CA ARCserve® Central Protection Manager

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

自上一版本的 CA ARCserve Central Protection Manager 以来已做出以下文档更新：

- 已进行更新以包括用户反馈、增强、改正以及其他小的改动，以便帮助改进产品或文档本身的使用性和理解性。
- 更新了指定高级备份设置 (p. 86)。此主题现在包括用于每次备份后生成文件系统编录以实现更快搜索的选项。
- 更新了查看 CA ARCserve Central Protection Manager 日志 (p. 138)。此主题现在包括两个新的模块选项：更新多节点和 CA ARCserve D2D 合并作业。删除了“操作前检查”和“提交 VM 备份作业”。
- 更新了按照 IP/名称添加节点时发生拒绝访问错误 (p. 166)。此主题现在包括禁用用户帐户控制 (UAC) 的两个解决方案。

目录

第 1 章： 介绍 CA ARCserve Central Protection Manager

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 Protection Manager 是 CA ARCserve Central Applications 提供的应用程序之一。CA ARCserve Central Protection Manager 允许您从中央位置管理 CA ARCserve D2D 和 CA ARCserve Backup 环境。单个应用程序提供有限的节点管理，但是 CA ARCserve Central Protection Manager 允许您执行以下操作：

- 添加一个或多个节点
- 从 Active Directory 服务器发现节点
- 发现并添加由管理程序管理的虚拟机
- 在添加的服务器上发现应用程序
- 创建并分配 CA ARCserve D2D 策略
- 提交还原作业用于管理的 CA ARCserve D2D
- 从管理的 CA ARCserve Backup 和 CA ARCserve D2D 服务器同步数据
- 部署 CA ARCserve D2D

该应用程序的工作原理

CA ARCserve Central Protection Manager 允许您从中央位置查看和管理保护的节点。

通过依次选择“开始”菜单 >“所有程序”>“CA”>“ARCserve Central Applications”>“CA ARCserve Central Protection Manager”，启动 CA ARCserve Central Protection Manager。将显示 CA ARCserve Central Protection Manager 主页，您可以使用以下导航功能访问任何 CA ARCserve Central Protection Manager 功能：

- **节点**－允许您使用各种工具管理节点和节点组、发现节点、向节点部署 CA ARCserve D2D 以及同步数据。
- **策略**－允许您添加、编辑、删除、复制和分配 CA ARCserve D2D 策略。此功能显示策略详细信息，并允许您根据相应的 CA ARCserve D2D 策略分配或取消分配节点。
- **配置**－允许您配置数据库的设置、CA ARCserve Backup 数据同步、SRM、发现、电子邮件配置、更新配置、首选项、管理员帐户、D2D 部署以及 IT 管理服务器。
- **查看日志 --** 允许您查看每个节点的活动日志。CA ARCserve Central Protection Manager 显示与该节点有关的所有日志消息。您可以通过指定以下选项来筛选此列表：
  - 重要级别（全部、信息、错误、警告，或错误和警告）
  - 模块（全部、通用、从发现导入节点、从管理程序导入节点、从文件导入节点、策略管理、CA ARCserve Backup 同步、CA ARCserve D2D 同步、CA ARCserve D2D 更新、更新、提交 CA ARCserve D2D 备份作业、更新多个节点、CA ARCserve D2D 合并作业）
  - 节点名称

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 Protection Manager

此部分包含以下主题：

先决条件安装任务

在您安装该应用程序之前，请完成以下先决条件任务：

- 阅读《版本说明》。《版本说明》介绍了系统要求、支持的操作系统以及本版本的 CA ARCserve Central Protection Manager 中已知问题的列表。
- 确认您的系统是否满足安装该应用程序所需的软硬件要求。
- 确保您的 Windows 帐号在计划安装 CA ARCserve Central Protection Manager 的计算机上有管理员权限或用于安装软件的任何其他等同权限。
- 确认您拥有要安装该应用程序的计算机用户名和密码。

- 确认您安装 CA ARCserve Central Protection Manager de 服务器和要部署策略的节点可以使用主机名相互通话。要确保 CA ARCserve Central Protection Manager 服务器和节点可以相互通信，请执行以下操作：
  - 从 CA ARCserve Central Protection Manager 服务器，使用节点的主机名 ping 节点。
  - 从想要保护的节点，使用服务器的主机名 ping CA ARCserve Central Protection Manager 服务器。
- 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。
- CA ARCserve Central Protection Manager 安装介质包含 Microsoft SQL Server 2008 R2 Express Edition，为了支持 CA ARCserve Central Protection Manager 数据库，这是至少所需的数据库应用程序。如果您想要使用 Microsoft SQL Server 支持 CA ARCserve Central Protection Manager 数据库，请在安装 CA ARCserve Central Protection Manager 之前，将 Microsoft SQL Server 安装在 CA ARCserve Central Protection Manager 服务器或远程服务器上。如果安装例程检测到不支持的 Microsoft SQL Server 版本，则安装将失败。有关 Microsoft SQL Server 的支持版本的详细信息，请参阅《版本说明》。

安装注意事项

在您安装 CA ARCserve Central Protection Manager 之前，请检查以下安装注意事项：

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

  安装应用程序时，安装软件包在安装产品组件之前先安装 CA ARCserve Central Applications 服务器模块。如果有必要向应用程序应用修补程序，则修补程序将在更新产品组件之前更新模块。
- 将 CA ARCserve D2D 部署到远程节点时，CA ARCserve Central Protection Manager 会在目标节点上安装 VMware Virtual Disk Development Kit (VDDK) 1.2.1。CA ARCserve Central Protection Manager 安装介质包含用于在 CA ARCserve Central Protection Manager 服务器和目标节点上安装 VMware Virtual Disk Development Kit (VDDK) 的安装文件。因此，您不需要从 VMware 网站下载 VDDK 安装文件，便可以将 CA ARCserve D2D 部署到远程节点。

安装 CA ARCserve Central Protection Manager

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 Protection Manager

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”。

“数据库设置”对话框将打开。

5. 在“数据库设置”对话框上，单击“选择数据库类型”旁边的下拉列表，并指定下列选项之一。
   - ARCserve Central Applications 默认数据库
   - Microsoft SQL Server

   在您指定一个数据库类型之后，指定数据库要求的选项将出现在“数据库设置”对话框上。
6. 执行以下操作之一：
   - **ARCserve Central Applications 默认数据库 --** 在“数据库设置”对话框上完成以下字段：
     - **指定安装路径** -- 指定您想安装 CA ARCserve Central Applications 默认数据库的位置。您可以接受默认路径或指定备用路径。
     - **指定数据文件路径 --** 指定您想安装 CA ARCserve Central Applications 默认数据库的数据文件的位置。您可以接受默认路径或指定备用路径。

     注意：CA ARCserve Central Applications 默认数据库不支持远程通讯。因此，请将默认数据库和数据文件安装在要安装该应用程序的计算机上。

- **Microsoft SQL Server 数据库 --** 在“数据库设置”对话框上完成以下字段：
  - **SQL Server 类型 --** 指定该应用程序用于与 SQL Server 数据库通讯的通讯类型。

    本地：当应用程序与 SQL Server 安装在同一台计算机上时，指定本地。

    远程：当应用程序与 SQL Server 安装在不同计算机上时，指定远程。
  - **SQL Server 名称 --** 如果指定的“SQL Server 类型”是“远程”，则需指定远程 SQL Server 名称。如果在本地使用 SQL Server，请从下拉列表中选择服务器。
  - **安全 --** 指定您想在 SQL Server 中进行身份验证的凭据类型。

    使用 Windows 安全 -- 指定“使用 Windows 安全”，来使用 Windows 凭据进行身份验证。

    使用 SQL Server 安全 -- 指定“使用 SQL Server 安全”，从而使用 SQL Server 凭据进行身份验证。然后指定 SQL Server 帐户的登录 ID 和密码。
  - **覆盖现有数据库 --** 如果您要允许安装程序检测并覆盖现有 CA ARCserve Central Applications 数据库，请指定覆盖数据库。

  单击“安装”。

  安装过程完成后，“安装报告”对话框将打开。

7. “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。

无人值守安装 CA ARCserve Central Protection Manager

CA ARCserve Central Applications 允许您无人值守安装 CA ARCserve Central Protection Manager。无人值守安装无需用户交互。下列步骤说明如何使用 Windows 命令行以无人值守方式安装应用程序。

无人值守安装 CA ARCserve Central Protection Manager

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。

如何卸载 CA ARCserve Central Protection Manager

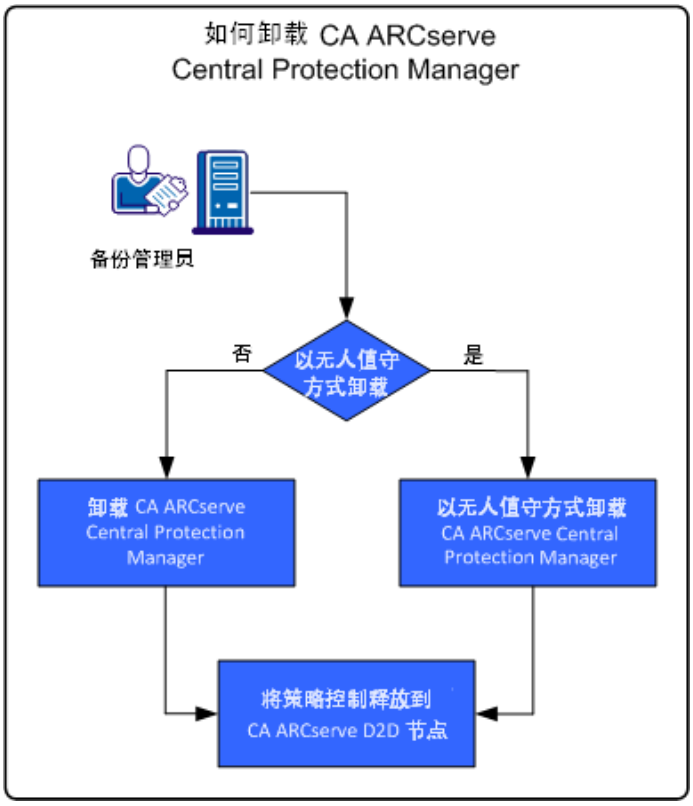
可以使用以下方法卸载 CA ARCserve Central Protection Manager：

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

取消分配策略

最佳做法是，卸载应用程序之前，从策略所分配到的节点取消分配所有策略。建议使用该方法，因为在将 CA ARCserve Central Protection Manager 策略分配给节点后，无法在节点上指定 CA ARCserve D2D 备份设置。此外，在卸载应用程序之后，无法从节点取消分配策略。CA ARCserve D2D 提供了一个命令行实用工具，允许您在卸载应用程序之后，从节点取消分配策略。

下图说明了如何卸载应用程序：



任务	参阅主题
使用 Windows 控制面板执行标准卸载。	卸载 CA ARCserve Central Protection Manager (p. 19)。
使用 Windows 命令行执行无人值守卸载。	以无人值守方式卸载 CA ARCserve Central Protection Manager (p. 20)。
卸载 CA ARCserve Central Protection Manager 之后从节点取消分配策略。	将策略控制释放到 CA ARCserve D2D 节点 (p. 21)。

卸载 CA ARCserve Central Protection Manager

您可以使用 Windows 控制面板中的“程序和功能”卸载 CA ARCserve Central Protection Manager。

遵循这些步骤:

1. 登录要卸载该应用程序的计算机。

   注意：请使用管理帐户或具有管理权限的帐户登录。

2. 从 Windows 的“开始”菜单中，依次单击“开始”>“控制面板”打开 Windows 控制面板。
3. 单击“程序和功能”打开“卸载或更改程序”窗口。
4. 找到并单击 CA ARCserve Central Protection Manager。

   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。

无人值守卸载 CA ARCserve Central Protection Manager

CA ARCserve Central Applications 允许您无人值守卸载 CA ARCserve Central Protection Manager。无人值守安装无需用户交互。下列步骤说明如何使用 Windows 命令行以无人值守方式卸载应用程序。

遵循这些步骤:

1. 登录要卸载该应用程序的计算机。

   注意：请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：使用以下语法可以无人值守方式卸载应用程序。

   ```
   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   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。使用以下产品代码以无人值守方式卸载 CA ARCserve Central Applications。

   CA ARCserve Central Protection Manager

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

   CA ARCserve Central HostBased VM Backup

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

   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。

将策略控制释放到 CA ARCserve D2D 节点

卸载 CA ARCserve Central Protection Manager 的过程不会从 CA ARCserve D2D 节点取消分配备份策略。该行为阻止您在卸载 Protection Manager 之后直接在 CA ARCserve D2D 节点上指定备份设置。最佳做法是，在卸载应用程序之前，从策略所分配到的节点取消分配所有策略。如果不采用此做法，您可以使用专门为此目的设计的实用工具将策略控制释放到节点。

遵循这些步骤:

1. 登录到 CA ARCserve D2D 节点。
2. 打开 Windows 命令行，转到以下目录：

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

3. 使用以下语法执行 ARCCentralAppMgrUtility.exe：

   ```
   ARCCentralAppMgrUtility.exe -clean pm|hbvb|vs [-debug]
   ```

   pm|hbvb|vs

   定义要解除对 CA ARCserve D2D 节点控制的应用程序。指定下列参数之一：

   pm

   CA ARCserve Central Protection Manager

   hbvb

   CA ARCserve Central HostBased VM Backup

   vs

   CA ARCserve Central Virtual Standby

   -debug

   -debug 选项不是必需的选项。如果指定该选项，实用工具将生成一个调试日志文件，该文件存储在以下目录中：

   ```
   <D2D_Home>\Log\ARCCentralAppMgrUtility.log
   ```

   示例：以下示例介绍了用于将策略控制释放到节点的语法。

   ```
   ARCCentralAppMgrUtility.exe -clean pm
   ```

策略控制将释放到节点。

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。
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。

组件	说明
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

第 3 章： CA ARCserve Central Protection Manager 入门

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

此部分包含以下主题：

确认 CA ARCserve Central Protection Manager 服务器可与节点进行通信

注意：这是配置 CA ARCserve Central Protection Manager 保护节点的可选步骤。

要帮助确保 CA ARCserve Central Protection Manager 可以将策略部署到节点并保护节点，您必须确认 Protection Manager 服务器和您想保护的节点可以使用其主机名相互通信。

确认 CA ARCserve Central Protection Manager 服务器可以与节点进行通信

1. 从 CA ARCserve Central Protection Manager 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 Protection Manager 服务器。

配置 CA ARCserve Backup 数据同步排定

CA ARCserve Backup 数据同步使您能够配置系统，设置用户将 CA ARCserve Backup 数据库与 CA ARCserve Central Protection Manager 数据库同步的排定时间和重复方式，例如，天数、星期几或月内某日。

遵循这些步骤:

1. 登录该应用程序。
2. 单击导航栏上的“配置”打开“配置”屏幕。
3. 在“配置”面板中，单击“CA ARCserve Backup 数据同步排定”以显示“CA ARCserve Backup 数据同步”选项。
4. 单击“启用”以启用“CA ARCserve Backup 数据同步”。

   注意：默认情况下，“CA ARCserve Backup 数据同步配置”处于启用状态。
5. 指定以下参数以排定 CA ARCserve Backup 数据同步：
   - 重复方式
   - 排定时间
6. 单击“保存”应用 CA ARCserve Backup 数据同步排定。
7. （可选）单击“立即执行”可立即启动 CA ARCserve Backup 数据同步过程。

配置 SRM 排定

CA ARCserve Central Protection Manager 允许备份管理员为 CA ARCserve D2D 节点配置排定，用于定义收集 SRM 数据的时间和频率。SRM（存储资源管理）用于收集以下内容信息：

- Microsoft SQL Server 和 Microsoft Exchange Server 实施的硬件、软件和应用程序数据。
- 来自由 CA ARCserve Central Applications 服务器管理的 CA ARCserve D2D 服务器的性能关键指标 (PKI) 数据。

  注意：对于 CA ARCserve Backup 节点，CA ARCserve Backup 收集 PKI 数据，然后在 CA ARCserve Backup 数据同步过程中，将该数据与 CA ARCserve Central Protection Manager 同步。

遵循这些步骤:

1. 登录该应用程序。
2. 单击导航栏上的“配置”打开“配置”屏幕。

3. 在“配置”面板上，单击“SRM 配置”显示 SRM 配置选项。
4. 单击“启用”以启用 SRM。

   注意：默认情况下，“SRM 配置”处于启用状态。
5. 指定以下参数以排定 SRM：
   - 重复方式
   - 排定时间
6. 单击“保存”应用 SRM 排定。
7. （可选）单击“立即执行”可立即启动 SRM 数据收集过程。

配置发现排定

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

- **每几天一**允许您按指定天数重复此方式。（默认设置）
- **每周选定的某天 --** 允许您在指定的星期几重复此方式。星期一、星期二、星期三、星期四、星期五是一星期内默认的日子。
- **每月选定的某天 --** 允许您在月内指定的日期重复此方式。默认选项是每月的 1 号。

将显示一个 Active Directory 列表供您在设置发现节点排定时查看。

配置电子邮件和报警设置

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

遵循这些步骤:

1. 登录该应用程序。

   从主页上的导航栏中，单击“配置”以打开“配置”屏幕。
2. 从“配置”面板中，单击“电子邮件和报警配置”以打开“电子邮件和报警配置”选项。

3. 填写下列字段：
   - **服务 --** 从下拉列表中指定电子邮件服务类型。（Google Mail、Yahoo Mail、Live Mail 或其他）。
   - **邮件服务器**—指定希望 CA ARCserve Central Applications 在发送电子邮件时使用的 SMTP 服务器的主机名。
   - **需要身份验证 --** 您指定的邮件服务器需要身份验证时请选择该选项。必需帐号名称和密码。
   - **主题 --** 指定默认电子邮件主题。
   - **发件人 --** 指定电子邮件发件人的电子邮件地址。
   - **收件人** -- 指定将接收电子邮件的一个或多个电子邮件地址，由分号 (;) 分隔。
   - **使用 SSL**—如果您指定的邮件服务器需要安全连接 (SSL)，请选择该选项。
   - **发送 STARTTLS --** 如果您指定的邮件服务器需要“STARTTLS”命令，请选择该选项。
   - **使用 HTML 格式 --** 允许您以 HTML 格式发送电子邮件。（默认已选择）
   - **启用代理设置 --** 如果有代理服务器，请选择该选项，然后指定代理服务器设置。
4. 单击“测试电子邮件”确认邮件配置设置正确无误。
5. （可选）从“发送电子邮件报警”部分，单击“发现的节点”，以便应用程序在发现新节点时发送电子邮件报警消息。
6. 单击“保存”。

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

电子邮件配置即被应用。

配置 IT 管理服务器设置

CA ARCserve Central Protection Manager 允许您将报警消息发送到 IT 管理服务器。要发送报警信息，将应用程序服务器配置为与 IT 管理服务器通信。

配置 IT 管理服务器设置

1. 登录 CA ARCserve Central Protection Manager，然后单击“导航”上“配置”
2. 从“配置”屏幕上，单击“配置”列表中的“IT 管理服务器配置”。
3. 完成以下 IT 管理服务器配置选项：
   - 单击“启用”。
   - 单击“Nimsoft”或“Kasaya”。
   - 指定重复方式。“重复方式”定义原始发送过程失败时在一周的哪几天重新向 IT 管理服务器发送报警通知。IT 管理服务器不可用或脱机时，发送报警的过程会失败。
   - 指定排定。排定定义在什么时间向 Nimsoft 服务器重新发送报警通知。
4. 单击“保存”。

CA ARCserve Central Protection Manager 服务器即被配置与 IT 管理服务器通信。

注意：单击“重置”可恢复到先前保存的值。

配置 CA ARCserve Central Applications 更新排定

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

配置 CA ARCserve Central Applications 更新排定

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

修改管理员帐户

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。

配置 D2D 部署设置

CA ARCserve Central Protection Manager 允许您配置 D2D 部署设置，以指定要将 CA ARCserve D2D 部署到的位置。

注意：要将 CA ARCserve D2D 部署到运行 Windows XP 的计算机，请禁用远程 Windows XP 计算机上的“使用简单文件共享”选项。

配置 D2D 部署设置

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. 在“配置”面板上，单击“D2D 部署配置”。

   此时将显示“D2D 部署配置”选项。

3. 填写配置屏幕上的下列字段：
   - **端口 --** 此端口号用于连接到基于 Web 的 UI。默认情况下，端口号为 8014。
   - **安装路径 --** 这是 CA ARCserve D2D 在远程服务器上的安装路径。默认情况下，该位置是 %Program Files%。
   - **允许安装程序安装驱动程序**（默认被选中） -- 指定是否要安装程序自动安装该驱动程序。
   - **重新启动（默认为“是”）** -- 指定在部署过程完成时是自动执行必要的系统重启还是要以后手动重启系统。
   - **使用 HTTPS**（默认为“否”） -- 与 HTTP 通信相比，HTTPS（安全）提供更高的安全级别。当您在网络中传送机密信息时，建议使用 HTTPS 通信协议。
4. 单击“保存”。

部署 D2D 配置即被应用。

配置数据库。

安装 CA ARCserve Central Protection Manager 后，您可以执行以下操作：

- 更新 CA ARCserve Central Protection Manager 数据库的设置。例如，您可以更新实例名称、端口值等等。
- 将 CA ARCserve Central Protection Manager 数据库应用程序更改为 Microsoft SQL Server。
- 将 CA ARCserve Central Protection Manager 数据库应用程序更改为 Microsoft SQL Server Express Edition。

配置 CA ARCserve Central Protection Manager 数据库

1. 从导航栏上，单击“配置”。
2. 从“配置”面板上，单击“数据库配置”。
3. 填写配置屏幕上的下列字段：
   - **SQL Server 计算机名** -- 指定运行 SQL Server 实例的服务器名。
   - **SQL Server 实例**--指定 SQL Server 实例的名称。
   - **SQL Server 端口** -- 指定此实例的端口号或启用自动检测选项。
   - **选择身份验证模式** -- Windows 身份验证模式是默认选择。

     注意：选择 SQL Server 和 Windows 身份验证模式将激活“用户名”和“密码”字段。
   - （可选）**测试** -- 单击“测试”验证应用程序是否可以与 Microsoft SQL Server 实例通讯。
   - **指定数据库连接池值** -- 对于最大和最小连接，请输入 1 到 99 的值。
4. 单击“保存”。

   注意：单击“重置”清除所有指定值，并加载初始数据。
5. （可选）如果应用程序正在向 CA ARCserve Central Reporting 提供数据，请打开 Windows 服务器管理器，重新启动以下服务：

   `CA ARCserve Central Applications 服务`

   数据库服务器配置即被应用。

重新创建 CA ARCserve Central Protection Manager 数据库

处于种种原因，您可能想重新创建 CA ARCserve Central Protection Manager 数据库。例如，您当前的数据库消耗 10 GB 以上的数据。以下过程说明如何重新创建 CA ARCserve Central Protection Manager 数据库。该过程适用于 Microsoft SQL Server 和 Microsoft SQL Server Express Edition 数据库。

重要说明！ 删除 CA ARCserve Central Protection Manager 数据库时，所有当前数据将丢失。

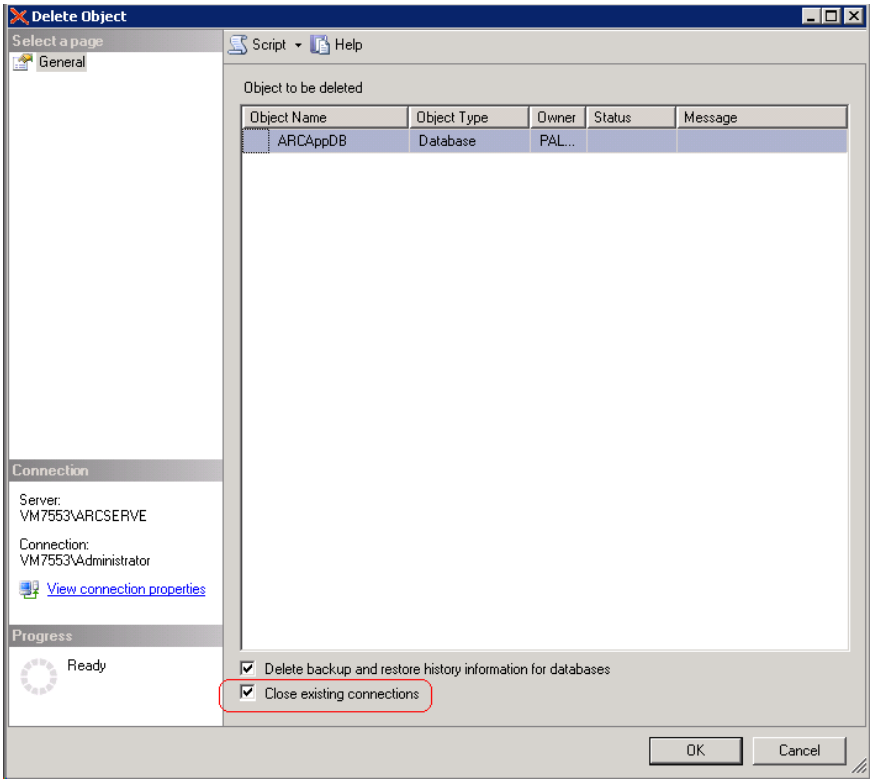
重新创建 CA ARCserve Central Protection Manager 数据库

1. 打开 Microsoft SQL Server Management Studio Express，然后登录到 ARCserve_APP 实例。

   注意：如果在 CA ARCserve Central Protection Manager 服务器上未安装 Microsoft SQL Server Management Studio Express，您可以从 Microsoft 下载中心下载该实用工具。

2. 右键单击“ARCAppDB”，然后单击弹出菜单上的“删除”。

   “添加对象”对话框打开。



3. 在“删除对象”对话框上，单击“关闭现有连接”选项，然后单击“确定”。

   “删除对象”对话框关闭，CA ARCserve Central Protection Manager 数据库即被删除。

4. 打开 CA ARCserve Central Protection Manager，然后单击导航栏上的“配置”。

   配置选项显示。

5. 单击“数据库配置”。

   数据库选项将显示。

6. 请确保在以下字段中指定的值正确：
   - **SQL Server 计算机名** -- 指定运行 SQL Server 实例的服务器名。
   - **SQL Server 实例**--指定 SQL Server 实例的名称。
7. （可选）填写以下字段：
   - **SQL Server 端口** -- 指定此实例的端口号或启用自动检测选项。
   - **选择身份验证模式** -- Windows 身份验证模式是默认选择。

     注意：选择 SQL Server 和 Windows 身份验证模式将激活“用户名”和“密码”字段。
   - **指定数据库连接池值** -- 对于最大和最小连接，请输入 1 到 99 的值。
8. 单击“测试”以建立与数据库的连接。
9. 单击“保存”。

CA ARCserve Central Protection Manager 重新创建数据库。数据库实例的名称是 ARCAppDB。

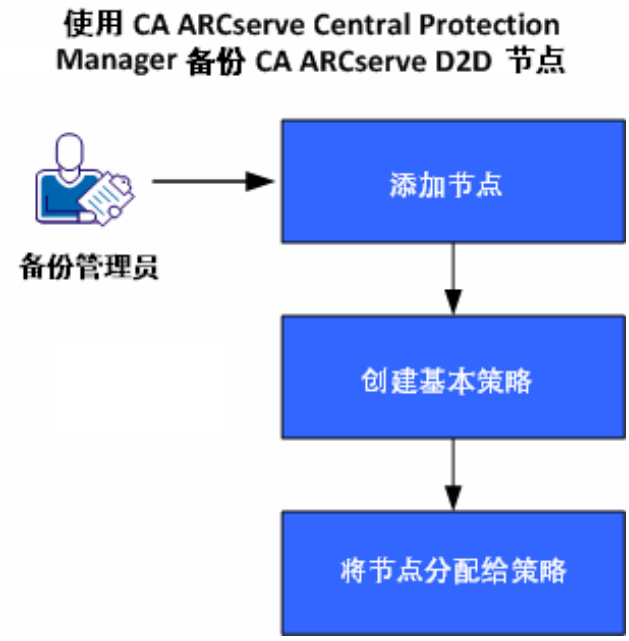
第 4 章： 使用 CA ARCserve Central Protection Manager

此部分包含以下主题：

使用 CA ARCserve Central Protection Manager 备份 CA ARCserve D2D 节点

使用 CA ARCserve Central Protection Manager，您可以创建用于定义如何以及何时备份和存储驻留在 CA ARCserve D2D 节点上的数据的策略。下列主题中包含的信息介绍了如何使用基本策略提交 CA ARCserve D2D 备份作业。基本策略可以保护在生产环境中运行的大多数 CA ARCserve D2D 节点。

下图说明了使用 CA ARCserve Central Protection Manager 创建基本备份策略并备份 CA ARCserve D2D 节点的过程：



按照以下步骤，使用 CA ARCserve Central Protection Manager 创建基本策略并备份 CA ARCserve D2D 节点：

1. 添加节点 (p. 43)。
2. 创建基本策略 (p. 43)。
3. 将节点分配给策略 (p. 47)。

添加节点

要使用某个策略备份 CA ARCserve D2D 节点，应首先定义想要备份的节点。

注意：您可以使用发现自动执行该任务。但是，发现仅检测在 Active Directory 服务器上的 Active Directory 中显示的节点。

遵循这些步骤:

1. 登录到 CA ARCserve Central Protection Manager，然后单击导航栏上的“节点”。
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”。
3. 完成“按照 IP/名称添加节点”对话框中的所有字段，然后单击“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”。

   注意：要添加更多节点，请重复步骤 2、3 和 4。

添加节点后，该节点将显示在默认组中。

创建基本策略

策略定义如何以及何时备份和存储驻留在 CA ARCserve D2D 节点上的数据。CA ARCserve Central Protection Manager 不包含默认策略。创建策略是备份驻留在节点上的数据的先决任务。

要创建基本策略，请指定保护设置并创建排定。保护设置定义要备份的数据、存储数据的位置以及存储数据的方式。排定定义备份节点的时间和频率。

遵循这些步骤:

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”打开“策略”屏幕。
2. 单击“新建”创建新的策略。
3. 在“新建策略”对话框的“策略名称”字段中，指定策略的名称。
4. 单击“备份设置”选项卡，然后单击“保护设置”以显示“保护设置”选项。

5. 指定备份目标。

   您可以指定一个本地路径（卷或文件夹），或者远程的共享文件夹（或映射驱动器）作为备份位置。

   - 如果指定备份到本地路径（卷或文件夹），指定的备份目标位置不能与源位置相同。如果无意中在目标中包含了源，备份作业将忽略这部分源且不将其包含在备份之内。

     重要说明！确认您指定的目标卷不包含系统信息。CA ARCserve D2D 不备份包含系统信息的目标卷。当尝试使用裸机恢复 (BMR) 恢复计算机时，恢复可能会失败。

     注意：不能在磁盘级还原动态磁盘。如果您的数据已备份到动态磁盘的卷上，则在 BMR 期间将无法还原该动态磁盘。

   - 在将数据备份到远程共享位置时，请指定访问远程计算机所需的位置路径和凭据。

6. 指定备份源。

   您可以指定备份整个节点或节点上的单个卷。

   请注意以下问题：

   - 如果选择整个计算机备份选项，CA ARCserve D2D 将自动发现连接到当前计算机的所有磁盘/卷，并将其包含在备份中。
   - 如果未选择备份系统/启动卷，则会显示一条警告消息。该消息指出备份无法用于执行 BMR。

7. 指定恢复点。

   指定保留的备份映像的数量。默认值为 31，最大值为 1344。修改该数量时，应考虑到目标位置上的可用空间量。

   如果超过指定的恢复点数量，CA ARCserve D2D 会将最早的增量子备份合并到父备份中，并重新创建基准映像。新的基准映像由父块及最早的子块组成。对于每次后续备份，会重复执行将最早子备份合并到父备份这一过程。该过程使您可以执行无限增量备份，同时维护同样的保留计数。

8. 指定要用于备份的压缩类型。

   压缩会减少对磁盘空间的占用，而且还可以抵消由于对 CPU 越来越多的占用而导致的对备份速度的负面影响。

   可用的压缩选项如下：

   无压缩

   未执行压缩。此选项的 CPU 使用率最低（速度最快），但是对于您的备份映像而言，磁盘空间占用最大。

   标准压缩

   已执行某些压缩。此选项将会在 CPU 使用率和磁盘空间占用之间实现良好的平衡。默认设置为标准压缩。

   最大压缩

   已执行最大压缩。此选项提供最高的 CPU 使用率（速度最慢），但是对于备份映像而言，磁盘空间占用最低。

   请注意以下问题：

   - 如果您的备份映像包含无法压缩的数据（如 JPG 图像、ZIP 文件等），则需要分配存储空间以便处理此类数据。
   - 如果您的目标没有足够的可用空间，请考虑提高备份的压缩设置。

9. 指定要用于增加安全性的加密设置。

   a. 指定要用于备份的加密算法类型。

      数据加密将数据转换为需要有解码机制才可识别的格式。CA ARCserve D2D 数据保护使用安全的 AES（高级加密标准）加密算法实现指定数据的最佳安全性和隐私。

      可用的格式选项是“不加密”、AES-128、AES-192 和 AES-256。（要禁用加密，请选择“不加密”）。

      - 完全备份及其所有的相关增量以及验证备份必须使用相同的加密算法。
      - 当您更改增量备份或验证备份的加密算法时，请执行一次完全备份。这意味着在更改加密算法之后，不管初始的备份类型如何，首次备份都将是完全备份。

        例如，如果您更改算法格式并手工提交自定义的增量或验证备份，它将自动转变为完全备份。

b. 指定加密算法后，提供（并确认）加密密码。

- 加密密码限制为最多 23 个字符。
- 完全备份及其所有的相关增量以及验证备份必须使用相同的密码来加密数据。
- 如果更改了增量备份或验证备份的加密密码，请执行一次完全备份。这意味着在更改加密密码之后，不管初始的备份类型如何，首次备份都将是完全备份。

  例如，如果您更改加密密码并手工提交自定义的增量或验证备份，它将自动转变为完全备份。

当启用加密时，会更新活动日志以描述用于每次备份的加密。

10. 指定调节备份。

    您可以指定写入备份的最大速度（MB/分钟）。您可以调节备份速度以减少 CPU 或网络使用率。但是，限制备份速度会对备份窗口产生负面影响。

11. 单击“排定”选项卡以显示“排定”选项。

12. 指定备份排定：

    设置开始日期和时间

    指定您的排定备份的开始日期和开始时间。

    增量备份

    指定增量备份的备份排定。

    可用的选项是“重复”和“从不”。如果选择“重复”选项，请指定两次备份尝试之间的已用时间（以分钟、小时或天计）。增量备份的最小设置为每 15 分钟一次。

    默认情况下，增量备份排定是每 1 天重复一次。

    完全备份

    指定完全备份的备份排定。

    按照排定，CA ARCserve D2D 会对源计算机中所有使用的块进行完全备份。可用的选项是“重复”和“从不”。如果选择“重复”选项，请指定两次备份尝试之间的已用时间（以分钟、小时或天计）。完全备份的最小设置为每 15 分钟一次。

    默认情况下，完全备份的排定是“从不”（无排定的重复）。

验证备份

指定验证备份的备份排定。

可用的选项是“重复”和“从不”。如果选择“重复”选项，请指定两次备份尝试之间的已用时间（以分钟、小时或天计）。验证备份的最小设置为每 15 分钟一次。

默认情况下，验证备份的排定是“从不”（无排定的重复）。

13. 单击“保存”。

基本备份策略即已创建。该策略将显示策略列表中，使用在“策略”屏幕上的“步骤 3”中指定的名称。

注意：如果排定同时执行多种类型的备份，将根据以下优先级执行备份类型：

- 优先级 1 - 完全备份
- 优先级 2 - 验证备份
- 优先级 3 - 增量备份

示例：当排定同时运行全部三种备份类型时，CA ARCserve D2D 将执行完全备份。当排定同时运行验证备份和增量备份，而未排定完全备份时，CA ARCserve D2D 将执行验证备份。仅当不与其他任何备份类型冲突时，才会执行排定的增量备份。

将节点分配给策略

创建基本策略后，将要使用其进行备份的 CA ARCserve D2D 节点分配给该策略。

遵循这些步骤:

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”打开“策略”屏幕。
2. 在“策略”屏幕的策略列表中，单击已创建的策略。
3. 单击“策略分配”选项卡以显示策略分配（列表）。
4. 单击“分配和取消分配”以打开“分配/取消分配策略”对话框。
5. 单击您要添加的一个或多个节点旁边的复选框，然后单击向右箭头。

   “许可协议”对话框将打开。

6. 阅读并接受本许可协议的条款，然后单击“完成”。

   节点将分配给您创建的策略，并立即得到部署。备份将根据您在“排定”选项卡上定义的排定启动。

7. 完成向策略分配节点后，请单击“确定”保存策略分配情况并关闭“分配和取消分配”对话框。

分配好节点后，CA ARCserve Central Protection Manager 将立即向节点部署策略。备份操作将根据您选择的保护设置启动，并按照您在策略中定义的排定进行。

如何在 CA ARCserve Central Protection Manager 中管理节点

CA ARCserve Central Protection Manager 为您提供了各种工具和选项来管理节点和节点组。本节介绍了如何为节点和节点组添加、删除、修改和同步数据。您还可以发现节点并将 CA ARCserve D2D 部署到节点上。

本节包括以下主题：

理解节点管理屏幕

节点管理是 CA ARCserve Central Applications 的入口组件。您可以通过 CA ARCserve Central Protection Manager 应用程序左边面板的导航栏访问它。

“节点管理”在此屏幕上包含要执行的四个类别操作。

- **节点** -- 允许您管理特定节点。有关管理节点的详细信息，请参阅“您使用节点可以做什么” (p. 50)。
- **节点组** --允许您管理特定节点组。有关详细信息，请参阅您使用节点组可以做什么 (p. 64)。
- **操作**－允许您备份数据 (p. 120)、还原数据 (p. 122)和部署数据 (p. 71)。
- **筛选** -- 允许您使用筛选将安装了特定应用程序的节点显示在一个组中。有关详细信息，请参阅“筛选节点组” (p. 73)。

位于“产品”列的每个节点的状态标识 CA ARCserve Backup 和 CA ARCserve D2D 图标。下表介绍了“产品”列中每个产品的状态：

图标	说明
	此状态具有字母“M”表示该节点是一个由 CA ARCserve Central Applications 管理的主 CA ARCserve Backup 服务器或单机 CA ARCserve Backup 服务器。
	此状态具有字母“M”和右下角的惊叹号，表示该节点是一个由 CA ARCserve Central Applications 管理的主 CA ARCserve Backup 服务器或单机 CA ARCserve Backup 服务器，但是已有“xx”小时没有成功同步了。（“xx”默认为 48 个小时），或者同步尚未执行。
	此状态没有字母“M”，表示该节点是不受 CA ARCserve Central Applications 管理的主 CA ARCserve Backup 服务器、单机 CA ARCserve Backup 服务器或成员 CA ARCserve Backup 服务器。
	该状态表示该节点包含旧版 CA ARCserve Backup
	此状态表示该节点不受 CA ARCserve Central Applications 管理，而且没有连接到 CA ARCserve D2D。
	该状态表示该节点包含旧版 CA ARCserve D2D。
	此状态具有字母“M”，表示该节点由 CA ARCserve Central Applications 管理，并已连接到 CA ARCserve D2D。
	此状态具有字母“M”，表示该节点由 CA ARCserve Central Applications 管理，但未连接到 CA ARCserve D2D。
	此状态具有字母“M”，表示该节点由 CA ARCserve Central Applications 管理，并已连接到 CA ARCserve D2D，但是有警告。
	此状态具有字母“M”并在右下角有一个惊叹号，表示该节点是一个由 CA ARCserve Central Applications 管理的 <caabr> 服务器，但是已有“xx”小时没有成功同步。（“xx”默认为 48 个小时），或者同步尚未执行。

您使用节点可以做什么

CA ARCserve Central Protection Manager 允许您添加、修改和删除节点、同步数据、指定节点设置、发现节点、将节点信息导出到 CSV 文件中以及确定各个节点的状态。

注意：当您将匹配 CA ARCserve Backup 和 CA ARCserve D2D 服务器的节点添加到 CA ARCserve Central Protection Manager，然后在每个节点上执行同步时，将生成特定节点的数据，并可以在 CA ARCserve Central Reporting 中查看。有关同步的详细信息，请参阅同步数据和选项 (p. 61)。

使用发现添加节点

CA ARCserve Central Protection Manager 允许您通过发现过程添加多个节点。

使用发现添加节点

1. 登录到应用程序，并单击导航栏上的“节点”。

   “节点”屏幕打开。

2. 单击“节点”工具栏上的“发现”。

   此时将打开“按 Active Directory 发现”对话框。

3. 填写下列字段：

   - 用户名（域）
   - 密码（域）
   - 计算机名筛选

   单击“添加”，然后单击“启动发现”。

   将运行发现 (p. 51)。

4. 发现节点完成后，将显示以下确认消息：

   是否要继续从发现结果添加节点?

   单击“是”将转到“从发现结果添加节点”。

   注意：要关闭消息而不添加节点，请单击“否”。

   此时将打开“从发现结果添加节点”屏幕，其中显示已发现的节点的列表。

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

   注意：您可以通过节点名称或域筛选列表来最小化列表。

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

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

8. 在“节点凭据”屏幕中，提供您想添加的节点的用户名和密码。您可以知道全局凭据，或将凭据应用到选定的节点。

9. 单击“完成”。

节点已被添加。

发现监控器对话框

“发现监控器”对话框显示在您的环境之内发现的节点的总体状态。

“发现监控器”对话框提供下列信息：

阶段

显示发现节点的三个阶段：“发现节点”、“更新数据”以及“发现已完成”。

状态

在发现过程中显示“活动”状态，在发现完成时，显示“已完成”。

所用时间

显示发现节点的用时。

已处理的节点数

显示在数据库中记录和更新的已处理节点数。

按 IP 地址或节点名称添加节点

CA ARCserve Central Protection Manager 允许您通过引用节点的 IP 地址或主机名，将 CA ARCserve D2D 和 CA ARCserve Backup 节点添加到节点组中。

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。

5. （可选）如果 CA ARCserve Backup 安装在节点上，而 CA ARCserve Central Protection Manager 凭据没有 CA ARCserve Backup 管理员权限，则将显示以下消息：

   必须有 ARCserve Backup 管理员权限。

   要继续，请指定 CA ARCserve Backup 管理员帐户的登录凭据，然后单击“确定”。

   注意： CA ARCserve Central Protection Manager 仅可以在 CA ARCserve Backup 主服务器和单机服务器上执行数据同步。当主服务器是分支服务器时，CA ARCserve Central Protection Manager 仅可以使 CA ARCserve Backup 数据与全局显示板服务器保持同步。

将添加节点。

从发现结果添加节点

通过该选项，您可以选择根据在“发现配置”面板中指定的设置自动检测到的节点。

遵循这些步骤:

1. 登录该应用程序。

   单击导航栏上的“节点”以打开“节点”屏幕。

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

   此时将打开“从发现结果添加节点”屏幕，其中显示已发现的节点的列表。

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

   注意：您可以通过节点名称或域筛选列表来最小化列表。

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

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

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

7. 单击“完成”。

节点已被添加。

通过从 ESX/VC 导入虚拟机添加节点

此“添加节点”选项允许您查找并添加您指定的 ESX 或 vCenter 服务器主机上的所有虚拟机。

注意：安装了 VMware 工具的计算机是仅可以找到的虚拟计算机。

通过从 ESX/VC 导入虚拟机添加节点

1. 登录到应用程序，并单击导航栏上的“节点”。

   “节点”屏幕打开。

2. 在“节点”工具栏中单击“添加”，然后在弹出菜单中单击“从 ESX/VC 导入虚拟机”。

   “发现节点”对话框将打开。

3. 完成“发现节点”对话框中的以下字段：

   - ESX 或 vCenter 服务器主机 -- 允许您指定您想扫描的管理程序。
   - 用户名
   - 密码
   - 端口
   - 协议

   单击“连接”。

   该应用程序扫描指定的管理程序。

4. 扫描完成后，单击“下一步”。

   “节点凭据”对话框将打开。

5. 在“节点凭据”对话框上，为检测到的所有虚拟机提供全局用户名和密码，然后单击“应用于所选”。

6. （可选）单击虚拟机输入该机的特定凭据。

7. 单击“完成”。

您选择的虚拟机将添加到节点组中。

从文件导入节点

CA ARCserve Central Protection Manager 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。

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。

更新节点

CA ARCserve Central Protection Manager 允许您更新以前添加的节点的信息。在下列状况出现时您更新节点：

- **所有节点：**
  - 在节点注册到 CA ARCserve Central Protection Manager 之后，新产品安装在节点上。
  - 在节点注册到 CA ARCserve Central Protection Manager 之后，节点的用户名或密码被更新。
- **CA ARCserve Backup 节点：**
  - CA ARCserve Backup 分支服务器被更新到一个 CA ARCserve Backup 主服务器。
  - 在 CA ARCserve Backup 中央主服务器注册到 CA ARCserve Central Protection Manager 之后，该中央主服务器被更新到 CA ARCserve Backup 主服务器。

  注意：当您添加或更新充当与中央主服务器关联的 CA ARCserve Backup 分支服务器的节点时，将在“节点”屏幕上的两个位置显示中央主服务器的主机名。“节点”屏幕上的第一个位置为“所有节点”组。不管服务器的主机名中包含多少个字符，都将在“所有节点”组中显示该服务器的全名。“节点”屏幕上的第二个位置为“全局显示板组”。当服务器的主机名包含的字符数超过 15 个时，该主机名将在“全局显示板组”中截短为 15 个字符。

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：更新在前一步骤中所描述的一个或多个字段时，“更新节点”对话框打开，以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。

删除节点

CA ARCserve Central Protection Manager 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”。

将节点导出到文件

使用 CA ARCserve Central Protection Manager，您可以使用凭据信息将选定节点组中的节点导出到 CSV 文件中。

将节点导出到文件

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. 选择要导出的“节点组”。

   将显示选定节点组的节点。

3. 单击“节点”工具栏上的“导出”。

   将显示一条消息，通知您该 CSV 文件将包含以纯文本形式显示的密码。

   单击“是”打开或保存 CSV 文件或单击“否”取消。

节点将导出到 CSV 文件中。

登录到 CA ARCserve D2D 节点

从 CA ARCserve Central Protection Manager 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。

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 Protection Manager 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 Protection Manager 服务器和 CA ARCserve Central Protection Manager 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。

状况	解决措施：
节点在 CA ARCserve Central Protection Manager 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 Protection Manager 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. 56)。
节点在 CA ARCserve Central Protection Manager 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. 118)。

合并作业选项

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

暂停节点上的合并作业

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

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

遵循这些步骤:

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“节点”打开“节点”屏幕。
2. 选择节点组，该组包含要暂停的合并作业的节点。

   将显示选定节点组的节点列表。
3. 单击要暂停的合并作业的节点。然后右键单击选定的节点，单击弹出式菜单中的“暂停合并作业”。

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

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

恢复节点上合并作业

通过 CA ARCserve Central Protection Manager，您可以恢复特定节点上已暂停的合并作业。

遵循这些步骤:

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“节点”打开“节点”屏幕。
2. 选择节点组，该组包含要恢复的合并作业的节点。

   将显示选定节点组的节点列表。
3. 单击已暂停现在又要恢复的合并作业的节点。然后右键单击选定的节点，单击弹出式菜单中的“恢复合并作业”。

   注意：备份作业未在运行且合并作业暂停时，“恢复合并作业”选项启用。

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

同步数据和选项

通过从 CA ARCserve Backup 主服务器 (asdb)、CA ARCserve D2D 或 Global Dashboard 中央主服务器 (central_asdb) 将信息传输到 CA ARCserve Central Protection Manager 数据库 (ARCAppDB)，CA ARCserve Central Protection Manager 可以同步每个节点的数据。

同步数据可以使得不同数据库中的数据保持一致和最新，因此中央站点数据库包含的信息与每个注册分支站点数据库的信息相同。

此部分包括以下主题

执行特定节点或节点组的 CA ARCserve Backup 数据的完全同步 (p. 61)
对特定节点或节点组执行 CA ARCserve Backup 数据的增量同步 (p. 62)
执行特定节点或节点组的 CA ARCserve D2D 数据的完全同步 (p. 63)

执行特定节点或节点组的 CA ARCserve Backup 数据的完全同步

CA ARCserve Central Protection Manager 允许您在特定节点或节点组上执行 CA ARCserve Backup 数据的完全同步。

在完全同步 CA ARCserve Backup 过程中，CA ARCserve Backup 数据库引擎将停止几分钟。此行为可以阻止任何 CA ARCserve Backup 作业信息的记录，直到数据库同步完成。

执行特定节点或节点组的 CA ARCserve Backup 数据的完全同步

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“节点”。

   “节点”屏幕将显示。

2. 选择您包含想要同步节点的节点组。

   将显示选定节点组的节点列表。

3. 执行以下操作之一：

   - 对于特定节点，从“组”右侧选择 CA ARCserve Backup 节点，然后从弹出菜单上单击“全面同步 CA ARCserve Backup”或从“节点”工具栏单击“同步数据”按钮。
   - 对于节点组，请右键单击节点组，然后在弹出菜单中单击“完全同步 CA ARCserve Backup”。

CA ARCserve Central Protection Manager 将提交选定节点或节点组的 CA ARCserve Backup 数据的完全同步。

对特定节点或节点组执行 CA ARCserve Backup 数据的增量同步

CA ARCserve Central Protection Manager 允许您在特定节点上执行 CA ARCserve Backup 数据的增量同步。

在执行最近一次同步之后，增量同步 CA ARCserve Backup 将同步修改、删除和添加的数据。同步的数据将在传输之前被压缩为最小大小。

对特定节点或节点组执行 CA ARCserve Backup 数据的增量同步

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“节点”。

   “节点”屏幕将显示。

2. 选择您包含想要同步节点的节点组。

   将显示选定节点组的节点列表。

3. 执行以下操作之一：

   - 对于特定节点，从“组”右侧选择 CA ARCserve Backup 节点，然后从弹出菜单上单击“增量同步 CA ARCserve Backup”或从“节点”工具栏单击“同步数据”按钮。
   - 对于节点组，请右键单击节点组，然后在弹出菜单中单击“增量同步 CA ARCserve Backup”。

CA ARCserve Central Protection Manager 将提交选定节点或节点组的 CA ARCserve Backup 数据的增量同步。

执行特定节点或节点组的 CA ARCserve D2D 数据的完全同步

CA ARCserve Central Protection Manager 允许您在特定节点或节点组上执行 CA ARCserve D2D 数据的完全同步。

执行特定节点或节点组的 CA ARCserve D2D 数据的完全同步

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“节点”。

   “节点”屏幕将显示。

2. 选择您包含想要同步节点的节点组。

   将显示选定节点组的节点列表。

3. 执行以下操作之一：

   - 对于特定节点，从“组”右侧选择 CA ARCserve D2D 节点，然后从弹出菜单上单击“全面同步 CA ARCserve D2D”或从“节点”工具栏单击“同步数据”按钮。
   - 对于节点组，请右键单击节点组，然后在弹出菜单中单击“完全同步 CA ARCserve D2D”。

CA ARCserve Central Protection Manager 将提交选定节点或节点组的 CA ARCserve D2D 数据的完全同步。

节点设置

CA ARCserve Central Protection Manager 允许您为每个 CA ARCserve Backup 或全局显示板中央主节点设置本地排定，从而可以执行增量备份。

应用 CA ARCserve Backup 数据同步排定

CA ARCserve Backup 设置允许您为每个 CA ARCserve Backup 节点设置自定义排定。

应用 CA ARCserve Backup 数据同步排定

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“节点”。

   “节点”屏幕将显示。

2. 从组列表中选择节点组，该组列表包含您想应用 CA ARCserve Backup 设置的目标节点。

   将显示选定节点组的节点列表。

3. 选择要应用该设置的节点，然后从弹出菜单单击“CA ARCserve Backup 数据同步排定”。

   “CA ARCserve Backup 数据同步排定”对话框将打开。

4. 选择下列选项之一：
   - **启用** -- 允许您通过输入重复方式和排定时间来指定排定选项：
     - 每隔天数
     - 每周选定的某天
     - 每月选定的某天
   - **禁用** -- 使用此选项，将不应用任何设置。
   - **使用全局** -- 允许您应用在 CA ARCserve Backup 配置模块中配置的全局设置。有关详细信息，请参阅“CA ARCserve Backup 数据同步排定”。
5. 单击“确定”。

将应用 CA ARCserve Backup 设置。

您使用节点组可以做什么

CA ARCserve Central Protection Manager 允许您使用该功能创建节点组，将单个节点分配到每个组，修改和删除节点组。

注意：您仅可以修改和删除您创建的节点组。

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。
- **vCenter/ESX 组**－通过“从 vCenter/ESX 导入虚拟机”选项添加节点时，vCenter/ESX 服务器的名称将添加到该组。
- **全局显示板组**－包含与中央主服务器关联的所有节点。

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。

注意：当您将 CA ARCserve Backup 全局显示板节点分配给节点组时，即使所有分支都不属于该节点组，所有 CA ARCserve Backup 分支也都会呈现到 CA ARCserve Backup 全局显示板节点。因此，当您选择在 CA ARCserve Central Reporting 应用程序中包含 CA ARCserve Backup 全局显示板节点的节点组时，报告将不显示来自全局显示板节点的所有分支的数据。

删除节点组

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

该应用程序使您可以删除已创建的节点组。

您不能删除以下节点组：

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

注意：删除节点组的过程不会从应用程序中删除单个节点。

遵循这些步骤:

1. 登录该应用程序。

   从主页上的导航栏中，单击“节点”打开“节点”屏幕。
2. 单击要删除的节点组，然后单击“节点组”工具栏中的“删除”。

   “确认”消息对话框打开。
3. 如果确定要删除该节点组，请单击“是”。

   注意：如果您不想删除该节点组，请单击“否”。

节点组即被删除。

使用发现搜索节点

CA ARCserve Central Protection Manager 允许您使用发现搜索节点。Protection Manager 基于保留在服务器 Active Directory 中的信息搜索节点。Active Directory 提供以下信息：

- 计算机名
- 操作系统信息（名称、版本、修补程序）
- 如果计算机上有 Microsoft Exchange Server
- 如果计算机上有 Microsoft SQL Server

使用发现搜索节点

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. 在“节点”类别中，单击“发现”以打开“按 Active Directory 发现”对话框。

3. 在“按 Active Directory 发现”对话框中填写以下字段，然后单击“添加”：

   - （域）用户名
   - （域）密码
   - 计算机名筛选

   单击“发现”。

   发现过程 (p. 51)将开始。

4. 当发现完成时，将显示以下确认消息：

   是否要继续从发现结果添加节点?

   执行以下操作之一：

   - 单击“是”将转到“从发现结果添加节点”。
   - 单击“否”关闭该消息。

   注意：如果选择“是”，请参阅使用发现添加节点 (p. 50)了解详细信息。

CA ARCserve D2D 部署任务

CA ARCserve Central Protection Manager 允许您远程或从本地将一个或多个节点同时部署到目标系统。此外，您还可以添加或编辑部署中的节点或从部署中删除节点。

本节包括以下主题：

将 CA ARCserve D2D 部署到节点

CA ARCserve Central Protection Manager 可让您发现最新版本的 CA ARCserve D2D，并将其部署至一个或多个新的或现有节点。

注意：要将 CA ARCserve D2D 部署到运行 Windows XP 的计算机，请禁用远程 Windows XP 计算机上的“使用简单文件共享”选项。

遵循这些步骤:

1. 登录到应用程序，并单击导航栏上的“节点”。
2. 在“节点”屏幕上，单击工具栏上的“部署”。

   “许可协议”对话框将打开。
3. 阅读并接受本许可协议的条款，然后单击“下一步”打开“D2D 部署”对话框。
4. 从“D2D 部署”对话框中，为基于通用标准的可用节点指定组和节点名称筛选。

   针对每个节点的“名称”、“版本”和“状态”现已显示。

   注意：“版本”列显示节点正在运行的当前 D2D 版本。
5. 单击这些节点旁边的复选框，或者针对已列出要部署 D2D 的所有节点单击“全选”。

   注意：单击“全选”后，该选项将变成“取消全选”，以便于您的操作。此外，如果从节点列表中选择了节点，您可以从“节点信息”选项卡编辑相应的节点字段。
6. 单击“立即部署”，将标题栏上显示的最新 D2D 版本部署至这些节点。

   注意：有关特定节点上的信息和部署状态，请突出显示节点，然后从右侧窗格选择相应的选项卡。

注意：CA ARCserve Central Protection Manager 可让您使用 D2D 部署实用工具安装、升级 CA ARCserve D2D 并将其最新版本部署至较低的版本或未安装 CA ARCserve D2D 的节点。

添加节点进行部署

CA ARCserve Central Protection Manager 允许添加多个节点进行部署。

添加节点进行部署

1. 登录到应用程序，并单击导航栏上的“节点”。
2. 在“节点”屏幕上，单击工具栏上的“部署”。

   “许可协议”对话框将打开。

3. 阅读并接受本“许可协议”的条款，然后单击“下一步”。

   “D2D 部署”对话框打开。

4. 单击“添加”，然后在“D2D 部署”对话框中完成以下字段：

   - 服务器名
   - 用户名
   - 密码
   - 端口
   - 安装路径
   - 允许设置安装驱动程序（默认选定）
   - 重新启动（默认为“是”）

     如果该节点使用成功的重新启动（是）进行部署，则该节点将添加到 CA ARCserve Central Applications 管理的节点列表中。

     如果该节点没有使用重新启动选项（否）进行部署，则该节点将添加到不受 CA ARCserve Central Applications 管理的节点组。

   - 使用 HTTPS（默认为“否”）

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

   注意：您可以查看“全部节点”和“未分组”组节点下添加的节点。

5. 单击“确定”添加节点。

编辑节点进行部署

CA ARCserve Central Protection Manager 允许您编辑节点进行部署。

编辑节点进行部署

1. 登录到应用程序，并单击导航栏上的“节点”。
2. 在“节点”屏幕上，单击工具栏上的“部署”。

   “许可协议”对话框将打开。

3. 阅读并接受本“许可协议”的条款，然后单击“下一步”。

   将显示“D2D 部署”屏幕。

4. 选择要编辑以便进行部署的节点，然后单击“编辑”打开“编辑”对话框。
5. 在“编辑”对话框中，编辑想要更改的数据，然后单击“确定”。

从部署删除节点

CA ARCserve Central Protection Manager 允许从部署删除一个或多个节点。

从部署删除节点

1. 登录到应用程序，并单击导航栏上的“节点”。
2. 在“节点”屏幕上，单击工具栏上的“部署”。

   “许可协议”对话框将打开。
3. 阅读并接受本“许可协议”的条款，然后单击“下一步”。

   将显示“D2D 部署”屏幕。
4. 从部署选择一个或多个节点进行删除。
5. 单击“删除”从 D2D 部署中删除节点。

筛选节点组

CA ARCserve Central Protection Manager 允许您使用筛选将安装了特定应用程序的节点显示在一个组中。CA ARCserve Central Protection Manager 允许筛选以下应用程序：

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

筛选节点组

1. 登录 CA ARCserve Central Protection Manager。

   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。

如何管理 CA ARCserve D2D 策略

CA ARCserve Central Protection Manager 提供了可用来管理 CA ARCserve D2D 策略的各种工具和选项。本节介绍了如何在远程服务器添加、删除、修改和部署 D2D 以及复制策略。您可以创建集中的备份策略，可同时分发给多个受管理的节点。

下面是一些集中备份策略的通用示例：

- 排定
- 作业
- 目标
- 事件
- 设置

本节包括以下主题：

创建策略

CA ARCserve Central Protection Manager 允许您创建一个或多个分配到 D2D 节点的策略。

遵循这些步骤:

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”打开“策略”屏幕。
2. 单击“新建”以打开“新建策略”对话框。
3. 在“备份设置” (p. 75)、“文件复制设置” (p. 90)、“复制恢复点” (p. 103)和“首选项” (p. 106)选项卡中输入“策略名称”并完成必填的字段。
4. 单击“保存”。

您想现在将策略分配给节点时，新策略将被保存并且提示消息。单击“否”，新策略在“策略”屏幕上显示。单击“是”，“分配/取消分配策略 (p. 119)”屏幕打开。

管理备份设置

备份设置允许您定义诸如以下行为，备份的源和目标、每个备份类型的排定，以及备份作业的设置和高级设置。这些设置可以随时通过“策略”屏幕修改。

要管理备份设置，请单击主页上导航栏中的“策略”，然后单击“新建”。

本节包括以下主题：

指定保护设置

CA ARCserve Central Protection Manager 允许您为要备份的数据指定保护设置。

指定扫描设置

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   “新建策略”对话框将打开，显示“备份设置”选项卡的“保护设置”选项。

3. 指定**备份目标**。

   您可以指定一个本地路径（卷或文件夹），或者远程的共享文件夹（或映射驱动器）作为备份位置。

   a. 如果您指定备份到本地路径（卷或文件夹），指定的备份目标则不能与备份源的位置相同。如果您无意中在目标中包括源，备份作业将忽略源的部分并不会在备份中包括它。

例如，如果您尝试备份由卷 C、D 和 E 构成的整个本地计算机，并还指定卷 E 作为您的目标，CA ARCserve D2D 则仅会将卷 C 和 D 备份到卷 E。来自卷 E 的数据不会包含在备份中。如果想备份所有的本地卷，请为目标指定一个远程位置。

重要说明！确认您指定的目标卷不包含系统信息，否则它将不受保护（备份），而您的系统在必要时将无法在裸机恢复 (BMR) 之后恢复。

注意：动态磁盘无法以磁盘级别还原。如果您的数据已备份到动态磁盘的卷上，则在 BMR 期间将无法还原该动态磁盘。

b. 如果您选择备份到远程共享位置，则您必须指定一个位置路径，或浏览到该位置，并提供用户凭据（用户名和密码）来访问远程计算机。

c. 如果自上次执行备份以来，指定的备份目标已经更改，您将需要选择备份类型。当您更改备份目标时，这些选项将启用。可用的选项是“完全备份”和“增量备份”。

- **完全备份 --** 指定执行的下一个备份将是完全备份。新的备份目标对旧的备份目标没有任何依存关系。如果您继续进行完全备份，不再需要前一个位置即可继续备份。您可以选择保留旧的备份以进行任何还原，或者如果您不想从旧的备份执行任何还原，则将其删除。它不会影响未来的备份。
- **增量备份 --** 指定执行的下一个备份将是增量备份。到新目标的下一个增量备份将在不从前一个目标复制所有备份的情况下执行。但是，新的位置依赖于前一个位置，因为更改将仅包括增量数据（而不是完全备份数据）。不要删除前一个位置中的数据。如果您将备份目标更改为其他文件夹并尝试执行增量备份，而以前的备份目标不存在，备份将会失败。

4. 指定**备份源**。

您可以指定备份整个计算机或计算机上的单个卷。

- **备份整个机器 --** 指定以备份整个机器。计算机上的所有卷都将得到备份。

  注意：如果选择了整个计算机备份选项，CA ARCserve D2D 将自动发现连接在当前计算机上的所有磁盘/卷，并且将其包括在备份中。

  例如，如果新磁盘在配置了备份设置之后连接到计算机，您将无需更改备份设置，将会自动保护新磁盘上的数据。

- **选择要备份的单个卷 --** 该卷筛选功能允许您指定仅备份选定的卷。然而，如果您指定在远程 CA ARCserve D2D 服务器上不存在的卷，则在备份期间自动跳过该卷。例如，指定备份卷 C、D 和 E；将其分配给仅包含卷 C 和 D 的 CA ARCserve D2D 服务器。该策略被分配给在 CA ARCserve D2D 服务器上的卷 C 和 D，将跳过卷 E，且一条警告消息将保存在活动日志中。

  您还可以选择/取消选择所有列出的卷。

  注意：如果某些卷被明确地选择进行备份，则将仅备份选定的卷。

  将为下列条件显示通知消息：

  - **BMR 相关 --** 如果未选择系统/启动卷进行备份，将显示警告消息，通知您该备份不能用于 BMR。

5. 指定**保留设置**。

   您可以根据要保留的恢复点数量（合并会话）或根据要保留的恢复集数量（删除恢复集并禁用无限增量）来设置保留策略。

   - 恢复点－这是建议选项。选择此选项后，可以充分利用无限增量备份功能并节省存储空间。
   - 恢复集－此选项通常用于大型存储环境。选择此选项后，可以创建和管理备份集，从而在您保护大量数据时，帮助您更高效地管理备份持续时间。当对备份时间的要求优先于空间限制时，您可以使用此选项。

   默认：保留恢复点

保留恢复点

选择此选项，指定要保留的恢复点（完全备份、增量备份，并检验备份映像）数量。

- **指定要保留的恢复点数目**

  当超过指定的限制时，CA ARCserve D2D 会将最早（最旧）的增量子备份合并为父备份以创建包括“父项加最早子项”块的基准映像。将最早子项备份合并到父备份的循环将重复应用于每个后续的备份，这将允许您执行无限的增量备份，同时维护相同的保留计数。

  注意：如果您的目标没有足够的可用空间，请考虑减少保存的恢复点数目。

  默认值：31

  最小值：1

  最大值：1344

- **运行合并作业** -- 选择何时运行合并作业的以下选项之一：
  - **尽快** -- 选择此选项在任何时候运行合并作业。
  - **以下时间范围期间的每一天** -- 选择此选项在指定时间范围内运行合并作业。设置时间范围有助于在合并作业运行长时间时避免将过多输入/输出操作引入给生产服务器。

    注意：在设置运行合并作业的时间范围时，确保您指定的时间范围在合并开始之前将允许相关的备份作业完成。

保留恢复集

选择此选项指定要保留的恢复集数量。使用此设置，您可以永久禁用无限增量备份，而无需合并任何会话。使用恢复集有助于解决完成合并作业所需的时间。

- **指定要保留的恢复集数目**

  选择此选项指定已保留的恢复集数量。恢复集是一系列备份，始于完全备份，然后是一系列的增量、检验或完全备份。

  示例集 1：

  - 完全
  - 增量
  - 增量
  - 验证
  - 增量

  示例集 2：

  - 完全
  - 增量
  - 完全
  - 增量

  要开始新的恢复集，需要一个完全备份。即使没有配置或排定要在指定时间执行的完全备份，也会将启动集的备份自动转变为完全备份。

  注意：计算现有恢复集时，不会计算不完整恢复集。仅当创建了下一个恢复集的起始备份时，才认为该恢复集为完整恢复集。

  默认值：2

  最小值：1

  最大值：100

注意：要删除恢复集以节省备份存储空间时，请减少保留集的数目，CA ARCserve D2D 会自动删除最旧的恢复集。不要尝试手动删除恢复集。

示例 1 - 恢复集：

- 备份开始时间为 2012 年 8 月 20 日上午 6 点。
- 增量备份每 12 小时运行一次。
- 新的恢复集于星期五的最后一次备份时开始。
- 要保留三个恢复集。

在此示例中，增量备份在每天的上午 6 点和下午 6 点运行。采用第一个备份（必须为完全备份）时将创建第一个恢复集。然后，第一个完全备份将标记为恢复集的起始备份。运行排定在星期五下午 6 点的备份时，它转变为完全备份，且将该备份标记为恢复集的开始备份。

示例 2 - 恢复集：

- 将要保留的恢复集数目指定为 1。

注意：CA ARCserve D2D 总是保持两个集，以便在开始下一恢复集之前，保留一个完整集。

示例 3 - 恢复集：

- 将要保留的恢复集数目指定为 2。

注意：在第四个恢复集即将开始时，CA ARCserve D2D 会删除第一个恢复集。执行此操作可确保在删除首次备份且第四个恢复集正在开始时，您仍然有两个恢复集（恢复集 2 和恢复集 3）在磁盘上可用。

即使仅保留一个恢复集，您也将需要至少两个完全备份的空间。

- **在以下间隔开始新的恢复集：**
  - **每周选定的某天** -- 指定选定用于开始新的恢复集的周内某日。
  - **每月选定的某天** -- 指定选定用于开始新的恢复集的月内某日。指定 1 到 30 或如果月中有 28、29、30 或 31 天，您可以指定月内最后一天作为创建恢复集的日子。
- **使用以下选项开始新的恢复集：**
  - **选定日的首次备份** -- 指定选定用于开始新的恢复集的周内某日。
  - **选定日的最后一次备份** -- 表示在指定日使用最后的排定备份开始新的恢复集。如果选择了最后一次备份来开始恢复集，但由于某种原因最后一次备份未能运行，则下一个排定备份会转换为完全备份从而开始恢复集。如果下一次备份临时运行（例如因紧急情况需要执行快速增量备份），您可以决定是要运行完全备份来开始恢复集，还是运行增量备份而通过下一次备份开始恢复集。

    注意：最后一次备份可能不是运行临时备份当天的最后一次备份。

6. 指定**压缩**类型。

   选择该选项指定要用于备份的压缩类型。

   压缩会减少对磁盘空间的占用，而且还可以抵消由于对 CPU 越来越多的占用而导致的对备份速度的负面影响。

可用的压缩选项如下：

- **无压缩**

  未执行压缩。此选项的 CPU 使用率最低（速度最快），但是对于您的备份映像而言，磁盘空间占用最大。

- **标准压缩**

  已执行某些压缩。此选项将会在 CPU 使用率和磁盘空间占用之间实现良好的平衡。这是默认设置。

- **最大压缩**

  已执行最大压缩。此选项提供最高的 CPU 使用率（速度最慢），但是对于备份映像而言，磁盘空间占用最低。

请注意以下情况：

- 如果您的备份映像包含不可压缩的数据（如 JPG 图像、ZIP 文件等），则需要分配额外的存储空间处理此类数据。如果您指定压缩选项，并且备份源包含无法压缩的数据，您将会注意到磁盘空间使用率的整体提升。
- 如果您将压缩级别从无压缩更改到标准或最大压缩；或者，如果您将压缩级别从标准或最大压缩更改为无压缩，则压缩级别更改之后首次执行的备份将是完全备份。在完全备份完成后，所有未来的备份（完全、增量或验证）将按排定执行。
- 如果您的目标没有足够的可用空间，请考虑提高备份的压缩设置。

7. 指定**加密**设置。

   a. 选择要用于备份的加密算法类型。

      数据加密将数据转换为需要有解码机制才可识别的格式。CA ARCserve D2D 数据保护使用安全的 AES（高级加密标准）加密算法实现指定数据的最佳安全性和隐私。

      可用的格式选项是“不加密”、AES-128、AES-192 和 AES-256。（要禁用加密，请选择“不加密”）。

      - 完全备份及其所有的相关增量以及验证备份必须使用相同的加密算法。
      - 如果增量备份或验证备份的加密算法有所更改，则必须执行完全备份。这意味着在更改加密算法之后，不管初始的备份类型如何，首次备份都将是完全备份。

        例如，如果您更改算法格式并手工提交自定义的增量或验证备份，它将自动转变为完全备份。

b. 当选择加密算法时，您必须提供（并确认）加密密码。

- 加密密码限制为最多 23 个字符。
- 完全备份及其所有的相关增量以及验证备份必须使用相同的密码来加密数据。
- 如果增量备份或验证备份的加密密码有所更改，则必须执行完全备份。这意味着在更改加密密码之后，不管初始的备份类型如何，首次备份都将是完全备份。

  例如，如果您更改加密密码并手工提交自定义的增量或验证备份，它将自动转变为完全备份。

c. CA ARCserve D2D 提供了加密密码管理，这样您就无需记得加密密码。

- 密码也将被加密。
- 如果您还原到同一计算机，密码将被记住并无需提供。
- 如果您还原到其他计算机，则需要密码。
- 如果您正在尝试导出包含加密数据的恢复点，而该恢复点属于当前计算机上执行的备份，则不需要密码。
- 如果您正在尝试从已导出的恢复点恢复加密数据，则总是需要密码。
- 无需密码即可浏览到加密的恢复点。
- 需要密码来执行 BMR。

d. 当启用加密时，活动日志将被更新。

- 将在活动日志中记录消息以便说明每个备份的选定加密算法。
- 将在活动日志中记录消息来表明增量备份或验证备份转变为完全备份的原因（密码更改或算法更改）。

注意：您的备份的加密设置不必保持相同。您可以随时更改这些设置，包括在几次备份同样的数据之后。

8. 指定**调节备份**。

   您可以指定写入备份的最大速度（MB/分钟）。您可以调节备份速度以减少 CPU 或网络使用率。然而，通过限制备份速度，将对备份窗口有负面影响。降低最大备份速度后，将增加执行备份所用的时间。

   注意：默认情况下，不会启用“调节备份”选项，而备份速度不受控制。

9. 单击“保存”。

保存设置即被保存。

指定备份排定

CA ARCserve Central Protection Manager 允许您指定备份的排定。

指定备份排定

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

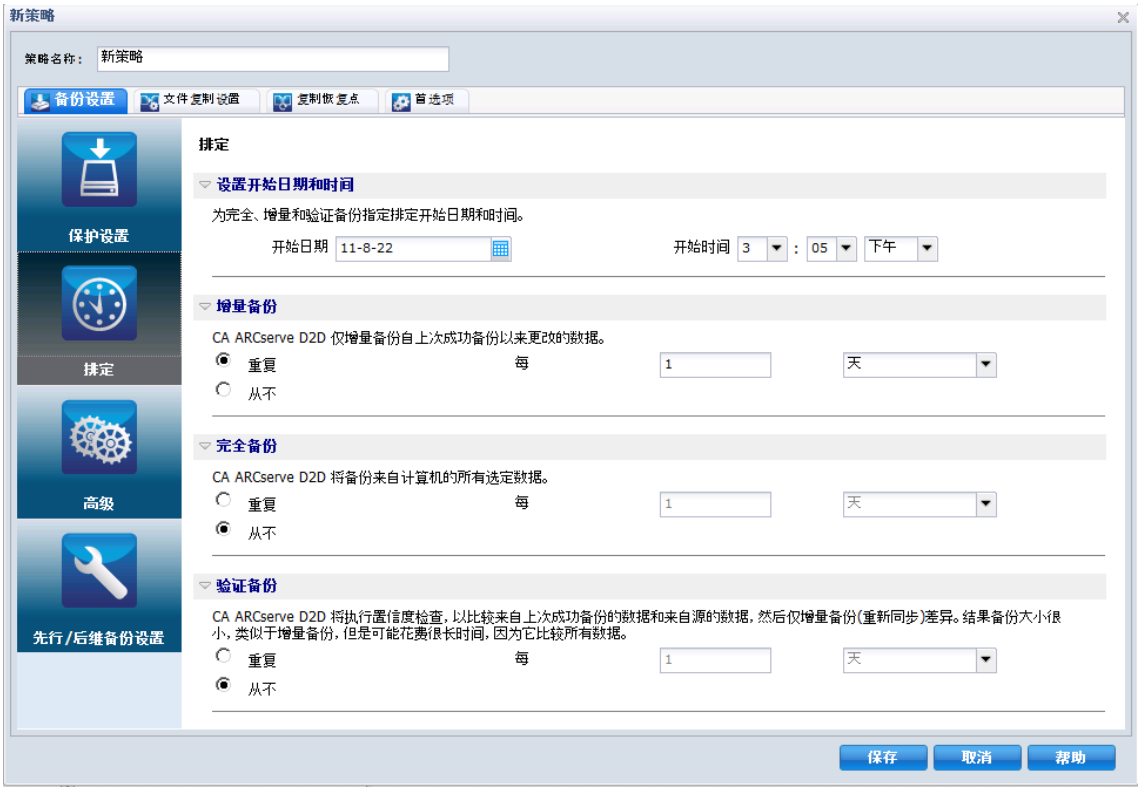
   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 单击“排定”选项卡，

   此时将打开“排定选项”对话框。



4. 指定您的备份排定选项：

   - **设置开始日期和时间** -- 指定排定备份的开始日期和开始时间。

     注意：在设置重复备份作业之间的间隔时，确保您留有足够的时间以允许在下一个备份作业开始之前，完成先前的作业和任何相关的合并作业。此时间量可根据自身的特定备份环境和历史进行预估。

   - **增量备份** -- 指定增量备份的备份排定。

     按照排定，CA ARCserve D2D 仅增量备份自上次成功备份以来更改的块。增量备份的优势在于，备份非常快，并只生成非常小的备份映像。这是执行备份的最理想方式，而您应当默认使用此选项。

     可用的选项是“重复”和“从不”。如果选择“重复”选项，则您必须也指定备份尝试之间经过的时间段（以分钟、小时或天为单位）。增量备份的最小设置为每 15 分钟一次。

     默认情况下，增量备份排定是每 1 天重复一次。

   - **完全备份** -- 指定完全备份的备份排定。

     按照排定，CA ARCserve D2D 会对源计算机中所有使用的块进行完全备份。可用的选项是“重复”和“从不”。如果选择“重复”选项，则您必须也指定备份尝试之间经过的时间段（以分钟、小时或天为单位）。完全备份的最小设置为每 15 分钟一次。

     默认情况下，完全备份的排定是“从不”（无排定的重复）。

   - **验证备份** -- 验证完全备份的备份排定。

     按照排定，CA ARCserve D2D 将通过对原始备份源执行已存储备份映像的可信度检查来验证受保护数据是否有效和完整，并在必要时重新同步该映像。验证类型备份将关注每个块的最新备份，并将内容和信息与源进行比较。这种对比将确认最新备份的块代表源的相应信息。如果任何块的备份映像与源（可能是因为自上次备份以来的系统更改）都不匹配，则 CA ARCserve D2D 将刷新（重新同步）不匹配块的备份。验证备份还可以（很少）用于获得完全备份的保证，而不占用完全备份的空间。

     验证备份的优势是，与完全备份相比，它生成的备份映像很小，因为仅备份更改的块（与上次备份不匹配的块）。验证备份的劣势是，备份时间较长，因为 CA ARCserve D2D 必须将所有源磁盘块与上次备份的块进行比较。

     可用的选项是“重复”和“从不”。如果选择“重复”选项，则您必须也指定备份尝试之间经过的时间段（以分钟、小时或天为单位）。验证备份的最小设置为每 15 分钟一次。

     默认情况下，验证备份的排定是“从不”（无排定的重复）。

5. 单击“保存”。

备份排定设置即被保存。

注意：如果在某一特定时刻，排定了同时执行多种类型的备份，那么将执行的备份类型基于以下优先级：

- 优先级 1 - 完全备份
- 优先级 2 - 验证备份
- 优先级 3 - 增量备份

例如，如果您排定所有三种类型的备份同时执行，CA ARCserve D2D 将执行完全备份。如果没有排定完全备份，但是排定同时执行验证备份和增量备份，CA ARCserve D2D 将执行验证备份。仅当没有与任何其他备份类型有冲突时，才会执行排定的增量备份。

指定高级备份设置

CA ARCserve Central Protection Manager 允许您指定备份的高级设置。

指定高级备份设置

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 单击“高级”选项卡。

   此时“高级设置”选项对话框打开。

4. 指定高级操作设置选项。

   - **截短日志** -- 指定在下一个成功备份之后为选定的应用程序截短积累的事务日志文件。

     CA ARCserve D2D 备份包括为其创建的快照映像和事务日志文件。在某个时间点上，不再需要较旧（已提交）的事务日志文件，可以将其清除以便为新的日志文件提供空间。清除这些日志文件的过程被称为截短日志。该选项能够截短已提交的事务日志文件，这会节约磁盘空间。

     可用的选项是“SQL Server”和“Exchange Server”。您可以选择其中一项、两项或不选择这些应用程序。如果选择任意应用程序，您还可以指定自动日志截短的排定时间段（每日、每周或每月）：

     注意：在没有执行成功备份的情况下，无法截短事务日志文件。

     - **每日** -- 在备份成功完成后的每一天，都将会立即清理已提交的事务日志。
     - **每周** -- 在备份成功完成后的 7 天之后，将会立即清理已提交的事务日志。
     - **每月** -- 在备份成功完成后的 30 天之后，将会立即清理已提交的事务日志。

     如果在排定执行清理的同时已经在运行某备份作业，清理操作会移至下一个排定作业。

     例如：

     如果您排定增量备份在每天下午 5:00 自动运行，并且在下午 4:55 手动启动完全备份，则假定备份在下午 5:10 成功结束。

     在这种情况下，排定在下午 5:00 的增量备份将被跳过，因为临时的完全备份仍在进行中。现在，已提交事务日志文件将在下一个成功备份作业之后进行清除。在这种情况下，将会在排定增量备份在下午 5:00 成功完成之后的第二天执行该清除。

- **目标上的保留空间**

  此值表示执行备份所需的计算空间百分比。该持续空间量会即刻在目标上得到保留，然后备份才开始写数据，这将有助于提高备份速度。

  默认值：10%。

  示例：将该值设置为 50%，当前备份需要备份 50 GB 的数据。在备份开始写数据之前，其首先保留 5 GB 的磁盘空间。5 GB 磁盘空间用完后，其则将再保留 5 GB 的磁盘空间。如果要备份的剩余数据少于 5 GB（假设还剩 2 GB 要备份），则剩余的 GB （在该示例中为 2 GB）将被保留。

- **编录**

  Exchange 粒度还原编录

  当选择此选项时，在每次备份之后能够自动生成 Exchange 粒度还原编录。默认情况下，启用了该选项。

  “Exchange 粒度还原”备份捕获整个 Exchange 数据库的一次性备份中 Exchange 的邮件消息、邮件文件夹和邮箱级别的相关信息。启用该选项后，您可以通过从 Exchange 内的对象列表进行选择并指明您要恢复的内容来执行 Exchange 数据库的粒度恢复，而无需先将 Exchange 数据库恢复或转储到备用位置。

  优势：使用 Exchange 粒度还原编录，无需等待很长时间即可执行还原浏览。

  劣势：当在每次备份期间生成 Exchange 粒度还原编录时，都会增加备份窗口（完成备份作业的额外时间）以及工作负荷。CA ARCserve D2D 必须进入每一个邮箱，验证并生成粒度信息，考虑到邮箱数量和数据大小，这会是一个比较耗时的任务。

  注意：如果禁用此选项，CA ARCserve D2D 将只保存 Exchange 的常规信息。在还原之前，您还可以在该时间生成 Exchange 粒度还原编录。

文件系统编录

当选择了此选项时，其能够生成文件系统编录。如果您的浏览时间过慢（特别是如果 CA ARCserve D2D 目标在 WAN 上），或如果按搜索还原的时间过慢，此选项帮助减少您的等待时间。在选择了此选项之后，此编录作业将为每个排定备份作业运行。

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

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

- **管理员帐号 --** 指定有权执行备份的用户名和密码。CA ARCserve D2D 将确认名称和密码有效且该用户属于管理员组。

  请注意以下问题：

  - 要指定域帐号，用户名的格式为完全限定的域用户名，格式为“<domain name>\<user name>”。
  - 如果 CA ARCserve D2D 服务器的“管理员帐户”信息被更改（用户名/密码），则推荐重新配置该对话框中的“管理员帐号”信息。
  - 如果您不指定“管理员帐号”凭据，则 CA ARCserve D2D 将在部署策略的位置自动输入帐号信息。

5. 单击“保存”。

高级备份设置即被保存。

指定先行/后继备份设置

CA ARCserve Central Protection Manager 允许您指定备份的设置。

指定先行/后继备份设置

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 单击“先行/后继备份设置”选项卡。

   “先行/后继备份设置选项”对话框打开。

4. 指定您的备份设置选项。
   - **操作 --** 指定为备份开始之前、捕获快照映像之后和/或备份完成时采取的操作运行脚本命令。您还可以基于特定的退出代码触发脚本命令，并选择该退出代码返回时采取的操作（运行作业或让作业失败）。
     - 如果返回了指定的退出代码，“运行作业”操作会让 CA ARCserve D2D 继续运行作业。
     - 如果返回了指定的退出代码，“让作业失败”操作会让 CA ARCserve D2D 取消作业。
5. 单击“保存”。

您的先行/后继备份设置即被保存。

管理文件复制设置

在执行第一个文件复制作业之前，您必须指定文件复制设置和策略。这些配置允许您指定以下行为，如，应用于文件复制作业的文件复制数据的源、复制文件的目标、每个文件复制作业的排定，以及设置和筛选。这些设置可以随时通过“策略”屏幕修改。

指定文件复制源

CA ARCserve Central Protection Manager 允许您将要执行文件复制的源文件指定到特定目标。

指定文件复制源

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。
2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。
3. 选择“文件复制设置”选项卡。

   “文件复制设置源”对话框将打开。
4. 选择“启用文件复制”选项来验证和保存文件复制设置的任何更改。默认情况下，该选项被禁用。

5. 指定您的文件复制源设置。

文件复制源

允许您在每次成功备份 CA ARCserve D2D 之后手动指定文件复制源和相应的策略（筛选）以及要执行的文件复制类型（复制并保留或复制并移动）。这些文件复制源可以添加、删除或修改。

注意：CA ARCserve D2D 将不复制应用程序文件、具有系统属性的文件和具有临时属性的文件。

- **添加源**

  单击时，“策略类型”对话框将打开，允许您选择将要执行（复制和保留，或复制和移动）的文件复制作业类型。在您选择策略类型之后，相应的“文件复制策略”对话框将打开，允许您添加要复制的源，并指定该源的相应策略。有关详细信息，请参阅指定文件复制策略 (p. 91)。

  注意：仅当前的备份源符合条件进行文件复制。您不能从之前没有经过 CA ARCserve D2D 备份的卷中添加源。

- **删除**

  单击将从该显示列表中删除选定的源。

- **修改**

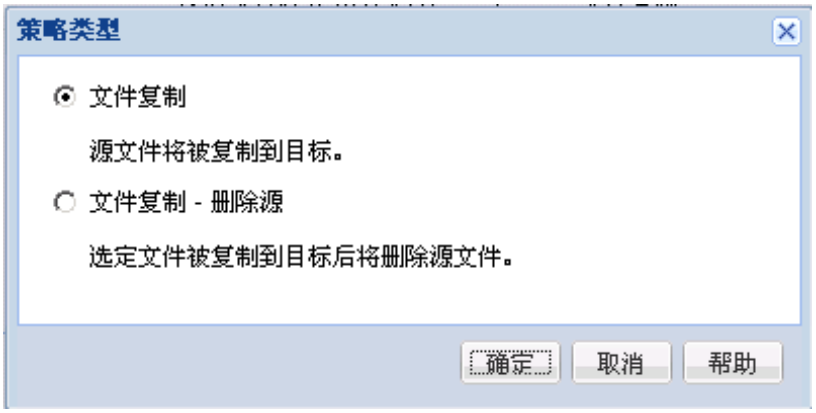
  单击时，“文件复制策略”对话框将打开，允许您为选定的源更改策略设置。有关详细信息，请参阅指定文件复制策略 (p. 91)。

6. 单击“保存设置”。

文件复制设置即被保存。

指定文件复制策略

当您单击“文件复制”的“添加源”选项时，“策略类型”对话框将打开，允许您初始选择将要执行的文件复制作业类型。



可用的类型是“文件复制”和“文件复制 - 删除源”。

文件复制

数据将从源复制到目标（保留在源位置）并提供多个存储版本。

文件复制 - 删除源

数据将从源移动到目标（从源位置删除），为源位置提供更多的可用空间。

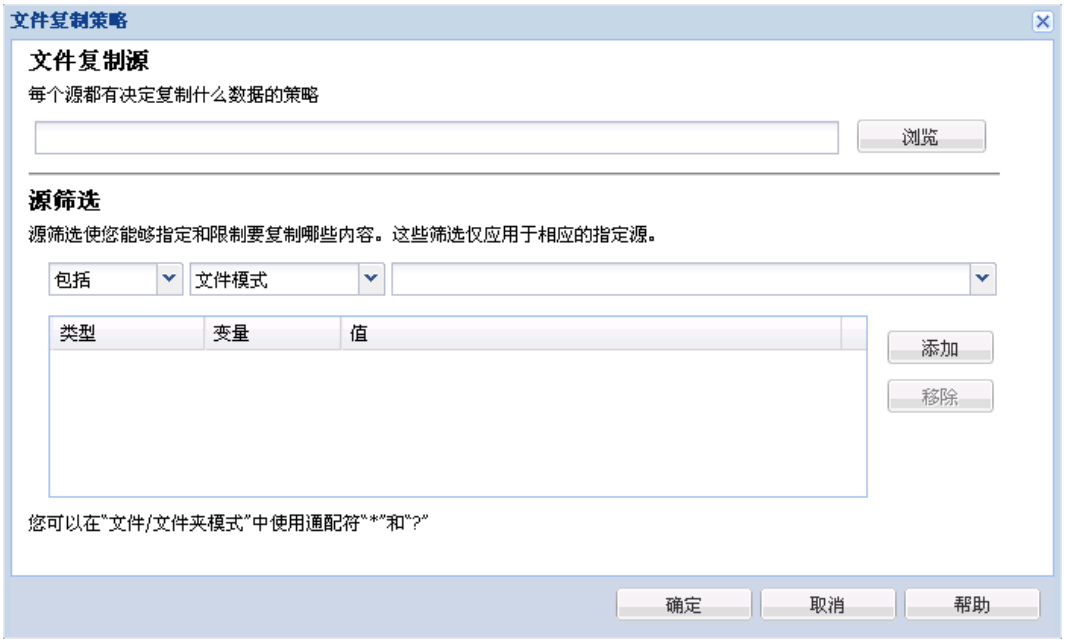
在您选择“文件复制 - 删除源”，将立即显示警告消息，提醒您的指定文件复制数据将删除，将不再初始源位置中可用。您需要单击“确定”才能进行到“文件复制策略”对话框。

重要说明！对于使用“文件复制 - 删除源”选项复制的文件，CA ARCserve D2D 将保留一个扩展名为“D2DARC”的存根文件。该存根文件将包含目标和文件移动时间的信息。

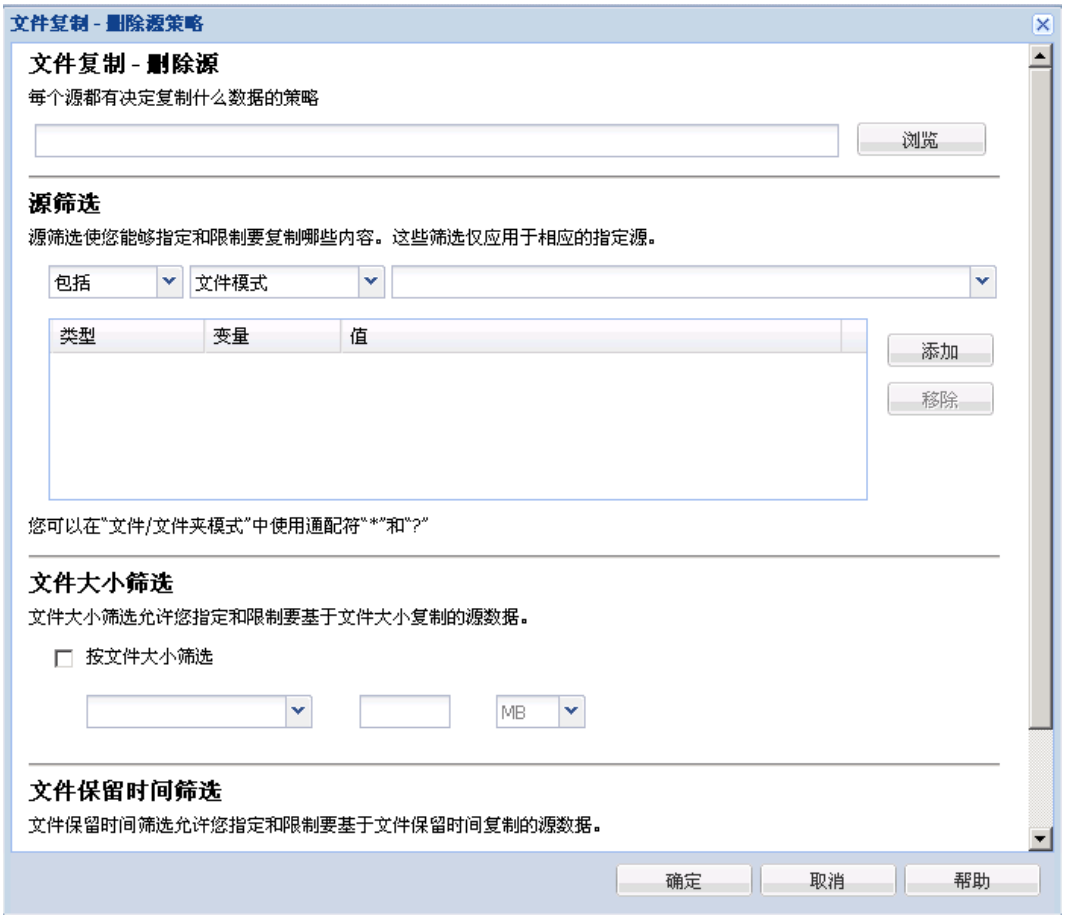
当您指定策略类型删除备份数据的源时，还需要指定相关策略。在“文件复制设置”对话框中，如果您想添加新的文件复制源，或修改现有文件复制源，则“文件复制策略”对话框允许您指定策略。

根据选定的策略类型，另外一个“文件复制策略”对话框将打开；但是，选择项是类似的。

已选择“文件复制”：



已选择“文件复制 - 删除源”：

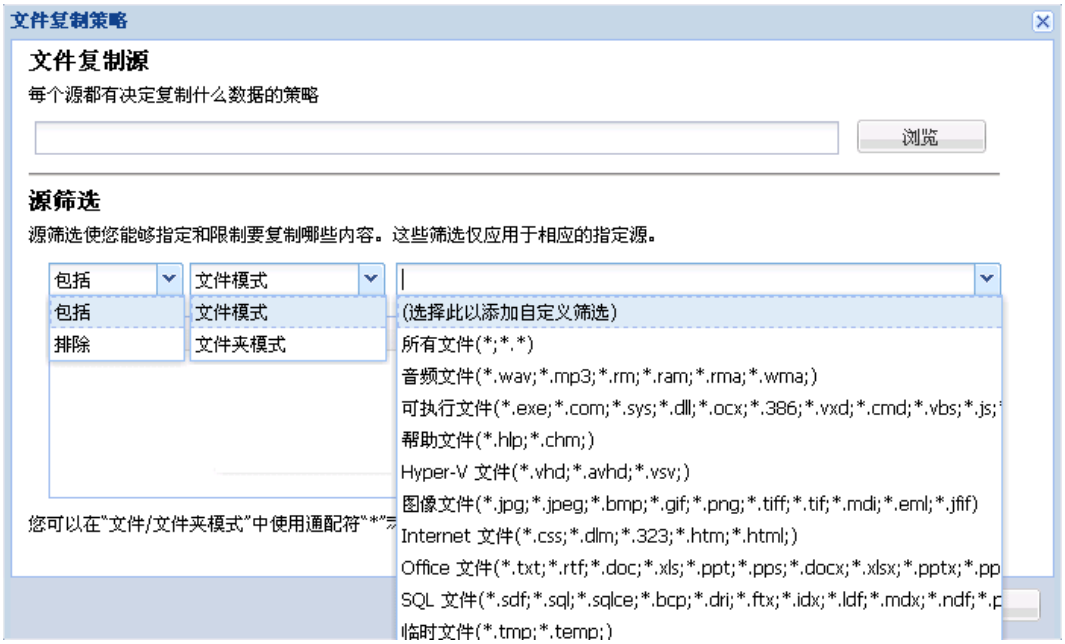


文件复制 - 删除源

允许您指定文件复制源，并设置执行文件复制的相应策略和文件复制类型。您可以浏览到源位置。

源筛选

筛选通过某些指定的类型和值，允许您限制要执行文件复制的对象。



筛选类型

有两种筛选类型：包括和排除。

“包括”筛选将仅对匹配指定值的文件复制源中的对象执行文件复制。

“排除”筛选将对匹配指定值之外的文件复制源中的所有对象执行文件复制。

通过使用逗号分隔每个筛选值，您可以在同一个文件复制请求中指定多个筛选。

- 指定多个“包括”筛选时，如果有任何一个“包括”筛选匹配，则数据将包含在文件复制中。
- 指定多个“排除”筛选时，如果有任何一个“排除”筛选匹配，则数据将排除在文件复制之外。
- 您可以在一个文件复制请求中混合“包括”和“排除”筛选。

注意：当“排除”和“包括”筛选中指定的参数冲突时，“排除”筛选始终具有更高的优先级，并将强制执行。“包括”筛选永远无法对一个已排除的对象执行文件复制。

筛选变量（模式）

有两种类型的变量模式筛选：“文件模式”和“文件夹模式”。

您可以使用“文件模式”或“文件夹模式”筛选将文件复制中的某些对象包括在内或排除在外。

筛选值

筛选值允许您限制执行文件复制的信息（通过仅选择您指定参数信息）如 .txt 文件。

CA ARCserve D2D 支持通配符，帮助在单个请求中选择多个对象进行文件复制。通配符是可代替单个字符或者一个文本串的特殊字符。

“值”窗口项中支持通配符星号 (*) 和问号 (?)。如果不知道完整的文件/文件夹模式值，您可以通过指定通配符来简化筛选结果。

- “*”- 使用星号可代替值中的 0 个或多个字符。
- “?”- 使用问号可代替值中的单个字符。

例如，如果不知道特定的文件名，您可以输入 *.txt 来排除扩展名为 .txt 的所有文件。您可以提供您知道的尽可能多的文件名，然后使用通配符填到空白处。

注意：当您选择“文件模式”作为筛选类型时，将会为许多常用文件（MS-Office 文件、图像文件、可执行文件、临时文件等）提供一个预定义筛选的下拉列表。

文件大小筛选（仅“文件复制 - 删除源”作业）

此筛选仅适用于“文件复制 - 删除源”作业（不是文件复制作业）。

文件大小筛选允许您根据文件大小限制要执行文件复制的源对象。当启用文件大小筛选时，您指定的参数将变成筛选，它将限制文件复制中包括的对象，以及不包括的对象。您可以选择范围（大于等于、小于等于，或介于之间），然后输入大小的值。

例如，如果您指定大于等于 10 MB，则 CA ARCserve D2D 仅对满足此条件的对象执行文件复制。所有不满足该文件大小条件的其他对象将不执行文件复制。

文件保留时间筛选（仅“文件复制 - 删除源”作业）

此筛选仅适用于“文件复制 - 删除源”作业（不是文件复制作业）。

文件保留时间筛选根据文件特定日期，允许您自动包括执行文件复制的源对象。您可以选择参数（未被访问的文件、未修改的文件和/或未创建的文件），然后为文件保留时间筛选输入年数、月数和天数。您选择多个文件保留时间筛选用于自动文件复制。

例如，如果您指定在 180 天后未修改的文件，那么 CA ARCserve D2D 将自动对所有满足此条件（在过去 180 天期间内没有修改）的文件执行文件复制。

重要说明！ 如果您同时指定文件大小和文件保留时间筛选（或多个文件保留时间筛选），那么仅对满足所有指定筛选参数的文件执行文件复制。不满足任何一个指定参数的文件将不执行文件复制。

指定“文件复制目标”

CA ARCserve Central Protection Manager 允许您为将要执行文件复制的信息指定目标设置。

指定“文件复制目标”

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 选择“文件复制设置”选项卡，然后选择“目标”以打开“文件复制设置目标”对话框。

4. 指定您的目标设置

   - **目标 --** 指定文件复制作业的目标位置。您只能选择一个目标。

     CA ARCserve D2D 允许您指定对备份文件执行文件复制的设置，目标为磁盘或云。对于文件复制，您可以指定执行复制和保持复制，以及备份数据的移动。两个过程是类似的（除了在您执行复制和移动时会有例外），数据将从源移动到目标（从源位置删除），在源中提供更多的可用空间。在您执行复制并保持时，数据将从源复制到目标（保留在源目标），并且提供多个存储版本。

     - **文件复制到本地或网络驱动器 --** 当选定时，允许您指定要将源文件/文件夹移动或复制到的位置的完整路径。您可以浏览到该目标位置。单击绿色箭头图标，允许您验证到指定目标的连接。
     - **文件复制到云 --** 当选定时，允许您指定要将源文件/文件夹移动或复制到的云位置。CA ARCserve D2D 当前支持将文件复制到多个云供应商，如 Amazon S3（简单存储服务）、Windows Azure、Fujitsu Cloud (Windows Azure) 以及 Eucalyptus-Walrus。这些云供应商是公用的 Web 服务，允许您随时从 Web 的任何位置安全地存储和检索任何数量的数据。

       您可以单击“配置”按钮来显示“云配置”对话框。有关详细信息，请参阅指定文件复制的云配置详细信息 (p. 99)。

       注意：在尝试连接到云时，为了消除任何潜在的时钟偏差错误，请验证您的计算机时区设置正确，并且时钟与全球时间同步。您应当始终将计算机时间与 GMT 时间对比。如果计算机时间与正确的全球时钟时间不同步（ 5 到 10 分钟之内），则 Amazon S3 将不工作。在必要时，请重置正确的计算机时间并重新运行您的存档作业。

     对于每一个目标选项，如果到指定目标的连接丢失或断开，CA ARCserve D2D 将进行若干次尝试继续文件复制作业。如果这些尝试不成功，将从失败发生的位置执行一个补偿作业。此外，活动日志将更新相应的错误消息，并发送电子邮件通知（如果配置）。

- **压缩** -- 指定用于文件复制作业的压缩类型。

  压缩通常会减少存储空间，而且还可以抵消由于对 CPU 越来越多的占用而导致的对文件复制速度的负面影响。

  可用的选项包括：

  - **无压缩** -- 将不执行压缩。此选项具有最低的 CPU 使用率（最快速度），但会使得文件复制占据最大容量的存储空间。
  - **标准压缩** -- 将执行某种压缩。此选项会在 CPU 使用率和存储空间要求之间实现良好平衡。这是默认设置。
  - **最大压缩** -- 将执行最大压缩。此选项提供最高的 CPU 使用率（最低速度），但是对文件复制的存储空间要求最低。

- **加密** -- 允许您为文件复制启用加密密码。

- **保留时间** -- 此设置仅适用于移动的文件复制数据（不是保留的文件复制数据）。

  指定存储数据在目标位置上保留的时间量（年数、月数、周数、天数）。在指定的保留时间结束时，存储数据从目标中清除。

  保留时间是根据一个月 30 天，一年 365 天来计算的。例如：如果您指定保留时间为 2 年、2 个月和 5 天，那么文件复制数据的保留时间总计为 795 天 (365 + 365+30 + 30 + 5)。

  重要说明！因为此保留时间设置仅适用于从源复制并移动到目标（不是复制并保留）的数据，所以理解以下情况是非常重要的，在指定的保留时间结束（即数据从目标清除）时，不再保留或存储所有这些移动的数据。

- **文件版本** -- 该设置仅适用于保留的复制数据（不是移动的复制数据）。

  指定保留并存储在目标位置中（云或磁盘）的副本数目。当超出该数目之后，将丢弃最早（最旧）的版本。当较新的版本添加到目标时，将重复最旧存储版本的丢弃循环，允许您始终维护指定数目的存储版本。

  例如，如果您指定文件版本保留计数为 5，并且您在五个时间点 t1、t2、t3、t4 和 t5 执行五次文件复制，则这些文件副本将作为五个文件复制版本保留，并可用于恢复。当执行第六次文件复制（保存新版本）之后，CA ARCserve D2D 将删除 t1 副本，因此五个要恢复的可用版本现在是 t2、t3、t4、t5 和 t6。

  默认情况下，丢弃之前在目标位置保留副本数是 15。

5. 单击“保存设置”。

您的文件复制目标设置即被保存。

为文件复制指定云配置详细信息

在此对话框中，您可以使用下拉菜单选择用于文件复制存储的云供应商类型。可用的选项包括 Amazon S3、Windows Azure、Fujitsu Cloud (Windows Azure) 和 Eucalyptus-Walrus。（Amazon S3 是默认供应商）。有关 Fujitsu Cloud (Windows Azure) 的更多信息，请参阅概述和注册。

注意：如果您要将 Eucalyptus-Walrus 作为您的文件复制云供应商，您将无法复制整个路径长度大于 170 个字符的文件。

每个云供应商的配置选项都是类似的（某些术语不同），并且将介绍任何不同之处。

1. 指定连接设置：

   供应商 URL

   标识云提供商的 URL 地址。

   （对于 Amazon S3、Windows Azure 和 Fujitsu Cloud (Windows Azure)，已经自动预填供应商 URL。对于 Eucalyptus-Walrus，供应商 URL 必须使用指定格式手动输入）。

   访问密钥 ID/帐户名称/查询 ID

   标识请求访问该位置的用户。

   （对于该字段，Amazon S3 使用访问密钥 ID，Windows Azure 和 Fujitsu Cloud (Windows Azure) 使用帐户名称，而 Eucalyptus-Walrus 使用查询 ID）。

   秘密访问密钥/密钥

   因为您的访问密钥未加密，所以该秘密访问密钥是用于验证该位置访问请求的可靠性的密码。

   重要说明！对于维护帐号的安全性，该秘密访问密钥至关重要。您应当将您的密钥和您的凭据存放在安全的地方。不要将您的秘密访问密钥嵌在网页或其他可公共访问的源代码中，并且不要通过非安全通道传送它。

   （对于该字段，Amazon S3 使用私密访问密钥。Windows Azure、Fujitsu Cloud (Windows Azure) 和 Eucalyptus-Walrus 使用私密密钥）。

启用代理

如果选择此选项，则还必须包括代理服务器的 IP 地址（或计算机名），以及代理服务器用于进行 Internet 连接的相应端口号。如果代理服务器要求身份验证，您还可以选择该选项。然后，您必须提供使用代理服务器时所需要的相应身份验证信息（用户名和密码）。

（代理服务器功能对于 Eucalyptus-Walrus 不可用）。

2. 指定高级设置：

存储桶名称/容器

移动或复制到云供应商的所有文件和文件夹都在您的存储桶（或容器）中进行存储和组织。存储桶像文件的容器，用于将对象分组和组织在一起。存储在云供应商处的每个对象都将置入存储桶中。

（对于该字段，Amazon S3 和 Eucalyptus-Walrus 使用“存储桶名称”。Windows Azure 和 Fujitsu Cloud (Windows Azure) 使用的是“容器”）。

注意：对于此步骤的剩余部分，除非指定，对存储桶的所有引用也可以应用于容器。

指定新存储桶名称：

a. 指定您的新存储桶名称。

注意：CA ARCserve Central Protection Manager 不创建存储桶名称，但会在将 CA ARCserve Central Protection Manager 策略成功分配给 CA ARCserve D2D 节点时为每个节点生成存储桶名称。每个 CA ARCserve D2D 节点的存储桶名称将自动加上前缀“d2dfilecopy-<hostname>-<user given name>”。

存储桶名称是唯一的，容易辩认，并且符合 Internet 域命名规则。任何两个存储桶不可以具有相同的名称。理解存储桶名称的有效语法是非常重要的。

对于 Amazon S3 和 Eucalyptus-Walrus，请参考 Amazon S3 文档获得关于存储桶命名要求的更多信息。

对于 Windows Azure 和 Fujitsu Cloud (Windows Azure)，请参考 Microsoft 文档了解有关容器命名要求的详细信息。

b. 仅对于 Amazon S3，从下拉菜单中选择可用地区。默认情况下，所有可用地区都包含在下拉菜单中，您可以选择想要创建新存储桶的地区。

地区允许您选择 Amazon S3 存储您创建的存储桶的地理区域。选择一个地区，该地区可让您实现数据的快速访问，并帮助您优化延迟、最大程度地降低成本或满足法规要求。

（对于 Windows Azure、Fujitsu Cloud (Windows Azure) 和 Eucalyptus-Walrus，地区是不可选择的）。

c. 指定值后单击“确定”。在云中验证和创建存储桶名称。

d. 在您成功创建新存储桶之后，“云配置”主对话框将再次出现，显示包含在“高级设置”字段中的新存储桶信息（名称和地区）。

启用减少冗余存储

仅针对 Amazon S3，该选项让您可以选择启用减少冗余存储 (RRS)。RRS 是 Amazon S3 中的存储选件，可通过在 Amazon S3 标准存储的较低冗余级别上存储非关键的可复制数据来帮助您降低成本。标准冗余存储选项和减少冗余存储选项都将数据存储在多个工具和多个设备上，但是有了 RRS，数据重复的次数更少，因此成本降低。使用 Amazon S3 标准存储或 RRS 时，你所预期的延迟和吞吐量应该相同。默认情况下，不选择该选项（Amazon S3 使用标准存储选件）。

3. 单击“测试连接”以验证到指定云位置的连接。

4. 单击“确定”以退出“云配置”对话框。

指定文件复制排定

CA ARCserve Central Protection Manager 允许您为将要执行文件复制的信息指定排定设置。

指定文件复制排定

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

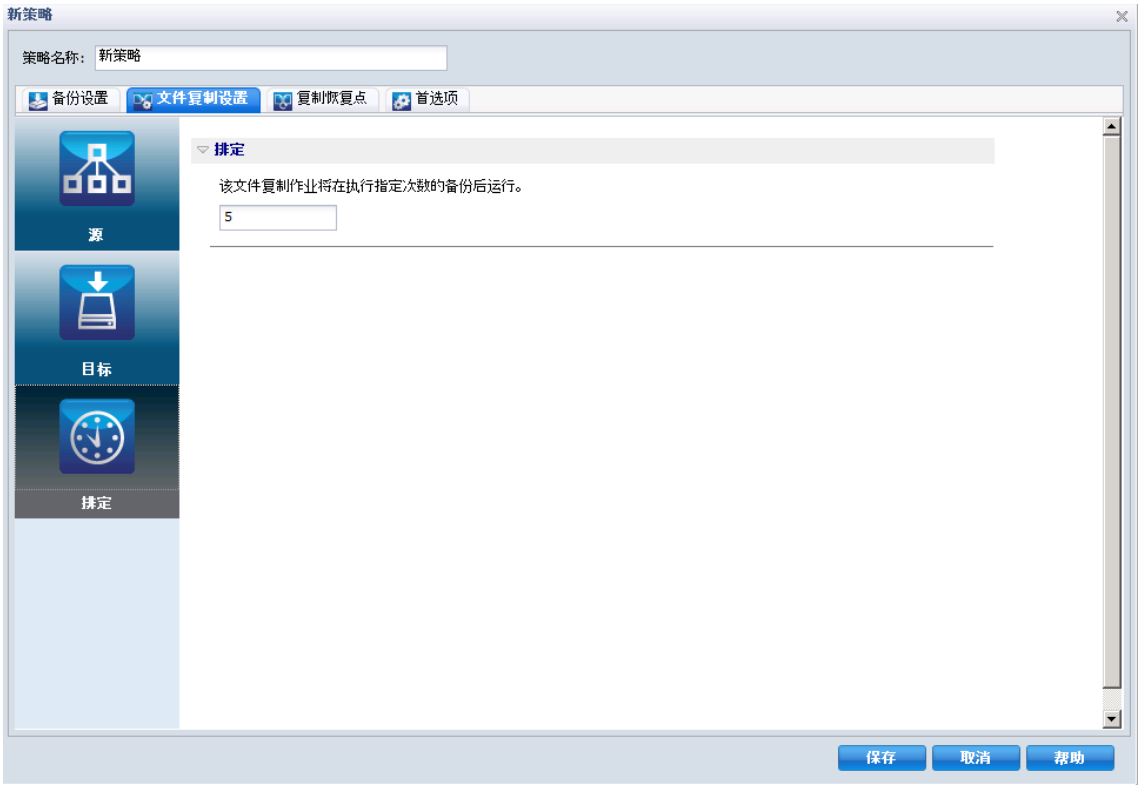
此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

此时打开“新建策略”对话框。

3. 选择“文件复制设置”选项卡，然后选择“排定”。

   “文件复制设置排定”对话框将打开。



4. 指定您的文件复制排定设置。

   - **排定** -- 在指定备份次数之后，启用数据的文件复制。

     在成功备份指定的数目之后，文件复制过程将自动启动，同时将基于您选定的文件复制策略。

     您可以使用该设置控制每天触发文件复制作业的次数。例如，如果您指定每 15 分钟运行一次备份作业，然后如果指定每 4 次备份运行一个文件复制作业，则每天将执行 24 个文件复制存档（每小时一次）。

     默认情况下，文件复制的排定是在每 5 次成功备份之后。（可以指定的备份最大数目是 700）。

5. 单击“保存设置”。

您的文件复制排定设置即被保存。

指定复制恢复点设置

CA ARCserve D2D 允许您为执行复制的恢复点指定排定设置（并在必要时导出）。为了更好地理解此对话框中的选项如何用于配置您的恢复点复制排定，请参阅复制恢复点 - 示例方案。

注意：恢复点复制过程仅是一个复制粘贴操作，不是剪切和粘贴操作。因此，无论何时执行排定的复制恢复点作业，CA ARCserve D2D 都将在指定的复制目标中创建另外的恢复点副本，同时，仍然在“备份设置”中指定的备份目标中保留恢复点的初始副本。

指定复制恢复点设置

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 选择“复制恢复点”选项卡。

   “复制恢复点”对话框将打开。

4. 指定您的恢复点复制排定设置。

启用复制恢复点

在指定的备份次数之后，启用恢复点的排定复制。如果不选中此选项，将不执行恢复点的排定复制。

目标

指定恢复点复制的位置（目标），或者您可以浏览到一个复制位置。您可以单击绿色箭头图标按钮来验证到指定位置的连接。

复制恢复点作业将在执行指定次数的备份后运行。

指定排定的恢复点复制过程自动启动的时间。

在成功备份指定的数目之后，恢复点复制过程将自动启动，同时将基于您选定的复制策略。

您可以使用此设置控制每天触发恢复点复制过程的次数。例如，如果您指定每 15 分钟运行一次备份作业，然后如果指定每 4 次备份后运行一次恢复点复制，则每天将执行 24 个恢复点复制作业（每小时一次）。

默认情况下，恢复点复制的排定是在每 8 次成功备份之后。

重要说明！如果您排定备份和复制作业以特定间隔运行，并且如果在备份作业时间的排定时间来到时，而复制作业当前正在运行（处于活动状态），则备份作业将失败。（下一个备份作业将按排定运行，如果它不与其他复制作业发生冲突，则应当是成功的）。因为复制操作几乎需要与执行完全备份相同的时间量，所以为恢复点复制作业设置频繁的排定不是最佳实践。

指定要保留的复制恢复点数目。

在指定的复制目标中，指定保留和存储恢复点的数目。当超出该数目之后，将丢弃最早（最旧）的恢复点。当较新的恢复点添加到目标时，将重复最旧恢复点的丢弃循环，允许您始终维护指定数目的存储恢复点。

注意：如果您的目标没有足够的可用空间，您可以考虑减少保存恢复点的数目。

默认情况下，保留计数将设成 31 个恢复点。

注意：恢复点的最大数目是 1344。

压缩

指定要用于恢复点复制的压缩类型。

压缩通常用以减少对磁盘空间的占用，而且还可以抵消由于对 CPU 越来越多的占用而导致的对备份速度的负面影响。

可用的选项包括：

- **无压缩**－不执行压缩。文件是纯 VHD。此选项的 CPU 使用率最低（速度最快），但是对于您的备份映像而言，磁盘空间占用最大。
- **无压缩 - VHD**－不执行压缩。文件将直接转换为 .vhd 格式，无需手工操作。此选项的 CPU 使用率最低（速度最快），但是对于您的备份映像而言，磁盘空间占用最大。
- **标准压缩** - 将执行某些压缩。此选项将会在 CPU 使用率和磁盘空间占用之间实现良好的平衡。此设置是默认设置。
- **最大压缩** - 将执行最大压缩。此选项提供最高的 CPU 使用率（速度最慢），但是对于备份映像而言，磁盘空间占用最低。

注意：如果您的备份映像包含不可压缩的数据（如 JPG 图像或 ZIP 文件），可分配额外的存储空间来处理此类数据。因此，如果您选择了任何级别的压缩选项，但同时在备份中有不可压缩的数据，则实际上可能导致磁盘空间使用的增加。

加密算法

指定要用于恢复点复制的加密算法类型。

数据加密将数据转换为需要有解码机制才可识别的格式。CA ARCserve D2D 数据保护使用安全的 AES（高级加密标准）加密算法实现指定数据的最佳安全性和隐私。

可用的格式选项是“不加密”、AES-128、AES-192 和 AES-256。（要禁用加密，请选择“不加密”）。

加密密码

如果要复制的恢复点先前已加密，您将需要提供（并确认）密码。

- 如果该恢复点正在复制到同一计算机上的位置，将记忆加密密码，该字段将自动填充。
- 如果该恢复点正在复制到其他计算机，则您将需要输入加密密码。

5. 单击“保存设置”。

复制恢复点设置随即保存。

管理“首选项”

CA ARCserve Central Protection Manager 允许您管理策略的一般需要。您可以生成新闻 Feed 或创建电子邮件报警通知或更新您的服务器或连接。

此部分包括以下主题

指定常规首选项 (p. 106)
指定电子邮件警报 (p. 108)
指定更新首选项 (p. 113)

指定常规首选项

CA ARCserve Central Protection Manager 允许您指定策略的一般首选项。

要指定一般首选项

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 选择“首选项”选项卡。

   “首选项”对话框将打开。

4. 指定您的首选项

   - **新闻 Feed** -- 启用此选项可显示来自专家咨询中心的最新消息和产品信息。
   - **社交网络** -- 启用此选项可在主页中显示 Facebook 和 Twitter 的链接。
   - **系统托盘通知** -- 可以选择下列选项之一：
     - 选择“全部”显示系统托盘中的所有通知。
     - 选择“错误和警告”仅显示系统托盘中的错误和警告。
     - 选择“无”不显示通知。
   - **视频** -- 选择一个要在 D2D 策略中使用的视频类型：
     - 使用 CA 支持视频
     - 使用 YouTube 视频（默认）

5. 单击“保存”。

常规首选项即被保存。

指定电子邮件警报

CA ARCserve Central Protection Manager 允许您指定“电子邮件报警”首选项。

要指定电子邮件报警

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 选择“首选项”选项卡，然后选择“电子邮件报警”。

   “首选项电子邮件报警”对话框将打开。

4. 指定您的电子邮件报警。

   - **启用电子邮件报警 --** 选择此选项可启用在此屏幕上的首选项。
   - **电子邮件设置 --** 单击此按钮可打开“电子邮件设置”对话框 (p. 111)。
   - **通知 --** 指定在选定事件完成后发送自动电子邮件报警通知。可以选择可用选项中的任何一个，也可以选择所有选项。

     可用选项将为下列事件发送报警通知：

     备份作业报警

     - **错过的作业 --** 针对所有错过的作业发送电子邮件报警通知。错过的作业是没有在排定时间运行的任何已排定作业。当某个其他作业正在运行或者较早开始的前一个作业尚未完成时，可能发生这种情况。例如，如果在某备份作业的排定时间正在运行导出或恢复作业，那么则会错过该备份作业。
     - **备份、目录、文件复制、还原或复制恢复点作业失败/崩溃 --** 针对所有不成功的备份、目录、文件复制、还原或复制恢复点作业尝试发送电子邮件报警通知。此类别包括所有失败的、未完成、取消的和错过的作业，以及崩溃的尝试。
     - **备份、目录、文件复制、还原或复制恢复点作业成功 --** 针对所有成功的备份、目录、文件复制、还原或复制恢复点作业尝试发送电子邮件报警通知。
     - **合并作业已停止、跳过、失败或崩溃** -- 针对所有已停止、跳过、失败或崩溃的合并作业发送报警通知。如果您启用该报警，一旦合并作业失败，您便会得到通知。合并失败可能有如下原因：会话被挂接、会话被编录作业锁定或者会话因其他原因被锁定。
     - **合并作业成功** -- 针对所有成功的合并作业发送报警。

     磁盘空间报警

     - **备份目标可用空间少于 --** 当备份目标的未使用空间量少于指定值时，发送电子邮件报警通知。对于该选项，您可以进一步选择总量的百分比或者将要发送报警通知的阈值级别的特定值（以 MB 为单位）。

     更新报警

     - **新的更新可用 --** 当 CA ARCserve D2D 的新更新可用时，发送电子邮件通知。如果检查更新或下载失败，也将发送电子邮件通知。

资源报警

- **启用资源报警 --** 当达到任何关键性能指标 (PKI) 阈值级别时，发送报警通知。要确保服务器高效且可靠，您需要持续监视性能以确定可能的问题，并快速解决瓶颈状况。

  定义这些性能指标的阈值级别完全取决于您和您对服务器的了解。设置不分对错，而这些报警通知应当以“正常”和可接受的性能为基础。例如，如果您的系统通常在 80% 的 CPU 负载下运行，那么将 CPU 使用率设为 75% 就不那么有用或有效。

  可以分别设置每个 PKI 参数，以便当达到相应的阈值级别时发送报警通知。每个 PKI 报警电子邮件将要发送的最大数目是每天 5 个。

- **CPU 使用 --** 指定的 CPU 使用报警阈值表示 CA ARCserve D2D 保护的服务器的 CPU 使用百分比。可以使用该报警通知来确保您的服务器不会经常过载。

  如果 CPU 使用率过高，服务器响应时间可能非常缓慢或根本不响应，此时应考虑延展（平衡）负载。

- **磁盘吞吐量 --** 指定的磁盘吞吐量报警阈值表示 CA ARCserve D2D 保护的服务器的磁盘吞吐量（MB/秒）。可以使用该报警通知来确保您将磁盘的能力最大化。

  如果磁盘吞吐量接近磁盘可以处理的最大值，应考虑升级到更加符合需求的磁盘。通常，磁盘越快，性能越高。

- **内存使用 --** 指定的内存使用报警阈值表示 CA ARCserve D2D 保护的服务器上的内存使用百分比。使用率是指正在使用的内存量。百分比越高，服务器性能将越差。

  如果内存使用率持续过高，您需要确定导致这种情况的进程。可以使用该指标设置可在应用程序或服务器可能需要升级时发送报警。

- **网络 I/O --** 指定的网络 I/O 报警阈值表示在 CA ARCserve D2D 保护的服务器上当前使用的 NIC 带宽百分比。使用率是指正在使用的网络接口卡（或 NIC）容量。百分比越高，网络性能将越差。

  如果网络使用率持续过高，您需要确定导致这种情况的进程，并解决问题。此外，如果对于您的具体网络容量，在备份期间网络使用率的百分比过高，您可能需要升级 NIC 卡来满足更高的吞吐量需求。

5. 单击“保存”。

电子邮件报警选项即被保存。

指定电子邮件设置

“电子邮件设置”对话框将电子邮件服务器和策略电子邮件配置的当前值自动填充到新策略。这些设置将应用到所有电子邮件报警通知，并且可以随时修改。

服务

用于发送报警通知的电子邮件提供商服务。可用选项有 Google Mail、Yahoo Mail、Live Mail 和“其他”。

- 如果选择“其他”，您必须将使用的邮件服务器和相应端口号识别为默认设置。
- 如果选择 Google Mail、Yahoo Mail 或 Live Mail，则邮件服务器和端口号字段将自动填充。

邮件服务器

CA ARCserve D2D 可用于发送电子邮件报警的 SMTP 邮件服务器主机名。

端口

邮件服务器的输出端口号。

要求身份验证

指定当尝试通过 Internet 发送电子邮件时，此邮件服务器是否要求身份验证。当选择此选项时，必须提供相应用户的帐户名和密码。

主题

CA ARCserve D2D 发送电子邮件报警通知的主题说明。默认情况下，这是“CA ARCserve D2D 报警”。

发件人

CA ARCserve D2D 用于发送电子邮件报警通知的电子邮件地址。

接收者

接收电子邮件报警通知的收件人的电子邮件地址。

注意：要输入多个电子邮件地址，每个地址均必须用分号字符隔开。

使用 SSL

电子邮件服务器要求 SSL（安全套接字层）连接来通过 Internet 传输数据。

发送 STARTTLS

电子邮件服务器要求发出 STARTTLS (Start TLS extension) 命令，在服务器之间启动安全的 SMTP 连接。

使用 HTML 格式

电子邮件报警通知将作为 HTML 发送。如果未选择此选项，则报警将作为纯文本发送。默认情况下，将选中该选项。

启用代理设置

指定是否连接到代理服务器来发送您的电子邮件报警通知。当选定此选项时，必须提供相应代理服务器的名称和端口号。

测试电子邮件

确认邮件配置设置正确无误。

指定更新首选项

CA ARCserve Central Protection Manager 允许您指定更新首选项。

指定更新首选项

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 单击“新建”创建新的策略。

   此时打开“新建策略”对话框。

3. 选择“首选项”选项卡，然后选择“更新”。

   “更新”对话框将打开。

4. 指定您的更新首选项。

   - **下载服务器 --** 指定 CA ARCserve D2D 服务器将连接的源服务器，以从其上下载可用更新。
     - **CA Technologies 服务器 --** 您可以使用该选项指定将 CA ARCserve D2D 更新从 CA Technologies 服务器直接下载到本地服务器。
     - **临时服务器 --** 使用该选项指定要用作临时服务器的服务器。

       如果您指定多个临时服务器，则第一个列出的服务器将被指定为主要临时服务器。CA ARCserve D2D 首先尝试连接到主要临时服务器。如果出于任何原因，第一个列出的服务器不可用，那么下一个列出的服务器将成为主要临时服务器。依次进行，直到最后列出的服务器成为主要临时服务器。（“临时服务器”列表可以最多有 5 个服务器）。
     - 可以使用“上移”和“下移”按钮来更改分段服务器的顺序。
     - 可以使用“删除”按钮从该列表中删除服务器。
     - 可以使用“添加服务器”按钮将新的服务器添加到该列表中。当您单击“添加服务器”按钮时，“分段服务器”对话框将打开，允许您指定添加的分段服务器的名称，以及当前默认的端口号。

       这是默认设置。

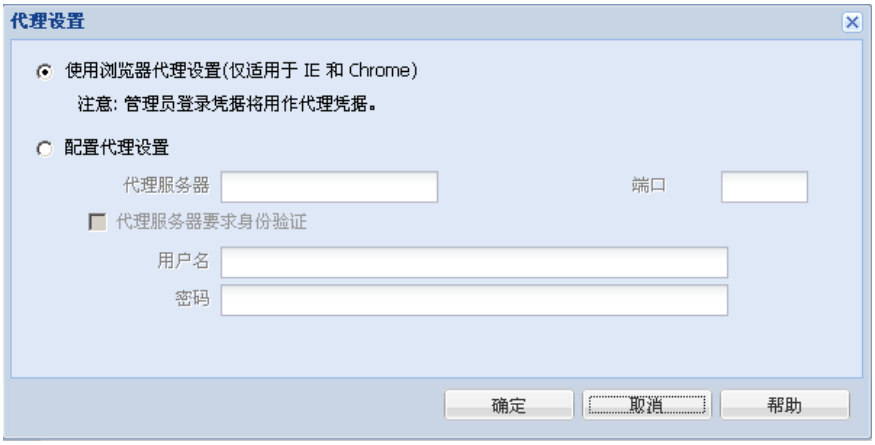
       注意：对于 D2D 策略，默认临时服务器是本地 CA ARCserve Central Applications 计算机。

       CA ARCserve D2D 更新将会从 CA Technologies 服务器直接下载到指定的临时服务器位置。在将更新下载到该分段服务器之后，您就可以进一步从分段服务器将更新下载到客户端服务器。如果选择临时服务器位置，则请指定临时服务器的主机名或 IP 地址以及相应的端口号。

- **代理设置** -- 仅当您选择 CA 服务器为下载服务器时可用。

  单击“代理设置”以指定是否想通过代理服务器下载 CA ARCserve D2D 更新。这将是到 CA 服务器的连接，您的下载服务器将从此处获取更新。

  当单击此按钮时，会打开“代理设置”对话框。



  - **使用浏览器代理设置（仅适用于 IE 和 Chrome）** -- 允许您使用为 CA ARCserve D2D 代理提供的凭据。
  - **配置代理设置** -- 代理服务器充当您的下载服务器（临时或客户端）和 CA 服务器之间的中介，以便确保提升安全性、性能以及管理控制。默认情况下，禁用该选项。

    选择此选项可使用代理服务器连接到 CA 服务器，获取 CA ARCserve D2D 更新信息。代理服务器将直接连接到 CA 服务器以获得更新信息。如果启用此选项，请包含代理服务器的 IP 地址（或主机名）和代理服务器用于 Internet 连接的相应端口号。

    如果不选择此选项，则下载服务器将直接连接到 CA 服务器，而不通过代理服务器。

    此外，还可以指定您的代理服务器是否将需要身份验证。在选定时，指定使用代理服务器时需要身份验证信息（用户 ID 和密码）。

- **测试连接** -- 让您测试以下连接并且在完成时显示状态消息：
  - 如果您选择“CA Technologies 服务器”作为下载服务器，则将通过指定的代理服务器测试计算机和 CA Technologies 服务器之间的连接。
  - 如果您选择“临时服务器”作为下载服务器，将测试计算机和指定临时服务器之间的连接。

    测试连接按钮用于测试每个列出的分段服务器的可用性，而相应的状态显示在“连接状态”字段中。

  注意：创建新策略时启动“首选项自动更新”对话框时，测试连接会被自动执行。

- **更新排定** -- 指定检查（和下载）新的 CA ARCserve D2D 更新的时间。

  选定该选项后，它将自动检查新的和可用的 CA ARCserve D2D 更新。如果选择该选项，则您可使用下拉式菜单功能指定何时执行该功能（每天执行或在每周指定的一天执行）以及这一天要执行该功能的时间。

  如果选择该选项但不指定天和时间，默认排定是在每个周日的凌晨 4 点执行自动检查。

  默认情况下，如果该检查确定有新的更新可用，CA ARCserve D2D 将自动下载该更新。如果您不想自动下载更新，您可以在 D2DPMSettings.INI 文件中禁用该功能。有关详细信息，请参阅《CA ARCserve D2D 用户指南》。

  如果不选择此选项，它将禁用所有自动检查和下载功能（并且它的状态将显示在主页的状态摘要下面）。

  这些更新功能仅可以手动触发。

  注意：如果已经配置，那么在更新的排定检查发现新的更新可用时，会向您发送电子邮件通知。另外，如果检查更新或下载失败，也将发送电子邮件通知。

5. 单击“保存”。

更新首选项即被保存。

编辑或复制策略

CA ARCserve Central Protection Manager 允许您在创建策略后编辑或复制策略。

编辑策略

1. 登录该应用程序。

   单击导航栏上的“策略”以打开“策略”屏幕。

2. 从“策略”屏幕，单击策略旁边的复选框，然后执行以下操作之一：
   - 单击工具栏上的“编辑”，然后编辑选定策略。
   - 单击工具栏上的“复制”，以从选定策略复制并创建新策略。

     注意：在您复制策略时，“复制策略”对话框打开。为新策略指定名称，然后单击“确定”。

   “编辑策略”对话框将打开。

3. 如果您想更改策略的名称，请在“策略名称”字段指定名称。
4. 指定所需的值，然后单击“保存”。

策略即被编辑或复制。

删除策略

CA ARCserve Central Protection Manager 允许您删除以前创建的策略。

注意：CA ARCserve Central Protection Manager 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。有关如何取消分配策略中节点的信息，请参阅从策略分配与取消分配节点 (p. 119)。

删除策略

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

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。

部署策略

CA ARCserve Central Protection Manager 允许您部署策略，不论其部署过多次，还是部署到远程服务器失败。

部署策略

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”。

   此时会打开“策略”屏幕。

2. 在“策略”列表中选择一个策略，然后单击“立即部署”。

   将立即部署该策略。

注意：当策略成功部署到 CA ARCserve D2D 节点时，CA ARCserve D2D 节点上的所有设置都无法更改。但“更新连接”按钮被启用。这样，如果访问凭据在远程服务器上更改，CA ARCserve D2D 可以将连接信息重新同步到备份目标。此外，您还可以在“节点列表”屏幕的“策略”列下查看策略部署状态。

从策略分配与取消分配节点

CA ARCserve Central Protection Manager 允许您分配与取消分配现有 D2D 策略中的节点。

遵循这些步骤:

1. 在 CA ARCserve Central Protection Manager 主页中，单击导航栏上的“策略”打开“策略”屏幕。
2. 从“策略”列表中选择一个策略，然后单击“策略分配”选项卡。

   分配给选定策略的节点的列表显示以下部署操作和操作之一（格式：*[操作] 部署状态*）：

   - [分配] 挂起
   - [取消分配] 正在部署
   - [重新同步] 完成
   - [更新] 失败
   - [重新部署] 部署 D2D 成功
   - [重新部署] 部署 D2D 失败
   - [重新部署] 部署 D2D 重新启动
3. 单击“分配”或“取消分配”按钮。

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

     注意： “节点名称”字段允许您使用通配符筛选节点。

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

5. 执行下列操作之一：

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

     节点即从“可用节点”列表移到“选定的节点”列表。

     注意：要选择和移动所有节点，请单击向右双箭头。

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

     节点即从“选定的节点”列表移到“可用节点”列表。

     注意：要选择和移动所有节点，请单击向左双箭头。

   单击“确定”。

   注意：下列消息在您取消分配策略时会出现：

   您正从从选定的节点取消分配策略。您可以保留当前设置以允许节点继续备份过程。是否要保留设置?"单击“是”将保留当前的 CA ARCserve D2D 设置，单击“否”将删除当前的 CA ARCserve D2D 设置，或者单击“取消”返回到“分配/取消分配策略”屏幕。

   如果您单击“否”，远程 CA ARCserve D2D 设置将丢失，CA ARCserve D2D 服务器将不受保护。

节点应用于指定的策略。

立即运行备份

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

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

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

遵循这些步骤:

1. 登录该应用程序。
2. 从主页上的导航栏中，单击“节点”打开“节点”屏幕。

3. 要指定希望备份的节点，请执行以下操作之一：
   - **节点级别：**单击包含想要备份的节点的组，然后单击想要备份的节点旁边的复选框。
   - **组级别：**单击包含想要备份的节点的组。
4. 然后执行下列操作之一备份节点：
   - 单击工具栏上的“备份”。
   - 右键单击选定的组或右键单击节点，然后单击上下文菜单上的“立即备份”。
5. 在“立即运行备份”对话框上，单击下列类型之一以指定备份类型：
   - **完全备份 --** 启动您的整个计算机或选定卷的完全备份。
   - **增量备份 --** 启动您的计算机的增量备份。增量备份仅备份自上一次备份以来已经更改的块。

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

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

出现确认屏幕，选定类型的备份立即启动。

请注意以下行为：

- 在“策略”对话框中指定的所有值均应用于作业。
- 如果自定义（临时）备份作业失败，将不创建补充作业。仅会为失败的排定作业创建补充作业。

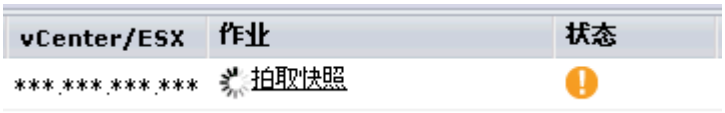
查看作业状态信息

作业正在运行时，您可以查看有关该作业的详细信息。（可选）您可以停止正在进行的作业。

遵循这些步骤:

1. 登录该应用程序。
2. 从主页上的导航栏中，单击“节点”打开“节点”屏幕。
3. 在“组”树中，单击包含您想查看作业状态的节点的组。

   如果作业正在进行，作业的阶段将显示在“作业”列中。



4. 单击“作业”列中的阶段以打开“备份状态监视器”对话框。
5. 在“备份状态监视器”对话框中，可以执行以下操作之一：
   - 单击“关闭”以关闭“备份状态监视器”对话框。
   - 单击“取消”以停止当前作业。

     注意：单击“取消”后，很快就会关闭“备份状态监视器”对话框。

如何在 CA ARCserve Central Protection Manager 中还原节点

CA ARCserve Central Protection Manager 提供了可用于还原节点的各种工具和选项。本节包含有关如何安全有效地还原数据的信息。

本节包含以下主题：

从恢复点还原数据 (p. 123)
从文件副本还原数据 (p. 125)
从文件和文件夹还原数据 (p. 128)
从虚拟机还原数据 (p. 131)
还原 Microsoft Exchange 电子邮件数据 (p. 135)

从恢复点还原数据

“浏览恢复点”允许您通过浏览可用恢复点（成功备份），从一个日历视图中还原任何应用程序。

从恢复点还原数据

1. 登录到应用程序，并单击导航栏上的“节点”。
2. 在“节点”屏幕中，展开包含要还原的节点的组。

   单击要还原的节点旁的复选框，然后单击工具栏上的“还原”。
3. 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。
4. 指定“备份位置”或浏览到存储备份映像的位置。

   注意：您可以单击“浏览”按钮旁边的绿色箭头，验证指定备份目标的连接。您必须输入用户名和密码凭据才能连接到远程网络共享。

   日历视图突出显示（绿色）所有显示的时间期间的日期（包含备份源的恢复点）。
5. 指定要还原的信息。
   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、备份时间、执行的备份类型，以及备份名称和目录状态。
   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）。
   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。

   单击“下一步”。

   将显示“还原选项”对话框。

6. 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。

   还原到原始位置

   还原到捕获备份映像的原始位置。

   注意：将 CA ARCserve D2D 日志文件夹还原到原始位置时，将跳过日志文件夹中的文件。对于 CA ARCserve Central HostBased VM Backup，默认情况下，此选项被禁用。要使用它，请在访客操作系统内安装 CA ARCserve D2D，然后还原。

   还原到：

   您可以指定一个位置或浏览到存储备份映像的位置。您可以单击绿色箭头图标按钮来验证到指定位置的连接。

   必要时，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。

7. 选择 CA ARCserve D2D 如何在还原过程中解决遭遇冲突的相关选项。

   可用的选项包括：

   覆盖现有文件

   覆盖（替换）位于还原目标的任何现有文件。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

   重新启动时替换任何活动文件。如果在还原尝试期间，CA ARCserve D2D 发现现有文件当前正在使用或者被访问，它将不立即替换该文件，而是为了避免任何问题，将推迟活动文件的替换，直到下次重新启动计算机再进行。（还原将立即进行，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，那么还原将跳过任何活动文件。

   重命名文件

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

   跳过现有文件

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

   默认情况下，将选中该选项。

8. （可选）从“目录结构”中选择“创建根目录”。

   这将允许 CA ARCserve D2D 在还原目标路径中重新创建相同的根目录结构。

   注意：如果未选中此选项，则要还原的文件或文件夹将直接还原到目标文件夹。

9. 输入备份加密密码，还原加密的数据，然后单击“下一步”。

   将显示“还原摘要”对话框。

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。

从文件副本还原数据

“浏览文件副本”选项允许您从 CA ARCserve D2D 文件副本中恢复数据。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”。
2. 在“节点”屏幕中，展开包含要还原的节点的组。

   单击要还原的节点旁的复选框，然后单击工具栏上的“还原”。

3. 在“还原”对话框中单击“浏览文件副本”。

   “浏览文件副本”对话框打开。

4. 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** -- 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，其中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。

5. 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级别之上的根目录）。

    如果您选择从“SubFolder2”级别还原，则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级别之上的根目录）。

    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。

  如果您尝试还原到之前执行加密备份的计算机，则不需要密码。但是，如果您尝试还原到其他计算机，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（时钟图标）：

  加密恢复点（带锁的时钟图标）：

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。

从文件和文件夹还原数据

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

从文件和文件夹还原数据

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”。

   此时将打开“查找要还原的文件/文件夹”对话框。

3. 指定“备份位置”和“文件复制位置”，或浏览到存储备份映像的位置。

   请注意以下问题：

   - 对于“备份位置”，您可以单击“浏览”按钮旁边的绿色箭头，验证指定备份目标的连接。您必须输入用户名和密码凭据才能连接到远程网络共享。
   - 对于“文件复制位置”，您可以单击“更改”以切换到本地或网络驱动器或云。有关“文件复制位置”的详细信息，请参阅“从文件副本还原数据” (p. 125)。

4. 指定要还原的文件或文件夹名称。

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

   文件或文件夹名称支持的通配符如下所示：

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

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

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

6. 单击“查找”以启动搜索。

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

7. 选择要从列表还原的版本，然后单击“下一步”。

   将显示“还原选项”对话框。

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。

   还原到原始位置

   还原到捕获备份映像的原始位置。

   注意：将 CA ARCserve D2D 日志文件夹还原到原始位置时，将跳过日志文件夹中的文件。

   还原到：

   您可以指定一个位置或浏览到存储备份映像的位置。您可以单击绿色箭头图标按钮来验证到指定位置的连接。

   必要时，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。

9. 选择 CA ARCserve D2D 如何在还原过程中解决遭遇冲突的相关选项。

   可用的选项包括：

   覆盖现有文件

   覆盖（替换）位于还原目标的任何现有文件。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

   重新启动时替换任何活动文件。如果在还原尝试期间，CA ARCserve D2D 发现现有文件当前正被使用或者被访问，它将不立即替换该文件，而是为了避免任何问题，将推迟活动文件的替换，直到下次重新启动计算机再替换。（还原将立即发生，但是任何活动文件的替换将在下一次重新启动期间完成）。

   注意：如果未选中此选项，那么还原将跳过任何活动文件。

   重命名文件

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

   跳过现有文件

   跳过且不覆盖（替换）位于还原目标的任何现有文件。仅从备份文件中还原您计算机上当前不存在的对象。

   默认情况下，将选中该选项。

10. （可选）从“目录结构”中选择“创建根目录”。

    这将允许 CA ARCserve D2D 在还原目标路径中重新创建相同的根目录结构。

    注意：如果未选中此选项，则要还原的文件或文件夹将直接还原到目标文件夹。

11. 输入备份加密密码，还原加密的数据，然后单击“下一步”。

    将显示“还原摘要”对话框。

12. 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。

从虚拟机还原数据

使用还原 VM （虚拟计算机）选项还原您之前备份的虚拟计算机。

从虚拟机还原数据

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”。该应用程序将使您登录到 CA ARCserve D2D。

2. 在“还原”对话框中单击“恢复 VM”。

   此时将打开“还原”对话框。

3. 指定备份位置（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. 指定要还原的虚拟机。

   下拉菜单包括指定备份位置的所有虚拟机。

5. 选择要还原的虚拟机映像的日历日期。

   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。

6. 选择要还原的恢复点。

   该恢复点的相应备份内容（包括任何应用程序）将显示，仅供参考之用。还原虚拟机时，将还原整个计算机。因此，您可以查看，但不能从选定虚拟机内部选择单个卷、文件夹或文件。

   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。

7. 指定要还原的备份信息后，单击“下一步”。

   将显示“还原选项”对话框。

8. 选择还原目标。

   还原到原始位置

   将虚拟机还原到捕获备份映像的原始位置。默认情况下，将选中该选项。

   有关详细信息，请参阅将 VM 还原到原始位置 (p. 132)。

   还原到备用位置

   将虚拟机还原到与备份映像捕获位置不同的位置。

   有关详细信息，请参阅将 VM 还原到备用位置 (p. 133)。

9. 指定 CA ARCserve D2D 将执行什么操作以解决在还原过程中遇到的任何冲突。

   可用选项为，是否覆盖现有虚拟机。默认情况下，未选中该覆盖选项。

   - 如果您选择该选项，还原过程将覆盖（替换）该虚拟机的位于指定还原目标的任何现有映像。无论虚拟机映像当前是否存在于还原目标之上，都会从备份文件还原它。
   - 如果不选择此选项，还原过程将创建此虚拟机的独立映像，它不会覆盖位于指定还原目标的任何现有映像。

10. 指定“后续恢复”选项。

    选择在还原过程结束时是否使虚拟机开机。默认情况下，未选择该开机选项。

将虚拟机还原到初始位置

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

如果您选择将 VM 还原到原始位置，请执行下列步骤：

遵循这些步骤:

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

   注意：有关“解决冲突”和“后续恢复”选项的详细信息，请参阅“从虚拟机还原数据 (p. 131)”。

   “设置源 vCenter/ESX 服务器的凭据”对话框显示。

2. 指定用于访问虚拟机的凭据。

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

3. 指定凭据后，单击“确定”。

   “还原摘要”对话框将打开。

4. 检查显示的信息以确认所有还原选项和设置都正确。

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

将虚拟机还原到备用位置

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

如果要将虚拟机还原到备用位置，请执行下列步骤：

遵循这些步骤:

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

   注意：有关“解决冲突”和“后续恢复”选项的详细信息，请参阅“恢复数据到虚拟机 (p. 131)”。

   “恢复选项”对话框展开，显示更多还原到备用位置的选项。

2. 指定 vCenter/ESX 服务器信息。

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

3. 指定 vCenter/ESX 服务器信息后，请单击“连接到该 vCenter/ESX 服务器”按钮。

   如果备用服务器访问凭据信息正确，将启用“其他信息”字段。

4. 指定其他信息。

   - **VM 名称 --** 指定您要还原的虚拟机的主机名。
   - **ESX 服务器 --** 指定目标 ESX 服务器。下拉菜单将包含与指定虚拟机关联的所有 ESX 服务器的列表。
   - **VM 数据存储 --** 指定目标 VM 数据存储。

5. 指定其他信息后，单击“下一步”。

   “还原摘要”对话框将打开。

6. 检查显示的信息以确认所有还原选项和设置都正确。

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

还原 Microsoft Exchange 电子邮件数据

每次 CA ARCserve D2D 执行了成功的备份后，备份的时间点快照映像也会被创建。这个恢复点集允许您精确定位和指定要还原的备份映像。对于 Microsoft Exchange Server，您便可以浏览这些恢复点，以便找到想要恢复的单个对象对象（邮箱、邮箱文件夹或邮件）。要执行 Exchange 粒度还原，帐号必须有必需的权限。有关详细信息，请参阅 Exchange 帐号必需权限。

注意：对于 Microsoft Exchange Server 2007 以及更高版本，消息处理 API (MAPI) 是 Exchange 粒度还原的先决条件。如果您的 Exchange Server 中未安装 MAPI，则邮箱或邮件级粒度还原可能会失败。有关在您的 Exchange Server 上安装 MAPI 的详细信息，请查看 Microsoft 下载中心。

还原 Microsoft Exchange 电子邮件数据

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“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：将显示通知消息，询问您是否想此时生成 Exchange 粒度还原目录。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。

   “还原选项”对话框显示，选定数据库的邮箱内容的相应列表将列出。

   注意：仅支持电子邮件还原。不支持还原日历、联系人、注意和任务项。

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

   注意：您可以选择全部内容、部分内容或多个 Exchange 对象进行还原。

   a. 如果您选择邮箱数据库，将还原该数据库中的所有邮箱。

   b. 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. 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. 如果您选择单个邮件级，将仅还原选定邮件对象。

      注意：仅适用于 Exchange 2003，当单个邮件备份后，如果将其还原，然后由 Outlook 之外的任何电子邮件客户端进行发送，并在其中附加某些类型的状态标记，则该邮件本身将变成已还原，但是附加标记将不会包含在还原的邮件中。

7. 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：

   - 将邮箱或邮件还原（到初始或备用位置），确保目标可用，否则还原尝试将失败。提交还原作业后，CA ARCserve D2D 仅验证目标。
   - 如果您尝试将邮件还原到一台计算机，而这些邮件中的电子邮件地址在该计算机中无效（在该域中不存在），或如果用户未登录该邮箱，则一些字段可能会和备份时不一样。
   - 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 无法找到更改的名称。要解决此问题，您可以指定将该邮箱还原到备用位置。

仅转储文件

将邮件还原到磁盘。该磁盘位置必须是本地路径。还原的邮件的层次结构与它们在对应 Exchange 邮箱中所具有的层次结构保持一致。文件名是邮件的主题。

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：\ / : * ？ " < > |

有两个选项，用于解决文件系统中的冲突情况。文件系统中的两个文件不能存在于相同文件夹下，而 Exchange 邮件可以。

- **重命名 --** 如果磁盘上有文件与邮件主题同名，则 CA ARCserve D2D 将在邮件主题后面加上一个数字。
- **覆盖** -- 如果磁盘上有文件与邮件主题名称相同，则 CA ARCserve D2D 将覆盖该文件。

还原到备用位置

将邮件还原到指定位置，或允许您浏览到备份映像的还原位置。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）。

指定用户名和密码后，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. 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）。

查看 CA ARCserve Central Protection Manager 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。
  - **从发现导入节点** -- 该选项允许允许您查看仅从发现导入的节点的相关日志。
  - **从管理程序导入节点 --** 该选项允许您查看仅从管理程序导入的节点的有关日志。
  - **从文件导入节点** -- 该选项允许您仅查看将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。
  - **CA ARCserve Backup 同步** -- 该选项允许您仅查看 CA ARCserve Backup 数据同步的相关日志。
  - **CA ARCserve D2D 同步** -- 该选项允许您仅查看 CA ARCserve D2D 数据同步的相关日志。
  - **CA ARCserve D2D 的更新** -- 该选项允许您仅查看 CA ARCserve D2D 中所做更改的相关日志。
  - **更新** -- 该选项允许您仅查看有关应用程序更新的日志。
  - **提交 CA ARCserve D2D 备份作业** -- 该选项允许您仅查看已提交的 CA ARCserve D2D 备份作业的相关日志。
  - **更新多个节点** -- 此选项允许您仅查看同时更新多个节点的有关日志。
  - **CA ARCserve D2D 合并作业** -- 此选项允许您仅查看 CA ARCserve D2D 合并作业的有关日志。
- **节点名称** -- 该选项允许您仅查看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 CA ARCserve Central Protection Manager 服务器所在的时区。

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。

应用最佳实践

考虑 CA ARCserve Central Protection Manager 应用程序的以下最佳实践：

- CA ARCserve Central Applications 可以通过 CA ARCserve Central Applications 本地计算机和远程计算机之间的通信从远程计算机检索特定节点的数据。

  为确保远程访问成功进行，必需以下限制：

  - **网络限制 --** 必须启用远程计算机上的名为“admin$”的远程管理员共享。要在远程计算机上启用 'admin$'，请单击以下链接以获得有关说明：

    http://support.microsoft.com/kb/947232

  - **用户帐号限制 --** 要登录到 CA ARCserve Central Applications，必须使用 CA ARCserve Central Applications 本地计算机的公告管理员帐号，或将管理权限添加到 CA ARCserve Central Applications 本地计算机和远程计算机中。

  注意：要添加节点，必须有远程计算机的管理权限。

- 要在 Windows Server 2008 R2 计算机上使用节点或 IP 地址添加节点，请基于以下要求之一使用该帐号：

  - 如果您从 CA ARCserve Central Applications 计算机和远程计算机使用管理员组帐号登录 CA ARCserve Central Applications，则您可以使用相同的帐号添加节点。
  - 如果您从 CA ARCserve Central Applications 计算机使用公告管理员帐号登录到 CA ARCserve Central Applications，则从远程计算机使用管理员组帐号添加节点。

- 要发现来自 Active Directory 的节点，请执行以下操作之一：

  - 如果您在连接 Windows 域的节点上安装 CA ARCserve Central Applications，那么 CA ARCserve Central Applications 可以访问在域控制器上的 Active Directory 信息。
  - 如果您在连接工作组的节点上安装 CA ARCserve Central Applications，那么必须在命令窗口中运行以下命令行，以确认 CA ARCserve Central Applications 可以访问关联的域控制器：

    ```
    nltest /dsgetdc:%domain_name%
    ```

    注意：如果该方法以 ERROR_NO_SUCH_DOMAIN (1355) 状态失败，那么您必须调整网络设置。

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 5 章： 将 CA ARCserve Central Protection Manager 与 IT 管理服务器工具集成

此部分包含以下主题：

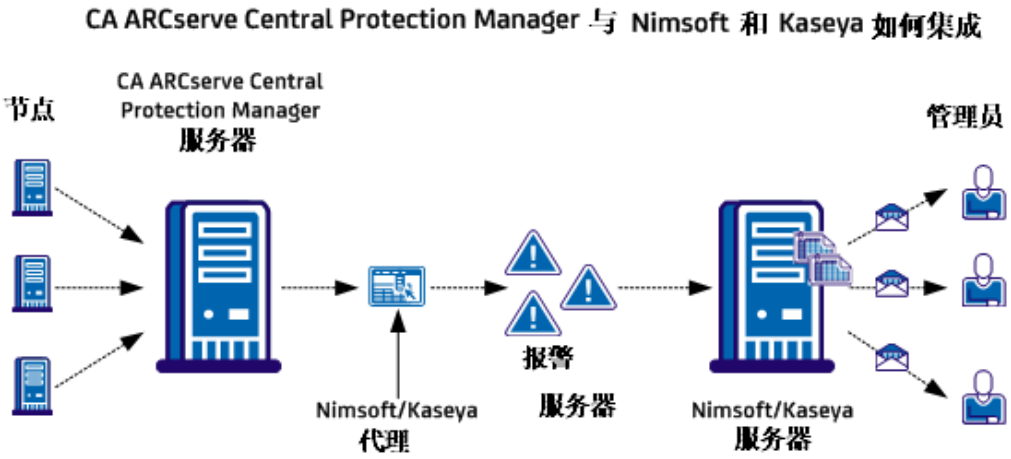
如何将 CA ARCserve Central Protection Manager 与 Nimsoft 和 Kaseya 集成

您可以配置 CA ARCserve Central Protection Manager 将报警消息的有关信息实时发布到 IT Management Server Infrastructure 管理工具。该功能允许 IT Server Management 管理员以适当的方式响应 CA ARCserve Central Protection Manager 报警。

CA ARCserve Central Protection Manager 可与下列 IT Management Server Infrastructure 管理工具集成：

- Nimsoft
  - 服务器：5.11
  - Robot：5.32
  - Unified Monitoring Portal：2.1.2
- Kaseya
  - 服务器：6.1.0.0
  - 代理：6.1.0.6

下图说明 CA ARCserve Central Protection Manager 如何与 Nimsoft 和 Kaseya 集成：



CA ARCserve Central Protection Manager 服务器监测安装 CA ARCserve D2D 的节点。CA ARCserve Central Protection Manager 服务器检测到报警状况时，它将报警发送到安装在 CA ARCserve Central Protection Manager 服务器上的 Nimsoft 或 Kaseya 代理。然后，代理立即将报警发送到 Nimsoft 或 Kaseya 服务器。

CA ARCserve Central Protection Manager 监测来自以下应用程序的报警：

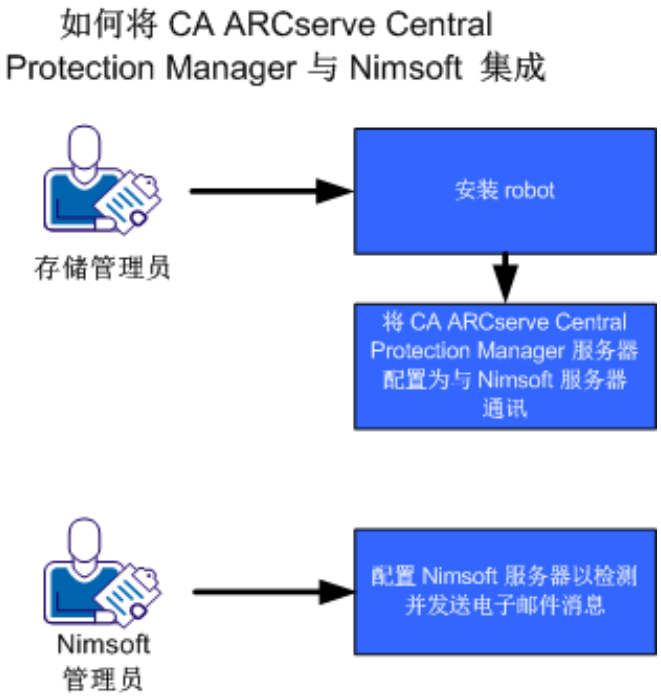
- CA ARCserve D2D
- CA ARCserve Central Virtual Standby
- CA ARCserve Central HostBased VM Backup
- CA ARCserve Central Protection Manager

Nimsoft 或 Kaseya 服务器生成运行这些应用程序的节点的有关报告，管理员使用 Nimsoft 和 Kaseya 管理工具查看这些报告。Nimsoft 和 Kaseya 服务器可以配置为根据预定义的条件将电子邮件发送给管理员。

如何将 CA ARCserve Central Protection Manager 与 Nimsoft 集成

存储管理员可以将 CA ARCserve Central Protection Manager 配置为将报警消息传送给 Nimsoft 服务器。Nimsoft 管理员可以将 Nimsoft IT 基础架构管理工具配置为检测 CA ARCserve Central Protection Manager 报警、生成报警报告及发送电子邮件。管理员可以使用这些报告管理 CA ARCserve D2D 节点的健康。

下图说明存储管理员如何将 CA ARCserve Central Protection Manager 与 Nimsoft IT 基础架构管理工具集成：



按照以下步骤将 CA ARCserve Central Protection Manager 与 Nimsoft 集成：

1. 安装 Robot (p. 146)。
2. 配置 CA ARCserve Central Protection Manager 服务器与 Nimsoft 服务器进行通信 (p. 147)。
3. 配置 Nimsoft 服务器检测和发送电子邮件 (p. 148)。

注意：CA ARCserve Central Protection Manager 服务器将包含本地化字符的报警消息发送到 Nimsoft 服务器时，本地化字符在 Nimsoft Unified Monitoring Portal (UMP) 报警控制台中会显示为乱码文字。要防止该问题发生，请配置 Nimsoft 服务器使用 UTF-8 编码。有关详细信息，请参阅《CA ARCserve Central Protection Manager 用户指南》中“来自本地化服务器的字符在 Nimsoft UMP 报警控制台中显示为乱码文字”。

安装 Robot

将 Robot 安装在 CA ARCserve Central Protection Manager 服务器上。Robot 允许 CA ARCserve Central Protection Manager 服务器与 Nimsoft 服务器进行通信，并将报警消息实时发送给它们。

注意：运行安装程序前，确保您拥有有效的许可。

遵循这些步骤:

1. 将 Robot 安装文件下载或复制到您的计算机。

   双击“*NimBUS Robot.exe*”以开始安装。

   “许可协议”对话框将打开。

2. 单击“许可”对话框上的“是”以开始安装。

   “选择目标位置”对话框打开。

3. 指定要安装 Robot 的位置，或者单击“下一步”以接受默认目录。

   “选择安装类型”对话框打开。

4. 单击“正常安装”，然后单击“下一步”。

   “Nimsoft 域”对话框打开，显示检测到的域的列表。

5. 单击“选择通过 IP 地址连接到网络界面”选项旁边的复选框，然后单击“下一步”。

   “指定 Nimsoft 集线器 IP 地址”对话框打开。

6. 在“集线器 IP”字段中，指定希望 CA ARCserve Central Protection Manager 服务器发送报警消息到 Nimsoft 集线器的 IP 地址。

   单击“下一步”。

   此时将打开选项对话框。

7. 在“选项”对话框中填写以下字段：

   （可选）第一探针端口

   允许您指定在启动探针时使用的第一个端口号。

   注意：不要指定允许操作系统生成随机端口。

   被动模式

   只有在 robot 无法与 Nimsoft 集线器进行通信时，才指定该模式。如果 Nimsoft 集线器可以与 CA ARCserve Central Protection Manager 服务器进行通信，单击“被动模式”旁边的复选框。

   注意：如果指定该选项，请手动将被动 robot 添加到集线器配置中。

   单击“下一步”。

   此时出现“开始复制文件”对话框。

8. 单击“下一步”。

   安装程序安装 robot。

9. 安装完成时，单击“完成”。

该 robot 便得以安装。

配置 CA ARCserve Central Protection Manager 服务器与 Nimsoft 服务器通信

CA ARCserve Central Protection Manager 允许您将报警消息发送到 Nimsoft IT 管理服务器。要发送报警信息，请将 CA ARCserve Central Protection Manager 服务器配置为与 Nimsoft 服务器通信。

遵循这些步骤:

1. 登录 CA ARCserve Central Protection Manager，然后单击导航栏上的“配置”。

   将显示配置选项。

2. 单击“配置”列表中的“IT 管理服务器配置”。

   IT 管理服务器配置选项显示。

3. 完成以下选项：

   a. 单击“启用”。

   b. 单击“Nimsoft”。

   c. 指定重复方式。“重复方式”定义原始发送过程失败时在一周的哪几天重新向 Nimsoft 服务器发送报警通知。Nimsoft 服务器不可用或脱机时，发送报警的过程会失败。

   d. 指定排定。排定定义在什么时间向 Nimsoft 服务器重新发送报警通知。

   单击“保存”。

CA ARCserve Central Protection Manager 服务器即被配置与 Nimsoft 服务器通信。

配置 Nimsoft 服务器检测和发送电子邮件

Nimsoft 管理员可以将 Alarm SubConsole 配置为检测到来自 CA ARCserve Central Protection Manager 服务器的报警消息时向指定收件人发送电子邮件消息。有关详细信息，请参阅 Nimsoft 文档。

在 Nimsoft Alarm SubConsole 中，查看报警的有关信息

Nimsoft Alarm SubConsole 允许 Nimsoft 管理员查看 CA ARCserve Central Protection Manager 报警的有关信息。Nimsoft Alarm SubConsole 提供 CA ARCserve Central Protection Manager 报警的以下有关信息：

主机名

指定将报警发送到 Nimsoft 服务器的 CA ARCserve Central Protection Manager 服务器的主机名。

源

指定将报警发送到 Nimsoft 服务器的 CA ARCserve Central Protection Manager 服务器的 IP 地址。

重要级别

指定发送到 Nimsoft 服务器的报警的重要级别。

子系统

指定遇到报警状况的服务器的主机名。

示例：报警状况发生在 CA ARCserve D2D 服务器上。该系统字段指定 CA ARCserve D2D 服务器的主机名。

子系统 ID

指定遇到报警状况的服务器的 IP 地址。

Alarm SubConsole 允许 Nimsoft 管理员执行各种任务，例如：

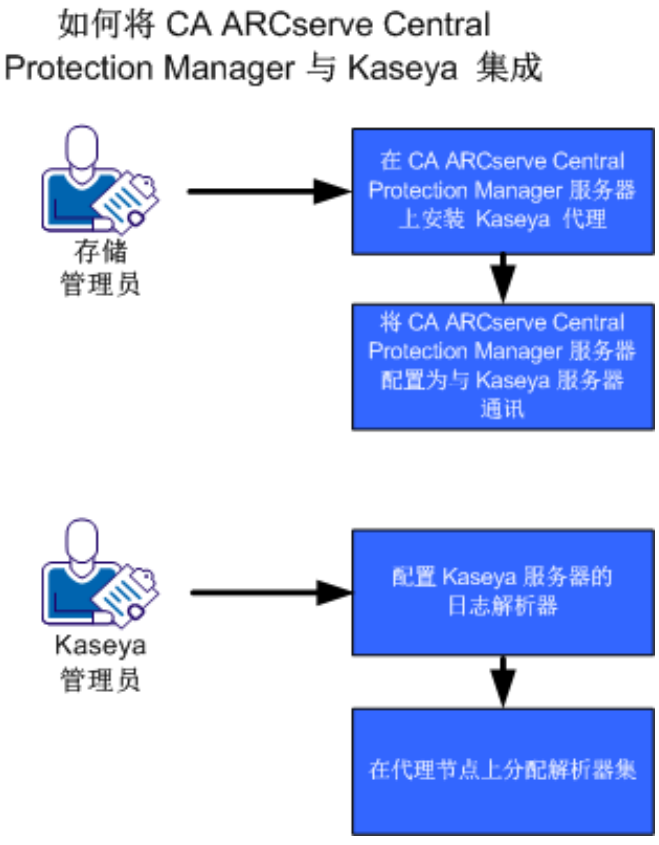
- 配置 Alarm SubConsole 在检测到报警时将电子邮件发送到指定收件人
- 查看报警的历史信息
- 确认报警
- 将警报分配给技术人员

注意：有关如何使用 Nimsoft Alarm SubConsole 的更多信息，请参阅 Nimsoft 文档。

如何将 CA ARCserve Central Protection Manager 与 Nimsoft Kaseya

存储管理员可以将 CA ARCserve Central Protection Manager 配置为将报警消息传送给 Kaseya 服务器。Kaseya 管理员可以将 Kaseya IT 基础架构管理工具配置为检测 CA ARCserve Central Protection Manager 报警、生成报警报告及发送电子邮件。管理员可以使用这些报告管理 CA ARCserve D2D 节点的健康。

下图说明存储管理员如何将 CA ARCserve Central Protection Manager 与 Kaseya IT 基础架构管理工具集成：



按照以下步骤将 CA ARCserve Central Protection Manager 与 Kaseya 集成：

1. 在 CA ARCserve Central Protection Manager 服务器上安装 Kaseya 代理 (p. 151)。
2. 配置 CA ARCserve Central Protection Manager 服务器与 Kaseya 服务器进行通信 (p. 151)。
3. 为 Kaseya 服务器配置日志解析器 (p. 152)。
4. 在代理节点上分配解析器集 (p. 154)。

安装 Kaseya 代理

在 CA ARCserve Central Protection Manager 服务器上安装 Kaseya 代理，以便允许其与 Kaseya 服务器进行通信。您通过从 Kaseya IT 管理控制台部署该代理，来安装它。

遵循这些步骤:

1. 打开浏览器窗口，并且登录到 Kaseya IT 管理控制台。

   从窗口左侧的导航栏，单击“代理”。

   代理选项显示。

2. 展开“安装代理”，然后单击“部署代理”。

   部署代理选项出现。

3. 请单击下列选项之一：

   单击可下载默认代理

   允许您将安装文件下载和保存到目标计算机上。

   下载完成后，在目标计算机上直接运行代理安装文件。

   创建包

   允许您创建一个安装包实用工具，以便在一个或多个台计算机上安装代理。按照屏幕说明，创建安装包。有关详细信息，请参阅 Kaseya 文档。

代理即得以安装。

配置 CA ARCserve Central Protection Manager 服务器与 Kaseya 服务器进行通信

CA ARCserve Central Protection Manager 允许您将报警消息发送到 Kaseya IT 管理服务器。要发送报警信息，请将 CA ARCserve Central Protection Manager 服务器配置为与 Kaseya 服务器通信。

遵循这些步骤:

1. 登录 CA ARCserve Central Protection Manager，然后单击导航栏上的“配置”。

   将显示配置选项。

2. 单击“配置”列表中的“IT 管理服务器配置”。

   IT 管理服务器配置选项显示。

3. 完成以下选项：
   a. 单击“启用”。
   b. 单击“Kaseya”。
   c. 指定重复方式。“重复方式”定义原始发送过程失败时在一周的哪几天重新向 Kaseya 服务器发送报警通知。Kaseya 服务器不可用或脱机时，发送报警的过程会失败。
   d. 指定排定。排定定义在什么时间向 Kaseya 服务器重新发送报警通知。

   单击“保存”。

CA ARCserve Central Protection Manager 服务器即被配置与 Kaseya 服务器通信。

为 Kaseya 服务器配置日志解析器

要查看 CA ARCserve Central Protection Manager 报警的有关信息，请配置 Kaseya 服务器读取 CA ARCserve Central Protection Manager 警报日志文件中的数据。

遵循这些步骤:

1. 打开浏览器窗口，并且登录到 Kaseya IT 管理控制台。
2. 从窗口左侧的导航栏，单击“监视器”。

   将显示监视器选项。
3. 展开“日志监控”，然后单击“日志解析器”。

   日志解析器配置选项出现。
4. 在“计算机.组 ID”列表中，单击 CA ARCserve Central Protection Manager 服务器旁边的复选框。

   从日志文件解析器下拉列表框，单击 <SelectLogParser>。

   单击“新建”。

   “日志文件解析器定义”对话框打开。
5. 填写“日志文件解析器定义”对话框中的下列字段：

   解析器名称

   定义日志文件解析器文件的名称。

日志文件路径

定义 CA ARCserve Central Protection Manager 服务器上的日志文件的路径。日志文件的路径如下：

```
<HOME_CA ARCserve Central
Applications>\ITMgmtIntegration\<log_fle_name>
```

CA ARCserve Central Protection Manager 生成支持 Unicode 和非 Unicode 字符的日志文件。这些日志文件名称如下：

非 Unicode：

```
CentralAppAlertsForKaseyaANSI.log
```

Unicode：

```
CentralAppAlertsForKaseyaUTF8.log
```

重要说明！ Kaseya IT 管理控制台不支持 Unicode 字符。因此，请使用名为 CentralAppAlertsForKaseyaANSI.log 的日志文件。

日志存档路径

定义 CA ARCserve Central Protection Manager 服务器上的已存档日志文件的路径。默认情况下，Protection Manager 在日志文件超过 10 MB 时存档它。

注意：关于 Protection Manager 何时存档日志文件，如果要指定其他值，请在以下文件中修改 MaxLogFileSize 的值(MB)：

```
<HOME_CA ARCserve Central
Applications>\ITMgmtIntegration\Configuration\Edge-ITMgmtIntegration.
INI
```

说明

定义日志文件解析器文件的说明。

模板

定义 CA ARCserve Central Protection Manager 服务器上该日志文件所包含的数据的格式。使用以下语法：

```
$CACentral Protection Manager 计算机名称$ [$生成报警的产品$] $生成报警的计
算机名称$ $重要级别$ $从原始产品的发送时间$ $报警消息$
```

输出模板

定义 Kaseya 服务器上输出数据的格式。使用以下语法：

```
$Protection Manager 服务器$ $生成者$ $主机名$ $重要级别$ $发送时间$ $消息$
```

日志文件参数

创建下列日志文件参数：

注意：在您指定（参数）类型后单击“应用”以保存参数。

CA ARCserve Central Protection Manager 计算机名称

类型：String

生成报警的产品

类型：String

生成报警的计算机名称

类型：String

重要级别

类型：String

从原始产品的发送时间

类型：DateTime

格式：YYYY-MM-DD hh:mm:ss

报警消息

类型：String

单击“保存”。

日志解析器定义即得到保存。

6. 单击“关闭”。

“日志解析器定义”对话框关闭，日志解析器定义文件得以创建，并应用于 CA ARCserve Central Protection Manager 服务器。

分配 Kaseya 服务器上的解析器集

您配置解析器集，以筛选 Kaseya 管理控制台中的 CA ARCserve Central Protection Manager 报警的有关信息。解析器集定义您筛选的条件。例如，您可以基于重要级别、备份失败等筛选报警。

遵循这些步骤:

1. 打开浏览器窗口，并且登录到 Kaseya IT 管理控制台。
2. 从窗口左侧的导航栏，单击“监视器”。

   将显示监视器选项。

3. 展开“日志监控”，然后单击“分配日志解析器”。

   分配日志解析器集选项出现。

4. 在“将日志解析器分配给选定计算机”部分中，指定您需要的报警选项。

5. 从“选择日志解析器”下拉列表，单击要分配解析器集的日志解析器。

   从“定义解析器集”下拉列表，单击 <新建解析器集>。

   “编辑解析器集”对话框打开。

6. 在“解析器集名称”字段中，指定解析器集的名称，然后单击“新建”。

   将显示解析选项。

7. 指定下列值：

   解析器列

   定义要筛选的参数。

   操作符

   定义您想如何筛选包含在参数内的数据。

   参数文件

   定义要筛选的参数的值。

   单击“添加”，然后单击“关闭”。

   筛选便应用于该解析器集，“编辑解析器集”对话框关闭。

   注意：有关如何指定解析器集筛选的示例，请参阅解析器集筛选示例。

8. 从“选择日志解析器”下拉列表，单击要应用的日志解析器。

   从“定义解析器集”下拉列表，单击您创建的解析器集。

   从“计算机 ID”列，单击要应用解析器集的服务器旁边的复选框。

   单击“应用”。

日志解析器和解析器集便得以分配。

解析器集筛选示例

要创建仅筛选包含错误的报警的解析器集，请指定以下值：

解析器列

重要级别

操作符

等于

参数筛选

错误

要创建显示所有报警的解析器集，而不管重要级别是什么，请指定以下值：

解析器列

重要级别

操作符

包含

参数筛选

错误、警告、信息

要创建仅显示失败备份的有关报警，请指定以下值：

解析器列

报警消息

操作符

包含

参数筛选

备份、失败

配置 Kaseya 服务器检测和发送电子邮件

Kaseya 管理员可以将管理控制台配置为检测到来自 CA ARCserve Central Protection Manager 服务器的报警消息时向指定收件人发送电子邮件消息。有关详细信息，请参阅 Kaseya 文档。

在 Kaseya 代理日志监视器中查看报警的有关信息

Kaseya 代理日志监视器允许您基于您在日志解析器和解析器集中定义的条件查看报警日志。日志允许您确定和执行修正操作，以纠正报警状况。

在 Kaseya 代理日志监视器中查看报警的有关信息

1. 打开浏览器窗口，并且登录到 Kaseya IT 管理控制台。

   从窗口左侧的导航栏，单击“代理”。

   代理选项显示。

2. 展开“计算机状态”，然后单击“代理日志”。

   代理日志显示在窗口右侧。

3. 从服务器列表，单击您想查看其信息的服务器。

   单击“刷新”。

指定服务器的报警消息的有关信息显示。

第 6 章： CA ARCserve Central Protection Manager 故障排除

本节提供故障排除信息，帮助您识别和解决在使用 CA ARCserve Central Protection Manager 时可能遇到的问题。

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：

- 确保 Windows Server 服务在 CA ARCserve Central Protection Manager 服务器和源虚拟机（节点）上正运行。
- 确保在 CA ARCserve Central Protection Manager 服务器和源虚拟机（节点）上 Windows 防火墙例外应用于 Windows 文件和打印机共享服务。
- 确认仅当节点不属于域时，Windows 防火墙例外才应用于 Windows Netlogon 服务。在 CA ARCserve Central Protection Manager 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 Protection Manager 服务器和源虚拟机（节点）上执行下列步骤。

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

     此时打开“本地安全策略”窗口。

4. 在“本地安全策略”窗口中展开“本地策略”，然后展开“安全选项”。

   此时出现“安全策略”。

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

   此时打开“网络访问: 本地帐户的共享和安全模型”对话框。

6. 单击“本地安全设置”。

   从下拉列表中选择“经典 - 本地用户以自己的身份验证” 。

   单击“确定”。

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

  1. 登录到 CA ARCserve Central Protection Manager 服务器，然后打开命令提示符。

     执行以下命令

     ```
     secpol.msc
     ```

     “本地安全策略”对话框将打开。

  2. 选择本地策略，然后单击安全选项。

     搜索“网络安全: LAN 管理器身份验证级别 ”。

     双击该选项。

     “属性”对话框打开。

  3. 选择以下选项，然后单击“确定”。

     发送 LM 和 NTLM - 若协商使用 NTLMv2 会话安全

  4. 在命令提示符下，执行以下命令：

     ```
     gpupdate
     ```

  该值即被应用。

空白网页出现或者 Javascript 错误发生

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

症状：

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

此问题在以下条件下发生：

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

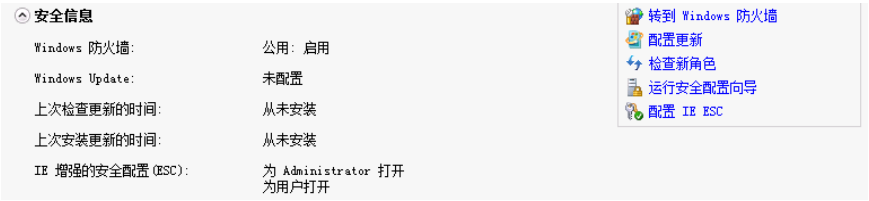
解决方案：

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

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

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

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



   Internet Explorer“增强的安全配置”对话框打开。

4. 在 Internet Explorer “增强的安全配置”对话框上，执行以下操作：
   - 关闭 Administrators--Click 检查
   - Users--单击“关”。

   单击“确定”。

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

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

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

   清除 Internet Explorer“增强的安全配置”旁边的复选框。

   单击“下一步”。

   按照屏幕上的说明完成配置，然后单击“完成”。

Internet Explorer 的“增强的安全性”即被禁用。

当登录到 CA ARCserve D2D 节点时，没有适当加载网页

Windows 平台上存在此问题。

症状：

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

解决方案：

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

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

1. 打开 Internet Explorer。

   在“工具”菜单中，单击“Internet 选项”。

   “Internet 选项”对话框将打开。

2. 单击“安全”选项卡。

   将出现“安全”选项。

3. 单击“Internet”区域。

   将显示“Internet”区域选项。

4. 单击“自定义级别”。

   “安全设置 - Internet 区域”对话框将打开。

5. 滚动到“脚本”类别。

   找到“活动脚本”。

   单击“启用”或“提示”选项。

6. 在“安全设置 - Internet 区域”对话框上单击“确定”。

   “安全设置 - Internet 区域”对话框将关闭。

7. 单击“Internet 选项”对话框的“确定”。

   “Internet 选项”对话框将关闭，“活动脚本”选项将应用。

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

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 Protection Manager 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 Protection Manager 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。

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

CA ARCserve Backup 同步过程失败

在 Windows 平台上有效。

症状：

CA ARCserve Backup 同步过程失败，可以在视图日志中查看。

解决方案：

在没有足够磁盘空间存储临时的同步数据（转储文件）时，CA ARCserve Backup 同步过程会失败。默认情况下，应用程序将转储文件存储到 ARCserve_Central_Applications_Home\ASBUSync 目录。

如果在 C:\Program Files 中的可用磁盘空间量有限制，而包含在 ASBUSync 内的文件消耗的磁盘空间量多于可用磁盘空间量，则该应用程序将无法检索需要完成同步过程所必需的 CA ARCserve Backup 数据库转储数据。因此，CA ARCserve Backup 同步过程失败。

或者，该应用程序允许您指定备用位置以存储 CA ARCserve Backup 同步数据。要解决该问题或防止该问题发生，请执行以下操作：

1. 登录 CA ARCserve Central Protection Manager 服务器。
2. 打开 Windows 注册表编辑器，并浏览至以下注册表项：

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve Central Application\CM`
3. 右键单击 CM，在弹出菜单上选择“新建”,然后单击“字符串值”。

   命名注册表项，如下所示：

   `ARCserveSyncPath`
4. 右键单击“ARCserveSyncPath”并单击弹出式菜单上的“修改”。

   “编辑字符串”对话框将打开。
5. 在“值数据”字段中，指定您想存储 CA ARCserve Backup 同步数据的备用位置。

   单击“确定”。

备用位置即被指定。

CA ARCserve D2D 重新部署操作失败

Windows 平台上存在此问题。

症状：

在将 CA ARCserve D2D 重新部署到节点时，部署过程未成功完成。发生下列任一事件时，该症状将更加明显：

- 在“D2D 部署”对话框的“部署状态”中显示下列消息之一：

  用户未成功登录。

  在目标计算机上安装了该产品的相同版本、更新版本或某一不受支持的版本。要安装该产品的当前版本，您必须从目标计算机卸载以前的版本。

  安装程序无法将文件复制到远程计算机。

- 节点未显示在“节点”屏幕上。
- 节点显示在“节点”屏幕上，但其状态不正确。例如，  图标显示在“节点”屏幕上，或  图标未显示在“节点”屏幕上。

解决方案：

在下列情况下会发生这些事件：

- CA ARCserve Central Applications Web 服务在部署过程中停止或重新启动，但目标服务器在安装 CA ARCserve D2D 之后未重新启动。
- CA ARCserve Central Applications 服务器在部署过程中重新启动，但目标服务器在安装 CA ARCserve D2D 之后未重新启动。

解决方案是执行以下操作：

1. 登录到 D2D 服务器并重新启动该服务器。
2. 登录到 Central Protection Manager 并完成下列任务之一：
   - 如果节点显示在“节点”屏幕上的节点列表中，但状态不正确，请更新节点。

     要更新节点，请单击节点，然后单击弹出式菜单上的“更新”。
   - 如果节点未显示在“节点”屏幕上的节点列表中，请手动添加该节点。

     要手动添加节点，请单击工具栏上的“添加”，然后单击弹出式菜单上的“按照 IP/名称添加节点”。

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。

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

在所有 Windows 操作系统上有效。所有浏览器受到影响。

症状：

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

解决方案：

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

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

更改节点的名称后节点不显示在“节点”屏幕上

在 Windows 平台上有效。

症状：

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

解决方案：

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

要在节点屏幕显示重命名的节点，请执行以下操作：

1. 重命名节点。
2. 打开“节点”屏幕，删除重命名的节点 (p. 58)。
3. 使用新名字添加节点 (p. 52)。

CA ARCserve Central Protection Manager 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 Protection Manager 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 Protection Manager 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 D2D 部署之后节点未得到管理

Windows 平台上存在此问题。

症状：

在我将 CA ARCserve D2D 部署到本地或远程服务器上的一个节点时，节点被添加到节点组，但是状态为“未受管理”。

该问题在以下情况发生：

- CA ARCserve D2D 被部署到远程节点，而未重新启动系统。
- CA ARCserve D2D 被部署到本地 CA ARCserve Central Applications 服务器，无论是否重新启动系统。

解决方案：

要解决该问题，请重新启动 CA ARCserve D2D 服务器，然后在 CA ARCserve Central Protection Manager 中更新 CA ARCserve D2D 节点信息。状态便为受管理。

如何设置节点数据删除的排定

Windows 平台上存在此问题。

症状：

默认情况下，节点数据删除排定被设在每天凌晨 2 点清除已删除节点的数据。我想自定义多个数据删除的排定。

解决方案：

要为节点数据删除创建自定义排定，请该注册表项的值 CA ARCserve Central Applications\CM\ShowDeleteNodeConfigurationUI 设置为 1。将注册表项设置为 1 会将“节点数据删除配置”选项卡添加到 CA ARCserve Central Protection Manager 应用程序的“配置”面板，以便您可以更改排定。

注意：要访问该注册表，直接登录到 CA ARCserve Central Protection Manager 服务器，然后转到“开始”>“运行”> Regedit。

CA ARCserve Central Applications 数据库服务未启动

在 Windows 平台以及 Microsoft SQL Server 和 Microsoft SQL Server Express Edition 数据库上有效。

症状：

在您启动或重新启动 CA ARCserve Central Protection Manager 服务器 或安装 CA ARCserve Central Applications 数据库的服务器时，CA ARCserve Central Applications 数据库服务未启动。

解决方案：

启动计算机时，服务向操作系统报告它们的启动状态。服务在预定时间（或超时时间）内未向操作系统报告状态时，Windows 将停止服务。默认情况下，在 CA ARCserve Central Applications 服务在启动时间的 30 秒钟内未向 Windows 报告状态时，Windows 将停止 CA ARCserve Central Applications 数据库服务。在数据库安装在缺乏足够资源的服务器上时，您更有可能遇到该类型问题。然而，可以通过增加启动超时时间，来防止该问题发生。要增加超时时间，请执行以下操作：

1. 打开 Windows“注册表编辑器”，并找到以下注册表键：
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`
2. 右键单击“Control”，指向“新建”，然后在弹出菜单上单击“项”。

   名为“New Key #1”的项即被创建。
3. 将“New Key #1”重命名为 ServicesPipeTimeout。
4. 右键单击“ServicesPipeTimeout”并单击弹出式菜单上的“修改”。

   “编辑 DWORD 值”对话框将打开。
5. 在“值数据”字段中，指定要为超时时间设置的值。以毫秒表示该值。例如，要将超时时间设置为 60 秒，在“值数据”字段指定 60000。

   注意：1 秒等于 1000 毫秒。

   单击“确定”。

   超时时间即被应用。
6. 要将更改应用到 Windows，请重新启动计算机。

将策略保存或分配到 CA ARCserve D2D 服务器时发生多连接错误

在所有 Windows 平台上有效。

症状：

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

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

解决方案：

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

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

    ```
    net session \\machinename /delete
    ```

  - 转到以下目录来断开该会话：

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

数据同步和策略部署操作失败

Windows 平台上存在此问题。

症状：

CA ARCserve D2D 数据同步操作启动之后，活动日志中显示以下消息：

应用程序无法登录到 CA ARCserve D2D 服务。

向节点部署策略时，将显示以下消息框：

部署策略失败（无法连接到节点）。

解决方案：

当节点在 CA ARCserve Central Protection Manager 服务器上注册之后从该节点卸载 CA ARCserve D2D，然后又手动将 CA ARCserve D2D 重新安装到该节点上时，会发生此行为。当使用 CA ARCserve Central Protection Manager 部署实用工具在节点上重新安装 CA ARCserve D2D 时，不会发生该行为。

该行为的解决方案是从“节点”屏幕更新节点。要更新节点，请单击节点，然后单击弹出式菜单上的“更新”。然后完成“更新节点”对话框中的必填字段。

错误代码故障排除

下表说明使用 CA ARCserve Central Protection Manager 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。
12884901935	无法连接到 *** 上的 CA ARCserve Backup 服务，错误代码是 12884901935。确保节点的所有条目正确，并且 CA ARCserve Backup 服务正在运行。	确保 CA ARCserve Communication Foundation 服务在节点上正运行。

错误代码	说明	可能的解决方法：
12884901936	无法连接到 *** 上的 CA ARCserve Backup 服务，错误代码是 12884901936。确保 CA ARCserve Central Applications 支持安装在节点上的 CA ARCserve Backup 服务版本。	进行以下验证： ■ CA ARCserve Central Applications 支持安装在节点上的 CA ARCserve Backup 服务版本。 ■ CA ARCserve Communication service 在节点上正运行

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。

来自本地化服务器的字符在 Nimsoft UMP 报警控制台中显示为乱码文字

在 Windows 上有效。

症状：

从本地化服务器接收的报警消息的字符在 Nimsoft Unified Monitoring Portal (UMP) 报警控制台中显示为乱码文字。

解决方案：

发送报警的服务器上运行的字符集不同于 Nimsoft 服务器上运行的字符集时，便发生此问题。该问题的解决方案为，配置 Nimsoft 服务器使用 UTF-8 编码。要配置 Nimsoft 服务器使用 UTF-8 编码，请执行以下操作：

1. 确保将显示板引擎配置成将 –Dfile.encoding=utf-8 用作启动参数。
2. 确保将 wasp Extra Java VM 参数选项定义为 –Dfile.encoding=utf-8。

注意：有关详细信息，请参阅 Nimsoft 文档。