

IBM Multi-Cloud Data Encryption  
由 SPx<sup>®</sup> 提供技术支持  
V 2.3

常见问题 (FAQ)



## 注意事项

在使用本信息及其支持的产品之前，请阅读第 11 页的『声明』中的信息。

本版本适用于 IBM Multi-Cloud Data Encryption V2.3（产品号 5737-C67）及所有后续发行版和修订版，直到在新版本中另有声明为止。

© Copyright IBM Corporation and others 2017, 2019

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

© **Copyright International Business Machines Corporation .**

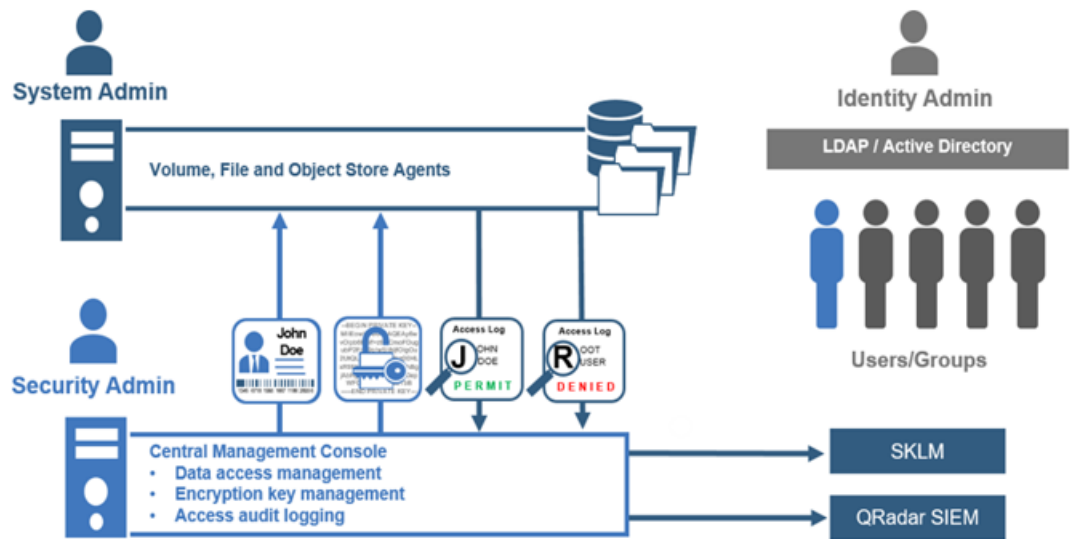
# 目录

第 1 章概述.....	1
第 2 章 MDE - 常见问题 (FAQ).....	3
一般常见问题.....	3
问：什么是 IBM Multi-Cloud Data Encryption (MDE)? .....	3
问：IBM Multi-Cloud Data Encryption (MDE) 支持什么操作系统? .....	3
问：MDE 代理程序支持什么文件系统? .....	3
问：IBM Multi-Cloud Data Encryption (MDE) 需要任何先决条件吗? .....	3
问：IBM Multi-Cloud Data Encryption (MDE) 支持什么浏览器? .....	3
问：IBM Multi-Cloud Data Encryption (MDE) 在 FIPS 方式下运行吗? .....	3
问：如果使用 Multi-Cloud Data Encryption (MDE)，是否需要在向远程系统发送我的数据时将 该数据加密？是否还需要与远程系统的 VPN 连接? .....	4
问：IBM Multi-Cloud Data Encryption (MDE) “向位级数据织入安全性”是什么意思? .....	4
问：请说明如何使用 IBM Multi-Cloud Data Encryption (MDE) 维护数据完整性。 .....	4
策略、供应和管理常见问题.....	4
问：“策略、供应和管理 (PPM)” 有什么用途? .....	4
问：“策略、供应和管理 (PPM)” 为什么使用基于角色的访问控制? .....	4
问：在“策略、供应和管理 (PPM)” 控制台中，什么是进程？它有什么用途? .....	4
问：在“策略、供应和管理 (PPM)” 控制台中，什么是选择器？它有什么用途? .....	4
问：在“策略、供应和管理 (PPM)” 控制台中，什么是路径集？它有什么用途? .....	4
问：在“策略、供应和管理 (PPM)” 控制台中，什么是数据类型？它有什么用途? .....	5
问：在“策略、供应和管理 (PPM)” 控制台中，什么是代理程序？它有什么用途? .....	5
问：“卷”代理程序应该在什么时候使用？它是如何工作的? .....	5
问：“使用策略的文件”代理程序应该在什么时候使用？它是如何工作的? .....	5
问：“使用策略的卷”代理程序应该在什么时候使用？它是如何工作的? .....	5
问：“对象存储”代理程序应该在什么时候使用？它是如何工作的? .....	5
问：在“策略、供应和管理 (PPM)” 控制台中，什么是作业？它有什么用途? .....	5
问：对于 IBM Multi-Cloud Data Encryption，什么时候需要使用外部 PostgreSQL 数据库? .....	6
证书常见问题.....	6
问：PPM 服务器证书有什么要求? .....	6
问：代理程序证书有什么要求? .....	6
问：PPM 支持网络地址转换 (NAT) 或端口地址转换 (PAT) 连接吗? .....	6
问：如何在网络地址转换 (NAT) 或端口地址转换 (PAT) 网络配置中为 PPM 服务器配置 PPM 服 务器证书? .....	6
问：当代理程序位于网络地址转换 (NAT) 或端口地址转换 (PAT) 网络配置中时，如何配置代理 程序证书? .....	6
问：对高可用性 (HA) 配置中的 PPM 服务器证书有什么要求? .....	6
密钥和密钥处理常见问题.....	7
问：IBM Multi-Cloud Data Encryption 可以执行哪些密钥处理操作? .....	7
问：为什么应该轮换密钥? .....	7
问：为什么应该撤销密钥? .....	7
问：为什么应该粉碎密钥? .....	7
问：IBM Multi-Cloud Data Encryption 将为我管理密钥吗? .....	7
安装与设置常见问题.....	7
问：IBM Multi-Cloud Data Encryption (MDE) 如何影响最终用户（即，非管理用户）? .....	7
问：MDE 代理程序是否可以安装在 Docker 主机上，并处理来自 Docker 容器中应用程序的所有 读取/写入请求? .....	7
配置常见问题.....	7
问：能否使用 IBM Multi-Cloud Data Encryption (MDE) 加密 HTML 文件? .....	7
操作常见问题.....	8

问：如何知道通过 IBM Multi-Cloud Data Encryption (MDE) 保护我的数据？ .....	8
问：在更改 IBM Multi-Cloud Data Encryption (MDE) 生产实现前应采取什么预防措施？ .....	8
问：能否将事件从 IBM Multi-Cloud Data Encryption (MDE) 转发到其他 SIEM（安全信息和事件管理）相关应用程序？ .....	8
问：区分大小写（大写）重要吗？ .....	8
问：什么是运输次序，它为什么很重要？ .....	8
问：我已提交快照激活作业，它仍在运行。将在什么时候完成？ .....	8
高可用性常见问题 .....	8
问：IBM Multi-Cloud Data Encryption (MDE) 部署什么时候需要高可用性？ .....	8
问：高可用性 (HA) IBM Multi-Cloud Data Encryption 部署需要负载均衡器吗？ .....	8
多租户常见问题 .....	9
问：多租户功能部件有什么用途？ .....	9
<b>声明 .....</b>	<b>11</b>
商标 .....	12
产品文档的条款和条件 .....	13
隐私策略注意事项 .....	13

# 第 1 章 概述

IBM Multi-Cloud Data Encryption (MDE) 是由 SPx® 技术支持的综合数据安全性产品，它将静态数据加密（通过代理程序）与充当中央管理控制台的策略供应管理器 (PPM) 的其他强大保护功能相结合。MDE 支持从一个中央位置进行代理程序供应、数据访问策略设置（操作访问定义和加密访问定义），以及多达 25,000 个代理程序的管理（密钥生命周期、代理程序更新和用户访问记录）。MDE 提供的无缝安全系统，可以灵活分配使用唯一加密拆分技术在文件系统级别或卷级别加密数据的代理程序。其提供超越标准加密的以数据为中心的保护，使数据加密更强健、更能抵御暴力攻击。它还提供更进一步的保护：通过定义详细的访问策略，在用户级别限制、监视和审计数据访问。



MDE 针对以下不同的管理员角色提供了职责分离：“产品管理员”和“安全管理员”。向“产品管理员”角色委派了配置和维护 MDE 产品所需的许可权。向“安全管理员”角色委派了供应和管理代理程序所需的许可权。图 1 描述了这些角色，“第 7 部分：MDE 管理用户管理”中将进一步讨论。

这四种代理程序类型适用于实施受保护或加密数据的策略定义的部署。“卷”代理程序实施卷策略定义以及一个或多个受保护卷的关联。“使用策略的文件”代理程序实施基于文件的操作访问策略定义以及一个或多个受保护文件路径的关联，其中每个受保护文件路径可具有其自己的操作和访问控制策略（通过详细的策略规范进行定义）。“使用策略的卷”代理程序利用卷代理程序的卷策略保护并且允许对一个或多个受保护文件路径应用和实施基于文件的操作访问控制策略。此外，“对象存储”代理程序可对发送到一个或多个基于云的对象存储器的数据进行加密和以加密方式分割数据。



---

## 第 2 章 MDE - 常见问题 (FAQ)

---

### 一般常见问题

---

#### 问：什么是 IBM Multi-Cloud Data Encryption (MDE)?

答：MDE 引入并启用代理程序供应、策略（操作访问和加密访问定义）以及从一个中心位置对多达 25,000 个代理程序的管理（生命周期更新和用户审计）。MDE 支持以下四种代理程序类型的部署：“卷”、“使用策略的文件”、“使用策略的卷”和“对象存储”。这些代理程序对最终用户来说安装简单并且无缝，并使管理员能够配置和部署软件以满足 IT 环境合规性需求。

#### 问：IBM Multi-Cloud Data Encryption (MDE) 支持什么操作系统？

答：MDE 当前支持以下操作系统：

- Red Hat® Enterprise Linux 6.2 kernel V2.6.32-220 和后续发行版
- Red Hat® Enterprise Linux 7.2+ kernel 版本
- CentOS 6.2 kernel V2.6.32-220 和后续发行版
- CentOS 7.2 kernel 版本和后续发行版
- Microsoft Windows Server® 2008R2
- Microsoft Windows Server® 2012
- Microsoft Windows Server® 2012R2
- Microsoft Windows Server® 2016

#### 问：MDE 代理程序支持什么文件系统？

答：MDE 支持以下文件系统：

- EXT3
- EXT4
- XFS（Red Hat®/CentOS 6.5 和更新版本）
- NTFS
- ReFS

#### 问：IBM Multi-Cloud Data Encryption (MDE) 需要任何先决条件吗？

答：MDE 作为 OVA 进行交付，因为在 VMware ESXi™ 或 Microsoft Hyper-V 上可很方便地部署并且可在大多数其他系统管理程序中运行。

#### 问：IBM Multi-Cloud Data Encryption (MDE) 支持什么浏览器？

答：可以使用 Mozilla Firefox、Google Chrome™、Microsoft Internet Explorer 和 Microsoft Edge 运行 MDE。

#### 问：IBM Multi-Cloud Data Encryption (MDE) 在 FIPS 方式下运行吗？

答：是，MDE 遵循 FIPS 140.2 合规标准，如产品数据表中所指定的那样。

**问：如果使用 Multi-Cloud Data Encryption (MDE)，是否需要在向远程系统发送我的数据时将该数据加密？是否还需要与远程系统的 VPN 连接？**

答：在可以访问文件位置的情况下，MDE 设计用于向远程站点（包括公共云站点）安全写入数据。但是，可能需要 VPN 才能连接到远程站点。

**问：IBM Multi-Cloud Data Encryption (MDE) “向位级数据织入安全性”是什么意思？**

答：由 SPx 技术支持的 MDE 将加密、在位级别分割的随机加密数据、认证（完整性检查）、容错和 COI 框架组成一个过程，以将可标识的数据和信息转换为纯随机且不可用的二进制元素。MDE 操作的结果是向数据结构中织入信息保障 (IA) 元素。安全性、数据弹性、信任和信息共享框架中都加入了数据并且依附于数据，因而使其不可分离。从数据创建开始到数据损毁和/或公开发布生命周期结束，数据和信息保护将得到保证。当数据进入静止状态（写入存储器）且被访问时，将继续进行保护。

**问：请说明如何使用 IBM Multi-Cloud Data Encryption (MDE) 维护数据完整性。**

答：使用必须与待读取数据匹配的消息认证代码来保证数据完整性。

## 策略、供应和管理常见问题

---

**问：“策略、供应和管理 (PPM)” 有什么用途？**

答：PPM 管理代理程序供应（数据保护模型）、策略（操作访问和加密访问定义）以及从一个中心位置对多达 25,000 个代理程序的管理（生命周期更新和用户审计）。它支持以下四种数据加密代理程序类型的部署：“卷”、“使用策略的文件”、“使用策略的卷”和“对象存储”。“卷”在块设备级别保护数据。“使用策略的文件”在文件级别保护数据，并提供基于文件的操作访问控制。“使用策略的卷”在块设备级别保护数据，并且还保护基于文件的操作访问控制。“对象存储”代理程序可对发送到一个或多个基于云的对象存储器的数据进行加密和以加密方式分割数据。

**问：“策略、供应和管理 (PPM)” 为什么使用基于角色的访问控制？**

答：PPM 利用平面静态的基于角色的访问控制 (RBAC) 设计。PPM 中的功能需要特定许可权。有以下两个不同角色：产品管理员和安全性管理员。虽然有一些许可权是共同的，角色分离为 IT 领导层提供了强大管理职责分离，以避免表现差的员工破坏 IT 环境。可添加其他每种类型的角色以适当支持更大或更复杂的 IT 环境。此外，客户还可以通过编程方式定义核准作业所需的管理人员数量，以及拒绝作业所需的管理人员数量。因此，对于每组角色，PPM 跟踪管理员核准数和拒绝数以确保有足够数量的管理员核准执行或拒绝。如果必需数量的管理员核准了该作业，那么该作业将执行。如果必需数量的管理员拒绝了该作业（可以不同于核准），那么将取消该作业。这将确保准确控制管理任务和安全性相关任务。核准和/或拒绝的顺序将被跟踪和记录以用于审计与合规性检查。

**问：在“策略、供应和管理 (PPM)” 控制台中，什么是进程？它有什么用途？**

答：进程也称为“通过策略的进程”，是一个进程或应用程序列表，为其分配了对 IBM Multi-Cloud Data Encryption 保护的数据的访问控制。进程与选择器绑定，以通过目标系统上的用户提供进程的访问控制。

**问：在“策略、供应和管理 (PPM)” 控制台中，什么是选择器？它有什么用途？**

答：选择器是用户、组和进程的无序列表。组合成一种数据类型，它为安全性管理员提供了一种简单方法，来识别将共享 MDE 保护数据或对该数据具有公共访问权的实体集合。选择器可包括可选用户、可选“组”字段以及组来源（内部或外部，如果已定义 LDAP），或一组可选的“通过策略的进程”。

**问：在“策略、供应和管理 (PPM)” 控制台中，什么是路径集？它有什么用途？**

答：路径集是受 MDE 策略保护的文件路径的无序列表（也可能从策略保护中排除，这取决于策略）。它为安全性管理员提供了一种简单方法，来列出受 MDE 保护的文件路径的集合。指定路径集时，安全性管理员必须为路径集合创建名称。保护是从提供的路径通过任何子目录递归的。Notes 字段是可选的。



**问：在“策略、供应和管理 (PPM)”控制台中，什么是数据类型？它有什么用途？**

答：数据类型是分配给指定数据类型的访问定义行的有序列表。每一行都包含选择器，以及 I/O 操作、操作定义和相关密钥。在创建代理程序时，数据类型与文件路径（或路径集）关联，以定义数据的操作访问控制和加密访问控制。

**问：在“策略、供应和管理 (PPM)”控制台中，什么是代理程序？它有什么用途？**

答：PPM 支持四种代理程序类型，每种提供不同类型的保护。这些代理程序类型为“卷”、“使用策略的文件”、“使用策略的卷”和“对象存储”。“卷”在卷级别保护数据。“使用策略的文件”在文件级别保护数据，并提供基于文件的操作访问控制以及可选的加密访问控制。“使用策略的卷”在卷级别保护数据，并提供基于文件的操作访问控制。“对象存储”代理程序可对发送到一个或多个基于云的对象存储器的数据进行加密和以加密方式分割数据。

**问：“卷”代理程序应该在什么时候使用？它是如何工作的？**

答：“卷”代理程序以受保护的预定义卷形式为 IT 提供了静态数据安全性。在部署时，卷代理程序将创建一组将应用于整个卷的密钥，因此将其作为单个单元以加密形式进行保护。因为已存储和/或编辑、添加或删除数据和文件，所以需要使用密码算法以确保卷中的所有数据得到适当保护。卷可能会分为一个或多个分区，每个分区都会得到同样的保护。卷保护最适合计划公开共享中到大型数据的用户组。

**问：“使用策略的文件”代理程序应该在什么时候使用？它是如何工作的？**

答：“使用策略的文件”代理程序为 IT 提供了非常强大的单独文件级保护。因为已部署文件代理程序，顶级目录将被标识为受保护数据的位置。存储在其中的每个文件将使用一组密钥单独保护，而用户、组和进程对文件的访问控制则通过 PPM 定义的策略来管理。此外，安全性管理员可定义能够应用于用户、组或进程的加密密钥，这样所选文件将以加密形式保护起来，共享目录访问权的其他人员则无法访问。由于访问了文件，可能会选择允许记录每个访问权（读和/或写）的选项以用于审计和跟踪。文件大小或具有文件保护的存储环境大小没有限制。“使用策略的文件保护”最适合保护共享或专用的各个文件。

**问：“使用策略的卷”代理程序应该在什么时候使用？它是如何工作的？**

答：“使用策略的卷”代理程序添加用户和组对受保护卷（或分区）的文件访问控制。在部署时，卷代理程序将创建一组将应用于整个卷的密钥，因此将其作为单个单元以加密形式进行保护。因为已存储和/或编辑、添加或删除文件，所以使用密码算法以确保卷中的所有数据得到适当保护。安全性管理员可以使用 PPM 为用户、组和进程定义文件访问控制策略。由于访问了文件，可能会选择允许记录每个访问权（读和/或写）的选项以用于审计和跟踪。“使用策略的卷保护”最适合除共享中到大型数据以外还需要文件访问控制的用户组。

**问：“对象存储”代理程序应该在什么时候使用？它是如何工作的？**

答：“对象存储”代理程序提供机会，将数据存储在高可伸缩、高效的对象存储器中（无论在本地还是在云端）。数据是客户控制的，并且始终专用和可用。对象存储所有者控制访问权。使用传输层安全性 (TLS) 协议对通过“对象存储”代理程序发送的数据进行本地加密和进一步保护传输中的数据。它通过支持 S3 云存储确保本地数据是安全的。“对象存储”代理程序在“M/N”模型上运行，它决定了在已创建的数据片总数 (N) 中重新构建数据 (M) 所需的数据片数。可以根据许可证存储在本地或远程位置的数据片称为“共享”。使用多个共享允许改善的数据流和针对数据弹性和故障容错增加的选项。支持的 M/N 分布式共享模式为 1:1、2:3 或 2:4。

**问：在“策略、供应和管理 (PPM)”控制台中，什么是作业？它有什么用途？**

答：PPM 包含可从 GUI 访问的作业系统，用于管理和跟踪各种部署、策略和维护任务的核准、计时和执行（与受保护数据以及对其具有访问权的人员/设备有关）。当管理员输入任务时，将创建作业，且新作业将添加到作业页面上显示的列表中。具有权限的管理员将可以选择核准、拒绝或放弃各个作业。

## 问：对于 IBM Multi-Cloud Data Encryption，什么时候需要使用外部 PostgreSQL 数据库？

答：强烈建议将外部 Postgres 数据库用于所有生产环境。只建议将内部数据库用于非常小的（很少的代理程序、很少的用户和组，或者只用于测试或 QA 设置）并且不太可能增大的安装。此外，在高可用性 (HA) 配置中部署 MDE 时，还需要 Postgres 数据库。

## 证书常见问题

---

### 问：PPM 服务器证书有什么要求？

答：PPM 服务器证书必须包含以下元素：

- 指定“服务器认证”的扩展密钥属性
- 指定 PPM 服务器标准域名 (FQDN) 的“主题备用名称”部分

### 问：代理程序证书有什么要求？

答：每个代理程序证书都必须包含以下元素：

- 指定“客户机认证”的扩展密钥属性
- 指定代理程序标准域名 (FQDN) 的“主题备用名称”部分

### 问：PPM 支持网络地址转换 (NAT) 或端口地址转换 (PAT) 连接吗？

答：是的。必须能够从代理程序访问 PPM 服务器才能建立通信，因为代理程序启动与 PPM 服务器的通信会话。建立通信后，它将保持打开。代理程序将使用此连接向 PPM 服务器发送事件数据。PPM 服务器将使用此连接向代理程序发送策略更新。

### 问：如何在网络地址转换 (NAT) 或端口地址转换 (PAT) 网络配置中为 PPM 服务器配置 PPM 服务器证书？

答：PPM 服务器证书必须包含以下元素：

- 指定“服务器认证”的扩展密钥属性
- 指定 PPM 服务器标准域名 (FQDN) 的“主题备用名称”部分
- 指定向外排面 IP 地址的“主题备用名称”部分

### 问：当代理程序位于网络地址转换 (NAT) 或端口地址转换 (PAT) 网络配置中时，如何配置代理程序证书？

答：代理程序证书必须包含以下元素：

- 指定“客户机认证”的扩展密钥属性
- 指定 PPM 服务器标准域名 (FQDN) 的“主题备用名称”部分
- 指定向外排面 IP 地址的“主题备用名称”部分

### 问：对高可用性 (HA) 配置中的 PPM 服务器证书有什么要求？

答：PPM 服务器证书必须包含以下元素：

- 指定“服务器认证”的扩展密钥属性
- 指定 PPM 服务器标准域名 (FQDN) 的“主题备用名称”部分，该部分组成了 PPM 集群和与 PPM 虚拟 IP 地址关联的 FQDN。

## 密钥和密钥处理常见问题

---

### 问：IBM Multi-Cloud Data Encryption 可以执行哪些密钥处理操作？

答：安全性管理员可以定义加密密钥以保护策略供应管理器 (PPM) 中的数据。这些密钥可以与数据类型、数据类型行和卷相关联。密钥处理操作包括创建、轮换、撤销和粉碎/清除。

### 问：为什么应该轮换密钥？

答：通常需要定期轮换密钥以确保充分保护数据以防止未经授权的访问。密钥轮换是将当前密钥替换为崭新的密钥，由于加密的性质，需要使用密码算法进行计算。许多专家建议企业 IT 商店（特别是具有云交互功能的商店）定期轮换密钥。目前已制定出需要定期轮换的标准，如 PCI-DSS。PPM 密钥轮换创建具有时间戳记的数据记录，它被记录下来用于审计以证明是否合规。

### 问：为什么应该撤销密钥？

答：使用策略供应管理器 (PPM) 撤销密钥将暂时禁用对受保护数据的访问。密钥通常是在数据保护遇到问题或在必须拒绝访问受保护数据的情况下撤销。稍后，如果将重新分发相同的密钥，数据可能会再次变为可访问。

### 问：为什么应该粉碎密钥？

答：粉碎密钥将永远禁用对受保护数据的访问。请不要选择此选项，除非不再需要此数据。

### 问：IBM Multi-Cloud Data Encryption 将为我管理密钥吗？

答：如果安全性管理员不希望手动管理加密密钥，策略供应管理器 (PPM) 可为每个新建的策略自动生成密钥。自动生成的密钥在创建时始终唯一并且在密钥管理页面上不可视。

## 安装与设置常见问题

---

### 问：IBM Multi-Cloud Data Encryption (MDE) 如何影响最终用户（即，非管理用户）？

答：非管理用户将享受到 IBM Multi-Cloud Data Encryption (MDE) 的安全性和高可用性，且不会察觉到与常规操作有任何差异。访问受管（受保护）目录中的文件不会影响其访问、写入或存储文件。

### 问：MDE 代理程序是否可以安装在 Docker 主机上，并处理来自 Docker 容器中应用程序的所有读取/写入请求？

答：是，“使用策略的文件”代理程序和“卷”代理程序都可用于保护数据。

- “使用策略的文件”代理程序可用于保护 Docker 卷路径，确保了该容器使用的应用程序数据是受保护的。
- “卷”代理程序可用于保护 Docker 容器路径。它可有效地对整个容器及其所有 I/O 进行加密。如果 Docker 卷存储在 Docker 容器路径外部，那么可以配置其他卷以保护外部 Docker 卷。
- 对于 Docker 主机来说，关键点是它必须在 Red Hat 7.2+ (3.10-\*) 上运行受支持的内核

## 配置常见问题

---

### 问：能否使用 IBM Multi-Cloud Data Encryption (MDE) 加密 HTML 文件？

答：此时，建议不要保护 HTML 文件。Web 站点上活动的 HTML 文件在加密时可能显示不正确。

## 操作常见问题

---

### 问：如何知道通过 IBM Multi-Cloud Data Encryption (MDE) 保护我的数据？

答：即使服务已停止并且访问了任何受保护的文件，MDE 保护也处于活动状态。

### 问：在更改 IBM Multi-Cloud Data Encryption (MDE) 生产实现前应采取什么预防措施？

答：当系统正在运行时，只能通过 ‘spxconfig’ 命令行或 GUI 做出较小修改。而重大更改则需要仔细准备并执行建议的备份。（请参阅生产生态系统的所有产品文档，然后再实施更改。）

### 问：能否将事件从 IBM Multi-Cloud Data Encryption (MDE) 转发到其他 SIEM（安全信息和事件管理）相关应用程序？

答：是的。它包含事件聚集和转发系统。此系统聚集受管代理程序中的事件以及内部生成的事件，并将其存储在内部事件日志中，该日志可从管理员仪表板查看并且可配置为向一个或多个收件人转发事件。

### 问：区分大小写（大写）重要吗？

答：是的，区分大小写非常重要。

- 创建选择器时，“用户”字段和“组”字段区分大小写
- 使用 Windows 创建路径集时，盘符必须大写，目录名称必须区分大小写
- 创建“卷”或“使用策略的卷”代理程序时，卷标区分大小写
- 应该始终假定值或字段是区分大小写的

### 问：什么是运输次序，它为什么很重要？

答：它很重要是因为创建和部署代理程序必须按特定顺序执行才能确保成功。

- 在部署“文件”代理程序前，目标卷必须联机、初始化、格式化并且创建了目录，具有相应许可权。
- 在部署“卷”代理程序前，该卷必须存在，联机并且初始化，但是未格式化。
- 在部署“使用策略的卷”代理程序前，该卷必须存在，联机并且初始化，但是未格式化。已定义的选择器必须存在于目标机器的本地或 LDAP/AD 层次结构中。

### 问：我已提交快照激活作业，它仍在运行。将在什么时候完成？

答：在代理程序能与 PPM 服务器通信前，任何快照更改或更新都不会生效。创建的作业将保持运行，直到 PPM 与代理程序之间成功通信或从 PPM 服务器中除去该代理程序。

## 高可用性常见问题

---

### 问：IBM Multi-Cloud Data Encryption (MDE) 部署什么时候需要高可用性？

答：高可用性 (HA) MDE 部署应该用于要求数据访问和保护管理服务达到 100% 可用的 IT 环境。如果 PPM 实例需要维护、发生故障或意外脱机，那么热备份实例将立即参与和恢复操作。

### 问：高可用性 (HA) IBM Multi-Cloud Data Encryption 部署需要负载均衡器吗？

答：是的。代理程序和 PPM 服务器之间需要设置两个负载均衡器（负载均衡器集群）。部署了两个或多个 PPM 服务器的每个位置中需要负载均衡器集群。负载均衡器在本地子网上相互通信并提供代理程序和管理员用于访问 PPM 服务器的虚拟 IP 地址（亦称“浮动 IP 地址”）。PPM HA 有许多场景：单个位置、多个数据中心等，每个都有其自己的部署选项和配置。

### 问：多租户功能部件有什么用途？

答：PPM 的多租户功能使 IT 提供者能够划分客户对 PPM 的控制。因此，在 IT 环境中每个客户将拥有其自己的单独的 PPM 登录、管理员、策略、仪表板、作业、事件等。客户可以共享存储器，甚至目录，但是其受保护的文件和卷将单独加密保护，不能相互访问。这样就使多个租户或客户能够安全地共享和利用同一存储空间；而每个租户的数据又是独立的，不会被其他租户或客户看到。



# 声明

---

本信息是为在美国国内供应的产品和服务而编写的。可从 IBM 处获取此材料的其他语言版本。但是，您可能需要拥有使用该语言的产品或产品版本的副本，才能进行访问。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您所在区域当前可获得的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。您可以用书面形式将许可查询寄往：

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

## **本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区：**

INTERNATIONAL BUSINESS MACHINES CORPORATION “按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某特定用途的保证。

某些管辖区域在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息可能包含技术方面不够准确的地方或印刷错误。本信息将定期更改；这些更改将编入本信息的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对任何非 IBM Web 站点的引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系：

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本文档中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。



此处包含的任何性能数据都是在可控环境下取得的。因此，其他操作环境中获得的结果可能存在很大差异。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的。实际结果可能会有差异。本文档的用户应该在其特定环境中验证适用的数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 尚未测试这些产品，无法确认性能、兼容性或其他任何与非 IBM 产品相关声明的准确性。对于非 IBM 产品的性能问题必须和这些产品的供应商一起解决。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可与此不同。

本信息仅用于规划的目的。在所描述的产品上市之前，此处的信息会有更改。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名称都是虚构的，与实际商业企业所用的名称和地址的任何雷同纯属巧合。

版权许可证：

本信息包含源语言形式的样本应用程序，用以阐明在不同操作平台上的编程技术。如果是为按照在编写样本程序的操作平台上的应用程序编程接口 (API) 进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例尚未在所有条件下经过全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。这些实例程序“按现状”提供，不附有任何种类的保证。对于因使用样本程序所引起的任何损害，IBM 概不负责。

凡这些实例程序的每份拷贝或其任何部分或任何衍生产品，都必须包括如下版权声明：

©（贵公司的名称）（年）。此部分代码是根据 IBM 公司的样本程序衍生出来的。© Copyright IBM Corp.（输入年份）。

如果您正在以软拷贝形式查看本信息，图片和彩色图例可能无法显示。

## 商标

SPx 和 Security First Corp 是 Security First Corp. 在全球许多管辖区域的商标或注册商标。其他产品和服务可能是 Security First Corp. 或其他公司的商标。

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp. 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。当前的 IBM 商标列表，可从 Web 站点上的“版权和商标信息”部分获取：<http://www.ibm.com/legal/copytrade.shtml>。

Adobe、Adobe 徽标、PostScript 以及 PostScript 徽标是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

Apache Software Foundation (ASF) 拥有代表 Apache 项目社区的所有与 Apache 有关的商标、服务标记和图形徽标，所有 Apache 项目的名称都是 ASF 的商标。

Node.JS 是 Joyent, Inc. 的注册商标。CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIA 94104。

Unicode 和 Unicode 徽标是 Unicode, Inc. 在美国和其他国家或地区的注册商标。

CentOS Marks 是 Red Hat, Inc.（“Red Hat”）的商标。

“Red Hat”、Red Hat Linux、Red Hat “Shadowman” 徽标和所列产品是 Red Hat, Inc. 在美国和其他国家或地区的商标或注册商标。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

Microsoft、Windows、Windows NT 以及 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。



## 产品文档的条款和条件

---

根据下列条款和条件授予出版物使用权。

### 适用性

这些条款和条件是对 IBM Web 站点的任何使用条款的补充。

### 个人使用

您可以为了个人使用而非商业性使用复制这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得分发、显示这些出版物或其中部分出版物，也不得制作其演绎作品。

### 商业性使用

您仅可在贵公司内部复制、分发和显示这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得制作这些出版物的演绎作品，也不得在贵公司外部复制、分发或显示这些出版物或其部分出版物。

### 权利

除非本许可权中明确授予，否则不得授予对这些出版物或其中包含的任何信息、数据、软件或其他知识产权的任何许可权、许可证或权利，无论明示的还是暗含的。

只要 IBM 认为这些出版物的使用会损害其利益或者 IBM 判定未正确遵守上述指示信息，IBM 将有权撤销本文授予的许可权。

只有您完全遵循所有适用的法律和法规，包括所有的美国出口法律和法规，您才可以下载、出口或再出口该信息

IBM 对这些出版物的内容不作任何保证。这些出版物“按现状”提供，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关适销和适用于某种特定用途的保证。

## 隐私策略注意事项

---

IBM 软件产品（包括软件即服务解决方案，以下统称“软件产品”）可能会使用 cookie 或其他技术来收集产品使用信息，以便帮助改善最终用户体验，定制与最终用户的交互或者满足其他用途。在许多情况下，软件产品不会收集任何个人可标识信息。一些软件产品可帮助您收集个人可标识信息。如果此软件产品使用 cookie 来收集个人可标识信息，那么有关此产品使用 cookie 的具体信息如下所述。此软件产品不使用 cookie 或其他技术来收集个人可标识信息。

如果针对此软件产品部署的配置使您作为客户能够通过 cookie 和其他技术收集最终用户的个人可标识信息，那么您应该咨询自己的法律顾问，以获取有关此类数据收集的任何适用法律（包括对于通知和许可的任何要求）的建议。

有关使用各种技术（包括 cookie）来实现这些目的的更多信息，请参阅 IBM 隐私策略 (<http://www.ibm.com/privacy>) 和 IBM 在线隐私声明 (<http://www.ibm.com/privacy/details>) 中标题为“Cookie、Web Beacon 和其他技术”的部分以及“IBM Software Products and Software-as-a-Service Privacy Statement” (<http://www.ibm.com/software/info/product-privacy>)。







部件号 CC0LSEN

GC43-5026-00



(1P) P/N: CC0LSEN

