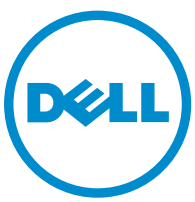
Dell DL4300 设备
用户指南



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。

2015 - 12

Rev. A01

目录

1

Dell DL4300 设备简介

本章介绍并概述 DL4300。其中描述了特性、功能和架构，并含有以下主题：

- 核心技术
- True Scale 架构
- 部署架构
- 产品功能

您的设备为统一数据保护树立了新的标准，它将备份、复制和恢复集成到一个解决方案中，可为保护虚拟机 (VM)、物理机和云环境提供最快、最可靠的备份。

您的设备借助内置的全局重复数据消除、压缩、加密和复制到任何私有云或公共云基础结构，最多能够处理数拍字节的数据。服务器应用程序以及数据可以在数分钟内恢复，以进行数据保留 (DR) 和符合规定。

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。

该设备结合了以下技术：

- 实时恢复
- 验证恢复
- 通用恢复
- 真正全局重复数据消除

这些技术针对云灾难恢复设计了安全集成，并提供快速而可靠的恢复。借助可扩展的对象存储，以及内置的全局重复数据消除、压缩、加密和复制到任何私有云或公共云基础结构，您的设备能够独一无二、非常迅速地处理最高达数拍字节的数据。

AppAssure 通过其核心技术以及对多虚拟机监控程序环境（包括那些在 VMware vSphere 和 Microsoft Hyper-V 上运行、由私有云和公共云组成的环境）的支持来应对传统工具的复杂性和低效问题。在提供这些技术优势的同时，AppAssure 还能够大幅降低 IT 管理和存储成本。

核心技术

以下主题详细介绍了 AppAssure 核心技术。

实时恢复

实时恢复是一种面向 VM 或服务器的即时恢复技术。通过该技术，可几乎不间断地访问虚拟服务器或物理服务器上的数据卷。在恢复整个卷时，可达到接近于零的 RTO 和仅需数分钟的 RPO。

备份和复制技术可记录多个 VM 或服务器的并发快照，提供近乎瞬时的数据和系统保护。您可以直接从备份文件恢复服务器的使用，无需等待生产存储完全还原。这样不仅可使用户保持生产效率，还能帮助 IT 部门缩短恢复时间，因而可满足当今日趋严格的恢复时间目标 (RTO) 和恢复点目标 (RPO) 服务级别协议要求。

验证恢复

验证恢复可确保您执行自动恢复测试和备份验证。它包括但不限于文件系统：Microsoft Exchange 2007、2010 和 2013，以及 Microsoft SQL Server 2005、2008、2008 R2、2012 和 2014 各种版本。验证恢复能够确保在虚拟和物理环境中恢复应用程序和备份。它采用全面的完整性检查算法，该算法基于 256 位 SHA 密钥，可在存档、复制和数据播种操作期间检查备份中每个磁盘块是否正确。这能够确保及早发现数据损坏，防止在备份过程中保留或传输损坏的数据块。

通用恢复

通用恢复技术为机器还原赋予了无限的灵活性。可以从物理系统向虚拟机、从虚拟机向虚拟机、从虚拟机向物理系统或从物理系统向物理系统还原备份，还可以将裸机还原到不同类型的硬件。例如 P2V、V2V、V2P、P2P、P2C、V2C、C2P 和 C2V。

通用恢复技术还能够加快虚拟机之间跨平台迁移的速度，例如从 VMware 迁移至 Hyper-V 或从 Hyper-V 迁移至 VMware。此外，此技术内置应用程序级、项目级和对象级恢复功能（恢复对象包括：个别文件、文件夹、电子邮件、日历项、数据库和应用程序）。借助 AppAssure，还可以从物理机到云或从虚拟机到云恢复或导出。

真正全局重复数据消除

设备提供真正全局重复数据消除功能，该功能通过 50:1 以上的空间缩减率来降低物理磁盘驱动器容量要求，同时仍满足数据存储要求。AppAssure True Scale 采用具有线速性能的内联块级压缩和重复数据消除功能，以及内置完整性检查，可防止数据损坏影响备份和存档过程的质量。

True Scale 架构

您的设备基于 AppAssure True Scale 架构构建。它利用动态多核管道架构，该架构经过优化，可为您的企业环境提供始终如一的可靠性能。True Scale 经过全新设计，可在不影响性能的情况下，实现线性扩展、高效存储、管理大数据以及分钟级的 RTO 和 RPO。它包括专用的对象和卷管理器，具有集成的全局重复数据消除、压缩、加密、复制和保留功能。下图展示了 AppAssure True Scale 架构。

图 1: AppAssure True Scale 架构

AppAssure 卷管理器和可扩展对象存储是 AppAssure True Scale 架构的基础。可扩展对象存储能够存储从虚拟服务器和物理服务器捕获的块级快照。卷管理器通过提供通用存储库或仅在必要时提供即时存储来管理众多对象存储。对象存储支持所有并发操作，它采用异步 I/O，可实现高吞吐量并最大限度减少延迟和提高系统利用率。存储库可以驻留在不同存储技术中，例如存储区域网络 (SAN)、直接连接存储 (DAS) 或网络连接存储 (NAS)。

AppAssure 卷管理器的作用与操作系统中卷管理器的作用类似，可对大小和类型各异的不同存储设备进行管理，并按照分条或顺序分配策略将这些设备整合至逻辑卷中。对象存储会对来自应用程序感知快照的对象进行保存、检索和维护，然后复制这些对象。卷管理器能够实现可扩展的 I/O 性能，可与全局重复数据消除、加密和保留管理配合使用。

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，AppAsure 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、组和用户。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。

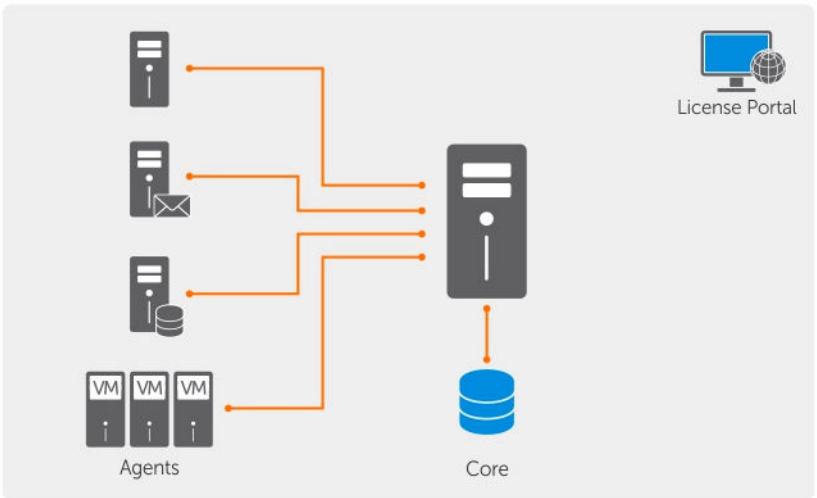


图 2: 基本部署架构

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。

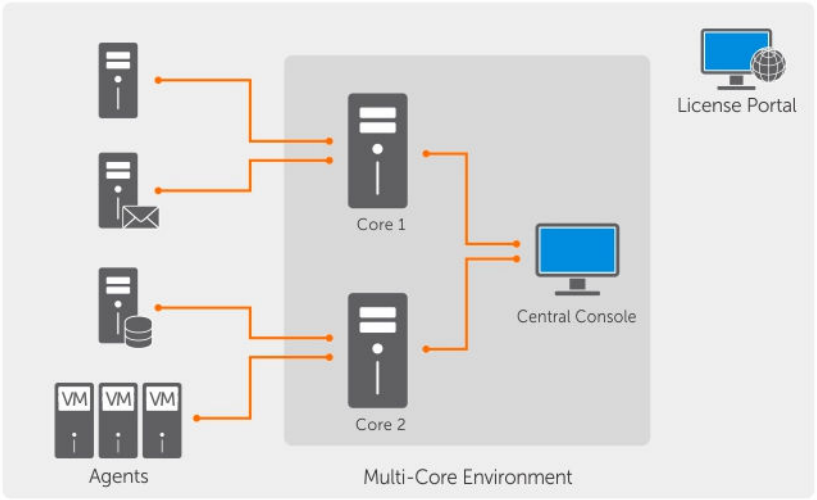


图 3: 多 Core 部署架构

Smart Agent

Smart Agent 会跟踪磁盘卷上更改的块，然后以预定义的保护间隔创建更改块的映像的快照。增量永久性块级别快照方法可防止反复将相同数据从受保护机器复制到 Core。Smart Agent 安装在由 Core 保护的机器上。

Smart Agent 具有应用程序感知功能并且在不使用时为休眠状态，CPU 利用率百分比接近零 (0) 并且内存开销小于 20 MB。当 Smart Agent 处于活动状态时，占用的处理器利用率最高为 2% 到 4%，内存不到 150 MB，其中包括将快照传输至 Core。

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 AppAssure 代理软件后，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。

DL4300 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 位版本的 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

快照流程是指将基本映像从受保护机器传输至 Core 的过程。仅在此时会在正常工作状态下将机器的完整副本在网络上传输，然后是创建增量快照。AppAssure Agent software for Windows 使用 Microsoft Volume Shadow copy Service (VSS) 来冻结和静默指向磁盘的应用程序数据以捕获文件系统一致并且应用程序一致的备份。如果创建了快照，VSS 以及目标服务器上的编写器会阻止将内容写入磁盘。如果向磁盘写入内容停止，则所有磁盘 I/O 操作会列队并仅在快照完成后才恢复，同时进行中的操作已完成，并且所有打开的文件已关闭。创建卷影副本的过程不会明显影响生产系统的性能。

由于本身支持所有 Windows 内部技术（例如 NTFS、注册表和 Active Directory 等），AppAssure 使用 Microsoft VSS 在创建快照之前将数据刷新到磁盘。此外，其他企业应用程序（例如 Microsoft Exchange 和 SQL）使用 VSS 编写器插件在准备创建快照和必须将已使用的数据库页面刷新到磁盘时获得通知，从而使数据库保持一致的事务性状态。请务必注意，VSS 的作用是将磁盘上的系统和应用程序数据置于静默状态，并不用于创建快照。捕获的数据会被立即传输并存储至 Core。使用 VSS 进行备份并不会使应用程序服务器长时间处于备份模式，因为创建快照的时间长度仅持续数秒，而非数小时。使用 VSS 进行备份的另一个好处在于，由于快照在卷级执行，AppAsssure 代理软件 可以一次创建大量数据的快照。

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：

- 存储库
- 真正全局重复数据消除（功能）
- 加密
- 复制
- 恢复即服务 (RaaS)
- 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

存储库

存储库使用重复数据消除卷管理器 (DVM) 实现支持多个卷的卷管理器，每个卷均可以驻留在不同的存储技术上，例如存储区域网络 (SAN)、直接连接存储 (DAS)、网络连接存储 (NAS) 或云存储。每个卷均包含具有重复数据消除功能的可扩展对象存储。可扩展对象存储相当于基于记录的文件系统，其中的存储分配单元是大小固定的数据块，被称作“记录”。此架构允许您为压缩和重复数据消除配置块级支持。前滚操作从磁盘密集型操作降低为元数据操作，因为前滚不再移动数据，而只移动记录。

DVM 能够将一系列对象存储整合至一个卷，可通过创建附加系统文件进行扩展。对象存储文件预先经过分配，可以随存储要求的变化按需添加。一个 Core 上最多可以创建 255 个独立存储库，通过添加新的文件范围还可以进一步扩大存储库大小。扩展后的存储库可包含多达 4096 个跨越不同存储技术的范围。存储库大小的上限是 32 EB。一个 Core 中可以存在多个存储库。

真正全局重复数据消除

真正全局重复数据消除是通过消除冗余或重复数据来降低备份存储需求的有效方法。重复数据消除非常有效，因为存储库中只存储多个备份中独一无二的数据实例。冗余数据也进行了存储，但并非物理存储，而只是使用指向存储库中独一无二数据实例的指针来代替。

传统备份应用程序每周都执行重复性完全备份，但是您的设备对机器执行增量数据块级备份。这种一直持续的增量方法与重复数据消除配合使用，有助于大幅降低提交至磁盘的数据总量。

典型的服务器磁盘布局包括操作系统、应用程序和数据。在大多数环境下，管理员通常在多个系统中使用通用的服务器和桌面操作系统风格，以便进行有效的部署和管理。跨多台机器同时进行数据块级备份时，无论源如何，都能够更加详细地看到备份中包含和不包含的内容。此数据包括整个环境中的操作系统、应用程序和应用程序数据。

图 4: 重复数据消除的图表

您的设备执行基于目标的内联重复数据消除，这表示先将快照数据传输至 Core，然后再执行重复数据消除。内联重复数据消除是指数据在提交至磁盘之前已消除重复内容。这种方法与源位置重复数据消除或后处理重复数据消除不同。源位置重复数据消除是在源位置执行重复数据消除，然后再传输至目标进行存储；而后处理重复数据消除是先将原始数据发送至目标，并在将数据提交至磁盘之后执行分析和重复数据消除。源位置重复数

据消除会消耗机器上宝贵的系统资源，而后处理重复数据消除方法要求在执行重复数据消除过程之前将所需的全部数据都存入磁盘（初始容量开销较大）。另一方面，在源或 Core 上，内联重复数据消除不需要附加的磁盘容量和 CPU 周期来执行重复数据消除过程。最后，传统备份应用程序每周执行重复性完全备份，而您的设备则一直对机器执行持续的增量数据块级备份。这种一直持续的增量方法与重复数据消除配合使用，有助于大幅降低提交至磁盘的数据总量，缩减比率高达 50:1。

加密

设备提供集成式加密功能来保护备份和静态数据，防止未经授权的访问和使用，从而确保数据隐私。只有具备加密密钥的用户才能访问和解密数据。系统中可以创建和存储的加密密钥数量不受限制。在密码块链 (CBC) 模式中，DVM 采用 256 位密钥实施 AES 256 位加密。快照数据加密采用线速内联方式执行，不会对性能造成影响。这是因为 DVM 采用多线程实现，它会针对部署所在的处理器应用硬件加速。

加密功能可直接应用于多租户环境。重复数据消除专门限于那些已由相同密钥加密的记录；即不会对两个由不同密钥加密的相同记录执行重复数据消除。此设计确保无法利用重复数据消除在不同的加密域之间泄露数据。这对于托管服务提供商来说非常有利，因为多租户（客户）的复制备份可以存储在一个 Core 中，而任何租户都不能查看或访问其他租户的数据。每个活动的租户加密密钥均可以在存储库中创建一个加密域，只有密钥的所有者才能查看、访问或使用其中的数据。在多租户方案中，数据在加密域内已经过分区和重复数据消除。

在复制方案中，设备使用 SSL 3.0 来保护复制拓扑中两个 Core 之间的连接安全，防止窃听和篡改。

复制

复制是从 AppAssure Core 复制恢复点并将其传输至不同位置的另一个 AppAssure Core 以进行灾难恢复的过程。该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，然后异步并且连续地将增量快照数据传输至远程灾难恢复站点的目标 Core。您可将出站复制配置为公司拥有的数据中心或远程灾难恢复站点（即自管目标 Core）。或者，可以将出站复制配置为第三方托管的服务提供商 (MSP) 或托管非现场备份和灾难恢复服务的云。在复制到第三方目标 Core 时，您可使用可让您请求连接并接收自动反馈通知的内置工作流。

复制以每个受保护机器为基础进行管理。在源 Core 上受保护或复制的任何机器（或所有机器）都可配置为复制到目标 Core。

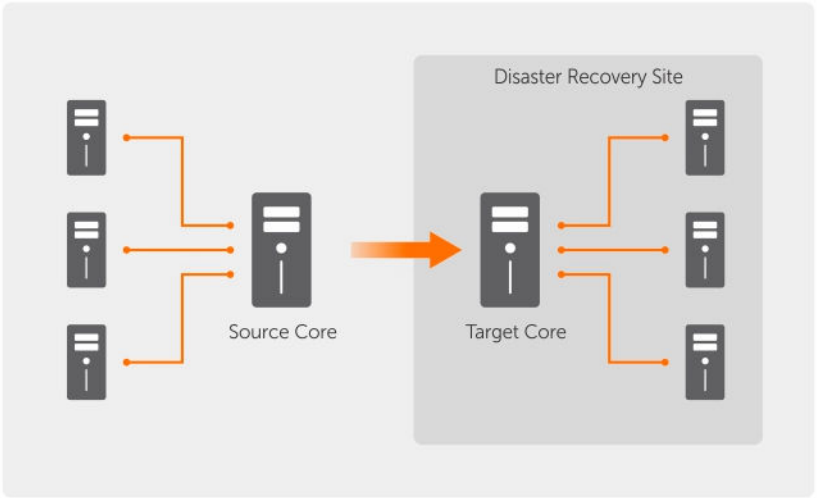


图 5: 基本复制架构

复制能够通过与重复数据消除紧密结合的独特读写匹配 (RMW) 算法进行自我优化。借助 RMW 复制，源和目标复制服务能够在传输数据之前与密钥进行匹配，然后仅通过 WAN 复制已经过压缩、加密和重复数据消除的数据，最终可将带宽需求降低至原来的十分之一。

复制过程从播种开始。播种是指初始传输受保护机器的基本映像（已消除重复数据）和增量快照的过程。这些数据总计可达数百乃至数千 GB。初始复制时可以使用外部介质播种到目标 Core。这对大型数据集或具有慢速链路的站点来说非常有用。播种存档中的数据已经过压缩、加密和重复数据消除。如果存档的总大小超过外部介质上的可用空间，则可以跨越多台设备进行存档。在播种过程中，系统会将增量恢复点复制到目标站点。将数据传输到目标 Core 后，新复制的增量恢复点会自动同步。

恢复即服务 (RaaS)

托管服务提供商 (MSP) 可以充分利用设备，将其作为一种交付恢复即服务 (RaaS) 的平台。RaaS 将客户的物理和虚拟服务器及其数据复制到服务提供商的云，将其作为虚拟机为恢复测试或实际恢复操作提供支持，以加快完成云中恢复过程。希望进行云中恢复的客户可以配置从本地 Core 上的受保护机器复制到 AppAssure 服务提供商。如果发生灾难，MSP 可以立即为客户启动虚拟机。

托管服务提供商可部署多租户 AppAssure RaaS 基础结构，该结构能够托管多个通常不会在一台或一组服务器上共享安全或数据的独立组织或业务部门（租户）。各租户的数据相互隔离并进行保护，其他租户或服务提供商无法访问。

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。

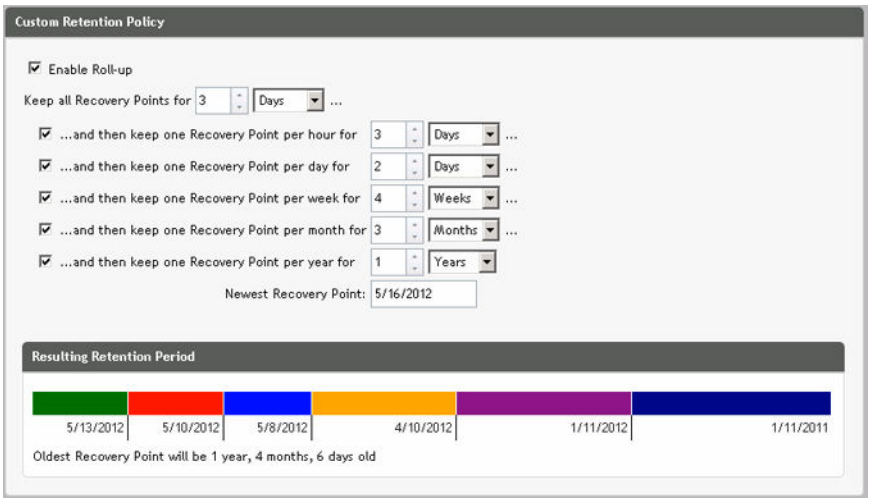


图 6: 自定义保留策略

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。

2

使用 DL4300 Core

访问 DL4300 Core 控制台

要访问 Core 控制台，请执行以下操作：

1. 在浏览器中更新可信站点。请参阅在 Internet Explorer 中更新可信站点。
2. 配置浏览器以远程访问 Core 控制台。请参阅配置浏览器以远程访问 Core 控制台。
3. 要访问 Core 控制台，请执行以下操作之一：
   - 从本地登录到 DL4300 Core 服务器，然后双击 **Core Console（Core 控制台）**图标。
   - 在 Web 浏览器中键入以下 URL 之一：
     - **https://<yourCoreServerName>:8006/apprecovery/admin/core**
     - **https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core**

在 Internet Explorer 中更新可信站点

要在 Microsoft Internet Explorer 中更新可信站点，请执行以下操作：

1. 打开 Internet Explorer。
2. 如果未显示 **File**（文件）、**Edit**（编辑）、View（查看）及其他菜单，请按 <F10> 键。
3. 单击 **Tools**（工具）菜单并选择 **Internet Options**（Internet 选项）。
4. 在 **Internet Options**（Internet 选项）窗口中，单击 **Security**（安全）选项卡。
5. 单击 **Trusted Sites**（可信站点），然后单击 **Sites**（站点）。
6. 在 **Add this website to the zone**（将该网站添加到区域）中，输入 **https://[Display Name]**，为 Display Name 使用您提供的新名称。
7. 单击 **Add**（添加）。
8. 在 **Add this website to the zone**（将该网站添加到区域）中，输入 **about:blank**。
9. 单击 **Add**（添加）。
10. 单击 **Close**（关闭），然后单击 **OK**（确定）。

配置浏览器以远程访问 Core 控制台

要从远程机器访问 Core 控制台，需要修改浏览器设置。

注: 要修改浏览器设置，请以管理员身份登录系统。

注: Google Chrome 使用 Microsoft Internet Explorer 设置，因此请使用 Internet Explorer 更改 Chrome 浏览器设置。

注: 从本地或远程访问 Core Web 控制台时，确保打开 **Internet Explorer Enhanced Security Configuration（Internet Explorer 增强的安全配置）**。要打开 **Internet Explorer Enhanced Security Configuration（Internet Explorer 增强的安全配置）**，请执行以下操作：

1. 打开**服务器管理器**。
2. 选择右侧显示的 **Local Server IE Enhanced Security Configuration（本地服务器 IE 增强的安全配置）**。确保该选项为 **On（开启）**。

配置 Internet Explorer 和 Chrome 中的浏览器设置

要修改 Internet Explorer 和 Chrome 中的浏览器设置，请执行以下操作：

1. 打开 Internet Explorer。
2. 在 **Tools（工具）**菜单中依次选择 **Internet Options（Internet 选项）**、**Security（安全）**选项卡。
3. 单击 **Trusted Sites**（可信站点），然后单击 **Sites**（站点）。
4. 取消选中 **Require server verification (https:) for all sites in the zone（该区域中所有站点都要求服务器验证 [https:]）**选项，然后将 http://*<托管 AppAssure Core 的设备服务器的主机名或 IP 地址>* 添加到 **Trusted Sites（可信站点）**中。
5. 单击 **Close**（关闭），选择 **Trusted Sites**（可信站点），然后单击 **Custom Level**（自定义级别）。
6. 滚动至 **Miscellaneous**（杂项）→ **Display Mixed Content**（显示混合内容），然后选择 **Enable**（启用）。
7. 滚动至屏幕底部的 **User Authentication**（用户验证）→ **Logon**（登录），然后选择 **Automatic logon with current user name and password**（自动使用当前用户名和密码登录）。
8. 单击 **OK**（确定），然后选择 **Advanced**（高级）选项卡。
9. 滚动至 **Multimedia**（多媒体），然后选择 **Play animations in webpages**（在网页中播放动画）。
10. 滚动至 **Security**（安全），选中 **Enable Integrated Windows Authentication**（启用集成 Windows 验证），然后单击 **OK**（确定）。

配置 Mozilla Firefox 浏览器设置

注: 要修改最新版本 Firefox 中的 Mozilla Firefox 浏览器设置，请禁用保护。右键单击 Site Identify（站点识别）按钮（位于 URL 左侧），转至 **Options（选项）**，然后单击 **Disable protection for now（立即禁用保护）**。

要修改 Mozilla Firefox 浏览器设置，请执行以下操作：

1. 在 Firefox 地址栏中键入 **about:config**，如果系统提示，则单击 **I'll be careful, I promise**（我会小心，我保证）。
2. 搜索词语 **ntlm**。

   搜索应至少返回三个结果。
3. 双击 **network.automatic-ntlm-auth.trusted-uris**，然后输入适合您的机器的以下设置：
   - 对于本地计算机，输入主机名。
   - 对于远程计算机，输入托管 AppAssure Core 的设备系统的主机名或 IP 地址（使用逗号分隔）；例如：*IP 地址,主机名*。
4. 重新启动 Firefox。

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

注: 如果正在使用该设备，建议使用 **Appliance**（设备）选项卡配置 Core。有关在初始安装后配置 Core 的更多信息，请参阅 **dell.com/support/home** 上的 *Dell DL4300 Appliance Deployment Guide*（Dell DL4000 设备部署指南）。

管理许可证

您可以直接从 Core 控制台管理许可证。通过该控制台可以更改许可证密钥和联系许可证服务器。还可以通过 Core 控制台中的 Licensing（许可）页面访问许可证门户。

Licensing（许可）页面包括以下信息：

- 许可证类型
- 许可证状态
- 许可证限制
- 受保护机器的数量
- 来自许可证服务器的最后响应的状态
- 与许可证服务器的最后联系的时间
- 联系许可证服务器的下一计划的尝试

更改许可证密钥

要更改许可证密钥，请执行以下操作：

1. 导航至 Core 控制台。
2. 选择 **Configuration（配置）** → **Licensing（许可）**。
   此时将显示 **Licensing**（许可）页面。
3. 在 **License Details（许可证详细信息）**部分中，单击 **Change License（更改许可证）**。
   此时将显示 **Change License**（更改许可证）对话框。
4. 在 **Change License**（更改许可证）对话框中，输入新许可证密钥并单击 **Continue**（继续）。

联系许可证门户服务器

Core 控制台会频繁联系门户服务器，以便与许可证门户中所做的任何更改保持同步。通常，与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。

要联系门户服务器，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）** → **Licensing（许可）**。
3. 从 **License Server**（许可证服务器）选项中，单击 **Contact Now**（立即联系）。

手动更改 AppAssure 语言

AppAssure 允许您将运行 AppAssure Appliance Configuration Wizard（AppAssure 设备配置向导）时选择的语言更改为任何支持的语言。
要将 AppAssure 语言更改为所需的语言：

1. 使用 `regdit` 命令启动注册表编辑器。
2. 导航至 **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery → Core → Localization**。
3. 打开 **Lcid**。
4. 选择 **decimal**（十进制）。
5. 在 `Value data`（值数据）框中输入所需语言值，支持的语言值如下：
   a. 英语：1033
   b. 巴西葡萄牙语：1046
   c. 西班牙语：1034
   d. 法语：1036
   e. 德语：1031
   f. 简体中文：2052
   g. 日语：1041
   h. 朝鲜语：1042
6. 右键单击并按给定顺序重新启动服务：
   a. Windows 管理规范
   b. SRM Web 服务
   c. AppAssure Core
7. 清除浏览器高速缓存。
8. 关闭浏览器，然后使用桌面图标重新启动 Core 控制台。

在安装过程中更改操作系统语言

在执行 Windows 安装的过程中，可以使用控制面板选择语言包和配置其他国际设置。
要更改操作系统语言：

注: 建议将操作系统语言和 AppAssure 语言设置为同一种语言。否则，某些信息可能会以混合的语言显示。

注: 建议先更改操作系统语言，然后再更改 AppAssure 语言。

1. 在 **Start**（开始）页面中，键入 `language`（语言），确保搜索范围设定为 Settings（设置）。
2. 在 **Results**（结果）面板中，选择 **Language**（语言）。
3. 在 **Change your language preferences**（更改您的语言首选项）窗格中，选择 **Add a language**（添加语言）。
4. 浏览或搜索所要安装的语言。
   例如选择 Catalan（加泰罗尼亚语），然后选择 Add（添加）。加泰罗尼亚语便将添加为您的语言之一。
5. 在 Change your language preferences（更改您的语言首选项）窗格中，选择所添加语言旁边的 **Options**（选项）。
6. 如果您的语言提供有语言包，请选择 `Download and install language pack`（下载并安装语言包）。

7. 安装语言包后，该种语言将显示为可以用作 Windows 显示语言。
8. 要将该语言设置为您的显示语言，请将其移至语言列表的顶部。
9. 先注销然后重新登录到 Windows，更改才会生效。

管理 Core 设置

Core 设置用于定义各种配置和性能设置。大多数设置都已针对最佳使用效果进行了配置，但可根据需要更改以下设置：

- 常规
- Nightly Jobs（每夜作业）
- Transfer Queue（传输队列）
- Client Timeout Settings（客户端超时设置）
- Deduplication Cache Configuration（清除重复高速缓存配置）
- Database Connection Settings（数据库连接设置）

更改 Core 显示名称

注: 建议在初始配置设备期间选择一个永久显示名称。如果以后更改显示名称，则必须手动执行多个步骤，以确保新主机名生效并且设备正常工作。有关更多信息，请参阅手动更改主机名。

要更改 Core 显示名称，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）** → **Settings（设置）**
3. 在 **General**（常规）窗格中，单击 **Change**（更改）。
   此时将显示 **General Settings**（常规设置）对话框。
4. 在 **Display Name（显示名称）**文本框中，输入 Core 的新显示名称。
   此名称将显示在 Core 控制台中。最多可输入 64 个字符。
5. 在 **Web Server Port**（Web 服务器端口）文本框中， 输入 Web 服务器的端口号。默认值为 8006。
6. 在 **Service Port**（服务端口）中，输入服务的端口号。默认值为 8006。
7. 单击 **OK（确定）**。

调整每夜作业时间

要调整每夜作业时间，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）** → **Settings（设置）**。
3. 在 **Nightly Jobs**（每夜作业）区域中，单击 **Change**（更改）。
   此时将显示 **Nightly Jobs**（每夜作业）对话框。
4. 在 **Nightly Jobs Time**（每夜作业时间）文本框中，输入执行每夜作业的新时间。
5. 单击 **OK（确定）**。

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，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Settings（设置）**。
3. 在 **Transfer Queue**（传输队列）窗格中，单击 **Change**（更改）。
   此时将显示 **Transfer Queue**（传输队列）对话框。
4. 在 **Maximum Concurrent Transfers**（最大并发传输数）文本框中，输入一个值以更新并发传输的数量。
   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。随着所处理的容量增加，对系统造成的负载也会增加。
5. 在 **Maximum Retries**（最大重试次数）文本框中，输入一个值以更新最大重试次数。
6. 单击**确定**。

调整客户端超时设置

要调整客户端超时设置，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Settings（设置）**。
3. 在 **Client Timeout Settings Configuration**（客户端超时设置配置）区域中，单击 **Change**（更改）。
   此时将显示 **Client Timeout Settings**（客户端超时设置）对话框。
4. 在 **Connection Timeout**（连接超时）对话框中，输入发生连接超时之前的分钟数和秒数。
5. 在 **Connection UI Timeout**（连接 UI 超时）对话框中，输入发生 UI 连接超时之前的分钟数和秒数。
6. 在 **Read/Write Timeout**（读/写超时）文本框中，输入读/写事件期间发生超时之前要等待的分钟数和秒数。
7. 在 **Read/Write UI Timeout**（读/写 UI 超时）文本框中，输入发生读/写 UI 超时之前要等待的分钟数和秒数。
8. 单击**确定**。

配置清除重复高速缓存设置

要配置清除重复高速缓存设置，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Settings（设置）**
3. 在 **Deduplication Cache Configuration**（清除重复高速缓存配置）区域中，单击 **Change**（更改）。
   此时将显示 **Deduplication Cache Configuration**（重复数据消除高速缓存配置）对话框。
4. 在 **Primary Cache Location**（主要高速缓存位置）文本框中，输入一个更新后的值以更改主要高速缓存位置。
5. 在 **Secondary Cache Location**（次要高速缓存位置）文本框中，输入一个更新后的值以更改次要高速缓存位置。
6. 在 **Metadata Cache Location**（元数据高速缓存位置）文本框中，输入一个更新后的值以更改元数据高速缓存位置。
7. 在 Dedupe Cache Size（**重复数据消除高速缓存大小**）文本框中，输入一个值，该值对应于要分配给重复数据消除高速缓存的空间量。
   从单位大小下拉字段中，选择 GB（千兆字节）或 TB（吉字节），以指定 Dedupe Cache Size（重复数据消除高速缓存大小）文本框中的值的测量单位。
8. 单击**确定**。

注: 必须重新启动 Core 服务才能使更改生效。

修改引擎设置

要修改引擎设置，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）** → **Settings（设置）**
3. 在 **Replay Engine Configuration** （Replay 引擎配置）窗格中，单击 **Change**（更改）。
   此时将显示 **Replay Engine Configuration**（Replay 引擎配置）对话框。
4. 根据下面的说明输入配置信息：

文本框	说明
IP 地址	• 要使用 TCP/IP 中的首选 IP 地址，请单击 **Automatically Determined**（自动确定） • 要手动输入 IP 地址，请单击 **Use a specific address**（使用指定地址）。
Preferable Port（首选端口）	输入端口号或接受默认设置（默认端口号为 8007）。端口用于指定引擎的通信通道。
端口使用中	表示端口正在用于 Replay Engine（Replay 引擎）配置。
允许端口自动分配	单击以允许自动分配 TCP 端口。
Admin Group（管理组）	输入管理组的新名称。默认名称为 **BUILTIN\Administrators**。
Minimum Async I/O Length（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。
Receive Buffer Size（接收缓冲区大小）	输入入站缓冲区大小或接受默认设置。默认设置为 8192。
Send Buffer Size（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。
Read Timeout（读取超时）	输入读取超时值或选择默认设置。默认设置为 00:00:30。
Write Timeout（写入超时）	输入写入超时值或选择默认设置。默认设置为 00:00:30。
无延迟	建议您将此复选框保持未选中状态，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 支持部门寻求指导。

5. 单击**确定**。

修改数据库连接设置

要修改数据库连接设置，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Settings（设置）**
3. 在 **Database Connection Settings**（数据库连接设置）区域中，选择以下操作之一：
   - 单击 **Apply Default**（应用默认设置）。
   - 单击 **Change**（更改）。

   此时将显示 **Database Connection Settings**（数据库连接设置）对话框。
4. 根据下面的说明输入用于修改数据库连接的设置：

文本框	说明
主机名	输入数据库连接的主机名。
Port（端口）	输入数据库连接的端口号。
User Name（用户名）（可选）	输入用于访问和管理数据库连接设置的用户名。此名称用来指定访问数据库连接的登录凭据。
Password（密码）（可选）	输入用于访问和管理数据库连接设置的密码。
Retain event and job history for, days（保留事件和作业历史天数）	输入数据库连接事件和作业历史的保留天数。
Max connection pool size（最大连接池大小）	设置高速缓存的数据库连接的最大数量以允许动态重新使用。默认设置为 100。
Min connection pool size（最小连接池大小）	设置高速缓存的数据库连接的最小数量以允许动态重新使用。默认设置为 0。

5. 单击 **Test Connection**（测试连接）以验证设置。
6. 单击**保存**。

关于存储库

存储库存储从受保护工作站和服务器捕获的快照。存储库可以基于不同的存储技术，如存储区域网络 (SAN)、直接连接存储 (DAS) 或网络连接存储 (NAS)。

创建存储库时，Core 将在指定位置预先分配数据和元数据所需的存储空间。您可在单个 Core 上跨不同技术创建最多 255 个独立存储库。此外，通过添加新文件延伸范围或规格可进一步增加存储库的大小。扩展存储库最多可包含 4096 个跨不同存储技术的延伸范围。

关键存储库概念和注意事项包括：

- 存储库基于 AppAssure 可扩展对象文件系统。

- 存储库中存储的所有数据均进行了全局重复数据消除。
- 可扩展对象文件系统可与全局重复数据消除、加密和保留管理共同提供可扩展的 I/O 性能。

注: DL4300 存储库存储在主要存储设备上。由于性能上的局限性，不支持 Data Domain 等存档存储设备。与此类似，存储库不应存储在连接到云的 NAS 文件管理器上，因为这些设备用作主要存储时在性能上通常存在局限性。

存储库管理路线图

存储库管理路线图包含创建、配置和查看存储库等任务，其中包括以下主题：

- 访问 Core 控制台
- 创建存储库
- 查看存储库详情
- 修改存储库设置
- 将存储位置添加至现有存储库
- 检查存储库
- 删除存储库
- 恢复存储库

注: 建议使用 **Appliance**（设备）选项卡配置存储库。

开始使用您的设备之前，必须在 Core 服务器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服务器捕获的快照。

配置存储库时可以执行多种任务，例如：指定数据存储将位于 Core 服务器上的哪个位置、指定可为各存储库添加多少位置、指定存储库的名称、指定存储库将支持多少当前操作等。

创建存储库时，Core 将在指定位置预先分配存储数据和元数据所需的空间。在单个 Core 上最多可创建 255 个独立存储库。为进一步增加单个存储库的大小，可添加新的存储位置或卷。

您可以在 Core 控制台中添加或修改存储库。

创建存储库

注: 如果您正在将该设备用作 SAN，则建议使用 **Appliance**（设备）选项卡来创建存储库，请参阅配置所选存储。

执行以下操作来手动创建存储库：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）** → **Repositories（存储库）**。
3. 单击 **Add new**（新增）。
   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。

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，此文本框包含词语 Repository 和一个索引号，该索引号是从 1 开始按顺序添加至新存储库的编号。可根据需要更改此名称。最多可输入 150 个字符。
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。
Comments（注释）	（可选）输入关于此存储库的说明。

5. 要为存储库定义特定的存储位置或卷，请单击 **Add Storage Location**（添加存储位置）。

   小心: 如果以后移除了您在此步骤中创建的 AppAssure 存储库，则存储库所在存储位置中的所有文件将被删除。如果未定义专用文件夹来存储存储库文件，则这些文件将被存储在根中；删除该存储库还将删除根的完整内容，从而导致灾难性数据丢失。

   注: 存储库存储在主要存储设备上。由于性能上的局限性，不支持 Data Domain 等存档存储设备。与此类似，存储库不应存储在连接到云的 NAS 文件管理器上，因为这些设备用作主要存储时在性能上通常存在局限性。

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

6. 指定如何添加存储位置的文件。可选择添加本地磁盘或 CIFS 共享上的文件。
   - 要指定本地机器，请单击 **Add file on local disk**（添加本地磁盘上的文件），然后根据下面的说明输入信息：

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**。 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。
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**。 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。

   - 或者指定网络共享位置，请单击 **Add file on CIFS share**（添加 CIFS 共享上的文件），然后根据下面的说明输入信息：

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，则定义专用文件夹名称（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。

文本框	说明
密码	指定用于访问网络共享位置的密码。

7. 在 **Details**（详细信息）窗格中，单击 **Show/Hide Details**（显示/隐藏详细信息），然后根据下面的说明输入存储位置的详细信息：

文本框	说明
大小	设置存储位置的大小或容量。默认值为 250 MB。可以选择以下单位： • MB • GB • TB **注:** 指定的大小不能超过卷的大小。 **注:** 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 或 Windows Server 2012 的 NTFS 卷，则文件大小限制为 256 TB。 **注:** 要验证操作系统，必须在目标存储位置安装 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： • On（开） • Off（关） • Sync（同步） 如果设置为默认值 On（开），则 Windows 将控制高速缓存。 **注:** 将写高速缓存策略设置为 On（开）可提高性能。如果使用早于 Server 2012 的 Windows Server 版本，则建议设置为 **Off**（关）。 如果设置为 **Off**（关），则 AppAssure 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。
Bytes per Sector（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。
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。

8. 单击**保存**。
   此时将显示 **Repositories**（存储库）屏幕，其中包括新添加的存储位置。
9. 要为存储库添加额外存储位置，请重复步骤 4 到步骤 7。
10. 单击 **Create（创建）**以便创建存储库。
    随即会在 **Configuration**（配置）选项卡中显示 **Repository**（存储库）信息。

查看存储库详情

要查看存储库详情，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Repositories（存储库）**。
3. 单击您要查看其详情的存储库的 **Status**（状态）列旁的 **>**。
4. 在展开的视图中，可以执行下列操作：
   - Modify Settings（修改设置）
   - Add a Storage Location（添加存储位置）
   - Check a Repository（检查存储库）
   - Delete a Repository（删除存储库）

   还会显示存储库的详情，并包括存储位置和统计信息。存储位置详情包括元数据路径、数据路径和大小。统计信息包括：
   - Deduplication（重复数据消除）- 报告块重复数据消除命中数目、块重复数据消除未命中数目，以及块压缩率。
   - Record I/O（记录 I/O）- 包含速率 (MB/s)、读取速率 (MB/s) 和写入速率 (MB/s)。
   - Storage Engine（存储引擎）- 包括速率 (MB/s)、读取速率 (MB/s) 和写入速率 (MB/s)。

修改存储库设置

添加存储库后，可以修改存储库设置，如说明或最大并发操作数等。此外还可以为存储库创建新存储位置。

要修改存储库设置，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Repositories（存储库）**。
3. 单击 **Actions（操作）**按钮下的 Compression Ratio（压缩比率）列旁边的 Settings（设置）图标，然后单击 **Settings**（设置）。

   此时将显示 **Repository Settings**（存储库设置）对话框。
4. 根据下面的说明编辑存储库信息：

字段	说明
Repository Name（存储库名称）	代表存储库的名称。默认情况下，此文本框包含词语 Repository 和一个索引号，该索引号即存储库的编号。 **注:** 无法编辑存储库名称。
Description（说明）	（可选）输入关于此存储库的说明。
Maximum Concurrent Operations（最大并发操作数）	定义您要存储库支持的并发请求数量。

字段	说明
Enable Deduplication（启用重复数据消除）	要关闭重复数据消除，请清除此复选框。要启用重复数据消除，请选中此复选框。 **注:** 对此设置的更改仅应用于更改设置后创建的备份。现有数据、从另一个 Core 复制的数据或从存档导入的数据将保留在从受保护机器捕获数据时设置的重复数据消除值。
Enable Compression（启用压缩）	要关闭压缩，请清除此复选框。要启用压缩，请选中此复选框。 **注:** 此设置仅应用于更改设置后创建的备份。现有数据、从另一个 Core 复制的数据或从存档导入的数据将保留在从受保护机器捕获数据时设置的压缩值。

5. 单击 **Save（保存）**。

扩展现有存储库

如果在设备中添加另一个 MD1400 DAS，则可以使用可用存储来扩展现有存储库。

要扩展现有存储库，请执行以下操作：

1. 安装 MD1400 DAS 后，打开 Core 控制台并选择 **Appliance**（设备）选项卡，单击 **Tasks**（任务）。
2. 在 **Tasks**（任务）屏幕中，单击新存储旁的 **Provision**（配置）。
3. 在 **Provisioning Storage**（配置存储）屏幕中，选择 **Expand the existing repository**（扩展现有存储库），选择要扩展的存储库。
4. 单击 **Provision**（配置）。

   在 **Tasks**（任务）屏幕中，存储设备旁的 **Status Description**（状态说明）显示为 **Provisioned**（已配置）。

将存储位置添加至现有存储库

通过添加存储位置，可定义存储库或卷的存储位置。

要将存储位置添加至现有存储库，请执行以下操作：

1. 单击您要添加存储位置的存储库的 **Status**（状态）列旁的 **>**。
2. 单击 **Add Storage Location**（添加存储位置）。

   此时将显示 **Add Storage Location**（添加存储位置）对话框。
3. 指定如何添加存储位置的文件。可选择添加本地磁盘或 CIFS 共享上的文件。
   - 要指定本地机器，请单击 **Add file on local disk**（添加本地磁盘上的文件），根据下面的说明输入信息：

文本框	说明
Metadata Path（元数据路径）	输入用于存储受保护元数据的位置。
Data Path（数据路径）	输入用于存储受保护数据的位置。

   - 要指定网络共享位置，请单击 **Add file on CIFS share**（添加 CIFS 共享上的文件），根据下面的说明输入信息：

文本框	说明
UNC Path（UNC 路径）	输入网络共享位置的路径。
User Name（用户名）	指定用于访问网络共享位置的用户名。
Password（密码）	指定用于访问网络共享位置的密码。

4. 在 **Details**（详细信息）部分中，单击 **Show/Hide Details**（显示/隐藏详细信息），然后根据下面的说明输入存储位置的详细信息：

文本框	说明
Size（大小）	设置存储位置的大小或容量。默认大小为 250 MB。可以选择以下单位： • MB • GB • TB **注:** 指定的大小不能超过卷的大小。 **注:** 如果存储位置是使用 Windows XP 或 Windows 7 的 NTFS 卷，则文件大小限制为 16 TB。 如果存储位置是使用 Windows 8 或 Windows Server 2012 的 NTFS 卷，则文件大小限制为 256 TB。 **注:** 要验证操作系统，必须在目标存储位置安装 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（关闭） • 同步 如果设置为默认值 **On**（打开），则 Windows 将控制高速缓存。 **注:** 将写高速缓存策略设置为 **On**（打开）可提高性能；但建议设置为 **Off**（关闭）。 如果设置为 **Off**（关闭），则 AppAssure 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。
Bytes per Sector（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。
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。

5. 单击 **Save（保存）**。
   此时将显示 **Repositories**（存储库）屏幕，其中包括新添加的存储位置。
6. 要为存储库添加更多存储位置，请重复步骤 4 到步骤 7。

7. 单击 **OK（确定）**。

检查存储库

设备可在发生错误时对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、硬件故障等。

注: 此过程必须仅用于诊断目的。

要检查存储库，请执行以下操作：

1. 在 **Configuration**（配置）选项卡中，单击 **Repositories**（存储库），选择要检查的存储库旁的 **>**。
2. 在 **Actions**（操作）窗格中，单击 **Check**（检查）。
   此时将显示 **Check Repository**（检查存储库）对话框。
3. 在 **Check Repository**（检查存储库）对话框中，单击 **Check**（检查）。

   注: 如果检查失败，请从存档还原存储库。

删除存储库

要删除存储库，请执行以下操作：

1. 在 **Configuration**（配置）选项卡中，单击 **Repositories**（存储库），选择要删除的存储库旁的 **>**。
2. 在 **Actions**（操作）窗格中，单击 **Delete**（删除）。
3. 在 **Delete Repository**（删除存储库）对话框中，单击 **Delete**（删除）。

   小心: 删除存储库后，将丢弃其中包含的数据且无法恢复。

   删除存储库时，必须检查 Open Manage System Administrator 并删除存放存储库的虚拟磁盘。删除虚拟磁盘后，您可以重新配置该磁盘，并重新创建存储库。

重新装载卷

要重新装载卷，请执行以下操作：

1. 导航至 Core 控制台。
2. **Appliance（设备）→ Tasks（任务）**。
3. 单击 **Remount Volumes**（重新装载卷）。
   即会重新装载卷。

解析外部卷

如果已配置的 MD1400 关闭或断开连接并且稍后再开启，则会在 Core 控制台中显示一个事件，报告 MD1400 已连接。但是，在 **Appliance**（设备）选项卡的 **Tasks**（任务）屏幕中不会显示允许恢复的任务。**Enclosures**（机柜）屏幕报告该 MD1400 处于 Foreign（外部）状态，并且此外部虚拟磁盘上的存储库标记为脱机。

要解决外部卷，请执行以下操作：

1. 在 Core 控制台中，选择 **Appliance**（设备）选项卡，然后单击 **Remount Volumes**（重新装载卷）。
   即会重新装载卷。
2. 选择 **Configuration**（配置）选项卡，然后单击 **Repositories**（存储库）。
3. 通过单击 **Status**（状态）旁的 **>** 展开具有红色状态指示符的存储库。
4. 要验证存储库的完整性，请单击 **Actions**（操作）下的 **Check**（检查）。

恢复存储库

如果设备导入存储库失败，它会在 **Tasks**（任务）屏幕中报告失败，其任务状态用红圈指示，并且状态说明报告 **Error, Completed — Exception**（错误，已完成 - 异常）。要在 **Tasks**（任务）屏幕中查看错误详细信息，请通过单击 **Status**（状态）列旁的 **>** 展开任务详细信息。**Status Details**（状态详情）报告恢复任务状态为异常，并且 **Error Message**（错误消息）列提供有关错误状况的附加详情。

要让存储库从导入失败状态中恢复，请执行以下操作：

1. 导航至 Core 控制台。
   Repositories（存储库）屏幕显示带有红色状态指示符的失败存储库。
2. 单击 **Configuration（配置）→ Repositories（存储库）**。
3. 通过单击 **Status**（状态）旁的 **>** 展开失败的存储库。
4. 在 **Actions**（操作）部分，单击 **Check**（检查），然后单击 **Yes**（是）以确认要运行检查。
   设备将恢复该存储库。

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。

添加加密密钥

要添加加密密钥，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Security（安全性）**。
   此时将显示 **Encryption Keys（加密密钥）**页面。
3. 单击 **Actions**（操作），然后单击 **Add Encryption Key**（添加加密密钥）。
   此时将显示 **Create Encryption Key**（创建加密密钥）对话框。
4. 在 **Create Encryption Key**（创建加密密钥）对话框中，根据下面的说明输入密钥的详细信息。

文本框	说明
名称	输入加密密钥的名称。
说明	输入加密密钥的说明。此说明用于提供加密密钥的更多详情。
密码短语	输入密码短语。此密码短语用于控制访问。

文本框	说明
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。

5. 单击**确定**。

小心: 建议保护密码短语。丢失密码短语会导致无法访问数据。

编辑加密密钥

要编辑加密密钥，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Security（安全性）**
   此时将显示 **Encryption Keys**（加密密钥）屏幕。
3. 选择要修改的加密密钥，然后单击 **Edit（编辑）**。
   此时将显示 **Edit Encryption Key**（编辑加密密钥）对话框。
4. 在 **Edit Encryption Key**（编辑加密密钥）对话框中，编辑加密密钥的名称或修改其说明。
5. 单击**确定**。

更改加密密钥密码短语

要更改加密密钥密码短语，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Security（安全性）**。
   此时将显示 Encryption Keys（加密密钥）页面。
3. 选择要修改的加密密钥，然后单击 **Change Passphrase（更改密码短语）**。
   此时将显示 **Change Passphrase**（更改密码短语）对话框。
4. 在 **Change Passphrase**（更改密码短语）对话框中，输入加密密钥的新密码短语，然后再次输入密码短语进行确认。
5. 单击**确定**。

小心: 建议保护密码短语。丢失密码短语会导致无法访问系统中的数据。

导入加密密钥

要导入加密密钥，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）→ Security（安全性）**。
3. 选择 **Actions**（操作）下拉菜单，然后单击 **Import**（导入）。
   此时将显示 **Import Key**（导入密钥）对话框。
4. 在 **Import Key**（导入密钥）对话框中，单击 **Browse**（浏览）找到您要导入的加密密钥，然后单击 **Open**（打开）。
5. 单击**确定**。

导出加密密钥

要导出加密密钥，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）** → **Security（安全性）**。
3. 在要导出的加密密钥的名称旁，单击 **>**，然后单击 **Export**（导出）。
   此时将显示 **Export Key**（导出密钥）对话框。
4. 在 **Export Key**（导出密钥）对话框中，单击 **Download Key**（下载密钥）以在安全位置保存并存储加密密钥。
5. 单击**确定**。

移除加密密钥

要移除加密密钥，请执行以下操作：

1. 导航至 Core 控制台。
2. 单击 **Configuration（配置）** → **Security（安全性）**。
3. 在要移除的加密密钥的名称旁，单击 **>**，然后单击 **Remove**（移除）。
   此时将显示 **Remove Key（移除密钥）**对话框。
4. 在 **Remove Key**（移除密钥）对话框中，单击 **OK**（确定）以移除加密密钥。

   注: 移除加密密钥不会取消数据加密。

管理云帐户

DL 设备允许您通过创建恢复点的备份存档将数据备份到云。利用 DL 设备，可以通过云存储提供程序创建、编辑和管理云帐户。您可以使用 Microsoft Azure、Amazon S3、Rackspace Cloud Block Storage 或其他基于 OpenStack 的云服务将数据存档到云。要管理云帐户，请参阅以下主题：

- 添加云帐户
- 编辑云帐户
- 配置云帐户设置
- 移除云帐户

添加云帐户

要将存档数据导出到云，先在 Core 控制台中添加云提供程序的帐户。

要添加云帐户，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools**（工具）选项卡。
2. 在左侧菜单中，单击 **Clouds**（云）。
3. 在 **Clouds**（云）页面中，单击 **Add New Account**（添加新帐户）。
   此时将打开 **Add New Account**（添加新帐户）对话框。
4. 从 **Cloud Type**（云类型）下拉列表中选择兼容的云提供程序。
5. 根据在步骤 4 中选择的云类型，输入下表所述详细信息。

表. 1: 添加云帐户

云类型	文本框	说明
Microsoft Azure	Storage Account Name（存储帐户名）	输入您的 Windows Azure 存储帐户的名称。
	Access Key（访问密钥）	输入您的帐户的访问密钥。
	Display Name（显示名称）	在 AppAssure 中创建此帐户的显示名称；例如 Windows Azure 1。
Amazon S3	Access Key（访问密钥）	输入您的 Amazon 云帐户的访问密钥。
	Secret Key（机密密钥）	输入此帐户的机密密钥。
	Display Name（显示名称）	在 AppAssure 中创建此帐户的显示名称；例如 Amazon 1。
Powered by OpenStack	User Name（用户名）	输入基于 OpenStack 的云帐户的用户名。
	API Key（API 密钥）	输入您的帐户的 API 密钥。
	Display Name（显示名称）	在 AppAssure 中创建此帐户的显示名称；例如 OpenStack 1。
	Tenant ID（租户 ID）	输入此帐户的租户 ID。
	Authentication URL（验证 URL）	输入此帐户的验证 URL。
Rackspace Cloud Block Storage	User Name（用户名）	输入您的 Rackspace 云帐户的用户名。
	API Key（API 密钥）	输入此帐户的 API 密钥。
	Display Name（显示名称）	在 AppAssure 中创建此帐户的显示名称；例如 Rackspace 1。

6. 单击 **Add**（添加）。
   该对话框将关闭，并且您的帐户显示在 Core 控制台的 **Clouds**（云）页面中。

编辑云帐户

执行以下步骤以编辑云帐户：

1. 在 Core 控制台中，单击 **Tools（工具）**选项卡。
2. 在左侧菜单中，单击 **Clouds（云）**。
3. 单击您要编辑的云帐户旁边的下拉菜单，然后单击 **Edit（编辑）**。
   此时将打开 **Edit Account（编辑帐户）**窗口。
4. 根据需要编辑详细信息，然后单击 **Save（保存）**。

   注: 不能编辑云类型。

配置云帐户设置

云配置设置可确定 AppAssure 应尝试连接到云帐户的次数，以及在超时之前可以尝试的时间长度。
要配置云帐户的连接设置，请执行以下操作：

1. 在 Core 控制台中，单击 **Configuration**（配置）选项卡。
2. 在左侧菜单中，单击 **Settings（设置）**。
3. 在 **Settings（设置）**页面中，向下滚动至 **Cloud Configuration（云配置）**。
4. 单击要配置的云帐户旁边的下拉菜单，然后执行以下操作之一：
   - 单击 **Edit（编辑）**。
     此时将显示 **Cloud Configuration（云配置）**对话框。
     1. 使用向上和向下箭头编辑以下选项之一：
        - **Request Timeout（请求超时）**：以分钟和秒为单位，用于确定当存在延迟时，AppAssure 在单次尝试连接到云帐户上应花费的时间长度。经过所输入的时间长度后，连接尝试将停止。
        - **Retry Count（重试次数）**：确定 AppAssure 应进行尝试的次数，超过此尝试次数后即确定无法访问云帐户。
        - **Write Buffer Size（写入缓冲区大小）**：确定保留用于将存档数据写入云的缓冲区大小。
        - **Read Buffer Size（读取缓冲区大小）**：确定保留用于从云读取存档数据的块大小。
     2. 单击 **Next（下一步）**。
   - 单击 **Reset（重设）**。将配置恢复到以下默认设置：
     - **Request Timeout（请求超时）**：01:30（分钟和秒）
     - **Retry Count（重试次数）**：3（次重试）

移除云帐户

您可以移除云帐户以中止云服务，或停止为特定 Core 使用该帐户。
要移除云帐户，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools（工具）**选项卡。
2. 在左侧菜单中，单击 **Clouds（云）**。
3. 单击您要编辑的云帐户旁边的下拉菜单，然后单击 **Remove（移除）**。
4. 在 **Delete Account（删除帐户）**窗口中，单击 **Yes（是）**以确认要移除该帐户。
5. 如果该云帐户当前正在使用中，则会弹出另一个窗口，询问您是否仍要移除该帐户。单击 **Yes（是）**以确认。

   注: 移除当前正在使用的帐户会导致为此帐户计划的所有存档作业失败。

了解复制

关于保护工作站和服务器

要保护数据，必须在 Core 控制台中添加您要保护的工作站和服务器；例如，您的 Exchange Server、SQL Server 或 Linux 服务器。

注: 在本节中，*机器*一词一般还指安装在该机器上的 AppAssure 代理软件。

在 Core 控制台中，可以识别安装了 AppAssure 代理软件的机器并指定要保护的卷、定义保护计划、添加额外的安全措施（例如加密）等。有关如何访问 Core 控制台以保护工作站和服务器的更多信息，请参阅保护机器。

关于复制

复制是指拷贝恢复点并将其传输至次要站点以进行灾难恢复的过程。此过程需要两个 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。可行的复制方案包括：

- **Replication to a Local Location**（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。
- **Replication to an Off-site Location**（复制到非现场位置）。目标 Core 位于非现场灾难恢复设施，以便在发生丢失时进行恢复。
- **Mutual Replication**（相互复制）。两个不同地点的数据中心各自包含一个 Core，都对代理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。
- **Hosted and Cloud Replication**（托管和云复制）。AppAssure 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。

  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：

- **Point to Point**（点到点）。将单个受保护机器从单个源 Core 复制到单个目标 Core。

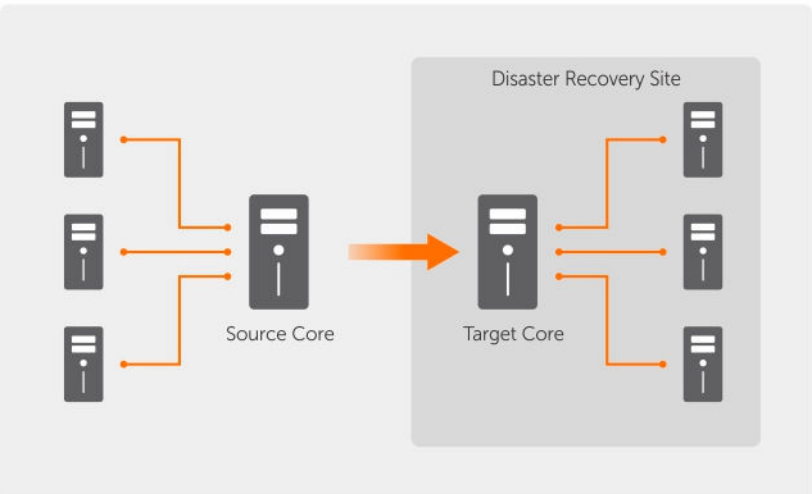


图 7: 基本复制架构图表

- **Multi-Point to Point**（多点到点）。将多个源 Core 复制到单个目标 Core。

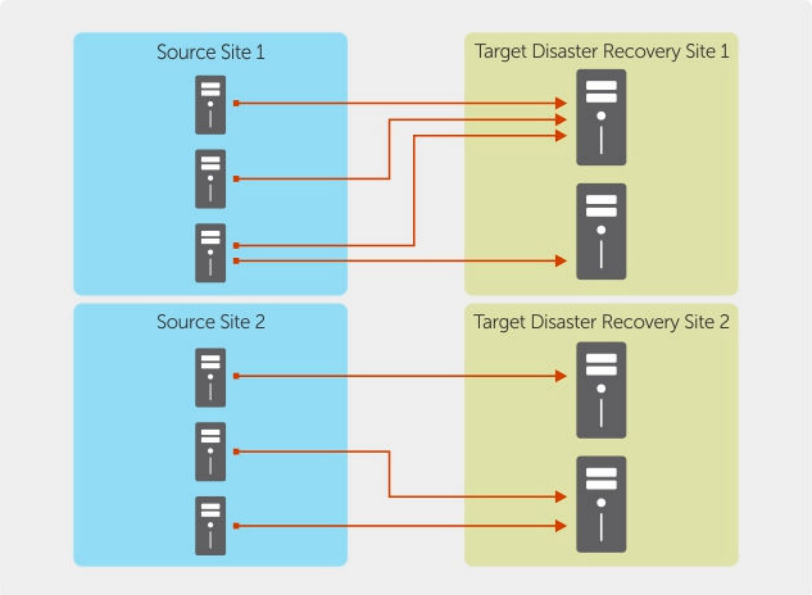


图 8: 多点复制架构图表

关于播种

复制过程从播种开始。播种是指初始传输受保护机器的基本映像（已消除重复数据）和增量快照的过程，这些数据总计可达数百乃至数千 GB。初始复制时可以使用外部介质播种到目标 Core，以便将初始数据传输到目标 Core。通常情况下，这对大型数据集或具有慢速链路的站点来说非常有用。

注: 虽然可以通过网络连接播种基础数据，但是不建议如此。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。例如，如果种子数据为 10 GB，而 WAN 链路的传输速率为 24 Mbps，则完成传输可能需要花费超过 40 天的时间。

种子存档中的数据已经过压缩、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。在播种过程中，系统会将增量恢复点复制到目标站点。目标 Core 使用种子存档后，新复制的增量恢复点会自动同步。

播种过程分为两个部分（也称为复制-消耗）：

- 第一部分是复制，即将初始复制的数据写入可移动介质源。复制时会将所有现有恢复点从源 Core 复制到本地可移动存储设备，如 USB 驱动器。复制完成后，必须将驱动器从源 Core 位置运输至远程目标 Core 位置。
- 第二部分是消耗，该部分将在目标 Core 接收所运输的驱动器并将已复制数据复制到存储库时发生。然后，目标 Core 将消耗恢复点并使用这些恢复点形成复制的受保护机器。

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。

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。

关于故障转移和故障回复

出现严重中断事件以致源 Core 和受保护机器发生故障时，DL 设备支持在复制环境下执行故障转移和故障回复。故障转移是指在系统故障或源 Core 及关联受保护机器异常终止时，切换至冗余或待机目标 Core。故障转移的主要目标是在故障源 Core 保护下的代理发生故障时，启动与之相同的新代理。次要目标是将目标

Core 切换至新模式，以便目标 Core 与在故障前保护初始代理的源 Core 一样，采用相同的方式保护故障转移代理。目标 Core 可以从复制的代理恢复实例，并立即开始对故障转移后的机器进行保护。

故障回复是指将受保护机器和 Core 还原到初始状态（故障前）的过程。故障回复的主要目标是将受保护机器（多数情况下，这是取代故障代理的新机器）还原到与新临时代理的最新状态相同的状态。完成还原后，它将由还原后的源 Core 进行保护。复制也会得到还原，目标 Core 将再次充当复制目标。

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短语才能恢复加密的数据。

关于复制的保留策略

源 Core 上的保留策略决定了复制到目标 Core 上的数据的保留策略，因为复制任务会传输通过前滚或临时删除而产生的合并恢复点。

注: 目标 Core 无法对恢复点进行前滚或临时删除。这些操作只能由源 Core 执行。

传输复制数据时的性能注意事项

如果源 Core 和目标 Core 之间的带宽无法支持传输所存储的恢复点，则复制将从目标 Core 的播种开始（使用基本映像和来自源 Core 上所选受保护服务器的恢复点）。播种过程只需执行一次，因为它是定期计划复制所需的基础。

准备进行复制时，必须考虑以下因素：

更改率

更改率是指受保护数据量的累积速率。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。如果卷上的一组数据块发生更改，则缩短保护间隔时间将降低更改率。

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。根据 Core 之间所传输数据量的大小，可能需要多个并行流以线速运行，最高需要 1 GB 以太网连接的速度。

注: ISP 指定的带宽即总可用带宽。输出带宽由网络上的所有设备共享。请确保具有足够的空余带宽可用于复制，以支持更改率。

受保护机器的数量

必须要考虑每个源 Core 上受保护机器的数量，以及计划要将多少受保护机器复制到目标 Core。AppAssure 允许按照每个受保护服务器执行复制，以便选择是否复制特定服务器。如果必须复制所有受保护服务器，则会严重影响更改率，特别是当源 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更是如此。

复制过程可能会非常费时，具体取决于网络配置。

下表例举了在合理的更改率下传输每 GB 数据所需的带宽

注: 要实现最佳效果，请遵循下表中列出的建议。

各种 WAN 连接的最大更改率

表. 2: 各种 WAN 连接的最大更改率

宽带	带宽	最大更改率
DSL	768 Kbps 及以上	330 MB/小时
电缆	1 Mbps 及以上	429 MB/小时
T1	1.5 Mbps 及以上	644 MB/小时
光纤	20 Mbps 及以上	838 GB/小时

如果数据传输期间出现链路故障，则在链路功能恢复后，将从传输的上一个故障点继续复制。

复制执行路线图

要使用 AppAssure 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的数据、监测和管理复制以及执行恢复。

在 AppAssure 中执行复制涉及执行以下操作：

- 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 Core。
- 配置第三方复制。有关复制到第三方目标 Core 的更多信息，请参阅复制到由第三方管理的 Core
- 复制已连接到源 Core 的新的受保护机器。有关复制受保护机器的更多信息，请参阅复制新的受保护机器。
- 复制现有受保护机器。有关配置代理进行复制的更多信息，请参阅复制机器上的代理数据。
- 设置代理的复制优先级。有关设置代理复制优先级的更多信息，请参阅设置代理的复制优先级。
- 根据需要监测复制。有关监测复制的更多信息，请参阅监测复制。
- 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

复制到自管 Core

自管 Core 是您具有访问权限的 Core，通常由公司管理并位于非现场位置。复制操作可全部在源 Core 上完成，除非您选择播种数据。播种要求您在源 Core 上配置复制后，在目标 Core 上消耗种子驱动器。

注: 此配置适用于到非现场位置的复制和相互复制。Core 必须安装在所有源和目标机器上。如果要配置系统以进行多点到点复制，则必须在所有源 Core 和一个目标 Core 上执行此任务。

配置源 Core 以复制到自管目标 Core

要配置源 Core 以复制到自管目标 Core，请执行以下操作：

1. 在 Core 中，单击 **Replication**（复制）选项卡。
2. 单击 **Add Target Core**（添加目标 Core）。
   此时将显示 **Replication**（复制）向导。
3. 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。

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 AppAssure 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	输入用于访问机器的用户名。例如 **Administrator**。
密码	输入用于访问机器的密码。

如果要添加的 Core 先前已经与此源 Core 配对，则执行以下操作：

a. 选择 **Use an existing target core（使用现有目标 Core）**。
b. 从下拉列表中选择目标 Core。
c. 单击 **Next**（下一步）。
d. 跳转至步骤 7。

4. 单击 **Next**（下一步）。
5. 在 **Details（详细信息）**页面中，输入此复制配置的名称；例如 SourceCore1。如果要重新启动或修复以前的复制配置，则选择 **My Core has been migrated and I would like to repair replication（我的 Core 已迁移，我想要修复复制）**。
6. 单击 **Next**（下一步）。
7. 在 **Agents**（代理）页面中，选择要复制的代理，然后使用 **Repository**（存储库）列中的下拉列表为每个代理选择存储库。
8. 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，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 **Agents**（代理）页面中，选择 **Use a seed drive to perform initial transfer**（使用种子驱动器执行初始传输）。如果您当前有一个或多个机器正在复制到目标 Core，则可以通过选择 **With already replicated**（包含已复制）将这些受保护机器加入种子驱动器。
b. 单击 **Next**（下一步）。
c. 在 **Seed Drive Location**（种子驱动器位置）页面中，使用 **Location type**（位置类型）下拉列表选择以下选项之一：
   - Local（本地）：在 **Location**（位置）文本框中，输入要保存种子驱动器的位置；例如 D:\work\archive。
   - Network（网络）：在 **Location**（位置）文本框中，输入要保存种子驱动器的位置，然后在 **User name**（用户名）和 **Password**（密码）文本框中输入网络共享的凭据。
   - Cloud（云）：在 **Account**（帐户）文本框中，选择该帐户。要选择云帐户，首先必须在 Core 控制台中添加此帐户。有关更多信息，请参阅添加云帐户。选择与您的帐户关联的 **Container**（容器）。选择要用于保存存档数据的 **Folder Name**（文件夹名称）。
d. 单击 **Next**（下一步）。

9. 在 **Seed Drive Option**（种子驱动器选项）对话框中，根据下面的说明输入信息：

文本框	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，则根据需要保留 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）。

文本框	说明
	• 选择空白文本框，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。
Customer ID（客户 ID）（可选）	（可选）输入由服务提供商分配给您的客户 ID。
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）— 从目录清除所有数据，然后再写入种子驱动器。
注释	输入存档的注释或说明。
Add all Agents to Seed Drive（将所有代理添加到种子驱动器）	选择要使用种子驱动器复制的代理。
Build RP chains (fix orphans)（构建 RP 链 [修复孤本]）	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。 AppAssure 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代理的最新恢复点，并且可能需要更多时间才能完成任务。
Use compatible format（使用兼容格式）	选择此选项可创建其格式与新版和旧版 AppAssure Core 兼容的种子驱动器。

10. 在 **Agents**（代理）页面中，选择要使用种子驱动器复制到目标 Core 的代理。
11. 单击 **Finish**（完成）。
12. 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。复制开始，但在使用种子驱动器并提供所需基本映像之前，会在目标 Core 上产生孤立恢复点。

在目标 Core 上消耗种子驱动器

仅当您在为自管 Core 配置复制时创建了种子驱动器的情况下，才需要执行此过程。
要在目标 Core 上消耗种子驱动器，请执行以下操作：

1. 如果种子驱动器被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 上的 Core 控制台中，选择 **Replication（复制）**选项卡。
3. 在 **Incoming Replication**（传入复制）下，使用下拉菜单选择正确的源 Core，然后单击 **Consume**（消耗）。

   随机显示 Consume（消耗）窗口。
4. 对于 **Location Type（位置类型）**，从下拉列表中选择以下选项之一：
   - Local（本地）

- Network（网络）
- Cloud（云）

5. 根据需要输入以下信息：

文本框	说明
Location（位置）	输入种子驱动器所在路径，例如 USB 驱动器或网络共享（例如 D:\）。
User name（用户名）	输入共享驱动器或文件夹的用户名。只有网络路径需要用户名。
Password（密码）	输入共享驱动器或文件夹的密码。只有网络路径需要密码。
Account（帐户）	从下拉列表中选择帐户。要选择云账户，首先必须在 Core 控制台中添加此账户。
Container（容器）	从下拉菜单中选择与您的帐户关联的容器。
Folder Name（文件夹名称）	输入保存有存档数据的文件夹名；例如，-Archive-[创建日期]- [创建时间]

6. 单击 **Check File**（检查文件）。

   Core 检查完文件后，会自动使用种子驱动器中包含的最旧和最新恢复点的日期填充 **Date Range（日期范围）**。它还会导入在为自管 Core 配置复制时输入的所有注释。

7. 在 **Consume**（消耗）窗口的 **Agent Names**（代理名称）下，选择要消耗其数据的机器，然后单击 **Consume**（消耗）。

   注: 要监测数据消耗进度，请选择 **Events**（事件）选项卡。

放弃未完成的种子驱动器

如果创建计划在目标 Core 上消耗的种子驱动器，但选择不将其发送到远程位置，则在源 Core **Replication**（复制）选项卡上保留未完成种子驱动器的链接。您可能想要放弃未完成种子驱动器，以采用不同或更新的种子数据。

注: 此过程会从源 Core 上的 Core 控制台中移除指向未完成种子驱动器的链接。但不会将该驱动器从其存储位置中移除。

要放弃未完成的种子驱动器，请执行以下操作：

1. 在源 Core 上的 Core 控制台中，选择 **Replication（复制）**选项卡。
2. 单击 **Outstanding Seed Drive (#)**（未完成的种子驱动器 (#)）。

   此时将显示 **Outstanding seed drives**（未完成的种子驱动器）部分。其中包含远程目标 Core 的名称、种子驱动器的创建日期和时间，以及种子驱动器上包含的恢复点的数据范围。

3. 单击要放弃的驱动器的下拉菜单，然后选择 **Abandon**（放弃）。

   此时将显示 **Outstanding Seed Drive**（未完成的种子驱动器）窗口。

4. 单击 **Yes**（是）确认操作。

   随即移除种子驱动器。如果源 Core 上不再有种子驱动器，则在下次打开 **Replication**（复制）选项卡时，不会显示 **Outstanding Seed Drive (#)**（未完成的种子驱动器 (#)）链接和 **Outstanding seed drives**（未完成的种子驱动器）部分。

复制到由第三方管理的 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 Core 不要求您具有目标 Core 的访问权限。当客户在一个或多个源 Core 上配置复制后，MSP 将完成目标 Core 的配置。

注: 此配置适用于托管和云复制。AppAssure Core 必须安装在所有源 Core 机器上。

为第三方管理的目标 Core 配置复制

注: 此配置适用于托管复制和云复制。如果要配置 AppAssure 以进行多点到点复制，则必须在所有源 Core 上执行此任务。

要为第三方管理的 Core 配置复制，请执行以下操作：

1. 导航至 Core 控制台，然后单击 **Replication（复制）**选项卡。
2. 在 **Actions**（操作）下拉菜单中，单击 **Add Remote Core**（添加远程 Core）。
3. 在 **Select Replication Type**（选择复制类型）对话框中，选择 **I have a subscription to a third-party providing off-site backup and disaster recovery services, and wish to replicate my backups to that service**（我订阅了提供非现场备份和灾难恢复服务的第三方服务，并且希望将我的备份复制到该服务），然后根据下表中的说明输入信息：

文本框	说明
Host Name（主机名）	输入远程 Core 机器的主机名、IP 地址或 FQDN。
Port（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。

4. 单击 **Continue**（继续）。
5. 在 **Add Remote Core**（添加远程 Core）中，执行以下操作：
   a. 选择要复制的受保护机器。
   b. 选择每个受保护机器的存储库。
   c. 输入订阅电子邮件地址和服务提供商分配的客户 ID。
6. 如果计划执行播种过程以便传输基础数据，请选择 **Use a seed drive to perform initial transfer**（使用种子驱动器执行初始传输）。
7. 单击 **Submit Request**（提交请求）。

   注: 如果选择 **Use a seed drive to perform initial transfer**（使用种子驱动器执行初始传输），将显示 **Copy to Seed Drive**（复制到种子驱动器）对话框。
8. 在 **Copy to Seed Drive**（复制到种子驱动器）对话框中，根据下表中的说明输入种子驱动器的信息。

文本框	说明
Location（位置）	输入要在其中保存初始数据的驱动器路径，如本地 USB 驱动器。
User name（用户名）	输入用于连接驱动器的用户名。 **注:** 如果种子驱动器位于网络共享中，则这是必填字段。
Password（密码）	输入用于连接驱动器的密码。 **注:** 如果种子驱动器位于网络共享中，则这是必填字段。
Maximum Size（最大大小）	选择以下选项之一： • 整个目标。 • 驱动器的部分可用空间。

文本框	说明
	要指定驱动器的一部分，请执行以下操作： a. 在文本框中输入所需的空间量。 b. 选择计量单位。
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**（请勿重复使用）— 不覆盖或清除此位置的任何现有数据。如果此位置为空，则种子驱动器写入将失败。 • **Replace this core**（更换此 Core）— 覆盖与此 Core 相关的任何预先存在的数据，但其他 Core 的数据保持不变。 • **Erase completely**（完全擦除）— 从目录清除所有数据，然后再写入种子驱动器。
Comment（注释）	输入存档的注释或说明。
Agents（代理）	选择要使用种子驱动器复制的代理。

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。

9. 单击 **Start**（开始），将种子驱动器写入所提供的路径。
10. 按照第三方服务提供商的指示发送种子驱动器。

检查复制请求

将从源 Core 向第三方目标 Core 发送一个复制请求。作为第三方，您可以检查该请求，然后为客户批准请求以开始复制，或者可以拒绝该请求以防止复制进行。

要检查第三方目标 Core 上的复制请求，请执行以下操作：

1. 打开目标 Core 上的 Core 控制台，然后选择 **Replication**（复制）选项卡。
2. 单击 **Pending Requests (#)**（挂起请求 (#)）。

   此时将显示 **Pending Replication Requests**（挂起复制请求）部分。
3. 在要检查的请求旁，从下拉菜单中选择 **Review**（检查）。

   此时将显示 **Review Replication Request**（复查复制请求）窗口。

   注: 由客户完成的请求决定了在 **Source Core Identity**（源 Core 标识）部分中显示的信息。
4. 在 Review Replication Request（检查复制请求）窗口中，执行以下操作之一：
   - 要拒绝请求，请单击 **Deny**（拒绝）。
   - 要批准请求，请执行以下操作：

     1. – 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 **Create a new source Core**（创建新的源 Core）。验证 **Core Name**（Core 名称）、客户 **Email Address**（电子邮件地址）和 **Customer ID**（客户 ID），根据需要编辑信息。
     2. 在 **Agents**（代理）下，选择要应用批准的机器，然后使用下拉列表选择每个机器的相应存储库。
     3. （可选）输入要在 **Comment**（注释）框中显示的注释。

4. 单击 **Send Response**（发送响应）。

已接受复制。

忽略复制请求

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检查的情况下直接拒绝请求，则可以使用此选项。

要忽略复制请求，请执行以下操作：

1. 在目标 Core 上的 Core 控制台中，选择 **Replication（复制）**选项卡。
2. 在 Replication（复制）选项卡中，单击 **Pending Requests (#)**（挂起请求 (#)）。
   此时将显示 **Pending Replication Requests**（挂起复制请求）部分。
3. 在要忽略的请求旁，使用下拉菜单选择 **Ignore**（忽略）。
   目标 Core 向源 Core 发送通知，告知请求被忽略。

监测复制

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。

要监测复制，请执行以下操作：

1. 在 Core 控制台中，单击 **Replication**（复制）选项卡。
2. 在此选项卡中，可以根据下面的说明查看和监测复制任务的状态信息：

表. 3: 监测复制

部分	说明	可执行的操作
Pending Replication Requests（挂起复制请求）	将复制请求提交至第三方服务提供商时，列出客户 ID、电子邮件地址和主机名。这些信息将列在此处，直到 MSP 接受请求。	在下拉菜单中，单击 **Ignore**（忽略）以忽略或拒绝请求。
Outstanding Seed Drives（未完成的种子驱动器）	列出已写入但尚未被目标 Core 消耗的种子驱动器。其中包括远程 Core 名称、创建日期以及日期范围。	在下拉菜单中，单击 **Abandon**（放弃）以放弃或取消播种过程。
Outgoing Replication（传出复制）	列出源 Core 要复制到的所有目标 Core。其中包括远程 Core 名称、存在状态、要复制的受保护机器数量，以及复制传输的进度。	在源 Core 上，可以从下拉菜单中选择以下选项： • **Details**（详细信息）- 列出 ID、URI、显示名称、状态、客户 ID、电子邮件地址和已复制 Core 的注释。 • **Change Settings**（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。 • **Add Agents**（添加代理）- 可以从下拉列表中选择主机、选择要复制的受保护机器，并为新的受保护机器的初始传输创建种子驱动器。

部分	说明	可执行的操作
Incoming Replication（传入复制）	列出目标机器从其接收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。	在目标 Core 上，可以从下拉菜单中选择以下选项： • **Details**（详细信息）- 列出 ID、主机名、客户 ID、电子邮件地址和已复制 Core 的注释。 • **Consume**（消耗）- 消耗来自种子驱动器的初始数据，并将其保存到本地存储库。

3. 单击 **Refresh**（刷新）按钮，将此选项卡的各部分更新为最新信息。

管理复制设置

您可以调整一些设置，以便影响源 Core 和目标 Core 上的复制执行方式。
要管理复制设置，请执行以下操作：

1. 在 Core 控制台中，单击 **Replication**（复制）选项卡。
2. 在 **Actions**（操作）下拉菜单中，单击 **Settings**（设置）。
3. 在 **Replication Settings**（复制设置）窗口中，根据下面的说明编辑复制设置：

选项	说明
Cache lifetime（高速缓存生存期）	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。
Volume image session timeout（卷映像会话超时）	指定源 Core 尝试将卷映像传输至目标 Core 时所花费的时间。
Max. concurrent replication jobs（最大并发复制作业）	指定允许一次复制到目标 Core 的受保护机器的数量。
Max. parallel streams（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。

4. 单击 **Save（保存）**。

移除复制

您可以通过多种方法停止复制并将受保护机器从复制中移除。选项包括：

- 从源 Core 上的复制中移除代理
- 移除目标 Core 上的代理
- 从复制中移除目标 Core
- 从复制中移除源 Core

注: 移除源 Core 将导致移除该 Core 保护的所有已复制的机器。

从源 Core 上的复制移除受保护的机器

要从源 Core 上的复制移除受保护的机器，请执行以下操作：

1. 从源 Core 中打开 Core 控制台，然后单击 **Replication（复制）**选项卡。
2. 展开 **Outgoing Replication**（传出复制）部分。
3. 在要从复制中移除的受保护机器的下拉菜单中，单击 **Delete**（删除）。
4. 在 **Outgoing Replication**（传出复制）对话框中，单击 **Yes**（是）确认删除。

移除目标 Core 上的受保护机器

要移除目标 Core 上的受保护机器，请执行以下操作：

1. 从目标 Core 中打开 Core 控制台，然后单击 **Replication（复制）**选项卡。
2. 展开 **Incoming Replication**（传入复制）部分。
3. 在要从复制中移除的受保护机器的下拉菜单中，单击 **Delete**（删除），然后选择以下选项之一。

选项	说明
Relationship Only（仅关系）	从复制中移除受保护机器，但保留已复制恢复点。
With Recovery Point（包括恢复点）	从复制中移除受保护机器，并且删除从该机器接收的所有已复制恢复点。

从复制中移除目标 Core

要从复制中移除目标 Core，请执行以下操作：

1. 从源 Core 中打开 Core 控制台，然后单击 **Replication（复制）**选项卡。
2. 在 **Outgoing Replication**（传出复制）下，单击要删除的远程 Core 旁的下拉菜单，然后单击 **Delete**（删除）。
3. 在 **Outgoing Replication**（传出复制）对话框中，单击 **Yes**（是）确认删除。

从复制中移除源 Core

注: 移除源 Core 将导致移除该 Core 保护的所有已复制代理。

要从复制中移除源 Core，请执行以下操作：

1. 从目标 Core 中打开 Core 控制台，然后单击 **Replication（复制）**选项卡。
2. 在 **Incoming Replication**（传入复制）下的下拉菜单中，单击 **Delete**（删除），然后选择以下选项之一。

选项	说明
Relationship Only（仅关系）	从复制中移除源 Core，但保留已复制恢复点。

选项	说明
With Recovery Points（包括恢复点）	从复制中移除源 Core，并且删除从该机器接收的所有已复制恢复点。

3. 在 **Incoming Replication**（传入复制）对话框中，单击 **Yes**（是）确认删除。

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 可以使用已复制恢复点恢复受保护代理和 Core。

您可以在目标 Core 上执行以下恢复选项：

- 安装恢复点。
- 回滚到恢复点。
- 执行虚拟机 (VM) 导出。
- 执行裸机还原 (BMR)。
- 执行故障回复（如果已设置故障转移/故障回复复制环境）。

故障转移和故障回复路线图

如果遇到源 Core 和关联受保护机器发生故障的灾难情况，可以在 AppAssure 中启用故障转移，以便将保护切换至相同的故障转移（目标）Core 并启动与故障代理相同的新（复制的）代理。修复源 Core 和代理后即可执行故障回复，以便将数据从故障转移 Core 和代理还原到源 Core 和代理。在 AppAssure 中，故障转移和故障回复包含以下过程。

- 设置故障转移环境。
- 对目标 Core 和关联代理执行故障转移。
- 通过执行故障回复还原源 Core。

设置故障转移环境

要设置故障转移环境，需要设置要复制的源和目标 Core 及关联代理。要为故障转移设置复制，请完成以下过程中的步骤。

要设置故障转移环境，请执行以下操作：

1. 安装源 Core 和目标 Core。
2. 安装一个受源 Core 保护的 AppAssure 代理。
3. 分别在源 Core 和目标 Core 上创建一个存储库。
   有关更多信息，请参阅创建存储库。
4. 添加受源 Core 保护的代理。
   有关更多信息，请参阅保护机器。
5. 设置从源 Core 到目标 Core 的复制，并复制受保护代理及所有恢复点。
   按照复制到自管 Core 中的步骤添加要复制到的目标 Core。

在目标 Core 上执行故障转移

如果遇到源 Core 和关联受保护机器发生故障的灾难情况，可以启用故障转移以便将保护切换至相同的故障转移（目标）Core。目标 Core 成为环境中唯一保护数据的 Core，然后可启动新代理以暂时替换故障代理。

要在目标 Core 上执行故障转移，请执行以下操作：

1. 在目标 Core 上导航至 Core 控制台，然后单击 **Replication（复制）**选项卡。
2. 在 **Incoming Replication**（传入复制）下，选择源 Core，然后展开个别代理下的详细信息。
3. 在该 Core 的 **Actions**（操作）菜单中，单击 **Failover**（故障转移）。
   在此表中，该机器的状态将变为 **Failover**（故障转移）。
4. 单击 **Machines**（机器）选项卡，然后选择具有带恢复点的关联 AppAssure 代理的机器。
5. 将该代理上的备份恢复点信息导出至虚拟机。
6. 关闭具有此 AppAssure 代理的机器。
7. 启动现在包含导出备份信息的虚拟机。
   需要等待安装设备驱动程序软件。
8. 重新引导虚拟机，等待代理服务启动。
9. 返回目标 Core 的 Core 控制台，验证新代理是否显示在 **Protected Machines**（受保护机器）下的 **Machines**（机器）选项卡以及 **Incoming Replication**（传入复制）下的 **Replication**（复制）选项卡上。
10. 强制创建多个快照，并验证是否正确完成。
    有关更多信息，请参阅强制创建快照。
11. 现在即可继续执行故障回复。
    有关更多信息，请参阅执行故障回复。

执行故障回复

修复或更换发生故障的原始源 Core 和受保护机器后，需要从故障转移机器移回数据以还原源机器。

要执行故障回复，请执行以下操作：

1. 在目标 Core 上导航至 Core 控制台，然后单击 **Replication（复制）**选项卡。
2. 在 **Incoming Replication**（传入复制）下，选择故障转移代理并展开详细信息。
3. 在 **Actions**（操作）菜单中，单击 **Failback**（故障回复）。
   此时将打开 **Failback Warnings**（故障回复警告）对话框，说明在单击 **Start Failback**（开始故障回复）按钮之前需要执行哪些步骤。
4. 单击 **Cancel**（取消）。
5. 如果故障转移机器正在运行 Microsoft SQL Server 或 Microsoft Exchange Server，请停止这些服务。
6. 在目标 Core 的 Core 控制台中，单击 **Tools**（工具）选项卡。
7. 创建故障转移代理的存档，并将其输出至磁盘或网络共享位置。
8. 创建存档后，导航至新修复的源 Core 上的 Core 控制台，然后单击 **Tools**（工具）选项卡。
9. 导入步骤 7 中创建的存档。
10. 返回至目标 Core 上的 Core 控制台，然后单击 **Replication**（复制）选项卡。
11. 在 **Incoming Replication**（传入复制）下，选择故障转移代理并展开详细信息。
12. 在 **Actions**（操作）菜单中，单击 **Failback**（故障回复）。
13. 在 **Failback Warnings**（故障回复警告）对话框中，单击 **Start Failback**（开始故障回复）。
14. 关闭故障转移期间创建的导出代理所在的机器。

15. 对源 Core 和代理执行裸机还原 (BMR)。

    注: 启动还原时，必须使用从目标 Core 导入到虚拟机上的代理的恢复点。

16. 等待 BMR 重新引导和代理服务重新启动，然后查看并记录机器的网络连接详细信息。
17. 导航至源 Core 上的 Core 控制台，然后在 **Machines**（机器）选项卡上修改机器保护设置，以便添加新的网络连接详细信息。
18. 导航至目标 Core 上的 Core 控制台，然后从 **Replication**（复制）选项卡删除代理。
19. 在源 Core 的 Core 控制台中，单击 **Replication**（复制）选项卡，然后添加要复制的目标 Core，从而再次在源和目标之间设置复制。

管理事件

管理 Core 事件可帮助监测 Core 的运行状况和使用情况。Core 包括预定义的事件集，可用于向管理员通知 Core 或备份作业中的严重问题。

通过 **Events**（事件）选项卡，可以管理通知组、电子邮件 SMTP 设置、减少重复和事件保留。Notification Groups（通知组）选项可用于管理通知组，通过该选项可执行以下操作：

- 指定要生成警报的事件：
  - Clusters（群集）
  - Attachability（可附加性）
  - Jobs（作业）
  - 许可
  - Log Truncation（日志截断）
  - Archive（存档）
  - Core Service（Core 服务）
  - 导出
  - Protection（保护）
  - 复制
  - Rollback（回滚）
  - SMTP 服务器设置
  - 已启用的跟踪日志
  - 云配置
- 指定警报类型（错误、警告和信息）。
- 指定警报的接收人和发送的目的地。选项包括：
  - Email Address（电子邮件地址）
  - Windows Events Logs（Windows 事件日志）
  - Syslog Server（系统日志服务器）
- 指定重复的时间阈值。
- 指定所有事件的保留期限。

配置通知组

要配置通知组，请执行以下操作：

1. 在 Core 中选择 **Configuration（配置）**选项卡。
2. 在 **Manage**（管理）选项中，单击 **Events**（事件）。
3. 单击 **Add Group**（添加组）。
   此时将打开 **Add Notification Group**（添加通知组）对话框，并显示三个面板：
   - **常规**
   - **Enable Events（启用事件）**
   - **Notification Options（通知选项）**
4. 在 **General**（常规）面板中，根据下表中的说明输入通知组的基本信息：

文本框	说明
名称	输入事件通知组的名称，此名称用于标识事件通知组。
说明	输入事件通知组的说明，此说明用于描述事件通知组的用途。

5. 在 **Enable Events**（启用事件）面板中，选择创建和报告事件日志（警报）的条件。
   您可以选择为下列事件创建警报：
   - **All Events（所有事件）**
   - **Appliance Events（设备事件）**
   - **Boot CD（引导 CD）**
   - **安全性**
   - **DatabaseRetention（数据库保留）**
   - **LocalMount**
   - **Clusters（群集）**
   - **Notification（通知）**
   - **Power Shell Scripting（Power Shell 脚本）**
   - **Push Install（推送安装）**
   - **Nightly Jobs（每夜作业）**
   - **Attachability（可附加性）**
   - **Jobs（作业）**
   - **许可**
   - **Log Truncation（日志截断）**
   - **Archive（存档）**
   - **Core Service（Core 服务）**
   - **导出**
   - **Protection（保护）**
   - **复制**
   - **Repository（存储库）**
   - **Rollback（回滚）**
   - **Rollup（前滚）**
6. 在 **Notification Options**（通知选项）面板中，指定如何处理通知过程。
   通知选项如下：

文本框	说明
Notify by e-mail（通过电子邮件通知）	指定电子邮件通知的收件人。您可以选择指定分隔多个电子邮件地址，以及抄送和密送地址。您可以选择： • **To:（收件人：）** • **CC:（抄送：）** • **BCC:（密件抄送：）**
Notify by Windows Event log（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。此选项用于指定是否应通过 Windows 事件日志报告警报通知。
Notify by sys logd（通过系统日志通知）	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： • **Hostname:（主机名：）** • **Port:1（端口：1）**

7. 单击**确定**。

配置电子邮件服务器和电子邮件通知模板

如果您要接收有关事件的电子邮件通知，请配置电子邮件服务器和电子邮件通知模板。

注: 您还必须配置通知组设置，包括启用 **Notify by email（通过电子邮件通知）**选项，才能通过电子邮件发送警报消息。有关指定接收电子邮件警报的事件的更多信息，请参阅 *Dell DL4300 Appliance User's Guide*（Dell DL4300 设备用户指南）中的"Configuring Notification Groups For System Events"（为系统事件配置通知组）。

要配置电子邮件服务器和电子邮件通知模板，请执行以下操作：

1. 在 Core 中选择 **Configuration（配置）**选项卡。
2. 在 **Manage**（管理）选项中，单击 **Events**（事件）。
3. 在 **Email SMTP Settings**（电子邮件 SMTP 设置）窗格中，单击 **Change**（更改）。
   此时将显示编辑 **Email Notification Configuration**（电子邮件通知配置）对话框。
4. 选择 **Enable Email Notifications**（启用电子邮件通知），然后输入如下描述的电子邮件服务器的详细信息：

文本框	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。命名规则包括主机名、域和后缀；例如 **smtp.gmail.com**。
端口	输入端口号，用于标识电子邮件服务器的端口；例如，Gmail 的端口 587。 默认值为 25。
超时（秒）	要指定在超时之前允许尝试连接的时长，请输入一个整数值。该值用于确定在尝试连接到电子邮件服务器时，经过多少秒之后会发生超时。

文本框	说明
	默认值为 30 秒。
TLS	如果邮件服务器使用传输层安全 (TLS) 或安全套接字层 (SSL) 等安全连接，则选择此选项。
用户名	输入电子邮件服务器的用户名。
密码	输入用于访问电子邮件服务器的密码。
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**。
电子邮件主题	输入电子邮件模板的主题，用于定义电子邮件通知模板的主题；例如，`<hostname> - <level> <name>`。
电子邮件	输入描述事件、发生时间和严重程度的模板正文信息。

5. 单击 **Send Test Email**（发送测试电子邮件）并检查结果。
6. 如果对测试结果满意，单击 **OK**（确定）。

配置减少重复

要配置减少重复，请执行以下操作：

1. 在 Core 中单击 **Configuration（配置）**选项卡。
2. 在 **Manage**（管理）选项中，单击 **Events**（事件）。
3. 在 **Repetition Reduction**（减少重复）区域中，单击 **Change**（更改）。
   此时将显示 Repetition Reduction（减少重复）对话框。
4. 选中 **Enable Repetition Reduction**（启用减少重复）。
5. 在 **Store events for X**（事件存储期限：X 分钟）文本框中，输入存储事件的分钟数以减少重复。
6. 单击**确定**。

配置事件保留

要配置事件保留，请执行以下操作：

1. 在 Core 中单击 **Configuration（配置）**选项卡。
2. 在 **Manage**（管理）选项中，单击 **Events**（事件）。
3. 在 **Database Connection Settings**（数据库连接设置）下，单击 **change**（更改）。
   此时将显示 **Database Connection Settings**（数据库连接设置）对话框。
4. 在 **Retain event and job history for**（保留事件和作业历史天数）文本框中，输入要保留事件相关信息的天数。
   例如，可以选择 30 天（默认）。
5. 单击**保存**。

管理恢复

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

关于系统信息

通过 AppAssure 可以查看有关 Core 的信息，包括系统信息、本地卷和已安装卷以及 AppAssure 引擎连接。

如果要卸载在 Core 上本地装载的个别或所有恢复点，可使用 **Tools**（工具）选项卡上的 **Mount**（装载）选项完成此操作。

查看系统信息

要查看系统信息，请执行以下操作：

1. 导航至 Core，然后选择 **Tools**（工具）选项卡。
2. 从 **Tools**（工具）选项中，单击 **System Info**（系统信息）。

下载安装程序

您可以从 Core 下载安装程序。在 **Tools**（工具）选项卡中，可选择下载代理安装程序或 Local Mount Utility。

注: 有关如何访问代理安装程序，请参阅 Downloading And Installing The Agent Installer（下载和安装代理安装程序）。有关部署代理安装程序的更多信息，请参阅 **Dell.com/support/home** 上的 *Dell DL4300 Appliance Deployment Guide*（Dell DL4300 设备部署指南）。有关如何访问 Local Mount Utility 安装程序，请参阅 About The Local Mount Utility（关于 Local Mount Utility）。有关 Local Mount Utility 的更多信息，请参阅 Downloading And Installing The Local Mount Utility（下载和安装 Local Mount Utility）。

关于代理安装程序

代理安装程序用于在计划由 Core 保护的机器上安装 AppAssure 代理应用程序。如果确定有一台机器需要代理安装程序，可从 Core 的 **Tools**（工具）选项卡下载 Web 安装程序。

注: Core 的下载要从许可证门户执行。要下载 Core 安装程序，请访问 **https://licenseportal.com**。

下载和安装代理安装程序

您可在受 Core 保护的任意机器上下载并部署代理安装程序。

要下载并安装代理安装程序，请执行以下操作：

1. 从许可证门户或从 Core 下载代理安装程序文件。

例如：Agent-X64-5.3.x.xxxxx.exe

2. 单击 **Save File**（保存文件）。

   有关安装代理的更多信息，请参阅 **Dell.com/support/home** 上的 *Dell DL4300 Appliance Deployment Guide*（Dell DL4300 设备部署指南）。

关于 Local Mount Utility

Local Mount Utility (LMU) 是一种可下载的应用程序，可用于从任何机器在远程 Core 上安装恢复点。这款轻型公用程序包括 `aavdisk` 和 `aavstor` 驱动程序，但不作为服务运行。默认情况下，此公用程序安装在 **C:\Program Files\AppRecovery\Local Mount Utility** 目录，并在机器的桌面上显示快捷方式。

虽然此公用程序旨在用于远程访问 Core，但也可以将 LMU 安装在 Core 上。在 Core 上运行时，此应用程序将识别和显示该 Core 上的所有装载，包括通过 Core 控制台执行的装载。同样，在 LMU 上执行的装载也会显示在控制台中。

下载并安装 Local Mount Utility

要下载和安装 Local Mount Utility，请执行以下操作：

1. 在要安装 LMU 的机器上，在浏览器中输入控制台 URL 并使用您的用户名和密码登录，以访问 Core 控制台。
2. 在 Core 控制台中，单击 **Tools（工具）**选项卡。
3. 在 **Tools**（工具）选项卡中，单击 **Downloads**（下载）。
4. 在 **Local Mount Utility** 下，单击 **Download web installer**（下载 Web 安装程序）链接。
5. 在 **Opening LocalMountUtility-Web.exe**（打开 LocalMountUtility-Web.exe）窗口中，单击 **Save File**（保存文件）。

   文件将保存至本地 Downloads 文件夹。在某些浏览器中，该文件夹将自动打开。
6. 在 **Downloads** 文件夹中，右键单击 **LocalMountUtility-Web** 可执行文件并单击 **Open**（打开）。

   根据机器的具体配置，可能会显示 **User Account Control**（用户帐户控制）窗口。
7. 如果显示 **User Account Control**（用户帐户控制）窗口，请单击 **Yes**（是）以允许程序对机器进行更改。

   此时将启动 **AppAssure Local Mount Utility** 安装向导。
8. 在 **AppAssure Local Mount Utility** 安装向导的 **Welcome**（欢迎）屏幕上，单击 **Next**（下一步）进入 **License Agreement**（许可协议）页面。
9. 在 **License Agreement**（许可协议）页面上，选择 **I accept the terms in the license agreement**（我接受许可协议中的条款），然后单击 **Next**（下一步）进入 **Prerequisites**（前提条件）页面。
10. 在 **Prerequisites**（前提条件）页面中，安装所需的全部必备组件，然后单击 **Next**（下一步）进入 **Installation Options**（安装选项）页面。
11. 在 **Installation Options**（安装选项）页面中，完成以下任务：
    a. 单击 **Change**（更改）按钮，选择 LMU 的目标文件夹。

       注: 默认目标文件夹为 **C:\Program Files\AppRecovery\LocalMountUtility**。

    b. 选择是否 **Allow Local Mount Utility to automatically send diagnostic and usage information to AppAssure Software, Inc.**（允许 Local Mount Utility 将诊断和使用信息自动发送至 AppAssure Software, Inc.）。
    c. 单击 **Next**（下一步）进入 **Progress**（进度）页面，然后下载此应用程序。此应用程序将下载至目标文件夹，进度栏中将显示下载进度。完成后，向导将自动进入 **Completed**（已完成）页面。
12. 单击 **Finish**（完成）关闭向导。

将 Core 添加至 Local Mount Utility

要装载恢复点，必须将 Core 添加至 LMU。可以添加无限数量的 Core。

要将 Core 添加至 Local Mount Utility，请执行以下操作：

1. 在已安装 LMU 的机器上，通过双击桌面图标启动 LMU。
2. 如果显示 **User Account Control**（用户帐户控制）窗口，请单击 **Yes**（是）以便允许程序对机器进行更改。
3. 在 AppAssure Local Mount Utility 窗口的左上角，单击 **Add core**（添加 Core）。
4. 在 **Add Core**（添加 Core）窗口中，根据下面的说明输入所需的凭据：

文本框	说明
Host name（主机名）	要从中装载恢复点的 Core 的名称。 **注:** 如果将 LMU 安装在 Core 上，LMU 将自动添加 localhost 机器。
Port（端口）	用于与 Core 通信的端口号。 默认端口号为 8006。
Use my Windows user credentials（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。
Use specific credentials（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。
User name（用户名）	用于访问 Core 机器的用户名。 **注:** 仅当选择 Use specific credentials（使用特定凭据）时，才可使用此选项。
密码	用于访问 Core 机器的密码。 **注:** 仅当选择 Use specific credentials（使用特定凭据）时，才可使用此选项。

5. 单击 **Connect**（连接）。
6. 如果要添加多个 Core，请根据需要重复步骤 3 到步骤 5。

使用 Local Mount Utility 浏览已装载恢复点

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。

要使用 Local Mount Utility 浏览已安装恢复点：

1. 在已安装 LMU 的机器上，通过双击桌面图标启动 LMU。
2. 在 **Local Mount Recovery**（本地安装恢复）主屏幕上，单击 **Active mounts**（活动安装）。
   此时将打开 **Active Mounts**（活动安装）窗口，其中会显示所有已安装的恢复点。

3. 单击要从中恢复的恢复点旁边的 **Explore**（浏览），以打开已消除重复数据的卷所在的文件夹。

使用 Local Mount Utility 装载恢复点

装载恢复点之前，LMU 必须连接至存储恢复点的 Core。如将 Core 添加至 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，如果先装载由某个 Core 保护的代理的恢复点，然后装载由不同 Core 保护的代理的恢复点，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。

要使用 Local Mount Utility 装载恢复点，请执行以下操作：

1. 在已安装 LMU 的机器上，通过双击桌面图标启动 LMU。
2. 在 **AppAssure Local Mount Utility** 主窗口中，展开导航树中的目标 Core，以显示受保护的代理。
3. 从导航树中选择所需的代理。
   恢复点显示在主框架中。
4. 展开要装载的恢复点，以显示各磁盘卷或数据库。
5. 右键单击要装载的恢复点，然后选择以下选项之一：
   - Mount（装载）
   - Mount Writable（装载可写）
   - Mount with previous writes（使用之前的写入装载）
   - Advanced mount（高级装载）
6. 在 **Advanced Mount**（高级装载）窗口中，根据下表中的说明完成各个选项：

文本框	说明
Mount point path（装载点路径）	要选择除默认装载点路径以外的恢复点路径，请单击 **Browse**（浏览）按钮。
Mount type（装载类型）	选择以下选项之一： • Mount Read-only（装载只读） • Mount Writable（装载可写） • Mount Read-only with previous writes（使用之前的写入装载只读）

7. 单击 **Mount**（装载）。

LMU 将自动打开包含已装载恢复点的文件夹。

注: 如果选择已装载的恢复点，则 **Mounting**（装载）对话框将询问是否卸载恢复点。

使用 Local Mount Utility 卸载恢复点

要使用 Local Mount Utility 卸载恢复点：

1. 在已安装 LMU 的机器上，通过双击桌面图标启动 LMU。
2. 在 **Local Mount Recovery**（本地安装恢复）主屏幕上，单击 **Active mounts**（活动安装）。
   此时将打开 **Active Mounts**（活动安装）窗口，其中会显示所有已安装的恢复点。
3. 选择下表中说明的选项之一以卸载恢复点。

选项	说明
Dismount（卸载）	仅卸载相邻的恢复点。

选项	说明
	a. 单击所选恢复点旁的 **Dismount**（卸载）。 b. 关闭该窗口。
Dismount all（全部卸载）	卸载所有已安装的恢复点。 a. 单击 **Dismount all**（全部卸载）。 b. 在 **Dismount All**（全部卸载）窗口中，单击 **Yes**（是）进行确认。 c. 关闭该窗口。

关于 Local Mount Utility 托盘菜单

LMU 托盘菜单位于桌面任务栏中。右键单击该图标可显示以下选项：

Browse Recovery Points（浏览恢复点）	打开 LMU 主屏幕。
Active Mounts（活动安装）	打开 Active Mounts（活动安装）屏幕。
选项	打开 Options（选项）屏幕，可在其中更改 **Default Mount Point Directory**（默认安装点目录）、**Default Core Credentials**（默认 Core 凭据）和 LMU 用户界面的 **Language**（语言）。
关于	打开许可信息的初始屏幕。
退出	关闭应用程序。

注: 使用主屏幕上方的 X 将应用程序最小化到托盘中。

使用 Core 和代理选项

通过在 LMU 主屏幕中右键单击 Core 或代理，可使用某些选项。其中包括：

- Localhost Options（Localhost 选项）
- Remote Core Options（远程 Core 选项）
- Agent Options（代理选项）

访问 Localhost 选项

要访问 Localhost 选项，请右键单击 Core 或代理，然后单击 **Reconnect to Core**（重新连接到 Core）。此时将更新并刷新 Core 中的信息；例如，最近添加的代理。

访问远程 Core 选项

要访问远程 Core 选项，请右键单击 Core 或代理，然后根据下面的说明选择一个远程 Core 选项：

选项	说明
Reconnect to core（重新连接到 Core）	刷新并更新 Core 中的信息，例如最近添加的代理。

选项	说明
Remove core（移除 Core）	从 **Local Mount Utility** 删除 Core。
Edit core（编辑 Core）	打开 **Edit Core**（编辑 Core）窗口，可在其中更改主机名、端口和凭据。

访问代理选项

要访问代理选项，请右键单击 Core 或代理，然后单击 **Refresh recovery points**（刷新恢复点）。此时将更新所选代理的恢复点列表。

管理保留策略

所有受保护服务器的定期备份快照会随着时间推移在 Core 上累积。保留策略用于长期保留备份快照，并帮助管理这些备份快照。保留策略通过每夜前滚流程实施，该流程有助于老化和删除旧备份。有关配置保留策略的信息，请参阅自定义保留策略设置。

存档到云

您可以从 Core 控制台将数据直接上载到多家云提供商，从而将数据存档到云。兼容的云包括 Windows Azure、Amazon、Rackspace 和任何基于 OpenStack 的提供商。

要将存档导出到云，请执行以下操作：

- 将您的云帐户添加到 Core 控制台。有关更多信息，请参阅添加云帐户。
- 存档您的数据，并将其导出到云帐户。
- 通过从云位置导入存档数据对存档数据进行检索。

关于存档

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，就需要创建长期（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。AppAssure 中的存档功能用于支持长期保留合规和非合规数据。它还用于将复制数据播种到远程副本 Core。

创建存档

要创建存档，请执行以下操作：

1. 在 Core 控制台中，单击 **Configuration**（配置）选项卡。
2. 在 **Manage**（管理）选项中，单击 **Archive**（存档）。
   此时将显示 **Create Archive**（创建存档）对话框。
3. 在 **Create Archive**（创建存档）对话框中，根据下面的说明输入存档的详细信息：

文本框	说明
Date range（日期范围）	要指定日期范围，请选择结束日期和开始日期。

文本框	说明
Archive password（存档密码）	输入存档的密码，用于建立保护存档的登录凭据。
Confirm（确认）	重新输入保护存档的密码，此密码用于验证在 **Archive Password**（存档密码）文本框中输入的信息。
Output Location（输出位置）	输入输出的位置，用于定义您要存档驻留的位置的路径。该路径可以是本地磁盘或网络共享。例如 **d:\work\archive** 或 **\\servername\sharename**（用于网络路径）。 **注:** 如果输出位置是网络共享，则输入用于连接共享的用户名和密码。
User name（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。
最大大小	输入用于存档的空间量。您可以选择： • Entire Target（整个目标） • 特定数量（MB 或 GB）
Recycle action（循环操作）	选择相应的循环操作。
注释	输入捕获存档时所必需的任何附加信息。

4. 单击 **Archive**（存档）。

设置计划存档

计划存档功能可让您设置自动创建所选机器的存档并保存到指定位置的时间。这适用于您希望保存计算机的频繁存档而无需麻烦手动创建存档的情况。完成以下过程中的步骤以计划自动存档。
要设置计划存档，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools（工具）**选项卡。
2. 从 **Archive（存档）**选项中，单击 **Scheduled（计划）**。
3. 在 Scheduled Archive（计划存档）页面中，单击 **Add（添加）**。
   此时将显示 **Add Archive Wizard（添加存档向导）**对话框。
4. 在 **Add Archive Wizard（添加存档向导）**的 **Location（位置）**页面中，从 **Location Type（位置类型）**下拉列表中选择以下选项之一：
   - Local: Output location（本地：输出位置）– 输入输出的位置。用于定义您要保留存档的位置路径。
   - 网络
     - Output location（输出位置）– 输入输出的位置。用于定义您要保留存档的位置路径。
     - User Name（用户名）：输入用户名。用于建立网络共享的登录凭据。
     - Password（密码）：输入网络路径的密码。用于建立网络共享的登录凭据。
   - Cloud（云）
     - Account（帐户）：从下拉列表中选择帐户。要选择云账户，首先必须在 Core 控制台中添加此账户。

- Container（容器）：从下拉菜单中选择与您的帐户关联的容器。
- Folder Name（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 AppAssure-5-Archive-[创建日期]-[创建时间]

5. 单击**下一步**。
6. 在向导的 **Machines（机器）**页面中，选择包含要存档的恢复点的受保护机器。
7. 单击 **Next（下一步）**
8. 在 **Options（选项）**页面上，从下拉列表中选择以下 Recycle Actions（循环操作）之一：
   - **Replace this Core（替换此 Core）**：覆盖与此 Core 相关的任何现有的存档数据，但保留其他 Core 的数据。
   - **Erase completely（完全擦除）**：先清除此目录中的所有存档数据，再写入新存档。
   - **Incremental（增量）**：允许向现有存档添加恢复点。此选项会比较恢复点，以避免重复写入存档中已存在的数据。
9. 在 **Schedule（计划）**页面上，选择以下发送数据频率选项之一：
   - Daily: At time（每天：时间）- 选择您要创建日常存档的时间。
   - Weekly（每周）
     - At day of week（星期几）：选择在一周中的某一天自动创建存档。
     - At time（时间）：选择您要创建日常存档的时间。
   - Monthly（每月）
     - At day of months（月份中的日期）：选择要自动创建存档的月份中的日期。
     - At time（时间）：选择您要创建日常存档的时间。
10. 要暂停存档并在稍后继续执行，请选择 **Initial pause archiving（初始暂停存档）**。

    您可能想要在继续存档前暂停计划存档，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存档。
11. 单击**完成**。

暂停或恢复计划存档

如果您选择在执行计划存档设置过程时初始暂停存档，则应在稍后恢复计划存档。
要暂停或恢复计划存档，请执行以下操作：

1. 导航至 **Core 控制台**，然后单击 **Tools（工具）**选项卡。
2. 从 **Archive（存档）**选项中，单击 **Scheduled（计划）**。
3. 在 **Scheduled Archive（计划存档）**页面中，执行以下操作之一：
   - 选择首选的存档，然后相应单击以下操作之一：
     - Pause（暂停）
     - Resume（恢复）
   - 单击首选存档旁边的下拉菜单，然后相应单击以下操作之一：
     - Pause（暂停）
     - Resume（恢复）

   存档状态会显示在 **Schedule（计划）**栏中。

编辑计划存档

1. 在 Core 控制台中，单击 **Tools（工具）**选项卡。
2. 从 **Archive（存档）**选项中，单击 **Scheduled（计划）**。
3. 在 Scheduled Archive（计划存档）页面中，单击您要更改的存档旁边的下拉菜单，然后单击 **Edit（编辑）**。

   此时将显示 **Add Archive Wizard（添加存档向导）**对话框。
4. 在 **Add Archive Wizard（添加存档向导）**的 **Location（位置）**页面中，从 **Location Type（位置类型）**下拉列表中选择以下选项之一：
   - Local: Output location（本地：输出位置）– 输入输出的位置。用于定义您要保留存档的位置路径。
   - Network（网络）
     - Output location（输出位置）– 输入输出的位置。用于定义您要保留存档的位置路径。
     - User Name（用户名）：输入用户名。用于建立网络共享的登录凭据。
     - Password（密码）：输入网络路径的密码。用于建立网络共享的登录凭据。
   - Cloud（云）
     - Account（帐户）：从下拉列表中选择帐户。要选择云账户，首先必须在 Core 控制台中添加此账户。
     - Container（容器）：从下拉菜单中选择与您的帐户关联的容器。
     - Folder Name（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 AppAssure-5-Archive-[创建日期]-[创建时间]
5. 单击**下一步**。
6. 在向导的 **Machines（机器）**页面中，选择包含要存档的恢复点的受保护机器。
7. 单击 **Next（下一步）**
8. 在 **Schedule（计划）**页面上，选择以下发送数据频率选项之一：
   - Daily: At time（每天：时间）- 选择您要创建日常存档的时间。
   - Weekly（每周）
     - At day of week（星期几）：选择在一周中的某一天自动创建存档。
     - At time（时间）：选择您要创建日常存档的时间。
   - Monthly（每月）
     - At day of months（月份中的日期）：选择要自动创建存档的月份中的日期。
     - At time（时间）：选择您要创建日常存档的时间。
9. 要暂停存档并在稍后继续执行，请选择 **Initial pause archiving（初始暂停存档）**。

   您可能想要在继续存档前暂停计划存档，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存档。
10. 单击**完成**。

检查存档

您可以通过执行存档检查扫描存档的结构完整性。此检查可验证存档内是否存在所有必要的文件。要执行存档检查，请完成以下过程中的步骤：

1. 在 Core 控制台中，单击 **Tools（工具）**选项卡。
2. 从 **Archive（存档）**选项中，单击 **Check Archive（检查存档）**。

此时将显示 **Check Archive（检查存档）**对话框。

3. 从下拉式列表中选择以下选项之一：
   - Local: Output location（本地：输出位置）– 输入输出的位置。用于定义您要保留存档的位置路径。
   - Network（网络）
     - Output location（输出位置）– 输入输出的位置。用于定义您要保留存档的位置路径。
     - User Name（用户名）：输入用户名。用于建立网络共享的登录凭据。
     - Password（密码）：输入网络路径的密码。用于建立网络共享的登录凭据。
   - Cloud（云）
     - Account（帐户）：从下拉列表中选择帐户。要选择云账户，首先必须在 Core 控制台中添加此账户。
     - Container（容器）：从下拉菜单中选择与您的帐户关联的容器。
     - Folder Name（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 AppAssure-5-Archive-[创建日期]-[创建时间]
4. 要执行结构完整性检查，请选择 **Structure integrity**（结构完整性）。
5. 单击 **Check File**（检查文件）。

导入存档

要导入存档，请执行以下操作：

1. 在 Core 控制台中，选择 **Configuration**（配置）选项卡。
2. 在 **Manage**（管理）选项中，依次单击 **Archive**（存档）和 **Import**（导入）。
   此时将显示 **Import Archive**（导入存档）对话框。
3. 在 **Import Archive**（导入存档）对话框中，根据下面的说明输入导入存档的详细信息：

文本框	说明
Input Location（输入位置）	选择导入存档的位置。
User name（用户名）	要建立访问权限以保护存档，请输入登录凭据。
密码	输入用于访问存档的密码。

4. 单击 **Check File**（检查文件），验证要导入的存档是否存在。
   此时将显示 **Restore（还原）**对话框。
5. 在 **Restore**（还原）对话框中，验证源 Core 的名称。
6. 选择要从存档导入的代理。
7. 选择存储库。
8. 单击 **Restore**（还原）以导入存档。

管理 SQL 可附加性

SQL 可附加性配置允许 Core 使用 Microsoft SQL Server 的本地实例对 SQL 数据库和 SQL Server 快照中的日志文件执行附加操作。Core 通过这种可附加性测试可检查 SQL 数据库的一致性，并确保备份快照中的所有数据文件（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运行，也可以将其作为每夜作业的一部分。

可附加性要求 AppAssure Core 机器上存在 Microsoft SQL Server 的本地实例。此实例必须是从 Microsoft 或许可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。

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 的磁盘存储格式在 64 位和 32 位环境中相同，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。

小心: Core 上的 SQL Server 版本不得低于所有已安装 SQL Server 的代理上的 SQL Server 版本。

配置 SQL 可附加性设置

在受保护的 SQL 数据库上执行可附加性检查之前，请选择 Core 机器上的一个本地 SQL Server 实例，以用于对代理机器执行检查。

注: 可附加性要求 AppAssure Core 机器上存在 Microsoft SQL Server 的本地实例。此实例必须是从 Microsoft 或许可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。

要配置 SQL 可附加性设置，请执行以下操作：

1. 导航至 Core 控制台，然后单击选项卡。
2. 单击 **Configuration（配置） → Settings（设置）**。
3. 在 Nightly Jobs（每夜作业）窗格中，单击 **Change（更改）**。
   此时将显示 **Nightly Job**（每夜作业）对话框。
4. 选择 **Attachability Check Job** （可附加性检查作业），然后单击 **Settings**（设置）。
5. 使用下拉菜单从以下选项中选择在 Core 上安装的 SQL Server 实例：
   您可以选择：
   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
   - **SQL Server 2014**
6. 选择凭据类型。
   您可以选择：
   - **Windows**
   - **SQL**
7. 根据下表中的说明，指定具有 Windows 或 SQL Server 实例管理权限的凭据：

文本框	说明
用户名	输入具有 SQL Server 登录权限的用户名。
密码	输入 SQL 可附加性的密码。用于控制登录活动。

8. 单击 **Test Connection**（测试连接）。

   注: 如果输入错误凭据，将显示一条消息，指出凭据测试失败。纠正凭据信息，然后再次运行连接测试。
9. 单击**保存**。
   此时即可在受保护 SQL Server 数据库上运行可附加性检查。

10. 在 Nightly Jobs（每夜作业）窗口中，单击 **OK（确定）。**
    现在可计划附加性检查随每夜作业一起执行。

配置每夜 SQL 可附加性检查和日志截断

要配置每夜 SQL 可附加性检查和日志截断，请执行以下操作：

1. 在 Core 的左侧导航区域中，选择要对其执行每夜可附加性检查和日志截断的机器，然后单击 **SQL Server Settings**（SQL Server 设置）。
2. 导航至 Core 控制台。
3. 单击 **Configuration（配置）→ Settings（设置）**。
4. 在 **Nightly Jobs（每夜作业）**部分中，单击 **Change（更改）**。
5. 根据组织的具体需要，选择或清除以下 SQL Server 设置：
   - **Attachability Check Job（可附加性检查作业）**
   - **Log Truncation Job（日志截断作业）**
6. 单击**确定**。
   可附加性和日志截断设置将对受保护的 SQL Server 生效。

管理 Exchange 数据库可装载性检查和日志截断

使用 AppAssure 备份 Microsoft Exchange Server 时，可在每个快照后对所有 Exchange 数据库执行可装载性检查。此损坏检测功能可以警示管理员留意潜在故障，确保 Exchange Server 上的所有数据在发生故障时都可以成功恢复。

注: 可装载性检查和日志截断功能仅适用于 Microsoft Exchange 2007、2010 和 2013。此外，必须在 Exchange 中为 AppAssure 代理服务帐户分配 Organizational Administrator（组织管理员）角色。

配置 Exchange 数据库可装载性和日志截断

可以查看、启用或禁用 Exchange 数据库服务器设置，包括自动可装载性检查、每夜校验和检查或每夜日志截断。

要配置 Exchange 数据库可装载性和日志截断，请执行以下操作：

1. 在 Core 控制台的左侧导航区域中，选择要为其配置可装载性检查和日志截断的机器。
   此时将显示所选机器的 **Summary**（摘要）选项卡。
2. 单击 **Exchange Server Settings**（Exchange Server 设置）。
   此时将显示 **Exchange Server Settings**（Exchange Server 设置）对话框。
3. 根据组织的具体需要，选择或清除以下 Exchange Server 设置：
   - **Enable automatic mountability check（启用自动可装载性检查）**
   - **Enable nightly checksum check（启用每夜校验和检查）**
   - **Enable nightly log truncation（启用每夜日志截断）**
4. 单击**确定**。
   可安装性和日志截断设置将对受保护的 Exchange Server 生效。

   注: 有关强制日志截断的信息，请参阅强制日志截断。

强制执行可装载性检查

要强制执行可装载性检查，请执行以下操作：

1. 在 AppAssure Core 控制台的左侧导航区域中，选择要对其强制执行可装载性检查的机器，然后单击 **Recovery Points**（恢复点）选项卡。
2. 单击列表中恢复点旁的 **>** 以展开视图。
3. 单击 **Force Mountability Check**（强制可装载性检查）。
   此时将显示一条消息，询问是否要强制执行可装载性检查。
4. 单击**是**。

   注: 有关如何查看可附加性检查状态的说明，请参阅查看事件和警报。

   系统将执行可装载性检查。

强制校验和检查

要强制校验和检查，请执行以下操作：

1. 在 Core 控制台的左侧导航区域中，选择要对其强制执行校验和检查的机器，然后单击 **Recovery Points**（恢复点）选项卡。
2. 单击列表中恢复点旁的 **>** 以展开视图。
3. 单击 **Force Checksum Check**（强制校验和检查）。
   Force Attachability Check（强制可附加性检查）窗口提示您是否要强制执行校验和检查。
4. 单击**是**。
   系统将执行校验和检查。

   注: 有关如何查看可附加性检查状态的信息，请参阅查看事件和警报。

强制日志截断

注: 此选项仅适用于 Exchange 或 SQL 机器。

要强制日志截断，请执行以下操作：

1. 导航至 Core 控制台，然后单击 **Machines（机器）**选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要截断日志的机器的超链接。
   - 或者，在导航窗格中选择要截断日志的机器。
3. 在该机器的 **Actions**（操作）下拉菜单中，单击 **Force Log Truncation**（强制日志截断）。
4. 确认是否继续强制日志截断。

恢复点状态指示器

在受保护 SQL 或 Exchange Server 上创建恢复点后，应用程序将在 **Recovery Points**（恢复点）表中显示相应的彩色状态指示器。显示的颜色取决于受保护机器的检查设置以及这些检查是否成功，如下表中所述。

注: 有关查看恢复点的更多信息，请参阅查看恢复点。

下表列出为 SQL 数据库显示的状态指示器。

SQL 数据库的恢复状态点颜色

状态颜色	说明
白色	表示存在以下情况之一： • SQL 数据库不存在。 • 未启用可附加性检查。 • 尚未运行可附加性检查。
黄色	表示 SQL 数据库处于脱机状态，无法执行检查。
红色	表示可附加性检查失败。
绿色	表示可附加性检查通过。

下表列出为 Exchange 数据库显示的状态指示器。

Exchange 数据库的恢复状态点颜色

术语标题	说明标题
白色	表示存在以下情况之一： • Exchange 数据库不存在。 • 未启用可安装性检查。 **注:** 这可以适用恢复点内的特定卷。
黄色	表示已启用 Exchange 数据库可安装性检查，但尚未运行检查。
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	表示可安装性检查或校验和检查通过。

注: 无关联 Exchange 或 SQL 数据库的恢复点将显示白色状态指示器。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。

3

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。

监测设备的状态

您可以使用 **Overall Status（总体状态）**页面上的 **Appliance（设备）**选项卡监测设备子系统的状态。**Overall Status（总体状态）**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。

Overall Status（总体状态）页面还提供用于深入查看每个子系统详细信息的工具链接，有助于对警告或错误进行故障排除。**System Administrator** 链接适用于 Appliance Hardware（设备硬件）和 Storage Hardware（存储硬件）子系统，可引导您登录到用于管理硬件的 System Administrator 应用程序。有关 System Administrator 应用程序的更多信息，请参阅位于 **dell.com/support/home** 上的 *OpenManage Server Administrator User's Guide*（OpenManage Server Administrator 用户指南）。**Provisioning Status**（配置状态）链接适用于 Storage Provisioning（存储配置）子系统，可打开 **Tasks**（任务）屏幕，其中显示该子系统的配置状态。如果存储可供配置，则会在配置任务旁边显示指向 **Actions（操作）**下的 **Provision**（配置）的链接。

配置存储

该设备配置可用的 DL4300 内部存储以及用于以下项目的所有已连接的外部存储柜：

- AppAssure 存储库

  注: 如果已配置光纤信道 HBA，则应手动执行存储库的创建过程。AppAssure 将不会自动在根目录中创建存储库。有关更多信息，请参阅 *Dell DL4300 Appliance Deployment Guide*（Dell DL4300 设备部署指南）。

- 受保护机器的虚拟待机

注: 支持连接到 H830 控制器的具有 1 TB、2 TB、4 TB 或 6 TB（提供高容量）驱动器的 MD1400。最多可以支持四个 MD1400。

注: DL4300 高容量配置支持 H830 PERC SAS 适配器或两个光纤信道 HBA。有关配置光纤信道 HBA 的更多信息，请参阅位于 **dell.com/support/home** 的 *DL4xxx — Fibre Channel Implementation*（DL4xxx - 光纤信道实施）白皮书。

开始在磁盘上配置存储之前，请确定您要为待机虚拟机配置多少存储。您可以分配任意百分比的可用容量来托管待机虚拟机。例如，如果使用存储资源管理 (SRM)，则可以在要配置的任意设备上分配最多 100% 的容量至虚拟机。使用 AppAssure 的实时恢复功能，您可以使用这些虚拟机来快速替换受设备保护的任意故障服务器。

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。

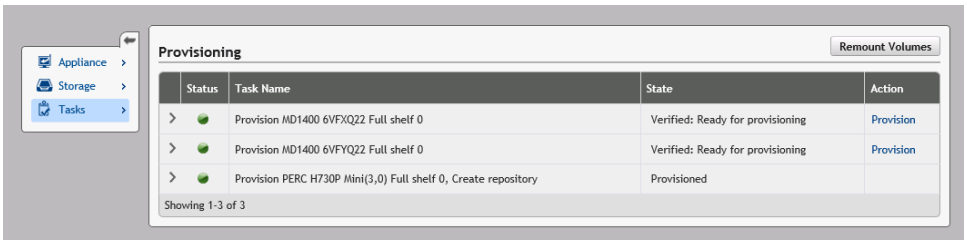
选择 **Appliance**（设备）选项卡时，AppAssure Appliance 软件会为系统中所有受支持的控制器分配可用存储空间，并验证硬件是否符合要求。

要完成所有可用存储的磁盘配置，请执行以下操作：

1. 在 **Appliance（设备）**选项卡中，单击 **Tasks（任务）→ Provisioning（配置）**。

   Provisioning（配置）屏幕将显示估计的配置容量。此容量用于创建新的 AppAssure 存储库。

   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. 单击您要配置的存储旁边的 Action（操作）栏中的 **Provision**（配置），打开 **Provisioning Storage**（配置存储）窗口。
3. 在 **Optional Storage Reserve**（可选存储保留）部分，选中 **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes**（分配一部分为待机虚拟机或其他目的配置的存储）复选框。否则，在 **Optional Storage Reserve**（可选存储保留）部分中所示的存储百分比将被连接的所有磁盘占用。
4. 单击 **Provision**（配置）。



配置所选存储

要配置所选存储，请执行以下操作：

1. 在 **Appliance**（设备）选项卡中，单击 **Tasks（任务）→ Provisioning**（配置）。

   Provisioning（配置）屏幕将显示估计的配置容量。该容量用于新建新的 AppAssure 存储库。
2. 要仅配置部分可用空间，请单击您要配置的存储空间旁边的 **Action**（操作）下的 **Provision**（配置）。
   - 要创建新存储库，请选择 **Create a new repository**（创建新存储库），然后提供存储库的名称。

     默认情况下，存储库名称显示为 Repository 1（存储库 1）。您可以选择覆盖该名称。
   - 要为现有存储库添加容量，请选择 **Expand the existing repository**（扩展现有存储库），然后从 **Existing Repositories**（现有存储库）列表中选择该存储库。

   注: 要添加容量，建议扩展现有存储库，而不是添加存储库。分离的存储库无法有效利用容量，因为不能跨不同的存储库执行重复数据消除。
3. 在 **Optional Storage Reserve**（可选存储保留）下，选择 **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes**（分配一部分为待机虚拟机或其他目的配置的存储），然后指定要分配给 VM 的存储百分比。
4. 单击 **Provision**（配置）。

   磁盘配置开始，并且 AppAssure 存储库创建状态显示在 **Tasks**（任务）屏幕的 **Status**（状态）区域。**Status**（状态）显示为 **Provisioned**（已配置）。
5. 要在磁盘配置完成后查看详细信息，请单击状态指示灯旁边的 **>**。

   Tasks（任务）页面将展开，并显示状态、存储库和虚拟磁盘详细信息（如果已分配）。

删除虚拟磁盘的空间分配

开始此过程之前，请确定您想要删除的虚拟磁盘。在 Core 控制台中，选择 **Appliance**（设备）选项卡，单击 **Tasks**（任务），然后展开包含虚拟磁盘的存储库，以查看虚拟磁盘详细信息。
要删除虚拟磁盘的空间分配，请执行以下操作：

1. 在 OpenManage Server Administrator 应用程序中，展开 **Storage**（存储）。
2. 展开承载该虚拟磁盘的控制器，然后选择 **Virtual Disks**（虚拟磁盘）。
3. 选择要移除的虚拟磁盘，然后从 **Tasks**（任务）下拉菜单中选择 **Delete**（删除）。
4. 确认删除后，在 Core 控制台 **Appliance**（设备）选项卡的 **Tasks**（任务）屏幕中显示该空间可供配置。

解决失败任务

AppAssure 通过 Core 控制台主页以及 **Appliance**（设备）选项卡的 **Tasks**（任务）屏幕上的事件来报告失败的验证、配置和恢复任务。

要了解如何解决失败的任务，请选择 **Appliance**（设备）选项卡，然后单击 **Tasks**（任务）。通过单击 **Status**（状态）旁边的 **>** 来展开失败任务，然后查看错误消息和建议的操作。

升级设备

要升级您的设备，请执行以下操作：

1. 从 **dell.com/support** 将 **Recovery and Update Utility** 下载到 DL4300 Backup to Disk appliance 中。
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、ASP .NET MVC3、LSI 提供程序、DL 应用程序、OpenManage Server Administrator 和 AppAssure 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。

   注: 作为 AppAssure Core 软件升级过程的一部分，Recovery and Upgrade Utility 会通知您当前已安装的 AppAssure 版本，并提示您确认是否要将 Core 软件升级到该公用程序中捆绑的版本。不支持 AppAssure Core 软件降级。
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. 从 **dell.com/support** 将 **Recovery and Update Utility** 下载到您的设备中。
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、ASP .NET MVC3、LSI 提供程序、DL 应用程序、OpenManage Server Administrator 和 AppAssure 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 AppAssure 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 AppAssure Core 软件。

   注: 不支持 AppAssure Core 软件降级。
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 AppAssure Appliance Configuration Wizard（AppAssure 设备配置向导），否则将启动 Core 控制台。

4

保护工作站和服务器

关于保护工作站和服务器

要保护数据，必须在 Core 控制台中添加您要保护的工作站和服务器；例如，您的 Exchange Server、SQL Server 或 Linux 服务器。

注: 在本节中，*机器*一词一般还指安装在该机器上的 AppAssure 代理软件。

在 Core 控制台中，可以识别安装了 AppAssure 代理软件的机器并指定要保护的卷、定义保护计划、添加额外的安全措施（例如加密）等。有关如何访问 Core 控制台以保护工作站和服务器的更多信息，请参阅保护机器。

配置机器设置

在 AppAssure 中添加机器保护后，即可轻松修改基本机器配置设置（例如名称和主机名）、保护设置（更改机器上卷的保护计划、添加或移除卷，或暂停保护）等。

查看和修改配置设置

要查看和修改配置设置：

1. 添加受保护机器后，请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后单击要修改的机器的超链接。
   - 在 **Navigation**（导航）窗格中选择要修改的机器。
2. 单击 **Configuration**（配置）选项卡。
   此时将显示 **Settings**（设置）页面。
3. 单击 **Edit**（编辑），以根据下表中的说明修改机器设置。

文本框	说明
显示名称	输入机器的显示名称。 在 Core 控制台中显示的此机器的名称。默认情况下，此名称是该机器的主机名。如果需要，可以将显示名称更改为更容易记住的名称。
主机名	输入机器的主机名称。
端口	输入机器的端口号。 Core 使用此端口与此机器通信。
存储库	选择一个存储库以存储恢复点。显示 Core 上用于存储此机器中的数据的存储库。

文本框	说明
	注: 仅当不存在恢复点或上个存储库丢失时，才可更改此设置。
加密密钥	根据需要编辑加密密钥。指定是否应将加密应用到此机器上每个卷的数据，这些数据将存储在存储库中。

查看机器的系统信息

Core 控制台中显示所有受保护的机器，其中包括机器以及每台机器的状态的列表。
要查看机器的系统信息，请执行以下操作：

1. 在 Core 控制台中的 **Protected Machines**（受保护机器）下，选择要查看其详细系统信息的机器。
2. 单击该机器的 **Tools**（工具）选项卡。
   关于机器的信息会显示在 **System Information**（系统信息）页面中。显示的详细信息包括：
   - 主机名
   - OS Version（操作系统版本）
   - OS Architecture（操作系统架构）
   - Memory(Physical)（内存 [物理]）
   - Display Name（显示名称）
   - Fully Qualified Domain Name（完全限定域名）
   - Virtual Machine Type（虚拟机类型）（如果适用）

   还将显示关于此机器上所包含卷的详细信息，其中包括：
   - 名称
   - 设备 ID
   - 文件系统
   - Capacity（容量）（包括 Raw [原始]、Formatted [格式化] 和 Used [已用]）
   - 处理器
   - Type of Processors（处理器类型）
   - Network Adapters（网络适配器）
   - IP Addresses associated with this machine（与此机器关联的 IP 地址）

配置系统事件的通知组

在 AppAssure 中，可以通过创建通知组来配置如何报告机器的系统事件，其中可能包括系统警报、错误等。
要配置系统事件的通知组，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要修改的机器的超链接。
   - 在导航窗格中选择要修改的机器。

   此时将显示 **Summary**（摘要）选项卡。
3. 单击 **Configuration**（配置）选项卡，然后单击 **Events**（事件）。
   此时将显示 **Notification Groups**（通知组）页面。

4. 单击 **Use custom alert settings**（使用自定义警报设置），然后单击 **Apply**（应用）。
   此时将显示 **Custom Notification Groups**（自定义通知组）屏幕。
5. 单击 **Add Group**（添加组），以添加要发送系统事件列表的新通知组。
   此时将显示 **Add Notification Group**（添加通知组）对话框。

   注: 要使用默认警报设置，请选择 **Use Core alert settings**（使用 Core 警报设置）选项。
6. 根据下表中的说明添加通知选项。

文本框	说明
名称	输入通知组的名称。
说明	输入通知组的说明。
Enable Events（启用事件）	选择要与此通知组共享的事件。您可以选择 **All**（全部）或选择事件的子集以包括： • **BootCd** • **LocalMount** • **Metadata（元数据）** • **Clusters（群集）** • **Notification（通知）** • **PowerShellScripting** • **PushInstall（推送安装）** • **Attachability（可附加性）** • **Jobs（作业）** • **许可** • **LogTruncation（日志截断）** • **Archive（存档）** • **CoreService（Core 服务）** • **导出** • **Protection（保护）** • **复制** • **Rollback（回滚）** • **Rollup（前滚）** 也可以按类型选择： • **信息** • **警告** • **Error（错误）** **注:** 当按类型选择时，默认情况下，将自动启用相应的事件。例如，如果选择 Warning （警告），则将启用 Attachability（可附加性）、Jobs（作业）、Licensing（许可）、Archive（存档）、CoreService（Core 服务）、Export（导出）、Protection（保护）、Replication（复制）和 Rollback（回滚）事件。

文本框	说明
Notification Options（通知选项）	选择指定如何处理通知的方法。以下选项可供选择： • **Notify by Email**（通过电子邮件通知）- 在 To（收件人）、CC（抄送）和 BCC（密件抄送）文本框中指定将事件发送到哪些电子邮件地址。 **注:** 要接收邮件，必须先配置 SMTP。 • **Notify by Windows Event log**（通过 Windows 事件日志通知）— Windows 事件日志将控制通知。 • **Notify by syslogd**（通过系统日志通知）— 指定将事件发送到哪个主机名和端口。 – **Host**（主机）— 输入服务器的主机名。 – **Port**（端口）— 输入与服务器进行通信的端口号。

7. 单击 **OK**（确定）保存所做的更改。
8. 要编辑现有通知组，请单击要编辑的通知组旁边的 **Edit**（编辑）。
   此时将打开 **Edit Notification Group**（编辑通知组）对话框，在此可编辑设置。

编辑系统事件的通知组

要编辑系统事件的通知组，请执行以下操作：

1. 导航至 Core 控制台，然后单击 **Machines（机器）**选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要修改的机器的超链接。
   - 或者，在导航窗格中选择要修改的机器。

   此时将显示 **Summary**（摘要）选项卡。
3. 单击 **Configuration**（配置）选项卡，然后单击 **Events**（事件）。
4. 单击 **Use custom alert settings**（使用自定义警报设置），然后单击 **Apply**（应用）。
   此时将显示 **Custom Notification Groups**（自定义通知组）屏幕。
5. 单击 **Action**（操作）列下的 **Edit**（编辑）图标。
   此时将显示 **Edit Notification Group**（编辑通知组）对话框。
6. 根据下表中的说明编辑通知选项。

文本框	说明
名称	代表通知组的名称。 **注:** 不能编辑通知组的名称。
说明	输入通知组的说明。
Enable Events（启用事件）	选择要与此通知组共享的事件。您可以选择 **All**（全部）或选择事件的子集以包括： • **BootCd** • **LocalMount** • **Metadata（元数据）** • **Clusters（群集）**

文本框	说明
	• **Notification（通知）** • **PowerShellScripting** • **PushInstall（推送安装）** • **Attachability（可附加性）** • **Jobs（作业）** • **许可** • **LogTruncation（日志截断）** • **Archive（存档）** • **CoreService（Core 服务）** • **导出** • **Protection（保护）** • **复制** • **Rollback（回滚）** • **Rollup（前滚）** 也可以按类型选择： • **信息** • **警告** • **Error（错误）** **注:** 当按类型选择时，默认情况下，将自动启用相应的事件。例如，如果选择 Warning （警告），则将启用 Attachability（可附加性）、Jobs（作业）、Licensing（许可）、Archive（存档）、CoreService（Core 服务）、Export（导出）、Protection（保护）、Replication（复制）和 Rollback（回滚）事件。
Notification Options（通知选项）	选择指定如何处理通知的方法。以下选项可供选择： • **Notify by Email**（通过电子邮件通知）— 在 To（收件人）、CC（抄送）和 BCC（密件抄送）文本框中指定将事件发送到的电子邮件地址。 **注:** 要接收电子邮件，必须先配置 SMTP。 • **Notify by Windows Event log**（通过 Windows 事件日志通知）— Windows 事件日志将控制通知。 • **Notify by syslogd**（通过系统日志通知）— 必须指定要将事件发送到的主机名和端口。 – **Host**（主机）— 输入服务器的主机名。 – **Port**（端口）— 输入与服务器进行通信的端口号。

7. 单击**确定**。

自定义保留策略设置

机器的保留策略用于指定代理机器的恢复点将在存储库中存储多长时间。保留策略用于在较长的时间内保留备份快照，并帮助管理这些备份快照。前滚流程强制执行保留策略，该流程有助于老化和删除旧备份。此任务也是修改群集节点设置过程中的一个步骤。

要自定义保留策略设置，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要修改的机器的超链接。
   - 在导航窗格中选择要修改的机器。

   此时将显示 **Summary**（摘要）选项卡。
3. 单击 **Configuration**（配置）选项卡，然后单击 **Retention Policy**（保留策略）。

   注: 要使用为 Core 配置的默认保留策略，请确保选择了 Use Core default retention policy（使用 Core 默认保留策略）选项。

   此时将显示 **Retention Policy**（保留策略）屏幕。
4. 要设置自定义策略，请单击 **Use custom retention policy**（使用自定义保留策略）。
   此时将显示 **Custom Retention Policy**（自定义保留策略）屏幕。
5. 选择 **Enable Rollup**（启用前滚），然后根据需要指定保留备份数据的时间间隔。下面介绍了保留策略选项：

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**。 您可以选择： • **Days（天）** • **Weeks（周）** • **Months（月）** • **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]	提供更精细的保留期限。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。 您可以选择： • **Days（天）** • **Weeks（周）** • **Months（月）** • **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]	提供更精细的保留期限。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。 您可以选择： • **Days（天）** • **Weeks（周）** • **Months（月）**

文本框	说明
	• **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]	提供更精细的保留期限。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。 您可以选择： • **Weeks（周）** • **Months（月）** • **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]	提供更精细的保留期限。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。 您可以选择： • **Months（月）** • **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。

Newest Recovery Point（最新恢复点）文本框显示最新的恢复点。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 月

...然后每月将一个恢复点保留 1 年

将 Newest Recovery Point（最新恢复点）设置为当前日、月和年。

在此示例中，最旧恢复点的期限为 1 年、4 个月又 6 天。

6. 单击 **Apply**（应用）保存所做的更改。

7. 要根据机器的当前保留策略执行前滚，请选择 **Force Rollup**（强制前滚），或让您定义的保留策略在每夜前滚期间应用。

查看许可证信息

您可以查看机器上安装的 AppAssure 代理软件的当前许可证状态信息。

要查看许可证信息，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要查看的机器的超链接。
   - 在导航窗格中选择要查看的机器。
3. 单击 **Configuration**（配置）选项卡，然后单击 **Licensing**（许可）。

   此时将显示 **Status**（状态）屏幕，并提供关于产品许可的详细信息。

修改保护计划

在 AppAssure 中，可以修改机器上特定卷的保护计划。

要修改保护计划，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要修改的机器的超链接。
   - 在导航窗格中选择要修改的机器。
3. 请执行以下操作之一：
   - 在机器的 **Summary**（摘要）选项卡的 **Volumes**（卷）表中，单击要自定义的卷保护计划的超链接。
   - 单击 **Configuration**（配置）选项卡，然后单击 **Protection Settings**（保护设置）。在卷列表中，单击要自定义的卷旁的 **Edit**（编辑）图标。

   此时将显示 **Protection Schedule**（保护计划）对话框。
4. 在 **Protection Schedule**（保护计划）对话框中，根据需要编辑以下用于保护数据的计划选项。下表介绍了各选项。

选项	说明
Interval（间隔时间）	**Weekday**（工作日）— 要以指定的间隔时间保护数据（例如，每 15 分钟），请选择 **Interval**（间隔时间），然后： • 要自定义在高峰时期的某个时间保护数据，可以从下拉菜单中选择 **Start Time**（开始时间）、**End Time**（结束时间）和 **Interval**（间隔时间）。 • 要在非高峰时期保护数据，请选中 **Protection interval during off-peak times**（非高峰期期间的保护间隔时间）复选框，然后从下拉菜单中选择保护间隔时间。 **Weekends**（周末）- 要在周末也保护数据，请选中 **Protection interval during weekends**（周末期间的保护间隔时间）复选框，然后从下拉菜单中选择间隔时间。 **注:** 如果 SQL 或 Exchange 数据库和日志位于不同的卷上，则这些卷必须属于同一保护组。

选项	说明
Daily（每天）	要每天保护数据，请选择 **Daily**（每天）选项，然后在 **Protection Time**（保护时间）下拉菜单中，选择开始保护数据的时间。
No Protection（无保护）	要从此卷移除保护，请选择 **No Protection**（无保护）选项。

如果要将这些自定义设置应用到此机器上的所有卷，请选择 **Apply to All Volumes**（应用到所有卷）。

5. 完成所有必要更改后，单击 **OK**（确定）。

修改传输设置

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代理级设置。要影响 Core 级别的传输，请参阅修改传输队列设置。

小心: 更改传输设置可能会对您的环境产生重大影响。在修改传输设置值之前，请参阅 Dell AppAssure 知识库 (https://support.software.dell.com/appassure/kb) 中的 Transfer Performance Tuning Guide（传输性能调整指南）。

共有三种传输类型：

Snapshots（快照）	此传输可备份受保护机器上的数据。
VM Export（VM 导出）	这种传输将使用所有备份信息和参数（由为保护机器而定义的计划所指定）创建虚拟机。
Rollback（回滚）	此过程将在受保护的机器上还原备份信息。

数据传输涉及通过从代理机器到 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。在备份代理机器、执行 VM 导出或执行回滚的过程中，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最佳支持，并根据您的环境调整性能。

要修改传输设置，请执行以下操作：

1. 在 Core 控制台中，执行以下操作之一：
   - 单击 **Machines**（机器）选项卡，然后单击要修改的机器的超链接。
   - 在导航窗格中，单击要修改的机器。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要修改的机器的超链接。
   - 在导航窗格中选择要修改的机器。

3. 单击 **Configuration**（配置）选项卡，然后单击 **Transfer Settings**（传输设置）。
   此时将显示当前传输设置。
4. 在 **Transfer Settings**（传输设置）页面中，单击 **Change**（更改）。
   此时将显示 **Transfer Settings**（传输设置）对话框。
5. 根据下表中的说明输入机器的 **Transfer Settings**（传输设置）选项。

文本框	说明
Priority（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。
Maximum Concurrent Streams（最大并发数据流）	设置发送至 Core 并由每个代理并行处理的最大 TCP 链路数目。 **注:** Dell 建议将此值设为 8。如果发生数据包丢弃，则尝试增加此设置的值。
Maximum Concurrent Writes（最大并发写入）	设置每个代理连接的最大同时磁盘写操作数目。 **注:** Dell 建议将此值设为您为 Maximum Concurrent Streams（最大并发数据流）选择的值。如果发生数据包丢失，则将此值设为稍小的值。例如，如果 Maximum Concurrent Streams（最大并发数据流）设为 8，则将此选项设为 7。
Maximum Retries（最大重试次数）	设置某些操作未完成时，各受保护机器的最大重试次数。
Maximum Segment Size（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。 **小心: 请勿更改此选项的默认设置。**
Maximum Transfer Queue Depth（最大传输队列深度）	指定可以并行发送的命令数。如果您的系统执行大量并发输入/输出操作，可将此选项调整至较高的数字。
Outstanding Reads per Stream（每数据流的等待读取数）	指定将在后端存储多少个排队读取操作。此设置可帮助控制代理排队。 **注:** Dell 建议将此值设为 24。
Excluded Writers（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，因此可能不会看到所有编写器。您可能看到的一些编写器包括： • ASR Writer（ASR 编写器） • BITS Writer（BITS 编写器） • COM+ REGDB Writer（COM+ REGDB 编写器） • Performance Counters Writer（性能计数器编写器） • Registry Writer（注册表编写器） • Shadow Copy Optimization Writer（卷影副本优化编写器） • SQLServerWriter（SQL Server 编写器）

文本框	说明
	• System Writer（系统编写器） • Task Scheduler Writer（任务计划程序编写器） • VSS Metadata Store Writer（VSS 元数据存储编写器） • WMI Writer（WMI 编写器）
Transfer Data Server Port（传输数据服务器端口）	设置传输端口。默认设置为 8009。
Transfer Timeout（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）。
Snapshot Timeout（快照超时）	指定等待创建快照的最长时间（分钟数和秒数）。
Network Read Timeout（网络读取超时）	以分钟和秒数指定等待读取连接的最长时间。如果在该时间未执行网络读取，则会重复操作。
Network Write Timeout（网络写入超时）	以秒数指定等待写入连接的最长时间。如果在该时间未执行网络写入，则会重复操作。

6. 单击 **OK（确定）**。

重新启动服务

要重新启动服务，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要重新启动的机器的超链接。
   - 在 **Navigation**（导航）窗格中选择要重新启动的机器。
3. 选择 **Tools**（工具）选项卡，然后单击 **Diagnostics**（诊断）。
4. 选择 **Restart Service**（重新启动服务）选项，然后单击 **Restart Service**（重新启动服务）按钮。

查看机器日志

如果机器发生任何错误或问题，请查看日志以进行故障排除。
要查看机器日志，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击包含您要查看的日志的机器超链接。
   - 在 **Navigation**（导航）窗格中，选择包含您要查看的日志的机器。
3. 选择 **Tools**（工具）选项卡，然后单击 **Diagnostics**（诊断）。
4. 单击 **View Log**（查看日志）链接。

保护机器

本主题介绍如何开始保护指定机器上的数据。

注: 机器必须安装代理软件才能受到保护。可以选择在此步骤之前安装代理软件，也可以在定义保护时在 **Connection（连接）**对话框中将该软件部署到代理。有关在保护机器的过程中安装代理软件的具体步骤，请参阅在保护代理的同时部署代理软件。

添加保护时，必须指定要保护的机器的名称或 IP 地址以及该机器上要保护的卷，还要定义每个卷的保护计划。

要同时保护多个机器，请参阅保护多个机器。

要保护机器，请执行以下操作：

1. 如果在安装代理软件后未这样做，则应重新引导安装了代理软件的机器。
2. 在 Core 机器上的 Core 控制台中，执行以下操作之一：
   - 在 **Protected Machines**（受保护机器）下的 **Home**（主页）选项卡中，单击 **Protect Machine**（保护机器）。
   - 选择 **Machines**（机器）选项卡，然后在 **Actions**（操作）下拉菜单中单击 **Protect Machine**（保护机器）。

   此时将显示 **Connect**（连接）对话框。
3. 在 **Connect**（连接）对话框中，根据下表中的说明输入有关要连接的机器的信息。

文本框	说明
主机	要保护的机器的主机名或 IP 地址。
Port（端口）	Core 用来与机器上的代理进行通信的端口号。默认端口号为 8006。
用户名	用于连接此机器的用户名，例如 administrator。
密码	用于连接至此机器的密码。

4. 单击 **Connect**（连接）以连接到此机器。

   注: 如果尚未在您指定的机器上安装代理软件，请按照在保护代理的同时部署代理软件步骤操作。部署代理软件后重新启动代理机器，然后继续执行下一个步骤。
5. 在 **Protect**（保护）对话框中，按照下表中的说明根据需要编辑设置。

字段	说明
Display Name（显示名称）	您在 **Connect（连接）**对话框中指定的主机名或 IP 地址将显示在此文本字段中。或者，也可以输入机器的新名称，以显示在 Core 控制台中。 **注:** 以后也可以通过访问 **Configuration**（配置）选项卡来更改现有机器的显示名称。
Repository（存储库）	在 Core 上选择用以存储此机器中的数据的存储库。
Encryption Key（加密密钥）	指定是否对此机器上已存储在存储库中的每个卷的数据应用加密。

字段	说明
	注: 存储库的加密设置在 Core 控制台中的 **Configuration（配置）**选项卡下进行定义。
Initially Pause Protection（初始暂停保护）	添加要保护的机器后，AppAssure 会自动开始创建数据的基本快照。可以选中此复选框以便在初始时暂停保护。准备好开始保护数据后，必须手动强制创建快照。有关手动强制创建快照的更多信息，请参阅手动强制创建快照。
Volume Groups（卷组）	在 Volume Groups（卷组）下，可以定义要保护的卷，并建立保护计划。 要为机器上的所有卷设置间隔 60 分钟的默认保护计划，请单击 **Apply Default**（应用默认设置）。 也可以选择机器上的任意卷，然后单独定义其保护参数。 初始设置应用间隔 60 分钟的默认保护计划。要修改任意卷的计划，请单击该卷的 **Edit**（编辑）。然后，可以进一步定义快照间隔（包括为周末定义独立计划），或者指定每天开始创建快照的时间。 有关为所选卷编辑保护计划的更多信息，请参阅创建卷的自定义计划。

6. 单击 **Protect**（保护）。
   首次为机器添加保护时，立即开始将基本映像（即受保护卷中的所有数据的快照）传输至 Core 上的存储库，除非您指定初始暂停保护。

   小心: 如果保护的是 Linux 机器，则绝不能手动卸载受保护的卷。如果您需要执行此操作，则在卸载卷之前必须执行以下命令：bsctl -d [path_to_volume]。在此命令中，[path_to_volume] 不是引用卷的装载点，而是引用卷的文件描述符；它必须采用类似此例的格式：/dev/sda1。

在保护代理的同时部署代理软件

您可在添加代理进行保护的过程中下载和部署代理。

注: 如果您已经在要保护的机器上安装了代理软件，则不需要执行此过程。

要在添加代理进行保护的过程中部署代理，请执行以下操作：

1. 在 **Protect Machine**（保护机器）→ **Connect**（连接）对话框中，输入适当的连接设置后，单击 **Connect**（连接）。
   此时将显示 **Deploy Agent**（部署代理）对话框。
2. 单击 **Yes**（是）将代理软件远程部署到机器。
   此时将显示 **Deploy Agent**（部署代理）对话框。
3. 按照以下步骤输入登录和保护设置：
   - **Host name**（主机名）- 指定您要保护的机器的主机名或 IP 地址。
   - **Port**（端口）- 指定 Core 用来与机器上的代理进行通信的端口号。默认值为 8006。
   - **User name**（用户名）- 指定用来连接到此机器的用户名；例如 administrator。
   - **Password**（密码）- 指定用来连接到此机器的密码。

- **Display name**（显示名称）- 指定显示在 Core 控制台上的机器的名称。显示名称可以与主机名相同。
- **Protect machine after install**（安装后保护机器）- 选择此选项将允许 AppAssure 在您添加要保护的机器后创建数据的基本快照。此选项默认选中。如果取消选中此选项，则在您准备好开始数据保护后必须手动强制创建快照。有关手动强制创建快照的更多信息，请参阅 *Dell DL4300 Appliance User's Guide*（Dell DL4300 设备用户指南）中的"Forcing A Snapshot"（强制创建快照）主题。
- **Repository**（存储库）- 选择用于存储来自此代理的数据的存储库。

  注: 您可将来自多个代理的数据存储在单个存储库中。
- **Encryption Key**（加密密钥）- 指定是否应对要存储在存储库中的此机器上每个卷的数据进行加密。

  注: 您可在 Core 控制台的 **Configuration**（配置）选项卡下定义存储库的加密设置。

4. 单击 **Deploy**（部署）。

   此时将关闭 **Deploy Agent**（部署代理）对话框。在您看到所选代理出现在受保护机器的列表中之前，可能有延迟。

创建卷的自定义计划

要创建卷的自定义计划，请执行以下操作：

1. 在 **Protect Machine**（保护机器）对话框（有关访问此对话框的信息，请参阅保护机器）中的 **Volume Groups（卷组）**下，选择要保护的卷，然后单击 **Edit（编辑）**。

   此时将显示 **Protection Schedule**（保护计划）对话框。
2. 在 **Protection Schedule**（保护计划）对话框中，根据下面的说明选择以下计划选项之一来保护数据：

文本框	说明
Interval（间隔时间）	您可以选择： • **Weekday**（工作日）— 要以特定间隔时间保护数据，请选择 **Interval**（间隔时间），然后： – 要自定义在高峰时期的某个时间保护数据，可以从下拉菜单中指定 **Start Time**（开始时间）、**End Time**（结束时间）和 **Interval**（间隔时间）。 – 要在非高峰时期保护数据，请选择 **Protection interval during off-peak times**（非高峰期期间的保护间隔时间），然后从 **Time**（时间）下拉菜单中选择保护间隔时间。 • **Weekends**（周末）— 要在周末也保护数据，请选择 **Protection interval during weekends**（周末期间的保护间隔时间）复选框，然后从下拉菜单中选择**间隔时间**。
Daily（每天）	要每天保护数据，请选择 **Daily protection**（每天保护）选项，然后在 **Time**（时间）下拉菜单中，选择开始保护数据的时间。
No Protection（无保护）	要从此卷移除保护，请选择 **No Protection**（无保护）选项。

   如果要将这些自定义设置应用到此机器上的所有卷，请选择 **Apply to All Volumes**（应用到所有卷）。
3. 完成所有必要更改后，单击 **OK**（确定）。
4. 要自定义任何附加卷，请重复步骤 2 和步骤 3。
5. 在 **Protect Machine**（保护机器）对话框中，单击 **Protect**（保护）。

修改 Exchange Server 设置

如果要保护 Microsoft Exchange Server 上的数据，必须在 Core 控制台中配置附加设置。

要修改 Exchange Server 设置，请执行以下操作：

1. 添加要保护的 Exchange Server 机器后，在 Core 控制台的 **Navigation**（导航）窗格中选择机器。

   此时将显示该机器的 **Summary**（摘要）选项卡。
2. 在 **Summary**（摘要）选项卡中，单击 **Exchange Server Settings**（Exchange Server 设置）链接。

   此时将显示 **Exchange Server Settings**（Exchange Server 设置）对话框。
3. 在 **Exchange Server Settings**（Exchange Server 设置）对话框中，可以选中或清除以下设置：
   - Enable automatic mountability check（启用自动可装载性检查）。
   - Enable nightly checksum check（启用每夜校验和检查）。通过选择以下选项可以进一步自定义此设置：
     - Automatically truncate Exchange logs after successful checksum check（校验和检查成功后自动截断 Exchange 日志）
     - Truncate log before checksum check completes（校验和检查完成前截断日志）
4. 也可以修改 Exchange Server 的登录凭据。为此，请向下滚动至 **Exchange Server Information**（Exchange Server 信息）部分，然后单击 **Change Credentials**（更改凭据）。

   此时将显示 **Set Exchange Credentials**（设置 Exchange 凭据）对话框。
5. 输入新凭据，然后单击 **OK**（确定）。

修改 SQL Server 设置

如果要保护 Microsoft SQL Server 上的数据，还需要在 Core 控制台中配置附加设置。

要修改 SQL Server 设置，请执行以下操作：

1. 添加要保护的 SQL Server 机器后，在 Core 控制台的 **Navigation**（导航）窗格中选择机器。

   此时将显示该机器的 **Summary**（摘要）选项卡。
2. 在 **Summary**（摘要）选项卡中，单击 SQL Server settings（SQL Server 设置）链接。

   此时将显示 **SQL Server Settings**（SQL Server 设置）对话框。
3. 在 **SQL Server Settings**（SQL Server 设置）对话框中，根据需要编辑以下设置：
   - Enable nightly attachability check（启用每夜可附加性检查）
   - Truncate log after successful attachability check (simple recovery model only)（成功检查可附加性后截断日志（仅简单恢复模式））
4. 也可以修改 SQL Server 的登录凭据。为此，请向下滚动至 **SQL Server Information**（SQL Server 信息）表，然后单击 **Change Credentials**（更改凭据）。

   此时将显示 **Set SQL Server Credentials**（设置 SQL Server 凭据）对话框。
5. 输入新凭据，然后单击 **OK**（确定）。

部署代理（推送安装）

AppAssure 需要 microsoft.net 进行代理安装。必须在客户端机器上安装 Microsoft.net，然后才能通过手动或推送安装过程来安装代理。

AppAssure 允许将 AppAssure 代理安装程序部署至各个要保护的 Windows 机器。要将安装程序推送至代理，请完成以下过程中的步骤。要同时向多个机器部署代理，请参阅部署到多个机器。

注: 必须为代理配置可实现远程安装的安全策略。

要部署代理，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在 **Actions**（操作）下拉菜单中，单击 **Deploy Agent**（部署代理）。
   此时将显示 **Deploy Agent**（部署代理）对话框。
3. 在 **Deploy Agent**（部署代理）对话框中，根据下表中的说明输入登录设置。

文本框	说明
Machine（机器）	输入要部署的机器的主机名或 IP 地址。
用户名	输入用于连接此机器的用户名（例如，administrator）。
密码	输入用于连接此机器的密码。
Automatic reboot after install（安装之后自动重新引导）	选择此选项可指定 Core 是否在 AppAssure 代理安装程序部署和安装完成后启动。

4. 单击 **Verify**（验证）以验证输入的凭据。
   Deploy Agent（部署代理）对话框将显示一条消息，指示正在执行验证。
5. 如果要取消验证过程，请单击 **Abort**（中止）。
   完成验证过程后，即会显示一条消息，指示验证已完成。
6. 单击 **Deploy**（部署）。
   此时将显示一条指示部署已开始的消息。您可以在 **Events**（事件）选项卡中查看进度。
7. 单击 **Show details**（显示详细信息）可查看关于代理部署状态的更多信息。
8. 单击**确定**。

复制新代理

添加源 Core 上要保护的 AppAssure 代理时，AppAssure 将提供相应的选项，以便将此新代理复制到现有目标 Core。

要复制新代理，请执行以下操作：

1. 导航至 Core 控制台，然后单击 **Machines（机器）**选项卡。
2. 在 **Actions**（操作）下拉菜单中，单击 **Protect Machine**（保护机器）。
3. 在 **Protect Machine**（保护机器）对话框中，根据下表中的说明输入信息。

文本框	说明
Host（主机）	输入要保护的机器的主机名或 IP 地址。
Port（端口）	输入 AppAssure Core 用来与机器上的代理进行通信的端口号。
Username（用户名）	输入用于连接此机器的用户名。例如，Administrator。
Password（密码）	输入用于连接此机器的密码。

4. 单击 **Connect**（连接）以连接到此机器。

5. 单击 **Show Advanced Options**（显示高级选项），然后根据需要编辑以下设置。

文本框	说明
Display Name（显示名称）	输入要在 Core 控制台中显示的机器的名称。
Repository（存储库）	在 AppAssure Core 上选择在其中存储此机器的数据的存储库。
Encryption Key（加密密钥）	指定是否对此机器上已存储在存储库中的每个卷的数据应用加密。 **注:** 存储库的加密设置在 Core 控制台中的 **Configuration（配置）**选项卡下进行定义。
Remote Core（远程 Core）	指定要将代理复制到的目标 Core。
Remote Repository（远程存储库）	目标 Core 上所需存储库的名称，此存储库将用来存储此机器的复制数据。
Pause（暂停）	如果要暂停复制（例如，暂停直到 AppAssure 创建新代理的基本映像），请选中此复选框。
Schedule（计划）	选择以下选项之一： • Protect all volumes with default schedule（使用默认计划保护所有卷） • Protect specific volumes with custom schedule（使用自定义计划保护特定卷） **注:** 默认计划为每 15 分钟。
Initially Pause Protection（初始暂停保护）	如果要暂停保护（例如，防止 AppAssure 创建基本映像，直到使用高峰期过后），请选中此复选框。

6. 单击 **Protect**（保护）。

管理机器

本部分介绍在管理机器时可执行的各种任务，例如从 AppAssure 环境中移除机器、设置复制、强制日志截断、取消操作等。

移除机器

1. 导航至 Core 控制台，然后单击 **Machines（机器）**选项卡。
2. 在 **Machines**（机器）选项卡中，执行以下操作之一：
   - 单击要移除的机器的超链接。
   - 或者，在导航窗格中选择要移除的机器。
3. 在 **Actions**（操作）下拉菜单中，单击 **Remove Machines**（移除机器），然后选择下表中说明的选项之一。

选项	说明
Relationship Only（仅关系）	从复制中移除源 Core，但保留已复制恢复点。
With Recovery Points（包括恢复点）	从复制中移除源 Core，并且删除从该机器接收的所有已复制恢复点。

复制机器上的代理数据

复制是指同一站点中的目标 Core 与源 Core 之间的关系；或两个使用慢速链路的站点间基于代理的关系。在两个 Core 之间建立复制关系后，源 Core 会将所选代理的增量快照数据异步传输至目标 Core 或源 Core。可以将出站复制配置到提供非现场备份和灾难恢复服务的托管服务提供商或自管 Core。要复制机器上的代理数据，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 选择要复制的机器。
3. 在 **Actions**（操作）下拉菜单中，单击 **Replication**（复制），然后完成以下选项之一：
   - 如果要设置复制，请单击 **Enable**（启用）。
   - 如果当前已完成复制设置，请单击 **Copy**（复制）。

   此时将显示 **Enable Replications**（启用复制）对话框。
4. 在 **Host**（主机）文本框中，输入主机名。
5. 在 **Agents**（代理）下，选择具有要复制的代理和数据的机器。
6. 如果需要，请选中复选框 **Use a seed drive to perform initial transfer**（使用种子驱动器执行初始传输）。
7. 单击 **Add**（添加）。
8. 要暂停或恢复复制，请在 **Actions**（操作）下拉菜单中单击 **Replication**（复制），然后根据需要单击 **Pause**（暂停）或 **Resume**（恢复）。

设置代理的复制优先级

要设置代理的复制优先级，请执行以下操作：

1. 在 Core 控制台中，选择要为其设置复制优先级的受保护机器，然后单击 **Configuration（配置）**选项卡。
2. 单击 **Select Transfer Settings**（选择传输设置），然后使用 **Priority**（优先级）下拉列表选择以下选项之一：
   - **Default（默认值）**
   - **Highest（最高）**
   - **Lowest（最低）**
   - **1**
   - **2**
   - **3**
   - **4**

   注: 默认优先级为 5。如果将两个代理的优先级分别设为 1 和 Highest（最高），则优先级为 Highest（最高）的代理将先于优先级为 1 的代理进行复制。

3. 单击 **OK（确定）**。

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）。

要取消机器上的操作，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 选择要取消其操作的机器。
3. 在 **Actions**（操作）下拉菜单中，单击 **Cancel**（取消），然后根据下面的说明选择一个选项：

文本框	说明
All Operations（所有操作）	取消该机器的所有活动操作。
Snapshot（快照）	取消当前正在进行中的快照。

查看机器状态和其他详细信息

要查看机器状态和其他详细信息，请执行以下操作：

1. 在 Core 控制台的导航窗格中，执行以下操作之一：
   - 选择 **Machines**（机器）选项卡，然后单击要查看的机器的超链接。
   - 在导航窗格中，单击要查看的机器。

此时将显示 **Summary**（摘要）选项卡。

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：

- Host name（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）
- Mountability Check status（可装载性检查状态）
- Checksum Check status（校验和检查状态）
- 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：

- Total size（总大小）
- Used Space（已用空间）
- Free space（可用空间）

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：

- 名称
- Install Path（安装路径）
- 版本

- Version Number（版本号）
- Database Name（数据库名称）
- Online status（联机状态）

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：

- 名称
- Install Path（安装路径）
- Data Path（数据路径）
- Name Exchange Databases Path（名称 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）

管理多个机器

本主题介绍管理员需要执行哪些任务才能将代理软件同时部署到多个 Windows 机器。
要部署和保护多个代理，请执行以下任务：

1. 将 AppAssure 部署到多个机器。
   请参阅部署到多个机器。
2. 监测批量部署活动。
   请参阅监测多个机器的部署。
3. 保护多个机器。
   请参阅保护多个机器。

   注: 如果在部署过程中选中 Protect Machine After Install（安装后保护机器）选项，则可以跳过此步骤。
4. 监测批量保护活动。
   请参阅监测多个机器的保护。

部署到多个机器

可以通过使用 AppAssure 的 Bulk Deploy（批量部署）功能来简化向多个 Windows 机器部署 AppAssure 代理软件的任务。您可以批量部署到：

- VMware vCenter/ESXi 虚拟主机上的机器
- Active Directory 域上的机器
- 任何其他主机上的机器

批量部署功能自动检测主机上的机器，并允许您选择要部署到的机器。或者，也可以手动输入主机和机器信息。

注: 您要部署的机器必须可以访问 Internet 以下载和安装 BITS，因为 AppAssure 使用 Web 版本的 AppAssure 代理安装程序来部署安装组件。如果无法访问 Internet，则可以从 Core 机器推送 AppAssure 代理安装程序。有关从 Core 机器推送代理安装的信息，请参阅从 Core 机器推送代理安装程序。您可从许可证门户下载 Core 和代理更新。

从 Core 机器推送代理安装程序

如果要部署的服务器未接入 Internet，则可以从 Core 机器推送实际代理安装文件。您的设备包含代理安装程序文件。

注: 从许可证门户下载 Core 和代理升级。

要从 Core 机器推送代理安装程序，请执行以下操作：

1. 在 Core 机器中，将代理安装文件 **Agent-X64–5.x.x.xxxxx.exe** 复制到 **C:\Program Files\apprecovery \core\installers** 目录。
2. 在 Core 控制台中，选择 **Configuration**（配置）选项卡，然后单击 **Settings**（设置）。
3. 在 **Deploy Settings**（部署设置）部分中，编辑 **Agent Installer Name**（代理安装程序名称）。

部署到 Active Directory 域上的机器

开始此过程之前，必须获得 Active Directory 服务器的域信息和登录凭据。

要将代理部署到 Active Directory 域上的多个机器，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools**（工具）选项卡，然后单击 **Bulk Deploy**（批量部署）。
2. 在 **Deploy Agent to Machines**（在机器上部署代理）窗口中，单击 **Active Directory**。
3. 在 **Connect to Active Directory**（连接至 Active Directory）对话框中，根据下表中的说明输入域信息和登录凭据：

文本框	说明
域	Active Directory 域的主机名或 IP 地址。
User name（用户名）	用于连接域的用户名；例如 Administrator。
密码	用于连接域的安全密码。

4. 单击 **Connect**（连接）。
5. 在 **Add Machines from Active Directory**（从 Active Directory 添加机器）对话框中，选择要部署 AppAssure 代理的机器，然后单击 **Add**（添加）。

   您添加的机器显示在 **Deploy Agent on Machines**（在机器上部署代理）窗口中。
6. 要输入机器的密码，请选择一个存储库，添加加密密钥，或者编辑机器的其他设置，然后单击该机器的 **Edit**（编辑）链接，再执行以下操作。
   a. 在 **Edit Settings**（编辑设置）对话框中，根据下表中的说明指定设置：

文本框	说明
Host name（主机名）	从步骤 3 自动提供。
Display name（显示名称）	根据在步骤 3 中提供的主机名自动分配。
Port（端口）	Core 用来与机器上的代理进行通信的端口号。
User name（用户名）	从步骤 3 自动提供。
密码	输入机器的密码。

文本框	说明
Automatic reboot after install（安装之后自动重新引导）	指定在部署后是否要自动重新引导机器。 **注:** 如果要通过选中 **Protect Machine After Install**（安装后保护机器）复选框在部署后自动保护机器，则必须选中此选项。
Protect Machine After Install（安装后保护机器）	指定在部署后是否要自动保护机器。这允许您跳过**"保护多个机器"**。
Repository（存储库）	使用下拉列表在 Core 上选择要在其中存储机器数据的存储库。所选存储库将用于所有受保护机器。 **注:** 仅当选择 **Protect machine after install**（安装后保护机器）时，才可使用此选项。
Encryption Key（加密密钥）	（可选）使用下拉列表指定是否对应存储在存储库中的机器上的数据应用加密。加密密钥将分配给所有受保护机器。 **注:** 仅当选择 **Protect machine after install**（安装后保护机器）时，才可使用此选项。

b. 单击**保存**。

7. 要验证 AppAssure 能否成功连接到每个机器，请在 **Deploy Agent on Machines**（在机器上部署代理）窗口中选择每个机器，然后单击 **Verify**（验证）。
8. **Deploy Agent on Machines**（在机器上部署代理）窗口会在每个机器旁边显示一个图标，表示该机器是否做好部署准备，如下所示：

文本框	说明
绿色图标	AppAssure 能够连接到机器，并且已准备好进行部署。
黄色图标	AppAssure 能够连接到机器；但是，代理已经与另一个 Core 机器配对。
红色图标	AppAssure 无法连接到机器。这可能是因为登录凭据不正确、机器已关闭、防火墙正在阻止通信，或者存在其他问题。要纠正问题，请单击工具栏上的 **Edit Settings**（编辑设置）或者机器旁边的 **Edit**（编辑）链接。

9. 成功验证机器后，选中要部署 AppAssure 代理的每个机器，然后单击 **Deploy**（部署）。
10. 如果选择了 **Protect machine after install**（安装后保护机器）选项，则在成功部署后，将自动重启机器并启用保护。

部署到 VMware vCenter 或 ESXi 虚拟主机上的机器

开始此过程之前，必须获得 VMware vCenter/ESXi 虚拟主机的主机位置信息和登录凭据。

注: 所有虚拟机必须安装 VM Tools；否则，AppAssure 无法检测到要部署的虚拟机的主机名。AppAssure 将使用虚拟机名称代替主机名，如果主机名与虚拟机名称不同，则可能会导致问题。

要部署到 vCenter/ESXi 虚拟主机上的多个机器，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools**（工具）选项卡，然后单击 **Bulk Deploy**（批量部署）。
2. 在 **Deploy Agent on Machines**（在机器上部署代理）窗口中，单击 **vCenter/ESXi**。
3. 在 **Connect to VMware vCenter Server/ESXi**（连接至 VMware vCenter Server/ESXi）对话框中，请根据下表中的说明输入主机信息和登录凭据，然后单击 **OK**（确定）。

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。
用户名	输入用于连接此虚拟主机的用户名；例如 administrator。
密码	输入用于连接此虚拟主机的安全密码。

4. 在 **Add Machines from VMware vCenter Server/ESXi**（从 VMware vCenter Server/ESXi 添加机器）对话框中，选中要部署 AppAssure 代理的机器旁边的复选框，然后单击 **Add**（添加）。
5. 在 **Deploy Agent on Machines**（在机器上部署代理）窗口中，可以查看所添加的机器。如果要选择存储库、加密密钥或机器的其他设置，请选中机器旁边的复选框并单击 **Edit Settings**（编辑设置）。

   有关各项设置的详细信息，请参阅部署到 Active Directory 域上的机器。
6. 验证 AppAssure 能否成功连接到每个机器。请在 **Deploy Agent on Machines**（在机器上部署代理）窗口中选择每个机器，然后单击 **Verify**（验证）。
7. **Deploy Agent on Machines**（在机器上部署代理）窗口会在每个机器旁边显示一个图标，表示该机器是否做好部署准备，如下所示：

文本框	说明
绿色图标	AppAssure 能够连接到机器，并且已准备好进行部署。
黄色图标	AppAssure 能够连接到机器；但是，代理已经与另一个 Core 机器配对。
红色图标	AppAssure 无法连接到机器。这可能是因为登录凭据不正确、机器已关闭、防火墙正在阻止通信，或者存在其他问题。要解决问题，请单击工具栏上的 **Edit Settings**（编辑设置）或者机器旁边的 **Edit**（编辑）链接。

8. 机器验证成功后，选择每个机器，然后单击 **Deploy**（部署）。
9. 如果选择了 **Protect machine after install**（安装后保护机器）选项，则在成功部署后，将自动重新引导机器并启用保护。

部署到任何其他主机上的机器

要部署到任何其他主机上的多个机器，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools**（工具）选项卡，然后单击 **Bulk Deploy**（批量部署）。
2. 在 **Deploy Agent on Machines**（在机器上部署代理）窗口中，执行以下操作之一：
   - 单击 **New**（新增）以使用 **Add Machine**（添加机器）对话框指定多个机器；这允许您输入新机器主机、登录凭据、存储库、加密密钥和其他信息。有关各项设置的详细信息，请参阅部署到 Active Directory 域上的机器。

     输入此信息后，单击 **OK**（确定）将其添加到 **Deploy Agent on Machines**（在机器上部署代理）列表中，或者单击 **OK & New**（确定和新）以添加另一个机器。

     注: 如果要在部署后自动保护机器，请选中 **Protect Machine after Install**（安装后保护机器）复选框。如果选中该复选框，机器将在启用保护之前自动重启。
   - 单击 **Manually**（手动）以指定列表中的多个机器；每行代表要为其部署代理的一个机器。在 **Add Machines Manually**（手动添加机器）对话框中，按如下所示输入机器的 IP 地址或名称、用户名和密码（使用双冒号分隔符进行分隔）：

     ```
     hostname::username::password::port For example:
     10.255.255.255::administrator::&11@yYz90z::8006 abc-
     host-00-1::administrator::99!zU$o83r::168
     ```
3. 在 **Deploy Agent on Machines**（在机器上部署代理）窗口中，可以查看所添加的机器。如果要选择存储库、加密密钥或机器的其他设置，请选中机器旁边的复选框并单击 **Edit Settings**（编辑设置）。

   有关各项设置的详细信息，请参阅部署到 Active Directory 域上的机器。

4. 验证 AppAssure 能否成功连接到每个机器。请在 **Deploy Agent on Machines**（在机器上部署代理）窗口中选择每个机器，然后单击 **Verify**（验证）。

   Deploy Agent on Machines（在机器上部署代理）窗口会在每个机器旁边显示一个图标，表示该机器是否做好部署准备，如下所示：

文本框	说明
绿色图标	AppAssure 能够连接到机器，并且已准备好进行部署。
黄色图标	AppAssure 能够连接到机器；但是，代理已经与另一个 Core 机器配对。
红色图标	AppAssure 无法连接到机器。这可能是因为登录凭据不正确、机器已关闭、防火墙正在阻止通信，或者存在其他问题。要纠正问题，请单击工具栏上的 **Edit Settings**（编辑设置）或者机器旁边的 **Edit**（编辑）链接。

5. 成功验证机器后，选中每个机器旁边的复选框，然后单击 **Deploy**（部署）。
6. 如果选择了 **Protect machine after install**（安装后保护机器）选项，则在成功部署后，将自动重新引导机器并启用保护。

监测多个机器的部署

将 AppAssure 代理软件部署到机器时，可以查看部署进度。

要监测多个机器的部署：

1. 在 Core 控制台中，单击 **Events**（事件）选项卡，在列表中找到部署作业，然后单击 **Details**（详细信息）列中的按钮。

   Monitor Active Task（监测活动任务）窗口将显示部署的详细信息。

   其中包括总体进度信息以及各个部署的状态。显示的详细信息包括：

   - 开始时间
   - 结束时间
   - 所耗时间
   - 剩余时间
   - 进度
   - 阶段
2. 请执行以下操作之一：
   - 单击 **Open in New window**（在新窗口中打开），以打开新窗口查看部署进度。
   - 单击 **Close**（关闭），然后部署任务在后台进行处理。

保护多个机器

将代理软件批量部署到 Windows 机器后，现在必须对其进行保护以便保护数据。如果在部署代理时选择了 **Protect Machine After Install**（安装后保护机器），则可以跳过此步骤。

注: 必须为代理机器配置可实现远程安装的安全策略。

要保护多个机器，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools**（工具）选项卡，然后单击 **Bulk Protect**（批量保护）。

   此时将显示 **Protect Machines**（保护机器）窗口。
2. 通过单击以下选项之一来添加要保护的机器。

   有关完成每个选项的详细信息，请参阅部署到多个机器。

- 单击 **Active Directory** 可指定 Active Directory 域上的机器。
- 单击 **vCenter/ESXi** 可指定 vCenter/ESXi 虚拟主机上的虚拟机。
- 单击 **New**（新）可使用 Add Machine（添加机器）对话框指定多个机器。
- 单击 **Manually**（手动）可通过键入主机名和凭据来指定列表中的多个机器。

3. 在 **Protect Machines**（保护机器）窗口中，可以查看所添加的机器。如果要选择存储库、加密密钥或机器的其他高级设置，请选中机器旁边的复选框并单击 **Edit Settings**（编辑设置）。
4. 按如下所示指定设置并单击 **OK**（确定）。

文本框	说明
用户名	输入用于连接此机器的用户名；例如，Administrator。
密码	输入用于连接此机器的安全密码。
Port（端口）	指定 Core 用来与机器上的代理进行通信的端口号。
Repository（存储库）	在 Core 上选择要在其中存储机器数据的存储库。所选存储库将用于所有受保护机器。
Encryption Key（加密密钥）	指定是否对存储在存储库中的机器上的代理应用加密。加密密钥将分配给所有要进行保护的机器。
Protection Schedule（保护计划）	指定进行机器保护的计划。默认计划为高峰运行期内 60 分钟，周末 60 分钟。 要编辑计划以满足企业需求，请单击 **Edit**（编辑）。 **注:** 有关更多信息，请参阅修改保护计划。
Initially Pause Protection（初始暂停保护）	也可以选择在首次运行时暂停保护；也就是说，在手动恢复保护之前，Core 不会创建机器的快照。

5. 验证 AppAssure 能否成功连接到每个机器。为此，请在 **Protect Machines**（保护机器）窗口中选中每个机器旁边的复选框，然后单击 **Verify**（验证）。
6. **Protect Machines**（保护机器）窗口会在每个机器旁边显示一个图标，表示该机器是否做好部署准备，如下所示：

Icon	说明
绿色图标	AppAssure 能够连接到机器，并且该机器已准备好接受保护。
黄色图标	AppAssure 能够连接到机器；但是，代理已经与另一个 Core 机器配对。
红色图标	AppAssure 无法连接到机器。这可能是因为登录凭据不正确、机器已关闭、防火墙正在阻止通信，或者存在其他问题。要纠正问题，请单击工具栏上的 **Edit Settings**（编辑设置）或者机器旁边的 **Edit**（编辑）链接。

7. 成功验证机器后，选中每个机器旁边的复选框，然后单击 **Protect**（保护）。

监测多个机器的保护

AppAssure 将保护策略和计划应用至机器时，可以对进度进行监测。

要监测针对多台机器的保护，请执行以下操作：

1. 单击 **Machines**（机器）选项卡，以查看保护的状态和进度。

此时将显示 **Protected Machines**（受保护机器）页面。

2. 单击 **Events**（事件）选项卡，以查看相关任务、事件和警报。

   此时会显示 **Tasks**（任务）页面。

文本框	说明
查看任务信息	传输卷时，状态、开始时间和结束时间将显示在 **Tasks**（任务）窗格中。单击 **Details**（详细信息）可查看关于任务的更多具体信息。
查看警报信息	当添加各个受保护机器时，系统将记录一个警报，以详细说明操作是否成功或是否已记录错误。警报级别将与事务日期和消息一起显示。如果要从页面中移除所有警报，请单击 **Dismiss All**（全部消除）。
查看事件信息	关于机器和所传输数据的详情显示在 **Events**（事件）窗格中。其中将显示事件级别、事务日期和时间消息。

管理快照和恢复点

恢复点是从个别磁盘卷创建的快照集合，并存储在存储库中。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 AppAssure 中，可以强制创建快照、临时暂停快照、查看存储库中当前恢复点的列表，以及根据需要删除它们。恢复点用于还原受保护机器，或者装载到本地文件系统。

AppAssure 在数据块级别捕获快照，并且具备应用程序感知功能。这表示在创建快照前，所有未结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。

AppAssure 使用低级别卷筛选驱动程序，后者先附加到已装载的卷上，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。

查看恢复点

要查看恢复点，请执行以下操作：

1. 在 Core 控制台的左侧导航区域中，选择要查看恢复点的机器，然后单击 **Recovery Points（恢复点）**选项卡。

可以查看关于机器上恢复点的信息，如下表中所述：

信息	说明
状态	表明恢复点的当前状态。
已加密	表明恢复点是否已加密。
目录	列出恢复点中包含的卷。
类型	将恢复点定义为基本恢复点或差异恢复点。
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。

查看特定恢复点

要查看特定恢复点，请执行以下操作：

1. 在 Core 控制台的左侧导航区域中，选择要查看恢复点的机器，然后选择 **Recovery Points**（恢复点）选项卡。

2. 单击列表中恢复点旁的 **>** 以展开视图。
   可以查看关于所选机器的恢复点内容的更详细信息，以及根据下表中的说明访问可在恢复点上执行的各种操作：

信息	说明
操作	**Actions（操作）**菜单包含可在所选恢复点上执行的下列操作： **Mount**（装载）- 选择此选项可装载所选恢复点。有关装载所选恢复点的更多信息，请参阅装载 Windows 机器的恢复点。 **Export**（导出）— 使用 Export（导出）选项，您可以将所选恢复点导出到 ESXi、VMware Workstation 或 HyperV。有关导出所选恢复点的更多信息，请参阅将 Windows 机器的备份信息导出到虚拟机。 **Rollback**（回滚）— 选择此选项从所选恢复点执行到所指定卷的还原。有关从所选恢复点执行还原的更多信息，请参阅从 AppAssure Core 启动恢复。

3. 单击所选恢复点中的卷旁的 **>** 以展开视图。

可根据下表中的说明，查看展开的恢复点中选定卷的相关信息：

文本框	说明
标题	指示恢复点中的特定卷。
Raw Capacity（原始容量）	指示整个卷上的原始存储空间容量。
Formatted Capacity（格式化容量）	指示在格式化卷后，卷上可用于存储数据的存储空间容量。
Used Capacity（已用容量）	指示卷上当前已用的存储空间容量。

安装 Windows 机器的恢复点

在 AppAssure 中，可以装载 Windows 机器的恢复点以通过本地文件系统访问已存储的数据。
要装载 Windows 机器的恢复点，请执行以下操作：

1. 在 Core 控制台中，执行以下操作之一：
   - 选择 **Machines**（机器）选项卡。

   a. 在包含您要装载的恢复点的机器或群集旁边，从 **Actions**（操作）下拉菜单中选择 **Mount**（装载）。
   b. 从 **Mount Recovery Point**（装载恢复点）对话框的列表中选择恢复点，然后单击 **Next**（下一步）。
   此时将显示 **Mount Recovery Points**（装载恢复点）对话框。

   - 在 Core 控制台中，选择要装载到本地文件系统的机器。

     此时将显示所选机器的 **Summary**（摘要）选项卡。

   a. 选择 **Recovery Points**（恢复点）选项卡。
   b. 在恢复点列表中，展开要装载的恢复点。

c. 在该恢复点的展开详细信息中，单击 **Mount**（装载）。
此时将显示 **Mount Recovery Points**（装载恢复点）对话框。

2. 在 **Mount**（装载）对话框中，根据下表中的说明编辑用于装载恢复点的文本框：

文本框	说明
Mount Location: Local Folder（装载位置：本地文件夹）	指定用于访问已装载恢复点的路径。
Volume Images（卷映像）	指定要装载的卷映像。
Mount Type（装载类型）	指定访问已装载恢复点数据的方式： • Mount Read-only（装载只读）。 • Mount Read-only with previous writes（使用之前的写入装载只读）。 • Mount Writable（装载可写）。
Create a Windows share for this Mount（创建此装载的 Windows 共享）	（可选）选中此复选框以指定是否可共享已装载的恢复点，然后设置对恢复点的访问权限，包括共享名和访问组。

3. 单击 **Mount**（装载）以装载恢复点。

卸载所选恢复点

可以卸载在 Core 本地装载的选定恢复点。
要卸载所选恢复点，请执行以下操作：

1. 在 Core 控制台中，选择 **Tools**（工具）选项卡。
2. 从 **Tools**（工具）选项中，单击 **System Info**（系统信息）。
3. 找到并选择要卸载的恢复点的装载显示，然后单击 **Dismount**（卸载）。

卸载所有恢复点

可以卸载在 Core 本地装载的所有恢复点。
要卸载所有恢复点，请执行以下操作：

1. 在 Core 控制台中，选择 **Tools**（工具）选项卡。
2. 从 **Tools**（工具）选项中，单击 **System Info**（系统信息）。
3. 在 **Local Mounts**（本地安装）部分，单击 **Dismount All**（全部卸载）。

在 Linux 机器上安装恢复点卷

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 AppAssure **aamount** 公用程序，例如：

```
sudo aamount
```

4. 在 AppAssure 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 AppAssure 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。

   此时将显示一个列表，其中显示此 AppAssure 服务器所保护的机器。它按行项目号、主机/IP 地址和机器的 ID 号列出所找到的机器（例如：`293cc667-44b4-48ab-91d8-44bc74252a4f`）。
7. 输入以下命令以列出当前为指定机器安装的恢复点：

   ```
   lr <line_number_of_machine>
   ```

   注: 也可以在此命令中输入机器 ID 号，而不是行项目号。

   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。此列表包含行项目号、日期/时间戳、卷的位置、恢复点的大小，以及卷的 ID 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`）。
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> <path>
   ```

   注: 也可以在命令中指定行号来表示恢复点，而不是指定恢复点 ID 号。在这种情况下，使用代理/机器行号（来自 lm 输出），后跟恢复点行号和卷号，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代理机器，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`。

   小心: 您绝不能手动卸载受保护的 Linux 卷。如果您需要执行此操作，则在卸载卷之前必须执行以下命令：`bsctl -d <path to volume>`。在此命令中，`<path to volume>` 不是卷的安装点，而是卷的文件描述符；它必须采用类似此例的格式：/dev/sda1。

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 AppAssure 中删除恢复点时，可以指定以下选项之一：

文本框	说明
Delete All Recovery Points（删除所有恢复点）	从存储库移除所选代理机器的所有恢复点。
Delete a Range of Recovery Points（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。

注: 不能恢复已删除的恢复点。

要移除恢复点，请执行以下操作：

1. 在 Core 控制台的左侧导航区域中，选择要查看恢复点的机器，然后单击 **Recovery Points（恢复点）**选项卡。
2. 单击 **Actions**（操作）菜单。
3. 选择以下选项之一：
   - 要删除所有当前存储的恢复点，请单击 **Delete All**（全部删除）。

- 要删除指定数据范围内的一组恢复点，请单击 **Delete Range**（删除范围）。此时将显示 **Delete**（删除）对话框。在 **Delete Range**（删除范围）对话框中，使用开始日期和时间以及结束日期和时间指定要删除的恢复点范围，然后单击 **Delete**（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。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的基本映像。

注: 对于目标 Core 上的复制恢复点，无法删除孤立恢复链。

要删除孤立恢复点链，请执行以下操作：

1. 在 Core 控制台中，选择您要删除其孤立恢复点链的受保护机器。
2. 单击 **Recovery Points**（恢复点）选项卡。
3. 在 **Recovery Points**（恢复点）下，展开孤立恢复点。

   此恢复点在 **Type**（类型）列中标记为 **Incremental Orphaned**（增量孤立）。
4. 单击 **Actions**（操作）旁的 **Delete**（删除）。

   此时将显示 **Delete Recovery Points**（删除恢复点）窗口。
5. 在 **Delete Recovery Points**（删除恢复点）窗口中，单击 **Yes**（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。

   孤立恢复点链已删除。

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，传输会立即开始，或被添加到队列中。只传输自上个恢复点以来发生更改的数据。如果以前没有恢复点，则传输受保护卷上的所有数据，称为基本映像。

要强制创建快照，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后在受保护机器的列表中，选择具有要强制创建快照的恢复点的机器或群集。
2. 单击该机器的 **Actions**（操作）下拉菜单，再单击 **Force Snapshot**（强制创建快照），然后根据下面的说明选择一个选项：
   - **Force Snapshot**（强制创建快照）- 对自上次创建快照起更新的数据创建增量快照。
   - **Force Base Image**（强制创建基本映像）- 对机器上的卷的所有数据创建完整快照。
3. 当 **Transfer Status**（传输状态）对话框中显示通知，说明快照已进入队列时，单击 **OK**（确定）。

   在 **Machines（机器）**选项卡中的机器旁将出现一个进度条，用于显示快照的进度。

暂停和恢复保护

暂停保护时，将暂时停止当前机器的所有数据传输。

要暂停和恢复保护，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 选择要暂停保护的机器。

   此时将显示该机器的 **Summary**（摘要）选项卡。

3. 在该机器的 **Actions**（操作）下拉菜单中，单击 **Pause**（暂停）。
4. 要恢复保护，请在 **Actions**（操作）菜单中单击 **Resume**（恢复）。

还原数据

您可立即将 Windows 机器已存储恢复点中的数据恢复或还原至物理机（针对 Windows 或 Linux 机器）或虚拟机。本部分的主题介绍如何将 Windows 机器的特定恢复点导出到虚拟机或将机器回滚到以前的恢复点。

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。有关详情，请参阅复制机器上的代理数据 。

注: 从 FAT32 EFI 分区引导的 Windows 8 和 Windows Server 2012 操作系统不可用于保护或恢复，弹性文件系统 (ReFS) 卷也是如此。

备份

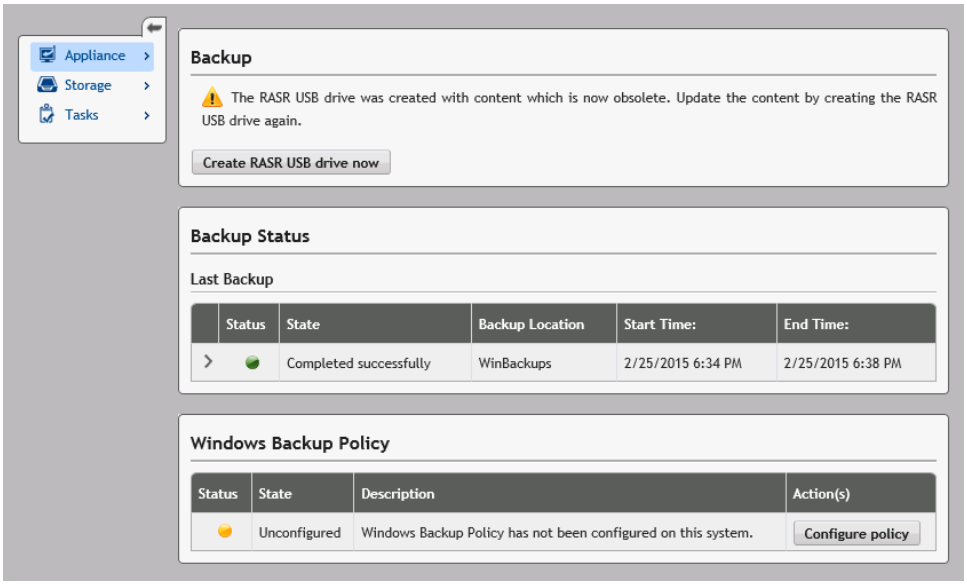
备份选项卡可让您配置备份策略并通过 RASR USB 闪存盘或 IDSDM 还原系统。要使用此功能，则应存在 Windows 备份虚拟磁盘。在执行 **AppAssure Appliance Configuration Wizard**（AppAssure 设备配置向导）期间会创建 Windows 备份虚拟磁盘。有关更多信息，请参阅 *Dell DL43000 Appliance Deployment Guide*（Dell DL43000 设备部署向导）中的“快速设备自行恢复”。如果没有 Windows 备份虚拟磁盘，将无法配置策略或创建 Windows 备份。

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

   注: 上述信息显示是否在运行 Windows 备份策略。



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(C:) • 恢复 • 裸机恢复 • System State（系统状态） 默认会选中上述所有项目。
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）。
   一旦完成配置，您可使用 **Windows Backup Policy**（Windows 备份策略）窗口中的选项 **Backup now**（立即备份）、**Delete policy**（删除策略）或 **View policy**（查看策略）。

关于将 Windows 机器中的受保护数据导出到虚拟机

AppAssure 支持将 Windows 备份信息一次性导出或连续导出（以支持虚拟待机）到虚拟机。将数据导出到待机虚拟机可为您提供数据的高可用性副本。如果受保护机器宕机，则可以启动虚拟机以执行恢复。

下图显示将数据导出到虚拟机的典型部署。

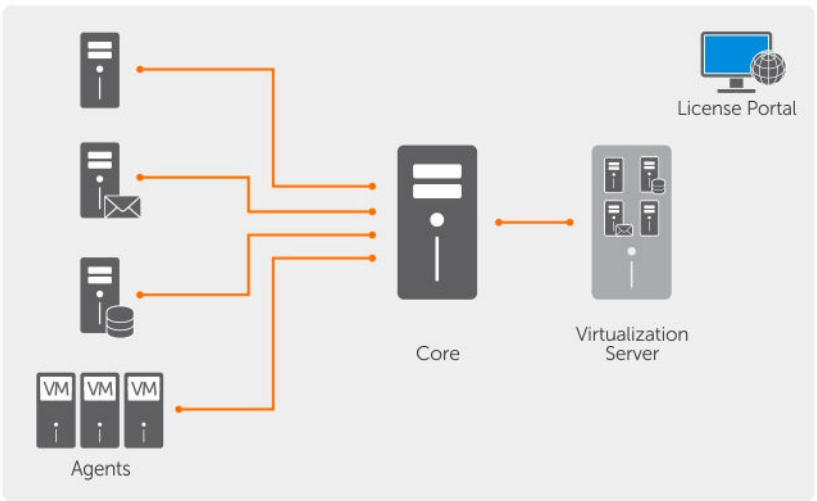


图 9: 将数据导出到虚拟机

通过将 Windows 机器中的受保护数据持续导出到虚拟机来创建虚拟待机。导出到虚拟机时，将导出恢复点中的所有备份数据，以及为您的机器的保护计划定义的参数。

您可执行将受保护 Windows 或 Linux 机器的恢复点虚拟导出到 VMware、ESXi、Hyper-V 和 Oracle VirtualBox。

注: Appliance（设备）选项卡显示所有虚拟机，但是只支持管理 Hyper-V 和 ESXi 虚拟机。要管理其他虚拟机，需要使用虚拟机监控程序管理工具。

注: 导出到的虚拟机必须运行经过许可的 ESXi、VMware Workstation 或 Hyper-V 版本，而不能是试用版或免费版。

动态和基本卷支持限制

AppAssure 支持创建所有动态卷和基本卷的快照。AppAssure 还支持导出位于单个物理磁盘上的简单动态卷。顾名思义，简单动态卷不是条带卷、镜像卷或跨越卷。非简单动态卷具有无法全面解读的随机磁盘几何结构，因此无法将其导出。AppAssure 能够导出复杂或非简单动态卷。

AppAssure 版本 5.3.1.60393 在用户界面中添加了一个复选框，提示您仅限导出简单动态卷。在随此版本更改用户界面之前，界面中显示了导出复杂或非简单动态磁盘的选项。但如果您尝试导出这些磁盘，则导出作业会失败。

将 Microsoft Windows 机器的备份信息导出到虚拟机

在 AppAssure 中，通过导出恢复点的所有备份信息以及为机器的保护计划所定义的参数，可以将 Microsoft Windows 机器的数据导出至虚拟机（VMware、ESXi、Hyper-V 和 Oracle VirtualBox）。

要将 Windows 备份信息导出至虚拟机，请执行以下操作：

1. 在 Core 控制台中，单击 **Machines**（机器）选项卡。
2. 在受保护机器列表中，选择具有要导出的恢复点的机器或群集。
3. 在该机器的 **Actions**（操作）下拉菜单中，单击 **Export**（导出），然后选择要执行的导出类型。可以从以下选项中选择：
   - ESXi Export（ESXi 导出）
   - VMware Workstation Export（VMware Workstation 导出）
   - Hyper-V Export（Hyper-V 导出）
   - Oracle VirtualBox Export（Oracle VirtualBox 导出）

   此时将显示 **Select Export Type**（选择导出类型）对话框。

使用 ESXi Export（ESXi 导出）导出 Windows 数据

在 AppAssure 中可以选择使用 ESXi Export（ESXi 导出）通过执行一次性或连续导出来导出数据。

执行 ESXi 一次性导出

要执行 ESXi 一次性导出，请执行以下操作：

1. 在 **Select Export Type**（选择导出类型）对话框中，单击 **One-time export**（一次性导出）。
2. 单击 **Next**（下一步）。
   此时将显示 **ESXi Export - Select Recovery Point**（ESXi 导出 - 选择恢复点）对话框。
3. 选择要导出的恢复点，然后单击 **Next**（下一步）。
   此时将显示 **Virtual Standby Recovery Point to VMware vCenter Server/ESXi**（虚拟待机恢复点到 VMware vCenter Server/ESXi）对话框。

定义虚拟机信息以执行 ESXi 导出

要定义虚拟机信息以执行 ESXi 导出，请执行以下操作：

1. 在 **Virtual Standby Recovery Point to VMware vCenter Server/ESXi**（虚拟待机恢复点到 VMware vCenter Server/ESXi）对话框中，根据下面的说明输入用于访问虚拟机的参数：

文本框	说明
主机名	输入主机名。
端口	输入主机端口。默认端口为 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。

2. 单击 **Connect**（连接）。

执行 ESXi 连续（虚拟待机）导出

要执行 ESXi 连续（虚拟待机）导出，请执行以下操作：

1. 在 **Select Export Type**（选择导出类型）对话框中，单击 **Continuous (Virtual Standby)**（连续（虚拟待机））。
2. 单击 **Next**（下一步）。

此时将显示 **Virtual Standby Recovery Point to VMware vCenter Server/ESXi**（虚拟待机恢复点到 VMware vCenter Server/ESXi）对话框。

3. 根据下表中的说明，输入用于访问虚拟机的参数。

文本框	说明
主机名	输入主机名。
端口	输入主机端口。默认端口为 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。

4. 单击 Connect（连接）。
5. 在 **Options**（选项）选项卡中，根据下表中的说明输入虚拟机信息。

文本框	说明
Virtual Machine Name（虚拟机名称）	输入即将创建的虚拟机的名称。例如 VM-0A1B2C3D4 **注:** 建议使用源自代理名称或与代理名称匹配的名称。您也可以创建源自虚拟机监控程序类型、IP 地址或 DNS 名称的名称。
Memory（内存）	指定内存使用量。可以从以下选项中选择： • 使用与源机器相同容量的 RAM • 单击 **Use a specific amount of RAM**（使用指定容量的 RAM），指定要使用多少 RAM。例如 4096 MB。允许的最小容量为 512 MB，最大容量则取决于主机的容量和限制。（推荐）
ESXi Datacenter（ESXi 数据中心）	输入 ESXi 数据中心的名称。
ESXi Host（ESXi 主机）	输入 ESXi 主机的凭据。
Data Store（数据存储）	输入数据存储的详细信息。
Version（版本）	选择虚拟机的版本。 **注:** 要使用 vSphere 客户端来管理虚拟机，请选择版本 8 或更低版本。
Resource Pool（资源池）	输入资源池名称。

6. 单击 **Start Export**（开始导出）。

使用 VMware Workstation Export（VMware Workstation 导出）导出 Windows 数据

在 AppAssure 中，可以选择使用 VMware Workstation Export（VMware Workstation 导出）通过执行一次性或连续导出来导出数据。要使用 VMware Workstation Export（VMware Workstation 导出）进行相应类型的导出，请完成以下过程中的步骤。

执行 VMware Workstation 一次性导出

要执行 VMware Workstation 一次性导出，请执行以下操作：

1. 在 **Select Export Type**（选择导出类型）对话框中，单击 **One-time export**（一次性导出）。
2. 单击 **Next（下一步）**。
   此时将显示 **VM Export - Select Recovery Point**（VM 导出 - 选择恢复点）对话框。
3. 选择要导出的恢复点，然后单击 **Next**（下一步）。
   此时将显示 **Virtual Standby Recovery Point to VMware Workstation/Server**（虚拟待机恢复点到 VMware Workstation/Server）对话框。

定义一次性导出设置以执行 VMware Workstation 导出

要定义一次性导出设置以执行 VMware Workstation 导出，请执行以下操作：

1. 在 **Virtual Standby Recovery Point to VMware Workstation/Server**（虚拟待机恢复点到 VMware Workstation/Server）对话框中，根据下面的说明输入用于访问虚拟机的参数：

文本框	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	输入用于登录虚拟机的凭据。 • 如果指定了网络共享路径，则必须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	输入用于登录虚拟机的凭据。 • 如果指定了网络共享路径，则必须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。

2. 在 **Export Volumes**（导出卷）窗格中，选择要导出的卷。例如 **C:** 和 **D:**。
3. 在 Options（选项）窗格中，按照下面的说明输入虚拟机和内存使用量的信息：

文本框	说明
虚拟机	输入即将创建的虚拟机的名称。例如 VM-0A1B2C3D4。 **注:** 建议使用源自代理名称或与代理名称匹配的名称。您也可以创建源自虚拟机监控程序类型、IP 地址或 DNS 名称的名称。
内存	指定虚拟机的内存。 • 单击 **Use the same amount of RAM as the source machine**（使用与源机器相同容量的 RAM），以指定 RAM 配置与源机器相同。 • 单击 **Use a specific amount of RAM**（使用指定容量的 RAM），指定要使用多少 RAM。例如 4096 MB。允许的最小容量为 512 MB，最大容量则取决于主机的容量和限制。（推荐）

4. 单击 **Export**（导出）。

执行 VMware Workstation 连续（虚拟待机）导出

要执行 VMware Workstation 连续（虚拟待机）导出，请执行以下操作：

1. 在 **Select Export Type**（选择导出类型）对话框中，单击 **Continuous (Virtual Standby)**（连续（虚拟待机）），然后单击 **Next**（下一步）。

   此时将显示 **VM Export - Select Recovery Point**（VM 导出 - 选择恢复点）对话框。
2. 选择要导出的恢复点，然后单击 **Next**（下一步）。

   此时将显示 **Virtual Standby Recovery Point to VMware Workstation/Server**（虚拟待机恢复点到 VMware Workstation/Server）对话框。
3. 根据下面的说明，输入用于访问虚拟机的参数：

文本框	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	输入用于登录虚拟机的凭据。 • 如果指定了网络共享路径，则必须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	输入用于登录虚拟机的凭据。 • 如果指定了网络共享路径，则必须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。

4. 在 **Export Volumes**（导出卷）窗格中，选择要导出的卷。例如 **C:** 和 **D:**。
5. 在 **Options**（选项）窗格中，按照下表中的说明输入虚拟机和内存使用量的信息。

文本框	说明
虚拟机	输入即将创建的虚拟机的名称。例如 `VM-0A1B2C3D4`。 **注:** 建议使用源自代理名称或与代理名称匹配的名称。您也可以创建源自虚拟机监控程序类型、IP 地址或 DNS 名称的名称。
内存	指定虚拟机的内存。 • 单击 **Use the same amount of RAM as the source machine**（使用与源机器相同容量的 RAM），以指定 RAM 配置与源机器相同。 • 单击 **Use a specific amount of RAM**（使用指定容量的 RAM），指定要使用多少 RAM；例如 4096 MB。允许的最小容量为 512 MB，最大容量则取决于主机的容量和限制。（推荐）

6. 单击 **Perform initial ad-hoc export**（执行初始临时导出）以测试数据的导出。
7. 单击 **Save**（保存）。

使用 Hyper-V Export（ESXi 导出）导出 Windows 数据

您可以选择使用 Hyper-V Export（Hyper-V 导出）通过执行一次性或连续导出来导出数据。要使用 Hyper-V Export（Hyper-V 导出）进行相应类型的导出，请完成以下过程中的步骤。
DL 设备支持将第一代 Hyper-V 导出到下列主机：

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

DL 设备支持将第二代 Hyper-V 导出到下列主机：

- Windows 8.1
- Windows Server 2012 R2

注: 并非所有受保护机器都可以导出到 Hyper-V 第二代主机。

只有使用下列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 Hyper-V 第二代主机：

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012R2 (UEFI)

注: 如果没有为 Hyper-V 主机分配足够的内存以执行导出操作，Hyper-V 导出到第二代虚拟机 (VM) 可能失败。

请完成以下针对相应类型的导出过程中的步骤。

执行 Hyper-V 一次性导出

要执行 Hyper-V 一次性导出，请执行以下操作：

1. 在 Core 控制台中，导航至要导出的机器。
2. 在 Summary（摘要）选项卡中，单击 **Actions（操作）** → **Export（导出）** → **One-time（一次性）**。
   在 **Protected Machines（受保护机器）**页面上会显示 **Export Wizard（导出向导）**。
3. 选择要导出的机器，然后单击 **Next（下一步）**。
4. 在 **Recovery Points（恢复点）**页面中，选择要导出的恢复点，然后单击 **Next（下一步）**。

定义一次性导出设置以执行 Hyper-V 导出

要定义一次性导出设置以执行 Hyper-V 导出，请执行以下操作：

1. 在 Hyper-V 对话框中，单击 **Use local machine**（使用本地机器），向分配了 Hyper-V 角色的本地机器执行 Hyper-V 导出。
2. 单击 **Remote host**（远程主机）选项，以便表明 Hyper-V 服务器位于远程机器上。如果选择 Remote host（远程主机）选项，请根据下表中的说明输入远程主机的参数：

文本框	说明
Host Name（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。
Port（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。
User Name（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。
Password（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。

3. 单击**下一步**。
4. 在 **Virtual Machines Options（虚拟机选项）**页面上的 **VM Machine Location（虚拟机位置）**文本框中，输入虚拟机的路径或位置。例如 **D:\export**。VM 的位置必须有足够的空间来容纳虚拟机所需的 VM 元数据以及虚拟驱动器。
5. 在 **Virtual Machine Name（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。
6. 单击以下选项之一：
   - **Use the same amount of RAM as the source machine（使用与源机器相同容量的 RAM）**，以指定虚拟机与源机器使用的 RAM 容量相同。
   - **Use a specific amount of RAM（使用指定容量的 RAM）**，以指定在导出后虚拟机拥有多少内存；例如 4096 MB。（推荐）
7. 要指定磁盘格式，请在 **Disk Format（磁盘格式）**旁单击以下选项之一：
   - **VHDX**
   - **VHD**

   注: 如果目标机器正在运行 Windows 8 (Windows Server 2012) 或更高版本，则 Hyper-V 导出支持 VHDX 磁盘格式。如果您的环境不支持 VHDX，则该选项被禁用。
8. 在 **Volumes（卷）**页面上，选择要导出的卷。对于作为受保护机器的有效备份的虚拟机，将包括受保护机器的引导驱动器。例如，C:\。

   对于 VHD，选择的卷不能大于 2040 GB。如果选择的卷大于 2040 GB 并且选择了 VHD 格式，将收到错误提示。
9. 在 **Summary（摘要）**页面中，单击 **Finish（完成）**以完成向导并开始导出。

执行 Hyper-V 连续（虚拟待机）导出

注: 只有包含 2 个虚拟机的 3 TB DL1000 配置支持一次性导出和连续导出（虚拟待机）功能。

要执行 Hyper-V 连续（虚拟待机）导出，请执行以下操作：

1. 在 Core 控制台中的 **Virtual Standby**（虚拟待机）选项卡上，单击 **Add**（添加）以启动 **Export Wizard**（导出向导）。在 **Export Wizard**（导出向导）的 **Protected Machines**（受保护机器）页面中，
2. 选择要导出的机器，然后单击 **Next**（下一步）。
3. 在 **Summary**（摘要）选项卡中，单击 **Export（导出）→ Virtual Standby**（虚拟待机）。
4. 在 Hyper-V 对话框中，单击 **Use local machine**（使用本地机器），向分配了 Hyper-V 角色的本地机器执行 Hyper-V 导出。
5. 单击 **Remote host**（远程主机）选项，以便表明 Hyper-V 服务器位于远程机器上。如果选择 Remote host（远程主机）选项，请根据下表中的说明输入远程主机的参数：

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。

6. 在 **Virtual Machines Options**（虚拟机选项）页面上的 **VM Machine Location**（虚拟机位置）文本框中，输入虚拟机的路径或位置。例如 D:\export。VM 的位置必须有足够的空间来容纳虚拟机所需的 VM 元数据以及虚拟驱动器。
7. 在 **Virtual Machine Name**（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。
8. 单击以下选项之一：
   - **Use the same amount of RAM as the source machine**（使用与源机器相同容量的 RAM），以指定虚拟机与源机器使用的 RAM 容量相同。
   - **Use a specific amount of RAM**（使用指定容量的 RAM），以指定在导出后虚拟机拥有多少内存；例如 4096 MB（推荐）。
9. 要指定 Generation（代系），可单击以下项目之一：
   - 第 1 代（建议）
   - 第 2 代
10. 要指定磁盘格式，请在 **Disk Format**（磁盘格式）旁单击以下选项之一：
    - **VHDX**（默认）
    - **VHD**

    注: 如果目标机器正在运行 Windows 8 (Windows Server 2012) 或更高版本，则 Hyper-V 导出支持 VHDX 磁盘格式。如果您的环境不支持 VHDX，则该选项被禁用。在 Network Adapters（网络适配器）页面上，选择要连接至交换机的虚拟适配器。
11. 在 **Volumes**（卷）页面上，选择要导出的卷。对于作为受保护机器的有效备份的虚拟机，将包括受保护机器的引导驱动器。例如，C:\。

    对于 VHD，选择的卷不能大于 2040 GB。如果选择的卷大于 2040 GB 并且选择了 VHD 格式，将收到错误提示。
12. 在 **Summary**（摘要）页面中，单击 **Finish**（完成）以完成向导并开始导出。

    注: 可以通过查看 **Virtual Standby**（虚拟待机）或 **Events**（事件）选项卡监测导出的状态和进度。

使用 Oracle VirtualBox 导出来导出 Microsoft Windows 数据

在 AppAssure 中，您可通过执行一次性导出或建立连续导出（用于虚拟待机），选择使用 Oracle VirtualBox 导出来导出数据。

请完成以下针对相应类型的导出过程中的步骤。

注: 要执行该导出类型，您应当在 Core 机器上安装 Oracle VirtualBox。Windows 主机支持 VirtualBox 版本 4.2.18 或更高版本。

执行 Oracle VirtualBox 一次性导出

要执行对于 Oracle VirtualBox 的一次性导出，请完成以下过程中的步骤。

要执行 Oracle VirtualBox 一次性导出

1. 在 AppAssure Core 控制台中，执行以下操作之一：
   - 在按钮栏上，单击 **Export**（导出）来启动 Export Wizard（导出向导），并执行以下操作：
     1. 在 **Select Export Type**（选择导出类型）页面上，选择 **One-time export**（一次性导出），然后单击 **Next**（下一步）。
     2. 在 **Protected Machines**（受保护机器）页面上，选择要导出至虚拟机的受保护机器，然后单击 **Next**（下一步）。
   - 导航至要导出的机器，然后在该机器的 **Actions**（操作）下拉菜单中的 **Summary**（摘要）选项卡上，选择 **Export**（导出）> **One-time**（一次性）。

   Export Wizard（导出向导）显示在 **Recovery Points**（恢复点）页面上。
2. 在 **Recovery Points**（恢复点）页面中，从 AppAssure Core 选择要导出的恢复点，然后单击 **Next**（下一步）。
3. 在 Export Wizard（导出向导）中的 **Destination**（目标）页面中，从 **Recover to Virtual machine**（恢复到虚拟机）下拉菜单中选择 **VirtualBox**，然后单击 **Next**（下一步）。
4. 在 **Virtual Machine Options**（虚拟机选项）页面中，选择 **Use Windows machine**（使用 Windows 机器）。
5. 根据下表中的说明，输入用于访问虚拟机的参数。

选项	说明
Virtual Machine Name（虚拟机名称）	输入所创建的虚拟机的名称。 **注:** 默认名称是源机器的名称。
Target Path（目标路径）	指定本地或远程目标路径以创建虚拟机。 **注:** 目标路径不能是根目录。 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。
Memory（内存）	通过单击以下选项之一，指定虚拟机的内存使用量： • 单击 **Use the same amount of RAM as source machine**（使用与源机器相同容量的 RAM），以指定 RAM 配置与源机器相同。 • 单击 **Use a specific amount of RAM**（使用指定容量的 RAM），指定要使用多少 RAM；例如 4096 MB。允许的最小容量为 512 MB，最大容量则取决于主机的容量和限制。（推荐）

6. 要指定虚拟机的用户帐户，请选择 **Specify the user account for the exported virtual machine（指定所导出虚拟机的用户帐户）**，然后输入以下信息。这是指当该虚拟机上存在多个用户帐户时，用于注册该虚拟机的特定用户帐户。当此用户帐户登录时，只有此用户可以在 VirtualBox 管理器中看到此虚拟机。如果未指定帐户，将为包含 Oracle VirtualBox 的 Windows 机器上的所有现有用户注册该虚拟机。
   - **User name（用户名）** - 输入用于注册该虚拟机的用户名。
   - **Password（密码）** - 输入此用户帐户的密码。
7. 单击**下一步**。

   所输入的名称将显示在 Hyper-V Manager 控制台的虚拟机列表中。
8. 在 Volumes（卷）页面上，选择要导出的卷。对于作为受保护机器的有效备份的虚拟机，将包括受保护机器的引导驱动器。例如，C:\。

9. 在 **Summary（摘要）**页面中，单击 **Finish（完成）**以完成向导并开始导出。

   注: 可以通过查看 **Virtual Standby（虚拟待机）**或 **Events（事件）**选项卡监测导出的状态和进度。

执行 Oracle VirtualBox 连续（虚拟待机）导出

完成以下过程中的步骤以创建虚拟待机并执行连续导出到 Oracle VirtualBox。

要执行 VirtualBox 连续（虚拟待机）导出

1. 在 AppAssure Core 控制台中，执行以下操作之一：
   - 在 **Virtual Standby（虚拟待机）**选项卡上，单击 **Add（添加）**以启动 Export Wizard（导出向导）。在 Export Wizard（导出向导）的 **Protected Machines（受保护机器）**页面中，选择要导出的受保护机器，然后单击 **Next（下一步）**。
   - 导航至要导出的机器，在该机器的 **Actions（操作）**下拉菜单中的 **Summary（摘要）**选项卡上，单击 **Export（导出）** > **Virtual Standby（虚拟待机）**。
2. 在 Export Wizard（导出向导）中的 **Destination（目标）**页面中，从 **Recover to Virtual machine（恢复到虚拟机）**下拉菜单中选择 **VirtualBox**，然后单击 **Next（下一步）**。
3. 在 **Virtual Machine Options（虚拟机选项）**页面中，选择 **Use Windows machine（使用 Windows 机器）**。
4. 根据下表中的说明，输入用于访问虚拟机的参数。

选项	说明
Virtual Machine Name（虚拟机名称）	输入所创建的虚拟机的名称。 **注:** 建议使用源自代理名称或与代理名称匹配的名称。您也可以创建源自虚拟机监控程序类型、IP 地址或 DNS 名称的名称。
Target Path（目标路径）	指定本地或远程目标路径以创建虚拟机。 **注:** 目标路径不能是根目录。 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。
Memory（内存）	通过单击以下选项之一，指定虚拟机的内存使用量： • 单击 **Use the same amount of RAM as the source machine**（使用与源机器相同容量的 RAM），以指定虚拟机与源机器之间的 RAM 使用相同。 • 单击 **Use a specific amount of RAM**（使用指定容量的 RAM），指定要使用多少 RAM；例如 4096 MB。允许的最小容量为 512 MB，最大容量则取决于主机的容量和限制。（推荐）

5. 要指定虚拟机的用户帐户，请选择 **Specify the user account for the exported virtual machine（指定所导出虚拟机的用户帐户）**，然后输入以下信息。这是指当该虚拟机上存在多个用户帐户时，用于注册该虚拟机的特定用户帐户。当此用户帐户登录时，只有此用户可以在 VirtualBox 管理器中看到此虚拟机。如果未指定帐户，将为包含 VirtualBox 的 Windows 机器上的所有现有用户注册该虚拟机。
   - **User name（用户名）**- 输入用于注册该虚拟机的用户名。
   - **Password（密码）**- 输入此用户帐户的密码。
6. 选择 **Perform initial one-time export（执行初始一次性导出）**以立即执行虚拟导出，而不是在下一个计划快照后导出。
7. 在 Volumes（卷）页面上，选择要导出的卷。对于作为受保护机器的有效备份的虚拟机，将包括受保护机器的引导驱动器。例如，C:\。

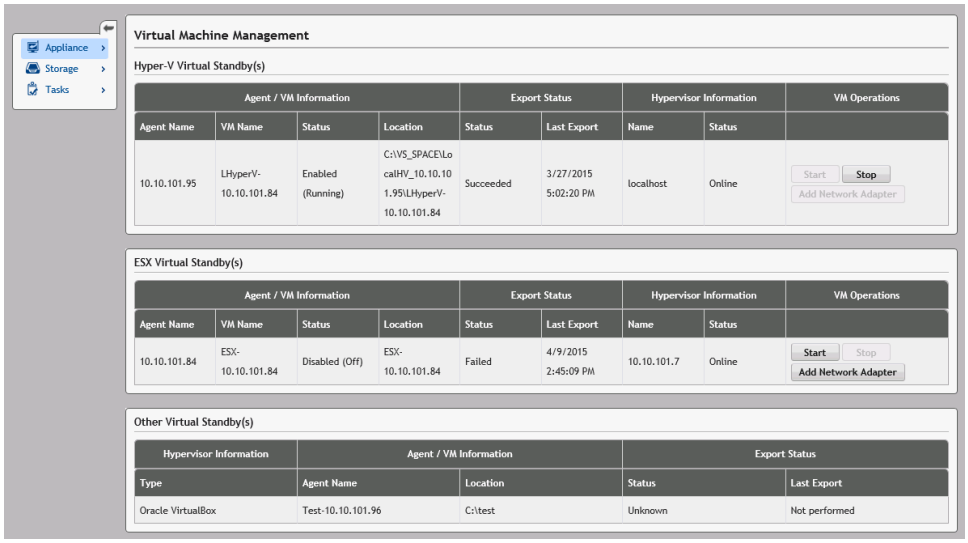
8. 在 **Summary（摘要）**页面中，单击 **Finish（完成）**以完成向导并开始导出。

注: 可以通过查看 **Virtual Standby（虚拟待机）**或 **Events（事件）**选项卡监测导出的状态和进度。

虚拟机管理

VM Management（VM 管理）选项卡显示受保护机器的状态。您可启动、停止和添加网络适配器（仅适用于 Hyper-V 和 ESXi 虚拟机）。要导航至 VM Management（VM 管理）选项卡，可单击 **Appliance（设备）→ VM Management**（VM 管理）。

注: 每次选择 **Appliance（设备）→ VM Management**（VM 管理）选项卡之后，可能最多需要 30 秒时间才会显示 Start（开始）、Stop（停止）和 Add Network Adapter（添加网络适配器）按钮。



Hyper-V 和 ESXi 虚拟待机的 VM 管理

字段	说明
Agent / VM Information（代理/ VM 信息）	**Agent Name**（代理名称）：指明您为其创建了虚拟待机的受保护机器的名称。 **VM Name**（VM 名称）：指明 VM 的名称。 **注:** 建议使用源自代理名称或与代理名称匹配的名称。您也可以创建源自虚拟机监控程序类型、IP 地址或 DNS 名称的名称。 **Status**（状态）：指明虚拟机的状态。可能的值包括: • Running（运行中） • Stopped（停止） • Starting（正在启动） • Suspended（已暂挂） • Stopping（正在停止） • Unknown（未知）（临时状态）

字段	说明
	注: 上述状态值取决于虚拟机监控程序类型。并非所有虚拟机监控程序都会显示所有状态值。
	Location（位置）：指明 VM 的位置。例如 D:\export。VM 位置必须有足够的空间来容纳虚拟机所需的 VM 元数据和虚拟驱动器。
Export Status（导出状态）	**状态** 1. 指明导出过程的以下状态： • Complete（完成） • Failed（故障） • In progress（正在进行） • Not Performed（未执行） 2. 如果导出当前正在进行中，则会显示导出的百分比。
	Last Export（上次导出）：指明上次导出时间。
Hypervisor Information（虚拟机监控程序信息）	**Name**（名称）：指明在其上创建 VM 的虚拟机监控程序的名称。
	Status（状态）：指明指向 Hyper-V 和 ESXi 虚拟机监控程序的连接的状态。 • Online（联机） • Offline（脱机） • Unknown（未知）（临时状态） **注:** 状态仅对 Hyper-V 和 ESXi 虚拟机监控程序显示。
VM Operations（VM 操作）	允许您启动或停止虚拟机，并添加网络适配器。

其他虚拟待机的 VM 管理

字段	说明
Hypervisor Information（虚拟机监控程序信息）	**Type**（类型）：指明虚拟机监控程序的类型。
Agent / VM Information（代理/ VM 信息）	**Agent Name**（代理名称）：指明您为其创建了虚拟待机的受保护机器的名称。
	Location（位置）：指明 VM 的位置。例如 D:\export。VM 位置必须有足够的空间来容纳虚拟机所需的 VM 元数据和虚拟驱动器。
Export Status（导出状态）	**状态** 1. 指明导出过程的以下状态： • Complete（完成） • Failed（故障）

字段	说明
	• In progress（正在进行） • Not Performed（未执行） 2. 如果导出当前正在进行中，则会以进度条形式显示导出的百分比。 **Last Export**（上次导出）：指明上次导出时间。

创建虚拟网络适配器

虚拟机必须有一个或多个虚拟网络适配器 (VNA) 方可连接至 Internet。对于受保护机器上的每个实际网络适配器 (RNA)，VM 应当有一个 VNA。VNA 和匹配的 RNA 应当有相似的配置。在创建“虚拟待机”时，您可将 VNA 添加至您的 VM，或者可以稍后添加 VAN。

在创建虚拟待机并配置虚拟机时，对于受保护机器中的每个适配器，会有一个建议的适配器。您可添加或移除所有或部分建议的适配器。每个 VM 的最大 VNA 数目取决于虚拟机监控程序类型。对于 Hyper-V，您最多可为每个虚拟机添加 8 个适配器。

要创建虚拟网络适配器，请执行以下操作：

1. 导航至 **VM Management**（VM 管理）页面。
2. 单击和 VM 关联的 **Add Network Adapter**（添加网络适配器）按钮来添加 VNA。

   注: 请勿为虚拟待机向仍然在运行备份或受保护机器导出的 VM 添加适配器。额外的 VNA 可导致将来的导出操作失败。

   注: 建议您在即将启动替换受保护机器的 VM 之前添加 VNA。务必通过 Virtual Standby（虚拟待机）选项卡停止或暂停 VM 的所有挂起的导出。

   Virtual Network Adapters and Switches（虚拟网络适配器和交换机）窗口打开。
3. 单击 **Create**（创建）来创建虚拟网络适配器。

   Create Virtual Network Adapter（创建虚拟网络适配器）窗口打开。
4. 从下拉菜单中选择现有虚拟交换机。

   注: 在为 ESXi 选择虚拟交换机时，下拉列表仅会列出名称中有“VM”或“Virtual Machine”的交换机。只能选择 **Virtual Machine Port Group**（虚拟机端口群）类型的交换机，您可通过 ESXi 虚拟机监控程序 GUI 验证交换机类型。
5. 单击 **Create**（创建）。

   注: 要移除虚拟网络适配器，可使用虚拟机监控程序管理界面。

启动 VM 操作

要启动 VM 操作，请执行以下操作：

1. 导航至 **VM Management**（VM 管理）窗口。
2. 单击和 VM 相关的 **Start**（开始）按钮进行启动。

   注: GUI 可能在显示机器的正确状态上有所延迟。在按下 Start（开始）按钮后，最长在 30 秒时间后，该按钮会保持禁用状态。仅当可以启动虚拟机时，才能启用 Start（开始）按钮。

注: 如果当前正在运行或即将开始指向虚拟机的导出任务，请勿单击 Start（开始）按钮。通过查看 **Protected Machines**（受保护机器）选项卡和 **Virtual Standby**（虚拟待机）选项卡可检查下个导出任务的计划。如果已经计划不久即会开始的导出任务，可取消或跳过导出任务，或者等待导出任务完成后再启动虚拟机。尽管您可以在导出任务正在运行时启动虚拟机，但如果在虚拟机正在运行时开始导出数据，导出会失败。

注: 建议您不要启动作为“虚拟待机”保留的 VM。“虚拟待机”VM 作为故障受保护机器的替代机器时处于活动或启动状态。如果受保护机器仍然处于活动状态，需要先通过 Virtual Standby（虚拟待机）选项卡停止或暂停 VM 的任何挂起的导出，再启动 VM。

停止 VM 操作

要停止 VM 操作，请执行以下操作：

1. 导航至 **VM Management**（VM 管理）窗口。
2. 单击和 VM 相关的 **Stop**（停止）按钮停止 VM。

注: 仅当虚拟机当前正在运行时方可启用 Stop（停止）按钮，并且该按钮在启动 VM 后大约 30 秒刷新时间内可用。

注: Start（开始）按钮在停止虚拟机后大约 30 秒内启用。

注: 一旦受保护的 VM 还原，则从虚拟机监控程序及其相应的虚拟待机移除 VM。为还原的受保护机器重新创建虚拟待机。由此可确保虚拟待机 VM 准确创建受保护机器的镜像。

执行回滚

在 AppAssure 中，回滚是指从恢复点还原机器上卷的过程。

注: 受保护的 Linux 机器通过使用命令行 `aamount` 公用程序也支持回滚功能。有关更多信息，请参阅使用命令行执行 Linux 机器的回滚。

要执行回滚，请执行以下操作：

1. 在 Core 控制台中，执行以下操作之一：
   - 单击 **Machines**（机器）选项卡，然后执行以下操作：

   a. 在受保护机器的列表中，选中要导出的机器旁的复选框。
   b. 在该机器的 **Actions（操作）**下拉菜单中，单击 **Rollback**（回滚）。
   c. 在 **Rollback - Select Recovery Point**（回滚 - 选择恢复点）对话框中，选择要导出的恢复点并单击 **Next**（下一步）。
      - 在 AppAssure Core 控制台的左侧导航区域中，选择要回滚的机器，从而打开该机器的 **Summary**（摘要）选项卡。
   d. 单击 **Recovery Points**（恢复点）选项卡，然后从列表中选择一个恢复点。
   e. 展开该恢复点的详细信息，然后单击 **Rollback**（回滚）。
2. 根据下表中的说明编辑回滚选项。

文本框	说明
Protected Machine（受保护机器）	指定原始代理机器作为回滚目标。源是指从中创建用于回滚的恢复点的代理。

文本框	说明
Recovery Console Instance（恢复控制台实例）	要将恢复点还原至以 URC 模式引导的机器，请输入用户名和密码。

3. 单击 **Load Volumes**（加载卷）。
   此时将显示 **Volume Mapping**（卷映射）对话框。

   注: Core 控制台不会自动映射 Linux 卷。要找到 Linux 卷，请浏览至您要回滚的卷。
4. 选择要回滚的卷。
5. 使用 **Destination**（目标）选项选择所选卷应回滚到的目标卷。
6. 从以下选项中进行选择：
   - **Live Recovery**（实时恢复）。选中时，将立即进行 Windows 卷的回滚。默认选中此选项。

     注: Live Recovery（实时恢复）选项不可用于 Linux 卷。
   - **Force Dismount**（强制卸载）。选中时，在执行回滚之前将强制卸载所有已装载的恢复点。默认选中此选项。
7. 单击 **Rollback**（回滚）。
   系统开始执行回滚到所选恢复点的过程。

使用命令行执行 Linux 机器的回滚

回滚是指从恢复点还原机器上的卷的过程。在 AppAssure 中，可以使用命令行 `aamount` 公用程序对受保护 Linux 机器上的卷执行回滚。

小心: 请勿尝试在系统或根 (/) 卷上执行回滚。

注: 在 Core 控制台中支持对受保护 Windows 机器执行回滚功能。有关更多信息，请参阅执行回滚。

要为 Linux 机器上的卷执行回滚，请执行以下操作：

1. 以 root 身份运行 AppAssure `aamount` 公用程序，例如：
   ```
   sudo aamount
   ```
2. 在 AppAssure 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 AppAssure 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 AppAssure 服务器所保护的机器。它按行项目号、主机/IP 地址和机器的 ID 号列出所找到的代理机器（例如：`293cc667-44b4-48ab-91d8-44bc74252a4f`）。
5. 要列出指定机器当前已装载的恢复点，请输入以下命令：
   ```
   lr <machine_line_item_number>
   ```

   注: 也可以在此命令中输入机器 ID 号，而不是行项目号。

   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。此列表包含行项目号、日期/时间戳、卷的位置、恢复点的大小，以及卷的 ID 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. 要选择进行回滚的恢复点，请输入以下命令：
   ```
   r [volume_recovery_point_ID_number] [path]
   ```

此命令将 ID 所指定的卷映像从 Core 回滚到指定路径。回滚路径是设备文件描述符的路径，而不是所装载到的目录。

注: 要标识恢复点，也可以在命令中指定行号来代替恢复点 ID 号。在这种情况下，使用代理/机器行号（来自 `lm` 输出），后跟恢复点行号和卷号，再后跟路径，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 3 个代理机器，而您为第 2 号机器输入 `lr` 命令，并希望将 23 恢复点卷 b 回滚至装载到目录 `/mnt/data` 的卷，则命令为：`r2 23 b /mnt/data`。

注: 可以回滚到 /，但只有在使用 Live CD 引导以执行裸机还原时才能这样做。有关更多信息，请参阅对 Linux 机器执行裸机还原。

7. 系统提示继续时，输入 `y` 进行确认。

   回滚继续后，系统将显示一系列消息，以告知您状态。

8. 成功完成回滚后，如果目标以前受到保护并安装，则 `aamount` 公用程序会自动装载内核模块并将其重新连接到所回滚的卷。如果未受到保护和安装，则将回滚卷装载至本地磁盘，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。

   小心: 请勿手动卸载受保护的 Linux 卷。如果您需要手动卸载受保护的 Linux 卷，则在卸载卷之前必须先执行以下命令：`bsctl -d [path to volume]`。

   在此命令中，[path to volume] 不是引用卷的安装点，而是引用卷的文件描述符；它必须采用类似此例的格式：`/dev/sda1`。

关于 Windows 机器的裸机还原

当服务器如预期运行时，将运行和执行所配置的任务。如果发生灾难性事件导致服务器无法运行，则需要立即执行步骤将服务器还原到之前的运行状态。该过程通常需要重新格式化机器，重新安装操作系统，通过备份恢复数据，并重新安装软件应用程序。

AppAssure 可以为 Windows 机器执行裸机还原 (BMR)，而无论硬件相似还是不同。此过程包括创建引导 CD 映像、将映像刻录到磁盘、从磁盘引导目标服务器、连接到恢复控制台实例、映射卷、启动恢复，然后监测该过程。裸机还原完成后，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，然后再进行特有的设置和配置。

其他情况下也可以选择执行裸机还原，包括硬件升级或服务器更换。

此外还支持使用命令行 `aamount` 公用程序对受保护的 Linux 机器执行 BMR 功能。有关更多信息，请参阅对 Linux 机器执行裸机还原。

对 Windows 机器执行裸机还原的前提条件

在开始执行 Windows 机器的裸机还原的过程之前，必须确保具备以下条件和标准：

- 备份服务器和工作中的 Core
- 要还原的硬件（不论新旧以及是否相似）
- 空白 CD 和 CD 刻录软件
- VNC 查看器（可选）
- 用于目标机器的 Windows 7 PE（32 位）兼容驱动程序存储和网络适配器驱动程序
- 存储控制器、RAID、AHCI 和目标操作系统的芯片组驱动程序

注: 只有当要执行的还原涉及不同的硬件时才需要存储控制器驱动程序。

对 Windows 机器执行裸机还原的路线图

要对 Windows 机器执行裸机还原，请执行以下操作：

1. 创建引导 CD。请参阅创建可引导 CD ISO 映像。
2. 将映像刻录到磁盘。
3. 从引导 CD 引导目标服务器。请参阅加载引导 CD。
4. 连接到恢复磁盘。
5. 映射卷。请参阅映射卷。
6. 启动恢复。请参阅从 AppAssure Core 启动恢复。
7. 监测进度。请参阅查看恢复进度。

创建可引导 CD ISO 映像

要执行 Windows 机器的裸机还原，必须在 Core 控制台中创建可引导 CD/ISO 映像，其中包含 AppAssure 通用恢复控制台界面。AppAssure 通用恢复控制台是用于直接从 AppAssure Core 还原系统驱动器或整个服务器的环境。

所创建的 ISO 映像是针对要还原的机器定制的；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引导 CD 所在机器不同的硬件，则必须在引导 CD 中包含存储控制器和其他驱动程序。请参阅在引导 CD 中注入驱动程序。

注: 国际标准化组织 (ISO) 是由各国负责确定和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。它支持 Windows 等多种操作系统。ISO 映像是包含所有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。

要创建可引导 CD ISO 映像，请执行以下操作：

1. 在想要还原的服务器所在的 Core 控制台中，选择 **Core**，然后单击 **Tools（工具）**选项卡。
2. 单击 **Boot CDs**（引导 CD）。
3. 选择 **Actions**（操作），然后单击 **Create Boot ISO**（创建引导 ISO）。
   此时将显示 **Create Boot CD**（创建引导 CD）对话框。要完成此对话框，请使用以下过程。

命名引导 CD 文件并设置路径

要命名引导 CD 文件并设置路径，请执行以下操作：

在 **Create Boot CD**（创建引导 CD）对话框中，输入 Core 服务器上用来存储引导映像的 ISO 路径。

如果要用来存储映像的共享磁盘空间不足，可根据需要设置路径；例如 D:\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。

创建连接

要创建连接，请执行以下操作：

1. 在 **Connection Options（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 **Obtain IP address automatically**（自动获取 IP 地址）。
- （可选）要指定恢复控制台的静态 IP 地址，请选择 **Use the following IP address**（使用下面的 IP 地址），然后在相应的字段中输入 IP 地址、子网掩码、默认网关和 DNS 服务器。必须指定所有这些字段。

2. 如果需要，在 **UltraVNC Options**（UltraVNC 选项）中选择 **Add UltraVNC**（添加 UltraVNC），然后输入 UltraVNC 选项。利用 UltraVNC 设置可以从远程管理使用中的恢复控制台。

   注: 此步骤是可选的。如果需要远程访问恢复控制台，则必须配置和使用 UltraVNC。使用引导 CD 时，不能使用 Microsoft 终端服务登录。

在引导 CD 中注入驱动程序

驱动程序注入用于促进恢复控制台、网络适配器及目标服务器存储之间的可操作性。

如果预期还原到不同的硬件，则必须在引导 CD 中注入存储控制器、RAID、AHCI、芯片集和其他驱动程序。这些驱动程序使操作系统能够成功检测和操作所有设备。

注: 请记住，引导 CD 将自动包含 Windows 7 PE 32 位驱动程序。

要在引导 CD 中注入驱动程序，请执行以下操作：

1. 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. 使用文件压缩公用程序（例如 WinZip）压缩包含驱动程序的文件夹。
3. 在 **Create Boot CD**（创建引导 CD）对话框中的 **Drivers**（驱动程序）窗格中，单击 **Add a Driver**（添加驱动程序）。
4. 要找到压缩后的驱动程序文件，请在文件系统中导航。选择该文件，然后单击 **Open**（打开）。

   已注入的驱动程序将在 **Drivers**（驱动程序）窗格中突出显示。

创建引导 CD

要创建引导 CD，在命名引导 CD 和指定路径、创建连接和注入驱动程序（可选）后，在 **Create Boot CD**（创建引导 CD）屏幕中单击 **Create Boot CD**（创建引导 CD）。即会创建 ISO 映像。

查看 ISO 映像创建进度

要查看 ISO 映像的创建进度，请选择 **Events**（事件）选项卡，然后可以在 **Tasks**（任务）下监测构建 ISO 映像的进度。

注: 此外还可以在 **Monitor Active Task**（监测活动任务）对话框中查看 ISO 映像的创建进度。

ISO 映像创建完成后，此映像将出现在 **Boot CDs**（引导 CD）页面中，可通过 **Tools**（工具）菜单访问。

访问 ISO 映像

要访问 ISO 映像，请导航至指定的输出路径，或者单击链接以将映像下载到随后可在新系统中加载该映像的位置。例如，网络驱动器。

加载引导 CD

当创建了引导 CD 映像后，请使用新创建的引导 CD 引导目标服务器。

注: 如果使用 DHCP 创建引导 CD，请记下 IP 地址和密码。

要加载引导 CD，请执行以下操作：

1. 导航至新服务器，加载引导 CD，然后启动机器。
2. 指定 **Boot from CD-ROM**（从 CD-ROM 引导），将加载以下内容：
   - Windows 7 PE
   - AppAssure 代理软件

   AppAssure 通用恢复控制台启动并显示机器的 IP 地址和验证密码。
3. 记录 Network Adapters Settings（网络适配器设置）窗格中显示的 IP 地址以及 Authentication（验证）窗格中显示的验证密码。在随后的数据恢复过程中将需要使用此信息，以便登录回控制台。
4. 如果要更改 IP 地址，请选择它并单击 **Change**（更改）。

   注: 如果在 Create Boot CD（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 **Network Adapter settings**（网络适配器设置）屏幕中。

将驱动程序注入目标服务器

如果要还原到不同的硬件，则必须在引导 CD 中注入存储控制器、RAID、AHCI、芯片集和其他驱动程序（如果尚未包含在引导 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。

如果您不确定目标服务器需要哪些驱动程序，请单击通用恢复控制台中的 System Info（系统信息）选项卡。此选项卡显示您要还原到的目标服务器上的所有系统硬件和设备类型。

注: 请记住，您的目标服务器将自动包含 Windows 7 PE 32 位驱动程序。

要将驱动程序注入目标服务器，请执行以下操作：

1. 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. 使用文件压缩公用程序（例如 WinZip）压缩包含驱动程序的文件夹，然后将其复制到目标服务器。
3. 在通用恢复控制台中，单击 **Driver Injection**（驱动程序注入）。
4. 要找到压缩后的驱动程序文件，请在文件系统中导航并选择该文件。
5. 如果在步骤 3 中单击了 **Driver Injection**（驱动程序注入），则单击 **Add Driver**（添加驱动程序）。如果在步骤 3 中单击了 **Load driver**（加载驱动程序），则单击 **Open**（打开）。

   系统注入所选驱动程序，并将在您重新引导目标服务器后加载到操作系统中。

从 Core 启动还原

要从 Core 启动还原，请执行以下操作：

1. 如果要还原的任意系统上的 NIC 进行了组合（绑定），则移除所有多余的网络线缆（只留下一条）。

   注: AppAssure 还原无法识别组合的 NIC。如果有多个活动连接，恢复过程将无法决定使用哪个 NIC。
2. 导航回 Core 服务器，然后打开 Core 控制台。
3. 在 **Machines**（机器）选项卡上，选择要从中还原数据的机器。
4. 单击该机器的 **Actions**（操作）菜单，再单击 **Recovery Points**（恢复点），以查看该机器的所有恢复点的列表。
5. 展开要用于还原的恢复点，然后单击 **Rollback**（回滚）。
6. 在 **Rollback**（回滚）对话框的 **Choose Destination**（选择目标）下，选择 **Recovery Console Instance**（Recovery Console 实例）。
7. 在 **Host**（主机）和 **Password**（密码）文本框中，输入要将数据还原到的新服务器的 IP 地址和验证密码。

注: Host（主机）和 Password（密码）值是在上一任务中记录的凭据。有关更多信息，请参阅加载引导 CD。

8. 单击 **Load Volumes**（加载卷）以将目标卷加载到新机器。

映射卷

可以选择以自动或手动方式将卷映射到目标服务器上的磁盘。自动对齐磁盘时，将清理磁盘并重新分区，所有数据将被删除。执行对齐时将按照卷所列出的顺序，并根据大小等因素将卷相应地分配给磁盘等。磁盘可被多个卷使用。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，您必须在还原之前已正确格式化新机器。有关更多信息，请参阅从 AppAssure Core 启动还原。

要映射卷，请执行以下操作：

1. 要自动映射卷，请执行以下操作：
   a. 在 **RollbackURC**（回滚 URC）对话框中，选择 **Automatically Map Volumes**（自动映射卷）选项卡。
   b. 在 **Disk Mapping**（磁盘映射）区域中的 **Source Volume**（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。
   c. 如果自动映射的目标磁盘是正确的目标卷，则选择 **Destination Disk**（目标磁盘）。
   d. 单击 **Rollback**（回滚），然后继续执行步骤 3。
2. 要手动映射卷，请执行以下操作：
   a. 在 **RollbackURC**（回滚 URC）对话框中，选择 **Manually Map Volumes**（手动映射卷）选项卡。
   b. 在 **Volume Mapping**（卷映射）区域中的 **Source Volume**（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。
   c. 在 **Destination**（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裸机还原的目标卷，然后单击 **Rollback**（回滚）。
3. 在 **RollbackURC**（回滚 URC）确认对话框中，检查恢复点源卷与回滚目标卷的映射。要执行回滚，请单击 **Begin Rollback**（开始回滚）。

警告: 如果选择 Begin Rollback（开始回滚），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。

查看恢复进度

要查看恢复进度，请执行以下操作：

1. 启动回滚过程后，将显示 **Active Task**（活动任务）对话框，其中显示已启动的回滚操作。

   注: 出现 **Active Task**（活动任务）对话框并不表示已成功完成任务。

2. （可选）要监测回滚任务进度，请在 Active Task（活动任务）对话框中单击 **Open Monitor Window**（打开监测窗口）。可在 **Monitor Open Task**（监测未完成任务）窗口中查看恢复状态以及开始时间和结束时间。

   注: 要返回源机器的恢复点，请在 **Active Task**（活动任务）对话框中单击 **Close**（关闭）。

启动已还原的目标服务器

要启动已还原的目标服务器，请执行以下操作：

1. 导航回目标服务器，然后在 **AppAssure 通用恢复控制台**界面中，单击 **Reboot**（重新引导）以启动该机器。
2. 指定正常启动 Windows。
3. 登录到机器。

   系统已还原到裸机还原之前的状态。

修复启动问题

请记住，如果要还原到不同的硬件，则必须在引导 CD 中注入存储控制器、RAID、AHCI、芯片集和其他驱动程序（如果尚未包含在引导 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。

要修复启动问题，请执行以下操作：

1. 如果在启动已还原的目标服务器时遇到问题，请通过重新加载引导 CD 来打开通用恢复控制台。
2. 在通用恢复控制台中，单击 **Driver Injection**（驱动程序注入）。
3. 在 Driver Injection（驱动程序注入）对话框中，单击 **Repair Boot Problems**（修复引导问题）。

   系统将自动修复目标服务器引导记录中的启动参数。
4. 在通用恢复控制台中，单击 **Reboot**（重新引导）。

对 Linux 机器执行裸机还原

您可以对 Linux 机器执行裸机还原 (BMR)，包括回滚系统卷。使用 AppAssure 命令行公用程序 `aamount` 回滚到引导卷基本映像。在对 Linux 机器执行 BMR 之前，必须先执行以下操作：

- 从 AppAssure 支持部门获取 BMR Live CD 文件，其中包含可引导版本的 Linux。

  注: 也可从许可证门户 **https://licenseportal.com** 下载 Linux Live CD 文件。
- 确保目标机器上的硬盘驱动器有足够的空间可用于创建目标分区，以容纳源卷。任何目标分区都应至少与原始源分区的大小相同。
- 确定回滚路径，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。

  注: 开始使用 AppAssure 命令之前，可以安装屏幕公用程序。屏幕公用程序支持滚动屏幕以查看大量数据，例如恢复点列表。有关安装屏幕公用程序的信息，请参阅安装屏幕公用程序

要对 Linux 机器执行裸机还原，请执行以下操作：

1. 使用从 AppAssure 获取的 Live CD 文件引导 Linux 机器并打开 Terminal（终端）窗口。
2. 如果需要，创建新磁盘分区，例如，以 root 身份运行 `fdisk` 命令，然后通过使用 `a` 命令将该分区设置为可引导。
3. 以 root 身份运行 AppAssure `aamount` 公用程序，例如：

   ```
   sudo aamount
   ```
4. 在 AppAssure 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 AppAssure Core 服务器的 IP 地址或主机名。
6. 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 AppAssure Core 服务器所保护的机器。它按行项目号、主机/IP 地址和机器的 ID 号列出所找到的机器（例如：293cc667-44b4-48ab-91d8-44bc74252a4f）。

7. 要列出所还原机器的当前已装载恢复点，请输入以下命令：

   `lr <machine_line_item_number>`

   注: 也可以在此命令中输入机器 ID 号，而不是行项目号。

   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。此列表包含行项目号、日期/时间戳、卷的位置、恢复点的大小，以及卷的 ID 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”）。

8. 要选择用于回滚的基本映像恢复点，请输入以下命令：

   `r <volume_base_image_recovery_point_ID_number> <path>`

   小心: 您必须确保系统卷未装载。

   此命令将 ID 所指定的卷映像从 Core 回滚到指定路径。回滚路径是设备文件描述符的路径，而不是所装载到的目录。

   注: 您也可以在命令中指定行号来代替恢复点 ID 号，以标识恢复点。即在代理/机器行号（来自 lm 输出）后面跟恢复点行号和卷号，再跟路径，例如 **r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**。在此命令中，**<path>** 是实际卷的文件描述符。

9. 系统提示继续时，输入 y 进行确认。

   回滚继续后，系统将显示一系列消息，以告知您状态。

10. 成功完成回滚后，如果需要，使用所还原的引导装载程序更新主引导记录。

    注: 只有在回滚到新磁盘时，才需要修复或设置引导装载程序。如果只是还原到同一磁盘，则不需要设置引导装载程序。

    小心: 请勿手动卸载受保护的 Linux 卷。如果您需要手动卸载受保护的 Linux 卷，则在卸载卷之前必须先执行以下命令：bsctl -d <path to volume>。

    在此命令中，<path to volume> 不是引用卷的装载点，而是引用卷的文件描述符；它必须采用类似此例的格式：**/dev/sda1**。

安装 Screen 公用程序

开始使用 AppAssure 命令之前，可以安装 screen 公用程序。screen 公用程序支持滚动屏幕以查看大量数据，例如恢复点列表。

要安装 screen 公用程序，请执行以下操作：

1. 使用 Live CD 文件，启动 Linux 机器。

   将打开终端窗口。

2. 输入以下命令：`sudo apt-get install screen`。
3. 要启动 screen 公用程序，请在命令提示符中键入 `screen`。

在 Linux 机器上创建可引导分区

要使用命令行在 Linux 机器上创建可引导分区，请执行以下操作：

1. 以 root 身份使用 **bsctl** 公用程序通过以下命令连接到所有设备：`sudo bsctl --attach-to-device /dev/<restored volume>`

注: 为每个已还原卷重复此步骤。

2. 使用以下命令装载每个已还原卷：

```
mount /dev/<restored volume> /mnt

mount /dev/<restored volume> /mnt
```

注: 一些系统配置可能在引导卷中包含引导目录。

3. 使用以下命令装载每个已还原卷的快照元数据：

```
sudo bsctl --reset-bitmap-store /dev/<restored volume>

sudo bsctl --map-bitmap-store /dev/<restored volume>
```

4. 使用 `blkid` 命令或 `ll /dev/disk/by-uuid` 命令验证通用唯一标识符 (UUID) 是否包含新卷。
5. 验证 `/etc/fstab` 是否包含根和引导卷的正确 UUID。
6. 使用以下命令安装 Grand Unified Bootloader (GRUB)：

```
mount --bind /dev/ /mnt/dev

mount --bind /proc/ /mnt/proc

chroot/mnt/bin/bash

grub-install/dev/sda
```

7. 验证 **/boot/grub/grub.conf** 文件是否包含引导卷的正确 UUID，或者根据需要使用文本编辑器进行更新。
8. 从 CD-ROM 驱动器中取出 Live CD 光盘，然后重新启动 Linux 机器。

查看事件和警报

要查看事件和警报，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台的 Machines（机器）选项卡上，单击要查看其事件的机器的超链接。
   - 在 Core 控制台的左侧**导航**区域中，选择要查看其事件的机器。
2. 单击 **Events**（事件）选项卡。

   此时将显示当前任务和警报的所有事件的日志。

5

保护服务器群集

关于服务器群集保护

在 AppAssure 中，服务器群集保护与各个群集节点（即群集中的各个机器）上安装的 AppAssure 代理以及保护这些代理的 Core 有关，所有这些组件就像是一个复合机器。

您可以轻松配置 Core，以保护和管理群集。在 Core 控制台中，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，Core 列示在导航树的顶部，而群集则位于 Core 的下方，其中包含关联的各个节点（安装有 AppAssure 代理）。

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。群集将显示在 Core 控制台的 Machines（机器）选项卡中，通过切换视图（使用 Show/Hide（显示/隐藏））可查看群集中包含的节点。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。您可以指定整个群集及其共享卷的设置，也可以导航至群集中的某个节点（机器），以单独配置该节点及其关联本地卷的设置。

支持的应用程序和群集类型

要正确保护群集，必须在群集中的每个机器或节点上安装 AppAssure 代理软件。AppAssure 支持下表中列出的应用程序版本和群集配置。

表. 4: 支持的应用程序和群集类型

应用程序	应用程序版本和相关群集配置	Windows 故障转移群集
Microsoft Exchange	2007 单一副本群集 (SCC)	2003、2008、2008 R2
	2007 群集连续复制 (CCR)	
	2010 数据库可用性组 (DAG)	2008、2008 R2
Microsoft SQL	2005、2008、2008 R2 单一副本群集 (SCC)	2003、2008、2008 R2
	2012 单一副本群集 (SCC)	2008、2008 R2、2012

支持的磁盘类型包括：

- 超过 2 TB 的 GUID 分区表 (GPT) 磁盘
- 动态磁盘
- 基本磁盘

支持的安装类型包括：

- 以驱动器号（例如，D:）连接的共享驱动器
- 单个物理磁盘上的简单动态卷（未进行分条、镜像或跨越卷）
- 作为装载点连接的共享驱动器

保护群集

本主题介绍如何在 AppAssure 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 AppAssure 代理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 AppAssure Core 关联的存储库。

有关设置存储库的信息，请参阅关于存储库。

要保护群集，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，导航至 **Home**（主页）选项卡，然后单击 **Protect Cluster**（保护群集）按钮。
   - 在 Core 控制台中的 **Machines**（机器）选项卡中，单击 **Actions**（操作），然后单击 **Protect Cluster**（保护群集）。
2. 在 **Connect to Cluster**（连接至群集）对话框中，输入以下信息：

文本框	说明
Host（主机）	要保护的群集、群集应用程序或某一群集节点的主机名或 IP 地址。 **注:** 如果使用某个节点的 IP 地址，则需要在此节点上安装并启动 AppAssure 代理。
Port（端口）	AppAssure Core 用来与代理进行通信的机器端口号。
User name（用户名）	用于连接此机器的域管理员的用户名，例如 **domain_name\administrator** 或 **administrator@domain_name.com** **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。
Password（密码）	用于连接至此机器的密码。

3. 在 **Protect Cluster**（保护群集）对话框中，为此群集选择一个存储库。
4. 要使用默认设置保护群集，请选择默认保护的节点，然后单击 **Protect**（保护）。

   注: 默认设置可确保按照 60 分钟间隔的默认计划保护所有卷。
5. 要输入群集的自定义设置（例如，自定义共享卷的保护计划），请执行以下操作：
   a. 单击 **settings**（设置）。
   b. 在 **Volumes**（卷）对话框中，选择要保护的卷，然后单击 **Edit**（编辑）。
   c. 在 **Protection Schedule**（保护计划）对话框中，根据下表中的说明选择一个计划选项来保护数据。

文本框	说明
Interval（间隔时间）	您可以选择： • **Weekday**（工作日）— 要以特定间隔时间保护数据，请选择 **Interval**（间隔时间），然后： – 要自定义在高峰期的某个时间保护数据，可以指定开始时间、结束时间和间隔时间。 – 要在非高峰时期保护数据，请选中 **Protect during off-peak times**（在非高峰期保护）复选框，然后选择保护的间隔时间。

文本框	说明
	• **Weekends**（周末）— 要在周末也保护数据，请选中 **Protect during weekends**（在周末期间保护）复选框，然后选择间隔时间。
Daily（每天）	要每天保护数据，请选择 **Daily**（每天）选项，然后为 **Protection Time**（保护时间）选择开始保护数据的时间。
No Protection（无保护）	要从此卷移除保护，请选择 **No Protection**（无保护）选项。

6. 完成所有必要更改后，单击 **Save**（保存）。
7. 要为群集中的节点输入自定义设置，请选择节点，然后单击该节点旁边的 **Settings**（设置）链接。
   - 重复步骤 5 以编辑保护计划。

   有关自定义节点的更多信息，请参阅保护群集中的节点。
8. 在 **Protect Cluster**（保护群集）对话框中，单击 **Protect**（保护）。

保护群集中的节点

本主题介绍如何保护已安装 AppAssure 代理的群集节点或机器上的数据。添加保护时，需要从可用节点列表中选择一个节点，并且指定主机名及域管理员的用户名和密码。

要保护群集中的节点，请执行以下操作：

1. 添加群集后，导航至该群集，然后单击 **Machines**（机器）选项卡。
2. 单击 **Actions**（操作）菜单，然后单击 **Protect Cluster Node**（保护群集节点）。
3. 在 **Protect Cluster Node**（保护群集节点）对话框中，酌情选择或输入以下信息，然后单击 **Connect**（连接）以添加机器或节点。

文本框	说明
主机	群集中可进行保护的节点的下拉列表。
Port（端口）	Core 用来与节点上的代理进行通信的端口号。
User name（用户名）	用于连接此节点的域管理员的用户名，例如，针对 **administrator@example_domain.com** 的 **example_domain\administrator**。
密码	用于连接至此机器的密码。

4. 单击 **Protect**（保护），开始使用默认保护设置保护此机器。

   注: 默认设置可确保使用 60 分钟间隔的计划保护所有卷。
5. 要为此机器输入自定义设置（例如，更改显示名称、添加加密或自定义保护计划），请单击 **Show Advanced Options**（显示高级选项）。
6. 根据需要编辑以下设置，如下表所述。

文本框	说明
Display Name（显示名称）	输入要在 Core 控制台中显示的机器的新名称。
Repository（存储库）	在 Core 上选择要用于存储此机器的数据的存储库。

文本框	说明
Encryption（加密）	指定是否对此机器上要存储在存储库中的每个卷的数据应用加密。 **注:** 存储库的加密设置在 Core 控制台中的 **Configuration（配置）**选项卡下进行定义。
计划	选择以下选项之一。 • Protect all volumes with default schedule（使用默认计划保护所有卷）。 • Protect specific volumes with custom schedule（使用自定义计划保护特定卷）。然后，在 **Volumes**（卷）下选择一个卷并单击 **Edit**（编辑）。有关设置自定义间隔的信息，请参阅保护群集。

修改群集节点设置的过程

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：

1. 请执行以下操作之一：
   - 导航至包含要修改的节点的群集，单击 **Machines**（机器）选项卡，然后选择要修改的机器或节点。
   - 或者，在 **Navigation**（导航）窗格的 **Cluster**（群集）标题下，选择要修改的机器或节点。
2. 要修改和查看配置设置，请参阅查看和修改配置设置。
3. 要配置系统事件的通知组，请参阅配置系统事件的通知组。
4. 要自定义保留策略设置，请参阅自定义保留策略设置。
5. 要修改保护计划，请参阅修改保护计划。
6. 要修改传输设置，请参阅修改传输设置。

配置群集设置的路线图

配置群集设置的路线图包括执行以下任务：

- 修改群集设置
- 配置群集事件通知
- 修改群集保留策略
- 修改群集保护计划
- 修改群集传输设置

修改群集设置

添加群集后，即可轻松修改基本设置（例如，显示名称）、保护设置（例如，保护计划、添加或移除卷、暂停保护）等。

要修改群集设置，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要修改的群集。

- 在左侧导航区域中选择要修改的群集。

2. 单击 **Configuration**（配置）选项卡。
   此时将显示 **Settings**（设置）页面。
3. 单击 **Edit**（编辑），根据下面的说明修改此页面上的群集设置：

文本框	说明
Display Name（显示名称）	输入群集的显示名称。 此群集的名称将显示在 Core 控制台中。默认情况下，该名称是群集的主机名。如果需要，可以将其更改为更具描述性的名称。
主机名	此设置代表群集的主机名。它列在此处仅供参考，无法进行修改。
Repository（存储库）	输入与群集关联的 Core 存储库。 **注:** 如果已创建此群集的快照，则此设置列在此处仅供参考，无法进行修改。
Encryption Key（加密密钥）	根据需要编辑和选择加密密钥。 此设置指定是否对此群集上要存储在存储库中的每个卷的数据应用加密。

配置群集事件通知

您可以通过创建通知组来配置如何报告群集的系统事件。这些事件可能是系统警报或错误。
要配置群集事件通知，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要修改的群集。
   - 在左侧导航区域中选择要修改的群集。
2. 单击 **Configuration**（配置）选项卡，然后单击 **Events**（事件）。
3. 选择下表中说明的选项之一。

文本框	说明
Use Core alert settings（使用 Core 警报设置）	此选项采用相关联的 Core 所使用的设置： a. 单击**应用**。 b. 完成步骤 5。
Use Custom alert settings（使用自定义警报设置）	使用此选项可配置自定义设置。继续执行步骤 4。

4. 如果选择 **Custom alert settings**（自定义警报设置），请单击 **Add Group**（添加组），以添加要发送系统事件列表的新通知组。
   此时将显示 **Add Notification Group**（添加通知组）对话框。
5. 根据下表中的说明添加通知选项。

文本框	说明
名称	输入通知组的名称。

文本框	说明
说明	输入通知组的说明。
Enable Events（启用事件）	选择要通知的事件，例如 Clusters（群集）。也可以按类型选择： • **Error（错误）** • **警告** • **信息** **注:** 当按类型选择时，默认情况下，将自动启用相应的事件。例如，如果选择 Warning （警告），则将启用 Attachability（可附加性）、Jobs（作业）、Licensing（许可）、Archive（存档）、CoreService（Core 服务）、Export（导出）、Protection（保护）、Replication（复制）和 Rollback（回滚）事件。
Notification Options（通知选项）	选择指定如何处理通知的方法。以下选项可供选择： • **Notify by Email**（通过电子邮件通知）— 在 To（收件人）、CC（抄送）和 BCC（密件抄送）文本框中指定将事件发送到的电子邮件地址。 • **Notify by Windows Event log**（通过 Windows 事件日志通知）— Windows 事件日志将控制通知。 • **Notify by syslogd**（通过系统日志通知）— 指定要将事件发送到的主机名和端口。

6. 单击 **OK**（确定）保存所做的更改，然后单击 **Apply**（应用）。
7. 要编辑现有通知组，请在列表中的通知组旁，单击 **Edit**（编辑）。
   此时将显示 **Edit Notification Group**（编辑通知组）对话框，可用于编辑设置。

修改群集保留策略

群集的保留策略用于指定群集中共享卷的恢复点将在存储库中保存多长时间。保留策略用于长期保留备份快照，并帮助管理这些备份快照。保留策略通过前滚流程执行，该流程有助于老化和删除旧备份。

1. 请执行以下操作之一：
   - 在 **Core** 控制台中，单击 **Machines**（机器）选项卡，然后选择要修改的群集。
   - 在左侧导航区域中选择要修改的群集。
2. 单击 **Configuration**（配置）选项卡，然后单击 **Retention Policy**（保留策略）。
3. 选择下表中的选项之一：

文本框	说明
Use Core default retention policy（使用 Core 默认保留策略）	此选项采用相关联的 Core 所使用的设置。单击 **Apply**（应用）。
Use Custom retention policy（使用自定义保留策略）	使用此选项可配置自定义设置。

注: 如果选择 **Custom alert settings**（自定义警报设置），请按照自定义保留策略设置中介绍的关于设置自定义保留策略的说明，从步骤 4 开始操作。

修改群集保护计划

只有群集具有共享卷时，才能修改保护计划。

要修改群集保护计划：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要修改的群集。
   - 在左侧导航区域中选择要修改的群集。
2. 单击 **Configuration**（配置）选项卡，然后单击 **Protection Settings**（保护设置）。
3. 按照修改保护计划中介绍的关于修改保护设置的说明，从步骤 2 开始操作。

修改群集传输设置

在 AppAssure 中，可以修改用于管理受保护群集的数据传输过程的设置。

注: 仅当群集具有共享卷时才能修改群集传输设置。

AppAssure 中有三种传输类型：

文本框	说明
Snapshots（快照）	备份受保护群集上的数据。
VM Export（VM 导出）	使用所有备份信息和参数（由为保护群集而定义的计划所指定）创建虚拟机。
Rollback（回滚）	还原受保护群集的备份信息。

要修改群集传输设置，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要修改的群集。
   - 在左侧导航区域中选择要修改的群集。
2. 单击 **Configuration**（配置）选项卡，然后单击 **Transfer Settings**（传输设置）。
3. 根据修改保护计划中的说明修改保护设置，从步骤 2 开始操作。

将受保护群集节点转换为代理

在 AppAssure 中，可以将受保护的群集节点转换为 AppAssure 代理，以便 Core 继续对其进行管理，但它不再是群集的一部分。这很有帮助，例如，当您想要从群集中移除群集节点但仍对其进行保护时，就可以这样做。

要将受保护群集节点转换为代理，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择包含要转换的机器的群集。单击该群集的 **Machines**（机器）选项卡。
   - 在左侧导航区域中，选择包含要转换的机器的群集，然后单击 **Machines**（机器）选项卡。
2. 选择要转换的机器，单击 Machines（机器）选项卡顶部的 **Actions**（操作）下拉菜单，然后单击 **Convert to Agent**（转换为代理）。

3. 要将机器重新添加至群集，请选择该机器，然后依次单击 **Summary**（摘要）选项卡、**Actions**（操作）菜单和 **Convert to Node**（转换为节点）。

查看服务器群集信息

查看群集系统信息

要查看群集系统信息：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要查看的群集。
   - 在左侧 **Navigation**（导航）区域中，选择要查看的群集。
2. 单击 **Tools**（工具）选项卡。

   System Information（系统信息）页面显示关于群集的系统详情，如名称、所包含的节点和关联状态，以及 Windows 版本、网络接口信息和卷容量信息。

查看群集事件和警报

有关查看群集中个别机器或节点的事件和警报的信息，请参阅查看事件和警报。

要查看群集事件和警报：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要查看的群集。
   - 在左侧 **Navigation**（导航）区域中的 **Clusters**（群集）下，选择要查看的群集。
2. 单击 **Events**（事件）选项卡。

   一个日志将显示当前任务的所有事件，以及该群集的所有警报。
3. 要筛选事件列表，可以酌情选中或清除 **Active**（活动）、**Complete**（完成）或 **Failed**（失败）复选框。
4. 在 **Alerts**（警报）表中，单击 **Dismiss All**（全部消除）以消除列表中的所有警报。

查看摘要信息

要查看摘要信息，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要查看的群集。
   - 在左侧 **Navigation**（导航）区域中的 **Clusters**（群集）下，选择要查看的群集。
2. 在 **Summary**（摘要）选项卡上，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。

   此选项卡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。
3. 要将此信息刷新为最新信息，请单击 **Actions**（操作）下拉菜单，然后单击 **Refresh Metadata**（刷新元数据）。

   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，请参阅查看机器状态和其他详细信息。

使用群集恢复点

恢复点也称为快照，是指群集上共享卷的文件夹和文件的时间点副本，它们存储在存储库中。恢复点用于恢复受保护的机器或装载到本地文件系统。在 AppAssure 中，可以查看存储库中的恢复点列表。要查看恢复点，请完成以下过程中的步骤。

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。

有关查看群集中个别机器的恢复点的信息，请参阅查看恢复点。

要使用群集恢复点：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要查看其恢复点的群集。
   - 在左侧导航区域中的 **Clusters**（群集）下，选择要查看其恢复点的群集。
2. 单击 **Recovery Points**（恢复点）选项卡。
3. 要查看关于特定恢复点的详细信息，请单击列表中某个恢复点旁的 **>**，以展开视图。
   有关可对恢复点执行的操作的信息，请参阅查看特定恢复点。
4. 选择要装载的恢复点。
   有关如何装载恢复点的信息，请参阅装载 Windows 机器的恢复点，从步骤 2 开始。
5. 要删除恢复点，请参阅移除恢复点。

管理群集的快照

您可通过强制创建快照或暂停创建当前快照来对快照进行管理。通过强制创建快照，可强制当前受保护的群集进行数据传输。强制创建快照时，传输会立即开始，或被添加到队列中。只传输自上个恢复点以来发生更改的数据。如果以前没有恢复点，则传输受保护卷上的所有数据（基本映像）。暂停快照时，将暂时停止当前机器的所有数据传输。

有关对群集中的个别机器强制创建快照的信息，请参阅强制创建快照。有关对群集中的个别机器暂停创建和恢复创建快照的信息，请参阅暂停和恢复保护。

强制创建群集快照

要强制创建群集的快照：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要查看其恢复点的群集。
   - 在左侧导航区域中的 **Clusters**（群集）下，选择要查看其恢复点的群集。
2. 在 **Summary**（摘要）选项卡上，单击 **Actions**（操作）下拉菜单，然后单击 **Force Snapshot**（强制创建快照）。

暂停和恢复创建群集快照

要暂停和恢复创建群集快照：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要查看其恢复点的群集。
   - 在左侧导航区域中的 **Clusters**（群集）下，选择要查看其恢复点的群集。
2. 在 **Summary**（摘要）选项卡上，单击 Actions（操作）下拉菜单，然后单击 **Pause Snapshots**（暂停快照）。
3. 在 **Pause Protection**（暂停保护）对话框中，选择下表中说明的选项之一：

文本框	说明
Pause until resumed（暂停直至恢复）	暂停快照，直至手动恢复保护。要恢复保护，请单击 **Actions**（操作）菜单，然后单击 **Resume**（恢复）。
Pause for（暂停达）	可以按天、小时和分钟指定暂停快照的时间长度。

卸载本地恢复点

要卸载本地恢复点：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要卸载其恢复点的群集
   - 在左侧导航区域中，选择要卸载其恢复点的群集。
2. 在 **Tools**（工具）选项卡的 **Tools**（工具）菜单下，单击 **Mounts**（安装）。
3. 在本地安装列表中，执行以下操作之一：
   - 要卸载一个本地安装，请找到并选择要卸载的恢复点安装，然后单击 **Dismount**（卸载）。
   - 要卸载所有本地安装，请单击 **Dismount All**（全部卸载）按钮。

执行群集和群集节点回滚

回滚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回滚。本部分介绍关于执行群集卷回滚的指南。

对 CCR (Exchange) 和 DAG 群集执行回滚

要对 SCC（Exchange、SQL）群集执行回滚，请执行以下操作：

1. 关闭所有节点，只保留一个。
2. 按照执行回滚和使用命令行执行 Linux 机器的回滚中的说明，使用机器的标准 AppAssure 步骤执行回滚。
3. 回滚结束后，从群集卷装载所有数据库。
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）群集执行回滚

要对 SCC（Exchange、SQL）群集执行回滚，请执行以下操作：

1. 关闭所有节点，只保留一个。
2. 按照执行回滚和使用命令行执行 Linux 机器的回滚中的说明，使用机器的标准 AppAssure 步骤执行回滚。
3. 回滚结束后，从群集卷装载所有数据库。
4. 逐个打开所有其他节点。

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。

复制群集数据

复制群集的数据时，需要在机器层级配置该群集中个别机器的复制。此外，还可以配置为复制共享卷的恢复点；例如，如果有 5 个要从源复制到目标的代理，即可采取此配置。

有关复制数据的更多信息和说明，请参阅复制机器上的代理数据。

从保护范围中移除群集

要从保护范围中移除群集，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要移除的群集；
   - 在左侧导航区域中，选择要移除的群集，以查看 **Summary**（摘要）选项卡。
2. 单击 **Actions**（操作）下拉菜单，然后单击 **Remove Machine**（移除机器）。
3. 选择以下选项之一。

选项	说明
Keep Recovery Points（保留恢复点）	保留当前为此群集存储的所有恢复点。
Remove Recovery Points（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。

从保护范围中移除群集节点

请完成以下过程中的步骤以从保护范围中移除群集节点。如果只要从群集中移除节点，请参阅将受保护群集节点转换为代理。要从保护范围中移除群集节点，

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择包含要移除的节点的群集。在该群集的 **Machines**（机器）选项卡上，选择要移除的节点。
   - 在左侧导航区域中的相关群集下，选择要移除的节点。
2. 单击 **Actions**（操作）下拉菜单，然后单击 **Remove Machine**（移除机器）。
3. 选择下表中说明的选项之一。

选项	说明
Relationship Only（仅关系）	从复制中移除源 Core，但保留已复制恢复点。
With Recovery Points（包括恢复点）	从复制中移除源 Core，并且删除从该机器接收的所有已复制恢复点。

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：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择包含要移除的节点的群集，再单击该群集的 **Machines**（机器）选项卡。
   - 在左侧导航区域中，选择包含要移除的节点的群集，然后单击 **Machines**（机器）选项卡。
2. 单击 **Machines**（机器）选项卡顶部的 **Actions**（操作）下拉菜单，然后单击 **Remove Machines**（移除机器）。
3. 选择下表中说明的选项之一。

选项	说明
Relationship Only（仅关系）	从复制中移除源 Core，但保留已复制恢复点。
With Recovery Points（包括恢复点）	从复制中移除源 Core，并且删除从该机器接收的所有已复制恢复点。

查看群集或节点报告

您可以创建和查看关于群集和个别节点的 AppAssure 活动的符合性和错误报告。这些报告包含关于群集、节点和共享卷的 AppAssure 活动信息。有关 AppAssure 报告的更多信息，请参阅关于报告。

有关报告工具栏中的导出和打印选项的更多信息，请参阅关于报告工具栏。

要查看群集或节点报告，请执行以下操作：

1. 请执行以下操作之一：
   - 在 Core 控制台中，单击 **Machines**（机器）选项卡，然后选择要为其创建报告的群集或节点。
   - 在左侧 **Navigation**（导航）区域中，选择要为其创建报告的群集或节点。
2. 单击 **Tools**（工具）选项卡，然后在 **Reports**（报告）菜单下选择以下选项之一：
   - **符合性报告**
   - **Errors Report（错误报告）**
3. 在 **Start Time**（开始时间）下拉日历中，选择一个开始日期，然后输入报告的开始时间。

   注: 在部署 AppAssure Core 或 AppAssure 代理软件之前，没有可用数据。
4. 在 **End Time**（结束时间）下拉日历中，选择一个结束日期，然后输入报告的结束时间。
5. 单击 **Generate Report**（生成报告）。

   如果报告包括多个页面，则可单击页码或报告结果顶部的箭头按钮来浏览结果。

   报告结果将显示在页面中。
6. 要将报告结果导出为可用格式（PDF、XLS、XLSX、RTF、MHT、HTML、TXT、CSV 或图像）之一，请从下拉列表中选择导出格式，然后执行以下操作之一：
   - 单击第一个 **Save**（保存）图标导出报告并保存到磁盘。
   - 单击第二个 **Save**（保存）图标导出报告并在新 Web 浏览器窗口中显示该报告。
7. 要打印报告结果，请执行下列操作之一：

- 单击第一个 **Printer**（打印机）图标打印整个报告。
- 单击第二个 **Printer**（打印机）图标打印报告的当前页面。

6

报告

关于报告

DL 设备允许生成和查看多个 Core 和代理机器的符合性、错误和摘要信息。

您可以选择联机查看报告、打印报告或者以多种支持的格式之一导出并保存报告。可以选择的格式包括：

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- 图像

关于报告工具栏

为所有报告提供的工具栏可用于通过两种不同方式打印和保存报告。下表介绍了打印和保存选项。

图标	说明
	打印报告
	打印当前页
	导出报告并保存到磁盘
	导出报告并在新窗口中显示 使用此选项可复制、粘贴和通过电子邮件发送 URL，供其他人使用 Web 浏览器查看报告。

关于符合性报告

Core 和 AppAssure 代理提供符合性报告。通过这些报告可以查看所选 Core 或代理执行的作业的状态。失败的作业以红色文本显示。未与代理关联的 Core 符合性报告中的信息为空。

作业的详细信息以列视图显示，包括以下类别：

- Core
- 受保护代理

- 类型
- 摘要
- 状态
- 错误
- 开始时间
- 结束时间
- 时间
- 工作总计

关于错误报告

错误报告是符合性报告的子集，并可用于 Core 和 AppAssure 代理。错误报告仅包含符合性报告中列出的失败作业，并将它们编辑到单个报告中，可供打印和导出。

在列视图中显示有关错误的详情，包括以下类别：

- Core
- 代理
- 类型
- 摘要
- 错误
- 开始时间
- 结束时间
- 所耗时间
- 工作总计

。

关于 Core 摘要报告

Core Summary Report（Core 摘要报告）包含有关所选 Core 上的存储库以及该 Core 所保护的代理的信息。这些信息在一份报告中显示为两个摘要。

存储库摘要

Core Summary Report（Core 摘要报告）的 **Repositories**（存储库）部分包含位于所选 Core 上的存储库的数据。存储库的详细信息以列视图显示，包括以下类别：

- 名称
- Data Path（数据路径）
- Metadata Path（元数据路径）
- Allocated Space（已分配空间）
- Used Space（已用空间）
- Free Space（可用空间）
- Compression/Dedupe Ratio（压缩/重复数据消除率）

代理摘要

Core Summary Report（Core 摘要报告）的 **Agents**（代理）部分包含受所选 Core 保护的所有代理的数据。

代理的详细信息以列视图显示，包括以下类别：

- 名称
- Protected Volumes（受保护卷）
- Total protected space（受保护的总空间）
- Current protected space（当前受保护空间）
- Change rate per day（每天更改率）（**Average**（平均值）、**Median**（中值））
- Jobs Statistic（作业统计）（**Passed**（通过）、**Failed**（失败）、**Canceled**（取消））

生成 Core 或代理报告

要生成 Core 或代理报告，请执行以下操作：

1. 导航至 Core 控制台并选择要运行报告的 Core 或代理。
2. 单击 **Tools**（工具）选项卡。
3. 在 **Tools**（工具）选项卡中，展开左侧导航区域中的 **Reports**（报告）。
4. 在左侧导航区域中，选择要运行的报告。可用报告取决于您在步骤 1 中做出的选择，如下所述。

Machine（机器）	Available Reports（可用报告）
Core	Compliance Report（符合性报告） Summary Report（摘要报告） Errors Report（错误报告）
Agent（代理）	Compliance Report（符合性报告） Errors Report（错误报告）

5. 在 **Start Time**（开始时间）下拉日历中，选择一个开始日期，然后输入报告的开始时间。

   注: 在部署 Core 或代理之前，没有可用数据。
6. 在 **End Time**（结束时间）下拉日历中，选择一个结束日期，然后输入报告的结束时间。
7. 对于 **Core Summary Report**（Core 摘要报告），如果要让 **Start Time**（开始时间）和 **End Time**（结束时间）涵盖 Core 的生存期，请选中 **All Time**（所有时间）复选框。
8. 对于 **Core Compliance Report**（Core 符合性报告）或 **Core Errors Report**（Core 错误报告），请使用 **Target Cores**（目标 Core）下拉列表选择要查看其数据的 Core。
9. 单击 **Generate Report**（生成报告）。

   报告生成后，可以使用工具栏打印或导出报告。

关于 Central Management Console Core 报告

DL 设备允许生成和查看多个 Core 的符合性、错误和摘要信息。在包含本部分介绍的相同类别的列视图中，提供了关于 Core 的详细信息。

从 Central Management Console 生成报告

要从 Central Management Console 生成报告，请执行以下操作：

1. 在 **Central Management Console Welcome**（Central Management Console 欢迎）屏幕中，单击位于右上角的下拉菜单。
2. 在下拉菜单中单击 **Reports**（报告），然后选择以下选项之一：
   - **Compliance Report（符合性报告）**
   - **Summary Report（摘要报告）**
   - **Failure Report（故障报告）**
3. 在左侧导航区域中，选择要为其运行报告的一个或多个 Core。
4. 在 **Start Time**（开始时间）下拉日历中，选择一个开始日期，然后输入报告的开始时间。

   注: 在部署 Core 之前，没有可用数据。
5. 在 **End Time**（结束时间）下拉日历中，选择一个结束日期，然后输入报告的结束时间。
6. 单击 **Generate Report**（生成报告）。

   报告生成后，可以使用工具栏打印或导出报告。

7

完成 DL4300 设备的完全恢复

DL4300 Backup To Disk Appliance 上的数据驱动器位于插槽 0–11 和 14–17 中，并采用 RAID 6 格式，它们最多可承受两个驱动器发生故障，而不会造成数据丢失。操作系统位于驱动器 12 和 13 上，这两个驱动器采用 RAID 1 虚拟磁盘格式。如果这两个磁盘都发生故障，则必须更换驱动器并重新安装必要软件，才能让设备恢复正常运行。要完成设备的完全恢复，必须执行以下操作：

- 为操作系统创建 RAID 1 分区
- 安装操作系统
- 运行 Recovery and Update Utility
- 重新装载卷

为操作系统创建 RAID 1 分区

小心: 请谨记，只能在包含操作系统的 RAID 1 虚拟磁盘上执行这些操作。请勿在包含数据的 RAID 6 虚拟磁盘上执行这些操作。

要创建 RAID 1 分区，请执行以下操作：

1. 确保插槽 12 和 13 中的磁盘是已知正常运行的磁盘。
2. 引导 DL4300 Backup to Disk Appliance。
3. 在引导过程中看到提示时，请按 <Ctrl><R> 组合键。
   此时将显示 **PERC BIOS Configuration Utility**（PERC BIOS 配置公用程序）屏幕。
4. 高亮显示 **VD Management**（VD 管理）选项卡顶部的控制器，然后按 <F2> 键，再选择 **Create New VD**（创建新 VD）。

   注: 如果 RAID-1 OS VD 已存在，则快速初始化 RAID-1 OS VD。
5. 在 **Virtual Disk Management**（虚拟磁盘管理）页面中，为 RAID Level（RAID 级别）选择 RAID 1。
6. 在 **Physical Disks**（物理磁盘）框中选择两个磁盘。

   注: 虚拟磁盘的大小不应超过 278.87 GB。
7. 输入 VD 名称，例如“OS”，将该虚拟磁盘标识为包含操作系统的磁盘。
8. 按 <Tab> 键将光标移动到初始化，然后按 <Enter> 键。

   注: 此阶段执行的初始化为快速初始化。
9. 单击 **OK**（确定）完成选择，或者按两次 <Ctrl><N> 组合键。
   此时将显示 **Ctrl Mgt**（控制管理）页面。
10. 导航至 **Select boot device**（选择引导设备）字段，然后选择包含操作系统的虚拟磁盘。
    此磁盘的容量约为 278 GB。
11. 选择 **Apply**（应用）并按 <Enter> 键。

12. 退出 **PERC BIOS Configuration**（PERC BIOS 配置）公用程序，然后按 <Ctrl><Alt><Del> 组合键重新引导系统。

安装操作系统

在您的设备上使用 Unified Server Configurator - Lifecycle Controller Enabled (USC-LCE) 公用程序来恢复操作系统：

1. 找到操作系统安装介质。
2. 确保您有用于运行该介质的驱动器。

   可以使用 USB 光盘驱动器或虚拟介质设备。通过 iDRAC 支持虚拟介质。有关通过 iDRAC 设置虚拟介质的更多信息，请参阅系统的 iDRAC 设备的用户指南。

   如果安装介质损坏或无法读取，则 USC 可能无法检测到受支持的光盘驱动器。在这种情况下，您可能收到一条错误消息，指出没有可用的光盘驱动器。如果介质无效（例如，CD 或 DVD 已损坏），则会显示一条消息，要求您插入正确的安装介质。
3. 引导系统并在显示 Dell 徽标的 10 秒内按 <F10> 键以启动 USC。
4. 单击左侧窗格中的 **OS Deployment**（操作系统部署）。
5. 单击右侧窗格中的 **Deploy OS**（部署操作系统）。
6. 选择相关操作系统并单击 **Next**（下一步）。

   USC 解压缩所选操作系统需要的驱动程序。驱动程序会解压缩到名为 **OEMDRV** 的内部 USB 驱动器。

   注: 解压缩驱动程序的过程可能需要几分钟。

   注: 18 小时后，将删除“OS Deployment”（操作系统部署）向导复制的所有驱动程序。在复制驱动程序的 18 小时内必须完成操作系统安装。要在 18 小时期间内删除驱动程序，请重新引导系统并按 <F10> 键重新进入 USC。使用 <F10> 键取消操作系统安装或者在重新引导时重新进入 USC，将在 18 小时期间内删除驱动程序。
7. 解压缩驱动程序和在 USC 提示后，插入操作系统安装介质。

   注: 安装 Microsoft Windows 操作系统时，解压的驱动程序会在操作系统安装期间自动安装。

运行 Recovery and Update Utility

要运行 Recovery and Update Utility，请执行以下操作：

1. 从 **dell.com/support** 下载 **Recovery and Update Utility**。
2. 将该公用程序复制到 DL4300 Backup to Disk Appliance 的桌面，并解压缩文件。
3. 双击 **launchRUU**。
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. 当系统显示 **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）。

   Windows Server 角色和功能、ASP .NET MVC3、LSI 提供程序、DL 应用程序、OpenManage Server Administrator 和 AppAssure Core 软件作为 Recovery and Update Utility 的一部分安装。
7. 如果系统再次提示，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）。

   此时将启动 **AppAssure Appliance Recovery**（AppAssure 设备恢复）向导。
9. 完成 AppAssure Appliance Recovery Wizard（AppAssure 设备恢复向导）的 **Collecting Information and Configuring**（收集信息和配置）阶段中的步骤，然后单击 **Next**（下一步）。

开始 **Disk Recovery**（磁盘恢复）阶段。

10. 查看关于 AppAssure 服务将被关闭的警告后，单击 **Next**（下一步）。
    将还原存储库以及所有虚拟待机机器的虚拟磁盘，并重新启动 AppAssure 服务。恢复即完成。

8

手动更改主机名

建议在初始配置 DL4300 Backup to Disk Appliance 期间选择一个主机名。如果以后使用 **Windows System Properties（Windows 系统属性）**更改主机名，则必须手动执行以下步骤，以确保新主机名生效并且设备正常工作：

1. 停止 AppAssure Core 服务
2. 删除 AppAssure Server 证书
3. 删除 Core Server 和注册表项
4. 更改 AppAssure 中的显示名称
5. 在 Internet Explorer 中更新可信站点

停止 Core 服务

要停止 AppAssure Core 服务，请执行以下操作：

1. 打开 **Windows Server Manager**。
2. 在左侧的导航树中，选择 **Configuration（配置）→ Services（服务）。**
3. 右键单击 **AppAssure Core Service**（AppAssure Core 服务），然后选择 **Stop**（停止）。

删除服务器证书

要删除 AppAssure Server 证书，请执行以下操作：

1. 打开命令行界面。
2. 键入 **Certmgr** 并按 <Enter> 键。
3. 在 **Certificate Manager**（证书管理器）窗口中，选择 **Trusted Root Certification Authorities（受信任根认证机构）→ Certificates（证书）**。
4. 删除其 **Issue To**（颁发目标）列中显示旧主机名并且 **Intended Purpose**（目标用途）列显示 **Server Authentication**（服务器验证）的证书。

删除 Core Server 和注册表项

要删除 Core Server 和注册表项，请执行以下操作：

1. 打开命令行界面。
2. 键入 **regedit** 并按 <Enter> 键以打开注册表编辑器。
3. 在导航树中，导航至 **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery** 并打开 Core 目录。
4. 删除 **webServer** 和 **serviceHost** 目录。

使用新主机名启动 Core

要使用您手动创建的新主机名启动 Core，请执行以下操作：

1. 启动 AppAssure Core 服务。
2. 右键单击桌面上的 **AppAssure 5 Core** 图标，然后单击 **Properties**（属性）。
3. 使用新 `<server name:8006>` 替换旧服务器名称。
   例如，**https://<servername:8006/apprecovery/admin/Core**。
4. 单击 **OK**（确定），然后使用 **AppAssure 5 Core** 图标启动 AppAssure Core 控制台。

更改显示名称

要更改显示名称，请执行以下操作：

1. 以管理员身份登录 **AppAssure Console**（AppAssure 控制台）。
2. 选择 **Configuration**（配置）选项卡，然后单击 **General**（常规）栏中的 Change（更改）按钮。
3. 输入新 **Display Name**（显示名称），然后单击 **OK**（确定）。

在 Internet Explorer 中更新可信站点

要在 Internet Explorer 中更新可信站点，请执行以下操作：

1. 打开 Internet Explorer。
2. 如果未显示 **File**（文件）、**Edit**（编辑）、View（查看）及其他菜单，请按 <F10> 键。
3. 单击 **Tools**（工具）菜单并选择 **Internet Options**（Internet 选项）。
4. 在 **Internet Options**（Internet 选项）窗口中，单击 **Security**（安全）选项卡。
5. 单击 **Trusted Sites**（可信站点），然后单击 **Sites**（站点）。
6. 在 **Add this website to the zone**（将该网站添加到区域）中，输入 **https://[Display Name]**，为 Display Name 使用您提供的新名称。
7. 单击 **Add**（添加）。
8. 在 **Add this website to the zone**（将该网站添加到区域）中，输入 **about:blank**。
9. 单击 **Add**（添加）。
10. 单击 **Close**（关闭），然后单击 **OK**（确定）。

9

附录 A — 脚本处理

关于 PowerShell 脚本处理

Windows PowerShell 是与 Microsoft .NET Framework 相连的环境，旨在实现管理自动化。AppAssure 包括用于 PowerShell 脚本处理的完整客户端软件开发工具包 (SDK)，管理员可通过利用脚本执行命令来实现 AppAssure 资源的自动化管理。

它允许具有管理权限的用户在指定情况下（例如，创建快照、执行可附加性检查和可安装性检查前后等）执行用户提供的 PowerShell 脚本。管理员可同时从 AppAssure Core 和代理执行脚本。脚本可接受参数，且脚本输出将写入 Core 和代理日志文件。

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**。

注: 在使用和执行 AppAssure 脚本之前，必须安装和配置 Windows PowerShell。

PowerShell 脚本处理的前提条件

在对 AppAssure 使用和执行 PowerShell 脚本之前，必须安装 Windows PowerShell 2.0。

注: 确保将 **powershell.exe.config** 文件放入 PowerShell 主目录。例如 **C:\WindowsPowerShell \powershell.exe**。

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_ise**。此外，还需要将配置文件 **powershell_ise.exe.config** 添加至配置文件 **powershell.exe.config** 所在的同一文件夹。

注: 配置文件 **powershell_ise.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。

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。

注: 脚本文件必须具有与示例脚本文件相同的名称。

表. 5: AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

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; }`	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。
`public Priority Priority { get; set; }`	获取或设置传输请求的优先级。
`public int MaxRetries { get; set; }`	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。
`public Guid ProviderId{ get; set; }`	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。
`public Collection<ExcludedWriter>ExcludedWriterIds { get; set; }`	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。此名称仅用于说明文件，不必与编写器的实际名称完全相同。
`public ushort TransferDataServerPort { get; set; }`	获取或设置包含 TCP 端口的值，此端口用于接收来自 Core 的连接，以便从代理向 Core 进行数据的实际传输。代理将尝试侦听此端口，但如果此端口正在使用，代理可改用不同端口。Core 所使用的端口号在每个已快照卷的 `VolumeSnapshotInfo` 对象的 `BlockHashesUri` 和 `BlockDataUri` 属性中指定。
`public TimeSpan SnapshotTimeout { get; set; }`	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。
`public TimeSpan TransferTimeout { get; set; }`	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。
`public TimeSpan NetworkReadTimeout { get; set; }`	获取或设置与此传输相关的网络读取操作超时。

方法	说明
`public TimeSpan NetworkWriteTimeout { get; set; }`	获取或设置与此传输相关的网络写入操作超时。

表. 6: BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

方法	说明
`public Guid AgentId { get; set; }`	获取或设置代理 ID。
`public bool IsNightlyJob { get; set; }`	获取或设置表示后台作业是否为每夜作业的值。
`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。

ExportJobRequest (namespace Replay.Core.Contracts.Export)

从参数 `BackgroundJobRequest` 继承其值。

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 VirtualMachineLocation Location { get; set; }`	获取或设置此导出的目标位置。这是抽象基类。
`public VolumeImageIdsCollection VolumeImageIds { 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。

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

从参数 `BackgroundJobRequest` 继承其值。

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

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。

方法	说明
public VolumeNameCollection VolumeNames { get; set; }	获取或设置用于传输的卷名称集合。
public ShadowCopyType ShadowCopyType { get; set; }	获取或设置用于传输的复制类型。可用值：Unknown（未知）、Copy（复制）和 Full（满）。
Public AgentTransferConfiguration TransferConfiguration { get; set; }	获取或设置传输配置。
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	获取或设置存储配置。
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 ForceBaseImage { get; set; }	获取或设置表示是否强制创建基本映像的值。
public bool IsLogTruncation { get; set; }	获取或设置表示作业日志是否截断的值。

表. 7: TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

方法	说明
public VolumeNameCollection VolumeNames { get; set; }	获取或设置用于传输的卷名称集合。
public ShadowCopyType ShadowCopyType { get; set; }	获取或设置用于传输的复制类型。可用值：Unknown（未知）、Copy（复制）和 Full（满）。
public AgentTransferConfiguration TransferConfiguration { get; set; }	获取或设置传输配置。
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	获取或设置存储配置。
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 ForceBaseImage { get; set; }	获取或设置表示是否强制执行基本映像的值。
public bool IsLogTruncation { get; set; }	获取或设置表示作业日志是否截断的值。
public uint LatestEpochSeenByCore { get; set; }	获取或设置最新的日期值。
public Guid SnapshotSetId { get; set; }	获取或设置 VSS 分配给此快照的 GUID。

方法	说明
`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。

表. 8: TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

方法	说明
`public VolumeNameCollection VolumeNames { get; set; }`	获取或设置用于传输的卷名称集合。
`public ShadowCopyType ShadowCopyType { get; set; }`	获取或设置用于传输的复制类型。可用值：`Unknown`（未知）、`Copy`（复制）和 `Full`（满）。
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	获取或设置传输配置。
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	获取或设置存储配置。
`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 ForceBaseImage { get; set; }`	获取或设置表示是否强制执行基本映像的值。
`public bool IsLogTruncation { get; set; }`	获取或设置表示作业日志是否截断的值。
`public uint LatestEpochSeenByCore { get; set; }`	获取或设置最新的日期值。

表. 9: VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

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 Method { get; set;}`	获取或设置 VM 名称。

VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

从参数 `System.Collections.ObjectModel.Collection<string>` 继承其值。

表. 10: VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

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。

方法	说明
	注: .NET 4.0 WCF (**https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312**)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。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。

方法	说明
`public override bool Equals(object obj)`	确定此实例与某个同样为 `VolumeNameCollection` 对象的指定对象是否具有相同值。（覆盖 `Object.Equals(Object)`。）
`public override int GetHashCode()`	返回此 `VolumeNameCollection` 的哈希代码。（覆盖 `Object.GetHashCode()`。）

表. 11: VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

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。

Pretransferscript.ps1

PreTransferScript 在传输快照前于代理端执行。

```
# 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 在传输快照后于代理端执行。

```
 # 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 端执行。

```
# 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.StorageConfiguration
}
```

Postexportscript.ps1

PostExportScript 在任何导出作业后于 Core 端执行。

注: 如果在初始启动后对导出的代理执行一次 **PostExportScript**，则无输入参数。常规代理将此脚本作为 **PostExportScript.ps1** 包含在 PowerShell 脚本文件夹中。

```
# 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 端执行。此脚本具有 **$JobClassName** 参数，有助于分别处理那些子作业。

```
 # 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 'AgentId:'
$NightlyAttachabilityJobRequestObject.AgentId;
                            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 'AgentId:' $RollupJobRequestObject.AgentId;
                    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 'AgentId:'
$ChecksumCheckJobRequestObject.AgentId;
                                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 端执行。此脚本具有 **$JobClassName** 参数，有助于分别处理那些子作业。

```
 # 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 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
                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 'AgentId:' $RollupJobRequestObject.AgentId;
                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 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                        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.Id;
                        echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
                }
                break;
        }
}
```

示例脚本

以下示例脚本旨在帮助具有管理权限的用户执行 PowerShell 脚本。

示例脚本包括：

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

10

获得帮助

查找说明文件和软件更新

在 AppAssure Core 控制台中有指向 AppAssure、设备说明文件和软件更新的直接链接。要访问这些链接，请单击 **Appliance（设备）**选项卡，然后单击 **Overall Status（总体状态）**。指向软件更新和说明文件的链接位于 **Documentation（说明文件）**部分下。

联系 Dell

注: 如果没有活动的 Internet 连接，您可以在购货发票、装箱单、帐单或 Dell 产品目录上查找联系信息。

Dell 提供多种联机和基于电话的支持和服务选项。如果您不能连接至 Internet，则可以在您的购买发票、装箱单、帐单或 Dell 产品目录中找到联系信息。具体的服务随您所在国家/地区以及产品的不同而不同，某些服务在您所在的地区可能不提供。要联系 Dell 了解销售、技术支持或客户服务问题，请访问 **software.dell.com/support**。