

IBM Multi-Cloud Data Encryption
由 SPx[®] 提供技术支持
V 2.3

管理员指南



注意事项

在使用本信息及其支持的产品之前，请阅读第 101 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 2017, 2019.**

目录

第 1 章简介.....	1
授权使用许可权.....	1
联系点.....	1
《管理员指南》的背景和目的.....	1
第 2 章一般概述.....	3
产品概述.....	3
代理程序类型.....	4
卷代理程序 (Volume Agent).....	4
“具有策略的文件” 代理程序.....	4
“具有策略的卷” 代理程序 (Volume with Policy Agent).....	5
“对象存储” 代理程序.....	5
代理程序功能部件矩阵.....	5
第 3 章规划注意事项.....	7
先决条件.....	7
最低系统需求.....	7
证书要求.....	8
代理程序的文件系统支持.....	8
网络设置.....	9
网络端口.....	9
OVA 配置.....	9
REST 界面.....	9
第 4 章产品安装.....	11
为安装做准备.....	11
许可.....	11
MDE OVA/VM 管理.....	11
安装 MDE.....	11
语言设置.....	12
数据库设置.....	12
内部数据库.....	13
外部数据库.....	13
服务器证书设置.....	13
密钥库、信任库和认证中心.....	13
公共密钥基础结构 (PKI) 设置.....	14
启动和首次登录.....	14
第 5 章 MDE 图形用户界面 (GUI).....	17
基本产品导航.....	17
产品仪表板.....	17
文本框自动补全.....	17
注意通知.....	17
高级属性.....	18
GUI 语言设置.....	18
第 6 章作业.....	21
作业描述.....	21
多管理员核准.....	22
作业核准.....	22

作业拒绝.....	22
作业放弃.....	22
作业信息.....	22
第 7 章 MDE 管理用户管理.....	25
管理用户角色.....	25
“产品管理员”角色.....	25
“安全性管理员”角色.....	25
管理用户管理.....	25
添加新的管理用户.....	25
编辑管理用户密码.....	25
编辑管理用户角色.....	26
编辑管理用户状态.....	26
除去管理用户.....	26
用户帐户锁定.....	27
LDAP 目录列表.....	27
用户源.....	28
第 8 章 事件.....	29
事件日志.....	29
事件详细信息.....	30
事件导出.....	30
事件转发.....	30
事件自变量.....	30
代理程序事件.....	31
可靠的事件.....	31
第 9 章 策略实施密钥管理.....	33
添加密钥.....	33
编辑密钥.....	33
密钥轮换.....	33
密钥撤销.....	35
密钥粉碎.....	35
自动生成的密钥.....	35
外部密钥库.....	35
KMIP 密钥库.....	36
硬件安全模块 (HSM).....	37
第 10 章 文件级策略定义.....	39
选择器.....	39
路径集.....	40
数据类型.....	40
数据类型行.....	40
数据类型行变量.....	41
流程.....	41
第 11 章 代理程序供应和管理.....	43
添加代理程序.....	43
身份.....	43
网络.....	44
“具有策略的文件”、“具有策略的卷”和“卷”代理程序创建.....	44
卷.....	46
“对象存储”代理程序创建.....	47
授权用户.....	50
代理程序工具.....	51
复审与构建.....	51
代理程序激活.....	52

查看代理程序.....	52
代理程序报告.....	52
安装代理程序.....	53
安装适用于 Linux 的代理程序.....	53
安装适用于 AIX 的代理程序.....	55
安装适用于 Windows 的代理程序.....	55
活动策略.....	57
编辑代理程序.....	57
编辑代理程序信息.....	57
添加/删除证书.....	58
代理程序工具.....	59
SU 数据访问.....	59
策略暂挂.....	60
策略更改.....	60
代理程序快照.....	64
保存代理程序编辑和快照.....	64
管理快照.....	65
卸载文件代理程序.....	66
卸载卷代理程序.....	67
卸载“卷”代理程序.....	67
卸载“具有策略的卷”代理程序.....	67
卸载“对象存储”代理程序.....	68
从 MDE 中除去代理程序.....	68
代理程序实用程序.....	69
第 12 章 操作.....	71
产品数据备份与复原.....	71
产品数据备份.....	71
产品数据复原.....	71
内核更新.....	72
升级.....	72
对于 MDE 服务器.....	72
用于代理程序目标 VM.....	73
服务数据.....	74
收集服务数据.....	74
从 PPM 日志中除去敏感信息.....	74
附录 A 样本代理程序安装过程.....	75
Red Hat/CentOS 流程.....	75
AIX 流程.....	76
Windows 服务器进程.....	76
附录 B 样本认证中心 (CA) 证书.....	79
附录 C 用于创建 PKCS12 文件的样本转换.....	83
附录 D 注意事项.....	85
更改分配的密钥.....	85
概述.....	85
背景.....	85
使用已加密的备份轮换密钥.....	85
概述.....	85
背景.....	85
附录 E 就地加密.....	87
命令选项.....	87

审计步骤.....	87
加密步骤.....	87
附录 F 代理程序调试日志记录.....	89
Linux 代理程序.....	89
Windows 代理程序.....	89
附录 G 非 OVA 部署.....	91
附录 H 软件版本检查.....	93
附录 I 词汇表.....	95
声明.....	101
商标.....	102
产品文档的条款和条件.....	103
隐私策略注意事项.....	103

第 1 章 简介

授权使用许可权

此软件的使用限于许可协议的条款。

联系点

有关 IBM Multi-Cloud Data Encryption (MDE) 的其他信息，请访问 IBM 支持 Web 站点 <https://www.ibm.com/support/home/>。

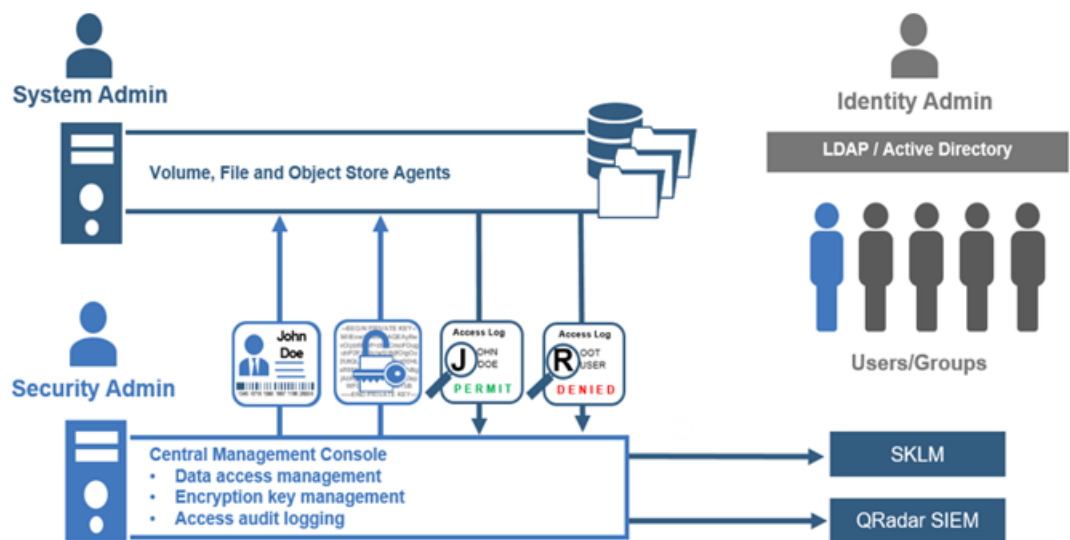
《管理员指南》的背景和目的

《管理员指南》是安装、管理和使用 MDE 的主要参考，以用于加密代理程序供应和管理、策略定义（访问和加密控制）、策略实施密钥管理以及在使用已部署代理程序的所选服务器上保护静态数据。本文档旨在供具有管理访问权并且了解其公司网络的系统管理员安装和管理产品。

第 2 章 一般概述

产品概述

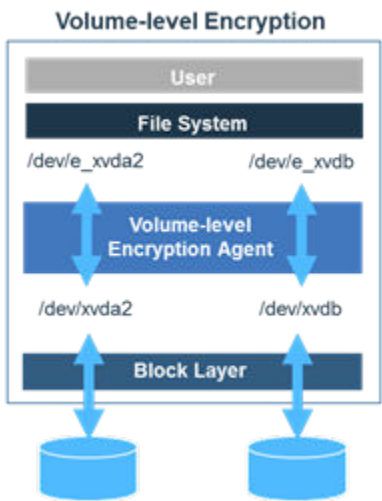
IBM Multi-Cloud Data Encryption (MDE) 是由 SPx® 技术支持的综合数据安全性产品，它将静态数据加密（通过代理程序）与充当中央管理控制台的策略供应管理器 (PPM) 的其他强大保护功能相结合。MDE 支持从一个中央位置进行代理程序供应、数据访问策略设置（操作访问定义和加密访问定义），以及多达 25,000 个代理程序的管理（密钥生命周期、代理程序更新和用户访问记录）。MDE 提供的无缝安全系统，可以灵活分配使用唯一加密拆分技术在文件系统级别或卷级别加密数据的代理程序。该技术提供的以数据为中心的防护超过标准加密，使数据加密更强健、更能抵御暴力攻击。通过定义详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



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“安全性管理员”。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“安全性管理员”角色委派了供应和管理代理程序所需的许可权。这些角色将在“第 7 部分：MDE 管理用户管理”中进一步讨论。

MDE 支持安装四种代理程序类型，它们提供用于实施策略定义的加密数据保护。

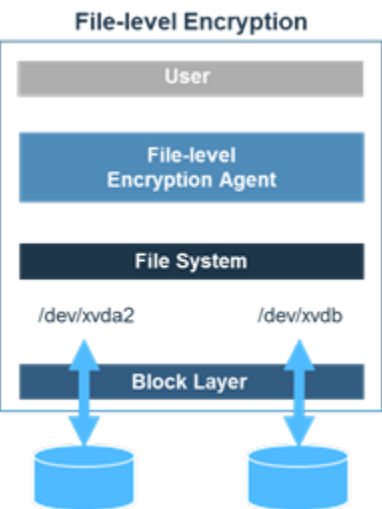
卷代理程序 (Volume Agent)



“卷”代理程序通过受限的访问策略控制提供卷级别加密。通过操作系统中的块驱动器实现，卷级别加密以受保护的预定义存储设备形式提供安全性。

整个卷已定义并作为一个单元加密保护。在添加、编辑或删除数据时，“卷”代理程序确保使用 PPM 管理的加密密钥为卷中的所有数据提供加密保护。

“具有策略的文件”代理程序



“具有策略的文件”代理程序将文件级加密与数据访问策略组合在一起。文件级加密在文件系统级提供单个文件保护。文件和存储环境大小仅受文件系统限制，而不受“具有策略的文件”代理程序的影响。受保护数据的位置是通过该路径定义的工作组密钥进行保护，在该位置中和下级位置存储的所有单个文件通过使用唯一且不可预测的初始化向量 (IV) 进行单独加密。受保护的数据可位于文件系统本地或通过 NFS 进行网络安装。

唯一文件级密钥由内部密钥管理系统处理。基于策略的访问控制在加密的基础上进行分层，从而允许定义具有最少权限的访问控制、指定访问记录以及将访问权限限制为特定系统功能（例如，读、读/写、复制、删除）。这些策略连同标准的 LDAP 或 Active Directory 许可权一起控制工作。如果用户对 LDAP 或 Active Directory 中的数据没有许可权，那么安全性管理员无法覆盖这些访问控制和授予数据访问权。

缺省情况下，所有用户将被排除，无法访问策略所涵盖的数据。安全性管理员需要定义哪些人员具有访问权。这样允许安全性管理员限制系统管理员、云供应商管理员和 root 用户，让他们无法访问受保护的数据。

“具有策略的卷”代理程序 (Volume with Policy Agent)

“具有策略的卷”代理程序利用卷代理程序的卷级别加密和基于文件的操作访问控制策略，您可对一个或多个受保护文件路径应用和实施这些策略。

“对象存储”代理程序

“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。根据许可证可在本地或远程位置上的已存储的数据片被称为“份额”。使用多个共享数据将允许改进数据流并添加针对数据弹性和容错的选项。支持的 M/N 分布式共享模式为 1:1、2:3 或 2:4。

“对象存储”代理程序 (OSA) 对发送到对象存储器的数据进行加密。它充当文件传输到对象存储器时的通道，并在传输过程中加密和拆分数据。通过“对象存储”代理程序从对象存储器检索的文件在检索时解密。对象存储器中的静态文件是加密的。只有授权用户才能通过“对象存储”代理程序发送/接收数据。

代理程序功能部件矩阵

代理程序功能部件	卷代理程序 (Volume Agent)	“具有策略的卷” 代理程序 (Volume with Policy Agent)	“具有策略的文 件”代理程序	“对象存储”代理 程序
加密整个卷	√	√		
逐个加密指定的受 保护目录中的文件			√	
文件级别策略		√	√	
文件访问审计日志		√	√	
防止管理员访问用 户数据			√	
加密对象存储器中 的数据				√

第 3 章 规划注意事项

先决条件

IBM Multi-Cloud Data Encryption (MDE) 安装是一个简单明了的过程，其中包括安装基本开放式虚拟设备 (OVA) 以及运行供应策略和管理 (PPM) 安装程序。

在准备过程中，建议您先复审整个安装指示信息，然后再安装软件。下面是成功安装和操作 IBM Multi-Cloud Data Encryption 的先决条件的列表。

1. 使用特许操作系统和受支持的系统管理程序 (VMware ESXi™) 部署和运行 PPM 的操作服务器。
2. 已打包的基本 OVA
3. PPM 安装程序
4. 一个或多个具有受支持代理程序操作系统 (Red Hat® / CentOS 6.2+ 或 7.2+、AIX 7.1 或 7.2 以及 Microsoft Windows Server® 2008 R2、Microsoft Windows Server® 2012 R2i 或 Microsoft Windows Server® 2016) 的目标服务器。
5. 浏览器：Google Chrome®、Microsoft Internet Explorer® 10+、Mozilla Firefox® ESR 52+。
6. PPM 和所有代理程序之间的网络访问。
7. 认证中心签名证书（密钥库、信任库和 CA 证书捆绑软件），用于在管理服务器 (PPM) 和所有代理程序之间建立安全会话。

请参阅“证书需求”和“服务器证书设置”以获取更多详细信息并参阅第 79 页的『附录 B 样本认证中心 (CA) 证书』以获取示例。

对于“对象存储”代理程序 (OSA)，以下是附加要求：

- S3 兼容对象存储器：Amazon Web Services S3 (AWS S3)，IBM Cloud Object Storage (COS S3)
- 对象存储器凭证：用户标识和密钥（密码）
- 利用 AWS S3 REST API 库或 Boto Python 库将数据指向 OSA 代理程序的应用程序或实用程序

重要注意事项：强烈建议 MDE、外部数据库和代理程序利用 NTP 来协调系统时间。这将确保事件/审计日志时间戳记排序正确。

最低系统需求

PPM VM 最低系统需求

- CPU 4
- 8 GB RAM
- 40 GB 的可用存储空间
- 需要网络访问权

Linux 代理程序最低系统需求

- 已启用 ADE-NI 的 64 位单核 CPU @2GHz
 - （建议使用已启用 AES-NI 的 64 位双核 CPU @2GHz）
 - 2 GB RAM（建议使用 4 GB RAM）
- 20 GB 的可用硬盘空间
 - 建议应提供 300 MB 或更大的日志文件空间

- 需要网络访问权
- 在 Red Hat/CentOS 上安装/更新以下包：curl、openssl 和 nss
- 初次安装代理程序期间的因特网访问权或对本地存储库的访问权
- 代理程序需要使用 SSL 证书

Windows 代理程序最低系统需求

- 64 位单核 CPU @2GHz 且支持 AES-NI - 建议使用 64 位双核 CPU @2GHz 且支持 AES-NI
- 4 GB RAM - 建议使用 8 GB RAM
- 20 GB 可用硬盘空间 - 建议日志文件的可用空间为 300 MB 或以上
- 需要网络访问权
- 代理程序需要使用 SSL 证书

注：需要 SSL（自签名或认证中心）证书/密钥对文件才能创建代理程序。可利用此证书在代理程序与 MDE 服务器之间建立安全的 TLS 连接。

证书要求

在 PPM 服务器和这些代理程序之间建立安全连接需要证书：证书需求包括以下内容：

- PPM 服务器要求代理程序提供的证书必须解析为该代理程序（DNS 主机名或 IP 地址）
- PPM 服务器要求代理程序提供的证书使客户机认证扩展密钥用法集
- 代理程序要求 PPM 服务器提供的证书必须解析为 PPM 服务器（DNS 主机名或 IP 地址）
- 代理程序要求 PPM 服务器提供的证书使服务器认证扩展密钥用法集

PPM 和代理程序应该同步到可靠时间来源以确保证书在有效期内。

要求每个已部署的代理程序都有唯一的证书。

代理程序的文件系统支持

“卷”代理程序在卷级别执行加密。“具有策略的文件”代理程序将使用或者在受支持的主机操作系统的文件系统中运行。“具有策略的文件”代理程序和“具有策略的卷”代理程序支持以下文件系统：

Linux 服务器

- EXT3
- EXT4
- XFS（在 Red Hat/CentOS 6.5 或更新版本上）
- NFS（NFSv3、NFSv4）

Windows 服务器

- NTFS
- ReFS（在 Windows Server 2012 R2 或更新版本上）

AIX

- JFS2

网络设置

关于此任务

MDE 要求在 MDE PPM 服务器和代理程序之间建立一致的网络连接。支持因特网协议 IPv4 和 IPv6。将静态 IP 分配或 DHCP 与静态租赁配合使用将满足此需求。此外，DNS 基础结构将正常工作并在生态系统中利用主机名。

网络端口

功能	缺省端口	可配置
Web	443	是
数据库	5432	是
外部 LDAP	无	是
LDAP 目录	无	是
电子邮件事件转发	无	是
系统日志事件转发	无	是

OVA 配置

对所提供的 MDE OVA 已进行预配置，将 MaxAuthTries 设置为 1。要通过 SSH 成功认证到 MDE VM，将需要更改 MaxAuthTries（不推荐）或者 SSH 客户机需要在命令行上或本地 SSH 客户机配置中将 PubkeyAuthentication 设置为“否”。

REST 界面

MDE 支持整个程序化 REST 界面。根 REST URL 为：

https://<Virtual Machine IP>/rest/

重要注意事项

REST API 将允许管理员执行不能通过 Web 界面访问的高级功能。可能会通过可使代理程序处于不受支持状态的方式来使用 REST API；因此，了解 REST API 编程知识至关重要。

有关更多详细信息，请参考 IBM Multi-Cloud Data Encryption (MDE) REST API 规范文档。

第 4 章 产品安装

为安装做准备

MDE 安装过程有三个步骤：

1. 先决条件
2. MDE 基本开放式虚拟设备 (OVA) 可用
3. 受支持的管理程序 (VMware ESXi™)

许可

MDE 不需要唯一产品许可证运行或配置代理程序（除在软件许可协议中提供的代理程序以外）。

MDE OVA/VM 管理

在部署 MDE OVA 后，更新系统以确保安装了最新的安全补丁和软件版本。

注：定期更新系统以获得安全补丁和更新的软件版本。

安装 MDE

关于此任务

要安装 MDE 软件：

使用文件（例如 `ibm_sw_mde_X.x.x-XX.bin`），用构建号替换 XX（表示可用软件的版本），并以 root 用户身份操作。

过程

1. 将 MDE 基本 OVA 部署到管理程序中。在此示例中，会将其称为“MDE VM”。
2. 以管理员身份登录并设置新密码。

MDE VM 使用可由管理员配置的 PAM 规范标准。PAM 密码长度必须大于 8 个字符，并且不能包含先前密码中的 5 个字符。

3. 记下 MDE VM 的 IP 地址。
4. 使用 SCP 或类似的文件传输方法将 `ibm_sw_mde_X.x.x-XX.bin` 上载到 MDE。
5. 使 bin 文件可执行。

```
[admin@localhost]$ chmod +x ./ibm_sw_mde_X.x.x-XX.bin
```

6. 执行 bin 文件。

```
[admin@localhost]$ ./ibm_sw_mde_X.x.x-XX.bin
```

7. 选择“英语”并点击 Enter 键。
8. 阅读许可证页面，移动到<确定>，点击“Enter”以继续操作。
9. 选择<是>并点击“Enter”以接受许可协议。
10. 抽取完成后，在<确定>上点击“Enter”以返回到命令行。

11. 以 root 用户身份安装 RPM。

```
[admin@localhost]$ sudo yum -y install rpms/*.rpm
```

12. MDE 现已安装，但尚未配置。

注: 在配置完成之前，请勿重新引导 MDE VM。

语言设置

关于此任务

MDE 针对 VM 脚本和 PPM GUI 支持多种语言。运行产品之前，您将需要配置缺省语言首选项。

注: 通过 RPM 将语言安装到 MDE VM 中。安装程序二进制文件随附一组内置语言 RPM。初始安装后，可以添加其他语言，并且可能需要重新启动 PPM 服务以便生效。

要配置缺省语言，请遵循下面的步骤：

过程

1. 运行 spsd-langsetup 脚本。

```
$ sudo /opt/securityfirst/spsd/bin/spsd-langsetup
```

2. 查看当前缺省语言代码。如果未设置任何语言代码，那么它将为空白。

```
设置缺省语言代码。
当前缺省值为：
```

3. 查看可用语言代码的列表。（下面的列表可能会显示您的产品版本中不可用的示例。）

```
可用语言代码：
en_US
ja_JP
ko_KR
```

4. 输入新的缺省语言代码。

```
输入新的缺省语言代码：en_US
缺省语言代码将为 en_US
```

5. 重新执行 spsd-langsetup 脚本以验证是否设置了缺省语言代码。

```
设置缺省语言代码。
当前缺省值为：en_US
```

数据库设置

关于此任务

MDE 支持内部或外部数据库配置。在任何一种情况下，您都需要将 MDE 配置为在首次启动 MDE 前与已配置的数据库通信。

要将数据库与 MDE 关联，您将需要修改 MDE VM /etc/spsd/db.props 文件。您将需要以 root 用户身份编辑此文件。

注: 运行 spsd-pgsetup 脚本将自动使用提示符中输入的值修改 db.props 文件。

配置文件属性以连接到相应的内部或外部数据库，如下所述。在重新启动 MDE 之前，数据库属性更改将不会生效。

重要注意事项

在修改 **db.props** 时，请遵守以下约束：

- 属性名称和 = 之间无空格
- = 和属性值之间无空格

内部数据库

当前，MDE 支持 PostgreSQL 作为内部数据库。

内部 Postgres 数据库

MDE OVA 已预先封装，其中安装了 PostgreSQL 软件。要配置数据库以使用 MDE，请遵循下面的步骤：

1. 运行带有 “--local” 脚本选项的 **spsd-pgsetup** 脚本。

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --local
```

注：“--local” 选项用于在内部 “本地” PostgreSQL 服务器上配置新的空数据库。

应用这些设置后，前进到 “服务器证书设置”。如果计划在远程目标上设置数据库，请前进到 “外部数据库”。

外部数据库

目前唯一受支持的外部数据库服务器是 PostgreSQL。您必须确保在执行此过程之前以下信息为已知：

- 可访问的 PostgreSQL 数据库服务器名称（或 IP 地址）
- 上述 PostgreSQL 服务器侦听的端口号
- 上述服务器上的现有数据库的名称
- 定义为上述服务器的所有者的现有用户的名称
- 上述数据库用户的密码

要配置数据库以使用 MDE，请运行 **spsd-pgsetup** 脚本。此命令中提供的所有值仅为示例：

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --host  
ext.postgres.svr1 --port 5432 --dbname policyDB --user policyDBuser  
--pass mypassword123
```

要将数据库升级到最新模式，请运行带有 “--upgrade” 脚本选项的 **spsd-pgsetup** 脚本

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --upgrade
```

注：运行带有 “upgrade” 选项的 **spsd-pgsetup** 脚本可确保数据库表正确配置到当前版本的 PPM。

在配置这些设置后，继续执行 “服务器证书设置”。

服务器证书设置

密钥库、信任库和认证中心

证书用于在管理服务器 (PPM) 和代理程序以及 Web 浏览器之间建立安全通信会话。PPM 需要认证中心 (CA) 签名所有证书。CA 建立所有通信会话参与者用于验证另一方身份的信任根。

- CA 签名证书及其对应的密钥组合成一个 java 密钥库。
- 必须将用于签署代理程序证书的来自 CA 的证书（或证书捆绑包）添加到 PPM 信任库。
- 以下 PPM 证书设置过程中使用了所有三个组件（密钥库、信任库和 CA 证书捆绑包）。

请参阅第 79 页的『附录 B 样本认证中心 (CA) 证书』以获取认证中心证书流程的样本。

通过 MDE VM 的 /opt/securityfirst/spsd/bin 目录中的

设置脚本 spsd-certsetup 来配置服务器 Web 证书密钥库和 Web 证书信任库。

要配置密钥库和信任库以及代理程序 CA 捆绑包，请参阅**粗体**的示例输入：

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ks /etc/ppm/certs/ppm.jks --kw password
```

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ts /etc/ppm/certs/trust.jks --tw password
```

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --aca /etc/ppm/certs/ca_bundle.pem
```

注

服务器证书组件（例如，密钥库、信任库和 CA 捆绑包）未提供，而是必须通过设置脚本生成并上载到 MDE VM。如果将通用访问卡 (CAC) 用于认证，那么需要启用 PKI 设置。

公共密钥基础结构 (PKI) 设置

关于此任务

通过 PKI 配置，PPM 可以提供 PPM 用户认证辅助方法。配置后，PPM 将接受客户机证书作为 Web 和 REST 会话的认证方法。

此证书必须由 PPM 信任的 CA 签署。PPM 将根据 spsd-certsetup 脚本中定义的规则来验证证书。

例如，以**粗体**形式输入以下内容：

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --crl-on --ocsp-on --pols-on oids
```

```
x.x.x.x.x.x.x.x,Y.Y.Y.Y.Y.Y
```

注

可以在与密钥库、信任库和 CA 捆绑软件相同的脚本执行中配置 PKI。为进行指导，此处对其进行了细分。

安装 MDE，配置数据库，添加证书和（可选）设置 PKI 后，您现在可以重新引导 MDE VM。

启动和首次登录

关于此任务

完成部署和配置后，重新引导 MDE 服务器，或者只是从 MDE 控制台启动服务“spsd”以启动 Web GUI 即可。您将需要通过虚拟机控制台或主机管理程序来检索虚拟机的 IP 地址或主机名。

打开受支持的 Web 浏览器并输入 IP 地址或主机名作为 URL 以访问 MDE 登录页面。

```
https://<MDE Server IP>
```

此时，可以从可用的支持语言列表更改语言设置。



Please Sign In

User name
Password
Directory
Login

缺省凭证为:

用户名 : admin
密码 : admin

注

- 首次登录后，需要更改缺省凭证
- MDE 支持 Firefox、Chrome、Microsoft Edge 和 Internet Explorer Web 浏览器的大多数版本
- 使用 PKI 客户机认证时，可以绕过登录页面并直接转至仪表板

第 5 章 MDE 图形用户界面 (GUI)

基本产品导航

MDE 包含页面顶部的导航菜单。一些菜单项包含子菜单列表。单击每个菜单项以浏览至相应页面或显示子菜单列表。



- **主页图标** - 产品“仪表板”主页的链接。
- **密钥** - 包含以下密钥相关子菜单页面链接的菜单：“外部密钥库”和“受管密钥”。
- **策略** - 包含以下策略相关子菜单页面链接的菜单：“数据类型”、“路径集”和“选择器”。
- **代理程序** - “代理程序”页面的链接。
- **作业** - “作业”页面的链接。
- **事件** - 包含以下事件相关子菜单页面链接的菜单：“转发”和“日志”。
- **用户** - 包含以下用户相关子菜单页面链接的菜单：“帐户”和“LDAP 目录”。
- **设置** - “设置”页面的链接。

注

MDE 支持基于角色的访问控制 (RBAC)，这意味着基于已登录用户的角色，一些导航项将不可用。因此，一些导航项可能对所有管理用户均不可用。

产品仪表板

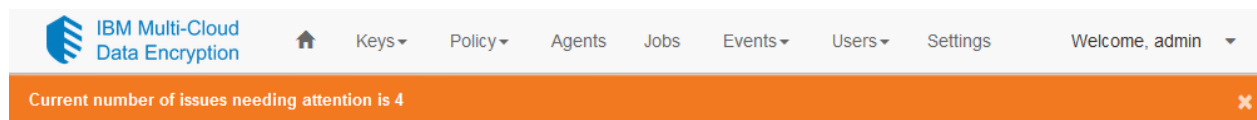
产品主页是主要登录仪表板页面。它旨在向已登录的管理员提供最新事件当前状态的摘要视图。主页包含最新事件、事件趋势和其他摘要数据

文本框自动补全

整个用户界面中都有文本输入字段。基于已输入字符的自动补全，一些文本输入字段将显示匹配条件。在出现自动补全建议列表前，这些字段可能需要多个字符

注意通知

在首次登录时，用户界面顶部将出现一个彩色条幅，指示解决问题所需的操作。



单击条幅中文本会将管理员重定向到显示各个项目的“问题”页面。

- ▶ The current number of job approvals allows unilateral action. [Dismiss](#)
- ▶ The number of users having Product Administrator role is nearing the threshold of required approvals or required rejections. [Dismiss](#)
- ▶ The number of users having Security Administrator role is nearing the threshold of required approvals or required rejections. [Dismiss](#)
- ▶ One or more users are defined as having both Product Administrator and Security Administrator roles. [Dismiss](#)

展开单个项目将显示如何解决该问题的详细信息。

- ▼ The current number of job approvals allows unilateral action. [Dismiss](#)

Summary It is best practice to require a minimum two administrators for job approval.

How to resolve Go to the "Advanced Properties" tab on the "Settings" page, and edit the "Number of approvals required to run a job" field. Note that it may also be wise to do this for number of rejectors as well, depending on company structure.

[Resolve](#)

一旦解决所有未解决的问题，将不显示条幅；但是，管理员可选择关闭当前页面的条幅。

注

可能会出现导致新建“需要注意”问题的新条件，此时该条幅将再次显示。

高级属性

允许“产品管理员”配置定义产品行为的高级属性。高级属性可通过“设置”页面进行访问。这些属性的作用域是本地实例，或者也可能是 MDE 生态系统（如果利用高可用性 (HA) 或多租户功能）。

Advanced Properties

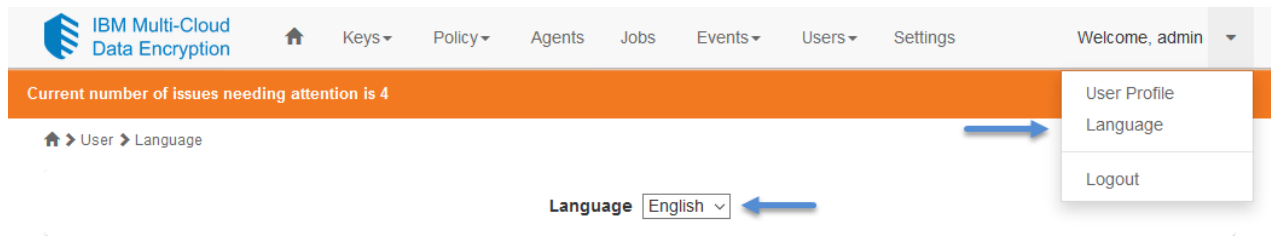
Property	Value	Description	Actions
com.securityfirstcorp.atlantis.bundles.haas.iterations	600000	Number of iterations used by REST API token hashing algorithm	Edit
com.securityfirstcorp.atlantis.jobs.requiredApprovers	1	Number of approvals required to run a job	Edit
com.securityfirstcorp.atlantis.jobs.requiredBuffers	2	The buffer number in between the number of users available and when we issue a warning	Edit
com.securityfirstcorp.atlantis.jobs.requiredRejectors	1	Number of rejections required to reject a job	Edit
events.maxLogLength	50000	Maximum number of entries in event log before rolling starts	Edit
com.securityfirstcorp.atlantis.bundles.userman.iterations	300000	Number of iterations used by user password hashing algorithm	Edit

要编辑属性，产品管理员必须单击“编辑”按钮。进行相应更改后，单击“保存”按钮，将创建一个作业。

GUI 语言设置

通过 GUI，在初始安装期间，从登录页面或主页进行选择时，可更改为其中一个已安装的受支持语言。

- **登录页面** - 位于页面的右上角。单击下拉菜单可显示受支持的语言列表。
- **主页** - 从右上角的下拉菜单中，选择“语言”以获取受支持的语言列表。

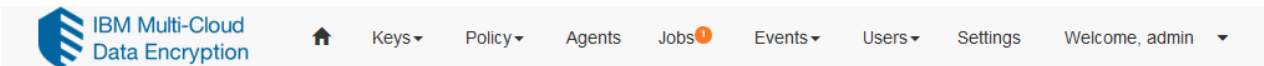


GUI 中显示的语言由以下层次结构确定（使用显示的第一个设置）：

1. 通过 PPM 用户界面设置的语言 cookie 的值。
2. 用户浏览器语言设置的值。
3. 通过 PPM CLI script-langsetup 设置的语言代码的值。
4. 第一个找到的已安装 PPM 语言包。

第 6 章 作业

MDE 包含一个作业系统，用于管理正在运行的任务的核准和计时。众多功能利用作业系统以等待确认前核准。创建作业后，将向“作业”页面上的列表添加一个新作业。



管理员将可以选择核准、拒绝或放弃每个作业。每个管理员只能对每个作业采取一次操作。

Type	State	Created	Started	Completed	Notes	Actions
User Create	Waiting	2017-09-22T23:21:01Z				Edit Note Approve Reject Abstain Show Info

作业描述

作业	说明	类别	角色
高级属性	修改高级属性	产品管理	产品管理员
修改密钥库	更改策略实施密钥库的位置/详细信息	产品设置	产品管理员
密钥轮换	在代理程序生态系统中轮换一组密钥	密钥管理	安全性管理员
密钥撤销	从代理程序生态系统中撤销一组密钥	密钥管理	安全性管理员
密钥粉碎	从代理程序生态系统中永久除去一组密钥导致数据丢失。	密钥管理	安全性管理员
添加代理程序	向生态系统供应和添加新代理程序	代理程序管理	安全性管理员
删除代理程序	从 MDE 管理中除去代理程序	代理程序管理	安全性管理员
修改代理程序	修改与代理程序有关的信息	代理程序管理	安全性管理员
策略更新	修改与代理程序关联的策略	代理程序管理	安全性管理员
创建新的管理用户	创建新的 MDE 管理员	MDE 管理用户管理	产品管理员
删除管理用户	除去 MDE 管理员	MDE 管理用户管理	产品管理员
添加管理用户角色	向 MDE 管理员添加角色	MDE 管理用户管理	产品管理员
除去管理用户角色	从 MDE 管理员除去角色	MDE 管理用户管理	产品管理员
更改管理用户密码	更改 MDE 管理员的密码	MDE 管理用户管理	产品管理员
更改管理用户状态	启用或禁用 MDE 管理用户帐户	MDE 管理用户管理	产品管理员

注册目录	为 MDE 管理用户配置 LDAP 服务器目录	MDE 管理用户管理	产品管理员
删除目录	从 MDE 中除去 LDAP 服务器目录	MDE 管理用户管理	产品管理员
更新目录	修改 LDAP 服务器目录	MDE 管理用户管理	产品管理员

多管理员核准

在 MDE 中可配置所需数量的核准人和拒绝者。缺省情况下，配置 MDE 以供单个管理员核准。强烈建议应该提供两个或多个管理员来核准作业。多管理员核准可防止单个管理员在 MDE 本身进行更改或对任何受管代理程序实例进行更改。

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

重要注意事项

管理用户的数量必须满足或超过“需要核准”或“需要拒绝”作业的数量。确保有必需数量的管理用户，然后更改这些值。

核准和拒绝阈值可能被作业类型覆盖。由系统定义的每种作业类型（除“属性更改”作业以外）在“高级属性”中都具有核准和拒绝阈值，在设置时将覆盖系统缺省值。设置属性后，它可能不会复原

“属性更改”作业是不具有核准和拒绝阈值的唯一作业类型，因为它控制对“高级属性”的修改。对于此作业，核准和拒绝阈值将始终是系统缺省值的较高值或为任何其他作业定义的最高覆盖值。该操作将确保通过属性更改过程不能破坏其他作业类型阈值。

作业核准

要核准作业，具有正确许可权的管理员必须浏览至“作业”页面，查找相应的作业，然后单击“核准”按钮。在达到所需数量的管理员核准后，作业将执行。

作业拒绝

要拒绝作业，具有正确许可权的管理员必须浏览至“作业”页面，查找相应的作业，然后单击“拒绝”按钮。在达到所需数量的管理员拒绝后，将永久取消该作业。

作业放弃

放弃作业指示管理员已看到该作业但不想核准或拒绝该作业。放弃最好被描述为“审计”位置并阻止管理员将来在同一作业上选择其他位置。

作业信息

MDE 中的每个作业都具有对其进行描述的不同消息。可单击“显示信息”按钮，将显示特定于作业的信息。此外，不同管理员对作业采取的任何操作（核准、拒绝、放弃）将与采取操作的管理员的用户名一起显示。

User Create	Done	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z	2017-09-22T23:22:36Z		<div>Hide Info</div>
-------------	------	----------------------	----------------------	----------------------	--	----------------------

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

Job Properties

User	ProductAdmin
------	--------------

第 7 章 MDE 管理用户管理

管理用户角色

MDE 利用基于角色的访问控制 (RBAC) 平面静态设计。MDE 中的特定功能需要特定许可权。完整的 MDE 许可权集分为两个不同的角色：产品管理员和安全性管理员。每个角色的其他管理员可随时添加。

“产品管理员”角色

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。

“安全性管理员”角色

向“安全性管理员”角色委派了供应和管理代理程序所需的许可权。包括但不限于：策略定义和指定、密钥管理、数据类型定义、代理程序管理、外部密钥库配置，以及针对策略的外部组的外部 LDAP 配置。

管理用户管理

产品管理员拥有在 MDE 中添加、修改和除去其他管理用户所需的许可权。

添加新的管理用户

当添加新管理用户时，系统将提示产品管理员输入新的管理用户名。

Edit User

New User Name

Cancel

Add User

填写唯一的用户名，然后系统将创建一个作业以将此管理用户添加到 MDE。

Type	State	Created	Started	Completed	Actions
Scheduler	Waiting	2019-03-20T16:14:01Z			<div>ApproveRejectAbstainHide Info</div>
<div><div>ApprovedNone</div><div>RejectedNone</div><div>AbstainedNone</div></div> <div><div>Type : User Create</div><div>Frequency : Once</div><div>Starts : Upon approval</div></div> <div><div>Job Properties</div><div>User</div><div>test</div></div>					

必须由所需数量的产品管理员核准该作业才能创建用户。

新增管理用户是使用到期密码和未定义的角色创建的。产品管理员必须编辑初始密码、角色和状态。这些更新中的每一次更新都将生成一个作业。作业必须先获得核准，新的管理用户在 MDE 中才能变为活动状态。

编辑管理用户密码

要编辑管理用户密码，请浏览至相应用户并选择“编辑密码”按钮。将显示密码输入对话框。

输入符合已确定规则的密码。输入后，保存更改，将创建一个作业。

必须由所需数量的管理用户核准该作业才能使密码更改生效

注：将提示新增管理员在初次登录时更改密码。

编辑管理用户角色

要编辑管理用户的角色，请找到用户行并选择“编辑角色”按钮。角色输入复选框将以内联方式显示。

执行编辑的管理用户将能够应用其拥有的相同角色，例如，“内置管理员用户”，这是可同时应用“产品管理员”和“安全性管理员”角色的初始用户。然后，授予相同角色的用户可执行相同操作。

ProductAdmin	Disabled	<input type="checkbox"/> Product Administrator <input type="checkbox"/> Security Administrator		2017-09-22T23:25:40Z	Save Cancel
--------------	----------	---	--	----------------------	-------------

选择所需角色并单击“保存更改”按钮，将创建一个作业。

必须由所需数量的管理员用户核准该作业才能使角色更改生效。

编辑管理用户状态

要编辑管理用户状态，请浏览至受影响的用户并选择“编辑状态”按钮。状态输入下拉列表将以内联方式显示。

ProductAdmin	Disable ▾	None		2017-09-22T23:25:40Z	Save Cancel
--------------	-----------	------	--	----------------------	-------------

状态值为：已启用、已禁用和已锁定。

- **已启用** - 管理用户处于活动状态并且能够执行操作。
- **已禁用** - 管理用户处于不活动状态并且无法执行操作
- **已锁定** - 管理用户已锁定并且无法执行操作。

选择所需状态，然后单击“保存”，将创建用于修改用户状态的作业。

必须由所需数量的管理用户核准该作业才能使状态更改生效。

除去管理用户

要除去管理用户，请找到目标用户行并单击“删除”按钮。将启动作业以从 MDE 中除去用户。此操作只能由具有“产品管理员”角色的用户执行。

Type	State	Created	Started	Completed	Notes	Actions
User Delete	Waiting	2017-09-22T23:37:05Z				<div>Edit Note</div> <div>Approve</div> <div>Reject</div> <div>Abstain</div> <div>Show Info</div>

必须由所需数量的管理用户核准该作业才能除去用户。

重要注意事项

- 除去管理用户是一项永久操作。
- 必须保持足够数量的管理用户才能满足所需的作业核准条件（请参阅“多管理员核准”部分）。
- 如果没有足够的管理用户，那么无法成功接受作业。

用户帐户锁定

为保护系统帐户和用户帐户免受暴力密码攻击，将在连续十 (10) 次登录尝试失败后锁定用户帐户。在明确开启用户帐户（请参阅“编辑管理用户状态”部分）或重新启动服务器服务前，将锁定用户帐户。

注

- 要重新启动服务器服务，请在虚拟机控制台中运行 **systemctl restart spsd**。
- 帐户锁定按每个服务器进行设置。在集群中的一个服务器上锁定的帐户不会自动锁定该集群中的其他服务器。
- 用户无法配置“帐户锁定”阈值。

LDAP 目录列表

产品管理员可以为 MDE 用户管理配置 LDAP 目录。LDAP 目录可以添加、修改或删除。每个操作将在生效前创建需要核准的作业。

添加/修改 LDAP 目录时，可用设置为：

- **目录标识** - LDAP 目录的标识。
- **类型** - LDAP 或 Active Directory 的下拉选项
- **绑定 DN** - 用于绑定到 LDAP 服务器的完整专有名称。

绑定 DN 样本语法如下所示：

```
uid={susername},ou=users,dc=company,dc=com
```

注: 选择“Active Directory”类型时，“绑定 DN”部分变灰，因为不需要此信息。

- **主机** - LDAP 服务器的 IP/主机名
- **端口** - LDAP 服务器的端口
- **安全** - 安全或不安全的 LDAP 连接的标识
- **操作** - 选择“保存”或“取消”

Directory ID	Type	Bind DN	Host	Port	Secure	Actions
LDAP1	LDAP	uid={susername},ou=users,dc=company,dc=com	10.10.10.1	536	<input checked="" type="checkbox"/>	<div>Save</div> <div>Cancel</div>

用户源

MDE 可以同时支持内部和外部定义的用户。 外部定义的用户将在用户列表的“目录”列中显示值。 内部定义的用户将使该字段为空。

Name	Status	Roles	Directory	PW Modified	Actions
admin	Enabled	Product Administrator, Security Administrator		2017-09-22T23:09:44Z	<a>Edit Password <a>Edit Roles <a>Delete
ProductAdmin	Enabled	Product Administrator		2017-09-22T23:25:40Z	<a>Edit Password <a>Edit Status <a>Edit Roles <a>Delete
SecurityAdmin	Enabled	Security Administrator		2017-09-22T23:42:22Z	<a>Edit Password <a>Edit Status <a>Edit Roles <a>Delete

第 8 章 事件

MDE 包括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。此外，它可以配置为将事件转发给一个或多个接收方

事件日志

通过选择顶级菜单栏上的“事件”菜单项，可以查看 MDE 事件日志。

🏠 > Events > Logs

☐ Show Redacted Events

ReloadExport CSV

Show 10▼ entries

Search:

Sequence▼	ID▲	Message▲	Type▲	Severity▲	Timestamp▲	Source▲
16	PS000D0005	Requested action change-passw...	SYSTEM	INFO	2017-09-22T23:42:22Z	localhost
15	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:22Z	localhost
14	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
13	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
12	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:42:21Z	localhost
11	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:42:21Z	localhost
10	PS000D0005	Requested action change-user-st...	SYSTEM	INFO	2017-09-22T23:36:47Z	localhost
9	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:36:47Z	localhost
8	PS000D0005	Requested action change-user-ro...	SYSTEM	INFO	2017-09-22T23:35:51Z	localhost
7	PS000D0001	User admin has requested action ...	AUDIT	INFO	2017-09-22T23:35:51Z	localhost

Showing 1 to 10 of 16 entries

FirstPrevious12NextLast

此页面显示单个顺序列表中的所有事件。每个事件都具有序列号、标识、消息、类型、严重性、接收时间戳记以及来源，如下所定义：

- **序列号** - 取决于事件接收顺序的编号。它是唯一的（即使同一事件重复发生），并且随时间递增。
- **标识** - 事件的唯一标识。同一事件的多个实例将具有共同的标识。
- **消息** - 用于标识触发事件的条件的描述性文本。一些事件可能支持变量插入，因此，虽然事件标识可能是共同的，但是文本可以稍有不同。
- **类型** - 描述事件来源是来自系统操作还是来自用户操作。类型为：
 - **系统** - 由自动执行的 MDE 操作发起的事件。
 - **审计** - 由用户操作发起的事件。
- **严重性** - 事件认知级别的相对指示。严重性类别为：
 - **参考** - 不需要任何操作，仅供参考
 - **警告** - 不需要立即进行操作；建议监视状态
 - **紧急** - 需要立即进行操作
- **时间戳记** - 事件发起时间的全球标准时间 (UTC) 格式的指示。

· **来源** - 发起事件的系统（代理程序或 MDE）的主机名或 IP。

MDE 事件日志大小可通过“高级设置”进行配置。达到集合大小限制后，在收到新事件时将轮换出最早的事件。

事件详细信息

事件可能具有不在事件消息中的扩展自变量。如果存在，事件将在事件日志的消息列中显示“详细信息”链接。单击“详细信息”按钮将显示扩展自变量

34	PS00140002	Agent 1 logged off: reason code 1006.	Details	2018-04-10T15:02:05Z	localhost
33	DEC02014	Read/write denied for user3 on /home/data/	Details	2018-04-10T15:01:19Z	cos5-file
32	DEC02010	Read denied for user4 on /home/data/	Details	2018-04-10T15:01:19Z	cos5-file
31	DEC02011	Write permitted for user1 on /home/development/	Details	2018-04-10T15:01:19Z	cos5-file

Details

Absolute process path:
Decision: Deny
Group name: user3
Operation: Read or Write

事件导出

MDE 允许管理员通过“事件”页面上的“导出 CSV”按钮将事件列表导出为 CSV 文件格式。

🏠 > Events > Logs

☐ Show Redacted Events

Reload Export CSV

单击“导出 CSV”按钮将事件文件下载到客户机。事件文件中的每一行都是日志中的一个事件。

事件文件包含以下列：事件序列号、事件标识、已编辑的标志、事件消息字符串（省略自变量）、事件类型、事件严重性、事件自变量、事件时间戳记和事件来源。

事件转发

接收的每个事件都将转发给每个已配置的事件接收方。事件在插入到内部事件日志的同时进行转发。

产品管理员或安全性管理员可以修改产品的事件接收方。配置之后，由 MDE 创建或接收的任何事件都将转发给接收方。受支持的接收方类型为系统日志。

🏠 > Events > Forwarding

Email Recipients

New Email Recipient

Email	Host	Port	Security	User	Password	Format	Actions
No Recipients							

Syslog Recipients

New Syslog Recipient

Host	Port	Format	Actions
No Recipients			

MDE 还支持已转发事件的多种格式。受支持的格式为：日志事件扩展格式 (LEEF)、公共事件格式 (CEF) 和云审计数据联合 (CADF) 事件模型。

事件自变量

除正常事件消息字符串以外，事件自变量将作为密钥/值参数发送。这些参数将由“spx”前缀和自变量名称的合并字符串进行标识。例如，如果事件包含用户名，那么字符串密钥/值配对可以是“spxuser=user1”。

代理程序事件

MDE 聚集每个受管（并且已连接的）代理程序中的系统事件和审计事件。这些事件显示在 MDE 事件日志中并且转发给任何已配置的事件接收方。

注

强烈建议 MDE 、外部数据库和所有代理程序利用 NTP 来协调系统时间。这将确保事件/审计日志时间戳记排序正确。

可靠的事件

从单个代理程序发送到 MDE 的事件会得到实时处理。这将确保如果缺少事件，MDE 将追溯到代理程序，请求缺失的事件，并以正确的顺序将其插入到事件日志中。

第 9 章 策略实施密钥管理

安全性管理员可以为 MDE 中的安全存储定义策略实施密钥。这些密钥可以与数据类型以及用于保护数据并提供加密访问控制的卷关联。

🏠 > Keys > Managed Keys

Submit Rotation JobNew Key

ID	Name	Created	Notes	Actions
1	Key1	2017-09-22T23:49:12Z		Edit Submit Revocation Job
2	Key2	2017-09-22T23:49:17Z		Edit Submit Revocation Job
3	Key3	2017-09-22T23:49:23Z		Edit Submit Revocation Job

添加密钥

当添加新密钥时，必须输入一个唯一名称。密钥名不区分大小写。密钥值未公开，用户无法编辑。注释字段是选填字段。

ID	Name	Created	Notes	Actions
	<input type="text"/>		<input type="text"/>	Save Cancel

注

密钥名称可以更改，但是用户无法修改实际密钥值。

密钥可以在“密钥”页面上创建，或在执行代理程序创建向导期间创建。在执行代理程序向导期间创建的所有“系统定义的”密钥将自动生成，无法管理。密钥只能在“密钥”页面上编辑。

编辑密钥

创建密钥后，安全性管理员可以修改密钥的名称。更改密钥名称不会更改实际底层密钥值。此外，还可以修改“注释”字段。

密钥轮换

MDE 使安全性管理员能够在代理程序生态系统中轮换密钥。从“密钥”页面，单击“提交密钥轮换作业”按钮。

系统将提示您上载公用密钥。此密钥将用于加密已轮换密钥的密钥第三方保管帐户。选择适当的关键字，添加密钥，然后单击“下一步”。

重要注意事项

SSL 密钥必须已进行 RSA 和 PEM 编码。

Key Rotation

This wizard will assist you in selecting keys to be scheduled for rotation. Once the keys are selected, a job to rotate the keys will be queued for approval.

Upload Public Key

Browse...

No file selected.

Add Public Key

Public Key

Next

将显示所有用户创建的密钥的列表。安全性管理员可以选择任意数量的密钥来轮换。

Key Rotation

Select one or more keys from the list of all keys:

☒ Key1

☐ Key2

☐ Key3

Back

Next

选择所需密钥后，将创建一个作业。

重要注意事项

如果密钥与多个代理程序关联，那么使用该密钥的所有代理程序将受到影响。

34 IBM Multi-Cloud Data Encryption 由 SPx® 提供技术支持： 管理员指南

在进行作业核准时，将向所有受影响的代理程序通知密钥轮换。该作业将继续运行，直至所有受影响的代理程序已完成密钥轮换流程。根据受影响代理程序的数量，此作业可能需要很长时间才能完成。

注

在使用外部密钥库时，它必须处于**联机**状态才能使密钥轮换成功。如果发生错误，请确保外部密钥库处于联机状态，然后重新引导 PPM 服务器或重新启动 PPM 服务 (spsd)。

密钥撤销

密钥撤销从 MDE 中除去密钥并将该密钥放在第三方保管帐户中。只有目前与任何活动策略都没有关联的密钥才能执行密钥撤销。在撤销密钥前，安全性管理员必须除去引用此密钥的策略。

从代理程序策略关联中除去利用密钥的路径不会解密磁盘上的数据，因此，如果需要访问数据，必须在除去与该路径关联的策略前从受保护的目录中迁移出数据。

完成撤销后，将无法访问受保护路径中剩下的任何数据。已撤销的密钥将存储在第三方保管帐户中并从正常的 PPM 操作中除去。

警告

“安全性管理员”必须更新代理程序策略以解除目标密钥与所有代理程序的关联，然后才能撤销此密钥。请参阅“编辑代理程序”部分以获取有关删除路径的更多信息。

密钥粉碎

密钥粉碎所使用的方法与密钥撤销相同；但是在完成密钥粉碎操作后，密钥将不放入第三方托管账户，从而使数据永远不可访问。

注

此功能仅可通过 REST API 提供，请参阅 REST API 文档以了解更多详细信息。

自动生成的密钥

如果安全性管理员不想管理策略实施密钥，那么 MDE 可以为每个新创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见。

重要注意事项

自动生成的密钥不能轮换或撤销。如果需要能够轮换或撤销密钥，请改为使用已命名密钥。

外部密钥库

可在以下两个位置之一存储密钥：内部安全数据库或外部密钥库。MDE 初始设置为仅使用内部安全数据库。如果安全性管理员计划利用外部密钥库，必须配置一个外部密钥库。外部密钥库只用于密钥保护。必须通过 MDE 完成外部密钥库的密钥管理。

注

用于设置外部密钥库的指示信息由外部密钥库供应商提供。

KMIP 密钥库

关于此任务

安全管理员将需要上载 Java 密钥库和 Java 信任库。遵循以下步骤来创建 Java 密钥库和 Java 信任库：

过程

1. 收集客户机证书文件和使用 PKCS12（公用密钥密码术标准 #12）格式的客户机专用密钥文件。在后面的步骤中，我们将此文件称为“client.p12”。（请参阅第 83 页的『附录 C 用于创建 PKCS12 文件的样本转换』以获取有关将客户机证书和客户机专用密钥组成 PKCS12 格式化文件的样本。）
2. 收集公用 CA 证书文件。在后面的步骤中，我们将此文件称为“sklm_ca.pem”。

```
[user@localhost]$ keytool -importkeystore -srckeystore client.p12 -keystore client.jks -storetype JKS
```

3. 将 PKCS12 文件导入到新的 Java 密钥库：

重要注意事项

此步骤中将会要求提供密码。请保留此密码以供稍后使用。

```
[user@localhost]$ keytool -v -list -keystore client.jks
```

4. 从文件中获取别名：
5. 将 CA 证书文件导入到新的 Java 信任库中：

```
[user@localhost]$ keytool -import -trustcacerts -alias sklm  
-file sklm_ca.pem -keystore sklmtrust.jks
```

重要注意事项

此步骤中将会要求提供密码。请保留此密码以供稍后使用。

6. 从文件中获取别名：

```
keytool -v -list -keystore trust.jks
```

将需要填写以激活外部密钥库的设置：

- **名称** - 用户定义的外部密钥库引用
- **状态** - 将使 MDE 了解，已定义的外部密钥库应该覆盖当前活动的密钥库。如果状态为活动，MDE 将开始使用该密钥库。如果状态为不活动，那么 MDE 将不再使用密钥库。
- **主机** - 外部密钥库的 IP 地址。
- **端口** - 外部密钥库的端口号。
- **客户机密钥库**
 - **密钥库别名** - 收集的密钥库别名。
 - **密钥库文件** - Java 密钥库文件。
 - **客户机密钥库密码** - 创建密钥库时设置的密码。
- **信任库**
 - **信任库别名** - 收集的信任库别名。
 - **信任库文件** - Java 信任库文件。
 - **信任库密码** - 创建信任库时的密码设置。
- **是否为主控** - 识别用作所有读和写操作的主密钥库的外部密钥库
 - 对于所定义的第一个密钥库，缺省值为“true”。
 - 如果未选择，那么将视为“克隆”密钥库，并将仅用于读操作。
 - 只能将一个外部密钥库指定为主密钥库。

Name	State	Host	Port	Client Keystore	Truststore	Is Master	Actions
<input type="text"/>	In: <input type="button" value="v"/>	<input type="text"/>	5696 <input type="button" value="v"/>	Alias <input type="text"/> Keystore Password <input type="password"/>	Alias <input type="text"/> Truststore Password <input type="password"/>	<input type="checkbox"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
				Keystore Upload <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/>	Truststore Upload <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/>		

注

MDE 当前支持外部密钥库产品：为 KMIP 配置的 IBM Security Key Lifecycle Manager (SKLM)。

硬件安全模块 (HSM)

关于此任务

使用 HSM 作为外部密钥库时，您将需要确保第三方产品根据制造商的指示信息完全配置并可操作。

HSM 的 64 位版本客户机软件需要由 PPM 产品管理员复制到 MDE VM。应使用 HSM 制造商的有关设置和配置通信的产品指示信息来抽取软件并随 SDK 选项一起进行安装。

使用随附客户机软件的实用程序或已证明为适用于 HSM 的实用程序来安装包装器密钥。包装器密钥是需要可供与 PPM 配合使用的 256 位对称密钥。

在 HSM 上创建此对称包装器密钥后，将会向其分配句柄。在 PPM GUI 页面中配置 HSM 时将需要此句柄。PPM 会将此句柄和策略密钥传递到 HSM 以包装策略密钥，然后 HSM 将返回要存储在 PPM 数据库中的已包装密钥。

安装和配置软件后，请确保 PPM 可以与 HSM 通信，重新引导 PPM VM。

从外部密钥库屏幕中，选择“新建 HSM 密钥库”。

[illegible]

需要填写以下设置来激活外部密钥库：

- **名称** - 用户定义的外部密钥库引用
- **状态** - 这将设置密钥库的计划状态
- **HSM 令牌** - HSM 使用分区的插槽编号
- **密钥句柄** - 这是分配给将用于包装策略密钥的密钥的句柄
- **HSM 密码** - 这是与客户将使用的分区关联的密码。

HSM Keystore

New HSM KeyStore

Name	State	HSM Token	Key Handle	HSM Password	Actions
<input type="text"/>	Inactive <div></div>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<div>SaveCancel</div>

注: 受支持的 HSM 产品：针对 HSM 密钥库配置的 SafeNet® Luna HSM。

第 10 章 文件级策略定义

MDE 使安全性管理员能够定义对各种数据类型的文件级控制（操作和加密）。以下术语在定义文件级数据控制时使用。

- **选择器** - 用户和组的无序列表，用于定义允许谁访问任何资源（或路径集）。（可选）可将已定义的过程标识为选择器的另一个组件。
- **路径集** - 策略保护的文件路径列表
- **数据类型** - 分配给指定数据类型的访问定义行的有序列表。每一行都包括一个选择器、I/O（读/写）操作和策略操作。
- **进程** - 可执行文件的文件路径。用于选择器，以与所标识的可执行文件一起定义访问控制。可选增强的访问控制。

创建数据类型后，它可以与一个或多个供应的代理程序相关联。以下部分将描述策略的配置。

选择器

选择器是通过一个或多个选择器行来定义用户和/或用户组的集合的策略对象。当添加新选择器时，安全性管理员必须在保存前提供名称。通过编辑选择器，可随时添加选择器注释和行。

每个选择器行包含以下字段：用户、组、流程。必须填充其中一个字段，然后再进行保存。

- **用户** - 目标系统定义的用户短名称。这与目标代理程序操作系统中的用户相匹配。此字段是选填字段。
- **组** - 目标系统或 LDAP 定义的用户组的短名称。这与目标代理程序操作系统中的用户组相匹配。此字段是选填字段。
- **流程** - 对产品定义的流程名称的引用。这与目标代理程序操作系统中的流程管理工具路径（和可选散列值）相匹配。此字段是选填字段。

Policy > Selectors

Expand AllCollapse All

SearchClearNew Selector

Name: Selector1

SaveCancelAdd New Row

Notes

User	Group	Process	Actions
<input type="text" value="user01"/>	<input type="text"/>	<input type="text"/>	Delete Row

使用逻辑 AND 操作组合每个选择器行中的值。如果在单行中设置多个字段，对于要匹配的行，所有字段必须匹配。如果任何已定义的行都匹配，那么选择器也匹配。选择器中的行排序不会影响策略匹配算法。

用户	组	流程	代理程序匹配行为
√			匹配用户
	√		匹配已定义的组中的任何用户
		√	匹配所定义的流程路径并可能限于所提供的任何散列值

✓	✓		仅在充当已定义的组的成员时匹配用户
✓		✓	仅在通过已定义的流程进行操作时匹配用户
	✓	✓	仅在通过已定义的流程进行操作时匹配已定义的组中的任何用户
✓	✓	✓	仅在充当已定义的组的成员并通过已定义的流程进行操作时匹配用户

注

选择器用户和/或组解决方案与安装“文件”代理程序的已配置的外部 LDAP 或 Active Directory 服务器配合使用。

路径集

路径集是一个或多个无序文件路径行的集合。当添加路径集时，安全性管理员必须提供该路径集的名称。要向路径集添加行，请单击“添加路径”按钮。每行都包含一个文件路径以及注释。

Policy > Path Sets

Expand AllCollapse All

SearchEnter TextClearNew Path Set

Name: Pathset1SaveCancelAdd Path

Notes

Path	Notes	Actions
<div>/protected</div>		<div>Delete Path</div>

安全性管理员必须提供文件路径。保护从所提供的路径向下追溯到任何子目录。注释字段是选填字段。

数据类型

数据类型是对数据启用文件级操作访问控制和/或加密访问控制的数据类型行定义的有序集合。每个数据类型都包含名称、策略实施密钥、用户注释以及有序行列表。

- 名称 - 用户定义的数据类型引用
- 用户注释 - 安全性管理员定义的注释字段。

数据类型行

- 各数据类型行都包含下列字段：顺序、选择器、操作和行为。
- 顺序 - 检查每个策略行所采用的优先级。将使用最先匹配的行。此字段是必填字段，但是如果只存在一行，将不显示。
 - 选择器 - 先前定义的选择器的选择。如果选择器中有任意行匹配，那么策略行将会匹配。此字段是必填字段。MDE 提供“全选”选择器，能够匹配任何用户。

- **操作** - 可执行的文件操作选择。选项为“读取”和“读取/写入”。此字段是必填字段。
- **行为** - 与操作相关联的访问行为选择。选项为“许可”、“拒绝”、“许可，日志”和“拒绝，日志”。此字段是必填字段。

数据类型行变量

“选择器”、“操作”和“行为”字段可以选择性地设置为可变。这样允许安全性管理员为将在代理程序创建期间完成的数据类型创建模板。可用字段设置为：“可以编辑”、“必须编辑”和“不可编辑”。

可以编辑

在创建代理程序期间，可以选择性地覆盖此字段。

必须编辑

在创建代理程序期间，必须设置此字段。

不可编辑

此字段必须在创建数据类型期间设置，在创建代理程序期间不能更改。

Create/Edit Datatype

Name

Datatype1

Notes

Rules

Order	Selector	Operation	Actions	Delete
1	<div><div>Not Editable</div><div>Selector1</div><div><input type="checkbox"/> Select All</div></div>	<div><div>Not Editable</div><div>Read or Write</div></div>	<div><div>Not Editable</div><div>Permit</div></div>	<div>Delete</div>
2	<div><div>Not Editable</div><div><input checked="" type="checkbox"/> Select All</div></div>	<div><div>Not Editable</div><div>Read or Write</div></div>	<div><div>Not Editable</div><div>Deny, Log</div></div>	<div>Delete</div>

Add New Row

Save

Cancel

在所有行都具有值和/或变量设置前，不能保存数据类型。

流程

流程识别可执行文件的文件系统路径。流程由以下字段组成：

- **名称** - 流程的名称
- **路径** - 文件系统可执行文件的绝对路径
- **操作系统** - 用于引用操作系统类型（Linux、Windows 和 AIX）的字段。
- **版本** - 用于操作系统版本的字段。
- **分发版** - 用于操作系统分发版名称（Red Hat、CentOS、Windows 和 AIX）的字段。

🏠 > Policy > Processes

Expand All Collapse All Search Clear New Process

▶ Name Save Cancel Add Hash

Path	OS	Version	Distribution
<input type="text" value="/usr/bin/cat"/>	<input type="text" value="Linux"/>	<input type="text" value="6.7"/>	<input type="text" value="CentOS"/>

Hash	Actions
------	---------

流程只能定义为文件路径，或者使用流程散列值列表进行定义。定义一个或多个散列值后，流程匹配将限于所列的散列。

注

流程散列值通过代理程序工具进行生成，并且应复制到 PPM 中。该工具将输出当前版本的可执行文件的散列值。

spxhash -p <path to executable>

示例：

```
[root@blkdr ~]# spxhash -p /usr/bin/vim
```

```
1202E81EF41273904A6DD381C35B2561F838F7E35B6B26959F8EEB646297A36A7C2
```

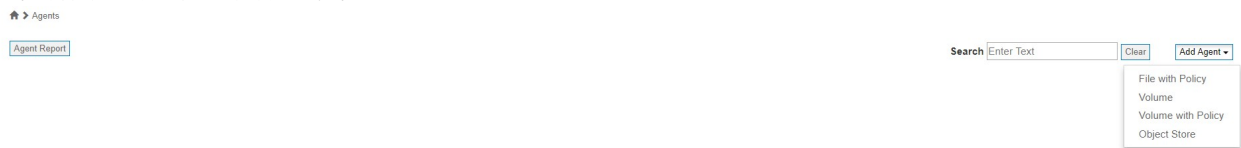

第 11 章 代理程序供应和管理

MDE 支持四种代理程序安装类型：“卷”、“具有策略的文件”、“具有策略的卷”和“对象存储”。每种代理程序类型都支持不同的数据保护方法。

- **卷** - 代理程序在块设备级别保护数据
- **具有策略的文件** - 代理程序保护文件级别的数据并提供基于文件的操作访问控制策略
- **具有策略的卷** - 代理程序在块设备级别保护数据并且还提供基于文件的操作访问控制策略
- **对象存储** - 代理程序保护发送到对象存储器的数据

添加代理程序

要添加代理程序，安全性管理员必须浏览至 MDE 的“代理程序”页面，然后单击“添加代理程序”下拉列表。将列出可用代理程序选项。



选择代理程序类型后，向导打开以使您能够创建代理程序。

注：建议在开始“添加代理程序”流程前添加所有期望的策略组件（选择器、路径集、密钥、数据类型和进程），因为在此流程期间无法创建这些组件。

供应代理程序的部分有六个：代理程序身份、网络信息、策略、卷、授权用户和工具。在添加代理程序前必须完成所有必需的部分。

身份

“身份”部分要求安全性管理员定义名称、UUID、操作系统和注释。

A screenshot of the 'Add File With Policy Agent' form. The form has a title bar with a close button. It is divided into two main sections: 'Required' and 'Optional'. Under 'Required', there are four fields: 'Name *' (text input), 'UUID *' (text input with a refresh button), 'Operating System *' (dropdown menu), and 'Notes' (text area). Under 'Optional', there are three radio buttons: 'Agent Identity' (selected), 'Network Information', and 'Policy'. At the bottom right, there is a 'Next' button.

- **名称** - 用户定义的代理程序引用。
- **UUID** - MDE 用于标识代理程序的唯一标识。
- **操作系统** - 目标代理程序的操作系统。
- **注释** - 此代理程序的安全性管理员注释。

输入所有必填字段后，单击**保存**以转至下一个步骤。

注：

- MDE 自动填充 UUID，但是在需要时安全性管理员可以对其进行替换。
- GUI 中指示了必填字段
- 代理程序的名称不唯一；因此，如果将相同的名称用于多个代理程序，那么事件日志消息传递可能误报消息源

网络

“网络”步骤要求安全性管理员定义代理程序和 MDE 的主机名或 IP 地址，以及在 MDE 和目标代理程序之间建立安全连接所需的证书。

Add File With Policy Agent

Required

✓ Agent Identity

⦿ Network Information

Optional

○ Policy

○ Authorized Users

○ Tools

* Required

IP address *

MDE Peer IP *

10.10.10.111

Certificates *

Subject	Fingerprint	Expiry	Private Key	Actions
No Certificates				
				Add Certificate

Back

Next

- **IP 地址** - 安装代理程序的服务器的 IP 地址或主机名。
- **MDE 同级 IP** - 从目标代理程序服务器实例看到的 MDE 的 IP 地址或主机名。
 注: MDE 自动填充 MDE 同级 IP，但是在需要时安全性管理员可以修改。
- **证书** - 用于在 MDE 和已安装的代理程序之间建立安全连接的已上载证书列表。此证书用于在代理程序和 MDE PPM 服务器之间建立相互认证的 TLS1.2 连接。

要上载证书，安全性管理员必须单击**添加证书**，浏览到所需证书，然后打开该证书。它将显示在“新代理程序网络”屏幕中。

注: 如果密钥库和信任库证书尚未上载到 MDE 且未向代理程序分配匹配的证书，那么代理程序和 PPM 将不进行通信，并且代理程序将不加密数据和强制实施策略。请参阅“服务器证书设置”部分以获取更多详细信息。

输入所有必填字段后，单击**下一步**以转至下一个步骤。

“具有策略的文件”、“具有策略的卷”和“卷”代理程序创建

“策略”步骤要求安全性管理员在所针对的代理程序上定义对文件路径的操作控制和加密控制。

添加路径

“具有策略的文件”和“具有策略的卷”代理程序可以向代理程序策略中添加路径定义。每个添加的路径都保护所针对的代理程序上的单个文件路径或分组的文件路径。添加的路径数目由安全性管理员定义。

重要注意事项

- 在应用策略时通过策略受保护的路径必须存在，否则策略应用将失败。
- 安装“具有策略的文件”代理程序后，必须使用可用的 **spxconvert** 命令手动处理现有文件和子目录。即使文件未加密，策略仍将生效。
- 安装后添加的新文件和目录将自动加密并通过策略受保护。

Add File With Policy Agent

Required

☒ Agent Identity
☒ Network Information

Optional

☒ Policy
☐ Authorized Users
☐ Tools

Add Path

Back
Next

要添加路径，请单击**添加路径**。

每个添加的路径都需要输入文件路径/路径集、密钥和数据类型。

Add File With Policy Agent

Required

☒ Agent Identity
☒ Network Information

Optional

☒ Policy
☐ Authorized Users
☐ Tools

* Required

File Policy Path (or Path Set) *

Delete

Storage
☒ Local
☐ Network

Key
☐ System Defined
☒ User Defined

Name

Datatype *

(remember to fill out any empty values below)

Selector	Operation	Actions
Select All	Read or Write	Permit

Add Path

Back
Next

- **文件策略路径（或路径集）** - 识别要受已识别的数据类型访问控制定义保护的路径或路径组。保护从所提供的文件路径追溯到任何子目录。
- **存储器** - 标识文件路径的位置。选项为本地或网络。如果选择“网络”，必须输入其他参数才能正确配置该网络存储器。（请参阅下面的配置信息）
- **密钥** - 用于加密与数据类型关联的路径的密钥。可以使用任何先前定义的用户定义的密钥或 MDE 管理的系统定义的密钥。此字段是否可见取决于使用的是“具有策略的文件”还是“具有策略的卷”（请参阅“注释”）。
- **数据类型** - 选择预先创建的数据类型。选定后，将以内联方式添加数据类型信息。如果使用包含变量的数据类型，那么必须在保存前输入这些变量。

注：

- 如果使用路径集，那么必须在添加新代理程序之前创建该路径集。否则，可以定义单个手动路径。
- 所使用的数据类型必须在添加新代理程序前创建。
- 如果新代理程序的类型为“具有策略的卷”，那么路径集将不包含策略实施密钥，因为通过卷策略定义来完成保护。

本地存储器配置

如果使用本地存储器，那么在定义文件策略路径时，请选择**本地存储器**选项。此操作将指示代理程序保护已定义的文件绝对路径/路径集。无需其他参数。

网络存储器配置

如果使用网络存储器，那么在定义文件策略路径时，请选择“网络存储器”选项。此操作会指示代理程序将已定义的网络存储器安装到已定义的文件绝对路径。路径集无法与网络存储器配合使用。需要使用其他参数。

网络存储器需要定义：协议、主机名/IP、共享、用户名、密码和高级安装选项。

- **协议** – 标识正在使用的网络存储器类型。选项为：NFSv4、NFSv3
- **主机名/IP** – 网络存储器系统的主机名/IP
- **共享** – 网络文件系统导出位置
- **用户名** – （NFSv3 无需使用）网络文件系统的认证用户名
- **密码** – （NFSv3 无需使用）网络文件系统的认证密码
- **高级安装选项** – 适用于 NFS 定义的选项，以逗号分隔

输入所有必填字段后，单击**下一步**以转至下一个步骤。

卷

添加卷

关于此任务

“卷”和“具有策略的卷”代理程序类型可以向代理程序策略添加一个或多个卷定义。每个添加的卷在所针对的代理程序上都是新的受保护块设备。

The screenshot shows a window titled "Add Volume With Policy Agent". On the left side, under "Required", "Agent Identity" and "Network Information" are checked. Under "Optional", "Volumes" is selected with a radio button. The main area has a "Volumes" section with a table containing "Device Label" and "Key" columns. A "Delete" button is next to the table. Below the table is an "Add Volume" button. To the right of the table is a checkbox labeled "Autogenerate Key Required". At the bottom right are "Back" and "Next" buttons.

要添加卷，请单击**添加卷**。每个添加的卷需要输入底层设备标签和策略实施密钥。

- **设备标签** - 识别受保护的设备。将策略部署到代理程序后，将需要通过运行 `spxdevice` 命令将设备标签关联到卷（请参阅“安装代理程序”部分）。
- **密钥** - 用于加密卷的密钥。可以使用任何先前定义的密钥或 MDE 管理的自动生成密钥。

重要注意事项

除非使用“自动生成密钥”选项，否则在添加代理程序之前必须定义所添加的策略实施密钥。请参阅“策略实施密钥管理”部分。

输入所有必填字段后，单击**下一步**以转至下一个步骤。

“对象存储”代理程序创建

MDE “对象存储”代理程序 (OSA) 充当客户机和后端对象存储器之间的中介。对象存储器客户机使用存储区凭证而不是后端对象存储器凭证来连接到 OSA。

管理员可配置 OSA 来连接到一个或多个对象存储提供程序。OSA 对通过 OSA 发送到已配置的后端对象存储器的数据进行加密和强制实施策略。如果配置了多个后端，那么拆分数据并将数据片发送到每个后端。

前端证书

“对象存储”代理程序要求证书配置在对象存储客户机和“对象存储”代理程序之间建立安全连接。要上载证书，安全性管理员必须单击“添加证书”按钮，浏览到所需证书，然后打开该证书。

Add Object Store Agent

Required

☒ Agent Identity

☒ Network Information

Optional

☒ **Front-End Certificates**

☐ Bucket Credentials

☐ Buckets

☐ Backends

☐ Authorized Users

☐ Tools

Front-End Certificate

Add Certificate

Subject	CN=localhost,OU=Development,O=Security First Corp.,L=Rancho Santa Margarita,ST=California,C=US
Fingerprint	e9cf021f7092bec53ec27ba29467b2d3e70b2b2e1d5ed6acd738af363860b2bd
Expiry	2016-11-09T23:11:06Z
Private Key	False

Back

Next

输入所有必填字段后，单击“下一步”以转至下一个步骤。

存储区凭证

MDE 可配置为与多个对象存储提供程序通信。每个提供程序将需要对存储区和存储区凭证进行配置。

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Front-End Certificates

⊙ Bucket Credentials

○ Buckets

○ Backends

○ Authorized Users

○ Tools

* Required

QHW1UOGRU90BFNYZQ0CH

Delete

Key ID *

QHW1UOGRU90BFNYZQ0CH

API Key *

78dKnlcLBiUkQgl6OLjtBKqNoglZw54S6g5SSiik5JX0wOvZ0xoIIZoTa=PGKK3B

Protocol *

IBM S3

XH2BW34YV12A0REPF3TW

Delete

Key ID *

XH2BW34YV12A0REPF3TW

API Key *

3AoMJ9fXv3p1xpU8xoAqfSt=DoEaX=3iY7UOyVn3ovUAQ4ssKAbQQvAv1jmHPeXh

Protocol *

AMZ S3

New Credential

Back

Next

要添加新凭证集，请单击“新建凭证”按钮。

存储区凭证需要下列定义：密钥标识、API 密钥和协议。

- **密钥标识** - 对象存储访问者的标识
- **API 密钥** - 提供给 S3 API 以关联到密钥标识的字符串密码
- **协议** - 与对象存储提供程序（Swift、IBM S3 和 Amazon S3）通信所使用的协议的标识。

MDE 将生成密钥标识和 API 密钥配对。如果需要，管理员可覆盖这些已生成的值。管理员将需要从受支持的对象存储提供程序中选择所需协议。

输入所有必填字段后，单击“下一步”以转至下一个步骤。

存储区

MDE 通过存储区关联来定义对象存储策略。每个存储区都需要下列定义：名称、记录拒绝和策略。

48 IBM Multi-Cloud Data Encryption 由 SPx® 提供技术支持：管理员指南

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

* Required

Bucket Name *

testBucket

Delete

Log Denials

☒

Policy

Key ID *	Access *	Log	Actions
XH2BW34YV12A0REPF3TW	Read or Write ▾	<input checked="" type="checkbox"/>	Delete
QHW1UOGRU90BFNYZQ0CH	Read or Write ▾	<input checked="" type="checkbox"/>	Delete

New Row

New Bucket

Optional

✓ Front-End Certificates

✓ Bucket Credentials

⊙ Buckets

○ Backends

○ Authorized Users

○ Tools

Back

Next

- **名称** - 对象存储器存储区的名称
- **记录拒绝** - 复选框选中。如果选中，“对象存储”代理程序将为访问拒绝创建审计日志。
- **策略** - 存储区访问控制的定义。策略可以包含多行。策略定义的每一行都需要：密钥标识、访问权、日志。
- **密钥标识** - 预先创建的存储区凭证密钥标识的条目。
- **访问权** - 选择以下任一访问权：读或写访问权、读访问权或写访问权。
- **日志** - 复选框选中。如果选中，“对象存储”代理程序将创建关于所提供行行为的访问许可权的审计日志。

输入所有必填字段后，单击“下一步”以转至下一个步骤。

后端

后端连接信息通过选择 **M:N** 来定义。此选择定义了对象存储数据的冗余和安全性。**N** 表示正在配置的后端对象存储提供程序的数量或“份额”。**M** 表示重构数据所需的份额的数量。受支持的配置为 **1:1**、**2:3**、**2:4**。

Add Object Store Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Front-End Certificates

✓ Bucket Credentials

✓ Buckets

⊙ Backends

○ Authorized Users

○ Tools

M:N 2:3

* Required

Share 1 *

URL *

ID *

Key *

Protocol *

IBM S3

Share 2 *

URL *

ID *

Key *

Protocol *

IBM S3

Share 3 *

URL *

ID *

Key *

Protocol *

IBM S3

Back

Next

每个份额都需要下列配置：URL、标识、密钥和协议。

- **URL** - 对象存储提供程序的访问 URL
- **标识** - 用于访问对象存储提供程序的帐户用户标识。
- **密钥** - 用于访问对象存储提供程序的用户标识帐户密钥。
- **协议** - 与对象存储提供程序（Swift、IBM S3 和 Amazon S3）通信所使用的协议的标识。

输入所有必填字段后，单击“下一步”以转至下一个步骤。

授权用户

“用户”步骤要求安全性管理员定义有权下载代理程序安装捆绑软件的 MDE 用户帐户。

如果用户未列为授权用户，并且如果该用户登录并查看代理程序，那么该用户在“代理程序信息”页面中将看不到下载链接。

Add File With Policy Agent

Required

✓ Agent Identity

✓ Network Information

Authorized Users

admin ✕

Optional

✓ Policy

☒ Authorized Users

☐ Tools

Back

Next

输入所有必填字段后，单击下一步以转至下一个步骤。

代理程序工具

代理程序支持以加密形式帮助传输数据的专用工具。有两种类型的工具：备份/复原和对象存储。

工具在代理程序供应期间或在“代理程序信息”页面上配置。备份/复原工具用于备份和复原加密的数据。它利用关联密钥来备份加密的数据，并提供在稍后的时间复原加密的数据的功能，即使已轮换策略密钥也是如此。备份/复原工具是可选的，不要求将工具关联到代理程序。对象存储工具是“对象存储”代理程序所必需的

代理程序工具矩阵

工具可用性基于代理程序类型，通过关联密钥启用。按代理程序类型分类的工具矩阵如下所示：

工具类型	卷	具有策略的卷	具有策略的文件	对象存储
备份/复原	✓	✓	✓	
对象存储				✓

工具密钥关联

要使密钥与工具关联，开始将先前定义的密钥名称输入到所需工具旁边的文本框，然后从列表中选择相应的密钥。

单击保存，将创建一个作业。核准后，将在代理程序上启用已配置的工具。

Add File With Policy Agent

Required

✓ Agent Identity

✓ Network Information

Backup/Restore

Type to filter and select a predefined key

Optional

✓ Policy

✓ Authorized Users

☒ Tools

Back

Next

注: 工具上不支持自动生成的密钥。 必须在创建代理程序之前定义密钥。

输入所有必填字段后，单击下一步以转至下一个步骤。

复审与构建

关于此任务

所有供应步骤完成后，用户将浏览至“复审”屏幕。

供应设置的复审页面将显示所有配置信息的完整视图。

Add File With Policy Agent

Agent Build Summary

Identity

Name

fileAgent

UUID

c5bf0b5a-99b2-4dcc-8e82-2a559d5319c4

Type

File with Policy

Operating System

CentOS / Red Hat 7

Notes

Network

Back

Build

复审内容的完整性和准确性，并单击**构建**来完成供应过程。将创建作业来添加代理程序。
作业经过核准后，将创建代理程序，并且安装包将可供下载和安装。

代理程序激活

核准代理程序构建作业后，新创建的代理程序在 MDE 中处于活动状态。安装代理程序后，它将使用已配置的 MDE 同级 IP 和所提供的证书来创建与 MDE 的相互认证的 TLS1.2 连接。

代理程序将在初次安装及后续启动时请求策略。MDE 将使用已配置的策略配置来响应。接收到策略后，将在代理程序上实施该策略。

查看代理程序

关于此任务

“代理程序”页面将显示已创建的代理程序的摘要列表。

Agents

Agent Report

SearchEnter TextClearAdd Agent

Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		<div>DetailsDelete Agent</div>

要参阅任何特定代理程序的详细信息，请单击“名称”列中的代理程序名称，或者单击“操作”列中的“详细信息”按钮。这将打开代理程序详细信息视图页面，其中显示供应信息、安装捆绑软件下载和其他有用信息。

代理程序报告

MDE 安全性管理员可以创建代理程序报告。此报告包含以下信息：代理程序总数、按类型和操作系统的代理程序计数以及报告生成起 30 天内登录的代理程序。日期基于 PPM 时间，即 UTC 时间。数据将按代理程序类型进行细分。

安装代理程序

关于此任务

供应步骤配置了代理程序将策略安装和部署到目标服务器实例所需的全部信息。要安装代理程序，请下载安装包，将其复制到目标系统，解压缩内容并运行设置脚本。

Agent Info

Edit Agent Info

Identity

Notes

NameAgent1

UUIDdab30682-19ee-4763-84d8-12fe2ba91948

IP Address1.1.1.1

TypeVolume with Policy

Operating SystemCentOS / Red Hat 7

Network

MDE Peer IP1.1.1.0

Certificates

Subject	Fingerprint	Expiry
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416eccc753e0f0f655462929d4f1534f369cbccc38165f	2016-11

Browse...

No file selected.

Users

Authorized Usersadmin

Install Files Download URL/rest/agents/1/install_bundle

Download Zip Bundle

Download Tar Bundle

Download Tokens

ID	State	
<div>Add Token</div>		

重要注意事项

确保所有用户、组和路径或在供应策略中识别的设备都已创建、附加和配置到系统。

安装适用于 Linux 的代理程序

存在 4 种代理程序类型：“卷”代理程序、“具有策略的文件”代理程序、“具有策略的卷”代理程序和“对象存储”代理程序。使用“代理程序供应”期间指定的“代理程序类型”。

Linux 卷代理程序设备配置

关于此任务

过程

1. 在 PPM 中创建卷（请记住第 11.1.5 节中使用的设备标签）。
2. 在代理程序 VM 上安装“gettext”软件包。
3. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
4. 在安装完成时重新引导代理程序 VM。
5. 以 root 用户身份运行 `spxdevice -e <label given in PPM> -m <mount point> -f <file system> -u <disk to use>`

```
spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

Linux “具有策略的文件”代理程序设备配置

关于此任务

过程

1. 在 PPM 中创建“具有策略的文件”代理程序
2. 创建任何所需用户
3. 创建任何需要的子目录
4. 对目录设置正确的许可权
5. 在代理程序 VM 上安装“gettext”软件包
6. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
7. 在安装完成时重新引导代理程序 VM
8. 通过命令“`spxinfo -l`”验证文件策略是否正确

注

路径旁边的星号指示存在暂挂加密的预先存在的数据。为就地对预先存在的目录结构和数据执行加密以及随时确定数据的状态，MDE 提供了一个名为“`spxconvert`”的命令行实用程序

请参阅第 87 页的『附录 E 就地加密』以获取命令及其使用的详细描述。

Linux “具有策略的卷”代理程序设备配置

关于此任务

过程

1. 在 PPM 中创建“具有策略的卷”代理程序（请记住所使用的设备标签）
2. 在代理程序 VM 上安装“gettext”软件包
3. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
4. 在安装完成时重新引导代理程序 VM
5. 以 root 用户身份运行 `spxdevice -e <label given in PPM> -m <mount point> -f <file system> -u <disk to use>`

```
[root@localhost]# spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

6. 创建任何所需的子目录和用户
7. 对目录设置正确的许可权
8. 重新引导代理程序 VM
9. `lsblk` - 用于验证磁盘是否存在，有时可能需要大约 30 秒时间
10. 通过命令“`spxinfo -l`”验证文件策略是否正确

注

在 Linux 上，可以在完整设备或分区上设置卷加密。要使用单个分区，只要在使用 `spxdevice -u` 选项时指定空分区（例如 `/dev/sdb1`）即可。

“Linux 对象存储”代理程序配置

关于此任务

过程

1. 在 PPM 中创建“对象存储”代理程序
2. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
3. 在安装完成时重新引导代理程序 VM

安装适用于 AIX 的代理程序

AIX 支持单个代理程序类型：“使用策略的文件”代理程序。使用“代理程序供应”期间指定的“代理程序类型”。

AIX “使用策略的文件”代理程序设备配置

1. 在 PPM 中创建“具有策略的文件”代理程序
2. 创建任何所需用户
3. 创建任何需要的子目录
4. 对目录设置正确的许可权
5. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
6. 在安装完成时重新引导代理程序 VM
7. 通过命令“`spxinfo -l`”验证文件策略是否正确

注：路径旁边的星号指示存在暂挂加密的预先存在的数据。为就地对预先存在的目录结构和数据执行加密以及随时确定数据的状态，MDE 提供了一个名为“`spxconvert`”的命令行实用程序

请参阅第 87 页的『附录 E 就地加密』以获取命令及其使用的详细描述。

安装适用于 Windows 的代理程序

存在 3 种代理程序类型：“卷”代理程序、“具有策略的文件”代理程序和“具有策略的卷”代理程序。使用“代理程序供应”期间指定的“代理程序类型”。

Windows 卷代理程序设备配置

关于此任务

过程

1. 在 PPM 中创建卷（请记住所使用的设备标签）。
2. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
3. 在安装完成时重新引导代理程序 VM
4. 运行“`spxdevice -e <label given at PPM> -d <disk number to use>`”以附加到整个磁盘。必须以管理员身份运行。

```
spxdevice -e PRODISK -d 1
```

5. 或者，运行 `spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system>` 以附加到将使用盘符进行格式化和安装整个磁盘。

```
spxdevice -e PRODISK -d 1 -m E -f NTFS
```

6. 或者，运行 “spxdevice -i <disk number to use>” 以编译打包要附加到特定分区的磁盘

```
spxdevice -i 1
```

7. 接下来，运行 “spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>” 以附加到特定分区并格式化文件系统的该分区

```
spxdevice -e PRODISK -v E -f NTFS
```

注: 在 Windows 上，可以在完整设备或分区上设置卷加密。

- 对于全磁盘加密，磁盘必须联机并已初始化，而磁盘空间不得格式化。盘符必须可用。
- 对于分区加密，必须在干净磁盘上通过 “spxdevice -i <disk number>” 创建备份设备。然后，必须创建具有盘符的原始分区。

请参阅 “spxdevice” 命令中的帮助以获取更多选项。

Windows “具有策略的文件” 代理程序设备配置

关于此任务

过程

1. 在 PPM 中创建 “具有策略的文件” 代理程序
2. 创建任何所需用户
3. 创建任何需要的子目录
4. 对目录设置正确的许可权
5. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
6. 通过命令 `spxinfo -l` 验证文件策略是否正确

注

路径旁边的星号指示存在暂挂加密的预先存在的数据。为就地对预先存在的目录结构和数据执行加密以及随时确定数据的状态，MDE 提供了一个名为 “spxconvert” 的命令行实用程序

请参阅第 87 页的『附录 E 就地加密』以获取命令及其使用的详细描述。

注

在 Windows 上，确保允许管理用户通过策略创建目标目录，因为在检索到策略后该策略即生效。

Windows “具有策略的卷” 代理程序设备配置

关于此任务

过程

1. 在 PPM 中创建 “具有策略的卷” 代理程序（请记住所使用的设备标签）
2. 安装代理程序 - 请参阅第 75 页的『附录 A 样本代理程序安装过程』以获取详细信息
3. 在安装完成时重新引导代理程序 VM
4. 运行 “spxdevice -e <label given at PPM> -d <disk number to use>” 以附加到整个磁盘。必须以管理员身份运行。

```
PS C:\> spxdevice -e PRODISK -d 1
```

5. 或者，运行 “spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system>” 以附加到将使用盘符进行格式化和安装的整个磁盘

```
PS C:\> spxdevice -e PRODISK -d 1 -m E -f NTFS
```

6. 或者，运行 “spxdevice -i <disk number to use>” 以编译打包要附加到特定分区的磁盘。

PS C:\> spxdevice -i 1

7. 接下来，运行 “spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>” 以附加到特定分区并格式化具有文件系统的分区。

PS C:\> spxdevice -e PRODISK -v E -f NTFS

注

在 Windows 上，可以在完整设备或分区上设置卷加密。

- 对于全磁盘加密，磁盘必须联机并已初始化，而磁盘空间不得格式化。盘符必须可用。
- 对于分区加密，必须在干净磁盘上通过 “spxdevice -i <disk number>” 创建备份设备。然后，必须创建具有盘符的原始分区。

请参阅 “spxdevice” 命令中的帮助以获取更多选项。

8. 将受保护的目录添加到卷
9. 重新启动计算机
10. spxinfo -l (应显示所有受保护目录的列表)

注

在 Windows 上，确保允许管理用户通过策略创建目标目录，因为在卷附加并可用后该策略即生效。

活动策略

每个代理程序都只能拥有一个活动策略。代理程序不会持久存储其策略。每次代理程序重新引导时，该代理程序都向 MDE 请求当前处于活动状态的策略。如果代理程序无法访问 MDE，那么缺省拒绝访问权将应用于代理程序上的所有受保护目录。

向代理程序发送新策略时，代理程序将在成功（或未成功）应用策略时向 MDE 发送事件。如果仍存在策略激活问题，请参阅以下位置中的 kernel_policy.log 文件：

- Linux/AIX: /var/log/spxagent/spx-policyagent
- Windows: C:\Windows\spxagent\PolicyAgent

编辑代理程序

在成功供应并核准代理程序后，必须通过 GUI 在“代理程序信息”页面上编辑该代理程序来执行对该代理程序的任何更改。要编辑代理程序，请查看代理程序详细信息。在“代理程序信息”页面上，代理程序的各个部分可以独立编辑。

编辑代理程序信息

单击“编辑代理程序信息”按钮将允许修改一些代理程序信息：名称、IP 地址、MDE 同级 IP 和注释。

Agent Info

[Edit Agent Info](#)

Identity

Notes

Name Agent1
UUID dab30682-19ee-4763-84d8-12fe2ba91948
IP Address 10.6.1.255
Type Volume with Policy
Operating System CentOS / Red Hat 7

Network

MDE Peer IP 10.6.1.105

Certificates

Subject	Fingerprint	Expir
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416ecc753e0f0f655462929d4f1534f369cbccc38165f	2016-

[Browse...](#) No file selected.

对 MDE 同级 IP 的更改将在 MDE 中立即实现，但是如果代理程序已安装，那么必须创建和安装新的安装包才能使更改生效。

注

UUID、操作系统和代理程序类型在初次供应后不可编辑。

添加/删除证书

通过在“代理程序信息”页面的证书部分中单击相应按钮，可添加和删除代理程序证书。

Network

MDE Peer IP 1.1.1.0

Certificates

Subject	Fingerprint	Expiry	
CN=agent,OU=agent,O=SFC,L=RSM,ST=California,C=US	ea584e4904fffa45a3416ecc753e0f0f655462929d4f1534f369cbccc38165f	2016-11-15T14:32:08Z	Delete Certificate

[Browse...](#) No file selected.

[Add Certificate](#)

要更新代理程序证书，请执行下列步骤：

- 为代理程序生成新证书
- 通过管理控制台将新证书上传到 PPM
 - 从“代理程序”页面，单击要更新的代理程序以显示“代理程序信息”页面
 - 单击“添加证书”按钮，选择新证书文件并单击“确定”按钮
 - 应该显示新证书
- 删除旧证书
 - 从“代理程序”页面，单击要更新的代理程序以显示“代理程序信息”页面
 - 确定要删除的证书
 - 单击“删除证书”按钮，将创建一个作业
 - 单击“关闭”按钮

- e. 从“作业”页面，在所需作业上单击“核准”按钮
- 4. 验证是否已从代理程序中删除证书
 - a. 从“代理程序”页面，单击要更新的代理程序以显示“代理程序信息”页面
 - b. 验证是否还有正确的证书

如果代理程序已安装，那么必须创建和安装新的安装包才能使证书更改生效。

代理程序工具

在“代理程序信息”页面上可添加在代理程序供应期间未配置的工具。此外，还可以修改已配置的工具。

关联密钥

要关联密钥，请将密钥名称输入到工具旁边的文本框中，然后从列表中选择该密钥。单击“保存”，将创建一个作业。核准后，将在代理程序上启用已配置的工具。

Add File With Policy Agent

Required

✓ Agent Identity

✓ Network Information

Optional

✓ Policy

✓ Authorized Users

⊙ Tools

Backup/Restore

Type to filter and select a predefined key

Back

Next

修改密钥

要修改密钥，请单击“编辑”按钮并将密钥名称输入到工具旁边的文本框中，然后从列表中选择该密钥。单击“保存”，将创建一个作业。核准后，将在代理程序上启用已配置的工具。

Tools

Backup/Restore

User Defined Key

Save

Cancel

SU 数据访问

应用策略访问控件时，缺省设置是拒绝 SU 数据访问。可能存在允许 SU 数据访问的情况。如果存在，“代理程序信息”页面上将有一个复选框，允许修改设置。

Other Configuration

☒ Block access when su user substitution is in use

切换该复选框将创建一个作业。核准后，SU 数据访问设置将相应地更改。

下表显示了 SU 数据访问控件：

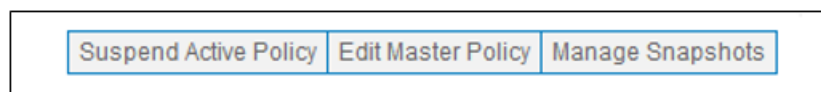
代理程序类型	操作系统	SU 数据访问缺省值	SU 数据访问可配置
卷	CentOS6/RedHat6	不适用	不适用
卷	CentOS7/RedHat7	不适用	不适用

卷	Windows	不适用	不适用
具有策略的卷	CentOS6/RedHat6	已阻止	是
具有策略的卷	CentOS7/RedHat7	已阻止	是
具有策略的卷	Windows	不适用	不适用
具有策略的文件	CentOS6/RedHat6	已阻止	是
具有策略的文件	CentOS7/RedHat7	已阻止	是
具有策略的文件	AIX	已阻止	是
具有策略的文件	Windows	不适用	不适用
对象存储	CentOS7/RedHat7	不适用	不适用

策略暂挂

“具有策略的卷”和“具有策略的文件”代理程序支持用于暂挂已定义的活动策略的功能。暂挂策略后，将拒绝针对受保护目录的所有操作。暂挂活动策略可在不更改活动快照定义的情况下完成。

要暂挂策略，请在“代理程序信息”策略部分的右侧角落中单击“暂挂活动策略”按钮，它将创建一个作业。



核准作业后，将立即暂挂策略，该按钮将切换并显示“重新启用活动策略”。

要重新启用暂挂的策略，请单击“重新启用活动策略”按钮，将创建一个作业。核准作业后，最后一个活动快照策略将立即生效。

策略更改

可以通过修改应用于受保护路径的策略、添加新的受保护路径或添加加密卷来进行策略更改。

对策略的更改不会修改当前数据的加密状态。它们将只影响在重新部署策略后创建的数据的处理。

重要注意事项

请不要从活动的代理程序中删除卷策略。此操作不受支持并可能导致目标系统处于非恒定状态。
您可以在活动的代理程序上创建新卷以及将旧卷保留不用。
或者，可以创建并部署新代理程序。

编辑策略

编辑代理程序的策略将允许修改文件策略路径、路径集和数据类型的关联或已加密的卷。

如果数据类型更改为可编辑的类型，那么这些字段的内联编辑将可用。要编辑该策略，请单击“编辑主策略”按钮。

Active Policy

Edit Master Policy Manage Snapshots

File Policy Path Pathset1

Datatype Datatype1

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Protected Volumes

Volume Policy Path

Device Label volume

Key Key1

图 1. “具有策略的卷” 代理程序示例

这将启动 “编辑主策略” 页面。

Edit Master Policy

File Policy Path (or Path Set) Pathset1

☐ Autogenerate Key

Datatype Datatype1

(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label volume

Key Key1 ☐ Autogenerate Key

Add Volume Add Path

Save Save and Snapshot Save, Snapshot and Activate Cancel

注

编辑 “主策略” 不会修改任何快照。

添加路径

关于此任务

要添加将放在策略下的新路径，请单击“添加路径”按钮。

Edit Master Policy

File Policy Path (or Path Set)

Pathset1

☐ Autogenerate Key

Datatype

Datatype1

(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label

volume

Key

Key1

☐ Autogenerate Key

Add Volume

Add Path

将打开一个新部分用于输入策略（类似于原始供应）。

File Policy Path (or Path Set)

Type policy path or select a predefined path s

Required

Delete

☐ Autogenerate Key

Datatype

Type to filter and select a predefined datatype

Required

(remember to fill out any empty values below)

Selector	Operation	Actions
----------	-----------	---------

Add Volume

Add Path

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

添加卷

关于此任务

要添加需要加密的新卷，请单击“添加卷”按钮。

Edit Master Policy

File Policy Path (or Path Set) **Pathset1**

☐ Autogenerate Key

Datatype


(remember to fill out any empty values below)

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

Volume Policy Path

Device Label

Key ☐ Autogenerate Key



将打开一个新部分用于输入（类似于原始供应）。

Volume Policy Path

Device Label **Required**

Key ☐ Autogenerate Key **Required**

删除路径

关于此任务

要从策略保护中删除路径，请针对预期路径单击“删除”按钮。一旦对策略配置进行了保存、创建快照和激活，该路径就将不再受访问控制策略的保护。写入到目录中的新文件将不再加密。现有文件将保持处于已加密状态并将不可访问。

注：要确保对数据的不间断访问，请在从策略中删除路径前从受保护的目录路径中复制/移动数据。

Edit Master Policy

File Policy Path (or Path Set)

Pathset1

Delete

☐ Autogenerate Key

Datatype

Datatype1

(remember to fill out any empty values below)

Selector	Operation	Actions
selector1	Read or Write	Permit

Volume Policy Path

Device Label

volume

Key

Key01

☐ Autogenerate Key

Add Volume

Add Path

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

代理程序快照

代理程序快照是代理程序相关策略配置的永久存储。快照已建立索引并且状态为“活动”或“不活动”。每个代理程序都只有一个活动快照。这是目前应用于代理程序的策略配置。要修改代理程序策略配置，管理员必须创建反映所需更改的新快照并激活该新快照。

保存代理程序编辑和快照

完成代理程序策略编辑后，您可以取消更改，保存更改，对更改进行保存和创建快照，或对更改进行保存、创建快照和激活。

Save

Save and Snapshot

Save, Snapshot and Activate

Cancel

取消更改

取消更改将还原为修改之前存在的策略配置。

保存更改

保存更改将存储更改以供将来使用，但是不会创建快照，因此这些更改无法应用于代理程序。

保存和创建快照

对更改进行保存和创建快照将存储更改以供将来使用，并创建可在以后查看和激活的快照。

保存、创建快照并激活

对更改进行保存、创建快照和激活将存储更改以供将来使用，创建可查看的快照，并立即创建将这些更改应用于代理程序的作业。

注：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。在 PPM 与代理程序之间成功通信或从 PPM 服务器中除去代理程序前，已创建的作业将保持运行。

管理快照

与代理程序关联的所有快照都可以通过“代理程序信息”视图上的“管理快照”按钮进行查看。

Active Policy

Edit Master PolicyManage Snapshots

File Policy PathPathset1

DatatypeDatatype1

Selector	Operation	Actions
Selector1	Read or Write	Permit
Select All	Read or Write	Deny, Log

单击此按钮将打开快照管理对话框。从此对话框中，安全性管理员可以查看快照详细信息，激活快照，取消激活与快照关联的策略，以及删除快照。

Agent Snapshots

ID	State	Actions
1	Inactive	ActivateDeleteView Details
2	Active	Deactivate PolicyView Details

OK

注

更改活动快照不会修改“主策略”。

查看详细信息

单击此按钮将显示与快照关联的策略的摘要视图。

Agent Snapshots

Snapshot Detail

Notes

Protection Policy

File Policy Path/protected2

DatatypeDatatype1

Selector	Operation	Key	Actions
----------	-----------	-----	---------

Back

OK

激活快照

激活快照将创建向代理程序发送策略的作业。核准后，快照将进入活动状态，并且其策略将覆盖代理程序上存在的任何策略。

注: 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。在 PPM 与代理程序之间成功通信或从 PPM 服务器中除去代理程序前，已创建的作业将保持运行。

删除快照

可以删除不活动的快照。删除快照会将其从 MDE 中永久除去。

卸载文件代理程序

关于此任务

如果希望移除文件代理程序，那么可以通过以下步骤来实现此操作：

从受保护目录中复制出数据。这将确保在取消激活策略后数据并非不可访问。

执行以下步骤来移除代理程序软件：

过程

1. Linux - 以 root 用户身份运行

a) 停止 spx-policyagent 服务

· 使用 CentOS 7 运行

```
systemctl stop spx-policyagent
```

· 使用 CentOS 6 运行

```
service spx-policyagent stop
```

b) 运行 `cd /opt/ibm/mde/spxagent/spx-fileagent/`。

c) 运行 `./fileagent_uninstall.sh`。

d) 输入 y 以确认破坏性操作。

e) 重新引导。

2. AIX - 以 root 用户身份运行

a) 停止 spx-policyagent 服务。

```
stopsrc -s spx-policyagent
```

b) 停止内核模块。

```
/opt/ibm/mde/spxagent/spx-fileagent/module/spx_kctrl_stop
```

c) 除去 RPM。

```
rpm -e fileagent*
```

注: 如果您需要准确的 rpm 名称而不是通配符运行，请使用

```
rpm -qa | grep fileagent
```

d) 重新引导。

3. Windows - 以管理员身份运行

· 通过 Windows GUI

- 浏览至控制面板中的“添加/删除程序”
- 选择“FileAgent”以进行卸载
- 提示时重新引导系统
- 通过 PowerShell CLI
 - msixexec /x <path to FileAgent.msi>
 - 提示时重新引导系统

要点: 授权用户不应使用 mv（移动）命令将数据移入/移出加密位置，因为这可能会导致 MDE 策略发生问题。

使用 cp（复制）命令先将数据备份到受保护（已加密）目录或从该目录中备份数据。

卸载卷代理程序

卸载“卷”代理程序

- Linux - 以 root 用户身份运行。

1. 卸载受保护的卷

```
umount /dev/mapper/<e_volume>
```

2. 停止 spx-policyagent 服务

- 使用 CentOS 7 运行

```
systemctl stop spx-policyagent
```

- 使用 CentOS 6 运行

```
service spx-policyagent stop
```

3. 运行 cd /opt/ibm/mde/spxagent/spx-volumeagent/。

4. 运行 ./volumeagent_uninstall.sh。

5. 输入 y 以确认破坏性操作。

6. 重新引导

- Windows - 以管理员身份运行

- 通过 Windows GUI

- 浏览至控制面板中的“添加/删除程序”
- 选择“VolumeAgent”以进行卸载
- 提示时重新引导系统

- 通过 PowerShell CLI

- msixexec/x <path to VolumeAgent.msi>
- 提示时重新引导系统

卸载“具有策略的卷”代理程序

关于此任务

过程

1. Linux - 以 root 用户身份运行

a) 卸载受保护目录

```
umount /dev/mapper/<e_volume>
```

b) 停止 spx-policyagent 服务

- 使用 CentOS 7 运行

```
systemctl stop spx-policyagent
```

- 使用 CentOS 6 运行

```
service spx-policyagent stop
```

c) 运行 `cd /opt/ibm/mde/spxagent/spx-hybridagent/`。

d) 运行 `./hybridagent_uninstall.sh`。

e) 输入 y 以确认破坏性操作。

f) 重新引导。

2. Windows - 以管理员身份运行

- 通过 Windows GUI

- 浏览至控制面板中的“添加/除去程序”。
- 选择“HybridAgent”以进行卸载。
- 在提示时重新引导系统。

- 通过 PowerShell CLI

- 运行 `msiexec /x <path to HybridAgent/msi>`。
- 在提示时重新引导系统。

卸载“对象存储”代理程序

关于此任务

所有用户帐户和许可权将继续存储在 PPM 中，直到从 PPM 中删除该代理程序。

过程

1. Linux - 以 root 用户身份运行

2. 停止 spx-policyagent 服务

```
systemctl stop spx
```

3. `cd /opt/ibm/mde/spxagent/spx-objectagent`

```
./objectagent_uninstall.sh
```

4. 输入 y 以确认破坏性操作

5. 重新引导。

从 MDE 中除去代理程序

可以使用 MDE 用户界面 (GUI) 从生态系统中除去受 MDE 管理的代理程序。

要除去代理程序，请单击“删除代理程序”按钮，将创建一个作业。作业经核准后，代理程序将从 MDE 中除去。

Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		Details Delete Agent

重要注意事项

- 从 MDE 中除去代理程序将使该代理程序无法连接到 MDE，从而导致目前受保护的数据在下次重新启动代理程序时变得不可访问。
- 除去代理程序不会解密数据。

代理程序实用程序

MDE 代理程序提供多个实用程序来帮助配置代理程序和保护敏感信息。有关每个实用程序的更多详细信息，请使用 “--help” 选项运行实用程序。

实用程序	功能	卷	具有策略的卷	具有策略的文件	对象存储
spxbackup	创建已识别数据的加密备份。	是	是	是	否
spxconvert	基于已定义的策略将受保护目录中预先已存在的数据从未加密转换为已加密。	否	否	是	否
spxdevice	将磁盘卷/分区映射到已定义的设备名。	是	是	否	否
spxhash	生成所指示流程的特定于版本的散列。	否	是	是	否
spximport	将已加密的数据导入到目录，而不是对数据进行双重加密。	否	否	是 (仅限 Windows)	否
spxinfo	列出通过已定义的策略保护的目录	否	是	是	否
spxobject	列出对象存储	否	否	否	是
spxrestore	复原已识别数据的加密备份。	是	是	是	否

第 12 章 操作

产品数据备份与复原

MDE 支持执行 MDE PPM 数据时间点备份的功能。此时间点备份可以复原，以使 MDE 恢复为备份收集时的状态。

注: 在执行备份或复原前，请通过 MDE VM 中的 “systemctl stop spsd” 命令停止 MDE 服务。

```
sudo systemctl stop spsd
```

产品数据备份

关于此任务

产品备份通过在 MDE VM 中运行的命令行脚本完成。

备份脚本 spsd-backup 位于 MDE VM 中的 /opt/securityfirst/spsd/bin 目录中。它将自动创建新文件，并在进行了此备份时使用时间戳记对其命名。

```
sudo /opt/securityfirst/spsd/bin/spsd-backup --help
Usage: spsd-backup [--nodb] [--help]
-----
--nodb      Don't backup the database
--help      Show this help
```

要运行备份：

```
sudo /opt/securityfirst/spsd/bin/spsd-backup
Dumping local buildinfo
Dumping local spsd properties
Dumping local PostgreSQL database a
Done - created spsd-backup-2017-04-04T144448-0700.tar.gz
```

产品数据复原

关于此任务

产品复原通过在 MDE VM 中运行的命令行脚本完成。

复原脚本 spsd-restore 位于 /opt/securityfirst/spsd/bin 目录中。

```
sudo /opt/securityfirst/spsd/bin/spsd-restore --help
Usage: spsd-restore [--nodb] [--noprops] [--help] FILE
-----
--nodb      Don't write the database
--noprops   Don't write local properties
--help      Show this help
```

要运行复原：

```
sudo /opt/securityfirst/spsd/bin/spsd-restore
spsd-backup-2017-04-04T144448-0700.tar.gz
```

注: 复原备份文件后，下次启动 MDE 将应用更改。

内核更新

关于此任务

在 Red Hat Enterprise Linux 7 或 CentOS 7 操作系统上运行的代理程序上需要内核更新时，请使用下列准则：

- 如果操作系统/内核更新在同一发行版内，自动支持新内核。
- 如果操作系统/内核升级到更高的发行版（即 RHEL 7.2 -> 7.4），那么运行下列步骤以构建对新内核的支持：
 - 例如：代理程序安装捆绑软件解压缩到 /root/agent

```
cd /root/agent/spx-installer
./agent_setup.sh -d /root/agent
Reboot
```

在 Red Hat Enterprise Linux 6 或 CentOS 6 上运行的代理程序不需要这些步骤。

升级

遵循以下步骤以将 MDE 产品升级至新版本。

注：这些步骤适用于 MDE 开放式虚拟设备。如果执行了非 OVA 安装，那么目录可能会更改。

对于 MDE 服务器

关于此任务

过程

1. 以 root 用户身份停止 PPM 策略服务。

```
systemctl stop spsd
```

2. 备份 MDE 数据：

```
/opt/securityfirst/spsd/bin/spsd-backup
```

3. 将新版本 MDE bin 文件移至 /home/admin 目录。
4. 删除现有的 rpms 目录。

```
rm -fr /home/admin/rpms
```

5. 更改对 MDE bin 文件的访问许可权。

```
chmod +x /home/admin/ibm_sw_mde_X.x.x-XX.bin
```

6. 运行新版本的 MDE bin 文件。

```
/home/admin/ibm_sw_mde_X.x.x-XX.bin
```

7. 安装 RPM。

```
yum -y install /home/admin/rpms/*
```

8. 运行升级脚本。

```
/opt/securityfirst/spsd/bin/spsd-pgsetup --upgrade
```

9. 再次启动 PPM 策略服务备份：

```
systemctl start spsd
```

从先前版本升级

关于此任务

必须执行下列步骤以允许策略运行！

过程

1. 浏览至“代理程序信息”页面
2. 单击“编辑主策略”
3. 单击“保存、快照和激活”
4. 核准作业
5. 返回到代理程序 VM 并尝试对策略中的目录执行读/写操作（以策略中对该目录具有权限的用户身份登录），然后验证是否不允许非定义用户。

用于代理程序目标 VM

Linux/AIX 代理程序

关于此任务

过程

1. 创建新代理程序目录并切换到新代理程序目录

```
mkdir [agent_new_directory]  
cd [agent_new_directory]
```

2. 下载或使用 curl 命令获取各个代理程序的安装捆绑软件

```
curl --header "Accept: application/x-tar" -u  
username:password  
https://<PPM IP address>/rest/agents/Agent ID #/install_bundle> install_bundle_name.tar
```

3. 解压缩安装捆绑软件

```
tar xvf <install_bundle_name>.tar
```

4. 运行 setup.sh 脚本以重新安装代理程序

```
./setup.sh
```

5. 提示时，回答是以重新引导代理程序。
6. 如果需要，可以从先前代理程序目录中删除所有先前安装程序文件。

```
rm -rf [/previous Agent directory]
```

Windows 代理程序

关于此任务

过程

1. 下载各个代理程序的安装捆绑软件
2. 解压缩安装捆绑软件

3. 运行 .msi 安装程序以安装新代理程序软件
4. 提示时，回答“是”以重新引导代理程序

服务数据

收集服务数据

服务数据收集通过在 MDE VM 中运行的脚本完成。

spsd-service 脚本位于 MDE VM 中的 /opt/securityfirst/spsd/bin 目录中。

```
sudo /opt/securityfirst/spsd/bin/spsd-service --help
Usage: spsd-service [OPTIONS]
-----
OPTIONS:
  --nodb          Don't dump the database
  --norest        Don't pull any data from the REST API
  --nosys         Don't pull system data (/var/log, /proc, and so on)
  --withcore      Pull in a core dump of spsd
  --help          Show this help
```

要运行服务数据收集：

```
sudo /opt/securityfirst/spsd/bin/spsd-service
```

从 PPM 日志中除去敏感信息

为在服务数据离开 PPM 逻辑边界时帮助保护 PPM 安装的隐私，以下 MDE 调试日志使用专用标记语法来标记敏感信息：

- bundleAll.log
- bundleWarnPlus.log
- debug.log
- warn.log

注：在服务数据 tarball（上述服务数据收集过程的结果）内，可在日志文件夹中找到这些日志。

标记的格式为 #<tagname>(<tagdata>)，其中 <tagdata> 被替换为要标记的数据，<tagname> 是下列其中一项：

- user - 用于标记用户名，不论是 MDE 用户，还是与 MDE 集成的外部服务的用户。例如：#user(admin)
- group - 用于标记组名。例如：#group(domainusers)
- email - 用于标记电子邮件地址。例如：#email(example@example.com)
- ip - 用于标记 IP 地址。例如：#ip(192.168.0.5)
- host - 用于标记网络主机名。例如：#host(dns.example.com)
- key - 用于标记公用密钥或相关值（如受管密钥名称）。例如：#key(HRKey2)
- cert - 用于标记证书数据（如连接代理程序的专有名称）。例如：#cert(C=US, ST=UT, L=Provo, O=Example Corp., OU=architecture, CN=docserver4)
- fingerprint - 用于标记证书指纹。例如：
#fingerprint(41:1A:B9:89:DB:77:90:77:39:D0:DF:5E:98:90:B7:17)

通过使用诸如此示例中从 bundleAll.log 中除去 #user 标记数据的过程，可从服务数据中除去标记：

```
gunzip spsd-service-2018-01-24T141620-0800.tar.gz
tar xf spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
sed -i '/\#user/c\REDACTED' logs/bundleAll.log
tar --delete --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
tar --append --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
gzip spsd-service-2018-01-24T141620-0800.tar
```


附录 A 样本代理程序安装过程

以下部分概述了代理程序安装捆绑软件的一般安装过程。这些只是示例方法，并非受支持的安装指示信息。

Red Hat/CentOS 流程

关于此任务

通过 **curl** 传输安装捆绑软件：

过程

1. 登录目标系统
2. 确保与 MDE 服务器的有效网络连接
3. 确保所有用户、组和路径或在策略中标识的设备都已创建、连接和配置到系统
4. 登录 MDE
5. 在 MDE 中，为目标系统供应代理程序
6. 在 MDE 中，查看代理程序详细信息并记录下载 URL

Users

Authorized Users admin

Install Files Download URL /rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. 从目标系统中，创建代理程序下载目录并切换到该目录
8. 使用以下 **curl** 命令下载 tar 捆绑软件：

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin https://<PPM IP>/<Download URL> > package.tar
```

使用 PPM 定义的用户示例：

```
[user@localhost]$ curl -k --header "Accept: application/x-tar" -u admin:admin-password https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

使用 PPM LDAP 定义的用户示例：

```
[user@localhost]$ curl -k --header "X-Directory: tenant1" --header "Accept: application/x-tar" -u john:secret https://1.1.1.10/rest/agents/1/install_bundle > package.tar
```

（假设目录标识为“tenant1”，用户为“john”，密码为“secret”）

9. 从目标系统将软件包解压缩：

```
[user@localhost]$ tar -xf package.tar
```

10. 从目标系统，以 root 用户身份运行设置脚本

```
[user@localhost]$ ./setup.sh
```

11. 在设置脚本完成后，将安装代理程序，策略将从 MDE 下载并会生效。

AIX 流程

关于此任务

传输安装捆绑软件：

1. 登录目标系统
2. 确保与 MDE 服务器的有效网络连接
3. 确保所有用户、组和路径或在策略中标识的设备都已创建、连接和配置到系统
4. 登录 MDE
5. 在 MDE 中，为目标系统供应代理程序
6. 在 MDE 中，查看代理程序详细信息并记录下载 URL

Users

Authorized Users admin

Install Files Download URL/rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. 从目标系统中，创建代理程序下载目录并切换到该目录
8. 将捆绑软件传输到目标系统。
9. 从目标系统将软件包解压缩：

```
[user@localhost]$ tar -xvf package.tar
```

10. 以 root 用户身份运行目标系统中的设置脚本。

```
[user@localhost]$ ./setup.sh
```

11. 在设置脚本完成后，将安装代理程序，策略将从 MDE 下载并会生效。

Windows 服务器进程

关于此任务

传输安装捆绑软件：

过程

1. 登录目标系统
2. 确保与 MDE 服务器的有效网络连接
3. 确保所有用户、组和路径或在策略中标识的设备都已创建、连接和配置到系统
4. 登录 MDE
5. 在 MDE 中，为目标系统供应代理程序
6. 在 MDE 中，查看代理程序详细信息并记录下载 URL

Users

Authorized Users admin

Install Files Download URL /rest/agents/1/install_bundle

[Download Zip Bundle](#)

[Download Tar Bundle](#)

7. 单击“下载 Zip 捆绑软件”以将代理程序软件的 zip 文件捆绑软件下载到本地系统
8. 将安装捆绑软件传输到目标系统
9. 在目标系统上，抽取 zip 文件捆绑软件的内容
10. 执行安装捆绑软件的 msi 文件

FileAgent-<version>.msi

示例：

PS C:\> FileAgent-4.2.11-0030.msi

11. 完成设置脚本并正确安装代理程序后，策略将生效。

注：需要重新引导。要绕过所请求的重新引导提示，您可以运行包含不重新引导选项的命令：
msiexec /i <agent_filename_version.msi> NO_REBOOT_PROMPT=1

附录 B 样本认证中心 (CA) 证书

关于此任务

MDE 需要由认证中心签署的证书在管理服务器 (PPM) 和代理程序之前建立安全会话。它将需要：

- 密钥库
- 信任库
- CA 证书捆绑软件

可以使用内部公司的基于 RSA 的认证中心或第三方认证中心来签署证书。在下面的 Linux 示例中，创建了以下项目：

- 创建证书签名请求 (CSR) 并发送到认证中心以进行签署。组合签名证书和密钥以创建密钥库。
- 使用认证中心的证书捆绑软件创建信任库。
- 创建代理程序证书。需要这些证书才能在 PPM 和代理程序之间进行通信。

提供此示例旨在为您方便起见，您在生成要签署的证书时应依附于认证中心。方括号 [name.pem] 内的名称表示在使用公司或第三方证书时可能不同或已更改的文件名。

要创建密钥库，您将需要向内部公司认证中心或第三方认证中心提交 CSR。

过程

1. 创建包含以下信息的 OpenSSL 配置文件（即 ppm.cnf）：

```
[req]
default_bits          = 4096
distinguished_name    = req_distinguished_name
req_extensions        = v3_req
prompt                = no

[req_distinguished_name]
C      = your_country
ST     = your_state_or_province
L      = your_locale_(city)
O      = your_organization
OU     = your_org_unit_(department)
CN     = your_ppm_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints      = CA:FALSE
extendedKeyUsage      = serverAuth
subjectAltName        = @alt_names

[alt_names]
DNS.1    = your_ppm_host.your_domain
IP.1     = your_ppm_ip_address
```

您需要更新 [req_distinguished_name] 和 [alt_names] 部分以反映组织的信息。

2. 创建 PPM CSR

```
openssl req -out [csr.pem] -new -newkey rsa:2048 -keyout [key.pem] -outform pem
```

3. CSR [csr.pem] 必须由 Certificate Authority (CA) 签署
4. 接收来自 CA 的签名证书后，验证扩展密钥用法和主体备用名称是否存在

```
openssl x509 -in [signed cert] -noout -text
```

5. 组合签名证书和密钥（来自第 2 步的密钥）

```
a.    openssl pkcs12 -export -out [ppm.p12] -inkey [key.pem] -in [signed-cert] -name ppm
```

```
b. keytool -importkeystore -srckeystore [ppm.p12] -keystore [ppm.jks] -storetype JKS
```

要创建信任库，您将需要认证中心的用于签署 CSR 的证书。这也称为 CA 证书捆绑软件。将下面的“ca_bundle.crt”替换为此证书的实际名称。

- a. 使用认证中心 (CA) 证书捆绑包创建信任库。如果 CA 证书捆绑包中有多个证书，必须将它们分开并分别导入到信任库。

```
a. keytool -import -trustcacerts -file [ca_bundle-1.crt] -alias CA1 -keystore [trust.jks]
b. keytool -import -trustcacerts -file [ca_buncle-2.crt] -alias CA2 -keystore [trust.jks]
c. continue for each certificate in bundle
```

- b. 将生成的 *.jks 和 [ca_bundle.crt] 文件复制到安全目录（即 /etc/ppm/certs）中的 PPM 服务器。在使用 spsd-certsetup 脚本更新 Web 和代理程序属性文件时将指定此位置。（请参阅下面的“管理服务器设置”）

还需要 MDE 代理程序证书。

- a. 创建包含以下信息的 OpenSSL 配置文件（即 host01.cnf）：

```
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[req_distinguished_name]
C = your_country
ST = your_state_or_province
L = your_locale_(city)
O = your_organization
OU = your_org_unit_(department)
CN = your_agent_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
extendedKeyUsage = clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = your_agent_host.your_domain
IP.1 = your_agent_ip_address
```

您需要更新 [req_distinguished_names] 和 [alt_names] 部分以反映组织的信息。

- b. 创建 MDE 代理程序 CSR

```
a. openssl req -out [host01.csr] -nodes -sha256 -newkey rsa:2048 -keyout [host01.key] -config [host01.cnf]
```

- c. 请求认证中心 (CA) 签署 CSR

- d. 接收来自 CA 的签名证书后，验证扩展密钥用法和主体备用名称是否存在

```
a. openssl x509 -in [signed-agent] -noout -text
```

- e. 如果由除 PPM 证书以外的其他 CA 签署代理程序证书，必须将 CA_bundle 证书导入到 PPM 信任库。请参阅上述 PPM 证书创建过程 (CSR) 中的第 5 步

- f. 组合签名证书和密钥

```
a. cat [signed-agent] [host01.key] > [host01.pem]
```

- g. 在 MDE 中为此主机创建代理程序时使用 [host01.pem] 证书/密钥对

```
a. [host01.pem] is uploaded using a browser during the PPM agent creation.
```

将 [host01.pem] 复制到工作站或共享资源，以使其在 PPM 代理程序创建期间可访问。

对将安装代理程序的每个主机都遵循此过程。

管理服务器设置

管理服务器设置必须在配置任何策略代理程序之前更新证书。这将要求在上载公司的密钥库和信任库以及 CA 证书捆绑软件之后执行服务器上的所提供脚本 (`/opt/securityfirst/spsd/bin/spsd-certsetup`) (请参阅《管理员指南》的“服务器证书设置”部分)。它还将要求重新启动 `spsd` 服务或重新引导管理服务器 (PPM)。未能执行此操作将导致代理程序无法与 MDE 管理服务器进行通信。

如果尚未更新证书并已配置代理程序，那么运行证书更新脚本，然后更新“代理程序信息”页面上的代理程序证书将会复原代理程序和 MDE 管理服务器之间的通信。

附录 C 用于创建 PKCS12 文件的样本转换

关于此任务

使用以下步骤将客户机专用密钥和客户机证书合并为单个 PKCS12（公用密钥密码术标准 #12）文件：

```
[user@localhost]$ openssl pkcs12 -export -out ppmclient.p12 -inkey client_key.pem -in client_cert.pem  
-name ppmclient
```

```
[user@localhost]$ keytool -v -list -keystore ppmclient.p12 -storetype pkcs12
```

附录 D 注意事项

更改分配的密钥

概述

我的受保护目录中包含数据，我想修改与该目录关联的密钥。

背景

目录中的数据使用数据创建（或数据移至该目录）时定义的密钥进行加密。更改策略密钥不会将已存在的数据迁移到新密钥。

策略已应用于代理程序并且处于活动状态时，修改受保护目录的密钥值可能会非常危险。虽然并未严格禁止，但是修改密钥值可能导致数据丢失。

可以

如果管理员希望将整个目录从一个密钥迁移到另一个密钥，那么数据首先必须从该目录中移出。目录清空后，通过策略关联的密钥值可进行更改并应用。然后，可以将数据移回到该目录并且将使用新密钥加密数据。

不可以

在没有先将数据从目录中迁移出来时，请不要修改与策略关联的密钥值以及激活策略。如果未遵循最佳实践方法，那么目录中最初存在的数据将继续使用原始密钥加密。将策略修改为新密钥后，数据将变得不可访问。此外，如果轮换原始密钥，那么数据将永远无法访问，因为无法将策略改回为原始密钥值。

使用已加密的备份轮换密钥

概述

我想备份受保护目录中的数据。

背景

使用其加密格式备份数据会在备份时将该数据与密钥值绑定在一起。如果在执行备份操作后轮换密钥，那么无法将关联数据正确复原。

密钥应该与受保护的位置相关联，而不是与数据相关联。这将避免在复原时发生无意造成的数据访问问题。

可以

目录中的数据使用数据创建（或数据移至该目录）时定义的密钥进行加密。最好在轮换密钥前先备份数据。可使用代理程序实用程序“spx-backup”来执行此操作。这样将使用不基于受保护目录且不受密钥轮换影响的密钥来备份数据。

不可以

以加密形式（例如，磁盘映像或 VM 快照）复制受保护的目录时，请务必谨慎。如果这样操作，那么在轮换原始密钥后数据可以变为不可访问。

附录 E 就地加密

为允许对已存在的目录结构和数据执行加密以及随时确定数据的状态，MDE 提供了一个名为“spxconvert”的命令行实用程序。

此功能不仅能够加密已存在的数据，而且也可在进行审计时使用，例如，支付卡行业 (PCI) 或健康保险可移植性和责任法案 (HIPAA)。

注：该功能仅与“文件”代理程序一起使用，并且不涵盖需要正式数据迁移的卷。

命令选项

spxconvert 用法：（使用方括号 [] 指示参数，并且包含类型）

-h (-?, ?) “打印此帮助对话框”

-a “执行加密文件审计”

-p [STR] “审计路径”

-e [STR] “加密文件中任何不受保护的文件”

-c “转储文件转换前/后的所有校验和”

-v “详细 - 额外打印附加信息”

Audit (-a)

缺省情况下，将针对策略目录中的所有文件执行审计。可使用 -p 选项缩小为单个目录。审计将打印未加密的目录的任何文件，打印加密目录中文件总数的文件计数。

Encrypt (-e)

转换指定目录中任何不受保护的文件。完成时，将向用户显示具有不匹配校验和的任何文件。可选的 -c 标志将在完成时打印所有文件的校验和，而不仅仅是冲突的校验和。由于性能原因仅可在完成时打印校验和，因为在转换后必须清空系统高速缓存。在每个文件后清空高速缓存会对性能产生严重的负面影响。

审计步骤

1. 显示是否有任何项暂挂加密：

spxinfo -l

1. 显示数据的详细信息：

spxconvert -a -v

1. 显示特定目录的详细信息：

spxconvert -p -v <path>

加密步骤

1. 显示暂挂加密的项：

spxinfo -l

1. 加密前显示所有校验和：

spxconvert -c -p <path>

1. 加密特定路径中任何文件：

spxconvert -p -v <path>

1. 加密后显示特定路径的所有校验和:

spxconvert -c -p <path>

附录 F 代理程序调试日志记录

缺省情况下，在策略代理程序运行时，日志记录将省略调试级别消息。要在代理程序日志中捕获调试级别消息，代理程序的系统管理员必须启用此功能部件，然后重新启动代理程序以开始捕获调试级别消息。

有效值为 1-6；但是，缺省值为“4”，并且设置为小于“4”的任何值可能会漏掉任何有用信息。

重要注意事项

- 启用调试级别日志记录可能披露敏感系统信息
- 由于调试消息的性质，代理程序日志文件的文件大小可能会大幅提高。

Linux 代理程序

关于此任务

通过找到位于 `/etc/sysconfig/spx-policyagent` 的配置文件来启用调试，并设置可写标志 (`chmod +w /etc/sysconfig/spx-policyagent`)。

将“`LOG_LEVEL=6`”附加到文件的底部（不带引号）。

Windows 代理程序

关于此任务

通过找到位于 `HKLM\SYSTEM\CurrentControlSet\Services\Spx Policy Agent\log level` 的注册表键来启用调试，并将值设置为“6”。

附录 G 非 OVA 部署

这些是如何为 PPM 部署设置非 OVA 环境的示例指示信息。仅当不部署所提供的 PPM OVA，而是创建用于部署 PPM 软件的您自己的 RHEL 或 CentOS 7.x 环境时，这些指示信息才适用。

在所有 PPM 节点上安装这些软件包。

注：这只是一个示例设置。还有许多将导致这些指示信息无效的特定于环境的需求。请联系支持人员以获取更多帮助。

1. 安装 Java 1.8 和 PostgreSQL 9.2。

注：在初始化数据库过程中将提示您输入密码。这将是 postgres “超级用户” 密码。

```
yum install -y postgresql-server java-1.8.0-openjdk-headless
passwd postgres
su - postgres
initdb --auth=md5 -W
exit
```

2. 安装防火墙策略。

以下示例显示如何使用 iptables 来安装防火墙策略。其他方法可能同样有效，可根据您的站点首选项来使用。示例：`yum install -y iptables iptables-services`

随后的两个命令假设您已安装并启用 firewalld。如果未安装 firewalld，那么运行这些命令将没有害处。

```
systemctl stop firewalld
systemctl disable firewalld
```

启动并清空 iptables 防火墙服务

```
systemctl start iptables.service
iptables -F
```

启用 iptables 服务 - 可选步骤 - 如果不需要基于本地软件的防火墙，您可以跳过

```
systemctl enable iptables.service
```

定义基本防火墙 - 可选步骤 - 如果不需要基于本地软件的防火墙，您可以跳过

```
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -j LOG --log-prefix
"SSH BruteForce: "
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
update --seconds 60 --hitcount 4 --name DEFAULT --rsource -m recent --set --name
ssh --rsource
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
service iptables save
```

3. 安装 Keepalive、HAProxy 和 PSMisc 软件包。

```
yum install -y haproxy keepalived psmisc
```

4. 下载 Zookeeper。

注：如果未安装 wget，那么请安装：

```
yum install -y wget
wget http://apache.claz.org/zookeeper/zookeeper-3.4.10/zookeeper-3.4.10.tar.gz
mkdir /home/admin
mv zookeeper-3.4.10.tar.gz /home/admin
```

5. 安装和配置可靠的网络时间来源。

虽然此示例显示 NTP 配置，但是其他可靠时间来源可能同样有效，可根据您的站点首选项来使用。

```
yum install -y ntp
sed -i "/server\ [0-9].rhel/ s/rhel/us/" /etc/ntp.conf
sed -i "/server\ [0-9].centos/ s/centos/us/" /etc/ntp.conf
systemctl stop chronyd
systemctl disable chronyd
systemctl start ntpd
systemctl enable ntpd
```

6. 安装 Extra Packages for Enterprise Linux (EPEL) 存储库

```
yum install -y epel-release
```

7. 安装不可预测的随机数字生成器（需要 EPEL）。

```
yum install -y haveged
```

8. 为服务数据收集安装 net-tools。

```
yum install -y net-tools
```

附录 H 软件版本检查

检查以下命令以检查软件版本。

PPM 版本

从 PPM VM Shell，执行以下命令：

```
cat /etc/ppm/buildinfo/release
```

Linux 代理程序版本

从 Linux CLI，运行以下命令：

```
yum list policyagent
```

AIX 代理程序版本

从 AIX CLI，执行以下命令：

```
rpm -qa | grep fileagent
```

Windows 代理程序版本

在 Windows 中浏览至添加/除去程序。滚动以查找代理程序名称。

代理程序类型	Windows 中的代理程序名称
具有策略的文件	FileAgent
卷	VolumeAgent
具有策略的卷	HybridAgent

附录 I 词汇表

术语	定义
高级加密标准新指令 (Advanced Encryption Standard New Instructions, AES-NI)	美国国家标准技术学会 (NIST) 于 2001 年确定的电子数据加密规范；基于 SPx 的产品使用此加密协议。
代理程序 (Agent)	运行 Security First 加密和访问控制软件的受管服务器。
Amazon Web Services (AWS) S3	存储和检索数据的简单存储服务，并且是高度可伸缩和廉价的对象存储器。
自动生成的密钥 (Auto-Generated Keys)	由 MDE 创建和管理的策略实施密钥。这些在策略创建期间由 Autogenerate Key 指示。
认证中心 (Certificate Authority)	签名数字证书的可信组织。CA 验证所提交的证书请求的身份和合法性。如果请求验证成功，那么 CA 发出签名证书。
证书撤销列表 (Certificate Revocation List, CRL)	发出对应的证书的认证中心 (CA) 撤销的已发布证书列表。
证书撤销列表分发点 (Certificate Revocation List Distribution Point, CRLDP)	证书中的起点字段，其中保存有关签发 CA 的已撤销证书的信息，包括名称、可选的撤销原因和 CRL 签发者名称。
云审计数据联合 (Cloud Auditing Data Federation, CADF)	转发到安全信息和事件管理 (SIEM) 系统的公共事件格式语法类型。
公共事件格式 (Comma Event Format, CEF)	转发到安全信息和事件管理 (SIEM) 系统的公共事件格式语法类型。
逗号分隔值 (Comma Separated Value, CSV)	使用逗号作为字段分隔符并使用回车作为记录分隔符的数据格式。
命令行界面 (Command Line Interface, CLI)	用户以文本行格式（命令行）向应用程序发出命令的交互类型。
全球标准时间 (Coordinated Universal Time, UTC)	全世界校准时钟和时间所依据的主要时间标准。
加密访问控制 (Cryptographic Access Controls)	通过利用不同加密材料来划分用户访问权的能力。
CURL	CURL 是提供库和命令行工具以供使用各种协议传输数据的计算机软件项目。
特异编码规则 (Distinguished Encoding Rules, DER)	DER 是 2002 年 ITU-T X.690 规范中定义的 ASN.1 编码规则之一。数据结构的编码规则提供传输语法，监管在计算机之间发送时流中字节组织方式。
域名 (Domain Name, DN)	通用唯一并且链接到 IP 目标信息的因特网资源名称
域名服务 (Domain Name Service, DNS)	将域名转换成 IP 地址的因特网服务。
动态主机配置协议 (Dynamic Host Configuration Protocol, DHCP)	一种客户机/服务器协议，用于自动向因特网协议 (IP) 主机提供其 IP 地址和其他相关配置信息（例如，子网掩码和缺省网关）。
文件代理程序 (File Agent)	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。每个受保护文件路径都可以拥有其自己的操作和加密访问控制。

图形用户界面 (Graphical User Interface, GUI)	一种用户界面类型，与基于文本的界面和输入的命令截然不同，它允许用户通过图形图标与 MDE 交互
健康保险可移植性和责任法案 (Health Insurance Portability and Accountability Act, HIPAA)	HIPAA 隐私条例需要提供商和组织确保受保护的健康信息 (PHI) 的机密性和安全性
高可用性 (High Availability, HA)	即使组件出现故障，系统操作仍继续，因为存在冗余（冗余电源、CPU、驱动器、软件等）
超文本传输协议 (Hypertext Transfer Protocol, HTTP)	作为万维网数据通信基础的应用程序协议。
系统管理程序 (Hypervisor)	也被称为虚拟机监视器。系统管理程序或虚拟机监视器 (VMM) 是用于创建、运行和管理虚拟机的计算机软件、固件或硬件。系统管理程序在其上运行一个或多个虚拟机的计算机被称为主机；每个虚拟机被称为访客机器。VMware 系统管理程序也被称为 ESXi 主机。
IBM Cloud Object Storage (COS S3)	提供静态数据和高可用性的存储平台，可保留大量数据，如备份、归档、视频文件和图像文件。
初始化向量 (Initialization Vector, IV)	任意或不可预测的随机数，可以与密钥一起用于数据加密，在任意会话期间仅使用一次。
Java 密钥库 (Java KeyStore, JKS)	Java 密钥库 (JKS) 是安全证书存储库 - 授权证书或公用密钥证书 - 以及对应的专用密钥。Java Development Kit (JDK) 提供一个工具（密钥工具）来管理密钥库中的密钥和证书。jks 扩展名是特定于 Java 的文件格式。
密钥撤销 (Key Revocation)	从代理程序环境中除去策略实施密钥，会导致可恢复的加密数据访问限制。此操作使数据暂时不可读。
密钥轮换 (Key Rotation)	在代理程序环境中迁移策略实施密钥，会导致没有用户可视的数据访问更改。
密钥粉碎 (Key Shredding)	从代理程序环境中除去策略实施密钥，会导致不可恢复的加密数据访问限制。此操作使数据永远不可读。
密钥库 (Keystore)	策略实施密钥的已配置存储位置。
轻量级目录访问协议 (Lightweight Directory Access Protocol, LDAP)	用于通过网络访问和维护分布式目录信息的供应商中立的行业标准开放协议。此软件协议使任何人都能在网络中找到组织、个人和其他资源（例如，文件和设备）。
日志事件扩展格式 (Log Event Extended Format, LEEF)	LEEF 是针对 IBM Security QRadar 的定制事件格式，其中包含 QRadar 的可读且易于处理的事件。支持事件有效内容的多种预定义事件属性。
逻辑卷管理器 (Logical Volume Manager, LVM)	存储设备管理器使用设备映射器 Linux 内核框架将存储设备收集到组，并根据需要从组合空间分配逻辑单元。大多数 Linux 分发版为 LVM-aware。
M/N (M:N)	确定在已创建的数据片（共享）总数 (N) 中重新构建数据 (M) 所需的数据片数的模型。
NT 文件系统 (NT File System, NTFS)	Microsoft 在 Windows NT 操作系统中开发的专有文件系统，用于存储和检索支持文件级安全性、压缩和审计的硬盘上的文件。
网络时间协议 (Network Time Protocol, NTP)	用于实现计算机系统之间时钟同步的联网协议。

对象标识 (Object Identifier, OID)	用于使用全局明确的持久名称命名任何对象或概念的标识标准化机制。
“对象存储”代理程序 (Object Store Agent)	“对象存储”代理程序对要发送的数据进行加密和分割, 并将数据安全地存储在高度可伸缩、高效的对象存储器中 - 在云端或/和本地。
联机证书状态协议 (Online Certificate Status Protocol, OCSP)	用于获取 X.509 数字证书的撤销状态的内部协议。
开放虚拟化归档 (Open Virtualization Archive, OVA)	tar 归档文件。它是已压缩成单个文件的所有 OVF 文件。
支付卡行业 (Payment Card Industry, PCI)	用于改进持卡人数据控制 and 安全性从而减少欺诈的标准。
PEM	一种广泛使用的安全证书编码格式, 它使用由 X.509 v3 标准定义的语法和内容来编码。
PostgreSQL	PostgreSQL (发音为 “post-gress-Q-L”) 是全球志愿者团队开发的开放式源代码关系数据库管理系统 (DBMS)。PostgreSQL 并非由任何公司或其他私有实体控制, 并且免费提供源代码。
受保护 (Protected)	已处理的任何数据。
公用密钥密码术标准 12 (Public Key Cryptography Standard #12, PKCS12)	公用密钥加密标准, 其定义用于将多个加密对象存储为单个文件的归档文件格式。通常用于将专用密钥与其 X.509 证书绑定, 或者绑定信任链的所有成员。可进行加密和签名。
公共密钥基础结构 (Public Key Infrastructure, PKI)	创建、管理、分发、使用、存储和撤销数字证书以及管理公用密钥加密所需的一组角色、策略和过程。
ReFS	Microsoft 的新文件系统, 随 Windows Server 2012 一起引入, 旨在最大程度地提高数据可用性、可伸缩性和数据完整性。
具象状态传输应用程序编程接口 (Representational State Transfer Application Program Interface, REST API)	RESTful API (也称为 RESTful Web service) 基于具象状态传输 (REST) 技术, 是在 Web service 开发中常用的通信体系结构样式和方法。
基于角色的访问控制 (Role Based Access Control, RBAC)	根据企业中各用户的角色, 控制对计算机或网络资源的访问权的方法。在此上下文中, 访问权是单个用户执行特定任务 (例如, 查看、创建或修改文件) 的能力。
RSA	Rivest, Shamir, and Adelman (RSA) 开发的公用密钥密码术, 使用公用和专用密钥来保护数据。
安全复制协议 (Secure Copy Protocol, scp)	在 Linux 中使用 scp 命令以通过安全 Shell (SSH) 协议在系统之间传输文件。
安全套接字层 (Secure Socket Layer, SSL)	加密因特网数据通信的加密协议, 其利用非对称密钥来交换对称密钥。需要认证中心和公用密钥基础结构以允许验证证书和所有者, 以及生成、签名和管理证书的有效性。
安全套接字 Shell (Secure Socket Shell, SSH)	为管理员提供访问远程计算机的安全方法的网络协议。SSH 还表示实现该协议的实用程序套件。
选择器 (Selector)	操作系统定义的用户和组, 可以访问数据、路径集和其他策略相关功能部件。

传输层安全性 (Transport Layer Security, TLS)	通过计算机网络提供安全通信的加密协议。
信任库 (Truststore)	信任库存储来自可信认证中心 (CA) 的证书，这些证书用于验证 SSL 连接中服务器的证书。
唯一标识 (Unique Identifier, UUID)	通用唯一标识 (UUID) 是软件构造中使用的标识标准。UUID (128 位数字) 用于唯一标识因特网上的一些对象或实例。
虚拟机 (Virtual Machine, VM)	基于真实计算机或假想计算机的计算机体系结构和功能的计算机系统仿真。
VMware ESXi™	基于真实计算机或假想计算机的计算机体系结构和功能的特定计算机系统仿真。
卷代理程序 (Volume Agent)	卷代理程序实施卷策略定义以及目标系统上一个或多个受保护卷的关联。
“具有策略的卷”代理程序 (Volume with Policy Agent)	其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。另外，也称为混合代理程序

声明[r]

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

Armonk, NY 10504-1785 U.S.A.

以下段落对于英国或与当地法律有不同规定的任何其他国家或地区均不适用：

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、适销或适用于某种特定用途的保证。某些国家或地区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 U.S.A.

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。

本信息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。

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。

本信息可能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。这些样本程序“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。根据您查看本信息的方式，一些图像和插图可能不显示。

商标[r]

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) 拥有所有 Apache 相关商标、服务标记以及代表 Apache 项目社区的图形徽标，所有 Apache 项目的名称都是 ASF 的商标。

Node.JS 是 Joyent, Inc. CORPORATION 的注册商标。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[r]

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。本出版物“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、非侵权和适用于某种特定用途的保证。

隐私策略注意事项[r]

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>)。

产品号：5737-C67

美国印刷

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*

以下段落对于英国或与当地法律有不同规定的任何其他国家或地区均不适用：

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。

本信息可能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) 拥有所有 Apache 相关商标、服务标记以及代表 Apache 项目社区的图形徽标，所有 Apache 项目的名称都是 ASF 的商标。

Node.JS 是 Joyent, Inc. CORPORATION 的注册商标。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>)。



SC43-5042-01

