CA ARCserve® Central Virtual Standby

用户指南

16.5 版本

ca technologies

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

自此文档的上一版 CA ARCserve Central Virtual Standby 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。
- 增添了为远程的 Virtual Standby 创建 CA ARCserve 复制和高可用性 方案 (p. 15)。此主题说明在创建远程 Virtual Standby 策略时如何从 CA ARCserve 复制和高可用性 创建 CA ARCserve D2D 和 CA ARCserve Central HostBased VM Backup 方案。
- 增添了从 CA ARCserve Replication 导入节点 (p. 35)。此主题说明可以如何从 CA ARCserve Replication 导入多个节点。
- 增添了配置远程转换器 (p. 35)。此主题说明如何转换 CA ARCserve D2D 恢复点，以便将它们注册到 Microsoft Hyper-V 或 VMware vCenter 或 ESXi。
- 更新了“创建策略”以创建 CA ARCserve Central Virtual Standby 策略 (p. 36)。此主题现在包括可以创建的两种类型策略：本地和远程 Virtual Standby 策略。
- 更新了节点管理任务 (p. 57)。此主题现在包括“从 CA ARCserve Replication 导入节点”选项。
- 增添了为一个或多个 CA ARCserve D2D 节点设置备份密码 (p. 60)。本主题将说明如何设置一个或多个 CA ARCserve D2D 备份密码，并且将它们传输到位于 MSP 站点的转换器。
- 更新了编辑或复制策略 (p. 69)。此主题现在包括两种类型的策略，您可以从中选择进行编辑或复制。
- 更新了查看日志 (p. 76)。此主题现在包括下列模块选项：暂停/恢复监控信号、暂停/恢复 Virtual Standby、更新多个节点、备用 VM 以及从 CA ARCserve Replication 导入节点。
- 添加了打开 Virtual Standby 虚拟机 (p. 99)。本节说明本地 (p. 99)和远程 (p. 105)打开 Virtual Standby 虚拟机的功能。
- 增添了管理 BMR 操作菜单 (p. 132)。本节说明三个类型 BMR 操作。
- 更新了按照 IP/名称添加节点时发生拒绝访问错误 (p. 168)。此主题现在包括禁用用户帐户控制 (UAC) 的两个解决方案。
- 增添了从防病毒扫描排除文件 (p. 190)。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。

目录

第 1 章： CA ARCserve Central Virtual Standby 简介

此部分包含以下主题：

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。

CA ARCserve Central Virtual Standby 是 CA ARCserve Central Applications 提供的应用程序之一。CA ARCserve Central Virtual Standby 与 CA ARCserve D2D 进行集成，允许您从 CA ARCserve D2D 备份会话配给虚拟机。通过该应用程序，您可以：

- 基于排定将存储在 CA ARCserve D2D 目标设备上的 CA ARCserve D2D 恢复点转换成 VMware 虚拟磁盘 (VMDK) 或 Microsoft 虚拟硬盘 (VHD) 格式。在源服务器出现故障时，通过恢复点快照，允许虚拟机充当 CA ARCserve D2D 源服务器。
- 将转换策略推送到 CA ARCserve D2D 源服务器。
- 在基于 VMware ESX Server 或 Windows Hyper-V 的虚拟机上存储恢复点快照。
- 如果出现紧急情况，手动或自动打开虚拟机。
- 将数据从恢复点快照恢复到到原始或备用源服务器（V2P 恢复）。

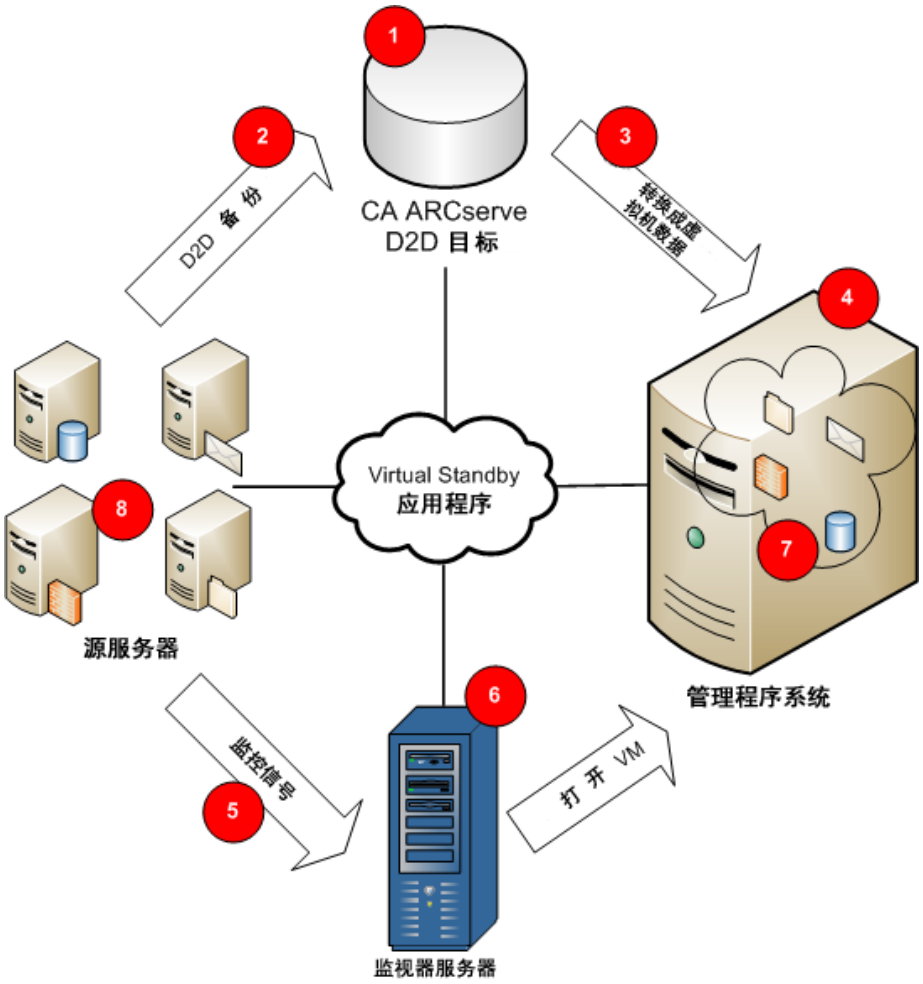
CA ARCserve Central Virtual Standby 的工作原理

Virtual Standby 使您可以通过执行以下操作来保护在环境中工作的 CA ARCserve D2D 源服务器：

- 基于排定将存储在 CA ARCserve D2D 目标设备上的 CA ARCserve D2D 恢复点转换成 VMware 虚拟磁盘 (VMDK) 或 Microsoft 虚拟硬盘 (VHD) 格式。
- 将转换的数据复制到管理程序系统。
- 从虚拟机 VMDK 或 VHD 数据创建恢复点快照。
- 监视源服务器的健康状况。
- 一检测到紧急情况，便从恢复点快照自动打开虚拟机。

  注意：可以将 Virtual Standby 配置为在问题发生时自动或手动打开恢复点快照。
- 纠正源服务器上的问题后，将数据从虚拟机恢复到源服务器。

下图说明此过程：



CA ARCserve D2D (1) 在源服务器的 CA ARCserve D2D 目标设备 (2) 上创建恢复点。Virtual Standby 将恢复点转换成虚拟机格式 (3)，并将数据作为恢复点快照存储在管理程序系统 (4) 上。

监视器服务器 (6) 监视源服务器的健康。如果监视器服务器无法从源服务器 (8) 检测监控信号 (5)，监视器服务器便使用包含在最近恢复点快照内的数据在管理程序系统 (4) 上打开瘦配给的虚拟机 (7)，以充当源服务器。CA ARCserve Central Virtual Standby 创建和源服务器一样大小的虚拟机分区。

在纠正源服务器上的问题后，您可以使用在管理程序系统上存储在 VM 中的数据 (7) 将源服务器 (8) 恢复到当前状态。

注意：如果虚拟机开机后您想备份它，您可以使用 CA ARCserve Central Protection Manager 将 CA ARCserve D2D 备份策略部署到该虚拟机。

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 CA ARCserve Central Virtual Standby

此部分包含以下主题：

先决条件安装任务

安装 CA ARCserve Central Virtual Standby 之前，请完成以下先决任务：

- 确保支持的最新版 CA ARCserve D2D 安装于：
  - 想要保护的源服务器
  - 指定用于存储恢复点快照的服务器

    注意：此要求仅适用于配置为监视节点（物理机或虚拟机）运行状况以及存储节点的恢复点快照的 Hyper-V 服务器。
  - 指定用于监视源服务器的服务器

  注意：如果已将 CA ARCserve Central Protection Manager 安装在生产环境中，可以使用 D2D 部署将 CA ARCserve D2D 安装在远程节点上。有关详细信息，请参阅《CA ARCserve Central Protection Manager 用户指南》。
- 在 Hyper-V 环境中，请确保 CA ARCserve D2D 安装在 Hyper-V 主机系统上。在 Hyper-V 环境中，Hyper-V 主机系统充当恢复点快照的存储位置和监视器服务器。
- 在 VMware 环境中，请确保 CA ARCserve D2D 安装在代理系统上。

  注意：在 VMware 环境中，目标 ESX 服务器数据存储充当恢复点快照的存储位置。代理系统可以有选择性地充当监视器服务器。
- 阅读版本说明文件。版本说明文件包含系统要求的说明、支持的操作系统和本版本中存在的已知问题列表。
- 确保您的系统满足安装 CA ARCserve Central Virtual Standby 所需的最低软硬件要求。

- 请确保您在计划安装 CA ARCserve Central Virtual Standby 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。
- 请确保您的帐号具有 VMware vCenter 或 ESX Server 管理权限和 Windows 管理权限。该帐号需要在 vCenter 服务器系统或 ESX 服务器系统上有 Global License 角色，以允许 VDDK 操作成功完成。
- 请确保您拥有要安装 CA ARCserve Central Virtual Standby 的计算机的用户名和密码。
- 请确保您拥有要监控源计算机的计算机的主机名和 IP 地址。
- 请确保您拥有要存储恢复点快照的计算机的主机名或 IP 地址。
- 请确保安装 CA ARCserve Central Virtual Standby 所需的所有许可都提供给您。
- 请确保 CA ARCserve D2D 版本号与 CA ARCserve Central Virtual Standby 版本号相同。
- 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。

远程 Virtual Standby 先决条件安装任务

远程 Virtual Standby 使您可以从复制的 CA ARCserve D2D 和 CA ARCserve Central HostBased VM Backup 会话创建 Virtual Standby 虚拟机。

使用 Virtual Standby 从复制的 CA ARCserve D2D 和 CA ARCserve Central HostBased VM Backup 会话创建 Virtual Standby 虚拟机之前，请依照以下顺序完成先决条件任务：

1. 安装 CA ARCserve 复制和高可用性。有关详细信息，请参阅《CA ARCserve 复制和高可用性 用户指南》。

   重要说明！执行远程 Virtual Standby 时，要运行 CA ARCserve 复制和高可用性，需要许可。

2. 配置 CA ARCserve D2D、CA ARCserve Central HostBased VM Backup 或二者以创建恢复点。有关详细信息，请参阅《CA ARCserve D2D 用户指南》或《CA ARCserve Central HostBased VM Backup 用户指南》。
3. 创建将恢复点复制到远程位置的复制方案。有关详细信息，请参阅为远程的 Virtual Standby 创建 CA ARCserve 复制和高可用性 方案 (p. 15)。

增添了为远程的 Virtual Standby 创建 CA ARCserve 复制和高可用性 方案

Virtual Standby 允许您创建用于将恢复点复制到远程位置的 CA ARCserve 复制和高可用性 方案。

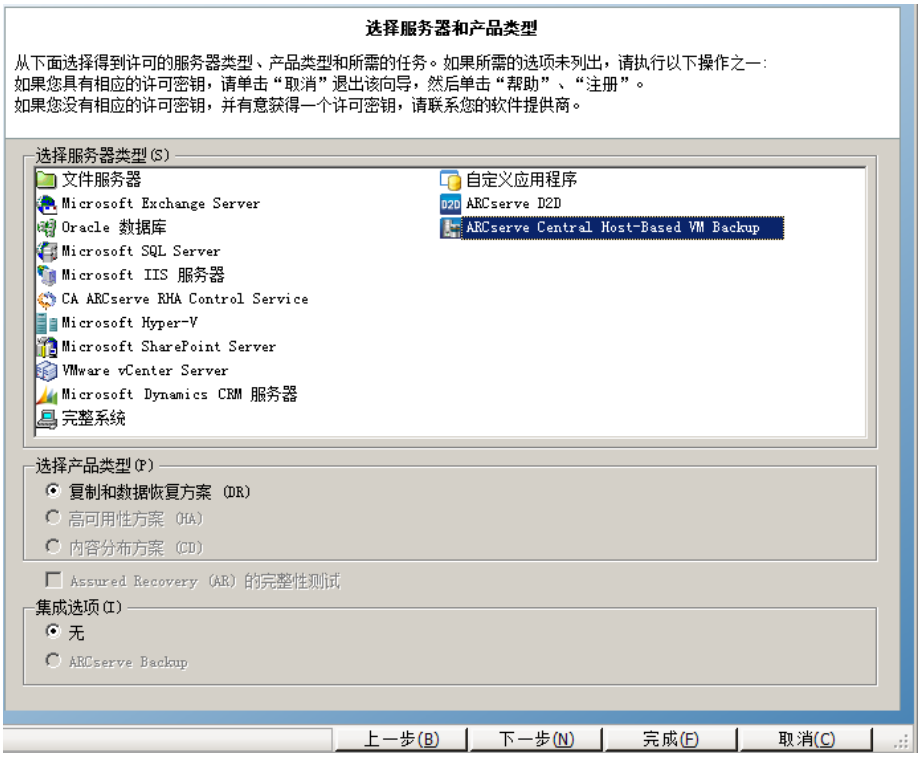
遵循这些步骤:

1. 打开 CA ARCserve 复制和高可用性 管理器。在“方案”菜单中单击“新建”或单击标准工具栏上的“新建”按钮。

   此时显示方案创建向导的欢迎屏幕。

2. 选择“创建新方案”。

   “选择服务器和产品类型”对话框将打开。



3. 选择以下选项，然后单击“下一步”。

   a. 服务器类型：ARCserve Central Host-Based VM Backup。

      注意：以下过程也适用于 ARCserve D2D。

   b. 产品类型：复制和数据恢复方案 (DR)。

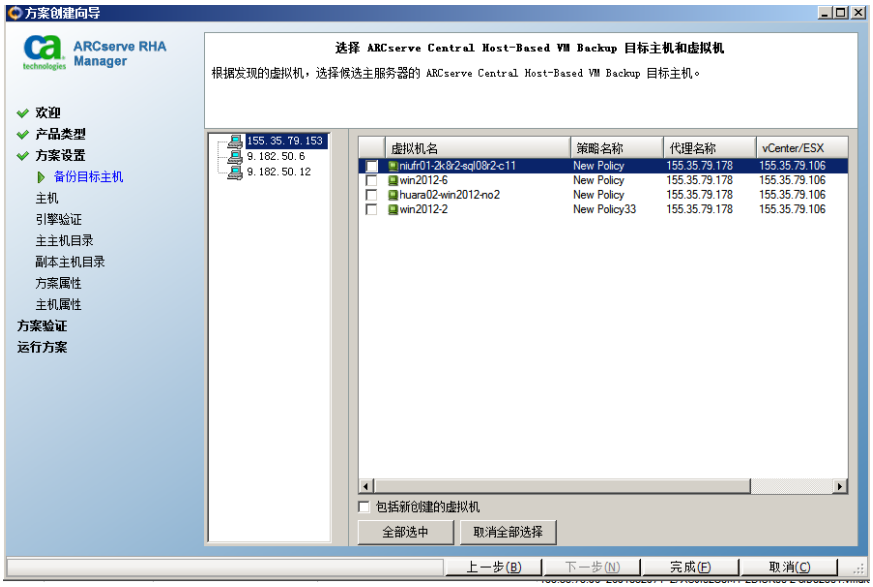
   c. 集成选项：无。

“ARCserve Central Host-Based VM Backup 服务器凭据”对话框打开。

4. 输入 Central Host-Based VM Backup 服务器凭据，然后单击“确定”。服务器名称基于您在第 3 步中的指定内容进行填充。

   ARCserve Central Host-Based VM Backup 目标主机和虚拟机选择项屏幕打开。

   注意：此屏幕不适用于 CA ARCserve D2D 方案并，仅为 CA ARCserve Central HostBased VM Backup 方案独有。



   CA ARCserve 复制和高可用性 连接到 CA ARCserve Central HostBased VM Backup 服务器，以获取策略并显示备份目标主机和其虚拟机。

5. 选择主机名，并且选择想要保护的虚拟机。

   包括新创建的虚拟机：指定运行此方案时将复制主要主机备份文件夹中的所有子文件夹。还复制任何新创建的 VM 备份文件夹。仅排除为选中的 VM 的文件夹。这些文件夹被标记为已排除文件夹。如果您不选择此选项，将仅复制选定的备份文件夹。

   在您运行此方案时，选定虚拟机的备份文件将得到复制。这些是 CA ARCserve D2D 创建的备份文件。

6. 输入以下主服务器和副本服务器详细信息：

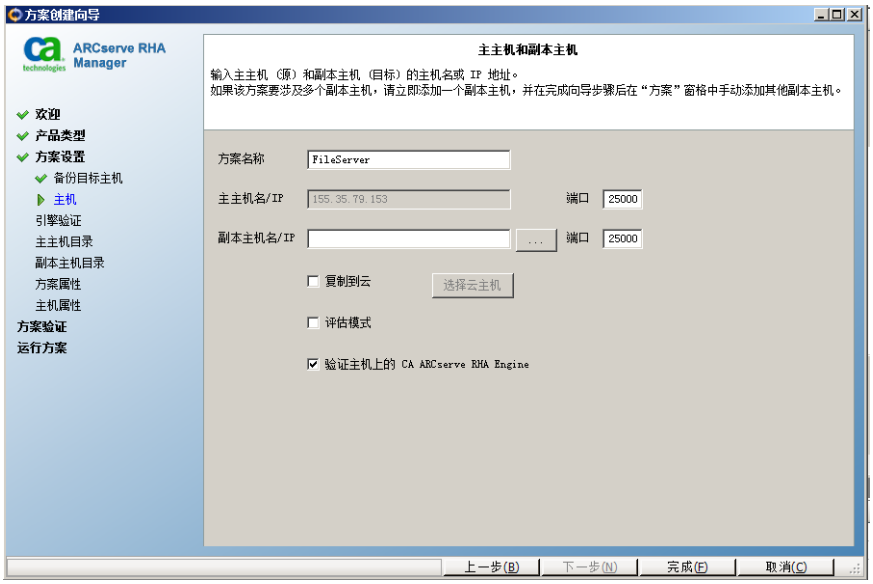
   方案名称：接受默认名称或输入唯一的名称。

   主主机名/IP：自动填充建立您的主机名选择项。

   副本主机名/IP：输入副本服务器的主机名或 IP 地址。该服务器为目标服务器。使用“浏览”按钮来搜索副本服务器。

   端口：接受默认的端口号 (25000) 或输入主服务器和副本服务器的新端口号。

   （可选）验证主机上的 CA ARCserve RHA Engine：启用该选项可验证 Engine 是否已安装且运行在指定主主机和副本主机上。



7. 单击“下一步”。

   “引擎验证”对话框将打开。

   如果您启用选项“验证主机上的 CA ARCserve RHA Engine”，则会打开“主机验证”屏幕。该软件会验证在前一屏幕上指定的主主机和副本主机是否存在并连接。

8. 单击“下一步”。

   此时将打开“主主机根目录”屏幕。

   RHA Engine 发现选定虚拟机的备份文件夹。这些备份文件夹自动被选择。

   注意：这些文件夹是 CA ARCserve D2D 创建的备份文件夹。

在您选择“选择 ARCserve Central Host-Based VM Backup 目标主机和虚拟机”屏幕中的“包括新创建的虚拟机”时，将选择复制主要的备份文件夹，而排除的文件夹将列在筛选窗格中。

9. 单击“下一步”。

   “副本主机根目录”对话框将打开。

10. 接受默认值，然后单击“下一步”。

    “方案属性”屏幕将打开。

11. 配置影响整个方案的属性。对于该示例，只是接受默认配置即可。也可以不在向导中配置这些属性。有关配置方案属性的详细信息，请参阅配置方案属性。

12. 单击“下一步”。

    此时将显示“主主机和副本主机属性”屏幕。

13. 配置与主主机或副本主机有关的属性。对于该示例，只是接受默认配置即可。有关如何配置主主机和副本主机属性的详细信息，请参阅配置主服务器或副本服务器属性。

    注意：选择不同的驱动器用于后台处理主服务器属性，这样默认的后台处理位置 (C:) 便不会塞满您的本地驱动器。（推荐）

14. 单击“下一步”。

    “方案验证”屏幕将打开。

    该软件验证新方案并验证参数以确保复制成功。验证完成后，屏幕会打开，显示所有问题和警告。即使警告显示，软件仍允许您继续。必要时，解决任何警告。

15. 解决完所有错误和警告后，单击“下一步”。

    此时将打开“方案运行”屏幕。

16. 选择“完成”

CA ARCserve 复制和高可用性 方案成功创建。现在，您可以运行此方案，并备份 CA ARCserve D2D 创建的虚拟机文件。

重要说明！建议您打开事件控制台以确认初始数据同步完成，否则备份作业失败。

安装注意事项

在安装 CA ARCserve Central Virtual Standby 之前，请查看以下安装注意事项：

- 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。

- 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 Virtual Standby 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
    ```

- CA ARCserve Central Virtual Standby 不支持在压缩卷和由文件系统加密的卷上创建虚拟磁盘映像。

  注意：该限制仅适用于 Hyper-V 管理程序。

- CA ARCserve Central Virtual Standby 不支持保护使用 JIS2004 Unicode 字符命名的 VMware 虚拟机。

- CA ARCserve Central Virtual Standby 不支持保护磁盘大小超过 2 TB 的虚拟机。

安装 CA ARCserve Central Virtual Standby

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 Virtual Standby

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”。

安装过程被执行。

在安装过程完成之后，“安装报告”对话框打开。

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。

卸载 CA ARCserve Central Virtual Standby

您可以使用位于 Windows “控制面板”的“程序和功能”卸载应用程序。

遵循这些步骤:

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。

以无人值守方式安装 CA ARCserve Central Virtual Standby

CA ARCserve Central Applications 允许您以无人值守安装 CA ARCserve Central Virtual Standby。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 Virtual Standby

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 自解压安装软件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。

以无人值守方式卸载 CA ARCserve Central Virtual Standby

CA ARCserve Central Applications 允许您以无人值守卸载 CA ARCserve Central Virtual Standby。无人值守安装无需用户交互。下列步骤说明如何使用 Windows 命令行卸载应用程序。

遵循这些步骤:

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：以下语法让您可以以无人值守方式卸载 CA ARCserve Central Virtual Standby。

   ```
   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED4835-964B-484B-A395-E2DF12E6F73D}
   ```

   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。

第 3 章： 配置 Virtual Standby 策略

此部分包含以下主题：

发现节点

CA ARCserve Central Virtual Standby 允许您使用若干方法发现或添加节点：

本地策略：

- 按 IP 地址或节点名称添加节点 (p. 29)
- 从文件导入节点 (p. 30)
- 从 CA ARCserve Central HostBased VM Backup 服务器添加节点 (p. 32)

远程策略：

- 从 CA ARCserve 复制和高可用性 导入节点 (p. 35)

按 IP 地址或节点名称添加节点

Virtual Standby 使您可以基于 IP 地址或节点名称添加节点。添加想要保护的 CA ARCserve D2D 源节点。

注意：此选项仅适用于本地虚拟备用策略。

按 IP 地址或节点名称添加节点

1. 从主页上选择导航栏上的“节点”。

   “节点”屏幕将显示。

2. 从“节点”工具栏，单击“添加”，然后在弹出式菜单上单击“按照 IP/名称添加节点”。

   “按照 IP/名称添加节点”对话框打开。

3. 完成“按照 IP/名称添加节点”对话框上的以下字段：
   - **IP/节点名称** -- 允许您指定节点的 IP 地址或名称。
   - **说明** -- 允许您指定节点的描述。
   - **用户名**--允许您指定登录节点时所需的用户名。
   - **密码** -- 指定登录节点所需的密码。

   单击“确定”。
4. （可选）如果新添加的节点未显示在节点列表中，请单击“节点”工具栏上的“刷新”。

“按照 IP/名称添加节点”对话框将关闭，节点即被添加。

从文件导入节点

CA ARCserve Central Virtual Standby 使您可以从文件导入多个节点。您可以从逗点分隔值文本文件 (.txt) 或电子表格 (.CSV) 导入节点。

该应用程序使您可以从文件导入多达 100 个节点。如果文件包含的节点超过 100 个，该应用程序仅导入前 100 个节点。如果您需要添加 100 个以上节点，使用文件导入 100 个， 然后手动添加剩余的节点。

注意：此选项仅适用于本地虚拟备用策略。有关如何手动添加节点的信息，请参阅“按 IP 地址或节点名称添加节点 (p. 29)”。

从文件导入节点

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“节点”工具栏，单击“添加”，然后从弹出式菜单上单击“从文件导入节点”。

   “选择节点”对话框将打开。
3. 单击“浏览”以指定包含要导入的节点的文件。

   注意：您可以指定逗号分隔值 (CSV) 文件或包含逗点分隔值的文本文件。

   单击“上传”。

   节点名称和相应的用户名显示在对话框上。

4. 单击“下一步”。

   “节点凭据”对话框将打开。

   如果提供的用户名和密码正确，绿色的对勾将显示在“已校验”字段中。如果提供的用户名和密码不正确，红色感叹号显示在“已校验”字段中。

5. 执行以下操作之一：

   - 要添加节点，请确认所有用户名和密码正确。要更改特定节点的凭据，请单击“节点名称”字段。

     “验证凭据”对话框打开。

     填写“验证凭据”对话框中的必需字段，然后单击“确定”。

   - 要将一个全局用户名和密码应用于所有节点，完成“用户名”和“密码”字段，然后单击“应用于所选”。

     该全局用户名和密码即应用于所有节点。

   单击“完成”。

节点已被添加。

从 CA ARCserve Central HostBased VM Backup 服务器添加节点

CA ARCserve Central HostBased VM Backup 是一种应用程序，让您可以使用安装在备份代理服务器上的 CA ARCserve D2D 的一个实例来备份虚拟机。通过 CA ARCserve Central Virtual Standby，您可以添加 CA ARCserve Central HostBased VM Backup 服务器正在保护的节点，从而可以为节点创建恢复点快照。这些虚拟机必须已分配有 CA ARCserve D2D 策略，并使用使用 CA ARCserve Central HostBased VM Backup 分配了这些策略。

请注意以下问题：

- 此选项仅适用于本地虚拟备用策略。
- CA ARCserve Central Virtual Standby 允许您通过若干方法添加节点：
  - 手动添加节点
  - 从文本文件导入节点
  - 从 CA ARCserve Central HostBased VM Backup 服务器添加节点

  通过 CA ARCserve Central Virtual Standby，您可以将策略直接应用于节点，但是通过 CA ARCserve Central HostBased VM Backup，您将策略应用于备份代理服务器。在您从 CA ARCserve Central HostBased VM Backup 服务器添加节点之后，该行为会继续进行。

  注意：有关将 CA ARCserve D2D 策略分配给虚拟机节点的信息，请参阅《*CA ARCserve Central HostBased VM Backup 用户指南*》。
- Virtual Standby 无法打开从 CA ARCserve Central HostBased VM Backup 服务器自动添加的节点的恢复点快照。但是，您可以打开从 CA ARCserve Central HostBased VM Backup 服务器手工添加的节点的恢复点快照。

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“节点”类别，单击“添加”，然后在弹出菜单上单击“从 CA ARCserve Central HostBased VM Backup 服务器添加虚拟机”。

   此时打开“从 CA ARCserve Central HostBased VM Backup 服务器添加虚拟机”对话框。

3. 完成“从 CA ARCserve Central HostBased VM Backup 服务器添加 VM”对话框上的以下字段：

   - **计算机名 -** 允许您指定 CA ARCserve Central HostBased VM Backup 服务器的 IP 地址或名称。
   - **用户名 -** 允许您指定登录 CA ARCserve Central HostBased VM Backup 服务器所需的用户名。
   - **密码 -** 指定登录 CA ARCserve Central HostBased VM Backup 服务器所需的密码。
   - **端口 -** 允许您指定应用程序与 CA ARCserve Central HostBased VM Backup 服务器通信时要使用的端口号。
   - **使用 HTTPS --** 允许您指定使用安全 HTTPS 通信。

   单击“确定”。

   将会出现以下事件之一：

   - 如果这是您第一次从该 ESX Server 系统导入节点，Virtual Standby 将导入包含 CA ARCserve Central HostBased VM Backup 策略分配的所有虚拟机。在导入过程完成之后，您可以在“节点”屏幕上验证节点。
   - 如果这不是您第一次从该 ESX Server 系统导入节点，“从 CA ARCserve Central HostBased VM Backup 服务器添加虚拟机”对话框将向您提供先前导入的节点的列表。然后，一个对话框会出现，询问您是否想覆盖先前导入的节点的信息。
   - 如果应用程序没有检测到新节点，“从 CA ARCserve Central HostBased VM Backup 服务器添加虚拟机”对话框则会关闭。然后，一条消息会出现，说明未导入任何节点。

4. 执行下列操作之一：

   - **要添加最新检测到的节点并覆盖先前检测到的节点：**请单击被检测为以前导入的节点旁的复选框，然后单击“确定”。

     应用程序添加了最新检测到的节点并覆盖了先前检测到的节点。应用程序仅覆盖应用于先前检测到的节点的状态和凭据。

   - **要仅添加新检测到的节点（不导入和覆盖先前检测到的节点）：**不要单击被检测为以前导入的节点旁的复选框，然后单击“确定”。

     应用程序仅添加最新检测到的节点。应用程序不会覆盖先前检测到的节点。

   - **要在没有添加最新检测到的节点和先前检测到的节点的情况下退出：**请单击“取消”。

     应用程序不添加任何节点。

5. （可选）单击工具栏上的“刷新”确认是否所有最新添加的节点都显示在节点列表中。

节点已被添加。

注意：在 CA ARCserve D2D 信息在 CA ARCserve Central HostBased VM Backup 服务器上被更新时，服务器自动通知 CA ARCserve Central Virtual Standby 从 CA ARCserve Central HostBased VM Backup 导入虚拟机并重新部署策略。如果 CA ARCserve Central Virtual Standby 不可用，您可以从 CA ARCserve Central HostBased VM Backup 手动导入虚拟机。

从 CA ARCserve Replication 导入节点

CA ARCserve Central Virtual Standby 允许您从 CA ARCserve 复制和高可用性 导入一个或多个节点。您可以通过指定要从中导入节点的复制管理器的信息，来导入节点。

注意：此选项仅适用于远程 Virtual Standby 策略 (p. 42)。在导入节点之前需要为远程的 Virtual Standby 策略创建 CA ARCserve 复制和高可用性方案 (p. 15)。

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“节点”工具栏，单击“添加”，然后从弹出式菜单上单击“从 CA ARCserve Replication 导入节点”。

   “从 CA ARCserve Replication 导入节点”对话框打开。

3. 指定包含想要导入的节点的 Replication 管理器的主机名、端口、协议、用户名以及密码。

   单击“连接”。

   节点名称、方案名称、转换器、备份位置以及配置状态显示在对话框上。

4. 单击“导入”。

节点成功导入并显示在“节点”屏幕上。

配置远程转换器

CA ARCserve Central Virtual Standby 允许您转换 CA ARCserve 复制和高可用性 保护的 CA ARCserve D2D 恢复点，这会自动将这些恢复点注册到 Microsoft Hyper-V、VMware vCenter 或 ESXi。

节点从 CA ARCserve 复制和高可用性 导入到 CA ARCserve Central Applications 时，便可以转换节点。CA ARCserve 复制和高可用性 副本主机文件夹是转换节点的地方。

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，或单击包含要转换的节点的组名称。

   与该组关联的节点显示在节点列表中。

3. 从“转换器”列单击要配置的转换器。

   “配置远程转换器”对话框打开。

4. 指定选定转换器的端口、协议、用户名以及密码，然后单击“更新”以保存信息。

转换器即得到配置。

创建 CA ARCserve Central Virtual Standby 策略

Virtual Standby 允许您创建两种策略类型，以定义您分配给 CA ARCserve D2D 节点的自定义转换策略。两种类型的策略是：

- 本地虚拟备用策略 (p. 36)
- 远程虚拟备用策略 (p. 42)

注意：要创建策略，CA ARCserve D2D 必须安装在监视器服务器上。

创建本地虚拟备用策略

Virtual Standby 允许您创建本地虚拟备用策略，以定义您分配给 CA ARCserve D2D 节点的自定义转换策略。

注意：要创建策略，CA ARCserve D2D 必须安装在监视器服务器上。

遵循这些步骤:

1. 登录 Virtual Standby 服务器，然后打开 Virtual Standby。

   从主页上的“导航”栏，单击“策略”。

   “策略”窗口打开。

2. 单击“新建”，然后单击弹出式菜单上的“新建本地虚拟备用策略”。

   “创建本地虚拟备用策略”对话框打开。

3. 在“策略名称”字段中，为策略指定名称。

   单击“Virtual Standby”选项卡。

   “虚拟化服务器”、“虚拟机”和“替代设置”选项显示。

4. 单击“虚拟化服务器”。

   “虚拟化服务器”选项出现。

5. 完成以下“虚拟化服务器”选项：

   VMware 系统：

   - **虚拟化类型 --** 单击“VMware”。
   - **ESX 主机/Virtual Center** - 指定 ESX 或 vCenter Server 系统的主机名。
   - **用户名 --** 指定登录 VMware 系统所需的用户名。

     注意：您指定的帐户必须是管理帐户或者是在 ESX 或 vCenter Server 系统上具有管理权限的帐户。
   - **密码 --** 指定登录 VMware 系统所需的用户名的密码。
   - **协议 --** 指定 HTTP 或 HTTPS 作为要用于源 CA ARCserve D2D 节点和监视服务器之间的通信协议。
   - **端口 --** 指定要用于源服务器和监视服务器之间的数据传输端口。
   - **ESX 节点 --** 该字段中的值根据在“ESX 主机/vCenter”字段指定的值变化而变化：
     - **ESX Server 系统 --** 在“ESX 主机/vCenter”字段中指定 ESX Server 系统时，该字段显示 ESX Server 系统的主机名。
     - **vCenter Server 系统 --** 在“ESX 主机/vCenter”字段中指定 vCenter Server 系统时，该字段允许您（从下拉列表）指定要与该策略关联的 ESX Server 系统。
   - **监视器服务器 --** 指定要用于监视源服务器状态的服务器的主机名。

     注意：在监视器服务器没有充当 CA ARCserve Central HostBased VM Backup 实施的代理服务器的情况下，该服务器可能是任何物理计算机或虚拟机。
   - **用户名 --** 指定登录监控系统所需的用户名。
   - **密码 --** 指定登录监控系统所需的用户名的密码。
   - **协议 --** 将 HTTP 或 HTTPS 指定为要用于 CA ARCserve Central Virtual Standby 服务器和 ESX 服务器系统（监视服务器）之间的通讯协议。
   - **端口 --** 指定要用于 CA ARCserve Central Virtual Standby 服务器和 ESX 服务器系统（监视服务器）之间的数据传输端口。

- **将监视器服务器用作数据传输的代理 --** 指定该选项以允许监视器服务器将转换数据从 CA ARCserve D2D 源节点复制到 ESX 服务器数据存储。如果启用该选项，Virtual Standby 使用光纤通道通信将转换数据从源节点传输到 ESX Server 数据存储，这要比使用 LAN 通信传输数据快。

  注意：默认情况下，“将监视器服务器用作数据传输的代理”选项被启用。您可以禁用该选项，以允许 CA ARCserve D2D 源服务器将转换数据直接复制到 ESX Server 系统上的数据存储。

Hyper-V 系统：

- **虚拟化类型 --** 单击“Hyper-V”。
- **Hyper-V 主机名 --** 指定 Hyper-V 系统的主机名。
- **用户名 --** 指定登录 Hyper-V 系统所需的用户名。

  注意：您指定的帐户必须是管理帐户或者是在 Hyper-V 系统上具有管理权限的帐户。
- **密码 --** 指定登录 Hyper-V 系统所需的用户名的密码。
- **端口 --** 指定要用于源服务器和监视服务器之间的数据传输端口。
- **用户名 --** 指定登录监控系统所需的用户名。
- **密码 --** 指定登录监控系统所需的用户名的密码。
- **协议 --** 将 HTTP 或 HTTPS 指定为要用于 CA ARCserve Central Virtual Standby 服务器和 Hyper-V 服务器系统（监视服务器）之间的通讯协议。
- **端口 --** 指定要用于 CA ARCserve Central Virtual Standby 服务器和 Hyper-V 服务器系统（监视服务器）之间的数据传输端口。

单击“虚拟机”。

“虚拟机”选项出现。

6. 完成下列“虚拟机”选项：

VMware 系统：

将下列虚拟机选项应用于 VMware 系统：

- **VM 名称前缀 -** 指定想为 ESX Server 系统上的虚拟机的显示名称添加的前缀。

  默认值：CAVM_

- **VM 资源池 --** 指定备用虚拟机要进行分组的资源池的名称。
- **CPU 计数 --** 指定备用虚拟机支持的最小及最大 CPU 计数。
- **内存 --** 指定要为备用虚拟机分配的 RAM 总量(MB)。

  注意：指定的 RAM 量必须是 2 的倍数。

- **VM 存储 --** 指定要存储转换数据的位置。
  - **为所有虚拟磁盘指定一个数据库 --** 允许应用程序将与虚拟机有关的所有磁盘复制到一个数据存储。
  - **为每个虚拟磁盘指定数据存储 --** 允许应用程序将虚拟机的磁盘有关信息复制到对应的数据存储。
- **VM 网络 --** 允许您定义 ESX Server 系统用于与虚拟机进行通信的 NIC、虚拟网络和路径。
  - **指定每个 NIC 的网络适配器类型，并且将该网络适配器连接到以下虚拟网络 --** 允许您定义如何将虚拟 NIC 映射到虚拟网络。当虚拟机包含虚拟 NIC 和虚拟网络时，指定该选项。
  - **为每个 NIC 指定网络适配器类型和虚拟网络 --** 允许您定义 NIC 用于通信的虚拟网络的名称。

Hyper-V 系统：

将下列虚拟机选项应用于 Hyper-V 系统：

- **VM 基本设置 --** 完成下列 VM 基本设置：
  - **VM 名称前缀 -** 指定想为 Hyper-V 系统上的虚拟机的显示名称添加的前缀。

    默认值：CAVM_

    CPU 计数 -- 指定备用虚拟系统支持的最小及最大 CPU 计数。
  - **内存 --** 指定要分配给备用虚拟机的 RAM 总量(MB)。

    注意：指定的 RAM 量必须是 4 的倍数。
- **VM 路径 --** 指定以下 VM 路径选项之一：
  - **为所有虚拟磁盘指定一个路径 --** 在 Hyper-V 服务器上指定要存储转换数据的位置。
  - **为每个虚拟磁盘指定路径 --** 在 Hyper-V 服务器上指定要为每个虚拟磁盘存储转换数据的位置。

  注意：CA ARCserve Central Virtual Standby 不支持在压缩卷和由文件系统加密的卷上创建虚拟磁盘映像（VHD 文件）。如果指定的路径位于压缩的或加密的 Hyper-V 卷上，Virtual Standby 会阻止您创建策略。
- **VM 网络 --** 允许您定义 Hyper-V 服务器用于与虚拟机进行通信的 NIC、虚拟网络和路径。指定下列选项之一并且完成必需字段。
  - **指定每个 NIC 的网络适配器类型，并且将该网络适配器连接到以下网络 --** 允许您定义如何将虚拟 NIC 映射到虚拟网络。当虚拟机包含虚拟 NIC 和虚拟网络时，指定该选项。
  - **为每个 NIC 指定网络适配器类型和虚拟网络 --** 允许您定义 NIC 用于通信的虚拟网络的名称。

单击“替代设置”。

“替代设置”选项显示。

7. 完成下列“替代设置”选项：

   恢复：

   选择下列方法之一：

   - **手动启动虚拟机 --** 允许您在源服务器失败或停止通信时手动打开和配给虚拟机。您希望在配给虚拟机且允许服务器充当源服务器之前分析失败原因时，请指定该选项。
   - **自动启动虚拟机 --** 允许您在源服务器失败或停止通信时自动打开和配给虚拟机。您想在源服务器失败或停止通信后允许虚拟机充当源服务器时，请指定该选项。

   注意：手动启动虚拟机是默认恢复选项。

   监控信号属性：

   - **超时 -** 指定监视器服务器在打开恢复点快照之前必须等待监控信号的时间长度。
   - **频率 -** 指定源服务器将监控信号传递给监视器服务器的频率。

     示例：指定的超时值是 60。指定的频率值是 10。源服务器将以 10 秒间隔传递监控信号。如果监视器服务器在上次检测到监控信号的 60 秒内没有检测到监控信号，监视器服务器会使用最新的恢复点快照打开虚拟机。

   单击“首选项”选项卡。

   “电子邮件报警”选项显示。

8. 完成以下电子邮件报警选项：

   - **源计算机缺失监控信号 --** 在监视器服务器未从源服务器检测到监控信号时，Virtual Standby 将发送报警通知。
   - **为配置成自动开机的源计算机打开的 VM --** Virtual Standby 打开已配置为在未检测到监控信号时自动开机的虚拟机时发送报警通知。
   - **配置成手动开机的源计算机缺失监控信号 --** Virtual Standby 从未配置为自动开机的源服务器检测到监控信号时发送报警通知。
   - **VM 存储可用空间少于 --** Virtual Standby 在定义的管理程序路径上检测的可用磁盘空间不足时 Virtual Standby 将发送报警通知。可用磁盘空间量少于用户定义的阈值时，监测便会发生。可以将阈值定义为绝对值 (MB) 或卷容量的百分比。
   - **Virtual Standby 错误/失败/崩溃 -** Virtual Standby 检测到在转换过程期间发生的错误时将发送报警通知。
   - **Virtual Standby 成功 --** Virtual Standby 检测到虚拟机成功开机时，它发送报警通知。

- **无法连接到管理程序 --** Virtual Standby 检测到其无法与 ESX Server 系统或 Hyper-V 系统通信时将发送报警通知。
- **许可故障 --** Virtual Standby 在 Virtual Standby 服务器、源服务器和监视器服务器上检测到许可问题时将发送报警通知。
- **Virtual Standby 未成功从恢复点快照启动 --** Virtual Standby 检测到虚拟机未自动打开且已指定“自动启动虚拟机”替代恢复选项时，其便会发送报警通知。

单击“保存”。

策略即被保存。

创建远程虚拟备用策略

Virtual Standby 允许您创建本地 Virtual Standby 策略，以定义您从 CA ARCserve 复制和高可用性 分配给节点的自定义转换策略。

遵循这些步骤:

1. 登录 Virtual Standby 服务器，然后打开 Virtual Standby。

   从主页上的“导航”栏，单击“策略”。

   “策略”窗口打开。

2. 单击“新建”，然后单击弹出式菜单上的“新建远程虚拟备用策略”。

   “创建远程虚拟备用策略”对话框打开。

3. 在“策略名称”字段中，为策略指定名称。

   单击“Virtual Standby”选项卡。

   “虚拟化服务器”和“虚拟机”选项显示。

4. 单击“虚拟化服务器”。

   “虚拟化服务器”选项出现。

5. 完成以下“虚拟化服务器”选项：

   VMware 系统：

   - **虚拟化类型 --** 单击“VMware”。
   - **ESX 主机/Virtual Center** - 指定 ESX 或 vCenter Server 系统的主机名。
   - **用户名 --** 指定登录 VMware 系统所需的用户名。

     注意：您指定的帐户必须是管理帐户或者是在 ESX 或 vCenter Server 系统上具有管理权限的帐户。
   - **密码 --** 指定登录 VMware 系统所需的用户名的密码。
   - **协议 --** 指定 HTTP 或 HTTPS 作为要用于源 CA ARCserve D2D 节点和监视服务器之间的通信协议。
   - **端口 --** 指定要用于源服务器和监视服务器之间的数据传输端口。
   - **ESX 节点 --** 该字段中的值根据在“ESX 主机/vCenter”字段指定的值变化而变化：
     - **ESX Server 系统 --** 在“ESX 主机/vCenter”字段中指定 ESX Server 系统时，该字段显示 ESX Server 系统的主机名。
     - **vCenter Server 系统 --** 在“ESX 主机/vCenter”字段中指定 vCenter Server 系统时，该字段允许您（从下拉列表）指定要与该策略关联的 ESX Server 系统。

   Hyper-V 系统：

   - **虚拟化类型 --** 单击“Hyper-V”。
   - **Hyper-V 主机名 --** 指定 Hyper-V 系统的主机名。
   - **用户名 --** 指定登录 Hyper-V 系统所需的用户名。

     注意：您指定的帐户必须是管理帐户或者是在 Hyper-V 系统上具有管理权限的帐户。
   - **密码 --** 指定登录 Hyper-V 系统所需的用户名的密码。
   - **协议 --** 指定 HTTP 或 HTTPS 作为要用于源 CA ARCserve D2D 节点和监视服务器之间的通信协议。
   - **端口 --** 指定要用于源服务器和监视服务器之间的数据传输端口。

   单击“虚拟机”。

   “虚拟机”选项出现。

6. 完成下列“虚拟机”选项：

   VMware 系统：

   将下列虚拟机选项应用于 VMware 系统：

   - **VM 名称前缀 -** 指定想为 ESX Server 系统上的虚拟机的显示名称添加的前缀。

     默认值：CAVM_
   - **VM 资源池 --** 指定备用虚拟机要进行分组的资源池的名称。
   - **CPU 计数 --** 指定备用虚拟机支持的最小及最大 CPU 计数。
   - **内存 --** 指定要为备用虚拟机分配的 RAM 总量(MB)。

     注意：指定的 RAM 量必须是 2 的倍数。
   - **VM 存储 --** 指定要存储转换数据的位置。
     - **为所有虚拟磁盘指定一个数据库 --** 允许应用程序将与虚拟机有关的所有磁盘复制到一个数据存储。
     - **为每个虚拟磁盘指定数据存储 --** 允许应用程序将虚拟机的磁盘有关信息复制到对应的数据存储。
   - **VM 网络 --** 允许您定义 ESX Server 系统用于与虚拟机进行通信的 NIC、虚拟网络和路径。
     - **指定每个 NIC 的网络适配器类型，并且将该网络适配器连接到以下虚拟网络 --** 允许您定义如何将虚拟 NIC 映射到虚拟网络。当虚拟机包含虚拟 NIC 和虚拟网络时，指定该选项。
     - **为每个 NIC 指定网络适配器类型和虚拟网络 --** 允许您定义 NIC 用于通信的虚拟网络的名称。

Hyper-V 系统：

将下列虚拟机选项应用于 Hyper-V 系统：

- **VM 基本设置 --** 完成下列 VM 基本设置：
  - **VM 名称前缀 -** 指定想为 Hyper-V 系统上的虚拟机的显示名称添加的前缀。

    默认值：CAVM_

    CPU 计数 -- 指定备用虚拟系统支持的最小及最大 CPU 计数。
  - **内存 --** 指定要分配给备用虚拟机的 RAM 总量(MB)。

    注意：指定的 RAM 量必须是 4 的倍数。
- **VM 路径 --** 指定以下 VM 路径选项之一：
  - **为所有虚拟磁盘指定一个路径 --** 在 Hyper-V 服务器上指定要存储转换数据的位置。
  - **为每个虚拟磁盘指定路径 --** 在 Hyper-V 服务器上指定要为每个虚拟磁盘存储转换数据的位置。

  注意：CA ARCserve Central Virtual Standby 不支持在压缩卷和由文件系统加密的卷上创建虚拟磁盘映像（VHD 文件）。如果指定的路径位于压缩的或加密的 Hyper-V 卷上，Virtual Standby 会阻止您创建策略。
- **VM 网络 --** 允许您定义 Hyper-V 服务器用于与虚拟机进行通信的 NIC、虚拟网络和路径。指定下列选项之一并且完成必需字段。
  - **指定每个 NIC 的网络适配器类型，并且将该网络适配器连接到以下网络 --** 允许您定义如何将虚拟 NIC 映射到虚拟网络。当虚拟机包含虚拟 NIC 和虚拟网络时，指定该选项。
  - **为每个 NIC 指定网络适配器类型和虚拟网络 --** 允许您定义 NIC 用于通信的虚拟网络的名称。

单击“首选项”选项卡。

“电子邮件报警”选项显示。

7. 完成以下电子邮件报警选项：
   - **VM 存储可用空间少于 --** Virtual Standby 在定义的管理程序路径上检测的可用磁盘空间不足时 Virtual Standby 将发送报警通知。可用磁盘空间量少于用户定义的阈值时，监测便会发生。可以将阈值定义为绝对值 (MB) 或卷容量的百分比。
   - **Virtual Standby 错误/失败/崩溃 -** Virtual Standby 检测到在转换过程期间发生的错误时将发送报警通知。
   - **Virtual Standby 成功 --** Virtual Standby 检测到虚拟机成功开机时，它发送报警通知。

- **无法连接到管理程序 --** Virtual Standby 检测到其无法与 ESX Server 系统或 Hyper-V 系统通信时将发送报警通知。
- **许可故障 --** Virtual Standby 在 Virtual Standby 服务器、源服务器和监视器服务器上检测到许可问题时将发送报警通知。
- **Virtual Standby 未成功从恢复点快照启动 --** Virtual Standby 检测到虚拟机未自动打开且已指定“自动启动虚拟机”替代恢复选项时，其便会发送报警通知。

单击“保存”。

策略即被保存。

向策略分配和取消分配节点

要创建恢复点快照，您应该将虚拟备用转换策略分配给要保护的 CA ARCserve D2D 节点。

Virtual Standby 允许您从策略取消分配节点。Virtual Standby 不允许您将多个策略分配给节点。要将节点分配给新策略时，您应该从节点取消分配当前策略，然后才能将新策略分配给节点。

遵循这些步骤:

1. 登录虚拟备用服务器，然后打开 Virtual Standby。

   从主页上的导航栏，单击“策略”以打开“策略”屏幕。

2. 从“策略”列表中，单击要分配或取消分配节点的策略。

   指定策略的详细信息显示在“策略详细信息”选项卡和“策略分配”选项卡中。

3. 单击“策略详细信息”选项卡以查看该策略的详细信息。

   （可选）单击工具栏上的“编辑”以编辑该策略的当前设置。

   注意：有关详细信息，请参阅“编辑策略”。

4. 单击“策略分配”选项卡。

   单击在“策略分配”选项卡上的“分配和取消分配”。

   此时打开“分配/取消分配策略”对话框。

5. 在“分配/取消分配策略”对话框指定以下字段：
   - **组** -- 选择包含想要分配的策略的组名称。
   - **节点名称筛选** -- 允许您基于通常标准筛选可用节点。

   注意：“筛选”字段支持使用通配符。

   示例：

   – Acc* 允许您筛选节点名称以 Acc 开头的所有节点。

   – *.123 允许您筛选 IP 地址中含有 .123 的所有节点。

   注意：要清除筛选结果，请在“筛选”字段单击“X”。
6. 执行下列操作之一：
   - **分配一个节点** -- 从“可用节点”列表，找到要分配给策略的节点。

     单击向右单箭头。

     节点便从“可用节点”列表移到“选定的节点”列表。
   - **分配多个节点** -- 从“可用节点”列表，单击向右双箭头。

     所有节点便从“可用节点”列表移到“选定的节点”列表。
   - **取消分配一个节点** -- 从“选定的节点”列表，找到要从策略取消分配的节点。

     单击向左单箭头。

     节点便从“选定的节点”列表移到“可用节点”列表。
   - **取消分配多个节点** -- 从“选定的节点”列表，单击向左双箭头。

     所有节点便从“选定的节点”列表移到“可用节点”列表。

   单击“确定”。

节点即被从策略分配/取消分配。

部署策略

在创建策略之后，您将节点分配给策略 (p. 46)，然后部署该策略。

以下行为适用于策略部署过程：

- 策略部署过程在以下条件下失败：
  - Windows Server 2008 Hyper-V Role 安装在 CA ARCserve D2D 源服务器（节点）上。
  - 已从 CA ARCserve Central HostBased VM Backup 导入 CA ARCserve D2D 节点。在 Host-Based VM Backup 代理系统上已启用 Windows Hyper-v 角色，并将备份代理系统指定为 Virtual Standby 目标。
- CA ARCserve Central Virtual Standby 无法自动打开从 CA ARCserve Central HostBased VM Backup 服务器添加的虚拟机。因此，在将包含恢复方式被定义为自动启动虚拟机的策略部署到受 Host-Based VM Backup 保护的节点时，Virtual Standby 会将该恢复方式的值更改为手动启动虚拟机。

遵循这些步骤:

1. 登录 Virtual Standby 服务器，然后打开 Virtual Standby。

   从主页上的导航栏，单击“策略”以打开“策略”屏幕。

2. 从“策略”列表上，单击要部署的策略。

   指定策略的详细信息显示在“策略详细信息”选项卡和“策略分配”选项卡中。

3. 单击“策略详细信息”选项卡以查看该策略的详细信息。

   （可选）单击工具栏上的“编辑”以编辑该当前策略设置。

   注意：有关详细信息，请参阅“编辑策略”。

4. 单击“策略分配”选项卡。

   此时将显示分配给策略的节点的相关详细信息。

   （可选）单击工具栏上的“分配和取消分配” 以向策略分配或取消分配节点。

   注意：有关详细信息，请参阅将节点分配给策略 (p. 46)或从策略取消分配节点。

5. 单击工具栏上的“立即部署”。

   “立即部署”确认信息出现。

6. 单击“确定”。

策略即被部署。

注意：您还可以从“节点”屏幕的“策略”列下，查看特定节点的策略部署状态。

第 4 章： CA ARCserve Central Virtual Standby 入门

以下各节说明如何配置 CA ARCserve Central Virtual Standby 来保护 CA ARCserve D2D 节点。

注意：在您可以完成该部分所述的配置之前，请确认已完成所有的先决条件安装任务 (p. 13)。

此部分包含以下主题：

登录 CA ARCserve Backup

您可以直接从安装该应用程序的计算机或使用支持的浏览器从远程计算机登录 CA ARCserve Central Virtual Standby。有关支持的操作系统的完整列表，请参阅《*CA ARCserve Central Virtual Standby 版本说明*》。

登录 CA ARCserve Central Virtual Standby

1. 执行以下选项之一：

   - 如果登录到安装 CA ARCserve Central Virtual Standby 的服务器；从程序文件启动应用程序。

     浏览器窗口打开，并显示 CA ARCserve Central Virtual Standby“登录”屏幕。

     完成登录屏幕上的以下字段：

     - 用户名
     - 密码

     单击“登录”。

   - 如果您未登录安装 CA ARCserve Central Virtual Standby 的服务器，请打开浏览器窗口，并在地址栏中指定以下 url：

     ```
     http://<CA ARCserve Central Application 服务器名>:<端口号>/virtualstandby/
     ```

     注意：可以指定安装 CA ARCserve Central Virtual Standby 的服务器的主机名或 IP 地址。默认端口为 8015。

     按 Enter 键。

     浏览器窗口打开，并显示 CA ARCserve Central Virtual Standby“登录”屏幕。

     完成登录屏幕上的以下字段：

     - 用户名
     - 密码

     单击“登录”。

   登录到 CA ARCserve Central Virtual Standby，主页打开。

为基于 VMware 的节点指定 ESX Server 或 vCenter Server 系统

注意：以下步骤仅适用于基于 VMware 的虚拟机源节点。

在各种基于 VMware 的实施中，Virtual Standby 可能无法检测到配置为驻留在 ESX Server 和 vCenter Server 系统上的虚拟机的源节点。该行为会阻止 Virtual Standby 将正确的许可应用于节点、将策略部署到节点以及执行转换作业。

下列步骤让您可以指定节点所在的 ESX Server 或 vCenter Server 系统的主机名或 IP 地址。在您完成该步骤后，Virtual Standby 可以对您想要保护的节点进行检测、应用许可、部署策略以及执行转换作业。如果有多个虚拟机驻留在充当一个源节点的 ESX Server 或 vCenter Server 系统上，该步骤让您可以为所有节点消耗一个许可，这会帮助降低保护源节点的总体成本。

为基于 VMware 的节点指定 ESX Server 或 vCenter Server 系统

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，然后从弹出菜单单击“指定 ESX 服务器”。

   此时打开“指定 ESX Server ”对话框。

   注意：如果应用程序检测到由 ESX Server 或者 vCenter Server 系统管理的虚拟机上没有安装 VMware 工具、虚拟机驻留在 Hyper-V 系统上或者检测到的节点不是虚拟机，则会出现错误消息。

4. 在“添加 ESX Server ”对话框上完成以下字段：

   - ESX/vCenter 主机

     注意：指定 ESX Server 或 vCenter Server 系统的主机名或 IP 地址。

   - 用户名
   - 密码
   - Port

     注意：默认通讯端口是 443。如果节点使用不同的端口号与 ESX Server 或 vCenter Server 系统进行通信，请指定使用的端口号。

   - Protocol

     注意：默认通信协议是 HTTPS。如果节点使用 HTTP 与 ESX Server 或 vCenter Server 系统进行通信，请单击“HTTP”。

   单击“确定”。

ESX Server 或 vCenter Server 系统被分配给节点。

第 5 章：使用 CA ARCserve Central Virtual Standby

此部分包含以下主题：

登录 CA ARCserve D2D 节点

从 Virtual Standby 主页，您可以登录 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”。

   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。

登录监视器服务器

通过 Virtual Standby，您可以直接登录到正在监视 CA ARCserve D2D 源节点的服务器。从监视器服务器，您可以执行维护任务并查看有关监视器服务器正在监视的源服务器的运行状况。您可以通过以下图标将 CA ARCserve D2D 节点与监视器服务器区分开来：

监视器服务器图标：

CA ARCserve D2D 节点图标：

登录监视器服务器

1. 登录 Virtual Standby 服务器，然后打开 Virtual Standby。

   从主页上的“导航”栏，单击“节点”。

   “节点”屏幕打开。

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. 执行以下操作之一：

   - 如果您知道监视器服务器的 IP 地址或主机名，请浏览至并单击要登录的监视器服务器，然后从弹出菜单单击“登录 D2D”。
   - 如果不知道监视器服务器的 IP 地址或主机名，请浏览至并单击您想登录其监视器服务器的 CA ARCserve D2D 节点，然后从弹出菜单上单击“登录监视器服务器”

   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。

您已登录到监视器服务器。

节点维护任务

Virtual Standby 允许您通过若干方法添加节点：

- 按 IP 地址或节点名称添加节点 (p. 29)
- 从文件导入节点 (p. 30)

  注意：该方法允许您从逗号分隔文件格式的节点列表导入多个节点。
- 从 CA ARCserve Central HostBased VM Backup 服务器添加节点 (p. 32)

  注意：该方法允许您导入 CA ARCserve Central HostBased VM Backup 应用程序保护的虚拟机节点。
- 从 CA ARCserve 复制和高可用性 导入节点 (p. 35)。

此外，您可以执行以下节点管理任务。

- 更新节点 (p. 57)。
- 增添了为一个或多个 CA ARCserve D2D 节点设置备份密码 (p. 60)。
- 删除节点 (p. 61)。
- 从节点释放许可 (p. 62)。
- 从监视器服务器停止监视节点。 (p. 63)
- 更改 CA ARCserve Central Applications 服务器的主机名后更新节点和策略 (p. 64)。

更新节点

Virtual Standby 允许您更新以前添加的节点的信息。

注意：您无法更新从 CA ARCserve Central HostBased VM Backup 服务器导入的节点。

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. 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。

   注意：如果对 CA ARCserve D2D 节点做了更改，“更新节点”对话框打开以便让您指定更多详细信息。

6. （可选）如果更新的信息未显示在节点列表中，单击工具栏上的“刷新”。

该节点即被更新。

增添了为一个或多个 CA ARCserve D2D 节点设置备份密码

提交 D2D 备份时，备份的密码即被存储在您正保护的 D2D 节点上。然后，CA ARCserve 复制和高可用性 将 D2D 恢复点复制到托管服务提供商 (MSP) 站点上。MSP 站点上的转换器则将复制的数据转化成虚拟机数据，并将数据存储在 MSP 站点上。然而，转换器无法转换复制的恢复点快照，因为备份密码位于 D2D 节点上。

为了确保转换器可以转换复制的恢复点快照，Virtual Standby 允许您为转换器可以用来转换数据的 D2D 数据指定备份密码。

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”。

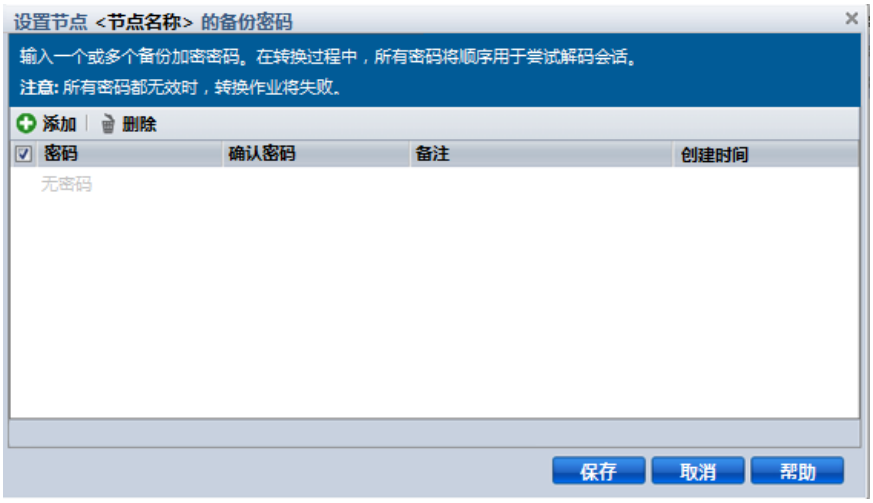
   “节点”屏幕将显示。

2. 从“组”栏上，单击“全部节点”组，或单击包含要设置备份密码的节点的组名称。

   与该组关联的节点显示在节点列表中。

3. 单击要设置备份密码的节点，然后右键单击，并从弹出菜单中选择“设置备份密码”。

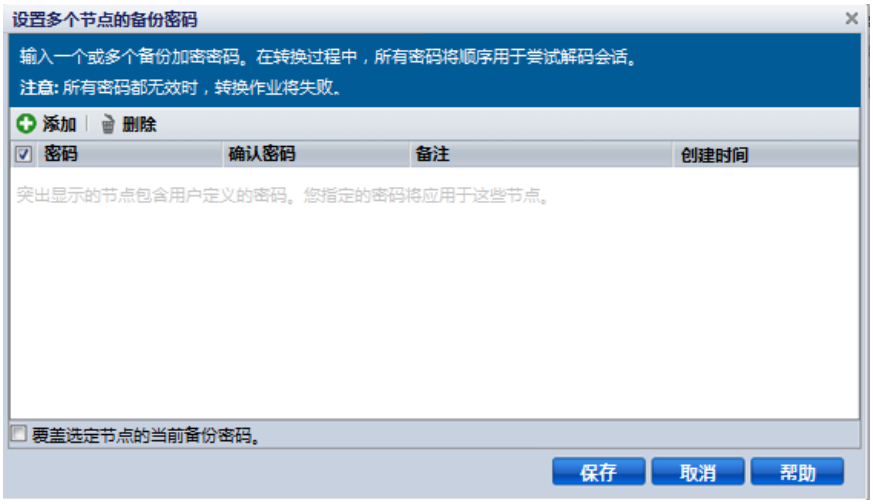
   “设置节点的备份密码”对话框打开。



您可以在“设置备份密码”对话框中为一个或多个节点执行以下任务：

- **添加** -- 单击“添加”可将一个或多个备份密码添加到选定节点。
- **删除** -- 单击“删除”可从选定节点删除一个或多个备份密码。

注意：对于多个节点，您可以选择“覆盖选定节点的当前备份密码”复选框，来覆盖多个节点的当前备份密码。



4. 单击“保存”。

   对话框关闭，选定远程节点的备份密码得到设置。

删除节点

Virtual Standby 允许您将节点从环境中删除。

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”。

释放节点的许可

CA ARCserve Backup 许可在基于计数的机制上工作。通过基于计数的许可，您可以将单个整体许可授予预定义数量活动许可权限已包含在整体许可池中的节点。根据先来先服务的原则从池中授予使用此许可的节点一个活动许可，直到达到可用许可权限总数。如果应用了所有的活动许可权限，而您想将许可添加给其他节点，请释放一个或多个节点的许可权限以便增加可用的许可数，然后其他节点才能使用该许可。

释放节点的许可

1. 登录该应用程序。
2. 在主屏幕中，通过单击“帮助”，然后单击“管理许可”，来打开“许可管理”对话框。

   此时打开“许可管理”对话框，并显示适用于物理计算机、基于 VMware 的虚拟机和基于 Hyper-V 的虚拟机的许可列表，如以下对话框所示：

3. 在“许可状态”部分中，选择想要从节点释放的许可。

   使用许可的节点显示在“许可管理”对话框的“经许可的计算机”部分中。

4. 单击要释放许可的节点旁的复选框。

   注意：单击“全部清除”来清除所有显示在“许可管理”对话框的“经许可的计算机”部分中的节点旁的复选框。

5. 单击“应用”。

   已释放指定节点的许可。

6. （可选）单击“刷新”可刷新使用指定许可的节点列表。

从监视器服务器停止监视节点

CA ARCserve Central Virtual Standby 允许您从监视器服务器上的“Virtual Standby”选项卡停止监视节点。

重要说明！停止监视节点之后，Virtual Standby 虚拟机可能不包含打开虚拟机所需的最新恢复点快照。此外，仅可以从管理程序系统为停止监视的节点打开虚拟机。

从监视器服务器停止监视节点

1. 登录监视器服务器。

   注意：有关详细信息，请参阅登录监控服务器 (p. 56)。

2. 在监视器服务器打开后，单击“Virtual Standby”选项卡。

   此时打开“Virtual Standby”屏幕。

3. 从“源”树，展开“全部”、“正运行的源”、“要求操作”或“正运行的 VM”以找到想要停止监视的源节点。

4. 右键单击想要停止监视的节点，然后单击弹出菜单上的“停止监视”。

   此时将显示警告消息。

5. 如果确实要停止监视指定的节点，请单击“是”。

节点即被从“源”树移除，监视器服务器即可停止监视该节点。

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

在您更改 CA ARCserve Central Virtual Standby 服务器的主机名后，您更新节点以及应用到节点的策略。您执行这些任务以维护 CA ARCserve Central Virtual Standby 服务器和 CA ARCserve Central Virtual Standby 服务器正在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。

方案	解决措施：
节点在 CA ARCserve Central Virtual Standby 服务器的主机名更改后被添加。	无需采取任何操作。
节点在 CA ARCserve Central Virtual Standby 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. 57)。
节点在 CA ARCserve Central Virtual Standby 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，请参阅部署策略 (p. 48)。

节点组管理任务

Virtual Standby 允许您管理您正在保护的 CA ARCserve D2D 节点组。

此部分包括以下主题：

添加节点组

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。

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。

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。

删除节点组

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。

筛选节点组

Virtual Standby 允许您使用筛选将安装特定应用程序的 CA ARCserve D2D 节点显示在一个组中。Virtual Standby 允许您筛选安装以下应用程序的节点：

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

筛选节点组

1. 登录 Virtual Standby 服务器，然后打开 Virtual Standby。

   从主页上的导航栏，单击“节点”。

   “节点”屏幕将显示。

2. 从“组”列表中，单击要筛选的组。

   注意：您可以筛选所有默认组（“全部节点”、“未分配”、SQL Server 和 Exchange）以及所有自定义名称的组。

   从“筛选”工具栏，单击要筛选的应用程序旁边的复选框。

该节点组即被删除。

Virtual Standby 策略管理任务

Virtual Standby 允许您管理您用来保护您的 CA ARCserve D2D 节点的转换策略。

- 创建 CA ARCserve Central Virtual Standby 策略 (p. 36)
- 向策略分配和取消分配节点 (p. 46)
  - 部署策略 (p. 48)
- 编辑或复制策略 (p. 69)
- 删除策略 (p. 70)

编辑或复制策略

Virtual Standby 允许您在创建策略后编辑或复制策略。

编辑策略

1. 登录 Virtual Standby 服务器，然后打开 Virtual Standby。

   从主页上的“导航”栏，单击“策略”。

   “策略”窗口打开。

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. 如果您想更改策略名称，请在“策略名称”字段指定名称。
4. 基于您选择的策略类型，将更改应用于“Virtual Standby”选项卡和“首选项”选项卡。
   - 本地虚拟备用策略 (p. 36)
   - 远程虚拟备用策略 (p. 42)

策略即被编辑。

删除策略

Virtual Standby 允许您删除以前创建的策略。

注意：Virtual Standby 不允许您删除分配给节点的策略。要删除已分配有节点的策略，您必须从策略取消分配节点，然后删除该策略。有关从策略如何取消分配节点，请参阅从策略取消分配节点。

删除策略

1. 登录 Virtual Standby 服务器，然后打开 Virtual Standby。

   从主页上的“导航”栏，单击“VCM 策略”。

   “策略”窗口打开。

2. 从“策略”列表上，单击要删除的策略。
3. 单击“策略”工具栏上的“删除”。

   删除确认消息将显示。

4. 单击“是”即可删除该策略。

   注意：如果误删了策略，您必须重新创建该策略。如果您不想删除策略，单击“否”

该策略即被删除。

应用程序配置任务

Virtual Standby 允许您指定电子邮件报警设置以及如何更新 Virtual Standby 安装。

本节包括以下主题：

配置电子邮件设置

您可以配置用于该应用程序的电子邮件设置，从而在您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“电子邮件配置”以显示“电子邮件配置”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. 单击“保存”。

   注意：您可以单击“重置”以恢复到先前保存值。

电子邮件配置即被应用。

配置自动更新

使用 CA ARCserve Central Virtual Standby，您可以定义何时检查产品更新，并可以定义更新 Virtual Standby 安装的频率。

配置自动更新

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。

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。

配置社交网络首选项

1. 登录该应用程序。

   从主页上的导航栏，单击“配置”。

   “配置”屏幕显示。

2. 从“配置”面板，单击“首选项配置”。

   “首选项”选项显示。

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的 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。

查看日志

“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。
     - **从文件导入节点** -- 该选项允许您仅查看将 CA ARCserve D2D 节点从文件导入到应用程序的过程的相关日志。
     - **策略管理** -- 该选项允许您仅查看有关策略管理的日志。
     - **更新** -- 该选项允许您仅查看有关应用程序更新的日志。
     - **暂停/恢复监控信号** -- 此选项允许您仅查看已经暂停或恢复监控信号的虚拟备用虚拟机的日志。
     - **暂停/恢复 Virtual Standby** -- 此选项允许您仅查看已经暂停或恢复 Virtual Standby 的虚拟备用虚拟机的日志。
     - **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。
     - **备用 VM** -- 此选项允许您仅查看已开机的虚拟机的日志。
     - **从 CA ARCserve Replication 导入节点** -- 此选项允许您仅查看从 CA ARCserve Replication 导入的节点的日志。
   - **节点名称** -- 该选项允许您仅查看有关特定节点的日志。

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”）。

单击“刷新”。

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。

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。

Virtual Standby 主页

监视器服务器上的“Virtual Standby”选项卡允许您查看您正在保护的所有 CA ARCserve D2D 服务器的有关信息。但是，源服务器上的“Virtual Standby”选项卡让您仅查看您登录的特定源服务器的相关信息。

本节包括以下主题：

如何使用 Virtual Standby 摘要屏幕

通过“Virtual Standby 摘要”屏幕显示的图标，可以快速直观了解当前状态，以及需要采取任何操作的紧迫性。

以下选项显示在主页上：

成功
(无需操作)

注意
(可能很快需要操作)

警告
(需要立即操作)

“Virtual Standby 摘要”屏幕显示以下信息：

- **服务器列表 --** 显示该监视器服务器正在保护的源服务器的列表。该列表按服务器的当前状态对服务器进行排序。例如，“全部”、“要求操作”、“服务器正运行”等等。

  注意：只有您登录到监视服务器，服务器列表才会出现。有关详细信息，请参阅如何使用服务器列表 (p. 79)。

- **Virtual Standby 摘要 --** 显示选定源服务器的摘要信息。有关详细信息，请参阅监视虚拟转换作业的状态 (p. 81)。

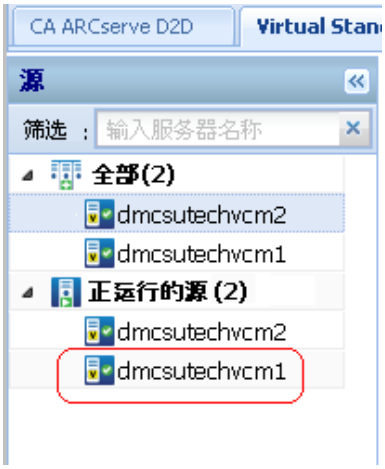
- **Virtual Standby 设置** -- 显示选定源服务器的虚拟转换设置的相关摘要信息。有关详细信息，请参阅查看源服务器的 Virtual Standby 设置 (p. 82)。
- **恢复点快照** -- 显示可用于选定源服务器的恢复点快照列表。有关详细信息，请参阅查看恢复点快照列表 (p. 82)。
- **任务** -- 显示您可以为选定源服务器执行的任务列表。有关详细信息，请参阅 Virtual Standby 监视任务 (p. 83)。
- **支持和社区访问** -- 提供一种机制，允许您启动各种与支持相关的功能。

  注意：有关支持和社区访问的更多信息，请参阅 CA ARCserve D2D 文档。

如何使用服务器列表

“Virtual Standby 摘要”屏幕上的服务器列表显示监视服务器正在保护的源服务器的列表。该列表按服务器的当前状态对服务器进行排序。例如，“全部”、“要求操作”、“源正运行”等等。

要执行维护任务或查看有关 CA ARCserve D2D 节点的信息，请单击“Virtual Standby”选项卡，然后单击服务器，如以下屏幕所示：



查看有关最近的 Virtual Standby 作业的摘要信息

通过“节点”屏幕，可以查看节点上次的 Virtual Standby（转换）作业的摘要信息。可以查看已成功完成和未成功完成的 Virtual Standby 作业的相关信息。

遵循这些步骤:

1. 登录 Virtual Standby 服务器。

   单击导航栏上的“节点”以打开“节点”屏幕。

2. 在“状态”列中，将鼠标指针悬停在显示的下列任一图标上：

    成功

    警告

    错误/失败

   此时将显示“节点状态摘要”消息框，提供最近成功的 Virtual Standby 作业的下列结果：

   最近的 Virtual Standby

   最近成功或未成功完成 Virtual Standby 作业的日期和时间。

   恢复点快照

   显示截至“最近的 Virtual Standby”，为节点转换的恢复点数。

   目标状态

   显示 Virtual Standby 目标上的可用磁盘空间量。目标可以包括：

   - 一个 ESX Server 数据存储，用于转换到 ESX Server 系统。
   - 卷上的可用磁盘空间，Hyper-V 服务器将在其中存储恢复点快照。

3. 将鼠标指针从“状态”图标上移开以关闭“节点状态摘要”消息框。

4. 在下列字段中，可以查看有关最近成功或未成功的 Virtual Standby 作业的详细信息：

   上次转换结果

   已成功完成或未成功完成的最近 Virtual Standby 作业的结果。例如，“已完成”、“已取消”、“已失败”。

   上次转换时间

   最近已成功完成或未成功完成的 Virtual Standby 作业的日期和时间。

监视虚拟转换作业的状态

Virtual Standby 允许您监视正在进行的虚拟转换作业的状态。此外，Virtual Standby 允许您查看虚拟转换数据的以及正在保护 CA ARCserve D2D 源服务器的虚拟机的有关摘要信息。

监视虚拟转换作业的状态

1. 打开 Virtual Standby，单击导航栏上的“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”。

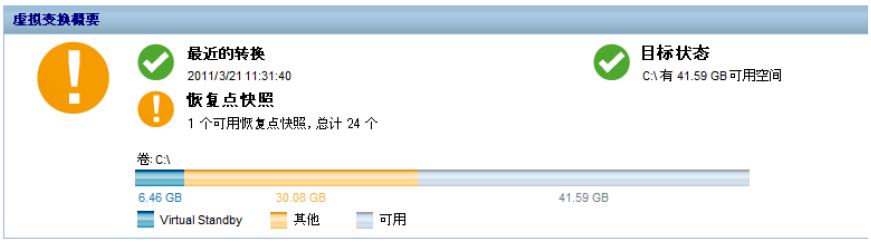
   CA ARCserve D2D 打开。

   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。

4. 单击“Virtual Standby”选项卡。

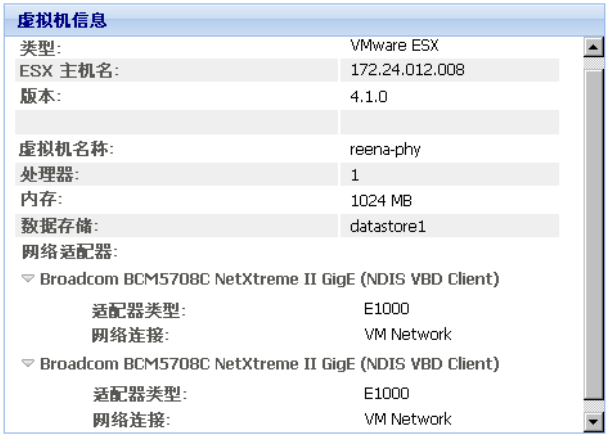
   （可选）如果 CA ARCserve D2D 服务器是监视器服务器，单击“服务器”列表，展开“全部”、“源正运行”或“要求操作”，然后单击要监视的服务器。

   Virtual Standby 显示正在进行的虚拟转换作业的有关信息，以及虚拟转换作业以及正在保护服务器的虚拟机的有关摘要信息。



查看源服务器的 Virtual Standby 设置

“Virtual Standby 摘要”屏幕显示正保护源服务器的虚拟机的有关信息。



查看恢复点快照列表

“Virtual Standby 摘要”屏幕显示最近恢复点快照的列表。

列表框显示 CA ARCserve D2D 服务器备份的完成日期和时间。

从恢复点快照列表中，您可以打开虚拟机。有关详细信息，请参阅打开恢复点快照。

注意：如果 Virtual Standby 目标是 VMware ESX 服务器，那么显示的恢复点快照的最大数目是 29。如果 Virtual Standby 目标是 Microsoft Hyper-V 服务器，那么显示的恢复点快照的最大数目是 24。

CA ARCserve Central Virtual Standby 监控作业

Virtual Standby 允许您执行以下监视任务：

- 暂停和恢复监控信号。
- 暂停和恢复 Virtual Standby 作业。
- 查看有关虚拟转换和恢复点快照的活动日志数据 (p. 83)。
- 打开恢复点快照。

查看作业的相关活动日志数据

Virtual Standby 允许查看虚拟转换作业的有关活动日志信息。活动日志包含您正在保护的 CA ARCserve D2D 源服务器的虚拟转换作业记录。

注意：活动日志（activity.log）存储在安装 CA ARCserve D2D 的服务器上的以下目录中：

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

查看作业的相关活动日志数据

1. 打开 Virtual Standby，然后单击导航栏上的“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 打开。

   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。

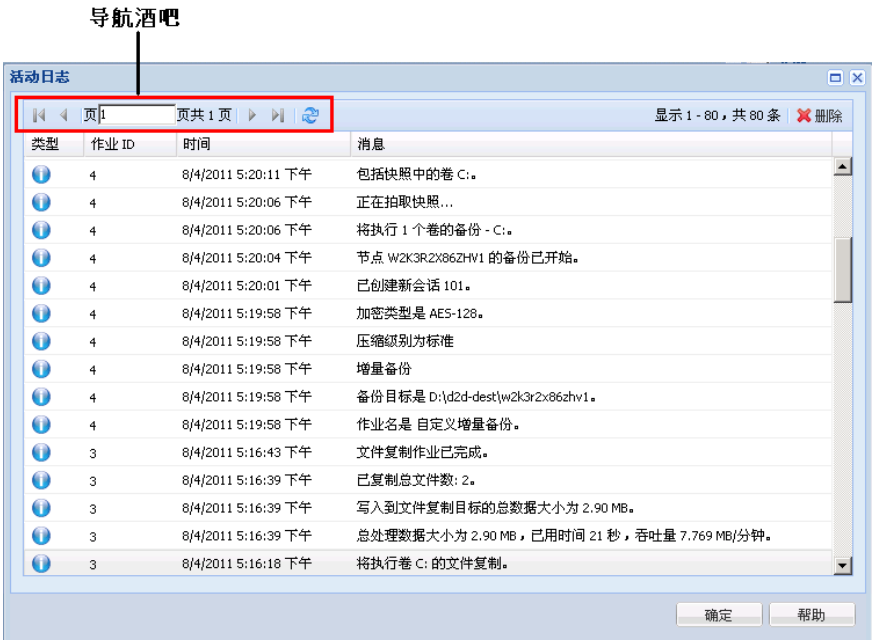
4. 单击“Virtual Standby”选项卡。

   此时打开“Virtual Standby 摘要”屏幕。

5. （可选）如果您登录到监视服务器，从“服务器”列表展开“全部”或“服务器正运行”，然后单击要查看其活动日数据的节点。

   从位于“Virtual Standby 摘要”屏幕右侧的“虚拟转换”任务列表中，单击“查看日志”。

   将显示“活动日志”对话框。



   使用导航栏来搜索并查看活动日志记录。下列图标出现在活动日志上：

   信息

   警告

   错误

   注意：有关删除活动日志记录的信息，请参阅删除活动日志记录 (p. 85)。

删除活动日志记录

Virtual Standby 允许您管理活动日志数据的总大小。活动日志包含您正在保护的 CA ARCserve D2D 源节点的作业记录。如果您正在保护大量的源服务器，执行频繁备份，或两者，活动日志会在 CA ARCserve D2D 节点上消耗大量的磁盘空间。

您可以删除早于指定日期的活动日志记录，或删除所有活动日志记录。

注意：活动日志（activity.log）存储在安装 CA ARCserve D2D 的服务器上的以下目录中：

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

删除活动日志记录

1. 打开 Virtual Standby，然后单击导航栏上的“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 打开。

   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。

4. 单击“Virtual Standby”选项卡。

   此时打开“Virtual Standby 摘要”屏幕。

5. （可选）如果您登录到监视服务器，从“服务器”列表展开“全部”或“服务器正运行”，然后单击要删除其活动日数据的节点。

6. 从位于“Virtual Standby 摘要”屏幕右侧的“虚拟转换”任务列表中，单击“查看日志”。

   将显示“活动日志”对话框。

7. 单击工具栏上的“删除”。

   “删除活动日志”对话框将打开。

8. 请单击下列选项之一：

   - **删除所有日志记录 --** 允许删除活动日志中的所有作业记录。

     注意：请慎用此选项。您无法恢复删除的活动日志记录。

   - **删除早于以下时间的所有日志记录 --** 允许您删除活动日志中早于指定日期的所有作业记录。

   单击“确定”。

记录即被从活动日志删除。

从 Virtual Standby 服务器查看有关 Virtual Standby 作业的状态信息

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

也可以从 Virtual Standby 服务器或直接从节点访问状态信息。有关如何从节点访问状态信息的信息，请参阅从节点查看有关 Virtual Standby 作业的状态信息 (p. 87)。

遵循这些步骤:

1. 登录 Virtual Standby 服务器。

   单击导航栏上的“节点”以打开“节点”屏幕。

2. 如果存在正在进行的 Virtual Standby 作业，“作业”字段中将显示作业所处的阶段，如以下屏幕所示：

3. 单击阶段将打开“Virtual Standby 状态监视器”对话框。

   注意：有关 Virtual Standby 状态监视器上显示的字段的信息，请参阅Virtual Standby 状态监视器 (p. 88)。

4. 单击“关闭”可关闭“虚拟备用状态监视器”对话框。

从节点查看有关 Virtual Standby 作业的状态信息

CA ARCserve Central Virtual Standby 将 CA ARCserve D2D 恢复点转换为恢复点快照。您可以查看正在进行的转换作业的相关状态信息。

也可以从 Virtual Standby 服务器或直接从节点访问状态信息。有关如何从 Virtual Standby 服务器访问状态信息的信息，请参阅从 Virtual Standby 服务器查看有关 Virtual Standby 作业的状态信息 (p. 86)。

遵循这些步骤:

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”。

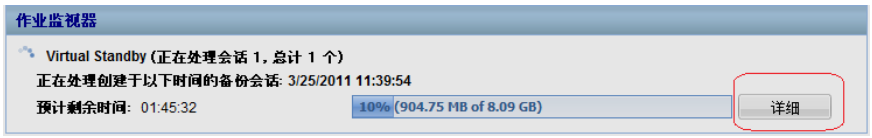
   您已登录到 CA ARCserve D2D 节点。

   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。

4. 单击“Virtual Standby”选项卡。

   此时打开“Virtual Standby 摘要”屏幕。

   如果存在正在运行的 Virtual Standby 作业，“作业监视器”字段中将显示一个状态对话框，如下图所示：

5. 单击“详细信息”将打开 Virtual Standby 状态监视器。

   注意：有关 Virtual Standby 状态监视器上显示的字段的信息，请参阅Virtual Standby 状态监视器 (p. 88)。

6. 单击“关闭”可关闭“虚拟备用状态监视器”对话框。

Virtual Standby 状态监视器

Virtual Standby 状态监视器将显示以下有关 Virtual Standby 作业的实时信息：

阶段

显示转换过程的当前阶段。

取消作业

使您可以终止转换作业。

正在处理

显示转换作业的整体进度，以及应用程序正在转换的恢复点的会话号。

当前配给点

显示有关应用程序正在转换的会话的状态信息。

源会话

指定应用程序正在转换的会话号。

开始时间

显示应用程序开始转换会话的日期和时间。

所用时间

显示自应用程序开始转换当前会话以来已用的时间长度。

吞吐量

显示应用程序转换会话的速率。

预计剩余时间

显示转换当前源会话的预计剩余时间长度。

全部会话

显示有关恢复点中应用程序正在转换的所有会话的状态信息。

已转换的会话数目

显示配给点中已转换的会话总数。

所用时间

显示自应用程序开始转换恢复点中包含的所有会话以来已用的时间长度。

预计剩余时间

显示转换恢复点中包含的所有会话的预计剩余时间。

未决会话数目

显示等待转换的会话数目。

查看分配给 CA ARCserve D2D 节点的策略的相关信息

该应用程序使您可以查看分配给 CA ARCserve D2D 节点的转换策略的相关信息。

查看分配给 CA ARCserve D2D 节点的策略的相关信息

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”。

   您已登录到 CA ARCserve D2D 节点。

   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。

4. 单击“Virtual Standby”选项卡。

   此时出现“Virtual Standby 摘要”屏幕。

5. 从“虚拟备用任务”列表中，单击“Virtual Standby 设置”。

   此时打开“Virtual Standby 设置”对话框。

   通过“Virtual Standby 设置”对话框，您可以查看分配给 CA ARCserve D2D 节点的策略中定义的“虚拟化服务器”、“虚拟机”、“替代服务器”以及“首选项”的相关信息。您无法在“Virtual Standby 设置”对话框中编辑分配给 CA ARCserve D2D 的策略。

   注意：有关如何编辑策略的信息，请参阅编辑策略。

6. 单击“取消”可关闭“Virtual Standby 设置”对话框。

Virtual Standby 设置

“Virtual Standby 设置”对话框包含分配给节点的策略的相关信息。您无法在该对话框中编辑策略。有关详细信息，请参阅编辑策略。

此时“Virtual Standby”选项卡上出现下列选项：

虚拟化服务器选项

- **VMware 系统：**

  下列选项应用于 VMware 系统：

  - **虚拟化类型 --** VMware。
  - **ESX 主机/Virtual Center** - 标识 ESX 或 vCenter Server 系统的主机名。
  - **用户名 --** 标识登录 VMware 系统所需的用户名。
  - **密码 --** 标识登录 VMware 系统所需的用户名的密码。
  - **协议 --** 显示在源 CA ARCserve D2D 节点和监视器服务器之间使用的通信协议。
  - **端口 --** 标识用于在源服务器和监视器服务器之间传输数据的端口。

- **监控：**

  下列选项应用于 VMware 系统。

  - **监视器服务器 --** 标识监视源服务器的服务器的主机名。
  - **用户名 --** 标识登录监视器服务器所需的用户名。
  - **密码 --** 标识登录监视器服务器所需的用户名的密码。
  - **协议 --** 标识在 CA ARCserve Central Virtual Standby 服务器和 ESX Server 系统（监视器服务器）之间使用的通信协议。
  - **端口 --** 标识用于在 CA ARCserve Central Virtual Standby 服务器和 ESX Server 系统（监视器服务器）之间传输数据的端口。
  - **将监视器服务器用作数据传输的代理 --** 标识监视器服务器将转换数据从 CA ARCserve D2D 源服务器复制到 ESX Server 数据存储。

    注意：默认情况下，“将监视器服务器用作数据传输的代理”选项被启用。您可以禁用该选项，以允许 CA ARCserve D2D 源服务器将转换数据直接复制到 ESX 服务器存储。

- **Hyper-V 系统：**

  下列选项应用于 Hyper-V 系统：

  - **虚拟化类型 --** Hyper-V。
  - **Hyper-V 主机名 --** 标识 Hyper-V 系统的主机名。
  - **用户名 --** 标识登录 Hyper-V 系统所需的用户名。
  - **密码 --** 标识登录 Hyper-V 系统所需的用户名的密码。
  - **端口 --** 标识用于在源服务器和监视器服务器之间传输数据的端口。

虚拟机选项

- **VMware 系统：**
  - **VM 名称前缀 --** 标识为 ESX Server 系统上虚拟机的显示名称添加的前缀。

    默认值：CAVM_
  - **VM 资源池 --** 标识备用虚拟机要进行分组的资源池的名称。
  - **删除存储 --** 标识要存储转换数据的位置。
    - **将一个数据存储用于所有虚拟机源磁盘 --** 表示应用程序将与虚拟机有关的所有磁盘复制到一个数据存储。
    - **为每个 VM 源磁盘选择数据存储 --** 表示应用程序将虚拟机的磁盘相关信息复制到对应的数据存储。
  - **网络 -** 标识 ESX Server 系统用于与虚拟机进行通信的 NIC、虚拟网络和路径。
    - **将所有虚拟 NIC 连接到以下虚拟网络 -** 标识映射到虚拟网络的虚拟 NIC。当虚拟机包含虚拟 NIC 和虚拟网络时，指定该选项。
    - **为每个虚拟 NIC 选择虚拟网络 -** 标识您想 NIC 用来进行通信的虚拟网络的名称。
  - **CPU 计数 --** 标识备用虚拟机支持的最小及最大 CPU 计数。
  - **内存 --** 标识为备用虚拟机分配的 RAM 总量 (MB)。

- **Hyper-V 系统：**
  - **VM 名称前缀 --** 标识为 Hyper-V 系统上虚拟机的显示名称添加的前缀。

    默认值：CAVM_
  - **路径 --** 标识要在 Hyper-v 服务器上存储转换数据的位置。
  - **网络 --** 标识 Hyper-V Server 用于与虚拟机进行通信的 NIC、虚拟网络和路径。
  - **CPU 计数 --** 标识备用虚拟机支持的最小及最大 CPU 计数。
  - **内存 --** 标识为备用虚拟机分配的 RAM 总量 (MB)。

替代设置

- **恢复：**
  - **手工启动虚拟机**—表示在源服务器失败或停止通信时手工打开和配给虚拟机。
  - **自动启动虚拟机 --** 表示在源服务器失败或停止通信时自动打开和配给虚拟机。
- **监控信号属性：**
  - **超时 -** 标识监视器服务器在打开恢复点快照之前必须等待监控信号的时间长度。
  - **频率 -** 标识源服务器将监控信号传递给监视器服务器的频率。

此时“首选项”选项卡上出现下列选项：

- **电子邮件报警：**
  - **源计算机缺失监控信号 --** 表示在监视器服务器未从源服务器检测到监控信号时，Virtual Standby 将发送报警通知。
  - **为配置成自动开机的源计算机打开的 VM --** 表示 Virtual Standby 打开已配置为在未检测到监控信号时自动开机的虚拟机时发送报警通知。
  - **配置成手工开机的源计算机缺失监控信号**—表示 Virtual Standby 从未配置为自动开机的源服务器检测到监控信号时发送报警通知。
  - **VM 存储可用空间少于 --** 标识 Virtual Standby 在定义的管理程序路径上检测到可用磁盘空间不足时将发送报警通知。可用磁盘空间量少于用户定义的阈值时，监测便会发生。可以将阈值定义为绝对值 (MB) 或卷容量的百分比。

- **Virtual Standby 错误/失败/崩溃 --** 表示 Virtual Standby 检测到在转换过程期间发生的错误时将发送报警通知。
- **Virtual Standby 成功**—表示创建 Virtual Standby 虚拟机的过程已成功完成。
- **无法连接到管理程序 --** 表示 Virtual Standby 检测到其无法与 ESX Server 系统或 Hyper-V 系统通信时将发送报警通知。
- **许可故障 --** 表示 Virtual Standby 在 Virtual Standby 服务器、源服务器和监视器服务器上检测到许可问题时将发送报警通知。
- **Virtual Standby 未成功从恢复点快照启动**—表示从恢复点快照创建 Virtual Standby 虚拟机的过程未成功完成。

从 Virtual Standby 服务器暂停和恢复 Virtual Standby 作业

虚拟转换是是一种 Virtual Standby 将来自源节点的 CA ARCserve D2D 恢复点转换成称作恢复点快照的虚拟机数据文件的过程。源节点出现故障时，Virtual Standby 使用恢复点快照打开该源节点的虚拟机。

作为最佳实践，允许虚拟转换过程持续运行。但是，如果要临时暂停本地和远程 Virtual Standby 服务器上的虚拟转换过程，可以从 Virtual Standby 服务器执行此操作。纠正源节点上的问题后，您可以恢复虚拟转换过程。

在您暂停 Virtual Standby 作业（转换作业）时，暂停操作不暂停当前正在进行的转换作业。暂停操作仅适用于预计在下一 CA ARCserve D2D 备份作业的结尾运行的作业。因此，直到明确地恢复（暂停）转换作业，下一转换作业才开始。

注意：也可以直接从节点暂停和恢复 Virtual Standby 作业。有关详细信息，请参阅从节点暂停和恢复 Virtual Standby 作业。

遵循这些步骤:

1. 登录到 Virtual Standby 服务器，并单击导航栏上的“节点”打开“节点”屏幕。
2. 执行以下任一操作来指定要暂停或恢复 Virtual Standby 作业的节点：
   - **节点级别：**单击包含要暂停或恢复的节点的组，然后单击要暂停或恢复的节点旁的复选框。
   - **组级别：**单击包含要暂停或恢复的节点的组。

3. 执行以下操作之一：

   - 单击工具栏上的“Virtual Standby”，然后在弹出式菜单中单击“暂停”或“恢复”临时暂停转换作业。

单击选定的组或单击节点，然后在弹出式菜单中单击“暂停 Virtual Standby”或“恢复 Virtual Standby”以恢复转换作业。

从节点暂停和恢复 Virtual Standby 作业

虚拟转换是是一种 Virtual Standby 将来自源节点的 CA ARCserve D2D 恢复点转换成称作恢复点快照的虚拟机数据文件的过程。源节点出现故障时，Virtual Standby 使用恢复点快照打开该源节点的虚拟机。

作为最佳实践，允许虚拟转换过程持续运行。但是，如果要临时暂停本地和远程 Virtual Standby 服务器上的虚拟转换过程，可以从 Virtual Standby 服务器执行此操作。纠正源节点上的问题后，您可以恢复虚拟转换过程。

在您暂停 Virtual Standby 作业（转换作业）时，暂停操作不暂停当前正在进行的转换作业。暂停操作仅适用于预计在下一 CA ARCserve D2D 备份作业的结尾运行的作业。因此，直到明确地恢复（暂停）转换作业，下一转换作业才开始。

注意：也可以从 Virtual Standby 服务器暂停和恢复 Virtual Standby 作业。有关详细信息，请参阅从 Virtual Standby 服务器暂停和恢复 Virtual Standby 作业。

遵循这些步骤:

1. 打开 Virtual Standby，然后单击导航栏上的“节点”以打开“节点”屏幕。
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，以便显示与指定组关联的所有节点。
3. 浏览并单击要暂停或恢复的节点，并从弹出菜单单击“登录 D2D”以打开 CA ARCserve D2D。
4. 单击“Virtual Standby”选项卡以打开“Virtual Standby 摘要”屏幕。
5. （可选）如果您登录到监视服务器，从“服务器”列表展开“全部”或“正运行的源”，然后单击要暂停或恢复其虚拟备用作业的节点。

   注意：如果 Virtual Standby 转换作业正在运行，将在 Virtual Standby 任务列表中显示“暂停 Virtual Standby”。如果 Virtual Standby 转换作业未运行，将在 Virtual Standby 任务列表中显示“恢复 Virtual Standby”。

6. 执行以下操作之一：

   - 单击“暂停 Virtual Standby”以临时暂停转换作业。

单击“恢复 Virtual Standby”以恢复转换作业。

从 Virtual Standby 服务器暂停和恢复监控信号

Virtual Standby 允许您暂停和恢复监视服务器检测到的监控信号。监控信号是源服务器和监视服务器就源服务器运行状况进行通信的过程。如果监视服务器在指定时间内未检测到监控信号，Virtual Standby 将配给虚拟机充当源节点。

示例：何时暂停或恢复监控信号

以下示例描述何时暂停和恢复监控信号：

- 在需要使节点（源服务器）脱机以进行维护时暂停监控信号。
- 在维护任务完成且节点（源服务器）联机时恢复监控信号。

请注意以下行为：

- 可以在组级别或单个节点级别暂停和恢复监控信号。
- 可以通过一个步骤为一个或多个节点暂停和恢复监控信号。
- 监控信号处于暂停状态时，CA ARCserve Central Virtual Standby 不打开恢复点快照。
- 在您升级源节点上的 CA ARCserve D2D 安装时，CA ARCserve Central Virtual Standby 暂停节点的监控信号。为了确保监视器服务器监视已升级的节点，请在节点上完成升级后恢复节点的监控信号。

注意：也可以从节点上的“Virtual Standby 摘要”屏幕暂停或恢复监控信号。有关详细信息，请参阅从节点暂停和恢复监控信号。

遵循这些步骤:

1. 登录 Virtual Standby 服务器。

   单击导航栏上的“节点”以打开“节点”屏幕。

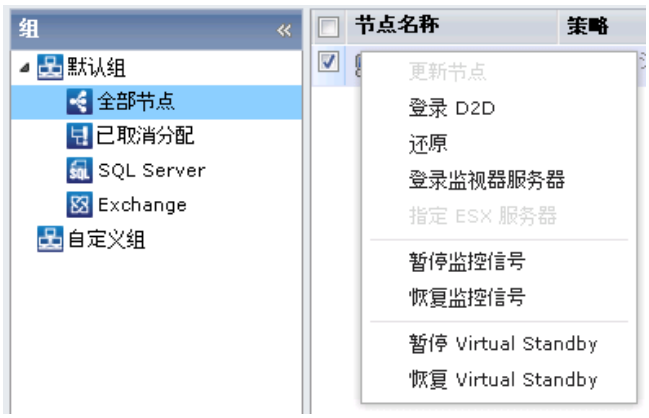
2. 执行以下任一操作来指定要暂停或恢复的节点：

   - **节点级别：**单击包含要暂停或恢复的节点的组，然后单击要暂停或恢复的节点旁的复选框。
   - **组级别：**单击包含要暂停或恢复的节点的组。

3. 然后执行以下任一操作来暂停或恢复监控信号：

   - 单击工具栏上的“监控信号”，然后在弹出式菜单中单击“暂停”或“恢复”，如以下屏幕中所示：

   - 右键单击选定的组或右键单击节点，然后在弹出式菜单中单击“暂停监控信号”或“恢复监控信号”，如以下屏幕中所示：



从节点暂停和恢复监控信号

Virtual Standby 允许您暂停和恢复监视服务器检测到的监控信号。监控信号是源服务器和监视服务器就源服务器运行状况进行通信的过程。如果监视服务器在指定时间内未检测到监控信号，Virtual Standby 将配给虚拟机充当源节点。

示例：何时暂停或恢复监控信号

以下示例描述何时暂停和恢复监控信号：

- 在需要使节点（源服务器）脱机以进行维护时暂停监控信号。
- 在维护任务完成且节点（源服务器）联机时恢复监控信号。

注意：也可以从 Virtual Standby 服务器上的“节点”屏幕暂停和恢复监控信号。有关详细信息，请参阅从 Virtual Standby 服务器暂停和恢复监控信号。

遵循这些步骤:

1. 登录 Virtual Standby 服务器。

   单击导航栏上的“节点”以打开“节点”屏幕。

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. 浏览至并单击要暂停或恢复监控信号的节点，然后从弹出菜单单击“登录 D2D”。

   CA ARCserve D2D 打开。

4. 单击“Virtual Standby”选项卡。

   此时打开“Virtual Standby 摘要”屏幕。

5. （可选）如果您登录到监视服务器，从“服务器”列表展开“全部”或“服务器正运行”，然后单击监控信号要被暂停或恢复的节点。

   注意：如果监控信号正在运行，将在“虚拟转换”任务列表中显示“暂停监控信号”。如果监控信号未运行，“恢复监控信号”将显示在“虚拟转换”任务列表中。

6. 执行以下操作之一：

   - 如果监控信号正在运行，单击“暂停监控信号”以临时暂停监控信号，暂时。

     示例：您想使服务器脱机以执行维护任务。

   - 如果监控信号未运行（暂停），单击“恢复监控信号”以恢复监控信号。

     示例：维护任务完成，您想使服务器联机。

监控信号暂停或恢复。

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。

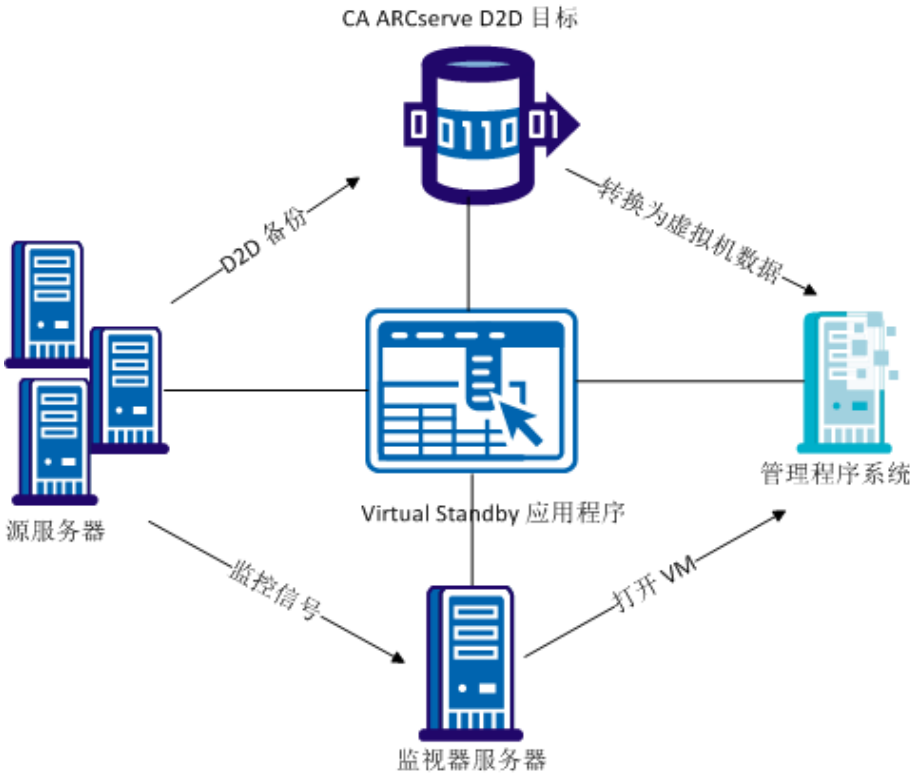
   注意：将协议更改为 HTTPS 时，Web 浏览器中会显示一则警告。出现此行为是由于自签名安全证书的缘故，用于提示您忽略该警告并继续操作，或者向浏览器添加该证书以阻止以后再次出现此警告。

第 6 章： 打开 Virtual Standby 虚拟机

此部分包含以下主题：

如何打开本地 Virtual Standby 虚拟机

此方案说明存储经理可以如何从 Virtual Standby 服务器暂停和恢复监控信号、从 Virtual Standby 服务器暂停和恢复虚拟转换过程、自动打开 Virtual Standby 计算机、如何在虚拟机打开后保护它们。



下表列出说明打开 Virtual Standby 计算机的任务的主题：

任务	参阅主题
在监视服务器无法从源服务器检测到监控信号时自动从恢复点快照打开 Virtual Standby 虚拟机。	[从恢复点快照打开 Virtual Standby 虚拟机](#) (p. 100)

任务	参阅主题
在 Virtual Standby 虚拟机开机之后保护它们。	在 Virtual Standby 虚拟机打开之后保护它们 (p. 103)

从恢复点快照打开 Virtual Standby 虚拟机

可以将 Virtual Standby 配置为在监视服务器未从源服务器检测到监控信号时，自动从恢复点快照打开 Virtual Standby 虚拟机。或者，使用 Virtual Standby，您可以在源服务器失败，发生紧急情况，或需要使源节点脱机以进行维护时，手动从恢复点快照打开 Virtual Standby 虚拟机。

注意：下列步骤描述如何手动从恢复点快照打开 Virtual Standby 虚拟机。有关如何让 Virtual Standby 自动打开恢复点快照的信息，请参阅创建 CA ARCserve Central Virtual Standby 策略 (p. 36)。

遵循这些步骤:

1. 打开 Virtual Standby，然后单击导航栏上的“节点”以打开“节点”屏幕。
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. 浏览至您要从恢复点快照打开的节点并单击该节点，然后单击“操作”工具栏上的“备用 VM”。

   “恢复点快照”对话框打开。
4. 在“恢复点快照”对话框上，选择以下选项之一：
   - 选择用于打开虚拟机的恢复点快照的日期和时间范围。

   或者
   - 选择“打开带有自定义网配置的备用虚拟机”复选框打开“备用 VM 网络配置”对话框。

     注意：如果尚未配置备用虚拟机，则会显示链接“未配置备用虚拟机网络。”。单击此链接配置网络。

   单击“保存”。针对 Virtual Standby 虚拟机的设置即被保存。

   单击“关闭”，“恢复点快照”对话框出现。

   单击“打开 VM”。

将使用包含在恢复点快照内的数据打开虚拟机。

注意：在虚拟机开机之后，可能会一次或多次提示您重新启动计算机。该行为发生的原因是因为 VMware 在虚拟机上安装了 VMware 工具，或者 Windows Hyper-V 在虚拟机上安装了集成服务。

从恢复点快照打开 Virtual Standby 虚拟机之后，您可能需要完成以下任务：

- 激活正在虚拟机上运行的 Windows 操作系统。
- 启动虚拟机上的 CA ARCserve D2D 备份。

  注意：有关使用 CA ARCserve Central Protection Manager 创建和分配 CA ARCserve D2D 备份策略的信息，请参阅《*CA ARCserve Central Protection Manager 用户指南*》。
- 使用主机名、IP 地址以及虚拟机的登录凭据更新 CA ARCserve Central Virtual Standby。
- 将节点分配给策略。

注意：仅当您想为打开的虚拟机创建恢复点快照时，才需要执行该任务。有关详细信息，请参阅将节点分配给策略 (p. 46)。

从 Hyper-V Manager 打开 Virtual Standby 虚拟机

需要手动打开 Virtual Standby 虚拟机时，最佳实践是从 CA ARCserve D2D 服务器上的“Virtual Standby”屏幕打开虚拟机。有关详细信息，请参阅从恢复点快照打开 Virtual Standby 虚拟机。但是，如果需要从 Hyper-V 服务器启动 Virtual Standby 虚拟机，那么可以使用 Hyper-V Manager 进行启动。

注意：使用 Hyper-V Manager，您可以访问 CA ARCserve Central Virtual Standby 创建的用于保护节点的恢复点快照。请不要删除这些快照。删除这些快照之后，下次 Virtual Standby 运行时，包含在这些快照内的数据之间的关系会变得不一致。数据不一致的情况下，将无法正确打开 Virtual Standby 虚拟机。

从 Hyper-V Manager 打开 Virtual Standby 虚拟机

1. 登录到监视您正在保护的节点的 Hyper-V 服务器。
2. 通过执行下列操作来启动 Hyper-V Manager：

   依次单击“开始”、“所有程序”、“管理工具”、“Hyper-V Manager”。

   此时将打开 Hyper-V Manager。

3. 从“Hyper-V Manager”目录树，展开“Hyper-V Manager”，然后单击包含要打开的虚拟机的 Hyper-V 服务器。

   与指定的 Hyper-V 服务器相关联的虚拟机将显示在中心窗格的“虚拟机”列表中。

4. 执行以下操作之一：

   - **使用最新的快照打开虚拟机：**在“虚拟机”列表中，右键单击需要打开的虚拟机，然后单击弹出式菜单上的“启动”。
   - **使用较旧的快照打开虚拟机：**

     a. 在“虚拟机”列表中，单击需要打开的虚拟机。

        与虚拟机相关联的快照将显示在“快照”列表中。

     b. 右键单击需要使用其来打开虚拟机的快照，然后单击弹出式菜单上的“应用”。

        此时将打开“应用快照”对话框。

     c. 单击“应用”。

     d. 在“虚拟机”列表中，右键单击需要打开的虚拟机，然后单击弹出式菜单上的“启动”。

   此时将打开 Virtual Standby 虚拟机。

必要时，可以在打开虚拟机之后备份虚拟机并创建恢复点快照。有关详细信息，请参阅在打开 Virtual Standby 虚拟机之后要执行的任务。

从 VMware vSphere Client 打开 Virtual Standby 虚拟机

需要手动打开 Virtual Standby 虚拟机时，最佳实践是从 CA ARCserve D2D 服务器上的“Virtual Standby”屏幕打开虚拟机。有关详细信息，请参阅从恢复点快照打开 Virtual Standby 虚拟机。但是，如果需要从 ESX Server 或 vCenter Server 系统启动 Virtual Standby 虚拟机，那么可以使用 VMware vSphere Client 进行启动。

注意：使用 VMware vSphere Client，您可以访问 CA ARCserve Central Virtual Standby 创建的用于保护节点的恢复点快照。请不要删除这些快照。删除这些快照之后，下次 Virtual Standby 运行时，包含在这些快照内的数据之间的关系会变得不一致。数据不一致的情况下，将无法正确打开 Virtual Standby 虚拟机。

从 VMware vSphere Client 打开 Virtual Standby 虚拟机

1. 打开 VMware vSphere Client，并登录到监视您正在保护的节点的 ESX Server 或 vCenter Server 系统。

   从目录树，展开 ESX Server 系统或 vCenter Server 系统，找到并单击需要打开的虚拟机。

2. 执行以下操作之一：

   - **使用最新的快照打开虚拟机：**单击“入门”选项卡，然后单击位于屏幕底部的“打开虚拟机”。
   - **使用较旧的快照打开虚拟机：**

     a. 单击工具栏上的“Snapshot Manager”按钮。

     此时将打开与虚拟机名称对应的“快照”对话框，显示虚拟机的可用快照列表。

     b. 从快照列表中，单击需要使用其来打开虚拟机的快照，然后单击“转到”。

   此时将打开 Virtual Standby 虚拟机。

必要时，可以在打开虚拟机之后备份虚拟机并创建恢复点快照。有关详细信息，请参阅在打开 Virtual Standby 虚拟机之后要执行的任务。

在 Virtual Standby 虚拟机打开之后保护它们

（手动或自动）打开 Virtual Standby 虚拟机后，CA ARCserve D2D 备份作业和 Virtual Standby 作业将不按排定运行。要在 Virtual Standby 虚拟机打开后恢复作业，请执行以下操作：

1. 在 Virtual Standby 策略中修改 VM 名称前缀。

   在 CA ARCserve Central Virtual Standby 打开 Virtual Standby 虚拟机时，应用程序将已打开虚拟机的虚拟机名称定义为 Virtual Standby 策略中指定的“VM 名称前缀”选项与源计算机的主机名的组合。

示例：

- VM 名称前缀：AA_
- 源节点的主机名：Server1
- Virtual Standby 虚拟机的虚拟机名称：AA_Server1

在 Virtual Standby 虚拟机开机后，如果您未在 Virtual Standby 策略中修改 VM 名称前缀，则会发生虚拟机名称冲突。在源节点和 Virtual Standby 虚拟机在相同管理程序上时，便会发生该类问题。

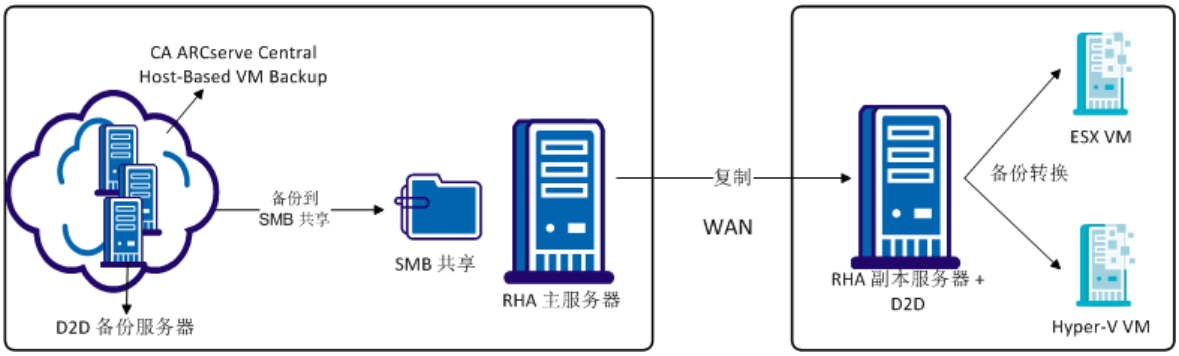
有关在 Virtual Standby 策略中修改 VM 名称前缀的信息，请参阅编辑策略 (p. 69)。必要时，您可以更新其他 Virtual Standby 策略设置。或者，您可以创建新的 Virtual Standby 策略来保护 Virtual Standby 虚拟机。有关创建新策略的信息，请参阅创建 CA ARCserve Central Virtual Standby 策略 (p. 36)。

2. 在您更新策略或创建新策略之后，将策略部署到 Virtual Standby 虚拟机。有关详细信息，请参阅部署策略 (p. 48)。
3. 在您将策略部署到 Virtual Standby 虚拟机之后，请恢复 Virtual Standby 作业。有关详细信息，请参阅暂停和恢复 Virtual Standby 作业。
4. 在您部署策略之后，请登录到 Virtual Standby 虚拟机上的 CA ARCserve D2D，然后为 CA ARCserve D2D 备份作业排定重复方式。有关详细信息，请参阅*《CA ARCserve D2D 用户指南》*。

注意：CA ARCserve Central Protection Manager 和 CA ARCserve Central Virtual Standby 具有一个机制，允许您每周自动将策略重新同步到受管 CA ARCserve D2D 节点。该机制允许 CA ARCserve Central Protection Manager 通过将 CA ARCserve D2D 节点上生效的策略重新部署到 Virtual Standby 虚拟机上，来重新启动 Virtual Standby 虚拟机上的备份作业。策略部署过程以此方式进行，是因为源节点和 Virtual Standby 虚拟机有相同主机名，这允许 CA ARCserve Central Protection Manager 重新同步策略。该行为的唯一限制是，CA ARCserve Central Protection Manager 服务器和 Virtual Standby 虚拟机必须能通过网络相互通信。在 CA ARCserve Central Protection Manager 将策略重新同步和部署到 Virtual Standby 虚拟机之后，您便可以恢复 Virtual Standby 虚拟机上的 Virtual Standby 作业。有关详细信息，请参阅暂停和恢复 Virtual Standby 作业。

如何打开远程 Virtual Standby 虚拟机

此方案说明存储经理可以充分利用和集成 CA ARCserve Replication 中已提供的功能，以便将 CA ARCserve D2D 和 CA ARCserve Central HostBased VM Backup 恢复点移至远程位置。此功能使 CA ARCserve Central Virtual Standby 能够转换这些复制的恢复点，并将它们自动注册到 Microsoft Hyper-V 或 VMware vCenter 或 ESXi。



下表列出说明打开 Virtual Standby 计算机的任务的主题：

任务	参阅主题
在源服务器出故障时，从复制的恢复点快照打开远程 Virtual Standby 虚拟机。	从恢复点快照打开远程 Virtual Standby 虚拟机 (p. 105)
在 Virtual Standby 虚拟机开机之后保护它们。	在 Virtual Standby 虚拟机打开之后保护它们 (p. 109)

从恢复点快照打开远程 Virtual Standby 虚拟机

可将 Virtual Standby 配置为，在源服务器出故障、紧急情况发生或使源节点脱机以进行维护时，从复制的恢复点快照打开 Virtual Standby 虚拟机。

注意：下列步骤说明如何从复制的恢复点快照打开远程 Virtual Standby 虚拟机。

遵循这些步骤:

1. 打开 Virtual Standby，然后单击导航栏上的“节点”以打开“节点”屏幕。
2. 从“组”列表，单击“全部节点”，或单击包含您要登录的 CA ARCserve D2D 或 CA ARCserve Central HostBased VM Backup 节点的组。

   节点列表显示与指定组关联的所有节点。

3. 浏览并单击从复制的恢复点创建的备用虚拟机节点，然后打开。从弹出式菜单单击以下选项之一：

   - **备用 VM 网络配置：**

     – 从“网络适配器设置”为每个网络适配器指定虚拟网络和 NIC （网络接口卡）以及 TCP/IP 设置。

     或者

     – 更新 DNS 服务器，以便根据“DNS 更新设置”选项卡的 TCP/IP 设置将客户从源计算机重定向到 Virtual Standby 虚拟机。

   - **备用 VM：**

     – 选择用于打开虚拟机的恢复点快照的日期和时间范围。

     或者

     – 选择“打开带有自定义网配置的备用虚拟机”复选框打开“备用 VM 网络配置”对话框。

       注意：如果尚未配置备用虚拟机，则会显示链接“未配置备用虚拟机网络。”。单击此链接配置网络。

   单击“保存”。

针对远程 Virtual Standby 虚拟机的设置即被保存。

注意：在虚拟机开机之后，可能会一次或多次提示您重新启动计算机。该行为发生的原因是因为 VMware 在虚拟机上安装了 VMware 工具，或者 Windows Hyper-V 在虚拟机上安装了集成服务。

从恢复点快照打开远程 Virtual Standby 虚拟机之后，您可能需要完成以下任务：

- 激活正在虚拟机上运行的 Windows 操作系统。
- 启动虚拟机上的 CA ARCserve D2D 备份。

  注意：有关使用 CA ARCserve Central Protection Manager 创建和分配 CA ARCserve D2D 备份策略的信息，请参阅《*CA ARCserve Central Protection Manager 用户指南*》。

- 使用主机名、IP 地址以及虚拟机的登录凭据更新 CA ARCserve Central Virtual Standby。
- 将节点分配给策略。

  注意：仅当您想为打开的虚拟机创建恢复点快照时，才需要执行该任务。有关详细信息，请参阅将节点分配给策略 (p. 46)。

从 Hyper-V 管理器打开远程 Virtual Standby 虚拟机

要从 Hyper-V 服务器打开远程 Virtual Standby 虚拟机时，可以使用 Hyper-V 管理器打开。

注意：Hyper-V 管理器允许您访问 CA ARCserve 复制和高可用性 复制的且 CA ARCserve Central Virtual Standby 转换的恢复点快照以保护节点。请不要删除这些快照。删除这些快照之后，下次 Virtual Standby 运行时，包含在这些快照内的数据之间的关系会变得不一致。数据不一致的情况下，将无法正确打开 Virtual Standby 虚拟机。

遵循这些步骤:

1. 登录到监视您正在保护的节点的 Hyper-V 服务器。
2. 通过执行下列操作来启动 Hyper-V 管理器：

   单击“开始”，单击“所有程序”，单击“管理工具”，然后单击“Hyper-V 管理器”以打开 Hyper-V 管理器。
3. 从“Hyper-V 管理器”目录树，展开“Hyper-V 管理器”，然后单击包含要打开的虚拟机的 Hyper-V 服务器。

   与指定的 Hyper-V 服务器相关联的虚拟机将显示在中心窗格的“虚拟机”列表中。
4. 执行以下操作之一：
   - **使用最新的快照打开远程虚拟机：**在“虚拟机”列表中，右键单击需要打开的虚拟机，然后单击弹出式菜单上的“启动”。
   - **使用较旧的快照打开远程虚拟机：**
     a. 在“虚拟机”列表中，单击需要打开的虚拟机。

        与虚拟机相关联的快照将显示在“快照”列表中。

     b. 右键单击要用于打开远程虚拟机的快照，然后单击弹出式菜单上的“应用”以打开“应用快照”对话框。

     c. 单击“应用”。

     d. 在“虚拟机”列表中，右键单击需要打开的虚拟机，然后单击弹出式菜单上的“启动”。

   此时将打开远程 Virtual Standby 虚拟机。

必要时，可以在打开远程虚拟机之后备份远程虚拟机并创建恢复点快照。有关详细信息，请参阅在打开 Virtual Standby 虚拟机之后要执行的任务。

从 VMware vSphere Client 打开远程 Virtual Standby 虚拟机

如果需要从 ESX Server 或 vCenter Server 系统启动远程 Virtual Standby 虚拟机，那么可以使用 VMware vSphere Client 进行启动。

注意：VMware vSphere Client 允许您访问 CA ARCserve 复制和高可用性 复制的且 CA ARCserve Central Virtual Standby 转换的恢复点快照以保护节点。请不要删除这些快照。删除这些快照之后，下次 Virtual Standby 运行时，包含在这些快照内的数据之间的关系会变得不一致。数据不一致的情况下，将无法正确打开 Virtual Standby 虚拟机。

遵循这些步骤:

1. 打开 VMware vSphere Client，并登录到监视您正在保护的节点的 ESX Server 或 vCenter Server 系统。

   从目录树，展开 ESX Server 系统或 vCenter Server 系统，找到并单击需要打开的虚拟机。

2. 执行以下操作之一：

   - **使用最新的快照打开远程虚拟机：**单击“入门”选项卡，然后单击位于屏幕底部的“打开远程虚拟机”。
   - **使用较旧的快照打开远程虚拟机：**

     a. 从 VMware vSphere Client，右键单击想要拍取快照的虚拟机的名称并选择“快照管理器”。此时将打开“<虚拟机名称>快照”对话框，显示远程虚拟机的可用快照列表。

     b. 从快照列表中，单击要用于打开远程虚拟机的快照，然后单击“转到”。

   此时将打开远程 Virtual Standby 虚拟机。

必要时，可以在打开虚拟机之后备份远程虚拟机并创建恢复点快照。有关详细信息，请参阅在打开 Virtual Standby 虚拟机之后要执行的任务。

在远程 Virtual Standby 虚拟机打开之后保护它们

打开远程 Virtual Standby 虚拟机后，CA ARCserve D2D 备份作业和 Virtual Standby 作业将不按排定运行。如果您想在远程 Virtual Standby 虚拟机打开后恢复作业，请执行以下操作：

1. 在 Virtual Standby 策略中修改 VM 名称前缀。

   在 CA ARCserve Central Virtual Standby 打开远程 Virtual Standby 虚拟机时，应用程序将已打开远程虚拟机的虚拟机名称定义为 Virtual Standby 策略中指定的“VM 名称前缀”选项与源计算机的主机名的组合。

   示例：

   - VM 名称前缀：AA_
   - 源节点的主机名：Server1
   - Virtual Standby 虚拟机的虚拟机名称：AA_Server1

   在远程 Virtual Standby 虚拟机开机后，如果您未在 Virtual Standby 策略中修改 VM 名称前缀，则会发生虚拟机名称冲突。在源节点和远程 Virtual Standby 虚拟机在相同管理程序上时，便会发生该类问题。

   有关在 Virtual Standby 策略中修改 VM 名称前缀的信息，请参阅编辑策略。必要时，您可以更新其他 Virtual Standby 策略设置。或者，您可以创建新的 Virtual Standby 策略来保护远程 Virtual Standby 虚拟机。有关创建新策略的信息，请参阅创建 CA ARCserve Central Virtual Standby 策略 (p. 36)。

2. 在您更新策略或创建新策略之后，将策略部署到远程 Virtual Standby 虚拟机。有关详细信息，请参阅部署策略 (p. 48)。

3. 在您将策略部署到远程 Virtual Standby 虚拟机之后，请恢复 Virtual Standby 作业。有关详细信息，请参阅暂停和恢复 Virtual Standby 作业 (p. 93)。

4. 在您部署策略之后，请登录到远程 Virtual Standby 虚拟机上的 CA ARCserve D2D，然后为 CA ARCserve D2D 备份作业排定重复方式。有关详细信息，请参阅 *《CA ARCserve D2D 用户指南》*。

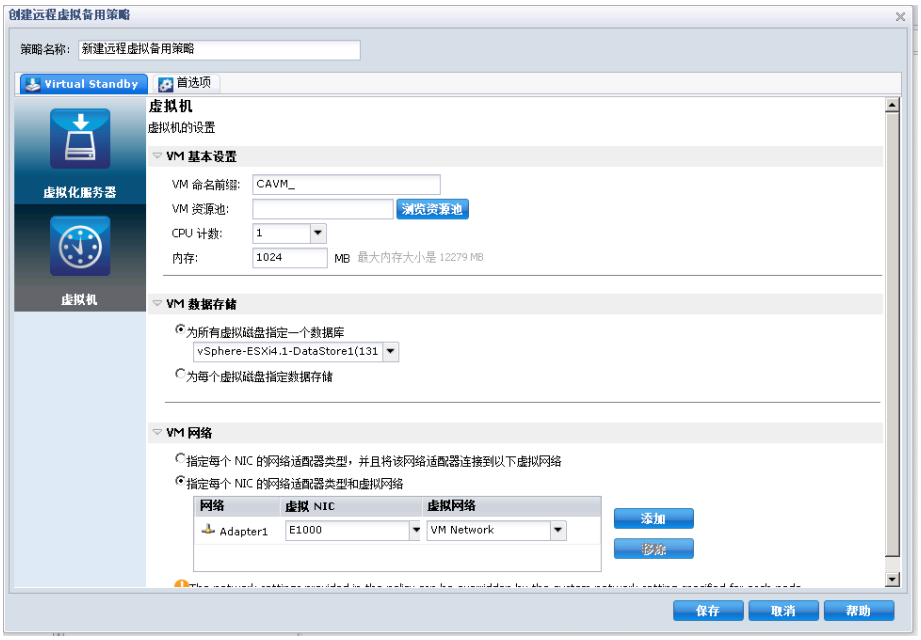
注意：CA ARCserve Central Protection Manager 和 CA ARCserve Central Virtual Standby 具有一个机制，允许您每周自动将策略重新同步到受管 CA ARCserve D2D 节点。该机制允许 CA ARCserve Central Protection Manager 通过将 CA ARCserve D2D 节点上生效的策略重新部署到远程 Virtual Standby 虚拟机上，来重新启动远程 Virtual Standby 虚拟机上的备份作业。策略部署过程以此方式进行，是因为源节点和远程 Virtual Standby 虚拟机有相同主机名，这允许 CA ARCserve Central Protection Manager 重新同步策略。该行为的唯一限制是，CA ARCserve Central Protection Manager 服务器和远程 Virtual Standby 虚拟机必须能通过网络相互通信。在 CA ARCserve Central Protection Manager 将策略重新同步和部署到远程 Virtual Standby 虚拟机之后，您便可以恢复远程 Virtual Standby 虚拟机上的 Virtual Standby 作业。有关详细信息，请参阅暂停和恢复 Virtual Standby 作业 (p. 93)。

应用程序确定要打开 NIC 的数量的方式

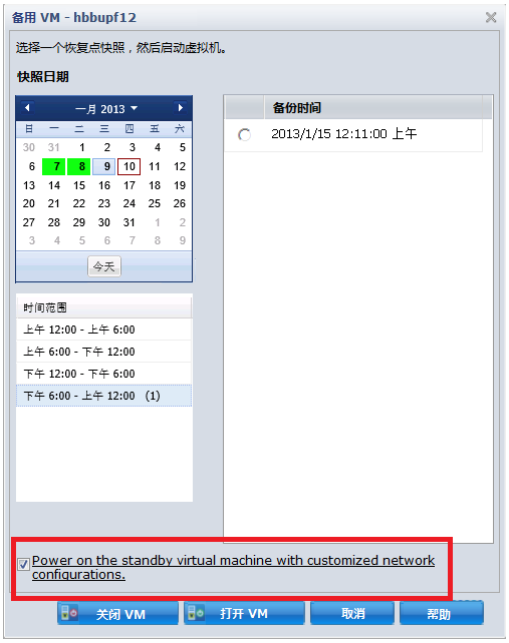
打开虚拟机时，Virtual Standby 基于是否配置了备用虚拟机网络，确定要打开的 NIC（网络接口卡）的数量。下表说明 Virtual Standby 如何确定打开备用虚拟机所需的 NIC 数量。

VM 网络在策略中定义的值	将*不*指定“打开带有自定义网配置的备用虚拟机”选项。	将*指*定“打开带有自定义网配置的备用虚拟机”选项。
定义的值与源计算机相同。	Virtual Standby 打开自上次备份作业起针对源计算机定义的 NIC 数量。	根据以下大量值 Virtual Standby 打开 NIC 数量： ■ 该数量已在自定义网络配置下定义。 ■ 自上次备份作业起针对源计算机定义的 NIC 数量。
定义的值是自定义值。	Virtual Standby 打开在策略中定义的自定义网络的数量。	根据以下大量值 Virtual Standby 打开 NIC 数量： ■ 该数量已在自定义网络配置下定义。 ■ 为自定义策略定义的 NIC 的数量。

以下对话框（编辑虚拟备用策略）说明定义包含要打开的 NIC 的自定义配置的策略的位置：



以下对话框（备用 VM - <主机名>）说明指定“打开带有自定义网配置的备用虚拟机”选项的位置：



如何保护打开的 Virtual Standby 虚拟机

（手动或自动）打开 Virtual Standby 虚拟机后，CA ARCserve D2D 备份作业和 Virtual Standby 作业将不按排定运行。要在 Virtual Standby 虚拟机打开后恢复作业，请执行以下操作：

1. 在 Virtual Standby 策略中修改 VM 名称前缀。

   在 CA ARCserve Central Virtual Standby 打开 Virtual Standby 虚拟机时，应用程序将已打开虚拟机的虚拟机名称定义为 Virtual Standby 策略中指定的“VM 名称前缀”选项与源计算机的主机名的组合。

   示例：

   - VM 名称前缀：AA_
   - 源节点的主机名：Server1
   - Virtual Standby 虚拟机的虚拟机名称：AA_Server1

   在 Virtual Standby 虚拟机开机后，如果您未在 Virtual Standby 策略中修改 VM 名称前缀，则会发生虚拟机名称冲突。在源节点和 Virtual Standby 虚拟机在相同管理程序上时，便会发生该类问题。

   有关在 Virtual Standby 策略中修改 VM 名称前缀的信息，请参阅编辑策略 (p. 69)。必要时，您可以更新其他 Virtual Standby 策略设置。或者，您可以创建新的 Virtual Standby 策略来保护 Virtual Standby 虚拟机。有关创建新策略的信息，请参阅创建 CA ARCserve Central Virtual Standby 策略 (p. 36)。

2. 在您更新策略或创建新策略之后，将策略部署到 Virtual Standby 虚拟机。有关详细信息，请参阅部署策略 (p. 48)。

3. 在您将策略部署到 Virtual Standby 虚拟机之后，请恢复 Virtual Standby 作业。有关详细信息，请参阅暂停和恢复 Virtual Standby 作业。

4. 在您部署策略之后，请登录到 Virtual Standby 虚拟机上的 CA ARCserve D2D，然后为 CA ARCserve D2D 备份作业排定重复方式。有关详细信息，请参阅 *《CA ARCserve D2D 用户指南》*。

注意：CA ARCserve Central Protection Manager 和 CA ARCserve Central Virtual Standby 具有一个机制，允许您每周自动将策略重新同步到受管 CA ARCserve D2D 节点。该机制允许 CA ARCserve Central Protection Manager 通过将 CA ARCserve D2D 节点上生效的策略重新部署到 Virtual Standby 虚拟机上，来重新启动 Virtual Standby 虚拟机上的备份作业。策略部署过程以此方式进行，是因为源节点和 Virtual Standby 虚拟机有相同主机名，这允许 CA ARCserve Central Protection Manager 重新同步策略。该行为的唯一限制是，CA ARCserve Central Protection Manager 服务器和 Virtual Standby 虚拟机必须能通过网络相互通信。在 CA ARCserve Central Protection Manager 将策略重新同步和部署到 Virtual Standby 虚拟机之后，您便可以恢复 Virtual Standby 虚拟机上的 Virtual Standby 作业。有关详细信息，请参阅暂停和恢复 Virtual Standby 作业。

第 7 章： 还原数据

此部分包含以下主题：

从 CA ARCserve D2D 恢复点还原数据

Virtual Standby 允许从可用的恢复点恢复数据。恢复点是 CA ARCserve D2D 源节点上的数据的时间点快照。从恢复点，您可以指定要恢复的数据。

从 CA ARCserve D2D 恢复点还原数据

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”。

   此时打开“浏览恢复点”对话框。

3. 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。必要时，输入用户名和密码凭据以获得该位置的访问权限。您可以单击绿色箭头验证图标，验证对源位置的访问权限是否适当。

   日历视图将突出显示（使用绿色）在显示的时间段内包含该备份源的恢复点的所有日期。

4. 指定要还原的数据。

   a. 选择您想还原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。

   b. 选择要还原的恢复点。

      将显示该恢复点的相应备份内容（包括任何应用程序）。

      注意：具有锁符号的时钟图标表示恢复点包含加密信息，可能需要密码才能还原。

   c. 选择要还原的内容。

      - 对于卷级还原，您可以指定还原整个卷或该卷内的选定文件或文件夹。
      - 对于应用程序级还原，您可以指定还原整个应用程序或该应用程序内的选定组件、数据库、实例等等。

5. 指定要还原的数据后，单击“下一步”。

   “还原选项”对话框随即打开。

6. 完成“还原选项”对话框上的以下选项：

   - **目标 --** 为还原选择目标。
     - 还原到原始位置 -- 允许您将数据从捕获备份映像的位置还原到原始位置。
     - 还原到 -- 允许您指定或浏览至将还原备份映像的位置。单击“还原至”字段旁边的箭头以验证与指定位置的连接。

       必要时，您将需要输入用户名和密码凭据来获得该位置的访问权限。

- **解决冲突 --** 允许您指定想要 CA ARCserve D2D 如何解决在还原过程中遇到的冲突。
  - 覆盖现有文件 -- 允许您覆盖（替换）位于还原目标的现有文件。所有对象将从备份文件中还原，而不论它们当前是否存在于您的计算机上。
  - 替换活动文件 -- 允许您在系统重新启动后替换活动文件。如果在还原尝试期间，CA ARCserve D2D 检测到现有文件当前正被使用，则它将不立即替换该文件，但为了避免任何问题，将推迟活动文件的替换，直到计算机下次重新启动后再替换。（还原将立即进行，但是任何活动文件的替换将在下一次系统重新启动过程中进行）。

    注意：如果未选中此选项，还原将跳过任何活动文件。
  - 重命名文件 -- 如果文件名已经存在，允许您创建新文件。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。数据便被还原到新文件。
  - 跳过现有文件 -- 让您跳过而非覆盖（替换）位于还原目标的任何现有文件。将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。

- **目录结构 --** 允许您指定 CA ARCserve D2D 在还原过程期间如何处理目录结构。
  - 创建根目录 -- 允许您指定如果在捕获的备份映像中不存在根目录结构，CA ARCserve D2D 将在还原目标路径上重新创建相同的根目录结构。

    当未选择（未选中）“创建根目录”选项时，要还原的文件/文件夹将直接还原到目标文件夹。

    示例：

    如果在备份期间，您捕获了文件“C:\Folder1\SubFolder2\A.txt”和“C:\Folder1\SubFolder2\B.txt”，并且在还原期间，您已将“D:\Restore”指定为还原目标。

    如果您选择单独还原“A.txt”和“B.txt”文件，则已还原文件的目标将是“D:\Restore\A.txt”和“D:\Restore\B.txt”（将不会重新创建指定文件层级之上的根目录）。

    如果您选择从“SubFolder2”层级还原，则已还原文件的目标将是“D:\Restore\SubFolder2\A.txt”和“D:\Restore\SubFolder2\B.txt”（将不会重新创建指定文件夹层级之上的根目录）。

    当选择（选中）“创建根目录”选项时，文件/文件夹的整个根目录路径（包括卷名称）将在目标文件夹中重新创建。如果要还原的文件/文件夹来自相同的卷名称，那么目标根目录路径将不包括卷名称。但是，如果要还原的文件/文件夹来自不同卷名称，那么目标根目录路径要包括卷名称。

    示例：

    如果在备份期间，您捕获文件“C:\Folder1\SubFolder2\A.txt”和“C:\Folder1\SubFolder2\B.txt”，以及“E:\Folder3\SubFolder4\C.txt”，并且在还原期间，您已指定“D:\Restore”为还原目标。

    如果您选择仅还原“A.txt”文件，还原文件的目标将是“D:\Restore\Folder1\SubFolder2\A.txt”（将重新创建没有卷名称的整个根目录）。

    如果您选择还原“A.txt”和“C.txt”文件，则还原文件的目标将是“D:\Restore\C\Folder1\SubFolder2\A.txt”和“D:\Restore\E\Folder3\SubFolder4\C.txt”（将重新创建具有卷名称的整个根目录）。

- **加密密码 --** 如果您尝试还原的恢复点数据被加密，您可能需要提供加密密码。

  如果您试图还原到以前执行该加密备份的相同计算机，则不需要密码。然而，如果您试图还原到不同的计算机，则需要密码。

  注意：下列图标表示恢复点是否包含加密的信息以及是否可能需要密码用于还原。

  未加密恢复点：

  加密的恢复点：

单击“下一步”。

“还原摘要”对话框将打开。

7. 验证“还原摘要”对话框中的信息是否正确。

   注意：如果想更改您指定的还原选项，请单击“上一步”回到相应对话框更改该值。

   单击“完成”。

将应用还原选项，数据将恢复。

从 CA ARCserve D2D 文件副本还原数据

Virtual Standby 允许您从 CA ARCserve D2D 文件副本恢复数据。文件副本是您复制到脱机存储（例如，磁盘或云）的 CA ARCserve D2D 恢复点的副本。在文件副本中您可以指定您想恢复的数据。

从 CA ARCserve D2D 文件副本还原数据

1. 登录到应用程序，并单击导航栏上的“节点”。

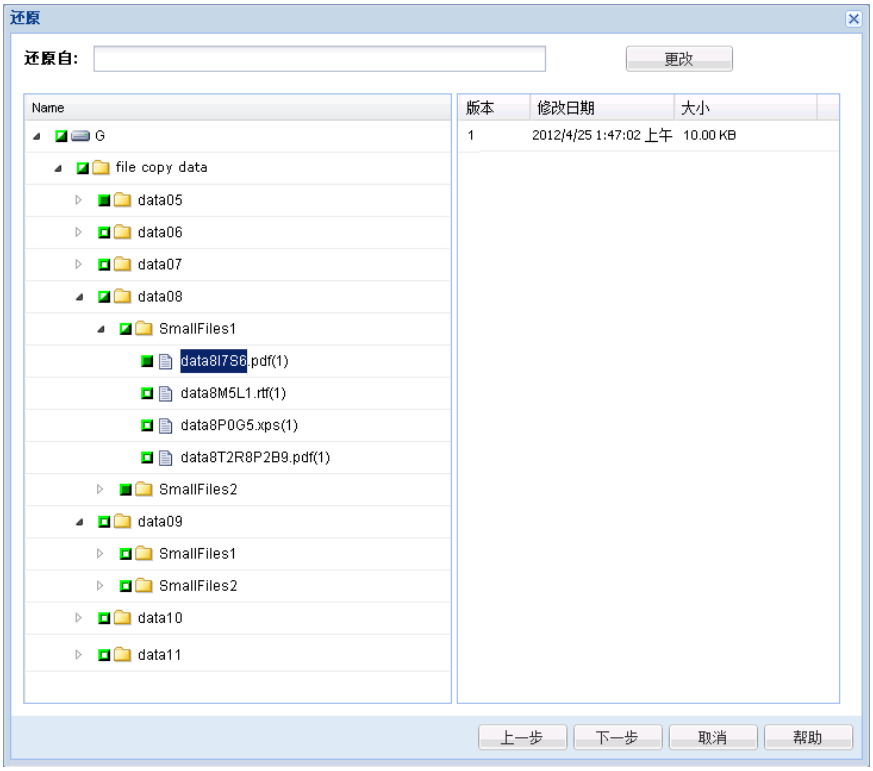
   在“节点”屏幕中，展开包含要还原的节点的组。

   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“浏览文件副本”。

   “浏览文件副本”对话框将打开，如下图所示。

   注意：在右侧窗格中当前显示的目标是默认目标。



3. 在“名称”窗格中指定您想恢复的文件副本数据。您可以指定文件和文件夹，或卷的任意组合。

   在您选择单个文件进行还原时，该文件的所有文件复制版本将显示在右侧窗格中。如果有多个版本，请选择您想恢复文件副本的版本。

   - **更改目标** -- 允许您浏览到存储文件副本映像的备用位置。

     将打开一个对话框，显示可用的备用目标选项。

   - **本地或网络驱动器** --“选择备份位置”对话框打开，允许您浏览至和选择其他本地或网络驱动器位置。
   - **云** --“云配置”对话框打开，允许您访问和选择备用云位置。

4. 单击“下一步”。

   “还原选项”对话框随即打开。

5. 完成“还原选项”对话框上的以下选项：

   - **目标** -- 为还原选择目标。
     - 还原到原始位置 -- 允许您将数据从捕获备份映像的位置还原到原始位置。
     - 还原到 -- 允许您指定或浏览至将还原备份映像的位置。单击“还原至”字段旁边的箭头以验证与指定位置的连接。

       必要时，您将需要输入用户名和密码凭据来获得该位置的访问权限。

- **解决冲突 --** 允许您指定想要 CA ARCserve D2D 如何解决在还原过程中遇到的冲突。
  - 覆盖现有文件 -- 允许您覆盖（替换）位于还原目标的现有文件。所有对象将从备份文件中还原，而不论它们当前是否存在于您的计算机上。
  - 替换活动文件 -- 允许您在系统重新启动后替换活动文件。如果在还原尝试期间，CA ARCserve D2D 检测到现有文件当前正被使用，则它将不立即替换该文件，但为了避免任何问题，将推迟活动文件的替换，直到计算机下次重新启动后再替换。（还原将立即进行，但是任何活动文件的替换将在下一次系统重新启动过程中进行）。

    注意：如果未选中此选项，还原将跳过任何活动文件。
  - 重命名文件 -- 如果文件名已经存在，允许您创建新文件。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。数据便被还原到新文件。
  - 跳过现有文件 -- 让您跳过而非覆盖（替换）位于还原目标的任何现有文件。将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。

- **目录结构 --** 允许您指定 CA ARCserve D2D 在还原过程期间如何处理目录结构。
  - 创建根目录 -- 允许您指定如果在捕获的备份映像中不存在根目录结构，CA ARCserve D2D 将在还原目标路径上重新创建相同的根目录结构。

    当未选择（未选中）“创建根目录”选项时，要还原的文件/文件夹将直接还原到目标文件夹。

    示例：

    如果在备份期间，您捕获了文件“C:\Folder1\SubFolder2\A.txt”和“C:\Folder1\SubFolder2\B.txt”，并且在还原期间，您已将“D:\Restore”指定为还原目标。

    如果您选择单独还原“A.txt”和“B.txt”文件，则已还原文件的目标将是“D:\Restore\A.txt”和“D:\Restore\B.txt”（将不会重新创建指定文件层级之上的根目录）。

    如果您选择从“SubFolder2”层级还原，则已还原文件的目标将是“D:\Restore\SubFolder2\A.txt”和“D:\Restore\SubFolder2\B.txt”（将不会重新创建指定文件夹层级之上的根目录）。

    当选择（选中）“创建根目录”选项时，文件/文件夹的整个根目录路径（包括卷名称）将在目标文件夹中重新创建。如果要还原的文件/文件夹来自相同的卷名称，那么目标根目录路径将不包括卷名称。但是，如果要还原的文件/文件夹来自不同卷名称，那么目标根目录路径要包括卷名称。

    示例：

    如果在备份期间，您捕获文件“C:\Folder1\SubFolder2\A.txt”和“C:\Folder1\SubFolder2\B.txt”，以及“E:\Folder3\SubFolder4\C.txt”，并且在还原期间，您已指定“D:\Restore”为还原目标。

    如果您选择仅还原“A.txt”文件，还原文件的目标将是“D:\Restore\Folder1\SubFolder2\A.txt”（将重新创建没有卷名称的整个根目录）。

    如果您选择还原“A.txt”和“C.txt”文件，则还原文件的目标将是“D:\Restore\C\Folder1\SubFolder2\A.txt”和“D:\Restore\E\Folder3\SubFolder4\C.txt”（将重新创建具有卷名称的整个根目录）。

- **加密密码 --** 如果您尝试还原的恢复点数据被加密，您可能需要提供加密密码。

  如果您试图还原到以前执行该加密备份的相同计算机，则不需要密码。然而，如果您试图还原到不同的计算机，则需要密码。

  注意：下列图标表示恢复点是否包含加密的信息以及是否可能需要密码用于还原。

  未加密恢复点：

  加密的恢复点：

单击“下一步”。

“还原摘要”对话框将打开。

6. 验证“还原摘要”对话框中的信息是否正确。

   注意：如果想更改您指定的还原选项，请单击“上一步”回到相应对话框更改该值。

   单击“完成”。

将应用还原选项，数据将恢复。

使用“查找要还原的文件/文件夹”还原数据

Virtual Standby 允许您在 CA ARCserve D2D 恢复点和文件副本中搜索要还原的特定文件或文件夹。

使用“查找要还原的文件/文件夹”还原数据

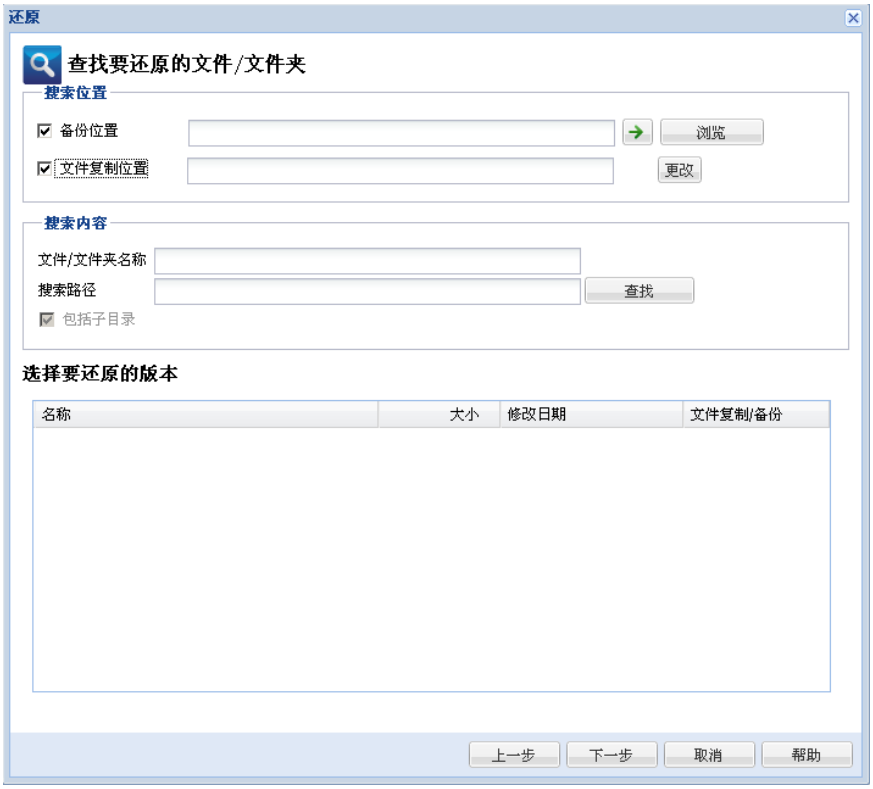
1. 登录到应用程序，并单击导航栏上的“节点”。

   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”。

   此时打开“查找要还原的文件/文件夹”对话框。



3. 指定搜索位置（备份和/或存档源）。

   您可以指定位置，或浏览至存储备份/存档映像的位置。必要时，输入用户名和密码凭据以获得该位置的访问权限。您可以单击绿色箭头验证图标，验证对源位置的访问权限是否适当。

4. 指定搜索内容（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。

   注意：必要时，您还可以指定一个路径，以进一步筛选您的搜索，然后选择是否包括或不包括子目录。

5. 单击“查找”以启动搜索。

   搜索的结果显示。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）。它还将指出是否已备份或存档被搜索文件。

6. 选择要还原的文件/文件夹版本（匹配项），然后单击“下一步”。

   “还原选项”对话框随即打开。

7. 完成“还原选项”对话框上的以下选项：

   - **目标 --** 为还原选择目标。
     - 还原到原始位置 -- 允许您将数据从捕获备份映像的位置还原到原始位置。
     - 还原到 -- 允许您指定或浏览至将还原备份映像的位置。单击“还原至”字段旁边的箭头以验证与指定位置的连接。

       必要时，您将需要输入用户名和密码凭据来获得该位置的访问权限。

- **解决冲突 --** 允许您指定想要 CA ARCserve D2D 如何解决在还原过程中遇到的冲突。
  - 覆盖现有文件 -- 允许您覆盖（替换）位于还原目标的现有文件。所有对象将从备份文件中还原，而不论它们当前是否存在于您的计算机上。
  - 替换活动文件 -- 允许您在系统重新启动后替换活动文件。如果在还原尝试期间，CA ARCserve D2D 检测到现有文件当前正被使用，则它将不立即替换该文件，但为了避免任何问题，将推迟活动文件的替换，直到计算机下次重新启动后再替换。（还原将立即进行，但是任何活动文件的替换将在下一次系统重新启动过程中进行）。

    注意：如果未选中此选项，还原将跳过任何活动文件。
  - 重命名文件 -- 如果文件名已经存在，允许您创建新文件。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。数据便被还原到新文件。
  - 跳过现有文件 -- 让您跳过而非覆盖（替换）位于还原目标的任何现有文件。将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。

- **目录结构 --** 允许您指定 CA ARCserve D2D 在还原过程期间如何处理目录结构。
  - 创建根目录 -- 允许您指定如果在捕获的备份映像中不存在根目录结构，CA ARCserve D2D 将在还原目标路径上重新创建相同的根目录结构。

    当未选择（未选中）“创建根目录”选项时，要还原的文件/文件夹将直接还原到目标文件夹。

    示例：

    如果在备份期间，您捕获了文件“C:\Folder1\SubFolder2\A.txt”和“C:\Folder1\SubFolder2\B.txt”，并且在还原期间，您已将“D:\Restore”指定为还原目标。

    如果您选择单独还原“A.txt”和“B.txt”文件，则已还原文件的目标将是“D:\Restore\A.txt”和“D:\Restore\B.txt”（将不会重新创建指定文件层级之上的根目录）。

    如果您选择从“SubFolder2”层级还原，则已还原文件的目标将是“D:\Restore\SubFolder2\A.txt”和“D:\Restore\SubFolder2\B.txt”（将不会重新创建指定文件夹层级之上的根目录）。

    当选择（选中）“创建根目录”选项时，文件/文件夹的整个根目录路径（包括卷名称）将在目标文件夹中重新创建。如果要还原的文件/文件夹来自相同的卷名称，那么目标根目录路径将不包括卷名称。但是，如果要还原的文件/文件夹来自不同卷名称，那么目标根目录路径要包括卷名称。

    示例：

    如果在备份期间，您捕获文件“C:\Folder1\SubFolder2\A.txt”和“C:\Folder1\SubFolder2\B.txt”，以及“E:\Folder3\SubFolder4\C.txt”，并且在还原期间，您已指定“D:\Restore”为还原目标。

    如果您选择仅还原“A.txt”文件，还原文件的目标将是“D:\Restore\Folder1\SubFolder2\A.txt”（将重新创建没有卷名称的整个根目录）。

    如果您选择还原“A.txt”和“C.txt”文件，则还原文件的目标将是“D:\Restore\C\Folder1\SubFolder2\A.txt”和“D:\Restore\E\Folder3\SubFolder4\C.txt”（将重新创建具有卷名称的整个根目录）。

- **加密密码 --** 如果您尝试还原的恢复点数据被加密，您可能需要提供加密密码。

  如果您试图还原到以前执行该加密备份的相同计算机，则不需要密码。然而，如果您试图还原到不同的计算机，则需要密码。

  注意：下列图标表示恢复点是否包含加密的信息以及是否可能需要密码用于还原。

  未加密恢复点：

  加密的恢复点：

单击“下一步”。

“还原摘要”对话框将打开。

8. 验证“还原摘要”对话框中的信息是否正确。

   注意：如果想更改您指定的还原选项，请单击“上一步”回到相应对话框更改该值。

   单击“完成”。

将应用还原选项，数据将恢复。

使用裸机恢复恢复源服务器

纠正这些问题或在源服务器上执行维护后，Virtual Standby 允许您将源服务器恢复到上次健康状态，并加入恢复点快照打开时发生的增量更改。

该恢复过程称作 V2P（虚拟到物理）恢复。

V2P 恢复过程利用 CA ARCserve D2D 裸机恢复 (BMR) 过程，将数据从虚拟机还原到物理计算机。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。

可以执行 BMR 之前，您必须有

- 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：如果您向动态磁盘执行 BMR，请不要执行任何 BMR 之前的磁盘操作（如清理或删除卷），否则可能无法识别磁盘是否存在。

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。

有关如何创建 ISO 或 BMR 优盘的详细信息，请参阅《CA ARCserve D2D 用户指南》中的“如何创建启动工具包”。

该应用程序让您可以使用下表中所述的方式恢复数据：

恢复方法	详细信息
从转换到基于 Hyper-V 的 Virtual Standby 虚拟机的数据恢复源服务器。	使用来自 Hyper-V Virtual Standby 虚拟机的数据恢复源服务器 (p. 135)。
从转换到基于 VMware 的 Virtual Standby 虚拟机的数据恢复源服务器。	使用来自 VMware Virtual Standby 虚拟机的数据恢复源服务器 (p. 140)。

管理 BMR 操作菜单

“BMR 操作”菜单包括以下三种类型的操作：

- 磁盘特定操作
- Volume/Partition 特定操作
- BMR 特定操作

磁盘特定操作

要执行磁盘特定操作，请选择磁盘标头，然后单击“操作”。

清理磁盘

此操作用于清理磁盘的所有分区并是：

- 删除磁盘的所有卷的备选方式。使用清理磁盘操作，您不必逐个删除每个卷。
- 用于删除非 Windows 分区。由于 VDS 限制，非 Windows 分区无法从 UI 删除，但是您可以使用此操作将其全部清除。

注意：在 BMR 期间，目标磁盘有非 Windows 分区或 OEM 分区时，您无法选择此分区并将其从 BMR UI 中删除。通常，如果曾在目标磁盘上安装了 Linux/Unix，将会发生。要解决该问题，请执行以下任务之一：

- 在 BMR UI 上选择磁盘标头，单击“操作”，使用“清理磁盘”操作擦除磁盘上的所有分区。
- 打开命令提示符并键入 Diskpart 以便打开 Diskpart 命令控制台。然后，键入“select disk x”（其中 'x 是磁盘数目），并键入“clean”以擦除磁盘上的所有分区。

转成 MBR

此操作用于将磁盘转换成 MBR（主引导记录）。只有在选定的磁盘是 GPT（GUID 分区表）磁盘且该磁盘上没有卷时才可用。

转成 GPT

此操作用于将磁盘转换成 GPT。只有在选定的磁盘是 MBR 磁盘且该磁盘上没有卷时才可用。

转成基本

此操作用于将磁盘转换成基本。只有在选定的磁盘是动态磁盘且该磁盘上没有卷时才可用。

转成动态

此操作用于将磁盘转换成动态磁盘。只有在选定的磁盘是基本磁盘时才可用。

使磁盘联机

此操作用于将磁盘联机。只有在选定的磁盘是在脱机状态时才可用。

磁盘属性

此操作用于查看详细的磁盘属性。它总是可用，且在选择此操作时，“磁盘属性”对话框出现。

Volume/Partition 特定操作：

要执行卷/分区操作，请选择磁盘主体区域，然后单击“操作”。从该菜单，您可以创建与源卷上的磁盘分区对应的新分区。

创建主分区

此操作用于在基本磁盘上创建分区。只有在选定区域是未分配的磁盘空间时才可用。

创建逻辑分区

此操作用于在基本 MBR 磁盘上创建逻辑分区。只有在选定区域是扩展分区时才可用。

创建扩展分区

此操作用于在基本 MBR 磁盘上创建扩展分区。只有在磁盘是 MBR 磁盘，且选定区域是未分配的磁盘空间时才可用。

创建系统保留分区

此操作用于在 BIOS 固件系统上创建系统保留的分区，并建立与源 EFI 系统分区的映射关系。只有在将 UEFI 系统还原到 BIOS 系统时才可用。

注意：如果以前已从 UEFI 转换成与 BIOS 兼容的系统，请使用“创建系统保留分区”操作来调整目标磁盘大小。

创建 EFI 系统分区

此操作用于在基本 GPT 磁盘上创建 EFI 系统分区。只有在目标计算机固件是 UEFI，且选定磁盘是基本 GPT 磁盘时才可用。

注意：如果以前已从 BIOS 转换成与 UEFI 兼容的系统，请使用“创建 EFI 系统分区”操作来调整目标磁盘大小。

注意：支持 UEFI 的系统还要求启动分区位于 GPT（GUID 分区表）磁盘上。如果要使用 MBR（主启动记录）磁盘，必须将该磁盘转换成 GPT 磁盘，然后使用“创建 EFI 系统分区”操作来调整磁盘大小。

改变卷大小

此操作用于调整卷大小。它是 Windows “扩展卷/压缩卷”的备选方式。只有在选定区域是有效磁盘分区时才可用。

删除卷

此操作用于删除卷。只有在选定区域是有效卷时才可用。

删除扩展分区

此操作用于删除扩展分区。只有在选定区域是扩展分区时才可用。

卷属性

此操作用于查看详细的卷属性。选择此操作时，“卷属性”对话框出现。

BMR 特定操作：

这些操作是针对 BMR 所特有。要执行 BMR 操作，请选择磁盘标头或磁盘主体区域，然后单击“操作”。

从以下位置映射磁盘

此操作用于建立源和目标动态磁盘之间的映射关系。只有在选定磁盘是动态磁盘时才可用。

注意：在映射到其他磁盘时，每一已映射目标卷的容量必须与对应源卷相同，或比其大。

从以下位置映射卷

此操作用于建立源和目标基本卷之间的映射关系。只有在选定的卷是基本卷时才可用。

注意：在映射到其他磁盘时，每一已映射目标卷的容量必须与对应源卷相同，或比其大。

提交

此操作总是可用。所有操作在内存中进行缓存，且不会修改目标磁盘，直到选择“提交”操作。

重置

此操作总是可用。重置操作用于放弃您的操作，并将磁盘布局还原为默认状态。此操作会清除所有缓存的操作。重置表示从配置文件和当前 OS 重新加载源和目标磁盘布局信息，并且丢弃任何用户更改的磁盘布局信息。

使用来自 Hyper-V Virtual Standby 虚拟机的数据恢复源服务器。

该应用程序使您可以使用转换到 Hyper-V Virtual Standby 虚拟机的 CA ARCserve D2D 数据恢复源服务器。

注意：该应用程序使用裸机恢复过程从 Hyper-V 虚拟机恢复源服务器。有关详细信息，请参阅使用裸机恢复恢复源服务器 (p. 130)。

通过 CA ARCserve D2D，可以执行 V2P（虚拟到物理）计算机的裸机恢复。该功能允许您从备用虚拟机的最新状态执行 V2P 恢复，从而帮助您减少生产计算机的损失。

选择“使用 Hyper-V 虚拟备用 VM 恢复”选项后，在返回到裸机恢复步骤以完成该过程之前，请执行下列步骤。

遵循这些步骤:

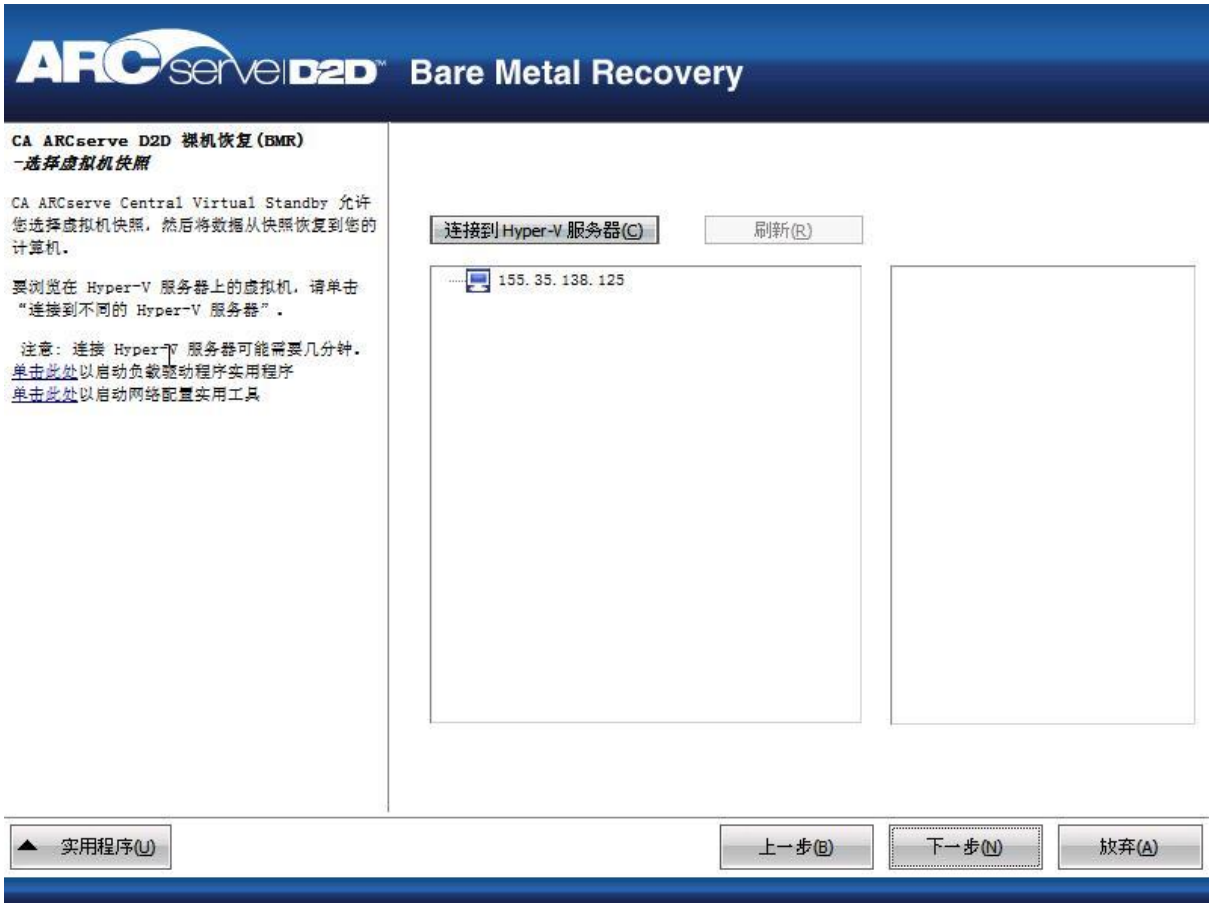
1. 从“选择裸机恢复 (BMR) 类型”向导屏幕，选择“使用 Hyper-V 虚拟备用 VM 恢复”选项。

2. 单击“下一步”。

   此时显示“选择虚拟机快照”屏幕，并显示“Hyper-V 身份验证”对话框，提示您输入 Hyper-v 服务器详细信息。

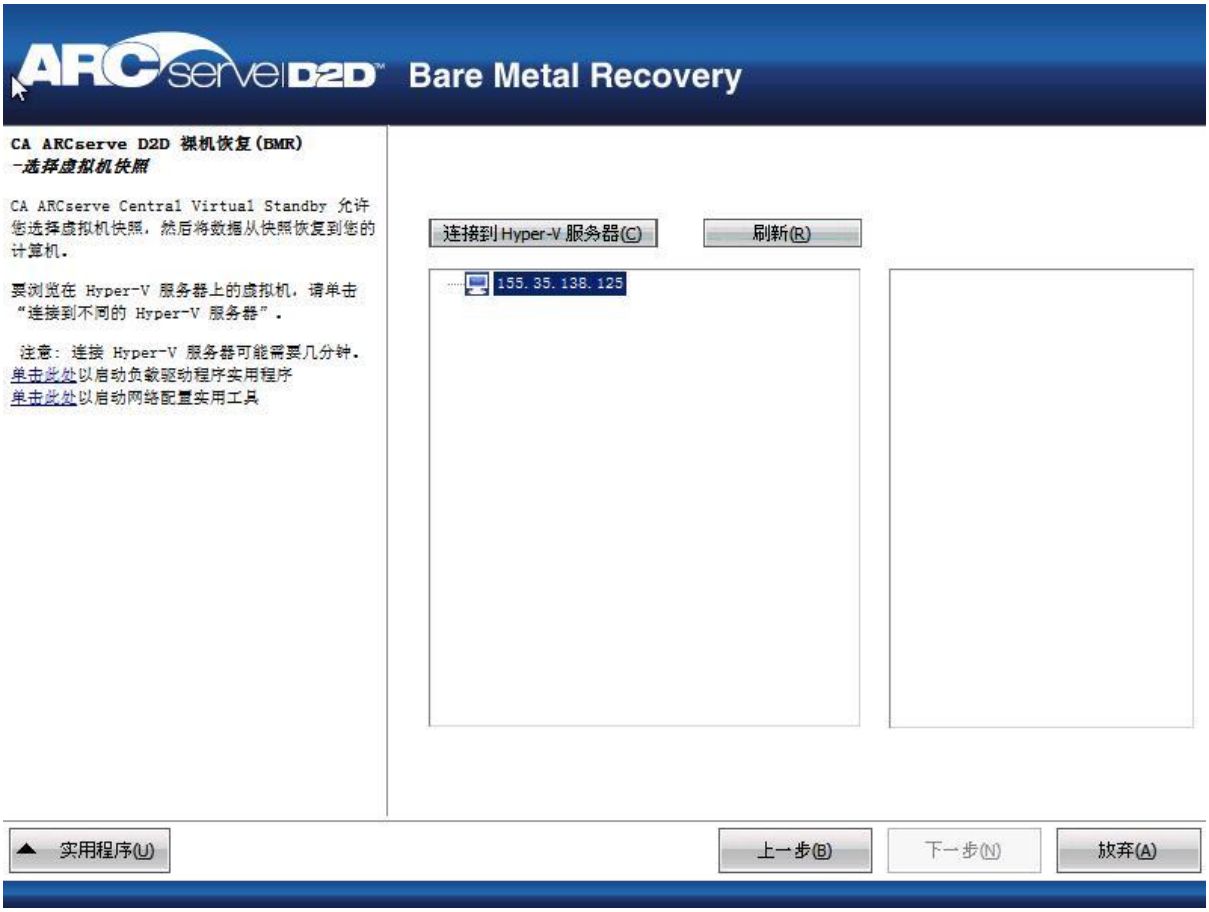
3. 输入身份验证信息，然后单击“确定”。

   CA ARCserve D2D 检测并显示 Hyper-V 服务器，后者具有使用 CA ARCserve Central Virtual Standby 转成指定 Hyper-V 服务器的所有虚拟机列表。



4. 选择包含您备份映像的恢复点快照的虚拟机。

   显示选定虚拟机的备份会话（恢复点快照）。



5. 选择要恢复的虚拟机备份会话（恢复点快照）。

   选定恢复点快照的相应详细信息（虚拟机名称、备份会话名称、已备份卷）显示在右侧窗格中。

   除选择一个所列恢复点之外，您还可以选择“当前状态”或“最新状态”恢复点。

   - 如果您正在恢复的虚拟机已开机，“当前状态”恢复点将显示。
   - 如果您正在恢复的虚拟机已关机，“最新状态”恢复点将显示。

     如果您选择“最新状态”恢复点，错误消息显示，通知您正在恢复的恢复点是最新（不是当前）状态，并要求您在继续恢复过程之前启动该虚拟机。

6. 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。

   请参阅执行裸机恢复以了解该过程的剩余步骤，并继续选择恢复模式的相应步骤。

使用来自 VMware Virtual Standby 虚拟机的数据恢复源服务器

该应用程序使您可以使用转换到 VMware Virtual Standby 虚拟机的 CA ARCserve D2D 数据恢复源服务器。

注意：该应用程序使用裸机恢复过程从 VMware 虚拟机恢复源服务器。有关详细信息，请参阅使用裸机恢复恢复源服务器 (p. 130)。

通过 CA ARCserve D2D，可以执行 V2P（虚拟到物理）计算机的裸机恢复。该功能允许您从备用虚拟机的最新状态执行 V2P 恢复，从而帮助您减少生产计算机的损失。

选择“使用 VMware 虚拟备用 VM 恢复”选项后，在返回到裸机恢复步骤以完成该过程之前，请执行下列步骤。

遵循这些步骤:

1. 从“选择裸机恢复 (BMR) 类型”向导屏幕，选择“使用 VMware 虚拟备用 VM 恢复”选项。

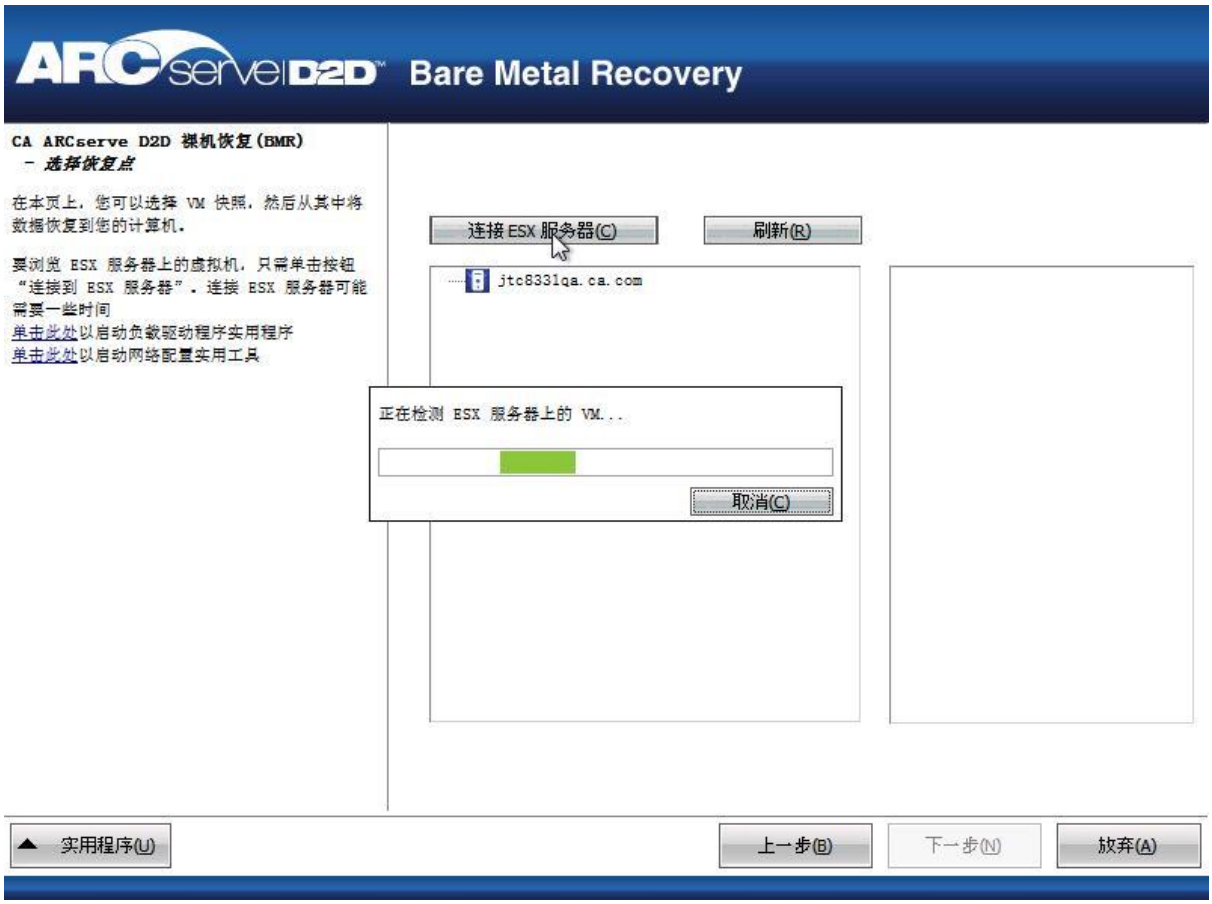
2. 单击“下一步”。

“选择恢复点”屏幕显示，并提供“ESX/VC 凭据”对话框。

3. 输入凭据信息，然后单击“确定”。

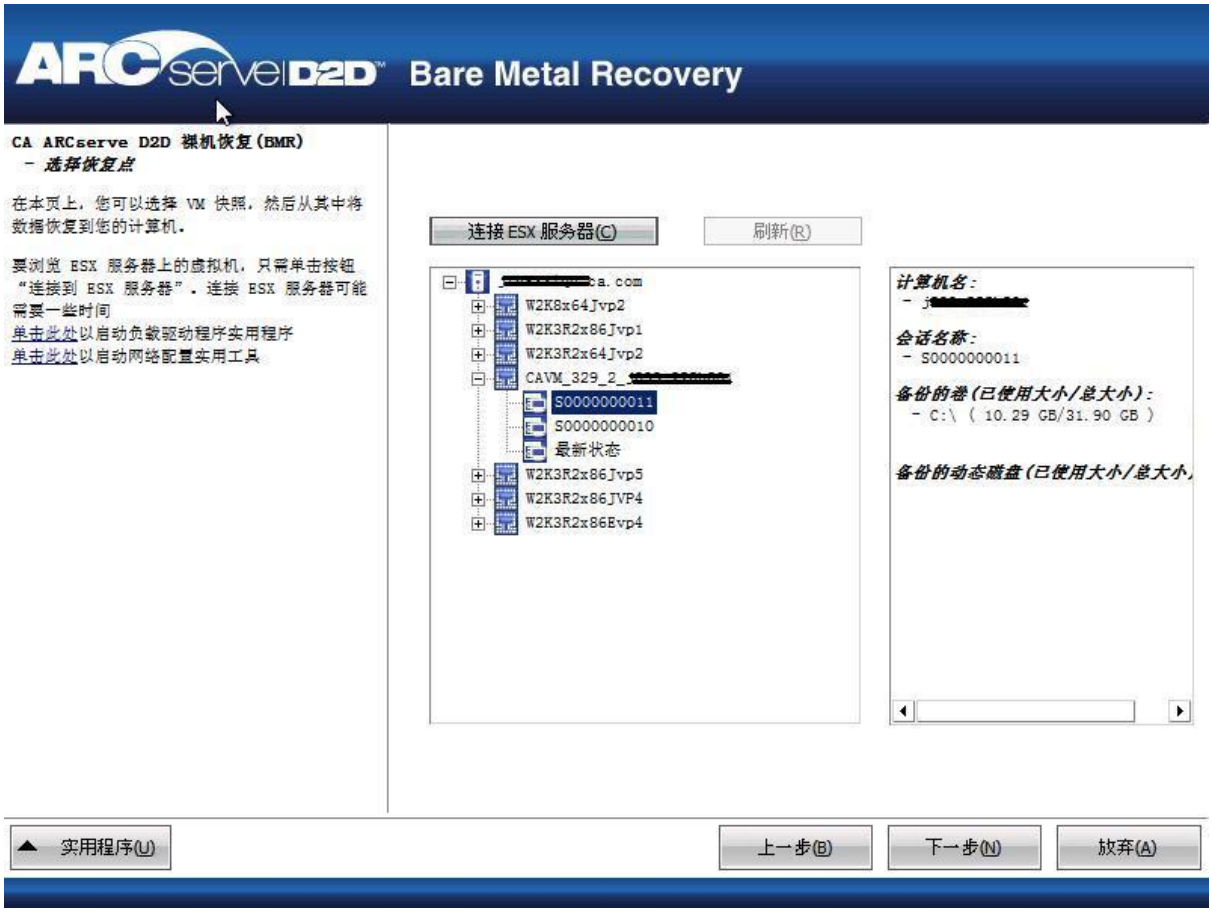
   “选择恢复点”屏幕显示。

   CA ARCserve D2D 便检索选定 VMware 服务器的所有恢复点快照，并在左侧窗格中显示 VMware 服务器，列出在选定 VMware 服务器上的所有虚拟机。



4. 选择包含备份映像的恢复点的虚拟机。

   显示选定虚拟机的备份会话（恢复点快照）。



5. 选择要恢复的虚拟机备份会话（恢复点快照）。

   选定恢复点快照的相应详细信息（虚拟机名称、备份会话名称、已备份卷、已备份动态磁盘）显示在右侧窗格中。

   除选择一个所列恢复点之外，您还可以选择“当前状态”或“最新状态”恢复点。

   - 如果您正在恢复的虚拟机已开机，“当前状态”恢复点将显示。
   - 如果您正在恢复的虚拟机已关机，“最新状态”恢复点将显示。

     如果您选择“最新状态”恢复点，错误消息显示，通知您正在恢复的恢复点是最新（不是当前）状态，并要求您在继续恢复过程之前启动该虚拟机。

6. 确认这是要还原的恢复点，然后单击“下一步”。

   BMR 向导屏幕显示可用恢复状态选项。

   请参阅执行裸机恢复以了解该过程的剩余步骤，并继续选择恢复模式的相应步骤。

还原 Microsoft Exchange 电子邮件

Virtual Standby 允许您从 CA ARCserve D2D 恢复点还原 Microsoft Exchange 数据。从恢复点，您可以恢复或还原邮箱、邮箱文件夹和个人电子邮件。

注意：要执行 Exchange 服务器数据的粒度还原，您的帐号必须有所需的访问权限。有关详细信息，请参阅*《CA ARCserve D2D 用户指南》*。

还原 Microsoft Exchange 电子邮件

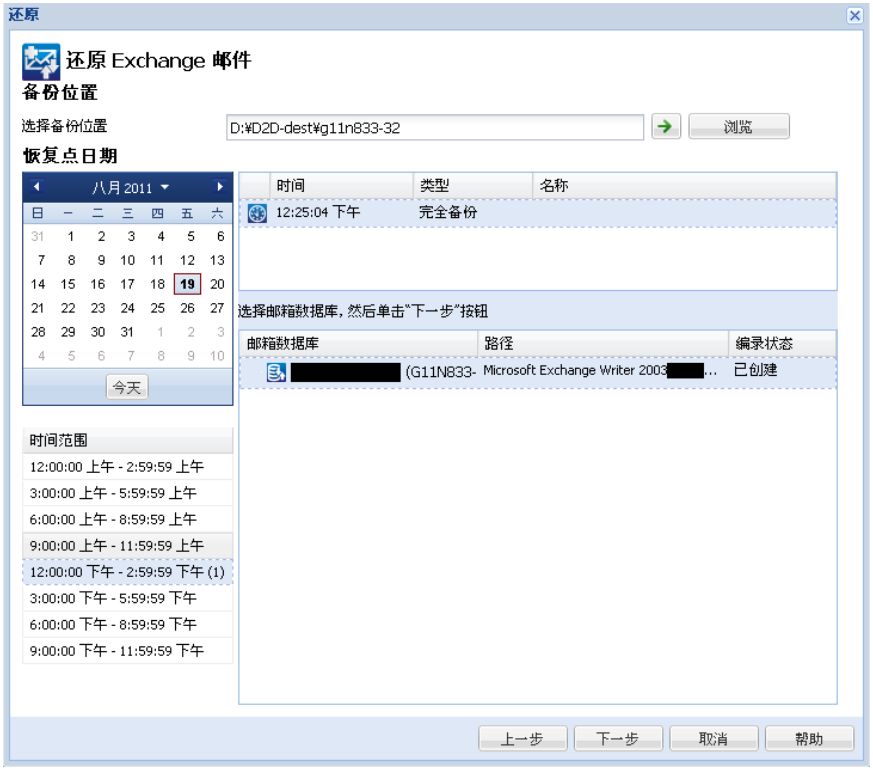
1. 登录到应用程序，并单击导航栏上的“节点”。

   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“还原 Exchange 邮件”。

   “还原 Exchange 邮件”对话框打开。



3. 指定备份位置。您可以指定一个位置或浏览到存储备份映像的位置。必要时，输入用户名和密码凭据以获得该位置的访问权限。您可以单击绿色箭头验证图标，验证对源位置的访问权限是否适当。

   日历视图将突出显示（使用绿色）在显示的时间段内包含该备份源的恢复点的所有日期。

4. 选择您想还原的备份映像的日历日期。

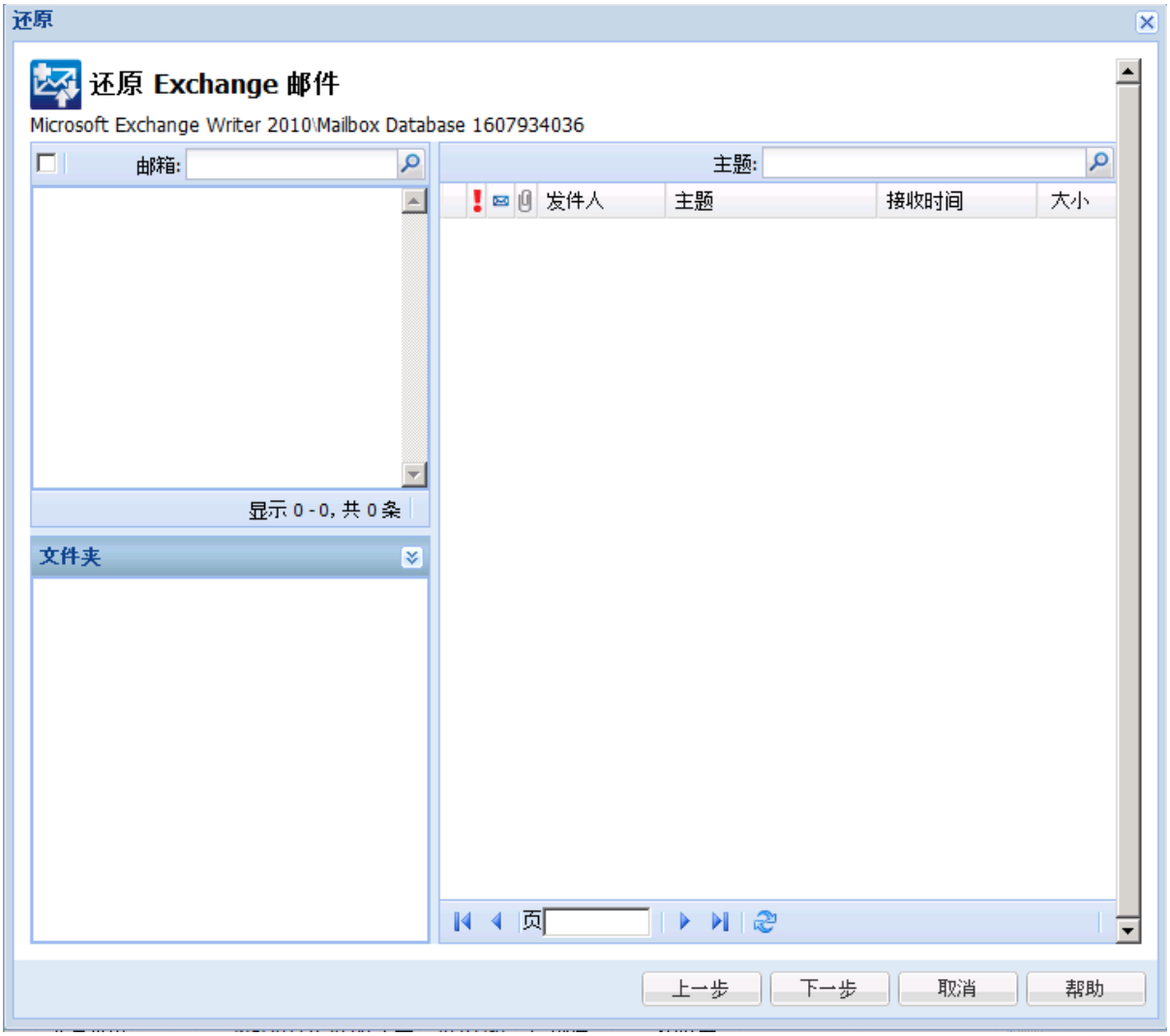
   将显示该日期的相应 Exchange 邮箱数据库，以及备份时间、执行的备份类型以及备份名称。

5. 选择要还原的 Exchange 邮箱数据库，然后单击“下一步”。

   注意：如果您在备份期间未启用“Exchange 粒度还原”选项（未生成编录），将显示通知消息，询问您是否要在此时生成 Exchange 粒度还原编录。如果选择“否”，不立即生成编录，则您将不能浏览至或选择粒度恢复点。因此，您将仅能从“浏览恢复点”还原对话框执行完全数据库还原。

   “还原 Exchange 邮件”对话框被更新，以显示选定数据库的邮箱内容列表。

   注意： Exchange 粒度还原仅支持电子邮件还原。不支持日历、联系人、便笺和任务还原。



6. 选择要还原的 Exchange 对象的层级（邮箱、文件夹或单个邮件）。

   您可以选择还原 Exchange 对象的整个内容或部分内容。您可以选择还原多个 Exchange 对象。

   注意： CA ARCserve D2D 不支持 Exchange 公共文件夹对象的粒度恢复。您需要使用“应用程序还原”恢复整个公共文件夹数据库，然后提取您需要的特定 Exchange 对象。

   注意： 使用 CA ARCserve D2D 从 Exchange 邮箱数据库还原单个邮箱/邮件对象时，用于还原的操作系统必须与在备份时所用的操作系统相同（包括相同的 Windows 版本号和 Service Pack 级别以及为支持它而需要的相关版本的 Visual C++ 可分发程序包）。

   注意： 从 CA ARCserve D2D UI 浏览和还原电子邮件的过程中，消息的“发件人”字段属性可能不会显示在从未登录到 Exchange 服务器的邮箱的 UI 中。然而，如果发生这种情况，电子邮件仍将得到正确还原。

   a. 您可以选择邮箱数据库。

      如果您选择邮箱数据库，将还原该数据库中的所有邮箱。

   b. 您可以选择邮箱（多个邮箱）进行还原。

      如果您选择邮箱级，将还原该邮箱中的所有相应内容（文件夹和单个邮件）。

   c. 您可以选择选定邮箱内的一个文件夹进行还原。

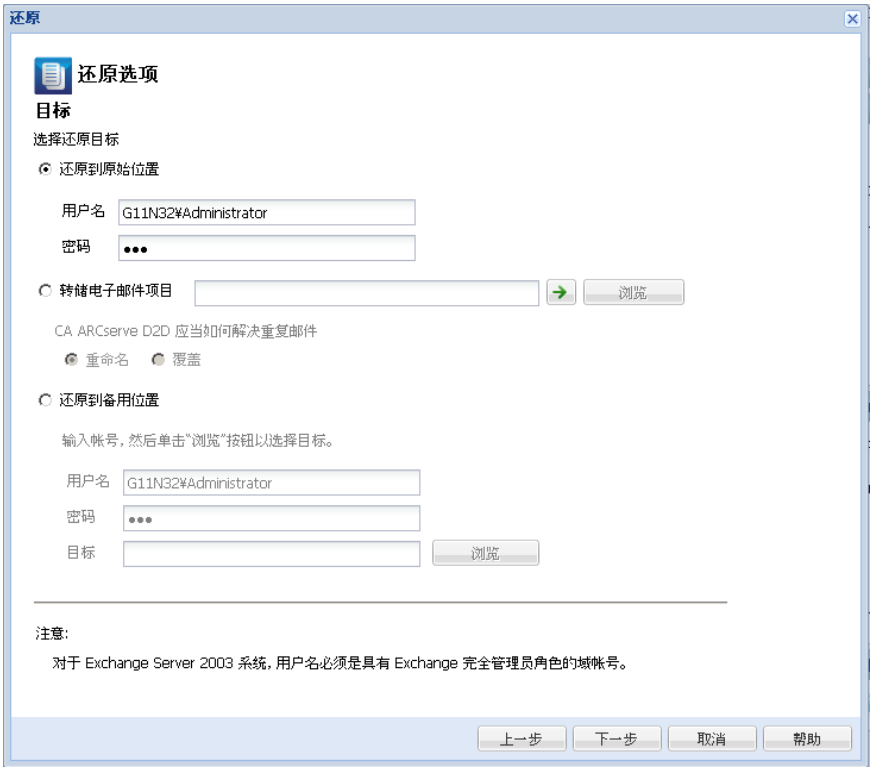
      如果您选择邮箱文件夹级，将还原该文件夹内的所有相应邮件内容。

   d. 您可以选择单个邮件进行还原。

      如果您选择单个邮件级，将仅还原选定邮件对象。

      注意： 对于 Exchange 2003，如果使用任何非 Outlook 的电子邮件客户端发送了要还原的单个邮件，并且该邮件在被备份时附有某种类型的标志状态标记，则该邮件本身会被还原，但是附着的标记不会被包含在还原的邮件中。

7. 指定要还原的 Exchange 对象后，单击“下一步”。



8. 为还原选择目标。

可用选项将还原到备份初始位置，或者还原到其他位置。

注意：对于 Exchange 2010，无法将存档的邮箱项目还原到原始位置。只能将存档的邮箱项还原到备用位置或本地磁盘。此外，无法将常规邮箱项目还原到存档邮箱。

还原到原始位置

将邮件还原到捕获备份映像的原始位置。邮件保持相同层次结构，并被还原到其原始邮箱和原始文件夹。

- 如果当前计算机不是活动的 Exchange 服务器，CA ARCserve D2D 将检测活动服务器的位置，然后将邮件还原到该活动的服务器。
- 如果邮箱已被移到其他 Exchange 服务器，但仍处于相同组织中，则 CA ARCserve D2D 会检测原始邮箱所在的新 Exchange 服务器，然后还原到该新服务器。
- 如果邮箱的显示名称已更改，将邮箱还原到原始位置（从早期的备份会话）的任何尝试将失败，因为 CA ARCserve D2D 将无法找到更改的名称。要解决该问题，您可以指定将该邮箱还原到备用位置。

注意：将邮箱或邮件还原到原始位置时，请确保目标邮箱可用，否则还原将失败。提交还原作业后，CA ARCserve D2D 仅验证目标。

仅转储文件

将邮件还原到磁盘。该磁盘位置可能是本地计算机，也可能是远程计算机。还原的邮件将保留与其在相应的 Exchange 邮箱中相同的层次结构。文件名将成为邮件的主题。

注意：如果邮件主题、文件夹名称或邮箱名称包含任何以下字符，字符在文件名中将被连字符 (-) 替换：\ / : * ？ " < > |

对于该选项，还需要指定您为解决冲突情况而想要 CA ARCserve D2D 执行的操作。在 Exchange 中，您在同一文件夹下可以有多个具有相同名称的邮件对象。但是，在文件系统中，具有相同名称的两个文件无法在同一文件夹下共存。

解决该冲突情况有两个选择：

- **重命名** - 如果在磁盘上有与邮件主题同名的文件，CA ARCserve D2D 将仍命名邮件主题，但是邮件主题结尾将附加数字。
- **覆盖** - 如果在磁盘上，具有配备与邮件主题同样的名称的文件，CA ARCserve D2D 将覆盖该文件。

注意：在您选择要还原到磁盘（转储）的单个邮件对象时，默认情况下还原邮件对象的格式将是 Outlook 邮件 (.MSG) 文件，而不是个人存储表 (.PST) 文件。

还原到备用位置

将邮件还原到指定位置，或允许您浏览至将还原备份映像的位置。目标必须是在相同 Exchange 组织中的邮箱，并且必需新的文件夹名称。（如果您正在尝试将邮件到还原备用位置，目标不能是公用文件夹）。

注意：将邮件还原到其他位置时，如果指定的目标文件夹已经存在，还原将继续。然而，如果指定的文件夹不存在，那么 CA ARCserve D2D 将首先创建文件夹，然后继续还原。

输入用户名和密码后，您可以单击“浏览”按钮以在当前组织中所有 Exchange 服务器、存储组、Exchange 数据库和邮箱的列表中导航。

选择任何邮箱作为目标。

9. 选择恢复选项后，单击“下一步”。

将显示“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，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。

    注意：Exchange 粒度还原的编录和还原作业正在进行时，备份会话将处于已挂接状态。不要在该挂接卷上执行任何操作（格式化、更改驱动器号、删除分区等）。

第 8 章： CA ARCserve Central Virtual Standby 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 Virtual Standby 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

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：

- 确认 Windows Server 服务正在 CA ARCserve Central Virtual Standby 服务器和源虚拟机（节点）上运行。
- 确认 Windows 防火墙例外应用于 CA ARCserve Central Virtual Standby 服务器和源虚拟机（节点）上的 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 Virtual Standby 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 Virtual Standby 服务器和源虚拟机（节点）上执行下列步骤。

  1. 登录到 CA ARCserve Central Virtual Standby 服务器，然后打开“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 Virtual Standby 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。

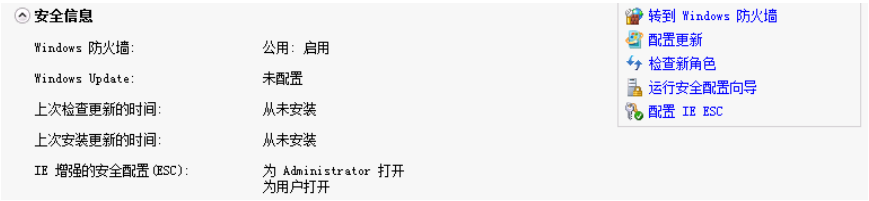
解决方案：

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。

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确工作。

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。

当登录到 CA ARCserve D2D 节点和监视器服务器时，网页加载不正确

在 Windows 平台上有效。

症状：

当从“节点”屏幕登录到 CA ARCserve D2D 节点和监视器服务器时，浏览器中的网页加载不正确、显示错误消息或者发生这两种情况。

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。

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。

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”。

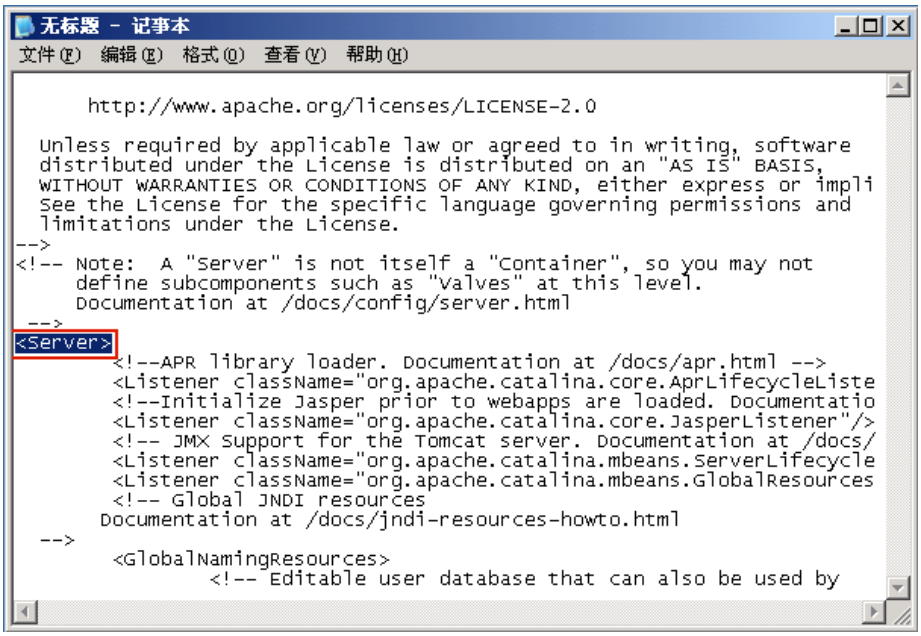
   CA ARCserve D2D Web Service 被停止。

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。



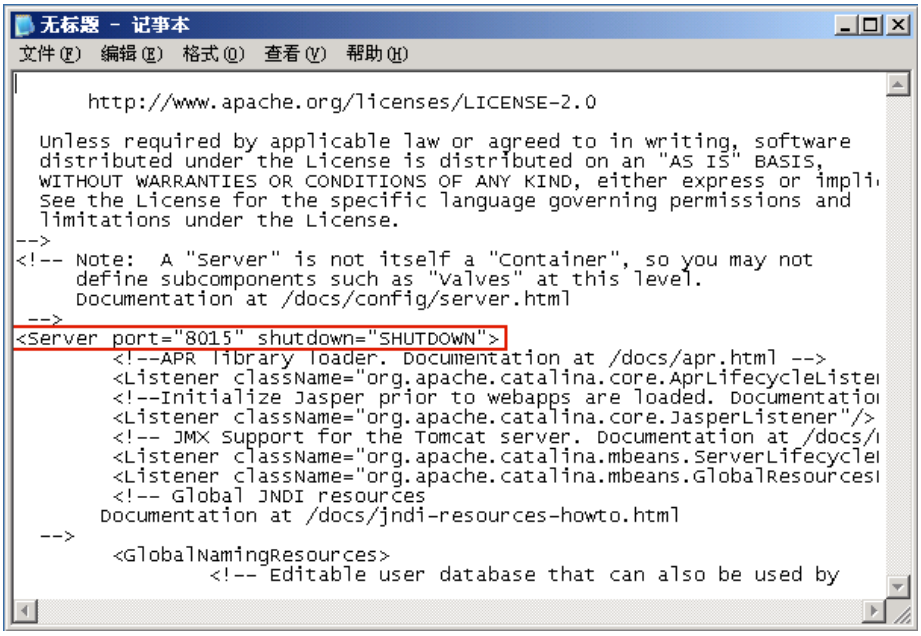
4. 按如下方式编辑 <Server> 标记：

从：

<Server>

到：

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



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 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-stder.*.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。

CA ARCserve Central Virtual Standby 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 Virtual Standby 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 Virtual Standby 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。

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

当添加节点时，无效凭据消息出现

Windows 平台上存在此问题。

症状：

在您尝试将节点添加到“节点”屏幕中时，以下消息出现：

无效凭据。

解决方案：

在以下情况下会发生此问题：

- 在“添加节点”对话框上指定的凭据不正确。
- 节点上的时间与在应用程序服务器上的时间不一样。

要解决此问题，请执行以下操作：

1. 登录到应用程序服务器，然后登录到应用程序。
2. 从主页上选择导航栏上的“节点”。

   “节点”屏幕将显示。
3. 从“节点”工具栏，单击“添加”，然后在弹出式菜单上单击“按照 IP/名称添加节点”。

   “按照 IP/名称添加节点”对话框打开。
4. 完成“按照 IP/名称添加节点”对话框上的以下字段：
   - **IP/节点名称** -- 允许您指定节点的 IP 地址或名称。
   - **说明** -- 允许您指定节点的描述。
   - **用户名**--允许您指定登录节点所需的用户名。
   - **密码** -- 指定登录节点所需的密码。

   单击“验证”。
5. 如果消息“无效凭据”出现，请执行以下操作：
   a. 确认您在“添加节点”对话框上指定了正确的证书，然后单击“验证”。
   b. 如果消息“无效凭据”出现，确认在应用程序服务器上的操作系统时间与节点上的操作系统时间一样。

      注意：操作系统时间可以处于不同时区。然而，操作系统时间不能是不同日期。特别是，要确认节点上的操作系统日期与应用程序服务器相比不晚于或早于一个公历日。

Windows XP 上的凭据无效消息

在运行 Windows XP 操作系统的计算机上有效。

症状：

在您从“节点”屏幕添加基于 Windows XP 的节点时，以下消息出现：

用户凭据无效。

解决方案：

在各种条件下，CA ARCserve Central Virtual Standby 都无法添加指定了 Windows“使用简单文件共享”文件夹选项的 Windows XP 节点。要解决此问题，请执行以下操作：

1. 登录到 Windows XP 节点，打开 Windows 资源管理器。
2. 在“工具”菜单中，单击“文件夹选项”。

   “文件夹选项”对话框将打开。
3. 单击“查看”，并滚动到“使用简单文件共享(推荐)”。
4. 清除“使用简单文件共享(推荐)”旁边的复选标记，然后单击“确定”。

   将禁用简单文件共享。
5. 登录到 CA ARCserve Central Virtual Standby 服务器，然后添加节点。

按照 IP/名称添加节点时发生拒绝访问错误

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：

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新 Windows 用户帐户从“按照 IP/名称添加节点”对话框中添加节点时，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。

结果导致您无法添加节点。

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：

禁用远程 UAC：

1. 单击“开始”，在“搜索程序和文件”字段中键入 regedit，然后按下 Enter 键，将打开 Windows 注册表编辑器。

   注意：您可能需要提供管理凭据才能打开 Windows 注册表编辑器。

2. 查找并单击以下注册表项：

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. 从“编辑”菜单，单击“新建”，然后单击 DWORD（32 位）值。
4. 指定 LocalAccountTokenFilterPolicy 作为新条目的名称，然后按下 Enter 键。
5. 右键单击 LocalAccountTokenFilterPolicy，然后单击“修改”。
6. 在“值数据”字段中指定 1，然后单击“确定”。
7. 退出注册表编辑器。

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。

更改节点名称后，节点屏幕中不显示该节点

在 Windows 平台上有效。

症状：

将节点添加到“节点”屏幕之后，该节点的主机名有所更改。该节点不再出现在“节点”屏幕上。

解决方案：

此现象是正常的。当从“节点”屏幕添加节点时，CA ARCserve Central Virtual Standby 保留该节点的名称。当重命名节点时，Virtual Standby 无法检测到该节点。因此，该节点不出现在“节点”屏幕上。

要在“节点”屏幕上显示重命名的节点，请执行以下操作：

1. 重命名节点。
2. 打开“节点”屏幕，然后删除重命名的节点 (p. 61)。
3. 使用其新名称添加该节点 (p. 29)。

发生未找到操作系统错误

Windows 平台上存在此问题。

症状：

打开 Virtual Standby 虚拟机操作失败时，将显示以下消息：

未找到操作系统。

解决方案：

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，请更新已恢复虚拟机上的 BIOS 以与源的 BIOS 匹配。

注意：请使用 (0:1) 来代表第一个 IDE 磁盘。

针对 Hyper-V 系统的 Virtual Standby 作业失败

在 Windows 系统上有效。

症状：

针对 Hyper-V 系统，Virtual Standby 作业失败。下列消息显示在活动日志中：

```
Virtual Standby 作业无法获取 Hyper-V VM。
```

解决方案：

Virtual Standby 作业在下列条件下失败：

- Virtual Standby Web 服务无法从 Hyper-V 系统检索有关虚拟机的信息。在 Hyper-V 系统上未运行必需的 Hyper-V 服务时，CA ARCserve Central Virtual Standby 服务器和 Hyper-V 系统之间会出现通信问题。

  解决方案：确认所有必需的 Hyper-V 服务都在 Hyper-V 系统上运行。

- Hyper-V 系统包含的可用磁盘空间数量不足以创建 Virtual Standby 虚拟机，或创建 Virtual Standby 虚拟机的快照。

  解决方案：考虑重新配置 Hyper-V 系统，以允许系统卷中存在更多可用磁盘空间。

注意：如果发现其他可能原因，请与 CA 支持联系。

由于内部错误，Virtual Standby 作业失败

在 Windows 系统上有效。

症状 1：

Virtual Standby 作业失败。在活动日志中显示以下其中一条消息：

```
无法转换虚拟磁盘
发生了内部错误，请与技术支持联系
```

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：

- 在 Virtual Standby 策略中指定的数据存储上没有足够的可用磁盘空间时，转换操作可能会失败。VDDK 返回消息，因为 VDDK API（当前）无法检测到数据存储上的可用磁盘空间量。要更正此问题，请在原始数据存储上释放完成该操作所需的磁盘空间量，然后重新提交作业。
- 网络干扰和很高的网络流量可能会导致转换操作失败。要解决此问题，请确认源节点与 ESX Server 系统或 vCenter Server 系统可以通过网络彼此进行通信，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。

  此问题是由于 VMware VDDK 连接限制引起的。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
  - ESXi 5：由所有 NFC 连接的传输缓冲区限制，并由主机强制执行；一个 ESXi 主机的所有 NFC 连接缓冲区的总和不能超过 32 MB。通过 vCenter Server 的连接有 52 个，包括每个主机的限制。

  注意：无法跨磁盘共享连接。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。
- 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。

症状 2：

Virtual Standby 作业失败。在活动日志中显示以下其中一条消息：

无法转换虚拟磁盘
发生了内部错误，请与技术支持联系

此外，VDDK 报告以下错误消息：

打开 vmdk 失败，并显示“找不到文件”错误。

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 未手工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。

症状 3：

Virtual Standby 作业失败。在活动日志中显示以下其中一条消息：

无法转换虚拟磁盘
发生了内部错误，请与技术支持联系

此外，VDDK 报告以下错误消息：

打开 vmdk 失败，或显示“服务器拒绝了连接”错误消息

解决方案 3：

此问题是由于 VMware VDDK 连接限制引起的。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

注意：无法跨磁盘共享连接。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。

Virtual Standby 作业无法使用 hotadd 传输模式

Windows 平台上存在此问题。

症状：

使用 hotadd 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。请联系技术支持。

此外，VDDK 报告以下错误消息：

未知错误。

解决方案：

未正确配置磁盘设置时，如果使用 hotadd 传输模式，恢复操作失败。

要配置磁盘，请执行下列操作：

1. 使用具有管理权限的帐号登录到备份代理系统。

   打开 Windows 命令行。

2. 在命令行上，键入以下命令：

   ```
   diskpart
   ```

   按 Enter 键。

   键入 SAN，然后按下 Enter 键。

   当前 SAN 策略显示。

3. 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。

4. 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

5. 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，请执行以下操作：

1. 使用具有管理权限的帐号登录到备份代理系统。

   打开 Windows“控制面板”，然后双击“管理工具”。

   “管理工具”窗口打开。

2. 从“收藏”列表，双击“计算机管理”。

   “计算机管理”对话框打开。

3. 展开“存储”，然后单击“磁盘管理”。

   磁盘显示。

4. 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。

Virtual Standby 作业结束，未显示任何会话警告消息

Windows 平台上存在此问题。

症状：

Virtual Standby 作业结束，且在活动日志中显示下列消息之一：

Virtual Standby 作业结束，未显示任何会话。

Virtual Standby 无法在 CA ARCserve D2D 服务器上检测到用于创建恢复点快照的备份会话。在 CA ARCserve D2D 服务器上可能不存在可以进行转换的备份会话。

解决方案：

在下列条件下，您将遇到此类型的问题：

- 您使用 CA ARCserve Central Protection Manager 将 CA ARCserve D2D 备份策略应用到该节点，并使用了下列条件之一。
  - CA ARCserve D2D 备份源设置已从“选择要备份的单个卷”选项更改为“备份整个计算机”选项，且在将 Virtual Standby 策略部署到该节点之后未使用更新的备份设置提交或完成某个完全备份。

    解决方案：提交 CA ARCserve D2D 节点的完全备份。
  - 将 Virtual Standby 策略部署到该节点之后，CA ARCserve D2D 备份源设置已从“备份整个计算机”选项更改为“选择要备份的单个卷”选项。

    解决方案：将 CA ARCserve D2D 备份源设置从“选择要备份的单个卷”选项更改为“备份整个计算机”选项，然后提交 CA ARCserve D2D 节点的完全备份。

备份和恢复作业不使用 SAN 传输模式

Windows 平台上存在此问题。

症状：

备份和恢复作业不使用 SAN 传输模式 (p. 195)。作业恢复为 NBD 传输模式 (p. 195)或 NBDSSL 传输模式 (p. 195)。“备份状态监视器”对话框的“传输模式”字段显示所使用的模式。

解决方案：

未在备份代理系统上正确配置 SAN LUN 时，可能会出现以上所述的症状。但是，如果 Windows 磁盘管理检测到 SAN LUN，且此问题仍存在，那么磁盘可能处于脱机状态，或者磁盘的读取属性不正确。要防止出现该行为，请重新配置磁盘。

要配置磁盘，请执行下列操作：

1. 使用具有管理权限的帐户登录到源节点或监视器服务器。
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。

使用 hotadd 传输模式的备份和恢复作业无法挂接磁盘

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将磁盘挂接到源节点或监视器服务器。此外，在活动日志中将显示以下消息：

无法打开 VMDK 文件 %1!s!。有关详细信息，请参阅调试日志 AFBackend.Log。请联系技术支持。

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. 如果磁盘是在转换作业期间进行连接的，请从代理系统中删除 hotadd 磁盘。

4. 重新提交作业。

错误代码故障排除

下表说明使用 CA ARCserve Central Virtual Standby 添加或更新节点时显示为弹出消息的错误代码。

错误代码	说明	可能的解决方法：
12884901933	无法连接到 *** 上的 CA ARCserve D2D 服务，错误代码是 12884901933。确保节点的所有条目正确，并且 CA ARCserve D2D 服务正在运行。	进行以下验证： ■ CA ARCserve D2D 服务在该节点上正运行。 ■ 为节点指定的主机名、IP 地址和通信协议正确。 ■ 在节点上的 CA ARCserve D2D Web 服务正在运行，且未被阻止，否则 DNS 无法解析节点的 IP 地址。 ■ 在节点上的 CA ARCserve D2D Web 服务正在运行，且 Windows 防火墙或任何其他防火墙未阻止通信。 ■ 连接到节点的网络电缆工作正常。 ■ 登录到节点的用户已获得使用无线网络通信所需的权限。

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

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。

虚拟机不自动打开

在 Windows 上有效。

症状：

虚拟机不自动打开。作为“恢复”的值，替代设置定义为自动启动虚拟机。

解决方案：

此为预期行为。应用程序无法自动打开从 CA ARCserve Central HostBased VM Backup 服务器添加的虚拟机。因此，在部署包含恢复方式（该方式针对由 Host-Based VM Backup 保护的节点定义为自动启动虚拟机）的策略时，Virtual Standby 会将恢复方式的值更改为手动启动虚拟机。

该行为的解决方案是使用 CA ARCserve D2D 或 CA ARCserve Central Protection Manager 保护虚拟机。

CA ARCserve Central Virtual Standby 无法与节点进行通信

在 Windows 系统上有效

症状：

CA ARCserve Central Virtual Standby 无法与节点进行通信

解决方案：

要确保 CA ARCserve Central Virtual Standby 可以将策略部署到节点并保护节点，请确认 Virtual Standby 服务器和您想保护的节点可以使用其主机名相互通信。

遵循这些步骤:

1. 从 CA ARCserve Central Virtual Standby 服务器，使用节点的主机名 ping 您想要保护的节点。
2. 从想要保护的节点，使用服务器的主机名 ping CA ARCserve Central Virtual Standby 服务器。

准备远程转换时出错。无法创建 VSS 快照

适用于所有 Windows 操作系统。

症状：

通过 vssadmin 实用工具手动创建 VSS 快照时，会出现以下错误消息：

“正在创建另一个卷影副本。请等几分钟再试。”

解决方案：

重新启动 Volume Shadow Copy 服务。

第 9 章： 应用最佳实践

此部分包含以下主题：

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。MSI 中包含的组件允许 CA ARCserve Central Applications 执行用于安装、升级和卸载 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：在您安装和卸载 CA ARCserve Central Applications 时，所有 CA ARCserve Central Applications MSI 软件包将调用此表中列出的组件。

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。
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。

组件	说明
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： /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： /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
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
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications

二进制文件名称	源
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

要确保 CA ARCserve Central Virtual Standby 和远程 Virtual Standby 正常工作，请排除指向 Hyper-V 虚拟机和 Hyper-V 进程的以下文件：

1. 虚拟机配置文件目录：
   - （默认）C:\ProgramData\Microsoft\Windows\Hyper-V
   - CA ARCserve Central Virtual Standby 虚拟机配置文件文件目录
2. 虚拟机虚拟硬盘文件目录：

- （默认）C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
- CA ARCserve Central Virtual Standby 虚拟机虚拟硬盘文件目录

3. 快照文件目录：
   - （默认）%systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots
   - CA ARCserve Central Virtual Standby 虚拟机快照文件目录
4. Hyper-V 进程：
   - %windows%\system32\Vmms.exe
   - %windows%\system32\Vmwp.exe

CA ARCserve Central Virtual Standby Licensing 的工作原理

CA ARCserve Central Virtual Standby 包含以下许可：

- CA ARCserve Central Virtual Standby-物理
- CA ARCserve Central Virtual Standby-VMware
- CA ARCserve Central Virtual Standby-Hyper-V

所有许可基于计数。CA ARCserve Central Virtual Standby 基于下列标准验证许可，并将许可授予给 CA ARCserve D2D 节点：

- CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-物理许可应用于您通过名称/IP 地址添加或从文件导入的全部 CA ARCserve D2D 节点。将策略应用于节点并启动虚拟转换过程后，CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-物理许可授予给节点。

  注意：这是 CA ARCserve Central Virtual Standby 许可的默认行为。

- CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-VMware 许可应用于通过名称/IP 地址添加或从文件导入的、且是在 ESX Server 系统或 vCenter Server 系统上的 VMware 虚拟机的全部 CA ARCserve D2D 节点。然而，在 CA ARCserve Central Virtual Standby 可以将 CA ARCserve Central Virtual Standby-VMware 许可应用于节点之前，您必须将节点与特定 ESX Server 系统或 vCenter Server 系统关联。

  注意：有关详细信息，请参阅为基于 VMware 的节点指定 ESX Server 或 vCenter Server 系统 (p. 53)。

  将策略应用于节点并且启动虚拟转换过程之后，CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-VMware 许可授予给每 ESX Server 系统。

- CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-VMware 许可应用于您从 CA ARCserve Central HostBased VM Backup 系统导入的所有虚拟机节点。将策略应用于节点并且启动虚拟转换过程之后，CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-VMware 许可授予给虚拟机节点。
- CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-Hyper-V 许可应用于通过名称/IP 地址添加或从文件导入的并且在 Hyper-V 管理程序上的全部 CA ARCserve D2D 节点。通过名称/IP 地址添加节点或从文件导入节点时，CA ARCserve Central Virtual Standby 会检测到 Hyper-V 服务器。通过名称/IP 地址添加节点，或从文件导入节点后，CA ARCserve Central Virtual Standby 将 CA ARCserve Central Virtual Standby-Hyper-V 许可授予给 CA ARCserve D2D 节点。

计数机制

下表说明给定方案所需要的 CA ARCserve Central Virtual Standby 许可数量。

D2D 节点类型	要求许可	计数机制
物理节点	CA ARCserve Central Virtual Standby-物理	每个节点一个许可
VMware 虚拟机	CA ARCserve Central Virtual Standby-VMware	每个 ESX/vCenter Server 系统一个许可
Hyper-V 虚拟机	CA ARCserve Central Virtual Standby-Hyper-V	每个 Hyper-V 系统一个许可

示例

- CA ARCserve Central Virtual Standby 保护 5 个物理 CA ARCserve D2D 节点。必需 5 个 CA ARCserve Central Virtual Standby-物理许可。
- CA ARCserve Central Virtual Standby 保护在一个 ESX Server 系统上的 3 个 VMware 虚拟机。必需 1 个 CA ARCserve Central Virtual Standby-VMware 许可。
- CA ARCserve Central Virtual Standby 保护分布在 10 个 ESX Server 系统上的 100 个 VMware 虚拟机。必需 10 个 CA ARCserve Central Virtual Standby-VMware 许可。
- CA ARCserve Central Virtual Standby 保护分布在 5 个 Hyper-V 系统上的 20 个 Hyper-V 虚拟机。必需 5 个 CA ARCserve Central Virtual Standby-Hyper-V 许可。

- CA ARCserve Central Virtual Standby 保护在 1 个 Hyper-V 系统上的 Hyper-V 虚拟机以及 1 个 ESX Server 系统上的 3 个 VMware 虚拟机。必需 1 个 CA ARCserve Central Virtual Standby-VMware 许可以及 1 个 CA ARCserve Central Virtual Standby-Hyper-V 许可。
- CA ARCserve Central Virtual Standby 保护从 CA ARCserve Central HostBased VM Backup 导入的且在 1 个 ESX Server 系统上的 VMware 虚拟机。必需 1 个 CA ARCserve Central Virtual Standby-VMware 许可。

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。

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。

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。

恢复点快照

恢复点快照是 CA ARCserve Central Virtual Standby 从 CA ARCserve D2D 恢复点创建的 VMware 虚拟磁盘 (VMDK) 或 Microsoft 虚拟硬盘 (VHD) 文件。在生产环境中运行 CA ARCserve D2D 的源服务器失败之后，CA ARCserve Central Virtual Standby 允许您使用恢复点快照打开虚拟机。

监视器服务器

监视服务器是验证 CA ARCserve Central Virtual Standby 环境中的源服务器的状态的服务器。

监控信号

监控信号是源节点发送给监视器服务器的电子信号，用以确定节点的状态。

虚拟转换

虚拟转换是 CA ARCserve Central Virtual Standby 将来自源节点的 CA ARCserve D2D 恢复点转换成称作恢复点快照的虚拟机数据文件的过程。

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。