看到“作业”标题。
此时将显示“作业”核心设置。

3 从作业网格中，从列表中选择您要删除的作业。从该作业的  下拉菜单中，选择**删除**。
已从列表中删除该作业。

4 从作业网格中，从列表中选择您想要重置其设置的作业。从该作业的  下拉菜单中，选择**重置为默认值**。
此作业的作业设置会重设为默认设置。

5 从作业网格中，选择要更改的作业。从该作业的  下拉菜单中，选择**编辑**。

6 此时将打开“作业设置：[作业名称]”对话框。

7 要更改 Core 的最大作业数量以进行一次性尝试，在“最大并行作业”文本框中，输入一个介于 1 至 50 的新值。

8 要更改 Core 在放弃作业前进行的其他尝试的次数设置，请在“尝试合计”文本框中输入一个介于 0 至 10 的新值。

9 单击**保存**。

“作业设置”对话框关闭，应用新作业设置。

管理许可证

许多 Rapid Recovery Core 用户会启用试用许可证，而其能力有限。试用许可证的有效期为 14 天，可通过组管理员延长一次，为期 28 天。一旦试用期满，在您获得和注册有效的非试用许可证之前，Rapid Recovery Core 将停止创建快照。

① **注：**有关输入许可证密钥或文件信息的信息（例如，要将试用许可证更新或更改为有效的长期许可证），请参阅[更新或更改许可证](#)。

许可证是使用许可证文件或许可证密钥进行验证的。

许可证文件是以 .lic 文件扩展名结尾的文本文件。许可证文件的示例包括以下各项：

- 许可证文件的长度可以为 9 个字符，包含三组的阿拉伯数字，每组用连字符隔开：例如，123-456-789.lic。
- 基于软件的许可证可以以格式 Software-<组名>.lic 显示，组名后面为客户名称或帐户：例如，Software-YourCompany.lic。
- Dell 设备许可证可以以格式 <设备系列>-<组名>.lic 显示，组名后面为客户名称帐户：例如 DL4X00 Series-YourCompany.lic。

许可证密钥的长度可以为 30 个字符，包含六组英语字母数字字符，每组用连字符隔开。例如，示例许可证密钥格式为 ABC12-DEF3G-H45IJ-6K78L-9MN10-OPQ11。

Rapid Recovery 使您能够直接从 Core Console 管理许可证或联系许可证服务器，方法是从图标栏中选择 （设置）并单击**许可**。

许可设置包括以下信息：

许可证详细信息：

-  **更改许可证。**使您能够通过上载许可证文件或输入许可证密钥来将现有许可证与 Core 相关联。
-  **添加许可证。**此选项仅适用于 Dell 备份设备，并且使您能够上载许可证文件或输入许可证密钥。
-  **许可证门户组。**此选项将打开许可证门户以便管理组。
- 许可证类型。**许可证的类型包括试用版、订阅版或企业版。有关更多信息，请参阅“Dell Data Protection | Rapid Recovery 许可证门户 User Guide”（《Dell Data Protection | Rapid Recovery 许可证门户用户指南》）中的主题“About Dell Data Protection | Rapid Recovery 许可证门户 Software License Types”（“关于 Dell Data Protection | Rapid Recovery 许可证门户软件许可证类型”）。
- 许可证状态。**表示许可证状态。活跃的状态可确保快照按计划进行。如果许可证被阻止或过期，或者如果 Core 无法在超过宽限期之前与 Dell Data Protection | Rapid Recovery 许可证门户通信，快照将在许可证更正前处于暂停状态。

许可证限制：

- 每日最大快照数。**表示受特定许可证限制的备份的数量。

许可证池：

- 池大小。**许可证池是可用于在 Dell Data Protection | Rapid Recovery 许可证门户中跨组和子组进行分配的非试用许可证的数量。该池的大小确定可分配的许可证数量。有关更多信息，请参阅“Dell Data Protection | Rapid Recovery 许可证门户 User Guide”（《Dell Data Protection | Rapid Recovery 许可证门户用户指南》）中的主题“Understanding License Pools”（了解许可证池）。
- 受该 Core 保护。**表示许可证池中受该 Core 保护的机器数量。
- 在组内全部保护。**表示和该 Core 位于同一许可证池中的受保护机器总数。

许可证服务器。这些设置适用于标准（家庭电话）许可证。这些设置不适用于家用电器和其它非家庭电话许可证：

- 许可证服务器地址。**显示与该 Core 关联的许可证服务器活跃的 URL。
- 来自许可服务器的最后响应。**表示最后尝试与许可证服务器门户通信是否成功。
- 与许可服务器的最后联系。**显示最后与许可证服务器成功联系的日期和时间。
- 联系许可证服务器的下一次尝试。**表示尝试与许可证服务器通信的下一个计划日期和时间。
- 现在联系。**此按钮将按需联系许可证服务器。请在对您的许可证配置进行更改后使用此选项，以立即注册更改，而不是等待下一次计划尝试。

有关许可证的更多信息，请参阅“Dell Data Protection | Rapid Recovery 许可证门户 User Guide”（《Dell Data Protection | Rapid Recovery 许可证门户用户指南》）。

有关添加或更改许可证密钥或文件的更多信息，请参阅[更新或更改许可证](#)。

有关联系许可证门户服务器的更多信息，请参阅[联系 Dell Data Protection | Rapid Recovery 许可证门户服务器](#)

您也可以查看单一受保护机器的许可证信息。有关更多信息，请参阅[查看机器的许可证信息](#)。

更新或更改许可证

在升级或购买长期 Rapid Recovery 许可证后，您将会通过电子邮件收到许可证文件或许可证密钥。

要升级试用许可证或更改现有许可证并将其与 Rapid Recovery Core Console 相关联，请完成以下过程中的步骤。

 **注：**如有必要，Dell 备份设备的用户也可以向 Core 添加许可证。有关更多信息，请参阅[添加许可证](#)。

有关获取许可证密钥的信息，或有关使用许可证门户下载软件、注册设备、管理许可证订阅和许可证组 and 生成许可证门户报告的详细信息，请参阅“Dell Data Protection | Rapid Recovery 许可证门户 User Guide”（《Dell Data Protection | Rapid Recovery 许可证门户用户指南》）。

如果您刚才安装了新的 Core，而系统要求您选择许可证文件或密钥，请跳至[步骤 5](#)。

1 导航至 Rapid Recovery Core Console。

2 在图标栏上，单击 （设置）。

3 在**设置**页面右侧向下滚动，直至您可以看到“许可”标题。
此时将显示 Core 许可设置。

4 要更新或更改与您的 Core 相关联的现有许可证，请在“许可证详细信息”核心设置区域顶部，单击  **更改许可证**。
此时将显示 **Change License**（更改许可证）对话框。

5 要输入许可证密钥或上传许可证文件，请执行以下操作之一：

- 如果您想要 **手动输入**许可证密钥，请在“更改许可证”对话框中小心地键入密钥，然后单击**继续**。
对话框将关闭并验证所选文件，该许可证将与您的 Core 相关联。
- 如果您想要 **上传**许可证文件，请在“更改许可证”对话框中单击**选择文件**。
在**文件上传**对话框中，导航浏览文件系统并找到您想要使用的新许可证文件。例如，找到 Software-YourCompany.lic。
- 选择该许可证文件，然后单击**打开**。
此时将显示“文件上传”对话框。“更改许可证”对话框中此时会显示所选许可证文件。
- 在**更改许可证**对话框中，单击**继续**。
对话框将关闭并验证所选文件，该许可证将与您的 Core 相关联。

6 在“设置”页面右侧向下滚动，直至您可以看到“许可证服务器”标题。
此时将显示“许可”核心设置。

7 在“许可证服务器”区域中，单击**现在联系**。

一旦许可证被应用到许可证服务器，任何相关的受保护机器将自动使用新的许可证更新。

添加许可证

Dell 备份设备所有者可以将一个或多个许可证添加到 Rapid Recovery Core Console。

一旦已升级或购买 Rapid Recovery 许可证，您将会通过电子邮件收到许可证文件或许可证密钥。

您也可以在 Core Console 上更新或更改现有许可证。有关更多信息，请参阅[更新或更改许可证](#)。

① 注：只有 Dell 备份设备用户才能看到“添加设备”按钮。

① 注：有关获取许可证密钥的信息，请参阅“*Dell Data Protection | Rapid Recovery 许可证门户 User Guide*”（《Dell Data Protection | Rapid Recovery 许可证门户用户指南》）。

1 导航至 Rapid Recovery Core Console。

2 在图标栏上，单击 （设置）。

3 在“设置”页面右侧向下滚动，直至您可以看到“许可”标题。
此时将显示 Core 许可设置。

4 要添加许可证并将其与您的 Core 相关联，在“许可证详细信息”核心设置区域顶部，单击**添加许可证**。在**添加许可证**对话框中，执行以下操作之一：

- 如果您想要 **手动输入**许可证密钥，请在“更改许可证”对话框中小心地键入密钥，然后单击**继续**。
对话框将关闭并验证所选文件，该许可证将与您的 Core 相关联。
- 如果您想要 **上传**许可证文件，请在“更改许可证”对话框中单击**选择文件**。
在**文件上传**对话框中，导航浏览文件系统并找到您想要使用的新许可证文件。例如，找到 Software-YourCompany.lic。
- 选择该许可证文件，然后单击**打开**。

此时将显示“文件上传”对话框。“更改许可证”对话框中此时会显示所选许可证文件。

- d 在**更改许可证**对话框中，单击**继续**。

对话框将关闭并验证所选文件，该许可证将与您的 Core 相关联。

- 5 在“设置”页面右侧向下滚动，直至您可以看到“许可证服务器”标题。

此时将显示“许可”核心设置。

- 6 在“许可证服务器”区域中，单击**现在联系**。

一旦许可证被应用到许可证服务器，任何相关的受保护机器将自动使用新的许可证更新。

联系 Dell Data Protection | Rapid Recovery 许可证门户服务器

Rapid Recovery Core Console 会频繁联系门户服务器，以便与 Dell Data Protection | Rapid Recovery 许可证门户中所做的任何更改保持同步。

对于非试用许可证，Rapid Recovery Core 将每小时联系许可证门户一次。如果 10 天宽限期过后，Core 无法联系许可证门户，那么 Core 将停止创建快照。

通常，与许可证门户服务器之间的通信会按照指定的间隔自动进行；但也可以根据需要启动通信。

要联系许可证门户服务器，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击**设置**，然后在**设置**页面右侧向下滚动，直至您可以看到“许可证服务器”标题。
- 3 从“许可证服务器”区域中，单击**现在联系**。

了解 SNMP 设置

简单网络管理协议 (SNMP) 是 IP 网络上的一种用于管理设备的协议。SNMP 主要用于监测设备在网络上需要注意的条件。本协议使用软件组件（代理）向管理计算机（管理器）报告信息。SNMP 代理处理管理器获取或设置一定参数的请求。SNMP 代理可以向管理器发送陷阱（有关具体事件的通知）。

SNMP 代理管理的数据对象组织成一个管理信息库 (MIB) 文件，其包含对象标识符 (OID)。每个 OID 标识一个可以通过 SNMP 读取或设置的变量。

Rapid Recovery 包括对 SNMP 版本 1.0 的支持。

您可以将 Rapid Recovery Core 配置为 SNMP 代理。然后 Core 可以报告警报、存储库状态和受保护机器等信息。SNMP 主机可以使用称为 SNMP 浏览器的独立应用程序读取此信息。您可以在可通过网络访问 Rapid Recovery Core 的任何机器上安装 SNMP 浏览器。

要确保 SNMP 浏览器可以收到 Core SNMP 事件通知，请验证通知组的通知选项是否已正确配置为由 SNMP 陷阱通知。

① | 注: 您可以使用默认组，也可以创建自定义通知组。过程是相同的。

打开通知组，选择**通知选项**选项卡，并确保由 **SNMP 陷阱通知** 已启用。默认情况下，通知组指定陷阱编号 1。如有必要，您可以更改陷阱编号以确保它与 SNMP 浏览器预期的设置相匹配。

有关更多信息和关于配置通知选项的特定详细信息，请参阅[配置通知组](#)。

或者，您可以从 Rapid Recovery Core 下载 MIB 文件。此文件可以使用 SNMP 浏览器阅读，舒适度远超直接阅读从 Core 接收的数据。

本部分包括以下主题：

- [配置 SNMP 设置](#)
- [下载 SNMP MIB 文件](#)

配置 SNMP 设置

使用 SNMP 设置控制 Core 和 SNMP 浏览器之间的通信。这包括 SNMP 端口、陷阱接收机端口和陷阱接收机的主机名称。

请使用此过程配置 Core 的 SNMP 设置。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击 **SNMP 配置**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“SNMP 配置”标题。此时会显示“SNMP 配置”设置。
- 3 如下表所述修改 SNMP 设置。

表. 21: SNMP 连接设置信息

文本框	说明
传入端口	输入 SNMP 连接的端口号。  注: 默认设置为 8161。
陷阱接收机端口	输入陷阱接收机的端口号。 默认设置为 162。
陷阱接收机主机名	输入 SNMP 连接的主机名。  注: 默认主机名为 localhost。

- 4 对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。

下载 SNMP MIB 文件

简单网络管理协议用于监测网络上的设备是否有需要注意的情况。当 Rapid Recovery Core 设置为 SNMP 代理时，Core 可以报告警报、存储库状态和受保护机器等信息。SNMP 主机可以通过使用一个称为 SNMP 浏览器的独立应用程序读取该信息。

SNMP 代理管理的数据对象组织成一个管理信息库 (MIB) 文件，其包含对象标识符 (OID)。每个 OID 标识一个可以通过 SNMP 读取或设置的变量。

您可以从 Rapid Recovery Core 上下载 MIB 文件。然后，可以通过 SNMP 浏览器阅读此文件（名为 dell-aa-core.mib），舒适度远超直接阅读从 Core 接收的数据。

使用此过程从 Rapid Recovery Core 下载 SNMP MIB 文件。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （更多），然后单击**下载**。
此时将显示**下载**页面。
- 3 向下滚动至“其他文件”窗格。
- 4 要下载 MIB 文件，请单击 **SNMP MIB 文件** 下载链接。
此时会显示“SNMP 配置”设置。
- 5 在**打开 dell-aa-core.mib** 对话框中，执行以下操作之一：
 - 要打开日志文件，请选择“打开方式”，然后选择用于查看基于文本的 MIB 文件的 SNMP 浏览器应用程序，最后单击**确定**。
dell-aa-core.mib 文件将在所选应用程序中打开。

- 要在本地保存文件，请选择**保存文件**，然后单击**确定**。
dell-aa-core.mib 文件将保存至“下载”文件夹。它可以使用 SNMP 浏览器或文本编辑器打开。

配置 vSphere 设置

VMware vSphere 是一套虚拟化软件，您可以从中管理 ESXi 或 vCenter Server 虚拟机。如果使用 vSphere，您不再需要将 Rapid Recovery Agent 软件加载到单个虚拟机上以保护它们。这称为无代理保护功能，仅适用于虚拟机。

使用此过程配置 Core 的 vSphere 设置。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置），然后执行以下操作之一：
 - 从“设置”页面左侧的 Core 设置列表中，单击 **vSphere**。
 - 在“设置”页面右侧向下滚动，直至您可以看到“vSphere”标题。
此时将显示 vSphere 设置。
- 3 根据下表中的说明修改 vSphere 设置。

表. 22: vSphere Core 设置信息

UI 元素	UI 类型	说明
连接生存期	数字调整框	建立与 ESXi 服务器连接超时之前的持续时间。使用 HH:MM:SS 格式。 注: 默认设置为 00:10:00 或十分钟。
最大同时合并	文本字段	设置受保护的虚拟机的最大同时合并数。 注: 默认设置为 0 。
最大重试次数	文本字段	设置超时之前连接至虚拟磁盘或读写操作的最大尝试次数。 注: 默认设置为 10 。
允许并行还原	布尔值（复选框）	选中此选项时，可为无代理虚拟机启用并行还原。 清除此选项时，此功能被禁用。 注: 默认设置是“否”（已清除）。

- 4 对于每个设置，当对您所做的更改满意后，请单击复选标记以保存更改并退出编辑模式，或单击 **X** 退出编辑模式而不保存。

备份并还原 Core 设置

您可以将 Core 设置信息备份到文件，如果 Core 计算机有问题或您想要将这些设置迁移至其他计算机，您稍后可以还原这些设置。已备份的信息包括存储库元数据（如存储库名称、数据路径和元数据路径）；Core 中受保护的机器；复制关系（目标和源）；配置用以虚拟备份的机器；以及有关加密密钥的信息。

该过程仅还原配置设置而未还原数据。安全性信息（如验证凭据）未存储在配置文件中。保存 Core 配置文件无安全性风险。

注: 在使用该过程还原 Core 设置前，您首先必须备份 Core 设置信息。

使用该过程备份和还原 Core 设置。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （设置）。

此时将显示 **Settings**（设置）页面。在设置类别上“设置”窗格的顶部，您会看到两个按钮 -“备份设置”和“恢复设置”。

3 如果您想要备份 Core 设置，请继续执行 [步骤 4](#)。如果您想要还原 Core 设置，请继续执行 [步骤 6](#)。

4 要以 XML 文件格式备份当前设置，单击“设置”页面顶部的 **备份设置**。

此时将显示“备份 Core 配置”对话框。

5 在“本地”路径文本框中，键入您希望将 Core 设置作为 XML 文件存储在其中的本地可访问 Core 计算机目录路径，然后单击 **备份**。

例如，键入 C:\Users\Your_User_Name\Documents\AA5CoreSettings，然后单击 **备份**。

名为 AppRecoveryCoreConfigurationBackup.xml 的文件将保存到您指定的本地目标文件夹中。

6 要使用该方法从之前保存的备份 XML 文件中还原 Core 设置，请执行以下步骤。

注：还原 Core 配置设置时，**Rapid Recovery Core** 服务将重新启动。

a 从 **设置** 页面顶部，单击 **还原**。

此时将显示 **还原 Core 配置** 对话框。

b 在 **本地路径** 文本框中，输入存储 Core 配置设置位置的本地路径。

例如，键入 C:\Users\Your_User_Name\Documents\AA5CoreSettings。

c 如果您不希望还原存储库信息，则继续执行 [步骤 g](#)。

d 或者，如果您想要还原配置在备份文件中的存储库信息，请选择 **还原存储库**，然后单击 **还原**。

此时将显示 **还原存储库** 对话框。

如果选择从备份配置数据还原存储库信息，则在保存 Core 设置时将显示配置的存储库以进行验证。默认情况下，将选择所有现有存储库。

e 验证要还原的存储库信息。如果验证列表中出现多个存储库，而您只要还原其中一些信息，然后取消选择不要还原的存储库。

f 如果您对想要还原的存储库选择满意，单击 **保存**。

此时将关闭 **还原存储库** 对话框。

g 在 **还原存储库** 对话框中，单击 **还原**。

还原存储库 对话框将关闭，而还原过程将开始。会显示一条警报提示存储库服务配置已更改。

h 如果有无法还原的配置设置，您将看到一条错误消息。查看错误的详细信息，以查看是否需要任何操作。有关更多信息，请参阅 [使用任务、警报和日记查看事件](#)。要继续，请单击 **关闭** 以清除错误对话框。

i 还原配置后，请验证以下各项：

- 解锁所有加密密钥。有关更多信息，请参阅 [解锁加密密钥](#)。
- 如果配置虚拟备用机来持续更新网络目标的 VM，您必须在成功同步前，指定虚拟备用机设置中的网络凭据。有关更多信息，请参阅 [VM 导出](#)。
- 如果已配置计划存档以备份到云存储帐户，那么您必须指定凭据以便 Core 可以连接到云帐户。有关使用云存储帐户链接 Core 的更多信息，请参阅 [添加云帐户](#)。
- 如果已设置复制，并且您想要还原到目标 Core，请验证源 Core 上的目标 Core 设置（特别是主机）。有关更多信息，如果管理您自己的 Core，请参阅 [复制到自管目标 Core](#)。如果复制到由第三方管理的 Core，请参阅 [复制到第三方目标 Core](#)。
- 如已配置 SQL 连接检查，并且执行检查的 SQL Server 实例位于 Core 计算机上，则在“连接”设置中指定 SQL 凭据。有关更多信息，请参阅 [管理 Core SQL 可附加性设置](#)。

验证“回放引擎”配置已还原，如未还原则更新设置以确保有效通信。有关更多信息，请参阅 [配置 Replay 引擎设置](#)。

Core 级工具

除了配置 Core 设置之外，您也可以使用下表中所述的 Core 级工具。

表. 23: 其他 Core 级工具

UI 元素	说明
系统信息	通过 Rapid Recovery 可以查看有关 Rapid Recovery Core 的信息，包括系统信息、本地卷和已安装卷以及 Replay 引擎连接。 有关“系统信息”页面上显示的信息的更多信息，请参阅 了解 Core 的系统信息 。 有关如何查看系统信息的更多信息，请参阅 查看 Core 的系统信息 。
下载 Core 日志文件	有关 Rapid Recovery Core 的各种活动的信息会保存到 Core 日志文件。要诊断可能的问题，您可以下载和查看您的 Rapid Recovery Core 的日志。有关如何访问和查看 Core 日志的更多信息，请参阅 访问 Core 日志 。 每个受保护机器还会保存活动日志。如果您从受保护机器选择每夜作业（称为“下载日志”），此日志可以上载到 Core。有关每夜作业的更多信息，请参阅 了解每夜作业 。有关如何配置 Core 每夜作业的更多信息，请参阅 配置 Core 的每夜作业 。有关如何为特定受保护机器配置每夜作业的更多信息，请参阅 自定义受保护机器的每夜作业 。

了解 Core 的系统信息

Rapid Recovery 可让您查看有关 Rapid Recovery Core 的信息。您可以查看常规信息、有关本地卷的信息以及有关安装的卷的信息。

在**常规**窗格中，您可以查看下表中所述的信息。

表. 24: 系统信息

UI 元素	说明
主机名	Rapid Recovery Core 的机器名称。
操作系统版本	安装在 Rapid Recovery Core 上的操作系统版本。
操作系统架构	列出托管 Rapid Recovery Core 的机器的基本架构和设计。可能包括芯片组，并列出 64 位系统。Rapid Recovery Core 仅支持 64 位系统。
内存（物理）	列出安装在 Core 机器上的随机存取内存容量。
显示名称	显示可配置 Core 的显示名称（请参阅 配置 Core 常规设置 ）。
完全限定域名	显示 Core 机器的完全限定域名。
元数据高速缓存位置	显示元数据高速缓存位置的路径。 有关更多信息，请参阅 了解清除重复项缓存大小和存储位置 。
主要高速缓存位置	显示主要重复高速缓存位置的路径。 有关更多信息，请参阅 了解清除重复项缓存大小和存储位置 。
次要高速缓存位置	显示次要重复高速缓存位置的路径。 有关更多信息，请参阅 了解清除重复项缓存大小和存储位置 。

卷窗格包括有关 Core 机器的存储卷的以下信息：名称、设备 ID、文件系统、原始容量、格式化的容量、已使用容量和安装点。

Replay 引擎连接窗格显示有关当前已安装恢复点的详细信息。您可以查看本地端点、远程端点、已安装的映像代理 ID、已安装的映像 ID 和已安装的映像显示名称。您可以查看安装是否可写入，查看认证用户、读取字节和写入字节。

您可以从“安装”页面卸载在 Core 上本地安装的恢复点。有关卸载恢复点的更多信息，请参阅[卸载恢复点](#)。

有关更多信息，请参阅[查看 Core 的系统信息](#)。

查看 Core 的系统信息

Core 的系统信息包括一般信息、关于本地卷的信息以及关于 Core 已安装卷的信息。有关本页面上可用信息的详细说明，请参阅[了解 Core 的系统信息](#)。

要查看 Core 的系统信息，请完成以下过程中的步骤。

① **注：**您也可以查看特定受保护计算机的系统信息。有关更多信息，请参阅[查看受保护机器的系统信息](#)。

- 1 导航至 Rapid Recovery Core Console。
- 2 单击图标栏上的 （更多），然后单击  **系统信息**。
此时将显示“系统信息”页面。

访问 Core 日志

有关 Rapid Recovery Core 的各种活动的信息会保存到 Core 日志文件。默认情况下，此文件名称为 AppRecovery.log，存储在路径 C:\ProgramData\AppRecovery\Logs 中。

① **注：**根据您的设置，AppRecovery 目录可能在 Rapid Recovery Core 上不可见。要查看此目录，您可能需要更改“文件夹选项”控制面板以显示隐藏文件、文件夹和驱动器。如果这些设置包括可隐藏已知文件类型的扩展名的选项，则 Core 日志文件可能显示为 AppRecovery，不含 .log 扩展名。

Core 日志包含有关已完成的 Core 作业、连接故障、在部分 Core 中尝试联系许可证门户的结果的信息以及其他信息。存储在 Core 日志文件中的每个语句前面都有四个限定词之一：INFO、DEBUG、ERROR 和 WARN。这些限定词可帮助在诊断问题时对存储在日志中的信息的性质进行分类。

① **注：**同样，每台受保护机器上还会存储一个包含与 Core 通信的尝试相关信息的日志文件。有关机器日志的更多信息，请参阅[访问受保护机器诊断](#)。

对问题进行故障排除或与 Dell Rapid Recovery 支持协作时，访问日志的功能会很有帮助。要访问日志，请参阅以下过程：

- [下载并查看 Core 日志文件](#)
- [下载并查看受保护计算机的日志文件](#)

下载并查看 Core 日志文件

如果遇到任何与 Core 有关的错误或问题，可以下载 Core 日志进行查看，或与您的 Dell Support 代表共享这些日志。

- 1 从 Rapid Recovery Core Console 的图标栏上，单击 （更多），然后单击  **Core 日志**。
- 2 在 **下载 Core 日志** 页面上，单击  **单击此处开始下载**。
- 3 如果系统提示您打开或保存该 CoreAppRecovery.log 文件，单击**保存**。
- 4 如果您看到 **Opening CoreAppRecovery.log** 对话框，执行以下操作之一：
 - 要打开日志文件，选择**打开方式**，然后选择应用程序（如记事本）来查看基于文本的日志文件，最后单击**确定**。
CoreAppRecovery.log 文件将在选定的应用程序中打开。
 - 要本地保存文件，请选择**保存文件**，然后单击**确定**。
CoreAppRecovery.log 文件将保存到**下载**文件夹中。它可以使用任何文本编辑器打开。

相关链接

[下载并查看 Core 日志文件](#)

[下载并查看受保护计算机的日志文件](#)

配置 Core 的路线图

配置一系列任务，例如创建和配置用于存储备份快照的存储库，定义用于保护数据安全的加密密钥，以及设置警报和通知。完成 Core 配置后，即可保护代理和执行恢复。

配置 Core 时，需要了解某些概念并执行以下初始操作：

- 创建存储库
- 配置加密密钥
- 配置事件通知
- 配置保留策略
- 配置 SQL 可附加性

存储库

本节介绍如何使用存储库。本节讨论了卷管理器存储库的重复数据删除，还介绍了其特征和属性。介绍了 Rapid Recovery 中使用的重复数据删除类型以及重复数据删除在整个应用程序中如何使用。然后，本节介绍了如何管理 DVM 存储库，包括创建存储库、查看和编辑存储库详细信息以及删除存储库。您可以了解如何在另一 Core 上打开一个 Core 上的存储库。最后，本节介绍了如何将恢复点从一个存储库手动迁移到另一存储库。

管理 DVM 存储库

使用 Rapid Recovery 之前，需要在 Rapid Recovery Core 上设置一个或多个存储库。存储库用于存储受保护数据；更具体地说，是存储从环境中的受保护机器捕获的快照。

管理 DVM 存储库时，需要执行以下操作：

- 1 **创建 DVM 存储库。**创建存储库之前，请考虑相应的技术类型。
有关存储库的更多信息，请参阅[了解存储库](#)。

有关创建 DVM 存储库的信息，请参阅[创建 DVM 存储库](#)。
- 2 **添加新存储位置。**有关向 DVM 存储库添加新存储位置的更多信息，请参阅[将存储位置添加至现有 DVM 存储库](#)。
- 3 **修改存储库设置。**有关修改存储库的存储库设置的更多信息，请参阅[查看或修改存储库详情](#)。
- 4 **检查存储库。**有关检查 DVM 存储库的更多信息，请参阅[检查存储库](#)。
- 5 **执行存储库优化作业。**有关存储库优化作业的更多信息，请参阅[关于存储库优化作业](#)。有关优化现有 DVM 存储库的步骤，请参阅[优化 DVM 存储库](#)。
- 6 **删除存储库。**有关删除存储库的更多信息，请参阅[删除存储库](#)。

创建 DVM 存储库

此过程介绍如何使用重复数据消除卷管理器 (DVM) 存储库技术在您的 Core 上创建存储库。

- 您必须具有对您要在其上创建 DVM 存储库的机器的管理访问权限。
- 此存储库类型需要在您定义为存储位置的卷上至少有 150GB 存储空间可用。
- DVM 存储库的存储位置必须位于连接到 Core 服务器的本地驱动器中。
- Core 服务器可以是任何 DL 系列设备（包括 DL1000）或可以是任何基于软件并符合系统要求的 Windows 服务器。

① **注：**建议通过 **Appliance（设备）** 选项卡创建存储库。有关更多信息，请参阅[配置存储](#)一节。

要创建 DVM 存储库，请完成下列步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏中，单击 （更多），然后选择 **Repositories（存储库）**。
此时将显示 **Repositories（存储库）** 页面。
- 在 **Repositories（存储库）** 页面中，DVM Repositories（DVM 存储库）窗格随即显示。
- 3 在页面顶部，单击 **Add New DVM Repository（添加新的 DVM 存储库）**。
此时将显示 **Add New Repository（添加新存储库）** 对话框。
- 4 根据下表中的说明输入信息。

表. 25: Add New Repository（添加新存储库）设置

文本框	说明
Repository Name （存储库名称）	输入存储库的名称。 默认情况下，此文本框包含词语 Repository（存储库）和一个数字，它与此 Core 的存储库数量相对应。 例如，如果它是第一个存储库，默认名称为 Repository 1。请根据需要更改此名称。 存储库名称必须包含介于 1 和 40 之间的字母数字字符，包括空格。请勿使用 禁止字符 或 禁止短语 。
Concurrent Operations（并发操作数）	定义希望存储库支持的并发请求数量。默认值为 64。
注释	（可选）输入关于此存储库的描述性说明。您可以输入至多 254 个字符。例如，键入 DVM Repository 2 。

- 5 单击 **Add Storage Location（添加存储位置）** 以定义存储库的特定存储位置或卷。此卷应为主存储位置。
-  **小心:** 为存储库的存储位置指定根目录内的专用文件夹。请勿指定根目录位置。例如，使用 **E:\Repository**，而非 **E:**。如果在此步骤中创建的存储库之后被删除了，您的存储库的存储位置上的所有文件都会被删除。如果您在根目录上指定存储位置，则卷（例如，**E:**）中的所有其他文件都会被删除。这可能会导致灾难性数据丢失。

此时将显示 **Add Storage Location（添加存储位置）** 对话框。

- 6 单击 **Add Storage Location（添加存储位置）** 以定义存储库的特定存储位置或卷。此卷应为主存储位置。
- 7 在 **Storage Location（存储位置）** 区域中，指定将文件添加到存储位置的方式。您可以选择添加本地连接的存储卷（例如，直接连接的存储、存储区域网络或网络连接存储）。您还可以指定通用 Internet 文件系统 (CIFS) 共享位置上的存储卷。
 - 单击 **Add file on local disk（在本地磁盘上添加文件）** 以指定本地机器，然后根据下表中的说明输入信息。

表. 26: 本地磁盘设置

文本框	说明
Data Path（数据路径）	输入用于存储受保护数据的位置。 例如，键入 X:\Repository\Data。 在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。
Metadata Path（元数据路径）	输入用于存储受保护元数据的位置。 例如，键入 X:\Repository\Metadata。 在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。

- 您也可以选择 **Add file on CIFS share（在 CIFS 共享上添加文件）** 指定一个网络共享位置，然后按下表所述输入相应的信息。

表. 27: CIFS 共享凭据

文本框	说明
UNC Path (UNC 路径)	输入网络共享位置的路径。 如果此位置位于根目录，请定义专用文件夹名称（例如，Repository）。 路径必须以 \\ 开始。指定路径时，只能使用字母数字字符、连字号和句点（只用于分隔主机名和域）。字母 a 至 z 区分大小写。请勿使用空格。不允许使用其他符号或标点符号。
用户名	指定用于访问网络共享位置的用户名。
密码	指定用于访问网络共享位置的密码。

- 8 在 **Storage Configuration (存储配置)** 区域中，单击 **More Details (详细信息)**，然后根据下表中的说明输入存储位置的详细信息。

表. 28: 存储配置详细信息

文本框	说明
大小	设置存储位置的大小或容量。最小大小为 1 GB。默认值为 250 GB。可以从以下各项中选择： - GB - TB ① 注: 指定的大小不能超过卷的大小。 如果存储位置是使用 Windows XP 或 Windows 7 的新技术文件系统 (NTFS) 卷，则文件大小限制为 16 TB。 如果存储位置是使用 Windows 8、8.1、Windows 10 或 Windows Server 2012、2012 R2 的 NTFS 卷，文件大小限制为 256 TB。 ① 注: 要让 Rapid Recovery 验证操作系统，在目标存储位置必须安装 Windows Management Instrumentation (WMI)。
Write Caching Policy (写高速缓存策略)	写高速缓存策略控制 Windows Cache Manager 在存储库中的使用方式，并帮助调整存储库以便在不同配置下实现最佳性能。 请将其设置为以下值之一： - On (打开) - Off (关) - Sync (同步) 如果设置为默认值 On (打开)，则 Windows 将控制高速缓存。这适用于 Windows 10 以及 Windows Server 2012 和更高版本。 ① 注: 将写高速缓存策略设置为 On (打开) 可提高性能。如果您使用的是 Windows Server 2008 SP2 或 Windows Server 2008 R2 SP2，则建议的设置为 Off (关闭)。 如果设置为 Off (关闭)，则 Rapid Recovery 将控制高速缓存。 如果设置为 Sync (同步)，则 Windows 将控制高速缓存以及同步输入/输出。
每扇区字节数	指定希望每个扇区包含的字节数。默认值为 512。
Average Bytes per Record (每个记录的平均字节数)	指定每个记录的平均字节数。默认值为 8192。

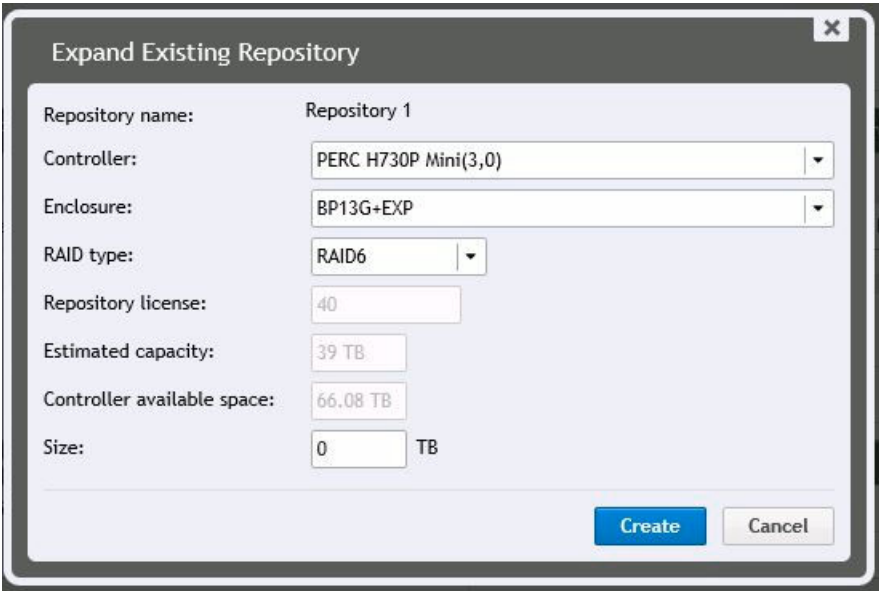
- 9 单击 **保存**。
- 此时将会关闭 **Add Storage Location (添加存储位置)** 对话框并将保存您的设置。**Add New Repository (添加新存储库)** 对话框会显示新存储位置。

- 10 （可选）重复执行步骤 6 到步骤 9 以添加存储库的附加存储位置。
- 11 如果此时已定义您想要为存储库创建的所有存储位置，请在 **Add Storage Location（添加存储位置）** 对话框中，单击 **Create（创建）**。
- 此时将关闭 **Add Storage Location（添加存储位置）** 对话框，并会应用您的更改。此时将会显示 **Repositories（存储库）** 页面，在 DVM Repositories（DVM 存储库）摘要表中会显示新添加的存储库。

扩展存储库

除 DL 1000 外，所有 DL 型号（1300、4300、4000）上都支持扩展存储库功能。应用的许可证类型限制存储库大小。要使用未使用的内部存储和外部机柜上的存储扩展存储库，请更新许可证。要更改许可证密钥，请参阅[更新或更改许可证](#)一节。要扩展现有存储库，请执行以下操作：

- 1 单击 **Appliance（设备） > Provisioning（配置）**。
- 2 在 **Repositories（存储库）** 部分中，在您想要扩展的存储库旁单击  → **Expand Existing Repository（扩展现有存储库）**。此时将显示 **Expand Existing Repository（扩展现有存储库）** 对话框。



- 3 在 **Expand Existing Repository（扩展现有存储库）** 框中，指定以下信息：

表. 29: 扩展现有存储库

文本框	说明
Repository Name（存储库名称）	将显示需要扩展的存储库的名称。
控制器	基于您是对内部存储还是对直接连接的存储机柜创建存储库，选择相应的存储控制器。
机柜	选择相应的存储机柜。
RAID type（RAID 类型）	选择相应的 RAID 配置。您具有以下 RAID 配置选项：1、5 或 6。
Repository license（存储库许可证）	将会显示存储库许可证。
Estimated capacity（估计的容量）	显示可用于创建存储库的估计容量。

文本框	说明
Controller available space (控制器可用空间)	显示控制器上的可用空间。
大小	输入需要创建的存储库的大小。

4 单击**创建**。
新存储位置将添加到现有存储库中。

存储库现已扩展到指定大小。

查看或修改存储库详情

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏中，单击 （更多），然后选择 **Repositories（存储库）**。此时将显示 **Repositories（存储库）** 页面。

- 此时将会显示 **DVM Repositories（DVM 存储库）** 窗格。
- 3 从 **Repositories（存储库）** 页面菜单，您可以执行以下常用操作：

选项	说明
Add New DVM Repository（添加新的 DVM 存储库）	添加新的 DVM 数据存储库。
Open Existing DVM Repository（打开现有 DVM 存储库）	从另一 Core 打开现有 DVM 存储库，这会将此存储库的所有权更改到此 Core。有关更多信息，请参阅 打开现有 DVM 存储库 。
刷新	查看或刷新存储库的列表。

- 4 在 **DVM Repositories（DVM 存储库）** 的窗格中，从任何 DVM 存储库的  下拉菜单中，您可以执行以下附加操作：

选项	说明
Add Storage Location（添加存储位置）	通过添加存储位置扩展现有存储库
选中	执行存储库检查
设置	查看或修改存储库设置。这些设置包括： - 查看存储库名称 - 查看或更改最大并发操作数 - 查看或更改存储库的说明 - 启用或禁用重复数据消除 - 对存储于存储库中的数据启用或禁用压缩
执行优化作业	执行存储库优化作业
删除	Delete a Repository（删除存储库）

 **注：**当扩展 DVM 存储库卷时，请先暂停保护。接着扩展卷，最后恢复保护。此操作会防止仅当扩展卷与特定传输阶段同时发生时可能出现的极个别错误。

您可在 Repositories（存储库）页面执行以下常规操作：

- 查看或刷新存储库的列表
- 添加新的存储库
- 从另一 Core 打开现有存储库，这会将所有权更改至该存储库

将存储位置添加至现有 DVM 存储库

① | 注: 建议您通过设备选项卡扩展存储库。有关更多信息, 请参阅 [扩展存储库](#)

通过向 DVM 存储库添加存储位置, 可定义存储库或卷的存储位置。

要指定存储库或卷的存储位置, 请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上, 单击  (更多), 然后选择**存储库**。
此时将显示 Repositories (存储库) 页面。

将显示“DVM 存储库”窗格。
- 3 在存储库摘要表中, 从表示您要为其添加存储位置的 DVM 存储库的行中, 单击**设置**, 然后选择**添加存储位置**。
此时将显示**添加存储位置**对话框。
- 4 指定将文件添加到存储位置时的方式。您可选择添加本地磁盘或 CIFS 共享上的文件。
 - 选择**添加本地磁盘上的文件**以指定本地机器, 然后根据下表中的说明输入信息。

表. 30: 本地磁盘设置

文本框	说明
数据路径	输入用于存储受保护数据的位置。 例如, 键入 X:\Repository\Data。 适用路径的相同限制: 只能使用字母数字字符、连字符或句点, 不允许使用空格或特殊字符。
元数据路径	输入用于存储受保护元数据的位置。 例如, 键入 X:\Repository\Metadata。 指定路径时, 只能使用字母数字字符、连字符和句点 (仅用于分隔主机名和域)。字母 a 至 z 不区分大小写。请勿使用空格。不允许使用其他符号或标点字符。

- 或者, 选择**添加 CIFS 共享上的文件**以指定一个网络共享位置, 然后按下表所述输入相应的信息。

表. 31: CIFS 共享凭据

文本框	说明
UNC 路径	输入网络共享位置的路径。 如果此位置位于根目录中, 则定义专用的文件夹名称 (例如 Repository)。 路径必须以 \\ 开头。指定路径时, 只能使用字母数字字符、连字符和句点 (仅用于分隔主机名和域)。字母 a 至 z 不区分大小写。请勿使用空格。不允许使用其他符号或标点字符。
用户名	指定用于访问网络共享位置的用户名。
密码	指定用于访问网络共享位置的密码。

- 5 在“存储配置”窗格中, 单击**更多详细信息**, 然后根据下表中的说明输入存储位置的详细信息。

表. 32: 存储位置详情

文本框	说明
大小	设置存储位置的大小或容量。默认大小为 250 GB。可以选择以下单位: • GB

- TB

① | 注: 最小大小为 1 GB。指定的大小不能超过卷的大小。

如果存储位置是使用 Windows XP 或 Windows 7 的新技术文件系统 (NTFS) 卷, 则文件大小限制为 16 TB。

如果存储位置是使用 Windows 8、8.1 或 Windows Server 2012、2012 R2 的 NTFS 卷, 则文件大小限制为 256 TB。

① | 注: 要让 **Rapid Recovery** 验证操作系统, 在目标存储位置必须安装 **Windows Management Instrumentation (WMI)**。

写高速缓存策略

写高速缓存策略控制 Windows Cache Manager 在存储库中的使用方式, 并帮助调整存储库以便在不同配置下实现最佳性能。

请将其设置为以下值之一:

- 打开
- 关闭
- 同步

如果设置为默认值打开, 则 Windows 将控制高速缓存。这适用于 Windows 10 和 Windows Server 2012 及更高版本。

① | 注: 将写高速缓存策略设置为打开可提高性能。如果您使用的是 **Windows Server 2008 SP2** 或 **Windows Server 2008 R2 SP2**, 建议的设置是“关”。

如果设置为“关”, 则 Rapid Recovery 将控制高速缓存。

如果设置为同步, 则 Windows 将控制高速缓存以及同步输入/输出。

每一扇区字节数

指定希望每个扇区包含的字节数。默认值为 512。

每个记录的平均字节数

指定每个记录的平均字节数。默认值为 8192。

- 6 (可选) 如果您要为所选存储库执行存储库优化作业, 请选择为 **[存储库名称] 运行存储库优化作业**。

Dell 建议在将存储位置添加至现有存储库时执行存储库优化作业。此作业可通过将重复数据消除应用到存储库中存储的数据来优化可用空间。

基于各种因素 (比如存储库大小、存储库中的数据量、可用网络带宽以及系统的输入和输出上的现有负载), 执行存储库优化作业的过程可能会在您的环境中花费大量时间和带宽。

有关存储库优化作业的更多信息, 请参阅[关于存储库优化作业](#)。

- 7 单击**保存**。

对话框关闭并保存存储位置。在存储库摘要表中, 如果您展开存储库详细信息, 则会显示您创建的存储位置。

有关检查 DVM 存储库的完整性

Rapid Recovery Core, 用户可在源和目标 Core 之间设置不同的保留策略。为了使使用不同保留策略的复制正常工作, 目标 Core 必须拥有与源 Core 相同的软件版本 (或更新版本)。

① | 注: Core 必须共享版本号的相同三位数 (例如, 都以 **6.0.1.xxxx** 或 **5.4.3.xxxx** 开头)。仅当目标 Core 是更新版本时, 内部版本号 (由 **xxxx** 表示) 才能不同。

现在, 管理员可用与源 Core 上不同的速率在目标 Core 上配置汇总。同样, 现在可以为任何复制机器定义自定义保留策略。例如, 您可以比在源 Core 上更快的速度汇总目标 Core 中的恢复点并具有较高的粒度。或者, 您可以比在目标 Core 中更慢的速率为任何所

选复制机器汇总恢复点，维护更细的粒度，这可能有助于合规性目的。有关使用与 Core 上默认策略不同的保留策略的更多信息，请参阅[自定义受保护机器的保留策略设置](#)。

如果您的 Core 已从 AppAssure 5.3.x 进行了升级，并且您使用了复制，则您必须先运行此作业，然后才能配置源 Core 和目标 Core 之间不同的保留策略，或在复制机器上配置自定义保留策略。

除非您有一个或多个符合条件的存储库（在 5.4.x 之前的版本创建并且尚未执行），您将无法看到或运行此作业。

运行此作业可验证指定存储库中存储的所有数据的完整性，从而确保您可以通过每个快照或基本映像恢复数据。如果完整性检查发现您存储库中的数据存在任何问题，请立即停止作业。Core 上该作业的事件详细信息会提示您联系 Dell 支持部门，以便您可以安排时间与支持代表配合执行其他过程以识别并修复数据不一致。

小心：运行此作业预计需要较长的时间。基于存储库和基础存储系统中数据的数量和类型，时间量会不同。作业正在运行时，任何其他事务都无法在该存储库中执行，包括传输（快照和基础映像备份以及复制）、每夜作业等。

此作业正在运行时，您可以执行其他存储库中的其他操作。

注：此作业会检查存储库内的所有内容的完整性。有关您可用于确存储库可安装和可用的 **Integrity Check** 作业的信息，请参阅[检查存储库](#)。

检查存储库

Rapid Recovery 允许您在发生错误时对 DVM 存储库卷执行诊断检查。Core 发生错误的原因可能是未正确关闭、硬件故障或其他环境、较低 IP 堆栈因素，这些因素可在 Rapid Recovery 功能中揭示。

注：此过程应仅用于诊断目的。例如，在发生硬件故障、错误关闭 Core 或存储库导入失败时运行此检查。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏中，单击 （更多），然后选择**存储库**。
此时将显示 **Repositories**（存储库）页面。

将显示“DVM 存储库”窗格。
- 3 要检查 DVM 存储库，请在 **DVM 存储库**窗格中表示 DVM 存储库的任意摘要表行中，单击 ，然后选择**检查**。
此时将显示 **Check Repository**（检查存储库）对话框。
- 4 在**检查存储库**对话框中，确认您了解将会取消与此存储库关联的所有活动任务并且您要继续。
活动作业将被取消，“检查存储库作业”将启动。
- 5 （可选）您可以跟踪作业的状态，方法是单击按钮栏中的**运行任务**下拉菜单，然后选择“维护存储库作业”。

关于存储库优化作业

使用 DVM 存储库时，您在每个快照中捕获的数据将执行重复数据删除。随着快照保存到存储库，此重复数据删除亦增量进行。系统会将每个信息字符串的一次出现保存到存储库中。当信息字符串重复时，系统将使用重复数据删除缓存中的原始字符串引用，以便节省存储库中的存储空间。

如果 DVM 重复数据删除缓存已满，则仅对缓存中已引用的快照数据执行重复数据删除。随着重复数据删除的发生，缓存会继续用新的唯一值进行更新，以便覆盖缓存中最旧的值。这会导致重复数据删除无法达到理想状态。

有关重复数据删除的更多信息，请参阅[了解清除重复项缓存大小和存储位置](#)。

您可以选择在缓存已满前增加 DVM 重复数据删除缓存，这可确保您在该存储库中的数据持续获得理想的重复数据删除效果。有关更多信息，请参阅[配置 DVM 清除重复项缓存设置](#)。

您也可以在缓存已满后，增加重复数据删除缓存。如果您要在增加缓存后回收存储库中的空间，您可以优化此存储库。此操作会将快照中的数据与重复数据删除缓存中的信息作比较。如果在存储库中发现任何重复的字符串，则该数据将以数据引用来替换，从而节省存储库中的存储空间。这有时也称为脱机重复数据删除，因为此重复数据删除过程在您请求时发生，而不是执行增量快照数据传输时发生。

优化过程会占用大量处理器资源。运行此作业所需的时间取决于多个因素。这些因素包括存储库大小、存储库中的数据量、可用网络带宽以及系统输入输出上的现有负载。您存储库中数据越多，此作业运行的时间越长。

当执行“存储库优化作业”时，以下操作将被替代或取消。

- 删除恢复点作业
- 维护存储库作业
- 检查存储库完整性作业

当执行优化作业时，以下操作将被替代或取消。

- 删除所有恢复点作业
- 删除恢复点链作业
- 维护存储库作业
- 删除恢复点作业基座
- 检查存储库完整性作业

有关优化现有 DVM 存储库的步骤，请参阅[优化 DVM 存储库](#)。

如果需要，您可以在有限的时间里中断存储库优化作业。有关更多信息，请参阅[中断或恢复存储库优化作业](#)。

优化 DVM 存储库

您必须在 Core 中具有 DVM 存储库方可执行此程序。

您可以对保存到现有 DVM 存储库的数据执行离线重复数据消除。通过启动存储库优化作业实现这一目标。

注: Dell 建议仅在增加重复项缓存大小后执行优化存储库作业。此操作让可让您回收存储库空间，更有效地使用 DVM 重复数据消除高速缓存。

要优化 DVM 存储库，请完成此过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （更多），然后选择**存储库**。
此时将显示 **Repositories**（存储库）页面。
- 3 在“DVM 存储库”窗格中，从代表您想要优化的存储库单击 ，然后选择**执行优化作业**。
将显示一个警告提示，要求您确认优化。
- 4 单击以确认优化。
优化作业优先于大多数其他作业。如有必要，您可中断正在进行的优化作业。有关中断或恢复此作业的更多信息，请参阅[中断或恢复存储库优化作业](#)。

中断或恢复存储库优化作业

当您启动优化存储库作业时，将对所选 DVM 存储库执行重复数据消除操作。此重复数据消除优化是一项处理器密集型作业，旨在节省存储库中的空间。有关详情，请参阅[关于存储库优化作业](#)。

一旦此作业启动，您可以使用以下步骤中断作业。这会暂停重复数据消除。如果您已经中断优化，您可以使用此步骤恢复该过程。

注: 此过程仅适用于 DVM 存储库，且仅当存储库优化作业已启动时才适用。

要中断或恢复存储库优化作业，请完成此过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏中，单击 （更多），然后选择**存储库**。
此时将显示 **Repositories**（存储库）页面。

将显示“DVM 存储库”窗格。
- 3 如果要中断优化作业，请执行以下操作：
 - a 在存储库摘要表中，从代表相应存储库的行中，单击 ，然后选择**中断优化作业**。
将显示一个警告提示，要求您确认中断。
 - b 单击以确认优化。
- 4 如果要恢复中断的优化作业，请执行以下操作：
 - a 在存储库摘要表中，从代表相应存储库的行中，单击 ，然后选择**继续优化作业**。
将显示一个警告提示，要求您确认中断。
 - b 在此对话框中，选择**继续从中断点执行作业**，然后单击**是**。
该对话框将关闭，并且存储库优化作业会从最后中断点恢复。

打开现有 DVM 存储库

作为 Rapid Recovery 的主存储库技术，DVM 存储库包含具体 Rapid Recovery Core 上的受保护计算机的快照数据（以恢复点的形式）。您可以从第二个 Core (Core B) 打开第一个 Core（例如 Core A）上的现有存储库。

❗ 注: 打开另一个 Core 上的存储库会更改存储库的所有权。打开现有存储库时，仅第二个 Core 可以访问相关信息。

如果使用 DVM 存储库，则原始 Core (Core A) 不得处于当前正在使用的状态。例如，计算机必须关闭且无网络访问，或者必须停止 Core 服务。

存储库可位于共享网络位置，也可位于第二个 Core 可访问的存储设备上。

要打开现有存储库，请完成以下过程。

- 1 导航到 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （更多），然后选择**存储库**。
此时将显示 **Repositories**（存储库）页面。

“DVM 存储库”窗格也会出现。
- 3 要打开现有 DVM 存储库，在页面顶部单击**打开现有 DVM 存储库**。
此时会显示**打开现有 DVM 存储库**对话框。
- 4 在**打开现有 DVM 存储库**对话框中，输入要打开的存储库的以下信息，然后单击**打开**。

表. 33: 打开现有 DVM 存储库选项

文本框	说明
路径	存储库路径（例如，D:\work\machine 用于本地路径，或者 \\10.10.99.155\repositories 用于 IP 地址，或者 \\servername\sharename 用于网络路径）。
用户名	如果存储库有网络路径，输入登录到该网络共享的用户名。
密码	如果存储库有网络路径，输入登录到该网络共享的密码。

对话框将关闭，且所选存储库将添加到当前 Core。

删除存储库

要删除存储库，请完成以下过程中的步骤。

- 1 导航到 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （更多），然后选择**存储库**。
此时将显示 **Repositories**（存储库）页面。
存储库页面中，将显示“DVM 存储库”窗格。
- 3 在存储库摘要表中，在表示您要删除的存储库的行上，单击  以展开下拉菜单，然后选择**删除**。
此时将显示一条警告消息以确认删除。
- 4 单击**是**以确认删除存储库。

 **小心:** 删除存储库后，将丢弃其中包含的数据且无法恢复。

在 DVM 存储库上运行检查存储库作业

执行此过程以检查整个 DVM 存储库的完整性。将 AppAssure 5.3.x 升级至版本 5.4 时，建议将此过程用于复制的目标 Core。执行完整性检查的时间可能很漫长，在此期间，无法在存储库中进行其他的操作。

如果您有一个用于一个目标 Core 的多个 DVM 存储库，那么针对每个存储库执行一次此过程。

 **注:** 如果您在目标 Core 上具有另一个 DVM 存储库，其“完整性检查”作业已完成，或者如果您为此目标 Core 创建新的附加存储库，则当完整性检查作业在您指定的 DVM 存储库上运行时，您可以在第二个存储库中执行操作。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏中，单击 （更多），然后选择**存储库**。
此时将显示 **Repositories**（存储库）页面。

此时将显示“DVM 存储库”窗格。
- 3 在存储库摘要表中，从代表您要检查的存储库的行中，单击 ，并从下拉菜单中选择**检查存储库作业**。
显示确认消息。

 **小心:** 在确认是否执行此作业前，您应仔细考虑所需的时间。作业在运行的同时，不能在存储库中执行其他的事务，包括传输（快照和基本映像备份、复制）和每夜作业等。

- 4 在**检查存储库作业**对话框中，要执行完整性检查，请单击**是**。
关闭对话框。将取消正在排队或正在进行的作业，并开始完整性检查作业。
- 5 要监控存储库的“检查存储库作业”的进度（包括确定检查后是否需要进行其他步骤），请在图标栏中单击 （事件）。
- 6 从**事件**页面中，单击作业的  **作业详细信息**以查看有关作业状态的更多信息。
 - 如果您在作业的任何子任务中查看到错误，指出错误，并给 Dell 技术支持代表提供信息。
 - 如果“检查存储库作业”成功完成所有子任务，则您可以为此存储库创建自定义保留策略。

管理安全性

Core 可对存储库内的受保护机器快照数据进行加密。Core 不是对整个存储库进行加密，您可以在保护存储库内的机器期间指定加密密钥，并将这些密钥重用于不同受保护机器。每个活动的加密密钥都会创建一个加密域，因此加密不会影响性能。这样一来，通过托

管多个加密域即可使单个 Core 支持多租户环境。在多租户环境中，数据将在加密域内进行分区和重复数据消除。由于您管理着加密密钥，因此丢失卷不会泄露密钥。关键安全概念和注意事项包括：

- 在兼容 SHA-3 的密码块链 (CBC) 模式下，采用 256 位 AES 进行加密。
- 重复数据消除在加密域内进行操作，以便确保隐私。
- 进行加密时不会影响性能。
- 您可以添加、移除、导入、导出、修改和删除 Core 上配置的加密密钥。
- 在 Core 上可创建无限数量的加密密钥。

应用加密或从受保护机器中移除加密

定义加密密钥并将其应用到存储库中一个或多个受保护机器中，这样可随时确保 Core 上受保护数据安全。您可将单个加密密钥应用到任意数目受保护机器中，但任何受保护机器一次仅能使用一个加密密钥。

Rapid Recovery 中重复数据消除的范围限制为使用相同存储库和加密密钥的受保护机器。因此，要最大化重复数据消除值，Dell 建议将单个加密密钥应用到可行的尽可能多的受保护机器中。但在 Core 上可创建无限数量的加密密钥。因此，如果法律合规性、安全规则、隐私政策或其他情况对此有要求，则可添加和管理任意数目的加密密钥。之后仅可将每个密钥应用到一个受保护机器，或应用到存储库中任意一组机器。

在任何时候将加密密钥应用到受保护机器，或从受保护机器分离加密密钥时，Rapid Recovery 将在发生下个计划的或强制创建的快照时，为该机器创建新基本映像。存储在基本映像中的数据（以及当应用加密密钥时创建的所有后续增量快照）由 256 位高级加密标准保护。目前尚不知如何折中此加密方法。

如果更改当前用于受保护机器的现有加密密钥的名称或密码，则在发生下个计划的或强制创建的快照时，Rapid Recovery Core 会捕获并反映密钥经过更新的属性。存储在该映像中的数据（以及当应用加密密钥时创建的所有后续增量快照）由 256 位高级加密标准保护。目前尚不知如何折中此加密方法。

当加密密钥创建并应用于受保护机器后，移除加密包含两个概念。首先是从受保护机器取消关联密钥。（可选）在从所有受保护机器分离加密密钥后，可将其从 Rapid Recovery Core 中删除。

本部分包括以下主题：

- [将加密密钥与受保护机器相关联](#)
- [应用“受保护机器”页面中的加密密钥](#)
- [取消加密密钥与受保护机器之间的关联](#)

将加密密钥与受保护机器相关联

您可使用以下任一种方法将加密密钥应用到受保护机器：

- **作为保护机器的一部分。**当使用该方法时，可同时将加密应用到一个或多个机器。此方法使您可添加新加密密钥或将现有密钥应用到已选择的机器或其他机器。
当首次定义机器保护时要使用加密，必须在相关“保护机器向导”中选择高级选项。本选项添加“加密”页面至向导 workflow。在页面中选择**启用加密**，再选择现有加密密钥或为新密钥指定参数。有关更多信息，请分别参阅[保护机器](#)或[关于保护多台计算机](#)。
- **通过修改机器的配置设置。**本方法每次将加密密钥应用到一个受保护机器。有两种修改 Rapid Recovery UI 中计算机配置设置的方法：
 - 修改特定受保护计算机的配置设置。您要用于这种方法的加密密钥必须已存在于 Rapid Recovery Core，属于通用密钥类型，而且必须处于未锁定状态。加密是“常规”设置的一部分。有关更多信息，请参阅[查看和修改受保护机器设置](#)。
 - 单击  **未加密**图标（位于“受保护计算机”页面上）。您可使用本方法创建和应用新的加密密钥，或将现有的未锁定通用密钥分配到指定的受保护计算机。有关更多信息，请参阅[应用“受保护机器”页面中的加密密钥](#)。

应用“受保护机器”页面中的加密密钥

在将加密密钥添加至 Rapid Recovery Core 后，可将其用于任意数目的受保护机器。

如果您在一个或多个机器的初始保护期间选择了某个加密密钥，该密钥将自动应用于您使用该向导保护的任何机器。在此情况下，无需此过程。

执行以下过程：

- 如果您想要向 Core 中的任何受保护机器应用现有通用的解锁加密密钥。
- 如果您刚使用主题[添加加密密钥](#)中所述的过程添加了新加密密钥，并想将该密钥应用到受保护的机器。
- 如果加密已应用到 Core 中受保护的机器，但您想要将密钥更改为 Core 中可用的其他通用解锁密钥。

小心： 将加密密钥应用到受保护机器后，Rapid Recovery 基于下个计划的或强制创建的快照为该机器创建新基本映像。

- 1 导航到 Rapid Recovery Core 并单击[受保护机器](#)。

此时将显示[受保护的机器](#)页面，其中列出了此 Core 保护的所有机器。未应用加密密钥的机器显示打开的小锁。闭合的小锁表示受保护机器已应用加密。

- 2 在“受保护机器”窗格中，单击您要配置的受保护机器的锁定图标。

此时将显示[加密配置](#)对话框。

- 3 请执行以下步骤之一：

- 如果您想要将现有加密密钥应用到此机器，请选择[使用现有密钥通过基于 Core 的加密来加密数据](#)，然后从下拉菜单中选择相应的密钥。单击[确定](#)进行确认。
- 如果您想要将现有加密密钥更改为其他通用解锁密钥，请选择[使用新密钥通过基于 Core 的加密来加密数据](#)，然后从下拉菜单中选择相应的密钥。单击[确定](#)进行确认。
- 如果您要创建新的加密密钥并将其应用到这台受保护的机器，请选择[使用新密钥通过基于 Core 的加密来加密数据](#)。根据下表中的说明输入密钥的详细信息。

表. 34: 新加密密钥详情

文本框	说明
名称	输入加密密钥的名称。 加密密钥的名称必须包含 1 至 64 个字母数字字符。请勿使用 禁止的字符 或 禁止的短语 。
说明	输入加密密钥的描述性注释。当在 Rapid Recovery Core Console 中查看加密密钥列表时，该信息在“说明”字段中显示。说明最多可包含 254 个字符。 最佳做法是避免使用 禁止的字符 和 禁止的短语 。
密码短语	输入用于控制访问的密码短语。 最佳做法是避免使用 禁止的字符 。 将密码短语存储在安全的位置。Dell Support 无法恢复密码。一旦创建加密密钥并将其应用到一个或多个受保护机器中，则当您丢失了密码短语将无法恢复数据。
确认密码短语	重新输入密码短语。这用于确认输入的密码短语。

- 4 单击[确定](#)。

关闭对话框。指定的加密密钥已应用于该受保护机器的未来备份，现在锁显示为闭合。

（可选）如果要立即应用加密密钥，则强制创建快照。有关详情，请参阅[强制创建快照](#)。

小心: 在密码块链 (CBC) 模式中, **Rapid Recovery** 采用 **256 位** 密钥实施 **AES 256 位** 加密。虽然使用加密是可选选项, 但 **Dell** 强烈建议您创建加密密钥并保护您定义的密码。将密码短语存储在安全的位置, 因为密码短语对于数据恢复至关重要。如果没有密码短语, 将无法进行数据恢复。

取消加密密钥与受保护机器之间的关联

加密密钥应用到受保护机器后, 存储在 **Rapid Recovery Core** 中的所有后续快照数据将得以加密。

您可取消加密密钥与受保护机器之间的关联。本操作不会解密现有备份数据, 但会在下一次计划或强制创建快照时产生该机器的新基本映像。

注: 如果要按照主题**移除加密密钥**中的说明从 **Core** 中移除加密密钥, 您必须首先取消加密密钥和所有受保护机器的关联。

执行本过程, 您可取消加密密钥与特定受保护机器之间的关联。

- 1 导航到 **Rapid Recovery Core** 并单击**受保护机器**。

此时将显示受保护的机器页面, 其中列出了此 **Core** 保护的所有机器。未应用加密密钥的机器将显示打开的小锁 。闭合的小锁  表示受保护机器已应用加密。

- 2 在“受保护机器”窗格中, 单击您要配置的受保护机器的  **已加密** 图标。
此时将显示**加密配置**对话框。
- 3 选择**使用含现有密钥的基于 Core 的加密来加密数据**, 然后从下拉菜单中选择 **(无)** 并单击**确定**。
- 4 如果您要将加密密钥从 **Rapid Recovery Core** 中移除, 首先使用该密钥为所有受保护机器重复本过程。然后执行主题**移除加密密钥**中说明的过程。

管理加密密钥

要管理 **Rapid Recovery Core** 的加密密钥, 单击图标栏中的  (更多), 然后选择**加密密钥**。此时将显示**加密密钥**页面。对于每个添加到 **Rapid Recovery Core** 中的加密密钥 (如果已定义), 您将看到下表所述的信息。

表. 35: 关于每个加密密钥的信息

UI 元素	说明
选择项	对于每个加密密钥, 您可以选中复选框以执行表上方菜单选项列表中的操作。
名称	与加密密钥关联的名称。
指纹	该参数是随机生成的英文大小写字母的 26 个字符的字母字符串, 可唯一确定每个加密密钥。
类型	类型描述了加密密钥的起始点及其要应用的能力。加密密钥可包含两种可能的类型之一: 通用。通用类型是当您创建加密密钥时的默认条件。与未锁定状态相结合的通用类型的密钥表示密钥可应用到受保护计算机。您无法手动锁定通用密钥类型; 您必须改为首先按过程更改加密密钥类型中的说明更改密钥类型。 复制。当源 Core 中的受保护计算机已启用加密时, 该计算机的恢复点将复制到目标 Core 中, 源中使用的任何加密密钥将自动显示在目标 Core 中并具有“复制”类型。收到复制密钥后的默认状态是锁定。您可通过提供密码解锁类型为“复制”的加密密钥。如果密钥类型为“未锁定”, 则您可手动锁定该密钥。有关更多信息, 请参阅主题解锁加密密钥。
州	状态表示是否可使用加密密钥。两种可能的状态如下: • 未锁定。未锁定状态表示可立即使用密匙。例如, 您可为受保护机器加密快照, 或执行目标 Core 上的复制恢复点的数据恢复。

- **已锁定。** 锁定状态表示密钥在通过提供密码短语解锁前无法使用。锁定是新导入的或复制的加密密钥的默认状态。

如果加密密钥的状态为已锁定，则在使用前必须将其解锁。

如果您之前解锁了已锁定的加密密钥，且已超出保持未锁定的时间，则状态将从未锁定更改为锁定。在密钥自动锁定后，您必须再次解锁密钥，这样才可使用它。有关更多信息，请参阅主题[解锁加密密钥](#)。

说明

说明是可选字段，建议提供关于加密密钥的有用信息，例如，其预期用途或密码短语提示信息。

在“加密密钥”窗格顶层，您可使用从另一 Rapid Recovery Core 中导出的文件添加加密密钥或导入密钥。您也可以删除摘要表中选择的密钥。

Core 具有加密密钥后，您可通过编辑名称或说明属性、更改密码、解锁已锁定的加密密钥或从 Rapid Recovery Core 中移除密钥等方式来管理现有密钥。您也可将密钥导出到文件中，该文件可导入到其他 Rapid Recovery Core。

当您从[加密密钥](#)页面中添加加密密钥时，密钥将在加密密钥列表中显示，但不应用到特定受保护计算机。关于如何应用从[加密密钥](#)窗格中创建的加密密钥，或如何从 Rapid Recovery Core 中完全删除密钥的相关信息，请参阅[应用加密或从受保护机器中移除加密](#)。

在[加密密钥](#)窗格中，您可以在存储库中管理保存到受保护计算机 Core 中的备份数据安全性，可通过执行以下操作实现：

- [添加加密密钥](#)
- [导入加密密钥](#)
- [解锁加密密钥](#)
- [编辑加密密钥](#)
- [更改加密密钥密码短语](#)
- [导出加密密钥](#)
- [移除加密密钥](#)
- [更改加密密钥类型](#)

添加加密密钥

在密码块链 (CBC) 模式中，Rapid Recovery 采用 256 位密钥实施 AES 256 位加密。虽然使用加密是可选选项，但 Dell 强烈建议您创建加密密钥并保护您定义的密码。

△ | 小心： 将密码存储在安全的位置。如果没有密码，您无法从加密的恢复点恢复数据。

在定义加密密钥后，您可使用它保护数据。加密密钥可由任意数目的受保护机器使用。

本步骤介绍如何从 Rapid Recovery Core Console 添加加密密钥。本过程不将密钥应用到当前正在 Core 上受保护的机器。您也可在保护机器过程中添加加密密钥。有关添加加密作为保护机器一部分的更多信息，请参阅[保护机器](#)。有关在初始保护时添加加密到两个或更多机器的更多信息，请参阅[关于保护多台计算机](#)。

要添加加密密钥，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏上，单击 （更多），然后选择**加密密钥**。
此时将显示**加密密钥**页面。
- 3 单击**添加加密密钥**。
此时将显示**创建加密密钥**对话框。
- 4 在**创建加密密钥**对话框中，根据下表中的说明输入密钥的详细信息。

表. 36: 创建加密密钥详情。

文本框	说明
名称	输入加密密钥的名称。 加密密钥的名称必须包含 1 至 64 个字母数字字符。请勿使用 禁止的字符 或 禁止的短语 。
说明	输入加密密钥的注释。 当从 Core Console 中查看加密密钥时，该信息在“说明”字段中显示。最多可输入 254 个字符。 最佳做法是避免使用 禁止的字符 和 禁止的短语 。
密码短语	输入用于控制访问的密码短语。 最佳做法是避免使用 禁止的字符 。
 小心: 将密码短语存储在安全的位置。Dell 支持无法恢复密码短语。一旦创建加密密钥并将其应用到一个或多个受保护机器中，则当您丢失了密码短语将无法恢复数据。	
确认密码	重新输入密码短语。这用于确认输入的密码短语。

- 单击 **确定**。
随即关闭对话框，且所创建的加密密钥将显示在“加密密钥”页面中。
- 如果要加密密钥应用到受保护机器，请参阅 [应用“受保护机器”页面中的加密密钥](#)。

导入加密密钥

您可从其他 Rapid Recovery Core 导入加密密钥，并使用该密钥为您 Core 中受保护机器的数据加密。要导入密钥，您必须能够从 Core 机器访问它，本地或通过网络。您还必须了解加密密钥的密码。

要导入加密密钥，请完成以下过程中的步骤。

① | 注: 本过程不将密钥应用到受保护机器。有关应用密钥的更多信息，请参阅 [应用“受保护机器”页面中的加密密钥](#)。

- 导航到 Rapid Recovery Core。
- 在图标栏上，单击 （更多），然后选择 **加密密钥**。
此时将显示 **加密密钥** 页面。
- 单击  **导入**。
此时将显示 **文件上传** 对话框。
- 在 **文件上传** 对话框中，导航到包含要导入之加密密钥的网络或本地目录。
例如，导航到已登录用户的 **下载** 文件夹。

密钥文件名以“EncryptionKey-”开头，接着是密钥 ID，最后以文件扩展名“.key”结尾。例如，示例加密密钥名称为 EncryptionKey-RandomAlphabeticCharacters.key。

- 选择要导入的密钥，然后单击 **打开**。
- 在 **导入密钥** 对话框中，单击 **确定**。
对话框将关闭，且导入的加密密钥将显示在 **加密密钥** 页面中。如果加密密钥在导出前用于保护卷，则密钥状态为“锁定”。

解锁加密密钥

加密密钥可能包含未锁定或锁定状态。未锁定的加密密钥可应用于受保护机器以确保为存储库中机器保存的备份数据的安全。在一个使用未锁定加密密钥的 Rapid Recovery Core 中，您也可从恢复点恢复数据。

当您加密密钥导入到 Rapid Recovery Core 中，其默认状态是“已锁定”。不论是否明确导入密钥或加密密钥是否添加到 Rapid Recovery Core 中（通过复制加密的受保护机器或导入加密的恢复点存档）皆是如此。

对于仅通过复制添加到 Rapid Recovery Core 中的加密密钥，当解锁密钥时，您可为加密密钥指定持续时间（按小时数、天数或月数）以保持已解锁状态。每天都以 24 小时为准，从解锁请求保存到 Rapid Recovery Core 的时间算起。例如，如果在周二 11:24 AM 解锁密钥且选择的持续时间是 2 天，则密钥会在同周的周四 11:24 AM 自动再解锁。

① | 注: 您不能使用锁定的加密密钥恢复数据或将其使用到受保护机器。您必须首先提供密码短语，然后解锁密钥。

您也可锁定未锁定的加密密钥，确保其在解锁前无法应用到任何受保护机器。要锁定“通用”状态下的加密密钥，您必须首先更改其状态为“已复制”。

如果未锁定加密密钥目前正用于保护 Core 中的机器，则您必须在将其锁定前取消其受保护机器的关联。

要解锁已锁定的加密密钥，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core。
- 2 在图标栏中，单击 （更多），然后选择**加密密钥**。
此时将显示**加密密钥**页面。“状态”栏表示已锁定的加密密钥有哪些。
- 3 找到您想要解锁的加密密钥，然后单击它的下拉菜单 ，并选择**解锁**。
将显示**解锁加密密钥**对话框。
- 4 在对话框的“密码”字段中，输入密码以解锁此密钥。
- 5 要指定密钥保持未锁定状态的持续时间，在“持续时间”选项中，请执行下列操作之一：
 - 要指定密钥在您明确锁定它之前保持已解锁状态，请在 Rapid Recovery 中选择**直至手动锁定**。
 - 要指定密钥在您配置的持续时间（单位为小时、天或月）内保持锁定，请执行以下操作：
 - 选择数字字段，输入 1 到 999 之间的值。
 - 将持续时间数字分别指定为小时、天或月。
 - 然后单击**确定**。该选项适用于通过复制添加的加密密钥。

随即关闭对话框，且所选加密密钥的更改将显示在“加密密钥”页面中。

- 要指定密钥在您指定的日期和时间之前保持锁定，请执行以下操作：
 - 选择**直到**选项。
 - 在文本字段中，或使用日历和时钟小部件，明确指定您想要加密密钥锁定的日期和时间。
 - 然后单击**确定**。该选项适用于通过复制添加的加密密钥。

随即关闭对话框，且所选加密密钥的更改将显示在“加密密钥”页面中。

锁定加密密钥

当某加密密钥状态已锁定时，它将无法应用到任何受保护的计算机，直到它解锁。要锁定“通用”类型的加密密钥，您必须首先将其类型更改为“已复制”。

要锁定加密密钥，请完成以下过程中的步骤。

- 1 导航到 Rapid Recovery Core。
- 2 在图标栏上，单击 （更多），然后选择**加密密钥**。
此时将显示**加密密钥**页面。“状态”列表示未锁定的加密密钥并显示每个密钥的类型。
- 3 找到您想要锁定的加密密钥。如果其类型为“通用”，则单击其下拉菜单 ，然后选择**将类型更改为“已复制”**。

此时将显示**更改加密密钥类型**对话框。

- 4 在此对话框中，确认要将密钥类型更改为**已复制**。
- 5 如果您已成功将加密密钥状态更改为“已复制”，则单击其下拉菜单 ，然后选择**锁定**。
此时将显示**锁定加密密钥**对话框。
- 6 在此对话框中，确认要锁定加密密钥。
关闭对话框，现在选择的加密密钥状态为已锁定。

 **注：**该选项适用于通过复制添加的加密密钥。

编辑加密密钥

定义加密密钥后，您可编辑加密密钥名称或密钥说明。当您在“加密密钥”窗格中查看加密密钥列表时，这些属性是可见的。

要编辑现有未锁定的加密密钥的名称或说明，请完成以下过程中的步骤。

 **小心：**编辑用于保护一台或多台机器加密密钥的名称或说明后，**Rapid Recovery** 会创建新的基本映像。该基本映像快照会在基于下个计划或强制快照发生于该机器上。

- 1 导航到 Rapid Recovery Core。
- 2 在图标栏上，单击 （更多），然后选择**加密密钥**。
此时将显示**加密密钥**页面。
- 3 找到您想要编辑的加密密钥，然后执行以下操作：
 - 如果密钥已锁定，您必须首先为其解锁。请参阅[解锁加密密钥](#)
 - 如果密钥已解除锁定，继续执行下述步骤。
- 4 单击下拉菜单  以指定加密密钥，然后选择**编辑**。
此时将显示 **Edit Encryption Key**（编辑加密密钥）对话框。
- 5 在该对话框中，编辑加密密钥的名称或说明，然后单击**确定**。
对话框将关闭，且所选加密密钥的更改将显示在**加密密钥**页面中。

更改加密密钥密码短语

要维护最大化安全性，您可为现有加密密钥更改密码短语。要更改加密密钥的密码短语，请完成以下过程中的步骤。

 **小心：**编辑用于保护一台或多台计算机的加密密钥的密码后，**Rapid Recovery Core** 会基于下个计划或强制快照为该计算机捕获增量快照。

- 1 导航到 Rapid Recovery Core。
- 2 在图标栏上，单击 （更多），然后选择**加密密钥**。
此时将显示**加密密钥**页面。
- 3 找到想要更新的加密密钥，单击其下拉菜单 ，然后选择**更改密码短语**。
此时将显示 **Change Passphrase**（更改密码短语）对话框。
- 4 在对话框的**密码**字段中，为加密密钥输入新密码。
- 5 在**确认密码**字段中，重新输入完全相同的密码。
- 6 单击**确定**。
随即关闭对话框，且密码短语将更新。
- 7 或者，如果您在“说明”字段中使用提示，则编辑加密密钥以更新提示。有关详情，请参阅[编辑加密密钥](#)。

 **小心:** 在带有 256 位键的密码块链 (CBC) 模式中, **Rapid Recovery** 采用 AES 256 位加密。**Dell** 建议将密码记录在安全位置, 并保持更新此信息。**Dell Support** 无法恢复密码。没有密码, 您将无法从加密的恢复点恢复信息。

导出加密密钥

您可从任何 Rapid Recovery Core 中导出加密密钥, 这样可专门在其他 Core 中使用它。执行该过程时, 密钥会保存到活动 Windows 用户帐户的**下载**文件夹中。

要导出加密密钥, 请完成以下过程中的步骤。

- 1 导航到 Rapid Recovery Core。
- 2 在图标栏上, 单击  (更多), 然后选择**加密密钥**。
此时将显示**加密密钥**页面。
- 3 找到您想要导出的加密密钥的位置, 然后单击其下拉菜单 , 然后选择**导出**。
此时会出现**打开 EncryptionKey-[name.key]**对话框。
- 4 在对话框中, 选择**保存文件**以便在安全位置保存并存储加密密钥, 然后单击**确定**。
加密密钥将作为文本文件下载到默认位置, 如活动 Windows 用户帐户的**下载**文件夹。
- 5 或者, 如果您想要将此密钥导入到不同的 Core, 可将文件复制到该 Core 上的可访问位置。

移除加密密钥

当您在“加密密钥”页面上删除加密密钥时, 密钥会从 Rapid Recovery Core 中删除。

 **注:** 删除加密密钥不会解密已使用此密钥保存的恢复点。您仍必须保留并提供密钥的密码才能为现有加密的恢复点恢复数据。

您无法移除已与任何受保护机器相关联的加密密钥。您必须首先使用密钥查看每个受保护机器的加密设置, 并取消关联要移除的加密密钥。有关更多信息, 请参阅主题[取消加密密钥与受保护机器之间的关联](#)。

要移除加密密钥, 请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core。
- 2 在图标栏中, 单击  (更多), 然后选择**加密密钥**。
此时将显示**加密密钥**页面。
- 3 找到您要删除的加密密钥。单击它的下拉菜单 , 并选择**移除**。
此时将显示**移除加密密钥**对话框。此时将显示一条消息, 要求确认移除加密密钥操作。
- 4 在对话框中, 确认要删除加密密钥。

 **注:** 删除加密密钥不会解密已使用此密钥保存的恢复点。您仍必须保留并提供密钥才能为现有加密的恢复点恢复数据。

对话框随即关闭, 且删除的加密密钥将不再显示在**加密密钥**页面中。

更改加密密钥类型

加密密钥在“加密密钥”窗格中列出两种可能类型之一: “通用”或“复制”。类型表示加密密钥可能的起始点, 并可确定您是否可更改其详细信息或密码。仅当类型是“通用”时才可修改这些属性。如果您需要修改“已复制”类型中密钥的这些属性, 您必须使用该过程将其类型更改为“通用”。当您把加密密钥的类型改为“通用”时, 需手动解锁并且它可用于加密其他受保护机器。

 **注:** 您必须知道密码以将类型从“已复制”更改为“通用”。

加密密钥也有两种可能状态：“锁定”或“未锁定”。该状态控制您将加密密钥应用到受保护机器或从加密恢复点还原数据的能力。仅当状态为“未锁定”时可手动更改加密密钥状态。

首次创建加密密钥时，其类型是“通用”且状态为“未锁定”。您可立即使用这样一个密钥（例如，加密受保护机器的备份）。但是，无法手动锁定“通用”密钥类型。如果要手动锁定“通用”类型的加密密钥，您必须使用该过程将类型更改为“已复制”。

如果加密密钥已用于加密一台或多台受保护机器的恢复点，则无法更改其类型。

按照此过程更改加密密钥类型。

- 1 导航到 Rapid Recovery Core。
- 2 在图标栏上，单击 （更多），然后选择**加密密钥**。
此时将显示**加密密钥**页面。Core 可访问的任何加密密钥都在摘要表中显示。每个加密密钥都列出“通用”或“已复制”类型。
- 3 找到您想要更新的加密密钥。
- 4 如果要“通用”加密密钥更改为“复制”，可执行以下操作：
 - a 单击其下拉菜单 ，然后选择**将类型更改为“已复制”**。
此时将显示**更改加密密钥类型**对话框。您将看到一条消息，以确认您想要将类型更改为“已复制”。
 - 在对话框中，确认您想要将类型更改为“复制”。对话框将关闭，且加密密钥类型将更新为“复制”。
- 5 如果要“复制”加密密钥更改为“通用”，需执行以下操作：
 - a 单击其下拉菜单 ，然后选择**将类型更改为“通用”**。
此时将显示**更改加密密钥类型**对话框。您将看到一条消息，以确认您想要将类型更改为“通用”。
 - 在对话框中，在**密码**字段中输入密码，然后单击**确定**以确认您想要将类型更改为“通用”。对话框将关闭，且加密密钥类型将更新为“通用”。

管理云帐户

本节介绍如何定义现有的云存储提供商的帐户链接，以及如何管理这些用于 Rapid Recovery 的云帐户。例如，您可以将 Rapid Recovery 数据存档到云，或从云中导入存档数据。

关于云帐户

Rapid Recovery 允许您将数据存档到一系列云提供商，或导入存储在云帐户中的已存档数据。兼容的云服务包括 Microsoft Azure、Amazon™、Rackspace 和任何基于 OpenStack 的提供商。

您可以将现有云帐户添加到 Rapid Recovery Core Console。添加后，您可以编辑信息、配置帐户连接选项，或从 Rapid Recovery 中删除帐户。

添加云帐户

在云帐户与您的 Core 之间朝任一方向移动数据之前，必须将云提供商帐户信息添加到 Rapid Recovery Core Console。当安全地缓存连接信息时，此信息会在 Core Console 中标识云帐户。然后，此过程会让 Rapid Recovery Core 连接到云帐户以执行您指定的操作。

要添加云帐户，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 图标栏上，单击  **更多**图标，然后选择**云帐户**。

此时会显示云帐户页面。

- 2 在云帐户页面中，单击**添加新帐户**。

此时将打开 **Add New Account**（添加新帐户）对话框。

- 3 从“云类型”下拉列表中选择兼容的云服务提供商。
- 4 根据在步骤 3 中选择的云类型，输入下表所述详细信息。

表. 37: 云帐户详细信息

云类型	文本框	说明
Microsoft Azure	存储帐户名称	输入 Microsoft Azure 存储帐户名称。 注: 该名称必须与 Azure 中的存储帐户名称精确匹配。名称只能包含小写字母和数字，长度在 3 到 24 个字符 之间。
	访问密钥	输入帐户的访问密钥。 注: 可以输入主要或次要密钥。要从您的 Azure 帐户获取访问密钥，请在设置下选中密钥。
	使用 https 协议	选择此选项以使用安全 https 协议，而非标准 http 协议。
	显示名称	输入此云帐户显示在 Rapid Recovery Core Console 上的显示名称；例如 Microsoft Azure 1。
Amazon™ S3	访问密钥	输入您 Amazon™ 云帐户的访问密钥。
	保密密钥	输入该帐户的保密密钥。
	显示名称	输入此云帐户显示在 Rapid Recovery Core Console 上的显示名称；例如 Amazon 1。
OpenStack 技术支持	地区	输入您云帐户的地区。
	用户名	输入基于 OpenStack 的云帐户的用户名。
	密码或 API 密钥	选择要使用密码还是 API 密钥，然后输入您对此帐户的选择。
	租户 ID	输入该帐户的租户 ID。
	验证 URL	输入该帐户的验证 URL。
	显示名称	输入此云帐户显示在 Rapid Recovery Core Console 上的显示名称；例如，OpenStack 1。
Rackspace Cloud 文件	地区	使用下拉列表为您的帐户选择地区。
	用户名	输入 Rackspace 云帐户的用户名。
	密码或 API 密钥	选择要使用密码还是 API 密钥，然后输入您对此帐户的选择。
	租户 ID	输入该帐户的租户 ID。
	验证 URL	输入该帐户的验证 URL。
	显示名称	输入此云帐户显示在 Rapid Recovery Core Console 上的显示名称；例如 Rackspace 1。

- 5 单击**保存**。

此时，对话框会关闭，您的帐户将出现在 Core Console 的**云帐户**页面上。

编辑云帐户

如果您需要更改信息以连接到云帐户，例如要更新密码或编辑显示名称，您可以在 Rapid Recovery Core Console 的“云帐户”页面上进行操作。要编辑云帐户，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 图标栏上，单击  **更多**图标，然后选择**云帐户**。
此时会显示**云帐户**页面。
- 2 在要编辑的云帐户旁边，单击下拉菜单，然后单击**编辑**。
此时将打开**编辑帐户**窗口。
- 3 根据需要编辑详细信息，然后单击**保存**。

 **注：**无法编辑云类型。

配置云帐户设置

云配置设置可让您确定 Rapid Recovery 连接到云帐户时的尝试连接间隔时间（超时之前）。要配置云帐户的连接设置，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 图标栏中，单击  **设置**。
此时将显示“设置”页面。
- 2 在左侧菜单中，单击**云帐户**。
- 3 在“云帐户”表中，单击要配置的云帐户旁边的下拉菜单，然后执行下列操作之一：
 - 要更改云帐户连接设置，请单击**编辑**。
 - 1 在“云配置”对话框中，执行以下任意操作：
 - 对于**请求超时**，请使用向上和向下箭头以确定在存在延迟的情况下，Rapid Recovery 在单次尝试连接到云帐户的过程中应花费的时间（以分钟和秒为单位）。输入的时间用完后，连接尝试将停止。
 - 对于**写入缓冲区大小**，请输入您要保留用于将存档数据写入云的缓冲区大小。
 - 对于**读取缓冲区大小**，请输入您要保留用于从云读取存档数据的块大小。
 - 2 单击**确定**。
 - 要将云配置返回到以下默认设置，请单击**重置**。
 - **请求超时**：01:30（分钟和秒）
 - **写入缓冲区大小**：8388608（字节）
 - **读取缓冲区大小**：8388608（字节）

删除云帐户

如果停止云服务，或决定停止将其用于特定的 Core，您可能想从 Core Console 删除您的云帐户。要删除云帐户，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 图标栏上，单击  **更多**图标，然后选择**云帐户**。
此时会显示**云帐户**页面。
- 2 在要编辑的云帐户旁边，单击下拉菜单，然后单击**删除**。
- 3 在**删除帐户**对话框中，单击**是**以确认要移除该帐户。

4 如果云帐户当前正在使用，会显示另一个对话框以询问您是否仍要删除。单击**是**进行确认。

注: 删除当前正在使用的帐户会导致此帐户计划的所有存档作业失败。

存档

本节介绍了创建存档的业务案例、如何使用 Rapid Recovery 创建存档以及可以将其存储在哪里。

了解存档

保留策略用于确定在短期（快速且昂贵）介质上存储备份的期限。有时，某些业务和技术要求延长这些备份的保留期限，但是使用快速存储的成本过高。因此，这种要求促成了长期（速度慢、价格低）存储的需要。企业通常使用长期存储来存档合规和非合规数据。Rapid Recovery 中的存档功能用于为延长保留合规和非合规数据提供支持；同时还用于将复制数据播种到远程复制 Core。

创建存档后，可通过以下方式使用存档：

- 存档可以安装为简单文件或文件夹恢复的文件系统。
- 存档可以用作裸机还原的来源。
- 存档可以导入到存储库中。

创建存档

您可以使用此步骤创建一次性或计划的存档。

如果您计划将存档创建到云位置，请首先将您的云帐户添加到 Rapid Recovery Core Console。有关详情，请参阅[添加云帐户](#)。

一次性存档是为指定机器按需创建的存档。计划的存档是按向导中指定的日期和时间自动定期创建的存档。计划定期存档的能力适用于此类情况：希望对要保存的机器进行频繁存档，但又无需面对每次手动创建存档带来的不便。

- 
- 1 在 Rapid Recovery Core Console 的按钮栏上，单击 **存档**。
将打开“存档向导”。
 - 2 在向导的**存档类型**页面上，选择下列选项之一：
 - 一次性存档
 - 持续存档（按计划）
 - 3 单击**下一步**。
 - 4 在**位置**页面中，从**位置类型**下拉式列表中选择一个选项，然后根据下表中的说明输入信息。

表. 38: 存档位置类型选项

选项	文本框	说明
本地	位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：d:\work\archive。
网络	位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：\\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络共享的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。

选项	文本框	说明
① 注: 要选择云帐户, 您必须先在 Core Console 中添加云帐户。有关详情, 请参阅 添加云帐户 。		
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	为将保存存档数据的文件夹输入名称。

- 5 单击**下一步**。
- 6 在向导的**机器**页面中, 选择要存档的受保护机器。
- 7 单击**下一步**。
- 8 请执行以下步骤之一:
 - 如果您选择创建一次性存档, 请转到[步骤 15](#)。
 - 如果您选择创建计划的存档, 请继续执行[步骤 9](#)
- 9 在**计划**页面上, 从**发送数据**下拉式列表中选择以下其中一个选项:
 - 每天
 - 每周
 - 每月
- 10 根据您在[步骤 9](#)中的选择, 输入下表中所述的信息。

表. 39: 发送数据选项

选项	文本框	说明
每天	指定设备执行该命令的时间	选择要创建的每日存档的小时数。
每周	周的某一天	选择一周中的某一天以自动创建存档。
	指定设备执行该命令的时间	选择您希望创建存档的某天的小时。
每月	月的某一天	选择一月中的某一天以自动创建存档。
	指定设备执行该命令的时间	选择您希望创建存档的某天的小时。

- 11 (可选) 完成向导后, 如果您不想存档作业在下一个计划的时间开始, 请选择**暂停初始存档**。

① | 注: 如果您在恢复存档前需要时间准备目标位置, 您可能要暂停计划存档。如果不选择此选项, 在计划时间开始归档。

- 12 单击**下一步**。
- 13 在持续存档的**选项**页面上, 选择下表中的其中一个循环操作。

表. 40: 持续存档循环选项

文本框	说明
Incremental (增量)	让您添加恢复点到现有存档。它会将恢复点进行比较, 以免复制已经在存档中存在的。
替换此 Core	覆盖与此 Core 相关的任何预先存在的存档数据, 但其他 Core 的数据保持不变。
完全擦除	从目录清除所有存档数据, 然后再写入新存档。

- 14 (可选) 选择 **建立恢复点链 (修复孤立恢复点)**, 然后跳至[步骤 18](#)。
- 15 在一次性存档的**选项**页面中, 根据下表中的说明输入信息。

表. 41: 一次性存档选项

文本框	说明
最大大小	大型数据存档可以分为多个段。要选择要为创建存档保留的最大空间量，请执行以下操作之一： - 选择整个目标以保留在 步骤 4 中指定目标上的指定路径中的所有可用空间。（例如，如果位置为 D:\work\archive，则将保留 D: 驱动器上的所有可用空间）。 - 选择空白文本框，使用向上和向下箭头输入所需的空間量，然后从下拉列表中选择度量单位以自定义要保留的最大空间。 注: Amazon™ 云存档自动分成 50 GB 的分段。Microsoft Azure 云存档自动分成 200 GB 的分段。
循环操作	选择以下循环操作选项之一： - 请勿重复使用。不覆盖或删除此位置的任何现有已存档数据。如果位置为空，Rapid Recovery 允许您选择其他位置。 - 替换此 Core。覆盖与此 Core 相关的任何预先存在的存档数据，但其他 Core 的数据保持不变。 - 完全擦除。从目录清除所有存档数据，然后再写入新存档。 - 增量。让您添加恢复点到现有存档。它会将恢复点进行比较，以免复制已经在存档中存在的数据。
注释	输入捕获存档时所必需的任何附加信息。如果日后导入存档，则将显示注释。
建立恢复点链（修复孤立恢复点）	选择此选项以存档整个恢复点链。默认情况下，将选中此选项。

16 单击**下一步**。

17 在**日期范围**页面中，手动输入要存档的恢复点的开始日期和结束日期，或通过单击日历窗口下方的时钟图标后面的日历图标来选择日期时间。

18 单击**完成**。

此时将关闭向导。

存档到云

当数据到达保留期截至日期，您可能希望通过创建旧数据存档延长保留期。将数据存档时，总会出现存放在哪里的问题。Rapid Recovery 允许您直接从 Core Console 上传存档到多个云服务提供商。兼容的云服务包括 Microsoft Azure、Amazon™、Rackspace 和任何基于 OpenStack 的提供商。

使用 Rapid Recovery 导出存档到云涉及以下过程：

- 添加云帐户到 Rapid Recovery Core Console。有关更多信息，请参阅[添加云帐户](#)。
- 归档数据并将其导出到云帐户。有关更多信息，请参阅[创建存档](#)。
- 通过将其从云位置导入，从而检索存档数据。有关更多信息，请参阅[导入存档](#)。

编辑计划存档

Rapid Recovery 允许您更改计划存档的详细信息。要编辑计划存档，请完成以下过程中的步骤。

- 在 Rapid Recovery Core Console 中，单击图标栏上的  **更多** 下拉菜单，然后选择**存档**。
- 在“存档”页面的“计划存档”下，单击您要更改的存档旁边的下拉菜单，然后单击**编辑**。
将打开**添加存档向导**。
- 在“存档向导”的**位置**页面上，从**位置类型**下拉式列表中选择以下选项之一：
 - 本地
 - 网络

- 云

4 根据您在 [步骤 3](#) 中选择的位置类型，输入存档的详细信息，如下表所述。

表. 42: 存档详情

选项	文本框	说明
本地	位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：d:\work\archive。
网络	位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：\\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络共享的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。
	① 注: 要选择云帐户，您必须先在 Core Console 中添加云帐户。有关详情，请参阅 添加云帐户 。	
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	为您要在其中保存存档数据的文件夹输入一个名称；例如，Rapid-Recovery-Archive-[创建日期]-[创建时间]。

5 单击**下一步**。

6 在向导的**机器**页面中，选择包含要存档的恢复点的受保护机器。清除您不想存档的机器。

7 单击**下一步**。

8 在**计划**页面上，从**发送数据**下拉式列表中选择以下其中一个选项：

- 每天
- 每周
- 每月

9 根据您在 [步骤 8](#) 中的选择，输入下表中所述的信息。

表. 43: 发送数据选项

选项	文本框	说明
每天	指定设备执行该命令的时间	选择要创建的每日存档的小时数。
每周	周的某一天	选择一周中的某一天以自动创建存档。
	指定设备执行该命令的时间	选择要创建的每日存档的小时数。
每月	月的某一天	选择一月中的某一天以自动创建存档。
	指定设备执行该命令的时间	选择要创建的每日存档的小时数。

10 （可选）要推迟存档并在以后恢复，请选择**暂停初始存档**。

① | **注:** 如果您在恢复存档前需要时间准备目标位置，您可能要暂停计划存档。如果不选择此选项，在计划时间开始归档。

11 单击**下一步**。

12 在**选项**页面上，使用**循环操作**下拉式列表选择下表中所述的其中一个选项：

表. 44: 存档循环选项

文本框	说明
Incremental (增量)	让您添加恢复点到现有存档。它会将恢复点进行比较，以免复制已经在存档中存在的数据。
替换此 Core	覆盖与此 Core 相关的任何预先存在的存档数据，但其他 Core 的数据保持不变。
完全擦除	从目录清除所有存档数据，然后再写入新存档。

13 (可选) 选择**建立恢复点链**(**修复孤立修复的**)。

14 单击**完成**。

Rapid Recovery 将您的更改应用到存档。

暂停或恢复计划存档

如果您具有计划定期重复的存档作业，您可以根据需要暂停或恢复此操作。

可能有时候，您想暂停计划的存档作业，例如，您需要对目标存档位置作出更改时。另外，执行**创建存档**过程时，如果选择初始时暂停存档，您可能稍后要恢复计划的存档。要暂停或恢复计划存档，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 中，单击图标栏上的  **更多** 菜单，然后单击**存档**。
- 2 在“计划的存档”下方的**存档**页面中，执行以下操作之一：
 - 选择首选存档，然后单击以下相应的操作之一：
 - Pause
 - Resume
 - 在首选存档旁边，单击下拉菜单，然后单击以下相应的操作之一：
 - Pause
 - Resume

计划栏中显示存档的状态。

强制执行存档作业

通过使用此过程，您可以随时强制 Rapid Recovery 在计划存档上执行存档作业。

要强制执行存档作业，您必须在 Core 上计划存档。

- 1 从 Rapid Recovery Core Console 的图标栏中，单击  **更多** 下拉列表，然后选择**存档**。
- 2 在“存档”页面的“计划存档”下，单击您要强制执行的存档旁边的下拉菜单，然后单击**编辑**。

Rapid Recovery 按照您为该存档选择的设置存档恢复点，而不考虑您设置的计划存档时间。

检查存档

检查存档会验证存档及其内容是否足够良好，足以进行还原。

您可以通过执行存档检查来扫描存档的结构、数据分段和索引文件的完整性。存档检查会验证存档内是否存在所有必要的文件以及文件是否良好。要执行存档检查，完成下列过程中的步骤。

- 
- 在 Rapid Recovery Core Console 中，单击图标栏上的 **更多** 下拉菜单，然后选择 **存档**。
 - 在 **存档** 页面中，单击 **检查**。
此时将显示 **Check Archive（检查存档）** 对话框。
 - 对于 **Location Type（位置类型）**，从下拉列表中选择以下选项之一：
 - 本地
 - 网络
 - 云
 - 根据您在 **步骤 3** 中选择的位置类型，按照下表中的说明输入存档的详细信息。

表. 45: 存档详情

选项	文本框	说明
本地	位置	输入存档的路径。
网络	位置	输入存档的路径。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络路径的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。
		 注: 要选择云帐户，您必须先 在 Core Console 中添加云帐户 。有关详情，请参阅 添加云帐户 。
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	选择保存存档数据的文件夹名称；例如，Rapid Recovery -5-Archive-[创建日期]-[创建时间]

- 选中或清除下表中说明的复选标记。默认全部选中。

 **注:** 请勿清除全部复选标记。您必须选择至少一个选项。

选项	说明
映射偏移量的索引文件	此选项会检查存档内部结构上的所有数据是否位于正确位置。
结构完整性	此选项可验证是否存在某些内部文件以及验证存档的文件夹结构。如果缺少任何文件或文件夹，检查将失败。
校验和完整性	此选项会检查存档中数据分段的完整性以确保数据分段处于良好状态。

- 单击 **检查文件**。
Rapid Recovery 会根据您的选择检查存档。

附加存档

通过附加存档，您可以查看来自存档的恢复点。

您必须具有在 Rapid Recovery Core 6.0.1 或更高版本中创建的、预先存在的存档才能完成此过程。有关详情，请参阅 [创建存档](#)。

当您附加存档时，您提供的存档名称在 Core Console 的左侧导航菜单中显示为一个存档菜单。存档中带有恢复点的每个受保护机器均在存档菜单下单独列出。您可以单击存档中的任何机器名称并浏览它的恢复点。然后，您可以对 Core 中当前可见的任何其他恢复点执行相同的操作。

附加存档还会缓存用于访问信息的凭据。在删除附加存档定义之前，您可以轻松地重新附加和分离存档，从而可以轻松访问它的恢复点。

使用此过程附加存档。

- 
- 在 Rapid Recovery Core Console 上，单击 **存档** 下拉菜单，然后选择 **附加存档**。
将显示**附加存档**对话框。
 - 在**名称**文本框中，输入此附加存档的名称。
您在此字段中键入的值将作为存档菜单名称显示在左侧导航菜单中。

根据适用于显示名称的最佳做法，存档名称应包含 1 到 64 个字母数字字符（含空格）。请勿使用**禁止字符**。或**禁止短语**。

- 在**位置类型**下拉式列表中，从以下选项中选择您的存档的位置类型：
 - 本地
 - 网络
 - 云
- 根据您在**步骤 3** 中选择的位置类型，输入存档的详细信息，如下表所述。

表. 46: 位置类型详细信息

选项	文本框	说明
本地	位置	输入存档的路径；例如 D:\Work\Archive。
网络	位置	输入存档的路径；例如 \\servername\sharename。
	用户名	输入用于登录网络共享的用户名。
	密码	输入用于登录网络共享的密码。
云	帐户	从下拉列表中选择帐户。  注: 要选择云帐户，您必须先在 Core Console 中添加云帐户。有关详情，请参阅添加云帐户。
	容器	从下拉菜单中选择与您的帐户关联的存档的容器。
	文件夹名称	输入存档数据的文件夹名称；例如，Rapid-Recovery-Archive-[创建日期]-[创建时间]。

- 单击 **Attach（连接）**。
存档将附加到此 Core 并作为文件系统安装内容。

导入存档

您可以使用此过程一次导入一个存档，或计划定期导入存档。

当您想要恢复存档数据时，您可以将整个存档导入到指定的位置。

 **小心:** 请仔细考虑后执行此步骤。导入某存档会因系统捕获到了该存档而用该存档中的内容重新填充存储库，替换存储库中的任何新数据。

要导入存档，请完成以下过程中的步骤。

- 
- 在 Rapid Recovery Core Console 的菜单栏上，单击 **Archive（存档）** 下拉菜单，然后选择 **Import Archive（导入存档）**。
Import Archive Wizard（导入存档向导） 将会打开。
 - 在向导的 **Import Type（导入类型）** 页面上，选择以下选项之一：
 - One-time import（一次性导入）

- Continuous import (by schedule) (连续导入 (按计划))

3 单击**下一步**。

4 在 **Location (位置)** 页面中，从下拉列表中选择您要导入存档的位置，然后按下表所述输入信息：

表. 47: 导入的存档位置类型选项

选项	文本框	说明
本地	位置	输入输出的位置。它用于定义您希望存档驻留的位置路径；例如：d:\work\archive。
网络	位置	输入输出的位置。它用于定义您希望存档驻留的位置路径；例如：\\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络路径的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。
 注: 要选择云帐户，首先必须在 Core Console 中添加云帐户。有关更多信息，请参阅添加云帐户。		
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	为您希望保存存档数据的文件夹输入一个名称。

5 单击**下一步**。

6 在向导的 **Archive Information (存档信息)** 页面上，如果要导入存档中包含的每个机器，请选择 **Import all machines (导入所有机器)**。

7 根据您的选择，完成以下选项之一：

- 如果在步骤 2 中选择了 **One-time import (一次性导入)**，在步骤 6 中选择了 **Import all machines (导入所有机器)**，并且 Core 上存在的所有机器（作为受保护、复制的或仅恢复点的机器），请转至步骤 12。
- 如果在步骤 2 中选择了 **Continuous import (by schedule) (连续导入 (按计划))**，在步骤 6 中选择了 **Import all machines (导入所有机器)**，并且 Core 上至少不存在的一个机器（作为受保护、复制的或仅恢复点的机器），请单击 **Next (下一步)**，然后转至步骤 9。
- 如果您步骤 6 中没有导入所有机器，请单击 **Next (下一步)**，然后继续执行步骤 8。

8 在 **Machines (机器)** 页面中，选择您想要从存档导入的机器。

- 如果在步骤 2 中选择了 **One-time import (一次性导入)**，并且 Core 上至少不存在的一个机器（作为受保护、复制的或仅恢复点的机器），请使用下拉列表为您要导入的每个机器选择一个存储库，然后转至步骤 12。
- 如果 Core 上已存在所有机器（作为受保护、复制的或仅恢复点的机器），请转至步骤 12。

9 单击**下一步**。

10 在 **Repository (存储库)** 页面上，请完成以下选项之一：

- 如果存储库与 Core 相关联，请从下表中选择其中一个选项。

表. 48: 存储库选项

选项	说明
Use an existing Repository (使用现有存储库)	从下拉列表中选择一个当前与此 Core 相关联的存储库。
Create a Repository (创建存储库)	在 Server (服务器) 文本框中，输入您要在其上保存新存储库的服务器的名称（例如 servername 或 localhost），然后参阅 创建 DVM 存储库 。
• 如果没有与此 Core 相关联的存储库，请输入您要在其上保存新存储库的服务器的名称（例如 servername 或 localhost），然后参阅创建 DVM 存储库。	

11 如果在步骤 2 中选择了 **Continuous import (by schedule) (连续导入 (按计划))**，请在 **Schedule (计划)** 页面上，选择下表中所述的选项。

表. 49: 计划导入选项

选项	说明
Daily（每天）	单击时钟图标并使用上箭头和下箭头选择何时开始存档作业。 如果使用的是 12 小时制，请单击 AM 或 PM 按钮以指定当天的时间。
Weekly（每周）	选择星期几以及您想要开始存档作业的时间。 如果使用的是 12 小时制，请单击 AM 或 PM 按钮以指定当天的时间。
Monthly（每月）	选择当月的日期以及您想要开始存档作业的时间。 如果使用的是 12 小时制，请单击 AM 或 PM 按钮以指定当天的时间。
暂停初始导入	如果在完成向导后不希望在下一个安排的时间开始导入作业，请选择此选项。  注: 您可能希望在继续导入前暂停计划的导入，以便有时间准备目标位置。如果不选择此选项，则会在计划的时间开始导入。

12 单击**完成**。

事件

Rapid Recovery Core 包括预定义的事件集。这些事件可用于向管理员通知有关 Core 的严重问题，或者与备份、虚拟导出和复制等相关的作业问题。

本节介绍如何查看 Rapid Recovery Core Console 上显示的事件。您还可以了解事件通知方法和配置，包括设置电子邮件通知。最后，可以配置通知以更改事件日志的保留时间，并减少重复的事件通知。

Rapid Recovery 事件

Rapid Recovery Core 包括预定义的事件集，可用于向管理员通知 Core 或受保护机器中备份作业中的严重问题。

- 通过配置通知组可定义触发警告的事件类型，以及系统使用的通知方法（电子邮件、弹出式警告等）。要了解更多信息，请参阅[配置通知组](#)。
- 如果您希望管理员使用电子邮件接收通知，则除了配置通知组外，必须配置电子邮件服务器，并配置电子邮件通知模板。要了解更多信息，请分别参阅[配置电子邮件服务器](#)和[配置电子邮件通知模板](#)。
- 您可使用减少重复功能，减少 Events（事件）页面中显示的同一类型和范围事件的数量。默认情况下启用减少重复功能。您可禁用该功能，也可控制在哪个时间跨度内，事件日志中事件合并为单一事件。要了解更多信息，请参阅[关于配置减少重复](#)。
- 您可控制事件和作业历史记录信息在 Core 控制台的 Events（事件）页面中保留的时长。要了解更多信息，请参阅[配置事件保留](#)。

使用任务、警报和日记查看事件

在 Core Console 中，您可以查看 Core 的事件，并可以查看特定受保护或已复制的机器的事件。

Core Console 上的**事件**页面将显示与 Rapid Recovery Core 相关的所有系统事件日志。要访问和查看 Core 的事件，单击 （事件）。

特定受保护或已复制的机器的**事件**页面将显示与该特定计算机相关的事件日志。要访问和查看所选计算机的事件，可在“受保护机器”菜单中单击该计算机名称，然后从计算机**摘要**页面中，单击**事件**菜单。

(Core 或指定机器上的)“事件”页面中的内容分为三个部分：任务、警报和日记。这些视图允许您视情况筛选有关各种事件的详细信息。

您可以配置通知组以定义接收各种事件通知的方式。有关详情，请参阅[配置通知组](#)。

要查看任务、警报或所有事件的日记，请完成以下过程中的步骤：

- [查看任务](#)
- [查看警报](#)
- [查看所有事件](#)

查看任务

任务是 Rapid Recovery Core 必须执行的作业，如传输定期计划备份中的数据或从恢复点执行还原。

当任务正在运行时，它将列示在 Core Console 顶部的**正在运行任务**下拉菜单中。单击一个正在运行的任务可打开“监控活动任务”对话框。

您还可以查看 Rapid Recovery Core 的所有任务或与特定机器关联的所有任务。

- 1 要查看 Rapid Recovery Core 的所有任务，请从图标栏中单击 （事件）。
如果您想要查看特定受保护机器的任务，请导航至指定机器的**摘要**页面，然后单击**事件**菜单。
- 2 要仅查看任务，请在页面的左侧顶部单击**任务**。这是默认视图。
此时将筛选事件列表，以便仅显示 Core 或所选机器的任务。
- 3 （可选）要按关键字、开始日期、结束日期或上述任意组合筛选任务列表，请执行以下操作：
 - a 要按关键字筛选，请在**搜索关键字**文本框中输入关键字。
例如，您可以按关键字进行筛选，如“汇总”、“存档”或“传输”。
 - b 要按开始日期和时间筛选，请使用以下选项之一输入开始日期和时间：
 - 在**起始时间**文本框中，以 MM/DD/YYYY HH:MM AM/PM 格式键入日期和时间。例如，要从 2016 年 1 月 1 日 8:00 AM 起搜索，请输入 1/1/2016 8:00 AM。
 - 要选择当前的日期和时间，请单击  **日历**小部件（位于**开始日期**文本框中），然后单击当前日期。将自动显示当前时间。
 - 请单击  **日历**小部件，选择日期，然后单击  **时钟**小部件，并使用控件选择所需的时间。单击日历之外的区域以接受所选的更改。
 - c 要进一步精简显示的任务列表，您还可以以相同的格式定义结束日期和时间。
此时将根据所选的标准立即筛选任务列表。
- 4 （可选）您可以如下筛选列表中显示的任务：

选项	说明
	要仅查看活动任务，请单击 活动任务 图标。
	要仅查看等待执行队列中的任务，请单击 已排入队列的任务 图标。
	要仅查看等待执行的任务，请单击 正在等待的任务 图标。
	要仅查看已完成的任务，请单击 已完成的任务 图标。
	要仅查看失败的任务，请单击 失败的任务 图标。

- 5 要导出任务列表，请从列表中选择一种格式，然后单击  **导出**。在出现的对话框中，确认导出，然后单击**确定**。

您可以使用以下格式导出：

表. 50: 导出格式

格式	说明
PDF	便携式文档格式（默认导出格式）
HTML	网页格式
CSV	逗号分隔的值
XLS	Microsoft Excel® 1997 - 2003 工作簿
XLSX	Excel 工作簿

所选类型的文件会下载到 Core 服务器上的默认位置。

- 6 请单击任何任务的  **作业详细信息** 图标以启动包含任务详细信息的新窗口，其中包括：
- 状态
 - 工作总计（已完成的大小或百分比）
 - 开始日期和时间
 - 结束日期和时间
 - 比率
 - 经过时间
 - 阶段（对于子任务）

查看警报

警报是与任务或事件相关的通知。警报类型包括错误、警告或信息。

您可以查看 Rapid Recovery Core 的重要警报或与特定机器关联的重要警报的日记。

- 1 要查看 Rapid Recovery Core 的警报，请从图标栏中单击 （事件），然后单击**警报**。
- 如果您想要查看特定受保护机器的警报，请导航至指定机器的**摘要**页面，单击**事件**菜单，然后单击**警报**。
- 此时将筛选事件列表以便仅显示 Core 或所选机器的重要警报。
- 2 （可选）要按开始日期、结束日期、警报消息说明或任意组合筛选重要警报列表，请执行以下操作：
- a 要按开始日期和时间筛选，请使用以下选项之一输入开始日期和时间：
- 在**起始时间**文本框中，以 MM/DD/YYYY HH:MM AM/PM 格式键入日期和时间。例如，要从 2016 年 1 月 1 日 8:00 AM 起搜索，请输入 1/1/2016 8:00 AM。
 - 要选择当前的数据和时间，请单击  **日历**小部件（位于**开始日期**文本框中），然后单击当前日期。将自动显示当前时间。
 - 请单击  **日历**小部件，选择日期，然后单击  “时钟”小部件，并使用控件选择所需的时间。单击日历之外的区域以接受所选的更改。
- b 要按警报消息说明进行筛选，请在**搜索消息**文本框中输入说明。
- 例如，要仅查看与代理程序相关的警报，则输入“agent”；要查看与传输相关的警报，则输入“transfer”；以此类推。
- c 要进一步精简显示的警报列表，您还可以以相同的格式定义结束日期和时间。
- 将根据所选的条件立即筛选警报列表。
- 3 （可选）如果要移除所有警报，请单击**全部消除**。

查看所有事件

您可以查看 Rapid Recovery Core 的所有事件或与特定机器关联的所有事件。

- 要查看 Rapid Recovery Core 的所有事件的日记，请从图标栏单击 （事件），然后单击**日记**。要查看 Rapid Recovery Core 的所有事件，请导航至 Rapid Recovery Core 主页，然后单击 （事件）。如果您想要查看特定受保护机器的所有事件的日记，请导航至指定机器的**摘要**页面，单击**事件**菜单，然后单击**日记**。
- （可选）要按开始日期、结束日期、警报消息说明或任意组合筛选所有事件的列表，请执行以下操作：
 - 要按开始日期和时间筛选，请使用以下选项之一输入开始日期和时间：
 - 在**起始时间**文本框中，以 MM/DD/YYYY HH:MM AM/PM 格式键入日期和时间。例如，要从 2016 年 1 月 1 日 8:00 AM 起搜索，请输入 1/1/2016 8:00 AM。
 - 要选择当前的数据和时间，请单击  **日历**小部件（位于**开始日期**文本框中），然后单击当前日期。将自动显示当前时间。
 - 请单击  **日历**小部件，选择日期，然后单击  “时钟”小部件，并使用控件选择所需的时间。单击日历之外的区域以接受所选的更改。
 - 要按警报消息说明进行筛选，请在**搜索消息**文本框中输入说明。
例如，要仅查看与代理程序相关的警报，则输入“agent”；要查看与传输相关的警报，则输入“transfer”；以此类推。
 - 要进一步精简显示的事件列表，您还可以以相同的格式定义结束日期和时间。
将根据所选的条件立即筛选事件列表。

了解电子邮件通知

您可设置 Rapid Recovery Core 为通过发送电子邮件至指定的电子邮件地址以通知特定事件。触发警告的事件可在通知组中定义，方法与其他通知方法相同。

① 注: 无论是否使用电子邮件作为通知方法，都必须建立通知组。要了解更多信息，请参阅 [配置通知组](#)。

如果您选择电子邮件作为其中一种通知选项，则还必须配置电子邮件 SMTP 服务器。Rapid Recovery Core 使用定义的服务器，根据通知组中的参数发送警告。

此外，您还必须定义电子邮件通知模板。Core 使用该模板定义每个警告的电子邮件主题行，以及电子邮件正文中的内容。模板具有默认设置；您可使用默认设置，也可根据需要，测试并进行修改。

本节包括以下主题：

- [配置电子邮件服务器](#)
- [配置电子邮件通知模板](#)

配置电子邮件服务器

要配置电子邮件服务器，请完成以下过程中的步骤。

① 注: 在系统发送电子邮件警报消息之前，您还必须配置通知组设置，包括启用通过电子邮件通知选项。有关指定事件以接收电子邮件警报的更多信息，请参阅[配置通知组](#)。

- 导航至 Rapid Recovery Core Console。
- 在图标栏中，单击 （设置），然后执行以下其中一个操作：

- 从“设置”页面左侧的 Core 设置列表中，单击 **SMTP 服务器**。
- 在“设置”页面右侧向下滚动，直至您看到 **SMTP 服务器** 标题。

将显示“SMTP 服务器”核心设置。

- 3 单击您要更改的设置。
您所选的设置将变为可编辑状态。
- 4 根据下表中的说明输入配置信息。

选项	说明
SMTP 服务器	输入电子邮件通知模板将使用的电子邮件服务器的名称。命名约定包括主机名、域和后缀；例如 smtp.gmail.com。
发件人	输入返回电子邮件地址。用于指定电子邮件通知模板的返回电子邮件地址；例如 noreply@localhost.com。
用户名	输入电子邮件服务器的用户名。
密码	输入与用户名关联且访问电子邮件服务器所需的密码。
端口	输入端口号。用于标识电子邮件服务器的端口；例如 Gmail 端口 587。 默认值为 25。
超时（秒）	输入一个整数值以指定尝试连接到电子邮件服务器的时长。此值用于确定发生超时之前的时间（秒）。 默认值为 60 秒。
TLS (TLS)	如果邮件服务器使用 Transport Layer Security (TLS) 或安全套接字层 (SSL) 等安全连接，则选择此选项。

- 5 对于每个设置，当您对所做的更改感到满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存更改。

 **小心：**如果您不确认每个更改，将不会更改您的设置。

- 6 单击 **发送测试电子邮件**，然后执行以下操作：
 - a 在 **发送测试电子邮件** 对话框中，输入测试消息的目标电子邮件地址，然后单击 **发送**。
 - b 如果测试消息失败，则退出错误对话框和 **发送测试电子邮件** 对话框，并修改电子邮件服务器配置设置。然后再次发送测试消息。
 - c 测试消息成功后，单击 **确定** 以确认成功操作。
 - d 检查接收测试电子邮件消息的电子邮件帐户。

配置电子邮件通知模板

当您启用通过电子邮件发送 Rapid Recovery 事件的通知时，默认将为您创建默认模板。为 Core 定义的 SMTP 电子邮件服务器会使用该模板来通过电子邮件发送有关 Rapid Recovery 事件的通知。

本主题介绍了配置默认电子邮件通知模板或自定义内容的过程。使用 Restore Defaults（恢复默认值）选项，您可以随时还原对默认通知模板所做的更改。

 **小心：**修改模板的风险由您自行承担。您负责测试对模板的任何修改。仅支持默认模板。

完成此过程中的步骤以配置电子邮件通知模板。

 **注：**您还必须先配置电子邮件服务器和通知组设置，包括启用 **Notify by email**（通过电子邮件发送通知）选项，然后才能发送电子邮件警报消息。有关配置用于发送警报的电子邮件服务器的更多信息，请参阅 [配置电子邮件服务器](#)。有关指定接收电子邮件警报的事件的更多信息，请参阅 [配置通知组](#)。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏中，单击 （更多），然后选择  **Notifications（通知）**。此时会显示 **Notifications（通知）** 页面。
- 3 在 Email Settings（电子邮件设置）窗格中，单击  **Change（更改）**。

此时将显示 **Edit Email Notification Configuration**（编辑电子邮件通知配置）对话框。

4 选择**启用电子邮件通知**。

该电子邮件模板已启用并可见。默认电子邮件模板的值如以下步骤中所述。

5 检查 Edit Email Notification Configuration（编辑电子邮件通知配置）对话框中的内容，并确定默认内容适合您的需求。

选项	说明
启用电子邮件通知	此设置可启用或禁用电子邮件通知模板。 - 要启用电子邮件通知，请选择此选项。 - 要禁用电子邮件通知，请取消选中此选项。
Email Subject（电子邮件主题）	此文本字段的内容控制着作为系统事件通知发送的电子邮件的主题行。默认电子邮件主题行如下所示： <code><hostName> <level>: <name> for <agentName></code>
电子邮件	此文本区域的内容控制着作为系统事件通知发送的电子邮件正文。默认电子邮件正文如下所示： <code><shortCompanyName> <coreProductName> on <hostName> has reported the <level> event "<name>"</code> <code>Date/Time: <localTimestamp></code> <code><message></code> <code><if(details.errorDetails)></code> <code><details.ErrorDetails.Message></code> <code><details.ErrorDetails.Details></code> <code><endif></code> <code>---</code> <code>About this event: <description></code> <code><coreAdminUrl></code>
Send Test Email（发送测试电子邮件）	单击此按钮可将测试电子邮件发送到您在最终的 Send Test Email（发送测试电子邮件） 对话框中指定的电子邮件地址。
Restore Defaults	单击此按钮从电子邮件模板中删除任何自定义的更改，并将 Email Subject（电子邮件主题）和 Email（电子邮件）字段还原为此表中所述的默认内容。
正常	单击此按钮可确认并保存 Edit Email Notification Configuration（编辑电子邮件通知配置）对话框中的设置。
取消	单击此按钮会取消 Edit Email Notification Configuration（编辑电子邮件通知配置）对话框中的任何更改。

6 如果您想自定义电子邮件模板，请对上一步骤所述文本或变量做出更改。默认使用的变量如下表所述。

选项	说明
hostName	Core 的主机名
details	特定事件的 details 对象。
agentName	与此事件关联的受保护机器的名称，如果事件有单个受保护机器的范围。
repositoryName	与此事件关联的存储库的名称，如果事件具有存储库的范围。
jobSummary	与此事件关联的作业的摘要，如果事件具有作业的范围。
remoteSlaveCoreName	与此事件关联的远程目标 Core 的名称，如果事件具有目标 Core 范围。
remoteMasterCoreName	与此事件关联的远程源 Core 的名称，如果事件具有源 Core 范围。
productName	产品的名称 Rapid Recovery Core。使用白标签，可此更改品牌的产品名称。
companyName	销售该产品的公司的名称。

7 在 **Email Subject（电子邮件主题）** 文本框中，输入电子邮件模板的主题。

Email Subject（电子邮件主题）用于定义电子邮件通知模板的主题，例如：<主机名> - <级别> <名称>。

8 在 **Email（电子邮件）** 文本框中，输入描述事件的模板正文信息、事件发生的时间以及严重性。

9 单击 **Send Test Email（发送测试电子邮件）**，然后执行以下操作：

- 在 Send Test Email（发送测试电子邮件）对话框中，输入测试邮件的目标电子邮件地址，然后单击 **Send（发送）**。

- b 如果测试邮件失败，请退出错误对话框和 Send Test Email（发送测试电子邮件）对话框中，然后单击 **OK（确定）** 以保存当前电子邮件模板的设置。然后，修改您的电子邮件服务器设置，如过程[配置电子邮件服务器](#)中所述。请确保您重新输入该电子邮件帐户的密码。保存这些设置，然后返回此过程。
- c 测试邮件成功后，单击 **OK（确定）** 确认成功操作。
- d 检查您将测试电子邮件发送到的电子邮件帐户。

测试结果满意后，请返回 Edit Email Notification Configuration（编辑电子邮件通知配置）对话框，然后单击 **OK（确定）** 以关闭对话框并保存您的设置。

系统事件的通知组、SMTP 设置和通知模板

通知组可定义向用户发送警告的一组特定事件，以及发送通知的方式。要配置或编辑通知组，请参阅 [配置通知组](#)。

如果要作为电子邮件发送警告，您还必须配置 Simple Mail Transfer Protocol (SMTP) 服务器设置。要了解设置电子邮件服务器配置设置的更多信息，请参阅 [配置电子邮件服务器](#)。

发送事件通知时，系统使用电子邮件通知。您可自定义该模板。要了解配置或自定义电子邮件通知模板的更多信息，请参阅 [配置电子邮件通知模板](#)。

配置通知组

① 注: 如果要以电子邮件的方式发送警报，则还必须配置简单邮件传输协议 (SMTP) 服务器设置，如以下过程所述。有关设置电子邮件服务器配置设置的更多信息，请参阅[配置电子邮件服务器](#)。

通知组允许您定义一组特定事件以提醒用户，以及该通知的发生方式。您可以配置通过以下方法发送警报：

- 通过电子邮件
- 在 Windows 事件日志中
- 使用 syslogd
- 使用弹出式警报
- 使用警报
- 使用 SNMP 陷阱

您可以配置具有不同通知参数的多个通知组。

可以在 Core 级别设置通知组，或为每个特定受保护机器设置通知组。

要配置警报的通知组，请完成以下过程中的步骤。

1 请执行以下步骤之一：

- 要在 Core 级别设置通知，请从图标栏中，单击 （更多），然后选择**通知**。将显示**通知**页面。
- 要为特定的受保护机器设置通知，请执行以下操作：
 - 1 在“受保护机器”菜单中，单击您想要为其指定通知的机器。此时将显示**自定义通知组**页面。
 - 2 在受保护机器的“摘要”页面中，从“更多”下拉菜单中选择**通知**。此时将显示**自定义通知组**页面。

2 单击  **添加组**

此时将显示**添加通知组**对话框。

通知组允许您定义一组特定事件以提醒用户，以及该通知的发生方式。您可以配置通过以下方法发送警报：

添加通知组对话框包含一个常规说明区域和两个选项卡：

- 启用警报
- 通知选项

3 在一般说明区域中，根据下表中的说明输入通知组的基本信息。

选项	说明
名称	输入事件通知组的名称。此信息为必填项。

 **小心：**您无法在未来更改为通知组名称输入的值。

说明	输入澄清事件通知组用途的说明。此信息是可选信息。

4 在**启用警报**选项卡上，按如下所示定义要记录、创建报告以及要接收警报的系统事件集：

选项	说明
所有警报	要为所有事件创建警报，请选择 All Alerts（所有警报） 。

错误	要为错误创建警报，请从 选择类型 菜单中单击 错误 。这由一个红色 X 表示。 

警告	要为警告创建警报，请从 选择类型 菜单中单击 警告 。这由一个黄色感叹号图标表示。 

信息	要为通知消息创建警报，请从 选择类型 菜单中单击 信息 。这由一个蓝色 i 表示。 

恢复默认值	要将警报类型还原为默认设置，请从 选择类型 菜单中，单击 还原默认值 。这由一个深蓝色向左箭头表示。 

5 要为特定事件类型（错误、警告或通知消息）创建警报，请执行以下操作：

- 如果**所有警报**选项没有显示警报组，请单击“所有警报”标签前的右尖括号 > 符号。符号会更改为向下的箭头，视图将展开以显示组。
- 然后单击任何特定警报组旁边的右尖括号 > 符号以显示组中的相关事件。
事件组类别包括：

- 存档
- 自动报告
- 可附加性
- 自动更新
- 备份存储库
- 启动 CD
- 云
- 群集
- Core 服务
- 数据库保留
- 清除重复高速缓存
- DVM 存储库
- Exchange
- 导出
- 作业
- 许可
- 本地安装
- 日志截断
- 元数据
- 每夜作业
- 通知

- 持久保存 Core 状态
- PowerShell Scripting
- 保护
- 推送安装
- 恢复点检查
- 远程安装
- 常用存储库
- 复制
- 还原
- 汇总
- 计划存档
- 安全
- 服务器日志
- vSphere
- 要为每个组中的所有事件定义警报，请选中**所有警报**的复选框。
- 要定义任意警报组中所有事件的警报，请选中该组旁的复选框。
- 要仅选择警报组内的某些警报类型，请展开该组，然后仅选择您想要记录，报告并设置警报的特定事件。

6 单击**通知选项**选项卡。

7 在**通知选项**选项卡中，指定如何处理通知过程。

选项	说明
通过电子邮件通知	指定电子邮件通知的收件人。您可以选择指定单独的多个电子邮件地址以及抄送和密送地址。 您可以选择： • 收件人： • 抄送： • 密件抄送：
通过 Windows 事件日志通知	如果要通过 Windows 事件日志报告警报，请选择此选项。
通过 syslogd 通知	如果要通过系统日志报告警报，请选择此选项。在以下文本框中指定系统日志的详细信息： • 主机： • 端口：
通过 Toast 警报通知	如果希望警报以弹窗形式显示在屏幕右下角中，则选择此选项。
通过警报通知	如果您想要警报显示为位于 Core Console 右下角的弹出式窗口，请选择此选项。
通过 SNMP 陷阱通知	Rapid Recovery Core 服务器作为 SNMP 代理程序，发送陷阱（有关特定事件的通知）给 SNMP 管理器。结果就是报告 Core 信息，如警报、存储库状态和受保护机器。如果希望通过 SNMP 陷阱通知 Core 事件，选择本选项。您还必须指定陷阱编号。例如，Rapid Recovery Core 使用的默认陷阱编号是 162。

8 单击**确定**。

此时将显示一条消息，指示创建组后无法更改定义的通知组名称。您可以随时更改通知组中的其他属性。

- 如果对组名称满意，请确认此消息并保存您的工作。
- 如果要更改组名称，请单击**否**以返回“创建通知组”窗口，更新组名称及任何其他通知组设置，然后保存您的工作。

通知组将显示在摘要表中。您可以使用任何参数集创建不同的通知组。

关于配置减少重复

管理员接收某些事件警报的能力至关重要。但是，在某些情况下，接收已经知道事件的重复通知也会非常令人沮丧或不方便。即使您希望立即了解的环境故障导致生成了一个警报，但相同的错误情况也可能在事件日志中生成数百或数千个事件。为了减少事件日志

中的重复，以及减少在 Core Console 中接收同一事件的重复电子邮件通知所带来的不便，Rapid Recovery 包含了一个减少重复设置，该设置默认已启用并设置为 5 分钟。本设置可以设定为最低 1 分钟以及最高 60 分钟。还可完全禁用。

当减少重复被禁用时，每次发生的同一类型和范围事件都将记录到数据库。无论该事件之前发生的过去时间，每次新发生都会显示在“事件”选项卡的“警报”部分。

当配置减少重复（例如，使用 5 分钟的默认时间）时，则首次出现的特定事件将记录到事件数据库中，同时显示在警报日志中。如果同一类型和范围的事件在设定事件阈值内再次记录，则对于阈值内的每次重复出现的事件，数据库事件计数都会增加 1。日志显示在“事件”页面的“警报”部分中。但是，它仅显示一次事件，该事件对应最新发生的日期和时间。相同的事件不会更新事件日志，除非从该事件第一次发生时算起时间阈值已到期。例如，如果设置为 5 分钟，然后事件在 6 分钟后再次发生，它将显示在日志中，并且您会收到另一则电子邮件消息。

配置减少重复

要配置事件的减少重复，请完成以下过程中的步骤。

- 1 导航到 Rapid Recovery Core Console。从图标栏上，单击 （更多），然后选择**通知**。此时会显示**通知**页面。
 - 2 在“减少重复”窗格中，查看现有设置。
 - 3 要启用、禁用或更改存储事件的阈值时间，单击  **更改**。此时将显示**编辑减少重复**对话框
 - 4 请执行以下步骤之一：
 - 要禁用减少重复，清除**启用减少重复**选项。
 - 要启用减少重复，选择**启用减少重复**选项。
 - 要更改重复相同事件被忽略的时间阈值（以分钟为单位），在 **___ 分钟**文本框中输入介于 1 和 60 之间的数字。
-  **注：**要更改此值，必须选中**启用减少重复**选项。
- 5 单击**确定**以保存设置，然后关闭对话框。

配置事件保留

将在一段指定时间内保存 Core 上跟踪的事件和作业。默认设置为 30 天。此数字可以设置为 0 天到 3652 天（约 10 年）。

要配置事件保留，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在图标栏中，单击 （设置），然后执行以下其中一个操作：
 - 从“设置”页面左侧的 Core 设置列表中，单击**数据库连接**。
 - 在“设置”页面右侧向下滚动，直至您看到**数据库连接**标题。将显示“数据库连接”设置。
- 3 要更改将事件信息保存到数据库的天数，请单击**保留期（天）**文本字段，输入一个介于 0 到 3652 之间的值，然后单击  以保存更改。
将根据指定的值调整事件保留期。

快速设备自行恢复

快速设备自行恢复 (RASR) 是一种裸机流程，可快速将设备恢复至运行状态。

RASR 提供两种恢复选项：

- 恢复出厂设置
- 将设备恢复至故障前的状态（恢复操作系统、配置和设置）

创建 RASR USB 闪存盘

要创建 RASR USB 闪存盘，请执行以下操作：

- 1 导航至 **Appliance**（设备）选项卡。
- 2 在左侧导航窗格中选择 **Appliance**（设备）> **Backup**（备份）。
此时将显示 **Create RASR USB Drive**（创建 RASR USB 驱动器）窗口。
① 注：在尝试创建 RASR 闪存盘之前，先插入 16 GB 或更大的 USB 闪存盘。
- 3 插入 16 GB 或更大的 USB 闪存盘后，单击 **Create RASR USB Drive now**（立即创建 RASR USB 驱动器）。
此时将显示 **Prerequisite Check**（前提条件检查）消息。
检查前提条件后，**Create the RASR USB Drive**（创建 RASR USB 驱动器）窗口将显示创建 USB 驱动器所需的最小大小以及 **List of Possible target paths**（可用目标路径列表）。
- 4 选择目标并单击 **Create**（创建）。
此时将显示警告对话框。
- 5 单击 **Yes**（是）。
将创建 RASR USB 驱动器闪存盘。
- 6 **① 注：**请确保使用 **Windows** 弹出驱动器功能来准备移除 USB 闪存盘。否则，USB 闪存盘中的内容可能损坏并且 USB 闪存盘将无法按预期正常工作。
移除为每个 DL 设备创建的 RASR USB 闪存盘、标签，并保存好以供将来使用。

执行 RASR

- ① 注：**Dell 建议您在设置设备之后创建 RASR USB 闪存盘。要创建 RASR USB 闪存盘，请参阅[创建 RASR USB 闪存盘](#)部分。
- ① 注：**请确保您有最新的 RUU，并可用在您的设备上。
- 。
- ① 注：**要使用 RASR 执行系统恢复，请参阅 Dell.com/support/home 中的 *使用 Rapid Appliance Self Recovery (RASR) 恢复 Dell™ DL 备份和恢复设备* 文档。

要执行出厂设置：

- 1 插入已创建的 RASR USB 闪存盘。
- 2 重新启动设备，并选择 **Boot Manager (F11)**（引导管理器 (F11)）。
- 3 在 **Boot Manager Main Menu**（引导管理器主菜单）中，选择 **One-shot BIOS Boot Menu**（一次性 BIOS 引导菜单）。
- 4 在 **Boot Manager Boot Menu**（引导管理器主菜单）中，选择附加的 USB 驱动器。
- 5 选择键盘布局。
- 6 然后单击 **Troubleshoot**（故障排除）> **Rapid Appliance Self Recovery**（快速设备自行恢复）。
- 7 选择目标操作系统 (OS)。
随即会启动 RASR 并显示欢迎屏幕。
- 8 单击**下一步**。
此时将显示 **Prerequisites check**（前提条件检查）屏幕。
① 注：在执行 RASR 之前，请务必检查所有硬件及其他前提条件。

9 单击**下一步**。

此时将显示 **Recovery Mode Selection**（恢复模式选择）屏幕，其中包含三个选项：

- **System Recovery**（系统恢复）
- **Windows Recovery Wizard**（Windows 恢复向导）
- **Factory Reset**（恢复出厂设置）

10 选择 **Factory Reset**（出厂重置）选项。

此选项将从出厂映像恢复操作系统磁盘。

11 单击**下一步**。

对话框中会显示以下警告消息：This operation will recover the operating system. All OS disk data will be overwritten。

12 单击 **Yes**（是）。

操作系统磁盘开始恢复为出厂设置。

13 恢复过程完成后会显示 **RASR Completed**（RASR 已完成）页面。请单击 **Finish**（完成）。

14 还原后引导系统。

15 **注**：仅当看到 **AppAssure Appliance Configuration Wizard**（AppAssure 设备配置向导）时继续执行，否则执行步骤 17。

等待加载 AppAssure Appliance Configuration Wizard（AppAssure 设备配置向导），您需要将其关闭。使用 Windows 任务管理器关闭该向导。

16 运行 RUU 软件包中的 **launchRUU.exe** 文件。按说明执行，并选择选项以继续执行 RUU 安装并完成 RUU 安装。

17 **DL Appliance Configuration Wizard**（DL 设备配置向导）启动，并指导您完成余下的恢复流程。

您的设备现在可正常运行。

Local Mount Utility

本节介绍如何下载、安装和使用基于 Windows 的 Rapid Recovery Local Mount Utility (LMU) 以装载恢复点，以及使用一台没有托管 Rapid Recovery Core 的机器从文件级别浏览内容。

关于 Local Mount Utility

LMU 是一个可下载的基于 Windows 的应用程序，允许您在任何 Windows 机器上以任何三种可用的模式安装 Rapid Recovery 恢复点。这种轻量级的实用程序可以安装在 32 位及 64 位 Windows 操作系统上，且包括 rapidrecovery-vdisk（以前称为 aavdisk）和 aavstor 驱动程序，但它不能作为一个服务运行。默认情况下，此实用程序安装在 C:\Program Files\AppRecovery\Local Mount Utility 目录中，并且在机器的桌面上显示为快捷方式。

虽然此实用程序旨在用于远程访问 Rapid Recovery Core 机器，但也可将 LMU 安装在与 Rapid Recovery Core 相同的机器上。在 Core 上运行时，此应用程序将识别和显示该 Core 上的所有安装，包括通过 Rapid Recovery Core Console 执行的安装。同样，在 LMU 上执行的安装也会显示在 Core Console 中。

当 LMU 与“邮箱还原”安装在同一机器上时，如果使用“邮箱还原”打开 Exchange 数据库，LMU 将自动启动它。“邮箱还原”是用于还原 Microsoft Exchange 数据存储和项目的 Dell Rapid Recovery 应用程序。在安装 LMU 或 Rapid Recovery Core 时可以安装它。有关“邮箱还原”的更多信息，请参阅《Dell Data Protection | Rapid Recovery Mailbox Restore for Microsoft Exchange 用户指南》。

注：Linux 机器使用一个命令行实用程序 **local_mount** 查询 Core 上的受保护机器及其相应的恢复点。同样，该工具可让用户远程安装恢复点卷；可让用户在文件级别浏览卷内容；允许用户从恢复点还原单个文件或整个卷，包括系统卷的 BMR。有关更多信息，请分别参阅在 [Linux 机器上安装恢复点卷](#)、[使用命令行还原 Linux 机器的卷](#)和对 [Linux 机器执行 Bare Metal Restore](#)。

在 Local Mount Utility 中处理 Rapid Recovery Core 机器

Local Mount Utility (LMU) 使您能够本地或远程处理无限数量的 Core 机器。如果您在一个 Rapid Recovery Core 机器上安装 LMU，该机器将作为 localhost 自动出现在 LMU 中。所有其它远程 Core 都将显示为各自的机器名称或 IP 地址，具体取您在添加时输入的信息。使用 LMU，您可以添加、编辑和删除 Core 机器。有关更多信息，请参阅以下过程：

相关链接

- [将 Core 机器添加到 Local Mount Utility](#)
- [更改 Local Mount Utility 选项](#)
- [在 Local Mount Utility 中编辑 Core 连接设置](#)
- [重新连接至 Core](#)
- [从 Local Mount Utility 中移除 Rapid Recovery Core 机器](#)

将 Core 机器添加到 Local Mount Utility

要安装恢复点，必须将 Core 机器添加至 LMU。可以添加无限数量的 Core。要通过添加 Core 设置 LMU，请完成以下过程。

- 在已安装 LMU 的机器上，双击桌面图标启动 LMU。
- 请执行以下步骤之一：
 - 从左上角的 Local Mount Utility 菜单中，单击**添加 Core**。
 - 右键单击左侧面板中的空白空间，然后单击**添加 Core**。

此时将显示**添加 Core**对话框。

- 在**添加 Core**对话框中，根据下表中的说明输入所需的凭据。

表. 51: Rapid Recovery Core 凭据

选项	说明
主机名	要从中安装恢复点的 Core 的名称或 IP 地址。  注: 如果在 Rapid Recovery Core 机器上安装 LMU，LMU 将自动添加 localhost 机器。
端口	用于与 Core 通信的端口号。 默认端口号为 8006。
使用我的 Windows 用户凭据	如果用于访问 Core 的凭据与 Windows 凭据相同，请选择此选项。
使用特定凭据	如果用于访问 Core 的凭据与 Windows 凭据不同，请选择此选项。
用户名	用于访问 Core 机器的用户名。  注: 仅当选择使用特定凭据时，此选项才可用。
密码	用于访问 Core 机器的密码。  注: 仅当选择使用特定凭据时，此选项才可用。

- 单击**连接**。
- 如果要添加多个 Core，请根据需要重复所有步骤。

更改 Local Mount Utility 选项

要更改连接至 LMU 的所有 Rapid Recovery Core 的选项，请完成以下过程。

- 1 从 Local Mount Utility 用户界面中，单击**选项**。
- 2 在**选项**对话框中，您可以更改下表中所述的设置。

表. 52: Core 设置

选项	说明
默认安装点存储库	使用 浏览 按钮或输入您想要用于安装恢复点的位置的路径。
使用我的 Windows 用户帐户凭据	如果选择此选项，则在默认情况下，登录 Core 时始终使用您的 Windows 凭据。
使用特定凭据	选择此选项可将以下凭据用于每个连接的 Core： • 用户名：输入要用于所有 Core 的用户名。 • 密码：输入要用于所有 Core 的密码。
Core 连接超时（秒）	输入 LMU 应不断尝试连接到 Core 的时间量，经过此时间之后，连接超时（单位可以是分钟:秒:毫秒）。
语言	选择要用于显示 LMU 的语言。可以从以下选项中选择： • 英语 • 法语 • 德语 • 葡萄牙语 • 西班牙语 • 简体中文 • 日语 • 韩语

在 Local Mount Utility 中编辑 Core 连接设置

要编辑您在将 Core 添加到 LMU 时建立的设置，请完成以下过程。

① 注：此过程不适用于 **localhost Core**。它只适用于**远程 Core 机器**。

- 1 从 Local Mount Utility 用户界面上，右键单击要编辑其设置的 Core，然后单击**编辑 Core**。
- 2 在**编辑 Core**对话框中，您可以更改下表中所述的设置。

表. 53: Core 设置

选项	说明
主机名	要从中安装恢复点的 Core 的名称。
① 注： 如果在 Rapid Recovery Core 机器上安装 LMU，LMU 将自动添加 localhost 机器。	
端口	用于与 Core 通信的端口号。 默认端口号为 8006。

选项	说明
使用我的 Windows 用户凭据	如果用于访问 Core 的凭据与 Windows 凭据相同，请选择此选项。
使用特定凭据	如果用于访问 Core 的凭据与 Windows 凭据不同，请选择此选项。
用户名	用于访问 Core 机器的用户名。
 注: 仅当选择使用特定凭据时，此选项才可用。	
密码	用于访问 Core 机器的密码。
 注: 仅当选择使用特定凭据时，此选项才可用。	

3 进行更改后，单击**确定**。

重新连接至 Core

如果与 Rapid Recovery Core 机器的连接中断，您可以使用以下步骤刷新连接。

从 Local Mount Utility 用户界面中，执行以下操作之一：

- 如果 Core 为离线状态，双击您想要重新建立连接的 Core。
LMU 会尝试重新建立与 Core 的连接。
- 如果 Core 为在线状态，可右键单击 Core，然后单击“重新连接到 Core”。
LMU 将刷新连接。

从 Local Mount Utility 中移除 Rapid Recovery Core 机器

要从 LMU 中移除 Core，请完成以下过程。

 **注:** 此选项不可用于位于本地主机上并标记为 **localhost** 的 **Rapid Recovery Core**。

- 1 从 Local Mount Utility 用户界面中，右键单击您想要移除的 Core，然后单击**移除 Core**。
- 2 要确认命令，请在对话框中单击**是**。
LMU 会从导航树中移除 Core 及其受保护的机器。

在 Local Mount Utility 中使用受保护机器

使用 Local Mount Utility (LMU)，您可以安装受保护机器并浏览这些机器中的恢复点，而不必再次登录与该机器关联的 Rapid Recovery Core Console。有关更多信息，请参阅以下过程：

- [使用 Local Mount Utility 安装恢复点](#)
- [使用 Local Mount Utility 浏览已安装的恢复点](#)
- [刷新恢复点](#)
- [使用 Local Mount Utility 卸载个别恢复点](#)
- [从单个 Rapid Recovery Core 或受保护机器上卸载所有恢复点](#)
- [使用 Local Mount Utility 卸载所有已安装的恢复点](#)

使用 Local Mount Utility 安装恢复点

使用 LMU，您可以安装与所连接的 Core 机器相关联的任何恢复点，包括受保护机器、复制的机器和仅有恢复点的机器。

安装恢复点之前，Local Mount Utility (LMU) 必须连接至存储恢复点的 Core。如过程[将 Core 机器添加到 Local Mount Utility](#) 中所述，可将无限数量的 Core 添加至 LMU；但是，此应用程序一次只能连接一个 Core。例如，如果先安装由某个 Core 保护的机器的恢复点，然后安装由不同 Core 保护的另一台机器的恢复点，那么 LMU 将自动与第一个 Core 断开连接，以便与第二个 Core 建立连接。

- 1 在 Local Mount Utility 用户界面中，展开导航树中的 Core，以显示受保护机器。
- 2 在导航树中，选择要从中安装恢复点的机器。
恢复点显示在主框架中。
- 3 展开要安装的恢复点，以显示各磁盘卷或数据库。
- 4 右键单击要安装的恢复点，然后选择以下选项之一：

选项	说明
安装	此选项允许您将恢复点安装为只读。
安装可写	此选项允许您对已安装的恢复点进行更改。
安装只读带此前写入	此选项会将恢复点安装为只读，并包括以前所做的任何更改。
高级安装...	此选项会打开“高级安装”对话框。

- 5 如果您选择了**高级安装**，请完成以下表中所述的选项。

表. 54: 高级安装选项

选项	说明
安装点路径	单击 浏览 以选择默认安装点路径以外的恢复点路径，或者手动输入首选路径。
安装类型	选择以下选项之一： • 安装只读 • 安装可写 • 安装只读带此前写入 有关每个选项的说明，请参阅 步骤 4 。

- 单击**安装**。
LMU 会自动打开包含已安装恢复点的文件夹。

❗ | 注: 如果选择已安装的恢复点，则“安装”对话框将提示是否卸载该恢复点。

使用 Local Mount Utility 浏览已安装的恢复点

浏览恢复点会在 Windows 资源管理器窗口中打开备份的数据，并允许您搜索卷和文件夹以选择要恢复的一个或多个项目。

然后，您可以通过使用 Windows 资源管理等文件管理器（或者通过编程使用 Windows API）将项目复制到您的首选位置来恢复这些项目。要浏览当前安装的恢复点，请完成以下过程。

❗ | 注: 如果在安装恢复点后立即进行浏览，则无需执行此过程，原因是安装程序完成后将自动打开包含此恢复点的文件夹。

- 1 从 Local Mount Utility 用户界面中，单击**活动安装**。
此时将打开“活动安装”窗口，显示所有已安装的恢复点。
- 2 展开导航树中以显示为每台机器安装的恢复点及其卷。
- 3 单击要浏览的卷旁边的**浏览**。

刷新恢复点

LMU 不从 Core 和受保护机器接收实时更新。要刷新受保护机器并查看其最新的恢复点，请完成以下步骤。

从 Local Mount Utility 用户界面中，右键单击您想要刷新的受保护机器，然后单击“刷新恢复点”。

使用 Local Mount Utility 卸载个别恢复点

要使用 LMU 卸载远程 Core 上的恢复点，请完成以下过程。

- 1 从 Local Mount Utility 用户界面中，单击**活动安装**。
此时将打开**活动安装**窗口，其中会显示所有已安装的恢复点。
- 2 （可选）在**活动安装**窗口中，您可以单击加号或减号图标以展开或折叠每个已安装的恢复点中的卷视图。
- 3 在**活动安装**窗口中，在要卸载每个恢复点或卷旁边，单击**卸载**。
卸载所选恢复点之后，将会显示一个进度窗口。
- 4 单击**活动安装**窗口右上方的 **X** 以关闭窗口并返回到 LMU。

从单个 Rapid Recovery Core 或受保护机器上卸载所有恢复点

完成以下过程仅卸载从单个 Core 或受保护机器中安装的恢复点。

- 1 从 Local Mount Utility 用户界面中，执行以下操作之一：
 - 右键单击您想要卸载所有恢复点的 Core。
 - 右键单击为您想要卸载所有恢复点的受保护机器。
 - 2 单击**为 [机器名称] 卸载全部**。
 - 3 要确认命令，在对话框中单击**是**。
- ④ | 注:** 如果有任何活动任务使用现有的安装，卸载这些装载会导致任务失败。
- 将根据您的选择卸载所有已安装的恢复点。

使用 Local Mount Utility 卸载所有已安装的恢复点

在 LMU 中一次性卸载所有恢复点有两个主要方式。您可以卸载所有恢复点而不查看当前安装了哪些恢复点，您也可以查看所有当前已安装的恢复点，然后将它们全部卸载。请参阅每种方式的相关步骤。

使用“卸载所有安装”按钮卸载所有恢复点

要一次性卸载所有已安装的恢复点，请完成以下过程。

- 1 从 Local Mount Utility 菜单中，单击**卸载所有安装**。
 - 2 要确认命令，在对话框中单击**是**。
- ④ | 注:** 如果有任何活动任务使用现有的安装，卸载这些装载会导致任务失败。

使用“活动安装”窗口卸载所有恢复点

要从“活动安装”窗口一次性卸载所有已安装的恢复点，请完成以下过程。

- 1 从 Local Mount Utility 用户界面中，单击**活动安装**。
- 2 在**活动安装**窗口中，单击**全部卸载**。
- 3 要确认命令，请在窗口中单击**是**。
- 4 在**活动安装**窗口中，单击**关闭**。

使用 Local Mount Utility 托盘菜单

LMU 托盘菜单位于桌面任务栏中。右键单击图标可显示下表中所述的选项：

表. 55: 托盘菜单选项

选项	说明
浏览恢复点	打开 LMU 主窗口。
活动安装	在 LMU 主窗口顶部打开“活动安装”对话框。
选项	在 LMU 主窗口顶部打开“选项”对话框。从“选项”对话框中，可以更改 LMU 用户界面的默认安装点目录和默认 Core 凭据。
关于	显示 Local Mount Utility 许可信息。
退出	关闭 LMU 应用程序。

管理您的设备

Core 控制台包含 **Appliance**（设备）选项卡，可用于配置空间、监测设备的运行状况，以及访问管理工具。

主题：

- 监测设备的状态
- Windows 备份
- 配置存储
- 删除虚拟磁盘的空间分配
- Recovery and Update Utility

监测设备的状态

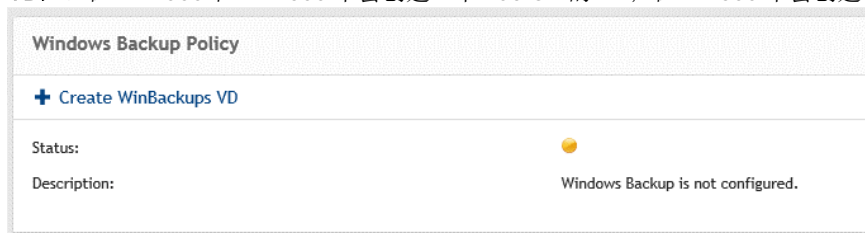
您可以使用 **Appliance**（设备）> **Health**（运行状况）页面上的 Appliance（设备）选项卡监测设备子系统的状态。**Health**（运行状态）页面在每个子系统旁边显示一个状态指示灯，以及指示子系统运行状况的状态说明。

Health（运行状况）页面还提供可深入了解每个子系统详情的工具链接，对警告或错误执行故障诊断时十分实用。**Provisioning Status**（配置状态）链接适用于存储配置子系统，可打开 **Provisioning**（配置）屏幕，显示该子系统的配置状态。**Rapid Appliance Self Recovery** 链接适用于 Rapid Appliance Self Recovery 子系统，可打开 **Backup**（备份）页面，您可在其中创建 RASR USB 闪存盘、监控 Windows 备份状态，并配置 Windows 备份策略。VM Management 链接打开 **Virtual Standby**（虚拟待机）页面，您可在其中管理虚拟机。**Server Administrator**（服务器管理员）链接适用于存储硬件子系统，打开系统的运行状况页面，您可在其中分析控制器、机柜、物理驱动器等的运行状况。**Controllers**（控制器）链接适用于设备硬件，打开 **Controllers**（控制器）页面，提供控制器和相关物理驱动器的详情。

Windows 备份

Windows 备份功能可用于所有 DL 系列，DL 1000 除外。**Appliance**（设备）> **Backup**（备份）选项卡可配置 Windows 备份策略，并显示上次备份的状态，以及之前备份的项目。要使用此 Windows 备份功能，必须存在 Windows 备份虚拟磁盘。

- 将设备升级至最新的 RUU (3.0.x) 后，如果 Windows 备份 VD（在 AppAssure 环境中创建）不存在，则会在完成 DL Appliance Configuration Wizard（DL 设备配置向导）后创建 Windows 备份虚拟磁盘。此时，如果 Windows 备份 VD 不存在，请在 **Windows Backup Policy**（Windows 备份策略）部分下的 **Backup**（备份）页面中单击 **+ Create WinBackups VD**（+ 创建 WinBackups VD）。在 DL 4000 和 DL 4300 中会创建一个 295 GB 的 VD；在 DL1300 中会创建一个 210 GB 的 VD。



- 将设备升级至最新的 RUU 后，如果 AppAssure 环境中存在创建的 Windows 备份 VD，请执行以下步骤以在 RR 环境中创建 Windows 备份 VD：
 - a 编辑 **ApplianceProvisioningConfiguration.xml**（该文件位于每个卷的根目录，因此您可对其编辑一次，然后复制到所需的位置）：

△| 小心: 请勿删除已有 Windows 备份 VD。

- 1 删除 <BackupVolumes> 标记之间的所有文本。
- 2 删除 </BackupVolumes> 标记。
- 3 编辑 <BackupVolumes> 标签, 改为 <Backupvolume/>
- 4 保存并关闭。
- b 转至 Core 控制台。
- c 单击 **Appliance (设备) > RASR** 选项卡。
- d 单击 **Create Windows Backup volume (创建 Windows 备份卷)** 按钮。
- e 如果空间足够, 则创建 Windows 备份 VD。

①| 注: 您也可使用 **Windows Server Backup** 功能配置 **Windows Backup**, 并将备份存储在任意位置, 但此时 **RASR** 页面中会显示一条错误, 因为这些备份无法得到控制, 且无法保证这些备份是否一致以使用 **RASR** 执行还原。

备份状态

Microsoft Windows 备份状态可在 **Last Backup (上次备份)** 选项卡下提供。如果当前正在运行备份, 则信息会显示在 **Current Backup (当前备份)** 选项卡下。要查看上次备份, 请执行以下步骤:

- 1 在 Core 控制台中, 导航至 **Appliance (设备) > Backup (备份)** 选项卡。
- 2 单击 **Status (状态)** 按钮旁的箭头来查看备份的状态。
- 3 **Last Backup (上次备份)** 窗格显示以下信息:
 - 状态
 - 状态
 - 备份位置
 - 开始时间
 - 结束时间
 - 错误说明
 - 所备份的项目

①| 注: 上述信息显示是否在运行 **Windows 备份策略**。

Backup Status	
Last Backup	
Status:	● (Completed successfully)
Backup Location:	F:
Start Time:	8/16/2016 7:34:00 PM
End Time:	8/16/2016 7:39:00 PM
Error Description:	
Error Actions:	
Items Backed Up	
State	Name
1	VolumeList
1	SystemState
1	BareMetalRecovery

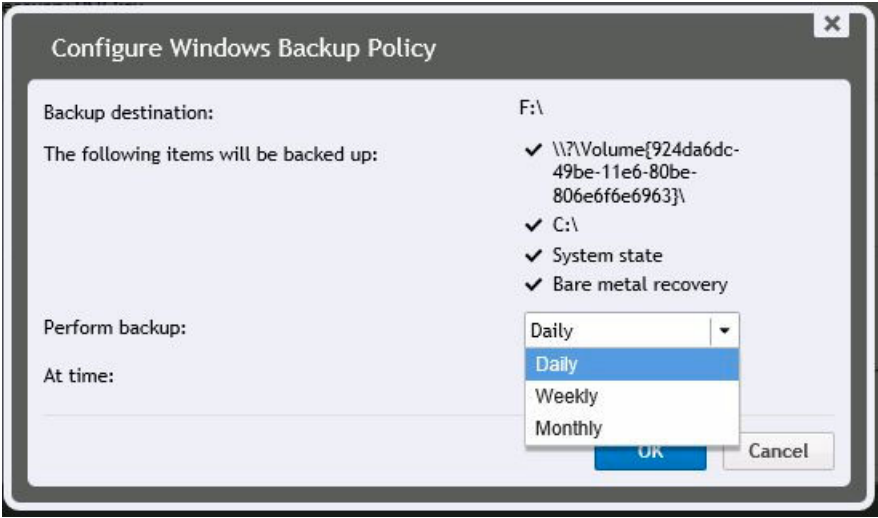
如果备份正在运行, 则会显示有关 **Current Backup Progress (当前备份进度)** 和 **Start Time (开始时间)** 的信息。

Windows 备份策略

要配置 Windows 备份策略，请执行以下步骤：

- 1 在 Core 控制台中，导航至 **Appliance**（设备） > **Backup**（备份）。
- 2 单击 **Configure Policy**（配置策略）按钮。

随即显示 **Windows Backup Policy**（Windows 备份策略）窗口。



- 3 如下所述输入参数：

文本框	说明
Following items will be backed up: （将备份以下项目：）	• OS 卷 • 恢复分区 • 裸机恢复二进制文件 默认会选中上述所有项目。
执行备份	选择 Winbackup 必须执行的频率。您具有以下选项：Daily（每天）、Weekly（每周）、和 Monthly（每月）。
Select the time to schedule the backup: （选择计划备份的时间：）	输入计划备份的时间。

- 4 单击 **Configure**（配置）。
- Winbackup 策略已配置并且 **Windows Backup Policy**（Windows 备份策略）部分中将显示详细信息。

一旦配置，您可以选择在任意时刻使用 **Backup now（立即备份）** 选项备份所选项并使用 **Windows Backup Policy（Windows 备份策略）** 部分中的 **Delete policy（删除策略）** 删除备份策略。

Windows Backup Policy

Backup now

Delete

Configure

Backup destination:

F:\

Perform backup:

Daily

At time:

1:00 PM

The following items will be backed up:

☒ \\?\Volume{924da6dc-49be-11e6-80be-806e6f6e6963}\

☒ C:\

☒ System state

☒ Bare metal recovery

配置存储

该设备配置可用的内部存储以及用于以下项目的所有已连接的受支持外部存储柜：

- 存储库\
- 适用于待机 VM 或其他任何目的的磁盘卷

开始在磁盘上配置存储之前，请确定要为待机虚拟机分配的存储大小。在创建 Rapid Recovery 存储库后，您可以分配剩余的任意百分比的可用容量来托管待机虚拟机。例如，如果使用 Storage Resource Management (SRM)，可以在创建 Rapid Recovery 存储库后分配剩余的全部容量。您只能在配置为托管虚拟机的设备上为待机虚拟机分配空间。通过 Rapid Recovery 的实时恢复功能，可以使用这些虚拟机来快速替代受此设备保护的故障服务器。

基于不需要待机虚拟机的中型环境，可以使用所有存储来备份大量代理。但是，如果您需要更多资源来运行待机虚拟机和备份较少的代理机器，则可以为较大的 VM 分配更多资源。

选择 **Appliance > Provisioning**（设备配置）选项卡时，Rapid Recovery Appliance 软件会为系统中所有受支持的控制器分配可用存储空间，并验证硬件是否符合要求。

要完成所有可用存储的磁盘配置，请执行以下操作：

- 1 单击 **Appliance > Provisioning**（设备配置）。
Provisioning（配置） 屏幕显示 **Repositories（存储库）** 和 **Storage Volumes（存储卷）** 部分。
 **小心:** 在继续操作之前，请确保已执行此过程中的步骤 2 到步骤 4。
- 2 配置可用的存储，以创建：
 - Repository（存储库）
 - 适用于待机 VM 或其他任何目的的磁盘卷
- 3 要创建存储库，请执行以下操作：
 - a 在 **配置** 页面中的 **Repositories（存储库）** 部分中，单击 **Add New Repository（添加新存储库）**
此时将显示 **Add New Repository（添加新存储库）** 对话框。
 - b 根据下表中的说明输入信息。

表. 56: 配置存储

文本框	说明
Repository Name（存储库名称）	输入存储库的显示名称。 默认情况下，该文本框包含文字 Repository 和一个编号，该编号与此 Core 的存储库的编号相对应。例如，如果是第二个存储库，则默认名称为 Repository 2。可根据需要更改该名称。

文本框	说明
	存储库名称必须包含 1 至 40 个字母数字字符，包括空格。请勿使用禁用字符或禁用短语，如需了解更多信息，请参见“Dell 数据保护 Rapid Recovery 6.0 用户指南”中的主题“禁用字符”或“禁用短语”。
控制器	根据您是在内部存储还是在直接连接存储机柜中创建存储库，选择相应的存储控制器。
机柜	选择相应的存储机柜。
RAID 类型	选择相应的 RAID 级别。您可选择以下 RAID 配置：1、5 或 6。
	注： 您的系统仅允许您以存储配置的 RAID 级别和出厂时支持的 RAID 级别创建存储库。要按所需的 RAID 配置创建存储库，您必须按所需的 RAID 级别配置存储。要按所需的 RAID 级别配置存储，请参见 www.dell.com/support/home 中的 Dell 适配器 文档。
预估容量	显示创建存储库可用的预估容量。
控制器可用空间	显示控制器中的可用空间。
大小	输入存储库的大小。
c 单击 创建 。	将创建一个新存储库。
4 创建适用于待机 VM 或其他任何目的的磁盘卷：	
a 在 Storage Volume（存储卷） 部分中，单击 Create Volume（创建卷） 。	
b 在 Create Volume（创建卷） 对话框中，为新磁盘卷指定以下信息：Volume name（卷名）、Controller（控制器）、Enclosure（机柜）、RAID type（RAID 类型）和 Size（大小）。	
	控制器可用空间显示为默认值。您可选择以下任一 RAID 配置：1、5 或 6。
c 单击 创建 。	新存储卷已创建。

删除虚拟磁盘的空间分配

如果您需要更改预配置的配置，请联系技术支持人员。有关更多信息，请参阅[联系 Dell](#) 部分。

Recovery and Update Utility

恢复与更新公用程序（Recovery and Update Utility，RUU）是一个一体式安装程序，旨在恢复和更新 DL 设备（DL1000、DL1300、DL4000 和 DL4300）软件。它包括 Rapid Recovery Core 软件和设备特定的组件。

RUU 包含更新版本的 Windows Server 角色和功能、.Net 4.5.2、LSI 提供程序、DL 应用程序、OpenManage Server Administrator 和 Rapid Recovery Core 软件。此外，恢复与更新公用程序还更新快速设备自行恢复（RASR）的内容。

注：如果您当前使用的是任何 AppAssure Core 版本、Rapid Recovery Core 6.0.2.144 或更早的版本，RUU 会强制更新为最新版本的 **Payload**。无法跳过该更新，且此更新无法恢复为之前的版本。如果您不想升级 Core 软件，请勿运行 RUU。

升级设备

要升级您的设备，请执行以下操作：

- 1 转至许可证门户的 Downloads（下载）部分或访问 support.dell.com 并下载 RUU 安装程序。
- 2 将该公用程序复制到 Appliance 桌面并解压缩文件。
- 3 双击 **launchRUU** 图标。
- 4 看到提示时，单击 **Yes（是）** 以确认未运行所列出的任何进程。

- 5 显示 **Recovery and Update Utility** 屏幕时，单击 **Start**（开始）。
- 6 系统提示重新引导时，单击 **OK**（确定）。
更新版本的 Windows Server 角色和功能、.Net 4.5.2、LSI 提供程序、DL 应用程序、OpenManage Server Administrator 和 Rapid Recovery Core 软件作为 Recovery and Update Utility 的一部分安装。除了这些以外，Recovery and Update Utility 也会更新 RASR 内容。
- ① **注：**如果您当前在使用任意 **AppAssure Core** 版本，**Rapid Recovery Core** 版本 **6.0.2.144** 或更早版本，RUU 会强制更新为 **Payload** 中可用的最新版本。更新不能跳过并且此更新是不可逆的。如果您不想升级 **Core** 软件，请勿运行 RUU。
- 7 如果系统提示，则重新引导系统。
- 8 安装所有服务和应用程序后，单击 **Proceed**（继续）。
Core 控制台启动。

修复您的设备

要修复您的设备，请执行以下操作：

- 1 转至许可证门户的 Downloads（下载）部分或访问 **support.dell.com** 并下载 RUU 安装程序。
- 2 将该公用程序复制到 Appliance 桌面并解压缩文件。
- 3 双击 **launchRUU** 图标。
- 4 看到提示时，单击 **Yes**（是）以确认未运行所列出的任何进程。
- 5 显示 Recovery and Update Utility 屏幕时，单击 **Start**（开始）。
- 6 系统提示重新引导时，单击 **OK**（确定）。
更新版本的 Windows Server 角色和功能、.Net 4.5.2、LSI 提供程序、DL 应用程序、OpenManage Server Administrator 和 Rapid Recovery Core 软件作为 Recovery and Update Utility 的一部分安装。
- 7 如果该公用程序中的捆绑版本与已安装版本相同，则 Recovery and Update Utility 会提示您确认是否要运行修复安装。如果不需要进行 Rapid Recovery Core 修复安装，则可以跳过此步骤。
- 8 如果该公用程序中的捆绑版本高于已安装版本，则 Recovery and Update Utility 会提示您确认是否要升级 Rapid Recovery Core 软件。
- ① **注：****Rapid Recovery Core** 软件不支持降级。
- 9 如果系统提示，则重新引导系统。
- 10 安装所有服务和应用程序后，单击 **Proceed**（继续）。
如果系统需要在修复后再次进行配置，则将启动 DL Appliance Configuration Wizard（DL 设备配置向导），否则将启动 Core Console。

保护工作站和服务器的

保护机器

本节介绍如何保护、配置和管理 Rapid Recovery 环境中的受保护计算机。

关于用 Rapid Recovery 保护计算机

要使用 Rapid Recovery 来保护数据，您需要在 Rapid Recovery Core Console 中添加要保护的工作站和服务器的，例如 Exchange Server、SQL Server、Linux 服务器等等。

必须在您想要保护 Core 的所有物理或虚拟机上安装 Rapid Recovery Agent 软件。

① 注: 此规则的例外情况就是，如果是对 VMware 或 ESXi 主机上的虚拟机进行保护，那么您可以使用无代理保护。有关包括无代理保护限制在内的更多信息，请参阅[理解 Rapid Snap for Virtual](#)。

在 Rapid Recovery Core Console 中，使用其中一个“保护计算机向导”，您可以确定您想要保护的计算机。可以执行以下操作：

- 您可以使用“保护机器向导”保护单个计算机，其中使用网络主机名称或 IP 地址连接到此计算机。有关如何保护单个计算机的更多信息，请参阅[保护机器](#)。
- 您可以使用“保护群集”功能保护网络群集，它可连接到使用网络主机名称或 IP 地址的群集及其节点。
- 您可以使用“保护多台计算机”向导来同时保护多台计算机，它通过 Microsoft Active Directory® 连接到计算机、vCenter 或 ESXi 主机；您也可以为手动输入的计算机列表指定网络主机名称或 IP 地址。

① 注: 戴尔建议您将同时保护的计算机数量限制为 50 台或更少，以防止因资源约束而导致保护操作失败。

在向向导中确定单个计算机的保护要求时，您可以指定要保护的卷。保护多台计算机时，默认所有卷都受到保护。（您可以稍后在单个计算机基础上进行更改）。

该向导还可让您定义保护自定义计划（或重新使用现有的计划）。

使用“高级”选项，您可以通过指定或将加密密钥应用到您要保护的计算机的备份以添加额外的安全措施。

最后，如果尚无备份，则您可以使用向导定义存储库。

安装 Agent 软件后，每台计算机必须在软件安装后重新启动。

有关如何保护工作站和服务器的更多信息，请参阅[保护机器](#)。

△ 小心: Rapid Recovery 不支持有 ext2 启动分区的 Linux 计算机的裸机恢复。在有此类分区的机器上所执行的任何 BMR 会导致机器不启动。如要在有 ext2 启动分区的 Linux 计算机上执行裸机恢复，那么您必须在开始保护和备份计算机前将 ext2 启动分区转换为 ext3 或 ext4。

关于使用 Rapid Recovery 保护 Linux 机器

Rapid Recovery Agent 软件兼容多个基于 Linux 的操作系统（有关详细信息，请参阅 *Rapid Recovery 安装和升级指南* 或 *Rapid Recovery 发行说明* 中包含的系统要求）。Rapid Recovery Core 只与 Windows 机器兼容。当您从 Rapid Recovery Core Console 管理受

保护的 Linux 机器时，适用于 Linux 机器的若干步骤就会与 Windows 对应的版本有所不同。此外，您可以使用 `local_mount` 命令行实用程序直接在受保护 Linux 机器上执行某些操作。

① | 注: `local_mount` 实用程序以前称为 `aamount`。

关于在 Rapid Recovery Core 中管理 Exchange 和 SQL Server

在受保护机器上检测到软件实例和相关文件时，将在 Rapid Recovery Core Console 中显示特定于 Exchange Server 和 SQL Server 的选项。在这些情况下，当您在 Core Console 中选择受保护机器时，可以使用附加选项。

例如，如果您在左侧导航菜单中选择受保护的 Exchange Server，则为该受保护机器显示的菜单选项中包括一个 **Exchange** 下拉菜单选项。

如果您在左侧导航菜单中选择受保护的 SQL Server，则为该受保护机器显示的菜单选项中包括一个 **SQL** 下拉菜单。

这些选项可能作用不同，但存在一些共性。您可以为受保护的 Exchange 和 SQL Server（不适用于其他受保护机器）实现的功能包括：

- **强制服务器日志截断。**SQL Server 和 Exchange Server 均包含服务器日志。截断 SQL 日志的过程将确定服务器上的可用空间。当您截断 Exchange Server 日志时，除了确定可用空间外，该过程还将释放服务器上更多的空间。
- **相关服务器的设置凭据。**Exchange Server 允许您在受保护服务器的“摘要”页面中设置受保护机器的凭据。SQL Server 允许您为单个受保护的 SQL Server 机器设置凭据，或为所有受保护的 SQL Server 设置默认凭据。
- **查看对 Exchange Server 或 SQL Server 中的恢复点执行的检查的状态。**从受保护的 SQL 或 Exchange Server 捕获的恢复点具有相应的彩色状态指示符。这些颜色指示与 SQL Server 或 Exchange Server 相关的各种检查是成功还是失败。

本部分包含以下特定于管理使用 Exchange Server 或 SQL Server 的受保护机器的主题：

- [了解恢复点状态指示器](#)
- [受保护的 Exchange Server 的设置和功能](#)
- [受保护 SQL 服务器的设置和功能](#)

关于保护服务器群集

在 Rapid Recovery 中，服务器群集保护与各个群集节点（即群集中的单个计算机）上安装的受保护 Rapid Recovery 计算机以及保护这些计算机的 Rapid Recovery Core 相关联，它们全部就像是一台复合的计算机。

您可以轻松配置 Rapid Recovery Core 以保护和管理群集。在 Core Console 中，群集以单独实体的形式进行组织，充当了包含相关节点的容器。例如，在左侧导航区域中，受保护群集将列示在**受保护计算机**菜单下。相关联的单个节点或代理机器直接显示在每个群集下。所有这些节点或代理计算机是已安装 Rapid Recovery Agent 软件的受保护计算机。如果单击群集，群集的**摘要**页面将显示在 Core Console 中。

在 Core 和群集层级，可以查看关于群集的信息，例如相关节点和共享卷的列表。当在 Core Console 中显示群集时，您可以单击顶部导航菜单中的**受保护节点**以查看群集中各节点的摘要表。从该摘要表中，您可以对各个节点执行类似如下的功能：强制创建快照；执行一次性导出或建立虚拟备用机；安装或查看恢复点；从恢复点还原；将群集节点转换到自身的受保护计算机；或将节点从保护中移除。如果节点是 Exchange 或 SQL Server，您还会看到截断日志的选项。

在群集层级，还可以查看群集中各节点相应的 Exchange 和 SQL 群集元数据。您可以为整个群集指定设置并指定该群集中的共享卷。

如果您在左侧导航菜单中单击群集中的任何节点，Core Console 中显示的信息将特定于群集的该节点。您可以在此处查看特定于该节点的信息，或为该节点配置设置。

支持群集共享卷

在 Rapid Recovery 6.x 版中，对群集共享卷 (CSV) 的支持限于运行 Windows Server 2008 R2 的 CSV 原生备份。您也可从恢复点恢复运行 Windows Server 2008 R2 的 CSV 卷，或执行虚拟输出至运行 Windows Server 2008 R2 的 Hyper-V CSV。您无法执行群集共享卷

的虚拟输出。Rapid Recovery 6.0.1 和更高版本中的全新功能可执行虚拟输出至运行 Windows Server 2012 或 Windows Server 2012 R2 的 Hyper-V CSV。

① | 注: Hyper-V 无代理功能仅与 Windows Server 2012 R2 和更高版本兼容。

对于其他操作系统，Rapid Recovery Agent 服务可在群集中的所有节点上运行，且群集可作为 Rapid Recovery Core 内的群集受到保护；但 CSV 不会显示在 Core 控制台中，且不会受到保护。所有本地磁盘（如操作系统卷）可收到保护。

下表说明了当前在 Rapid Recovery Core 中为群集共享卷提供的支持。

表. 57: Rapid Recovery 支持群集共享卷

Rapid Recovery 全集共享卷支持	保护、复制、前滚、装载、存档	还原 CSV 卷	虚拟导出至 Hyper-V CSV
Rapid Recovery	6.0	6.0	6.0.x
Windows Server 2008 R2	是	是	是
Windows Server 2012	否	否	是
Windows Server 2012 R2	否	否	是

¹ 不包括 Hyper-V 无代理功能，Hyper-V 无代理功能仅与 Windows Server 2012 R2 和更高版本兼容。

虽然 Rapid Recovery 也会让您保护群集共享卷上的某些其他操作系统，但这样做您将自行承担风险。Dell 仅支持上表中的配置。

支持的动态和基本卷

Rapid Recovery 支持对所有动态和基本卷进行快照。Rapid Recovery 同时也支持导出单个物理磁盘上的简单动态卷。顾名思义，简单动态卷不是带区卷、镜像卷、跨区卷或 RAID 卷。

动态磁盘的虚拟导出行为不同，具体取决于您想要导出的卷受 Rapid Recovery Agent 软件保护还是它是使用无代理保护的虚拟机。这是因为非简单或复杂动态卷具有 Rapid Recovery Agent 无法全面解读的随机磁盘几何结构。

当您尝试从装有 Rapid Recovery Agent 软件的机器导出复杂的动态磁盘时，用户界面中将显示一则通知，提醒您导出限于简单动态卷。如果您尝试使用 Rapid Recovery Agent 导出简单动态卷以外的任何其他内容，则导出作业将会失败。

相反，您以无代理方式保护的虚拟机的动态卷支持保护、虚拟导出、还原数据和 BMR 以及用于存储库存储，但存在一些重要限制。例如：

- 保护：**如果动态卷跨接多个磁盘，您必须共同保护这些磁盘以保持卷的完整性。
- 虚拟导出：**您可以使用无代理保护从 ESXi 主机导出复杂的动态卷（例如，带区卷、镜像卷、跨区卷或 RAID 卷）。但是，卷在磁盘级别导出，不执行卷分析。例如，如果导出跨接两个磁盘的动态卷，则导出将包括两个不同的磁盘卷。

⚠ | 小心: 当导出跨接多个磁盘的动态卷时，您必须使用原始系统卷导出动态磁盘以保留磁盘类型。

- 还原数据：**当导出跨接多个磁盘的动态卷时，您必须使用原始系统卷还原动态磁盘以保留磁盘类型。如果仅还原一个磁盘，您可以解除磁盘配置。

存储库存储：此外，Rapid Recovery 支持在复杂的动态卷上创建存储库（带区卷、镜像卷、跨区卷或 RAID 卷）。托管存储库的机器的文件系统必须是 NTFS 或 ReFS。

卸载 Rapid Recovery Agent 软件安装程序

Rapid Recovery 可让您从 Rapid Recovery Core 下载安装程序。从**下载**页面中，您可以选择下载 Agent Installer、Local Mount Utility (LMU) 或 SNMP MIB 文件。有关 LMU 的更多信息，请参阅 [Local Mount Utility](#)。有关 SNMP 的更多信息，请参阅[了解 SNMP 设置](#)。

- ① **注:** 要访问 **Agent Installer**, 请参阅[下载 Rapid Recovery Agent 安装程序](#)。有关部署 **Agent Installer** 的更多信息, 请参阅“**Dell Data Protection | Rapid Recovery Installation and Upgrade Guide**”（《**Dell Data Protection | Rapid Recovery 安装和升级指南**》）。

Agent Installer 用于在计划由 Rapid Recovery Core 保护的机器上安装 Rapid Recovery Agent 应用程序。如果确定有一台机器需要 Agent Installer, 可从 Rapid Recovery Core Console 的“下载”页面下载 Web 安装程序。

- ① **注:** Core 的下载是从 **Dell Data Protection | Rapid Recovery** 许可证门户执行的。要下载 **Rapid Recovery Core** 安装程序, 请访问<https://licenseportal.com>。有关更多信息, 请参阅“**Dell Data Protection | Rapid Recovery 许可证门户 User Guide**”（《**Dell Data Protection | Rapid Recovery 许可证门户用户指南**》）。

下载 Rapid Recovery Agent 安装程序

下载 Rapid Recovery Agent 安装程序并将其部署到您要在 Rapid Recovery Core 上保护的任何计算机上。要下载该 Web Installer, 请完成以下过程中的步骤。

- 1 要直接从您要保护的计算机上下载该 Agent Web 安装程序, 请执行以下操作:
 - a 在网页浏览器中, 打开 Dell Data Protection | Rapid Recovery 许可证门户 (<https://licenseportal.com>)。
 - b 从左侧导航菜单, 单击**下载**。
 - c 从**基于 Windows 的应用程序**窗格中, 向下滚动到 **Windows Agent** 行, 然后单击**下载**以下载相应的安装程序（32 位或 64 位系统）。将安装程序文件（例如 Agent-X64-6.0.1.xxxx.exe）保存至下载目标文件夹。
- 2 要从 Core 中下载该 Web 安装程序, 在 Core Console 的图标栏中单击  **更多**图标, 然后选择**下载**。
- 3 在**下载**页面中, 从 **Agent** 窗格中单击**下载 Web 安装程序**。
- 4 在**打开 Agent-Web.exe** 对话框中, 单击**保存文件**。
将安装程序文件（例如 Agent-X64-6.0.1.xxxx.exe）保存至下载目标文件夹。
- 5 将安装程序移动到相应的计算机并安装 Rapid Recovery Agent 软件。
有关安装 Rapid Recovery Agent 软件的更多信息, 请参阅“**Rapid Recovery Installation and Upgrade Guide**”（《**Rapid Recovery 安装和升级指南**》）。

通过 Core Console 将代理同时部署到多个机器

您可以将 Rapid Recovery Agent 软件同时部署到多个 Windows 机器。这些机器可以是 Active Directory 域的一部分或 vCenter 或 ESX(i) 虚拟主机; 或者它们可以是已由本地 Rapid Recovery Core 保护的机器, 比如在 Rapid Recovery Agent 软件升级情况下。您还可以选择手动将软件部署到与特定域或主机相不一定关联的机器。

您也可以通过 Core Console 手动将 Rapid Recovery Agent 软件部署到一个或多个 Linux 机器。

- ⚠ **小心:** 如果 Linux 机器上已安装有 **AppAssure Agent**, 则在安装 **Rapid Recovery Agent** 之前, 请使用 **shell** 脚本从该机器上卸载 **AppAssure Agent**。有关从 Linux 机器卸载该代理的信息, 请参阅主题[从 Linux 机器卸载 AppAssure Agent 软件](#)。要成功将该 Agent 软件部署到 Linux 机器, 请参阅[有关在 Linux 机器上安装 Agent 软件](#)这一主题中的前提条件。这些主题可在 **Dell Data Protection | Rapid Recovery Installation and Upgrade Guide**（**Dell 数据保护 | 《Rapid Recovery 安装和升级指南》**）中找到。

部署 Rapid Recovery Agent 软件不会自动保护机器。在部署后, 您必须从 Core Console 按钮栏中选择 **Protect Multiple Machines**（**保护多个机器**）选项。

- ① **注:** 同时部署到多个机器时所用的功能先前被称为“批量部署”。同时保护多个机器时所用的功能先前被称为“批量保护”。

要同时部署和保护多个机器, 请执行以下任务:

- 将 Rapid Recovery Agent 部署到多个机器。请参阅[将 Rapid Recovery Agent 软件部署到一台或多台机器](#)。
- 监测部署。请参阅[验证多台机器的部署](#)。
- 保护多个机器。请参阅[关于保护多台计算机](#)。

- ① **注:** 如果您在部署期间选择了 **Protect Machine After Install**（在安装后保护机器）选项，请跳过此任务。
- 监测批量保护活动。请参阅[监测多台机器的保护](#)。

将 Rapid Recovery Agent 软件部署到一台或多台机器

可以使用“部署 Agent 软件向导”来简化将 Rapid Recovery Agent 软件部署到一台或多台 Windows 机器的任务。

- ① **注:** 在过去，此功能称为“批量部署”。

当您使用“部署 Agent 软件向导”时，Rapid Recovery 可以自动检测主机上的机器，并可让您选择想要部署到的机器。对于 Active Directory 或者 vCenter 或 ESX(i) 以外的其他域或主机上的机器，您可以使用其 IP 地址和合适的凭据手动连接到各台机器。您也可以将软件升级推送到本地 Rapid Recovery Core 已保护的机器。

在 Core Console 内，您可以完成以下任一任务：

- 部署到 [Active Directory 域上的机器](#)
- 部署到 [VMware vCenter/ESX\(i\) 虚拟主机上的机器](#)
- 在受保护的计算机上部署 [Rapid Recovery Agent 软件升级](#)
- [手动部署到机器](#)

- ① **注:** Dell 建议将要同时部署到的机器数量限制为 50 台或更少，以防止遇到可能会导致部署操作失败的资源限制。

- ① **注:** 目标机器必须能够访问 Internet 才能下载和安装位，因为 Rapid Recovery 使用 Web 版本的 **Rapid Recovery Agent Installer** 部署安装组件。如果 Internet 访问不可用，请使用 **Core Console** 将安装程序下载至介质（例如 USB 驱动器），然后在您想要保护的机器上实际安装软件。有关更多信息，请参阅[下载 Rapid Recovery Agent 安装程序](#)。

部署到 Active Directory 域上的机器

使用此过程可将 Rapid Recovery Agent 软件同时部署到 Active Directory 域上的一台或多台计算机。开始此过程之前，必须获得现有 Active Directory 服务器的域信息和登录凭据。

- 1 在 Rapid Recovery Core Console 中，单击**保护**下拉菜单，然后单击**部署 Agent 软件**。此时会打开“部署 Agent 软件向导”。
- 2 在向导的**连接**页面中，从**源**下拉列表中选择 **Active Directory**。
- 3 按照下表中的说明输入域信息和登录凭据。

表. 58: 域信息和凭据

文本框	说明
主机	Active Directory 域的主机名或 IP 地址。
用户名	用于连接域的用户名，例如 Administrator；或者，如果该机器位于域中，则为 [domain name] \Administrator。
密码	用于连接域的安全密码。

- 4 单击**下一步**。
- 5 在**机器**页面上，选择要为其部署 Rapid Recovery Agent 软件的机器。
- 6 或者，要在 Agent 安装完成后自动重启受保护机器，请选择 **Agent 安装后，自动重启计算机（推荐）**。
- 7 单击**完成**。
系统将自动验证您所选的每台机器。
如果 Rapid Recovery 在自动验证期间检测到任何问题，向导将前进到“警告”页面，您可在该页面从所选项中清除机器并手动验证所选机器。如果添加的计算机通过自动验证，它们将显示在“部署 Agent 到机器”窗格中。
- 8 如果出现“警告”页面，但您仍对选择满意，再次单击**完成**。

Rapid Recovery Agent 软件将部署到指定机器。机器仍未受保护。当您完成[保护 Active Directory 域上的多个机器](#)后，保护才开始。

部署到 VMware vCenter/ESX(i) 虚拟主机上的机器

使用此过程可将 Rapid Recovery Agent 软件同时部署到 VMware vCenter/ESX(i) 虚拟主机上的一台或多台计算机。开始此过程之前，您必须具有以下信息：

- VMware vCenter/ESX(i) 虚拟主机的登录凭据。
- 主机位置。
- 您想要保护的每台计算机的登录凭据。

① 注：所有虚拟机必须安装 **VMware** 工具，否则 **Rapid Recovery** 无法检测到要部署的虚拟机的主机名。**Rapid Recovery** 将使用虚拟机名称代替主机名，如果主机名与虚拟机名不同，则会导致问题。

- 1 在 Rapid Recovery Core Console 中，单击**保护**下拉菜单，然后单击**部署 Agent 软件**。此时会打开**部署 Agent 软件向导**。
- 2 在向导的**连接**页面中，从**源**下拉列表中选择 **vCenter / ESX(i)**。
- 3 按照下表中的说明输入主机信息和登录凭据。

表. 59: vCenter/ESX(i) 连接设置

文本框	说明
主机	VMware vCenter Server/ESX(i) 虚拟主机的名称或 IP 地址。
端口	用于连接此虚拟主机的端口。 默认设置为 443。
用户名	用于连接到虚拟主机的用户名，例如 Administrator；或者，如果计算机位于域中，则为 [domain name] \Administrator。
密码	用于连接此虚拟主机的安全密码。

- 4 单击**下一步**。
- 5 在向导的**计算机**页面中，从下拉菜单中选择以下选项之一：
 - 主机和群集
 - VM 和模板
- 6 展开计算机列表，然后选择您要为其部署软件的虚拟机。
如果 Rapid Recovery 检测到计算机处于离线状态或未安装 VMware 工具，此时会出现一个通知。
- 7 如果您希望在部署后自动重启机器，选择 **Agent 安装后，自动重启机器（推荐）**。
- 8 单击**下一步**。
Rapid Recovery 将自动验证您所选的每台计算机。
- 9 在向导的**调整**页面中，按以下格式输入每台计算机的凭据：hostname::username::password。

① 注：在每行输入一台计算机。

- 10 单击**完成**。
系统将自动验证您所选的每台机器。
如果 Rapid Recovery 在自动验证期间检测到任何问题，向导将前进到“警告”页面，您可在该页面从所选项中清除机器并手动验证所选机器。如果添加的计算机通过自动验证，它们将显示在“部署 Agent 到机器”窗格中。
- 11 如果出现“警告”页面，但您仍对选择满意，再次单击**完成**。

Rapid Recovery Agent 软件将部署到指定机器。机器仍未受保护。当您完成**保护 VMware vCenter/ESX(i) 虚拟主机中的多台机器**后，保护才开始。

在受保护的计算机上部署 Rapid Recovery Agent 软件升级

您可以使用“部署 Agent 软件向导”将 Rapid Recovery Agent 软件的升级推送至受本地 Rapid Recovery Core 保护的计算机上。

- 1 在 Rapid Recovery Core Console 中，单击**保护**下拉菜单，然后单击**部署 Agent 软件**。
此时会打开**部署 Agent 软件向导**。
- 2 在向导的**连接**页面中，从**源**下拉列表中选择**本地 Core**。
- 3 单击**下一步**。
- 4 在向导的**计算机**页面上，选择要为其部署 Rapid Recovery Agent 软件升级的受保护机器。
- 5 单击**完成**。
系统将自动验证您所选的每台机器。
如果 Rapid Recovery 在自动验证期间检测到任何问题，向导将前进到**警告**页面，您可在该页面从所选项中清除机器并手动验证所选机器。如果添加的计算机通过自动验证，它们将显示在**部署 Agent 到机器**窗格中。
- 6 如果出现**警告**页面，但您仍对选择满意，再次单击**完成**。

手动部署到机器

使用下面的过程将 Rapid Recovery Agent 部署到本地 Core、Active Directory 或 vCenter/ESXi 以外的任何类型主机上的多台机器上。

- 1 在 Rapid Recovery Core Console 上，单击**保护**下拉菜单，然后选择**部署 Agent 软件**。
此时会打开**部署 Agent 软件向导**。
- 2 在向导的**连接**页面中，从**源**下拉列表中选择**手动**。
- 3 单击**下一步**。
- 4 在向导的**机器**页面中，以以下格式在对话框中输入计算机详细信息：hostname::username::password::port。示例包括：
10.255.255.255::administrator::&11@yYz90z::8006
abc-host-00-1::administrator::99!zU\$083r::168
- 5 如果您希望在部署后自动重启机器，选择**Agent 安装后，自动重启机器（推荐）**。
- 6 单击**完成**。
系统将自动验证您所选的每台机器。
如果 Rapid Recovery 在自动验证期间检测到任何问题，向导将前进到**警告**页面，您可在该页面从所选项中清除机器并手动验证所选机器。如果添加的计算机通过自动验证，它们将显示在**部署 Agent 到机器**窗格中。
- 7 如果出现**警告**页面，但您仍对选择满意，再次单击**完成**。

Rapid Recovery Agent 软件将部署到指定机器。机器仍未受保护。当您完成**手动保护多台计算机**后，保护才开始。

验证多台机器的部署

将 Rapid Recovery Agent 软件同时部署到两台或多台计算机后，您可以查看“受保护计算机”菜单下列出的每台计算机以验证是否成功。

您还可以在“事件”页面中查看有关批量部署进程的信息。要验证部署，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console，单击 （事件），然后单击**警报**。
此时警报事件显示在列表中，其中显示事件启动的时间和一条消息。对于 Agent 软件的每个成功部署，您将看到一条警报，指示已添加受保护机器。
- 2 （可选）单击受保护机器的任何链接。
此时将显示所选计算机的**摘要**页面，其中显示如下的相关信息：
 - 受保护机器的主机名称
 - 上次快照（如适用）

- 下一次计划快照的时间（根据所选计算机的保护计划而定）
- 用于此受保护计算机的加密密钥（如有）。
- Agent 软件版本。

修改部署设置

要修改部署设置，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 中，单击 （设置）。
- 2 在 **设置** 页面的左侧列中单击 **部署** 以导航到的“部署”部分。
- 3 通过单击您想要更改的设置以使其成为可编辑的文本框或下拉列表，从而修改以下任何选项，然后单击  以保存设置。

表. 60: 部署选项

选项	说明
Agent Installer Name（代理安装程序名称）	输入代理程序可执行文件的名称。默认为 Agent-web.exe。
Core Address（Core 地址）	输入 Core 的地址。
接收超时失败	输入无活动超时的等待分钟数。
最大并行安装	输入您想要同时安装的最大安装程序数量。默认并限制为 100。
安装之后自动重新启动	选择“是”以选择该复选框，“否”以清除该复选框。
部署之后保护	选择“是”以选择该复选框，“否”以清除该复选框。

了解保护计划

保护计划定义备份何时从受保护代理计算机传输至 Rapid Recovery Core。

保存到 Core 的首次备份传输称为基本映像快照。全部指定卷（包括操作系统、应用程序和设置）上的所有数据将被保存到 Core，根据要传输的数据量，这会花费大量时间。此后，增量快照（较小的备份，仅包含受保护计算机自上次备份以来更改的数据）将按照定义的时间间隔（例如每 60 分钟）定期保存到 Core。此备份较基本映像包含较少的数据，因此需要的传输时间较短。

最初使用“保护机器向导”或“保护多台机器向导”定义保护计划。使用向导时，您可以自定义保护计划（选择周期或每天保护时间）以适应您的业务需要。然后，您可以在特定受保护计算机“摘要”页面的“保护计划”对话框中修改现有计划或随时创建新的计划。

Rapid Recovery 提供默认保护计划，包括具有单一时段（从 12:00 AM 至 11:59 PM）涵盖整周的单一时间段。默认时间间隔（快照之间的时间段）为 60 分钟。首次启用保护后，该计划也将激活。因此，使用默认设置时，无论当前时间如何，首次备份将每小时整点（12:00 AM、1:00 AM、2:00 AM 等）进行。

选择时间段可让您查看默认保护计划，并相应地做出调整。选择每天保护时间将导致 Rapid Recovery Core 每天在指定时间备份一次指定的受保护计算机。

您可以使用可用的工作日和周末时间段自定义计划以定义高峰和非高峰时间。例如，如果受保护计算机大多数情况下是在工作日使用，那么您可以将工作日周期的时间间隔缩短为 20 分钟，从而导致三个快照，每小时创建三次快照。或者，您可以将周末时间段的时间间隔由 60 分钟增加至 180 分钟，从而在流量较低时每 3 小时创建一次快照。

或者，可更改默认计划以定义每日高峰和非高峰时段。为此，可将默认开始和结束时间更改为更小的时间范围（例如，12:00 AM 至 4:59 PM）并设置相应的时间间隔（例如 20 分钟）。这表示高峰时段期间频繁备份。然后，您可以为剩余的时间跨度（5:00 PM 至 11:59 PM）添加额外的工作日时间范围，并设置相应（可能是更大）的时间间隔（例如 180 分钟）。这些设置定义了包括每天 5:00 PM 至 12:00 PM 的非高峰期。此自定义将导致从 5:00 PM 至 11:59 PM 期间每 3 小时创建一次快照；从 12:00 AM 直到 4:59 PM 期间每 20 分钟创建一次快照。

当使用“保护计划”对话框修改或创建保护计划时，Rapid Recovery 允许您选择将该计划另存为一个可重复使用的模板，届时您可以将其应用到其他受保护的计算机。

保护向导中的其他选项包括设置每天保护时间。这将导致在定义期间（默认设置为 12:00 PM）每天创建单个备份。

如果使用向导保护一台或多台计算机，则您可以在初始时暂停保护，这样可定义保护计划而不保护计算机。如果准备根据创建的保护计划开始保护机器，则必须明确恢复保护。有关恢复保护的更多信息，请参阅[暂停和恢复保护](#)。（可选）如果要立即保护机器，则可以强制创建快照。有关更多信息，请参阅[强制创建快照](#)。

保护机器

如果已在要保护的机器上安装了 Rapid Recovery Agent 软件，但尚未重新启动，请立即重启机器。

本主题介绍如何开始使用 Protect Machine Wizard（保护机器向导）保护您指定的单个机器上的数据。

① 注：除非 VMware 或 ESXi 主机上使用无代理保护，否则您想要保护的机器必须安装有 **Rapid Recovery Agent** 软件才能得到保护。您可以选择在此过程之前安装 Agent 软件，也可以在 **Protect Machine Wizard**（保护机器向导）中将该软件部署到目标机器上。

有关无代理保护及其限制的更多信息，请参阅[理解 Rapid Snap for Virtual](#)。

有关安装该 Agent 软件的更多信息，请参阅 *Dell Data Protection | Rapid Recovery 许可证门户 and Upgrade Guide*（Dell 数据保护 | 《Rapid Recovery 安装和升级指南》）中的“安装 Rapid Recovery Agent 软件”。如果未在保护机器前先安装该 Agent 软件，您将不能在此向导中选择特定卷加以保护。在这种情况下，代理机器上的所有卷默认都会包含在保护范围内。Rapid Recovery 支持配置有 EISA 分区的机器的保护和恢复。支持范围还包括使用 Windows 恢复环境（Windows RE）的 Windows 8 和 8.1 以及 Windows 2012 和 2012 R2 机器。

要使用一个过程同时保护多个机器，请参阅[关于保护多台计算机](#)。

添加保护时，您需要定义连接信息（如 IP 地址和端口）并为您想要保护的机器提供凭据。（可选）您可以提供一个要显示在 Core Console 中替代 IP 地址的显示名称。如果您更改该名称，则当您在 Core Console 中查看详细信息时，您将无法看到受保护机器的 IP 地址。您还可为机器定义保护计划。

如果您选择高级配置，则保护过程会包括您可访问的可选步骤。Advanced（高级）选项包含存储库功能和加密。例如，您可以指定现有的 Rapid Recovery 存储库来保存快照，或创建一个新的存储库。您也可以指定将现有的加密密钥（或添加一个新的加密密钥）来应用于保存到此机器 Core 中的数据。有关加密密钥的更多信息，请参阅[了解加密密钥](#)。

根据您的环境，保护向导的工作流程可能略有不同。例如，如果 Rapid Recovery Agent 软件已安装在您要保护的机器上，则系统将不会提示您通过向导安装该软件。同样，如果 Core 上已存在存储库，则系统将不会提示您创建一个存储库。

⚠ 小心： Rapid Recovery 不支持带有 ext2 引导分区的 Linux 机器的裸机还原。在具有这种类型分区的机器上执行任何裸机还原都会导致机器无法启动。如果您希望将来能够在此机器上执行裸机还原，则您必须先将任何 ext2 分区转换为 ext3 或 ext4，然后才能开始保护和备份机器。

1 请执行以下操作之一：

- 如果您是通過 Protect Machine Wizard（保护机器向导）开始的，请继续执行[步骤 2](#)。
- 如果您是从 Rapid Recovery Core Console 按钮栏开始的，请单击 **Protect**（保护）。

此时将显示 **Protect Machine Wizard**（保护机器向导）。

2 在 **Welcome**（欢迎）页面中，选择相应的安装选项：

- 如果不需要定义存储库或建立加密，请选择 **Typical（典型）**。
 - 如果您需要创建存储库，或为所选机器备份指定不同的存储库，或者想要使用向导建立加密，请选择 **Advanced (show optional steps)（高级（显示可选步骤））**。
 - （可选）如果您不想以后再看到 Protect Machine Wizard（保护机器向导）的 **Welcome（欢迎）** 页面，请选中 **Skip this Welcome page the next time the wizard opens（下次向导打开时跳过此欢迎页面）** 选项。
- 3 在您满意 Welcome（欢迎）页面上所做的选择时，请单击 **Next（下一步）**。
- 此时将显示 **Connection（连接）** 页面。
- 4 在 **Connection（连接）** 页面中，根据下表中的说明输入有关要连接的机器的信息，然后单击 **Next（下一步）**。

表. 61: 机器连接设置

文本框	说明
主机	要保护的机器的主机名或 IP 地址。
端口	Rapid Recovery Core 用来与机器上的 Agent 进行通信的端口号。 默认端口号为 8006。
用户名	用于连接到此机器的用户名；例如，Administrator（或者，如果机器处于域中，则为 [域名] \Administrator）。
密码	用于连接至此机器的密码。

如果 Protect Machine Wizard（保护机器向导）中接下来显示 **Install Agent（安装 Agent）** 页面，则意味着 Rapid Recovery 在机器上没有检测到 Rapid Recovery Agent 并且将安装该软件的最新版本。请转至 [步骤 7](#)。

如果该向导中接下来显示 **Upgrade Agent（升级 Agent）** 页面，则意味着您想要保护的机器上已存在一个较旧版本的 Agent 软件。

① 注: Agent 软件必须安装在您想要保护的机器上，并且必须重新启动该机器，这样才能备份到 Core。要让安装程序重新启动受保护机器，请选择选项 **After installation, restart the machine automatically (recommended)（在安装后，自动重新启动机器（建议））**，然后单击 **Next（下一步）**。

- 5 在 **Upgrade Agent（升级 Agent）** 页面中，执行以下操作之一：
- 要部署 Agent 软件的新版本（与 Rapid Recovery Core 的版本匹配），请选择 **Upgrade the Agent to the latest version of the software（将 Agent 升级到软件的最新版本）**。
 - 要继续保护机器而不更新 Agent 软件版本，请取消选中 **Upgrade the Agent to the latest version of the software（将 Agent 升级到软件的最新版本）** 选项。
- 6 单击 **下一步**。
- 7 （可选）在 **Protection** 页面，如果您想要名称而非 IP 地址显示在此保护机器的 Rapid Recovery Core Console 中，请在对话框的 **Display Name（显示名称）** 字段中，键入名称。
- 您可以至多输入 64 个字符。请勿使用主题 [禁止字符](#) 中所述的特殊字符。此外，对于显示名称，请勿以主题 [禁止短语](#) 中所述的任何字符组合开头。
- 8 根据下面的说明选择相应的保护计划：
- 要使用默认保护计划，请在 Schedule Settings（计划设置）选项中，选择 **Default protection（默认保护）**。

根据默认保护计划，Core 将对受保护机器上的所有卷每小时拍摄一次快照。要在关闭向导后随时更改保护设置，包括选择要保护的卷，请转至 Summary（摘要）页面以找到特定的受保护机器。

- 要定义不同的保护计划，请在 Schedule Settings（计划设置）选项中选择 **Custom protection（自定义保护）**。

- 9 继续按如下所示进行配置：

- 如果在 Protect Machine Wizard（保护机器向导）中选择了 Typical（典型）配置，请单击 **Finish（完成）** 以确认您的选择，关闭向导，并保护您指定的机器。
首次为机器添加保护时，除非您指定初始暂停保护，否则在您定义计划后会将基本映像（即受保护卷中所有数据的快照）传输至 Rapid Recovery Core 上的存储库。
- 如果选择了 Protect Machine Wizard（保护机器向导）的 Typical（典型）配置并指定了自定义保护，请单击 **Next（下一步）** 以设置自定义保护计划。有关定义自定义保护计划的详情，请参阅 [创建自定义保护计划](#)。

- 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置和默认保护，请单击 **Next（下一步）**，然后前进到 [步骤 14](#) 以查看存储库和加密选项。
 - 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置并指定了自定义选项，则单击 **Next（下一步）** 并前进到 [步骤 11](#) 以选择要保护的卷。
- 10 在 **Protection Volumes（保护卷）** 页面中，选择要保护的卷。如果列出了任何您不想纳入保护的卷，则在 Check（选中）列中单击清除选择。然后单击 **Next（下一步）**。

注：通常情况下，最佳做法是至少保护系统保留卷和包含操作系统的卷（通常为 C 驱动器）。

- 11 在 **Protection Schedule（保护计划）** 页面中，定义自定义保护计划，然后单击 **Next（下一步）**。有关定义自定义保护计划的详细信息，请参阅 [创建自定义保护计划](#)。

如果已配置存储库信息，并且在步骤 1 中所选了 Advanced（高级）选项，则会显示 Encryption（加密）页面。继续执行 [步骤 13](#)。

- 12 在 **Repository（存储库）** 页面上，执行以下操作：

- 如果您已经有了一个存储库并想要存储此机器中的数据以保护现有存储库，请执行以下操作：
 - 1 选择 **Use an existing repository（使用现有存储库）**。
 - 2 从列表中选择一个现有存储库。
 - 3 单击 **下一步**。

此时将显示 **Encryption（加密）** 页面。跳至 [步骤 13](#) 还可以定义加密。

- 如果您希望创建存储库，请选择 **Create a Repository（创建存储库）**，然后完成以下步骤。
 - 1 在 **Repository（存储库）** 中，输入下表所述信息。

表. 62: Add New Repository（添加新存储库）设置

文本框	说明
Repository Name (存储库名称)	输入存储库的名称。 默认情况下，此文本框包含词语 Repository（存储库）和一个数字，它与此 Core 的存储库数量相对应。例如，如果它是第一个存储库，默认名称为 Repository 1。请根据需要更改此名称。 存储库名称必须包含介于 1 和 40 之间的字母数字字符，包括空格。请勿使用 禁止字符 或 禁止短语 。
Concurrent Operations (并发操作数)	定义希望存储库支持的并发请求数量。默认值为 64。
注释	(可选) 输入关于此存储库的描述性说明。您可以输入至多 254 个字符。例如，键入 DVM Repository 2 。

- 2 单击 **Add Storage Location（添加存储位置）** 以定义存储库的特定存储位置或卷。此卷应为主存储位置。

小心：为存储库的存储位置指定根目录内的专用文件夹。请勿指定根目录位置。例如，使用 E:\Repository \，而非 E:\。如果在此步骤中创建的存储库之后被删除了，您的存储库的存储位置上的所有文件都会被删除。如果您在根目录上指定存储位置，则卷（例如，E:\）中的所有其他文件都会被删除。这可能会导致灾难性数据丢失。

此时将显示 **Add Storage Location（添加存储位置）** 对话框。

- 3 单击 **Add Storage Location（添加存储位置）** 以定义存储库的特定存储位置或卷。此卷应为主存储位置。
- 4 在 **Storage Location（存储位置）** 区域中，指定将文件添加到存储位置的方式。您可以选择添加本地连接的存储卷（例如，直接连接的存储、存储区域网络或网络连接存储）。您还可以指定通用 Internet 文件系统 (CIFS) 共享位置上的存储卷。
- 单击 **Add file on local disk（在本地磁盘上添加文件）** 以指定本地机器，然后根据下表中的说明输入信息。

表. 63: 本地磁盘设置

文本框	说明
Data Path (数据路径)	输入用于存储受保护数据的位置。

文本框	说明
	例如，键入 X:\Repository\Data。 在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。
Metadata Path (元数据路径)	输入用于存储受保护元数据的位置。 例如，键入 X:\Repository\Metadata。 在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。

- 您也可以选择 **Add file on CIFS share**（在 CIFS 共享上添加文件）指定一个网络共享位置，然后按下表所述输入相应的信息。

表. 64: CIFS 共享凭据

文本框	说明
UNC Path (UNC 路径)	输入网络共享位置的路径。 如果此位置位于根目录，请定义专用文件夹名称（例如，Repository）。 路径必须以 \\ 开始。指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。字母 a 至 z 区分大小写。请勿使用空格。不允许使用其他符号或标点符号。
用户名	指定用于访问网络共享位置的用户名。
密码	指定用于访问网络共享位置的密码。

- 5 在 **Storage Configuration**（存储配置）区域中，单击 **More Details**（详细信息），然后根据下表中的说明输入存储位置的详细信息。

表. 65: 存储配置详细信息

文本框	说明
大小	设置存储位置的大小或容量。最小大小为 1 GB。默认值为 250 GB。可以从以下各项中选择： - GB - TB ① 注: 指定的大小不能超过卷的大小。 如果存储位置是使用 Windows XP 或 Windows 7 的新技术文件系统 (NTFS) 卷，则文件大小限制为 16 TB。 如果存储位置是使用 Windows 8、8.1、Windows 10 或 Windows Server 2012、2012 R2 的 NTFS 卷，文件大小限制为 256 TB。 ① 注: 要让 Rapid Recovery 验证操作系统，在目标存储位置必须安装 Windows Management Instrumentation (WMI)。
Write Caching Policy (写高速缓存策略)	写高速缓存策略控制 Windows Cache Manager 在存储库中的使用方式，并帮助调整存储库以便在不同配置下实现最佳性能。 请将其设置为以下值之一： - On（打开） - Off（关） - Sync（同步） 如果设置为默认值 On（打开），则 Windows 将控制高速缓存。这适用于 Windows 10 以及 Windows Server 2012 和更高版本。 ① 注: 将写高速缓存策略设置为 On（打开）可提高性能。如果您使用的是 Windows Server 2008 SP2 或 Windows Server 2008 R2 SP2，则建议的设置为 Off（关闭）。

文本框	说明
	如果设置为 Off（关闭），则 Rapid Recovery 将控制高速缓存。
	如果设置为 Sync（同步），则 Windows 将控制高速缓存以及同步输入/输出。
每扇区字节数	指定希望每个扇区包含的字节数。默认值为 512。
Average Bytes per Record（每个记录的平均字节数）	指定每个记录的平均字节数。默认值为 8192。

6 单击下一步。

如果您在步骤 1 中选择了 **Advanced（高级）** 选项，此时将显示 **Encryption（加密）** 页面。

13 另外，在 **Encryption（加密）** 页面上，要启用加密，请选择 **Enable Encryption（启用加密）**。

在 **Encryption（加密）** 页面中将显示 Encryption key（加密密钥）字段。

注：如果启用加密，它将应用于此机器上所有受保护卷中的数据。您可以稍后从 **Rapid Recovery Core Console** 更改加密设置。有关加密的更多信息，请参阅主题 [了解加密密钥](#)。

小心：Rapid Recovery 在密码块链 (CBC) 模式中使用 AES 256 位加密和 256 位密钥。虽然使用加密是可选的，但是 Dell 强烈建议您建立加密密钥，并保护您定义的密码短语。请将密码短语保存在安全位置，因为它对于数据恢复至关重要。如果没有密码短语，将无法进行数据恢复。

14 在 **Encryption（加密）** 页面上，选择以下选项之一：

- 如果您想使用已在此 Rapid Recovery Core 上定义的加密密钥加密这些受保护的机器，请选择 **Encrypt data using an existing Encryption key（使用现有的加密密钥加密数据）**，然后从下拉菜单中选择相应的密钥。继续执行 [下一步](#)。
- 如果您想要将新的加密密钥添加到 Core 并对这些受保护的机器应用该密钥，请根据下表中的说明输入信息。

表. 66: 加密密钥设置

文本框	说明
名称	输入加密密钥的名称。 加密密钥的名称必须包含介于 1 和 130 之间的字母数字字符。其中不能包含特殊字符，例如反斜杠、斜杠、管道、冒号、星号、引号、问号、左方括号或右方括号、& 符号或散列值。
说明	输入加密密钥的注释。 当从 Core Console 查看加密密钥时，此信息会显示在 Description（说明）字段中。
密码短语	输入用于控制访问的密码短语。 最佳做法是为了避免上述列出的特殊字符。 密码短语记录在安全位置。Dell 支持部门无法恢复密码短语。一旦您创建加密密钥并将其应用于一个或多个受保护的机器，则一旦该密码短语丢失，您将无法恢复数据。
确认密码短语	重新输入刚输入的密码短语。

15 单击 **Finish（完成）** 以保存并应用设置。

首次为机器添加保护时，除非您指定初始暂停保护，否则在您定义计划后会将基本映像（即受保护卷中所有数据的快照）传输至 Rapid Recovery Core 上的存储库。

保护群集

本主题介绍如何在 Rapid Recovery 中添加要保护的群集。添加要保护的群集时，需要指定群集、群集应用程序或包含 Rapid Recovery Agent 的一个群集节点或机器的主机名或 IP 地址。

注：系统将使用存储库来存储从受保护节点捕获的数据快照。在开始保护群集中的数据之前，应至少设置一个与 **Rapid Recovery Core** 关联的存储库。

有关设置存储库的信息，请参阅[了解存储库](#)。

- 1 在 Rapid Recovery Core Console 中，单击**保护**按钮下拉菜单，然后单击**保护群集**。
- 2 在“连接到群集”对话框中，输入以下信息。

表. 67: 连接到群集设置

文本框	说明
主机	群集、群集应用程序或某一群集节点的主机名或 IP 地址。
端口	Rapid Recovery Core 用来与 Agent 进行通信的机器端口号。 默认端口号为 8006。
用户名	用于连接此机器的域管理员的用户名，例如 domain_name\administrator。
❗ 注: 必须输入此域名。不能使用本地管理员用户名连接到群集。	
密码	用于连接此机器的密码。

- 3 单击**连接**。
- 4 在“保护群集”对话框中，为此群集选择一个存储库。
- 5 如果您想要使用基于 Core 的加密保护此群集的恢复点，请选择一个加密密钥。
- 6 如果不希望在完成本程序后立即开始保护，选择**初始暂停保护**。
- 7 要使用默认设置保护群集，请选择默认保护的节点，然后跳到[步骤 10](#)。

- ❗ | 注:** 默认设置计划每 60 分钟为所有卷创建一个快照。
- 8 要输入群集的自定义设置（例如，自定义共享卷的保护计划），请执行以下其中一项操作，然后参阅[创建自定义保护计划](#)。
 - 要自定义单个节点的设置，请在您要自定义的节点旁边，单击**设置**，然后单击相关卷旁边的**功能**。
 - 要自定义群集设置，请单击对话框底部的“设置”按钮，然后单击相关卷旁边的**功能**。

有关自定义节点的更多信息，请参阅[保护群集中的节点](#)。

- 9 完成所有必要更改后，单击**保存**。
- 10 在“保护群集”对话框中，单击**保护**。

修改群集节点设置

为群集节点添加保护后，即可轻松修改这些机器或节点的基本配置设置（例如，显示名称、主机名等）、保护设置（例如，更改机器上本地卷的保护计划、添加或移除卷、暂停保护）等。

要修改群集节点设置，必须执行以下任务：

- 在 Rapid Recovery Core Console 中，导航至包含要修改的节点的群集，并选择您想要修改的机器或节点。
- 要修改和查看配置设置，请参阅[配置通知组](#)。
- 要配置系统事件的通知组，请参阅[查看和修改受保护机器设置](#)。
- 要自定义保留策略设置，请参阅[自定义受保护机器的保留策略设置](#)。
- 要修改保护计划，请参阅[修改保护计划](#)。
- 要修改传输设置，请参阅[关于修改传输设置](#)。

保护群集中的节点

此任务要求您首先保护群集。有关详情，请参阅[保护群集](#)。

本主题介绍如何保护已安装 Rapid Recovery Agent 的群集节点或机器上的数据。此过程可让您将保护群集时可能忽略的单个节点添加到保护中。

- 1 在 Rapid Recovery Core Console 中的“受保护机器”下，单击包含您要保护的节点的群集。
- 2 在群集的“摘要”页面上，单击**受保护节点**。
- 3 在“受保护节点”页面中，单击**保护群集节点**。
- 4 在“保护群集节点”对话框中，根据需要选择或输入以下信息。

表. 68: 保护群集节点设置

文本框	说明
主机	群集中可进行保护的节点的下拉列表。
端口	Rapid Recovery Core 用来与节点上的 Agent 进行通信的端口号。
用户名	用于连接此节点的域管理员的用户名，例如，example_domain\administrator 或 administrator@example_domain.com。
密码	用于连接此机器的密码。

- 5 要添加节点，请单击**连接**。
- 6 要开始使用默认保护设置保护此节点，请转至**步骤 13**。

① | 注: 默认设置可确保使用 **60 分钟** 间隔的计划保护所有卷。

- 7 在“保护 [节点名称]”对话框中，如果您想要使用默认设置以外的存储库，请使用下拉式列表选择一个存储库。
- 8 如果您想要使用基于 Core 的加密保护此群集的恢复点，请使用下拉式列表选择一个加密密钥。
- 9 如果不希望在完成本程序后立即开始保护，选择**初始暂停保护**。
- 10 要输入自定义设置（例如，自定义共享卷的保护计划），请执行以下操作：
 - a 要自定义单个卷的设置，请在您要自定义的卷旁边，单击相关卷旁边的**功能**。
 - b 请参阅**创建自定义保护计划**。
- 11 单击 **Protect**（保护）。

创建自定义保护计划

要在使用向导定义保护时创建自定义计划以保护受保护机器上的数据，请完成以下过程中的步骤。

- 1 在保护向导（“保护计算机”、“保护多台计算机”、“保护群集”）的**保护**页面中，选择“自定义保护”。
- 2 单击**下一步**。
- 3 在**保护卷**页面中，选择要保护的卷，然后单击**下一步**。
- 4 在**保护计划**页面中，要更改任意期间的间隔计划，请执行以下操作：
 - a 选择**期间**。
此时将显示现有期间，且可以进行修改。可编辑的字段包括每个期间的开始时间、结束时间和间隔时间（每 X 分钟）。
 - b 针对每个期间，单击间隔文本框并键入相应的间隔（以分钟为单位）。
例如，选中默认间隔时间 60，并将其替换为值 20 以便在此期间每 20 分钟执行快照。
- 5 要创建工作日的高峰和非高峰时段，请更改工作日期间的时间范围以便未包括 24 小时时间段，然后设置高峰范围的最佳间隔时间，再选择**剩余时间创建快照**并设置非高峰期间隔时间，方法是执行以下操作：
 - a 选择**期间**。
此时将显示现有期间，且可以进行修改。
 - b 单击**从框**或使用时钟图标以更改此期间的开始时间。
 - c 单击**至框**或使用时钟图标以更改此期间的结束时间。
 - d 单击间隔时间文本框，然后输入适当的间隔时间（以分钟为单位）。
例如，选中默认间隔时间 60，并将其替换为值 20 以便在此期间您选定的时间范围内每 20 分钟执行快照。
 - e 选择**其他时间进行快照**，然后输入间隔时间（以分钟为单位）。
- 6 要设置每天执行单个备份的时间，请选择**每天保护时间**，然后以 HH:MM AM 格式输入时间。例如，要在上午 9:00 执行每天备份，则输入 09:00 PM。

- 7 要在未开始备份时定义计划，请选择**初始暂停保护**。
从向导暂停保护后，在您明确恢复保护之前，将保持暂停状态。恢复保护后，将按照您创建的设计执行备份。有关恢复保护的更多信息，请参阅**暂停和恢复保护**。
- 8 如果对保护计划的更改满意，则视情况单击**完成**或**下一步**。返回相应向导的过程以完成任何剩余要求。

修改保护计划

保护计划定义备份何时从受保护代理计算机传输至 Rapid Recovery Core。最初使用“保护机器向导”或“保护多台机器向导”定义保护计划。

随时可以在特定代理机器的“摘要”选项卡中修改现有保护计划。

- ① **注：**有关保护计划的概念信息，请参阅**了解保护计划**。有关保护单台计算机的信息，请参阅**保护机器**。有关批量保护（保护多台计算机）的信息，请参阅**关于保护多台计算机**。有关使用上述向导之一自定义保护代理时的保护周期的信息，请参阅**创建自定义保护计划**。有关修改现有保护计划的信息，请参阅**修改保护计划**。

要修改受保护机器上卷的现有保护计划，请完成以下过程中的步骤。

- 1 在 Core Console 中，单击受保护计算机列表中您要更改保护计划的受保护计算机。
- 2 在您所选计算机的页面上，选择适用的卷，然后单击**设置计划**。
要一次选择所有卷，请单击标题行中的复选框。最初，所有卷共享相同的保护计划。

- ① **注：**通常，最好至少保护系统保留卷及包含操作系统的卷（通常为 C 驱动器）。

此时将显示“保护计划”对话框。

- 3 在“保护计划”对话框中，执行以下操作之一：
 - 如果之前已创建保护计划模板，并且想要将其应用到该受保护的计算机，可从下拉列表中选择模板，然后转到**步骤 7**。
 - 如果要从计划中移除现有时间段，请清除每个时间段选项旁的复选框，然后转到**步骤 7**。选项包括以下项：
 - 周一 - 周五：此时间范围表示通常的五天工作周。
 - 周六 - 周日：此时间范围表示通常的周末。
 - 如果您想要将新的保护计划另存为模板，请继续执行**步骤 4**。
 - 4 当工作日的开始时间和结束时间为 12:00 AM 到 11:59 PM 时，则存在单个时间段。要更改已定义期间的开始时间或结束时间，请执行以下操作：
 - a 选择相应的时间段。
 - b 要更改此时间段的开始时间，请使用**开始时间**下的时钟图标。
例如，使用箭头来显示时间 08:00 AM。
 - c 要更改此时间段的结束时间，请使用**结束时间**下的时钟图标。
例如，使用箭头来显示时间 06:00 PM。
 - d 根据自己的需求更改时间间隔。例如，如果定义高峰时段。将时间间隔由 60 分钟更改为 20 分钟以便每小时创建三次快照。
 - 5 如果您在**步骤 7**中定义了 12:00 AM 至 11:59 PM 以外的时间段，并且您希望在其余时间范围内执行备份，则必须通过执行以下操作来添加附加时间段以定义保护：
 - a 在相应的类别下，单击**添加时间段**。
 - b 单击时钟图标，选择所需的相应开始和结束时间。
例如，将开始时间设置为 12:00 AM，并将结束时间设置为 07:59 AM。
 - c 根据自己的需求更改时间间隔。例如，如果定义非高峰时段。将时间间隔由 60 分钟更改为 120 分钟以便每两小时创建一次快照。
 - 6 如果需要，则继续创建其他时间段，并视情况设置开始时间和结束时间及时间间隔。
- ① **注：**如果您想要移除添加的时间段，单击时间段最右侧的回收站图标，然后单击**是**以确认。
- 7 要从您设置的计划中创建模板，单击**另存为模板**。
 - 8 在“保存模板”对话框中，输入模板名称，然后单击**保存**。
 - 9 当保护计划符合您的要求后，单击**Apply（应用）**。

随即关闭“保护计划”对话框。

暂停和恢复保护

暂停保护时，将暂时停止从所选机器到 Rapid Recovery Core 的所有数据传输。恢复保护时，Rapid Recovery Core 将遵循保护计划中的要求，从而基于该计划定期备份数据。

您可以暂停保护任何 Rapid Recovery 受保护机器：

- 使用“保护机器向导”或“保护多台机器向导”创建保护时。
- 在 Rapid Recovery Core 左侧导航区域的“受保护机器”菜单中（暂停所有受保护机器的保护）。
- 在“受保护机器”页面中（单击“受保护机器”菜单时可访问）。
- 在“受保护机器”下拉菜单的特定受保护机器中。
- 在特定受保护机器的每个页面顶部。

如果使用“保护机器向导”或“保护多台机器向导”暂停保护，则在明确恢复之前将暂停保护。

如果在向导之外暂停保护，则可以选择在恢复之前暂停保护，或在指定时间（以天、小时和分钟的任意组合指定）内暂停保护。如果暂停一段时间，则在该时间过期时，系统将根据保护计划自动恢复保护。

您可以恢复保护任何已暂停的 Rapid Recovery 受保护机器：

- 在 Rapid Recovery Core 左侧导航区域的“受保护机器”下拉菜单中（恢复所有受保护机器的保护）。
- 在“受保护机器”下拉菜单的特定受保护机器中。
- 在“受保护机器”页面中（单击“受保护机器”菜单时可访问）。
- 在特定受保护机器的每个页面顶部。

要暂停或恢复保护（视情况而定），请使用以下过程。

- 1 在 Rapid Recovery Core Console 中，要暂停所有计算机的保护，请单击左侧导航区域中的“受保护机器”下拉菜单，然后执行以下操作：
 - a 选择**暂停保护**。
此时将显示“暂停保护”对话框。
 - b 使用下列所述的选项之一选择相应的设置，然后单击**确定**。
 - 如果要暂停保护直至明确恢复，请选择**暂停直至恢复**。
 - 如果要在指定期间暂停保护，请选择**暂停时间**，然后在“天”、“小时”和“分钟”控件中输入或选择适当的暂停时间（视情况而定）。
- 2 要恢复所有计算机的保护，请执行以下操作：
 - a 选择**恢复保护**。
此时将显示“恢复保护”对话框。
 - b 在“恢复保护”对话框中，选择**是**。
随即关闭“恢复保护”对话框，并恢复所有机器的保护。
- 3 要暂停对单台机器的保护，则在左侧导航区域中，单击您想要影响的机器右侧的下拉菜单，然后执行以下操作：
 - a 选择**暂停保护**。
此时将显示“暂停保护”对话框。
 - b 使用下列所述的选项之一选择相应的设置，然后单击**确定**。
 - 如果要暂停保护直至明确恢复，请选择**暂停直至恢复**。
 - 如果要在指定期间暂停保护，请选择**暂停时间**，然后在“天”、“小时”和“分钟”控件中输入或选择适当的暂停时间（视情况而定）。
- 4 要恢复单台机器的保护，请执行以下操作：
 - a 选择**恢复保护**。
此时将显示“恢复保护”对话框。
 - b 在“恢复保护”对话框中，选择**是**。

随即关闭“恢复保护”对话框，并恢复所选机器的保护。

5 要从机器页面暂停单台机器的保护，请导航到要影响的机器。

此时将显示所选机器的“摘要”页面。

a 在页面顶部单击**暂停**。

此时将显示“暂停保护”对话框。

b 使用下列所述的选项之一选择相应的设置，然后单击**确定**。

- 如果要暂停保护直至明确恢复，请选择**暂停直至恢复**。
- 如果要在指定期间暂停保护，请选择**暂停时间**，然后在“天”、“小时”和“分钟”控件中输入或选择适当的暂停时间（视情况而定）。

6 如果要恢复保护，请执行以下操作：

a 在页面顶部单击**恢复**。

b 在“恢复保护”对话框中，单击**是**。

随即关闭“恢复保护”对话框，并恢复对所选机器的保护。

管理受保护机器

本节介绍如何查看、配置和管理 Rapid Recovery 环境中的受保护机器。

关于管理受保护机器

可以用于管理受保护机器的任务被细分为几个类别。

- 您可以使用主题 Rapid Recovery 中所述的选项在 [Rapid Recovery Core](#) 中查看受保护机器。
- 您可以配置机器设置、访问系统信息或配置某台机器事件的通知。有关更多信息，请参阅[配置机器设置](#)。
- 您可以访问受保护机器的诊断。有关更多信息，请参阅[下载并查看受保护计算机的日志文件](#)。
- 您可以移除机器的保护，取消当前操作或查看受保护机器的许可证信息。有关更多信息，请参阅[管理机器](#)。
- 您可以查看和管理保存到 Core 的数据。有关更多信息，请参阅[管理快照和恢复点](#)。

查看受保护机器

从 Rapid Recovery Core Console 上的**主页**页面上，当查看摘要表视图时，您可以在“受保护机器”窗格中看到任何受 Core 保护的机器的摘要信息。

① 注：软件代理将代表用户采取特定行动。受保护机器有时被称为代理程序，因为它们运行 **Rapid Recovery Agent** 软件以方便在 **Rapid Recovery Core** 上执行数据备份和复制。

您可以查看每台机器的状态、显示名称，使用的存储库，上次快照的日期和时间，机器存储库存在的恢复点数量以及快照使用的存储库存储空间量。

要管理任何受保护机器的各个方面，首先导航到希望查看、配置或管理的机器。从“主页”页面上，有三种方式导航到受保护机器：

- 可以从“受保护机器”窗格中单击任何受保护机器的 IP 地址或显示名称。这会将您转到所选受保护机器的“摘要”页面。
- 在左侧导航区域中，您可以单击**受保护机器**菜单的标题。此时将显示 Protected Machines（受保护机器）页面。在“受保护机器”页面上，您可以查看有关每台机器的摘要信息。有关本页面的详细说明，请参阅[查看受保护机器的摘要信息](#)。
- 在左侧导航区域的“受保护机器”菜单下，您可以单击任何受保护机器的 IP 地址或显示名称。这会将您转到所选受保护机器的“摘要”页面。有关本页面的详细说明，请参阅[查看受保护机器的摘要信息](#)。

查看群集摘要信息

要查看关于群集的摘要信息，包括与群集的关联 Quorum 相关的信息，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的“受保护机器”下，单击您要查看的群集。
将显示机器的“摘要”页面。
- 2 在“摘要”页面上，可以查看群集名称、群集类型、仲裁类型（如果适用）以及仲裁路径（如果适用）等信息。此页面还会显示关于此群集中卷的概览信息，包括大小和保护计划。如果适用，也可以查看不同群集的 SQL Server 或 Exchange Server 信息。
- 3 要查看最新的信息，请单击刷新。

有关查看群集中个别机器或节点的摘要和状态信息的信息，请参阅[查看受保护机器](#)。

配置机器设置

在 Rapid Recovery 中添加要保护机器后，您可以轻松查看和修改管理该受保护机器行为的设置。当您修改特定机器设置时，这些设置会取代在 Core 级别设置的行为。

您可以在 Rapid Recovery Core Console 中查看和配置以下机器设置：

- **General（常规）**。常规机器配置设置包括显示名称、主机名、端口、加密密钥和存储库。有关为机器配置常规设置的信息，请参阅[查看和修改受保护机器设置](#)。
- **Nightly jobs（每夜作业）**。为特定受保护机器显示的 Core 每夜作业设置的子集允许您取代在 Core 级别上的每夜作业设置。这包括汇总，它可让您管理保留策略。根据受保护机器的类型，某些设置可能会有所不同。
- **Transfer settings（传输设置）**。特定于管理所选受保护机器数据传输过程的设置。有关受这些设置影响的数据传输类型的信息，请参阅[关于修改传输设置](#)。
- **Excluded Writers（排除的写入程序）**。这些设置允许您排除写入程序。这些设置是特定于机器的。写入程序是 Microsoft 发布的特定 API，允许其他软件组件参与使用 Microsoft 卷影服务 (VSS)。参与卷快照的 Rapid Recovery 中的每个写入程序都会列在 Excluded Writers（排除的写入程序）设置中。如果写入程序正在干扰或妨碍成功备份传输，则可以逐个禁用这些写入程序。除非您由 Dell 支持代表指导，否则 Dell 建议不要动这些设置。
- **License details（许可证详细信息）**。这些是特定的受保护机器的许可证的详细信息。这些设置报告从 Core 和 Dell Data Protection | Rapid Recovery 许可证门户中的信息。这些设置是只读的。要更改这些设置，请更新 Core 和许可证门户之间您的许可证信息。请参阅您的许可证管理员的详细信息。有关更多信息，请参阅 *Dell Data Protection | Rapid Recovery 许可证门户 User Guide*（Dell 数据保护 | 《Rapid Recovery 许可证门户用户指南》）。

查看或更改机器级设置、排除的写入程序和许可证的详细信息中的过程通常相同。有关更多信息，请参阅[查看和修改受保护机器设置](#)。

修改机器每夜作业的过程是不同的。有关为机器配置每夜作业设置的信息，请参阅[自定义受保护机器的每夜作业](#)。

在某些情况下，您可能想要为受保护机器调整数据传输速率。有关更多信息，请参阅[关于修改传输设置](#)。

查看和修改受保护机器设置

机器设置有助于确定受 Core 保护的机器的行为。当您修改特定机器的设置时，这些设置会取代在 Core 级别设置的行为。

要查看和修改常规设置、传输设置、排除的编写器设置以及受保护机器的许可设置，请完成以下过程中的步骤。

① | 注：要查看和修改每夜作业设置，请参阅[自定义受保护机器的每夜作业](#)。

此任务也是[修改群集节点设置](#)中的一个步骤。

- 1 在 Rapid Recovery Core Console 中的“受保护机器”菜单下方，单击您想查看或修改配置设置的机器的 IP 地址或机器名称。
此时将显示所选机器的摘要页面。
- 2 单击设置菜单。
此时将显示设置页面，其中显示所选机器的设置。（可选）要从页面上的任意位置显示设置类别，请单击页面左侧相应的超链接。

当您单击想要更改的设置时，该设置会变为可编辑的文本字段或下拉菜单。

对于每个设置，当对您所做的更改满意后，单击  以保存更改并退出编辑模式，或单击  以退出编辑模式而不保存。

- 3 要修改受保护机器的常规设置，请单击相应的设置，然后根据下表中的说明输入配置信息。

表. 69: 受保护机器的常规设置

文本框	说明
显示名称	输入机器的显示名称。 这是显示在 Rapid Recovery Core Console 中的受保护机器的名称。最多可输入 64 个字符。默认情况下，该名称是该机器的主机名。如果需要，可以将该名称更改为更易使用的名称。请勿使用 禁止字符 或 禁止短语。
主机名	输入机器的主机名。
端口	输入机器的端口号。 Rapid Recovery Core 服务使用此端口与该机器进行通信。默认端口号为 8006。
加密密钥	如果希望将已为此 Rapid Recovery Core 定义的加密密钥应用到此受保护机器上每个卷的数据，您可以在这里指定加密密钥。密钥必须解锁。如果不存在加密密钥，您可以添加加密密钥。有关管理加密密钥的更多信息，请参阅管理加密密钥。 如果本受保护机器上的卷经过加密，您可以更改到其他加密密钥。或者，您可以从加密密钥下拉菜单中选择（无）以取消关联加密密钥。 注: 应用加密密钥、更改加密密钥或取消关联受保护机器的加密密钥后，Rapid Recovery 将在下次计划或强制快照时制作新的基本映像。
存储库	选择一个存储库以存储恢复点。 显示 Rapid Recovery Core 上配置的用于存储此机器中的数据的存储库。 存储库卷可以位于本地（位于连接到 Core 服务器的存储上），也可以位于 CIFS 共享位置的卷上。 注: 只有当不存在恢复点或以前的存储库丢失时，才可以更改此页面上的存储库设置。
4	要修改受保护机器的每夜作业设置，请参阅 自定义受保护机器的每夜作业 。
5	要修改受保护的 Exchange Server 的 Exchange 设置，请在“Exchange Server 设置”部分中，单击启用自动可安装性检查并执行以下操作： - 要启用自动可安装性检查，请选中复选框，然后单击 。 - 要禁用自动可安装性检查，请清除复选框，然后单击 。 有关自动可安装性检查的更多信息，请参阅关于 Exchange 数据库可安装性检查。
6	要修改受保护机器的传输设置，请单击相应的设置，然后根据下表中的说明输入配置信息。 注: 有关传输设置的概念信息，请参阅关于修改传输设置。

表. 70: 受保护机器的传输设置

文本框	说明
 （还原默认值）	此控件可将所有传输设置还原为系统默认设置。
优先级	设置受保护机器之间的传输优先级。允许您相对于其他受保护机器分配优先级。选择 1 至 10 之间的数字，其中 1 代表最高优先级。默认设置指定的优先级为 5。 注: 优先级将应用于队列中的传输。

文本框	说明
最大并发数据流	对于 DVM 存储库中受保护的机器，设置发送至 Core 并由每台受保护机器并行受处理的最大 TCP 链路数目。 注: Dell 建议将此值设置为 8。如果发生数据包丢失，则尝试增加此设置的值。
最大并发写入数	设置每个受保护机器连接的最大同时磁盘写操作数目。 注: Dell 建议将此值设置为您为“最大并发数据流”选择的值。如果发生数据包丢失，则将此值设置为稍小的值。例如，如果“最大并发数据流”设为 8，则将此选项设为 7。
使用 Core 默认最大重试次数	选择此选项时，如果某些操作未能完成，则使用各受保护机器的默认重试次数。
最大分段大小	指定计算机在单个 TCP 分段中可收到的最大数据量（以字节为单位）。默认设置为 4194304。请勿更改此设置的默认值，除非 Dell Support 代表指示您这样做。
最大传输队列深度	指定可以并行发送的命令数。默认设置为 64。 如果您的系统执行大量并发输入/输出操作，则可将此选项调整至较高的数字。
每数据流的等待读取数	指定将在后端存储的排队读取操作数。此设置有助于控制受保护机器排队。默认设置为 0。
传输数据服务器端口	设置传输端口。默认设置为 8009。
传输超时	指定允许数据包处于静态而不进行传输的时间长度（分钟数和秒数）。
快照超时	指定等待创建快照的最长时间（分钟数和秒数）。
快照清理超时	以分钟和秒为单位指定删除受保护机器上的 VSS 快照的过程的最长时间。
网络读取超时	指定等待读取连接的最长时间（分钟数和秒数）。如果在该段时间内无法执行网络读取，则会重试此操作。
网络写入超时	指定等待写入连接的最长时间（以秒为单位）。如果在该段时间内无法执行网络写入，则会重试此操作。

7 要修改排除的编写器的设置，请单击相应的设置，然后根据下表中的说明输入配置信息。

表. 71: 受保护机器的排除的编写器设置

文本框	说明
排除的编写器	选择要排除的编写器。由于列表中显示的编写器特定于您正在配置的机器，因此可能不会看到列表中的所有编写器。您可能看到的一些编写器包括： - ASR 编写器 - COM+ REGDB 编写器 - 性能计数器编写器 - 注册表编写器 - 卷影副本优化编写器 - SQL Server 编写器 - 系统编写器 - 任务计划程序编写器 - VSS 元数据存储编写器 - WMI 编写器

8 受保护机器的许可证详细信息是只读的。下表介绍了许可证详细信息。

表. 72: 受保护机器的许可证详细信息

文本框	说明
过期日期	表示所选受保护机器的许可证的过期日期。
许可证状态	表示所选受保护机器的许可证的当前状态。
许可证类型	表示所选受保护机器的许可证的类型。
代理类型	指明当前受保护机器是物理还是虚拟代理。

更改 Hyper-V 主机或节点的设置

此程序适用于使用 Rapid Recovery Rapid Snap for Virtual（无代理保护）的 Hyper-V 主机或节点来保护虚拟机 (VM)。

Hyper-V 主机使用 Rapid Snap for Virtual（无代理保护）保护左侧导航区域中由主机图标指示的虚拟机  受无代理保护的具有虚拟机的 Hyper-V 主机的设置与典型受保护机器不同。对主机设置所做的更改适用于该主机上的虚拟机。

- 1 在 Core 控制台中，在左侧导航区域中的受保护机器下，单击您想要更改其设置的 Hyper-V 主机。
此时会为主机打开 **Summary（摘要）** 页面。
- 2 在主机的菜单栏中，单击 **Settings（设置）**。
此时将会打开 **Settings（设置）** 页面。
- 3 在 **General（常规）** 下，单击您想要更改的设置。
您所选的设置将可编辑、作为文本字段或下拉菜单。
- 4 根据下表中的说明输入配置信息。

表. 73: General（常规）设置的信息

文本框	说明
显示名称	在 Rapid Recovery Core Console 中显示的受保护机器的名称。您可以输入至多 64 个字符。默认情况下，这是机器的主机名。如果需要，您可以将显示名称更改为用户友好名称。请勿使用 禁止字符 或 禁止短语 。
主机名	受保护机器的名称，如其在机器元数据中所示。

 **注:** 请勿更改此设置，如果这样做，则可能会中断受保护机器和 Core 之间的连接。

- 5 在 **Transfer Queue（传输队列）** 下，要更改一次可能出现在主机上的传输作业数，请单击设置 **Maximum concurrent transfers（最大并发传输数）**。

 **注:** 为了获得最佳性能，建议将 Hyper-V 主机或节点的最大并发传输数设置为 1，这是默认设置。

- 6 在 **Nightly Jobs（每夜作业）** 下，要更改可用每夜作业的设置，请单击 **Change（更改）**。
此时会显示 **Nightly Jobs（每夜作业）**。
- 7 根据下表中的说明输入配置信息。

表. 74: Nightly Jobs（每夜作业）设置的信息

文本框	说明
Clear orphaned registry keys on protected Hyper-V host（清除受保护	在数据传输期间因连接虚拟磁盘和将其断开连接所导致的从注册表中删除不必要的文件。

文本框	说明
Hyper-V 主机上孤立的注册表项)	
Check integrity of recovery points (检查恢复点的完整性)	执行为 Hyper-V 主机上的虚拟机创建的每个恢复点的完整性检查。
8 单击 确定 。	
9 在 Auto Protection (自动保护) 下，要确定当新虚拟机添加到 Hyper-V 主机时是否自动保护这些虚拟机，请单击设置 Auto protect new machines (自动保护新机器) 。	

更改 Hyper-V 受保护虚拟机的设置

此程序适用于使用 Rapid Recovery Rapid Snap for Virtual (无代理保护) 进行保护的 Hyper-V 虚拟机 (VM)。

受 Rapid Snap for Virtual (无代理保护) 保护的 Hyper-V 虚拟机在左侧导航区域通过主机图标  标示出来。Hyper-V 无代理虚拟机的设置与典型的受保护机器相同，**设置**页面底部的 Hyper-V 部分除外。以下任务仅提供 **Hyper-V** 部分设置的说明。对于所有其他受保护机器设置，请参阅[查看和修改受保护机器设置](#)。

- 1 在 Core Console 上，在左侧导航区域的**受保护机器**下，单击要更改其设置的 Hyper-V 虚拟机。
此时，该虚拟机的**摘要**页面会打开。
- 2 在该主机的菜单栏上，单击**设置**。
此时，**设置**页面会打开。
- 3 在左侧列表中，单击 **Hyper-V**。
您选择的设置将变为可编辑，采用文本字段或下拉菜单形式。
- 4 在 **Hyper-V** 下，单击**快照配置**。
您选择的设置将变为可编辑，采用下拉菜单形式。
- 5 从该下拉菜单中，选择下表中所述的选项之一。

表. 75: Hyper-V 设置信息

文本框	说明
尝试在传输过程中先创建 VSS 快照，如果失败，请创建一个检查点	如果 VSS 快照成功，恢复点将处于应用程序一致状态。如果 VSS 快照失败并创建了检查点，恢复点将处于崩溃一致状态。
在传输过程中不创建 VSS 快照	生成处于崩溃一致状态的恢复点。
在传输过程中仅使用 VSS 快照。如果 VSS 快照创建失败，整个传输将失败	仅生成应用程序一致恢复点。如果 VSS 快照失败，不会生成任何恢复点。

更改 VMware 受保护虚拟机的 vSphere 设置

此程序适用于使用 Rapid Recovery Rapid Snap for Virtual (无代理保护) 进行保护的 VMware ESXi 或 Workstation 虚拟机 (VM)。

受无代理保护的 VMware 虚拟机的设置包括用于典型受保护机器的相同设置，但有一个例外。**设置**页面的 **vSphere** 部分包括只适用于受无代理保护的 VMware 虚拟机的设置。以下任务仅提供**设置**页面的 **vSphere** 部分的说明。对于所有其他受保护机器设置，请参阅[查看和修改受保护机器设置](#)。

- 1 在 Core Console 上左侧导航区域中的“受保护机器”下，单击要更改其设置的 Hyper-V 主机。
此时，该主机的**摘要**页面会打开。
- 2 在该主机的菜单栏上，单击**设置**。
此时，**设置**页面会打开。
- 3 在左侧列表中，单击 **vSphere**。
您选择的设置将变为可编辑，采用文本字段或下拉菜单形式。
- 4 在 **vSphere** 下，单击想要更改的设置。
您选择的设置将变为可编辑，采用文本字段或下拉菜单形式。

5 根据下表中的说明输入配置信息。

表. 76: vSphere 设置信息

文本框	说明
允许 Rapid Recovery 删除用户创建的 VMware	默认设置为“否”。
允许传输已用容量无效的卷	默认设置为“是”。
允许停顿的快照	默认设置为“是”。

关于修改传输设置

在 Rapid Recovery 中，可以修改用于管理受保护机器的数据传输流程的设置。本部分介绍的传输设置是受保护机器级设置。要影响 Core 级别的传输，请参阅 [修改传输队列设置](#)。

Rapid Recovery 支持 Windows 8 和 Windows Server 2012 的正常传输（基本和增量），以及还原、裸机还原和虚拟机导出。

Rapid Recovery 中有三种传输类型：

- **快照。** 备份受保护机器上的数据。提供两类快照：所有受保护数据的基本映像，以及自上一次快照后更新数据的增量快照。这类传输会创建恢复点，存储在与 Core 相关联的存储库中。要了解更多信息，请参阅 [管理快照和恢复点](#)。
- **虚拟机导出。** 从恢复点创建虚拟机 (VM)，包含受保护机器备份中的所有数据，以及操作系统和驱动程序和相关数据，以确保虚拟机可引导。要了解更多信息，请参阅 [VM 导出](#)。
- **还原。** 将备份信息还原至受保护的机器。要了解更多信息，请参阅 [关于从恢复点还原卷](#)。

① | 注：使用 EFI 系统分区还原 Windows 系统过程中，总是重新写入整个卷。

Rapid Recovery 中的数据传输涉及通过从受保护机器到 Core 的网络传输一定量的数据。对于复制，还会从原始或源 Core 传输到目标 Core。

可以通过某些性能选项设置为您的系统优化数据传输。在备份受保护机器、执行 VM 导出或执行还原的过程中，这些设置控制数据带宽使用量。以下因素会影响数据传输性能：

- 并发代理数据传输数目
- 并发数据流数目
- 磁盘上的数据更改量
- 可用网络带宽
- 存储库磁盘子系统性能
- 可用于数据缓冲的内存容量

您可以调节性能选项以便为业务需求提供支持，并根据您的环境调整性能。要了解更多信息，请参阅 [限制传输速度](#)。

限制传输速度

当通过网络在受保护服务器和 Core 之间传输备份数据或复制的恢复点时，您可以有意降低传输速度。此过程称为限制。

限制传输速度时，实际上是在限制专用于从 Rapid Recovery 执行文件传输的网络带宽量。例如，当设置复制时，限制可以降低从之前的恢复点传输到复制的 Core 这一操作占用所有网络带宽的可能性。

⚠ | 小心：并不始终需要或推荐限制传输速度。提供此信息是为了方便您深入了解 Rapid Recovery 环境中性能问题的潜在解决方案。例如，有时，限制或许能够解决与由于传输受保护或复制的 Core 的大量数据而反复发生的传输故障或网络降速相关的问题。

确定最佳限制方法涉及多种因素。受保护机器的类型是关键因素。例如，繁忙的 Microsoft Exchange 服务器的更改率高于鲜少使用的传统 Web 服务器。

受保护机器上的存储卷的输入和输出功能也可能导致效率提高或降低。

您的网络速度是另一个关键因素，存在许多变数。现有的主干网（例如，1 GbE 与 10 GbE）、体系结构、配置、NIC 组合的蓄意使用甚至所使用的电缆的类型均会影响网络传输速度。如果您的环境中有一个较慢的广域网，并且传输作业在备份或复制时失败，请考虑使用下面其中一些设置限制传输速度。

归根结底，网络限制的过程涉及试验和错误。Dell 建议您调整和测试您的传输设置，并定期返回查看这些设置，以确保您的设置持续满足您的需求。

调整传输速度这一操作应在单台机器上完成。在 Core Console 中，导航到特定机器，选择“设置”并调整传输速度。有关查看和更改这些设置的具体信息，请参阅[查看和修改受保护机器设置](#)。该主题还包括用于限制传输的每个设置的说明。这些说明可能有助于确定应首先尝试哪些设置。

下表中介绍了限制传输速度涉及的四大主要设置：

表. 77: 用于限制传输速度的受保护机器设置

机器级别设置	默认设置	建议的限制设置
最大并发数据流	8	4
最大并发写入数	8	4
最大分段大小	4194304	2097152
每数据流的等待读取数	0	从 24 开始

Dell 建议在更改“每个流未完成的读取”的默认设置之前先调整和测试其他设置，除非 Dell Support 代表另有指示。当优化和测试此设置时，请从值 24 开始。

当您指定受保护机器传输参数限制时，这些限制将应用于每个作业。如果两个传输作业同时发生或重叠，则将占用两倍的带宽。如果网络覆盖中涉及四个传输作业，则将占用四倍的带宽；以此类推。

自定义受保护机器的每夜作业

每夜作业可在相应 Configuration（配置）选项卡中以 Core 级别和机器级别进行配置。以 Core 级别设置每夜作业设置时，更改应用至所有受 Core 保护的相关机器。以机器级别对每夜作业所做的更改取代以 Core 级别所做的更改，仅适用于指定的机器。

要获取所有每夜作业的列表，包括每项说明和范围，请参阅主题 [了解每夜作业](#)。

请完成以下程序中的这些步骤，以对单个受保护机器的每夜作业进行更改。

- 1 在 Rapid Recovery Core 控制台中，在 Protected Machines（受保护机器）菜单下，单击要自定义每夜作业的机器的 IP 地址或机器名。
随即显示所选机器的 **Summary（摘要）** 页面。
- 2 单击 **Settings（设置）** 菜单。
随即显示 **Settings（设置）** 页面，显示所选机器的配置设置。
- 3 或者，也可单击 **Nightly Jobs（每夜作业）** 链接，以在 Settings（设置）页面中向下滚动，以查看每夜作业设置。
- 4 在 Nightly Jobs（每夜作业）标题下，单击  **Change（更改）**。
此时将显示 **Nightly Jobs（每夜作业）** 对话框。

-  **注：**要了解 Rollup（前滚）设置的相关信息，包括设置自定义保留策略，请参阅 [自定义受保护机器的保留策略设置](#)。
- 5 在 **Nightly Jobs（每夜作业）** 对话框中，选择要包含每夜运行的作业，或清除要为此机器忽略的选项。

 **注：**选项视机器而异。例如，使用 **Exchange Server** 的受保护机器可能包括检查 **Exchange** 数据库校验和和截断 **Exchange** 日志。
 - 6 单击**确定**。

① **注:** 该流程的结果仅应用至所选受保护的机器。要应用至其他机器，请为要自定义的每个机器重复该流程。要为 Core 保护的所有机器更改每夜作业设置。请参阅 [配置 Core 的每夜作业](#)。

查看受保护机器的系统信息

Rapid Recovery Core Console 让您可以轻松访问有关 Core 上受保护机器的系统信息。

常规窗格包括有关 Core 机器和环境的常规信息。卷窗格列出有关 Core 机器上的存储卷的信息。Replay 引擎连接窗格显示有关所有受保护机器上的卷的信息。

要查看受保护机器的详细系统信息，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console，从左侧导航区域中的“受保护机器”菜单中，单击受保护机器的名称。此时将显示所选受保护机器的摘要页面。
- 2 在摘要页面上，在摘要窗格底部单击  系统信息。
- 3 在系统信息页面上，您可以查看有关所选受保护机器的以下详细信息。
 - **系统信息。** 这包括主机名称、操作系统版本、操作系统体系结构、内存（物理）、显示名称、完全限定域名、高速缓存元数据位置、主要高速缓存位置、次要高速缓存位置和虚拟机类型（如果适用）。
 - **卷。** 这包括卷名称、设备 ID、文件系统、格式化的容量、已使用容量和安装点。
 - **处理器。** 这包括体系结构和内核数量。
 - **网络适配器。** 这包括适配器类型和速度。
 - **IP 地址。** 这包括 IP 地址和系列。

管理机器

本部分介绍管理机器时可以执行的各种任务。主题包括：

- [移除机器](#)
- [从保护范围中移除群集](#)
- [查看机器的许可证信息](#)
- [下载并查看受保护计算机的日志文件](#)
- [将受保护群集节点转换为受保护机器](#)

移除机器

当在 Rapid Recovery Core 上从保护范围中移除某台机器时，您有两种选择：您可以保留恢复点到 RR Core，或者移除恢复点。如果保留恢复点，您将拥有被称为“仅恢复点”的机器。使用移除当前保护机器的恢复点，您可以在未来继续还原机器，但是仅可还原至保存恢复点捕捉的状态。

如果移除恢复点，本操作将删除之前的 Rapid Recovery Core 受保护机器的任何快照数据。

 **小心:** 如果删除恢复点，您将无法恢复该机器的数据。

要从 Rapid Recovery 环境的保护范围中移除机器，请完成以下过程中的步骤。

- 1 从 Rapid Recovery Core Console，在左侧导航窗格的“受保护机器”下方，单击要移除的机器。
- 2 在相关机器的“摘要”页面上，单击**移除机器**。
- 3 在对话框中，如果您还想要从存储库中移除此机器的所有恢复点，请选择**移除恢复点**。
- 4 要确认您选择移除机器，请单击**是**。

Rapid Recovery 从保护范围中移除机器，并取消该机器的所有活动任务。

从保护范围中移除群集

要从保护范围中移除群集，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的“受保护机器”下，单击您要删除的群集。
- 2 在群集的“摘要”页面上，单击**移除群集**。
- 3 （可选）在此对话框中，要从存储库中删除此群集的所有当前存储的恢复点，请选择**移除恢复点**。
- 4 在此对话框中，单击**是**进行确认。

从保护范围中移除群集节点

要从保护范围中移除群集节点，请完成以下过程中的步骤。

如果要仅从群集中删除节点，请参阅[将受保护群集节点转换为受保护机器](#)。

- 1 在 Rapid Recovery Core Console 的“受保护机器”下，单击您要删除的群集。
- 2 在节点的“摘要”页面上，单击**删除机器**。
此时将显示“删除节点”对话框。
- 3 （可选）在此对话框中，要从存储库中删除此群集的所有当前存储的恢复点，请选择**移除恢复点**。
- 4 在此对话框中，单击**是**进行确认。

从保护范围中移除群集的所有节点

要从保护范围中移除群集的所有节点，请完成以下过程中的步骤。

 **小心:** 如果删除所有群集节点，则群集也将删除。

- 1 在 Rapid Recovery Core Console 的“受保护机器”下，单击您要删除节点的群集。
- 2 在群集的“摘要”页面上，单击**受保护节点**。
- 3 在“受保护节点”页面上，选择所有节点。
- 4 单击**移除机器**下拉菜单，然后选择下表中所述的选项之一。

表. 78: 移除节点选项

选项	说明
移除并保留恢复点	保留当前为此群集存储的所有恢复点。
移除恢复点	从存储库中移除当前为此群集存储的所有恢复点。

- 5 在“删除节点”对话框中，单击**是**进行确认。

查看机器的许可证信息

您可以查看受保护计算机上安装的 Rapid Recovery Agent 软件的当前许可证状态信息。

- 1 在 Rapid Recovery Core Console 中，单击“受保护计算机”下要进行修改的计算机。
此时将显示所选计算机的**摘要**页面。
- 2 单击**设置**菜单。
此时将显示**设置**页面，其中显示所选计算机的配置设置。
- 3 单击**许可**链接，向下滚动“设置”页面以查看特定计算机的许可设置。
将显示“状态”屏幕，并显示关于产品许可的详细信息。

下载并查看受保护计算机的日志文件

如果您的受保护计算机遇到任何错误或问题，您可以下载计算机日志进行查看或与您的 Dell Support 代表联系。

- 1 在 Core Console 的左侧导航区域中的“受保护计算机”菜单下，单击箭头以展开受保护计算机的上下文相关菜单。向下滚动到**更多**，展开该菜单，然后选择  **Agent 日志**。
此时将显示**下载 Agent 日志**页面。
- 2 在**下载 Agent 日志**页面上，单击  **单击此处开始下载**。
- 3 在**正在打开 AgentAppRecovery.log**对话框中，执行以下操作之一：
 - 要打开日志文件，选择**打开方式**，然后选择应用程序（如记事本）来查看基于文本的日志文件，最后单击**确定**。
AgentAppRecovery.log 文件将用选定的应用程序打开。
 - 要将文件保存在本地，选择**保存文件**，然后单击**确定**。
AgentAppRecovery.log 文件将保存到您的“下载”文件夹。它可以使用任何文本编辑器打开。

相关链接

[下载并查看 Core 日志文件](#)

将受保护群集节点转换为受保护机器

在 Rapid Recovery 中，可以将受保护群集节点转换为受保护机器，以便 Core 继续对其进行管理，但它不再是群集的一部分。例如，在需要从群集中移除群集节点，但仍对其进行保护时，此功能便非常有用。

- 1 在 Rapid Recovery Core Console 中，导航至包含要转换的机器的群集，然后单击**受保护节点**。
- 2 在**受保护节点**页面上，从要转换的特定节点中单击“操作”下拉菜单，然后选择**转换为代理程序**。
- 3 要将机器重新添加至群集，请选择该机器，然后从“摘要”页面的“操作”菜单中，选择**转换为群集节点**，然后单击**是**以确认操作。

了解自定义组

Rapid Recovery Core Console 将在左侧导航区域中显示“受保护机器”菜单。这包括添加到您的 Rapid Recovery Core 上保护中的所有机器或服务器群集。在此下方，可能会显示其他菜单，具体取决于您是否在 Core 中包括这些对象。通过相同的方式，您可以创建自定义组，其显示为左侧导航区域中的最后一个菜单类型。

自定义组的主要优势在于其能够将 Core 对象聚集到一个逻辑容器中。这可以帮助您根据特定目的（例如，按组织、成本中心、部门、地理区域等）来组织和管理 Core 对象。

创建组的行为始终会向新的自定义组添加一个组成员（例如，受保护机器或服务器群集、复制机器或仅有恢复点的机器）。在您创建组时，添加的对象由您的原点确定。在理想的情况下，接着可以将其他成员添加到该组。此后，您可以执行应用于该自定义组的所有成员的组操作，如**执行组操作**中所述。

自定义组可以包括受保护机器、服务器群集、复制机器和仅有恢复点的机器。服务器群集的行为方式与受保护机器相同，不过服务器群集和其节点相当于单个实体。如果尝试将服务器群集中的节点添加到组，则会添加整个群集。

自定义组可能包含类似或不同的成员。对于包含类似成员的组，所有组操作将应用于组的所有成员。例如，如果强制创建受保护机器的自定义组的快照，则将备份每个机器。对于包含不同成员的组（例如，受保护机器和被复制的机器），如果应用强制复制等组操作，此操作将仅应用于被复制的机器。

您可以创建一个或多个组。单个受保护机器或复制机器可以包括在一个或多个组中。这样，您可以采用所选的任何方式分组 Core 上的机器，且可以对该特定组执行操作。

每个自定义组都会使用您指定的标签显示在左侧导航区域中，包含标准受保护机器的组会在自定义组中第一个显示；被复制的机器会显示在受保护机器下方（如果适用）。如果存在仅有恢复点的机器，这些机器会列在被复制的机器下方。

在左侧导航区域中，在 Core 上受保护的對象会各自显示在自己的菜单中。在这些菜单中，自定义组显示在最后面。

将机器包括在组中不会将其从原始位置移除。例如，如果有三台受保护机器：Agent1、Agent2 和 Agent3，且将 Agent1 添加到 CustomGroup1，则 Agent1 将显示在两个位置中。

有关更多信息，请参阅以下主题：

- [修改自定义组名称](#)
- [移除自定义组](#)
- [执行组操作](#)
- [在一个页面中查看自定义组的所有机器](#)

创建自定义组

在受保护机器或复制菜单中的任何机器名称上滚动光标时，将显示一个箭头以打开下拉菜单。在此菜单中，您可以创制自定义标签。

要创建自定义组，请使用以下过程。

- 1 导航至 Rapid Recovery Core Console。
- 2 从受保护机器、被复制的机器或仅有恢复点的机器菜单中，执行以下操作：
 - a 将光标放置在菜单中的机器上。
 - b 单击该机器的下拉菜单。
 - c 向下滚动并选择**标记为**，然后单击**新建标签**。此时会显示**创建标签**对话框。
- 3 在**名称**字段中，为您的自定义组输入适当的标签。
请使用描述性名称以传达组的用途。例如，要按部门为受保护机器、被复制的机器和仅有恢复点的机器分组，请键入 Accounting Department。您稍后可以重命名组。

① | 注：标签必须是 50 个或以下的字符。您可以在单词之间包括一个空格。您必须为自定义组提供标签。

- 4 对标签名称满意后，单击**确定**。
该对话框会关闭，自定义组在左侧导航区域中显示为最后一个元素。
- 5 （可选）您可以向此组添加其他受保护机器、被复制的机器或仅有恢复点的机器。导航至相应菜单中的机器名称，单击它的下拉菜单，向下滚动并选择**标记为**，然后单击自定义组的名称。
此时您便可以对该组执行组操作。有关详情，请参阅[执行组操作](#)。

修改自定义组名称

修改自定义组名称时，只有标签会更改。机器名称保持不变。

要修改自定义组名称，请使用以下过程。

- 1 导航至 Rapid Recovery Core Console。
- 2 在“受保护机器”菜单中，在要修改的自定义组上滚动光标。
- 3 单击该组的下拉菜单，然后单击**编辑**。
会显示**编辑标签**对话框，在该对话框内可编辑自定义组的名称。
- 4 在**名称**字段中，更新文本，或为您的自定义组删除现有标签文本并键入新的标签。
请使用描述性名称以传达组的用途。例如，要按地理区域为受保护机器、被复制的机器和仅有恢复点的机器分组，请键入 Tokyo。您稍后可以重命名组。

① | 注：标签必须是 50 个或以下的字符。您可以在单词之间包括一个空格。您必须为自定义组提供标签。

- 5 对标签名称满意后，单击**确定**。
该对话框会关闭，修改后的自定义组在左侧导航区域中显示为最后一个元素。
- 6 （可选）您可以向此组添加其他受保护机器、被复制的机器或仅有恢复点的机器。导航至相应菜单中的机器名称，单击它的下拉菜单，向下滚动并选择**标记为**，然后单击自定义组的名称。

移除自定义组

移除自定义组时，将从“受保护机器”菜单中删除该组。不会移除位于该组中的机器，且仍可以在相应的标准菜单中找到有关机器。

要移除自定义组，请使用以下过程。

- 1 导航至 Rapid Recovery Core Console。
- 2 在“受保护机器”菜单中，在要移除的自定义组上滚动光标。
- 3 单击该组的下拉菜单，然后单击**移除标签**。
此时将显示一条消息，要求确认移除该组。
- 4 确认删除自定义组。
对话框将关闭，且将从导航区域中删除自定义组。

执行组操作

您可以对 Rapid Recovery Core Console 左侧导航区域中显示的任何组执行组操作。如果组包含不同的成员（例如，被复制的机器和仅有恢复点的机器），则只会对相关组成员执行您请求的操作。

要对自定义组执行组操作，请使用以下过程。

- 1 导航至 Rapid Recovery Core Console。
- 2 在“受保护机器”菜单中，在要执行组操作的自定义组上滚动光标。
- 3 单击该组的下拉菜单，然后如下选择一项操作：
 - 要强制创建所有受保护机器的增量快照或基本映像，请视情况单击**强制快照**或**强制基本映像**。有关详情，请参阅[强制创建快照](#)。
 - 要暂停对组中所有受保护机器的保护，请单击**暂停保护**，然后指定恢复参数。有关详情，请参阅[暂停和恢复复制](#)。
 - 要恢复已暂停保护的组中所有受保护机器的保护，请单击**恢复保护**，然后确认要恢复。有关详情，请参阅[暂停和恢复复制](#)。
 - 要刷新组中所有对象的信息，请单击**刷新元数据**。
 - 要暂停此组中所有被复制的机器的复制，请在“复制”下单击**暂停**。有关详情，请参阅[暂停和恢复复制](#)。
 - 要恢复此组中已暂停复制的所有被复制的机器的复制，请在“复制”下，单击**恢复**。有关更多信息，请参阅[暂停和恢复复制](#)。
 - 要强制为此组中所有被复制的机器执行复制，请在“复制”下单击**强制**。有关详情，请参阅[强制复制](#)。
 - 要为此组中所有被复制的机器移除复制，请在“复制”下单击**移除**。有关详情，请参阅[从目标 Core 删除传入复制](#)。
 - 要从此 Core 中移除仅有恢复点的机器并放弃恢复点，请在“仅恢复点”下，单击**移除恢复点**。
 - 仅对于自定义组，要修改自定义组的标签，请选择**编辑**。有关详情，请参阅[修改自定义组名称](#)。
 - 仅对于自定义组，要从导航菜单中删除自定义组，请选择**删除标签**。有关详情，请参阅[移除自定义组](#)。

在一个页面中查看自定义组的所有机器

单击自定义组名称可转到“机器”页面，其中会列出该自定义组中的所有机器。然后，您可以从“操作”菜单中对所有机器执行某些功能，或可以从每个单独的机器中选择命令以单个执行功能。

关于保护多台计算机

您可以在使用“保护多台计算机向导”的同时添加 Rapid Recovery Core 上要保护的两台或多台 Windows 计算机。要使用 Rapid Recovery 来保护数据，您需要在 Rapid Recovery Core Console 中添加要保护的工作站和服务器的，例如 Exchange Server、SQL Server、Linux 服务器等等。

与保护单台计算机相同，同时保护多台计算机需要您在要保护的每台计算机上安装 Rapid Recovery Agent 软件。

① 注: 此规则的例外情况就是，如果是对 VMware 或 ESXi 主机上的虚拟机进行保护，那么您可以使用无代理保护。有关包括无代理保护限制在内的更多信息，请参阅[理解 Rapid Snap for Virtual](#)。

必须为受保护机器配置可实现远程安装的安全策略。

要连接到计算机，这些计算机必须已开启电源并且可以访问。

有多种方法可以将 Agent 软件同时部署到多台机器。例如：

- 您可以使用“部署 Agent 软件向导”将 Rapid Recovery Agent 软件安装到多台计算机。有关更多信息，请参阅[将 Rapid Recovery Agent 软件部署到一台或多台机器](#)。
- 您可以将 Rapid Recovery Agent 软件作为“保护多台计算机向导”的一部分进行部署。

如果选择高级配置，则保护多台计算机这一流程将包括您可以访问的可选步骤。高级选项包括存储库功能和加密。例如，您可以指定一个现有 Rapid Recovery 存储库来保存快照，或者创建一个新的存储库。您也可指定一个现有加密密钥（或添加一个新的加密密钥）以应用于保存到受保护计算机 Core 中的数据。

“保护多台机器向导”的工作流可能会因环境而略有不同。例如，如果 Rapid Recovery Agent 软件已安装在要保护的计算机上，则系统不会提示您从向导安装此软件。同样，如果存储库已存在于 Core 中，则系统不会提示您创建存储库。

保护多台计算机时，应根据您的配置，遵循相应的流程。请参阅以下用于保护多台计算机的选项：

- [保护 Active Directory 域上的多个机器](#)
- [保护 VMware vCenter/ESX\(i\) 虚拟主机中的多台机器](#)
- [手动保护多台计算机](#)

保护 Active Directory 域上的多个机器

使用此过程可同时保护 Active Directory 域上的一个或多个机器。

- 1 在 Rapid Recovery Core Console 中，单击 **Protect（保护）** 下拉菜单，然后单击 **Protect Multiple Machines（保护多个机器）**。此时会打开 Protect Multiple Machines Wizard（保护多个机器向导）。
- 2 在向导的 **Welcome（欢迎）** 页面中，选择以下选项之一：
 - 典型值
 - Advanced (show optional steps)（高级（显示可选步骤））
- 3 单击**下一步**。
- 4 在向导的 **Connection（连接）** 页面中，从 **Source（源）** 下拉列表中，选择 **Active Directory**。
- 5 按照下表中的说明输入域信息和登录凭据。

表. 79: 域信息和凭据

文本框	说明
主机	Active Directory 域的主机名或 IP 地址。
用户名	用于连接到域的用户名；例如，Administrator 或者，如果机器处于域中，则为 [域名]\Administrator。
密码	用于连接域的安全密码。

- 6 单击**下一步**。
- 7 在向导的 **Select Machines（选择机器）** 页面中，选择您想要保护的机器。
系统会自动验证您选中的每个机器。
- 8 单击**下一步**。
如果 Protect Multiple Machines Wizard（保护多个机器向导）中显示 **Protection（保护）** 页面，请跳转到步骤 11。
如果尚未将 Agent 软件部署到您想要保护的机器上，或是任何您指定的机器因其他原因而无法受到保护，则 Warnings（警告）页面上将显示所选机器。
- 9 （可选）在向导的 **Warnings（警告）** 页面上，您可以通过选择机器，然后单击在工具栏上的 **Verify（验证）**，验证任何机器。
- 10 根据需要，可在 **Warnings（警告）** 页面中，选择 **After Agent installation, restart the machines automatically（在 Agent 安装后，自动重新启动机器）**。

 **注:** Dell 建议选择此选项。您必须重新启动代理机器，才能对其提供保护。

- 11 如果状态表明该机器可供访问，请单击 **Next**（下一步）以安装 Rapid Recovery Agent 软件。
此时将会显示 **Protection**（保护）页面。
- 12 在向导的 **Protection**（保护）页面中，根据下面的说明选择相应的保护计划。
 - 如果希望使用默认保护计划，请在 Schedule Settings（计划设置）选项中选择 **Default protection (hourly snapshots of all volumes)**（默认保护（每小时为所有卷创建快照））。
 - 如果希望定义不同的保护计划，请在 Schedule Settings（计划设置）选项中选择 **Custom protection**（自定义保护）。
- 13 继续按如下所示进行配置：
 - 如果在 Protect Machine Wizard（保护机器向导）中选择了 Typical（典型）配置，请单击 **Finish**（完成）以确认您的选择，关闭向导，并保护您指定的机器。
首次为机器添加保护时，除非您指定初始暂停保护，否则在您定义计划后会将基本映像（即受保护卷中所有数据的快照）传输至 Rapid Recovery Core 上的存储库。
 - 如果在 Protect Machine Wizard（保护机器向导）中选择了 Typical（典型）配置并指定了自定义保护，请单击 **Next**（下一步），请参阅[创建自定义保护计划](#)。
 - 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置和默认保护，请单击 **Next**（下一步），然后前进到[步骤 15](#) 以查看存储库和加密选项。
 - 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置并指定了自定义保护，请单击 **Next**（下一步）以设置自定义保护计划。有关定义自定义保护计划的详情，请参阅[创建自定义保护计划](#)。
- 14 单击**下一步**。
- 15 在向导的 **Repository**（存储库）页面中，执行以下操作之一：
 - 如果您已经有了一个存储库并想要存储此机器中的数据以保护现有存储库，请执行以下操作：
 - 1 选择 **Use an existing repository**（使用现有存储库）。
 - 2 从列表选择一个现有存储库。
 - 3 单击**下一步**。

此时将显示 Encryption（加密）页面。跳至[步骤 19](#) 还可以定义加密。

- 如果您希望创建存储库，请选择 **Create a Repository**（创建存储库），然后完成以下步骤。
 - 1 在 **Repository**（存储库）中，输入下表所述信息。

表. 80: Add New Repository（添加新存储库）设置

文本框	说明
Repository Name (存储库名称)	输入存储库的名称。 默认情况下，此文本框包含词语 Repository（存储库）和一个数字，它与此 Core 的存储库数量相对应。例如，如果它是第一个存储库，默认名称为 Repository 1。请根据需要更改此名称。 存储库名称必须包含介于 1 和 40 之间的字母数字字符，包括空格。请勿使用禁止字符或禁止短语。
Concurrent Operations（并发操作数）	定义希望存储库支持的并发请求数量。默认值为 64。
注释	（可选）输入关于此存储库的描述性说明。您可以输入至多 254 个字符。例如，键入 DVM Repository 2 。

- 2 单击 **Add Storage Location**（添加存储位置）以定义存储库的特定存储位置或卷。此卷应为主存储位置。

 **小心:** 为存储库的存储位置指定根目录内的专用文件夹。请勿指定根目录位置。例如，使用 E:\Repository \，而非 E:\。如果在此步骤中创建的存储库之后被删除了，您的存储库的存储位置上的所有文件都会被删除。如果您在根目录上指定存储位置，则卷（例如，E:\）中的所有其他文件都会被删除。这可能会导致灾难性数据丢失。

此时将显示 **Add Storage Location**（添加存储位置）对话框。

- 3 单击 **Add Storage Location**（添加存储位置）以定义存储库的特定存储位置或卷。此卷应为主存储位置。
- 4 在 **Storage Location**（存储位置）区域中，指定将文件添加到存储位置的方式。您可以选择添加本地连接的存储卷（例如，直接连接的存储、存储区域网络或网络连接存储）。您还可以指定通用 Internet 文件系统 (CIFS) 共享位置上的存储卷。

- 单击 **Add file on local disk**（在本地磁盘上添加文件）以指定本地机器，然后根据下表中的说明输入信息。

表. 81: 本地磁盘设置

文本框	说明
Data Path（数据路径）	输入用于存储受保护数据的位置。 例如，键入 X:\Repository\Data。 在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。
Metadata Path（元数据路径）	输入用于存储受保护元数据的位置。 例如，键入 X:\Repository\Metadata。 在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。

- 您也可以选择 **Add file on CIFS share**（在 CIFS 共享上添加文件）指定一个网络共享位置，然后按下表所述输入相应的信息。

表. 82: CIFS 共享凭据

文本框	说明
UNC Path（UNC 路径）	输入网络共享位置的路径。 如果此位置位于根目录，请定义专用文件夹名称（例如，Repository）。 路径必须以 \\ 开始。指定路径时，只能使用字母数字字符、连字号和句点（只用于分隔主机名和域）。字母 a 至 z 区分大小写。请勿使用空格。不允许使用其他符号或标点符号。
用户名	指定用于访问网络共享位置的用户名。
密码	指定用于访问网络共享位置的密码。

- 在 **Storage Configuration**（存储配置）区域中，单击 **More Details**（详细信息），然后根据下表中的说明输入存储位置的详细信息。

表. 83: 存储配置详细信息

文本框	说明
大小	设置存储位置的大小或容量。最小大小为 1GB。默认值为 250 GB。可以从以下各项中选择： - GB - TB ① 注: 指定的大小不能超过卷的大小。 如果存储位置是使用 Windows XP 或 Windows 7 的新技术文件系统 (NTFS) 卷，则文件大小限制为 16 TB。 如果存储位置是使用 Windows 8、8.1、Windows 10 或 Windows Server 2012、2012 R2 的 NTFS 卷，文件大小限制为 256 TB。 ① 注: 要让 Rapid Recovery 验证操作系统，在目标存储位置必须安装 Windows Management Instrumentation (WMI)。
Write Caching Policy（写高速缓存策略）	写高速缓存策略控制 Windows Cache Manager 在存储库中的使用方式，并帮助调整存储库以便在不同配置下实现最佳性能。 请将其设置为以下值之一： - On（打开） - Off（关） - Sync（同步）

如果设置为默认值 On（打开），则 Windows 将控制高速缓存。这适用于 Windows 10 以及 Windows Server 2012 和更高版本。

① **注:** 将写高速缓存策略设置为 On（打开）可提高性能。如果您使用的是 **Windows Server 2008 SP2 或 Windows Server 2008 R2 SP2**，则建议的设置为 Off（关闭）。

如果设置为 Off（关闭），则 Rapid Recovery 将控制高速缓存。

如果设置为 Sync（同步），则 Windows 将控制高速缓存以及同步输入/输出。

每扇区字节数	指定希望每个扇区包含的字节数。默认值为 512。

Average Bytes per Record（每个记录的平均字节数）	指定每个记录的平均字节数。默认值为 8192。

6 单击下一步。

如果您在步骤 1 中选择了 **Advanced（高级）** 选项，此时将显示 **Encryption（加密）** 页面。

- 16 另外，在向导的 **Encryption（加密）** 页面上，要启用加密，请选择 **Enable Encryption（启用加密）**。
在 Encryption（加密）页面中将显示 Encryption key（加密密钥）字段。

① **注:** 如果启用加密，它将应用于此机器上所有受保护卷中的数据。您可以稍后从 **Rapid Recovery Core Console** 的 **Encryption Keys（加密密钥）** 页面中更改设置。有关加密的更多信息，请参阅主题 [了解加密密钥](#)。

△ **小心:** **Rapid Recovery** 在密码块链 (CBC) 模式中使用 AES 256 位加密和 256 位密钥。虽然使用加密是可选的，但是 **Dell** 强烈建议您建立加密密钥，并保护您定义的密码短语。请将密码短语保存在安全位置，因为它对于数据恢复至关重要。如果没有密码短语，将无法进行数据恢复。

- 17 如果您想使用已在此 Rapid Recovery Core 上定义的加密密钥加密这些受保护的机器，请选择 **Encrypt data using an existing Encryption key（使用现有的加密密钥加密数据）** 并从下拉菜单中选择相应的密钥。
继续执行步骤 19。
- 18 如果您想要将新加密密钥添加到 Core 并对这些受保护的机器应用该密钥，请根据下表中的说明输入信息。

表. 84: 加密密钥设置

文本框	说明
名称	输入加密密钥的名称。 加密密钥的名称必须包含介于 1 和 130 之间的字母数字字符。其中不能包含特殊字符，例如反斜杠、斜杠、管道、冒号、星号、引号、问号、左方括号或右方括号、& 符号或散列值。
说明	输入加密密钥的注释。 当从 Core Console 查看加密密钥时，此信息会显示在 Description（说明）字段中。
密码短语	输入用于控制访问的密码短语。 最佳做法是为了避免上述列出的特殊字符。 密码短语记录在安全位置。Dell 支持部门无法恢复密码短语。一旦您创建加密密钥并将其应用于一个或多个受保护的机器，则一旦该密码短语丢失，您将无法恢复数据。
确认密码短语	重新输入刚输入的密码短语。

- 19 单击 **Finish（完成）** 以保存并应用设置。
该向导将会关闭。
- 20 如果出现 **Warning（警告）** 页面，而您仍对您的选择感到满意，请再次单击 **Finish（完成）**。

如有必要，可将 Rapid Recovery Agent 软件部署到指定的机器，这些机器会添加到 Core 中并受到保护。

保护 VMware vCenter/ESX(i) 虚拟主机中的多台机器

使用此过程可同时保护 VMware vCenter/ESX(i) 虚拟主机上的一台或多台机器。

小心: 如果您使用无代理保护, Dell 建议您一次限制对不超过 200 个虚拟机进行保护。例如, 使用 **Protect Multiple Machines Wizard** (保护多台机器向导) 时请勿选择超过 200 个虚拟机。保护 200 个以上的虚拟机会降低性能。在一段时间内, Core 可无代理保护的虚拟机的数量没有限制。例如, 今天您可保护 200 个虚拟机, 明天您可保护其他 200 个虚拟机。

- 1 在 Rapid Recovery Core 控制台中, 单击 **Protect** (保护) 下拉菜单, 然后单击 **Protect Multiple Machines** (保护多台机器)。随即打开 Protect Multiple Machines Wizard (保护多台机器向导)。
- 2 在 Welcome (欢迎) 页面中, 选择以下任一选项:
 - 典型值
 - 高级 (显示可选步骤)
- 3 单击**下一步**。
- 4 在向导的 Connection (连接) 页面中, 从 **Source** (源) 下拉列表中选择 **vCenter / ESX(i)**。
- 5 按下表所述, 输入主机信息和登录凭据。

表. 85: vCenter/ESX(i) 连接设置

文本框	说明
主机	输入 VMware vCenter Server/ESX(i) 虚拟主机的名称或 IP 地址。
端口	用于连接至虚拟主机的端口。 默认设置为 443。
用户名	用于连接至虚拟主机的用户名; 例如, Administrator 或 [域名]\Administrator (如果机器在域中)。
密码	输入用于连接此虚拟主机的安全密码。

- 要使用无代理保护, 请选择 **Protect selected VMs Agentlessly** (以无代理方式保护所选虚拟机), 然后查看 [保护无 Rapid Recovery Agent 的 vCenter/ESXi 虚拟机](#)。
- 6 在 Select Machines (选择机器) 页面中, 从下拉菜单中选择以下任一选项:
 - 主机和群集
 - 虚拟机和模板
 - 7 展开机器的列表, 然后选择要保护的虚拟机。
如果 Rapid Recovery 检测到机器处于脱机状态或未安装 VMware Tools, 则会显示一条通知。
 - 8 单击**下一步**。
 - 9 在 Adjustments (调整) 页面中, 以下列格式输入每台机器的凭据: `hostname::username::password`。

注: 每行输入一台机器。

- 10 单击**下一步**。
如果 Protect Multiple Machines Wizard (保护多台机器向导) 中接下来显示 Protection (保护) 页面, 请跳至[步骤 14](#)。
如果尚未在要保护的机器中部署代理软件, 或由于其他原因导致指定的任何机器无法得到保护, 则 Warnings (警告) 页面中会显示选择的机器。
- 11 或者, 在 Warnings (警告) 页面中, 您可通过选择机器, 然后单击工具栏中的 **Verify** (验证) 以验证任何机器。
- 12 或者在 Warnings (警告) 页面中, 选择 **After Agent installation, restart the machines automatically** (安装代理后, 自动重新启动机器)。

注: Dell 建议选中此选项。您必须重新启动代理机器后, 这些机器才能受到保护。

- 13 如果状态表明该机器可通信, 请单击 **Next** (下一步) 以安装代理软件。
此时会显示 Protection (保护) 页面。
- 14 在 Protection (保护) 页面中, 如下所述, 请选择相应的保护计划。

- 要使用默认保护计划，请在 Schedule Settings（计划设置）选项中选择 **Default protection (hourly snapshots of all volumes)**（默认保护 [每小时为所有卷创建快照]）。
- 要定义不同的保护计划，请在 **Schedule Settings**（计划设置）选项中选择 Custom protection（自定义保护）。

15 继续按如下所示进行配置：

- 如果在 Protect Machine Wizard（保护机器向导）中选择了 Typical（典型）配置，则单击 **Finish**（完成）以确认您的选择，关闭向导，并保护您指定的机器。
首次为机器添加保护时，会按照您定义的计划，将基本映像（即受保护卷中的所有数据的快照）传输至 Rapid Recovery Core 上的存储库，除非您指定初始暂停保护。
- 如果选择了 Protect Machine Wizard（保护机器向导）的 Typical（典型）配置并指定了自定义保护，则单击 **Next**（下一步）以设置自定义保护计划。有关定义自定义保护计划的详情，请参阅 [创建自定义保护计划](#)。
- 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置，则单击 **Next**（下一步），然后前进到 [步骤 17](#) 以查看存储库和加密选项。
- 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置并指定了自定义保护，则单击 **Next**（下一步）以设置自定义保护计划。有关定义自定义保护计划的详情，请参阅 [创建自定义保护计划](#)。

16 单击**下一步**。

17 在 **Repository**（存储库）页面中，执行以下操作之一：

- 如果您已创建存储库并希望存储此机器中的数据以在现有存储库中提供保护，请执行以下操作：
 - 1 选择 **Use an existing repository**（使用已有存储库）。
 - 2 从列表中选择已有存储库。
 - 3 单击**下一步**。

此时显示 **Encryption**（加密）页面。跳至 [步骤 18](#) 可选择定义加密。

- 如果您希望创建存储库，请选择 **Create a Repository**（创建存储库），然后执行以下步骤。
 - 1 在 **Repository**（存储库），输入下表所述信息。

表. 86: 添加新存储库设置

文本框	说明
Repository Name (存储库名称)	输入存储库的显示名称。 默认情况下，该文本框包含文字 Repository 和一个编号，该编号与此 Core 的存储库的编号相对应。例如，如果是第一个存储库，则默认名称为 Repository 1。可根据需要更改该名称。 存储库名称必须包含 1 至 40 个字母数字字符，包括空格。请勿使用 禁止字符 或 禁止短语 。
Concurrent Operations (并发 操作数)	定义希望存储库支持的并发请求数量。默认值为 64。
注释	您也可输入该存储库的说明注释。您最多可输入 254 个字符。例如，输入 DVM Repository 2 。

2 单击 **Add Storage Location**（添加存储位置），以定义该存储库的特定存储位置或卷。该卷应为主存储位置。

 **小心：**为您的存储库在根路径内定义存储位置的专属文件夹。请勿指定根路径位置。例如，使用 **E:\Repository**，而不要使用 **E:**。如果稍后移除您在此步骤中创建的存储库，存储库的该存储位置中的所有文件将被删除。如果您在根路径定义了您的存储位置，则卷（如 **E:**）中的其他所有文件将被删除，这回导致灾难性的数据损失。

此时将显示 **Add Storage Location**（添加存储位置）对话框。

- 3 单击 **Add Storage Location**（添加存储位置），以定义该存储库的特定存储位置或卷。该卷应为主存储位置。
- 4 在 **Storage Location**（存储位置）区域，指定如何为存储位置添加文件。您可选择添加本地附加存储卷（如直接附加存储、存储区域网络，或网络附加存储）。您也可在公共因特网文件系统 (CIFS) 共享位置中指定存储卷。
 - 单击 **Add the file on local disk**（在本地磁盘上添加文件）以指定本地机器，然后根据下表中的说明输入信息。

表. 87: 本地磁盘设置

文本框	说明
Data Path (数据路径)	输入用于存储受保护数据的位置。 例如, 输入 X:\Repository\Data。 指定路径时, 只能使用字母数字字符、连字号和句点 (仅用于分隔主机名和域)。您仅可使用反斜线字符定义路径中的级别。请勿使用空格。不允许使用其他符号或标点符号。
Metadata Path (元数据路径)	输入用于存储受保护元数据的位置。 例如, 输入 X:\Repository\Metadata。 指定路径时, 只能使用字母数字字符、连字号和句点 (仅用于分隔主机名和域)。您仅可使用反斜线字符定义路径中的级别。请勿使用空格。不允许使用其他符号或标点符号。

- 您也可以选择 **Add file on CIFS share (在 CIFS 共享上添加文件)** 指定一个网络共享位置, 然后按下表所述输入相应的信息。

表. 88: CIFS 共享凭据

文本框	说明
UNC 路径	输入网络共享位置的路径。 如果该位置位于根路径, 请定义专属文件夹名称 (例如, Repository)。 路径必须以 \\ 开头。指定路径时, 只能使用字母数字字符、连字号和句点 (只用于分隔主机名和域)。字母 a 至 z 区分大小写。请勿使用空格。不允许使用其他符号或标点符号。
用户名	指定用于访问网络共享位置的用户名。
密码	指定用于访问网络共享位置的密码。

- 在 **Storage Configuration (存储配置)** 区域, 单击 **More Details (更多详细信息)**, 并按下表所述, 输入存储位置的详细信息。

表. 89: 存储配置详细信息

文本框	说明
大小	设置存储位置的大小或容量。最小为 1 GB。默认为 250 GB。您可选择以下选项: - GB - TB ① 注: 指定的大小不能超过卷的大小。 如果存储位置是使用 Windows XP 或 Windows 7 的新技术文件系统 (NTFS) 卷, 则文件大小限制为 16 TB。 如果存储位置为使用 Windows 8、8.1、Windows 10, 或 Windows Server 2012、2012 R2 的 NTFS 卷, 则文件大小限制为 256 TB。 ① 注: 要让 Rapid Recovery 验证操作系统, 在目标存储位置必须安装 Windows Management Instrumentation (WMI)。
Write Caching Policy (写高速缓存策略)	写高速缓存策略控制 Windows Cache Manager 在存储库中的使用方式, 并帮助调整存储库以便在不同配置下实现最佳性能。 请将其设置为以下值之一: - On (打开) - Off (关) - Sync (同步)

文本框	说明

如果设置为默认值 On（开），Windows 将控制缓存。这适用于 Windows 10，以及 Windows Server 2012 和更高版本。

① 注: 将写高速缓存策略设置为 On（开）可导致性能加快。如果使用 Windows Server 2008 SP2 或 Windows Server 2008 R2 SP2，则建议设置为 Off（关）。

如果设置为 Off（关闭），则 Rapid Recovery 将控制高速缓存。

如果设置为 Sync（同步），则 Windows 将控制高速缓存以及同步输入/输出。

每扇区字节数	指定希望每个扇区包含的字节数。默认值为 512。

Average Bytes per Record（每个记录的平均字节数）	指定每个记录的平均字节数。默认值为 8192。

6 单击下一步。

如果您在步骤 1 中选择 **Advanced（高级）** 选项，则此时显示 **Encryption（加密）** 页面。

- 18 另外，在 Encryption（加密）页面中，要启用加密，请选择 **Enable Encryption（启用加密）**。

在 Encryption（加密）页面中将显示 Encryption key（加密密钥）字段。

① 注: 如果您启用了加密，则会应用至该代理机器中所有受保护卷的数据。您之后可通过 **Rapid Recovery Core 控制台** 的 **Configuration（配置）** 选项卡更改这些设置。要了解与加密相关的详情，请参阅主题 [了解加密密钥](#)。

△ 小心: Rapid Recovery 在密码块链 (CBC) 模式中使用 AES 256 位加密和 256 位密钥。虽然使用加密是可选的，但是 Dell 强烈建议您建立加密密钥，并保护您定义的密码短语。请将密码短语保存在安全位置，因为它对于数据恢复至关重要。如果没有密码短语，将无法进行数据恢复。

- 19 如果您要使用已在此 Rapid RecoveryCore 中定义的加密密钥加密这些受保护的机器，请选择 **Encrypt data using an existing Encryption key（使用已有加密密钥加密数据）**，然后从下拉菜单中选择相应的密钥。

继续执行 [步骤 21](#)。

- 20 如果您要向 Core 添加新的加密密钥，并应用该密钥至这些受保护的机器，请按下表所述输入信息。

表. 90: 加密密钥设置

文本框	说明
名称	输入加密密钥的名称。 加密密钥名称必须包含 1 至 130 个字母数字字符。不得包含特殊字符，如反斜线、斜线、管道字符、冒号、星号、引号、问号、左右括号、& 符号或井号。
说明	输入加密密钥的注释。 通过 Core 控制台查看加密密钥时，该信息会显示在 Description（说明）字段中。
密码短语	输入用于控制访问的密码短语。 最佳做法是避免使用上述特殊字符。 将密码记录在安全位置。Dell Support 无法恢复密码。创建加密密钥并将其应用至一个或多个受保护的机器后，如果您丢失该密码，则无法恢复数据。
确认密码短语	重新输入刚输入的密码短语。

- 21 单击 **Finish（完成）** 以保存并应用设置。

- 22 如果显示 Warning（警告）页面，但您仍对选择满意，请再次单击 **Finish（完成）**。

Rapid Recovery Agent 软件部署在指定的机器中（如有需要），机器被添加至 Core 的保护中。

手动保护多台计算机

使用此流程可手动输入您要保护的每台计算机。例如，保护 Linux 机器时使用该流程。

- 1 在 Rapid Recovery Core Console 上，单击**保护**下拉菜单，然后单击**保护多台计算机**。
此时“保护多台计算机向导”将打开。
- 2 在**欢迎**页面上，选择以下选项之一：
 - 典型值
 - 高级（显示可选步骤）
- 3 单击**下一步**。
- 4 在向导的**连接**页面中，从**源**下拉列表中选择**手动**。
- 5 单击**下一步**。
- 6 在**选择计算机**页面上以如下格式在对话框中输入详细信息 hostname::username::password::port。端口设置是可选的。
示例包括：
10.255.255.255::administrator::&l1@yYz90z::8006
abc-host-00-1::administrator::99!zU\$o83r::168
- 7 单击**下一步**。
如果接下来在“保护多台计算机向导”中显示**保护**页面，则跳到**步骤 11**。
如果 Agent 软件尚未部署到要保护的计算机，或由于其他原因无法保护您指定的任何计算机，则所选计算机将显示在**警告**页面中。
- 8 （可选）在**机器警告**页面中，您可以选择任何机器，然后在工具栏中单击**验证**以验证该机器。
- 9 （可选）在**机器警告**页面中，选择**安装 Agent 后自动重新启动机器**。

注：Dell 建议此选项。您必须先重新启动代理机器，然后才能保护该机器。重新启动以确保代理服务正在运行，且如果相关，正常内核模块用于保护机器。

- 10 如果状态指示机器可以访问，则单击**下一步**以安装代理软件。
此时将显示**保护**页面。
- 11 在**保护**页面中，如下所述选择相应的保护计划。
 - 如果要使用默认保护计划，则在“计划设置”选项中选择**默认保护（每小时对所有卷创建快照）**。
 - 如果要定义不同的保护计划，则在“计划设置”选项中选择**自定义保护**。
- 12 继续进行配置，如下所示：
 - 如果已选择“保护机器向导”的“典型”配置和指定的默认保护，则单击**完成**以确认选择，关闭向导并保护指定的机器。
首次为计算机添加保护时，基本映像（即受保护卷中所有数据的快照）将在您定义计划后传输至 Rapid Recovery Core 上的存储库，除非您已指定在初始时暂停保护。
 - 如果已选择“保护计算机向导”的“典型”配置并已指定自定义保护，则单击**下一步**，请参阅**创建自定义保护计划**。
 - 如果已选择“保护计算机向导”的“高级”配置和默认保护，则单击**下一步**，然后前进到**步骤 14**以查看存储库和加密选项。
 - 如果已选择“保护计算机向导”的“高级”配置并已指定自定义保护，则单击**下一步**以设置自定义保护计划。有关定义自定义保护计划的详细信息，请参阅**创建自定义保护计划**。
- 13 在**存储库**页面上，执行以下操作：
 - 如果您已拥有存储库，并希望将此要保护的计算机中的数据存储在现有数据库中，可执行以下操作：
 - 1 选择**使用现有存储库**。
 - 2 从列表中选择现有存储库。
 - 3 单击**下一步**。
此时将显示**加密**页面。跳到**步骤 19**并选择性地定义加密。
 - 如果您要创建存储库，请选择**创建存储库**，然后完成以下步骤。
 - 1 在**存储库**上，根据下表中的说明输入信息。

表. 91: 添加新存储库设置

文本框	说明
存储库名称	输入存储库的显示名称。 默认情况下，此文本框包含词语 Repository 和一个数字，该数字与此 Core 的存储库数目相对应。例如，如果这是第一个存储库，则默认名称为 Repository 1。根据需要更改名称。 存储库名称必须包含 1 到 40 个字母数字字符（包括空格）。请勿使用 禁止字符 或 禁止短语 。
并发操作数	定义希望存储库支持的并发请求数量。默认值为 64。
注释	（可选）输入关于此存储库的说明。最多可输入 254 个字符。例如，键入 DVM Repository 2 。

- 2 单击**添加存储位置**以定义存储库的特定存储位置或卷。此卷应为主存储位置。

 **小心:** 在根目录中定义专用文件夹作为存储库的存储位置。请勿指定根目录位置。例如，使用 **E:\Repository**，而不是 **E:**。如果您在此步骤中创建的存储库稍后被删除，那么您存储库所在存储位置上的所有文件将随之被删除。如果您的存储位置定义在根目录中，那么卷（如 **E:**）中的其他所有文件将被删除，这可能会造成灾难性的数据丢失。

此时将显示**添加存储位置**对话框。

- 3 单击**添加存储位置**以定义存储库的特定存储位置或卷。此卷应为主存储位置。
- 4 在**存储位置**区域中，指定将文件添加到存储位置的方式。您可以选择添加本地连接的存储卷，例如：直接连接的存储、存储区域网络或网络连接的存储。您还可以在通用网络文件系统 (CIFS) 共享位置上指定存储卷。
- 选择**添加本地磁盘上的文件**以指定本地机器，然后根据下表中的说明输入信息。

表. 92: 本地磁盘设置

文本框	说明
数据路径	输入用于存储受保护数据的位置。 例如，键入 X:\Repository\Data。 指定路径时，只能使用字母数字字符、连字符和句点（仅用于分隔主机名和域）。您只能使用反斜杠字符来定义路径中的级别。请勿使用空格。不允许使用其他符号或标点字符。
元数据路径	输入用于存储受保护元数据的位置。 例如，键入 X:\Repository\Metadata。 指定路径时，只能使用字母数字字符、连字符和句点（仅用于分隔主机名和域）。您只能使用反斜杠字符来定义路径中的级别。请勿使用空格。不允许使用其他符号或标点字符。

- 或者，选择**添加 CIFS 共享上的文件**以指定一个网络共享位置，然后按下表所述输入相应的信息。

表. 93: CIFS 共享凭据

文本框	说明
UNC 路径	输入网络共享位置的路径。 如果此位置位于根目录中，则定义专用的文件夹名称（例如 Repository）。 路径必须以 \\ 开头。指定路径时，只能使用字母数字字符、连字符和句点（仅用于分隔主机名和域）。字母 a 至 z 不区分大小写。请勿使用空格。不允许使用其他符号或标点字符。
用户名	指定用于访问网络共享位置的用户名。
密码	指定用于访问网络共享位置的密码。

- 5 在**存储配置**区域中，单击**更多详细信息**，然后根据下表中的说明输入存储位置的详细信息。

表. 94: 存储配置详细信息

文本框	说明
大小	设置存储位置的大小或容量。最小大小为 1 GB。默认大小为 250 GB。可以选择以下单位： • GB • TB ① 注: 指定的大小不能超过卷的大小。 如果存储位置是使用 Windows XP 或 Windows 7 的新技术文件系统 (NTFS) 卷，则文件大小限制为 16 TB。 如果存储位置为使用 Windows 8、8.1、Windows 10 或 Windows Server 2012、2012 R2 的 NTFS 卷，则文件大小限制为 256 TB。 ① 注: 要让 Rapid Recovery 验证操作系统，则在目标存储位置必须安装 Windows Management Instrumentation (WMI)。
写高速缓存策略	写高速缓存策略控制 Windows Cache Manager 在存储库中的使用方式，并帮助调整存储库以便在不同配置下实现最佳性能。 请将其设置为以下值之一： • 打开 • 关闭 • 同步 如果设置为默认值打开，则 Windows 将控制高速缓存。这适用于 Windows 10 和 Windows Server 2012 及更高版本。 ① 注: 将写高速缓存策略设置为打开可提高性能。如果您使用的是 Windows Server 2008 SP2 或 Windows Server 2008 R2 SP2，则建议的设置为“关闭”。 如果设置为“关闭”，则 Rapid Recovery 将控制高速缓存。 如果设置为同步，则 Windows 将控制高速缓存以及同步输入/输出。
每扇区字节数	指定希望每个扇区包含的字节数。默认值为 512。
每个记录的平均字节数	指定每个记录的平均字节数。默认值为 8192。

6 单击下一步。

如果您在步骤 1 中选择了**高级**选项，那么此时将显示**加密**页面。

14 或者，要在**加密**页面上启用加密，可选择**启用加密**。

在 **Encryption（加密）** 页面中将显示 Encryption key（加密密钥）字段。

① | 注: 如果启用加密，则将对计算机上所有受保护卷的数据应用加密。您稍后可以在 **Rapid Recovery Core Console** 中的加密密钥页面上更改设置。有关加密的更多信息，请参阅主题**了解加密密钥**。

△ | 小心: 在密码块链 (CBC) 模式中，**Rapid Recovery** 采用 256 位密钥实施 AES 256 位加密。虽然使用加密是可选选项，但 **Dell** 强烈建议您创建加密密钥并保护您定义的密码。将密码短语存储在安全的位置，因为密码短语对于数据恢复至关重要。如果没有密码短语，将无法进行数据恢复。

15 如果要使用已在该 Rapid Recovery Core 上定义的加密密钥对这些受保护计算机进行加密，可选择**使用现有加密密钥对数据进行加密**，并从下拉菜单中选择相应的密钥。

继续执行**步骤 17**。

16 如果要将新加密密钥添加到 Core 中并将该密钥应用到这些受保护机器，则输入下表所述的信息。

表. 95: 加密密钥设置

文本框	说明
名称	输入加密密钥的名称。 加密密钥的名称必须包含 1 至 130 之间的字母数字字符。不可使用特殊字符，例如，反斜杠、正斜杠、竖线、冒号、星号、引号、问号、开方括号或闭方括号、和号或#号。
说明	输入加密密钥的注释。 当从 Core Console 中查看加密密钥时，该信息在“说明”字段中显示。
密码短语	输入用于控制访问的密码短语。 最佳做法是避免以上列出的特殊字符。 将密码短语存储在安全的位置。Dell Support 无法恢复密码。一旦创建加密密钥并将其应用到一个或多个受保护机器中，则当您丢失了密码短语将无法恢复数据。
确认密码短语	重新输入刚输入的密码。

- 17 单击**完成**以保存并应用设置。
此时将关闭向导。
- 18 如果此时出现**警告**页面并且您仍满意您的选择，则可再次单击**完成**。

Rapid Recovery Agent 软件将部署到指定的计算机上，如有必要，计算机可添加至 Core 上的保护。

监测多台机器的保护

随着 Rapid Recovery 将保护策略和计划应用至计算机，您可以对进度进行监控。

在 Rapid Recovery Core Console 中，导航至 Rapid Recovery 的“主页”页面，然后单击 （事件）。
此时将显示**事件**页面，并细分为“任务”、“警报”和“事件”。传输卷时，状态、开始时间和结束时间将显示在“任务”窗格中。
您也可以按状态（活动、正在等待、已完成、已排入队列和已失败）来筛选任务。有关更多信息，请参阅[查看任务](#)。

① | 注: 要仅查看等待执行的任务，请确保选择“等待任务”图标。

当添加各个受保护机器时，系统将记录一个警报，以列出操作是否成功或是否已记录错误。有关更多信息，请参阅[查看警报](#)。
有关查看所有事件的信息，请参阅[查看所有事件](#)。

受保护的 Exchange Server 的设置和功能

如果您在 Core 中保护 Microsoft Exchange Server，您可以在 Rapid Recovery Core Console 中配置其他设置，并且可以执行其他功能。

在与 Exchange Server 相关的 Core Console 中提供了单个设置 - **启用自动可安装性检查**。如果启用，会自动执行 Exchange Server 可安装性检查。当受保护机器的状态为绿色（活动）或黄色（暂停）时，可以使用此设置。

有关详情，请参阅[关于 Exchange 数据库可安装性检查](#)。

您也可以从受保护的 Exchange Server 机器上的“恢复点”窗格中按需执行可安装性检查。有关详情，请参阅[强制执行 Exchange 数据库可安装性检查](#)。

以下是可对受 Core 保护的 Exchange Server 执行的功能。

- **指定 Exchange Server 凭据。**Rapid Recovery Core 可让您设置凭据，以便 Core 可以验证登录到 Exchange Server 以获取信息。有关为 Exchange Server 设置凭据的更多信息，请参阅[设置 Exchange Server 机器的凭据](#)。
- **截断 Exchange 日志。**当您为 Exchange Server 日志执行强制日志截断时，此过程会确定受保护 Exchange Server 上的可用空间并恢复空间。有关按需截断 Exchange Server 日志的更多信息，请参阅[强制执行 SQL 机器日志截断](#)。也可以作为每夜作业的一部分执行此过程。
- **强制执行 Exchange 数据库的可安装性。**此功能会检查是否可安装 Exchange 数据库，以便检测损坏并向管理员发出警报，从而可以成功恢复 Exchange Server 上的所有数据。有关按需强制进行可安装性检查的更多信息，请参阅[强制执行 Exchange 数据库可安装性检查](#)。

您也可以强制在每次创建快照后自动执行可安装性检查。有关可安装性检查的更多信息，请参阅[关于 Exchange 数据库可安装性检查](#)。
- **强制执行 Exchange Server 恢复点的校验和检查。**此功能会检查包含 Exchange 数据库文件的恢复点的完整性。有关按需强制进行校验和检查的更多信息，请参阅[强制执行 Exchange 数据库文件的校验和检查](#)。

您可以在每夜作业过程中截断 Exchange 日志并强制进行校验和检查。有关您可以计划为每夜作业的任务的更多信息，请参阅[了解每夜作业](#)。有关配置每夜作业的信息，请参阅[配置 Core 的每夜作业](#)。

设置 Exchange Server 机器的凭据

为了设置登录凭据，Exchange Server 必须存在于受保护的卷上。如果 Rapid Recovery 未检测到 Exchange Server 存在状态，则“设置凭据”功能将不显示在 Core Console 中。

保护 Microsoft Exchange Server 上的数据后，则可以在 Rapid Recovery Core Console 中设置登录凭据。

完成此过程中的步骤以便为每个 Exchange Server 设置凭据。

- 1 在 Rapid Recovery Core Console 的左侧导航区域中，选择要为其设置凭据的受保护 Exchange Server 机器。

将显示受保护 Exchange Server 的**摘要**页面。
- 2 在**摘要**页面顶部的链接中，单击 Exchange 菜单右边的向下箭头 ▼，然后从出现的下拉菜单中，选择**设置凭据**。

此时会显示受保护 Exchange Server 的**编辑 Exchange 凭据**对话框。
- 3 在**编辑 Exchange 凭据**对话框中，根据如下所示输入您的凭据：
 - a 在**用户名**文本字段，输入有权访问 Exchange Server 的用户的用户名；例如，Administrator（或者如果机器位于域中，则为 [域名]\Administrator）。
 - b 在**密码**文本字段，输入与指定连接 Exchange Server 的用户名关联的密码。
 - c 单击**确定**，以确认设置，并关闭对话框。

强制执行 SQL 机器日志截断

要强制执行日志截断，Exchange 数据库必须出现在受保护卷上。如果 Rapid Recovery 未检测到数据库的存在，则日志截断检查将不显示在 Core Console 中。

当您为受保护 Exchange 服务器强制执行日志截断时，日志大小将减小。要按需强制执行日志截断，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的左侧导航区域中，选择要强制执行日志截断的受保护 Exchange Server。

此时将显示受保护机器的**摘要**页面。
- 2 在页面顶部单击 **Exchange** 下拉菜单，然后选择**强制日志截断**。
- 3 在生成的对话框中，单击以确认您要强制日志截断。

关闭对话框。系统将开始截断 Exchange Server 日志。如果此类事件已启用 Toast 警报，您将看到一条消息，显示日志截断过程开始。

关于 Exchange 数据库可安装性检查

使用 Rapid Recovery 备份 Microsoft Exchange Server 时，可在创建每个快照后对所有 Exchange 数据库执行可安装性检查。此损坏检测功能可以警告管理员注意潜在故障，确保 Exchange Server 上的所有数据在发生故障时都可以成功恢复。

要启用或禁用此功能，请转到受保护机器的**设置**菜单，并将**启用自动可安装性检查**选项分别设置为“是”或“否”。有关修改受保护机器的设置的更多信息，请参阅[查看和修改受保护机器设置](#)。

可安装性检查不是每夜设置的一部分。但是，如果启用了自动可安装性检查，并且已启用“截断 Exchange 日志”每夜作业，则将在日志截断完成后触发可安装性检查。

您也可以从受保护的 Exchange Server 机器上的**恢复点**窗格中按需执行可安装性检查。有关详情，请参阅[强制执行 Exchange 数据库可安装性检查](#)。

① 注：可安装性检查仅适用于 **Microsoft Exchange 2007、2010 和 2013**。此外，必须在 **Exchange** 中为 **Rapid Recovery Agent** 服务帐户分配“组织管理员”角色。

强制执行 Exchange 数据库可安装性检查

为了强制执行可安装性检查，Exchange 数据库必须存在于受保护的卷上。如果 Rapid Recovery 未检测到数据库存在状态，则可安装性检查功能将不显示在 Core Console 中。

要强制系统按需对特定 Exchange Server 恢复点执行可安装性检查，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的左侧导航区域中，选择要对其强制进行可安装性检查的受保护 Exchange Server 机器，然后单击**恢复点**菜单。
- 2 向下滚动到**恢复点**窗格。
- 3 浏览恢复点以查找所需的恢复点。（可选）单击列表中恢复点右侧的  箭头以展开视图。在展开的恢复点信息中，您可以看到恢复点中包含的卷。
- 4 在**恢复点**窗格中，从代表正确恢复点的行中，单击 ，并从下拉菜单中选择**强制可安装性检查**。
- 5 在出现的对话框中，单击以确认您要强制执行可安装性检查。
关闭对话框。系统将执行可安装性检查。如果已为此类型的事件启用弹出式警报，您将看到一则消息表明可安装性检查启动。

有关如何查看可安装性检查状态的指示，请参阅[使用任务、警报和日记查看事件](#)。

强制执行 Exchange 数据库文件的校验和检查

要强制执行校验和检查，Exchange 数据库必须存在于受保护卷上。如果 Rapid Recovery 未检测到数据库的存在，则校验和检查功能将不显示在 Core Console 中。

要强制系统对特定 Exchange Server 恢复点执行校验和检查，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的左侧导航区域中，选择要对其强制执行校验和检查的受保护 Exchange Server，然后单击**恢复点**菜单。
此时会显示受保护 Exchange Server 的**恢复点**页面。
- 2 向下滚动至**恢复点**窗格。
- 3 导航浏览恢复点以查找所需的恢复点。或者单击列表中恢复点旁的  箭头以展开视图。在展开的恢复点信息中，您可以看到恢复点中包含的卷。
- 4 在**恢复点**窗格中，从代表正确恢复点的行单击 ，然后从下拉菜单中选择**强制校验和检查**。
- 5 在生成的对话框中，单击以确认您要强制执行校验和检查。
关闭对话框。系统将执行校验和检查。如果此类型事件已启用 Toast 警报，您将看到一条消息，以显示校验和检查开始。

有关如何查看校验和检查状态的说明，请参阅[使用任务、警报和日记查看事件](#)。

受保护 SQL 服务器的设置和功能

如果您在 Core 中保护 Microsoft SQL Server，您可以在 Rapid Recovery Core Console 中配置其他设置，并且可以执行其他功能。

在与 SQL Server 相关的 Core Console 中提供了单个设置 - **可附加性**。

Rapid Recovery Core 可让您执行 SQL 可附加性检查以验证包含 SQL 数据库的恢复点的完整性。此操作会检查 SQL 数据库的一致性，并确保备份快照中包含所有支持性 MDF（数据）和 LDF（日志）文件。

在以前的版本中，SQL 可附加性检查曾经要求使用 Core 机器上获得许可的 SQL Server 版本。Rapid Recovery Core 现在允许从 Core 上的 SQL Server 实例或从受保护 SQL Server 机器上获得许可的 SQL Server 版本执行 SQL 可附加性检查。

可附加性设置可让您指定要使用哪个获得许可的 SQL Server 版本来执行此检查。有关配置可附加性设置的更多信息，请参阅[管理 Core SQL 可附加性设置](#)。

有关 SQL 可附加性的更多信息，请参阅[关于 SQL 可附加性](#)。

以下是可对受 Core 保护的 SQL Server 执行的功能。

- **指定 SQL Server 凭据。** Rapid Recovery Core 可让您设置凭据，以便 Core 可以验证登录到 SQL 服务器以获取信息。您可以为单个受保护的 SQL Server 机器设置凭据，或为所有受保护的 SQL Server 设置默认凭据。
有关为 SQL 服务器设置凭据的更多信息，请参阅[设置 SQL Server 机器凭据](#)。
- **截断 SQL 日志。** 当您为 SQL Server 日志执行强制日志截断时，此过程会确定受保护服务器上的可用空间。此过程不恢复任何空间。
有关按需截断 SQL Server 日志的更多信息，请参阅[强制执行 SQL 机器日志截断](#)。
- **强制执行 SQL Server 的可附加性检查。** 此功能会检查 SQL 数据库的一致性，并确保备份快照中包含所有支持性 MDF（数据）和 LDF（日志）文件。
有关按需强制对 SQL 服务器进行可附加性检查的更多信息，请参阅[强制执行 SQL Server 可附加性检查](#)。

除指定凭据以外，可以按需完成以上列表所述的每个功能，也可以将这些功能配置为在为 Core 执行每夜作业期间发生。有关您可以计划为每夜作业的任务的更多信息，请参阅[了解每夜作业](#)。有关配置每夜作业的信息，请参阅[配置 Core 的每夜作业](#)。

设置 SQL Server 机器凭据

您必须将 SQL Server 机器添加到 Rapid Recovery Core 上的保护中，然后再执行该过程。有关保护机器的更多信息，请参阅[保护机器](#)。

保护 Microsoft SQL Server 上的数据后，则可以在 Rapid Recovery Core Console 中设置单个实例或所有 SQL Server 的登录凭据。

完成此过程中的步骤以便为每个 SQL Server 设置凭据。

- 1 在 Rapid Recovery Core Console 的左侧导航区域中，选择要为其设置凭据的受保护 SQL Server 机器。
将显示受保护 SQL Server 的**摘要**页面。
- 2 在**摘要**页面顶部的链接中，单击 Exchange 菜单右边的向下箭头 ▼，然后从出现的下拉菜单中，执行以下操作之一：
 - 如果要设置所有 SQL Server 数据库实例的默认凭据，请单击**为所有实例设置默认凭据**，在**编辑默认凭据**对话框中，执行以下操作：
 - 1 在**用户名**文本字段中，为有权访问所有关联的 SQL 服务器的用户输入用户名；例如，Administrator（或者如果机器位于域中，则为 [域名]\Administrator）。
 - 2 在**密码**文本字段，输入与指定连接 SQL Server 的用户名关联的密码。
 - 3 单击**确定**，以确认设置，并关闭对话框。
 - 如果要设置单个 SQL Server 数据库实例的凭据，请单击受保护 SQL Server 机器的显示名称，然后在**编辑实例凭据**对话框中，执行以下操作：

- 1 选择凭据类型（默认为 Windows 或 SQL）
- 2 在**用户名**文本字段，为有限访问 SQL 服务器的用户输入用户名；例如，Administrator（或者如果机器位于域中，则为 [域名]\Administrator）。
- 3 在**密码**文本字段，输入与指定连接 SQL Server 的用户名关联的密码。
- 4 单击**确定**，以确认设置，并关闭对话框。

强制执行 SQL 机器日志截断

日志截断可用于使用 SQL Server 的机器。要强制执行日志截断，请完成以下过程中的步骤。

① 注：当为 SQL 机器进行时，截断会确定磁盘上的可用空间，但是不会减小日志大小。

- 1 在 Rapid Recovery Core Console 的左侧导航区域中，选择要强制执行日志截断的机器。
此时将显示受保护机器的**摘要**页面。
- 2 从**摘要**页面（或者从此受保护机器的任何页面）中，在页面顶部单击 **SQL** 下拉菜单，然后选择**强制执行日志截断**。
- 3 单击**是**以确认要强制执行日志截断。

关于 SQL 可附加性

SQL 可附加性功能可让 Rapid Recovery Core 将 SQL 主数据库文件（.MDF 文件）和日志数据库文件（.LDF 文件）附加到受保护 SQL Server 的快照。使用 Microsoft SQL Server 的本地实例捕获快照。

与保护 SQL Server 机器的 Rapid Recovery 用户相关的问题包括：哪个 SQL Server 实例执行可附加性检查，以及执行 SQL 可附加性检查的方法（按需还是作为每夜作业的一部分）。

Core 通过这种可附加性检查验证 SQL 数据库的一致性，并确保备份快照中的所有 MDF 和 LDF 文件可用。

可附加性检查可根据需要针对特定恢复点执行，也可以将其作为每夜作业的一部分。

要按需执行 SQL 可附加性检查，请参阅[强制执行 SQL Server 可附加性检查](#)。要在为每夜作业操作指定的时间每天执行一次 SQL 可附加性，请在每夜作业中启用选项**检查 SQL 数据库的可附加性**。有关设置 Core 的每夜作业的更多信息，请参阅[配置 Core 的每夜作业](#)。有关设置特定机器（在本例中为受保护的 SQL Server）的每夜作业的更多信息，请参阅[自定义受保护机器的每夜作业](#)。

在以前的版本中，SQL 可附加性需要在 Core 机器上安装和配置 Microsoft SQL Server 的本地实例。Rapid Recovery Core 现在可让您选择从 Core 上的 SQL Server 实例或从受保护 SQL Server 机器上的 SQL Server 实例执行可附加性检查。您选择的实例必须是从 Microsoft 或许经销商获得的完全许可的 SQL Server 版本。Microsoft 不允许使用被动 SQL 许可证。

无论您指定哪种 SQL Server 实例，该实例随后都会用于所有可附加性检查。将在 Core 设置和每夜作业之间同步可附加性。例如，如果您指定为每夜作业使用 SQL Server 的 Core 实例，按需可附加性检查随后也会使用 Core。相反，如果您指定使用特定受保护机器上的 SQL Server 实例，所有按需和每夜可附加性检查随后会使用受保护机器上的本地实例。

选择要用作全局 Core 设置的一部分的 SQL Server 实例。有关详情，请参阅[管理 Core SQL 可附加性设置](#)。

① 注：从受保护的 SQL Server 机器执行可附加性检查需要在该服务器上安装 **Rapid Recovery Agent** 软件。SQL 可附加性不支持无代理程序的保护。

Rapid Recovery Core 中的可附加性支持 SQL Server 2005、2008、2008 R2、2012 和 2014。在 SQL Server 实例上，用于执行测试的帐户必须分配有 sysadmin 角色。

SQL Server 的磁盘存储格式与 64 位和 32 位环境中的格式相同，并且可附加性能够跨两个版本运行。如果将数据库从某个环境中运行的服务器实例分离，则该数据库可以附加到在另一个环境中运行的服务器实例。

① 注：Core 上的 SQL Server 版本不得低于所有已安装 SQL Server 的受保护机器上的 SQL Server 版本。

强制执行 SQL Server 可附加性检查

为了强制执行可附加性检查，SQL 数据库必须存在于受保护的卷上。如果 Rapid Recovery 未检测到数据库存在状态，则可附加性检查功能将不显示在 Core Console 中。

要强制系统对特定 SQL Server 恢复点执行可附加性检查，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的左侧导航区域中，选择要对其强制进行可附加性检查的受保护 SQL Server 机器，然后单击**恢复点**菜单。
- 2 向下滚动到**恢复点**窗格。
- 3 浏览恢复点以查找所需的恢复点。（可选）单击列表中恢复点右侧的 ► 箭头以展开视图。
在展开的恢复点信息中，您可以看到恢复点中包含的卷。
- 4 在**恢复点**窗格中，从代表正确恢复点的行中，单击 ，并从下拉菜单中选择**强制可附加性检查**。
- 5 在出现的对话框中，单击以确认您要强制执行可附加性检查。
关闭对话框。系统将执行可附加性检查。

有关如何查看可附加性检查状态的指示，请参阅[使用任务、警报和日记查看事件](#)。

理解 Rapid Snap for Virtual

通过安装 Rapid Recovery Agent 软件，您可保护 Rapid Recovery Core 上的物理机或虚拟机。受支持的操作系统在主题“Rapid Recovery Agent 软件要求”中的系统要求中进行了说明。

Rapid Recovery 现在提供其他方式以保护机器。

Rapid Recovery 的 Rapid Snap for Virtual 功能（也称为无代理保护）可保护 VMware ESXi 或 Hyper-V 主机上的虚拟机 (VM)，而无需在每个虚拟机上安装 Rapid Recovery Agent。

小心: Dell 建议您一次限制对不超过 200 个虚拟机提供无代理保护。例如，使用 **Protect Multiple Machines Wizard**（保护多台机器向导）时请勿选择超过 200 个虚拟机。保护 200 个以上的虚拟机会降低性能。在一段时间内，Core 可无代理保护的虚拟机的数量没有限制。例如，今天您可保护 200 个虚拟机，明天您可保护其他 200 个虚拟机。

保护 vCenter/ESXi VMs

您可通过 Rapid Recovery 保护 vCenter/ESXi 虚拟机而无需在虚拟机或 ESXi 主机上安装 Rapid Recovery Agent 便可实现无代理保护。要保护 ESXi 环境，Rapid Recovery Core 可与 VMware 的原生快照技术配合运行。

Rapid Recovery 无代理保护使用 ESXi 客户端和现有应用程序界面 (API) 保护单个主机上的所选虚拟机，而无需安装 Rapid Recovery Agent 软件。Rapid Recovery Core 之后与虚拟机磁盘 (VMDK) 进行通信，以决定受保护卷的所需详情。由于 Rapid Recovery 根据卷（而非 VMDK）创建恢复点，因此每个卷可单独安装、恢复和导出。

注: Rapid Recovery 建议在要在 vSphere 或 ESXi 主机上保护的虚拟机 (VM) 上安装 **VMware Tools**。当在使用 **Windows 操作系统 (OS)** 的虚拟机上安装 **VMware Tools** 后，**Rapid Recovery Core** 采集的备份会使用 **Microsoft Volume Shadow Services (VSS)**。要了解安装有或未安装 **VMware Tools** 的无代理虚拟机行为的相关信息，请参阅 [安装 VMware 工具以实现无代理程序保护所具备的优势](#)。

无代理保护还会使用 VMware Changed Block Tracking (CBT) 以缩短增量快照所需的时间。CBT 决定 VMDK 文件中哪些区块发生变化，使 Rapid Recovery 仅备份自上次快照以来发生变化的那部分磁盘。这种备份方法通常会导致缩短备份操作，并可减少网络资源消耗和存储元素。

使用无代理保护具有多项益处。部分最实用的属性包含以下特征：

- 主机上无需安装其他软件。

- 通过无代理保护可选择自动保护添加至 ESXi 主机的新虚拟机。
- 保护过程中不要求重新启动。
- 不要求为每个单独的虚拟机提供凭据。
- 即使虚拟机处于关机状态，无代理保护也可保护该虚拟机。
- 无代理保护可恢复至磁盘。
- 传输过程中，无代理保护不要求卷有剩余空间。
- 无代理保护支持所有来宾操作系统。
- 无代理保护可导出动态磁盘或卷。

① 注: 如果动态卷很复杂（条带化、镜像、扩展或 RAID），则会作为磁盘映像导出这些卷，并会在导出的虚拟机上完成导出操作后解析为卷。

虽然可出于多种原因为 ESXi VM 采用无代理保护，但应选择最适合您的环境和业务需要的保护方法。除上述益处外，选择无代理保护时还应考虑以下因素：

- 无代理保护不支持从卷级别提供动态卷保护（例如扩展、条带化、镜像或 RAID 卷），而是从磁盘级别提供保护。
- 无代理保护不支持实时恢复。要了解该功能的更多信息，请参阅 [了解实时恢复](#)。
- 将每个单独卷恢复至受保护的虚拟机后，您必须重新启动虚拟机。
- 无代理保护不会收集 Microsoft SQL 或 Microsoft Exchange 元数据。
- 您无法执行 SQL 连接性检查、日志截断，或对在无代理受保护机器上采集的恢复点执行安装性检查。
- 无代理保护不会收集或显示卷标，或驱动器号。
- 如果虚拟磁盘类型为厚配置置零，则无代理保护不会显示虚拟机中实际使用的空间大小。

如果您为 ESXi VM 选择使用无代理保护，则主机必须符合以下最低要求，无代理保护才能成功。

- 主机必须运行 ESXi 5.0.0 内部版本 623860 或更高版本。
- 主机必须满足 *Rapid Recovery 安装和升级指南* 中所述的最低系统要求。
- 对于卷级别的保护，VMDK 必须包含 Master Boot Record (MBR) 分区表或 GUID 分区表 (GPT)。没有这些分区表的 VMDK 作为整个磁盘（而非单独卷）得到保护。
- 每个 VMware 虚拟机必须安装 VMware Tools，以确保快照的一致性。

保护 Hyper-V 服务器和群集

要以无代理方式保护 Hyper-V 服务器，您无需在任何虚拟机上安装 Rapid Recovery Agent。您只需要在主机或群集节点上安装即可。代理可保护主机上的虚拟硬盘，并将硬盘文件的任何变更转换至卷映像或磁盘映像（取决于文件系统）。新的驱动程序为主机和群集共享卷 (CSVs) 上的虚拟机提供文件级支持。

① 注: Rapid Recovery 支持 VHDx 磁盘文件格式。它不支持 VHD 格式。

要保护 CSV 上的虚拟机，必须使用 Protect Multiple Machines Wizard（保护多个机器向导）中的自动部署功能，在每个群集节点上安装 Rapid Recovery Agent 和驱动程序。通过这些节点，代理可通过为每个文件创建两类更改，保护 CSV 上运行的所有虚拟机。第一类更改仅在快照或全新系统重新启动之前或之后保存。第二类更改保留在磁盘上，以提供增量快照，即使出现电源故障或异常关闭时也是这样。安装在节点上的代理在传输数据前将所有更改合并为一个。

当主机或节点正在运行时，Rapid Recovery 会创建一个应用程序一致的备份。如果主机未运行，则不会创建备份；但如果其中一个节点未运行，则 Rapid Recovery 可继续在群集上生成虚拟机的快照。

① 注: 要获得最佳性能，建议将 Hyper-V 主机或节点的最大并行传输设置为 1，这是默认设置。

无代理 Hyper-V 保护拥有很多与在每个虚拟机上安装代理的传统保护相同的功能，其中包括：

- 存档
- 恢复点完整性检查
- 安装恢复点
- 自动查找新虚拟机（对无代理保护是唯一的）

- 复制
- 恢复虚拟机
- 恢复 CSV
- 使用 VHDX 格式在 CIFS 上恢复
- 以来宾 VHDX 格式恢复文件
- Rollup（前滚）
- 虚拟导出至 Hyper-V VM 和其他管理程序，包括 ESXi、VMware Workstation 和 VirtualBox

但选择无代理 Hyper-V 保护时需要考虑到某些限制。无法执行的功能包括：

- Exchange 安装完整性检查
- SQL 可附加性检查
- 实时恢复
- 使用 VHD 格式在 CIFS 上恢复虚拟机
- 以来宾 VHD 格式恢复文件

① 注: 对于应用程序一致性快照而言，您必须在每个虚拟机上安装 SCSI 控制器。如果未安装此控制器，结果总是为崩溃一致性快照。

安装 VMware 工具以实现无代理程序保护所具备的优势

在不使用 Rapid Recovery Agent 的情况下保护虚拟机 (VM) 时，Dell 建议您在 vSphere 或 ESXi 主机上的受保护虚拟机上安装 VMware 工具以充分利用 Microsoft 卷影服务 (VSS) 功能。

无代理程序保护使用 VMware 原生的快照技术来备份受保护的数据。在使用 Windows 操作系统 (OS) 的虚拟机上安装了 VMware 工具时，Rapid Recovery Core 捕获的备份也可以使用 VSS。未安装 VMware 工具时，Rapid Recovery 仍然会收集快照，但缺少 VMware 工具的情况可能会对您的受保护虚拟机上的数据状态产生不良影响。

有两种可能的数据状态：

- **崩溃一致。**虚拟机操作系统会启动，并且可以读取并理解文件系统。
- **应用程序一致。**虚拟机操作系统会启动，并且可以读取并理解文件系统。此外，事务处理应用程序的文件处于一致状态。例如，对于 SQL Server，日志与数据库文件匹配，数据库可快速轻松地打开。

如果您从崩溃一致状态恢复事务处理应用程序，数据库会返回到最后一个有效的状态。最新的有效状态可能来自崩溃之时，也可能来自崩溃之前。如果状态来自崩溃之前，数据库必须前滚一点，以使数据文件与日志中的信息相匹配。当您第一次打开数据库时，此过程会花费一些时间，这会导致启动机器时出现延迟。

根据是否安装了 VMware 工具以及虚拟机的开机状态，以下条件将适用：

表. 96: 虚拟机的备份类型条件

VMware 工具	虚拟机已开机	备份类型
未安装	是	崩溃一致
未安装	无（异常关闭）	崩溃一致
未安装	无（顺利关闭）	应用程序一致
已安装	是	应用程序一致
已安装	无（异常关闭）	崩溃一致
已安装	无（顺利关闭）	应用程序一致

保护无 Rapid Recovery Agent 的 vCenter/ESXi 虚拟机

完成以下过程以实现 ESXi 虚拟机的无代理保护。

- ①

注: Rapid Recovery 建议将 VMware Tools 安装到您想在 vSphere 或 ESXi 主机上保护的虚拟机上。当 VMware Tools 安装到使用 Windows 操作系统的虚拟机上时, Rapid Recovery Core 捕获的备份会使用 Microsoft 卷影服务 (VSS)。有关在带有或不带 VMware Tools 的无代理虚拟机的行为的信息, 请参阅[安装 VMware 工具以实现无代理程序保护所具备的优势](#)。
- △

小心: Dell 建议您限制一次仅对不超过 200 个虚拟机使用无代理保护。例如, 请勿在使用保护多个机器向导时选择 200 个以上的虚拟机。保护超过 200 个虚拟机会导致性能下降。Core 在一段时间内进行无代理保护的虚拟机数量没有限制。例如, 您可以今天保护 200 个虚拟机并在明天保护另外的 200 个虚拟机。

- 1

在 Rapid Recovery Core Console 中, 单击 **Protect (保护)** 下拉菜单, 然后单击 **Protect Multiple Machines (保护多个机器)**。此时会打开 Protect Multiple Machines Wizard (保护多个机器向导)。
- 2

在 **Welcome (欢迎)** 页面上, 选择以下选项之一:
 - 典型值
 - Advanced (show optional steps) (高级 (显示可选步骤))
- 3

单击**下一步**。
- 4

在向导的 **Connection (连接)** 页面中, 从 **Source (源)** 下拉列表中, 选择 **vCenter / ESX(i)**。
- 5

根据下表中的说明, 输入主机信息和登录凭据。

表. 97: vCenter/ESX(i) 连接设置

文本框	说明
主机	输入 VMware vCenter Server/ESX(i) 虚拟主机的名称或 IP 地址。
端口	用于连接到虚拟主机的端口。 默认设置为 443。
用户名	用于连接到虚拟主机的用户名; 例如, Administrator 或者, 如果机器处于域中, 则为 [域名] \Administrator。
密码	输入用于连接到此虚拟主机的安全密码。

- 6

确保 **Protect selected VMs Agentlessly (无代理保护所选虚拟机)** 处于选中状态。(此选项默认处于选中状态)。
- 7

在 **Select Machines (选择机器)** 页面中, 选择您想要保护的虚拟机。您可以使用下拉菜单以显示主机和群集列表或虚拟机和模板的列表。
- ①

注: VMware 更改块跟踪必须在您想要保护的每个虚拟机上启用。如果未启用, 则 Rapid Recovery 将自动启用 CBT 以确保得到保护。
- 8

如果想要在将新虚拟机添加到主机时自动保护它们, 请选择 **Auto protect new machines (自动保护新机器)**, 然后完成以下步骤。

a

单击**下一步**。

b

在 **Auto Protection (自动保护)** 页面中, 选择预计要在其中添加新机器的任何容器。
- 9

单击**下一步**。
- 10

在 Protection (保护) 页面中, 根据需要选择以下保护计划之一:
 - 如果希望使用默认保护计划, 请在 Schedule Settings (计划设置) 选项中选择 **Default protection (hourly snapshots of all volumes) (默认保护 (每小时为所有卷创建快照))**。
 - 如果希望定义不同的保护计划, 请在 Schedule Settings (计划设置) 选项中选择 **Custom protection (自定义保护)**。
- 11

继续按如下所示进行配置:
 - 如果选择了 Typical (典型) 配置和指定的默认保护, 请单击 **Finish (完成)** 以确认您的选择, 并关闭向导, 您指定的机器现已得到保护。

第一次为机器添加保护时, 除非您指定了初始暂停保护, 否则基本映像 (受保护卷上的所有数据的快照) 会根据您定义的计划传输到 Rapid Recovery Core 上的存储库中。

- 如果您选择了典型配置和指定的自定义保护，请单击 **Next（下一步）** 以设置自定义保护计划。有关定义自定义保护计划的详细信息，请参阅[创建自定义保护计划](#)。
 - 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置和默认保护，请单击 **Next（下一步）**，然后继续[步骤 13](#) 以查看存储库和加密选项。
 - 如果选择了 Protect Machine Wizard（保护机器向导）的 Advanced（高级）配置并指定了自定义保护，请单击 **Next（下一步）** 以设置自定义保护计划。有关定义自定义保护计划的详细信息，请参阅[创建自定义保护计划](#)。
- 12 单击**下一步**。
- 13 在 **Repository（存储库）** 页面上，执行以下操作：
- 如果您已经有了一个存储库并想要存储此机器中的数据以保护现有存储库，请执行以下操作：
 - 选择 **Use an existing repository（使用现有存储库）**。
 - 从列表选择一个现有存储库。
 - 单击**下一步**。

此时将显示 **Encryption（加密）** 页面。跳至[步骤 19](#) 还可以定义加密。

- 如果您希望创建存储库，请选择 **Create a Repository（创建存储库）**，然后完成以下步骤。
 - 在 **Repository（存储库）** 中，输入下表所述信息。

表. 98: Add New Repository（添加新存储库）设置

文本框	说明
Repository Name （存储库名称）	输入存储库的名称。 默认情况下，此文本框包含词语 Repository（存储库）和一个数字，它与此 Core 的存储库数量相对应。例如，如果它是第一个存储库，默认名称为 Repository 1。请根据需要更改此名称。 存储库名称必须包含介于 1 和 40 之间的字母数字字符，包括空格。请勿使用 禁止字符或禁止短语 。
Concurrent Operations（并发 操作数）	定义希望存储库支持的并发请求数量。默认值为 64。
注释	（可选）输入关于此存储库的描述性说明。您可以输入至多 254 个字符。例如，键入 DVM Repository 2 。

- 2 单击 **Add Storage Location（添加存储位置）** 以定义存储库的特定存储位置或卷。此卷应为主存储位置。

 **小心：**为存储库的存储位置指定根目录内的专用文件夹。请勿指定根目录位置。例如，使用 **E:\Repository**，而非 **E:**。如果在此步骤中创建的存储库之后被删除了，您的存储库的存储位置上的所有文件都会被删除。如果您在根目录上指定存储位置，则卷（例如，**E:**）中的所有其他文件都会被删除。这可能会导致灾难性数据丢失。

此时将显示 **Add Storage Location（添加存储位置）** 对话框。

- 3 单击 **Add Storage Location（添加存储位置）** 以定义存储库的特定存储位置或卷。此卷应为主存储位置。
- 4 在 **Storage Location（存储位置）** 区域中，指定将文件添加到存储位置的方式。您可以选择添加本地连接的存储卷（例如，直接连接的存储、存储区域网络或网络连接存储）。您还可以指定通用 Internet 文件系统 (CIFS) 共享位置上的存储卷。
- 单击 **Add file on local disk（在本地磁盘上添加文件）** 以指定本地机器，然后根据下表中的说明输入信息。

表. 99: 本地磁盘设置

文本框	说明
Data Path（数据 路径）	输入用于存储受保护数据的位置。 例如，键入 X:\Repository\Data 。

文本框	说明
	在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。
Metadata Path (元数据路径)	输入用于存储受保护元数据的位置。 例如，键入 X:\Repository\Metadata。 在指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。您仅可以使用反斜杠字符来定义路径级别。请勿使用空格。不允许使用其他符号或标点字符。

- 您也可以选择 **Add file on CIFS share**（在 CIFS 共享上添加文件）指定一个网络共享位置，然后按下表所述输入相应的信息。

表. 100: CIFS 共享凭据

文本框	说明
UNC Path (UNC 路径)	输入网络共享位置的路径。 如果此位置位于根目录，请定义专用文件夹名称（例如，Repository）。 路径必须以 \\ 开始。指定路径时，只能使用字母数字字符、连字符和句点（只用于分隔主机名和域）。字母 a 至 z 区分大小写。请勿使用空格。不允许使用其他符号或标点符号。
用户名	指定用于访问网络共享位置的用户名。
密码	指定用于访问网络共享位置的密码。

- 在 **Storage Configuration**（存储配置）区域中，单击 **More Details**（详细信息），然后根据下表中的说明输入存储位置的详细信息。

表. 101: 存储配置详细信息

文本框	说明
大小	设置存储位置的大小或容量。最小大小为 1 GB。默认值为 250 GB。可以从以下各项中选择： - GB - TB ① 注: 指定的大小不能超过卷的大小。 如果存储位置是使用 Windows XP 或 Windows 7 的新技术文件系统 (NTFS) 卷，则文件大小限制为 16 TB。 如果存储位置是使用 Windows 8、8.1、Windows 10 或 Windows Server 2012、2012 R2 的 NTFS 卷，文件大小限制为 256 TB。 ① 注: 要让 Rapid Recovery 验证操作系统，在目标存储位置必须安装 Windows Management Instrumentation (WMI)。
Write Caching Policy (写高速缓存策略)	写高速缓存策略控制 Windows Cache Manager 在存储库中的使用方式，并帮助调整存储库以便在不同配置下实现最佳性能。 请将其设置为以下值之一： - On (打开) - Off (关) - Sync (同步) 如果设置为默认值 On (打开)，则 Windows 将控制高速缓存。这适用于 Windows 10 以及 Windows Server 2012 和更高版本。 ① 注: 将写高速缓存策略设置为 On (打开) 可提高性能。如果您使用的是 Windows Server 2008 SP2 或 Windows Server 2008 R2 SP2，则建议的设置为 Off (关闭)。 如果设置为 Off (关闭)，则 Rapid Recovery 将控制高速缓存。

文本框	说明
	如果设置为 Sync（同步），则 Windows 将控制高速缓存以及同步输入/输出。
每扇区字节数	指定希望每个扇区包含的字节数。默认值为 512。
Average Bytes per Record（每个记录的平均字节数）	指定每个记录的平均字节数。默认值为 8192。

6 单击下一步。

如果您在步骤 1 中选择了 **Advanced（高级）** 选项，此时将显示 **Encryption（加密）** 页面。

- 14 另外，在 Encryption（加密）页面上，要启用加密，请选择 **Enable Encryption（启用加密）**。
在 Encryption（加密）页面中将显示 Encryption key（加密密钥）字段。

注: 如果启用加密，它将应用于此代理机器上所有受保护卷中的数据。您可以稍后从 **Rapid Recovery Core Console** 的 **Configuration（配置）** 选项卡更改设置。有关加密的更多信息，请参阅主题 [了解加密密钥](#)。

小心: **Rapid Recovery** 在密码块链 (CBC) 模式中使用 **AES 256 位加密** 和 **256 位密钥**。虽然使用加密是可选的，但是 **Dell** 强烈建议您建立加密密钥，并保护您定义的密码短语。请将密码短语保存在安全位置，因为它对于数据恢复至关重要。如果没有密码短语，将无法进行数据恢复。

- 15 如果您想使用已在此 **Rapid Recovery Core** 上定义的加密密钥加密这些受保护的机器，请选择 **Encrypt data using an existing Encryption key（使用现有的加密密钥加密数据）** 并从下拉菜单中选择相应的密钥。
继续执行 [步骤 17](#)。
- 16 如果您想要将加密密钥添加到 Core 并对这些受保护的机器应用该密钥，请根据下表中的说明输入信息。

表. 102: 加密密钥设置

文本框	说明
名称	输入加密密钥的名称。 加密密钥的名称必须包含介于 1 和 130 之间的字母数字字符。其中不能包含特殊字符，例如反斜杠、斜杠、管道、冒号、星号、引号、问号、左方括号或右方括号、& 符号或散列值。
说明	输入加密密钥的注释。 当从 Core Console 查看加密密钥时，此信息会显示在 Description（说明）字段中。
密码短语	输入用于控制访问的密码短语。 最佳做法是避免此表的名称说明中列出特殊字符。 密码短语记录在安全位置。Dell 支持部门无法恢复密码短语。一旦您创建加密密钥并将其应用于一个或多个受保护的机器，则一旦该密码短语丢失，您将无法恢复数据。
确认密码短语	重新输入刚输入的密码短语。

- 17 单击 **完成**。
Rapid Recovery 会将所选虚拟机及其主机添加到受保护机器的列表中。

访问受保护机器诊断

在 Rapid Recovery 中，您可以下载并查看单台受保护机器的诊断信息。此外，Rapid Recovery 可让您下载并查看 Core 的日志数据。

要访问日志，请参阅以下过程：

- [下载并查看 Core 日志文件](#)
- [下载并查看受保护计算机的日志文件](#)

下载并查看受保护计算机的日志文件

如果您的受保护计算机遇到任何错误或问题，您可以下载计算机日志进行查看或与您的 Dell Support 代表联系。

- 1 在 Core Console 的左侧导航区域中的“受保护计算机”菜单下，单击箭头以展开受保护计算机的上下文相关菜单。向下滚动到**更多**，展开该菜单，然后选择  **Agent 日志**。
此时将显示**下载 Agent 日志**页面。
- 2 在**下载 Agent 日志**页面上，单击  **单击此处以开始下载**。
- 3 在**正在打开 AgentAppRecovery.log**对话框中，执行以下操作之一：
 - 要打开日志文件，选择**打开方式**，然后选择应用程序（如记事本）来查看基于文本的日志文件，最后单击**确定**。
AgentAppRecovery.log 文件将用选定的应用程序打开。
 - 要将文件保存在本地，选择**保存文件**，然后单击**确定**。
AgentAppRecovery.log 文件将保存到您的“下载”文件夹。它可以使用任何文本编辑器打开。

下载并查看受保护计算机的日志文件

如果您的受保护计算机遇到任何错误或问题，您可以下载计算机日志进行查看或与您的 Dell Support 代表联系。

- 1 在 Core Console 的左侧导航区域中的“受保护计算机”菜单下，单击箭头以展开受保护计算机的上下文相关菜单。向下滚动到**更多**，展开该菜单，然后选择  **Agent 日志**。
此时将显示**下载 Agent 日志**页面。
- 2 在**下载 Agent 日志**页面上，单击  **单击此处开始下载**。
- 3 在**正在打开 AgentAppRecovery.log**对话框中，执行以下操作之一：
 - 要打开日志文件，选择**打开方式**，然后选择应用程序（如记事本）来查看基于文本的日志文件，最后单击**确定**。
AgentAppRecovery.log 文件将用选定的应用程序打开。
 - 要将文件保存在本地，选择**保存文件**，然后单击**确定**。
AgentAppRecovery.log 文件将保存到您的“下载”文件夹。它可以使用任何文本编辑器打开。

相关链接

[下载并查看 Core 日志文件](#)

查看机器状态和其他详细信息

完成此程序中的步骤，以查看机器的状态以及其他详细信息。

在 Rapid Recovery Core 控制台中，导航至要查看的受保护机器。

在 Summary（摘要）页面上将显示关于该机器的信息。显示的详细信息包括以下内容：

- 主机名
- Last Snapshot taken（创建的上一个快照）
- Next Snapshot scheduled（计划的下一个快照）
- Encryption status（加密状态）
- Version number（版本号）
如果机器上安装了 Exchange Server，还将显示关于服务器的详细信息，其中包括：
- 上次成功执行的安装性检查

- 上次成功执行的校验和检查
- Last Log Truncation performed（上次执行的日志截断）
还将显示关于此机器上所包含卷的详细信息，其中包括：
- 卷名称
- 计划
- Current Schedule（当前计划）
- Next Snapshot（下一个快照）
- File System type（文件系统类型）
- 总空间大小的空间使用情况
- 如果机器上安装了 SQL Server，还将显示关于服务器的详细信息，其中包括：

联机状态

- 名称
- Install Path（安装路径）
- Version（版本）
如果机器上安装了 Exchange Server，还将显示关于服务器和邮件存储区的详细信息，其中包括：
- Version（版本）
- Install Path（安装路径）
- Data Path（数据路径）
- Database Name（数据库名称）
- Exchange Databases Path（Exchange 数据库路径）
- Log File Path（日志文件路径）
- Log Prefix（日志前缀）
- System Path（系统路径）
- MailStore Type（邮件存储区类型）

管理机器

本部分介绍管理机器时可以执行的各种任务。主题包括：

- [移除机器](#)
- [从保护范围中移除群集](#)
- [查看机器的许可证信息](#)
- [下载并查看受保护计算机的日志文件](#)
- [将受保护群集节点转换为受保护机器](#)

移除机器

当在 Rapid Recovery Core 上从保护范围中移除某台机器时，您有两种选择：您可以保留恢复点到 RR Core，或者移除恢复点。如果保留恢复点，您将拥有被称为“仅恢复点”的机器。使用移除当前保护机器的恢复点，您可以在未来继续还原机器，但是仅可还原至保存恢复点捕捉的状态。

如果移除恢复点，本操作将删除之前的 Rapid Recovery Core 受保护机器的任何快照数据。

 **小心：**如果删除恢复点，您将无法恢复该机器的数据。

要从 Rapid Recovery 环境的保护范围中移除机器，请完成以下过程中的步骤。

- 1 从 Rapid Recovery Core Console，在左侧导航窗格的“受保护机器”下方，单击要移除的机器。
- 2 在相关机器的“摘要”页面上，单击**移除机器**。

- 3 在对话框中，如果您还想要从存储库中移除此机器的所有恢复点，请选择**移除恢复点**。
- 4 要确认您选择移除机器，请单击**是**。
Rapid Recovery 从保护范围中移除机器，并取消该机器的所有活动任务。

取消机器上的操作

您可以取消机器上当前正在执行的操作。可以指定仅取消当前快照，也可以指定取消所有当前操作（包括导出、复制等）。

- 1 在 Rapid Recovery Core Console 中，在“受保护计算机”下的左侧导航区域中，单击要取消操作的计算机。
- 2 单击**事件**。
- 3 单击最右边的“作业详细信息”图标以查看进行中的事件或您要取消的操作。
- 4 在“监控活动任务”对话框中，单击**取消**。

查看机器的许可证信息

您可以查看受保护计算机上安装的 Rapid Recovery Agent 软件的当前许可证状态信息。

- 1 在 Rapid Recovery Core Console 中，单击“受保护计算机”下要进行修改的计算机。
此时将显示所选计算机的**摘要**页面。
- 2 单击**设置**菜单。
此时将显示**设置**页面，其中显示所选计算机的配置设置。
- 3 单击**许可**链接，向下滚动“设置”页面以查看特定计算机的许可设置。
将显示“状态”屏幕，并显示关于产品许可的详细信息。

VM 导出

本节介绍如何导出恢复点以创建虚拟机。

关于使用 Rapid Recovery 导出至虚拟机

从 Rapid Recovery Core，您可以将恢复点从存储库导出到虚拟机。此过程（有时称为虚拟导出）是一种物理到虚拟 (P2V) 过程，它从恢复点创建虚拟机。虚拟机是受保护机器的可引导克隆。

① | 注: 使用的恢复点必须是完整的恢复点链的一部分。有关恢复点链的更多信息，请参阅主题**恢复点链和孤立恢复点**。

您可以从 Core Console 中的“Virtual Standby”页面或者通过选择 **VM 导出**（从按钮栏上的  **还原**下拉菜单中选择）来执行虚拟导出。

当您从 Rapid Recovery Core 执行虚拟导出时，您有两个选项：

- 您可以执行**一次性虚拟导出**，这表示恢复点信息中时间的单个快照。
- 您可以创建 **Virtual Standby**。使用 Virtual Standby，在从源机器捕获各个计划或强制快照后，Core 将持续更新您从所选恢复点创建的虚拟机快照。这样做将创建高可用性资源用于数据恢复。如果受保护机器出现故障，您可以引导虚拟机以快速暂时更换它，从而使您有时间恢复原始受保护机器，而不会造成较长停机时间。

下图显示将数据导出到虚拟机的典型部署。

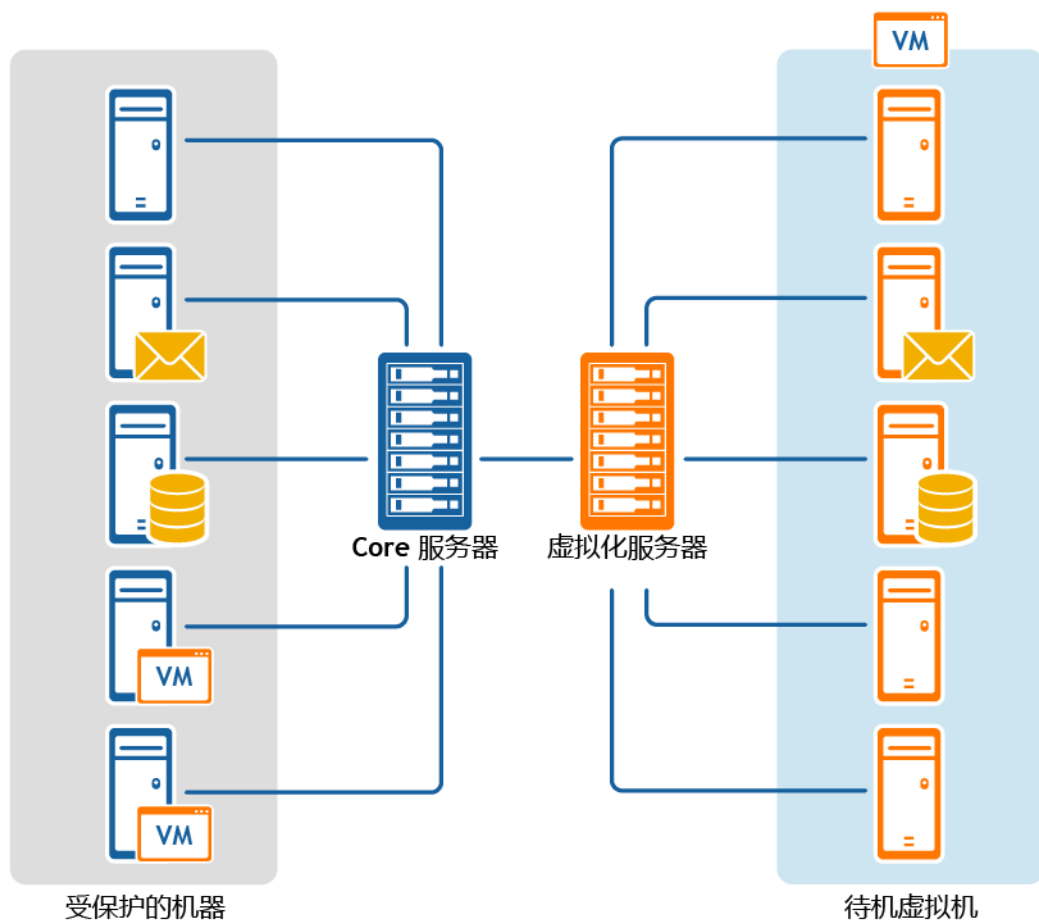


图 8: Virtual Standby 部署

① | 注: 在涉及复制的配置中, 所示的 **Core** 代表目标 **Core**。

当导出到虚拟机时, 将导出以下信息:

- 恢复点中的所有备份数据
- 原始受保护机器中的操作系统和设置

您可以为受保护的 Windows 或 Linux 机器执行恢复点虚拟导出到 VMware、ESXi、Hyper-V 和 VirtualBox。

① | 注: 对于 **ESXi**、**VMware Workstation** 或 **Hyper-V**, 虚拟机必须是这些虚拟机经过许可的版本, 而不能是试用版或免费版。

如果在两个 Core (源和目标) 之间设置了复制, 则在初始复制完成后, 只能从目标 Core 导出数据。

执行 ESXi 一次性导出

要执行 ESXi 一次性导出, 请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 按钮栏中, 单击**还原**下拉菜单, 然后单击**虚拟机导出**。
- 2 在“虚拟机导出向导”中, 选择**一次性导出**。
- 3 单击**下一步**。
- 4 在“计算机”页面上, 选择您想要导出的受保护计算机。

- 5 单击**下一步**。
- 6 在“恢复点”页面中，选择要导出的恢复点。
- 7 单击**下一步**。
- 8 在“导出向导”的“目标”页面中，在“恢复到虚拟机”下拉菜单中选择 **ESX(i)**。
- 9 根据下表中的说明输入用于访问虚拟机的参数，然后单击**下一步**。

表. 103: 虚拟机参数

选项	说明
主机名	输入主机名。
端口	输入主机端口。默认为 443。
用户名	输入用于登录到主机计算机的用户名。
密码	输入用于登录主机计算机的密码。

- 10 在“虚拟机选项”页面上，根据下表中的说明输入信息。

表. 104: 虚拟机选项

选项	说明
资源池	从下拉列表中选择资源池。
虚拟机配置位置	从下拉列表中选择数据存储。
虚拟机名称	输入虚拟机的名称。
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数量	希望用于已导出虚拟机的处理器 (CPU) 数量。最小值为 1。
每个处理器的 Core 数量	您希望每个处理器具有的 Core 数量。最小值为 1。
磁盘配置	从下列选项中选择磁盘配置类型： - 精简。精简配置将创建大小为原始卷上已用空间而不是整个卷大小的虚拟磁盘。例如，如果原始卷为 1 TB，但仅包含 2 GB 的已用空间，Rapid Recovery 将创建 2 GB 的虚拟磁盘。 - 完整。完整配置将创建大小与受保护服务器的原始卷相同的磁盘或卷，即使原始卷仅有一部分被使用。例如，如果卷大小为 1 TB，但仅包含 2 GB 已用空间，那么 Rapid Recovery 将创建 1 TB 的虚拟磁盘。
磁盘映射	从以下选项中指定磁盘映射类型： - Automatic（自动） - 手动 - 使用 VM
版本	从下拉式列表中选择用于创建虚拟机的 ESXi 版本。

- 11 单击**下一步**。
- 12 在“卷”页面中，选择要导出的卷，然后单击**下一步**。
- 13 在“摘要”页面中，单击**完成**以完成向导并开始导出。

 **注:** 您可以通过查看 **Virtual Standby** 或“事件”页面以监控导出状态和进度。

执行 ESXi 连续 (Virtual Standby) 导出

完成此过程中的步骤，以使用 Rapid Recovery 执行到 ESXi 虚拟机 (VM) 的连续导出。

1 在 Rapid Recovery Core Console 中，执行以下操作之一：

- 从 Core Console 的按钮栏中，单击  还原下拉菜单，然后选择 **VM 导出**。
 - 在“虚拟机导出向导”中，选择**连续（虚拟备用）**。
 - 单击**下一步**。
 - 从 Core Console 的图标栏上，单击  （虚拟备用）。
 - 在**虚拟备用**页面中，单击**添加**以启动“虚拟机导出向导”。
- 2 在“虚拟机导出向导”的**机器**页面中，选择要导出的受保护机器。
- 3 单击**下一步**。
- 4 在**恢复点**页面中，选择要用于导出的恢复点。
- 5 单击**下一步**。
- 6 在“导出向导”的**目标**页面中，在“恢复到虚拟机”下拉菜单中选择 **ESXi**。
- 7 根据下表中的说明输入用于访问虚拟机的信息，然后单击**下一步**。

表. 105: ESXi 凭据

选项	说明
主机名	输入主机名。
端口	输入主机端口。默认为 443。
用户名	输入用于登录主机的凭据。
密码	输入用于登录主机的凭据。

8 在 **Virtual Machine Options**（虚拟机选项）页面中，输入下表所述信息。

表. 106: 虚拟机选项

选项	说明
资源池	从下拉列表中选择资源池。
数据存储	从下拉列表中选择数据存储。
虚拟机名称	输入虚拟机名称。
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数量	要用于导出的虚拟机的处理器 (CPU) 数量。最小值为 1。
每个处理器的内核数	要用于每个处理器的内核数量。最小值为 1。
磁盘配置	从下列选项中选择磁盘配置类型：

选项	说明
	- 精简。精简配置可创建一个虚拟磁盘，其大小等于原始卷上已使用空间的大小，而不是整个卷大小。例如，如果原始卷为 1 TB，但仅包含 2 GB 的已使用空间，则 Rapid Recovery 将创建一个 2 GB 的虚拟磁盘。 - 完整。完整配置可创建一个新的磁盘或卷，其大小与受保护服务器的原始卷大小相同，即使原始卷仅有一部分正在使用。例如，如果原始卷为 1 TB 大小，但包含 2 GB 的已使用空间，则 Rapid Recovery 将创建一个 1 TB 的虚拟磁盘。
磁盘映射	酌情（自动、手动或利用 VM）指定磁盘映射类型。
版本	选择虚拟机的版本。
执行初始一次性导出	选择以便立即而不是在下个计划快照之后执行虚拟导出（可选）。

- 9 单击**下一步**。
- 10 在**卷**页面中，选择要导出的卷，然后单击**下一步**。
- 11 在**摘要**页面中，单击**完成**以完成向导并开始导出。

① **注：**可以通过查看“**虚拟备用**”或“**事件**”页面监控导出状态和进度。

执行 VMware Workstation 一次性导出

要执行 VMware Workstation 一次性导出，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的按钮栏中，单击**还原**下拉菜单，然后单击 **VM 导出**。
- 2 在“虚拟机导出向导”中，选择**一次性导出**。
- 3 单击**下一步**。
- 4 在“机器”窗格中选择要导出的受保护机器。
- 5 单击**下一步**。
- 6 在“恢复点”页面中，选择要用于导出的恢复点。
- 7 单击**下一步**。
- 8 在“导出向导”的“目标”页面中，在“恢复到虚拟机”下拉菜单中选择 **VMware Workstation**，然后单击**下一步**。
- 9 在“虚拟机选项”页面上，按照下表中的说明输入用于访问虚拟机的参数。

表. 107: 虚拟机参数

选项	说明
VM Machine Location (VM 机器位置)	指定要在其上面创建虚拟机的本地文件夹或网络共享的路径。 ① 注： 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效登录凭据。此帐户必须拥有该网络共享的读取和写入权限。
用户名	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效用户名。 - 如果输入本地路径，则不需输入用户名。
密码	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效密码。 - 如果输入本地路径，则不需输入密码。
虚拟机名称	输入即将创建的虚拟机的名称；例如 VM-0A1B2C3D4。

选项	说明
 注: 默认名称是源机器的名称。	
版本	指定虚拟机的 VMware Workstation 的版本。您可以选择： • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
RAM 的容量 (MB)	要指定虚拟机的内存使用量，请单击以下选项之一： • 使用与源机器相同容量的 RAM • 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数	要用于导出的虚拟机的处理器 (CPU) 数。最小值为 1。
每个处理器的核数	您想要每个处理器拥有的核数。最小值为 1。

- 10 单击**下一步**。
- 11 在“卷”页面中，选择要导出的卷，例如 C:\ 和 D:\，然后单击**下一步**。
- 12 在“摘要”页面中，单击**完成**以完成向导并开始导出。

 **注:** 您可以查看“**Virtual Standby**”或“**事件**”选项卡以监测导出状态和进度。

执行 VMware Workstation 连续 (Virtual Standby) 导出

完成此过程中的步骤，以使用 Rapid Recovery 执行到 VMWare Workstation 虚拟机 (VM) 的连续导出。

- 1 在 Rapid Recovery Core Console 中，执行以下操作之一：

- 从 Core Console 的按钮栏中，单击  **还原**下拉菜单，然后选择 **VM 导出**。
 - 1 在“虚拟机导出向导”中，选择**连续（虚拟备用）**。
 - 2 单击**下一步**。

- 从 Core Console 的图标栏上，单击  （虚拟备用）。
 - 在**虚拟备用**页面中，单击**添加**以启动“虚拟机导出向导”。

- 2 在“虚拟机导出向导”的**机器**页面中，选择要导出的受保护机器。
- 3 单击**下一步**。
- 4 在**恢复点**页面中，选择要用于导出的恢复点。
- 5 单击**下一步**。
- 6 在“虚拟机导出向导”的**目标**页面中，在“恢复到虚拟机”下拉菜单中选择 **VMware Workstation**，然后单击**下一步**。
- 7 在 **Virtual Machine Options（虚拟机选项）** 页面中，根据下表中的说明输入用于访问虚拟机的参数。

表. 108: 虚拟机参数

选项	说明
目标路径	指定要在其上面创建虚拟机的本地文件夹或网络共享的路径。

- 注:** 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效登录凭据。此帐户必须拥有该网络共享的读取和写入权限。

用户名	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效用户名。 - 如果输入本地路径，则不需输入用户名。
密码	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效密码。 - 如果输入本地路径，则不需输入密码。
虚拟机	输入即将创建的虚拟机的名称；例如 VM-0A1B2C3D4。 注: 默认名称是源机器的名称。
版本	指定虚拟机的 VMware Workstation 的版本。您可以选择： - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数量	要用于导出的虚拟机的处理器 (CPU) 数量。最小值为 1。
每个处理器的内核数	要用于每个处理器的内核数量。最小值为 1。

8 选择**执行初始一次性导出**以便立即而不是在下个计划快照之后执行虚拟导出。

9 单击**下一步**。

10 在**卷**页面中，选择要导出的卷，例如 C:\ 和 D:\，然后单击**下一步**。

11 在**摘要**页面中，单击**完成**以完成向导并开始导出。

- 注:** 可以通过查看“虚拟备用”或“事件”页面监控导出状态和进度。

执行 Hyper-V 一次性导出

要执行 Hyper-V 一次性导出，请完成以下过程中的步骤。

- 在 Rapid Recovery Core Console 的按钮栏中，单击**还原**下拉菜单，然后单击 **VM 导出**。
- 在“虚拟机导出向导”中，选择**一次性导出**。
- 单击**下一步**。
- 在**计算机**页面中，选择要导出的受保护机器。
- 单击**下一步**。
- 在**恢复点**页面中，选择要用于导出的恢复点。

- 7 单击**下一步**。
- 8 在**目标**页面中，从“导出到虚拟机”下拉菜单中选择 **Hyper-V**。
- 9 要导出到分配了 Hyper-V 角色的本地机器，请单击**使用本地机器**。
- 10 要表示 Hyper-V 服务器位于远程计算机上，请单击**远程主机**，然后按照下表中的说明输入远程主机的信息。

表. 109: 远程主机信息

文本框	说明
主机名	输入 Hyper-V 服务器的 IP 地址或主机名。它代表远程 Hyper-V 服务器的 IP 地址或主机名。
端口	输入机器的端口号。它代表 Core 与此机器进行通信时所使用的端口。
用户名	输入具有 Hyper-V 服务器工作站管理权限的用户的用户名。它用来指定虚拟机的登录凭据。
密码	输入具有 Hyper-V 服务器工作站管理权限的用户帐户的密码。它用来指定虚拟机的登录凭据。

- 11 单击**下一步**。
- 12 在**虚拟机选项**页面中的 **VM 机器位置** 文本框中，输入虚拟机的路径；例如 D:\export。此路径用来确定虚拟机的位置。

注: 您需要指定本地和远程 Hyper-V 服务器的虚拟机位置。此路径应该是 Hyper-V 服务器的有效本地路径。系统会自动创建非现存目录。不应尝试手动创建目录。不允许导出至共享文件夹（例如，导出到 \\data\share）。
- 13 在**虚拟机名称**文本框中，输入虚拟机的名称。
所输入的名称将显示在 Hyper-V Manager 控制台的虚拟机列表中。
- 14 要指定内存使用量，请单击以下选项之一：
 - **使用与源计算机相同容量的 RAM。** 选择此选项以确定虚拟机与源计算机使用的 RAM 容量相同。
 - **使用指定容量的 RAM。** 如果要指定 RAM 的容量（以 MB 为单位），请选择此选项。
最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
- 15 要指定磁盘格式，请在“磁盘格式”旁单击以下选项之一：
 - VHDX
 - VHD

注: 如果目标机器运行 Windows 8 (Windows Server 2012) 或更高版本，则 Hyper-V 导出支持 VHDX 磁盘格式。如果客户环境不支持 VHDX，则会禁用该选项。
如果导出到第 2 代 Hyper-V，仅支持 VHDX 磁盘格式。
- 16 要指定 Hyper-V 导出到哪一代，请单击下列选项之一：
 - 第 1 代
 - 第 2 代

注: 仅第 2 代支持安全启动选项。
- 17 为导出的 VM 指定相应的网络适配器。
- 18 在 **Volumes (卷)** 页面中，选择要导出的卷；例如 C:\。

注: 如果选定的卷比下列所示的应用程序支持的相应最大分配大，或超过可用空间容量，您将收到一个错误。

 - 对于 VHDX 磁盘格式，所选卷不得大于 64 TB。
 - 对于 VHD 磁盘格式，所选卷不得大于 2040 GB。
- 19 在**卷**页面中，单击**完成**以完成向导并开始导出。

注: 可以通过查看虚拟备用或事件页面监控导出状态和进度。

执行 Hyper-V 连续 (Virtual Standby) 导出

使用 Rapid Recovery 完成此过程中的步骤以执行连续导出到 Hyper-V 虚拟机 (VM)。

1 在 Rapid Recovery Core Console 中，执行以下操作之一：

- 在 Core Console 按钮栏中，单击按钮栏中的  还原下拉菜单，然后选择 **VM 导出**。
 - 在“虚拟机导出向导”中，选择**连续 (Virtual Standby)**。
 - 单击**下一步**。
 - 单击 Core Console 图标栏中的  (Virtual Standby)。
 - 在 **Virtual Standby** 页面中，单击**添加**以启动“虚拟机导出向导”。
- 2 在“虚拟机导出向导”的**计算机**页面中，选择您想要导出的受保护计算机。
- 3 单击**下一步**。
- 4 在**恢复点**页面中，选择要导出的恢复点。
- 5 单击**下一步**。
- 6 在**目标**页面中，在“导出到虚拟机”下拉菜单中，选择 **Hyper-V**，然后执行以下操作之一：
- 要导出到分配了 Hyper-V 角色的本地机器，请单击**使用本地机器**。
 - 要表明 Hyper-V 服务器位于远程计算机上，请单击**远程主机**，然后根据下表中的说明输入远程主机的参数。

表. 110: 远程主机信息

文本框	说明
主机名	输入 Hyper-V 服务器的 IP 地址或主机名。它代表远程 Hyper-V 服务器的 IP 地址或主机名。
端口	输入机器的端口号。它代表 Core 与此机器进行通信时所使用的端口。
用户名	输入具有 Hyper-V 服务器工作站管理权限的用户的用户名。它用来指定虚拟机的登录凭据。
密码	输入具有 Hyper-V 服务器工作站管理权限的用户帐户的密码。它用来指定虚拟机的登录凭据。

- 7 单击**下一步**。
- 8 在**虚拟机选项**页面的**虚拟机位置**文本框中，输入虚拟机的路径，例如 D:\export。此路径用来确定虚拟机的位置。
- ① 注:** 您需要指定本地和远程 **Hyper-V** 服务器的虚拟机位置。此路径应该是 **Hyper-V** 服务器的有效本地路径。系统会自动创建非现存目录。不应尝试手动创建目录。不允许导出至共享文件夹，（例如，\\data\share）。
- 9 在**虚拟机名称**对话框中，输入虚拟机的名称。
所输入的名称将显示在 Hyper-V Manager 控制台的虚拟机列表中。
- 10 要指定内存使用量，请单击以下选项之一：
- 使用与源计算机相同容量的 RAM**。选择此选项以识别虚拟计算机与源计算机之间相同的 RAM 使用情况。
 - 使用特定容量的 RAM**。如果您想要指定 RAM 的容量（以 MB 为单位），请选择此选项。
最小容量为 1024 MB，而该应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
- 11 要指定磁盘格式，请在“磁盘格式”旁单击以下选项之一：
- VHDX
 - VHD
- ① 注:** 如果目标机器运行 **Windows 8 (Windows Server 2012)** 或更高版本，则 **Hyper-V** 导出支持 **VHDX** 磁盘格式。如果客户环境不支持 **VHDX**，则会禁用该选项。
如果导出到第 2 代 Hyper-V，仅支持 **VHDX** 磁盘格式。
- 12 要指定 Hyper-V 导出到哪一代，请单击下列选项之一：
- 第 1 代

- 第 2 代

① | 注: 仅第 2 代支持安全启动选项。

13 为导出的 VM 指定相应的网络适配器。

14 在 **Volumes (卷)** 页面中, 选择要导出的卷; 例如 C:\。

① | 注: 如果选定的卷比下列所示的应用程序支持的相应最大分配大, 或超过可用空间容量, 您将收到一个错误。

- 对于 VHDX 磁盘格式, 所选卷不得大于 64 TB。
- 对于 VHD 磁盘格式, 所选卷不得大于 2040 GB。

15 选择**执行初始一次性导出**以便立即而不是在下个计划快照之后执行虚拟导出。

16 在**卷**页面中, 单击**完成**以完成向导并开始导出。

① | 注: 您可以通过查看 **Virtual Standby** 或事件页面以监控导出状态和进度。

执行 VirtualBox 一次性导出

要执行 VirtualBox 一次性导出, 请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的按钮栏中, 单击**还原**下拉菜单, 然后单击 **VM 导出**。
- 2 在“虚拟机导出向导”中, 选择**一次性导出**。
- 3 单击**下一步**。
- 4 在“机器”窗格中选择要导出的受保护机器。
- 5 单击**下一步**。
- 6 在“恢复点”页面中, 选择要用于导出的恢复点。
- 7 单击**下一步**。
- 8 在“导出向导”的“目标”页面中, 在“恢复到虚拟机”下拉菜单中选择 **VirtualBox**, 然后单击**下一步**。
- 9 在“虚拟机选项”页面中, 选择**使用 Windows 机器**。
- 10 根据下表中的说明, 输入用于访问虚拟机的参数。

表. 111: 虚拟机参数

选项	说明
虚拟机名称	输入要创建的虚拟机名称。 ① 注: 默认名称是源机器的名称。
目标路径	指定要创建虚拟机的本地或目标路径。 ① 注: 目标路径不得是根目录。如果指定网络共享路径, 则需要输入已在目标机器上注册的帐户的有效登录凭据 (用户名和密码)。此帐户必须拥有该网络共享的读取和写入权限。
内存	要指定虚拟机的内存使用量, 请单击以下选项之一: • 使用与源机器相同容量的 RAM • 使用指定容量的 RAM, 然后以 MB 为单位指定容量 最小容量为 1024 MB, 应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。

11 要指定虚拟机的用户帐户, 请选择**指定导出的虚拟机的用户帐户**, 然后输入以下信息。如果虚拟机中存在多个用户帐户, 则指虚拟机将注册的特定用户帐户。此用户帐户登录时, 仅此用户会在 VirtualBox 管理器中看到此虚拟机。如果未指定帐户, 则将通过 VirtualBox 针对 Windows 机器中的所有现有用户注册虚拟机。

- 用户名 - 输入注册虚拟机的用户名。
- 密码 - 输入此用户帐户的密码。

12 单击**下一步**。

- 13 在“卷”页面中，选择要导出的卷，例如 C:\ 和 D:\，然后单击下一步。
- 14 在“摘要”页面中，单击**完成**以完成向导并开始导出。

① | **注:** 您可以查看“**Virtual Standby**”或“**事件**”选项卡以监测导出状态和进度。

执行 VirtualBox 连续 (Virtual Standby) 导出

要执行此步骤，Core 计算机上必须安装 VirtualBox。

完成此过程中的步骤，以使用 Rapid Recovery 执行到 VirtualBox 虚拟机 (VM) 的连续导出。

- 1 在 Rapid Recovery Core Console 中，执行以下操作之一：



- 从 Core Console 的按钮栏中，单击 **还原** 下拉菜单，然后选择 **VM 导出**。

- 1 在“虚拟机导出向导”中，选择**连续（虚拟备用）**。 2 单击**下一步**。



- 从 Core Console 的图标栏上，单击 **虚拟备用**（虚拟备用）。
 - 在**虚拟备用**页面中，单击**添加**以启动“虚拟机导出向导”。

- 2 在“虚拟机导出向导”的**机器**页面中，选择要导出的受保护机器。
- 3 单击**下一步**。
- 4 在**恢复点**页面中，选择要用于导出的恢复点。
- 5 单击**下一步**。
- 6 在“导出向导”的**目标**页面中，在**恢复到虚拟机**下拉菜单中选择 **VirtualBox**。
- 7 在 **Virtual Machine Options**（虚拟机选项）页面中，选择 **Remote Linux Machine**（远程 Linux 机器）。
- 8 根据下表中的说明，输入有关虚拟机的信息。

表. 112: 移除 Linux 机器设置

选项	说明
VirtualBox 主机名	输入 VirtualBox 服务器的 IP 地址或主机名。此字段代表远程 VirtualBox 服务器的 IP 地址或主机名。
端口	输入机器的端口号。此端口号代表 Core 与此机器进行通信时所使用的端口。
虚拟机名称	输入要创建的虚拟机名称。 ① 注: 默认名称是源机器的名称。
目标路径	指定要创建虚拟机的目标路径。 ① 注: 建议从根目录创建根文件夹，以便虚拟机从根目录运行。如果未使用根目录，则将需要在设置导出之前在目标机器上手动创建目标文件夹。您还需要在导出后手动连接或加载虚拟机。
用户名	目标机器上的帐户的用户名，例如 root。
密码	目标机器上的用户帐户的密码。
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。

- 9 选择**执行初始一次性导出**以便立即而不是在下个计划快照之后执行虚拟导出。
- 10 单击**下一步**。

- 11 在**卷**页面中，选择要导出的数据所在的卷，然后单击**下一步**。
- 12 在**摘要**页面中，单击**完成**以完成向导并开始导出。
- ① **注:** 可以通过查看“**虚拟备用**”或“**事件**”页面监控导出状态和进度。

管理导出

如果您的 Core 已建立虚拟导出，则每个虚拟导出的配置参数将显示为**虚拟备用**页面上的一行。在这里，您可以查看当前已设置之导出的状态并管理您的虚拟备用机器。您可以添加虚拟备用、强制导出、暂停或恢复虚拟备用，或者移除连续导出的要求。

执行一次性导出时，该作业将列在**虚拟备用**页面的导出队列中。此时，您可以暂停、恢复或取消导出操作。

- ① **注:** Rapid Recovery 支持 Hyper-V 导出到 Window 8、Window 8.1、Windows Server 2012 和 2012 R2。

如果虚拟机已开机，则虚拟导出到虚拟备用 VM 不会发生。

要管理虚拟导出，请完成以下过程中的步骤。

- 1 在 Core Console 的图标栏上，单击 （虚拟备用）。
- 此时将显示**虚拟备用**页面。此处，您可以查看已保存导出设置的两个表。它们包含下表所述信息。

表. 113: 虚拟备用信息

列	说明
选择项目	对于摘要表中的每一行，您可以选择复选框以执行表前菜单选项列表中的操作。
状态指示器	“状态”列中的彩色球显示虚拟备用的状态。如果将鼠标悬停在彩色圆圈上，将显示状态条件。 - 绿色。虚拟备用已成功配置、处于活动状态且未暂停。下一快照完成之后紧接着执行下个导出。 - 黄色。虚拟备用暂停，但参数仍被定义并保存在 Core 中。但是，在执行新的传输后，不会自动启动导出作业，且此受保护机器将没有新的导出，直到状态发生改变。
机器名称	源机器的名称。
目标	数据导出的目标虚拟机和路径。
导出类型	导出的虚拟机平台类型，例如 ESXi、VMware、Hyper-V 或 VirtualBox。
上次导出	上次导出的日期和时间。 如果导出已添加但未完成，则会显示一条消息，以指明尚未执行导出。如果导出失败或被取消，则也会显示相应的消息。
设置	 下拉菜单可让您执行以下功能： 编辑。可让您编辑虚拟备用设置。 强制。强制执行虚拟导出。 暂停。暂停虚拟导出。仅在状态为“活动”时可用。 恢复。恢复虚拟导出。仅在状态为“已暂停”时可用。 移除。移除连续导出的要求。不会移除最近更新的已导出 VM。

表. 114: 导出队列信息

列	说明
选择项目	对于摘要表中的每一行，您可以选择复选框以执行表前菜单选项列表中的操作。
目标	数据导出的目标虚拟机和路径。
导出类型	导出的虚拟机平台类型，例如 ESXi、VMware、Hyper-V 或 VirtualBox。
计划类型	一次性或连续导出类型。
状态	导出进度，在进度条中以百分比显示。

- 要管理保存的导出设置，请选择导出，然后单击以下选项之一：
 - 编辑。** 打开**虚拟机导出向导至 VM 选项**页面。在这里，您可以更改已导出虚拟机的位置、更改虚拟机类型的版本，或者为导出指定 RAM 或处理器。要立即开始 VM 导出，请选择**执行初始一次性导出**。
 - 强制。** 强制执行新的导出。在 Virtual Standby 已暂停然后恢复时，此选项可能非常有用，这意味着导出作业只会在执行新传输后重新启动。如果不想等待新传输，则可以强制执行导出。
 - 暂停。** 暂停活动导出。
 - 恢复。** 在下个计划或强制快照时恢复持续导出的要求。
- 要从系统中移除导出，请选择该导出，然后单击**移除**。
该导出配置将从系统中永久移除。移除虚拟备用配置不会移除由于配置而导出的任何虚拟机。
- 要管理同时运行的导出数量，请执行以下操作：
 - 在“导出队列”中，单击**设置**。
 - 在**最大并发导出数**对话框中，输入您想要同时运行的导出的数量。默认数量为 5。
 - 单击**保存**。
- 要取消“导出队列”中列出的一次性导出或连续导出，请选择该导出，然后单击**取消**。
- 要添加新的 Virtual Standby 导出，您可以单击**添加**以启动“导出向导”。有关为特定虚拟机设置 Virtual Standby 的更多信息，请参阅以下主题之一：
 - [导出数据到 ESXi 虚拟机](#)
 - [导出数据到 VMware 工作站虚拟机](#)
 - [导出数据到 Hyper-V 虚拟机](#)
 - [导出数据到 VirtualBox 虚拟机](#)

导出数据到 ESXi 虚拟机

在 Rapid Recovery 中，您可以通过执行一次性导出或创建连续导出（适用于虚拟备用机）来将数据导出到 ESXi。请完成相应导出类型的以下过程中的步骤。

执行 ESXi 一次性导出

要执行 ESXi 一次性导出，请完成以下过程中的步骤。

- 在 Rapid Recovery Core Console 按钮栏中，单击**还原**下拉菜单，然后单击**虚拟机导出**。
- 在“虚拟机导出向导”中，选择**一次性导出**。
- 单击**下一步**。
- 在“计算机”页面上，选择您想要导出的受保护计算机。
- 单击**下一步**。
- 在“恢复点”页面中，选择要导出的恢复点。
- 单击**下一步**。

- 8 在“导出向导”的“目标”页面中，在“恢复到虚拟机”下拉菜单中选择 **ESX(i)**。
- 9 根据下表中的说明输入用于访问虚拟机的参数，然后单击**下一步**。

表. 115: 虚拟机参数

选项	说明
主机名	输入主机名。
端口	输入主机端口。默认为 443。
用户名	输入用于登录到主机计算机的用户名。
密码	输入用于登录主机计算机的密码。

- 10 在“虚拟机选项”页面上，根据下表中的说明输入信息。

表. 116: 虚拟机选项

选项	说明
资源池	从下拉列表中选择资源池。
虚拟机配置位置	从下拉列表中选择数据存储。
虚拟机名称	输入虚拟机的名称。
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数量	希望用于已导出虚拟机的处理器 (CPU) 数量。最小值为 1。
每个处理器的 Core 数量	您希望每个处理器具有的 Core 数量。最小值为 1。
磁盘配置	从下列选项中选择磁盘配置类型： - 精简。精简配置将创建大小为原始卷上已用空间而不是整个卷大小的虚拟磁盘。例如，如果原始卷为 1 TB，但仅包含 2 GB 的已用空间，Rapid Recovery 将创建 2 GB 的虚拟磁盘。 - 完整。完整配置将创建大小与受保护服务器的原始卷相同的磁盘或卷，即使原始卷仅有一部分被使用。例如，如果卷大小为 1 TB，但仅包含 2 GB 已用空间，那么 Rapid Recovery 将创建 1 TB 的虚拟磁盘。
磁盘映射	从以下选项中指定磁盘映射类型： - Automatic（自动） - 手动 - 使用 VM
版本	从下拉式列表中选择用于创建虚拟机的 ESXi 版本。

- 11 单击**下一步**。
- 12 在“卷”页面中，选择要导出的卷，然后单击**下一步**。
- 13 在“摘要”页面中，单击**完成**以完成向导并开始导出。

注: 您可以通过查看 **Virtual Standby** 或“事件”页面以监控导出状态和进度。

执行 ESXi 连续 (Virtual Standby) 导出

完成此过程中的步骤，以使用 Rapid Recovery 执行到 ESXi 虚拟机 (VM) 的连续导出。

1 在 Rapid Recovery Core Console 中，执行以下操作之一：

- 从 Core Console 的按钮栏中，单击  还原下拉菜单，然后选择 **VM 导出**。
 - 在“虚拟机导出向导”中，选择**连续（虚拟备用）**。
 - 单击**下一步**。
 - 从 Core Console 的图标栏上，单击  （虚拟备用）。
 - 在**虚拟备用**页面中，单击**添加**以启动“虚拟机导出向导”。
- 2 在“虚拟机导出向导”的**机器**页面中，选择要导出的受保护机器。
- 3 单击**下一步**。
- 4 在**恢复点**页面中，选择要用于导出的恢复点。
- 5 单击**下一步**。
- 6 在“导出向导”的**目标**页面中，在“恢复到虚拟机”下拉菜单中选择 **ESXi**。
- 7 根据下表中的说明输入用于访问虚拟机的信息，然后单击**下一步**。

表. 117: ESXi 凭据

选项	说明
主机名	输入主机名。
端口	输入主机端口。默认为 443。
用户名	输入用于登录主机的凭据。
密码	输入用于登录主机的凭据。

8 在 **Virtual Machine Options**（虚拟机选项）页面中，输入下表所述信息。

表. 118: 虚拟机选项

选项	说明
资源池	从下拉列表中选择资源池。
数据存储	从下拉列表中选择数据存储。
虚拟机名称	输入虚拟机名称。
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数量	要用于导出的虚拟机的处理器 (CPU) 数量。最小值为 1。
每个处理器的内核数	要用于每个处理器的内核数量。最小值为 1。
磁盘配置	从下列选项中选择磁盘配置类型： 精简。精简配置可创建一个虚拟磁盘，其大小等于原始卷上已使用空间的大小，而不是整个卷大小。例如，如果原始卷为 1 TB，但仅包含 2 GB 的已使用空间，则 Rapid Recovery 将创建一个 2 GB 的虚拟磁盘。

选项	说明
	完整。完整配置可创建一个新的磁盘或卷，其大小与受保护服务器的原始卷大小相同，即使原始卷仅有一部分正在使用。例如，如果原始卷为 1 TB 大小，但包含 2 GB 的已使用空间，则 Rapid Recovery 将创建一个 1 TB 的虚拟磁盘。
磁盘映射	酌情（自动、手动或利用 VM）指定磁盘映射类型。
版本	选择虚拟机的版本。
执行初始一次性导出	选择以便立即而不是在下个计划快照之后执行虚拟导出（可选）。

- 单击**下一步**。
- 在**卷**页面中，选择要导出的卷，然后单击**下一步**。
- 在**摘要**页面中，单击**完成**以完成向导并开始导出。

① | 注: 可以通过查看“虚拟备用”或“事件”页面监控导出状态和进度。

导出数据到 VirtualBox 虚拟机

在 Rapid Recovery 中，您可以通过执行一次性导出或创建连续导出（适用于 Virtual Standby）来将数据导出到“Hyper-V 导出”。

① | 注: 当前不支持对 **Windows 10** 受保护机器执行 **VirtualBox** 导出。

请完成相应导出类型的以下过程中的步骤。

① | 注: 要执行此类导出，应在 **Core** 机器上安装 **VirtualBox**。**Windows** 主机支持 **Virtual Box 4.2.18** 或更高版本。

执行 VirtualBox 一次性导出

要执行 VirtualBox 一次性导出，请完成以下过程中的步骤。

- 在 Rapid Recovery Core Console 的按钮栏中，单击**还原**下拉菜单，然后单击 **VM 导出**。
- 在“虚拟机导出向导”中，选择**一次性导出**。
- 单击**下一步**。
- 在“机器”窗格中选择要导出的受保护机器。
- 单击**下一步**。
- 在“恢复点”页面中，选择要用于导出的恢复点。
- 单击**下一步**。
- 在“导出向导”的“目标”页面中，在“恢复到虚拟机”下拉菜单中选择 **VirtualBox**，然后单击**下一步**。
- 在“虚拟机选项”页面中，选择**使用 Windows 机器**。
- 根据下表中的说明，输入用于访问虚拟机的参数。

表. 119: 虚拟机参数

选项	说明
虚拟机名称	输入要创建的虚拟机名称。 ① 注: 默认名称是源机器的名称。
目标路径	指定要创建虚拟机的本地或目标路径。 ① 注: 目标路径不得是根目录。如果指定网络共享路径，则需要输入已在目标机器上注册的帐户的有效登录凭据（用户名和密码）。此帐户必须拥有该网络共享的读取和写入权限。

选项	说明
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
11	要指定虚拟机的用户帐户，请选择 指定导出的虚拟机的用户帐户 ，然后输入以下信息。如果虚拟机中存在多个用户帐户，则指虚拟机将注册的特定用户帐户。此用户帐户登录时，仅此用户会在 VirtualBox 管理器中看到此虚拟机。如果未指定帐户，则将通过 VirtualBox 针对 Windows 机器中的所有现有用户注册虚拟机。 - 用户名 - 输入注册虚拟机的用户名。 - 密码 - 输入此用户帐户的密码。
12	单击 下一步 。
13	在“卷”页面中，选择要导出的卷，例如 C:\ 和 D:\，然后单击 下一步 。
14	在“摘要”页面中，单击 完成 以完成向导并开始导出。

 **注：**您可以查看“**Virtual Standby**”或“**事件**”选项卡以监测导出状态和进度。

执行 VirtualBox 连续 (Virtual Standby) 导出

要执行此步骤，Core 计算机上必须安装 VirtualBox。

完成此过程中的步骤，以使用 Rapid Recovery 执行到 VirtualBox 虚拟机 (VM) 的连续导出。

1 在 Rapid Recovery Core Console 中，执行以下操作之一：

- 从 Core Console 的按钮栏中，单击  **还原**下拉菜单，然后选择 **VM 导出**。
 - 在“虚拟机导出向导”中，选择**连续（虚拟备用）**。
 - 单击**下一步**。

- 从 Core Console 的图标栏上，单击 （虚拟备用）。
 - 在**虚拟备用**页面中，单击**添加**以启动“虚拟机导出向导”。

- 在“虚拟机导出向导”的**机器**页面中，选择要导出的受保护机器。
- 单击**下一步**。
- 在**恢复点**页面中，选择要用于导出的恢复点。
- 单击**下一步**。
- 在“导出向导”的**目标**页面中，在**恢复到虚拟机**下拉菜单中选择 **VirtualBox**。
- 在 **Virtual Machine Options**（虚拟机选项）页面中，选择 **Remote Linux Machine**（远程 Linux 机器）。
- 根据下表中的说明，输入有关虚拟机的信息。

表. 120: 移除 Linux 机器设置

选项	说明
VirtualBox 主机名	输入 VirtualBox 服务器的 IP 地址或主机名。此字段代表远程 VirtualBox 服务器的 IP 地址或主机名。
端口	输入机器的端口号。此端口号代表 Core 与此机器进行通信时所使用的端口。
虚拟机名称	输入要创建的虚拟机名称。  注：默认名称是源机器的名称。
目标路径	指定要创建虚拟机的目标路径。

选项	说明
注: 建议从根目录创建根文件夹，以便虚拟机从根目录运行。如果未使用根目录，则将需要在设置导出之前在目标机器上手动创建目标文件夹。您还需要在导出后手动连接或加载虚拟机。	
用户名	目标机器上的帐户的用户名，例如 root。
密码	目标机器上的用户帐户的密码。
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。

- 选择**执行初始一次性导出**以便立即而不是在下个计划快照之后执行虚拟导出。
- 单击**下一步**。
- 在**卷**页面中，选择要导出的数据所在的卷，然后单击**下一步**。
- 在**摘要**页面中，单击**完成**以完成向导并开始导出。

注: 可以通过查看“虚拟备用”或“事件”页面监控导出状态和进度。

导出数据到 VMware 工作站虚拟机

在 Rapid Recovery 中，您可以通过执行一次性导出，或创建连续导出（适用于 Virtual Standby）将数据导出到 VMware 工作站。请完成相应导出类型的以下过程中的步骤。

执行 VMware Workstation 一次性导出

要执行 VMware Workstation 一次性导出，请完成以下过程中的步骤。

- 在 Rapid Recovery Core Console 的按钮栏中，单击**还原**下拉菜单，然后单击 **VM 导出**。
- 在“虚拟机导出向导”中，选择**一次性导出**。
- 单击**下一步**。
- 在“机器”窗格中选择要导出的受保护机器。
- 单击**下一步**。
- 在“恢复点”页面中，选择要用于导出的恢复点。
- 单击**下一步**。
- 在“导出向导”的“目标”页面中，在“恢复到虚拟机”下拉菜单中选择 **VMware Workstation**，然后单击**下一步**。
- 在“虚拟机选项”页面上，按照下表中的说明输入用于访问虚拟机的参数。

表. 121: 虚拟机参数

选项	说明
VM Machine Location（VM 机器位置） 注: 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效登录凭据。此帐户必须拥有该网络共享的读取和写入权限。	
用户名	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效用户名。 - 如果输入本地路径，则不需输入用户名。

选项	说明
密码	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效密码。 - 如果输入本地路径，则不需输入密码。
虚拟机名称	输入即将创建的虚拟机的名称；例如 VM-0A1B2C3D4。 注: 默认名称是源机器的名称。
版本	指定虚拟机的 VMware Workstation 的版本。您可以选择： - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
RAM 的容量 (MB)	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数	要用于导出的虚拟机的处理器 (CPU) 数。最小值为 1。
每个处理器的核数	您想要每个处理器拥有的核数。最小值为 1。

- 10 单击**下一步**。
- 11 在“卷”页面中，选择要导出的卷，例如 C:\ 和 D:\，然后单击**下一步**。
- 12 在“摘要”页面中，单击**完成**以完成向导并开始导出。

注: 您可以查看“Virtual Standby”或“事件”选项卡以监测导出状态和进度。

执行 VMware Workstation 连续 (Virtual Standby) 导出

完成此过程中的步骤，以使用 Rapid Recovery 执行到 VMWare Workstation 虚拟机 (VM) 的连续导出。

- 1 在 Rapid Recovery Core Console 中，执行以下操作之一：

- 从 Core Console 的按钮栏中，单击  **还原** 下拉菜单，然后选择 **VM 导出**。
- 1 在“虚拟机导出向导”中，选择**连续（虚拟备用）**。
- 2 单击**下一步**。

- 从 Core Console 的图标栏上，单击  （虚拟备用）。
- 在**虚拟备用**页面中，单击**添加**以启动“虚拟机导出向导”。

- 2 在“虚拟机导出向导”的**机器**页面中，选择要导出的受保护机器。
- 3 单击**下一步**。
- 4 在**恢复点**页面中，选择要用于导出的恢复点。
- 5 单击**下一步**。
- 6 在“虚拟机导出向导”的**目标**页面中，在“恢复到虚拟机”下拉菜单中选择 **VMware Workstation**，然后单击**下一步**。
- 7 在 **Virtual Machine Options（虚拟机选项）** 页面中，根据下表中的说明输入用于访问虚拟机的参数。

表. 122: 虚拟机参数

选项	说明
目标路径	指定要在其上面创建虚拟机的本地文件夹或网络共享的路径。 <i>注:</i> 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效登录凭据。此帐户必须拥有该网络共享的读取和写入权限。
用户名	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效用户名。 - 如果输入本地路径，则不需输入用户名。
密码	输入用于导出的网络位置的登录凭据。 - 如果指定了网络共享路径，则需要输入已在目标机器上注册的帐户的有效密码。 - 如果输入本地路径，则不需输入密码。
虚拟机	输入即将创建的虚拟机的名称；例如 VM-0A1B2C3D4。 <i>注:</i> 默认名称是源机器的名称。
版本	指定虚拟机的 VMware Workstation 的版本。您可以选择： - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
内存	要指定虚拟机的内存使用量，请单击以下选项之一： - 使用与源机器相同容量的 RAM - 使用指定容量的 RAM，然后以 MB 为单位指定容量 最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。
处理器数量	要用于导出的虚拟机的处理器 (CPU) 数量。最小值为 1。
每个处理器的内核数	要用于每个处理器的内核数量。最小值为 1。

8 选择**执行初始一次性导出**以便立即而不是在下个计划快照之后执行虚拟导出。

9 单击**下一步**。

10 在**卷**页面中，选择要导出的卷，例如 C:\ 和 D:\，然后单击**下一步**。

11 在**摘要**页面中，单击**完成**以完成向导并开始导出。

注: 可以通过查看“虚拟备用”或“事件”页面监控导出状态和进度。

导出数据到 Hyper-V 虚拟机

在 Rapid Recovery 中，您可以通过执行一次性导出或创建连续导出（适用于 Virtual Standby）来将数据导出到“Hyper-V 导出”。

Rapid Recovery 支持对以下主机使用第 1 代 Hyper-V 导出：

- Windows 8
- Windows 8.1

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Rapid Recovery 支持对以下主机使用第 2 代 Hyper-V 导出：

- Windows 8.1
- Windows Server 2012 R2

① | 注：并非所有受保护的机器都可以导出到第二代 Hyper-V 主机。

仅限具有以下统一可扩展固件接口 (UEFI) 操作系统的受保护机器支持虚拟导出到第二代 Hyper-V 主机：

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012 R2 (UEFI)

① | 注：如果 Hyper-V 主机没有分配足够的 RAM 以执行导出，则 Hyper-V 导出到第二代 VM 可能会失败。

请完成相应导出类型的以下过程中的步骤。

执行 Hyper-V 一次性导出

要执行 Hyper-V 一次性导出，请完成以下过程中的步骤。

- 1 在 Rapid Recovery Core Console 的按钮栏中，单击**还原**下拉菜单，然后单击 **VM 导出**。
- 2 在“虚拟机导出向导”中，选择**一次性导出**。
- 3 单击**下一步**。
- 4 在**计算机**页面中，选择要导出的受保护机器。
- 5 单击**下一步**。
- 6 在**恢复点**页面中，选择要用于导出的恢复点。
- 7 单击**下一步**。
- 8 在**目标**页面中，从“导出到虚拟机”下拉菜单中选择 **Hyper-V**。
- 9 要导出到分配了 Hyper-V 角色的本地机器，请单击**使用本地机器**。
- 10 要表示 Hyper-V 服务器位于远程计算机上，请单击**远程主机**，然后按照下表中的说明输入远程主机的信息。

表. 123: 远程主机信息

文本框	说明
主机名	输入 Hyper-V 服务器的 IP 地址或主机名。它代表远程 Hyper-V 服务器的 IP 地址或主机名。
端口	输入机器的端口号。它代表 Core 与此机器进行通信时所使用的端口。
用户名	输入具有 Hyper-V 服务器工作站管理权限的用户的用户名。它用来指定虚拟机的登录凭据。
密码	输入具有 Hyper-V 服务器工作站管理权限的用户帐户的密码。它用来指定虚拟机的登录凭据。

- 11 单击**下一步**。
- 12 在**虚拟机选项**页面中的 **VM 机器位置**文本框中，输入虚拟机的路径；例如 D:\export。此路径用来确定虚拟机的位置。

① | 注：您需要指定本地和远程 Hyper-V 服务器的虚拟机位置。此路径应该是 Hyper-V 服务器的有效本地路径。系统会自动创建非现存目录。不应尝试手动创建目录。不允许导出至共享文件夹（例如，导出到 \\data\share）。
- 13 在**虚拟机名称**文本框中，输入虚拟机的名称。
 所输入的名称将显示在 Hyper-V Manager 控制台的虚拟机列表中。

14 要指定内存使用量，请单击以下选项之一：

- **使用与源计算机相同容量的 RAM。** 选择此选项以确定虚拟机与源计算机使用的 RAM 容量相同。
- **使用指定容量的 RAM。** 如果要指定 RAM 的容量（以 MB 为单位），请选择此选项。
最小容量为 1024 MB，应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。

15 要指定磁盘格式，请在“磁盘格式”旁单击以下选项之一：

- VHDX
- VHD

① 注：如果目标机器运行 **Windows 8 (Windows Server 2012)** 或更高版本，则 **Hyper-V** 导出支持 **VHDX** 磁盘格式。如果客户环境不支持 **VHDX**，则会禁用该选项。
如果导出到第 2 代 Hyper-V，仅支持 **VHDX** 磁盘格式。

16 要指定 Hyper-V 导出到哪一代，请单击下列选项之一：

- 第 1 代
- 第 2 代

① 注：仅第 2 代支持安全启动选项。

17 为导出的 VM 指定相应的网络适配器。

18 在 **Volumes (卷)** 页面中，选择要导出的卷；例如 C:\。

① 注：如果选定的卷比下列所示的应用程序支持的相应最大分配大，或超过可用空间容量，您将收到一个错误。

- 对于 **VHDX** 磁盘格式，所选卷不得大于 64 TB。
- 对于 **VHD** 磁盘格式，所选卷不得大于 2040 GB。

19 在 **卷** 页面中，单击 **完成** 以完成向导并开始导出。

① 注：可以通过查看虚拟备用或事件页面监控导出状态和进度。

执行 Hyper-V 连续 (Virtual Standby) 导出

使用 Rapid Recovery 完成此过程中的步骤以执行连续导出到 Hyper-V 虚拟机 (VM)。

1 在 Rapid Recovery Core Console 中，执行以下操作之一：

- 在 Core Console 按钮栏中，单击按钮栏中的  还原下拉菜单，然后选择 **VM 导出**。

1 在“虚拟机导出向导”中，选择 **连续 (Virtual Standby)**。

2 单击 **下一步**。

- 单击 Core Console 图标栏中的  (Virtual Standby)。

- 在 **Virtual Standby** 页面中，单击 **添加** 以启动“虚拟机导出向导”。

2 在“虚拟机导出向导”的 **计算机** 页面中，选择您想要导出的受保护计算机。

3 单击 **下一步**。

4 在 **恢复点** 页面中，选择要导出的恢复点。

5 单击 **下一步**。

6 在 **目标** 页面中，在“导出到虚拟机”下拉菜单中，选择 **Hyper-V**，然后执行以下操作之一：

- 要导出到分配了 Hyper-V 角色的本地机器，请单击 **使用本地机器**。
- 要表明 Hyper-V 服务器位于远程计算机上，请单击 **远程主机**，然后根据下表中的说明输入远程主机的参数。

表. 124: 远程主机信息

文本框	说明
主机名	输入 Hyper-V 服务器的 IP 地址或主机名。它代表远程 Hyper-V 服务器的 IP 地址或主机名。
端口	输入机器的端口号。它代表 Core 与此机器进行通信时所使用的端口。
用户名	输入具有 Hyper-V 服务器工作站管理权限的用户的用户名。它用来指定虚拟机的登录凭据。
密码	输入具有 Hyper-V 服务器工作站管理权限的用户帐户的密码。它用来指定虚拟机的登录凭据。

7 单击**下一步**。

8 在**虚拟机选项**页面的**虚拟机位置**文本框中，输入虚拟机的路径，例如 `D:\export`。此路径用来确定虚拟机的位置。

① 注: 您需要指定本地和远程 Hyper-V 服务器的虚拟机位置。此路径应该是 Hyper-V 服务器的有效本地路径。系统会自动创建非现存目录。不应尝试手动创建目录。不允许导出至共享文件夹，（例如，`\\data\share`）。

9 在**虚拟机名称**对话框中，输入虚拟机的名称。

所输入的名称将显示在 Hyper-V Manager 控制台的虚拟机列表中。

10 要指定内存使用量，请单击以下选项之一：

- **使用与源计算机相同容量的 RAM。** 选择此选项以识别虚拟计算机与源计算机之间相同的 RAM 使用情况。
- **使用特定容量的 RAM。** 如果您想要指定 RAM 的容量（以 MB 为单位），请选择此选项。
最小容量为 1024 MB，而该应用程序允许的最大容量为 65536 MB。内存使用量的最大容量受主机可用 RAM 容量限制。

11 要指定磁盘格式，请在“磁盘格式”旁单击以下选项之一：

- VHDX
- VHD

① 注: 如果目标机器运行 **Windows 8 (Windows Server 2012)** 或更高版本，则 Hyper-V 导出支持 VHDX 磁盘格式。如果客户环境不支持 VHDX，则会禁用该选项。

如果导出到第 2 代 Hyper-V，仅支持 VHDX 磁盘格式。

12 要指定 Hyper-V 导出到哪一代，请单击下列选项之一：

- 第 1 代
- 第 2 代

① 注: 仅第 2 代支持安全启动选项。

13 为导出的 VM 指定相应的网络适配器。

14 在 **Volumes (卷)** 页面中，选择要导出的卷；例如 `C:\`。

① 注: 如果选定的卷比下列所示的应用程序支持的相应最大分配大，或超过可用空间容量，您将收到一个错误。

- 对于 VHDX 磁盘格式，所选卷不得大于 64 TB。
- 对于 VHD 磁盘格式，所选卷不得大于 2040 GB。

15 选择**执行初始一次性导出**以便立即而不是在下个计划快照之后执行虚拟导出。

16 在**卷**页面中，单击**完成**以完成向导并开始导出。

① 注: 您可以通过查看 **Virtual Standby** 或事件页面以监控导出状态和进度。

管理老化数据

本节介绍如何管理保存到您存储库的老化快照数据。它包括有关保留您存储库中的恢复点、保留策略以及汇总恢复点以节省空间所导致过程的信息。它介绍了将恢复点从您的存储库重新放置到 Dell DR 备份和重复数据消除设备上的新能力。

本节还介绍如何存档数据以进行不会汇总的长期存储，以及如何访问已存档的恢复点。

关于 Rapid Recovery 数据保留和存档

您的 Core 每次捕获快照时，数据都会作为恢复点保存到您的存储库中。恢复点随着时间推移自然累积。Core 使用保留策略以确定快照数据保留在存储库中的时长。在每夜作业的汇总过程中，Core 会实施保留策略以减少使用的存储空间量。在汇总过程中，每个恢复点的日期会与最新恢复点的日期进行比较。然后，Core 会组合或“汇总”较旧的恢复点。随时间推移，当最旧的恢复点的保留时间已超出了最长保留期时，较旧的恢复点最终会替换为较新的恢复点。

要保留在其他情况下会被组合并最终删除的恢复点，您可以从 Core Console 创建存档。存档是一个文件，其中包含创建存档时 Core 上受保护机器的整套恢复点。

您可将存档存储在文件系统中，或云中的存储帐户上。

如果您需要访问恢复点中的数据，您可以在未来附加（对于 Rapid Recovery 6.x 和更高版本）或导入存档，从而将这些恢复点还原到您的存储库。然后，就像对 Core 中当前的任何其他恢复点一样，您可以对该数据执行相同的操作。

① 注: 由于 Core 可识别存档中恢复点的原始日期，可能会在下次每夜作业期间再次汇总或删除导入的恢复点。如果要保留较旧的恢复点，您可以为相关机器禁用汇总，也可以延长保留期。

管理保留策略

保留策略是一组规则，说明开始回滚恢复点前，Core 保留这些恢复点的时长。保留策略可设置为基于小时、天、周、月和年回滚。您可设置六条规则（默认策略设置五条规则）。

由于您可每 5 分钟备份一次，因此保留策略中的第一条规则通常设置保留所有恢复点的时长。例如，如果您每十五分钟备份一次机器，则该机器每天会在存储库中保存 96 个恢复点，直至回滚开始。如果不管您的保留策略，大量的数据将快速充满您的存储库。

① 注: 管理员应留意会影响网络通信的频繁备份。其他影响网络通信的因素包括其他传输（如复制）、数据的变化率、网络硬件、线缆和交换机。

Core 最初预设为默认保留策略。默认策略工作保留：

- 所有恢复点保留三天
- 每小时一个恢复点，保留两天
- 每天一个恢复点，保留四天
- 每周一个恢复点，保留三周
- 每月一个恢复点，保留两个月
- 每年一个恢复点，保留 X 年（默认策略中禁用）。

根据该默认策略，最旧的恢复点通常为 92 天前。超过默认策略原始日期的数据将被删除。

以 Core 级别设置保留策略将自动应用至所有 Core 保护的机器。您可更改默认策略以满足您的需要。

对于任何机器，您也可创建自定义保留策略。以机器级别设置策略，您可指定默认 Core 策略以外的不同保留策略。要了解配置保留策略的更多信息，请参阅 [配置 Core 默认保留策略设置](#) 和 [自定义受保护机器的保留策略设置](#)。

配置 Core 默认保留策略设置

Core 的保留策略指定受保护机器的恢复点在存储库中存储的时长。

Core 保留策略是由合成流程执行的，该流程作为运行夜间作业的一个组件执行。然后，超出在保留策略中所指定的该期限的恢复点被“合成”（合并）至覆盖较粗粒度期间的恢复点。基于每夜应用该保留策略将导致持续合成旧有备份。这最终会导致基于保留策略中指定的要求，删除最旧的恢复点。

可对源和目标 Core 配置不同的保留设置。

① 注: 本主题特定用于 **Rapid Recovery Core** 中的自定义保留策略设置。当您在 **Core** 中保存自定义保留策略设置时，将建立可应用于所有受此 **Core** 保护的机器的默认保留策略设置。要了解为单独受保护机器自定义保留策略设置的更多信息，请参阅 [自定义受保护机器的保留策略设置](#)。

- 1 导航至 Rapid Recovery Core 控制台。
- 2 在图标栏中单击 （设置），然后执行以下任一操作：
 - 从 Settings（设置）页面左侧的 Core 设置列表中单击 **Nightly Jobs（每夜作业）**。
 - 向下滚动 Settings（设置）页面的右侧，直至您看到 **Nightly Jobs（每夜作业）** 标题。随即显示 Nightly Jobs（每夜作业）Core 设置。
- 3 在 **Nightly Jobs（每夜作业）** 下方单击  **Change（更改）**。此时将显示 **Nightly Jobs（每夜作业）** 对话框。
- 4 要根据需要指定保留备份数据的时间间隔，请在 Nightly Jobs（每夜作业）窗格中，选择 **Rollup（前滚）**，然后单击 **Settings（设置）**。此时会显示 **Configuration（配置）** 对话框的 Core default retention policy（使用 Core 默认保留策略）。
- 5 要随时将 Core 保留策略设置恢复至默认值，请在 Configuration（配置）对话框底部单击 **Restore Defaults（恢复默认值）**，然后单击 **Yes（是）** 确认。
所有设置恢复至 **步骤 6** 中表格所述的默认值。
- 6 要定义保留策略，请首先指定决定初始备份快照保留时长的主要设置，然后继续定义级联前滚集要求，用于确定应对恢复点执行前滚的间隔时间。
下表介绍了保留策略选项。

表. 125: 默认保留策略的计划选项

文本框	说明
Keep all Recovery Points for （保留所有恢复点）n [retention time period]	指定恢复点的保留期限。 输入代表保留期限的数字，然后选择时间期限。默认值为 3 天。 您可选择：Days（天）、Weeks（周）、Months（月），或 Years（年）
...and then keep one Recovery Point per hour for（...然后每小 时将一个恢复点保留为）n [retention time period]	提供更具体的保留期限。它用作主设置的一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 2 天。 您可选择：Days（天）、Weeks（周）、Months（月），或 Years（年）
...and then keep one Recovery Point per day for（...然后每天 将一个恢复点保留为）n [retention time period]	提供更具体的保留期限。此设置用作一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 4 天。 您可选择：Days（天）、Weeks（周）、Months（月），或 Years（年）
...and then keep one Recovery Point per week for（...然后每 周将一个恢复点保留为）n [retention time period]	提供更具体的保留期限。此设置用作一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 3 周。 您可选择：Weeks（周）、Months（月），或 Years（年）
...and then keep one Recovery Point per month for（...然后每	提供更具体的保留期限。此设置用作一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 2 月。

文本框	说明
月将一个恢复点保留为) n [retention time period]	您可选择: Months (月), 或 Years (年)
...and then keep one Recovery Point per year for (...然后每年将一个恢复点保留为) n [retention time period]	输入代表保留期限的数字, 然后选择时间期限。 您可以选择: Years (年)

最旧的恢复点将通过保留策略设置决定。

下面是如何计算保留期限的示例。

保留所有恢复点 3 天。

...然后每小时将一个恢复点保留 3 天

...然后每天将一个恢复点保留 4 天

...然后每周将一个恢复点保留 3 周

...然后每月将一个恢复点保留 2 个月

...然后每月将一个恢复点保留 1 年

在此示例中，最旧恢复点的期限为 1 年、4 个月又 6 天。

- 对保留策略设置满意后，单击 **Save**（保存）。
Configuration（配置）对话框关闭。
- 在 **Nightly Jobs**（每夜作业）对话框中，单击 **OK**（确定）。
Nightly Jobs（每夜作业）对话框关闭。您定义的保留策略将在每夜前滚过程中应用。

为任何单独的受保护机器指定保留策略时您也可应用这些设置。要了解为受保护机器设置保留策略的更多信息，请参阅 [自定义受保护机器的保留策略设置](#)。

自定义受保护机器的保留策略设置

受保护机器的保留策略指定了多长时间将恢复点保存在存储库中。通常情况下，每台受保护机器使用为 Core 建立的默认保留策略，除非您按本程序中所述指定一个自定义保留策略。

使用本程序定义自定义受保护机器（包括复制的机器）的保留策略。

- 从 Rapid Recovery Core 控制台的 Protected Machines（受保护机器）菜单中，单击要修改的机器的名称。
随即显示所选机器的 **Summary**（摘要）页面。
- 单击 **Settings**（设置）菜单。
随即显示 **Settings**（设置）页面，显示所选机器的配置设置。
- 或者，也可单击 **Nightly Jobs**（每夜作业）链接，以在 Settings（设置）页面中向下滚动，以查看每夜作业设置。
- 在 Nightly Jobs（每夜作业）标题下，单击  **Change**（更改）。
此时将显示 **Nightly Jobs**（每夜作业）对话框。
- 要指定保留所需备份数据的时间间隔，请选择 **Rollup**（前滚），然后单击 **Settings**（设置）。
随即显示保留策略的 **Configuration**（配置）对话框。
- 如果要为复制机器自定义保留策略，且如果显示一条警告，告知您应对存储库执行 Integrity Check（完整性检查），请继续执行此步骤。否则，跳至下一步。

- a 如果您准备好要执行该作业，请单击 **Check Integrity**（检查完整性）
- b 单击 **Yes**（是）以确认 Integrity Check（完整性检查）作业。

注：运行该作业将根据存储库的大小花费大量时间。此过程内，您无法在存储库内执行其他操作（快照、复制、虚拟输出等）。要了解该作业的相关信息，请参阅[有关检查 DVM 存储库的完整性](#)。

• Check Integrity（检查完整性）作业成功完成所有子作业后，将返回至该程序，并继续执行下一步骤。

7 在 **Configuration**（配置）对话框中，执行以下任一操作：

- 要对此受保护机器使用默认保留策略，请选择 **Use Core default retention policy**（使用 Core 默认保留策略），然后单击 **Save**（保存）。默认策略将应用至该代理。
- 要为该代理定义自定义保留策略，请选择 **Use custom retention policy**（使用自定义保留策略），然后继续执行下一步。

Configuration（配置）对话框展开，以显示自定义保留策略信息。

8 输入保留恢复点的自定义计划，如下表中所述。

表. 126: 自定义保留策略的计划选项

文本框	说明
Keep all Recovery Points for （保留所有恢复点）n [retention time period]	指定恢复点的保留期限。 输入代表保留期限的数字，然后选择时间期限。默认值为 3 天。 您可选择：Days（天）、Weeks（周）、Months（月）和 Years（年）
...and then keep one Recovery Point per hour for（...然后每小 时将一个恢复点保留为）n [retention time period]	提供更具体的保留期限。它用作主设置的一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 2 天。 您可选择：Days（天）、Weeks（周）、Months（月）和 Years（年）
...and then keep one Recovery Point per day for（...然后每天 将一个恢复点保留为）n [retention time period]	提供更具体的保留期限。此设置用作一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 4 天。 您可选择：Days（天）、Weeks（周）、Months（月）和 Years（年）
...and then keep one Recovery Point per week for（...然后每 周将一个恢复点保留为）n [retention time period]	提供更具体的保留期限。此设置用作一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 3 周。 您可选择：Weeks（周）、Months（月）和 Years（年）
...and then keep one Recovery Point per month for（...然后每 月将一个恢复点保留为）n [retention time period]	提供更具体的保留期限。此设置用作一个构建块，以便进一步定义将恢复点保存多长时间。 输入代表保留期限的数字，然后选择时间期限。默认值为 2 月。 您可选择：Months（月）和 Years（年）
...and then keep one Recovery Point per year for（...然后每年 将一个恢复点保留为）n [retention time period]	输入代表保留期限的数字，然后选择时间期限。 您可以选择：Years（年）

下面是如何计算保留期限的示例。

保留所有恢复点 3 天。

...然后每小时将一个恢复点保留 3 天

...然后每天将一个恢复点保留 4 天

...然后每周将一个恢复点保留 3 周

...然后每月将一个恢复点保留 2 个月

...然后每月将一个恢复点保留 1 年

在本例中，最早的恢复点为 1 年，3 个月。

- 9 如果您想保留主存储库中的所有恢复点，请清除 **Relocate outdated recovery points to an R3 repository**（重新分配过期的恢复点至 R3 存储库）选项，并跳至下一步。
- 10 如果您要将恢复点从主存储库重新分配至存储在 Dell DR 系列备份设备中的 R3 存储库，请执行以下操作：
 - a 选择 **Relocate outdated recovery points to an R3 repository**（重新分配过期的恢复点至 R3 存储库）选项。
 - b 指定多久后将恢复点从主存储库重新分配至 R3 存储库。
您可指定时间的长度为周、月或年。您可设置的最短期间为 1 周。
 - c 从 **Select a repository**（选择存储库）下拉菜单中，选择要将指定恢复点绑定至的 R3 存储库。

注：无论恢复点位于哪里（本地 DVM 存储库或 DR 备份设备中的远程 R3 存储库中），这些恢复点仍遵守保留策略，并仍将进行前滚。如果您需要保留较旧的恢复点，一种方式是进行归档。其他方式是禁用前滚或扩展相关受保护机器的保留期。

- 11 单击**保存**。

强制执行受保护机器的汇总

您可通过强制恢复点在受保护机器级别汇总来绕过计划的保留策略。

- 1 在 Rapid Recovery Core Console 的“受保护机器”菜单中，单击特定受保护机器的名称。
此时将显示所选机器的**摘要**页面。
- 2 单击受保护机器视图顶部的**更多**下拉菜单，然后选择**保留策略**。
将显示指定机器的**保留策略**页面。
- 3 单击**强制汇总**。
- 4 在此对话框中，单击**是**进行确认。
Rapid Recovery 启动此机器的汇总，而不考虑保留策略计划。

复制

本节介绍如何配置和管理从 Rapid Recovery 源 Core 到 Rapid Recovery 目标 Core 的受保护数据复制，以完成灾难恢复。

Rapid Recovery 中的复制

本节提供概念和过程方面的信息，以便帮助了解和配置 Rapid Recovery 中的复制功能。

复制是从 Rapid Recovery Core 复制恢复点并将其发送至另一个 Rapid Recovery Core 以满足灾难恢复目的的过程。此过程需要两个或多个 Core 之间配对的“源-目标”关系。

源 Core 复制所选受保护机器的恢复点，然后不断将快照数据异步传输至目标 Core。

除非您通过设置复制计划更改默认行为，否则 Core 会在完成每个备份快照、校验和检查、可附加性检查和每夜作业后立即启动复制作业。有关详情，请参阅[计划复制](#)。

为获得最佳的数据安全性，管理员通常在远程灾难恢复站点使用目标 Core。您可以将上述出站复制配置到公司自己的数据中心或远程灾难恢复站点（即“自管”目标 Core）。或将上述出站复制配置到托管服务提供商 (MSP) 提供的非现场备份和灾难恢复服务。复制到第三方 Core 时，可以使用允许提出连接请求和接收自动反馈通知的内置工作流。

复制按受保护的机器进行管理。可以将任何源 Core 上的受保护或复制机器（或全部机器）配置为复制到目标 Core。

可能的复制方案包括：

- **复制到本地位置。**目标 Core 位于本地数据中心或现场位置，并且将始终保持复制。在此配置下，丢失 Core 不会妨碍恢复。
- **复制到非现场位置。**目标 Core 位于非现场灾难恢复设施内，以备在发生丢失时进行恢复。
- **相互复制。**两个不同地点的数据中心各自包含一个 Core，都对机器进行保护并相互充当对方的非现场灾难恢复备份。在此方案下，各个 Core 会将受保护机器复制到位于另一数据中心的 Core。
- **托管和云复制。**Rapid Recovery MSP 合作伙伴在数据中心或公共云中维护多个目标 Core。在每个 Core 上，MSP 合作伙伴可让一个或多个客户从位于客户站点的源 Core 将恢复点复制到 MSP 的目标 Core，并收取费用。

① | **注：**在此方案下，客户仅有权访问自己的数据。

可能的复制配置包括：

- **点对点复制。**将一个或多个受保护机器从单个源 Core 复制到单个目标 Core。

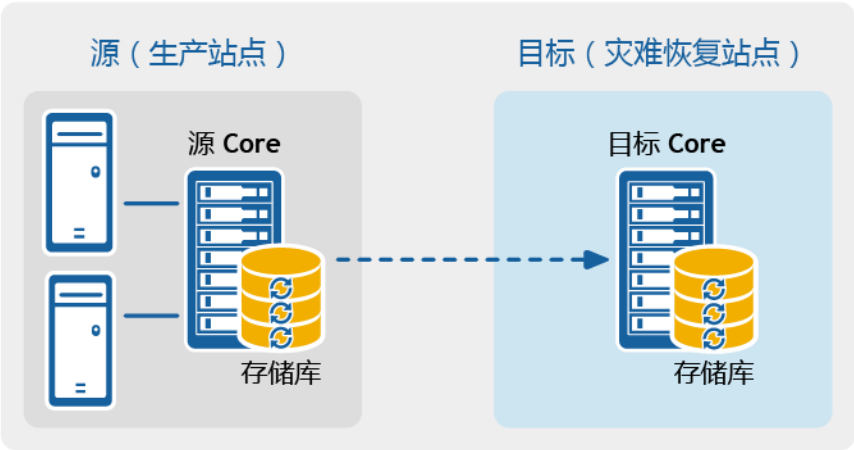


图 9: 点对点复制配置

- **多点到点复制。**将受保护机器从多个源 Core 复制到单个目标 Core。

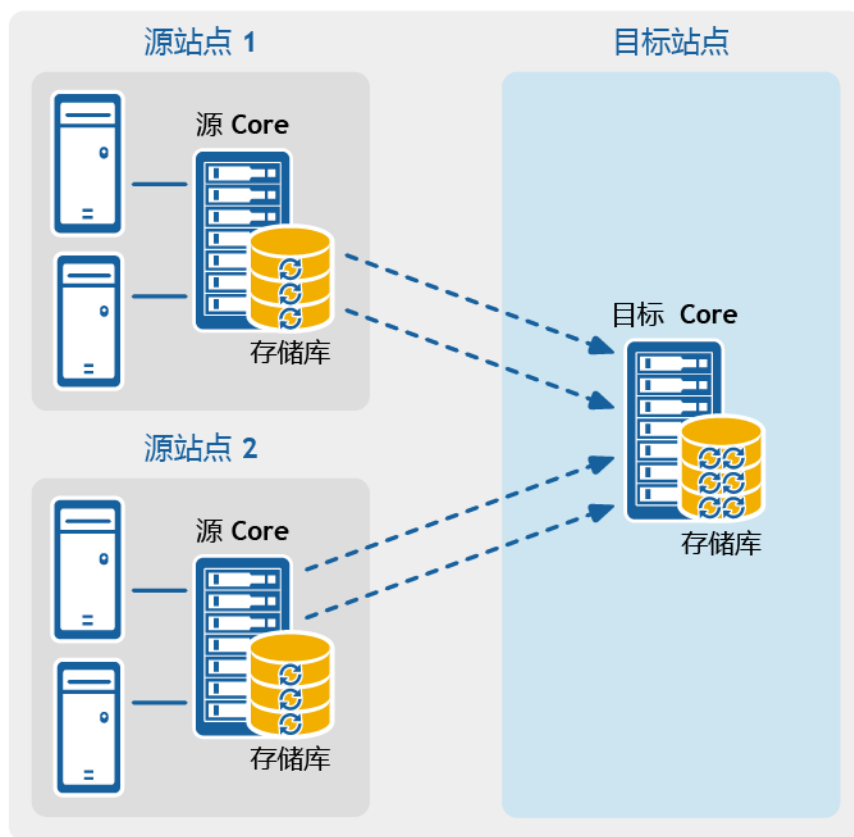


图 10: 多点到点复制配置

- **点到多点复制。** 将一个或多个受保护机器从单个源 Core 复制到多个目标 Core。

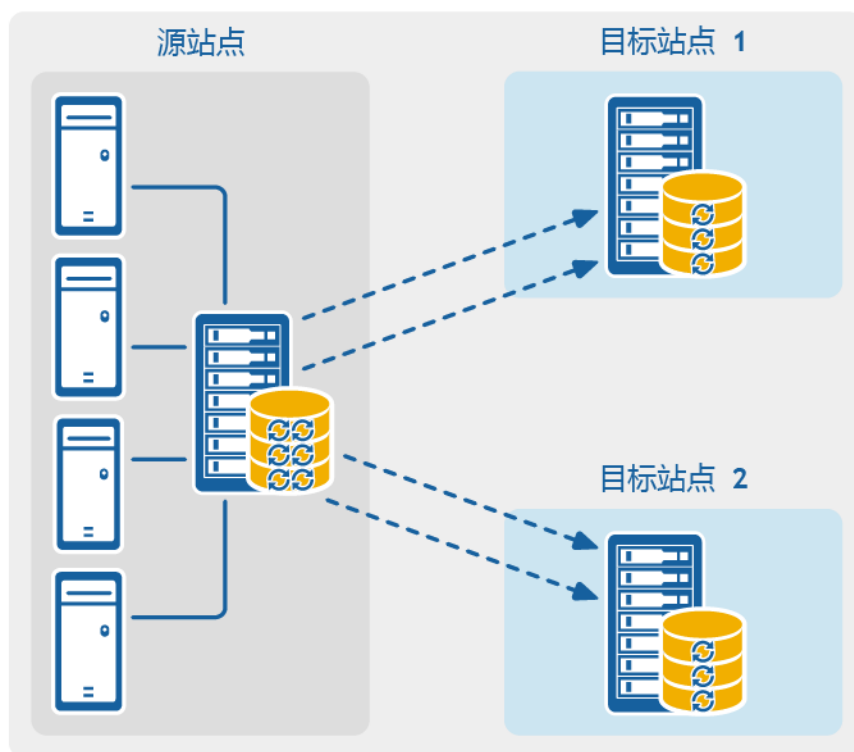


图 11: 点到多点复制配置

- **多跃点复制。** 将一个或多个受保护机器从一个目标 Core 复制到另一个目标 Core，从而在复制的 Core 上产生额外的故障转移或恢复选项。

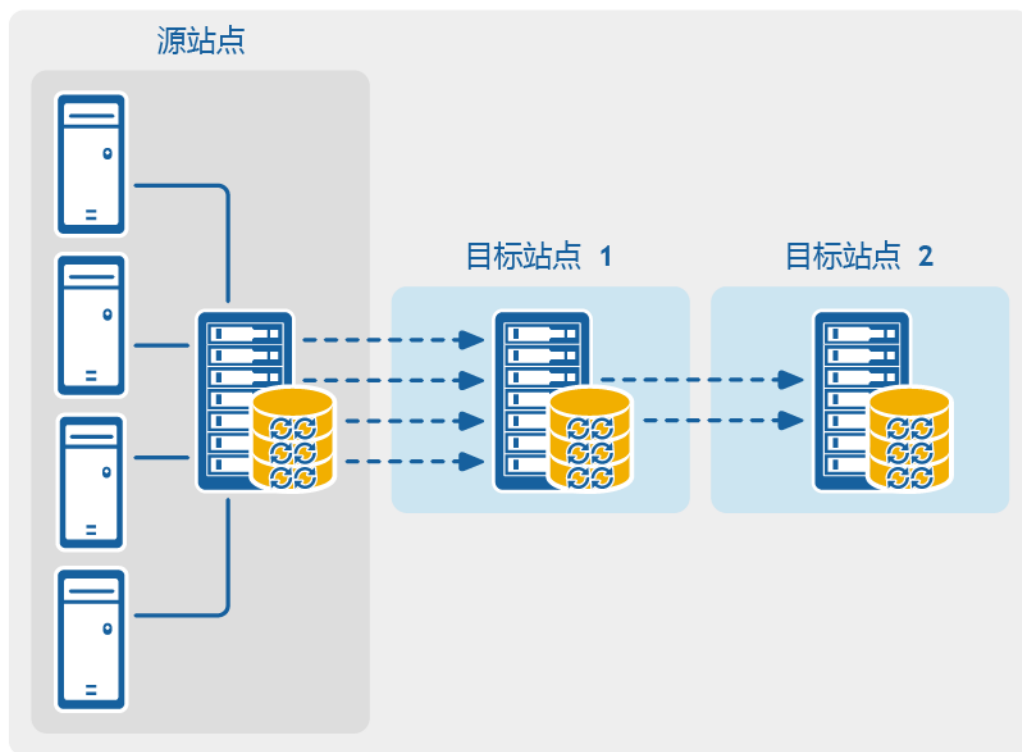


图 12: 多跃点复制配置

如果使用 Dell 数据保护备份设备（例如 DL1x00 或 DL4x00 系列），您复制到的目标 Core 必须配置一个有效的软件许可证。在购买时，这些硬件设备包括一个复制目标许可证。在您购买设备时收到的欢迎电子邮件消息中检查您的许可证密钥。如需帮助，请访问许可帮助网站 (<https://support.software.dell.com/licensing-assistance>) 或发送电子邮件至 license@software.dell.com。

恢复点链和孤立恢复点

Rapid Recovery 可捕获受保护机器的快照，并将数据保存到存储库作为恢复点。保存到 Core 的第一个恢复点称为基本映像。基本映像包括您选择保护的每个卷的操作系统、应用程序和设置，以及这些卷上的所有数据。连续备份是增量快照，其中仅包含受保护的卷上自上次备份以来发生更改的数据。基本映像与所有增量快照合在一起，形成完整的恢复点链。

通过完整的恢复点链，您可以使用 Rapid Recovery 可用的所有恢复选项轻松可靠地还原数据。这些选项包括文件级还原、卷级还原和裸机还原。

由于逻辑上您无法从不存在的数据进行还原，因此，对于不完整的恢复点链，您将无法在卷级别还原数据或执行裸机还原。在此情况下，您仍然可以在文件级别还原恢复点中存在的任何数据。

如果您要从恢复点还原的信息位于 Core 不可用的先前备份中（较早的增量快照或基本映像），则该恢复点被称为孤立恢复点。孤立恢复点在一些复制情形中属于常见现象。

例如，当您第一次建立复制时，您用于从已复制的恢复点还原数据的选项将受到限制。直到来自源 Core 的所有备份数据传输至目标 Core 并从孤立恢复点创建了完整的恢复点链后，您才能执行文件级还原。

当复制开始时

默认情况下，Core 会在每个定期计划备份传输完成后立即将复制传输作业加入队列。因此，除非自定义了受保护机器的复制计划，否则它的复制计划将基于它的标准备份快照计划。

当您第一次设置复制时，如果源 Core 上存在一个或多个恢复点，复制过程会立即开始，下列情况除外：

- 您选择了初始时暂停复制的选项，或
- 您选择了使用种子驱动器执行初始传输的选项。

如果您在初始时暂停复制，复制将在您明确恢复复制时开始。

如果您设置复制并指定使用种子驱动器，到目标 Core 的复制将随同下一个定期计划备份快照开始。

① | 注：您也可以在建复制后强制备份受保护机器。这会导致复制在受保护机器快照完成后立即开始。

如果您在设置复制时指定了种子驱动器，则仅复制将来的备份传输。如果您希望来自原始受保护机器的现有恢复点存在于目标 Core 上，您必须播种来自受保护机器的数据。要播种数据，请从源 Core 创建种子驱动器，然后在目标 Core 上使用种子驱动器。

您也可以自定义受保护机器的复制计划。例如，如果您使用默认保护计划（每小时一个备份），您可以指定源 Core 按照不同的计划复制到目标 Core（例如，每天在 2AM 运行一次）。

确定您的播种需求和策略

以下主题讨论了从已复制数据进行还原，以及您是否需要从源 Core 播种恢复点数据。

需要播种数据时

当您第一次建立复制时，除非您指定使用种子驱动器，否则源 Core 会开始将所选机器的所有恢复点传输到目标 Core。通过网络传输数据可能会耗费大量时间。相关因素包括您的网络速度、您的网络体系结构的稳定性以及传输至目标 Core 的数据量。例如，如果源 Core 上的备份数据为 10GB，而 WAN 链路的传输速率为 24Mbps，则完成传输可能需要大约一小时。

根据您想要复制到目标 Core 的信息量，种子驱动器可能合计数百或数千 GB 的数据。许多组织选择不使用所需的网络带宽，而是选择定义和使用种子驱动器。有关详情，请参阅[复制数据传输的性能注意事项](#)。

如果您在定义复制时指定使用种子驱动器，则只有建立复制后保存到源 Core 的恢复点会复制到目标 Core。建立复制之前保存在源 Core 上的备份将不会出现在目标 Core 上，除非您使用以下过程明确播种数据。

要避免因密集传输历史数据而拖慢网络速度，请使用**种子驱动器**将您之前的备份数据播种到目标 Core。种子驱动器是一个存档文件，该文件会从源 Core 复制一组经过重复数据消除的基本映像和增量快照。种子驱动器文件包含您要从源 Core 复制到目标 Core 的受保护机器的所有过往恢复点。

将种子驱动器文件移至随后可供目标 Core 使用的存储卷。然后使用来自种子驱动器的信息。此过程包括将带有种子驱动器映像的卷附加到目标 Core 以及从 Core Console 将数据导入存储库。此过程可修复孤立对象，使复制到目标 Core 的增量快照与其基本映像统一起来，以便形成一个或多个完整的恢复点链。此过程有时也称为“复制-使用”。

并非总是需要从源 Core 播种数据。例如：

- 如果您为新的 Rapid Recovery Core 设置复制，则不需要播种。
- 如果过往快照中的数据对于您复制的数据并非至关重要，并且您只需恢复设置复制后保存的数据，则不需要播种。

① **注:** 在这种情况下，Dell 建议在设置复制之前或之后立即捕获新的基本映像。此步骤可确保在将来要从中还原数据的目标 Core 上存在完整的恢复点链。

- 如果您在设置复制之前立即捕获了基本映像，并且仅需要从该日期之后捕获的数据进行还原，则不需要播种。
- 如果您在未指定种子驱动器的情况下设置了复制，则快照数据会通过网络从源 Core 传输到目标 Core。

如果您遇到了其中一种情况，则无需播种数据。在此类情况下，可以从源 Core 完成整个复制。

如果您为带有现有恢复点的 Core 设置复制，并且可能需要在卷级别进行还原，想要执行 BMR，或想要从较早的基本映像或增量快照还原数据，则需要播种。在这些情况下，请考虑您的播种需求和策略。查看本主题中的信息并决定您是否要播种到目标 Core 以及您将使用哪种方法。

播种数据的方法

如果想要目标 Core 上复制的机器能够访问先前保存在原始源 Core 上的数据，请使用以下其中一种方法播种目标 Core：

- 1 **通过网络连接播种到目标 Core。** 定义复制时指定使用种子驱动器。然后，您可以与目标 Core 共享包含种子驱动器的文件夹，并通过网络使用种子驱动器文件。对于大型数据或慢速连接，通过此方法播种可能会耗费大量时间并占用大量网络带宽。

① **注:** Dell 不建议通过网络连接播种大量数据。初始播种时可能会涉及数量非常庞大的数据，这可能会使一般的 WAN 连接不堪重负。

- 2 **使用物理存储介质从源 Core 传输备份数据。** 将种子驱动器文件传输至便携式外部可移动存储设备。通常情况下，此方法对大型数据集或网络连接速度慢的站点来说非常有用。使用此方法播种时，您需要执行以下步骤：
 - a 从源 Core 创建种子存档，将其保存到可移动介质。
 - b 将种子驱动器运至到目标 Core 的物理位置。
 - c 将驱动器连接至目标 Core。
 - d 将种子驱动器中的数据传输到目标 Core 的存储库。

如果是复制到第三方 Core，在 MSP 收到您的介质后，数据中心代表通常会连接介质并在您准备好将种子数据传输（或导入）进 Core 时向您发出通知。

① **注:** 由于需要将大量数据复制到存储设备，因此建议使用 eSATA、USB 3.0 或其他高速连接。如果种子数据存档的总大小超过可移动介质上的可用空间，则可以跨越多台设备进行存档。

- 3 **对于存储在虚拟主机上的源 Core 和目标 Core，请使用虚拟硬盘传输备份数据。** 如果您的源 Core 和目标 Core 均在虚拟主机上，您可以定义和使用虚拟存储介质上的种子驱动器。使用此方法播种时，您需要执行以下步骤：
 - a 从源 Core 创建种子驱动器文件，将其保存到虚拟存储卷。
 - b 从源 Core 分离该卷并将其附加到目标 Core。
 - c 将种子驱动器中的数据传输到目标 Core 的存储库。

① **注:** 虽然可以在播种完成之前在源 Core 和目标 Core 之间复制增量快照，但从源 Core 传输到目标 Core 的已复制快照在初始数据被使用之前保持孤立，而且它们与复制的基本映像相结合。

相关链接

- 有关使用种子驱动器的过程的详细信息，请参阅主题[在目标 Core 上使用种子驱动器](#)。
- 有关孤立恢复点的更多信息，请参阅[删除孤立恢复点链](#)。
- 有关准备种子驱动器的信息，请参阅[了解种子驱动器](#)和[在目标 Core 上使用种子驱动器](#)。

相关链接

[在目标 Core 上使用种子驱动器](#)
[删除孤立恢复点链](#)

复制数据传输的性能注意事项

如果源 Core 和目标 Core 之间的带宽无法支持传输存储的恢复点，请设置复制并指定使用种子驱动器。此过程会将来自源 Core 上的所选受保护服务器的基本映像和恢复点播种到目标 Core 上。可以随时执行播种过程。可在初始数据传输过程中执行播种，其用作定期计划复制的基础。如果复制已暂停或已删除，您也可以播种以前复制的机器的数据。在此情况下，“建立恢复点链”选项可用于将尚未复制的恢复点复制到种子驱动器。

准备进行复制时，请考虑以下因素：

- **更改率。**更改率是指受保护数据的累积速率。此速率取决于受保护卷上变化的数据量以及卷的保护间隔时间。一些机器类型通常具有更高的更改率，例如 Exchange 电子邮件服务器。用于降低更改率的一种方法是缩短保护间隔时间。
 - **带宽。**带宽是指源 Core 和目标 Core 之间的可用传输速度。带宽必须大于更改率，以便使复制与快照创建的恢复点保持同步。对于 Core 之间的超大型数据传输，可能需要多个并行流以线速运行，最高达 1 GB 以太网连接的速度。
- ① **注：**ISP 指定的带宽通常是总可用带宽。网络上的所有设备均共享传出带宽。请确保具有足够的空余带宽可用于复制，以便支持更改率。
- **受保护机器数量。**必须要考虑每个源 Core 上受保护机器的数量，以及计划要将多少机器复制到目标 Core。您不需要复制源 Core 上的每台受保护机器；Rapid Recovery 可让您对受保护的机器进行逐一复制，因此您可以根据需要仅选择复制某些机器。如果必须复制源 Core 上的所有受保护机器，更改率通常会更高。当源 Core 和目标 Core 之间的带宽对于要复制的恢复点数量和大小来说不足时，此因素会带来影响。

各种 WAN 连接的最大更改率如下表所示，其中列举了在合理的更改率下传输每 GB 数据所需的带宽。

表. 127: 每 GB 数据所需的带宽示例

宽带	带宽	最大更改率
DSL	768 Kbps 及以上	330MB/小时
电缆	1 Mbps 及以上	429MB/小时
T1	1.5 Mbps 及以上	644MB/小时
光纤	20 Mbps 及以上	8.38GB/小时

① **注：**要实现最佳效果，请遵循上表中列出的建议。

如果数据传输期间出现链路故障，则在链路功能还原后，将从传输的上一个故障点继续复制。

复制过程可能会非常费时，具体取决于网络配置。确保您拥有足够的带宽来支持复制、其他 Rapid Recovery 传输（例如备份）和您必须运行的任何其他重要应用程序。

如果您遇到问题，因而无法成功通过网络传输数据（尤其是对于某些受保护或被复制的机器），请考虑调整这些机器的数据传输速率。有关更多信息，请参阅[关于修改传输设置](#)和[限制传输速度](#)。

关于复制和加密恢复点

虽然种子驱动器不包含源 Core 注册表和证书的备份，但如果对从源 Core 复制到目标 Core 的恢复点进行加密，则种子驱动器将包含来自源 Core 的加密密钥。在传输至目标 Core 后，复制的恢复点将保持加密状态。目标 Core 的所有者或管理员需要密码才能恢复加密的数据。

关于复制的保留策略

源 Core 和目标 Core 上的保留策略不同步。在初始操作及每夜作业运行期间，将在每个 Core 上单独执行汇总或按需删除。

有关保留策略的更多信息，请参阅[管理保留策略](#)。

复制到自管目标 Core

此配置适用于到非现场位置的复制和相互复制。以下步骤是前提条件：

- Rapid Recovery Core 必须安装在所有源和目标机器上。
- 如果您已为多点复制配置 Rapid Recovery，您必须在所有源 Core 和一个目标 Core 上执行此任务。有关这些复制配置的说明，请参阅[复制](#)。
- 如果您需要创建种子驱动器并将其转移至物理可移动存储卷以执行现有恢复点的初始传输，您必须准备好一个适当的便携式存储设备。您还必须能够物理访问源 Core 机器，以连接驱动器并复制种子驱动器存档。
- 如果使用自管目标 Core 中的种子驱动器，则您或受信任的管理员必须具有对目标 Core 的物理访问权限。

自管目标 Core 是您拥有访问权限的 Core。例如，自管 Core 通常由公司管理并位于非现场位置，或托管在与源 Core 的地理位置不同的地方。除非您选择使用种子驱动器播种数据，否则复制操作完全可在源 Core 上进行设置。在此类情况下，您必须使用此过程创建一个种子驱动器，然后将种子驱动器连接到目标 Core 以使用存档的恢复点数据。有关更多信息，请参阅[确定您的播种需求和策略](#)。

完成以下过程中的步骤可配置源 Core 以复制到自管目标 Core。

- 1 导航至源 Core 的 Rapid Recovery Core Console。
- 2 在按钮栏上，单击  **Replicate（复制）**。
此时将显示 **Replication Wizard（复制向导）**。
- 3 在 Replication Wizard 的 **Target Core（目标 Core）** 页面上，如果您正在与先前已经与此源 Core 配对的目标 Core 建立复制，请选择 **Use an existing target Core（使用现有目标 Core）**，然后从下拉列表中选择相应的目标 Core。跳至步骤 5。
- 4 在 Replication Wizard 的 **Target Core（目标 Core）** 页面上，如果您正在首次从此源 Core 建立与目标 Core 的复制，请选择 **I have my own Target Core（我有自己的目标 Core）**，然后根据下表中的说明输入信息。

表. 128: 目标 Core 的信息

文本框	说明
主机名	输入要复制到的 Core 机器的主机名或 IP 地址。
端口	输入 Rapid Recovery Core 将用来与机器进行通信的端口号。 默认端口号为 8006。
用户名	输入访问机器的用户名。
密码	输入用于访问机器的密码。

- 5 单击**下一步**。

 **注:** 如果目标 Core 上不存在任何存储库，此时会显示警告，告知您可以将源 Core 与目标 Core 进行配对，但您只有建立一个存储库后，才能将代理（受保护机器）复制到此位置。有关如何针对 Core 设置存储库的信息，请参阅[创建 DVM 存储库](#)。
- 6 在 **Request（请求）** 页面上，输入此复制配置的名称；例如，SourceCore1。这是用于目标 Core 的 Replication（复制）页面上 Incoming Replication（传入复制）窗格的显示名称。
- 7 单击**下一步**。
- 8 在 **Protected Machines（受保护机器）** 页面中，选择要复制的受保护机器，然后使用 Repository（存储库）列中的下拉列表为每个受保护机器选择一个存储库。
- 9 如果您打算执行播种过程以传输基本数据，请完成以下步骤：

 **注:** 由于需要将大量数据复制到便携式存储设备，Dell 建议使用 eSATA、USB 3.0 或其他高速连接方式连接至便携式存储设备。
 - a 在 Replication Wizard（复制向导）的 **Protected Machines（受保护机器）** 页面上，选择 **Use a seed drive to perform the initial transfer（使用种子驱动器执行初始传输）**。

- 如果您当前有复制到目标 Core 的一个或多个受保护机器，您可以通过选择 **Include already replicated recovery points in the seed drive**（在种子驱动器中包含已复制恢复点），在种子驱动器中包含这些受保护机器。
- b 单击下一步。
- c 在 Replication Wizard（复制向导）的 **Seed Drive Location**（种子驱动器位置）页面中，使用 **Location Type**（本地类型）下拉列表以从以下目标类型中进行选择：
- 本地
 - 网络
 - 云
- d 基于您在步骤 c 中选择的位置类型，根据下表中的说明输入种子驱动器文件的详细信息。

表. 129: 存档的详细信息

选项	文本框	说明
本地	输出位置	输入输出的位置。它用于定义您希望种子驱动器存档驻留的位置路径；例如：D:\work\archive。
网络	输出位置	输入输出的位置。它用于定义您希望种子驱动器存档驻留的位置路径；例如：\\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络路径的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。
		注: 要选择云帐户，首先必须在 Core Console 中添加云帐户。有关更多信息，请参阅 添加云帐户 。
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	输入将保存存档数据的文件夹的名称。默认名称为 Rapid-Recovery-Archive-[创建日期]-[创建时间]

- e 单击下一步。
- f 在 Replication Wizard（复制向导）的 **Seed Drive Options**（种子驱动器选项）页面中，根据下表中的说明输入信息。

表. 130: Seed Drive Options（种子驱动器选项）

项目	说明
最大大小	大型数据存档可划分为多个分段。通过执行以下操作之一，选择您要保留用于创建种子驱动器的最大分段大小： • 选择 Entire Target（整个目标） 以保留在 Seed Drive Location（种子驱动器位置）页面中提供的路径中的所有可用空间供将来使用（例如，如果位置为 D:\work\archive，则根据需保留 D: 驱动器上的所有可用空间以用于复制种子驱动器，但在开始复制过程后立即不再保留）。 • 选择文本框，输入数量，然后从下拉列表中选择计量单位，以自定义要保留的最大空间。默认值为 250MB。
Recycle action（循环操作）	如果此路径已包含种子驱动器，则选择以下选项之一： • Do not reuse（不重用）。不覆盖或清除此位置的任何现有种子数据。如果此位置为空，则种子驱动器写入将失败。 • Replace this core（替换此 Core）。覆盖与此 Core 相关的任何预先存在的种子数据，但其他 Core 的数据保持不变。 • Erase completely（完全擦除）。从目录清除所有种子数据，然后再写入种子驱动器。
注释	输入说明种子驱动器的注释。
Add all Agents to Seed Drive（将所	选择此选项可使用种子驱动器复制源 Core 上的所有受保护机器。此选项默认处于选中状态。

项目	说明
有代理添加到种子驱动器)	
Build recovery point chains (fix orphans) (构建恢复点链 (修复孤立恢复点))	选择此选项可将整个恢复点链复制到种子驱动器。默认选中此选项。 注: AppAssure 5.4 中的典型播种仅将最新恢复点复制到种子驱动器, 从而减少创建种子驱动器所需的时间和空间量。选择将恢复点 (RP) 链构建到种子驱动器要求种子驱动器上有足够的空间来存储来自指定受保护机器的最新恢复点, 并且可能需要更多时间才能完成任务。

g 请执行以下操作之一:

- 如果您已取消选中 **Add all Agents to Seed Drive** (将所有代理添加到种子驱动器) 复选框, 请单击 **Next** (下一步)。
- 如果您选中了 **Add all Agents to Seed Drive** (将所有代理添加到种子驱动器), 请转到步骤 10。

h 在 Replication Wizard (复制向导) 的 **Protected Machines** (受保护机器) 页面上, 选择想要使用种子驱动器复制到目标 Core 的受保护机器。

10 单击**完成**。

11 如果您创建了种子驱动器, 请将其发送至目标 Core。

源 Core 与目标 Core 的配对已完成。

除非您选择了该选项以初始暂停复制, 复制过程会立即开始。

- 1 如果您选择了该选项以使用种子驱动器, 复制会在目标 Core 上产生孤立恢复点, 直到种子驱动器被使用并提供所需的基本映像。
- 2 如果您指定使用某驱动器, 种子驱动器存档文件会传输到卷 (共享的文件夹、虚拟磁盘或可移动存储介质)。之后, 会使用该种子驱动器。

查看传入和传出复制

如果您单击图标栏中的**复制**  图标, **复制** 页面将显示。此页面可使您了解来自此 Core 范围的复制。它包括两个窗格:

- **传出复制**窗格列出了此 Core 中在另一个 Core 上复制的任何受保护机器。
- **传入复制**窗格中列出了此 Core 上复制的机器, 以及从中复制这些机器的源 Core。

本节介绍了上述窗格中显示的信息。

下表介绍了与来自此 Rapid Recovery Core 的传出复制有关的信息。

表. 131: 有关传出复制的信息

UI 元素	说明
选择项目	对于摘要表中的每一行, 您可以选中复选框以执行表格上方菜单选项列表中的操作。
类型	显示机器类型。您可以展开目标 Core 以显示单个被复制的机器。
状态指示器	复制状态。“状态”栏中的彩色圆圈显示复制机器是否在线或无法访问。如果将鼠标悬停在彩色圆圈上, 将显示状态条件。状态条件包括绿色 (已建立复制和在线)、黄色 (暂停复制)、红色 (验证错误) 和灰色 (离线或无法访问)。
复制名称	来自此源 Core 的机器复制到的 Core 机器的显示名称。
机器	列出了复制到所选目标 Core 的机器数。
同步	上次复制传输到目标 Core 的日期和时间。
	当您单击此列中的操作下拉菜单时, 您会看到一个操作列表, 执行这些操作可影响特定的复制关系。

您可以在“传出复制”网格中列出的两个或多个目标 Core 上执行操作。要在多个目标 Core 上执行操作，请在网格中选中每个 Core 的复选框，然后从网格上方的菜单中，选择希望执行的操作。您可以执行下表中所述的操作。

表. 132: “传出复制”窗格中可用的全局操作

UI 元素	说明
添加目标 Core	可让您定义另一个目标 Core 以复制此源 Core 上的受保护机器。
刷新	刷新表中显示的信息。
Force	强制复制。
Pause	暂停已建立的复制。
Resume	恢复已暂停的复制。
Copy	打开复制向导，允许您将所选受保护机器的现有恢复点复制到种子驱动器。
删除	删除传出复制。
种子驱动器	如果在设置复制时，数据复制到种子驱动器，则会出现此菜单选项。 显示有关种子驱动器文件的信息，包括保存种子驱动器的日期和时间。可折叠菜单表示目标 Core 以及从中生成种子驱动器文件的受保护机器。
	当您单击此列中的操作下拉菜单时，您会看到一个操作列表，执行这些操作可影响特定的复制关系。

下表介绍了与来自另一个 Core 的传入复制有关的信息。

表. 133: 有关传入复制的信息

UI 元素	说明
选择项目	对于摘要表中的每一行，您可以选中复选框以执行表格上方菜单选项列表中的操作。
类型	显示机器类型。您可以展开源 Core 以显示单个被复制的机器。
状态指示器	复制状态。“状态”栏中的彩色圆圈显示复制机器是否在线或无法访问。如果将鼠标悬停在彩色圆圈上，将显示状态条件。状态条件包括绿色（已建立复制和在线）、黄色（暂停复制）、红色（验证错误）和灰色（离线或无法访问）。
复制名称	包含在此目标 Core 上被复制的受保护机器的源 Core 机器的显示名称。 使用“复制向导”在源 Core 上建立复制时，可以选择指定此名称。
机器	列出了源 Core 上复制到此目标 Core 的受保护机器的数量。
同步	上次从源 Core 进行复制传输的日期和时间。
	当您单击此列中的操作下拉菜单时，您会看到一个操作列表，执行这些操作可影响特定的复制关系。

您可以在“传入复制”网格中列出的两个或多个源 Core 上执行操作。要在多个源 Core 上执行操作，请在网格中选中每个 Core 的复选框，然后从网格上方的菜单中，选择希望执行的操作。您可以执行下表中所述的操作。

表. 134: “传入复制”窗格中可用的全局操作

UI 元素	说明
刷新	刷新表中显示的信息。
Force	强制复制。
Pause	暂停已建立的复制。
Resume	恢复已暂停的复制。
删除	删除传入复制。

配置复制

要使用 Rapid Recovery 复制数据，必须配置用于复制的源 Core 和目标 Core。配置复制后，即可复制受保护机器数据、监测和管理复制以及执行恢复。

在 Rapid Recovery 执行复制时需要进行以下操作：

- 在目标 Core 上设置存储库。要了解向目标 Core 添加存储库的更多信息，请参阅 [创建 DVM 存储库](#)。
- 配置自管复制。有关复制到自管目标 Core 的更多信息，请参阅[复制到自管目标 Core](#)。
- 配置第三方复制。有关复制到第三方目标 Core 的更多信息，请参阅[复制到第三方目标 Core](#)。
- 复制已有受保护机器。要了解复制已受源 Core 保护的机器的更多信息，请参阅 [添加机器至现有复制](#)。
- 消耗种子驱动器。要了解在目标 Core 中消耗种子驱动器数据的更多信息 [在目标 Core 上使用种子驱动器](#)。
- 为受保护机器设置复制优先级。要了解受保护机器复制的优先级的更多信息，请参阅 [设置 受保护机器的复制优先级](#)。
- 设置受保护机器的复制计划。要了解设置复制计划的更多信息，请参阅 [计划复制](#)。
- 根据需要监测复制。有关监测复制的更多信息，请参阅 [查看传入和传出复制](#)。
- 根据需要管理复制设置。有关管理复制设置的更多信息，请参阅[管理复制设置](#)。
- 发生灾难或数据丢失时恢复已复制数据。有关恢复已复制数据的更多信息，请参阅[恢复已复制数据](#)。

复制到第三方目标 Core

第三方 Core 是由 MSP 管理和维护的目标 Core。复制到由第三方管理的 Core 无需客户具有目标 Core 的访问权限。

复制到第三方 Core 的过程包括客户及第三方必须完成的任务。在客户提交一个或多个源 Core 的复制请求后，MSP 必须审核请求以完成目标 Core 上的配置。

① 注: 此配置适用于托管复制和云复制。**Rapid Recovery Core 必须安装在所有源 Core 机器上。如果要配置 Rapid Recovery 以进行多点到点复制，则必须在所有源 Core 上执行此任务。**

要复制到第三方管理的目标 Core，请完成以下任务：

- [向第三方服务提供商提交复制请求](#)
- [审核客户的复制请求](#)
- [忽略客户的复制请求](#)

向第三方服务提供商提交复制请求

如果属于订购了第三方管理（如 MSP）的 Core 的最终用户，则完成以下过程中的步骤以向第三方服务提供商提交复制请求。

- 1 导航至 Rapid Recovery Core。
- 2 从图标按钮栏中，单击  复制。
此时将显示复制向导。
- 3 在“复制向导”的目标 Core 页面上，选择我订购了第三方非现场备份和灾难恢复服务，然后根据下表中的说明输入信息。

表. 135: 第三方目标 Core 信息

文本框	说明
主机名	输入第三方 Core 机器的主机名、IP 地址或 FQDN。
端口	输入第三方服务提供商提供的端口号。 默认端口号为 8006。

- 如果要添加的 Core 之前已与此源 Core 配对，则可以执行以下操作：
 - 1 选择使用现有目标 Core。
 - 2 从下拉列表中选择目标 Core。
 - 3 单击下一步。
 - 4 跳转至步骤 7。
- 4 单击下一步。
- 5 在“复制向导”的请求页面上，根据下表中的说明输入信息。

表. 136: 第三方目标 Core 详情

文本框	说明
电子邮件地址	输入与第三方服务订阅关联的电子邮件地址。
客户 ID（可选）	（可选）输入服务提供商分配的客户 ID。

- 6 单击下一步。
- 7 在“复制向导”的受保护机器页面上，选择要复制到第三方 Core 的受保护机器。
- 8 如果要执行播种过程以便传输基础数据，请完成以下步骤：

- ① 注: 由于需要将大量数据复制到便携式存储设备，因此建议使用 eSATA、USB 3.0 或其他高速连接方式连接至便携式存储设备。
 - a 在“复制向导”的受保护机器页面上，选择使用种子驱动器执行初始传输。
 - 如果当前要将一个或多个受保护机器复制到目标 Core，则可以选择包括种子驱动器中已复制的恢复点选项以包括种子驱动器上的这些机器。
 - b 单击下一步。
 - c 在“复制向导”的种子驱动器位置页面上，使用位置类型下拉式列表从以下目标类型中进行选择：
 - 本地
 - 网络
 - 云
 - d 根据您在步骤 c 中选择的位置类型，输入存档的详细信息，如下表所述。

表. 137: 存档详情

选项	文本框	说明
本地	输出位置	输入输出的位置。它用于定义希望种子驱动器存档驻留的位置路径；例如：D:\work\archive。
网络	输出位置	输入输出的位置。它用于定义希望存档驻留的位置路径；例如：\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络共享的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。 注: 要选择云帐户，您必须先在 Core Console 中添加云帐户。有关详情，请参阅添加云帐户。
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	为将保存存档数据的文件夹输入名称。默认名为 Rapid-Recovery-Archive-[创建日期]-[创建时间]

- e 单击下一步。
- f 在“复制向导”的**种子驱动器选项**页面上，根据下表中的说明输入信息。

表. 138: 种子驱动器选项

项目	说明
最大大小	大型数据存档可以分为多个段。要选择要为创建种子驱动器保留的最大空间量，请执行以下操作之一： - 选择整个目标以保留在“种子驱动器位置”页面上指定路径中的所有可用空间（例如，如果位置为 D:\work\archive，则将保留 D: 驱动器上的所有可用空间）。 - 选择空白文本框，输入所需的空间量，然后从下拉列表中选择度量单位以自定义要保留的最大空间。
循环操作	如果此路径已包含种子驱动器，则选择以下选项之一： 请勿重复使用。不覆盖或清除此位置的任何现有种子数据。如果此位置为空，则种子驱动器写入将失败。 替换此 Core。覆盖与此 Core 相关的任何预先存在的种子数据，但其他 Core 的数据保持不变。 完全擦除。从目录清除所有种子数据，然后再写入种子驱动器。
注释	输入描述种子驱动器的注释。
将所有代理添加到种子驱动器	选中此选项将使用种子驱动器复制源 Core 上的所有受保护机器。默认情况下，将选中此选项。
建立恢复点链（修复孤立恢复点）	选中此选项可将整个恢复点链复制到种子驱动器。默认情况下，将选中此选项。 注: 通常，在 AppAssure 5.4 中播种只会将最新恢复点复制到种子驱动器，这可以减少创建种子驱动器所需的时间和空间。如果选择构建种子驱动器的恢复点 (RP) 链，则在种子驱动器上需要足够的空间以存储指定受保护机器或机器的最新恢复点，且完成此任务可能需要额外的时间。

- g 请执行以下步骤之一：
- 如果清除**将所有代理添加到种子驱动器**复选框，请单击下一步。
 - 如果选择**将所有代理程序添加到种子驱动器**，则转到**步骤 9**。
- h 在“复制向导”的**机器**页面上，选择要使用种子驱动器复制到目标 Core 的受保护机器。

9 单击**完成**。

10 如果已创建种子驱动器，则会按第三方服务提供商指示发送该种子驱动器。

审核客户的复制请求

最终用户完成过程 [向第三方服务提供商提交复制请求](#) 后，将从源 Core 向第三方目标 Core 发送一个复制请求。作为第三方，您可以审核该请求，然后为客户批准请求以开始复制，或者可以拒绝该请求以阻止进行复制。

可以从以下选项中选择：

- [批准复制请求](#)
- [拒绝复制请求](#)

批准复制请求

要批准第三方目标 Core 上的复制请求，请完成以下过程。

- 1 在目标 Core 上，导航至 Rapid Recovery Core Console。
- 2 从图标栏中，单击 （复制）。
此时会显示**复制**页面。
- 3 在**复制**页面中，单击**请求 (#)**。
此时将显示 **Pending Replication Requests**（挂起复制请求）部分。
- 4 在“挂起的复制请求”下，单击要审核的请求旁的下拉菜单，然后单击**审核**。
此时将显示 **Review Replication Request**（复查复制请求）窗口。

① **注：**由客户完成的请求决定了在此窗口的“源 Core 标识”部分中显示的信息。

- 5 在“源 Core 标识”中，执行以下操作之一：
 - 选择 **Replace an existing replicated Core**（替换现有复制的 Core），然后从下拉列表中选择 Core。
 - 选择**创建新的源 Core**，然后确认提供的 Core 名称、客户电子邮件地址和客户 ID 是否正确。根据需要编辑该信息。
- 6 在“代理”下，选择要应用批准的机器，然后使用“存储库”列中的下拉列表选择每个机器的相应存储库。
- 7 （可选）在**注释**文本框中，输入要包括在客户答复中的说明或消息。
- 8 单击**发送响应**。
随即接受复制。

拒绝复制请求

要拒绝客户发送至第三方 Core 的复制请求，请完成以下过程中的步骤。

要在不审查的情况下拒绝请求，请参阅[忽略客户的复制请求](#)。

- 1 在目标 Core 上，导航至 Rapid Recovery Core Console。
- 2 从图标栏中，单击 （复制）。
此时会显示**复制**页面。
- 3 在**复制**页面中，单击**请求 (#)**。
此时将显示 **Pending Replication Requests**（挂起复制请求）部分。
- 4 在“挂起的复制请求”下，单击要审核的请求旁的下拉菜单，然后单击**审核**。
此时将显示 **Review Replication Request**（复查复制请求）窗口。
- 5 单击**拒绝**。

随即拒绝复制。拒绝通知显示在源 Core 的“事件”页面上的“警报”下。

忽略客户的复制请求

作为目标 Core 的第三方服务提供商，您可以选择忽略来自客户的复制请求。如果客户误发请求或您想要在不审核的情况下拒绝请求，则可以使用此选项。

有关复制请求的更多信息，请参阅[审核客户的复制请求](#)。

要忽略客户的复制请求，请完成以下过程。

- 1 在目标 Core 上，导航至 Rapid Recovery Core Console。
- 2 从图标栏中，单击 （复制）。
此时会显示**复制**页面。
- 3 在**复制**页面中，单击**请求 (#)**。
此时将显示 **Pending Replication Requests**（挂起复制请求）部分。
- 4 在“挂起的复制请求”下，单击要忽略的请求旁的下拉菜单，然后单击**忽略**。
- 5 在**忽略请求**对话框中，单击**是**以确认命令。
向源 Core 发送通知，告知请求被忽略，且请求将从目标 Core 的“复制”页面中删除。

添加机器至现有复制

在源 Core 与目标 Core 之间建立复制后，可以添加要复制到目标的新受保护机器。要将新的受保护机器添加至配对的目标 Core 进行复制，请在源 Core 上完成以下过程中的步骤。

有关复制的更多信息，请参阅[复制](#)和[复制到自管目标 Core](#)。

- 1 导航至源 Core 的 Rapid Recovery Core Console。
- 2 在按钮栏上，单击  **复制**。
此时将打开“复制向导”，并显示**受保护机器**页面。
- 3 在**受保护机器**页面上，选择要复制的受保护机器，然后使用“存储库”列中的下拉式列表选择每个受保护机器的存储库。
- 4 如果要执行播种过程以便传输基础数据，请完成以下步骤：
 - ① **注：**由于需要将大量数据复制到便携式存储设备，因此建议使用 **eSATA、USB 3.0** 或其他高速连接方式连接至便携式存储设备。
 - a 在“复制向导”的**受保护机器**页面上，选择**使用种子驱动器执行初始传输**。
 - 如果当前要将一个或多个受保护机器复制到目标 Core，则可以选择**包括种子驱动器中已复制的恢复点**选项以包括种子驱动器上的这些机器。
 - b 单击**下一步**。
 - c 在向导的**种子驱动器位置**页面上，使用**位置**类型下拉列表从以下目标类型中进行选择：
 - 本地
 - 网络
 - 云
 - d 根据您在**步骤 c**中选择的位置类型，输入存档的详细信息，如下表所述。

表. 139: 存档详情

选项	文本框	说明
本地	输出位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：d:\work\archive。
网络	输出位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络共享的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。
		注: 要选择云帐户，您必须先在 Core Console 中添加云帐户。有关详情，请参阅 添加云帐户 。
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	为将保存存档数据的文件夹输入名称。默认名为 Rapid-Recovery-Archive-[创建日期]-[创建时间]

e 单击下一步。

f 在向导的**种子驱动器选项**页面上，根据下表中的说明输入信息。

表. 140: 种子驱动器选项

项目	说明
最大大小	大型数据存档可以分为多个段。要选择要为创建种子驱动器保留的最大空间量，请执行以下操作之一： - 选择整个目标以保留在“种子驱动器位置”页面上指定路径中的所有可用空间（例如，如果位置为 D:\work\archive，则将保留 D: 驱动器上的所有可用空间）。 - 选择空白文本框，输入所需的空间量，然后从下拉列表中选择度量单位以自定义要保留的最大空间。
循环操作	如果此路径已包含种子驱动器，则选择以下选项之一： - 请勿重复使用。不覆盖或删除此位置的任何现有种子数据。如果此位置为空，则种子驱动器写入将失败。 - 替换此 Core。覆盖与此 Core 相关的任何预先存在的种子数据，但其他 Core 的数据保持不变。 - 完全擦除。从目录清除所有种子数据，然后再写入种子驱动器。
注释	输入描述种子驱动器的注释。
将所有代理添加到种子驱动器	选中此选项将使用种子驱动器复制源 Core 上的所有受保护机器。默认情况下，将选中此选项。
建立恢复点链（修复孤立）	选中此选项可将整个恢复点链复制到种子驱动器。默认情况下，将选中此选项。
	注: 通常，在 Rapid Recovery 5.4 中播种只会将最新恢复点复制到种子驱动器，这可减少创建种子驱动器所需的时间和空间。如果选择构建种子驱动器的恢复点 (RP) 链，则在种子驱动器上需要足够的空间以存储指定受保护机器或机器的最新恢复点，且完成此任务可能需要额外的时间。

g 请执行以下步骤之一：

- 如果清除**将所有代理添加到种子驱动器**复选框，请单击下一步。
- 如果选择**将所有代理程序添加到种子驱动器**，则转到**步骤 5**。

h 在向导的**受保护机器**页面上，选择要使用种子驱动器复制到目标 Core 的受保护机器。

5 单击**完成**。

在目标 Core 上使用种子驱动器

要在目标 Core 上使用种子驱动器文件中的数据，请完成以下过程。

① **注:** 只有在作为**复制到自管目标 Core**或**复制到第三方目标 Core**的一部分创建了种子驱动器文件时，才需要执行此过程。

- 1 如果种子驱动器文件保存到便携式存储设备（例如 USB 驱动器），则将该驱动器连接到目标 Core。
- 2 在目标 Core 上打开 Rapid Recovery Core Console，并在图标栏中单击 （复制）。
此时会显示**复制**页面。
- 3 在**复制**页面的“传入复制”下，单击正确源 Core 的下拉菜单，然后单击**使用**。
此时将显示**使用**对话框。
- 4 在**位置类型**字段中，从下拉式列表中选择以下选项之一：
 - 本地
 - 网络
 - 云
- 5 根据您在**步骤 4**中选择的位置类型，输入种子驱动器存档文件的详细信息，如下表所述。

表. 141: 存档详情

选项	文本框	说明
本地	位置	输入存档的路径。
网络	位置	输入存档的路径。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络路径的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。
		① 注: 要选择云帐户，您必须先在 Core Console 中添加云帐户。有关详情，请参阅 添加云帐户 。
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	输入保存存档数据的文件夹名称；例如，Rapid-Recovery-Archive-[创建日期]-[创建时间]

- 6 单击**检查文件**。
此时 Core 将搜索文件。

找到文件后，便会在“使用”窗口中显示以下文本框，并会使用从**步骤 4**、**步骤 5**和文件中收集到的数据预先填充这些文本框。“日期范围”将显种子驱动器中包含的的最旧和最新恢复点的日期。系统将自动导入在创建种子驱动器时输入的所有注释。
- 7 在**使用**对话框的“代理程序”下，选择要使用数据的机器。
- 8 单击**使用**。
- 9 要监测数据使用进度，请查看 “事件”页面。

放弃种子驱动器

如果您创建种子驱动器是为了将其用于目标 Core，但后来又选择不使用它，您可以放弃种子驱动器。

在您放弃种子驱动器或使用它之前，未完成的种子驱动器的链接将保留在源 Core 的“传出复制”窗格中。

在您从种子驱动器发送信息之前，孤立的恢复点（存在于原始受保护机器上，而非目标 Core 上）不能用于还原数据。

小心: 如果您放弃种子驱动器，则原始恢复点（在种子驱动器文件中定义）随后将在下一次复制作业过程中通过网络发送至目标 Core。通过网络发送旧的恢复点可能会使网络大幅变慢，尤其是存在大量恢复点时。

要放弃未完成的种子驱动器，请完成以下过程中的步骤。

注: 在 Core Console 中放弃种子驱动器不会影响来自其存储位置的种子驱动器文件。

- 1 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。
- 2 在**复制**页面的“传出复制”窗格中，单击**种子驱动器 (#)**。
在“传出复制”窗格中，显示的一个部分包含了有关未完成的种子驱动器的信息。
- 3 （可选）请单击向下箭头 ▼ 以展开可折叠菜单。
将显示与未完成的种子驱动器有关的信息，包括目标 Core 和种子驱动器中包含的恢复点的日期范围。
- 4 单击  以打开要放弃的种子驱动器文件的下拉菜单，然后选择**放弃**。
- 5 在确认窗口中，确认您要放弃种子驱动器。
随即移除种子驱动器。

如果源 Core 上不再存在种子驱动器，则将从“传出复制”窗格中删除“种子驱动器 (#)”链接和未完成的种子驱动器部分。

管理复制设置

Rapid Recovery 可让您在整体、Core 和受保护机器级别监控、计划和调整复制。

您可以编辑以下复制设置：

- 要计划复制作业，请参阅[计划复制](#)。
- 要创建已为复制配对的受保护机器的种子驱动器，请参阅 [使用“复制”功能创建种子驱动器](#)。
- 要监控复制作业的进度，请参阅[查看传入和传出复制](#)。
- 要暂停或恢复暂停的复制作业，请参阅[暂停和恢复复制](#)。
- 要强制执行传入或传出受保护机器的复制，请参阅[强制复制](#)。
- 要管理所有目标 Core 和复制过程的设置，请参阅[管理传出复制设置](#)。
- 要管理单个目标 Core 的设置，请参阅[更改目标 Core 设置](#)。
- 要管理将复制到目标 Core 的单个受保护机器的优先级设置，请参阅[设置 受保护机器的复制优先级](#)。

计划复制

除非您通过设置复制计划更改默认行为，否则 Core 会在完成每个备份快照、校验和检查、可附加性检查和每夜作业后立即启动复制作业。有关详情，请参阅[计划复制](#)。

您可以更改复制计划以减少网络上的负载。

要设置任何复制机器的复制计划，请完成以下过程中的步骤。

- 1 在目标 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。
- 2 在“传出复制”窗格中，单击  以打开要计划复制的 Core 旁的下拉菜单，然后选择**计划**。

将打开 **[Core 名称] 的复制计划** 对话框。

3 选择以下三个选项之一：

- **始终**。每次新快照、校验和检查及可附加性检查后以及每夜作业完成后复制。
- **每天（仅在指定时间期间内启动复制）**。仅在指定的时间范围内开始复制。
 - 1 在**起始时间**文本框中，输入应进行复制的最早时间。
 - 2 在**结束时间**文本框中，输入应进行复制的最晚时间。

① | 注：如果计划的时间结束后复制还在进行，复制作业会在分配的时间段后完成。

- **自定义**。仅在提供的时间范围内开始复制，让您可以为工作日设置一个时间范围，为周末设置另一个时间范围。
 - 1 在“工作日”旁的**起始时间**文本框中，输入应在工作日进行复制的最早时间，然后在**结束时间**文本框中，输入应在工作日进行复制的最晚时间。
 - 2 在“周末”旁的**起始时间**文本框中，输入应在周末进行复制的最早时间，然后在**结束时间**文本框中，输入应在周末进行复制的最晚时间。

4 单击**保存**。

计划将应用于到所选目标 Core 的所有复制。

使用“复制”功能创建种子驱动器

如果在配置复制时选择不创建种子驱动器，则可使用受保护机器下拉菜单中的“复制”功能创建种子驱动器。

- 1 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。
- 2 在**复制**页面的“传出复制”窗格中，单击 ▼ 以展开为您要创建种子驱动器的机器提供保护的 Core。选项将展开以显示指定 Core 中的每个受保护机器。
- 3 单击表格的第一行以选择要为其创建种子驱动器的每台机器。
- 4 在菜单中“传出复制”窗格下，单击**复制**。将显示**复制向导**。
- 5 在向导的**种子驱动器位置**页面上，使用**位置**下拉式列表从以下目标类型中进行选择：
 - 本地
 - 网络
 - 云
- 6 根据您在上一步中选择的位置类型，输入种子驱动器存档的详细信息，如下表所述。

表. 142: 存档详情

选项	文本框	说明
本地	输出位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：d:\work\archive。
网络	输出位置	输入输出的位置。用于定义希望存档驻留的位置的路径，例如：\\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络共享的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。 ① 注： 要选择云帐户，您必须先在 Core Console 中添加云帐户。有关详情，请参阅 添加云帐户 。
	容器	从下拉菜单中选择与您的帐户关联的容器。

选项	文本框	说明
	文件夹名称	为将保存存档数据的文件夹输入名称。默认名为 Rapid-Recovery-Archive-[创建日期]-[创建时间]

7 单击**下一步**。

8 在“种子驱动器选项”页面上，根据下表中的说明输入信息。

表. 143: 种子驱动器选项

项目	说明
最大大小	大型数据存档可以分为多个段。要选择要为创建种子驱动器保留的最大空间量，请执行以下操作之一： - 选择整个目标以保留在“种子驱动器位置”页面上指定路径中的所有可用空间（例如，如果位置为 D:\work\archive，则将保留 D: 驱动器上的所有可用空间）。 - 选择空白文本框，输入所需的空間量，然后从下拉列表中选择度量单位以自定义要保留的最大空间。
循环操作	如果此路径已包含种子驱动器，则选择以下选项之一： 请勿重复使用。不覆盖或清除此位置的任何现有种子数据。如果此位置为空，则种子驱动器写入将失败。 替换此 Core。覆盖与此 Core 相关的任何预先存在的种子数据，但其他 Core 的数据保持不变。 完全擦除。从目录清除所有种子数据，然后再写入种子驱动器。
注释	输入描述种子驱动器的注释。
将所有代理添加到种子驱动器	选中此选项将使用种子驱动器复制源 Core 上的所有受保护机器。默认情况下，将选中此选项。
建立恢复点链（修复孤立恢复点）	选中此选项可将整个恢复点链复制到种子驱动器。默认情况下，将选中此选项。 注: 通常，在 Rapid Recovery 5.4 中播种只会将最新恢复点复制到种子驱动器，这可减少创建种子驱动器所需的时间和空间。如果选择构建种子驱动器的恢复点链，则在种子驱动器上需要足够的空间以存储指定受保护机器的最新恢复点，且完成此任务可能需要额外的时间。

- 9 请执行以下步骤之一：
- 如果清除**将所有代理添加到种子驱动器**复选框，请单击**下一步**。
 - 如果选择**将所有代理程序添加到种子驱动器**，则转到**步骤 10**。
- 10 在向导的**受保护机器**页面中，选择要为其创建种子驱动器的受保护机器。
- 11 单击**完成**。

监控复制

完成复制设置后，可以监测源 Core 和目标 Core 复制任务的状态。此外还可以刷新状态信息、查看复制详情等。

- 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。
- 在此页面中，可以根据下表中的说明查看和监控复制任务的状态与信息。

表. 144: 复制任务

部分	说明	可执行的操作
种子驱动器 (#)	您在定义复制时指定使用种子驱动器之后，在您放弃或使用它之前，一个 种子驱动器 (#) 接会显示	在下拉菜单中，单击 放弃 以放弃或取消种子过程。wn 菜单

部分	说明	可执行的操作
	示在源 Core 的“传出复制”窗格中。显示的数字指示了挂起的种子驱动器的数量。 注: 除非种子驱动器挂起，否则此链接不会出现。 单击此链接可列出已写入但尚未被目标 Core 使用的种子驱动器。进一步展开可折叠菜单可显示与未完成的种子驱动器有关的信息，包括目标 Core 和种子驱动器中包含的恢复点的日期范围。	
传出复制	列出源 Core 要复制到的所有目标 Core。它包括状态指示符、目标 Core 名称、要复制的机器数量以及复制传输的进度。	在源 Core 上的  下拉菜单中，您可以选择以下选项： 详细信息。 列出 ID、URL、显示名称、状态、客户 ID、电子邮件地址和已复制 Core 的注释。 更改设置。 列出显示名称，并且允许编辑目标 Core 的主机和端口。 计划。 可设置到此目标 Core 的复制的自定义计划。 添加机器。 可以从下拉列表中选择主机，选择要复制的受保护机器，并为新受保护的初始传输创建种子驱动器。（可选）您可以选择包括已添加到复制的机器的恢复点。 删除。 允许您删除源和目标 Core 之间的复制关系。执行此操作将停止到此 Core 的所有复制。
传入复制	列出目标机器从其接收已复制数据的所有源机器。其中包括远程 Core 名称、状态、机器和进度。 列出目标机器从其接收已复制数据的所有源 Core。列出的源 Core 的显示名称来源于定义复制时“复制向导”中的值。它包括状态指示符、远程 Core 名称以及复制传输的进度。	在目标 Core 上的  下拉菜单中，您可以选择以下选项： 详细信息。 列出已复制 Core 的 ID、主机名、客户 ID、电子邮件地址和注释。 使用。 使用来自种子驱动器的初始数据，并将其保存到本地存储库。 删除。 允许您删除目标和源 Core 之间的复制关系。执行此操作将停止来自此 Core 的所有复制。
挂起的复制请求	此信息仅适用于托管服务提供商。客户单击“传入复制”窗格中的 请求 链接时，会显示摘要表部分，其中列出了客户 ID、电子邮件地址和请求的主机名。	在下拉菜单中，单击 忽略 以忽略或拒绝请求，或 审查 以审查挂起的请求。

暂停和恢复复制

您可以临时暂停源（传出）Core 或目标（传入）Core 的复制。

用于暂停复制的选项仅在复制处于活动状态时可用。用于恢复复制的选项仅在复制暂停时可用。

要暂停或恢复复制，请完成以下过程中的步骤。

- 1 打开 Rapid Recovery Core Console，并从图标栏中单击 （复制）。此时会显示 **复制** 页面。
- 2 要暂停所有已复制的机器的复制，请执行以下操作：

- a 单击摘要表顶部的复选框以选择源 Core 和目标 Core。
 - b 单击摘要表前面的菜单中的**暂停**。
所选 Core 中所有受保护机器的复制将暂停。
- 3 要仅暂停某些机器的复制，请执行以下操作：
 - a 请单击任何 Core 右侧的 ▼ 箭头。
视图将展开以显示来自所选 Core 的正在复制的每台受保护机器。
 - b 单击第一列以选择要为其暂停复制的每台机器。再次单击任何选择以清除您不想为其暂停复制的机器的复选框。
 - c 单击摘要表前面的菜单中的**暂停**。
所选受保护机器的复制将暂停。
- 4 要恢复所有已复制的机器的复制，请执行以下操作：
 - a 单击摘要表顶部的复选框以选择源 Core 和目标 Core。
 - b 单击摘要表顶部菜单中的**恢复**。
所选 Core 中所有受保护机器的复制将恢复。
- 5 要仅恢复某些机器的复制，请执行以下操作：
 - a 请单击任何 Core 右侧的 ▼ 箭头。
视图将展开以显示来自所选 Core 的正在复制的每台受保护机器。
 - b 单击第一列以选择要为其恢复复制的每台机器。再次单击任何选择以清除您不想为其恢复复制的机器的复选框。
 - c 单击摘要表顶部菜单中的**恢复**。
所选受保护机器的复制将恢复。

强制复制

从源 Core，您可以随时强制复制，而不是等待复制作业排在特定事件之后（例如备份或可附加性检查）。

要在源 Core 或目标 Core 上强制复制，请完成以下过程中的步骤。

- 1 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。
此时会显示**复制**页面。
- 2 请执行以下步骤之一：
 - 要在源 Core 上强制复制，请从**传出复制**窗格中，选择一个 Core，并从摘要表顶部菜单中，单击  **强制**。
 - 要在目标 Core 上强制复制，请从**传入复制**窗格中，选择一个 Core，并从摘要表顶部菜单中，单击  **强制**。
将显示“强制复制”对话框。
- 3 （可选）如果您想要修复任何孤立恢复点链，请选择**还原孤立恢复点链**。
- 4 要确认，请在“强制复制”对话框中，单击**是**。
对话框随即关闭，然后强制进行复制。

管理传出复制设置

对这些设置进行的更改将影响指向与此源 Core 关联的所有目标 Core 的数据传输。

- 1 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。
此时会显示**复制**页面。
- 2 在摘要表顶部的 **传出复制**窗格中，单击 （设置）。
此时将显示**复制设置**对话框。
- 3 在**复制设置**对话框中，根据下表中的说明编辑复制设置。

表. 145: 复制设置

选项	说明
高速缓存生存期（秒）	指定源 Core 每次执行目标 Core 状态请求时中间相隔的时间长度。
卷映像会话超时（分钟）	指定源 Core 尝试将卷映像传输至目标 Core 时所花费的时间。
最大并行流	指定单个受保护机器在复制该机器的数据时，允许其一次使用的网络连接数量。
最大传输速度 (MB/s)	指定传输复制数据的速度限制。
最大传输数据大小 (GB)	指定复制数据的传输数据块的最大大小（以 GB 为单位）。
Restore Defaults	选择此选项以将所有复制设置更改为系统默认设置。

 **注:** 选择此选项前，请记下任何自定义设置。系统不会提示您确认此操作

4 满足需求后，单击**保存**以保存复制设置并关闭对话框。

更改目标 Core 设置

您可以从源 Core 更改单个目标 Core 的主机和端口设置。

- 1 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。

在**传出复制**窗格中，对于每个配置为从此源 Core 复制恢复点的目标 Core，摘要表都包含一行条目。
- 2 请单击要修改的目标 Core 的 （设置）下拉菜单，然后选择**更改设置**。此时将显示 **Settings**（设置）对话框。
- 3 编辑下表中说明的任意选项。

表. 146: 目标 Core 设置

选项	说明
主机	输入目标 Core 的主机。
端口	输入目标 Core 用于与源 Core 通信的端口。

 **注:** 默认端口号为 8006。

4 单击**保存**。

设置 受保护机器的复制优先级

复制优先级确定了首先将哪些复制作业发送至 Core。使用 1 到 10 的范围按顺序设置优先级，其中优先级 1 代表最高优先级，10 代表最低优先级。当您第一次建立任何机器的复制时，其优先级设置为 5。您可以从源 Core 查看和更改受保护机器级别的优先级。

在某些情况下，可能会放弃一些复制作业。例如，如果您的环境出现异常的高更改率，或者您的网络不具有足够的带宽，复制作业可能会被放弃。如果您设置的计划限制了您的环境中发生复制的具体小时，则尤其可能出现此情况。有关设置计划复制的更多信息，请参阅[计划复制](#)。

要确保首先对重要的机器执行复制，请将关键服务器的优先级设置为较低的数字（1 到 5）。将重要性较低的机器的优先级设置为较高的数字（6 到 10）。

将任何受保护机器的复制优先级设置为 4 可确保该机器的复制作业在默认复制优先级为 5 的机器之前启动。优先级为 3 的机器的复制作业在队列中会排在 4 之前，以此类推。优先级数字越低，它的复制作业就发送得越早。很容易便可以记住：优先级 1 代表最重要。复制优先级为 1 的机器是队列中首先进行复制的机器。

要编辑受保护机器复制时的优先级设置，请完成以下步骤。

- 1 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。
- 2 在**传出复制**窗格中，单击任何源 Core 右侧的 ▼ 箭头。视图将展开以显示来自此源 Core 的、正在复制到指定目标 Core 的每台受保护机器。
- 3 请单击要设置优先级的受保护机器的 （设置）下拉菜单，然后单击**设置**。会出现一个对话框。
- 4 单击**优先级**下拉式列表，然后根据您的要求，从 **1（最高）** 到 **10（最低）** 中选择一个优先级。
- 5 单击**保存**。对话框将关闭，并且将更新所选机器的复制优先级。

移除复制

复制指的是将受保护机器的恢复点从一个 Rapid Recovery Core（源 Core）有意复制到第二个 Core（目标）上。

复制的目的是为原始受保护机器维护一个具有高可用性的数据副本。为获得最佳的数据安全性，Dell 建议将目标 Core 放置在单独的地理位置。

除非您通过设置复制计划更改默认行为，否则 Core 会在完成每个备份快照、校验和检查、可附加性检查和每夜作业后立即启动复制作业。有关详情，请参阅[计划复制](#)。

当您删除复制时，即停止将恢复点从源 Core 进一步复制到目标 Core。删除复制永远不会影响原始（源）Core 上保存的数据。

此外，当您删除复制时，您可以选择在目标 Core 上保留从原始机器复制的恢复点，也可以删除它们。如果为删除的复制机器保留恢复点，则该机器的恢复点将在 Core 中表示为仅有恢复点的机器。您可以浏览这些保留的恢复点中的数据，或在文件级别还原文件（当它们存留在目标 Core 上时）。

您可以使用以下任意一项方法来删除复制：

- [从源 Core 删除传出复制](#)
- [从目标 Core 删除传入复制](#)

从源 Core 删除传出复制

要从源 Core 上的复制中删除一个或多个受保护机器，请完成此过程中的步骤。

- 1 在源 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。

在**传出复制**窗格中，对于每个配置为从此源 Core 复制恢复点的目标 Core，摘要表都包含一行条目。
- 2 （可选）单击任意目标 Core 右侧的 ▼ 箭头。视图将展开以显示来自此源 Core 的、正在复制到指定目标 Core 的每台受保护机器。
- 3 按如下所示，选择您要从传出复制中删除的受保护机器：
 - 要完全删除此源 Core 和任何目标 Core 之间的现有复制关系，请单击任何目标 Core 的 （设置）下拉菜单，然后选择**删除**。

- 要在指定的目标 Core 中删除一部分机器的传出复制，请展开视图以显示正在复制的所有机器，并选中您要删除的每个复制机器的复选框。清除您要继续复制的所有机器的复选框。然后，从摘要表上方的菜单中，单击  **删除**。

显示的确认消息将询问您是否要删除复制关系。

- 4 在出现的对话框中，单击**是**以确认删除。

从目标 Core 删除传入复制

要从目标 Core 上的复制中删除一个或多个受保护机器，请完成此过程中的步骤。

① 注: 您也可以从源 Core 的“复制”页面上的“传出复制”窗格中删除受保护机器的复制。有关更多信息，请参阅[从源 Core 删除传出复制](#)

- 1 在目标 Core 上打开 Rapid Recovery Core Console，并从图标栏中，单击 （复制）。此时会显示**复制**页面。在“传入复制”窗格中，摘要表为带有此目标 Core 复制的受保护机器的每个源 Core 包含了一行条目。
- 2 选择要删除的被复制的机器，如下所示：
 - 要删除从源 Core 复制到目标 Core 的**所有**机器，请在“传入复制”窗格中，选中该 Core 的复选框。
 - 要从同一源 Core 删除较小的机器子集，请执行以下操作：
 - a 请单击源 Core 右边的 ▼ 箭头。
视图将展开以显示来自所选源 Core 的、复制到目标 Core 的每个机器。
 - b 选中要删除的每个复制机器对应的复选框。
 - c 从所选源 Core 的父级行中，单击 （设置）下拉菜单，然后选择**删除**。
将显示**移除复制**对话框。
- 3 在**移除复制**对话框中，执行以下操作之一：
 - 如果您想要在目标 Core 上保留已复制的恢复点，请清除选项**删除现有恢复点**。
 - 如果要删除从该机器接收的所有已复制恢复点以及从复制中删除源 Core，请选择**删除现有恢复点**。
- 4 单击**是**以确认删除。

⚠ 警告: 如果您选择此选项，所有复制到此 Core 的恢复点都会被删除。

将从此目标 Core 上的复制中删除源 Core 上所选的受保护机器。（可选）如果您选择了删除恢复点的选项，将从此 Core 的存储库中删除它们。

恢复已复制数据

源 Core 上维持“日常”复制功能，但只有目标 Core 能够完成灾难恢复所必需的功能。

进行灾难恢复时，目标 Core 可以使用已复制的恢复点来恢复受保护机器。您可以在目标 Core 上执行以下恢复选项：

- **安装恢复点。**有关更多信息，请参阅[安装恢复点](#)。
- **回滚到恢复点。**有关更多信息，请参阅[关于从恢复点还原卷或使用命令行还原 Linux 机器的卷](#)。
- **执行虚拟机 (VM) 导出。**有关更多信息，请参阅[关于使用 Rapid Recovery 导出至虚拟机](#)。
- **执行裸机还原 (BMR)。**有关更多信息，请参阅[执行 Windows 机器的裸机还原](#)。

恢复数据

管理恢复

Rapid Recovery Core 可立即从恢复点执行到物理机或虚拟机的数据还原或机器恢复。恢复点包含从数据块级别捕获的代理卷快照。这些快照具有应用程序感知功能，表示在创建快照前，所有打开的事务和滚动事务日志均已完成，同时高速缓存已刷新到磁盘。通过将应用程序感知快照与验证的恢复配合使用，可使 Core 执行多种类型的恢复，包括：

- 恢复文件和文件夹
- 使用实时恢复来恢复数据卷
- 使用实时恢复来恢复 Microsoft Exchange Server 和 Microsoft SQL Server 的数据卷
- 使用通用恢复进行裸机还原
- 使用通用恢复裸机还原到不同硬件
- 临时和持续导出至虚拟机

快照和恢复点

本节介绍如何使用和管理由 Rapid Recovery 生成的快照和恢复点。它包括有关安装、查看和强制实施，以及迁移和删除恢复点的信息。

管理快照和恢复点

恢复点是从个别磁盘卷创建并存储在存储库中的快照集合。快照捕获并存储给定时间点的磁盘卷状态，而生成该数据的应用程序仍处于使用状态。在 Rapid Recovery 中，可强制创建快照、暂时停止快照、查看存储库中当前恢复点的列表以及在需要时删除恢复点。恢复点用于还原受保护的机器或安装到本地文件系统。

Rapid Recovery 在数据块级别捕获这些快照，并且具备应用程序感知功能。这表示在创建快照前，所有开放性事务、滚动事务日志均已完成，同时高速缓存已写入到磁盘。

Rapid Recovery 使用低级别卷筛选驱动程序，后者先附加到已安装的卷上，然后跟踪下一个待处理快照的所有数据块级更改。Microsoft 卷影服务 (VSS) 有助于创建应用程序崩溃一致性快照。

查看受保护机器的恢复点页面

完成以下过程中的步骤，以查看受保护机器的完整恢复点列表。

① 注：如果要保护来自 **DAG 或 CCR 服务器群集** 的数据，则群集层级不会显示关联的恢复点。这些恢复点仅在节点或机器层级上可见。

- 1 在 Rapid Recovery Core Console 中，导航至要查看其恢复点的受保护机器。
- 2 从在页面顶部的菜单中，单击**恢复点**。
此时将显示“恢复点”页面，显示“恢复点摘要”窗格和“恢复点”窗格。

可以查看关于机器上恢复点的摘要信息，如下表中所述。

表. 147: 恢复点摘要信息

信息	说明
恢复点总计	列出保存到此机器存储库中的恢复点总数。
受保护数据合计	指出这些恢复点在存储库中所用存储空间。
DVM 存储库	列出保存这些恢复点的存储库的名称。
DVM 存储库状态	以图形方式显示恢复点所占空间量。显示已用存储库百分比、空间大小和存储库总空间。在图表上单击，以查看剩余空间量。

可以查看关于机器上恢复点的信息，如下表中所述。

表. 148: 恢复点信息

信息	说明
图标	恢复点  或恢复点（展开时）内卷  的图片说明。恢复点显示一个右箭头  ，表示可以展开详细信息。
已加密	指明恢复点是否已加密。
状态	表明恢复点的当前状态。
目录	列出恢复点中包含的卷。单击  （信息），以查看空间使用情况和文件系统。
类型	将恢复点定义为基本映像或增量（差异）快照。
创建日期	显示恢复点的创建日期。
大小	显示存储库中恢复点所使用的空间量。
	“设置”下拉菜单可让您执行所选恢复点的特定功能。

3 （可选）展开恢复点，以查看受保护的卷。

相关链接

[查看计算机的恢复点](#)

了解恢复点状态指示器

在受保护 SQL 或 Exchange Server 上捕获恢复点后，应用程序将在“恢复点”网格中创建相应的彩色状态指示灯。此网格将在查看特定计算机的恢复点时显示在**恢复点**窗格中。显示的颜色取决于受保护计算机的检查设置，以及这些检查是成功还是失败，如下表中所述。

① | **注:** 有关查看恢复点的更多信息，请参阅[查看受保护机器的恢复点页面](#)。

Exchange 数据库的恢复状态点颜色

下表列出了 Exchange 数据库的状态指示器。

表. 149: Exchange 数据库状态指示器

状态颜色	说明
白色	表示在恢复点、卷或卷组内未检测到 Exchange 数据库。
黄色	表示尚未运行 Exchange 数据库可安装性检查。
红色	表示至少一个数据库上的可安装性或校验和检查失败。
绿色	表示恢复点包含一个或多个数据库，可安装性检查已启用，并且可安装性检查或校验检查已通过。

SQL 数据库的恢复状态点颜色

下表列出了 SQL 数据库的状态指示器。

表. 150: SQL 数据库状态指示器

状态颜色	说明
白色	表示在恢复点、卷或卷组内未检测到 SQL 数据库。
黄色	SQL 数据库处于脱机状态，表示无法进行和尚未执行可连接性检查。
红色	表示连接性检查失败或 SQL 数据库处于脱机状态。
绿色	表示可附加性检查完成。

① 注: 不与 Exchange 或 SQL 数据库相关联的恢复点将以白色状态指示灯显示。如果恢复点同时存在 Exchange 和 SQL 数据库，则将针对该恢复点显示最严重的状态指示器。

安装恢复点

在 Rapid Recovery 中，可以安装 Windows 机器的恢复点以通过本地文件系统访问存储的数据。

① 注: 要使用 local_mount 实用程序安装 Linux 恢复点，请参阅在 Linux 机器上安装恢复点卷。

① 注: 如果从已启用重复数据消除的机器还原的数据安装恢复点，您还必须在 Core 服务器上启用重复数据消除。

- 1 在 Rapid Recovery Core Console 中，导航至要安装到本地文件系统的机器。
此时将显示所选受保护机器的摘要页面。
- 2 单击恢复点菜单。
此时会显示所选机器的恢复点页面。
- 3 或者，在恢复点窗格中，从恢复点列表中单击右箭头 ► 符号以展开恢复点详细信息，其中显示恢复点中包含的卷。
- 4 在您想要安装的恢复点的行中，单击 ，从下拉菜单中选择安装。
此时会显示安装向导，显示卷页面。
- 5 在卷页面上，选择要安装的恢复点的每个卷，然后单击下一步。
此时将显示安装向导的安装选项页面。
- 6 在安装选项页面中，根据下表中的说明编辑用于安装恢复点的设置。

表. 151: 安装选项设置

选项	说明
本地文件夹	指定用于访问已安装恢复点的路径。 例如, 选择 C:\ProgramData\AppRecovery\MountPoints\ MountPoint1。
安装类型	指定访问已安装恢复点数据的方式: • Read-only (只读) • 只读带此前写入 • 可写
创建此安装的 Windows 共享	(可选) 选中此复选框以指定是否可共享已安装的恢复点, 然后设置对恢复点的访问权限, 包括共享名和允许的组。

7 单击**完成**以安装恢复点。

① **注:** 如果要目录或文件从已安装的恢复点复制到其他 Windows 机器, 则可以使用 Windows 资源管理器复制有关目录或文件及默认权限或原始文件访问权限。有关详细信息, 请参阅[使用 Windows 资源管理器还原目录或文件至使用 Windows 资源管理器还原目录或文件并保留权限](#)。

8 (可选) 在任务执行过程中, 您可以在 Core Console 的**正在运行的任务**下拉菜单中查看其进度, 或者可以在**事件**页面上查看详细信息。有关监测 Rapid Recovery 事件的更多信息, 请参阅[使用任务、警报和日记查看事件](#)。

卸载恢复点

要卸载在 Core 上安装的恢复点, 请完成以下过程中的步骤。

① **注:** 卸载远程安装的恢复点时, 其操作可参阅[断开连接](#)。

- 在 Rapid Recovery Core Console 中, 单击图标栏中的  (更多), 然后选择  **安装**。
此时将显示**安装**页面。有“本地安装”(安装在 Core 上的恢复点) 窗格和“远程安装”(使用 Local Mount Utility 安装的恢复点) 窗格。在每个窗格中, 已安装的各个恢复点将显示在列表中。
 - 要卸载本地安装, 在**本地安装**窗格中, 执行以下操作:
 - 选择本地安装点或您要卸载的点。
 - 要卸载所有恢复点, 单击“本地安装”表标题栏中的复选框以选择所有安装点。
 - 要卸载一个或多个恢复点, 单击表示要断开连接安装点的每行第一列中的复选框。
 - 单击  **卸载**。
此时会显示一个确认对话框。
 - 单击以确认您要卸载所选的恢复点。
系统将卸载本地恢复点。
- ① **注:** 如果启用闹钟警报, 您可能会看到相应安装点正在卸载的警报。
- 要断开连接远程安装的恢复点, 在**远程安装**窗格中, 执行以下操作:
 - 选择远程安装点或您要断开连接的点。
 - 要断开连接所有恢复点, 单击“远程安装”表标题栏中的复选框以选择所有安装点。
 - 要断开连接一个或多个恢复点, 单击表示要断开连接安装点的每行第一列中的复选框。
 - 单击  **断开连接**。
此时会显示一个确认对话框。
 - 单击以确认您要断开所选的恢复点的连接。
系统将断开本地恢复点的连接。

① | 注: 如果启用闹钟警报, 您可能会看到相应安装点正在断开连接的警报。

- 4 酌情确认之前安装的恢复点不再出现在“本地安装”或“远程安装”列表中。

使用 Linux 恢复点

从受保护 Linux 机器上安装和卸载恢复点时, 建议和支持的方法是使用 `local_mount` 实用程序。

下列步骤具体介绍了使用 `local_mount` 安装和卸载 Linux 恢复点。

① | 注: 有关用其他方式管理 Linux 恢复点的信息, 请参阅[管理快照和恢复点](#), 因为所有其他管理可在 **Core Console** 中进行。

在 Linux 机器上安装恢复点卷

使用 Rapid Recovery 中的 `local_mount` 实用程序, 可以从远程将恢复点中的卷装载为 Linux 机器上的本地卷。

① | 注: 执行此过程时, 请勿试图将恢复点安装到包含 `aavdisk` 文件的 `/tmp` 文件夹中。

- 1 创建用于安装恢复点的新目录 (例如, 可以使用 `mkdir` 命令)。
- 2 验证目录是否存在 (例如, 使用 `ls` 命令)。
- 3 以 root 或超级用户身份运行 Rapid Recovery `local_mount` 实用程序, 例如:

```
sudo local_mount
```

- 4 在 Rapid Recovery 安装提示符中, 输入以下命令以列出受保护的机器。

```
lm
```

- 5 看到提示时, 输入 Rapid Recovery Core 服务器的 IP 地址或主机名。

- 6 输入 Core 服务器的登录凭据, 即用户名和密码。

将显示受 Rapid Recovery 服务器保护的机器的列表。按行项目编号、主机/IP 地址和机器的 ID 编号指出每个机器。

例如: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba

- 7 输入以下命令以列出指定机器可用的恢复点:

```
lr <line_number_of_machine>
```

① | 注: 请注意, 您也可以在此命令中输入机器 ID 编号, 而不是行项目编号。

此时将显示该机器的基本和增量恢复点的列表。此列表包含行项目编号、日期和时间戳、卷的位置、恢复点的大小, 以及卷的 ID 编号, 其末端包含一个用于标识恢复点的序列号。

例如, 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

- 8 输入以下命令以选择并在指定的安装点/路径中安装所指定的恢复点。

```
m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
```

该命令中的标志决定如何安装恢复点。您可以使用以下选项之一:

- [r] - 安装只读 (默认)。该标志可以让您安装恢复点, 但您无法对其进行更改。
- [w] - 安装可写。该标志可以让您安装恢复点, 也可对其进行更改。
- [v] - 使用之前的写入安装。带 "V" 标志的安装可让您安装恢复点, 包括在之前可写入安装中所做, 但目前未在恢复点中显示的更改。
- [n] - 不安装 nbd 到 <path>。在您执行本地安装时, nbd (Network Block Device) 在 Core 和受保护机器之间进行套接连接。该标志可让您在不需要安装 nbd 的情况下安装恢复点, 在想手动检查恢复点的文件系统时会有帮助。

① 注: 您也可以在命令中指定行号来代替恢复点 ID 编号, 以标识恢复点。在这种情况下, 使用机器行号 (来自 `lm` 输出), 后跟恢复点行号和卷号, 然后是路径, 例如: `m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>`。例如, 如果 `lm` 输出结果中列出三个受保护机器, 您为 2 号机器输入 `lr` 命令, 并将 23 恢复点卷 `b` 安装到 `/tmp/mount_dir`, 则命令为: `m 2 23 b /tmp/mount_dir`

① 注: 如果从兼容操作系统中安装 BTRFS 卷 (请参阅 *Dell Data Protection | Rapid Recovery Installation and Upgrade Guide* [Dell Data Protection | Rapid Recovery 安装和升级指南] 中的“Rapid Recovery release 6.1 operating system installation and compatibility matrix”[Rapid Recovery 6.1 版操作系统安装和兼容性值表] 主题), 则必须包括以下参数:

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

9 要验证安装是否成功, 请输入以下命令, 该命令将列出已连接的远程卷:

```
l
```

在 Linux 机器上卸载恢复点

要卸载 Linux 机器上的恢复点, 请完成此过程中的步骤。

1 以 root 或超级用户身份运行 Rapid Recovery `local_mount` 实用程序, 例如:

```
sudo local_mount
```

2 在 Rapid Recovery 安装提示符中, 输入以下命令以列出受保护的机器。

```
lm
```

3 看到提示时, 输入 Rapid Recovery Core 服务器的 IP 地址或主机名。

4 输入 Core 服务器的登录凭据 (用户名和密码)。

将显示受 Rapid Recovery 服务器保护的机器的列表。

5 输入以下命令以列出指定机器可用的恢复点:

```
lr <line_number_of_machine>
```

① 注: 请注意, 您也可以在此命令中输入机器 ID 编号, 而不是行项目编号。

将显示和包括该机器的基本和增量恢复点的列表。此列表包含行项目编号、日期/时间戳、卷的位置、恢复点的大小, 以及卷的 ID 编号 (其末端包含一个用于标识恢复点的序列号)。

例如: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

6 运行 `l or list` 命令以获取已安装的 Network Block Device (NBD) 设备列表。如果您安装任何恢复点, 您将在执行 `l or list` 命令后获取 NBD 设备的路径。

7 要卸载恢复点, 请输入以下命令。

```
umount <path_of_nbd-device>
```

8 运行 `l or list` 命令以验证是否成功卸载恢复点。

强制创建快照

通过强制创建快照可强制当前受保护机器进行数据传输。强制创建快照时, 如果其他作业正在运行, 传输会立即开始或被添加到队列中。

您可以从两种类型的快照中选择。

如果您选择增量快照并且以前没有恢复点, 则将捕获基本映像。强制创建快照不会更改任何计划快照的计时。

① 注: Rapid Recovery 支持 Windows 8、Windows 8.1、Windows Server 2012 和 Windows Server 2012 R2 进行基本映像和增量快照的传输。

- 基本映像指机器上受保护卷中的所有数据的快照。
- 增量快照捕获自最后一个快照以来更改的所有数据。

- 1 在 Rapid Recovery Core Console 中，导航至具有要强制创建快照的恢复点的机器或群集。
- 2 在“摘要”页面上的“摘要”窗格中，单击**强制快照**。
此时会显示“强制快照”对话框。
- 3 在“强制快照”对话框中，在复选框中单击一个或多个卷或保护组。
- 4 分别单击**强制快照**或“强制基本映像”。
- 5 如果您选择基本映像，请单击以确认您要创建基本映像。
根据卷中您要备份的数据量，基本映像可能会花费很长时间。

您所选的快照进行排队，并在其他作业完成后立即开始。

移除恢复点

您可以从存储库轻松移除特定机器的恢复点。在 Rapid Recovery 中删除恢复点时，可以指定以下选项之一。

- **删除所有恢复点。**从存储库移除所选受保护机器的所有恢复点。
- **删除一个范围内的恢复点。**移除指定范围内的所有恢复点，包括从当前恢复点向前直到并包含基本映像（机器上的所有数据），以及从当前恢复点向后直到下一个基本映像的所有恢复点。

① 注: 不能恢复已删除的恢复点。如果您需要存储在恢复点中的数据，请考虑先存档数据。

- 1 在 Rapid Recovery Core Console 中，单击**受保护计算机**菜单下您要查看并删除恢复点的计算机名称或 IP 地址。
此时将显示所选受保护计算机的“摘要”视图。
- 2 在计算机名称或 IP 地址的旁边，单击**恢复点**菜单。
此时将显示选定计算机的**恢复点**页面。
- 3 向下滚动到**恢复点**窗格。
选项将在窗格标题下显示，包括“刷新”、“删除范围”和“全部删除”。
- 4 要删除所有当前存储的恢复点，在“恢复点”窗格标题下，单击**全部删除**，然后在确认对话框中单击以确认删除。
- 5 要删除指定数据范围内的一组恢复点，请执行以下操作：
 - a 在“恢复点”窗格标题下，单击**删除范围**。
此时将显示**删除范围内恢复点**对话框。
 - b 在**删除范围内恢复点**对话框的**自**字段中，选择您要开始删除的恢复点。
 - c 在**到**字段中，选择定义您要删除的最后一个恢复点的日期和时间。
 - d 单击 **Delete**（删除）。
 - e 在确认对话框中，单击以确认删除。

删除孤立恢复点链

孤立恢复点是没有与基本映像关联的增量快照。后续快照继续基于此恢复点构建；但是，由于没有基本映像，因此产生的恢复点不完整，并且不太可能包含完成恢复所需的数据。这些恢复点被视为孤立恢复点链的一部分。如果发生这种状况，最佳解决方案是删除该链并创建新基本映像。

有关强制创建基本映像的更多信息，请参阅[强制创建快照](#)。

- 1 在 Rapid Recovery Core Console 中，导航到要删除其孤立恢复点链的受保护机器。
- 2 从在页面顶部的菜单中，单击**恢复点**。
- 3 在“恢复点”窗格中，展开孤立恢复点。
此恢复点在“类型”列中标记为“增量孤立”。
- 4 单击“操作”旁的**删除**。
此时将显示“删除恢复点”窗口。

- 5 在“删除恢复点”窗口中，单击**是**。

小心: 删除此恢复点将删除整个恢复点链，包括在该恢复点之前或之后发生的所有增量恢复点，直到下一个基本映像。此操作无法撤消。
随即删除孤立恢复点链。

手动迁移恢复点到其他存储库

如果希望从存储库移除受保护机器的恢复点而不将其删除，您可以使用此过程将它们手动迁移到其他存储库。此过程涉及从源存储库存档恢复点，然后将存档导入目标存储库。

例如，如果现有存储库已满，或者如果您的需求更改且希望使用不同的 Core 和存储库保护计算机，您可以执行此过程。

小心: 如果您的存储库之前从 AppAssure 5.3 或 5.4 升级且用过复制，Dell 建议在迁移之前对目标 Core 中的每个存储库执行“检查存储库作业”。执行此作业可阻止将任何违规数据复制到新的目标存储库。“检查存储库作业”仅在适用于您的 Core 时才在 UI 中可见，并且运行起来可能需要大量时间。有关此作业的信息，请参阅[有关检查 DVM 存储库的完整性](#)。有关执行此作业的信息，请参阅[在 DVM 存储库上运行检查存储库作业](#)。

- 1 在 Rapid Recovery Core Console 中，暂停对受保护机器或希望迁移其恢复点的计算机的保护。有关更多信息，请参阅[暂停和恢复保护](#)。
- 2 取消受保护机器或希望迁移其恢复点的计算机的所有当前操作，或者等待它们全部完成。
- 3 存档暂停机器的恢复点。有关更多信息，请参阅[创建存档](#)。
- 4 存档和验证存档后，移除您想要迁移的受保护机器上的现有恢复点。有关更多信息，请参阅[移除恢复点](#)。

注: 如果不移除现有恢复点，您将无法更改受保护机器的存储库。

- 5 为已迁移的恢复点创建新的存储库，或者确保存在一个新的目标存储库。有关更多信息，请参阅[创建 DVM 存储库](#)。
 - 如果希望使用现有存储库，继续执行步骤 6。
- 6 完成以下步骤，更改暂停的每台机器的存储库：
 - a 在 Core Console 上，单击导航树中的受保护机器。
 - b 在受保护机器的摘要页面上，单击**设置**。
 - c 在**设置**页面的一般窗格中，单击**存储库**下拉列表，然后选择输入在步骤 4 中创建的存储库的名称。
 - 如果希望使用现有存储库，选择现有存储库的名称。

注: 当迁移恢复点到现有存储库时，确保现有存储库具有足够可用空间以容纳迁移的恢复点。

- d 单击**确定**。
- 7 恢复暂停机器的保护。有关更多信息，请参阅[暂停和恢复保护](#)。
 - 8 为移动的所有受保护机器制作新的基本映像。有关详情，请参阅[强制创建快照](#)并使用“强制基本映像”选项。
 - 9 导入希望迁移机器的已归档数据。有关更多信息，请参阅[导入存档](#)。

还原数据

本节介绍如何还原备份数据。

关于使用 Rapid Recovery 还原数据

Rapid Recovery Core 可立即从恢复点还原数据或将机器恢复到物理或虚拟机机器。恢复点包含数据块级别捕获的代理卷快照。这些快照具有应用程序感知功能，表示在创建快照前，所有打开的事务和滚动事务日志均已完成，同时高速缓存已刷新到磁盘。通过将应用程序感知快照与 Verified Recovery 配合使用，可使 Core 执行多种类型的恢复，包括：

- 恢复文件和文件夹
- 使用 Live Recovery 来恢复数据卷

- 使用 Live Recovery 来恢复 Microsoft Exchange Server 和 Microsoft SQL Server 的数据卷
- 使用 Universal Recovery 进行裸金属恢复
- 使用 Universal Recovery 执行裸金属恢复到不同硬件
- 临时和持续导出至虚拟机

① 注: 当您还原数据或执行虚拟导出时，所使用的恢复点必须是完整恢复点链的一部分。有关恢复点链的更多信息，请参阅[恢复点链和孤立恢复点](#)主题。

了解实时恢复

“实时恢复”是用于将数据存储在 Rapid Recovery Core 中的功能。如果受保护机器遇到非系统 Windows 卷发生的数据故障，则可以从 Rapid Recovery Core 上的恢复点还原数据。在还原向导中选择“实时恢复”使用户能够立即继续业务操作，停机时间接近于零。在还原期间，“实时恢复”可让您立即访问数据，即使 Rapid Recovery 会在后台继续还原数据也不例外。此功能允许接近于零的恢复时间，即使还原涉及数 TB 的数据也不例外。

Rapid Recovery Core 使用基于唯一数据块的备份和恢复技术，实现在恢复过程中对目标服务器的完全用户访问权限。所请求的数据块将按需还原，以实现无缝恢复。

“实时恢复”适用于受 Rapid Recovery Core 保护的物理机器和虚拟机，下列情况例外：

- “实时恢复”可以访问非系统 Windows 卷。无法使用“实时恢复”来还原 C:\ 驱动器和系统保留的分区。
- “实时恢复”可使用 Rapid Recovery Agent 访问基于 Windows 的卷。无代理卷或 Linux 卷不能利用“实时恢复”。

“实时恢复”可让您直接从备份文件还原物理服务器或虚拟服务器。还原非系统卷时，Rapid Recovery 会立即向操作系统显示卷元数据，从而使该数据按需可用。例如，如果 Microsoft Exchange 的数据库卷已损坏，则“实时恢复”可以在数分钟内还原卷、数据库和 Exchange 服务。

此功能提供了恢复大量数据的最快方法，将停机时间减至最少。用户可以立即继续业务操作。

“实时恢复”开始后，恢复的卷及其内容立即可用。Rapid Recovery Core 继续在后台还原数据，即使卷、其数据、应用程序和服务均恢复正常生产状态。如果请求特定数据，后台进程会立即优先还原此数据。这项强大的功能甚至还能够满足最当最严格的服务级别协议。

开始“实时恢复”后，会在受保护机器上快速还原目标卷的元数据（目录结构、安全描述符、NTFS 文件属性、可用空间映射等）。此后，卷及其内容即可供系统使用。Rapid Recovery Agent 开始从 Rapid Recovery Core 服务器还原数据块，将数据库写入目标卷。

对尚未还原的数据的请求将立即得到应答，进行请求的程序或系统不知道刚刚还原了数据块。

从恢复点还原数据

Rapid Recovery 可保护 Windows 和 Linux 机器上的数据。受保护的代理机器的备份作为恢复点保存到 Rapid Recovery Core。从这些恢复点，您可以使用以下三种方式之一还原您的数据。

在 Rapid Recovery Core Console 中，您可以从非系统卷的恢复点还原整个卷，以取代目标机器上的卷。您只能对 Windows 机器执行此操作。有关更多信息，请参阅[关于从恢复点还原卷](#)。

您无法直接从恢复点还原包含操作系统的卷，因为要还原的目标机器正在使用还原过程中包括的操作系统和驱动程序。如果要从恢复点还原到系统卷（例如，代理机器的 C 驱动器），则必须执行 Bare Metal Restore (BMR)。此操作需要从恢复点创建可启动映像，其中包括操作系统、配置文件及数据，然后从该可启动映像启动目标机器以完成还原。如果要还原的机器使用 Windows 操作系统或 Linux 操作系统，则启动映像会有所不同。如果要从恢复点还原到 Windows 机器上的系统卷，请参阅[执行 Windows 机器的裸机还原](#)。如果要从恢复点还原到 Linux 机器上的系统卷，请参阅[执行 Windows 机器的裸机还原](#)。

最后，与还原整个卷相比，您可以从 Windows 机器安装恢复点，然后浏览单个文件夹和文件以便仅恢复特定文件集。有关更多信息，请参阅[使用 Windows 资源管理器还原目录或文件](#)。如果需要执行此操作并保留原始文件权限（例如，在文件服务器上还原用户的文件夹时），请参阅[使用 Windows 资源管理器还原目录或文件并保留权限](#)。

本部分中的主题介绍有关还原物理机上的数据的信息。有关将受保护数据从 Windows 机器导出到虚拟机的更多信息，请参阅[VM 导出](#)。

① 注：恢复 Windows 机器上的数据时，如果要还原的卷已启用 Windows 重复数据消除，则将需要确保核心服务器上也启用了重复数据消除。Rapid Recovery 支持 Windows 8、Windows 8.1、Windows 10、Windows Server 2012 和 Windows Server 2012 R2 进行一般传输（基本映像和增量快照），以及还原数据、裸机还原和虚拟导出。有关支持和不支持备份及恢复的卷类型的更多信息，请参阅[支持的动态和基本卷](#)。

关于从恢复点还原卷

您可将受保护机器上的卷从存储在 Rapid Recovery Core 中的恢复点进行还原。

① 注：在之前的版本中，该流程指执行回滚。

① 注：Rapid Recovery 支持保护和恢复配置为 EISA 分区的机器。支持还扩展至使用 Windows Recovery Environment (Windows RE) 的 Windows 8、Windows 8.1、Windows Server 2012 和 Windows Server 2012 R2 机器。

通过单击 Rapid Recovery 按钮栏中的 Restore（还原）图标，您可开始从 Rapid Recovery Core 控制台的任意位置还原。当您开始以此方式还原时，必须指定要还原哪些在 Core 中受保护的机器，然后追溯到要还原的卷。

您也可进入特定机器的 Recovery Points（恢复点）页面，单击特定恢复点的下拉菜单，然后选择 **Restore（还原）**。如果您以此方式开始还原，请从[步骤 5](#) 开始执行本流程。

如果您要从恢复点还原至系统卷，或使用引导 CD 从恢复点还原，则必须执行 Bare Metal Restore (BMR)。要了解 BMR 的相关信息，请参阅[了解 Windows 机器执行 Bare Metal Restore](#)，要了解 Windows 或 Linux 操作系统的前提条件信息，请分别参阅[对 Windows 机器执行裸机还原的先决条件](#)和[对 Linux 机器执行 Bare Metal Restore 的先决条件](#)。您可按每个操作系统的路线图所述，通过 Core 控制台访问 BMR 功能。您也可通过 Restore Machines Wizard（还原机器向导）执行 BMR。该流程将在向导中的相应点指导您前往流程使用“还原机器向导”执行裸机还原。

从恢复点还原卷

受保护机器必须安装 Agent 软件，并且必须具有用于执行还原操作的恢复点。

完成以下过程，以从恢复点还原卷。

- 1 要从“还原”图标还原受保护机器上的卷，请导航至 Core Console，然后单击 Rapid Recovery 按钮栏中的**还原**。
此时将显示“还原机器向导”。
- 2 在“受保护机器”页面中，选择要还原其数据的受保护机器，然后单击**下一步**。
此时将显示“恢复点”页面。
- 3 在恢复点列表中，搜索要还原到代理机器的快照。
 - 如有必要，请使用页面底部的按钮以显示恢复点的其他页面。
 - （可选）为限制向导的“恢复点”页面中显示的恢复点数量，则可以按卷（如果已定义）或按恢复点的创建日期进行筛选。
- 4 单击任何恢复点以进行选中，然后单击**下一步**。
此时将显示“目标”页面。
- 5 在“目标”页面中，选择要将数据还原到的目标机器，如下所示：
 - 为将数据从所选恢复点还原到同一代理机器，且如果要还原的卷不包括系统卷，则选择**恢复到受保护机器（仅非系统卷）**，确认已选择目标机器，然后单击**下一步**。
此时将显示“卷映射”页面。继续执行[步骤 9](#)。
 - 为将数据从所选恢复点还原到其他受保护机器（例如，使用 Machine1 中的数据替换 Machine2 的内容），则选择**恢复到受保护机器（仅非系统卷）**，从列表中选择目标机器，然后单击**下一步**。

此时将显示“卷映射”页面。继续执行 [步骤 9](#)。

- 如果要从选定恢复点还原到同一机器，或使用启动 CD 的其他机器上，此过程被视为裸机还原 (BMR)。有关 BMR 的信息，请参阅 [了解 Windows 机器执行 Bare Metal Restore](#)。

注：根据想要还原代理机器的操作系统不同，执行 BMR 会有具体要求。要了解这些先决条件，请分别参阅 [对 Windows 机器执行裸机还原的先决条件](#) 和 [对 Linux 机器执行 Bare Metal Restore 的先决条件](#)。

如果要还原的卷包括系统卷，则选择 **使用启动 CD 恢复到任何目标机器**。此选项会提示您创建启动 CD。

- 要利用使用 Restore Machine Wizard 的所选恢复点中的信息继续创建启动 CD，请单击 **下一步** 并继续执行 [执行 Windows 机器的裸机还原](#)。
 - 如果已创建启动 CD 且已使用启动 CD 启动目标机器，则继续执行 [#GUID-07C2DA5A-B8E2-4D01-82D5-E7A1F14E155E/ID-2490-0000487F](#) 主题的步骤 8。
- 如果要从恢复点还原到系统卷（例如，名为 Machine1 的代理机器的 C 驱动器），此过程也被视为 BMR。选择 **使用启动 CD 恢复到任何目标机器**。此选项会提示您创建启动 CD。
 - 要使用所选恢复点中的信息继续创建启动 CD，请单击 **下一步** 并继续执行 [执行 Windows 机器的裸机还原](#)。
 - 如果您已经创建启动 CD，则继续执行 [步骤 6](#)。
- 6 使用启动 CD 启动要还原的机器。有关更多信息，对于 Windows 机器上的 BMR，请参阅 [加载启动 CD 并启动目标机器](#)，对于 Linux 机器上的 BMR，请参阅 [加载 Live DVD 并启动目标机器](#)。
- 7 回到 Core 服务器上，在“还原机器向导”的“目标”页中，选择 **我已有在目标机器上运行的启动 CD**，然后输入想要连接的下表中介绍的机器信息。

表. 152: 机器信息

文本框	说明
IP 地址	要还原的机器的 IP 地址。此 IP 地址与显示在 URC 中的 IP 地址相同。
身份验证密钥	连接所选服务器的特定密码。此身份验证密钥与显示在 URC 中的“身份验证密钥”相同。

- 8 单击 **下一步**。

如果输入的连接信息与 URC 匹配，且如果 Core 和目标服务器在网络上可以正确地互相识别，则将加载所选恢复点的卷。此时将显示“磁盘映射”页面。

要通过“还原机器向导”完成 BMR，请继续执行 [#unique_342/ID-2490-00004B0D](#) 主题中的步骤 9。

注：Rapid Recovery 支持 FAT32 和 ReFS 分区。仅完全还原和 BMR 支持被用作 ReFS 存在的驱动程序限制。可以在用户模式、VM 导出等中实施还原。如果 Core 保护至少一个包含 ReFS 文件系统的代理卷，则应在提供 ReFS 的本机支持的 Windows 8/2012 上安装。否则，功能将受到限制，且涉及安装卷映像之类的操作将无法运行。Rapid Recovery Core Console 会在这些情况下显示适用的错误消息。

此版本还不支持对存储空间磁盘配置（Windows 8.1 的功能）执行 Bare Metal Restore。有关详细信息，请参阅 [Rapid Recovery 安装和升级指南](#)。

- 9 在“磁盘映射”页面中，针对恢复点中要还原的每个卷选择相应的目标卷。如果不希望还原卷，则在“目标卷”列中选择 **不还原**。
- 10 选择 **显示高级选项**，然后执行以下操作：
- 在还原到 Windows 机器时，如果要使用 Live Recovery，则选择 **Live Recovery**。
使用 Rapid Recovery 中的 Live Recovery 即时恢复技术，您可以立即将 Windows 机器已存储恢复点中的数据恢复或还原至物理机或虚拟机，其中包括 Microsoft Windows 存储空间。Live Recovery 不可用于 Linux 机器或使用无代理保护的虚拟机。
 - 如果您想要强制所选卷在还原开始之前卸载，请选择 **强制卸载**。
- 小心：**如果在还原数据之前不强制卸载，则还原可能会失败，并出现卷在使用中错误。
- 11 单击 **下一步**。
- 12 在“卸载数据库”页面上，如果您想要还原的卷包含 SQL 或 Microsoft Exchange 数据库，系统将提示您卸载它们。
如果要在还原完成后重新安装这些数据库，请选择 **还原恢复点后自动重新安装所有数据库**。
- 13 单击 **下一步**。
“警告”页面可能会出现并提示您关闭您想要还原的卷上的所有程序。如果是，再次单击 **下一步**。
- 14 在“摘要”页面上，选择 **重要事项！** 选项 **我了解此操作会将所选卷覆盖为选定恢复点中的数据**，以确认您了解卷还原的后果。

 **警告:** 此选项强调选定恢复点还原日期与时间之后保存的所有数据的后果。

15 单击**完成**。

使用 Windows 资源管理器还原目录或文件

您可以使用 Windows 资源管理器将目录和文件从已安装的恢复点复制并粘贴到任何 Windows 机器。如果要仅将恢复点的一部分分发给用户，则此功能非常有用。

复制目录和文件时，将使用执行复制操作的用户的访问权限，并将其应用于粘贴的目录和文件。如果要将目录和文件还原到用户并保留原始文件权限（例如，在文件服务器上还原用户的文件夹时），请参阅[使用 Windows 资源管理器还原目录或文件并保留权限](#)。

- 1 安装包含要还原的数据的恢复点。有关详细信息，请参阅[安装恢复点](#)。
- 2 在 Windows 资源管理器中，导航至已安装的恢复点，然后选择要还原的目录和文件。右键单击并选择**复制**。
- 3 在 Windows 资源管理器中，导航至要还原数据的目标机器位置。右键单击并选择**粘贴**。

使用 Windows 资源管理器还原目录或文件并保留权限

您可以使用 Windows 资源管理器将目录和文件从已安装的恢复点复制并粘贴到任何 Windows 机器，同时保留文件访问权限。

例如，如果需要还原仅供文件服务器上特定用户访问的文件夹，则可使用复制和带权限粘贴命令，以确保还原的文件保留限制访问的权限。通过这种方式，您可以避免手动将权限应用于还原的目录和文件。

 **注:** “带权限粘贴”命令随 **Rapid Recovery Core** 和 **Agent** 软件一同安装。此命令中 **Local Mount Utility** 中不可用。

- 1 安装包含要还原的数据的恢复点。有关详细信息，请参阅[安装恢复点](#)。
- 2 在 Windows 资源管理器中，导航至已安装的恢复点，然后选择要还原的目录和文件。右键单击并选择**复制**。
- 3 在 Windows 资源管理器中，导航至要还原数据的目标机器位置。右键单击并选择**带权限粘贴**。

 **注:** 在此步骤中，如果禁用右键菜单中的带权限粘贴命令，则 **Windows** 资源管理器无法感知要复制的文件：重复[步骤 2](#) 以在右键菜单中启用“带权限粘贴”命令。

执行群集和群集节点还原

还原是从恢复点还原机器上的卷的过程。对于服务器群集，可以在节点或机器层级执行还原。本部分介绍关于执行群集卷回滚的指南。

执行 CCR 和 DAG (Exchange) 群集的还原

要对 CCR 和 DAG (Exchange) 群集执行还原，请完成以下过程中的步骤。

- 1 关闭所有节点，只保留一个。
- 2 根据[关于从恢复点还原卷](#)和[使用命令行还原 Linux 机器的卷](#)中的说明，使用机器的标准 Rapid Recovery 步骤执行还原。
- 3 还原结束后，安装群集卷的所有数据库。
- 4 打开所有其他节点。
- 5 对于 Exchange，请导航至 Exchange 管理控制台，然后对每个数据库执行 Update Database Copy（更新数据库副本）操作。

对 SCC（Exchange、SQL）群集执行还原

要对 SCC（Exchange、SQL）群集执行还原，请完成以下过程中的步骤。

- 1 关闭所有节点，只保留一个。
- 2 根据[关于从恢复点还原卷和使用命令行还原 Linux 机器的卷](#)中的说明，使用机器的标准 Rapid Recovery 步骤执行还原。
- 3 还原结束后，从群集卷装载所有数据库。
- 4 逐个打开所有其他节点。

① **注：**无需回滚仲裁磁盘。它可自动再生或通过使用群集服务功能再生。

从连接的存档中还原

可通过两种方式从存档还原数据：您可将存档作为源执行裸机还原 (BMR)；也可连接存档，从存档装载恢复点，然后还原存档数据。

当连接存档时，存档会显示在 Core 控制台 Archives（存档）页面的 Attached Archives（已连接存档）下方，存档的内容可通过左侧导航区域进行访问。内容显示在存档名称的下方。存档的机器显示为仅恢复点机器，这样您可采取与访问当前受保护机器相同的方法访问恢复点，方法是：装载恢复点，找到要恢复的项目，使用 Windows Explorer 将项目复制粘贴到目标。

与将存档导入至存储库相比，从连接的存档还原具有优势。

- 与将整个存档导入至存储库相比，从连接存档还原要节省时间。
- 同时，当您导入存档时，会将存档的恢复点添加至存储库。
由于这些存档的恢复点有可能是存储库中最旧的项目，因此可能会根据您的保留策略在下一个每夜作业过程中前滚。
- 最后，即使在断开存档连接后，Core 也会记住与存档的连接关联，这样在之后便可更轻松、更快速地连接存档。
您可通过删除连接移除关联。

要从连接的存档中还原数据，请使用相关链接完成以下步骤：

① **注：**从连接的存档进行还原的流程假定您已具有前滚恢复点的存档。

- 1 连接存档。
- 2 装载包含要恢复数据的恢复点。
- 3 使用以下任一方法还原数据：
 - 从恢复点还原数据，如文件或文件夹。
 - 还原整个恢复点。
 - 将恢复点导出至虚拟机。

相关链接

[附加存档](#)

[安装恢复点](#)

[使用 Windows 资源管理器还原目录或文件](#)

[关于使用 Rapid Recovery 导出至虚拟机](#)

[Windows 备份](#)

[了解存档](#)

[导入存档](#)

[从存档执行 BMR](#)

了解 Windows 机器执行 Bare Metal Restore

本节介绍如何从类似或不同于裸机的硬件还原受保护的 Windows 机器。

Windows 机器的裸机还原

服务器按预期运行时可执行已经为它们配置的任务。仅当服务器发生故障时才会出现异常。如果发生灾难性事件导致服务器无法运行，则需要执行即时步骤以还原该机器的全部功能。

Rapid Recovery 提供了为 Windows 或 Linux 机器执行裸机还原 (BMR) 的功能。BMR 是还原特定系统的全部软件配置的过程。该过程使用“裸机”一词，是因为还原操作不仅会从服务器恢复数据，而且会重新格式化硬盘驱动器，并重新安装操作系统及所有软件应用程序。要执行 BMR，您应指定受保护机器中的恢复点，然后回滚（执行还原）到指定的物理机或虚拟机。如果正执行还原到系统卷，这被视为 BMR。如果正执行还原并需要启动 CD，这也被视为 BMR。其他情况下也可以选择执行 Bare Metal Restore，包括硬件升级或服务器更换。在这两种情况下，从恢复点执行还原，以便升级或更换硬件。

Rapid Recovery 支持从可进行保护或恢复的 FAT32 EFI 分区以及弹性文件系统 (ReFS) 卷引导的 Windows 8、8.1 和 Windows Server 2012、2012 R2 操作系统。

① 注: 此版本还不支持对存储空间磁盘配置 (Windows 8.1 的功能) 执行 Bare Metal Restore。目前，仅支持完整还原和 BMR，因为 ReFS 存在驱动程序限制，因此将在用户模式、VM 导出等情形中执行还原。如果 Core 保护至少一个包含 ReFS 文件系统的代理卷，则应在 Windows 8、Windows 8.1、Windows Server 2012 或 Windows Server 2012 R2 机器上安装，因为这些操作系统提供 ReFS 的本机支持。否则，功能将受到限制且需要安装卷映像之类的操作将无法运行。Rapid Recovery Core Console 将在此类情况下提供相应的错误消息。只有支持的 Linux 操作系统适用于保护或恢复。其中包括 Ubuntu®、Red Hat® Enterprise Linux®、CentOS™ 和 SUSE® Linux Enterprise Server (SLES®)。有关详细信息，请参阅《Dell Data Protection | Rapid Recovery 安装和升级指南》。

可以对物理机或虚拟机执行 BMR。另一个优点是，无论硬件相似还是不同，Rapid Recovery 都可执行 BMR。在 Rapid Recovery 中执行 BMR 会将操作系统与特定平台分隔开来，以实现可移植性。

对相似硬件执行 BMR 的示例包括更换现有系统的硬件驱动器或使用相同机器转换出故障服务器。

对不同硬件执行 BMR 的示例包括使用不同制造商生产的服务器或使用不同配置还原故障服务器。此过程包括创建启动 CD 映像、将映像刻录到磁盘、从启动映像启动目标服务器、连接到 Recovery Console 实例、映射卷、启动恢复，然后监测该过程。Bare Metal Restore 完成后，可以继续执行在还原的服务器上加载操作系统和软件应用程序的任务，然后再创建配置所需的特有设置。

Bare Metal Restore 可用于灾难恢复应用场景，以及在升级或更换服务器时用于迁移数据。

执行 Windows 机器的裸机还原

要执行 Windows 机器的裸机还原，请执行以下任务。

- 创建 Windows 引导映像。引导 CD ISO 映像将用于启动目标驱动器，通过该驱动器您可访问通用恢复控制台，以与 Core 上的备份通信。请参阅 [了解 Windows 机器启动 CD 创建](#)。
 - 如果您要求物理介质启动目标机器，您看需要将引导 CD ISO 映像传输至介质。请参阅 [将启动 CD ISO 映像转移到介质](#)。
 - 在所有情况下，您必须将引导映像加载至目标服务器中，并从引导映像启动服务器。请参阅 [加载启动 CD 并启动目标机器](#)。

① 注: 该流程说明如何通过 **Create Boot CD**（创建引导 CD）对话框管理引导 CD 映像。您也可通过 **Restore Machine Wizard**（还原机器向导）执行这些步骤，从向导的 **Boot CD**（引导 CD）页面启动。当您从向导的 **Destination**（目标）页面中指定使用引导 CD 恢复至任何目标机器时可访问此项。要获取作为裸机还原的一部分，通过 **Restore Machine Wizard**（还原机器向导）管理 Windows 引导映像的分步说明，请参阅 [关于使用“还原机器向导”执行裸机还原](#)。

- 启动 Bare Metal Restore for Windows（Windows 裸机还原）。从引导 CD 启动目标机器后，您可启动 BMR。请参阅 [针对 BMR 使用通用恢复控制台](#)。该过程包含以下任务：
 - 从 Core 上的恢复点启动还原操作。请参阅 [选择恢复点并启动 BMR](#)。
 - 映射卷。请参阅 [关于裸机还原的磁盘映射](#)。

- 如果还原至不同的硬件，且引导 CD 中没有所需的存储和网络驱动程序，则需要通过便携式媒体设备加载驱动程序。要了解详情，请参阅 [使用 Universal Recovery Console 加载驱动程序](#)。
- 通过 Restore Machine Wizard（还原机器向导）执行 BMR。或者，管理 Windows 引导映像和启动 BMR 的流程（包括所有子任务）可通过 Restore Machine Wizard（还原机器向导）执行。要了解启动该向导的信息，请参阅 [关于从恢复点还原卷](#) 的步骤 1 至步骤 5，然后参考[关于使用“还原机器向导”执行裸机还原](#)。
- 验证 Bare Metal Restore（裸机还原）。启动裸机还原后，您可验证和监控进度。请参阅 [验证裸机还原](#)。
 - 您可以监控还原进度。请参阅 [查看恢复进度](#)。
 - 完成之后，您可以启动还原的服务器。请参阅 [启动已还原的目标服务器](#)
 - 故障排除 BMR 过程。请参阅 [通用恢复控制台连接故障排除](#) 和 [修复启动问题](#)。

对 Windows 机器执行裸机还原的先决条件

在开始对 Windows 机器执行 Bare Metal Restore 的过程之前，必须确保符合以下条件 and 标准：

- 一个 64 位中央处理器 (CPU)。Rapid Recovery 启动 CD 包括 Win PE 5.1 操作系统。Rapid Recovery BMR 与基于 x86 的 CPU 不兼容。只能在 64 位 CPU 上执行裸机还原。
- ① **注：**从 6.0 开始才有此新要求。
- 要还原的机器的备份。您必须具有正常运行的 Rapid Recovery Core，其中包含要还原的受保护服务器的恢复点。
 - 要还原的硬件（不论新旧以及是否相似）。目标机器必须符合代理的安装要求；有关详细信息，请参阅 *《Dell Data Protection / Rapid Recovery 安装和升级指南》*。
 - 映像介质和软件。您必须具备空白 CD 或 DVD 和磁盘刻录软件，或创建 ISO 映像的软件。如果要使用虚拟网络计算软件（如 UltraVNC）远程管理机器，则必须具备 VNC Viewer。
 - 兼容的存储驱动程序和网络适配器驱动程序。如果还原到不同的硬件，则目标机器的存储驱动程序和网络适配器驱动程序必须兼容，包括 RAID、AHCI 和芯片组驱动程序（如适用）。
 - 存储空间和分区（如适用）。确保硬盘驱动器上有足够的空间，可在目标机器上创建目标分区以包含源卷。任何目标分区应至少与原始源分区一样大。
 - 兼容的分区。从可进行保护或恢复的 FAT32 EFI 分区以及弹性文件系统 (ReFS) 卷引导的 Windows 8、8.1、Windows 10、Windows Server 2012 和 Windows Server 2012 R2。UEFI 分区将视为简单的 FAT32 卷。完全支持和保护增量传输。Rapid Recovery 支持 UEFI 系统的 BMR，包括自动分区的 GPT 磁盘。

关于使用“还原机器向导”执行裸机还原

通过向导管理 Windows 启动映像包括以下操作：

- 开始创建启动 CD。
- 定义映像 Core 机器上的路径。
- 选择适合您想要还原的硬件的恢复环境。
- （可选）使用网络或 UltraVNC 定义所还原代理的连接参数。
- （可选）为您想要还原的硬件注入驱动程序。
- （可选）将启动映像传输到物理介质。
- 启动您要将数据从 CD 还原到其中的机器。
- 连接到通用恢复控制台。
- 映射卷。
- 从 Core 上的选定恢复点启动裸机还原。

- ① **注：**该过程介绍了如何从“还原机器向导”管理启动 CD 映像，将其作为使用向导执行 BMR 过程的一部分。您也可以从“创建引导 CD”对话框管理启动映像。有关管理在“还原机器向导”外部管理启动 CD 映像的信息，请参阅[了解 Windows 机器启动 CD 创建](#)。

使用“还原机器向导”执行裸机还原

您可以使用“还原向导”创建启动 CD 以及执行裸机还原 (BMR)。

执行 BMR 前，请酌情参阅[对 Windows 机器执行裸机还原的先决条件](#)或[对 Linux 机器执行 Bare Metal Restore 的先决条件](#)。如果从 Core Console 中为 Windows 机器启动您的 BMR，请参阅[执行 Windows 机器的裸机还原](#)。

受保护机器必须已安装 Agent 软件，且必须具有从中执行还原操作的恢复点。

- 1 要在受保护机器上恢复卷，请导航至 Core Console，然后单击 Rapid Recovery 按钮栏中的**还原**。
此时将显示“还原机器向导”。
- 2 在“机器”页面中，选择要恢复的受保护机器，然后单击**下一步**。
此时将显示“恢复点”页面。
- 3 选择您想要用于还原机器的恢复点。
 - （可选）如果要限制显示的恢复点数量，则可以按卷（如果已定义）或按恢复点的创建日期进行筛选。您也可以搜索特定的恢复点。
- 4 单击**下一步**。
- 5 在“目标”页面上，选择**使用启动 CD 恢复到任何目标机器**。
 - 如果尚未在想要还原的机器上装入启动 CD，请单击**下一步**，然后继续执行[步骤 6](#)。
 - 如果您已经将启动 CD 装入到 BMR 目标机器上，请选择**我已经有在目标机器上运行的启动 CD**，单击**下一步**，然后转到[步骤 16](#)。
- 6 在“启动 CD”页面的“输出路径”文本框中，输入应存储启动 CD ISO 映像的路径。
 - 注：**如果要用来存储映像的共享驱动器的磁盘空间不足，可根据需要在路径中创建磁盘；例如 `F:\filename.iso`。
 - 注：**文件扩展名必须为 `.iso`。指定路径时，只能使用字母数字字符、连字符、反斜杠（仅作为路径分隔符）和句点（仅用于分隔主机名和域）。字母 `a` 至 `z` 不区分大小写。请勿使用空格。不允许使用其他符号或标点字符。
- 7 （可选）要设置目标机器的网络参数，或要添加 UltraVNC 功能，请选择**显示高级选项**，然后执行以下步骤之一：
 - 要建立与 BMR 目标的网络连接，请选择**使用下列 IP 地址**，然后根据下表中的说明输入信息。

表. 153: 网络连接选项

选项	说明
IP 地址	所还原机器的 IP 地址。
子网掩码	所还原机器的子网掩码。
默认网关	指定已还原机器的默认网关。
DNS 服务器	指定已还原机器的域名服务器。

- 如果您具有 UltraVNC 帐户并想要使用它来完成 BMR，请选择**添加 UltraVNC**，然后根据下表中的说明输入信息。

表. 154: UltraVNC 连接凭据

选项	说明
密码	您的 UltraVNC 帐户的密码。
端口	您想要用来连接至 BMR 目标的端口。默认端口号为 5900。

- 8 单击**下一步**。
- 9
 - 要为还原的机器建立网络连接，请根据下表中的说明选择**使用以下 IP 地址**。
 - 要定义 UltraVNC 信息，请根据下表中的说明选择**添加 UltraVNC**。
如果需要远程访问 Recovery Console，则使用此选项。使用启动 CD 时，不能使用 Microsoft Terminal Services 登录。

表. 155: UltraVNC 连接

选项	说明
密码	指定此 UltraVNC 连接的密码。
端口	指定此 UltraVNC 连接的端口。 默认端口号为 5900。

- 10 如果对“启动 CD”页面上的选择满意，则单击**下一步**。
- 11 （可选）在“驱动程序注入”页面中，如果您计划还原到不同的硬件，通过完成以下步骤为您的目标系统注入相应的存储控制器和其他驱动程序：
- 从服务器制造商的网站下载驱动程序，然后将其解压缩。
 - 使用相应的压缩实用程序（例如 WinZip）将每个驱动程序压缩成 .zip 文件。
 - 在“还原机器向导”的“驱动程序注入”页面中，单击**添加驱动程序存档**。
 - 浏览档案系统以找到压缩后的驱动程序文件，选择该文件，然后单击**打开**。
 - 重复**步骤 c** 和 **步骤 d**，根据需要直到您注入所有必需的驱动程序。
- 有关注入驱动程序的更多信息，请参阅[了解启动 CD 中的驱动程序注入](#)。

① 注: 并非所有版本的 Windows 都与自动驱动程序注入兼容。如果您的操作系统不兼容，请将驱动程序手动保存到 C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\。

Rapid Recovery 将创建启动 CD ISO 映像。

- 12 单击**下一步**。
- 13 启动 BMR 目标机器，然后完成以下选项之一：
- 如果可以从启动 CD ISO 映像启动目标机器，则立即启动目标机器。
 - 如果不能启动目标机器，将 ISO 映像复制到物理介质（CD 或 DVD），在目标机器中载入光盘，配置要从启动 CD 加载的机器，然后从启动 CD 重新启动。

① 注: 您可能需要更改目标机器的 BIOS 设置，以确保首先加载的卷是启动 CD。

从启动 CD 启动时，目标机器将显示“通用恢复控制台”(URC) 界面。此环境用于直接从 Rapid Recovery Core 还原系统驱动器或所选卷。请记住 URC 中的 IP 地址和身份验证密钥凭据，每次从启动 CD 启动时都会刷新上述信息。

- 14 返回 Core Console 的“连接”页面，如下输入要还原机器的 URC 实例中的身份验证信息：

表. 156: 验证选项

选项	说明
IP 地址	目标机器上的 URC 中提供的 IP 地址。
身份验证密钥	目标机器上的 URC 中提供的身份验证密钥。

- 15 单击**下一步**。
- 16 在“磁盘映射”页面中，如果您想要手动映射卷，请继续执行**步骤 10**。如果要自动映射卷，请完成以下步骤：
- 从“卷映射”下拉菜单中，选择**自动**。
 - 从卷列表中，确保选中要还原的卷。默认会选中所有卷。
如果不想恢复所列的卷，请清除此选项。

① 注: 要执行还原，必须至少选择一个卷。

- 在右侧，选择还原的目标磁盘。
 - 单击**下一步**。
 - 在“磁盘映射预览”页面中，查看所选还原操作的参数。
 - 转至**步骤 18**。
- 17 要手动映射卷，请在“磁盘映射”页面上完成以下步骤：
- 从“卷”下拉菜单中，选择**手动**。
 - 在“目标”列中，选择您想要还原的目标卷。（可选）如果不想还原列出的卷，请清除此选项。

 **注:** 要执行还原, 必须至少选择一个卷。

18 单击**完成**。

 **小心:** 目标驱动器上的所有现有分区和数据将被永久移除, 并被所选恢复点的内容取代, 其中包括操作系统和所有数据。

19 如果要还原的卷包含 SQL 或 Microsoft Exchange 数据库, 如果正在执行 Live Restore, 则在“卸载数据库”页面中将提示您卸载这些数据库。(可选) 如果要在还原完成后重新安装这些数据库, 请选择**还原恢复点后自动重新安装所有数据库**。

20 单击**还原**。

21 在状态消息中, 单击**确定**确认还原过程已开始。

还原即开始。您可以在“事件”页面上监控进度。有关更多信息, 请参阅[使用任务、警报和日记查看事件](#)。

了解 Windows 机器启动 CD 创建

Windows 的裸机还原需要称为启动 CD 的启动映像, 可通过在 Rapid Recovery Core Console 中定义参数进行创建。可根据特定需求创建此映像。您将使用此映像来启动目标 Windows 机器。根据所使用的环境, 您可能需要将此映像传输至 CD 或 DVD 等物理介质。然后, 您必须虚拟或物理加载启动映像, 并从启动映像启动 Windows 服务器。

在对 Windows 机器执行裸机还原 (BMR) 时的第一步是在 Rapid Recovery Core Console 中创建启动 CD 文件。此文件是可启动的 ISO 映像, 其中包含 Rapid Recovery 通用恢复控制台 (URC) 界面, 它是一种用于直接从 Rapid Recovery Core 还原系统驱动器或整个服务器的环境。

所创建的启动 CD ISO 映像与要还原的机器相符; 因此, 其中必须包含正确的网络和大容量存储驱动程序。如果预期将还原到与创建恢复点所在机器不同的硬件, 则必须在启动 CD 中包含存储控制器和其他驱动程序。有关在启动 CD 中注入这些驱动程序的信息, 请参阅[了解在启动 CD 中注入驱动程序](#)。

了解在启动 CD 中注入驱动程序

启动 CD 映像需要存储驱动程序以识别服务器的驱动程序以及网络适配器驱动程序, 以便通过网络与 Rapid Recovery Core 通信。

在为 Windows 生成启动 CD 时, 将自动包括通用的一组 Windows 8.1 x64 存储控制器和网络适配器驱动程序。这将满足更新的 Dell 系统的要求。创建启动 CD 时, 其他制造商的系统或较旧的 Dell 系统可能需要注入存储控制器或网络适配器驱动程序。如果发现所创建的启动 CD 未包含完成还原所需的驱动程序, 则还可以使用 URC 将驱动程序加载到目标机器。有关更多信息, 请参阅[使用 Universal Recovery Console 加载驱动程序](#)。

创建启动 CD 时, 驱动程序注入用于促进 Recovery Console、网络适配器及目标服务器存储之间的可操作性。

从恢复点还原的数据包括硬件之前已有的驱动程序。如果要执行 Bare Metal Restore 到不同的硬件, 则在数据还原到驱动器后, 还必须在使用 URC 还原的操作系统中注入存储控制器驱动程序。这些驱动程序将确保已还原的操作系统使用新的硬件集启动。还原后启动操作系统后, 您便可以下载并安装操作系统与其新硬件互动所需的任何其他驱动程序。

创建启动 CD ISO 映像

Rapid Recovery 使用“启动 CD”一词表示保留用于执行裸机还原 (BMR) 的 ISO 映像的便携式存储位置。该映像包括 Rapid Recovery 通用恢复控制台 (URC)。

要在机器上执行 BMR, 您必须从启动 CD 中启动机器, 这将启动 URC。URC 使我们能够将 BMR 目标连接到您要用来完成还原的恢复点的位置。

- 1 从 Rapid Recovery Core Console (在上面保护了您需要还原的服务器) 的图标栏中, 单击“更多”菜单, 然后单击**启动 CD**。
- 2 在“启动 CD”页面中, 单击**创建启动 CD**。
此时将显示“创建启动 CD”对话框。
- 3 在“创建启动 CD”对话框的**输出路径**文本框中, 输入您要存储启动 CD ISO 映像的位置。

① **注:** 文件扩展名必须为 **.iso**。指定路径时, 只能使用字母数字字符、连字符、反斜杠 (仅作为路径分隔符) 和句点 (仅用于分隔主机名和域)。字母 **a** 至 **z** 不区分大小写。请勿使用空格。不允许使用其他符号或标点字符。

4 在“连接选项”中, 执行以下操作之一:

- 要使用动态主机配置协议 (DHCP) 动态获取 IP 地址, 请选择 **自动获取 IP 地址**。
- 要为 URC 指定静态 IP 地址, 请选择 **使用下列 IP 地址**, 然后输入以下信息:
 - IP 地址
 - 子网掩码
 - 默认网关
 - DNS 服务器

① **注:** 必须指定所有上述四个字段。

5 如果需要远程访问恢复控制台, 并且您安装了 UltraVNC, 请在“UltraVNC 选项”下完成以下步骤:

① **注:** UltraVNC 可让您远程管理正在使用的 URC。使用启动 CD 时, 不能使用 **Microsoft Terminal Services** 登录。

- a 选择 **添加 UltraVNC**。
- b 输入您的 **UltraVNC 密码**。
- c 输入 **UltraVNC 端口**。默认端口号为 5900。

① **注:** 仅当已安装 UltraVNC 时, “UltraVNC 选项”才可用。要使这些选项可用, 请转到 <http://www.uvnc.com/downloads/ultravnc/> 下载适用于 x64 体系结构的 UltraVNC 版本 1.0.9.1 或更高版本。安装它, 然后将 **winvnc.exe** 文件保存至 **C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64**。

6 如果您计划还原到不同的硬件, 通过完成以下步骤为您的目标系统注入相应的存储控制器和其他驱动程序:

① **注:** 并非所有版本的 Windows 都与自动驱动程序注入兼容。如果您的操作系统不兼容, 请将驱动程序手动保存到 **C:\Program Files\AppRecovery\Core\BootCdKit\Drivers**。

- a 从服务器制造商的网站下载驱动程序, 然后将其解压缩。
- b 使用相应的压缩实用程序 (例如 WinZip) 将每个驱动程序压缩成 .zip 文件。
- c 在“创建启动 CD”对话框的“驱动程序”窗格中, 单击 **添加驱动程序存档**。
- d 浏览档案系统以找到压缩后的驱动程序文件, 选择该文件, 然后单击 **打开**。
驱动程序文件将显示在“创建启动 CD”对话框的“驱动程序”窗格中。
- e 重复 **步骤 c** 和 **步骤 d**, 根据需要直到您添加所有必需的驱动程序。
- f 在“驱动程序”窗格中, 选择要移动的驱动程序。

有关注入驱动程序的更多信息, 请参阅 [了解在启动 CD 中注入驱动程序](#)。

7 单击 **创建启动 CD**。

Rapid Recovery 将创建启动 CD, 并使用您提供的文件名保存。

8 要监控此任务的进度, 请转至图标栏, 然后单击“事件”图标。

有关监控 Rapid Recovery 事件的更多信息, 请参阅 [使用任务、警报和日记查看事件](#)。

当 ISO 映像创建完成后, 映像记录将显示在“启动 CD”页面中, 您可以从图标栏的“更多”菜单访问此页面。

要访问 ISO 映像, 请导航至指定的输出路径, 或者单击“启动 CD”页面上的链接, 将映像保存到随后可将它加载到新系统的位置; 例如, 网络驱动器。

将启动 CD ISO 映像转移到介质

创建启动 CD 文件时, 它将作为 ISO 映像存储在您指定的路径中。您必须能够将此映像作为驱动器安装在将执行 Bare Metal Restore 的服务器上。

您可以将启动 CD ISO 映像刻录到系统启动时可访问的光盘 (CD) 或数字视盘 (DVD) 介质。

从启动 CD 启动机器时, 将自动启动 Universal Recovery Console。

如果在虚拟机上执行 BMR，则无需执行此步骤。只要在驱动器中加载 ISO 映像，并编辑该虚拟机的设置以从该驱动器启动。

加载启动 CD 并启动目标机器

创建启动 CD 映像后，需要使用新创建的启动 CD 启动目标服务器。

要连接到 Rapid Recovery Core Console 或要使用 Chromium 下载附加的驱动程序，您必须先加载以太网控制器和网络适配器。有关详情，请参阅[使用 Universal Recovery Console 加载驱动程序](#)。

① **注：**如果使用 DHCP 创建启动 CD，则必须获取 IP 地址和密码。

- 1 在新的服务器上，从适当的位置加载启动 CD 映像，然后从启动 CD 映像启动服务器以加载 Rapid Recovery Agent 软件和 Win PE 5.1。

此时目标机器会显示蓝色的 Dell 屏幕，并在屏幕顶部显示三个图标按钮。

- 2 要打开 Rapid Recovery 通用恢复控制台 (URC) 用户界面，请单击屏幕顶部的 Dell 图标。
机器的 IP 地址和密码会出现在“验证”下面。

① **注：**每次使用启动 CD 启动机器时，将生成新的临时密码。记录“网络适配器设置”窗格中显示的 IP 地址以及“身份验证”窗格中显示的身份验证密码。在随后的数据恢复过程中将需要使用此信息，以便登录回 Console。

① **注：**若未提供 IP 地址，请加载以太网控制器和网络适配器。

- 3 如果要更改 IP 地址，请选择它并单击更改。

① **注：**如果在“创建引导 CD”对话框中指定了 IP 地址，通用恢复控制台将使用该地址并显示在“网络适配器设置”屏幕中。

机器已准备就绪，可以连接到 Core 了；请选择恢复点，然后继续执行裸机还原过程。

针对 BMR 使用通用恢复控制台

对 Windows 机器启动裸机还原 (BMR) 之前，必须满足以下条件：

- 要还原 Core 中保存的恢复点，则必须具备相应的硬件。有关更多信息，请参阅[对 Windows 机器执行裸机还原的先决条件](#)。
- 必须使用启动 CD 映像启动 BMR 目标 Windows 机器。有关更多信息，请参阅[了解 Windows 机器启动 CD 创建](#)。

BMR 将使用您选择的恢复点启动机器。恢复点包括之前硬件中的驱动程序。如果要还原到不同的硬件，则在数据还原到驱动器后，还必须在使用 URC 还原的操作系统中注入存储控制器驱动程序。这些驱动程序将确保已还原的操作系统使用新的硬件集启动。在操作系统启动后，即可下载并安装操作系统与新硬件交互需要的任何附加驱动程序。

要从 Rapid Recovery Core Console 启动 BMR，请执行以下任务。

- [选择恢复点并启动 BMR](#)
- [关于裸机还原的磁盘映射](#)
- [使用 Universal Recovery Console 加载驱动程序](#)

此过程是[执行 Windows 机器的裸机还原](#)中的一个步骤。

关于通用恢复控制台工具

通用恢复控制台 (URC) 包括对可帮助您完成裸机还原 (BMR) 的工具的访问权限。

您可以通过在启动到 URC 的 BMR 目标上，单击 Dell 初始屏幕顶部的中心图标来找到以下工具：

- **Far Manager。**此工具类似于 Windows 资源管理器。它可让您浏览服务器上的文件，直到您完成 BMR 并安装了带有其自己的浏览功能（例如 Windows 资源管理器）的操作系统。

- **Chromium。**此浏览器是 Google Chrome™ 的开放源代码基础，可让您在已加载网络控制器的服务器上通过 URC 浏览 Internet。
- **PuTTY。**此工具是一个开放源代码终端仿真程序。在 Rapid Recovery BMR 的上下文中，它可让您连接到不包括用户界面的 NAS 存储设备中。如果您要从存档还原且存档位于 NAS 上，则可能必须使用此功能。
- **记事本。**如在 Windows 操作系统中一样，此工具可让您键入未格式化的注释以及查看日志文件。
- **任务管理器。**如在 Windows 操作系统中一样，此工具可让您在进行还原时管理进程和监控服务器的性能。
- **注册表编辑器。**如在 Windows 操作系统中一样，此工具可让您更改 BMR 目标的系统注册表。
- **命令提示符。**此工具可让您在 URC 外部的 BMR 目标上执行命令，直到您安装了用户界面为止。

使用 Universal Recovery Console 加载驱动程序

此功能可用于添加未包括在 ISO 映像中、但成功执行裸机还原所必需的任何驱动程序。

此任务是执行 Windows 机器的裸机还原中的一个步骤。它是针对 BMR 使用通用恢复控制台过程的一部分。

创建启动 CD 时，您可以将必要的驱动程序添加到 ISO 映像中。启动到目标机器后，您也可以从 Universal Recovery Console (URC) 加载存储或网络驱动程序。

如果要还原到不同的硬件，则必须注入存储控制器、RAID、AHCI、芯片组和其他驱动程序（如果尚未包含在启动 CD 中）。一旦在还原过程后重新启动系统，这些驱动程序使操作系统能够成功操作目标服务器上的所有设备。

要使用 URC 加载驱动程序，请完成以下过程之一中的步骤。

- [使用便携式介质在通用恢复控制台中加载驱动程序](#)
- [在 URC 中使用 Chromium 加载驱动程序](#)

使用便携式介质在通用恢复控制台中加载驱动程序

以下任务是此过程的先决条件：

- [创建启动 CD ISO 映像](#)
- [将启动 CD ISO 映像转移到介质](#)
- [加载启动 CD 并启动目标机器](#)

完成以下步骤使用便携式介质设备在通用恢复控制台 (URC) 中加载驱动程序。

- 1 在连接到互联网的机器上，从制造商的网站下载服务器的驱动程序，然后将其解压缩。
- 2 使用相应的压缩实用程序（例如 WinZip）将每个驱动程序压缩成 .zip 文件。
- 3 将驱动程序的 .zip 文件复制并保存到便携式介质设备（如 USB 驱动器上）。
- 4 从连接的机器中移除介质并将其插入启动目标服务器。
- 5 在目标服务器上，加载启动 CD，然后启动机器。
此时会显示戴尔启动画面。
- 6 要启动 URC，请单击 **Dell** 图标。
URC 将打开到“启动 CD 驱动程序管理器”选项卡。
- 7 展开**其他设备**列表。
此列表中显示了硬件必需但启动 CD 中未包括的驱动程序。
- 8 右键单击列表中的某个设备，然后单击**加载驱动程序**。
- 9 在“选择驱动程序加载模式”窗口中，选择以下选项之一：
 - 加载单个驱动程序软件包（驱动程序将加载而不验证设备支持）
 - 扫描文件夹的驱动程序软件包（将在选定文件夹搜索选定设备的驱动程序）
- 10 展开便携式介质设备的驱动器，选择驱动程序（文件扩展名为 .inf），然后单击**确定**。
驱动程序将加载到当前的操作系统。
- 11 在“信息”窗口中，单击**确定**确认驱动程序已成功加载。

12 根据需要为要加载的每个驱动程序重复此步骤。

在 URC 中使用 Chromium 加载驱动程序

以下任务是此过程的先决条件：

- [创建启动 CD ISO 映像](#)
- [将启动 CD ISO 映像转移到介质](#)
- [加载启动 CD 并启动目标机器](#)

处于 URC 中时，要使用通过启动 CD 安装的 Chromium 浏览器来加载驱动程序，请完成以下过程。

- 1 在目标服务器上，加载启动 CD，然后启动机器。
此时会显示戴尔启动画面。
- 2 要启动 URC，请单击 **Dell** 图标。
URC 将打开到“启动 CD 驱动程序管理器”选项卡。
- 3 在 BMR 目标上，单击屏幕顶部的工具（中心图标），然后单击 **Chromium**。
- 4 在 Chromium 浏览器中，导航至可下载所需驱动程序的网站。
- 5 将一个或多个驱动程序下载到所选位置（例如本地文件夹或网络文件共享）。
- 6 展开**其他设备**列表。
此列表中显示了硬件必需但启动 CD 中未包括的驱动程序。
- 7 右键单击列表中的某个设备，然后单击**加载驱动程序**。
- 8 在“选择驱动程序加载模式”窗口中，选择以下选项之一：
 - 加载单个驱动程序软件包（加载驱动程序而不验证设备支持）
 - 扫描文件夹以找到驱动程序软件包（将在选定文件夹中搜索选定设备的驱动程序）
- 9 导航至在其中保存驱动程序的位置，选择驱动程序，然后单击**确定**。
驱动程序将加载到当前的操作系统。
- 10 在“信息”窗口中，单击**确定**确认驱动程序已成功加载。
- 11 根据需要为要加载的每个驱动程序重复此步骤。

选择恢复点并启动 BMR

通用恢复控制台 (URC) 在裸机还原 (BMR) 目标机器上可访问之后，您必须选择要还原的恢复点。

导航至 Core Console 以选择要加载的恢复点，然后指定 Recovery Console 作为已还原数据的目标。

① | 注：对所有 **Windows** 机器执行 BMR 时，此步骤为必需步骤；而对 **Linux** 机器执行 BMR 时，此步骤为可选步骤。

此任务是[执行 Windows 机器的裸机还原](#)中的一个步骤。它是[针对 BMR 使用通用恢复控制台](#)过程的一部分。

如果从 Core Console 对 Linux 机器执行 BMR，则此任务也是对 [Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。它是[使用命令行对 Linux 机器启动 Bare Metal Restore](#) 过程的一部分。

- 1 在 Rapid Recovery Core Console 中，从受保护的机器列表中，单击要还原的受保护机器的名称。
此时将显示所选计算机的摘要页面。
- 2 单击**恢复点**。
- 3 在要用于 BMR 的恢复点旁边，单击下拉菜单，然后单击**还原**。
此时将显示“还原机器向导”。
- 4 选择**使用启动 CD 恢复到任何目标机器**。
- 5 选择**我已有在目标机器上运行的启动 CD**。
此时将显示身份验证文本框。

6 根据下表中的说明输入要还原的机器的信息。

表. 157: 目标机器信息

文本框	说明
IP 地址	要还原的机器的 IP 地址。此 IP 地址与显示在 URC 中的 IP 地址相同。
身份验证密钥	连接所选服务器的特定密码。此身份验证密钥与显示在 URC 中的“身份验证密钥”相同。

7 单击 **下一步**。

如果输入的连接信息与 URC 匹配，且如果 Core 和目标服务器在网络上可以正确地互相识别，则将加载所选恢复点的卷，并将显示“磁盘映射”页面。在这种情况下，您的下一步是映射卷。

8 请继续至[关于裸机还原的磁盘映射](#)以了解您的磁盘映射选项。

关于裸机还原的磁盘映射

连接到 Universal Recovery Console 后，您需要在恢复点中列出的卷与目标硬件上现有的卷之间映射卷。

Rapid Recovery 尝试自动映射卷。如果接受默认映射，则会对目标机器上的磁盘进行清理并重新分区，且将删除任何之前存在的数据。执行对齐时将按照卷在恢复点中所列出的顺序，并根据大小等因素将卷相应地分配给磁盘等。如果目标驱动器上有足够的空间，则使用自动磁盘对齐时将无需分区。磁盘可被多个卷使用。请注意，如果手动映射驱动器，则无法两次使用同一磁盘。

对于手动映射，还原之前必须已正确格式化新机器。目标机器在恢复点中的每个卷必须有一个单独的分区，包括系统保留卷。有关详情，请参阅[针对 BMR 使用通用恢复控制台](#)。

完成以下其中一个磁盘映射选项的步骤：

- [为 BMR 自动映射磁盘](#)
- [为 BMR 手动映射磁盘](#)

小心: Rapid Recovery 支持 FAT32 和 ReFS 分区，目前，仅支持完整还原和 BMR，因为 ReFS 存在驱动程序限制，因此将在用户模式、虚拟机导出等情形中执行还原。如果 Core 保护至少一个包含 ReFS 文件系统的代理程序卷，则应在提供 ReFS 的本机支持的 Windows 8、Windows 8.1、Windows 10、Windows Server 2012 和 Windows Server 2012 R2 机器上安装它。否则，功能将受到限制，且涉及安装卷映像之类的操作将无法运行。Rapid Recovery Core Console 会在这些情况下显示适用的错误消息。

小心: 不支持对存储空间磁盘配置（Windows 8.1 的功能）执行裸机还原。有关详细信息，请参阅 *Dell Data Protection | Rapid Recovery 安装和升级指南*。

此任务是执行 Windows 机器的裸机还原中的一个步骤。它是[针对 BMR 使用通用恢复控制台](#)过程的一部分。

如果从 Core Console 对 Linux 机器执行 BMR，则此任务也是对 Linux 机器执行 Bare Metal Restore 中的一个步骤。它是[启动 Linux 的裸机还原](#)过程的一部分。

为 BMR 自动映射磁盘

此过程可让您在使用还原机器向导进行裸机还原 (BMR) 期间自动映射磁盘。

要自动选择您想要恢复的卷以及要还原它们的位置，请完成以下过程中的步骤。

- 1 在还原机器向导的“磁盘映射”页面上，在“卷映射”旁边，从下拉菜单中选择**自动**。
- 2 在左侧的表中，验证是否已列出并选中了相应的卷。
① | 注: 对于 BMR，通常至少应还原系统保留卷和系统卷（通常但并非总是 C:\ 卷）。您必须至少选择一个卷才能执行 BMR。
- 3 在右侧的表中，选择目标机器上要映射至的一个或多个磁盘。
- 4 单击 **下一步**。
- 5 在“磁盘映射预览”页面上，查看还原点卷与还原的目标卷的映射。

6 要开始还原，请单击**完成**。

小心: 如果选择开始还原，则目标驱动器上的所有现有分区和数据将被永久移除，并被所选恢复点的内容取代，其中包括操作系统和所有数据。

为 BMR 手动映射磁盘

本过程介绍如何指定哪些磁盘应该存储在所还原机器上的哪些位置。

要手动映射磁盘，您必须先在 BMR 目标机器的命令行中使用 DiskPart 以创建和格式化目标卷。有关更多信息，请参阅 Microsoft Developer Network 上的 [DiskPart 命令行选项（标准 7 SP1）](#)。

完成以下过程中的步骤，手动选择您想要恢复的卷以及要还原它们的位置。

- 1 在“还原机器向导”的“磁盘映射”页面中，从下拉菜单中选择**手动**。
注: 如果执行裸机还原 (BMR) 的机器的驱动器上不存在卷，则无法看到此选项或者需要手动映射卷。
- 2 在“卷映射”区域的“源卷”下，确认选择了源卷，并且在下方列出并选中了相应的卷。
- 3 在“目标”下，从下拉菜单中选择相应的目标，即对所选恢复点执行 BMR 的目标卷，然后单击**还原**。
- 4 在确认对话框中，查看恢复点源卷与还原目标卷的映射。
- 5 要开始还原，请单击**开始还原**。

小心: 如果选择开始还原，则目标驱动器上所有现有分区和数据将被永久移除，并替换为所选恢复点的内容，其中包括操作系统和所有数据。

从存档执行 BMR

Rapid Recovery 可让您使用存档的恢复点从裸机还原机器。

以下任务是此过程的先决条件：

- [创建启动 CD ISO 映像](#)
- [加载启动 CD 并启动目标机器](#)

从通用恢复控制台 (URC) 中，您可以访问 Rapid Recovery Core 并检索恢复点以进行还原。您也可以选择从存储在存档中的恢复点执行裸机还原。URC 可让您访问此存档，不管它是位于本地驱动器、网络共享上还是云帐户上。

- 1 在 URC 中，单击**从存档还原**选项卡。
- 2 在**位置类型**下拉列表中，选择存档的位置。可以从以下选项中选择。
 - 本地
 - 网络
 - 云
- 3 根据选择的位置类型，输入下表所述的凭据。

表. 158: 位置类型凭据选项

位置类型	选项	说明
本地	本地路径	存档的当前位置。
	网络	存档的当前位置。
网络	用户	网络共享访问权限的用户名。
	密码	网络共享访问权限的密码。
云	云类型	云存储位置的提供商。从以下选项中进行选择：

位置类型	选项	说明
		• Microsoft Azure • Amazon™ S3 • OpenStack 技术支持 • Rackspace® Cloud Files
4	如果您选择了一种云类型，请填写与您的云提供程序相关的凭据。	
	• 对于 Microsoft Azure，请完成以下步骤： 1 输入以下凭据： • 存储帐户名称 • 访问密钥 2 对于“容器名称”，从下拉列表选择一个容器。 3 对于“云路径”，从下拉列表中选择存档的路径。 • 对于 Amazon™ S3，请完成以下步骤： 1 输入以下凭据： • 访问密钥 • 机密密钥 2 对于“容器名称”，从下拉列表选择一个容器。 3 对于“云路径”，从下拉列表中选择存档的路径。 • 对于 Powered by OpenStack 或 Rackspace Cloud Files 帐户，请完成以下步骤： 1 输入以下信息： • 地区 • 用户 2 选择以下选项之一： • 密码 • API 密钥 3 在文本框中，根据您在步骤 C 中的选择输入信息。 4 输入以下信息： • 租户 ID • 验证 URL • 容器名称 • 云路径	
5	单击 下一步 。	
6	在 机器 页面上，选择要还原的机器，然后单击 下一步 。	
7	在 恢复点 页面上，选择要用于还原机器的恢复点，然后单击 下一步 。	
8	在 映射 页面上，选择下列其中一个选项，然后完成相应的步骤：	
	• 从卷映射下拉列表中，选择自动。 1 在左侧的表中，验证是否已列出并选中了相应的卷。 ① 注：对于 BMR，通常至少应还原系统保留卷和系统卷（通常是但并非始终是 C:\ 卷）。您必须至少选择一个卷才能执行 BMR。 2 在右侧的表中，选择目标机器上要卷映射至的一个或多个磁盘。 • 从卷映射下拉列表中，选择手动。 ① 注：要手动映射磁盘，您必须先要在命令行上使用 DiskPart 来创建和格式化目标卷。有关更多信息，请参阅 Microsoft Developer Network 上的 DiskPart 命令行选项（标准 7 SP1）。 ① 注：如果要执行裸机还原 (BMR) 的机器的驱动器上不存在卷，则无法看到此选项或者需要手动映射卷。 • 在目标卷下，从下拉菜单中，选择恢复点中每个卷的相应目标卷。	

- 9 在**安装映射路径**文本框中，输入映射文件的临时存储的目标。
默认位置是 `X:\ProgramData\AppRecovery\IndexEntriesMaps`。

① 注：要确保您的目标具有足够的可用空间，请将总安装卷容量除以 **1,024**。例如，使用公式 $(\text{Mount volume total capacity}) / 1024 = \text{Free space}$ ，而 $1 \text{ TB} / 1024 = 1 \text{ GB}$ 。

- 10 单击**还原**。
URC 会将卷映射到一个或多个新的磁盘。
- 11 单击**还原**。
URC 会将数据还原到目标机器。您可以在**还原进度**选项卡上查看进度。
- 12 还原完成后，取出启动 CD。
- 13 要将 BMR 目标机器引导到 Windows，请重新启动机器。

加载驱动程序到操作系统

此过程介绍如何在裸机还原 (BMR) 目标上将驱动程序加载到操作系统。

要将驱动程序注入操作系统，您需要先完成以下任务：

- 在 Rapid Recovery Core Console 中使用“启动 CD 构建程序”创建启动 CD。有关更多信息，请参阅[创建启动 CD ISO 映像](#)。
- 在 BMR 目标中加载启动 CD。有关更多信息，请参阅[加载启动 CD 并启动目标机器](#)。
- 为存储和网络加载所需的驱动程序或控制器。有关更多信息，请参阅[使用 Universal Recovery Console 加载驱动程序](#)。
- 使用 Rapid Recovery Core Console 中的“还原机器向导”或使用通用恢复控制台 (URC) 中的存档来执行还原。有关更多信息，请参阅[使用“还原机器向导”执行裸机还原](#)和[从存档执行 BMR](#)。

执行还原后，只有当您在裸机还原 (BMR) 目标上将驱动程序注入到操作系统后，该过程才完成。此任务是在 URC 中加载驱动程序的补充。

- 在您选择的 BMR 过程（参见先决条件）中单击“还原”后，单击**现有 Windows 驱动程序管理**选项卡。
- 从下拉列表中选择操作系统。
URC 将搜索可用的驱动程序。
- 要加载附加的驱动程序，请单击**强制加载**。
- 浏览档案系统以找到压缩后的驱动程序文件，然后选择该文件。
- 单击**确定**。
URC 会将驱动程序加载到您选择的操作系统中。
- 为需要加载的每个附加驱动程序重复[步骤 3](#)至[步骤 5](#)。
- 重新启动 BMR 目标机器。
BMR 便完成了。如果您在重新启动时遇到问题，请参阅[修复启动问题](#)。

对 Linux 机器执行 Bare Metal Restore

在 Rapid Recovery 中，您可以对 Linux 机器执行裸机还原 (BMR)，包括还原系统卷。还原 Linux 机器时，将回滚到启动卷恢复点。可以通过命令 `local_mount` 公用程序及在 Core Console UI 中使用 BMR 功能。

- ⚠ 小心：**在开始 BMR 过程之前，请确保要还原的任何 Linux 机器不包括 **ext2** 启动分区。在采用 **ext2** 分区类型的机器上执行 BMR 时，该过程通常会产生无法启动的机器。在此情况下，要执行 BMR，您需要在开始保护和备份机器前，将任何 **ext2** 分区转换成 **ext3**、**ext4** 或 **XFS** 分区。
- ⚠ 小心：**当 BMR 之后首次启动已还原的 Linux 机器时，**Rapid Recovery** 将创建已还原机器的基本映像。取决于机器上的数据量，该过程花费的时间比增量快照要多。有关基本映像和增量快照的更多信息，请参阅[了解保护计划](#)。

要对 Linux 机器执行 Bare Metal Restore，请执行以下任务。

- 管理 Linux 启动映像。此 Linux Live DVD 启动 ISO 映像用于启动目标驱动器，您可以在其中访问 Universal Recovery Console 以与 Core 上的备份通信。请参阅[管理 Linux 引导映像](#)。
 - 要获取 BMR 的启动映像，您必须先确定您需要哪个映像，然后从许可证门户下载该映像。请先后参阅[关于 Linux 的启动 ISO 映像](#)和[下载 Linux 的启动 ISO 映像](#)。
 - 如果需要物理介质以启动目标 Linux 机器，则将需要将 ISO 映像传输到介质。请参阅[将 Live DVD ISO 映像保存至介质](#)。
 - 在所有情况下，您需要从启动映像将启动映像加载到目标服务器并启动服务器。请参阅[加载 Live DVD 并启动目标机器](#)。
 - 加载介质后，您必须将 Linux 机器连接到 Rapid Recovery Core。请参阅[从 Rapid Recovery Core 连接到 BMR 目标](#)。
- 管理分区。在 Linux 机器上执行 BMR 之前，您可能需要创建或安装分区。请参阅[管理 Linux 分区](#)。
 - 要执行 BMR 的 Linux 系统必须具有与恢复点中源卷相同的分区。如果需要，您可能需要在目标系统上创建额外的分区。请参阅[在目标驱动器上创建分区](#)。
 - 如果要执行手动 BMR，则必须先安装分区。请参阅[从命令行安装分区](#)。从命令行执行 BMR 的过程包括安装分区的步骤。请参阅[使用命令行对 Linux 机器启动 Bare Metal Restore](#)。

如果您正为 Core Console 中的 BMR 使用自动分区，则无需安装分区。Rapid Recovery 将还原要还原的恢复点中包括的相同分区。
- 对 Linux 启动 Bare Metal Restore。从 Live DVD 启动映像启动目标机器后，便可启动 BMR。所需的任务取决于是从 Rapid Recovery 用户界面还是使用 local_mount utility 公用程序从命令行执行此操作。请参阅[启动 Linux 的裸机还原](#)。
 - 如果使用 Core Console，则将需要从 Core 上的恢复点启动还原。请参阅[选择恢复点并启动 BMR](#)。
 - 如果使用 Core Console，则将需要从 UI 映射卷。请参阅[关于裸机还原的磁盘映射](#)。
 - （可选）如果从命令行还原，则可以启动 screen 公用程序，以便增强在终端控制台中滚动和查看命令的能力。默认情况下，将会打开此公用程序。如果您已将其关闭，则可以再次启动。有关详情，请参阅[启动 Screen 实用程序](#)。
 - 如果使用 local_mount，则会在命令行执行所有任务。有关详情，请参阅[使用命令行对 Linux 机器启动 Bare Metal Restore](#)。
- 验证 Bare Metal Restore。启动 Bare Metal Restore 后，您可以验证并监测有关进度。请参阅[从命令行验证裸机还原](#)。
 - 您可以监测还原的进度。请参阅[查看恢复进度](#)。
 - 完成后，您便可以启动已还原的服务器。请参阅[启动已还原的目标服务器](#)。
 - BMR 过程故障排除。请参阅[通用恢复控制台连接故障排除](#)和[修复启动问题](#)。

对 Linux 机器执行 Bare Metal Restore 的先决条件

在开始对 Linux 机器执行 Bare Metal Restore 的过程之前，必须确保符合以下条件 and 标准：

- 要还原的机器的备份。您必须具有正常运行的 Rapid Recovery Core，其中包含要还原的受保护服务器的恢复点。
- 要还原的硬件（不论新旧以及是否相似）。目标机器必须符合代理的安装要求；有关详细信息，请参阅《Rapid Recovery 安装和升级指南》。
- Live DVD 启动映像。获取包含 Linux 可启动版本的 Linux Live DVD ISO 的映像。从 Dell Data Protection | Rapid Recovery 许可证门户（网址为 <https://licenseportal.com>）下载。如果下载 Live DVD 时遇到任何问题，请联系 Dell Rapid Recovery 支持。
- 映像介质和软件。如果使用物理介质，则必须具有空白 CD 或 DVD 和磁盘刻录软件或创建 ISO 映像的软件。
- 兼容的存储驱动程序和网络适配器驱动程序。如果还原到不同的硬件，则目标机器的存储驱动程序和网络适配器驱动程序必须兼容，包括目标操作系统的 RAID、AHCI 和芯片集驱动程序（如适用）。
- 存储空间和分区（如适用）。确保硬盘驱动器上有足够的空间，可在目标机器上创建目标分区以包含源卷。任何目标分区应至少与原始源分区一样大。
- 还原路径。确定还原路径，即设备文件描述符的路径。要确定设备文件描述符的路径，请在终端窗口中使用 fdisk 命令。

管理 Linux 引导映像

对 Linux 执行 Bare Metal Restore 需要 Live DVD 启动映像，您可以从 Dell Data Protection | Rapid Recovery 许可证门户下载此映像。您将使用此映像来启动目标 Linux 机器。根据所使用的环境，您可能需要将此映像传输至 CD 或 DVD 等物理介质。然后，您必须虚拟或物理加载启动映像，并从启动映像启动 Linux 服务器。

① **注：**Live DVD 之前称为 Live CD。

管理 Linux 启动映像是[对 Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。

您可以执行以下任务：

关于 Linux 的启动 ISO 映像

对 Linux 机器执行裸机还原 (BMR) 的第一步是从 Dell Data Protection | Rapid Recovery 许可证门户 下载 Linux Live DVD ISO 映像。Live DVD 可与 Rapid Recovery 支持的所有 Linux 文件系统搭配使用，并包括 Linux 可启动版本、屏幕实用程序以及 Rapid Recovery 通用恢复控制台 (URC) 界面。Rapid Recovery 通用恢复控制台是一种用于直接从 Rapid Recovery Core 还原系统驱动器或整个服务器的环境。

① 注：国际标准化组织 (ISO) 是由各国负责设定文件系统标准的机构的代表所组成的国际组织。ISO 9660 是用于光盘介质数据交换的文件系统标准，并且支持多种操作系统。ISO 映像是包含每个磁盘扇区以及磁盘文件系统的数据的存档文件或磁盘映像。

下载 Linux 的启动 ISO 映像

您必须下载与您的 Rapid Recovery 版本匹配的 Live DVD ISO 映像。Live DVD 的最新版本可从 Dell Data Protection | Rapid Recovery 许可证门户获得，网址为 <https://licenseportal.com>。如果您需要另一个版本，请联系 Dell Rapid Recovery 支持。

① 注：有关 Dell Data Protection | Rapid Recovery 许可证门户的更多信息，请参阅“Dell Data Protection | Rapid Recovery 许可证门户”（《Dell Data Protection | Rapid Recovery 许可证门户用户指南》）。

此任务是[对 Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。它是[管理 Linux 引导映像](#)过程的一部分。

要下载 Live DVD ISO 映像，请完成以下过程中的步骤。

- 1 登录到 Dell Data Protection | Rapid Recovery 许可证门户（网址为 <https://licenseportal.com>）。
- 2 访问下载区域。
- 3 向下滚动到“基于 Linux 的应用程序”，并在“Linux Live DVD”部分单击**下载**。
- 4 保存 Live DVD ISO 映像。如果要还原虚拟机，则可以将其保存到网络位置，然后将虚拟机设置为从与 ISO 映像关联的 CD 或 DVD 驱动器启动。
- 5 如果要物理机还原，则将启动 CD ISO 映像刻录到可以启动目标机器的光盘 (CD) 或数字视盘 (DVD)。有关详情，请参阅[将 Live DVD ISO 映像保存至介质](#)。

将 Live DVD ISO 映像保存至介质

下载 Linux Live DVD 文件后，它作为 ISO 映像存储在指定的路径中。您必须能够从 Live DVD 映像启动目标 Linux 机器。

此任务是[对 Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。它是[管理 Linux 引导映像](#)过程的一部分。

您可以将启动 CD ISO 映像刻录到光盘 (CD) 或数字视盘 (DVD) 介质中。

如果在虚拟机上执行 BMR，则无需执行此步骤。只要在驱动器中加载 ISO 映像，并编辑该虚拟机的机器设置以从该驱动器启动。您也可以使用虚拟导出还原 linux 虚拟机。有关详情，请参阅[VM 导出](#)。

加载 Live DVD 并启动目标机器

获取 Live DVD ISO 映像后，您需要从新创建的 Live DVD 启动 Linux 机器。

此任务是[对 Linux 机器执行裸机还原](#)中的一个步骤。它是[管理 Linux 启动映像](#)过程的一部分。

- 1 导航至新服务器，然后从相应的位置加载 Live DVD 映像。指定服务器将从 Live DVD 映像启动。
- 2 启动机器。
此时将显示 Rapid Recovery 初始屏幕，并打开终端窗口，其中显示机器的 IP 地址和身份验证密码。

① 注：每次使用 Live DVD 映像启动机器时，将生成新的临时密码。

- 3 记录简介屏幕上显示的 IP 地址和身份验证密码。在随后的数据恢复过程中将需要使用此信息，以便登录回 Console。

从 Rapid Recovery Core 连接到 BMR 目标

使用 Live DVD 启动目标 Linux 机器后，用户便可以从 Core 连接到该机器以开始裸机恢复过程。您可以使用以下两种方法之一执行此过程：

- 从 Rapid Recovery Core Console 启动还原。有关更多信息，请参阅[启动 Linux 的裸机还原](#)。
- 使用 aamount 实用程序从命令行启动还原。有关更多信息，请参阅[使用命令行对 Linux 机器启动 Bare Metal Restore](#)。

管理 Linux 分区

执行 BMR 时，将还原数据的目标驱动器必须与要还原的恢复点具有相同的分区。您可能需要创建分区以满足此要求。

您可以使用 aamount 公用程序从命令行启动还原，也可以从 Rapid Recovery Core Console 启动还原。如果要通过用户界面还原，则必须先安装分区。

管理 Linux 分区是[对 Linux 机器执行 Bare Metal Restore](#)中的一个步骤。

您可以执行以下任务：

相关链接

- [在目标驱动器上创建分区](#)
- [在目标驱动器上格式化分区](#)
- [从命令行安装分区](#)

在目标驱动器上创建分区

通常，执行 BMR 时，目标驱动器是可能包含单个分区的新卷。目标机器上的驱动器必须与恢复点具有相同的分区表，包括卷大小。如果目标驱动器未包含相同的分区，则必须在执行 Bare Metal Restore 之前创建分区。使用 fdisk 实用程序在目标驱动器上创建与源驱动器上相同的分区。

△ | 小心：下面的过程只是一个示例。客户环境会有所不同。您应更改所使用的命令，以与您环境的具体情况相匹配。

此任务是[对 Linux 机器执行 Bare Metal Restore](#)中的一个步骤。它是[管理 Linux 分区](#)过程的一部分。

- 1 （可选）您可以使用 Screen 公用程序。默认情况下，此公用程序将启动并保持活动，直到重新引导机器为止。

① | 注：如果您显式将其关闭，然后要再次打开，请参阅[启动 Screen 实用程序](#)。

- 2 在命令行中输入以下命令，并按 **Enter** 以更改以管理员身份运行的权限，然后列出现有磁盘分区：

```
sudo fdisk -l
```

此时将显示所有卷的列表。

此示例假设要创建分区的卷是 /dev/sda。如果卷不同（例如，对于老式驱动器，可能会显示 /dev/hda），则相应地更改命令。

- 3 要创建新的启动分区，请输入以下命令，然后按 **Enter**：

```
sudo fdisk /dev/sda
```

- 4 要创建新的启动分区，请输入以下命令，然后按 **Enter**：

```
n
```

- 5 要创建新的主分区，请输入以下命令，然后按 **Enter**：

```
p
```

- 6 要指定分区号，请输入分区号，然后按 **Enter**。例如，要指定分区 1，则输入 1，然后按 **Enter**。

- 7 要使用第一个扇区 2048，请按 **Enter**。

- 8 要将相应的数量分配给启动分区，请输入加号并分配数量，然后按 **Enter**。

例如，要为启动分区分配 500 M，请输入以下命令，然后按 **Enter**：

```
+512000K
```

- 9 要切换启动分区的可启动标志（以便可启动分区），请输入以下命令，然后按 **Enter**：

```
a
```

- 10 要为相应的分区分配可启动标志，请输入分区号，然后按 **Enter**。例如，要为分区 1 分配可启动标志，请输入 1，然后按 **Enter**。

- 11 根据需要对磁盘进行分区。

- 12 要保存 fdisk 实用程序中的所有更改，请输入以下命令，然后按 **Enter**：

```
w
```

在目标驱动器上格式化分区

在目标驱动器上的新卷上创建分区之后，要执行裸机还原，如果您未在使用自动分区，则必须格式化分区，然后才能安装这些分区。如果您遇到这种情况，请按照以下步骤采用 ext3、ext4 或 XFS 格式来格式化分区。

对于所有其他情况，您不需要如本主题中所述那样格式化分区。

此任务是对 [Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。它是 [管理 Linux 分区](#) 过程的一部分。

- 1 （可选）您可以使用 Screen 公用程序。默认情况下，此公用程序将启动并保持活动，直到重新引导机器为止。

① **注：**如果您显式将其关闭，然后要再次打开，请参阅 [启动 Screen 实用程序](#)。

- 2 在命令行中输入以下命令，并按 **Enter** 以更改以管理员身份运行的权限，然后列出现有磁盘分区：

```
sudo fdisk -l
```

此时将显示所有卷的列表。

此示例假设要格式化的分区是 /dev/sda1。如果卷不同（例如，对于老式驱动器，可能会显示 /dev/hda），则相应地更改命令。

- 3 请根据要用于目标分区的格式，选择以下命令之一：

- 要格式化 ext3 格式的分区，请输入以下命令，然后按 **Enter**：

```
sudo mkfs.ext3 /dev/sda1
```

- 要格式化 ext4 格式的分区，请输入以下命令，然后按 **Enter**：

```
sudo mkfs.ext4 /dev/sda1
```

- 要采用 XFS 格式来格式化分区，请输入以下命令，然后按 **Enter**：

```
sudo mkfs.xfs /dev/sda1
```

所选分区进行相应格式化。

- 4 （可选）如果需要格式化其他分区，请重复此过程。

从命令行安装分区

如果使用 Rapid Recovery Core Console 执行 BMR，则必须先在目标机器上安装相应的分区。在 Universal Recovery Console 的命令行中执行此操作。

此任务是对 [Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。它是 [管理 Linux 分区](#) 过程的一部分。

执行还原前，要在 Linux 机器上安装分区，请完成以下过程中的步骤。

- 1 在命令行中输入以下命令，并按 **Enter** 以更改以管理员身份运行的权限，然后列出现有磁盘分区：

```
sudo fdisk -l
```

此时将显示所有卷的列表。

- 2 将执行 BMR 所需的所有分区格式化到安装目录。这些分区必须与恢复点中的卷匹配。例如，如果要安装的卷是 sda1，且安装目录是 mnt，则输入以下命令，然后按 **Enter**：

- 3 将执行 BMR 所需的所有分区安装到安装目录。这些分区必须与恢复点中的卷匹配。例如，如果要安装的卷是 sda1，且安装目录是 mnt，则输入以下命令，然后按 **Enter**：

```
mount /dev/sda1 /mnt
```
- 4 根据需要重复步骤 3，直到已安装所有需要的卷。
安装卷后，您可以从 Rapid Recovery Core Console 执行目标 Linux 机器还原。请参阅[启动 Linux 的裸机还原](#)。

启动 Linux 的裸机还原

对 Linux 机器启动裸机还原 (BMR) 之前，必须满足以下条件。

- 要还原 Core 中保存的恢复点，则必须具备相应的硬件。有关更多信息，请参阅[对 Linux 机器执行 Bare Metal Restore 的先决条件](#)。
- 必须使用 Live DVD 启动映像启动 BMR 目标 Linux 机器。有关更多信息，请参阅[管理 Linux 引导映像](#)。
- 要还原的 Linux 机器上的卷数量必须与恢复点中的卷数量匹配。您还必须决定是从 Rapid Recovery Core Console 还原还是使用 local_mount 从命令行还原。有关更多信息，请参阅[管理 Linux 分区](#)。
- 如果要从 Core Console UI 还原，则启动 BMR 的第一步是选择相应的恢复点，然后指定从 Universal Recovery Console 获得的 IP 地址和临时密码以启动硬件还原。然后，您必须映射驱动器并开始还原。

此过程是[对 Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。

要从 Rapid Recovery Core Console 启动 BMR，请执行以下任务。

- [选择恢复点并启动 BMR](#)
- [关于裸机还原的磁盘映射](#)

如果要使用 local_mount 实用程序从命令行还原，则必须先设置相应的权限、安装卷、执行 local_mount、从机器列表中获取关于 Core 的信息、连接 Core、获取恢复点列表、选择要回滚到裸机的恢复点，以及启动还原。

(可选) 您可能想要启动 Screen 实用程序。

要从命令行启动 BMR，请执行以下任务。

- [启动 Screen 实用程序](#)
- [使用命令行对 Linux 机器启动 Bare Metal Restore](#)

启动 Screen 实用程序

Live DVD 中包括 Screen 实用程序，此实用程序在从 Live DVD 启动到 Universal Recovery Console 时可用。Screen 可让用户在单个 Secure Shell (SSH) 会话或控制台窗口中同时管理多个 shell。此公用程序允许您在终端窗口中执行一项任务（如验证安装的卷），并在该任务正在运行时，打开或切换到其他 shell 实例以执行另一项任务（如运行 local_mount 公用程序）。

Screen 实用程序还具有其自身的回卷缓冲区，可让您滚动屏幕以查看大量的数据，如恢复点列表。

① | 注: 此实用程序为方便使用而提供；您可以选择使用 **Screen 实用程序**。

默认情况下，Screen 实用程序在 Live DVD 启动的机器上启动。然而，如果您已经关闭此应用程序，必须使用以下过程从 Live DVD 启动 Screen 实用程序。

如果机器从 Live DVD 启动，则在终端窗口中，键入 screen 然后按 **Enter**。

Screen 实用程序启动。

使用命令行对 Linux 机器启动 Bare Metal Restore

在要执行 BMR 的机器上可访问 Live DVD ISO 映像，且目标机器与要还原到裸机的恢复点的卷数量和大小匹配后，则可以使用 local_mount 公用程序从命令行启动还原。

① | 注: 此组件以前称为 **aamount**。

如果要使用 Rapid Recovery Core Console UI 执行 BMR，请参阅[选择恢复点并启动 BMR](#)。

① | 注: 执行此过程时，请勿试图将恢复点安装到包含 **rapidrecovery-vdisk**（前身为 **aavdisk**）文件的 **/tmp** 文件夹中。

此任务是对 Linux 机器执行 Bare Metal Restore 中的一个步骤。它是使用命令行对 Linux 机器启动 Bare Metal Restore 过程的一部分。

要在 Core 上选择恢复点以回滚到物理或虚拟 BMR 目标机器，请完成以下过程中的步骤。

- 1 要以 root 身份运行 Rapid Recovery local_mount 公用程序，请输入以下命令，然后按 **Enter**:
`sudo local_mount`
- 2 要列出受保护机器，请输入以下命令，然后按 **Enter**:
`lm`
- 3 显示提示时，根据下表中的说明输入 Rapid Recovery Core 的连接信息，并在输入每个所需的命令后按 Enter:

表. 159: Rapid Recovery Core 连接信息

文本框	说明	要求
Rapid Recovery Core 的 IP 地址或主机名	Rapid Recovery Core 的 IP 地址或主机名。	是
域	Rapid Recovery Core 的域。此项为可选。	否
用户	Core 上的管理用户的用户名	是
密码	用于将管理用户连接到 Core 的密码。	是

此时将显示列表，其中显示受 Rapid Recovery Core 保护的机器。它按行项目编号、主机显示名称或 IP 地址和机器的 ID 编号列出所找到的机器。

- 4 要列出想要还原的机器的恢复点，请使用以下语法输入列出恢复点命令，然后按 **Enter**:
`lr <machine_line_item_number>`

① | 注: 您也可以在此命令中输入机器 ID 编号，而不是行项目编号。

此时列表将显示该机器的基本和增量恢复点。此列表包括：

- 行项目编号
- 日期和时间戳
- 恢复点中按字母编号的卷列表
- 卷的位置
- 恢复点的大小
- 卷的 ID 号，其末端包含一个用于标识恢复点的序列号

- 5 要选择用于还原的恢复点，请输入以下命令，然后按 **Enter**:
`r <recovery_point_ID_number> <path>`

△ | 小心: 必须确保未安装系统卷。

① | 注: 如果从 Live DVD 启动机器，则未安装系统卷。

此命令将 ID 所指定的卷映像从 Core 回滚到指定路径。还原路径是设备文件描述符的路径，而不是所安装到的目录。

① **注:** 您也可以在命令中指定行号来代替恢复点 ID 编号，以标识恢复点。在该情况下，使用代理/机器行号（来自 `lm` 输出），后跟恢复点行号和卷号（来自恢复点中按字母编号的卷列表），再后跟路径。例如：

```
r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>
```

例如，键入：

```
r 1 24 a /dev/sda1
```

在此命令中，`<path>` 是实际卷的文件描述符。

- 6 系统提示继续时，输入 `y` 进行确认，然后按 **Enter**。
还原开始后，系统将显示一系列消息，以告知您还原完成的状态。

① **注:** 如果收到异常消息，则可以在 `local_mount.log` 文件中找到有关异常的详细信息。`local_mount.log` 文件位于 `/var/log/apprecovery` 中。

- 7 成功完成还原后，键入 `exit` 并按 **Enter** 可退出 `local_mount`。
- 8 下一步是验证还原。有关详情，请参阅[从命令行验证裸机还原](#)。

使用命令行还原 Linux 机器的卷

在 Rapid Recovery 中，您可以使用命令行 `local_mount` 实用程序还原受保护 Linux 机器上的卷。

① **注:** 在以前，此过程称为**回滚**。执行此过程时，请勿试图将恢复点安装到包含 `rapidrecovery-vdisk`（前身为 `aavdisk`）文件的 `/tmp` 文件夹中。**Rapid Recovery Core Console** 内的受保护机器也支持还原卷操作。有关更多信息，请参阅[关于从恢复点还原卷](#)。

△ **小心:** 如要还原系统或根 (`/`) 分区或整个操作系统，请参阅[对 Linux 机器执行 Bare Metal Restore](#)。

- 1 以 root 用户身份运行 Rapid Recovery `local_mount` 实用程序，例如：

```
sudo local_mount
```

- 2 在 Rapid Recovery 安装提示符中，输入以下命令以列出受保护的机器。

```
lm
```

- 3 看到提示时，输入 Rapid Recovery Core 服务器的 IP 地址或主机名。

- 4 输入此服务器的登录凭据，即用户名和密码。

此时将显示一个列表，其中显示此 Rapid Recovery 服务器所保护的机器。它按机器的项目编号、主机/ IP 地址和 ID 号列出找到的受保护机器（例如：7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2）。

- 5 要列出指定机器当前已安装的恢复点，请输入以下命令：

```
lr <machine_line_item_number>
```

① **注:** 请注意，您也可以在此命令中输入机器 ID 编号，而不是行项目编号。

此时将显示一个列表，其中显示该机器的基本和增量恢复点。此列表包含行项目编号、日期/时间戳、卷的位置、恢复点的大小，以及卷的 ID 编号，其末端包含一个用于标识恢复点的序列号（例如，“293cc667-44b4-48ab-91d8-44bc74252a4f:2”）。

- 6 要选择进行还原的恢复点，请输入以下命令：

```
r <volume_recovery_point_ID_number> <device_path>
```

此命令将 ID 所指定的卷映像从 Core 回滚到指定路径。还原路径是设备文件描述符的路径，而不是所安装到的目录。

- 您也可以在命令中指定行号来代替恢复点 ID 编号，以标识恢复点。在这种情况下，使用受保护机器行号（来自 `lm` 输出），后跟恢复点行号和卷号，然后是路径，例如：`r <machine_line_item_number> <recovery_point_line_number> <volume_letter> <path>`。在此命令中，`<path>` 是实际卷的文件描述符。

例如，如果 `lm` 输出列出了三个受保护机器，您为受保护机器号 `1r` 输入了 `2` 命令，并且想要将 `23` 恢复点卷 `b` 还原到安装到目录 `/dev/sda5`，的卷，命令将为：

```
r2 23 b /dev/sda5
```

① 注：如果需要，可以还原到 `/`。如果使用 **Live DVD** 执行裸机还原，则假定为您想要还原到不同的机器。有关更多信息，请参阅[启动 Linux 的裸机还原](#)。

7 系统提示继续时，输入 `y` 进行确认。

还原继续后，系统将显示一系列消息，以告知您状态。

8 成功完成还原后，如果目标以前受到保护并已安装，则 `local_mount` 实用程序会自动安装内核模块并将其重新连接到所还原的卷。如果未受到保护且未安装，则需要将还原的卷安装至本地磁盘，然后验证文件是否已还原（例如，可以依次使用 `sudo mount` 命令和 `ls` 命令）。

验证裸机还原

执行裸机还原后，您便可以验证还原的进度。成功完成此操作后，您便可以启动已还原的服务器。如果在连接到通用恢复控制台来完成恢复时遇到困难，以及需要修复已还原机器的启动问题时，可参见提供的一些故障排除步骤。

您可以执行以下任务：

相关链接

[查看恢复进度](#)

[启动已还原的目标服务器](#)

[通用恢复控制台连接故障排除](#)

[修复启动问题](#)

查看恢复进度

要查看从 Rapid Recovery Core Console 启动的恢复点还原数据的进度（包括裸机恢复），请完成以下过程中的步骤。

- 1 启动从恢复点还原数据的过程后，在任务正在执行时，您可以从 Core Console 的“正在运行的任务”下拉菜单查看其进度。
- 2 （可选）您可以在“事件”页面中查看详细信息。有关监控 Rapid Recovery 事件的更多信息，请参阅[查看任务、警报和事件](#)。

启动已还原的目标服务器

要启动已还原的目标服务器，请完成以下过程中的步骤。

① 注：在启动已还原的目标服务器之前，应验证恢复是否成功。有关更多信息，请参阅[查看恢复进度](#)。

此任务是[执行 Windows 机器的裸机还原](#)中的一个步骤。它是[验证裸机还原](#)过程的一部分。

- 1 在目标服务器上，验证 Rapid Recovery 通用恢复控制台处于活动状态。
- 2 从已还原的服务器弹出启动 CD（或断开包含启动 CD 映像的物理介质）。
- 3 在通用恢复控制台中，单击屏幕顶部的“电源”菜单图标，然后单击**重新启动**。
- 4 指定正常启动操作系统。
- 5 登录到机器。系统将还原到其在恢复点中捕获到的状态。

通用恢复控制台连接故障排除

以下是连接到启动 CD 映像的故障排除步骤，这些步骤是[选择恢复点并启动 BMR](#)过程的一部分。

如果显示一个错误，指示 Core 无法连接到远程服务器，则可能会存在多个可能的原因。

- 验证 URC 中显示的 IP 地址和当前密码是否与“Recovery Console 实例”对话框中输入的信息相同。
- 要访问要还原数据的服务器，Core 必须能够在网络中识别该服务器。要确定是否可以执行服务器标识操作，您可以在 Core 中打开命令提示符，然后 ping 目标 BMR 服务器的 IP 地址。您也可以在此目标服务器上打开命令提示符，然后 ping Rapid Recovery Core 的 IP 地址。
- 验证 Core 与目标 BMR 服务器之间的网络适配器设置是否兼容。

修复启动问题

以下任务是此过程的先决条件：

- [创建启动 CD ISO 映像](#)
- [加载启动 CD 并启动目标机器](#)
- [使用 Universal Recovery Console 加载驱动程序](#)

要修复启动问题，请完成以下过程中的步骤。请记住，如果要还原到不同的硬件，则必须注入存储控制器、RAID、AHCI、芯片集和其他驱动程序（如果尚未包含在启动 CD 中）。这些驱动程序使操作系统能够成功操作目标服务器上的所有设备。有关详情，请参阅[使用 Universal Recovery Console 加载驱动程序](#)。要修复目标服务器上的启动问题，请完成以下过程。

- 1 从通用恢复控制台中，单击**现有 Windows 驱动程序管理器**选项卡。
- 2 单击**修复启动问题**。
系统将自动修复目标服务器启动记录中的启动参数。

从命令行验证裸机还原

Dell 建议执行以下步骤以从命令行验证已完成的裸机还原。

此任务是[对 Linux 机器执行 Bare Metal Restore](#)中的一个步骤。

相关链接

- [对已还原的卷执行文件系统检查](#)
- [使用命令行使还原的 Linux 机器可启动](#)

对已还原的卷执行文件系统检查

从命令行执行 Bare Metal Restore 后，您应对已还原的卷执行文件系统检查，以确保从恢复点还原的数据未损坏。

此任务是[对 Linux 机器执行 Bare Metal Restore](#)中的一个步骤。它是[从命令行验证裸机还原](#)过程的一部分。

要对已还原的卷执行文件系统检查，请执行以下任务。

- 1 在已还原的 Linux 机器的 Universal Recovery Console 命令行中，要验证是否已安装相应的分区，请输入以下命令，然后按 **Enter**：
`df`
- 2 如果未安装已还原的卷，则跳到[步骤 3](#)。如果已安装已还原的卷，则输入以下命令并按 Enter 以卸载该卷：
`umount <mount point>`
- 3 要对已还原的卷运行文件系统检查，请输入以下命令，然后按 Enter：
`fsck -f <volume>`
如果 fsck 未返回任何错误，则表明文件系统通过验证。
- 4 要再次安装相应的卷，请以 `mount <volume> <folder>` 格式键入以下命令，然后按 **Enter**。

例如，如果卷路径为 prod/sda1 且要安装的文件夹路径为 mnt，则输入以下命令，然后按 **Enter**：

```
mount /dev/sda1 /mnt
```

使用命令行使还原的 Linux 机器可启动

对已还原的卷完成干净的文件系统检查后，必须创建可启动分区。

GNU Grand Unified Bootloader (GRUB) 是一款启动加载程序，可让管理员配置用于启动系统的操作系统或特定内核配置。完成 BMR 后，必须修改 GRUB 的配置文件，以便机器将相应的通用唯一标识符 (UUID) 用于根卷。在此步骤之前，您必须安装根卷和启动卷，然后检查每个卷的 UUID。这将确保您能从分区启动。

① 注：该过程适用于使用 **GRUB1 或 GRUB2** 的 **Linux 机器**。使用该过程时，确保启动分区处于正常和受保护状态。

Grub 或 GRUB2 通常随 Linux 操作系统安装。您可以使用 Linux 发行版随附的版本执行此过程。如果未安装 GRUB 的某个版本，则您必须重新安装适合您的 Linux 发行版的默认版本。

△ 小心：当 BMR 之后首次启动已还原的 Linux 机器时，**Rapid Recovery** 将创建已还原机器的基本映像。取决于机器上的数据量，该过程花费的时间比增量快照要多。有关基本映像和增量快照的更多信息，请参阅[了解保护计划](#)。

此任务是对 [Linux 机器执行 Bare Metal Restore](#) 中的一个步骤。它是从[命令行验证裸机还原](#)过程的一部分。

要使用命令行创建可启动分区，请执行以下任务。

1 您必须先安装根卷，然后再安装启动卷。使用以下命令安装每个已还原的卷：

a 要安装根卷，请输入以下命令，然后按 **Enter**：

```
mount /<restored volume[root]> /mnt
```

例如，如果 /dev/sda2 是根卷，则键入 mount /dev/sda2 /mnt，然后按 **Enter**。

b 要安装启动卷，请输入以下命令，然后按 **Enter**：

```
mount /<restored volume[boot]> /mnt/boot
```

例如，如果 /dev/sda1 是启动卷，则键入 mount /dev/sda1 /mnt/boot，然后按 **Enter**。

① 注：一些系统配置可能会在根卷中包含启动目录。

2 如果卷大小不断增加 — 即，如果新 Linux 机器上的目标卷大于恢复点中的卷 — 则必须删除任何现有位图数据文件。

3 使用 blkid 命令获取新卷的通用唯一标识符 (UUID)。输入以下命令，然后按 **Enter**：

```
blkid [volume]
```

① 注：您还可以使用 **ls -l /dev/disk/by-uuid** 命令。

4 如果要对目标机器上的全新磁盘执行 BMR，则在根卷的 fstab 中注释掉交换分区。

5 应在已还原的卷而不是 Live DVD 中修改 fstab 和 mtab 路径。无需修改 Live DVD 中的路径。要准备安装 Grand Unified Bootloader (GRUB)，请输入以下命令。在输入每个命令后，按 **Enter**：

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

```
mount --bind /sys /mnt/sys
```

6 要更改根目录，请输入以下命令，然后按 **Enter**：

```
chroot /mnt /bin/bash
```

7 获取已安装恢复点 /etc/fstab 文件中的分区旧 UUID，将其与根卷（适用于 Ubuntu 和 CentOS）、启动卷（适用于 CentOS 和 RHEL），或数据分区的 UUID 进行比较，请键入以下命令，然后按 **Enter**：

```
less /mnt/etc/fstab
```

8 获取已安装恢复点 /etc/mtab 文件中的分区旧 UUID，将其与根卷（适用于 Ubuntu 和 CentOS）、启动卷（适用于 CentOS 和 RHEL），以及数据分区的 UUID 进行比较，请键入以下命令，然后按 **Enter**：

```
less /mnt/etc/mtab
```

- 9 如果使用 SLES 11, 则通过键入以下命令, 在每条命令后面按 Enter 来安装 GRUB:
- ```
grub-install --recheck /dev/sda
```
- ```
grub-install /dev/sda
```
- 10 如果使用 Ubuntu、CentOS 6.x、RHEL 6.x 或 Oracle Linux 6.x, 则通过键入以下命令然后按 Enter 来安装 GRUB:
- ```
grub-install /dev/sda
```
- 11 如果使用 SLES 12、CentOS 7、RHEL 7 或 Oracle 7, 则通过键入以下命令然后按 Enter 来安装 GRUB2:
- ```
grub2-install /dev/sda
```
- 12 完成安装后, 请运行下列更新之一:
- 对于 SLES:

```
grub-install.unsupported --recheck /dev/sda
```

```
grub-install.unsupported /dev/sda
```

```
update-grub
```

❗ 注: 如果 `update-grub` 命令在 Linux 发行版上不存在, 则省略此选项。
 - 对于其他发行版:

```
grub-install /dev/sda
```

```
update-grub
```

❗ 注: 如果 `update-grub` 命令在 Linux 发行版上不存在, 则省略此选项。
- 13 从 CD-ROM 或 DVD 驱动器移除 Live DVD 磁盘, 然后重新启动 Linux 机器。

生成并查看报告

本节提供了 Rapid Recovery Core 和 Rapid Recovery Central Management Console 中可用报告的概览。

主题：

- [关于 Rapid Recovery 报告](#)
- [Central Management Console](#)

关于 Rapid Recovery 报告

您可以从 Rapid Recovery Core Console 中生成报告。也可从 Central Management Console 获取其中部分报告。

下表对可用报告进行了说明。

表. 160: Rapid Recovery 报告

报告类型	说明
作业报告	提供了与成功作业、失败作业和出错作业的状态有关的报告。可以在失败报告中进一步查看失败的作业。 可以从 Core Console 和 Central Management Console 中运行此作业类型。 • 从 Core 运行时，此报告可以指定一个或多个 Core 的详细信息。默认情况下，这组信息包括所有机器的作业 - 指定 Core 中的每个受保护机器、复制机器和仅有恢复点的机器。在报告参数中，您可以自定义报告。使用筛选器选择或排除一些机器。您也可以选择或排除机器独立的作业（在此情况下，报告仅显示 Core 作业的状态）。 • 在 Core Console 中从受保护机器的角度运行时，生成的报告仅显示该受保护机器的作业的状态。 • 从 Central Management Console 运行时，此报告可以指定控制台中配置的任意 Core 或 Core 组的组合的详细信息。唯一可配置的参数是报告类型和日期范围。 有关此报告类型的更多信息，请参阅了解“作业”报告。
失败报告	根据指定的条件提供了有关失败的 Core 作业的信息。 可以从 Core Console 和 Central Management Console 中运行此作业类型。 • 从 Core 运行时，此报告可以包括受保护机器的详细信息或排除这些信息。与作业报告类似，此报告也可以仅从 Core 中选定的受保护机器运行。生成的报告仅显示与所选受保护机器的失败作业有关的详细信息。 • 从 Central Management Console 运行时，此报告可以指定控制台中配置的任意 Core 或 Core 组的组合的失败事件。唯一可配置的参数是报告类型和日期范围。 有关此报告类型的更多信息，请参阅了解失败报告。
摘要报告	提供摘要信息。默认情况下，这组信息包括所有机器的作业 - 指定 Core 中的每个受保护机器、复制机器和仅有恢复点的机器。在报告参数中，您可以自定义报告。使用筛选器选择或排除一些机器。您也可以选择或排除机器独立的作业（在此情况下，报告仅显示 Core 作业的状态）。 从任何单个受保护机器的角度来看，此报告不可用。 可以从 Core Console 和 Central Management Console 中运行此作业类型。 • 从 Core Console 运行时，此报告中的信息类别包括 Core、许可证和存储库。信息以列表、图表和表格的形式显示。

报告类型	说明
	从 Central Management Console 运行时，此报告可以指定控制台中配置的任意 Core 或 Core 组的组合的摘要信息。唯一可配置的参数是报告类型和日期范围。 此报告中的信息类别包括 Core、许可证和存储库。摘要报告还包括有关受保护机器的报告以及成功的作业与所有作业之比。信息以列表、图表和表格的形式显示。 有关此报告类型的更多信息，请参阅了解摘要报告。
存储库报告	此报告类型提供了所选 Core 上所有存储库的报告。您还可以选择 Core 可用的任何单个存储库。仅可从 Core Console 使用此报告，并且仅可从 Core 的角度进行查看。 有关此报告类型的更多信息，请参阅了解存储库报告。
计划报告	您也可以从 Core Console 中计划其中任意报告。计划报告会导致您指定的报告按照您定义的计划重复生成。（可选）您可以在每次报告生成时创建电子邮件通知。有关计划、修改、暂停或删除报告的更多信息，请参阅从 Core Console 管理计划报告。

根据您选择的报告类型和参数，您可以对一个或多个 Rapid Recovery Core 生成报告，或为一个或多个受保护机器生成报告。

在 Central Management Console 中，您可以为该控制台中配置的任意 Core 或 Core 组的组合生成报告。

从 Core Console 生成报告

您可以从 Core Console 按需生成报告。以下规则适用：

- 可以从 Core 的角度生成所有报告。
- 此外，可从受保护机器的角度生成两种作业类型（“作业”报告和“失败”报告）。对于此类报告，仅生成与所选机器相关的数据。
- 仅当所选 Core（或受保护机器）上的作业失败时，失败报告才包含数据。

生成按需报告的方法类似（无论是从 Core 的角度生成报告，还是从受保护机器的角度生成报告）。但是，导航略有不同。

您也可以计划重复生成报告。有关计划、修改、暂停或删除报告的更多信息，请参阅[从 Core Console 管理计划报告](#)。

按需生成 Core 报告

按照[关于 Rapid Recovery 报告](#)主题中的描述，您可以从 Core Console 中生成所有可用的报告。

完成以下过程中的步骤，从 Rapid Recovery Core 的角度生成报告。

- 1 导航至 Rapid Recovery Core Console。
- 2 从图标栏中，单击 （更多），然后选择**报告**。
此时会显示**作业报告**页面。在页面标题中报告名称的右侧，将出现一个向下的箭头，可以从中选择另一个报告类型。

如果您想要生成作业报告，请继续执行[步骤 6](#)以开始指定您的报告条件。
- 3 要选择另一个报告类型，请单击报告名称右侧的箭头查看可用报告的菜单。
- 4 有关定义计划报告的信息，请参阅[计划报告](#)。
- 5 要仅生成存储库报告，请跳至[步骤 11](#)。
- 6 对于作业、作业摘要、故障或摘要报告，请从**日期范围**下拉菜单中选择一个日期范围。
如果您没有选择日期范围，将使用默认选项（最近 31 天）。您可以从下表的选项中选择。

选项	说明
过去 24 小时	报告过去一天（与您生成报告的时间相比）的活动。
过去 7 天	报告上一周（与您生成报告的时间相比）的活动。
过去 31 天	报告过去 31 天（与您生成报告的时间相比）的活动。
过去 90 天	报告过去 90 天（与您生成报告的时间相比）的活动。
过去 365 天	报告过去 1 年（与您生成报告的时间相比）的活动。
所有时间	此时间段跨 Core 的终生。
自定义	该时间段需要您进一步指定开始日期和结束日期。
当月至今	报告从当前日历月的第一天到您生成报告的日期之间的活动。
当年至今	报告从当前日历年的第一天到您生成报告的日期之间的活动。

① **注:** 对于所有情况，在部署 Core 软件之前或者在 Core 上保护机器之前，没有可用的报告数据。

- 对于作业或故障报告，请从**目标 Core** 下拉菜单中选择您要为其生成报告的相应 Core。

默认选项包括所有可用的 Core。

- 从**受保护机器**下拉菜单中，选择您要为其生成报告的一台或多台机器。

默认情况下，该组信息包括所有机器的作业，其中包括每个受保护机器、复制的机器以及指定 Core 中仅限恢复点的机器。在报告参数中，您可以自定义报告。使用筛选器选择或排除一些机器。您也可以选择或排除与机器无关的作业，在此情况下报告仅显示 Core 作业的状态。

您可以选择：

选项	说明
Select all（全选）	此选项选择此 Core 上保护的所有受保护机器。
① 注: 您可以选择所有机器，然后清除一些选择，指定所有机器中的一部分机器。	
与机器无关	选择此选项可生成从 Core 角度包括作业的报告。创建或删除存储库、创建启动 CD 等作业类型与特定机器无关。如果将代理软件部署到尚未受到保护的机器，此作业类型也被视为与机器无关。这些作业未在所生成报告的“受保护机器”列中列出受保护机器。 相反，如果您将代理软件部署到已在 Core 上保护的机器，受保护机器的名称也将包括在报告中。它不被视为与机器无关。
受保护机器	此选项列出了此 Core 上保护的机器。您可以选择全部受保护机器或一部分受保护机器。
仅限恢复点	此选项列出受到了保护但在存储库中仍保存有恢复点的机器。
[源 Core]	如果您的 Core 是目标 Core，并且为源 Core 上保护的任何机器复制恢复点，则会出现该源 Core 的名称（全部为大写字母）。此选项列出了该源 Core 上保护的所有机器。您可以选择此目标 Core 中复制的所有机器，或者您可以选择这些机器中的一部分。
[自定义组]	如果您在此 Core 上创建了任何自定义组，每个自定义组的名称将显示为选项。此时会显示该自定义组中的每个对象。您可以选择该组中的所有对象或这些对象的子集。

- 如果要生成摘要报告，请跳至**步骤 12**。

- 对于作业、作业摘要或故障报告，请从**作业类型**下拉菜单中选择相应的作业类型。

默认情况下，该组信息包括所选受保护机器的所有作业。在报告参数中，您可以自定义报告。使用筛选器选择或排除“主作业”类别的每个作业以及“其他作业”类别的每个作业。或者您可以在定义作业参数时展开每个类别，然后只从您要显示在报告中的任一类别中选择作业类型。单击任何作业类型的复选框以选择或清除该类型。您可以选择任一类别的部分或全部作业。

您可以从以下**其他**作业类型中选择：

- 对于存储库报告，从“存储库”菜单中选择要包括在报告中的存储库。

默认选项包括所有可用的存储库。

- 单击**预览**按指定的条件生成报告。

如果未找到您选择的报告条件，仍会生成报告，但此报告包含空行。例如，如果没有错误，报告中“错误”列中的内容为空。

- 请执行以下步骤之一：

- 联机查看生成的报告。
- 通过更改以下条件动态更新报告，然后再次单击**预览**。

- 使用**报告**菜单选择导出格式（包括默认格式 PDF），然后单击  以导出报告。有关“报告”菜单的更多信息，请参阅[使用“报告”菜单](#)。
- 使用**报告**工具栏查看、处理和打印报告。有关“报告”工具栏的更多信息，请参阅[使用“报告”工具栏](#)。

按需生成受保护机器报告

您可以为任何受保护机器生成作业报告或失败报告。

要生成受保护机器的报告，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 在“受保护机器”菜单中，单击您想要为其查看报告的受保护机器。
将显示所选受保护机器的摘要页面。
- 3 在页面顶部受保护机器名称旁边的菜单选项中，单击“报告”旁边的向下箭头，然后选择报告类型。
 - 如果要为与此受保护机器相关的所有作业（包括失败的作业）生成报告，请单击**作业报告**，并开始指定您的报告条件。
 - 如果要仅生成与此受保护机器相关的失败作业列表，请单击**失败报告**，并开始指定您的报告条件。
- 4 对于作业或失败报告，请从**日期范围**下拉菜单中，选择一个日期范围。

如果您没有选择日期范围，将使用默认选项（过去 31 天）。您可以从下表选项中进行选择。

选项	说明
过去 24 小时	报告过去一天（相对于您生成报告的时间）的活动。
过去 7 天	报告最近一周（相对于您生成报告的时间）的活动。
过去 31 天	报告过去 31 天（相对于您生成报告的时间）的活动。
过去 90 天	报告过去 90 天（相对于您生成报告的时间）的活动。
过去 365 天	报告过去一年（相对于您生成报告的时间）的活动。
所有时间	此时间段跨越整个 Core 生命周期。
自定义	此时间段需要您进一步指定开始和结束日期。
当月至今	报告从当前日历月的第一天到您生成报告的日期之间的活动。
当年至今	报告从当前日历年的第一天到您生成报告的日期之间的活动。

① 注：在所有情况下，在部署 Core 软件之前或机器在 Core 上受保护之前，没有报告数据可用。

- 5 从**作业类型**下拉菜单中，选择相应的作业类型。
默认情况下，这组信息包括所选受保护机器的所有作业。在报告参数中，您可以自定义报告。使用筛选器以选择或排除“主作业”类别中的每个作业，以及“其他作业”类别中的每个作业。或者，您可以在定义作业参数时展开其中每个类别，然后从任一类别中仅选择要在报告中显示的作业类型。单击任意作业类型的复选框以选择或清除该类型。您可以从任一类别中选择部分或全部作业。
- 6 单击**预览**以使用指定的条件生成报告。
如果未找到您选择的报告条件，仍会生成报告，但此报告包含一个空行。例如，如果没有错误，“错误”列中的内容在报告中为空。
- 7 请执行以下步骤之一：
 - 在线查看生成的报告。
 - 通过更改任一条件来动态更新报告；然后再次单击**预览**。
 - 使用**报告菜单**以选择导出格式并导出报告。有关“报告”菜单的详细信息，请参阅[使用“报告”菜单](#)。
 - 使用**报告工具栏**以查看，操作或打印报告。有关“报告”工具栏的详细信息，请参阅[使用“报告”工具栏](#)。

从 Core Console 管理计划报告

您可以从 Core Console 计划任何可用的报告。计划报告会导致报告在未来反复生成。计划定义了是否要每天、每周或每月生成报告。

（可选）生成每个报告时，Rapid Recovery 可向一个或多个收件人发送电子邮件通知。电子邮件指定了报告类型、报告格式和日期范围，并将报告作为附件包含在内。

① 注: 在您可以通过电子邮件发送报告之前，您必须配置 Core 的 SMTP 服务器。有关详情，请参阅[配置电子邮件服务器](#)。

无论您是否选择发送电子邮件通知，您都可以在本地或 Core 服务器可以访问的网络位置保存生成的报告。

您必须指定电子邮件通知和发送，或者您必须指定一个位置来保存报告。您还可以同时选择这两个选项。

本部分包括以下主题：

相关链接

- [计划报告](#)
- [修改报告计划](#)
- [暂停、恢复或删除计划报告](#)

计划报告

您可以计划 Core Console 中提供的报告。然后，报告会按您定义的计划生成，直到您暂停或删除报告为止。

您必须指定电子邮件通知和发送，或者您必须指定一个位置来保存报告。您还可以同时选择这两个选项。

要计划报告，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 从图标栏中，单击 （更多），然后选择**报告**。
此时会显示**作业报告**页面。当前报告名称右侧会显示一个向下箭头。
- 3 单击报告名称右侧的箭头，并从下拉菜单中选择**计划报告**。
此时会显示**计划报告**页面。
- 4 要计划重复生成报告，请单击**添加**。
此时会显示**设置报告计划向导**。
- 5 在向导的**配置**页面中，输入要计划的报告的详细信息，然后单击**下一步**。下表介绍了配置选项。

表. 161: 计划报告配置选项

机器	可用报告
名称	键入您要分配给此特定计划的显示名称。 默认名称为“计划报告 1”。将名称限制为不超过 64 个字符。 请勿使用 禁止字符 或 禁止短语 。
报告格式	选择报告输出格式。如果您没有选择任何值，将使用默认格式 (pdf)。
报告类型	选择您要重复生成的报告类型。
标签	选择您要在计划报告上显示的标签。需要至少一个标签。 “自定义组”功能允许您对一个逻辑容器（您为其定义了一个标签）中的 Core 对象分组。 通过在“设置报告计划向导”中使用“标签”参数，您可以选择为其运行计划报告的自定义组。 如果不存在自定义标签，“标签”下拉菜单中的可用选项包括“全选”和“受保护机器”。如果显示自定义组，每个组将显示为一个选项。您可以选择或清除以下任意选项以在计划报告中包括或排除这些对象。
受保护机器	选择要包括在报告中的一个或多个受保护机器。

机器	可用报告
	此选项不可用于存储库报告。
作业类型	选择您想在报告中显示的作业类型。 默认情况下，这组信息包括所有机器的作业 - 指定 Core 中的每个受保护机器、复制机器和仅有恢复点的机器。在报告参数中，您可以自定义报告。使用筛选器选择或排除一些机器。您也可以选择或排除机器独立的作业（在此情况下，报告仅显示 Core 作业的状态）。 作业类型参数不可用于 Core 摘要和资源库已计划的报告类型。

6 在向导的**目标**页面中，选择要计划的报告的目标。您必须选择以下选项之一，也可以同时选择两者。如果满意，则单击**下一步**。

- 在**发送到电子邮件地址**字段中，输入一个或多个有效的电子邮件地址，以便在计划报告生成时通过电子邮件消息通知用户。

① | 注: 如果您未指定电子邮件通知和发送，则您必须指定存储位置。

- 选择**另存为文件**以将生成的报告文件保存到指定的位置，并在**位置类型**下拉菜单中，选择一个本地、网络或云存储选项。然后如下表所述，在**位置**字段中指定其他位置信息。

表. 162: 计划报告的位置选项

位置类型	位置类型说明	位置
本地	选择位置类型“本地”以在 Core 可访问的本地路径中保存生成的报告。	在“位置”字段中指定路径。 键入 Core 可本地访问的位置。 例如，要将报告存储在 D 驱动器上的 Reports 文件夹中，请输入 D:\Reports\。
网络	选择位置类型“网络”以在 Core 可访问的网络路径中保存生成的报告。在“位置”字段中指定路径。	在“位置”字段中指定路径。 键入 Core 可从网络访问的位置。使用格式 \\servername\sharename。 例如，要将报告存储在数据服务器上名为 Reports 的共享文件夹中，请输入 \\Data\Reports\。 在“用户名”和“密码”字段中指定网络凭据。
云	选择位置类型“云”以在 Core 中配置的云存储帐户中保存生成的报告。 必须首先定义存储帐户，然后才能执行此步骤。有关设置用于 Core 的云存储帐户的信息，请参阅管理云帐户。	从“帐户”字段中，选择用于存储生成的报告的相应云存储帐户。 从“容器”字段中，指定存储帐户中相应的容器。 从“文件夹名称”字段中，指定用于存储未来生成的报告的文件夹。

7 对“目标”选项感到满意后，请单击**下一步**。

8 在向导的**计划**页面上，从**发送数据**菜单中，选择一个选项以确定您指定的报告的生成频率。您可以每天、每周或每月生成报告。每个选项都有自己的参数，如下表所述。

表. 163: 计划报告的生成频率选项

频率	频率详细信息	频率参数
每天	在指定时间每天生成并保存或发送一次指定的报告。	要更改生成报告的默认时间，请在时间文本字段中键入新的值，或使用控件更改小时、分钟以及 AM 或 PM。

频率	频率详细信息	频率参数
	此操作的默认时间为 0:00 AM（基于 Core 服务器上的时间）。	
每周	在指定周中日的指定时间每周生成并保存或发送一次指定的报告。 此操作的默认时间为周日 0:00 AM（基于 Core 服务器上的时间）。	要更改生成报告的默认周中日，请从“星期几”菜单中，选择一周中的某一天。 要更改生成报告的默认时间，请在时间文本字段中键入新的值，或使用控件更改小时、分钟以及 AM 或 PM。
每月	在指定的日期和时间每月生成并保存或发送一次指定的报告。 此操作的默认日期为每月第一天的 0:00 AM（基于 Core 服务器上的时间）。	要更改生成报告的默认日期，请从“一月中的一天”菜单中，选择一个日期。 要更改生成报告的默认时间，请在时间文本字段中键入新的值，或使用控件更改小时、分钟以及 AM 或 PM。

9 （可选）在向导的**计划**页面上，如果您想要在恢复暂停的报告之前阻止生成计划报告，请选择**初始时暂停报告**。
如果想要按计划生成此报告，请清除此选项。

10 对于计划感到满意后，请单击**完成**以退出向导，然后保存您的工作。
新报告计划将出现在“摘要报告”摘要表中。

修改报告计划

计划报告后，您可以修改其参数或详细信息。您可以编辑报告配置信息（报告名称、输出格式、报告类型、包括的存储库）。您也可以更改电子邮件通知选项以及保存所生成报告的目的地。最后，您也可以更改报告的计划。

完成此过程中的步骤以修改计划报告的参数。

- 1 导航至 Rapid Recovery Core Console。
- 2 从图标栏中，单击 （更多），然后选择**报告**。
此时会显示**作业报告**页面。在当前报告名称的右侧会显示一个向下箭头。
- 3 单击报告名称右侧的箭头，并从下拉菜单中选择**计划报告**。
此时会显示**计划报告**页面。
- 4 在“计划报告”摘要表中，从您想要修改的报告所在的行，单击 “设置”图标，然后选择**编辑**。
此时会出现**设置报告计划向导**。
- 5 浏览此向导的各个页面，更改必要的参数。有关此向导中的任何参数的信息，请参阅[计划报告](#)主题。
- 6 在向导的**计划**页面上，单击**完成**以关闭向导并保存您所做的更改。
向导关闭，报告计划已修改。

暂停、恢复或删除计划报告

计划报告后，报告会按定义的计划生成。如果您想暂停生成计划报告，您可以暂停计划。

如果计划报告已暂停，且您希望恢复生成报告，您可以按照此过程所述恢复报告。

如果您当前正在生成计划报告，并且不再需要生成该报告，可将其删除。

要确定计划报告是否已暂停，请检查计划报告摘要表中的状态列。绿色球体表示活动计划报告；黄色球体表示已暂停的计划；红色球体表示错误。

要暂停、恢复或删除报告的计划，请完成以下过程中的步骤。

- 1 导航至 Rapid Recovery Core Console。
- 2 从图标栏中，单击（更多），然后选择**报告**。
此时会显示**作业报告**页面。当前报告名称右侧会显示一个向下箭头。
- 3 单击报告名称右侧的箭头，并从下拉菜单中选择**计划报告**。
此时会显示**计划报告**页面。
- 4 在“计划报告”摘要表中，使用彩色指示符查看所有计划报告的状态。
- 5 对于您想要暂停或恢复的每个报告，请选中第一列中的复选框。
- 6 从摘要表上方的“计划报告”选项中，执行以下操作之一：
 - 要暂停生成所选报告，请单击**暂停**。
 - 要恢复生成已暂停的计划报告，请单击**恢复**。
 - 要删除现有计划报告的所选计划，请单击**删除**。删除计划报告仅可阻止在未来生成报告。如果已保存以前的计划报告，它们不会被删除。

使用“报告”菜单

查看报告时，“报告”菜单显示在页面顶部。此菜单包括报告标题，它同时也是一个下拉菜单，可让您查看可用的报告类型。此菜单下面有一个或多个筛选器，帮助您定义您的报告条件。

可用的特定筛选器取决于报告类型。有关每种报告类型适用的参数的信息，请参阅相关主题了解该报告类型。

在“报告”菜单的右侧，会显示某些控件。下表中介绍的这些控件可帮助您生成和导出报告。

表. 164: 报告菜单控件

UI 元素	说明
“预览”按钮	单击“预览”按钮以基于筛选器中所选的报告类型和报告参数生成报告。
“导出格式”下拉菜单	“导出”下拉菜单允许您选择报告输出格式。如果您没有选择值，则使用默认格式 (pdf)。
“下载”按钮/图标	“下载”按钮将以“导出”菜单中选定的格式类型生成报告。

报告现在包括测量单位，可更轻松地确定是否以 GB、TB 或秒表示列。

如果不满意所生成或导出的报告的外观，您可以更改报告中使用的字体。有关更多信息，请参阅[管理报告设置](#)。

生成报告后，您可以使用报告工具栏。

相关链接

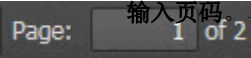
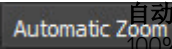
- [了解“作业”报告](#)
- [了解失败报告](#)
- [了解摘要报告](#)
- [了解 Central Management Console Core 报告](#)

使用“报告”工具栏

从“报告”菜单生成报告后，报告显示在“报告”工具栏下方。该工具栏可帮助您操作报告输出（包括保存和打印报告）。

在工具栏左侧，提供了一个“切换”边栏选项。此工具可扩大或收缩边栏，允许用户访问更多的显示选项。在工具栏右侧，“工具”选项可展开一个下拉菜单，其中提供了报告导航控件。“报告”工具栏的元素如下表所述。

表. 165: 报告工具栏图标

图标	说明
	“切换”边栏。 所有报告页面显示为缩略图。边栏中的其他选项不受支持。
	边栏：显示缩略图。 这是生成的报告的所有页面的默认视图。
	边栏：显示文档概述。 不支持此功能。
	边栏：显示附件。 报告没有附件。不支持此功能。
	查找。 允许您在生成的报告中搜索文本。包含了选项以高亮度显示与您输入的条件匹配的所有文本，以及匹配或忽略大小写。
	上一页。 移动报告视图至上一页。
	下一页。 在报告视图中进入下一页。
	输入页码。 单击页码文本字段，输入有效的页码，然后按 Enter 键以在报告视图中进入该页。
	缩小。 可让您缩小生成的报告的视图。每次连续单击都会令视图进一步缩小，最小为 25%。
	放大。 可让您放大生成的报告的视图。每次连续单击都会令视图进一步放大，最大为 1000%。
	自动缩放。 使您能够控制生成的报告的缩放视图，包括按实际大小、适合页面、全宽或按百分比（包括 50%、75%、100%、125%、150%、200%、300% 或 400%）进行查看。
	打开文件。 可让您浏览文件系统以查找和打开已保存的报告。
	打印。 可让您打印生成的报告。
	工具。 当您单击此图标时，“工具”下拉菜单可展开或收起。“工具”选项如下所述。
	工具：转至第一页。 将您导航到生成的报告的第一页。
	工具：转至最后一页。 将您导航到生成的报告的最后一页。

图标	说明
	工具： 顺时针旋转 。此选项可顺时针方向旋转生成的报告的画布。
	工具： 逆时针旋转 。此选项可逆时针方向旋转生成的报告的画布。
	工具： 手动工具 。在您选择此工具时，它可让您通过单击和跨屏幕拖动来移动报告。
	工具： 文档属性 。提供有关生成的报告的文档属性的信息。单击 关闭 以关闭此窗口。

有关生成报告的信息，请参阅[从 Core Console 生成报告](#)。有关为 Central Management Console 中的多个 Core 生成报告，请参阅[从 Central Management Console 生成报告](#)。

了解“作业”报告

作业报告可用于 Rapid Recovery Core 和 Core 上的受保护机器。您通过此报告可以查看所选 Core 或受保护机器执行的作业的状态。报告中显示的没有数据的数据行或列表示测试参数为空。例如，如果显示的某一列（例如“错误”）没有信息，则表明所选记录未发生错误。如果报告生成空行，则所选记录的作业反映了与机器无关的活动。

有关如何从 Core 生成“作业”报告的信息，请参阅[按需生成 Core 报告](#)。有关如何为受保护机器生成“作业”报告的信息，请参阅[按需生成受保护机器报告](#)。

生成作业报告时，报告详细信息包括以下内容：

- 报告的选择条件
- 为您指定的日期范围内的每个作业显示了一行条目的摘要表。除了列出相应的 Core、受保护机器和作业类型外，每行还包括：
 - 作业的摘要
 - 作业状态
 - 与作业相关的任何错误
 - 作业的开始和结束日期
 - 作业持续时间（秒）
 - 总工作量（MB）

如果信息与特定类别不相关，报告中的该单元格将不显示任何信息。例如，如果指定的受保护机器的 Core 没有错误，则报告中对应该行的错误列为空。

了解作业摘要报告

作业摘要报告仅在从 Core 视角报告时可用；此报告不可用于受保护机器的报告。此报告具有单独摘要，显示与 Core 上执行的所有作业相关的摘要信息，其中包括失败、通过和取消的作业数量。它显示的详细信息多于作业报告，因为它将每项作业指定为单独行。

有关如何生成“作业摘要”报告的信息，请参阅[从 Core Console 生成报告](#)。

此报告类型的报告参数包括：

- Date range（日期范围）
- 受保护机器
- 作业类型

在生成“工作摘要”报告时，报告详细信息包括报告的选择条件，以及关于受保护机器、卷和作业类型信息。

Core 信息

“摘要”报告的 Core 部分包含有关所报告的 Rapid Recovery Core 的数据。此信息包括：

- Rapid Recovery Core 中受保护机器的数量。
- 带有失败作业的机器数量

受保护机器摘要

“摘要”报告的“受保护机器”部分包含所选 Rapid Recovery Core 保护的所有机器的数据，以及这些机器的卷。

图表显示了每台机器上每个作业类型的行，其中包括成功作业（任何类型）的比率，通过、失败和已取消作业的数量。（已取消的作业未纳入到这些统计信息之中。）

了解失败报告

失败报告是作业报告的子集，可用于 Rapid Recovery Core 和 Core 上的受保护机器。失败报告仅包含作业报告中列出的已取消作业和失败作业，并将其编译成可以打印和导出的单个报告。如果报告生成后显示一个空行，则您的报告条件中指定的日期范围内没有发生任何错误。

① | 注：目标 Core 和受保护机器参数的结果只会针对 Core 级别报告显示。

有关如何从 Core 生成“作业”报告的信息，请参阅[按需生成 Core 报告](#)。有关如何为受保护机器生成“作业”报告的信息，请参阅[按需生成受保护机器报告](#)。

在您生成失败报告时，将显示一个摘要表，其中为您指定的日期范围内的每个作业显示了一行条目。除了列出相应的 Core、受保护机器和作业类型外，每行还包括：

- 作业的摘要
- 作业状态
- 与作业相关的任何错误
- 作业的开始和结束日期
- 作业持续时间（秒）
- 总工作量 (MB)

了解摘要报告

“摘要”报告可用于一个或多个 Core。不可从受保护机器的报告获取此报告。“摘要”报告包含有关所选 Rapid Recovery Core 上的存储库以及该 Core 所保护的机器的信息。这些信息在一份报告中显示为两个摘要。

有关如何生成“摘要”报告的信息，请参阅[从 Core Console 生成报告](#)。

此报告类型的报告参数包括：

- Date range（日期范围）
- 受保护机器

在生成“摘要”报告时，报告详细信息包括报告的选择条件，以及关于存储库和受保护机器的信息。

Core 信息

“摘要”报告的 Core 部分包含有关所报告的 Rapid Recovery Core 的数据。此信息包括：

- 许可证密钥（标识符）
- Rapid Recovery Core 软件的当前版本

存储库摘要

“摘要报告”的“存储库”部分包含位于所选 Rapid Recovery Core 上的存储库的数据。此信息包括：

- Rapid Recovery Core 中的存储库数量
- Core 上的存储库的摘要。

受保护机器摘要

“摘要”报告的“受保护机器”部分包含所选 Rapid Recovery Core 保护的所有机器的数据。这包括一个图表和一个摘要表。

图表显示了受保护机器的成功作业（任何类型）与失败作业之比。（已取消的作业未纳入到这些统计信息之中。）

X 或水平轴显示受保护机器的数量。Y 或垂直轴显示成功的分层。具体而言，Y 轴按受保护机器显示了有多少个机器具有以下特征：

- 未执行作业
- 小于 50% 成功率
- 50% 或更高成功率
- 100% 成功率

在图表下显示了受保护机器的相关信息。此信息包括：

- 受保护机器的数量
- 带有失败作业的受保护机器的数量
- 按受保护机器显示信息的摘要表，其中显示：
 - 受保护机器的名称
 - 机器保护的卷
 - 受保护的空間大小，以 GB 为单位（总空间和当前空间）
 - 每天更改率（平均和中值）
 - 作业统计（成功、已完成、失败、已取消）
 - 如果已应用加密
- Core 版本

了解存储库报告

“存储库”报告包含有关所选 Rapid Recovery Core 上的存储库以及该 Core 所保护的机器的信息。这些信息在一份报告中显示为两个摘要。

有关如何从 Core 生成“存储库”报告的信息，请参阅[按需生成 Core 报告](#)。

此报告类型的报告参数仅包括存储库。

生成存储库报告时，每个存储库的报告详情包括 Core 上存储库的摘要列表。

Central Management Console

Rapid Recovery Central Management Console 是一个可选组件，面向具有两个或更多 Rapid Recovery Core 的环境。此组件是一个 Web 门户，提供一个集中界面供您分组、管理多个 Core 和为它们生成报告。

Central Management Console 的操作系统要求与 Rapid Recovery Core 的要求相同。这些组件既可安装在同一机器上也可安装在不同的机器上，具体视您的需求而定。

安装后，您必须通过单独添加您想要管理的 Core 或者将它们添加为 Core 组的一部分来配置 Central Management Console。

注: 您必须以本地管理员权限运行安装程序。

Windows 8、8.1 和 10 以及 Windows Server 2012 和 2012 R2 操作系统必须在服务器上安装 ASP.NET 4.5 功能，才能正确加载 GUI。作为 Rapid Recovery 安装程序的一部分，此配置包括在内。

有关安装此组件的更多信息，请参阅《Rapid Recovery 安装和升级指南》中的主题“安装 Dell Data Protection | Rapid Recovery Central Management Console”。

有关配置此组件的更多信息，请参阅《Dell Data Protection | Rapid Recovery 用户指南》中的主题 Dell Data Protection | Rapid Recovery。

有关了解此组件的用户界面的更多信息，请参阅《Dell Data Protection | Rapid Recovery 用户指南》中的主题 Dell Data Protection | Rapid Recovery。

了解 Rapid Recovery Central Management Console

打开 Central Management Console 时，将在“控制台”视图中显示信息。此时会显示**欢迎**页面，您可以看到以下元素：

表. 166: Rapid Recovery Central Management Console 中的用户界面元素

UI 元素	说明
品牌区	对于典型环境，Central Management Console 左上方的品牌名称显示完整的产品名称 Dell Data Protection Rapid Recovery。单击品牌区域上的任意位置会将 Web 浏览器用户定向到 Dell 支持网站上的产品说明文件。
左侧导航区	左侧导航区显示在品牌区下方，在用户界面的左侧。导航区域的功能会根据从 Central Management Console 右上角所选的模式而有所不同 控制台模式。在导航区域中，当处于“控制台”模式下时，单击任何 Core 或 Core 组会在 Rapid Recovery Core Console 中打开所选的 Core 或 Core 组。 报告模式。在导航区域中，当处于“报告”模式下时，选择 Core 或 Core 组将确定生成报告时显示的信息。 管理模式。在导航区域中，当处于在“管理”模式下时，可以浏览 Core 和 Core 组的设置。也可以在“管理”模式下添加和删除 Core 和 Core 组。单击箭头可展开和折叠菜单。包含的内容是以下层级结构级别：组织、Core 组和 Core。如果您单击向左箭头，导航区域将会折叠。要展导航区域，请单击向右箭头。
“链接”菜单	联系 Dell 支持部门。 在新的浏览器窗口中链接到 Dell 支持网站，可访问在线聊天、视频教程、Rapid Recovery 知识库文章、常见问题等。
“链接”菜单	说明文件。 在新的浏览器窗口中链接到 Dell 支持网站，可访问在线聊天、视频教程、Rapid Recovery 知识库文章、常见问题等。
“链接”菜单	版本。 列出 Central Management Console 的当前版本。单击此链接将打开“关于”对话框。
“链接”菜单	模式选择器。 在链接菜单的右上角，当前已登录 Windows 的用户的名称会出现在下拉菜单中。

UI 元素

说明

从此菜单中，您可以更改 Central Management Console 的视图。您可以从以下视图中选择：

控制台。这是默认模式，在该模式下，可以从一个位置查看您环境中的 Core 和 Core 组。

报告。在此模式下，可以从在此控制台中配置的 Core 生成、查看和导出报告。

管理。从“管理”模式中，您可以从 Central Management Console 单独或分组移除 Core 或添加其他 Core。

语言。在支持本地化的版本中，列出了“语言”选项。选择此选项会打开“切换语言”对话框，从中可以为 Central Management Console 选择显示语言。

清除帐户高速缓存。选择此选项可清除已登录用户帐户的现有信息。

您可以通过从模式选择器（页面右上方的下拉菜单）中选中某个选项来更改 Central Management Console 的视图。例如：

- 要管理已配置的 Core 或 Core 组，请使用“控制台”视图。
- 要配置 Central Management Console，请切换到“管理”视图。
- 要生成报告，请切换到“报告”视图。

可以查看和管理的 Core 会出现在左侧导航菜单中。您可以配置单个 Core，或按组组织它们。可以使用 Windows 用户名或组限制对特定组中 Core 的访问权限。

配置 Rapid Recovery Central Management Console

配置 Rapid Recovery Central Management Console 涉及添加 Core 和 Core 组、建立它们的设置以及指定组的访问权限设置（如果需要）。

完成配置后，可从一个中心位置管理设置和所有 Core。

要配置 Central Management Console，可以执行下面的“相关链接”中列出的所有任务。

相关链接

- [将 Core 添加至 Central Management Console](#)
- [在 Central Management Console 中配置 Core 设置](#)
- [将 Core 组添加至 Central Management Console](#)
- [配置 Core 组设置](#)
- [配置 Core 组访问权限](#)

将 Core 添加至 Central Management Console

如果要将 Core 添加到 Core 组，必须先创建该组。有关详情，请参阅[将 Core 组添加至 Central Management Console](#)。您也可以在以后编辑 Core 的详细信息以指定组。

将一个或多个 Core 添加到 Central Management Console 以对其进行管理，或从单个接口生成报告。

要将 Core 添加到 Central Management Console，请完成以下过程中的步骤。

- 1 从 Rapid Recovery Central Management Console 中，单击模式选择器下拉列表，然后选择**管理**。
页面将刷新，显示“添加 Core”、“添加组”和“删除”图标。
- 2 从左侧导航菜单的顶部，单击**添加 Core**。
此时将显示**添加 Core** 页面。
- 3 根据下表中的说明输入连接至 Core 所需的信息。

表. 167: 添加 Core 详细信息

文本框	说明
父组	(可选) 如果您希望 Core 加入现有 Core 组, 请从相应的组织中选择父组。
显示名称	输入 Core 的显示名称。 显示名称必须限制为不超过 150 个字符。最佳做法是让此名称不超过 33 个字符。 请勿使用禁止的字符或禁止的短语。有关禁止的字符或禁止的短语的更多信息, 请参阅 <i>Dell Data Protection Rapid Recovery User Guide</i> (Dell Data Protection Rapid Recovery 用户指南)。
主机名	输入用于访问 Core 的 IP 地址。 如果您要添加的 Core 是当前服务器, 则可以使用 localhost。
端口	输入用于建立连接的端口号。默认值为 8006。
用户名	为新添加的 Core 输入用于访问 Core 服务的用户名。
密码	为新添加的 Core 输入用于访问 Core 服务的密码。

- 单击**测试连接**以测试配置。
如果测试成功, 将显示成功消息。单击**确定**以关闭该确认消息。
- 单击**保存**。
将会保存您所做的更改, 并且现在已将 Core 添加至父组。

相关链接

将 Core 组添加至 [Central Management Console](#)

在 Central Management Console 中配置 Core 设置

要在 Central Management Console 中配置 Core 设置, 请完成以下过程中的步骤。

- 从 Rapid Recovery Central Management Console 中, 单击模式选择器下拉列表, 然后选择**管理**。
页面将刷新, 显示“添加 Core”、“添加组”和“删除”图标。
- 从左侧导航菜单中, 单击相应的 Core 的名称。
此时将显示所选 Core 的**设置**页面。
- 在“设置”选项卡中, 根据下表中的说明修改 Core 信息。

表. 168: Core 设置

文本框	说明
父组	为要添加的新 Core 设置选择 Core 父组。
显示名称	输入 Core 的显示名称。
用户名	输入 Core 的用户名。
密码	输入 Core 的密码。
管理门户应如何连接到 [Core 名称]?	选择指定该连接的选项。您可以选择： - 使用 [Core 名称] 的最后已知 IP 地址 (xxx.xxx.xxx.xxx) 或 - 使用主机名或 IP 地址 [主机名或 IP 地址]。 如果选择通过使用主机名或 IP 地址指定连接, 则必须在主机名或 IP 地址字段中输入相应的信息。

文本框	说明
[Core 名称] 正在侦听哪个端口？	选择任一端口选项。您可以选择： - 默认端口 (8006) 或 - 自定义端口 [端口] 如果选择指定该端口，请在“自定义端口”字段中输入端口号。
4 单击 测试连接 。	如果测试成功，将显示一条消息，指示连接成功。
5 单击 保存 。	

将 Core 组添加至 Central Management Console

要将 Core 组添加至 Rapid Recovery Central Management Console，请完成以下过程中的步骤。

- 1 从 Rapid Recovery Central Management Console 中，单击模式选择器下拉列表，然后选择**管理**。页面将刷新，显示“添加 Core”、“添加 Core 组”和“删除”图标。
- 2 从左侧导航菜单的顶部，单击**添加组**。此时将显示**添加组**页面。
- 3 按下表所述选择父组和显示名称。

表. 169: 添加 Core 组

文本框	说明
父组	为要添加的新 Core 组选择 Core 父组。
显示名称	输入 Core 组的显示名称。 显示名称必须限制为不超过 150 个字符。最佳做法是让此名称不超过 33 个字符。 请勿使用禁止的字符或禁止的短语。有关禁止的字符或禁止的短语的更多信息，请参阅 <i>Dell Data Protection Rapid Recovery User Guide</i>。（Dell Data Protection Rapid Recovery 用户指南）。
4 单击 保存 。	

相关链接

[将 Core 组添加至 Central Management Console](#)

配置 Core 组设置

配置 Core 组设置或访问之前，必须先创建该组。有关更多信息，请参阅[将 Core 组添加至 Central Management Console](#)。

要配置 Core 组设置，请完成以下过程中的步骤。

- 1 从 Rapid Recovery Central Management Console 中，单击模式选择器下拉列表，然后选择**管理**。页面将刷新，显示“添加 Core”、“添加 Core 组”和“删除”图标。
- 2 从左侧导航菜单中，单击您要配置的 Core 组的名称。此时将显示所选 Core 组的“设置”页面。
- 3 根据下表中的说明修改 Core 组的信息。

表. 170: Core 组设置

文本框	说明
父组	为要添加的新 Core 组设置选择 Core 父组。
显示名称	输入 Core 组的显示名称。 显示名称必须限制为不超过 150 个字符。最佳做法是让此名称不超过 33 个字符。 请勿使用禁止的字符或禁止的短语。有关禁止的字符或禁止的短语的更多信息，请参阅《Dell Data Protection Rapid Recovery 用户指南》。

4 单击**保存**。

配置 Core 组访问权限

配置 Core 组设置或访问之前，必须先创建该组。有关更多信息，请参阅[将 Core 组添加至 Central Management Console](#)。

要在 Central Management Console 中添加或查看 Core，当前用户帐户必须是 Active Directory 域管理员组的成员。或者，您也可以使用下面的过程提供对单个用户或组的访问权限。

要配置 Core 组访问权限，请完成以下过程中的步骤。

- 从 Rapid Recovery Central Management Console 中，单击模式选择器下拉列表，然后选择**管理**。
页面将刷新，显示“添加 Core”、“添加组”和“删除”图标。
- 从左侧导航菜单中，单击您要配置的 Core 组的名称。
此时将显示所选 Core 组的**设置**页面。
- 单击**访问**选项卡。
此时将显示 Core 组的访问权限设置。
- 单击**添加**。
此时会显示**允许访问**对话框。您可以提供对个人或组的访问权限。
- 请执行以下步骤之一：
 - 如果提供对个人的访问权限，则在**名称**文本字段中，输入个人的姓名，然后单击**用户**。此为默认选项。
例如，键入 administrator（或者如果机器在域中，则键入 [域名]\Administrator）。
 - 如果要提供对组的访问权限，则在**名称**文本字段中，输入组的名称，然后单击**组**。
例如，键入 AdminGroup（或者如果机器在域中，则键入 [域名]\AdminGroup）。
- 单击**检查名称**以验证是否所指定的用户名或组名是否可访问。
如果输入的名称有效，将显示“帐户已验证”讯息。
- 输入并验证名称后，请单击**保存**。
允许访问对话框将关闭并保存您所做的更改。访问名称将出现在 Core 组的“访问”选项卡中。

了解 Central Management Console Core 报告

Rapid Recovery 可为多个 Rapid Recovery Core 生成和查看作业报告、故障报告和摘要信息。Core 的详情列在摘要表格中，使用与以下章节中所述相同的目录。[了解“作业”报告](#)、[了解失败报告](#)和 [了解摘要报告](#)。

有关如何为多个 Core 生成报告的信息，请参阅。[从 Central Management Console 生成报告](#)。

从 Central Management Console 生成报告

要从 Central Management Console 为多个 Rapid Recovery Core 生成报告，请完成以下过程。

- 1 从 Rapid Recovery Central Management Console 中，单击右上角的模式选择器下拉菜单，然后选择**报告**。
此时会显示报告选择页面。默认选择 CoreJobReport。在报告名称右侧，会显示一个向下箭头，您可以从中选择其他报告类型。
- 2 在左侧导航菜单中，选择您要包含到报告中的单个 Rapid Recovery Core 或 Core 组的任意组合。
- 3 从报告类型下拉菜单中，选择您想要生成的报告类型。您可以选择以下选项之一：
 - 作业报告
 - 错误报告
 - 摘要报告
 - 作业摘要报告

有关这些报告类型的更多信息，请参阅 [关于 Rapid Recovery 报告](#)。

- 4 请从日期范围下拉菜单中，选择一个日期范围。
您可以从下表选项中进行选择。

选项	说明
天	报告过去一天（相对于您生成报告的时间）的活动。
周	报告最近一周（相对于您生成报告的时间）的活动。
月	报告过去 31 天（相对于您生成报告的时间）的活动。
年份	报告过去一年（相对于您生成报告的时间）的活动。
所有时间	此时间段跨越整个 Core 生命周期。
自定义	此时间段需要您进一步指定开始和结束日期。

-  **注:** 在所有情况下，在部署 Core 软件之前或机器在 Core 上受保护之前，没有报告数据可用。
- 5 请执行以下步骤之一：
 - 单击**预览**以在线生成并查看生成的报告。
 - 通过更改报告条件来动态更新报告；然后再次单击**预览**。
 - 选择导出格式（包括默认格式 XLSX），然后单击**下载**。
 - 使用**报告工具栏**以查看，操作或打印报告。有关“报告”工具栏的更多信息，请参阅 [使用“报告”工具栏](#)。

了解 Rapid Recovery Command Line Management 实用程序

Dell Data Protection | Rapid Recovery 包含多个软件组件。与本主题相关的关键组件包括以下组件：

- Rapid Recovery Core 可管理受保护机器的验证、用于备份和复制目的的数据传输计划、导出至虚拟机、报告以及裸机还原 (BMR) 至类似或不同的硬件。
- Rapid Recovery Agent 负责卷快照及将数据快速传输到 Core 管理的存储库。
- Rapid Recovery Command Line Management 实用程序 cmdutil.exe 提供了第三方访问以管理系统功能。此工具允许对 Rapid Recovery Core 管理功能编写脚本。

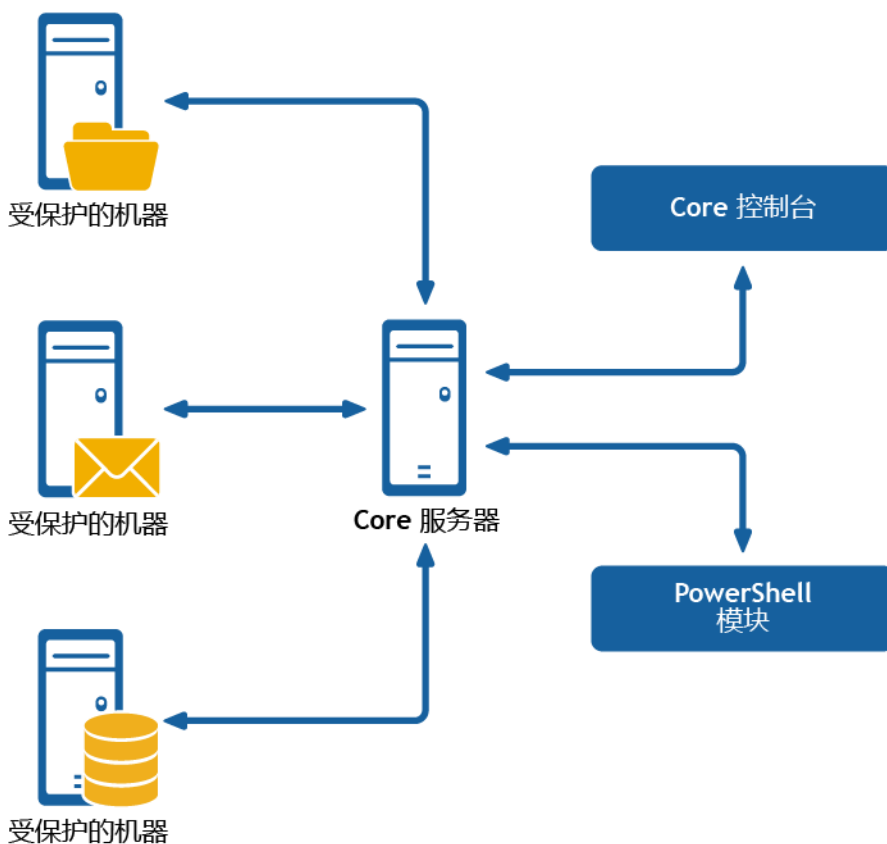


图 13: Rapid Recovery Command Line Management 提供了命令行功能

Rapid Recovery Command Line Management 是一款 Windows 命令行实用程序，用户可以通过该实用程序与 Rapid Recovery Core 服务器交互。它提供了 Rapid Recovery Core Console 图形用户界面所提供的部分功能。例如，Rapid Recovery Command Line Management 实用程序可以安装恢复点或强制创建快照。

Rapid Recovery Command Line Management 实用程序将嵌入到 Rapid Recovery Core 的每个安装中。要打开默认安装的 Command Line Management 实用程序，请导航至路径 `C:\Program Files\AppRecovery\Core\CoreService\`，然后双击 `cmdutil.exe` 文件。

在“命令行”模式中，操作标志可以通过选择命令选项和限定符传递到 Rapid Recovery Command Line Management 实用程序以执行有限的管理功能。

主题：

- [命令](#)
- [本地化](#)

命令

本节介绍 Rapid Recovery Command Line Management 实用程序可用的命令和选项。以下命令可供使用：

- [存档](#)
- [CancelActiveJobs](#)
- [CheckRepository](#)
- [CreateArchiveRepository](#)
- [CreateBootCD](#)
- [CreateRepository](#)
- [DeleteRepository](#)
- [Dismount](#)
- [DismountArchiveRepository](#)
- [EditEsxServer](#)
- [Force](#)
- [ForceAttach](#)
- [ForceChecksum](#)
- [ForceLogTruncation](#)
- [ForceMount](#)
- [ForceReplication](#)
- [ForceRollup](#)
- [ForceVirtualStandby](#)
- [帮助](#)
- [List](#)
- [安装](#)
- [MountArchiveRepository](#)
- [NewCloudAccount](#)
- [OpenDvmRepository](#)
- [Pause](#)
- [Protect](#)
- [ProtectCluster](#)
- [ProtectEsxServer](#)
- [RemoveAgent](#)
- [RemoveArchiveRepository](#)
- [RemovePoints](#)
- [RemoveScheduledArchive](#)
- [RemoveVirtualStandby](#)
- [Replicate](#)
- [复制](#)

- [RestoreAgent](#)
- [RestoreArchive](#)
- [RestoreUrc](#)
- [Resume](#)
- [SeedDrive](#)
- [StartExport](#)
- [UpdateRepository](#)
- [版本](#)
- [VirtualStandby](#)

存档

企业通常使用长期存储来存档合规和非合规数据。Rapid Recovery 中的存档功能可延长合规和非合规数据的保留期限。通过指定 `-path` 参数和凭据，管理员可以在本地存储位置或网络位置保存存档。

使用

此命令的使用如下：

```
/archive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -path [location] -startdate [time string] -enddate [time string] -archiveusername [name] -archivepassword [password] -comment [text]
```

命令选项

下表介绍 `archive` 命令可用的选项：

表. 171: 存档命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	存档 Core 上所有受保护机器的所有恢复点。
-protectedserver	要存档恢复点的受保护机器。您可以指定以双引号括起并用空格分隔的多个机器名称。
-path	存档数据应放置的位置；例如：d:\work\archive 或网络路径 \\servername\sharename。
-startdate	按创建日期选择恢复点的开始日期。值必须用双引号括起，例如 "04/30/2012 02:55 PM"。
-enddate	可选。按创建日期选择恢复点的结束日期。值必须用双引号括起，例如： "05/31/2012 11:00 AM"。默认情况下，将使用当前时间系统。

选项	说明
- archiveusername	可选。远程机器的用户名。仅网络路径需要。
- archivepassword	可选。远程机器的密码。仅网络路径需要。
-comment	可选。注释文本必须用双引号括起，例如：-comment “comment goes here...”。

示例：

存档 Core 上所有机器中创建日期从 04/30/2012 02:55 PM 起的所有恢复点：

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path d:\work\archive -startdate "04/30/2012 02:55 PM" -all
```

存档属于两台受保护机器的日期范围内的恢复点：

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver "10.20.30.40" "20.20.10.1" -path d:\work\archive -startdate "04/30/2012 02:55 PM" -enddate "05/31/2012 11:00 AM"
```

CancelActiveJobs

使用 cancelactivejobs 命令以取消执行特定类型的所有正在执行的作业，例如传输或复制。

使用

此命令的使用如下：

```
/cancelactivejobs -core [host name] -user [user name] -password [password] -jobtype [job type filter]
```

命令选项

下表介绍 cancelactivejobs 命令可用的选项：

表. 172: CancelActiveJobs 命令选项

选项	说明
-?	显示有关命令的帮助。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	确定应取消其作业的受保护机器。

选项	说明
-all	选择并取消所有受保护服务器中指定类型的事件。
-jobtype	可选。指定作业类型筛选器。可用的值包括： • 'transfer'（数据传输） • 'repository'（存储库维护） • 'replication'（本地和远程复制） • 'backup'（备份和还原） • 'bootcdbuilder'（创建启动 CD） • 'diagnostics'（上传日志） • 'exchange'（Exchange Server 文件检查） • 'export'（恢复点导出） • 'pushinstall'（部署代理） • 'restore'（恢复点还原） • 'rollup'（恢复点汇总） • 'sqlattach'（代理可附加性检查） • 'mount'（安装存储库） 默认情况下，将取消指定类型的所有作业。

示例：

取消 Core 10.10.10.10 上的所有传输作业：

```
>cmdutil /cancelactivejobs -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -
jobtype transfer
```

CheckRepository

您可以使用 CheckRepository 命令验证在 AppAssure Core 或 Rapid Recovery Core 中创建的现有 DVM 存储库的完整性。

使用

此命令的使用如下：

```
/checkrepository -repository [repository name] | -all [check all repositories] -core [host
name] -user [user name] -password [password] name] -force
```

命令选项

下表介绍 CheckRepository 命令可用的选项：

表. 173: CheckRepository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	可选。此选项会检查与 Core 关联的所有 DVM 存储库。
-repository	DVM 存储库的名称。
-force	可选。此选项执行检查时不需要您的确认。

示例：

开始检查 DVM 存储库：

```
>cmdutil /checkrepository -repository "Repository1" -core 10.10.10.10 -user administrator -password 23WE@#$sdd
```

CreateArchiveRepository

当您创建存档存储库时，您就为计划存档的内容创建了一个目标。此功能可让您安装一个存档恢复点以及还原机器，而不用导入存档。

使用

此命令的使用如下：

```
/createarchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name] -path [path to the archive] -archiveusername [network user name] -archivepassword [network password] -cloudaccountname [name of the cloud account] -cloudcontainer [name of the cloud container]
```

命令选项

下表介绍 CreateArchiveRepository 命令可用的选项：

表. 174: CreateArchiveRepository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-name	必需。存档存储库的名称。

选项	说明
-path	现有存档的路径。它可以是本地、网络或云位置。例如：d:\work\archive 或 \\servername\sharename。
-archiveusername	可选。此选项是远程机器的登录。仅对于网络路径是必需的。
-archivepassword	可选。此选项是远程机器的密码。仅对于网络路径是必需的。
-cloudaccountname	可选。此选项是现有云帐户的显示名称。仅对于云路径是必需的。
-cloudcontainer	可选。云容器是存档所在位置。仅对于云路径是必需的。

示例：

创建名为“NewArchive:”的存档存储库。

```
>cmdutil /createarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path d:\work\archive
```

此外，如果存档包含多个位置，则命令应包括从 1 到 N 排序的所有分段的路径，其中 N 表示分段数量。

创建名为“NewSegmentArchive”的存档存储库。

```
>cmdutil /createarchiverepository -name NewSegmentArchive -path1 \\RemmoteServer1\Share\Archive\Segment1 - archiveusername1 Administrator -archivepassword1 23WE@#sdd -path2 Archives\NewSegment -cloudcontainer2 ArchiveContainer -cloudaccountname AmazonS3Local - path3 d:\work\archive\Third
```

CreateBootCD

此命令可让您创建裸机还原 (BMR) 启动 CD，而不需要使用 Rapid Recovery Core Console。

使用

此命令的使用如下：

```
/createbootcd -ip [IP address] -mask -defaultgateway -dnsserver -vncpassword -vncport -isofilepath [destination for the boot image]
```

命令选项

下表介绍 CreateBootCD 命令可用的选项：

表. 175: CreateBootCD 命令选项

选项	说明
-?	显示此帮助消息。
-ip	可选。此选项指定目标 BMR 机器的 IP 地址。默认情况下，它会自动生成。

选项	说明
-mask	可选。此选项指定目标 BMR 机器的子网掩码。默认情况下，它会自动生成。
-defaultgateway	可选。此选项指定目标 BMR 机器的默认网关。默认情况下，它会自动生成。
-dnsserver	可选。此选项指定目标 BMR 机器的 DNS 服务器。默认情况下，它会自动生成。
-vncpassword	可选。此选项指定现有 UltraVNC 帐户的用户密码。默认情况下，此选项为空。
-vncport	可选。此选项指定要用于 UltraVNC 的端口。仅当您使用了 -vncpassword 选项时，才能更改它。默认情况下，端口为 5900。
-isofilepath	可选。此选项指定启动 CD 文件的补丁。默认路径为 C:\ProgramData\AppRecovery\Boot CDs。

示例：

创建启动 CD。

```
>cmdutil /createbootcd -ip 192.168.20.188 -mask 255.255.255.0 -defaultgateway 192.168.20.2 -dnsserver 192.168.20.2 -isofilepath D:\bcd\newbcd3.iso
```

CreateRepository

使用 createrepository 命令以在本地机器及共享位置中创建新的 DVM 存储库。

使用

在本地位置中创建存储库时的命令使用如下：

```
/createrepository -name [repository name] -size [size allocated for repository] -datapath [data path of repository] -metadatapath [metadata path of repository] -core [host name] -user [user name] -password [password]
```

在共享位置中创建 DVM 存储库时的命令用法如下：

```
/createrepository -name [repository name] -size [size allocated for repository] -uncpath [path for data and metadata] -shareusername [user name for share location] -sharepassword [password for share user name] -concurrentoperations [number of operations to occur at one time] -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 createrepository 命令可用的选项：

表. 176: CreateRepository 命令选项

选项	说明
-?	显示有关命令的帮助。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-name	存储库名称。
-size	存储库存储位置的大小。可用单位包括 b、Kb、Mb、Gb、Tb 和 Pb。
-datapath	仅适用于本地位置。确定存储库存储位置的数据路径。
-metadatapath	仅适用于本地位置。确定存储库存储位置的元数据路径。
-uncpath	仅适用于共享位置。确定存储库存储位置的数据路径和元数据路径。
-shareusername	仅适用于共享位置。确定共享位置的用户名。
-sharepassword	仅适用于共享位置。确定共享位置的密码。
-comment	可选。存储库的说明。
-concurrentoperations	可选。一次可处于挂起状态的操作的最大数量。默认值为：64。

示例：

在本地位置中创建 DVM 存储库：

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -datapath d:\repository -metadatapath d:\repository -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

在共享位置中创建 DVM 存储库：

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -uncpath \\share\repository -shareusername login -sharepassword pass123 -comment "First repository." -concurrentoperations 8 -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

DeleteRepository

您可以使用 DeleteRepository 命令删除在 AppAssure Core 或 Rapid Recovery Core 中创建的整个 DVM 存储库。

使用

此命令的使用如下：

```
/deleterepository -core [host name] -user [user name] -password [password] name] -name [repository name] | -a [all repositories]
```

命令选项

下表介绍 DeleteRepository 命令可用的选项：

表. 177: DeleteRepository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-a	可选。此选项会删除与 Core 关联的所有 DVM 存储库。
-name	您想要删除的 DVM 存储库的名称。

示例:

删除所有 DVM 存储库:

```
>cmdutil /deleterepository -a
```

删除名为“RepositoryName:”的存储库。

```
>cmdutil /deleterepository -name RepositoryName
```

Dismount

使用 dismount 命令卸载 -path 选项指定的已安装恢复点，通过 -protectedserver 参数卸载所选 Agent 的恢复点或通过 -all 参数卸载所有已安装的恢复点。

使用

此命令的使用如下:

```
/dis[mount] -core [host name] -user [user name] -password [password] [-all | -protectedserver [name | IP address] | -path [location]
```

命令选项

下表介绍 dismount 命令可用的选项:

表. 178: Dismount 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	卸载所有已安装的恢复点。
-protectedserver	卸载当前代理的所有已安装恢复点。
-path	卸载所选安装点。

示例:

卸载已安装到文件夹 c:\mountedrecoverypoint 的恢复点:

```
>cmdutil /dismount -core 10.10.10.10 -user administrator -password 23WE@#sdd -path c:\mountedRecoveryPoint
```

DismountArchiveRepository

从已安装存档中检索到您需要的信息后，您应卸载存档以避免潜在问题。

使用

此命令的使用如下:

```
/dismountarchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name]
```

命令选项

下表介绍 DismountArchiveRepository 命令可用的选项:

表. 179: DismountArchiveRepository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-name	必需。存档存储库的名称。

示例:

卸载名为“NewArchive:”的存储库。

```
>cmdutil /dismountarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path d:\work\archive
```

EditEsxServer

当您需要对无代理保护的 VMware ESX(i) 虚拟机数量进行更改时，可以使用 editesxserver 命令。

使用

此命令的使用如下：

```
/editEsxServer -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -add | -remove -virtualMachines [virtual machines collection | all] -autoProtect [object ID or name collection]
```

命令选项

下表介绍 editesxserver 命令可用的选项：

表. 180: EditEsxServer 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-repository	必需。将与您要用来保护虚拟机的 Core 关联的存储库的名称。 注: 必须用双引号将名称括起。
-protectedserver	使用此选项可编辑特定受保护机器的 vCenter 和 ESX(i) 对象。
-add	使用此选项可以添加指定的 vCenter 或 ESXi 对象。
-remove	使用此选项可移除指定的 vCenter 或 ESXi 对象。
-virtualmachines	可选。此选项允许您列出您想要保护的虚拟机。
-autoprotect	可选。此选项允许您列出您想要自动保护的新虚拟机。

示例:

使用 Core 自动保护 vCenter 或 ESXi 服务器的特定 vCenter 或 ESXi 对象:

```
>cmdutil /editEsxServer -protectedserver 10.10.8.150 -add -autoprotect "Folder1" "Folder2"
```

Force

force 命令可强制创建指定受保护机器的快照。通过强制创建快照可强制当前受保护机器进行数据传输。强制创建快照时，传输将立即启动或添加到队列中。只会传输上个恢复点以来发生更改的数据。如果没有上个恢复点，则会传输受保护卷上的所有数据。

使用

此命令的使用如下:

```
/force [snapshot] default | [base] [-all | -protectedserver [name | IP address]] -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 force 命令可用的选项:

表. 181: Force 命令选项

选项	说明
-?	显示此帮助消息。
-force	可选。要创建的快照类型。可用值: 'snapshot' (增量快照) 和 'base' (基本映像快照)。默认情况下，将执行增量快照。
-core	可选。远程 Core 主机 IP 地址 (含可选的端口号)。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	强制创建 Core 上所有机器的快照。
-protectedserver	强制创建特定受保护机器的快照。

示例:

强制创建 Core 上所有机器的快照:

```
>cmdutil /force snapshot -core 10.10.10.10 -user administrator -password 23WE@#$$dd -all
```


ForceAttach

forceattach 命令可强制执行 SQL 数据库文件可附加性检查。强制执行可附加性检查时，检查会立即开始。

使用

此命令的使用如下：

```
/forceattach -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

命令选项

下表介绍 forceattach 命令可用的选项：

表. 182: ForceAttach 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	对其执行可附加性检查的受保护机器。
-rpn	对其执行检查的恢复点的序号（运行 /list rps 命令以获取序号）。要使用单个命令对多个恢复点执行检查，您可以指定用空格分隔的多个序号。
-time	按创建时间选择恢复点。您必须以“mm/dd/yyyy hh:mm tt”格式（例如，“2/24/2012 09:00 AM”）指定确切的时间。务必指定 PC 中所设置时区的日期和时间值。

示例：

对序号为 5 和 7 的恢复点执行可附加性检查：

```
>cmdutil /forceattach -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22 -rpn 5 7
```

ForceChecksum

forcechecksum 命令可用于强制检查出现在指定恢复点上的 Exchange Message Database (MDB) 的完整性。强制执行校验和检查时，会立即开始使用命令。

使用

此命令的使用如下：

```
/forcechecksum -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] -time [time string]
```

命令选项

下表介绍 forcechecksum 命令可用的选项：

表. 183: ForceChecksum 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	对其执行校验和检查的受保护机器。
-rpn	对其执行检查的恢复点的序号（运行 /list rps 命令以获取序号）。要使用单个命令对多个恢复点执行检查，您可以指定用空格分隔的多个序号。
-time	按创建时间选择恢复点。您必须以“mm/dd/yyyy hh:mm tt”格式（例如，“2/24/2012 09:00 AM”）指定确切的时间。务必指定 PC 中所设置时区的日期和时间值。

示例：

对序号为 5 和 7 的恢复点执行校验和检查：

```
>cmdutil /forcechecksum -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 5 7
```

ForceLogTruncation

强制日志截断可按需一次性执行此作业。此操作将立即截断指定 SQL Server 代理的日志。

使用

此命令的使用如下：

```
/[forcelogtruncation | flt] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address]
```

命令选项

下表介绍 forcelogtruncation 命令可用的选项：

表. 184: ForceLogTruncation 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	对其执行日志文件截断的受保护机器。

示例：

对受保护服务器执行强制日志截断：

```
>cmdutil /forcelogtruncation -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -protectedserver 10.10.20.20
```

ForceMount

使用 forcemount 命令以进行一次性恢复点可安装性检查。此检查将确定指定的一个或多个恢复点是否可以安装并用于还原备份数据。您必须列出要进行该检查的一个或多个特定恢复点，或创建恢复点的时间范围。

使用

此命令的使用如下：

```
/forcemount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

命令选项

下表介绍 forcemount 命令可用的选项：

表. 185: ForceMount 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	对其执行可安装性检查的受保护机器。
-rpn	对其执行检查的恢复点的序号（运行 /list rps 命令以获取序号）。要使用单个命令对多个恢复点执行检查，您可以指定用空格分隔的多个序号。
-time	按创建时间选择恢复点。您必须以“mm/dd/yyyy hh:mm tt”格式（例如，“2/24/2012 09:00 AM”）指定确切的时间。务必指定 PC 中所设置时区的日期和时间值。

示例：

对序号为 5 和 7 的恢复点执行可安装性检查：

```
>cmdutil /forcemount -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.20.20 -rpn 5 7
```

ForceReplication

使用 forcereplication 命令以强制将源 Core 中的已复制数据一次性传输到目标 Core。您可以复制一台特定受保护机器或复制所有受保护机器。受保护服务器必须已配置以进行复制。

使用

此命令的使用如下：

```
/[forcereplication |frep] -core [host name] -user [user name] -password [password] -targetcore [host name] -all | -protectedserver [name | IP address]
```

命令选项

下表介绍 forcereplication 命令可用的选项：

表. 186: ForceReplication 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-targetcore	应对其执行强制复制的目标 Core 的主机名。
-protectedserver	您想要复制的受保护机器。
-all	强制复制将复制到目标 Core 的所有机器。

示例：

强制复制特定目标 Core 上的受保护服务器：

```
>cmdutil /forcereplication -target core 10.10.10.10 -protectedserver 10.20.30.40
```

ForceRollup

使用 forcerollup 命令以强制汇总受保护机器上的恢复点。

使用

此命令的使用如下：

```
[/[forcerollup | fro] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address]
```

命令选项

下表介绍 forcerollup 命令可用的选项：

表. 187: ForceRollup 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据
-protectedserver	可选。要对其执行汇总的受保护机器。

示例：

强制汇总 Core 上的 10.10.10.1 代理。

```
>cmdutil /forcerollup -core 10.10.10.10 - user administrator -password 23WE@#sdd -protectedserver 10.10.10.1
```

ForceVirtualStandby

将数据从受保护的机器导出到虚拟机会创建虚拟待机机器。如果您有连续的虚拟导出设置，您可以使用此命令强制 Rapid Recovery 按需导出数据，而不考虑预先确定的计划。

使用

此命令的使用如下：

```
/forcevirtualstandby -core [host name] -user [user name] -password [password login] -protectedserver [name] | -all
```

命令选项

下表介绍 ForceVirtualStandby 命令可用的选项：

表. 188: ForceVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	虚拟化机器的名称或空格分隔的名称。
-all	此命令指定是否要强制执行所有已计划的虚拟导出。

示例：

强制执行所有虚拟待机导出：

```
>cmdutil /forcevirtualstandby -all
```

针对两台机器强制执行虚拟待机：

```
>cmdutil /forcevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

帮助

help 命令可显示可用命令的列表及其定义。此命令还将提供版权和版本的详细信息。

使用

此命令的使用如下：

```
/help
```

示例：

请求命令行帮助：

```
>cmdutil /help
```

List

list 命令将返回有关当前受 Core 保护的指定代理程序或服务器列表的所有恢复点、活动作业、已完成的作业、失败的作业、无效（失败）的恢复点、有效（通过）的恢复点、安装、受保护服务器、卷、虚拟化服务器、未受保护的卷、群集、保护组、SQL 数据库、Exchange 数据库、复制的服务器及存储库的信息。默认情况下，将返回最近的记录。您可以列出所有记录或使用数目参数指定将显示的记录数。此参数应包含字母“l”（表示最新的恢复点）和“f”（表示第一个恢复点）。每个恢复点均具有其自身的编号，管理员可以将此编号用于安装。

使用

此命令的使用如下：

```
/list [rps | passed | failed | mounts | volumes | protectedservers | activejobs | completed jobs | failedjobs | virtualizedservers | unprotectedvolumes | clusters | protectiongroups | sqldatabases | exchangemailstores | replicatedservers | repositories] -protectedserver [name | IP address] -core [host name] -user [user name] -password [password] -number [all | l<number> | f<number> | <number>] -jobtype
```

命令选项

下表介绍 list 命令可用的选项：

表. 189: List 命令选项

选项	说明
-?	显示此帮助消息。
-list	选择以下选项之一： - 所有恢复点 ('rps') - 有效恢复点 ('passed') - 无效恢复点 ('failed') - 安装 ('mounts') - 受保护卷 ('volumes') - 未受保护卷 ('unprotectedvolumes') - 受保护机器 ('protectedservers') - 活动作业 ('activejobs')

选项	说明
	- 失败的作业 ('failedjobs') - 已完成的作业 ('completedjobs') - 虚拟化服务器 ('virtualizedservers') - 群集 ('clusters') - 保护组 ('protectiongroups') - SQL Server 数据库 ('sqldatabases') - MS Exchange 数据库 ('exchangemailstores') - 复制的服务器 ('replicatedservers') - 存储库 ('repositories')
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	仅用于显示作业。显示 Core 服务器上特定类型（活动、失败、已完成）的所有事件。
-protectedserver	要显示恢复点的受保护机器。
-number	可选。要显示的数据项目数。仅用于以下分类符：'rps'、'activejobs'、'completedjobs'、'failedjobs'。可用的值包括： - all（提取所有数据项目） - l[number] 或 [number]（提取 ## 个最大的数据项目） - f[number]（提取前 ## 个数据项目） 仅在显示恢复点和作业时生效。
-jobtype	可选。按作业类型筛选输出。可用的值包括： 'transfer'（数据传输） 'repository'（存储库维护） 'replication'（本地和远程复制） 'backup'（备份和还原） 'bootcdbuilder'（创建启动 CD） 'diagnostics'（上传日志） 'exchange'（Exchange Server 文件检查） 'export'（恢复点导出） 'pushinstall'（部署代理） 'restore'（恢复点还原） 'rollup'（受保护机器汇总） 'sqlattach'（代理可附加性检查） 'mount'（安装存储库）

示例:

列出最近 30 个恢复点:

```
>cmdutil /list rps -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22 -number 130
```

查看受保护机器执行的所有失败的数据传输作业:

```
>cmdutil /list failed jobs -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22 -number all -jobtype transfer
```

安装

mount 命令将安装一个或多个驱动器的快照。您可以指定安装是否应为读、写或只读带此前写入。默认选择是只读。

使用

此命令的使用如下:

```
/mount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -mounttype [read | write | readOnlyWithPreviousWrites] -drives [drive names] -volumes [volume names] -path [location] -rpn [number | numbers] | -time [time string]
```

命令选项

下表介绍 mount 命令可用的选项:

表. 190: Mount 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要安装一个或多个恢复点的受保护机器。
-mounttype	可选。指定安装模式。可用值包括 'read' (read-only)、'readOnlyWithPreviousWrites' (对以前的写入为只读) 和 'write' (可写入)。默认模式为 read-only。
-volumes	可选。要安装的卷名称列表。如果未指定，则将安装所有卷。必须使用双引号括起并用空格分隔值；例如: "c:" "d:"。请勿在卷名称中使用尾部反斜杠。
-path	恢复点安装所在的 Core 服务器上文件夹的路径。如果不存在此类文件夹，则将自动创建一个文件夹。

选项	说明
-rpn	可选。要安装的恢复点的序号（使用 /list rps 命令以获取序号）。指定多个空格分隔的序号以使用单个命令安装多个恢复点。在此情况下，每个恢复点中的数据将存储在单独的子文件夹中。注：如果未指定 -time 和 -rpn 选项，则将安装成功通过完整性检查的最新恢复点。
-time	可选。确定选择要安装的一个或多个恢复点。可用值包括：“latest”、“passed”、“mm/dd/yyyy hh:mm tt”格式的确切时间（例如，“2/24/2012 09:00 AM”）。务必指定 PC 中所设置时区的日期和时间值。如果未指定 -time 和 -rpn 选项，则将安装成功通过完整性检查的最新恢复点。
-localdrive	可选。执行安装到本地 PC 上的用户磁盘。

示例：

在只读模式下安装包含“c:\”和“d:\”卷的最新恢复点：

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -mounttype read -volumes "c:" "d:"
```

安装序号为 2 和 7 的恢复点：

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -rpn 2 7
```

MountArchiveRepository

要在 Rapid Recovery 中从存档还原数据，您必须先安装存档。

使用

此命令的使用如下：

```
/mountarchiverepository -core [host name] -user [user name] -password [password] -name [archive repository name]
```

命令选项

下表介绍 mountarchiverepository 命令可用的选项：

表. 191: MountArchiveRepository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-name	必需。存档存储库的名称。

示例:

安装名为“NewArchive:”的存储库。

```
>cmdutil /mountarchiverepository -name NewArchive
```

NewCloudAccount

使用 NewCloudAccount 命令可将云提供程序的帐户添加到 Rapid Recovery Core。您随后可以使用该帐户来存储用于保留或复制的存档。

使用

此命令的使用如下:

```
/newcloudaccount -core [host name] -user [user name] -password [password] -displayname [name for the account] -type [cloud account provider] -username [user name for the account] -key [secret key] -region [region for account] tenanatid [tenant ID] -authurl [authorization URL]
```

命令选项

下表介绍 NewCloudAccount 命令可用的选项:

表. 192: NewCloudAccount 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-displayname	要用于云帐户的名称。
-type	云帐户的类型。支持的值包括: - amazon - openstack - rackspace - windowsazure "windows azure" - azure
-username	要添加的云帐户的用户名。这是在验证过程中使用的凭据。属性具有以下变化形式，具体视云类型而定: - Amazon - 访问密钥 - OpenStack - 用户名

选项	说明
	• Rackspace - 用户名 • Windows Azure - 存储帐户名称
-key	要添加的云帐户的验证密钥。这是在验证过程中使用的凭据。属性具有以下变化形式，具体视云类型而定： • Amazon - 机密密钥 • OpenStack - API 密钥 • Rackspace - API 密钥 • Windows Azure - 访问密钥
-region	要添加的云帐户的地区。仅 OpenStack 和 Rackspace 帐户需要此选项。
-tenantid	用来验证 OpenStack 云帐户的 ID。仅 OpenStack 云帐户需要此选项。
-authurl	用来验证 OpenStack 云帐户的 URL。仅 OpenStack 云帐户需要此选项。

示例：

添加一个新的云帐户，其名为“Amazon S3 Account”，其访问密钥为“akey”，其机密密钥为“skey”。

```
>cmdutil /newcloudaccount -displayname "Amazon S3 Account" -type amazon -username akey -key skey
```

OpenDvmRepository

使用此命令可打开在 AppAssure Core 或 Rapid Recovery Core 中创建的现有 DVM 存储库。

使用

此命令的使用如下：

```
/opendvmrepository -localpath [local path] -sharepath [network share path] -shareusername [user name for network share] -sharepassword [network share password]
```

命令选项

下表介绍 OpenDvmRepository 命令可用的选项：

表. 193: OpenDvmRepository 命令选项

选项	说明
-?	显示此帮助消息。
-localpath	本地 Core 上具有 DVM 存储库的文件夹的路径。
-sharepath	CIFS 共享上具有 DVM 存储库的文件夹的路径。
-shareusername	用于登录共享文件夹的用户名。

选项	说明
-sharepassword	用于登录共享文件夹的密码。

示例：

在本地机器上打开现有 DVM 存储库：

```
>cmdutil /opendvmrepository -localpath E:\Repository
```

Pause

管理员可以暂停快照、导出到虚拟机或复制 Core。pause 命令接受三个参数：snapshot、vmexport、和 replication。只能指定一个参数。如果指定时间参数，则可以在一段时间后暂停快照。

用户可以通过三种方式暂停复制：

- 在所有受保护机器的源 Core 上。(-[outgoing])。
管理员必须通过传出复制配对指定远程机器名称以暂停源 Core 上的传出复制：


```
>cmdutil /pause replication /o 10.10.12.10
```
- 在单个受保护机器的源 Core 上。(-protectedserver):

```
>cmdutil /pause replication /protectedserver 10.10.12.97
```
- 在目标 Core 上(-incoming)。
如果本地 Core 是目标 Core，则管理员可以使用传入参数指定源 Core 来暂停复制：


```
>cmdutil /pause replication /i 10.10.12.25
```

使用

此命令的使用如下：

```
/pause [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

命令选项

下表介绍 pause 命令可用的选项：

表. 194: Pause 命令选项

选项	说明
-?	显示此帮助消息。
-pause	[snapshots]、[replication] 或 [vmexport]。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	可选。暂停所选 Core 上的所有代理。
-protectedserver	可选。暂停当前受保护的服务器。
-incoming	可选。复制到 Core 机器的远程 Core 的主机名。
-outgoing	可选。数据复制到的远程目标 Core 的主机名。
-time	可选。恢复快照（仅适用于快照暂停）的时间，格式为“天-小时-分钟”。

示例：

暂停为特定受保护服务器创建快照：

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -protectedserver 10.10.10.4
```

暂停为受保护机器创建快照，并在三天、20 小时和 50 分钟后恢复创建快照：

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -protectedserver 10.10.10.4 -time 3-20-50
```

暂停 Core 上所有受保护机器的导出到虚拟机：

```
>cmdutil /pause vmexport -core 10.10.10.10 /user administrator -password 23WE@#$$sdd -all
```

暂停 Core 上特定受保护机器的传出复制：

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -protectedserver 10.10.1.76
```

暂停目标 Core 上所有受保护机器的传出复制：

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -outgoing 10.10.1.63
```

暂停目标 Core 上所有机器的传入复制：

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -incoming 10.10.1.82
```

Protect

protect 命令可添加受 Core 保护的服务器。

使用

此命令的使用如下：

```
/protect -core [host name] -user [user name] -password [password] -repository [name] -agentname [name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -volumes [volume names]
```

命令选项

下表介绍 protect 命令可用的选项：

表. 195: Protect 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-repository	Core 上存储受保护机器数据的存储库名称。该名称必须使用双引号括起。
-agentname	要保护的服务器的名称或 IP 地址。
-agentusername	受保护服务器的用户名。
-agentpassword	受保护服务器的密码。
-agentport	受保护服务器端口号。
-volumes	保护的卷列表。必须使用双引号引起并用空格分隔值。请勿在卷名称中使用尾部反斜杠；例如：“c:”、“d:”。

示例：

使用 Core 保护服务器的特定卷：

```
>cmdutil /protect -core 10.10.10.10 -username administrator -password 23WE@#$sdd -repository "Repository 1" -agentname 10.10.9.120 -agentport 5002 -agentusername administrator agentpassword 12345 -volumes "c:" "d:"
```

ProtectCluster

protectcluster 命令可添加受 Core 保护的群集。

使用

此命令的使用如下：

```
/protectcluster -core [host name] -user [user name] -password [password] -repository [name] -clustername [name | IP address] -clusterusername [user name] -clusterpassword [password] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes collection]
```

命令选项

下表介绍 protectcluster 命令可用的选项：

表. 196: ProtectCluster 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-repository	Core 上存储受保护机器数据的存储库名称。该名称必须使用双引号括起。
-clustername	要保护的群集的名称或 IP 地址。
-clusterusername	受保护群集的用户名。
-clusterpassword	受保护群集的密码。
-clusterport	受保护群集服务器端口号。
-clustervolumes	保护的卷列表。必须使用双引号引起并用空格分隔值。请勿在卷名称中使用尾部反斜杠；例如：“c:”、“d:”。
-clusternodes	群集节点和每个节点中要保护的卷的列表。

示例：

使用 Core 保护群集服务器的特定卷：

```
>cmdutil /protectcluster -core 10.10.10.10 -username administrator -password 23WE@#$$dd -
repository "Repository 1" -clustername 10.10.8.150 -clusterport 8006 -clusterusername
clusterAdmin clusterpassword password -volumes "C:\ClusterStorage\Volume1" -clusternodes
nodeName 10.10.8.150 volumes "c:" nodeName 10.10.8.151 volumes "c:"
```

ProtectEsxServer

当您想要将 VMware ESX(i) 虚拟机添加为保护对象时，可以使用 protectesxserver 命令。

使用

此命令的使用如下：

```
/protectesxserver -core [host name] -user [user name] -password [password] -repository
[repository name] -server [name | IP address] -serverusername [user name] -serverpassword
```

[password for server login] -serverport [port] -virtualMachines [virtual machines collection | all] -autoProtect [object ID or name collection]

命令选项

下表介绍 protectesxserver 命令可用的选项：

表. 197: ProtectEsxServer 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-repository	必需。将与您要用来保护虚拟机的 Core 关联的存储库的名称。 ① 注: 必须用双引号将名称括起。
-server	要保护的 vCenter 或 ESXi 服务器的名称或 IP 地址。
-serverusername	用于登录到您想要保护的 vCenter 或 ESXi 服务器的用户名。
-serverpassword	用于登录到您想要保护的 vCenter 或 ESXi 服务器的密码。
-serverport	可选。您想要保护的 vCenter 或 ESXi 服务器的端口号。
-virtualmachines	可选。此选项允许您列出您想要保护的虚拟机。
-autoprotect	可选。此选项允许您列出您想要自动保护的新虚拟机。

示例：

使用 Core 保护 vCenter 或 ESXi 服务器中的特定虚拟机：

```
>cmdutil /protectesxserver -core 10.10.10.10 -user admin -password password -repository "Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root -serverpassword password -virtualmachines "VM1" "VM2" -autoprotect "Folder1"
```

RemoveAgent

RemoveAgent 命令可用于移除受 Core 保护的机器，可选择性地删除已移除机器的恢复点。如果不删除恢复点，Rapid Recovery 将保留它们并将它们标识仅限于恢复点的机器。

使用

此命令的使用如下：

```
/removeagent -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -deleterecoverypoints
```

命令选项

下表介绍 RemoveAgent 命令可用的选项：

表. 198: RemoveAgent 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要移除保护的服务器的名称或 IP 地址。
-deleterecoverypoints	可选。删除想要移除的机器上的所有恢复点。

示例：

移除机器的保护，并删除关联的恢复点：

```
>cmdutil /removeagent -protectedserver 10.10.1.1 -deleterecoverypoints
```

RemoveArchiveRepository

您可以使用 removearchiverepository 命令从 Rapid Recovery Core 中删除存储库。

使用

此命令的使用如下：

```
/removearchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name]
```


命令选项

下表介绍 removearchiverepository 命令可用的选项：

表. 199: RemoveArchiveRepository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-name	必需。存档存储库的名称。

示例：

从本地 Core 中移除名为“NewArchive”的存储库：

```
>cmdutil /removearchiverepository -name NewArchive
```

RemovePoints

removepoints 命令可用于删除受保护机器的特定恢复点。

使用

此命令的使用如下：

```
/removepoints -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

命令选项

下表介绍 removepoints 命令可用的选项：

表. 200: RemovePoints 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要从中删除恢复点的服务器的名称或 IP 地址
-rpn	可选。要删除的恢复点的序号（使用 /list rps 命令以获取序号）。指定多个空格分隔的序号以使用单个命令删除多个恢复点。
-time	可选。通过创建时间确定选择要删除的一个或多个恢复点。以 "mm/dd/yyyy hh:mm tt" 格式指定确切的时间（例如，"2/24/2012 09:00 AM"）。务必指定 PC 中所设置时区的日期和时间值。

示例：

删除序号为 5 和 7 的恢复点：

```
>cmdutil /removepoints -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22 -rpn 5 7
```

RemoveScheduledArchive

使用此命令可停止现有 Rapid Recovery 计划的连续的存档。

使用

此命令的使用如下：

```
/removescheduledarchive -core [host name] -user [user name] -password [password] name] -all -ids [id | id1 id2]
```

命令选项

下表介绍 removescheduledarchive 命令可用的选项：

表. 201: RemoveScheduledArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	此选项指定是否移除与此 Core 相关联的所有计划存档。
-ids	使用此选项可列出您要移除的每个计划存档的一个或多个 ID。用空格分隔多个 ID。

示例：

移除所有计划存档：

```
>cmdutil /removescheduledarchive -all
```

移除一个计划存档：

```
>cmdutil /removescheduledarchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

RemoveVirtualStandby

可在 Rapid Recovery 命令公用程序中使用此命令来停止将数据连续导出到虚拟机。

使用

此命令的使用如下：

```
/removevirtualstandby -core [host name] -user [user name] -password [password login] -protectedserver [name] | -all
```

命令选项

下表介绍 removevirtualstandby 命令可用的选项：

表. 202: RemoveVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	虚拟化机器的名称或空格分隔的名称。
-all	此命令指定是否要移除所有已计划的虚拟导出。

示例：

移除所有虚拟待机导出：

```
>cmdutil /removevirtualstandby -all
```

针对两台机器移除虚拟待机导出：

```
>cmdutil /removevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

Replicate

使用 Replicate 命令在两个 Rapid Recovery Core 间建立复制。

使用

此命令的使用如下：

```
/replicate -request [email | email customer ID] -targetserver [host name | hostname port |
hostname user name password | hostname port user name password] -replicationname [name] -
seeddrive [localpath | network path username password] [comment] -protectedserver [name | name
repository]
```

命令选项

下表介绍 Replicate 命令可用的选项：

表. 203: Replicate 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据
-request	可选。如果希望使用非现场备份和灾难恢复服务的第三方提供者的订阅，请指定此选项。
-targetserver	要在其中建立复制的服务器的名称。它包括以下参数： - port - user name - password port 参数是可选，默认值为 8006。如果您使用 request 选项，您还应使用目标服务器的用户名和密码。
-replicationname	可选。如果您没有使用 request 选项，则使用复制作业的名称。
-seeddrive	可选。使用此选项为初始数据传输指定种子驱动器。comment 为可选参数。
-protectedserver	您想要复制的受保护机器的列表。如果您使用 request 选项，仅列出受保护机器的名称或 IP 地址。否则，将列出受保护机器以及相应的远程存储库名称。

示例:

使用网络共享中的种子驱动器将两个受保护机器复制到远程 Core:

```
>cmdutil /replicate -targetserver 10.10.1.100 Administrator 123Q -replicationname
ReplicationName -seeddrive Network \\10.10.1.100\seeddrive Administrator 123Q -protectedserver
10.10.1.1 Repository1 10.10.1.2 Repository2
```

复制

使用 replication 命令可以控制两个 Rapid Recovery Core 之间的现有复制以及管理挂起的复制请求。

① 注: 此命令继承 Replicate 命令，它在 Core 之间建立连接（称为配对），并使用种子驱动器进行初始数据传输。有关此命令的更多信息，请参阅 Replicate。

使用

此命令的使用如下:

```
/replication [-list [incoming | outgoing | pending] -accept | -deny | -ignore | -delete | -
edit] -id [replication ID] -protectedserver [name | name repository] -responsecomment [comment]
-deleterecoverypoints -scheduletype [type] -dailystarttime [time] -dailyendtime [time] -
weekdaystarttime [time] -weekdayendtime [time] -weekendstarttime [time] -weekendendtime [time]
```

命令选项

下表介绍 replication 命令可用的选项:

表. 204: Replication 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据
-list	传入或输出复制作业或挂起复制请求的列表。
-accept	接受复制请求。
-deny	拒绝复制请求。
-ignore	忽略复制请求。
-delete	使用此选项删除现有复制作业或从复制作业中删除机器。仅指定 -id 参数以删除整个复制关系，或同时指定 -id 和 -protectedserver 参数以只从复制中删除特定机器。

选项	说明
-edit	编辑现有复制计划的计划。
-id	复制作业或挂起复制请求的标识符。它可以是远程 Core ID、主机名、客户 ID、电子邮件地址或挂起复制请求 ID。
-protectedserver	响应复制请求时，使用此选项将您的响应应用于具有存储库名称或 ID 的受保护服务器列表。使用参数“all”可将响应应用到所有请求的机器。
-responsecomment	您通过对挂起复制请求的响应提供的注释。
-deleterecoverypoints	如果来自已删除的复制机器中的特定恢复点也应删除，则使用此选项。
-scheduletype	如果您使用 -edit 选项，则此选项指定复制计划的类型。包括以下四个值之一： - atalltimes - 在任意时间自动复制。 - daily - 每天复制。指定 -dailystarttime 和 -dailyendtime 参数。 - custom - 使用每日复制时，使用此值可计划在工作日或周末复制。指定 -weekdaystarttime、-weekdayendtime、-weekendstarttime 和 -weekendendtime 参数。
-dailystarttime	仅用于 -scheduletype 选项的 daily 值。它用于建立应该发生复制的时间范围。使用此选项可指定您希望复制开始的最早当日时间。
-dailyendtime	仅用于 -scheduletype 选项的 daily 值。它用于建立应该发生复制的时间范围。使用此选项可指定您希望复制开始的最迟当日时间。
-weekdaystarttime	仅用于 -scheduletype 选项的 custom 值。它用于建立应该发生复制的时间范围。使用此选项可指定您希望复制开始的最早工作日时间。
-weekdayendtime	仅用于 -scheduletype 选项的 custom 值。它用于建立应该发生复制的时间范围。使用此选项可指定您希望复制开始的最迟工作日时间。
-weekendstarttime	仅用于 -scheduletype 选项的 custom 值。它用于建立应该发生复制的时间范围。使用此选项可指定您希望复制开始的最早周末时间。
-weekendendtime	仅用于 -scheduletype 选项的 custom 值。它用于建立应该发生复制的时间范围。使用此选项可指定您希望复制开始的最迟周末时间。

示例：

列出所有传入复制：

```
>cmdutil /replication -list incoming
```

接受两个保护机器的挂起复制请求：

```
>cmdutil /replication -accept -id customer@email.address -protectedserver 10.10.1.1 Repository1
10.10.1.2 Repository2 -responsecomment A response comment
```

拒绝挂起复制请求：

```
>cmdutil /replication -deny -id customer@email.address
```

删除具有复制的恢复点的现有复制：

```
>cmdutil /replication -delete -id RemoteServerHostname -deleterecoverypoints
```

从现有复制中移除两个机器：

```
>cmdutil /replication -delete -id "156d7a46-8e44-43f4-9ed8-60d998e582bf" -protectedserver 10.10.1.1 10.10.1.2
```

使用指定的工作日和周末时间编辑复制计划：

```
>cmdutil /replication -edit -id RemoteServerHostName -scheduletype custom -weekdaystarttime "9:00 AM" -weekdayendtime "6:00 PM" -weekendstarttime "9:00 AM" -weekendendtime "6:00 PM"
```

RestoreAgent

restoreagent 命令可让您从特定 Rapid Recovery 恢复点还原受保护机器或卷。

使用

此命令的使用如下：

```
/restoreagent -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs | names | all] -targetmachine [name] -targetvolume [volume name] -forcedismount -autorestart
```

命令选项

下表介绍 restoreagent 命令可用的选项：

表. 205: RestoreAgent 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要还原的服务器的名称或 IP 地址。
-rpn	要用来还原机器的恢复点的标识号。要查找正确编号，请使用命令 /list rps。
-volumes	要还原的卷的 ID 或名称。要还原所有受保护卷，请使用 -volumes all。
-targetmachine	您要将受保护机器还原到的机器的名称。
-targetvolume	您要将机器还原到的卷的名称或 ID。
-forcedismount	可选。使用此选项以强制按需卸载数据库。
-autorestart	可选。如果需要重新启动 Exchange Server 机器，请使用此命令。

示例:

将机器还原到 IP 地址为 192.168.20.130 的受保护机器，包括强制卸载数据库选项：

```
>cmdutil /restoreagent -protectedserver 192.168.20.130 -rpn 259 -volumes "F:" "E:" "C:" -
targetmachine 192.168.20.174 -targetvolume "E:" "G:" "F:" -forcedismount
```

RestoreArchive

此命令将还原本地存档或共享中的存档，并将还原的数据放置在指定的存储库中。

使用

此命令的使用如下：

```
/restorearchive -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address] -repository [name] -archiveusername [name] -archivepassword
[password] -path [location]
```

命令选项

下表介绍 restorearchive 命令可用的选项：

表. 206: RestoreArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	从存档文件中还原所有受保护机器的数据。
-protectedserver	要还原恢复点的受保护机器。您可以指定以双引号括起并用空格分隔的多个机器名称。
-repository	Core 上存储还原的恢复点的存储库名称。该名称必须使用双引号括起。
-archiveusername	可选。远程机器的用户名。仅网络路径需要。
-archivepassword	可选。远程机器的密码。仅网络路径需要。
-path	要还原的存档数据的位置；例如：d:\work\archive 或网络路径 \\servername\sharename。

示例:

还原所有受保护服务器的存档数据:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE0#$$sdd -all -
repository repository1 -path d:\work\archive
```

还原特定受保护服务器的存档数据:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE0#$$sdd -
protectedserver "10.10.20.30" "20.10.10.5" -repository repository1 -path d:\work\archive
```

RestoreUrc

restoreurc 命令可让您使用通用恢复控制台 (URC) 将特定 Rapid Recovery 恢复点中的受保护机器或卷还原到裸机。

使用

此命令的使用如下:

```
/restoreurc -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs |
names | all] -targetmachine [IP address] -urcpassword [password from the URC] -targetdisk [disk
number | all]
```

命令选项

下表介绍 restoreurc 命令可用的选项:

表. 207: RestoreUrc 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要将 URC 还原到的服务器的名称或 IP 地址。
-rpn	要用来还原机器的恢复点的标识号。要查找正确编号，请使用命令 /list rps。
-volumes	要还原的卷的 ID 或名称。要还原所有受保护卷，请使用 -volumes all。
-targetmacchine	您要将受保护机器还原到的机器的名称。
-urcpassword	URC 中的身份验证密钥。
-targetdisk	您要将机器还原到的磁盘编号。要使用 URC 从机器中选择所有磁盘，请使用 -targetdisk all。

示例:

使用 URC 将机器还原到磁盘 0 和 1，URC 机器的 IP 地址为 192.168.20.175:

```
>cmdutil /restoreurc -protectedserver 192.168.20.130 -rpn 259 -volumes "C:" "E:" -targetmachine 192.168.20.175 -urcpassword ***** -targetdisk 0 1
```

Resume

管理员可以此命令来恢复快照、导出到虚拟机及复制。您必须通过参数指定您的恢复需求。以下参数有效: snapshot、vmexport 和 replication。有关更多详细信息，请参阅 [Pause](#)。

使用

此命令的使用如下:

```
/resume [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

命令选项

下表介绍 resume 命令可用的选项:

表. 208: Resume 命令选项

选项	说明
-?	显示此帮助消息。
-restore	[snapshots]、[replication] 或 [vmexport]。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	恢复所选 Core 上的所有代理。
-protectedserver	恢复当前受保护的服务器。
-incoming	复制到 Core 机器的远程 Core 的主机名。
-outgoing	数据复制到的远程目标 Core 的主机名。

示例:

恢复特定受保护服务器的快照:

```
>cmdutil /resume snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.10.4
```

恢复 Core 上所有受保护机器的导出到虚拟机:

```
>cmdutil /resume vmexport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

恢复 Core 上特定受保护机器的传出复制:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.1.76
```

恢复目标 Core 上所有受保护机器的传出复制:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -outgoing 10.10.1.63
```

恢复目标 Core 上所有机器的传入复制:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -incoming 10.10.1.82
```

SeedDrive

当您建立 Rapid Recovery 复制时，您可以为初始数据传输使用种子驱动器。

使用

此命令的使用如下:

```
/seeddrive [-list | -startcopy | -startconsume | -abandon] -path [local | network path] -seeddriveusername [user name] -seeddrivepassword [password] -remotecore [name] [-targetcore [name or IP] | -protectedserver [name] | -all] -usecompatibleformat
```

命令选项

下表介绍 seeddrive 命令可用的选项:

表. 209: SeedDrive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-list	未完成的种子驱动器与扩展信息的列表。
-startcopy	开始将数据复制到种子驱动器。
-startconsume	开始使用种子驱动器。
-abandon	放弃未完成的种子驱动器请求。
-path	种子驱动器的本地或网络路径。
-seeddriveusername	可选。种子驱动器网络位置的用户名。
-seeddrivepassword	可选。种子驱动器网络位置的密码。
-targetcore	可选。只能与 -copy 选项一起使用。它是远程 Core 的名称或 IP 地址。所有复制到此 Core 的受保护机器均接收种子驱动器恢复点。
-remotecore	只能与 -consume 选项一起使用。它是从中创建或使用了种子驱动器恢复点的远程 Core 的名称。
-protectedserver	用于创建或使用恢复点的种子驱动器的受保护机器的名称或 IP 地址。例如：-protectedserver "10.10.60.48" "10.10.12.101"。
-all	此选项可指定是使用还是复制所有可用的受保护机器。
-usecompatibleformat	新存档格式提供更好的性能；但它与旧 Core 不兼容。处理传统 AppAssure Core 时，请使用此选项。

示例：

列出未完成的种子驱动器：

```
>cmdutil /seeddrive -list
```

将两个受保护机器复制到网络共享上的种子驱动器：

```
>cmdutil /seeddrive -startcopy -remotecore TargetCoreName -path \\10.10.1.1\Share\Seed\ -seeddriveusername Administrator -seeddrivepassword 12345 -usecompatibleformat
```

开始使用种子驱动器：

```
>cmdutil /seeddrive -startconsume -path \\10.10.1.1\Share\Seed\ -seeddriveusername Adminsitrator -seeddrivepassword 12345 -remotecore RemoteCoreName
```

放弃未完成的种子驱动器请求：

```
>cmdutil /seeddrive -abandon RemoteCoreHostName
```

StartExport

startexport 命令可强制将受保护机器中的数据一次性导出到虚拟服务器。您可以导出到 ESXi、VMware Workstation、Hyper-V 或 VirtualBox 虚拟机。如果要导出到 ESXi，则必须指定密集或精简磁盘配置。

使用

此命令的使用如下：

```
/startexport -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -volumes [volume names] -rpn [recovery point number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual hostport number] -hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocalmachine]
```

命令选项

下表介绍 startexport 命令可用的选项：

表. 210: StartExport 命令选项

选项	说明
-?	显示此帮助消息。
-exporttype	将数据从受保护服务器导出到 ESXi 服务器 ('esxi')、VMware Workstation 服务器 ('vm')、Hyper-V 服务器 ('hyperv') 或 VirtualBox 服务器 ('vb')。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要导出恢复点的受保护机器。
-volumes	可选。要导出的卷名称列表。如果未指定，则将导出所有卷。必须使用双引号括起并用空格分隔值；例如：“c:” “d:”。请勿在卷名称中使用尾部反斜杠。
-rpn	可选。要导出的恢复点的序号（使用 Get-RecoveryPoints 命令以获取序号）。如果未指定 'time' 和 'rpn' 选项，则将导出最近的恢复点。
-time	可选。确定选择要导出的一个或多个恢复点。您需要以“mm/dd/yyyy hh:mm tt”格式指定确切的时间（例如，“2/24/2012 09:00 AM”）。务必指定 PC 中所设置时区的日期和时间值。注：如果未指定 'time' 和 'rpn' 选项，则将导出最近的恢复点。
-vmname	虚拟机的 Windows 名称。
-hostname	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器主机名。
-linuxhostname	仅适用于 VirtualBox 导出。虚拟服务器主机名。
-hostport	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器端口号。
-hostusername	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器主机的用户名。
-hostpassword	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器主机的密码。

选项	说明
-ram	使用此选项在虚拟服务器中分配特定数量的 RAM。
-usesourceram	可选。使用此选项在源机器包含的虚拟服务器上分配相同容量的 RAM。
-diskprovisioning	此选项仅适用于 ESXi 导出。可选。您要在虚拟机上分配的磁盘空间容量。使用以下两种规格之一： - 完整 - 此规格使虚拟磁盘与受保护机器上的原始驱动器一样大。 - 精简 - 此规格分配在原始驱动器上占用的实际磁盘空间容量再加上额外的几 MB。 默认规格为“精简”。
-diskmapping	此选项仅适用于 ESXi 导出。可选。此选项确定如何将受保护机器中的磁盘映射到虚拟机。使用以下值之一： - 自动 - 此值自动映射磁盘。 - 手动 - 此值可让您手动映射磁盘。 - 使用 VM - 此值将虚拟磁盘存储在您选择的数据存储中。 默认值为“自动”。
-targetpath	仅适用于 VMware Workstation 或 VirtualBox 导出。此选项指定您要存储虚拟机文件的文件夹的本地或网络路径（或 Linux 路径，仅限于 VirtualBox）
-pathusername	仅适用于 VMware Workstation 导出。它是网络机器的用户名。仅当您在 -targetpath 选项中指定网络路径时需要。
-pathpassword	仅适用于 VMware Workstation 导出。它是网络机器的密码。仅当您在 -targetpath 选项中指定网络路径时需要。
-uselocalmachine	仅适用于 Hyper-V 导出。可选。使用此命令连接到本地 Hyper-V 服务器。此选项忽略 -hostname、-hostport、-hostusername 和 -hostpassword 选项。

示例：

将数据导出到特定名称且与源受保护服务器具有相同 RAM 和磁盘大小容量的 ESXi 虚拟机：

```
>cmdutil /startexport -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

使用恢复点 #4 中的受保护数据在本地驱动器上创建 VMware Workstation 机器文件：

```
>cmdutil /startexport -exporttype vmstation -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 4 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```

创建要存储在远程机器上的 Hyper-V 机器文件：

```
>cmdutil /startexport -exporttype hyperv -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -vmlocation \\WIN7-Bobby\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword 12QWsdxc@# -ram 4096
```

UpdateRepository

updaterepository 命令可将新存储位置添加到现有存储库。

使用

此命令的使用如下：

```
/updaterepository -name [repository name] -size [size of the repository] [-datapath [data path]
-metadatapath [metadata path] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password] -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 updaterepository 命令可用的选项：

表. 211: UpdateRepository 命令选项

选项	说明
-?	显示此帮助消息。
-name	存储库名称。
-size	存储库存储位置的大小。可用单位包括 b、Kb、Mb、Gb、Tb 和 Pb。
-datapath	仅适用于本地位置。确定存储库存储位置的数据路径。
-metadatapath	仅适用于本地位置。确定存储库存储位置的元数据路径。
-uncpath	仅适用于共享位置。确定存储库存储位置的数据路径和元数据路径。
-shareusername	仅适用于共享位置。确定共享位置的用户名。
-sharepassword	仅适用于共享位置。确定共享位置的密码。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。

示例：

在本地 DVM 存储库中创建新的存储位置：

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -datapath d:\repository -
metadatapath d:\repository -core 10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

在共享位置创建 DVM 存储库的存储位置：

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -uncpath \\share\repository -
shareusername login -sharepassword 23WE@#$sdd -core 10.10.10.10:8006 -username administrator -
password 23WE@#$sdd
```

版本

version 命令显示有关安装在指定服务器上的 Rapid Recovery 软件版本信息。如果不指定 Core 或受保护服务器，返回的信息将适用于当前正在工作的 Core 上。

使用

此命令的使用如下：

```
/[version | ver] -protectedserver [name | IP address]
```

命令选项

下表介绍 version 命令可用的选项：

表. 212: Version 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	可选。要查看哪个受保护机器的版本信息。如果不指定保护机器，返回的信息将是有关您正工作的 Core 机器。

示例：

显示有关安装在当前 Rapid Recovery Core 上的 Rapid Recovery 版本的信息：

```
>cmdutil /version
```

VirtualStandby

您可以使用 virtualstandby 命令从 Rapid Recovery 受保护机器导出数据到兼容的虚拟机。

使用

此命令的使用如下：

```
/virtualstandby -edit -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -volumes [volume names] -vmname [virtual machine name] -gen2 -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total
```

megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocal machine] -initialexport

命令选项

下表介绍 virtualstandby 命令可用的选项：

表. 213: VirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-exporttype	此选项将数据从受保护机器导出到以下指定的虚拟服务器之一： - esxi (ESXi) - vm (VMware Workstation) - hyperv (Hyper-V) - vb (VirtualBox)
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	使用此选项可指定您想要导出其恢复点的受保护机器。
-volumes	可选。使用此选项可列出在您想要导出的卷的名称。如果您未指定卷，则导出恢复点中的所有卷。使用双引号括起并用空格分隔值："c:" "d:"。请勿在卷名称中使用尾部斜杠。
-ram	使用此选项在虚拟服务器中分配特定数量的 RAM。
-usesourceram	可选。使用此选项在源机器包含的虚拟服务器上分配相同容量的 RAM。
-vmname	虚拟机的 Windows 名称。
-gen2	可选。此选项指定虚拟机服务器的第 2 代。如果不指定代，此命令将会使用第 1 代。以下操作系统支持第 2 代： - Windows - Windows Server 2012 R2 - Windows 8.1 - Ubuntu Linux - CentOs - RHEL - Oracle Linux 7
-hostname	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器主机名。
-linuxhostname	仅适用于 VirtualBox 导出。虚拟服务器主机名。
-hostport	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器端口号。

选项	说明
-hostusername	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器主机的用户名。
-hostpassword	仅适用于 ESXi 和 Hyper-V 虚拟导出。虚拟服务器主机的密码。
-diskprovisioning	仅适用于 ESXi 导出。可选。您要在虚拟机上分配的磁盘空间容量。使用以下两种规格之一： - 完整 - 此规格使虚拟磁盘与受保护机器上的原始驱动器一样大。 - 精简 - 此规格分配在原始驱动器上占用的实际磁盘空间容量再加上额外的几 MB。 默认规格为“精简”。
-diskmapping	仅适用于 ESXi 导出。可选。此选项确定如何将受保护机器中的磁盘映射到虚拟机。使用以下值之一： - 自动 - 此值自动映射磁盘。 - 手动 - 此值可让您手动映射磁盘。 - 使用 VM - 此值将虚拟磁盘存储在您选择的数据存储中。 默认值为“自动”。
-targetpath	仅适用于 VMware Workstation 或 VirtualBox 导出。此选项指定您要存储虚拟机文件的文件夹的本地或网络路径（或 Linux 路径，仅限于 VirtualBox）。
-pathusername	仅适用于 VMware Workstation 导出。它是网络机器的用户名。仅当您在 -targetpath 选项中指定网络路径时需要。
-pathpassword	仅适用于 VMware Workstation 导出。它是网络机器的密码。仅当您在 -targetpath 选项中指定网络路径时需要。
-uselocalmachine	仅适用于 Hyper-V 导出。可选。使用此命令连接到本地 Hyper-V 服务器。此选项忽略 -hostname、-hostport、-hostusername 和 -hostpassword 选项。
-edit	可选。此选项允许您编辑现有虚拟机。它会忽略 -exporttype 和 -initialexport 选项。
-initialexport	可选。此选项用于指定在配置了连续备用虚拟机后是否启动初始的按需虚拟机器导出。

示例：

设置 Virtual Standby 导出至 ESXi 虚拟机以及源受保护服务器的名称、RAM 容量以及磁盘大小。

```
>cmdutil /virtualstandby -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@#
$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -
hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

设置 Virtual Standby 导出至本地驱动器上的 VMWare Workstation 机器文件：

```
>cmdutil /virtualstandby -exporttype vm -core 10.10.10.10 -user administrator -password 23WE@#
$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```

设置 Virtual Standby 导出至 Hyper-V 机器文件，并将其存储在远程机器上：

```
>cmdutil /virtualstandby -exporttype hyperv -core 10.10.10.10 -user adminstrator -password
23WE@#$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -vmlocation \\WIN7-Bobby
\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword
12QWsdxc@# -ram 4096
```

本地化

在安装 Rapid Recovery Core 的同一台机器上运行时，Rapid Recovery Command Line Management 实用程序将根据为 Rapid Recovery Core 设置的语言显示其语言。在此版本中，支持的语言包括英文、中文（简体）、法语、韩语、德语、日语、葡萄牙语（巴西）和西班牙语。

如果 Rapid Recovery Command Line Management 实用程序安装在单独的机器上，则英文是唯一支持的语言。

Core Console 参考

本附录包括描述 Rapid Recovery Core Console 中所提供的多种功能和图标的参考表格。它可作为 [Dell Data Protection | Rapid Recovery User Guide](#)。（Dell Data Protection | Rapid Recovery 用户指南）的 Dell Data Protection | Rapid Recovery 章节的补充。

主题：

- [查看 Core Console 用户指南](#)
- [查看 Protected Machines（受保护机器）面板](#)

查看 Core Console 用户指南

Core Console 是主要的用户界面 (UI)，用户通过它与 Rapid Recovery 互动。登录到 Rapid Recovery Core Console 时，您将看到以下元素。

表. 214: 包括在 Core Console 中的 UI 元素

UI 元素	说明
品牌区	对于典型环境，Core Console 左上方带有完整的产品名称，包括 Dell 徽标。单击品牌区的任意位置会在网页浏览器上打开新的选项卡，其中显示支持网站上的产品说明文档。
按钮条	显示在品牌区右侧的按钮栏包含可从 Core Console 任何位置访问的按钮。这些按钮可启动向导以完成常见任务，如保护计算机；执行从恢复点的还原；创建、连接或导入存档；或从此源 Core 复制到目标 Core。 按钮栏中的每个按钮在表. 215: 按钮栏按钮和菜单 表中有进一步说明。
正在运行的任务计数	显示当前正在运行的作业数量。根据系统状态，此值是动态的。如果单击下拉菜单，则将显示当前正在运行的所有作业的状态摘要。针对任何作业单击 X ，即可选择取消该作业。
帮助下拉菜单	帮助 菜单包括以下选项： • 帮助。链接到产品帮助，可在独立浏览器窗口打开。 • 说明文件。链接到 Dell Support 网站上的 Rapid Recovery 技术说明文件。 • 支持。链接到 Dell Support 网站，可访问在线聊天、视频教程、Rapid Recovery 知识库文章、常见问题等。 • 快速启动指南。“快速启动指南”是配置和使用 Rapid Recovery 的建议任务的指引式流程。每次登录 Core Console 向导都将自动打开，除非您禁用此功能。您还可以从“帮助”菜单中打开快速入门指南。有关“快速启动指南”的更多信息，请参阅了解快速入门指南。 • 有关。打开“关于 Dell Data Protection Rapid Recovery Core”对话框，其中包括版本信息和软件介绍。
服务器日期和时间	运行 Rapid Recovery Core 服务的机器的当前时间显示在 Core Console 的右上方。将鼠标悬停在时间上时，服务器日期也会出现。该日期和时间由日志、计划和报告等事件系统记录。例如，应用保护计划时，将使用显示在 Core Console 上的时间。即使数据库服务器或运行浏览器的客户端机器上的时区不同亦如此。
图标栏	图标栏包括 Core Console 中可访问的主要功能的图形形式：它将显示在用户界面 (UI) 的左侧、品牌区域的正下方。在图标栏中单击相应的项目可转到 UI 的相应部分，以便管理功能。 图标栏中的每个图标在表. 216: 图标栏 表中有进一步说明。
左侧导航区	左侧导航区域显示在用户界面左侧、图标栏的下方。

- 左侧导航区域包含文本筛选器和“受保护机器”菜单。
- 如果您已添加复制到该 Core，则该区域将包含“复制机器”菜单。
- 如果有移除保护的机器，但存储了恢复点，则该区域包含“仅限恢复点”菜单。
- 如果添加任何自定义组，则该区域包含“自定义组”菜单。
- 如果您已附加存档，则此区域包含已附加存档的菜单。

您可以切换左侧导航区。如果需要在 UI 主导航区中查看更多内容，此功能将非常有用。要隐藏此部分，单击左侧导航和主导航区之间的灰色边框。要再次显示 UI 元素，请再次单击灰色边框。

左侧导航区域中的每个元素在表. 218: 左侧导航区域和菜单表中有进一步说明。

上下文相关的
帮助



在 Rapid Recovery Core Console 中，每次单击“帮助”图标（蓝色问号）时，会打开一个浏览器窗口，其大小可调整，并带有两个框架。左侧的框架包含显示“Dell Rapid Recovery User Guide”（《Dell Rapid Recovery 用户指南》）上主题的导航树。右侧的框架显示选定帮助主题的内容。在任何给定的时间，帮助导航树展开，以显示在其选定主题层次结构中的位置。您可以使用上下文相关帮助功能浏览所有的“用户指南”主题。浏览主题完成后关闭浏览器。也可以从**帮助**菜单的**帮助**选项打开帮助。

按钮条

有关按钮栏的详细信息在下表中显示。

表. 215: 按钮栏按钮和菜单

UI 元素

说明

按钮栏：“保护”按钮和菜单



保护按钮可启动“保护计算机向导”，您可保护 Rapid Recovery Core 中的单台机器。此外，对于其他保护选项，您可以访问该按钮旁边的下拉菜单，其中包括以下选项。

- **保护机器**选项是启动“保护机器向导”以保护单台机器的另一种方法。
- **保护群集**选项允许连接到服务器群集。
- **保护多台机器**选项可打开“保护多台机器向导”，以便允许同时保护两台或多台机器。
- **部署 Agent 软件**选项可让您在一台或多台机器上同时安装 Rapid Recovery Agent 软件。此功能使用“部署 Agent 软件向导”。

按钮栏：“还原”按钮和菜单



还原按钮用以打开“还原机器向导”以允许从存储在受保护机器保护中的恢复点还原数据。另外，对于其他还原或导出选项，您可以访问此按钮旁边的下拉菜单，其中包括以下选项。

- **还原机器**选项是启动“还原机器向导”以还原数据的另一种方法。
- **安装恢复点**选项可启动“安装向导”，以便您安装来自受保护机器的恢复点。
- **VM 导出**选项用于打开“导出向导”。该向导可以从存储在 Rapid Recovery Core 中的恢复点创建虚拟机。您可以创建一次性导出，或者可以定义虚拟机参数，该虚拟机在每次受保护机器快照后会持续更新。

按钮栏：“存档”按钮和菜单



存档按钮可打开“存档向导”。使用该向导，您可从所选恢复点创建一次性存档，或者可以根据您定义的计划创建存档并持续保存至该存档。

此外，对于其他存档选项，您可以访问该按钮旁边的下拉菜单，其中包括以下选项。

- **创建存档**选项是启动“创建存档向导”来存档创建一次性存档或持续存档的另一种方法。
- **导入存档**选项可启动“导入存档向导”，可让您导入存档。
- **附加存档**选项可安装存档，以便您以文件系统形式读取内容。

UI 元素	说明
按钮栏：“复制”按钮	 复制按钮用以打开“复制向导”。使用该向导，您可指定目标 Core、选择源 Core 上受保护机器以及将所选机器上的恢复点复制到指定存储库中的目标 Core。 定义复制时，您可以暂停，也可以立即开始复制。 此外，您可以指定种子驱动器是否用于从现有恢复点复制数据到目标 Core。

图标栏

有关图标栏的详细信息在下表中显示。

表. 216: 图标栏

UI 元素	说明
图标栏	图标栏包括 Core Console 中可访问的主要功能的图形形式：单击相应的项目可转到用户界面的相应部分，可以管理功能。图标栏中的图标包括：
图标栏：“主页”图标	 主页。单击“主页”图标以导航到“Core 主页”页面。
图标栏：“复制”图标	 复制。单击“复制”图标以查看或管理传入或传出复制。
图标栏：“虚拟备用”图标	 Virtual Standby。单击 Virtual Standby 图标将信息从恢复点导出至可启动虚拟机。
图标栏：“事件”图标	 事件。单击“事件”图标以查看与 Rapid Recovery Core 关联的所有系统事件的日志。
图标栏：“设置”图标	 设置。单击“设置”图标以查看或管理 Rapid Recovery Core 的设置。您可以备份或还原 Core 配置设置。您可以设置一般设置以控制端口或显示方面。此外，您还可以在以下类别中配置设置：自动更新；每夜作业；传输队列设置；客户端超时设置；DVM 清除重复项缓存设置；Replay 引擎设置；部署设置。您可以查看或更改数据库连接；SMTP 服务器设置；云存储帐户；更改报告的字体设置。您可以设置 SQL 可附加性设置；Core 作业设置；许可证设置；SNMP 设置；vSphere 设置。
图标栏：“更多”图标	 更多。单击“更多”图标以访问其他重要功能。每个功能都有自己的图标，如下所列。
图标栏：“更多”图标	系统信息  系统信息。单击“系统信息”以显示 Rapid Recovery Core 服务器的数据。您可以查看主机名、操作系统、架构和 Core 内存。您可以查看 Core Console 上显示的名称。您也可以在网络上查看 Core 的完全限定域名，以及高速缓存元数据路径和重复高速缓存。 有关更改显示名称的更多信息，请参阅了解 Core 的系统信息。 有关清除重复项缓存的更多信息，请参阅了解清除重复项缓存大小和存储位置。 有关调整设置的信息，请参阅配置 DVM 清除重复项缓存设置。
图标栏：“更多”图标	存档  存档。Rapid Recovery 可让您管理 Core 中信息的存档。您可以查看有关计划或附加存档，也可以添加、检查或导入存档。

UI 元素	说明
图标栏：“更多” 图标	 安装。 可让您查看和拆卸本地安装以及查看和断开远程安装。
图标栏：“更多” 图标	 启动 CD。 可让您管理启动 CD，通常用于裸机还原 (BMR)。您可以创建启动 CD ISO 映像、删除现有映像；或者单击映像路径以打开和保存。
图标栏：“更多” 图标	 存储库。 可让您查看和管理与您 Core 关联的存储库。
图标栏：“更多” 图标	 加密密钥。 可让您查看、管理、导入或添加加密密钥，以便应用于受保护机器。如果未使用，则可以删除加密密钥。
图标栏：“更多” 图标	 云帐户。 可让您查看和管理 Core 和云存储帐户之间的连接。
图标栏：“更多” 图标	 保留策略。 可让您查看和修改 Core 的保留策略，其中包括将恢复点回滚并最终删除之前保留的时间。
图标栏：“更多” 图标	 通知。 可让您配置有关 Core 事件的通知、定义电子邮件通知的 SMTP 服务器设置以及设置减少重复以抑制相同事件的重复通知。
图标栏：“更多” 图标	 下载。 您可以下载 Agent 软件 Web 安装程序、Local Mount Utility 或包含用于 SNMP 浏览器中的事件信息的 MIB 文件。
图标栏：“更多” 图标	 报告。 可让您访问 Core 报告或计划报告以在正在进行基础上生成。
图标栏：“更多” 图标	 Core 日志。 可让您下载 Core 日志文件以供诊断使用。

左侧导航菜单

下表介绍了可能显示在左侧导航区域中的整套菜单：

表. 217: 左侧导航菜单选项

UI 元素	说明
受保护机器菜单	如果 Core 中保护了一个或多个机器，则“受保护机器”菜单显示为左侧导航区域中的第一个菜单。 如果您单击此窗格中显示的特定机器名称，将显示“摘要”页面，其中显示了所选机器的摘要信息。有关可以在“摘要”页面上完成内容的更多信息，请参阅查看受保护机器的摘要信息。
复制机器菜单	如果您看到另一个 Rapid Recovery Core 的名称显示为顶层导航菜单，则您正在其上查看 Core Console 的 Core 是目标 Core。该菜单的名称排在源 Core 后面，其下列出的每个机器都代表一个来自该源 Core、在此目标 Core 上复制的机器。 如果此目标 Core 从多个源 Core 复制恢复点，则每个源 Core 都会在左侧导航区域中显示为其自己的可导航菜单。 如果您单击被复制的机器菜单中显示的特定机器名称，将显示“摘要”页面，其中显示了所选被复制的机器的摘要信息。 有关复制的更多信息，请参阅复制。

UI 元素	说明
仅恢复点菜单	如果您看到“仅有恢复点”菜单，您的 Core 会保留它曾经保护或复制的机器的恢复点。尽管该机器不再继续捕获新的快照，之前在您的 Core 上捕获的恢复点仍将保留。这些恢复点可用于文件级别的恢复，但无法用于裸机还原，还原整个卷或添加快照数据。
自定义组菜单	如果您创建了任何自定义组，自定义组菜单将显示在导航菜单中。自定义组是用于汇聚机器（例如，按智能或组织，或者按地理位置）的逻辑容器。自定义组可以包含异型对象（受保护机器、复制机器等）。您可以定义自定义组的标签；和其他菜单类似，名称在菜单中以字母全部大写的形式显示。 您可以为自定义组中的项目执行操作，方法是单击自定义组标题右侧的箭头。例如，您可以强制为自定义组中的每个受保护机器创建快照。 有关创建和管理自定义组的更多信息，请参阅了解自定义组。
附加存档菜单	如果您将任何存档附加到您的 Core，左侧导航菜单中将列出每个存档。其标签是存档的名称。此列表中包括存档中包含的每个机器。

左侧导航区域中每个元素的详细信息在下表中显示。

表. 218: 左侧导航区域和菜单

UI 元素	说明
计算机菜单文本筛选器	 文本筛选器是一个文本字段，可让您筛选“受保护机器”、“复制的机器”和“仅有恢复点机器”菜单中显示的项目。如果在此筛选器中键入您的搜索条件，则只有符合搜索条件的机器显示在相应菜单中。
展开和压缩详细信息	 单击文本筛选器右侧的箭头以展开和压缩“受保护机器”、“复制的机器”和“仅有恢复点机器”菜单的详细信息。
受保护机器菜单	   “受保护机器”菜单将出现在 UI 左侧导航区。在该菜单中，您可以查看任何受保护机器、受保护群集，或配置在 Core 中的复制机器。如果您拥有受保护组或仅有恢复点机器，它们将显示为该菜单的一部分。通过单击该菜单标签左侧的箭头，您可以折叠或展开 Core 中任何受保护机器的视图。 显示的图标可描绘计算机类型： • 一个简单的机器图标描绘的是已安装 Rapid Recovery Agent 软件的物理机器或受保护虚拟机。 • 多机器图标描绘的则是受保护的群集。 • 中空的两个机器图标描绘的是使用无代理保护的 Vmware 虚拟机。 • 中空的三个机器图标图标描绘的是 VMware vCenter 主机。 如果单击“受保护机器”菜单，将显示“受保护机器”页面，并在该“受保护机器”窗格中显示该 Core 上的所有受保护机器。有关详情，请参阅查看“受保护机器”菜单。
复制机器菜单	如果从其他 Rapid Recovery Core 上复制的机器，则该 Core 的名称将作为单独的菜单显示在“受保护机器”菜单下方。从列出的源 Core 上复制到该目标 Core 上的每个计算机将显示在此菜单下。 对于每台复制的机器，其图标表示被复制的计算机的类型。例如，如果复制单台计算机，则图标显示一台计算机。如果复制服务器群集，则图标显示一个群集。 通过单击此菜单标签左侧的箭头，您可以折叠或展开任何复制的机器的视图。 在“复制机器”菜单中，您可以在所有复制机器上执行操作。 如果您单击“复制的机器”菜单，将显示“机器”页面。此页面列出了另一（源）Core 上复制到此目标 Core 的受保护机器的数量。有关详情，请参阅从导航菜单查看被复制的机器。

UI 元素	说明
仅恢复点菜单	如果之前受 Core 保护的机器移除保护，但恢复点不删除，则将显示“仅限恢复点”菜单。每台具有保留恢复点的之前受保护机器将显示在此列表中。 通过单击此菜单标签左侧的箭头，您可以折叠或展开任何仅有恢复点机器的视图。 在“仅限恢复点”菜单中，您可以删除该 Core 上所有“仅限恢复点”机器的恢复点。 如果单击“仅限恢复点”菜单，将显示“机器”页面，显示存储恢复点的机器。有关详情，请参阅查看“仅限恢复点”菜单。
自定义组菜单	如果 Core 包括任何自定义组，则左侧导航区包括“自定义组”菜单。该自定义组中的每个对象将显示在此列表中。 通过单击此菜单标签左侧的箭头，您可以折叠或展开 Core 中任何自定义组的视图。 在“自定义组”菜单中，可以执行组中类似项目的操作。 如果单击“自定义组”菜单，则将显示“计算机”页面，它显示组中显示的每个 Rapid Recovery 对象窗格：受保护机器、复制的机器和仅有恢复点机器。有关更多信息，请参阅查看自定义群菜单。
已附加存档菜单	 如果您已连接任何存档到 Core，则左侧导航区域将包含每个已附加存档的菜单。存档中包含的每台受保护机器将显示在此列表中。菜单标签使用保存存档时指定的名称。 通过单击此菜单标签左侧的箭头，您可以折叠或展开已连接到 Core 的任何存档的视图。 在“已附加存档”菜单中，您可执行组中类似项目的操作。 如果单击“已附加存档”菜单，则将显示“机器”页面，它显示组中显示的 Rapid Recovery 对象窗格：受保护机器、复制的机器和仅有恢复点机器。有关更多信息，请参阅查看自定义群菜单。

查看 Protected Machines（受保护机器）面板

Protected Machines（受保护机器）面板包含此 Rapid RecoveryCore 中所有受保护机器的相关信息。对于每个受保护的机器（如果已保护任何机器），您将看到网格中列出以下表格中所述信息。

表. 219: 每个受保护机器的相关信息

UI 元素	说明
选择项目	对于摘要表格中的每行，您可选中复选框，以通过表格上方的菜单选项列表中执行操作。
类型	显示机器类型。
状态指示灯	Status（状态）列中的彩色圆圈显示机器处于联机状态还是无法通信。如果您将指针悬停在彩色圆圈的上方，会显示状态条件。状态条件包括绿色（联机并受保护）、黄色（暂停保护）、红色（授权错误）和灰色（脱机或无法通信）。
Encryption status（加密状态）	锁定图标表示所选受保护机器的加密状态。打开的锁表示没有加密；闭合的锁表示已建立加密密钥。要了解加密的更多信息，请参阅 了解加密密钥 。
Display name（显示名称）	受保护机器的显示名称。
最后一个快照	列出此机器最后一次备份传输的日期和时间。
Repository Name（存储库名称）	列出存储此机器的数据的存储库。
Recovery Points（恢复点）	列出恢复点的数量，以及它们在存储库中占用多少空间。

UI 元素	说明
Version（版本）	机器中所加载的 Rapid Recovery Agent 软件的版本。
操作	当您单击该列中 Settings（设置）下拉菜单时，会显示可特别在所选受保护机器上执行的一组操作。

如果此 Core 中任何受保护机器被配置为虚拟待机，则会显示以下表格中所述的额外信息。

表. 220: 针对虚拟待机配置的受保护机器的相关信息

UI 元素	说明
上次导出	上次虚拟导出的日期和时间。
目标	将受保护机器保存为虚拟机的目标。例如 ESXi、VMware Workstation、Hyper-V 或 VirtualBox。
状态	为虚拟待机配置的机器的状态。状态条件包括“In Sync（同步中）”、“Paused（已暂停）”和“Not enabled（未启用）”。

从 Protected Machines（受保护机器）面板的 Actions（操作）下拉菜单中，您可执行下表中所述的操作。部分操作仅针对 Exchange server 或 SQL server 显示，标有

表. 221: Protected Machines（受保护机器）面板中可用的操作

UI 元素	说明
Force Snapshot（强制快照）	您可强制为所选受保护机器上的所有受保护卷生成增量快照或基础快照。要了解更多信息，请参阅 强制创建快照 。
One-time Export（一次性导出）	启动 Virtual Machine Export Wizard（虚拟机导出向导）。您可通过该向导，以任意受支持的 VM 格式，执行恢复点数据从受保护机器到虚拟机的一次性导出。要了解更多信息，请参阅 VM 导出 。
Virtual Standby（虚拟待机）	启动 Virtual Machine Export Wizard（虚拟机导出向导）。您可通过该向导，以任意受支持的 VM 格式，执行虚拟机待机恢复点数据从受保护机器到虚拟机的持续导出。要了解更多信息，请参阅 VM 导出 。
Mount（装载）	启动 Mount Wizard（安装向导）。您可通过该向导通过所选受保护机器安装恢复点。
Recovery Points（恢复点）	打开 Recovery Points Summary（恢复点摘要）页面。
还原	启动 Restore Machine Wizard（恢复机器向导）。您可通过此流程从 Core 中恢复点恢复数据至受保护的机器。要了解更多信息，请参阅 关于从恢复点还原卷 。
Remove Machine（移除机器）	从 Rapid Recovery Core 的保护中移除所选机器，您可选择删除或保留 Rapid Recovery Core 中已有的恢复点。要了解更多信息，请参阅 移除机器 。

您可在受保护机器网格中列出的两台或更多机器上执行操作。要在多台机器上执行操作，请选择每台受保护机器的复选框。然后，从摘要表格上方的菜单中，您可执行下表所述的任意操作。

表. 222: 选择机器后，Protected Machines（受保护机器）窗格中提供额外操作

UI 元素	说明
Force Snapshot（强制快照）	您可强制为所选受保护机器上的所有受保护卷生成增量快照。要了解更多信息，请参阅 强制创建快照 。
Force Base Image（强制基本映像）	您可强制为所选受保护机器上的所有受保护卷生成基本映像。要了解更多信息，请参阅 强制创建快照 。

UI 元素	说明
保护 > 暂停或恢复	您可暂停对所选机器提供保护（如果保护处于活动状态），也可恢复所选机器的保护（如果保护已暂停）。要了解更多信息，请参阅 暂停和恢复保护 。
复制	您可启用、强制、复制、暂停或恢复复制。您也可将现有恢复点复制到种子驱动器。要了解更多信息，请参阅 管理复制设置 。
取消	您可取消所选机器所有当前处于活动状态的操作，也可仅取消所选机器当前正在执行的快照。这不会影响将来计划的操作。
移除机器	从 Rapid Recovery Core 的保护中移除所选机器，您可选择删除或保留 Rapid Recovery Core 中已有的恢复点。要了解更多信息，请参阅 移除机器 。

从每个受保护机器的 Configuration（配置）下拉菜单中，您可执行下表中所述的操作。部分操作仅针对 Exchange server 或 SQL server 显示，如图所示。

表. 223: Protected Machines（受保护机器）面板中可用的操作

UI 元素	说明
Force Snapshot（强制快照）	您可强制为所选机器上的一个或多个卷生成增量快照或基本映像。要了解更多信息，请参阅 强制创建快照 。
强制 Exchange 日志截断	对于受保护的 Exchange Server 机器会强制截断 Exchange 日志，这可为 Exchange Server 腾出空间。要了解更多信息，请参阅 强制执行 SQL 机器日志截断 。
强制 SQL 日志截断	对于受保护的 SQL Server 机器会强制截断 SQL Server 日志，这可为 SQL Server 确定剩余空间。要了解更多信息，请参阅 强制执行 SQL 机器日志截断 。
导出	启动 Export Wizard（导出向导）。您可通过该向导将恢复点数据从受保护机器导出至任何受支持虚拟机格式的虚拟机。您可执行一次性导出或设置用于持续导出的虚拟待机。要了解更多信息，请参阅 VM 导出 。
Mount（装载）	打开 Mount Recovery Point（安装恢复点）对话框，您可通过该对话框浏览保存在 Rapid Recovery Core 中的快照数据，以安装特定恢复点。要了解更多信息，请分别参阅 安装恢复点 或 在 Linux 机器上安装恢复点卷 。
Recovery Points（恢复点）	打开所选代理机器的 Recovery Points（恢复点）选项卡。要了解更多信息，请参阅 管理快照和恢复点 。
还原	启动 Restore Machine Wizard（恢复机器向导）。您可通过此流程从 Core 中恢复点恢复数据至受保护的机器。要了解更多信息，请参阅 关于从恢复点还原卷 。
Remove Machine（移除机器）	从 Rapid Recovery Core 的保护中移除所选机器，您可选择删除或保留 Rapid Recovery Core 中已有的恢复点。要了解更多信息，请参阅 移除机器 。

查看受保护机器的事件

在**事件**页面上，您可以查看选定受保护机器上的已发生或正在进行的作业。页面顶部的按钮，可导航至三个类别活动中的作业列表：

- **任务。**为使操作成功，Rapid Recovery 必须执行的作业。
- **警报。**与任务或事件相关的包含错误和警告的通知。
- **日记。**所有受保护机器的任务和警报的组合。

下表包含**事件**页面上每个元素的介绍。

表. 224: “事件”页面元素

UI 元素	说明
搜索关键字	可在每一类中搜索指定项目。仅可用于任务。
发件人	为缩小结果范围，您可以输入开始搜索的日期。仅可用于任务。
收件人	为缩小结果范围，您可以输入停止搜索的日期。仅可用于任务。
状态图标	每个图标表示不同的作业状态。对于警报和任务，通过单击其中一个图标，您可按该状态筛选列表，本质上可生成报告。再次单击图标将移除筛选的状态。您可以通过多个状态进行筛选。状态包括： • 活动。正在进行的作业。 • 排队。一项作业开始前须等待另一作业完成。 • 正在等待。等待您批准或完成的作业，如种子驱动器。（有关种子驱动器的更多信息，请参阅复制。） • 完成。成功完成的作业。 • 失败。失败并未完成的作业。
服务图标	该按钮将服务作业添加到作业列表中。单击此图标时，每个状态图标上将显示一个较小的服务图标，可以让您筛选具有这些状态的服务作业（如果存在）。服务作业包括删除索引文件或移除机器保护。
导出类型下拉列表	下拉列表包含可以导出事件报告的格式。仅可用于任务。它包括以下格式： • PDF • HTML • CSV • XLS • XLSX
 （导出图标）	将事件报告导出到选择的格式。仅可用于任务。
页面选择	事件报告可以包括多个页面的多个作业。 事件 页面底部的数字和箭头可让您导航报告的其他页面。

事件页面显示表中的所有事件。下表列出了为每个项目显示的信息。

表. 225: “事件”摘要表的详细信息

UI 元素	说明
状态	显示任务、警报或日记项目的状态。可用于警报或日记项目，单击标题以按状态筛选结果。
名称	名称仅可用于任务。此文本字段列出了为这台受保护机器完成的作业类型。示例包括卷的传输、维护存储库、汇总、执行可安装性检查、执行校验和检查，等等。
开始时间	可用于任务、警报和日记项目。显示了作业或任务开始时的日期和时间。
结束时间	仅可用于任务。显示了任务完成时的日期和时间。
 作业详细信息	仅可用于任务。打开 监控活动任务 对话框，使得您可以查看特定作业或任务的详细信息。这些详细信息包括作业 ID、Core 传输数据的速率（如果相关）、作业完成经过时间、总工作量（以 GB 为单位）以及与作业关联的所有子任务。
Message（消息）	可用于警报和日记项目。此文本字段提供了警报或日记项目的描述性消息。

查看受保护机器的 More（更多）菜单

More（更多） 菜单提供额外选项，以帮助管理所选受保护的机器。要访问这些工具，请单击 More（更多）下拉菜单并选择下表所述任一选项。

表. 226: 受保护机器的 More（选项）中可用的工具

UI 元素	说明
	显示受保护机器的相关信息、系统信息、卷、处理器、网络适配器和该机器的 IP 地址。 有关更多信息，请参阅 查看受保护机器的系统信息 。
System Information （系统信息）	
	从 Local Mounts（本机装载）窗格中，您可查看或卸载装载在本机的卷。从 Remote Mounts（远程装载）窗格中，您可查看或卸载使用本机装载实用工具装载的卷。 要了解卸载卷的信息，请参阅 卸载恢复点 。
Mounts（装载）	要了解在本机装载恢复点的信息，请分别参阅 安装恢复点 或 在 Linux 机器上安装恢复点卷 。
	您可指定所选机器的保留策略。您可选择使用 Core 的默认策略，也可仅为此机器使用不同的保留策略。要了解更多信息，请参阅 自定义受保护机器的保留策略设置 。
Retention Policy（保留策略）	
	您可为与所选机器相关的事件指定自定义通知组。这不会更改已在 Core 中设置的通知。要了解更多信息，请参阅 配置通知组 。
通知	
	您可下载并查看使用 Rapid Recovery Agent 软件保护的机器的日志文件。要了解更多信息，请参阅 下载并查看受保护计算机的日志文件 。
Agent Log（代理日志）	

了解 Rapid Recovery PowerShell 模块

Dell Data Protection | Rapid Recovery 包含多个软件组件。与本主题相关的关键组件包括以下组件：

- Rapid Recovery Core 可管理受保护机器的验证、用于备份和复制目的的数据传输计划、导出至虚拟机、报告以及裸机还原 (BMR) 至类似或不同的硬件。
- Rapid Recovery Agent 负责创建卷快照以及将数据快速传输到 Core 管理的存储库。
- Rapid Recovery PowerShell 模块是一个 Windows 实用程序，可让用户通过使用 Windows PowerShell® 脚本与 Core 服务器进行交互。此模块提供了 Rapid Recovery Core Console 图形用户界面 (GUI) 所提供的部分功能。例如，Rapid Recovery PowerShell 模块可安装 Rapid Recovery 恢复点或强制创建受保护机器的快照。

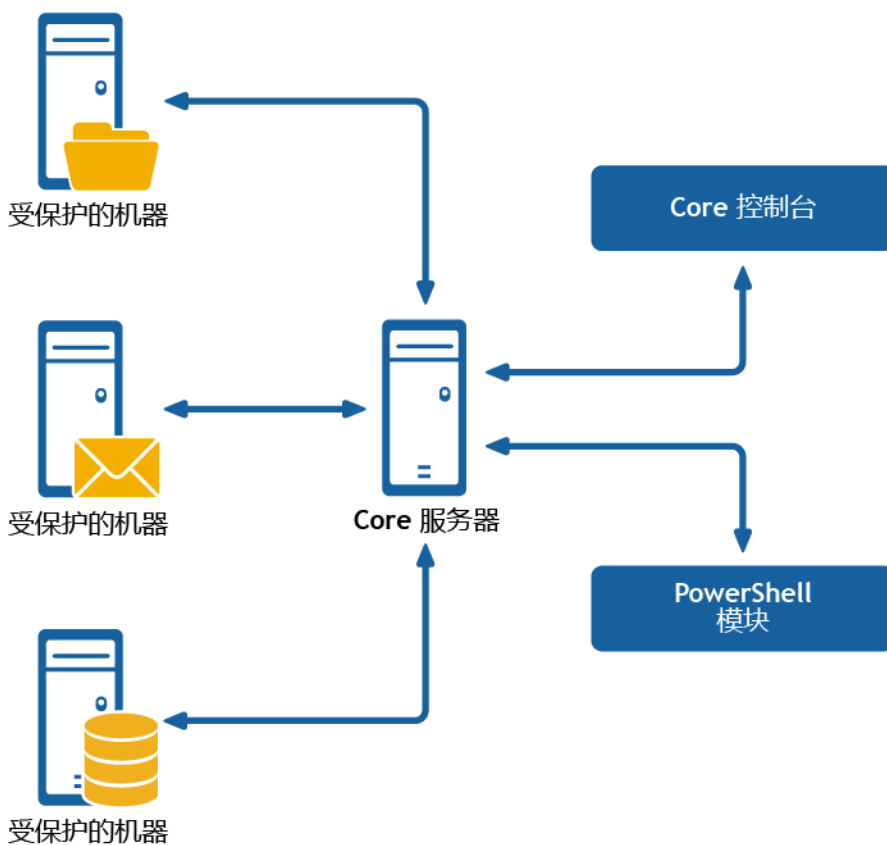


图 14: PowerShell 模块与 Rapid Recovery Core 交互

PowerShell 是一个与 Microsoft .NET Framework 相连的环境，旨在实现管理自动化。本节介绍了管理员在不与 Rapid Recovery Core GUI 进行交互的情况下可用于为某些功能编写脚本的 Rapid Recovery PowerShell 模块和 cmdlet。

① | 注：也可将 **PowerShell** 脚本作为前后脚本运行。有关更多信息和示例脚本，请参阅[使用脚本扩展 Rapid Recovery 作业](#)。

主题：

- 使用 PowerShell 的先决条件
- 使用命令和命令行工具

- Rapid Recovery PowerShell 模块 cmdlet
- 本地化
- 限定符

使用 PowerShell 的先决条件

使用 Rapid Recovery PowerShell 模块前，必须要安装有 Windows PowerShell 2.0 或更高版本。由于 PowerShell 3.0 中引入的新功能，包括更轻松的对象属性访问、PowerShell Web 访问及 REST 调用支持，Dell 建议使用 PowerShell 3.0 或更高版本。

① | 注: 请确保将 **powershell.exe.config** 文件置于 **PowerShell** 主目录下。例如，**C:\WindowsPowerShell\powershell.exe.config**

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0.30319"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

启动 PowerShell 并导入模块

与其他系统模块不同，默认情况下不会加载 Rapid Recovery PowerShell 模块。对于每个会话，可先用管理权限打开 Windows PowerShell，再导入模块。完成该过程中的步骤可启动 PowerShell 并导入 Rapid Recovery PowerShell 模块。

- 1 打开 Windows PowerShell 的提升的命令提示符。例如，在“开始”菜单中输入 Windows PowerShell，在随即打开的 Windows PowerShell 应用程序中，右击并选择**以管理员身份运行**。

Windows PowerShell 在一个新的命令窗口中打开。

- 2 输入以下命令，然后按 Enter 键：

```
Import-Module "RapidRecoveryPowerShellModule"
```

为当前对话导入 Rapid Recovery PowerShell 模块。可开始在已有的命令窗口中运行命令行工具。

使用命令和命令行工具

命令行工具是 Windows PowerShell 脚本中执行单个功能的指定命令。一个命令行工具通常表示为一组动名配对。命令行工具返回的结果是一个对象。

您可通过管道传输 PowerShell 命令，确保一个命令行工具的输出作为另一个命令行工具的输入。作为一个简单的例子，您可请求 Rapid Recovery PowerShell 模块中的命令列表并按名称为该列表排序。其示例脚本为：

```
Get-Command -module rapidrecoverypowershellmodule | sort-object name
```

获得命令行工具帮助和示例

一旦您已打开 PowerShell 并导入 Rapid Recovery PowerShell 模块，便可使用 Get-Help <command_name> cmdlet 随时请求其他信息。例如，要获得关于虚拟机导出命令行工具的信息，请输入以下命令行工具，然后按 Enter 键：

```
Get-Help Start-VMExport
```

返回的对象包括命令名称、概要、语法及任何可用于命令的选项。

获得某个特定 cmdlet 的帮助信息的另一种方式是键入命令名称，后跟 -?。例如：

```
Start-VMExport -?
```

您也可请求命令行工具示例，要执行的命令如下：

```
>Get-Help Start-VMExport -examples
```

Rapid Recovery PowerShell 模块 cmdlet

本节介绍 Rapid Recovery PowerShell 模块中可用的 cmdlet 和选项。Rapid Recovery PowerShell 模块中的所有 cmdlet 均支持以下常见参数：

- Verbose
- Debug（调试）
- ErrorAction
- ErrorVariable
- WarningAction
- WarningVariable
- OutBuffer
- OutVariable

有关详情，请使用 `Get-Help about_commonparameters`。

下表列出了可用的命令行工具。

表. 227: Rapid Recovery PowerShell 模块中的 cmdlet

命令行工具名称	说明
Edit-EsxiVirtualStandby	编辑现有 ESXi 虚拟备用配置。
Edit-HyperVVirtualStandby	编辑现有 Hyper-V 虚拟备用配置。
Edit-VBVirtualStandby	编辑现有 VirtualBox 虚拟备用配置。
Edit-VMVirtualStandby	编辑现有 VMware Workstation 虚拟备用配置。
Edit-ScheduledArchive	编辑现有计划存档配置。
Get-ActiveJobs	检索活动的作业集合。
Get-CloudAccounts	获取有关保存到 Core 的云帐户的信息。
Get-Clusters	检索受保护群集的集合。
Get-CompletedJobs	检索已完成的作业集合。
Get-ExchangeMailStores	检索 Exchange 邮件存储的集合。
Get-Failed	获取有关失败的恢复点的信息。
Get-FailedJobs	检索失败的作业集合。
Get-Mounts	显示所有已安装的恢复点。
Get-Passed	获取有关成功的恢复点的信息。
Get-ProtectedServers	获取有关受保护服务器的信息。

命令行工具名称	说明
Get-ProtectionGroups	检索保护组的集合。
Get-QueuedJobs	检索正在队列中等待的作业集合。
Get-RecoveryPoints	获取有关恢复点的信息。
Get-ReplicatedServers	获取有关复制的服务器的信息。
Get-Repositories	获取有关存储库的信息。
Get-ScheduledArchive	获取有关定期存档作业的信息。
Get-SqlDatabases	检索 SQL 数据库的集合。
Get-UnprotectedVolumes	检索未受保护卷的集合。
Get-VirtualizedServers	获取有关虚拟化服务器的信息。
Get-Volumes	获取有关卷的信息。
New-Base	强制创建基本映像快照。
New-CloudAccount	将新的云帐户添加至 Core。
New-EncryptionKey	创建新的加密密钥。
New-EsxiVirtualStandby	创建新的 ESXi 虚拟备用虚拟机。
New-HyperVVirtualStandby	创建新的 Hyper-V 虚拟备用虚拟机。
New-Mount	安装恢复点。
New-Replication	设置和强制复制。
New-Repository	创建新的 DVM 存储库。
New-ScheduledArchive	计划新的重复存档。
New-Snapshot	强制快照。
New-VBVirtualStandby	创建新的 VirtualBox 虚拟备用虚拟机。
New-VMVirtualStandby	创建新的 VMware Workstation 虚拟备用虚拟机。
Push-Replication	强制复制。
Push-Rollup	强制汇总。
Remove-Agent	从保护中移除机器。
Remove-Mount	卸载恢复点。
Remove-Mounts	卸载所有已安装的恢复点。
Remove-RecoveryPoints	删除受保护机器的恢复点。
Remove-Repository	删除现有 DVM 存储库。
Remove-ScheduledArchive	中断计划存档。
Remove-VirtualStandby	从 Core 移除虚拟备用虚拟机。
Resume-Replication	恢复复制。

命令行工具名称	说明
Resume-RepositoryActivity	恢复存储库活动。
Resume-ScheduledArchive	恢复计划存档。
Resume-Snapshot	恢复快照。
Resume-VirtualStandby	恢复导出数据到虚拟备用虚拟机。
Start-Archive	存档恢复点。
Start-AttachabilityCheck	对受保护的 MS SQL 数据库强制执行可附加性检查。
Start-ChecksumCheck	对受保护的 Exchange 邮件存储强制执行校验和检查。
Start-EsxiExport	强制导出到 ESXi 服务器。
Start-HypervExport	强制导出到 Hyper-V 服务器。
Start-LogTruncation	强制执行日志截断。
Start-MountabilityCheck	对受保护的 Exchange 邮件存储强制执行可安装性检查。
Start-Protect	保护服务器。
Start-ProtectCluster	保护群集。
Start-RepositoryCheck	强制 DVM 存储库检查。
Start-RestoreArchive	用恢复点还原存档。
Start-ScheduledArchive	强制计划存档的数据传输。
Start-VBExport	强制导出到 VirtualBox 服务器。
Start-VirtualStandby	强制数据传输到现有虚拟备用虚拟机。
Start-VMExport	强制导出到 VMWare Workstation 工作站服务器。
Stop-ActiveJobs	取消活动的作业。
Suspend-Replication	暂停复制。
Suspend-RepositoryActivity	暂停存储库的活动。
Suspend-ScheduledArchive	暂停计划存档的数据传输。
Suspend-Snapshot	暂停快照。
Suspend-VirtualStandby	暂停数据传输到虚拟备用虚拟机。
Update-Repository	将盘区添加至 DVM 存储库。

Edit-EsxiVirtualStandby

Edit-EsxiVirtualStandby 命令可让您使用 PowerShell 更改到 ESXi 虚拟机 (VM) 的现有虚拟导出。

使用

此命令的使用如下：

```
Edit-EsxiVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-HostPassword <String>] [-DiskProvisioning <String>] [-DiskMapping <String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-ErrorAction<ActionPreference>] [-WarningAction<ActionPreference>] [-ErrorVariable String] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

命令选项

下表介绍 Edit-EsxiVirtualStandby 命令可用的选项：

表. 228: Edit-EsxiVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-all	显示所有作业，包括由 Core 和所有受保护的服务器所执行的作业。
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）； l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）； f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为： 'transfer'（数据传输）、'repository'（存储库维护）、 'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点导出）、'pushinstall'（部署代理程序）、'rollback'（从恢复点还原）、'rollup'（恢复点汇总）、'sqlattach'（代理程序可附加性检查）和 'mount'（安装存储库）。默认情况下，将返回指定类型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括： #d 或 DD（该处的 # 是表示以前到现在天数时间段的一个数字） #h 或 #H（该处的 # 是表示以前到现在时段的一个数字） “时间日期 1”、“时间日期 2”（要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围）。

示例:

列出本地 Core 上所有活动的作业:

```
>Get-activejobs -all
```

Edit-HyperVVirtualStandby

Edit-HyperVVirtualStandby 命令可让您使用 PowerShell 更改到 Hyper-V 虚拟机 (VM) 的现有虚拟导出。

使用

此命令的使用如下:

```
Edit-HyperVVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-HostPassword <String>] [-VMLocation <String>] [-UseLocalMachine] [-gen2] [-UseVhdx] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

命令选项

下表介绍 Edit-HyperVVirtualStandby 命令可用的选项:

表. 229: Edit-HyperVVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址 (含可选的端口号)。默认情况下, 将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名, 则还必须提供密码。 如果未提供此信息, 则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码, 则还必须提供登录。 如果未提供此信息, 则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业, 由 IP 地址指示。
-all	显示所有作业, 包括由 Core 和所有受保护的服务器所执行的作业。
-number	可选。确定要显示多少个记录。可用值为: all (显示所有工作); l[number] 或 [number] (提取 ## 个按执行和时间分类的最近的工作); f[number] (显示第一 ## 个按执行和时间分类的恢复作业)。默认情况下, 显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为: 'transfer' (数据传输)、'repository' (存储库维护)、'replication' (本地和远程复制)、'backup' (备份和还原)、'bootcdbuilder' (创建启动 CD)、'diagnostics' (上传日志)、'exchange' (Exchange Server 文件检查)、'export' (恢复点

选项	说明
	导出)、'pushinstall' (部署代理程序)、'rollback' (从恢复点还原)、'rollup' (恢复点汇总)、'sqlattach' (代理程序可附加性检查) 和 'mount' (安装存储库)。默认情况下, 将返回指定类型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括: #d 或 DD (该处的 # 是表示以前到现在天数时间段的一个数字) #h 或 #H (该处的 # 是表示以前到现在时段的一个数字) “时间日期 1”、“时间日期 2” (要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围)。

示例:

列出本地 Core 上所有活动的作业:

```
>Get-activejobs -all
```

Edit-ScheduledArchive

Edit-ScheduledArchive 命令可让您使用 PowerShell 更改现有计划存档。

使用

此命令的使用如下:

```
Edit-ScheduledArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -path
[location] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -scheduletype
[type] -dayofweek [name] -dayofmonth [number] -time [time] -initialpause -id [id]
```

命令选项

下表介绍 Edit-ScheduledArchive 命令可用的选项:

表. 230: Edit-ScheduledArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址 (含可选的端口号)。默认情况下, 将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名, 则还必须提供密码。 如果未提供此信息, 则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码, 则还必须提供登录。 如果未提供此信息, 则将使用已登录用户的凭据。
-protectedserver	具有您想要存档的恢复点的受保护机器。您可以指定以双引号括起并用逗号分隔的多个机器名称。

选项	说明
-all	所有受保护机器的存档恢复点。
-path	保存存档数据的路径。例如： - 本地机器: "d:\work\archive" - 网络路径: "\\servername\sharename" - 云帐户中的文件夹: "文件夹名称" 注: 对于本地和网络位置，符号数不能大于 100，对于云位置，符号数不能大于 150。
-cloudaccountname	可选。仅用于云存档。要在其中保存存档的云帐户的名称。
-cloudcontainer	可选。仅用于云存档。选择将保存存档的选定云帐户中的云容器名称。当您使用该选项时，您还应指定 "-cloudaccountname" 参数。
-recycleaction	循环操作的类型。通过使用以下四个值之一进行指定： "replacethiscore" - 覆盖任何与本 core 有关的预存在已存档数据，但保持其他 core 的数据不变。 "erasecompletely" - 在写入新存档之前，清除目录的所有已存档数据。 "incremental" - 允许添加恢复点到现有存档。它会将恢复点进行比较，以免复制已经在存档中存在的数 据。
-scheduletype	计划间隔的类型。通过使用以下四个值之一指定选项： "daily" - 用于每日自动创建的存档。 "weekly" - 用于每周自动创建的存档。您必须指定 "-dayofweek" 参数。 "monthly" - 用于每月自动创建的存档。您必须指定 "-dayofmonth" 参数。如果某个月没有指定的日期 - 例 如，"31" - 则该月中不会进行存档。 "lastdayofmonth" - 用于在每月最后一天自动创建存档。
-dayofweek	仅用于 "-scheduletype" 参数的 "weekly" 选项。在星期几自动创建存档（例如，"周一"）。
-dayofmonth	仅用于 "-scheduletype" 参数的 "monthly" 选项。自动创建存档的月中日期（例如，"15"）。
-time	您希望创建存档的某天的小时。
-initialpause	可选。如果您想在配置存档计划后初始时暂停存档，请指定此选项。
-id	要编辑的计划存档的标识符。

示例：

编辑本地 Core 上的计划存档：

```
>Edit-ScheduledArchive -protectedserver protectedserver1 -path d:\work\archive -
cloudaccountname cloud1 -cloudcontainer cloudarchives -recycleaction incremental -scheduletype
daily -time 12:00 AM -initialpause -i
d archiveid
```

Edit-VBVirtualStandby

Edit-VBVirtualStandby 命令可让您使用 PowerShell 更改到 VirtualBox 虚拟机 (VM) 的现有虚拟导出。

使用

此命令的使用如下：

```
Edit-VBVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-LinuxHostName <String>] [-HostPort <UInt32>] [-AccountUserName <String>] [-AccountPassword
<String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam]
[-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-
WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

命令选项

下表介绍 Edit-VBVirtualStandby 命令可用的选项：

表. 231: Edit-VBVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-all	显示所有作业，包括由 Core 和所有受保护的服务器所执行的作业。
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）；l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）；f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为：'transfer'（数据传输）、'repository'（存储库维护）、 'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点 导出）、'pushinstall'（部署代理程序）、'rollback'（从恢复点还原）、'rollup'（恢复点汇 总）、'sqlattach'（代理程序可附加性检查）和 'mount'（安装存储库）。默认情况下，将返回指定类 型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括： #d 或 DD（该处的 # 是表示以前到现在天数时间段的一个数字）

选项	说明
	#h 或 #H（该处的 # 是表示以前到现在时段的一个数字）
	“时间日期 1”、“时间日期 2”（要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围）。

示例：

列出本地 Core 上所有活动的作业：

```
>Get-activejobs -all
```

Edit-VMVirtualStandby

Edit-VMVirtualStandby 命令可让您使用 PowerShell 更改到 VMware 工作站虚拟机 (VM) 的现有虚拟导出。

使用

此命令的使用如下：

```
Edit-VMVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User
<String>] [-Core <String>]
[-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction
<ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer
<Int32>]
```

命令选项

下表介绍 Edit-VMVirtualStandby 命令可用的选项：

表. 232: Edit-VMVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-all	显示所有作业，包括由 Core 和所有受保护的服务器所执行的作业。
-number	可选。确定要显示多少个记录。可用值为：

选项	说明
	all（显示所有工作）；l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）；f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为：'transfer'（数据传输）、'repository'（存储库维护）、'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点导出）、'pushinstall'（部署代理程序）、'rollback'（从恢复点还原）、'rollup'（恢复点汇总）、'sqlattach'（代理程序可附加性检查）和 'mount'（安装存储库）。默认情况下，将返回指定类型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括： #d 或 DD（该处的 # 是表示以前到现在天数时间段的一个数字） #h 或 #H（该处的 # 是表示以前到现在时段的一个数字） “时间日期 1”、“时间日期 2”（要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围）。

示例：

列出本地 Core 上所有活动的作业：

```
>Get-ActiveJobs -all
```

Get-ActiveJobs

Get-ActiveJobs 命令可返回 Core 中所有活动的作业。-jobtype 参数可用于观测特定作业。

使用

此命令的使用如下：

```
Get-ActiveJobs -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -  
jobtype [type] -time [time]
```

命令选项

下表介绍 Get-ActiveJobs 命令可用的选项：

表. 233: Get-ActiveJobs 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-all	显示所有作业，包括由 Core 和所有受保护的服务器所执行的作业。
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）；l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）；f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为：'transfer'（数据传输）、'repository'（存储库维护）、'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点导出）、'pushinstall'（部署代理程序）、'rollback'（从恢复点还原）、'rollup'（恢复点汇总）、'sqlattach'（代理程序可附加性检查）和 'mount'（安装存储库）。默认情况下，将返回指定类型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括： #d 或 DD（该处的 # 是表示以前到现在天数时间段的一个数字） #h 或 #H（该处的 # 是表示以前到现在时段的一个数字） “时间日期 1”、“时间日期 2”（要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围）。

示例：

列出本地 Core 上所有活动的作业：

```
>Get-activejobs -all
```

Get-Clusters

Get-Clusters 命令可返回与 Core 中受保护的服务器群集有关的信息。

使用

此命令的使用如下：

```
Get-Clusters -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 Get-Clusters 命令可用的选项：

表. 234: Get-Clusters 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。

示例:

列出本地 Core 上受保护的服务器群集:

```
>Get-Clusters
```

Get-CompletedJobs

Get-CompletedJobs 命令可返回在 Core 上完成的作业列表。-jobtype 参数可用于观测特定作业。

使用

此命令的使用如下:

```
Get-CompletedJobs -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -  
jobtype [type] -time [time]
```

命令选项

下表介绍 Get-CompletedJobs 命令可用的选项:

表. 235: Get-CompletedJobs 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-all	显示所有作业，包括由 Core 和所有受保护的服务器所执行的作业。
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）；l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）；f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为：'transfer'（数据传输）、'repository'（存储库维护）、'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点导出）、'pushinstall'（部署代理程序）、'rollback'（从恢复点还原）、'rollup'（恢复点汇总）、'sqlattach'（代理程序可附加性检查）和 'mount'（安装存储库）。默认情况下，将返回指定类型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括： #d 或 DD（该处的 # 是表示以前到现在天数时间段的一个数字） #h 或 #H（该处的 # 是表示以前到现在时段的一个数字） “时间日期 1”、“时间日期 2”（要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围）。

示例：

列出本地 Core 上所有活动的作业：

```
>Get-CompletedJobs -all
```

列出本地 Core 上所有已完成的创建存储库作业：

```
>Get-CompletedJobs -jobtype repository
```

Get-ExchangeMailStores

Get-ExchangeMailStores 命令可返回与受 Core 保护的 Exchange Server 上的邮件存储有关的信息。

使用

此命令的使用如下：

```
Get-ExchangeMailStores -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

命令选项

下表介绍 Get-ExchangeMailStores 命令可用的选项：

表. 236: Get-ExchangeMailStores 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。

示例：

为本地 Core 的 Exchange 服务器列出 Exchange 邮件存储：

```
>Get-ExchangeMailStores -protectedserver 10.10.10.10
```

Get-Failed

Get-Failed 命令可返回与本地 Core 上失败的恢复点有关的信息。

使用

此命令的使用如下：

```
Get-Failed -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

命令选项

下表介绍 Get-Failed 命令可用的选项：

表. 237: Get-Failed 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。

选项	说明
	如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）；l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）；f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。

示例：

列出所有失败的恢复点：

```
>Get-failed -protectedserver 10.10.10.10
```

Get-FailedJobs

Get-FailedJobs 命令可返回本地 Core 中所有失败的作业。

使用

此命令的使用如下：

```
Get-FailedJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -
jobtype [type] -time [time]
```

命令选项

下表介绍 Get-FailedJobs 命令可用的选项：

表. 238: Get-FailedJobs 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-all	显示所有作业，包括由 Core 和所有受保护的服务器所执行的作业。

选项	说明
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）；l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）；f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为：'transfer'（数据传输）、'repository'（存储库维护）、'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点导出）、'pushinstall'（部署代理程序）、'rollback'（从恢复点还原）、'rollup'（恢复点汇总）、'sqlattach'（代理程序可附加性检查）和 'mount'（安装存储库）。默认情况下，将返回指定类型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括： #d 或 DD（该处的 # 是表示以前到现在天数时间段的一个数字） #h 或 #H（该处的 # 是表示以前到现在时段的一个数字） “时间日期 1”、“时间日期 2”（要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围）。

示例：

列出本地 Core 上所有失败的作业：

```
>Get-FailedJobs -all
```

列出本地 Core 上所有失败的创建备份作业：

```
>Get-FailedJobs -type backup
```

Get-Mounts

Get-Mounts 命令可返回本地 Core 上安装的所有恢复点。

使用

此命令的使用如下：

```
Get-Mounts -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address]
```

命令选项

下表介绍 Get-Mounts 命令可用的选项：

表. 239: Get-Mounts 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。

示例：

显示所有已安装的恢复点：

```
>Get-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22
```

Get-Passed

Get-Passed 命令可返回与已通过 Core 上的验证检查的恢复点有关的信息。

使用

此命令的使用如下：

```
Get-Passed -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

命令选项

下表介绍 Get-Passed 命令可用的选项：

表. 240: Get-Passed 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。

示例:

列出通过验证检查的本地 Core 上所有恢复点:

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

Get-ProtectedServers 命令可返回与本地 Core 上的受保护机器有关的信息。

使用

此命令的使用如下:

```
Get-ProtectedServers -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 Get-ProtectedServers 命令可用的选项:

表. 241: Get-ProtectedServers 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址 (含可选的端口号)。默认情况下, 将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名, 则还必须提供密码。 如果未提供此信息, 则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码, 则还必须提供登录。 如果未提供此信息, 则将使用已登录用户的凭据。

示例:

列出本地 Core 上所有当前受保护的机器:

```
>Get-ProtectedServers
```

Get-ProtectionGroups

Get-ProtectionGroups 命令可返回与本地 Core 上的保护组有关的信息。

使用

此命令的使用如下：

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address]
```

命令选项

下表介绍 Get-ProtectionGroups 命令可用的选项：

表. 242: Get-ProtectionGroups 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。

示例：

列出本地 Core 上的保护组：

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-QueuedJobs

Get-QueuedJobs 命令可从 Core 返回所有正在等待开始的作业。

使用

此命令的使用如下：

```
Get-QueuedJobs -core [host name] -user [login] -password [password] -all | -protectedserver  
[name | IP address] -number [all | f[number] | l[number] | number] -jobtype [type] -time [time]
```

命令选项

下表介绍 Get-ActiveJobs 命令可用的选项：

表. 243: Get-ActiveJobs 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-all	显示所有作业，包括由 Core 和所有受保护的服务器所执行的作业。
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）；l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）；f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。
-jobtype	可选。指定作业类型筛选器。可用值为：'transfer'（数据传输）、'repository'（存储库维护）、'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点导出）、'pushinstall'（部署代理程序）、'rollback'（从恢复点还原）、'rollup'（恢复点汇总）、'sqlattach'（代理程序可附加性检查）和 'mount'（安装存储库）。默认情况下，将返回指定类型的所有作业。
-time	可选。按开始作业的日期和时间筛选输出。输入的可用类型包括： #d 或 DD（该处的 # 是表示以前到现在天数时间段的一个数字） #h 或 #H（该处的 # 是表示以前到现在时段的一个数字） “时间日期 1”、“时间日期 2”（要显示从逗号前出现的指定日期到逗号后的指定日期的自定义时间范围）。

示例：

列出本地 Core 上的所有已排入队列的作业：

```
>Get-QueuedJobs -all
```

Get-RecoveryPoints

Get-RecoveryPoints 命令可返回与本地 Core 上受保护机器的恢复点有关的信息。

使用

此命令的使用如下：

```
Get-RecoveryPoints -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

命令选项

下表介绍 Get-RecoveryPoints 命令可用的选项：

表. 244: Get-RecoveryPoints 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-number	可选。确定要显示多少个记录。可用值为： all（显示所有工作）； l[number] 或 [number]（提取 ## 个按执行和时间分类的最近的工作）； f[number]（显示第一 ## 个按执行和时间分类的恢复作业）。默认情况下，显示 20 个最近的作业。

示例：

列出本地 Core 上受保护机器的恢复点：

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

Get-ReplicatedServers 命令可返回与本地 Core 上复制的机器有关的信息。

使用

此命令的使用如下：

```
Get-ReplicatedServers -core [host name] -user [user name] -password [password]
```

使用命令返回值时，Dell 建议您考虑安全性。例如，此命令将返回每个复制的服务器的管理员密码。如果在来自目标 Core 的 MSP 环境中使用，这可能会暴露管理员用户的登录密码。对于具有加密存储库数据的环境，这不会造成实质的安全问题。

命令选项

下表介绍 Get-ReplicatedServers 命令可用的选项：

表. 245: Get-ReplicatedServers 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。

示例：

列出本地 Core 上所有复制的服务器：

```
>Get-ReplicatedServers
```

Get-Repositories

Get-Repositories 命令可返回与本地 Core 上的存储库有关的信息。

使用

此命令的使用如下：

```
Get-Repositories -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 Get-Repositories 命令可用的选项：

表. 246: Get-Repositories 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。

选项	说明
	如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。

示例:

列出本地 Core 上的存储库:

```
>Get-Repositories
```

Get-ScheduledArchives

Get-ScheduledArchives 命令可让您使用 PowerShell 查看与此 Core 关联的现有 Rapid Recovery 计划存档的相关信息。

使用

此命令的使用如下:

```
Get-ScheduledArchives -core [host name] -user [login] -password [password]
```

命令选项

下表介绍 Get-ScheduledArchives 命令可用的选项:

表. 247: Get-ScheduledArchives 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。

示例:

获得此 Core 上的计划存档的相关信息:

```
>Get-ScheduledArchives -core 10.10.10.10 -user administrator -password password
```

Get-SqlDatabases

Get-SqlDatabases 命令可返回来自指定受保护机器的 SQL 数据库列表。

使用

此命令的使用如下：

```
Get-SqlDatabases -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

命令选项

下表介绍 Get-SqlDatabases 命令可用的选项：

表. 248: Get-SqlDatabases 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。

示例：

列出本地 Core 上所有 SQL 数据库作业：

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-UnprotectedVolumes

Get-UnprotectedVolumes 命令可返回与 Core 上可保护但当前未受保护的卷有关的信息。

使用

此命令的使用如下：

```
Get-UnprotectedVolumes
-core [host name] -user [user name] -password [password] -protectedserver [server name or IP
address]
```

命令选项

下表介绍 Get-UnprotectedVolumes 命令可用的选项：

表. 249: Get-UnprotectedVolumes 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。

示例：

列出指定代理机器上用于保护（但未受保护）的所有卷：

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-VirtualizedServers

Get-VirtualizedServers 命令可返回有关虚拟化服务器的信息。

使用

此命令的使用如下：

```
Get-VirtualizedServers -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 Get-VirtualizedServers 命令可用的选项：

表. 250: Get-VirtualizedServers 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。

示例：

列出本地 Core 上所有虚拟化服务器：

```
>Get-VirtualizedServers
```

Get-Volumes

Get-Volumes 命令可返回与受 Core 保护的指定机器上的卷有关的信息。

使用

此命令的使用如下：

```
Get-Volumes -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

命令选项

下表介绍 Get-Volumes 命令可用的选项：

表. 251: Get-Volumes 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。

示例：

列出指定机器上的所有卷：

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-Base

New-Base 命令可强制创建新的基本映像，从而传输当前受保护机器的数据。强制创建基本映像时，传输将立即启动或添加到队列中。只会传输上个恢复点以来发生更改的数据。如果没有上个恢复点，则会传输受保护卷上的所有数据。

使用

此命令的使用如下：

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 New-Base 命令可用的选项：

表. 252: New-Base 命令选项

选项	说明
-?	显示此帮助消息。
-all	所有代理的基本映像。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	强制当前受保护机器的名称。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

示例：

强制创建所有受保护机器的基本映像：

```
>New-Base -all
```

New-CloudAccount

New-CloudAccount 命令可让您向 Rapid Recovery Core 添加新的云帐户。

使用

此命令的使用如下：

```
New-CloudAccount -core [host name] -user [login] -password [password] -displayname [display name] -type [cloud account type] -username [user name] - key [secret key] -region [region] - tenantid [tenant Id] - authurl [authorization url]
```

命令选项

下表介绍 New-CloudAccount 命令可用的选项：

表. 253: New-CloudAccount 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-displayname	要显示的云帐户的名称。
-type	要添加的云帐户的类型。支持的值包括： - amazon - openstack - rackspace - windowsazure "windows azure" - azure
-username	要添加的云帐户的用户名。它用于验证过程。此属性解析为“访问密钥”（对于 Amazon™ 云）、“用户名”（对于 Rackspace 和 OpenStack）以及“存储帐户名”（对于 Windows Azure 云帐户）。
-key	要添加的云帐户的密钥。它用于验证过程。此属性解析为“机密密钥”（对于 Amazon™ 云）、“Api 密钥”（对于 Rackspace 和 OpenStack）以及“访问密钥”（对于 Windows Azure 云帐户）。
-region	要添加的云帐户的地区。仅 RackSpace 和 OpenStack 云帐户创建需要此属性。

选项	说明
-tenantid	OpenStack 云帐户的验证过程中使用的标识符。仅 OpenStack 云帐户创建需要此选项。
-authurl	OpenStack 云帐户的验证过程中使用的 URL。仅 OpenStack 云帐户创建需要此选项。

示例：

创建名为“Amazon S3 Account”的新 Amazon™ S3 云帐户，其访问密钥为“akey”，机密密钥为“skey”。

```
>New-CloudAccount -displayname "Amazon S3 Account" -type Amazon -username akey -key skey
```

New-EncryptionKey

New-EncryptionKey 命令可让您创建新密钥以保护 Rapid Recovery 备份数据。

使用

此命令的使用如下：

```
New-EncryptionKey -core [host name] -user [login] -password [password] -name [encryption key
name] -passphrase [pas
sphrase] -comment [comment]
```

命令选项

下表介绍 New-EncryptionKey 命令可用的选项：

表. 254: New-EncryptionKey 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-name	要创建的加密密钥的名称。
-passphrase	要创建的加密密钥的密码。
-comment	可选。加密密钥的说明。

示例：

在本地 Core 上创建加密密钥：

```
>New-EncryptionKey -name EncryptionKey1 -passphrase 123456
```

New-EsxiVirtualStandby

New-EsxiVirtualStandby PowerShell 命令可让您使用 Rapid Recovery 创建新的 ESXi 虚拟备用机器。

使用

此命令的使用如下：

```
New-EsxiVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -initialexport
```

命令选项

下表介绍 New-EsxiVirtualStandby 命令可用的选项：

表. 255: New-EsxiVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-volumes	可选。列出要导出的卷名称。如果未指定，则将导出恢复点中的所有卷。必须使用双引号括起并用空格分隔值；例如： "c:", "d:"。  注：请勿在卷名称中使用尾部反斜杠。
-vmname	虚拟机 Microsoft Windows 名称。
-hostname	虚拟服务器主机的名称。
-hostport	与虚拟服务器通信时使用的端口号。

选项	说明
-hostusername	用于登录到虚拟服务器主机的用户名。
-hostpassword	用于登录到虚拟服务器主机的密码。
-ram	在虚拟服务器中分配特定容量的 RAM。
-usesourceram	可选。在虚拟服务器上分配与源受保护机器相同容量的 RAM。
-diskprovisioning	可选。要在虚拟机上分配的磁盘空间量。可用的值包括： - 完整 - 指定“完整”以使虚拟磁盘与受保护服务器上的原始驱动器一样大。 - 精简 - 指定“精简”以分配原始驱动器上占用的实际磁盘空间量外加额外的数 MB 空间。 默认磁盘配置为“精简”。
-diskmapping	可选。它决定了如何将磁盘从恢复点映射到虚拟机。可用的值包括： 'auto' 'manual' 'withvm' 默认设置为 'auto'。
-initialexport	可选。如果您需要在配置虚拟备用后启动初始按需虚拟机导出，请指定此选项。

示例：

创建新的 ESXi 虚拟备用机器：

```
>New-EsxiVirtualStandby -protectedserver 10.10.10.4 -vmname ExportedMachine -hostname 10.10.10.127 -hostport 443 -hostusername root -hostpassword pass123 -usesourceram -diskprovisioning thin -diskmapping auto
```

New-HyperVVirtualStandby

New-HyperVVirtualStandby PowerShell 命令可让您使用 Rapid Recovery 创建新的 Hyper-V 虚拟机 (VM)。

使用

此命令的使用如下：

```
New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host password] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

命令选项

下表介绍 New-HyperVVirtualStandby 命令可用的选项：

表. 256: New-HyperVVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-volumes	可选。列出要导出的卷名称。如果未指定，则将导出恢复点中的所有卷。必须使用双引号括起并用空格分隔值；例如："c:","d:"。 注: 请勿在卷名称中使用尾部反斜杠。
-vmname	虚拟机 Microsoft Windows 名称。
-gen2	可选。指定以使用第 2 代虚拟机。如果未指定，则使用第 1 代。从 Windows Server 2012 R2 到 Windows 8.1，Rapid Recovery 均支持第 2 代。
-usevhdx	可选。如果您指定此选项，Rapid Recovery 使用 VHDX 磁盘格式创建虚拟机。如果您未指定此选项，它使用 VHD 磁盘格式。第 2 代仅使用 VHDX 格式。
-uselocalmachine	可选。连接到本地 Hyper-V 服务器。当您指定此值时，Rapid Recovery 会忽略以下选项： • 主机名称 • hostport • hostusername • hostpassword
-hostname	虚拟服务器主机的名称。
-hostport	与虚拟服务器通信时使用的端口号。
-hostusername	用于登录到虚拟服务器主机的用户名。
-hostpassword	用于登录到虚拟服务器主机的密码。
-vmlocation	您要在其中存储虚拟机文件的文件夹的本地或网络路径。
-ram	在虚拟服务器中分配特定容量的 RAM。
-usesourceram	可选。在虚拟服务器上分配与源受保护机器相同容量的 RAM。
-initialexport	可选。如果您需要在配置虚拟备用后启动初始按需虚拟机导出，请指定此选项。

示例:

创建新的 Hyper-V 虚拟备用机器:

```
>New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual ho
    st name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host passwo
    rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

New-Mount

New-Mount 命令将安装一个或多个驱动器的快照。

使用

此命令的使用如下:

```
New-Mount -core [host name] -user [user name] -password [password] -protectedserver [machine
name] -mounttype [read | write | readonlywithpreviouswrites] -drives [drive names] -path
[location] -time [MM/DD/YYYY hh:mm:ss tt | passed | latest] -rpn [number]
```

命令选项

下表介绍 New-Mount 命令可用的选项:

表. 257: New-Mount 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-protectedserver	受保护服务器 IP 地址或机器名称（取决于特定机器受保护的方式）。
-time	可选。安装恢复点的时间戳。此时间戳应采用当前 PC 上操作系统指定的格式。管理员可以通过传递的参数值指定最近或最后检查的恢复点获取最新恢复点。默认情况下，将选择最晚时间选项。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。如果未提供此信息，则将使用已登录用户的凭据。
-path	Core 机器上恢复点将安装的路径。
-mounttype	可选。指定安装模式。可用选项包括 'read'、'readOnlyWithPreviousWrites'（只读带此前写入）、'write'（可写）。默认模式是 read-only。

选项	说明
-volumes	可选。空格分隔的要安装的卷名称列表。如果卷名称包含空格或特殊字符，则必须使用双引号进行指定。如果未指定，则将安装所有卷。
-drivers	可选。逗号分隔的要安装的卷名称列表。如果未指定，则将安装所有卷。 注: 此选项过时，使用 '-volumes' 代替。
-rpn	可选。安装的恢复点数量。您可以使用 get-mounts 命令获取此数量。为 rpn 参数指定多个数字以使用单个命令安装不同的点。 注: 如果设置安装大量点，则每个点将位于不同的子目录中。此名称说明恢复点的创建时间。调用卸载时，将删除所有子目录。您应手动删除父目录。

示例:

```
>New-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path C:\MountedRecoveryPoint -mounttype read -volumes c "d, ko"
```

安装大量恢复点:

```
>New-Mount -rpn 10 52 41 -protectedserver localhost -path "D:/Folder for mount"
```

安装特定创建时间的恢复点:

```
>New-Mount -protectedserver 10.10.5.56 -path "D:/Folder for mount" -time "8/24/2012 11:46 AM"
```

Resume-Replication

New-Replication 命令可让您为受保护的服务器设置和强制执行复制。

使用

此命令的使用如下:

```
New-Replication -core [host name] -user [login] -password [password] -targetserver [host name] -protectedserver [name | IP address]
```

命令选项

下表介绍 New-Replication 命令可用的选项:

表. 258: New-Replication 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-replicationname	目标 Core 上的复制配置的名称。
-targetserver	目标 Core 的主机名、用户名和密码。
-protectedserver	目标 Core 上用于设置复制的受保护机器和存储库的名称。

示例：

为 IP 为 10.10.10.4 的受保护机器创建新复制：

```
>New-Replication -targetserver 10.10.10.128 -protectedserver 10.10.10.4
```

New-Repository

New-Repository 命令可在 Rapid Recovery Core 中创建新的 DVM 存储库。指定的大小必须介于 250MB 和 16TB 之间。

使用

此命令的使用如下：

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath [location]
```

命令选项

下表介绍 New-Repository 命令可用的选项：

表. 259: New-Repository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-name	存储库名称。
-size	存储库盘区的大小。可用单位：b、Kb、Mb、Gb、Tb、Pb。
-datapath	仅适用于本地位置。确定存储库盘区的数据路径。
-metadatapath	仅适用于本地位置。确定存储库盘区的元数据路径。
-uncpath	仅适用于共享位置。确定存储库盘区的数据路径和元数据路径。

选项	说明
-shareusername	仅适用于共享位置。确定共享位置的登录。
-sharepassword	仅适用于共享位置。确定共享位置的密码。
-comment	可选。存储库的说明。
-concurrent Operations	可选。一次可处于挂起状态的操作的最大数量。默认值：64。

示例：

在本地驱动器 E: 内创建最小的新 DVM 存储库：

```
>New-Repository -name Repository2 -size 250Mb -datapath e:\Repository\Data -metadatapath e:\Repository\Metadata
```

New-ScheduledArchive

New-ScheduledArchive 命令可让您使用 PowerShell 更改现有计划存档。

使用

此命令的使用如下：

```
New-ScheduledArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address] -path [location] -archiveusername [name] -archivepassword [password] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -schdeuletype [type] -dayofweek [name] -dayofmonth [number] -time [time]
```

命令选项

下表介绍 New-ScheduledArchive 命令可用的选项：

表. 260: New-ScheduledArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	具有您想要存档的恢复点的受保护机器。您可以指定以双引号括起并用逗号分隔的多个机器名称。
-all	所有受保护机器的存档恢复点。

选项	说明
-path	保存存档数据的路径。例如： - 本地机器: "d:\work\archive" - 网络路径: "\\servername\sharename" - 云帐户中的文件夹: "文件夹名称" 注: 对于本地和网络位置，符号数不能大于 100，对于云位置，符号数不能大于 150。
-archiveusername	可选。用于登录远程机器的用户名。仅网络路径要求。
-archivepassword	可选。用于登录远程机器的密码。仅网络路径要求。
-cloudaccountname	可选。仅用于云存档。要在其中保存存档的云帐户的名称。
-cloudcontainer	可选。仅用于云存档。选择将保存存档的选定云帐户中的云容器名称。当您使用该选项时，您还应指定 "-cloudaccountname" 参数。
-recycleaction	循环操作的类型。通过使用以下四个值之一进行指定： "replacethiscore" - 覆盖任何与本 core 有关的预存在已存档数据，但保持其他 core 的数据不变。 "erasecompletely" - 在写入新存档之前，清除目录的所有已存档数据。 "incremental" - 允许添加恢复点到现有存档。它会将恢复点进行比较，以免复制已经在存档中存在的数
-schedulesype	计划间隔的类型。通过使用以下四个值之一指定选项： "daily" - 用于每日自动创建的存档。 "weekly" - 用于每周自动创建的存档。您必须指定 "-dayofweek" 参数。 "monthly" - 用于每月自动创建的存档。您必须指定 "-dayofmonth" 参数。如果某个月没有指定的日期 - 例如，"31" - 则该月中不会进行存档。 "lastdayofmonth" - 用于在每月最后一天自动创建存档。
-dayofweek	仅用于 "-schedulesype" 参数的 "weekly" 选项。在星期几自动创建存档（例如，"周一"）。
-dayofmonth	仅用于 "-schedulesype" 参数的 "monthly" 选项。自动创建存档的月中日期（例如，"15"）。
-time	您希望创建存档的某天的小时。
-initialpause	可选。如果您想在配置存档计划后初始时暂停存档，请指定此选项。

示例：

为 Core 上的所有机器存档创建日期始于 04/30/2012 02:55 PM 的所有恢复点，并替换与此 Core 相关的预先存在的已存档数据：

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path "d:\work\archive" -startdate "04/30/2012 02:55 PM" -all -recycleaction replacethiscore
```

为两个受保护机器存档一个日期范围以内的恢复点，清除目录中的所有已存档数据，然后再写入新存档：

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver "10.20.30.40" "20.20.10.1" -path "d:\work\archive" -startdate "04/30/2012 02:55 PM" -enddate "05/31/2012 11:00 AM" -recycleaction erasecompletely
```

对于 Core 上的所有机器，为创建日期始于 04/30/2012 02:55 PM 的所有恢复点创建增量存档并保存到具有名称 "Amazon S3" 和容器 "Container" 的云帐户中：

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path "ArchiveOnCloud" -cloudaccountname "Amazon S3" -cloudcontainer "Container" -startdate "04/30/2012 02:55 PM" -all -recycleaction incremental
```

New-Snapshot

New-Snapshot 命令可强制创建快照，从而传输当前受保护机器的数据。强制创建快照时，传输将立即启动或添加到队列中。只会传输上个恢复点以来发生更改的数据。如果没有上个恢复点，则会传输受保护卷上的所有数据。

使用

此命令的使用如下：

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 New-Snapshot 命令可用的选项：

表. 261: New-Snapshot 命令选项

选项	说明
-?	显示此帮助消息。
-all	强制所有受保护机器。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	强制当前受保护机器的名称。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

示例：

强制创建所有受保护机器的快照：

```
>New-Snapshot -all
```

New-VBVirtualStandby

New-VBVirtualStandby 命令可让您使用 PowerShell 创建一个到 VirtualBox 虚拟机 (VM) 的新虚拟导出。

使用

此命令的使用如下：

```
New-VBVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total megabytes] | -usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location] -pathusername [login] -pathpassword [password] -initialexport
```

命令选项

下表介绍 New-VBVirtualStandby 命令可用的选项：

表. 262: New-VBVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-volumes	可选。列出要导出的卷名称。如果未指定，则将导出恢复点中的所有卷。必须使用双引号括起并用空格分隔值；例如："c:", "d:"。  注：请勿在卷名称中使用尾部反斜杠。
-vmname	虚拟机 Microsoft Windows 名称。
-ram	在虚拟服务器中分配特定容量的 RAM。
-usesourceram	可选。在虚拟服务器上分配与源受保护机器相同容量的 RAM。
-linuxhostname	Linux VirtualBox 服务器主机名。
-hostport	Linux VirtualBox 服务器端口。
-targetpath	您要在其中存储虚拟机文件的文件夹的本地、网络或 Linux 路径。
-pathusername	用于登录网络机器的用户名。仅当您为目标路径指定网络位置时才需要。
-pathpassword	用于登录网络机器的密码。仅当您为目标路径指定网络位置时才需要。
-accountusername	可选。您可以指定用于注册导出的虚拟机的用户帐户。这是用于登录用户帐户的用户名。仅将此选项用于本地或网络机器。
-accountpassword	可选。您可以指定用于注册导出的虚拟机的用户帐户。这是用于登录用户帐户的密码。仅将此选项用于本地或网络机器。

选项	说明
-initialexport	可选。如果您需要在配置虚拟备用后启动初始按需虚拟机导出，请指定此选项。

示例：

在指定位置创建一个名为 ExportedMachine1 的 VirtualBox 虚拟备用机器：

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

New-VMVirtualStandby

New-VMVirtualStandby PowerShell 命令可让您使用 Rapid Recovery 创建新的 VMware Workstation 虚拟备用机器。

使用

此命令的使用如下：

```
New-VMVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total
megabytes] | -usesourceram] -targetpath [location] -pathusername [login] -pathpassword
[password] -initialexport
```

命令选项

下表介绍 New-VMVirtualStandby 命令可用的选项：

表. 263: New-VMVirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	为特定受保护机器显示作业，由 IP 地址指示。
-volumes	可选。列出要导出的卷名称。如果未指定，则将导出恢复点中的所有卷。必须使用双引号括起并用空格分隔值；例如："c:","d:"。 注： 请勿在卷名称中使用尾部反斜杠。
-vmname	虚拟机 Microsoft Windows 名称。
-ram	在虚拟服务器中分配特定容量的 RAM。

选项	说明
-usesourceram	可选。在虚拟服务器上分配与源受保护机器相同容量的 RAM。
-pathusername	用于登录网络机器的用户名。仅当您为目标路径指定网络位置时才需要。
-pathpassword	用于登录网络机器的密码。仅当您为目标路径指定网络位置时才需要。
-initialexport	可选。如果您需要在配置虚拟备用后启动初始按需虚拟机导出，请指定此选项。

示例：

创建新的 VMware Workstation 虚拟备用：

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

脚本将暂停，要求用户指定相应工作站的索引号。输入要完成的脚本的索引号（在这种情况下，索引号为 2）。示例继续：

```
2
Verify location ...
Virtual Standby successfully configured
PS C:\Users\Administrator>
```

Push-Replication

Push-Replication 命令可强制为一个或多个受保护机器执行复制。

使用

此命令的使用如下：

```
Push-Replication -core [host name] -user [user name] -password [password] -targetcore [host
name] -all | -protectedserver [machine name | IP address]
```

命令选项

下表介绍 Push-Replication 命令可用的选项：

表. 264: Push-Replication 命令选项

选项	说明
-?	显示此帮助消息。
-all	强制创建复制到目标 Core 的所有机器的复制。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	强制复制目标 Core 上的受保护机器名称。

选项	说明
-user	可选。远程 Core 主机的登录。如果您指定登录，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

示例：

推送单个受保护机器的复制：

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-targetcore 10.10.10.20:8006 -protectedserver 10.10.5.22
```

推送所有受保护机器的复制：

```
>Push-Replication -all
```

Push-Rollup

Push-Rollup 命令可强制为受保护机器执行汇总。

使用

此命令的使用如下：

```
Push-Rollup -core [host name] -user [user name] -password [password] -protectedserver [machine
name | IP address]
```

命令选项

下表介绍 Push-Rollup 命令可用的选项：

表. 265: Push-Rollup 命令选项

选项	说明
-?	显示此帮助消息。
-all	强制所有受保护机器。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	强制当前受保护机器的名称。
-user	可选。远程 Core 主机的登录。如果您指定登录，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

示例:

推送单个受保护机器的汇总:

```
>Push-Rollup -core 10.10.10.10:8006 -user administrator -password 23WE0#$sdd -protectedserver 10.10.5.22
```

推送所有受保护机器的汇总:

```
>Push-Rollup -all
```

Remove-Agent

Remove-Agent PowerShell 命令可让您从 Rapid Recovery Core 保护中删除机器。

使用

此命令的使用如下:

```
Remove-Agent -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -deleterecoverypoints -all
```

命令选项

下表介绍 Remove-MountAgent 命令可用的选项:

表. 266: Remove-Agent 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	卸载当前受保护机器的所有已安装恢复点。
-deleterecoverypoints	可选。删除此受保护机器的所有恢复点。
-all	可选。删除 Core 中的所有受保护机器。

示例:

卸载所有受保护机器及其恢复点:

```
>Remove-Agent -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -
deleterecoverypoints -all
```

Remove-Mount

Remove-Mount 命令将卸载 /Path 指定的已安装恢复点。使用 -protectedserver 参数卸载所选机器的点, 或使用 -all 参数卸载所有已安装恢复点的点。

使用

此命令的使用如下:

```
Remove-Mount -core [host name] -user [user name] -password [password] [-
protectedserver [machine name] | -path [mount path]]
```

命令选项

下表介绍 Remove-Mount 命令可用的选项:

表. 267: Remove-Mount 命令选项

选项	说明
-?	显示此帮助消息。
-all	卸载所有已安装的恢复点。
-core	可选。远程 Core 主机 IP 地址 (含可选的端口号)。默认情况下, 将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码, 则还必须提供登录。 如果未提供此信息, 则将使用已登录用户的凭据。
-path	卸载所选安装点。
-protectedserver	卸载当前受保护机器的所有已安装恢复点。
-user	可选。远程 Core 主机的用户名。如果您指定用户名, 则还必须提供密码。如果未提供此信息, 则将使用已登录用户的凭据。

示例:

卸载路径指定的恢复点:

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -path C:
\mountedRecoveryPoint
```

Remove-Mounts

Remove-Mounts 命令将卸载所有已安装的恢复点。

使用

此命令的使用如下：

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 Remove-Mounts 命令可用的选项：

表. 268: Remove-Mounts 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

示例：

卸载指定的 Core 上的所有恢复点：

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Remove-RecoveryPoints

Remove-RecoveryPoints PowerShell 命令可用于删除特定机器的恢复点。

使用

此命令的使用如下：

```
Remove-RecoveryPoints -core [host name] -user [login] -password [password] -[range | chain | all] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string | time interval specified by two time strings]
```

命令选项

下表介绍 Remove-RecoveryPoints 命令可用的选项：

表. 269: Remove-RecoveryPoints 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	卸载当前受保护机器的所有已安装恢复点。
-rpn	可选。仅用于链删除（带增量或孤立点的链的基本映像）。要删除的恢复点的序号（使用 Get-RecoveryPoints 命令以获取序号）。您可指定数个空格分隔的序号以单命令删除多个恢复点。
-time	使用此选项删除恢复点链。 可选。要删除单个恢复点，请按创建时间选择恢复点。以 "mm/dd/yyyy hh:mm tt" 格式指定确切的时间（例如，"2/24/2012 09:00 AM"）。务必指定计算机中所设置时区的日期和时间值。 必填。对于日期范围，请使用逗号和空格分隔的两个时间字符串来指定时间间隔，以便选择要删除的恢复点范围。
-range	可选。要按时间间隔删除的恢复点范围。
-chain	可选。带有按恢复点编号或恢复点创建时间选择的、要删除的顺序增量或一组顺序孤立点的基本映像。
-all	可选。删除 Core 中的所有受保护机器。

示例：

删除按日期指定的恢复点：

```
>Remove-RecoveryPoints -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -time "2/24/2012 09:00 AM"
```

Remove-Repository

Remove-Repository PowerShell 命令可从 Core 删除 Rapid Recovery 存储库及其内容。

使用

此命令的使用如下：

```
Remove-Repository -core [host name] -user [login] -password [password] -name [repository name] -all
```

命令选项

下表介绍 Remove-Repository 命令可用的选项：

表. 270: Remove-Repository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-name	要删除的存储库的名称。
-all	删除与此 Core 关联的所有存储库。

示例：

删除本地 Core 上的所有存储库：

```
>Remove-repository -all
```

Remove-ScheduledArchive

如果您计划让 Rapid Recovery 定期存档特定机器的恢复点，您可以使用 Remove-ScheduledArchive PowerShell 命令以从 Core 中删除该计划存档。

使用

此命令的使用如下：

```
Remove-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

命令选项

下表介绍 Remove-ScheduledArchive 命令可用的选项：

表. 271: Remove-ScheduledArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-all	删除与此 Core 关联的所有存档。
-id	要删除的存档的标识符。要列出多个存档，请使用空格分隔每个 ID。

示例：

从本地 Core 移除多个计划存档：

```
>Remove-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Remove-VirtualStandby

如果您计划让 Rapid Recovery 持续将数据导出至虚拟机，您可以使用 Remove-VirtualStandby PowerShell 命令以取消并删除此计划作业。

使用

此命令的使用如下：

```
Remove-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP ad  
dress]
```

命令选项

下表介绍 Remove-VirtualStandby 命令可用的选项：

表. 272: Remove-VirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-all	删除与此 Core 关联的所有虚拟待机作业。
-protectedserver	您要删除虚拟待机的受保护机器的名称或 IP 地址。

示例：

删除与此 Core 关联的所有虚拟待机作业：

```
>Remove-VirtualStandby -all
```

Resume-Replication

Resume-Replication 命令可让您恢复复制。有关更多详细信息，请参阅 [Suspend-Replication](#)。

使用

此命令的使用如下：

```
Resume-Replication -core [host name] -user [user name] -password [password] -all | -protectedserver [machine name | IP address] -incoming [host name] | -outgoing [host name]
```

命令选项

下表介绍 Resume-Replication 命令可用的选项：

表. 273: Resume-Replication 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-all	所有受保护的服务器。
-protectedserver	恢复指定机器的复制。
-incoming	复制到 Core 机器的远程 Core 的主机名。恢复远程 Core 上所有受保护机器的复制。
-outgoing	数据复制到的远程目标 Core 的主机名。恢复远程 Core 上所有受保护机器的复制。

示例：

通过指定使用的存储库，恢复本地 Core 上 IP 为 10.10.10.128 的受保护机器的复制：

```
>Resume-Replication replicationname Replication1 -targetserver 10.10.10.128,Administrator,123asdQ -protectedserver 10.10.10.4
```

```
# Repository
- -----
```

```
1 Repository A
2 Repository B
Please, input number of Repository from the list above or type 'exit' to exit:
```

脚本将暂停，要求用户指定相应存储库的索引号。输入要完成的脚本的索引号（在这种情况下，索引号为 2）。示例继续：

```
2
Replication job was started.
True
PS C:\Users\Administrator>
```

Resume-Snapshot

管理员可以恢复快照、导出到虚拟机及执行复制。有关更多详细信息，请参阅 [Start-VMExport](#)。

使用

此命令的使用如下：

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

命令选项

下表介绍 Resume-Snapshot 命令可用的选项：

表. 274: Resume-Snapshot 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-all	所有受保护的服务器。
-protectedserver	恢复创建指定机器的快照。

示例：

恢复本地 Core 上 IP 为 10.10.10.4 的受保护机器的快照：

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume-VirtualStandby

Resume-VirtualStandby PowerShell 命令可让您恢复暂挂的数据导出，以便继续导出到 Rapid Recovery 虚拟备用机器。

使用

此命令的使用如下：

```
Resume-VirtualStandby -core [host name] -user [login] -password [password] -all | -protectedserver [name(s) | IP address]
```

命令选项

下表介绍 Resume-VirtualStandby 命令可用的选项：

表. 275: Resume-VirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。

选项	说明
	如果未提供此信息，则将使用已登录用户的凭据。
-all	为所有虚拟备用机器恢复导出。
-protectedserver	带有您想恢复的虚拟备用机器的受保护机器的名称 - 以逗号和空格分隔。

示例：

为受保护机器恢复虚拟备用导出：

```
>Resume-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22
```

Resume-VMExport

Resume-VMExport 命令可使管理员导出到虚拟机。有关更多详情，请参阅 [Suspend-VMExport](#)。

使用

此命令的使用如下：

```
Resume-VMExport -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

命令选项

下表介绍 Resume-VMExport 命令可用的选项：

表. 276: Resume-VMExport 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-all	所有受保护的服务器。
-protectedserver	恢复创建指定机器的快照。

示例:

恢复本地 Core 上每个受保护机器的导出到虚拟机:

```
>Resume-VMExport -all
```

Start-Archive

企业通常使用长期存储来存档合规和非合规数据。Rapid Recovery 中的存档功能用于延长合规和非合规数据的保留期限。通过指定 / Path 命令和凭据, 管理员可以在本地存储位置或网络位置保存存档。

使用

此命令的使用如下:

```
Start-Archive -path -startdate -enddate [-all] | -protectedserver [machine name] or [IP]] -core [host name] -user [user name] -password [password]
```

命令选项

下表介绍 Start-Archive 命令可用的选项:

表. 277: Start-Archive 命令选项

选项	说明
-?	显示此帮助消息。
-path	位置路径。示例路径: 'D:\work\archive' 或网络路径: '\\servername\sharename'。
-all	存档 Core 上所有机器的恢复点。
-core	可选。远程 Core 主机 IP 地址 (含可选的端口号)。默认情况下, 将与安装在本地机器上的 Core 建立连接。
-startdate	已创建恢复点的日期范围的开始日期。应采用当前 PC 上 OS 指定的格式。
-enddate	日期范围的结束日期。默认为当前时间。
-password	可选。远程 Core 主机的密码。如果您指定密码, 则还必须提供用户名。如果未提供此信息, 则将使用已登录用户的凭据。
-protectedserver	存档指定机器的恢复点。
-user	可选。远程 Core 主机的用户名。如果您指定用户名, 则还必须提供密码。如果未提供此信息, 则将使用已登录用户的凭据。
-archiveusername	可选。仅网络路径需要。
-archivepassword	可选。仅网络路径需要。

选项	说明
-comment	可选。示例：-comment 'Before install new application'。

示例：

存档 Core 上所有机器的所有恢复点：

```
>Start-Archive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-AttachabilityChec

Start-AttachabilityCheck 命令对受 Core 保护的所有 SQL Server 数据库进行强制可附加性检查。

使用

此命令的使用如下：

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]
- protectedserver [machine name | IP address] -rpn [number | numbers] | -time [time string]
```

命令选项

下表介绍 Start-AttachabilityCheck 命令可用的选项：

表. 278: Start-AttachabilityCheck 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	对其执行 SQL 可附加性检查的受保护机器。
-rpn	可选。对其执行 SQL 可附加性检查的恢复点的序号。 您可使用 -GetRecoveryPoints 命令获得恢复点序号。您可指定多个空格分隔的序号以使用单个命令执行多个恢复点的检查。 📘 注： 如果该命令中未指定‘time’和‘rpn’选项，则最近的恢复点用于可附加性检查。
-time	可选。确定 SQL 可附加性检查要选择的恢复点。您需要使用格式“MM/DD/YYYY hh:mm tt”（例如，“04/24/2015 09:00 AM”）指定确切的时间。指定您的本地机器上设置的时区的日期时间值。 📘 注： 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。

示例:

对指定的受保护 SQL 服务器的最近恢复点执行 SQL 可附加性检查:

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start-ChecksumCheck

Start-ChecksumCheck PowerShell 命令可强制对 Exchange Server 恢复点进行校验和检查。

使用

此命令的使用如下:

```
Start-ChecksumCheck -core [host name] -user [login] -password [password] -protectedserver [name  
| IP address] -rpn [number | numbers] | -time [time string]
```

命令选项

下表介绍 Start-ChecksumCheck 命令可用的选项:

表. 279: Start-ChecksumCheck 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	受保护机器的名称。
-rpn	可选。仅用于链删除（带增量或孤立点的链的基本映像）。要检查的恢复点的序号（使用 Get-RecoveryPoints 命令以获取序号）。您可指定数个空格分隔的序号以单命令删除多个恢复点。
-time	可选。按创建时间（而不是序号）选择要检查的恢复点。以 "mm/dd/yyyy hh:mm tt" 格式指定确切的时间（例如，"2/24/2012 09:00 AM"）。务必指定计算机中所设置时区的日期和时间值。

示例:

在两个恢复点上开始校验和检查:

```
> Start-ChecksumCheck -core 10.10.10.10 -user administrator -password 23WE@#sdd -  
protectedserver 10.10.5.22 -rpn 5 7
```

Start-EsxiExport

Start-EsxiExport PowerShell 命令触发启动从选择的 Rapid Recovery 恢复点虚拟导出至 ESX(i) 服务器虚拟机。

必要参数包括含有要导出恢复点的受保护机器的名称；您将向其导出的虚拟机名称；将要在虚拟机上分配的 RAM 容量；主机名称和 Linux 服务器主机的端口以及将存储产生的虚拟机文件的本地、网络或 Linux 文件夹的路径。

使用

此命令的使用如下：

```
Start-EsxiExport -core [host name] -user [user name] -password [password] -protectedserver [machine name | IP address] -volumes [volume names] -rpn [number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm]
```

命令选项

下表介绍 Start-EsxiExport 命令可用的选项：

表. 280: Start-EsxiExport 命令选项

选项	说明
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要导出恢复点的受保护机器。
-volumes	可选。要导出的卷名称列表。如果未指定，则将导出指定恢复点中的所有卷。必须使用双引号引起并用空格分隔每个值。请勿在卷名称中使用尾部反斜杠。例如，指定“C:”而非“C:/”
-rpn	可选。要导出的恢复点序号。（您可使用 Get-RecoveryPoints 命令获得恢复点序号。 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-time	可选。确定导出将要选择的恢复点。您需要使用格式“MM/DD/YYYY hh:mm tt”（例如，“04/24/2015 09:00 AM”）指定确切的时间。指定您的本地机器上设置的时区的日期时间值。 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-vmname	虚拟机的 Windows 名称。
-hostname	虚拟服务器主机名。
-hostport	虚拟服务器端口号。

选项	说明
-hostusername	登录到虚拟服务器主机的用户名。
-hostpassword	虚拟服务器主机的密码。
-ram	在虚拟服务器中分配特定容量的 RAM。
-usesourceram	可选。在虚拟服务器中分配与源受保护机器相同容量的 RAM。
-diskprovisioning	可选。将在虚拟机上分配的磁盘空间容量。指定“密集”以使虚拟磁盘与受保护服务器上的原始驱动器一样大，或指定“精简”以分配在原始驱动器上占用的实际磁盘空间容量外加一些额外的容量 (MB)。默认情况下，选择“精简”配置。
-diskmapping	可选。选择‘auto’、‘manual’或‘withvm’。默认情况下，启用自动映射。
-resetup	可选。重新创建虚拟机（如果它已存在于指定位置）。
-datacenter	可选。指定要使用的数据中心。
-resourcepool	可选。指定要使用的资源池。
-datastore	可选。指定要使用的数据存储。
-computeresource	可选。指定要使用的计算资源。
-version	可选。指定要使用的 ESXi 版本。

Start-HypervExport

Start-HypervExport PowerShell 命令触发启动从选择的 Rapid Recovery 恢复点虚拟导出至 Hyper-V 服务器虚拟机。

使用

此命令的使用如下：

```
Start-HypervExport -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] | -time [time string] [-vmname [uselocalmachine] | -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] -hostpassword [virtual host password] -vmlocation [location]] [-ram [total megabytes] | -usesourceram] -diskformat [VHD | VHDX]
```

命令选项

下表介绍 Start-HypervExport 命令可用的选项：

表. 281: Start-HypervExport 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要导出恢复点的受保护机器。
-volumes	可选。要导出的卷名称列表。如果未指定，则将导出指定恢复点中的所有卷。必须使用双引号引起并用空格分隔每个值。请勿在卷名称中使用尾部反斜杠。例如，指定“C:”而非“C:/”
-rpn	可选。要导出的恢复点序号。（您可使用 Get-RecoveryPoints 命令获得恢复点序号。 ❗ 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-time	可选。确定导出将要选择的恢复点。您需要使用格式“MM/DD/YYYY hh:mm tt”（例如，“04/24/2015 09:00 AM”）指定确切的时间。指定您的本地机器上设置的时区的日期时间值。 ❗ 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-vmname	虚拟机的 Windows 名称。
-gen2	可选。指定以使用第 2 代虚拟机。如果未指定，则使用第 1 代。从 Windows Server 2012 R2 到 Windows 8.1, Rapid Recovery 均支持第 2 代。
-usevhdx	可选。如果您指定此选项，Rapid Recovery 使用 VHDX 磁盘格式创建虚拟机。如果您未指定此选项，它使用 VHD 磁盘格式。第 2 代仅使用 VHDX 格式。
-uselocalmachine	可选。连接本地 Hyper-V 服务器。如果使用该参数，则忽略以下选项：主机名、主机端口、主机用户名、主机密码。
-hostname	虚拟服务器主机名。
-hostport	虚拟服务器端口号。
-hostusername	登录到虚拟服务器主机的用户名。
-hostpassword	虚拟服务器主机的密码。
-vmlocation	您要在其中存储虚拟机文件的文件夹的本地或网络路径。
-ram	在虚拟服务器中分配特定容量的 RAM。
-usesourceram	可选。在虚拟服务器中分配与源受保护机器相同容量的 RAM。

Start-LogTruncation

Start-LogTruncation 命令强制执行指定受保护的 SQL Server 或 Microsoft Exchange Server 的日志截断。

使用

此命令的使用如下：

```
Start-LogTruncation -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -target [sql | exchange]
```

命令选项

下表介绍 Start-LogTruncation 命令可用的选项：

表. 282: Start-LogTruncation 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	存档指定机器的恢复点。
-target	指定日志截断类型（'sql'或'exchange'）。如果未指定，则在所有数据库上截断日志。

示例：

截断 SQL 日志：

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

截断 Exchange 服务器日志：Core 上所有机器的所有恢复点：

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

Start-MountabilityCheck 命令对受保护的 Microsoft Exchange 邮件存储强制执行可安装性检查。

使用

此命令的使用如下：

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -rpn [number | numbers] | -time [time string]
```

命令选项

下表介绍 Start-MountabilityCheck 命令可用的选项：

表. 283: Start-MountabilityCheck 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	存档指定机器的恢复点。
-rpn	可选。要导出的恢复点序号。（您可使用 -GetRecoveryPoints 命令获得恢复点序号。 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-time	可选。确定导出将要选择的恢复点。您需要使用格式“MM/DD/YYYY hh:mm tt”（例如，“04/24/2015 09:00 AM”）指定确切的时间。指定您的本地机器上设置的时区的日期时间值。 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。

示例:

对 Core 上所有机器的所有恢复点启动可安装性检查:

```
> Start-MountabilityCheck -protected EX01
```

Start-Protect

Start-Protect 命令可使管理员添加受 Core 保护的服务器。

使用

```
Start-Protect -core [host name] -user [user name] -password [password] -repository [repository name] -agent [name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -volumes [volume names]
```

命令选项

下表介绍 Start-Protect 命令可用的选项:

表. 284: Start-Protect 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-repository	存储受保护机器数据的 Core 上的存储库名称。
-agentname	受保护机器名称或 IP 地址。
-agentusername	登录受保护的服务器。
-agentpassword	受保护服务器的密码。
-agentport	受保护服务器端口号。
-volumes	保护的卷列表。必须使用双引号引起并用空格分隔值。请勿在卷名称中使用尾部反斜杠。例如，“c:”、“d:”。

示例：

保护服务器的卷：

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername administrator -agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

Start-ProtectCluster 命令可让管理员添加受 Core 保护的服务器群集。

使用

此命令的使用如下：

```
Start-ProtectCluster -core [host name] -user [user name] -password [password] -repository [repository name] -clustername [name | IP address] -clusterusername [user name for cluster] -clusterpassword [password for cluster] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes names and volumes]
```

命令选项

下表介绍 Start-ProtectCluster 命令可用的选项：

表. 285: Start-ProtectCluster 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。

选项	说明
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-repository	存储受保护机器数据的 Core 上的存储库名称。该名称必须使用双引号括起。
-clustername	要保护的群集名称。
-clusterusername	受保护群集的用户名。
-clusterpassword	受保护群集的密码。
-clusterport	受保护群集的端口号。
-clustervolumes	保护的卷列表。必须使用双引号引起并用空格分隔值。请勿在卷名称中使用尾部反斜杠。例如，“c:”、“d”。
-clusternodes	要保护的含卷的群集节点列表。首先指定标签“nodename”，接着输入节点名称。然后指定标签“volumes”，接着输入节点的卷列表。 例如：“nodename”，“10.10.10.10”，“volumes”，“c:”，“e:”，“nodename”，“10.10.10.11”，“volumes”，“c:”

示例：

保护服务器的卷：

```
>Start-ProtectCluster -repository "Repository 1" -clustername 10.10.9.120 -clusterusername administrator -clusterpassword 12345 -clusterport 5002 -clustervolumes "c:" "d:" -clusternodes nodename 10.10.10.10 volumes "c:" "e:"
```

Start-RepositoryCheck

Start-RepositoryCheck PowerShell 命令可检查存储库的完整性。

使用

此命令的使用如下：

```
Start-RepositoryCheck -name [repository name] | -all [check all repositories] -password [password] -force
```

命令选项

下表介绍 Start-RepositoryCheck 命令可用的选项：

表. 286: Start-RepositoryCheck 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。如果未提供此信息，则将使用已登录用户的凭据。
-repository	必填。要检查的存储库的名称。
-all	可选。检查与此 Core 关联的所有存储库。
-force	可选。在不确认的情况下执行存储库检查。

示例：

开始检查存储库：

```
>Start-RepositoryCheck -repository newRepository1 -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd
```

Start-RestoreArchive

企业通常使用长期存储来存档合规和非合规数据。Rapid Recovery 中的存档功能用于延长合规和非合规数据的保留期限。通过指定 -Path 命令和凭据，管理员可以在本地存储位置或网络位置保存存档。

使用

此命令的使用如下：

```
Start-RestoreArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -repository [name] -archiveusername [name] -archivepassword [password] -path [location] -cloudaccountname [name] -cloudcontainer [name]
```

命令选项

下表介绍 Start-RestoreArchive 命令可用的选项：

表. 287: Start-RestoreArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-all	所有受保护机器的存档恢复点。
-protectedserver	具有您想要存档的恢复点的受保护机器。您可以指定以双引号括起并用逗号分隔的多个机器名称。
-repository	您想要在其中放置还原的恢复点的存储库的名称。您必须用双引号将名称括起；例如，"Repository1"。
-archiveusername	可选。用于登录远程机器的用户名。仅网络路径要求。
-archivepassword	可选。用于登录远程机器的密码。仅网络路径要求。
-path	保存存档数据的路径。例如： - 本地机器：“d:\work\archive” - 网络路径：“\\servername\sharename” - 云帐户中的文件夹：“文件夹名称” ❗ 注：对于本地和网络位置，符号数不能大于 100，对于云位置，符号数不能大于 150。
-cloudaccountname	可选。仅用于云存档。要在其中保存存档的云帐户的名称。
-cloudcontainer	可选。仅用于云存档。选择将保存存档的选定云帐户中的云容器名称。当您使用该选项时，您还应指定“-cloudaccountname”参数。
-manifestcore	可选。指定您想要从已还原存档清单中使用的 Core。

示例：

存档 Core 上所有机器的所有恢复点，并将其存储在本地机器上：

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-ScheduledArchive

Start-ScheduledArchive PowerShell 命令可强制 Rapid Recovery 计划存档按需开始，不依赖于预先建立的计划。

使用

此命令的使用如下：

```
Start-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

命令选项

下表介绍 Start-ScheduledArchive 命令可用的选项：

表. 288: Start-ScheduledArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-all	强制执行所有计划存档。
-id	您想要强制执行的计划存档的 ID 编号或空格分隔的标识符。

示例：

开始多个计划的存档作业：

```
>Start-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Start-VBExport

start-VBExport 命令触发启动从选择的恢复点虚拟导出至 Oracle VirtualBox 服务器虚拟机。

必要参数包括含有要导出恢复点的受保护机器的名称；您将向其导出的虚拟机名称；将要在虚拟机上分配的 RAM 容量；主机名称和 Linux 服务器主机的端口以及将存储产生的虚拟机文件的本地、网络或 Linux 文件夹的路径。

使用

此命令的使用如下：

```
Start-VBExport -core -user [user name] -password [password] -protectedserver [machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] |  
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |  
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]  
pathusername [user name] - pathpassword [password]
```

命令选项

下表介绍 Start-VBExport 命令可用的选项：

表. 289: Start-VBExport 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要导出恢复点的受保护机器。
-volumes	可选。要导出的卷名称列表。如果未指定，则将导出指定恢复点中的所有卷。必须使用双引号引起并用空格分隔每个值。请勿在卷名称中使用尾部反斜杠。例如，指定“C:”而非“C:/”
-rpn	可选。要导出的恢复点序号。（您可使用 Get-RecoveryPoints 命令获得恢复点序号。） 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-time	可选。确定导出将要选择的恢复点。您需要使用格式“MM/DD/YYYY hh:mm tt”（例如，“04/24/2015 09:00 AM”）指定确切的时间。指定您的本地机器上设置的时区的日期时间值。 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-vmname	虚拟机的 Windows 名称。
-ram	在虚拟服务器中分配特定容量的 RAM。
-usesourceram	可选。在虚拟服务器中分配与源受保护机器相同容量的 RAM。
-linuxhostname	Linux VirtualBox 服务器主机名。
-hostport	Linux VirtualBox 服务器端口。。
-targetpath	存储虚拟机文件的文件夹的本地、网络或 Linux 路径。
-pathusername	网络机器的用户名。仅当您在参数 -targetpath 中指定网络路径时需要。
-pathpassword	网络机器的密码。仅当您在参数 -targetpath 中指定网络路径时需要。
-accountusername	可选。当您可指定一个用户帐户以注册导出的虚拟机时可使用。仅对于本地或网络机器。
-accountpassword	可选。仅在您为本地或网络机器使用参数 -accountusername。指定一个用户帐户以注册导出的虚拟机时使用。

示例:

从机器 10.10.12.97 上最新恢复点导出所有卷 到一个称为 NewVirtualBoxVM 的 VM 中:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram usesourceram -targetpath D:/exports
```

Start-VirtualStandby

Start-VirtualStandby PowerShell 命令可强制 Rapid Recovery 将数据导出到虚拟待机机器。此按需导出可在定期计划的虚拟待机导出之外发生。

使用

此命令的使用如下：

```
Start-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

命令选项

下表介绍 Start-VirtualStandby 命令可用的选项：

表. 290: Start-VirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-all	为所有虚拟待机机器强制执行导出。
-protectedserver	您想强制导出的受保护机器的名称 - 以逗号和空格分隔。

示例：

为受保护机器强制执行 Virtual Standby 导出：

```
>Start-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Start-VMExport

Start-VMExport 命令触发启动从选择的恢复点虚拟导出至 VMware 工作站服务器虚拟机。

必要参数包括含有要导出恢复点的受保护机器的名称；您将向其导出的虚拟机名称；将要在虚拟机上分配的 RAM 容量以及将存储产生的虚拟机文件的本地或网络文件夹的路径。

使用

此命令的使用如下：

```
Start-VMExport -core -user [user name] -password [password] -protectedserver [machine name] or  
[IP address]] -volumes [volume names] -rpn [number | numbers] |  
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |  
-usesourceram] -linuxhostnme [linux hostname] -hostport [linux port] -targetpath [location]  
pathusername [user name] - pathpassword [password]
```

命令选项

下表介绍 Start-VMExport 命令可用的选项：

表. 291: Start-VMExport 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	要导出恢复点的受保护机器。
-volumes	可选。要导出的卷名称列表。如果未指定，则将导出指定恢复点中的所有卷。必须使用双引号引起并用空格分隔每个值。请勿在卷名称中使用尾部反斜杠。例如，指定“C:”而非“C:/”
-rpn	可选。要导出的恢复点序号。（您可使用 Get-RecoveryPoints 命令获得恢复点序号。 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-time	可选。确定导出将要选择的恢复点。您需要使用格式“MM/DD/YYYY hh:mm tt”（例如，“04/24/2015 09:00 AM”）指定确切的时间。指定您的本地机器上设置的时区的日期时间值。 注: 如果该命令中未指定‘time’和‘rpn’选项，则将导出最近的恢复点。
-vmname	虚拟机的 Windows 名称。
-ram	在虚拟服务器中分配特定容量的 RAM。
-usesourceram	可选。在虚拟服务器中分配与源受保护机器相同容量的 RAM。
-targetpath	存储虚拟机文件的文件夹的本地、网络或 Linux 路径。
-pathusername	网络机器的用户名。仅当您在参数 -targetpath 中指定网络路径时需要。
-pathpassword	网络机器的密码。仅当您在参数 -targetpath 中指定网络路径时需要。
-version	要使用的 VMware Tools 版本。有效版本为：7、8、9 或 10。

示例:

从机器 10.10.12.97 上最新恢复点导出所有卷 到一个称为 NewVMwareVM 的 VM 中:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -targetpath D:/exports
```

Stop-ActiveJobs

Stop-ActiveJobs 为指定的受保护机器取消活动作业。

使用

此命令的使用如下:

```
Stop-ActiveJobs [-protectedserver [machine name | IP address]] [-core [host name]] -user [user name] -password [password] -jobtype [jobtype]
```

命令选项

下表介绍 Stop-ActiveJobs 命令可用的选项:

表. 292: Stop-ActiveJobs 命令选项

选项	说明
-?	显示此帮助消息。
-all	选择并取消所有受保护机器中指定类型的事件。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-protectedserver	确定应取消其作业的受保护机器。
-jobtype	可选。指定作业类型筛选器。可用值: 'transfer'（数据传输）、'repository'（存储库维护）、'replication'（本地和远程复制）、'backup'（备份和还原）、'bootcdbuilder'（创建启动 CD）、'diagnostics'（上传日志）、'exchange'（Exchange Server 文件检查）、'export'（恢复点导出）、'pushinstall'（向受保护机器部署 Agent 软件）、'rollback'（从恢复点还原数据）、'rollup'（恢复点汇总）、'sqlattach'（代理程序可附加性检查）、和 'mount'（非存储库）。默认情况下，将取消指定类型的所有作业。

示例:

停止受保护机器中的传输作业:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -jobtype transfer
```

停止特定受保护机器的所有作业:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -all
```

Suspend-Replication

Suspend-Replication 命令可让管理员暂停复制。

用户可以通过三种方式暂停复制:

- 暂停所有受保护机器的主 Core 上的复制 (-outgoing parameter)
管理员必须通过传出复制配对指定远程机器名称以暂停主 Core 上的传出复制。

```
>Suspend-replication -outgoing 10.10.12.10
```
- 暂停单个受保护机器的主 Core 上的复制 (-protectedserver 参数)

```
>Suspend-replication -protectedserver 10.10.12.97
```
- 暂停目标 Core 上的复制 (-incoming parameter)
如果本地 Core 是目标 Core, 则管理员可以使用 -incoming 参数指定主 Core 来暂停复制。

命令选项

下表介绍 Suspend-Replication 命令可用的选项:

表. 293: Suspend-Replication 命令选项

选项	说明
-?	显示此帮助消息。
-all	暂停所选 Core 上的所有受保护机器。
-core	可选。远程 Core 主机 IP 地址 (含可选的端口号)。默认情况下, 将与安装在本地机器上的 Core 建立连接。
-pause	[snapshots]、[replication] 或 [vmexport]。
-password	可选。远程 Core 主机的密码。如果您指定密码, 则还必须提供用户名。如果未提供此信息, 则将使用已登录用户的凭据。
-protectedserver	暂停当前受保护的服务器。
-user	可选。远程 Core 主机的用户名。如果您指定用户名, 则还必须提供密码。如果未提供此信息, 则将使用已登录用户的凭据。
-incoming	复制到 Core 机器的远程 Core 的主机名。暂停远程 Core 上所有受保护机器的复制。
-outgoing	数据复制到的远程目标 Core 的主机名。暂停远程 Core 上所有受保护机器的复制。

示例:

对于具有 IP 地址 10.10.1.76 的单个受保护机器，暂停具有 IP 地址 10.10.1.15 的远程 Core 上的传出复制:

```
>Suspend-replication -core 10.10.1.15 -protectedserver 10.10.1.76
```

对于所有受保护机器，暂停从本地 Core 到具有 IP 地址 10.10.1.63 的远程目标的传出复制:

```
>Suspend-replication -outgoing 10.10.1.63
```

在具有 IP 地址 10.10.1.15 的远程 Core 上暂停来自 10.10.1.82 的传入复制（管理员仅可暂停整个机器的传入复制）:

```
>Suspend-replication -core 10.10.1.15 -incoming 10.10.1.82
```

Suspend-RepositoryActivity

Suspend-RepositoryActivity PowerShell 命令可暂停 Rapid Recovery 存储库的活动。暂挂活动会锁定存储库，从而防止任何数据进入或离开。

使用

此命令的使用如下:

```
Suspend-RepositoryActivity -core [host name] -user [login] -password [password] -all | -repository ["name" | "name1 " "name2"]
```

命令选项

下表介绍 Suspend-RepositoryActivity 命令可用的选项:

表. 294: Suspend-RepositoryActivity 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-all	暂挂与此 Core 关联的所有存储库的活动。
-repository	要锁定的存储库的名称。该名称必须使用双引号括起。您可以指定多个空格分隔的存储库。

示例：

暂挂多个存储库的活动：

```
>Suspend-RepositoryActivity -repository "repository1" "repository2"
```

暂挂所有存储库上的活动：

```
>Suspend-RepositoryActivity -all
```

Suspend-ScheduledArchive

Suspend-ScheduledArchive PowerShell 命令可暂停 Rapid Recovery 计划存档。此命令会阻止按计划进行存档，直到您重新激活它为止。。

使用

此命令的使用如下：

```
Suspend-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

命令选项

下表介绍 Suspend-ScheduledArchive 命令可用的选项：

表. 295: Suspend-ScheduledArchive 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-all	暂停所有计划存档。
-id	要暂挂的计划存档的 ID 编号或空格分隔的标识符。

示例：

暂挂多个计划存档：

```
>Suspend-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Suspend-Snapshot

Suspend-Snapshot 命令可使管理员暂停快照。

使用

此命令的使用如下：

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |  
-protectedserver [name | IP address] -time [time string]
```

命令选项

下表介绍 Suspend-Snapshot 命令可用的选项：

表. 296: Suspend-Snapshot 命令选项

选项	说明
-?	显示此帮助消息。
-all	暂停所选 Core 上的所有受保护机器。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。 默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-time	恢复快照（仅适用于快照暂停）的时间，格式为 ‘Day-Hours-Minutes’ 。

示例：

暂停本地 Core 上受保护机器（IP 为 10.10.10.4）的快照并在特定时间恢复：

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend-VirtualStandby

Suspend-VirtualStandby PowerShell 命令可暂停将数据导出到 Rapid Recovery 虚拟待机机器。

使用

此命令的使用如下：

```
Suspend-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

命令选项

下表介绍 Suspend-VirtualStandby 命令可用的选项：

表. 297: Suspend-VirtualStandby 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。 如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供登录。 如果未提供此信息，则将使用已登录用户的凭据。
-all	为所有虚拟待机机器暂停导出。
-protectedserver	带有您想暂挂的虚拟待机机器的受保护机器的名称 - 以逗号和空格分隔。

示例：

为受保护机器暂挂虚拟待机导出：

```
>Suspend-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$$sdd -
protectedserver 10.10.5.22
```

Suspend-VMExport

Suspend-VMExport 命令可使管理员暂停导出到虚拟机。

使用

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```


命令选项

下表介绍 Suspend-VMExport 命令可用的选项：

表. 298: Suspend-VMExport 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-all	暂停所选 Core 上的所有受保护机器。
-protectedserver	暂停当前受保护的服务器。

示例：

暂停本地 Core 上 IP 为 10.10.10.4 的受保护机器的虚拟机导出：

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

Update-Repository 命令可将盘区添加到现有 DVM 存储库。指定的大小必须介于 250MB 和 16TB 之间。

使用

```
Update-Repository -name [repository name] -size [size] [[[-datapath [datapath]
-metadatapath [metadata path]] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password]]] -core [host name] -user [user name]
-password [password]
```

命令选项

下表介绍 Update-Repository 命令可用的选项：

表. 299: Update-Repository 命令选项

选项	说明
-?	显示此帮助消息。
-core	可选。远程 Core 主机 IP 地址（含可选的端口号）。默认情况下，将与安装在本地机器上的 Core 建立连接。

选项	说明
-user	可选。远程 Core 主机的用户名。如果您指定用户名，则还必须提供密码。如果未提供此信息，则将使用已登录用户的凭据。
-password	可选。远程 Core 主机的密码。如果您指定密码，则还必须提供用户名。如果未提供此信息，则将使用已登录用户的凭据。
-name	DVM 存储库名称。
-size	DVM 存储库盘区的大小。可用单位：b、Kb、Mb、Gb、Tb、Pb。
-datapath	仅适用于本地位置。确定 DVM 存储库盘区的数据路径。
-metadatapath	仅适用于本地位置。确定 DVM 存储库盘区的元数据路径。
-uncpath	仅适用于共享位置。确定 DVM 存储库盘区的数据路径和元数据路径。
-shareusername	仅适用于共享位置。确定共享位置的登录。
-sharepassword	仅适用于共享位置。确定共享位置的密码。

示例：

添加盘区到最小的 DVM 存储库：

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -metadatapath C:\repository\Metadata
```

本地化

在安装有 Rapid Recovery Core 的同一机器上运行时，Rapid Recovery PowerShell 模块基于为 Core 设置的语言确定其显示语言。本地化的 Rapid Recovery 版本（例如，此版本）支持英语、中文（简体）、法语、韩语、德语、日语、葡萄牙语（巴西）和西班牙语。

如果 Rapid Recovery PowerShell 模块安装在单独的机器上，则英文是唯一支持的语言。

限定符

下表介绍 Rapid Recovery PowerShell 模块可用的限定符。

表. 300: Rapid Recovery PowerShell 模块限定符

限定符	使用
-core <Rapid Recovery Core Name>	Core 的主机名。 默认值：Localhost
-ProtectedServer <Protected Server Name>	Rapid Recovery Agent 的主机名/IP 地址。 默认值：如果多个服务器受保护，则为 Localhost；否则为受保护的单个服务器。
-Mode <READ, READWRITE, WRITE>	恢复点安装模式。 默认值：Read。
-Volumes <Snapshot Volume Letter>	来自 Rapid Recovery Agent 的快照卷号。

限定符	使用
	默认值: All。
-User <User Name>	用于连接到 Rapid Recovery Core 的用户名。 此用户通常为服务用户。
-Domain <Domain Name>	/User 中定义的用户所属的域。
-Password <Password>	/User 中定义的用户密码。
-Path <Target path to mount, dismount recovery points or archive location>	例如: C:\RapidRecoveryMount。

使用脚本扩展 Rapid Recovery 作业

Rapid Recovery 允许管理员在特定情况下通过执行命令和脚本来实现资源的自动化管理。Rapid Recovery 软件支持将 PowerShell 脚本用于 Windows 和将 Bourne Shell 脚本用于 Linux。

每次在 Rapid Recovery Core 上启动复制、虚拟导出或备份快照等操作时，系统便会自动创建 Core 作业。您可以通过在操作前后运行脚本将这些作业延期。这些脚本称作前后脚本。

本节介绍可供管理员在 Windows 和 Linux Rapid Recovery 中指定情况下所使用的脚本。

小心： 本文档中提供的示例 PowerShell 和 Bourne 脚本运行时将起到限定管理者设计的作用。修改运作脚本时采取预防措施，以保留工作版本。此处包含对脚本示例的任何修改或您创建的任何脚本都被认为是自定义，这通常不在 Dell Support 覆盖范围内。

主题：

- 在 Rapid Recovery 中使用 PowerShell 脚本
- PowerShell Scripting 的输入参数
- 示例 PowerShell 脚本
- 使用 Rapid Recovery 中的 Bourne Shell 脚本
- Bourne Shell Scripting 的输入参数
- 示例 Bourne Shell 脚本

在 Rapid Recovery 中使用 PowerShell 脚本

Windows PowerShell 是一个与 Microsoft .NET Framework 相连的环境，旨在实现管理自动化。Rapid Recovery 包括用于 PowerShell 脚本处理的完整客户端软件开发工具包 (SDK)，它允许具有管理权限的用户在指定情况下运行用户提供的 PowerShell 脚本，例如创建快照、运行可附加性检查和可安装性检查前后等。管理员可同时从 Rapid Recovery Core 和受保护机器运行脚本。脚本可接受参数，且脚本输出将写入 Core 和受保护机器日志文件。

① 注： 对于每夜作业，保留一个脚本文件和 JobType 输入参数以区分每夜作业。

脚本文件位于 %ALLUSERSPROFILE%\AppRecovery\Scripts 文件夹中。

- 在 Windows 7 中，%ALLUSERSPROFILE% 文件夹的路径为：C:\ProgramData。
- 在 Windows 2003 中，该文件夹的路径为：Documents and Settings\All Users\Application Data\。

① 注： 运行 Rapid Recovery 脚本之前，必须安装和配置 Windows PowerShell。

有关如何使用 PowerShell 脚本的更多信息，请参阅示例 PowerShell 脚本、PowerShell Scripting 的输入参数、Bourne Shell Scripting 的输入参数和示例 Bourne Shell 脚本。

PowerShell Scripting 的先决条件

对 Rapid Recovery 运行 PowerShell 脚本之前，必须安装 Windows PowerShell 2.0 或更高版本。由于 PowerShell 3.0 中引入的新功能，包括更轻松的对象属性访问、PowerShell Web 访问及 REST 调用支持，Dell 建议使用 PowerShell 3.0 或更高版本。

① 注： 将 powershell.exe.config 文件置于 PowerShell 主目录下。例如 C:\WindowsPowerShell\powershell.exe.config。

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0.30319"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

测试 PowerShell 脚本

如果要测试您计划运行的脚本，可使用 PowerShell 图形编辑器 powershell_is。此外，还需要将配置文件 powershell_is.exe.config 添加至配置文件 powershell.exe.config 所在的文件夹。

注: 要配置文件，powershell_is.exe.config 必须与 powershell.exe.config 文件具有相同的内容。

小心: 如果前 PowerShell 脚本或后 PowerShell 脚本失败，则作业也将失败。

本地化

在安装有 Rapid Recovery Core 的同一计算机上运行时，Rapid Recovery PowerShell 模块基于该 Core 的语言设置确定其显示语言。本地化 Rapid Recovery 版本，例如此版本支持英文、中文（简体）、法语、韩语、德语、日语、葡萄牙语（巴西）和西班牙语。

如果 Rapid Recovery PowerShell 模块安装在单独的计算机上，则英文是唯一支持的语言。

限定符

下表介绍 Rapid Recovery PowerShell 模块可用的限定符。

表. 301: Rapid Recovery PowerShell 模块限定符

限定符	使用
-core <Rapid Recovery Core Name>	Core 的主机名。 默认值: Localhost
-ProtectedServer <Protected Server Name>	Rapid Recovery Agent 的主机名/IP 地址。 默认值: 如果多个服务器受保护，则为 Localhost；否则为受保护的单个服务器。
-Mode <READ, READWRITE, WRITE>	恢复点安装模式。 默认值: Read。
-Volumes <Snapshot Volume Letter>	来自 Rapid Recovery Agent 的快照卷号。 默认值: All。
-User <User Name>	用于连接到 Rapid Recovery Core 的用户名。 此用户通常为服务用户。

限定符	使用
-Domain <Domain Name>	/User 中定义的用户所属的域。
-Password <Password>	/User 中定义的用户密码。
-Path <Target path to mount, dismount recovery points or archive location>	例如: C:\RapidRecoveryMount。

PowerShell Scripting 的输入参数

示例脚本中使用了所有可用的输入参数。下表对这些参数进行了说明。

① | 注: 脚本文件必须具有与示例脚本文件相同的名称。

AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents)

下表显示 AgentProtectionStorageConfiguration 参数可用的对象。

表. 302: AgentProtectionStorageConfiguration 参数的对象

方法	说明
public Guid RepositoryId { get; set; }	获取或设置用于存储代理恢复点的存储库的 ID。
public string EncryptionKeyId { get; set; }	获取或设置此代理恢复点的加密密钥的 ID。空字符串表示未加密。

AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

下表显示 AgentTransferConfiguration 参数可用的对象。

表. 303: AgentTransferConfiguration 参数的对象

方法	说明
public uint MaxConcurrentStreams { get; set; }	获取或设置 Core 和代理之间用于传输数据的并发 TCP 连接的最大数量。
public uint MaxTransferQueueDepth { get; set; }	获取或设置可排队写入的数据块盘区的最大数量。从传输流读取一系列数据块时，这一系列数据块将置于生产者或消费者队列，其中消费者线程将读取这些数据块并将其写入日期对象。如果存储库写入速度慢于网络读取速度，此队列将会填满。队列已满并停止读取的点为最大传输队列深度。
public uint MaxConcurrentWrites { get; set; }	获取或设置在某个日期的任何指定时间未完成的数据块写入操作的最大数量。如果收到的附加数据块超出该参数指定的写入操作的最大数量，则将忽略这些附加数据块，直至未完成的写入操作之一完成。
public ulong MaxSegmentSize { get; set; }	获取或设置在单个请求中传输的连续数据块的最大数量。根据测试，较高或较低的值可能最佳。

方法	说明
<code>public Priority Priority { get; set; }</code>	获取或设置传输请求的优先级。
<code>public uint GetChangedBlocksRetries { get; set; }</code>	如果从代理程序对已变更数据块的初始检索失败，则获取或设置重试次数。
<code>public int MaxRetries { get; set; }</code>	获取或设置一个失败传输在被认定失败之前应重试的最大次数。
<code>public bool UseDefaultMaxRetries { get; set; }</code>	如果包含，则使用重试次数（在传输配置中指定）的默认最大数量。
<code>public Guid ProviderId { get; set; }</code>	获取或设置 VSS 提供程序将对此主机上的快照使用的 GUID。管理员通常会接受默认值。
<code>public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }</code>	获取或设置不应包含在此快照中的 VSS 编写器 ID 的集合。编写器 ID 由编写器的名称决定。此名称仅用于说明，不必提供与编写器名称完全相同的匹配项。
<code>public ushort TransferDataServerPort { get; set; }</code>	获取或设置包含 TCP 端口的值，此端口用于接受来自 Core 的连接，以便从受保护机器向 Core 实际传输数据。Agent 将尝试侦听此端口，但是，如果此端口正在使用，则受保护机器可转而使用不同的端口。Core 应使用在 VolumeSnapshotInfo 对象的 BlockHashesUri 和 BlockDataUri 属性中为每个捕获的卷所指定的端口号。
<code>public TimeSpan CleanSnapshotTimeout { get; set; }</code>	获取或设置传输完成后清洁快照需要等待的时间长度。
<code>public TimeSpan SnapshotTimeout { get; set; }</code>	获取或设置在 VSS 快照操作放弃或超时之前，等待其完成的时间量。
<code>public TimeSpan TransferTimeout { get; set; }</code>	获取或设置在放弃快照之前，等待 Core 进行进一步联系的时间量。
<code>public TimeSpan NetworkReadTimeout { get; set; }</code>	获取或设置与此传输相关的网络读取操作超时。
<code>public TimeSpan NetworkWriteTimeout { get; set; }</code>	获取或设置与此传输相关的网络写入操作超时。
<code>public uint InitialQueueSize { get; set; }</code>	获取或设置请求的初始队列的大小。
<code>public uint MinVolumeFreeSpacePercents { get; set; }</code>	获取或设置卷上的最小可用空间量，以百分比表示。如果可用空间低于此参数指定的量，则将删除所有更改日志并强制创建基本映像。
<code>public uint MaxChangeLogsSizePercents { get; set; }</code>	获取或设置驱动程序更改日志作为卷容量的一部分的最大大小，以百分比表示。如果更改日志的一部分大于此值，则将删除所有更改日志并强制创建基本映像。
<code>public bool EnableVerification { get; set; }</code>	获取或设置表示是否应对发送到 Core 的每个数据块执行诊断验证的值。

BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

下表显示 BackgroundJobRequest 参数可用的对象。

表. 304: BackgroundJobRequest 参数的对象

方法	说明
<code>public AgentIdsCollection AgentIds { get; set; }</code>	获取或设置受保护机器的 ID。
<code>public bool IsNightlyJob { get; set; }</code>	获取或设置表示后台作业是否为每夜作业的值。

方法	说明
public Guid NightlyJobTransactionId { get; set; }	获取或设置每夜作业事务 ID。
public Guid JobId { get; set; }	获取或设置后台作业 ID。
public bool Force { get; set; }	获取或设置表示是否强制执行作业的值。
public uint JobStartsCount { get; set; }	获取或设置要启动一个作业的尝试次数。
public virtual bool InvolvesAgentId(Guid agentId)	确定表示具体代理是否包含在作业中的值。

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

从参数 DatabaseCheckJobRequestBase 继承其值。

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

从参数 BackgroundJobRequest 继承其值。

表. 305: DatabaseCheckJobRequestBase 参数的对象

方法	说明
public string RecoveryPointId { get; set; }	获取或设置将在数据库中检查的恢复点的 ID。

ExportJobRequest (namespace Replay.Core.Contracts.Export)

从参数 BackgroundJobRequest 继承其值。

下表显示 ExportJobRequest 参数可用的对象。

表. 306: ExportJobRequest 参数的对象

方法	说明
public uint RamInMegabytes { get; set; }	获取或设置用于导出 VM 的内存大小。如果设置为零 (0)，将使用源机器的内存大小。
public ushort CpuCount { get; set; }	获取或设置已导出 VM 的 CPU 数量。设置为 0 将使用源计算机的 CPU 数量。
public ushort CoresPerCpu { get; set; }	获取或设置已导出 VM 每个 CPU 的核数。设置为 0 将使用源计算机每个 CPU 的核数。
public VirtualMachineLocation Location { get; set; }	获取或设置此导出的目标位置。这是抽象基类。

方法	说明
public VolumemageldsCollection Volumemagelds { get; private set; }	获取或设置要包括在 VM 导出中的卷映像。
public ExportJobPriority Priority { get; set; }	获取或设置导出请求的优先级。

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

从参数 BackgroundJobRequest 继承其值。

表. 307: NightlyAttachabilityJobRequest 参数的对象

方法	说明
public int SimultaneousJobsCount { get; set; }	获取或设置可以同时运行的作业数量。

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

从参数 BackgroundJobRequest 继承其值。

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

下表显示 TakeSnapshotResponse 参数可用的对象。

表. 308: TakeSnapshotResponse 参数的对象

方法	说明
public Guid SnapshotSetId { get; set; }	获取或设置 VSS 分配给此快照的 GUID。
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	获取或设置包括在快照中的每个卷的快照信息集合。

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

从参数 BackgroundJobRequest 继承其值。

下表显示 TransferJobRequest 参数可用的对象。

表. 309: TransferJobRequest 参数的对象

方法	说明
<pre>public VolumeNameCollection VolumeNames { get; set; }</pre>	获取或设置用于传输的名称集合。 VolumeNames 是包含以下数据的数据结构： • GuidName。与卷关联的 Guid，如果未设置 DisplayName，则用作名称。 • DisplayName。卷的显示名称。
<pre>public VolumeNameCollection TransferredVolumes { get; set; }</pre>	获取或设置已传输卷集合。
<pre>public VolumeNameCollection DependentVolumeNames { get; set; }</pre>	获取或设置独立卷集合。
<pre>public QuotaSettingsCollection EnabledDiskQuotas { get; set; }</pre>	获取或设置卷上已启用的配额。
<pre>public ShadowCopyType ShadowCopyType { get }</pre>	获取用于传输的复制类型。可用的值包括： • Copy • Full
<pre>public AgentTransferConfiguration TransferConfiguration { get; set; }</pre>	获取或设置传输配置。 AgentTransferConfiguration 是将包含以下数据的对象： • MaxConcurrentStreams。Core 和代理之间用于传输数据的并发 TCP 连接的最大数量 • MaxTransferQueueDepth。可排队等待的数据块盘区的最大数量 • MaxConcurrentWrites。在某个日期的任何指定时间未完成的数据块写入操作的最大数量。如果在此数量的数据块写入操作未完成时收到附加数据块，则将忽略附加数据块，直至未完成的数据块之一写入为止。 • MaxSegmentSize。在单个请求中传输的连续数据块的最大数量 • Priority。是将包含以下数据的对象： • 未定义 • 一 • 二 • 三 • 四 • 五 • 六 • 七 • 八 • 九 • 十 • 最高（等于一） • 最低（等于十） • 默认值（等于五） • MaxRetries。一个失败传输在被认定失败之前应重试的最大次数 • UseDefaultMaxRetries。该值表示重试的最大次数为默认值 • ProviderId。VSS 提供程序将对此主机上的快照使用的 GUID。用户通常使用默认设置。
<pre>public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }</pre>	获取或设置存储配置。

方法	说明
public string Key { get; set; }	生成伪随机（而非密码保护）密钥，此密钥可用作验证传输请求的一次性密码。
public bool IsBaseImage { get; set; }	获取或设置表示是否进行基本映像的值。
public bool IsForced { get; set; }	获取或设置表示是否已强制传输的值。
public Guid ProtectionGroupId { get; set; }	获取或设置受保护组 ID。
public TargetComponentTypes LogTruncationTargets { get; set; }	获取或设置表示要执行日志截断的数据库（SQL 或 Exchange）的值。
public bool ForceBaseImage { get }	获取表示是否强制创建基本映像的值。
public bool IsLogTruncation { get }	获取表示是否执行日志截断作业的值。

TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

从 TransferScriptParameterBase 参数继承其值。

TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

下表显示 TransferPostscript 参数可用的对象。从 TransferScriptParameterBase 参数继承其值。

表. 310: TransferPostscript 参数的对象

方法	说明
public VolumeNameCollection VolumeNames (get; set;)	获取或设置用于传输的卷名称集合。 VolumeNames 是包含以下数据的数据结构： • GuidName。与卷关联的 Guid，如果未设置 DisplayName，则用作名称。 • DisplayName。卷的显示名称。
public ShadowCopyType ShadowCopyType { get; set; }	获取或设置用于传输的复制类型。ShadowCopyType 是具有值的枚举。可用的值包括： • Unknown • Copy • Full
public AgentProtectionStorageConfigurationCom mon StorageConfiguration { get; set; }	获取或设置存储配置。
public AgentTransferConfiguration TransferConfiguration { get; set; }	获取或设置传输配置。 AgentTransferConfiguration 是将包含以下数据的对象： • MaxConcurrentStreams。Core 和代理之间用于传输数据的并发 TCP 连接的最大数量 • MaxTransferQueueDepth。可排队等待的数据块盘区的最大数量

方法	说明
	- MaxConcurrentWrites。在某个日期的任何指定时间未完成的数据块写入操作的最大数量。如果在此数量的数据块写入操作未完成时收到附加数据块，则将忽略附加数据块，直至未完成的数据块之一写入为止。 - MaxSegmentSize。在单个请求中传输的连续数据块的最大数量 - Priority。是包含以下数据的对象： "未定义 "一 "二 "三 "四 "五 "六 "七 "八 "九 "十一 "最高（等于一） "最低（等于十） "默认值（等于五） - MaxRetries。一个失败传输在被认定失败之前应重试的最大次数 - UseDefaultMaxRetries。该值表示重试的最大次数为默认值 - ProviderId。VSS 提供程序将对此主机上的快照使用的 GUID。管理员通常会接受默认值。
<pre>public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)</pre>	- ExcludedWriterIds。不应包含在此快照中的 VSS 写入程序 ID 的集合。写入程序 ID 由写入程序的名称来确定。此名称仅用于说明文件，不必与写入程序的实际名称完全相同。 - TransferDataServerPort。包含 TCP 端口的值，此端口用于接受来自 Core 的连接，以便从代理向 Core 实际传输数据。 - SnapshotTimeout。在 VSS 快照操作放弃或超时之前，等待其完成的时间量。 - TransferTimeout。在放弃快照之前，等待 Core 进行进一步联系的时间量。 - NetworkReadTimeout。与此传输相关的网络读取操作超时。 - NetworkWriteTimeout。与此传输相关的网络写入操作超时。 - InitialQueueSize。请求的初始队列的大小。 - MinVolumeFreeSpacePercents。卷上的最小可用空间量，以百分比表示。 - MaxChangeLogsSizePercents。驱动程序更改日志作为卷容量的一部分的最大大小，以百分比表示。 - EnableVerification。该值表示是否应对发送到 Core 的每个数据块运行诊断验证。
<pre>public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }</pre>	获取或设置存储配置 AgentProtectionStorageConfiguration 对象包含以下数据： - RepositoryId。将用于存储此代理恢复点的存储库的名称 - EncryptionKeyId。此代理恢复点的加密密钥的 ID。空字符串表示未加密
<pre>public string Key { get; set; }</pre>	密钥方法将生成伪随机（而非密码保护）密钥，此密钥可用作验证传输请求的一次性密码。
<pre>public bool ForceBaseImage { get; set; }</pre>	获取或设置表示是否强制传输执行基本映像捕获的值。
<pre>public bool IsLogTruncation { get; set; }</pre>	获取或设置表示日志是否截断的值。

方法	说明
public uint LatestEpochSeenByCore { get; set; }	获取或设置最新的日期值。 LatestEpochSeenByCore 方法是 Core 创建的最近快照的序数。这是使用 VSS 创建此特定快照时筛选器驱动程序分配给该快照的“日期”。
public Guid SnapshotSetId { get; set; }	获取或设置 VSS 分配给此快照的 GUID。
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	获取或设置包括在快照中的每个卷的快照信息集合。

TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution)

下表显示 TransferScriptParameterBase 参数可用的对象。

表. 311: TransferScriptParameterBase 参数的对象

方法	说明
public AgentTransferConfiguration TransferConfiguration { get; set; }	获取或设置传输配置。
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	获取或设置存储配置。

VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

下表显示 VirtualMachineLocation 参数可用的对象。

表. 312: VirtualMachineLocation 参数的对象

方法	说明
public string Description { get; set; }	获取或设置此位置的人工可读说明。
public string Name { get; set; }	获取或设置 VM 名称。

VolumImageldsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

从参数 System.Collections.ObjectModel.Collection<string> 继承其值。

VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

下表显示 VolumeName 参数可用的对象。

表. 313: VolumeName 参数的对象

方法	说明
public string GuidName { get; set;}	获取或设置卷 ID。
public string DisplayName { get; set;}	获取或设置卷名称。
public string UrlEncode()	获取可在 URL 上明确传递的 URL 编码的名称版本。 ① 注: .NET 4.0 WCF 中存在路径转义字符无法在 URI 模板中正常工作的已知问题 (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312)。由于卷名称包含“\”和“?”，因此，必须使用其他特殊字符来替换特殊字符“\”和“?”。
public string GetMountName()	为这一可用于将卷映像安装至某文件夹的卷返回名称。

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

从参数 System.Collections.ObjectModel.Collection<VolumeName> 继承其值。

下表显示 VolumeNameCollection 参数可用的对象。

表. 314: VolumeNameCollection 参数的对象

方法	说明
public override bool Equals(object obj)	确定此实例和同样为 VolumeNameCollection 对象的某个指定对象是否具有相同的值。(Overrides Object.Equals(Object).)
public override int GetHashCode()	返回此 VolumeNameCollection 的哈希码。(Overrides Object.GetHashCode().)

VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

下表显示 VolumeSnapshotInfo 参数可用的对象。

表. 315: VolumeSnapshotInfo 参数的对象

方法	说明
public Uri BlockHashesUri { get; set;}	获取或设置可用于读取卷数据块的 MD5 哈希值的 URI。
public Uri BlockDataUri { get; set;}	获取或设置可用于读取卷数据块的 URI。

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

从参数 System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo> 继承其值。

示例 PowerShell 脚本

以下示例脚本旨在帮助具有管理权限的用户运行 PowerShell 脚本。

相关链接

[PreTransferScript.sh](#)
[PostTransferScript.ps1](#)
[PreExportScript.ps1](#)
[PostExportScript.ps1](#)
[PreNightlyJobScript.ps1](#)
[PostNightlyJobScript.ps1](#)

PreTransferScript.ps1

PreTransferScript 在传输快照前于受保护机器上运行。

示例 PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
    echo 'TransferPrescriptParameterObject parameter is null'
}
else {
    echo 'TransferConfiguration:' $TransferPrescriptParameterObject.TransferConfiguration
    echo 'StorageConfiguration:' $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

PostTransferScript 在传输快照后于受保护机器上运行。

示例 PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];
# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
    echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
    echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType
    echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage
    echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

PreExportScript.ps1

PreExportScript 在任何导出作业前于 Core 上运行。

示例 PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
    echo 'ExportJobRequestObject parameter is null'
}
else {
    echo 'Location:' $ExportJobRequestObject.Location
    echo 'Priority:' $ExportJobRequestObject.Priority
}
```

PostExportScript.ps1

PostExportScript 在任何导出作业后于 Core 上运行。

① **注:** 如果在初始启动后对导出的受保护机器运行一次 **PostExportScript**，则无输入参数。常规受保护机器应将此脚本作为 **PostExportScript.ps1** 包含在 **PowerShell** 脚本文件夹中。

示例 PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
    echo 'ExportJobRequestObject parameter is null'
}
else {
    echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
    echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

PreNightlyJobScript 在任何每夜作业前于 Core 端运行。此脚本具有 \$JobClassName 参数，有助于分别处理那些子作业。

示例 PreNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod, [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
```

```

        echo 'NightlyAttachabilityJobRequestObject parameter is null';
    }
    else {
        echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
        echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
    }
    break;
}
# working with Rollup Job
RollupJob {
    $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
    echo 'Rollup job results:';
    if($RollupJobRequestObject -eq $null) {
        echo 'RollupJobRequestObject parameter is null';
    }
    else {
        echo 'SimultaneousJobsCount:' $RollupJobRequestObject.SimultaneousJobsCount;
        echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
        echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
    }
    $AgentsCollection = $Agents -as "System.Collections.Generic.List`1[System.Guid]"
    if($AgentsCollection -eq $null) {
        echo 'AgentsCollection parameter is null';
    }
    else {
        echo 'Agents GUIDs:'
        foreach ($a in $AgentsCollection) {
            echo $a
        }
    }
    break;
}
# working with Checksum Check Job
ChecksumCheckJob {
    $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
    echo 'Exchange checksumcheck job results:';
    if($ChecksumCheckJobRequestObject -eq $null) {
        echo 'ChecksumCheckJobRequestObject parameter is null';
    }
    else {
        echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
        echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
        echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
    }
    break;
}
# working with Log Truncation Job
TransferJob {
    $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
    echo 'Transfer job results:';
    if($TransferJobRequestObject -eq $null) {
        echo 'TransferJobRequestObject parameter is null';
    }
    else {
        echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
        echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
    }
    echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
    break;
}
}

```

PostNightlyJobScript.ps1

PostNightlyJobScript 在任何每夜作业后于 Core 上运行。此脚本具有 \$JobClassName 参数，有助于分别处理那些子作业。

示例 PostNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results: ';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results: ';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as "System.Collections.Generic.List`1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
            echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                echo $a
            }
        }
        break;
    }
# working with Checksum Check Job
```

```
ChecksumCheckJob {
    $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
    echo 'Exchange checksumcheck job results: ';
    if($ChecksumCheckJobRequestObject -eq $null) {
        echo 'ChecksumCheckJobRequestObject parameter is null';
    }
    else {
        echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
        echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
        echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
    }
    break;
}
# working with Log Truncation Job
TransferJob {
    $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
    echo 'Transfer job results: ';
    if($TransferJobRequestObject -eq $null) {
        echo 'TransferJobRequestObject parameter is null';
    }
    else {
        echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
        echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
    }
    echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
    $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
    if($TakeSnapshotResponseObject -eq $null) {
        echo 'TakeSnapshotResponseObject parameter is null';
    }
    else {
        echo 'ID of this transfer session:' $TakeSnapshotResponseObject.SnapshotSetId;
        echo 'Volumes:' $TakeSnapshotResponseObject.VolumeSnapshots;
    }
    break;
}
}
```

使用 Rapid Recovery 中的 Bourne Shell 脚本

Bourne shell (sh) 是基于 Unix 操作系统的一种 Shell 语言或命令行解释器。Bourne shell 在 Rapid Recovery 中与 Linux 搭配使用以自定义环境，以及指定特定操作按预定顺序运行。.sh 是 Bourne shell 文件的文件扩展名和命名约定。

Bourne Again Shell (BASH) 是一种类似的 Shell 语言，实现了相同语法、参数和变量扩展、重定向和引用。BASH 也使用同一 .sh 文件扩展名。此处的信息同样应用于 BASH。

使用传输和导出前后 script hook，您可以在传输或导出前后运行系统操作。例如，您可能想要在进行传输时禁用特定 cronjob，并在传输完成后启用它。再例如，您需要运行命令以刷新应用程序特定数据到磁盘。内容将写入临时文件并使用 exec 运行。然后使用脚本第一行中定义的解释器运行脚本，例如，(#!/usr/bin/env bash)。如果指定的解释器不可用，脚本将使用 \$SHELL 环境变量定义的默认 shell。

您可以替代并使用任何解释器。例如，在脚本的 #! 行上，您可以根据偏好将“bash”替换为“zsh”（Z 外壳程序）、“tcsh”（tee 外壳程序）等。

您可以将 TransferPrescript 参数可用的对象或您自己的命令添加到 PreTransferScript.sh 和 PostTransfer.sh 脚本以自定义脚本。

本节介绍了管理员在 Rapid Recovery（适用于 Windows 和 Linux）中的指定情况下可使用的脚本。它包括以下主题：

- [Bourne Shell Scripting 的输入参数](#)
- [示例 Bourne Shell 脚本](#)

Bourne Shell Scripting 的先决条件

Rapid Recovery 可在传输前和传输后在 Linux Agent 机器上运行 Bourne Shell 脚本。使用 Rapid Recovery Agent 软件保护的 Linux 机器支持以下脚本。

① **注:** 请注意，如果脚本无法执行，传输作业将失败。

- PreTransferScript.sh
- PostTransferScript.sh
- PostExportScript.sh

要使用这些脚本，请确保它们驻留在 `/opt/apprecovery/scripts/` 目录中。

支持传输和后传输脚本参数

Linux 上支持以下传输脚本参数。有关详情，请参阅[示例 Bourne Shell 脚本](#)。

- TransferPrescriptParameter_VolumeNames=\$TransferPrescriptParameter_VolumeNames
- TransferPrescriptParameter_ShadowCopyType=\$TransferPrescriptParameter_ShadowCopyType
- TransferPrescriptParameter_TransferConfiguration=\$TransferPrescriptParameter_TransferConfiguration
- TransferPrescriptParameter_StorageConfiguration=\$TransferPrescriptParameter_StorageConfiguration
- TransferPrescriptParameter_Key=\$TransferPrescriptParameter_Key
- TransferPrescriptParameter_ForceBaseImage=\$TransferPrescriptParameter_ForceBaseImage
- TransferPrescriptParameter_IsLogTruncation=\$TransferPrescriptParameter_IsLogTruncation
- TransferPrescriptParameter_LatestEpochSeenByCore=\$TransferPrescriptParameter_LatestEpochSeenByCore

Linux 上支持以下传输后脚本参数。

- TransferPostscriptParameter_VolumeNames=\$TransferPostscriptParameter_VolumeNames
- TransferPostscriptParameter_ShadowCopyType=\$TransferPostscriptParameter_ShadowCopyType
- TransferPostscriptParameter_TransferConfiguration=\$TransferPostscriptParameter_TransferConfiguration
- TransferPostscriptParameter_StorageConfiguration=\$TransferPostscriptParameter_StorageConfiguration
- TransferPostscriptParameter_Key=\$TransferPostscriptParameter_Key
- TransferPostscriptParameter_ForceBaseImage=\$TransferPostscriptParameter_ForceBaseImage
- TransferPostscriptParameter_IsLogTruncation=\$TransferPostscriptParameter_IsLogTruncation
- TransferPostscriptParameter_LatestEpochSeenByCore=\$TransferPostscriptParameter_LatestEpochSeenByCore

测试 Bourne Shell Scripting

您可以使用脚本 (.sh) 文件编辑器测试要运行的脚本。

① **注:** 如果前 Bourne Shell 脚本或后 Bourne Shell 脚本失败，则作业也会失败。有关作业的信息，请参阅 `/var/log/apprecovery/apprecovery.log` 文件。成功的脚本返回退出代码 0。

Bourne Shell Scripting 的输入参数

下表介绍了 Rapid Recovery 中 Bourne Shell 脚本的参数。

TransferPrescriptParameters_VolumeNames

下表显示 TransferPrescript 参数可用的对象。

表. 316: TransferPrescript 对象

方法	说明
<code>public VolumeNameCollection VolumeNames (get; set;)</code>	获取或设置用于传输的卷名称集合。 VolumeNames 是包含以下数据的数据结构： - GuidName。与卷关联的 Guid，如果未设置 DisplayName，则用作名称。 - DisplayName。卷的显示名称。
<code>public ShadowCopyType ShadowCopyType { get; set; }</code>	获取或设置用于传输的复制类型。ShadowCopyType 是具有值的枚举。可用的值包括： - Unknown - Copy - Full
<code>public string Key { get; set; }</code>	密钥方法将生成伪随机（而非密码保护）密钥，此密钥可用作验证传输请求的一次性密码。
<code>public bool ForceBaseImage { get; set; }</code>	获取或设置表示是否强制传输执行基本映像捕获的值。
<code>public bool IsLogTruncation { get; set; }</code>	获取或设置表示日志是否截断的值。
<code>public uint LatestEpochSeenByCore { get; set; }</code>	获取或设置最新的日期值。 LatestEpochSeenByCore 方法是 Core 创建的最近快照的序数。这是使用 VSS 创建此特定快照时筛选器驱动程序分配给该快照的“日期”。

TransferPostscriptParameter

下表显示 TransferPostscript 参数可用的对象。

表. 317: TransferPostscript 对象

方法	说明
<code>public VolumeNameCollection VolumeNames (get; set;)</code>	获取或设置用于传输的卷名称集合。 VolumeNames 是包含以下数据的数据结构： - GuidName。与卷关联的 Guid，如果未设置 DisplayName，则用作名称。 - DisplayName。卷的显示名称。
<code>public ShadowCopyType ShadowCopyType { get; set; }</code>	获取或设置用于传输的复制类型。ShadowCopyType 是具有值的枚举。可用的值包括： - Unknown - Copy - Full
<code>public string Key { get; set; }</code>	密钥方法将生成伪随机（而非密码保护）密钥，此密钥可用作验证传输请求的一次性密码。

方法	说明
<code>public bool ForceBaseImage { get; set; }</code>	获取或设置表示是否强制传输执行基本映像捕获的值。
<code>public bool IsLogTruncation { get; set; }</code>	获取或设置表示日志是否截断的值。
<code>public uint LatestEpochSeenByCore { get; set; }</code>	获取或设置最新的日期值。 LatestEpochSeenByCore 方法是 Core 创建的最近快照的序数。这是使用 VSS 创建此特定快照时筛选器驱动程序分配给该快照的“日期”。

示例 Bourne Shell 脚本

本部分介绍管理用户可用的示例 Bourne Shell 脚本以在受保护机器上运行。

- ⚠ **小心:** 本文中提供的示例 **Bourne** 脚本运行时将起到限定管理者设计的作用。修改运作脚本时采取预防措施，以保留工作版本。对此处包含的脚本示例做出的任何修改，或您创建的任何脚本，都被认为是自定义，这通常不在 **Dell Support** 涵盖的范围以内。
- ① **注:** 受保护机器将使用“**exec**”**shell** 命令启动脚本。您可以在脚本的第一行中定义有关信息以指示应运行脚本的解释器。如果未指定解释器，则默认 **shell** 将解释脚本。如果选择默认 **shell** 以外的解释器，则必须确保指定的解释器在所有受保护机器上可用。

受保护机器的示例脚本包括：

PreTransferScript.sh

PreTransferScript 在传输快照前于受保护机器上运行。

以下脚本将输入参数的值存储在 Pre(Post)TransferScriptResult.txt 中，该文件位于并存储在根主目录中。

示例 PreTransferScript

```
#!/bin/bash
echo "TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
TransferPrescriptParameter_LatestEpochSeenByCore=
$TransferPrescriptParameter_LatestEpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

PostTransferScript 在传输快照后于受保护机器上运行。

以下脚本将输入参数的值存储在 Pre(Post)TransferScriptResult.txt 中，该文件位于并存储在根主目录中。

示例 PostTransferScript

```
#!/bin/bash
echo "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
TransferPostscriptParameter_LatestEpochSeenByCore=
```

```
$TransferPostscriptParameter_LatestEpochSeenByCore" > ~/PostTransferScriptResult.txt  
exit 0
```

PostExportScript.sh

PostExportScript 在传输后于受保护机器上运行。

以下脚本将输入参数的值存储在 Pre(Post)ExportScriptResult.txt 中，该文件位于并存储在根主目录中。

示例 PostExportScript

```
#!/bin/bash  
echo  
"$curr_name-exported" > /etc/hostname  
exit 0
```

Rapid Recovery API

本节中的目的是简介和概述 Rapid Recovery Representational State Transfer (REST) 应用程序接口 (API)、它们的用法及功能。

Rapid Recovery Web Service API 是 REST 样式的，允许您自动化与自定义 Rapid Recovery 软件解决方案中的特定功能和任务，以帮助实现业务目标。

可从 Dell Data Protection | Rapid Recovery 许可证门户的[下载](#)页面访问这些 API。

主题：

- [目标用户](#)
- [使用 Rapid Recovery REST API](#)
- [下载并查看 Core 和 Agent API](#)
- [推荐的补充阅读](#)

目标用户

Rapid Recovery API 仅供要在应用程序中集成与扩展 Rapid Recovery 的应用程序开发者以及要要与 Rapid Recovery Core 服务器的互动编写脚本的管理员使用。

使用 Rapid Recovery REST API

Rapid Recovery API 是 REST 样式的 API，即它们使用 HTTP 请求提供通过 URI 路径对资源（数据实体）的访问。Rapid Recovery API 使用标准 HTTP 方法，例如，GET、PUT、POST 和 DELETE。由于 REST API 基于开放标准，因此您可使用任何支持 HTTP 调用的语言或工具。

应用程序开发者和管理员有两种使用 Rapid Recovery API 的方式。这两种方式如下：

- 使用 C# 或其他 .NET 语言以直接使用 Rapid Recovery .NET 客户端 DLL 文件。
- 直接与 HTTP 端点通信以生成您自己的 XML。

推荐第一种方法。客户端 DLL 包含在 Rapid Recovery SDK 中。调用 Rapid Recovery API 的方法与您使用任何 .NET 4.5X Windows Communication Foundation (WCF) 服务的方法一致。

下载并查看 Core 和 Agent API

Dell Data Protection | Rapid Recovery 软件开发者套件 (SDK) 包括 Rapid Recovery Core 和 Rapid Recovery Agent 组件的 REST API 以及样本和支持文件。这些内容均包含在以下文件夹中，然后压缩成包括以下组件的存档：

表. 318: SDK 存档中包括的组件

文件夹名称	目录	说明
Core.Contracts	Rapid Recovery Core API	包含 API 以帮助开发者或管理员为 Rapid Recovery Core 中的功能编写脚本。有两套服务合约。

文件夹名称	目录	说明
		1 在 Web 浏览器中打开 CoreWeb.Client HTML 文件以查看有关一般 REST 标准的信息。其中列出了服务合约。当您单击任何相应的超链接统一资源标识符 (URI) 时，浏览器会打开 Core.Contracts/docWeb/ 目录中的信息。出现的页面显示了有关一般 REST 服务操作的信息，包括方法和说明。 2 在 Web 浏览器中打开 Core.Client HTML 文件以查看详细的 C# 信息。当您单击任何超链接服务合约（类）时，浏览器会打开 Core.Contracts/doc/ 目录中的信息。出现的页面显示了选定类中所有 C# 方法的详细信息。
Agent.Contracts	Rapid Recovery Agent API（已摒弃）	包含开发者或管理员可用于操作受保护机器上的 Rapid Recovery Agent 的 API。  小心: Agent API 已被摒弃，并将从未来的 SDK 版本中移除。不建议直接操作 Agent API。对于这些 API 的使用将被视为自定义，并且不会受到支持。出于历史记录的原因，说明文件中提供了此信息。 1 在 Web 浏览器中打开 AgentWeb.Client HTML 文件以查看有关一般 REST 标准的信息。 2 在 Web 浏览器中打开 Agent.Client HTML 文件以查看详细的 C# 信息。
AppRecoveryAPI Samples	代码示例和动态链接库	AppRecoveryAPISamples 包含使用 C# 编程语言编写的代码示例。如果使用 API 来自定义您的 GUI、管理系统等，这些文件代表了用于查看代码片段的良好起点。 AppRecoveryAPISamples\Dependencies 包含 Rapid Recovery Core 使用的动态链接库 (DLL) 文件。DLL 包含数据合约（Core 熟悉的类型）和服务合约（可用于强制 Core 执行某个操作的管理方法和操作）。如果您想自定义您自己的图形用户界面，或使用管理系统处理 Rapid Recovery Core，则需要这些 DLL。  注: 使用的 DLL 版本必须与 Core 版本相匹配。

您可以用存档的形式下载 SDK (API-Reference-x.x.x-xxxx)。每个 x 代表相关版本的内部版本号中的一个数字。

完成以下过程中的步骤以获取 SDK，将其下载到指定的目标位置，然后解压缩文件以准备使用 Core 和 Agent API。

- 1 登录到 Dell Data Protection | Rapid Recovery 许可证门户（网址为 <https://licenseportal.com>）。
- 2 在许可证门户的左侧导航菜单中，单击 **下载**。
此时会显示许可证门户的 **下载** 页面。
- 3 在 **下载** 页面的“基于 Windows 的应用程序”部分中，向下滚动到 SDK 的说明，然后单击 **下载**。
- 4 将下载的存档保存到您的首选位置。
- 5 解压缩存档。
在新的 API-Reference-x.x.x-xxxx 文件夹中，您可以看到单独的各组文件，如以上表所述。
- 6 在 Web 浏览器打开上表所述的密钥 HTML 文件以查看有关 API 的指南。

推荐的补充阅读

*Dell Data Protection | Rapid Recovery 安装和升级指南*概述了 Rapid Recovery 体系结构，并介绍了用于安装 Rapid Recovery 组件以及从较早版本升级 Core 或 Agent 组件的必要步骤。

您可以从以下链接查看或下载该指南：<https://support.software.dell.com/rapid-recovery/release-notes-guides/>。

Dell 致力于倾听客户的需求，提供客户所信赖和注重的全球创新技术、业务解决方案与服务。有关更多信息,请访问 <http://software.dell.com>。

联系 Dell

有关销售或其他询问问题，请访问 <http://software.dell.com/company/contact-us.aspx> 或拨打 + 1-949-754-8000。

技术支持资源

已购买 Dell 软件且拥有有效维护合同的客户及拥有试用版产品的客户均可享受技术支持服务。要访问支持门户网站，请转到 <https://support.software.dell.com>。

支持门户网站无限时全天候提供各种自助工具，您可以使用这些工具快速且独立地解决问题。此外，支持门户网站可通过在线服务请求系统直达产品支持工程师。

支持门户网站使您可以：

- 创建、更新和管理服务请求（案例）。
- 查看知识库文章。
- 获取产品通知。
- 下载软件。有关试用软件，请转至 <http://software.dell.com/trials>。
- 参与社区讨论。

Agent

Rapid Recovery Agent 是安装到物理或虚拟机上的软件，为 Rapid Recovery Core 增加保护。

Rapid Recovery

通过将备份、复制和恢复整合到一个解决方案中，Rapid Recovery 树立了新的统一数据保护标准，此解决方案旨在成为保护虚拟机 (VM) 以及物理和云环境的最快、最可靠的备份方案。

基本映像

保存到 Core 的首次备份传输称为基本映像快照。所有指定卷上的所有数据（包括操作系统、应用程序和设置）将保存到 Core。有关详情，请参阅[快照](#)。

Central Management Console

Rapid Recovery Central Management Console 是一个可选组件，面向具有两个或更多 Rapid Recovery Core 的环境。此组件是一个 Web 门户，其提供一个中央界面，在其中，您可以使用基于 Web 的单一界面分组、管理和生成多个 Core 的报告。

校验和

校验和是一项创建数据块功能，其创建的数据块用于检测传输或存储过程中产生的意外错误。

群集

请参阅 [Windows 故障转移群集](#)。

Cluster Continuous Replication (CCR)

CCR 是一种非共享存储故障转移群集解决方案，它采用内置的异步日志传送技术，可在故障转移群集中的辅助服务器上为每个存储组创建和维护一个副本。CCR 旨在作为一种单数据中心或双数据中心解决方案，提供高可用性和站点弹性。它是 Exchange 2007 中可用的两种群集邮箱服务器 (CMS) 部署之一。

群集节点

群集节点是指作为 Windows 故障转移群集一部分的单台机器。

压缩

网络存储行业协会 (SNIA) 将压缩定义为对数据进行编码以减小数据大小的过程。

Core

Rapid Recovery Core 是 Rapid Recovery 体系结构的中心组件。Core 提供备份、恢复、保留、复制、存档和管理的核心服务。就复制而言，Core 也称为源 Core。源 Core 是发起复制的 Core，而目标 Core 是复制到的目标（在自己的专用服务器上的另一个 Rapid Recovery Core，受保护机器或群集在此处复制）。

Core Console

Rapid Recovery Core Console 是一种基于 Web 的界面，可用于全面管理 Rapid Recovery Core。

数据库可用性组 (DAG)

DAG 是指一组 Microsoft Exchange Server 2010 邮箱服务器（最多 16 台），这些服务器自动从数据库、服务器或网络故障进行数据库级恢复。DAG 使用连续复制和部分 Windows 故障转移群集技术提供高可用性和站点弹性。DAG 中的邮箱服务器可相互监测对方是否发生故障。邮箱服务器添加至 DAG 后，将与 DAG 中的其他服务器配合工作，以自动从数据库故障进行数据库级恢复。

加密

数据加密的目的是仅供具有相应解密密钥的授权用户访问。使用密码块链 (CBC) 模式下的 256 位 AES 加密数据。在 CBC 中，每个数据块在加密前使用之前的密文块执行逻辑异或，采用这种方式，每个新的密文块均依赖所有先前的密文块。密码短语用作初始化向量。

事件

事件是 Core 登录的过程。通过在图标栏内单击 （事件）图标，以在 Core Console 内查看事件。当您单击 （事件）图标时，默认视图显示**任务**页面。此视图显示与作业相关的事件。向您发出通知的优先级事件可在**警报**页面查看。所有事件的日志显示在**日记**页面。通过设置或修改现有通知组，您可以自定义任何事件通知。此操作可通过将其显示在**警报**页面上提高事件的优先级。系统将使用组别通知选项中的通知方法集通知通知组内的成员。

全局重复数据消除

存储网络行业协会 (SNIA) 将重复数据消除定义为使用共享备份引用替换多个粒度级别的数据的多个备份，从而节省存储空间或带宽。Rapid Recovery 卷管理器在逻辑卷中执行全局重复数据消除。重复数据消除的粒度级别为 8 KB。Rapid Recovery 中重复数据消除的范围限制为使用相同存储库和加密密钥的受保护机器。

增量快照

增量快照是仅由上次备份后的受保护机器更改的数据的备份组成。这将基于定义的间隔定期保存到 Core（例如，每 60 分钟）。有关详情，请参阅[快照](#)。

许可证密钥

许可证密钥是注册 Rapid Recovery 软件或设备的一种方法。（您也可以使用许可证文件。）在 Dell Data Protection | Rapid Recovery 许可证门户上注册帐户时，您可以获取许可证密钥或文件。有关详情，请参阅[许可证门户](#)。

许可证门户

Dell Data Protection | Rapid Recovery 许可证门户是一个 Web 界面，在其中，用户和合作伙伴可以下载软件、注册 Rapid Recovery 设备和管理许可证订阅。许可证门户用户可以注册帐户、下载 Rapid Recovery Core 和 Agent 软件、管理组、跟踪组活动、注册机器、注册设备、邀请用户以及生成报告。有关更多信息，请参阅 *Dell Data Protection | Rapid Recovery 许可证门户用户指南*。

Live Recovery

Rapid Recovery Live Recovery 是虚拟机和服务器的即时恢复技术。该技术能够让您几乎连续地访问虚拟服务器或物理服务器上的数据卷，可在接近于零的 RTO 和仅数分钟的 RPO 内恢复整个卷。

Local Mount Utility

Local Mount Utility (LMU) 是一个可下载应用程序，用于从任何机器在远程 Rapid Recovery Core 上安装恢复点。

日志截断

日志截断是一种从事务日志删除日志记录的功能。对于 SQL Server 机器，您强制截断 SQL Server 日志时，此过程将确定 SQL 服务器可用空间量。对于 Exchange Server 机器，您强制截断 Exchange Server 日志时，此操作将释放 Exchange 服务器空间。

管理角色

Rapid Recovery Central Management Console 引入了管理角色的新概念，通过管理角色，可在受信数据和服务管理员之间划分管理责任以及访问权限控制，从而支持安全而高效的管理委派。

可安装性

Exchange 可安装性是一项损坏检测功能，可在发现潜在故障时提醒管理员，并确保 Exchange Server 上的所有数据均可在出现故障时成功恢复。

对象文件系统

Rapid Recovery 可扩展对象存储是一个对象文件系统组件。它将所有数据块（派生出快照的来源）当作对象，并用于存储、检索、维护和复制这些对象。它专用于与全局重复数据消除、加密和保留管理一起提供可扩展的输入和输出 (I/O) 性能。对象文件系统直接与行业标准存储技术接合。

密码短语

密码短语是在加密数据时所使用的密钥。如果密码短语丢失，则无法恢复数据。

PowerShell Scripting

Windows PowerShell 是一个与 Microsoft .NET Framework 相连的环境，旨在实现管理自动化。Rapid Recovery 包括用于 PowerShell 脚本的完整客户端 SDK，该脚本允许管理员通过直接执行命令或利用脚本执行命令来实现 Rapid Recovery 资源的自动化管理。

禁止字符

禁止字符是命名 Rapid Recovery Core Console 中的对象时不应使用的字符。例如，当定义受保护机器的显示名称时，不要使用以下任何特殊字符：

表. 319: 禁止字符

字符	字符名称	禁止自
?	问号	机器显示名称、加密密钥、存储库、路径说明
	管道	机器显示名称、加密密钥、存储库、路径说明
:	冒号	机器显示名称、加密密钥、存储库 指定路径时，支持使用此符号；例如，c:\data。
/	斜杠	机器显示名称、加密密钥、存储库、路径说明
\	反斜杠	机器显示名称、加密密钥、存储库 指定本地或网络路径时，支持使用此符号；例如，c:\data 或 \\ComputerName\SharedFolder\
*	星号	机器显示名称、加密密钥、存储库、路径说明
"	引号	机器显示名称、加密密钥、存储库、路径说明
<	左尖括号	机器显示名称、加密密钥、存储库、路径说明
>	右尖括号	机器显示名称、加密密钥、存储库、路径说明

禁止短语

禁止短语是不应作为 Rapid Recovery Core Console 中的任何对象名称的短语（或字符集），因为它们为操作系统使用所预留。最佳实践是，尽可能避免使用这些短语。例如，当定义受保护机器的显示名称时，不要使用以下任何短语：

表. 320: 禁止短语

短语	一般用途	禁止自
con	控制台	机器显示名称、加密密钥、存储库、路径说明
prn	打印机端口	机器显示名称、加密密钥
aux	辅助端口	机器显示名称、加密密钥
nul	空值	机器显示名称、加密密钥
com1、com2... 到 com9	通信端口	机器显示名称、加密密钥
lpt1、lpt2... 到 lpt9	行打印终端端口	机器显示名称、加密密钥、存储库、路径说明

受保护机器

受保护机器 - 有时也称为“代理程序”- 是在 Rapid Recovery Core 中受保护的物理计算机或虚拟机。按照预定义的保护间隔时间，备份数据从受保护机器传输到 Core 中指定的存储库。基本映像将所有数据传输到恢复点（包括操作系统、应用程序和设置）。

每个后续的增量快照仅提交受保护机器的指定磁盘卷上发生更改的数据块。基于软件的受保护机器安装有 Rapid Recovery Agent 软件。也可以通过无代理程序的方式保护一些虚拟机，其中存在一些限制。

Quorum

Quorum 是指在故障转移群集中使给定群集持续运行所需联机的元素数量。此处所说的元素是指群集节点。此术语也指用于维护群集恢复所需配置数据的所选 Quorum 型资源。此数据包含已应用于群集数据库的所有更改的详细信息。一般来说，其他群集资源均可访问 Quorum 资源，因此，任何群集节点均可访问数据库的最新更改。默认情况下，每个服务器群集只有一个 Quorum 资源。具体的 Quorum 配置（故障转移群集设置）将决定出现多少故障时会阻止群集运行。

恢复点

恢复点是各个磁盘卷的快照集合。例如 C:、D: 和 E:。

仅有恢复点的机器

仅有恢复点的机器在 Core 上代表来自先前在 Core 上受保护的、但已删除的机器的恢复点。如果您删除复制，但保留恢复点，这同样会导致仅有恢复点的机器。可以在文件级别查看和恢复信息。您不能使用仅有恢复点的机器执行 BMR 或还原完整卷，也不可以向仅有恢复点的机器添加更多数据。

远程 Core

远程 Core 表示使用 Local Mount Utility 或 Central Management Console 的非 Core 机器访问的 Rapid Recovery Core。

复制

复制是从 Rapid Recovery Core 复制恢复点并将其发送至另一个 Rapid Recovery Core 以满足灾难恢复目的的过程。此过程需要两个或多个 Core 之间配对的“源-目标”关系。复制按受保护的机器进行管理。可以将任何源 Core 上的受保护或复制机器（或全部机器）配置为复制到目标 Core。恢复点被复制到目标 Core。

存储库

存储库是 Rapid Recovery Core 上的基本映像与从受保护机器中捕获的增量快照的集合。存储库必须存储在快速的主要存储设备上。DVM 存储库的存储位置可以是在 Core 机器上（在这种情况下，它仅通过受支持的 Windows 操作系统来托管）。它可以使用直接连接存储，存储区域网络或一个适当级别的网络连接服务器。

REST API

Representational State Transfer (REST) 是一个专为可扩展性而设计的简单无状态软件体系结构。Rapid Recovery 为其应用程序接口 (API) 使用此体系结构以自动执行和自定义某些功能和任务。为 Core 功能和受保护机器（代理程序）功能提供了一组独立的 REST API。

还原

从 Rapid Recovery Core 上保存的恢复点恢复机器上的一个或多个存储卷的过程被称为执行还原。这之前被称为回滚。

保留

保留定义了受保护机器的备份快照在 Rapid Recovery Core 上存储的时间长度。保留策略通过前滚进程在恢复点上强制执行。

汇总

汇总进程是一种内部夜间维护程序，通过压缩和消除过时的恢复点来强制执行保留策略。Rapid Recovery 仅减少对元数据的汇总操作。

播种

播种是指在复制中初始传输受保护代理的基本映像（已消除重复数据）和增量快照的过程，此过程可增加高达数百乃至数千 GB 的数据。首次复制可以使用外部介质播种至目标 Core，这对大型数据集或链接速度慢的站点来说非常有用。

服务器群集

请参阅 [Windows 故障转移群集](#)。

SharePoint 备份

SharePoint 备份是一个数据副本，用于在系统故障后还原和恢复 SharePoint 服务器上的数据。从 SharePoint 备份，您可以执行完整 SharePoint 服务器场或服务场的一个或多个组件的还原。

单一副本群集

单一副本群集是一种共享存储故障转移群集解决方案，在群集节点共享的存储上使用存储组的单一副本。它是 Exchange 2007 中可用的两种群集邮箱服务器部署之一。

Smart Agent

Rapid Recovery Smart Agent 安装在受 Rapid Recovery Core 保护的机器上。Smart Agent 追踪磁盘卷上发生更改的数据块并以预定义的保护时间间隔创建已更改数据块的快照。

快照

快照是一个常见的行业术语，用于定义当应用程序正在运行时，获取和存储指定磁盘卷状态的能力。当发生停机或系统故障而需要进行系统恢复时，快照就至关重要。Rapid Recovery 快照具有应用程序感知能力，这表示在创建快照前，所有开放性事务以及滚动事务日志均已完成，同时高速缓存已刷新。Rapid Recovery 使用 Microsoft 卷影服务 (VSS) 来帮助创建应用程序崩溃一致性快照。

SQL 可附加性

SQL 可连接性是在 Rapid Recovery Core 中运行的一项测试，用于确保所有 SQL 恢复点无误并可在发生故障时进行备份。

SQL 备份

SQL 备份是一个数据副本，用于在系统故障后还原和恢复 SQL 服务器上的数据。从 SQL 备份，您可以执行完整 SQL 数据库或 SQL 数据库的一个或多个组件的还原。

SQL 差异备份

差异数据库备份是上次完整备份 SQL 数据库后的所有数据更改的累积副本。差异备份通常较创建完整数据库备份更快，并减少恢复数据库所需的事务日志数量。

目标 Core

目标 Core 有时也称为副本 Core，它是从源 Core 接收所复制数据（恢复点）的 Rapid Recovery Core。

Transport Layer Security

Transport Layer Security (TLS) 是用于确保互联网通信安全的现代加密网络协议。互联网工程任务组定义的此协议是安全套接字层 (SSL) 的替代技术。SSL 仍普遍使用，且这两种协议可互操作（TLS 客户端可降级与 SSL 服务器通信）。

True Scale

True Scale 是 Rapid Recovery 的可扩展架构。

Universal Recovery

Rapid Recovery Universal Recovery 技术提供无限的机器还原灵活性。它可用于从/向任何所选物理或虚拟平台执行整体恢复，也可以从任何物理或虚拟源向虚拟机执行增量恢复更新。它还可以对单独的文件、文件夹、电子邮件、日历项目、数据库和应用程序执行应用程序级、项目级和对象级恢复。

Verified Recovery

Verified Recovery 技术用于执行自动恢复测试和备份验证。该技术支持多种文件系统和服务器。

Virtual Standby

Virtual Standby 是一个过程，用于创建受保护机器的克隆虚拟机。原始源机器可以是物理或虚拟，但产品始终为虚拟。您可以按需一次性创建虚拟待机，或者您可以定义要求以创建可引导的虚拟机，然后在从原始受保护机器上捕获每个快照后持续更新它。

卷管理器

Rapid Recovery 卷管理器用于管理对象，并存储对象以及将对象显示为逻辑卷。它利用动态管道架构提供 TruScale 可扩展性、并行性以及异步输入和输出 I/O 模型，从而实现高吞吐量，同时最大限度地降低 I/O 延迟。

空白标签

Rapid Recovery 为备份和灾难恢复服务提供商提供了空白标签或改名功能，可将 Rapid Recovery 更改为提供商自己的品牌名称，然后将其作为自有产品或服务进行销售或分发。

Windows 故障转移群集

Windows 故障转移群集是指一个独立计算机组，这些计算机配合工作以提高应用程序和服务的可用性。群集服务器（称为节点）由软件和物理电缆连接。如果其中一个群集节点发生故障，则由另一个节点开始提供服务（这一过程称为故障转移）。这可以最大限度地缩短用户的服务中断时间。Rapid Recovery 支持对多种 SQL Server 和 Exchange Server 群集提供保护。