CA Spectrum®

Cisco 设备管理指南

版本 9.3

CA Technologies 产品引用

本文档参考 CA Spectrum® Infrastructure Manager (CA Spectrum)。

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： Cisco 设备支持概述

此部分包含以下主题：

设备支持

CA Spectrum CISCO 设备认证提供了 Cisco MIB 和陷阱支持、说明性设备标识、OneClick 视图和 Cisco 技术支持。CA Spectrum CISCO 设备认证还针对特定设备和固件提供了 CA Spectrum 标准功能。

设备系列认证的示例包括 Catalyst、PIX 防火墙、无线 LAN 控制器和 Aironet。

基于固件的认证示例包括 Cisco IOS、CatOS 和统一计算系统 (UCS)。

如果没有特定的设备系列认证可供您的 CISCO 设备使用，则可使用以下基于固件的模型类型之一：

- Rtr_Cisco - 为运行 IOS 固件的 Cisco 路由器建模。
- SwCiscoIOS - 为运行 IOS 固件的 Cisco 交换机建模。
- RtrCatOS - 为运行 CatOS 固件的 Cisco 路由器建模。
- SwCatOS - 为运行 CatOS 固件的 Cisco 交换机建模。
- CiscoNXOS - 为运行 NX-OS 固件的 Cisco Nexus 设备建模。
- GnCiscoDev - 为未运行 IOS 或 CatOS 固件的 Cisco 设备建模。

MIB 源

根据 CISCO 设备固件，可在以下 MIB 源中找到相应的机箱和主板或模块信息：

OLD-CISCO-CHASSIS-MIB

Cisco 已弃用该 MIB。因此，该信息可能不完整。要查看该 MIB 的内容，请在 OneClick 中查看“Cisco 机箱视图”子视图。

CISCO-STACK-MIB

CatOS 设备支持该 MIB。该 MIB 已被弃用，以支持 ENTITY-MIB。要查看该 MIB 的内容，请查看“MIB 工具”实用工具。

注意：有关 MIB 工具的详细信息，请参阅*《认证用户指南》*。

ENTITY-MIB

该 MIB 包含新设备的最新主板或模块信息。但是，旧设备不会正确填充该 MIB。要查看该 MIB 的内容，请在 OneClick 中查看“实体视图”子视图。

第 2 章： Cisco 统一计算系统

此部分包含以下主题：

Cisco UCS 概述

Cisco 统一计算系统 (UCS) 由一组协同工作的专用设备构成，包括机箱和服务器的刀片。UCS 为数据中心提供支持，包括提供动态 IT 基础架构并统一网络、计算和虚拟资源。

CA Spectrum 允许您查看 Cisco UCS 的以下关键组件：

UCS Manager

在交换矩阵互连交换机上运行的 Web 服务代理。Cisco UCS Manager 支持基于 XML 的 API 以实现客户端交互。

交换矩阵互连 (FI) 交换机

- 通常，每个 UCS 系统都配有两个交换机；Cisco 建议使用冗余配置
- 运行 NX-OS
- 承载 UCS Manager

机箱

无代理、无交换机、刀片服务器机箱，每个 UCS Manager 最多可配置 40 个机箱。每个机箱均支持 8 个半宽或 4 个全宽服务器刀片。

刀片

充当虚拟化主机的服务器平台。

服务配置文件

刀片服务器的逻辑视图。它们存储在 FI 交换机中，包含刀片服务器身份信息（标识和网络信息）。

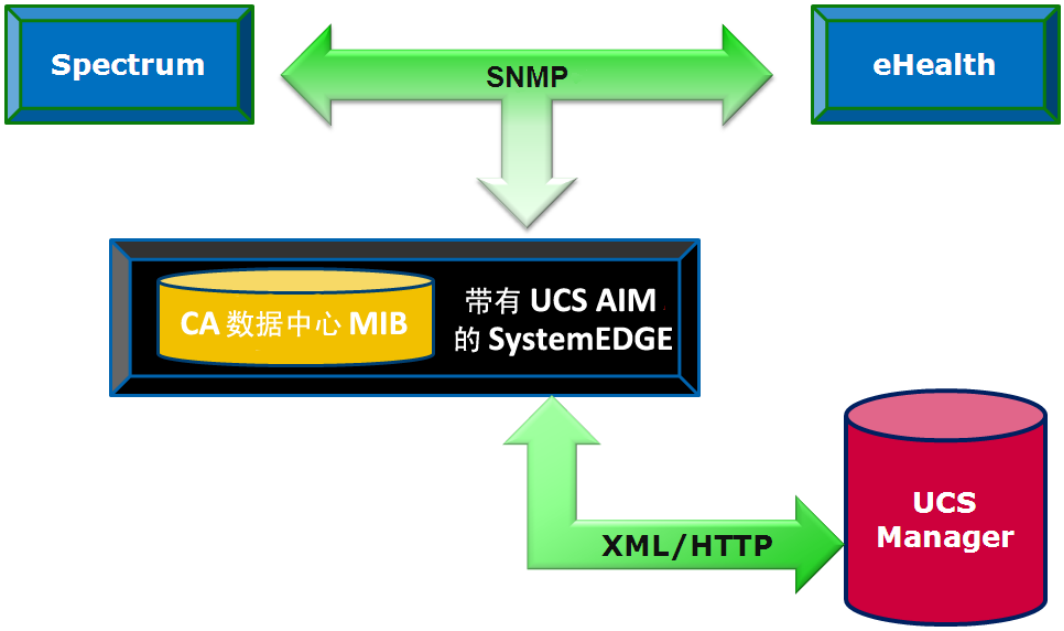
解决方案体系结构

可以通过采用专用 SystemEDGE Application Insight Module (AIM) 来启用对 Cisco UCS 的 CA Spectrum 支持。该 AIM 与 UCS 基于 XML 的 API 进行通信，以获取有关 UCS 托管环境的信息。随后，会将数据写入一对 CA 开发的 MIB 中。采用这种解决方案，诸如 CA eHealth 等其他 SNMP 客户端将可以使用 AIM。

UCS AIM 是 SystemEDGE SNMP 代理的一个扩展，可以支持多个 UCS 系统。CA 开发的 MIB 包括：

- 常规数据中心 MIB (CADATACENTERA)
- UCS 特定的数据中心扩展 MIB (CACUCSEXTENSIONA)

如下图所示，CA 产品（如 CA Spectrum 和 CA eHealth）使用 SNMP 连接到承载 UCS AIM 的 SystemEDGE，以获取 Cisco UCS 详细信息。UCS AIM 使用 XML/HTTP 以连接到 UCS Manager。



功能

CA Spectrum UCS 认证功能包括：

- 自动设备发现和建模 - 为 UCS 组件创建模型，并维护刀片模型和所有驻留 ESX 主机之间的关联
- 连接 - 生成 UCS 系统组件的准确物理（第 2 层）拓扑映射

- 增强的故障管理 - 识别和抑制有症状的警报，并通过代理管理辅助进行故障隔离
- 专用 UCS 视图 - 允许您查看 UCS 特定的数据
- 智能陷阱转发 - 支持在单个 UCS 组件上生成警报
- 机箱管理（非特定 UCS）- 利用 CA Spectrum 的丰富的机箱管理功能集

自动设备发现和建模

认证会在创建承载 UCS AIM 的 Host_SystemEDG 模型时自动为 UCS 系统组件建模。此模型可标识为 Cisco UCS Manager。它会在检测到 UCS AIM MIB 后创建 cacucsaimApp 应用程序模型类型。然后，该应用程序模型会创建 UCS 系统组件，如交换矩阵互连、机箱、刀片、服务配置文件等。

注意：并非所有 UCS 组件都已建模，如交换矩阵扩展器、电源、媒体适配器或接口。

接下来，会对所有刀片上之前建模的 ESX 主机执行搜索。将在相应刀片和 ESX 模型之间创建一种关联，使用户能够了解这种硬件到软件的关系。

最后，会创建容器模型来表示每个 UCS 系统。这些模型与 SystemEDGE 主机驻留在同一容器（如 Universe）中。每个容器均提供 UCS 系统组件的一个逻辑拓扑分组。

将定期轮询 UCS AIM MIB，以从 UCS 环境中收集状态和建模信息。有关配置轮询时间间隔的详细信息，请参阅控制 Cisco UCS AIM 轮询 (p. 21)。

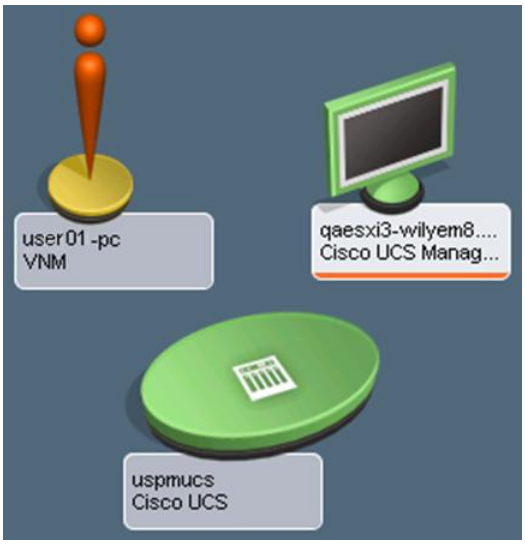
重要说明！在给定格局中，不能为其 UCS AIM 监控同一 UCS 系统的多个 Host_SystemEDGE 模型建模。不支持此配置。

如果承载 UCS AIM 的 Host_SystemEDGE 是虚拟设备，请先对其建模，然后再对承载相应虚拟技术 AIM 的 Host_SystemEDGE 进行建模。否则，UCS 容器可能会错误地在虚拟技术的物理主机容器中创建。此情况会中断 CA Spectrum 故障隔离算法。

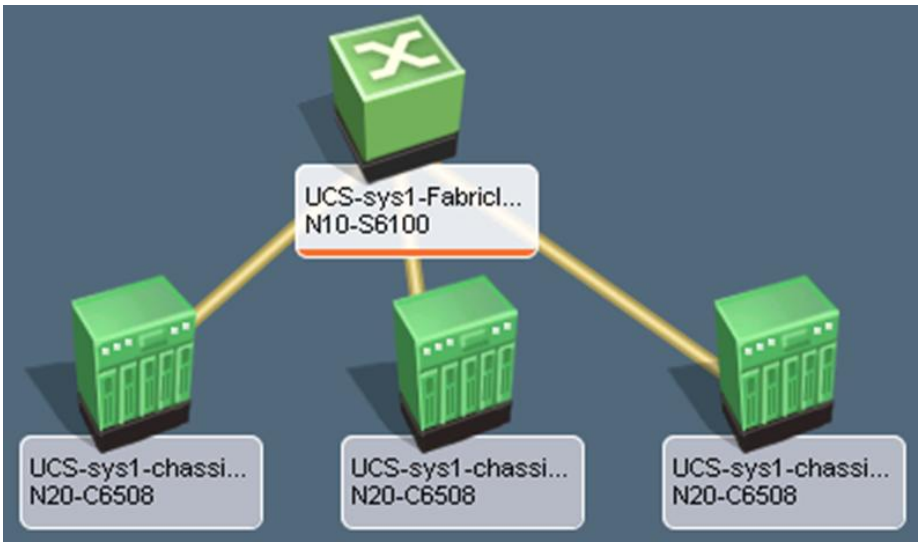
UCS 容器模型

为了表示 UCS 容器，CA Spectrum 使用带有机箱标志的标准容器图标。UCS 容器具有 CiscoUCSContainer 类型的模型。每个容器将单个 UCS 系统的所有从拓扑上来说意义重大的模型（多达 2 个 FI 和 40 个机箱）收集到一起。UCS 容器的内容无法修改。

UCS 容器如下图所示：



下图显示了 UCS 容器内容的一个示例：



UCS 交换矩阵互连模型

UCS 交换矩阵互连使用 CA Spectrum 的标准交换机图标。如果该设备是通过 IP 地址或发现建模的，并且其 NX-OS SNMP 代理已启用（默认情况下，会禁用该代理），则会创建一个 CiscoUCSFabricInterconnect 类型的模型。否则，自动 UCS 发现将创建一个 Pingable 模型。该模型不包括任何设备接口，也不包括到上游设备的任何连接。请注意，IP 地址建模可以发生在 UCS 发现之后，在这种情况下，Pingable 模型会被 CiscoUCSFabricInterconnect 模型替代。

UCS 交换矩阵互连模型支持专用 UCS OneClick 视图，并且是 UCS 交换矩阵互连陷阱和警报的目标模型。

UCS 机箱模型

UCS 机箱使用 CA Spectrum 的标准机箱图标，具有 CiscoUCSChassis 类型的模型。OneClick 的“组件详细信息”面板中的“接口”选项卡已针对 UCS 机箱进行了一些改进，现在可以显示机箱内的刀片，以帮助进行刀片管理。

UCS 机箱还扩展了 CA Spectrum 的故障隔离功能，以便提供并置硬件资源的警报关联。

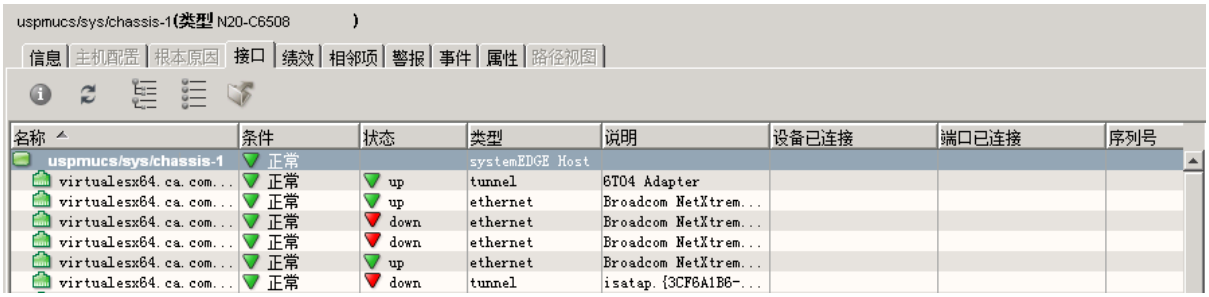
UCS 机箱模型支持专用 UCS OneClick 视图，并且是 UCS 机箱陷阱和警报的目标模型。

UCS 刀片模型

UCS 刀片在 CA Spectrum 中建模，但与交换矩阵互连交换机和机箱不同，它们在其父 UCS 容器内及 CA Spectrum 拓扑的任何其他位置都不可见。但是，每个机箱的 UCS 刀片都会在机箱的“接口”选项卡中列出。UCS 刀片具有 CiscoUCSBlade 类型的模型。

CA Spectrum 会在刀片和驻留在该刀片上的 ESX 主机之间自动建立关联。此关联通过对先前建模的 ESX 主机执行搜索并获得 UUID（全局唯一标识符）值来实现。随后会检查刀片 UUID。找到匹配项后，ESX 主机模型会与该刀片模型关联。自动关联仅支持 ESX 主机。CA Spectrum 理解该刀片（硬件）与 ESX 主机（软件）的关联关系，并利用这种关系增强故障隔离功能。您会看到有意义的警报详细信息，例如，ESX 主机因其刀片发生故障而失去了联系。

建立关联后，ESX 主机模型就会替代机箱模型“接口”选项卡中的刀片模型。



您可以手动将 UCS 刀片与相应的 SNMP 代理模型关联，使用户可以了解刀片（硬件）与代理（软件）之间的关联关系。

UCS 刀片模型支持专用 UCS 基于硬件的 OneClick 视图，该视图包括以下类型的信息：

- 统计信息，如 CPU 负载、内存和存储利用率
- 映像清单（BIOS 及固件）和 BIOS H/W 配置
- 刀片服务器的物理接口
- 服务配置文件详细信息

UCS 刀片模型是 UCS 刀片陷阱和警报的目标模型。

详细信息

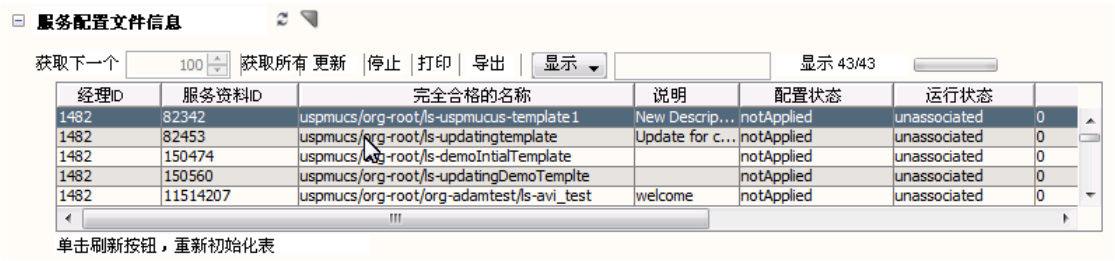
手动刀片/SNMP 设备关联 (p. 20)

UCS 服务配置文件模型

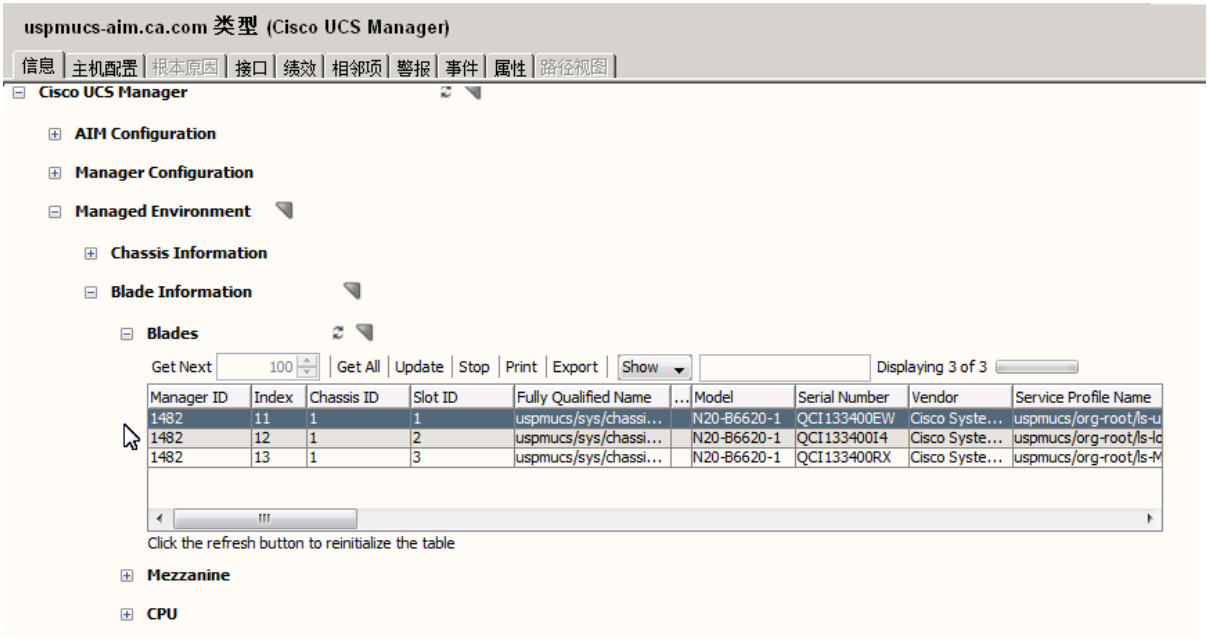
在 Cisco 统一计算系统中开通的刀片服务器由服务配置文件指定。服务配置文件是关于服务器及其 LAN 和 SAN 网络连接的软件定义。UCS 服务配置文件具有 CiscoUCSServiceProfile 类型的模型。

服务器、网络和存储管理员可创建服务配置文件。服务配置文件存储在 Cisco UCS 6100 系列交换矩阵互连中。如果服务配置文件部署在刀片服务器上，UCS Manager 会自动配置刀片服务器、其网络适配器、交换矩阵扩展器以及交换矩阵互连，以支持在服务配置文件中指定的配置。

CA Spectrum 为由 UCS Manager 定义的每个服务配置文件创建模型。可以从“OneClick Locator”选项卡查看它们，现在，该选项卡中包括一个“服务配置文件模型类”搜索选项。此外，服务配置文件详细信息还会显示在各个 OneClick 视图中。在承载 UCS AIM 的 Host_SystemEDGE 模型上，依次选择“Cisco UCS Manager”、“管理的环境”和“服务配置文件信息”选项。然后，您就能看到 Host_SystemEDGE 管理的 UCS 系统中的所有服务配置文件的名称、ID、说明、关联的刀片以及各种状态。



CA Spectrum 还会显示与每个 UCS Manager 机箱中安装的每个刀片关联的服务配置文件。



UCS 服务配置文件模型是 UCS 服务配置文件警报的目标模型。

连接

UCS 交换矩阵互连模型在加入连接时，需要在上游设备与机箱中的刀片式服务器之间提供边界交换节点。

UCS 交换矩阵互连的上游

交换矩阵互连接口的上游连接通过标准桥接表完成。完成这些连接需要执行以下步骤：

- 在交换矩阵互连中启用本地 NX-OS SNMP 代理。
- 通过 IP 地址或发现为设备建模。

详细信息

UCS 交换矩阵互连模型 (p. 12)

UCS 交换矩阵互连的下游

从 UCS 交换矩阵互连到其构成机箱的下游 FCoE 连接显示为标准 CA Spectrum L2 连接。这些连接以编程方式创建，而不是通过标准桥接表或 UCS MIB 创建。

增强的故障管理

针对 UCS 增强的故障管理包括两种类型的警报：

- 故障警报
  - 表示 L2 可用性出现问题
  - 已通过特别关联逻辑得到增强
- 代理已丢失警报
  - 表示无法从 SystemEDGE UCS AIM 主机获得更新的 UCS 信息
  - 包括主机自身的“代理不可用”警报

UCS 故障管理增强还包括机箱级别和刀片级别可用性警报以及陷阱生成的、表示基础架构和环境问题的警报。

UCS 利用警报关联的优点，可以：

- 精确找出根本原因
- 抑制外来警报
- 将症状与根本原因相关联
- 显示影响

在机箱级别和 UCS 系统级别都会发生 UCS 警报关联。

如果出现故障（失去联系）警报，机箱级别警报关联会使用包括机箱、其刀片和所有 SNMP 刀片代理模型的域。如果所有这些域实体（也就是机箱、刀片和 SNMP 刀片代理）都失去联系，则会在机箱上生成单个“机箱关闭”警报。整套“失去联系”警报都与它关联。

如果出现代理已丢失警报，机箱级别警报关联会使用包括机箱及其刀片的一个较小的域。其中，所有刀片的“代理已丢失”警报都与机箱的“代理已丢失”警报关联。

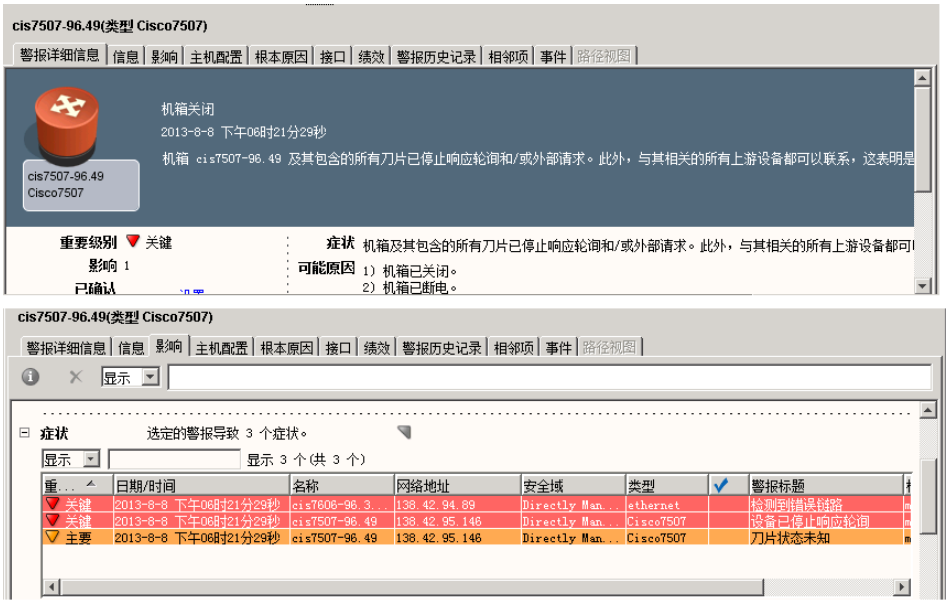
UCS 系统级别警报关联使用包括 SystemEDGE 主机、FI、子机箱和刀片的域。如果 CA Spectrum 和 SystemEDGE 主机之间的通信已断开，则所有 FI、机箱和刀片上都会出现“代理已丢失”警报。该主机上会出现“代理不可用”警报。

所有组件的“代理已丢失”警报与主机的“代理不可用”警报关联。这些关联会分层级地执行。“代理不可用”警报自身与表示通信失败原因的警报关联。例如，它会指出失去联系、管理丢失或处于维护模式。随后，您可以在警报窗口中查看该顶级全局警报。

根本原因隔离示例

根本原因隔离类似于以下示例：

- UCS 机箱被无意关闭，这会影响到刀片（以及其上运行的服务）。因此，所有刀片上的单个“失去联系”警报会与“机箱关闭”警报关联，以指明机箱出现了故障。
- CA Spectrum 与 SystemEDGE 主机失去联系。因此，所有 FI、机箱和刀片上的“代理已丢失”警报都会分层级地与主机的“代理不可用”警报关联。



机箱和刀片可用性警报

机箱可用性警报包括“机箱关闭”和“刀片状态未知”（其与“机箱关闭”关联）。

刀片可用性警报包括“刀片已移除”和“刀片出现故障”（刀片存在但是处于故障状态）。这两个警报都与父机箱上现有的“刀片状态未知”警报关联。请注意，默认情况下，刀片模型会有两个小时的过时时间，用户可在此时间内更换刀片。

服务配置文件警报

我们不仅显示所有服务配置文件详细信息，还为每个服务配置文件创建了 CA Spectrum 模型。CA Spectrum 主动监控服务配置文件的状态，并且基于每个服务配置文件的操作状态生成事件和警报。

陷阱生成的警报

UCS 支持陷阱生成的警报，此类警报表示存在基础架构和环境问题。会适当地进行区分。示例包括“刀片已添加”、“刀片已移除”、“电源工作不正常”和“温度警告”。

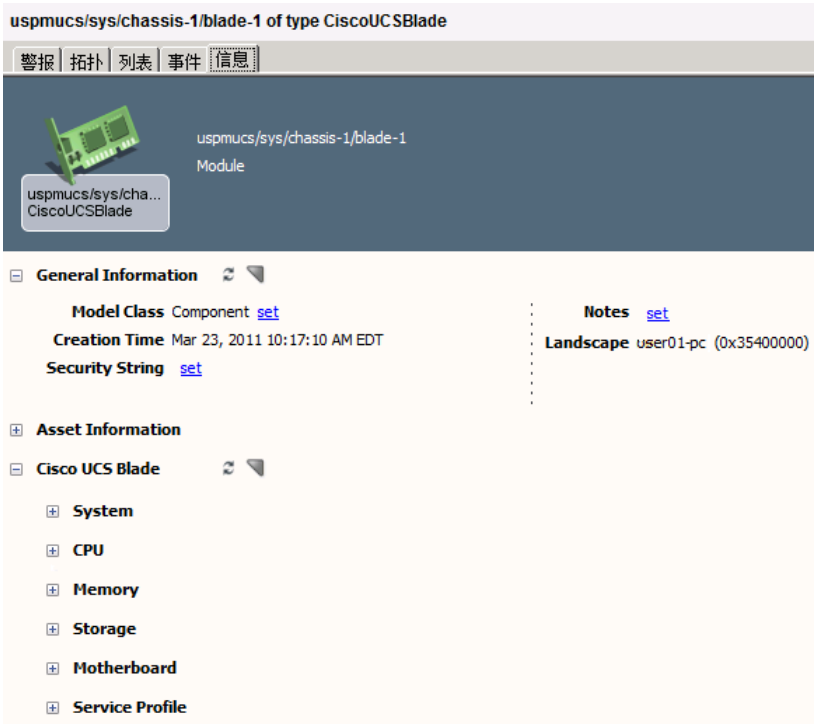
专用 UCS 视图

专用 UCS 视图可用于以下设备类型（在括号中表示）：

- SystemEDGE 主机 (Cisco UCS Manager)

  此视图包括托管环境的表视图。
- 交换矩阵互连（Cisco UCS 交换机）
- 机箱（Cisco UCS 机箱）
- 刀片（Cisco UCS 刀片）
- 服务配置文件 (N/A)

OneClick 视图显示硬件详细信息，如内存 DIMM、夹层卡、交换矩阵互连扩展器和接口。



智能陷阱转发

所有 UCS 陷阱都从 UCS AIM 生成，因此会从 SystemEDGE 主机到达 CA Spectrum 中。因此，CA Spectrum 采用转发机制在正确的 UCS 组件上生成事件或陷阱。可通过检查陷阱变量值来确定正确的组件。如果找不到适用的组件，会在 SystemEDGE 主机上断言陷阱事件。

机箱管理

UCS 可使用 CA Spectrum 中提供的大量机箱管理功能：

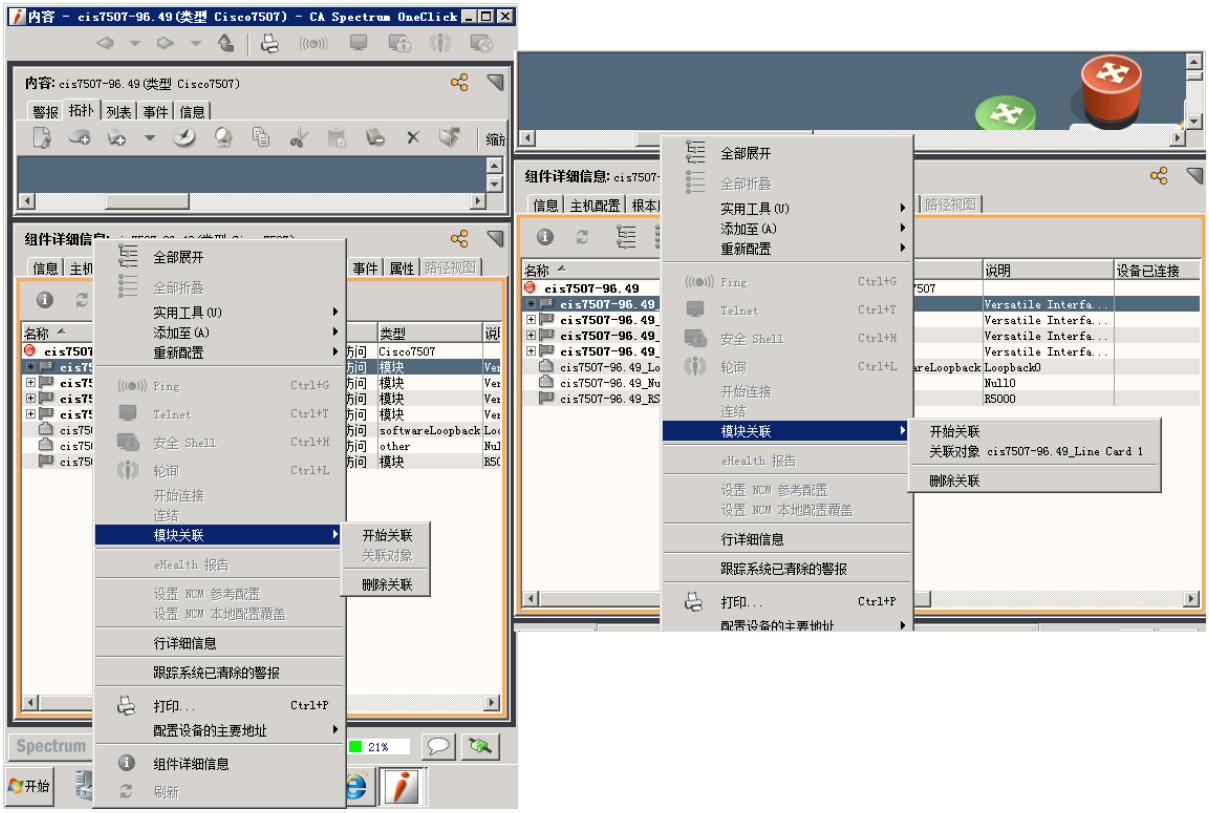
- 手动刀片/SNMP 设备关联
- 刀片和托管设备可见性
- 定位器搜索

有关详细信息，请参阅*《认证用户指南》*中的“基于机箱的支持”一节。

手动刀片/SNMP 设备关联

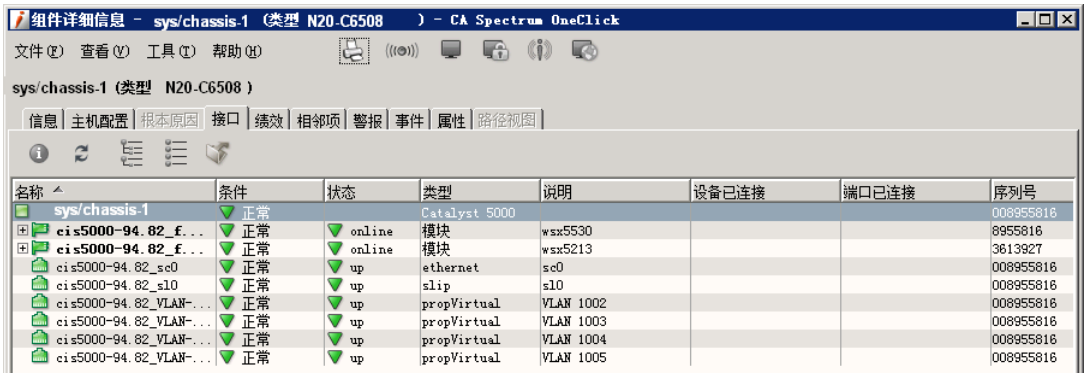
手动刀片/SNMP 设备关联将机箱的一个刀片绑定到支持 SNMP 的刀片代理模型。此关联能够从代理模型快速确定系统/机箱位置。SNMP 模型不会移到 UCS 容器中，但是它会替代机箱的“接口”选项卡中的刀片。

为了支持此集成，SNMP 代理模型将集成到机箱错误关联中。刀片/代理关联还能通过基于机箱的定位器搜索来标识 SNMP 模型。



刀片和托管设备可见性

通过包含关联的 SNMP 设备，扩展的“接口”选项卡可允许用户查看机箱的刀片和托管设备。



定位器搜索

基于机箱的搜索会在“定位器”选项卡的“机箱”节点下列出。这些搜索有助于快速定位机箱及其组件。

搜索包括：

- 所有机箱
- 所有机箱托管设备
- 所有模块
- 托管设备 - 按机箱名称
- 模块 - 按机箱名称

控制 Cisco UCS AIM 轮询

排除网络问题或调整 Cisco UCS Manager 性能时，更改 Cisco UCS AIM (cacucsaimApp) 轮询速率以增加或减少频率。可以通过在 Cisco UCS AIM 应用程序模型上设置 Poll_Interval 属性来配置轮询速率。

遵循这些步骤:

1. 打开 OneClick，并在“导航”窗格中选择“定位器”。
2. 展开“应用程序模型”，然后双击“按设备 IP 地址”。

   此时将打开“搜索”对话框。
3. 在“设备 IP 地址”字段中输入您的 Cisco UCS Manager 的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 Cisco UCS Manager 的应用程序模型列表。
4. 选择 cacucsaimApp 应用程序模型。

   将在“组件详细信息”面板中显示该应用程序模型的详细信息。
5. 在“组件详细信息”窗格中选择“信息”。
6. 展开“CA Spectrum 建模信息”。
7. 单击“轮询时间间隔(秒)”字段中的“设置”，输入新值，然后按 Enter 键。

   注意：将“轮询时间间隔”值从任意数字更改为 0 时还会将“轮询”字段设置为“关闭”，从而禁用 UCS AIM 轮询。如果将“轮询时间间隔”设置为 0，并将“轮询”字段设置为“打开”，UCS AIM 轮询将使用为 Cisco UCS Manager 设备设置的轮询时间间隔继续进行。

   Cisco UCS AIM 轮询速率便配置好了。

第 3 章： Cisco Catalyst

Cisco Catalyst 设备支持

CA Spectrum 支持具有多个增强的认证的 Catalyst 设备系列，包括 1200、1400、1900、2820、3000、3200、4000、4500、5000 和 6500。

对于 Catalyst 2900 和 Catalyst 3500 设备系列，特定的增强认证取决于支持的 MIB 集。

CA Spectrum 为 Catalyst 2900 系列设备建模，如下所示：

- HubCat29xx 模型类型为运行 IOS 固件且支持 CISCO-C2900-MIB 的 Catalyst 2900 系列交换机建模。
- SwCiscoIOS 模型类型为运行 IOS 固件但不支持 CISCO-C2900-MIB 的 Catalyst 2900 系列交换机建模。Catalyst 2970 和 Catalyst 2948g 设备属于此类别。
- SwCat4xxx 模型类型为运行 CatOS 固件的 Catalyst 2900 系列交换机建模。

CA Spectrum 为 Catalyst 3500 系列设备建模，如下所示：

- HubCat29xx 模型类型为运行 IOS 固件且支持 CISCO-C2900-MIB 的 Catalyst 3500 系列交换机建模。
- SwCiscoIOS 模型类型为运行 IOS 固件但不支持 CISCO-C2900-MIB 的 Catalyst 3500 系列交换机建模。Catalyst 3550 系列属于此类别。

Cisco Catalyst 主板故障隔离概述

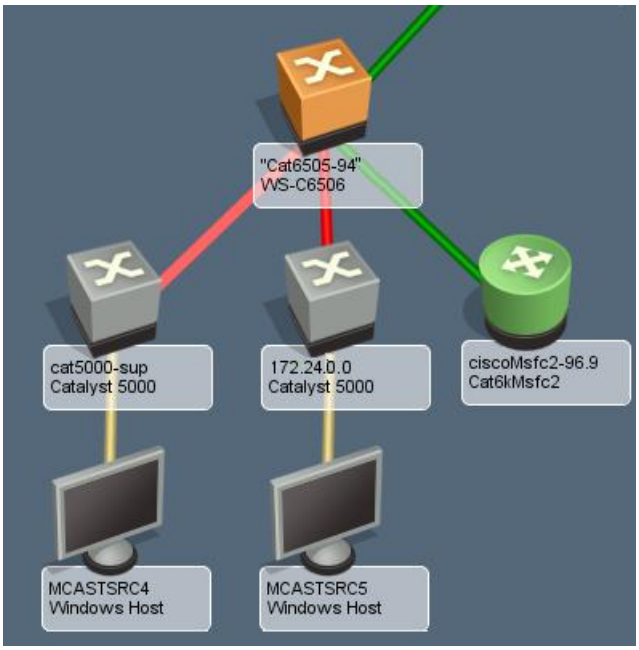
CA Spectrum 支持主板被拔出或发生故障。

在传统的故障隔离方案中，当基于-机箱的设备的主板发生故障时，CA Spectrum 会在所有下游设备模型上生成关键警报。主板出现故障的设备模型还会保持其正常运行状况。但是，此行为不会指出到底是哪个设备发生了故障。

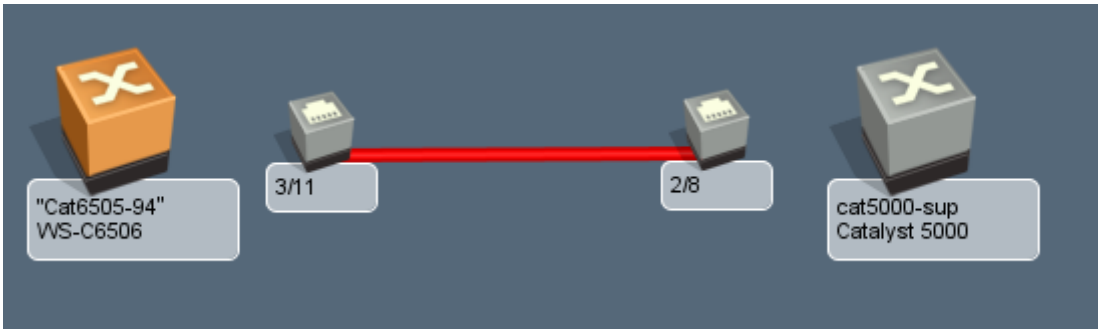
对于同一情况，支持 CISCO-STACK-MIB 的 Catalyst 基于机箱的设备增强了故障隔离功能，可抑制下游设备模型，在主板出现故障的设备模型上生成主要警报，并在主板模型上生成关键警报。与主板模型关联的端口也会被抑制，这样，就不仅能明确指示是哪台设备发生了故障，还能指示是哪个主板出现了故障。

带有下游设备的 Catalyst 设备示例

在以下示例中，连接的设备将“启用活动链路”设置为 TRUE。拔出 Catalyst 主板后，通过该主板连接到端口的设备将会宕掉。该事件会触发 CA Spectrum 以确定故障的原因。在该示例中，两个下游交换机和主机受到了影响。

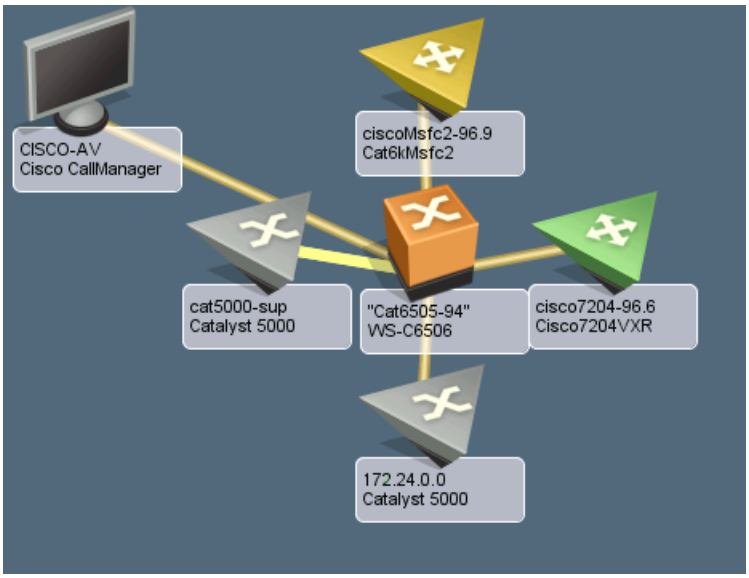


下图显示了“链路信息”视图。“链路信息”视图显示了警报的根本原因。

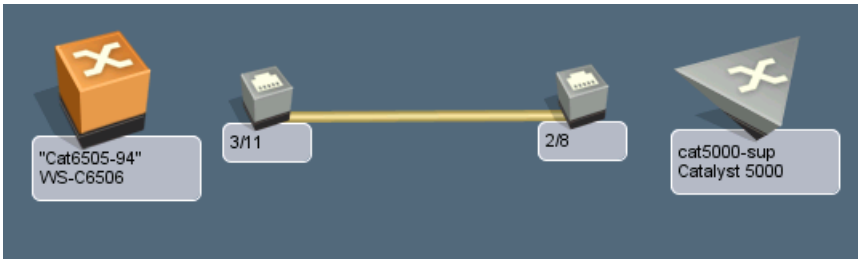


带有下游设备的 Catalyst 设备示例

在以下示例中，连接的设备将“启用活动链路”设置为 FALSE。拔出 Catalyst 主板后，会接收到陷阱，通过该主板连接到端口的设备将会宕掉。该事件会触发 CA Spectrum 以确定故障的原因。在该示例中，两个下游交换机（离页引用）和主机（不在视图中）受到了影响。

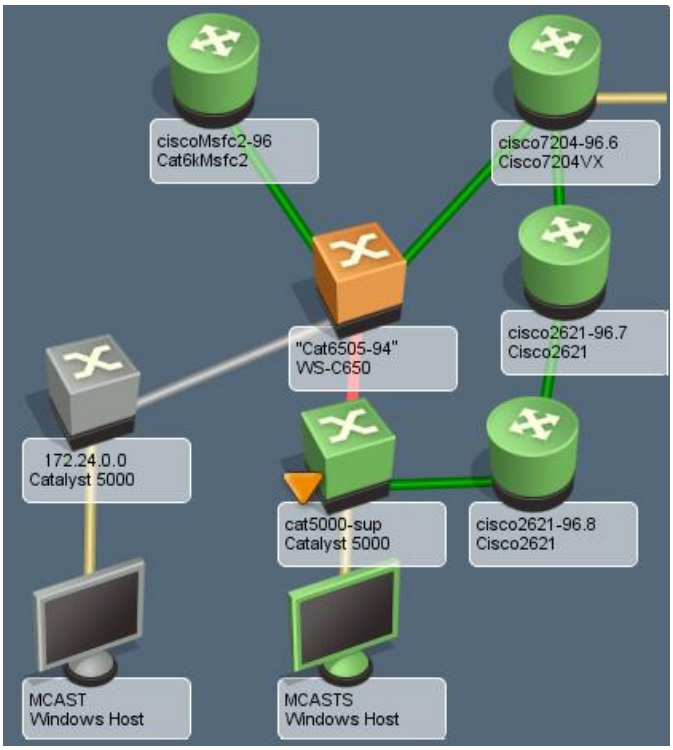


下图显示了“链路信息”视图。“链路信息”视图显示了警报的根本原因。



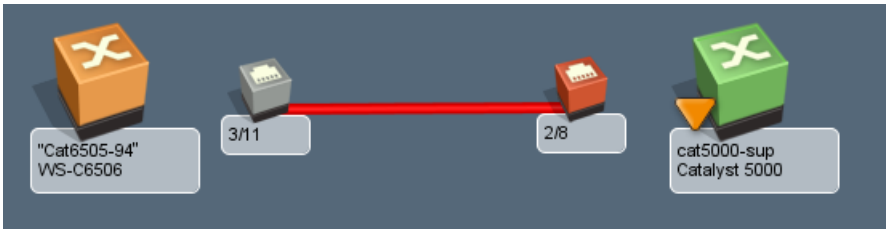
带有配备多管理路径的下游设备的 Catalyst 示例

在以下示例中，连接的设备将“启用活动链路”设置为 TRUE。拔出 Catalyst 主板后，通过该主板连接到端口的设备将会宕掉。该事件会触发 CA Spectrum 以确定故障的原因。在该示例中，一个下游交换机和主机受到了影响。



注意：使用第二个管理路径的交换机会始终保持联系，并警报其端口。

下图显示了“链路信息”视图。“链路信息”视图显示了警报的根本原因。



第 4 章： Cisco 技术支持

此部分包含以下主题：

路由器冗余

通过 CISCO-HSRP-MIB，可以管理 Cisco IOS 专有热待机路由器协议 (HSRP)。

HSRP 让主机看似在使用单个路由器，并且即使实际第一跃点路由器失败，也依然会保持连接。多个路由器参与该协议。它们一起模拟采用静态 IP 地址（也称为虚拟 IP 地址）的单个虚拟路由器。末端主机会将其数据包转发给虚拟路由器。

转发数据包的路由器被称为活动路由器。如果活动路由器出现故障，则待机路由器将替换该活动路由器。HSRP 提供一种机制，可使用参与路由器上的 IP 地址来确定活动和待机路由器。如果活动路由器出现故障，待机路由器就会接管，不会造成主机连接出现重大中断。

HSRP 组建模

CA Spectrum 会为它发现的每个热待机路由器协议 (HSRP) 组创建模型。CA Spectrum 按虚拟 IP 地址标识它们。该虚拟 IP 地址会被添加到 HSRP 组的活动路由器的“冗余排除地址”中。每个 HSRP 组模型都知道 HSRP 组中的活动和待机路由器。

OneClick 使用下列路由器冗余聚焦方法让您查看 HSRP 组成员资格：

资源管理器搜索

提供一个视图，其中显示的 HSRP 组成员带有相应的“活动”或“待机”标签。可以在“资源管理器”选项卡中选择容器，在“内容”面板中选择“拓扑”选项卡，单击聚焦图标，然后选择“路由器冗余”。

定位器搜索

显示适用于 HSRP 组模型的搜索。可以在“定位器”选项卡中打开“路由器冗余”目录。对于每个模型，“内容”面板包含有关 HSRP 组模型的信息，包括虚拟 IP、组 ID 和组成员资格。

HSRP 组成员资格

CA Spectrum 监控每个热待机路由器协议 (HSRP) 组，以查找状态和成员资格更改。CA Spectrum 使用活动路由器设备模型的轮询时间间隔来轮询活动路由器的 HSRP 组表。CA Spectrum 还会响应设备发送的状态更改陷阱。

如果某个路由器故障转移，则会在 HSRP 组模型上断言一个主要警报，指示路由器冗余已丢失，且待机路由器不再可用。CA Spectrum 将在检测到新的待机路由器后清除此警报。

注意：组模型的“信息”选项卡提供了“报告选择更改”设置。如果启用了该设置，则每次选择新的活动路由器时，CA Spectrum 都会生成警报。CA Spectrum 不会清除此警报。

更改 HSRPMode 属性的状态

可以限制对正在通过 HSRP 部署运行的网络设备的 SNMP 请求数，以防止网络性能降低。可以将 HSRPMode 属性的状态设置为下列三种状态之一：

关闭

不轮询 HSRP 表。

被动

HSRP 表在激活时轮询一次。其他时间，CA Spectrum 会依靠陷阱的更新来更新该信息。

Active（活动）

除被动处理之外，HSRP 表每个轮询时间间隔轮询一次。

遵循这些步骤:

1. 从“定位器”选项卡中展开“应用程序模型”。
2. 选择“按名称”。

   此时将打开“搜索”对话框。
3. 在“搜索”对话框的“模型类型”名称文本框中，键入“CiscoHSRPApp”。

   将显示所有 CiscoHSRPApp 设备的列表。
4. 在列表中选择所有设备，然后右键单击选择“实用工具”、“属性编辑器”。

   此时将打开“属性编辑器”对话框。
5. 在左侧窗格中，展开“用户定义”，并单击“添加”超链接。

   此时将打开“属性选择器”对话框。

6. 在筛选文本框中键入“HSRPMode ”，然后单击“确定”。

   属性 HSRPMode 将添加在“用户定义”下。

7. 选择“HSRPMode”，然后单击向右箭头将其移至右侧窗格。

   现在，您可以在右侧窗格中设置 HSRPMode 属性的状态。

8. 在左侧窗格中，展开“SNMP 通信”以选择*“轮询时间间隔(秒)”*，然后单击向右箭头将其移至右侧窗格。

   现在，您可以在右侧窗格中设置“轮询时间间隔”的值。

9. 在右侧窗格中，清除“无更改”，并设置“轮询时间间隔”的值，然后将 HSRPMode 的状态设置为“关闭”、“被动”或“活动”。

您已经更改 HSRPMode 的状态，并在您格局的所有设备模型上设置了“轮询时间间隔”的值。

SNMPv3 设备发现

在具有 VLAN 的 Cisco 交换机上发现 SNMPv3 设备时，不能对每个 VLAN 的索引桥接信息使用 community_string@VLAN_ID 格式。但是，可以创建上下文。

为了让 CA Spectrum 读取桥接信息，请使用以下格式创建这些上下文：

```
vlan-<VLAN_ID>
```

示例：创建 SNMP v3 用户

该示例创建了一个 SNMPv3 用户上下文，使用的是 CA Spectrum 可以阅读的格式：

```
(enable) set snmp user <level1-vlan> nonvolatile

(OUTPUT) Snmp user was set to level1-vlan authProt no-auth  privProt no-priv
```

示例：创建 SNMP 组

该示例创建了一个 SNMP 组上下文，使用的是 CA Spectrum 可以阅读的格式：

```
(enable) set snmp group <v3-level1-vlan> user <level1-vlan> security-model v3
nonvolatile

(OUTPUT) Snmp group was set to v3-level1-vlan user level1-vlan and version v3,
nonvolatile.
```

示例：创建 SNMP 访问组

该示例创建了一个 SNMP 访问组上下文，使用的是 CA Spectrum 可以阅读的格式：

```
(enable) set snmp access <v3-level1-vlan> security-model v3 noauthentication read
<defaultUserView> write <defaultUserView> notify <defaultUserView> nonvolatile

(OUTPUT) Snmp access group was set to v3-level1-vlan version v3 level
noauthentication, readview defaultUserView, writeview defaultUserView,
notifyview defaultUserView context match: exact, nonvolatile.

(enable) set snmp access <v3-level1-vlan> security-model v3 noauthentication read
<defaultUserView> write <defaultUserView> notify <defaultUserView> context
<vlan> prefix nonvolatile

(OUTPUT) Snmp access group was set to v3-level1-vlan version v3 level
noauthentication, readview defaultUserView, writeview defaultUserView,
notifyview defaultUserView context: vlan, context match: prefix, nonvolatile.
```

Syslog 陷阱支持

系统消息日志 (syslog) 协议允许您将来自 Cisco 设备的文本消息发送到网络管理软件。文本消息会作为 SNMP 陷阱发送给 CA Spectrum 事件管理器。通过 Syslog 陷阱支持，路由器设备可以标识文本消息并在必要时上报给警报。Syslog 陷阱支持还允许 Cisco 路由器模型图标传递警报重要级别信息。

如果如 CISCO 设备图标所示发生了警报，就会在“警报日志”中显示 CA Spectrum 警报重要级别和 syslog 消息。

将根据从 0 到 7（从最严重到最不严重）的重要级别范围对 syslog 消息进行分类。警报显示在“警报日志”中。由于这些警报与 CISCO 设备模型关联，因此相应的模型图标会根据警报的重要级别更改颜色并闪烁。

下表列出了重要级别代码及其说明：

重要级别	说明
0	紧急 - 系统不可用
1	警报 - 需要立即采取行动
2	关键 - 关键状况
3	错误 - 错误状况

重要级别	说明
4	警告 - 警告状况
5	通知 - 正常但重要的状况
6	信息 - 仅信息性消息
7	调试 - 仅在调试期间出现的消息

下表列出了 syslog 消息重要级别到 CA Spectrum 警报重要级别的映射关系：

警报重要级别	颜色
0-1	红色
2-3	橙色
4	黄色

警报重要级别为 5 到 7 的消息不会生成警报，因为它们属于次重要。设施（硬件设备、协议、模块或系统软件）会列出这些消息。

设施代码是消息引用的设施的缩写。设施可能是某个特定的硬件设备、协议或软件。在每个设施之内，消息根据重要级别（从最高 (0) 到最低 (7)）列出。*助记符*是用来唯一标识消息的大写字符串。

每个消息后面会显示解释和建议的操作。只有在系统保持运行状态时，才会显示消息。以下行是一个 syslog 消息示例：

01/01/2001,18:31:15:SYS-5-MOD_INSERT:模拟 5 已插入。

对该消息的解析如下：

- 01/01/2001,18:31:15 是错误发生的日期和时间（如果设置了系统日志消息，会出现该信息）。
- SYS 是设施类型。
- 5 是重要级别，表示它处于正常但重要的状况。
- MOD_INSERT 是唯一标识消息的助记符。
- “模拟 5 已插入”是说明状况的消息文本。

系统消息日志 (syslog) 程序会在日志文件中保存该系统消息，或将消息指向其他设备。通过 Syslog 软件可以执行以下功能：

- 保存日志信息，以用于监控和故障排除
- 选择日志记录信息的类型和目标

默认情况下，交换机会将正常但重要的系统消息记录到其内部缓冲区，并将这些消息发送给系统控制台。您可以根据设施的类型和重要级别指定必须以何种方式保存系统消息。可对消息标记时间戳，以改进实时调试和管理。

将 Syslog 陷阱映射添加到 CA Spectrum

CA Spectrum 包括 SpectroSERVER 将 Cisco syslog 陷阱映射到 CA Spectrum 事件需使用的三个文本文件。

下表显示了这些 syslog 文本文件：

设备 Syslog 消息	文本文件
Cisco 路由器	<$SPECROOT>/SS/CsVendor/Cisco_Router/Rtr.txt
Catalyst 交换机	<$SPECROOT>/SS/CsVendor/Ctron_CAT/Switch.txt
Cisco PIX	<$SPECROOT>/SS/CsVendor/CiscoPIX/Pix.txt

这些文本文件的每一行中都包含将 syslog 消息映射到 CA Spectrum 事件的相关信息。这些行采用以下格式（使用单个空格作为字段之间的分隔符）：

<设施> <重要级别> <助记符> <事件代码>

遵循这些步骤:

1. 向包含之前信息的文件添加行。

   例如，为了增加对 Cisco 路由器 %SPE-3 SM_DOWNLOAD_FAILED syslog 消息的支持，请将以下行添加到 Rtr.txt 文件中：SPE 3 SM_DOWNLOAD_FAILED 0xffff0001，其中 0xffff0001 是您选择的任意代码。

2. 为事件和警报创建“事件格式”和“可能原因”文件。

   在本示例中，创建了 Eventffff0001 和 Probffff0001。可以在这些文件中输入任意文本。以下变量数据可以从“事件消息”中读取，并显示在“事件格式”文件中：

   ```
   {S 1} - 设施
   {T T1_210017 2} - 重要级别
   {S 3} - 助记符
   {S 4} - 消息
   ```

3. 添加事件至警报的映射。使用前一个示例，添加以下行：

   0xffff0001 E 50 A 2,0xffff0001

   注意：在 Rtr.txt 文件所在的同一目录中必须存在 EventDisp 文件。

   如果 SpectroSERVER 接收到此 syslog 陷阱，会生成一个橙色警报。

注意：可以在 SpectroSERVER 运行时执行该配置。SpectroSERVER 会每分钟检查一次对 *.txt 文件所做的更改。

Syslog 消息筛选

通过“Cisco Syslog 消息筛选 OneClick”视图，可以筛掉不需要的 syslog 消息。筛选 syslog 消息可以阻止不需要的警报或事件。SS/CsVendor/SYSLOG 包含八个文件，分别对应不同的筛选类别。要选择助记符所属的筛选类别，可将助记符移至所需的 SS/CsVendor/SYSLOG 文件。

下表显示了 SS/CsVendor/SYSLOG 文件和相应的筛选：

文件	相应的筛选
Syslog0	Protocol_Filter
Syslog1	System_Filter
Syslog2	Environment_Filter
Syslog3	Software_Filter
Syslog4	Security_Filter
Syslog5	Hardware_Configuration_Filter
Syslog6	Connection_Configuration_Filter
Syslog7	PIX_Firewall_Filter

注意：助记符可与任意筛选交换。

对这些筛选的说明如下：

Protocol_Filter

影响 Syslog0 文件。将此筛选设置为 True，可以筛选其设施涉及到协议的所有 syslog 消息。例如，BGP、OSPF、SNMP、SPANTREE。

System_Filter

影响 Syslog1 文件。将此筛选设置为 True，可以筛选其设施涉及到系统的所有 syslog 消息。例如，CBUS、MEMSCAN。

Environment_Filter

影响 Syslog2 文件的内容。将此筛选设置为 True，可以筛选出涉及到环境变量的所有 syslog 消息。例如，LCFE、LCGE。

Software_Filter

影响 Syslog3 文件的内容。将此筛选设置为 True，可以筛选出涉及到内部软件的所有 syslog 消息。例如，PARSER、RSP、GRPGE。

Security_Filter

影响 Syslog4 文件的内容。将此筛选设置为 True，可以筛选出涉及到系统安全性的所有 syslog 消息。例如，RADIUS、SECURITY。

Hardware_Configuration_Filter

影响 Syslog5 文件的内容。将此筛选设置为 True，可以筛选出涉及到设备硬件配置的所有 syslog 消息。例如，IOCARD、MODEM、DIALSHELF。

Connection_Configuration_Filter

影响 Syslog6 文件的内容。将此筛选设置为 True，可以筛选出涉及到设备连接配置的所有 syslog 消息。例如，MROUTE、ISDN、X25。

PIX_Firewall_Filter

影响 Syslog7 文件的内容。将此筛选设置为 True，可以筛选出涉及到 Cisco PIX Firewall 设备的所有 syslog 消息。

隧道接口建模

CA Spectrum 可以对支持 CISCO-IPSEC-FLOW-MONITOR-MIB 和 CISCO-IPSEC-MIB 的 Cisco 设备进行 Cisco IPSec 隧道接口管理。这些 MIB 可用于 Cisco 固件版本 12.1 (4) 或更高版本。

CA Spectrum 支持以下 IPSEC VPN 管理功能：

- 隧道接口的建模（站点对站点）
- 自动连接映射
- 接口模型标识
- 接口模型老化
- 链路断开陷阱关联
- 隧道接口的状态监控

以下属性可控制 IPSEC VPN 管理：

- CreateTunnelLIf
- Interface_Polling_Interval

配置 CreateTunneLIf

CreateTunnelLIf 属性指示是否为设备上定义的每个 IPSec 隧道创建隧道接口模型。如果为 TRUE，则表明 CA Spectrum 会在接口重新配置期间读取外部表。这些外部表定义了当前的隧道接口。CA Spectrum 将创建相应的隧道接口模型，以作为相关物理接口的子接口。

遵循这些步骤:

1. 导航到“定位器”选项卡，展开“应用程序模型”文件夹，并双击“按设备 IP 地址”。

   将打开“搜索”对话框。

2. 输入要配置的支持 Cisco IPSec- 的设备的 IP 地址，然后单击“确定”。

   设备将显示在“内容”面板中。

3. 从“内容”面板中选择 CiscIPSecExtAp 设备。
4. 在“组件详细信息”面板中选择“属性”选项卡。
5. 在左侧窗格中选择 CreateTunneLIf 并单击向右箭头按钮，将其移至右侧窗格。
6. 在右侧窗格中双击 CreateTunneLIf 以更改其值。

   注意：将 CreateTunneLIf 设置为 No 会禁用 Cisco IPSec 隧道建模。

配置 Interface_Polling_Interval

Interface_Polling_Interval 属性定义隧道表轮询时间间隔（以秒为单位）。如果设置为 0，则不会轮询表。

遵循这些步骤:

1. 导航到“定位器”选项卡，展开“应用程序模型”文件夹，并双击“按设备 IP 地址”。

   将打开“搜索”对话框。

2. 输入要配置的支持 Cisco IPSec- 的设备的 IP 地址，然后单击“确定”。

   设备将显示在“内容”面板中。

3. 在“内容”面板中选择该设备。
4. 在“组件详细信息”面板中选择“属性”选项卡。
5. 在左侧窗格中选择 Interface_Polling_Interval 并单击向右箭头按钮，将其移至右侧窗格。
6. 在右侧窗格中双击 Interface_Polling_Interval 以更改其值。

VLAN 索引支持

CA Spectrum 可以测试特定 CISCO 设备是否支持 VLAN 索引团体字符串。VLAN 索引团体字符串可防止身份验证失败陷阱。

如果 CISCO 设备支持 VLAN 索引团体字符串，VLANIndexingSupported (0x4a0037) 属性值将设置为 Supported 1。

如果 Cisco 设备不支持 VLAN 索引团体字符串，VLANIndexingSupported (0x4a0037) 属性值将设置为枚举 NotSupported 0。不会执行进一步的 VLAN 索引读取操作。该配置可防止生成身份验证失败陷阱。

如果由于缺少 CISCO 设备的 VLANS 信息而未对该设备进行测试，则请测试该设备。在设备上执行发现，或要启用 VLAN 覆盖，请将 VLANIndexingSupported (0x4a0037) 属性值设置为 Test 2。

如果设备的配置更改为支持 VLAN 索引团体字符串，请通过属性编辑器在该设备的 Transparnt_App 模型上将该属性值更改为 VLANIndexingSupported (0x4a0037)。

第 5 章： CiscoWorks 集成

此部分包含以下主题：

CiscoWorks 简介

通过 CA Spectrum r9.2.1，CA Spectrum 可与 Cisco 的 CiscoWorks 应用程序进行无缝集成。CiscoWorks 提供了一个功能强大的工具来管理 Cisco 设备。

现在，可以在 CiscoWorks 中选择 Cisco 设备并直接进入“设备中心”页。

CiscoWorks 集成

“OneClick 管理”网页提供了对“CiscoWorks 配置”页面的访问。在该页面中，可以设置 CiscoWorks Web 服务器的名称和端口，并将该信息保存到 devman/config 目录中的 ciscoworks-config.xml 文件中。只有在配置文件中设置了服务器名称后，才能创建相应的菜单选项。