McAfee ePolicy Orchestrator 4.0
产品手册

McAfee®

目录

ePolicy Orchestrator 4.0 简介

ePolicy Orchestrator 4.0 提供一种可伸缩平台，可以为安全产品及其所在的系统集中进行策略管理与实施。同时，它还提供全面的报告和产品部署功能，并可通过一个管理点管理全部上述功能。

目录

ePolicy Orchestrator 4.0 组件及其功能

ePolicy Orchestrator 软件由以下组件组成：

- ePO 服务器 — 托管环境的中心。该服务器为所有托管系统提供安全策略和任务、控件更新并处理事件。
- 主资料库 — ePO 服务器上的所有 McAfee 更新和签名的中心位置。主资料库从 McAfee 或用户定义的来源站点检索用户指定的更新和签名。
- 分布式资料库 — 策略性地分布在整个环境中，托管系统可以从中接收签名、产品更新和产品安装文件，对带宽影响最小。根据网络建立的方式，您可以建立 SuperAgent、HTTP、FTP 或 UNC 共享分布式资料库。
- McAfee Agent — ePO 服务器和每个托管系统之间进行信息传递和策略实施的载体。代理为每个托管系统检索更新、确保任务实施、实施策略及转发事件。

ePO 服务器

ePO 服务器提供管理、报告和实施功能，并包括：

- 强大的数据库，搜集网络中客户端系统的产品运行信息。
- 查询系统，允许监视公司的安全状态，并对收集的数据迅速采取操作。
- 软件资料库，存储您部署到网络中的产品和产品更新（如 DAT 文件）。

ePolicy Orchestrator 服务器可以将用户划分为独立的组，以进行自定义的策略管理。每个服务器最多可管理 250,000 个系统。

McAfee Agent

此代理安装在使用 ePolicy Orchestrator 管理的系统上。

此代理在后台静默运行时，会执行以下操作：

- 从托管系统收集信息和事件，并将它们发送给 ePolicy Orchestrator 服务器。

- 在托管系统上安装产品和更新。
- 在托管系统上实施策略和任务，并将事件重新发送到 ePO 服务器。

您可以从控制台部署代理（到 Windows 系统），或将代理安装包复制到可移动介质或网络共享，以便在系统上手动安装或通过登录脚本安装。在 UNIX 系统上，必须手动安装代理。

使用本手册

本手册提供有关产品配置和使用的信息。有关系统要求和安装说明，请参阅《安装手册》。

本资料是按照在生产环境中首次设置 ePolicy Orchestrator 时 McAfee 建议的顺序组织的，任何可查看特定主题的用户都可以对其进行访问。

首次设置 ePolicy Orchestrator？

本手册不但可以帮助管理员首次设置 ePolicy Orchestrator 环境，还可以为有经验的用户提供一个参考工具。根据不同的环境，您执行某些任务的顺序也可略有不同。

在首次设置 ePolicy Orchestrator 时，McAfee 建议采用以下顺序：

1 配置 ePolicy Orchestrator 服务器 — 设置用户帐户和权限，配置设置以及熟悉用户界面。

2 组织系统以进行管理 — 使用系统树可以组织通过 ePolicy Orchestrator 管理的所有系统并对这些系统采取操作。在设置其他功能前，必须创建系统树。

3 分发代理 — 要管理的每个系统都必须安装 McAfee Agent。本部分提供有关在环境中分发和维护代理的详细信息。

4 创建资料库 — 通过 ePolicy Orchestrator 将任何产品、组件或更新部署到托管系统之前，您必须先配置和创建更新资料库。

5 管理产品策略和任务 — 通过 ePolicy Orchestrator 将任何产品、组件或更新部署到托管系统之前，McAfee 建议先为这些产品和组件配置策略设置。尽管不一定要在部署之前配置策略设置，但这样做可确保产品和组件的设置尽快满足要求。

6 部署软件和更新 — 创建和配置更新资料库和策略设置之后，即可通过 ePolicy Orchestrator 将产品、组件和更新部署到相关系统。

7 配置高级功能 — 托管环境启动并运行之后，您可以配置和实现 ePolicy Orchestrator 的高级功能，如通知、查询和仪表板。

读者

本手册中的信息主要面向负责公司安全程序的网络管理员，并假定客户已在实验室环境安装并使用 ePolicy Orchestrator。

在何处查找 McAfee 企业产品信息

McAfee 文档囊括了产品实施的每个阶段（从评估新产品到维护现有产品）的信息。有的产品可能会用到其他文档。在产品发布之后，有关该产品的附属信息会输入到 McAfee 服务门户网站的在线知识库中。

评估阶段	安装阶段	设置阶段	维护阶段
我的公司如何从此产品中受益？ 评估教程 • 在测试环境中准备、安装和部署软件。 • 常见任务的详细说明。	安装之前、安装期间和安装之后。 发行说明 • 当前版本中的已知问题。 • 上个版本发布后解决的问题。 • 对产品及文档所做的最新修改。 《安装手册》 • 在工作环境中准备、安装和部署软件。	启动并运行产品。 《产品手册》和“联机帮助” • 为环境设置和自定义软件。 联机帮助 • 通过 ePolicy Orchestrator 管理和部署产品。 • 有关产品选项的详细信息。	维护软件。 联机帮助 • 维护软件。 • 参考信息。 • 产品手册中的所有信息。 快速参考卡 • 提供常用以及很少用但很重要的任务的详细说明。 知识库 (knowledge.mcafee.com) • 发行说明和文档。 • 补充的产品信息。 • 已知问题的解决方法。

查找 McAfee 企业产品的发行说明和文档。

1 访问 knowledge.mcafee.com，然后在“Useful links”（有用链接）下选择“Product Documentation”（产品文档）。

2 选择 <产品名> | <产品版本>，然后从文档列表中选择所需的文档。

配置 ePolicy Orchestrator 服务器

ePO 服务器是托管环境的中心，提供一个位置来管理整个网络的系统安全。

如果您的公司或机构规模庞大，或已划分成多个大型地点，请考虑在每个地点安装一个单独的服务器。这样做可以在本地局域网内完成管理代理、发送更新、向分布式资料库复制等工作，从而减少网络通讯量。如果通过广域网、虚拟专用网或其他速度更慢的网络连接（一般存在于远程站点之间）进行通讯，网络通讯量会对您的资源影响很大。

是否首次配置 ePO 服务器？

首次配置 ePO 服务器时：

1 查看有关用户帐户、权限集、服务器设置和服务器任务的概念性信息。

2 确定如何灵活实现权限集与用户帐户。

3 创建用户帐户和权限集，并根据需要分配权限集。

4 设置联系人列表和电子邮件服务器设置。

目录

ePO 用户帐户

用户帐户向用户提供访问和使用软件的方法。用户帐户与权限集关联，权限集定义允许用户对软件执行的操作。

您必须创建用户帐户和权限集才能满足登录到 ePO 服务器的每个用户的要求。

用户有两种类型，即全局用户和其他用户。

全局管理员

全局管理员具有读取权限、写入权限以及执行所有操作的权限。安装服务器时，会创建一个用户名为“admin”的全局管理员帐户。

您可以为需要全局管理权限的用户创建其他全局管理员帐户。

全局管理员独有的权限包括：

- 创建、编辑和删除来源站点和备用站点。
- 更改服务器设置。
- 添加和删除用户帐户。
- 添加、删除和分配权限集。
- 将事件导入 ePolicy Orchestrator 数据库并限制可以在其中存储的事件。

权限集如何工作

权限集是一组权限，可以将权限集分配给用户的帐户来将其授予任何用户。可以将一个或多个权限集分配给不是全局管理员的任何用户（全局管理员对所有产品和功能具有所有权限）。

权限集只授予权限和访问权限 — 甚至无权删除权限或访问权限。当多个权限集应用到用户帐户后，这些权限集会进行合并。例如，如果某个权限集没有服务器任务的任何权限，但其他应用到相同帐户的权限集授予对服务器任务的所有权限，则该帐户拥有对服务器任务的所有权限。在计划将权限集授予环境中用户的策略时，请考虑这一点。

何时分配权限集？

全局管理员可以在创建或编辑用户帐户以及在创建或编辑权限集时分配现有的权限集。

安装新产品时会发生什么情况？

安装新产品扩展时，它可能会将一个或多个权限集组添加到权限集。例如，在安装 VirusScan Enterprise 扩展时，会将 VirusScan Enterprise 部分添加到每个权限集。 最初，新添加的部分会在每个权限集中列出，且尚未授予任何权限。然后，全局管理员可以通过现有权限集或新权限集将权限授予用户。

默认权限集

ePolicy Orchestrator 4.0 随附有默认权限集，提供对 ePolicy Orchestrator 功能的权限。这些权限集为：

- 执行浏览者 — 提供对仪表板、事件和联系人的查看权限，可以查看与整个系统树相关的信息。
- 全局浏览者 — 提供对功能、产品和系统树的全局查看访问权限，但扩展、多服务器汇总数据、注册的服务器和软件例外。
- 组管理员 — 提供对 ePolicy Orchestrator 功能的查看和更改权限。每个分配此权限集的用户至少需要一个以上的权限集，授予对所需产品和系统数组的访问权限。
- 组浏览者 — 提供对 ePolicy Orchestrator 功能的查看权限。每个分配此权限集的用户至少需要一个以上的权限集，授予对所需产品和系统数组的访问权限。

联系人

维护一个电子邮件地址的列表，ePolicy Orchestrator 使用这些电子邮件地址将电子邮件发送到指定的用户，以对事件进行响应。当前通知、查询和导出功能都会使用此列表。

服务器设置及其控制的行为

各个设置可以控制 ePolicy Orchestrator 服务器的行为方式。您可以随时更改大多数设置。但是，只有重新安装软件才能更改服务器名称或服务器进行 HTTP 通讯时使用的端口号。

ePO 服务器设置的类型为：

- 电子邮件服务器 — 指定 ePolicy Orchestrator 发送电子邮件时的电子邮件服务器。
- 事件过滤 — 指定代理转发的事件。
- 全局更新 — 指定是否以及如何启用全局更新。
- MyAvert Security Threats — 指定 MyAvert Security Threats 的代理服务器设置和更新频率。
- 端口 — 指定服务器在与代理及数据库通讯时使用的端口。
- 打印和导出 — 指定如何将信息导出为其他格式以及指定用于 PDF 导出的模板。
- 资料库包 — 指定是否可以将任何包签入任何分支。只有版本高于 3.6 版的代理才能从当前分支之外的分支中检索更新之外的包。
- 安全密钥 — 指定和管理代理与服务器安全通讯密钥、资料库密钥。
- 系统树分类 — 指定在环境中是否以及如何启用系统树分类。

可用的服务器任务及其功能

下面介绍默认的服务器任务集合。有关这些任务的详细信息，请查看本手册的相关章节。

改进服务器任务

现在服务器任务的可配置性更好，可以在一个任务中将多个操作和子操作链在一起执行，而且可以更灵活地进行计划。

服务器任务操作

- 事件迁移 — 如果从早期版 ePolicy Orchestrator 的安装升级，则使用此任务可以将事件从旧数据库迁移到新数据库，以便您可以对历史记录数据运行查询。McAfee 建议您在升级后，尽快将此任务安排在非工作时间执行。
- NT 域/Active Directory 同步 — 同步映射到系统树组的选定的 Windows NT 域和 Active Directory 容器。此任务也可以手动执行。
- 清除审核日志 — 根据用户配置的存在时间删除审核日志中的条目。
- 清除事件日志 - 基于用户配置的标准删除数据库中的事件。
- 清除通知日志 — 根据用户配置的时间删除通知日志中的条目。
- 清除服务器任务日志 — 根据用户配置的存在时间删除服务器任务日志中的条目。
- 资料库纳入 — 从来源站点检索包，然后将其放入主资料库。
- 资料库复制 — 从主资料库更新分布式资料库。
- 汇总数据: 托管系统 — 从其他注册的 ePO 服务器导入摘要数据。
- 汇总数据: 符合性历史记录 — 从其他注册的 ePO 服务器导入摘要符合性数据。
- 运行查询 — 运行选定的查询，并允许您将与查询结果的子操作链起来。例如，您可以将结果通过电子邮件发给组织中的某个人员，也可以将代理部署到查询结果中的所有系统。
- 运行标记标准 — 根据选定的标记标准评估所有托管系统，并将标记应用到所有匹配的系统。

审核日志

使用审核日志可以维护和访问所有 ePO 用户操作的记录。审核日志条目显示在可排序的表中。为更灵活地进行处理，您还可以过滤日志，以便仅显示失败的操作，或仅显示某个存在时间内的条目。

审核日志显示七列：

- 操作 — ePO 用户尝试使用的操作的名称。
- 完成时间 — 完成操作的时间。
- 详细信息 — 有关操作的更多信息。
- 优先级 — 操作的重要性。
- 开始时间 — 启动操作的时间。
- 成功 — 指定操作是否成功完成。
- 用户名 — 采取操作所使用的登录用户帐户的用户名。

审核日志条目可用作为查询的对象。您可以通过查询构建器向导创建以此数据作为操作目标的查询，或使用以此数据作为操作目标的默认查询。例如，“失败的登录尝试”查询会检索所有失败登录尝试的表。

事件日志

使用事件日志可以快速查看和排序数据库中的事件。事件日志只能按存在时间清除。

您可以选择在可排序的表中所显示的列。您可以从选择各种事件数据来作为列。

根据您所管理的产品，您还可以对事件采取某些操作。可以通过页底部的按钮使用操作。

通用事件格式

现在所有托管产品都使用通用事件格式。此格式的字段可以用作事件日志的列。这些字段包括：

- 采取的操作 — 产品响应威胁所采取的操作。
- 代理 GUID — 转发事件的代理的唯一标识符。
- DAT 版本 — 发送事件的系统上的 DAT 版本。
- 检测产品主机名 — 检测产品所在的系统的名称。
- 检测产品 ID — 检测产品的 ID。
- 检测产品 IPv4 地址 — 检测产品所在的系统的 IPv4 地址（如适用）。
- 检测产品 IPv6 地址 — 检测产品所在的系统的 IPv6 地址（如适用）。
- 检测产品 MAC 地址 — 检测产品所在的系统的 MAC 地址（如适用）。
- 检测产品名称 — 检测托管产品的名称。
- 检测产品版本 — 检测产品的版本号。
- 引擎版本 — 检测产品引擎的版本号（如适用）。
- 事件类别 — 事件的类别。可能的类别根据产品的不同而有所不同。
- 事件生成时间 (UTC) — 检测到事件的时间（协调世界时）。
- 事件 ID — 事件的唯一标识符。
- 接收到事件的时间 (UTC) — ePO 服务器收到事件的时间（协调世界时）。
- 文件路径
- 主机名 — 发送事件的系统的名称。
- IPv4 地址 — 发送事件的系统的 IPv4 地址。
- IPv6 地址 — 发送事件的系统的 IPv6 地址。
- MAC 地址 — 发送事件的系统的 MAC 名称。
- 网络协议 — 网络中威胁类别的威胁目标协议。
- 端口号 — 网络中威胁类别的威胁目标端口。
- 进程名称 — 目标进程名称（如适用）。
- 服务器 ID
- 威胁名称 — 威胁的名称。
- 威胁来源主机名 — 产生威胁的系统名称。
- 威胁来源 IPv4 地址 — 产生威胁的系统的 IPv4 地址。
- 威胁来源 IPv6 地址 — 产生威胁的系统的 IPv6 地址。
- 威胁来源 MAC 地址 — 产生威胁的系统的 MAC 地址。
- 威胁来源 URL — 产生威胁的 URL。
- 威胁来源用户名 — 产生威胁的用户名。
- 威胁类型 — 威胁的类别。
- 用户名 — 威胁来源用户名或电子邮件地址。

从任何表或图表中导出数据

ePolicy Orchestrator 中任何图表或表中的数据都可以导出为四种不同的格式。导出的结果是历史数据，而且无法刷新。

导出报告中的数据是不可操作的，这一点与控制台中的查询结果不同。

报告可以采用下列几种格式：

- CSV — 采用此格式可以在电子表格应用程序（如 Microsoft Excel）中使用数据。
- XML — 采用此格式可以转换数据以用于其他用途。
- HTML — 采用此报告格式可以通过 Web 页的形式查看导出的结果。
- PDF — 需要打印结果时使用此报告格式。

可以对导出的数据命名，并将其保存到任何位置，或以电子邮件附件的形式发送。

MyAvert Security Threats

MyAvert Security Threats 页会将对企业用户前十位中高度风险威胁通知给您。您无须手动从新闻媒体（电视、收音机和报纸）、信息网站、邮寄列表或您的同事处搜索此信息。McAfee Avert 会自动将这些威胁通知给您。

保护状态和风险评估

您可以轻松确定主资料库当前分支中的 DAT 和引擎文件是否能抵御前十位威胁，如果不能，则确定是否能抵御最高风险级别的任何新威胁。

可用的保护

资料库中的 DAT 和引擎文件已可抵御 Avert 已知的所有威胁。若要确定每个托管系统是否受到保护，可以根据 DAT 和引擎文件覆盖范围来运行查询。

暂停中低度风险威胁防护

暂停由 AVERT 评估为中度风险威胁的更新 DAT 文件。不过，附加的病毒特征码 (EXTRA.DAT) 文件中提供有已更新的保护，如果在发生诸如病毒发作等情况下需要得到保护，但下个完整的 DAT 文件尚未提供，则可以手动下载该文件。

暂停高度风险威胁的防护

暂停由 AVERT 评估为高度风险威胁的更新 DAT 文件。不过，附加的病毒特征码 (EXTRA.DAT) 文件中提供有已更新的保护，如果在发生诸如病毒发作等情况下需要得到保护，但下个完整的 DAT 文件尚未提供，则可以手动下载该文件。

登录和注销 ePO 服务器

使用这些任务可以登录 ePO 服务器和从 ePO 服务器注销。在使用 ePolicy Orchestrator 之前，必须使用有效的帐户凭据登录 ePO 服务器。

任务

- 登录 ePO 服务器

▸ 注销 ePO 服务器

登录 ePO 服务器

使用此任务可以登录 ePO 服务器。您只有具有有效的凭据才能登录。通过为每个 ePO 服务器打开一个新浏览器会话，可以登录到多个 ePO 服务器。

任务

1 打开 Internet 浏览器，然后转至服务器的 URL。此时会出现“登录 ePolicy Orchestrator”对话框。

2 输入有效帐户的“用户名”和“密码”。

注意: 密码是区分大小写的。

3 选择希望软件显示的“语言”。

4 单击“登录”。

注销 ePO 服务器

使用此任务可以注销 ePO 服务器。结束使用软件后，可以从 ePO 服务器注销。

任务

- 要从服务器注销，请单击任何页顶部的“注销”，或关闭浏览器。

查看服务器版本号

您可以查看 ePolicy Orchestrator 服务器的版本号、版本和许可信息。

- 要查看版本号、版本，请登录至所需的 ePolicy Orchestrator 服务器。此信息出现在标题栏中。
- 若要查看许可信息，请转至登录页。
- 要查看扩展版本信息，请转至“配置”|“扩展”。

使用用户帐户

使用这些任务可以创建和维护用户帐户。

任务

▸ 创建用户帐户
▸ 编辑用户帐户
▸ 删除用户帐户

创建用户帐户

使用此任务可以创建用户帐户。只有全局管理员才能添加、编辑或删除用户帐户。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“用户”。
2 单击“新建用户”。此时会出现“新建用户”页。
3 输入用户名。
4 选择是启用还是禁用此帐户的登录状态。如果此帐户是供未加入组织的人员所使用的帐户，则可能要将其禁用。
5 选择新帐户是使用“ePO 身份验证”还是使用“Windows 身份验证”，然后提供所需的凭据。
6 （可选）在“注释”文本框中，提供用户的全名、电子邮件地址、电话号码和描述。
7 选择将用户作为全局管理员，或为此用户选择所需的权限集。
8 单击“保存”以保存当前的输入并返回到“用户”选项卡。新用户应出现在“用户”列表。

编辑用户帐户

使用此任务可以编辑用户帐户。全局管理员可以更改任何用户帐户的密码。其他用户只能更改其自己帐户的密码。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“用户”。
2 在“用户”列表中选择要编辑的用户，然后单击“编辑”。
3 根据需要编辑帐户。
4 单击“保存”。

删除用户帐户

使用此任务可以删除用户帐户。只有全局管理员才能删除用户帐户。

注意: McAfee 建议禁用帐户的“登录状态”而不是删除它，除非您确认已将与此帐户关联的所有重要信息都已传送给其他用户。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“用户”。
2 在“用户”列表中，选择要删除的用户，然后单击“删除”。
3 单击“确定”。

使用权限集

使用这些任务可以创建和维护权限集。

任务

- 为用户帐户创建权限集
- 复制权限集

为用户帐户创建权限集

使用此任务可以创建权限集。

开始之前

只有全局管理员才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“权限集”，然后单击“新建权限集”。

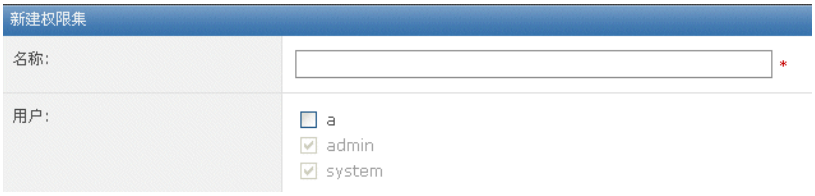

图 1：新建权限集页

2 输入权限集的名称，然后选择将此权限集分配给的用户。
3 单击“保存”。此时会出现“权限集”页。
4 从“权限集”列表中选择新权限集。其详细信息会出现在右侧。
5 单击要授予权限的任何部分旁的“编辑”。
6 在出现的“编辑权限集”页上，选择相应的选项，然后单击“保存”。
7 对所有需要的权限集部分重复此操作。

复制权限集

使用此任务可以复制权限集。只有全局管理员才能复制权限集。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“权限集”，然后选择要在“权限集”列表中编辑的权限集。其详细信息会出现在右侧。
2 单击“复制”，在“操作”窗格中输入“新名称”，然后单击“确定”。
3 从“权限集”列表中选择新副本。其详细信息会出现在右侧。
4 单击要授予权限的任何部分旁的“编辑”。
5 在出现的“编辑权限集”页上，选择相应的选项，然后单击“保存”。
6 对要授予权限的权限集的所有部分重复此操作。

编辑权限集

使用此任务可以编辑权限集。只有全局管理员才能编辑权限集。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“权限集”，然后选择要在“权限集”列表中编辑的权限集。其详细信息会出现在右侧。
2 单击要授予权限的任何部分旁的“编辑”。
3 在出现的“编辑权限集”页上，选择相应的选项，然后单击“保存”。
4 对所有需要的权限集部分重复此操作。

删除权限集

使用此任务可以删除权限集。只有全局管理员才能删除权限集。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“权限集”，然后选择要在“权限集”列表中删除的权限集。其详细信息会出现在右侧。
2 单击“删除”，然后在“操作”窗格中单击“确定”。权限集不会再出现在“权限集”列表中。

使用联系人

使用这些任务可以创建和维护可能从 ePolicy Orchestrator 接收电子邮件的人员的电子邮件地址信息。

任务

- 创建联系人
- 编辑联系人
- 删除联系人

创建联系人

使用此任务可以将电子邮件地址添加到“联系人”。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“联系人”，然后单击“新建联系人”。

图 2：新建联系人页

2 输入联系人的名、姓和电子邮件地址。

3 单击“保存”。新联系人将出现在“联系人”页中。

编辑联系人

使用此任务可以编辑“联系人”页上现有条目中的信息。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“联系人”，然后选择联系人。
2 单击“编辑”。此时会出现“编辑联系人”页。
3 根据需要编辑信息。
4 单击“保存”。

删除联系人

使用此任务可以删除“联系人”页中的条目。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“联系人”，然后选择联系人。
2 单击“删除”，然后在“操作”窗格中单击“确定”。联系人不会再出现在列表中。

使用服务器设置

使用这些任务可以创建和维护服务器设置。在此只介绍常规服务器设置。特定于功能的服务器设置将在介绍这些功能的部分中介绍。例如，在“组织系统以进行管理”中介绍系统树分类服务器设置。

任务

- 指定电子邮件服务器
- 配置导出报告的模板和位置
- 确定转发到服务器的事件
- 查看和更改通讯端口

指定电子邮件服务器

使用此任务可以指定 ePolicy Orchestrator 发送电子邮件所使用的电子邮件服务器。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，然后在“设置”列表中单击“电子邮件服务器”。
2 单击“编辑”。此时会出现“编辑电子邮件服务器”页。
3 输入 SMTP 服务器名称和 SMTP 服务器端口。

4 选择是否要通过电子邮件服务器的身份验证，并且如果选择“身份验证”，请提供凭据。
5 输入 ePolicy Orchestrator 发送的邮件上返回地址的电子邮件地址。
6 单击“保存”，然后选择“电子邮件服务器”。
7 在“测试电子邮件”旁的内容区域中，输入接收电子邮件的有效电子邮件地址，然后单击“测试”验证设置。

配置导出报告的模板和位置

使用此任务可以定义导出为文档的表和仪表板的外观和存储位置。可以配置以下选项：

- 页眉和页脚，包括自定义徽标、名称、页码等。
- 打印的页面大小和方向。
- 存储导出表和仪表板的目录。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，然后在“设置”列表中选择“打印和导出”。
2 单击“编辑”。此时会出现“编辑打印和导出”页。
3 在“导出文档的页眉和页脚”旁：
   a 单击“编辑徽标”以提供用作页眉的自定义图像或文本。
   b 从下拉列表中选择要在页眉和页脚中显示的所需元数据。
   c 选择“页面大小”。
   d 选择“页面方向”。
4 输入新位置或默认位置之外的位置来保存导出的文档。
5 单击“保存”。

确定转发到服务器的事件

使用此任务可以确定将哪些事件转发到服务器。此选择会影响环境中使用的带宽，以及基于事件的查询的结果。

开始之前

只有全局管理员才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，选择“事件过滤”，然后单击页面底部的“编辑”。此时会出现“编辑事件过滤”页。

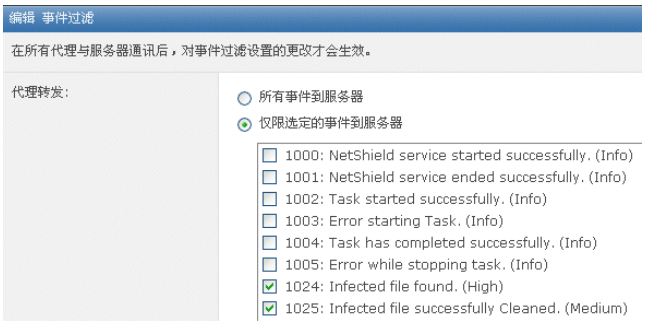

图 3：编辑事件过滤页

2 选择希望代理转发给服务器的事件，然后单击“保存”。

对这些设置的更改会在所有代理与 ePO 服务器通讯后生效。

查看和更改通讯端口

使用此任务可以查看 ePolicy Orchestrator 与分布式组件通讯所用的端口。这些端口最初是在安装时配置的。安装后，您只能更改代理进行通讯所使用的两个端口。如果您需要更改其他端口，则必须重新安装服务器，并在安装向导中重新配置端口。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，选择“端口”，然后单击页底部的“编辑”。此时会出现“编辑端口”页。

2 根据需要更改代理与服务器通讯端口或代理广播通讯端口，然后单击“保存”。

注意: 代理与服务器通讯使用代理与服务器通讯端口；SuperAgent 唤醒呼叫使用代理广播端口。

使用服务器任务日志

使用这些任务可以查看和维护服务器任务日志。

任务

- 查看服务器任务日志
- 过滤服务器任务日志
- 清除服务器任务日志

查看服务器任务日志

使用此任务可以查看服务器任务的状态和长期运行的操作。

“状态”栏中会出现每个服务器任务的状态：

- 已完成 — 任务已成功完成。

- 已失败 - 任务已启动，但未成功完成。
- 正在进行 — 任务已启动但未完成。
- 等待 — 当任务等待另一个任务完成时会出现该消息。
- 已终止 — 任务在完成前已终止。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“服务器任务日志”。

2 单击日志中的任一条目可以查看其详细信息。

图 4：服务器任务日志详细信息页

过滤服务器任务日志

随着服务器任务日志大小的增长，您可以过滤服务器任务日志，以便只显示最近的活动。您还可以过滤日志，以便只显示最近 1 天、最近 7 天、最近 30 天的条目，或按“失败”任务状态或“正在进行”任务状态显示。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“服务器任务日志”。

2 从“过滤器”下拉列表中选择所需的过滤器。

清除服务器任务日志

随着服务器任务日志大小的增长，您可以清除日志中早于用户配置的天数、周数、月数或年数的项目。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“服务器任务日志”，然后单击“清除”。

2 在“操作”面板中，输入天数、周数、月数或年数。该存在时间和早于该存在时间的所有项目都会被删除。

3 单击“确定”。

使用审核日志

使用这些任务可以查看和清除审核日志。审核日志会记录 ePO 用户采取的操作。

任务

- 查看审核日志
- 清除审核日志
- 按计划清除审核日志

查看审核日志

使用此任务可以查看管理员操作的历史记录。清除审核日志的频率以及所依据的存在时间决定了可用的数据。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“审核日志”。管理员操作的详细信息显示在表中。

图 5：审核日志页

2 单击任何列标题可以按该列排序表（字母顺序）。

3 从“过滤器”下拉列表中，选择选项以缩小可见数据的数量。您可以删除除失败操作外的所有操作，或只显示选定时间内发生的操作。

4 单击任一条目可以查看其详细信息。

图 6：审核日志条目详细信息页

清除审核日志

使用此任务可以清除审核任务。您只能按存在时间清除审核日志记录。如果清除审核日志，则会永久删除记录。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“审核日志”。
2 单击“清除”。
3 在“操作”面板中的“清除早于此天数的记录”旁，输入一个数字，并选择时间单位。
4 单击“确定”。

早于指定时间范围的所有记录都会被清除。

按计划清除审核日志

使用此任务可以通过计划的服务器任务清除任务日志。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“服务器任务”，然后单击“新建任务”。此时会出现“服务器任务生成器”向导的“描述”页。
2 提供任务的名称并描述任务，然后单击“下一步”。此时会出现“操作”页。
3 从下拉列表中选择“清除审核日志”。
4 选择是否按存在时间或从查询结果中清除。如果按查询清除，则必须选择可生成审核日志条目的表的查询。
5 单击“下一步”此时会出现“计划”页。
6 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。
7 查看任务的详细信息，然后单击“保存”。

使用事件日志

使用这些任务可以查看和清除事件日志。

任务

- 查看事件日志
- 清除事件
- 按计划清除事件日志

查看事件日志

使用此任务可以查看事件日志。

开始之前

您必须具有相应的权限才能执行此任务。

任务

1 转至“报告”|“事件日志”。

2 单击任一列表标题可以对事件排序。您还可以从“选项”下拉列表中选择“选择列”来选择符合您需要的不同表列。

3 选择表中的事件，然后单击“显示相关系统”来了解发送选定事件的系统的详细信息。

清除事件

使用此任务可以清除数据库中的事件记录。清除事件记录会永久将其删除。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“事件日志”。

2 单击“清除”。

3 在“操作”面板中的“清除早于此天数的记录”，输入一个数字，并选择时间单位。

4 单击“确定”。

早于指定存在时间的记录都会被永久删除。

按计划清除事件日志

使用此任务可以通过计划的服务器任务清除事件日志。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“服务器任务”，然后单击“新建任务”。此时会出现“服务器任务生成器”向导的“描述”页。

2 提供任务的名称并描述任务，然后单击“下一步”。此时会出现“操作”页。

3 从下拉列表中选择“清除事件日志”。

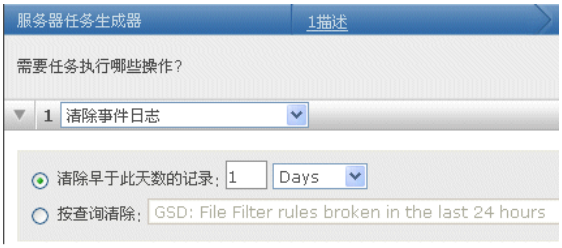

图 7：清除事件日志服务器任务操作

4 选择是否按存在时间或从查询结果中清除。如果按查询清除，则必须选择可生成事件表的查询。

5 单击“下一步”此时会出现“计划”页。

6 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。

7 查看任务的详细信息，然后单击“保存”。

使用 MyAvert Security Threats

使用这些任务可以将威胁通知标记为已读取或未读取，或将其删除。数据会按发现威胁的日期排序。另外，您可以单击威胁名称以查看 McAfee Avert 网站中有关每个威胁的信息。

注意: 每个用户都可以查看其帐户唯一的“MyAvert”页。如果某个用户删除威胁通知或将其标记为已读取或未读取，则在其他用户帐户登录时，表中不显示这些操作。

任务

- 配置 MyAvert 更新频率和代理服务器设置
- 查看威胁通知
- 删除威胁通知

配置 MyAvert 更新频率和代理服务器设置

使用此任务可以配置 MyAvert Security Threats 的代理服务器设置和更新频率。

任务

1 转至“配置”|“服务器设置”，选择“MyAvert Security Threats”，然后单击“编辑”。

2 选择希望更新 MyAvert 威胁通知的频率。

3 然后，选择是否使用代理服务器访问此服务。如果您选择使用代理服务器，请提供所需的详细信息来使用代理服务器。

查看威胁通知

使用此任务可以查看通知威胁并将威胁标记为已读取或未读取。您可以按威胁的重要性过滤威胁，或是否已将其标记为已读取或未读取进行过滤。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“MyAvert”。

图 8：MyAvert Security Threats 页

2 如果要缩小可查看通知的范围，请从“过滤器”下拉列表中选择选项。

3 如果要将通知标记为已读取或未读取，请选择所需的威胁，然后根据需要单击“标记已读取”或“标记未读取”。您可能需要从“过滤器”下拉列表中选择“读取”或“未读”来查看要标记的通知。

删除威胁通知

使用此任务可以删除“MyAvert”页中的威胁通知。您无法删除仍处于暂停保护状态的任何威胁通知。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“MyAvert”。

2 选择受到保护的威胁通知，然后单击“删除”。

将表和图表导出为其他格式

使用此任务可以导出数据以用于其他用途。您可以导出为 HTML 和 PDF 之类的最终格式进行查看，也可以导出为 CSV 或 XML 文件，供其他应用程序使用和转换数据。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 在显示数据（表或图表）的页中，从“选项”菜单中选择“导出表”或“导出数据”。此时会出现“导出”页。

图 9：导出页

2 选择是分别导出数据文件，还是导出为一个存档 (ZIP) 文件。

3 选择导出文件的格式。如果导出到 PDF 文件，请选择页面大小和方向。

4 选择是否将文件作为电子邮件附件发给选定的收件人，或是否将其保存到服务器上提供链接的位置。您可以打开文件，也可以右键单击文件以保存到其他位置。

注意: 如果输入多个收件人的电子邮件地址，则必须使用逗号或分号分隔每个条目。

5 单击“导出”。

随即会创建文件，并以电子邮件附件的方式发给收件人，或将您带到一个页面，可在此通过链接访问这些文件。

计划服务器任务时允许的 Cron 语法

Cron 语法是由空格分隔的 6 个或 7 个字段组成。下表详细说明已接受的 Cron 语法（按字段递减排列）。大多数 Cron 语法都是可接受的，但也有一些不支持的情况。例如，您无法同时指定星期和日期的值。

字段名称	允许的值	允许的特殊字符
秒	0 - 59	, - * /
分钟	0 - 59	, - * /
小时	0 - 23	, - * /
日期	1 - 31	, - * ? / L W C
月	1 - 12 或 JAN - DEC	, - * /
星期	1 -7 或 SUN - SAT	, - * ? / L C #
年（可选）	空，或 1970 - 2099	, - * /

允许的特殊字符的注释

- 允许使用逗号 (,) 指定其他值。例如，“5,10,30”或“MON,WED,FRI”。
- 星号 (*) 用来表示“每个”。例如，分钟字段中的“*”表示“每分钟”。
- 可使用问号 (?) 指定“星期”或“日期”字段中无特定的值。

  注意: 问号必须在这些字段中的其中一个使用，不能在两个字段中同时使用。

- 斜杠 (/) 表示增量。例如，分钟字段中的“5/15”表示任务在 5、20、35 和 50 分钟运行。
- “L”字母在“星期”字段或“日期”字段中表示最后一个。例如，“0 15 10 ? * 6L”表示每月最后一个星期五早上 10:15。
- 字母“W”表示“工作日”。因此，如果您创建的日期为“15W”，这表示离该月 15 日最近的工作日。另外，您可以指定“LW”，表示该月的最后一个工作日。
- 英镑字符“#”表示该月的第 N 天。例如，在星期字段中使用“6#3”表示每月的第三个星期五，“2#1”表示第一个星期一，“4#5”表示第五个星期三。

  注意: 如果该月没有第五个星期三，则任务不会运行。

组织系统以进行管理

ePolicy Orchestrator 4.0 提供一些新功能并改进现有功能来组织和管理系统。

- 目录已被系统树取代，使用系统树可以轻松管理策略和任务，并组织系统和组。
- 标记 — 使用此新功能可以创建标签，可以根据分配给标记的标准，手动或自动将标签应用到系统。您可以根据标记（如 IP 地址分类）将系统分类到组，或将标记用作查询标准。
- NT 域和 Active Directory 同步 — 现在使用此功能可以：
  - 完全同步 Active Directory 结构。
  - 控制系统树中可能的重复系统条目。
  - 在从域和容器中删除系统后，控制系统树中的系统。
- 自动将系统分类到组中 — 除以前的 IP 地址分类功能外，现在也可以将标记用作分类标准。可以单独使用每个分类标准类型，也可以组合这些类型来使用。

系统树包含所有 ePolicy Orchestrator 管理的系统；它是管理这些系统上的策略和任务的主要界面。您可以将系统分成逻辑组（如按职能部门或地理位置划分），也可以根据 IP 地址或标记对它们进行分类。您可以为系统树任何层级上的系统管理策略（产品配置设置）和安排任务（如更新病毒特征码文件）。

在配置该软件部署或管理环境中的安全软件之前，您必须规划如何对系统进行合理组织以进行管理，并选择将系统放入并保存在系统树中的方法。

提示: 许多因素都会影响创建和组织系统树的方式。因此，McAfee 建议您在开始创建系统树之前，先通读本手册。

是否首次设置系统树？

首次设置系统树：

1 了解本部分的概念性主题，这样您可以将它与其他功能一起使用来有效组织系统。

2 评估用系统填入系统树并保持最新的方法。例如，通过 Active Directory 同步或基于标准的分类来填充系统树。

3 创建并填充系统树。

目录

系统树

系统树以单元的形式组织托管系统，以便完成监控、分配策略、计划任务和采取操作。

组

系统树是一个分层结构，您可以在名为组的单元中对系统进行分组。

组具有以下特征：

- 全局管理员或具有相应权限的用户可以创建组。
- 组可以包括系统和其他组。
- 全局管理员或具有相应权限的用户可以管理组。

通过将具有相似属性或要求的系统分组到这些单元中，您可以在一个位置管理系统的策略，而不必分别为每个系统设置策略。

在规划的过程中，应该考虑在构建系统树之前将系统组织成组的最佳方式。

不明来源组

系统树的根（我的组织）包括不明来源组。根据创建和维护系统树的方法，服务器使用不同的特征来确定放置系统的位置。不明来源组存储无法确定位置的系统。

不明来源组具有以下特征：

- 不能删除。
- 不能重命名。
- 不能更改其分类标准（尽管可以为您在此组中创建的子组提供分类标准）。
- 该组始终位于列表的最后位置，而不按字母顺序排序。
- 对系统树具有查看权限的所有用户都可以查看不明来源组中的系统。
- 系统分类到不明来源组后，它会放置在与系统域名称相同的子组中。如果此类组不存在，请创建这样一个组。

注意: 如果您删除系统树中的系统，则还需要删除其代理。否则，这些系统会因代理继续与服务器进行通讯而仍然出现在不明来源组中。

继承

继承是一个非常重要的属性，可以简化策略和任务管理。因为具有继承功能，系统树层次结构中的子组将继承其父组中设置的策略。例如：

- 在“我的组织”层级设置的策略会由其下的组继承。
- 组策略由该组中的子组或单个系统来继承。

默认情况下，对添加到系统树中的所有组和单个系统均启用继承功能。这样，您只需在少数几个位置设置策略和计划客户端任务即可。

不过，可以在系统树的任何位置（只要用户对此位置具有相应的权限）通过应用新策略来中断继承，从而自定义继承。您可以锁定策略分类来保留继承。

规划系统树时的考虑事项

构建一个有效而完备的系统树可以简化维护。在每个环境中，有关管理、网络和职责的许多实际情况都会影响系统树的组织结构方式。在建立和填充系统树的组织结构之前，请先对其进行规划。特别是大型网络，您想一次完成系统树的构建时，就更应进行规划。

因为每个网络都是不同的，并且要求使用不同的策略（以及可能采用不同的管理），所以 McAfee 建议您在实施软件之前，首先规划系统树。

无论您选择哪些方法创建和填充系统树，在规划系统树时您都需要考虑所处的环境。

管理员访问权限

在规划系统树组织结构时，应考虑对系统负有管理职责的人员的访问权限要求。

例如，您组织中的网络管理非常分散，不同的管理员负责管理网络的不同部分。出于安全原因，您可能没有可以访问网络每一部分的全局管理员帐户。在这种情况下，您可能无法使用一个全局管理员帐户设置策略和部署代理。您可能转而需要根据这些部分将系统树组织成组，并创建帐户和权限集。

要考虑的问题包括：

- 谁负责管理哪些系统？
- 谁有权查看系统信息？
- 谁无权访问系统及系统信息？

这些问题会影响系统树组织以及创建并应用到用户帐户的权限集。

环境界限及其对系统组织的影响

组织系统的管理方式取决于网络中的界限划分。这些界限划分对系统树的组织结构所产生的影响与对网络拓扑的组织结构所产生的影响不同。

McAfee 建议您评估网络和组织中的下列界限划分，以决定在定义系统树的组织结构时是否必须考虑这些因素。

拓扑界限

网络已由 NT 域或 Active Directory 容器定义。网络环境组织得越好，使用同步功能创建和维护系统树就越简单。

地理界限

安全管理就是在安全与性能之间取得平衡。组织您的系统树以便充分利用有限的网络带宽。考虑服务器连接网络各部分的方式，尤其是远程地点，它们经常通过慢速广域网或虚拟专用网连接，而不是通过快速的局域网连接。您可能要为这些远程站点分别配置不同的更新策略和代理与服务器通讯策略，以最大程度降低通过慢度连接的网络通讯量。

首先根据地理位置对系统进行分组，对配置策略有以下几点好处：

- 您可以配置组的更新策略，以便让所有系统从附近的一个或多个分布式软件资料库中进行更新。
- 您可以安排客户端任务在适合您站点位置的时间运行。

职责界限

许多大型网络都按负责管理网络不同部分的不同人员或组进行划分。有时，这些界限划分与拓扑或地理界限划分不一致。访问和管理系统树部分的人员会影响系统树的结构。

功能界限

一些网络是根据使用网络的人员的角色（如销售员和工程师）来划分的。即使网络未按职能界限划分，如果不同的组需要不同的策略，您也需要根据职能来组织系统树部分。

业务组可能运行需要特殊安全策略的特定软件。例如，可以将电子邮件交换服务器分到组，并设置 VirusScan Enterprise 按访问扫描的特定排除项。

子网和 IP 地址范围

在许多情况下，网络的组织单元使用特定的子网或 IP 地址范围，因此您可以针对地理位置创建一个组并为其设置 IP 过滤器。同样，如果网络在地理位置上并不分散，您可以将网络位置（如 IP 地址）用作主要的分组标准。

如有可能，请考虑使用基于 IP 地址信息的分类标准来自动执行系统树创建和维护。为系统树中适用的组设置 IP 子网掩码或 IP 地址范围标准。 这些过滤器将使用相应的系统自动填充位置。

标记和具有类似特征的系统

您可以使用标记来自动分类到组。标记标识具有类似特征的系统。如果您可以按特征来组织组，则可以基于标准来创建和分配标记，然后使用这些标记作为组分类标准，以确保这些系统自动放在相应的组中。

如有可能，请考虑使用基于标记的分类标准以自动将相应的系统填充到组。

操作系统和软件

请考虑对装有类似操作系统的系统进行分组，以轻松管理操作系统特定的产品和策略。如果有一些运行 Windows 95 或 Windows 98 的旧系统，则可以为这些旧版系统一起创建一个组，分别部署和管理这些系统上的安全产品。另外，通过为这些系统分配一个相应的标记，也可以将这些系统自动分类到组中。

标记及其工作方式

标记是 ePolicy Orchestrator 4.0 提供的新功能。标记与标签类似，您可以自动（基于标准）或手动应用到一个或多个系统。在应用标记后，则可以使用这些标记组织系统树中的系统，或者运行可产生可操作的系统列表的查询。因此，将标用作组织标准，您可以应用策略、分配任务以及对具有相同标记的系统采取一组操作。

标记的特点

使用标记可以：

- 将一个或多个标记应用到一个或多个系统。
- 手动应用标记。
- 在代理与服务器通讯时，根据用户定义的标准自动应用标记。
- 从标记应用中排除系统。
- 运行查询以对具有某些标记的系统进行分组，然后直接对所产生的系统列表采取操作。
- 基于标记的系统树分类可以将系统自动分组到所需的系统树组。

使用标记的人员

具有相应权限的用户可以：

- 创建和编辑标记及标记标准。
- 将现有标记应用到他们具有访问权限的组中的系统以及从中删除现有标记。
- 排除系统，以避免接收特定的标记。
- 使用查询查看具有某些标记的系统并对其采取操作。
- 使用具有链式标记操作的计划查询可以维护其具有访问权限的系统树部分中特定系统上的标记。
- 根据标记配置分类标准可以确保系统位于系统树的相应组中。

标记的类型

标记类型有两种：

- 无标准的标记。这些标记只能应用到系统树中的选定系统（手动）以及查询结果中列出的系统。
- 基于标准的标记。这些标记在每次代理与服务器通讯时都应用于所有非排除的系统。此类标记使用的标准基于代理发送的任何属性。还可以根据需要将它们应用于非排除的系统。

Active Directory 和 NT 域同步

ePolicy Orchestrator 4.0 改进了与 Active Directory 和 NT 域的集成功能，可以将其作为系统来源，甚至（在使用 Active Directory 的情况下）作为系统树结构的来源。

Active Directory 同步

如果您的网络运行 Active Directory，则可以使用 Active Directory 同步来利用 Active Directory 同步设置创建、填充和维护部分或所有系统树。定义好后，可以使用 Active Directory 中的任何新系统（及子容器）更新系统树。

ePolicy Orchestrator 4.0 版增强了 Active Directory 集成功能。除可以使用以前的功能外，您现在可以：

- 导入系统和 Active Directory 子容器（作为系统树组）并保持与 Active Directory 同步更新，从而实现与 Active Directory 结构同步。每次同步时，系统树中的系统和结构都会更新，以反映 Active Directory 的系统和结构。
- 将 Active Directory 容器（及其子容器）中的系统以扁平列表的形式导入同步组。
- 控制如何处理可能出现的重复系统。
- 使用系统描述（从 Active Directory 中随系统一起导入）。

早期版 ePolicy Orchestrator 提供有两个任务：Active Directory 导入和 Active Directory 发现。现在，使用此过程可以将系统树与 Active Directory 系统结构集成在一起：

1 在系统树中作为映射点的每个组中配置同步设置。在同一个位置，可以配置是否：

2
- 将代理部署到发现的系统。
- 在从 Active Directory 中删除系统后，从系统树中删除系统。
- 允许或不允许已在系统树的其他位置存在重复的系统条目。

3 使用“立即同步”操作可以根据同步设置将 Active Directory 系统（以及可能的结构）导入系统树。

4 使用 NT 域/AD 目录同步服务器任务可以根据同步设置，定期同步系统（以及可能的 Active Directory 结构）与系统树。

Active Directory 同步的类型

Active Directory 同步有两种类型（仅限系统以及系统与结构）。您使用哪种类型取决于要与 Active Directory 集成的级别。

使用每种类型，您可以控制同步，方法是选择是否：

- 将代理自动部署到比 ePolicy Orchestrator 新的系统。在开始同步时，如果要导入大量系统且带宽有限，则可能不希望在最初同步时进行此设置。代理安装包大小大约为 3.62 MB。但是，您可能希望将代理自动部署到后续同步期间在 Active Directory 发现的任何新系统。
- 从 Active Directory 删除系统后，即从 ePolicy Orchestrator 删除这些系统（及其代理）。
- 如果系统存在于系统树的其他位置，则会防止将系统添加到组。如果您手动移动系统或将系统移到其他位置，则会确保没有重复的系统。
- 从同步操作中排除某些 Active Directory 容器。同步时，会忽略这些容器及其系统。

系统和结构

使用此同步类型时，Active Directory 结构中的更改会在下次同步时传递到系统树结构。在 Active Directory 中添加、移动或删除系统或容器时，这些系统或容器也会在系统树的对应位置得以添加、移动或删除。

何时使用此同步类型

使用此同步类型可以确保系统树（或部分系统树）与 Active Directory 结构完全相同。

如果 Active Directory 的组织结构符合您的安全管理需要，而且您希望系统树继续与已映射的 Active Directory 结构类似，请在后续同步时使用此同步类型。

仅限系统

使用此同步类型可以从 Active Directory 容器（包括非排除子容器）中将系统以扁平列表的方式导入映射的系统树组。然后，您可以通过将分类标准分配到组，将这些系统移到系统树的所需位置。

如果选择此同步类型，则在系统树的其他位置存在系统时，务必选择不再次添加这些系统。这可以防止系统树中的系统存在重复的条目。

何时使用此同步类型

在以下情况下使用此同步类型：将 Active Directory 用作 ePolicy Orchestrator 的系统的一般来源，但安全管理的组织要求不符合 Active Directory 中容器和系统的组织结构。

NT 域同步

将 NT 域作为填充系统树的来源。将组与 NT 域同步时，此域中的所有系统都会以扁平列表的形式放入此组。 您可以在单个组中管理这些系统，也可以创建子组来满足细微的组织要求。使用某个方法（如自动分类）自动填充这些子组。

如果要将系统移到系统树的其他组或子组，则在系统存在于系统树中其他位置的情况下，务必选择不重新添加系统。

与 Active Directory 同步不同，只有系统名称与 NT 域进行同步，不同步系统描述。

基于标准的分类

与 ePolicy Orchestrator 的早期版本类似，您可以使用 IP 地址信息自动将托管系统分类到特定组。您还可以基于标记创建分类标准，这与将标签分配到系统相似。您可以使用任一标准类型或两种标准类型以确保系统位于系统树中您所希望的位置。

系统仅需匹配组分类标准的一个标准就可以放在组中。

创建组并设置分类标准后，采取“测试分类”操作可以确认标准和分类顺序来获得所需的结果。

在将分类标准添加到组后，可以运行“立即分类”操作。此操作会自动将选定系统移到相应的组。不符合任何组分类标准的系统会移到不明来源组。

首次连接到服务器的新系统会自动添加到正确的组中。不过，如果在初次代理与服务器通讯后定义分类标准，则必须对这些系统运行“立即分类”操作，以立即将其立即移到相应的组，或等到下一次代理与服务器通讯为止。

系统的分类状态

您可以启用或禁用任何系统或系统集合的系统树分类。如果禁用某个系统的系统树分类，则不对此系统执行分类操作。

ePO 服务器上的系统树分类设置

要进行分类，必须在服务器和系统上启用分类。默认情况下，会在每次代理与服务器通讯时启用分类。

测试分类系统

使用此功能可以查看分类操作时放置系统的位置。“测试分类”页会显示系统以及对系统分类所在位置的路径。虽然此页并不显示系统的分类状态，但如果在该页上选择系统（甚至选择禁用分类的系统），单击“移动系统”也会将这些系统放在所标识的位置。

设置如何影响分类

您可以选择三个服务器设置来确定是否对系统分类以及何时分类。另外，通过对系统树中的选定系统启用或禁用系统树分类，您可以选择是否分类任一系统。

服务器设置

服务器含有三个设置：

- 禁用系统树分类 — 如果基于标准的分类没有满足您的安全管理要求，而且您想使用其他系统树功能（如 Active Directory 同步）来组织系统，则选择此设置可以防止其他 ePO 用户误配置组的分类标准，并将系统移到不需要的位置。
- 每次代理与服务器通讯时对系统分类 — 在每次代理与服务器通讯时再次对系统分类。更改组的分类标准后，系统会在下次代理与服务通讯时移到新组。
- 对系统分类一次 — 系统会在下次代理与服务器通讯时对系统分类，只要选择此设置，系统会标记为在代理与服务器通讯时不再分类。不过，选择此类系统并单击“立即分类”会对系统进行分类。

系统设置

您可以禁用或启用任何系统的系统树分类。如果禁用了某个系统的系统树分类，则不论采取何种分类操作，都不会对该系统进行分类。如果启用了系统的系统树分类，则手动执行“立即分类”操作可以始终对该系统分类，而且可能在代理与服务器通讯时分类，这取决于系统树分类服务器设置。

IP 地址分类标准

在许多网络中，子网和 IP 地址信息反映了组织的特点，例如地理位置或工作职能。如果 IP 地址组织方式符合您的要求，则请考虑使用此信息，通过为此类组设置 IP 地址分类标准来创建和维护部分或全部系统树结构。此功能已在此版本的 ePolicy Orchestrator 中更改，现在可以在整个树中随机设置 IP 分类标准，您不再需要确保子组的 IP 地址分类标准是父组 IP 地址分类标准的子集（只要父组没有分配的标准 ）。配置好后，您可以在代理与服务器通讯时分类系统，也可以仅在手动启动分类操作时分类系统。

请注意，IP 地址分类标准在不同的组中不能重叠。组分类标准的每个 IP 范围或子网掩码应覆盖一组唯一的 IP 地址。如果标准发生重叠，则这些系统最终所在的组取决于“组”选项卡上子组的顺序。

基于标记的分类标准

除了使用 IP 地址信息将系统分类到相应的组，您可以根据分配给系统的标记定义分类标准。

可以将基于标记的标准与基于 IP 地址的标准搭配使用以进行分类。

组顺序和分类

为了更灵活地管理系统树，您可以配置组的子组的顺序，从而进一步配置分类过程中考虑放置系统的顺序。在多个子组都有匹配标准时，更改此顺序会更改系统在系统树中的最终位置。

另外，如果您使用全部捕获组，则这些组必须是列表中的最后一个子组。

捕获全部组

捕获全部组是在组的“分类标准”页上，将组的分类标准设置为“所有其他”的组。只有位于分类顺序最后一个位置的子组才可为捕获全部组。这些组会接收分类到父组，但没有分类到任何捕获全部对等组中的所有系统。

如何将系统首次放入系统树

当代理首次与服务器通讯时，服务器会使用某种算法将系统放在系统树中。如果服务器找不到放置系统的位置，则会将系统放在不明来源组中。

首次代理与服务器通讯

每次代理与服务器通讯时，服务器都会尝试按 GUID 在系统树中查找系统（只有代理首次连接到服务器的系统在数据库中有代理 GUID ）。如果找到匹配的系统，则将此系统留在现有的位置。

如果找不到匹配的系统，则服务器会使用某种算法将系统分类到相应的组。只要路径中的每个父组都没有不匹配的标准，则不管该系统在结构中有多深，都可以将其分类到系统树中任何基于标准的组中。基于标准的子组的父组必须没有标准或没有匹配的标准。

请记住，子组放置在“组”选项卡上的顺序，会决定服务器搜索具有匹配标准的组时所考虑的子组的顺序。

1 服务器会在与域名称同名的组中搜索没有代理 GUID（其代理之前从未连接到服务器）但有匹配名称的系统。如果找到这样的一个系统，则此系统被放在该组中。在 Active Directory 或 NT 域首次同步时，或已手动将系统添加到系统树时会发生这种情况。

2 如果仍未找到匹配的系统，则服务器会搜索与域同名且系统所来自的组。如果找不到这样一个组，则会在不明来源组下创建一个组，然后将系统放在此处。

3 更新该系统的属性。

4 如果服务器配置为在每次代理与服务器通讯时运行分类标准，则服务器会将所有基于标准的标记应用到系统。

5 接着发生什么情况取决于是否启用服务器和系统的系统树分类标准。

- 如果禁用了服务器或系统的系统树分类，则系统会保持位置不变。
- 如果启用了服务器和系统的系统树分类，则会根据分类标准将系统移到系统树组中。

  注意: 默认情况下，通过 Active Directory 或 NT 域同步添加的系统会禁用系统树分类。因此，首次代理与服务器通讯时不对这些系统进行分类。

6 服务器会根据所有最高层级组在“我的组织”组的“组”选项卡中的分类顺序来考虑这些组的分类标准。系统会被放到具有匹配标准的第一个组，或放到所认为的捕获全部组中。

   a 在系统分类到组中后，会根据“组”选项卡上的该组的子组的分类顺序了解该组的每个子组是否具有匹配的标准。

   b 这一过程会持续进行，直到为系统找不到具有匹配标准的子组为止，然后将系统放在找到的具有匹配标准的最后一个组中。

7 如果找不到此类最高层级组，则会根据其分类来考虑这些组的子组（没有分类标准）。

8 如果找不到这样一个基于第二层级标准的组，则会考虑第二层级无限制组的基于标准的第三层级组。

   注意: 不考虑与匹配标准不符的组的子组，组必须具有匹配标准，或没有标准才能考虑将系统放到其子组中。

9 这会沿着整个系统树向下进行，直到将系统分类到某个组为止。

   注意: 如果服务器的系统树分类设置配置为仅在首次代理与服务器通讯时分类，则会在系统上设置一个标记，除非服务器设置更改为在每次代理与服务器通讯时启用分类，否则该系统不会在代理与服务器通讯时再次分类。

10 如果服务器不能将该系统分类到任何组中，则会将它放到不明来源组中与域同名的子组内。

使用标记

使用这些任务可以创建标记并将标记应用到系统。

任务

- 使用标记构建器创建标记
- 从自动标记中排除系统
- 将标记应用到选定的系统
- 自动将基于标准的标记应用到所有匹配的系统

使用标记构建器创建标记

使用此任务可以通过“标记构建器”向导创建标记。标记可以在以下情况下使用针对每个系统评估的标准：

- 在代理与服务器通讯时自动使用。
- 在采取“运行标记标准”操作时。
- 在选定的系统上通过“应用标记”操作手动使用，不考虑标准。

没有标准的标记只能手动应用到选定的系统。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“标记目录”，然后单击“新建标记”。此时会出现“任务构建器”向导的“描述”页。

2 输入名称和有意义的描述，然后单击“下一步”。此时会出现“标准”页。

3 选择并配置所需的标准，然后单击“下一步”。此时会出现“评估”页。

   注意: 若要自动应用标记，则必须为标记配置标准。

4 选择是否只在采取“运行标记标准”操作时，或同时在每次代理与服务器通讯时，按照标记的标准评估系统，然后单击“下一步”。此时会出现“预览”页。

   注意: 如果没有配置标准，则这些选项不可用。当按照标记标准评估系统时，标记会应用到符合标准且尚未从标记中排除的系统。

5 验证此页上的信息，然后单击“保存”。

   注意: 如果标记有标准，则此页会显示按照系统标准评估时接收此标记的系统的数量。

此标记会添加到“标记目录”页上标记的列表中。

从自动标记中排除系统

使用此任务可以排除系统应用特定的标记。或者，可以使用查询收集系统，然后从查询结果的这些系统中排除所需的标记。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”，然后选择包含系统的组。

2 选择所需的系统，然后单击页底部的“排除标记”。

   注意: 如果没有看到此按钮，请单击“更多操作”。

3 在“操作”面板中，从下拉列表中选择要从选定系统排除的所需标记，然后单击“确定”。

4 验证已从标记中排除的系统：

   a 转至“系统”|“标记目录”，然后在“标记”列表中选择所需的标记。

   b 在详细信息窗格的“含此标记的系统”旁，单击链接以获取从自动标记中排除的系统的数量。此时会显示“从此标记排除的系统”页。

   c 验证所需的系统是否在列表中。

将标记应用到选定的系统

使用此任务可以手动将标记应用到系统树中的选定系统。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”，然后选择包含所需系统的组。

2 选择所需的系统，然后单击页底部的“应用标记”。

注意: 如果没有看到此按钮，请单击“更多操作”。

3 在“操作”面板中，从下拉列表中选择所需标记以应用到选定系统，然后单击“确定”。

4 确认已应用标记：

a 转至“系统”|“标记目录”，然后在标记列表中选择所需的标记。

b 在详细信息窗格的“含此标记的系统”旁，单击链接以获取手动标记的系统的数量。此时会显示“含有手动应用的标记的系统”页。

c 验证所需的系统是否在列表中。

自动将基于标准的标记应用到所有匹配的系统

使用这些任务可以自动将基于标准的标记应用到匹配此标准的所有系统

任务

- 将基于标准的标记应用到所有匹配的系统
- 按计划应用基于标准的标记

将基于标准的标记应用到所有匹配的系统

使用此任务可以将基于标准的标记应用到符合标准的所有系统，但已从标记中排除的系统除外。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“标记目录”，然后从“标记”列表中选择所需的标记。

2 单击“运行标记标准”。

3 在“操作”面板中，选择是否手动重置标记和排除的系统。

注意: 这会删除系统中不符合标准的标记，并将标记应用到符合标准但已排除接收标记的系统。

4 单击“确定”。

5 确认系统已应用标记：

a 转至“系统”|“标记目录”，然后在标记列表中选择所需的标记。

b 在详细信息窗格的“含此标记的系统”旁，单击链接可以获取含有按标准应用标记的系统的数量。此时会显示“含有按标准应用的标记的系统”页。

c 验证所需的系统是否在列表中。

标记会应用到符合其标准的所有系统。

按计划应用基于标准的标记

使用此任务可以计划一个定期执行的任务，以将标记应用到符合其标准的所有系统。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“服务器任务”，然后单击“新建任务”。此时会出现“服务器任务生成器”页。

2 命名并描述此任务，并选择是否在创建任务后启用任务，然后单击“下一步”。此时会出现“操作”页。

3 从下拉列表中选择“运行标记标准”，然后从“标记”下拉列表中选择所需的标记。

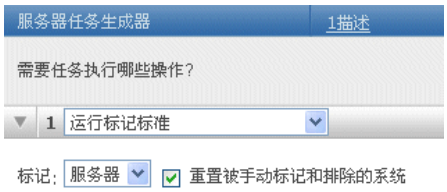

图 10：运行标记标准服务器任务操作

4 选择是否手动重置标记和排除的系统。

注意: 这会删除系统中不符合标准的标记，并将标记应用到符合标准但已排除接收标记的系统。

5 单击“下一步”此时会出现“计划”页。

6 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。

7 查看任务设置，然后单击“保存”。

服务器任务会添加到“服务器任务”页的列表中。如果在“服务器任务生成器”向导中选择启用任务，则它会在下次计划的时间运行。

创建和填充组

使用这些任务可以创建和填充组。您可以使用两种方法将系统填充到组：一种是输入各系统的 NetBIOS 名称，另一种是直接从网络导入的系统。

组织系统树并非只有一种方法，因为每个网络的情况各不相同，您的系统树组织结构也可能与网络布局一样是特有的。尽管您不必使用所提供的每一种方法，但可以使用多种方法。

例如，如果您在网络中使用 Active Directory，则会考虑导入 Active Directory 容器，而不是导入 NT 域。如果 Active Directory 或 NT 域组织结构不能用于安全管理，您可以在文本文件中创建系统树，然后将其导入您的系统树。如果您使用的是小型网络，则可以手动创建系统树并导入每个系统。

最佳实践

尽管您不需要使用所有系统树创建方法，但是，也可能不仅仅使用一种创建方法。许多情况下，将所选多种方法结合使用既可轻松地创建系统树，也可以通过其他结构使策略管理更有效。

例如，您也许会分两个阶段创建系统树。首先，您可以通过将整个 NT 域或 Active Directory 容器导入组，创建系统树结构的 90%。然后，您可以手动创建子组，将可能具有类似防病毒或安全策略要求的系统归为一类。在此情况下，您可以在这些子组上使用标记以及基于标记的分类标准，以确保它们最终会自动位于所需的组。

如果您希望所有或部分系统树镜像 Active Directory 结构，则可以导入且定期同步系统树与 Active Directory。

如果 NT 域非常大或跨越了几个地理区域，则可以创建子组，并将每个组中的系统指向不同的分布式资料库以提高更新效率。或者，您可以创建更小的职能分组（如根据不同的操作系统类型或业务职能）来管理不同的策略。在此情况下，您还可以使用标记和基于标记的分类标准，以确保系统位于组中。

如果您组织的 IP 地址信息与安全管理需求相符，请考虑在分发代理前，将 IP 地址分类标准分配到这些组，以确保在代理首次签入服务器时，系统会自动放在正确的位置。如果要在环境中实现标记，还可以使用标记作为组的分类标准，或甚至使用 IP 地址和标记分类标准的组合。

不过，您可以创建含有许多层级组的详细系统树。McAfee 建议您创建的结构满足您的使用需要即可。在大型网络中，同一容器内包含成百上千个系统是很平常的。在少数几个位置分类策略比维护精心创建的系统树要容易。

尽管可以将所有系统添加到系统树的一个组中，但是这样的单层列表很难为不同系统设定不同的策略，尤其是对于大型网络。

任务

手动创建组

使用此任务可以手动创建组。您可以使用两种方法将系统填充到这些组：一种是输入各系统的 NetBIOS 名称，另一种是直接从网络导入系统。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“组”，然后在系统树中选择在其下创建其他组的所需组。

2 单击页底部的“新建子组”。此时会出现“新建子组”对话框。

3 输入所需的名称，然后单击“确定”。新建组会出现在系统树中。

4 根据需要重复此过程，直到可以用所需的系统填充这些组为止。将系统添加到系统树中，然后通过以下操作确保这些系统到达所需的组：

- 手动输入系统名称。
- 从 NT 域或 Active Directory 容器导入系统。 您可以定期将域或容器与组同步，以便于维护。
- 在组上设置基于 IP 地址或基于标记的分类标准。当具有匹配 IP 地址信息或匹配标记的系统中的代理签入时，这些系统会被自动放在相应的组中。

手动将系统添加到现有组

使用此任务可以将网络邻居中的系统导入组。您还可以导入网络域或 Active Directory 容器。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”，然后单击“新建系统”。此时会出现“新建系统”页。

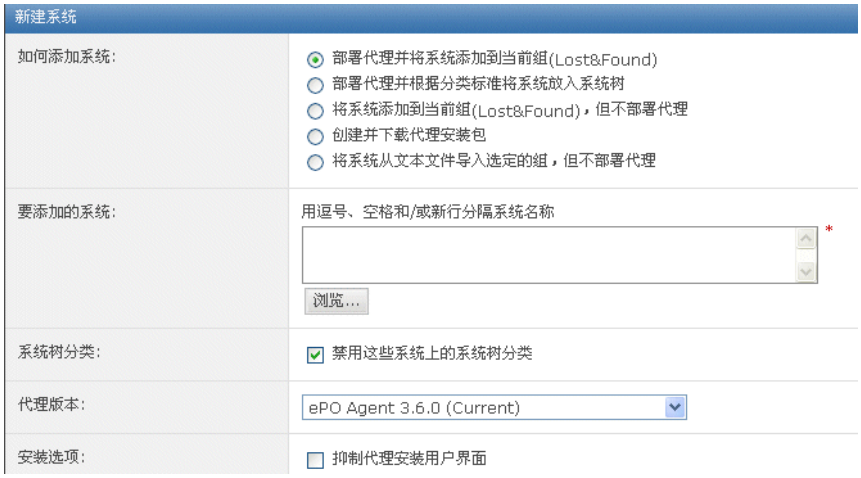

图 11：新建系统页

2 选择是否将代理部署到新系统，以及是否根据分类标准，将系统添加到选定的组或某个组。

3 在“要添加的系统”旁，在文本框中输入每个系统的 NetBIOS 名称，名称间由逗号、空格或换行符分隔。或者，单击“浏览”以选择系统。

4 如果选择“部署代理并将系统添加到当前组”，则可以启用自动系统树分类。执行此操作将分类标准应用到这些系统。

5 如果选择将代理部署到新系统：

   a 选择要部署的代理版本。

   b 选择是否抑制系统上的代理安装用户界面。如果不希望最终用户看到安装界面，请选择此选项。

   c 配置代理安装路径或接受默认路径。

   d 输入有效的凭据以安装代理。

6 单击“确定”。

从文本文件导入系统

使用这些任务可以创建系统和组的文本文件来导入系统树。

任务

- 创建组和系统的文本文件
- 从文本文件导入系统和组

创建组和系统的文本文件

使用此任务可以创建一个文本文件，其中含有要导入组的网络系统的 NetBIOS 名称。您可以导入系统的简单列表，或者将系统分成组，然后将指定的系统添加到这些组中。您可以手动创建文本文件。在大型网络中，使用其他网络管理工具可以生成网络中系统的文本文件列表。

通过在文本文件中输入组和系统名称，可以定义组和系统。然后，将该信息导入 ePolicy Orchestrator。您必须使用网络实用程序（如 Microsoft Windows Resource Kit 附带的 NETDOM.EXE 实用程序）生成包含网络中系统完整列表的全部文本文件。在具有此文本文件后，您可以通过手动编辑该文本文件创建系统的组，并将整个结构导入系统树中。

无论您如何生成文本文件，您必须使用正确的语法，然后才能将其导入。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 将每个系统单列一行。要将系统分成组，请输入组名并后带一个反斜杠 (\)，然后在下面列出属于该组的系统，每个系统单列一行。

```
GroupA\system1
GroupA\system2
GroupA\system3
GroupA\system4
```

2 确认组和系统的名称，文本文件的语法，然后将此文本文件保存到服务器上的临时文件夹。

从文本文件导入系统和组

使用此任务可以从您创建和保存的文本文件中，将系统或系统组导入系统树。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”，然后单击“新建系统”。此时会出现“新建系统”页。
2 选择“将系统从文本文件导入选定的组，但不部署代理”。
3 单击“浏览”，然后选择文本文件。
4 选择如何处理已存在于系统树其他位置的系统。
5 单击“确定”。

系统会导入系统树中的选定组中。如果在文本文件中已将系统分成组，则服务器会创建组，并导入系统。

将系统分类到基于标准的组

使用这些任务可以配置和实现分类以对系统分组。对于要分类到组中的系统，必须在服务器和所需的系统上启用分类，并且必须配置组的分类标准和分类顺序。

任务

- 将分类标准添加到组
- 启用服务器的系统树分类
- 启用和禁用系统的系统树分类
- 手动分类系统

将分类标准添加到组

使用此任务可以配置组的分类标准。分类标准可以基于 IP 地址信息或标记。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“组”，然后在“系统树”中选择组。

2 在“分类标准”旁，单击“编辑”。此时会显示选定组的“分类标准”页。

3 选择“符合下面任一标准的系统”，然后出现标准选择项目。

注意: 尽管可以为组配置多个分类标准，但系统只需匹配一个标准即可放在此组中。

4 配置标准。选项包括：

- 标记 — 添加特定的标记，以确保来到父组中的具有此类标记的系统会分类到此组中。
- IP 地址 — 使用此文本框可以将 IP 地址范围或子网掩码定义为分类标准。地址位于此范围的任何系统都会分类到此组。

5 根据需要重复此步骤，直到为该组配置了分类标准为止，然后单击“保存”。

启用服务器的系统树分类

使用此任务可以启用服务器的系统树分类。只有启用服务器和所需系统的系统树分类才能对系统进行分类。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，在“设置类别”列表中选择“系统树分类”，然后单击“编辑”。

2 选择是仅在首次代理与服务器通讯时对系统分类，还是每次代理与服务器通讯时都对系统分类。

如果您选择仅在首次代理与服务器通讯时分类，则会在下次代理与服务器通讯时对所有启用的系统进行分类，而且只要选择此选项，都不会再次分类。但是，手动采取“立即分类”操作，或将设置改为在每次代理与服务器通讯时分类，即可对这些系统分类。

如果您选择在每次代理与服务器通讯时分类，则只要选择了此选项，所有启用的系统都会在每次代理与服务器通讯时分类。

启用和禁用系统的系统树分类

使用此任务可以启用或禁用系统的系统树分类。系统的分类状态决定是否可以将其分类到基于标准的组。或者，您可以更改任何系统表（如查询结果）中系统的分类状态，还可以在计划查询的结果上自动更改。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后选择所需的系统。

2 单击“更改分类状态”，然后选择是启用还是禁用选定系统的系统树分类。

注意: 您可能需要单击“更多操作”来访问“更改分类状态”选项。若要查看系统的分类状态，请将列添加到“系统”页。

图 12：更改分类状态选项

根据系统树分类的服务器设置，这些系统会在下次代理与服务器通讯时分类。否则，只能采取“立即分类”操作进行分类。

手动分类系统

使用此任务可以使用启用的基于标准的分类将系统分类到组。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后选择包含所需系统的组。

2 选择系统，然后单击“立即分类”。您可能需要单击“更多操作”访问此选项。此时会出现“立即分类”对话框。

注意: 如果要在分类前预览分类结果，请单击“测试分类”。（但是，如果您从“测试分类”页中移动系统，则会对所有选定的系统分类，甚至对已禁用系统树分类的系统进行分类。）

3 单击“确定”以对系统分类。

导入 Active Directory 容器

使用此任务可以通过将 Active Directory 来源容器映射到系统树组，可以将系统从网络的 Active Directory 容器直接导入系统树。与以前的版本不同，您现在可以：

- 同步系统树结构与 Active Directory 结构，这样在 Active Directory 中添加或删除容器时，也会在系统树中添加或删除相应的组。
- 在从 Active Directory 中删除系统后，从系统树中删除系统。
- 在系统存在于其他组中时，防止系统树中出现重复的系统条目。

开始之前

您必须具有相应的权限才能执行此任务。

最佳实践

此功能的实施取决于您是初次创建系统树，还是从具有现有系统树结构且未使用 Active Directory 集成的早期版本升级。

如果您一直在使用 ePolicy Orchestrator 的早期版本，并已完全填充了该系统树，则仍然可以通过将系统树组映射到 Active Directory 来利用 Active Directory 集成。您可以使用此功能创建

Active Directory 容器和系统树组之间的映射点，以将在 Active Directory 中发现的所有新系统都导入系统树的相应位置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“组”，然后在“系统树”中选择所需的组。该组应为要将 Active Directory 容器映射到的组。

注意: 您不能同步系统树的“我的组织”或“不明来源”组。

图 13：同步设置页

2 在“同步类型”旁，单击“编辑”。此时会显示选定组的“同步设置”页。

3 在“同步类型”旁，选择“Active Directory”。此时会显示 Active Directory 同步选项。

4 选择要在此组和所需 Active Directory 容器（及其子容器）之间进行的 Active Directory 同步的类型。

- 系统和容器结构 — 如果希望此组完全反映 Active Directory 结构，请选择此选项。同步后，会修改此组下的系统树结构，以反映它所映射到的 Active Directory 容器的结构。在 Active Directory 中添加或删除容器时，也会在系统树中添加或删除容器。从 Active Directory 中添加、移动或删除系统时，也会在系统树中添加、移动或删除系统。
- 仅限系统 — 如果您只希望将 Active Directory 容器（和非排除的子容器）中的系统填充此组，则选择此选项。不会像镜像 Active Directory 时创建子组。

5 选择是否为已存在于系统树中其他组的系统创建重复的系统条目。

提示: McAfee 建议不要选择此选项，特别是如果您仅将 Active Directory 同步作为安全管理的起始点，并使用系统树管理功能（如标记分类）在映射点下进一步进行组织细分，就更是如此。

6 在“Active Directory 域”中，输入 Active Directory 域的全限定名称。

7 在“Active Directory 凭据”中，输入 ePolicy Orchestrator 检索 Active Directory 信息所使用的 Active Directory 用户凭据。

8 在“容器”旁，单击“浏览”，并在“选择 Active Directory 容器”对话框中选择来源容器，然后单击“确定”。

9 要排除特定的子容器，请单击“排除项”旁的“添加”，选择要排除的容器，然后单击“确定”。

10 选择是否将代理自动部署到新系统。如果部署，请务必配置部署设置。

提示: 如果容器很大，McAfee 建议您在初始导入过程中不要部署代理。将 3.62 MB 的代理包同时部署到多个系统时可能会产生网络通讯问题。因而，应先导入容器，然后逐次将代

理部署到几个系统组中，而不是同时进行部署。在最初的代理部署后，请考虑重新访问此页并选择此选项，以便代理会自动安装到已添加到 Active Directory 的新系统。

11 选择从 Active Directory 域中删除系统后，是否还从系统树中删除系统。

12 若要立即将组与 Active Directory 同步，请单击“立即同步”。
单击“立即同步”会在同步组前将任何更改保存到同步设置。如果您已启用 Active Directory 同步通知规则，则会为每个添加或删除的系统生成事件（这些事件出现在通知日志中，并是可查询的）。如果将代理部署到已添加的系统，则会开始对每个添加的系统进行部署。同步完成后，系统会更新“上次同步”时间，显示同步完成的时间和日期，不显示完成任何代理部署的时间。

注意: 或者，您可以为首次同步计划一个 NT 域/Active Directory 同步服务器任务。如果您要在首次同步时将代理部署到新系统，而带宽是主要考虑因素时，此方法很有用。

13 同步完成后，查看系统树的结果。

导入系统后，如果您没有选择自动分发代理，则将代理分发到这些系统。同时，请考虑设置一个可重复执行的 NT 域/Active Directory 同步服务器任务，以确保系统树保持为最新，始终具有 Active Directory 容器中的所有新系统或组织更改。

将 NT 域导入现有组

使用此任务可以将系统从 NT 域导入已手动创建的组。

通过将整个 NT 域与指定的组同步，可以自动填充组。通过此方法，可以轻松将网络中的所有系统以扁平列表的形式一次添加到系统树中，但不添加系统描述。

如果域很大，您可以创建子组来协助您进行策略管理或系统树组织。为此，首先将域导入系统树组，然后手动创建逻辑子组。

提示: 要跨几个域管理相同的策略，请将每个域导入同一组中的子组，可以在这个组上设置每个子组继承的策略。

使用此方法时，请：

- 在子组上设置 IP 地址或标记分类标准，以自动对导入的系统进行分类。
- 计划一个可重复执行的 NT 域/Active Directory 同步服务器任务，以便轻松地执行维护。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“组”，然后在系统树中选择或创建组。

2 在“同步类型”旁，单击“编辑”。此时会显示选定组的“同步设置”页。

图 14：同步设置页

3 在“同步类型”旁，选择“NT 域”。此时会显示域同步设置。

4 在“ 位于系统树中其他位置的系统”旁，选择如何处理在同步过程中要添加，但已存在于系统树中其他组中的系统。

注意: McAfee 建议不要选择“将系统添加到同步组并将其放置在当前的系统树位置”，特别是，如果您仅使用 NT 域同步作为安全管理的开始点，并使用其他系统树管理功能（如标记分类）在映射点下进行细微的组织管理，就更是如此。

5 在“域”旁，单击“浏览”，然后选择要将映射到此组的 NT 域，然后单击“确定”。或者，您可以直接在文本框中输入域的名称。

注意: 输入域名时，请不要使用全限定域名。

6 选择是否将代理自动部署到新系统。如果部署，请务必配置部署设置。

提示: 如果域很大，McAfee 建议您在最初导入 NT 域时不要部署代理。将 3.62 MB 的代理包同时部署到多个系统时可能会产生网络通讯问题。因而，应先导入域，然后逐次将代理部署到几个较小的系统组中，而不是同时进行部署。但是，在代理部署完成后，请在最初部署代理后考虑重新访问此页并选择此选项，以便代理会自动安装到通过域同步添加到组（或其子组）的任何新系统。

7 选择从 NT 域中删除系统时，是否还从系统树中删除系统。

8 若要立即同步组与域，请单击“立即同步”，然后在将域中的系统添加到组中时等待。

注意: 单击“立即同步”会在同步组前保存同步设置的更改。如果已启用 NT 域同步通知规则，则会为添加或删除的每个系统生成事件。（这些事件出现在通知日志中，而且是可查询的。）如果选择将代理部署到已添加的系统，则会开始对每个添加的系统进行部署。同步完成后，会更新“上次同步”时间。此时间和日期是同步完成的时间和日期，而不是完成代理部署的时间和日期。

9 如果要手动同步组与域，请单击“比较和更新”。此时会出现“手动比较和更新”页。

注意: 单击“比较和更新”会将更改保存到同步设置。

a 如果要通过此页从组中删除任何系统，请选择是否在删除系统时还删除代理。

b 根据需要，选择要添加到该组或从该组中删除的系统，然后单击“更新组”以添加选定的组。此时会出现“同步设置”页。

10 单击“保存”，然后查看系统树中的结果（如果已单击“立即同步”或“更新组”）。

在系统添加到系统树后，如果在同步时没有选择部署代理，则将代理分发到这些系统上。同时，请考虑设置一个可重复执行的 NT 域/Active Directory 同步服务器任务，以将此组保持为最新，始终具有 NT 中的所有新系统。

按计划同步系统树

使用此任务可以安排一个服务器任务，该任务用映射域或 Active Directory 容器中的更改来更新系统树。根据组的同步设置，此任务可以：

- 将网络上的新系统添加到指定的组。
- 在创建新 Active Directory 容器后，添加相应的新组。
- 删除 Active Directory 容器时删除相应的组。
- 将代理部署到新系统。
- 删除域或容器中不再存在的系统。
- 将站点或组的策略和任务应用到新系统中。
- 防止出现或允许重复的系统条目（这些系统已存在于系统树中，但已移到其他位置）。

注意: 代理使用这种方式无法部署到所有操作系统中。您需要将代理手动分发到某些系统中。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“服务器任务”，然后单击页底部的“新建任务”。此时会出现“服务器任务生成器”的“描述”页。

2 对任务命名，并选择是否在创建任务后启用该任务，然后单击“下一步”。此时会出现“操作”页。

3 从下拉列表中，选择“NT 域/Active Directory 同步”。

4 选择是否同步所有同步组或选定的组。如果您只同步某些已同步的组，则单击“选择同步组”，然后选择特定的组。

5 单击“下一步”此时会出现“计划”页。

6 安排该任务，然后单击“下一步”。此时会出现“摘要”页。

7 查看任务详细信息，然后单击“保存”。

注意: 除在计划的时间运行的任务外，您可以通过单击“服务器任务”选项卡上任务旁的“运行”来立即运行此任务。

手动使用 NT 域更新同步组

使用此任务可以同步组及其映射到的 NT 域，包括：

- 添加当前在域中的系统。
- 从系统树中删除不再出现在域中的系统。
- 从不再属于指定域的所有系统中删除代理。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“组”，然后选择映射到 NT 域的组。

2 在“同步类型”旁，单击“编辑”。此时会出现“同步设置”页。

3 在接近页的底部，单击“比较和更新”。此时会出现“手动比较和更新”页。

4 如果从组中删除系统，则选择是否从已删除的系统中删除代理。

5 单击“全部添加”或“添加”，以将系统从网络域导入选定的组。

单击“全部删除”或“删除”，从选定的组删除系统。

6 完成后，单击“更新组”。

手动移动系统树内的系统

使用此任务可以将系统从系统树中的一个组移到另一个组。您可以从显示系统表（包括查询结果）的任何页中移动系统。

即使您已经具有一个组织结构完善的系统树，它能够镜像实际的网络层次结构，并且您可以使用自动任务和工具定期将系统同步，但您可能仍然需要在组之间手动移动系统。例如，您可能需要定期移动不明来源组中的系统。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后浏览到系统并进行选择。

2 单击“移动系统”。此时会出现“选择新组”页。

注意: 您可能需要单击“更多操作”访问此操作。

3 在移动系统时，选择在选定的系统上是启用还是禁用系统树分类。

4 选择放置系统的组，然后单击“确定”。

分发代理以管理系统

有效管理网络系统依赖于运行最新活动代理的每个系统。

可以通过几种方法来分发代理。您所采用的方法取决于：

- 环境的实际情况。
- 是升级代理还是首次分发代理。

是否首次分发代理？

首次在整个环境中部署代理时，请：

1 阅读本章中的信息，了解代理及其策略和任务以及分发代理的方法。

2 配置代理分发到的系统树组的代理策略设置。

3 使用所选方法将代理分发到所需的位置。

目录

代理和 SuperAgent

代理是 ePolicy Orchestrator 的分布式组件，必须将其安装在网络中要管理的每个系统上。SuperAgent 是一种启用后可通过网络广播网段分发广播唤醒呼叫的代理。SuperAgent 还可以用作分发产品和更新的来源站点。

代理在 ePO 服务器、更新资料库、托管系统和产品之间收集和发送信息。没有安装代理，ePolicy Orchestrator 就无法管理系统。

代理安装文件夹

默认情况下，托管系统和服务器上的代理安装文件夹的位置是不同的。

在服务器系统上，代理安装于以下位置：

<SYSTEM_DRIVE>\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

在托管系统上，如果代理是在安装其他产品的过程中安装的，或者从控制台推送到该系统，则默认情况下将其安装在以下位置：

<SYSTEM_DRIVE>\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

在托管系统上，如果将代理从 2.5.1 版升级，则在卸载现有代理之后，新代理也会默认安装在以下位置：

<SYSTEM_DRIVE>\PROGRAM FILES\NETWORK ASSOCIATES\COMMON FRAMEWORK

小心: 安装代理后，必须先将其删除，才能更改其安装目录。

代理语言包

无论是默认还是自定义代理安装包都安装英文版。对于全新安装，默认情况下这些包位于主资料库中。

每个代理语言包仅包含以该语言显示用户界面所需的那些文件。可以将代理语言包复制到分布式资料库中。

在首次代理与服务器通讯后，代理将检索与当前使用的区域设置相对应的新包，并应用该包。采用这种方式，代理只检索针对每个托管系统上使用的区域设置的语言包。

注意: 在应用新的语言包之前，界面仍以当前语言显示。

托管系统上可以存储多个语言包，因此用户能够通过更改区域设置来切换语言。如果本地没有与选定区域设置相对应的语言包，则界面将以英文显示。

代理语言包有以下几种语言版本：

- 葡萄牙语（巴西）
- 中文（简体）
- 中文（繁体）
- 英语
- 荷兰语
- 法语（标准）
- 德语（标准）
- 意大利语
- 日语
- 韩语
- 波兰语
- 西班牙语
- 瑞典语

代理安装包

安装服务器时会创建 FRAMEPKG.EXE 文件。它是一个自定义的安装包，用于安装向服务器报告的代理。该包包含服务器名称及其 IP 地址、ASCI 端口号以及使代理可以与服务器通讯的其他信息。

默认情况下，代理安装包安装在以下位置：

C:\PROGRAM FILES\MCAFEE\EPO\DB\SOFTWARE\CURRENT\ ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE

这是服务器用于部署代理的安装包。

默认的代理安装包不包含嵌入的用户凭据。在系统上执行安装时，将使用当前登录用户的帐户。

代理与服务器之间的通讯

在代理与服务器通讯期间，两者会使用 SPIPE 交换信息，SPIPE 是 ePolicy Orchestrator 为进行安全的网络传输而使用的一种专用网络协议。在每次通讯时，代理都会收集当前系统属性以及任何事件，并将其发送到服务器。服务器会将所有新的或更改后的策略、任务和资料库列表发送到代理。然后，代理将在托管系统本地实施新策略。

可以用下列三种方法启动代理与服务器之间的通讯：

- 代理与服务器通讯间隔 (ASCI)
- 代理安装后由代理主动进行通讯
- 代理唤醒呼叫
- 手动从托管系统进行通讯

代理与服务器通讯间隔

代理与服务器通讯间隔 (ASCI) 在“McAfee Agent”策略页的“常规”选项卡上设置。此设置决定了代理连接到服务器以进行数据交换及获取更新指令的频率。默认情况下，ASCI 设置为 60 分钟；代理每小时签入服务器一次。

在决定是否修改此策略设置时，必须考虑您组织的威胁响应要求、可用带宽以及存放服务器的硬件。请注意，ASCI 通讯可能会产生大量的网络通讯，尤其是在大型网络中更会如此。在这种情况下，远程站点中可能有以慢速网络连接相连的代理。对于这些代理，您可能希望设置频率较低的 ASCI。下表列出针对常用网络连接速度的一般 ASCI 建议。

一般建议的 ASCI 设置

网络规模	建议的 ASCI
千兆级局域网	60 分钟
100MB 级局域网	60 分钟
广域网	360 分钟
拨号或 RAS	360 分钟
10MB 级局域网	180 分钟
无线局域网	150 分钟

注意: 有关平衡带宽、服务器硬件和确定 ASCI 的完整信息，请参阅《ePolicy Orchestrator 4.0 硬件评估和带宽使用手册》白皮书。

代理安装后由代理主动进行通讯

安装代理之后，代理会在代理服务停止并重新启动后的 10 分钟内，以随机时间间隔连接到服务器。后续通讯会以代理策略中设置的 ASCI（默认为 60 分钟）进行。

可以在安装后使用 /P 命令行选项运行 CMDAGENT.EXE 来强制代理立即与服务器进行通讯。

唤醒呼叫

唤醒呼叫提示代理连接到服务器。唤醒呼叫可以手动发送，也可以安排为一个客户端任务。如果已对策略进行更改或签入了更新，并希望在下次 ASCI 后便将其应用到托管系统，唤醒呼叫功能非常有用。

唤醒呼叫还可以在“服务器任务生成器”向导计划的查询结果上配置。

SuperAgent 和广播唤醒呼叫

如果要使用代理唤醒呼叫启动代理与服务器之间的通讯，则应考虑将每个广播网段上的一个代理转换为 SuperAgent。SuperAgent 会分散代理唤醒呼叫对带宽造成的影响，最大程度减少网络通讯量。

服务器将 SuperAgent 唤醒呼叫发送到选定系统树部分中的 SuperAgent，而不是将代理唤醒呼叫从服务器发送到每个代理。当 SuperAgent 收到此唤醒呼叫时，会将广播唤醒呼叫发送到广播网段中的所有代理。这会减少网络通讯量。在 ePolicy Orchestrator 可能要通过慢速广域网或虚拟专用网连接管理远程站点中代理的大型网络中，此功能非常有用。

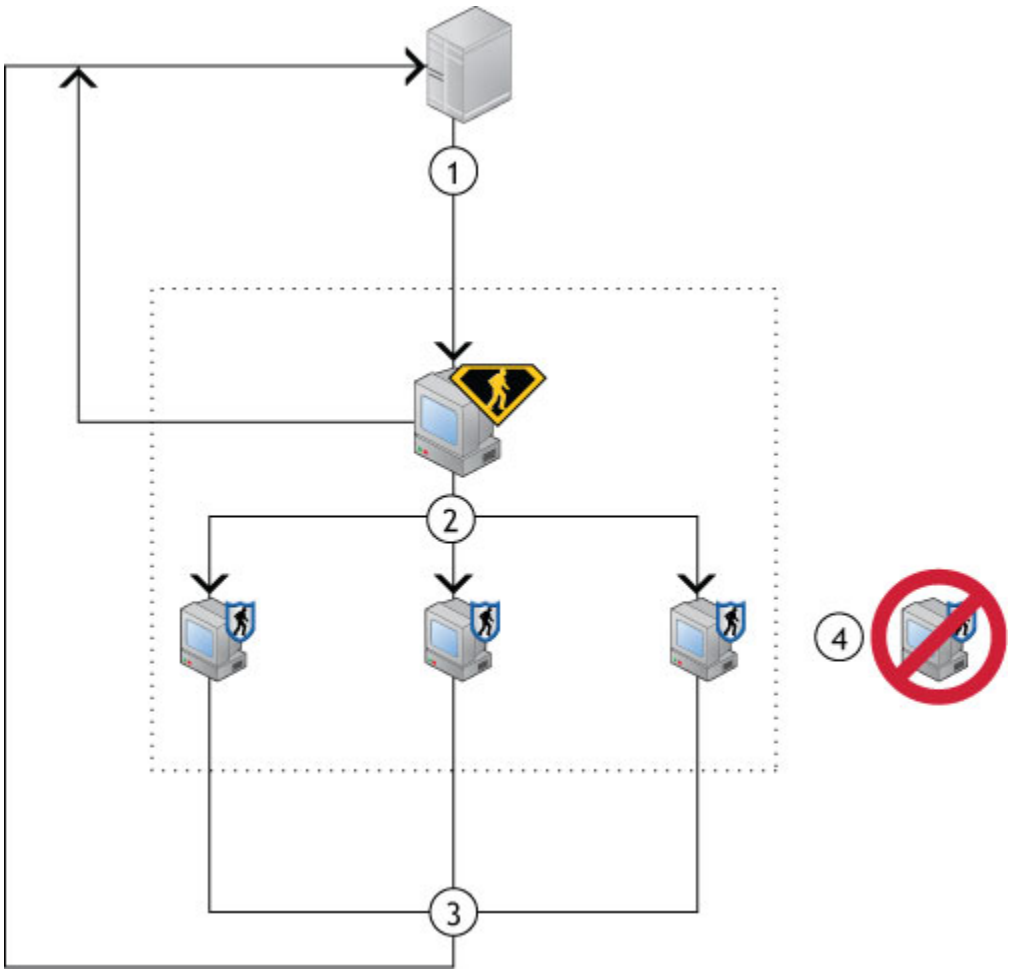

图 15：SuperAgent 和广播唤醒呼叫

1 服务器向所有 SuperAgent 发送唤醒呼叫。

2 SuperAgent 向同一广播网段内的所有代理发送广播唤醒呼叫。

3 所有代理（常规代理和 SuperAgent）都与服务器交换数据。

4 对于广播网段中没有运行 SuperAgent 的任何代理，系统将不提示其与服务器进行通讯。

最佳实践

要在适当位置部署足够数量的 SuperAgent，请先确定环境中的广播网段，然后在每个网段中选择存放 SuperAgent 的系统（最好是服务器）。请注意，没有 SuperAgent 的广播网段中的代理不会接收广播唤醒呼叫，因此，请不要连接到服务器。

与常规代理唤醒呼叫类似，SuperAgent 唤醒呼叫使用 SPIPE 协议。确保没有阻止代理唤醒通讯端口（默认为 8081）和代理广播通讯端口（默认为 8082）。

代理活动日志

在确定代理状态或排除故障时，代理日志文件非常有用。有两种日志文件可以记录代理活动，都位于托管系统上的代理安装文件夹中。

代理活动日志

代理活动日志是名为 agent_<system>.xml 的 XML 文件，其中 <system> 是安装代理的系统的 NetBIOS 名称。此日志文件会记录与策略实施、代理与服务器通讯以及事件转发等相关的代理活动。您可以定义此日志文件的大小限制。

在“McAfee Agent”策略页上的“记录”选项卡上，可以配置记录代理活动的级别。

详细代理活动日志

详细代理活动日志文件名为 agent_<system>.log，其中 <system> 是安装代理的系统的 NetBIOS 名称。除了代理活动日志中存储的信息之外，详细的活动日志还包括故障排除消息。此文件最大为 1MB。当此日志文件达到 1MB 时，会生成一个备份副本 (agent_<system>_backup.log)。

代理策略设置

代理策略设置决定环境中的代理的性能和行为，包括：

- 代理连接到服务器的频率。
- 代理在托管系统上实施策略的频率。
- 代理将事件文件提供给服务器的频率。
- 代理到何处获取产品和更新包。

在整个网络中分发大量代理之前，请仔细考虑希望代理在环境各部分中的行为方式。尽管可以在分发代理后配置代理策略，但 McAfee 建议在分发前设置代理策略，以防对资源产生不必要的影响。

有关代理策略页上选项的完整描述，请在显示选项的页上单击“?”。不过，在此先讨论最重要的策略设置。

优先级事件转发

托管系统上的代理和安全软件在正常工作期间会不断生成软件事件。其中包括有关常规操作的信息事件（如代理在本地实施策略时产生的事件）以及严重事件（如检测到病毒但未清除病毒时产生的事件）。这些事件在每次代理与服务器通讯时发送到服务器，然后存储在数据库中。在大型网络中，典型的 ePolicy Orchestrator 部署每小时可以生成数千个此类事件。您很可能不想查看每一个事件。

通常，您可能想立即了解严重级别较高的事件。可以将代理配置为立即转发等于或大于指定严重级别的事件（由生成事件的产品决定具体的事件严重性）。如果要使用通知功能，则必须启用立即上载严重级别较高的事件，以便这些功能能够按预期工作。

您可以在“McAfee Agent”策略页的“事件”选项卡上启用立即上载事件。

全部属性和最少属性

每次代理与服务器通讯时，代理都会将信息从托管系统发送到服务器，您便可以从 ePolicy Orchestrator 查看各系统的属性。

在首次通讯期间，代理将发送完整的属性集。在此之后，代理仅发送上次通讯后已更改的属性。

但是，在以下情况下代理会再次发送完整属性集：

- 已将策略设置为发送全部属性，并已在托管系统上实施策略。
- 代理上的属性版本与 ePO 服务器上的属性版本至少差了两个版本。

列出的属性取决于在“McAfee Agent”策略页的“常规”选项卡上选择的是发送全部属性还是发送最少属性。

全部属性

如果指定收集全部属性集，代理将收集以下内容：

- 系统属性：
  - 系统硬件信息
  - 安装的软件信息
  - 处理器速度。
  - 操作系统。
  - 时区。
  - 最近更新属性的日期和时间。
- 产品属性：
  - 安装路径。
  - 检测特征码 (DAT) 文件版本号。
  - 产品版本号。
  - 为每个产品配置的特定策略设置

最少属性

如果您指定仅收集最少属性，则代理仅收集下列产品属性：

- 安装路径。
- 检测特征码 (DAT) 文件版本号。
- 产品版本号。
- 为每个产品配置的特定策略设置

代理策略和分布式资料库

默认情况下，代理可以从其资料库列表 (SITELIST.XML) 文件中的任一资料库进行更新。代理可以使用网络 ICMP ping 命令或资料库的子网地址来确定列表中前五个资料库中响应最快的分布式资料库。通常，这是距离网络中系统最近的分布式资料库。例如，距 ePO 服务器较远的远程地点中的托管系统可能选择本地分布式资料库。相反，与服务器位于相同局域网中的代理可能直接从主资料库进行更新。

如果需要对代理使用的分布式资料库加强控制，则可以在“McAfee Agent”策略页的“资料库”选项卡上启用或禁用特定的分布式资料库。允许代理从任意分布式资料库进行更新可以确保它们一定能从某个位置获取更新。使用网络 ICMP ping 命令，代理会从资料库列表中前五个资料库中

最近的分布式资料库进行更新。每当代理服务 (McAfee Framework Service) 启动或资料库列表发生变化时，代理都会选择资料库。

代理服务器设置

若要访问 McAfee 更新站点，代理必须能访问 Internet。使用代理策略设置配置托管系统的代理服务器设置。“McAfee Agent”策略页的“代理服务器”选项卡包括以下设置：

- 使用 Internet Explorer 代理服务器设置。
- 配置自定义代理服务器设置。
- 禁用任何代理服务器。

默认设置为“使用 Internet Explorer 代理服务器设置”，允许代理使用该系统上安装的 Internet Explorer 浏览器中当前配置的代理服务器位置和凭据信息。不过，您可能需要使用 ePolicy Orchestrator 为网络中的系统配置自定义代理服务器设置。例如，这些系统也许使用不同的浏览器，而没有安装 Internet Explorer 浏览器。

安全密钥

ePolicy Orchestrator 和代理使用密钥安全地进行代理与服务器的通讯，以及对未签名的包进行签名和验证。

代理会在执行代理的下一次更新客户端任务时更新对密钥的更改。

代理与服务器安全通讯密钥

代理使用代理与服务器安全通讯 (ASSC) 密钥安全地与服务器通讯。您可以将任一 ASSC 密钥对设为主要密钥对，即当前分配给已部署代理的密钥对。使用列表中其他密钥的现有代理会在下次更新后更改为新主要密钥。在删除旧密钥前，请务必等到所有代理都更新到新主要密钥为止。

3.6 版之前的代理使用旧版密钥。如果要从早期版本的 ePolicy Orchestrator 升级，则默认情况下可以将旧版密钥设为主要密钥。

主资料库密钥对

主资料库私钥用于对主资料库中所有未经签名的内容进行签名。预计在 McAfee Agent 4.0 中使用这些密钥。

4.0 版或更高版本的代理使用公钥验证源自此 ePO 服务器上主资料库中的资料库内容。如果内容未进行签名，或使用未知资料库专用密钥签名，则会将下载内容视为无效，并将其删除。

对于每个服务器安装，此密钥对是唯一的。但是，通过导出和导入密钥，您可以在多个服务器环境中使用相同的密钥对。

使用这些密钥是一种新功能，而且只有 4.0 版或更高版本的代理符合新协议。

其他资料库公钥

代理可以使用公钥来验证环境中其他主资料库或 McAfee 来源站点提供的内容。向此服务器报告的每个代理都会使用此列表中的密钥来验证来自组织中其他 ePO 服务器或来自 McAfee 所有的来源的内容。

如果代理下载的内容来自代理没有相应公钥的来源，则代理会将内容丢弃。

使用这些密钥是一种新功能，而且只有 4.0 版或更高版本的代理才能使用新协议。

代理分发的方法

由于不同环境有各种不同的情况和要求，因此可以使用多种方法将代理分发到要管理的系统上。在使用以下任一方法前，应先对每种方法进行权衡。

下表详细介绍分发代理不同方法的优缺点。

表 1：代理分发方法的优缺点

方法	优点	缺点
创建目录时部署代理	自动执行，不需要执行其他步骤。	如果通过导入大型 NT 域或 Active Directory 容器来创建站点，可能会产生巨大的网络通讯量来传送资源。
从 ePolicy Orchestrator 部署代理	这是分发代理的一种有效方法。	必须将具有管理员权限的用户凭据嵌入相应的系统。此外，您还必须确保运行 Microsoft XP Service Pack 2 的系统已经将 FRAMEPKG.EXE 文件添加到防火墙例外情况列表中。
使用登录脚本	对于系统频繁登录网络的环境而言，这是一种很有效的方法。只需操作一次即可自动部署代理。	不经常登录网络的系统，运行的可能不是最新的代理。
手动安装	如果您不使用 ePolicy Orchestrator 来部署代理，或者您有很多 Windows 95 和 Windows 98 系统，但是不想在这些系统上启用文件及打印共享，那么这是一种很有效的方法。	如果系统很多，则此方法会很耗时。
将代理包括在映像中	避免了其他形式的分发可能对带宽造成的影响。将此任务集成到其他任务中可以减少开销。	如果您并没有持续使用映像，则此方法不能有效确保覆盖范围达到要求。
在非托管 McAfee 产品上启用代理	节省大量带宽和时间。	禁用的代理可能已过期，因此要求您运行部署任务将代理升级到最新版本。如果您不删除代理并重新安装，则无法更改代理安装文件夹。启用的代理与通过其他一些方法在网络中部署的代理可能位于不同的文件夹。

创建自定义代理安装包

使用此任务可以创建自定义代理安装包。

如果您使用 ePolicy Orchestrator 部署功能之外的方法（如登录脚本或第三方部署软件），则当用户没有本地管理员权限时，必须创建一个含有嵌入管理员凭据的自定义代理安装包 (FRAMEPKG.EXE)。安装代理时将使用嵌入的用户帐户凭据。

注意: 只有在将包文件名添加到 Windows 防火墙的例外情况列表之后，Microsoft Windows XP Service Pack 2 以及更高版本的操作系统才允许使用嵌入的管理员凭据。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”，然后单击“新建系统”。此时会出现“新建系统”页。

2 在“如何添加系统”旁，选择“创建并下载代理安装包”。

3 输入所需的“代理安装的凭据”，然后单击“确定”。

4 出现提示时，选择下载和保存安装包的位置。

5 可以根据需要分发自定义安装包文件。

分发代理

使用这些任务中的任何一个可以在环境中分发代理。您所选的方法取决于环境要求。

任务

- 使用 ePolicy Orchestrator 部署代理
- 通过登录脚本安装代理
- 手动安装代理
- 在非托管 McAfee 产品上启用代理
- 将代理包括在映像中
- 使用其他部署产品
- 将代理分发到 WebShield 设备和 Novell NetWare 服务器

使用 ePolicy Orchestrator 部署代理

使用此任务可以通过 ePolicy Orchestrator 将代理部署到系统。这种方法采用 Windows NT 的推送技术。

如果已填充了大量的系统树部分，则建议使用此方法。例如，如果已通过导入域或 Active Directory 容器来创建系统树部分，且选择在导入过程中不进行部署，则使用此方法。

开始之前

若要使用此方法，则必须满足以下几个要求：

- 必须已将系统添加到系统树。

  注意: 如果尚未创建系统树，则可以在向系统树中添加组和系统的同时，将代理安装包部署到系统。但是，如果通过导入大型 NT 域或 Active Directory 容器来创建系统树，则 McAfee 建议不要执行此过程。这样做可能会导致网络通讯量过大。

- 指定域管理员凭据。必须在某个系统上具有域管理员权限才能访问默认的 Admin$ 共享文件夹。ePO 服务器服务需要访问此共享文件夹，才能安装代理和其他软件。
- 验证 ePO 服务器能否与所需系统进行通讯。

  在开始部署大型代理之前，请使用 ping 命令验证服务器能否与每个网段中的一些系统通讯。

  如果目标系统响应该 ping 命令，则说明 ePolicy Orchestrator 可以到达这些网段。

  注意: 安装代理之后，ePO 服务器并不需要使用 ping 命令测试托管系统，代理与服务器即可进行通讯。这只是一种确定能否从服务器部署代理的有用测试方法。

- 验证能否从服务器访问所需系统上的 Admin$ 共享文件夹。

  此测试还验证管理员凭据，因为如果没有管理员权限，将无法访问远程 Admin$ 共享文件夹。

  要从 ePO 服务器访问所需系统上的 Admin$ 共享，请选择“开始”|“运行”，然后通过指定系统名称或 IP 地址，输入指向客户端 Admin$ 共享的路径。

  如果各系统之间通过网络正确连接，并且您的凭据具有足够权限，同时 Admin$ 共享文件夹也存在，则会出现“Windows 资源管理器”对话框。

- 确保已启用文件及打印共享。默认情况下，在 Windows 95、Windows 98 和 Windows ME 系统上禁用此功能。此外，如果网络中有运行这些操作系统的系统，应确保可由 ePolicy Orchestrator 管理这些系统。默认情况下，这些系统不允许 ePO 管理。要使这些系统能够通过 ePO 进行管理，请从 Microsoft 网站下载 VCREDIST.EXE 和 DCOM 1.3 更新，然后根据需要在每个客户端上安装它们。
- 确保在 Windows XP Home 系统上启用了网络访问。在运行 Windows XP Home 的系统上，若要从 ePolicy Orchestrator 部署代理，或安装自定义代理安装包，您必须启用网络访问。

  要在运行 Windows XP Home 的系统上启用网络访问，请转至“开始”|“控制面板”|“性能和维护”|“管理工具”|“本地安全策略”|“安全设置”|“本地策略”|“安全选项”|“网络访问：本地帐户的共享和安全模式”，然后选择“经典 - 本地用户以自己的身份验证”。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”，然后选择要将代理部署到的组或系统。

2 单击“部署代理”。此时会出现“部署 McAfee Agent”页。

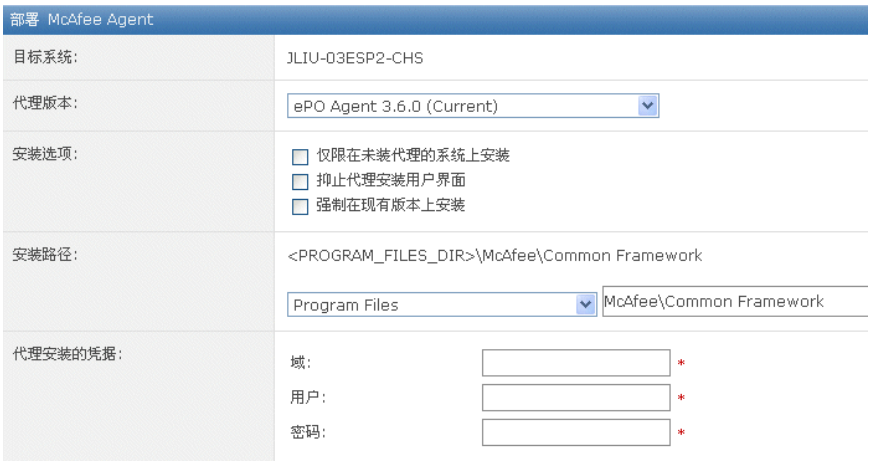

图 16：部署 McAfee Agent 页

3 从下拉列表中选择所需的“代理版本”。

4 如果将代理部署到组，请选择是否包含其子组中的系统。

5 选择是否：

- 仅限在尚未安装由此 ePO 服务器管理的代理的系统上安装
- 抑止代理安装用户界面
- 强制在现有版本上安装

  如果选择“仅限在尚未安装由此 ePO 服务器管理的代理的系统上安装”，则此选项不可用。

注意: 当新代理出现问题，需要重新安装早期版本时，可能需要强制安装。建议仅在降级代理时使用此选项。

6 接收默认的“安装路径”或从下拉列表中选择。

7 指定对系统具有权限的“代理安装的凭据”。

8 单击“确定”将代理安装包发送到选定系统。

通过登录脚本安装代理

使用此任务可以安装并使用网络登录脚本在登录到网络上的系统中安装代理。

使用网络登录脚本是一种可靠的方法，可确保登录到网络的每个系统都运行代理。可以通过创建登录脚本来调用一个批处理文件，检查要登录网络的系统是否已安装代理。如果没有代理，则该批处理文件可以先安装代理，然后再允许系统登录。在安装后的十分钟内，代理会连接到服务器以获取更新策略，同时系统将添加到系统树中。

此方法适用于以下情况：

- 分类过滤器或 NT 域名分配给了系统树部分。
- 您已经有一个托管环境，并想确保登录网络的新系统成为托管系统。
- 您已经有一个托管环境，并想确保系统运行代理的最新版本。

最佳实践

McAfee 建议先使用网络域名或分类过滤器来创建系统树各部分，以将所需系统添加到所需的组。如果不这样做，则所有系统都将添加到“不明来源”组，您必须在以后手动移动它们。

登录脚本的详细信息取决于您的需要。有关编写登录脚本的信息，请参阅操作系统文档。此任务会提供基本示例。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 将服务器上的 FRAMEPKG.EXE 代理安装包复制到网络服务器上所有系统均具有权限的共享文件夹。

   登录到网络的系统会被定向到此文件夹，以便在登录时运行代理安装包并安装代理。

   默认情况下，代理安装包位于以下位置：

   C:\PROGRAM FILES\MCAFEE\EPO\DB\SOFTWARE\CURRENT\ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE

2 创建一个含有嵌入管理员用户凭据的自定义代理安装包。在系统上安装代理需要这些凭据。

3 创建一个批处理文件，内含系统登录网络时要在系统上执行的命令行。此批处理文件的内容因您的需求而异，但用途如下：

   - 检查是否已在所需位置安装了代理。
   - 如果代理不存在，则运行 FRAMEPKG.EXE。

   下面是一个批处理文件示例，它检查是否已安装代理，如果没有安装，则运行 FRAMEPKG.EXE 来安装代理。

   ```
   IF EXIST “C:\Windows\System32\ePOAgent\NAIMAS32.EXE”
   \\<COMPUTER>\<FOLDER>\UPDATE$\FRAMEPKG.EXE /FORCEINSTALL /INSTALL=AGENT
   IF EXIST “C:\ePOAgent\FRAMEWORKSERVICE.EXE” GOTO END_BATCH
   \\MyServer\Agent\UPDATE$\FRAMEPKG.EXE /FORCEINSTALL /INSTALL=AGENT
   :END_BATCH
   ```

   注意: 用于分发的安装文件夹可能与本示例中的文件夹有所不同，具体情况取决于指定安装代理的位置。

   此示例会检查：

   - 2.5.1 旧版代理的默认安装位置，如果该版本存在，则将其升级到 3.5 版代理。
   - 3.5 版代理的默认安装文件夹，如果该版本不存在，则安装新的代理。

4 将 EPO.BAT 批处理文件保存到主域控制器 (PDC) 服务器的 NETLOGON$ 文件夹。每当系统登录到网络时，都会从 PDC 运行该批处理文件。

5 在登录脚本中添加一行，以调用 PDC 服务器上的批处理文件。此命令行与以下示例类似：
CALL \\PDC\NETLOGON$\EPO.BAT

每个系统在登录到网络时都将运行该脚本并安装代理。

手动安装代理

使用此任务可以在系统本地运行安装程序。

对于以下情况，此方法是安装代理的理想方法：

- 您的组织要求在系统上手动安装该软件。
- 您只想用 ePolicy Orchestrator 进行策略管理。
- 您拥有运行 Windows 95、Windows 98 或 Windows ME 的系统，但不想在这些系统上启用文件及打印共享。
- 创建系统树的各部分时指定了 IP 分类过滤器或 NT 域名。

您可以在系统上安装代理，也可以将 FRAMEPKG.EXE 安装程序分发给用户，让他们自己运行安装程序。

安装代理之后，该代理将连接到服务器，并将新的系统添加到系统树中。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 将代理安装包分发到所需系统。

如果您希望最终用户（具有本地管理员权限）在其自己的系统上安装代理，则可以将代理安装包文件分发给他们。您可以采用电子邮件附件的形式发送该文件、将其复制到介质上或保存到共享网络文件夹中。

2 双击 FRAMEPKG.EXE，在代理正在安装时，请稍候。在十分钟内，代理会首次连接到 ePO 服务器。

3 如有必要，请使用 CMDAGENT/p 命令行强制代理连接，不必再等待十分钟。

在非托管 McAfee 产品上启用代理

使用此任务可以在环境中现有的 McAfee 产品上启用代理。

购买 ePolicy Orchestrator 之前，您可能已经在网络中使用过 McAfee Enterprise 产品。某些使用 AutoUpdate 更新程序的较新 McAfee 产品（如 VirusScan Enterprise）在安装时会附带安装此代理，但安装后的代理处于禁用状态。若要开始使用 ePolicy Orchestrator 管理这些产品，则可以启用系统上已有的代理。

在每个系统上启用代理而不是部署 3.63MB 的代理安装包，可以节省大量网络带宽。

注意: 如果您不删除代理并重新安装，则无法更改代理安装文件夹。您启用的代理与通过其他方法在网络中部署的代理可能位于不同的文件夹。

为所需的系统树部分指定分类过滤器或 NT 域名可以节省宝贵的时间。

您必须将 SITELIST.XML 资料库列表文件从 ePO 服务器复制到所需系统。资料库列表包含网络地址信息，代理在安装之后连接到服务器时需要用到这些信息。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 将资料库列表 (SITELIST.XML) 从“主资料库”页导出到系统上的临时文件夹，如 C:\TEMP。

2 在所需系统上运行以下命令：
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML

/SITEINFO 是导出的 SITELIST.XML 文件的位置。

引用临时文件夹中的 SITELIST.XML 文件。默认情况下，FRMINST.EXE 文件安装在以下位置：

C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

注意: 现有的 McAfee 产品很可能与旧版本的代理一起安装。这些代理不会自动升级到 ePO 服务器上的最新版本。请启用并运行配置为在托管系统上升级已启用的代理的部署任务。

将代理包括在映像中

使用此信息可以通过映像安装代理。用户首次登录到使用包含代理的公用映像所建立的系统时，会为该系统指定一个唯一的 ID，即全局唯一标识符 (GUID)。

小心: 在为此目的创建映像之前，请先从代理注册表项中删除代理 GUID 注册表值。GUID 会在代理与 ePO 服务器通讯的第一个 ASCI 期间重新生成。

此方法适用于以下情况：

- 您的组织为新系统使用标准安装映像。
- 只有在环境中的某些系统需要维修时，您才有权访问这些系统。

有关说明，请参阅您首选的映像创建产品的文档。

使用其他部署产品

您可能已经使用其他网络部署产品来部署软件。可以使用许多此类工具来部署代理，如 Microsoft Systems Management Server (SMS)、IBM Tivoli 或 Novell ZENworks。请配置所选部署工具，以分发 ePO 服务器上的 FRAMEPKG.EXE 代理安装包。

有关说明，请参阅所需部署工具的文档。

将代理分发到 WebShield 设备和 Novell NetWare 服务器

您不能使用 ePolicy Orchestrator 将代理分发到 WebShield® 设备或 Novell NetWare 服务器。而应使用登录脚本或手动安装。

这些系统要求使用不同的代理，您可以从 McAfee 网站下载它们。默认情况下，ePO 服务器上未安装这些代理的安装包。

有关详细信息，请参阅产品文档。

强制代理连接到服务器

使用此任务可以强制新代理立即连接到 ePO 服务器。您可以在任何刚安装代理的系统上执行此任务。此任务在手动安装代理后很有用。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 在刚安装代理的系统上，选择“开始”|“运行”，输入 command，然后按 Enter 键打开 DOS 命令窗口。
2 在命令窗口中，找到包含 CMDAGENT.EXE 文件的代理安装文件夹。
3 输入以下命令。
CMDAGENT /p
4 按 Enter 键。代理将立即连接到服务器。

当代理首次连接到服务器时，系统将作为托管系统添加到系统树中。如果已经为系统树配置了基于标准的分类，则系统会添加到与其 IP 地址或标记对应的位置。否则，系统会添加到“不明来源”组中。将系统添加到系统树之后，便可以通过 ePollicy Orchestrator 管理其策略。

升级现有代理

使用这些任务可以升级环境中的现有代理。

如果您一直在使用旧版 ePolicy Orchestrator，并且在环境中存在早期代理版本，则可以在安装 ePO 服务器之后升级这些代理。升级代理的过程取决于在托管系统上运行的早期代理版本。

注意: ePolicy Orchestrator 4.0 并不完全支持某些早期代理版本的功能。要使代理完全发挥作用，请升级到 3.6 Patch 1 或更高版本的代理。

任务

- 使用登录脚本或手动安装升级代理
- 使用 ePolicy Orchestrator 升级代理

使用登录脚本或手动安装升级代理

如果您不使用 ePolicy Orchestrator 将代理或产品部署到托管系统，则可以使用您首选的代理分发方法升级现有代理。如果不使用 ePolicy Orchestrator 升级代理（如手动或使用网络登录脚本升级），则与首次安装代理效果相同。您必须使用首选方法分发 FRAMEPKG.EXE 安装文件，并在系统上启动。

使用 ePolicy Orchestrator 升级代理

使用此任务可以通过“产品部署”客户端任务升级现有代理。此方法可进一步控制升级的位置和时间。此部署任务与将产品（如 VirusScan Enterprise）部署到已运行代理的系统上所使用的部署任务相同。

最佳实践信息

您可以使用该部署任务升级代理。McAfee 会定期发布代理的新版本。您可以通过 ePolicy Orchestrator 部署和管理这些新版本的代理。如果有可用的新版本代理，您可以从 McAfee 更新站点下载代理安装包，并将其签入主资料库。然后使用部署任务来升级代理。

小心: 使用部署任务升级代理与使用更新客户端任务更新现有代理不同。升级代理的目的是在旧版代理的基础上安装新版代理，如在 3.0 版的代理上安装 3.6 版的代理。更新任务会使用其他更新（如 DAT 文件和补丁程序）来更新现有版本的代理，或将代理从 3.0.1 更新到 3.0.2 版。

任务

要获得选项定义，请在包含选项的页面上单击“?”。

1 确保已将所需的代理安装包签入主软件资料库。
2 转至“系统”|“系统树”|“客户端任务”，然后选择系统树中要升级代理的部分。
3 单击“新建任务”。此时会出现“客户端任务构建器”向导的“描述”页。
4 对任务命名，从下拉列表中选择“产品部署(McAfee Agent)”，然后单击“下一步”。此时会出现“配置”页。
5 从下拉列表中选择代理版本。
6 从“操作”下拉列表中选择“安装”。
7 添加任何命令行选项。
8 选择是否在每个策略的实施间隔运行任务。
9 选择是否在成功部署后运行更新任务，然后单击“下一步”。
10 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。
11 确认任务的详细信息，然后单击“保存”。

此任务会添加到系统树中任何分配此任务的客户端任务的列表中。

删除代理

使用这些任务可以从系统中删除代理。

注意: 您不能使用“产品部署”任务删除代理，该任务用于删除诸如 VirusScan Enterprise 等产品。

任务

- 从命令行运行 FRMINST.EXE
- 从系统树中删除系统时删除代理
- 从系统树中删除组时删除代理
- 从查询结果的系统中删除代理

从命令行运行 FRMINST.EXE

使用此任务可以从命令行删除代理。

任务

- 使用 /REMOVE=AGENT 命令行选项运行代理安装 (FRMINST.EXE) 程序。默认情况下，该文件位于：

  C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

从系统树中删除系统时删除代理

使用此任务可以在从系统树中删除系统时，也同时删除系统中的代理。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后在包含您要删除系统的“系统树”下选择组。
2 从列表中选择系统，然后单击页底部的“删除”（您可能须先单击“更多操作”）。

3 在“操作”面板上，选择“删除代理”，然后单击“确定”。

选定系统会从系统树中删除，其代理也会在下次代理与服务器通讯时删除。

从系统树中删除组时删除代理

使用此任务可以在从系统树中删除组时，同时删除该组中所有系统中的代理。

小心: 删除组时，也会删除所有子组和子系统。如果在删除系统时选中“从所有系统中删除代理”复选框，则 ePolicy Orchestrator 会从所有子组中删除代理。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“组”，然后在“系统树”下选择所需的组。

2 单击页底部的“删除组”（您可能须先单击“更多操作”）。此时会出现“删除组”对话框。

3 选择“从所有系统中删除代理”，然后单击“确定”。

所选系统会从系统树中删除，其代理也会在下次代理与服务器通讯时删除。

从查询结果的系统中删除代理

使用此任务可以从查询（如“代理版本摘要”查询）结果列出的系统中删除代理。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 运行所需的查询。

2 从查询结果中选择系统，然后单击页底部的“删除”。

3 在系统提示是否删除代理时，在“操作”面板上，单击“是”。

在下一次代理与服务器进行通讯时将卸载代理。

维护代理

使用这些任务可以确保环境中的代理处于最新状态，并按预期工作。您可能需要定期执行这些任务。

任务

- 手动将唤醒呼叫发送到系统
- 手动将唤醒呼叫发送到组
- 按计划发送唤醒呼叫
- 查看代理活动日志
- 查看代理和产品属性
- 从托管系统运行代理任务
- 使用安全密钥

手动将唤醒呼叫发送到系统

使用此任务可以手动将代理或 SuperAgent 唤醒呼叫发送到系统树中的系统。在进行策略更改并希望代理连接以获取更新时，此功能很有用。

开始之前

在将代理唤醒呼叫发送到系统之前，确保在“McAfee Agent”策略页的“常规”选项卡上启用并应用了系统所在组的唤醒支持（默认情况下启用）。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后选择包含系统的组。

2 从列表中选择系统，然后单击“唤醒代理”。此时会出现“唤醒 McAfee Agent”页。

注意: 您可能需要单击“更多操作”以显示此操作。

图 17：唤醒 McAfee Agent 页

3 确认在“目标系统”旁显示系统。

4 选择是发送“唤醒呼叫类型”旁的“代理唤醒呼叫”还是“SuperAgent 唤醒呼叫”。

5 接受默认值，或输入不同的“随机选择”时间（0 - 60 分钟）。请仔细考虑根据可用带宽所决定的接收唤醒呼叫的系统数量。如果输入 0，则代理会立即响应。

6 在常规通讯时，代理仅发送自上次代理与服务器通讯以来发生变化的属性。默认情况下，此任务设置为“获取完整的产品属性”。若要在此唤醒呼叫后发送全部属性，必须选择此选项。

7 单击“确定”以发送代理或 SuperAgent 唤醒呼叫。

手动将唤醒呼叫发送到组

使用此任务可以手动将代理或 SuperAgent 唤醒呼叫发送到系统树组中。在进行了策略更改并希望代理连接以获取更新时，此功能很有用。

开始之前

在将代理唤醒呼叫发送到此类组之前，确保在“McAfee Agent”策略页的“常规”选项卡上启用并应用了该组的唤醒支持（默认情况下为启用）。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“组”，然后在“系统树”下选择的组。

2 单击“唤醒代理”。此时会出现“唤醒 McAfee Agent”页。

注意: 您可能需要单击“更多操作”以显示此操作。

3 确认在“目标组”旁显示组。

4 选择是将代理唤醒呼叫发送到“此组中的所有系统”还是“此组和子组中的所有系统”。

5 选择是发送“类型”旁的“代理唤醒呼叫”还是“SuperAgent 唤醒呼叫”。

6 接受默认值，或输入不同的“随机选择”时间（0 - 60 分钟）。如果输入 0，则代理会立即响应。

7 在常规通讯时，代理仅发送自上次代理与服务器通讯以来发生变化的属性。默认情况下，此任务设置为“获取完整的产品属性”。若要在此唤醒呼叫后发送全部属性，必须选择此选项。

8 单击“确定”以发送代理或 SuperAgent 唤醒呼叫。

按计划发送唤醒呼叫

使用此任务可以创建计划的代理唤醒呼叫。

注意: SuperAgent 代理唤醒呼叫无法通过安排计划来执行。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“客户端任务”，然后选择将唤醒呼叫发往的组或系统。

2 单击“新建任务”。此时会出现“客户端任务构建器”向导的“描述”页。

3 对任务命名，从下拉列表中选择“代理唤醒呼叫(McAfee Agent)”，然后单击“下一步”。此时会出现“配置”页。

4 选择接收唤醒呼叫的代理是发送全部属性，还是发送最少属性，然后单击“下一步”。

5 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。

6 确认任务详细信息，然后单击“保存”。

完成后，在选定系统树组的“客户端任务”选项卡上的可用任务列表中，会出现计划的任务。如果已启用此任务，则在下个计划的时间，该任务会在接收任务的系统上运行。若要确保全部所需的系统都具有任务信息，请将手动唤醒呼叫发给这些系统。

查看代理活动日志

使用这些任务可以查看代理活动日志。代理活动日志记录代理的活动。详细信息的数量取决于在“McAfee Agent”策略页的“记录”选项卡上选定的策略设置。

可以从托管系统或控制台查看这些日志文件。

任务

- 从托管系统查看代理活动日志
- 从 ePO 服务器中查看代理活动日志

从托管系统查看代理活动日志

使用此任务可以从安装代理的系统查看代理活动日志。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 右键单击系统任务栏中的代理图标。

   注意: 只有在“McAfee Agent”策略页的“常规”选项卡上选择了“显示 McAfee 系统任务栏图标(仅限 Windows)”选项，代理图标才会显示在系统任务栏中。如果该图标不可见，请选择此选项并应用它。查看完日志文件内容之后，可以通过取消选择该选项并应用更改来再次隐藏该图标。

2 从菜单中选择“状态监视器”。状态监视器出现之后，将显示代理活动日志。

3 完成后，请关闭状态监视器。

从 ePO 服务器中查看代理活动日志

使用此任务可以从服务器中查看系统的代理活动日志。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后选择系统。

2 单击“查看代理日志”。

3 若要查看 FrameSvc.exe 或 NaPrdMgr.exe 详细日志的备份副本，请单击“早期”。

   注意: 尽管在默认情况下启用了远程查看日志文件功能，但您可以禁用此功能。如果您无法远程查看日志，请确认在“McAfee Agent”策略页的“记录”选项卡上选择了“启用对日志的远程访问”选项。

查看代理和产品属性

使用此任务可以验证属性是否与所做的策略更改相符。此任务在进行故障排除时很有用。可用的属性取决于在“ePO 代理”策略页上是将代理配置为发送全部属性还是发送最少属性。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后选择系统。

2 单击列表中的系统。此时会显示系统、已安装产品和代理的属性。

从托管系统运行代理任务

使用这些任务可以从安装代理的系统中执行选定的任务。

如果您可以访问安装代理的托管系统，则可以查看并管理代理的某些功能。

注意: 只有在“McAfee Agent”策略页的“常规”选项卡上选中了“显示 McAfee 系统任务栏图标”，托管系统上才会显示代理界面

任务

- 手动运行更新
- 将全部属性发送到 ePO 服务器
- 立即将事件发送到 ePO 服务器

手动运行更新

使用此任务可以从托管系统中运行更新。

任务

1 右键单击 McAfee 系统任务栏图标。

2 选择“McAfee Agent”|“立即更新”。代理从代理策略中确定的资料库中执行更新。

产品更新包括：

- 补丁程序发行版。
- 旧版产品插件 (.DLL) 文件。
- Service Pack 发行版。
- SuperDAT (SDAT*.EXE) 包。
- 补充检测特征码 (EXTRA.DAT) 文件。
- 检测特征码 (DAT) 文件。

将全部属性发送到 ePO 服务器

使用此任务可以将全部属性从托管系统发送到服务器。

任务

1 右键单击托管系统上的 McAfee 系统任务栏图标，然后选择“McAfee Agent”|“状态监视器”。此时会出现“代理状态监视器”。

2 单击“收集并发送属性”。

立即将事件发送到 ePO 服务器

使用此任务可以立即将事件从托管系统发送到服务器。

任务

1 右键单击托管系统上的 McAfee 系统任务栏图标，然后选择“McAfee Agent”|“状态监视器”。此时会出现“McAfee Agent 状态监视器”。

2 单击“发送事件”。

更新策略

使用此任务可以提示代理从托管系统连接到服务器以更新策略设置。

任务

1 右键单击所需系统上的 McAfee 系统任务栏图标，然后选择“McAfee Agent”|“状态监视器”。此时会出现“代理状态监视器”。

2 单击“检查新策略”。

实施策略

使用此任务可以提示代理实施托管系统上所有配置好的策略：

任务

1 右键单击所需系统上的 McAfee 系统任务栏图标，然后选择“McAfee Agent”|“状态监视器”。此时会出现“代理状态监视器”。

2 单击“实施策略”。

查看代理设置

使用此任务可以从托管系统中查看代理设置。

任务

1 右键单击托管系统上的 McAfee 系统任务栏图标。

2 选择“McAfee Agent”|“设置”。
代理设置包括：

- 代理 ID (GUID)。
- 系统名称。
- 登录用户的用户名。
- 策略实施间隔。
- ASCI。

查看代理和产品版本号

使用此过程可以从托管系统查看代理和产品版本号。在安装新代理版本，或确认实际安装的代理版本与服务器上代理属性中显示的版本是否相同时，此方法非常有用。

任务

1 右键单击 McAfee 系统任务栏图标。

2 选择“McAfee Agent”|“关于”。

使用安全密钥

使用这些任务可以使用和管理安全密钥。

任务

- 在多服务器环境中使用 ASSC 密钥
- 生成和使用新 ASSC 密钥
- 导出 ASSC 密钥以允许代理访问多个 ePO 服务器
- 查看使用 ASSC 密钥对的系统
- 将 ASSC 密钥对设为主要密钥对
- 删除 ASSC 密钥

在多服务器环境中使用 ASSC 密钥

使用任一任务可以确保所有代理都可以与环境中任何必需的服务器通讯。

早期版 ePolicy Orchestrator 会使代理轻松地与组织内的多个 ePO 服务器通讯。将 ASSC 密钥导入其他 ePO 服务器，会使由来源 ePO 服务器管理的 3.6 版或更高版本的代理成功与其他 ePO 服务器通讯。

这两个策略可确保代理与多个服务器通讯。对所有 ePO 服务器使用通用主要 ASSC 密钥对，或对每个 ePO 服务器使用不同的主要 ASSC 密钥对，并使每个服务器了解其他服务器的密钥。

任务

对所有服务器和代理使用相同的 ASSC 密钥对

使用此任务可以确保所有 ePO 服务器和代理都使用相同的 ASSC 密钥对。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 从所需的 ePO 服务器导出所需的 ASSC 密钥。
2 将 ASSC 密钥导入所有其他服务器。
3 在所有服务器上将导入的密钥设置为的主要密钥。
4 运行代理更新任务，以便立即让所有代理都使用密钥。
5 在所有代理都使用新密钥后，删除所有无用的密钥。
6 备份所有密钥。

每个 ePO 服务器使用不同的 ASSC 密钥对

使用此任务可以在每个 ePO 服务器都需要唯一 ASSC 密钥对的环境中，确保所有代理都可以与任何需要的服务器通讯。

通过将所需密钥对导入代理可以与其通讯的所有服务器，可以确保代理可以与多个服务器进行通讯。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 从环境中每个 ePO 服务器中导出主 ASSC 密钥对。
2 将这些密钥分别导入各服务器。

生成和使用新 ASSC 密钥

使用此任务可以生成新的代理与服务器安全通讯 (ASSC) 密钥。 如果发现密钥遭损坏，则可以生成新密钥。McAfee 建议定期创建和使用新 ASSC 密钥，例如每三个月使用一个。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，然后在“设置类别”列表中选择“安全密钥”。

2 单击详细信息窗格中的“编辑”。此时会出现“编辑安全密钥”页。

3 单击“代理与服务器安全通讯密钥”列表旁的“新建密钥”。

4 如果希望代理使用新密钥，请在列表中选择密钥，然后单击“设为主要密钥”。

   3.6 版或更高版本的代理在其下一个任务完成后，会在第一次代理与服务器通讯时开始使用新密钥。

5 只有在所有代理都停止使用旧密钥后，才能将其删除。

   列表中每个密钥的右侧是当前使用此密钥的代理的数量。

6 备份所有密钥

导出 ASSC 密钥以允许代理访问多个 ePO 服务器

使用此任务可以导出 ASSC 密钥，供环境中的其他 ePO 服务器使用。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，然后在“设置类别”列表中选择“安全密钥”。

2 在详细信息窗格中，单击“编辑”。

3 在“代理与服务器安全通讯密钥”列表中，选择所需的密钥，然后单击“导出”。此时会出现“导出代理与服务器通讯密钥”对话框。

4 单击“确定”。此时会出现“文件下载”对话框。

5 单击“保存”，然后浏览到保存 ZIP 文件的位置。

6 根据需要更改文件的名称，然后单击“保存”。

查看使用 ASSC 密钥对的系统

使用此任务可以查看其代理使用“代理与服务器安全通讯密钥”列表中特定 ASSC 密钥对的系统。您在将其他密钥对设为主要密钥对后，可能希望查看仍使用先前密钥对的系统。如果您了解代理都不使用某个密钥对，请删除该密钥对。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，在“设置类别”列表中选择“安全密钥”，然后单击“编辑”。

2 在“代理与服务器安全通讯密钥”列表中，选择所需的密钥，然后单击“查看代理”。

此时会出现“使用 ASSC 密钥对的系统”页。此页会显示一个标准表，列出代理正在使用所选密钥的所有系统。单击列表中的任何系统可查看其详细信息，或选择所需系统旁的复选框，采取表下任何可用的操作。

将 ASSC 密钥对设为主要密钥对

使用此任务可以将“代理与服务器安全通讯密钥”列表中列出的其他密钥对设置为主要密钥对。请在导入或生成新密钥对后执行此操作。

只有当环境中没有安装 3.6 版或更高版本的代理，才将旧版密钥对设为主要密钥对。新版代理无法使用旧版密钥对。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，在“设置类别”列表中选择“安全密钥”，然后单击“编辑”。

2 在“代理与服务器安全通讯密钥”列表中选择所需的密钥，然后单击“设为主要密钥”。

3 如果需要，可以为代理创建可立即运行的更新任务，以便代理在下次代理与服务器通讯时更新。

   注意: 在从列表中删除早期主要密钥对前，请等到所有代理都开始使用新主要密钥对为止。在代理的下一次更新任务完成后，代理开始使用新密钥对。您可以随时查看哪些代理正在使用列表中的任一 ASSC 密钥对。

4 备份所有密钥。

删除 ASSC 密钥

使用此任务可以删除“代理与服务器安全通讯密钥”中未使用的 ASSC 密钥。

小心: 请不要删除当前任何代理使用的任何密钥，否则这些代理便无法与服务器通讯。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，在“设置类别”列表中选择“安全密钥”，然后单击“编辑”。

2 在“代理与服务器安全通讯密钥”列表中选择所需的密钥，然后单击“删除”。此时会出现“删除密钥”对话框。

3 单击“确定”以从此服务器中删除密钥对。

在多服务器环境中使用主资料库密钥

使用这些任务可以确保 3.6 或更高版本的代理可以使用来自环境中 ePO 服务器中的内容。

服务器会使用主资料库私钥对签入资料库的所有未签名的内容进行签名。代理使用主资料库公钥来验证从组织中的资料库或 McAfee 来源站点检索的内容。

每个安装的主要密钥对都是唯一的。如果您使用多服务器，则每个服务器使用不同的密钥。如果您的代理可能会下载来自不同主资料库的内容，则必须确保代理（4.0 或更高版本）将内容识别为有效内容。

可以通过两种方法确保这一点：

- 对所有服务器和代理使用相同的主资料库密钥对
- 确保将代理配置为识别环境中使用的任何资料库公钥。

任务

- 对所有服务器使用一个主资料库密钥对
- 确保代理可以使用其他 ePO 服务器中的内容

对所有服务器使用一个主资料库密钥对

使用此任务可以确保多服务器环境中的所有 ePO 服务器和代理都使用相同的主资料库密钥对。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至要将其 SC 密钥对用于环境中所有服务器的服务器上的“配置”|“服务器设置”，在“设置类别”列表中选择“安全密钥”，然后单击“编辑”。
2 在“本地主资料库密钥对”旁，单击“导出密钥对”。此时会出现“导出主资料库密钥对”对话框。
3 单击“确定”。此时会出现“文件下载”对话框。
4 单击“保存”。此时会出现“另存为”对话框。
5 浏览到保存包含 SC 密钥文件的 ZIP 文件所在的位置。此位置应为其他服务器可以访问的位置，然后单击“保存”。
6 转至环境中其他服务器的上“配置”|“服务器设置”，在“设置类别”列表中选择“安全密钥”，然后单击“编辑”。
7 单击“导入和备份密钥”旁的“导入”。此时会出现“导入密钥”向导。
8 浏览到包含导出主资料库密钥文件的 ZIP 文件，然后单击“下一步”。
9 确认这些密钥是要导入的密钥，然后单击“保存”。

导入的主资料库密钥对会替换现有的主资料库密钥对。代理在下一次代理更新任务时开始使用主资料库密钥对。

确保代理可以使用其他 ePO 服务器中的内容

使用此任务可以在每个服务器使用不同主资料库密钥的情况下，确保代理可以使用来自多服务器环境中其他 ePO 服务器的内容。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至环境中每个服务器的“配置”|“服务器设置”，在“设置类别”列表中选择“安全密钥”，然后单击“编辑”。
2 在“本地主资料库密钥对”旁，单击“导出公钥”。此时将出现“导出主资料库公钥”对话框。
3 单击“确定”。此时会出现“文件下载”对话框。
4 单击“保存”。此时会出现“另存为”对话框。
5 浏览到保存包含密钥文件的 ZIP 文件所在的位置。此位置是其他服务器可以访问的位置，然后单击“保存”。
6 在从每个服务器中导出公钥后，转至每个服务器上的“配置”|“服务器设置”，在“设置类别”列表中选择“安全密钥”，然后单击“编辑”。
7 单击“导入和备份密钥”旁的“导入”。此时会出现“导入密钥”对话框。
8 浏览到包含导出的 ZIP 文件的位置，选择文件，然后单击“下一步”。
9 确认这是所需的主资料库公钥，然后单击“保存”。
10 重复此步骤，直到环境中所用的所有主资料库公钥都导入每个服务器为止。

在下一次代理更新任务完成后，代理会在环境中识别由主资料库私钥签名的内容。

备份和还原安全密钥

使用这些任务可以备份和还原安全密钥。McAfee 建议定期备份所有安全密钥，并将其存储在安全的网络位置，万一 ePO 服务器丢失密钥，还可以轻松将其还原。

注意: McAfee 建议先备份所有密钥，然后再对密钥管理设置进行任何更改。

任务

- 备份所有安全密钥
- 从备份文件还原安全密钥

备份所有安全密钥

使用此任务可以备份当前在此 ePO 服务器上管理的所有安全密钥。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，从“设置类别”列表中选择“安全密钥”，然后单击“编辑”。此时会出现“编辑安全密钥”页。
2 单击靠近页底部的“全部备份”。此时会出现“文件下载”对话框。
3 单击“保存”。此时会出现“另存为”对话框。
4 浏览到要存储 ZIP 文件的安全网络位置，然后单击“保存”。

从备份文件还原安全密钥

使用此任务可以从备份文件还原所有安全密钥。

开始之前

您必须已创建了所有密钥的备份 ZIP 文件。

小心: 还原安全密钥会删除所有现有密钥，并用备份 ZIP 文件中的密钥取代。所需的密钥必须在备份文件中。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，从“设置类别”列表中选择“安全密钥”，然后单击“编辑”。此时会出现“编辑安全密钥”页。
2 单击页底部的“全部还原”。此时会出现“还原安全密钥”向导。
3 浏览到备份的 ZIP 文件并选择此文件，然后单击“下一步”。
4 确认此文件中的密钥是要用来覆盖现有密钥的版本，然后单击“还原”。

代理命令行选项

使用命令代理 (CMDAGENT.EXE) 工具可以从托管系统执行选定的代理任务。CMDAGENT.EXE 会在安装代理时安装在托管系统上。使用此程序或 McAfee 系统任务栏图标可以在托管系统本地执行此任务。

CMDAGENT.EXE 文件位于代理安装文件夹中。默认情况下，此位置为：

C:\PROGRAM FILES\MCAFEE\COMMON FRAMEWORK

选项定义

选项	描述
/C	检查新策略。代理与 ePO 服务器通讯来获取新策略或更新过的策略，然后在收到这些策略时立即实施。
/E	提示代理本地实施策略。
/P	将属性和事件发送到 ePO 服务器。
/S	显示代理监视器。

代理安装命令行选项

在运行代理安装包 (FRAMEPKG.EXE) 或代理框架安装 (FRMINST.EXE) 程序时，您可以使用以下命令行选项（取决于是否已安装代理）。

当您使用部署任务升级到代理的新版本时，可以使用这些命令行选项。

下表介绍所有代理安装命令行选项。这些选项不区分大小写，但它们的值是区分大小写的。

FRAMEPKG.EXE 和 FRMINST.EXE 命令行选项

命令	描述
/DATADIR	指定系统上用于存储代理数据文件的文件夹。默认位置为：<Documents and Settings>\All Users\Application Data\McAfee\Common Framework。如果操作系统没有 Documents and Settings 文件夹，则默认位置为代理安装文件夹内的 Data 文件夹。 示例：FRAMEPKG /INSTALL=AGENT /DATADIR=<AGENT DATA PATH>
/DOMAIN/USERNAME/PASSWORD	指定 NT 域以及用于安装代理的帐户凭据。该帐户必须具有在所需系统上创建和启动服务的权限。如果保留为未指定，则会使用当前登录帐户的凭据。如果要使用所需系统的本地帐户，请将系统名称用作域。 示例：FRAMEPKG /INSTALL=AGENT /DOMAIN=Domain1 /USERNAME=jdoe /PASSWORD=password
/FORCEINSTALL	指定卸载现有代理，然后安装新代理。使用此选项只能更改安装目录或降级代理。使用此选项时，McAfee 建议为新安装指定其他目录 (/INSTDIR)。 示例：FRAMEPKG /INSTALL=AGENT /FORCEINSTALL /INSTDIR=c:newagentdirectory
/INSTALL=AGENT	安装并启用代理。 示例：FRAMEPKG /INSTALL=AGENT
/INSTALL=UPDATER	如果已安装 AutoUpdate 7.0 组件，且不会更改代理的启用状态，则启用它。此命令行选项可以升级代理。 示例：FRAMEPKG /NSTALL=UPDATER
/INSTDIR	指定所需系统上的安装文件夹。可以使用 Windows 系统变量，如 <SYSTEM_DRIVE>。如果未指定，则默认位置为 <DRIVE>:\program files\mcafee\common framework。 示例：FRAMEPKG /INSTALL=AGENT /INSTDIR=C:\ePOAgent

命令	描述
/REMOVE=AGENT	禁用代理，并在没有使用时将其删除。 示例：FRMINST /REMOVE=AGENT
/SILENT 或 /S	在静默模式下安装代理，即最终用户看不到安装界面。 示例：FRAMEPKG /INSTALL=AGENT /SILENT
/SITEINFO	指定特定资料库列表 (SITELIST.XML) 文件的文件夹路径。 示例：FRAMEPKG /INSTALL=AGENT /SITEINFO=C:\MYSITELIST.XML
/USELANGUAGE	指定要安装的代理的语言版本。如果选择的区域设置不属于具有区域 ID 的 12 种语言，则软件会以英文显示。如果安装多语言版本，则在操作系统中选定的区域设置决定所显示的语言版本。 示例：FRAMEPKG /INSTALL=AGENT /USELANGUAGE 0404

创建资料库

安全软件只有在安装了最新的更新时才会发挥有效的作用。例如，如果 DAT 文件已过期，则即使最好的防病毒软件也无法检查到新的威胁。因此，开发一个强大的更新策略来使您的安全软件保持最新状态是非常重要的。

ePolicy Orchestrator 软件的资料库架构具有很大的灵活性，可以确保在环境允许的情况下轻松地自动部署和更新软件。有了资料库基础架构之后，即可创建用于确定软件更新的方式、位置和时间的更新任务。

是否首次创建资料库？

如果首次创建并设置资料库，请：

1 了解每个类型的资料库、资料库分支和站点的用途。

2 确定要使用的资料库类型及其位置。

3 创建并填充资料库。

目录

资料库类型及其功能

为了将产品和更新传递到整个网络，ePolicy Orchestrator 提供了几种类型的资料库，同时使用这几种资料库可以创建强大的更新基础架构。使用这些类型的资料库可以灵活性地设计更新策略，以确保系统保持最新状态。

主资料库

主资料库会在环境中维护最新版本的安全软件和更新。此资料库是环境中其余系统的软件和更新的来源。每个 ePolicy Orchestrator 服务器都有一个主资料库。

主资料库在安装时配置。但是，必须确保正确配置了代理服务器设置。默认情况下，ePolicy Orchestrator 使用 Microsoft Internet Explorer 代理服务器设置。

分布式资料库

分布式资料库存放主资料库内容的副本。请考虑使用分布式资料库，并将其策略性地放置于整个网络中，以确保托管系统能得到更新，同时最大限度地降低网络通讯量（特别是在连接速度很慢的情况下）。

在更新主资料库时，ePolicy Orchestrator 会将内容复制到分布式资料库。

复制可以：

- 在通过全局更新将指定的包类型签入主资料库时自动进行。
- 在重复计划包含复制任务时进行。
- 通过运行“立即复制”任务手动进行。

大型组织可能有多个办公地点，各个地点之间采用有限带宽连接。分布式资料库会限制低带宽连接上的更新通讯量。如果在远程位置创建分布式资料库，并将远程位置中的系统配置为从此分布式资料库进行更新，则只需通过慢速连接将更新复制到此分布式资料库一次，而不必复制到远程位置中的每个系统一次。

如果启用全局更新，则只要选定的更新和包签入主资料库，分布式资料库就会自动更新托管系统。您不必花费额外的时间来创建和配置资料库或更新任务。

来源站点

来源站点会为主资料库提供所有更新。默认的来源站点为 McAfee HTTP 更新站点 (HttpSite)，但您可以根据需要更改来源站点，也可以创建多个来源站点。McAfee 建议使用 McAfee HTTP (HttpSite) 或 FTP (FTPSite) 更新站点作为来源站点。

注意: 来源站点不是必需的。您可以手动下载更新，然后将这些更新签入主资料库。然而，使用来源站点可自动执行此过程。

McAfee 会定期在这些站点上发布软件更新。例如，每天发布 DAT 文件。请在更新可用时，使用它们来更新主资料库。

可以使用纳入任务将来源站点内容复制到主资料库。

McAfee 更新站点提供检测特征码 (DAT) 和扫描引擎文件更新，还提供一些语言包。您必须手动将所有其他包和更新签入主资料库。

备用站点

备用站点是一种已启用作为备用的来源站点，当托管系统无法访问常用的资料库时，可以从备用站点中检索更新。例如，当网络中断或病毒发作时，访问已建立的位置可能很困难。因此，在这种情况下，托管系统可以通过备用站点来保持最新状态。默认的备用站点是 McAfee HTTP (McAfeeHttp) 更新站点。您只能启用一个备用站点。

如果托管系统使用代理服务器来访问 Internet，则必须为这些系统配置代理策略设置，以使其在访问此备用站点时使用代理服务器。

分布式资料库的类型

ePolicy Orchestrator 支持四种类型的分布式资料库。在确定要使用的分布式资料库类型时，要考虑到您所处的环境和需求。根据您的网络，您不限于只使用一种类型，而可能需要使用多种类型。

SuperAgent 资料库

将存放 SuperAgent 的系统用作分布式资料库。SuperAgent 资料库与其他类型的分布式资料库相比具有以下几个优势：

- 在将资料库添加到资料库列表之前，会先在主机系统上自动创建文件夹位置。

- 自动启用 SuperAgent 资料库文件夹的文件共享。
- SuperAgent 资料库不需要其他复制或更新凭据，其帐户权限是在代理转换为 SuperAgent 时创建的。

  提示: 尽管 SuperAgent 广播唤醒呼叫功能要求在每个广播网段中都有 SuperAgent，但是对于 SuperAgent 资料库功能没有这种要求。托管系统只需要“看到”资料库所在的系统即可。

- SuperAgent 和全局更新使用一种专用协议 SPIPE。

  提示: McAfee 建议将 SuperAgent 资料库和全局更新结合使用，以确保托管环境保持最新状态。

FTP 资料库

如果无法使用 SuperAgent 资料库，请使用现有的 FTP 服务器来存放分布式资料库。可以使用现有的 FTP 服务器软件（如 Microsoft Internet 信息服务 (IIS)）创建新文件夹和站点位置来存放分布式资料库。有关详细信息，请参阅 Web 服务器文档。

HTTP 资料库

如果您无法使用 SuperAgent 资料库，请使用现有的 HTTP 服务器来存放分布式资料库。可以使用现有的 HTTP 服务器软件（如 Microsoft Internet 信息服务 (IIS)）创建新文件夹和站点位置来存放分布式资料库。有关详细信息，请参阅 Web 服务器文档。

UNC 共享资料库

如果您无法使用 SuperAgent 资料库，可以在现有服务器上创建 UNC 共享文件夹来存放分布式资料库。请确保在网络上启用该文件夹的共享功能，以便 ePolicy Orchestrator 服务器可以将文件复制到其中。

非托管资料库

如果您无法使用托管分布式资料库，则 ePolicy Orchestrator 管理员可以创建和维护未由 ePolicy Orchestrator 管理的分布式资料库。

如果某个分布式资料库不受管理，则本地管理员必须手动使该资料库保持最新状态。

创建分布式资料库之后，可以使用 ePolicy Orchestrator 将特定系统树组的托管系统配置为通过该资料库进行更新。

提示: McAfee 建议您通过 ePolicy Orchestrator 来管理所有分布式资料库。通过这种方法并经常使用全局更新或计划复制任务，可确保托管环境保持最新状态。仅当您的网络或组织策略不允许使用托管分布式资料库的情况下，才能使用非托管资料库。

资料库分支及其用途

ePolicy Orchestrator 提供了三种资料库分支，从而可以在主资料库和分布式资料库中维护三个版本的所有包。资料库分支包括“当前”、“早期”和“评估”。默认情况下，ePolicy Orchestrator 只使用“当前”分支。您可以在将包添加到主资料库时指定分支。您也可以在运行或计划更新和部署任务时指定分支，将不同版本分发到网络的不同部分。

更新任务可以从资料库的任何分支检索更新，但是部署任务只使用“当前”分支。

若要使用“评估”分支和“早期”分支获取包而非更新，则必须在“资料库包”服务器设置中将其选中。3.6 版和早期版代理只能从“评估”分支和“早期”分支中检索更新包。

当前分支

“当前”分支是主要的资料库分支，其中包含最新的包和更新。产品部署包只能添加到“当前”分支中。

评估分支

在将新 DAT 和引擎更新部署到整个组织之前，您可能希望先在少数网段或系统中对其进行测试。在将新 DAT 和引擎签入主资料库时，请指定评估分支，然后将其部署到少数测试系统。对测试系统监控数小时后，可以将新 DAT 添加到当前分支并将其部署到整个组织。

早期分支

使用“早期”分支可以在将新 DAT 和引擎文件添加到“当前”分支之前，保存和存储上一周的 DAT 和引擎文件。当环境中的新 DAT 或引擎文件出现问题时，您可以根据需要将早期版本重新部署到系统中。ePolicy Orchestrator 只保存每种文件类型最近的早期版本。

在将新文件添加到主资料库时，可以选择“将现有包移动到‘早期’分支”来启用早期分支。从来源站点纳入更新及手动将包签入主资料库时，均可使用该选项。

资料库列表文件及其使用

资料库列表 (SITELIST.XML) 文件包含您管理的所有资料库的名称。资料库列表包含位置和加密网络凭据，托管系统使用这些信息来选择资料库和检索更新。服务器在代理与服务器通讯期间将资料库列表发送给代理。

如果需要，可以将资料库列表导出到外部文件（SITELIST.XML 或 SITEMGR.XML）。

使用导出的 SITELIST.XML 文件可以：

- 备份和还原资料库列表（如果需要重新安装服务器的话）。
- 在安装时导入产品（如 VirusScan Enterprise）。
- 在安装时导入到代理。
- 从早期安装的 ePolicy Orchestrator 或另一 McAfee 产品导入资料库列表。

使用导出的 SITEMGR.XML 文件可以：

- 备份和还原分布式资料库和来源站点（如果需要重新安装服务器的话）。
- 从早期安装的 ePolicy Orchestrator 中导入分布式资料库和来源站点。

资料库如何协同工作

在您的环境中，各资料库协同工作，将更新和软件提交给托管系统。您可能需要分布式资料库，也可能不需要。

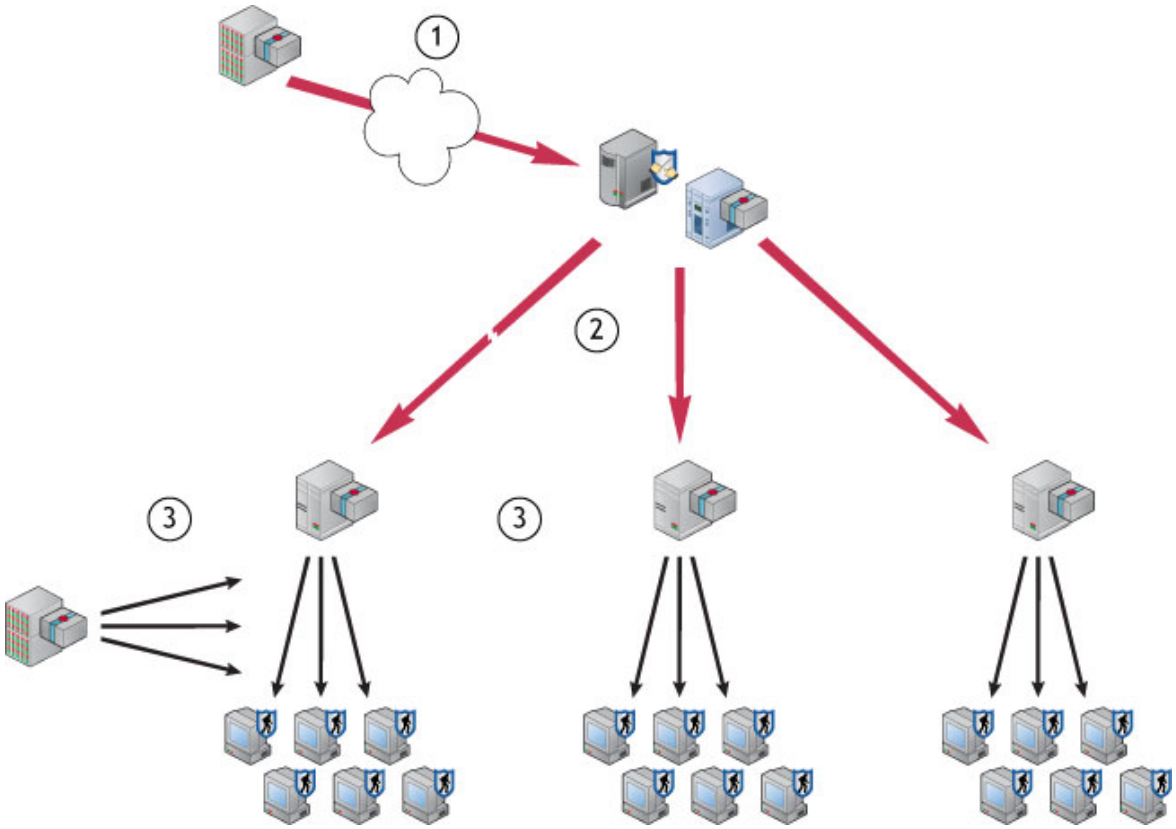

图 18：站点和资料库将包传给系统

1 主资料库会定期从来源站点纳入 DAT 和引擎更新文件。

2 主资料库将更新复制到本地局域网中的托管系统，以及网络的分布式资料库中。

3 网络中的托管系统从附近的资料库检索更新。如果托管系统无法访问分布式资料库或主资料库，则会从备用站点检索更新。

确保访问来源站点

使用这些任务可以确保在将 McAfeeHttp 和 McAfeeFtp 站点用作来源站点和备用站点时，主资料库和托管系统可以访问 Internet。McAfee 建议使用 Internet Explorer 的代理服务器设置。

您还可以在控制台配置代理服务器设置。如果无法使用 Internet Explorer 浏览器中的代理服务器设置，或者您未使用代理服务器，则可能需要执行此操作。

任务

- 对主资料库使用 Internet Explorer 代理服务器设置
- 配置主资料库的自定义代理服务器设置

对主资料库使用 Internet Explorer 代理服务器设置

使用这些任务可以将 Internet Explorer 和 ePolicy Orchestrator 配置为使用 Internet Explorer 的代理服务器设置。如果必须通过 Internet 访问来源站点（如 McAfee 更新站点），则主资料库会使用代理服务器设置来检索包。如果您的组织使用代理服务器连接到 Internet，则您必须使用代理服务器。

默认情况下，ePO 配置为使用 ePO 服务器上安装的 Internet Explorer 浏览器的代理服务器设置。

注意: 使用 Internet Explorer 代理服务器设置时，用户必须登录 ePO 服务器系统来运行计划的任务。如果不希望某个帐户登录到服务器（即使已锁定），则必须手动输入代理服务器身份验证信息。

任务

- 配置 Internet Explorer 代理服务器设置
- 配置 ePolicy Orchestrator 使用 Internet Explorer 代理服务器设置

配置 Internet Explorer 代理服务器设置

如果无法从服务器系统访问 Internet，则使用此任务可以配置 Internet Explorer 中的 LAN 和代理服务器设置。

开始之前

使用此任务之前，可以确认已正确配置这些 Internet Explorer 设置。在服务器上启动 Internet Explorer，并浏览 www.mcafee.com。如果可以访问此站点，则代理服务器设置配置正确。

任务

1 启动 Internet Explorer。
2 从菜单栏中选择“工具”|“Internet 选项”。
3 选择“连接”选项卡，然后在该对话框的底部选择“局域网设置”。
4 在“局域网设置”对话框中，选择“为 LAN 使用代理服务器”。
5 单击“高级”。此时会出现“代理服务器设置”对话框。
6 将代理服务器信息输入相应的字段中。若要使用默认来源站点和备用站点，请输入 HTTP 和 FTP 的信息。
7 选中“对所有协议均使用相同的代理服务器”，以使 FTP 和 HTTP 均可正确使用代理服务器。
8 单击“确定”以关闭“代理服务器设置”对话框。
9 选择“对于本地地址不使用代理服务器”选项。
10 单击“确定”以关闭“局域网设置”对话框。
11 单击“确定”以关闭“Internet 选项”对话框。

配置 ePolicy Orchestrator 使用 Internet Explorer 代理服务器设置

使用此任务可以将 ePolicy Orchestrator 配置为使用 Internet Explorer 的代理服务器设置。此为默认设置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”，然后单击“配置代理服务器设置”。此时会出现“配置代理服务器设置”页。

图 19：配置代理服务器设置页

2 确保选中“类型”旁的“使用 Internet Explorer 设置”。

3 单击“确定”。

配置主资料库的自定义代理服务器设置

如果必须使用主资料库的自定义代理服务器设置，请使用此任务。如果 ePolicy Orchestrator 无法使用 Internet Explorer 浏览器中的代理服务器设置，或不使用代理服务器，则必须配置代理服务器设置或选择不使用代理服务器设置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”，然后单击“配置代理服务器设置”。此时会出现“配置代理服务器设置”页。

2 选择“手动配置代理服务器设置”。
如果服务器不需要代理服务器来访问 Internet，则选择“不使用代理服务器”设置，然后单击“确定”。

3 在“代理服务器身份验证”旁，根据是从 HTTP 资料库、FTP 资料库，还是同时从两种资料库纳入更新来配置相应的设置。

4 在“代理服务器”旁，选择是对所有通讯使用一个代理服务器，还是对 HTTP 和 FTP 代理服务器分别使用不同的代理服务器。然后，输入代理服务器的“地址”（IP 地址或全限定域名）和“端口”号。

注意: 如果使用的是默认来源站点和备用站点，或者要配置另一个 HTTP 来源站点和 FTP 备用站点（反之亦然），请在此处配置 HTTP 和 FTP 代理服务器身份验证信息。

5 在“排除项”旁，选择“绕过本地地址”，然后指定服务器可以直接连接到的所有分布式资料库，方法是输入这些系统的 IP 地址或全限定域名，中间用分号格开。

6 单击“确定”以保存这些设置。

使用来源站点和备用站点

使用这些任务可以更改默认的来源站点和备用站点。只有全局管理员才能定义、更改或删除来源站点或备用站点。您可以编辑设置，删除现有的来源站点和备用站点，或者在这两种站点之间进行切换。

McAfee 建议使用默认的来源站点和备用站点。如果需要使用不同的站点来达到此目的，则可以创建新站点。

任务

- 切换来源站点和备用站点
- 创建来源站点
- 编辑来源站点和备用站点
- 删除来源站点或备用站点

切换来源站点和备用站点

使用此任务可以更改将哪些资料库作为来源站点和备用站点。根据网络配置情况，您可能会发现通过 HTTP 或 FTP 进行更新效果会更好。因此，您可能要在来源站点和备用站点之间进行切换。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“来源站点”。此时会出现可用作来源站点或备用站点的所有站点的列表。

图 20：来源站点选项卡

2 在列表中找到要作为备用的站点，然后单击其旁边的“启用备用”。

创建来源站点

使用此任务可以创建新的来源站点。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 请转至“软件”|“来源站点”，然后单击“新建来源站点”。此时会出现“来源站点构建器”向导。

2 在“描述”页上，输入唯一名称，选择“HTTP”、“UNC”或“FTP”，然后单击“下一步”。

3 在“服务器”页上，提供站点的地址和端口信息，然后单击“下一步”。

- 如果选择了“FTP”，请在“URL”中输入 Web 地址，在“端口”中输入 FTP 端口号。
- 如果选择了“HTTP”，请在“URL”中输入 Web 地址，在“端口”中输入 HTTP 端口号。（您也可以在“URL”文本框中输入服务器名称或 IP 地址。）
- 如果选择了“UNC”，请在“复制 UNC 路径”中输入站点所在的网络目录。请使用此格式：\\<计算机>\<文件夹>。可以使用变量定义此位置。

4 在“凭据”页上，提供托管系统用来连接到此资料库的下载凭据，然后单击“下一步”。请使用对存放站点的 HTTP 服务器、FTP 服务器或 UNC 共享具有只读权限的凭据。

- 如果选择了“FTP”，请选择“匿名”或“FTP 身份验证”（如果服务器要求身份验证），然后在“用户名”、“密码”和“确认密码”中输入用户帐户信息。
- 如果选择了“HTTP”，请选择“匿名”或“HTTP 身份验证”（如果服务器要求身份验证），然后在“用户名”、“密码”和“确认密码”中输入用户帐户信息。
- 如果选择了“UNC”，请在“域”、“用户名”、“密码”和“确认密码”中，输入用户帐户信息。

若要对您指定的用户帐户进行测试，请单击“测试凭据”。

5 单击“下一步”此时会出现“摘要”页。

6 单击“保存”将站点添加到列表中。

编辑来源站点和备用站点

使用此任务可以编辑来源站点或备用站点的设置，如 URL 地址、端口号和下载身份验证凭据。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“来源站点”。此时会出现可以用作来源站点或备用站点的所有站点的列表。

图 21：来源站点选项卡

2 在列表中找到站点，然后单击其旁边的“编辑设置”。此时会出现“来源站点构建器”向导。

3 根据需要编辑向导页上的设置，然后单击“保存”。

删除来源站点或备用站点

使用此任务可以删除来源站点或备用站点。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 请转至“软件”|“来源站点”，然后单击站点旁的“删除”。此时会出现“删除来源站点”对话框。

2 单击“确定”。

此站点随即从“来源站点”页中删除。

将 SuperAgent 用作分布式资料库

使用这些任务可以在 SuperAgent 所在的系统上创建和配置资料库。只有代理分发所需的系统之后，您才可以创建资料库。

任务

- 创建 SuperAgent 资料库
- 选择要复制到 SuperAgent 资料库的包
- 删除 SuperAgent 分布式资料库

创建 SuperAgent 资料库

使用此任务可以创建 SuperAgent 资料库。所需的系统必须安装有 ePO 代理并正在运行。McAfee 建议将 SuperAgent 资料库与全局更新结合起来使用。

此任务假定您了解所需系统在系统树中的位置。McAfee 建议创建“SuperAgent”标记，这样便可以使用“标记目录”页或通过运行查询来轻松查找系统。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，从“产品”下拉列表中选择“McAfee Agent”，然后从“类别”下拉列表中选择“常规”。

2 创建新策略，复制现有策略，或打开已应用到存放 SuperAgent 的系统（要存放 SuperAgent 资料库的系统）的策略。

3 选择“常规”选项卡，然后确保选中“将代理转换为 SuperAgent”。

4 选中“将运行 SuperAgent 的系统用作分布式资料库”，然后输入资料库的文件夹路径位置。在复制期间，主资料库会将更新复制到此位置。您可以使用标准的 Windows 变量，如 <PROGRAM_FILES_DIR>。

   注意: 通过此 SuperAgent 资料库进行更新的托管系统可以访问此文件夹。无需手动启用文件共享。

5 单击“保存”。

6 将此策略分配给每个要存放 SuperAgent 资料库的系统。

代理在下一次连接到服务器时，会检索新的配置。创建分布式资料库后，如果您指定的文件夹不存在，则会在系统上创建该文件夹。如果 ePolicy Orchestrator 无法创建您指定的文件夹，则将创建以下两个文件夹中的一个：

- <DOCUMENTS AND SETTINGS>\ ALL USERS\APPLICATION DATA\MCAFEE\FRAMEWORK\DB\SOFTWARE
- <AGENT INSTALLATION PATH>\DATA\DB\SOFTWARE

另外，此位置将添加到资料库列表 (SITELIST.XML) 文件中。这样，整个托管环境中的系统均可通过该站点进行更新。

如果不想等到下一次代理与服务器通讯，则可以将代理唤醒呼叫发送到所需的系统。

选择要复制到 SuperAgent 资料库的包

使用此任务可以选择将哪些资料库特定的包复制到任一分布式资料库。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库”。此时会出现所有分布式资料库的列表。

2 找到所需 SuperAgent 资料库，然后单击“操作”下的“编辑包类型”。

3 根据需要选择包类型。

注意: 确保选择了任一使用此资料库的托管系统所需的所有包。托管系统会转到一个资料库获取所有包，如果系统所要查找的包类型不存在，则该任务会失败。此功能可确保不会在整个环境中复制只由数个系统使用的包。

4 单击“保存”。

删除 SuperAgent 分布式资料库

使用此任务可以从主机系统和资料库列表 (SITELIST.XML) 中删除 SuperAgent 分布式资料库。新配置将在下次代理与服务器通讯时生效。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 在系统树的所需分配点中或在“策略目录”页中，打开所需的 McAfee Agent 策略页（以编辑模式）。

2 在“常规”选项卡上，取消选中“将运行 SuperAgent 的系统用作分布式资料库”，然后单击“保存”。

注意: 若要删除有限数量的现有 SuperAgent 分布式资料库，请先复制分配给这些系统的 McAfee Agent 策略，取消选中“将运行 SuperAgent 的系统用作分布式资料库”，然后再保存它。可以根据需要分配此新策略。

此时将删除 SuperAgent 资料库，并从资料库列表中删除。但是，只要“将代理转换为 SuperAgent”选项处于选定状态，该代理就仍然充当 SuperAgent。

创建并配置 FTP、HTTP 和 UNC 资料库

使用这些任务可以在现有的 FTP、HTTP 服务器或 UNC 共享上存放分布式资料库。尽管不必使用专用服务器，但是系统功能要足够强，以便所需数量的托管系统能连接到服务器获取更新。

任务

- 在 FTP、HTTP 服务器或 UNC 共享上创建文件夹位置
- 将分布式资料库添加到 ePolicy Orchestrator

在 FTP、HTTP 服务器或 UNC 共享上创建文件夹位置

使用此任务可以在分布式资料库系统上创建存放资料库内容的文件夹：

任务

- 对于 UNC 共享资料库，请在系统上创建文件夹并启用共享。
- 对于 FTP 或 HTTP 资料库，请使用现有的 FTP 或 HTTP 服务器软件（如 Microsoft Internet 信息服务 (IIS)）来创建新文件夹和站点位置。有关详细信息，请参阅 Web 服务器文档。

将分布式资料库添加到 ePolicy Orchestrator

使用此任务可以将新分布式资料库添加到资料库列表，并将其配置为使用您创建的文件夹。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库”，然后单击“新建资料库”。此时会出现“分布式资料库构建器”向导。

2 在“描述”页上，输入唯一名称，选择“HTTP”、“UNC”或“FTP”，然后单击“下一步”。这是出现在资料库列表中的名称。该名称不必是存放资料库的系统的名称。

3 在“服务器”页上，提供资料库的地址和端口信息，然后单击“下一步”。
   - 如果选择了“FTP”，请在“URL”中输入 Web 地址，在“端口”中输入 FTP 端口号（默认值为“21”）。
   - 如果选择了“HTTP”，请在“URL”中输入 Web 地址，在“端口”中输入 HTTP 端口号（默认值为“80”），在“复制 UNC 路径”中输入资料库所在的网络目录。（您也可以在“URL”文本框中输入服务器名称或 IP 地址。）
   - 如果选择了“UNC”，请在“复制 UNC 路径”中输入资料库所在的网络目录。请使用此格式：\\<计算机>\<文件夹>。可以使用变量定义此位置。

4 在“凭据”页上，提供托管系统用来连接到此资料库的“下载凭据”，然后单击“下一步”。请使用对存放资料库的 HTTP 服务器、FTP 服务器或 UNC 共享具有只读权限的凭据。
   - 如果选择了“FTP”，请选择“匿名”或“FTP 身份验证”（如果服务器要求身份验证），然后在“用户名”、“密码”和“确认密码”中输入用户帐户信息。
   - 如果选择了“HTTP”，请选择“匿名”或“HTTP 身份验证”（如果服务器要求身份验证），然后在“用户名”、“密码”和“确认密码”中输入用户帐户信息。
   - 如果选择了“UNC”，则可使用已登录帐户的凭据，或在“域”、“用户名”、“密码”和“确认密码”中输入用户帐户信息。

5 单击“测试凭据”。几秒钟后，会显示一条确认消息，指示系统可以使用身份验证信息访问该站点。

   如果凭据不正确，请检查：
   - 用户和密码。
   - 向导上一面板上的 URL 或路径。
   - 系统上的 HTTP、FTP 或 UNC 站点。

6 输入“复制凭据”。服务器在将 DAT 文件、引擎文件或其他产品更新从主资料库复制到分布式资料库时，需要使用这些凭据。这些凭据在分布式资料库所在的域中必须同时具有读取和写入权限：

- 如果选择了“FTP”，请在“用户名”、“密码”和“确认密码”中输入用户帐户信息。
- 如果选择了“HTTP”，并且 HTTP 服务器要求身份验证，请在“域”、“用户名”和“密码”字段中输入用户帐户信息。
- 如果选择了“UNC”，请在“域”、“用户名”、“密码”和“确认密码”中，输入网络目录的用户帐户信息。

7 单击“测试凭据”。几秒钟后，会显示一条确认消息，指示系统可以使用身份验证信息访问该站点。

8 单击“下一步”此时会出现“包类型”页。

9 选择是将所有包还是选定的包复制到此分布式资料库，然后单击“下一步”。

注意: 确保没有取消选择使用此资料库的托管系统所需的所有包。托管系统会访问一个资料库以获取所有包，如果该资料库中没有所需的包类型，则任务将失败。此功能可确保不会在整个环境中复制只由数个系统使用的包。

10 单击“保存”以添加资料库。ePolicy Orchestrator 会将新的分布式资料库添加到其数据库。

启用 UNC 和 HTTP 资料库的文件夹共享

使用此任务可以共享 HTTP 或 UNC 分布式资料库上的文件夹。对于这些资料库，ePolicy Orchestrator 要求启用文件夹，以在整个网络中共享，以便 ePolicy Orchestrator 服务器可以将文件复制到其中。这仅用于复制目的。配置为使用分布式资料库的托管系统将使用相应协议（HTTP、FTP 或 Windows 文件共享），而不需要文件夹共享。

任务

1 在系统上，使用 Windows 资源管理器找到创建的文件夹。

2 右键单击该文件夹，然后选择“共享”。

3 在“共享”选项卡中，选择“共享该文件夹”。

4 根据需要配置共享权限。通过资料库进行更新的系统只需要读取权限，但是管理员帐户（包括 ePolicy Orchestrator 服务器服务使用的帐户）要求具有写入权限。有关为共享文件夹配置相应安全设置的信息，请参阅 Microsoft Windows 文档。

5 单击“确定”。

编辑分布式资料库

使用此任务可以编辑分布式资料库。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库”，然后选择所需资料库旁的“编辑设置”。此时会打开“分布式资料库构建器”向导，显示分布式资料库的详细信息。

2 根据需要更改配置、身份验证和包选择选项。

3 单击“保存”。

删除分布式资料库

使用此任务可以删除 HTTP、FTP 或 UNC 分布式资料库。执行此操作会从资料库列表中删除这些分布式资料库，并删除分布式资料库的内容。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 请转至“软件”|“分布式资料库”，然后单击所需资料库旁的“删除”。

2 在“删除资料库”对话框上，单击“确定”。

注意: 删除资料库并不会删除资料库所在系统上的包。

使用资料库列表文件

使用这些任务可以导出 SITELIST.XML 文件以供代理和支持产品使用，或导出 SITEMGR.XML 文件，以在重新安装 ePO 服务器时使用，或用于导入其他要使用相同分布式资料库或来源站点 ePO 的服务器。

任务

- 导出资料库列表 SITELIST.XML 文件
- 导出资料库列表 SITEMGR.XML 文件以作为备份或由其他服务器使用
- 从 SITEMGR.XML 文件中导入分布式资料库
- 从 SITEMGR.XML 文件中导入来源站点

导出资料库列表 SITELIST.XML 文件

使用此任务可以将资料库列表 (SITELIST.XML) 文件导出到文件，以便手动传送到系统，或在安装支持的产品时导入。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”，然后单击“导出站点列表”。此时会出现“文件下载”对话框。

2 单击“保存”。此时会出现“另存为”对话框。

3 浏览到保存 SITELIST.XML 文件的位置，然后单击“保存”。

导出此文件后，可以在安装支持的产品时将其导入。有关说明，请参阅该产品的安装手册。

您也可以将资料库列表分发到托管系统，然后将其应用于代理。

导出资料库列表 SITEMGR.XML 文件以作为备份或由其他服务器使用

使用此任务可以将分布式资料库和来源站点的列表导出为 SITEMGR.XML 文件。如果重新安装 ePO 服务器，或要与其他 ePO 服务器共享分布式资料库或来源站点，使用此文件可以还原分布式资料库和来源站点。

您可以在“分布式资料库”或“来源站点”页导出此文件。不过，在将此文件导入其中任一页时，只会导入此页中列出的文件中的项目。例如，将此文件导入“分布式资料库”页时，只会导入文件中的分布式资料库。因此，如果要导入分布式资料库和来源站点，则必须导入文件两次，一次一页。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库”（或“软件”|“来源站点”），然后单击“导出资料库”（或“导出来源站点”）。此时会出现“文件下载”对话框。
2 单击“保存”，然后浏览并选择保存文件的位置。
3 如果需要，请对文件重命名，然后单击“保存”。

从 SITEMGR.XML 文件中导入分布式资料库

使用此任务可以从资料库列表文件中导入分布式资料库。在重新安装服务器后，或如果希望一个服务器与另一个服务器使用相同的分布式资料库，此任务很有用。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库”，然后单击“导入资料库”。此时会出现“导入资料库”对话框。
2 浏览到已导出的 SITEMGR.XML 文件，然后选择该文件。此时会出现“导入资料库”页。
3 选择要导入此服务器的所需分布式资料库，然后单击“确定”。

选定的资料库会添加到此服务器上的资料库列表中。

从 SITEMGR.XML 文件中导入来源站点

使用此任务可以从资料库列表文件中导入来源站点。在重新安装服务器后，或如果希望一个服务器与另一个服务器使用相同的分布式资料库，此任务很有用。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 请转至“软件”|“来源站点”，然后单击“导入来源站点”。此时会出现“导入来源站点”对话框。
2 浏览到已导出的 SITEMGR.XML 文件，然后选择该文件。此时会出现“导入来源站点”页。
3 选择要导入此服务器的所需来源站点，然后单击“确定”。

选定的来源站点会添加到此服务器上的资料库列表中。

更改多个分布式资料库上的凭据

使用此任务可以更改多个相同类型的分布式资料库上的凭据。如果环境中有很多分布式资料库，则此任务很有用。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库”，然后单击“更改凭据”。此时会出现“更改凭据”向导的“资料库类型”页。
2 选择要更改凭据的分布式资料库类型，然后单击“下一步”。此时会出现“资料库选择”页。
3 选择所需的分布式资料库，然后单击“下一步”。此时会出现“凭据”页。
4 根据需要编辑凭据，然后单击“下一步”。此时会出现“摘要”页。
5 查看信息，然后单击“保存”。

通过策略和客户端任务管理产品

从一个位置管理产品是 ePolicy Orchestrator 的主要功能，可以通过产品策略和客户端任务协同完成。策略会确保产品的功能得到正确配置，而客户端任务是在任何客户端软件所在的托管系统上运行的计划的操作。

是否首次配置策略和任务？

首次配置策略和任务时，请：

1 了解 ePolicy Orchestrator 的产品管理。

2 计划系统树部分的产品策略和客户端任务。

3 创建策略并将策略分配到组和系统。

4 创建客户端任务并将客户端任务分配到组和系统。

目录

扩展及其功能

扩展是在 ePO 服务器上安装的 ZIP 文件，以便管理环境中的其他安全产品。扩展包含管理此类产品所需的文件、组件和信息。扩展会替换早期版本的 NAP 文件。

扩展添加的功能

安装托管产品扩展后，添加的功能可能包括：

- 策略页。
- 服务器任务。
- 客户端任务。

- 默认查询。
- 通过查询构建器向导选择的新结果类型，图表类型和属性。
- 默认仪表板和仪表板监视器。
- 可以分配给用户帐户的功能权限。
- 其他产品特定的功能。

扩展文件的位置

某些扩展在安装 ePolicy Orchestrator 时自动安装。对于默认情况下没有安装扩展的产品，请参阅产品 CD 或产品下载中的产品文档，以了解名称及其位置。

策略管理

策略是您创建、配置并实施的设置的集合。策略会确保托管安全软件产品得到相应的配置和执行。例如，如果最终用户禁用防病毒扫描，则可设置一个策略在策略实施间隔重新启用扫描（默认间隔为 5 分钟）。

某些策略与在托管系统上安装的产品界面中配置的设置相同。其他策略设置是配置产品或组件的主要界面。ePolicy Orchestrator 控制台允许您从中心位置配置所有产品和系统的策略设置。

策略类别

大多数产品的策略设置都按类别分组。每个策略类别是指策略设置的特定子集。策略是按类别创建的。在“策略目录”页中，策略按产品和类别显示。当打开现有策略或创建新策略时，策略设置会通过各选项卡进行组织。

显示策略的位置

要按策略类别查看已创建的所有策略，请转至“系统”|“策略目录”页，然后从下拉列表中选择所需的“产品”和“类别”。在“策略目录”页上，用户只能查看其具有权限的产品的策略。

要根据产品查看应用到系统树特定组的策略，请转至“系统”|“系统树”|“策略”页，选择所需的组，然后从下拉列表中选择所需的“产品”。

注意: 每个类别都有一个 McAfee Default 策略。您不能删除、编辑、导出或重命名这些策略，但无须将 McAfee Default 策略分配到任何组或系统。

实施策略设置

对每个托管产品或组件，选择代理是否为产品或组件实施所有选择的策略，或不实施任何选择的策略。

在“策略”页中，选择是否对选定组中的产品或组件实施策略。

在“策略目录”页中，可以依据策略来查看已应用但未实施策略的分配。

何时实施策略

重新配置策略设置后，下次代理与服务器通讯时会将新策略传递到托管系统并实施。此通讯频率由“McAfee Agent”策略页上“常规”选项卡上的“代理与服务器通讯间隔”设置决定，或由代理唤醒任务计划决定（取决于实现代理与服务器通讯的方式）。默认情况下，该间隔设置为每 60 分钟一次。

策略设置在托管系统上生效之后，代理会继续以固定间隔在本地实施策略设置。此实施间隔由“McAfee Agent”策略页上“常规”选项卡上的“策略实施间隔”设置决定。默认情况下，该间隔设置为每 5 分钟一次。

McAfee 产品的策略设置会在策略设置更改后的策略实施间隔及每次代理与服务器通讯时立即实施。

注意: 在间隔之后，实施 Norton AntiVirus 产品策略之前，最多有 3 分钟的延迟。代理首先更新包含策略信息的 GRC.DAT 文件，然后 Norton AntiVirus 产品会从 GRC.DAT 文件读取策略信息，这项操作大约 3 分钟一次。

导出和导入策略

如果有多个服务器，则可以通过 XML 文件在这些服务器间导出和导入策略。在此类环境中，策略只需创建一次。

您可以导出和导入个别策略，或是针对特定产品导出和导入所有策略。

如果您需要重新安装服务器，则此功能也可以用于备份策略。

策略应用

可以通过继承或分配这两种方法中的一种将策略应用到任何系统。

继承

继承决定是否从组或系统的父级获取其策略设置和客户端任务。默认情况下，在整个系统树中启用继承。

在系统树的任何位置分配新策略来中断此继承后，设置为从此分配点继承策略的所有子组和系统都会中断继承。

分配

您可以将策略目录中的任何策略分配给任何组或系统（前提是您具有相应的权限）。分配操作允许您针对具体需求定义策略设置一次，然后将策略应用到多个位置。

在您将新策略分配给系统树的特定组后，设置为从此分配点继承策略的所有子组和系统都会分配有此策略。

分配锁定

您可以锁定任何组或系统的策略分配（前提是您具有相应的权限）。分配锁定可以防止：

- 在系统树的相同层级具有相应权限的其他用户无意中替换策略。
- 较低权限（或相同权限，但所在系统树的层级较低）的其他用户替换策略。

分配锁定与策略设置一起继承。

如果要在系统树的顶层分配特定策略，并且确保其他用户不会在系统树的其他位置将其替换，则分配锁定很有用。

分配锁定只锁定对策略的分配，但不禁止策略所有者对策略设置进行更改。因此，如果要锁定策略分配，您必须是策略的所有者。

策略所有权

您可以通过“策略目录”页使用有权限的产品和功能的所有策略。为防止任何用户编辑其他用户的命名策略，每一个策略仅分配给一位所有者，即创建该策略的用户。

所有权规定，除策略的创建者或全局管理员以外，任何人都不能修改或删除策略。具有相应权限任何用户都可以在“策略目录”页中分配任何策略，但只有所有者或全局管理员可以对其编辑。

如果您要将不属于您所有的策略分配给托管系统，请注意，如果该命名策略的所有者对其进行修改，则分配有该策略的所有系统都会接收这些修改。

因此，如果要使用其他用户所有的策略，McAfee 建议先复制策略，然后再将副本分配到所需的位置。这样您就拥有分配的策略。

客户端任务及其功能

ePolicy Orchestrator 允许创建和计划在托管系统上运行的客户端任务。

您可以为整个系统树、特定组或单个系统定义任务。与策略设置一样，客户端任务从系统树中的父组进行继承。

在 ePO 服务器上安装的扩展文件决定了可用的客户端任务。

客户端任务一般用于：

- 产品部署。
- 产品功能。（例如，VirusScan Enterprise 按需扫描任务。）
- 升级和更新。

有关信息和说明，请参阅托管产品的产品文档。

产品管理

使用此任务可以安装扩展 (ZIP) 文件。必须先安装产品的扩展，然后 ePolicy Orchestrator 才可管理产品。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 确保扩展文件位于网络上的可访问位置。
2 转至“配置”|“扩展”，然后单击“安装扩展”。此时会出现“安装扩展”对话框。
3 浏览到所需的扩展 (ZIP) 文件并选择该文件，然后单击“确定”。
4 确认产品名出现在“扩展”列表中。

查看策略信息

使用这些任务可以查看有关策略、其分配、继承和其所有者的详细信息。

任务

- 查看将策略分配到的组和系统
- 查看策略设置
- 查看策略所有权

查看将策略分配到的组和系统

使用此任务可以查看策略分配到的组和系统。该列表只显示分配点，而不显示继承该策略的每个组或系统。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后选择所需的“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。

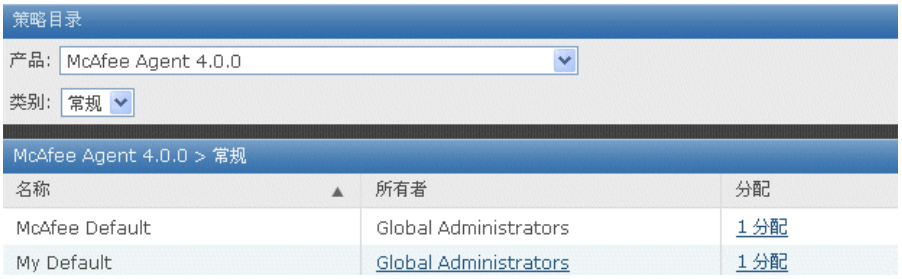

图 22：策略目录页

2 在所需策略行上的“分配”下，单击表明分配策略的组或系统数的蓝色文本（如“6 个分配”）。

在“分配”页中，将显示策略分配到的每个组或系统，同时会显示其“节点名称”和“节点类型”。

查看策略设置

使用此任务可以查看策略的特定设置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后选择所需的“产品”和“类别”。选定类别的所有已创建的策略都将出现在详细信息窗格中。

2 单击所需策略旁的“编辑”。此时会显示策略页及其设置。

注意: 您还可以在访问特定组的分配策略时查看此信息（通过“系统”|“系统树”|“策略”访问）。

查看策略所有权

使用此任务可以查看策略的所有者。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后选择所需的“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。
2 策略的所有者显示在“所有者”下。

查看禁用策略实施的分配

使用此任务可以按策略类别查看已禁用策略实施的分配。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后选择所需的“产品”和“类别”。
2 单击“产品实施状态”旁的蓝色文本，该文本指出禁用实施的分配的数量（如果有）。此时会出现“查看禁用策略实施的分配”页。
3 单击列表中的任一项目可转至其“策略”页。

查看分配给组的策略

使用此任务可以查看分配给组的策略。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“策略”，然后在“系统树”中选择组。按产品组织的所有已分配的策略都会出现在详细信息窗格中。
2 单击任一策略可以查看其设置。

查看分配给特定系统的策略

使用此任务可以查看分配给特定系统的策略。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后在“系统树”中选择所需的组。属于此组的所有系统都会出现在详细信息窗格中。
2 选择系统，然后单击“修改单个系统上的策略”。
3 选择产品。此时会显示分配给此系统的产品的策略。
4 单击任一策略可以查看其设置。

查看组的策略继承

使用此任务可以查看特定组的策略继承。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“策略”。按产品组织的所有已分配的策略都会出现在详细信息窗格中。
2 所需策略行的“继承来源”下会显示继承策略的来源组的名称。

查看并重置中断的继承

使用此任务可以查看继承中断的位置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“策略”。按产品组织的所有已分配的策略都会出现在详细信息窗格中。

2 在所需策略行的“中断的继承”下，显示此策略的继承中断的组和系统的数量。

注意: 这是策略继承中断的组或系统的数量，而不是未继承策略的系统数量。例如，如果只有一个特定的组不继承该策略，则无论该组内有多少个系统，都会以“1 个未继承”来表示。

3 单击表示已中断继承的子组或系统数量的蓝色文本。此时会出现“查看中断的继承”页，该页会显示这些组和系统的名称的列表。

4 要重置其中任何组或系统的继承，请选中该名称旁的复选框，然后单击“重置继承”。

使用策略目录

使用这些任务可以创建和维护“策略目录”页中的策略。

任务

- 在策略目录页上创建策略
- 复制策略目录页中的策略
- 在策略目录中编辑策略设置
- 重命名策略目录中的策略
- 删除策略目录中的策略

在策略目录页上创建策略

使用此任务可以在“策略目录”页上创建新策略。默认情况下，在此创建的策略不会分配给任何组或系统。您在此处创建策略时，自定义策略会添加到“策略目录”。

您可以在部署产品前后创建策略。

任务

1 转至“系统”|“策略目录”，然后从下拉列表中选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。

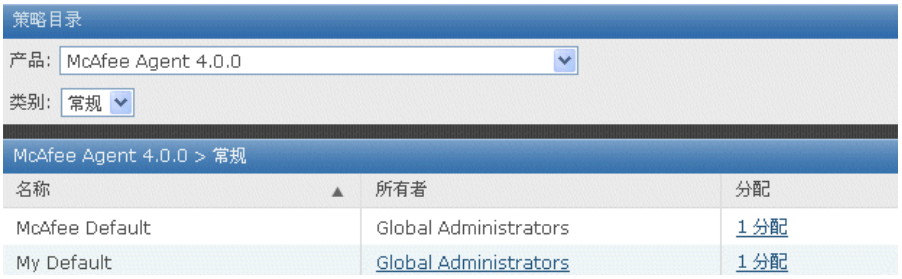

图 23：策略目录页

2 单击页底部的“新建策略”。此时会出现“创建新策略”对话框。

3 从“基于此现有策略来创建策略”下拉列表中，选择要复制的策略。

4 在“新策略名称”字段中输入新策略的名称，然后单击“确定”。此时会出现新策略的“策略设置”对话框。

5 根据需要编辑每个选项卡上的策略设置。

6 单击“保存”。

复制策略目录页中的策略

使用此任务可以基于现有策略创建新策略。例如，如果某个策略与要创建的策略相似，则可以复制该现有策略，然后进行所需的更改。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后从下拉列表中选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。

2 找到要复制的策略，然后单击该策略行中的“复制”。此时会出现“复制现有策略”对话框。

3 在字段中输入新策略的名称，然后单击“确定”（例如 Sales Europe）。新策略随即会显示在“策略目录”页中。

4 单击列表中新策略名称旁的“编辑”。此时将出现策略设置。

5 根据需要编辑设置，然后单击“保存”。

在策略目录中编辑策略设置

使用此任务可以修改策略的设置，您的用户帐户只有具备相应的权限才能编辑所需产品的策略设置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后从下拉列表中选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。

2 找到所需的策略类别，然后单击其旁的“编辑”。此时将出现策略设置。

3 根据需要编辑设置，然后单击“保存”。

重命名策略目录中的策略

使用此任务可以重命名策略。您的用户帐户只有具备相应的权限才能编辑所需产品的策略设置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后从下拉列表中选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。

2 找到所需的策略，然后单击策略行中的“重命名”。此时会出现“重命名策略”对话框。

3 输入现有策略的新名称，然后单击“确定”。

删除策略目录中的策略

使用此任务可以删除“策略目录”中的策略。删除策略时，当前将该策略应用到的所有组和系统都会继承其父组中的策略。在删除策略前，请先查看该策略分配到的组和系统，如果您希望组或系统不继承其父组的策略，则分配其他策略。

如果删除应用到“我的组织”组的策略，则会分配此类别的 McAfee Default 策略。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后从下拉列表中选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。

2 找到所需的策略，然后单击策略行中的“删除”。

3 当出现提示时，单击“确定”。

使用策略

使用这些任务可以分配和管理环境中的策略。

任务

更改策略的所有者

使用此任务可以更改策略的所有者。默认情况下，所有权会分配给创建策略的用户。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。

2 查找所需的策略，然后单击策略的“所有者”。此时会出现“分配策略所有者”对话框。

3 从列表中选择所需的策略所有者，然后单击“确定”。

在 ePO 服务器之间共享策略

使用这些任务可以在服务器之间共享策略。为此，必须从来源服务器的“策略目录”页将策略导出到 xml 文件，然后将该文件导入目标服务器上的“策略目录”页。

任务

导出单个策略

使用此任务可以将策略导出为 XML 文件。使用此文件可以将策略导入其他 ePO 服务器，或保留为策略的备份。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后从下拉列表中选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。
2 找到所需的策略类别，然后单击该策略旁的“导出”。此时会出现“下载文件”页。
3 右键单击链接，并选择“目标另存为”。
4 命名策略 XML 文件，并将其保存到某个位置。确保目标 ePolicy Orchestrator 服务器可以访问该位置。

导出产品的所有策略

使用此任务可以将产品的所有策略导出到 XML 文件。使用此文件可以将策略导入其他 ePO 服务器，或保留为策略的备份。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后选择“产品”和“类别”。该类别的所有创建的策略都将出现在详细信息窗格中。
2 单击页顶部“产品策略”旁的“导出”。此时会出现“下载文件”页。
3 右键单击链接，并选择“目标另存为”。
4 命名策略 XML 文件，并将其保存到所需位置。确保目标 ePolicy Orchestrator 服务器可以访问该位置。

导入策略

使用此任务可以导入策略 XML 文件。无论是导出单个策略还是所有命名策略，其导入步骤都是相同的。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“策略目录”，然后单击页顶部“产品策略”旁的“导入”。
2 浏览到所需的策略 xml 文件并选择该文件，然后单击“确定”。

导入的策略随即会添加到策略目录。

将策略分配到系统树的组

使用此任务可以将策略分配到系统树的特定组。您可以在部署产品前后分配策略。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“策略”，然后选择所需的“产品”。此时会在详细信息窗格中显示每个按类别分类的已分配策略。

2 找到所需的策略类别，然后单击“编辑分配”。此时会出现“策略分配”页。

3 如果策略被继承，请选择“继承自”旁的“中断继承并在下面分配策略和指定设置”。

4 从“分配的策略”下拉列表中选择所需的策略。

注意: 您还可以在此位置编辑选定策略的设置，或创建新策略。

5 选择是否锁定策略继承。锁定策略继承会防止继承此策略的所有系统在其位置分配其他策略。

6 单击“保存”。

将策略分配到托管系统

使用此任务可以将策略分配到特定托管系统。您可以在部署产品前后分配策略。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后在“系统树”下选择所需的组。此组内的所有系统（不包括子组）都会显示在详细信息窗格中。

2 选择所需的系统，然后单击“修改单个系统上的策略”。此时会出现该系统的“策略分配”页。

3 选择所需的“产品”。此时会列出该产品的策略类别，其中含有系统的已分配策略。

4 找到所需的策略类别，然后单击“编辑分配”。

5 如果策略被继承，请选择“继承自”旁的“中断继承并在下面分配策略和指定设置”。

6 从“分配的策略”下拉列表中选择所需的策略。

注意: 您还可以在此位置编辑选定策略的设置，或创建新策略。

7 选择是否锁定策略继承。

8 单击“保存”。

将策略分配到组内的多个托管系统

使用此任务可以将策略分配到组内的多个托管系统。您可以在部署产品前后分配策略。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后在“系统树”中选择所需的组。此组内的所有系统（不包括子组）都会显示在详细信息窗格中。

2 选择所需的系统，然后单击“分配策略”。此时会出现“分配策略”页。

3 从下拉列表中选择“产品”、“类别”和“策略”，然后单击“保存”。

对组中的产品实施策略

使用此任务可以启用或禁用系统树组上产品的策略实施。默认情况下启用策略实施，并在系统树中继承。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“策略”，然后在“系统树”中选择所需的组。
2 选择所需的“产品”，然后单击“实施状态”旁的蓝色文本。此时会出现“实施”页。
3 如果要更改实施状态，则必须先选择“中断继承并在下面分配策略和指定设置”。
4 在“实施状态”旁，选择相应的“实施”或“未实施”。
5 选择是否锁定策略继承。这会防止继承此策略的系统在其位置分配不同的策略。
6 单击“保存”。

对系统上的产品实施策略

使用此任务可以启用或禁用系统上产品的策略实施。默认情况下启用策略实施，并在系统树中继承。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后在系统所属的“系统树”下选择组。此时会在详细信息窗格中显示属于此组的系统的列表。
2 选择所需的系统，然后单击“修改单个系统上的策略”。此时会出现“策略分配”页。
3 选择所需的“产品”，然后单击“实施状态”旁的蓝色文本。此时会出现“实施”页。
4 如果要更改实施状态，则必须先选择“中断继承并在下面分配策略和指定设置”。
5 在“实施状态”旁，选择相应的“实施”或“未实施”。
6 单击“保存”。

复制和粘贴分配

使用这些任务可以将策略分配从一个组或系统复制并粘贴到另一个组和系统。通过该方法可以在系统树不同部分的组和系统之间轻松共享多个分配。

任务

- 从组复制策略分配
- 从系统中复制策略分配
- 将策略分配粘贴到组
- 将策略分配粘贴到特定的系统

从组复制策略分配

使用此任务可以从系统树的组中复制策略分配。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“策略”，然后在“系统树”下选择所需的组。
2 在详细信息窗格中，单击“复制分配”。
3 选择要复制策略分配的产品或功能，然后单击“确定”。

从系统中复制策略分配

使用此任务可以从特定的系统中复制策略分配。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后在“系统树”下选择所需的组。属于选定组的系统将会出现在详细信息窗格中。
2 选择所需的系统，然后单击“修改单个系统上的策略”。
3 单击“复制分配”，然后选择要为其复制策略的所需产品或功能，然后单击“确定”。

将策略分配粘贴到组

使用此任务可以将策略分配粘贴到组。您必须已从组或系统复制策略分配。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“策略”，然后在“系统树”中选择所需的组。
2 在详细信息窗格中，单击“粘贴分配”。如果该组已分配有某些类别的策略，则会出现“覆盖策略分配”页。
3 选择要用已复制的策略替换的策略类别，然后单击“确定”。

将策略分配粘贴到特定的系统

使用此任务可以将策略分配粘贴到特定的系统。您必须已从组或系统复制策略分配。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后选择所需的“系统树”的组。属于选定组的所有系统都将出现在详细信息窗格中。
2 选择要将策略分配粘贴到的系统，然后单击“修改单个系统上的策略”。
3 在详细信息窗格中，单击“粘贴分配”。如果该系统已分配有某些类别的策略，则会出现“覆盖策略分配”。
4 确认替换分配。

使用客户端任务

使用这些任务可以创建和维护客户端任务。

任务

创建并计划客户端任务

使用此任务可以创建和计划客户端任务。所有客户端任务的过程都类似。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“客户端任务”，在系统树中选择所需的组，然后单击“新建任务”。
2 输入要创建任务的名称，添加注释，然后从下拉列表中选择产品和任务类型。例如，选择“更新”。
3 选择是否启用计划，然后单击“下一步”。此时会出现“配置”页。所显示的此向导页及其选项取决于所选的任务类型。
4 配置设置，然后单击“下一步”。此时会出现“计划”页。
5 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。
6 查看任务设置，然后单击“保存”。

此任务会添加到选定组以及继承此任务的任何组的客户端任务列表中。

编辑客户端任务

使用此任务可以编辑任何现有任务的客户端任务设置或计划信息。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“客户端任务”，然后在系统树中选择所需的组。
2 单击任务旁的“编辑”。此时会出现“客户端任务构建器”向导。
3 根据需要编辑任务设置，然后单击“保存”。

托管系统会在下次代理与服务器通讯时接收这些更改。

删除客户端任务

使用此任务可以删除不需要的客户端任务。您可以删除任何您创建的客户端任务，但部署任务除外。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“客户端任务”，然后在系统树中选择所需的组。
2 单击所需客户端任务旁的“删除”
3 单击“确定”。

常见问题

何谓策略？

策略是与策略类别相对应的自定义产品设置子集。对于每个策略类别，您可以根据需要创建、修改或删除任意数量的命名策略。

何谓 McAfee Default 策略和 My Default 策略？

安装时，每个策略类别都至少都包含有两个策略。这两个策略的名称为 McAfee Default 策略和 My Default 策略。这两个策略是首次安装时提供的仅有策略。这两个策略的配置最初都是相同的。

McAfee Default 命名策略不可编辑、重命名或删除。不过可以编辑、重命名和删除 My Default 策略。

分配新策略的组的子组和系统会发生什么情况？

设置为继承特定策略类别的所有子组和系统都会继承应用到父组的策略。

在策略目录中修改策略后，会对应用此策略的组和系统带来什么影响？

应用策略的所有组和系统都会在下次代理与服务器通讯时接收对策略所做的任何修改。然后在每个策略实施间隔执行该策略。

分配的新策略未能在托管系统上实施。为什么？

新策略分配在下次代理与服务器通讯时实施。

已将策略分配从一个组或系统（来源）粘贴到另一个组或系统（目标），但分配给目标位置的策略与来源位置不同。为什么不同？

在您复制并粘贴策略分配时，只会粘贴真正的分配。如果来源位置此前继承了您已选择复制的策略，则粘贴到目标的是继承特征，因此，目标此后从其父级继承策略（属于该特定策略类别），这个策略与继承到来源的策略可能不同。

部署软件和更新

除管理安全产品外，ePolicy Orchestrator 还可以将产品部署到网络系统中。使用 ePolicy Orchestrator 可以部署产品及其更新。

如果计划使用 ePolicy Orchestrator 之外的工具部署安全产品和更新，则可略过本节。

是否首次部署包？

首次部署包：

1 了解产品部署和 ePolicy Orchestrator 可以部署的包类型。

2 配置纳入和复制任务。

3 配置部署和更新任务。

4 将产品和更新包签入主资料库。

目录

部署产品和更新的包

ePolicy Orchestrator 部署基础架构支持部署产品和组件，以及对二者进行更新。

ePolicy Orchestrator 可以部署的每个 McAfee 产品都会提供一个产品部署包 ZIP 文件。在将包签入主资料库后，ePolicy Orchestrator 可以将这些包部署到任何托管系统。ZIP 文件包含以安全格式压缩的产品安装文件。

ZIP 文件同时用于检测特征码 (DAT) 和引擎更新包。

您可以在部署前后配置产品策略设置。McAfee 建议先配置策略设置，然后再将产品部署到网络系统。此方法会节省时间，并可以尽快保护您的系统。

这些包类型可以通过纳入任务或手动签入主资料库。

支持的包类型

包类型	描述	来源
检测特征码 (DAT) 文件 文件类型：ZIP	McAfee 每天定期发布 DAT 文件。	McAfeeFtp 和 McAfeeHttp 更新站点和 McAfee 站点。使用纳入任务可以将 DAT 文件直接下载到主资料库，或手动下载并签入主资料库。
扫描引擎 文件类型：ZIP	McAfee 防病毒产品的最新扫描引擎，如 VirusScan Enterprise。通常每年对引擎更新一次或两次。	McAfeeFtp 和 McAfeeHttp 更新站点和 McAfee 网站。使用纳入任务可以直接将引擎文件下载到主资料库，或手动下载并签入到主资料库。
SuperDAT (SDAT.EXE) 文件 文件类型：SDAT.EXE	SuperDAT 文件在一个更新包中同时提供 DAT 和引擎文件。如果带宽是一个考虑因素，McAfee 建议分别更新 DAT 和引擎文件。	McAfee 网站。下载 SuperDAT 文件并将其手动签入主资料库中。
补充检测特征码 (EXTRA.DAT) 文件 文件类型：EXTRA.DAT	EXTRA.DAT 文件处理自上一次发布的 DAT 文件以来出现的一个或多个特定威胁。如果出现严重的威胁，请立即分发 EXTRA.DAT 文件，而不必等到将签名添加到下一个 DAT 文件后再分发。EXTRA.DAT 文件来自 McAfee 网站。您可以通过 ePolicy Orchestrator 进行分发。纳入任务不会检索 EXTRA.DAT 文件。	McAfee 网站。手动下载附加病毒特征码文件并将其签入主资料库。
产品部署包 文件类型：ZIP	产品部署包包含 McAfee 产品的安装软件。	产品 CD 或已下载产品的 ZIP 文件。手动将产品部署包签入主资料库。有关具体位置的信息，请参阅对应产品的文档。在安装 ePO 服务器过程中，只有代理和 System Compliance Profiler 部署包会签入主资料库。
代理安装包 文件类型：ZIP	代理安装包包含代理的安装软件。	主资料库 — 已在安装时签入。要获得将来的代理版本，必须手动将代理安装包签入主资料库。
代理语言包 文件类型：ZIP	代理语言包包含采用本地语言显示代理信息所需的文件。	主资料库 — 已在安装时签入。要获得将来的代理版本，必须手动将代理语言包签入主资料库。

包签名和安全

由 McAfee 创建和发布的所有包均使用 DSA（数字签名算法）签名验证系统的密钥对进行签名，并使用 168 位 3DES 加密算法进行加密。还有一个密钥专用于对敏感数据进行加密或解密。

签入未经 McAfee 签名的包时，您会收到通知。如果确信包的内容正确且合法，可以继续进行签入这些包会采用上述相同方式加以保护，但在签入时由 ePolicy Orchestrator 进行签名。

数字签名可以保证包由 McAfee 提供或由您签入，并且没有被篡改或损坏。代理只信任由 ePolicy Orchestrator 或 McAfee 签名的包文件。这样可以防止您的网络从未经签名或不受信任的来源接收包。

旧版产品支持

以前的产品使用单层目录结构，并通过自动更新和自动升级客户端任务来安装产品更新。而使用 AutoUpdate 7.0 的新产品则采用分层目录结构和更新任务来安装产品更新。

如果在自动更新或自动升级任务设置中指定的更新位置是由 ePolicy Orchestrator 管理的分布式资料库，则在将相应的包签入主资料库时，必须启用旧版产品支持。这会将包复制到两个目录结构中，从而支持旧版产品。

包的顺序和依赖性

如果一个产品更新依赖于另一个产品更新，则必须按照要求的顺序将它们的包签入主资料库中。例如，如果补丁程序 2 需要补丁程序 1，则必须先签入补丁程序 1，再签入补丁程序 2。包在签入后无法重新排序。您必须先删除它们，然后按正确的顺序再次签入。如果签入的包会替代现有包，则现有包会被自动删除。

产品和更新部署

ePO 的资料库基础架构允许您从中央位置将产品和更新包部署到托管系统。尽管使用相同的资料库，但是两者之间仍然存在差异。

产品部署包和更新包的比较

产品部署包	更新包
必须手动签入主资料库。	通过纳入任务，可以自动从来源站点复制 DAT 和引擎更新包。所有其他更新包都必须手动签入主资料库。
可以使用全局更新复制到分布式资料库并安装在托管系统上。	可以通过全局更新自动复制到分布式资料库并安装在托管系统上。
如果未对产品部署实现全局更新，则必须为托管系统配置和计划部署任务才能获取包。	如果未对产品实施全局更新，则必须配置和计划更新客户端任务，以让托管系统可以获取包。

产品部署和更新过程

按照下列分发 DAT 和引擎更新包的简要过程执行操作：

1 使用纳入任务或手动将更新包签入主资料库。

2 如使用全局更新，则只要配置好全局更新并启用即可，无需执行其他任何操作。

如果未使用全局更新，则需使用复制任务将主资料库的内容复制到分布式资料库。

3 如果未使用全局更新，则为代理创建和计划更新或部署任务以便在托管系统上获得并安装更新。

部署任务

签入产品部署包之后，可以使用“产品部署”客户端任务将产品安装到托管系统上。此任务会安装可通过 ePolicy Orchestrator 部署且已签入主资料库的任何产品。

最佳实践

您可以对任何组或单个系统运行产品部署任务。在部署产品时，McAfee 建议您考虑包的大小及主资料库或分布式资料库与托管系统之间的可用带宽。将产品部署到许多系统除可能会使 ePO 服务器或网络崩溃之外，还会使故障排除变得更为复杂。

您可以考虑分阶段一次性地将产品安装到几组系统中。如果网速较快，则可以尝试将产品部署到几百台客户端计算机。如果网速较慢或不太稳定，则可以尝试分组进行部署。将产品部署到每个组时，请监控部署情况并运行报告以确认安装顺利并解决个别系统出现的问题。

如果部署安装在托管系统子集上的 McAfee 产品或组件，请：

1 使用标记标识这些系统。

2 创建并运行对标记的查询来对表中的系统进行分组。

3 将软件部署到系统。

更新任务

将更新包签入主资料库并复制到分布式资料库之后，托管系统上的代理仍需了解向分布式资料库获取更新的具体时间。如果使用全局更新，则可以忽略此过程。

您可以通过创建和配置更新客户端任务来控制托管系统接收更新包的时间和方式。如果未使用全局更新，则只有创建这些任务才能通过 ePolicy Orchestrator 控制客户端更新。

使用全局更新时不必创建此任务，但您可以另外创建一个每日任务作为备用。

创建更新客户端任务时的注意事项

计划客户端更新任务时应该考虑以下事项：

- 在由所有系统继承的最高系统树层级上，创建一个更新客户端任务以每天更新 DAT 和引擎文件。如果您的组织是个大型组织，则可以使用随机时间间隔来化解带宽影响。另外，对于那些在不同时区均设有办事处的大型网络，按照托管系统的本地系统时间运行任务（而不是所有系统在相同时间运行）有助于平衡网络负载。
- 如果使用计划复制任务，请将该任务安排在复制任务至少一个小时后执行。
- 至少每天运行一次 DAT 和引擎文件更新任务。托管系统有时会由于不在网络上而错过计划任务，因此经常运行该任务可以确保这些系统收到更新。
- 最大限度地提高带宽利用率，并计划多个客户端更新任务，在不同时段更新不同的组件。例如，可以创建一个任务只更新 DAT 文件，然后创建另一个更新任务每周或每月更新一次 DAT 和引擎文件（通常引擎包的发布频率较低）。
- 对于不使用 Windows 代理的产品，应该额外创建和计划一些任务。
- 创建任务来更新主工作站应用程序（如 VirusScan Enterprise），以确保它们都能接收更新文件。安排该任务每天运行一次或运行多次。

全局更新

McAfee 建议采用全局更新作为您的更新策略。全局更新使复制到分布式资料库和更新托管系统的过程自动完成，而无需执行复制和更新任务。将内容签入主资料库会启动全局更新。在大多数环境中，整个过程应该在一小时之内完成。

此外，您可以指定使用哪些包和更新来启动全局更新。然而，当仅指定某些内容启动全局更新时，请确保创建一个复制任务来分发未选择用来启动全局更新的内容。

注意: 在使用全局更新时，McAfee 建议将定期纳入任务（更新主资料库）安排在网络通讯量最低时进行。尽管全局更新的速度比其他方法快得多，但在更新时会增加网络通讯量。

全局更新过程

全局更新会通过此过程在一个小时内更新大多数环境：

1 将内容签入主资料库。

2 主资料库的内容自动复制到分布式资料库中。

3 将具有 SITESTAT.XML 文件的 SuperAgent 唤醒呼叫广播到所有代理。此文件列出主资料库的内容。如果托管系统所需的包位于此列表中，则代理将转到分布式资料库以获取该包。

4 所有代理将访问其分布式资料库来获取新的更新。

要求

全局更新的实现要求如下：

- 将 SuperAgent 安装在每个广播网段上。如果在同一广播网段上没有 SuperAgent 唤醒呼叫，则托管系统无法接收 SuperAgent 唤醒呼叫。全局更新会利用 SuperAgent 唤醒呼叫通知代理目前可以获取新的更新。
- 在整个环境中设置并配置分布式资料库。McAfee 建议使用 SuperAgent 资料库，但是这并不是必需的，因为所有类型的分布式资料库都可以使用全局更新功能。
- 如果使用 SuperAgent 资料库，则托管系统必须能够“看到”用来进行更新的资料库。尽管每个广播网段上都需要有 SuperAgent，这样系统才能接收唤醒呼叫，而每个广播网段上并不一定需要有 SuperAgent 资料库，但是托管系统必须能够“看到”用来进行更新的 SuperAgent 资料库。

纳入任务

使用纳入任务可通过来源站点的 DAT 和引擎更新包更新主资料库。DAT 和引擎文件都必须经常更新。McAfee 每天都会发布最新的 DAT 文件，而引擎文件的发布频率较低。这些包应尽快部署到托管系统，以便为它们提供最新威胁防护。

使用此版本，您可以指定从来源站点复制到主资料库的包。

注意: 必须将 EXTRA.DAT 文件手动签入主资料库。McAfee 网站上提供了这些文件。

计划的资料库纳入服务器任务将在您指定的时间和日期定期自动运行。例如，您可以计划在每个星期四上午 5:00 运行“资料库纳入”任务。

您还可以使用“立即纳入”任务将更新立即签入主资料库。例如，当 McAfee 就快速传播的病毒向您发出警报，并发布一个针对该病毒进行防护的新 DAT 文件时。

如果纳入任务失败，必须将包手动签入主资料库中。

更新主资料库之后，便可以使用全局更新或复制任务将这些更新自动分发到系统。

计划纳入任务时的注意事项

计划纳入任务时应该考虑以下事项：

- 带宽和网络使用率。如果您使用的是全局更新，则建议将纳入任务安排在其他资源的带宽使用率很低的情况下运行。利用全局更新，更新文件会在纳入任务完成之后自动分发。
- 任务的频率。虽然每天都发布 DAT 文件，但是您可能不想每天都使用资源进行更新。
- 复制和更新任务。计划复制任务和客户端更新任务，以确保在整个环境中分发更新文件。

复制任务

使用复制任务可以将主资料库的内容复制到分布式资料库。除非已将主资料库内容复制到所有分布式资料库，否则有些系统将无法接收这些内容。而且要确保所有分布式资料库都处于最新状态。

注意: 如果您使用全局更新来分发全部更新，尽管建议将复制任务作为备用方法，但您的环境中可能不需要复制任务但是，如果您不使用全局更新分发任何更新，则必须安排“资料库复制”服务器任务，或运行“立即复制”任务。

计划定期资料库复制服务器任务是确保分布式资料库处于最新状态的最好方法。计划每天复制任务可确保托管系统保持最新状态。使用资料库复制任务，可使复制到分布式资料库的过程自动完成。

有时，您可能会将文件签入主资料库并想立即将其复制到分布式资料库，而不是等到下一次计划复制时进行复制。在这种情况下，可以运行立即复制任务手动更新分布式资料库。

完全复制与增量复制

创建复制任务时，可选择“增量复制”或“完全复制”。增量复制使用的带宽较少，它只复制位于主资料库中但尚未复制到分布式资料库的新更新。而完全复制则会复制主资料库的所有内容。

提示: McAfee 建议计划一个每日增量复制任务和一个每周完全复制任务。这样，每周只更新基本增量变化，从而最大限度地提高了网络带宽的利用率，并保证了完整性。

资料库的选择

新分布式资料库会添加到包含所有可用分布式资料库的资料库列表文件中。每当托管系统的代理与 ePO 服务器进行通讯时，都会更新此文件。而且当代理 (McAfee Framework Service) 服务启动及资料库列表更改时，代理都会进行资料库选择。

选择性复制为单一资料库的更新提供更多控制项。计划复制任务时，可选择以下项目：

- 适用于该任务的具体分布式资料库。在不同的时间复制到不同的分布式资料库可以降低对带宽资源的影响。在创建或编辑复制任务时可以指定这些资料库。
- 复制到分布式资料库的特定文件和签名。通过只选择签入分布式资料库中的每个系统所需的文件类型可以降低对带宽资源的影响。定义或编辑分布式资料库时，可以选择要复制到分布式资料库的包。

注意: 此功能专用于更新只在环境中的几个系统上安装的产品，例如 GroupShield 和 WebShield。使用该功能可以只将这些更新分发到这些系统所使用的分布式资料库。

代理如何选择资料库

默认情况下，代理会尝试从资料库列表文件中的任何资料库进行更新。代理也可以使用网络 ICMP ping 或子网地址比较算法来查找响应时间最快的分布式资料库。通常情况下，这是网络中距离系统最近的分布式资料库。

您也可以在代理策略设置中启用或禁用分布式资料库，从而严格控制代理使用哪些分布式资料库进行更新。McAfee 建议不要在策略设置中禁用资料库。允许代理从任何分布式资料库进行更新可确保代理能够收到更新。

服务器任务日志

服务器任务日志除了提供所有服务器任务的有关信息外，还提供纳入和复制任务的有关信息。它提供任务的状态以及可能发生的任何错误。

服务器任务日志中的复制任务信息

“报告”|“服务器任务日志”选项卡包含以下有关复制任务的信息：

- 开始日期和任务持续时间。
- 每个站点的任务状态（展开时显示）。
- 错误、警告、任务代码及其应用站点。

服务器任务日志中的纳入任务信息

“报告”|“服务器任务日志”选项卡包含以下有关纳入任务的信息：

- 开始日期和任务持续时间。
- 错误或警告及其代码。
- 签入主资料库的每个包的状态。
- 所有正在签入主资料库的任何新包的信息。

手动签入包

使用此任务可以将部署包手动签入主资料库，以使 ePolicy Orchestrator 可部署这些包。

开始之前

您必须具有相应的权限才能执行此任务。

注意: 不能在纳入任务或复制任务正在运行时签入包。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”，然后单击“签入包”。此时会出现“签入包”向导。

图 24：主资料库选项卡

2 选择包类型，然后浏览到所需的包文件并选择此文件。

3 单击“下一步”。此时会出现“包选项”页。

4 在“将包签入此分支”旁，选择所需的分支。

如果系统要求在整个工作环境中部署新包之前测试这些包，则 McAfee 建议在签入包时使用评估分支。在测试完包后，可以将这些包移到“软件”|“主资料库”选项卡上的当前分支。

5 在“选项”旁，选择是否：

- 支持 Netshield for NetWare — 签入 NetShield for NetWare 的包。
- 将现有包移到“早期”分支 — 签入新包时，将同类型（但版本不同）的现有包移到早期分支。

6 单击“保存”开始签入该包。在包签入时，请稍候。

新包会出现在“主资料库”选项卡上的“主资料库中的包”列表中。

使用产品部署任务将产品部署到托管系统

使用这些任务可以通过“产品部署”客户端任务将产品部署到托管系统。ePolicy Orchestrator 4.0 允许为单个系统或系统树的组创建此任务。

任务

- 为托管系统的组配置部署任务
- 配置部署任务以将产品安装在托管系统上

为托管系统的组配置部署任务

使用此任务可以配置“产品部署”任务，以将产品部署到系统树的托管系统的组。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“客户端任务”，然后在系统树中选择组。
2 单击“新建任务”，然后对此任务命名，并从“任务类型”下拉列表中选择“产品部署(McAfee Agent)”。
3 将任何描述信息添加到“注释”字段。

  只有在您打开此组或继承此组中任务的子组中的任务时，才会看到在此添加的信息。

4 单击“下一步”此时会出现“配置”页。
5 选择将包部署到的所需平台。
6 在“要部署的产品”旁，从第一个下拉列表中选择所需的产品。

  列出的产品是那些已经将 PKGCATALOG.Z 文件签入主资料库的产品。如果在此处看不到要部署的产品，则必须首先签入该产品的 PKGCATALOG.Z 文件。

7 将“操作”设置为“安装”，然后选择包的语言版本。
8 若要指定命令行安装选项，请在“命令行”文本字段中输入所需的命令行选项。有关要安装的产品的命令行选项的信息，请参阅产品文档。
9 单击“下一步”此时会出现“计划”页。
10 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。
11 查看并确认“产品部署”任务的详细信息，然后单击“保存”。

配置部署任务以将产品安装在托管系统上

使用此任务可以通过“产品部署”任务将产品部署到单个系统。

在单个系统需要以下各项时，为该系统创建产品部署客户端任务：

- 同一组中其他系统不需要的已安装产品。
- 与组中的其他系统不同的计划。例如，系统所在的时区与对等系统所在的时区不同。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“系统”，然后在系统树中选择包含所需系统的组。
2 选择所需系统旁的复选框。
3 单击“修改单个系统上的任务”。此时会出现分配给此系统的任务的列表。

   注意: 您可能需要单击“更多操作”来访问“修改单个系统上的任务”。

4 单击“新建任务”。此时会出现“客户端任务构建器”的“描述”页。
5 从“类型”下拉列表中选择“产品部署(McAfee Agent)”。
6 可以将任何描述信息添加到“注释”字段。

   在此添加的信息只有在您打开要为其配置任务的系统上的任务时才可见。

7 在“继承”旁，选择此系统是否应从系统树的父组中继承任务的计划和设置。
8 从“产品”下拉列表中选择“McAfee Agent”，然后从“类型”下拉列表中选择“产品部署”。
9 单击“下一步”此时会出现“配置”页。
10 选择将包部署到的所需平台。
11 在要部署的“产品”旁，从下拉列表中选择所需的产品。

   列出的产品是那些已经将 PKGCATALOG.Z 文件签入主资料库的产品。如果在此处看不到要部署的产品，则必须首先签入该产品的 PKGCATALOG.Z 文件。

12 将“操作”设置为“安装”，然后选择包的语言版本。
13 若要指定命令行安装选项，请在“命令行”文本字段中输入所需的命令行选项。有关要安装的产品命令行选项的信息，请参阅产品文档。
14 单击“下一步”此时会出现“计划”页。
15 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。
16 查看并确认“产品部署”任务的详细信息，然后单击“保存”。

使用全局更新自动部署更新包

使用此任务可以启用服务器上的全局更新。全局更新会自动将用户指定的更新包部署到托管系统。

开始之前

- 必须创建资料库，而且接收 SuperAgent 唤醒呼叫的所有代理都可以使用这些资料库。
- 包含要接收 SuperAgent 唤醒呼叫的代理的每个广播网段中都必须有 SuperAgent。
- 只有全局权利员才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，选择“全局更新”，然后单击页面底部的“编辑”。

图 25：编辑全局更新页

2 在“编辑全局更新”页上，选择“状态”旁的“启用”。

3 如果需要，请编辑“随机时间间隔”。默认值为“20 分钟”。

每个客户端的更新将在随机时间间隔的某个随机选定时间内执行，这有助于分散网络负载。例如，如果您使用 20 分钟的默认随机时间间隔更新 1000 台客户端，在此时间间隔每分钟大约更新 50 台客户端，这样就可以降低网络和服务器上的负载。如果不使用随机时间间隔，则全部 1000 台客户端将尝试同时更新。

4 在“包类型”旁，选择开始更新的包。

只有此处指定组件的新包签入主资料库或移到其他分支时，全局更新才会启动更新。所以要慎重选择这些组件。

5 完成后，请单击“保存”。

启用全局更新之后，它会在您下次签入的任何选定包或移到其他分支后启动更新。

注意: 在您准备开始自动更新时，请务必运行“立即纳入”任务，并计划重复的“资料库纳入”服务器任务。

使用纳入和复制任务更新包

在创建了资料库基础结构后，使用这些任务可以实现基于任务的更新策略。如果在环境中不使用全局更新，则必须依赖这些任务。

开始之前

确保已创建资料库，并位于托管系统可以访问到的位置。

任务

- 使用纳入任务更新主资料库
- 将包从主资料库复制到分布式资料库

使用纳入任务更新主资料库

使用这些任务中的任何一个可以从 McAfee 更新站点或用户配置的来源站点中更新主资料库的内容。

您可以计划或立即运行纳入任务。

开始之前

确保配置了代理服务器设置，这样主资料库就可以访问来源站点。

任务

- 按计划运行纳入任务
- 运行立即纳入任务

按计划运行纳入任务

使用此任务可以计划从来源站点更新主资料库的重复纳入任务。根据计划要求，或者如果您希望在不同时间复制到不同的分布式资料库，则可能需要创建多个服务器任务。使用立即纳入任务可以选择从来源站点复制哪些包。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”，然后单击页面底部的“计划纳入”。此时会出现“服务器任务生成器”向导的“描述”页。

2 命名并描述该任务。

3 选择是启用任务还是禁用任务，然单击“下一步”。此时会出现“操作”页。

可以手动运行已禁用的任务，但不要在计划的时间运行。

4 从下拉列表中选择“资料库纳入”。

图 26：资料库纳入服务器任务操作

5 选择要将内容纳入主资料库的来源站点。

6 选择要接收包的分支。

选择“评估”，可以先在实验室环境中测试包。

选择“当前”，可以使用包而不先进行测试。

7 选择是否纳入：

- 全部包

- 选定的包 — 如果选中此选项，则必须单击“选择包”，然后选择此任务运行时要从来源站点纳入的包。

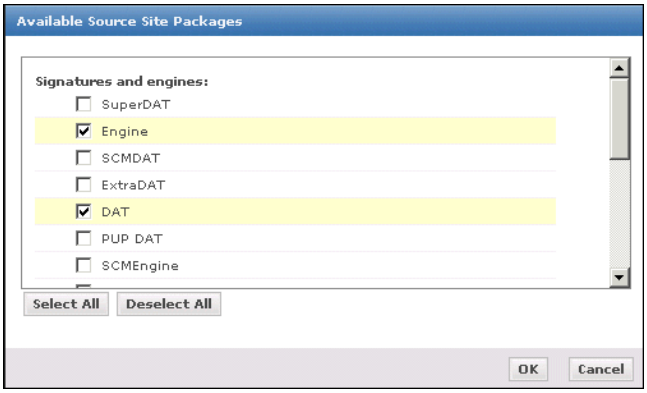

图 27：可用来源站点包对话框

8 选择是否：

- 支持 NetShield for Netware
- 将相同类型的现有包移到‘早期’分支

9 击单“下一步”。此时会出现向导的“计划”页。

10 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。

注意: “计划”页比早期版本的计划功能具有更大的灵活性。除了在所有计划类型中有更精细的计划外，还可以通过选择“高级”计划类型来使用 Cron 语法。

11 查看摘要信息，然后单击“保存”。

计划资料库纳入任务将被添加到“服务器任务”页上的任务列表中。

运行立即纳入任务

使用此任务可以启动纳入任务，以立即从来源站点更新主资料库。对此版本而言，您可以选择将哪些包从来源站点复制到主资料库。

开始之前

- 您必须具有相应的软件权限才能执行此任务。
- 必须配置代理服务器设置才能允许主资料库访问来源站点。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”，然后单击页面底部的“立即纳入”。此时会显示“立即纳入”向导。

2 从可用资料库的列表中选择来源站点。

3 选择接收包的资料库分支。

选择“评估”，可以先在实验室环境中测试包。

选择“当前”可以使用包而不先进行测试。

4 如果环境中装有 NetShield for NetWare，请选择“支持 NetShield for NetWare”。

5 选择“将相同类型的现有包移到‘早期’分支”，以将当前分支中保存的当前包版本移到早期分支。

6 击单“下一步”。此时会出现“包选择”页。

7 选择要从来源站点复制的包，然后单击“下一步”。此时会出现“摘要”页。

8 验证任务详细信息，然后单击“确定”开始纳入任务。此时会显示“服务器任务日志”页 ，可以在此监视任务完成之前的任务的状态。

将包从主资料库复制到分布式资料库

使用任一任务可以将主资料库的内容复制到分布式资料库。您可以安排定期运行“资料库复制”服务器任务，也可以运行“立即复制”任务立即进行复制。

任务

- 按计划运行资料库复制服务器任务
- 运行立即复制任务

按计划运行资料库复制服务器任务

使用此任务可以创建计划的资料库复制服务器任务。

开始之前

- 您必须具有相应的权限才能执行此任务。
- 您必须设置分布式资料库，并将其添加到 ePolicy Orchestrator。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库” ，然后单击“计划复制”。此时会出现“服务器任务生成器”向导的“描述”页。

2 命名并描述该任务。

3 选择是启用任务还是禁用任务，然单击“下一步”。此时会出现“操作”页。

可以手动运行已禁用的任务，但不要在计划的时间运行。

4 从下拉列表中选择“资料库复制”。

图 28：资料库复制服务器任务操作

5 从“复制类型”下拉列表中，选择“增量”或“完全”。

选择“增量”只会复制主资料库和分布式资料库之间的差异。

选择“完全”会将主资料库的所有内容复制到分布式资料库。

6 选择“复制到”旁的“全部资料库”或“选定的资料库”。

注意: 如果选择“选定的资料库”，则必须单击“选择资料库”，以选择在启动此任务时接收包的分布式资料库。

7 击单“下一步”。此时会出现向导的“计划”页。

8 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。

注意: “计划”页比早期版本的计划功能具有更大的灵活性。除了在所有计划类型中有更精细的计划外，还可以通过选择“高级”计划类型来使用 Cron 语法。

9 查看摘要信息，然后单击“保存”。

计划资料库纳入任务将被添加到“服务器任务”页上的任务列表中。

运行立即复制任务

使用此任务可以将主资料库内容立即复制到分布式资料库。

开始之前

- 您必须具有相应的权限才能执行此任务。
- 必须设置任何要复制的分布式资料库，并将其添加到 ePolicy Orchestrator。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“分布式资料库” ，然后单击“立即复制”。此时会出现“立即复制”向导的“资料库”页。

2 选择要进行复制的分布式资料库，然后单击“下一步”。

如果您不确定哪些分布式资料库需要更新，请复制到所有分布式资料库。

3 选择“增量复制”或 “完全复制” ，然后单击“下一步”。

注意: 如果您是第一次复制到分布式资料库，即使您选择增量复制，实质上也是完全复制。

4 单击“开始复制”启动任务。此时会显示“服务器任务日志”页 ，在此会显示任务完成之前的任务的状态。复制时间取决于主资料库的更改情况以及复制到的分布式资料库的数量。

任务完成之后，您可以启动立即更新客户端任务，使其他位置的托管系统可以获取分布式资料库中的更新。

配置代理策略以使用分布式资料库

使用此任务可以自定义代理选择分布式资料库的方式。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 在“McAfee Agent”|“常规”策略页中的“资料库”选项卡上，选择“使用此资料库列表”。

2 在“资料库选择”下，指定对资料库进行排序的方法：

- Ping 时间 — 将 ICMP ping 发送到最近的五个资料库（基于子集值），并按响应时间排序。
- 子网值— 比较客户端系统和所有资料库的 IP 地址，并按数位的匹配程度对资料库进行排序。IP 地址越相近，资料库在列表中的位置越靠前。
- 资料库列表中的使用顺序— 按列表中的资料库顺序选择资料库。

3 取消选中资料库列表中资料库名称旁的复选框，可以禁用资料库。

4 如果在“资料库选择”中选择“用户定义的列表”，请单击“上移”或“下移”以指定客户端系统选择分布式资料库的顺序。

5 完成后，单击“保存”。

使用未托管的本地分布式资料库

使用此任务可以将主资料库内容复制并粘贴到未托管的分布式资料库。创建后，您必须手动配置托管系统以转至非托管的资料库来获取文件。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 从服务器复制主资料库文件夹中的所有文件和子目录。默认情况下，它位于服务器上的以下位置：

C:\Program Files\Mcafee\ePO\4.0.0\DB\Software

2 将复制的文件和子文件夹粘贴到分布式资料库系统的资料库文件夹。

3 将托管系统的代理策略配置为使用新的未托管分布式资料库：

a 创建新代理策略或打开现有的策略进行编辑。

小心: 不能中断策略选项卡的策略继承。因此，在将此策略应用到系统时，确保只有所需的系统接收和继承策略以使用未托管的分布式资料库。

b 选择“资料库”选项卡。

c 单击“资料库列表”旁的“添加”。此时会出现“添加资料库”页。

d 输入“资料库名称”文本字段中的名称。该名称不必是存放资料库的系统的名称。

e 在“检索文件来源”下，选择资料库的类型。

f 在“资料库配置”下，使用适合资料库类型的相应语法输入创建的位置。

g 输入端口号，或保留默认端口。

h 根据需要配置身份验证凭据。

i 单击“确定”以将新分布式资料库添加到列表。

j 在列表中选择新资料库。

类型为“本地”，表示其未被 ePolicy Orchestrator 管理。如果选择“资料库列表”中的非托管资料库，则会启用“编辑”和“删除”按钮。

k 单击“保存”。

此策略应用到的任何系统都会在下次代理与服务器通讯时收到新策略。

手动签入引擎、DAT 和 EXTRA.DAT 更新包

使用此任务可以手动将更新包签入主资料库，以使用 ePolicy Orchestrator 部署这些包。有些包只能手动签入。

开始之前

您必须具有相应的权限才能执行此任务。

注意: 不能在纳入或复制任务正在执行时签入包。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”，然后单击“签入包”。此时会出现“签入包”向导。

2 选择包类型，然后浏览到所需的包文件并选择此文件。

3 单击“下一步”。此时会出现“包选项”页。

4 在“分支”旁，选择所需的分支。

如果您的环境要求先测试新包，然后再部署这些包，则 McAfee 建议使用“评估”分支。在测试完包后，可以将这些包移到“软件”|“主资料库”选项卡上的当前分支。

5 在“选项”旁，选择是否：

- 支持 Netshield for NetWare - 如果要为 NetShield for NetWare 签入包，则选择此选项。
- 将现有包移到“早期”分支 - 如果要将现有包（签入时同一类型）移到“早期”分支，则选择此选项。

6 单击“保存”开始签入该包。在包签入时，请稍候。

新包会出现在“主资料库”页上的“主资料库中的包”列表中。

使用计划更新任务定期更新托管系统

使用此任务可以创建和配置更新任务。如果不使用全局更新，McAfee 建议使用日常更新客户端任务，确保系统具有最新的 DAT 和引擎文件。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“系统”|“系统树”|“客户端任务”，在系统树中选择要将任务应用到的所需组，然后单击“新建任务”。此时会出现“客户端任务构建器”向导的“描述”页。

2 命名并描述该任务。

3 从“类型”下拉列表中选择“更新(McAfee Agent)”，然后单击“下一步”。此时会出现“配置”页。

4 选择是否将“更新正在进行”对话框显示给最终用户。如果选择此选项，您还可以将推迟更新功能提供给最终用户。

5 单击“下一步”此时会出现“计划”页。

6 根据需要计划任务，然后单击“下一步”。此时会出现“摘要”页。

7 查看任务的详细信息，然后单击“保存”。

任务会添加到应用到组和系统的客户端任务的列表中。代理将在下次与服务器通讯时接收新的更新任务信息。如果启用了此任务，更新任务将在下一个计划的日期和时间运行。根据为该客户端代理配置策略的方式，每个系统将从相应的资料库进行更新。

确认客户端正在使用最新的 DAT 文件

使用此任务可以检查托管系统上 DAT 文件的版本。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

- 转至“报告”|“查询”，在“查询”列表中选择“VSE: DAT 部署”，然后单击“运行查询”。

  注意: 有关该查询的详细信息，请参阅 VirusScan Enterprise 文档。

分发之前评估新的 DAT 和引擎

使用此任务可以通过评估分支测试更新包。您可能需要在将 DAT 和引擎文件部署到整个组织之前，在一些系统上进行测试。

ePolicy Orchestrator 为此提供了三个资料库分支。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 创建一个计划“复制纳入”任务，将更新包复制到主资料库评估分支。安排该任务在 McAfee 发布更新的 DAT 文件之后运行。

2 在系统树中创建或选择一个组作为评估组，然后为系统创建一个仅使用评估分支的 McAfee Agent 策略。（在“更新”选项卡的“资料库分支更新选择”区域中。）

   这些策略将在下次代理连接至服务器时生效。下次更新代理时，将从评估分支检索更新。

3 为评估系统创建计划更新客户端任务，此任务会更新资料库评估分支中的 DAT 和引擎文件。安排该任务在资料库纳入任务开始 1 或 2 个小时后运行。

   如果在评估组层级创建的评估更新任务会使该任务仅对该组运行。

4 监视评估组中的系统，直到满意要求为止。

5 使用“软件”|“主资料库”选项卡上的“更改分支”操作，将包从主资料库的评估分支移到当前分支。将这些包添加到当前分支后，就可以在工作环境中使用这些包。下次任何从当前分支检索包的更新客户端任务运行时，新 DAT 文件和引擎就会分发到使用此任务的系统。

在各分支之间手动移动 DAT 和引擎包

在将包签入主资料库后，使用此任务可以手动在评估分支、当前分支和早期分支之间移动包。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”。此时会出现“主资料库中的包”表。

2 在所需包的行中，单击“更改分支”。此时会出现“更改分支”页。

3 选择是否将包移到或复制到其他分支。

4 选择接收包的分支。

   注意: 如果网络中装有 NetShield for NetWare，请选择“支持 NetShield for NetWare”。

5 单击“确定”。

从主资料库中删除 DAT 或引擎包

使用此任务可以从主资料库中删除包。定期签入新更新包时，新更新包会取代旧版更新包，或将其移动到早期分支（如果您使用早期分支）。不过，您可能需要手动从主资料库中删除 DAT 或引擎包。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“软件”|“主资料库”。此时会出现“主资料库中的包”表。

2 在所需包的行中，单击“删除”。此时会出现“删除包”对话框。

3 单击“确定”。

发送通知

ePolicy Orchestrator 通知功能会在托管系统或 ePolicy Orchestrator 服务器上发生事件时提醒您。您可以在 ePolicy Orchestrator 中配置通知规则，以在 ePolicy Orchestrator 服务器接收和处理特定事件时，发送电子邮件消息或 SNMP 陷阱以及运行外部命令。生成通知消息的事件类别和此类消息发送频率的配置有很大的灵活性。

此功能专用于在满足规则条件时通知特定人员。这些条件包括（但不限于）：

- 防病毒软件产品检测威胁。尽管许多防病毒软件产品都受到支持，但来自 VirusScan Enterprise 的事件包含来源攻击者的 IP 地址，因此您可以隔离系统，防止感染环境中的其他系统。
- 病毒发作。例如，在 5 分钟内收到 1000 个检测到病毒的事件。
- ePolicy Orchestrator 服务器事件的高级符合性。例如，某个复制任务没有完成。

您还可以将通知规则配置成在满足指定条件时，执行命令并启动已注册的可执行文件。

是否首次设置通知？

服务器 > 系统树 > 代理 > 资料库 > 策略和任务 > 部署 > **高级功能**

首次设置通知时：

1 了解通知以及它如何与系统树和网络一起工作。

2 制定实施计划。哪些用户需要了解哪些事件？

3 如果您计划实现使用 SNMP 服务器、注册的可执行文件和外部命令的通知功能，请对它们进行定义。

4 创建通知规则。

目录

通知及其工作方式

在计划实现通知功能之前，应了解此功能是如何与 ePolicy Orchestrator 及系统树配合工作的。

注意: 此功能不遵循策略实施的继承模型。

当环境中的系统上发生事件时，这些事件会传递给服务器，而通知规则（与包含受影响的系统的组及其上的每个父组关联）由这些事件触发。如果满足任何此类规则的条件，则会根据该规则的配置发送通知消息或运行外部命令。

这种设计允许您在系统树的不同层级上配置不同的规则。这些规则的以下几项可以不同：

- 发送通知消息的阈值。例如，某个特定组的管理员希望，如果 10 分钟内在组中的 100 个系统上检测到病毒，则发送通知，但全局管理员却不希望在此情况下发送通知，除非相同时间内在整个环境中的 1000 个系统上检测到病毒。
- 通知消息的接收者。例如，某个特定组的管理员希望，仅当在组中发生指定数量的病毒检测事件时才接收通知。或者，全局管理员希望每个组管理员在整个系统树内发生指定数量的病毒检测事件时才接收通知消息。

限制与累积

您可以基于累积和限制来设置阈值，从而配置通知消息的发送时间。

累积

利用累积可以确定规则发送通知消息的事件阈值。例如，配置同一规则在以下情况下发送通知消息：服务器在一小时内从不同的系统收到 100 个病毒检测事件，且从任何系统收到 1000 个病毒检测事件。

限制

在将规则配置为将可能的病毒发作情况通知给您后，使用限制可以确保不会收到过多的通知消息。如果您管理的是大型网络，则可能会在一个小时之内收到数万个事件，但基于此类规则仅创建数千条通知消息。通知允许您对基于单一规则的通知消息的数量进行限制。例如，您可以在此同一规则中指定在 1 小时内仅接收一条通知消息。

通知规则和系统树案例

为说明此功能与系统树是如何配合工作的，我们假设以下两种案例。

在这两个案例中，我们都假定系统树的每个组均配置了类似的规则。每条规则均配置为在 60 分钟内从任何产品收到 100 个病毒检测事件时发送一条通知消息。为便于参考，将每个规则命名

为 VVirusDetected_<groupname>，其中 <groupname> 是出现在系统树中的组名（如 VirusDetected_Subgroup2c）。

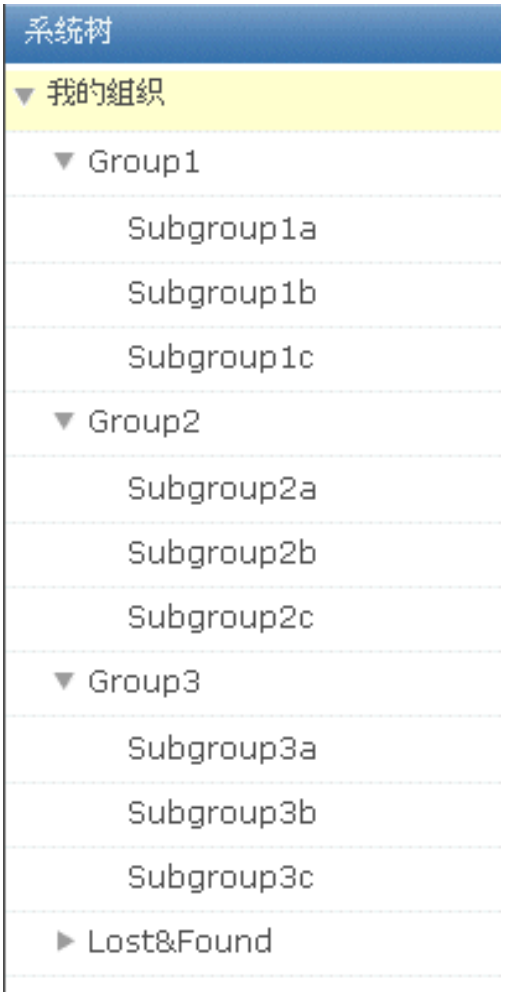

图 29：系统树通知案例

案例一

在此案例中，某天 60 分钟内在 Subgoup2C 中检测到 100 个病毒检测事件。

此情况符合规则 VirusDetected_Subgroup2C、VirusDetected_Group2 和 VirusDetected_MyOrganization 的条件，根据规则的配置发送通知消息（或启动已注册的可执行文件）。

案例二

在此案例中，假设某天 60 分钟内在 Subgroup2C 中检测到 50 个病毒检测事件，在 Subgroup3B 中检测到 50 个病毒感染事件。

此情况符合 VirusDetected_MyOrganization 规则条件，根据规则配置发送通知消息（或启动已注册的可执行文件）。这是可以应用于全部 100 个事件的唯一规则。

默认规则

ePolicy Orchestrator 提供了六个默认规则，在您对此功能有了进一步的了解后，就可以启用这些规则以立即使用。

注意: 默认规则在启用后，会将通知消息发给 ePO 安装向导中提供的电子邮件地址。

在启用任何默认规则之前，请：

- 指定发送通知消息的来源电子邮件服务器（位于“配置”|服务器设置）。
- 确保收件人的电子邮件地址是要接收电子邮件的地址。此地址在向导的“通知”页配置。

默认通知规则

规则名称	关联事件	配置
每日未知产品通知	来自所有未知产品的事件。	每天最多发送一条通知消息。
每日未知类别通知	未知类别的任何事件。	每天最多发送一条通知消息。
检测到病毒但未删除	来自任何产品的“检测到病毒但未删除”事件。	发送通知消息： • 当 1 小时内收到的事件数量超过 1000 个时。 • 最多每两小时发送一次。 • 包含来源系统 IP 地址、实际病毒名称以及实际产品信息（如果有）。 • 受影响的系统数量至少为 500 个。
检测到病毒(启发式)但未删除	来自任何产品的“检测到病毒(启发式)但未删除”事件。	发送通知消息： • 当 1 小时内收到的事件数量超过 1000 个时。 • 最多每两小时发送一次。 • 包含来源系统 IP 地址、实际病毒名称以及实际产品信息（如果有）。 • 受影响的系统数量至少为 500 个。
资料库更新或复制失败	资料库更新或复制失败	接收到任何事件时发送通知消息。
检测到不符合的计算机	“检测到不符合的计算机”事件。	从“生成符合性事件”服务器任务收到任何事件时发送通知消息。

计划

在创建发送通知的规则之前，进行计划可以节约时间：

- 在环境中触发通知消息的事件类型（产品和服务器）。
- 哪些人应该收到哪些通知消息。例如，没有必要将 A 组发生的复制失败事件通知给 B 组的管理员，但您可能希望所有管理员都了解在 A 组发现了感染病毒的文件。
- 要为每条规则设置的阈值类型和级别。例如，您可能不希望病毒发作期间每次检测到感染病毒的文件时均收到电子邮件。相反，您可以将此类电子邮件设置为最多每五分钟发送一次，无论该服务器接收事件的频率如何。
- 在满足某条规则条件时，要运行哪些命令或注册的可执行文件。

确定转发事件的方式

使用这些任务可以确定转发事件的时间以及立即转发哪些事件。

服务器从代理接收通知。您必须配置策略，以便立即将事件转发到服务器或仅在代理与服务器通讯间隔转发。

如果选择立即发送事件（这是默认设置），则代理会在收到这些事件后立即转发。如果您希望所有事件在发生时立即发送到服务器，以便通知功能可以对其进行处理，请将代理配置为立即发送事件。

如果选择不立即发送所有事件，则代理仅立即转发那些被发出事件的产品指定为高优先级的事件。其他事件仅在代理与服务器通讯时发送。

任务

- 确定立即转发的事件
- 确定要转发的事件

确定立即转发的事件

使用此任务可以确定是立即转发事件，还是仅在代理与服务器通讯间隔转发。

如果当前应用的策略没有设置为立即上载事件，则可以编辑当前应用的策略或创建新 McAfee Agent 策略。此设置在“事件”选项卡上配置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 打开所需的代理策略，然后单击“事件”。
2 选择“启用优先级事件转发”。
3 选择事件严重性。所选严重性（以及更高严重性）的事件会立即转发到服务器。
4 要控制通讯量，请输入“上载间隔时间”（分钟）。
5 若要控制通讯量大小，请输入“每次上载的最大事件数”。
6 单击“保存”。

确定要转发的事件

使用此任务可以确定将哪些事件转发到服务器。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“服务器设置”，选择“事件过滤”，然后单击页面底部的“编辑”。
2 选择所需的事件，然后单击“保存”。

只有所有代理都连接后，这些设置才能生效。

设置 ePO 通知

使用这些任务可以配置所需的资源以发挥“通知”的最大效用。

使用此功能前，必须具有：

- 通知权限 — 创建或编辑权限集，并确保将其分配给相应的 ePO 用户。
- 电子邮件服务器 — 通过“配置”|“服务器设置”配置电子邮件 (SMTP) 服务器。
- 电子邮件联系人列表 — 通过“配置”|“联系人”指定可供您选择通知消息收件人的列表。
- SNMP 服务器 — 指定创建规则时要使用的 SNMP 服务器的列表。您可以配置这些规则在满足条件时向 SNMP 服务器发送 SNMP 陷阱，以启动通知消息。
- 外部命令 — 指定满足规则条件时运行的外部命令的列表。

任务

▸ 授予用户对通知的相应权限
▸ 使用 SNMP 服务器
▸ 使用注册的可执行文件和外部命令

授予用户对通知的相应权限

使用此任务可以确保所有所需的管理员对“通知”具有相应权限。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“权限集”。
2 单击“新建权限集”，或选择现有的权限集。
3 在“通知”旁，单击“编辑”。
4 选择所需的通知权限：
   - 无权限
   - 查看通知规则和通知日志

     注意: 此权限还具有查看 SNMP 服务器、注册的可执行文件和外部命令的功能。

   - 创建和编辑通知规则；查看通知日志

     注意: 此权限还具有查看 SNMP 服务器、注册的服务器和外部命令的功能。

   - 创建和编辑通知规则；查看和清除通知日志；创建和编辑 SNMP 服务器和外部命令
5 单击“保存”。
6 重复步骤 2 到步骤 4，直到您创建并编辑了所需的权限集为止。
7 如果您已为此创建了新的权限集，请转至“配置”|“用户”。
8 选择要将新权限集分配到的用户，然后单击“编辑”。
9 在“权限集”旁，选中包含所需通知权限的权限集旁的复选框，然后单击“保存”。
10 重复步骤 6 到步骤 8，直到所有用户都分配了适当的权限集为止。

使用 SNMP 服务器

使用这些任务可以将通知配置为使用 SNMP 服务器。您可以将“通知”配置为将 SNMP（Simple Network Management Protocol，简单网络管理协议）陷阱发送到 SNMP 服务器，这样您就可以接收 SNMP 陷阱，并在同一位置使用网络管理应用程序查看环境中有关系统的详细信息。

注意: 您无需进行其他配置或启动任何服务，就可以配置此功能。

任务

添加 SNMP 服务器

使用此任务可以添加 SNMP 服务器。要接收 SNMP 陷阱，您必须添加 SNMP 服务器的信息，这样 ePolicy Orchestrator 便会了解发送陷阱的位置。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“SNMP 服务器”，然后单击页底部的“新建 SNMP 服务器”。此时会显示“新建 SNMP 服务器”页。

2 提供 SNMP 服务器的名称和地址，然后单击“保存”。

已添加的 SNMP 服务器会出现在“SNMP 服务器”列表中。

复制 SNMP 服务器

使用此任务可以复制现有的 SNMP 服务器。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“SNMP 服务器”，然后单击新条目所基于的 SNMP 服务器旁的“复制”。

2 提供新名称，然后单击“保存”。

新 SNMP 服务器会出现在“SNMP 服务器”列表中。

编辑 SNMP 服务器

使用此任务可以编辑现有的 SNMP 服务器条目。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“SNMP 服务器”，然后单击所需 SNMP 服务器旁的“编辑”。

2 根据需要编辑“名称”和“地址”信息，然后单击“保存”。

删除 SNMP 服务器

使用此任务可以从通知中删除 SNMP 服务器。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“SNMP 服务器”，然后单击所需 SNMP 服务器旁的“删除”。

2 出现提示时，确认要删除 SNMP 服务器。

SNMP 服务器会从“SNMP 服务器”列表中删除。

导入 .MIB 文件

使用此任务可以建立规则以将通知消息通过 SNMP 陷阱发到 SNMP 服务器。您必须导入位于以下位置的 NAICOMPLETE.MIB 文件：

\Program Files\McAfee\ePolicy Orchestrator\MIB

网络管理程序使用此文件可以对 SNMP 陷阱中的数据进行解码，使其变为可理解的文本。

有关导入和实现 .MIB 文件的说明，请参阅网络管理程序的产品文档。

使用注册的可执行文件和外部命令

使用这些任务可以通过添加注册的可执行文件并向这些文件分配到命令来配置外部命令。您可以将通知规则配置为在启动规则时执行外部命令。

开始之前

在配置外部命令的列表前，请将注册的可执行文件放在服务器上规则可以访问的位置。

任务

- 使用注册的可执行文件
- 使用外部命令

使用注册的可执行文件

使用这些任务可以添加、编辑和删除注册的可执行文件。

开始之前

您必须具有相应的权限才能执行这些任务。

您必须从 ePO 服务器系统使用浏览器会话。

任务

- 添加注册的可执行文件
- 编辑注册的可执行文件
- 删除注册的可执行文件

添加注册的可执行文件

使用此任务可以将注册的可执行文件添加到可用资源。然后，您可以配置命令及其参数，并将其分配到注册的可执行文件。

开始之前

您必须具有相应的权限才能执行此任务。

您必须从 ePO 服务器系统使用浏览器会话。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“注册的可执行文件”，然后单击页面底部的“新建注册的可执行文件”。此时会出现“新建注册的可执行文件”页。

2 输入注册的可执行文件的名称。

3 输入路径，或浏览到触发规则时要规则执行的注册的可执行文件，选择此文件，然后单击“保存”。

新的注册的可执行文件会出现在“注册的可执行文件”列表中。

编辑注册的可执行文件

使用此任务可以编辑现有注册的可执行文件的条目。

开始之前

您必须具有相应的权限才能执行此任务。

您必须从 ePO 服务器系统使用浏览器会话。

任务

1 转至“自动”|“注册的可执行文件”，然后选择列表中所需可执行文件旁的“编辑”。此时会出现“编辑注册的可执行文件”页。

2 编辑名称，或选择系统上其他可执行文件，然后单击“保存”。

删除注册的可执行文件

使用此任务可以删除注册的可执行文件条目。

开始之前

- 您必须具有相应的权限才能执行此任务。
- 您必须从 ePO 服务器系统使用浏览器会话。

任务

1 转至“自动”|“注册的可执行文件”，然后选择列表中所需可执行文件旁的“删除”。

2 出现提示时，单击“确定”。

3 单击“确定”。

使用外部命令

使用这些任务可以添加、编辑和删除触发通知规则时启动注册的可执行文件的外部命令。

任务

- 添加与注册的可执行文件一起使用的外部命令
- 编辑外部命令
- 删除外部命令

添加与注册的可执行文件一起使用的外部命令

使用此任务可以对现有的注册可执行文件添加命令，配置命令的参数。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“外部命令”，然后单击页面底部的“新建外部命令”。此时会出现“新建外部命令”页。
2 输入命令的名称。
3 选择要将命令分配到的所需“注册的可执行文件”。
4 为命令行输入所需的“参数”，并根据需要插入任何变量，然后单击“保存”。

注意: 不支持在“参数”中使用扩展字符（例如 | 和 > ）将数据输出传送到文本文件（管道），但可以将其包含在自定义的可执行文件中实现这一点。

新外部命令会添加到“外部命令”列表。

编辑外部命令

使用此任务可以编辑现有的外部命令。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 请转至“自动”|“外部命令”，然后单击所需命令旁的“编辑”。此时会出现“编辑外部命令”页。
2 编辑命令的名称，选择其他注册的可执行文件，或更改命令的参数。
3 单击“保存”。

删除外部命令

使用此任务可以删除现有的外部命令。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 请转至“自动”|“外部命令”，然后单击所需命令旁的“删除”。
2 出现提示时，单击“确定”。
3 单击“确定”。

创建和编辑通知规则

使用这些任务可以创建和编辑通知规则。通过这些规则可以定义通知发送的时间、方式和收件人。

注意: 通知规则不存在顺序依赖性。

任务

- 描述规则
- 设置规则的过滤器
- 设置规则的阈值
- 配置规则的通知

描述规则

使用此任务可以开始创建规则。在“通知规则构建器”向导的“描述”页上可以：

- 指定该规则所应用的系统树组。
- 命名并描述该规则。
- 设置通知消息的优先级（仅在以电子邮件的形式发送时才能设置）。
- 启用或禁用规则。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“通知规则”，然后单击“新建规则”，或单击现有规则旁的“编辑”。此时会出现“通知规则构建器”向导，且同时显示“描述”页。

图 30：通知规则页

2 为此规则输入唯一名称。

注意: 每个服务器上的规则名称必须是唯一的。例如，如果某个用户创建一个名为“紧急警报”的规则，则其他用户（包括全局管理员）就不能创建同名规则。

3 在“注释”文本框中输入描述。

4 单击“定义于”文本框旁的“...”，然后在“选择树组”对话框中，选择规则应用到的所需系统树组。

5 将规则优先级设置为“高”、“中”或“低”。

注意: 规则的优先级用于在收件人收件箱中的电子邮件上设置标记。例如，选择“高”会在通知电子邮件旁出现一个红色的感叹号，而选择“低”则会在通知电子邮件旁出现一个蓝色的向下箭头。优先级对规则或事件的处理没有任何影响。

6 在“状态”旁选择规则是“启用”还是“禁用”。

7 击单“下一步”。

设置规则的过滤器

使用此任务可以在“通知规则构建器”向导的“过滤器”页上为通知规则设置过滤器。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 选择事件可以触发规则的“操作系统”的类型。

2 选择“产品”，这些产品的事件会启动该规则。

3 选择启动该规则的事件“类别”。

注意: “产品”和“类别”选择项目均必须为真才能触发规则并发送通知消息。例如，如果您选择“VirusScan”和“检测到病毒但未清理”，则该规则不会针对 Symantec Anti-Virus 的“检测到病毒但未清理”事件发送消息。如果只考虑事件类别，则选择“任何产品”。

4 在“威胁名称”中定义与威胁比较相符的使用模式：

a 从下拉列表中选择一个运算符。

b 输入运算符所作用的任意文本。

例如，使用病毒名称。选择“包含”作为运算符，然后在文本框中输入“nimda”。这会确保扫描事件来获取包含“nimda”的任何文本行。

注意: 如果您选择根据威胁名称进行过滤，则必须实际选择“产品”、“类别”和“威胁名称”，该规则才会发送通知消息。

5 单击“下一步”。

设置规则的阈值

使用此任务可以在“通知规则构建器”向导的“阈值”页上定义触发规则的时间。

规则的阈值是累积和限制的组合。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 在“累积”旁，选择是“对每个事件发送一条通知”，还是“如果此时间内发生多个事件，则发送通知”（即在一个定义好的时间长度内）。如果选择后者，请以分钟、小时或天为单位定义时间。

2 如果选择“如果此时间内发生多个事件，则发送通知”，则可以选择在符合指定的条件时发送通知。这些条件是：

- 当受影响的系统数量至少为一个已定义的系统数量。
- 当事件数量至少为一个已定义的事件数量。

- 任意一个（两项全选）。

注意: 您可以选择一项或两项都选。例如，您可以设置规则，在受影响的系统数量超过 300 或事件数量超过 3000 时发送通知，以先超过的阈值为准。

3 如果需要，在“限制”旁，选择“发送通知最大间隔时间为”，定义必须经过多长时间该规则才能再次发送通知消息。时间以分钟、小时或天为单位。

4 单击“下一步”。

配置规则的通知

使用此任务可以配置“通知规则构建器”向导的“通知”页上由规则触发的通知。这些通知可以是电子邮件、SNMP 陷阱或外部命令。消息的大小取决于目标、消息的类型和消息收件人的数量。

通过使用通知类型下拉列表旁的“+”和“-”按钮，可以将规则配置成触发多条消息、SNMP 陷阱和外部命令。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 如果您希望通知消息以电子邮件或文本寻呼机消息的形式发送，请从下拉列表中选择“电子邮件”。

a 在“收件人”旁，单击“...”，然后选择邮件的收件人。此可用收件人的列表来自“联系人”（“配置”|“联系人”）。另外，您可以手动输入逗号分隔的电子邮件地址。

b 输入邮件的“主题”行。（可选）您可以将任何可用变量直接插入主题。

c 输入要在邮件“正文”中显示的任何文本。（可选）您可以将任何可用变量直接插入正文。

d 从“以下列语言的值替换变量”下拉列表中，选择显示变量的语言。

e 如果完成，请单击“下一步”，或单击“+”再添加一个通知。

2 如果您希望通知消息以 SNMP 陷阱形式发送，请从下拉列表中选择“SNMP 陷阱”。

a 从下拉列表中选择所需的“SNMP 服务器”。

b 从“以下列语言的值替换变量”下拉列表中，选择显示变量的所需语言。

c 在 SNMP 陷阱中选择“要包含的变量”。

- 通知规则名称
- 规则定义于
- 选定的类别
- 首个事件时间
- 事件描述
- 事件实际数量
- 实际类别
- 来源系统
- 受影响的系统名称
- 受影响的对象
- 规则组
- 选定的产品
- 选定的威胁或规则名称
- 事件 ID
- 实际的系统数量
- 实际产品
- 实际威胁或规则名称
- 受影响的系统 IP 地址
- 通知发送时间
- 其他信息

注意: 有些事件不包含此信息。如果您选择的信息未出现，则表明该信息在事件文件中不可用。

d 如果完成，请单击“下一步”，或单击“+”再添加一个通知。

3 如果您希望通知是执行外部命令：

a 从“外部命令”下拉列表中选择所需的外部命令。

b 从“以下列语言的值替换变量”下拉列表中，选择显示变量的所需语言。

c 如果完成，请单击“下一步”，或单击“+”再添加一个通知。

4 单击“下一步”后，将会出现“摘要”页。确认信息正确，然后单击“保存”。

新通知规则将出现在“通知规则”列表中。

查看通知的历史记录

使用这些任务可以在“通知日志”页上访问不同类型的信息，并对这些信息采取操作。

“通知日志”页允许您查看已发送通知的历史记录。您可以按产品或类别查看所有已发送通知的综合摘要，也可以查看所有已发送的特定通知的列表。

任务

- 配置通知日志
- 查看通知日志条目的详细信息
- 清除通知日志

配置通知日志

使用此任务可以配置和查看系统树的指定位置、一段指定的时间内，按产品、类别、优先级或规则名称发送的通知数量的摘要。

在此版 ePolicy Orchestrator 中，可以立即以摘要表、饼图或条形图形式显示通知日志中的信息。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“通知日志”。

2 从“时间过滤器”下拉列表中，选择要查看通知历史记录的所需时间段。

3 单击“系统树过滤器”文本框旁的“...”。此时会显示“选择过滤所依据的组”对话框。

4 选择所需的系统树组以查看其通知历史记录。

注意: 用户仅限于查看对部分系统树有权限的通知历史记录。

5 从“分组方式”下拉列表框中，选择“产品”、“类别”、“优先级”或“规则名称”。此选择会确定显示日志条目时，这些条目是如何组织的。

6 从“显示类型”下拉列表中，选择“摘要表”、“饼图”或“条形图”。此选择确定显示数据的格式。您可以单击任一显示类型中的元素，以进一步查看项目的详细信息。

7 使用“排序方式”下拉列表可以按所需的顺序显示条目。

查看通知日志条目的详细信息

使用此任务可以查看通知的详细信息。可以通过单击任何列的标题，按该列的数据对此列表进行排序。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 根据需要配置通知日志。

2 单击显示中的所需摘要表行、饼图扇区或条形。此时会出现一个标准表，显示与已单击的主要显示元素对应的所有通知的列表。

   注意: 用户只能查其具有权限的系统树节点的通知。

3 若要对列表排序，请从“排序方式”下拉列表中使用选项。

4 单击表中的任一通知可以查看其详细信息。

清除通知日志

使用此任务可以清除通知日志中的通知。可以根据通知的存在时间来清除通知。

注意:清除通知日志中的项目时，符合时间标准的所有通知都会被清除，无论这些通知来自系统树的哪一部分。

开始之前

您必须具有权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“通知日志”，然后单击页面底部的“清除”。此时会显示“清除通知日志”对话框。

2 选择天数、周数、月树或年数，以清除具有该存在时间或具有更早时间的所有项目，或选择运行创建好的用于此用途的查询。

符合此标准的通知日志条目会永久删除。

产品和组件列表

您可以配置规则，针对特定产品和组件的特定事件类别生成通知消息。下面是您可以为其配置规则的产品和组件列表以及所有可能的事件类别列表。

支持的产品和组件

- Desktop Firewall
- Host Intrusion Prevention
- ePO Server
- McAfee Agent
- GroupShield Domino
- GroupShield Exchange
- System Compliance Profiler
- Symantec NAV
- NetShield for NetWare
- PortalShield
- Stinger
- 未知产品
- Virex
- VirusScan Enterprise
- LinuxShield
- Security Shield

常见问题

如果为病毒检测设置了通知规则，是否在病毒发作时会收到每个已接收事件的通知消息？

不会，您可以这样配置规则，即只有在指定的时段内发生指定数量的事件时才发送一次通知，或者在指定时间内最多只能发送一次通知。

是否可以创建一条具有多个收件人的通知？

可以，您可以在“通知规则构建器”向导中为多个收件人输入电子邮件地址。

是否可以创建一条生成多个通知类型的规则？

可以，ePolicy Orchestrator 的通知功能在每条规则中支持以下通知的任意组合：

- 电子邮件（包括标准 SMTP、SMS 和文本寻呼机）。
- SNMP 服务器（通过 SNMP v1 陷阱）。
- 安装在 ePolicy Orchestrator 服务器上的任何外部工具。

查询数据库

ePolicy Orchestrator 4.0 随附有自己的查询和报告功能。这些功能可高度自定义，非常灵活且易于使用。随附的“查询构建器”向导可以创建和运行在用户配置的图表和表中产生用户配置数据的查询。

为便于您开始操作，McAfee 包含一组默认查询，其提供的信息与早期版本的默认报告提供的信息相同。

是否首次设置查询？

首次设置查询时：

1 了解查询的功能和“查询构建器”向导。

2 查看默认查询，并根据需要编辑任何查询。

3 如果默认查询无法满足需要，请根据您的要求创建查询。

目录

查询

查询是检索和显示数据库中数据的可配置对象。查询的结果会以图表和表的形式显示。可以采用多种格式将任何查询结果导出，这些格式都可以下载并以电子邮件附件的形式发送。某些查询可以用作仪表板监视器。

查询结果是可操作的

现在查询结果是可操作的。表（和深入查询表）中显示的查询结果具有多种可对表中的选定项目采取的操作。例如，您可以将代理部署到查询结果表中的系统。可以在结果页的底部使用操作。

将查询用作仪表板监视器

几乎可以将任何查询（使用表显示最初结果的查询除外）用作仪表板监视器。仪表板监视器会以用户配置的时间间隔（默认值为 5 分钟）自动刷新。

导出的结果

可以采用四种不同格式将查询结果导出。导出的结果是历史数据且不能进行刷新，与将查询用作仪表板监视器一样。与控制台中显示的查询结果和基于查询的监视器类似，您可以深入查询 HTML 导出报告以获取详细信息。

但导出报告中的数据是不可操作的，这一点与控制台中的查询结果不同。

报告可以采用下列几种格式：

- CSV — 采用此格式可以在电子表格应用程序（如 Microsoft Excel）中使用数据。
- XML — 采用此格式可以转换数据以用于其他用途。
- HTML — 采用此报告格式可以通过 Web 页的形式查看导出的结果。
- PDF — 需要打印结果时使用此报告格式。

在服务器间共享查询

任何查询都可以导入和导出，这使您可以在服务器间共享查询。在多服务器环境中，任何查询都只需创建一次。

公共查询和个人查询

查询可以分为个人查询或公共查询。个人查询存在于用户的“我的查询”列表中，只有创建者才可使用。公共查询存在于“公共查询”列表中，有权使用公共查询的所有人都可以使用。

只有全局管理员才能使用大多数默认查询，全局管理员必须公开这些默认查询，其他用户才可以访问。默认情况下，有几个查询是公共查询，可以通过默认仪表板使用。

只有具有相应权限的用户才能公开个人查询。

查询权限

使用查询权限可以将特定级别的查询功能分配给权限集，而权限集会分配给各用户。

可用的权限包括：

- 无权限 — “查询”选项卡对无权限的用户不可用。
- 使用公共查询 — 授予权限以使用由具有相同权限的用户创建和公开的所有查询。
- 使用公共查询；创建并编辑个人查询 — 授予权限以使用由具有相同权限的用户创建和公开的所有查询，以及提供使用“查询构建器”向导创建和编辑个人查询的功能。
- 编辑公共查询；创建并编辑个人查询；公开个人查询 — 授予权限以使用和编辑任何公共查询，创建并编辑任何个人查询，以及提供任何可以访问公共查询的用户使用任何个人查询的功能。

注意: 若要运行某些查询，您还需要与查询结果类型关联的功能集的权限。另外，在查询结果页中，对结果项目采取的操作取决于用户具有权限的功能集。

查询构建器

ePolicy Orchestrator 提供一个便捷的四步向导来创建和编辑自定义查询。通过此向导，您可以配置检索和显示的数据，以及数据的显示方式。

结果类型

在“查询构建器”向导中首先要选择结果类型。此选择会确定查询将检索的数据类型。此选择还会确定向导其余部分的可用选择项目。

结果类型包括:

- 审核日志条目 — 检索 ePO 用户所进行的更改和操作的信息。
- 符合性历史记录 — 检索一段时间的符合性计数的信息。此查询类型及其结果取决于“运行查询”服务器任务，此任务会根据某个（布尔饼图）查询的结果生成符合性事件。另外，创建符合性历史记录查询时，时间单位必须与服务器任务的计划时间间隔相符。McAfee 建议先创建饼图查询，接着创建生成符合性事件的服务器任务，最后创建符合性历史记录查询。
- 事件 — 检索从托管系统发来的事件的信息。
- 托管系统 — 检索运行 McAfee Agent 的系统的有关信息。
- 通知 — 检索有关已发送通知的信息。
- 资料库 — 检索资料库及其状态的数据。
- 汇总的符合性历史记录 — 检索一段时间注册的 ePO 服务器中符合性计数的信息。此查询取决于在此 ePO 服务器和注册的服务器上运行的服务器任务。
- 汇总的托管系统 — 从注册的 ePO 服务器中检索有关系统的摘要信息。

图表类型

ePolicy Orchestrator 提供许多显示所检索数据的图表和表。这些图表和表及其深入查询表都是高度可配置的。

注意: 表中不包含深入查询表。

图表类型包括：

- 条形图
- 布尔饼图
- 分组条形图
- 分组摘要表
- 折线图
- 饼图
- 摘要表
- 表

表列

指定表的列。如果您选择“表”作为数据的主要显示方式，则会以此配置该表。如果您选择了一种图表类型作为数据的主要显示方式，则会以此配置深入查询表。

表中显示的查询结果是可操作的。例如，如果用系统填充了表，则可以直接从表中部署或唤醒这些系统中的代理。

过滤器

通过选择属性和运算符来指定标准，以限制查询检索的数据。

多个服务器汇总查询

ePolicy Orchestrator 4.0 现在提供运行可报告多个 ePO 数据库中摘要数据的查询的功能。“查询构建器”向导中有这些结果类型，您可以对此类型的查询使用这些结果类型：

- 汇总的托管系统
- 汇总的符合性历史记录

这些查询类型的结果是不可操作的。

工作原理

若要汇总数据以供汇总查询使用，必须注册要包含在查询中的每个服务器（包括本地服务器）。

注册服务器后，必须在报告服务器（执行多个服务器报告的服务器）上配置“数据汇总”服务器任务。“数据汇总”服务器任务会从报告中涉及的所有数据库中检索信息，并填充报告服务器上的 eporollup_ 表。

汇总查询会对报告服务器上的这些数据库表进行查询。

注意: 使用“汇总的符合性历史记录”查询类型需要一个额外的查询（在托管系统上使用布尔饼图）和一个额外的“运行查询”服务器任务（使用子操作以生成符合性事件），以在每个您要将其数据包含在“汇总的符合性历史记录”查询类型的服务器上运行。

准备汇总查询

使用这些任务可以确保填充报告服务器上的 eporollup_ 表，并随时使用基于汇总查询结果类型的查询。应对要将数据包含在查询结果中的每个服务器执行这些任务。

注意: 使用“汇总的符合性历史记录”结果类型还需要在每个服务器上创建对托管系统的基于布尔饼图的查询。此外，在每个服务器上，需要通过子操作创建“运行查询”服务器任务，以生成基于此查询的符合性事件。

任务

- 注册 ePO 服务器
- 创建数据汇总服务器任务

注册 ePO 服务器

使用此任务可以将每个 ePO 服务器注册到包含在汇总查询中的报告服务器。您还必须注册报告服务器。注册服务器会确保可从每个服务器中获取摘要数据，以填充本地数据库中的 eporollup_ 表。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“网络”|“已注册的服务器”，然后单击“新建服务器”。此时会出现“已注册的服务器生成器”向导。
2 选择服务器类型并输入名称和描述，然后单击“下一步”。此时会出现“详细信息”页。
3 提供服务器、其数据库服务器以及访问服务器的凭据的详细信息，然后单击“保存”。

创建数据汇总服务器任务

使用此任务可以创建“数据汇总”服务器任务，该任务会用注册的服务器中的摘要数据填充报告服务器上的所需表。

最佳实践

McAfee 建议在此服务器上为每个注册的服务器创建一个“汇总数据”服务器任务。此任务包含每个所需的“汇总数据”操作，每个操作仅针对一个注册的服务器执行。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“服务器任务”，然后单击“新建任务”。此时会出现“服务器任务生成器”向导

2 输入任务的名称和描述，选择是否启用此任务，然后单击“下一步”。此时会出现“操作”页。

3 选择所需的“数据汇总”操作，并选择此操作应用到的所需注册服务器。

注意: McAfee 建议每个注册的服务器创建一个服务器任务，并将其配置为运行两个“汇总数据”操作。

4 单击“下一步”此时会出现“计划”页。

5 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。

注意: 如果您在汇总符合性历史记录数据，则确保“汇总符合性历史记录”查询的时间单位符合注册的服务器上“生成符合性事件”服务器任务的计划类型。

6 查看设置，然后单击“保存”。

使用查询

使用这些任务可以创建、使用和管理查询。

任务

- 创建自定义查询
- 运行现有查询
- 按计划运行查询
- 公开个人查询
- 复制查询
- 在 ePO 服务器之间共享查询

创建自定义查询

使用此任务可以通过“查询构建器”向导创建自定义查询。您可以查询系统属性、产品属性、许多日志文件、资料库等等。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“查询”，然后单击“新建查询”。此时会出现“查询构建器”向导的“结果类型”页。

2 选择此查询的数据类型。此选择会决定向导后续页上的可用选项。

3 单击“下一步”此时会出现“图表”页。

4 选择显示主要查询结果的图表或表的类型。您可以使用不同的配置选项，具体取决于图表类型。

5 单击“下一步”此时会出现“列”页。

6 从“可用列”列表中选择要作为结果表中列的属性，然后根据需要通过列标题上的箭头图标进行排序。

注意: 如果在“图表”上选择“表”，则您在此选择的列为该表中的列。否则，这些列是深入查询表中的列。

7 单击“下一步”此时会出现“过滤器”页。

8 选择属性以缩小搜索结果的范围。选定的属性会显示在内容窗格中，其中含有的运算符可以指定标准以缩小为该属性返回的数据的范围。确保您所做的选择提供在上一步中配置的表列中显示的数据。

9 单击“运行”。“未保存的查询”页显示可操作的查询结果，因此您可以对任何表或深入查询表中的项目采取任何可用的操作。

- 如果要再次使用此查询，请单击“保存”，将其添加到“我的查询”列表中。
- 如果查询没有返回预期的结果，请单击“编辑查询”以返回“查询构建器”并编辑此查询的详细信息。
- 如果不需要保存查询，请单击“关闭”。

运行现有查询

使用此任务可以在“查询”页上运行现有查询。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“查询”，然后从“查询”列表中选择查询。

2 单击“运行”。此时会出现查询结果。深入查询报告并根据需要对项目采取操作。可用操作取决于用户的权限。

3 完成后，单击“关闭”。

按计划运行查询

使用此任务可以创建并计划一个运行查询并对查询结果采取操作的服务器任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“自动”|“服务器任务”，然后单击“新建任务”。此时会出现“任务构建器”向导的“描述”页。

2 提供任务的名称并描述任务，然后单击“下一步”。此时会出现“操作”页。

3 从下拉列表中选择“运行查询”。

4 所选要运行的所需查询。

5 选择显示结果所采用的语言。

图 31：运行查询服务器任务操作

6 选择对结果采取的操作。可用操作取决于用户的权限，并包括：

- 通过电子邮件发送文件 — 采用用户配置的格式（PDF、XML、CSV 或 HTML）将查询结果发给指定的收件人。
- 移动到 — 将查询结果中的所有系统移到系统树的组中。此选项仅对产生系统表的查询有效。
- 更改分类状态 — 对查询结果的所有系统启用或禁用系统树分类。此选项仅对产生系统表的查询有效。
- 排除标记 — 从查询结果中的所有系统中排除指定的标记。此选项仅对产生系统表的查询有效。
- 生成符合性事件 — 根据查询中与标准不符的系统的百分比或实际数量的阈值生成事件。此操作专用于在托管系统上检索数据的基于符合性的布尔饼图查询（如“ePO: 符合性摘要”默认查询）。此操作可以部分取代早期版本 ePolicy Orchestrator 的符合性检查服务器任务。
- 资料库复制 — 将主资料库内容复制到查询结果中的分布式资料库。对返回过期资料库列表的查询（如“ePO: 分布式资料库状态”默认查询），此操作很有用。此选项仅对产生分布式资料库的表的查询有效。
- 清除标记 — 从查询结果中的所有系统中删除指定的标记。此选项仅对产生系统表的查询有效。
- 分配策略 — 将指定的策略分配给查询结果中的所有系统。此选项仅对产生系统表的查询有效。
- 导出到文件 — 将查询结果导出为指定的格式。导出文件放置在“打印和导出”服务器设置中指定的位置。
- 应用标记 — 将指定的标记应用到查询结果中的所有系统（未排除此标记的系统）。此选项仅对产生系统表的查询有效。
- 编辑描述 — 覆盖数据库中查询结果中所有系统的现有系统描述。此选项仅对产生系统表的查询有效。
- 部署代理 — 根据此页上的配置将代理部署到查询结果中的系统。此选项仅对产生系统表的查询有效。
- 唤醒代理 — 根据此页上的配置将代理唤醒呼叫发送到查询结果中的所有系统。此选项仅对产生系统表的查询有效。

注意: 您可以对查询结果选择多项操作。单击“+”按钮可以添加要对查询结果采取的其他操作。请务必确保放置操作的顺序与对查询结果采取操作的顺序一致。

7 单击“下一步”此时会出现“计划”页。

8 根据需要安排任务，然后单击“下一步”。此时会出现“摘要”页。

9 验证任务的配置，然后单击“保存”。

任务会添加到“服务器任务”页的列表中。如果已启用此任务（默认设置），则它会在下个计划的时间运行。如果已禁用此任务，则只有单击“服务器任务”页上此任务旁的“运行”才能运行。

公开个人查询

使用此任务可以公开个人查询。对公共查询具有权限的所有用户都可以访问您公开的任何个人查询。

开始之前

您必须具有相应的权限才能执行此任务。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“查询”，然后从“我的查询”列表中选择所需的查询。

2 单击页底部的“公开”。

注意: 要访问“公开”操作，可能需要单击“更多操作”。

3 当出现提示时，单击“操作”面板中的“确定”。

此查询会添加到“公共查询”列表。现在，可以访问公共查询的所有用户都可以访问此查询。

复制查询

使用此任务可以根据现有查询来创建查询。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“查询”，然后从“查询”列表中选择所需的查询。

2 单击“复制”，提供副本的名称，然后单击“确定”。

3 在“查询”列表中选择新查询，然后单击“编辑”。此时会显示“查询构建器”向导，其设置与复制来源的查询完全相同。

4 根据需要编辑查询，然后单击“保存”。

在 ePO 服务器之间共享查询

使用这些任务可以导入和导出查询，以便在多个服务器之间使用。

任务

- 导出查询供其他 ePO 服务器使用
- 导入查询

导出查询供其他 ePO 服务器使用

使用此任务可以将查询导出为 XML 文件，然后可以将此文件导入其他 ePO 服务器。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“查询”，然后从“查询”列表中选择查询。

2 单击“导出”，然后在“操作”面板中单击“确定”。此时会出现“文件下载”对话框。

3 单击“保存”，为 XML 文件选择所需的位置，然后单击“确定”。

此文件便保存在指定的位置。

导入查询

使用此任务可以导入从其他 ePO 服务器导出的查询。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“报告”|“查询”，然后单击“导入查询”。此时会出现“导入查询”对话框。

2 单击“浏览”。此时会出现“选择文件”对话框。

3 选择导出的文件，然后单击“确定”。

4 单击“确定”。

查询会添加到“我的查询”列表。

将查询结果导出为其他格式

使用此任务可以导出查询结果以用于其他用途。您可以导出为 HTML 和 PDF 格式进行查看，也可以导出为 CSV 或 XML 文件，供其他应用程序使用和转换数据。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 在显示查询结果的页中，从“选项”菜单中选择“导出表”或“导出数据”。此时会出现“导出”页。

2 选择是分别导出数据文件，还是导出为一个存档 (ZIP) 文件。

3 如果需要，请选择是仅导出图表数据，还是导出图表数据及深入查询表。

4 选择导出文件的格式。如果导出为 PDF 文件，请选择页面大小和方向。

5 选择是否将文件作为电子邮件附件发给选定的收件人，或是否将其保存到服务器上提供链接的位置。您可以通过右键单击文件，将其打开或保存到其他位置。

   注意: 如果输入多个收件人的电子邮件地址，则必须使用逗号或分号分隔每个条目。

6 单击“导出”。

随即会创建文件，并以电子邮件附件的方式发给收件人，或将您带到一个页面，可以在此通过链接访问这些文件。

默认查询及其显示的内容

这些查询可以用于各种用途及任务。本主题介绍每个默认查询。安装的任何产品扩展都可以添加其自己的默认查询。默认查询标题以产品缩写开头。（例如，VirusScan 企业查询全部以“VSE”

开头）。本文档的此部分仅介绍 McAfee Agent 和 ePO 查询。有关其默认查询的其他信息，请参阅产品文档。

MA: 代理通讯摘要查询

使用此查询（采用其默认设置）可以查看托管系统的布尔饼图，该饼图根据代理是否在前一天与服务器进行通讯来划分。

查询结果

查询结果以布尔饼图的形式显示，您可以使用该饼图深入查询组成饼图各扇区的系统。

ePolicy Orchestrator 3.6 中的比较报告

此查询会替代以下各项的全部或部分：

- 代理与服务器的连接信息

MA: 代理版本摘要查询

使用此查询（采用其此默认设置）可以查看按托管系统运行的代理版本组织的托管系统的饼图。

查询结果

查询结果以饼图的形式显示，可以使用该饼图深入查询组成每个扇区的系统的表。

ePolicy Orchestrator 3.6 中的比较报告

此查询会替代以下各项的全部或部分：

- 代理版本

ePO: 符合性历史记录查询

使用此查询（采用其默认设置）可以查看环境中不符合系统的百分比（一段时间）。

开始之前

此查询及其结果取决于“生成符合性事件”服务器任务。安排此服务器任务以定期间隔运行，并确保选中“保存结果”复选框。此查询取决于基于托管系统的布尔饼图查询（如默认的“ePO: 符合性摘要”查询）。

查询结果

查询结果以折线图的形式显示。详细信息取决于“ePO: 符合性摘要”查询的已定义符合性。

ePolicy Orchestrator 3.6 中的比较报告

此查询会替代以下各项的全部或部分：

- DAT/病毒特征码部署摘要
- DAT 引擎覆盖范围

ePO: 符合性摘要查询

使用此查询（采用其默认设置）可以按 VirusScan Enterprise、McAfee Agent 和 DAT 文件版本显示环境中的哪些托管系统是符合的，哪些系统是不符合的。

此查询仅考虑最近 24 小时与服务器通讯的系统。

查询结果

此查询结果以布尔饼图的形式显示。一个扇区代表符合的系统，另一个扇区代表不符合的系统。每个扇区中系统的数量显示在扇区标签中。您可以深入查询任一扇区的可操作系统表。

ePolicy Orchestrator 3.6 中的比较报告

此查询会替代以下各项的全部或部分：

- DAT/病毒特征码部署摘要
- DAT 引擎覆盖范围

ePO: 恶意检测历史记录查询

使用此查询（采用其默认设置）可以查看上个季度内部病毒检测数量的折线图。

查询结果

查询结果会以折线图的形式显示，可用于深入查询事件及发生事件的系统的详细信息。

ePolicy Orchestrator 3.6 中的比较报告

此查询会替代以下各项的全部或部分：

- DAT/病毒特征码部署摘要
- DAT 引擎覆盖范围

ePO: 分布式资料库状态查询

使用此查询（采取其默认设置）可以查看分布式资料库的布尔饼图，该饼图按分布式资料库上次复制是否成功来划分。

查询结果

查询结果以布尔饼图的形式显示，可用于深入查询该饼图扇区资料库的表，该表显示每个资料库的名称、类型和状态。

ePO: ePO 控制台中失败的用户操作查询

使用此查询（采用其默认设置）可以查看审核日志中所有失败操作的表。

查询结果

查询结果以表的形式显示，可用于深入查询审核操作、事件以及发生事件的系统的详细信息。

ePO: 失败登录尝试查询

使用此查询（采用其默认设置）可以查看按审核日志中所有登录尝试是否成功来划分的这些登录尝试的布尔饼图。

查询结果

查询结果以布尔饼图的形式显示，可用于深入查询事件以及发生事件所针对的用户的详细信息。

ePO: 多服务器符合性历史记录查询

使用此查询（采用其默认设置）可以查看注册服务器中不符合系统的百分比（一段时间）。

开始之前

此查询及其结果取决于“数据汇总: 符合性历史记录”服务器任务。计划“数据汇总: 符合性历史记录”服务器任务以定期时间间隔运行，并确保选中“保存结果”复选框。另外，创建此类型的服务器任务时，计划类型必须符合此查询的时间单位。默认情况下，此查询的时间单位符合默认汇总数据（本地 ePO 服务器）服务器任务的计划类型。

查询结果

此查询返回折线图。详细信息取决于配置“数据汇总: 符合性历史记录”服务器任务的配置方式。

ePolicy Orchestrator 3.6 中的比较报告

此查询会替代以下各项的全部或部分：

- DAT/病毒特征码部署摘要
- DAT 引擎覆盖范围

ePO: 按最高层级组组织的系统的查询

使用此查询（采用其默认设置）可以查看按最高层级系统树组组织的托管系统的条形图。

查询结果

查询的结果会以条形图的形式显示，可用于深入查询组成每个条形的系统。

ePO: 标记为服务器的系统的查询

使用此查询（采取其默认设置）可以查看环境中按系统是否含有“服务器”标记来划分的系统的布尔饼图。

查询结果

查询的结果会以布尔饼图的形式显示，可用于深入查询组成每个扇区的系统。

ePO: 按产品当日的检测查询

使用此查询（采用其默认设置）可以查看最近 24 小时内按检测产品组织的检测的饼图。

查询结果

查询结果会以饼图的形式显示，可用于深入查询事件以及发生事件所针对系统的详细信息。

ePolicy Orchestrator 3.6 中的比较报告

此查询会替代以下各项的全部或部分：

- 最近 24 小时的感染数量

使用仪表板评估环境

使用仪表板可以持续监视您的环境。仪表板是监视器的集合。监视器可以是从图表的查询到小型 Web 应用程序（如 MyAvert Threat Service）等多种形式，并按照用户配置的时间间隔刷新。

用户只有具有相应的权限才能使用和创建仪表板。

是否首次设置仪表板？

首次设置仪表板时：

1 阅读本部分的概念主题，深入了解仪表板和仪表板监视器。

2 确定要使用的默认仪表板和默认监视器。

3 创建任何所需的仪表板及其监视器，并确保激活可从导航栏的选项卡使用的任何仪表板。

目录

仪表板及其工作方式

仪表板是用户选择和配置的监视器的集合，提供有关环境的当前数据。

将查询用作仪表板监视器

可以将任何基于图表的查询用作以用户配置的频率刷新的仪表板，因此，您可以在活动仪表板上使用最有用的查询。

默认仪表板监视器

此版本的 ePolicy Orchestrator 随附有几个默认监视器：

- MyAvert Threat Service — 可让您持续了解哪些 DAT 和引擎可用，防护哪些威胁以及当前主资料库中的最新版本。
- 快速系统搜索 — 基于文本的搜索字段，支持按系统名称、IP 地址、MAC 地址或用户名来搜索系统。
- McAfee 链接 — 指向 McAfee 站点的超链接，包括 ePolicy Orchestrator 支持、Avert Labs WebImmune 和 Avert Labs 威胁库。

设置仪表板访问权限和行为

使用这些任务可以确保用户对仪表板具有适当的访问权限，以及配置刷新仪表板的频率。

任务

- 将仪表板权限授予用户
- 配置仪表板的刷新频率

将仪表板权限授予用户

使用此任务可以将所需的仪表板权限授予用户。用户要访问或使用仪表板，必须具有适当的权限。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“配置”|“权限集”，然后单击“新建权限集”，或在“权限集”列表中选择权限集。
2 在“仪表板”旁，单击“编辑”。此时会出现“编辑权限集: 仪表板”页。
3 选择权限：
   - 无权限
   - 使用公共仪表板
   - 使用公共仪表板；创建并编辑个人仪表板
   - 编辑公共仪表板；创建并编辑个人仪表板；公开发布个人仪表板
4 单击“保存”。

配置仪表板的刷新频率

使用此任务可以配置刷新用户仪表板的频率（分钟）。每个用户帐户的刷新频率设置都各不相同。

设置刷新频率时，请考虑您预期随时登录的用户数量。每个用户登录并显示仪表板时，都会在刷新仪表板时对性能产生额外的影响。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“仪表板”，然后从“选项”下拉列表中选择“编辑仪表板首选项”。此时会出现“仪表板首选项”页。
2 在“仪表板页面刷新间隔”旁，输入两次刷新之间的分钟数。
3 单击“保存”。

使用仪表板

使用这些任务可以创建和管理仪表板。

任务

- 创建仪表板

创建仪表板

使用此任务可以创建仪表板。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“仪表板”，然后从“选项”下拉列表中选择“管理仪表板”。此时会出现“管理仪表板”页。

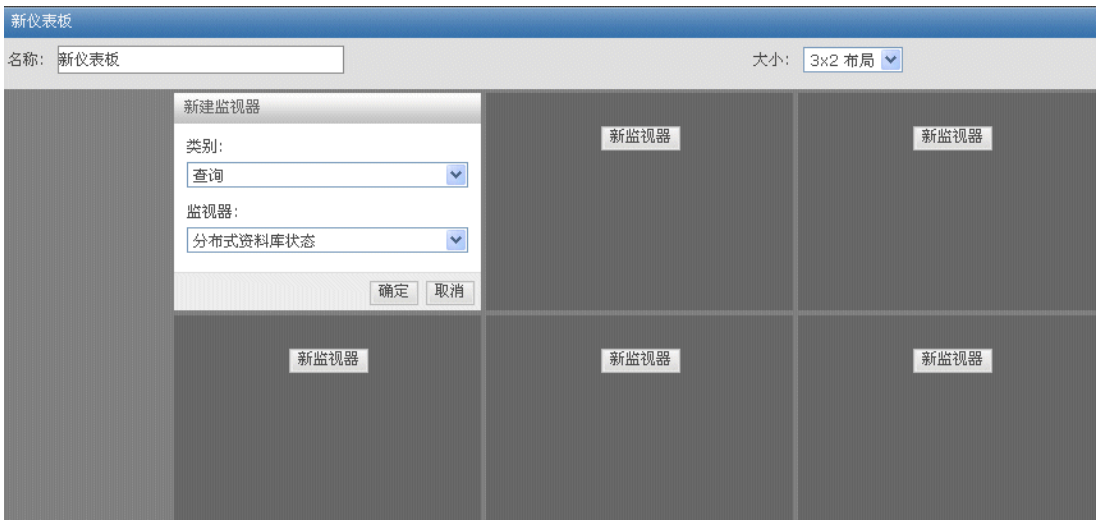

图 32：新建仪表板页

2 单击“新建仪表板”。

3 输入名称，然后选择仪表板的大小。

4 对于每个监视器，单击“新监视器”，然后选择要在仪表板中显示的监视器。

5 单击“保存”，然后选择是否激活此仪表板。活动仪表板随后会显示在“仪表板”的选项卡栏。

激活仪表板

使用此任务可以将某个仪表板作为活动集的一部分。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“仪表板”，单击“选项”，然后选择“管理仪表板”。此时会出现“管理仪表板”页。

2 从“仪表板”列表中选择仪表板，然后单击“激活”。

3 当出现提示时，单击“确定”。

4 单击“关闭”。

选定的仪表板会立即出现在选项卡栏上。

选择全部活动仪表板

使用此任务可以选择组成活动集的所有仪表板。活动仪表板可以从“仪表板”下的选项卡栏进行访问。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“仪表板”，然后从“选项”下拉列表中选择“选择活动仪表板”。

图 33：选择活动仪表板页

2 从“可用仪表板”列表中单击所需的仪表板。这些仪表板将会添加到内容窗格。

3 重复此操作，直到选择了所有需要的仪表板。

4 可以在选项卡栏上调整选定仪表板的顺序。

5 单击“确定”。

只要您转至产品的“仪表板”区域，选定的仪表板就显示在选项卡栏上。

公开仪表板

使用此任务可以公开专用仪表板。对公共仪表板有权限的任何用户都可以使用公共仪表板。

任务

要获得选项定义，请在显示选项的页面上单击“?”。

1 转至“仪表板”，然后从“选项”下拉列表中选择“管理仪表板”。

2 从“可用仪表板”列表中选择所需的仪表板，然后单击“公开”。

3 当出现提示时，单击“确定”。

仪表板会显示在“管理仪表板”页上的“公共仪表板”列表中。

附录：维护 ePolicy Orchestrator 数据库

无论您是将 MSDE 还是 SQL 数据库与 ePolicy Orchestrator 一同使用，都需要在一段时间后维护数据。这样才会确保获得最佳性能并保护其中的数据。

根据 ePolicy Orchestrator 的部署情况，计划每周花数小时进行定期的数据库备份和维护。本部分中的许多任务都应以每周或每日的频率定期执行。某些任务仅在特定的时间才需要执行，如出现问题时。

您可以组合使用多种工具来维护 ePolicy Orchestrator 数据库。根据您是将 Microsoft Data Engine (MSDE) 还是 SQL Server 数据库用作 ePolicy Orchestrator 数据库，所使用的工具集可能有所不同。请注意，您可以使用 Microsoft SQL Server Enterprise Manager 来维护 MSDE 数据库和 SQL Server 数据库。

目录

执行每日或每周数据库维护

若要防止数据库变得很大以及保持最佳性能，请定期维护数据库。如有可能，McAfee 建议每日执行维护，或至少每周执行一次维护。定期执行此维护可以减少数据库大小，从而提高数据库性能。

此任务根据您运行的是 MSDE 数据库还是 SQL 数据库而有所不同。

任务

执行 MSDE 数据库每周维护

使用 SQLMAINT.EXE 实用程序可以定期对 MSDE 数据库执行清理和维护。默认情况下，SQLMAINT.EXE 实用程序安装在服务器上的 MSDE 安装文件夹中。

请至少每周运行一次此实用程序。您可以使用 SQLMAINT.EXE 命令提示符实用程序执行例行的数据库维护活动。此程序可用于执行 DBCC 检查，以转储数据库及其事务日志，更新统计数据以及重建索引。

下面的过程很简单，并没有涉及使用 SQLMAINT 来维护 MSDE 数据库的方方面面，而只介绍每周对数据库所必须执行的工作。有关 SQLMAINT 的其他信息以及对数据库所执行工作，请参阅 Microsoft 网站。

任务

1 在命令提示符处输入以下命令（命令区分大小写）：

```
SQLMAINT -S <SERVER> -U <USER> -P <PASSWORD> -D <DATABASE> -RebldIdx 5 -RmUnusedSpace 50
 10 -UpdOptiStats 15
```

其中，<SERVER> 是服务器的名称，<USER> 和 <PASSWORD> 是用户帐户的用户名和密码，<DATABASE> 是数据库的名称。默认数据库名称为 EPO_<SERVER>，其中 <SERVER> 是 ePolicy Orchestrator 服务器的名称。

2 按 Enter 键。

定期维护 SQL Server 数据库

使用 SQL Enterprise Manager 可以定期维护 SQL 数据库。

以下任务并没有涉及在 SQL Enterprise Manager 中维护 SQL 数据库的方方面面。有关还可以执行哪些维护数据库的操作的详细信息，请参阅 SQL 文档。

备份事务日志与与简单还原不相容。如果您有多个具有不同还原模式的数据库，则可以分别为每个还原模式创建不同的数据库维护计划。通过这种方法，您可以包含一个步骤，只将事务日志备份到不使用简单还原模式的数据库上。

建议使用简单还原模式，因为该模式可以防止事务日志变得很大。执行简单还原时，如果检查点完成，则会从活动数据库中丢弃检查点之前的事务日志。检查点会在备份时自动产生。建议您制定一个数据库维护计划，执行 ePO 数据库备份以及“简单还原”。这样，在成功创建备份后，就会丢弃活动数据库中的部分事务日志，因为备份文件存而不再需要它。

将还原模式设为简单还原。这是对 SQL Server 设置所进行的一次性更改，而且非常重要。默认情况下，当通过简单还原模式安装 MSDE 数据库时，SQL Server 会通过其他还原模式安装，该模式不允许轻易清理事务日志。这可能会导致日志变得很大。

注意: 如果选择不使用简单还原，则需要定期备份事务日志。

有关将还原模式设置为简单还原的信息，请参阅 SQL 或 MSDE 文档。

定期备份 ePolicy Orchestrator 数据库

McAfee 建议定期备份 ePolicy Orchestrator 数据库来保护数据，并防止硬件和软件故障。您可能需要从某个备份还原，如同需要重新安装服务器一样。

备份频率取决于您愿意损失的数据量。数据库备份至少要每周进行一次，但如果您对部署进行了许多更改，则可能希望每天备份一次。您也可以在自动执行每夜作业时进行每日备份。另外，您可以将工作分散开，即每日进行增量备份，然后每周进行完全备份。请将备份副本保存到活动数据库所在服务器之外的服务器 -- 如果您的数据库服务器崩溃，也不想丢失备份的话。

备份过程会根据您所备份的是 SQL 数据库还是 MSDE 数据库而有所不同。若要备份 SQL Server 数据库，请参阅 SQL Server 文档。

任务

- 备份 SQL 数据库 -- 请参阅 SQL 文档
- 备份 MSDE 数据库

备份 SQL 数据库 -- 请参阅 SQL 文档

如果将 Microsoft SQL Server 或 SQL 2005 Express 用作数据库，请参阅 SQL Server 产品文档。

备份 MSDE 数据库

如果将 Microsoft Data Engine (MSDE) 用作 ePolicy Orchestrator 数据库，则可以使用数据库备份实用程序 (DBBAK.EXE) 备份和还原数据库服务器上的 ePolicy Orchestrator MSDE 数据库。

提示: 数据库备份实用程序会在服务器服务运行时工作。但是，McAfee 建议先停止服务器服务，然后再开始备份。

您可以利用此实用程序备份 MSDE 数据库，并将其还原到相同数据库服务器的相同路径。您无法使用该实用程序更改数据库的位置。

任务

1 停止“McAfee ePolicy Orchestrator 4.0 服务器”服务，并确保 SQL Server (MSSQLSERVER) 服务正在运行。有关说明，请参阅操作系统产品文档。

2 关闭 ePolicy Orchestrator。

3 启动数据库备份实用程序 (DBBAK.EXE)。默认位置为：

C:\PROGRAM FILES\MCAFEE\EPO

4 输入“数据库服务器名称”。

5 输入“数据库名称”。

6 选择“NT 身份验证”或“SQL 帐户”。

如果选择了“SQL 帐户”，请输入此数据库的“用户名”和“密码”。

7 输入“备份文件路径”。

8 单击“备份”。

9 备份过程完成后，单击“确定”。

10 启动“McAfee ePolicy Orchestrator 4.0 服务器”服务，并确保 MSSQLSERVER 服务正在运行。有关说明，请参阅操作系统产品文档。

更改 SQL Server 信息

使用此任务可以编辑 SQL Server 连接配置详细信息。在其他程序（如 SQL Server Enterprise Manager）中更改 SQL Server 身份验证模式后，使用此任务对更改 ePolicy Orchestrator 中的用户帐户信息很有用。如果需要使用特权 SQL 用户帐户来提高网络的安全性，则可以这样做。

您可以使用下列所指的页调整任何数据库配置文件信息，这些信息以前常通过 CFGNAIMS.EXE 文件进行调整。

关于此页的信息：

- 身份验证 — 如果数据库已启动，请使用常规 ePO 用户身份验证，且只有全局管理员可以访问。如果数据库关闭，则需要从运行服务器的系统进行连接。
- 必须重新启动 ePO 服务器才能使任何配置更改生效。

- 如果其他方法都不起作用，可以手动编辑配置文件 (${orion.server.home}/conf/orion/db.properties)，即输入纯文本密码，启动服务器，然后使用配置页来重新编辑数据库配置，以存储加密版的密码。

任务

1 在 ePolicy Orchestrator 中访问此 URL：

http://server/core/config

2 在“配置数据库设置”页中，向下滚动此页，然后根据需要更改凭据。

3 完成后，单击“确定”。

4 重新启动系统以应用更改。

还原 ePolicy Orchestrator 数据库

如果您一直按照 McAfee 的建议定期备份数据库，则还原数据库就非常简单。您并不需要经常还原，或根本不需要还原。除了软硬件故障外，如果要升级服务器或数据库服务器硬件，才需要从备份还原数据库。

还原过程会根据您所备份的是 SQL 数据库还是 MSDE 数据库而有所不同。若要还原 SQL Server 数据库，请参阅 SQL Server 文档。

任务

- 还原 SQL 数据库 -- 请参阅 SQL 文档
- 从备份还原 MSDE 数据库

还原 SQL 数据库 -- 请参阅 SQL 文档

如果将 Microsoft SQL Server 或 SQL 2005 Express 用作数据库，请参阅 SQL Server 产品文档。

从备份还原 MSDE 数据库

利用此实用程序，可以备份 MSDE 数据库并将其还原到相同数据库服务器的相同路径。您无法使用该实用程序更改数据库的位置。

任务

1 停止“McAfee ePolicy Orchestrator 4.0 Server”服务，并确保 SQL Server (MSSQLSERVER) 服务正在运行。有关说明，请参阅操作系统产品文档。

2 关闭所有 ePolicy Orchestrator 控制台和远程控制台。

3 启动数据库备份实用程序 (DBBAK.EXE)。默认位置为：

C:\PROGRAM FILES\MCAFEE\EPO

4 输入“数据库服务器名称”。

5 输入“数据库名称”。

6 选择“NT 身份验证”或“SQL 帐户”。

如果选择了“SQL 帐户”，请输入此数据库的“用户名”和“密码”。

7 输入“备份文件”路径。

8 单击“还原”。

9 当系统询问是否覆盖整个 ePolicy Orchestrator 数据库时，单击“是”。

10 还原过程完成后，单击“确定”。

11 启动“McAfee ePolicy Orchestrator 4.0 Server”服务，并确保 MSSQLSERVER 服务正在运行。有关说明，请参阅操作系统产品文档。

索引

字母

D

F

G

H

J

K

L

M

N

P

Q

S

T

W

X

Y

Z