

CA Spectrum®

Alarm Notification Manager 用户指南

版本 9.3



本文档包括内嵌帮助系统和以电子形式分发的材料（以下简称“文档”），其仅供参考，CA 随时可对其进行更改或撤销。

未经 CA 事先书面同意，不得擅自复制、转让、翻印、透露、修改或转录本文档的全部或部分內容。本文档属于 CA 的机密和专有信息，不得擅自透露，或除以下协议中所允许的用途，不得用于其他任何用途：(i) 您与 CA 之间关于使用与本文档相关的 CA 软件的单独协议；或者 (ii) 您与 CA 之间单独的保密协议。

尽管有上述规定，但如果您为本文档中所指的软件产品的授权用户，则您可打印或提供合理数量的本文档副本，供您及您的雇员内部用于与该软件相关的用途，前提是所有 CA 版权声明和标识必须附在每一份副本上。

打印或提供本文档副本的权利仅限于此类软件所适用的许可协议的有效期限内。如果该许可因任何原因而终止，您应负责向 CA 书面证明已将本文档的所有副本和部分副本已退还给 CA 或被销毁。

在所适用的法律允许的范围内，CA 按照“现状”提供本文档，不附带任何保证，包括但不限于商品适销性、适用于特定目的或不侵权的默示保证。CA 在任何情况下对您或其他第三方由于使用本文档所造成的直接或间接的损失或损害都不负任何责任，包括但不限于利润损失、投资受损、业务中断、信誉损失或数据丢失，即使 CA 已经被提前明确告知这种损失或损害的可能性。

本文档中涉及的任何软件产品的使用均应遵照有关许可协议的规定且根据本声明中的条款不得以任何方式修改此许可协议。

本文档由 CA 制作。

仅提供“有限权利”。美国政府使用、复制或透露本系统受 FAR Sections 12.212、52.227-14 和 52.227-19(c)(1) - (2) 以及 DFARS Section 252.227-7014(b)(3) 的相关条款或其后续条款的限制。

版权所有 © 2013 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

CA Spectrum®

CA Spectrum® Alarm Notification Manager (SANM)

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	7
关于 SANM.....	7
CA Spectrum 如何监控警报.....	7
AlarmNotifier.....	8
Attention!.....	9
警报资源文件.....	9
第 2 章：创建和编辑警报通知策略	11
创建警报通知策略.....	11
为策略定义筛选.....	12
将筛选添加到现有策略中.....	14
更改筛选顺序.....	15
编辑筛选.....	16
添加筛选参数.....	16
删除筛选.....	17
向策略添加模型或警报.....	17
编辑警报通知策略.....	18
第 3 章：将策略与应用程序相关联	19
关联过程.....	19
SANM 默认策略.....	19
将策略与应用程序相关联.....	20
“排定”子视图.....	20
排定关联.....	21
其他实用工具.....	21
assigticket 实用工具.....	21
clearticket 实用工具.....	22
updatealarm 实用工具.....	22
第 4 章：监控 SANM 进程	25
SANM 事件.....	25
SANM 事件代码.....	25
跟踪策略.....	26
摘要跟踪文件.....	26
详细跟踪文件.....	27

第 5 章： SANM 和 AlarmNotifier 29

AlarmNotifier 增强功能.....	29
启动 AlarmNotifier.....	29
访问警报管理参数.....	31
确认始发事件数据已保存.....	32
警报确认.....	32
用户可清除警报.....	33
启用 SANM 的脚本参数.....	33
电子邮件通知.....	34
第三方应用程序.....	35
启用 SANM 的 .alarmrc 参数.....	37

第 6 章： 在分布式 SpectroSERVER 环境中使用 SANM 41

格局和警报监控.....	41
跨多个格局的 SANM 策略管理.....	41
如何在单个格局中创建 SANM 策略.....	42
如何在多个格局中创建 SANM 策略.....	42
确定受监控格局的方法.....	43

第 1 章：简介

此部分包含以下主题：

[关于 SANM](#) (p. 7)

[CA Spectrum 如何监控警报](#) (p. 7)

[警报资源文件](#) (p. 9)

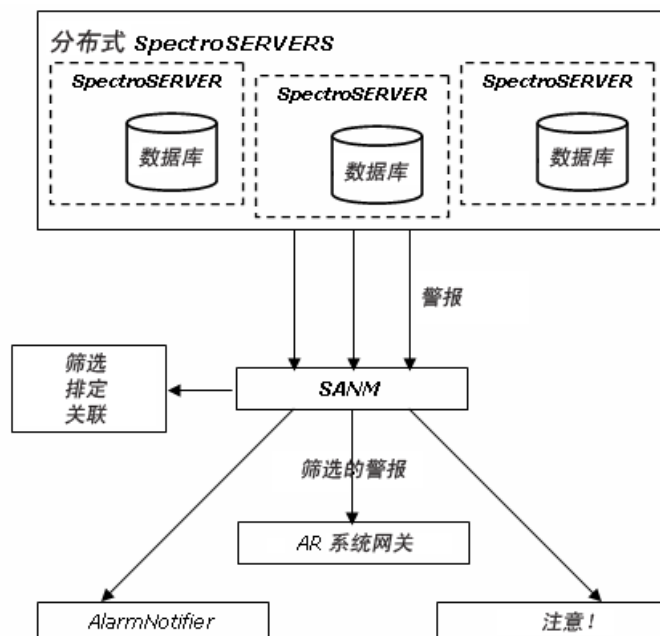
关于 SANM

CA Spectrum Alarm Notification Manager (SANM) 是 CA Spectrum 组件，该组件可以增强 CA Spectrum 警报处理应用程序的功能。CA Spectrum 可使用多个警报处理应用程序，包括 AlarmNotifier 和 Attention!。这些应用程序通过发送电子邮件通知、创建故障单等操作来响应 CA Spectrum 警报。通过 SANM，您可以创建警报通知策略，并将其与应用程序相关联。

CA Spectrum 如何监控警报

CA Spectrum、警报处理应用程序和 SANM 在警报监控过程中协同工作。

下图显示了警报监控过程：



下面的工作流说明了 CA Spectrum 监控警报的方式：

1. CA Spectrum 轮询建模的网络元素，并更新 SpectroSERVER 数据库中每个元素的状态。
2. CA Spectrum 在从网络接收到陷阱或检测到网络模型中的关键状态更改时，会生成警报。在 OneClick 控制台中，模型图标从绿色更改为指示警报重要级别的其他颜色。
 - CA Spectrum 在“组件详细信息”窗格的“警报详细信息”选项卡上为每个警报发布具体信息。
 - CA Spectrum 在“组件详细信息”面板的“事件”选项卡上发布警报事件信息。
3. 有关 CA Spectrum 已生成的警报的数据将传递给 SANM。通过 SANM，您可以创建警报通知策略，并将其与警报处理应用程序相关联。此外，通过“SANM 排定”子视图，您可以排定应用程序与策略的关联，并自动完成关联过程。
4. 仅当出现策略中指定的警报类型时，SANM 才会将警报信息传递给警报处理应用程序。

AlarmNotifier

SANM 筛选要发送给 AlarmNotifier 的警报。如果既安装了 SANM 又安装了 AlarmNotifier，AlarmNotifier 将获得以下功能：

- 可以向 AlarmNotifier 的单个实例应用 SANM 警报筛选策略。
- AlarmNotifier 可以从分布式 SpectroSERVER 环境的所有格局生成警报通知。
- 提供了额外的命令，可用于确认警报并从 AlarmNotifier 清除警报。
- 新的启动命令，可用于启动 AlarmNotifier 的多个实例。可以将每个实例与不同的 SANM 警报通知策略相关联。
- 其他的新启动命令，可用于创建摘要或详细跟踪文件。
- AlarmNotifier 脚本具有新参数，其中包含有关故障排除警报的信息。
- AlarmNotifier 资源文件具有新参数，用于获取有关警报的详细信息。
- 通过 SANM 可以在指定的时间自动将不同的策略与 AlarmNotifier 相关联。

Attention!

Attention! 是一个客户端-服务器网络监控和通知系统。**Attention!** 应用程序可提醒系统管理员注意关键的系统和网络事件。支持的报警格式包括字母数字寻呼、电话、电子邮件、PA 通告、电子留言板和自定义通知。可以将 SANM 用作 CA Spectrum 与 **Attention!** 之间集成的基础。

警报资源文件

警报资源文件 `.alarmrc` 包含定义 SANM 默认值的操作参数。可以修改这些参数来自定义 SANM 警报管理。

可以在 `<$SPECROOT>/Notifier` 目录中找到警报资源文件。有关详细信息，请参阅《*Alarm Notifier 用户指南*》。

建议您在修改文件之前，先创建文件的备份副本。

如果重新安装 CA Spectrum 或升级版本，安装会将您的资源文件 `.alarmrc` 保存到备份目录。使用其他名称保存的资源文件的版本保存在 `<$SPECROOT>/SANM` 目录中。该目录还包含重新安装或升级中包含的默认资源文件。

第 2 章： 创建和编辑警报通知策略

此部分包含以下主题：

[创建警报通知策略 \(p. 11\)](#)

[编辑筛选 \(p. 16\)](#)


[向策略添加模型或警报 \(p. 17\)](#)

创建警报通知策略

警报通知策略指定警报处理应用程序接收和筛选不需要警报的警报类型。可以创建警报通知策略，以便确定哪些应用程序接收您选择的类型的警报。

遵循这些步骤：

1. 单击 OneClick 控制台的“导航”面板中的“定位器”选项卡。

2. 在 SANM 下选择“所有应用程序”，然后单击 （启动选定的搜索）。

此时将打开“选择要搜索的格局”对话框。

3. 选择要在您的搜索中包括的格局，然后单击“确定”。

可用应用程序及其正在使用的策略显示在右侧的“内容”面板中。策略详细信息显示在“内容”面板下面的“组件详细信息”面板中。

注意：请至少运行 AlarmNotifier 一次。否则，搜索不返回模型。AlarmNotifier 文件位于 `<$$SPECROOT>/Notifier` 目录中。

4. 在“组件详细信息”面板中，单击链接以在“常规信息”下创建或设置策略。

此时将打开“选择策略”对话框。

5. 单击“创建”。

此时将打开“创建 SANM 策略”对话框。

6. 在“名称”文本框中输入策略名称。
7. （可选）创建要与新策略关联的一个或多个筛选。


注意：建议您分配指示策略使用时间的策略名称。例如，使用类似“ciscoRtrPM”这样的名称，以便您可以识别集合中的 Cisco 路由器策略。

8. 单击“确定”。
新策略即会创建。

为策略定义筛选

您可以定义警报通知策略筛选，以便细化通知策略。一个筛选必须与一个策略相关联。筛选包括的参数可按重要级别和设备类型包括或排除警报。可以在指定的格局上或在指定的拓扑中针对指定类型的警报设置筛选。

遵循这些步骤：

1. 单击 OneClick 控制台的“导航”面板中的“定位器”选项卡。
2. 在 SANM 下选择“所有应用程序”，然后单击 （启动选定的搜索）。
此时将打开“选择要搜索的格局”对话框。
3. 选择要在您的搜索中包括的格局，然后单击“确定”。
可用应用程序及其正在使用的策略显示在右侧的“内容”和“组件详细信息”面板中。
4. 在“组件详细信息”面板中，单击“常规信息”子视图中的创建/设置策略链接。
此时将打开“选择策略”对话框。
5. 单击“创建”。
此时将打开“创建 SANM 策略”对话框。
6. 单击“添加”按钮。
此时将打开“添加筛选”对话框。
7. 输入以下信息：
名称
定义新筛选名称。
说明
（可选）说明该筛选。

存在时长

(可选) 指示筛选保留警报的时间。警报会在存在时长之后传递给警报处理应用程序。

通知数据

(可选) 定义与警报通知一起发送的数据。

8. 定义筛选的参数:

- a. (可选) 选择“格局”选项卡以定义筛选的格局。要定义格局，请在“包括”和“排除”列表中选择服务器。可以通过使用提供的箭头按钮，在“包括”和“排除”列表之间移动服务器。

注意：OneClick 将旧 SANM UI 的格局和服务器参数组合为格局这一个参数。

- b. (可选) 选择“重要级别”选项卡以定义要包括或排除的警报重要级别。要定义重要级别，请从“包括”和“排除”列表中选择警报重要级别。

- c. (可选) 选择“设备类型”选项卡以指定筛选的设备类型，如下所示：

- 选择一个选项，以查看要包括或排除的设备类型的列表。
- 输入设备类型，然后单击“添加”以将其添加到包括或排除列表中。

注意：输入现有设备类型的名称，或者计划创建的设备类型的名称。

- 单击“浏览”以从现有设备类型的列表中进行选择。
- 选择设备类型，然后单击“删除”将其从列表中删除。
- 选择设备类型，然后单击“修改”以编辑该设备类型。

- d. (可选) 选择“集合”选项卡以指定筛选的策略集合。位于这些集合中的设备的警报会被筛选出来。容器的包括、排除、添加、删除、修改和浏览步骤与之前的选项卡步骤相同。

- e. (可选) 选择“拓扑”选项卡以指定筛选的拓扑容器。位于这些拓扑中的设备的警报会被筛选出来。该步骤与之前的选项卡步骤相同。

- f. (可选) 选择“警报类型”选项卡以包括或排除特定类型的警报。

- g. (可选) 选择“模型类型”选项卡以包括或排除特定类型的模型。

- h. (可选) 选择“位置”选项卡以指定筛选的位置容器。


位于这些位置中的设备的警报会被筛选出来。


- i. （可选）选择“组织”选项卡以指定筛选的组织容器。
位于这些组织中的设备的警报会被筛选出来。
 - j. （可选）选择“IP 地址/范围”选项卡以指定筛选的 Internet 协议 (IP) 地址。
SANM 仅将在指定的网络、子网或 IP 地址范围内生成的警报传递给警报处理应用程序。
 - k. （可选）选择“模型名称”选项卡以指定筛选的模型名称。
9. 单击“确定”。
- 此时即定义了新筛选。
- 注意：**如果创建具有多个参数的筛选，请创建 AND 条件。因此，要想使筛选返回任何结果，所有的参数都必须都返回 TRUE。要创建 OR 条件，请创建两个筛选，其中每个筛选都具有不同的筛选参数。
10. 在“创建 SANM 策略”对话框的“名称”字段中输入新策略的名称，然后单击“确定”。
- 注意：**建议您分配指示策略使用时间的策略名称。例如，使用类似“ciscoRtrPM”这样的名称，以便您可以识别集合中的 Cisco 路由器策略。
- 新策略即会创建。

将筛选添加到现有策略中

可以将筛选添加到现有策略中。

遵循这些步骤：

1. 单击 OneClick 控制台的“导航”面板中的“定位器”选项卡。
2. 依次选择“SANM”、“所有策略”，然后单击 （启动选定的搜索）。
此时将打开“选择要搜索的格局”对话框。
3. 选择要在您的搜索中包括的格局，然后单击“确定”。
现有策略会显示在右侧的“内容”面板中。
4. 选择要为其添加筛选的策略。
策略详细信息会显示在“组件详细信息”面板中。



5. 在“组件详细信息”面板的“信息”选项卡下，展开“筛选”菜单。
6. 单击 （打开对话框以便将筛选添加到该策略中）。
此时将打开“添加筛选”对话框。
7. 按照[定义新筛选](#) (p. 12)中所述输入筛选信息，然后保存该信息。
筛选即会添加到策略。

更改筛选顺序

可以更改与策略关联的筛选的处理顺序。

此功能仅适用于通知数据。例如，如果筛选 1 的通知数据包括 jack@xyz.com，筛选 2 的通知数据包括 jill@xyz.com，则警报通知程序将返回 jack@xyz.com:jill@xyz.com。如果更改顺序，输出将为 jill@xyz.com:jack@xyz.com。



遵循这些步骤：

1. 单击 OneClick 控制台的“导航”面板中的“定位器”选项卡。
2. 依次选择“SANM”、“所有策略”，然后单击 （启动选定的搜索）。
此时将打开“选择要搜索的格局”对话框。
3. 选择要在您的搜索中包括的格局，然后单击“确定”。
现有策略会显示在右侧的“内容”面板中。
4. 选择要更改其筛选顺序的策略。
策略详细信息显示在“内容”面板下面的“组件详细信息”面板中。
5. 在“信息”选项卡下展开“筛选”菜单，然后单击 （打开对话框以便设置通知数据顺序）。
此时将打开“设置顺序”对话框。
6. 选择筛选。
7. 使用箭头按钮在顺序中上下移动筛选，然后单击“确定”。
筛选即会根据新顺序进行处理。

编辑筛选

编辑筛选以更改筛选参数的值。可以添加、编辑和删除筛选参数。

遵循这些步骤:

1. 单击 OneClick 控制台的“导航”面板中的“定位器”选项卡。
2. 依次选择“SANM”、“所有策略”，然后单击 （启动选定的搜索）。
此时将打开“选择要搜索的格局”对话框。
3. 选择要在您的搜索中包括的格局，然后单击“确定”。
现有策略会显示在“内容”面板中。
4. 在筛选表中选择筛选，然后单击 （打开对话框以便编辑选定的筛选）。
将打开筛选以进行编辑。
5. 根据需要编辑“名称”、“说明”、“存在时长”、“通知数据”字段。
6. 单击每个参数选项卡以添加、编辑和删除相应的参数值，如[定义新筛选](#) (p. 12)所述。
注意：如果删除参数的所有值，则筛选将不再包括该参数。
7. 如果要仅查看筛选中包括的参数，请选中“仅显示筛选参数”复选框。
8. 单击“确定”。
至此便编辑了筛选。

添加筛选参数

可以向筛选添加参数以提高筛选级别。

注意：可以通过向参数添加值来向筛选添加参数。也就是说，如果某参数在您创建筛选时未包括，则定义该参数的值会将该参数添加到筛选。

遵循这些步骤:

1. 打开筛选以进行[编辑](#) (p. 16)。
2. 单击要添加到筛选的参数的选项卡。
3. 向参数添加一个或多个值，如[定义新筛选](#) (p. 12)所述。
4. 单击“确定”。

该参数即会添加到筛选。

删除筛选

可以删除不再需要的筛选。

要删除筛选，请在筛选表中选择筛选，然后单击 **X** (永久删除所选项目)。

该筛选即会删除。

向策略添加模型或警报

可以向策略添加模型或警报。

遵循这些步骤:

1. 单击 OneClick 控制台的“导航”面板中的“资源管理器”选项卡。
模型或警报详细信息会显示在右侧的“内容”面板中。
2. 右键单击模型或警报，然后依次选择“添加到”、“SANM 策略”、“添加”。

此时将打开“选择策略”对话框。

3. 选择策略，然后单击“确定”。

此时将打开“选择写入选项”对话框。

注意: 要删除项，请选择“删除”。

4. 选择一个选项。

模型或警报即会添加到选定的策略。

编辑警报通知策略

不管策略是否与应用程序关联，都可以在保存策略之前或者之后对其进行编辑。如果策略与应用程序关联，则只要保存更改，SANM 就会开始实施新策略。

重要说明！ 要想使修改的策略立刻生效，Archive Manager 必须在运行并且连接到 SpectroSERVER。

第 3 章： 将策略与应用程序相关联

此部分包含以下主题：

[关联过程](#) (p. 19)

[“排定”子视图](#) (p. 20)

[其他实用工具](#) (p. 21)

关联过程

在创建警报通知策略之后，需将策略与一个或多个警报处理应用程序相关联。策略和应用程序之间的关联将始终有效，直到您将其他策略与该应用程序关联或者删除关联的策略。

SANM 会实施一个规则，即应用程序一次只能有一个关联的策略。要使应用程序可以在不同的时间处理不同的警报，请在运行时手动将策略与应用程序相关联。或者使用“排定”子视图在指定的日期和时间自动排定关联。要使用不同的策略运行同一个应用程序，请启动该应用程序的多个实例，其中每个实例都具有唯一名称。然后将不同的策略与应用程序实例相关联。

要更改与应用程序关联的策略，请将策略（如默认策略）与该应用程序相关联。如果您删除关联的策略，SANM 会将默认策略与应用程序相关联。编辑一个与多个警报处理应用程序关联的策略会更改所有应用程序的策略。不需要将策略与每个应用程序重新关联。

SANM 默认策略

在首次启动应用程序或者删除与应用程序关联的策略时，SANM 会将默认策略与每个应用程序相关联。也可以显式将默认策略与应用程序相关联。

默认策略是空策略；它不会筛选警报。也就是说，与默认策略关联的应用程序将接收在 SANM 连接到的 SpectroSERVER 的格局映射的每个格局中出现的所有警报通知。

可以修改默认策略以添加筛选，但是在默认情况下，SANM 会继续将其与应用程序相关联。


如果删除与应用程序关联的策略，SANM 会将默认策略与该应用程序相关联。因此，在删除策略之前，请先检查是否已修改默认策略。如果删除与应用程序关联的策略，或者修改默认策略，则 SANM 会显示一条警告。

在删除关联的策略时，可以避免关联与应用程序关联的默认策略。首先将其他策略与应用程序相关联。当前策略会自动删除。

将策略与应用程序相关联

在 OneClick 中可以将策略与应用程序相关联。

遵循这些步骤:

1. 单击 OneClick 控制台的“导航”面板中的“定位器”选项卡。
2. 依次选择“SANM”、“所有应用程序”，然后单击 （启动选定的搜索）。
此时将打开“选择要搜索的格局”对话框。
3. 选择要在您的搜索中包括的格局，然后单击“确定”。
现有应用程序会显示在右侧的“内容”面板中。
4. 单击“创建/设置策略”链接。
此时将打开“选择策略”对话框。
5. 选择策略，然后单击“确定”。
策略即会与应用程序关联。

“排定”子视图

“排定”子视图会自动完成关联过程，并允许您根据排定实施警报通知策略。例如，如果希望某个警报应用程序采取措施，以在晚间响应警报，可以创建一个特殊的夜间策略，并排定每天下午 6 点将此策略与应用程序关联。然后，可以排定每天上午 7 点将另一个白天策略与同一个应用程序关联。通过“排定”子视图，您可以执行排定的关联。每次要更改警报筛选时，可以避免手动关联新策略。

可以在 OneClick 的“事件”选项卡上验证“排定”子视图执行的操作结果。

排定关联

在 OneClick 中可以排定策略与应用程序的关联。

遵循这些步骤:

1. 单击 OneClick 控制台的“导航”面板中的“定位器”选项卡。
2. 依次选择“SANM”、“所有应用程序”，然后单击 （启动选定的搜索）。
此时将打开“选择要搜索的格局”对话框。
3. 选择要在您的搜索中包括的格局，然后单击“确定”。
现有应用程序会显示在右侧的“内容”面板中。
4. 选择要排定其策略的 SANM 应用程序。
5. 在“组件详细信息”面板中，展开“信息”选项卡下的“已排定策略”菜单，然后单击 （打开对话框以便将策略排定为当前策略）。
此时将打开“选择策略并排定”对话框。
6. 选择一个策略，再选择排定，然后单击“确定”。

注意：可以通过单击“创建”按钮创建自定义策略和排定。

已排定策略会显示在“已排定策略”表中。

其他实用工具

AlarmNotifier 包括三个可用于管理现有警报的实用工具：

- assigticket
- clearticket
- updatealarm

assigticket 实用工具

assigticket 实用工具用于使用分配有故障单的用户名填充警报的“故障单 ID”字段。

请使用以下语法运行该实用工具：

```
assignticket modelhandle alarmid assignee [username]
```

modelhandle

指示已发出警报的模型的句柄。

alarmid

指示要向其写入的警报的 ID。

assignee

指示分配有故障单的用户名称。

username

(可选) 指定用于连接到 SpectroSERVER 的 CA Spectrum 用户帐户的名称。

clearticket 实用工具

使用 clearticket 实用工具可清除警报。

请使用以下语法运行该实用工具：

```
clearticket -mh model_handle -ai alarm_ID -su username
```

-mh *model handle*

指示警报所在的模型的句柄。

-ai *alarm_ID*

指示要清除的警报的 ID。

-su *username*

指定用于连接到 SpectroSERVER 的用户帐户的名称。

updatealarm 实用工具

使用 updatealarm 实用工具可设置任意警报的任意属性的值。

请使用以下语法运行该实用工具：

```
updatealarm modelhandle alarmid attrid attrvalue [username]
```

modelhandle

指示已发出警报的模型的句柄。

alarmid

指示要向其写入的警报的 ID。

attrid

指示要向其写入的属性的 ID。

attrvalue

指示要向属性写入的值。

username

(可选) 指定用于连接到 SpectroSERVER 的用户帐户的名称。

第 4 章： 监控 SANM 进程

此部分包含以下主题：

[SANM 事件](#) (p. 25)

[跟踪策略](#) (p. 26)

SANM 事件

OneClick 中的“事件”选项卡会列出在 SpectroSERVER 上发生的事件。用户执行 SANM 操作时，操作的结果会与其他 CA Spectrum 事件一起显示在“事件”选项卡上。将列出有关事件的下列信息：

- 操作的日期和时间
- 应用程序名称和策略名称
- 用户的主机和用户名
- 事件的说明
- 事件代码

注意：有关使用“事件”选项卡的详细信息，请参阅《*操作员指南*》。

SANM 事件代码

每个 SANM 事件代码都与一个 SANM 操作相对应。使用下列 SANM 事件代码可找到 SANM 操作条目，或者筛选出并非特定于 SANM 操作的所有条目。

00d70000

应用程序已在 SANM 中注册

00d70001

应用程序未在 SANM 中注册

00d70002

关联已创建

00d70004

排定的关联已创建

00d70006

策略已创建

00d70008

策略已修改

00d7000a

应用程序已创建

00d7000b

应用程序创建失败

跟踪策略

要收集有关策略如何为启用 SANM 的应用程序工作的信息，可以在应用程序启动时为该应用程序创建详细或摘要跟踪文件。

- **详细跟踪文件：**指示在针对策略进行评估时策略警报中不匹配的筛选。
- **摘要跟踪文件：**指示当关联的应用程序启动时警报通知传递到该应用程序的时间。摘要跟踪文件不包括有关不满足策略中指定条件的警报的信息。

将 SANM 执行的基于策略的操作的记录用作一个决策工具。该结果可以确认您对某应用程序应用了正确的策略，或者它们可能会迫使您细化策略。例如，您可能会发现，您无意中排除了应传递到应用程序的警报。

摘要跟踪文件

摘要跟踪文件包括发送给应用程序的所有警报通知（已设置、已清除、已更新）的摘要，如下所示：

```
00-5-24 15:48:44 SANM Trace Entry 1
针对格局 0x540000 上设置的警报 52 向 AlarmNotifier 发送了通知

00-5-24 15:48:44 SANM Trace Entry 2
针对格局 0x540000 上更新的警报 21 向 AlarmNotifier 发送了通知

00-5-24 15:48:44 SANM Trace Entry 3
针对格局 0x540000 上清除的警报 26 向 AlarmNotifier 发送了通知
```

摘要跟踪文件不指示不满足策略的警报。

详细跟踪文件

详细跟踪文件包括有关满足和不满足策略条件的警报的条目。警报条目包括警报属性值，这些值将与筛选参数值进行比较。位于“警报值”和“筛选值”之间的“匹配”下的箭头符号指示匹配。如果该值不匹配，箭头将不会出现。

下面是一个指示警报满足策略的跟踪文件示例：

```

AlarmNotifier Trace Entry 305

Applying first_shift to Alarm 8982 set on landscape 0x540000
Applying Filter 1, tag: Abner or Abbott

ALARM VALUES          MATCH FILTER VALUES
-----
LANDSCAPE              --> LANDSCAPE
0x540000                0x540000
                        remaining values ignored

MODEL TYPE             MODEL TYPE
Pingable                --> Pingable
                        remaining values ignored

DEVICE LOCATION        DEVICE LOCATION
World:USA:NorthEast:  --> USA

ALARM SEVERITY         ALARM SEVERITY
CRITICAL                --> MAINTENANCE
                        SUPPRESSED
                        MAJOR
                        CRITICAL
                        remaining values ignored

ALARM CAUSE            ALARM CAUSE
0x10007                 --> 0x10005
                        0x10007

SPECTROSERVER HOST     SPECTROSERVER HOST
coffee                 --> coffee
                        remaining values ignored

-----
FILTER 1 PASSED

Alarm Passed Policy

Notification sent to AlarmNotifier for Alarm 8982 set on landscape
0x540000

```

下面是一个指示警报不满足策略的跟踪文件示例：

```
AlarmNotifier Trace Entry 306

Applying first_shift to Alarm 8986 set on landscape 0x540000
Applying Filter 1, tag: Abner or Abbot

ALARM VALUES          MATCH  FILTER VALUES
-----
LANDSCAPE              -->    LANDSCAPE
    0x540000           -->    0x540000
                        remaining values ignored

MODEL TYPE             -->    MODEL TYPE
    Pingable           -->    Pingable
                        remaining values ignored

DEVICE LOCATION        -->    DEVICE LOCATION
    World:USA:NorthEast: -->    USA

ALARM SEVERITY        ALARM SEVERITY
    INTIAL              MAINTENANCE
                        SUPPRESSED
                        MAJOR
                        CRITICAL
                        remaining values ignored

ALARM CAUSE            ALARM CAUSE
    0x10004             0x10005
                        0x10007

SPECTROSERVER HOST    -->    SPECTROSERVER HOST
    coffee              -->    coffee
                        remaining values ignored

-----
                                FILTER 1 FAILED

Alarm Failed Policy

Notification NOT sent to AlarmNotifier for Alarm 8986 set on
```

报警属性与这些筛选不匹配

第 5 章： SANM 和 AlarmNotifier

此部分包含以下主题：

[AlarmNotifier 增强功能](#) (p. 29)

[启动 AlarmNotifier](#) (p. 29)

[访问警报管理参数](#) (p. 31)

[警报确认](#) (p. 32)

[用户可清除警报](#) (p. 33)

[启用 SANM 的脚本参数](#) (p. 33)

[启用 SANM 的 .alarmrc 参数](#) (p. 37)

AlarmNotifier 增强功能

如果在系统上安装了 SANM，则 AlarmNotifier 会获得一些额外的功能。这些功能包括用于指定应用程序名称和创建跟踪文件的额外启动选项、警报确认和警报清除命令，以及脚本和资源文件参数。SANM 还允许 AlarmNotifier 在分布式环境中运行。

启动 AlarmNotifier

AlarmNotifier 位于 `<$SPECROOT>/Notifier` 目录中。默认情况下，该目录包含以下文件：

- .alarmrc
- AlarmNotifier
- ClearScript
- README
- SetScript
- UpdateScript

AlarmNotifier 包括以下额外的文件和目录:

AlarmAck

确认警报。

AlarmClear

清除警报。

Trace

显示跟踪文件。

要启动 AlarmNotifier, 请在 `<${SPECROOT}/Notifier` 目录中使用以下 AlarmNotifier 命令:

```
AlarmNotifier [-r resourcefile] [-n application][-tl summary|details [-tn tracefile] [-ts size]]
```

-r resourcefile

允许您指定除默认资源文件 `.alarmrc` 之外的其他资源文件。

-n application

允许您覆盖资源文件中 `APPLICATION` 参数指定的应用程序名称值。可以为 AlarmNotifier 应用程序实例指定其他名称。通过此选项, 您可以启动 AlarmNotifier 的多个实例, 并将其中的每一个实例与不同的 `SANM` 警报筛选策略相关联。如果未向资源文件中的 `APPLICATION` 参数分配名称, 请在启动时使用 `-n` 选项来指定应用程序名称。

-tl summary | details

允许您在指定的级别 (摘要或详细) 激活追踪。AlarmNotifier 跟踪文件的默认格式为应用程序名称加上跟踪文件的创建日期。

-tn tracefile

允许您指定除默认名称之外的其他跟踪文件名称, 仅当使用了 `-tl` 选项时才提供该选项。请将此选项与 `-tl` 选项一起使用。

在使用跟踪文件选项时, 默认情况下输出文件会写入 `<${SPECROOT}/Notifier/trace` 目录。要显式命名输出文件和路径, 请使用 `[-tn filename]` 选项。如果 `<filename>` 是相对路径, 则跟踪输出会写入相对于当前目录的文件。如果 `<filename>` 是绝对路径, 则跟踪输出会写入绝对路径。

-ts size

允许您指定跟踪文件中的行数。请将此选项与 `-tl` 选项一起使用。应用程序会将此行数写入文件, 然后环绕到文件的开头。条目会按顺序编号, 在最后一个条目后会出现 `END OF TRACE` 行。跟踪文件中的默认行数是 10000。

访问警报管理参数

通过“警报管理”视图，您可以控制警报管理的某些方面。此视图中的两个参数“生成警报事件”和“将事件添加到警报中”可确定 SpectroSERVER 如何对警报更新作出反应。

可以在 OneClick 中查看和修改警报管理参数，以便控制警报管理的某些方面。

遵循这些步骤:

1. 打开 OneClick。
2. 在“导航”面板中的 Universe 视图中选择 VNM 模型。
相应的详细信息会显示在右侧的“内容”面板和“组件详细信息”面板中。
3. 在“组件详细信息”面板中，选择“信息”选项卡，并打开“警报管理”菜单。

下列警报管理参数会影响警报事件更新:

生成警报事件

启用警报更改事件（指示警报已生成、更新或清除）的生成。

默认: 已启用（是）。

重要说明! 如果禁用“生成警报事件”，用户将不会在“事件”视图中看到警报历史记录和事件信息。此外，Spectrum Report Manager 的多个功能也将无法正常运行。强烈建议使用默认设置“是”运行。

将事件添加到警报中

控制是否将警报更改事件添加到每个警报。如果禁用了该参数，则警报更改事件将不会显示在警报的“组件详细信息”面板的“事件”选项卡中。如果启用，会添加影响警报的所有事件，从而增加发生计数。例如，还会添加事件类型不同但生成相同警报的事件，例如警报管理或警报清除事件。

默认: 已禁用（否）。

注意: 有关详细信息，请参阅《分布式 SpectroSERVER 管理员指南》。

确认始发事件数据已保存

高流量水平可能会导致 **Archive Manager** 无法持续稳定地提供与报告的警报关联的事件。在这种情况下，您仍然可以检索到有关与警报关联的事件的一些基本信息。默认情况下，**SpectroSERVER** 会存储此信息。

注意： 仅可检索与警报关联的第一个事件（始发事件）的相关信息。

警报管理应用程序模型的 **Store_Originating_Event** 属性 (0x1296f) 确定始发事件信息是否可用于 **AlarmNotifier**。确认已采用默认设置“是”（已启用），以便事件信息在故障转移的情况下可用。

遵循这些步骤：

1. 单击 **OneClick** 控制台的“导航”面板中的“定位器”选项卡。
2. 展开“应用程序模型”。
3. 双击“按名称”。
4. 将打开“搜索”框。
5. 在“模型名称包含”字段中键入“**AlarmMgmt**”，然后单击“确定”。
将在“结果”面板中显示报警管理模型。
6. 选择“**AlarmMgmt**”模型。
将在“组件详细信息”面板中显示相应详细信息。
7. 在“组件详细信息”面板中，单击“属性”选项卡。
8. 在“搜索”框中键入“**store**”以查找 **Store_Originating_Event** 属性。
9. 双击它以验证右侧窗格中的值。

警报确认

AlarmAck 命令允许您确认警报。此命令可在任何 **shell** 命令提示符处使用以确认特定警报，也可以合并到脚本中。如果操作成功，**AlarmAck** 会返回 0 值。否则，它会返回一个非零值。

要确认警报，请使用以下语法运行 AlarmAck 命令：

```
AlarmAck -a alarm -l landscape
```

-a *alarm*

定义警报 ID。

-l *landscape*

定义发出警报的格局的格局句柄。

注意：仅可用于分布式 SpectroSERVER 环境。

要确认模型的所有警报，请使用以下语法运行 AlarmAck 命令：

```
AlarmAck -m modelhandle
```

-m *modelhandle*

指定出现警报状况的模型的模型句柄。

用户可清除警报

AlarmClear 命令会清除用户可清除警报。要确定警报是否是用户可清除警报，请检查警报通知中 UserClearable 参数的值。AlarmClear 可从任何 shell 命令提示符处启动以清除特定警报，也可以将其合并到脚本中。如果操作成功，AlarmClear 会返回 0 值。否则，它会返回一个非零值。

可以使用以下语法运行 AlarmClear 命令以清除警报：

```
AlarmClear -a alarm -l landscape
```

-a *alarm*

定义警报 ID。

-l *landscape*

定义发出警报的格局的格局句柄。

启用 SANM 的脚本参数

当 SetScript、UpdateScript 和 ClearScript 脚本在安装了 SANM 的计算机上运行时，它们具有额外的参数。

下面的列表说明了启用 SANM 的脚本参数：

绿色闪光

在 ClearScript 通知中显示，但不在 SetScript 或 UpdateScript 通知中显示。

启用后，清除的警报会显现 *绿色闪光* 状态：模型的“绿色闪光”选项已启用，且 .alarmrc 资源文件中的 GET_FLASH_GREEN 参数设置为 True。即使 SetScript 和 UpdateScript 通知不会显示此字段，该参数也会传递到这些脚本，但它无效且具有默认值 False。

位置

标识包含其警报已设置、更新或清除的网络元素的位置模型。该元素必须在 OneClick World 拓扑视图中建模。您可以在位置模型的冒号分隔的层级列表中找到包含有问题网络元素的模型的位置模型。例如，一个包含在美国东北部地区波士顿建筑物的一层 222 房间内的模型的警报如下所示：

```
USA:Northeast:BostonBldg:FirstFloor:Room222.
```

警报存在时长

指定 SANM 保持来自与该策略关联的 AlarmNotifier 实例的警报的时间长度。“警报存在时长”在 SANM 策略的筛选中设置。如果警报必须以不同的时长通过多个筛选，则 SANM 会使用最短的非零警报存在时长间隔。

通知数据

列出 SANM 传递到与该策略关联的 AlarmNotifier 实例的通知数据条目（用户名）。这些条目在 SANM 策略的筛选中指定。AlarmNotifier 脚本可配置为向通知数据条目中的那些用户发起电子邮件通知。

可能原因

是与警报关联的可能原因文本。

事件消息

是有关与警报关联的事件的消息。如果 CA Spectrum 警报没有关联的事件，或者事件不包括警报信息，则此字段为空。

电子邮件通知

如果使用 AlarmNotifier 脚本发送电子邮件通知，请在脚本中设置 VARFORMAIL 参数的值。此参数指定电子邮件消息的发送对象。

如果使用启用 SANM 的 AlarmNotifier，请使用 NotificationData 参数来设置 VARFORMAIL 的值。如果将 NotificationData 用作 VARFORMAIL 的值，则电子邮件会发送给在与调用脚本的 AlarmNotifier 实例关联的 SANM 策略的 NotificationData 参数中指定的用户。例如，如果通知数据条目的格式为 “John: Mary or Sue: Lynn, Jeff”，则电子邮件会发送给 John、Mary、Lynn 和 Jeff，但不会发给 Sue，因为 AlarmNotifier 会将冒号解释为一个 AND 运算符，但对 OR 运算符不采取操作。

VARFORMAIL 参数的其他可能的值是 RepairPerson 或两者。如果 AlarmNotifier 未与 SANM 一起运行，则 RepairPerson 选项是其唯一可用的选项。这两个选项指示电子邮件通知发送给指定的 RepairPerson 和由 NotificationData 参数指定的用户。

注意：有关配置 AlarmNotifier 脚本以发送电子邮件通知的详细信息，请参阅《AlarmNotifier 用户指南》。

第三方应用程序

可以自定义或替换 SetScript、ClearScript 或 UpdateScript，以便与第三方应用程序集成。如果创建自己的脚本或可执行文件，需要了解从 CA Spectrum 向接收脚本或可执行文件传递了哪些参数。脚本或可执行文件必须按正确的顺序接收 CA Spectrum 向其传递的所有参数。

注意：包含警报的模型的所有 CA Spectrum 属性都可以传递给 AlarmNotifier，并且可在脚本中使用。有关详细信息，请参阅《AlarmNotifier 用户指南》。

下表显示了 USE_NEW_INTERFACE .alarmrc 参数设置为 TRUE 时传递给每个脚本的每个参数的编号、名称和格式：

参数	名称	格式
1	日期	mm/dd/yy
2	时间	hh:mm:ss
3	模型类型	文本
4	模型名称	文本
5	警报 ID	整数
6	重要级别	文本
7	原因	文本
8	修复屏幕	文本

参数	名称	格式
9	服务器	文本
10	格局	十六进制
11	模型句柄	十六进制
12	模型类型句柄	十六进制
13	IP 地址	xxx.xxx.xxx.xxx
14	安全字符串	文本
15	警报状态	文本
16	已确认	文本
17	可清除	文本
18	绿色闪光	文本
19	位置	文本
20	时长	整数
21	通知数据	文本

下表显示了 USE_NEW_INTERFACE .alarmrc 参数设置为 FALSE 时传递给每个脚本的每个参数的编号、名称和格式：

参数	名称	格式
1	日期	mm/dd/yy
2	时间	hh:mm:ss
3	模型类型	文本
4	模型名称	文本
5	警报 ID	整数
6	重要级别	文本
7	原因	文本
8	修复屏幕	文本
9	状态	文本
10	服务器	文本
11	格局	十六进制
12	模型句柄	十六进制

参数	名称	格式
13	模型类型句柄	十六进制
14	IP 地址	xxx.xxx.xxx.xxx
15	安全字符串	文本
16	警报状态	文本
17	已确认	文本
18	可清除	文本
19	绿色闪光	文本
20	可能原因	文本
21	位置	文本
22	时长	整数
23	通知数据	文本
24	事件消息	文本

如果 `USE_NEW_INTERFACE` 设置为 `TRUE`，则“状态”、“可能原因”和“事件消息”参数会作为环境变量发送。参数顺序也会因此受到影响。如果 `USE_NEW_INTERFACE` 设置为 `FALSE`，请在您的脚本中使用以下语法将数据从“可能原因”和“事件消息”参数读取到变量中，如下所示：

```
<variablename>=`echo "$2" | tr '\350' '\012' | tr '\351' ' '`
```

当脚本解析来自新行的额外数据或其他特殊字符时，就需要使用此语法以避免问题。

注意：有关 `USE_NEW_INTERFACE` .alarmrc 参数的详细信息，请参阅《*AlarmNotifier 用户指南*》。

启用 SANM 的 .alarmrc 参数

在安装了 SANM 的计算机上运行 AlarmNotifier 时，AlarmNotifier 资源文件 .alarmrc 有几个额外的参数。

下面的列表说明了启用 SANM 的参数：

APPLICATION

定义标识此 AlarmNotifier 应用程序的应用程序名称。如果在网络上使用多个 AlarmNotifier 应用程序，请使用唯一的应用程序名称（如 AlarmNotifier1 或 AlarmNotifier2）来对其加以区分。然后，您可以对每个应用程序使用唯一的 SANM 警报通知策略。如果在调用 AlarmNotifier 时使用 n 选项，则 APPLICATION 参数值会被忽略。

默认值： AlarmNotifier

GET_LOCATIONS

允许您指定是否通知您带有警报的设备的位置。如果您对位置信息不感兴趣，可将此参数设置为 False。False 设置会覆盖在警报通知策略中指定为筛选参数的所有位置，从而减少网络流量。

GET_PROBABLE_CAUSES

允许您指定是否要接收与每条警报关联的可能原因文本。如果您对可能原因信息不感兴趣，可将此参数设为 False，从而改善 AlarmNotifier 性能。

默认值： True。

GET_EVENTS

允许您指定是否接收与警报关联的事件消息。如果您对事件信息不感兴趣，可将此参数设置为 False。排除事件可减少 AlarmNotifier 产生的网络流量，并改善性能。

默认值： True。

GET_FLASH_GREEN

允许您指定是否接收模型的绿色闪光状态。ClearScript 是唯一一个显示绿色闪光状态的脚本。如果为模型启用了“绿色闪光”，该模型在警报清除之后会继续呈现绿色闪光状态。闪烁状态表明出现了警报，即使这些警报不再存在。如果 GET_FLASH_GREEN 的值设置为 False，则绿色闪光状态始终以 false 值向 ClearScript 传递。如果设置为 True，则绿色闪光状态将以 False 或 True 值正确地传递。

默认值： True。

MSG_TIMESTAMP_FORMAT

为所有 SANM 消息上的时间戳设置格式。输出字符串的最大长度是 127 个字符。除转换字符串之外的其他任何字符都作为时间戳中的文本输出。默认设置是 %X %x:。冒号 (:) 会附加到时间戳的结尾。例如，要输出当前区域设置的日期/时间和时区名称，字符串 %x %X %Z 会作为值输入。如果保留为空，则消息上不会输出任何时间戳。如果输入了不正确的字符串，该字符串会显示为输出中的文本。

POLICY_LANDSCAPE

允许您指定 AlarmNotifier 对所有 SANM 策略定义使用的格局。此参数与 SANM .sanmrc 文件中的 POLICY_LANDSCAPE 设置一起使用。

SHOW_ALL_EVENTS

允许您指定是接收为警报生成的最近事件还是所有事件。如果设置为 False，AlarmNotifier 只会转发最近的事件。例如，假定已基于事件创建了警报，然后有人更新了该警报的状态。当警报状态更改时，生成了与该警报有关的另一个事件。在这种情况下，AlarmNotifier 仅接收第二个事件的状态。这种筛选的目的是要消除已转发的事件。如果在乎消息的大小，例如，如果事件消息作为页面发送，则筛选就变得尤为重要。

默认值： False。

第 6 章：在分布式 SpectroSERVER 环境中使用 SANM

此部分包含以下主题：

[格局和警报监控 \(p. 41\)](#)

[跨多个格局的 SANM 策略管理 \(p. 41\)](#)

格局和警报监控

通过分布式 SpectroSERVER (DSS) 环境，您可以在几个 SpectroSERVER 中划分网络管理任务。创建具有多个 SpectroSERVER 的网络模型时，SANM 可以同时从多个 SpectroSERVER 访问信息。

格局是 CA Spectrum 中的一个术语，表示单个 SpectroSERVER 管理的网络域。如果 SANM 在分布式环境中运行，它会监控来自所有格局的警报。即使不同的格局可以在 DSS 环境中相互建模，启用 SANM 的应用程序也不会接收重复的警报信息。

因为在 DSS 环境中 SANM 跨 VNM 对警报进行评估，您可能需要限制接收的警报通知的类型。在 DSS 环境中，可通过慎重定义警报通知策略中的参数、格局、子网 IP 地址和设备位置，限制警报通知的数目。

跨多个格局的 SANM 策略管理


在分布式环境中配置 SANM 有两种方法可供选择。可以在任意格局上创建 SANM 策略，并允许 SANM 读取所有格局中的所有策略。或者，可以在一个格局上创建所有 SANM 策略，并仅允许 SANM 读取该格局中的策略。无论哪种情况，都可以将任意格局中的警报处理应用程序与 SANM 策略相关联。

如何在单个格局中创建 SANM 策略

如果设置了分布式环境，使得所有格局的所有策略都从单个 SpectroSERVER 进行了定义和管理，则可以在分布式环境中的任意 SpectroSERVER 上安装警报处理应用程序。- 如果应用程序资源文件中的值都是正确的，应用程序会查找包含 SANM 策略定义的服务器，并将其与相应的策略相关联。此配置可减少网络上用于关联警报处理应用程序和 SANM 策略的初始流量，还有助于持续进行 SANM 策略管理。

注意：不能在格局之间迁移或移动 SANM 策略。如果要制定此配置，并在各个格局上定义了策略，则必须在将管理 SANM 策略的新格局上重新创建这些策略。

要在一个格局中配置所有 SANM 策略，请执行下列步骤：

1. 将 .alarmrc 文件中的 POLICY_LANDSCAPE 参数更改为安装了 SANM 并已在其中创建和管理策略的 SpectroSERVER 的格局句柄。
2. 将警报处理应用程序资源文件 (.alarmrc、.arsgrc) 中的 POLICY_LANDSCAPE 参数更改为安装了 SANM 的 SpectroSERVER 的格局句柄。此参数会指示应用程序在何处查找定义的策略。
3. 重新启动安装了 SANM 的 SpectroSERVER，并重新启动警报处理应用程序，使对资源文件参数所做的更改得以被读取。
4. 在 OneClick 的“定位器”选项卡上依次打开“SANM”、“所有策略”，然后单击 （启动选定的搜索）。

仅有的可用策略是在此格局上创建的策略。其 POLICY_LANDSCAPE 参数设置为此格局的格局句柄的所有警报处理应用程序都会显示在应用程序列表中。

如何在多个格局中创建 SANM 策略

可以设置一个分布式环境，以便 SANM 策略可以在任意 SpectroSERVER 上进行定义和管理。分布式环境中任意 SpectroSERVER 上的警报处理应用程序都可以访问所有这些策略。

要在多个格局中配置 SANM 策略，请验证以下要求：

- .sanmrc 文件中的 POLICY_LANDSCAPE 参数一定不能具有关联的值。
- 警报处理应用程序资源文件 (.alarmrc、.arsgrc 等) 中的 POLICY_LANDSCAPE 参数也一定不能具有关联的值。

然后，执行下列步骤：

1. 重新启动安装了 SANM 的 SpectroSERVER。
2. 重新启动警报处理应用程序，使对资源文件参数所做的更改得以被读取。
3. 打开 OneClick。确认在分布式环境中创建的所有策略均可用。
4. 确认分布式环境中的所有警报处理应用程序均可用于关联。

确定受监控格局的方法

可以使用以下方法来确定哪些格局受 SANM 监控：

- 使用 CA Spectrum 命令行界面 (CLI) 应用程序连接到与 SANM 连接的 SpectroSERVER。然后在命令行上输入 **show landscapes**。
CLI 应用程序会显示在该服务器中建模的所有格局的列表。
注意：有关详细信息，请参阅《*命令行界面用户指南*》。
- 打开您为启用 SANM 的应用程序指定的任意一个详细跟踪文件。跟踪文件指示与 SANM 连接的 SpectroSERVER 的格局映射中每个格局的连接状态。默认情况下，跟踪文件会存储在启用 SANM 的应用程序的主目录下的 **trace** 目录中。

