CA Spectrum®

主机系统资源管理用户指南

版本 9.3

CA Technologies 产品引用

本指南涉及以下产品：

- CA Spectrum®
- CA Spectrum® Report Manager (Report Manager)
- CA SystemEDGE (SystemEDGE)

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 简介

关于主机系统资源管理器

*主机资源监控*是一种 CA Spectrum 机制，用于定义主机资源的各种状况和阈值，以便在满足或违反它们时生成事件和警报。资源监控的目的是，提醒网络管理员注意可能影响主机性能和服务水平协议的重大资源事件。

为了帮助您监控资源，CA Spectrum 提供了对以下资源监控代理的管理支持：

- CA SystemEDGE 代理
- CA Unicenter NSM 系统代理
- Dell OpenManage
- Fujitsu ServerView 代理（用于 PRIMERGY 服务器）
- HP Systems Insight Manager
- iAgent
- IBM Director
- Net-SNMP (UC Davis)
- Sun 管理中心

通过对监控代理的此支持，可以查看和评估有关网络中主机系统上资源状态的最新相关信息。

主机系统资源管理的概念

以下术语和概念对于了解和使用 CA Spectrum 主机系统资源管理很重要。

警报状况

*警报状况*是指在 RFC 2790 监控规则中指定的进程阈值。

配置阈值

*配置阈值*是指在 NSM 代理监控规则中指定的进程阈值。

文件系统

*文件系统*是主机上的任何数据存储系统。

主机

*主机*是与网络中的其他系统进行通信的任何计算机系统。在本指南中，主机是指在 CA Spectrum 中进行建模并支持 RFC 2790 主机资源 MIB、NSM 代理专有的 MIB 或日志文件监控的任何设备。

主机资源

*主机资源*是可以监控的进程、文件系统、处理器、内存以及其他主机元素。

日志文件

*日志文件*是包括有关主机或主机应用程序的状态信息的任何文件。

监控器规则

通过 OneClick 中的*监控器规则*，可以将 CA Spectrum 警报与资源状态更改和资源活动阈值相关联。

进程

*进程*是在主机上运行的任何应用程序。

监控任务概述

本指南提供有关在 OneClick 中完成以下任务的说明：

- 创建和管理进程监控规则
- 创建和管理文件系统监控规则
- 创建应用于 CA Spectrum 全局集合容器器的文件系统监控规则集，以便自动创建监控规则
- 创建日志文件监控器

创建进程和文件系统监控规则

为主机模型创建进程或文件系统监控规则时，会指定导致 CA Spectrum 生成警报的状况。创建监控规则时，可以指定多个可用状况。也可以指定 CA Spectrum 是为监控规则模型还是主机模型生成警报。

详细信息：

创建进程监控规则 (p. 15)
创建文件系统监控规则 (p. 37)

RFC 2790 主机资源 MIB 监控规则警报状况和阈值

支持 RFC 2790 主机资源 MIB 的主机的进程监控规则包括以下警报状况：

- 进程启动
- 进程停止
- 进程实例计数超过特定数
- 进程实例计数降至特定数之下

文件系统监控规则包括以下警报状况：

- 达到文件系统利用率阈值
- 文件系统脱机

有关 RFC 2790 主机资源监控规则的详细信息，请参阅配置 RFC 2790 进程监控规则参数 (p. 18)。

NSM 代理监控规则阈值

下表显示了可以为 NSM 代理进程监控规则指定的配置阈值。可用阈值取决于主机类型（UNIX 或 Windows）以及主机上代理的版本（3.1 或 r11）。

有关详细信息，请参阅 NSM 代理进程监控规则参数 (p. 19)。

	平台和 NSM 代理版本			
配置阈值	**Win r11**	**UNIX r11**	**Win 3.1**	**UNIX 3.1**
子项	X	X	X	X
CPU 使用率	X	X	X	X
长期 CPU 使用率		X		
句柄	X			
实例	X	X	X	X
重新启动	X	X		
运行时	X			
大小	X	X	X	X
线程	X	X	X	

使用规则集自动创建监控规则

规则集是监控规则的集合。可以将一个或多个规则集应用于全局集合容器，以便为该容器中的模型自动创建监控规则。将支持 RFC 2790 MIB 或 NSM 代理的模型添加到集合时，会在模型上自动配置监控规则。将为规则集中的规则适用的任何进程或文件系统配置规则。

例如，包括 svchost.exe 进程的监控规则的规则集将应用于全局集合。该集合配置为在 CA Spectrum 中对主机进行建模时添加 Windows 主机。在添加到集合的所有主机模型上，配置了 svchost.exe 的监控规则。相反，从集合中删除主机时，监控规则将从主机中删除。

对与全局集合关联的规则集中的规则进行的修改，将应用于该规则的所有实例。此类型的规则具有一个指示器，表明它属于规则集（或者规则集“拥有”它）。可以在规则集名称中检查规则集所有权。在 OneClick 中所有受监控的进程表和受监控的文件系统表中，该名称将出现在“规则所有者”字段中。

假定您要更改 svchost.exe 监控的警报状况。在 svchost.exe 规则中，将最大进程计数阈值从 10 更改为 12。然后，更改将应用于集合中的所有 svchost.exe 监控规则实例。

有关详细信息，请参阅创建规则集 (p. 41)。

关于创建日志文件监控器

支持日志文件监控的代理使用正则表达式来查找日志文件文本。通常，监控日志文件以查找有关系统或应用程序错误状况的信息。文本匹配项的发现可导致 CA Spectrum 在产生日志文件条目的设备上生成警报。

有关详细信息，请参阅日志文件监控 (p. 47)。

主机资源监控和服务水平协议

通过主机资源监控，可以监控可以影响在服务水平协议 (SLA) 中定义的网络服务的主机资源。例如，进程监控规则可以确定，病毒防护进程是否已意外停止，或者恶意进程在主机上是否已启动。文件系统监控规则可以确定，主机上的磁盘驱动器或物理 RAM 是已达到容量还是接近容量。业务服务的生存能力可能取决于进程是否正在主机上运行，或者主机是否提供了足够的数据存储容量。

注意：有关设置服务管理系统和 SLA 的详细信息，请参阅《*Service Manager 用户指南*》。

主机资源事件和警报报告

通过 CA Spectrum Report Manager 应用程序，可以生成有关主机模型的事件和警报的报告。为受监控进程和文件系统的阈值违反生成警报和报告。也可以通过从日志文件解析的错误消息生成警报。

注意：有关详细信息，请参阅《*Report Manager 用户指南*》。

在 OneClick 中管理主机系统资源入门

本节介绍如何调用在其中配置监控规则、规则集和受监控主机资源信息的视图的工作区。

注意：有关 OneClick 控制台接口元素的详细信息，请参阅《*操作员指南*》。

访问工作区以创建和管理监控规则

从支持监控代理的主机模型的上下文创建和管理监控规则。

遵循这些步骤:

1. 从“内容”面板中选择要为其创建监控规则的主机。
2. 在“组件详细信息”面板中的“信息”选项卡下，展开“系统资源”选项。

   通过“正在运行的进程和受监控的进程”部分，可以创建和管理进程监控规则。有关详细信息，请参阅进程监控 (p. 15)。

   通过“受监控的日志和进程日志”部分，可以创建日志文件监控规则。有关详细信息，请参阅日志文件监控 (p. 47)。

   通过“文件系统”部分，可以创建文件系统监控规则。有关详细信息，请参阅文件系统监控 (p. 37)。

访问工作区以创建和管理规则集

与为特定主机创建的监控规则不同，CA Spectrum 为全局集合创建不同的规则。对于已向其应用规则集的全局集合中包括的任何主机，CA Spectrum 将创建您在规则集中指定的规则。此功能自动完成为多种不同主机类型创建监控规则的过程。

在“内容”面板中管理规则集。

遵循这些步骤:

- 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

  “内容”面板将列出已创建的任何规则集。

  未设置默认规则。有关创建和管理规则集以及将其应用于全局集合的详细信息，请参阅使用监控规则集 (p. 41)。

查看监控规则信息

通过 OneClick，可以在“组件详细信息”面板中查看有关受监控进程和文件系统的综合信息。

查看有关进程监控规则的信息：

- 依次选择“定位器”、“系统及应用程序监控”、“所有受监控的进程”。

  注意：由于没有为 SystemEDGE 主机的规则创建进程模型，因此 SystemEDGE 主机的监控规则不出现在此视图中。

查看有关文件系统监控规则的信息：

- 依次选择“定位器”、“系统及应用程序监控”、“所有受监控的文件系统”。

此视图提供了有关选定主机以及该主机上监控配置的信息。与规则关联的监控代理确定此视图提供的信息。

第 2 章： 进程监控

进程监控规则指定一旦满足就会导致 CA Spectrum 生成警报的标准。本节介绍如何通过进程监控代理为主机模型设置进程监控规则。有关设置自动化方法以便为全局集合容器中包括的模型创建进程监控规则的信息，请参阅使用监控规则集 (p. 41)。

此部分包含以下主题：

创建进程监控规则

可以为主机模型创建进程监控规则，而不管进程是否在主机上运行。

注意：只有具有相应权限的用户才能创建进程监控规则。有关详细信息，请参阅系统及应用程序监控权限 (p. 79)。

遵循这些步骤:

1. 在“内容”面板中，选择要为其创建监控规则的主机模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板中的“信息”选项卡上，依次展开“系统资源”、“正在运行的进程和受监控的进程”。

   将出现此主机类型的可用进程选项。

   注意：RFC 2790 表示支持 RFC 2790 主机资源 MIB 的主机。

3. 展开“正在运行的进程”和“受监控的进程”。

   “正在运行的进程”表列出了选定主机模型的正在运行的进程。

   “受监控的进程”表列出了已为选定主机模型创建的进程监控规则。

4. 要为选定的主机模型创建进程监控规则，请使用以下方法之一：
   - 如果进程正在运行，请在“正在运行的进程”表中右键单击该进程，然后选择“监控该进程”。
   - 如果进程未运行，则它不会包括在“正在运行的进程”表中。单击“受监控的进程”表上方的“添加”。然后，可以为定期运行但当前未运行而且您想了解它们何时启动的进程指定进程监控规则。例如，您想要了解病毒扫描和系统维护进程何时运行。

     注意：对于 NSM 代理监控，要创建监视匹配标准指定的多个不同进程的监控规则时，请使用此方法。有关详细信息，请参阅 NSM 代理进程监控规则参数 (p. 19)。

   将根据主机类型，打开一个对话框。如果从“正在运行的进程”表中选择了进程，则对话框包括进程名称和其他信息。如果使用“添加”选项调用了对话框，则系统将提示您提供所有进程信息。

5. 配置进程监控规则设置：
   - 对于支持 RFC 2790 主机资源 MIB 的代理，请参阅 RFC 2790 进程监控规则参数 (p. 18)。
   - 对于支持 NSM 代理版本 3.1 或 r11 的代理，请参阅 NSM 代理进程监控规则参数 (p. 19)。
   - 对于 SystemEDGE 主机代理，请参阅 SystemEDGE 主机进程监控规则参数 (p. 28)。

6. 单击“确定”。

   将发生以下事件：
   - 进程监控规则将添加到“受监控的进程”表。表的各列表示特定于选定主机上监控代理类型的预定义进程标识符信息。规则将应用于满足进程匹配选择标准的进程的所有相同实例。
   - 将为 RFC 2790 和 NSM 代理规则创建进程模型。

   注意：监控规则中的本地所有权表示，已为特定的主机显式创建规则，因此它不是规则集的一部分。有关规则集的详细信息，请参阅使用监控规则集 (p. 41)。

7. 根据主机类型，指定位于“受监控的进程”表上方的警报生成和代理轮询选项：

   监视新进程的时间间隔(秒)

   指定 CA Spectrum 检查“正在运行的进程”表以查找监控规则监视的进程的新实例的频率。CA Spectrum 检测到进程的新实例正在运行时，将更新“受监控的进程”表中受监控进程的“正在运行的数量”值。

生成警报 -

为因规则违反产生的警报选择目标。可以指定 CA Spectrum 在进程监控规则模型或主机模型上创建警报。

注意：警报始终在 SystemEDGE 主机的主机模型上，因为没有为 SystemEDGE 主机上的规则创建进程模型。

代理轮询时间间隔(秒)

指定代理从主机设备收集进程信息的频率。最小值为 30 秒。

代理轮询方法

指定代理收集进程数据的方式和时间：

已禁用

代理不检索进程信息（通过轮询或通过 GET 请求），并且它将警报状况的所有状态指示设置为“被动”或“正常”。

轮询时间间隔并查询

代理既通过轮询又通过 GET 请求来检索进程信息。

仅轮询时间间隔

代理仅通过轮询来检索进程信息。

仅查询

代理仅通过 GET 请求来检索进程信息。

区分进程

主机可以随时运行特定进程的多个实例。典型的示例有 Windows 主机上的 svchost.exe 进程以及 Linux 和 UNIX 主机上的 nfsd 进程。可以创建应用于所有进程实例、某些进程实例或某个进程实例的进程监控规则。例如，如果决定监控 svchost.exe 的所有实例，则不要按参数或名称区分它们。

对于 CA Spectrum，在 svchost.exe 进程监控规则中指定的警报状况和阈值将应用于进程的所有实例。假定规则指定进程启动和停止的警报，则 CA Spectrum 将为每个实例的每次启动和停止生成警报。换句话说，CA Spectrum 将规则应用于“正在运行的进程”表中与“受监控的进程”表中的条目匹配（按进程名称）的每个条目。

可以为进程的一个实例或一组相同的实例创建规则。在这种情况下，必须将该实例或实例组与您不希望监控的实例区分开。可以使用唯一名称和/或参数来区分它们。通过区分选项，可以在进程实例之间建立许多不同类型的区别。

进程监控规则参数

本节介绍以下主机类型的进程监控规则参数：

- RFC 2790 (p. 18)
- NSM 代理 (p. 19)
- SystemEDGE 主机 (p. 28)

RFC 2790 进程监控规则参数

为支持 RFC 2790 监控的主机创建进程监控规则时，可以指定以下参数：

- 进程标识符，包括进程名称和进程区分器
- 进程启动/停止和进程计数警报状况
- 轮询“正在运行的进程”表，以查找具有关联监控规则的进程的新实例

监控器信息

可以选择性地监控进程的所有实例或进程的特定实例。在监控规则中使用以下参数：

进程名称

标识主机模型上的进程。可以使用此设置区分进程实例，也可以使用“匹配参数”字段提供更精确的区分。

对于支持 RFC 2790 监控的主机，在此字段中输入的值不区分大小写。它将转换为小写形式，如在“受监控的进程”(RFC 2790) 表中显示的那样。此外，不允许重复条目。如果创建具有相同进程名称（和“匹配参数”值，如果已指定）的新条目，则新条目将替换现有的条目。将更新已更改的任何配置设置。

匹配参数

指定区分同一进程的同名实例的一个或多个进程参数。可以添加参数，也可以在保存配置之前修改进程附带的参数。此设置与“进程名称”一起使用以区分进程实例。有关详细信息，请参阅关于区分进程 (p. 17)。

描述性名称

标识进程的绰号。与其固有名字相比，我们建议提供更明确传达进程的作用或功能的描述性名称（例如，用“java 运行时”表示 javaw.exe 进程）。此设置不充当进程区分器。

警报配置

在 RFC 2790 监控规则中，可以指定以下警报状况：

进程计数小于

指定进程实例计数小于特定值时，CA Spectrum 是否生成警报。进程计数等于或大于该值时，CA Spectrum 将清除警报。

进程计数大于

指定进程实例计数大于特定值时，CA Spectrum 是否生成警报。进程计数等于或小于该值时，CA Spectrum 将清除警报。

进程启动

指定每当启动进程时 CA Spectrum 是否生成警报。进程停止时，CA Spectrum 将清除进程启动警报。

进程停止

指定每当停止进程时 CA Spectrum 是否生成警报。进程启动时，CA Spectrum 将清除进程停止警报。

NSM 代理进程监控规则参数

进程监控规则在“添加受监控的进程”对话框中定义，如创建进程监控规则 (p. 15)中所述。为支持 NSM 代理监控的主机创建进程监控规则时，可以指定以下参数：

- 进程监控规则标识符
- 进程匹配标准
- 配置阈值监控选项
- 配置阈值
- 高级选项，如聚合状态评估策略、资源群集组以及聚合违反阈值

注意：您的 NSM 代理版本和代理主机平台确定您对所有这些设置以及本节介绍的选项的访问权限。

可以为所有平台上的所有 NSM 代理版本指定代理轮询时间间隔和方法。有关详细信息，请参阅创建进程监控规则 (p. 15)。

监控器信息

“添加受监控的进程”对话框包括以下进程监控规则标识符。可用的标识符取决于 NSM 代理版本和代理主机平台：

监控器名称

标识监控规则的名称。CA Spectrum 按监控器名称区分相同的监控规则配置。此名称必须是唯一的。

描述性名称

标识监控规则的绰号或简短的描述性词语。

下表介绍了唯一地标识每种代理类型的进程监控器的属性或字段：

版本	监控器标识字段
Win r11	监控器名称* 描述性名称（可选）
UNIX r11	监控器名称* 描述性名称（可选）
Win 3.1	描述性名称（可选） 进程名称* 路径* 用户*
UNIX 3.1	进程名称* 参数 * 路径 * 用户 *

* 唯一地标识进程监控器。

进程匹配标准

在 NSM 代理上实施进程监控规则之前，按照阈值标准识别您希望 CA Spectrum 评估的进程。可以使用正则表达式和字符串比较来识别进程。

重要说明！ r11 代理支持在匹配标准中使用正则表达式，但是 3.1 代理仅支持使用通配符 (*)。

下表介绍了用作每种类型的 NSM 代理的进程匹配标准的属性或字段。

注意：对于 r11 NSM 代理，“匹配类型”将应用于所有其他匹配标准属性的组合。它定义如何评估其他进程匹配字段的组合。

版本	监控器标识字段
Win r11	进程名称 匹配类型 路径 用户
UNIX r11	进程名称 匹配类型 参数 路径 用户
Win 3.1	进程名称 路径 用户
UNIX 3.1	进程名称 参数 路径 用户

根据您正在使用的 NSM 代理版本和代理主机平台，“添加受监控的进程”对话框包括以下字段和选项：

进程名称

标识要匹配的进程或进程文本模式。可以使用文本字符串标识符或正则表达式来指定文本搜索模式。

注意：如果未指定其他进程匹配标准，则将监控与“进程名称”字段中的名称匹配的所有进程。

匹配类型

可用于指定与进程匹配标准匹配或不匹配的一个或多个进程。

注意：“进程名称”匹配标准不区分大小写。

选项包括：

正向正则表达式

代理将搜索与正则表达式形式的进程名称匹配的进程。

反向正则表达式

代理将搜索与正则表达式形式的进程名称不匹配的进程。

正向字符串比较

代理将搜索与字符串比较形式的进程名称匹配的进程。

反向字符串比较

代理将搜索与字符串比较形式的进程名称不匹配的进程。

参数

标识要匹配的进程参数。根据您正在使用的 NSM 版本和平台，可以将参数指定为文本字符串或正则表达式。

路径

标识要匹配的一个或多个进程的路径名称。可以将路径指定为文本字符串或正则表达式。

用户

标识要匹配的进程帐户的用户名。您可以将用户名指定为文本字符串或正则表达式，具体取决于所使用的 NSM 版本和平台。

NSM 代理的阈值配置

阈值配置定义由监控器监视的内容。创建监控规则时，可以指定多个阈值。例如，可以指示监控器仅监视进程消耗的 CPU 时间量。或者，可以指示监控器监视 CPU 使用率以及进程子项、线程和句柄，还可以监视进程重新启动的频率。

CA Spectrum 将针对警告阈值违反生成主要（橙色）警报，针对关键阈值违反生成关键（红色）警报。警报生成取决于监控规则的总体状态。

您可以指定的阈值取决于主机平台（Windows 或 UNIX）以及主机上运行的 NSM 代理版本（3.1 或 r11）。

下表介绍了对每个 NSM 代理可用的阈值和监控选项：

阈值	**监控选项** **平台和代理版本**			
	Win r11	**UNIX r11**	**Win 3.1**	**UNIX 3.1**
子项	不监控 宕掉-警告 宕掉-关键	不监控 宕掉-警告 宕掉-关键	不监控 宕掉-警告 宕掉-关键	不监控 监视器

阈值	监控选项 平台和代理版本 Win r11	UNIX r11	Win 3.1	UNIX 3.1
CPU 使用率	不监控 仅警告 仅关键 仅最小值 仅最大值 全部	不监控 仅警告 仅关键 仅最小值 仅最大值 全部	不监控 仅警告 仅关键 两者	不监控 仅警告 仅关键 两者
长期 CPU 使用率	N/A	不监控 仅警告 仅关键 仅最小值 仅最大值 全部	N/A	N/A
句柄	不监控 宕掉-警告 宕掉-关键	N/A	N/A	N/A
实例	不监控 宕掉-警告 宕掉-关键	不监控 宕掉-警告 宕掉-关键	不监控 宕掉-警告 宕掉-关键	不监控 监视器
重新启动	不监控 宕掉-警告 宕掉-关键	不监控 宕掉-警告 宕掉-关键	N/A	N/A
运行时	不监控 宕掉-警告 宕掉-关键	N/A	N/A	N/A
大小	不监控 仅警告 仅关键 仅最小值 仅最大值 全部	不监控 宕掉-警告 宕掉-关键	不监控 仅警告 仅关键 两者	不监控 监视器
线程	不监控 宕掉-警告 宕掉-关键	不监控 宕掉-警告 宕掉-关键	不监控 宕掉-警告 宕掉-关键	N/A

注意：为特定的最小值或最大值阈值指定值“-1”可禁用该阈值。例如，您可以选择指定监控器监视最小阈值而不监视最大阈值，或者相反。

子项

指定监控器是否监视进程子项计数。

注意：对于 Windows 上的版本 r11，此选项位于“资源”>“类型”下拉列表中。

CPU 使用率/CPU 短期使用情况/CPU 长期使用情况

指定监控器是否监视进程使用的 CPU 时间量。

一些可用的选项包括：

警告阈值

此值可以介于百分之一 (1) 和百分之九十九 (99) 之间，但是它必须在关键阈值百分比值以下。对于多个进程实例，将所有实例的最大值与此值进行比较。

关键阈值

此值可以介于百分之二 (2) 和百分之百 (100) 之间，但是它必须超过警告阈值百分比值。对于多个进程实例，将所有实例的最大值与此值进行比较。

CPU 间隔

此值定义以秒为单位的总值，用作计算 CPU 值的基础。具体地说，进程的 CPU 使用率（以秒为单位）指的就是此间隔。可以将值设置为大于零 (0) 的任何值或设置为 -1。

- 如果设置为 -1，则 CPU 值将计算为 CPU 使用率（以秒为单位），自启动代理或者创建进程监控规则起使用到当前时间。
- 如果 CPU 间隔设置为大于当前代理轮询时间间隔的值，且此时间第一次未过去，则将推算 CPU 值。
- 如果 CPU 间隔设置为小于当前代理轮询时间间隔的值，则 CPU 值将计算为上次代理轮询时间间隔值的适当比重。
- 如果 CPU 间隔设置为大于当前代理轮询时间间隔的值，并且此时间已过去，则 CPU 值将计算为可变的总和（当前轮询时间间隔的值与上次轮询时计算的值的总和），并根据其占 CPU 间隔的比重进行加权。
- 如果间隔设置为 -1，则忽略用于阈值的任何过载 (%)。

最小/最大单位

用于 CPU 使用率阈值的度量单位，以秒为单位或作为百分比。

实例

指定监控器是否监视进程实例计数。

资源

指定监控器是否监视以下资源类型之一：

线程

指定进程线程计数。

句柄

指定进程中的每个线程当前打开的句柄总数。

子项

指定进程子项计数。

运行时

指定进程自创建以来已运行的时间（以秒为单位）。

重新启动

指定监控器是否监视进程重新启动计数。确定代理用来确定以下情况的策略：何时针对阈值违反将重新启动警报状况的状态设置为“宕掉”。

要求进程不得停止或启动

如果任何进程停止或启动，则将状态设置为“宕掉”。

要求进程不得停止

如果任何进程停止，则将状态设置为“宕掉”。

要求进程不得启动

如果任何进程启动，则将状态设置为“宕掉”。

要求某些进程继续执行

如果所有进程停止，则将状态设置为“宕掉”。

大小

指定监控器是否监视进程消耗的内存量（以 KB 为单位）。

线程

指定监控器是否监视进程线程计数。

注意：对于 Windows 上的版本 r11，此选项位于“资源”>“类型”下拉列表中。

监控选项

监控选项指定 NSM 代理是否监视特定的配置阈值以及要监视哪些阈值类型（警告或关键，最小值或最大值）。

根据主机平台（Windows 或 UNIX）、NSM 代理版本（3.1 或 r11）以及正在配置的特定警报状况，“添加受监控的进程”对话框中的“监控器”下拉列表包含以下选项：

不监控

无警报。代理忽略阈值设置。

监控

关键警报。代理监控所有阈值的最小值和最大值。

仅警告

主要警报。代理仅评估警告阈值（最小值和最大值）以确定进程的状态。

仅关键

关键警报。代理仅评估关键阈值（最小值和最大值）以确定进程的状态。

仅最小值

主要（警告）和关键（关键）警报。代理仅评估最小阈值（警告和关键）以确定进程的状态。

仅最大值

主要（警告）和关键（关键）警报。代理仅评估最大阈值（警告和关键）以确定进程的状态。

全部

主要（警告）和关键（关键）警报。代理将评估所有阈值。

宕掉-警告

主要警报。资源处于错误状况时，代理将使用警告重要级别。这样，就可以将阈值违反指定为不如宕掉-关键违反重要。

宕掉-关键

关键警报。资源处于错误状况时，代理将使用关键重要级别。这样，就可以将阈值违反指定为比宕掉-关键违反更重要。

两者

主要（警告）和关键（关键）警报。代理同时评估警告阈值和关键阈值以确定进程的状态。

高级选项

通过高级选项，可以在监控器监视两个或多个进程、进程资源群集组以及聚合警报状况违反阈值（在被满足时，会将进程的状态降级并触发 CA Spectrum 警报生成）时，为配置阈值违反指定评估策略。

注意：可用的高级选项取决于您正在配置的主机平台（Windows 或 UNIX）和 NSM 代理版本（3.1 或 r11）。

评估策略（仅限 r11）

指定代理如何计算它将与监视多个不同进程的监控器的警报状况阈值进行比较的值。它还指定在阈值违反的违反者列表中包括的其他进程。

注意：NSM 代理版本 3.1 将来自所有受监视进程实例的最差值（单个策略）与警报状况阈值进行比较，以确定阈值遵从性。

评估策略选项包括：

单个（默认值）

指定代理将所有进程实例的最差值（最低和/或最高）与警报状况阈值进行比较。如果值违反阈值状况，则违反者列表将包括单独违反最严重阈值的所有实例。

最小值

指定代理将所有进程实例的最低值（最小值）与警报状况阈值进行比较。如果值违反阈值状况，则违反者列表将包括具有相同最小值的所有实例。

最大值

指定代理将所有进程实例的最高值（最大值）与警报状况阈值进行比较。如果值违反阈值状况，则违反者列表将包括具有相同最大值的所有实例。

总和

指定代理将所有进程实例的累计值（总和）与警报状况阈值进行比较。如果值违反阈值状况，则违反者列表将包括所有的实例。

平均值

指定代理将所有进程实例的平均值与警报状况阈值进行比较。如果值违反阈值状况，则违反者列表将包括单独违反最严重阈值的所有实例。

群集资源组（仅限 r11）

标识群集资源组。

聚合违反阈值

此选项指定连续的代理轮询循环数，在循环中任何阈值需要处于“次于正常”状态后监控器的聚合状态才更改。此值必须大于 0。“聚合违反阈值”字段对 UNIX 3.1 不可用。

选定主机模型的“受监控的进程”表中的“状态”字段指示聚合状态状况。

如果 NSM 代理未能检索进程信息

如果负责检索进程监控信息的 NSM 代理子代理关闭，则 CA Spectrum 将做出如下响应：

- 在主机模型上生成“NSM 进程监控代理已丢失”警报
- 在进程模型上断言已抑制的 APPLICATION_LOST 警报状况

进程监控子代理重新启动时，CA Spectrum 清除主机模型上的“NSM 进程监控代理已丢失”警报，并清除关联的进程模型上的 APPLICATION_LOST 警报。

NSM 代理进程监控规则的状态指示

选定主机模型的“受监控的进程”表中的“状态”字段指示监控器的聚合状态状况。“状态”字段表示在监控器上定义的每个阈值的状态值的最差聚合。

任何阈值处于被违反状态超过特定的连续代理轮询循环数时，聚合状态将进入未达最佳状态。“聚合违反阈值”字段定义在聚合状态值更改之前任何阈值处于被违反状态的连续次数。在聚合状态处于未达最佳状态之前，CA Spectrum 不会为违反的阈值生成警报。

SystemEDGE 主机进程监控规则参数

进程监控规则在“添加进程监控表项目”对话框中定义。有关详细信息，请参阅创建进程监控规则 (p. 15)。

为 SystemEDGE 主机创建进程监控规则时，可以指定以下参数：

- 进程监控规则标识符
- 配置阈值监控选项
- 配置阈值
- 高级选项，如发送陷阱以及监控父进程或 Windows 服务

注意：为 SystemEDGE 主机创建规则时，不创建进程模型。因此，在“定位器”选项卡中搜索并查看规则时，监控规则不会出现。

监控器信息

“添加进程监控表项目”对话框包括以下进程监控规则标识符：

索引

指定唯一标识进程监控器条目的整数值。如果在创建条目时此字段保留为空或者设置为 0，则将自动选择未使用的索引。

进程名称

标识要匹配的进程文本模式。可以使用文本字符串标识符或正则表达式来指定文本搜索模式。

匹配参数

指示是同时匹配进程名称和参数还是仅匹配进程名称。

说明

标识监控规则的绰号或简短的描述性词语。

阈值配置

阈值配置定义监控器监视的属性和度量标准。根据 SystemEDGE 主机版本，创建监控规则时，可以指定适用的阈值。

可以使用以下参数：

属性

是要监控的进程属性。

运算符

是用于将当前值与阈值进行比较的布尔运算符。“无运算”仅跟踪当前值；它不会与阈值进行比较。

阈值

是代理用来与当前值进行比较的阈值。此参数与“运算符”参数一起使用。

间隔

是代理连续采样之间的时间（以秒为单位）。值介于 30 到 MAXINT 之间且必须是 30 的倍数。

采样类型

是对受监控对象执行的采样类型。

绝对

度量实际的值（如测量仪）。

增量

度量值的变化（如计数器）。

重要级别

是用于对象状态模型的重要级别。

注意：此阈值并非对所有的 SystemEDGE 主机版本都可用。

对象类

是用于对象状态模型的对象类。

注意：此阈值并非对所有的 SystemEDGE 主机版本都可用。

对象属性

是用于对象状态模型的对象属性。

注意：此阈值并非对所有的 SystemEDGE 主机版本都可用。

对象实例

是用于对象状态模型的对象实例。

注意：此阈值并非对所有的 SystemEDGE 主机版本都可用。

执行操作

指定越过阈值时执行的命令（一个字符串，最多为 4096 个字符）。操作脚本必须存在于主机上。

发送参数

指示是否将默认参数发送到操作脚本或程序（如陷阱类型或说明字段）。

高级选项

通过高级选项，可以指定要在监控过程中执行的操作。

发送 SNMP 陷阱

指示是否发送 SNMP 陷阱。

发送进程启动陷阱

指示是否发送进程启动陷阱。

句柄进程启动陷阱

指示在发生进程启动陷阱时是否执行操作、记录事件并发送 SNMP 陷阱。此标志便于同时设置三个单独的标志。

发送未就绪陷阱

指示是否发送未就绪陷阱。

单个

发送单个未就绪陷阱。

连续

发送连续未就绪陷阱。

发送进程清除陷阱

指示是否发送进程清除陷阱。

监控父进程

指示是否监控父进程。

监控 Windows 服务

指示是否监控 Windows 服务。

重新初始化条目

指示是否重新初始化条目。

日志事件

指示是否记录事件。

监控 *x* 个进程

指示是否监控指定数目的进程。

出现 *x* 个连续事件后违规

指示在出现指定数目的连续事件之后是否发送陷阱。

允许 *x* 个连续违规陷阱

指示是否允许指定数目的连续违规陷阱。

编辑进程监控规则

可以编辑本地的进程监控规则。也可以在主机模型的上下文中编辑规则集拥有的规则。在后一种情况下，修改会将规则的所有权从规则集变换到模型（“规则所有者”值转换为“本地”）。

重要说明！要编辑规则，您必须在创建规则的所有格局中具有用户模型。

遵循这些步骤:

1. 在“内容”面板中，选择具有要编辑的进程监控规则的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板的“信息”选项卡中，展开“系统资源”、“正在运行的进程和受监控的进程”、“受监控的进程”。

   “受监控的进程”表列出了选定模型的进程监控规则。

3. 选择要编辑的进程监控规则，然后单击“编辑”。

   此时将打开“编辑进程监控表项目”对话框。

4. 根据需要修改设置，然后单击“确定”。

   对选定模型的进程监控规则进行的更改将立即生效。

删除进程监控规则

可以删除本地进程监控规则和由主机模型的规则集拥有的规则。在前一种情况下，停止对进程的监控。在后一种情况下，按照规则集中的规则，删除还停止对特定模型的监控。但是，删除规则集中的规则是暂时的。下次更新规则集时，将重新建立规则指定的进程监控。有关详细信息，请参阅删除规则集之外的规则 (p. 46)。

删除进程监控规则时，CA Spectrum 和进程监控代理将停止监控在规则中指定的进程的所有相同（无差别）实例。此外，规则将从代理 MIB 中删除。

遵循这些步骤:

1. 在“内容”面板中，选择具有要删除的进程监控规则的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板中，依次展开“系统资源”、“正在运行的进程和受监控的进程”、“受监控的进程”。

   “受监控的进程”表列出了选定模型的进程监控规则。

3. 选择要删除的进程监控规则，然后单击“删除”。

   系统将提示您确认删除。

4. 确认删除。

   将删除进程监控规则。

   由选定模型的规则指定的进程监控将立即停止。

维护模式

进程监控器处于维护模式时，不监控进程。不生成与该进程的监控相关的任何事件或警报。

升级正在运行多个关键应用程序的主机上的单个应用程序时，将进程监控器置于维护模式可能很有用。进行升级时，只能将与该特定应用程序关联的进程置于维护模式。对其他应用程序的监控可以继续。

也可以排定维护模式，这样就可以指定一天中对进程发出警报的时间。

只有 RFC 2790 和 NSM 代理进程监控才支持维护模式。

注意：主机设备处于维护模式时，将自动挂起对该设备的进程监控。

将进程监控器置于维护模式

可以随时将进程监控器置于维护模式。此过程介绍如何立即将进程监控器置于维护模式。

遵循这些步骤:

1. 在“内容”面板中，选择要将其进程监控器置于维护模式的主机模型。

   注意：仅 RFC 2790 和 NSM 代理进程监控支持维护模式。

2. 在“组件详细信息”面板的“信息”选项卡中，展开“系统资源”、“正在运行的进程和受监控的进程”和“RFC 2790”（如果适用）。
3. 从“受监控的进程”或“受监控的进程(RFC 2790)”表执行以下步骤之一，将进程监控器置于维护模式：
   - 选择要置于维护模式的进程监控器，然后单击表上方的“维护”按钮。
   - 右键单击要置于维护模式的进程监控器，然后选择“切换维护模式”。

   进程监控器现在处于维护模式，且其图标更改为褐色。在“受监控的进程”表的“条件”列中反映了该模式。如果图标未立即更改，请单击“刷新”。

注意：可以使用此相同过程使进程监控器退出维护模式。

排定进程监控器的维护模式

通过应用维护排定，可以排定进程监控器处于维护模式的时间。可以应用现有的排定，也可以创建新的排定。可以将多个排定应用于进程监控器。

遵循这些步骤:

1. 在“定位器”选项卡上，依次选择“系统及应用程序监控”、“所有受监控的进程”。
2. 在“内容”面板中选择要对其应用维护排定的进程监控器。

   注意：仅 RFC 2790 和 NSM 代理进程监控支持维护模式。
3. 在“组件详细信息”面板中，展开“进程监控详细信息”子视图，查找“维护中”，然后单击“排定”。

   此时将打开“添加/删除排定”对话框。应用于进程监控器的任何维护排定将出现在“当前排定”列中。
4. （可选）应用现有的排定。从“可用排定”列中选择一个排定，然后单击向左箭头将其移至“当前排定”列。
5. 单击“创建”。

   此时将打开“创建排定”对话框。
6. 为排定选择开始日期、开始时间以及结束时间或持续时间。
7. 选择“重复”因子。

   注意：让“重复”设置为“无”可创建一次性维护模式窗口。
8. 提供说明以标识排定。
9. 单击“确定”。

   “创建排定”对话框将关闭。新的排定将出现在“添加/删除排定”对话框的“当前排定”列中。
10. 单击“确定”。

    “添加/删除排定”对话框将关闭。会对进程监控器应用维护模式排定更改。更改将出现在“已分配的维护排定”列表中。

从设备模型下滚维护警报

将设备置于维护模式时，在该设备上生成的维护警报可以下滚到关联的进程模型。通过将 rollMMAlarmToApp 属性设置为 true 启用此传播。启用此选项时，警报也将下滚到与设备关联的应用程序模型。

注意：有关将设备置于维护模式的信息，请参阅《*操作员指南*》。有关修改模型属性的信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

进程模型内部条件

CA Spectrum 可以维护进程模型的条件，而不使进程监控事件生成警报。在服务或资源监控器内并入多个受监控进程模型时，此功能可能很有用。违反服务策略时，可以在服务模型上生成单个警报，而不是每次违反进程监控规则时，都在设备或进程模型上生成警报。

默认情况下，禁用该功能。通过使用属性编辑器将 EnableInternalCondition 属性的值设置为 Yes，可以启用它。对于 NSM 进程监控，此属性位于设备模型上；对于 RFC 2790 进程监控，此属性位于 rfc2790App 应用程序模型上。启用或禁用该功能时，将在关联的进程模型上清除任何现有的进程监控警报，且其 InternalCondition 属性设置为 Normal。

启用该功能且“生成警报 - ”选项设置为“进程模型”时，进程监控事件不生成警报。相反，设置进程模型的 InternalCondition 属性以反映进程模型的条件。在“定位器”选项卡上“系统及应用程序监控”、“所有受监控的进程”表中“内部条件”列上显示了此属性的值。在进程模型的“属性”选项卡上也可以找到该值。

启用“内部条件”功能时，不要将日志文件监控器映射到任何进程模型。日志文件监控事件将继续生成警报。

对于支持 RFC 2790 监控的主机：

- 启用或禁用该功能时：
  - 手动清除受影响设备模型上存在的任何进程监控警报。
  - 将重新断言进程计数条件；但是，不重新断言进程启动和进程停止条件。
- 如果在其格局中的设备上启用“内部条件”功能时重新启动 SpectroSERVER，则必须禁用该功能，然后在设备上重新启用它。这些步骤可确保，进程模型的内部条件与进程监控器的实际条件准确同步。

第 3 章：文件系统监控

文件系统监控规则 (RFC 2790) 指定导致 CA Spectrum 生成警报的文件系统警报状况。在为其创建规则的主机模型上发生以下状况时，将生成警报：

- 文件系统利用率
- 文件系统脱机

本节介绍如何为特定的主机模型设置文件系统监控。有关为全局集合容器中的模型自动创建文件系统监控规则的信息，请参阅使用监控规则集 (p. 41)。

创建文件系统监控规则

创建文件系统监控规则时，可以指定任何文件系统（联机或脱机）。CA Spectrum 创建规则的模型。

在配置文件系统监控规则期间，定义导致 CA Spectrum 生成警报的警报状况。此类警报状况的示例包括系统利用率阈值或脱机的文件系统。

注意：只有具有相应权限的用户才能创建文件系统监控规则。有关详细信息，请参阅系统及应用程序监控权限 (p. 79)。

遵循这些步骤:

1. 在“内容”面板中，选择具有要监控的文件系统的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板中，依次展开“系统资源”、“文件系统”。

   将出现对此主机类型可用的文件系统监控选项。

3. 展开“文件系统(RFC 2790)”和“受监控的文件系统(RFC 2790)”。

   “文件系统(RFC 2790)”表列出了选定模型的文件系统。“受监控的文件系统(RFC 2790)”表列出了已为选定模型创建的文件系统监控规则。

4. 使用以下方法之一为选定模型创建文件系统监控规则：

   - 如果要监控的文件系统可用，请在“文件系统(RFC 2790)”表中右键单击该文件系统，然后选择“监控该文件系统”。

- 如果文件系统不可用并因此未包括在“文件系统(RFC 2790)”表中，请在“受监控的文件系统(RFC 2790)”表上单击“添加”。这样就可以指定（例如）您要了解的处于脱机状态的文件系统，并监控它何时联机。

此时将打开“添加文件系统监控器”对话框。如果从“文件系统(RFC 2790)”表中选择了文件系统，则该框包括文件系统名称。

5. 配置所需的设置。可用设置包括：

文件系统名称

指定文件系统。如果添加了要监控的文件系统但它当前不可用，请键入名称。如果添加了可用的文件系统，则名称会自动输入。

对于支持 RFC 2790 监控的主机，在此字段中输入的值不区分大小写。此字段将转换为小写形式，如“受监控的文件系统(RFC 2790)”表中显示的那样。不允许重复条目。如果创建具有相同文件系统名称的新条目，则新条目将替换先前的条目，更新已更改的任何配置设置。

说明

指定文件系统的绰号或别名。

阈值类型

指定按照容量百分比还是存储单位（字节、KB、MB、GB、TB）监控文件系统利用率阈值。

利用率阈值

指定事件、次要警报、主要警报和关键警报的阈值。度量标准不再超过阈值时，CA Spectrum 将清除阈值警报。

脱机时的警报

指定在文件系统脱机时 CA Spectrum 是否生成警报。文件系统恢复联机时，CA Spectrum 将清除警报。

6. 单击“确定”。

文件系统监控规则将添加到“受监控的文件系统(RFC 2790)”表。CA Spectrum 生成警报，以响应在规则中指定的警报状况阈值违反。

注意：监控规则的“规则所有者”字段中的“本地”值指示，该规则已为特定的主机显式创建，因此它不是规则集的一部分。有关规则集的详细信息，请参阅使用监控规则集 (p. 41)。

7. 从“生成警报 - ”下拉列表中选择因规则违反导致的警报的目标。可以指定 CA Spectrum 在监控规则模型或主机模型上创建警报。

编辑文件系统监控规则

可以编辑本地文件系统监控规则和由主机模型的规则集拥有的规则。在后一种情况下，修改会将规则的所有权从规则集变换到模型（“规则所有者”值转换为“本地”）。但是，更改和所有权转换是暂时的，因为下次更新规则集时，将重新建立原始规则规范和所有权。有关详细信息，请参阅编辑规则集之外的规则 (p. 45)。

重要说明！要编辑规则，您必须在创建规则的所有格局中具有用户模型。

遵循这些步骤:

1. 在“内容”面板中，选择具有要编辑的文件系统监控规则的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板中，依次展开“系统资源”、“文件系统”、“受监控的文件系统(RFC 2790)”。

   “受监控的文件系统(RFC 2790)”表列出了文件系统监控规则。

3. 选择要编辑的文件系统规则，然后单击“编辑”。

   此时将打开“编辑文件系统监控器”对话框。只读设置已变灰。

4. 根据需要修改设置，然后单击“确定”。

   对选定模型的文件系统监控规则进行的更改将立即生效。

删除文件系统监控规则

可以删除本地文件系统监控规则和由主机模型的规则集拥有的规则。在前一种情况下，停止对文件系统的监控。在后一种情况下，按照规则集中的规则，删除还停止对特定模型的监控。但是，删除规则集规则是暂时的，因为下次更新规则集时，将重新建立由规则指定的文件系统监控。有关详细信息，请参阅删除规则集之外的规则 (p. 46)。

遵循这些步骤:

1. 在“内容”面板中，选择具有要删除的文件系统监控规则的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板中，依次展开“系统资源”、“文件系统”、“受监控的文件系统(RFC 2790)”。

   “受监控的文件系统(RFC 2790)”表列出了文件系统监控规则。

3. 选择要删除的文件系统监控规则，然后单击“删除”。

   系统将提示您确认删除。

4. 确认删除。

   由选定模型的规则指定的文件系统监控将立即停止。

第 4 章： 使用监控规则集

规则集是可以应用于全局集合的进程和文件系统监控规则的集合。规则集自动完成设置和管理对在 CA Spectrum 中建模的主机的监控的过程。为特定主机模型创建进程或文件系统监控规则时，该规则仅应用于该主机模型。如果要将相同的规则应用于其他主机模型，请为每个主机模型重复创建相同的规则。如果要为所有模型编辑该规则，请修改每个主机模型的每个规则实例。此任务显然是管理大量主机模型的主机监控的乏味而低效的方法。

通过将规则集应用于全局集合，可利用效率更高的方法管理 IT 基础架构资源。将主机模型添加到集合时，CA Spectrum 创建引用那些模型的进程或文件系统的监控规则。而且，修改规则集中的监控规则时，所做的修改将应用于集合中的所有主机模型。从集合中删除主机模型时，这些模型的所有监控规则也将被删除。

创建规则集

可以创建同时包含主机进程和文件系统的多个监控规则的规则集，也可以创建仅包含主机进程或文件系统的监控规则的规则集。可以将所需数目的规则集应用于全局集合。也可以将同一规则集应用于多个集合。

重要说明！ 仔细计划规则集的实施，以避免重复规则或实施冲突规则。重复的或冲突的规则可导致意外结果，并使故障排除变得很困难。此外，请验证对其应用规则集的全局集合是否包括适合那些规则集中监控规则的主机模型。

创建规则集时，请牢记以下要点：

- 规则集必须具有唯一名称。
- 规则集中包括的规则不覆盖全局集合中包括的主机模型的同名本地监控规则。如果已为特定主机模型创建本地监控规则，且该模型包括在已对其应用包含同名规则的规则集的全局集合中，则本地规则将得到保留，并对该模型保持有效。

注意： 只有具有相应权限的用户才能创建监控规则集。有关详细信息，请参阅系统及应用程序监控权限 (p. 79)。

遵循这些步骤:

1. 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

   “内容”面板将列出已创建的任何规则集。

   不存在默认规则集。

2. 单击 （按类型新建规则集），然后根据正在使用的代理选择以下选项之一：

   - RFC2790
   - NSM 代理：
     - r11 Windows
     - r11 UNIX
     - 3.1 Windows
     - 3.1 UNIX

   将出现“新的规则集”对话框。

3. 在“规则集名称”字段中键入规则集的名称，然后单击“确定”。

   新的规则集将出现在列表中。现在可以将进程监控和文件系统监控的配置规则添加到规则集。此外，可以将规则集应用于全局集合容器。

将监控规则添加到规则集

将规则集应用于全局集合之前或之后，可以将监控规则添加到规则集。

遵循这些步骤:

1. 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

   “内容”面板列出了规则集。

   注意: 如果未列出规则集，请为规则创建规则集，如创建规则集 (p. 41)中所述。

2. 选择要向其添加监控规则的规则集。

   “组件详细信息”面板显示了有关规则集的信息。

3. 在“信息”选项卡上，指定要添加到规则集的规则的类型：

   - 要添加进程监控规则，请展开“进程监控规则”。
   - 要添加文件系统监控规则，请展开“文件系统监控规则”。

     注意： NSM 规则集不支持文件系统监控规则。

   每个规则表都列出了已添加到规则集的规则。

4. 对于要添加到规则集的规则类型，单击“添加”。

   此时将打开“添加受监控的进程”对话框或“添加文件系统监控器”对话框。

5. 配置所需的设置。

   - 有关配置进程监控规则的信息，请参阅进程监控规则参数 (p. 18)。
   - 有关创建文件系统监控规则的信息，请参阅创建文件系统监控规则 (p. 37)。

6. 单击“确定”。

   规则将添加到规则集。

将规则集应用于全局集合

将规则集应用于全局集合将自动完成创建监控规则的过程。CA Spectrum 自动为全局集合中的所有模型创建监控规则。

将规则集应用于全局集合时，请考虑以下事实：

- 如果从全局集合中删除模型，则由规则集指定的所有监控规则将从模型中删除。
- 如果从全局集合中包括的特定模型的规则集编辑某规则，则该规则的所有权将更改为本地所有权。该规则不再与规则集中的规则关联，且仅应用于该特定模型。
- 如果删除与全局集合关联的规则集（反之亦然），则由该规则集指定的规则将从集合中的模型删除。

遵循这些步骤:

1. 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

   “内容”面板列出了规则集。

   注意：如果未列出规则集，请创建规则集，如创建规则集 (p. 41)中所述。

2. 右键单击要应用于全局集合的一个或多个规则集，然后选择“应用/删除全局集合”。

   将出现“将全局集合添加到规则集/将其从中删除”对话框。

   在对话框左侧列出的所有全局集合当前应用于选定的规则集。尚未应用在右侧列出的全局集合。

3. 在“没有应用于”列表中，双击要对其应用规则集的全局集合。

   选定的全局集合将移动到“应用于”列表。

   注意：不能将全局集合同时应用于多个规则集。

4. （可选）选中“重新应用”复选框，以重新应用在对话框中单击“确定”时已应用于规则集的一个或多个全局集合。

5. 单击“确定”以应用所做的更改。

   注意：仅应用在对话框中进行的更改。除非已选中“重新应用”复选框，否则将不重新应用在“应用于”列表中已出现的全局集合。

   选定规则集的“信息”选项卡中的“应用的全局集合列表”显示对其应用该规则集的全局集合。

从全局集合中删除规则集

从全局集合中删除规则集时，CA Spectrum 将从全局集合中的所有模型删除规则集中的监控规则。

遵循这些步骤:

1. 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

   “内容”面板列出了规则集。

2. 右键单击要从其删除全局集合的一个或多个规则集，然后选择“应用/删除全局集合”。

   将出现“将全局集合添加到规则集/将其从中删除”对话框。

   注意：也可以单击“结果”选项卡工具栏中的  启动此对话框。

   在对话框左侧列出的所有全局集合当前应用于选定的规则集。尚未应用在右侧列出的全局集合。

3. 在“应用于”列表中，双击要从规则集中删除的全局集合。

   选定的全局集合将移动到“没有应用于”列表。

   注意：不能将全局集合同时从多个规则集中删除。

4. （可选）选中“重新应用”复选框，以重新应用在对话框中单击“确定”时已应用于规则集的一个或多个全局集合。

5. 单击“确定”以应用所做的更改。

   注意：仅应用在对话框中进行的更改。除非已选中“重新应用”复选框，否则将不重新应用在“应用于”列表中已出现的全局集合。

将更新选定规则集的“信息”选项卡中的“应用的全局集合列表”。将不再显示已删除的一个或多个全局集合。

编辑规则集中的规则

编辑应用于全局集合的规则集中的规则时，修订的规则设置将扩展到全局集合中的所有模型。

重要说明！要编辑规则，您必须在创建规则的所有格局中具有用户模型。

遵循这些步骤:

1. 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

   “内容”面板列出了规则集。

2. 选择包含要编辑的规则的规则集。

   “组件详细信息”面板显示了有关规则集的信息。

3. 在“组件详细信息”面板中，指定要编辑的规则类型（进程监控规则或文件系统监控规则）。

   每个规则类型表都列出了规则集中已包括的规则。

4. 选择一个规则，然后单击“编辑”。

   此时将打开“编辑”对话框。

   注意：某些设置不能进行编辑。

5. 编辑设置，然后单击“确定”。

   修改后的设置将立即生效。

编辑规则集之外的规则

在某些情况下，可能希望修改全局集合中特定模型的监控规则，即使该规则属于已应用于全局集合的规则集。您可能不希望修改应用于规则集中的规则，因为修改稍后将应用于全局集合中的所有模型。但是，您仍希望将模型保留在集合中。

在这种情况下，将规则转换为模型的本地版本。可以从规则集之外的特定模型的上下文修改此规则，以达到此结果。

从规则集中删除规则

从应用于全局集合的规则集中删除规则时，该规则将从全局集合中的所有模型删除。

遵循这些步骤:

1. 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

   “内容”面板列出了规则集。

2. 选择包含要删除的规则的规则集。

   “组件详细信息”面板显示了有关规则集的信息。

3. 在“组件详细信息”面板中，指定要从规则集中删除的规则类型（进程监控规则或文件系统监控规则）。

   每个规则表都列出了规则集中已包括的规则。

4. 选择规则，然后单击“删除”。

   规则将从规则集及其规则表中删除。

删除规则集之外的规则

在某些情况下，可能希望删除全局集合中特定模型的规则，即使该规则属于已应用于全局集合的规则集。您可能不希望删除规则集中的规则，并进而为全局集合中的所有模型删除它。但是，您仍希望将模型保留在集合中。

在这种情况下，从规则集之外的特定模型的上下文中删除此规则。但是，更新规则集和全局集合之间的关联时，将为模型重新创建已删除的规则。

删除规则集

删除应用于全局集合的规则集时，该规则集中的所有规则都将从集合中的模型删除。

遵循这些步骤:

1. 依次选择“定位器”、“系统及应用程序监控”、“所有监控规则”。

   “内容”面板列出了所有的可用规则集。

2. 选择要删除的规则集，然后单击“删除”。

第 5 章：日志文件监控

本章介绍如何在 OneClick 中为以下代理设置日志文件监控：

- iAgent
- CA SystemEDGE 代理
- CA Unicenter NSM 代理

本章还介绍如何配置 iAgent syslog 服务器监控以及将陷阱转发到 CA Spectrum。

设置日志文件监控需要执行以下任务：

- 指定启动陷阱和事件生成的标准。在日志文件中检测到指定的信息类型时，将生成陷阱和事件。
- （可选）指定日志文件和受监控的进程模型之间的关联。然后生成事件以响应进程模型的日志文件条目。在进程模型上而不是进程主机模型上生成事件。

关于日志文件监控进程

可以配置网络上的各种设备，以将数据发送到 iAgent、SystemEDGE 代理或 NSM 服务器上的日志文件。或者，这些服务器之一上的应用程序可以将数据发送到日志文件。在任一情况下，都可以配置这些代理以监控这些日志文件，并基于日志文件条目中的内容生成 SNMP 陷阱。

日志文件监控涉及设置文本模式匹配系统，以检测和解析日志文件中是否有您指定的信息类型。然后，监控代理将包含有关已解析文本的数据的陷阱发送到 CA Spectrum。接下来将此数据映射到 CA Spectrum 事件，且在代理模型或与它有关的设备或进程上断言警报。也可以使用事件条件规则配置 CA Spectrum，以从“日志文件中的文本匹配”事件创建粒度更精细的事件和（可选）警报。因此，您会收到在基础架构中已发生且指示潜在或实际问题的事件的通知。有关详细信息，请参阅《*事件配置用户指南*》。

您正在监控的日志文件的语法取决于日志文件的类型和发送到它的数据。由于应用程序日志文件直接与您正在监控的应用程序匹配，因此不需要特殊的日志文件语法。但是，CA Spectrum 以不同方式处理从其他设备收集数据的其他日志文件。因此，这些日志文件条目必须符合特定的语法标准。

不管要监控的日志文件类型如何，无论应用程序日志文件还是包含来自多个设备的多个应用程序的条目的 syslog 文件，都必须定义标识或解析要监控的信息类型的正则表达式 (regex)。regex 语法必须与代理类型兼容。找到匹配文本时，监控代理将包含匹配文本的陷阱发送到 CA Spectrum。CA Spectrum 将陷阱与在主机模型上断言的事件关联。

注意：有关定义正则表达式的详细信息，请参阅《*事件配置用户指南*》。

配置 CA Spectrum 以处理 Syslog 文件匹配 (p. 59)说明如何配置代理以监控日志文件中生成陷阱的信息字符串。

注意：iAgent 只能监控 iAgent 服务器上存在的日志文件。它无法监控映射网络驱动器上的日志文件。

详细信息：

日志文件语法 (p. 48)

日志文件语法

可以监控应用程序日志或从其他设备接收数据的日志文件（如 Syslog 文件）。监控应用程序日志的日志文件不需要特殊的语法。但是，为了使 CA Spectrum 断言有关相应设备模型的陷阱信息，从网络上的设备接收信息的日志文件必须具有以下格式（它基于 BSD Syslog 和 Cisco IOS 格式）：

<MessagePrefix>%<MessageHeader><Additional_Information>

<MessagePrefix>

包含消息的日期和时间，以及在条目中包含的信息源的 IP 地址或主机名。可能有在前缀内散布的其他信息，但是它必须包含这两则信息。

注意：如果使用主机名来标识源，则它可以采用 myhost.ca.com 或 myhost 格式。

<MessageHeader>

必须具有以下格式：*<A>-<B>-*

<A>

包含任意数量的大写字母字符、下划线或字符串“Aprisma”。

<B>

包含任意数量的大写字母字符、数字字符或下划线。

<C>

包含任意数量的大写字母字符、下划线或短划线。

<Additional_Information>

可以包含任何数据。

通常，可以在以下类型的日志文件中找到此语法：

- 来自 Cisco 或 Riverstone 设备的 Solaris syslog 文件条目。
- 来自其他类型的设备的 Solaris syslog 文件条目，使用前面介绍的 *<MessageHeader>* 格式。
- 来自 Cisco 或 Riverstone 设备的 Kiwi syslog 文件条目。
- 来自其他类型的设备的 Kiwi syslog 文件条目，使用前面介绍的 *<MessageHeader>* 格式。
- CA 日志文件。

注意：有关配置 CA Spectrum 以处理 iAgent 陷阱的信息，请参阅配置 CA Spectrum 以处理 Syslog 文件匹配 (p. 59)。

详细信息：

关于日志文件监控进程 (p. 47)

为 iAgent 主机创建日志文件监控器

以下过程介绍如何为 iAgent 主机代理设置日志文件监控。

遵循这些步骤:

1. 在“内容”面板中，选择具有要监控的日志文件的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板的“信息”选项卡中，展开“系统资源”、“受监控的日志和进程日志”、“受监控的日志”。

   将显示“受监控的日志”列表。

   注意：某些列表字段是代理特定的。

3. 在“受监控的日志”列表中单击“添加”。

   将打开代理的“添加日志文件监控器”对话框。

4. 根据需要，配置日志文件监控器设置。尤其要注意以下必需设置和可选设置：

   日志文件名

   标识受监控的日志文件。

正则表达式

标识要在日志文件中解析的文本模式。

注意：有关定义正则表达式的详细信息，请参阅《*事件配置用户指南*》。

说明

向其他用户指出监控器的作用。

发现匹配时发送陷阱/发送陷阱

指定在正则表达式检测到匹配文本模式时，代理是否将陷阱发送到 CA Spectrum。

5. 单击“确定”。

   监控配置将添加到“受监控的日志”列表，且监控立即开始。

NSM 代理的日志文件监控器

可以在 OneClick 中为 NSM 代理设置日志文件监控和文件监控。以下定义描述了这两个监控器有何不同：

NSM 日志文件监控器

NSM 日志文件监控器监视文件内容中的特定模式。

NSM 文件监控器

NSM 文件监控器仅监视文件是否存在。

通过 NSM 代理日志文件监控，可以执行以下任务。

- 编辑和查看 NSM 代理的文件监控器
- 编辑和查看 NSM 代理的日志监控器
- 查看 NSM 代理的文件和日志监控器的状态更改

使用 OneClick 设置 NSM 代理的日志文件监控器

可以使用 OneClick 为 NSM 主机代理设置日志文件监控。

遵循这些步骤:

1. 在“内容”面板中，选择具有要监控的日志文件的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板的“信息”选项卡中，展开“系统资源”、“受监控的日志和文件”、“受监控的日志”。

   将出现“受监控的日志”列表。

3. 在“受监控的日志”列表中单击“添加”。

   此时将打开“添加日志文件监控器”对话框。

4. 根据需要，配置日志文件监控器设置。提供了以下选项：

   监控器名称

   标识此日志文件监控器的名称。

   文件名

   标识要监控的日志文件的完整路径和文件名（或带通配符的文件名）。

   正向模式

   如果在文件中找到指定的正则表达式，则将监控器置于关闭状态。

   反向模式

   如果在文件中找*不*到指定的正则表达式，则将监控器置于关闭状态。

   切换正向模式

   如果在文件中找到指定的正则表达式，则将监控器置于打开状态。仅当“状态策略”为“toggled”或“toggledEOF”时，此字段才可用。

   切换反向模式

   如果在文件中找*不*到指定的正则表达式，则将监控器置于打开状态。仅当“状态策略”为“toggled”或“toggledEOF”时，此字段才可用。

   开始

   是开始字符位置。

结束

是结束字符位置。

状态策略

定义监控器处理文件的方式。提供了以下选项：

poll

在每次轮询开始时，将监控器状态设置为打开。如果进行了匹配，则状态更改为关闭。除非它是新监控器（在这种情况下，读取整个文件），否则从上次读取位置扫描文件。

historical

发生匹配时，将监控器状态设置为关闭，且在日志文件的生存期内状态保持为关闭。因此，将重新创建日志文件。除非它是新监控器（在这种情况下，读取整个文件），否则从上次读取位置扫描文件。

startFromPreviousRead

发生匹配时，将监控器状态设置为关闭，且在您重置它之前，状态保持为关闭。从上次读取位置扫描文件。

toggled

可用于指定关闭模式，与“historical”属性一样，还可以指定打开模式（通过切换正向和反向模式属性形成），对其进行比较以将状态更改回打开。从上次读取位置扫描文件。

firstLineOnly

仅读取文件的第一行。在每次轮询开始时，将监控器状态设置为打开。如果发现匹配项，则状态更改为关闭。

pollEOF

在每次轮询开始时，将监控器状态设置为打开。如果发现匹配项，则状态更改为关闭。除非它是新监控器（在这种情况下，读取在文件结尾处开始），否则从上次读取位置扫描文件。

startFromPreviousReadEOF

发生匹配时，将监控器状态设置为关闭，且在您重置它之前，状态保持为关闭。除非它是新监控器（在这种情况下，读取在文件结尾处开始），否则从上次读取位置扫描文件。

toggledEOF

可用于指定关闭模式，与“historical”属性一样，还可以指定打开模式（通过切换正向和反向模式属性形成），对其进行比较以将状态更改回开启。除非它是新监控器（在这种情况下，读取在文件结尾处开始），否则从上次读取位置扫描文件。

rescan

如果文件长度已增加，则从开头重新扫描文件。如果文件超过 10 KB，则将监控器设置为“未知”。

监控器状态

可用于禁用监控器的状态面，而不与陷阱发送匹配。提供了以下选项：

downCritical

指示状态更改像配置的那样工作，并引发了关键报警。

doNotMonitor

指示已监控日志文件，但是状态始终为打开。

downWarning

指示状态更改像配置的那样工作，并引发了警告报警。

陷阱发送策略

定义应用于监控器状态陷阱的策略。提供了以下选项：

never

指示状态更改从不会导致发送陷阱。

once

指示仅当监控器状态更改时才发送状态更改陷阱。

perPoll

指示每次轮询时都发送状态更改陷阱，即使状态未更改，但只要自上次轮询以来发生了匹配状况就发送。

each

指示为代理发现的每个匹配项发送状态更改陷阱。对于切换属性，监控器关闭时，切换模式是查找的下一个匹配。因此，将不匹配后续的关闭模式。

匹配陷阱策略

定义应用于匹配陷阱的策略。提供了以下选项：

send

为找到的每个匹配项发送陷阱。对于切换属性，监控器关闭时，切换模式是查找的下一个匹配。因此，除非关闭了状态监控，否则将不匹配后续的关闭模式。

doNotSend

不为找到的每个匹配项发送陷阱。

历史记录策略

定义是否在历史记录表中存储陷阱详细信息。提供了以下选项：

generateHistory

指示在历史记录表中记录状态陷阱。

noGenerateHistory

指示在历史记录表中不记录状态陷阱。

5. 单击“确定”。

   监控配置将添加到“受监控的日志”列表。监控立即开始。

使用 OneClick 为 NSM 代理设置文件监控器

可以使用 OneClick 为 NSM 主机代理设置文件监控。

遵循这些步骤:

1. 在“内容”面板中，选择具有要监控的文件的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板的“信息”选项卡中，展开“系统资源”、“受监控的日志和文件”、“受监控的文件”。

   将显示“受监控的文件”列表。

3. 在“受监控的文件”列表中单击“添加”。

   此时将打开“添加文件监控器”对话框。

4. 配置文件监控器设置。尤其要注意以下必需设置和可选设置：

   监控器名称

   标识文件监控器的名称。

   文件名

   标识此监控器监视的文件的名称。

   文件存在

   指示文件是否存在。

陷阱发送策略

指定 NSM 代理发送陷阱的频率。提供了以下设置：

never

从不发送陷阱。

once

仅当状态已更改时才发送陷阱。

perPoll

如果状态为关闭，则在每次轮询时都发送状态陷阱。

历史记录策略

有关“历史记录策略”设置的详细信息，请参阅使用 OneClick 为 NSM 代理设置日志文件监控器 (p. 51)。

5. 单击“确定”。

   监控配置将添加到“受监控的文件”列表，且监控立即开始。

为 SystemEDGE 主机创建日志文件监控器

可以使用 OneClick 为 SystemEDGE 主机代理设置日志文件监控。

遵循这些步骤:

1. 在“内容”面板中，选择具有要监控的日志文件的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板的“信息”选项卡中，展开“系统资源”、“受监控的日志和进程日志”、“受监控的日志”。

   将出现“受监控的日志”列表。

3. 在“受监控的日志”列表中单击“添加”。

   将打开代理的“添加日志文件监控器”对话框。

4. 根据需要，配置日志文件监控器设置：

   “日志文件名”或“目录名”

   根据“监控器类型”，标识受监控的日志文件或目录。

监控器类型

标识监控日志文件还是监控目录。

文件

指示监控日志文件。

目录

指示监控目录。也可以指定是否以递归方式监控，以及是否追踪符号链接。

说明

（可选）是指示监控器作用（例如）的简短说明。

间隔

是日志文件的连续扫描之间的间隔（以分钟为单位）。

重要级别

是用于此监控器条目的重要级别。

解析文件

是用于在日志文件中进行匹配的正则表达式（最多 256 个字符）。值必须是 ed(1) 中定义的有效字符串。

不匹配

指示在解析日志文件时是否应用逻辑 NOT 运算符。

执行操作

是一个字符串（最多 4096 个字符），指定找到匹配项后执行的命令。操作脚本必须存在于主机上。

发送参数

指示是否将默认参数发送到操作脚本或程序（如陷阱类型或说明字段）。

发送 SNMP 陷阱

指定在正则表达式检测到匹配文本模式时，代理是否将陷阱发送到 CA Spectrum。

发送未就绪陷阱

指示是否发送未就绪陷阱。

单个

发送单个未就绪陷阱。

连续

发送连续未就绪陷阱。

重新初始化条目

指示是否重新初始化条目。

出现 *x* 个连续匹配后违规

指示在出现指定数目的连续匹配之后是否发送陷阱。

日志事件

指定是否记录事件。

5. 单击“确定”。

   监控配置将添加到“受监控的日志”列表，且监控立即开始。

日志到进程的映射

CA Spectrum 可以在已解析日志文件条目引用的进程上而不是主机模型上生成事件。要配置这样的事件，请验证主机模型的进程监控规则是否引用进程。此外，将进程与包括与进程相关的条目的日志文件关联。有关进程监控规则的详细信息，请参阅进程监控 (p. 15)。

为 RFC 2790 代理和 SystemEDGE 主机指定映射

可以使用 OneClick 为 RFC 2790 代理指定日志到进程的映射。

遵循这些步骤:

1. 在“内容”面板中，选择具有要监控的日志文件的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板中，依次展开“系统资源”、“受监控的日志和进程日志”、“受监控的进程日志文件映射”。

   将出现“受监控的进程日志文件映射”列表。

3. 在“受监控的进程日志文件映射”列表中单击“添加”。

   将出现“添加日志到进程映射”对话框。

4. 输入以下数据：

   日志文件名

   是要监控的日志文件。

   进程名称

   是在进程监控规则中指定的进程。

5. 单击“确定”。

   映射将添加到“受监控的进程日志文件映射”列表。只要从日志文件解析有关进程的文本，CA Spectrum 就会在受监控的进程模型上生成事件。

NSM r11 代理的映射

可以使用 OneClick 为 NSM r11 代理指定日志到进程的映射。

注意：无法为 NSM 3.1 代理创建映射。

遵循这些步骤:

1. 在“内容”面板中，选择具有要监控的日志文件的模型。

   此主机设备的信息将出现在“组件详细信息”面板中。

2. 在“组件详细信息”面板中，依次展开“系统资源”、“受监控的日志和文件”、“受监控的进程日志文件映射”。

   将出现“受监控的进程日志文件映射”列表。

3. 在“受监控的进程日志文件映射”列表中单击“添加”。

   此时将打开“添加日志到进程映射”对话框。

4. 输入以下数据：

   日志文件名

   日志文件的名称。

   监控器名称

   进程监控器的名称。此值可能不同于在进程监控规则中为进程指定的名称。

5. 单击“确定”。

   映射将添加到“受监控的进程日志文件映射”列表。只要从日志文件解析有关进程的文本，CA Spectrum 就会在受监控的进程模型上生成事件。

管理受监控的日志和进程日志映射设置

可以使用 OneClick 编辑和删除受监控的日志和进程日志文件映射设置。

- 要编辑受监控的日志和进程日志文件映射设置，请选择要修改的配置条目，在配置条目列表上单击“编辑”，编辑条目，然后单击“确定”。

  注意：无法编辑活动的监控器条目。要编辑处于活动状态的监控器条目，请将条目的状态更改为 notInService(2) 或 notReady(3)。可以在 MIB 工具中使用 SET 命令执行此任务。

- 要删除受监控的日志和进程日志文件映射设置，请选择要删除的配置条目，在配置条目列表上单击“删除”，然后单击“确定”。

配置 CA Spectrum 以处理 Syslog 文件匹配

可以配置 CA Spectrum 以从 iAgent、SystemEDGE 和 NSM 代理处理 syslog 文件匹配。

陷阱处理概述

代理基于日志文件条目的内容生成的每个陷阱都具有 OID。此 OID 基于代理的 AlertMap 文件中的陷阱映射生成 CA Spectrum 事件 0x3e00009。此事件是在模型上断言的。

每个日志文件条目（最多 255 个字符）的匹配行和生成陷阱的日志文件名将作为陷阱信息的一部分发送。CA Spectrum 解析陷阱数据，以确定日志文件条目的原始源。源可以是 IP 地址、主机名、CA Spectrum 模型句柄或应用程序日志文件名。

处理包含 IP 地址、主机名或模型句柄的陷阱

如果 IP 地址、主机名或模型句柄已作为日志文件条目的源提取，则 CA Spectrum 可以找到与 IP 地址、主机名或模型句柄匹配的设备模型，并可以在此模型上断言事件。如果日志文件条目符合日志文件语法 (p. 48)中所述的语法，为了使在设备模型上断言的事件变得富有意义，则可以创建 ParseMap 文件以自定义事件及其内容。

注意：CA Spectrum 包含许多 ParseMap 文件。并非始终必须创建该文件。

如果未创建 ParseMap 文件，则发送到设备模型的事件与在代理的模型上断言的事件相同。

创建 ParseMap 文件

ParseMap 文件指定与传入陷阱中的信息关联的事件。此外，ParseMap 文件允许您指定将日志文件条目文本的各部分用作事件变量。可以将这些变量与事件规则一起使用以处理事件。

注意：有关事件处理和事件规则的信息，请参阅《*事件配置用户指南*》。

如“日志文件语法”中所述，日志文件条目包含以下组件：

<MessagePrefix>%<MessageHeader><Additional_Information>

通过查找其名称与日志文件条目中 *<MessageHeader>* 的文本匹配的 ParseMap 文件，CA Spectrum 识别处理陷阱的 ParseMap 文件。以下日志是日志文件条目的示例：

```
2004-2-19 11:19:14 Local7.Info 172.19.38.36 Feb 19 09:14:50
```

```
%SNMP-I-SENT_TRAP, Sending notification linkUp to 192.168.32.44
```

条目的 *<MessageHeader>* 部分是 SNMP-I-SENT_TRAP。因此，CA Spectrum 将查找名为 SNMP-I-SENT_TRAP 的 ParseMap 文件。为具有唯一 *<MessageHeader>*、配置为生成陷阱的每个日志条目创建 ParseMap 文件。

注意：许多 ParseMap 文件可供在 CA Spectrum 中使用。可以在以下目录中找到它们：*<$SPECROOT>*/SS/CsVendor/ParseMaps。

遵循这些步骤:

1. 使用任何文本编辑器创建新的文本文件。

   可以对文本文件进行编辑了。

2. 在文本文件的第一行中，为要生成的事件键入新的事件文件名。事件文件名必须以 Eventffff 开始且以 xxxx 结束，其中 x 是任何有效的十六进制数字。

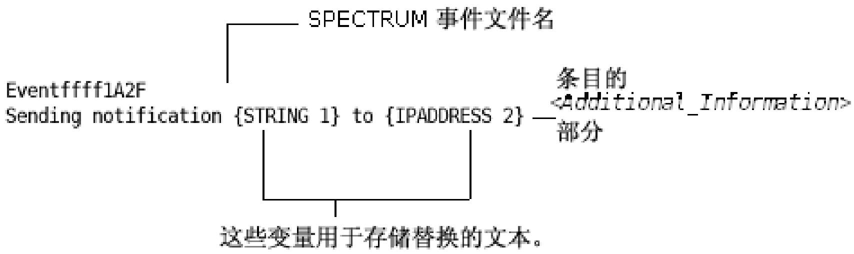
   例如，Eventffff1A2F 和 Eventffff1234 是有效的事件文件名；而 Event012za8b 则不是。

3. 在文本文件中添加换行符（按 Enter 键）。

4. 将此行用作日志文件条目的 *<Additional_Information>* 部分。可以将此文本的各部分指定为事件变量，事件变量可用于处理具有事件规则的事件。

   使用数据类型和整数指定变量。有效的数据类型有 STRING、STRINGNOWS、INTEGER 和 IPADDRESS。有关重要信息，请参阅 STRING 数据类型使用准则 (p. 62)。

下图显示了上一节所示的日志条目的有效 ParseMap 文件。变量 1 将 Uplink 存储为字符串。变量 2 将 192.168.32.44 存储为 IP 地址。



5. 在 <*$SPECROOT*>/SS/CsVendor/ParseMaps 目录中保存文本文件。此文本文件的名称必须与日志文件条目的 <*MessageHeader*> 部分匹配。在此示例中，文件名应为 SNMP-I-SENT_TRAP。

   注意：请勿在文件名中包括文件扩展名。

   仅处理 ParseMap 文件的前两行。不处理后续行上包括的信息，但是可以包括它们以供参考。

详细信息：

日志文件语法 (p. 48)

ParseMap 文件示例

以下行序列是随 CA Spectrum 提供的、名为 SYS-0-MOD_TEMPMAJORFAIL 的 ParseMap 文件的示例。可以在以下目录中找到 ParseMap 文件：<*$SPECROOT*>/SS/CsVendor/ParseMaps。

```
Event04bd1522

Module {STRING 1} major temperature threshold exceeded

%SYS-0-MOD_TEMPMAJORFAIL: Module {STRING} major temperature threshold exceeded
```

这将指示匹配的 syslog 文件：

```
Jul 28 10:56:42 [10.253.9.11.2.45] 7931: *Jul 28 10:50:47.271:
%SYS-0-MOD_TEMPMAJORFAIL: Module 100 major temperature threshold exceeded
```

这会导致在 IP 地址为 10.253.9.11 的模型上生成事件 Event04bd1522，即使代理生成了陷阱。

STRING 数据类型使用准则

本节提供有关在 ParseMap 文件中使用 STRING 数据类型的重要信息。

有效的 STRING 数据类型

如“创建 ParseMap 文件”中所述，以下数据类型是有效的，可在变量中使用。

STRING

匹配所有的字符串字符，直到下一个文本、数据类型或字符串结尾。

STRINGNOWS

匹配所有的字符串字符，直到下一个空格、文本、数据类型或字符串结尾。

INTEGER

匹配任何正整数值。

IPADDRESS

匹配任何有效的 IPv4 地址。

STRING 变量中的空格

由于空格在 STRING 变量的定义中是有效的字符，请始终以可识别的模式分隔多个 STRING 标记。

例如，以下 ParseMap 是*有效的*条目：

```
{STRING 1}, {STRING 2}
```

```
{STRING 1} {IPADDRESS 2} {STRING 3}
```

```
{STRING 1} 文字文本 {STRING 2}
```

```
{STRINGNOWS 1} {STRING 2}
```

但是，请勿包含以下条目，因为生成的正则表达式变得不明确：

```
{STRING 1}{STRING 2}
```

```
{STRING 2} {STRING 2}
```

创建事件格式文件

在 ParseMap 文件中指定的每个事件代码都必须具有单独的事件格式文件。断言事件时，事件格式文件的文本将出现在事件日志中。创建事件格式文件时，请牢记警报负责人接收的有关事件的大多数信息来自事件消息文本。

使用文本编辑器创建事件格式文件，并将该文件放置在以下目录中：<*$SPECROOT*>/SG-Support/CsEvFormat。必须将事件格式文件命名为 Event<*xxxxxxxx*>，其中 <*xxxxxxxx*> 是在 ParseMap 文件中为事件提供的事件代码。例如，如果具有事件代码为 0xffff1A2F 的事件，则 CA Spectrum 使用名为 Eventffff1A2F 的事件格式文件。

要使事件消息的文本变得富有意义，可以使用在事件的 ParseMap 文件中分配的变量和可用于所有事件格式文件的内置变量。

注意：有关创建事件格式文件的完整说明（包括可用的内置变量），请参阅《*事件配置用户指南*》。

示例：事件格式文件

将以下事件格式文件用于 ParseMap 文件生成的事件。

使用数据类型 O（八位字节）和从 ParseMap 文件分配的变量 1，插入了 IP 地址变量。使用数据类型 s（字符串）和从 ParseMap 文件分配的变量 2，插入了设备名称变量。内置变量 {d "%w- %d %m-, %Y - %T"}、{m}、{t} 和 {e} 显示事件的日期、模型名称、模型类型名称和事件 ID。

```
{d "%w- %d %m-, %Y - %T"} A device {m} of type {t} has reported a problem.

Its ip address is {S 1} and the device name is {S 2}. - (event [{e}])
```

基于事件生成警报

可以指定对在 ParseMap 文件中创建的事件进行进一步处理。可以基于事件生成警报，也可以将事件用作事件规则的一部分。为此，请确定可以在其上断言此事件并可以在每种模型类型的 EventDisp 文件中指定相应的事件处理的所有模型类型。如果希望处理事件的方式对每种模型类型都是相同的，则可以在全局 EventDisp 文件中指定事件处理。

如果已指定基于事件创建警报，请创建一个可能原因文件，断言警报时将在 OneClick 控制台中显示该文件。

注意：有关 EventDisp 和可能原因文件的详细信息，请参阅《*事件配置用户指南*》。

将更改应用于 SpectroSERVER

要激活新的或已更新的事件格式和 ParseMap 文件，请将更改应用于 SpectroSERVER。使用在事件配置编辑器中找到的“更新”命令，使用命令行界面，或者通过先停止再重新启动 SpectroSERVER，可以完成此操作。有关其中每种方法的详细信息，请参阅《*事件配置用户指南*》。

为代理模型启用事件转发

可以配置代理的模型以将事件转发到远程格局上的模型。将模型的 SBG_AlertForwardingEnabled (0x3dc000c) 属性设置为 TRUE。

第 6 章： 应用程序监控

SystemEDGE Application Insight Module (AIM)

SystemEDGE 代理提供了插件体系结构，通过该体系结构它可以在初始化时加载 Application Insight Module (AIM)。这些 AIM 提供了可扩展的灵活方法，以支持应用程序特定的语义知识。

CA Spectrum 支持以下 AIM：

- Apache Web 服务器
- Microsoft IIS
- 用于 DB2、Oracle、SQL Server 和 Sybase 的 CA Insight DPM

注意：SystemEDGE AIM 可从选定 SystemEDGE 代理的“组件详细信息”面板中的“信息”选项卡进行访问。

此外，CA Spectrum 报告由 Insight AIM 通过陷阱发送的警报。每个 Insight AIM 发出对其类型唯一的陷阱，这样就可以区分 Insight AIM 代理类型。详细的每警报信息还包括数据库名称、警报类型和警报说明。

Insight AIM 警报类型随代理类型的不同而有所不同，并涵盖各种应通知的状况。这些 AIM 警报与 CA Spectrum 中的其他警报没有什么不同，出现在相同的表中，并提供相同的功能。

Apache Web 服务器

通过用于 Apache 的 AIM，可以监控 Apache Web 服务器的运行状况和可用性。

此模块与 SystemEDGE 代理一起使用以提供以下信息：

- 您的 Web 服务器接收到的“命中”次数。可以跟踪每日的量并设置监控点，以监视不寻常的流量水平或者拒绝服务攻击。
- Web 日志文件和 Web 服务器文件正在消耗的空间量。
- 空闲服务和活动进程。可以判定 Apache Web 服务器进程监控空闲服务的有效程度，在空闲服务数太低时看到警告，并可以监控活动进程数。
- Apache Web 服务器正在使用的系统资源（CPU 和内存）的百分比。

- Web 服务器上的瓶颈是否与 CPU、内存、磁盘或网络相关。

Microsoft IIS

用于 Microsoft IIS 的 AIM 为您提供了监控 Microsoft IIS 应用程序及其系统资源使用情况所需的信息。

此模块与 SystemEDGE 代理一起使用，以允许您执行以下任务：

- 监控 Microsoft IIS 及其服务（Web、FTP、SMTP 和 NNTP）的可用性。
- 自动地重新启动失败的任何服务。
- 确定 Microsoft IIS 是否开始消耗重要级别的系统资源，包括中央处理单元 (CPU) 使用率、磁盘空间和内存。
- 跨 Web、FTP、SMTP 和 NNTP 服务监控安全性、系统和应用程序事件的日志。
- 跨 Active Server Pages (ASP)、通用网关接口 (CGI) 和 Internet 服务器应用程序接口 (ISAPI) 应用程序扩展页面检测错误统计信息，其中包括 Web 404（找不到页面）错误和 ASP 脚本错误。

CA Insight DPM

Insight AIM 提供有关 DBMS 类型的性能、配置、可用性和运行状况的重要信息，用于实时管理以及长期趋势分析和容量规划。

Insight AIM 实现了管理信息库 (MIB)，该库包括特定于每种支持的 DBMS 类型的变量。支持以下 DBMS 类型：

- DB2
- Oracle
- SQL Server
- Sybase

第 7 章： CA Unicenter NSM 代理

此部分包含以下主题：

CA Unicenter NSM 代理简介

CA Spectrum 管理模块 SM-CAI1000 在 CA Spectrum 中提供了对从 OneClick 界面管理 CA Unicenter NSM 代理的支持。此管理模块为 NSM 代理的 CA Unicenter r11 和 3.1 版本提供了以下 CA Spectrum 功能：

- CA Spectrum 为 NSM 代理主机提供了独特的设备模型类型。通过此支持，可以在 CA Spectrum 中管理 NSM 代理及其主机设备。
- OneClick 界面显示由 NSM 代理收集的系统信息，并允许您在 NSM 代理主机上配置进程、日志文件和文件监控。

  注意：进程监控器是 CA Spectrum 中的模型，因此可以为监控器模型设置警报状况，通过 CA Spectrum Report Manager 应用程序生成有关监控器模型事件和警报的报告，并将监控器模型并入 CA Spectrum 服务水平协议管理配置。

  有关 NSM 代理的进程监控功能的详细信息，请参阅进程监控 (p. 15)。

  有关 NSM 代理的日志文件和文件监控功能的详细信息，请参阅为 NSM 代理创建日志文件监控器 (p. 50)。

- CA Spectrum 在接收到 NSM 代理陷阱时生成事件和警报。
- CA Spectrum 提供对 NSM 代理主机设备的专有界面的了解。
- CA Spectrum 从 OneClick 内提供 CA Unicenter Web 管理界面（如代理显示板）的启动点。

NSM 代理支持

CA Spectrum 管理模块 SM-CAI1000 支持下表中列出的 CA Unicenter NSM r11 和 NSM 3.1 系统代理：

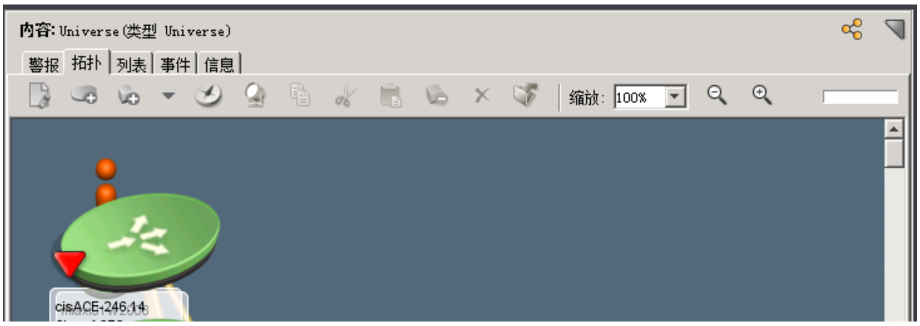
NSM r11 系统代理	NSM 3.1 系统代理
UNIX 系统代理 (caiUxsA2)	UNIX 系统代理 (caiUxOs)
Windows 系统代理 (caiWinA3)	Windows 系统代理 (caiW2kOs)
Active Directory 服务代理 (caiAdsA2)	Active Directory 服务代理 (caiAdsA2)
日志代理 (caiLogA2)	日志代理 (caiLogA2)
性能代理 (hpxAgent)	性能代理 (hpxAgent)

下表按支持的 NSM 代理和 Unicenter 版本以及 CA Spectrum 模型类型提供更详细的信息。

注意：UNIX 模型类型 (Host_NSMSysUnix) 也可用于对 Solaris 和 Linux 代理进行建模。

Unicenter 版本和代理平台	说明	CA Spectrum 模型类型
UNIX 系统代理 (caiUxsA2)	为 NSM r11 提供 Unix、Solaris 和 Linux 代理支持	Host_NSMSysUnix
Windows 系统代理 (caiWinA3)	为 NSM r11 提供 Windows 代理支持	Host_NSMSysWin
UNIX 系统代理 (caiUxOs)	为 NSM 3.1 提供 Unix 代理支持	Host_NSMv3SysUnix
Windows 系统代理 (caiW2kOs)	为 NSM 3.1 提供 Windows 代理支持	Host_NSMv3SysWin

下图显示了 OneClick“拓扑”选项卡中已建模 NSM 代理主机的示例：



NSM MIB 支持

CA Spectrum 通过 CA Unicenter NSM 代理管理模块支持 CA 专有的 Unicenter NSM MIB。有关详细的 NSM 代理 MIB 信息，请参阅《CA Unicenter 网络和系统管理 MIB 参考》文档。

NSM MIB：

- caiUxsA2
- caiWinA3
- caiLogA2
- caiAdsA2
- hpxAgent
- caiUxOs
- caiW2kOs

在 CA Spectrum 中对 NSM 代理进行建模

使用 CA Spectrum 发现可以自动地对 NSM 代理进行发现和建模，也可以手动对其进行建模。在 CA Spectrum 中对 NSM 代理进行建模时，请考虑以下因素：

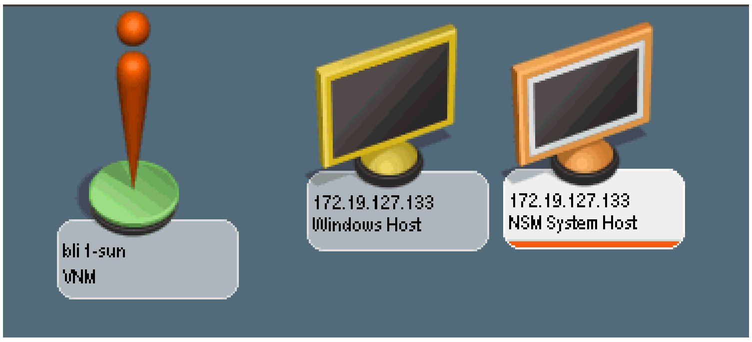
- 运行其他 SNMP 代理的 NSM 代理主机
- 用于访问 NSM Web 门户的建模注意事项

注意：有关建模的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

运行其他 SNMP 代理的 NSM 代理主机

在 CA Spectrum 中对 NSM 代理进行建模和管理时，请注意在主机设备上运行的其他代理在发现期间也可以由 CA Spectrum 发现和建模。因为默认情况下 NSM 代理使用 UDP 端口 6665 进行 SNMP 通信，而不是使用标准的 SNMP 端口 161。

例如，如果 Windows 工作站正在运行绑定到端口 6665 的 NSM 代理和绑定到端口 161 的 Microsoft SNMP 代理，则 CA Spectrum 将为设备创建两个模型，即 NSM 系统主机设备模型和 Windows 主机设备模型，如下图所示：



此情形可能由于以下原因而导致性能不佳：

- CA Spectrum 中存在不必要的重复模型。
- 可降低网络和 CA Spectrum 性能的冗余 SNMP 通信和轮询。
- 由于多个管理代理提供性能数据而导致代理主机计算机的性能降低。

要避免此情形，请执行以下操作：

- 在发现和建模之前，除了要用来管理系统的管理代理外，停止并删除所有的管理代理。此清理可避免在 CA Spectrum 中为同一主机创建和管理多个模型。
- 如果必须在给定的主机系统上运行多个代理，请考虑仅对要通过 CA Spectrum 管理的代理手动建模。

用于访问 NSM Web 门户的建模注意事项

为了可以访问 NSM Web 门户和 OneClick 中的报告启动点，必须首先使用名称服务而不是 IP 地址，在 CA Spectrum 中对 NSM 代理进行建模。

注意：有关在 OneClick 中对设备进行建模的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

只要在 CA Spectrum 中已按 IP 而不是按名称服务对 NSM 代理主机进行建模，就可以删除模型，配置 CA Spectrum 模型命名，然后对代理手动重新建模。

对代理手动重新建模

1. 在“拓扑”选项卡中右键单击带 IP 名称的 NSM 代理设备模型，然后单击“删除”。

   模型将从 CA Spectrum 中删除。

2. 在“拓扑”视图中右键单击“VNM”图标，然后单击“组件详细信息”。

   “组件详细信息”窗口将在 VNM 的上下文中打开。

3. 在 VNM 的“组件详细信息”窗口的“信息”选项卡中，展开“SpectroSERVER 控制”子视图。

4. 单击“设置顺序”以更改 VNM 上的模型命名顺序。

   此时将打开“设置顺序”对话框。

5. 选择“名称服务”，并使用向上箭头按钮将它移动到列表的顶部，然后单击“确定”。

   “设置顺序”对话框将关闭。

6. 在 OneClick 拓扑视图中，使用“按 IP 新建模型”按钮对 NSM 代理主机重新建模。

   将用设备的名称服务命名新的 NSM 代理模型。

CA Spectrum 中的 NSM 代理接口支持

NSM 代理不支持标准 MIB-II 接口表，而是使用在相关 CA MIB 中定义的专有接口表。由于此行为，NSM 代理管理模块旨在提供基于专有 NSM 接口表的接口支持。下表提供了 MIB-2 属性和对应的专有 NSM MIB 对象之间的关联。

MIB-2 属性	NSM r11 Windows 操作系统代理 (caiWinA3) 属性	NSM 3.1 Windows 操作系统代理 (caiW2kOs) 属性	NSM r11 Unix 操作系统代理 (caiUxsA2) 属性	NSM 3.1 Unix 操作系统代理 (caiUxOs) 属性
ifIndex	winEHIfIndex	w2kEHIfIndex	uxsEHIfIndex	ux3EHIfIndex
ifType	winEHIfType	w2kEHIfType	uxsEHIfType	ux3EHIfType
ifSpeed	winEHIfSpeed	w2kEHIfSpeed	uxsEHIfSpeed	ux3EHIfSpeed
ifPhysAddress	winEHIfPhysAddress	w2kEHIfPhysAddress	uxsEHIfPhysAddres	ux3EHIfPhysAddress
ifDescr	winEHIfDescr	w2kEHIfDescr	uxsEHIfDescr	ux3EHIfDescr
IpAdEntAddr	winEHIfIpAdEntAddr	w2kEHIfIpAdEntAddr	uxsEHIfIpAdEntAddr	ux3EHIfIpAdEntAddr

MIB-2 属性	NSM r11 Windows 操作系统代理 (caiWinA3) 属性	NSM 3.1 Windows 操作系统代理 (caiW2kOs) 属性	NSM r11 Unix 操作系统代理 (caiUxsA2) 属性	NSM 3.1 Unix 操作系统代理 (caiUxOs) 属性
ifAdminStatus	winEHIfAdminStatus	w2kEHIfAdminStatus	uxsEHIfAdminStatus	ux3EHIfAdminStatus
ifOperStatus	ifOperStatus	w2kEHIfOperStatus	uxsEHIfOperStatus	ux3EHIfOperStatus
ifLastChange	winEHIfLastChange	w2kEHIfLastChange	uxsEHIfLastChange	ux3EHIfLastChange

查看 NSM 代理信息

通过 CA Spectrum OneClick 可以查看 NSM 系统代理收集的信息。可以在“系统资源”子视图部分中配置进程、日志文件和文件监控。其他视图提供通过专有 MIB 值提供的只读信息。

可以在 OneClick 中访问 NSM 代理信息。此过程假定已通过发现功能或者通过手动建模，对网络中的 NSM 代理进行了建模。

遵循这些步骤:

1. 在“拓扑”选项卡中，选择已建模的 NSM 代理设备的图标。

   “组件详细信息”面板将显示选定 NSM 代理模型的“信息”选项卡。

2. 展开“系统资源”子视图。

   将显示 NSM 代理特定的信息。

详细信息：

在 CA Spectrum 中对 NSM 代理进行建模 (p. 69)

NSM 代理显示板和性能报告

CA Unicenter NSM 代理管理模块为 NSM 代理显示板和性能报告提供了 OneClick 启动点。使用从 OneClick 管理页面可用的 NSM 配置实用工具，可以配置启动点。

注意：为了访问启动点，需要在 CA Spectrum 中按设备名称而不是 IP 地址对 NSM 代理进行建模。

OneClick 中的 NSM 启动点包括：

- NSM 代理显示板
- NSM 性能报告

配置 CA Spectrum 以启动 NSM 用户界面

为了让 Unicenter NSM 显示板和报告服务器从 CA Spectrum 中根据上下文启动，请在 OneClick Web 服务器上配置适用于您的环境的值。在 OneClick 管理页面中使用“NSM 配置”页面来配置值。

CA Spectrum 将配置值保存到默认 <*安装区域*>/tomcat/webapps/spectrum/WEB-INF/topo/config/nsm-system-config.xml 文件的自定义版本中（位于 <*安装区域*>/custom/topo/config/ 目录）。升级时不覆盖此目录，因此将保留您的 NSM 配置值。

可以配置用于启动 Unicenter NSM 显示板的自定义值。

遵循这些步骤:

1. 在 OneClick 主页中单击“管理”。

   将打开“管理”页面。

2. 单击左侧面板中的“NSM 配置”。

   将打开“NSM 配置”窗口。

3. 根据需要完成以下字段：

   NSM 显示板服务器名称

   标识 NSM 显示板服务器 (server.domain.extension)。

   NSM 显示板服务器端口

   默认值为 9090。

   NSM 报告服务器

   标识 NSM 报告服务器 (server.domain.extension)。

   NSM 报告端口

   默认值为 9090。

4. 单击“保存”。
5. 重新启动所有正在运行的 OneClick 客户端，以使更改生效。

   自定义值就配置好了。

启动代理显示板

要启动代理显示板，请在 OneClick“拓扑”视图中右键单击 NSM 代理设备模型，然后选择要启动的 NSM 代理显示板。

将打开 Unicenter 显示板 Web 界面。

启动性能报告

OneClick 为每种 NSM 模型类型提供了性能报告菜单选择。通过右键单击 NSM 设备模型，可访问性能报告菜单选择。此菜单选择将启动基于 Unicenter WRS 的系统性能报告。

为了从 OneClick 启动 NSM 性能报告，必须满足以下所有条件：

- 必须在 NSM 代理主机上安装了 hpxAgent。
- 要求与之连接的 WRS 必须已安装系统性能报告。
- WRS 还需要为给定主机服务器提供数据的连接。
- 必须按配置 CA Spectrum OneClick 以启动 NSM 用户界面 (p. 73)中所述对 OneClick 进行配置。

要启动报告 Web 界面，请右键单击表示 NSM 主机的 NSM 代理设备模型，然后单击“NSM 性能报告”。

将打开 Unicenter Web 报告服务器界面。

Trap-to-Alarm 映射

CA Unicenter NSM 代理管理模块将 NSM 代理陷阱集成到 CA Spectrum 事件和警报处理中。

CA Spectrum 处理由 NSM 代理（包括系统和性能代理）发送的陷阱。对于接收到的状态为“警告”或“关键”的每个 NSM 系统或性能代理陷阱，CA Spectrum 将生成警报，如下表所示。CA Spectrum 接收到相关的“正常”陷阱时，CA Spectrum 将清除对应的警报。

CA Spectrum 接收到的 NSM 陷阱	生成的 CA Spectrum 警报
警告陷阱	次要警报
关键陷阱	主要警报

陷阱处理基于 NSM 代理模型类型。每种模型类型为多个代理处理陷阱，如下表所述。

模型类型	代表这些代理处理陷阱
Host_NSMSysUnix	caiUxsA2 caiLogA2 hpxAgent
Host_NSMSysWin	caiWinA3 caiLogA2 caiAdsA2 hpxAgent
Host_NSMv3SysUnix	caiUxOs caiLogA2 hpxAgent
Host_NSMv3SysWin	caiW2kOs caiLogA2 caiAdsA2 hpxAgent

事件代码和可能原因文件 ID 范围

下表列出了 NSM 代理 MIB 的事件代码和可能原因文件 ID。

NSM 代理 MIB	关联的 CA Spectrum 事件代码和可能原因文件的范围
caiUxsA2	Event04ef0000 - Event04ef00e9 Prob04ef0002 - Prob04ef00e3
caiWinA3	Event04ef1000 - Event04ef10c7 Prob04ef1002 - Event04ef10c1
caiLogA2	Event04ef2000 - Event04ef2010 Prob04ef2002 - Prob04ef200e
caiAdsA2	Event04ef3000 - Event04ef3042 Prob04ef3002 - Prob04ef303e
hpxAgent	Event04ef4000 - Event04ef4008 Prob04ef4002 - Prob04ef4006
caiUxOs	Event04ef5000 - Event04ef5069 Prob04ef5002 - Prob04ef5067
caiW2kOs	Event04ef6000 - Event04ef6099 Prob04ef6002 - Prob04ef6095

CA Spectrum 中的 NSM 系统代理状态

为了使 NSM 代理模型的状态保持最新，CA Spectrum 按照设备轮询时间间隔定期轮询两个 NSM 系统代理 MIB 属性。默认情况下，间隔为 5 分钟（300 秒）。

注意：有关更改轮询时间间隔的信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

被轮询的属性指示给定 NSM 系统代理主机上警告或关键资源的数目。一个属性表示 NSM 系统代理的资源警告总数，另一个属性表示处于关键状况的资源总数。如果给定 NSM 系统代理的警告或关键资源数大于零，则 CA Spectrum 创建相应的警报。属性的值为零时，将清除此警报。下表显示了每种支持的模型类型的被轮询属性以及生成的警报。

模型类型	被轮询的属性	资源警告总数大于零时生成的事件/次要警报 ID	关键资源总值大于零时生成的事件/主要警报 ID
Host_NSMSysUnix	uxsA2StatusGeneralTotalWarn uxsA2StatusGeneralTotalCrit	0x04ef00ea	0x04ef00ec
Host_NSMSysWin	winA3StatusGeneralTotalWarn winA3StatusGeneralTotalCrit	0x04ef10c8	0x04ef10ca
Host_NSMv3SysUnix	uxsStatusGeneral TotalWarning uxsStatusGeneral TotalCritical	0x04ef506a	0x04ef506c
Host_NSMv3SysWin	w2kStatusGeneral TotalWarn w2kStatusGeneral TotalCrit	0x04ef609a	0x04ef609c

注意：轮询时资源警告总数或关键资源总数分别为零时，将清除这些警报。

附录 A： 系统及应用程序监控权限

本节列出了与 OneClick 用户的系统及应用程序监控相关的权限。

注意：有关配置权限的详细信息，请参阅《*管理员指南*》。

系统及应用程序监控

控制对系统及应用程序监控权限的访问。取消选择此权限将自动取消选择以下权限：

管理规则集

允许用户创建监控规则集。

监控文件系统

允许用户创建文件系统监控规则。

监控进程

允许用户创建进程监控规则。