

CA ARCserve® Central Host-Based VM Backup

用户指南

16.5 版本



本文档包括内嵌帮助系统和以电子形式分发的材料（以下简称“文档”），其仅供参考，CA 随时可对其进行更改或撤销。

未经 CA 事先书面同意，不得擅自复制、转让、翻印、透露、修改或转录本文档的全部或部分内容。本文档属于 CA 的机密和专有信息，不得擅自透露，或除以下协议中所允许的用途，不得用于其他任何用途：(i) 您与 CA 之间关于使用与本文档相关的 CA 软件的单独协议；或者 (ii) 您与 CA 之间单独的保密协议。

尽管有上述规定，但如果您为本文档中所指的软件产品的授权用户，则您可打印或提供合理数量的本文档副本，供您及您的雇员内部用于与该软件相关的用途，前提是所有 CA 版权声明和标识必须附在每一份副本上。

打印或提供本文档副本的权利仅限于此类软件所适用的许可协议的有效期内。如果该许可因任何原因而终止，您应负责向 CA 书面证明已将本文档的所有副本和部分副本已退还给 CA 或被销毁。

在所适用的法律允许的范围内，CA 按照“现状”提供本文档，不附带任何保证，包括但不限于商品适销性、适用于特定目的或不侵权的默示保证。CA 在任何情况下对您或其他第三方由于使用本文档所造成的直接或间接的损失或损害都不负任何责任，包括但不限于利润损失、投资受损、业务中断、信誉损失或数据丢失，即使 CA 已经被提前明确告知这种损失或损害的可能性。

本文档中涉及的任何软件产品的使用均应遵照有关许可协议的规定且根据本声明中的条款不得以任何方式修改此许可协议。

本文档由 CA 制作。

仅提供“有限权利”。美国政府使用、复制或透露本系统受 FAR Sections 12.212、52.227-14 和 52.227-19(c)(1) - (2) 以及 DFARS Section 252.227-7014(b)(3) 的相关条款或其后续条款的限制。

版权所有 © 2013 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication 和 High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

联系 CA

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：<http://www.ca.com/worldwide>。

CA ARCserve Central Applications 支持链接：

CA Support 联机提供了丰富的资源集，用于解决您的技术性问题，并允许轻松访问重要的产品信息。使用 CA Support，您可以轻松访问始终可用的可信建议。下列链接允许您访问可用的各个 CA Support 站点：

- **了解您可以获得的支持** -- 以下链接提供维护计划和支持服务的有关信息，包括条款和条件、声明、服务水平目标 (SLO) 和服务时间。
<https://support.ca.com/prodinfo/centappssupportofferings>
- **注册以获得支持** -- 以下链接将您带到 CA Support 在线注册表单，该表单用于激活您的产品。
<https://support.ca.com/prodinfo/supportregistration>
- **访问技术支持** -- 以下链接将您带到 CA ARCserve Central Applications 的一站式产品支持页面。
<https://support.ca.com/prodinfo/arccentapps>

文档更改

自上一版本的 CA ARCserve Central HostBased VM Backup 以来已做出以下文档更新：

- 已进行更新以包括用户反馈、增强、改正以及其他小的改动，以便帮助改进产品或文档本身的使用性和理解性。
- 更新了[创建备份策略](#) (p. 68)。此主题现在包括“备份设置” / “高级”选项卡的两个新选项：“在目标上保留空间”和“首选项” / “电子邮件报警”选项卡：添加了两个新的合并作业报警，删除了合并失败。
- 更新了[编辑或复制备份策略](#) (p. 72)。此主题现在包括“备份设置” / “高级”选项卡的两个新选项：在目标上保留空间和编录。
- 更新了[查看 CA ARCserve Central HostBased VM Backup 日志](#) (p. 78)。此主题现在在模块下拉框中包括两个新选项：更新多节点和 CA ARCserve D2D 合并作业。
- 更新了[恢复整个虚拟机](#) (p. 92)。此主题现在更新为反映对话框的最新设计。
- 更新了[更新节点时发生访问被拒绝错误](#) (p. 115)。此主题现在包括禁用用户帐户控制 (UAC) 的两个解决方案。
- 更新了[执行裸机恢复](#) (p. 143)。此主题现在更新为包括新的实用工具（为裸机恢复创建启动工具包）以便创建 WinPE ISO 执行 BMR。不再提供 ISO 文件。此外，此主题还包括支持将 UEFI 计算机上进行的备份 BMR 到 BIOS 计算机以及从 BIOS 计算机 BMR 到 UEFI 计算机。
- 增加了[如何创建启动工具包](#) (p. 157)。增加此主题以包括用于创建 WinPE ISO 映像以执行 BMR 的新实用工具的新增功能和功能。
注意：删除了“创建启动工具包”，替换为此主题。
- 使用有关如何还原 Microsoft Exchange 应用程序的新方案主题更新了“应用程序还原 - Microsoft Exchange 服务器”。此主题现在包括 Exchange 2013 支持，请参阅查看还原先决条件和注意事项。
- 添加了[将虚拟机恢复到备选 ESX 服务器或 Hyper-V 服务器时，CA ARCserve Central HostBased VM Backup 不识别动态磁盘上的卷](#) (p. 141)。此主题说明在动态磁盘上检索卷的解决方案。
- 增添了[从防病毒扫描排除文件](#) (p. 176)。此主题说明在防病毒扫描之前要排除的文件、文件夹和进程。
- 以下主题得到更新，可提供内置或域管理员凭据以登录到虚拟机来宾操作系统。
 - [先决条件安装任务](#) (p. 17)

- [操作前检查项目的解决方案](#) (p. 55)
- [更新节点时发生访问被拒绝错误](#) (p. 115)

目录

第 1 章： CA ARCserve Central HostBased VM Backup 介绍	11
简介.....	11
关于 CA ARCserve Central HostBased VM Backup	11
CA ARCserve Central HostBased VM Backup 工作原理	12
CA ARCserve Central Applications 总目录.....	13
第 2 章： 安装与配置 CA ARCserve Central HostBased VM Backup	15
如何安装 CA ARCserve Central HostBased VM Backup	15
先决条件安装任务.....	17
安装 CA ARCserve Central HostBased VM Backup	19
以无人值守方式安装 CA ARCserve Central HostBased VM Backup.....	21
如何卸载 CA ARCserve Central HostBased VM Backup	23
卸载 CA ARCserve Central HostBased VM Backup	24
以无人值守方式卸载 CA ARCserve Central HostBased VM Backup.....	24
如何配置 CA ARCserve Central HostBased VM Backup 来保护 CA ARCserve D2D 节点.....	26
配置 CA ARCserve Central Protection Manager 服务器	27
配置发现排定.....	28
配置电子邮件和报警设置.....	29
配置更新排定.....	30
配置社交网络首选项.....	33
修改管理员帐号.....	34
第 3 章： 使用 CA ARCserve Central HostBased VM Backup	35
如何设置您的生产环境.....	35
如何使用 CA ARCserve Central HostBased VM Backup 主页.....	36
登录 CA ARCserve D2D 节点.....	36
如何管理 CA ARCserve Central HostBased VM Backup 的节点任务.....	37
从 CA ARCserve Central HostBased VM Backup 发现节点	40
添加节点.....	41
更新节点.....	44
删除节点.....	45
合并作业选项.....	45
如何管理 CA ARCserve Central HostBased VM Backup 的节点组任务.....	47
添加节点组.....	48
删除节点组.....	50
修改节点组.....	51
如何备份虚拟机环境.....	53

执行备份作业的操作前检查.....	54
立即运行备份.....	58
执行应用程序级备份.....	64
执行仅包含已用块数据的完全磁盘备份。.....	65
查看作业状态信息.....	65
如何管理 CA ARCserve Central HostBased VM Backup 的策略.....	67
创建备份策略.....	68
编辑或复制备份策略.....	72
从备份策略分配和取消分配节点.....	74
查看 CA ARCserve Central HostBased VM Backup 日志.....	76
查看特定节点的活动日志信息.....	78
在报告中查看 CA ARCserve Central HostBased VM Backup 状态.....	79
将链接添加到导航栏中.....	80
保护裸设备映射的注意事项.....	80
更改服务器通信协议.....	81
定义备份的传输模式.....	82

第 4 章： 还原和恢复虚拟机 85

还原方法.....	85
从恢复点还原.....	86
通过安装恢复点进行还原.....	89
使用“查找要还原的文件/文件夹”还原数据.....	89
恢复整个虚拟机.....	92
还原注意事项.....	96
应用程序级还原.....	96
还原 Exchange Server 数据.....	97
还原 SQL Server 数据.....	102

第 5 章： CA ARCserve Central HostBased VM Backup 故障排除 107

当尝试添加节点时，出现“无法连接到指定的服务器”消息.....	109
空白网页出现或者 Javascript 错误发生.....	111
当登录到 CA ARCserve D2D 节点时，没有适当加载网页.....	112
如何解决页面加载问题.....	114
当访问 CA ARCserve Central Applications 时，乱码显示在浏览器 Windows 中.....	115
更新节点时发生访问被拒绝错误.....	115
在您登录到应用程序时，显示证书错误.....	117
快照创建错误导致备份失败.....	118
恢复 VM 操作因未知错误失败.....	119
使用 hotadd 传输模式的备份和恢复操作无法挂接磁盘.....	121
使用 HOTADD 或 SAN 传输模式恢复数据时，恢复操作失败.....	121
发生未找到操作系统错误.....	123
VM 恢复后未保留 MAC 地址更改.....	124

CA ARCserve D2D Web 服务在 CA ARCserve D2D 上失败.....	125
CA ARCserve Central HostBased VM Backup 无法与远程节点上的 CA ARCserve D2D Web 服务进行通信.....	127
CA ARCserve D2D Web 服务运行缓慢.....	128
更改块跟踪失败.....	130
由于 ESXi 许可，备份失败.....	130
备份失败，备份代理系统的事件日志中记录了事件 1530.....	131
指定 hotadd 传输模式时，备份使用 NBD 传输模式完成.....	132
增量备份作业被处理为验证备份作业.....	133
因为无法标识块，所以备份作业失败.....	133
无法打开 VMDK 文件。.....	134
更改节点的名称后节点不显示在“节点”屏幕上.....	134
将策略保存或分配到 CA ARCserve D2D 服务器时发生多连接错误.....	135
因无法访问 ESX 服务器，虚拟机备份失败，.....	135
添加新选项卡链接无法在 Internet Explorer 8、9 和 Chrome 中正确启动.....	136
添加新选项卡链接、RSS 源和社交网络反馈无法在 Internet Explorer 8 和 9 中正确启动.....	139
使用日本键盘时无法在筛选字段中指定星号或下划线作为通配符.....	140
恢复虚拟机使用不同的传输模式，而不是指定模式.....	140
将虚拟机恢复到备选 ESX 服务器或 Hyper-V 服务器时，CA ARCserve Central HostBased VM Backup 不识别动态磁盘上的卷.....	141
在使用 HotAdd 传输模式为大小超过 2 TB 的磁盘备份数据时发生的还原数据问题.....	142

第 6 章：应用最佳实践 143

执行虚拟机的裸机恢复.....	143
如何创建启动工具包.....	157
定义并行备份的数量限制.....	169
增加 VMVixMgr 日志文件中保留的消息数量.....	170
保护 CA ARCserve D2D 备份代理.....	171
安装过程如何影响操作系统.....	171
包含不正确文件版本信息的二进制文件.....	173
不包含嵌入清单的二进制文件.....	173
具有在清单中要求的管理员特权权限级别的二进制文件.....	174
从防病毒扫描排除文件.....	176

词汇表 179

第 1 章： CA ARCserve Central HostBased VM Backup 介绍

此部分包含以下主题：

[简介 \(p. 11\)](#)

[关于 CA ARCserve Central HostBased VM Backup \(p. 11\)](#)

[CA ARCserve Central HostBased VM Backup 工作原理 \(p. 12\)](#)

[CA ARCserve Central Applications 总目录 \(p. 13\)](#)

简介

CA ARCserve Central Applications 将核心数据保护和管理技术与协同运行的目标应用程序的生态系统进行组合，从而有利于在全局环境中进行数据的现场或远程保护、复制、移动和转换。

CA ARCserve Central Applications 易于使用、管理和安装。它使组织可以对他们的信息进行自动控制，从而能够基于整体商业价值就数据的访问、可用性和安全做出明智的决策。

关于 CA ARCserve Central HostBased VM Backup

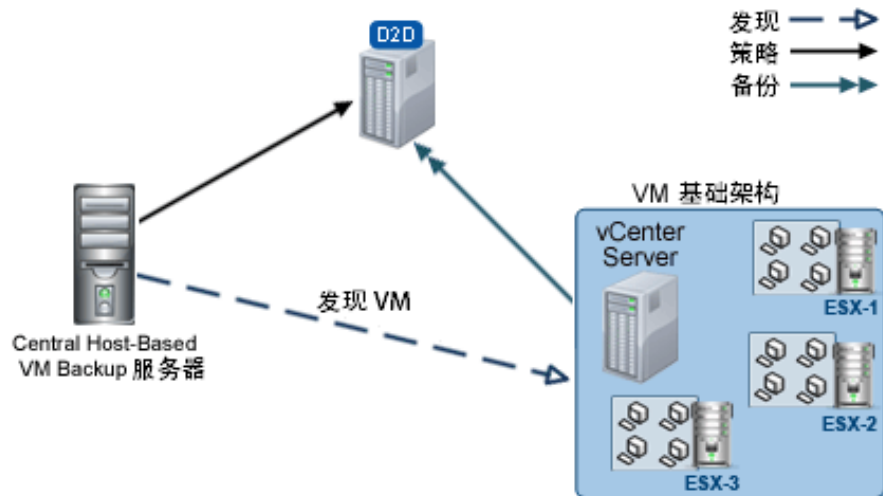
CA ARCserve Central Applications 之一是 CA ARCserve Central HostBased VM Backup 应用程序。该应用程序可与轻量级备份解决方案 CA ARCserve D2D 一起使用，允许您保护多个虚拟机，无需在每个虚拟机上安装软件或代理。此功能可将在同一台物理服务器上运行多个备份操作的负面影响降至最低，并允许您从虚拟机备份执行文件级恢复、应用程序级恢复或裸机恢复 (BMR)。

CA ARCserve Central HostBased VM Backup 可按照需要轻松扩展，因此您可以添加虚拟机而无需购买其他许可或者在生产环境中的每台虚拟机上都安装软件。

CA ARCserve Central HostBased VM Backup 工作原理

CA ARCserve Central HostBased VM Backup 允许您使用安装在代理上的一台 CA ARCserve D2D 实例即可保护运行 ESX 或 vCenter 服务器上的虚拟机。使用以下清单开始：

1. 将 CA ARCserve D2D 安装在您的环境中充当备份代理的一台计算机（物理或虚拟）上。有关安装说明，请参阅《CA ARCserve D2D 用户指南》中的主题“安装 CA ARCserve D2D”。确保代理得到正确配置。
2. 添加节点进行管理。指定 ESX 服务器，应用程序便会检测到在其上运行的并满足要求的虚拟机。
3. 创建备份策略。在每个策略中，指定安装 CA ARCserve D2D 的备份代理。
4. 将备份策略分配给每个 VM，以便您可以使用运行在备份代理上的单个 CA ARCserve D2D 实例来保护所有 VM。
5. 创建节点组以更好地管理您的虚拟机环境。例如，您可以按业务功能或已安装应用程序对节点进行分组，然后分配一个配置的策略，以保护与特定功能有关的节点或运行特定应用程序的节点。



CA ARCserve Central Applications 总目录

CA ARCserve Central Applications 帮助系统中包含的主题还以 PDF 格式作为用户指南。该指南最新的 PDF 版本和帮助系统可通过 CA ARCserve Central Applications 总目录访问。

CA ARCserve Central Applications 版本说明文件包含关于系统要求、操作系统支持、应用程序恢复支持以及其他您可能在安装该产品之前需要知道的其他信息。此外，版本说明文件包含您在使用 CA ARCserve Central Applications 之前应当注意的已知问题列表。版本说明的最新版本可以通过 CA ARCserve Central Applications 总目录访问。

第 2 章：安装与配置 CA ARCserve Central HostBased VM Backup

此部分包含以下主题：

[如何安装 CA ARCserve Central HostBased VM Backup \(p. 15\)](#)

[如何卸载 CA ARCserve Central HostBased VM Backup \(p. 23\)](#)

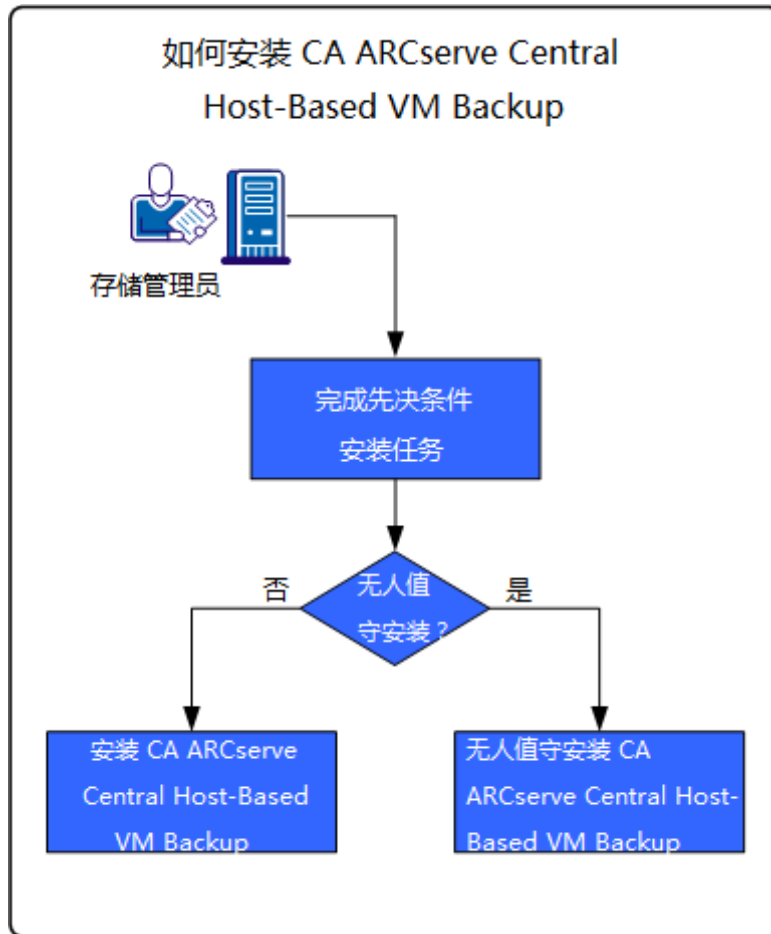
[如何配置 CA ARCserve Central HostBased VM Backup 来保护 CA ARCserve D2D 节点 \(p. 26\)](#)

如何安装 CA ARCserve Central HostBased VM Backup

此场景介绍了存储管理员如何使用以下方法安装 CA ARCserve Central HostBased VM Backup：

- 标准安装—该方法使用安装向导安装应用程序。
- 无人值守安装—该方法使您可以使用 Windows 命令行以无人值守的方式执行安装。

下图说明了如何安装应用程序：



下表列出了描述安装 CA ARCserve Central HostBased VM Backup 的任务的主题：

任务	参阅主题
执行先决条件安装任务，并在安装应用程序之前查看安装注意事项。	先决条件安装任务 (p. 17)
使用安装向导执行标准安装。	安装 CA ARCserve Central HostBased VM Backup (p. 19)
使用 Windows 命令行执行无人值守安装。	以无人值守方式安装 CA ARCserve Central HostBased VM Backup (p. 21)

有关安装应用程序后更新各种 Windows 操作系统组件的信息，请参阅《CA ARCserve Central HostBased VM Backup 用户指南》中的“应用最佳实践”部分。

先决条件安装任务

安装应用程序之前，请完成以下先决条件任务并查看安装注意事项：

先决任务

- 阅读《版本说明》。版本说明中介绍了系统要求、支持的操作系统以及本版本应用程序中存在的已知问题的列表。
- 确保您的系统满足安装该应用程序所需的软硬件要求。
- 确保在正在保护的虚拟机上可以并且已经启用更改块跟踪。

注意：有关更改块跟踪的详细信息，请参阅 VMware 网站上的以下知识库文档：

<http://kb.vmware.com/kb/1020128>

- 确保您的 Windows 帐号在计划安装 CA ARCserve Central HostBased VM Backup 的计算机上有管理员权限或用于安装软件的任何其他等同权限。
- 确保您的 vCenter Server 或 ESX Server 帐号有 VMware 和 Windows 管理权限。将该帐号分配给 vCenter Server 系统或 ESX Server 系统的 Global License 角色，以让 VDDK 操作成功完成。

- 确认您拥有要安装该应用程序的计算机用户名和密码。
- 确认 CA ARCserve D2D 已安装在可以保护您生产环境中的虚拟机的备份代理系统上。
- 如果您希望从 VM 备份获得粒度还原功能，请确认提供来自具有管理员权限的任何用户的内置或域管理员凭据，以登录到虚拟机来宾操作系统。
- CA ARCserve Central Applications 允许您使用部署实用工具在远程节点上安装 CA ARCserve D2D，并将以前版本升级到最新版本。要使用最新版 CA ARCserve D2D 备份远程节点上的数据，您必须获得最新版 CA ARCserve D2D 许可，并将在节点上应用许可。如果在节点上安装或升级后 31 天之内未应用许可，CA ARCserve D2D 将停止工作。

安装注意事项

在您安装 CA ARCserve Central HostBased VM Backup 之前，复查以下安装注意事项：

- CA ARCserve Central Applications 安装软件包安装名为“CA ARCserve Central Applications 服务器”的模块。该服务器是所有应用程序通用的模块。该模块包含允许 CA ARCserve Central Applications 相互通信的 Web 服务、二进制文件和配置。

安装应用程序时，安装软件包在安装产品组件之前先安装 CA ARCserve Central Applications 服务器模块。如果有必要向应用程序应用修补程序，则修补程序将在更新产品组件之前更新模块。

- 安装 CA ARCserve Central HostBased VM Backup 后，在备份代理系统和用于执行操作前检查的计算机上下载和安装 VMware VIX API 版本 1.11。VMware VIX 用于从备份执行文件级和应用程序级还原。

注意：对于 VIX API 1.11，所有虚拟机必须已更新，具有最新的 VMware 工具。

- CA ARCserve D2D 将在安装 CA ARCserve D2D 的所有计算机上安装 VMware 虚拟磁盘开发工具包 (VDDK)。您不需要在您的备份代理系统上下载和安装 VDDK。

如果要使用其他版本的 VDDK，请下载并安装 VDDK，然后将 VDDKDirectory 注册表的值（位于 HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D 下）修改为安装新 VDDK 的安装文件夹。

VDDK 的默认位置如下：

- x64 操作系统

c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit

注意：将 VDDK64.zip 文件从 VDDK 安装目录解压缩至 VDDK64 文件夹。

例如 c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

- **x86 操作系统**

c:\Program Files\VMware\VMware Virtual Disk Development Kit

- 要执行特定还原操作，需要 CA ARCserve D2D 的本地安装。有关详细信息，请参阅主题 [“还原注意事项”](#) (p. 96)。CA ARCserve D2D 的许可包含在 CA ARCserve Central HostBased VM Backup 中。要获得产品安装文件，请访问 CA 支持。
- 支持裸设备映射的虚拟兼容性，但不支持物理兼容性。

安装 CA ARCserve Central HostBased VM Backup

安装向导将指导您完成一个或多个 CA ARCserve Central Applications 的安装过程。

注意：安装应用程序前，请阅读“版本说明”文件，并确认在先决条件任务中说明的所有任务已完成。

安装 CA ARCserve Central HostBased VM Backup

1. 将 CA ARCserve Central Applications 安装包下载到要安装应用程序的计算机，然后双击安装文件。

安装包将其内容提取到您的计算机，然后“先决条件组件”对话框打开。

2. 在“先决条件组件”对话框上单击“安装”。

注意：只有当安装程序检测到必需先决条件组件未安装在您的计算机上时，“先决条件组件”对话框才会打开。

安装程序安装先决条件组件后，“许可协议”对话框打开。

3. 完成“许可协议”对话框中的必要选项，然后单击“下一步”。

“配置”对话框随即打开。

4. 在“配置”对话框上，完成以下内容：

- **组件** -- 指定要安装的应用程序。

注意：如果要使用套件安装包安装该应用程序，您可以安装多个应用程序。

- **位置** -- 接受默认安装位置，或单击“浏览”以指定其他安装位置。默认位置如下：

C:\Program Files\CA\ARCserve Central Applications

- **磁盘信息** -- 确认您的硬盘驱动器有足够可用磁盘空间安装应用程序。

- **Windows 管理员名称** -- 使用以下语法指定 Windows 管理员帐号的用户名：

域\用户名

- **密码** -- 指定用户帐号的密码。

- **指定端口号** -- 指定与基于 Web 的用户界面通信时想使用的端口号。作为最佳实践，您应当接受默认端口号。默认端口号如下：

8015

注意：如果您想指定备用端口号，可用端口号从 1024 到 65535。指定备用端口号前，确认指定端口号空闲并可用。安装程序阻止您使用不可用的端口安装应用程序。

- **将 HTTPS 用于 Web 通信** -- 指定 HTTPS 通信用于数据传输。默认情况下，其未被选中。

注意：与 HTTP 通信相比，HTTPS（安全）通信提供更高级别的安全。如果您在网络中传送机密信息，建议使用 HTTPS 通信协议。

- **允许安装程序将 CA ARCserve Central Applications 服务和程序作为例外注册到 Windows 防火墙** -- 确保已选择该选项旁边的复选框。如果您想从远程计算机配置和管理 CA ARCserve Central Applications，必需防火墙例外。

注意：对于本地用户，您不需要注册防火墙例外。

单击“下一步”。

安装过程完成之后，会打开“安装报告”。

5. “安装报告”对话框概要说明安装。如果您想立即检查应用程序的更新，请单击“检查更新”，然后单击“完成”。

该应用程序即被安装。

以无人值守方式安装 CA ARCserve Central HostBased VM Backup

CA ARCserve Central Applications 允许您以无人值守安装 CA ARCserve Central HostBased VM Backup。无人值守安装无需用户交互。下列步骤说明如何使用 Windows 命令行安装应用程序。

以无人值守方式安装 CA ARCserve Central HostBased VM Backup

1. 在您想启动无人值守安装进程的计算机上，打开 Windows 命令行。
2. 将 CA ARCserve Central Applications 自解压安装包下载到您的计算机。

使用以下命令行语法启动无人值守安装进程：

```
"CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR>  
-Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
```

用法：

s

允许您以无人值守模式运行可执行文件包。

v

允许您指定其他命令行选项。

q

允许您以无人值守模式安装应用程序。

-Path:<INSTALLDIR>

（可选）允许您指定目标安装路径。

示例：

```
-Path:"C:\Program Files\CA\ARCserve Central Applications\"
```

注意：如果 INSTALLDIR 的值包含空格，请使用反斜杠和引号将路径括起来。另外，路径不能以反斜杠字符结束。

-Port:<PORT>

（可选）允许您指定通信的端口号。

示例：

```
-Port:8015
```

-U:<UserName>

允许您指定用于安装和运行应用程序的用户名。

注意：用户名必须是管理帐户，或者具有管理权限的帐户。

-P:<Password>

允许您指定用户名的密码。

-Products:<ProductList>

(可选) 允许您指定以无人值守方式安装 CA ARCserve Central Applications。如果您不指定该参数的值，无人值守安装过程将安装 CA ARCserve Central Applications 的全部组件。

CA ARCserve Central HostBased VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

全部 CA ARCserve Central Applications

ALL

注意： 下列示例说明了以无人值守方式安装一个、两个、三个或全部 CA ARCserve Central Applications 需要使用的语法：

-Products:CMX64

-Products:CMX64,VCMX64

-Products:CMX64,VCMX64,REPORTINGX64

-Products:ALL

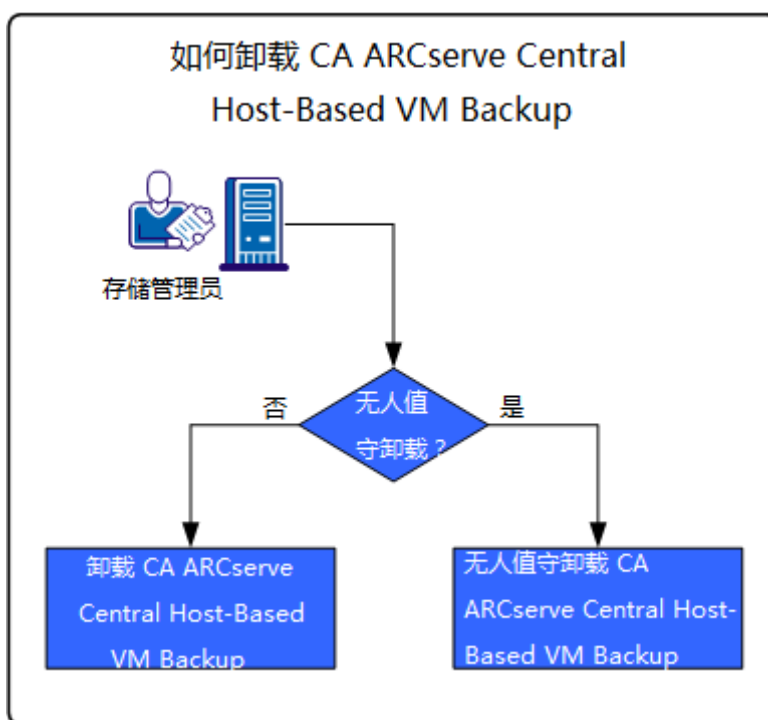
该应用程序即以无人值守方式安装。

如何卸载 CA ARCserve Central HostBased VM Backup

可以使用以下方法卸载 CA ARCserve Central HostBased VM Backup:

- 标准卸载—该方法使用 Windows 控制面板卸载应用程序。
- 无人值守卸载—该方法使您可以使用 Windows 命令行以无人值守的方式执行卸载。

下图说明了如何卸载应用程序:



任务	参阅主题
使用 Windows 控制面板执行标准卸载。	卸载 CA ARCserve Central HostBased VM Backup (p. 24)
使用 Windows 命令行执行无人值守卸载。	以无人值守方式卸载 CA ARCserve Central HostBased VM Backup (p. 24)

有关卸载应用程序后更新各种 Windows 操作系统组件的信息, 请参阅《CA ARCserve Central HostBased VM Backup 用户指南》中的“应用最佳实践”部分。

卸载 CA ARCserve Central HostBased VM Backup

您可以使用位于 Windows “控制面板” 的 “程序和功能” 卸载应用程序。

卸载 CA ARCserve Central HostBased VM Backup

1. 从 Windows 的 “开始” 菜单，单击 “开始”，然后单击 “控制面板”。

Windows “控制面板” 打开。

2. 从 Windows “控制面板”，单击 “查看方式” 旁边的下拉列表，然后 “大图标” 或 “小图标”。

Windows “控制面板” 应用程序的图标以网格布局显示。

3. 单击 “程序和功能”。

“卸载或更改程序” 窗口打开。

4. 找到并单击要卸载的应用程序。

右键单击该应用程序，然后单击弹出菜单中的 “卸载”。

按照屏幕说明卸载该应用程序。

该应用程序即被卸载。

以无人值守方式卸载 CA ARCserve Central HostBased VM Backup

CA ARCserve Central Applications 允许您以无人值守卸载 CA ARCserve Central HostBased VM Backup。以无人值守方式卸载不需要用户参与。下列步骤说明如何使用 Windows 命令行卸载应用程序。

以无人值守方式卸载 CA ARCserve Central HostBased VM Backup

1. 登录要卸载该应用程序的计算机。

注意： 您必须使用管理账号或具有管理权限的帐号登录。

2. 打开 Windows 命令行，执行以下命令启动无人值守卸载过程：

```
<INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
```

或者，

```
<INSTALLDIR>%\Setup\uninstall.exe /q /ALL
```

示例： 以下语法允许您以无人值守方式卸载 CA ARCserve Central HostBased VM Backup。

```
"%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
```


用法:

<INSTALLDIR>

允许您指定安装该应用程序的目录。

注意: 执行与计算机操作系统的体系结构相对应的句法:

<ProductCode>

允许您指定要以无人值守方式卸载的应用程序。

注意: 无人值守卸载过程允许您安装一个或多个 CA ARCserve Central Applications。使用以下产品代码以无人值守方式卸载 CA ARCserve Central Applications:

CA ARCserve Central HostBased VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

该应用程序即以无人值守方式卸载。

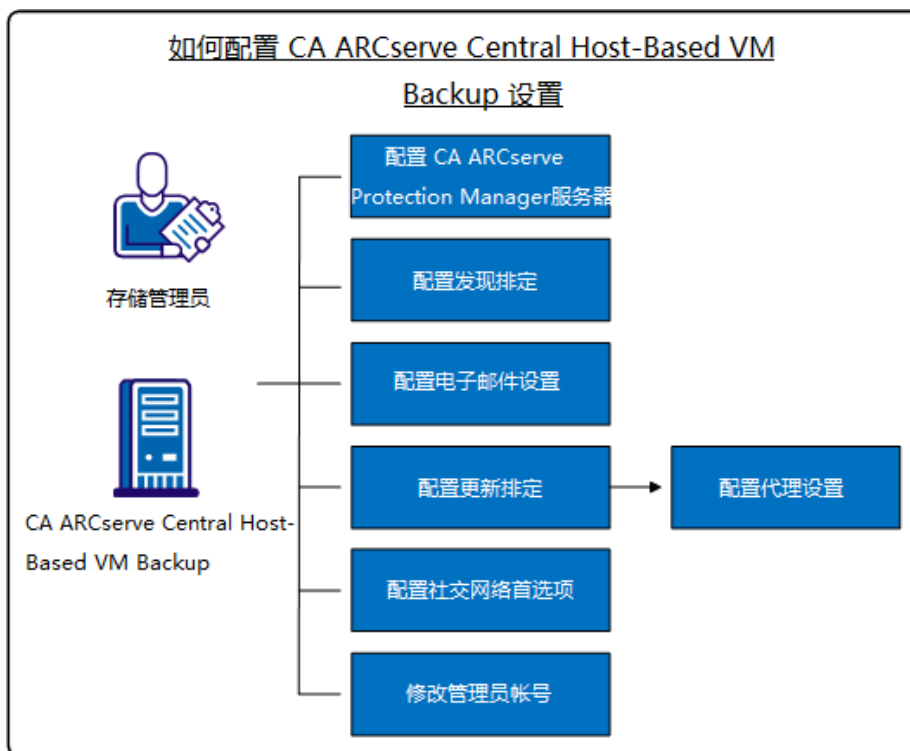
如何配置 CA ARCserve Central HostBased VM Backup 来保护 CA ARCserve D2D 节点

通过该应用程序，您可以指定电子邮件报警和排定的配置设置，并可以指定如何更新您的 CA ARCserve Central HostBased VM Backup 安装。

开始指定您的配置设置之前，您需要先在执行备份作业的服务器上安装 CA ARCserve D2D。该对等服务器（或代理服务器）可以是单台计算机，也可以是多台计算机，具体取决于您的需要。有关说明，请参阅《CA ARCserve D2D 用户指南》中的主题“安装 CA ARCserve D2D”。

您可以在同一计算机或单独的计算机上安装 CA ARCserve Central HostBased VM Backup。安装过程是基于向导的，以使设置变得很轻松。有关详细信息，请参阅安装 CA ARCserve Central HostBased VM Backup。

下图介绍了可以为应用程序设置的配置类型：



此场景介绍了以下主题：

- [配置 CA ARCserve Central Protection Manager 服务器](#) (p. 27)
- [配置发现排定](#) (p. 28)
- [配置电子邮件设置](#) (p. 29)
- [配置更新排定](#) (p. 30)
 - [配置代理设置](#) (p. 31)

- [配置社交网络首选项](#) (p. 33)
- [修改管理员帐号](#) (p. 34)

配置 CA ARCserve Central Protection Manager 服务器

通过配置 CA ARCserve Central Protection Manager 服务器，您可以将 CA ARCserve Central HostBased VM Backup 中的当前设置更改为 CA ARCserve Central Protection Manager 服务器设置。配置好设置后，您便可以从 CA ARCserve Central Reporting 中查看 Host-Based VM Backup 发现的节点电子邮件报警信息。

遵循这些步骤:

1. 登录到 CA ARCserve Central HostBased VM Backup 服务器，然后单击导航栏上的“配置”。
“配置”屏幕显示。
2. 从“配置”面板上，单击“CA ARCserve Central Protection Manager 配置”。
3. 填写下列字段:

- **CA ARCserve Central Protection Manager 服务器**

注意：如果安装了 CA ARCserve Central Protection Manager 和 CA ARCserve Central HostBased VM Backup，以下字段默认为本地 CA ARCserve Central Protection Manager 服务器。如果未安装 CA ARCserve Central Protection Manager，字段为空，需要您来手动配置。您可从 CA ARCserve Central Reporting 中查看已发现节点报警通知。

- **计算机名** -- 安装 CA ARCserve Central Protection Manager 的计算机的主机名。
- **用户名** -- 登录到安装有 CA ARCserve Central Protection Manager 的计算机所需的用户名。
- **密码** -- 该用户的密码。
- **端口** -- 必须用来与 CA ARCserve Central Protection Manager Web 服务通信的端口号。
- **HTTPS** -- 选中或不选中该选项取决于 CA ARCserve Central Protection Manager 服务器中配置的连接。
- **自动检测端口和协议** -- 允许您获得 Protection Manager 数据库的 CA ARCserve Central Protection Manager 端口和协议，并填充上述字段。

注意：只有当允许对 CA ARCserve Central Protection Manager 服务器进行远程注册表访问时，该选项才会被启用。

要验证是否允许进行远程注册，请执行以下步骤：

1. 转到安装有 CA ARCserve Central Protection Manager 的 CA ARCserve Central Protection Manager 服务器。
 2. 导航到 services.msc 并验证是否已启动“远程注册”服务。
 3. 设置为“自动”。
- **测试** -- 允许您确认 CA ARCserve Central Protection Manager 的访问信息正确。
4. 单击“保存”。

配置发现排定

可以基于重复方式和排定时间配置节点的发现排定。默认情况下，“发现配置”被禁用。要启用该配置，请单击“启用”选项以指定您希望的重复方式类型以及开始执行节点发现的排定时间。可以指定以下参数来配置发现排定：

- **每几天** -- 允许您按指定天数重复此方式。（默认设置）
- **每周选定的某天** -- 允许您在指定的星期几重复此方式。星期一、星期二、星期三、星期四、星期五是一星期内默认的日子。
- **每月选定的某天** -- 允许您在月内指定的日期重复此方式。默认选项是每月的 1 号。

会显示一个 vCenter/ESX 主机列表，供您在设置节点发现排定时查看。

配置电子邮件和报警设置

您可以配置用于应用程序的电子邮件和报警设置，以便在指定的条件下自动发送报警。

遵循这些步骤:

1. 登录该应用程序。
从主页上的导航栏中，单击“配置”以打开“配置”屏幕。
2. 从“配置”面板中，单击“电子邮件和报警配置”以打开“电子邮件和报警配置”选项。
3. 填写下列字段：
 - **服务** -- 从下拉列表中指定电子邮件服务类型。（Google Mail、Yahoo Mail、Live Mail 或其他）。
 - **邮件服务器**—指定希望 CA ARCserve Central Applications 在发送电子邮件时使用的 SMTP 服务器的主机名。
 - **需要身份验证** -- 您指定的邮件服务器需要身份验证时请选择该选项。必需帐号名称和密码。
 - **主题** -- 指定默认电子邮件主题。
 - **发件人** -- 指定电子邮件发件人的电子邮件地址。
 - **收件人** -- 指定将接收电子邮件的一个或多个电子邮件地址，由分号 (;) 分隔。
 - **使用 SSL**—如果您指定的邮件服务器需要安全连接 (SSL)，请选择该选项。
 - **发送 STARTTLS** -- 如果您指定的邮件服务器需要“STARTTLS”命令，请选择该选项。
 - **使用 HTML 格式** -- 允许您以 HTML 格式发送电子邮件。（默认已选择）
 - **启用代理设置** -- 如果有代理服务器，请选择该选项，然后指定代理服务器设置。
4. 单击“测试电子邮件”确认邮件配置设置正确无误。

5. (可选)从“发送电子邮件报警”部分,单击“发现的节点”,以便应用程序在发现新节点时发送电子邮件报警消息。
6. 单击“保存”。

注意: 您可以单击“重置”恢复到之前保存的值,或单击“删除”删除保存的设置。删除电子邮件和报警设置后,您将无法接收电子邮件报警消息。

电子邮件配置即被应用。

配置更新排定

该应用程序允许您设置一个排定,自动从 CA 服务器或本地软件分段服务器下载产品更新。

遵循这些步骤:

1. 登录该应用程序。
2. 单击导航栏上的“配置”打开“配置”屏幕。
3. 从“配置”面板上,单击“更新配置”。
更新配置选项显示。
4. 选择下载服务器
 - **CA 服务器** -- 单击“代理设置”以访问下列选项:
 - **使用浏览器代理设置** -- 允许您使用为浏览器代理设置提供的凭据。
注意: “使用浏览器代理设置”选项对 Internet Explorer 和 Chrome 有影响。
 - **配置代理设置** -- 指定代理服务器的 IP 地址或主机名以及和端口号。如果您指定的服务器需要身份验证,单击“代理服务器需要身份验证”,然后提供凭据。
单击“确定”以返回到“更新配置”。
 - **临时服务器** -- 如果选择该选项,请单击“添加服务器”以将一个临时服务器添加到列表中 输入其主机名和端口号,然后单击“确定”。
如果您指定多个临时服务器,应用程序将试图使用列出的第一台服务器。如果连接成功,列出的剩余服务器将不用于暂存。
5. (可选)单击“测试连接”以验证服务器连接,并等候测试完成。

6. （可选）自动“单击检查更新”，然后指定日期和时间。您可以指定每日或每周排定。

单击“保存”应用更新配置。

配置代理设置

CA ARCserve Central Applications 允许您指定代理服务器与 CA 支持进行通信，检查并下载可用更新。要启用此功能，您指定要代表 CA ARCserve Central Applications 服务器进行通信的代理服务器。

遵循这些步骤：

1. 登录到应用程序，单击导航栏上的“配置”。
将显示配置选项。
2. 单击“更新配置”。
更新配置选项将显示。
3. 单击“代理服务器设置”。
“代理服务器设置”对话框将打开。

4. 请单击下列选项之一：

- **使用浏览器代理设置** -- 允许应用程序检测和使用应用于浏览器的相同代理设置，从而连接到 CA Technologies 服务器来获得更新信息。

注意：该行为仅适用于 Internet Explorer 和 Chrome 浏览器。

- **配置代理设置** -- 允许您定义应用程序将用来与 CA 支持通信检查更新的备用服务器。备用服务器（代理）有助于确保提升安全性、性能和管理控制。

填写下列字段：

- **代理服务器** - 指定代理服务器的主机名称或 IP 地址。
- **端口** -- 指定代理服务器将用来与 CA 支持网站进行通信的端口号。
- **（可选）代理服务器要求身份验证** -- 如果代理服务器的登录凭据不与 CA ARCserve Central Applications 服务器的凭据一致，请单击“代理服务器要求身份验证”旁边的复选框，并且指定需要登录到代理服务器的用户名和密码。

注意：使用以下格式指定用户名：<domain name>/<user name>。

单击“确定”。

此代理服务器设置已配置。

注意：为了确保 CA ARCserve Central HostBased VM Backup 可以将策略部署到节点并且保护 CA ARCserve D2D 节点，请确保 Host-Based VM Backup 服务器和代理服务器可以使用其各自的主机名相互通信。请执行下列操作：

1. 从 CA ARCserve Central HostBased VM Backup 服务器，使用服务器的主机名 ping 代理服务器。
2. 从代理服务器，使用服务器的主机名 ping CA ARCserve Central HostBased VM Backup 服务器。

配置社交网络首选项

CA ARCserve Central Applications 允许您管理可以帮助您管理每个应用程序的社交网络工具。您可以生成新闻 feed，指定与流行社交网络网站的链接，并且选择视频源网站。

遵循这些步骤:

1. 登录该应用程序。
从主页上的导航栏中，单击“配置”以打开“配置”屏幕。
2. 从“配置”面板中，单击“首选项配置”以打开“首选项”选项。

The screenshot shows a configuration panel with three sections:

- 新闻 Feed**: 显示来自专家咨询中心的最新消息和产品信息
- 社交网络**: 在主页显示 facebook 和 twitter 的链接
- 视频**: 使用 CA 支持视频 使用 YouTube 视频

3. 指定需要的选项:
 - **新闻 Feed** -- 允许应用程序显示关于 CA ARCserve Central Applications 和 CA ARCserve D2D 相关新闻和产品信息 RSS Feed（来自专家咨询中心）。这些 Feed 显示在主页上。
 - **社会网络** -- 允许应用程序在主页上显示访问 Twitter 和 Facebook 的图标，从而访问 CA ARCserve Central Applications 和 CA ARCserve D2D 相关社交网络网站。
 - **视频** -- 允许您选择视频类型以查看 CA ARCserve Central Applications 和 CA ARCserve D2D 产品。（使用 YouTube 视频是默认视频。）

单击“保存”。

“社交网络”选项即被应用

4. 从导航栏，单击“主页”。
“主页”随即显示。
5. 刷新浏览器窗口。
“社交网络”选项即被应用

修改管理员帐号

CA ARCserve Central Applications 允许您在安装应用程序之后修改管理员帐户的用户名、密码，或二者都修改。该管理员帐号仅用于登录屏幕上的默认显示用户名。

注意：指定的用户名必须是 Windows 管理帐号或具有 Windows 管理权限的帐号。

遵循这些步骤：

1. 登录到应用程序，单击导航栏上的“配置”。
将显示配置选项。
2. 单击“管理员帐号”
3. “管理员帐号设置”出现。
4. 根据需要更新以下字段：
 - 用户名
 - 密码单击“保存”

管理员帐户已修改。

第 3 章：使用 CA ARCserve Central HostBased VM Backup

此部分包含以下主题：

[如何设置您的生产环境](#) (p. 35)

[如何使用 CA ARCserve Central HostBased VM Backup 主页](#) (p. 36)

[登录 CA ARCserve D2D 节点](#) (p. 36)

[如何管理 CA ARCserve Central HostBased VM Backup 的节点任务](#) (p. 37)

[如何管理 CA ARCserve Central HostBased VM Backup 的节点组任务](#) (p. 47)

[如何备份虚拟机环境](#) (p. 53)

[如何管理 CA ARCserve Central HostBased VM Backup 的策略](#) (p. 67)

[查看 CA ARCserve Central HostBased VM Backup 日志](#) (p. 76)

[查看特定节点的活动日志信息](#) (p. 78)

[在报告中查看 CA ARCserve Central HostBased VM Backup 状态](#) (p. 79)

[将链接添加到导航栏中](#) (p. 80)

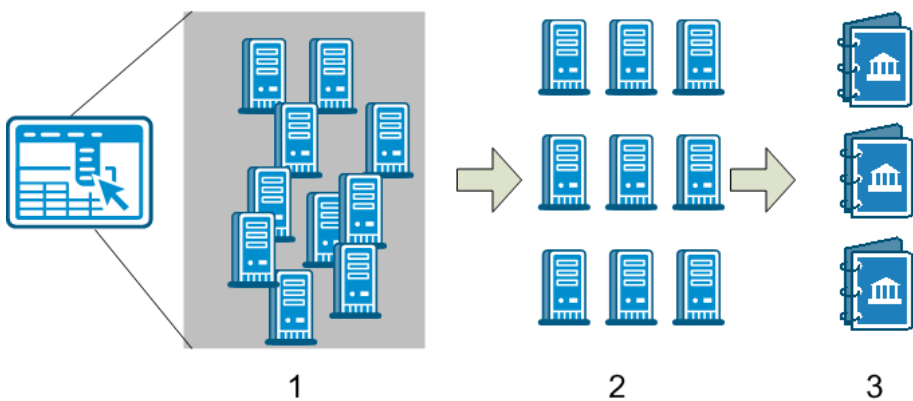
[保护裸设备映射的注意事项](#) (p. 80)

[更改服务器通信协议](#) (p. 81)

[定义备份的传输模式](#) (p. 82)

如何设置您的生产环境

保护您的虚拟机环境需要几个基本操作：



1. 将节点添加到 CA ARCserve Central HostBased VM Backup 中。您可以导入 ESX 或 vCenter 服务器承载的所有虚拟机。
2. 对节点进行分组使其更易于管理。例如，您可以按照业务功能或已安装的应用程序对节点进行分组。
3. 创建备份策略并将策略分配给节点。所有节点都根据您设置的策略进行了备份。

如何使用 CA ARCserve Central HostBased VM Backup 主页

启动 CA ARCserve Central HostBased VM Backup 会在您的 Web 浏览器中打开主页。在主页中，可以执行以下任务：

- **左侧导航：**
 - **节点**—通过“节点”屏幕，可以按照节点组、安装的应用程序和分配的 vSphere 策略来查看虚拟机环境。
 - **策略**—通过“vSphere 策略”屏幕，可以为环境中的所有节点创建、编辑和分配备份策略。
 - **配置**—通过“配置”屏幕，可以为应用程序指定电子邮件报警和自动更新排定。
 - **查看日志**—通过“查看日志”屏幕，可以查找特定问题：信息、错误或警告。
 - **添加新选项卡**—可以手动添加要监视的任何网站的名称和 URL。
 - **CA 支持**—可以访问各种支持和社交网站，包括 Facebook 和 Twitter。

登录 CA ARCserve D2D 节点

从 Host-Based VM Backup 主页，可以登录到 CA ARCserve D2D 节点。

登录到 CA ARCserve D2D 节点

1. 打开应用程序，然后在导航栏中单击“节点”。
“节点”屏幕将显示。
2. 从“组”列表，单击“全部节点”，或单击包含您要登录的 CA ARCserve D2D 节点的组。
节点列表显示与指定组关联的所有节点。

3. 浏览并单击要登录的节点，然后从弹出菜单单击“登录 D2D”。

此时将打开 CA ARCserve D2D 的 CA ARCserve Central HostBased VM Backup 版本。

注意：如果新的浏览器窗口未打开，确认您的浏览器的弹出窗口选项允许所有弹出窗口或仅允许该网站的弹出窗口。

您已登录到 CA ARCserve D2D 节点。







注意：首次登录到 CA ARCserve D2D 节点时，一个 HTML 页面可能会打开，并显示警告消息。使用 Internet Explorer 时，该情况会出现。要纠正该状况，请关闭 Internet Explorer，然后重复步骤 3。您便应可以成功登录到 CA ARCserve D2D 节点。

如何管理 CA ARCserve Central HostBased VM Backup 的节点任务

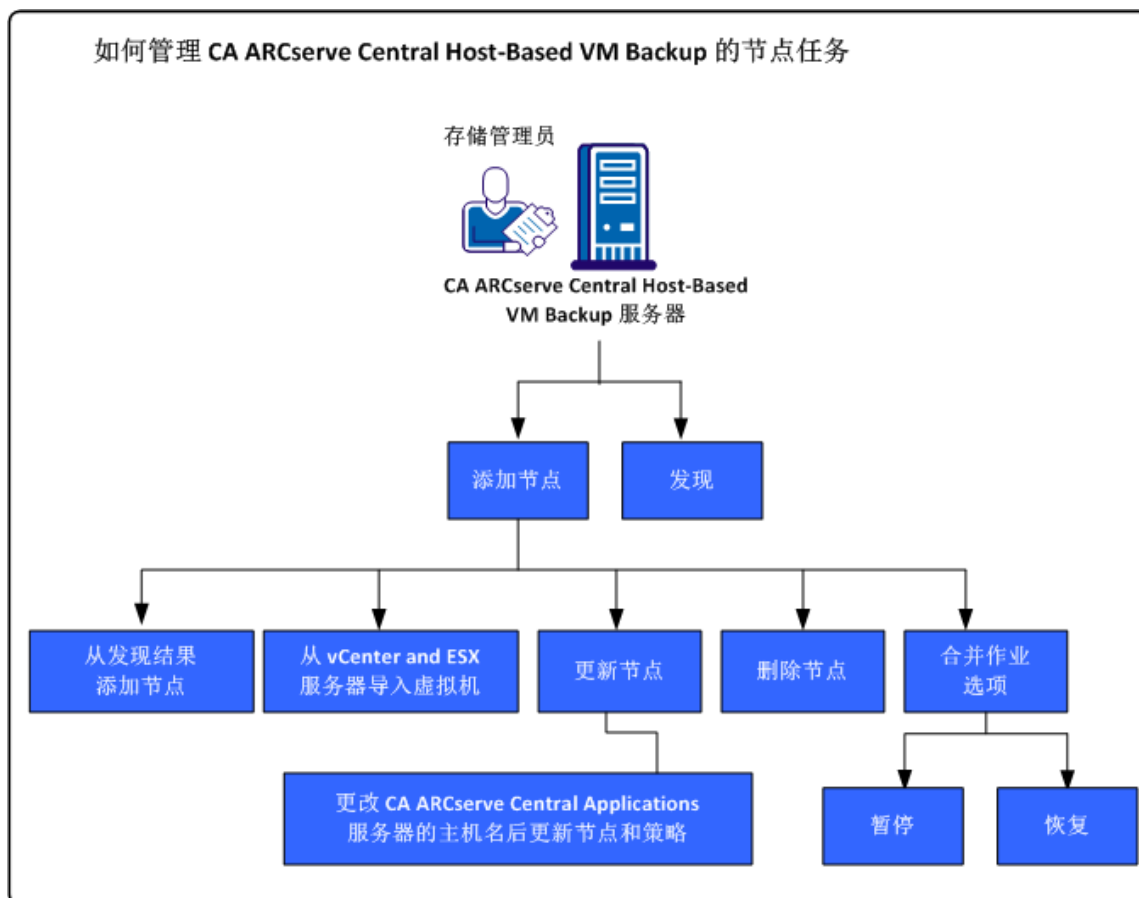
此场景介绍了存储管理员如何管理节点。例如，从“节点”屏幕添加或发现节点，将节点分配给节点组以及更新或删除节点。

下表介绍了“节点”屏幕上显示的各个项：

列名	说明
节点名称	显示节点的名称。 注意： 列出的某些节点可能尚不可选择。原因是服务器检测不到这些节点。例如，节点可能已从服务器中删除。
策略	显示策略的名称和策略部署状态。
虚拟机名	显示虚拟机的名称。
vCenter/ESX	显示可帮助检测虚拟机的服务器详细信息。
作业 (p. 65)	显示备份作业的状态并向您提供指向 备份状态监视器 (p. 66)的链接，以获取更多详细信息。

列名	说明
状态	<p>显示节点的状态：</p> <ul style="list-style-type: none"> ■  = 错误/失败 ■  = 警告 ■  = 成功 <p>如果将鼠标放在图标上，将显示“节点状态摘要”弹出表格，并显示以下类别的结果：</p> <ul style="list-style-type: none"> ■ 上次备份—显示备份类型、日期和时间以及状态。 ■ 恢复点—显示您的受监视服务器的恢复点数目。 ■ 目标容量—显示备份目标上的可用空间量。
上次备份结果	显示上次备份作业的状态。
上次备份时间	显示上次备份作业的日期和时间。
PFC 状态	<p>显示备份作业的操作前检查状态：</p> <ul style="list-style-type: none"> ■  = 错误/失败 ■  = 警告 ■  = 成功 <p>图标确定了是否可以对特定节点运行备份作业。如果将鼠标放在图标上，将显示“验证”弹出表格，并显示以下类别的结果：</p> <ul style="list-style-type: none"> ■ 更改块跟踪 (CBT)—显示备份的 CBT 结果。 ■ VMware Tools—显示 VMware 工具是否已安装。 ■ 磁盘—显示磁盘的状态。 ■ 电源状态—显示虚拟机是否已打开。 ■ 凭据—显示用户凭据的状态。 ■ 应用程序—显示节点上应用程序的安装状态。 <p>有关详细信息，请参阅主题执行备份作业的操作前检查 (p. 54)。</p>
应用程序	显示与节点关联的应用程序。
OS	显示与节点关联的操作系统。
说明	显示节点的说明。

下图说明了您可以在节点上执行的任务。



此场景介绍了添加或更新节点时可以使用的选项：

- [发现](#) (p. 40)
- [添加节点](#) (p. 41)
 - [自动从自动发现结果添加节点](#) (p. 41)
 - [从 vCenter 和 ESX 服务器导入虚拟机](#) (p. 42)
- [更新节点](#) (p. 44)
 - [更改 CA ARCserve Central Applications 服务器的主机名后更新节点和策略](#) (p. 44)
- [删除节点](#) (p. 45)
- [合并作业选项](#) (p. 45)
 - [在节点上暂停合并作业](#) (p. 46)
 - [在节点上恢复合并作业](#) (p. 46)

从 CA ARCserve Central HostBased VM Backup 发现节点

CA ARCserve Central HostBased VM Backup 允许您通过将 vCenter Server 和 ESX Server 系统添加到您的环境中来自动发现节点。通过添加这些系统，应用程序可以自动检测到这些系统承载的虚拟机。

重要说明！ 在发现节点期间，要求您指定 vCenter 服务器或 ESX 服务器系统的主机名或 IP 地址。通过该信息，发现过程可以发现附在 vCenter 服务器和 ESX 服务器系统上的虚拟机。当您发现需要修改 vCenter 服务器或 ESX 服务器系统的主机名或 IP 地址时，重复此主题中的步骤，然后重新部署备份策略以便使用更新的主机名或 IP 地址创建新的备份集。

遵循这些步骤:

1. 登录到应用程序，并单击导航栏上的“节点”以打开“节点”屏幕。
2. 单击工具栏上的“发现”以打开“按 vCenter/ESX 服务器发现节点”对话框。
3. 在“按 vCenter/ESX 服务器发现节点”对话框中，完成以下字段：
 - vCenter/ESX 主机
 - 用户名
注意：您指定的帐户必须是在 ESX Server 或 vCenter Server 系统上具有管理权限的帐户。
 - 密码
 - 端口单击“添加”。
- 注意：**重复此步骤可添加更多 vCenter/ESX Server 系统。
4. 单击“发现”以启动发现过程。
此时将打开“发现监视器”，其中显示发现进度。
5. 当发现过程完成时，会显示一条确认消息：是否要继续从发现结果添加节点？
单击“是”将显示“从发现结果添加节点”屏幕，如果要添加更多 hypervisor，则单击“否”。
注意：要自动检测节点并将其添加到“节点名称”列表中，请参阅主题配置发现排定以获取更多详细信息。
6. 从“已发现的节点”列表中，单击要添加的节点，然后单击向右箭头。节点即被添加到“要保护的节点”列表中。
7. 单击“下一步”打开“节点凭据”屏幕。

8. 为每个要添加的节点提供用户名和密码或指定适当的全局凭据。
单击“完成”。
您选择的节点将添加到所选节点组的“节点”屏幕上的“节点名称”列表中。
9. (可选)单击“刷新”。现在,您添加的服务器将在“节点”屏幕上的“组”列表中列出。
10. (可选)单击“发现”并重复之前的步骤,直到添加完所有服务器。

添加节点

随着您的环境不断增长,您可以使用“节点”屏幕添加节点,然后将节点分配给组,以便在应用程序内进行管理。该应用程序仅添加符合以下条件的虚拟机:

- 来宾操作系统为 Windows
- VMware 硬件版本为 7 或更高。

您可以按照以下过程添加节点:

- [从发现结果添加节点 \(p. 41\)](#)—发现允许您输入 ESX 和 vCenter 服务器详细信息,检测在每台服务器上运行的虚拟机,然后将检测到的节点手动或自动添加到可管理和保护这些节点的应用程序。

将根据您在“配置”屏幕上指定的排定来扫描添加到“发现”列表的服务器,直到将其删除。无需重新输入服务器详细信息。“发现”列表仅显示自上次扫描以来添加到服务器的新虚拟机。它不显示已经在应用程序中管理的 VM。您也可以运行“发现”,而不等待下一排定扫描。

- [从 vCenter/ESX 导入虚拟机 \(p. 42\)](#)

此选项是一个手动过程。此过程要求您每次启动该选项时指定 ESX 或 vCenter 服务器详细信息。如果不希望重新输入服务器详细信息,可以将服务器添加到发现列表。此选项列出了指定服务器上检测到的所有虚拟机,即使已在应用程序中管理这些虚拟机。

从发现结果添加节点

通过该选项,您可以选择根据在“发现配置”面板中指定的设置自动检测到的节点。

遵循这些步骤:

1. 登录该应用程序。
单击导航栏上的“节点”以打开“节点”屏幕。

2. 在“节点”类别中，单击“添加”，然后在弹出式菜单上单击“从发现结果添加节点”。

此时将打开“从发现结果添加节点”屏幕，其中显示已发现的节点的列表。

3. 在“已发现的节点”列表中，选择您要添加的节点，然后单击箭头将其添加到“要保护的节点”列表中。完成后单击“下一步”。

注意：您可以通过节点名称或域筛选列表来最小化列表。

4. （可选）选择一个或多个节点，然后单击“隐藏选定的节点”来隐藏您不想备份的节点。

5. （可选）选中“显示隐藏的节点”选项在“已发现的节点”列表上显示任何隐藏的节点。要再次隐藏节点，请取消选中该选项。

6. 在“节点凭据”屏幕中，提供您想添加的节点的用户名和密码。您可以指定全局凭据，也可以将凭据应用于选定的节点。

7. 单击“完成”。

节点已被添加。

从 vCenter/ESX 导入虚拟机

您可以使用“从 vCenter/ESX Server 导入虚拟机”选项来添加节点。通过此任务，应用程序可以发现在指定主机上运行的所有虚拟机，但不会执行定期自动扫描。如果您在稍后添加虚拟机，则请重复该步骤，否则不会识别新的虚拟机。

请考虑此选项与“发现”任务之间的以下不同之处：

- 每次启动此选项时指定 ESX 服务器和 vCenter 服务器详细信息。
- 您可以将指定的任何服务器添加发现列表中，这样您便无需每次输入凭据。
- 每次使用此选项时列出所有可用的虚拟机。甚至还列出由应用程序管理的虚拟机。

遵循这些步骤：

1. 登录该应用程序。
单击导航栏上的“节点”以打开“节点”屏幕。
2. 在工具栏上单击“添加”，然后在弹出式菜单上单击“从 vCenter/ESX 导入虚拟机”。
“发现节点”对话框将打开。

3. 完成“发现节点”对话框中的以下字段：

- vCenter/ESX 主机

注意：作为最佳实践，如果在环境中运行 VMware Distributed Resource Scheduling (DRS)，则导入虚拟机时应指定 vCenter Server 系统的主机名或 IP 地址。该方法确保 CA ARCserve Central HostBased VM Backup 可以检测到在您的环境中运行的虚拟机并且启用 DRS 的虚拟机的备份成功完成。虚拟机跨 ESX 服务器移动时，为了防止备份失败，建议在导入虚拟机时，不指定 ESX 服务器的主机名或 IP 地址。

有关 Distributed Resource Scheduling 的更多信息，请参阅 VMware 网站。

- 用户名
- 密码
- Port
- 协议

单击“连接”并等待扫描完成。

4. （可选）启用选项“自动将 vCenter/ESX 服务器添加到发现列表中”。

5. 单击“下一步”打开“节点凭据”对话框。

6. 在“节点凭据”屏幕上，为检测到的所有虚拟机提供全局用户名和密码，然后单击“应用于所选”选项。也可以单击某个 VM 输入特定凭据。

7. 单击“完成”。

您选择的虚拟机将添加到指定的节点组中。

注意：CA ARCserve Central HostBased VM Backup 无法检测到处于关机状态或未安装 VMware Tools 的虚拟机的主机名。在这些状况下，在您导入节点之后，“未知”显示在节点屏幕上的“主机名”字段中。此外，“节点名称”筛选（在“节点”屏幕上）无法筛选使用“Unknown”命名的节点。

更新节点

CA ARCserve Central HostBased VM Backup 允许您更新以前添加的节点的信息。

遵循这些步骤:

1. 登录该应用程序。
从主页上的导航栏，单击“节点”。
“节点”屏幕将显示。
2. 从“组”栏上，单击“全部节点”组，或单击包含要更新的节点的组名称。
与该组关联的节点显示在节点列表中。
3. 单击想要更新的节点，然后右键单击，并从弹出菜单单击“更新节点”。
“更新节点”对话框将打开。
注意: 要更新节点组的所有节点，请右键单击节点组名，然后从弹出式菜单单击“更新节点”。
4. 根据需要更新节点详细信息。
注意: 要更新“节点”列表上的多个节点，请选择所需的节点、右键单击任何节点，然后从弹出式菜单中单击“更新节点”。用户名和密码对于选定的所有节点而言都是相同的。默认情况下，已选中“指定新凭据”选项和“控制节点”复选框。您可以为选定节点指定新用户名和密码，并可强制此服务器管理这些节点。此外，您还可以选择“使用现有的凭据”来应用当前的用户名和密码。字段将被禁用。
5. 单击“确定”。
“更新节点”对话框关闭，节点即被更新。

更改 CA ARCserve Central Applications 服务器的主机名后更新节点和策略

更改 CA ARCserve Central HostBased VM Backup 服务器的主机名后，更新节点以及应用于这些节点的策略。执行这些任务以维护服务器与该服务器保护的节点之间的关系。下表说明可能的状况以及针对每一状况的解决措施。

状况	解决措施:
节点在 CA ARCserve Central HostBased VM Backup 服务器的主机名更改后被添加。	无需解决措施。

状况	解决措施:
节点在 CA ARCserve Central HostBased VM Backup 服务器的主机名更改之前被添加，策略未应用到节点。	更新节点。有关详细信息，请参阅 更新节点 (p. 44) 。
节点在 CA ARCserve Central HostBased VM Backup 服务器的主机名更改之前被添加，策略应用到节点。	重新应用策略。有关详细信息，请参阅“将策略分配给虚拟机”。

删除节点

您可以根据需要删除节点。

遵循这些步骤:

1. 登录该应用程序。
单击导航栏上的“节点”以打开“节点”屏幕。
2. 从“组”栏上，单击“全部节点”组，或单击包含要删除的节点的组名称。
与该组关联的节点显示在节点列表中。
3. 选中想要删除的一个或多个节点，然后单击工具栏上的“删除”。
将显示一条确认消息。
4. 执行以下操作之一：
 - 单击“是”即可删除该节点。
 - 如果您不想删除该节点，请单击“否”。

合并作业选项

通过 CA ARCserve Central HostBased VM Backup，您可以在任何时候暂停并恢复每个节点的合并作业。暂停并恢复合并作业的过程不会影响正在进行的作业。

暂停节点上的合并作业

通过 CA ARCserve Central HostBased VM Backup，您可以暂停特定节点上的合并作业。

例如，合并作业可以消耗系统资源并导致备份作业缓慢运行。使用暂停选项停止正在进行的合并作业，以便正在进行的备份作业可以其最高的效率完成。备份完成之后，您可以恢复合并作业。

遵循这些步骤:

1. 在 CA ARCserve Central HostBased VM Backup 主页中，单击导航栏上的“节点”打开“节点”屏幕。
2. 选择节点组，该组包含要暂停的合并作业的节点。
将显示选定节点组的节点列表。
3. 单击要暂停的合并作业的节点。然后右键单击选定的节点，单击弹出式菜单中的“暂停合并作业”。

注意: 默认情况下，“暂停合并作业”选项被禁用。节点正在运行合并作业时，正如在作业列中所示，“暂停合并作业”选项变为启用。

暂停选定节点的合并作业且在 CA ARCserve D2D 主页上进行验证。

恢复节点上合并作业

通过 CA ARCserve Central HostBased VM Backup，您可以恢复特定节点上的已暂停合并作业。

遵循这些步骤:

1. 在 CA ARCserve Central HostBased VM Backup 主页中，单击导航栏上的“节点”打开“节点”屏幕。
2. 选择节点组，该组包含要恢复的合并作业的节点。
将显示选定节点组的节点列表。
3. 单击已暂停现在又要恢复的合并作业的节点。然后右键单击选定的节点，单击弹出式菜单中的“恢复合并作业”。

注意: 备份作业未在运行且合并作业暂停时，“恢复合并作业”选项启用。

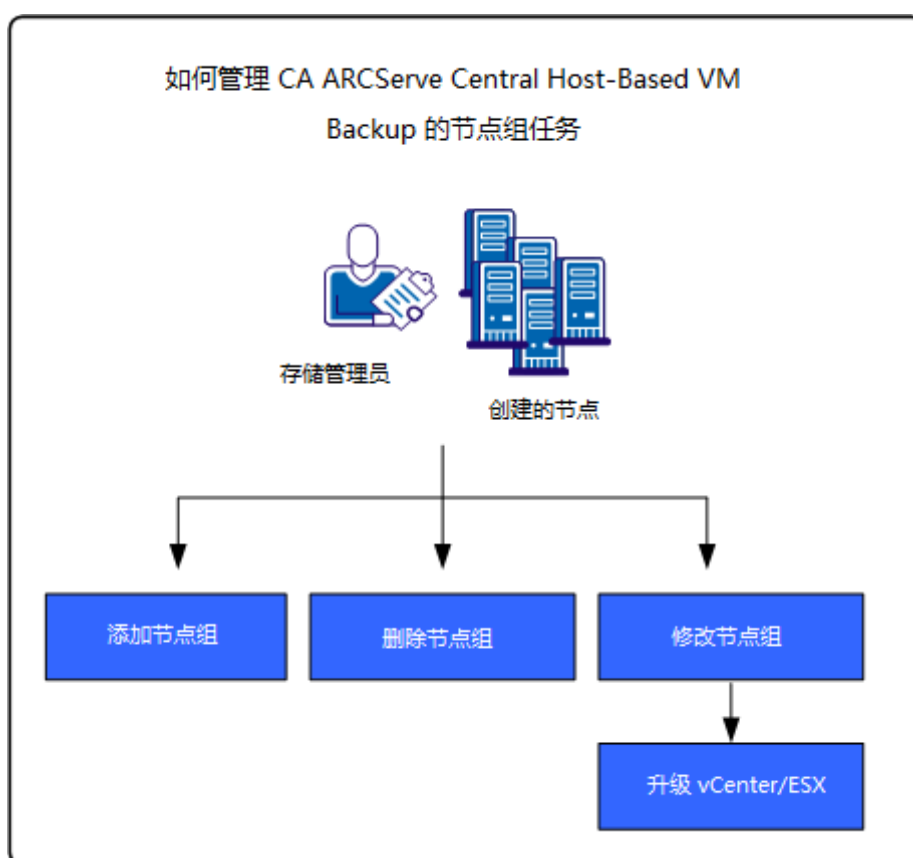
恢复选定节点的合并作业且在 CA ARCserve D2D 主页上进行验证。

如何管理 CA ARCserve Central HostBased VM Backup 的节点组任务

通过 CA ARCserve Central HostBased VM Backup，存储管理员可以轻松保护多个虚拟机，如同保护一个虚拟机一样。

首先添加节点。您可以按应用程序或节点用途对这些节点进行分组。通过创建节点组，可以轻松实现虚拟机环境可视化。您可以创建备份策略并将策略分配给节点，以简化虚拟环境的保护。有关更多详细信息，请参阅[如何管理 CA ARCserve Central HostBased VM Backup 的策略](#) (p. 67)。

下图介绍了可以对节点组执行的任务：



此场景介绍了以下主题：

- [添加节点组](#) (p. 48)
- [删除节点组](#) (p. 50)
- [修改节点组](#) (p. 51)

添加节点组

当您首先从 ESX 或 vCenter 服务器主机导入虚拟机时，新的节点组会自动被添加。

节点组让您基于共同特征管理一批 CA ARCserve D2D 源计算机。例如，您可以定义按他们支持的部门分类的节点组：会计、营销、法律，人力资源等等。

应用程序包含以下节点组：

■ 默认组：

- **全部节点** -- 包含与该应用程序关联的所有节点。
- **没有组的节点** -- 包含所有与应用程序关联且未被分配给节点组的所有节点。
- **没有策略的节点** -- 包含所有与应用程序关联且未分配策略的所有节点。
- **SQL Server** -- 包含与该应用程序关联且安装 Microsoft SQL Server 的所有节点。
- **Exchange** -- 包含与该应用程序关联且安装 Microsoft Exchange Server 的所有节点。

注意： 您不能修改或删除默认节点组。

- **自定义组** -- 包含自定义的节点组。
- **vCenter/ESX 组** -- 通过“从 vCenter/ESX 导入虚拟机”选项添加节点时，vCenter/ESX 服务器的名称将添加到该组。

遵循这些步骤：

1. 登录该应用程序。
从主页上的导航栏中，单击“节点”打开“节点”屏幕。
2. 单击“节点组”工具栏上的“添加”。
“添加组”对话框打开，节点显示在“可用节点”列表中。
3. 指定节点组的组名称。
4. 在“添加组”对话框上指定以下字段：
 - **组** -- 选择包含想要分配的节点的组名称。
 - **节点名称筛选** -- 允许您基于通常标准筛选可用节点。

注意： “节点名称筛选”字段支持使用通配符。

例如，Acc* 允许您筛选节点名称以 Acc 开头的所有节点。要清除筛选结果，请单击“筛选”字段中的 X。

5. 要将节点添加到节点组中，请选择想要添加的节点，然后单击向右单箭头。

这些节点便从“可用节点”列表移到“选定的节点”列表中，并被分配给节点组。

注意：要从当前组选择并移动所有节点，请单击向右双箭头。

6. （可选）要将节点从“选定的节点”列表中移到“可用节点”列表，请单击向左单箭头。

注意：要选择并移动当前组中的所有节点，请单击向左双箭头。

7. 单击“确定”。

节点组即被添加。

删除节点组

您可以根据需要删除节点组。当您删除手工添加的组时，不会从应用程序中删除虚拟机。但是，如果您删除从 ESX 或 vCenter Server 发现自动创建的组，则该组及所有虚拟机便从应用程序中被删除。

该应用程序使您可以删除已创建的节点组。

您不能删除以下节点组：

- **全部节点** -- 包含与该应用程序关联的所有节点。
- **没有组的节点** -- 包含所有与应用程序关联且未被分配给节点组的所有节点。
- **没有策略的节点** -- 包含所有与应用程序关联且未分配策略的所有节点。
- **SQL Server** -- 包含与该应用程序关联的所有节点，并且在这些节点中安装 Microsoft SQL Server。
- **Exchange** -- 包含与该应用程序关联的所有节点，并且在这些节点中安装 Microsoft Exchange Server。

注意：删除节点组的过程不会从应用程序中删除单个节点。

遵循这些步骤：

1. 登录该应用程序。
从主页上的导航栏中，单击“节点”打开“节点”屏幕。
2. 单击要删除的节点组，然后单击“节点组”工具栏中的“删除”。
“确认”消息对话框打开。
3. 如果确定要删除该节点组，请单击“是”。

注意：如果您不想删除该节点组，请单击“否”。

节点组即被删除。

修改节点组

该应用程序使您可以修改已创建的节点组。您可以从节点组添加和删除节点，并更改节点组的名称。

注意： 您不能修改以下节点组：

- **全部节点** -- 包含与该应用程序关联的所有节点。
- **没有组的节点** -- 包含所有与应用程序关联且未被分配给节点组的所有节点。
- **没有策略的节点** -- 包含所有与应用程序关联且未分配策略的所有节点。
- **SQL Server** -- 包含与该应用程序和安装的 Microsoft SQL Server 关联的所有节点。
- **Exchange** -- 包含与该应用程序和安装的 Microsoft Exchange Server 关联的所有节点。

遵循这些步骤：

1. 登录该应用程序。
从主页上的导航栏，单击“节点”。
“节点”屏幕将显示。
2. 单击想要修改的节点组，然后单击“节点组”工具栏的“修改”。
“修改组”对话框打开。
3. 要修改组名称，请在“组名称”字段指定新名称。
4. 要将节点添加到节点组中，请选择想要添加到该节点组的节点，然后单击向右箭头。
这些节点便从“可用节点”列表移到“选定的节点”列表中，并被分配给节点组。
注意： 要将所有节点从“可用节点”列表移到“选定的节点”列表中，请单击向右双箭头。
5. 要从节点组中删除节点，请单击向左箭头或向左双箭头，分别删除一个或全部节点。

6. （可选）要基于通常标准筛选可用节点，请在“节点名称筛选”字段中指定筛选值。

注意：“筛选”字段支持使用通配符。

例如，Acc* 允许您筛选节点名称以 Acc 开头的所有节点。要清除筛选结果，请单击“筛选”字段中的 X。

7. 单击“确定”。

节点组即被修改。

更新 vCenter 和 ESX 服务器详细信息

CA ARCserve Central HostBased VM Backup 允许您更新先前添加的 vCenter 和 ESX 服务器详细信息。

遵循这些步骤：

1. 在“节点”屏幕中，从“组”栏展开“vCenter/ESX 组”。
2. 选择要更新服务器详细信息的 vCenter/ESX 组，右键单击，然后单击“更新 vCenter/ESX”。

此时将打开“更新 vCenter/ESX”对话框。

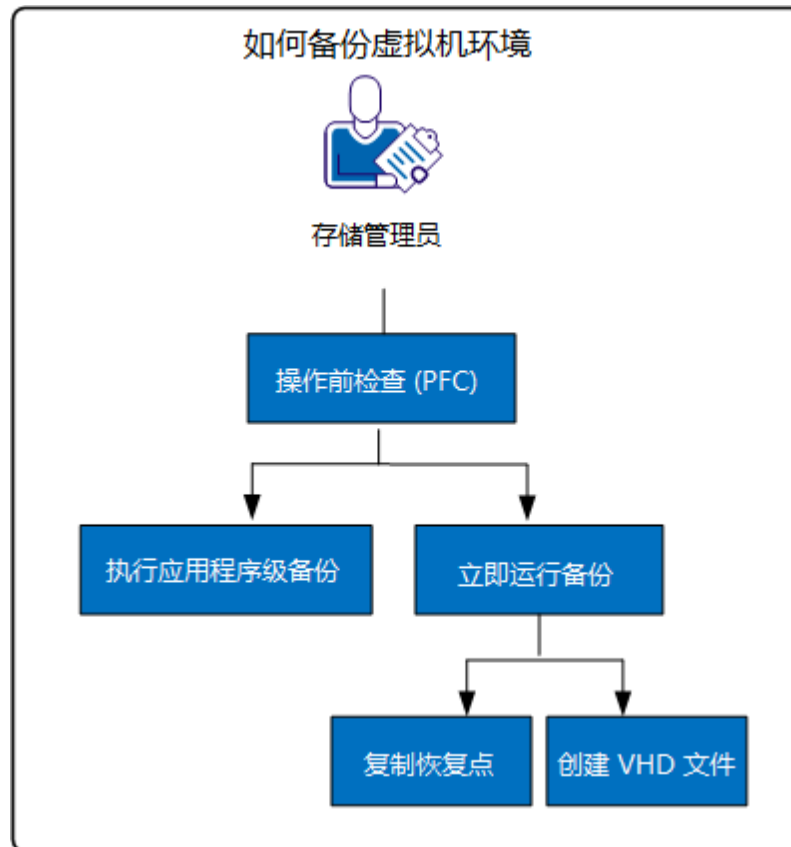
3. 相应地更新 vCenter/ESX 服务器详细信息。
4. 单击“确定”。

“更新 vCenter/ESX”对话框将关闭，节点组即被更新。

如何备份虚拟机环境

此场景介绍了存储管理员如何备份和保护您环境中的所有虚拟机。

下图说明了如何备份虚拟机环境。



以下列表介绍了图中所示的过程：

- [执行备份作业的操作前检查](#) (p. 54)
- [立即运行备份](#) (p. 58)
 - [复制备份恢复点](#) (p. 61)
 - [创建 VHD 文件](#) (p. 64)
- [执行应用程序级备份](#) (p. 64)

执行备份作业的操作前检查

CA ARCserve Central HostBased VM Backup 功能中包括一个名为“操作前检查 (PFC)”的实用工具，可针对特定节点运行重要检查，以检测可导致备份作业失败的条件。执行以下操作时，将自动运行 PFC：

- 从 vCenter Server/ESX Server 系统导入虚拟机
- 从发现结果添加节点
- 更新节点

此外，您还可以手动执行操作前检查。

遵循这些步骤：

1. 登录该应用程序。
单击导航栏上的“节点”以打开“节点”屏幕。
2. 执行以下操作之一，以指定要从中运行操作前检查的节点：
 - **节点级别：**单击包含要运行操作前检查的节点的组，然后单击节点旁边的复选框。右键单击节点，然后从上下文菜单中单击“操作前检查”。
 - **组级别：**右键单击包含节点的组，然后单击“操作前检查”。
将显示一条消息“开始对虚拟机进行操作前检查”。
3. 滚动到“PFC 状态”列，然后查看操作前检查的状态。

下表介绍了 PFC 执行的检查：

项目	说明
更改块跟踪 (CBT)	(CBT) 是一种跟踪虚拟机上更改的磁盘扇区的功能。这有助于最大程度地减小备份大小。 该项目可确认 CBT 是否已启用。
VMware Tools	该项目可确认是否在每台虚拟机上都安装了 VMware Tools。
磁盘	此项检验虚拟机的磁盘。
电源状态	该项目可确认虚拟机是否已打开。
Credentials	该项目可确认用户凭据是否有效。
应用程序	该项目可确认是否已安装 Microsoft SQL Server 和 Microsoft Exchange Server。

有关解决操作前检查结果的错误和警告的详细信息，请参阅主题[操作前检查项目的解决方案](#) (p. 55)。

操作前检查项目的解决方案

下表介绍了可帮助您解决操作前检查结果中的错误和警告的解决方案：

更改块跟踪 (CBT)

状态	消息	解决方法
警告	已对现有快照启用更改块跟踪。将应用完全磁盘备份。	<p>要应用使用的快备份，请执行以下步骤：</p> <ol style="list-style-type: none"> 1. 删除与虚拟机关联的所有快照。 2. 登录到 Host-Based VM 代理服务。 3. 打开注册表编辑器，并找到以下注册表项： HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\<VM-InstanceUUID> <p>注意：将 <VM-InstanceUUID> 替换成 CBT 失败的虚拟机的 UUID 值。该值可以在连接到 CA ARCserve D2D 时所使用的虚拟机的 URL 中找到。</p> <ol style="list-style-type: none"> 4. 将注册表项设置为 "full disk backupForFullBackup"=0。 5. 创建/设置注册表项 ResetCBT=1。 6. 提交备份作业。

VMware Tools

状态	消息	解决方法
警告	过时。	安装 VMware Tools 的最新版本。
警告	未安装或未运行。	安装 VMware Tools 的最新版本并确保该工具正在运行。

磁盘

状态	消息	解决方法
错误	VM 不支持 VM 快照，因为它具有为共享总线配置而配置的 SCSI 控制器。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 VM。
警告	物理裸设备映射 (RDM) 磁盘不会被备份。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 VM。
警告	虚拟裸设备映射 (RDM) 磁盘将作为完整磁盘进行备份。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 VM。
警告	独立磁盘不会被备份。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 VM。
警告	应用程序将 NFS 数据存储上的磁盘作为完整磁盘进行备份。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 VM。

电源状态

状态	消息	解决方法
警告	已关闭	打开虚拟机。
警告	已挂起	打开虚拟机。

Credentials

状态	消息	解决方法
警告	不正确凭据。	提供有效的用户凭据。
警告	未提供。	提供有效的用户凭据。

应用程序

状态	消息	解决方法
警告	不支持应用程序级还原，因为 VM 具有 IDE 磁盘。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 Microsoft SQL Server 和 Exchange Server 数据。
警告	主机服务器上未安装 VMware VIX。	从 VMware 网站下载 VIX 并将其安装在 CA ARCserve Central Applications 主机服务器上。
警告	CA ARCserve Central HostBased VM Backup 服务器上的 VMware VIX 过时。	从 VMware 网站下载 VIX 并将其安装在 CA ARCserve Central Applications 主机服务器上。
警告	不支持应用程序级还原，因为不支持 ESX Server。	将 ESX Server 升级到 4.1 或更高版本，或者使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 Microsoft SQL Server 和 Exchange Server 数据。
警告	不支持应用程序级还原，因为没有足够的 SCSI 插槽可以使用。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 Microsoft SQL Server 和 Exchange Server 数据。
警告	源位于动态磁盘上。不支持应用程序级还原。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 Microsoft SQL Server 和 Exchange Server 数据。 注意: 在装有 Windows Server 2008 或更高版本且在 ESX Server 4.1 或更高版本上运行动态磁盘的虚拟机上，VMware 不支持应用程序级别的静止。

状态	消息	解决方法
警告	无法检索应用程序的有关信息。这会阻碍应用程序级备份成功完成。	提供内置或域管理员凭据，以登录到虚拟机来宾操作系统。 由于 VMware 限制，仅支持在具有付费许可的 ESX 服务器上运行的 VM 上进行备份。不支持在具有免费许可的 ESXi 服务器上备份。
警告	启用存储空间的系统不支持应用程序级恢复。仅可以恢复整个虚拟机。	使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 来备份 Microsoft SQL Server 和 Microsoft Exchange Server 数据。

立即运行备份

通常，备份自动执行，并由排定设置控制。然而，可能有些时候您需要立即执行临时备份（完全、增量或验证）。

临时备份基于需要，而不是作为备份计划的一部分而提前排定。例如，如果您有针对完全、增量和验证备份的重复排定，并且您想对计算机做重大更改，则应立即执行临时备份，而不是等候下一个排定备份发生。

临时备份还允许您添加自定义（未排定）恢复点，以便可以在必要时回滚到这个之前的时间点。例如，如果安装修补程序或 Service Pack 后发现它降低了计算机的性能，您可能希望回滚到不包括该修补程序或 Service Pack 的临时备份会话。

遵循这些步骤:

1. 登录该应用程序。
2. 从主页上的导航栏中，单击“节点”打开“节点”屏幕。
3. 要指定希望备份的节点，请执行以下操作之一：
 - **节点级别：**单击包含想要备份的节点的组，然后单击想要备份的节点旁边的复选框。
 - **组级别：**单击包含想要备份的节点的组。
4. 然后执行下列操作之一备份节点：
 - 单击工具栏上的“备份”。
 - 右键单击选定的组或右键单击节点，然后单击上下文菜单上的“立即备份”。

5. 在“立即运行备份”对话框上，单击下列类型之一以指定备份类型：
 - **完全备份** -- 启动您的整个计算机或选定卷的完全备份。
 - **增量备份** -- 启动您的计算机的增量备份。增量备份仅备份自上一次备份以来已经更改的块。

注意：增量备份的优势在于，备份速度快且生成的备份映像较小。这是执行备份的最理想方式。
 - **验证备份** -- 通过检查每个块的最近备份并将内容和信息与原始源进行对比，而启动整个计算机的验证备份。这种对比将确认最新备份的块代表源的相应信息。如果任何块的备份映像不匹配源，CA ARCserve D2D 将刷新（重新同步）不匹配块的备份。请注意执行验证备份的以下优势和劣势：
 - 优势—与完全备份相比，由于仅备份更改块（与上次备份不匹配的块），因此验证备份生成的备份映像非常小。
 - 劣势—由于要将所有的源磁盘块与上次备份的块进行比较，因此备份时间较长。

注意：如果向备份源添加了一个新卷，则无论选择何种总体备份方法，都会完全备份新添加的卷。
6. （可选）指定备份名称，然后单击“确定”。如果不指定名称，默认情况下会将其命名为 Customized/Full/Incremental/Verify Backup。

出现确认屏幕，选定类型的备份立即启动。

请注意以下行为：

- 在“策略”对话框中指定的所有值均应用于作业。
- 如果自定义（临时）备份作业失败，将不创建补充作业。仅会为失败的排定作业创建补充作业。
- CA ARCserve Central HostBased VM Backup 会按优先级顺序应用以下备份作业：
 - 完全
 - 校验
 - 增量

如果提交了“立即备份”作业并且有作业正在队列中等候，则会发生以下情况：

- 如果提交了“完全备份”作业并且有“验证备份”作业正在队列中等候，则“完全备份”作业会覆盖队列中的“验证备份”作业。
- 如果提交了“完全备份”作业并且有“增量备份”作业正在队列中等候，则“完全备份”作业会覆盖队列中的“增量备份”作业。
- 如果提交了“验证备份”作业并且有“增量备份”作业正在队列中等候，则“验证备份”作业会覆盖队列中的“增量备份”作业。
- 如果提交了“验证备份”作业并且有“完全备份”作业正在队列中等候，则会跳过“验证备份”作业。
- 如果提交了“增量备份”作业并且有“完全备份”作业正在队列中等候，则会跳过“增量备份”作业。
- 如果提交了“增量备份”作业并且有“验证备份”作业正在队列中等候，则会跳过“增量备份”作业。

复制恢复点

每次 CA ARCserve D2D 执行了成功的备份后，备份的时间点快照映像也会被创建。这组恢复点允许您精确找到和指定要复制的备份映像。您可以执行以下操作来保护备份：

- 复制/导出恢复点信息，以便在发生大灾难时将其安全存储在异地。
- 将恢复点保存到多个位置。
- 如果您的目标即将变满，但您仍想保留所有恢复点，那么合并您的备份。

当您选择恢复点进行复制时，还会同时捕获重新创建完全且最新的备份映像所需的所有以前的备份块。

遵循这些步骤：

1. 登录该应用程序。

单击导航栏上的“节点”以打开“节点”屏幕。

2. 在“组”列表中，单击“全部节点”，或单击包含含有您要复制的恢复点的 CA ARCserve D2D 节点的组。

节点列表显示与指定组关联的所有节点。

3. 浏览并单击要登录的节点，然后从弹出菜单单击“登录 D2D”。

CA ARCserve D2D 随即打开，您便登录到 CA ARCserve D2D 节点的主页。

注意： 帮助确保已启用浏览器窗口上的弹出选项。

4. 从 CA ARCserve D2D 主页选择“复制恢复点”。

“复制恢复点”对话框将打开。

5. 在“备份位置”字段中，指定备份源。您可以指定一个位置或浏览到存储备份映像的位置。您可以单击绿色箭头图标按钮来验证到指定位置的连接。必要时，输入用户名和密码凭据以获得该位置的访问权限。

6. 在“虚拟机”字段中，单击“选择虚拟机”旁边的下拉列表，以指定包含要复制的恢复点的虚拟机。

日历视图突出显示在显示的时间段内包含该备份源的恢复点的所有日期。

7. 指定恢复点进行复制。

a. 选择您想复制的备份映像的日历日期。

将显示该日期的相应恢复点，以及备份时间、执行的备份类型以及备份名称。

注意：具有锁符号的时钟图标表示恢复点包含加密信息，需要密码才能还原。

b. 选择想要复制的恢复点。

将显示该恢复点的相应备份内容（包括任何应用程序）。

8. 单击“下一步”。

此时将打开“复制选项”对话框。

注意：该对话框中显示两个密码字段。“密码”字段用于使用密码解密源会话，“加密密码”字段用于加密目标会话。

a. 如果导出的恢复点先前已加密，则需要密码。

- 如果导出的恢复点是运行复制恢复点作业的同台计算机的备份会话，将会保存并自动填充加密密码。
- 如果导出的恢复点是其他计算机的备份会话，则需要加密密码。

b. 选择目标。

您可以指定一个位置或浏览到存储选定恢复点的副本的位置。您可以单击绿色箭头图标按钮来验证到指定位置的连接。必要时，请输入用户名和密码。

c. 选择要执行的压缩级别。

注意：指定的备份压缩级别与复制压缩级别无关。例如，在备份目标中，压缩级别可设为“标准”；但是，当您提交复制作业时，压缩可以更改为“无压缩”或“最大压缩”。

执行压缩会减少对磁盘空间的占用，而且还可以抵消由于对 CPU 越来越多的占用而导致对备份速度产生负面影响。

可用的选项包括：

- **无压缩**—不执行压缩。文件是纯 VHD。此选项的 CPU 使用率最低（速度最快），但是对于您的备份映像而言，磁盘空间占用最大。
- **标准压缩**—执行部分压缩。此选项将会在 CPU 使用率和磁盘空间占用之间实现良好的平衡。此选项是默认设置。
- **最大压缩**—执行最大压缩。此选项提供最高的 CPU 使用率（速度最慢），但是对于备份映像而言，磁盘空间占用最低。

请考虑以下几点：

- 如果您的备份映像包含不可压缩的数据（如 JPG 图像、ZIP 文件），将需要额外的存储空间来处理此类数据。因此，如果在备份中有不可压缩的数据时选择任意压缩选项，实际上可能导致增加使用的磁盘空间。
- 如果将压缩级别从“无压缩”更改为“标准压缩”或“最大压缩”，或者从“标准压缩”或“最大压缩”更改为“无压缩”，则更改之后首次执行的备份将自动成为完全备份。在完全备份执行后，所有未来的备份（完全、增量或验证）将按排定执行。

d. 如果您还想要加密复制的恢复点，请输入以下信息：

您可以为复制的恢复点更改、添加，或删除加密。

- 选择要用于副本的加密算法类型。
可用的格式选项是“不加密”、AES-128、AES-192 和 AES-256。
- 提供（并确认）加密密码。

9. 单击“创建副本”。

状态通知窗口将出现，选定恢复点类型的复制过程将立即启动。

注意：CA ARCserve D2D 一次仅允许一个恢复点复制作业运行。

恢复点映像将从备份源复制到复制目标。

从 CA ARCserve Central HostBased VM Backup 创建 VHD 文件

该 CA ARCserve D2D 过程允许您从每次成功备份后创建的恢复点创建虚拟硬盘 (VHD) 文件。有关详细信息，请参阅 CA ARCserve D2D “附录”。

遵循这些步骤:

1. 执行[复制恢复点](#) (p. 61)过程。
2. 当复制完成时，浏览至您指定的目标，并导航至 CA ARCserve D2D 主机。
3. 打开文件夹 VStore\S0000000001。
4. 查找扩展名为 D2D 的所有文件，并将所有扩展名更改为 VHD。将所有文件重命名后，您便可以将它们用作常规 VHD 文件。

执行应用程序级备份

通常，保护 Microsoft Exchange 或 SQL Server 系统不需要执行特殊步骤。

要执行完全应用程序备份，请确保已确认以下几点：

- 所有应用程序编写器处于稳定状态。使用 *vssadmin* 查看编写器状态。
- 备份的所有数据库都处于正常状态。例如，对于 SQL Server，请确保数据库状态不是“正在还原”。

您还可以分别截断 SQL 和 Exchange Server 的事务日志。

注意：升级到 ESX 服务器时，在来宾操作系统内升级 VMware Tools，然后执行应用程序级备份，以避免“过期”错误。

执行仅包含已用块数据的的完全磁盘备份。

在执行完全磁盘备份之后检索已用块数据，有助于减少备份窗口，并减少备份目标的空间要求。

注意：由于 VMware 限制，恢复点快照存在时，将无法从虚拟机检索已用块。在这种情况下，将在虚拟机上执行完全磁盘备份。

提交完全磁盘备份后，执行以下步骤以检索已用块数据：

1. 删除与虚拟机关联的所有快照。
2. 登录到 CA ARCserve Central HostBased VM Backup 虚拟机。
3. 打开注册表编辑器，并找到以下注册表项：
HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\VM_InstanceUUID
4. 将注册表项 “full disk backupForFullBackup” 设置为 0。
5. 创建或设置注册表项 “ResetCBT” 到 1。
6. 提交备份作业。

查看作业状态信息

CA ARCserve Central Virtual Standby 将 CA ARCserve D2D 恢复点转换为恢复点快照。您可以查看有关正在进行的 Host-Based VM Backup 作业的状态信息。

作业正在运行时，您可以查看有关该作业的详细信息。也可以停止当前作业。

遵循这些步骤：

1. 登录该应用程序。
2. 单击导航栏上的“节点”以打开“节点”屏幕。
3. 如果具有正在进行的 Host-Based VM Backup 作业，将在“作业”字段中显示作业的阶段，如以下屏幕中所示：

节点名称	策略	虚拟机名称	vCenter/ESX	作业
██████████	新策略	██████████	*****	正在开始备份

- 单击阶段可打开“备份状态监视器”对话框。

注意：有关“备份状态监视器”中显示的字段的信息，请参阅“[备份状态监视器 \(p. 66\)](#)”。

- 执行以下选项之一：

- 单击“关闭”以关闭“备份状态监视器”对话框。
- 单击“取消”以停止当前作业。

注意：单击“取消”后，很快就会关闭“备份状态监视器”对话框。

更多信息：

[查看作业状态信息 \(p. 65\)](#)

基于主机的 VM 备份监视作业

您可以从“节点”屏幕查看虚拟机备份的状态。从“作业”字段中搜索具有正在进行的作业的节点，然后单击链接，即可打开此对话框。

虚拟机备份分两个阶段执行。首先，备份虚拟硬盘，然后，生成编录（如果备份成功）。编录允许您还原文件和文件夹以及整个虚拟机。

监视器显示了有关备份状态作业的以下实时信息：

- **阶段一（备份和编录监视器）**显示此过程中的当前点，以进度条的阴影部分表示。
- **开始时间一（备份和目编录监视器）**显示基于策略配置启动操作的日期和时间。
- **已用时间一（备份和编录监视器）**显示开始时间与当前时间之间的差异。
- **预计剩余时间一（仅限备份监视器）**显示预计完成作业所需的时间。
- **正在处理一（仅限编录监视器）**显示当前正在为其生成编录的卷驱动器号或应用程序。
- **因压缩而节省的空间一（仅限备份监视器）**显示在备份操作策略中指定压缩时节省的磁盘空间部分。
- **压缩级别一（仅限备份监视器）**显示用于备份的压缩类型。选项包括“无压缩”、“标准压缩”（默认设置）或“最大压缩”。
- **加密一（仅限备份监视器）**显示配置备份作业时选择的加密方法。

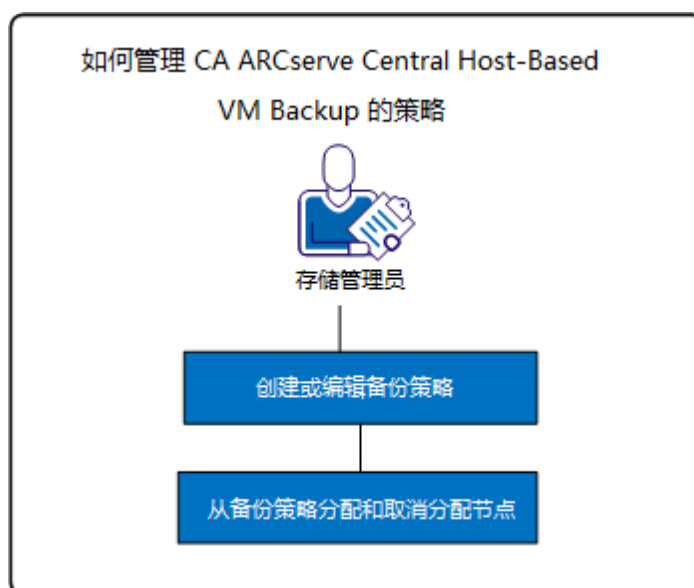
- **写速度限制**—（仅限备份监视器）如果在备份策略的“保护设置”屏幕上设置了“调节备份”，则显示该值。
- **写速度**—（仅限备份监视器）显示实际写速度（以 MB/分钟为单位）。
- **读取速度**—（仅限备份监视器）显示实际读取速度（以 MB/分钟为单位）。

如何管理 CA ARCserve Central HostBased VM Backup 的策略

备份策略定义如何以及何时备份从 vCenter/ESX 服务器导入的节点。存储管理员可以创建和编辑备份策略，然后将这些策略分配给节点或从节点取消分配。

注意：可以将一个策略分配给一个或多个节点。但是，不能将一个或多个策略分配给一个节点。

下图说明了管理备份策略的过程。



以下列表介绍了图中所示的过程：

- [创建备份策略](#) (p. 68)
- [编辑备份策略](#) (p. 72)
- [从备份策略分配和取消分配节点](#) (p. 74)

创建备份策略

创建备份策略的过程使用 CA ARCserve D2D 界面来配置备份设置，具有少许差异。您可以创建基于类似备份需求（例如，按已安装应用程序或排定）的策略。

以下过程概述了创建简单的 CA ARCserve D2D 备份作业策略所需的步骤。有关创建 CA ARCserve D2D 备份策略的完整详细信息，请参阅附录中相应的 CA ARCserve D2D 主题。

注意：在基于主机的备份操作期间，如果您正使用 hotadd 作为传输模式，以下消息将出现：

在可以使用在驱动器 <driveLetter> 中的磁盘前，您需要格式化它。要格式化它吗？

单击“取消”忽略该消息。操作系统检测到虚拟硬盘添加到备份代理服务器时，会显示该消息。操作系统假定虚拟硬盘是需要格式化的新设备。如果错误地单击“格式化磁盘”，不会造成任何损失，因为虚拟硬盘是只读的。

遵循这些步骤：

1. 登录该应用程序。
单击导航栏上的“策略”以打开“策略”屏幕。
2. 单击工具栏上的“新建”以打开“新建策略”对话框。
3. 输入正确说明该策略的“策略名称”。

4. 在“备份设置”选项卡上，单击“保护设置”并指定以下信息：
 - **备份目标** — 指定要用于保存备份会话的本地卷或远程共享文件夹。
 - **CA ARCserve D2D VM 备份代理** — 指定安装了 CA ARCserve D2D 的服务器的主机名或 IP 地址。如果尚未安装 CA ARCserve D2D，您可以使用 CA ARCserve Central Protection Manager 来部署它。为该服务器提供适当的凭据。默认情况下，端口号为 8014。如果您在 CA ARCserve D2D 安装期间更改了该默认值，请指定正确的端口号。
 - **保留设置** -- 您可以根据要保留的恢复点数量（合并会话）或根据要保留的恢复集数量（删除恢复集并禁用无限增量）来设置保留策略。默认选项是“保留恢复点”。有关详细信息，请参阅《CA ARCserve Central Protection Manager 用户指南》中的“指定保护设置”。
 - **压缩** — 选择压缩级别。默认值为“标准压缩”。您可以选择不压缩或“最大压缩”。
 - **加密** — 指定加密级别。默认值为“不加密”。指定加密级别时，请提供用于还原加密数据的加密密码。
 - **调节备份** — 输入备份写入磁盘的比率。降低该比率可减少 CPU 或网络负载，但是请注意，这样做会增加备份时间。默认情况下，该选项被禁用。
5. 单击“排定”并填写以下信息：
 - **开始日期和时间** — 指定您想要开始备份作业的日期和时间。
 - **增量备份** — 定义您的增量备份作业的重复排定。默认值是每天重复一次“增量备份”。
 - **完全备份** — 定义您的完全备份作业的重复排定。默认情况下，此值设置为“从不重复”。
 - **验证备份** — 定义验证备份作业的重复排定。默认情况下，此值设置为“从不重复”。

6. 单击“高级”并填写以下信息：
 - **截短日志** -- 如果您想要截短应用程序日志文件，请启用下列选项：
 - **SQL Server** — 指定每日、每周或每月的截短排定。
 - **Exchange Server** — 指定每日、每周或每月的截短排定。
 - **在目标上保留空间** -- 指定为执行一次备份所要保留的空间百分比。该持续空间量会即刻在目标上得到保留，然后备份才开始写数据，这将有助于提高备份速度。
 - **编录** -- 选择每次备份后生成文件系统编录以实现更快搜索的选项以减少浏览器搜索等待时间。

如果未选中该选项，可以在备份后立即执行还原，无需等待编录作业完成。默认情况下，未启用该选项。请注意以下事项：

 - 为每个备份作业生成文件系统编录时，它会增加存储元数据文件和编录文件所需的磁盘存储量以及 CPU 使用量。此外，如果备份源包含许多文件，生成编录的过程可能非常耗时。
 - 选择 ReFS 卷作为备份源时，无法生成编录。之后，警告消息显示向您通知这种情况。
7. 单击“先行/后继备份设置”，并指定任何所需的先行/后继备份命令。在需要时提供适当的凭据：
 - **在备份启动之前运行命令** — 输入在开始备份作业之前运行的脚本命令。
 - **退出代码** -- 如果您想针对特定的退出代码触发脚本命令，请启用该选项。
 - **运行作业** — 如果已选定，软件会在返回指定的退出代码时继续运行作业。
 - **让作业失败** — 如果已选定，软件会在返回指定的退出代码时中止备份作业。
 - **在拍取快照之后运行命令** — 输入拍取快照之后运行的脚本命令。
 - **在备份结束之后运行命令** — 输入备份完成之后运行的脚本命令。

8. (可选)单击“首选项”选项卡。根据需要配置以下任一电子邮件报警:

- 错过的作业
- 无法连接 vCenter/ESX (备份前)
- 许可故障
- 备份、编录、还原或复制作业失败/崩溃/取消
- 备份、编录、还原或复制作业成功
- 目标可用空间少于
- 合并作业已停止、已跳过、失败或崩溃
- 合并作业成功
- 跳过/合并的作业队列中等待的作业

如果启用这些选项,请单击“电子邮件设置”来配置您的电子邮件服务器。提供服务类型、邮件服务器和端口。如果需要身份验证,请启用该选项并且提供凭据。

- 指定要显示在电子邮件中的主题,例如,“CA ARCserve Central HostBased VM Backup 报警”。
- 指定“发件人”值,例如,“CA ARCserve Central HostBased VM Backup”。
- 指定所有收件人的电子邮件地址。使用分号 (;) 分隔每个地址。

您可以通过提供代理服务器名称、端口和所需的凭据来启用“代理设置”。

单击“确定”。

9. 单击“保存”。

编辑或复制备份策略

CA ARCserve Central HostBased VM Backup 允许您在创建 CA ARCserve D2D 备份策略后编辑或复制它们。

遵循这些步骤:

1. 登录该应用程序。
单击导航栏上的“策略”以打开“策略”屏幕。
2. 从“策略”屏幕，单击策略旁边的复选框，然后执行以下操作之一：
 - 单击工具栏上的“编辑”，然后编辑选定策略。
 - 单击工具栏上的“复制”，以从选定策略复制并创建新策略。
注意：在您复制策略时，“复制策略”对话框打开。为新策略指定名称，然后单击“确定”。
“编辑策略”对话框将打开。
3. 如果您想更改策略的名称，请在“策略名称”字段指定名称。
4. 在“备份设置”选项卡上，单击“保护设置”并完成以下信息：
 - **备份目标** — 指定要用于保存备份会话的远程共享文件夹。
 - **CA ARCserve D2D VM 备份代理** — 指定安装了 CA ARCserve D2D 的服务器的主机名或 IP 地址。如果尚未安装 CA ARCserve D2D，您可以使用 CA ARCserve Central Protection Manager 来部署它。为该服务器提供适当的凭据。默认情况下，端口号为 8014。如果您在 CA ARCserve D2D 安装期间更改了该默认值，请指定正确的端口号。
 - **保留设置** -- 您可以根据要保留的恢复点数量（合并会话）或根据要保留的恢复集数量（删除恢复集并禁用无限增量）来设置保留策略。默认选项是“保留恢复点”。有关详细信息，请参阅《CA ARCserve Central Protection Manager 用户指南》中的“指定保护设置”。
 - **压缩** — 选择压缩级别。默认值为“标准压缩”。您可以选择不压缩或“最大压缩”。
 - **加密** — 指定加密级别。默认值为“不加密”。指定加密级别时，请提供用于还原加密数据的加密密码。
 - **调节备份** — 输入备份写入磁盘的比率。降低该比率可减少 CPU 或网络负载，但是请注意，这样做会增加备份时间。默认情况下，该选项被禁用。

5. 单击“排定”并填写以下信息：
 - **开始日期和时间** — 指定您想要开始备份作业的日期和时间。
 - **增量备份** — 定义您的增量备份作业的重复排定。默认值是每天重复一次“增量备份”。
 - **完全备份** — 定义您的完全备份作业的重复排定。默认情况下，此值设置为“从不重复”。
 - **验证备份** — 定义验证备份作业的重复排定。默认情况下，此值设置为“从不重复”。
6. 单击“高级”并填写以下信息：
 - **截短日志** -- 如果您想要截短应用程序日志文件，请启用下列选项：
 - **SQL Server** — 指定每日、每周或每月的截短排定。
 - **Exchange Server** — 指定每日、每周或每月的截短排定。
 - **在目标上保留空间** -- 指定为执行一次备份所要保留的空间百分比。该持续空间量会即刻在目标上得到保留，然后备份才开始写数据，这将有助于提高备份速度。
 - **编录** -- 选择“每次备份后生成文件系统编录以便搜索更快”选项以减少您的浏览器搜索等待时间。

如果未选择此选项，还原在备份之后可以立即执行，而无需等待编录作业完成。默认情况下，此选项未启用。

注意：为每个备份作业生成文件系统编录时，它会增加存储元数据文件和编录文件所需的磁盘存储量以及 CPU 使用量。此外，如果备份源包含许多文件，生成编录的过程可能非常耗时。

注意：如果您选择 ReFS 或具有重复数据消除的 NTFS 卷作为备份源，编录无法生成，警告消息会显示，向您通知此状况。

7. 单击“先行/后继备份设置”，并指定任何所需的先行/后继备份命令。在需要时提供适当的凭据：
 - **在备份启动之前运行命令** — 输入在开始备份作业之前运行的脚本命令。
 - **退出时代码** -- 如果您想针对特定的退出代码触发脚本命令，请启用该选项。
 - **运行作业** — 如果已选定，软件会在返回指定的退出代码时继续运行作业。
 - **让作业失败** — 如果已选定，软件会在返回指定的退出代码时中止备份作业。
 - **在拍取快照之后运行命令** — 输入拍取快照之后运行的脚本命令。
 - **在备份结束之后运行命令** — 输入备份完成之后运行的脚本命令。
8. (可选)单击“首选项”选项卡。根据需要配置任何所需的电子邮件报警。如果启用这些选项，请单击“电子邮件设置”来配置您的电子邮件服务器。
9. 单击“保存”。

策略即被编辑或复制。

从备份策略分配和取消分配节点

要保护多个虚拟机，请选择要使用的策略并将其分配给一个或多个节点。

遵循这些步骤:

1. 登录该应用程序。
 - 单击导航栏上的“策略”以打开“策略”屏幕。
2. 在“策略”屏幕中，单击“策略分配”选项卡。
3. 在“策略”列表中，选择要分配的策略。
 - 单击“分配和取消分配”以打开“分配/取消分配策略”对话框。
4. 在“分配/取消分配策略”对话框指定以下字段：
 - **组** -- 让您选择包含想要分配的节点的组名称。
 - **节点名称筛选** -- 允许您基于通常标准筛选可用节点。

注意：“节点名称”字段允许您使用通配符筛选节点。

例如，Acc* 允许您筛选节点名称以 Acc 开头的所有节点。要清除筛选结果，请单击“筛选”字段中的 X。

5. 执行下列操作之一：

- **将节点分配给策略** -- 选择想要添加的节点，然后单击向右单箭头。

节点即从“可用节点”列表移到“选定的节点”列表。

注意：要选择和移动所有节点，请单击向右双箭头。

- **从策略取消分配节点** -- 选择要取消分配的节点，然后单击向左单箭头。

节点即从“选定的节点”列表移到“可用节点”列表。

注意：要选择和移动所有节点，请单击向左双箭头。

单击“确定”。

6. 在必要时提供全局用户名和密码，并将其应用于选定的节点。

单击“确定”。

选定的节点被添加到“策略分配”列表，部署状态为“[已分配] 挂起”。

注意：您也可以在“节点”屏幕上查看部署状态。

7. 单击“立即部署”可将分配的策略立即应用到指定的节点。使用“刷新”按钮来更新状态。

在“节点”屏幕上，您在“策略分配”列表中指定的节点的状态现在“策略”列中显示分配的策略。单击“节点名称”，并选择“登录 D2D”以检查您的备份作业的状态。

查看 CA ARCserve Central HostBased VM Backup 日志

“查看日志”包含关于您的应用程序所执行操作的全面信息。日志提供运行的每个作业的审核记录（最近的活动首先列出），有助于解决可能出现的任何问题。

遵循这些步骤：

1. 从主页上，单击导航栏上“查看日志”。
此时出现“查看日志”屏幕。
2. 从下拉列表，指定要查看的日志信息。
 - **重要级别** -- 该选项您允许指定要查看的日志的重要级别。可以指定以下重要级别选项：
 - **全部** -- 该选项允许您查看所有日志，无论重要级别是什么。
 - **信息** -- 该选项允许您仅查看说明一般信息的日志。
 - **错误** -- 该选项允许您仅查看说明发生的严重错误的日志。
 - **警告** -- 该选项允许您仅查看说明发生的警告错误的日志。
 - **错误和警告** -- 该选项允许您仅查看发生的严重错误和警告错误。

- **模块** -- 该选项允许您指定您要查看其日志的模块。可以指定以下模块选项：
 - **全部** -- 该选项允许您查看有关所有应用程序组件的日志。
 - **常规** -- 该选项允许您查看常规过程的日志。
 - **从发现导入节点** -- 该选项允许您查看仅从自动发现导入的节点的相关日志。
 - **从管理程序导入节点** -- 该选项允许您查看仅从管理程序导入的节点的有关日志。
 - **策略管理** -- 该选项允许您仅查看有关管理策略的日志。
 - **更新** -- 该选项允许您仅查看有关更新应用程序的日志。
 - **操作前检查** -- 该选项允许您仅查看运行每个节点的“操作前检查”状态的日志。
 - **提交 VM 备份作业** -- 该选项允许您仅查看已为虚拟机备份作业提交节点的日志。
 - **更新多个节点** -- 此选项允许您仅查看同时更新多个节点的有关日志。
 - **CA ARCserve D2D 合并作业** -- 此选项允许您仅查看 CA ARCserve D2D 合并作业的有关日志。
- **节点名称** -- 该选项允许您仅查看特定节点的日志。

注意：此字段支持通配符“*”和“?”。例如，输入“lod*”返回以“lod”开头的计算机名的所有活动日志。

注意：能够组合应用“重要级别”、“模块”和“节点名称”选项。例如，您可以查看与节点 X（“节点名称”）的更新（“模块”）有关的错误（“重要级别”）。

日志基于指定查看选项显示。

注意：日志中显示的时间基于您的应用程序的数据库服务器的所在时区。

查看特定节点的活动日志信息

CA ARCserve Central HostBased VM Backup 允许您查看特定 CA ARCserve D2D 节点的活动日志信息。活动日志提供运行的每个作业的审核记录（最近的活动首先列出），可能有助于解决出现的任何问题。

查看特定节点的活动日志信息

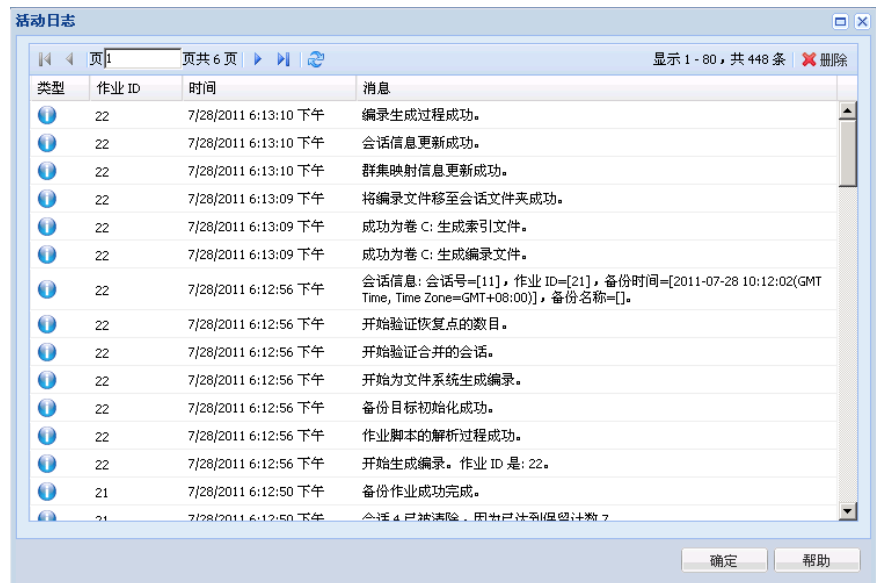
1. 打开应用程序，然后在导航栏中单击“节点”。
“节点”屏幕将显示。
2. 从“组”列表，单击“全部节点”，或单击包含您要登录的 CA ARCserve D2D 节点的组。
节点列表显示与指定组关联的所有节点。
3. 浏览并单击要登录的节点，然后从弹出菜单单击“登录 D2D”。

CA ARCserve D2D 随即打开，您便登录到 CA ARCserve D2D 节点的主页。

注意：如果新的浏览器窗口未打开，确认您的浏览器的弹出窗口选项允许所有弹出窗口或仅允许该网站的弹出窗口。

- 单击在“任务”列表上的“查看日志”。

活动日志打开，如下所示：



活动日志提供以下信息：

- **类型** -- 指定活动的重要级别，其包括“信息”、“警告”和“错误”。
- **作业 ID** -- 指定活动适用的作业。
- **时间** -- 指定活动适用的日期和时间。
- **消息** -- 描述活动。

- 单击“确定”以关闭活动日志。

在报告中查看 CA ARCserve Central HostBased VM Backup 状态

如果您安装了 CA ARCserve Central Protection Manager 和 CA ARCserve Central Reporting，您可以将基于主机的 VM 备份代理服务添加到 CA ARCserve Central Protection Manager，然后生成虚拟保护状态报告，以查看基于主机的备份代理的状态。

有关虚拟保护状态报告的详细信息，请参阅《CA ARCserve Central Reporting 用户指南》。

将链接添加到导航栏中

导航栏中，每个 CA ARCserve Central Applications 有一个“添加新选项卡”链接。使用此功能为您想管理的其他基于 Web 的应用程序在导航栏中添加条目。但是，对于安装的每个应用程序，都会自动在导航栏中添加一个新链接。例如，如果您在“计算机 A”上安装 CA ARCserve Central Reporting 和 CA ARCserve Central Virtual Standby，然后启动 CA ARCserve Central Reporting，CA ARCserve Central Virtual Standby 将自动添加到导航栏。

注意：仅当其他 CA ARCserve Central Applications 位于同一计算机上时，才会检测到安装的每个应用程序。

遵循这些步骤：

1. 在应用程序的导航栏中，单击“添加新选项卡”链接。
2. 指定您要添加的应用程序或网站的名称和 URL。例如，www.google.com。
如需要，可指定图标的位置。
3. 单击“确定”。

新选项卡将添加到导航栏的底部。

请注意以下事项：

- 默认情况下，已添加“CA 支持”链接以方便使用。

可以通过突出显示新建的选项卡并单击“删除”链接来删除此选项卡。

保护裸设备映射的注意事项

当保护裸设备映射 (RDM) 时，请考虑以下行为：

- 应用程序不支持保护物理兼容模式裸设备映射（该类型的磁盘是物理设备）。在备份过程期间，应用程序会忽略备份源中的物理兼容模式裸设备映射。该行为的解决方案是将 CA ARCserve D2D 安装在访客操作系统内，并采用与您备份物理磁盘同样的方法来执行备份。

- 应用程序支持保护虚拟兼容模式裸设备映射。但是, 请考虑以下限制:
 - 对于完全备份, 应用程序让您可以备份完全虚拟兼容模式 RDM 磁盘。但是, 如果您不使用数据压缩, 备份数据集可能和源磁盘一样大小。
 - CA ARCserve Central HostBased VM Backup 将虚拟兼容模式 RDM 磁盘还原为普通虚拟磁盘。在恢复过程完成之后, 磁盘不再被配置成, 或者表现为虚拟 RDM。
 - 备份虚拟兼容模式 RDM 的另一种方法是在访客操作系统内安装 CA ARCserve D2D, 并采用与您备份物理磁盘同样的方法来备份 RDM。

更改服务器通信协议

默认情况下, CA ARCserve Central Applications 使用超文本传输协议 (HTTP) 进行其所有组件间的通信。如果您对在这些组件间传输的密码的安全性有顾虑, 可以将使用的协议更改为安全超文本传输协议 (HTTPS)。当您不需要此额外的安全级别时, 可以将使用的协议重新更改为 HTTP。

遵循这些步骤:

1. 使用管理帐户或具有管理权限的帐户登录到安装该应用程序的计算机。

注意: 如果您没有使用管理帐户或具有管理权限的帐户进行登录, 请将命令行配置为使用“以管理员身份运行”权限运行。
2. 打开 Windows 命令行。

3. 执行以下操作之一：
 - **将协议从 HTTP 更改为 HTTPS:**

从以下默认位置（BIN 文件夹的位置可能会因您安装应用程序的位置而异）启动“changeToHttps.bat”实用工具：

```
C:\Program Files\CA\ARCserve Central Applications\BIN
```

协议更改成功后，将显示以下消息：

通信协议变成 HTTPS。
 - **将协议从 HTTPS 更改为 HTTP:**

从以下默认位置（BIN 文件夹的位置可能会因您安装应用程序的位置而异）启动“changeToHttp.bat”实用工具：

```
C:\Program Files\CA\ARCserve Central Applications\BIN
```

协议更改成功后，将显示以下消息：

通信协议变成 HTTP。
4. 重新启动浏览器并重新连接到 CA ARCserve Central Applications。

注意：将协议更改为 HTTPS 时，Web 浏览器中会显示一则警告。出现此行为是由于自签名安全证书的缘故，用于提示您忽略该警告并继续操作，或者向浏览器添加该证书以阻止以后再次出现此警告。

定义备份的传输模式

您可以针对使用 Host-Based VM Backup 执行的 D2D 备份作业定义特定的传输模式（传输数据）。默认情况下，Host-based VM backup 使用的模式可使 Host-Based VM Backup 优化备份操作的性能（提高速度）。但是，如果您需要为备份操作指定特定的传输模式，可以配置本主题中介绍的注册表项。

Host-Based VM Backup 可使用下列传输模式执行备份：

- [HOTADD 传输模式](#) (p. 179)
- [NBD 传输模式](#) (p. 179)
- [NBDSSL 传输模式](#) (p. 179)
- [SAN 传输模式](#) (p. 179)

请注意以下事项：

- 这是一项可选的配置任务。默认情况下，Host-Based VM Backup 使用可优化备份操作性能的传输模式来执行备份。
- 如果您配置此注册表项来使用特定传输模式，而该模式不可用，则 Host-Based VM Backup 将使用可用的默认传输模式来执行备份操作。

遵循这些步骤:

1. 登录到虚拟机的 CA ARCserve D2D 备份代理系统。

打开 Windows 注册表编辑器，并浏览至以下注册表键:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA_ARCSERVE  
D2D\AFBackupDll\{VM-InstanceUUID}]。
```

2. 右键单击“VM-InstanceUUID”，选择“新建”，然后在弹出式菜单上单击“字符串值”。

命名新字符串值，如下所述:

EnforceTransport

3. 右键单击“EnforceTransport”，在弹出式菜单上单击“修改”以打开“编辑字符串”对话框。

4. 在“值数据”字段中，指定要在备份作业中使用的传输模式。指定以下值之一:

hotadd

[HOTADD 传输模式](#) (p. 179)

nbd

[NBD 传输模式](#) (p. 179)

nbdssl

[NBDSSL 传输模式](#) (p. 179)

san

[SAN 传输模式](#) (p. 179)

5. 单击“确定”应用该值，并关闭“编辑字符串”对话框。

传输模式现已定义，并在作业下次运行时使用。

第 4 章： 还原和恢复虚拟机

可用的还原和修复选项取决于您的系统如何得到备份。例如，您不能使用通过 CA ARCserve Central HostBased VM Backup 创建的备份会话来执行应用程序级或 Microsoft Exchange 粒度还原操作，但是可以使用通过 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 创建的会话来执行该操作。可用于 CA ARCserve D2D 的某些还原选项可能无法用于此应用程序。例如，“还原到原始位置”无法用于应用程序的备份，因为代理服务器的位置与备份源虚拟机的位置不同。

有关详细信息，请参阅“[还原注意事项](#) (p. 96)”以帮助您决定何时使用可用的“[还原方法](#) (p. 85)”。

此部分包含以下主题：

[还原方法](#) (p. 85)

[还原注意事项](#) (p. 96)

[应用程序级还原](#) (p. 96)

还原方法

您的备份会话的创建方式决定使用什么还原方法。例如，仅可以使用本地安装的 CA ARCserve D2D 执行一些还原方法。其他方法需要在备份时打开虚拟机。

[浏览恢复点](#) (p. 86)

允许您从日历视图中查找可用的恢复点（成功的备份）。使用该方法还原文件、文件夹，或执行应用程序级还原过程。

可以使用该方法还原使用 CA ARCserve D2D、CA ARCserve Central HostBased VM Backup 或 CA ARCserve Central Protection Manager 创建的备份。

[查找要还原的文件/文件夹](#) (p. 89)

允许您找到特定文件或文件夹进行还原。

可以使用该方法还原使用 CA ARCserve D2D 创建的备份。如果备份时已打开虚拟机，它也可用于还原使用 CA ARCserve Central HostBased VM Backup 和 CA ARCserve Central Protection Manager 创建的备份。

[恢复 VM \(p. 92\)](#)

允许您从日历视图中浏览所有可用恢复点（成功的备份）。您便可以指定您想恢复的虚拟机。

该方法可用于还原使用 **CA ARCserve Central HostBased VM Backup** 创建的备份，首先配给一个虚拟机，然后从您指定的恢复点还原操作系统、应用程序和数据。

[应用程序还原 \(p. 96\)](#)

为了无需重新构建 **Microsoft Exchange** 或 **SQL Server** 便可完全还原它，请从本地安装的 **CA ARCserve D2D** 单击“浏览恢复点”方法。

[裸机恢复 \(p. 143\)](#)

裸机恢复 (BMR) 是从裸机状态恢复计算机（包括其操作系统、软件应用程序、设置和数据）的过程。BMR 需要您具有 **Windows** 映像或启动工具包以及至少一个完全备份。可以使用该方法还原使用 **CA ARCserve D2D**、**CA ARCserve Central HostBased VM Backup**、**CA ARCserve Central Virtual Standby** 和 **CA ARCserve Central Protection Manager** 创建的备份。然而，如果在备份期间虚拟机关机，便不可能进行 BMR。

从恢复点还原

“浏览恢复点”还原方法允许您从日历视图查找成功的备份（称作恢复点）。您便可以浏览并选择要还原的备份内容，包括应用程序。使用“浏览恢复点”方法还原的过程与使用 **CA ARCserve D2D** 的还原过程一样，但有一个例外。要还原虚拟机恢复点，您无法使用还原到原始位置选项。

遵循这些步骤:

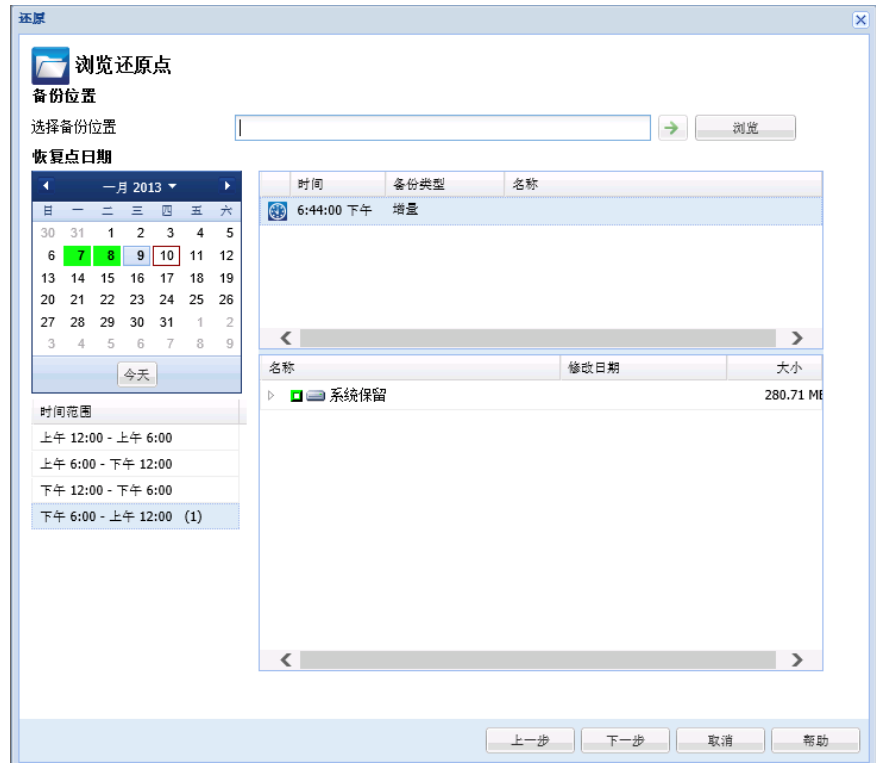
1. 登录到应用程序，并单击导航栏上的“节点”。

在“节点”屏幕中，展开包含要还原的节点的组。

单击要还原的节点旁的复选框，然后单击工具栏上的“还原”。

2. 在“还原”对话框中单击“浏览恢复点”。

将打开“还原”对话框，并根据您选择的节点来提供“备份位置”。需要时，将其更改为其他备份目标，然后提供用户凭据。



- 单击恢复点日期，然后单击恢复点时间。选择要还原的内容。选择整个卷或文件、文件夹、数据库或应用程序。所选内容旁边的纯绿色框表示已选择该项进行还原。完成操作后，请单击“下一步”。



- 在“还原选项”对话框上，指定还原目标。
 - **还原到原始位置(禁用)** -- 对于 CA ARCserve Central HostBased VM Backup 会话，您无法还原到原始位置。在 VM 的来宾 OS 中要将文件或文件夹还原到它们的原始位置，您需要在该 VM 的来宾 OS 中安装 CA ARCserve D2D，或还原到该 VM 上的网络共享文件夹。
 - **还原到** -- 指定您想还原到的目标。
 - **覆盖现有文件** -- 替换位于目标的文件。
 - **替换活动文件** -- 替换重新启动时正被使用或访问的文件。
 - **重命名文件** -- 如果该文件名已存在，创建新文件。此选项会将源文件复制到目标，文件名相同，但扩展名不同。数据被还原到具有新扩展名的文件。
 - **跳过现有文件** -- 跳过而非替换位于目标的现有文件。这是默认设置。
 - **创建根目录** -- 在目标上重新创建在备份映像中找到的相同根目录结构。
- 单击“下一步”。在“还原摘要”屏幕上，请确保所有选项正确。如果不正确，单击“上一步”返回。如果正确，单击“完成”以启动还原过程。

通过安装恢复点进行还原

通过“安装恢复点”还原方式，您可以将恢复点安装到备份代理系统。要安装恢复点，您必须登录到 CA ARCserve D2D 用户界面。

遵循这些步骤:

1. 登录到 CA ARCserve Central HostBased VM Backup，然后单击导航栏上的“节点”。
2. 在“节点”屏幕中，展开包含要还原的节点的组。

单击要还原的节点旁的复选框，然后单击工具栏上的“还原”。

此时将打开 CA ARCserve D2D 的 CA ARCserve Central HostBased VM Backup 版本。

注意: 请确认浏览器的弹出选项允许所有弹出窗口或仅允许该网站的弹出窗口，以便可以打开新的浏览器。

有关“安装恢复点”对话框的详细信息，请单击 CA ARCserve D2D 主页中对话框屏幕上的“帮助”。

使用“查找要还原的文件/文件夹”还原数据

每次应用程序成功执行备份时，会将所有备份的文件或文件夹都包含在备份的快照映像中。该还原方法允许确切地指定要还原的文件/文件夹。

遵循这些步骤:

1. 登录到应用程序，并单击导航栏上的“节点”。
在“节点”屏幕中，展开包含要还原的节点的组。
单击要还原的节点旁的复选框，然后单击工具栏上的“还原”。
2. 在“还原”对话框中单击“查找要还原的文件/文件夹”。
3. 在“查找要还原的文件/文件夹”对话框上，指定或浏览至备份位置。如果要从 CA ARCserve Central HostBased VM Backup 会话还原，您不能指定文件复制位置。只有要从 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 备份会话还原时，才允许进行文件复制还原。

4. 指定要还原的文件或文件夹名称。

注意：“计算机名”字段支持全名搜索和通配符搜索。如果不知道完整的文件名，您可以通过在“文件名”字段中指定通配符“*”和“?”来简化搜索结果。

文件或文件夹名称支持的通配符如下所示：

- “*” -- 使用星号代替文件名或文件夹名中的 0 或多个字符。
- “?” -- 使用问号代替文件名或文件夹名中的单个字符。

例如，如果指定 *.txt，则文件扩展名为 .txt 的所有文件都会显示在搜索结果中。

5. （可选）指定一个路径名来进一步筛选搜索，并选择包括或不包括子目录、文件和文件夹。
6. 单击“查找”以启动搜索。

搜索的结果将显示。如果搜索发现相同被搜索文件的多个匹配项（恢复点），将列出按日期排序的所有结果（最新的列于首位）。

7. 选择要从列表还原的版本，然后单击“下一步”。

将显示“还原选项”对话框。您仅可以还原到备用位置。指定或浏览要将备份映像存储到的位置。单击绿色箭头验证连接。需要时，提供用户凭据。

8. 选择冲突解决选项:

覆盖现有文件

覆盖（替换）位于还原目标的任何现有文件。将从备份文件中还原所有对象，不管它们当前是否存在于您的计算机上。

替换活动文件

重新启动时替换任何活动文件。如果在还原尝试期间，软件发现现有文件当前正在使用或者被访问，它将不立即替换该文件，而是为了避免任何问题，将推迟活动文件的替换，直到下次重新启动计算机再进行。（还原将立即发生，但是任何活动文件的替换将在下一次重新启动期间完成）。

注意：如果未选中此选项，那么还原将跳过任何活动文件。

重命名文件

如果该文件名存在，创建新文件。选择此选项会将源文件复制到目标（文件名相同，但扩展名不同）。然后数据将还原到此新文件。

跳过现有文件

跳过且不覆盖（替换）位于还原目标的任何现有文件。仅从备份文件还原当前在您的计算机上不存在的对象。

默认情况下，将选中该选项。

9. （可选）从“目录结构”中选择“创建根目录”。

该选项在还原目标路径中重新创建相同的根目录结构。

注意：如果未选中此选项，则文件或文件夹将直接还原到目标文件夹。

10. 输入备份加密密码，还原加密的数据，然后单击“下一步”。

将显示“还原摘要”对话框。

11. 检查显示的信息以确认所有还原选项和设置都正确。

- 如果摘要信息不正确，单击“上一步”返回到相应对话框，以更改错误设置。
- 如果摘要信息正确，单击“完成”以启动还原过程。

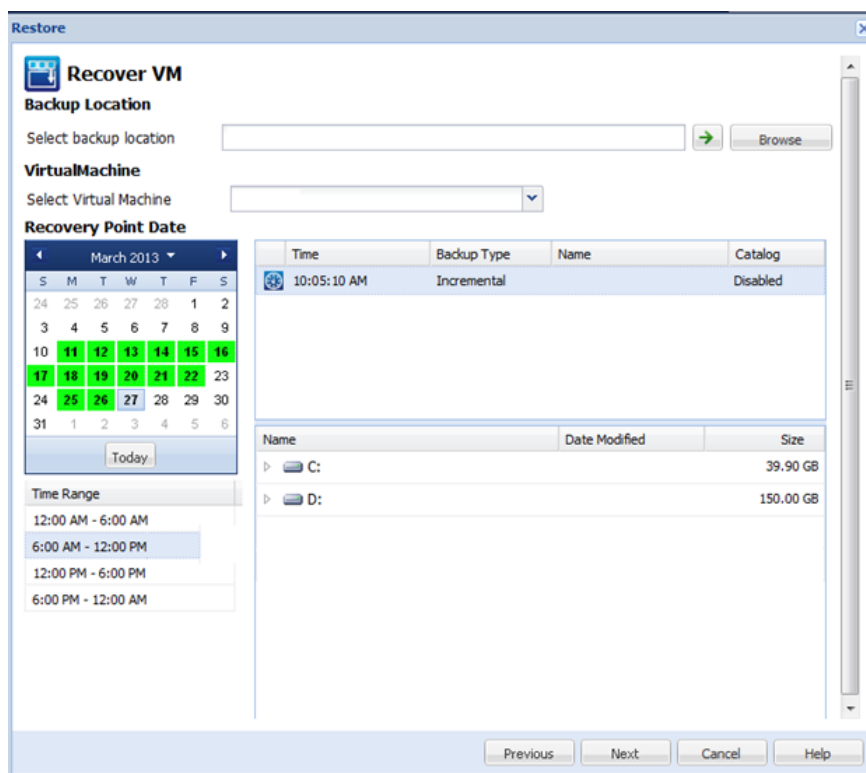
恢复整个虚拟机

您可以从 CA ARCserve Central HostBased VM Backup 会话恢复整个虚拟机。

该备份方法类似执行 BMR。可以使用该方法恢复 Windows 来宾操作系统、应用程序和数据。

遵循这些步骤:

1. 登录到应用程序，并单击导航栏上的“节点”。
在“节点”屏幕中，展开包含要还原的节点的组。
单击要还原的节点旁的复选框，然后单击工具栏上的“还原”。该应用程序将使您登录到 CA ARCserve D2D。
2. 在“还原”对话框中单击“恢复 VM”。
3. 此时将打开“还原”对话框。根据您从“节点”屏幕中选择的 VM 来填充“备份位置”和“虚拟机”字段。需要时，更改这些值。



指定存储虚拟机备份会话的源。如果有提示，输入用户凭据。

下拉菜单列出在“备份位置”字段的位置的所有虚拟机。

4. 从日历，单击要恢复的虚拟机映像的日期。从“时间范围”列表，单击要恢复的备份映像。与您的选择对应的内容显示，供您参考。您不能选择单个卷、文件夹或文件。整个虚拟机被还原。

5. 单击“下一步”。在“还原选项”对话框上，选择还原目标。

还原到原始位置

将虚拟机还原到捕获备份映像的原始位置。默认情况下，将选中该选项。

有关详细信息，请参阅[将 VM 还原到原始位置](#) (p. 93)。

还原到备用位置

将虚拟机还原到与备份映像捕获位置不同的位置。

有关详细信息，请参阅[将 VM 还原到备用位置](#) (p. 94)。

6. 指定冲突解决和后续恢复选项。默认情况下，未选择这些选项。
 - 覆盖现有虚拟机 -- 替换 vCenter/ESX 服务器上的任何现有虚拟机映像。
 - 打开虚拟机 -- 在还原过程完成之后打开虚拟机。
7. 单击“下一步”。如果提示，请输入备份源的 vCenter/ESX 服务器凭据，然后单击“确定”。
8. 在“还原摘要”对话框上，请确保所有选项正确。如果不正确，单击“上一步”返回。如果正确，单击“完成”以启动恢复过程。

将虚拟机还原到初始位置

在还原 VM（虚拟机）配置过程中，您需要选择将虚拟机还原到哪里。可用的选择项包括“还原到原始位置”和“还原到备用位置”。

如果您选择将 VM 还原到原始位置，请执行下列步骤：

遵循这些步骤：

1. 在“恢复选项”对话框上，指定“解决冲突”和“后续恢复”选项后，请选择“还原到原始位置”，然后单击“下一步”。

注意：有关“解决冲突”和“后续恢复”选项的详细信息，请参阅“从虚拟机还原数据”。

“设置源 vCenter/ESX 服务器的凭据”对话框显示。

2. 指定用于访问虚拟机的凭据。
 - **vCenter/ESX 服务器** -- 指定目标 vCenter 或 ESX 服务器系统的主机名或 IP 地址。
 - **VM 名称** -- 指定您要还原的虚拟机的主机名。
 - **协议** -- 指定要用于与目标服务器进行通讯的协议。可用的选择项包括 HTTP 和 HTTPS。
 - **端口号** -- 指定要用于源服务器和目标之间的数据传输端口。默认情况下，端口号为 443。
 - **用户名** -- 指定有权登录要还原的虚拟机的用户名。
 - **密码** -- 指定该用户名的对应密码，在登录要还原的虚拟机时必需该密码。
3. 指定凭据后，单击“确定”。

“还原摘要”对话框将打开。
4. 检查显示的信息以确认所有还原选项和设置都正确。
 - 如果摘要信息不正确，单击“上一步”返回到相应对话框，以更改错误设置。
 - 如果摘要信息正确，单击“完成”以启动还原过程。

将虚拟机还原到备用位置

在还原 VM（虚拟机）配置过程中，您需要选择要将虚拟机还原到什么位置的选项。可用的选择项包括“还原到原始位置”和“还原到备用位置”。

如果要将虚拟机还原到备用位置，请执行下列步骤：

遵循这些步骤：

1. 在“恢复选项”对话框上，指定“解决冲突”和“后续恢复”选项后，请选择“还原到备用位置”。

注意：有关“解决冲突”和“后续恢复”选项的详细信息，请参阅“恢复数据到虚拟机”。

“恢复选项”对话框展开，显示更多还原到备用位置的选项。

2. 指定 vCenter/ESX 服务器信息。
 - **vCenter/ESX 服务器** -- 指定目标 vCenter 或 ESX 服务器系统的主机名或 IP 地址。
 - **用户名** -- 指定有权登录要还原的虚拟机的用户名。
 - **密码** -- 指定该用户名的对应密码，在登录要还原的虚拟机时必需该密码。
 - **协议** -- 指定要用于与目标服务器进行通讯的协议。可用的选择项包括 HTTP 和 HTTPS。
 - **端口号** -- 指定要用于源服务器和目标之间的数据传输端口。默认情况下，端口号为 44。
3. 指定 vCenter/ESX 服务器信息后，请单击“连接到该 vCenter/ESX 服务器”按钮。

如果备用服务器访问凭据信息正确，将启用“其他信息”字段。

4. 指定其他信息。
 - **VM 名称** -- 指定您要还原的虚拟机的主机名。
 - **ESX 服务器** -- 指定目标 ESX 服务器。下拉菜单将包含与指定虚拟机关联的所有 ESX 服务器的列表。
 - **资源池** -- 指定要用于虚拟机恢复的资源池或 vApp 池。单击“浏览资源池”按钮以显示“选择资源池”对话框。该对话框包含可用于目标 ESX 服务器的所有资源池和 vApp 池的列表。选择要用于虚拟机恢复的池。如果不想为该虚拟机恢复分配资源池或 vApp 池，可以将此字段留空。
- 注意：**资源池是已配置的 CPU 和内存资源集合。vApp 池是可以作为单个对象管理的一个或多个虚拟机的集合。
- **VM 数据存储** -- 为虚拟机恢复或虚拟机中的每个虚拟磁盘指定目标 VM 数据存储。

一个虚拟机可以有多个虚拟磁盘，您可以为每个虚拟磁盘指定不同的数据存储。

例如：

- Disk0 可以还原到 Datastore1。
- Disk1 可以还原到 Datastore1。
- Disk2 可以还原到 Datastore2。

重要说明！对于虚拟机数据存储，仅当用户拥有完全的 VMware 系统管理员权限时才会填充此字段。如果用户没有适当的管理员权限，在您连接到 vCenter/ESX Server 之后，CA ARCserve Central HostBased VM Backup 不会继续还原过程。

5. 指定其他信息后，单击“下一步”。
“还原摘要”对话框将打开。
6. 检查显示的信息以确认所有还原选项和设置都正确。
 - 如果摘要信息不正确，单击“上一步”返回到相应对话框，以更改错误设置。
 - 如果摘要信息正确，单击“完成”以启动还原过程。

还原注意事项

使用下表帮助您确定在下列状况下使用什么还原方式。

还原方式:	如果您想:	注意事项:
浏览恢复点（使用该方法来执行应用程序级还原。） 查找要还原的文件/文件夹	还原损坏的文件、文件夹、数据库或应用程序。	<ul style="list-style-type: none"> ■ CA ARCserve Central HostBased VM Backup: 要还原文件或文件夹，在备份的时间必须打开 VM。“还原至原始位置”不可用。将网络驱动器映射到原始位置，或将其作为共享访问，然后还原到映射或共享位置。将 CA ARCserve D2D 安装在新 VM 的来宾操作系统中，然后还原应用程序数据库。有关详细信息，请参阅主题“应用程序级还原”。 ■ CA ARCserve D2D 或 CA ARCserve Central Protection Manager: 请参阅该应用程序用户指南。
恢复 VM	配给虚拟机，还原操作系统、应用程序和数据	<ul style="list-style-type: none"> ■ CA ARCserve Central HostBased VM Backup: 推荐 ■ CA ARCserve D2D 或 CA ARCserve Central Protection Manager: 不受支持

也可以使用 BMR 和应用程序级还原过程执行恢复。有关详细信息，请参阅主题“[还原方法](#)” (p. 85)。

应用程序级还原

CA ARCserve Central Applications 允许您保护和恢复数据，而且帮助您让使用数据的应用程序得到备份和运行。应用程序级还原使用“浏览恢复点”还原方法。在应用程序级还原过程中，您无需执行完全灾难恢复，便可以恢复 Microsoft Exchange 或 SQL Server。

在开始执行应用程序级还原过程之前，可能需要执行以下任务：

- 使用 Windows 来宾操作系统配给新的虚拟机
- 将 CA ARCserve D2D 安装在来宾操作系统中。
- 对于 Exchange Server 应用程序还原操作：
 - 确保帐号对于 Exchange Server 2003 有 Exchange 管理员（完全控制）角色权限，或者对于 Exchange Server 2007/2010/2013 有 Exchange 组织管理员或服务器管理员角色权限。
 - 将 Exchange Server 2007 数据库还原到恢复存储组时，在受保护的服务器上创建恢复存储组。同样，将 Exchange Server 2010 或 2013 数据库还原到恢复数据库时，请在受保护的服务器上创建恢复数据库。
 - 阅读有关如何执行还原的完整步骤（《CA ARCserve D2D 用户指南》中有述）。

还原 Exchange Server 数据

您可以在以下环境中对 Microsoft Exchange Server 数据执行应用程序级还原：

- Exchange Server 2003：单服务器环境。不支持群集环境。
- Exchange Server 2007：单服务器环境、本地连续复制 (LCR) 和群集连续复制 (CCR) 环境。对于 Exchange Server 2007 CCR，在主动和被动节点上都本地安装 CA ARCserve D2D。您可以在从主动节点执行备份操作，也可以从被动节点执行，但是您仅可以在主动节点上执行还原操作。不支持单一副本群集 (SCC)。
- Exchange Server 2010：单服务器环境和数据库可用性组 (DAG) 环境。对于 DAG 环境，确保 CA ARCserve D2D 安装在 DAG 中的所有服务器上。您可以从任何服务器对主动和被动数据库副本执行备份操作，但是只能对主动数据库副本执行还原操作。
- Exchange Server 2013：支持备份和还原 Microsoft 卷影复制服务 (VSS)。不支持粒度恢复技术 (GRT)。

您可以将 Microsoft Exchange Server 数据还原到以下级别：

- Microsoft Exchange 编写器级：还原所有 Exchange Server 数据。
- 存储组级：还原特定存储组（不适用于 Microsoft Exchange Server 2010）。
- 邮箱存储级：还原特定邮箱存储（仅适用于 Microsoft Exchange Server 2003）。
- 邮箱数据库级：还原特定邮箱数据库（适用于 Exchange Server 2007 和 2010）。

注意： 在开始之前，请执行[应用程序级还原](#) (p. 96)中的必要先决条件。

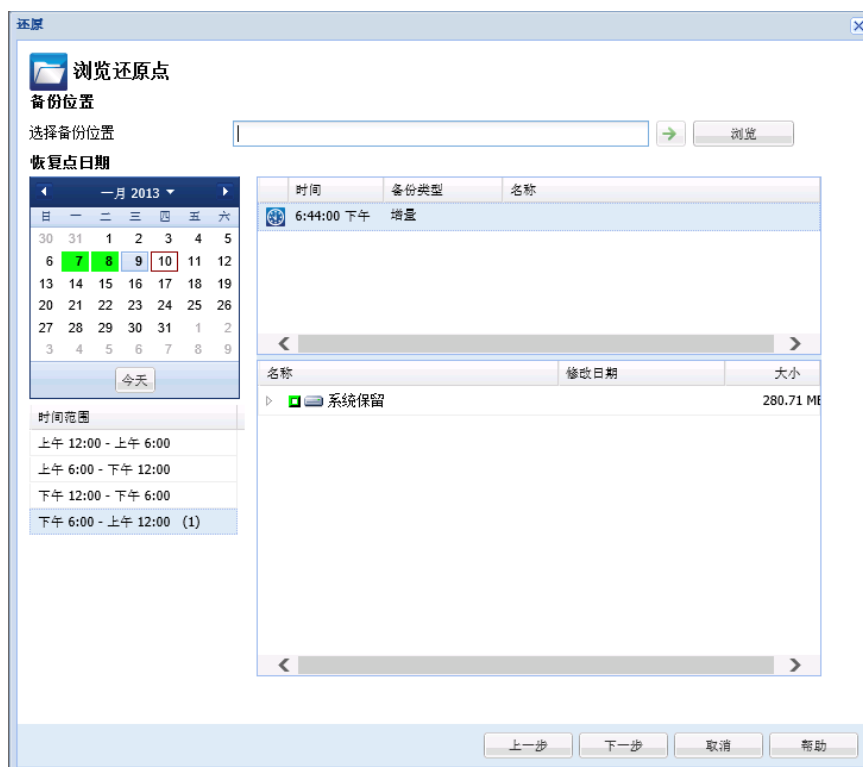
重要说明！ 不支持从 CA ARCserve Central HostBased VM Backup 会话还原 Microsoft Exchange Server 用户邮箱项。要在粒度级别还原 Microsoft Exchange Server 数据，请使用 CA ARCserve Central Protection Manager 或 CA ARCserve D2D 备份 Exchange Server 数据。

还原 Exchange Server 数据

1. 确保 CA ARCserve D2D 安装在来宾操作系统上。
2. 登录到要还原 Exchange Server 数据的虚拟机上的来宾操作系统。
3. 启动 CA ARCserve D2D，然后在 CA ARCserve D2D 导航面板上单击“还原”以打开“还原”对话框。
4. 单击“浏览恢复点”以打开“浏览恢复点”对话框。
5. 在“浏览恢复点”对话框的“选择备份位置”字段中，指定要从中还原 Exchange Server 数据的 Host-Based VM Backup 虚拟机上的备份会话的路径。以下路径是 Host-Based VM Backup 虚拟机上备份会话的路径示例：

```
https://<server name>/<share name>/vm@<host name or IP address of the ESX Server system>
```

- 在日历上，单击恢复点日期和时间。



- 单击“下一步”打开“还原选项”对话框。
- 为还原选择目标。

可用选项包括：还原到备份的原始位置，仅还原转储文件，或还原到恢复存储组/恢复邮箱数据库。

还原到原始位置

还原到捕获备份映像的原始位置。

仅转储文件

仅还原转储文件。

对于该选项，CA ARCserve D2D 会将 Microsoft Exchange 数据库文件还原到指定文件夹，但不会在恢复后使其联机。您便可以将该文件移至其他服务器，并手动将其挂接到 Exchange 服务器，以查看包含在文件中的数据。

注意：当恢复邮箱数据库存在时，使用“仅转储文件”选项的还原将失败。

重播登录数据库

指定当数据库文件转储到目标文件夹时，您可以重播并应用所有的 Exchange 事务日志文件并将它们提交到数据库文件。当数据库下一次启动时，会应用尚未写入数据库文件的事务日志文件，然后数据库才会对您再次可用。

注意：该选项不适用于 Microsoft Exchange Server 2003。

还原到恢复存储组 (Exchange 2007)

将数据库还原到恢复存储组 (RSG)。

RSG 是可用于进行恢复的存储组。您可以从恢复存储组中的备份还原 Microsoft Exchange 邮箱数据库，然后从中恢复并提取数据，而不会影响最终用户正在访问的生产数据库。

- 如果选中单个存储组或同一存储组中的数据库（公共文件夹数据库除外）进行还原，那么默认的还原目标为“还原到恢复存储组”（或“还原到恢复数据库”）。
- 如果选中多个存储组或多个存储组中的数据库进行还原，仅可将 Exchange 还原到原始位置或使用“仅转储文件”选项还原。默认还原目标为“还原到原始位置”。

将 Exchange 2007 数据库还原到恢复存储组之前，必须创建具有同一名称的恢复存储组和邮箱数据库。

如果您想将 MailboxDatabase1 从 First Storage Group 还原到恢复存储组，则必须创建一个恢复存储组并将数据库“MailboxDatabase1”添加到该恢复存储组。

注意：该选项不适用于 Microsoft Exchange Server 2003。

在还原前卸载数据库，在还原后安装数据库

通常在还原之前，Microsoft Exchange 将执行一些检查以确保：

- 要还原的数据库处于“已卸载”状态下。
- 数据库还原正常。

为了保护 Microsoft Exchange 生产数据库不被异常还原，将添加一个开关，以允许数据库在还原过程中被覆盖。如果未设置该开关，Microsoft Exchange 将拒绝还原数据库。

对于 CA ARCserve D2D，这两个选项由选项“在还原前卸载数据库，在还原后安装数据库”选项控制。通过该选项，CA ARCserve D2D 允许自动启动还原过程，无需手动操作。（您也能指定手动卸载/挂接数据库）。

- 如果选中，指定恢复过程在还原过程之前将自动卸载 Exchange 数据库，然后在还原过程完成之后挂接数据库。此外，如果选中，该选项在还原过程中还允许 Exchange 数据库被覆盖。
- 如果未选中，指定恢复过程将不在恢复之前自动卸载 Exchange 数据库，不在恢复之后挂接数据库。

Exchange 管理员必须执行一些手动操作，如卸载 Exchange 数据库，在数据库上设置“允许覆盖”标志，以及挂接 Exchange 数据库。（挂接数据库过程中恢复过程由 Exchange 执行）。

此外，如果未选中，该选项在还原过程中不允许 Exchange 数据库被覆盖。

还原到恢复数据库 (Exchange 2010)

将数据库还原到恢复数据库。恢复数据库是可以用于恢复的数据库。您可以从备份将 Microsoft Exchange 邮箱数据库还原到恢复数据库，然后从中恢复并提取数据，而不会影响最终用户正在访问的生产数据库。

在将 Exchange 2010 数据库还原到恢复数据库前，必须先创建恢复数据库。

注意：该选项不适用于 Microsoft Exchange Server 2003 和 2007。

9. 单击“下一步”打开“还原摘要”对话框。
10. 检查显示的信息以确认所有还原选项和设置都正确。
 - 如果摘要信息不正确，请单击上一步返回到相应对话框，以更改错误设置。
 - 如果摘要信息正确，单击完成以启动还原过程。

还原 SQL Server 数据

您可以对以下软件执行应用程序级 Microsoft SQL Server 数据还原：

- Microsoft SQL Server 2005 Express、Standard、Workgroup 和 Enterprise
- Microsoft SQL Server 2008、SQL Server 2008 R2 Express、Web、Standard、Workgroup 和 Enterprise

注意： 在开始之前，请先阅读[应用程序级还原](#) (p. 96)中的先决条件。

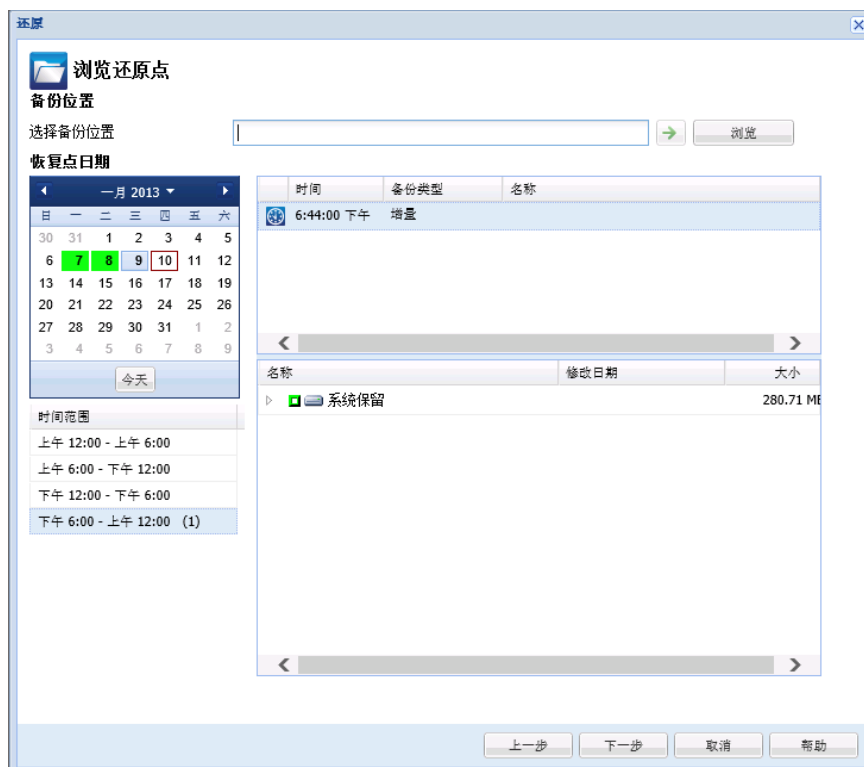
重要说明！ Microsoft SQL Server 粒度还原在 CA ARCserve Central HostBased VM Backup 控制台上无法运行。要还原 Microsoft SQL Server 数据，请在来宾虚拟机上安装 CA ARCserve D2D。

遵循这些步骤：

1. 确保 CA ARCserve D2D 安装在来宾操作系统上。
2. 登录到要将 SQL Server 数据所还原到的虚拟机上的来宾操作系统。
3. 启动 CA ARCserve D2D，然后在 CA ARCserve D2D 导航面板上单击“还原”以打开“还原”对话框。
4. 单击“浏览恢复点”以打开“浏览恢复点”对话框。
5. 在“浏览恢复点”对话框的“选择备份位置”字段中，指定要从中还原 SQL Server 数据的 Host-Based VM Backup 虚拟机上的备份会话的路径。以下路径是 Host-Based VM Backup 虚拟机上备份会话的路径示例：

```
https://<server name>/<share name>/vm@<host name or IP address of the ESX Server system>
```

- 选择恢复点（日期和时间），然后选择要还原的 Microsoft SQL Server 数据库。



- 单击“下一步”打开“还原选项”对话框。

为还原选择目标。可用选项包括：还原到备份的原始位置，仅还原转储文件，或还原到备用位置。

还原到原始位置

还原到捕获备份映像的原始位置。

仅转储文件

仅还原转储文件。

当应用程序崩溃并包含可用于对该问题的原因进行故障排除的其他（具有时间戳）信息时，会创建转储文件。

当选择该选项时，您即可指定或浏览转储文件将要还原到的文件夹位置。

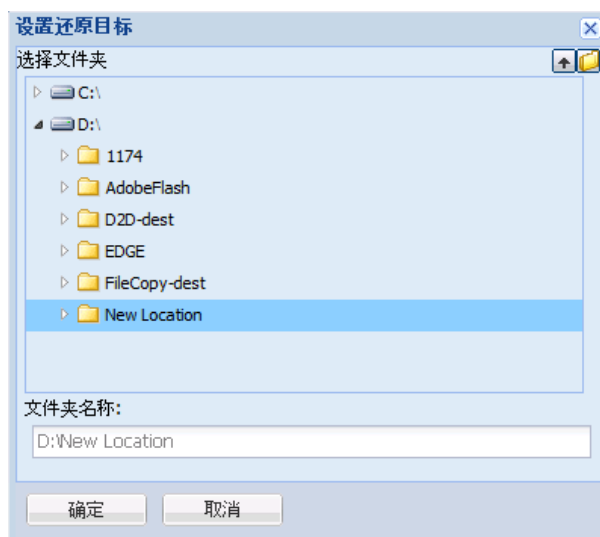


还原到备用位置

还原到备用位置（而非原始位置）。

实例名	数据库名	新数据库名	备用文件位置
ARCSERVE_APP	ARCAAppDB	ARCAAppDB	<input type="button" value="浏览"/>

因为备份能够被复制到网络位置，所以可以被多个 SQL Server 实例使用。可以从实例级执行多个数据库还原（同时）。从该列表，您可以选择数据库实例，并指定新的数据库名称以及将数据库还原到的备用位置。此外，您还可以浏览至数据库要还原到的备用位置。



8. 单击“下一步”打开“还原摘要”对话框。
9. 检查显示的信息以确认所有还原选项和设置都正确。
 - 如果摘要信息不正确，请单击上一步返回到相应对话框，以更改错误设置。
 - 如果摘要信息正确，单击完成以启动还原过程。

第 5 章： CA ARCserve Central HostBased VM Backup 故障排除

本节介绍了故障排除信息，以帮助您确定和解决使用 CA ARCserve Central HostBased VM Backup 时可能会遇到的问题。

此部分包含以下主题：

[当尝试添加节点时，出现“无法连接到指定的服务器”消息](#) (p. 109)

[空白网页出现或者 Javascript 错误发生](#) (p. 111)

[当登录到 CA ARCserve D2D 节点时，没有适当加载网页](#) (p. 112)

[如何解决页面加载问题](#) (p. 114)

[当访问 CA ARCserve Central Applications 时，乱码显示在浏览器 Windows 中](#) (p. 115)

[更新节点时发生访问被拒绝错误](#) (p. 115)

[在您登录到应用程序时，显示证书错误](#) (p. 117)

[快照创建错误导致备份失败](#) (p. 118)

[恢复 VM 操作因未知错误失败](#) (p. 119)

[使用 hotadd 传输模式的备份和恢复操作无法挂接磁盘](#) (p. 121)

[使用 HOTADD 或 SAN 传输模式恢复数据时，恢复操作失败](#) (p. 121)

[发生未找到操作系统错误](#) (p. 123)

[VM 恢复后未保留 MAC 地址更改](#) (p. 124)

[CA ARCserve D2D Web 服务在 CA ARCserve D2D 上失败](#) (p. 125)

[CA ARCserve Central HostBased VM Backup 无法与远程节点上的 CA ARCserve D2D Web 服务进行通信](#) (p. 127)

[CA ARCserve D2D Web 服务运行缓慢](#) (p. 128)

[更改块跟踪失败](#) (p. 130)

[由于 ESXi 许可，备份失败](#) (p. 130)

[备份失败，备份代理系统的事件日志中记录了事件 1530](#) (p. 131)

[指定 hotadd 传输模式时，备份使用 NBD 传输模式完成](#) (p. 132)

[增量备份作业被处理为验证备份作业](#) (p. 133)

[因为无法标识块，所以备份作业失败](#) (p. 133)

[无法打开 VMDK 文件。](#) (p. 134)

[更改节点的名称后节点不显示在“节点”屏幕上](#) (p. 134)

[将策略保存或分配到 CA ARCserve D2D 服务器时发生多连接错误](#) (p. 135)

[因无法访问 ESX 服务器，虚拟机备份失败，](#) (p. 135)

[添加新选项卡链接无法在 Internet Explorer 8、9 和 Chrome 中正确启动](#) (p. 136)

[添加新选项卡链接、RSS 源和社交网络反馈无法在 Internet Explorer 8 和 9 中正确启动](#) (p. 139)

[使用日本键盘时无法在筛选字段中指定星号或下划线作为通配符](#) (p. 140)

[恢复虚拟机使用不同的传输模式，而不是指定模式](#) (p. 140)

[将虚拟机恢复到备选 ESX 服务器或 Hyper-V 服务器时，CA ARCserve Central HostBased VM Backup 不识别动态磁盘上的卷](#) (p. 141)

[在使用 HotAdd 传输模式为大小超过 2 TB 的磁盘备份数据时发生的还原数据问题](#) (p. 142)

当尝试添加节点时，出现“无法连接到指定的服务器”消息

Windows 平台上存在此问题。

症状：

当尝试从“节点”屏幕添加或连接节点时，出现以下消息。

无法连接到指定的服务器。

解决方案：

如果在尝试从“节点”屏幕添加节点时出现以上消息，以下更正操作可以帮助您解决该问题：

- 确保 Windows Server 服务在 CA ARCserve Central HostBased VM Backup 服务器和源虚拟机（节点）上正运行。
- 确保在 CA ARCserve Central HostBased VM Backup 服务器和源虚拟机（节点）上 Windows 防火墙例外应用于 Windows 文件和打印机共享服务。
- 确认仅当节点不属于域时，Windows 防火墙例外才应用于 Windows Netlogon 服务。在 CA ARCserve Central HostBased VM Backup 服务器和源虚拟机（节点）上执行该任务。
- 确认应用于“本地帐户的共享和安全模型”的值是“经典”。要应用“经典”值，请执行以下操作：

注意：在 CA ARCserve Central HostBased VM Backup 服务器和源虚拟机（节点）上执行下列步骤。

1. 登录 CA ARCserve Central HostBased VM Backup 服务器并打开“控制面板”。
2. 在“控制面板”中打开“管理工具”。
3. 双击“本地安全策略”。

此时打开“本地安全策略”窗口。

4. 在“本地安全策略”窗口中展开“本地策略”，然后展开“安全选项”。

此时出现“安全策略”。

5. 右键单击“网络访问:本地帐户的共享和安全模型”，然后单击弹出式菜单上的“属性”。

此时打开“网络访问:本地帐户的共享和安全模型”对话框。

6. 单击“本地安全设置”。

从下拉列表中选择“经典-本地用户以自己的身份验证”。

单击“确定”。

- 确保应用于 LAN 管理器身份验证级别的本地策略的值被设置为“发送 LM 和 NTLM - 若协商使用 NTLMv2 会话安全”。要应用该值，请执行以下操作：

1. 登录到 CA ARCserve Central HostBased VM Backup 服务器，然后打开命令提示符。

执行以下命令

```
secpol.msc
```

“本地安全策略”对话框将打开。

2. 选择本地策略，然后单击安全选项。

搜索“网络安全:LAN 管理器身份验证级别”。

双击该选项。

“属性”对话框打开。

3. 选择以下选项，然后单击“确定”。

发送 LM 和 NTLM - 若协商使用 NTLMv2 会话安全

4. 在命令提示符下，执行以下命令：

```
gpupdate
```

该值即被应用。

空白网页出现或者 Javascript 错误发生

在 **Windows Server 2008** 和 **Windows Server 2003** 操作系统上有效。

症状:

使用 Internet Explorer 打开 CA ARCserve Central Applications 网站时, 空白网页显示, 或者发生 Javascript 错误。在 Windows Server 2008 和 Windows Server 2003 操作系统上打开 Internet Explorer 时, 发生该问题。

此问题在以下条件下发生:

- 您正在使用 Internet Explorer 8 或 Internet Explorer 9 查看您的应用程序, 并且浏览器未将该 URL 识别为是受信任站点。
- 您正在使用 Internet Explorer 9 查看您的应用程序时, 正在使用的通信协议是 HTTPS。

解决方案:

要解决该问题, 请禁用您用来查看应用程序的计算机上的 Internet Explorer “增强的安全性”。

要在 **Windows Server 2008** 系统上禁用 Internet Explorer 的 “增强的安全性”, 请执行以下操作:

1. 使用管理员帐号或有管理权限的帐号登录到用于查看报表的 Windows Server 2008 计算机。
2. 右键单击桌面的 “计算机”, 然后单击 “管理” 以打开 “服务器管理器” 窗口。
3. 从 “服务器管理器” 窗口, 单击 “服务器管理器” (服务器名称)。

从 “服务器摘要” 部分, 打开 “安全信息”, 单击 “配置 IE ESC”, 如下所示:



Internet Explorer “增强的安全配置” 对话框打开。

4. 在 Internet Explorer “增强的安全配置”对话框上，执行以下操作：

- 关闭 Administrators--Click 检查
- Users--单击“关”。

单击“确定”。

Internet Explorer “增强的安全配置”对话框关闭，Internet Explorer 的“增强的安全性”即被禁用。

要在 Windows Server 2003 系统上禁用 Internet Explorer 的“增强的安全性”，请执行以下操作：

1. 使用管理员帐号或有管理权限的帐号登录到用于查看报表的 Windows Server 2003 计算机。
2. 打开 Windows “控制面板”，然后打开“添加或删除程序”。
3. 从“增加或删除程序”对话框，单击“添加/删除 Windows 组件”选项以访问“Windows 组件向导”屏幕。

清除 Internet Explorer “增强的安全配置”旁边的复选框。

单击“下一步”。

按照屏幕上的说明完成配置，然后单击“完成”。

Internet Explorer 的“增强的安全性”即被禁用。

当登录到 CA ARCserve D2D 节点时，没有适当加载网页

Windows 平台上存在此问题。

症状：

当从“节点”屏幕登录到 CA ARCserve D2D 节点时，浏览器中的网页加载不正确、显示错误消息或者这两种情况都会发生。

解决方案：

此行为主要影响 IE 浏览器。当 Active 脚本编制、ActiveX 控件或 Java 程序在您的计算机上禁用或在您的网络上阻止时，Web 页可能加载不正确。

您可以通过刷新您的浏览器窗口来纠正此问题。但是，如果刷新浏览器窗口没有纠正此问题，请执行以下操作：

1. 打开 Internet Explorer。
在“工具”菜单中，单击“Internet 选项”。
“Internet 选项”对话框将打开。
2. 单击“安全”选项卡。
将出现“安全”选项。
3. 单击“Internet”区域。
将显示“Internet”区域选项。
4. 单击“自定义级别”。
“安全设置 - Internet 区域”对话框将打开。
5. 滚动到“脚本”类别。
找到“活动脚本”。
单击“启用”或“提示”选项。
6. 在“安全设置 - Internet 区域”对话框上单击“确定”。
“安全设置 - Internet 区域”对话框将关闭。
7. 单击“Internet 选项”对话框的“确定”。
“Internet 选项”对话框将关闭，“活动脚本”选项将应用。

注意：如果此解决方案没有改正此问题，请咨询您的系统管理员，验证其他程序（如反病毒或防火墙程序）没阻止活动脚本、ActiveX 控件或 Java 程序。

如何解决页面加载问题

Windows 平台上存在此问题。

症状:

在您登录到 CA ARCserve Central Applications、CA ARCserve D2D 节点以及监视服务器时，以下错误消息显示在浏览器窗口中。

消息 1:

该网页上的错误可能导致它无法正常工作。

消息 2:

!

解决方案:

由于种种理由，网页无法正确加载。下表说明通常原因和相应解决措施：

原因	解决措施:
基础 HTML 源代码有问题。	刷新网页，然后再试一次。
您的网络阻挡了活动脚本、ActiveX 或 Java 程序。	允许您的浏览器使用活动脚本、ActiveX 或 Java 程序。
您的防病毒应用程序已配置为扫描临时 Internet 文件和下载的程序。	筛选您的防病毒应用程序，以便允许与 CA ARCserve Central Applications 网页关联的 Internet 相关文件。
安装在您的计算机上的脚本引擎损坏或过时。	更新脚本引擎。
安装在您的计算机上的显卡驱动程序损坏或过时。	更新显卡驱动程序。
安装在您的计算机上的 DirectX 组件损坏或过时。	更新 <DirectX> 组件。

当访问 CA ARCserve Central Applications 时，乱码显示在浏览器 Windows 中

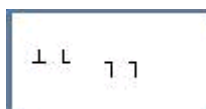
在所有 Windows 操作系统上有效。所有浏览器受到影响。

症状：

在您登录到 CA ARCserve Central Applications 时，乱码显示在您的浏览器窗口的内容区域中。

解决方案：

在使用 HTTPS 通信安装 CA ARCserve Central Applications，然后试图使用 HTTP 通信访问 CA ARCserve Central Applications 时便发生该问题。基础 CA ARCserve Central Applications Web 服务组件无法将 HTTP URL 转化成 HTTPS URL。因此，乱码便显示在您的浏览器窗口中。例如：



为了解决该问题，安装或配置应用程序使用 HTTPS 通信时请使用 HTTPS 访问 CA ARCserve Central Applications。

更新节点时发生访问被拒绝错误

在支持用户帐户控制 (UAC) 的所有 Windows 操作系统上有效。

注意： Windows Vista 或更高版本。

症状 1：

如果您提供的 Windows 用户帐户不是内置管理员或域用户帐户，且属于管理员组成员，那么当在“从 vCenter/ESX 导入虚拟机”对话框的“节点凭据”对话框输入密码时，会显示以下消息：

需要管理员权限。

结果导致您无法应用节点凭据。

症状 2：

如果在导入操作期间导入节点但不提供节点凭据，那么当尝试使用不是内置管理员或域用户帐户且属于管理员组成员的 Windows 用户帐户执行更新节点操作时，会显示以下消息：

拒绝访问。请确保用户具有管理员权限，远程注册表访问不受已添加计算机的本地安全策略限制。

结果导致您无法更新节点。

解决方案:

当计算机上运行的 Windows 操作系统支持 UAC 时,那么在该计算机上启用 UAC 则可出现这种预期行为。UAC 是 Windows 的一种功能,仅允许管理员帐户从远程位置登录计算机。

使用以下方法之一解决此问题:

- 提供内置或域管理员凭据。
- 禁用 UAC:
 1. 使用管理员帐户登录到节点。
 2. 打开 Windows “控制面板”。
 3. 打开 “用户帐户”。
 4. 从 “更改用户帐户” 屏幕中,单击 “更改用户帐户控制设置”,然后执行以下操作之一:
 - **Windows Vista 和 Windows Server 2008:** 在 “更改用户帐户” 屏幕中,单击 “启用或禁用用户帐户控制(UAC)”。然后在 “打开用户帐户控制(UAC)以使您的计算机更安全” 屏幕中,清除 “使用用户帐户控制(UAC)帮助保护您的计算机” 旁的复选框,然后单击 “确定”。

重新启动计算机以应用对 UAC 的更改。
 - **Windows Server 2008 r2 和 Windows 7:** 在 “选择何时通知您有关计算机更改的消息” 屏幕中,将滑块从 “始终通知” 移到 “从不通知”。单击 “确定”,关闭 Windows 控制面板。

重新启动计算机以应用对 UAC 的更改。

在您登录到应用程序时，显示证书错误

Windows 平台上存在此问题。

症状：

在您登录到应用程序时，以下消息在您的浏览器窗口中显示：

- **Internet Explorer:**

该网站的安全证书有问题。

- **Firefox:**

该连接不可信。

- **Chrome:**

该站点的安全证书不可信！

如果指定让您继续访问该网站的选项，您便可以成功登录该应用程序。然而，每次登录该应用程序时，您都会遇到该状况。

解决方案：

当您指定使用 **HTTPS** 作为通信协议时，该状况就会发生。要暂时性地解决该问题，请在您的浏览器窗口中单击让您继续访问该网站的链接。然而，下次登录到该应用程序，您会再次遇到该消息。

与 **HTTP** 通信协议相比，**HTTPS** 协议通信提供更高的安全性。如果想继续使用 **HTTPS** 通信协议通信，您可以从 **VeriSign** 购买安全证书，然后在应用程序服务器上安装该证书。或者，您可以将该应用程序使用的通信协议更改为 **HTTP**。要将通信协议更改为 **HTTP**，请执行以下操作：

1. 登录到安装该应用程序的服务器。

2. 浏览到以下目录：

`C:\Program Files\CA\ARCserve Central Applications\BIN`

3. 执行以下批处理文件：

`ChangeToHttp.bat`

4. 在批处理文件执行之后，打开 **Windows** 服务器管理器。

重新启动以下服务：

`CA ARCserve Central Applications 服务`

快照创建错误导致备份失败

Windows 平台上存在此问题。

提交基于虚拟机的 VMware 备份时，会出现以下症状：

症状 1

备份作业失败，活动日志中显示下列消息：

无法拍取快照。ESX/vCenter 报告错误。发生常规系统错误。VMX 的协议错误。

解决方案 1

该错误是一个 VMware 问题。要解决该问题，请在来宾操作系统内卸载并重新安装 VMware Tools，然后重新提交作业。

症状 2

备份作业失败，活动日志中显示下列消息：

无法拍取虚拟机的快照。ESX Server/vCenter Server 报告以下错误：无法创建静止的快照，因为创建快照操作超出在冻结的虚拟机中暂停 I/O 的时间限制。

解决方案 2

当 VSS 创建快照出错时，发生此错误。VSS 可能会在下列情况下发生错误：

VSS 编写器的状态不稳定。

要确定发生这种行为的原因并加以纠正，请采取下列补救措施：

1. 在虚拟机的来宾操作系统上，从命令行运行“vssadmin list writers”命令。
2. 确认所有 VSS 编写器均处于正常状态。
3. 如果编写器处于下列状态，请联系 Microsoft 或编写器的供应商，了解有关修复这些错误的信息。

```
state=Failed  
Last Error=No Error
```

注意：重新启动编写器通常可以解决该问题。

VSS 在创建快照时出错。

要确定发生这种行为的原因并加以纠正，请采取下列补救措施：

1. 审查来宾操作系统中的 Windows 事件日志。检查开始备份时是否存在与 VSS 组件有关的错误。
2. 当 VSS 因磁盘空间不足报告错误时，请释放卷上与该错误相关的磁盘空间。
3. 当 VSS 或 Windows Volsnap 驱动程序出现超时错误时，虚拟机内部运行的应用程序处于高度活跃状态。高度活跃的状态会阻碍 VSS 创建一致的快照。要纠正该情况，请安排在应用程序对卷执行较少的输入和输出操作时进行备份。
4. 当 Windows 事件日志指示 VolSnap 驱动程序遇到错误时，请参阅 Microsoft Technet Library 中的 [Volume Snapshot Driver Integrity](#) 文章，了解如何纠正 VolSnap 驱动程序错误的信息。

恢复 VM 操作因未知错误失败

在 Windows 系统上有效。

症状：

恢复虚拟机操作失败。您可以提交恢复 VM 作业，但是以下消息显示在活动日志中：

无法恢复虚拟磁盘。

此外，VDDK 报告以下错误消息：

未知错误。

解决方法 1:

要解决此问题，请考虑以下解决方案：

- 当原始数据存储中没有足够的可用磁盘空间时，恢复 VM 作业会失败。VDDK 返回消息，因为 VDDK API（当前）无法检测到原始数据存储上的可用磁盘空间量。（数据存储是您指定用于恢复虚拟机的位置。）要解决此问题，请在原始数据存储中释放完成该操作所需的磁盘空间量，然后重新提交作业。
- 网络干扰和高网络流量可能导致恢复 VM 作业失败。要解决此问题，请确认代理服务器以及 ESX Server 系统或 vCenter Server 系统可以通过网络互相通信，然后重新提交作业。
- 包括将 VM 作业备份或恢复到 ESX Server 系统或 vCenter Server 系统的多个并行连接（其中包括通过 VMware vSphere Client 的 vSphere SDK 连接）可能会导致这些作业失败。要解决此问题，请关闭所有不必要的连接，然后重新提交作业。有关允许的并行连接的最大数量的信息，请参阅[无法打开 VMDK 文件](#) (p. 134)。
- 检查 VMware vSphere Client 日志的“任务和事件”部分，以发现特定虚拟机的内部错误。更正内部错误，然后重新提交作业。

示例：另一个应用程序或操作正在使用 VMDK 文件。要解决此问题，请释放该文件，然后重新提交作业。

解决方法 2:

此问题在以下条件下发生：

- VDDK 未正确处理快照。
- VDDK 未手动删除快照或在虚拟机内部。

要解决此问题，请重新提交作业。如果作业再次失败，请删除恢复的虚拟机，然后重新提交作业。

使用 hotadd 传输模式的备份和恢复操作无法挂接磁盘

Windows 平台上存在此问题。

症状:

使用 hotadd 传输模式的备份和恢复作业无法向代理系统挂接磁盘。

解决方案:

要解决此问题，请执行以下操作：

1. 打开 VMware vSphere Client。
使用管理凭据登录到 ESX Server 系统或 vCenter Server 系统。
2. 选择代理虚拟机，并编辑该代理虚拟机的设置。
3. 删除附加到源虚拟机或代理虚拟机的 hotadd 磁盘。
4. 重新提交作业。

使用 HOTADD 或 SAN 传输模式恢复数据时，恢复操作失败

Windows 平台上存在此问题。

症状:

使用 HOTADD 或 SAN 传输模式恢复数据时，恢复操作失败 下列消息显示在活动日志中：

发生未知错误。联系技术支持。

解决方案:

未正确配置磁盘设置时，如果使用 [HOTADD 传输模式](#) (p. 179)或 [SAN 传输模式](#) (p. 179)，恢复操作失败。

要配置磁盘，请执行以下步骤:

1. 使用具有管理权限的帐号登录到备份代理系统。
2. 打开 Windows 命令行。
3. 在命令行上，键入以下命令：
`diskpart`
按 Enter 键。
4. 键入 SAN，然后按下 Enter 键。
当前 SAN 策略显示。

5. 键入以下命令：

```
SAN POLICY = OnlineAll
```

按 Enter 键。

SAN 策略被配置成，不自动挂接 SAN 承载的卷。

6. 要清除特定 SAN 磁盘的只读属性，请从磁盘列表中选择磁盘，然后键入以下命令：

```
attribute disk clear readonly
```

按 Enter 键

7. 键入 exit，然后按下 Enter 键。

磁盘即被配置，然后您可以重新提交作业。

如果作业再次失败，请使用代理系统上的磁盘管理手动挂接 HOTADD 磁盘。

要手动挂接磁盘，请执行以下步骤：

1. 使用具有管理权限的帐号登录到备份代理系统。
2. 打开 Windows “控制面板”，然后双击“管理工具”。
“管理工具”窗口打开。
3. 从“收藏”列表，双击“计算机管理”。
“计算机管理”对话框打开。
4. 展开“存储”，然后单击“磁盘管理”。
磁盘显示。
5. 右键单击要挂接的磁盘，然后单击“联机”。

磁盘即被挂接，您便可以重新提交作业。

发生未找到操作系统错误

在 **Windows** 平台上有效。

症状 1

当您使用“还原到备用位置”选项恢复虚拟机后，尝试启动虚拟机上的访客操作系统时，出现下列消息：

未找到操作系统。

解决方案 1

以上行为可在包含 **SCSI** 和 **IDE** 设备的虚拟机上发生。如果发生该问题，请检查磁盘在您的虚拟机上的配置方式，并确认已恢复虚拟机的启动顺序是否与源虚拟机一样。如果启动顺序不同，您必须更新已恢复虚拟机上的 **BIOS** 以便匹配源虚拟机的启动顺序。

注意： 第一个 **IDE** 磁盘应当使用 **(0:1)**。

症状 2

当您恢复虚拟机后，尝试启动虚拟机上的访客操作系统时，出现下列消息：

未找到操作系统。

解决方案 2

如果发生以上问题，请检查磁盘在虚拟机上的配置方式，并确认副本虚拟机的启动顺序是否与源虚拟机一样。

VM 恢复后未保留 MAC 地址更改

在 **Windows** 平台上有效。

症状:

恢复虚拟机后不再保留虚拟机的 MAC 地址。

解决方案:

恢复期间不保留 MAC 地址以防止重复。要保留 MAC 地址信息，请在代理服务器上设置以下注册表项：

位置: SOFTWARE\CA\CA ARCSERVE D2D

键名: RetainMACForVDDK

值类型: 字符串

键值: 1

在具有两个 NIC 卡的虚拟机上，如果您想将其中一个设为“手工”，请设置 RetainMACForVDDK 注册表项。否则，所有卡都会在恢复之后设为“自动”。

CA ARCserve D2D Web 服务在 CA ARCserve D2D 上失败

Windows 平台上存在此问题。

症状:

运行在 CA ARCserve D2D 节点上的 Web 服务启动，然后失败，或无法启动。

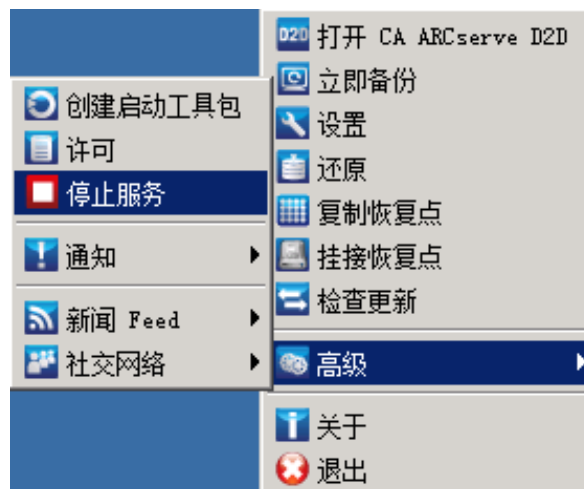
解决方案:

当 CA ARCserve D2D web 服务使用的端口与 VMware vCenter web 服务（Tomcat）使用的端口一样时，就会发生该问题。

CA ARCserve D2D 使用的端口可能与 Tomcat 使用的默认端口发生冲突。在 Tomcat 之前启动 CA ARCserve D2D 时，该冲突将导致 Tomcat 失败。要解决该问题，您可以按如下方式更改 Tomcat 默认端口：

1. 访问 CA ARCserve D2D 监视器，单击“高级”选项，然后选择“停止服务”。

CA ARCserve D2D Web Service 被停止。




2. 访问 Tomcat server.xml 文件以编辑/配置 Tomcat 的行为。

Tomcat server.xml 文件位于以下文件夹结构中：

C:\Program Files\CA\ARCserve Central Applications\TOMCAT\conf

3. 在 server.xml 文件内找到 <Server> 标记。



```
无标题 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<!-- Note: A "Server" is not itself a "Container", so you may not
define subcomponents such as "valves" at this level.
Documentation at /docs/config/server.html
-->
-->
<Server>
  <!--APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleListe
  <!--Initialize Jasper prior to webapps are loaded. Documentatio
  <Listener className="org.apache.catalina.core.JasperListener"/>
  <!-- JMX support for the Tomcat server. Documentation at /docs/
  <Listener className="org.apache.catalina.mbeans.ServerLifecycle
  <Listener className="org.apache.catalina.mbeans.GlobalResources
  <!-- Global JNDI resources
  Documentation at /docs/jndi-resources-howto.html
  -->
  <GlobalNamingResources>
    <!-- Editable user database that can also be used by
```

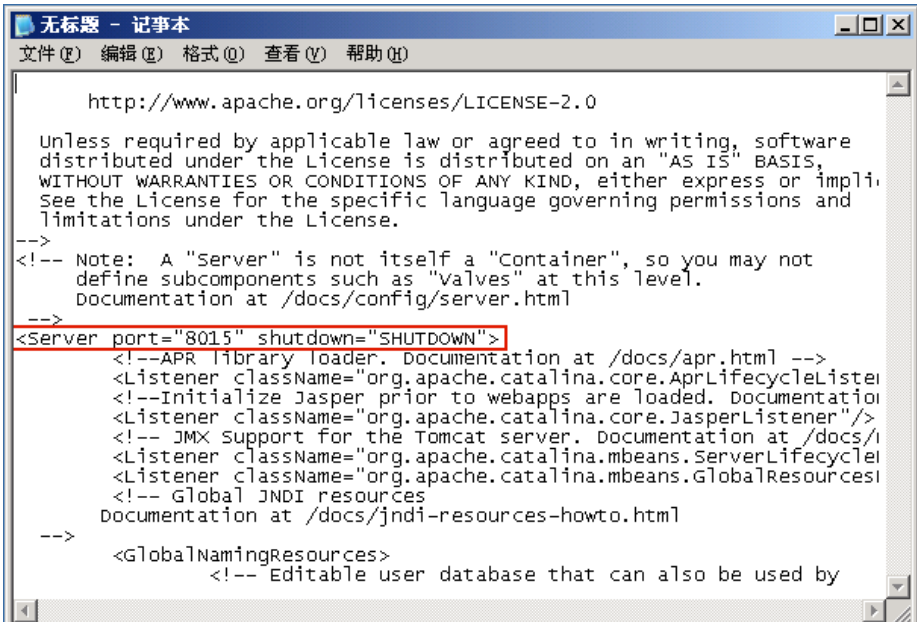
4. 按如下方式编辑 <Server> 标记:

从:

<Server>

到:

<Server port="8015" shutdown="SHUTDOWN">



```
无标题 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<!-- Note: A "Server" is not itself a "Container", so you may not
define subcomponents such as "valves" at this level.
Documentation at /docs/config/server.html
-->
-->
<Server port="8015" shutdown="SHUTDOWN">
  <!--APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleListe
  <!--Initialize Jasper prior to webapps are loaded. Documentatio
  <Listener className="org.apache.catalina.core.JasperListener"/>
  <!-- JMX support for the Tomcat server. Documentation at /docs/
  <Listener className="org.apache.catalina.mbeans.ServerLifecycle
  <Listener className="org.apache.catalina.mbeans.GlobalResources
  <!-- Global JNDI resources
  Documentation at /docs/jndi-resources-howto.html
  -->
  <GlobalNamingResources>
    <!-- Editable user database that can also be used by
```

5. 保存并关闭 web.xml 文件。

关闭 Tomcat 的命令现在便得到配置，这样，必须在指定端口 (8015) 上由服务器接收该命令。

6. 访问 CA ARCserve D2D 监视器，单击“高级”选项，然后选择“启动服务”。

CA ARCserve D2D Web Service 被启动。

CA ARCserve Central HostBased VM Backup 无法与远程节点上的 CA ARCserve D2D Web 服务进行通信

在 Windows 系统上有效。

症状：

CA ARCserve Central HostBased VM Backup 无法与远程节点上的 CA ARCserve D2D Web 服务进行通信

解决方案：

下表描述 CA ARCserve Central HostBased VM Backup 无法与远程节点上的 CA ARCserve D2D Web 服务进行通信的原因以及相应的解决措施：

原因	解决措施：
当应用策略时，网络不可用或不稳定。	请确保网络可用并且稳定，然后重试。
在应用程序试图与节点进行通信时，CA ARCserve D2D 计算机无法可以处理该负荷。	请确保远程 CA ARCserve D2D 节点的 CPU 处于正常状态，然后重试。
当应用策略时，远程节点上的 CA ARCserve D2D 服务未运行。	请确保远程节点上的 CA ARCserve D2D 正在运行，然后重试。
CA ARCserve D2D 服务未正常通信。	请重新启动远程节点上的 CA ARCserve D2D 服务，然后重试。

CA ARCserve D2D Web 服务运行缓慢

在 Windows 系统上有效。

症状 1:

在 CA ARCserve D2D 系统上的 CA ARCserve D2D Web 服务运行缓慢。您可以检测到其他症状，如：

- CA ARCserve D2D Web 服务停止响应或占用 100% 的 CPU 资源。
- CA ARCserve D2D 节点性能下降或无法与 Web 服务进行通信。

解决方法 1:

在各种环境配置中，您会发现 CA ARCserve D2D Web 服务占用过多的 CPU 时间，或响应缓慢。默认情况下，Tomcat 被配置为将有限内存量分配给节点，这可能不适合于您的环境。要验证该问题，请查看以下日志文件：

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log  
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stderr.*.log  
<D2D_home>\TOMCAT\logs\catalina.*.log  
<D2D_home>\TOMCAT\logs\localhost.*.log
```

搜索以下消息：

```
java.lang.OutOfMemoryError
```

要解决该问题，请增加分配的内存量。

要增加内存，请执行以下操作：

1. 打开注册表编辑器，并选择以下注册表项：

- x86 操作系统：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun  
2.0\CASAD2DWebSvc\Parameters\Java
```

- x64 操作系统：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software  
Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
```


2. 执行以下操作之一：

- 如果日志文件中的消息是：

```
java.lang.OutOfMemoryError: PermGen space
```

将以下内容附加到 Options 的值后面。

```
-XX:PermSize=128M -XX:MaxPermSize=128M
```

注意：您可能需要增加 -XX:MaxPermSize 的值以满足您的环境的要求。

- 如果日志文件中的消息为以下消息之一：

```
java.lang.OutOfMemoryError: Java heap space
```

```
java.lang.OutOfMemoryError: GC overhead limit exceeded
```

增加以下 DWORD 的值：

```
JvmMx
```

3. 重新启动 CA ARCserve D2D Web 服务。

症状 2

排定的备份将被跳过并停止运行。

解决方案 2

当您将并行备份的 MAX 值配置为 20 或小于 20 时，请执行下列操作：

1. 增加以下 DWORD 的值：

```
JvmMx=256
```

注意：此 DWORD 在解决方案 1 中被引用。

2. 将以下内容附加到 Options 的值后面。

```
-XX:MaxPermSize=128M
```

注意：此 DWORD 在解决方案 1 中被引用。

当您将并行备份的 MAX 值配置为大于 20 或小于 50 时，请执行下列操作：

1. 增加以下 DWORD 的值：

```
JvmMx=512
```

注意：此 DWORD 在解决方案 1 中被引用。

2. 将以下内容附加到 Options 的值后面。

```
-XX:MaxPermSize=256M
```

注意：此 DWORD 在解决方案 1 中被引用。

更改块跟踪失败

在 **Windows** 上有效。

症状：

虚拟机备份失败，并在虚拟机上启用了更改块跟踪。

解决方案：

下表描述了可能导致启用了更改块跟踪的虚拟机备份失败的环境条件：

条件	解决方法
虚拟机上存在用户生成的快照，并且禁用了更改块跟踪。	启用或重置更改块跟踪，让完全备份作业继续执行。 注意： 完全备份作业利用 VMDK 文件中已使用和未使用的数据块继续执行。
虚拟机上安装的 VMware 硬件版本不正确。	验证虚拟机上是否安装了 VMware 硬件 7.0 版或更高版本。
虚拟机上安装的 ESX Server 版本不正确。	验证虚拟机上是否安装了 ESX Server 4.0 版或更高版本。
ESX Server 系统遇到了硬关闭。硬关闭可能会导致更改块跟踪备份失败。	CA ARCserve Central HostBased VM Backup 自动在虚拟机上启用更改块跟踪。
当虚拟机处于打开状态时，ESX Server 系统遇到了（完全）重新启动。	CA ARCserve Central HostBased VM Backup 自动在虚拟机上启用更改块跟踪。
使用 Storage vMotion 移动了虚拟机。	CA ARCserve Central HostBased VM Backup 自动在虚拟机上启用更改块跟踪。

由于 ESXi 许可，备份失败

Windows 平台上存在此问题。

症状：

CA ARCserve D2D 完全、增量和验证备份作业失败。下列消息显示在 CA ARCserve D2D 活动日志中：

VM 服务器 <server_name> 不具有已付费的 ESX 许可

解决方案：

由于 VMware 限制，无法备份运行在有免费许可的 ESXi 服务器上的虚拟机。要保护这些 VM，请应用购买的许可。

备份失败，备份代理系统的事件日志中记录了事件 1530

在 Windows 平台上有效。

症状：

CA ARCserve Central HostBased VM Backup 作业失败。事件 1530 记录在备份代理系统的应用程序事件日志中。

环境/再现步骤：

- Microsoft SQL Server 或 Microsoft Exchange Server 已安装在虚拟机上。
- 用户使用管理员帐户或作为管理员组的成员的帐户登录到或已经登录到 CA ARCserve Central HostBased VM Backup 代理服务器。
- 备份作业启动后，用户从代理服务器注销。
- 备份作业失败。事件 1530 已记录在应用程序事件日志中。

警告... Microsoft-Windows-User Profiles Service 1530 没有 Windows 检测到其他应用程序或服务仍在使用您的注册表文件。此文件即将卸载。之后，承载您的注册表文件的应用程序或服务可能无法正常运行。

原因：

Windows Server 2008 包含会用户从计算机注销时卸载用户配置文件的用户配置文件服务。因此，可能不会创建 COM 对象，从而导致 Host-Based VM Backup 无法调用其 COM 模块。

解决方案：

要防止备份作业失败，请完成下列步骤：

注意：必须具备上述所有症状，此解决方案才有效。

1. 使用管理员帐户或作为管理员组的成员的帐户，登录到 Host-Based VM Backup 代理服务器。
2. 在“运行”对话框中输入 gpedit.msc，启动本地组策略编辑器。
3. 从本地组策略编辑器中，依次展开“计算机配置”、“管理模板”、“系统”和“用户配置文件”。
4. 从“用户配置文件”目录中，双击“用户注销时不强制卸载用户注册表”以打开“用户注销时不强制卸载用户注册表”对话框。
5. 从“用户注销时不强制卸载用户注册表”对话框中，单击“已启用”，然后单击“确定”。

注意：值 DisableForceUnload 现已添加至注册表。

6. 重新启动 Host-Based VM Backup 服务器。

指定 hotadd 传输模式时，备份使用 NBD 传输模式完成

Windows 平台上存在此问题。

症状：

为备份指定 [hotadd 传输模式](#) (p. 179)时虚拟机备份使用 [NBD 传输](#) (p. 179) 模式完成。

解决方案：

CA ARCserve Central HostBased VM Backup 使您可以备份在 ESX Server 系统上的虚拟机。使用 hotadd 传输模式备份虚拟机时，您最多可以将 15 个虚拟磁盘连接到 CA ARCserve D2D 虚拟机代理服务器上的每个 SCSI 控制器。提交包括 15 个以上虚拟磁盘的备份，并且 CA ARCserve D2D 虚拟机代理服务器上仅有一个 SCSI 控制器时，该单个 SCSI 控制器无法容纳所有虚拟机。因此，CA ARCserve Central HostBased VM Backup 将备份 NBD 传输模式的数据。

要防止发生此行为，请验证在 CA ARCserve D2D 虚拟机代理服务器上是否有足够数量的 SCSI 控制器可以容纳备份作业中的所有虚拟机。

增量备份作业被处理为验证备份作业

在 Windows 上有效。

症状：

提交或排定使用 Hotadd 传输模式处理的增量备份作业时，将发生下列行为：

- 增量备份作业转成验证备份作业。针对该作业的活动日志条目指示增量备份作业已转成验证备份作业。
- 备份的虚拟机的 VI 客户端的快照管理器包含合成的帮手快照。
- 受影响的虚拟机的 VI 客户端中的“编辑设置”对话框指示备份代理系统上连接了错误的磁盘。与错误磁盘关联的 VMDK URL 和与备份代理系统关联的 VMDK URL 不同。

解决方案：

要更正此行为，请使用在 [VMware 知识库文章 1003302](#) 中所描述的说明从备份代理系统中删除错误的 VMDK 文件（磁盘）。此外，VMware 建议在数据存储的可用空间的数量要是虚拟机文件累积大小的两倍。

因为无法标识块，所以备份作业失败

在 Windows 上有效。

症状：

对于特定虚拟机，所有备份作业失败，下列消息显示在活动日志中：
应用程序无法识别虚拟机上使用或更改的块。在虚拟机运行期间重新启动 ESX Server 系统时，可能会发生此问题。下次备份作业运行时，应用程序将重置更改块跟踪，并执行验证备份操作。

解决方案：

要解决该问题，请在虚拟机上执行磁盘合并操作。要执行磁盘合并，请执行以下步骤。

1. 打开 VMware VI Client。
2. 展开受影响的虚拟机的 ESX 服务器系统。
3. 右键单击受影响的虚拟机，选择“快照”，然后单击弹出菜单上的“合并”以合并磁盘。
4. 重新提交备份。

无法打开 VMDK 文件。

Windows 平台上存在此问题。

症状：

多个并行备份作业在 NBD（或 LAN）传输模式下失败。下列消息显示在活动日志中：

无法打开 VMDK 文件。

解决方案：

这是 VMware 连接限制。下列的网络文件复制 (NFC) 协议限制适用：

- ESX 4：最多 9 个直接连接
- ESX 4 到 vCenter Server：最多 27 个连接
- ESXi 4：最多 11 个直接连接
- ESXi 4 到 vCenter Server：最多 23 个连接

不能跨磁盘共享连接。最大限制不适用于 SAN 和 hotadd 连接。如果 NFC 客户端无法正确关闭，连接可以仍打开十分钟。

更改节点的名称后节点不显示在“节点”屏幕上

在 **Windows** 平台上有效。

症状：

将节点添加到“节点”屏幕后，该节点的主机名便发生更改。节点便不再显示在“节点”屏幕上。

解决方案：

此行为是正常的。CA ARCserve Central HostBased VM Backup 保持该节点被从节点屏幕添加时所具有的名称。当重命名该节点，应用程序将无法检测到该节点。因此，节点不显示在节点屏幕上。

要在节点屏幕显示重命名的节点，请执行以下操作：

1. 重命名节点。
2. 打开“节点”屏幕，[删除重命名的节点](#) (p. 45)。
3. 使用新名字添加节点。

将策略保存或分配到 CA ARCserve D2D 服务器时发生多连接错误

在所有 Windows 平台上有效。

症状:

在您尝试将策略保存或分配到 CA ARCserve D2D 服务器时，以下错误消息会出现：

验证备份目标失败。不允许通过同一用户使用多个用户名并行连接到服务器或共享资源。断开所有以前到服务器或共享资源的连接，然后重试。

解决方案:

如果在您尝试将策略保存或分配到 CA ARCserve D2D 服务器时出现上述消息，以下纠正性操作可以帮助您解决该问题：

- “计算机(或域)名称\用户名”指定“用户名”字段。
- 转到承载共享文件夹的远程服务器，然后从 CA ARCserve Central Applications 服务器或 CA ARCserve D2D 服务器删除所有会话。执行以下操作之一来删除会话：
 - 运行以下命令行：

```
net session \\machinename /delete
```
 - 转到以下目录来断开该会话：

```
Compmgmt.msc > 系统工具 > 共享文件夹 > 会话 > 断开会话
```
- 确认您正使用同样的用户名访问远程共享文件夹。
- 再次保存和部署策略。

因无法访问 ESX 服务器，虚拟机备份失败，

Windows 平台上存在此问题。

症状:

虚拟机备份失败。下列消息显示在活动日志中：

无法创建虚拟机快照。

解决方案:

多个备份在一个 ESX Server 系统上并行运行时，虚拟机备份会失败。多个备份在多个 ESX Server 系统上并行运行时，该问题不会发生。为了备份虚拟机，CA ARCserve Central HostBased VM Backup 拍取虚拟机上的数据的快照。多个快照操作在一个系统上同时进行，ESX Server 系统会停止响应。虽然 ESX Server 系统停止响应的时间是暂时的，但备份操作被中断，这会导致备份操作失败。

要防止备份失败，请使用适合您的环境的解决方案：

- 减少您同时备份的虚拟机的数量。例如，如果您同时备份 8 个虚拟机，将数量减少到 7 个虚拟机，重新提交备份，然后分析结果。必要时，减少备份的虚拟机的数量，直到备份不失败，或上面的消息不显示在活动日志中。

要在备份中减少虚拟机的数量，您应从策略取消分配虚拟机。有关详细信息，请参阅从虚拟机取消分配策略。

- 定义并行备份的数量限制 该方法帮助您控制在环境中可以同时运行的备份作业的数量。有关详细信息，请参阅[定义并行备份数量限制](#) (p. 169)。

添加新选项卡链接无法在 Internet Explorer 8、9 和 Chrome 中正确启动

在 Windows 上有效

症状:

如果向导航栏中添加一个指定 HTTPS URL 的新选项卡链接，单击该新选项卡时会显示以下错误消息：

- Internet Explorer 8 和 9:
因为内容未由有效的安全证书签署，因此被阻止。
- Chrome:
网页不可用。

解决方案:

要为 Internet Explorer 更正此问题，请执行以下操作：

- **Internet Explorer 8:**
单击消息栏并选择“显示阻止的内容”。
- **Internet Explorer 9:**
在页面底部的消息栏中单击“显示内容”按钮。页面将刷新，并成功打开添加的选项卡链接。

要为 Chrome 更正此问题，请执行下列步骤：

第 1 步 - 导出证书:

1. 在 Chrome 中打开新选项卡，并输入 HTTPS URL。
将显示警告消息“站点的安全证书不受信任!”
2. 从地址栏中，单击带有“X”的锁。
将打开一个带有“认证信息”链接的弹出窗口。
3. 单击“证书信息”链接。
此时将打开“证书”对话框。
4. 单击“详细信息”选项卡，然后单击“复制到文件”，将证书保存到您的本地计算机。
此时将打开“证书导出向导”对话框。

5. 单击“下一步”选择导出文件时所要使用的格式。
注意：默认情况下会选择 DER 编码二进制文件 X.509 (.CER)。
6. 单击“下一步”浏览到要保存证书的位置。
7. 单击“下一步”完成“证书导出向导”，然后单击“完成”。
证书成功导出。

第 2 步 - 导入证书：

1. 从 Chrome 中打开“工具选项”。
此时将打开“选项”屏幕。
2. 选择“高级选项”选项，并单击“管理来自 HTTPS/SSL 的证书”。
此时将打开“证书”对话框。
3. 单击“导入”。
此时将打开“证书导入向导”对话框。
4. 单击“下一步”，以浏览您在本地计算机上保存的证书。
5. 单击“下一步”打开“证书存储”。
此时将打开“证书存储”对话框。
6. 单击“浏览”打开“选择证书存储”对话框。
此时将打开“选择证书存储”对话框。
7. 从文件列表中选择“可信根证书颁发机构”，然后单击“确定”。
将显示“证书存储”对话框。
8. 单击“下一步”完成“证书导入向导”，然后单击“完成”。
“安全警告”对话框将打开，指出您即将安装证书。
单击“是”接受协议条款。

成功导入证书。

添加新选项卡链接、RSS 源和社交网络反馈无法在 Internet Explorer 8 和 9 中正确启动

在 Windows 上有效

症状:

对于 HTTPS CA ARCserve Central Applications URL:

如果向导航栏中添加一个指定 HTTP URL 的新选项卡链接，单击该新选项卡和反馈链接时会显示以下错误消息:

到网页的导航已取消。

此外，不会显示 RSS 源。

注意: 即使您不选择新添加的选项卡链接，反馈链接也会显示该错误消息。

解决方案:

要解决此问题，请执行以下操作:

■ **Internet Explorer 8:**

在登录后，当弹出安全警告消息“是否只查看安全传送的网页内容?”时单击“否”。单击“否”允许将不安全内容发送至您的网页。

■ **Internet Explorer 9:**

在页面底部显示的消息栏中单击“显示所有内容”按钮。页面将刷新，并成功打开添加的选项卡链接。

使用日本键盘时无法在筛选字段中指定星号或下划线作为通配符

在 Windows 上有效

症状:

由于美国键盘和日本键盘之间键码不同，日本键盘不允许在以下筛选字段中输入通配符“*”和其他特殊字符（如下划线字符“_”）：

■ 仅适用于 Firefox:

- “节点” > “添加组” - “节点名称筛选” 字段
- “策略” > “策略分配” 选项卡 > “分配和取消分配策略” - “节点名称筛选” 字段
- “还原” > “节点资源管理器” - “节点名称” 字段
- “节点” > “从自动发现结果添加节点” > “要保护的节点” - “节点名称” 字段

解决方案:

要防止出现这种情况，请打开文本编辑应用程序，如记事本。在文本编辑器中键入特殊字符，如“*”和“_”。然后将字符从文本编辑器复制到字段中。

恢复虚拟机使用不同的传输模式，而不是指定模式

Windows 平台上存在此问题。

症状:

虚拟机的恢复使用不同的传输模式，而不是在注册表项中指定的模式

解决方案：

此行为影响精简磁盘。要更正此问题，请执行这些步骤：

1. 登录到虚拟机的 CA ARCserve D2D 备份代理系统。
2. 打开注册表编辑器，并找到以下注册表项：
HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFRestoreDll
3. 将注册表项 “EnforceTransportForRecovery” 设置为下列传输模式之一：
 - NBD
 - NBDSSL
4. 提交虚拟机的恢复。

将虚拟机恢复到备选 ESX 服务器或 Hyper-V 服务器时，CA ARCserve Central HostBased VM Backup 不识别动态磁盘上的卷

Windows 平台上存在此问题。

症状：

将虚拟机恢复到备选的 ESX 服务器或 Hyper-V 服务器时，应用程序无法识别动态磁盘上的卷。

虚拟机启动时，一些磁盘变成脱机，且相应的卷不可用。

解决方案：

要检索卷，请登录到备用虚拟机，并从 diskmgmt.msc 手动将磁盘设置为联机。

在使用 HotAdd 传输模式为大小超过 2 TB 的磁盘备份数据时发生的还原数据问题

症状:

在我使用 VMware HotAdd 传输模式备份大小超过 2 TB 的 VMDK（虚拟机磁盘）文件时，备份成功，但是还原的数据已损坏。

解决方案:

由于 VMware VDDK（虚拟磁盘开发工具包）的一个已知问题，备份作业成功，但是还原的数据已损坏。要解决该问题，您可以执行以下步骤之一：

- 重新配置您的备份计划，以允许在不同的备份代理上运行备份作业，以便它不会使用 HotAdd 传输模式运行。
- 设置注册表设置，以强制在备份期间使用的传输模式不是 HotAdd。您可以使用 SAN 或 NBD/NBDSSL。

有关此 VMware 问题的详细信息，请参阅 VMware 文档

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2068424。

第 6 章：应用最佳实践

此部分包含以下主题：

[执行虚拟机的裸机恢复](#) (p. 143)

[定义并行备份的数量限制](#) (p. 169)

[增加 VMVixMgr 日志文件中保留的消息数量](#) (p. 170)

[保护 CA ARCserve D2D 备份代理](#) (p. 171)

[安装过程如何影响操作系统](#) (p. 171)

[从防病毒扫描排除文件](#) (p. 176)

执行虚拟机的裸机恢复

当执行备份作业的同时虚拟机开机时，会支持裸机恢复。

裸机恢复 (BMR) 是一种从“裸机”还原计算机系统的过程，包括重新安装操作系统和软件应用程序，然后还原数据和设置。通过 BMR 过程，您可以通过最少的付出还原完整的计算机，甚至可以还原到不同的硬件。BMR 可以实现，是因为在块级备份过程期间，CA ARCserve D2D 不仅捕获数据，而且捕获与以下项相关的所有信息：

- 操作系统
- 已安装的应用程序
- 配置设置
- 必要的驱动程序

从“裸机”执行计算机系统完全重建所需的所有相关信息都将备份到一系列块中，并存储在备份位置。



视频

CA Support: [如何执行裸机恢复](#)

YouTube: [如何执行裸机恢复](#)

可以执行 BMR 之前，您必须有

- 以下项目之一：
 - 刻录到 CD/DVD 上的已创建 BMR ISO 映像
 - 刻录到便携式优盘上的已创建 BMR ISO 映像

注意：CA ARCserve D2D 利用启动工具包实用工具将 WinPE 映像和 CA ARCserve D2D 映像组合在一起，以创建 BMR ISO 映像。然后将此 ISO 映像刻录到可启动介质上。随后就可以使用任何一个可启动介质（CD/DVD 或优盘）来初始化新的计算机系统，以及开始裸机恢复过程。为了确保您保存的映像始终为最新版本，最好每次更新 CA ARCserve D2D 时创建新的 ISO 映像。

- 至少一个完全备份可用。
- 至少 1 GB RAM 安装在该虚拟机以及要恢复的源服务器上。
- 要将 VMware 虚拟机恢复到被配置为作为物理服务器运行的 VMware 虚拟机，请确保 VMware Tools 安装在目标虚拟机上。

动态磁盘仅在磁盘级别还原。如果您的数据已备份到动态磁盘的本地卷上，则在 BMR 期间将无法还原该动态磁盘。在此方案中，要在 BMR 期间还原，您必须执行以下任务之一，然后在复制的恢复点执行 BMR：

- 备份到其他驱动器上的卷。
- 备份到远程共享。
- 将恢复点复制到其他位置。

注意：如果使用多个动态磁盘执行 BMR，BMR 可能会由于某些异常错误（例如无法启动、无法识别的动态卷等）而失败。如果发生此问题，您难以仅使用 BMR 还原系统磁盘，然后在计算机重新启动后，可以在正常环境中还原其他动态卷。

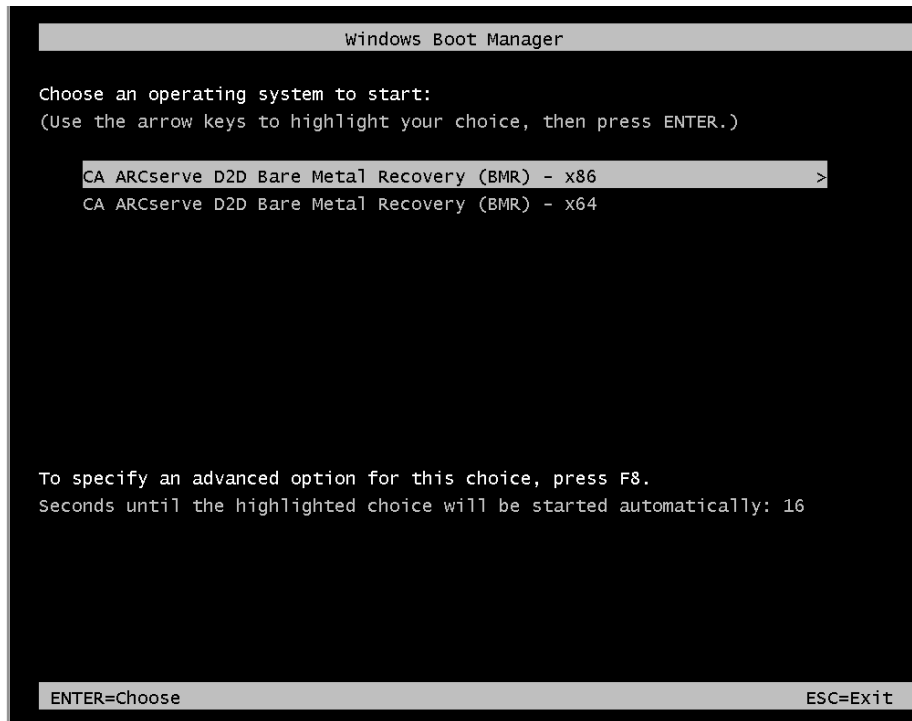
无论使用哪种方法创建启动工具包映像，BMR 过程基本上是相同的。

注意：BMR 过程无法创建存储空间。如果源计算机具有存储空间，执行 BMR 期间将无法在目标计算机上创建存储空间。可以在执行 BMR 之前将那些卷还原为常规磁盘/卷或手动创建存储空间，然后将数据还原到所创建的存储空间中。

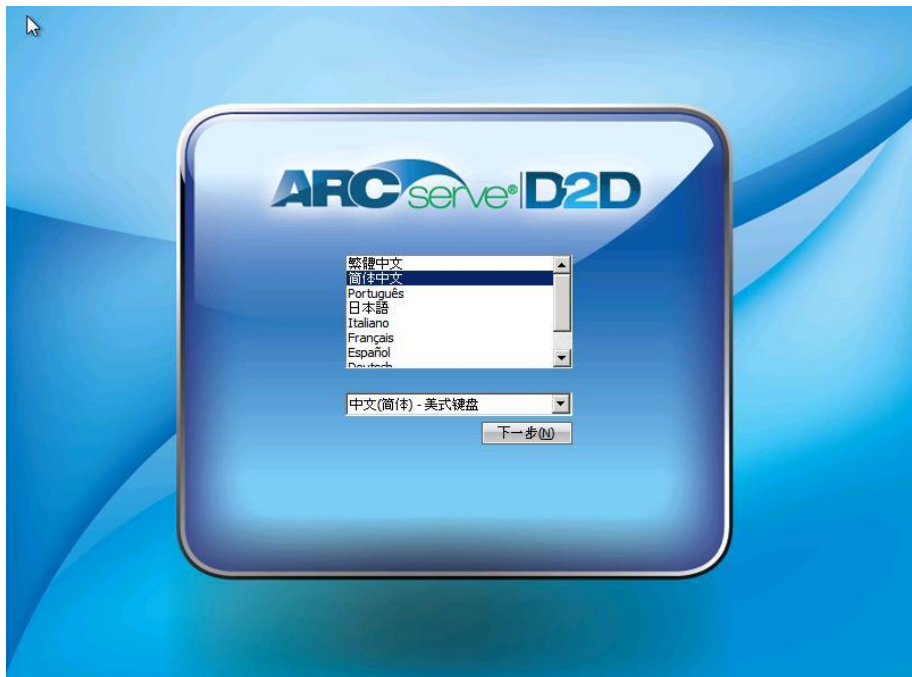
使用裸机恢复还原数据：

1. 插入保存的启动工具包映像介质，然后启动计算机。
 - 如果要使用刻录到 CD/DVD 上的 BMR ISO 映像，请插入保存的 CD/DVD。
 - 如果要使用刻录到优盘上的 BMR ISO 映像，请插入保存的优盘。
- “BIOS 设置实用工具” 屏幕显示。

- 从“BIOS 设置实用工具”屏幕，选择“CD-ROM 驱动器”选项或“USB”选项，以开始启动过程。选择体系结构 (x86/x64) 并按 Enter 键继续。



- CA ARCserve D2D 语言选择屏幕显示。选择语言，然后按“下一步”继续。



裸机恢复过程即被启动，初始 BMR 向导屏幕显示。



4. 从 BMR 向导屏幕，选择您想执行的 BMR 类型：

■ **恢复使用 CA ARCserve D2D 备份的数据**

允许您恢复使用 CA ARCserve D2D 备份的数据。该选项将与使用 CA ARCserve D2D 或 CA ARCserve Central HostBased VM Backup 应用程序执行的备份会话结合使用。

如果您选择该选项，自此继续该过程。

■ **使用 Hyper-V 虚拟备用 VM 恢复**

让您为虚拟转换到 Hyper-V 虚拟机的计算机恢复数据。该选项将与 CA ARCserve Central Virtual Standby 应用程序结合使用。

注意：对于该选项，只有使用 CA ARCserve Central Virtual Standby 执行到 VHD 文件的虚拟转换（对于 Hyper-V）时您才能恢复数据。

如果您选择该选项，请参阅使用 Hyper-V 虚拟备用 VM 恢复以继续该过程。

■ **使用 VMware 虚拟备用 VM 恢复**

让您为虚拟转换到 VMware 虚拟机的计算机恢复数据。该选项将与 CA ARCserve Central Virtual Standby 应用程序结合使用。

注意：对于该选项，只有使用 CA ARCserve Central Virtual Standby 执行到 VMDK 文件的虚拟转换（对于 VMware）时您才能恢复数据。

如果您选择该选项，请参阅使用 VMware 虚拟备用 VM 恢复以继续该过程。

5. 单击“下一步”。

“选择恢复点”向导屏幕显示。



6. 从“选择恢复点”向导屏幕，选择包含备份映像的恢复点的计算机（或卷）。

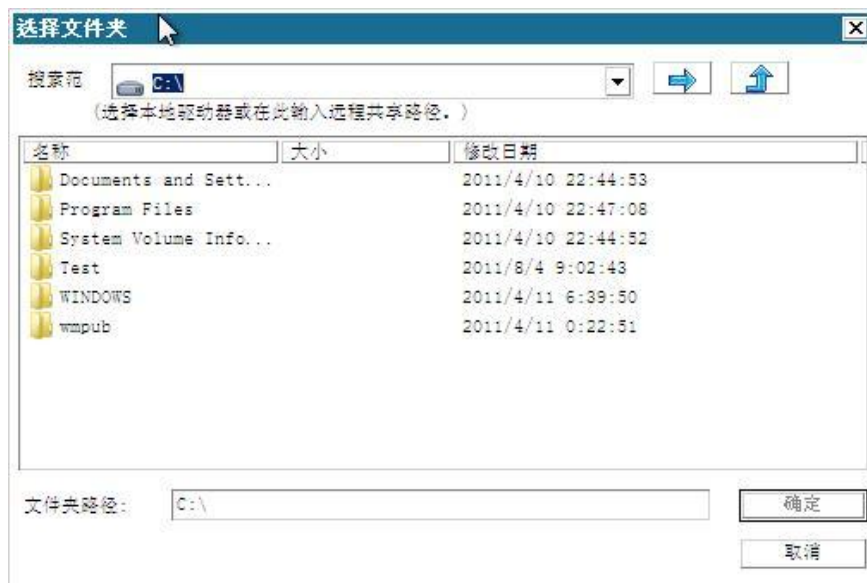
CA ARCserve D2D 允许您从任何本地驱动器或网络共享恢复。

- 如果从本地备份恢复，BMR 向导会自动检测和显示包含恢复点的所有卷。
- 如果从远程共享恢复，请浏览至存储恢复点的远程位置。如果包含恢复点的计算机有多个，则会显示所有计算机。

您还可以需要远程计算机的访问权限信息（用户名和密码）。

注意：网络必须启动并运行，才能浏览远程恢复点。必要时，您可以检查/刷新您的网络配置信息，或从“实用程序”菜单加载任何缺失的驱动程序。

7. 如果 BMR 模块无法检测到任何本地目标卷，则会自动显示“选择文件夹”对话框。提供备份所在的远程共享。



- 选择存储备份的恢复点的文件夹，然后单击“确定”。（您可以单击箭头图标以验证到所选位置的连接）。

现在，BMR 向导屏幕显示以下信息：

- 计算机名（在左上角窗格中）。
- 相关备份信息（在右上角窗格中）。
- 所有的相应恢复点（在左下角窗格中）。

注意：对于支持的操作系统，您可以基于从 UEFI 计算机到与 BIOS 兼容的计算机以及从 BIOS 计算机到与 UEFI 兼容的计算机上进行的备份执行 BMR。有关固件转换支持系统的完整列表，请参阅“支持 UEFI/BIOS 转换的操作系统”。

- 对于不支持固件转换的操作系统，要对 UEFI 系统执行 BMR，必须以 UEFI 模式启动计算机。BMR 不支持使用不同固件还原计算机。要确认启动固件是 UEFI 而不是 BIOS，请依次单击“实用程序”、“关于”。
- 对于支持固件转换的操作系统，选择恢复点之后，如果检测到源计算机与您的系统固件不同，将会询问您是否要将 UEFI 转换成与 BIOS 兼容的系统或将 BIOS 转换成与 UEFI 兼容的系统。



9. 选择要还原的恢复点。

选定恢复点的相关信息显示（在右下窗格中）。该显示内容包括诸如已执行（保存）备份的类型、备份目标以及备份的卷等信息。

如果恢复点包含加密的会话（恢复点钟图标带锁），则会显示需要密码屏幕。输入会话密码，然后单击“确定”。

输入加密密码

当前密码长度: 0 个字符
最大密码长度: 23 个字符

注意：如果您的计算机是域控制器，CA ARCserve D2D 在 BMR 期间将支持 Active Directory (AD) 数据库文件的非授权还原。（CA ARCserve D2D 不支持还原 MSCS 群集）。

10. 确认这是要还原的恢复点，然后单击“下一步”。

BMR 向导屏幕显示，并提供可用的恢复模式选项。

ARCserve D2D™ Bare Metal Recovery

CA ARCserve D2D 裸机恢复 (BMR)
- 选择恢复模式

您要使用哪个恢复模式？

快速模式(F)
快速模式将自动使用计算机默认设置恢复该系统，用户参与最少。

高级模式(D)
高级模式将帮助您自定义还原过程。使用该模式您将能够：
在基本卷或动态卷上选择还原数据的位置。
在重新启动之前插入设备驱动程序。

注意：在单击“下一步”之后，BMR 向导将在目标计算机中创建新的分区，以便匹配源计算机中的现有分区。这可能会破坏目标计算机中的所有现有分区并创建新的分区。

11. 选择恢复模式。

可用选项是“高级模式”和“快速模式”。

- 如果您想自定义恢复过程，请选择“高级模式”。
- 如果在恢复过程中要最少的交互，请选择“快速模式”。

默认：快速模式。

注意：只有当您选择“高级模式”时，该过程的剩余部分才适用，并提供指导您完成 BMR 过程的信息。

12. 单击“下一步”。

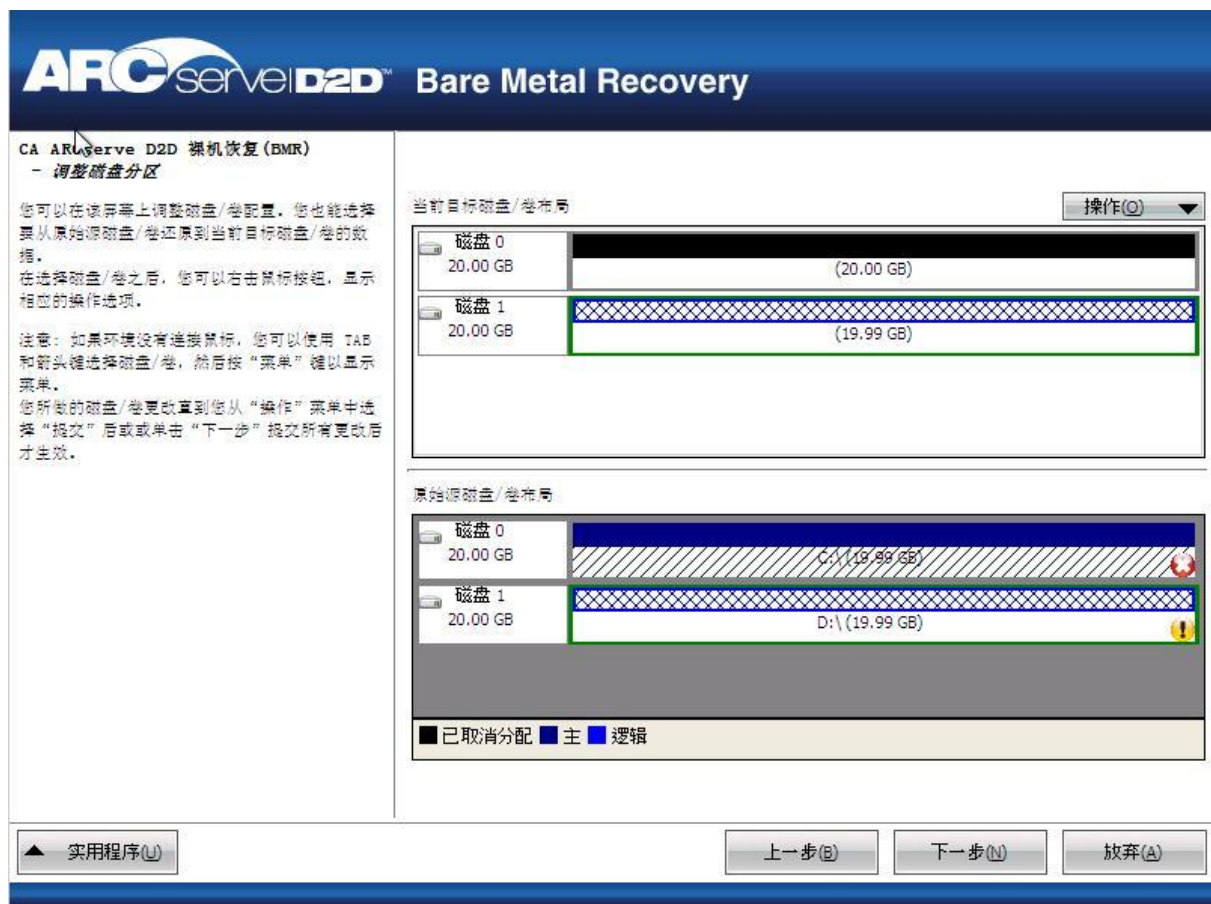
BMR 实用工具开始查找要恢复的计算机，并显示相应的磁盘分区信息。

上窗格显示当前（目标）计算机上的磁盘配置，下窗格显示原始（源）计算机上的磁盘分区信息。

重要说明！源卷显示的红色 X 图标表示，此卷包含系统信息且没被分配（映射）到目标卷。来自源磁盘的该系统信息卷在 BMR 期间必须被分配给目标磁盘且被还原，否则重新启动将失败。

注意：如果您执行 BMR 并且将系统卷还原到没有配置为启动盘的磁盘，那么在 BMR 完成后将无法启动计算机。请确保您将系统卷还原到正确配置的启动盘上。

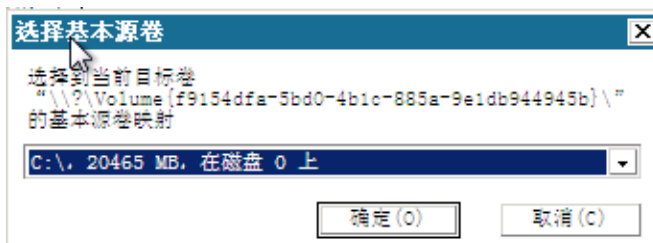
注意：在还原到其他磁盘/卷时，新磁盘/卷的容量必须与原始磁盘/卷相同，或比其大。此外，磁盘调节大小仅适用于基本磁盘，不适用于动态磁盘。



13. 如果您看到的当前驱动器信息显示不正确，您可以访问“实用程序”菜单，检查缺失的驱动程序。
14. 必要时，在目标磁盘/卷窗格上，您可以单击“操作”下拉菜单以显示可用选项。有关这些选项的更多信息，请参阅“管理 BMR 操作菜单”。

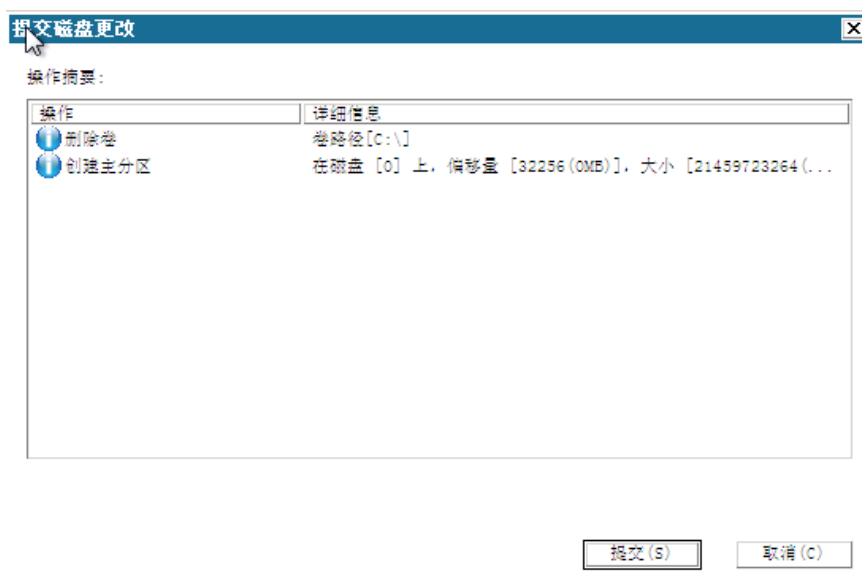
15. 单击每个目标卷，然后从弹出菜单，选择“映射卷源”选项以将源卷分配给该目标卷。

此时打开“选择基本源卷”对话框。



16. 在“选择基本源卷”对话框中单击下拉菜单，并选择要分配给选定目标卷的可用源卷。单击“确定”。
 - 在目标卷上，显示复选标记图标，表示已映射到该目标卷。
 - 在源卷上，红色 X 图标变成绿色图标，表示该源卷已经被分配给目标卷。
17. 当您确信想要还原的所有卷和包含系统信息的所有卷被分配给目标卷时，单击“下一步”。

“提交磁盘更改”屏幕打开，显示选定操作的摘要。对于正创建的每个新卷，将显示相应信息。



18. 您确认摘要信息正确后，单击“提交”。（如果信息不正确，单击“取消”）。

注意：对硬盘驱动器的所有操作不会生效，直至将其提交。

在目标计算机上，新的卷被创建并被映射到相应的源计算机。

19. 当更改完成时，单击“确定”。

此时打开“还原设置摘要”屏幕，显示要还原的卷的摘要。

注意：在还原摘要窗口底部，“目标卷”列中列出的驱动器号自动生成于 Windows 预安装环境 (WinPE)。它们可能不同于“源卷”列中所列的驱动器号。然而，即使驱动器号不同，仍会将数据还原到正确的卷上。



20. 您确认摘要信息正确后，单击“确定”。

还原过程将开始。BMR 向导屏幕显示每个卷的还原状态。

- 根据正在还原的卷的大小，该操作可能花费一些时间。
- 在此过程中，将逐块还原为该复制点备份的任何内容，并在目标计算机上创建源计算机的副本。
- 默认情况下，会选择恢复后自动重新启动系统的选项。必要时，您可以清除该选项，在以后手工重新启动。
- 必要时，您可以随时取消或放弃操作。



21. 从“实用程序”菜单，您可以访问 BMR 活动日志，并使用“保存”选项保存活动日志。

默认情况下，活动日志被保存到以下位置：

X:\windows\system32\dr\log。

注意：要避免遇到 Windows 生成的错误，不要使用 BMR “活动日志”窗口的“另存为”选项在桌面上保存活动日志，或在桌面创建新的文件夹。

22. 如果要还原到不同硬件（用来连接硬盘驱动器的 SCSI/FC 适配器可能已经更改），且在原始系统中未检测到兼容驱动程序，则会显示“驱动程序注入”页面，以让您为这些设备提供驱动程序。

您可以浏览并选择要注入到已恢复系统的驱动程序，这样，即使您恢复到使用不同硬件的计算机，您仍可以在 BMR 之后恢复计算机。

23. 在 BMR 过程完成后，将显示确认通知。

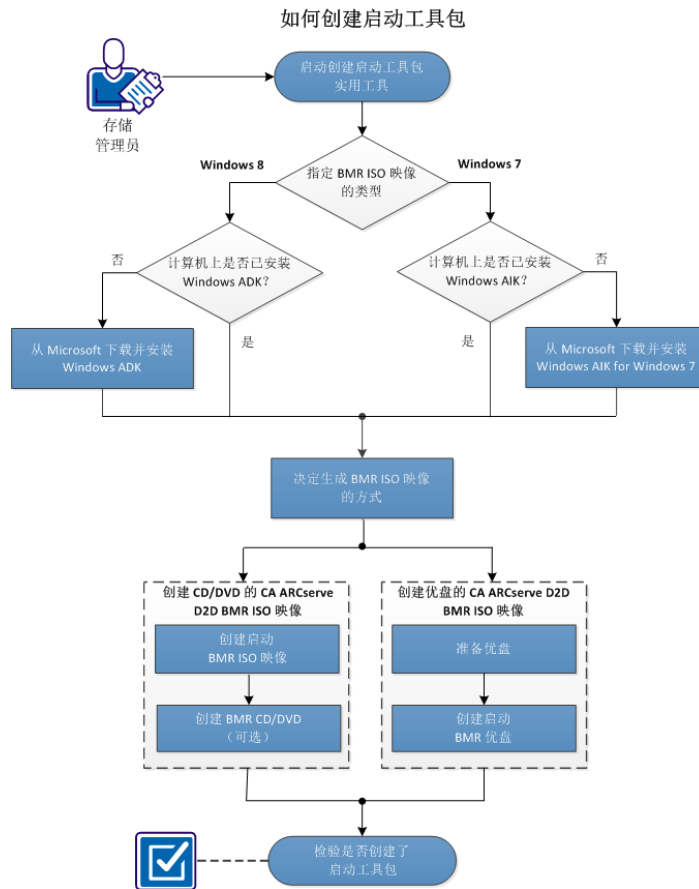
注意：在 BMR 完成后：

- 执行的首次备份是“验证备份”。
- 确认已将 BIOS 配置为从启动卷被还原到的磁盘启动。
- 重新启动计算机后，如果您已还原到不同硬件，则您可能需要手工配置网络适配器。
- 计算机重新启动时，Windows 错误恢复屏幕可能会显示，表明 Windows 未成功关闭。如果发生该问题，您可以安全忽略此警告，并继续正常启动 Windows。
- 对于动态磁盘，如果磁盘的状态为脱机，您可以从磁盘管理 UI（通过运行 Diskmgmt.msc 控制实用程序访问）手工将其更改为联机。
- 对于动态磁盘，如果动态卷处于故障冗余状态，您可以从磁盘管理 UI（通过运行 Diskmgmt.msc 控制实用程序访问）手工重新同步卷。

如何创建启动工具包

CA ARCserve D2D 利用启动工具包实用工具将 WinPE（Windows 预安装环境）映像和 CA ARCserve D2D 映像组合在一起，以创建 BMR ISO 映像。然后将此 ISO 映像刻录到可启动介质上。执行裸机恢复时，使用 CA ARCserve D2D 可启动介质（CD/DVD 或优盘）初始化新的计算机系统，并开始裸机恢复过程。

下图说明了创建启动工具包的过程：



要创建启动工具包，请执行以下任务：

1. [启动“创建启动工具包”实用工具](#) (p. 159)
2. [确定生成 BMR ISO 映像的方式](#) (p. 162)
3. [创建 CD/DVD 的 CA ARCserve D2D BMR ISO 映像](#) (p. 163)
 - a. [创建可启动的 BMR ISO 映像](#) (p. 163)
 - b. (可选) [创建 BMR CD/DVD](#) (p. 164)
4. [创建优盘的 CA ARCserve D2D BMR ISO 映像](#) (p. 165)
 - a. [准备优盘](#) (p. 166)
 - b. [创建可启动的 BMR 优盘](#) (p. 167)
5. [确认已创建启动工具包](#) (p. 169)

附加视频

此程序包含附加的教学视频。选择 CA Support 或 YouTube 作为该视频的查看源。来自 CA Support 和 YouTube 的视频版本是相同的，仅仅查看源不同。



CA Support: [如何创建启动工具包](#)

YouTube: [如何创建启动工具包](#)

启动“创建启动工具包”实用工具

CA ARCserve D2D 提供“创建用于裸机恢复的启动工具包”实用工具，帮助您生成基于 WinPE 的 ISO 映像。该 ISO 映像包含在必要时执行裸机恢复 (BMR) 所需的所有信息。

遵循这些步骤:

1. 您可以从系统托盘监视器的高级选项或“开始”菜单启动“创建启动工具包”实用工具。

启动“创建启动工具包”实用工具,并显示“指定 BMR ISO 映像的类型”屏幕。



2. 指定要创建 (Windows 8 或 Windows 7) 的 BMR ISO 映像类型, 然后单击“下一步”。

注意: 不支持 Windows XP、Windows Vista 和 Windows Server 2003 创建 BMR ISO 映像。对于这些操作系统, 您可以使用 Windows 的 Windows Vista SP1、Windows 2003 SP2 或更高版本来创建 BMR ISO 映像。

■ **Windows 8**

启动后, 该实用工具将立即检查您的计算机, 以确定是否已安装 Windows 评估和部署工具包 (ADK)。Windows ADK 是一种 Microsoft 工具, 可用于将 Windows 操作系统部署到计算机。

注意: 可以在运行以下操作系统的计算机上安装 Windows ADK:

- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012

■ **Windows 7**

启动后, 该实用工具将立即检查您的计算机, 以确定是否已安装 Windows 自动安装工具包 (AIK)。Windows AIK 是一种 Microsoft 工具, 可用于将 Windows 操作系统部署到计算机。

注意：可以在运行以下操作系统的计算机上安装 Windows AIK for Windows 7:

- Windows 2003 SP2
- Windows Vista SP1
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

3. 要创建可启动 ISO 映像，计算机上必须已安装 Windows ADK 或 Windows AIK（可适用）。
 - a. 如果 Windows ADK（或 AIK）已安装，实用工具将前进到“选择启动工具包方法”屏幕，以便可以继续创建启动工具包。
 - b. 如果未安装 Windows ADK（或 AIK），相应的 Windows 信息屏幕将打开。您需要下载并安装 Microsoft 下载中心的 Windows ADK（或 AIK）。

注意：有关安装 Windows ADK（或 AIK）的更多信息，请参阅以下网站：

- [安装 Windows ADK](#)
- [安装 Windows AIK for Windows 7](#)

可以使用下列方法之一安装 Windows ADK（或 AIK）：

- 直接从 Microsoft 网站下载安装介质，然后将 Windows ADK（或 AIK）安装到计算机上。
- 单击信息屏幕上的链接可打开 Microsoft 网站，以便下载 Windows ADK（或 AIK）并将其安装到计算机上。

安装 Windows ADK（或 AIK）后，单击“下一步”，此时实用工具将前进到“选择启动工具包方法”屏幕，以便可以继续创建启动工具包。

注意：对于 Windows ADK 安装，需要以下功能支持创建启动工具包：

- 部署工具
- Windows 预安装环境（Windows PE）

注意：对于 Windows AIK 安装，请选择“Windows AIK 设置”。

确定生成 BMR ISO 映像的方式

“创建启动工具包”实用工具提供两个生成 ISO 映像的选项：



- [创建可启动的 BMR ISO 映像](#) (p. 163)

该方式创建可以刻录到 CD/DVD 上以便存储的 ISO 映像。这是默认选项。有关详细信息，请参阅“[创建 CD/DVD 的 CA ARCserve D2D BMR ISO 映像](#) (p. 163)”。

- [创建可启动的 BMR 优盘](#) (p. 167)

该方式创建 ISO 映像，并将其直接刻录到便携式优盘上以便存储。有关详细信息，请参阅“[创建优盘的 CA ARCserve D2D BMR ISO 映像](#) (p. 165)”。

随后可以使用任何一个可启动介质来初始化新的计算机系统，以及开始裸机恢复过程。为了确保您保存的映像始终为最新版本，最好每次更新 CA ARCserve D2D 时创建新的 ISO 映像。

注意：如果要在虚拟计算机 (VM) 上执行 BMR，那么也可以直接将 ISO 映像连接到 VM，以便在无需首先将其刻录到 CD/DVD 的情况下启动 BMR 过程。

创建 CD/DVD 的 CA ARCserve D2D BMR ISO 映像

创建 CA ARCserve D2D BMR ISO 映像的过程包括：

- [创建可启动的 BMR ISO 映像](#) (p. 163)
- [创建 BMR CD/DVD](#) (p. 164)

创建可启动的 BMR ISO 映像

如果选择创建 BMR ISO 映像，可以将该映像刻录到可启动介质（CD 或 DVD）上，以便初始化新的计算机系统，以及开始裸机恢复过程。

遵循这些步骤：

1. 从“选择启动工具包方法”屏幕中，选择“创建可启动的 BMR ISO 映像”，然后单击“下一步”。

此时将打开“选择平台和目标”对话框。

2. 选择适用于 ISO 映像的平台。

可以选择两个可用选项之一，也可选择两个。如果选择两个平台，将导致创建映像的时间增加。

注意：从 32 位平台创建的 ISO 映像应用于还原 32 位服务器。从 64 位平台创建的 ISO 映像应用于还原 64 位服务器。如果要启动 UEFI 固件系统，请确保选择了 x64 平台选项。

可用的选项包括：

- 适用于 x86 平台的 BMR ISO 映像（仅）。
- 适用于 x64 平台的 BMR ISO 映像（仅）。
- 适用于 x86 和 x64 平台的 BMR ISO 映像。

3. 指定目标。

指定或浏览到将创建和存储 BMR ISO 映像文件的位置。

4. 指定生成的 BMR ISO 映像文件的名称。

5. 指定平台和目标后，单击“下一步”。

此时将打开“选择语言”对话框。

6. 选择适用于生成的 BMR ISO 映像的语言。在执行 BMR 过程中，用户界面和键盘将以选定的语言集成。

可以选择适用于 BMR ISO 映像的一种或多种不同的语言。但是，选定的每种语言都将导致创建映像的时间增加。选择的语言越多，完成该操作所需的时间就越长。因此，应该只选择确实需要的语言。

7. 单击“下一步”。

此时将打开“指定驱动程序”对话框。

8. 指定用要集成到 BMR ISO 映像中的驱动程序填充驱动程序列表的驱动程序。

驱动程序窗格启用后，您可以指定要从 BMR ISO 映像添加或删除的任何其他驱动程序。

注意：将 VirtualBox Host-Only 以太网适配器驱动程序集成到 BMR ISO 映像中时，可能与 Windows ADK 组件有冲突。为了避免任何冲突，最好不要将此驱动程序集成到 BMR ISO 映像中。

- a. 包括本地驱动程序：将本地关键设备驱动程序（仅 NIC、FC 或 SCSI 的 oem 驱动程序）载入到驱动器列表中。单击时，实用工具会检查您的计算机以确定是否有任何关键设备驱动程序需要针对此计算机添加到 BMR ISO 映像。如果发现任何关键设备驱动程序，他们会自动添加到列表。
 - b. 添加驱动程序：浏览要添加到驱动程序列表的驱动程序。
 - c. 删除驱动程序：从不想添加到 BMR ISO 映像的列表中删除所选的任何驱动程序。
9. 单击“创建”以启动过程，并创建可启动 BMR ISO 映像。
在该过程中将显示状态。
 10. 过程完成后将打开确认屏幕，指示已成功生成 BMR ISO 映像。此屏幕也显示映像的位置和平台，以及一个用于浏览到该位置的可点击链接。

创建 BMR CD/DVD

创建 ISO 映像并将其保存到指定目标后，需要将此映像刻录到可启动的 CD 或 DVD 上。随后可以使用该可启动介质来初始化新的计算机系统，以及开始裸机恢复 (BMR) 过程。

为了确保所保存的 ISO 映像始终为最新版本：

- 每次更新 CA ARCserve D2D 时，应创建新的 ISO 映像。
- 如果已将 ISO 映像保存到远程位置，则只有在需要执行 BMR 时才需刻录 CD/DVD。
- 如果已将 CA ARCserve D2D 安装到多个计算机上，则在执行 BMR 之前应从已知正常的计算机创建新的 ISO 映像（和相应的 CD/DVD），以便映像包含所有最新的 CA ARCserve D2D 更新。

创建优盘的 CA ARCserve D2D BMR ISO 映像

创建 CA ARCserve D2D BMR 优盘的过程包括：

[准备优盘](#) (p. 166)

[创建可启动的 BMR 优盘](#) (p. 167)

准备优盘

将 BMR ISO 映像刻录到优盘上之前，必须准备好优盘。要创建可启动的 BMR 优盘，必须激活优盘以便能够启动系统。可以使用“DiskPart”命令来激活优盘。

重要说明！ 如果优盘需要格式化，此过程将擦除当前存储在优盘上的所有数据。执行此过程之前，请确认此优盘上没有重要信息。如果之前已将优盘格式化，则此过程将覆盖名称相同的任何文件。

遵循这些步骤:

1. 打开命令提示符（如果您的操作系统要求，则使用管理权限）。
2. 键入 **Diskpart** 并按 Enter 键。
3. 键入 **List Disk** 并按 Enter 键。

此时将显示检测到的所有磁盘的列表。确定所显示的磁盘中哪个是您的 USB 磁盘。

4. 通过键入 **Select Disk <n>**（“n”是 USB 磁盘的磁盘编号）来选择 USB 磁盘，并按下 Enter 键。
5. 键入 **Clean** 并按 Enter 键。

此时系统将显示“DiskPart 成功地清除了磁盘”。

6. 键入 **create partition primary** 并按 Enter 键。

此时系统将显示“成功地创建了指定分区”。

7. 键入 **select partition 1** 并按 Enter 键。

此时系统将显示“分区 1 现在是所选分区”。

8. 键入 **active** 并按 Enter 键。

此时系统将显示“DiskPart 将当前分区标为活动”。

9. 必要时，可以将优盘格式化为 FAT32 或 NTFS 文件系统。

键入 **format fs=fat32 quick** 或 **format fs=ntfs quick**

现在优盘已准备好，可以使用。

```
管理员: 命令提示符 - diskpart
c:\>diskpart

Microsoft DiskPart 版本 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
在计算机上: W2K8R2CUPEF1

DISKPART> list disk

  磁盘 ###  状态      大小   可用   Dyn  Gpt
-----
  磁盘 0    联机      50 GB   0 B   0    *
  磁盘 1    联机     100 GB   0 B   0    *
  磁盘 2    联机     1904 MB   0 B   0    *

DISKPART> select disk 2
磁盘 2 现在是所选磁盘。

DISKPART> clean
DiskPart 成功地清除了磁盘。

DISKPART> create partition primary
DiskPart 成功地创建了指定分区。

DISKPART> select partition 1
分区 1 现在是所选分区。

DISKPART> active
DiskPart 将当前分区标为活动。

DISKPART> format fs=fat32 quick
   100 百分比已完成
DiskPart 成功格式化该卷。

DISKPART> exit_
```

创建可启动的 BMR 优盘

如果选择创建可启动的 BMR（裸机恢复）优盘，可以将该 ISO 映像直接刻录到优盘上，以便初始化新的计算机系统，以及开始裸机恢复过程。

遵循这些步骤:

1. 必要时，请准备优盘。有关详细信息，请参阅[准备优盘](#) (p. 166)。
2. 从“选择启动工具包方法”屏幕中，选择“创建可启动的 BMR 优盘”，然后单击“下一步”。

此时将打开“选择平台和目标”对话框。

3. 选择适用于 ISO 映像的平台。

可以选择两个可用选项之一，也可选择两个。如果选择两个平台，将导致创建映像的时间增加。

注意：从 32 位平台创建的 ISO 映像应用于还原 32 位服务器。从 64 位平台创建的 ISO 映像应用于还原 64 位服务器。如果要启动 UEFI 固件系统，请确保选择了 x64 平台选项。

可用的选项包括：

- 适用于 x86 平台的 BMR ISO 映像（仅）。
- 适用于 x64 平台的 BMR ISO 映像（仅）。
- 适用于 x86 和 x64 平台的 BMR ISO 映像。

4. 指定 USB 驱动器。

指定或浏览到 BMR ISO 映像文件将创建和刻录到优盘的驱动器位置。

注意：对于 USB 驱动器，如果要启动 UEFI 固件系统，应将 USB 驱动器格式化为 FAT32 文件系统。

5. 验证准备好的优盘是否已插入指定的驱动器。

6. 指定平台和位置后，单击“下一步”。

此时将打开“选择语言”对话框。

7. 选择适用于生成的 BMR ISO 映像的语言。在执行 BMR 过程中，用户界面和键盘将以选定的语言集成。

可以选择适用于 BMR ISO 映像的一种或多种不同的语言。但是，选定的每种语言都将导致创建映像的时间增加。选择的语言越多，完成该操作所需的时间就越长。因此，应该只选择确实需要的语言。

8. 单击“下一步”。

此时将打开“指定驱动程序”对话框。

9. 必要时，可选择“集成其他驱动程序”选项。

驱动程序窗格启用后，您可以指定要从 BMR ISO 映像添加或删除的任何其他驱动程序。

10. 单击“创建”以启动过程，并创建可启动 BMR ISO 映像。

在该过程中将显示状态。

11. 过程完成后将打开确认屏幕，指示已成功生成 BMR ISO 映像并将其刻录到优盘上。此屏幕也显示映像的位置和平台，以及一个用于浏览到该位置的可点击链接。

确认已创建启动工具包

成功创建 BMR ISO 映像后，“创建启动工具包”实用工具将显示一个连接到映像保存位置的链接。确认 BMR ISO 映像已保存在该位置。默认情况下，映像将保存到 Libraries/Documents 文件夹，默认映像名称格式包括：

```
<PRODUCT>_BMR_<Platform>_<OS Kernel>_<version>(Build xxx).ISO
```

示例：

```
D2D_BMR_x86x64_w8_r16.5 (Build 1234).ISO
```

定义并行备份的数量限制

您可以定义同时运行的 CA ARCserve D2D 备份作业的数量限制。该功能允许您优化备份环境中的 CA ARCserve D2D 虚拟机代理服务器的性能。默认情况下，Host-Based VM Backup 最多可同时运行 10 个 D2D 备份作业。在包含许多与 CA ARCserve D2D 虚拟机代理系统关联的虚拟机的环境中，如并行运行大量备份，可能会对网络和备份性能造成不利影响。

注意：并行作业的数量超过定义的限制时，超过限制的作业将进入作业队列。

遵循这些步骤：

1. 登录到 CA ARCserve D2D 虚拟机代理系统。
2. 打开 Windows 注册表编辑器，并浏览至以下注册表键：
HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA_ARCSERVE D2D
3. 右键单击 CA ARCserve D2D，选择“新建”，然后单击弹出菜单上的“字符串值”。
命名注册表项，如下所示：
VsphereMaxJobNum
4. 右键单击“VsphereMaxJobNum”并单击弹出式菜单上的“修改”。
“编辑字符串”对话框将打开。

5. 在“值数据”字段中，指定要允许同时运行的 CA ARCserve D2D 备份作业的数量。
 - 下限--1
 - 上限--无。
6. 单击“确定”。限制即被定义。
7. 重新启动 CA ARCserve D2D Web 服务。

增加 VMVixMgr 日志文件中保留的消息数量

VMVixMgr 日志文件中保留与 VMware VIX 操作相关的消息。有关 VMware VIX API 的更多信息，请访问 VMware 网站。

VMVixMgr 日志文件 (VMVixMgr.log) 存储在备份代理系统的以下目录中：

```
C:\Program Files\CA\ARCserve D2D\Logs
```

日志文件默认不能超出 500 KB。当日志文件超出 500 KB 时，日志文件中包含的消息将被覆盖。这种行为可防止日志文件超出 500 KB。

定义了以 15 分钟间隔备份数据的排定后，当日志文件超出 500 KB 时，日志文件极有可能会被覆盖。增加日志文件的大小可在日志文件中保留更多消息。

最佳做法是，仅在定义了以 15 分钟间隔备份数据的计划后再增加日志文件的大小。

遵循这些步骤：

1. 登录到备份代理系统。
 2. 打开 Windows 注册表编辑器，并浏览至以下注册表键：

```
HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D
```
 3. 右键单击“CA ARCserve D2D”，选择“新建”，然后在弹出式菜单上单击“DWORD”。
- 命名 DWORD，如下所述：
- ```
VixMgrLogSize
```
- 注意：**如果该 DWORD 不存在，则日志文件的默认值实际为 500 KB
4. 创建 DWORD 后，右键单击“VixMgrLogSize”，然后在弹出式菜单上单击“修改”以打开“编辑 DWORD”对话框。

5. 在“编辑 DWORD”对话框的“值数据”字段中，指定日志文件的值（以 KB 为单位）。例如 750、1000 等。
6. 单击“确定”应用该值，并关闭“编辑 DWORD”对话框。

## 保护 CA ARCserve D2D 备份代理

使用 CA ARCserve Central HostBased VM Backup 创建的备份会话存储在备份代理上。有几种方法可以保护备份代理，这取决于配置。

- 如果正在运行 CA ARCserve Central Protection Manager，您可以添加备份代理为要保护的节点。有关详细信息，请参阅《CA ARCserve Central Protection Manager 用户指南》。
- 在备份代理上启动本地运行的 CA ARCserve D2D 实例，然后配置备份设置。选择“整个计算机”作为备份源。有关详细信息，请参阅《CA ARCserve D2D 用户指南》。
- 如果正在运行 CA ARCserve Backup，您可以配置备份作业来保护代理。

## 安装过程如何影响操作系统

CA ARCserve Central Applications 安装过程使用名为 Microsoft Installer Package (MSI) 的安装引擎更新各种 Windows 操作系统组件。使用 MSI 中包含的组件，CA ARCserve Central Applications 可执行能让您安装或升级 CA ARCserve Central Applications 的自定义操作。

下表介绍了自定义操作以及受影响的组件：

**注意：**安装 CA ARCserve Central Applications 时，所有 CA ARCserve Central Applications MSI 程序包均将调用本表中列出的组件。

| 组件                 | 说明                                          |
|--------------------|---------------------------------------------|
| CallAllowInstall   | 允许安装过程检查与当前应用程序安装相关的条件。                     |
| CallPreInstall     | 在安装过程中读取和写入 MSI 属性。例如，从 MSI 中读取应用程序安装路径。    |
| CallPostInstall    | 在安装过程中执行与安装相关的各种任务。例如，将应用程序注册到 Windows 注册表。 |
| CallAllowUninstall | 允许卸载过程检查与当前应用程序安装相关的条件。                     |

| 组件                             | 说明                                                                                                                                                                             |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CallPreUninstall               | 在卸载过程中执行与卸载相关的各种任务。例如，从 Windows 注册表取消注册应用程序。                                                                                                                                   |
| CallPostUninstall              | 允许卸载过程在安装的文件卸载后执行各种的任务。例如，删除剩余文件。                                                                                                                                              |
| ShowMsiLog                     | 如果最终用户选择“SetupCompleteSuccess”、“SetupCompleteError”或“SetupInterrupted”对话框中的“显示 Windows Installer 日志”复选框然后单击“完成”，将在记事本中显示 Windows Installer 日志文件。（这仅适用于 Windows Installer 4.0。） |
| ISPrint                        | 打印对话框的 ScrollableText 控件内容。这是 Windows Installer .dll 自定义操作。dll 文件的名称为 SetAllUsers.dll，其入口点为 PrintScrollableText。                                                               |
| CheckForProductUpdates         | 使用“FLEXnet 连接”检查产品更新。此自定义操作启动可执行文件 Agent.exe，并传递以下路径：<br>/au[ProductCode] /EndOfInstall                                                                                        |
| CheckForProductUpdatesOnReboot | 使用“FLEXnet 连接”在重新启动时检查产品更新。此自定义操作启动可执行文件 Agent.exe，并传递以下路径：<br>/au[ProductCode] /EndOfInstall /Reboot                                                                          |

- **更新的目录**--在默认情况下，安装过程在下列目录中安装和更新应用程序文件：

C:\Program Files\CA\<应用程序名称> (例如 ARCserve Central Applications 或 ARCserve D2D)

您可以将应用程序安装到默认安装目录中，或者安装到备用目录中。安装过程将把各种系统文件复制到下列的目录：

C:\WINDOWS\SYSTEM32

- **更新的 Windows 注册表键** -- 安装过程将更新下列 Windows 注册表键：

默认注册表键：

HKLM\SOFTWARE\CA\<应用程序名称> (例如 *ARCserve Central Applications* 或 *ARCserve D2D*)

安装过程将根据系统的当前配置，创建新的注册表键，并修改其他各种注册表键。

- **安装的应用程序** -- 安装过程会将以下应用程序安装到您的计算机中：
  - CA Licensing
  - Microsoft Visual C++ 2010 SP1 Redistributable
  - Java Runtime Environment (JRE) 1.7.0\_06
  - Tomcat 7.0.29

## 包含不正确文件版本信息的二进制文件

CA ARCserve Central Applications 安装第三方、其他 CA 产品和 CA ARCserve Central Applications 开发的二进制文件，但一些二进制文件包含不正确文件版本信息。下表描述了这些二进制文件。

| 二进制文件名称        | 源                        |
|----------------|--------------------------|
| UpdateData.exe | CA 许可                    |
| zlib1.dll      | Zlib Compression Library |

## 不包含嵌入清单的二进制文件

CA ARCserve Central Applications 安装第三方、其他 CA Technologies 产品和 CA ARCserve Central Applications 开发的二进制文件，但一些二进制文件不包含嵌入清单，也不包含文本清单。下表描述了这些二进制文件。

| 二进制文件名称          | 源          |
|------------------|------------|
| BaseLicInst.exe  | CA License |
| UpdateData.exe   | CA License |
| vcredist_x64.exe | Microsoft  |

| 二进制文件名称          | 源         |
|------------------|-----------|
| vcredist_x86.exe | Microsoft |
| tomcat7.exe      | Tomcat    |

## 具有在清单中要求的管理员特权权限级别的二进制文件

CA ARCserve Central Applications 安装第三方、其他 CA Technologies 产品和 CA ARCserve Central Applications 开发的二进制文件，但一些二进制文件具有管理员权限或最高可用权限级别。您必须使用管理帐户或具有最高可用权限的帐户登录，才能运行各种 CA ARCserve Central Applications 服务、组件和应用程序。与这些服务、组件和应用程序对应的二进制文件包含对基本用户帐户不可用的 CA ARCserve Central Applications 特定功能。因此，Windows 将通过指定密码或通过使用具有管理员权限的帐户来提示您确认某项操作，以完成该操作。

- **管理权限** - 管理配置文件或具有管理员权限的帐户对所有 Windows 和系统资源具有读取、写入和执行权限。如果您没有管理权限，系统会提示您输入继续操作所需的管理人员用户的用户名/密码。
- **最高可用权限** - 具有最高可用权限的帐户是一个基本用户帐户和具有运行身份管理权限的超级用户帐户。

下表描述了这些二进制文件。

| 二进制文件名称                                                        | 源                                |
|----------------------------------------------------------------|----------------------------------|
| APMSetupUtility.exe                                            | CA ARCserve Central Applications |
| ArcAppUpdateManager.exe                                        | CA ARCserve Central Applications |
| CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe | CA ARCserve Central Applications |
| CA ARCserve Central ApplicationsPMConfigSettings.exe           | CA ARCserve Central Applications |
| CCIConfigSettings.exe                                          | CA ARCserve Central Applications |
| CfgUpdateUtil.exe                                              | CA ARCserve Central Applications |
| CfgUpdateUtil.exe                                              | CA ARCserve Central Applications |
| D2DAutoUpdateUninstallUtility.exe                              | CA ARCserve Central Applications |
| D2DPMConfigSettings.exe                                        | CA ARCserve Central Applications |
| D2DUpdateManager.exe                                           | CA ARCserve Central Applications |
| DBConfig.exe                                                   | CA ARCserve Central Applications |

---

| 二进制文件名称                      | 源                                |
|------------------------------|----------------------------------|
| FWConfig.exe                 | CA ARCserve Central Applications |
| RemoteDeploy.exe             | CA ARCserve Central Applications |
| RestartHost.exe              | CA ARCserve Central Applications |
| SetupComm.exe                | CA ARCserve Central Applications |
| SetupFW.exe                  | CA ARCserve Central Applications |
| SetupWrapper.exe             | CA ARCserve Central Applications |
| Uninstall.exe                | CA ARCserve Central Applications |
| UpdateInstallCommander.exe   | CA ARCserve Central Applications |
| UpgradeDataSyncupUtility.exe | CA ARCserve Central Applications |
| jbroker.exe                  | Java Runtime Environment         |
| jucheck.exe                  | Java Runtime Environment         |

---

## 从防病毒扫描排除文件

通过临时阻止对文件的访问或隔离或删除错误分类为可疑或危险的文件，防病毒软件可能会干扰该应用程序的平稳运行。您可以配置多数防病毒软件，以便将特定进程、文件或文件夹排除，以便您不会扫描无须保护的数据。应该适当配置您的防病毒软件，以便它不会干扰备份和还原操作，或任何其他进程。

以下进程、文件夹和文件应当被排除在防病毒扫描之外：

- 进程列表
  - C:\Program Files\CA\ARCserve Central Applications\BIN\CCIConfigSettings.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\CfgUpdateUtil.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\DBConfig.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\GetApplicationDetails.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\GetVolumeDetails.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\VixGetApplicationDetails.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\VixGetVolumeDetails.exe
  - C:\Program Files\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Program Files\CA\ARCserve Central Applications\Deployment\Asremsvc.exe
  - C:\Program Files\CA\ARCserve Central Applications\Deployment\CheckProdInfo.exe
  - C:\Program Files\CA\ARCserve Central Applications\Deployment\DeleteMe.exe
  - C:\Program Files\CA\ARCserve Central Applications\Deployment\SetupComm.exe
  - C:\Program Files\CA\ARCserve Central Applications\Deployment\RestartHost.exe
  - C:\Program Files\CA\ARCserve Central Applications\Update Manager\D2DAutoUpdateUninstallUtility.exe



- C:\Program Files\CA\ARCserve Central Applications\Update Manager\D2DPMConfigSettings.exe
- C:\Program Files\CA\ARCserve Central Applications\Update Manager\D2DUpdateManager.exe
- C:\Program Files\CA\ARCserve Central Applications\Update Manager\UpgradeDataSyncupUtility.exe
- C:\Program Files\CA\ARCserve Central Applications\TOMCAT\BIN\tomcat7.exe
- C:\Program Files\CA\ARCserve D2D\TOMCAT\JRE\jre7\bin
  - java.exe
  - java-rmi.exe
  - javaw.exe
  - keytool.exe
  - rmid.exe
  - rmiregistry.exe
- C:\Program Files (x86)\CA\SharedComponents\CA\_LIC
  - CALicnse.exe
  - CAminfo.exe
  - CAregit.exe
  - ErrBox.exe
  - lic98log.exe
  - lic98Service.exe
  - lic98version.exe
  - LicDebug.exe
  - LicRCmd.exe
  - LogWatNT.exe
  - mergecalic.exe
  - mergeolf.exe



# 词汇表

---

## HOTADD 传输模式

Hotadd 传输模式是一种数据传输方法，可让您备份配有 SCSI 磁盘的虚拟机。有关详细信息，请参阅 VMware 网站上的《虚拟磁盘 API 编程指南》。

## NBD 传输模式

网络块设备 (NBD) 传输模式，也称 LAN 传输模式，使用网络文件副本 (NFC) 协议进行通信。当使用 NBD 时，各种 VDDK 和 VCB 操作将单独的连接用于它在每个 ESX/ESXi Server 和 NBD Server 主机上访问的每个虚拟磁盘。

## NBDSSL 传输模式

网络块设备安全套接字层 (NBDSSL) 传输模式使用网络文件复制 (NFC) 协议进行通信。NBDSSL 使用 TCP/IP 通信网络传输加密数据。

## SAN 传输模式

SAN (存储区域网络) 传输模式允许您使用光纤通道通信将备份数据从连接到 SAN 的代理系统传输到存储设备。

## SRM

存储器资源管理 (SRM) 是一种收集信息以便有效管理环境的功能，例如收集应用程序数据、硬件和软件数据或性能关键指标。

## 节点

节点是由一个或多个 CA ARCserve Central Applications 管理的物理或虚拟计算机。

## 节点组

节点组是可以组织由一个或多个 CA ARCserve Central Applications 管理的所有节点的方式，如按用途、按操作系统或按已安装应用程序。

## 同步

同步是一种将不同数据库的数据保持最新以便中央站点数据库与注册分支、节点或站点保持一致的过程。

## 自动发现

自动发现是一种检测到节点并将它们添加到一个或多个 CA ARCserve Central Applications 中以进行集中管理的过程。

## 备份代理

备份代理是运行 CA ARCserve D2D 的主机计算机。代理执行在 CA ARCserve Central HostBased VM Backup 中配置的备份操作。

---

## 恢复点

恢复点是由父加最旧子块组成的备份映像。子备份与父备份合并以创建新的恢复点映像，以便始终维护指定的值。

## 策略

策略是在一个或多个 CA ARCserve Central Applications 中保护节点的一套规范。

## 编录文件

编录文件是 CA ARCserve D2D 数据库中所含备份数据方面的信息目录。有关 CA ARCserve D2D 编录文件的更多信息，请参阅《CA ARCserve D2D 用户指南》。

## 操作前检查

操作前检查 (PFC) 是一个实用工具，通过此工具，可以在节点上运行重要检查来检测可能导致备份作业失败的状况。可以通过单击“节点”屏幕上“PFC 状态”列中的图标来查看节点 PFC 的结果。

