HP Data Protector for PCs 7.0
安装和管理指南

HP 部件号：不适用
出版日期：2011 年 6 月
第 1 版

目录

关于本指南

本指南提供以下相关信息：

- 安装 HP Data Protector for PCs
- 配置 HP Data Protector for PCs 策略
- 用户台式机和笔记本上的 HP Data Protector for PCs 代理软件
- 确定可以支持的Agent数
- 获取对 Data Protector for PCs 的支持

目标读者

本指南旨在供想要安装和配置 HP Data Protector for PCs 的管理员使用。 它将有助于您熟悉以下内容：

- Windows 管理

文档约定和符号

约定	元素
蓝色文本：“关于本指南”（第 5 页）	交叉引用链接和电子邮件地址
蓝色且带下划线的文本：http://www.hp.com	网站地址
加粗文本	• 按键 • 键入到 GUI 元素（比如框）中的文本 • 单击或选中的 GUI 元素，比如菜单和列表项目、按钮、选项卡和复选框
斜体文本	强调的文本
`Monospace` 文本	• 文件和目录名称 • 系统输出 • 代码 • 命令及其参数和参数值
`Monospace, italic` 文本	• 代码变量 • 命令变量
`Monospace, bold` 文本	强调的 monospace 文本

重要信息： 提供阐释信息或特定说明。

注意： 提供其他信息。

常规信息

有关 Data Protector for PCs 的常规信息，请访问 http://www.hp.com/go/dataprotector。

HP 技术支持

有关全球技术支持信息，请访问 HP 支持网站：

http://www.hp.com/support

在与 HP 联系之前，请收集以下信息：

- 产品型号名称和编号
- 技术支持注册号（如果适用）
- 产品序列号
- 错误消息
- 操作系统类型和修订级别
- 详细问题

订阅服务

HP 建议在“订户业务选择”网站注册产品：

http://www.hp.com/go/e-updates

注册之后，您将收到有关产品增强功能、新驱动程序版本、固件升级和其他产品资源的电子邮件通知。

HP 网站

有关其他信息，请访问以下 HP 网站：

- http://www.hp.com
- http://www.hp.com/go/dataprotector
- https://h20230.www2.hp.com/selfsolve/manuals
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

文档反馈

HP 欢迎您提出反馈。

要提供有关产品文档的意见和建议，请将邮件发送到 DP.DocFeedback@hp.com。 提交的所有内容均视为 HP 的宝贵财产。

1 概述和先决条件

Data Protector for PCs 概述

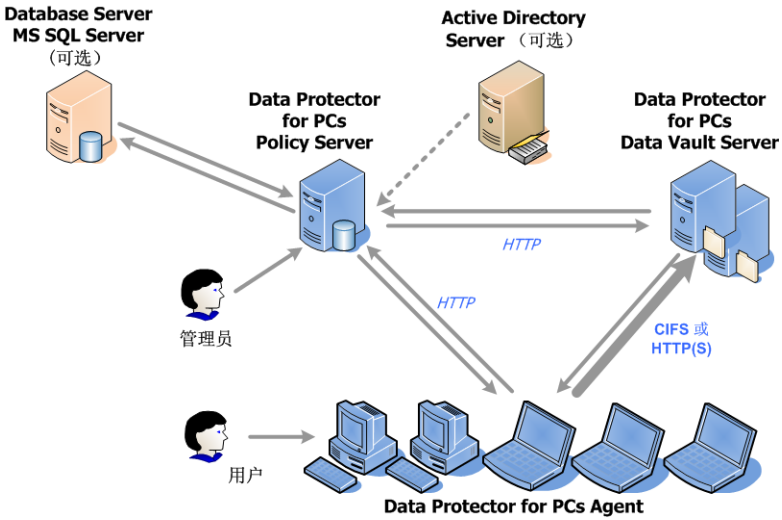
HP Data Protector for PCs 由两个主要软件组件（Policy Server 和代理）组成。 Policy Server 在 Windows 服务器上运行 — 请参见“支持矩阵”了解支持的版本 (https://h20230.www2.hp.com/selfsolve/manuals)。 代理在每个台式机或便携式计算机上以后台方式运行。

Policy Server 还可以访问 Active Directory 服务器中包含的组和组织单位。

用户的数据将备份到 Data Vault。 Data Vault Server 应该不同于 Policy Server。 如果使用的是 Windows 文件共享 Data Vault，而不是建议的 Web Data Vault，则这些 Data Vault 位于文件服务器的一个或多个 Windows 文件共享上。

下图说明了 Data Protector for PCs 的体系结构：

图 1 **Data Protector for PCs** 体系结构



各种策略将控制从台式机和便携式计算机备份的文件以及这些备份的保存位置。 您可以通过 Policy Server 控制台定义这些策略。 然后使用 SOAP 协议通过 HTTP 端口 80 自动将策略分发到代理。这些策略将保存在 Policy Server 上。

代理可以执行这些策略。 当用户更改受这些策略保护的数据文件时，将在台式机/便携式计算机的本地硬盘上创建以前版本，并在对文件的更改进行压缩后将其复制到所有适用的 Data Vault。

只要备份了文件，代理就会向 Policy Server 发出通知，其中包含用户对文件所做更改的审核历史记录。 此外，每个代理还会定期将“运行状况”信息发送到 Policy Server。您可以通过 Policy Server 控制台生成此数据的报告。

Data Vault 位于 Data Vault Server 上。 可以使用以下两种不同的协议将客户端数据复制到 Data Vault： CIFS（适用于 Windows 文件共享 Data Vault）或 HTTP（适用于 Web Data Vault）。

Data Vault Server 应该位于不同于 Policy Server 的系统上。 对于 HTTPS，Web Data Vault Server 软件将与 Data Protector for PCs Cleanup 软件一起在其上运行。 对于 Windows 文件共享 Data Vault，其上仅安装 Cleanup 软件。

如果使用 Active Directory，则可以配置 Policy Server 以访问组和组织单位。 然后可以根据用户的组或组织单位成员身份将 Data Vault 分配给用户。 还可以根据用户的成员身份在报告中选择用户。

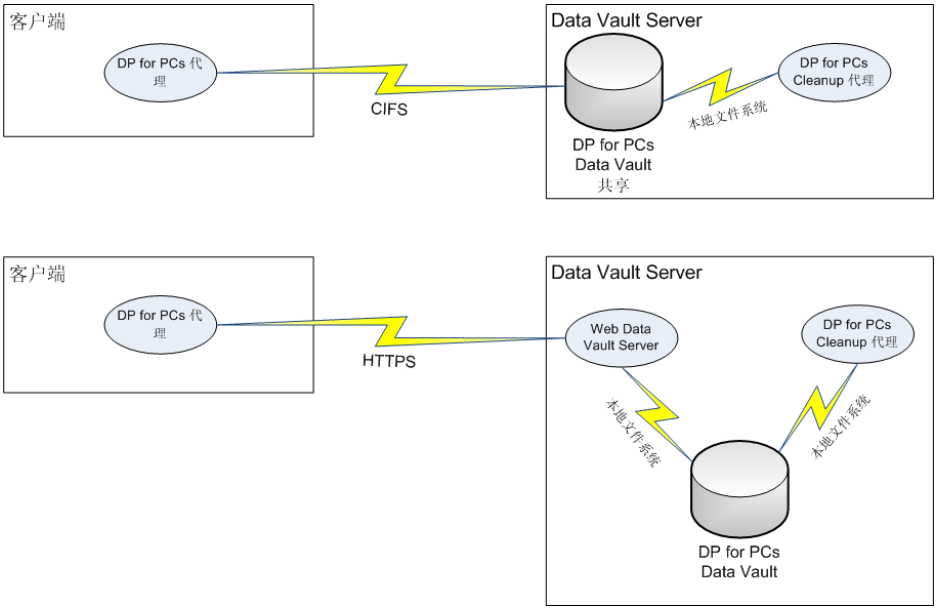
Data Vault

Data Protector for PCs 可能有两种类型的 Data Vault：

- Web Data Vault — 基于 HTTPS 协议。 它们可在高延迟环境中提供最高级别的安全性以及更好的吞吐量，因此建议使用此类型 Data Vault。
- Windows 文件共享 Data Vault — 基于 CIFS 协议，在 Data Protector for PCs 的早期版本中使用。

这两种 Data Vault 的数据结构相同，因此可以将现有 Windows 文件共享 Data Vault 转换成 Web Data Vault。

图 2 Windows 文件共享 Data Vault 与 Web Data Vault 比较



证书处理

Web Data Vault 强制要求使用 SSL。 在 Web Data Vault 安装期间确定证书的类型。为了保证产品开箱即可正常运行（例如，出于评估目的），可以使用自签名证书安装

Web Data Vault Server。 这不及使用受信任的颁发机构 (CA) 颁发的证书来得安全。为确保绝对安全，应在您的环境中导入受信任的颁发机构签发的 Data Vault Server 证书，并将其添加到服务器组件中。

自签名证书

创建 Data Vault 策略时，可以定义是否允许使用自签名证书。 在这种情况下，无需在代理端执行任何操作。 通过安装发布的自签名证书的有效期为 20 年。

导入证书

导入过程要求提供一个 PEM 格式文件，其中包含私钥以及包含公钥的匹配证书。 请注意，应将该文件按原样复制到 Web Data Vault 服务器配置目录。 根据证书文件的创建过程，该文件可能会加密。 在这种情况下，运行 Web Data Vault 服务器的 Windows 服务进程会显示交互式提示以获取解密密码。 安装过程中以及将来每次重新启动该服务时（例如，重启系统之后）都会出现此提示。 尽管可以将该密码手动添加到 Web 服务器配置文件中以避免出现此提示，但安装过程不支持该操作。 建议不要使用加密证书文件，也不要将密码存储在该文件旁边的某个文件中。

注意：
“受信任的颁发机构”一词意味着运行代理的客户端计算机将认为该 CA 可信，并接受由其签发的证书。 假设已通过添加该 CA 签发的证书及其连锁机构中其他可能的证书，对客户端计算机的 Windows 证书存储进行了相应的设置。 代理不包含任何用于建立此信任的机制。 它依赖于 Windows 机制。

交换证书

安装后，可以随时使用 `DvConfig` 实用工具（在 CLI 一段的“从 CLI (DvConfig) 配置 Web Data Vault 选项”（第 18 页）中介绍）交换 Web Data Vault Server 上的证书。例如，可以将最初使用自签名证书设置的安装重新配置成使用导入证书。

Data Protector for PCs 安装概述

注意： 如果要更新 Data Protector for PCs 的安装，请参见“更新 Data Protector for PCs”（第 36 页）。

安装 Data Protector for PCs 可分为三个阶段：

1. 安装 **Data Protector for PCs Policy Server**。
   请参见 “安装 Data Protector for PCs Policy Server”（第 13 页）。
2. 安装 **Data Protector for PCs Web Data Vault Server** 软件。
   请参见 “安装、配置和维护 Web Data Vault Server”（第 16 页）。
3. 配置保护策略。
   请参见 “配置 Data Protector for PCs 保护策略”（第 20 页）。

4. 在台式机和便携式计算机上安装 **Data Protector for PCs** 代理。
   请参见 “安装 Data Protector for PCs 代理”（第 32 页）。

先决条件

Policy Server

有关受支持的操作系统，请参见“支持矩阵”。

注意： 在 **Windows 2003 64** 位操作系统上安装：Policy Server 在 64 位 Windows 操作系统上以 32 位兼容模式运行。 这意味着 Internet Information Services (IIS) 必须以 32 位模式运行。 否则，安装程序在检查先决条件时会检测到此情况。 然后，它会提供用于将 IIS 设置为 32 位模式的选项。 如果要求 IIS 处于 64 位模式下的服务器（比如具有 Web 邮件 — Outlook Web Access 的 Microsoft Exchange 2007）上有其他 Web 应用程序，则不能在该服务器上安装 Policy Server。 这不适用于在 Windows 2008 上安装 Policy Server。

服务器必须安装以下各项：

- 支持 ASP.NET 应用程序的 Internet Information Services 6.0、7.0、7.5 或更高版本。

  对于 Windows 2003，IIS 6.0 是必备软件，必须在安装 Policy Server 之前安装。对于 Windows 2008，Data Protector for PCs 提供 IIS 7.0 和 7.5 的安装（如果尚未安装）。

- Microsoft ASP.NET 2.0

服务器上还需要安装以下各项：

- Microsoft Installer 3.1 或更高版本（.NET Framework 2.0 SP1 的必需软件）。
- Microsoft .NET Framework 2.0 SP1 或更高版本。 向导将安装 2.0 SP1。
- Microsoft SQL Express（如果不存在其他 SQL 版本）

而且，只有 Internet Information Services 7.0 和 7.5 才需要以下 IIS 组件。 如果未安装这些软件，则向导会为您提供机会安装这些软件：

- IIS 静态内容 Web 服务器 — 用于为静态 html 文件、文档和图像提供服务
- IIS ASP.NET — 用于部署 ASP.NET 2.0 和 .NET Framework
- IIS 安全 — 用于使用 Policy Server 控制台所需的集成 Windows 身份验证。
- IIS 6 管理兼容性 — 允许安装程序以同样的方式在尽可能远的范围内配置 IIS 6 和 IIS 7

数据库

Data Protector for PCs 需要访问 Microsoft SQL Server 数据库。 有关受支持的版本，请参见"支持矩阵"。

可以使用 Microsoft Enterprise Manager 验证（和更改）SQL Server 安装的身份验证模式：

1. 右键单击 SQL Server 实例，选择属性，并单击安全选项卡。
2. 应当已选择 **SQL Server** 和 **Windows** 选项（而不是仅 **Windows** 选项）。 否则，请选择该选项并单击确定。

或者，在 Data Protector for PCs 安装期间，还可以安装 Microsoft SQL Server Express Edition 版本的实例。

Data Protector for PCs Web Data Vault Server

- Web Data Vault Server 应安装在不同于 Policy Server 的系统上。（也可以将其安装在同一个系统上，但仅适于评估目的）。
- 应安装 Java Runtime Environment 1.6 或更高版本。
- 变量 `JAVA_HOME` 和 `JRE_HOME` 必须指向 Java Runtime 安装目录。

Data Protector for PCs 代理

Data Protector for PCs 代理软件可以安装在运行 Windows 的用户台式机和笔记本上。有关受支持的平台，请参见“支持矩阵”。

2 安装 Data Protector for PCs Policy Server

注意： 通过执行标准安装步骤，可以将已安装的 Data Protector for PCs Policy Server 更新到较新的版本。 有关更多详细信息，请参见“更新 Policy Server”（第 36 页）。

快速安装

有关 Data Protector for PCs Policy Server 的要求，请参见“Policy Server”（第 11 页）。

1. 插入 Data Protector for PCs 安装 CD-ROM。 如果安装向导没有自动启动，请通过双击安装 CD-ROM 的根目录中的 `setup.hta`，手动运行该向导。
2. 按照屏幕上的说明操作。
3. Data Protector for PCs Policy Server 要求访问 Microsoft SQL Server 数据库。 选择使用 **Microsoft SQL Server Express** 的现有 **Data Protector for PCs** 实例，或者单击使用 **Microsoft SQL Server** 的现有实例。 如果选择使用现有 SQL Server，则需要为具有足够特权创建新数据库的帐户提供数据库服务器连接字符串和凭据。
4. 在向导的安装 **Data Protector for PCs Policy Server** 页上单击安装开始安装。
5. 安装完成后，单击下一步。 然后，可以选择运行 Data Protector for PCs Policy Server 控制台。
6. 在单独的系统上安装 Web Data Vault Server。 单击主安装屏幕上的安装 **Data Vault**。

注意： 安装期间，Cleanup 软件将始终随 Web Data Vault Server 软件一起安装。 对于仅托管 Windows 文件共享 Data Vault 的 Data Vault Server，建议在 Data Vault 上进行本地安装以提高性能。

详细安装

注意：

仅 **Windows 2003** 服务器：如果此服务器的 .NET 2.0 Framework 运行时安全策略对本地 Intranet 安全区域设置为完全信任，则只能从网络上共享的 CD-ROM 或从网络文件共享安装 Data Protector for PCs Policy Server。 如果服务器没有本地 CD-ROM 驱动器，请使用“管理工具”中的“.NET Framework 2.0 配置”工具将本地 Intranet 安全区域的运行时安全策略更改为完全信任，或将服务器文件夹从 CD 复制到服务器上的本地磁盘。

必须登录到具有“管理员”权限的帐户才能执行 Data Protector for PCs Policy Server 安装。

1. 插入 Data Protector for PCs 安装 CD-ROM。 如果安装向导没有自动启动，请通过双击安装 CD-ROM 的根目录中的 `setup.hta`，手动运行该向导。
2. 单击安装 **Policy Server**。

   如果系统显示询问，请选择从其当前位置打开（或运行）此程序，而不是将此程序保存到磁盘。

3. Data Protector for PCs Policy Server 需要安装 .NET Framework 2.0 SP1。 如果尚未安装此 SP1，系统会询问您是否要从 CD-ROM 进行安装。

   此安装需要 Windows Installer 3.1 或更高版本，因此如有必要，系统会询问您是否要从 CD 安装 Windows Installer 3.1。

4. 安装向导会检查是否安装了其他必备软件：

   - Internet Information Services (IIS)
   - ASP.NET 2.0

   如果缺少任一款必备软件，请在列表中单击该必备软件以了解有关如何安装它的详细信息。

   单击下一步。

5. 安装 Microsoft SQL Server。

   使用现有 **Microsoft SQL Server** 实例：

   a. 单击使用现有 **Microsoft SQL Server** 实例。
   b. 在数据库服务器字段中，输入现有数据库服务器的连接字符串。
   c. 在登录和密码字段中，输入具有足够权限创建新数据库的帐户所对应的凭据。通常，该账户将是“sa”帐户。
   d. 单击下一步。 输入的连接信息将用于对现有数据库服务器进行连接测试。 如果连接成功，向导将继续执行步骤 6。

   安装 **Microsoft SQL Server Express Edition** 的 **Data Protector for PCs** 实例：

   a. 选择安装 **Microsoft SQL Server Express** 的 **DataProtectorNE** 实例，并单击下一步。
   b. 单击安装，安装 Microsoft SQL Server 2005 Express Edition 的名为“DataProtectorNE”的实例。 安装完成后，单击下一步。

6. 安装 Data Protector for PCs Policy Server 软件

   a. 在欢迎屏幕上，单击下一步开始安装。

      - Data Protector for PCs Policy Server 控制台将作为 Web 应用程序安装在虚拟目录 `C:\Inetpub\wwwroot\dpnepolicy` 中。
      - Data Protector for PCs Web 服务将安装在 `C:\Inetpub\wwwroot\dpnepolicyservice` 中。

      两者都在端口 80 上使用 HTTP 协议。

   b. Policy Server 安装完成后，单击关闭和下一步。

7. 现在需要安装 Cleanup 程序。 单击安装开始安装。
8. Cleanup 安装完成后，单击下一步。

   可以从 Data Protector for PCs Policy Server 控制台集中管理 Data Protector for PCs。由于该控制台基于浏览器，因此可以通过可建立浏览器与 Policy Server 间连接（使用 HTTP 端口 80）的任意计算机管理 Data Protector for PCs。

要在 Policy Server 上从浏览器运行 Data Protector for PCs Policy Server 控制台，请选中运行 **Policy Server** 控制台复选框并单击完成。

注意： 安装期间在 Policy Server 上安装了 Cleanup 软件。 还建议在 Data Vault 上安装该软件，以便提高性能。

注意：

Policy Server 控制台的浏览器设置：如果在浏览器中显示 Policy Server 控制台页时遇到问题，请检查浏览器安全设置。 该控制台需要满足以下条件：

- 必须启用 JavaScript。
- 必须为 dpnepolicy 网站禁用弹出阻止程序。
- 可能需要根据特定的浏览器及其版本，修改其他限制性安全设置。

附带安装 **Microsoft SharePoint**：在运行 Microsoft SharePoint 的服务器上安装 Policy Server 后，如果运行 Policy Server 控制台，可能会收到 404 错误“找不到该页面”。 http://support.microsoft.com/kb/828810 上的 Microsoft 知识库文章描述了此问题及解决办法。 请注意，此问题适用于所有 ASP.NET Web 应用程序，而不仅仅是 Policy Server。

要让 Policy Server 在使用 SharePoint 的服务器上运行，需要执行以下操作：

1. 使用 SharePoint 管理工具为两个 Policy Server Web 应用程序创建排除：`dpnepolicy` 和 `dpnepolicyservice`。
2. 修改两个 Policy Server `web.config` 文件（`dpnepolicy\web.config` 和 `dpnepolicyservice\web.config`）以添加 `<httpHandlers>` 和 `<trust>` XML 代码，如上面引用的 Microsoft 知识库文章中所述。

---

3 安装、配置和维护 Web Data Vault Server

安装和配置 Web Data Vault Server

注意： 在不同于 Policy Server 的单独系统上安装 Web Data Vault Server （也可以将其安装在同一个系统上，但仅适于评估目的）。

1. 插入 Data Protector for PCs 安装 CD-ROM。 如果安装向导没有自动启动，请通过双击安装 CD-ROM 的根目录中的 `setup.hta`，手动运行该向导。
2. 单击安装 **Data Vault**。
3. 选择以下两个选项之一：
   - **Web Data Vault Server**（建议）。 选择此项还会在服务器上安装 Cleanup 软件。
   - 适用于 **Windows** 文件共享 **Data Vault** 的 **Cleanup** 软件。 如果只想使用 Windows 文件共享 Data Vault，请选择此项。

   有关详细信息，请参见 “Data Vault”（第 9 页）。
4. 按照屏幕上的说明完成安装过程。
5. 从 Policy Server 获取许可证后，如果要安装 Web Data Vault Server，请开始配置 Web Data Vault。

   在“服务器设置”屏幕中，输入服务器的完全限定域名 (FQDN) 和 SSL 端口。 在 Policy Server 上配置 Web Data Vault 策略时，也需要使用此 FQDN。 该名称必须能由所有客户端进行解析，否则，可能无法将其中的部分内容备份到该服务器上的 Data Vault。
6. 在“证书设置”屏幕中，必须选择以下两个选项之一：
   - 导入受信任颁发机构 (CA) 发布的现有 SSL 证书。 建议使用此选项，可提供最高安全级别。
   - 创建自签名 SSL 证书。 此选项提供的安全级别较低，应仅用于评估目的。

   注意： 安装后，可以随时使用 `DvConfig` 实用工具交换 Web Data Vault Server 上的证书。 这包括将使用自签名证书的安装重新配置成使用导入证书。 请参见 “从 CLI (DvConfig) 配置 Web Data Vault 选项”（第 18 页）。
7. 下一个屏幕将要求您提供 Data Vault Server 中两种类型用户的名称：
   - 管理用户 — 负责管理任务，例如创建和删除 Data Vault 以及迁移客户端备份数据。
   - 备份用户 — 执行最终用户操作，例如备份和恢复文件。

   这些用户特定于 Data Protector for PCs Web Data Vault Server。 创建或编辑此服务器的 Web Data Vault 时，需要输入这两类用户的详细信息。

注意： 密码长度必须至少为 8 个字符。

8. 依次单击下一步和完成，完成 Web Data Vault Server 的安装和配置以及 Cleanup 软件的安装。

维护 Web Data Vault

1. 在“Data Vault 策略”页面上，输入服务器的完全限定域名和 SSL 端口以及备份用户的帐户凭据。 然后单击配置 **Data Vault**。
2. 提交管理用户帐户凭据，将显示“维护 Web Data Vault Server”页面。

   此时可以选择或删除现有的 Web Data Vault。 还可以添加新的 Data Vault。

   注意： 只能选择当前未连接到其他 Data Vault 策略的现有 Data Vault。
3. 确保单击页面底部的保存以保存 Data Vault 策略。
4. 如果已添加新的 Data Vault，可以测试此 Vault 是否存在以及配置是否正确（可选）。

将数据从 Windows 文件共享 Data Vault 迁移到 Web Data Vault

对于 Windows 文件共享 Data Vault 和 HTTPS Web Data Vault，其 Data Vault 中的数据布局相同。 这表示可以将数据从现有 DPNE 6.x Data Vault 迁移到新的 Web Data Vault。

注意： 只能对属于同一个 Policy Server 或共享相同加密密码的 Data Vault 执行数据迁移。

有两种可能的数据迁移方案：

- 使用同一个系统托管 Web Data Vault。

  注意： 不支持通过 Windows 文件共享和 Web Data Vault 并行访问相同的目录。
- 将整个 Data Vault 移到其他系统。

在这两种情况中，都必须在数据应驻留的本地系统上安装 Web Data Vault Server。

将数据从现有 **Windows** 文件共享 **Data Vault** 迁移到 **Web Data Vault**：

注意：

- 在非工作时间执行迁移，以便尽量减小对运行备份的影响。
- 查看 Windows 任务管理器，确保 `DPNECleanup.exe` 当前未运行。
- 检查 Policy Server 上的清理策略，确保迁移期间未计划运行 `DPNECLeanup.exe`。

1. 安装 Web Data Vault Server 并将 Policy Server 和代理更新到 7.0 版。 确保安装 7.0 版后对所有代理执行了重启，因为这些代理只有重启后才能开始将数据备份到 Web Data Vault。
2. 禁用 Data Vault 策略页面上相应的 Windows 文件共享策略，可以使代理停止将数据复制到 Data Vault。
3. 如果要对 Web Data Vault 使用相同的目录，则通过 CIFS 停止共享该目录。
4. 如果 Web Data Vault 与 Windows 文件共享 Data Vault 位于不同的服务器上，则必须将数据复制到其文件夹路径长度不超过 67 个字符的计算机中。 如果 Data Vault 位于相同的服务器上，除非出于其他原因特意这样做，否则无需将数据复制到新位置。
5. 创建新 Web Data Vault 之前，确定初始更新进程的行为。 如果所有代理都执行了初始更新，可以跳过初始更新，此时已在现有 Data Vault 上完成备份数据。 跳过初始更新的选项不直接属于 Data Vault 策略，而是所引用复制策略的一部分。 确保 Data Vault 策略选择了正确选项（即关闭了“初始更新”并具有适当的限制和计划设置）。 为此创建新复制策略，或修改现有策略（在这种情况下，引用该复制策略的所有 Data Vault 策略都将受到影响）。
6. 为 Web Data Vault 创建并保存新的 Data Vault 策略。 创建新 Web Data Vault 时，必须提供文件夹路径，在此示例中，该路径是正在迁移的 Windows 文件共享 Data Vault 实际数据所驻留的位置。 选择步骤 5 中创建的复制策略。按照与原始 Windows 文件共享 Data Vault 策略（例如，网络设置、Active Directory 设置）中相同的设置方式设置 Data Vault 策略的其他选项。
7. 确定代理将文件成功备份到新 Web Data Vault 后，删除原始 Windows 文件共享 Data Vault 策略。

策略保存后，代理将使用 HTTPS 协议将数据重新复制到新 Web Data Vault。

从 CLI (DvConfig) 配置 Web Data Vault 选项

从 CLI 使用该实用工具，可以更改 Web Data Vault 的配置参数（例如，备份用户和管理用户及其密码）、导入新证书、更改 SSL 以及创建新的自签名证书。

在更改任何参数之前，必须通过停止 Windows 服务 HP Data Protector for PCs Data Vault Server 来停止 Web Data Vault Server。

完成更改后，重新启动 Web Data Vault 服务。 所有更新的策略都将重新分配给代理。

注意： 如果使用 DvConfig 更改 Web Data Vault 服务器上的 SSL 端口、备份用户名或密码，请确保更改 Policy Server 上相应的 Data Vault 策略以保持一致。

用法:

```
DvConfig [-adminUser 登录:密码 -backupUser 登录:密码] [-h] [-i 证书文件 | -s 主机名] [-p 端口] [-v]
```

-adminUser 登录:密码
设置 DvAdmin 帐户的凭据。 如果未给定登录帐户或密码，则使用默认值“DvAdmin”。

-backupUser 登录:密码
设置 DvBackup 帐户的凭据。 如果未给定登录帐户或密码，则使用默认值“DvBackup”。

–h
打印此消息。

-i 证书文件
导入现有证书。

-p 端口设置 SSL 端口。

–s 主机名创建完全限定域名的自签名证书。

–v
打印版本信息并退出。

4 配置 Data Protector for PCs 保护策略

安装 Data Protector for PCs 后进行初始设置

安装 Data Protector for PCs 之后，Policy Server 控制台中会立即显示“初始设置”窗口。在设置 Data Protector for PCs 的策略之前，必须成功完成两个配置步骤：

1. 定义或导入加密密码。

   为安全起见，必须在使用 Data Protector for PCs 之前定义加密密码。 这可以确保所有文件都在用户计算机上进行了加密，并且通过网络上进行加密传输。 使用相同密码对所有用户的文件以及所有集中配置的 Data Vault 中的文件进行加密。

   - 集中定义的 Data Vault（通过 Policy Server 控制台定义）将始终使用基于 Data Protector for PCs 加密密码的加密。
   - 使用本地定义的 Data Vault（由用户通过其计算机定义），用户可以选择是否使用加密，并选择自己的密码。

   首次安装 Data Protector for PCs 时，必须生成或导入密码才能继续操作。 生成密码之后，出于安全考虑，需要导出该密码。 将其保存在安全位置。 以后可使用该文件进行导入。

   单击设置加密策略以管理密码，并按照窗口上的说明操作。

   注意： 生成或导入密码之后，无法对其进行更改。

2. 获取 **Data Protector for PCs** 许可证。

   如果正在评估 Data Protector for PCs，则无需进一步获取许可即可对数量不限的用户提供 60 天保护。 购买 Data Protector for PCs 时，需要访问 https://webware.hp.com/welcome.asp 上的 HP License Key Delivery Service，以便下载随后需要输入的许可证密钥。 可以购买以下许可证：

   - 适用于 100 个代理的 TA032AA 或 TA032AAE
   - 适用于 1000 个代理的 TA033AA 或 TA033AAE
   - 适用于 100 个代理以及 HP Data Protector Starter Pack Windows 的 TA036AA 或 TA036AAE（B6961BA 或 B6961BAE）

   必须在评估期结束之前输入永久许可证密钥。 否则，过了 60 天，代理就再也不能将数据复制到其 Local Repository 或 Data Vault。 但是，仍然可以恢复以前保护的文件版本。

   单击许可证管理以管理许可证，然后单击为 **Data Protector for PCs** 用户输入许可证密钥。 按照窗口上的说明操作。

注意： 安装代理时，会将许可证分发给代理。

成功完成这些配置步骤之后，您可以使用完全运行的 Policy Server 控制台。 如果刚安装了 Data Protector for PCs，请按照下一节中介绍的顺序配置 Data Protector for PCs 的其他元素。

第一次配置

Data Protector for PCs 预配置了一些足以满足大多数组织要求的策略。 建议先配置 Data Vault 策略、复制策略和文件保护策略，然后再将 Data Protector for PCs 代理软件安装到用户的台式机和笔记本上。

注意： 可以修改 Data Protector for PCs 预配置的策略，而不是配置新策略。 在每个阶段仅选择编辑现有策略，而不是创建新策略。

您可以从 Policy Server 控制台中为安装配置保护策略。 可以将集中定义的策略分发到所有的 Data Protector for PCs 代理，并在用户的台式机和便携式计算机上执行。

1. 在安装向导结束时或随时使用以下 URL 从浏览器运行 Data Protector for PCs Policy Server 控制台：

   `http://policyserver/dpnepolicy/`

   其中“`policyserver`”是 Data Protector for PCs Policy Server 的名称。 必须以“管理员”身份登录该服务器。

2. 配置 **Data Vault** 策略。

   Data Vault 策略设置受策略保护的用户文件连续备份的目标（Web Data Vault 或 Windows 文件共享）。 更改文件时，以前版本和编辑的文件可以自动备份到一个或多个目标。 可以向每个用户组分配一个或多个 Data Vault。 例如，可能定义名为 **Sales** 的 Data Vault 策略，并将其分配给用户组 **Dallas.Sales**、**San Francisco.Sales**、**Chicago.Sales** 和 **Atlanta.Sales**。

   - 集中定义的 Data Vault（通过 Policy Server 控制台定义）将始终使用基于 Data Protector for PCs 加密密码的加密。
   - 使用本地定义的 Data Vault（用户通过其代理软件进行定义），用户可以选择是否使用加密，并选择自己的密码。

注意： 所有 **Data Vault** 的要求：

Data Protector for PCs 将为备份到文件服务器的文件设置与原始文件相同的访问权限 (ACL)。 如果用户可以在其计算机上访问原始文件，则意味着用户只能恢复备份的文件。

Windows 文件共享 **Data Vault** 的要求：

如果使用标准 Windows 文件共享 Data Vault，该共享应位于 Windows 文件服务器（无需与 Policy Server 位于同一台计算机）上。 但是，如果仅评估带少量已安装代理的 Data Protector for PCs，则使 Policy Server 和 Data Vault 文件服务器位于同一台计算机上可能会非常有用。

创建 **Data Vault** 策略：

a. 单击左侧导航窗格中的策略 **> Data Vault > Data Vault** 策略。

b. 单击创建新 **Data Vault** 策略。

c. 按照窗口上的说明操作。 根据所选的是基于 WEB 的 Data Vault 还是 Windows 文件共享 Data Vault，该过程将有所不同。

注意： 创建 Data Vault 时，文件夹或共享路径的长度不得超过 66 个字符。

最佳做法：

暂时将“复制策略”设置为“默认”。

对于 **Windows** 文件共享 **Data Vault** 的清理：

- 如果 Data Vault 位于此 Policy Server 上，请保留此计算机名称的默认设置。
- 如果 Data Vault 位于其他 Windows 文件服务器上，则在其上安装 Data Vault Cleanup 软件并将该计算机指定为清理计算机。

3. 配置复制策略。

复制策略对可以同时复制到 Data Vault 的客户端数设置限制。 它还定义初始和计划的 Data Vault 更新以补充连续备份。 可以向每个复制策略分配一个或多个 Data Vault。

复制策略可定义以下内容：

- 可以将文件同时复制到 Data Vault 的代理数。
- 定期更新计划，这些更新将检查在 Data Vault 上是否存在用户所需的所有文件，如果不存在，将复制所有缺少的文件。 此操作可进一步确保所有用户文件都已正确复制到 Data Vault。
- 是否应执行初始更新（或复制）。 需要初始更新，因为在常规的 Data Protector for PCs 操作期间，每次用户更改 Data Protector for PCs 连续保护的文件时，只会将与更改相关的信息复制到 Data Vault。

默认复制策略适用于没有设置显式复制策略的所有 Data Vault。 可以更改默认复制策略的设置，但不能将其删除或重命名。

创建复制策略：

a. 单击左侧导航窗格中的策略。
b. 单击设置复制策略。
c. 单击创建新的复制策略。
d. 按照窗口上的说明操作。

最佳做法：

- 限制： 将时间周期设置为正常工作时间，并且为其他时间设置更低的限制。
- 初始更新： 启用初始更新以确保备份由文件保护策略保护的所有用户文件。
- 每周/每月更新文件： 由于更新应涉及极少的文件副本（如有），所以启用 Data Vault 更新以确保正确备份了所有受策略保护的用户文件。

4. 配置文件保护策略。

文件保护策略允许您指定要保护的文件以及以前版本将保留的时间。 例如，可以为 Word 文档、Excel 电子表格和 PowerPoint 演示文稿定义名为 **Office** 文档的文件保护策略。

可以保护存储在本地磁盘驱动器上的文件。

有两种类型的策略：

- 连续文件保护— 在文件保存到磁盘或从中删除时提供实时保护。 通常，任何可以从菜单选择保存的文件或文档都应使用 Continuous File Protection 策略保护。

  Data Protector for PCs 包含多种示例策略。 在安装之后默认选择三项： **Office Documents**、**Software Development** 和 **Web Documents**。 可以使用这些策略，也可以创建自己的策略。

- 打开文件保护 — 通过定期获取文件的“快照”（通常每小时一次）对文件进行保护。 通常，任何超大型（大于 100 MB）、全天候打开或缺少保存菜单选项的文件都应使用此方法进行保护。 此类型的常见文件包括电子邮件和数据库文件。

  Data Protector for PCs 包含四个示例： **Microsoft Outlook**、**Microsoft Outlook Express**、**Windows Mail** 和 **Thunderbird**。 可以使用这些策略，也可以创建自己的策略。

  注意： Data Protector for PCs 不支持使用 Open File Proection 策略备份 EFS 加密文件，因此不得对 .pst 等文件进行 EFS 加密。

创建文件保护策略：

a. 单击左侧导航窗格中的策略。
b. 单击设置文件保护策略。
c. 单击创建新的 **Continuous File Protection** 策略或创建新的 **Open File Protection** 策略。

d. 按照窗口上的说明操作。

注意： 创建文件保护策略并设置排除或包括规则时，对于 Open File Protection 策略，文件扩展名不得超过 9 个字符；对于 Continuous File Protection 策略，文件扩展名不得超过 29 个字符。

对于 Open File Protection 策略，可以在包括规则中选择不带扩展名的文件。 此操作不适用于 Continuous File Protection 策略。

重要信息： 此时，您已经配置了 Data Protector for PCs 需要的所有基本策略。Data Protector for PCs 预配置了可满足大多数组织要求的其他策略。 建议您立即开始在用户台式机和便携式计算机上安装代理（请参见“安装 Data Protector for PCs 代理”（第 32 页））。 随后，可以返回检查并配置其余的 Data Protector for PCs 策略，例如清理策略、用户控制策略、代理更新策略和报告数据保留策略。

配置其余的策略

1. 配置 **Active Directory** 访问。

   注意： 将 **Active Directory** 组与 **Data Vault** 关联：可以在 Data Vault 策略中将 Data Vault 与 Active Directory 组关联。 关联组的所有成员都将备份到关联 Data Vault。 无法关联单个用户。 而且，如果关联组织单位 (OU)，则仅关联该 OU 中的组。 直接属于 OU 中的任何用户均不与 Data Vault 关联。 Active Directory 组的列表可能错误地包括了安全组以外的组，比如通讯组。 但是，只有安全组将实际与 Data Vault 关联。

   多个用户：如果两个或更多用户共享一台计算机，他们必须属于同一个 Active Directory 组。

   如果要按组或组织单位分配 Data Vault，或者要按组或组织单位进行报告，需要配置 Policy Server 以使其可以访问 Active Directory。

   配置 Active Directory 访问将启用 Data Vault 的组和组织单位的成员选项（请参见“第一次配置”（第 21 页））。

   配置 **Active Directory** 访问：

   a. 单击左侧导航窗格中的配置。

   b. 单击配置 **Active Directory** 访问。

   c. 按照窗口上的说明操作。

2. 配置清理策略。

   用户计算机上的 Data Protector for PCs Local Repository 和 Data Vault Server 上的 Data Vault 需要定期清理，以便删除早于文件保护策略中定义的保留设置的版本。

   配置清理策略：

   a. 单击左侧导航窗格中的策略。

   b. 单击设置清理策略。

c. 按照窗口上的说明操作。

这样一来，Data Vault 就可以支持更多的用户仅在周末（从周五晚上或周六早晨开始）运行清理进程，从而获得最大运行时间：

a. 在 Policy Server 管理控制台中打开“清理策略”页面，然后更改 **Data Vault** 清理计划。

b. 不选择除星期五和星期六以外的所有时间：

- 如果选星期五，则选择深夜时间作为开始时间，例如 10:00 PM。
- 如果选星期六，则选择清晨时间作为开始时间，例如 1:00 AM。

仅在周末执行清理：

- 提供用于从 Data Vault 恢复的文件列表最多在一周后将过时。 用户可以始终手动重新扫描 Data Vault 上的数据，从而获取最新数据的视图。
- 由于仅在周末执行清理，因此备份版本过时后仍会存在最多一周时间。
- 配额管理不是最新的。 如果用户超过其配额，则可能要等到执行了清理后，才能重新获得 Data Vault 上的可用空间。 另一方面，由于空间使用量报告是清理进程的一部分，因此系统可能无法立即确认是否超过配额。

最佳做法：

- **Local Repository** 清理计划： 默认保留 1 小时。
- **Data Vault** 清理计划： 默认设置“每天午夜清理”应能满足大多数安装的要求。有关 Data Vault 容量的详细信息，请参见“大小调整建议”（第 27 页）。
- 可以将 DPNECleanup 配置成按可重复使用且可扩展的方式使用多个线程，以便更好地利用 CPU 和磁盘，从而存储更多的数据。 请参见“配置多线程清理”（第 30 页）。

3. 配置用户控制策略。

用户控制策略决定了用户对分发到其计算机的公司策略有多大控制权。

配置用户控制策略：

a. 单击左侧导航窗格中的策略。

b. 单击设置用户控制策略。

c. 按照窗口上的说明操作。

最佳做法：

为自助服务恢复设置允许用户控制。

4. 配置代理更新策略。

该策略指定所有受 Data Protector for PCs 保护的台式机和便携式计算机将使用的 Data Protector for PCs 代理版本，这些台式机和便携式计算机将自动更新到此版本。

配置代理更新策略：

a. 单击左侧导航窗格中的策略。

b. 单击设置代理更新策略。
c. 按照窗口上的说明操作。

5. 配置报告数据保留。

此策略将针对信息的每种主要类别，设置出于报告目的数据保留时间。

配置报告数据保留：

a. 单击左侧导航窗格中的配置。
b. 单击配置报告数据保留。
c. 按照窗口上的说明操作。

其他配置任务

首次安装 Data Protector for PCs 时通常会执行这些任务。

获取 **Data Protector for PCs** 软件的许可证。

如果正在评估 Data Protector for PCs，则无需进一步获取许可就可以对数量不限的用户提供 60 天的保护。 购买 Data Protector for PCs 时，需要访问 https://webware.hp.com/welcome.asp 上的 HP License Key Delivery Service，以便下载随后需要输入的许可证密钥。

输入许可证密钥：

1. 单击左侧导航窗格中的许可证管理。
2. 单击输入 **HP Data Protector for PCs** 用户许可证密钥。
3. 按照窗口上的说明操作。

如果要输入多个许可证，可以创建一个文本文件，每行包含一个许可证密钥字符串。然后可以使用“导入许可证密钥”字段导入该文件。

注意： 安装代理时，会将许可证分发给代理。

移动许可证

如果需要更改 Policy Server 的 IP 地址以便将服务器移动到另一个系统，或者需要将许可证从一个 Policy Server 移动到另一个 Policy Server，请联系 HP License Key Delivery Service（网址为 https://webware.hp.com/welcome.asp）。

设置、导入和导出加密密码。

为安全起见，必须在使用 Data Protector for PCs 之前定义加密密码。 这可以确保所有文件都在用户计算机上进行了加密，并且通过网络上进行加密传输。 使用相同的密码对所有用户的文件以及所有集中配置的 Data Vault 中的文件进行加密。

- 集中定义的 Data Vault（通过 Policy Server 控制台定义）将始终使用基于 Data Protector for PCs 加密密码的加密。
- 使用本地定义的 Data Vault（由用户通过其计算机定义），用户可以选择是否使用加密，并选择自己的密码。

首次安装 Data Protector for PCs 时，必须生成或导入密码后才能继续操作。 生成密码之后，为了安全起见，请导出该密码。 将其保存在安全位置。 以后可使用该文件进行导入。

注意： 生成或导入密码之后，无法对其进行更改。

管理加密密码：

1. 单击左侧导航窗格中的策略。
2. 单击加密策略。
3. 按照窗口上的说明操作。

确定可以支持的Agent数

很难给出在所有环境中都适用的一般规则，因此这里给出的示例清楚地描述了给定数量有效的上下文。

影响大小调整的因素

Data Protector for PCs 环境的大小调整有点复杂。 影响特定环境可支持的用户数的技术因素包括：

- Data Vault 的处理功率（针对每夜的备份数据整理）
- Data Vault 服务器上的网络和 I/O 带宽
- Data Vault 服务器上的磁盘空间
- Policy Server 上的 SQL 数据库大小
- 网络带宽以及 Policy Server 的处理功率

其中哪个因素可能会导致任意给定的安装中产生瓶颈，取决于所使用的 Data Protector for PCs 的配置设置和模式：

- Data Vault 上的用户数
- 配置的保护策略所涉及的文件数和文件大小
- 受保护文件的更改频率
- 受保护文件类型的保留设置

大小调整建议

Data Vault

使用每日清理计划时，如果平均数据特征值约为如下数字，则具有 14 TB 磁盘空间的 Data Vault 可支持最多 **3,500** 个Agent的用户群：

- 平均受保护文件数： 5000
- 本地磁盘上受保护文件的平均总大小： 10 GB
- Data Vault 上的平均总大小（已压缩）： 4 GB

如果需要保护的平均数据量超过此示例中给出的数字，只需增加 Data Vault 上的磁盘容量就能为数据提供更多空间，但 Data Vault 可能无法再及时完成每夜的备份数据整理。 请考虑下列可能性：

- 仅在周末运行 Data Vault 清理。 有关如何执行此操作的详细信息，请参见“配置其余的策略”（第 24 页）中的步骤 2“配置清理策略”。 在给定相同平均数据特征值的情况下，此操作可以将具有 40 TB 磁盘容量的 Data Vault 可支持的代理数量增加到 10,000。
- 考虑将最终用户数据分布在多个 Data Vault 上。

此类 Data Vault 的硬件规格如下：

Data Vault 类型	每日清理 （最多 **3,500** 个代理）	每周清理 （最多 **10,000** 个代理）
Windows 文件共享	3 GHz 双核，4 GB RAM，14 TB 磁盘空间	3 GHz 双核，4 GB RAM，40 TB 磁盘空间
Web Data Vault	3 GHz 四核，4 GB RAM，14 TB 磁盘空间	3 GHz 四核，4 GB RAM，40 TB 磁盘空间

如果用户的数据量低于平均数，或许能够在 Data Vault 上托管超过此数量的用户。

注意： HP 强烈建议将 Data Vault 的操作系统和备份数据保存在以物理方式隔离的磁盘上，以获得最佳性能。

为获取最佳性能，应定期对 Data Vault 磁盘进行碎片清理。

Policy Server

在 Policy Server 上生成的通信量直接取决于服务器托管的Agent数。 使用 Data Protector for PCs 随附的 MS SQL Server Express 版可以强制将数据库最大容量设为 4 GB，并且最多可以支持 5,000 个代理[1] 。

如果环境中需要支持的Agent数超过 5,000 个，则可以包含其他 Policy Server，也可以用 Microsoft SQL Server 的完整版本取代 MS SQL Express。 这样，Policy Server 就可以轻松地将规模扩大到 50,000 个Agent。如果决定使用 MS SQL Server 的完整版本，请考虑将 Policy Server 的主内存升级到至少 3 GB。

出于性能考虑，Policy Server 应该在不同于 Data Vault Server 的独立服务器上运行。Policy Server 和 Data Vault Server 也可以在同一台服务器上运行，但仅限于评估目的。

必须至少有一个 Policy Server，但 Data Vault 和 Policy Server 的数量不必匹配。

1. 在 Policy Server 上使用“报告数据保留”的默认设置（30 天）。

网络注意事项

注意： Web Data Vault 不受高延迟的影响。 以下内容仅适用于 Windows 文件共享 Data Vault。

通常在 Windows 文件共享 Data Vault 上，如果 Data Protector for PCs Agent和 Data Vault 之间的网络延迟大于 50 毫秒，HP 不建议执行从 Data Protector for PCs Agent到 Data Vault 的初始更新。这通常适用于采用速度较慢的 WAN 连接的家庭办公室或远程办公室。 初始更新会执行，但需要很长时间。

如果环境中包含地处多个站点的办公室，并且有些站点的网络延迟大于 50 毫秒，请考虑在多个站点安装 Data Vault，以便所有办公室都可以至少到达一个 Data Vault，且延迟不超过 50 毫秒。

初始更新完成后，可以从公司网络上的任何位置（甚至从家庭办公室）执行更新。 这些更新的规模通常很小，甚至通过缓慢的网络连接也足以顺利进行。

如果初始更新必须通过高延迟连接执行，则可能要好几天才能完成，但它可以被中断，而不会造成任何损害。 Data Protector for PCs 重新连接到 Data Vault 后，就会立即从停止点继续更新。

提示： 如果您不知道办公室之间属于哪类延迟，可以从一个站点的计算机使用 `ping` 命令 Ping 另一个站点的计算机。 每个成功的 Ping 操作都会报告延迟。

5 配置多线程清理

DPNECleanup 的性能限制了 Data Vault 上的备份用户数据量。 可以将其配置成按可重复使用且可扩展的方式使用多个线程，以便更好地利用 CPU 和磁盘，从而存储更多的数据。

使用多线程 Cleanup 时，计划程序参数“-s”将导致采用默认参数“-e -f -u -p -d 1000”，其中默认包括多线程清理且 Auto-Adjuster 延迟为 1 秒。 如果不希望使用这些默认设置（例如，要禁用多线程执行或对其进行调整），请从计划程序调用中删除参数“-s”，并附加单独的 CLI 参数。

注意：

尽管在某些情况下可能希望禁用多线程 Cleanup，但建议在 Data Vault 上保留“-e -f -u”作为 Cleanup 调用的参数。

从 CLI 使用 DPNECleanup.exe

通过 DPNECleanup.exe 的参数 -p，可使 Cleanup 进行初始化并启动 Parallel Engine，从而使多线程得以执行。 Parallel Engine 提供了七个可选的命令行参数。 DPNECleanup 可执行文件可以检索这些参数，并将它们传送到 Parallel Engine。

如果未设置 -p，DPNECleanup 将以串行模式运行。 在这种模式下，Parallel Engine 完全不可用。

dpnecleanup

-a 关联将处理器关联设置为给定数值，处理器关联反映了线程使用的 CPU 内核的设置位数。

-d 延迟设置 Auto-Adjuster 开始运行之前的延迟时间（毫秒），使 Parallel Engine 有充足时间来启动大量线程和创建某些系统利用率。 默认情况下，使用 -s 参数会导致产生 1000 毫秒（或 1 秒）的延迟。

-m maxCpuUsage
将需要的最大 CPU 利用率（在通过关联定义的所有内核上）设置为 maxCpuUsage%，Auto-Adjuster 将尽量达到该值。maxCpuUsage 应该是 1 至 100 之间的整数。默认值为“0”，表示没有任何限制（CPU 利用率 100%）。

-o
恒定资源，表示已禁用 Auto-Adjuster，并且 Parallel Engine 不会更改并发线程的数量。使用 -r 可调整并发线程的数量。 使用 -o 参数运行时，将忽略 -d、-m 和 -q 参数。

-p
启动多线程 Cleanup。

-q maxQueueLength
设置所需的最大平均磁盘队列长度，Auto-Adjuster 将尽量达到该值。 该值应为浮点数。默认为 2.0。

`-r resourceCount`

将并发资源（线程）数设置为给定数值。 默认情况下与 `-o` 结合使用，系统将使用 2^（CPU 计数）个并发线程运行。 如果 Auto-Adjuster 正在运行，则给定的值将表示线程上并发资源的限制。 此处的默认的最大值为“0”，表示没有任何限制。

`-z [Idle|BelowNormal|Normal|AboveNormal|High|Realtime]`

设置所有线程的处理优先级。 默认值为 `Normal`。

`-s`

服务器清理。 为所有 Data Vault（无论集中定义还是用户定义）设置清理。 随着多线程的运行，执行该命令时，此参数将由参数“`-e -f -u -p -d 1000`”取代。

`-e`

企业清理。 为通过 Policy Server 的策略集中定义的 Data Vault 设置清理。

`-f`

快速清理。 通常，仅在服务器处于空闲状态时才运行代理清理。 通过该选项，可随时启动清理。

`-u`

用户定义的清理。 为通过用户创建的本地策略定义的 Data Vault 设置清理。

6 安装 Data Protector for PCs 代理

注意： 安装代理时，会将许可证分发给代理。

Data Protector for PCs 代理可用两种方式进行安装：

- 分别安装在每个客户端计算机上。 请参见 “在单个客户端计算机上安装 Data Protector for PCs 代理”（第 32 页）。
- 从所有客户端计算机均可访问的文件服务器跨企业部署。 请参见 “跨企业部署 Data Protector for PCs Agent”（第 33 页）。

在单个客户端计算机上安装 Data Protector for PCs 代理

先决条件

Data Protector for PCs 代理软件可以安装到运行 Windows 的用户的台式机和笔记本上。 有关受支持的平台，请参见“支持矩阵”。

必须登录到具有“管理员”权限的帐户。

安装步骤

1. 插入 Data Protector for PCs 安装 CD-ROM。 安装向导应当自动启动。 如果安装向导没有自动启动，请通过双击安装 CD-ROM 的根目录中的 `setup.hta` 手动运行该向导。
2. 单击安装或更新 **Data Protector for PCs** 代理软件。 如果出现“打开或保存”对话框，请选择打开（或运行）。
3. 如果用户计算机没有安装 Microsoft Windows Installer 3.1 或更高版本，则向导会提供机会进行安装。 出现“更新 Windows Installer”对话框时，单击确定进行安装。
4. 如果用户计算机没有安装 Microsoft .NET Framework 2.0 SP1 或更高版本，则向导会提供机会进行安装。 “安装 Microsoft .NET Framework 2.0 SP1”对话框出现时，单击确定进行安装。
5. 向导会自动安装 Data Protector for PCs 代理。 按照屏幕上的说明操作。 在安装期间，系统会要求您输入 Policy Server 的详细信息。
6. 安装和配置完成后，单击完成。 如果在 Policy Server 上设置了 Open File Protection 策略，则会要求您重新启动系统。

   现在应能在系统任务栏上看到 Data Protector for PCs 图标（具体显示哪一种图标取决于保护状态：  ）.
7. 测试 Data Protector for PCs 代理是否正常运行：
   a. 在桌面上选择或创建一个测试文件，如 Word 文档或 Excel 电子表格。 对其做一些更改，并单击保存。

b. 在桌面、Windows 资源管理器或“打开”对话框中右键单击测试文件。 应该可在显示的菜单中看到三个 Data Protector for PCs 条目（搜索和恢复文件...、复制版本和打开包含 **XXX** 的版本...）。

c. 选择打开包含 **XXX** 的版本...，应当看见刚创建或编辑文档的带有时间戳的版本的列表。 如果选择其中一个版本，则它将在合适的应用程序中作为只读文档打开。 这就是用户从本地 Data Protector for PCs 存储库中恢复其文档以前版本的方式。

8. 对希望通过 Data Protector for PCs 保护的其他用户的台式机和便携式计算机重复步骤 1 到步骤 8。

跨企业部署 Data Protector for PCs Agent

可以使用安装 CD-ROM 上包含的“Data Protector for PCs Agent部署工具包”跨企业初始部署 Data Protector for PCs Agent。

注意： 无法在启用 UAC（用户帐户控制）的 Vista PC 上使用部署工具包。 要解决此问题，请禁用 UAC 或以交互方式安装代理。

在下面描述的步骤中，首先将 `CD-ROM:\Agent` 中的“Data Protector for PCs Agent部署工具包”复制到文件服务器上可供所有用户访问的目录下。 然后使用 `SetupConfig.exe` 在该目录中创建参数文件。 最后，建立机制以在各用户计算机的共享目录中运行 `StartInstall.exe`。 例如，可以使用登录脚本。 然后，可以从 Data Protector for PCs Policy Server 控制台使用“Agent部署”报告监视部署情况。

工具包内容

Data Protector for PCs 部署工具包内含以下组件：

`SetupConfig.exe`	创建和编辑初始化文件。
`StartInstall.exe`	以特权用户身份启动 `Setup.exe`。
`Setup.exe`	安装必备软件和 `DataProtectorNE.ini`。
`DataProtectorNE.msi`	用于安装代理软件的 Data Protector for PCs Windows Installer 程序包。
`DataProtectorNE64.msi`	用于在 64 位计算机上安装代理软件的 Data Protector for PCs Windows Installer 程序包。
`DataProtectorNE*.*.mst`	用于安装本地化代理软件的 Data Protector for PCs Windows Installer 程序包。
`WindowsInstaller.exe`	更新 Windows Installer（安装 .NET 时需要）。
`NetFx20SP1_x64.exe`, `NetFx20SP1_x86.exe`	安装 NET Framework 2.0 SP1。
`Setup.ini`	Data Protector for PCs 安装设置参数文件。 此文件将使用 `SetupConfig.exe`（请参见下面的步骤 4）进行创建。

部署和安装过程

1. 将发行 CD-ROM 的 Agent 目录中的文件复制到想要使用“Data Protector for PCs Agent部署工具包”的所有用户均可访问的目录。 此目录可以是常见 netlogon 共享目录，如 `\\yourserver\DPNEDeploy`。
2. 确保新创建的目录包含上面列出的文件。 可以删除所有其他文件。
3. 打开 DOS 命令窗口 (`cmd.exe`) 和 `cd`，并转到步骤 1 中创建的目录。
4. 运行 `SetupConfig.exe` 以创建或编辑参数文件 `Setup.ini`。 第一次运行 `SetupConfig.exe` 时，必须输入所有参数的值。 之后，可以重复运行 `SetupConfig.exe` 以更改参数。 如果不想更改参数，只需按 **Enter**。

   所需参数包括：

   - 指向安装程序包的 **UNC** 路径 – 指向步骤 1 中在其中复制文件的共享目录的完整路径，如 `\\yourserver\DPNEDeploy`。
   - **Data Protector for PCs Policy Server** 的名称。 这可以是 `YOURSERVER` 之类的 NetBIOS 名称，或 `yourserver.yourcompany.com` 之类的完全限定域名。
   - 用户名 – 使用“Data Protector for PCs Agent部署工具包”的计算机上具有管理员权限的用户的用户名，如“域管理员”组的成员。 它通常是完全限定用户名（包括域），如 `YOURCOMPANY\JerryAdmin`。
   - 密码 – 与用户名关联的密码。 必须键入密码两次以进行确认。
5. 在客户端计算机上，运行 `StartInstall.exe`，例如 `\\yourserver\DPNEDeploy\StartInstall`。 然后，将使用在 `Setup.ini` 中指定的用户名和密码以低优先级在后台运行 `Setup.exe`。 这可以作为登录脚本的一部分完成。 请注意，无法在启动脚本中包括它，因为计算机帐户没有足够的网络权限。
6. `Setup.exe` 将确定客户端计算机是否可以支持 Data Protector for PCs。 有关受支持的 Windows 平台，请参见“支持矩阵”。
7. `Setup.exe` 将确定是否安装 .NET Framework V2.0 SP1。 如果未安装，将安装该组件，然后可能需要重新启动计算机。
8. `Setup.exe` 将确定是否已安装 Data Protector for PCs。 如果未安装或者版本已过时，则会安装 Data Protector for PCs。

注意：

在步骤 4–7 中出现的任何错误都会在 Data Protector for PCs Policy Server 上和本地计算机的“应用程序事件日志”中记录消息。

可以使用 Data Protector for PCs Policy Server 控制台检查“Agent部署”的进度：

1. 登录到 Data Protector for PCs Policy Server 控制台。
2. 在左侧导航窗格中报告下，选择**Agent**部署。

   将显示到目前为止的初始部署摘要。 其中显示：

   - 已成功完成部署的计算机数。

- 正在进行部署的计算机数。
- 部署失败的计算机数。

3. 单击计算机数列中的数字以显示处于所选部署状态的计算机的列表。

   显示每台计算机的当前状态。 例如，如果在特定计算机上部署失败，则信息列将给出发生的错误。 通过单击计算机的 NETBIOS 名称，可以获取有关计算机的其他详细信息。

7 更新 Data Protector for PCs

如果要将 Data Protector for PCs 从 6.**x** 版更新到 7.0 版，请按以下顺序操作：

1. 将 Policy Server 更新到 7.0 版。 请参见 “更新 Policy Server”（第 36 页）。
2. 安装 Web Data Vault Server。 请参见“安装、配置和维护 Web Data Vault Server”（第 16 页）的“安装 Web”。
3. 将代理更新到 7.0 版。

   可以使用“手动更新”进行更新，也可以使用“代理更新策略”来“自动”更新。 有关更多详细信息，请参见 “更新代理”（第 36 页）。

更新 Policy Server

通过执行标准安装步骤，可以将已安装的 Data Protector for PCs Policy Server 更新到较新的版本。 所有现有配置（比如 Data Vault 配置、许可等）都将在较新的版本中可用。

更新 **Policy Server**：

1. 插入 Data Protector for PCs 安装 CD-ROM。 如果安装向导没有自动启动，请通过双击安装 CD-ROM 的根目录中的 `setup.hta`，手动运行该向导。
2. 在向导的“安装 Data Protector for PCs”页上单击安装 **Policy Server** 开始更新。
3. 按照屏幕上的说明操作。
4. 安装程序将检测现有 Policy Server 安装并提供更新。
5. 按照屏幕上的说明操作。
6. 安装完成后，单击下一步。 然后，可以选择运行 Data Protector for PCs Policy Server 控制台。

注意： 如果在 Policy Server 上安装了 Cleanup 软件，还需要更新该软件。 可以手动更新，也可以使用“代理更新策略”进行更新。

更新代理

如果更新了 Data Protector for PCs 服务器的版本，则使用 Notebook Extension 先前版本的现有代理仍会像以前一样继续运行。 可以使用“手动更新”进行更新，也可以使用“代理更新策略”来“自动”更新。

注意： 更新完成后，所有代理都必须重新启动后才能使用新的 Web Data Vault。 系统任务栏中的气球消息以及用户计算机上“Data Protector for PCs 运行状态”面板中的“摘要”选项卡将指示执行此操作。

使用代理更新策略的自动代理更新

通过使用 Policy Server 的代理更新策略，可以“自动”更新代理。 安装程序包将自动传递到所有连接的客户端，并且更新将以完全自动的方式完成。 不会中断最终用户的操作。

1. 在 Policy Server 控制台中，选择策略 > 代理更新策略。
2. 如果刚更新了 Policy Server，则安装过程已上载了新的代理更新程序包。 在 Policy Server 控制台中，尚未选择此新版本。

   选择新代理版本以使该版本可用。
3. 通过调整“限制”，可以调整每分钟允许的最大更新数。
4. 单击保存代理更新策略。
5. 现在，代理将自动更新到最新版本。 Cleanup 代理也将自动更新。

注意： 可以使用报告检查代理更新进度：“代理部署”。

手动代理更新

通过执行标准安装过程，可以将现有 Data Protector for PCs 代理更新到较新的版本。

在将代理更新到较新的版本之前，确保代理版本与 Data Protector for PCs Policy Server 的版本兼容。

1. 插入 Data Protector for PCs 安装 CD-ROM。 如果安装向导没有自动启动，请通过双击安装 CD-ROM 的根目录中的 `setup.hta`，手动运行该向导。
2. 在向导的“安装 Data Protector for PCs”页上单击安装代理开始更新。
3. 按照屏幕上的说明操作。
4. 安装程序将检测现有代理安装并提供更新。
5. 按照屏幕上的说明操作。

8 如何获取对 Data Protector for PCs 的支持

Data Protector for PCs 附送一年维护。 这使您可以：

- 获得电话支持，以便与支持技术人员通话。
- 更新 Data Protector for PCs Server 和 Data Protector for PCs Agent软件。 可以从 Data Protector 网站下载最新版本或 CD-ROM 映像。 请访问 http://www.hp.com/go/dataprotector。

词汇表

Active Directory
（**Windows** 特定术语）Windows 网络中的目录服务。 它包含有关网络资源的信息，并使这些资源可供用户和应用程序访问。 目录服务提供一致的方式来命名、描述、查找、访问以及管理资源（不管它们驻留在哪个物理系统上）。

Agent
在每个用户的台式机/便携式计算机上运行的 Data Protector for PCs 软件。 它在 TCP 端口 80 上通过 Web 服务（SOAP 和 XML）与 Policy Server 通信。

Continuous File Protection
Continuous File Protection 是 Data Protector for PCs 的 Continuous Data Protection 方法，此方法会在保存文件时自动存储该文件中的更改。 此方法适用于用户保存的数据文件（而不是数据库或 Outlook 文件之类始终打开的文件）。 每个 Continuous File Protection 策略保护在某方面相关的一组文件。 Data Protector for PCs 为常用的文件类型（如 Office 文档和图片）预配置了策略。 可以编辑这些文件保护策略，也可以创建您自己的策略。 该策略还指定受保护文件的以前版本的保留时间。

Data Vault
有两种类型的 Data Vault：

- Web Data Vault。 这些 Data Vault 使用 HTTPS 协议，可以为客户端计算机与 Data Vault 之间的数据传输提供最高级别的安全性，并能在高延时环境中获得获得更好的吞吐量，因此推荐使用此类型 Data Vault 。
- Windows 文件共享 Data Vault。 它们是文件服务器上的共享文件夹，其中的文件根据 Data Vault 策略进行存储。 文件服务器必须支持 Windows 文件共享协议 (CIFS/SMB)。 它们不能在具有高网络延迟的环境中使用。

这两种类型的 Data Vault 的数据结构相同，因此可以将现有 Windows 文件共享 Data Vault 转换成 Web Data Vault。

可以基于用户的组或组织单位成员身份为用户分配一个或多个 Data Vault 策略。

Local Repository
Local Repository 是Agent计算机上用于存储受保护文件和文件更改的安全存储位置，通常位于系统硬盘驱动器上。 它是隐藏的系统目录。 通过右键单击桌面上、Windows 资源管理器中或“打开”对话框中的文件，用户可以快速恢复以前版本。 受 Continuous File Protection 策略保护的文件在保留期到期之前保存在本地计算机上的隐藏目录中。 受 Open File Protection 策略保护的文件在复制到 Data Vault 之前只是临时存储在本地 Version Store 中。 Local Repository 的路径通常为 `C:\{DPNE}`。

Open File Protection
Open File Protection 通过定期获取文件级快照来备份始终打开的文件，例如 Outlook 个人文件夹和许多数据库文件。 这有时称为“近似”Continuous Data Protection。 Open File Protection 策略定义对打开文件的保护（由包括和排除规则集进行定义）。 例如，可以通过将包含规则指定为“结尾为‘.pst’”，定义应用于 Outlook .pst 文件的名为“Outlook 个人文件夹”的策略。 如果要排除已存档的 .pst 文件，则可以创建作为“包含‘存档’”的排除规则。 策略还指定受保护文件的以前版本的保留时间。 Open File Protection 策略适用于所有用户。

Policy Server
Policy Server 提供对 Data Protector for PCs 策略的集中管理。 它还收集来自Agent的状态信息并提供有关其部署和操作的报告。

备份用户
Web Data Vault Server 上执行最终用户操作（如备份和恢复文件）的用户。

策略
策略是一组规则，在 Policy Server 中集中定义，由每个台式机/便携式计算机/笔记本上的Agent执行。

初始更新
Data Protector for PCs 在用户修改文件时通过保存更改来连续保护文件。 用户创建新的 Data Vault 时，Data Protector for PCs 必须对用户的所有受保护文件进行初始更新以将其保存到该 vault。 用户可以选择如何完成初始更新，是立即完成还是在后台进行。

复制策略

复制策略可定义以下内容：

- 可以同时将文件复制到 Data Vault 的Agent数。
- 定期更新计划，这些更新将检查 Data Vault 上是否存在用户所需的所有文件，如果不存在，将复制所有缺少的文件。 此操作可进一步确保所有用户文件都已正确复制到 Data Vault。
- 是否应执行初始更新。 需要初始更新，因为在常规的 Data Protector for PCs 操作期间，每次用户更改 Data Protector for PCs 连续保护的文件时，只会将更改相关的信息复制到 Data Vault。

如果刚安装了 Data Protector for PCs，则需要设置复制策略以对用户的所有受保护文件进行初始更新。

管理用户

Web Data Vault Server 上负责管理任务（如创建和删除 Data Vault 以及迁移客户端备份数据）的用户。

控制台

基于浏览器的控制台是集中定义 Data Protector for PCs 策略的位置。 您必须是管理员组的成员。

清理策略

文件保护策略设置的保留期通过定期运行的清理任务得到强制实施。 清理策略中定义了清理频率。 默认情况下，用户的 Local Repository 每小时清理一次，所有本地定义的 Data Vault 每天清理一次。 集中定义的 Windows 文件共享 Data Vault 由通过 Data Vault 策略分配的计算机进行清理，Web Data Vault 由 Data Vault Server 上本地运行的 Cleanup 进行清理。 清理策略适用于所有用户。

受保护的文件

受保护的文件是由 Data Protector for PCs 自动备份的文件。 在 Continuous File Protection 和 Open File Protection 策略中定义了受保护的文件类型。

用户控制策略

此策略将确定单个用户对其台式机/便携式计算机/笔记本上运行的Agent软件的控制权。 可以锁定Agent，以便对用户完全隐藏策略，可以允许用户查看策略但不能更改策略，还可以允许其添加自己的策略。 可以单独设置对每个主要 Data Protector for PCs 策略的控制级别。 用户控制策略适用于所有用户。

索引