System Center Monitoring Pack for Endpoint Protection，Linux 版本

Microsoft Corporation

发布时间： 10/26/2015

将关于本文档的反馈或建议发送至 mpgfeed@microsoft.com。请在反馈中加入管理包指南名称。

Operations Manager 团队鼓励您在 Management Pack Catalog (http://go.microsoft.com/fwlink/?LinkID=82105) 的管理包页面检查，提供关于监视包的反馈。

目录

SCEP 管理包指南

本管理包允许您在包含工作站和服务器的联网环境中，从中央位置的 System Center 2012 Operations Manager 管理 System Center Endpoint Protection (SCEP)。凭借 Operations Manager 任务管理系统，您可以管理远程计算机上的 SCEP，查看警报和运行状况，快速应对新问题和威胁。

System Center 2012 Operations Manager 本身不提供任何其他形式的恶意代码防护。System Center 2012 Operations Manager 依赖安装 Linux 操作系统的计算机上的 SCEP 解决方案。

本指南依据 4.5.10.1 版 SCEP 管理包编写。

指南历史记录

版本	发行日期	变更
4.5.9.1	05/16/2012	本指南的原始版本。
4.5.10.1	11/06/2012	支持新的 Linux 分发。 某些管理包工具的更贴切描述。

版本更改 4.5.10.1

版本 4.5.10.1 的 System Center Endpoint Protection 管理包包括以下更改：

- 支持新的 Linux 分发：
  - Red Hat Enterprise Linux Server 5
  - SUSE Linux Enterprise 10
  - CentOS 5，6
  - Debian Linux 5，6
  - Ubuntu Linux 10.04，12.04
  - Oracle Linux 5，6

  注意： 仅在使用 System Center 2012 Operations Manager Service Pack 1 及更高版本时支持这些新的分发。
- 为以下内容添加更贴切的描述：
  - 活跃恶意软件监视器
  - 活跃恶意软件（来自规则）警报

支持的配置

Operations Manager 2007 R2 支持的配置 (http://go.microsoft.com/fwlink/?LinkId=90676) 简要介绍支持的配置。

此管理包要求 System Center 2012 Operations Manager 2007 R2 或更高版本。下表详细介绍此管理包支持的操作系统：

操作系统名称	x86	x64
Red Hat Enterprise Linux Server 5，6	是	是
SUSE Linux Enterprise 10，11	是	是
CentOS 5，6	是	是
Debian Linux 5，6	是	是
Ubuntu Linux 10.04，12.04	是	是
Oracle Linux 5，6	是	是

必要条件

运行此管理包必须满足以下要求：

- System Center Operations Manager 2007 R2 累积更新 5 (http://support.microsoft.com/kb/2449679)

以下列出用于 SCEP 的管理包已经集成在 System Center 2012 Operations Manager 2007 R2 中，或可从在线目录下载。

.

ID	名称	版本
Microsoft.Linux.Library	Linux 操作系统库	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	实例组库	6.1.7221.0
Microsoft.SystemCenter.Library	系统中心核心库	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS-管理库	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	数据仓库库	6.1.7221.0
Microsoft.Unix.Library	Unix 核心库	6.1.7000.256
Microsoft.Unix.Service.Library	Unix 服务模板库	6.1.7221.0
Microsoft.Windows.Library	Windows 核心库	6.1.7221.0
System.Health.Library	运行状况库	6.1.7221.0
System.Library	系统库	6.1.7221.0

重要信息 使用 System Center 2012 Operations Manager 监视 Linux SCEP 产品必须先在配置文件 */etc/opt/microsoft/scep/scep.cfg* 中或通过 SCEP Web 界面启用才能正常工作。请确保上述配置文件中的 'scom_enabled' 参数设置为 *'scom_enabled = yes'*，或在 Web 界面的**配置** > **全局** > **后台程序选项** > **启用 SCOM** 下更改相应设置。

本管理包中的文件

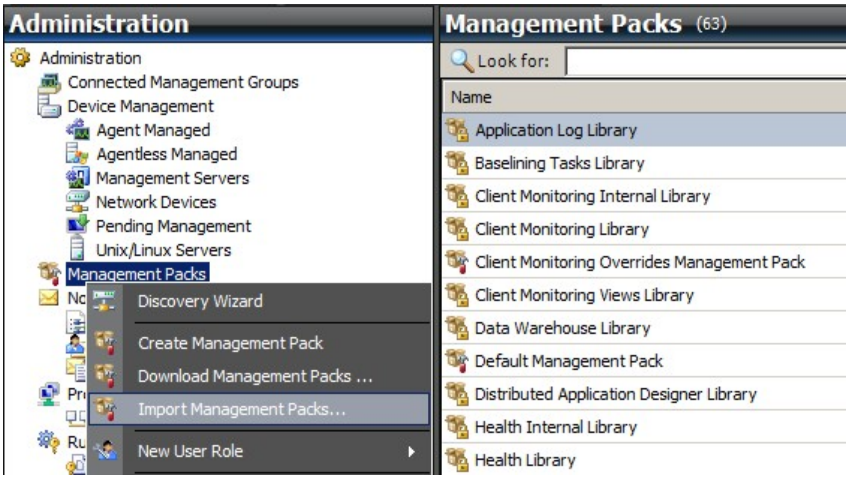
SCEP 管理包包括以下文件：

文件名	说明
Microsoft.SCEP.Linux.Library.mp	包含类定义及其相互关系，以及监视器类型和模块类型定义。
Microsoft.SCEP.Linux.Application.mp	实施监视和警报、任务和视图。

快速入门

开始监视 SCEP 的前提条件是将管理包导入 Operations Manager 并识别要监视的计算机（过程称为 "发现"）。

导入管理包

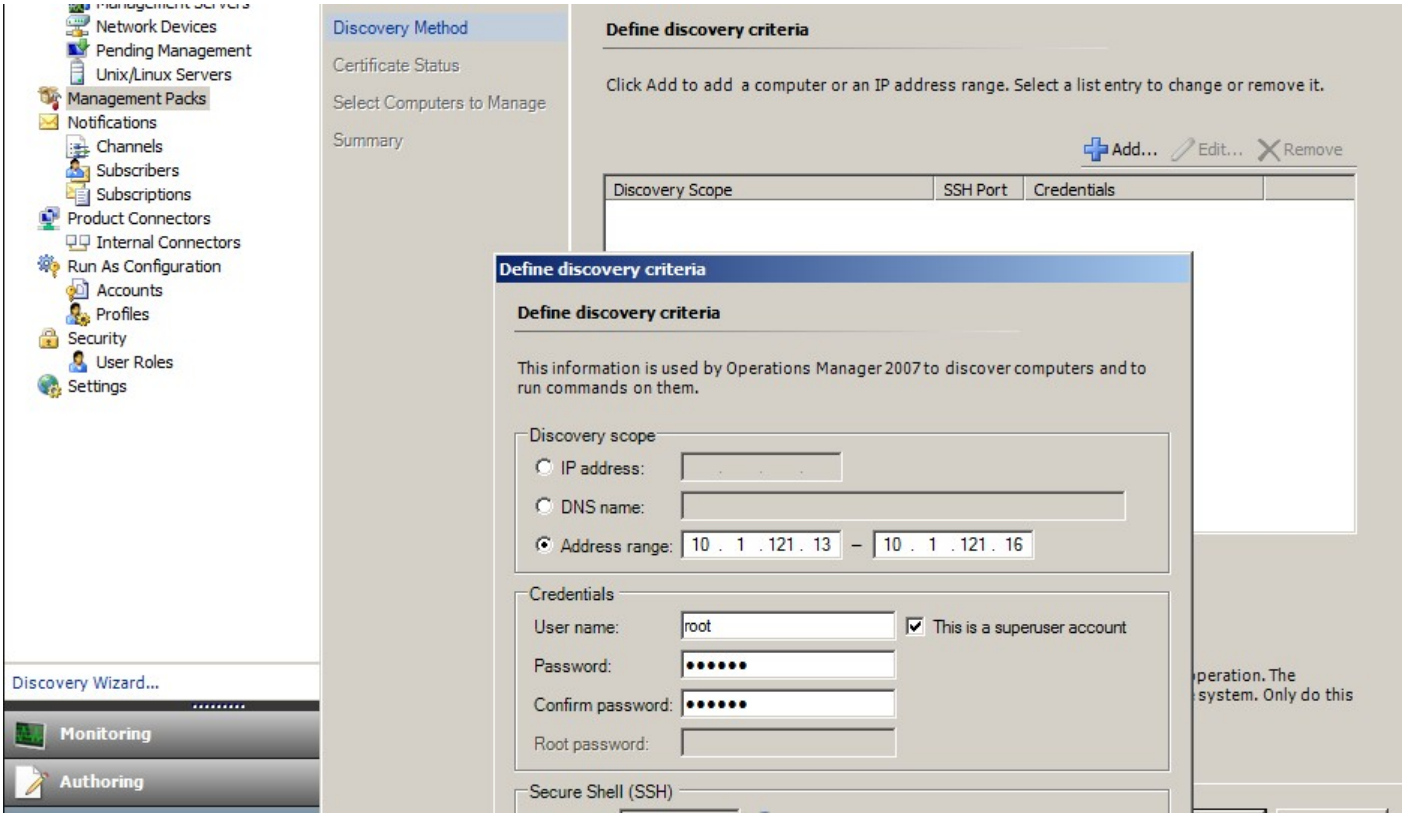


1. 单击操作控制台窗口左窗格的 **Administration** 工作区。
2. 右键单击 **Management Packs** 并选择右键菜单中的 **Import Management Packs...**。
3. 在管理包窗口中单击 **Add** 按钮，选择下拉菜单中的 **Add from disk...**。
4. 确认希望 Operations Manager 搜索并安装本地磁盘没有的依赖项，方法是单击 **Online Catalog Connection** 弹出窗口中的 **Yes**。
5. 确保选择两个列出的文件（Microsoft.SCEP.Linux.Application.mp 和 Microsoft.SCEP.Linux.Library.mp）并单击 **Install**。

注意： 有关导入管理包的更多说明，请参见如何在 Operations Manager 2007 中导入管理包 (http://go.microsoft.com/fwlink/?LinkId=142351)。

发现

成功导入 *mp 文件后，需要执行计算机发现。



1. 在 **Administration** 工作区中（操作控制台窗口的左窗格）单击 **Discovery wizard...** 链接（左窗格底部）。
2. 在计算机和设备管理向导中选择 **Unix/Linux computers** 选项，单击 **Next** 继续。
3. 在 '定义发现条件 '部分中单击 **Add** 按钮。
4. 设置要扫描的 IP **Address range**和适用于 System Center 2012 Operations Manager 将安装其代理的计算机的 SSH **Credentials**。
5. 单击 **OK** 确认作用域和凭据条件，单击 **Discover** 按钮开始发现过程。
6. 完成后，将一个显示列表，允许您选择监视 管理的系统。

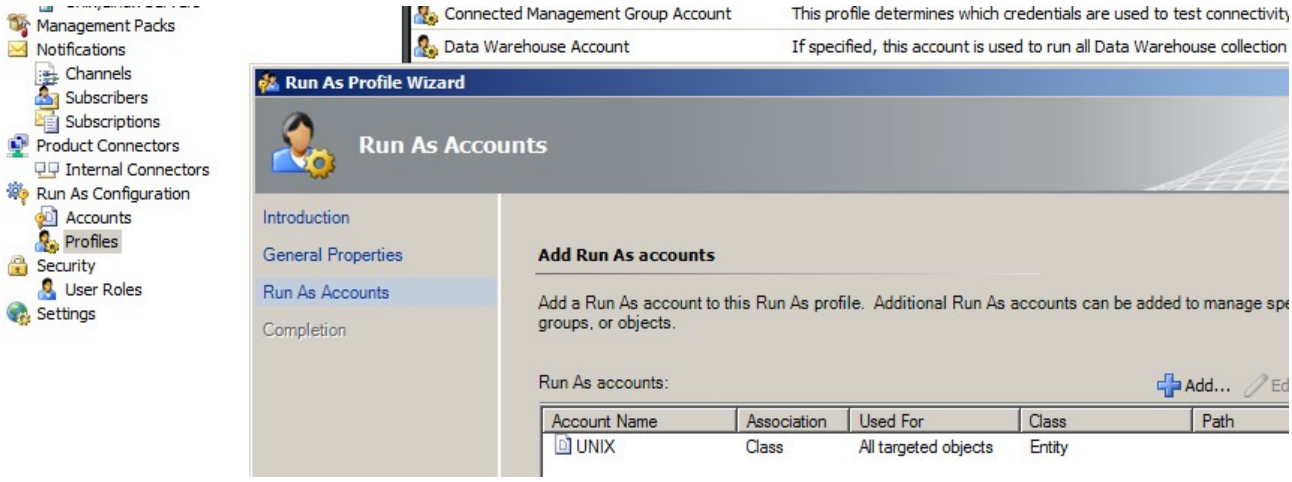
注意：以下 Linux 版本上支持安装 Linux 代理。如果无法使用发现安装 Linux 代理，请参见以下 Microsoft 文章手动安装跨平台代理 (http://technet.microsoft.com/en-us/library/dd789016.aspx) 中的手动安装说明。

注意： 发现具有 SCEP 安装的 Linux 服务器以 8 小时间隔在所有通过 Operations Manager 管理的 Linux 计算机上进行（即它们安装了适合系统版本的 Linux 管理包）。发现创建所有服务模块实体：受保护 Linux 服务器和嵌套实体或不受保护 Linux 服务器（可以在相应部分中找到）。当存在 'scep_daemon 服务（停止或运行）时，SCEP 可视为完全安装。因此安装管理包时发生第一次发现，而下一次在发现周期的 8 小时后实现。如果卸载 SCEP 产品包，则相应服务器将自动移至不受保护（无 SCEP 的服务器），反之亦然。

运行方式帐户配置

要创建 Unix 帐户，请使用以下说明：

1. 在 **Administration** 工作区中（左窗格）导航至 **Run As Configuration** > **Accounts**。
2. 要窗口新帐户，打开**操作** 窗格（右窗格）中的 **Actions** 部分，单击**创建运行方式帐户 ...**
3. 在 常规属性 窗口中，选择 **Run As Account type** 下拉菜单中的 **Basic Authentication**。
4. 创建帐户后，需要将新帐户添加到配置文件才能分发。为此，右键单击 **Run As Configuration** > **Profiles** 下的 **Unix Privileged Account** 配置文件，选择 **Properties** 并完成向导分配新创建的帐户。



注意： 有关创建运行方式帐户的更多信息，请参见 System Center 2012 Operations Manager 2007 R2 联机库中的[配置跨平台运行方式帐户](http://go.microsoft.com/fwlink/?LinkId=160348) (http://go.microsoft.com/fwlink/?LinkId=160348) 主题。

完成所有上述步骤后，新发现的 Linux 服务器将在 **Monitoring** > **System Center Endpoint Protection Linux** > **具有 SCEP 的服务器**下短时间可用（几分钟）。

安装 SCEP 语言包

语言包格式如下：
Microsoft.SCEP.Linux.Application.LNG.mp 和 Microsoft.SCEP.Linux.Library.LNG.mp

使用上面**导入管理包**部分中介绍的相同步骤安装语言包。要显示 System Center 2012 Operations Manager 中安装的语言，请使用以下说明：

1. 单击 Windows **开始** 图标，导航至**控制面板**。
2. 在 控制面板 中单击**地区和语言选项**。
3. 在**管理**选项卡中更改非 Unicode 程序的系统区域设置。在**位置**选项卡中，根据安装的语言包更改当前位置。

管理包的目的

SCEP 管理包具有以下功能：

- 实时监视和警报安全事件及安全运行状况状态。
- 允许服务器管理员在服务器上远程执行安全相关任务。这些任务的主要目标是修复与安全有关的可用性问题。

视图

服务器管理员可以使用 Operations Manager 控制台监视所有安装了 SCEP 的计算机。 System Center Endpoint Protection Linux 可使用以下视图：

- **活动警报** - 所有严重级别的所有 SCEP 活动警报。不包括关闭的警报。
- **仪表板** - 显示具有 SCEP 和活跃警报工作区的服务器。
- **具有 SCEP 的服务器** - 显示所有受保护的 Linux 服务器。
- **没有 SCEP 的服务器** - 显示所有不受保护的 Linux 服务器。
- **任务状态** - 列出所有执行的任务。

使用 System Center 2012 Operations Manager 管理包监视 SCEP 状态时，可以即时了解 SCEP 健康状况。

您无需等待发出警报，可以随时单击 Operations Manager 监视控制台的 **Monitoring** > **System Center Endpoint Protection Linux** > **具有 SCEP 的服务器**窗口，查看 SCEP 组件的摘要状态。组件状态在 状态 字段中以彩色图标指示：

图标	状态	说明
	Healthy	绿色图标表示成功，或者存在无需操作的信息。
	Warning	黄色图标表示错误或警告。
	Critical	红色图标可以表示严重错误或严重性问题或服务不可用。
	Not monitored	没有图标说明没有收集到影响状态的数据。

视图可以获得非常长的对象列表。要查找特定对象或对象组，可以使用 Operations Manager 工具栏上的作用域、搜索和查找按钮。有关更多信息，请参见[如何使用作用域、搜索和查找管理监视数据](http://go.microsoft.com/fwlink/?LinkId=91983) (http://go.microsoft.com/fwlink/?LinkId=91983) 主题。

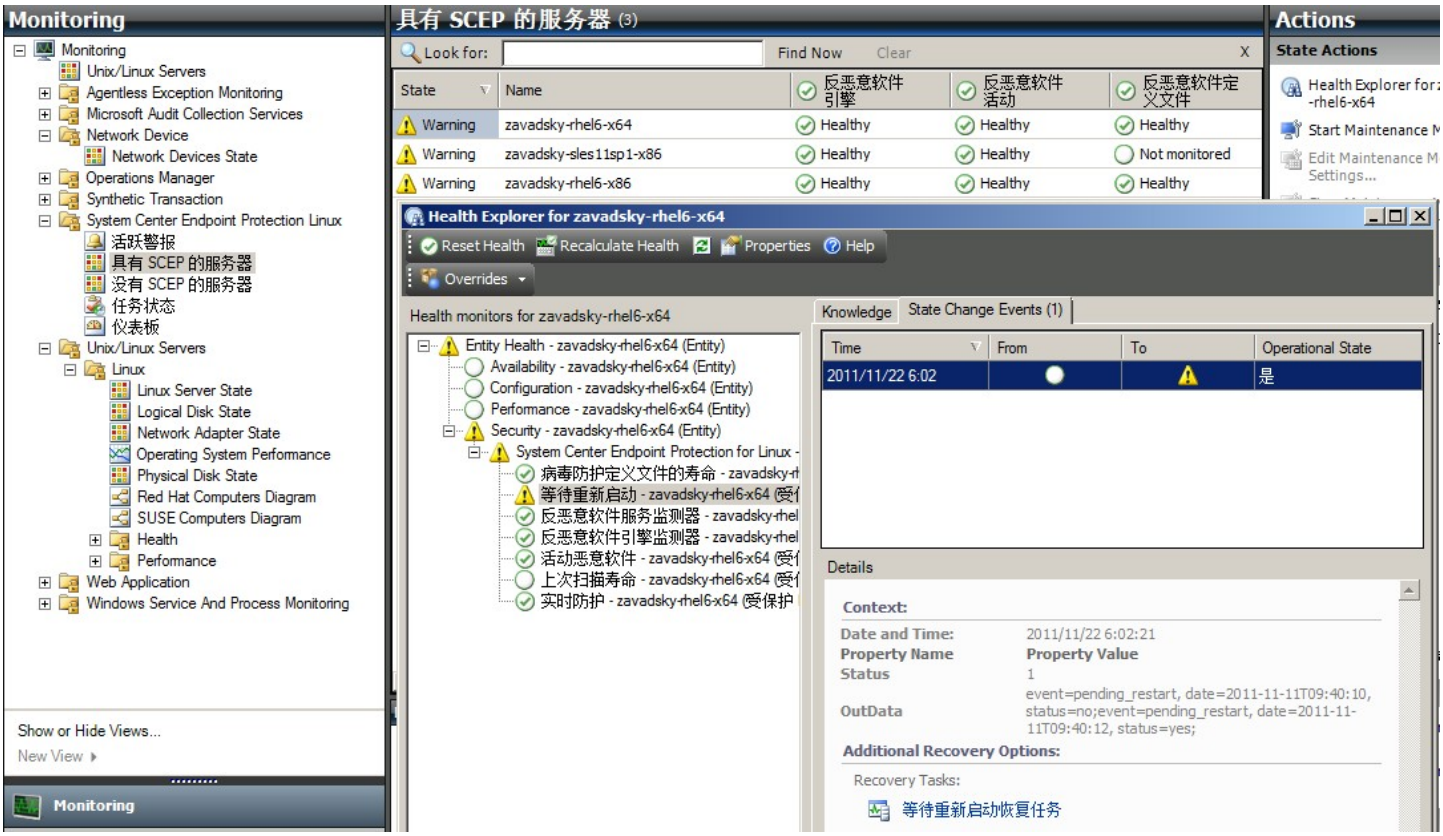
监视器

在 Operations Manager 2007 中，监视器可以用于评估所监视对象中发生的各种情况。

SCEP 共有 17 个可用监视器：

- 9 个单元监视器 -基础监视组件，用于监视特定计数器、事件、脚本和服务。
- 2 个聚合监视器 -用于将多个监视器组合到一个监视器的聚合汇总，然后使用该监视器设置运行状况和生成警报。
- 6 个依赖项监视器 - 包含现有监视器状态数据的参考。

注意： 有关监视器的更多信息，请参考 Operations Manager 2007 R2 帮助（在 System Center 2012 Operations Manager 中按 F1 键）。



SCEP 运行状况监视器具有以下结构和属性。

活动恶意软件

监视器类型	单元监视器
目标	受保护 Linux 服务器
数据源	监视文本日志文件：/var/log/scep/eventlog_scom.dat
间隔	事件驱动

监视器类型	单元监视器
警报	是。不自动解决
重置行为	8 小时后自动恢复健康状况。警报保持活动状态以保留关于未处理的恶意软件的信息。
注释	如果找到恶意软件且未得到清理，此监视器会将状态更改为 严重 ”。8 小时后，状态会自动恢复为 正常 ”（这是因为，系统无法准确判断恶意软件是否已经得到清理 删除）。要求管理员介入以考虑所处的场景并手动关闭标签。
状态	健康 -无恶意软件 严重 -活动恶意软件
已启用	True
恢复任务	否

此监视器跟踪失败的恶意软件清理操作。如果客户端报告未能清理恶意软件，此监视器将报告严重状态。

病毒防护定义文件的寿命

监视器类型	单元监视器
目标	受保护 Linux 服务器
数据源	用于获得监视数据的命令： /opt/microsoft/scep/sbin/scep_daemon --status
间隔	每 8 小时
警报	是。自动解决
状态	健康 -寿命 <= 3 天 警告 -寿命 > 3 天且寿命 <= 5 天 严重 -寿命 > 5 天
已启用	True
恢复任务	是，手动（不自动恢复）

最新定义文件有助于确保计算机防范最新恶意软件威胁。

反恶意软件引擎

监视器类型	单元监视器
目标	受保护 Linux 服务器
数据源	监视文本日志文件： /var/log/scep/eventlog_scom.dat
间隔	事件驱动
警报	是。自动解决
状态	健康 -已启用 已禁用 -警告
已启用	True
恢复任务	是，手动（不自动恢复）

建议始终启用反恶意软件防护。
注意： 此监视器跟踪病毒防护的状态，与实时防护不同。禁用反恶意软件引擎后，无法启动手动扫描。

反恶意软件服务

监视器类型	单元监视器
目标	受保护 Linux 服务器
数据源	监视过程状态：scep_daemon
间隔	每 10 分钟
警报	是。自动解决
状态	健康 -运行 严重 -不运行
已启用	True
恢复任务	是，手动（不自动恢复）

当客户端计算机上的反恶意软件服务 (scep_daemon) 未运行或没有响应，或者反恶意软件引擎未正常工作时，监视器报告严重状态。

上次扫描寿命

监视器类型	单元监视器
目标	受保护 Linux 服务器
数据源	用于获得监视数据的命令： /opt/microsoft/scep/sbin/scep_daemon --status
间隔	每 8 小时
警报	否
状态	健康 -寿命 <= 7 警告 -寿命 > 7
已启用	True
恢复任务	是，手动（不自动恢复）

此监视器跟踪自上次计算机扫描后经过的时间（与扫描类型无关）。我们建议计划每周运行一次扫描。

等待重新启动

监视器类型	单元监视器
目标	受保护 Linux 服务器
数据源	监视文本日志文件： /var/log/scep/eventlog_scom.dat
间隔	事件驱动
警报	是。自动解决
状态	无 -健康 是 -警告
已启用	True
恢复任务	是，手动（不自动恢复）

此监视器跟踪是否需要重新启动系统使配置更改生效（尤其是启用 禁用实时防护的情况下）。监视器对此状态的手动更新运行以下调用： /opt/microsoft/scep/sbin/scep_daemon --status。

实时防护

监视器类型	单元监视器
目标	受保护 Linux 服务器
数据源	监视文本日志文件： /var/log/scep/eventlog_scom.dat 监视器还可以对手动状态更新使用以下调用： /opt/microsoft/scep/sbin/scep_daemon --status。
间隔	事件驱动
警报	是。自动解决
状态	已启用 -健康 已禁用 -警告
已启用	True
恢复任务	是，手动（不自动恢复）

监视实时防护的状态。当病毒、间谍软件或其他潜在有害软件尝试在您的计算机上自我安装时，实时防护提醒您。

System Center Endpoint Protection for Linux

监视器类型	聚合监视器
目标	受保护 Linux 服务器
状况	最坏
警报	否
已启用	True
恢复任务	否

此监视器是所有 SCEP 7 个 Protected Linux 服务器安全单元监视器的运行状况汇总（最坏情况）。如果状态未初始化，则说明尚未开始监视此对象，或没有为此对象定义安全监视器。

反恶意软件引擎

监视器类型	依赖项监视器
目标	反恶意软件引擎
警报	否
已启用	True
恢复任务	否

在所监视计算机的列表中显示受保护 Linux 服务器 反恶意软件引擎单元监视器的状态。

反恶意软件服务

监视器类型	依赖项监视器
目标	反恶意软件引擎
警报	否
已启用	True
恢复任务	否

在所监视计算机的列表中显示受保护 Linux 服务器 反恶意软件服务单元监视器的状态。

反恶意软件定义文件

监视器类型	依赖项监视器
目标	反恶意软件定义文件
警报	否
已启用	True
恢复任务	否

在所监视计算机的列表中显示受保护 Linux 服务器 反恶意软件定义文件寿命监视器的状态。

活动恶意软件

监视器类型	依赖项监视器
目标	反恶意软件活动
警报	否
已启用	True
恢复任务	否

在反恶意软件活动运行状况资源管理器中显示受保护 Linux 服务器 活动恶意软件监视器的状态。

计算机 Ping

监视器类型	单元监视器
目标	反恶意软件活动
间隔	每 60 分钟
警报	否
状态	可以连接 -健康 无法连接 -严重
已启用	False
恢复任务	否

当服务器没有应答时，将状态更改为严重。

恶意软件活动

监视器类型	单元监视器
目标	反恶意软件活动
数据源	监视文本日志文件： /var/log/scep/eventlog_scom.dat
间隔	事件驱动
警报	否
状态	无恶意软件 -健康 检测到恶意软件活动 -严重
已启用	True
恢复任务	否

此监视器在检测到恶意软件后（已清理或未处理）5 分钟内切换为严重状态，接下来 60 分钟保持严重状态。在警报期内每次新的肯定检测后严重状态更新。即，如果 60 分钟内没有在系统上检测到恶意软件，监视器将恢复健康状态。

服务器恶意软件爆发

监视器类型	聚合监视器
目标	反恶意软件活动
状况	最好
警报	否
已启用	True
恢复任务	否

聚合监视器：恶意软件活动，计算机 Ping。
如果肯定恶意软件检测后（已清理或未处理）60 分钟内服务器没有反应，则将状态更改为严重。如果在一段未收到服务器应答的时间后，连接恢复后很快检测到恶意软件，也可以触发状态更改为严重。

恶意软件爆发

监视器类型	依赖项监视器
目标	受保护服务器监视器
状况	最坏的 95%
警报	否
已启用	True
恢复任务	否

显示反恶意软件活动 服务器恶意软件爆发监视器的状态。
如果过去 60 分钟内超过 5% 的 Linux 计算机（受保护和不受保护）登记恶意软件检测，则此监视器更改为严重状态。

SCEP Linux 计算机角色运行状况汇总

监视器类型	依赖项监视器
目标	Linux 计算机
警报	否
已启用	True
恢复任务	否

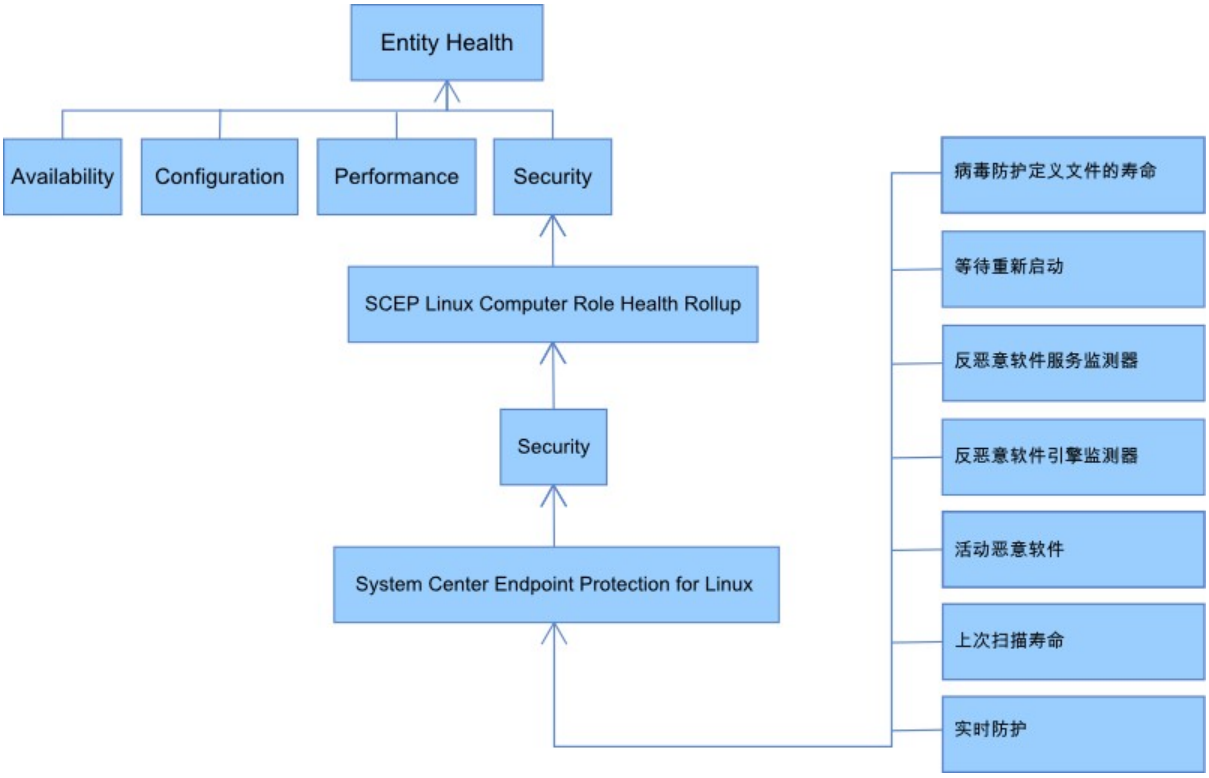
将受保护的 Linux 计算机实体状态传递给 Linux 计算机 安全父监视器。

运行状况汇总

本管理包将 Linux 操作系统监视拓展为分层结构，每一层依赖下一层来健康运行。该结构的顶层是整个 Entity Health 环境，安全环境的最低层是所有监视器。当某一层改变状况时，其上一层随之更改状况以匹配。这种行为称为 “汇总运行状况”。

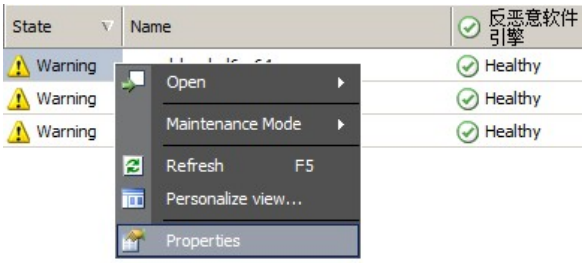
例如，如果实时防护恢复警告状态，而所有其他组件健康运行，则警告状态将通过树结构传输到根 (Entity Health)，后者也将获得警告状态。

下图显示管理包中如何汇总对象的的运行状况。



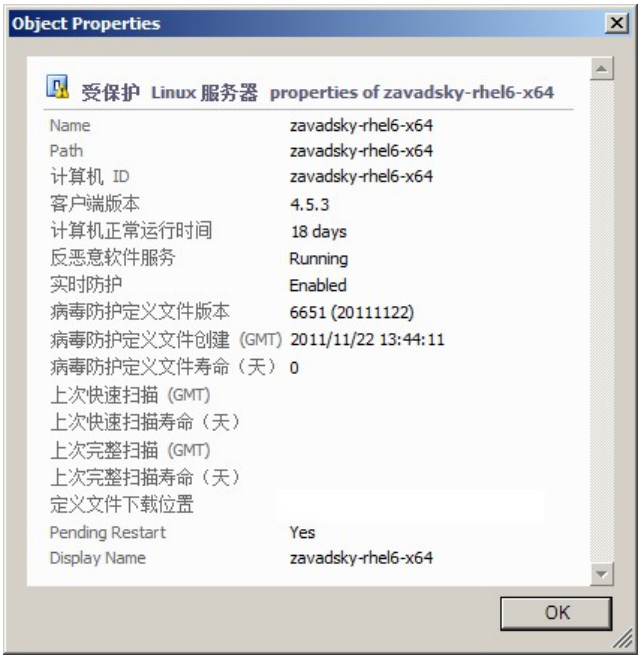
对象属性

要查看对象属性，右键单击对象然后选择 **Properties**。



受保护 Linux 服务器对象具有以下属性：

- **计算机标识符** - 服务器标识符，域名。
- **显示名称** - 服务器名称，域名。
- **客户端版本** - 已安装的 SCEP 产品的版本。
- **计算机正常运行时间** - 服务器正常运行时间（计算机正常工作而不停机的时间度量）对管理包正常工作来说不是关键数据，因此缺少它可能意味着管理包错误。
- **反恶意软件防护服务** - 反恶意软件防护状态（运行 *未*运行）。
- **实时防护** - 实时防护状态，缺少意味着 SCEP 问题。
- **病毒防护定义文件 ...**- 病毒库状态数据（版本、创建日期、寿命），缺少数据说明 SCEP 存在问题。
- **上次快速 *完*整扫描 ...**- 关于上次计算机扫描的数据。如果尚未执行扫描（快速扫描 *完*整扫描），则不显示数据。
- **定义下载位置** - 更新服务器地址 *名*称。首次成功更新后显示信息。
- **等待重新启动** - 关于因新安装或更改 SCEP 配置而需要重新启动以应用更改的信息。



警报

警报指示监视对象上发生特定严重级别（严重程度）的预定义状况。警报由规则定义。**Monitoring** > **System Center Endpoint Protection Linux** > **活跃警报**中可访问 Operations Manager 控制台中的视图，该视图显示控制台用户具有特定对象查看权限的警报。

注意： 如果同一服务器重复产生相同类型的更多警报（例如活动恶意软件），则仅显示第一个（忽略多余警报）。

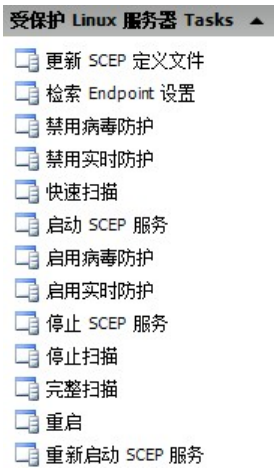
警报	间隔	优先级	严重级别	说明
重复恶意软件感染	事件驱动	高	严重	给定时间间隔（30 分钟）内重复检测到恶意软件时（3 次），产生警报。警报包含服务器数据和恶意软件的基础信息。
已清除恶意软件	事件驱动	低 中等	信息 -已清除恶意软件 警告 -需要用户交互，例如重新启动服务器	关于成功清除的恶意软件的警报。包含特定恶意软件的所有可用数据。每个检测的恶意软件生成一个独立事件。SCEP Linux 根据清除过程的消息分配优先级和严重级别，其中： 已清除 = 低 +信息 已清除但需要操作（例如重新启动）= 中等 +警告。
活动恶意软件（来自监视器）	事件驱动	高	严重	关于未清除恶意软件的警报。包含特定恶意软件的所有可用数据。
活动恶意软件（来自规则）	事件驱动	高 中 低	严重 中等 低 -根据恶意软件类型	和上面相同。用于其他监视 标签系统的连接器。 **注意：** 此规则（警报）默认禁用。
System Center Endpoint Protection 反恶意软件服务关闭	300 秒	中等	严重	关于反恶意软件服务 SCEP (scep_daemon) 不可用的警报。包括相应服务器名称和 SCEP 版本。
已禁用反恶意软件防护	事件驱动	中等	警告	关于已禁用的反恶意软件防护的警报。包括相应服务器名称。
已禁用实时防护	事件驱动	中等	警告	关于已禁用的实时防护的警报。包括相应服务器名称。
定义文件过期	每 8 小时	中等	警告（寿命 <= 5 天且寿命 > 3 天） 严重（寿命 > 5 天）	关于 3 天以上未更新病毒库的警报。包括相应服务器名称和病毒库寿命。

恶意软件爆发	事件驱动	高	严重	Forefront Endpoint Protection 在计算机上检测到超过 5% 的活动恶意软件。可能恶意软件正在您的计算机上传播。建议确保所有服务器使用最新定义文件。如果您需要更改触发此警报的活跃威胁数量，请改写恶意软件爆发监视器的相关参数（参见替代一章）。

任务

SCEP 管理包执行 13 个任务。这些任务都是立即执行的。任务执行后立刻显示输出，或者可以以后在任务状态窗口中查看。任务执行要求的最大时间为 180 秒。替代不可用，所有任务都是通过 SSH 执行的 BASH 命令。

可以在 操作控制台 窗口右窗格的 **Monitoring** > **System Center Endpoint Protection Linux** > **具有 SCEP 的服务器** 下调用任务。



- **禁用病毒防护** - 禁用病毒防护的所有组件，禁用手动扫描。
- **启用病毒防护** - 启用病毒防护的所有组件。
- **禁用实时防护** - 禁用实时防护。
- **启用实时防护** - 启用实时防护。
- **完整扫描** - 更新病毒库并运行完整计算机扫描。
- **快速扫描** - 更新病毒库并运行快速计算机扫描。
- **停止扫描** - 停止所有运行的计算机扫描。
- **检索服务器设置** - 显示当前 SCEP 产品状态，显示的参数列表与受保护 Linux 服务器实体的属性相同。显示的数据不传输到受保护 Linux 服务器。
- **重新启动反恶意软件服务** - 重新启动 SCEP 反恶意软件服务 (scep_daemon)。
- **停止反恶意软件服务** - 停止 SCEP 反恶意软件服务 (scep_daemon)。
- **启动反恶意软件服务** - 启动 SCEP 反恶意软件服务 (scep_daemon)。
- **更新反恶意软件定义文件** - 启动病毒库更新。
- **重新启动** - 重新启动 Linux 计算机。

配置 SCEP 管理包

最佳做法：创建管理包用于自定义

Operations Manager 默认将所有自定义（如改写）保存到默认管理包。作为最佳做法，您应为要自定义的每个密封管理包创建单独的管理包。

创建管理包用于存储密封管理包的自定义设置时，新管理包的名称可以以自定义的管理包名称为基础，例如 "SCEP 2012 Customizations"。

创建新管理包用于存储每个密封管理包的自定义，可便于将自定义从测试环境导出到生产环境。还便于删除管理包，因为您必须先删除任何依赖项然后才能删除管理包。如果所有管理包的自定义保存在默认管理包中，而您需要删除单个管理包，则必须先删除默认管理包，这样会同时删除其他管理包的自定义。

安全配置

计算机必须运行 SSHD 服务，SSH 端口（默认值 22）必须打开。System Center 2012 Operations Manager 使用合适的 Run As Account（位于 Operations Manager 监视控制台的 **Administration** > **Run As Configuration** 窗格）和 **Basic Authentication** 类型通过端口连接到远程 Linux 计算机。

运行方式配置文件名称	注释
Unix Privileged Account	用于远程监视 Unix 服务器，以及在需要权限时重新启动进程。

此管理包不使用 Unix Action Account。

警告　使用根帐户监视计算机在密码破坏时存在潜在安全风险。

如果不希望使用根帐户进行监视和管理，可以使用标准用户帐户，但此帐户需要具有执行 *sudo* 命令的权限。因此每个被监视的 Linux SCEP 工作站的 /etc/sudoers 文件中必须存在以下配置才能为所选用户帐户授权 sudo 提升。以下是用户名 user1 的配置示例：

```
#--------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)    NOPASSWD:     /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /sbin/reboot
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c pkill scep_sci
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#--------------------------------------------------------------------------
```

调节性能阈值规则

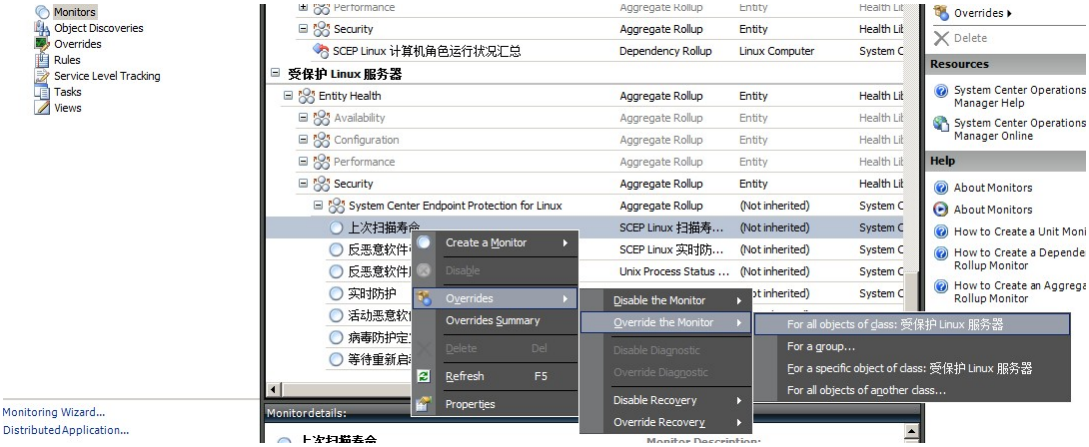
下表列出默认阈值可能需要额外调节以适合环境的性能阈值规则。评估这些规则以确定默认阈值是否适合您的环境。如果默认阈值不适合您的环境，可能需要通过应用替代来调整阈值。

规则名称	替代参数	默认阈值	调节限制
重复恶意软件感染规则	重复感染计数阈值	3 次	设置小于 2 的值会使规则无效。
重复恶意软件感染规则	重复感染时间窗口	30 分钟	我们不建议设置该值低于手动扫描的持续时间，因为两者重叠可能阻碍产生警报。
活动恶意软件警报规则	已启用	False	如果使用其他监视 标签系统的连接器，可以启用此警报。

替代

替代可以用于优化 System Center 2012 Operations Manager 中监视对象的设置。这包括来自导入的管理包的监视器、规则、对象发现和属性。

要替代监视器，在操作控制台中单击 **Authoring** 按钮并展开 **Management Pack Objects** > **Monitors**。在 监视器 窗格中找到并完全展开对象类型，单击监视器，然后单击 **Overrides**。



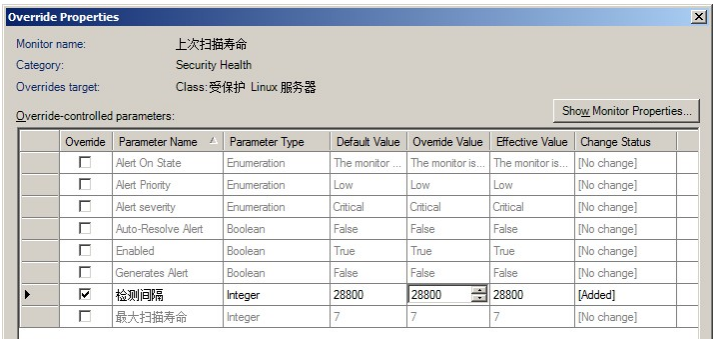
使用 替代 窗口创建或修改以下任意参数的替代：

- **活跃恶意软件监视器退却时间**（仅与活跃恶意软件监视器有关）
- **反恶意软件定义文件寿命**（仅与反恶意软件定义文件寿命监视器有关）
- **检测间隔**（仅与上次扫描寿命监视器有关）
- **警报状态**
- **警报优先级**
- **警报严重性**
- **自动解决警报**
- **已启用** - 确定启用或禁用所选监视器。
- **生成警报**
- **SCEP 日志文件路径**

如果默认替代不适合您的环境，可能需要通过应用替代来调整阈值：

替代参数	监视器名称	默认值	调节注释
Ping 间隔	计算机 Ping	3600 秒	用于检查受保护 Linux 服务器可用性的间隔。更短持续时间会在计算机因攻击停止响应时，更快触发服务器恶意软件爆发监视器上的错误状态。因此对网络、受监视计算机和 System Center 2012 Operations Manager 服务器的负载也增加。
恶意软件爆发时间窗口	恶意软件活动	3600 秒	监视器在恶意软件活动后恢复健康状态所需的间隔。时间窗口监视器值应高于计算机 Ping/Ping 间隔，才能使该组合正常工作。 如果在恶意软件爆发时间窗口间隔期间，超过设定的恶意软件爆发百分比值（参见恶意软件爆发）数量的计算机登记恶意软件活动，则生成恶意软件爆发警报。 注意：这与服务器恶意软件爆发不同，后者不生成警报。
活跃恶意软件监视器退却时间	活动恶意软件	28800 秒	从检测到恶意软件到将恶意软件视为已清理的时间间隔。
SCEP 日志文件路径	活动恶意软件	/var/log/scep/eventlog_scom.log	记录 System Center 2012 Operations Manager 事件的文件路径。除非发生问题，否则不要更改此参数。
严重状态的反恶意软件定义文件的寿命	反恶意软件定义文件寿命	5 天	此间隔后，生成错误警报通知过期 SCEP 产品。
健康状态的反恶意软件定义文件的寿命	反恶意软件定义文件寿命	3 天	反恶意软件定义文件的最大允许寿命，期间定义文件可视为最新。该值应始终小于严重状态的反恶意软件定义文件的寿命值。
间隔	反恶意软件定义文件寿命	28800 秒	用于检查反恶意软件定义文件寿命的间隔。
间隔	反恶意软件服务	300 秒	用于检查反恶意软件服务可用性的间隔。

进程名称	反恶意软件服务	scep_daemon	反恶意软件服务的名称。如果监视器可以工作，请勿更改该值。
检测间隔	上次扫描寿命	28800 秒	用于检查上次扫描执行的间隔。
最大扫描寿命	上次扫描寿命	7 天	按照 SCEP 产品设置，进行设置。如果计划每 7 天扫描一次，请将该值设置为 7 天。
日志文件路径	等待重新启动	/var/log/scep/eventlog_scom.log	记录 System Center 2012 Operations Manager 事件的文件路径。除非发生问题，否则不要更改此参数。
SCEP 日志文件路径	实时防护	/var/log/scep/eventlog_scom.log	记录 System Center 2012 Operations Manager 事件的文件路径。除非发生问题，否则不要更改此参数。
百分比	恶意软件爆发	95%	要使整个被监视组视为健康，Linux 服务器（受保护 +未保护）中需要恢复健康状态的服务器百分比。如果在总数的 5% 或更多服务器上检测到恶意软件，则生成恶意软件爆发。



注意： 有关替代的更多信息，请参见[如何使用替代监视](http://go.microsoft.com/fwlink/?LinkID=117777) (http://go.microsoft.com/fwlink/?LinkID=117777)。

链接

以下链接提供本管理包关联的常用任务的相关信息：

- [管理管理包的生命周期](http://go.microsoft.com/fwlink/?LinkId=211463)
  (http://go.microsoft.com/fwlink/?LinkId=211463)
- [如何在 Operations Manager 2007 中导入管理包](http://go.microsoft.com/fwlink/?LinkID=142351)
  (http://go.microsoft.com/fwlink/?LinkID=142351)
- [如何使用替代监视](http://go.microsoft.com/fwlink/?LinkID=117777)
  (http://go.microsoft.com/fwlink/?LinkID=117777)
- [如何在 Operations Manager 2007 中创建运行方式帐户](http://go.microsoft.com/fwlink/?LinkID=165410)
  (http://go.microsoft.com/fwlink/?LinkID=165410)
- [配置跨平台运行方式帐户](http://go.microsoft.com/fwlink/?LinkId=160348)
  (http://go.microsoft.com/fwlink/?LinkId=160348)
- [如何修改现有运行方式配置文件](http://go.microsoft.com/fwlink/?LinkID=165412)
  (http://go.microsoft.com/fwlink/?LinkID=165412)
- [如何导出管理包自定义](http://go.microsoft.com/fwlink/?LinkId=209940)
  (http://go.microsoft.com/fwlink/?LinkId=209940)
- [如何删除管理包](http://go.microsoft.com/fwlink/?LinkId=209941)
  (http://go.microsoft.com/fwlink/?LinkId=209941)
- [如何使用作用域、搜索和查找管理监视数据](http://go.microsoft.com/fwlink/?LinkId=91983)
  (http://go.microsoft.com/fwlink/?LinkId=91983)
- [使用 SCOM 2007 R2 监视 Linux](http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
  (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- [手动安装跨平台代理](http://technet.microsoft.com/en-us/library/dd789016.aspx)
  (http://technet.microsoft.com/en-us/library/dd789016.aspx)
- [使用 System Center 2012 - Operations Manager 配置 sudo 提升用于 UNIX 和 Linux 监视](http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)
  (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

有关 Operations Manager 和监视包的问题，请参见 System Center Operations Manager 社区论坛 (http://go.microsoft.com/fwlink/?LinkID=179635)。
System Center Operations Manager Unleashed blog (http://opsmgrunleashed.wordpress.com/) 是一个有用资源，包含特定监视包的 ‮按示例 ‬帖子。

有关 Operations Manager 的更多信息，请参见以下博客：

- Operations Manager Team Blog (http://blogs.technet.com/momteam/default.aspx)
- Kevin Holman's OpsMgr Blog (http://blogs.technet.com/kevinholman/default.aspx)
- Thoughts on OpsMgr (http://thoughtsonopsmgr.blogspot.com/)
- Raphael Burri's blog (http://rburri.wordpress.com/)
- BWren's Management Space (http://blogs.technet.com/brianwren/default.aspx)
- The System Center Operations Manager Support Team Blog (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++ (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Notes on System Center Operations Manager (http://blogs.msdn.com/mariussutara/default.aspx)

有关故障排除，请访问以下论坛线索：

- Microsoft.Unix.Library 丢失 (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)