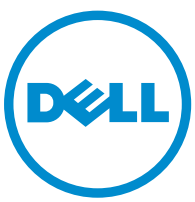
Dell DL1000 设备
用户指南



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 DL1000 简介

Dell DL1000 将备份和复制组合到统一数据保护产品中。它提供基于备份的可靠应用程序数据恢复，以保护虚拟机和物理机。您的设备可以利用内置的全局重复数据消除、压缩、加密和复制到特定私有云或公共云基础结构来处理多达数 TB 的数据。可在数分钟内恢复服务器应用程序和数据，以用于数据保留 (DR) 和符合性用途。

DL1000 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。

Dell DL1000 核心技术

该设备结合了以下技术：

- 实时恢复
- 通用恢复
- 真正全局重复数据消除
- Encryption（加密）

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。该技术能够让您几乎不间断地访问虚拟服务器或物理服务器上的数据卷。

DL1000 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。您可以通过装载恢复点恢复服务器的使用，而无需等待完全还原到生产存储。

通用恢复

通用恢复可提供无限的机器还原灵活性。您可以将备份从物理系统还原到虚拟机，从虚拟机还原到虚拟机，从虚拟机还原到物理系统，或从物理系统还原到物理系统，以及执行裸机还原到不同硬件。

通用恢复技术还可加快虚拟机之间的跨平台移动。例如，从 VMware 移动到 Hyper-V，反之亦然。它嵌入在应用程序级别、项目级别和对象级别恢复中（单个文件、文件夹、电子邮件、日历项目、数据库和应用程序）。

真正全局重复数据消除

真正全局重复数据消除通过对机器执行增量块级备份来消除冗余或重复数据。

典型的服务器磁盘布局包括操作系统、应用程序和数据。在大多数环境中，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版本，以便进行有效的部署和管理。跨多台机器执行块级备份时，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 1: 真正全局重复数据消除的图表

加密

DL1000 提供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，确保数据隐私。使用加密密钥可以访问和解密数据。快照数据加密采用线速内联方式，不会对性能造成影响。

Dell DL1000 数据保护功能

Dell DL1000 Core

Core 是 DL1000 部署架构的中心组件。Core 存储和管理机器备份，并提供备份、恢复、保留、复制、存档和管理服务。Core 是自包含网络的可寻址计算机，运行 Microsoft Windows Server 2012 R2 Foundation 和 Standard 操作系统的 64 位版本。设备对接收自代理的数据执行基于目标的内联压缩、加密和重复数据消除。然后 Core 将快照备份存储在存储库中，而存储库位于设备上。Core 之间进行复制配对。

存储库驻留在 Core 的内部存储中。通过从启用 JavaScript 的 Web 浏览器访问以下 URL 来管理 Core：**https://CORENAME:8006/apprecovery/admin**。

Dell DL1000 Smart Agent

Smart Agent 安装在受 Core 保护的机器上。Smart Agent 可跟踪磁盘卷上变更的块，然后以预定义的保护间隔创建变更块的映像快照。采用不断进行增量块级快照的方法可避免将受保护机器上的相同数据重复复制到 Core。

配置代理后，代理将使用智能技术跟踪受保护磁盘卷上变更的块。当快照就绪时，系统将使用基于套接字的智能多线程连接将其迅速传输到 Core。

快照流程

当基本映像从受保护的机器传输到 Core 时，便会开始 DL1000 保护流程。在此阶段，机器的完整副本将在正常操作下跨网络传输，然后将不断传输增量快照。DL1000 Agent for Windows 使用 Microsoft 卷影复制服务

(VSS) 来冻结和停顿磁盘上的应用程序数据，从而捕获文件系统一致且应用程序一致的备份。创建快照后，目标服务器上的 VSS 编写器会阻止将内容写入磁盘。停止向磁盘写入内容时，所有磁盘 I/O 操作将进行排队，快照完成之后才会恢复，同时会完成正在进行的操作并关闭所有打开的文件。创建卷影副本的过程对生产系统的性能无明显影响。

在创建快照之前，DL1000 使用 Microsoft VSS 将数据刷新到磁盘，这是因为后者内置了对所有 Windows 内部技术（例如 NTFS、注册表、Active Directory）的支持。此外，其他企业级应用程序（例如 Microsoft Exchange 和 SQL）使用 VSS 编写器插件来获取关于正在准备快照的通知，以及需要将其已使用的数据库页面刷新到磁盘的通知，从而使数据库保持一致的事务处理状态。捕获的数据将迅速传输并存储到 Core 上。

复制 - 灾难恢复站点或服务提供商

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。该过程要求两个或多个 Core 之间具有成对的“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提供商。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。

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。首次复制可以使用外部介质将数据播种到目标 Core。通常情况下，这对大型数据集或具有慢速链接的站点来说非常有用。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。在目标 Core 使用种子存档后，将自动同步新复制的增量恢复点。

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，DL1000 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。

恢复即服务

托管服务提供商 (MSP) 可以充分利用 DL1000，将其作为一种交付恢复即服务 (RaaS) 的平台。RaaS 通过复制客户的物理和虚拟服务器来加快实现云中恢复。服务提供商的云被用作虚拟机来为恢复测试或实际恢复操作提供支持。希望执行云中恢复的客户可以配置从本地 Core 上的受保护机器到 AppAssure 服务提供商的复制。如果发生灾难，MSP 可以立即为客户启动虚拟机。

DL1000 并非多租户。MSP 可以在多个站点使用 DL1000，并在自己一方创建多租户环境。

虚拟化和云

DL1000 Core 可直接用于云，使您可以利用云的计算能力进行恢复和存档。

DL1000 可以将任何受保护或已复制的机器导出至经过许可的 VMware 或 Hyper-V 版本。如果连续导出，虚拟机会在每次快照后进行增量更新。增量更新非常迅速，并且提供一键启动的待机克隆功能。支持的虚拟机导出包括：

- VMware Workstation 或 Server 文件夹
- 直接导出至 vSphere 或 VMware ESXi 主机
- 导出至 Oracle VirtualBox
- Windows Server 2008 (x64) 上的 Microsoft Hyper-V Server
- Windows Server 2008 R2 上的 Microsoft Hyper-V Server
- Windows Server 2012 R2 上的 Microsoft Hyper-V Server

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

Dell DL1000 部署架构

DL1000 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称为“代理”的受保护机器。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。DL1000 Core 使用基本映像和增量快照来编辑受保护代理的恢复点。

此外，DL1000 具有应用程序感知功能，因为它能检测是否存在 Microsoft Exchange 和 SQL 及其相应的数据库和日志文件。备份通过使用应用程序感知型块级快照来执行。DL1000 可针对受保护的 Microsoft Exchange 服务器执行日志截断。

下图显示了一个简单的 DL1000 部署。DL1000 代理安装在文件服务器、电子邮件服务器、数据库服务器等机器上，或安装在连接到单个 DL1000 Core（包含中央存储库）并为其提供保护的虚拟机上。Dell 软件许可证门户管理环境中的代理和 Core 的许可证订用、组和用户。许可证门户允许用户登录、激活帐户、下载软件和按照环境中的许可证来部署代理和 Core。

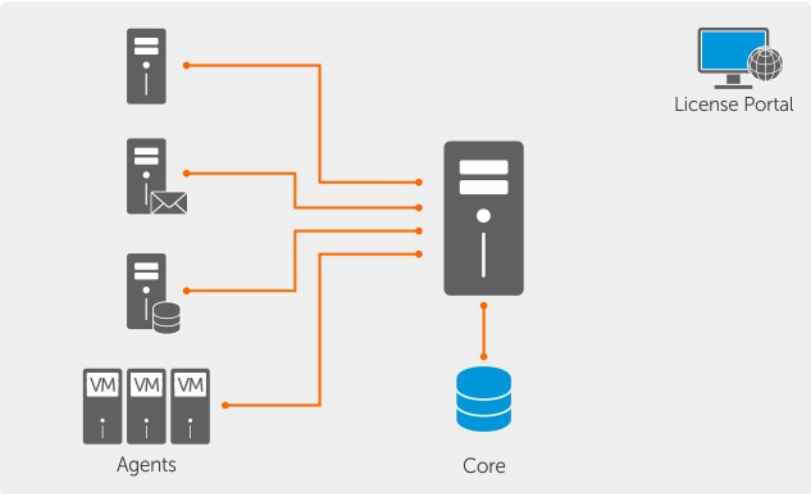


图 2: Dell DL1000 部署架构

也可以按照下图中的显示部署多个 DL1000 Core。中央控制台可管理多个 Core。

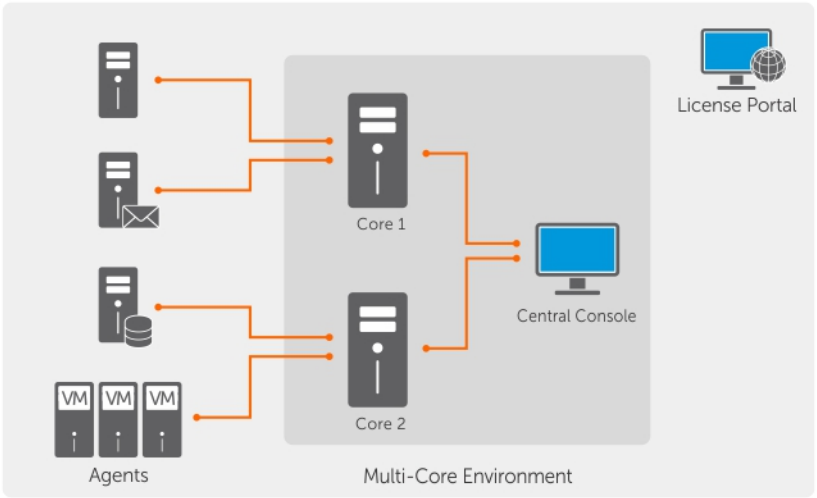


图 3: DL1000 多 Core 部署架构

您可能需要的其他信息

注: 有关所有 Dell OpenManage 文档，请访问 **dell.com/openmanagemanuals**。

注: 请经常访问 **dell.com/support/home** 以获得更新，并首先阅读这些更新，因为这些更新通常会取代其他说明文件中的信息。

注: 有关任何 Dell OpenManage Server Administrator 的相关文档，请参阅 **dell.com/openmanage/manuals**。

您的产品文档包括：

使用入门指南	提供系统功能、设置系统和技术规范的概述。此说明文件也已随系统附带。
系统安装说明	提供有关如何针对 AppAssure 解决方案设置硬件和安装软件的信息。
用户手册	提供有关系统功能的信息，并说明如何排除系统故障以及如何安装或更换系统组件。
部署指南	提供有关硬件部署和设备初始部署的信息。
用户指南	提供关于配置和管理系统的信息。
发行说明	提供有关 Dell DL1000 设备的产品信息和其他信息。
互操作性指南	提供有关 DL1000 设备支持的软件和硬件的信息，以及使用注意事项、建议和规则。
OpenManage Server Administrator 用户指南	提供有关使用 Dell OpenManage Server Administrator 管理您的系统的信息。
资源介质	系统随附的介质提供了用于配置和管理系统的说明文件和工具，包括与操作系统、系统管理软件、系统更新以及随系统购买的系统组件相关的说明文件和工具。

2

使用 DL1000

访问 DL1000 Core 控制台

要访问 DL1000 Core 控制台，请执行以下操作：

1. 更新浏览器中的可信站点。
2. 配置浏览器以远程访问 DL1000 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 DL1000 Core 控制台，请执行以下操作之一：
   - 从本地登录到 DL1000 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 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）**。

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）。

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。

管理许可证

您可以直接从 Core 控制台管理 DL1000 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 Dell AppAssure 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

- 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
- 许可证限制

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，选择 **Configuration（配置）** → **Licensing（许可）**。
   随即会显示 **Licensing**（许可）页面。
2. 在 **License Details（许可证详细信息）**页面中，单击 **Change（更改）**。
   此时将显示 **Change License Key**（更改许可证密钥）对话框。
3. 在 **Change License Key**（更改许可证密钥）对话框中，输入新许可证密钥并单击 **OK**（确定）。

联系许可证门户服务器

Core 控制台联系门户服务器以更新在许可证门户中做出的更改。与门户服务器之间的通信按指定间隔自动进行；但是，您可以按需发起通信。
要联系门户服务器，请执行以下操作：

1. 导航至 Core 控制台，然后单击 **Configuration（配置）** → **Licensing**（许可）。
   随即会显示 **Licensing**（许可）页面。
2. 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: 在设备的初始配置过程中，建议选择一个永久显示名称。如果以后更改该名称，则必须手动执行数个步骤来确保新主机名生效且设备正常工作。

要更改 Core 显示名称，请执行以下操作：

1. 导航至 Core 控制台，单击 **Configuration（配置）→ Settings（设置）**。
2. 在 **General（常规）**部分中，单击 **Change（更改）**。
   此时将显示 **Display Name**（显示名称）对话框。
3. 在 **Display Name（显示名称）**文本框中，输入 Core 的新显示名称。
4. 单击**确定**。

更改每夜作业时间

“每夜作业”选项为受 Core 保护的代理计划前滚、可附加性和截断作业。
要调整每夜作业时间，请执行以下操作：

1. 导航至 Core 控制台，然后选择 **Configuration（配置）→ Settings（设置）**。
2. 在 **Nightly Jobs（每夜作业）**部分中，单击 **Change（更改）**。
   此时将显示 **Nightly Jobs**（每夜作业）对话框。
3. 在 **Nightly Jobs Time（每夜作业时间）**文本框中，输入新的开始时间。
4. 单击**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，单击 **Configuration（配置）→ Settings（设置）**。
2. 在 **Transfer Queue（传输队列）**部分中，单击 **Change（更改）**。
   此时将显示 **Transfer Queue**（传输队列）对话框。
3. 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。
4. 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。
5. 单击**确定**。

调整客户端超时设置

客户端超时设置指定在连接到客户端时，服务器在超时之前等待的秒数或分钟数。
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，然后单击 **Configuration（配置）→ Settings（设置）**。
2. 在 **Client Timeout Settings Configuration（客户端超时设置配置）**部分中，单击 **Change（更改）**。
   此时将显示 **Client Timeout Settings**（客户端超时设置）对话框。
3. 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。
4. 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。
5. 单击**确定**。

配置清除重复高速缓存设置

全局重复数据消除可减少备份数据所需的磁盘存储空间量。Deduplication Volume Manager (DVM) 将一组存储位置组合到单个存储库中。重复数据消除高速缓存保存对唯一数据块的引用。默认情况下，重复数据消除高速缓存为 1.5 GB。如果冗余信息量过多导致重复数据消除高速缓存填满，则存储库无法继续充分利用重复数据消除来处理新添加的数据。在这种情况下，您可以通过在 Core 控制台中更改重复数据消除高速缓存配置来增加重复数据消除高速缓存的大小。

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，单击 **Configuration（配置）** → **Settings（设置）**。
2. 在 **Deduplication Cache Configuration（重复数据消除高速缓存配置）**部分中，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。
3. 在 **Primary Cache Location（主要高速缓存位置）**文本框中，输入更新的主要高速缓存位置。
4. 在 **Secondary Cache Location（次要高速缓存位置）**文本框中，输入更新的次要高速缓存位置。
5. 在 **Metadata Cache Location（元数据高速缓存位置）**文本框中，输入更新的元数据高速缓存位置。
6. 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，单击 **Configuration（配置）** → **Settings（设置）**。
2. 在 **Replay Engine Configuration（Replay 引擎配置）**部分中，单击 **Change（更改）**。
   此时将显示 **Replay Engine Configuration**（Replay 引擎配置）对话框。
3. 在 **Replay Engine Configuration（Replay 引擎配置）**对话框中，指定 **IP address（IP 地址）**。选择以下选项之一：
   - 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 IP Address（使用特定 IP 地址）**。
4. 根据下面的说明输入配置信息：

文本框	说明
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。
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。

文本框	说明
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。

5. 选择 **No Delay**（无延迟）。
6. 单击**确定**。

修改部署设置

要修改部署设置，请执行以下操作：

1. 导航至 Core 控制台，然后依次单击 **Configuration（配置）**选项卡和 **Settings（设置）**。
2. 在 **Deploy Settings（部署设置）**窗格中，单击 **Change（更改）**。
   此时将显示 **Deploy Settings（部署设置）**对话框。
3. 在 **Agent Installer Name（代理安装程序名称）**文本框中，输入代理可执行文件的名称。默认为 Agentweb. exe。
4. 在 **Core Address（Core 地址）**文本框中，输入 Core 的地址。
5. 在 **Failed Receive Timeout（接收失败超时）**文本框中，输入无活动超时的等待分钟数。
6. 在 **Max Parallel Installs（最大并行安装数）**文本框中，输入可以并行安装的最大安装数。
7. 选择以下一项或全部两项可选设置：
   - Automatic reboot after install（安装之后自动重新引导）
   - Protect After Deploy（部署后保护）
8. 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，单击 **Configuration（配置）→ Settings（设置）**。
2. 在 **Database Connection Settings（数据库连接设置）**部分中，执行以下操作之一：
   - 要还原默认配置，请单击 **Restore Default（恢复默认值）**。
   - 要修改数据库连接设置，请单击 **Change（更改）**。

   单击更改后，将显示 **Database Connection Settings（数据库连接设置）**对话框。
3. 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
Host Name（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。

文本框	说明
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。

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

管理事件

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、服务器设置、已启用的跟踪日志、云配置、减少重复和事件保留。

使用 Notification Groups（通知组）选项可以管理通知组，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）
  - Licensing（许可）
  - Log Truncation（日志截断）
  - Archive（存档）
  - Core Service（Core 服务）
  - Export（导出）
  - Protection（保护）
  - Replication（复制）
  - Rollback（回滚）
- 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 控制台中，选择 **Configuration（配置）→ Events（事件）**。
2. 单击 **Add Group**（添加组）。
   此时将打开 **Add Notification Group（添加通知组）**对话框，并显示两个面板：
   - **启用警报**
   - **Notification Options（通知选项）**

启用警报

使用 Enabling Alerts（启用警报）可以定义要记录的系统事件集、创建报告和设置警报。

注: 要为所有事件创建警报，请选择 **All Alerts（所有警报）**。

- 要创建特定于错误、警告、通知消息或其组合的警报，请选择以下选项之一：
  - 红色三角形图标（错误）
  - 黄色三角形图标（警告）
  - 蓝色圆形（信息）
  - 曲线箭头（恢复默认值）
- 要为特定事件创建警报，请单击相关组旁边的 **>** 符号，然后选中复选框以启用警报。

配置通知选项

1. 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。可以按如下所示输入多个不同的电子邮件地址以及密送和抄送地址： • **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 事件日志报告警报通知，则选择此选项。
Notify by sys logd（通过系统日志通知）	如果要通过 sys logd 报告警报，则选择此选项。在以下文本框中输入 sys logd 的详细信息： • **Hostname:（主机名：）** • **Port:1（端口：1）**

文本框	说明
Notify by Toast alerts（通过弹出式警报通知）	如果您要警报以弹出窗口的形式出现在屏幕右下角，则选择此选项。

2. 单击**确定**。

   将显示以下消息：**The Group name cannot be changed after the creation of the Notification Group. are you sure you want to use this name?**（在创建通知组后无法更改组名称，是否确定要使用此名称？）。

   - 要保存组名称，请单击 **Yes（是）**。
   - 要更改组名称，请单击 **No（否）**。返回 **Notification Options（通知选项）**窗口，更新组名称及其他通知组设置，然后保存更改。

配置电子邮件服务器

注: 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，才能发送电子邮件警报消息。

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 控制台中，单击 **Configuration（配置）→ Events（事件）**。
2. 在 **Email Settings（电子邮件设置）**窗格中，单击 **SMTP server（SMTP 服务器）**。

   此时将显示 **SMTP Server Settings（SMTP 服务器设置）**对话框。
3. 按如下所示输入电子邮件服务器的详细信息：

文本框	说明
SMTP Server（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**。
From（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**。
Username（用户名）	输入电子邮件服务器的用户名。
Password（密码）	输入用于访问电子邮件服务器的密码。
Port（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。
Timeout (seconds)（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。 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。

4. 单击 **Send Test Email（发送测试电子邮件）**，执行以下步骤：
   a. 在 Send Test Email（发送测试电子邮件）对话框中，输入测试邮件的目标电子邮件地址，然后单击 **Send（发送）**。

b. 如果测试邮件失败，则退出错误对话框和 **Send Test Email（发送测试电子邮件）**对话框，然后修改您的电子邮件服务器配置设置。重复步骤 4。
c. 单击 **OK（确定）**以确认。
d. 验证是否已发送测试电子邮件消息。
e. 返回 SMTP Server Settings（SMTP 服务器设置）对话框，单击 **Save（保存）**以关闭对话框并保存您的设置。

配置电子邮件通知模板

要接收有关事件的电子邮件通知，必须配置电子邮件服务器和电子邮件通知模板。

注: 要接收电子邮件警报消息，请配置通知组设置，并启用 **Notify by email**（通过电子邮件通知）选项。

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 控制台中，单击 **Configuration（配置）→ Events**（事件）。
2. 在 **Email Settings**（电子邮件设置）窗格中，单击 **Change**（更改）。
   此时将显示 **Edit Email Notification Configuration**（编辑电子邮件通知配置）对话框。
3. 选择 **Enable email notifications**（启用电子邮件通知），然后按如下所示输入电子邮件服务器的详细信息：

文本框	说明
Email Subject（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>`。
Email（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。

4. 单击 **Send Test Email**（发送测试电子邮件），执行以下步骤：
   a. 在 Send Test Email（发送测试电子邮件）对话框中，输入测试邮件的目标电子邮件地址，然后单击 **Send**（发送）。
   b. 如果测试邮件失败，则退出错误对话框和 Send Test Email（发送测试电子邮件）对话框，单击 **OK（确定）**以保存当前的电子邮件模板设置，然后修改您的电子邮件服务器设置，请参阅配置电子邮件服务器和电子邮件通知模板。确保重新输入该电子邮件帐户的密码。保存设置，然后返回步骤 4。
   c. 单击 **OK**（确定）以确认。
   d. 验证是否已发送测试电子邮件消息。
   e. 返回 **Edit Email Notification Configuration**（编辑电子邮件通知配置）对话框，单击 **OK**（确定）以关闭对话框并保存设置。

配置减少重复

要配置减少重复，请执行以下操作：

1. 在 Core 控制台中，单击 **Configuration（配置）→ Events（事件）**。
2. 在 **Repetition Reduction（减少重复）**部分中，单击 **Change（更改）**。
   此时将显示 **Enable Repetition Reduction（启用减少重复）**对话框。
3. 选中 **Enable Repetition Reduction**（启用减少重复）。
4. 在 **Store events for（事件存储期限）**文本框中，输入存储减少重复事件的分钟数。
5. 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 控制台中，单击 **Configuration（配置）→ Settings（设置）**。
2. 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。
3. 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）。
4. 单击**保存**。

管理存储库

存储库用于存储从受保护工作站和服务器捕获的快照。DL1000 已预配置存储库。存储库可以驻留在系统的内部存储中。

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。

查看存储库详情

要查看存储库详情，请执行以下操作：

1. 在 Core 控制台中，单击 **Configuration（配置）→ Repositories（存储库）**。
2. 单击您要查看其详情的存储库的 **Status**（状态）列旁的 **>**。
3. 存储库的详细信息包括存储位置和统计信息。存储位置详细信息包括元数据路径、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）- 包括速率 (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)。

检查存储库

Core 控制台可以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. 单击 **Configuration（配置）→ Repositories（存储库）**。
2. 单击 **Actions（操作）**按钮下的 Compression Ratio（压缩比率）列旁边的 Settings（设置）图标。
3. 单击 **Check（检查）**。
   此时将显示 **Check Repository**（检查存储库）对话框。
4. 在 **Check Repository**（检查存储库）对话框中，单击 **Check**（检查）。

注: 执行检查时，与此存储库关联的所有活动任务将被取消。在检查开始之前，会显示一条消息，要求您确认继续检查。建议重建恢复点高速缓存。检查失败将导致需要从存档还原存储库。

管理安全性

DL1000 提供了强大的加密功能。通过加密，他人将无法访问受保护机器的备份。只有拥有加密密钥的用户可以访问和解密数据。加密不会影响性能。关键安全性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、修改和删除在 Core 上配置的加密密钥。

添加加密密钥

要添加加密密钥，请执行以下操作：

1. 在 Core 控制台中，单击 **Configuration（配置）→ Security（安全性）**。
2. 从 **Actions（操作）**下拉菜单中，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。
3. 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
Name（名称）	输入加密密钥的名称。
Description（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。
Passphrase（密码短语）	输入密码短语。此密码短语用于控制访问。
Confirm Passphrase（确认密码短语）	重新输入密码短语。这用于确认输入的密码短语。

4. 单击**确定**。

小心: 建议保护密码短语。丢失密码短语会导致无法恢复数据。

编辑加密密钥

要编辑加密密钥，请执行以下操作：

1. 在 Core 控制台中，单击 **Configuration（配置）→ Security（安全性）**。
   此时将显示 **Encryption Keys**（加密密钥）屏幕。
2. 在要编辑的加密密钥的名称旁，单击 **>**，然后单击 **Edit**（编辑）。
   此时将显示 **Edit Encryption Key**（编辑加密密钥）对话框。
3. 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。
4. 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. 在 Core 控制台中，单击 **Configuration（配置）→ Security（安全性）**。
2. 在要编辑的加密密钥的名称旁，单击 **>**，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。
3. 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。
4. 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. 在 Core 控制台中，单击 **Configuration（配置）→ Security（安全性）**。
2. 从 **Actions（操作）**下拉菜单中单击 **Import（导入）**。
   此时将显示 **Import Key**（导入密钥）对话框。
3. 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）。
4. 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. 在 Core 控制台中，单击 **Configuration（配置）→ Security（安全性）**。
2. 在您要导出的加密密钥的 Configuration（配置）下拉菜单中，选择 **Export（导出）**。
   此时将显示 **Export Key**（导出密钥）对话框。
3. 在 **Export Key（导出密钥）**对话框中，单击 **Save File（保存文件）**以便在安全位置保存并存储加密密钥。
4. 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. 在 Core 控制台中，单击 **Configuration（配置）→ Security（安全性）**。
2. 在您要移除的加密密钥的 Configuration（配置）下拉菜单中，选择 **Remove（移除）**。
   此时将显示 **Remove Key（移除密钥）**对话框。
3. 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。

云类型	文本框	说明
	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。

监测 DL1000

可以使用 **Overall Status（总体状态）**页面上的 **Appliance（设备）**选项卡监测 DL1000 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）页面还提供工具链接，可深入查看每个子系统的详细信息，有助于对警告或错误进行故障排除。**System Administrator** 链接适用于设备硬件和存储硬件子系统，可提示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/manuals** 的 *OpenManage Server Administrator User's Guide*（OpenManage Server Administrator 用户指南）。

升级 DL1000

注: Dell 建议您使用安装程序从 Dell 许可证激活门户下载最新可用的 AppAssure 版本。

注: 对于其他软件升级，您将收到升级到最新版本的通知。

修复 DL1000

注: 开始修复过程之前，确保停止 Core 服务。

快速设备自行恢复

快速设备自行恢复 (RASR) 是一种裸机还原流程，将操作系统驱动器重建为默认出厂映像。
要执行 RASR，请执行以下操作：

注: Dell 建议您在设置设备之后创建 RASR USB 闪存盘。要创建 RASR USB 闪存盘，请参阅创建 RASR USB 闪存盘部分。

1. 插入已创建的 RASR USB 闪存盘。
2. 通过 RASR USB 闪存盘重新引导设备。
3. 单击 **Rapid Appliance Self Recovery（快速设备自行恢复）**。

将会显示欢迎屏幕。

4. 单击**下一步**。

   此时将显示 **Prerequisites check（前提条件检查）**屏幕。

   注: 在执行 RASR 之前，请务必检查所有硬件及其他前提条件。

5. 单击**下一步**。

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

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

6. 选择 **Factory Reset（恢复出厂设置）**选项。

   此选项将从出厂映像恢复操作系统磁盘。

7. 单击**下一步**。

   此时将显示 **Storage Configuration（存储配置）**屏幕。

8. 在 **OS Recovery（操作系统恢复）**屏幕中，在对话框中显示以下警告消息：`This operation will recover the operating system. All OS disk data will be overwritten.`（此操作将恢复操作系统。所有操作系统磁盘数据将被覆盖）。

9. 单击**是**。

   操作系统磁盘开始恢复为出厂设置。

10. 单击**完成**。

创建 RASR USB 闪存盘

注: 软件初始设置完成后，将自动启动 **AppAssure Appliance Configuration Wizard**（AppAssure 设备配置向导）。**Appliance**（设备）选项卡状态图标为黄色。

要创建 RASR USB 闪存盘，请执行以下操作：

1. 导航至 **Appliance**（设备）选项卡。
2. 在左侧导航窗格中选择 **Appliance（设备）→ Backup**（备份）。

   此时将显示 **Create RASR USB Drive**（创建 RASR USB 驱动器）窗口。

   注: 在尝试创建 RASR 闪存盘之前，先插入 16 GB 或更大的 USB 闪存盘。

3. 插入 16 GB 或更大的 USB 闪存盘后，单击 **Create RASR USB Drive now**（立即创建 RASR USB 驱动器）。

   此时将显示 **Prerequisite Check**（前提条件检查）消息。

   检查前提条件后，**Create the RASR USB Drive**（创建 RASR USB 驱动器）窗口将显示创建 USB 驱动器所需的最小大小以及 **List of Possible target paths**（可用目标路径列表）。

4. 选择目标并单击 **Create**（创建）。

   此时将显示警告对话框。

5. 单击 **Yes**（是）。

   将创建 RASR USB 驱动器闪存盘。

6. **注:** 请确保使用“安全移除 USB 驱动器”或“Windows 弹出驱动器”功能以准备移除 USB 闪存盘。否则，USB 闪存盘中的内容可能会损坏并且 USB 闪存盘将无法按预期正常工作。

   卸下闪存盘，贴上标签并存放以供将来使用。

3

保护工作站和服务器

关于保护工作站和服务器

要使用 DL1000 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: 在本章中，*机器*一词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。

部署代理（推送安装）

DL1000 允许将 AppAssure 代理安装程序部署到要保护的单个 Windows 机器。完成以下步骤可将安装程序推送到代理。要同时将代理部署到多个机器，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 控制台的左侧导航区域中，单击 **Protected Machines（受保护机器）**。
2. 单击 **Actions（操作）** → **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。
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。
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**。

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 AppAssure 代理软件才能受到保护。可以选择在此步骤之前安装 AppAssure 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。要在保护机器的过程中安装 AppAssure 代理软件，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. 重新引导安装了 AppAssure 代理软件的机器（如果尚未执行此操作）。
2. 在 Core 机器上的 Core 控制台中，单击按钮栏上的 **Protect（保护）** → **Protect Machine（保护机器）**。

   此时将显示 **Protect Machine Wizard（保护机器向导）**。
3. 在 **Welcome（欢迎）**页面中，选择相应的安装选项：
   - 如果不需要定义存储库或建立加密，请选择 **Typical（典型）**。
   - 如果您以后不想看到 **Protect Machine Wizard（保护机器向导）**的 **Welcome（欢迎）**页面，请选中 **Skip this Welcome page the next time the wizard opens（下次向导打开时跳过此欢迎页面）**选项。
4. 单击 **Next（下一步）**。
5. 在 **Connection（连接）**页面中，根据下表中的说明输入有关要连接的机器的信息。

文本框	说明
Host（主机）	要保护的机器的主机名或 IP 地址。
Port（端口）	AppAssure 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。
Username（用户名）	用于连接此机器的用户名，例如 administrator。
Password（密码）	用于连接至此机器的密码。

6. 单击 **Next（下一步）**。如果在 **Protect Machine Wizard（保护机器向导）**中接下来显示 **Protection（保护）**页面，则跳转至步骤 7。

   注: 如果在 **Protect Machine Wizard（保护机器向导）**中接下来显示 **Install Agent（安装代理）**页面，则表示在指定的机器上尚未安装代理软件。单击 **Next（下一步）**以安装代理软件。必须在您要保护的机器上安装代理软件，再重启该机器，然后才能将其备份到 Core。要让安装程序重新引导代理机器，请选中 **After installation, restart the machine automatically (recommended)（安装后自动重启机器 [推荐]）**选项，然后单击 **Next（下一步）**。
7. 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。
8. 选择相应的保护计划：
   - 要使用默认保护计划，请在 **Schedule Settings（计划设置）**选项中选中 **Default protection (3 hour snapshots of all volumes)（默认保护 [每 3 小时为所有卷创建快照]）**。对于默认保护计划，Core 将

每隔 3 小时为代理机器创建一次快照。最短可以每小时为代理机器创建一次快照。要在关闭该向导后随时更改保护设置，包括选择要保护哪些卷，请转到特定代理机器的 Summary（摘要）选项卡。

- 要定义不同的保护计划，请在 **Schedule Settings（计划设置）**选项中选择 **Custom protection（自定义保护）**。

9. 选择以下选项之一：
   - 如果在 **Protect Machine Wizard（保护机器向导）**中选择了 Typical（典型）配置，则单击 **Finish（完成）**以确认您的选择，关闭向导，并保护您指定的机器。
   - 首次为机器添加保护时，在您定义的计划后会将基本映像（即受保护卷中的所有数据的快照）传输至 AppAssure Core 上的存储库，除非您指定初始暂停保护。
   - 如果选择了 **Protect Machine Wizard（保护机器向导）**的 Typical（典型）配置并指定了自定义保护，则单击 **Next（下一步）**以设置自定义保护计划。有关定义自定义保护计划的详情，请参阅“创建自定义保护计划”。
   - 如果选择了 **Protect Machine Wizard（保护机器向导）**的 Advanced（高级）配置和默认保护，则单击 **Next（下一步）**，然后前进到步骤 12 以查看存储库和加密选项。
   - 如果选择了 **Protect Machine Wizard（保护机器向导）**的 Advanced（高级）配置并指定了自定义选项，则单击 **Next（下一步）**并前进到步骤 10 以选择要保护的卷。
10. 在 **Protection Volumes（保护卷）**页面中，选择代理机器上的要保护的卷。如果列出了任何不想纳入保护的卷，则在 Check（选中）列中单击以清除选择。然后单击 **Next（下一步）**。

    注: 建议保护系统保留卷和包含操作系统的卷（通常为 C 驱动器）。
11. 在 **Protection Schedule（保护计划）**页面中，定义自定义保护计划。
12. 在 **Repository（存储库）**页面中，选择 **Use an existing repository（使用现有存储库）**。
13. 单击 **Next（下一步）**。

    此时将显示 **Encryption（加密）**页面。
14. （可选）要启用加密，请在 **Encryption（加密）**页面中选择 **Enable Encryption（启用加密）**。

    在 **Encryption（加密）**页面中将显示 **Encryption key（加密密钥）**字段。

    注: 如果启用加密，将应用至此代理机器上的所有受保护卷中的数据。以后可以通过 Core 控制台中的 **Configuration（配置）**选项卡更改设置。

    小心: AppAssure 在密码块链 (CBC) 模式中使用 AES 256 位加密和 256 位密钥。虽然使用加密是可选的，但是 Dell 强烈建议您建立加密密钥，并保护您定义的密码短语。请将密码短语保存在安全位置，因为它对于数据恢复至关重要。如果没有密码短语，将无法进行数据恢复。
15. 按下表所述输入信息，以添加 Core 的加密密钥。

文本框	说明
Name（名称）	输入加密密钥的名称。
Description（说明）	输入说明以提供加密密钥的附加详情。
Passphrase（密码短语）	输入用于控制访问的密码短语。
Confirm Passphrase（确认密码短语）	重新输入刚输入的密码短语。

16. 单击 **Finish（完成）**以保存并应用设置。

    首次为机器添加保护时，在您定义的计划后会将基本映像（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。

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。

要暂停保护，请执行以下操作：

1. 在 Core 控制台中，单击左侧导航区域中的 **Protected Machines（受保护机器）**下拉菜单。
2. 为您要暂停保护的机器选择 **Pause Protection（暂停保护）**。

   此时将显示 **Pause Protection（暂停保护）**对话框。
3. 选择以下选项之一，然后单击 **OK（确定）**。
   - 如果要暂停保护直至显式恢复，则选择 **Pause until resumed（暂停直至恢复）**。
   - 要在指定期间暂停保护，请选择 **Pause for（暂停期间）**，然后在 Days（天）、Hours（小时）和 Minutes（分钟）控件中键入或选择相应的暂停期间。

   注: 要恢复保护，请从 **Protected Machines（受保护机器）**下拉菜单中选择 **Resume Protection（恢复保护）**。

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. 在左侧导航窗格中单击 **Protected Machines**（受保护机器）。
2. 单击 **Actions（操作）** → **Deploy Agent**（部署代理）。

   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。
   - **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。
   - **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。默认选中此选项。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。
   - **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。
   - **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。
   - **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。

了解保护计划

保护计划定义何时将备份从受保护代理机器传输至 AppAssure Core。

最初使用 **Protect Machine Wizard（保护机器向导）**或 **Protect Multiple Machines Wizard（保护多个机器向导）**定义保护计划。然后可以随时从特定代理机器的 Summary（摘要）选项卡修改现有计划。

AppAssure 提供默认保护计划，并定义了两个保护期间。第一个期间是平日（周一至周五），定义了单个时间段（从 12:00 AM 至 11:59 PM）。默认间隔（两个快照间隔的时间段）为 3 小时。第二个期间是周末（周六和周日）。第二个期间的默认间隔为 3 小时。

首次启用保护时，会激活该计划。因此，如果使用默认设置，无论当前处于一天中的任何时间，首次备份将每隔 3 小时进行。

保存至 Core 的首次备份传输称为基本映像快照。所有指定卷上的所有数据（包括操作系统、应用程序和设置）均保存到 Core 中。此后，增量快照（较小的备份，仅包含代理至上次备份以来发生更改的数据）将基于所定义的间隔定期保存到 Core 中。

您可以创建自定义计划以更改备份频率。例如，可以将平日期间的间隔更改为 60 分钟，从而每小时创建一次快照。也可以将周末的间隔从 60 分钟延长至 180 分钟，从而在流量较低时，每 3 小时创建一次快照。

Protection Schedule Wizard（保护计划向导）页面中的其他选项包括每日保护时间设置。此设置可在每天的定义期间内创建单个备份（默认设置为 12:00 PM）。

初始暂停保护的选项可在您显式恢复保护之前阻止创建基本映像（实际上会阻止所有备份）。在您准备好开始基于已建立的保护计划保护机器时，必须显式恢复保护。

创建自定义计划

1. 在 **Protect Machine Wizard**（保护机器向导）或 **Protect Multiple Machines Wizard**（保护多个机器向导）的 **Protection Schedule**（保护计划）页面中，要更改任意期间的间隔计划，请执行以下操作：
   a. 选择 **Periods**（期间）。

      将显示现有期间并且可以修改。可编辑字段包括各期间的开始时间、结束时间和间隔（分钟）。
   b. 单击间隔字段，并输入相应的间隔（分钟）。

      例如，高亮度显示现有间隔，将其值替换为 **60**，以在此期间内每隔 60 分钟执行快照。
2. 要为平日创建高峰和非高峰期间，请更改平日期间的时间范围，使其不包括 24 小时期间，设置高峰的最佳间隔，选择 **Take snapshots for the remaining time**（为其余时间创建快照），然后通过执行以下操作设置非高峰间隔：
   a. 选择 **Periods**（期间）。

      将显示现有期间并且可以修改。
   b. 单击 **From**（从）框以更改此期间的开始时间。

      此时将显示 **Choose Time**（选择时间）对话框。
   c. 将 Hours（小时）和 Minutes（分钟）滑块相应地拖移至所需的开始时间，然后单击 **Done**（完成）。要指定当前时间，请单击 **Now（现在）**。
   d. 单击 **To**（至）框以更改此期间的结束时间。

      此时将显示 **Choose Time**（选择时间）对话框。
   e. 将 Hours（小时）和 Minutes（分钟）滑块相应地拖移至所需的开始时间，然后单击 **Done**（完成）。要指定当前时间，请单击 **Now**（现在）。

3. 要为每天发生的单个备份设置一天中的单一时间，请选择 **Daily protection time**（每天保护时间），然后以 HH:MM AM 格式输入时间。
4. 要定义计划而不开始备份，请选择 **Initially pause protection**（初始暂停保护）。

   从向导暂停保护后，将保持暂停至您显式恢复为止。在您恢复保护后，将根据您建立的计划执行备份。
5. 单击 **Finish**（完成）或 **Next**（下一步）。

修改保护计划

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，选择包含您想要更改的已定义保护计划的机器。

   此时将显示该机器的 Summary（摘要）选项卡。
2. 选择要更改的受保护机器的卷，然后单击 **Set a schedule（设置计划）**。要一次选择所有卷，请单击标题行中的复选框。

   最初，所有卷共享同一保护计划。通常情况下，最佳做法是至少保护系统保留卷和包含操作系统的卷（通常是 C 驱动器）。

   此时将显示 **Protection Schedule**（保护计划）对话框。
3. 在 **Protection Schedule（保护计划）**对话框中，如果以前创建了保护计划模板并且想要将其应用到此代理，则从下拉列表中选择模板，然后转到步骤 9。
4. 如果要将此新保护计划保存为模板，则在文本框中输入模板名称。
5. 如果要从计划中移除现有时间期间，则清除每个时间期间选项旁边的复选框。包括以下选项：
   - **Mon - Fri.（周一 - 周五）**：此时间范围表示典型的五天工作周。
   - **Sat - Sun.（周六 - 周日）**：此时间范围表示典型的周末。
6. 如果平日的开始时间和结束时间为 12:00 AM 至 11:59 PM，则存在单个期间。要更改已定义期间的开始时间和结束时间，请执行以下操作：
   a. 选择相应的时间期间。
   b. 单击 **Start Time（开始时间）**框以更改此期间的开始时间。
   c. 将 Hours（小时）和 Minutes（分钟）滑块相应地拖移至所需的开始时间，然后单击 **Done（完成）**。要指定当前时间，请单击 **Now（现在）**。
   d. 单击 **End Time（结束时间）**框以更改此期间的结束时间。

      此时将显示 **Choose Time（选择时间）**对话框。
   e. 将 Hours（小时）和 Minutes（分钟）滑块相应地拖移至所需的开始时间，然后单击 **Done（完成）**。要指定当前时间，请单击 **Now（现在）**。
   f. 根据您的要求更改间隔。例如，如果定义高峰期间，则将间隔从 60 分钟更改为 20 分钟，以便每小时创建三次快照。
7. 如果您在步骤 6 中定义了 12:00 AM 至 11:59 PM 以外的期间，然后您希望在其余时间范围内执行备份，则必须通过执行以下操作来添加附加期间以定义保护：
   a. 单击 **+ Add period（+ 添加期间）**。

      在相应的类别（平日或周末）下，将显示新的时间期间。如果第一个期间的开始时间晚于 12:00 AM，则 AppAssure 会在 12:00 自动开始此期间。按照上述示例，此第二个期间从 12:00 AM 开始。您可能需要调整开始时间和结束时间的小时或分钟。
   b. 按照所需的开始时间和结束时间，相应地拖移 Hours（小时）和 Minutes（分钟）滑块控件。
   c. 根据您的需求更改间隔。例如，如果定义非高峰期间，则将间隔从 60 分钟更改为 120 分钟，以便每两小时创建一次快照。
8. 如果需要，继续创建其他期间，并设置相应的开始时间、结束时间和间隔。

注: 如果要移除已添加的期间，请单击该期间最右端的 **X**。如果您错误地移除了某个期间，可以单击 **Cancel（取消）**。

9. 当保护计划符合您的要求后，单击 **Apply（应用）**。

   Protection Schedule（保护计划）对话框将关闭。

配置受保护机器设置

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. 在 Core 控制台中，导航至要修改的机器。
2. 单击 **Configuration（配置）→ Settings（设置）**。
3. 单击 **Change**（更改）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 使用默认端口 8006 与此机器通信。
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。
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。 **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。

查看机器的系统信息

在 Core 控制台中显示所有受保护机器。

要查看机器的系统信息，请执行以下操作：

1. 在 Core 控制台的左侧导航区域中，在 **Protected Machines（受保护机器）**下选择机器以查看详细系统信息。
2. 单击 **Tools**（工具）选项卡。

   System Information（系统信息）选项卡显示以下内容：

   - Host Name（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：

- Name（名称）
- Device ID（设备 ID）
- File System（文件系统）
- Capacity（容量）（包括 Raw [原始]、Formatted [格式化] 和 Used [已用]）

显示的其他机器信息包括：

- Processors（处理器）
- Network Adapters（网络适配器）
- IP Addresses associated with this machine（与此机器关联的 IP 地址）

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. 在导航窗格中选择要查看的机器。
2. 单击 **Configuration（配置）** → **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: 更改传输设置会对您的 AppAssure 环境产生重大影响。在修改传输设置值之前，请参阅 Dell AppAssure 知识库中的 Transfer Performance Tuning Guide（传输性能调节指南）。

DL1000 中有三种传输类型：

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。
还原	此过程将在受保护的机器上还原备份信息。

DL1000 中的数据传输涉及通过从 AppAssure 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，导航至要修改的机器。
2. 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 **Transfer Settings（传输设置）**页面。
3. 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。
4. 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。

文本框	说明
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） • 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。

5. 单击**确定**。

存档数据

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 **Tools（工具）** → **Archive（存档）** → **Create**（创建）。

此时将显示 **Add Archive Wizard**（添加存档向导）对话框。

2. 在 **Add Archive Wizard**（添加存档向导）的 **Create**（创建）页面中，从 **Location Type**（位置类型）下拉列表中选择以下选项之一：
   - 本地
   - 网络
   - 云
3. 根据您在步骤 3 中选择的位置类型，输入存档的详细信息，如下表所述。

表. 2: 创建存档

选项	文本框	说明
本地	输出位置	输入输出的位置。它用于定义您希望存档驻留的位置路径；例如：d:\work\archive。
网络	输出位置	输入输出的位置。它用于定义您希望存档驻留的位置路径；例如：\\servername\sharename。
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络路径的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。 **注:** 要选择云帐户，必须首先将其添加到 Core 控制台中。请参阅添加云帐户。
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	输入将保存存档数据的文件夹的名称。默认名称为 AppAssure-5-Archive-[创建日期]-[创建时间]

4. 单击 **Next**（下一步）。
5. 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。
6. 单击 **Next**（下一步）。
7. 在 **Options**（选项）页面中，输入下表所述信息。

文本框	说明
Maximum Size（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，选择您希望保留用于创建存档的最大空间量： • 选择 Entire Target（整个目标）以保留在步骤 4 中指定的目标所提供路径中的所有可用空间。（例如，如果位置为 D:\work\archive，则保留 D：驱动器上的所有可用空间。） • 选择空白文本框，使用向上和向下箭头输入数量，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。

文本框	说明
	注: Amazon 云存档会自动划分为 50 GB 分段。Windows Azure 云存档会自动划分为 200 GB 分段。
Recycle action（循环操作）	选择以下回收操作选项之一： • **Do not reuse**（不重用）：不覆盖或清除此位置的任何现有存档数据。如果此位置为空，则存档写入将失败。 • **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）：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。
注释	输入捕获存档所需的附加信息。在您以后导入该存档时将显示注释。
Use compatible format（使用兼容格式）	选择此选项可使用与以前版本的 Core 兼容的格式存档数据。 **注:** 新格式提供更出色的性能；但是与旧版 Core 不兼容。

8. 单击 **Next**（下一步）。
9. 在 Date Range（日期范围）页面中，输入要存档的恢复点的 Start Date（开始日期）和 Expiration Date（过期日期）。
   - 要输入时间，请单击所显示的时间（默认为 8:00 AM）以显示用于选择小时和分钟的滑动条。
   - 要输入日期，请单击文本框以显示日历，然后单击所需日期。
10. 单击 **Finish**（完成）。

导入存档

要导入存档，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools（工具）→ Archive（存档）→ Import**（导入）。
2. 对于 **Location Type**（位置类型），从下拉列表中选择以下选项之一：
   - 本地
   - 网络
   - 云
3. 根据您在步骤 3 中选择的位置类型，输入存档的详细信息，如下表所述。

表. 3: 导入存档

选项	文本框	说明
本地	输出位置	输入输出的位置。此选项用于定义存档所在的位置路径；例如 `d:\work\archive`ea.
网络	输出位置	输入输出的位置。它用于定义您希望存档驻留的位置路径；例如：\\servername\sharename。

选项	文本框	说明
	用户名	输入用户名。用于建立网络共享的登录凭据。
	密码	输入网络路径的密码。用于建立网络共享的登录凭据。
云	帐户	从下拉列表中选择帐户。 **注:** 要选择云帐户，必须首先将其添加到 Core 控制台中。请参阅添加云帐户。
	容器	从下拉菜单中选择与您的帐户关联的容器。
	文件夹名称	输入将保存存档数据的文件夹的名称。默认名称为 AppAssure-5-Archive-[创建日期]-[创建时间]

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。

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。

查看系统诊断程序

在 AppAssure 中提供了诊断信息，以供您查看任何受保护机器的机器日志数据。此外，您可以查看和上载 Core 的诊断信息。

查看机器日志

如果机器发生错误或问题，查看日志可能有助于进行故障排除。

要查看机器日志，请执行以下操作：

1. 在 Core 控制台中，单击 **Tools（工具）→ Diagnostics（诊断）→ View Log（查看日志）**。
   此时将显示 **Download Core Log（下载 Core 日志）**页面。
2. 选择 **Click here to begin the download（单击此处开始下载）**。
   此时会显示一条消息，提示您打开或保存该文件。

3. 选择您希望采用的处理日志文件的方法。

上载机器日志

1. 导航至 Core 控制台，单击 **Tools（工具）** → **Diagnostics（诊断）** → **Upload Log（上载日志）**。
   显示**上载日志**页面。
2. 选择 **Click here to begin the upload（单击此处开始上载）**。
   此时将显示 Events（事件）选项卡，可供查看 Core 和所有受保护机器的日志信息的上载进度。

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。您可以取消某个当前快照或取消所有当前操作，其中包括导出和复制。
要取消机器上的操作，请执行以下操作：

1. 在 Core 控制台中，选择要取消其操作的机器。
2. 在 **Events（事件）**中，展开要取消的事件或操作的事件详细信息。
3. 单击 **Cancel（取消）**。

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 控制台中，导航至要查看的受保护机器。

在 **Summary**（摘要）页面上将显示关于该机器的信息。显示的详细信息包括以下内容：

- 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：

- Name（名称）
- File System type（文件系统类型）
- Space Usage（空间使用情况）
- Current Schedule（当前计划）
- Next Snapshot（下一个快照）
- 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：

- Online status（联机状态）
- Name（名称）
- Install Path（安装路径）
- Version（版本）

如果机器上安装了 Exchange Server，还将显示关于服务器和邮件存储区的详细信息，其中包括：

- Version（版本）
- Install Path（安装路径）
- Data Path（数据路径）
- 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 AppAssure 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: 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。您可以从许可证门户下载 Core 和代理更新。

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，请执行以下操作：

1. 在 Core 控制台中，单击 **Events（事件）** → **Alerts**（警报）。
2. 导航至 AppAssure Core Home（主页）选项卡，然后单击 **Events**（事件）选项卡。

   在列表中会显示警报事件，包括事件触发时间和消息。对于每个成功的代理软件部署，您将看到一个警报，指示已添加受保护机器。
3. （可选）单击任意受保护机器的链接。

   此时将显示所选机器的 Summary（摘要）选项卡，其中显示以下相关信息：
   - 受保护机器的主机名
   - 最后一个快照（如果适用）
   - 下一个快照的计划时间（根据您选择的保护计划）
   - 剩余时间
   - 此受保护代理所使用的加密密钥（如果有）
   - 代理软件的版本

保护多个机器

将 AppAssure 代理软件批量部署到 Windows 机器后，必须对机器进行保护以保护其数据。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 **Protect（保护）** → **Bulk Protect（批量保护）**。

   此时将显示 **Protect Multiple Machines Wizard（保护多个机器向导）**窗口。
2. 选择相应的安装选项：
   - 如果不需要定义存储库或建立加密，请选择 **Typical（典型）**。
   - 如果您以后不想看到 Protect Machine Wizard（保护机器向导）的 Welcome（欢迎）页面，请选中 **Skip this Welcome page the next time the wizard opens（下次向导打开时跳过此欢迎页面）**。
3. 单击 **Next（下一步）**。

   此时将显示 **Connection（连接）**页面。
4. 通过单击以下选项之一来添加要保护的机器。
   - 单击 **Active Directory** 以指定 Active Directory 域上的机器。根据下表中的说明输入凭据，然后单击 **Next（下一步）**。
   - 单击 **vCenter/ESXi** 以指定 vCenter/ESXi 虚拟主机上的虚拟机。根据下表中的说明输入凭据，然后单击 **Next（下一步）**。

文本框	说明
Host（主机）	Active Directory 域或 VMware vCenter Server/ESX(i) 虚拟主机的主机名或 IP 地址。
Username（用户名）	输入用于连接此机器的用户名；例如，Administrator。

文本框	说明
Password（密码）	输入用于连接此机器的安全密码。

- 要手动添加机器，请选择 **Add the machines manually（手动添加机器）**，然后单击 **Next（下一步）**。

5. 在 **Machines（机器）**页面中，要手动指定机器，请在单个行中输入每个机器的以下连接详细信息，然后单击 **Next（下一步）**。`hostname::username::password::port`
6. 在 **Machines（机器）**页面中，要指定从 Active Directory 域 VMware vCenter/ESX(i) 虚拟主机确定的机器，请从列表中选择要保护的每个相应机器，然后单击 **Next（下一步）**。

   系统自动验证您添加的每个机器，然后显示 **Protection（保护）**页面。
7. 在 **Protection（保护）**页面中，选择相应的保护计划：
   - 要使用默认保护计划，请在 **Schedule Settings（计划设置）**选项中选择 **Default protection (hourly snapshots of all volumes)（默认保护 [每小时为所有卷创建快照]）**。
   - 要定义不同的保护计划，请在 Schedule Settings（计划设置）选项中选择 **Custom protection（自定义保护）**，然后单击 **Next（下一步）**。
8. 继续按如下所示进行配置：
   - 如果在 **Protect Multiple Machines Wizard（保护多个机器向导）**中选择了 Typical（典型）配置，则单击 **Finish（完成）**以确认您的选择，关闭向导，并保护您指定的机器。
   - 如果在 **Protect Multiple Machines Wizard（保护多个机器向导）**中选择了 Typical（典型）配置并指定了自定义保护，则单击 **Next（下一步）**，然后设置自定义计划。
   - 如果在 Protect Machine Wizard（保护机器向导）中选择了 Advanced（高级）配置，则单击 **Next（下一步）**，然后继续执行步骤 9 以查看存储库和加密选项。
9. 在 **Repository（存储库）**页面中，选择 **Use an existing repository（使用现有存储库）**。
10. 单击 **Next（下一步）**。

    此时将显示 **Encryption（加密）**页面。
11. 要启用加密，请在 **Encryption（加密）**页面中选择 **Enable Encryption（启用加密）**。

    在 **Encryption（加密）**页面中将显示 Encryption key（加密密钥）字段。

    注: 如果启用加密，将应用至您指定要保护的机器上的所有受保护卷的数据。以后可以通过 Core 控制台中的 **Configuration（配置）**选项卡更改设置。有关加密的更多信息，请参阅管理安全性。
12. 按下表所述输入信息，以添加 Core 的加密密钥。

文本框	说明
Name（名称）	输入加密密钥的名称。
Description（说明）	输入说明以提供加密密钥的附加详情。
Passphrase（密码短语）	输入用于控制访问的密码短语。
Confirm Passphrase（确认密码短语）	重新输入刚输入的密码短语。

13. 单击 **Finish（完成）**以保存并应用设置。

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。

要监测多个机器的保护，请导航至 Core 控制台 Home（主页）选项卡，然后单击 **Events（事件）**。

Events（事件）选项卡显示任务、警报和事件。传输卷时，在 Tasks（任务）窗格中显示状态、开始时间和结束时间。还可以按状态（活动、等待中、已完成和失败）筛选任务。

在添加各个受保护机器时，系统将记录一个警报，指示操作是否成功或是否已记录错误。

4

恢复数据

管理恢复

AppAssure Core 可立即从恢复点执行到物理机或虚拟机的数据还原或机器恢复。恢复点包含从数据块级别捕获的代理卷快照。这些快照具有应用程序感知功能，表示在创建快照前，所有打开的事务和滚动事务日志均已完成，同时高速缓存已刷新到磁盘。通过将应用程序感知快照与验证的恢复配合使用，可使 Core 执行多种类型的恢复，包括：

- 恢复文件和文件夹
- 使用实时恢复来恢复数据卷
- 使用实时恢复来恢复 Microsoft Exchange Server 和 Microsoft SQL Server 的数据卷
- 使用通用恢复进行裸机还原
- 使用通用恢复裸机还原到不同硬件
- 临时和持续导出至虚拟机

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，选择要查看其恢复点的机器，然后选择 **Recovery Points**（恢复点）。
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）选项可以将所选恢复点导出到 ESXi、VMware Workstation 或 HyperV。 **Restore**（还原）- 选择此选项可以执行从所选恢复点到所指定卷的还原。
目录	对于展开恢复点中的每个卷，Contents（内容）区域包含一行，其中列出每个卷的以下信息： **Status**（状态）指示恢复点的当前状态。 **Title**（标题）列出恢复点中的特定卷。 **Size**（大小）显示存储库中恢复点所使用的空间量。

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，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。
2. 选择 **Recovery Points**（恢复点）选项卡。
3. 在恢复点列表中，单击 **>** 以展开要装载的恢复点。
4. 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。
5. 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。

6. 单击 **Mount**（装载）以装载恢复点。

卸载所选恢复点

要卸载所选恢复点，请执行以下操作：

1. 导航至 Core 控制台，单击 **Tools（工具）→ Mounts（装载）**。
2. 在 **Local Mounts（本地装载）**页面中，单击要卸载的恢复点的装载点旁边的 **Dismount（卸载）**。
3. 在 Dismounting the Recovery Point（卸载恢复点）窗口中，单击 **Yes（是）**以确认。

卸载所有恢复点

要卸载所有恢复点，请执行以下操作：

1. 导航至 Core 控制台，单击 **Tools（工具）→ Mounts（装载）**。
2. 在 **Local Mounts（本地装载）**页面中，单击 **Dismount All（全部卸载）**。

3. 在 **Dismounting the Recovery Point（卸载恢复点）**窗口中，单击 **Yes（是）**以确认。

为 Linux 机器装载恢复点

使用 AppAssure 中的 **aamount** 公用程序可以从远程将恢复点中的卷装载为 Linux 机器上的本地卷。

1. 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 装载提示符中，输入以下命令以列出受保护的机器：**lm**。
5. 看到提示时，输入 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 AppAssure 服务器保护的机器的列表。使用以下信息标识每个机器：行项目号、主机/IP 地址和机器的 ID 号。例如：293cc667-44b4-48ab-91d8-44bc74252a4f。
7. 输入以下命令以列出可用于指定机器的恢复点：**lr <line_number_of_machine>** 。
8. 输入以下命令以选择并在指定的装载点/路径中装载所指定的恢复点：**m <volume_recovery_point_ID_number> <path>** 。
9. 要验证装载是否成功，请输入以下命令以列出已连接的远程卷：**l**

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基本映像。有关强制创建基本映像的更多信息，请参阅强制创建快照。

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。

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，选择具有要强制快照的恢复点的机器或群集。
2. 单击 **Volumes（卷）**部分中的 **Summary（摘要）**选项卡，然后选择下述选项之一：
   - **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。

还原数据

使用 AppAssure 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。

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。

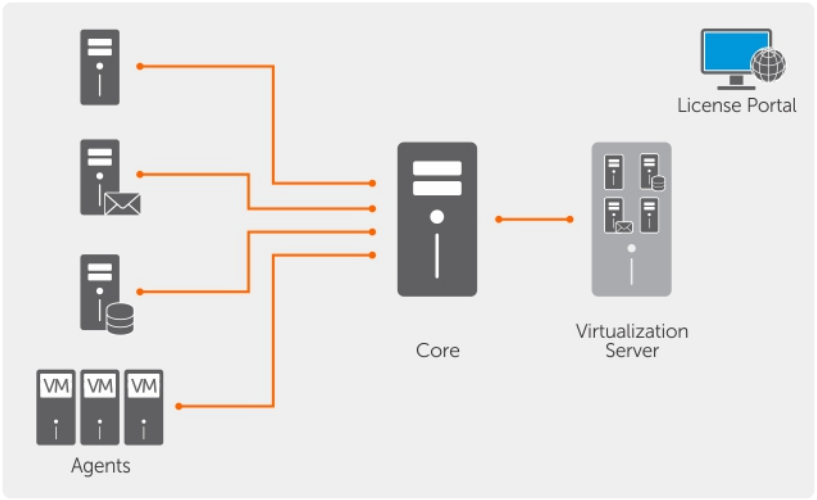


图 4: 将数据导出到虚拟机

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

Dell 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。简单动态卷不进行分条、镜像或跨越卷。

在导出向导中无法选择动态磁盘（如前所述，不包括简单动态磁盘）。非简单、动态卷具有无法完全解读的随机磁盘几何结构。因此，AppAssure 不支持导出复杂或非简单的动态卷。

管理导出

在 Core 控制台中的 **Virtual Standby（虚拟待机）**选项卡上，可以查看已设置的导出的状态，包括一次性导出和虚拟待机的连续导出。在此选项卡上，可以通过暂停、停止、移除导出来管理导出，或查看即将进行的导出队列。

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

1. 在 Core 控制台中，导航至 **Virtual Standby**（虚拟待机）选项卡。

   在 **Virtual Standby**（虚拟待机）选项卡中，可以查看已保存导出设置的表格，其中包含如下表所述的信息。

菜单	说明
状态	**注:** 虚拟待机配置的状态通过图标颜色进行定义。 绿色 - 虚拟待机已配置成功、处于活动状态并且未暂停。下一次虚拟待机导出将在下一个快照后执行。 黄色 - 虚拟待机已暂停，并且仍由 Core 进行保存。但是，在新传输后，导出作业将不会自动启动，并且此代理将不再有新的虚拟待机导出。
机器名称	源机器的名称。
目标	将数据导出到的虚拟机和路径。
导出类型	用于导出的虚拟机平台类型，例如 ESXi、VMware、Hyper-V 或 VirtualBox。
上次导出	上次导出的日期和时间。如果最近添加了导出并且该导出尚未完成，则会显示一条消息，指示该导出尚未执行完成。如果导出失败或被取消，也会显示相应的消息。

2. 要管理已保存的导出设置，请选择一个导出，然后单击以下选项之一：
   - **Pause**（暂停）：暂停导出。
   - **Resume**（恢复）：重新启动已暂停的导出。
   - **Force**（强制）：强制执行新导出。当虚拟待机在暂停后恢复时（这表示导出作业只会在新传输后重新启动），可以用到此选项。如果您不想等待新传输，则可以强制导出。
3. 要从系统中移除导出，请单击 **Remove**（移除）。移除导出时，该导出将从系统中永久移除，您将无法重新启动该导出。
4. 要查看有关当前队列中尚未完成的活动导出的详细信息，请单击 **Show Export Queue**（显示导出队列）。

   此时会显示下表：

菜单	说明
机器名称	源机器的名称。
目标	虚拟待机已配置成功、处于活动状态并且未暂停。下一次虚拟待机导出将在下一个快照后执行。
导出类型	虚拟待机已暂停，并且仍由 Core 进行保存。但是，在新传输后，导出作业将不会自动启动，并且此代理将不再有新的虚拟待机导出。
计划类型	导出类型为 One-time（一次性）或 Continuous（连续）。
状态	导出的进度，以百分比形式显示在进度条中。

将 Windows 机器的备份信息导出到虚拟机

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 Windows 机器的数据导出至虚拟机（VMware、ESXi 和 Hyper-V）。

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

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 **Protected Machines（受保护机器）**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：
   - One-time（一次性）
   - Virtual Standby（虚拟待机）

   此时将显示 **Export Wizard（导出向导）**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 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 **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 **ESX(i)**。
2. 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。

3. 在 **Virtual Machine Options**（虚拟机选项）页面中，输入下表所述信息。

文本框	说明
Resource Pool（资源池）	从下拉列表中选择资源池。
Data Store（数据存储）	从下拉列表中选择数据存储。
Virtual Machine Name（虚拟机名称）	输入虚拟机的名称。
Memory（内存）	指定内存使用量。

文本框	说明
Disk Provisioning（磁盘配置）	选择磁盘配置类型：Thin（精简）或 Thick（密集）。
Disk Mapping（磁盘映射）	指定磁盘映射类型：Automatic（自动）或 Manual（手动）。
Version（版本）	选择虚拟机的版本。

4. 单击 **Next**（下一步）。
5. 在 **Volumes**（卷）页面中，选择要导出的卷，然后单击 **Next**（下一步）。
6. 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 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 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，然后单击 **Actions（操作）** → **Export（导出）** → **Virtual Standby（虚拟待机）**。
2. 在 **Export Wizard（导出向导）**的 **Destination（目标）**页面中，从 **Recover to a Virtual Machine（恢复到虚拟机）**下拉菜单中选择 **ESXi**。
3. 输入用于访问虚拟机的信息，如下表中所述，然后单击 **Next（下一步）**。

文本框	说明
Host name（主机名）	输入主机名。
Port（端口）	输入主机端口。默认为 443。
User name（用户名）	输入用于登录主机的凭据。
Password（密码）	输入用于登录主机的凭据。

4. 在 **Virtual Machine Options（虚拟机选项）**页面中，输入下表所述信息。

文本框	说明
Resource Pool（资源池）	从下拉列表中选择资源池。
Data Store（数据存储）	从下拉列表中选择数据存储。
Virtual Machine Name（虚拟机名称）	输入虚拟机的名称。

文本框	说明
Memory（内存）	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）
Disk Provisioning（磁盘配置）	选择磁盘配置类型：Thin（精简）或 Thick（密集）。
Disk Mapping（磁盘映射）	指定磁盘映射类型：Automatic（自动）或 Manual（手动）。
Version（版本）	选择虚拟机的版本。

5. 单击 **Next（下一步）**。
6. 在 **Volumes（卷）**页面中，选择要导出的卷，然后单击 **Next（下一步）**。
7. 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 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 Core 控制台中，导航至要导出的机器。
2. 在 **Summary（摘要）**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 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 **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 **VMware Workstation**，然后单击 **Next（下一步）**。
2. 在 **Virtual Machine Options（虚拟机选项）**页面中，根据下表中的说明输入用于访问虚拟机的参数。

文本框	说明
Location（位置）	指定要在其上面创建虚拟机的本地文件夹或网络共享的路径。 **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。

文本框	说明
User Name（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。
Password（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。
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:** 默认名称是源机器的名称。
Version（版本）	指定虚拟机的 VMware Workstation 版本。您可以选择： • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Memory（内存）	通过单击以下选项之一，指定虚拟机的内存使用量： • Use the same amount of RAM as the source machine（使用与源机器相同容量的 RAM）- 指定 RAM 配置与源机器相同。 • 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）

3. 单击 **Next（下一步）**。
4. 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 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 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）**的 **Destination（目标）**页面中，单击 **Recover to a Virtual Machine（恢复到虚拟机）** → **VMware Workstation**。
3. 单击 **Next（下一步）**。
4. 在 **Virtual Machine Options（虚拟机选项）**页面中，根据下表中的说明输入用于访问虚拟机的参数。

文本框	说明
Target Path（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。
User Name（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。
Password（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。
Virtual Machine（虚拟机）	输入即将创建的虚拟机的名称；例如 VM-0A1B2C3D4。 **注:** 默认名称是源机器的名称。
Version（版本）	指定虚拟机的 VMware Workstation 版本。您可以选择： • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Memory（内存）	通过单击以下选项之一，指定虚拟机的内存量： • Use the same amount of RAM as the source machine（使用与源机器相同容量的 RAM）- 指定 RAM 配置与源机器相同。 • 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。

5. 选择 **Perform initial ad-hoc export（执行初始临时导出）**以立即执行虚拟导出，而不是在下一个计划快照后导出。
6. 单击 **Next（下一步）**。
7. 在 **Volumes（卷）**页面中，选择要导出的卷（例如 C:\ 和 D:\），然后单击 **Next（下一步）**。
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。

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

在 AppAssure 中，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。

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 Windows 数据

在 AppAssure 中，您可通过执行一次性或连续导出，或通过建立连续导出（用于虚拟待机），选择使用 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 Oracle VirtualBox 一次性导出：

1. 在 Core 控制台中，导航至要导出的 Linux 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）。
5. 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）。
6. 在 **Virtual Machine Options**（虚拟机选项）页面中，选择 **Remote Linux Machine**（远程 Linux 机器）。
7. 按如下所示输入用于访问虚拟机的参数：

文本框	说明
VirtualBox 主机名	输入 VirtualBox 服务器的 IP 地址或主机名。此字段代表远程 VirtualBox 服务器的 IP 地址或主机名。
端口	输入机器的端口号。此数字代表 Core 与此机器进行通信时所使用的端口。
虚拟机名称	指定目标路径以创建虚拟机。
用户名	目标机器上的帐户的用户名，例如 root。
密码	输入用于登录主机的凭据。
内存	指定虚拟机的内存。

8. 在 **Volumes**（卷）页面中，选择要导出的数据所在的卷，然后单击 **Next**（下一步）。
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

要执行 VirtualBox 连续（虚拟待机）导出，请执行以下操作：

1. 在 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。

文本框	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）	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。

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 ad-hoc export（执行初始临时导出）**以立即执行虚拟导出，而不是在下一个计划快照后导出。
7. 单击 **Next（下一步）**。
8. 在 **Volumes（卷）**页面中，选择要导出的卷（例如 C:\ 和 D:\），然后单击 **Next（下一步）**。
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。

从恢复点还原卷

可以从 AppAssure Core 中存储的恢复点还原受保护机器上的卷。要从恢复点还原卷，请执行以下操作：

1. 在 Core 控制台中，单击 **Restore（还原）**选项卡。

   此时将显示 **Restore Machine Wizard（还原机器向导）**。

2. 在 **Protected Machines（受保护机器）**页面中，选择要还原其数据的受保护机器，然后单击 **Next（下一步）**。

   注: 受保护机器必须安装代理软件，并且必须具有用于执行还原操作的恢复点。

   此时将显示 **Recovery Points（恢复点）**页面。

3. 在恢复点列表中，搜索要还原到代理机器的快照。

   注: 如果需要，使用页面底部的导航按钮来显示附加恢复点。或者，如果要限制在向导的 Recovery Points（恢复点）页面中显示的恢复点数量，可以按卷（如果已定义）或按恢复点的创建日期进行筛选。

4. 单击任意恢复点以将其选中，然后单击 **Next（下一步）**。

   此时将显示 **Destination（目标）**页面。

5. 在 **Destination（目标）**页面中，按如下所述选择要将数据还原到的机器：

   - 如果要将所选恢复点的数据还原到同一代理机器（例如 Machine1），并且如果要还原的卷不包括系统卷，则选择 **Recover to a protected machine (only non-system volumes)（恢复至受保护机器 [仅非系统卷]）**，确认选中了目标卷 (Machine1)，然后单击 **Next（下一步）**。此时将显示 **Volume Mapping（卷映射）**页面。继续执行步骤 7。
   - 如果要将所选恢复点的数据还原到不同的受保护机器（例如，使用 Machine1 的数据替换 Machine2 的内容），则选择 **Recover to a protected machine (only non-system volumes)（恢复至受保护机器 [仅非系统卷]）**，再从列表中选择目标机器（例如 Machine2），然后单击 **Next（下一步）**。此时将显示 **Volume Mapping（卷映射）**页面。继续执行步骤 7。
   - 如果要使用引导 CD 从所选恢复点还原到同一机器或不同机器，并且如果要还原的卷不包括系统卷，则选择 **Recover to any target machine using a boot CD（使用引导 CD 恢复到任意目标机器）**。
   - 要继续并使用所选恢复点的信息创建引导 CD，请单击 **Next（下一步）**并继续执行步骤 10。
   - 如果您已创建引导 CD 并且已使用引导 CD 启动目标机器，则继续执行步骤 17。
   - 如果要从恢复点还原到系统卷（例如，代理机器 Machine1 的 C 驱动器），必须执行 BMR。有关为 Windows 执行 BMR 的更多信息，请参阅为 Windows 机器启动裸机还原。
   - 有关为 Linux 执行 BMR 的更多信息，请参阅“对 Linux 机器执行裸机还原的路线图”为 Linux 机器启动裸机还原。

6. 要连接到目标机器上的通用恢复控制台 (URC)，请执行以下操作：

   a. 选择 **I already have a boot CD running on the target machine（我已在目标机器上运行引导 CD）**。

   b. 在 IP address（IP 地址）文本框中，输入包含引导 CD 的目标机器的 IP 地址。

   c. 在 Authentication Key（验证密钥）文本框中，输入目标机器上的 URC 的验证密钥，然后单击 **Next（下一步）**。

   此时将显示 **Disk Mapping（磁盘映射）**页面。继续执行步骤 20。

7. 在 **Volume Mapping（卷映射）**页面中，对于您要还原的恢复点中的每个卷，选择相应的目标卷。如果不想还原某个卷，则在 Destination Volumes（目标卷）列中，选择 **Do not restore（不还原）**。

8. 选择 **Show advanced options（显示高级选项）**，然后执行以下操作：

   - 对于还原到 Windows 机器，如果要使用实时恢复，则选择 **Live Recovery（实时恢复）**。

利用 AppAssure 中的实时恢复立即恢复技术，可以从 Windows 机器的已保存恢复点立即将数据恢复或还原到物理机或虚拟机，其中包含 Microsoft Windows Storage Space。实时恢复不可用于 Linux 机器。

- 如果要强制卸载，请选择 **Force Dismount（强制卸载）**。

  如果在还原数据之前不强制卸载，则还原可能会失败，并出现卷在使用中错误。

9. 继续执行步骤 20。
10. 在 Boot CD（引导 CD）页面中，执行以下操作：
    a. 在 **Output path（输出路径）**文本字段中，键入应存储引导 CD ISO 映像的路径。
    b. 在 **Environment（环境）**下，选择最适合所还原硬件的架构：
       - 要在具有 64 位架构的任何 Windows 机器上还原，请选择 **Windows 8 64-bit（Windows 8 64 位）**。
       - 要在具有 32 位 (x86) 架构的任何机器上还原，请选择 **Windows 7 32-bit（Windows 7 32 位）**。
11. （可选）要设置所还原代理的网络参数或使用 UltraVNC，请选择 **Show advanced options（显示高级选项）**，然后执行以下操作之一：
    - 要为所还原机器建立网络连接，请根据下表中的说明选择 **Use the following IP address（使用下面的 IP 地址）**。

选项	说明
IP Address（IP 地址）	指定所还原机器的 IP 地址或主机名。
Subnet Mask（子网掩码）	指定所还原机器的子网掩码。
Default Gateway（默认网关）	指定所还原机器的默认网关。
DNS Server（DNS 服务器）	指定所还原机器的域名服务器。

    - 要定义 UltraVNC 信息，请根据下表中的说明选择 **Add UltraVNC（添加 UltraVNC）**。如果需要从远程访问恢复控制台，则使用此选项。使用引导 CD 时，不能使用 Microsoft 终端服务登录。

选项	说明
Password（密码）	指定此 UltraVNC 连接的密码。
Port（端口）	指定此 UltraVNC 连接的端口。默认端口为 5900。

12. 单击 **Next（下一步）**。
13. 要注入驱动程序，请执行以下操作：
    a. 选择 **Add an archive of drivers（添加驱动程序存档）**。
    b. 导航至包含存档的 ZIP 文件，选择该 ZIP 文件，然后单击 **Open（打开）**。该存档将上载并显示在 Driver Injection（驱动程序注入）页面中。
    c. 然后单击 **Next（下一步）**。
14. 在 ISO Image（ISO 映像）页面中，可以查看引导 CD ISO 映像的创建状态。当引导 CD 创建成功时，单击 **Next（下一步）**。

    此时将显示 **Connection（连接）**页面。
15. 启动要从引导 CD 还原数据的代理机器。
    - 从 ISO 映像引导代理机器（如果可行）。

- 如果不可行，则将 ISO 映像复制到物理介质（CD 或 DVD），在代理机器中加载光盘，配置机器从引导 CD 加载，然后从引导 CD 重启。

注: 您可能需要更改代理机器的 BIOS 设置，以确保首先加载的卷是引导 CD。

代理机器在从引导 CD 启动时会显示通用恢复控制台 (URC) 界面。此环境用于直接从 AppAssure Core 还原系统驱动器或所选卷。记下 URC 中的 IP 地址和验证密钥凭据（每次从引导 CD 启动时都会刷新）。

16. 在 Core 控制台的 **Connection（连接）**页面中，按如下所示输入所还原机器的 URC 实例的验证信息：
    a. 在 IP Address（IP 地址）文本框中，输入要从恢复点还原的机器的 IP 地址。
    b. 在 Authentication Key（验证密钥）文本框中，输入 URC 信息。
    c. 单击 **Next（下一步）**。

    此时将显示 **Disk Mapping（磁盘映射）**页面。
17. 要手动映射卷，请继续执行步骤 18。要自动映射卷，请执行以下操作：
    a. 选择 **Automatic volume mapping（自动映射卷）**。
    b. 在 **Automatic volume mapping（自动映射卷）**区域中，选择要还原的卷。如果不想还原某个列出的卷，则清除相应选项。

    注: 必须选择至少一个卷才能执行还原。
    c. 选择还原的目标磁盘。
    d. 单击 **Next（下一步）**，然后继续执行步骤 19。
18. 如果要手动映射卷，请执行以下操作：
    a. 选择 **Manual volume mapping（手动映射卷）**。
    b. 在 **Manual volume mapping（手动映射卷）**区域中，从每个卷的 **Destination Volumes（目标卷）**下拉列表中选择要还原的卷。如果不想还原某个列出的卷，则清除相应选项。

    注: 必须选择至少一个卷才能执行还原。
    c. 单击 **Finish（完成）**。

    小心: 如果选择 Finish（完成），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。

    Restore Machine Wizard（还原机器向导）将关闭，并且恢复点的选定卷中的数据被还原到目标机器。继续执行步骤 22。
19. 在 **Disk Mapping Preview（磁盘映射预览）**页面中，检查所选还原操作的参数。要执行还原，请单击 **Finish（完成）**。

    小心: 如果选择 Finish（完成），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。

    Restore Machine Wizard（还原机器向导）将关闭，并且恢复点的选定卷中的数据被还原到目标机器。继续执行步骤 22。
20. 如果您要还原的卷包含 SQL 或 Microsoft Exchange 数据库，则在 **Dismount Databases（卸载数据库）**页面上，系统会提示您卸载这些数据库。或者，如果您要在还原完成后重新装载这些数据库，则选择 **Automatically remount all databases after the recovery point is restored（还原恢复点后自动重新装载所有数据库）**。单击 **Finish（完成）**。
21. 单击 **OK（确定）**以确认表示还原过程已启动的状态消息。
22. 要监测还原操作的进度，请在 Core 控制台中单击 **Events（事件）**。

使用命令行为 Linux 机器还原卷

在 AppAssure 中，可以使用命令行 `aamount` 公用程序在受保护的 Linux 机器上还原卷。要使用命令行为 Linux 机器还原卷，请执行以下操作：

小心: 您不应尝试还原系统卷或根 (/) 卷。

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. 输入以下命令以列出当前为指定机器装载的恢复点：
   `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`。
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。

为 Windows 机器启动裸机还原

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。

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，请参阅为 Linux 机器启动裸机还原。

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。
2. 将映像刻录到磁盘。
3. 从引导 CD 引导目标服务器。
4. 连接到恢复磁盘。
5. 映射卷。
6. 启动恢复。
7. 监测进度。

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，在还原之前必须已正确格式化新机器。

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 **Restore Machine Wizard（还原机器向导）**的 **Disk Mapping（磁盘映射）**页面中，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 **Restore（还原）**，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 **Restore Machine Wizard（还原机器向导）**的 **Disk Mapping（磁盘映射）**页面中，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 **Restore（还原）**。

   小心: 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）。

为 Linux 机器启动裸机还原

DL1000 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 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。

5

复制恢复点

复制

复制是指拷贝恢复点并将其传输至次要站点以用于灾难恢复的过程。此过程需要两个 Core 之间具有配对的“源-目标”关系。复制按受保护的机器进行管理，即每一台受保护机器的备份快照都会复制到目标副本 Core。完成复制设置后，源 Core 会持续以异步方式将增量快照数据传输至目标 Core。您可以将上述出站复制配置到公司自己的数据中心或远程灾难恢复站点（即“自管”目标 Core），或配置到托管服务提供商 (MSP) 提供的非现场备份和灾难恢复服务。要复制到 MSP，可以使用允许您提出连接请求、接收自动反馈通知的内置工作流。

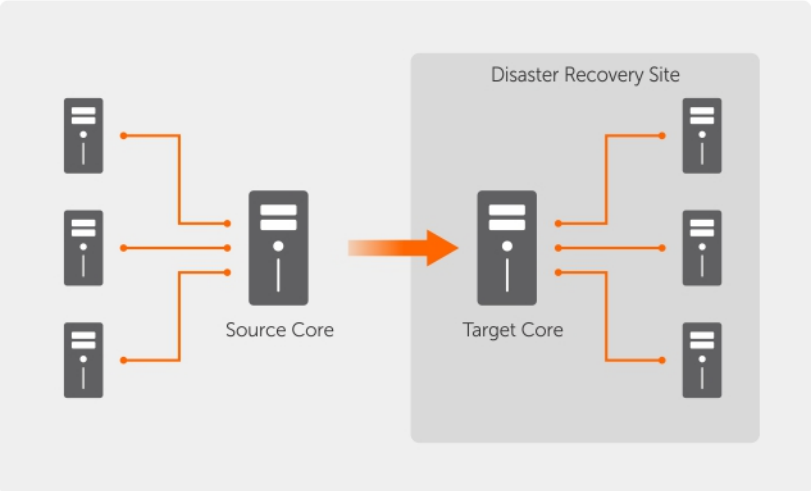


图 5: 基本复制架构

复制过程从播种开始。播种是指初始传输受保护代理的基本映像和增量快照（已消除重复数据）的过程，这些数据总计可达数百乃至数千 GB。首次复制可以使用外部介质将数据播种到目标 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。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。在目标 Core 消耗种子存档后，将自动同步新复制的增量恢复点。

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）。 • 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	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。

文本框	说明
建 RP 链 [修复孤本]）	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。

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）。

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）**。

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. 4: 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	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、

部分	说明	可执行的操作
	机器数量，以及复制传输的进度。	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。
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。
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）。

了解故障转移和故障回复

出现严重中断事件以致源 Core 和代理发生故障时，AppAssure 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 及关联代理异常终止时，切换至冗余或待机目标 (AppAssure Core)。故障转移的主要目标是启动与故障代理相同的新代理。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。

故障回复是指将代理和 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代理（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。

执行故障转移

如果遇到源 Core 和关联代理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。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）。
   此时将显示 **Fail Over（故障转移）**对话框，并列出完成故障转移所需的后续步骤。
4. 单击 **Continue**（继续）。
5. 在左侧导航区域中的 **Protected Machines（受保护机器）**中，选择具有带恢复点的关联 AppAssure 代理软件的机器。
6. 将该代理上的备份恢复点信息导出至虚拟机。
7. 将该代理上的备份恢复点信息导出至虚拟机。
8. 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。
9. 重新引导虚拟机，等待代理服务启动。
10. 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）**下以及 **Incoming Replication（传入复制）**下的 **Replication（复制）**选项卡中。
11. 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。
12. 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 和代理后，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 **Fail Back（故障回复）**对话框，说明需要完成的步骤，完成这些步骤后可以单击 **Continue（继续）**按钮以完成故障回复。
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. 强制创建机器快照。有关更多信息，请参阅强制创建快照。
7. 关闭故障转移后的机器。
8. 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。
   有关创建存档的更多信息，请参阅创建存档。
9. 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。
10. 导入步骤 8 中创建的存档。
    有关更多信息，请参阅导入存档。
11. 返回至目标 Core 上的 Core 控制台，然后单击 **Replication**（复制）选项卡。
12. 在 **Incoming Replication**（传入复制）下，选择故障转移代理并展开详细信息。
13. 在 **Failback（故障回复）**对话框中，单击 **Continue（继续）**。
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。

    有关更多信息，请参阅配置机器设置。

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。

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

获得帮助

查找说明文件和软件更新

Core 控制台提供了 AppAssure 和 DL1000 设备说明文件和软件更新的直接链接。

说明文件

要访问说明文件的链接，请执行以下操作：

1. 在 Core 控制台中，单击 **Appliance（设备）**选项卡。
2. 在左侧窗格中，导航至 **Appliance（设备）** → **Documentation（说明文件）**链接。

软件更新

要访问软件更新的链接，请执行以下操作：

1. 在 Core 控制台中，单击 **Appliance（设备）**选项卡。
2. 在左侧窗格中，导航至 **Appliance（设备）** → **Software Updates（软件更新）**链接。

联系 Dell

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，您可以在您的购买发票、装箱单、账单或 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 解决有关销售、技术支持或客户服务问题，请访问 **software.dell.com/support**。

说明文件反馈

单击任意 Dell 说明文件页面中的**反馈**链接，填写表格，然后单击**提交**以发送您的反馈。